Collaborative Testing Services, Inc
FORENSIC TESTING PROGRAM

P.O. Box 650820
Sterling, VA 20165-0820
e-mail: forensics@cts-interlab.com
Telephone: +1-571-434-1925
Web site: www.cts-forensics.com

Computer Hard Drive - Windows Analysis Test No. 23-5561/2 Summary Report

Participants were provided with data yielded from an extraction of a Windows 10 Computer Hard Drive. Additionally, participants in the 5562 test received a physical USB drive. Examiners were asked to analyze the sample material and answer questions utilizing their own tools and methods. Data were returned from 136 participants, 48 of which also returned results associated with the physical USB. These results are compiled in the following tables:

Report Contents: Page

This report contains the data received from the participants in this test. Since these participants are located in many countries around the world, and it is their option how the samples are to be used (e.g., training exercise, known or blind proficiency testing, research and development of new techniques, etc.), the results compiled in the Summary Report are not intended to be an overview of the quality of work performed in the profession and cannot be interpreted as such. The Summary Comments are included for the benefit of participants to assist with maintaining or enhancing the quality of their results. These comments are not intended to reflect the general state of the art within the profession.

Participant results are reported using a randomly assigned "WebCode". This code maintains participant's anonymity, provides linking of the various report sections, and will change with every report.

Manufacturer's Information

The Computer Hard Drive – Windows Analysis test consisted of evidence data acquired from a Windows 10 computer hard drive The extracted data was provided in an E01 file format. Participants were asked to examine the extracted data as it relates to a simulated scenario utilizing their own software and methods.

All participants enrolled in the 23-5562: Computer Hard Drive – Windows & Removable Media Storage Analysis test received an additional component, a physical USB drive shipped in a sealed manila envelope. These participants were also asked to perform evidence acquisition, extraction, and analysis.

SAMPLE PREPARATION/VALIDATION
A scripted scenario discussing a case related to a suspected computer intrusion was created to generate user data on a Windows Hard Drive. The execution of the test production took place within the following date range, 11 February 2023 and 9 March 2023. Multiple system and third-party applications were used to perform activities and generate the intended artifacts. A USB device was used to add user activity on the computer and onto the removable media storage device provided to participants enrolled in 23-5562.

Data from the subject computer's hard drive was acquired and analyzed using commercial and open-source industry standard forensic tools. Following sample validation, the image was uploaded to the CTS Portal for download by test participants. MD5 digest (cryptographic checksum, or 'hash') was calculated for the compressed data and provided to participants to enable validation of a successful download of the file(s).

The subject USB flash drive was duplicated (cloned) using validated forensic duplication hardware and the SHA1 digest for each duplicated flash device was validated prior to shipment to participants.

VERIFICATION: The combination of internal test validation and the responses received from predistribution testing structured the final questions utilized in this test. The following list of tools were utilized in the validation of this test: Autopsy 4.20.0, EnCase 8.11, FTK Imager 4.5.0.3, RegRipper 3.0, ExifTool 12.05, PhotoRec 7.2, PECMD 1.5.0, HxD 2.4.0.0 and 7zip 19.0. CTS does not endorse any particular tools.

PLEASE NOTE: Questions marked with asterisks (**) did not show a clear consensus during preliminary review of the participant's responses. Further information and discussion will be available in the final report.

Manufacturer's Information, continued

SCENARIO PROVIDED TO PARTICIPANTS

Sister Mary Gallagher (a teacher at St. Clotilde's School) was reviewing students' scores when she noticed several of the grades in the school's student information system (SIS) were different from those she remembered entering. Investigation by school administrators discovered discrepancies in grades for many other students. Review of SIS logs determined multiple students' grades had been changed by a SIS account belonging to one of the school's guidance counselors, Stan Mackey.

Mackey denied accessing the students' accounts, but did remember receiving emails related to his SIS account. The SIS logs showed Mackey's account had been accessed remotely from Internet Protocol (IP) addresses allocated to AT&T. Mackey denied having an AT&T account.

Administrators at St. Clotilde's contacted the city police who initiated an investigation. Information provided by AT&T in response to a subpoena showed, at the time of the alleged accesses, the IP addresses in question had been assigned to subscriber John Lightman, 333 South Arden Boulevard.

The police obtained a warrant to search the above residence for evidence of the computer intrusion. During the search they seized a laptop computer and a USB flash storage device.

You are being provided with:
- a copy of the forensic image acquired by the police of the laptop seized during the search, and
- the USB flash storage device seized by police during the search (5562 only)

You have appropriate legal authority to examine the device for evidence related to the computer intrusion and to perform analysis to answer the following questions (5561).

You have appropriate legal authority to examine both devices for evidence related to the computer intrusion and to perform analysis to answer the following questions (5562). The USB device should be handled as an item of original evidence provided to your lab for acquisition and analysis (5562).

Manufacturer's Information, continued

Question ***Manufacturer's Expected Response***

1** **Provide the acquisition SHA-1 hash for the provided image (decompressed image file), 23-5561.E01.**
B5D7DDA9B578E937f1ADE6F90C13CFBBF7CAD8F1

2 **How many partitions are on the hard drive (device imaged as 23-5561.E01)? Provide a NUMERIC response (e.g., 1, 2, 3).**
2

3 **What is the hostname (Computer name) for this computer?**
DAVID-LAPTOP

4 **What operating system (include version and edition) was installed on this computer?**
Windows 10 Home

5 **Who is the registered owner of this operating system installation?**
David Lightman

6 **What "replaceString" did user David Lightman LAST use in Notepad, as recorded by the user's registry?**
st.clotildes

7 **When was the computer LAST shutdown gracefully? Provide your response in UTC+0, using the date/time (24-hour) picker which presents the date in the following format: YYYY-MM-DD.**
2023-03-08 12:45

8 **Was the Guest user account ever logged into?**
No

9 **What is the Security ID (SID) of the registered owner's user account?**
S-1-5-21-3501254099-4204809888-2000606956-1007

10 **What is the configured time zone?**
Eastern Standard Time, or UTC-5

11 **Provide the make and model of device used to capture the photo with hash b793ec04a43c6ff0b09d52e0d14c7bb0ecafc712.**
Google Pixel 5

12 **On March 6, 2023 (3/6/23), at 7:56 PM (local time) David Lightman sent an image (photo) via WhatsApp Chat message to another party. Provide the large font text at the top of (in) the image.**
Gradebook – Grades – Quarter 1

13 **What website did user David Lightman visit with the Google Chrome browser on 25 February 2023 (2023-02-25) at 21:52:02 GMT? Provide the full URL.**
http://stclotildes.institute/sample-page/

14 **What is the path and filename of the file containing the term "Xenoglaux"? (e.g., /directory/subdirectory/name.extension)**
C:\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf

Manufacturer's Information, continued

Question ***Manufacturer's Expected Response***

15 **Describe the difference between the URLs in the images attached to the email message sent by David Lightman March 5, 2023 3:34 PM**
A period (dot) is present between the text "st" and "clotildes" in one of the URLs.

16 **Who is listed as the author of crafty.doc?**
David Lightman

17 **On what date and time, and to what user account was the LAST successful login to this computer? Provide your response in UTC+0, using the date/time (24-hour) picker which presents the date in the following format: YYYY-MM-DD.**
Date and Time: 2023-03-08 12:44
User Account: David Lightman

18 **What is the original (pre-deletion) path and name of $IB5V1XN.jpg (found in the user David Lightman's Recycle Bin on C:)? (e.g., /directory/subdirectory/name.extension)**
C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg

19** **What user account (name) is the owner of C:\Users\Mark\Desktop\qujysbx38kia1.jpg?**
David Lightman

20 **What is the filetype (MIME type) for the file with SHA-1 hash c9abb4c11ccec6950fb58f146ac84269dedc2223?**
Portable Network Graphic or PNG

21** **Provide the name of the regular file (i.e. NOT hidden, deleted, aliased, etc.) in C:\Windows\System32\drivers with the earliest (oldest) ($STANDARD_INFORMATION Attribute) created time.**
wincatyawn.sys

22** **Describe the content of the file identified in Question 21 (regular file in C:\Windows\System32\drivers with the earliest (oldest) ($STANDARD_INFORMATION Attribute) created time).**
"A picture of a cat" and variations describing the same information.

23 **What email client and version did the administrator install?**
Mozilla Thunderbird (x64 en-US) v. 102.8.0

24** **Provide the email addresses for the two email accounts configured in the user installed IMAP email client for user David Lightman.**
david.lightman75@outlook.com and
admin@clotildes.institute and/or admin@st.clotildes.institute

25 **Provide the email address of the person with whom user David Lightman communicated with about changing grades.**
Email Address: jennymack16@outlook.com
Name of Person: Jennifer Mack

26 **To what email address was an email message sent containing "Expired Password - Reset Required" in the subject?**
stephen.falken@stclotildes.institute

Manufacturer's Information, continued

Question ***Manufacturer's Expected Response***

27 **In the image, there are several red bordered jpeg image files of animals. Locate one of these photos and provide the black font text that appears in the photo.**
2023A, 2023R or 2023T

28 **Provide the GPS coordinates where the photo racetrack.jpg was taken. Provide your response in the format ##.##### (Indicate directionality as N or S), ##.##### (Indicate directionality as E or W).**
39.2421 N, 77.9732 W and varying formats that represent the same location.

29 **In unallocated space on the "C" (second) partition on the computer hard drive is a deleted jpeg image of a black and white F-18 aircraft with "NASA" on the tail flying in a dark blue sky. The MD5 hash of this file is ce47fda2b3b78478a9c0610ca859bcda. Provide the SHA1 hash of this file.**
28A7CA82C03C0C6F686E05DC951BC78A7679334B

30 **In unallocated space on the "C" (second) partition on the computer hard drive is a deleted jpeg image of four owls standing on the ground. The MD5 hash of this file is 8f3faa6a67485cd264a74c33e70808d8. Provide the SHA-1 hash of this file.**
E90E098A1A3BCB853FE255E6820B0084B1381048

31 **Locate the keyword that begins "Iera", continues 6 letters, and ends "nae". Provide the word and location (path and filename) where it is found. Please note, the keyword starts with a capital letter "I" like in the word 'India'. (e.g., ill, +6 letters, + ion, = illustration)**
Word: Ieraglaucinae,
Location: C:\Windows\System32\config\SOFTWARE:family\subfamily , OR
C:\Windows\System32\config\SOFTWARE.log

32 **According to user David Lightman's registry hive 'most recently used' records, what "Rich Text File" did he open?**
superpostiion.rtf

33 **According to the data IN the associated prefetch file, when was NOTEPAD.exe LAST executed? Provide your response in UTC+0, using the date/time (24-hour) picker which presents the date in the following format: YYYY-MM-DD.**
2023-03-08 00:21

Manufacturer's Information, continued

Removable Media Analysis: *USB Drive*
Test No. 23-5562

Question ***Manufacturer's Expected Response***

34 **Provide the SHA256 hash for the USB device.**
6B5C8BD30A01B303A968D88F467192BF0CD4D21659E95D8A0A38D667E1B31AB2

35 **How many active partitions are on the device? Provide a NUMERIC response (e.g., 1, 2, 3).**
3

36 **What type of filesystem is on the second partition (named "NEW VOLUME")?**
exFAT

37 **What is the parent directory for ItchyBlackKoala.xls?**
DarkFierceLocust

38** **What is the filetype of the file with SHA-1 hash 9b810eb160adcb2cabac5aa318b36ea34244e281?**
7-zip file

39 **In unallocated space on the USB flash drive is a jpeg photo file of a white rock on a black background. The SHA-1 hash of this file is 446b6fe695c878b6651d58378acc9a2503d50048. Provide the MD5 hash of this file.**
73BB4AE1D3C52A8B2B371D5CB059D145

40 **A directory of files was created on the USB on 7 March 2023 (2023-03-07) at 02:28:38 (UTC+0). Provide the name of the directory.**
spoof reset page

41 **Compare the "Created" and "Modified" timestamps of the directory and files referenced in question 40. What do the relative "Created" and "Modified" timestamps indicate about the files' placement on the USB?**
"They were copied from another volume" and variations of this text providing a similar description.

42 **Provide the URL contained in the file with SHA-1 hash 9f2271430d2cd6d897024ee589e8c9db192d8af2.**
http://portal.st.clotildes.institute/PasswordReset.php

43 **Provide the SHA256 hash of GracefulGrievingUrchin.rar?**
B53E2BE6204E0645558D79333BFD17AFF33DE31E06E178C6CF243BB175EFDA98

44 **What is the filetype (MIME) of GracefulGrievingUrchin.rar?**
jpeg (or jpg) image file

Summary Comments

The purpose of this Computer Hard Drive – Windows Analysis Test is to allow participants to evaluate their proficiency in analyzing digital artifacts using their own tools and methods. The participants were provided with a scripted scenario, the data extracted from a Windows 10 computer hard drive, and a series of questions related to the extracted data. Additionally, participants enrolled in the 23-5562: Computer Hard Drive – Windows & Removable Media Storage Analysis test received a physical USB drive. These participants were asked to perform evidence acquisition, extraction, and analysis. (See Manufacturer's Information for preparation details, test scenario, and test questions.)

The participants were requested to analyze various digital artifacts including: image details, settings, external media, native and third-party applications, communications, and web browser history.

A total of 88 participants returned results for the 5561 Computer Hard Drive - Windows Analysis test. Of the 33 total questions, three did not reach a consensus response, questions #1, #19 and #24. Question #1 asked for the SHA-1 hash of the decompressed image file. The majority reported the expected hash and 25 participants reported the hash of the compressed image file (Zip file). Question #19 asked for the user account name of the owner of a specified file. The majority reported the expected response of David Lightman but 54 participants reported Mark. Question #24 asked for the two email accounts configured in the user install IMAP email client for user David Lightman. The majority reported one of the two expected email addresses, david.lightman75@outlook.com. However, only 73% of those participants also reported the other expected email address of admin@clotildes.institute or admin@st.clotildes.institute.

A total of 48 participants returned results for the 5562 Removable Media Storage Analysis test. Of the eleven questions, only question #38 did not achieve a consensus response. The goal of this question was to find the filetype of the file associated with a specified hash value. Approximately 74% reported the expected response of 7-Zip whereas others reported system file.

Detailed explanation and screenshots of expected responses can be found within Tables 1 and 2 under the "Expected Response Explanation" section for each question.

Participants are encouraged to follow their laboratory's policies and procedures when evaluating their responses to these proficiency test questions.

Report Amendment for 9 October 2023: After further review and communication with our expert, some of the wording in questions # 21 and 22 were deemed ambiguous and potentially misleading. These questions requested that the participant provide the name of the regular file (i.e. NOT hidden, deleted, aliased, etc.) in C:\Windows\System32\drivers with the earliest (oldest) ($STANDARD_INFORMATION Attribute) created time and the question 22 asked for the participant to describe the content of the file identified in question 21. The term "regular" was ambiguous and the further clarification offered in the question "(i.e. NOT hidden, deleted, aliased, etc.)" should not have included the descriptor "Not aliased." For these reasons, highlighting of inconsistencies from the expected response (also the consensus result) are removed.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 1 - Examination Questions

Question 1: Provide the acquisition SHA-1 hash for the provided image (decompressed image file), 23-5561.E01.

Manufacturer's Expected Response: B5D7DDA9B578E937f1ADE6F90C13CFBBF7CAD8F1

WebCode Test	Response ** Inconsistencies not highlighted; No consensus achieved **
2A9WQN-5561	F75A656549ECF8FD5453FAA9514FD5BEDA58A55F
2P2VAR-5561	F75A656549ECF8FD5453FAA9514FD5BEDA58A55F
2PJFNF-5562	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
2VQ8RL-5562	f75a656549ecf8fd5453faa9514fd5beda58a55f
2ZFN6X-5561	F75A656549ECF8FD5453FAA9514FD5BEDA58A55F
3CDK6E-5562	B5D7DDA9B578E937F1ADE6F90C13CFBBF7CAD8F1
3DPEPK-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
3M9X4P-5561	b5d7dda9b578e937f1adc6f90c13cfbbf7cad8f1
42BM2N-5561	F75A656549ECF8FD5453FAA9514FD5BEDA58A55F
48GFVJ-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
4U7ZP2-5562	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
649HZ6-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
68RW46-5562	b5d7 dda9 b578 e937 f1ad e6f9 0c13 cfbb f7ca d8f1
6DZZCR-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
6MKCN6-5562	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
6Q2RXW-5562	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
6Q4JPC-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
6QKH3A-5562	f75a656549ecf8fd5453faa9514fd5beda58a55f
6TR3NP-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
72ZUTD-5561	B5D7DDA9B578E937F1ADE6F90C13CFBBF7CAD8F1

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 1 - Examination Questions

WebCode Test	Response ** Inconsistencies not highlighted; No consensus achieved **
78PAK7-5562	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
7JUP4F-5561	65NGkzkj5t4p2vct6vx3nfrjk7
7PQ8PM-5562	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
7XZLMH-5562	f75a656549ecf8fd5453faa9514fd5beda58a55f
82VWX9-5562	F75A656549ECF8FD5453FAA9514FD5BEDA58A55F
83AEYT-5562	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
8CB97J-5561	F75A656549ECF8FD5453FAA9514FD5BEDA58A55F
8LJ9TK-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
96TUNQ-5561	F75A656549ECF8FD5453FAA9514FD5BEDA58A55F
98ZV8C-5561	F75A656549ECF8FD5453FAA9514FD5BEDA58A55F
99QBZK-5562	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
9AJ8JM-5561	7b58342be594965e8feeaf9768a167c90547ffb8
9J9Q8U-5562	65NGKZKJ5T4P2VCT7KUVCT6VX3NFRJK7
A8QHYB-5562	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
A8VQBZ-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
ABK3AJ-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
ACTERK-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
ADYU2Y-5562	B5D7DDA9B578E937F1ADE6F90C13CFBBF7CAD8F1 (decompressed image file) F75A656549ECF8FD5453FAA9514FD5BEDA58A55F (compressed image file)
AKG6BT-5562	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
AM94QQ-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
BFKZWF-5562	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
BQRG78-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 1 - Examination Questions

WebCode Test	Response ** Inconsistencies not highlighted; No consensus achieved **
C4LMC9-5562	B5D7DDA9B578E937F1ADE6F90C13CFBBF7CAD8F1
C897D8-5561	F75A656549ECF8FD5453FAA9514FD5BEDA58A55F
CF2CBE-5562	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
CKAXYB-5561	F75A656549ECF8FD5453FAA9514FD5BEDA58A55F
CP6N6M-5561	F75A656549ECF8FD5453FAA9514FD5BEDA58A55F
D7PUVD-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
DB6AM4-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
DGVH9K-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
DXVP3C-5562	f75a656549ecf8fd5453faa9514fd5beda58a55f
E2RHRZ-5562	B5D7DDA9B578E937F1ADE6F90C13CFBBF7CAD8F1
E4ZNBG-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
EV7HHF-5561	B5D7DDA9B578E937F1ADE6F90C13CFBBF7CAD8F1
F3JVRX-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
FZVEJB-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
G973T4-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
GJ39KG-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
GYTEQP-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
HQVXJW-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
HUFQTD-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
HW2LD2-5562	[Participant did not return results for this question.]
J84AQF-5562	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
JE9W33-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 1 - Examination Questions

** Inconsistencies not highlighted; No consensus achieved **

WebCode Test	Response
JGBUAC-5562	Hash Calc SHA1: f75a656549ecf8fd5453faa9514fd5beda58a55f FTK Imager SHA1: b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1 FTK Imager produces different MD5 and SHA1 due to including the CRC check in an E01. This means it will be different from HashCalc because HashCalc will look at the file as a whole including the CRC check.
JJDU63-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
JL32PY-5562	B5D7DDA9B578E937F1ADE6F90C13CFBBF7CAD8F1
JLRZA6-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
JPKFX7-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
KR28JR-5562	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
KR4V3R-5561	B5D7DDA9B578E937F1ADE6F90C13CFBBF7CAD8F1
KXRBW6-5562	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
KZVDDT-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
LDKC3B-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
M9HYHY-5561	B5D7DDA9B578E937F1ADE6F90C13CFBBF7CAD8F1
MF4Q7B-5561	f75a656549ecf8fd5453faa9514fd5beda58a55f
MF8B24-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
NADTWE-5561	F75A656549ECF8FD5453FAA9514FD5BEDA58A55F
NE7TEF-5562	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
NTANM4-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
NTZJR4-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
P3ACZC-5561	F75A656549ECF8FD5453FAA9514FD5BEDA58A55F
P79FU7-5561	B5D7DDA9B578E937F1ADE6F90C13CFBBF7CAD8F1
P8ZNUA-5561	5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
PFEMA7-5562	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
PFVN93-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 1 - Examination Questions

** Inconsistencies not highlighted; No consensus achieved **

WebCode Test	Response
PLGGK2-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
PPMYM4-5562	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
PTKDEZ-5562	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
PUTRGY-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
PWJXV6-5561	b5d7dda9b578e937fladebf90c13cfbbf7cad8f1
Q2CFQV-5561	B5D7DDA9B578E937F1ADE6F90C13CFBBF7CAD8F1
Q33NQX-5561	B5D7DDA9B578E937F1ADE6F90C13CFBBF7CAD8F1
Q3RHY2-5561	F75A656549ECF8FD5453FAA9514FD5BEDA58A55F
QMR3Q2-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
QRJAR3-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
QTHAXU-5561	f75a656549ecf8fd5453faa9514fd5beda58a55f
RAK67E-5562	B5D7DDA9B578E937F1ADE6F90C13CFBBF7CAD8F1
RBBDCA-5562	B5D7DDA9B578E937F1ADE6F90C13CFBBF7CAD8F1
RGH4EF-5562	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
RRMUMV-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
RRXTDK-5562	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
RV3JKZ-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
TC4JAF-5562	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
TCGEBD-5561	723b38249ecdc873485e89909219504b
TEPC2R-5562	B5D7DDA9B578E937F1ADE6F90C13CFBBF7CAD8F1
TKFNZV-5561	B5D7DDA9B578E937F1ADE6F90C13CFBBF7CAD8F1
TNEXBT-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 1 - Examination Questions

** Inconsistencies not highlighted; No consensus achieved **

WebCode Test	Response
TVF9MD-5562	B5D7DDA9B578E937F1ADE6F90C13CFBBF7CAD8F1
TX22EP-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
U3RQC6-5561	F75A656549ECF8FD5453FAA9514FD5BEDA58A55F
UKBK6E-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
URA8XZ-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
UVZCUQ-5562	B5D7DDA9B578E937F1ADE6F90C13CFBBF7CAD8F1
V4KY4K-5562	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
VCE6WL-5561	F75A656549ECF8FD5453FAA9514FD5BEDA58A55F
VJH9N7-5561	B5D7DDA9B578E937F1ADE6F90C13CFBBF7CAD8F1
VTZR3B-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
VVVB8V-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
WC9E49-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
WD8DHB-5561	f75a656549ecf8fd5453faa9514fd5beda58a55f
WK4CUH-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
WNN64Y-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
WX2YKZ-5561	b5d7dda9b578e937flade6f90c13cfbb7cad8f1
WZGLVL-5562	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
XA2A8Z-5562	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
XEVDXV-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
XJ99G2-5562	B5D7DDA9B578E937F1ADE6F90C13CFBBF7CAD8F1
XQ9B22-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
XVDHZK-5562	[Participant did not return results for this question.]

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 1 - Examination Questions

** Inconsistencies not highlighted; No consensus achieved **

WebCode Test	Response
XWDAB7-5561	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
XX78KX-5561	65NGKZKJ5T4P2VCT7KUVCT6VX3NFRJK7
Y63G92-5562	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
YDJQ3P-5561	f75a656549ecf8fd5453faa9514fd5beda58a55f
YPNENR-5562	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
ZPR26J-5561	f75a656549ecf8fd5453faa9514fd5beda58a55f

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 1 - Examination Questions

Question 1: Provide the acquisition SHA-1 hash for the provided image (decompressed image file), 23-5561.E01.

Consensus Result:

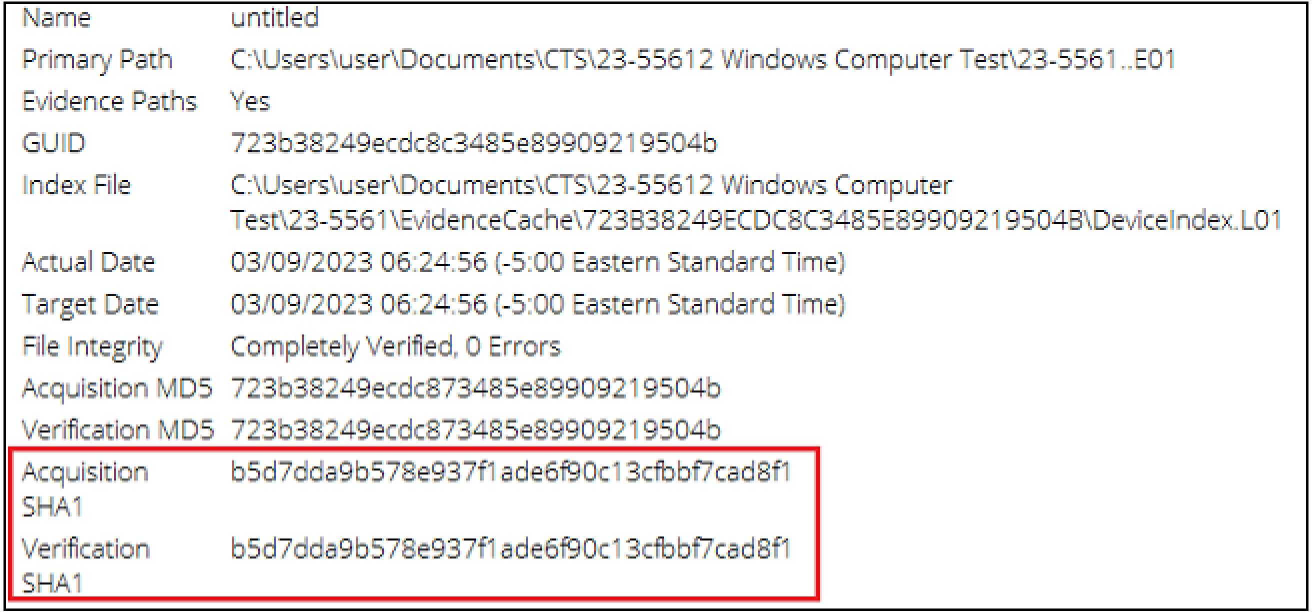
A consensus was not achieved for this question. One hundred participants (74.6%) reported the expected SHA-1 hash. Twenty-five participants (18.6%) reported the SHA-1 hash of the entire compressed file.

Expected Response Explanation:

The verification hash is embedded in the .E01 (EWF) forensic container file by the acquisition tool. Forensic tools that support the Expert Witness Format (EWF) will parse and display this information.

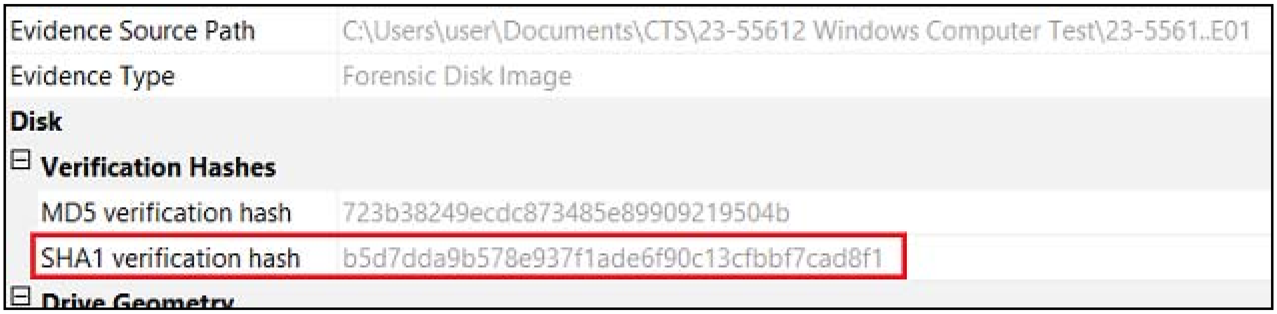
Expected Response Illustration:

EnCase parse of 23-5561.E01 metadata



Name	untitled
Primary Path	C:\Users\user\Documents\CTS\23-55612 Windows Computer Test\23-5561..E01
Evidence Paths	Yes
GUID	723b38249ecdc8c3485e89909219504b
Index File	C:\Users\user\Documents\CTS\23-55612 Windows Computer Test\23-5561\EvidenceCache\723B38249ECDC8C3485E89909219504B\DeviceIndex.L01
Actual Date	03/09/2023 06:24:56 (-5:00 Eastern Standard Time)
Target Date	03/09/2023 06:24:56 (-5:00 Eastern Standard Time)
File Integrity	Completely Verified, 0 Errors
Acquisition MD5	723b38249ecdc873485e89909219504b
Verification MD5	723b38249ecdc873485e89909219504b
Acquisition SHA1	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
Verification SHA1	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1

FTK Imager parse of 23-5561.E01 metadata



Evidence Source Path	C:\Users\user\Documents\CTS\23-55612 Windows Computer Test\23-5561..E01
Evidence Type	Forensic Disk Image
Disk	
⊟ **Verification Hashes**	
MD5 verification hash	723b38249ecdc873485e89909219504b
SHA1 verification hash	b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1
⊟ **Drive Geometry**	

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 2 - Examination Questions

Question 2: How many partitions are on the hard drive (device imaged as 23-5561.E01)? Provide a NUMERIC response (e.g., 1, 2, 3).

Manufacturer's Expected Response: 2

WebCode Test	Response
2A9WQN-5561	2
2P2VAR-5561	2
2PJFNF-5562	2
2VQ8RL-5562	2
2ZFN6X-5561	2
3CDK6E-5562	2
3DPEPK-5561	2
3M9X4P-5561	2
42BM2N-5561	2
48GFVJ-5561	2
4U7ZP2-5562	2
649HZ6-5561	2
68RW46-5562	2
6DZZCR-5561	2
6MKCN6-5562	2
6Q2RXW-5562	2
6Q4JPC-5561	2
6QKH3A-5562	2
6TR3NP-5561	2
72ZUTD-5561	2

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 2 - Examination Questions	
WebCode Test	**Response**
78PAK7-5562	2
7JUP4F-5561	2
7PQ8PM-5562	2
7XZLMH-5562	2
82VWX9-5562	2
83AEYT-5562	2
8CB97J-5561	2
8LJ9TK-5561	2
96TUNQ-5561	2
98ZV8C-5561	2
99QBZK-5562	2
9AJ8JM-5561	2
9J9Q8U-5562	2
A8QHYB-5562	2
A8VQBZ-5561	2
ABK3AJ-5561	2
ACTERK-5561	2
ADYU2Y-5562	2
AKG6BT-5562	2
AM94QQ-5561	2
BFKZWF-5562	2
BQRG78-5561	2

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 2 - Examination Questions

WebCode Test	Response
C4LMC9-5562	2
C897D8-5561	2
CF2CBE-5562	2
CKAXYB-5561	2
CP6N6M-5561	2
D7PUVD-5561	2
DB6AM4-5561	2
DGVH9K-5561	2
DXVP3C-5562	2
E2RHRZ-5562	2
E4ZNBG-5561	2
EV7HHF-5561	2
F3JVRX-5561	2
FZVEJB-5561	2
G973T4-5561	2
GJ39KG-5561	2
GYTEQP-5561	2
HQVXJW-5561	2
HUFQTD-5561	2
HW2LD2-5562	[Participant did not return results for this question.]
J84AQF-5562	2
JE9W33-5561	2

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 2 - Examination Questions

WebCode Test	Response
JGBUAC-5562	2
JJDU63-5561	2
JL32PY-5562	2
JLRZA6-5561	2
JPKFX7-5561	2
KR28JR-5562	2
KR4V3R-5561	2
KXRBW6-5562	2
KZVDDT-5561	2
LDKC3B-5561	2
M9HYHY-5561	2
MF4Q7B-5561	2
MF8B24-5561	2
NADTWE-5561	2
NE7TEF-5562	2
NTANM4-5561	2
NTZJR4-5561	2
P3ACZC-5561	2
P79FU7-5561	2
P8ZNUA-5561	2
PFEMA7-5562	2
PFVN93-5561	2

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 2 - Examination Questions

WebCode Test	Response
PLGGK2-5561	2
PPMYM4-5562	2
PTKDEZ-5562	2
PUTRGY-5561	2
PWJXV6-5561	2
Q2CFQV-5561	2
Q33NQX-5561	2
Q3RHY2-5561	2
QMR3Q2-5561	2
QRJAR3-5561	2
QTHAXU-5561	2
RAK67E-5562	2
RBBDCA-5562	2
RGH4EF-5562	2
RRMUMV-5561	2
RRXTDK-5562	2
RV3JKZ-5561	2
TC4JAF-5562	2
TCGEBD-5561	2
TEPC2R-5562	2
TKFNZV-5561	2
TNEXBT-5561	2

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 2 - Examination Questions

WebCode Test	Response
TVF9MD-5562	2
TX22EP-5561	2
U3RQC6-5561	2
UKBK6E-5561	2
URA8XZ-5561	2
UVZCUQ-5562	2
V4KY4K-5562	2
VCE6WL-5561	2
VJH9N7-5561	2
VTZR3B-5561	2
VVVB8V-5561	2
WC9E49-5561	2
WD8DHB-5561	2
WK4CUH-5561	2
WNN64Y-5561	2
WX2YKZ-5561	2
WZGLVL-5562	2
XA2A8Z-5562	2
XEVDXV-5561	2
XJ99G2-5562	2
XQ9B22-5561	2
XVDHZK-5562	[Participant did not return results for this question.]

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 2 - Examination Questions

WebCode Test	Response
XWDAB7-5561	2
XX78KX-5561	2
Y63G92-5562	2
YDJQ3P-5561	2
YPNENR-5562	2
ZPR26J-5561	2

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 2 - Examination Questions

Question 2: How many partitions are on the hard drive (device imaged as 23-5561.E01)? Provide a NUMERIC response (e.g., 1, 2, 3).

Consensus Result:

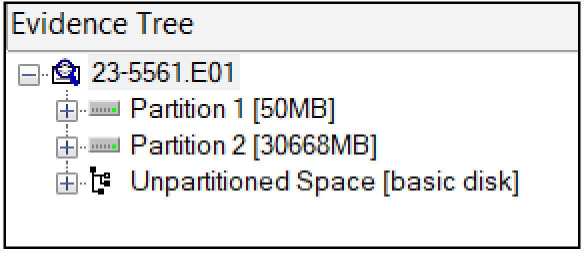
2

Expected Response Explanation:

Most forensic tools will display a drive geometry summary showing the partition table.

Expected Response Illustration:

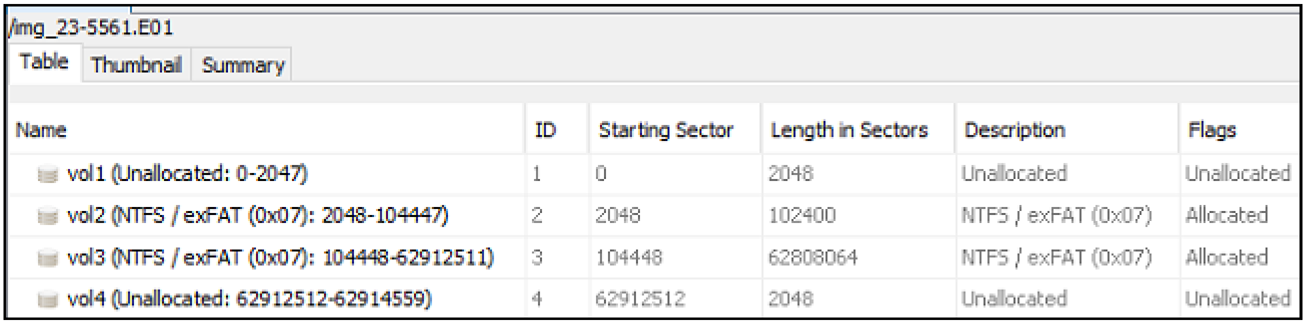
FTK Report of Drive Geometry



Evidence Tree

- 23-5561.E01
  - Partition 1 [50MB]
  - Partition 2 [30668MB]
  - Unpartitioned Space [basic disk]

Autopsy Report of Drive Geometry



/img_23-5561.E01

Name	ID	Starting Sector	Length in Sectors	Description	Flags
vol1 (Unallocated: 0-2047)	1	0	2048	Unallocated	Unallocated
vol2 (NTFS / exFAT (0x07): 2048-104447)	2	2048	102400	NTFS / exFAT (0x07)	Allocated
vol3 (NTFS / exFAT (0x07): 104448-62912511)	3	104448	62808064	NTFS / exFAT (0x07)	Allocated
vol4 (Unallocated: 62912512-62914559)	4	62912512	2048	Unallocated	Unallocated

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3 - Examination Questions

Question 3: What is the hostname (Computer name) for this computer?

Manufacturer's Expected Response: DAVID-LAPTOP

WebCode Test	Response
2A9WQN-5561	DAVID-LAPTOP
2P2VAR-5561	DAVID-LAPTOP
2PJFNF-5562	DAVID-LAPTOP
2VQ8RL-5562	DAVID-LAPTOP
2ZFN6X-5561	DAVID_LAPTOP
3CDK6E-5562	DAVID-LAPTOP
3DPEPK-5561	DAVID-LAPTOP
3M9X4P-5561	DAVID-LAPTOP
42BM2N-5561	DAVID-LAPTOP
48GFVJ-5561	DAVID-LAPTOP
4U7ZP2-5562	DAVID-LAPTOP
649HZ6-5561	DAVID-LAPTOP
68RW46-5562	DAVID-LAPTOP
6DZZCR-5561	David-Laptop
6MKCN6-5562	David-Laptop
6Q2RXW-5562	DAVID-LAPTOP
6Q4JPC-5561	David-Laptop
6QKH3A-5562	DAVID-LAPTOP
6TR3NP-5561	DAVID-LAPTOP
72ZUTD-5561	DAVID-LAPTOP
78PAK7-5562	DAVID-LAPTOP

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3 - Examination Questions

WebCode Test	Response
7JUP4F-5561	noname
7PQ8PM-5562	DAVID-LAPTOP
7XZLMH-5562	DAVID-LAPTOP
82VWX9-5562	DAVID-LAPTOP
83AEYT-5562	DAVID-LAPTOP
8CB97J-5561	DAVID-LAPTOP
8LJ9TK-5561	David-Laptop
96TUNQ-5561	DAVID-LAPTOP
98ZV8C-5561	DAVID-LAPTOP
99QBZK-5562	DAVID-LAPTOP
9AJ8JM-5561	DAVID-LAPTOP
9J9Q8U-5562	DAVID-LAPTOP
A8QHYB-5562	DAVID-LAPTOP
A8VQBZ-5561	DAVID-LAPTOP
ABK3AJ-5561	DAVID-LAPTOP
ACTERK-5561	DAVID-LAPTOP
ADYU2Y-5562	DAVID-LAPTOP
AKG6BT-5562	DAVID-LAPTOP
AM94QQ-5561	DAVID-LAPTOP
BFKZWF-5562	David-Laptop
BQRG78-5561	David-Laptop
C4LMC9-5562	DAVID-LAPTOP

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3 - Examination Questions

WebCode Test	Response
C897D8-5561	DAVID-LAPTOP
CF2CBE-5562	DAVID-LAPTOP
CKAXYB-5561	DAVID-LAPTOP
CP6N6M-5561	DAVID-LAPTOP
D7PUVD-5561	DAVID-LAPTOP
DB6AM4-5561	DAVID-LAPTOP
DGVH9K-5561	DAVID-LAPTOP
DXVP3C-5562	DAVID – LAPTOP
E2RHRZ-5562	DAVID-LAPTOP
E4ZNBG-5561	DAVID-LAPTOP
EV7HHF-5561	DAVID-LAPTOP
F3JVRX-5561	DAVID-LAPTOP
FZVEJB-5561	DAVID-LAPTOP
G973T4-5561	david-laptop
GJ39KG-5561	DAVID-LAPTOP
GYTEQP-5561	DAVID-LAPTOP
HQVXJW-5561	DAVID-LAPTOP
HUFQTD-5561	DAVID-LAPTOP
HW2LD2-5562	[Participant did not return results for this question.]
J84AQF-5562	DAVID-LAPTOP
JE9W33-5561	DAVID-LAPTOP
JGBUAC-5562	DAVID-LAPTOP

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3 - Examination Questions

WebCode Test	Response
JJDU63-5561	DAVID-LAPTOP
JL32PY-5562	DAVID-LAPTOP
JLRZA6-5561	DAVID-LAPTOP
JPKFX7-5561	David-Laptop
KR28JR-5562	DAVID-LAPTOP
KR4V3R-5561	DAVID-LAPTOP
KXRBW6-5562	DAVID-LAPTOP
KZVDDT-5561	DAVID-LAPTOP
LDKC3B-5561	David-Laptop
M9HYHY-5561	DAVID-LAPTOP
MF4Q7B-5561	DAVID-LAPTOP
MF8B24-5561	DAVID-LAPTOP
NADTWE-5561	DAVID-LAPTOP
NE7TEF-5562	DAVID-LAPTOP
NTANM4-5561	DAVID-LAPTOP
NTZJR4-5561	DAVID-LAPTOP
P3ACZC-5561	David-Laptop
P79FU7-5561	DAVID-LAPTOP
P8ZNUA-5561	DAVID-LAPTOP
PFEMA7-5562	DAVID-LAPTOP
PFVN93-5561	DAVID - LAPTOP
PLGGK2-5561	DAVID-LAPTOP

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3 - Examination Questions

WebCode Test	Response
PPMYM4-5562	DAVID-LAPTOP
PTKDEZ-5562	DAVID-LAPTOP
PUTRGY-5561	David-Laptop
PWJXV6-5561	DAVID-LAPTOP
Q2CFQV-5561	David-Laptop
Q33NQX-5561	DAVID-LAPTOP
Q3RHY2-5561	DAVID-LAPTOP
QMR3Q2-5561	DAVID-LAPTOP
QRJAR3-5561	DAVID-LAPTOP
QTHAXU-5561	DAVID-LAPTOP
RAK67E-5562	DAVID-LAPTOP
RBBDCA-5562	DAVID-LAPTOP
RGH4EF-5562	DAVID-LAPTOP
RRMUMV-5561	DAVID-LAPTOP
RRXTDK-5562	David-Laptop
RV3JKZ-5561	David-Laptop
TC4JAF-5562	DAVID-LAPTOP
TCGEBD-5561	DAVID-LAPTOP
TEPC2R-5562	DAVID-LAPTOP
TKFNZV-5561	DAVID-LAPTOP
TNEXBT-5561	DAVID-LAPTOP
TVF9MD-5562	DAVID-LAPTOP

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3 - Examination Questions

WebCode Test	Response
TX22EP-5561	DAVID-LAPTOP
U3RQC6-5561	David-Laptop
UKBK6E-5561	David-Laptop
URA8XZ-5561	DAVID-LAPTOP
UVZCUQ-5562	DAVID-LAPTOP
V4KY4K-5562	DAVID-LAPTOP
VCE6WL-5561	DAVID-LAPTOP
VJH9N7-5561	DAVID-LAPTOP
VTZR3B-5561	Computer Name: DAVID-LAPTOP
VVVB8V-5561	DAVID-LAPTOP
WC9E49-5561	DAVID-LAPTOP
WD8DHB-5561	DAVID-LAPTOP
WK4CUH-5561	David-Laptop
WNN64Y-5561	DAVID-LAPTOP
WX2YKZ-5561	David - Laptop
WZGLVL-5562	DAVID-LAPTOP
XA2A8Z-5562	DAVID-LAPTOP
XEVDXV-5561	DAVID-LAPTOP
XJ99G2-5562	DAVID-LAPTOP
XQ9B22-5561	DAVID-LAPTOP
XVDHZK-5562	[Participant did not return results for this question.]
XWDAB7-5561	DAVID-LAPTOP

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3 - Examination Questions

WebCode Test	Response
XX78KX-5561	DAVID-LAPTOP
Y63G92-5562	DAVID-LAPTOP
YDJQ3P-5561	DAVID - LAPTOP
YPNENR-5562	DAVID-LAPTOP
ZPR26J-5561	David-Laptop

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3 - Examination Questions

Question 3: What is the hostname (Computer name) for this computer?

Consensus Result:

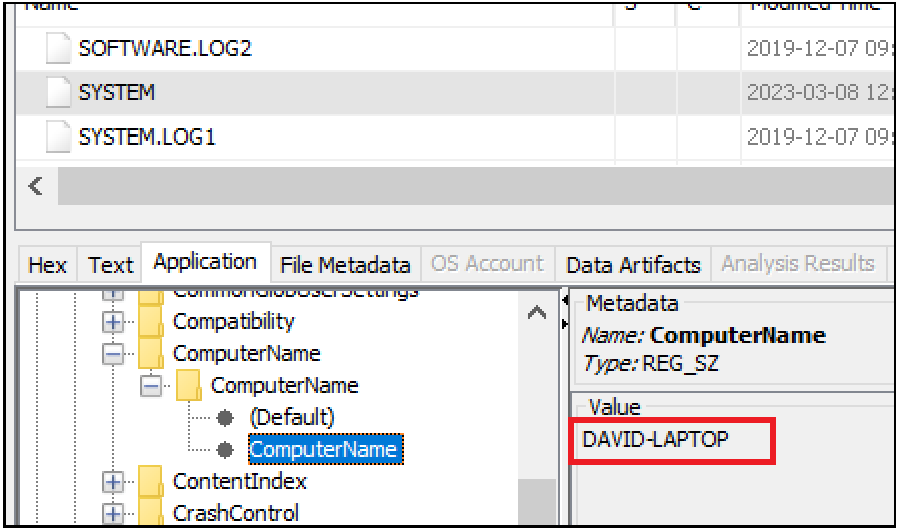
DAVID-LAPTOP

Expected Response Explanation:

This value is stored in the Windows System Registry at ControlSet001\Control\ComputerName\ComputerName

Expected Response Illustration:

Autopsy view of computer name registry key



Name	S	C	Modified Time
SOFTWARE.LOG2			2019-12-07 09:
SYSTEM			2023-03-08 12:
SYSTEM.LOG1			2019-12-07 09:

Metadata

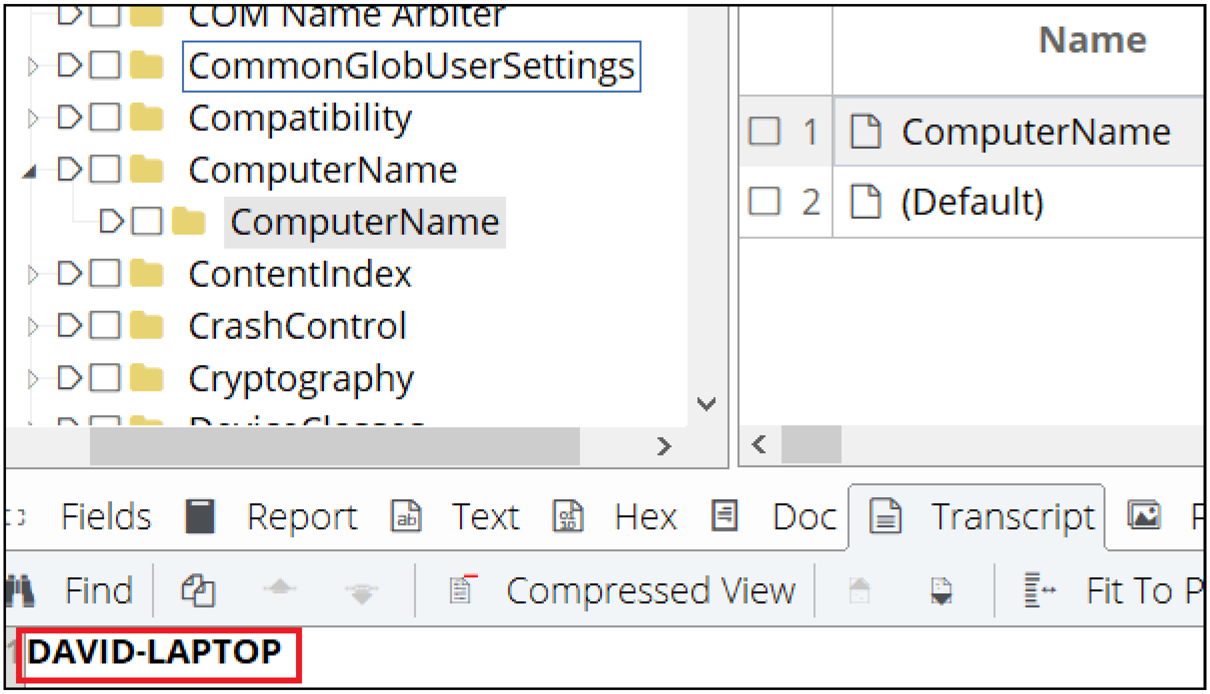
Name: **ComputerName**

Type: REG_SZ

Value

DAVID-LAPTOP

EnCase view of computer name registry key



	Name
☐ 1	ComputerName
☐ 2	(Default)

DAVID-LAPTOP

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4 - Examination Questions

Question 4: What operating system (include version and edition) was installed on this computer?

Manufacturer's Expected Response: Windows 10 Home

WebCode Test	Response
2A9WQN-5561	Windows 10 Home (2009), version 6.3
2P2VAR-5561	Windows 10 Home (2009) Version 6.3
2PJFNF-5562	Windows 10 Home
2VQ8RL-5562	Windows 10 Home (version 6.3 and edition 2009)
2ZFN6X-5561	Windows 10 Home 6.3
3CDK6E-5562	Windows 10 Home- release 2009 - build 19041
3DPEPK-5561	Windows 10 Home 6.3 Core
3M9X4P-5561	Windows Home 10 (2009) version 6.3
42BM2N-5561	Windows 10 Home (2009) version: 6.3, Edition: Core
48GFVJ-5561	Windows 10 Home 6.3
4U7ZP2-5562	Windows 10 Home
649HZ6-5561	Windows 10 Home (2009) version 6.3
68RW46-5562	Windows 10 Home (2009), version number 6.3
6DZZCR-5561	Windows 10 Home 21H2
6MKCN6-5562	Windows 10 Home (2009) 6.3
6Q2RXW-5562	Windows 10 Home
6Q4JPC-5561	Windows 10 Home Version 6.3
6QKH3A-5562	Windows 10 Home (2009). Version 6.3
6TR3NP-5561	Windows 10 Home (2009) Version 6.3 Build 19044
72ZUTD-5561	Windows 10 Home (2009) version 6.3
78PAK7-5562	Windows 10 Home

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4 - Examination Questions

WebCode Test	Response
7JUP4F-5561	windows 10 home
7PQ8PM-5562	Windows 10 Home Edition (2009) Version 6.3
7XZLMH-5562	WINDOWS 10 HOME (2009) VERSION 6.3
82VWX9-5562	OS: Windows 10 Home (2009) Version: 6.3 OS version: Core Build number: 19044
83AEYT-5562	Windows 10 Home (2009) Version 6.3
8CB97J-5561	Windows 10 Home (2009) 6.3
8LJ9TK-5561	Windows 10 Home (2009) v6.3
96TUNQ-5561	Windows 10 Home / 6.3 / Core
98ZV8C-5561	Microsoft Windows 10, Version 6.3, Core Edition
99QBZK-5562	Windows 10 Home (2009) Version 6.3
9AJ8JM-5561	Windows 10 Home (2009) Ver 6.3
9J9Q8U-5562	Windows 10 Home (2009) Version 6.3
A8QHYB-5562	Windows 10 Home (2009) version 6.3 build 19044
A8VQBZ-5561	Windows 10 Home (2009) v 6.3
ABK3AJ-5561	Windows 10 Home Version 6.3
ACTERK-5561	Windows 10 Home version 6.3
ADYU2Y-5562	Windows 10 Home (2009) Version 6.3
AKG6BT-5562	Windows 10 Home (2009) version 6.3 build number 19044
AM94QQ-5561	Windows 10 Home
BFKZWF-5562	Windows 10 Home (2009) Version : 6.3
BQRG78-5561	Windows 10 Home (2009) (Version 6.3, Display Version: 21H2)
C4LMC9-5562	Windows 10 Home

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4 - Examination Questions

WebCode Test	Response
C897D8-5561	Window 10 Home (2009) version 6.3
CF2CBE-5562	Windows 10 Home (2009) Version 6.3
CKAXYB-5561	Windows 10 Home, version: 6.3, edition: Core
CP6N6M-5561	Windows 10 Home (2009) 6.3
D7PUVD-5561	Windows 10 Home (2009) version 6.3
DB6AM4-5561	Windows 10 Home, Display version 21H2, CurrentBuild Number 19044, Version 2009 (Extended build string 19041.1.amd64fre.vb_release.191206-1406)
DGVH9K-5561	Windows 10 Home (2009), version 6.3, build 19044
DXVP3C-5562	Windows 10 Home (2009) v. 6.3
E2RHRZ-5562	Windows 10 Home (2009) 6.3
E4ZNBG-5561	Windows 10 Home (2009)(Version 6.3)
EV7HHF-5561	WINDOWS 10 HOME
F3JVRX-5561	Windows 10 Home 21H2 19044(6.3)
FZVEJB-5561	Windows 10 Home - version 21H2
G973T4-5561	windows 10 home (2009) version 6.3
GJ39KG-5561	Windows 10 Home (2009) v6.3
GYTEQP-5561	Microsoft Windows 10 Home
HQVXJW-5561	Windows 10 Home 6.3
HUFQTD-5561	Windows 10 Home version 2009 edition 19044
HW2LD2-5562	[Participant did not return results for this question.]
J84AQF-5562	Windows 10 Home Multiprocessor Free 6.3.19041.vb_release.191206-1406
JE9W33-5561	Windows 10 Home, version 6.3
JGBUAC-5562	Operating system version and edition Version: 6.3 Edition: Windows 10 Home (2009)

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4 - Examination Questions

WebCode Test	Response
JJDU63-5561	Windows 10 Home
JL32PY-5562	Windows 10 Home 19044
JLRZA6-5561	Windows 10 Home (2009) version 6.3
JPKFX7-5561	Windows 10 Home 6.3
KR28JR-5562	Windows 10 Home
KR4V3R-5561	Windows 10 Home, Core, 2009, 19044.2604
KXRBW6-5562	Windows 10 Home (2009) version 6.3
KZVDDT-5561	Windows 10 Home (2009) v6.3
LDKC3B-5561	Windows 10 Home
M9HYHY-5561	Windows 10 home
MF4Q7B-5561	Windows 10 Home (2009); Version 6.3
MF8B24-5561	Windows 10 Home (2009) V. 6.3
NADTWE-5561	Windows 10 Home Edition
NE7TEF-5562	Windows 10 Home(2009) 6.3
NTANM4-5561	Windows 10 Home (2009) Version 6.3
NTZJR4-5561	Windows 10 Home
P3ACZC-5561	Windows 10 Home (2009) 6.3
P79FU7-5561	WINDOWS 10 HOME
P8ZNUA-5561	Windows 10 Home (2009) version 6.3 (Build 19044)
PFEMA7-5562	Windows 10 Home (2009), 6.3
PFVN93-5561	Windows 10 Home v6.3, Edition Core
PLGGK2-5561	Windows 10 Home

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4 - Examination Questions

WebCode Test	Response
PPMYM4-5562	Windows 10 Home (2009) Version 6.3
PTKDEZ-5562	Windows 10 Home (2009), Version: 6.3
PUTRGY-5561	Windows 10 Home (2009) Version : 6.3
PWJXV6-5561	Windows 10 Home 6.3 Core
Q2CFQV-5561	Windows 10 Home 19044
Q33NQX-5561	Windows 10 21H2 Home Edition
Q3RHY2-5561	Windows 10 Home (2009) Version 6.3 Edition: Core
QMR3Q2-5561	Windows 10 Home 19044
QRJAR3-5561	Windows 10 Home 21H2 Build 19044
QTHAXU-5561	Windows 10 Home, version 6.3
RAK67E-5562	Windows 10 Home (version number 6.3)
RBBDCA-5562	Windows 10 Home
RGH4EF-5562	OS =Windows 10 Home (2009) - Version Number =6.3 - Operating System Version =Core - Build Number =19044
RRMUMV-5561	Windows 10 Home (2009) Version 6.3
RRXTDK-5562	Windows 10 Home (2009)
RV3JKZ-5561	Windows 10 Home (2009) Version : 6.3
TC4JAF-5562	Windows 10 Home (2009) v6.3
TCGEBD-5561	Windows 10 Home (2009) Version 6.3 Build 19044
TEPC2R-5562	Windows 10 home
TKFNZV-5561	Windows 10 home
TNEXBT-5561	Windows 10 Home
TVF9MD-5562	Windows 10 Home (2009) version 6.3

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4 - Examination Questions

WebCode Test	Response
TX22EP-5561	Windows 10 Home(2009) core v.6.3
U3RQC6-5561	Windows 10 Home (2009) Core, Version 6.3, Build Number 19044
UKBK6E-5561	Windows 10 Home 19044
URA8XZ-5561	Windows 10 Home (2009) Version 6.3
UVZCUQ-5562	Windows 10 Home Version 6.3 - 21H2
V4KY4K-5562	Windows 10 Home (2009) versión 6.3
VCE6WL-5561	Windows 10 Home (Version 2009) v6.3
VJH9N7-5561	Windows 10 Home edition version 21H2
VTZR3B-5561	Windows 10 Home (2009) Version: 6.3 Operating system version: Core Build Number: 19044
VVVB8V-5561	Windows 10 Home (2009) Version 6.3 Build 19044
WC9E49-5561	Windows 10 Home
WD8DHB-5561	Windows 10 Home (2009) Version 6.3
WK4CUH-5561	Windows 10 Home
WNN64Y-5561	Windows 10 Home 2009 edition 19044
WX2YKZ-5561	Windows 10 Home 2009
WZGLVL-5562	Win 10 Home (2009) 6.3
XA2A8Z-5562	Windows 10 Home (2009) Version 6.3
XEVDXV-5561	Windows 10 Home 6.3
XJ99G2-5562	Windows 10 Home v6.3
XQ9B22-5561	Windows 10 Home Version 6.3 Core Edition
XVDHZK-5562	[Participant did not return results for this question.]
XWDAB7-5561	Windows 10 Home

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4 - Examination Questions

WebCode Test	Response
XX78KX-5561	Windows 10 Home (2009) v.6.3
Y63G92-5562	Windows 10 Home(2009) version 6.3 19044 21H2
YDJQ3P-5561	Windows 10 Home (2009) v. 6.3
YPNENR-5562	Windows 10 Home (2009) version V6.3
ZPR26J-5561	Windows 10 Home Edition 6.3

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4 - Examination Questions

Question 4: What operating system (include version and edition) was installed on this computer?

Consensus Result:

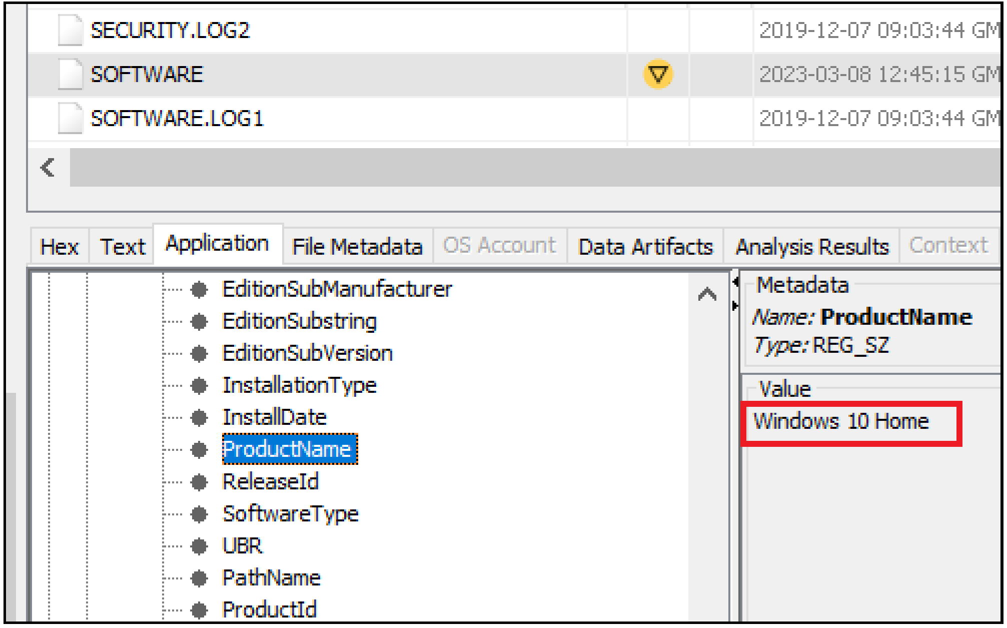
Windows 10 Home and variations representing the same information.

Expected Response Explanation:

This information is found in the registry at C:\Windows\System32\Config\Software: Microsoft\Windows NT\CurrentVersion: ProductName

Expected Response Illustration:

Autopsy view showing Windows version and edition in the Software registry hive

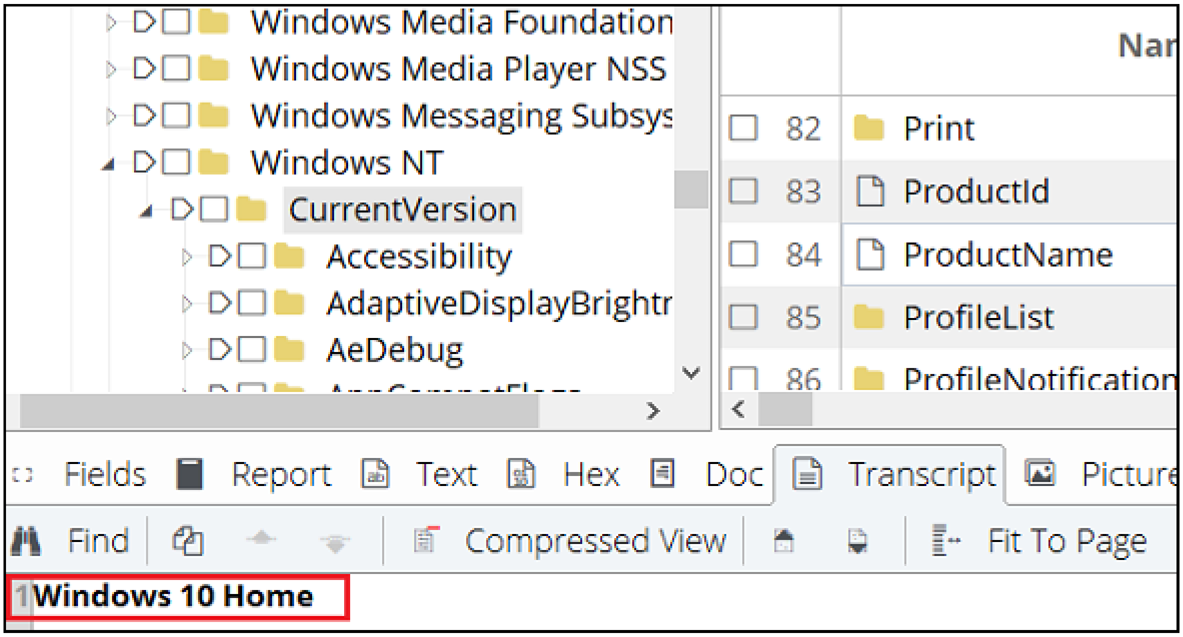


SECURITY.LOG2		2019-12-07 09:03:44 GM
SOFTWARE		2023-03-08 12:45:15 GM
SOFTWARE.LOG1		2019-12-07 09:03:44 GM

Metadata
Name: **ProductName**
Type: REG_SZ

Value
Windows 10 Home

EnCase view showing Windows version and edition in the Software registry hive



1 **Windows 10 Home**

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 5 - Examination Questions

Question 5: Who is the registered owner of this operating system installation?

Manufacturer's Expected Response: David Lightman

WebCode Test	Response
2A9WQN-5561	David Lightman
2P2VAR-5561	David Lightman
2PJFNF-5562	David Lightman
2VQ8RL-5562	David Lightman
2ZFN6X-5561	David Lightman
3CDK6E-5562	David Lightman
3DPEPK-5561	David Lightman
3M9X4P-5561	David Lightman
42BM2N-5561	David Lightman
48GFVJ-5561	David Lightman
4U7ZP2-5562	David Lightman
649HZ6-5561	David Lightman
68RW46-5562	David Lightman
6DZZCR-5561	David Lightman
6MKCN6-5562	David Lightman
6Q2RXW-5562	David Lightman
6Q4JPC-5561	David Lightman
6QKH3A-5562	David Lightman
6TR3NP-5561	David Lightman
72ZUTD-5561	David Lightman
78PAK7-5562	David Lightman

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 5 - Examination Questions

WebCode Test	Response
7JUP4F-5561	david lightman
7PQ8PM-5562	David Lightman
7XZLMH-5562	DAVID LIGHTMAN
82VWX9-5562	David Lightman
83AEYT-5562	David Lightman
8CB97J-5561	David Lightman
8LJ9TK-5561	David Lightman
96TUNQ-5561	David Lightman
98ZV8C-5561	David Lightman
99QBZK-5562	David Lightman
9AJ8JM-5561	David Lightman
9J9Q8U-5562	David Lightman
A8QHYB-5562	David Lightman
A8VQBZ-5561	David Lightman
ABK3AJ-5561	David Lightman
ACTERK-5561	David Lightman
ADYU2Y-5562	David Lightman
AKG6BT-5562	David Lightman
AM94QQ-5561	David Lightman
BFKZWF-5562	David Lightman
BQRG78-5561	David Lightman
C4LMC9-5562	David Lightman

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 5 - Examination Questions

WebCode Test	Response
C897D8-5561	David Lightman
CF2CBE-5562	David Lightman
CKAXYB-5561	David Lightman
CP6N6M-5561	David Lightman
D7PUVD-5561	David Lightman
DB6AM4-5561	David Lightman
DGVH9K-5561	David Lightman
DXVP3C-5562	David Lightman
E2RHRZ-5562	David Lightman
E4ZNBG-5561	David Lightman
EV7HHF-5561	David Lightman
F3JVRX-5561	David Lightman
FZVEJB-5561	David Lightman
G973T4-5561	david lightman
GJ39KG-5561	David Lightman
GYTEQP-5561	David Lightman
HQVXJW-5561	David Lightman
HUFQTD-5561	David Lightman
HW2LD2-5562	[Participant did not return results for this question.]
J84AQF-5562	David Lightman
JE9W33-5561	David Lightman
JGBUAC-5562	David Lightman

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 5 - Examination Questions

WebCode Test	Response
JJDU63-5561	David Lightman
JL32PY-5562	David Lightman
JLRZA6-5561	David Lightman
JPKFX7-5561	David Lightman
KR28JR-5562	David Lightman
KR4V3R-5561	David Lightman
KXRBW6-5562	David Lightman
KZVDDT-5561	David Lightman
LDKC3B-5561	David Lightman
M9HYHY-5561	David lightman
MF4Q7B-5561	David Lightman
MF8B24-5561	David Lightman
NADTWE-5561	David Lightman
NE7TEF-5562	David Lightman
NTANM4-5561	David Lightman
NTZJR4-5561	David Lightman
P3ACZC-5561	David Lightman
P79FU7-5561	David Lightman
P8ZNUA-5561	David Lightman
PFEMA7-5562	David Lightman
PFVN93-5561	David Lightman
PLGGK2-5561	David Lightman

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 5 - Examination Questions

WebCode Test	Response
PPMYM4-5562	David Lightman
PTKDEZ-5562	David Lightman
PUTRGY-5561	David Lightman
PWJXV6-5561	David Lightman
Q2CFQV-5561	David Lightman
Q33NQX-5561	David Lightman
Q3RHY2-5561	David Lightman
QMR3Q2-5561	David Lightman
QRJAR3-5561	David Lightman
QTHAXU-5561	David Lightman
RAK67E-5562	David Lightman
RBBDCA-5562	David Lightman
RGH4EF-5562	David Lightman
RRMUMV-5561	David Lightman
RRXTDK-5562	David Lightman
RV3JKZ-5561	David Lightman
TC4JAF-5562	David Lightman
TCGEBD-5561	David Lightman
TEPC2R-5562	David Lightman
TKFNZV-5561	David Lightman
TNEXBT-5561	David Lightman
TVF9MD-5562	David Lightman

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 5 - Examination Questions

WebCode Test	Response
TX22EP-5561	David Lightman
U3RQC6-5561	David Lightman
UKBK6E-5561	David Lightman
URA8XZ-5561	David Lightman
UVZCUQ-5562	David Lightman
V4KY4K-5562	David Lightman
VCE6WL-5561	David Lightman
VJH9N7-5561	David Lightman
VTZR3B-5561	David Lightman
VVVB8V-5561	David Lightman
WC9E49-5561	David Lightman
WD8DHB-5561	David Lightman
WK4CUH-5561	David Lightman
WNN64Y-5561	David Lightman
WX2YKZ-5561	David Lightman
WZGLVL-5562	David Lightman
XA2A8Z-5562	David Lightman
XEVDXV-5561	David Lightman
XJ99G2-5562	David Lightman
XQ9B22-5561	David Lightman
XVDHZK-5562	[Participant did not return results for this question.]
XWDAB7-5561	David Lightman

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 5 - Examination Questions

WebCode Test	Response
XX78KX-5561	David Lightman
Y63G92-5562	David Lightman
YDJQ3P-5561	David Lightman
YPNENR-5562	David Lightman
ZPR26J-5561	David Lightman

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 5 - Examination Questions

Question 5: Who is the registered owner of this operating system installation?

Consensus Result:

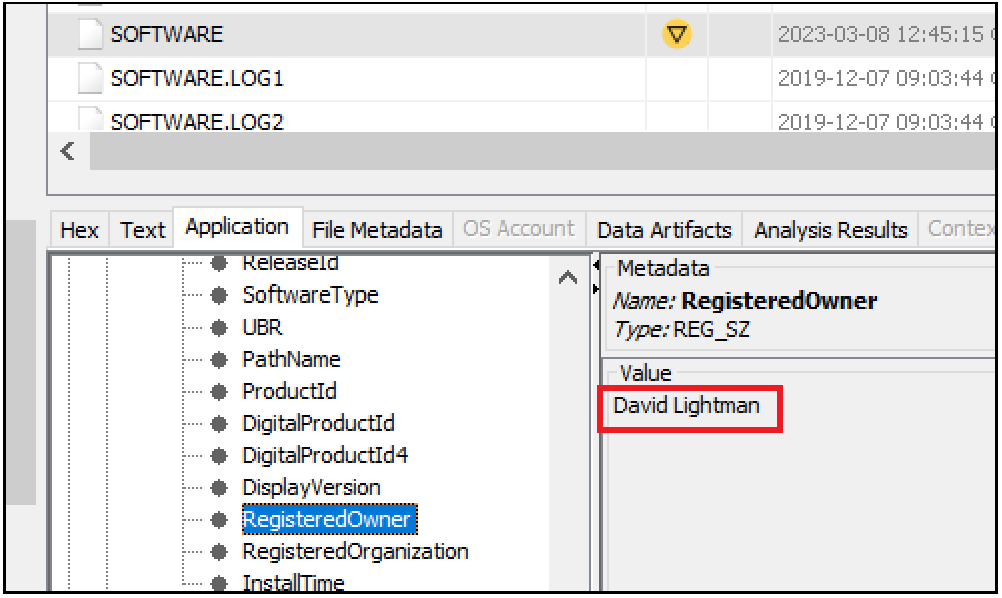
David Lightman

Expected Response Explanation:

This information is found in the registry at C:\Windows\System32\Config\Software: Microsoft\Windows NT\CurrentVersion: Registered Owner

Expected Response Illustration:

Autopsy view showing the registered owner in the Software registry hive



File	Date
SOFTWARE	2023-03-08 12:45:15
SOFTWARE.LOG1	2019-12-07 09:03:44
SOFTWARE.LOG2	2019-12-07 09:03:44

Metadata

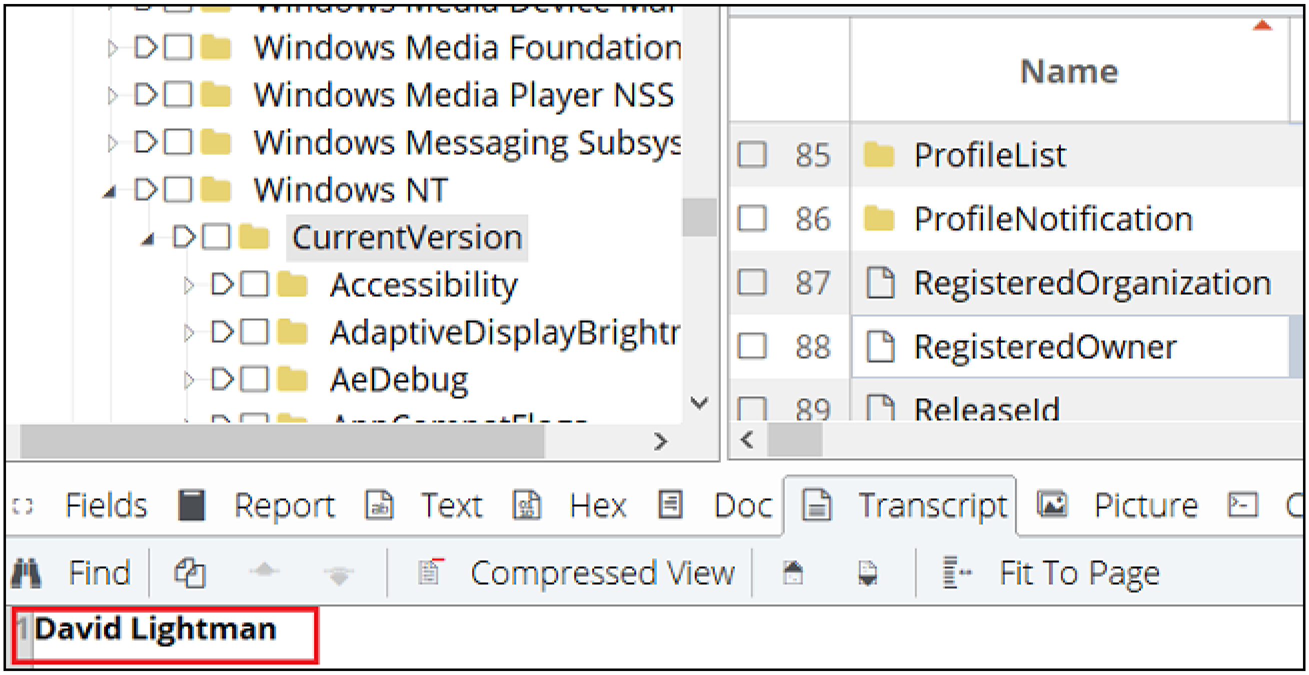
Name: **RegisteredOwner**

Type: REG_SZ

Value

David Lightman

EnCase view showing the registered owner in the Software registry hive



	Name
85	ProfileList
86	ProfileNotification
87	RegisteredOrganization
88	RegisteredOwner
89	ReleaseId

1 **David Lightman**

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6 - Examination Questions

Question 6: What "replaceString" did user David Lightman LAST use in Notepad, as recorded by the user's registry?

Manufacturer's Expected Response: st.clotildes

WebCode Test	Response
2A9WQN-5561	st.clotildes
2P2VAR-5561	st.clotildes
2PJFNF-5562	CTS
2VQ8RL-5562	UnsightlyAdorableToad
2ZFN6X-5561	st.clotildes
3CDK6E-5562	st.clotildes
3DPEPK-5561	st.clotildes
3M9X4P-5561	cts
42BM2N-5561	st.clotildes
48GFVJ-5561	st.clotildes
4U7ZP2-5562	st.clotildes
649HZ6-5561	st.clotildes
68RW46-5562	st.clotildes
6DZZCR-5561	st.clotildes
6MKCN6-5562	st.clotildes
6Q2RXW-5562	st.clotildes
6Q4JPC-5561	st.clotildes
6QKH3A-5562	st.clotildes
6TR3NP-5561	st.clotildes
72ZUTD-5561	st.clotildes

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6 - Examination Questions

WebCode Test	Response
78PAK7-5562	st.clotildes
7JUP4F-5561	st.clotildes
7PQ8PM-5562	st.clotildes
7XZLMH-5562	st.clotildes
82VWX9-5562	st.clotildes
83AEYT-5562	st.clotildes
8CB97J-5561	st.clotildes
8LJ9TK-5561	st.clotildes
96TUNQ-5561	st.clotildes
98ZV8C-5561	st.clotildes
99QBZK-5562	st.clotildes
9AJ8JM-5561	st.clotildes
9J9Q8U-5562	st.clotildes
A8QHYB-5562	st.clotildes
A8VQBZ-5561	st.clotildes
ABK3AJ-5561	NOT IN SCOPE
ACTERK-5561	Not in Scope
ADYU2Y-5562	st.clotildes
AKG6BT-5562	st.clotildes
AM94QQ-5561	st.clotildes
BFKZWF-5562	st.clotildes
BQRG78-5561	st.clotildes

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6 - Examination Questions

WebCode Test	Response
C4LMC9-5562	st.clotildes
C897D8-5561	st.clotildes
CF2CBE-5562	st.clotildes
CKAXYB-5561	st.clotildes
CP6N6M-5561	st.clotildes
D7PUVD-5561	st.clotildes
DB6AM4-5561	st.clotildes
DGVH9K-5561	Glaucidium
DXVP3C-5562	st.clotildes
E2RHRZ-5562	st.clotildes
E4ZNBG-5561	st.clotildes
EV7HHF-5561	st.clotildes
F3JVRX-5561	st.clotildes
FZVEJB-5561	st.clotildes
G973T4-5561	st.clotildes
GJ39KG-5561	st.clotildes
GYTEQP-5561	st.clotildes
HQVXJW-5561	st.clotildes
HUFQTD-5561	st.clotildes
HW2LD2-5562	[Participant did not return results for this question.]
J84AQF-5562	st.clotildes
JE9W33-5561	st.clotildes

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6 - Examination Questions

WebCode Test	Response
JGBUAC-5562	st.clotiles
JJDU63-5561	st.clotildes
JL32PY-5562	st.clotildes
JLRZA6-5561	st.clotildes
JPKFX7-5561	St.clotildes
KR28JR-5562	st.clotildes
KR4V3R-5561	st.clotildes
KXRBW6-5562	st.clotildes
KZVDDT-5561	st.clotildes
LDKC3B-5561	st.clotildes
M9HYHY-5561	st.clotildes
MF4Q7B-5561	st.clotildes
MF8B24-5561	st.clotildes
NADTWE-5561	st.clotildes
NE7TEF-5562	st.clotildes
NTANM4-5561	st.clotildes
NTZJR4-5561	st.clotildes
P3ACZC-5561	st.clotildes
P79FU7-5561	st.clotildes
P8ZNUA-5561	st.clotildes
PFEMA7-5562	st.clotildes
PFVN93-5561	st.clotildes

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6 - Examination Questions

WebCode Test	Response
PLGGK2-5561	St.clotildes
PPMYM4-5562	st.clotildes
PTKDEZ-5562	st.clotildes
PUTRGY-5561	st.clotildes
PWJXV6-5561	st.clotildes
Q2CFQV-5561	st.clotildes
Q33NQX-5561	st.clotildes
Q3RHY2-5561	St. Clotildes
QMR3Q2-5561	st.clotildes(2023-03-08 0:22:46 UTC+0)
QRJAR3-5561	st.clotildes
QTHAXU-5561	st.clotildes
RAK67E-5562	st.clotildes
RBBDCA-5562	st.clotildes
RGH4EF-5562	st.clotildes
RRMUMV-5561	st.clotildes
RRXTDK-5562	st.clotildes
RV3JKZ-5561	st.clotildes
TC4JAF-5562	st.clotildes
TCGEBD-5561	st.clotildes
TEPC2R-5562	St clotides
TKFNZV-5561	St clotides
TNEXBT-5561	st.clotildes

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6 - Examination Questions

WebCode Test	Response
TVF9MD-5562	st.clotildes
TX22EP-5561	st.clotildes
U3RQC6-5561	st.clotildes
UKBK6E-5561	st.clotildes
URA8XZ-5561	st.clotildes
UVZCUQ-5562	st.clotildes
V4KY4K-5562	st.clotildes
VCE6WL-5561	st.clotildes
VJH9N7-5561	st.clotildes
VTZR3B-5561	st.clotildes
VVVB8V-5561	st.clotildes
WC9E49-5561	Consolas
WD8DHB-5561	st.clotildes
WK4CUH-5561	st.clotildes
WNN64Y-5561	St.clotildes
WX2YKZ-5561	Not currently within scope of the lab.
WZGLVL-5562	st.clotildes
XA2A8Z-5562	St. Clotildes
XEVDXV-5561	Not in scope
XJ99G2-5562	st.clotildes
XQ9B22-5561	st.clotildes
XVDHZK-5562	[Participant did not return results for this question.]

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6 - Examination Questions

WebCode Test	Response
XWDAB7-5561	st.clotildes
XX78KX-5561	st.clotildes
Y63G92-5562	st.clotildes
YDJQ3P-5561	st.clotildes
YPNENR-5562	st.clotildes
ZPR26J-5561	st.clotildes

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6 - Examination Questions

Question 6: What "replaceString" did user David Lightman LAST use in Notepad, as recorded by the user's registry?

Consensus Result:

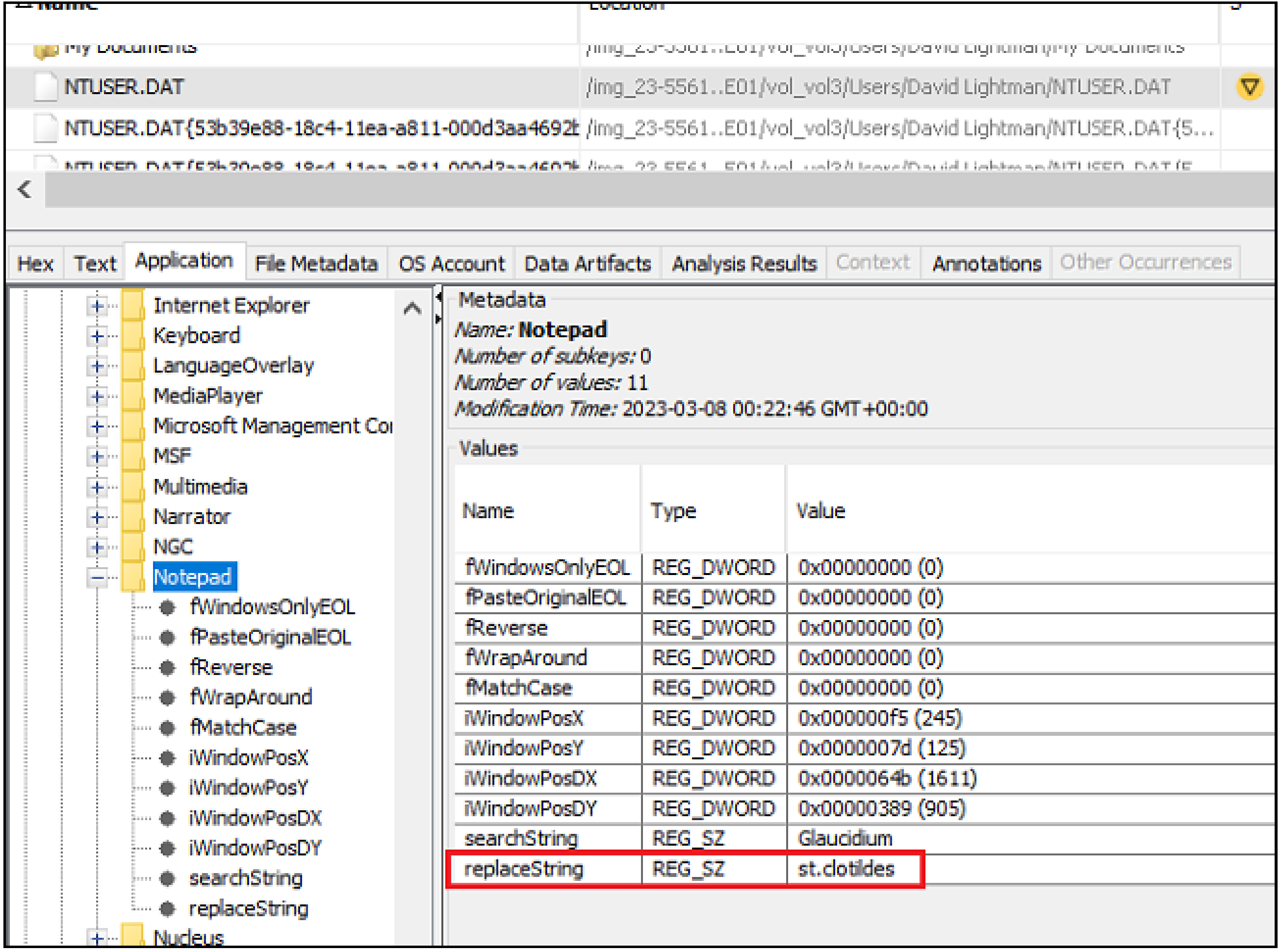
st.clotildes

Expected Response Explanation:

This information is found in David Lightman's user registry at \Users\David Lightman\NTUSER.DAT:Software\Microsoft\Notepad

Expected Response Illustration:

Autopsy view of \Users\David Lightman\NTUSER.DAT:Software\Microsoft\Notepad



Name	Location
NTUSER.DAT	/img_23-5561..E01/vol_vol3/Users/David Lightman/NTUSER.DAT
NTUSER.DAT{53b39e88-18c4-11ea-a811-000d3aa4692b	/img_23-5561..E01/vol_vol3/Users/David Lightman/NTUSER.DAT{5...

Metadata

Name: **Notepad**
Number of subkeys: 0
Number of values: 11
Modification Time: 2023-03-08 00:22:46 GMT+00:00

Values

Name	Type	Value
fWindowsOnlyEOL	REG_DWORD	0x00000000 (0)
fPasteOriginalEOL	REG_DWORD	0x00000000 (0)
fReverse	REG_DWORD	0x00000000 (0)
fWrapAround	REG_DWORD	0x00000000 (0)
fMatchCase	REG_DWORD	0x00000000 (0)
iWindowPosX	REG_DWORD	0x000000f5 (245)
iWindowPosY	REG_DWORD	0x0000007d (125)
iWindowPosDX	REG_DWORD	0x0000064b (1611)
iWindowPosDY	REG_DWORD	0x00000389 (905)
searchString	REG_SZ	Glaucidium
replaceString	REG_SZ	st.clotildes

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7 - Examination Questions

Question 7: When was the computer LAST shutdown gracefully? Provide your response in UTC+0, using the date/time (24-hour) picker which presents the date in the following format: YYYY-MM-DD.

Manufacturer's Expected Response: 2023-03-08 12:45

WebCode Test	Response
2A9WQN-5561	2023-03-08 12:45
2P2VAR-5561	2023-03-08 12:45
2PJFNF-5562	2023-03-08 12:44
2VQ8RL-5562	2023-03-08 12:45
2ZFN6X-5561	2023-03-08 12:45
3CDK6E-5562	2023-03-08 12:45
3DPEPK-5561	2023-03-08 12:45
3M9X4P-5561	2023-03-08 00:45
42BM2N-5561	2023-03-08 12:45
48GFVJ-5561	2023-03-08 12:45
4U7ZP2-5562	2023-03-08 12:45
649HZ6-5561	2023-03-08 12:45
68RW46-5562	2023-03-08 12:45
6DZZCR-5561	2023-03-08 12:45
6MKCN6-5562	2023-03-08 12:45
6Q2RXW-5562	2023-03-08 12:45
6Q4JPC-5561	2023-03-08 12:45
6QKH3A-5562	2023-03-08 12:45
6TR3NP-5561	2023-03-08 12:45
72ZUTD-5561	2023-03-08 12:45

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7 - Examination Questions

WebCode Test	Response
78PAK7-5562	2023-03-08 12:45
7JUP4F-5561	2023-03-08 12:45
7PQ8PM-5562	2023-03-08 12:45
7XZLMH-5562	2023-03-08 12:45
82VWX9-5562	2023-03-08 20:45
83AEYT-5562	2023-03-08 00:45
8CB97J-5561	2023-03-08 12:45
8LJ9TK-5561	2023-03-08 03:02
96TUNQ-5561	2023-03-08 12:45
98ZV8C-5561	2023-03-08 12:45
99QBZK-5562	2023-03-08 12:45
9AJ8JM-5561	2023-03-08 12:45
9J9Q8U-5562	2023-03-08 12:45
A8QHYB-5562	2023-03-08 12:45
A8VQBZ-5561	2023-03-08 12:45
ABK3AJ-5561	2023-03-08 12:45
ACTERK-5561	2023-03-08 12:45
ADYU2Y-5562	2023-03-08 12:45
AKG6BT-5562	2023-03-08 12:45
AM94QQ-5561	2023-03-08 12:45
BFKZWF-5562	2023-03-08 12:45
BQRG78-5561	2023-03-08 12:45

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7 - Examination Questions

WebCode Test	Response
C4LMC9-5562	2023-03-08 12:45
C897D8-5561	2023-03-08 12:45
CF2CBE-5562	2023-03-08 12:45
CKAXYB-5561	2023-03-08 12:45
CP6N6M-5561	2023-03-08 12:45
D7PUVD-5561	2023-03-08 17:45
DB6AM4-5561	2023-03-08 12:45
DGVH9K-5561	2023-03-08 12:45
DXVP3C-5562	2023-03-08 12:45
E2RHRZ-5562	2023-03-08 12:45
E4ZNBG-5561	2023-03-08 12:45
EV7HHF-5561	2023-03-08 12:45
F3JVRX-5561	2023-03-08 12:45
FZVEJB-5561	2023-03-08 12:45
G973T4-5561	2023-03-08 02:59
GJ39KG-5561	2023-03-08 12:45
GYTEQP-5561	2023-03-08 12:45
HQVXJW-5561	2023-03-08 12:45
HUFQTD-5561	2023-03-08 12:45
HW2LD2-5562	[Participant did not return results for this question.]
J84AQF-5562	2023-03-08 12:45
JE9W33-5561	2023-03-08 12:45

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7 - Examination Questions

WebCode Test	Response
JGBUAC-5562	2023-03-08 12:45
JJDU63-5561	2023-03-08 12:45
JL32PY-5562	2023-03-08 12:45
JLRZA6-5561	2023-03-08 12:45
JPKFX7-5561	2023-03-08 12:45
KR28JR-5562	2023-03-08 12:45
KR4V3R-5561	2023-03-08 12:45
KXRBW6-5562	2023-03-08 17:45
KZVDDT-5561	2023-03-08 12:45
LDKC3B-5561	2023-03-08 12:45
M9HYHY-5561	2023-03-08 12:45
MF4Q7B-5561	2023-03-08 12:45
MF8B24-5561	2023-03-08 12:45
NADTWE-5561	2023-03-08 12:45
NE7TEF-5562	2023-03-08 12:45
NTANM4-5561	2023-03-08 12:45
NTZJR4-5561	2023-03-08 12:45
P3ACZC-5561	2023-03-08 12:45
P79FU7-5561	2023-03-08 12:45
P8ZNUA-5561	2023-03-08 12:45
PFEMA7-5562	2023-03-08 12:45
PFVN93-5561	2023-03-08 12:45

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7 - Examination Questions

WebCode Test	Response
PLGGK2-5561	2023-03-08 12:45
PPMYM4-5562	2022-03-08 12:44
PTKDEZ-5562	2023-03-08 12:45
PUTRGY-5561	2023-03-08 02:59
PWJXV6-5561	2023-03-08 10:45
Q2CFQV-5561	2023-03-08 12:45
Q33NQX-5561	2023-03-08 12:45
Q3RHY2-5561	2023-03-08 12:45
QMR3Q2-5561	2023-03-08 12:45
QRJAR3-5561	2023-03-08 12:45
QTHAXU-5561	2023-03-08 12:45
RAK67E-5562	2023-03-08 12:45
RBBDCA-5562	2023-05-08 12:45
RGH4EF-5562	2023-03-08 12:45
RRMUMV-5561	2023-03-08 12:45
RRXTDK-5562	2023-03-08 12:45
RV3JKZ-5561	2023-03-08 02:59
TC4JAF-5562	2023-03-08 12:45
TCGEBD-5561	2023-03-08 12:45
TEPC2R-5562	2023-03-08 12:45
TKFNZV-5561	2023-03-08 12:45
TNEXBT-5561	2023-03-08 12:45

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7 - Examination Questions

WebCode Test	Response
TVF9MD-5562	2023-03-08 12:45
TX22EP-5561	2023-03-08 12:45
U3RQC6-5561	2023-03-08 12:45
UKBK6E-5561	2023-03-08 03:02
URA8XZ-5561	2023-03-08 12:45
UVZCUQ-5562	2023-03-08 12:45
V4KY4K-5562	2023-03-08 12:45
VCE6WL-5561	2023-03-08 12:45
VJH9N7-5561	2023-03-08 12:45
VTZR3B-5561	2023-03-08 12:45
VVVB8V-5561	2023-03-08 12:45
WC9E49-5561	2023-03-08 16:45
WD8DHB-5561	2023-03-08 12:45
WK4CUH-5561	2023-03-08 12:45
WNN64Y-5561	2023-03-08 12:45
WX2YKZ-5561	2023-03-08 16:45
WZGLVL-5562	2023-03-08 04:02
XA2A8Z-5562	2023-03-08 12:45
XEVDXV-5561	2023-03-08 12:45
XJ99G2-5562	2023-03-08 12:45
XQ9B22-5561	2023-03-08 12:45
XVDHZK-5562	[Participant did not return results for this question.]

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7 - Examination Questions

WebCode Test	Response
XWDAB7-5561	2023-03-08 12:45
XX78KX-5561	2023-03-08 12:45
Y63G92-5562	08/03/20232 12:45:15
YDJQ3P-5561	2023-03-08 12:45
YPNENR-5562	2023-03-08 12:45
ZPR26J-5561	2023-03-08 12:45

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7 - Examination Questions

Question 7: When was the computer LAST shutdown gracefully? Provide your response in UTC+0, using the date/time (24-hour) picker which presents the date in the following format: YYYY-MM-DD.

Consensus Result:

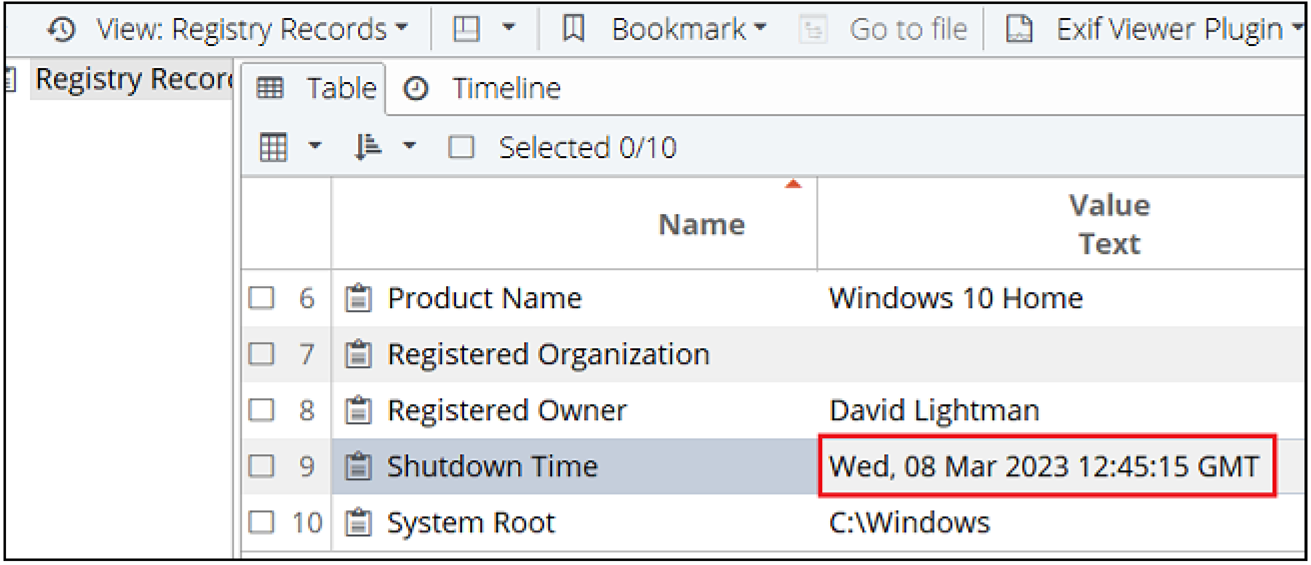
2023-03-08 12:45

Expected Response Explanation:

Information regarding the last shutdown time is found in the registry at C:\Windows\System32\Config\SYSTEM: ControlSet001\Control\Windows\ShutdownTime

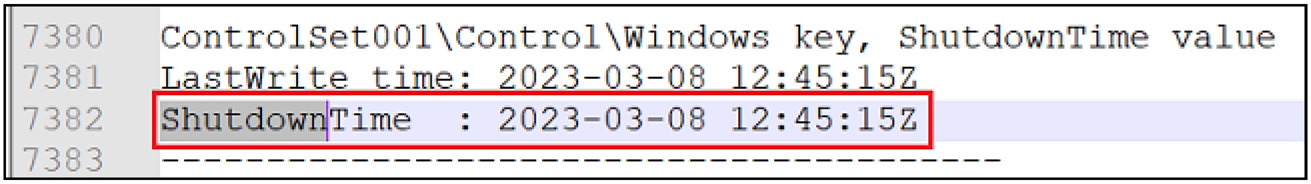
Expected Response Illustration:

EnCase display of ShutdownTime



	Name	Value Text
□ 6	Product Name	Windows 10 Home
□ 7	Registered Organization	
□ 8	Registered Owner	David Lightman
□ 9	Shutdown Time	Wed, 08 Mar 2023 12:45:15 GMT
□ 10	System Root	C:\Windows

RegRipper parse of ShutdownTime



```
ControlSet001\Control\Windows key, ShutdownTime value
LastWrite time: 2023-03-08 12:45:15Z
ShutdownTime  : 2023-03-08 12:45:15Z
----------------------------------------------------
```

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 8 - Examination Questions

Question 8: Was the Guest user account ever logged into?

Manufacturer's Expected Response: No

WebCode Test	Response
2A9WQN-5561	No
2P2VAR-5561	No
2PJFNF-5562	No
2VQ8RL-5562	No
2ZFN6X-5561	No
3CDK6E-5562	No
3DPEPK-5561	No
3M9X4P-5561	No
42BM2N-5561	No
48GFVJ-5561	No
4U7ZP2-5562	No
649HZ6-5561	No
68RW46-5562	No
6DZZCR-5561	No
6MKCN6-5562	No
6Q2RXW-5562	No
6Q4JPC-5561	No
6QKH3A-5562	No
6TR3NP-5561	No
72ZUTD-5561	No
78PAK7-5562	No

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 8 - Examination Questions

WebCode Test	Response
7JUP4F-5561	No
7PQ8PM-5562	No
7XZLMH-5562	No
82VWX9-5562	No
83AEYT-5562	No
8CB97J-5561	No
8LJ9TK-5561	No
96TUNQ-5561	No
98ZV8C-5561	No
99QBZK-5562	No
9AJ8JM-5561	No
9J9Q8U-5562	No
A8QHYB-5562	No
A8VQBZ-5561	No
ABK3AJ-5561	[Participant did not return results for this question.]
ACTERK-5561	No
ADYU2Y-5562	No
AKG6BT-5562	No
AM94QQ-5561	No
BFKZWF-5562	No
BQRG78-5561	No
C4LMC9-5562	No

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 8 - Examination Questions	
WebCode Test	Response
C897D8-5561	No
CF2CBE-5562	No
CKAXYB-5561	No
CP6N6M-5561	No
D7PUVD-5561	No
DB6AM4-5561	No
DGVH9K-5561	No
DXVP3C-5562	No
E2RHRZ-5562	No
E4ZNBG-5561	No
EV7HHF-5561	No
F3JVRX-5561	No
FZVEJB-5561	No
G973T4-5561	No
GJ39KG-5561	No
GYTEQP-5561	No
HQVXJW-5561	No
HUFQTD-5561	No
HW2LD2-5562	[Participant did not return results for this question.]
J84AQF-5562	Yes
JE9W33-5561	No
JGBUAC-5562	No

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 8 - Examination Questions

WebCode Test	Response
JJDU63-5561	No
JL32PY-5562	No
JLRZA6-5561	No
JPKFX7-5561	No
KR28JR-5562	No
KR4V3R-5561	No
KXRBW6-5562	No
KZVDDT-5561	No
LDKC3B-5561	No
M9HYHY-5561	No
MF4Q7B-5561	No
MF8B24-5561	No
NADTWE-5561	No
NE7TEF-5562	No
NTANM4-5561	No
NTZJR4-5561	No
P3ACZC-5561	No
P79FU7-5561	No
P8ZNUA-5561	No
PFEMA7-5562	No
PFVN93-5561	No
PLGGK2-5561	No

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 8 - Examination Questions

WebCode Test	Response
PPMYM4-5562	No
PTKDEZ-5562	No
PUTRGY-5561	No
PWJXV6-5561	No
Q2CFQV-5561	No
Q33NQX-5561	No
Q3RHY2-5561	No
QMR3Q2-5561	No
QRJAR3-5561	No
QTHAXU-5561	No
RAK67E-5562	No
RBBDCA-5562	No
RGH4EF-5562	No
RRMUMV-5561	No
RRXTDK-5562	No
RV3JKZ-5561	No
TC4JAF-5562	No
TCGEBD-5561	No
TEPC2R-5562	No
TKFNZV-5561	No
TNEXBT-5561	No
TVF9MD-5562	No

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 8 - Examination Questions

WebCode Test	Response
TX22EP-5561	No
U3RQC6-5561	No
UKBK6E-5561	No
URA8XZ-5561	No
UVZCUQ-5562	No
V4KY4K-5562	No
VCE6WL-5561	No
VJH9N7-5561	No
VTZR3B-5561	No
VVVB8V-5561	No
WC9E49-5561	No
WD8DHB-5561	No
WK4CUH-5561	No
WNN64Y-5561	No
WX2YKZ-5561	[Participant did not return results for this question.]
WZGLVL-5562	No
XA2A8Z-5562	No
XEVDXV-5561	[Participant did not return results for this question.]
XJ99G2-5562	No
XQ9B22-5561	No
XVDHZK-5562	[Participant did not return results for this question.]
XWDAB7-5561	No

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 8 - Examination Questions

WebCode Test	Response
XX78KX-5561	No
Y63G92-5562	No
YDJQ3P-5561	No
YPNENR-5562	No
ZPR26J-5561	No

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 8 - Examination Questions

Question 8: Was the Guest user account ever logged into?

Consensus Result:

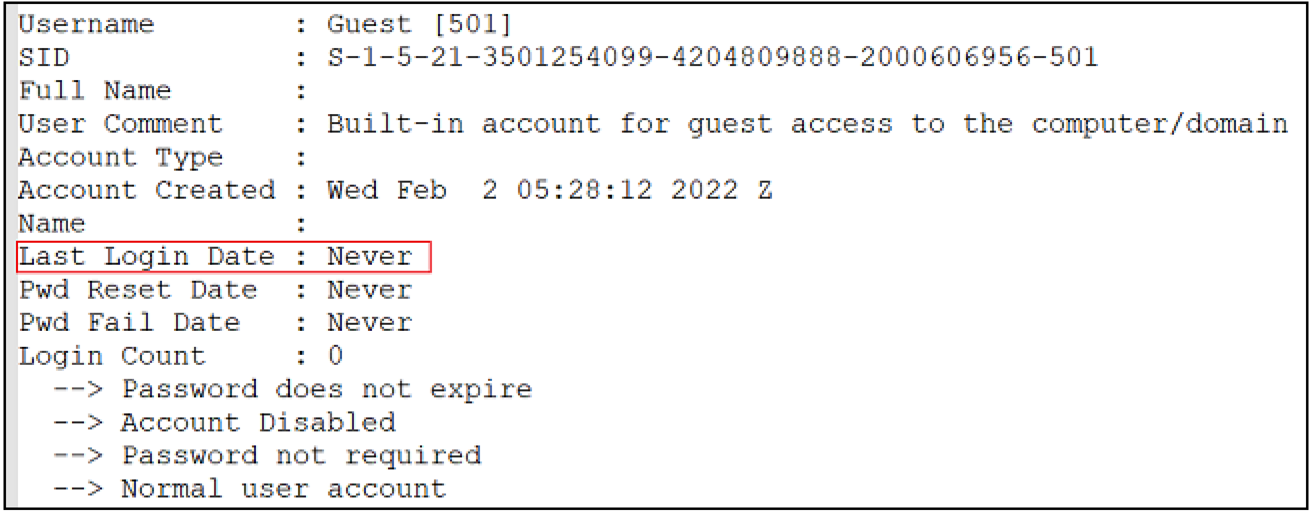
No

Expected Response Explanation:

There are two sources for this information. The security event logs and the Security Accounts Manager (SAM) registry hive. Review of the security event logs (security.evtx) for records related to the Guest account show no successful logins. A review of the SAM registry hive indicates the last login to the Guest account was "never."

Expected Response Illustration:

RegRipper parse of the SAM registry hive



```
Username        : Guest [501]
SID             : S-1-5-21-3501254099-4204809888-2000606956-501
Full Name       :
User Comment    : Built-in account for guest access to the computer/domain
Account Type    :
Account Created : Wed Feb  2 05:28:12 2022 Z
Name            :
Last Login Date : Never
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Login Count     : 0
  --> Password does not expire
  --> Account Disabled
  --> Password not required
  --> Normal user account
```

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 9 - Examination Questions

Question 9: What is the Security ID (SID) of the registered owner's user account?

Manufacturer's Expected Response: S-1-5-21-3501254099-4204809888-2000606956-1007

WebCode Test	Response
2A9WQN-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
2P2VAR-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
2PJFNF-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
2VQ8RL-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
2ZFN6X-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
3CDK6E-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
3DPEPK-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
3M9X4P-5561	1007
42BM2N-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
48GFVJ-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
4U7ZP2-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
649HZ6-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
68RW46-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
6DZZCR-5561	S-1-5-21-3501254099-4204809888-20000606956-1007
6MKCN6-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
6Q2RXW-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
6Q4JPC-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
6QKH3A-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
6TR3NP-5561	1007
72ZUTD-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
78PAK7-5562	S-1-5-21-3501254099-4204809888-2000606956-1007

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 9 - Examination Questions

WebCode Test	Response
7JUP4F-5561	s-1-5-21-3501254099-4204809888-2000606956-1007
7PQ8PM-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
7XZLMH-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
82VWX9-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
83AEYT-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
8CB97J-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
8LJ9TK-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
96TUNQ-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
98ZV8C-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
99QBZK-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
9AJ8JM-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
9J9Q8U-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
A8QHYB-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
A8VQBZ-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
ABK3AJ-5561	NOT IN SCOPE
ACTERK-5561	Not in Scope
ADYU2Y-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
AKG6BT-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
AM94QQ-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
BFKZWF-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
BQRG78-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
C4LMC9-5562	S-1-5-21-3501254099-4204809888-2000606956-1007

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 9 - Examination Questions

WebCode Test	Response
C897D8-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
CF2CBE-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
CKAXYB-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
CP6N6M-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
D7PUVD-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
DB6AM4-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
DGVH9K-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
DXVP3C-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
E2RHRZ-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
E4ZNBG-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
EV7HHF-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
F3JVRX-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
FZVEJB-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
G973T4-5561	S-1-5-21-3501254099-420480988802000606956-1007
GJ39KG-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
GYTEQP-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
HQVXJW-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
HUFQTD-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
HW2LD2-5562	[Participant did not return results for this question.]
J84AQF-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
JE9W33-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
JGBUAC-5562	S-1-5-21-3501254099-4204809888-2000606956-1007

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 9 - Examination Questions

WebCode Test	Response
JJDU63-5561	1007
JL32PY-5562	1007
JLRZA6-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
JPKFX7-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
KR28JR-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
KR4V3R-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
KXRBW6-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
KZVDDT-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
LDKC3B-5561	S-1-5-21-3501254099-4204809888-1007
M9HYHY-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
MF4Q7B-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
MF8B24-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
NADTWE-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
NE7TEF-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
NTANM4-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
NTZJR4-5561	S-1-5-21-3501254099-2000606956-1007
P3ACZC-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
P79FU7-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
P8ZNUA-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
PFEMA7-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
PFVN93-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
PLGGK2-5561	S-1-5-21-3501254099-4204809888-2000606956-1007

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 9 - Examination Questions	
WebCode Test	**Response**
PPMYM4-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
PTKDEZ-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
PUTRGY-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
PWJXV6-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
Q2CFQV-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
Q33NQX-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
Q3RHY2-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
QMR3Q2-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
QRJAR3-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
QTHAXU-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
RAK67E-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
RBBDCA-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
RGH4EF-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
RRMUMV-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
RRXTDK-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
RV3JKZ-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
TC4JAF-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
TCGEBD-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
TEPC2R-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
TKFNZV-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
TNEXBT-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
TVF9MD-5562	S-1-5-21-3501254099-4204809888-2000606956-1007

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 9 - Examination Questions

WebCode Test	Response
TX22EP-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
U3RQC6-5561	1007
UKBK6E-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
URA8XZ-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
UVZCUQ-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
V4KY4K-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
VCE6WL-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
VJH9N7-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
VTZR3B-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
VVVB8V-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
WC9E49-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
WD8DHB-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
WK4CUH-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
WNN64Y-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
WX2YKZ-5561	Not currently within scope of the lab.
WZGLVL-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
XA2A8Z-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
XEVDXV-5561	Not in scope
XJ99G2-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
XQ9B22-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
XVDHZK-5562	[Participant did not return results for this question.]
XWDAB7-5561	S-1-5-21-3501254099-4204809888-2000606956-1007

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 9 - Examination Questions

WebCode Test	Response
XX78KX-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
Y63G92-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
YDJQ3P-5561	S-1-5-21-3501254099-4204809888-2000606956-1007
YPNENR-5562	S-1-5-21-3501254099-4204809888-2000606956-1007
ZPR26J-5561	S-1-5-21-3501254099-4204809888-2000606956-1007

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 9 - Examination Questions

Question 9: What is the Security ID (SID) of the registered owner's user account?

Consensus Result:

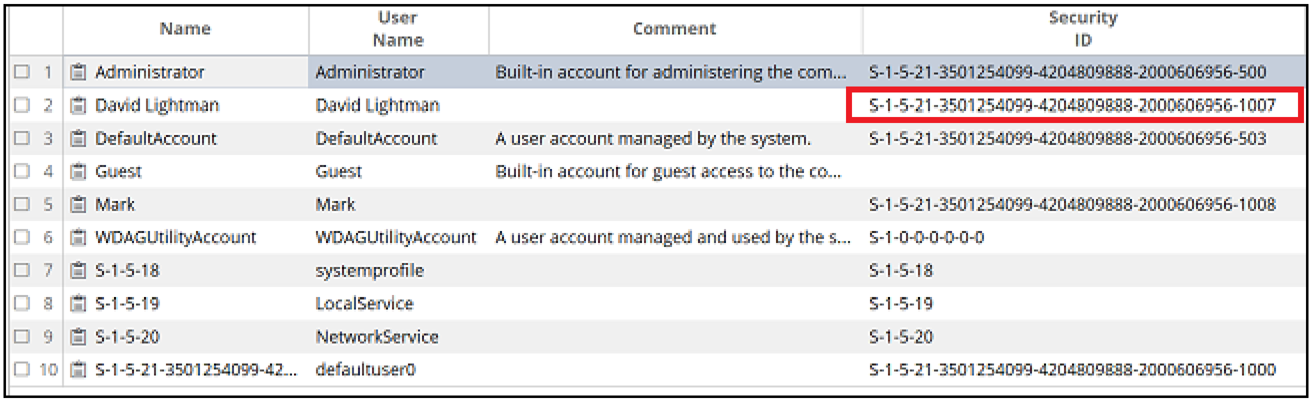
S-1-5-21-3501254099-4204809888-2000606956-1007

Expected Response Explanation:

Information about user (and system) accounts is found in the System Accounts Manager registry hive at C:\Windows\System32\Config\SAM and can be parsed with most forensic suites or a standalone tool like RegRipper or RegistryExplorer.

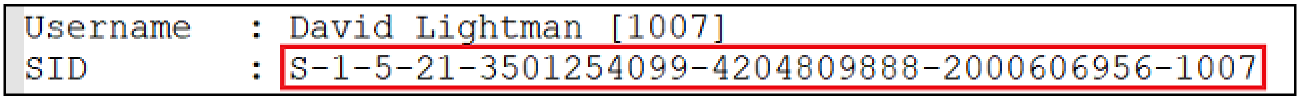
Expected Response Illustration:

EnCase Processor View of User Accounts



	Name	User Name	Comment	Security ID
☐ 1	Administrator	Administrator	Built-in account for administering the com...	S-1-5-21-3501254099-4204809888-2000606956-500
☐ 2	David Lightman	David Lightman		S-1-5-21-3501254099-4204809888-2000606956-1007
☐ 3	DefaultAccount	DefaultAccount	A user account managed by the system.	S-1-5-21-3501254099-4204809888-2000606956-503
☐ 4	Guest	Guest	Built-in account for guest access to the co...	
☐ 5	Mark	Mark		S-1-5-21-3501254099-4204809888-2000606956-1008
☐ 6	WDAGUtilityAccount	WDAGUtilityAccount	A user account managed and used by the s...	S-1-0-0-0-0-0-0
☐ 7	S-1-5-18	systemprofile		S-1-5-18
☐ 8	S-1-5-19	LocalService		S-1-5-19
☐ 9	S-1-5-20	NetworkService		S-1-5-20
☐ 10	S-1-5-21-3501254099-42...	defaultuser0		S-1-5-21-3501254099-4204809888-2000606956-1000

RegRipper view of User Accounts



```
Username    : David Lightman [1007]
SID         : S-1-5-21-3501254099-4204809888-2000606956-1007
```

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 10 - Examination Questions

Question 10: What is the configured time zone?

Manufacturer's Expected Response: Eastern Standard Time, or UTC-5

WebCode Test	Response
2A9WQN-5561	Eastern Standard Time
2P2VAR-5561	Eastern Standard Time with Daylight Savings enabled.
2PJFNF-5562	Eastern Standard Time
2VQ8RL-5562	(UTC-05:00) Eastern Time (US & Canada)
2ZFN6X-5561	Eastern Standard Time
3CDK6E-5562	Eastern Standard Time
3DPEPK-5561	Eastern Standard Time
3M9X4P-5561	Eastern Daylight Time
42BM2N-5561	Eastern Standard Time
48GFVJ-5561	Eastern Standard Time
4U7ZP2-5562	Eastern Standard Time
649HZ6-5561	Eastern Standard Time
68RW46-5562	Eastern Standard Time
6DZZCR-5561	Eastern Standard
6MKCN6-5562	Eastern Standard Time
6Q2RXW-5562	Eastern Standard Time
6Q4JPC-5561	Eastern Standard Time (UTC -5)
6QKH3A-5562	Eastern Standard Time -300 (Minutes)
6TR3NP-5561	Eastern with Daylight Savings Time
72ZUTD-5561	Eastern Standard Time
78PAK7-5562	Eastern Standard Time (UTC-5)

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 10 - Examination Questions

WebCode Test	Response
7JUP4F-5561	est
7PQ8PM-5562	Eastern Standard Time
7XZLMH-5562	EASTERN STANDARD TIME
82VWX9-5562	Eastern Standard Time
83AEYT-5562	Eastern Standard Time
8CB97J-5561	(UTC-05:00) Eastern Time (US & Canada)
8LJ9TK-5561	(UTC-05:00) Eastern Time (US & Canada)
96TUNQ-5561	Eastern Standard Time
98ZV8C-5561	Eastern Standard Time
99QBZK-5562	Eastern Standard Time
9AJ8JM-5561	Eastern Standard Time
9J9Q8U-5562	Eastern
A8QHYB-5562	Eastern Standard Time
A8VQBZ-5561	Eastern Standard Time (UTC -5)
ABK3AJ-5561	Eastern Standard Time
ACTERK-5561	Eastern Standard Time
ADYU2Y-5562	Eastern Standard Time
AKG6BT-5562	Eastern Standard Time
AM94QQ-5561	Eastern Standard Time
BFKZWF-5562	(UTC-05:00) Eastern Time (US & Canada)
BQRG78-5561	Eastern Standard Time (EST)
C4LMC9-5562	Eastern Standard Time

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 10 - Examination Questions

WebCode Test	Response
C897D8-5561	(UTC-05:00) Eastern Time (US & Canada)
CF2CBE-5562	(UTC-05:00) Eastern Time (US & Canada)
CKAXYB-5561	Eastern Standard Time with DaylightTime Active
CP6N6M-5561	(UTC-05:00) Eastern Time (US & Canada)
D7PUVD-5561	(UTC-05:00) Eastern Time (US & Canada)
DB6AM4-5561	(UTC-05:00) Eastern Standard Time
DGVH9K-5561	Eastern
DXVP3C-5562	Eastern Standard Time (UTC - 5:00)
E2RHRZ-5562	Eastern Standard Time
E4ZNBG-5561	Eastern Standard Time
EV7HHF-5561	Eastern Standard Time
F3JVRX-5561	Eastern Standard Time
FZVEJB-5561	Eastern Standard Time
G973T4-5561	(UTC-05:00) Eastern time (us&canada)
GJ39KG-5561	Eastern Standard Time
GYTEQP-5561	Eastern Standard Time
HQVXJW-5561	Eastern Standard Time
HUFQTD-5561	Eastern Standard Time
HW2LD2-5562	[Participant did not return results for this question.]
J84AQF-5562	(UTC-05:00) Eastern Time (US & Canada)
JE9W33-5561	Eastern Standard Time
JGBUAC-5562	(UTC-05:00) Eastern Time (US & Canada)

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 10 - Examination Questions

WebCode Test	Response
JJDU63-5561	Eastern Standard Time
JL32PY-5562	Eastern Standard Time
JLRZA6-5561	Eastern Standard Time
JPKFX7-5561	(UTC -05:00) Eastern Time (US & Canada)
KR28JR-5562	Eastern Standard Time
KR4V3R-5561	Eastern Standard Time
KXRBW6-5562	(UTC-05:00) Eastern Time (US & Canada)
KZVDDT-5561	Eastern Standard Time (UTC-05:00)
LDKC3B-5561	Eastern Standard Time
M9HYHY-5561	Eastern Standard Time
MF4Q7B-5561	Eastern Standard Time (EST)
MF8B24-5561	Eastern Standard Time
NADTWE-5561	Eastern Standard Time
NE7TEF-5562	(UTC-05:00) Eastern Time (US & Canada)
NTANM4-5561	Eastern Standard Time
NTZJR4-5561	Eastern Standard Time
P3ACZC-5561	Eastern Standard Time
P79FU7-5561	Eastern Standard Time
P8ZNUA-5561	Eastern Daylight Time
PFEMA7-5562	(UTC-05:00) Eastern Time (US & Canada)
PFVN93-5561	Eastern Standard Time
PLGGK2-5561	Eastern Standard Time

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 10 - Examination Questions

WebCode Test	Response
PPMYM4-5562	Eastern Standard Time
PTKDEZ-5562	Eastern Standard Time
PUTRGY-5561	(UTC-05:00) Eastern Time (US & Canada)
PWJXV6-5561	Eastern Time Zone
Q2CFQV-5561	(UTC-05:00) Eastern Time (US & Canada)
Q33NQX-5561	Eastern Stadard Time
Q3RHY2-5561	Eastern Standard Time
QMR3Q2-5561	Eastern standard time
QRJAR3-5561	Eastern Standard Time (UTC-5)
QTHAXU-5561	Eastern Standard Time
RAK67E-5562	Eastern Standard Time
RBBDCA-5562	Eastern Standard Time
RGH4EF-5562	Eastern Standard Time (Active Time Bias UTC -5)
RRMUMV-5561	Eastern Standard Time
RRXTDK-5562	(UTC-05:00) Eastern Standard Time (US & Canada)
RV3JKZ-5561	(UTC-05:00) Eastern Time (US & Canada)
TC4JAF-5562	(UTC-05:00) Eastern Time (US & Canada)
TCGEBD-5561	Eastern Standard Time
TEPC2R-5562	Eastern Standard Time
TKFNZV-5561	Eastern Standard Time
TNEXBT-5561	Eastern Standard Time with Daylight Savings
TVF9MD-5562	Eastern Standard Time (UTC -05:00) Eastern Time (US+Canada)

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 10 - Examination Questions

WebCode Test	Response
TX22EP-5561	(UTC-05:00) Eastern Standard Time (US & Canada)
U3RQC6-5561	Eastern Time Zone
UKBK6E-5561	Eastern Standard Time
URA8XZ-5561	(UTC-05:00) Eastern Time (US & Canada)
UVZCUQ-5562	Eastern Standard Time
V4KY4K-5562	Eastern Standard Time (UTC-05:00) Eastern Time (US & Canada)
VCE6WL-5561	Eastern Standard Time
VJH9N7-5561	Eastern Standard Time
VTZR3B-5561	(UTC-05:00) Eastern Time (US & Canada)
VVVB8V-5561	Eastern Standard Time
WC9E49-5561	Eastern Standard Time(EST)
WD8DHB-5561	(UTC-05:00) Eastern Time (US & Canada)
WK4CUH-5561	Eastern Standard Time
WNN64Y-5561	Eastern Standard Time
WX2YKZ-5561	Not currently within scope of the lab.
WZGLVL-5562	(UTC-05:00) Eastern Time (US & Canada)
XA2A8Z-5562	(UTC-05:00) (US & Canada) Eastern Standard Time
XEVDXV-5561	Eastern Standard Time
XJ99G2-5562	Eastern Daylight Time
XQ9B22-5561	Eastern Standard Time
XVDHZK-5562	[Participant did not return results for this question.]
XWDAB7-5561	Eastern Standard Time

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 10 - Examination Questions

WebCode Test	Response
XX78KX-5561	Eastern Standard Time with Daylight Savings Enabled
Y63G92-5562	Eastern Standard Time
YDJQ3P-5561	Eastern Standard Time (UTC - 5:00)
YPNENR-5562	(UTC-05:00) Eastern Time (US & Canada)
ZPR26J-5561	Eastern Standard Time

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 10 - Examination Questions

Question 10: What is the configured time zone?

Consensus Result:

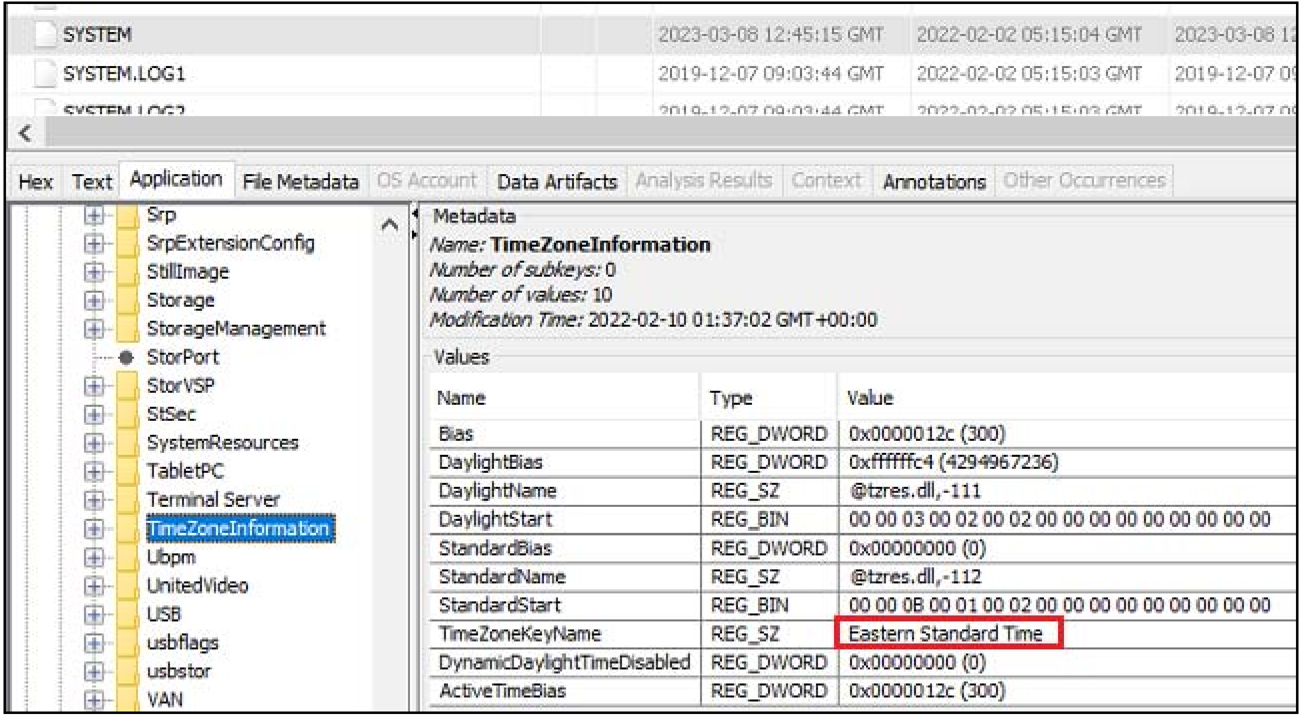
Eastern Standard Time

Expected Response Explanation:

Time zone setting information is found in the SYSTEM registry hive at C:\Windows\System32\Config\SYSTEM:ControlSet001\Control\TimeZoneInformation and can be parsed with most forensic suites or a standalone tool like RegRipper or RegistryExplorer.

Expected Response Illustration:

Autopsy View of TimeZoneInformation key



SYSTEM	2023-03-08 12:45:15 GMT	2022-02-02 05:15:04 GMT	2023-03-08 12
SYSTEM.LOG1	2019-12-07 09:03:44 GMT	2022-02-02 05:15:03 GMT	2019-12-07 0

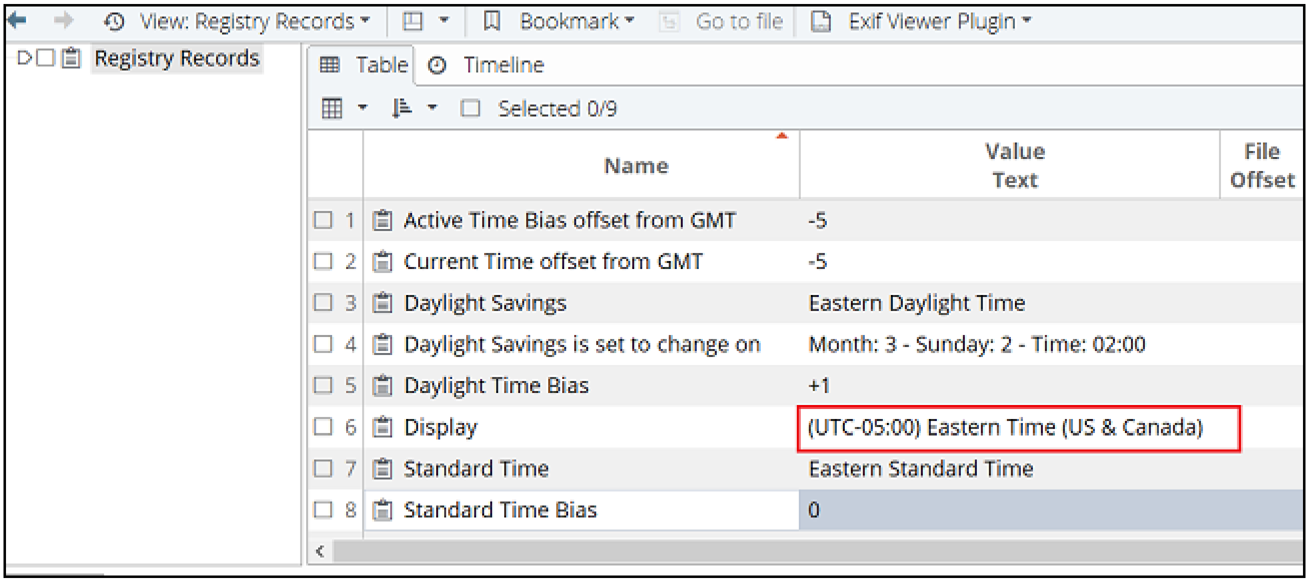
Metadata

Name: **TimeZoneInformation**
Number of subkeys: 0
Number of values: 10
Modification Time: 2022-02-10 01:37:02 GMT+00:00

Values

Name	Type	Value
Bias	REG_DWORD	0x0000012c (300)
DaylightBias	REG_DWORD	0xffffffc4 (4294967236)
DaylightName	REG_SZ	@tzres.dll,-111
DaylightStart	REG_BIN	00 00 03 00 02 00 02 00 00 00 00 00 00 00 00 00
StandardBias	REG_DWORD	0x00000000 (0)
StandardName	REG_SZ	@tzres.dll,-112
StandardStart	REG_BIN	00 00 0B 00 01 00 02 00 00 00 00 00 00 00 00 00
TimeZoneKeyName	REG_SZ	Eastern Standard Time
DynamicDaylightTimeDisabled	REG_DWORD	0x00000000 (0)
ActiveTimeBias	REG_DWORD	0x0000012c (300)

EnCase View of TimeZoneInformation key



	Name	Value Text	File Offset
1	Active Time Bias offset from GMT	-5	
2	Current Time offset from GMT	-5	
3	Daylight Savings	Eastern Daylight Time	
4	Daylight Savings is set to change on	Month: 3 - Sunday: 2 - Time: 02:00	
5	Daylight Time Bias	+1	
6	Display	(UTC-05:00) Eastern Time (US & Canada)	
7	Standard Time	Eastern Standard Time	
8	Standard Time Bias	0	

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 11 - Examination Questions

Question 11: Provide the make and model of device used to capture the photo with hash b793ec04a43c6ff0b09d52e0d14c7bb0ecafc712.

Manufacturer's Expected Response: Google Pixel 5

WebCode Test	Response
2A9WQN-5561	Google Pixel 5
2P2VAR-5561	Google Pixel 5
2PJFNF-5562	model of device : Pixel 5 make : Google
2VQ8RL-5562	Google Pixel 5
2ZFN6X-5561	Google Pixel 5
3CDK6E-5562	Google Pixel 5
3DPEPK-5561	Google Pixel 5
3M9X4P-5561	Google Pixel 5
42BM2N-5561	Google Pixel 5
48GFVJ-5561	Google Pixel 5
4U7ZP2-5562	Google Pixel 5
649HZ6-5561	Google Pixel 5
68RW46-5562	Make: Google. Camera Model Name: Pixel 5
6DZZCR-5561	Google Pixel 5
6MKCN6-5562	Google and Pixel 5
6Q2RXW-5562	Make: Google, Model: Pixel 5
6Q4JPC-5561	b793ec04a43c6ff0b09d52e0d14c7bb0ecafc712
6QKH3A-5562	Google Pixel 5
6TR3NP-5561	Google Pixel 5
72ZUTD-5561	Google Pixel 5 back camera 4.38mm f/1.73

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 11 - Examination Questions

WebCode Test	Response
78PAK7-5562	Google Pixel 5
7JUP4F-5561	Google Pixel 5
7PQ8PM-5562	Google Pixel 5
7XZLMH-5562	GOOGLE PIXEL 5
82VWX9-5562	Make: Google Model: Pixel 5
83AEYT-5562	Google Pixel 5
8CB97J-5561	Google Pixel 5
8LJ9TK-5561	Make: Google, Model: Pixel 5
96TUNQ-5561	Make: Google / Model: Pixel 5
98ZV8C-5561	Google Pixel 5
99QBZK-5562	Google Pixel 5
9AJ8JM-5561	Google Pixel 5
9J9Q8U-5562	Google Pixel 5
A8QHYB-5562	Google Pixel 5
A8VQBZ-5561	Google Pixel 5
ABK3AJ-5561	NOT IN SCOPE
ACTERK-5561	Not in Scope
ADYU2Y-5562	Google Pixel 5
AKG6BT-5562	Google Pixel 5
AM94QQ-5561	Google, Pixel 5
BFKZWF-5562	Google Pixel 5
BQRG78-5561	Google Pixel 5

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 11 - Examination Questions

WebCode Test	Response
C4LMC9-5562	Google Pixel 5
C897D8-5561	Google Pixel 5
CF2CBE-5562	Make: Google, Model: Pixel 5
CKAXYB-5561	Google Pixel5
CP6N6M-5561	Google Pixel 5
D7PUVD-5561	Google Pixel 5
DB6AM4-5561	Google, Pixel 5
DGVH9K-5561	Google Pixel 5
DXVP3C-5562	Google Pixel 5
E2RHRZ-5562	Google Pixel 5
E4ZNBG-5561	Google Pixel 5
EV7HHF-5561	Google Pixel 5
F3JVRX-5561	Google Pixel 5
FZVEJB-5561	Google Pixel 5
G973T4-5561	Make: Google Model: Pixel 5
GJ39KG-5561	Google Pixel 5
GYTEQP-5561	Google Pixel 5
HQVXJW-5561	Google, Pixel 5
HUFQTD-5561	Google Pixel 5
HW2LD2-5562	[Participant did not return results for this question.]
J84AQF-5562	Google Pixel 5
JE9W33-5561	Google Pixel 5

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 11 - Examination Questions

WebCode Test	Response
JGBUAC-5562	Google Pixel 5
JJDU63-5561	Google Pixel 5
JL32PY-5562	Google, Pixel 5
JLRZA6-5561	Google Pixel 5
JPKFX7-5561	Camera Google Pixel 5 back camera 4.38 mm f/173
KR28JR-5562	Google Pixel 5
KR4V3R-5561	Google Pixel 5
KXRBW6-5562	Google Pixel 5
KZVDDT-5561	Google Pixel 5
LDKC3B-5561	Google Pixel 5
M9HYHY-5561	Make: Google Model: Pixel 5 back camera 4.38mm f/1.73
MF4Q7B-5561	Google Pixel 5
MF8B24-5561	Google Pixel 5
NADTWE-5561	Google Pixel 5
NE7TEF-5562	Goole Pixel 5
NTANM4-5561	Make: Google; Model: Pixel 5
NTZJR4-5561	Google Pixel 5
P3ACZC-5561	Google Pixel 5
P79FU7-5561	Google Pixel 5
P8ZNUA-5561	Google Pixel 5
PFEMA7-5562	Google Pixel 5
PFVN93-5561	Google Pixel 5

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 11 - Examination Questions

WebCode Test	Response
PLGGK2-5561	Google Pixel 5
PPMYM4-5562	Google Pixel 5
PTKDEZ-5562	Google Pixel 5
PUTRGY-5561	Google Pixel 5
PWJXV6-5561	Google Pixel 5
Q2CFQV-5561	Google Pixel 5
Q33NQX-5561	Google Pixel 5
Q3RHY2-5561	Google Pixel 5
QMR3Q2-5561	Google Pixel 5
QRJAR3-5561	Google Pixel 5
QTHAXU-5561	Make: Google. Model: Pixel 5.
RAK67E-5562	Google Pixel 5
RBBDCA-5562	Google Pixel 5
RGH4EF-5562	Make =Google – Model =Pixel 5
RRMUMV-5561	Google Pixel 5
RRXTDK-5562	Make: Google. Model: Pixel 5.
RV3JKZ-5561	Make: Google Model: Pixel 5
TC4JAF-5562	Make: Google Model: Pixel 5
TCGEBD-5561	Make: Google Model: Pixel 5
TEPC2R-5562	Make : Google . Model: Pixel 5 camera 4.38mm f/1.73
TKFNZV-5561	Make : Google . Model: Pixel 5 camera 4.38mm f/1.73
TNEXBT-5561	Google Pixel 5

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 11 - Examination Questions

WebCode Test	Response
TVF9MD-5562	Google Pixel 5
TX22EP-5561	Make : Google, Model : Pixel 5
U3RQC6-5561	Google Pixel 5
UKBK6E-5561	Google Piexel 5
URA8XZ-5561	Make: Google, Model: Pixel 5
UVZCUQ-5562	Google Pixel 5
V4KY4K-5562	Google Pixel 5
VCE6WL-5561	GOOGLE PIXEL 5
VJH9N7-5561	The make is Google and the Model is Pixel 5
VTZR3B-5561	Google Pixel 5
VVVB8V-5561	Google Pixel 5
WC9E49-5561	Google Pixel 5
WD8DHB-5561	Google Pixel 5
WK4CUH-5561	Google Pixel 5
WNN64Y-5561	Google Pixel 5
WX2YKZ-5561	Not currently within scope of the lab.
WZGLVL-5562	Google Pixel 5
XA2A8Z-5562	Google Pixel 5
XEVDXV-5561	Not in scope
XJ99G2-5562	Make: Google & Model: Pixel 5
XQ9B22-5561	Google Pixel 5
XVDHZK-5562	[Participant did not return results for this question.]

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 11 - Examination Questions

WebCode Test	Response
XWDAB7-5561	Google Pixel 5
XX78KX-5561	Google Pixel 5
Y63G92-5562	Google Pixel 5
YDJQ3P-5561	Google Pixel 5
YPNENR-5562	Make: Google, Model: Pixel 5
ZPR26J-5561	Google Pixel 5

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 11 - Examination Questions

Question 11: Provide the make and model of device used to capture the photo with hash b793ec04a43c6ff0b09d52e0d14c7bb0ecafc712.

Consensus Result:

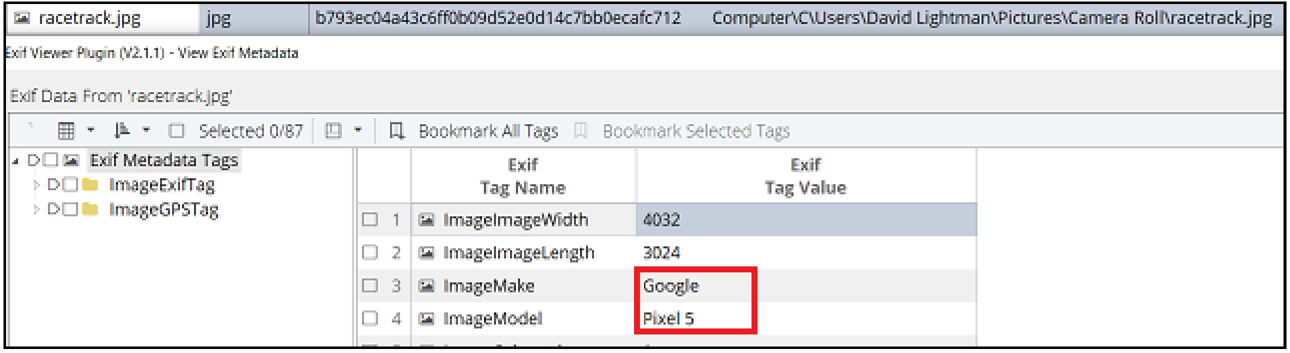
Google Pixel 5 and any slight variation easily identified as a spelling error.

Expected Response Explanation:

Camera capture information is often embedded as EXIF text in jpeg files. Some forensic tools index this kind of metadata. This file can be found by searching its hash, then parsing with an EXIF parsing tool.

Expected Response Illustration:

EnCase EXIF viewer plugin



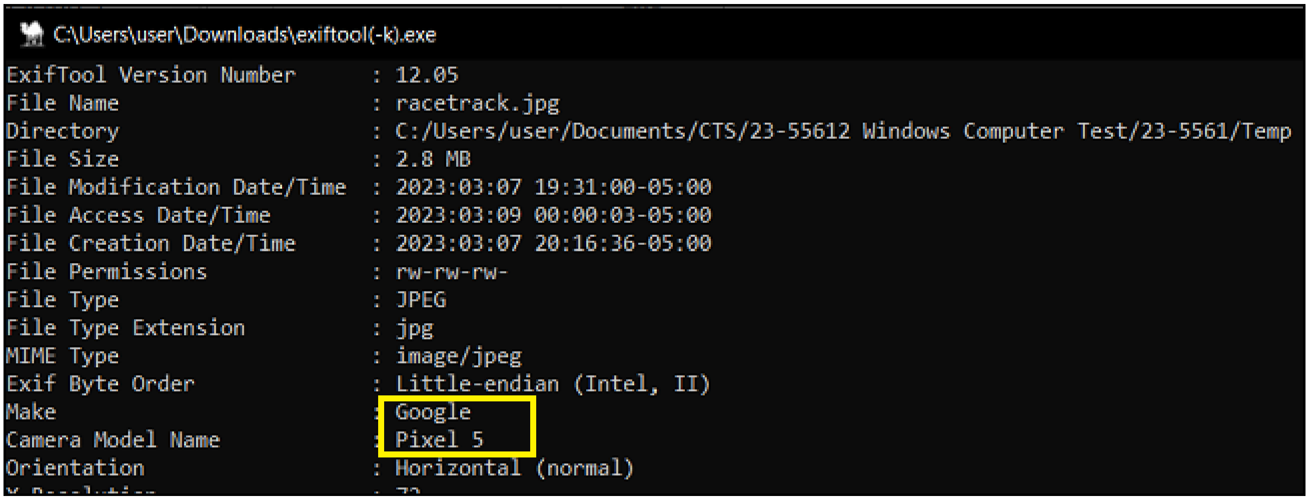
racetrack.jpg | jpg | b793ec04a43c6ff0b09d52e0d14c7bb0ecafc712 | Computer\C\Users\David Lightman\Pictures\Camera Roll\racetrack.jpg

Exif Viewer Plugin (V2.1.1) - View Exif Metadata

Exif Data From 'racetrack.jpg'

		Exif Tag Name	Exif Tag Value
□	1	ImageImageWidth	4032
□	2	ImageImageLength	3024
□	3	ImageMake	Google
□	4	ImageModel	Pixel 5

ExifTool parse of racetrack.jpg



C:\Users\user\Downloads\exiftool(-k).exe

```
ExifTool Version Number         : 12.05
File Name                       : racetrack.jpg
Directory                       : C:/Users/user/Documents/CTS/23-55612 Windows Computer Test/23-5561/Temp
File Size                       : 2.8 MB
File Modification Date/Time     : 2023:03:07 19:31:00-05:00
File Access Date/Time           : 2023:03:09 00:00:03-05:00
File Creation Date/Time         : 2023:03:07 20:16:36-05:00
File Permissions                : rw-rw-rw-
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Little-endian (Intel, II)
Make                            : Google
Camera Model Name               : Pixel 5
Orientation                     : Horizontal (normal)
X Resolution                    : 72
```

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12 - Examination Questions

Question 12: On March 6, 2023 (3/6/23), at 7:56 PM (local time) David Lightman sent an image (photo) via WhatsApp Chat message to another party. Provide the large font text at the top of (in) the image.

Manufacturer's Expected Response: Gradebook – Grades – Quarter 1

WebCode Test	Response
2A9WQN-5561	Gradebook - Grades - Quarter 1
2P2VAR-5561	Gradebook - Grades - Quarter 1
2PJFNF-5562	Gradebook-Grades-Quater 1
2VQ8RL-5562	Gradebook - Grades - Quarter 1
2ZFN6X-5561	Gradebook – Grades – Quarter 1
3CDK6E-5562	Gradebook – Grades - Quarter 1
3DPEPK-5561	Gradebook – Grades - Quarter 1
3M9X4P-5561	Gradebook - Grades - Quarter 1
42BM2N-5561	Gradebook – Grades – Quarter 1
48GFVJ-5561	Gradebook - Grades - Quarter 1
4U7ZP2-5562	Gradebook - Grades - Quarter 1
649HZ6-5561	Gradebook - Grades - Quarter 1
68RW46-5562	Gradebook - Grades - Quarter 1
6DZZCR-5561	MCO 270
6MKCN6-5562	Gradebook - Grades - Quarter 1
6Q2RXW-5562	Gradebook – Grades – Quarter 1
6Q4JPC-5561	Gradebook – Grades – Quarter 1
6QKH3A-5562	Gradebook – Grades - Quarter 1
6TR3NP-5561	"Rosario Student Informati"
72ZUTD-5561	Gradebook – Grades – Quarter 1

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12 - Examination Questions

WebCode Test	Response
78PAK7-5562	Gradebook – Grades – Quarter 1
7JUP4F-5561	gradebook - grades - quarter 1
7PQ8PM-5562	Gradebook - Grades - Quarter 1
7XZLMH-5562	GRADEBOOK – GRADES – QUARTER 1
82VWX9-5562	Gradebook – Grades - Quarter 1
83AEYT-5562	Gradebook - Grades – Quarter 1
8CB97J-5561	Gradebook - Grades - Quarter 1
8LJ9TK-5561	Gradebook – Grades – Quarter 1
96TUNQ-5561	Gradebook – Grades – Quarter 1
98ZV8C-5561	Gradebook - Grades - Quarter 1
99QBZK-5562	Gradebook - Grades - Quarter 1
9AJ8JM-5561	Gradebook - Grades - Quarter 1
9J9Q8U-5562	Gradebook - Grades - Quarter 1
A8QHYB-5562	Rosario Student Informati
A8VQBZ-5561	Gradebook - Grades - Quarter 1
ABK3AJ-5561	NOT IN SCOPE
ACTERK-5561	Not in Scope
ADYU2Y-5562	Gradebook – Grades – Quarter 1
AKG6BT-5562	Gradebook – Grades – Quarter 1
AM94QQ-5561	Gradebook – Grades – Quarter 1
BFKZWF-5562	Gradebook - Grades - Quarter 1
BQRG78-5561	Gradebook - Grades - Quarter 1

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12 - Examination Questions

WebCode Test	Response
C4LMC9-5562	Gradebook - Grades - Quarter 1
C897D8-5561	Gradebook-Grades-Quarter 1
CF2CBE-5562	Gradebook - Grades - Quarter 1
CKAXYB-5561	Gradebook-Grades-Quarter 1
CP6N6M-5561	Gradebook - Grades - Quarter 1
D7PUVD-5561	Gradebook – Grades – Quarter 1
DB6AM4-5561	Gradebook – Grades – Quarter 1
DGVH9K-5561	Gradebook - Grades - Quarter 1
DXVP3C-5562	Gradebook - Grades - Quarter 1 (No data found for March 6, on March 7, this image is found)
E2RHRZ-5562	Gradebook – Grades – Quarter 1
E4ZNBG-5561	Gradebook – Grades – Quarter 1
EV7HHF-5561	Gradebook – Grades – Quarter 1
F3JVRX-5561	Gradebook – Grades – Quarter 1
FZVEJB-5561	"Gradebook – Grades – Quarter 1"
G973T4-5561	Gradebook - Grades - Quarter 1
GJ39KG-5561	Gradebook - Grades - Quarter 1
GYTEQP-5561	Gradebook - Grades - Quarter 1
HQVXJW-5561	Gradebook – Grades – Quarter 1
HUFQTD-5561	Gradebook – Grades – Quarter1
HW2LD2-5562	[Participant did not return results for this question.]
J84AQF-5562	Gradebook - Grades- Quarter 1
JE9W33-5561	Gradebook – Grades – Quarter 1

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12 - Examination Questions

WebCode Test	Response
JGBUAC-5562	Gradebook-Grades-Quarter 1
JJDU63-5561	Gradebook - Grades - Quarter 1
JL32PY-5562	Gradebook – Grades – Quarter 1
JLRZA6-5561	Gradebook - Grades - Quarter 1
JPKFX7-5561	GRADEBOOK-GRADES-QUARTER1
KR28JR-5562	Gradebook – Grades – Quarter 1
KR4V3R-5561	Gradebook - Grades - Quarter 1
KXRBW6-5562	Gradebook – Grades – Quarter 1
KZVDDT-5561	Gradebook - Grades - Quarter 1
LDKC3B-5561	Gradebook - Grades - Quarter 1
M9HYHY-5561	Gradebook – Grades – Quarter 1
MF4Q7B-5561	Gradebook – Grades – Quarter 1
MF8B24-5561	Gradebook-Grades-Quarter 1
NADTWE-5561	Gradebook – Grades – Quarter 1
NE7TEF-5562	Gradebook - Grades - Quarter 1
NTANM4-5561	Gradebook - Grades - Quarter 1
NTZJR4-5561	Gradebook - Grades - Quarter 1
P3ACZC-5561	Gradebook-Grades-Quarter 1
P79FU7-5561	Gradebook – Grades – Quarter 1
P8ZNUA-5561	Gradebook-Grades-Quarter 1
PFEMA7-5562	Gradebook – Grades – Quarter 1
PFVN93-5561	Gradebook-Grades-Quarter 1

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12 - Examination Questions

WebCode Test	Response
PLGGK2-5561	Gradebook - Grades - Quarter 1
PPMYM4-5562	Gradebook - Grades - Quarter 1
PTKDEZ-5562	Gradebook - Grades - Quarter 1
PUTRGY-5561	Gradebook - Grades - Quarter 1
PWJXV6-5561	Gradebook-Grades-Quarter1
Q2CFQV-5561	Gradebook-Grades-Quarter 1
Q33NQX-5561	Gradebook - Grades - Quarter 1
Q3RHY2-5561	Gradebook-Grades-Quarter 1
QMR3Q2-5561	Gradebook-Grades-Quarter1
QRJAR3-5561	Gradebook-Grades-Quarter 1
QTHAXU-5561	Gradebook-Grades Quarter 1
RAK67E-5562	Gradebook - Grades - Quarter 1
RBBDCA-5562	Gradebook - Grades - Quarter 1
RGH4EF-5562	(from file: IMG-20230306-WA0001.jpg) Gradebook – Grades – Quarter 1
RRMUMV-5561	Gradebook – Grades – Quarter 1
RRXTDK-5562	Gradebook - Grades - Quarter 1
RV3JKZ-5561	Gradebook - Grades - Quarter 1
TC4JAF-5562	Gradebook - Grades - Quarter 1
TCGEBD-5561	Gradebook - Grades - Quarter 1
TEPC2R-5562	Gradebook - Grades - Quarter 1
TKFNZV-5561	Gradebook - Grades - Quarter 1
TNEXBT-5561	Gradebook - Grades - Quarter 1

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12 - Examination Questions

WebCode Test	Response
TVF9MD-5562	Gradebook-Grades-Quarter 1
TX22EP-5561	Gradebook – Grade – Quarter 1
U3RQC6-5561	Gradebook – Grades – Quarter 1
UKBK6E-5561	Gradebook - Grades - Quarter1
URA8XZ-5561	Gradebook - Grades - Quarter 1
UVZCUQ-5562	Gradebook - Grades - Quarter 1
V4KY4K-5562	Gradebook – Grades – Quarter 1
VCE6WL-5561	GradeBook - Grades - Quarter 1
VJH9N7-5561	Gradebook – Grades – Quarter 1
VTZR3B-5561	Gradebook – Grades – Quarter 1
VVVB8V-5561	Gradebook – Grades – Quarter 1
WC9E49-5561	[Participant did not return results for this question.]
WD8DHB-5561	Gradebook – Grades – Quarter 1
WK4CUH-5561	Gradebook - Grades - Quarter 1
WNN64Y-5561	Gradebook - Grades - Quarter 1
WX2YKZ-5561	Not currently within scope of the lab.
WZGLVL-5562	Gradebook - Grades - Quarter 1
XA2A8Z-5562	Gradebook - Grades - Quarter 1
XEVDXV-5561	Not in scope
XJ99G2-5562	Gradebook - Grades - Quarter 1
XQ9B22-5561	Gradebook – Grades – Quarter1
XVDHZK-5562	[Participant did not return results for this question.]

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12 - Examination Questions

WebCode Test	Response
XWDAB7-5561	Gradebook-Grades-Quarter 1
XX78KX-5561	Gradebook – Grades – Quarter 1
Y63G92-5562	Gradebook-Grades-Quarter1
YDJQ3P-5561	Gradebook - Grades - Quarter 1 (No data found for March 6, on March 7, this image is found)
YPNENR-5562	Gradebook - Grades - Quarter 1
ZPR26J-5561	Gradebook-Grades-Quarter 1

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12 - Examination Questions

Question 12: On March 6, 2023 (3/6/23), at 7:56 PM (local time) David Lightman sent an image (photo) via WhatsApp Chat message to another party. Provide the large font text at the top of (in) the image.

Consensus Result:

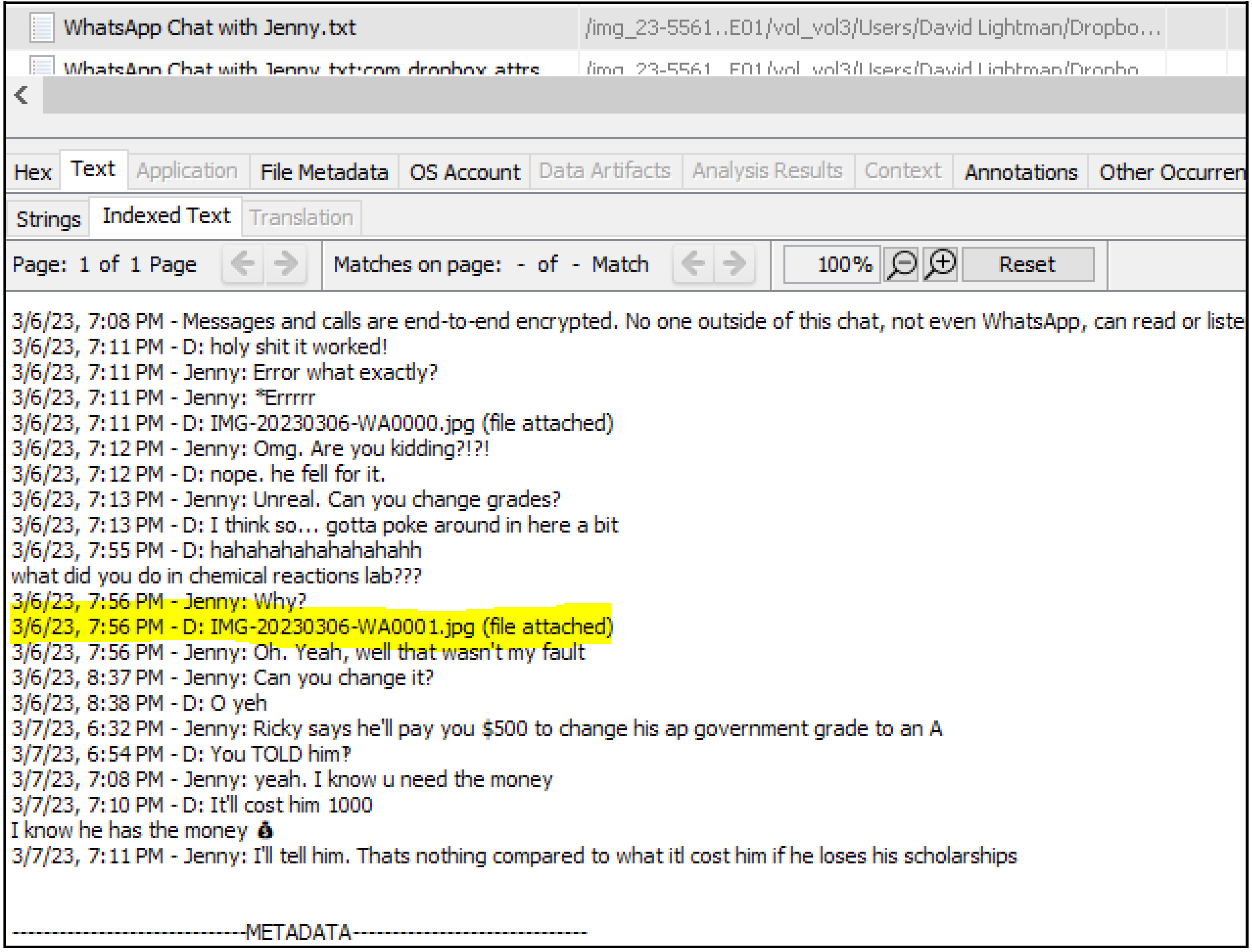
"Gradebook – Grades – Quarter 1" and any slight variation easily identified as a spelling error.

Expected Response Explanation:

An exported WhatsApp chat can be found via keyword search (for WhatsApp) in C:\Users\David Lightman\Dropbox\e\. That chat lists the messages sent and received. Among those is a record of a photo IMG-20230306-WA0001.jpg, sent on March 6, 2023 at 7:56 PM.

Expected Response Illustration:

C:\Users\David Lightman\Dropbox\e\WhatsApp Chat with Jenny.txt



WhatsApp Chat with Jenny.txt
/img_23-5561..E01/vol_vol3/Users/David Lightman/Dropbo...
WhatsApp Chat with Jenny.txt:com.dropbox.attrs
/img_23-5561..E01/vol_vol3/Users/David Lightman/Dropbo
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurren
Strings
Indexed Text
Translation
Page: 1 of 1 Page
Matches on page: - of - Match
100%
Reset

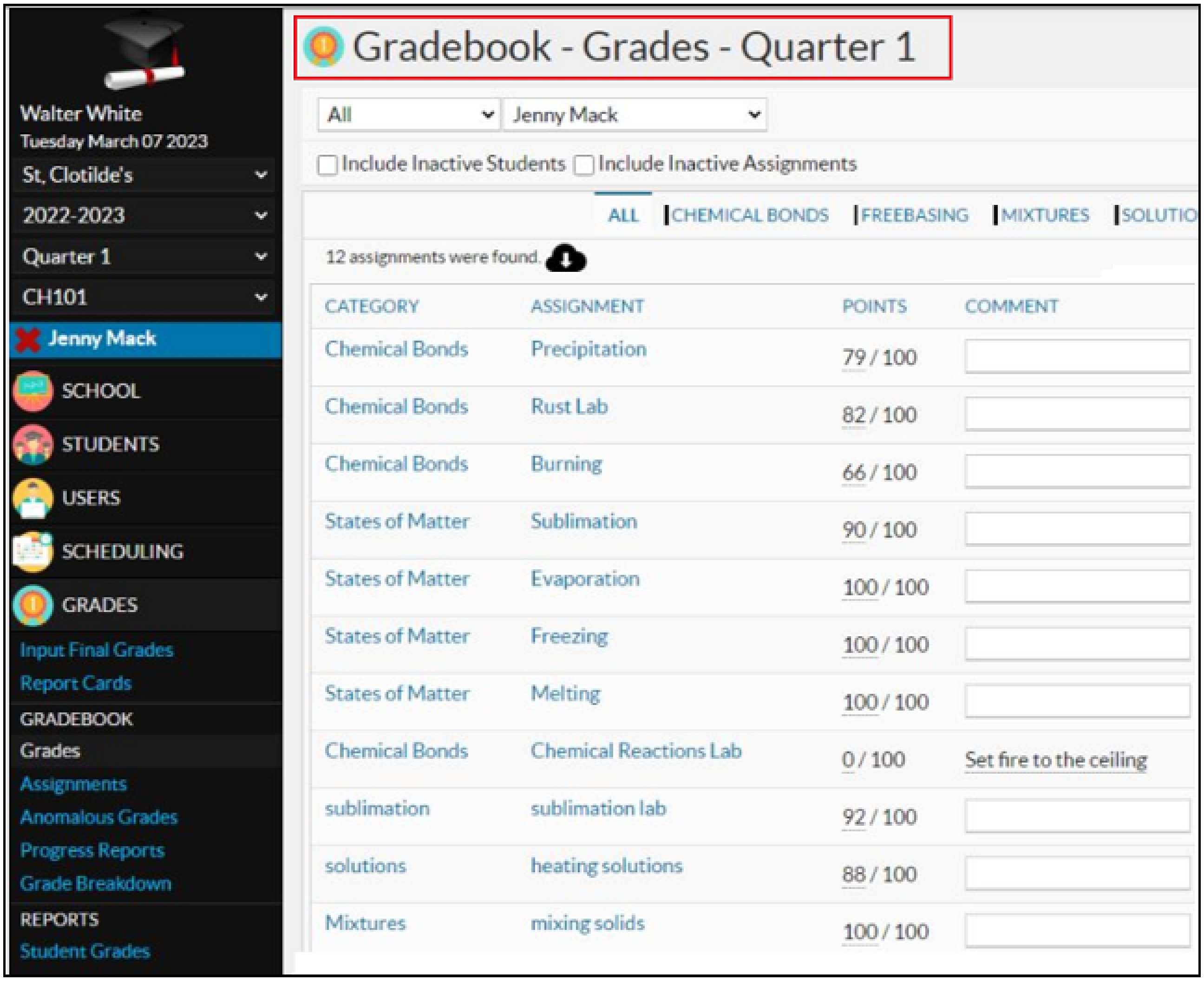
```
3/6/23, 7:08 PM - Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or liste
3/6/23, 7:11 PM - D: holy shit it worked!
3/6/23, 7:11 PM - Jenny: Error what exactly?
3/6/23, 7:11 PM - Jenny: *Errrrr
3/6/23, 7:11 PM - D: IMG-20230306-WA0000.jpg (file attached)
3/6/23, 7:12 PM - Jenny: Omg. Are you kidding?!?!
3/6/23, 7:12 PM - D: nope. he fell for it.
3/6/23, 7:13 PM - Jenny: Unreal. Can you change grades?
3/6/23, 7:13 PM - D: I think so... gotta poke around in here a bit
3/6/23, 7:55 PM - D: hahahahahahahahahh
what did you do in chemical reactions lab???
3/6/23, 7:56 PM - Jenny: Why?
3/6/23, 7:56 PM - D: IMG-20230306-WA0001.jpg (file attached)
3/6/23, 7:56 PM - Jenny: Oh. Yeah, well that wasn't my fault
3/6/23, 8:37 PM - Jenny: Can you change it?
3/6/23, 8:38 PM - D: O yeh
3/7/23, 6:32 PM - Jenny: Ricky says he'll pay you $500 to change his ap government grade to an A
3/7/23, 6:54 PM - D: You TOLD him?
3/7/23, 7:08 PM - Jenny: yeah. I know u need the money
3/7/23, 7:10 PM - D: It'll cost him 1000
I know he has the money 💰
3/7/23, 7:11 PM - Jenny: I'll tell him. Thats nothing compared to what itl cost him if he loses his scholarships


------------------------------METADATA------------------------------
```

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12 - Examination Questions

Users\David Lightman\Dropbox\e\IMG-20230306-WA0001.jpg



Walter White
Tuesday March 07 2023
St, Clotilde's
2022-2023
Quarter 1
CH101
Jenny Mack

Gradebook - Grades - Quarter 1

All | Jenny Mack

□ Include Inactive Students □ Include Inactive Assignments

12 assignments were found.

CATEGORY	ASSIGNMENT	POINTS	COMMENT
Chemical Bonds	Precipitation	79 / 100	
Chemical Bonds	Rust Lab	82 / 100	
Chemical Bonds	Burning	66 / 100	
States of Matter	Sublimation	90 / 100	
States of Matter	Evaporation	100 / 100	
States of Matter	Freezing	100 / 100	
States of Matter	Melting	100 / 100	
Chemical Bonds	Chemical Reactions Lab	0 / 100	Set fire to the ceiling
sublimation	sublimation lab	92 / 100	
solutions	heating solutions	88 / 100	
Mixtures	mixing solids	100 / 100	

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13 - Examination Questions

Question 13: What website did user David Lightman visit with the Google Chrome browser on 25 February 2023 (2023-02-25) at 21:52:02 GMT? Provide the full URL.

Manufacturer's Expected Response: http://stclotildes.institute/sample-page/

WebCode Test	Response
2A9WQN-5561	http://stclotildes.institute/sample-page/
2P2VAR-5561	http://stclotildes.institute/sample-page/
2PJFNF-5562	http://stclotildes.institute/sample-page/
2VQ8RL-5562	http://stclotildes.institute/sample-page/
2ZFN6X-5561	http://stclotildes.institute/sample-page
3CDK6E-5562	st.clotildes.institute
3DPEPK-5561	http://stclotildes.institute/sample-page/
3M9X4P-5561	http://stclotildes.institute/sample-page/
42BM2N-5561	http://stclotildes.institute/sample-page/
48GFVJ-5561	http://stclotildes.institute/sample-page/
4U7ZP2-5562	http://stclotildes.institute/sample-page/
649HZ6-5561	http://stclotildes.institute/sample-page/
68RW46-5562	http://stclotildes.institute/sample-page/
6DZZCR-5561	http://stclotildes.institute/sample-page1
6MKCN6-5562	http://stclotildes.institute/sample-page/
6Q2RXW-5562	http://stclotildes.institute/sample-page/
6Q4JPC-5561	http://stclotildes.institute/sample-page/
6QKH3A-5562	http://stclotildes.institute/sample-page/
6TR3NP-5561	http://portal.stclotildes.institute/index.php
72ZUTD-5561	http://stclotildes.institute/sample-page/

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13 - Examination Questions

WebCode Test	Response
78PAK7-5562	http://stclotildes.institute/sample-page/
7JUP4F-5561	http://stclotildes.institute/sample-page/
7PQ8PM-5562	http://stclotildes.institute/sample-page/
7XZLMH-5562	http://stclotildes.institute/sample-page/
82VWX9-5562	http://stclotildes.institute/sample-page/
83AEYT-5562	http://stclotildes.institute/sample-page/
8CB97J-5561	http://stclotildes.institute/sample-page/
8LJ9TK-5561	http://stclotildes.institute/sample-page/
96TUNQ-5561	http://stclotildes.institute/sample-page/
98ZV8C-5561	http://stclotildes.institute/sample-page/
99QBZK-5562	http://stclotildes.institute/sample-page/
9AJ8JM-5561	http://stclotildes.institute/sample-page/
9J9Q8U-5562	http://stclotildes.institute/sample-page/
A8QHYB-5562	http://stclotildes.institute/sample-page/
A8VQBZ-5561	http://stclotildes.institute/sample-page/
ABK3AJ-5561	NOT IN SCOPE
ACTERK-5561	Not in Scope
ADYU2Y-5562	http://stclotildes.institute/sample-page/
AKG6BT-5562	http://stclotildes.institute/sample-page/
AM94QQ-5561	http://stclotildes.institute/sample-page/
BFKZWF-5562	http://stclotildes.institute/sample-page/
BQRG78-5561	http://stclotildes.institute/sample-page/

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13 - Examination Questions

WebCode Test	Response
C4LMC9-5562	http://stclotildes.institute/sample-page/
C897D8-5561	http://stclotildes.institute/sample-page/
CF2CBE-5562	http://stclotildes.institute/sample-page/
CKAXYB-5561	http://stclotildes.institute/sample-page/
CP6N6M-5561	http://stclotildes.institute/sample-page/
D7PUVD-5561	http://stclotildes.institute/sample-page/
DB6AM4-5561	http://stclotildes.institute/sample-page/
DGVH9K-5561	http://stclotildes.institute/sample-page/
DXVP3C-5562	http://stclotildesinstitute/sample-page/
E2RHRZ-5562	http://stclotildes.institute/sample-page/
E4ZNBG-5561	http://stclotildes.institute/sample-page/
EV7HHF-5561	http://stclotildes.institute/sample-page/
F3JVRX-5561	http://stclotildes.institute/sample-page/
FZVEJB-5561	http://stclotildes.institute/sample-page/
G973T4-5561	http://stclotildes.institute/sample-page/
GJ39KG-5561	http://stclotildes.institute/sample-page/
GYTEQP-5561	http://stclotildes.institute/sample-page/
HQVXJW-5561	http://stclotildes.institute/sample-page/
HUFQTD-5561	http://stclotildes.institute/sample-page/
HW2LD2-5562	[Participant did not return results for this question.]
J84AQF-5562	http://stclotildes.institute/sample-page/
JE9W33-5561	http://stclotildes.institute/sample-page/

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13 - Examination Questions

WebCode Test	Response
JGBUAC-5562	http://stclotildes.institute/sample-page/
JJDU63-5561	http://stclotildes.institute/sample-page/
JL32PY-5562	http://stclotildes.institute/sample-page/
JLRZA6-5561	http://stclotildes.institute/sample-page/
JPKFX7-5561	http://stclotildes.institute/sample-page/
KR28JR-5562	http://stclotildes.institute/sample-page/
KR4V3R-5561	http://stclotildes.institute/sample-page/
KXRBW6-5562	http://stclotildes.institute/sample-page/
KZVDDT-5561	http://stclotildes.institute/sample-page/
LDKC3B-5561	http://stclotildes.institute/sample-page/
M9HYHY-5561	http://stclotildes.institute/sample-page/
MF4Q7B-5561	http://stclotildes.institute/sample-page/
MF8B24-5561	http://stclotildes.institute/sample-page/
NADTWE-5561	http://stclotildes.institute/sample-page/
NE7TEF-5562	http://stclotildes.institute/sample-page/
NTANM4-5561	http://stclotildes.institute/sample-page/
NTZJR4-5561	http://stclotildes.institute/sample-page/
P3ACZC-5561	http://stclotildes.institute/sample-page/
P79FU7-5561	http://stclotildes.institute/sample-page/
P8ZNUA-5561	http://stclotildes.institute/sample-page/
PFEMA7-5562	http://stclotildes.institute/sample-page/
PFVN93-5561	http://stclotildes.institute/sample-page/

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13 - Examination Questions

WebCode Test	Response
PLGGK2-5561	http://stclotildes.institute/sample-page
PPMYM4-5562	http://stclotildes.institute/sample-page/
PTKDEZ-5562	http://stclotildes.institute/sample-page/
PUTRGY-5561	http://stclotildes.institute/sample-page/
PWJXV6-5561	http://stclotildes.institute/sample-page/
Q2CFQV-5561	http://stclotildes.institute/sample-page/
Q33NQX-5561	http://stclotildes.institute/sample-page/
Q3RHY2-5561	http://stclotildes.institute/sample-page/
QMR3Q2-5561	http://stclotildes.institute/sample-page/
QRJAR3-5561	http://stclotildes.institute/sample-page/
QTHAXU-5561	http://stclotildes.institute/sample-page/
RAK67E-5562	http://stclotildes.institute/sample-page/
RBBDCA-5562	http://stclotildes.institute/sample-page/
RGH4EF-5562	http://stclotildes.institute/sample-page/
RRMUMV-5561	http://stclotildes.institute/sample-page/
RRXTDK-5562	http://stclotildes.institute/sample-page/
RV3JKZ-5561	http://stclotildes.institute/sample-page/
TC4JAF-5562	http://stclotildes.institute/sample-page/
TCGEBD-5561	http://stclotildes.institute/sample-page/
TEPC2R-5562	http://stclotildes.institute/sample-page/
TKFNZV-5561	http://stclotildes.institute/sample-page/
TNEXBT-5561	http://stclotildes.institute/sample-page/

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13 - Examination Questions

WebCode Test	Response
TVF9MD-5562	http://stclotildes.institute/sample-page/
TX22EP-5561	http://stclotildes.institute/sample-page/
U3RQC6-5561	http://stclotildes.institute/sample-page/
UKBK6E-5561	http://stclotildes.institute/sample-page/
URA8XZ-5561	http://stclotildes.institute/sample-page/
UVZCUQ-5562	http://stclotildes.institute/sample-page/
V4KY4K-5562	http://stclotildes.institute/sample-page/
VCE6WL-5561	http://stclotildes.institute/sample-page/
VJH9N7-5561	http://stclotildes.institute/sample-page/
VTZR3B-5561	http://stclotildes.institute/sample-page/
VVVB8V-5561	http://stclotildes.institute/sample-page/
WC9E49-5561	News.google.com
WD8DHB-5561	http://stclotildes.institute/sample-page/
WK4CUH-5561	http://stclotildes.institute/sample-page/
WNN64Y-5561	http://stclotildes.institute/sample-page/
WX2YKZ-5561	Not currently within scope of the lab.
WZGLVL-5562	http://stclotildes.institute/sample-page/
XA2A8Z-5562	http://stclotildes.institute/sample-page/
XEVDXV-5561	Not in scope
XJ99G2-5562	Website: stclotildes.institute & URL: http://stclotildes.institute/sample-page
XQ9B22-5561	http://stclotildes.institute/sample-page/
XVDHZK-5562	[Participant did not return results for this question.]

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13 - Examination Questions

WebCode Test	Response
XWDAB7-5561	http://stclotildes.institute/sample-page/
XX78KX-5561	http://stclotildes.institute/sample-page/
Y63G92-5562	http:/stclotildes.institute/sample-page
YDJQ3P-5561	http://stclotildesinstitute/sample-page/
YPNENR-5562	http://stclotildes.institute/sample-page/
ZPR26J-5561	http://stclotildes.institute/sample-page/

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13 - Examination Questions

Question 13: What website did user David Lightman visit with the Google Chrome browser on 25 February 2023 (2023-02-25) at 21:52:02 GMT? Provide the full URL.

Consensus Result:

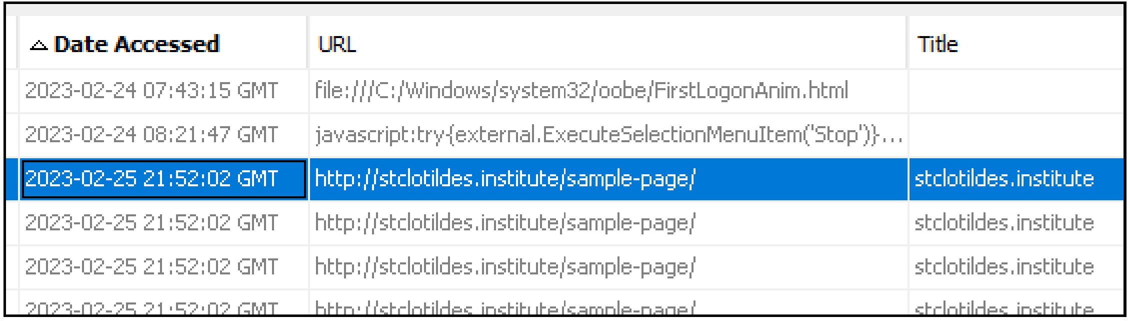
http://stclotildes.institute/sample-page/

Expected Response Explanation:

Chrome history events for this user are stored in
C:\Users\David Lightman\AppData\Local\Google\Chrome\User Data\Default\History

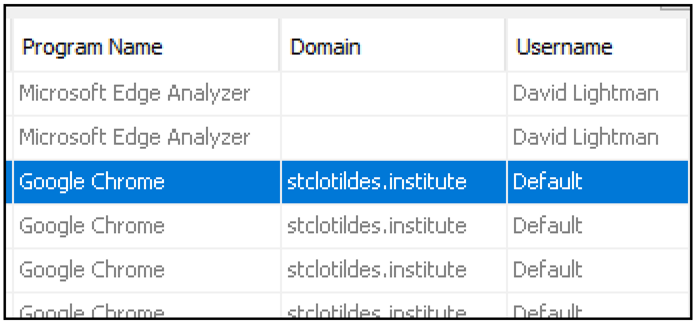
Expected Response Illustration:

Autopsy view of Chrome browser history record - part 1



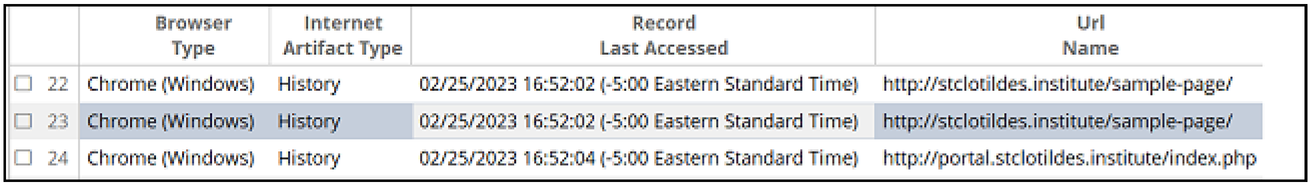
Date Accessed	URL	Title
2023-02-24 07:43:15 GMT	file:///C:/Windows/system32/oobe/FirstLogonAnim.html	
2023-02-24 08:21:47 GMT	javascript:try{external.ExecuteSelectionMenuItem('Stop')}…	
2023-02-25 21:52:02 GMT	http://stclotildes.institute/sample-page/	stclotildes.institute
2023-02-25 21:52:02 GMT	http://stclotildes.institute/sample-page/	stclotildes.institute
2023-02-25 21:52:02 GMT	http://stclotildes.institute/sample-page/	stclotildes.institute
2023-02-25 21:52:02 GMT	http://stclotildes.institute/sample-page/	stclotildes.institute

Autopsy view of Chrome browser history record - part 2



Program Name	Domain	Username
Microsoft Edge Analyzer		David Lightman
Microsoft Edge Analyzer		David Lightman
Google Chrome	stclotildes.institute	Default
Google Chrome	stclotildes.institute	Default
Google Chrome	stclotildes.institute	Default
Google Chrome	stclotildes.institute	Default

Encase view of Chrome browser history record



	Browser Type	Internet Artifact Type	Record Last Accessed	Url Name
☐ 22	Chrome (Windows)	History	02/25/2023 16:52:02 (-5:00 Eastern Standard Time)	http://stclotildes.institute/sample-page/
☐ 23	Chrome (Windows)	History	02/25/2023 16:52:02 (-5:00 Eastern Standard Time)	http://stclotildes.institute/sample-page/
☐ 24	Chrome (Windows)	History	02/25/2023 16:52:04 (-5:00 Eastern Standard Time)	http://portal.stclotildes.institute/index.php

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 14 - Examination Questions

Question 14: What is the path and filename of the file containing the term “Xenoglaux”? (e.g., /directory/subdirectory/name.extension)

Manufacturer's Expected Response: C:\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf

WebCode Test	Response
2A9WQN-5561	file path: Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf filename: eccentricgoomyprawn.pdf
2P2VAR-5561	23-5561.LE01 - Partition 2 (Microsoft NTFS, 29.95 GB)\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
2PJFNF-5562	eccentricgoomyprawn.pdf untitled\D\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
2VQ8RL-5562	Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf
2ZFN6X-5561	/Users/David/Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf
3CDK6E-5562	\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgroomyprawn.pdf
3DPEPK-5561	C:\Users\David Lightman\Documents\UnsightlyAdorableToad\ eccentricgoomyprawn.pdf
3M9X4P-5561	\Users\David Lightman\Documents\Unsightly Adorable Toad\eccentricgoomyprawn.pdf
42BM2N-5561	\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
48GFVJ-5561	/Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf
4U7ZP2-5562	/img_23-5561.E01/vol_vol3/Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf
649HZ6-5561	Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
68RW46-5562	Partition 2 (Microsoft NTFS, 29.95 GB)\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
6DZZCR-5561	/[root]/users/David Lightman/Documents/Unsightly Adorable Toad/eccentricgoomyprawn.pdf
6MKCN6-5562	\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
6Q2RXW-5562	Path: Partition2/NONAME[NTFS]/[root]/Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf, File Name: eccentricgoomyprawn.pdf
6Q4JPC-5561	23-5561.E01 - Partition 2 (Microsoft NTFS, 29.95 GB)\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
6QKH3A-5562	Path - My Computer (Computer)\d3162b92-9365-467a-956b-92703aca08af\UnsightlyAdorableToad\eccentricgoomyprawn.pdf File name - eccentricgoomyprawn.pdf
6TR3NP-5561	Partition 2 (Microsoft NTFS, 29.95 GB)\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
72ZUTD-5561	Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 14 - Examination Questions

WebCode Test	Response
78PAK7-5562	C:\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
7JUP4F-5561	users/david lightman/documents/unsightlyadorabletoad/eccentricgoomyprawn.pdf
7PQ8PM-5562	\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
7XZLMH-5562	\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
82VWX9-5562	Filename: eccentricgoomyprawn.pdf Filepath: Partition 2 (Microsoft NTFS, 29.95 GB)\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
83AEYT-5562	C:\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
8CB97J-5561	\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
8LJ9TK-5561	Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf
96TUNQ-5561	23-5561.E01/Partition 2/NONAME [NTFS]/[root]/Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf
98ZV8C-5561	C:\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
99QBZK-5562	\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgroomyprawn.pdf
9AJ8JM-5561	23-5561.E01/Partition 2/NONAME [NTFS]/[root]/Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf
9J9Q8U-5562	\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
A8QHYB-5562	23-5561.E01 - Partition 2 (Microsoft NTFS, 29.95 GB)\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
A8VQBZ-5561	\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
ABK3AJ-5561	NOT IN SCOPE
ACTERK-5561	Not in Scope
ADYU2Y-5562	\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
AKG6BT-5562	root\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
AM94QQ-5561	/Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf
BFKZWF-5562	Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
BQRG78-5561	/Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 14 - Examination Questions

WebCode Test	Response
C4LMC9-5562	/Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf
C897D8-5561	/Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf
CF2CBE-5562	Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
CKAXYB-5561	/[root]/Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf
CP6N6M-5561	\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
D7PUVD-5561	Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
DB6AM4-5561	C:/Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf
DGVH9K-5561	Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
DXVP3C-5562	C:\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
E2RHRZ-5562	Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
E4ZNBG-5561	\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
EV7HHF-5561	/Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf
F3JVRX-5561	C:/Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf
FZVEJB-5561	\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
G973T4-5561	FileName: eccentricgoomyprawn.pdf Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
GJ39KG-5561	.\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
GYTEQP-5561	\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
HQVXJW-5561	C:\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
HUFQTD-5561	C:\Users\David Lightman\Documents\Unsightly Adorable Toad\eccentricgoomyprawn.pdf
HW2LD2-5562	[Participant did not return results for this question.]
J84AQF-5562	\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb\eccentricgoomyprawn.pdf.wedb
JE9W33-5561	C\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 14 - Examination Questions

WebCode Test	Response
JGBUAC-5562	Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
JJDU63-5561	/Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf
JL32PY-5562	/Users/David Lightman/Documents/UnsightlyAdorableToad\eccentricgoomyprawn.pdf
JLRZA6-5561	Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
JPKFX7-5561	C:/Users/DavidLightman/Documents/UnsightlyAdorabe/eccentricgoomyprawn.pdf
KR28JR-5562	C:\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
KR4V3R-5561	Partition 2 [C:]\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
KXRBW6-5562	Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
KZVDDT-5561	\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
LDKC3B-5561	Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf
M9HYHY-5561	/Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf File name : eccentricgoomyprawn.pdf
MF4Q7B-5561	23-5561.E01 - Partition 2 (Microsoft NTFS, 29.95 GB)\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
MF8B24-5561	\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
NADTWE-5561	\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
NE7TEF-5562	\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
NTANM4-5561	Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
NTZJR4-5561	root\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
P3ACZC-5561	/Users/David Lightman/Documents/UnsightlyAdorabletoad/eccentricgoomyprawn.pdf
P79FU7-5561	/Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf
P8ZNUA-5561	\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
PFEMA7-5562	/Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf
PFVN93-5561	C:/Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 14 - Examination Questions

WebCode Test	Response
PLGGK2-5561	\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
PPMYM4-5562	Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
PTKDEZ-5562	Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
PUTRGY-5561	Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
PWJXV6-5561	/documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf
Q2CFQV-5561	C:\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
Q33NQX-5561	\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
Q3RHY2-5561	\Users\Davis Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
QMR3Q2-5561	/[root]/Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf
QRJAR3-5561	/Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf
QTHAXU-5561	/Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf
RAK67E-5562	Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf
RBBDCA-5562	\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf.webd (AND .pdf) present in both files but .webd ONLY contains the term)
RGH4EF-5562	C\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
RRMUMV-5561	\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
RRXTDK-5562	/Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf
RV3JKZ-5561	FileName: eccentricgoomyprawn.pdf Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
TC4JAF-5562	C:\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
TCGEBD-5561	C:\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
TEPC2R-5562	eccentricgoomyprawn.pdf /Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf
TKFNZV-5561	eccentricgoomyprawn.pdf /Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf
TNEXBT-5561	23-5561.E01/Partition 2/NONAME [NTFS]/[root]/Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 14 - Examination Questions

WebCode Test	Response
TVF9MD-5562	Users\David Lightman\Documensts\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
TX22EP-5561	Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf
U3RQC6-5561	C:\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf, eccentricgoomyprawn.pdf
UKBK6E-5561	C:\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
URA8XZ-5561	Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
UVZCUQ-5562	\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
V4KY4K-5562	\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
VCE6WL-5561	Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
VJH9N7-5561	/Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf
VTZR3B-5561	Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
VVVB8V-5561	\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
WC9E49-5561	D:/Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf
WD8DHB-5561	C: \Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
WK4CUH-5561	C:\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
WNN64Y-5561	C:\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
WX2YKZ-5561	Not currently within scope of the lab.
WZGLVL-5562	Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
XA2A8Z-5562	Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
XEVDXV-5561	Not in scope
XJ99G2-5562	Path: \Users\David Lightman\Documents\UnsightlyAdorableToad\ & File name: eccentricgoomyprawn.pdf
XQ9B22-5561	23-5561.e01/Partition 2/NONAME [NTFS]/[root]/Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf
XVDHZK-5562	[Participant did not return results for this question.]

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 14 - Examination Questions

WebCode Test	Response
XWDAB7-5561	/Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf
XX78KX-5561	/Users/David Lightman/Documents/UnsightlyAdorableToad/eccentricgoomyprawn.pdf
Y63G92-5562	Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
YDJQ3P-5561	C:\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
YPNENR-5562	Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf
ZPR26J-5561	\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 14 - Examination Questions

Question 14: What is the path and filename of the file containing the term “Xenoglaux”? (e.g., /directory/subdirectory/name.extension)

Consensus Result:

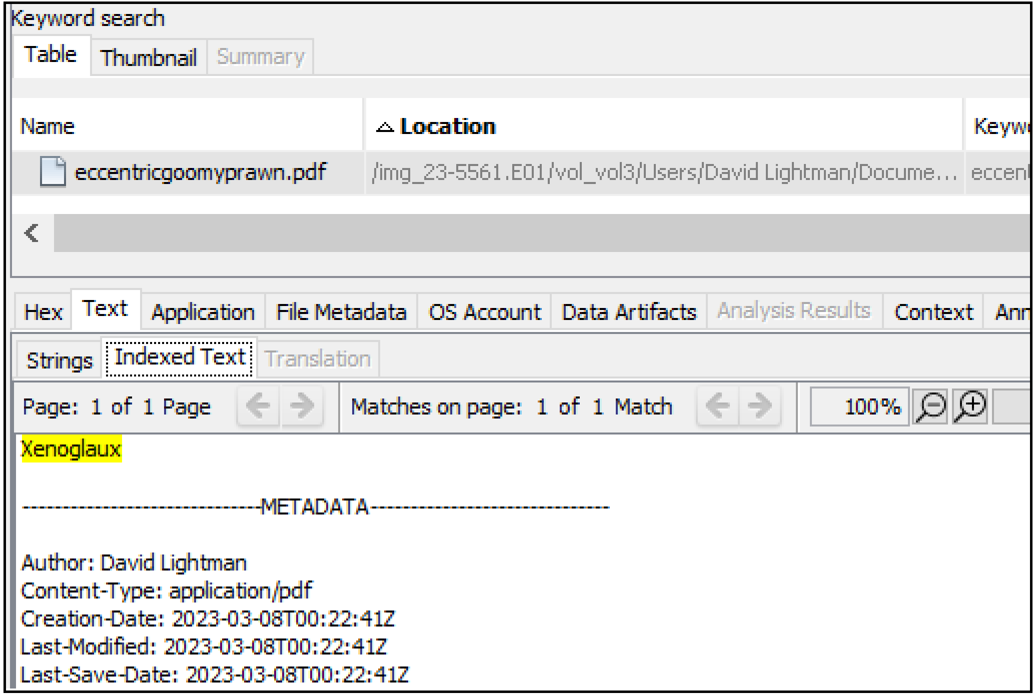
C:\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf and slight variations representing the same information.

Expected Response Explanation:

A simple keyword search with any tool capable of searching within compound files will locate this term.

Expected Response Illustration:

Autopsy view of keyword search results



Name	Location	Keyw
eccentricgoomyprawn.pdf	/img_23-5561.E01/vol_vol3/Users/David Lightman/Docume…	eccen

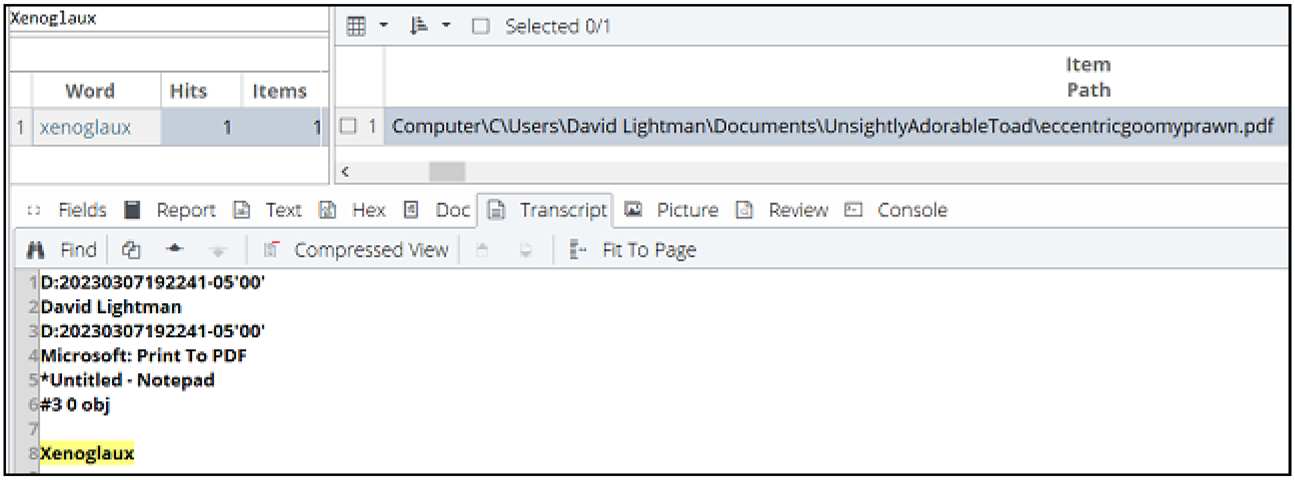
Page: 1 of 1 Page
Matches on page: 1 of 1 Match

Xenoglaux

-----------------------------METADATA------------------------------

Author: David Lightman
Content-Type: application/pdf
Creation-Date: 2023-03-08T00:22:41Z
Last-Modified: 2023-03-08T00:22:41Z
Last-Save-Date: 2023-03-08T00:22:41Z

EnCase view of keyword search results.



	Word	Hits	Items
1	xenoglaux	1	1

		Item Path
☐	1	Computer\C\Users\David Lightman\Documents\UnsightlyAdorableToad\eccentricgoomyprawn.pdf

```
D:20230307192241-05'00'
David Lightman
D:20230307192241-05'00'
Microsoft: Print To PDF
*Untitled - Notepad
#3 0 obj

Xenoglaux
```

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15 - Examination Questions

Question 15: Describe the difference between the URLs in the images attached to the email message sent by David Lightman March 5, 2023 3:34 PM

Manufacturer's Expected Response: A period (dot) is present between the text "st" and "clotildes" in one of the URLs.

WebCode Test	Response
2A9WQN-5561	One URL is portal.stclotildes.institute, the other is portal.st.clotildes.institute (added a "." in the URL name)
2P2VAR-5561	The difference is that there is a "." after "http://portal.st" in the second URL.
2PJFNF-5562	http://portal.stclotildes.institute -> http://portal.st.clotildes.institute
2VQ8RL-5562	portal.stclotildes.institute and portal.st.clotildes.institute (stclotildes and st.clotildes)
2ZFN6X-5561	In the bottom hyperlink there is a . after “st” in "portal.st.clotildes". This is different than the hyperlink at the top.
3CDK6E-5562	http://portal.st.clotildes.institute and htttp://portal.stclotildes.institue
3DPEPK-5561	Period after the “st” in “stclotildes” is present in one image but not the other.
3M9X4P-5561	porta.stclotildes vs portal.st.clotildes
42BM2N-5561	portal.stclotildes portal.st.clotildes
48GFVJ-5561	One URL contains “stclotildes” and the other contains “st.clotildes”
4U7ZP2-5562	The image 9921895D756D45E18301784D807AB7C6.png is wider and has "Subject RosarioSIS - Password Reset" written at the top. The image C23157603457462C882AE2F8C07767CE.png is narrower and does not have "RosarioSIS Issue - Password Reset" written at the top.
649HZ6-5561	portal.stclotildes vs portal.st.clotildes
68RW46-5562	The URL in 9921895D756D45E18301784D807AB7C6.png is http://portal.stclotildes.institute..... The URL in C23157603457462C882AE2F8C07767CE.png is http://portal.st.clotildes.institute.... which leads to a different site.
6DZZCR-5561	They are identical except for one has a "." between "st" and "clotildes". So it is stclotildes in one url and st.clotildes in the other
6MKCN6-5562	The URL in the attached image is a hyperlink that moves to the site when clicked.
6Q2RXW-5562	st.clotildes.institute refers to a different web domain than stclotildes.institute
6Q4JPC-5561	There is a period between st and clotildes in one and not the other.
6QKH3A-5562	Time different. May be due to time zone difference - One URL shows ‘portal.st.clotildes’, other shows ‘portal.stclotildes’
6TR3NP-5561	First attachment is “portal.stclotildes.institute”. Second attachment is “portal.st.clotildes.institute”.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15 - Examination Questions

WebCode Test	Response
72ZUTD-5561	One of the URL's start with 'http://portal.stclotildes…' and the other one starts with 'http://portal.st.clotildes…'
78PAK7-5562	The difference is an extra dot in one of the URLs between "st" and "clotides". (One begins with "http://portal.stclotides.institute", the other begins with "http://portal.st.clotides.institute").
7JUP4F-5561	website name stclotildes vs st.clotildes
7PQ8PM-5562	One of the URLs contain: st.clotildes and the other contains: stclotildes.
7XZLMH-5562	In the image named 'C23157603457462C882AE2F8C07767CE.png', there is a dot between 'st' and 'clotildes', while in the image named '9921895D756D45E18301784D807AB7C6.png', there is not.
82VWX9-5562	The URL links are different within the 2 images. One contains '…portal.stclotildes.institute…' while the other is '…portal.st.clotildes.institute…'
83AEYT-5562	The difference between the two URLs is an extra point (.). the second URL contains an extra character which is the point "." appearing on the word "st.clotildes". However, this point "." doesn't exist on the first URL.
8CB97J-5561	Changes in the domain between portal.stclotildes and portal.st.clotildes
8LJ9TK-5561	Difference: there is "stclotildes" in one URL, and the other is "st.slotildes".
96TUNQ-5561	Different website address http://portal.stclotildes.institute and http://portal.st.clotildes.institute
98ZV8C-5561	One of the emails is st.clotildes and the other is stclotildes
99QBZK-5562	http://portal.stclotildes.institute/ --vs-- http://portal.st.clotildes.institute/
9AJ8JM-5561	One password reset link URL begins "http://portal.stclotildes.institute…." the other URL begins with "http://portal.st.clotildes.institute…."
9J9Q8U-5562	There is a period after "st" on one but not the other attachment.
A8QHYB-5562	One has a period (.) in between st and clotildes. One used the domain portal.stclotidles.institute, the other used portal.st.clotildes.institute
A8VQBZ-5561	The second URL has an extra period
ABK3AJ-5561	NOT IN SCOPE
ACTERK-5561	Not in Scope
ADYU2Y-5562	Both URL's are identical with the exception of the first segment (domain) where the URL in the attachment named C23157603457462C882AE2F8C07767CE.png is: • http://portal.st.clotildes.institute/ And the image named 9921895D756D45E18301784D807AB7C6.png contains the following URL • http://portal.stclotildes.institute/ http://portal.stclotildes.institute/ is the legitimate website, whereas http://portal.st.clotildes.institute/ is the false website.
AKG6BT-5562	One of them begins http://portal.st.clotildes, the other http://portal.stclotildes – The second one is missing a "dot" between "st" and "clotildes"
AM94QQ-5561	In one of the URLs there is an extra period between the word st and clotildes.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15 - Examination Questions

WebCode Test	Response
BFKZWF-5562	the first url has the word (stclotildes) while the second url has the word is (st.clotildes) with extra dot in the URL
BQRG78-5561	The URL in the upper image begins with "http://portal.stclotildes.institute/", whereas the URL in the lower image has a period between "st" and "clotildes" ("http://portal.st.clotildes.institute/").
C4LMC9-5562	in one of them, a dit was added between "st" and "clotildes". you have "portal.stclotildes.institute" in one and "portal.st.clotildes.institute" in the other
C897D8-5561	The difference is after word "portal" one URLs followed by ".st.clotildes", another URLs followed by ".stclotildes"
CF2CBE-5562	http://portal.stclotildes.institute/PasswordReset.php , http://portal.st.clotildes.institute/PasswordReset.php (Extra Dot)
CKAXYB-5561	In the first URL there is no .(period) between st and clotildes (stclotildes). There is a . (period) in the second URL between st and clotildes (st.clotildes)
CP6N6M-5561	Changes in the domain between portal.stclotildes and portal.st.clotildes
D7PUVD-5561	The URL's differ in that at the start of the address one has an extra full stop in it after .st as shown in the brackets; http://portal.st(.)clotildes.institute
DB6AM4-5561	The URL in 9921895D756D45E18301784D807AB7C6.png points to the domain http://portal.stclotildes.institute/... The URL in C23157603457462C882AE2F8C07767CE.png points to the domain http://portal.st.clotildes/...
DGVH9K-5561	one is portal.st.clotildes.institute and the other is portal.stclotildes.institue (The difference is the period after "ST")
DXVP3C-5562	There is an extra "." in the link he later admits he owns. portal.stclotildes.institute... vs. portal.st.clotildes.institute...
E2RHRZ-5562	Portal.st.clotildes <- one URL includes the "." While the other one does not.
E4ZNBG-5561	The URLs are slightly different, one has a "." between the st of stclotides. "…http://portal.st.clotildes…" while the other is "…http://portal.stclotildes…"
EV7HHF-5561	There is a "." (dot) between "stclotildes" in one of them and not in the other.
F3JVRX-5561	Existence of a period(.) between 'st' and 'clotildes' (http://portal.stclotildes.institute, http://portal.st.clotildes.institute)
FZVEJB-5561	The URLs contained within the two images are near identical, however the URL contained within 9921895D756D45E18301784D807AB7C6.png does not bear a full stop (period) at "…stclotildes…", whereas the URL contained within C23157603457462C882AE2F8C07767CE.png bears a full stop at "…st.clotildes…"
G973T4-5561	Different File Extensions
GJ39KG-5561	"stclotildes" vs "st.clotildes"
GYTEQP-5561	The period in between st and clotildes.
HQVXJW-5561	st.clotildes and stclotildes
HUFQTD-5561	The period (.) after the st in the second link
HW2LD2-5562	[Participant did not return results for this question.]

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15 - Examination Questions

WebCode Test	Response
J84AQF-5562	A dot between st and clotildes Portal.stclotildes / Portal.st.clotildes
JE9W33-5561	“stclotildes” vs. “st.clotildes”
JGBUAC-5562	"http://portal.stclotildes.institute" "http://portal.st.clotildes.institute" One of the urls doesn't have a "." in the url.
JJDU63-5561	The second URL has a period between st and clotildes whereas the first URL does not (portal.stclotildes.institute compared to portal.st.clotildes.institute).
JL32PY-5562	The difference between two URL is that one is fake web site while the other is legitimate web site. A fake web site is 'http://portal.stclotildes.institute/~~~'. and The site imitated that of 'St.Clotildes.institute', so that site looks like the grading portal. Legitimate web site is 'http://portal.st.clotildes.institute/~~~'.
JLRZA6-5561	One begins with http://portal.st.clotildes and the other begins with http://portal.stclotildes
JPKFX7-5561	In the first one is "portal.stclotildes" and in the second one "portal.st.clotildes"
KR28JR-5562	Additional "." character within stclotildes in the two URL's. “portal.stclotildes.institute” vs “portal.st.clotildes.institute”
KR4V3R-5561	"stclotildes" vs. "st.clotildes" = the added "."
KXRBW6-5562	The URL’s differ in that at the start of the address one has an extra full stop in it after .st as shown in the brackets; http://portal.st(.)clotildes.institute
KZVDDT-5561	In 'C23157603457462C882AE2F8C07767CE.png' image, there is a dot following 'portal.st' as 'http://portal.st.clotildes', but in '9921895D756D45E18301784D807AB7C6.png' image, there is no dot between 'portal.st' and 'clotildes' as 'http://portal.stclotildes'.
LDKC3B-5561	one link has a period between st and clotildes and the other does not. stclotildes vs st.clotildes
M9HYHY-5561	The different is in the first URL there is no (.) after the st (portal.stclotildes) , while the other URL there is (.)after the st (portal.st.clotildes).
MF4Q7B-5561	To Reset the Password
MF8B24-5561	The period after st. is not there in one but is there in the other
NADTWE-5561	In one part of the URL is “portal stclotildes.institute” and the other is ‘portal.st.clotildes.institute” (the is a period between the ‘st’ and ‘clotildes’).
NE7TEF-5562	A similar spelling (st.clotildes) was used in the middle of the hyperlinked URL to induce access to other sites.
NTANM4-5561	One URL displays http://portal.stclotildes.institute/ and the other URL displays http://portal.st.clotildes.institute/
NTZJR4-5561	One has portal.stclotildes and the other has portal.st.clotildes
P3ACZC-5561	http://portal.stclotildes.institute/PasswordReset.php versus http://portal.st.clotildes.institute/PasswordReset.php
P79FU7-5561	stclotildes -> st.clotildes
P8ZNUA-5561	Lightman’s spoofed site is “st.clotildes” (with dot) and the real school site is “stclotildes” (w/o dot)

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15 - Examination Questions

WebCode Test	Response
PFEMA7-5562	One URL has a "." between st and clotildes and the other does not.
PFVN93-5561	There is a dot between st.clotildes in one URL, and is absent in the other (stclotildes)
PLGGK2-5561	There is a period (.) in "st.clotildes" in one URL and it is missing in the other URL (stclotildes).
PPMYM4-5562	Extra Dot
PTKDEZ-5562	The second URL in the image has an additional dot (.) between "st" and "clotildes".
PUTRGY-5561	the extra Dot in the URLs is the different , one is (stclotildes) second is (st.clotildes)
PWJXV6-5561	One has a . after st. (st.clotildes vs stclotildes)
Q2CFQV-5561	stclotildes and st.clotildes
Q33NQX-5561	The domain names in the two links are different, one is portal.stclotildes.institute and the other is portal.st.clotildes.institute with an extra dot in the domain name.
Q3RHY2-5561	one has a link that begins with portal.stclotildes.institute and the other is portal.st.clotildes.institute
QMR3Q2-5561	They're identical
QRJAR3-5561	One has "stclotildes", and the other has "st.clotildes"
QTHAXU-5561	Difference is among the first characters of the URLs: http://portal.stclotildes.institute/ and http://portal.st.clotildes.institute/. Specifically: st.clotides and stclotildes.
RAK67E-5562	One uses st.clotildes the other uses stclotildes
RBBDCA-5562	"=" is relaced with "-"
RGH4EF-5562	the first is: portal.stclotildes the second is: portal.st.clotildes – shows the URL with an additional period (full-stop) separating the st.
RRMUMV-5561	One URL contains "stclotildes" and the other URL contains "st.clotildes"
RRXTDK-5562	There is a DOT separating the word stclotildes. http://portal.stclotildes.institute/....... http://portal.st.clotildes.institute/.....
RV3JKZ-5561	Different File Extensions
TC4JAF-5562	"portal.st.clotildes.institue" "portal.stclotildes.institue". Difference is "." between "st" and "clotildes".
TCGEBD-5561	The URL's are different in that one is portal.st.clotildes.institute and the other is portal.stclotildes.institute
TEPC2R-5562	The different between the URLs is the dot (.) in the first URL there is no dot 'stclotildes', but in the second there is dot "st.clotides"

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15 - Examination Questions

WebCode Test	Response
TKFNZV-5561	The different between the URLs is the dot (.) in the first URL there is no dot ‘stclotildes’, but in the second there is dot “st.clotides”
TNEXBT-5561	One shows an extra period in domain. http://portal.st.clotildes.institute/ and http://portal.stclotildes.institute/
TVF9MD-5562	http://portal.st.clotildes.institute/... http://portal.stclotildes.institute/...
TX22EP-5561	portal.stclotildes.institute, portal.st.clotildes.institute
U3RQC6-5561	One says stclotildes and the other says st.clotildes
UKBK6E-5561	different domain : portal.stclotildes.institute , portal.st.clotildes.institute
URA8XZ-5561	http://portal.stclotildes.institute/PasswordReset.php? http://portal.st.clotildes.institute/PasswordReset.php? (extra dot)
UVZCUQ-5562	Extra full stop in the second URL
V4KY4K-5562	They´re identical.
VCE6WL-5561	one url displays //portal.stclotildes and the other displays //portal.st.clotildes so there is a DOT between st AND clotildes
VJH9N7-5561	One of the URLs starts with “http://portal.stclotildes” the other starts with http:// portal.st.clotildes”. Note that the second example includes a ‘.’ (period or full stop) prior to the text string “clotildes” which is absent in the first example.
VTZR3B-5561	A dot is present between “portal.st(.)clotildes”. There is also a subject present within one “RosarioSIS – Password Reset” and not in the other.
VWB8V-5561	An additional “.” was added to the address. Portal.stclotildes vs portal.st.clotildes
WC9E49-5561	Portal.st.clotildes and portal.stclotildes, one of them is missing a dot.
WD8DHB-5561	The difference is in domains. The one domain is stclotildes.institute and the other is st.clotildes.institute
WK4CUH-5561	One has an added period after the ST making it http://portal.st.clotildes.institute instead of http://portal.stclotildes.intitute which changes the domain it points to.
WNN64Y-5561	There is a period (.) after the st in the second link.
WX2YKZ-5561	Not currently within scope of the lab.
WZGLVL-5562	path: .stclotildes. and .st.clotildes.
XA2A8Z-5562	Additional dot in the second URL between ST and Clotildes
XEVDXV-5561	Not in scope
XJ99G2-5562	One URL contains : 'stclotildes' and the other link has it recorded as st.clotildes.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15 - Examination Questions

WebCode Test	Response
XQ9B22-5561	portal.stclotildes.institute vs portal.st.clotildes.institute There is an extra dot in the second word for one of the URLs.
XVDHZK-5562	[Participant did not return results for this question.]
XWDAB7-5561	The url in the first image is 'stclotildes.institute' owned by the school. The url in the second image is 'st.clotildes.institute' owned by David Lightman.
XX78KX-5561	The dot (.) is present in between st and clotildes in one graphic and is not present in the other.
Y63G92-5562	difference there is a dot between st and clotides in the second png, so one image shows stclotides and the second shows st.clotides
YDJQ3P-5561	There is an extra "." in the link he later admits he owns. portal.stclotildes.institute... vs. portal.st.clotildes.institute...
YPNENR-5562	http://portal.stclotildes.institute/PasswordReset.php? http://portal.st.clotildes.institute/PasswordReset.php? extra dot
ZPR26J-5561	Two URLs at the first look seem to look identical. However they are not, first URL doesn’t have a "." in the "stcolidites" word http://portal.stclotildes.institute and the second one has a "." in the "stcolidites" word http://portal.st.clotildes.institute.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15 - Examination Questions

Question 15: Describe the difference between the URLs in the images attached to the email message sent by David Lightman March 5, 2023 3:34 PM

Consensus Result:

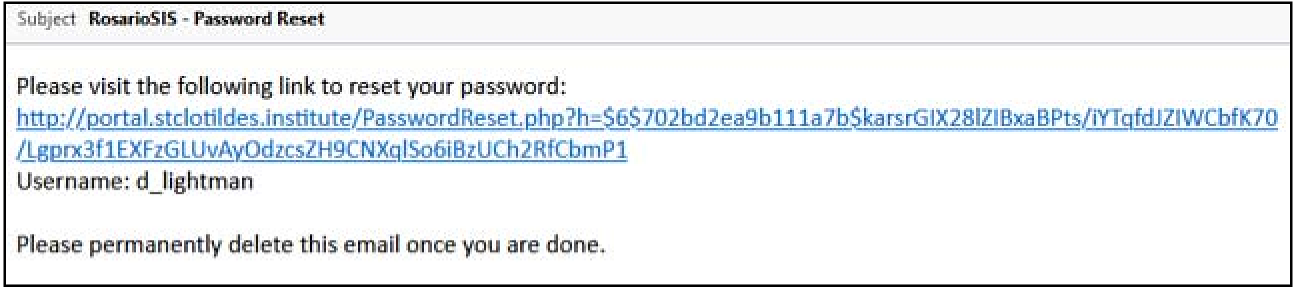
"A period (dot) is present between the text "st" and "clotildes" in one of the URLs" and variations describing the same information.

Expected Response Explanation:

The URLs look very similar, but each will take the user to a completely different website, potentially controlled by different people. This is common in phishing attacks where the use of a 'masquerade' domain is effective in fooling users into providing their login details to 3rd parties.

Expected Response Illustration:

Attached image 1 (9921895D756D45E18301784D807AB7C6.png)

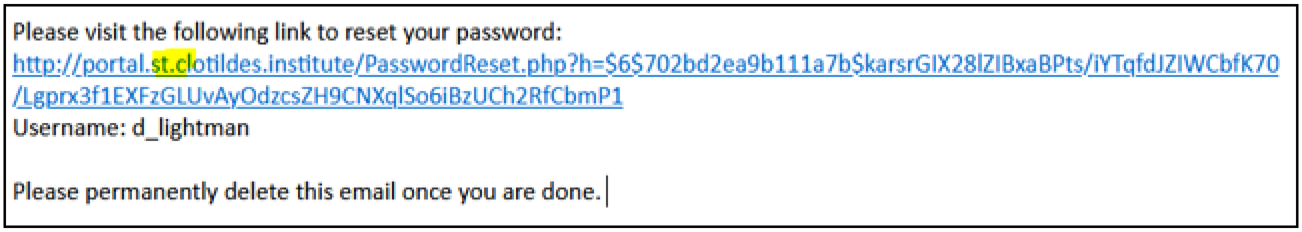


Subject RosarioSIS - Password Reset

Please visit the following link to reset your password:
http://portal.stclotildes.institute/PasswordReset.php?h=$6$702bd2ea9b111a7b$karsrGIX28lZIBxaBPts/iYTqfdJZIWCbfK70/Lgprx3f1EXFzGLUvAyOdzcsZH9CNXqlSo6iBzUCh2RfCbmP1
Username: d_lightman

Please permanently delete this email once you are done.

Attached image 2 (C23157603457462C882AE2F8C07767CE.png)



Please visit the following link to reset your password:
http://portal.st.clotildes.institute/PasswordReset.php?h=$6$702bd2ea9b111a7b$karsrGIX28lZIBxaBPts/iYTqfdJZIWCbfK70/Lgprx3f1EXFzGLUvAyOdzcsZH9CNXqlSo6iBzUCh2RfCbmP1
Username: d_lightman

Please permanently delete this email once you are done.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16 - Examination Questions

Question 16: Who is listed as the author of crafty.doc?

Manufacturer's Expected Response: David Lightman

WebCode Test	Response
2A9WQN-5561	David Lightman
2P2VAR-5561	David Lightman
2PJFNF-5562	David Lightman
2VQ8RL-5562	David Lightman
2ZFN6X-5561	David Lightman
3CDK6E-5562	David Lightman
3DPEPK-5561	David Lightman
3M9X4P-5561	David Lightman
42BM2N-5561	David Lightman
48GFVJ-5561	David Lightman
4U7ZP2-5562	David Lightman
649HZ6-5561	David Lightman
68RW46-5562	David Lightman
6DZZCR-5561	David Lightman
6MKCN6-5562	David Lightman
6Q2RXW-5562	David Lightman
6Q4JPC-5561	David Lightman
6QKH3A-5562	David Lightman
6TR3NP-5561	David Lightman
72ZUTD-5561	David Lightman
78PAK7-5562	David Lightman

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16 - Examination Questions

WebCode Test	Response
7JUP4F-5561	david lightman
7PQ8PM-5562	David Lightman
7XZLMH-5562	David Lightman
82VWX9-5562	David Lightman
83AEYT-5562	David Lightman
8CB97J-5561	David Lightman
8LJ9TK-5561	David Lightman
96TUNQ-5561	David Lightman
98ZV8C-5561	David Lightman
99QBZK-5562	David Lightman
9AJ8JM-5561	David Lightman
9J9Q8U-5562	David Lightman
A8QHYB-5562	David Lightman
A8VQBZ-5561	David Lightman
ABK3AJ-5561	NOT IN SCOPE
ACTERK-5561	Not in Scope
ADYU2Y-5562	David Lightman
AKG6BT-5562	David Lightman
AM94QQ-5561	David Lightman
BFKZWF-5562	David Lightman
BQRG78-5561	David Lightman
C4LMC9-5562	David Lightman

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16 - Examination Questions

WebCode Test	Response
C897D8-5561	David Lightman
CF2CBE-5562	David Lightman
CKAXYB-5561	David Lightman
CP6N6M-5561	David Lightman
D7PUVD-5561	David Lightman
DB6AM4-5561	David Lightman
DGVH9K-5561	David Lightman
DXVP3C-5562	David Lightman
E2RHRZ-5562	David Lightman
E4ZNBG-5561	David Lightman
EV7HHF-5561	David Lightman
F3JVRX-5561	David Lightman
FZVEJB-5561	David Lightman
G973T4-5561	David Lightman
GJ39KG-5561	David Lightman
GYTEQP-5561	David Lightman
HQVXJW-5561	David Lightman
HUFQTD-5561	David Lightman
HW2LD2-5562	[Participant did not return results for this question.]
J84AQF-5562	David Lightman
JE9W33-5561	David Lightman
JGBUAC-5562	David Lightman

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16 - Examination Questions

WebCode Test	Response
JJDU63-5561	David Lightman
JL32PY-5562	David Lightman
JLRZA6-5561	David Lightman
JPKFX7-5561	David Lightman
KR28JR-5562	David Lightman
KR4V3R-5561	David Lightman
KXRBW6-5562	David Lightman
KZVDDT-5561	David Lightman
LDKC3B-5561	David Lightman
M9HYHY-5561	David Lightman
MF4Q7B-5561	David Lightman
MF8B24-5561	David Lightman
NADTWE-5561	David Lightman
NE7TEF-5562	David Lightman
NTANM4-5561	David Lightman
NTZJR4-5561	David Lightman
P3ACZC-5561	David Lightman
P79FU7-5561	David Lightman
P8ZNUA-5561	David Lightman
PFEMA7-5562	David Lightman
PFVN93-5561	David Lightman
PLGGK2-5561	David Lightman

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16 - Examination Questions

WebCode Test	Response
PPMYM4-5562	David Lightman
PTKDEZ-5562	David Lightman
PUTRGY-5561	David Lightman
PWJXV6-5561	David Lightman
Q2CFQV-5561	David Lightman
Q33NQX-5561	David Lightman
Q3RHY2-5561	David Lightman
QMR3Q2-5561	David Lightman
QRJAR3-5561	David Lightman
QTHAXU-5561	David Lightman
RAK67E-5562	David Lightman
RBBDCA-5562	David Lightman
RGH4EF-5562	David Lightman
RRMUMV-5561	David Lightman
RRXTDK-5562	David Lightman
RV3JKZ-5561	David Lightman
TC4JAF-5562	David Lightman
TCGEBD-5561	David Lightman
TEPC2R-5562	David Lightman
TKFNZV-5561	David Lightman
TNEXBT-5561	David Lightman
TVF9MD-5562	David Lightman

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16 - Examination Questions

WebCode Test	Response
TX22EP-5561	David Lightman
U3RQC6-5561	David Lightman
UKBK6E-5561	David Lightman
URA8XZ-5561	David Lightman
UVZCUQ-5562	David Lightman
V4KY4K-5562	David Lightman
VCE6WL-5561	David Lightman
VJH9N7-5561	"David Lightman"
VTZR3B-5561	David Lightman
VVVB8V-5561	David Lightman
WC9E49-5561	David Lightman
WD8DHB-5561	David Lightman
WK4CUH-5561	David Lightman
WNN64Y-5561	David Lightman
WX2YKZ-5561	Not currently within scope of the lab.
WZGLVL-5562	David Lightman
XA2A8Z-5562	David Lightman
XEVDXV-5561	Not in scope
XJ99G2-5562	David Lightman
XQ9B22-5561	David Lightman
XVDHZK-5562	[Participant did not return results for this question.]
XWDAB7-5561	David Lightman

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16 - Examination Questions

WebCode Test	Response
XX78KX-5561	David Lightman
Y63G92-5562	David Lightman
YDJQ3P-5561	David Lightman
YPNENR-5562	David Lightman
ZPR26J-5561	David Lightman

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16 - Examination Questions

Question 16: Who is listed as the author of crafty.doc?

Consensus Result:

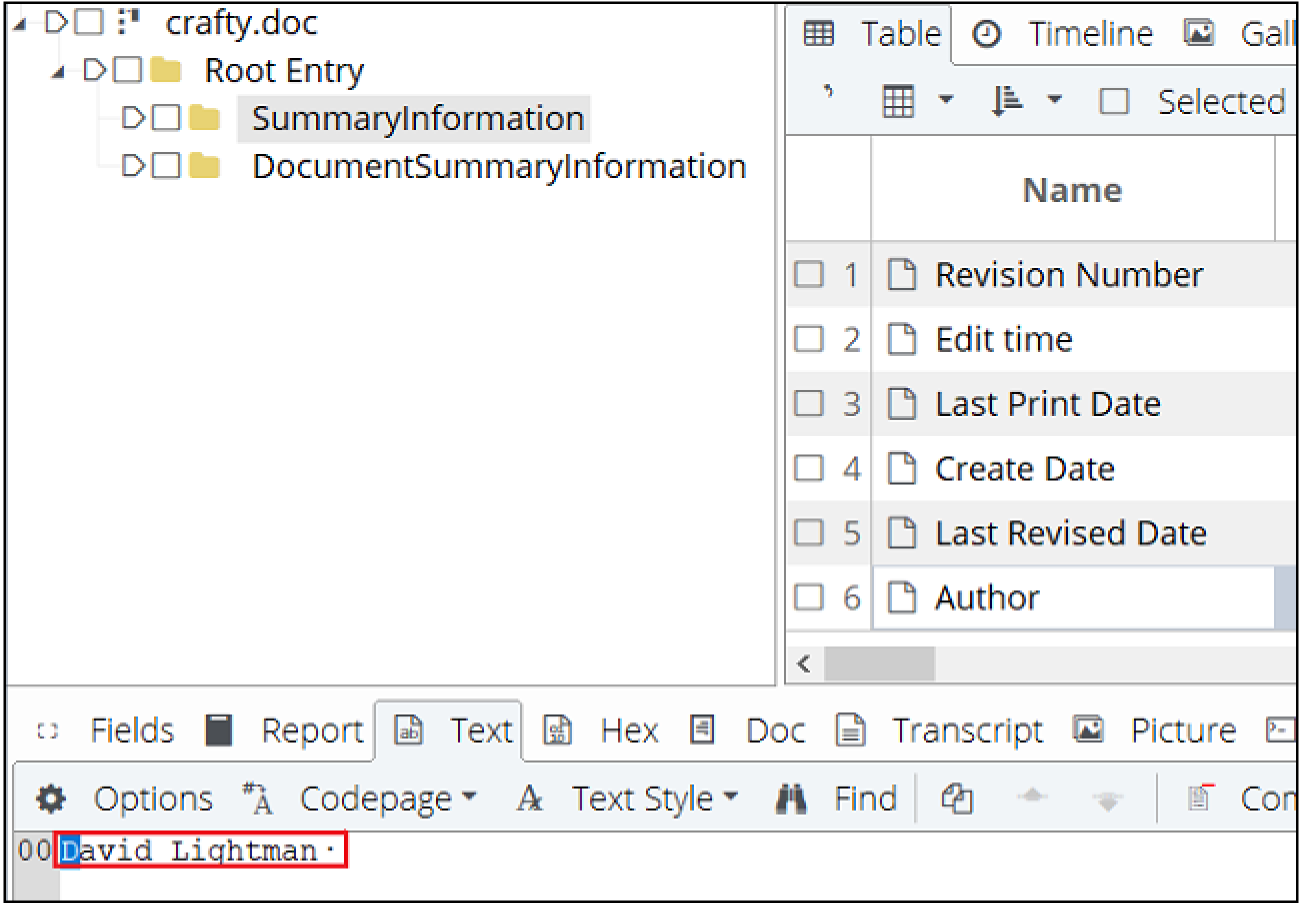
David Lightman

Expected Response Explanation:

Microsoft Word documents contain metadata fields including one identifying the author.

Expected Response Illustration:

EnCase view of crafty.doc metadata



- crafty.doc
  - Root Entry
    - SummaryInformation
    - DocumentSummaryInformation

	Name
1	Revision Number
2	Edit time
3	Last Print Date
4	Create Date
5	Last Revised Date
6	Author

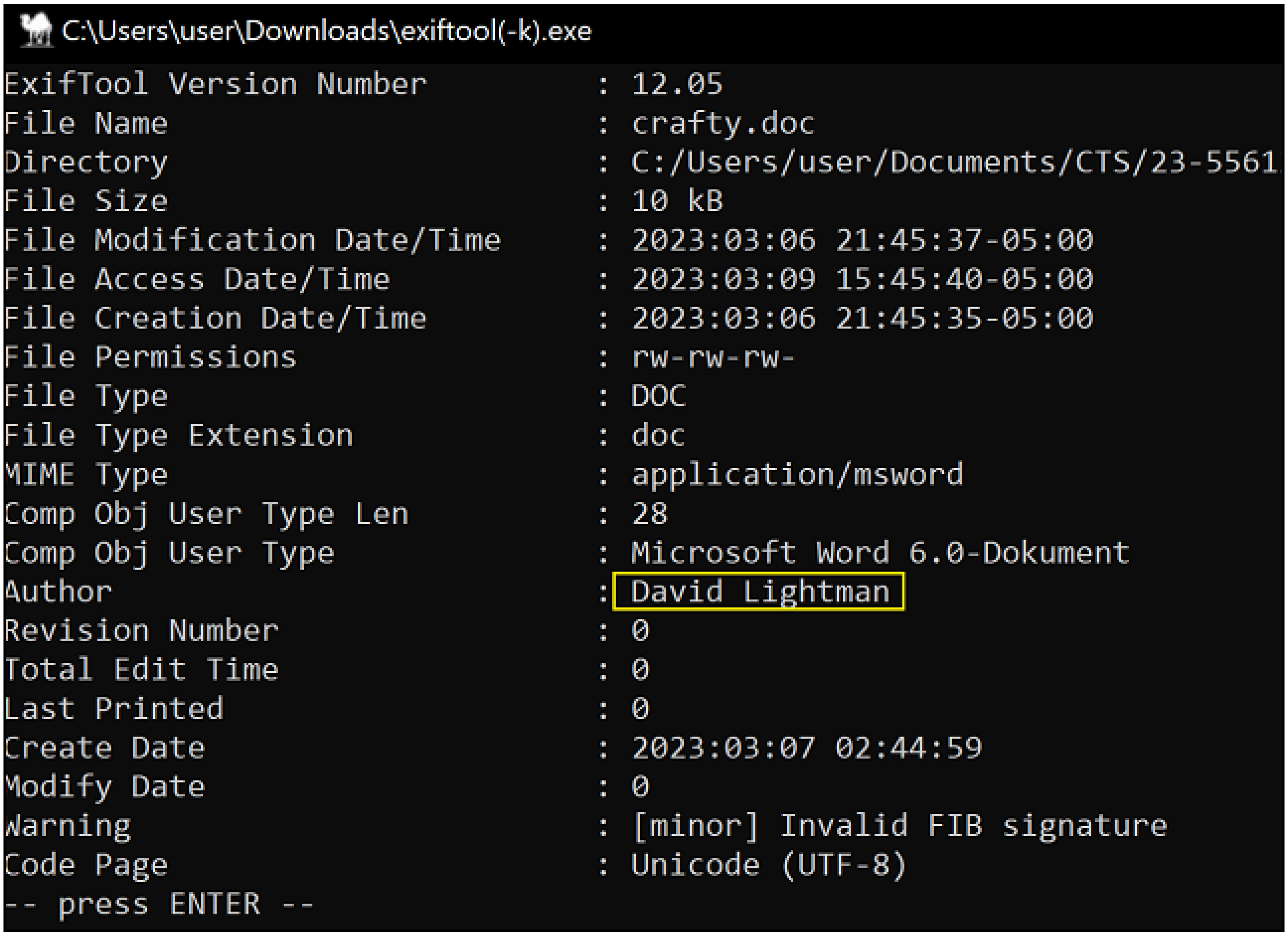
```
00David Lightman·
```

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16 - Examination Questions

ExifTool parse of crafty.doc metadata



C:\Users\user\Downloads\exiftool(-k).exe

```
ExifTool Version Number         : 12.05
File Name                       : crafty.doc
Directory                       : C:/Users/user/Documents/CTS/23-5561
File Size                       : 10 kB
File Modification Date/Time     : 2023:03:06 21:45:37-05:00
File Access Date/Time           : 2023:03:09 15:45:40-05:00
File Creation Date/Time         : 2023:03:06 21:45:35-05:00
File Permissions                : rw-rw-rw-
File Type                       : DOC
File Type Extension             : doc
MIME Type                       : application/msword
Comp Obj User Type Len          : 28
Comp Obj User Type              : Microsoft Word 6.0-Dokument
Author                          : David Lightman
Revision Number                 : 0
Total Edit Time                 : 0
Last Printed                    : 0
Create Date                     : 2023:03:07 02:44:59
Modify Date                     : 0
Warning                         : [minor] Invalid FIB signature
Code Page                       : Unicode (UTF-8)
-- press ENTER --
```

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17 - Examination Questions

Question 17: On what date and time, and to what user account was the LAST successful login to this computer? Provide your response in UTC+0, using the date/time (24-hour) picker which presents the date in the following format: YYYY-MM-DD.

Manufacturer's Expected Response: Date and Time: 2023-03-08 12:44
User Account: David Lightman

WebCode Test	Response
2A9WQN-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
2P2VAR-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
2PJFNF-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman
2VQ8RL-5562	Date and Time: 2023-03-08 12:45, User Account: David-Laptop
2ZFN6X-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
3CDK6E-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman
3DPEPK-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
3M9X4P-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
42BM2N-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
48GFVJ-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
4U7ZP2-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman
649HZ6-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman (S-1-5-21-3501254099-4204809888-2000606956-1007)
68RW46-5562	Date and Time: 2023-03-08 12:45, User Account: David Lightman
6DZZCR-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
6MKCN6-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman
6Q2RXW-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman
6Q4JPC-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
6QKH3A-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman
6TR3NP-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
72ZUTD-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17 - Examination Questions

WebCode Test	Response
78PAK7-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman
7JUP4F-5561	Date and Time: 2023-03-08 00:44, User Account: david lightman
7PQ8PM-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman
7XZLMH-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman
82VWX9-5562	Date and Time: 2023-03-08 12:44, User Account: Date and Time: 2023-03-08 12:44:49 User Account: David Lightman. There is a system account with a successful login with a later date and time, details for this are below: Date and time: 2023-03-08 14:45:12 User account: SYSTEM
83AEYT-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman
8CB97J-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
8LJ9TK-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
96TUNQ-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
98ZV8C-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
99QBZK-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman
9AJ8JM-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
9J9Q8U-5562	Date and Time: 2023-03-08 07:45, User Account: DAVID-LAPTOP$
A8QHYB-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman
A8VQBZ-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
ABK3AJ-5561	NOT IN SCOPE
ACTERK-5561	Not in Scope
ADYU2Y-5562	Date and Time: 2023-03-08 12:45, User Account: David Lightman
AKG6BT-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman
AM94QQ-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
BFKZWF-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17 - Examination Questions

WebCode Test	Response
BQRG78-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
C4LMC9-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman
C897D8-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
CF2CBE-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman
CKAXYB-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
CP6N6M-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
D7PUVD-5561	Date and Time: 2023-03-08 17:44, User Account: David Lightman
DB6AM4-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
DGVH9K-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
DXVP3C-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman
E2RHRZ-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman
E4ZNBG-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
EV7HHF-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
F3JVRX-5561	Date and Time: 2023-03-08 00:45, User Account: David Lightman
FZVEJB-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
G973T4-5561	Date and Time: 2023-06-23 12:44, User Account: David Lightman
GJ39KG-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
GYTEQP-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
HQVXJW-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
HUFQTD-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
HW2LD2-5562	[Participant did not return results for this question.]
J84AQF-5562	Date and Time: 2023-03-08 17:44, User Account: David Lightman

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17 - Examination Questions

WebCode Test	Response
JE9W33-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
JGBUAC-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman S-1-5-21-3501254099-4204809888-2000606959-1007
JJDU63-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
JL32PY-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman
JLRZA6-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
JPKFX7-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
KR28JR-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman
KR4V3R-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
KXRBW6-5562	Date and Time: 2023-03-08 17:44, User Account: David Lightman
KZVDDT-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman (SID: S-1-5-21-3501254099-4204809888-2000606956-1007)
LDKC3B-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
M9HYHY-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
MF4Q7B-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
MF8B24-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
NADTWE-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
NE7TEF-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman
NTANM4-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
NTZJR4-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
P3ACZC-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
P79FU7-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
P8ZNUA-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
PFEMA7-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17 - Examination Questions

WebCode Test	Response
PFVN93-5561	Date and Time: 2023-03-08 02:04, User Account: David Lightman
PLGGK2-5561	Date and Time: 2023-03-08 17:44, User Account: David Lightman
PPMYM4-5562	Date and Time: 2022-03-08 12:44, User Account: David Lightman
PTKDEZ-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman
PUTRGY-5561	Date and Time: 2023-03-08 12:45, User Account: David Lightman
PWJXV6-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
Q2CFQV-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
Q33NQX-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
Q3RHY2-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
QMR3Q2-5561	Date and Time: 2023-03-08 12:43, User Account: David Lightman
QRJAR3-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
QTHAXU-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
RAK67E-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman
RBBDCA-5562	Date and Time: 2023-05-08 12:44, User Account: .\David Lightman
RGH4EF-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman
RRMUMV-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
RRXTDK-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman (ID 4624, logon type 2 - local logon)
RV3JKZ-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
TC4JAF-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman
TCGEBD-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
TEPC2R-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman
TKFNZV-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17 - Examination Questions

WebCode Test	Response
TNEXBT-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
TVF9MD-5562	Date and Time: 2023-03-08 12:44, User Account: \David Lightman
TX22EP-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
U3RQC6-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
UKBK6E-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
URA8XZ-5561	Date and Time: 2022-03-08 12:44, User Account: David Lightman
UVZCUQ-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman
V4KY4K-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman
VCE6WL-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
VJH9N7-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
VTZR3B-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
VWB8V-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
WC9E49-5561	Date and Time: 2023-03-09 00:44, User Account: David Lightman
WD8DHB-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
WK4CUH-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
WNN64Y-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
WX2YKZ-5561	Not currently within scope of the lab.
WZGLVL-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman
XA2A8Z-5562	Date and Time: 2023-03-23 02:04, User Account: Mark
XEVDXV-5561	Not in scope
XJ99G2-5562	Date and Time: 2023-03-08 12:45, User Account: David Lightman
XQ9B22-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17 - Examination Questions

WebCode Test	Response
XVDHZK-5562	[Participant did not return results for this question.]
XWDAB7-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
XX78KX-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
Y63G92-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman
YDJQ3P-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman
YPNENR-5562	Date and Time: 2023-03-08 12:44, User Account: David Lightman
ZPR26J-5561	Date and Time: 2023-03-08 12:44, User Account: David Lightman

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17 - Examination Questions

Question 17: On what date and time, and to what user account was the LAST successful login to this computer? Provide your response in UTC+0, using the date/time (24-hour) picker which presents the date in the following format: YYYY-MM-DD.

Consensus Result:

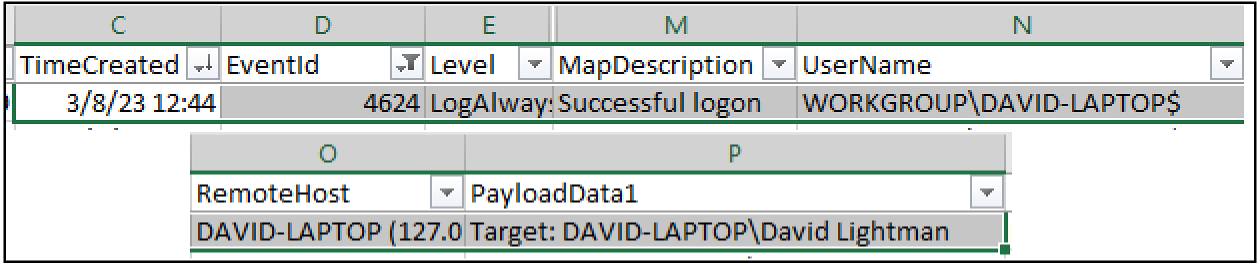
Date and Time: 2023-03-08 12:44 (times 12:43 and 12:45 were also accepted)
User Account: David Lightman

Expected Response Explanation:

Records of login events are stored in the Windows Security Event Log at C:\Windows\System32\winevt\Logs\Security.evtx. Parsing this file with Windows event viewer or an appropriate forensic tool, sorting by time and filtering by event ID 4624 and login type 2 will show the last successful login and the target user account. The last login date for a user is also recorded in the System Accounts Manager registry hive.

Expected Response Illustration:

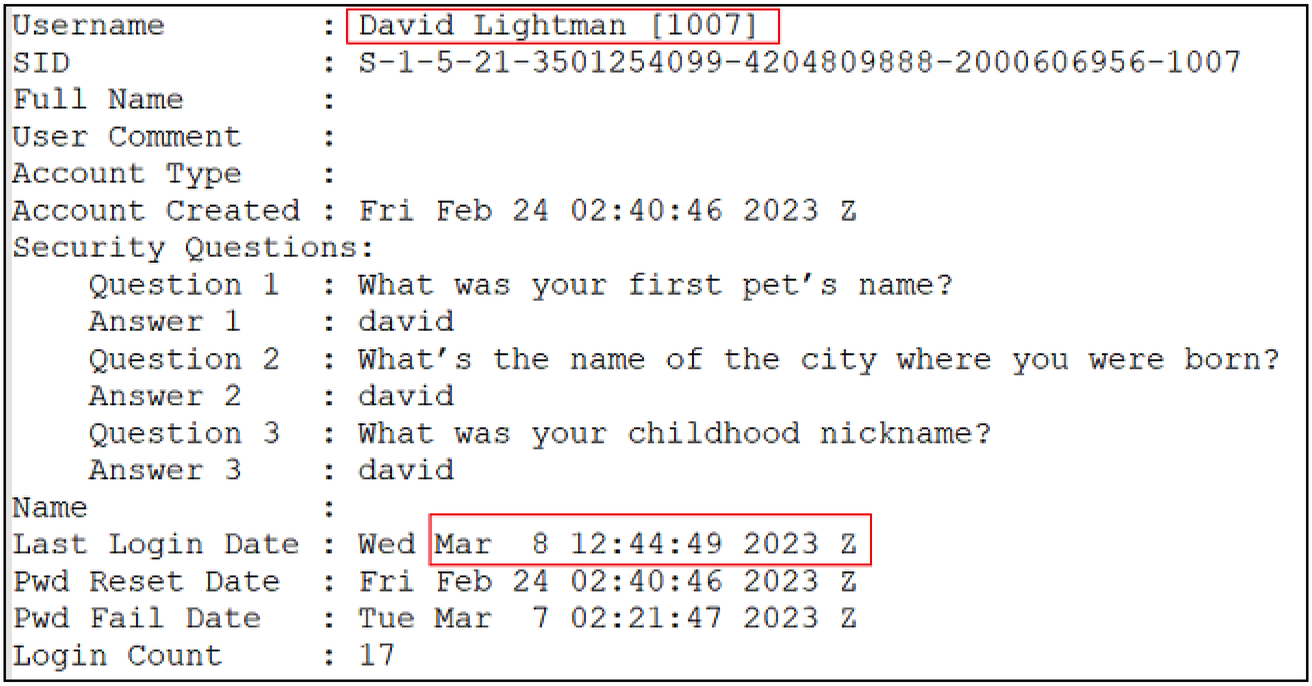
Evtx Explorer Parse of Security.evtx



C	D	E	M	N
TimeCreated	EventId	Level	MapDescription	UserName
3/8/23 12:44	4624	LogAlway:	Successful logon	WORKGROUP\DAVID-LAPTOP$

O	P
RemoteHost	PayloadData1
DAVID-LAPTOP (127.0	Target: DAVID-LAPTOP\David Lightman

RegRipper view of SAM hive login data for David Lightman



```
Username        : David Lightman [1007]
SID             : S-1-5-21-3501254099-4204809888-2000606956-1007
Full Name       :
User Comment    :
Account Type    :
Account Created : Fri Feb 24 02:40:46 2023 Z
Security Questions:
    Question 1  : What was your first pet's name?
    Answer 1    : david
    Question 2  : What's the name of the city where you were born?
    Answer 2    : david
    Question 3  : What was your childhood nickname?
    Answer 3    : david
Name            :
Last Login Date : Wed Mar  8 12:44:49 2023 Z
Pwd Reset Date  : Fri Feb 24 02:40:46 2023 Z
Pwd Fail Date   : Tue Mar  7 02:21:47 2023 Z
Login Count     : 17
```

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18 - Examination Questions

Question 18: What is the original (pre-deletion) path and name of $IB5V1XN.jpg (found in the user David Lightman's Recycle Bin on C:)? (e.g., /directory/subdirectory/name.extension)

Manufacturer's Expected Response: C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg

WebCode Test	Response
2A9WQN-5561	\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
2P2VAR-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
2PJFNF-5562	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
2VQ8RL-5562	David Lightman/Pictures/44hwqmwufwka1.jpg
2ZFN6X-5561	C:/Users/David Lightman/Pictures/44hwqmwufwka1.jpg
3CDK6E-5562	\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
3DPEPK-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
3M9X4P-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
42BM2N-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
48GFVJ-5561	/Users/David Lightman/Pictures/44hwqmwufwka1.jpg
4U7ZP2-5562	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
649HZ6-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
68RW46-5562	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
6DZZCR-5561	/Users/David Lightman/Pictures/44hwqmwufwka1.jpg
6MKCN6-5562	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
6Q2RXW-5562	Path: C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg, Name: 44hwqmwufwka1.jpg
6Q4JPC-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
6QKH3A-5562	Time different. May be due to time zone difference - One URL shows 'portal.st.clotildes', other shows 'portal.stclotildes'
6TR3NP-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
72ZUTD-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18 - Examination Questions

WebCode Test	Response
78PAK7-5562	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
7JUP4F-5561	users\david lightman\pictures\44hwqmwufwka.jpg
7PQ8PM-5562	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
7XZLMH-5562	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
82VWX9-5562	Name: 44hwqmwufwka1.jpg File path: C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
83AEYT-5562	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
8CB97J-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
8LJ9TK-5561	C:/Users/David Lightman/Pictures/44hwqmwufwka1.jpg
96TUNQ-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
98ZV8C-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
99QBZK-5562	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
9AJ8JM-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
9J9Q8U-5562	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
A8QHYB-5562	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
A8VQBZ-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
ABK3AJ-5561	NOT IN SCOPE
ACTERK-5561	Not in Scope
ADYU2Y-5562	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
AKG6BT-5562	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
AM94QQ-5561	/Users/David Lightman/Pictures/44hwqmwufwka1.jpg
BFKZWF-5562	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
BQRG78-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18 - Examination Questions

WebCode Test	Response
C4LMC9-5562	/Users/David Lightman/Pictures/44hwqmwufwka1.jpg
C897D8-5561	/Users/David Lightman/Pictures/44hwqmwufwka1.jpg
CF2CBE-5562	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
CKAXYB-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
CP6N6M-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
D7PUVD-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
DB6AM4-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
DGVH9K-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
DXVP3C-5562	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
E2RHRZ-5562	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
E4ZNBG-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
EV7HHF-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
F3JVRX-5561	C:/Users/David Lightman/Pictures/44hwqmwufwka1.jpg
FZVEJB-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
G973T4-5561	File Name : 44hwqmwufwka1.jpg File Original Path : C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
GJ39KG-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
GYTEQP-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
HQVXJW-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
HUFQTD-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
HW2LD2-5562	[Participant did not return results for this question.]
J84AQF-5562	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
JE9W33-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18 - Examination Questions

WebCode Test	Response
JGBUAC-5562	\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
JJDU63-5561	/Users/David Lightman/Pictures/44hwqmwufwka1.jpg
JL32PY-5562	C:/Users/David Lightman/Pictures/44hwqmwufwka1.jpg
JLRZA6-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
JPKFX7-5561	C:/Users/DavidLightman/Pictures/44hwqmwnfwka1.jpg
KR28JR-5562	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
KR4V3R-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
KXRBW6-5562	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
KZVDDT-5561	\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
LDKC3B-5561	/Users/David Lightman/Pictures/44hwqmwufwka1.jpg
M9HYHY-5561	Path: Path: C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg Name: 44hwqmwufwka1.jpg
MF4Q7B-5561	\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
MF8B24-5561	\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
NADTWE-5561	\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
NE7TEF-5562	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
NTANM4-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
NTZJR4-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
P3ACZC-5561	C:\Users\David Lightman\Pictures\44hwqmwufwkal.jpg
P79FU7-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
P8ZNUA-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
PFEMA7-5562	/Users/David Lightman/Pictures/44hwqmwufwka1.jpg
PFVN93-5561	C:\Users\David Lightman\Pictures\44hwqmwufwkal.jpg

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18 - Examination Questions

WebCode Test	Response
PLGGK2-5561	Users\David Lightman\Pictures\44hwqmwufwka1.jpg
PPMYM4-5562	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
PTKDEZ-5562	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
PUTRGY-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
PWJXV6-5561	David Lightman/pictures/44hwqmwufwka1.jpg
Q2CFQV-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
Q33NQX-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
Q3RHY2-5561	C:\Users\David Lightman\Pictures\44hqmwufwka1.jpg
QMR3Q2-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
QRJAR3-5561	/Users/David Lightman/Pictures/44hwqmwufwka1.jpg
QTHAXU-5561	\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
RAK67E-5562	Users/David Lightman/Pictures/44hwqmwufwka1.jpg
RBBDCA-5562	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
RGH4EF-5562	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
RRMUMV-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
RRXTDK-5562	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
RV3JKZ-5561	File Name : 44hwqmwufwka1.jpg File Original Path : C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
TC4JAF-5562	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
TCGEBD-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
TEPC2R-5562	Path: Path: C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg Name: 44hwqmwufwka1.jpg
TKFNZV-5561	Path: Path: C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg Name: 44hwqmwufwka1.jpg
TNEXBT-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18 - Examination Questions

WebCode Test	Response
TVF9MD-5562	C:\Users\David Lightman\Pictures
TX22EP-5561	C:/Users/David Lightman/Pictures/44hwqmwufwka1.jpg
U3RQC6-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
UKBK6E-5561	C:\Users\David Lightman\Pictures\44hwqmwufwkal.jpg
URA8XZ-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
UVZCUQ-5562	\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
V4KY4K-5562	\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
VCE6WL-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
VJH9N7-5561	C:/Users/David Lightman/Pictures/44hwqmwufwka1.jpg
VTZR3B-5561	\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
VVVB8V-5561	\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
WC9E49-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
WD8DHB-5561	C: \Users\David Lightman\Pictures\44hwqmwufwka1.jpg
WK4CUH-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
WNN64Y-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
WX2YKZ-5561	Not currently within scope of the lab.
WZGLVL-5562	c:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
XA2A8Z-5562	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
XEVDXV-5561	Not in scope
XJ99G2-5562	Original Path: C:\Users\David Lightman\Pictures & Original Name: 44hwqmwufwka1.jpg
XQ9B22-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
XVDHZK-5562	[Participant did not return results for this question.]

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18 - Examination Questions

WebCode Test	Response
XWDAB7-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
XX78KX-5561	/Users/David Lightman/Pictures/44hwqmwufwka1.jpg
Y63G92-5562	\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
YDJQ3P-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
YPNENR-5562	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg
ZPR26J-5561	C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18 - Examination Questions

Question 18: What is the original (pre-deletion) path and name of $IB5V1XN.jpg (found in the user David Lightman's Recycle Bin on C:)? (e.g., /directory/subdirectory/name.extension)

Consensus Result:

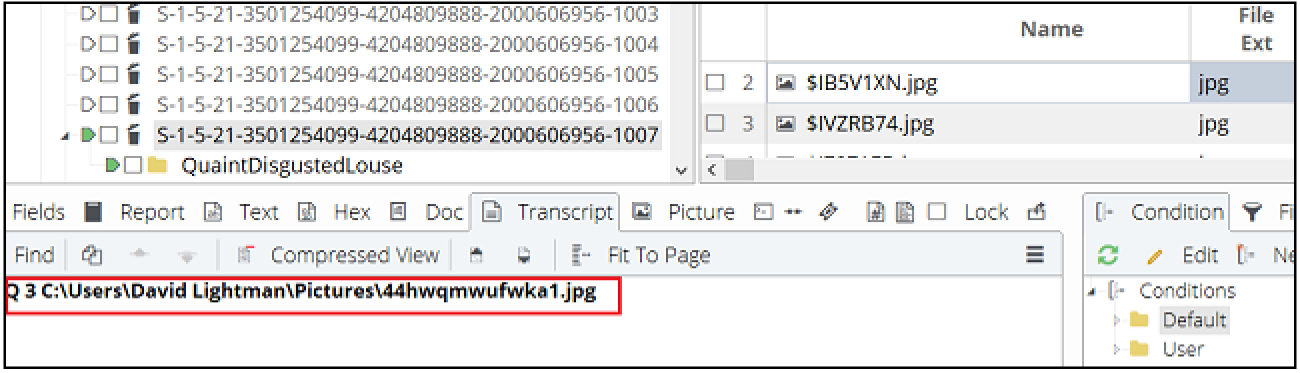
C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg

Expected Response Explanation:

Every user on a system has a folder in C:\$Recycle.Bin named with their Security Identifier, or SID. In this case, the user David Lightman's SID is S-1-5-21-3501254099-4204809888-2000606956-1007. Within that folder are generally a pair of files for each recycled file. One, beginning with $I, which contains the metadata for the recycled file and another, beginning with $R, containing the file's content.

Expected Response Illustration:

EnCase view of Recycle Bin Files



S-1-5-21-3501254099-4204809888-2000606956-1003
S-1-5-21-3501254099-4204809888-2000606956-1004
S-1-5-21-3501254099-4204809888-2000606956-1005
S-1-5-21-3501254099-4204809888-2000606956-1006
S-1-5-21-3501254099-4204809888-2000606956-1007
QuaintDisgustedLouse

	Name	File Ext
2	$IB5V1XN.jpg	jpg
3	$IVZRB74.jpg	jpg

Q 3 C:\Users\David Lightman\Pictures\44hwqmwufwka1.jpg

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 19 - Examination Questions

Question 19: What user account (name) is the owner of C:\Users\Mark\Desktop\qujysbx38kia1.jpg?

Manufacturer's Expected Response: David Lightman

** Inconsistencies not highlighted; No consensus achieved **

WebCode Test	Response
2A9WQN-5561	Mark
2P2VAR-5561	Mark
2PJFNF-5562	Mark
2VQ8RL-5562	Mark
2ZFN6X-5561	David Lightman
3CDK6E-5562	David Lightman
3DPEPK-5561	David Lightman
3M9X4P-5561	Mark
42BM2N-5561	David Lightman
48GFVJ-5561	David Lightman
4U7ZP2-5562	Mark
649HZ6-5561	David Lightman
68RW46-5562	David Lightman
6DZZCR-5561	David Lightman
6MKCN6-5562	Mark
6Q2RXW-5562	David Lightman
6Q4JPC-5561	David Lightman
6QKH3A-5562	Mark
6TR3NP-5561	David Lightman – 1007
72ZUTD-5561	David Lightman
78PAK7-5562	David Lightman

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 19 - Examination Questions

** Inconsistencies not highlighted; No consensus achieved **

WebCode Test	Response
7JUP4F-5561	mark
7PQ8PM-5562	Mark
7XZLMH-5562	David Lightman
82VWX9-5562	Mark
83AEYT-5562	David Lightman
8CB97J-5561	DAVID-LAPTOP\Mark
8LJ9TK-5561	Mark
96TUNQ-5561	David Lightman
98ZV8C-5561	Mark, but was in David Lightburn's account first, found as a thumbcache and recycled file
99QBZK-5562	David Lightman SID 1007
9AJ8JM-5561	Mark
9J9Q8U-5562	Mark is the user under this path, but David Lightman was the owner until it was deleted on 3-7-2023 from the Dropbox folder.
A8QHYB-5562	David Lightman
A8VQBZ-5561	David Lightman
ABK3AJ-5561	NOT IN SCOPE
ACTERK-5561	Not in Scope
ADYU2Y-5562	David Lightman
AKG6BT-5562	David Lightman
AM94QQ-5561	David Lightman
BFKZWF-5562	Mark
BQRG78-5561	David Lightman
C4LMC9-5562	David Lightman

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 19 - Examination Questions

WebCode Test	Response ** Inconsistencies not highlighted; No consensus achieved **
C897D8-5561	Mark
CF2CBE-5562	Mark
CKAXYB-5561	David Lightman
CP6N6M-5561	DAVID-LAPTOP\Mark
D7PUVD-5561	Mark
DB6AM4-5561	David Lightman
DGVH9K-5561	David Lightman
DXVP3C-5562	Mark
E2RHRZ-5562	Mark
E4ZNBG-5561	Mark
EV7HHF-5561	David Lightman
F3JVRX-5561	David Lightman
FZVEJB-5561	David Lightman
G973T4-5561	Mark
GJ39KG-5561	Mark
GYTEQP-5561	Mark
HQVXJW-5561	David Lightman
HUFQTD-5561	David Lightman
HW2LD2-5562	[Participant did not return results for this question.]
J84AQF-5562	Mark
JE9W33-5561	David Lightman
JGBUAC-5562	Mark

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 19 - Examination Questions

WebCode Test	Response ** Inconsistencies not highlighted; No consensus achieved **
JJDU63-5561	David Lightman
JL32PY-5562	David Lightman
JLRZA6-5561	David Lightman
JPKFX7-5561	David Lightman
KR28JR-5562	David Lightman
KR4V3R-5561	David Lightman
KXRBW6-5562	Mark
KZVDDT-5561	David Lightman
LDKC3B-5561	David Lightman
M9HYHY-5561	Mark
MF4Q7B-5561	Mark
MF8B24-5561	David Lightman
NADTWE-5561	David Lightman
NE7TEF-5562	Mark
NTANM4-5561	Mark
NTZJR4-5561	Mark
P3ACZC-5561	David Lightman
P79FU7-5561	David Lightman
P8ZNUA-5561	David Lightman
PFEMA7-5562	Mark
PFVN93-5561	David Lightman
PLGGK2-5561	David Lightman

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 19 - Examination Questions

WebCode Test	Response ** Inconsistencies not highlighted; No consensus achieved **
PPMYM4-5562	Mark
PTKDEZ-5562	David Lightman
PUTRGY-5561	Mark
PWJXV6-5561	David Lightman
Q2CFQV-5561	David Lightman
Q33NQX-5561	David Lightman
Q3RHY2-5561	David Lightman
QMR3Q2-5561	David Lightman
QRJAR3-5561	David Lightman
QTHAXU-5561	David Lightman
RAK67E-5562	David Lightman
RBBDCA-5562	David Lightman
RGH4EF-5562	David Lightman
RRMUMV-5561	David Lightman
RRXTDK-5562	David Lightman
RV3JKZ-5561	Mark
TC4JAF-5562	David Lightman
TCGEBD-5561	Mark
TEPC2R-5562	Mark
TKFNZV-5561	Mark
TNEXBT-5561	Mark
TVF9MD-5562	Mark

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 19 - Examination Questions

** Inconsistencies not highlighted; No consensus achieved **

WebCode Test	Response
TX22EP-5561	David Lightman
U3RQC6-5561	Mark
UKBK6E-5561	Mark
URA8XZ-5561	Mark
UVZCUQ-5562	David Lightman
V4KY4K-5562	Mark
VCE6WL-5561	David Lightman
VJH9N7-5561	David Lightman
VTZR3B-5561	Account “David Lightman” originally owned this image within a Dropbox folder, this was then moved over to account “Mark”. The owner is still attributed to “David Lightman”.
VVVB8V-5561	David Lightman
WC9E49-5561	David Lightman
WD8DHB-5561	David Lightman
WK4CUH-5561	David Lightman
WNN64Y-5561	David Lightman
WX2YKZ-5561	Not currently within scope of the lab.
WZGLVL-5562	David Lightman
XA2A8Z-5562	David Lightman
XEVDXV-5561	Not in scope
XJ99G2-5562	Mark
XQ9B22-5561	Administrators
XVDHZK-5562	[Participant did not return results for this question.]
XWDAB7-5561	David Lightman

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 19 - Examination Questions

** Inconsistencies not highlighted; No consensus achieved **

WebCode Test	Response
XX78KX-5561	Mark
Y63G92-5562	David Lightman
YDJQ3P-5561	Mark
YPNENR-5562	Mark
ZPR26J-5561	David Lightman

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 19 - Examination Questions

Question 19: What user account (name) is the owner of C:\Users\Mark\Desktop\qujysbx38kia1.jpg?

Consensus Result:

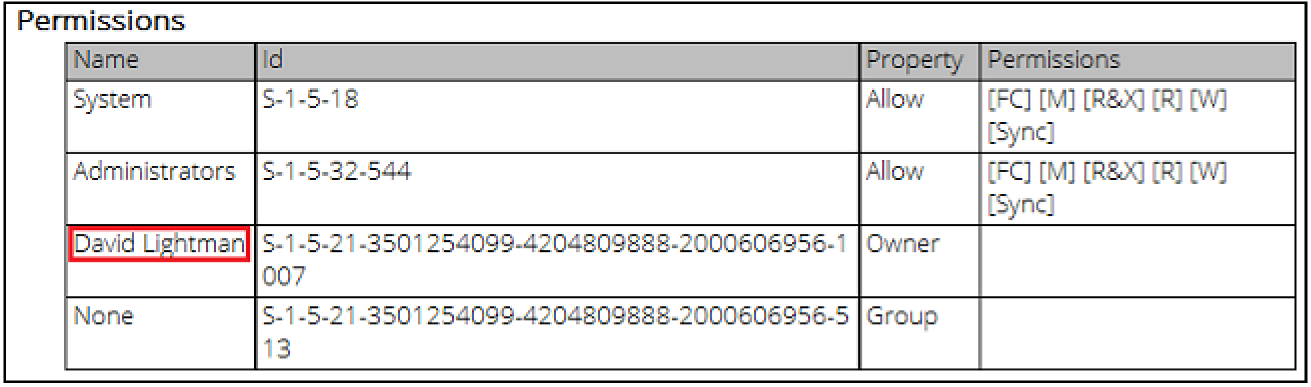
A consensus was not achieved for this question. Seventy-eight participants (60%) reported the expected account name, David Lightman. Fifty-one participants (39%) reported Mark. The file listed in the question was found in Mark's profile (directory) but he was not the owner. The intent of this question was for the participant to provide the file ownership information contained in the NTFS file system metadata for the file. The file location (path or directory) does not indicate ownership.

Expected Response Explanation:

NTFS file system metadata include file permissions and ownership. This information can be viewed with most forensic tools.

Expected Response Illustration:

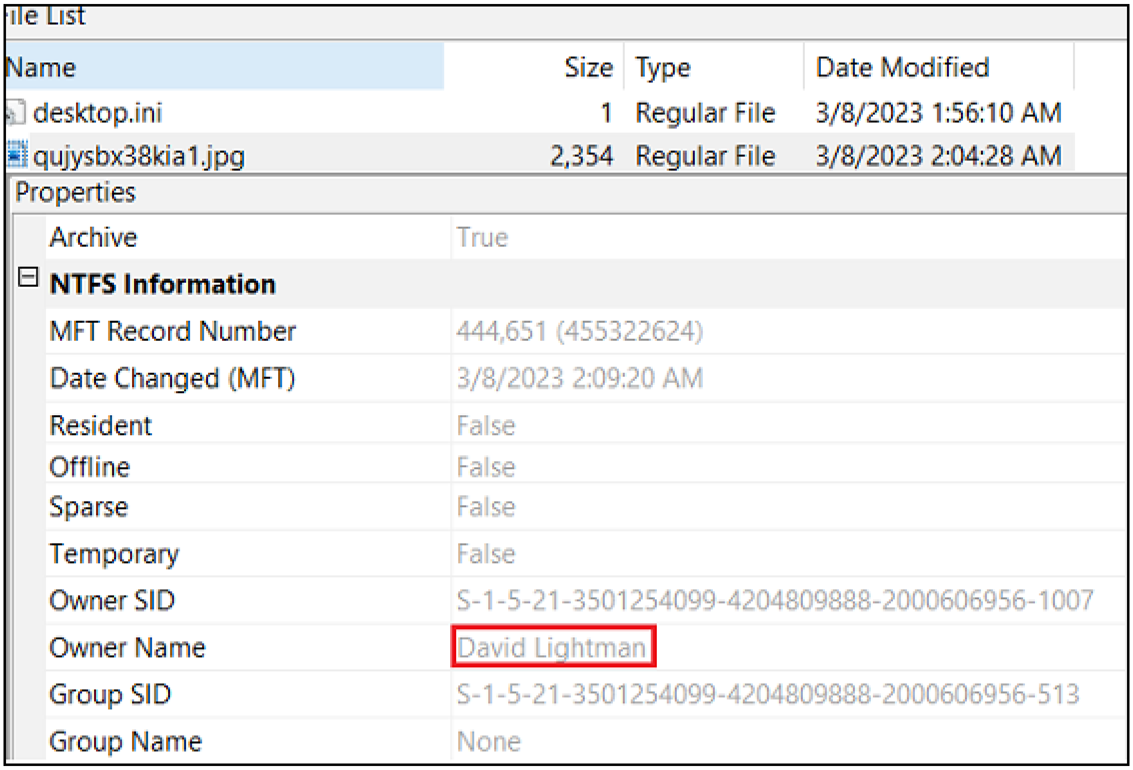
EnCase view of qujysbx38kia1.jpg permissions



Permissions

Name	Id	Property	Permissions
System	S-1-5-18	Allow	[FC] [M] [R&X] [R] [W] [Sync]
Administrators	S-1-5-32-544	Allow	[FC] [M] [R&X] [R] [W] [Sync]
David Lightman	S-1-5-21-3501254099-4204809888-2000606956-1007	Owner	
None	S-1-5-21-3501254099-4204809888-2000606956-513	Group	

FTK Imager view of qujysbx38kia1.jpg permissions



ile List

Name	Size	Type	Date Modified
desktop.ini	1	Regular File	3/8/2023 1:56:10 AM
qujysbx38kia1.jpg	2,354	Regular File	3/8/2023 2:04:28 AM

Properties

Archive	True
⊟ **NTFS Information**	
MFT Record Number	444,651 (455322624)
Date Changed (MFT)	3/8/2023 2:09:20 AM
Resident	False
Offline	False
Sparse	False
Temporary	False
Owner SID	S-1-5-21-3501254099-4204809888-2000606956-1007
Owner Name	David Lightman
Group SID	S-1-5-21-3501254099-4204809888-2000606956-513
Group Name	None

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20 - Examination Questions

Question 20: What is the filetype (MIME type) for the file with SHA-1 hash c9abb4c11ccec6950fb58f146ac84269dedc2223?

Manufacturer's Expected Response: Portable Network Graphic or PNG

WebCode Test	Response
2A9WQN-5561	PNG
2P2VAR-5561	PNG
2PJFNF-5562	png
2VQ8RL-5562	JoyousSillyHedgehog.dat (image/png)
2ZFN6X-5561	PNG
3CDK6E-5562	PNG – portable network graphics
3DPEPK-5561	PNG image file
3M9X4P-5561	.dat (image or picture filetype)
42BM2N-5561	.png
48GFVJ-5561	image/png
4U7ZP2-5562	Portable Network Graphic
649HZ6-5561	Picture
68RW46-5562	image/png
6DZZCR-5561	.dat
6MKCN6-5562	png
6Q2RXW-5562	PNG
6Q4JPC-5561	.dat
6QKH3A-5562	Image/png
6TR3NP-5561	Image/png
72ZUTD-5561	PNG

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20 - Examination Questions

WebCode Test	Response
78PAK7-5562	image/png
7JUP4F-5561	png
7PQ8PM-5562	.PNG (image/png)
7XZLMH-5562	.png
82VWX9-5562	PNG file (image/png)
83AEYT-5562	image/png
8CB97J-5561	image/png
8LJ9TK-5561	image/png
96TUNQ-5561	PNG
98ZV8C-5561	Image / PNG
99QBZK-5562	PNG
9AJ8JM-5561	PNG
9J9Q8U-5562	It is .dat file
A8QHYB-5562	image/png
A8VQBZ-5561	image/png
ABK3AJ-5561	NOT IN SCOPE
ACTERK-5561	Not in Scope
ADYU2Y-5562	Png
AKG6BT-5562	PNG file (Portable network graphic)
AM94QQ-5561	image/png
BFKZWF-5562	image/png
BQRG78-5561	PNG (Portable Network Graphic)

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20 - Examination Questions

WebCode Test	Response
C4LMC9-5562	PNG
C897D8-5561	image/png
CF2CBE-5562	image/png
CKAXYB-5561	PNG
CP6N6M-5561	image/png
D7PUVD-5561	.dat
DB6AM4-5561	Portable Network Graphic (image/png)
DGVH9K-5561	image/PNG (0x89 0x50 0x4E 0x47)
DXVP3C-5562	.dat = DATA
E2RHRZ-5562	Image
E4ZNBG-5561	.PNG
EV7HHF-5561	.png Portable Network Graphics image/png
F3JVRX-5561	image/png
FZVEJB-5561	PNG
G973T4-5561	JoyousSillyHedgehog.dat image/png
GJ39KG-5561	Picture
GYTEQP-5561	image/png
HQVXJW-5561	image/png
HUFQTD-5561	PNG
HW2LD2-5562	[Participant did not return results for this question.]
J84AQF-5562	PNG
JE9W33-5561	image/png

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20 - Examination Questions

WebCode Test	Response
JGBUAC-5562	.dat
JJDU63-5561	PNG
JL32PY-5562	dat (signature : png)
JLRZA6-5561	Image/png
JPKFX7-5561	Portable Network Graphic (PNG)
KR28JR-5562	image/png
KR4V3R-5561	image/png
KXRBW6-5562	.dat
KZVDDT-5561	.png
LDKC3B-5561	image/png
M9HYHY-5561	Image - PNG
MF4Q7B-5561	JoyousSillyHedgehog.dat (File Type .DAT)
MF8B24-5561	.png
NADTWE-5561	jpg
NE7TEF-5562	png
NTANM4-5561	PNG
NTZJR4-5561	image
P3ACZC-5561	png
P79FU7-5561	.png
P8ZNUA-5561	PNG
PFEMA7-5562	PNG (Image)
PFVN93-5561	PNG

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20 - Examination Questions

WebCode Test	Response
PLGGK2-5561	PNG filetype
PPMYM4-5562	Picture
PTKDEZ-5562	image/png
PUTRGY-5561	image/png
PWJXV6-5561	PNG
Q2CFQV-5561	image/png
Q33NQX-5561	image/png
Q3RHY2-5561	PNG
QMR3Q2-5561	The extention is .dat but signature is png .
QRJAR3-5561	PNG
QTHAXU-5561	PNG
RAK67E-5562	Image/png
RBBDCA-5562	PNG (Image)
RGH4EF-5562	Portable Network Graphic (PNG)
RRMUMV-5561	.png image/x-png
RRXTDK-5562	image/png
RV3JKZ-5561	JoyousSillyHedgehog.dat image/png
TC4JAF-5562	image/png
TCGEBD-5561	image/png
TEPC2R-5562	Image - PNG
TKFNZV-5561	Image - PNG
TNEXBT-5561	PNG

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20 - Examination Questions

WebCode Test	Response
TVF9MD-5562	PNG
TX22EP-5561	image/png
U3RQC6-5561	Image .png
UKBK6E-5561	PNG , \Users\David Lightman\Documents\FragileShinyJellyfish\JoyousSillyHedgehog.dat
URA8XZ-5561	image/png
UVZCUQ-5562	image/png
V4KY4K-5562	(Image File) *.PNG [89 50 4E 47 ..]
VCE6WL-5561	PNG
VJH9N7-5561	Image/PNG
VTZR3B-5561	PNG
VVVB8V-5561	PNG
WC9E49-5561	Portable Network Graphic (PNG)
WD8DHB-5561	PNG
WK4CUH-5561	PNG
WNN64Y-5561	PNG
WX2YKZ-5561	Not currently within scope of the lab.
WZGLVL-5562	image/png
XA2A8Z-5562	PNG
XEVDXV-5561	Not in scope
XJ99G2-5562	image/png
XQ9B22-5561	Image - PNG
XVDHZK-5562	[Participant did not return results for this question.]

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20 - Examination Questions

WebCode Test	Response
XWDAB7-5561	image/png
XX78KX-5561	image/png
Y63G92-5562	.png (portable network Graphic)
YDJQ3P-5561	.dat = DATA
YPNENR-5562	image/png
ZPR26J-5561	image/png

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20 - Examination Questions

Question 20: What is the filetype (MIME type) for the file with SHA-1 hash c9abb4c11ccec6950fb58f146ac84269dedc2223?

Consensus Result:

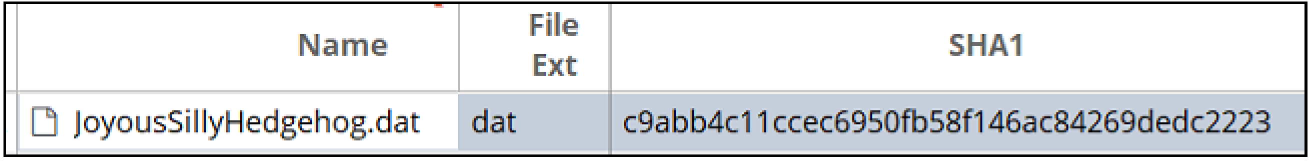
PNG or image/PNG

Expected Response Explanation:

The file can be located with a sorted list of SHA-1 hashes for all files on the device. The file is named JoyousSillyHedgehog.dat, suggesting it is a raw data format file and will not be displayed as an image by Windows or by a forensic tool if file signatures analysis has not been performed. However, internally it has the 89 50 4E 47 0D 0A (%PNG) header and is actually a Portable Network Graphic (PNG) file.

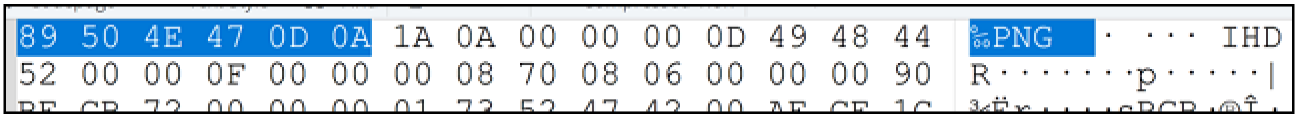
Expected Response Illustration:

EnCase Table view showing hash and filename



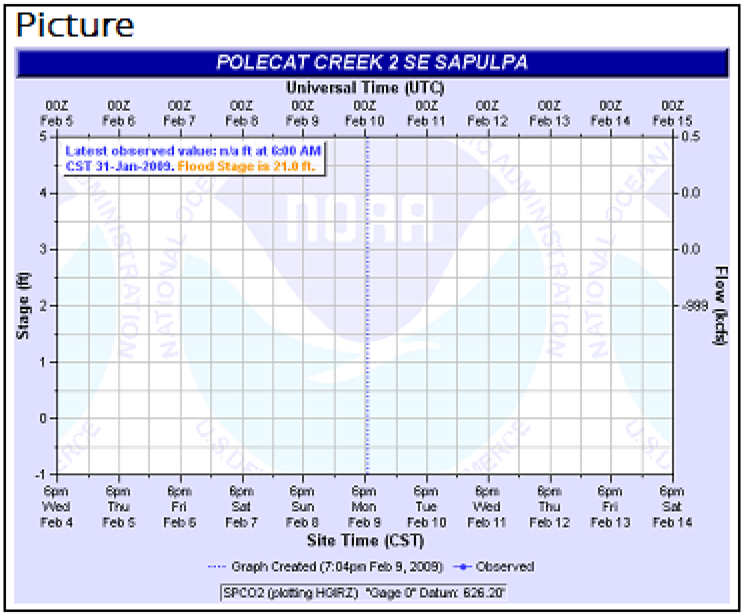
Name	File Ext	SHA1
JoyousSillyHedgehog.dat	dat	c9abb4c11ccec6950fb58f146ac84269dedc2223

EnCase Hex view showing file header



```
89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44   ‰PNG · ··· IHD
52 00 00 0F 00 00 00 08 70 08 06 00 00 00 90   R·······p·····|
BE CB 72 00 00 00 01 73 52 47 42 00 AE CE 1C   ¾Ër····sRGB·®Î·
```

JoyousSillyHedgehog.dat



Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21 - Examination Questions

Question 21: Provide the name of the regular file (i.e. NOT hidden, deleted, aliased, etc.) in C:\Windows\System32\drivers with the earliest (oldest) ($STANDARD_INFORMATION Attribute) created time.

Manufacturer's Expected Response: wincatyawn.sys

WebCode Test	** Inconsistencies not highlighted; No consensus achieved ** Response
2A9WQN-5561	wincatyawn.sys
2P2VAR-5561	gmreadme.txt
2PJFNF-5562	mfc120u.dll, mfcm120.dll, msvcr120.dll, vccorlib120.dll, msvcp120.dll, mfcm120u.dl
2VQ8RL-5562	wincatyawn.sys
2ZFN6X-5561	Wincatyawn.sys
3CDK6E-5562	wincatyawn.sys
3DPEPK-5561	wincatyawn.sys
3M9X4P-5561	wincatyawn.sys
42BM2N-5561	wincatyawn.sys
48GFVJ-5561	wincatyawn.sys
4U7ZP2-5562	netr28ux.sys
649HZ6-5561	wincatyawn.sys
68RW46-5562	wincatyawn.sys
6DZZCR-5561	Wincatyawn.sys
6MKCN6-5562	gmreadme.txt
6Q2RXW-5562	wincatyawn.sys
6Q4JPC-5561	wincatyawn.sys
6QKH3A-5562	wincatyawn.sys
6TR3NP-5561	wincatyawn.sys
72ZUTD-5561	wincatyawn.sys

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21 - Examination Questions

WebCode Test	Response ** Inconsistencies not highlighted; No consensus achieved **
78PAK7-5562	wincatyawn.sys
7JUP4F-5561	wincatyawn.sys
7PQ8PM-5562	wincatyawn.sys
7XZLMH-5562	wincatyawn.sys
82VWX9-5562	wincatyawn.sys
83AEYT-5562	wincatyawn.sys
8CB97J-5561	wincatyawn.sys
8LJ9TK-5561	wincatyawn.sys
96TUNQ-5561	wincatyawn.sys
98ZV8C-5561	wincatyawn.sys
99QBZK-5562	wincatyawn.sys
9AJ8JM-5561	wincatyawn.sys
9J9Q8U-5562	wincatyawn.sys
A8QHYB-5562	wincatyawn.sys
A8VQBZ-5561	wincatyawn.sys
ABK3AJ-5561	NOT IN SCOPE
ACTERK-5561	Not in Scope
ADYU2Y-5562	wincatyawn.sys
AKG6BT-5562	wincatyawn.sys
AM94QQ-5561	wincatyawn.sys
BFKZWF-5562	wincatyawn.sys
BQRG78-5561	wincatyawn.sys

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21 - Examination Questions

** Inconsistencies not highlighted; No consensus achieved **

WebCode Test	Response
C4LMC9-5562	wincatyawn.sys
C897D8-5561	wincatyawn.sys
CF2CBE-5562	wincatyawn.sys
CKAXYB-5561	wincatyawn.sys
CP6N6M-5561	wincatyawn.sys
D7PUVD-5561	wincatyawn.sys
DB6AM4-5561	wincatyawn.sys
DGVH9K-5561	The only non-alias, non system file is gmreadme.txt. wincatyawn.sys is the oldest file, but it is an alias. Next oldest are system files, with 10 files that all have the same date/time. ***See Notes [Table 3: Additional Comments] for concerns/questions
DXVP3C-5562	UMDF
E2RHRZ-5562	gmreadme.txt
E4ZNBG-5561	Patch_7662.bin
EV7HHF-5561	wincatyawn.sys
F3JVRX-5561	wincatyawn.sys
FZVEJB-5561	wincatyawn.sys
G973T4-5561	wincatyawn.sys
GJ39KG-5561	2/5/2017 02:33:02 UTC
GYTEQP-5561	wincatyawn.sys
HQVXJW-5561	wincatyawn.sys
HUFQTD-5561	wincatyawn.sys 2017-02-05 02:33:02 (UTC) (2/4/2017 9:33:02 PM (Local))
HW2LD2-5562	[Participant did not return results for this question.]
J84AQF-5562	wincatyawn.sys 5/2/17 3:33:02
JE9W33-5561	wincatyawn.sys

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21 - Examination Questions

WebCode Test	Response ** Inconsistencies not highlighted; No consensus achieved **
JGBUAC-5562	wincatyawn.sys date and time: 05/02/2017 02:33:02
JJDU63-5561	wincatyawn.sys
JL32PY-5562	wincatyawn.sys
JLRZA6-5561	wincatyawn.sys
JPKFX7-5561	Microsoft.Bluetooth.Avrcp.Transport.sys
KR28JR-5562	wincatyawn.sys
KR4V3R-5561	wincatyawn.sys
KXRBW6-5562	wincatyawn.sys
KZVDDT-5561	wincatyawn.sys
LDKC3B-5561	wincatyawn.sys
M9HYHY-5561	wincatyawn.sys
MF4Q7B-5561	wincatyawn.sys
MF8B24-5561	wincatyawn.sys
NADTWE-5561	wincatyawn.sys
NE7TEF-5562	gmreadme.txt
NTANM4-5561	gmreadme.txt
NTZJR4-5561	wincatyawn.sys
P3ACZC-5561	wincatyawn.sys
P79FU7-5561	wincatyawn.sys
P8ZNUA-5561	wincatyawn.sys
PFEMA7-5562	wincatyawn.sys
PFVN93-5561	wincatyawn.sys

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21 - Examination Questions

** Inconsistencies not highlighted; No consensus achieved **

WebCode Test	Response
PLGGK2-5561	wincatyawn.sys
PPMYM4-5562	wincatyawn.sys
PTKDEZ-5562	wincatyawn.sys
PUTRGY-5561	wincatyawn.sys
PWJXV6-5561	wincatyawn.sys
Q2CFQV-5561	wincatyawn.sys
Q33NQX-5561	wincatyawn.sys
Q3RHY2-5561	wincatyawn.sys
QMR3Q2-5561	wincatyawn.jpg
QRJAR3-5561	BthA2dp.sys
QTHAXU-5561	wincatyawn.sys
RAK67E-5562	wincatyawn.sys
RBBDCA-5562	wincatyawn.sys
RGH4EF-5562	bcmfn2.sys
RRMUMV-5561	wincatyawn.sys
RRXTDK-5562	wincatyawn.sys
RV3JKZ-5561	wincatyawn.sys
TC4JAF-5562	wincatyawn.sys
TCGEBD-5561	wincatyawn.sys
TEPC2R-5562	wincatyawn.sys
TKFNZV-5561	wincatyawn.sys
TNEXBT-5561	dbx-dev.sys

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21 - Examination Questions

WebCode Test	Response ** Inconsistencies not highlighted; No consensus achieved **
TVF9MD-5562	wincatyawn.sys
TX22EP-5561	wincatyawn.sys
U3RQC6-5561	wincatyawn.sys
UKBK6E-5561	BtaMPM.sys
URA8XZ-5561	wincatyawn.sys
UVZCUQ-5562	wincatyawn.jpg
V4KY4K-5562	wincatyawn.sys
VCE6WL-5561	wincatyawn.sys (content extension is JPG)
VJH9N7-5561	wincatyawn.sys
VTZR3B-5561	wincatyawn.sys
VVVB8V-5561	wincatyawn.sys
WC9E49-5561	Wincatyawn.sys
WD8DHB-5561	wincatyawn.sys
WK4CUH-5561	wincatyawn.sys
WNN64Y-5561	Wincatyawn.sys 2017-02-05 02:33:02 UTC (2/4/2017 9:33:02 PM)
WX2YKZ-5561	Not currently within scope of the lab.
WZGLVL-5562	wincatyawn.sys
XA2A8Z-5562	wincatyawn.sys
XEVDXV-5561	Not in scope
XJ99G2-5562	wincatyawn.sys
XQ9B22-5561	wincatyawn.sys
XVDHZK-5562	[Participant did not return results for this question.]

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21 - Examination Questions

** Inconsistencies not highlighted; No consensus achieved **

WebCode Test	Response
XWDAB7-5561	wincatyawn.sys
XX78KX-5561	wincatyawn.sys
Y63G92-5562	gmreadme.txt
YDJQ3P-5561	UMDF
YPNENR-5562	wincatyawn.sys
ZPR26J-5561	wincatyawn.sys

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21 - Examination Questions

Question 21: Provide the name of the regular file (i.e. NOT hidden, deleted, aliased, etc.) in C:\Windows\System32\drivers with the earliest (oldest) ($STANDARD_INFORMATION Attribute) created time.

Consensus Result:

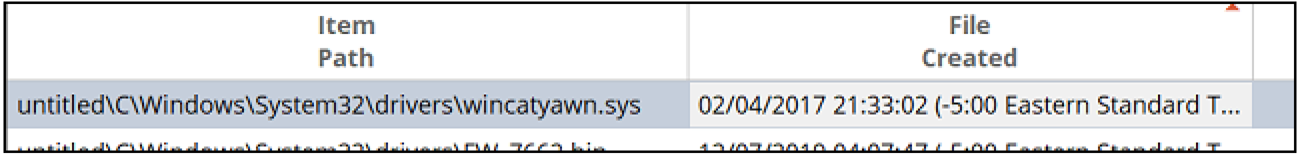
As of October 9, 2023, the text in this question is considered ambiguous or potentially misleading. The term "Regular" was ambiguous and the further clarification offered should not have included the descriptor "Not aliased." Consequently, no results are being highlighted as inconsistent by CTS. The manufacturer's expected response of wincatyawn.sys was reported by a total of 111 participants (85%).

Expected Response Explanation:

Viewing all files in the given directory and sorting by created time shows wincatyawn.sys as the oldest file by the $STANDARD_INFORMATION Attribute.

Expected Response Illustration:

EnCase view of wincatyawn.sys created datetime



Item Path	File Created
untitled\C\Windows\System32\drivers\wincatyawn.sys	02/04/2017 21:33:02 (-5:00 Eastern Standard T...
untitled\C\Windows\System32\drivers\FW-7662.bin	12/07/2019 04:07:47 (-5:00 Eastern Standard T

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22 - Examination Questions

Question 22: Describe the content of the file identified in Question 21 (regular file in C:\Windows\System32\drivers with the earliest (oldest) ($STANDARD_INFORMATION Attribute) created time).

Manufacturer's Expected Response: "A picture of a cat" and variations describing the same information.

WebCode Test	Response ** Inconsistencies not highlighted; No consensus achieved **
2A9WQN-5561	Image of black cat, lying on its back, yawning.
2P2VAR-5561	contains information related to the Roland Sound Canvas Sound Set copyright protection.
2PJFNF-5562	Microsoft Visual C++ Redistributable Package
2VQ8RL-5562	Black cat yawn (jpeg file)
2ZFN6X-5561	Photo of a black cat with its mouth open and paws stretched out.
3CDK6E-5562	JPEG image of a black cat in a wicker basket or chair.
3DPEPK-5561	Image of a Cat in a basket with its mouth open and front paws up.
3M9X4P-5561	A yawning black cat
42BM2N-5561	Black cat with arms up , mouth open , tongue out
48GFVJ-5561	JPEG image of a cat
4U7ZP2-5562	The netr28ux.sys is a driver file for a wireless card
649HZ6-5561	Picture of a black cat with mouth open and paws up, on tan wicker.
68RW46-5562	A black cat on a wicker chair, yawning.
6DZZCR-5561	Picture of a small black cat with paws up and mouth open
6MKCN6-5562	This file contains the Roland SoundCanvas Sound Set which is protected under the following copyright
6Q2RXW-5562	A yawning black cat photo
6Q4JPC-5561	A Black Cat on its back with mouth open and appearing to be yawning.
6QKH3A-5562	jpeg image of cat black cat stretching up and yawning
6TR3NP-5561	Black kitten yawning with wicker in the background
72ZUTD-5561	Black cat laying on its back with its mouth open and paws in the air.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22 - Examination Questions

WebCode Test	Response ** Inconsistencies not highlighted; No consensus achieved **
78PAK7-5562	Picture of a black cat
7JUP4F-5561	black cat yawning
7PQ8PM-5562	The file is actually a .jpg of a black cat with its tongue out and hands in the air.
7XZLMH-5562	Black cat yawning with paws in the air.
82VWX9-5562	File is NOT a .sys file, it has the file header of a JPEG When opened with an image view (in this case irfanview), image is of a yawning cat.
83AEYT-5562	A picture showing a cat yawning
8CB97J-5561	The wincatyawn.sys is a jpeg image. The image is of a cat with black fur and green eyes, stretching its lim bs whilst opening its mouth wide exposing its fangs, which looks like a yawn.
8LJ9TK-5561	A black cat.
96TUNQ-5561	Black Kitten
98ZV8C-5561	Picture of a black cat on a wicker object. The cat is yawning with its front paws raised up.
99QBZK-5562	The file shows a black kitten on its back with its mouth open and arms stretched out
9AJ8JM-5561	Playful/yawning black kitten in a basket.
9J9Q8U-5562	Photo of black kitten with paws raised.
A8QHYB-5562	Image of a black cat with it's arms up and mouth open.
A8VQBZ-5561	It is a JPEG image of a black cat yawning
ABK3AJ-5561	NOT IN SCOPE
ACTERK-5561	Not in Scope
ADYU2Y-5562	The filename suggests the file extension is .sys, however the file type is actually reported as a jpg and the contents of the file support this as an image of a black cat with arms raised.
AKG6BT-5562	The file is a jpeg image, it shows a black cat lay on its back on a wicker chair.
AM94QQ-5561	Picture of a black cat.
BFKZWF-5562	A picture of a cat
BQRG78-5561	The content of the file "wincatyawn.sys" is a picture of a black cat yawning and laying on an apparent wicker chair.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22 - Examination Questions

** Inconsistencies not highlighted; No consensus achieved **

WebCode Test	Response
C4LMC9-5562	pictureof a black kitten
C897D8-5561	image file (JPEG Image Standard)
CF2CBE-5562	a picture of a black cat
CKAXYB-5561	The file type for the file is JPEG. The picture depicts a black cat with its paws outstretched, on a wicker background
CP6N6M-5561	The wincatyawn.sys is a jpeg image. The image is of a cat with black fur and green eyes, stretching its limbs whilst opening its mouth wide exposing its fangs, which looks like a yawn.
D7PUVD-5561	Black kitten on a beige rattan seat laying on its back with front paws raised and mouth wide open
DB6AM4-5561	The file identified in Question 21 is named wincatyawn.sys and is a .jpg file. The .jpg file contains an image of a cat that appears to be yawning.
DGVH9K-5561	gmreadme.txt is a text file for Roland SoundCanvas. wincatyawn.sys is an image file of a black cat who appears to be yawning while laying on its back on a basket-type background.
DXVP3C-5562	.dll files = Dynamic Link Library + resources for .dll (.dll.mui)
E2RHRZ-5562	Copyright text file (.txt)
E4ZNBG-5561	This is a binary file with the numbers “20140315060646”.
EV7HHF-5561	From the content of the file it appears to be a graphic of the JPG format, if you open the graphic and view the content of the graphic is appears to be a black cat.
F3JVRX-5561	The jpg file of the suppressed black cat image with the extension changed to sys
FZVEJB-5561	The content of this file is shown to be JPEG picture data, as identified via the file signature. The content of the picture shows a black cat laying on what appears to be a wicker basket type material, with its front paws outstretched and mouth open.
G973T4-5561	It's a Black Cat
GJ39KG-5561	wincatyawn.sys
GYTEQP-5561	A black cat yawning
HQVXJW-5561	cat stretching
HUFQTD-5561	Black cat on back with mouth open tongue out with front paws in the air on some type of wicker
HW2LD2-5562	[Participant did not return results for this question.]
J84AQF-5562	A Black Cat Picture
JE9W33-5561	The picture depicts an apparent kitten, black in color, lying on its back with its arms outstretched, and its mouth open and tongue sticking out. The background behind the kitten appears to be some sort of wicker material, light brown in color.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22 - Examination Questions

WebCode Test	Response ** Inconsistencies not highlighted; No consensus achieved **
JGBUAC-5562	A black cat yawning
JJDU63-5561	Photo of a black cat yawning
JL32PY-5562	The file type is JPEG, and The file size is 756, 452 bytes. MAC Information is as follow. (1)Modification Time : 2018-05-25 15:12 (2)Access Time : 2023-03-06 08:19 (3)Creation Time : 2017-02-05 11:33
JLRZA6-5561	It is a small black kitten with arms extended and mouth wide open in a wicker basket.
JPKFX7-5561	Windows 10 Bluetooth device drivers
KR28JR-5562	JPEG - Picture of a black cat
KR4V3R-5561	A black cat, lying on their back, on a wicker chair, yawning, and with its front legs extended above its head.
KXRBW6-5562	Black kitten on a beige rattan seat laying on its back with front paws raised and mouth wide open
KZVDDT-5561	The file is in JPEG file interchange format (JFIF) as the file structure starts with 'FF D8 FF E0', and the content of the picture is a black cat with an opening mouth.
LDKC3B-5561	picture of a kitten
M9HYHY-5561	The file is an image (JPEG) of a black cat
MF4Q7B-5561	The header of this file is JFIF. A JFIF file is a bitmap graphic that uses JPEG compression.
MF8B24-5561	Yawning Cat with stretched out paws
NADTWE-5561	The file is a JPG file showing a black kitten on a wicker chair; its front legs/paws are extended and its mouth is open wide.
NE7TEF-5562	This file contains the Roland SoundCanvas Sound Set which is protected under the following copyright.
NTANM4-5561	This is a text file for the Roland SoundCanvas Sound Set. It discusses the Microsoft End User License Agreement.
NTZJR4-5561	Yawning Black Cat
P3ACZC-5561	.jpg of a black cat with paws stretched out with mouth open
P79FU7-5561	a black cat
P8ZNUA-5561	image of a black cat yawning
PFEMA7-5562	The file wincatyawn.sys is actually an image file looking at the content.
PFVN93-5561	JPEG of black kitten stretching and yawning

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22 - Examination Questions

** Inconsistencies not highlighted; No consensus achieved **

WebCode Test	Response
PLGGK2-5561	An image of a black cat (on wicker) yawning with tongue out.
PPMYM4-5562	JFIF(image) that shows a black cat
PTKDEZ-5562	A photo of a black cat with its hands up.
PUTRGY-5561	It's a Black Cat
PWJXV6-5561	Black kitten lying on its back while face up on wicker furniture, yawning with out stretched front legs.
Q2CFQV-5561	A black cat.
Q33NQX-5561	A picture of cat.
Q3RHY2-5561	Picture of a black cat yawning
QMR3Q2-5561	That's not .sysfile. Correctly signature is such as .jpg, .jpeg. jpe
QRJAR3-5561	Bluetooth A2DP Driver
QTHAXU-5561	Upside down black cat with open mouth.
RAK67E-5562	It's a picture of a cat yawning
RBBDCA-5562	Picture of cat yawning
RGH4EF-5562	Windows Executable
RRMUMV-5561	It is a JPG image of a black cat in a basket or wicker chair with its paws stretched up and its mouth wide open,
RRXTDK-5562	It's a black cat stretching.
RV3JKZ-5561	It's a Black Cat
TC4JAF-5562	Image of yawning black cat. File signature is JPG.
TCGEBD-5561	MIME type is image/jpeg, file seems to be a picture of a black cat on its back with legs/paws extended, that may be laying in a wicker basket or chair.
TEPC2R-5562	The file is an image (JPEG) of a black cat
TKFNZV-5561	The file is an image (JPEG) of a black cat
TNEXBT-5561	executable file related to Dropbox

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22 - Examination Questions

WebCode Test	Response ** Inconsistencies not highlighted; No consensus achieved **
TVF9MD-5562	JFIF file - JPEG of a black cat on back stretching/paws stretched out
TX22EP-5561	Picture of the cat, image/jpg
U3RQC6-5561	Picture of a black cat
UKBK6E-5561	Bluetooth driver file
URA8XZ-5561	a picture of a black cat
UVZCUQ-5562	Image depicting a cat
V4KY4K-5562	Image of a black cat meowing
VCE6WL-5561	a black cat on its back mouth open and front legs extended
VJH9N7-5561	The file is a .jpg image which is a picture of black cat laying on its back in a basket. The cat is yawning and has its front legs stretched.
VTZR3B-5561	A black kitten lay on its back with its paws raised, the kitten is yawning
VVVB8V-5561	Black cat with paws out
WC9E49-5561	It is an Executable system file
WD8DHB-5561	Picture of black cat (the cat is on its back with wide open mouth)
WK4CUH-5561	a black cat yawning
WNN64Y-5561	Black cat laying on back in a wicker chair with arms in air and open mouth with tongue hanging out.
WX2YKZ-5561	Not currently within scope of the lab.
WZGLVL-5562	black cat picture - .jpg file
XA2A8Z-5562	This is a file with an incorrect file extension. It is actually a JPG image of a Cat Yawning
XEVDXV-5561	Not in scope
XJ99G2-5562	This is a still image (JPEG) of a black cat stretching
XQ9B22-5561	Black cat yawning with front paws up.
XVDHZK-5562	[Participant did not return results for this question.]

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22 - Examination Questions

** Inconsistencies not highlighted; No consensus achieved **

WebCode Test	Response
XWDAB7-5561	The cat is spreading its paws and yawning.
XX78KX-5561	A black cat with their paws above their head pawning on a wicker background
Y63G92-5562	Copyright notification relating to Roland soundcanvas
YDJQ3P-5561	.dll files = Dynamic Link Library + resources for .dll (.dll.mui)
YPNENR-5562	picture of a black cat
ZPR26J-5561	The content of the file is an image of a black cat.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22 - Examination Questions

Question 22: Describe the content of the file identified in Question 21 (regular file in C:\Windows\System32\drivers with the earliest (oldest) ($STANDARD_INFORMATION Attribute) created time).

Consensus Result:

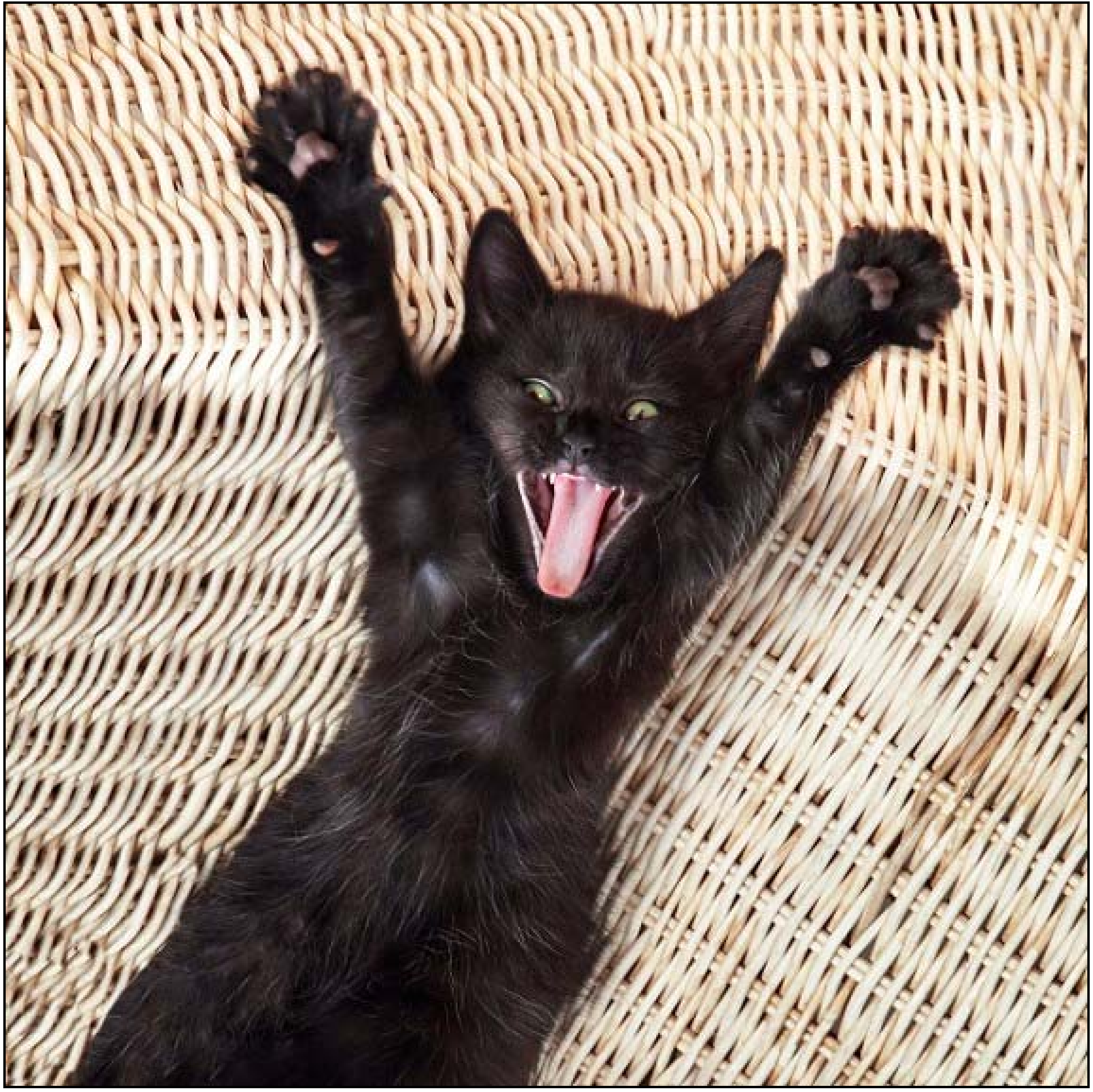
As of October 9, 2023, the text used for this question was deemed ambiguous or potentially misleading. The term “Regular” was ambiguous and further clarification provided in the related Question #21 should not have included the descriptor “Not aliased.” Consequently, no results are being highlighted as inconsistent by CTS. The manufacturer’s expected response of “A picture of a cat” and variations describing the same information was reported by a total of 118 participants (87%).

Expected Response Explanation:

wincatyawn.sys is a jpg photograph file containing an image of a black cat. Its file extension has been changed to .sys so it will not be displayed as an image by Windows or by a forensic tool if file signatures analysis has not been performed

Expected Response Illustration:

wincatyawn.sys



Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23 - Examination Questions

Question 23: What email client and version did the administrator install?

Manufacturer's Expected Response: Mozilla Thunderbird (x64 en-US) v. 102.8.0

WebCode Test	Response
2A9WQN-5561	privateemail v1.1
2P2VAR-5561	Mozilla Thunderbird 102.8.0
2PJFNF-5562	Mozilla Thunderbird (x64 en-US) 102.8.0
2VQ8RL-5562	Mozilla Thunderbird version 102.8.0
2ZFN6X-5561	Mozilla Thunderbird version 102.8.0
3CDK6E-5562	Mozilla Thunderbird 102.8.0 (x64 en-US)
3DPEPK-5561	Mozilla Thunderbird 102.8.0 (en-US)
3M9X4P-5561	Mozilla Thunderbird
42BM2N-5561	Mozilla Thunderbird, version: 102.8.0
48GFVJ-5561	Mozilla Thunderbird (x64 en-US) 102.8.0
4U7ZP2-5562	Mozilla Thunderbird, App Version: 102.8.0
649HZ6-5561	Mozilla Thunderbird, version 102.8.0
68RW46-5562	Mozilla Thunderbird (v102.8.0)
6DZZCR-5561	Mozilla Thunderbird v. 102.8.0
6MKCN6-5562	Mozilla Thunderbird and 102.8.0
6Q2RXW-5562	Mozilla Thunderbird version 102.8.0
6Q4JPC-5561	Mozilla Thunderbird v.102.8.0
6QKH3A-5562	Mozilla Thunderbird version 102.8.0
6TR3NP-5561	Mozilla Thunderbird (x64 en-US) 102.8.0
72ZUTD-5561	Mozilla Thunderbird (x64 en-US) Version 102.8.0
78PAK7-5562	Mozilla Thunderbird (x64 en-US) v.102.8.0

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23 - Examination Questions

WebCode Test	Response
7JUP4F-5561	thunderbird
7PQ8PM-5562	Mozilla Thunderbird version 102.8.0
7XZLMH-5562	Mozilla Thunderbird version 102.8.0
82VWX9-5562	Mozilla Thunderbird Version 102.8.0
83AEYT-5562	Mozilla Thunderbird (x64 en-US) version 102.8.0
8CB97J-5561	Mozilla Thunderbird (x64 en-US) Version 102.8.0
8LJ9TK-5561	Mozilla Thunderbird (x64 en-US) v102.8.0
96TUNQ-5561	Mozilla Thunderbird (x64 en-US) / 102.8.0
98ZV8C-5561	Mozilla Thunderbird 102.8.0
99QBZK-5562	Thunderbird version 102.8.0
9AJ8JM-5561	Mozilla Thunderbird 102.8.0
9J9Q8U-5562	Mozilla Thunderbird (x64 en-US), Version 102.8.0
A8QHYB-5562	Thunderbird 102.8.0
A8VQBZ-5561	Mozilla Thunderbird (x64 en-US) v. 102.8.0
ABK3AJ-5561	NOT IN SCOPE
ACTERK-5561	Not in Scope
ADYU2Y-5562	Mozilla Thunderbird 102.8.0
AKG6BT-5562	Mozilla Thunderbird version 102.8.0
AM94QQ-5561	Mozilla Thunderbird 102.8.0
BFKZWF-5562	Mozilla Thunderbird (x64 en-US) Version : 102.8.0
BQRG78-5561	Mozilla Thunderbird (version 102.8.0)
C4LMC9-5562	Thunderbird 102.8.0

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23 - Examination Questions

WebCode Test	Response
C897D8-5561	Mozilla Thunderbird (x64 en-US) version 102.8.0
CF2CBE-5562	Mozilla Thunderbird (x64 en-US), v102.8.0
CKAXYB-5561	Mozilla Thunderbird 102.8.0 (en-US)
CP6N6M-5561	Mozilla Thunderbird (x64 en-US) Version 102.8.0
D7PUVD-5561	Mozilla Thunderbird (x64 en-US)
DB6AM4-5561	Mozilla Thunderbird v102.8.0 (x64 en-US)
DGVH9K-5561	Mozilla Thunderbird v102.8.0
DXVP3C-5562	Thunderbird v. 102.8.0
E2RHRZ-5562	Mozilla Thunderbird (en-US) v102.8.0
E4ZNBG-5561	Mozilla Thunderbird (x64 en-US) Version 102.8.0
EV7HHF-5561	Mozilla Thunderbird (x64 en-US) 102.8.0
F3JVRX-5561	Mozilla Thunderbird (x64 en-US), Version 102.8.0
FZVEJB-5561	Mozilla Thunderbird version 102.8.0
G973T4-5561	Mozilla Thunderbird (x64 en-US) , Version : 102.8.0
GJ39KG-5561	Mozilla Thunderbird 102.8.0
GYTEQP-5561	Thunderbird 102.8.0
HQVXJW-5561	Mozilla Thunderbird (x64 en-US) 102.8.0
HUFQTD-5561	Mozilla Thunderbird v. 102.8.0
HW2LD2-5562	[Participant did not return results for this question.]
J84AQF-5562	Mozilla Thunderbird (x64 en-US) 102.8.0
JE9W33-5561	Mozilla Thunderbird 102.8.0
JGBUAC-5562	Mozilla Thunderbird 102.8.0

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23 - Examination Questions

WebCode Test	Response
JJDU63-5561	Thunderbird 102.8.0
JL32PY-5562	Thunderbird v.102.8.0
JLRZA6-5561	Mozilla Thunderbird version 102.8.0
JPKFX7-5561	Mozilla thunderbird 102.8.0
KR28JR-5562	Mozilla Thunderbird (x64 en-US) v.102.8
KR4V3R-5561	Mozilla Thunderbird 102.8.0 (x64 en-US)
KXRBW6-5562	Mozilla Thunderbird (x64 en-US)
KZVDDT-5561	Mozilla Thunderbird (x64 en-US) V.102.8.0
LDKC3B-5561	Mozilla Thunderbird 102.8.0
M9HYHY-5561	Mozilla Thunderbird (x64 en-US) version 102.8.0
MF4Q7B-5561	Mozilla Thunderbird (x64 en-US), version 102.8.0
MF8B24-5561	Mozilla Thunderbird V 102.8.0
NADTWE-5561	Thunderbird 102.8.0
NE7TEF-5562	Mozilla Thunderbird and 102.8.0
NTANM4-5561	Mozilla Thunderbird v.102.8.0
NTZJR4-5561	Mozilla Thunderbird
P3ACZC-5561	Mozilla Thunderbird 102.8.0
P79FU7-5561	Mozilla Thunderbird (x64 en-US) 102.8.0
P8ZNUA-5561	Thunderbird v. 102.8.0
PFEMA7-5562	Mozilla Thunderbird (x64 en-US), 102.8.0
PFVN93-5561	Thunderbird 102.8.0
PLGGK2-5561	Thunderbird 102.8.0

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23 - Examination Questions

WebCode Test	Response
PPMYM4-5562	Mozilla Thunderbird (x64 en-US) 102.8.0
PTKDEZ-5562	Mozilla Thunderbird 102.8.0
PUTRGY-5561	Mozilla Thunderbird (x64 en-US) , Version : 102.8.0
PWJXV6-5561	Mozilla Thunderbird 102.8.0
Q2CFQV-5561	Mozilla Thunderbird (x64 en-US) 102.8.0
Q33NQX-5561	Mozilla Thunderbird 102.8.0
Q3RHY2-5561	Mozilla Thunderbird Version: 102.8.0
QMR3Q2-5561	Thunderbird 91.6.0
QRJAR3-5561	Thunderbird
QTHAXU-5561	Mozilla Thunderbird, version 102.8.0
RAK67E-5562	Monzilla Thunderbird
RBBDCA-5562	Thunderbird v102.8.0
RGH4EF-5562	Mozilla Thunderbird (x64 en-US) v 102.8.0
RRMUMV-5561	Mozilla Thunderbird Version 102.8.0
RRXTDK-5562	Mozilla Thunderbird (x64 en-US) v.102.8.0
RV3JKZ-5561	Mozilla Thunderbird (x64 en-US) , Version : 102.8.0
TC4JAF-5562	Mozilla Thunderbird (x64 en-US) 102.8.0
TCGEBD-5561	Mozilla Thunderbird v102.8.0
TEPC2R-5562	Mozilla Thunderbird (x64 en-US) version 102.8.0
TKFNZV-5561	Mozilla Thunderbird (x64 en-US) version 102.8.0
TNEXBT-5561	Mozilla Thunderbird
TVF9MD-5562	Mozilla Thunderbird 102.8.0

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23 - Examination Questions

WebCode Test	Response
TX22EP-5561	Mozilla Thunderbird (x64 en-US) 102.8.0
U3RQC6-5561	Dropbox Version 1.3.733.1
UKBK6E-5561	Mozilla Thunderbird 102.8.0 (x64 en-US)
URA8XZ-5561	Mozilla Thunderbird (x64 en-US) - version 102.8.0
UVZCUQ-5562	Mozilla Thunderbird Version 102.8.0
V4KY4K-5562	Mozilla Thunderbird version 102.8.0
VCE6WL-5561	Mozilla Thunderbird (x64 en-US) v.102.8.0
VJH9N7-5561	Thunderbird version 102.8.0
VTZR3B-5561	Mozilla Thunderbird (x64 en-US)
VVVB8V-5561	Mozilla Thunderbird (x64 en-US) version 102.8.0
WC9E49-5561	Mozilla Thunderbird 102.8.0
WD8DHB-5561	Mozilla Thunderbird 102.8.0
WK4CUH-5561	Mozilla Thunderbird v.102.8.0
WNN64Y-5561	Mozilla Thunderbird v. 102.8.0
WX2YKZ-5561	Not currently within scope of the lab.
WZGLVL-5562	Mozilla Thunderbird (x64 en-US) 102.8.0
XA2A8Z-5562	Mozilla Thunderbird 102.8.0
XEVDXV-5561	Not in scope
XJ99G2-5562	Mozilla Thunderbird (x64 en-US) version 102.8.0
XQ9B22-5561	Mozilla Thunderbird (x64 en-US) version 102.8.0
XVDHZK-5562	[Participant did not return results for this question.]
XWDAB7-5561	Mozilla Thunderbird (x64 en-US) 102.8.0

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23 - Examination Questions

WebCode Test	Response
XX78KX-5561	Mozilla Thunderbird (x64 en-US) v. 102.8.0
Y63G92-5562	Mozilla Thunderbird(x64 en-us)
YDJQ3P-5561	Thunderbird v. 102.8.0
YPNENR-5562	Mozilla Thunderbird (x64 en-US), v102.8.0
ZPR26J-5561	Mozilla Thunderbird v102.8.0

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23 - Examination Questions

Question 23: What email client and version did the administrator install?

Consensus Result:

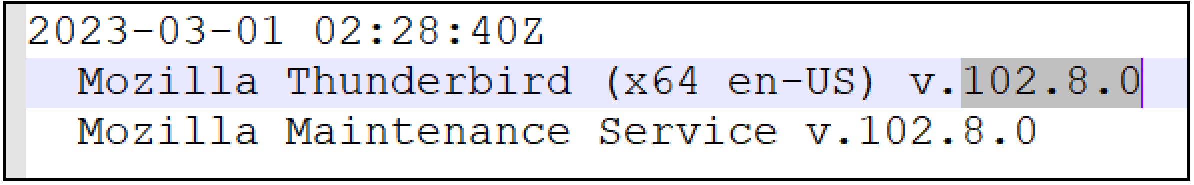
Mozilla Thunderbird (x64 en-US) v. 102.8.0

Expected Response Explanation:

Installed applications are recorded in the SOFTWARE Registry Hive in the Microsoft\Windows\CurrentVersion\Uninstall key

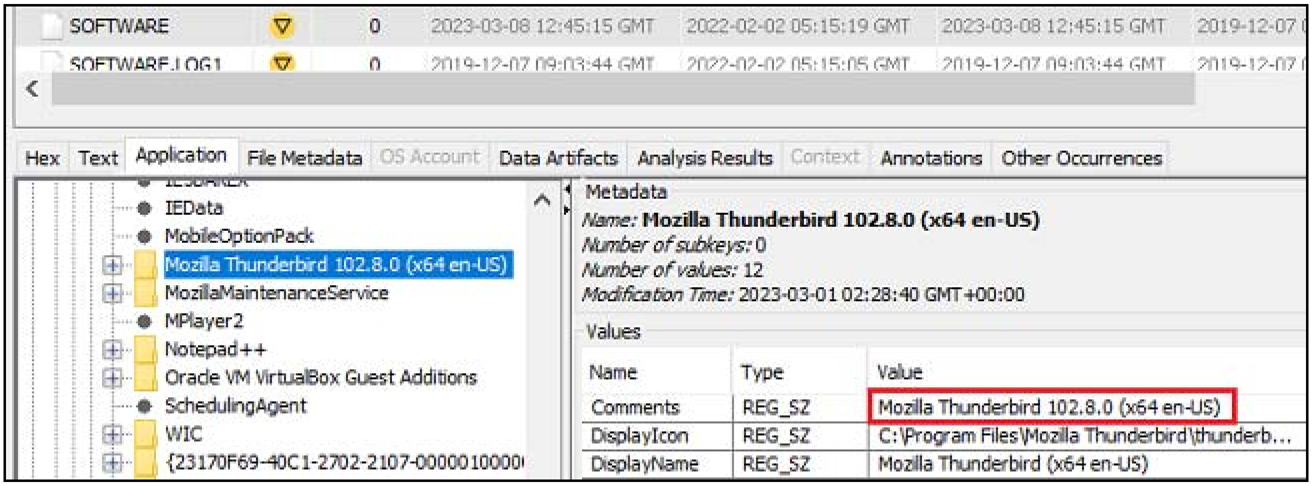
Expected Response Illustration:

RegRipper parse of SOFTWARE Microsoft\Windows\CurrentVersion\Uninstall key



```
2023-03-01 02:28:40Z
  Mozilla Thunderbird (x64 en-US) v.102.8.0
  Mozilla Maintenance Service v.102.8.0
```

Autopsy view of SOFTWARE Microsoft\Windows\CurrentVersion\Uninstall key



SOFTWARE	0	2023-03-08 12:45:15 GMT	2022-02-02 05:15:19 GMT	2023-03-08 12:45:15 GMT	2019-12-07
SOFTWARE.LOG1	0	2019-12-07 09:03:44 GMT	2022-02-02 05:15:05 GMT	2019-12-07 09:03:44 GMT	2019-12-07

Metadata

Name: **Mozilla Thunderbird 102.8.0 (x64 en-US)**
Number of subkeys: 0
Number of values: 12
Modification Time: 2023-03-01 02:28:40 GMT +00:00

Values

Name	Type	Value
Comments	REG_SZ	Mozilla Thunderbird 102.8.0 (x64 en-US)
DisplayIcon	REG_SZ	C:\Program Files\Mozilla Thunderbird\thunderb...
DisplayName	REG_SZ	Mozilla Thunderbird (x64 en-US)

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions

Question 24: Provide the email addresses for the two email accounts configured in the user installed IMAP email client for user David Lightman.

Manufacturer's Expected Response: david.lightman75@outlook.com and admin@clotildes.institute and/or admin@st.clotildes.institute

WebCode Test	Response ** Inconsistencies not highlighted; No consensus achieved **
2A9WQN-5561	mail.privateemail.com and outlook.office365.com
2P2VAR-5561	admin@st.clotildes.institue, david.lightman75@outlook.com
2PJFNF-5562	david.lightman75@outlook.com stephen.falken@stclotildes.institute
2VQ8RL-5562	david.lightman75@outlook.com
2ZFN6X-5561	David.lightman75@outlook.com, Stephen.falken@stclotildes.institute
3CDK6E-5562	david.lightman75@outlook.com and admin@st.clotildes.institute
3DPEPK-5561	david.lightman75@outlook.com and Admin@clotildes.institute
3M9X4P-5561	admin@st.clotildes.institute and david.lightman75@outlook.com
42BM2N-5561	admin@clotildes.institute, David.Lightman75@outlook.com
48GFVJ-5561	admin@clotildes.institute and david.lightman75@outlook.com
4U7ZP2-5562	david.lightman75@outlook.com; admin@clotildes.institute
649HZ6-5561	admin@st.clotildes.institute, david.lightman75@outlook.com
68RW46-5562	admin@clotildes.institute & david.lightman75@outlook.com
6DZZCR-5561	admin@st.clotildes.institute ; david.lightman75@outlook.com
6MKCN6-5562	david.lightman75@outlook.com
6Q2RXW-5562	admin@clotildes.institute, david.lightman75@outlook.com
6Q4JPC-5561	admin@clotildes.institute, david.lightman75@outlook.com
6QKH3A-5562	admin@st.clotildes.institute, admin@clotildes.institute
6TR3NP-5561	RosarioSIS <admin@clotildes.institute> and david.lightman75@outlook.com
72ZUTD-5561	admin@clotildes.institute and david.lightman75@outlook.com

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions

WebCode Test	Response ** Inconsistencies not highlighted; No consensus achieved **
78PAK7-5562	david.lightman75@outlook.com; admin@clotildes.institute
7JUP4F-5561	admin@clotildes.institute admin@st.clotildes.institute
7PQ8PM-5562	david.lightman75@outlook.com and admin@clotildes.institute
7XZLMH-5562	david.lightman75@outlook.com and admin@clotildes.institute
82VWX9-5562	admin@st.clotildes.institute, david.lightman75@outlook.com
83AEYT-5562	admin@clotildes.institute, david.lightman75@outlook.com
8CB97J-5561	david.lightman75@outlook.com; admin@clotildes.institute
8LJ9TK-5561	admin@clotildes.institute, david.lightman75@outlook.com
96TUNQ-5561	david.lightman75@outlook.com / admin@clotildes.institute
98ZV8C-5561	david.lightman75@outlook.com and admin@clotildes.institute@mail.privateemail.com
99QBZK-5562	admin@clotildes.institute david.lightman75@outlook.com
9AJ8JM-5561	admin@clotildes.institute, admin@st.clotildes.institute
9J9Q8U-5562	admin@clotildes.institute and david.lightman75@outlook.com
A8QHYB-5562	david.lightman75@outlook.com, admin@clotildes.institute
A8VQBZ-5561	david.lightman75@outlook.com, admin@clotildes.institute
ABK3AJ-5561	NOT IN SCOPE
ACTERK-5561	Not in Scope
ADYU2Y-5562	admin@st.clotildes.institute admin@clotildes.institute
AKG6BT-5562	david.lightman75@outlook.com and admin@clotildes.institute
AM94QQ-5561	admin@st.clotildes.institute and david.lightman75@outlook.com
BFKZWF-5562	david.lightman75@outlook.com admin@clotildes.institute
BQRG78-5561	admin@clotildes.institute & david.lightman75@outlook.com

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions

WebCode Test	Response ** Inconsistencies not highlighted; No consensus achieved **
C4LMC9-5562	david.lightman75@outlook.com and admin@clotildes.institute
C897D8-5561	david.lightman75@outlook.com, francismilligan599@gmail.com
CF2CBE-5562	david.lightman75@outlook.com, admin@st.clotildes.institute
CKAXYB-5561	admin@clotildes.institute david.lightman75@outlook.com
CP6N6M-5561	david.lightman75@outlook.com; admin@clotildes.institute
D7PUVD-5561	Mail.privateemail.com, Outlook.office365.com
DB6AM4-5561	admin@clotildes.institute david.lightman75@outlook.com
DGVH9K-5561	david.lightman75@outlook.com and admin@clotildes.institute
DXVP3C-5562	david.lightman75@outlook.com and admin@st.clotildes.institute
E2RHRZ-5562	david.lightman75@outlook.com, stephen.falken@stclotildes.institute
E4ZNBG-5561	David.lightman75@outlook.com admin@st.clotildes.institue
EV7HHF-5561	david.lightman75@outlook.com admin@clotildes.institute
F3JVRX-5561	david.lightman75@outlook.com stephen.falken@stclotildes.institute
FZVEJB-5561	admin@stclotildes.institute & david.lightman75@outlook.com
G973T4-5561	david.lightman75@outlook.com admin@st.clotildes.institute
GJ39KG-5561	admin@clotildes.institute / david.lightman75@outlook.com
GYTEQP-5561	david.lightman75@outlook.com and admin@st.clotildes.institute
HQVXJW-5561	david.lightman75@outlook.com, stephen.falken@stclotildes.institute
HUFQTD-5561	david.lightman75@outlook.com admin@clotildes.institute
HW2LD2-5562	[Participant did not return results for this question.]
J84AQF-5562	Einstitute@mail.privateemail.com / David.lightman75@outlook.com
JE9W33-5561	admin@clotildes.institute, david.lightman75@outlook.com

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions

WebCode Test	Response ** Inconsistencies not highlighted; No consensus achieved **
JGBUAC-5562	david.lightman75@outlook.com admin@clotildes.institute
JJDU63-5561	admin@clotildes.institute and david.lightman75@outlook.com
JL32PY-5562	david.lightman75@outlook.com
JLRZA6-5561	david.lightman75@outlook.com and admin@clotildes.institute
JPKFX7-5561	david.lightman75@outlook.com admin@clotildes.institute
KR28JR-5562	david.lightman75@outlook.com & admin@clotildes.institute
KR4V3R-5561	david.lightman75@outlook.com stephen.falken@stclotildes.institute
KXRBW6-5562	Mail.privateemail.com, Outlook.office365.com
KZVDDT-5561	david.lightman75@outlook.com, jennymack16@outlook.com
LDKC3B-5561	admin@st.clotildes.insitute, and david.lightman75@outlook.com
M9HYHY-5561	mail.privateemail.com admin@clotildes.institute outlook.office365.com david.lightman75@outlook.com
MF4Q7B-5561	david.lightman75@outlook.com; jennymack16@outlook.com
MF8B24-5561	david.lightman75@outlook.com, admin@st.clotildes.institute
NADTWE-5561	admin@clotildes.institute and david.lightman75@outlook.com
NE7TEF-5562	david.lightman75@outlook.com
NTANM4-5561	david.lightman75@outlook.com and admin@st.clotildes.institute
NTZJR4-5561	david.lightman75@outlook.com, admin@st.clotildes.institute
P3ACZC-5561	david.lightman75@outlook.com and admin@clotildes.institute
P79FU7-5561	david.lightman75@outlook.com & admin@clotildes.institute
P8ZNUA-5561	david.lightman75@outlook.com admin@st.clotildes.institute
PFEMA7-5562	admin@clotildes.institute, david.lightman75@outlook.com
PFVN93-5561	david.lightman75@outlook.com; admin@clotildes.institute

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions

** Inconsistencies not highlighted; No consensus achieved **

WebCode Test	Response
PLGGK2-5561	david.lightman75@outlook.com admin@clotildes.institute
PPMYM4-5562	david.lightman75@outlook.com, admin@clotildes.institute
PTKDEZ-5562	admin@clotildes.institute
PUTRGY-5561	david.lightman75@outlook.com admin@clotildes.institute
PWJXV6-5561	david.lightman75@outlook.com, RossarioSIS<admin@clotildes.institute>
Q2CFQV-5561	admin@clotildes.institute, david.lightman75@outlook.com
Q33NQX-5561	david.lightman75@outlook.com, admin@clotildes.institute
Q3RHY2-5561	admin@clotildes.institute and david.lightman75@outlook.com
QMR3Q2-5561	david.lightman75@outlook.com, francismilligan599@gmail.com
QRJAR3-5561	admin@clotildes.institute, david.lightman75@outlook.com
QTHAXU-5561	David.lightman@outlook.com, admin@clotides.institute
RAK67E-5562	david.lightman75@outlook.com, admin@clotildes.institute
RBBDCA-5562	david.lightman75@outlook.com & admin@st.clotildes.institute
RGH4EF-5562	admin@clotildes.institute david.lightman75@outlook.com
RRMUMV-5561	admin@st.clotildes.institute admin@clotildes.institute
RRXTDK-5562	"admin@st.clotildes.institute" <admin@clotildes.institute> and david.lightman75@outlook.com
RV3JKZ-5561	david.lightman75@outlook.com admin@st.clotildes.institute
TC4JAF-5562	"david.lightman75@outlook.com" and "admin@clotildes.institute"
TCGEBD-5561	admin@clotildes.institute david.lightman75@outlook.com
TEPC2R-5562	(mail.privateemail.com admin@clotildes.institute) (outlook.office365.com david.lightman75@outlook.com)
TKFNZV-5561	(mail.privateemail.com admin@clotildes.institute) (outlook.office365.com david.lightman75@outlook.com)
TNEXBT-5561	david.lightman75@outlook.com

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions

** Inconsistencies not highlighted; No consensus achieved **

WebCode Test	Response
TVF9MD-5562	david.lightman75@outlook.com & admin@st.clotildes.institute
TX22EP-5561	david.lightman75@outlook.com, admin@clotildes.institue
U3RQC6-5561	admin@st.clotildes.institute, admin@clotildes.institute
UKBK6E-5561	david.lightman75@outlook.com, admin@clotildes.institute
URA8XZ-5561	david.lightman75@outlook.com, admin@st.clotildes.institute
UVZCUQ-5562	david.lightman75@outlook.com admin@clotildes.institute
V4KY4K-5562	"admin@clotildes.institute" & "david.lightman75@outlook.com"
VCE6WL-5561	david.lightman75@outlook.com and admin@clotildes.institute
VJH9N7-5561	admin@clotildes.institute david.lightman75@outlook.com
VTZR3B-5561	david.lightman75@outlook.com, admin@st.clotildes.institute
VVVB8V-5561	admin@st.clotildes.institute and david.lightman75@outlook.com
WC9E49-5561	francismilligan599@gmail.com, david.lightman75@outlook.com
WD8DHB-5561	david.lightman75@outlook.com; admin@st.clotildes.institute
WK4CUH-5561	david.lightman75@outlook.com admin@clotildes.institute
WNN64Y-5561	David.lightman75@outlook.com admin@clotildes.institute
WX2YKZ-5561	Not currently within scope of the lab.
WZGLVL-5562	david.lightman75@outlook.com, admin%40clotildes.institute@mail.privateemail.com
XA2A8Z-5562	david.lightman75@outlook.com admin@clotildes.institute
XEVDXV-5561	Not in scope
XJ99G2-5562	Admin@clotildes.institute & David.lightman75@outlook.com
XQ9B22-5561	admin@clotildes.institute and david.lightman75@outlook.com
XVDHZK-5562	[Participant did not return results for this question.]

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions

WebCode Test	Response ** Inconsistencies not highlighted; No consensus achieved **
XWDAB7-5561	david.lightman75@outlook.com / admin@clotildes.institute
XX78KX-5561	david.lightman75@outlook.com and admin@st.clotildes.institute
Y63G92-5562	jennymack16@outlook.com and david.lightman75@outlook.com
YDJQ3P-5561	david.lightman75@outlook.com and admin@st.clotildes.institute
YPNENR-5562	david.lightman75@outlook.com, admin@st.clotildes.institute
ZPR26J-5561	david.lightman75@outlook.com and admin@st.clotildes.institute

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions

Question 24: Provide the email addresses for the two email accounts configured in the user installed IMAP email client for user David Lightman.

Consensus Result:

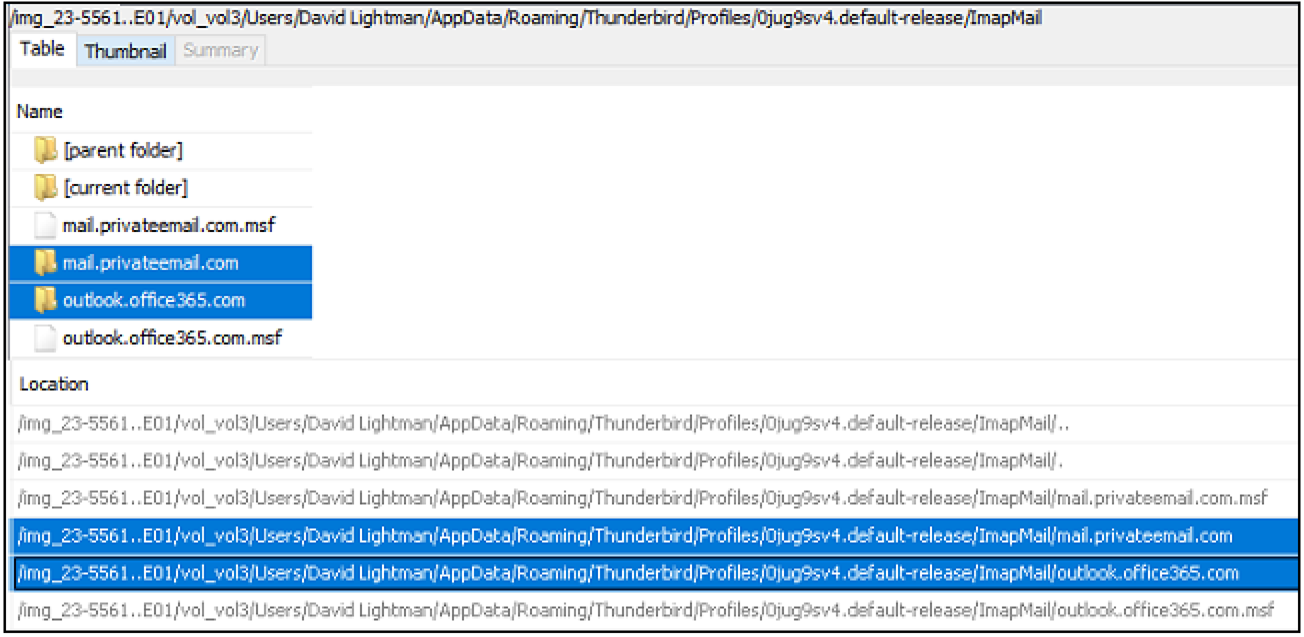
A consensus was not achieved for this question. This question was looking for two email accounts. A total of 119 participants (92%) reported the expected email address: david.lightman75@outlook.com. However, only 95 of those participants reported the second email address: admin@clotildes.institute or admin@st.clotildes.institute, for an overall total of 73% of participants reporting the two expected emails.

Expected Response Explanation:

Thunderbird stores IMAP email under the user's profile at C:\Users\David Lightman\AppData\Roaming\Thunderbird\Profiles\0jug9sv4.default-release\ImapMail\. There are two accounts located in this directory one for outlook.office365.com, david.lightman75@outlook.com; and one for mail.privateemail.com, admin@clotildes.institute or admin@st.clotildes.institute.

Expected Response Illustration:

Autopsy view of Thunderbird IMAP directory



/img_23-5561..E01/vol_vol3/Users/David Lightman/AppData/Roaming/Thunderbird/Profiles/0jug9sv4.default-release/ImapMail

Name
[parent folder]
[current folder]
mail.privateemail.com.msf
mail.privateemail.com
outlook.office365.com
outlook.office365.com.msf

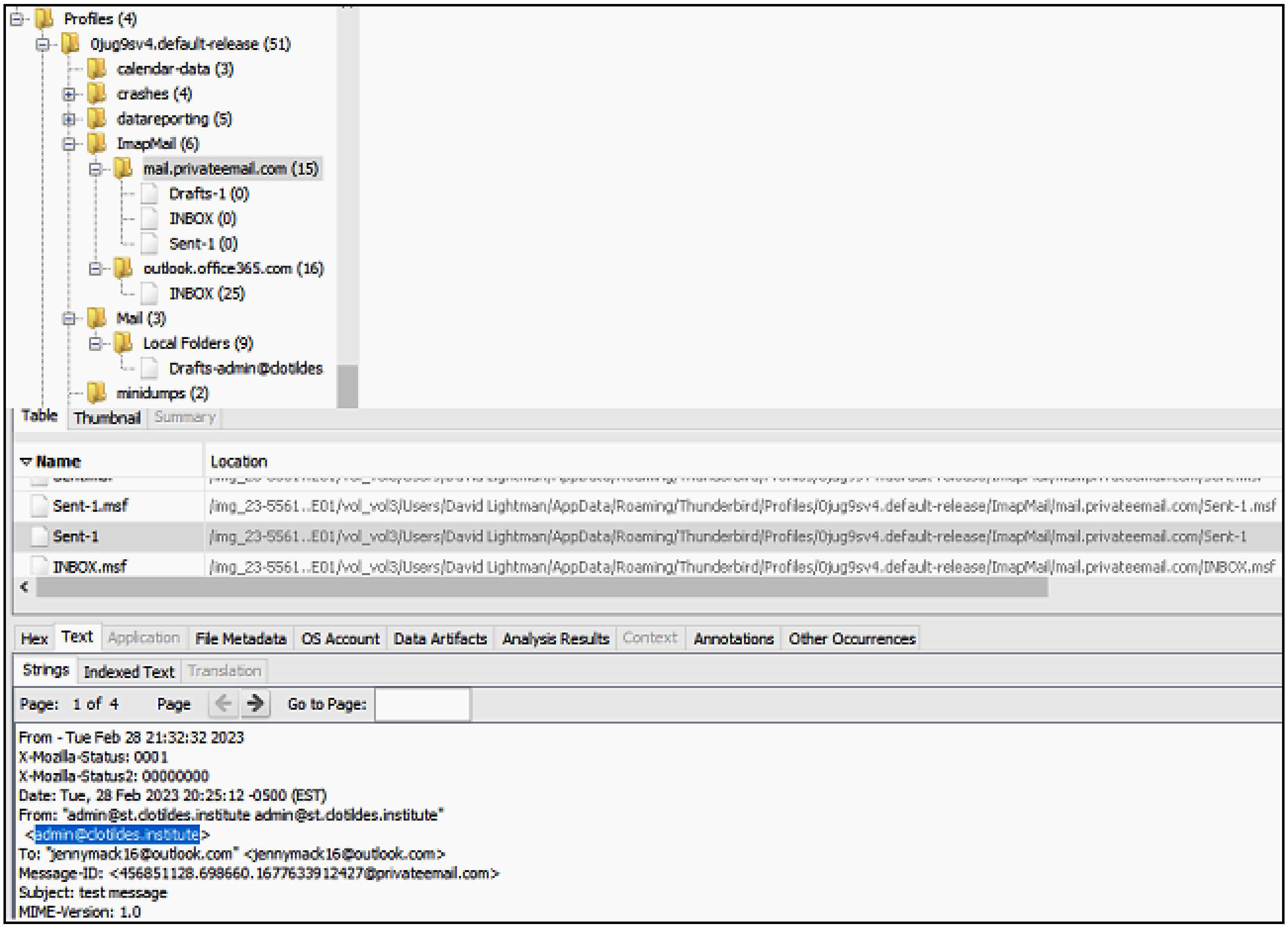
Location
/img_23-5561..E01/vol_vol3/Users/David Lightman/AppData/Roaming/Thunderbird/Profiles/0jug9sv4.default-release/ImapMail/..
/img_23-5561..E01/vol_vol3/Users/David Lightman/AppData/Roaming/Thunderbird/Profiles/0jug9sv4.default-release/ImapMail/.
/img_23-5561..E01/vol_vol3/Users/David Lightman/AppData/Roaming/Thunderbird/Profiles/0jug9sv4.default-release/ImapMail/mail.privateemail.com.msf
/img_23-5561..E01/vol_vol3/Users/David Lightman/AppData/Roaming/Thunderbird/Profiles/0jug9sv4.default-release/ImapMail/mail.privateemail.com
/img_23-5561..E01/vol_vol3/Users/David Lightman/AppData/Roaming/Thunderbird/Profiles/0jug9sv4.default-release/ImapMail/outlook.office365.com
/img_23-5561..E01/vol_vol3/Users/David Lightman/AppData/Roaming/Thunderbird/Profiles/0jug9sv4.default-release/ImapMail/outlook.office365.com.msf

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions

IMAP folder containing messages from admin@clotildes.institute



- Profiles (4)
  - 0jug9sv4.default-release (51)
    - calendar-data (3)
    - crashes (4)
    - datareporting (5)
    - ImapMail (6)
      - mail.privateemail.com (15)
        - Drafts-1 (0)
        - INBOX (0)
        - Sent-1 (0)
      - outlook.office365.com (16)
        - INBOX (25)
    - Mail (3)
      - Local Folders (9)
        - Drafts-admin@clotildes
    - minidumps (2)

Name	Location
Sent-1.msf	/img_23-5561..E01/vol_vol3/Users/David Lightman/AppData/Roaming/Thunderbird/Profiles/0jug9sv4.default-release/ImapMail/mail.privateemail.com/Sent-1.msf
Sent-1	/img_23-5561..E01/vol_vol3/Users/David Lightman/AppData/Roaming/Thunderbird/Profiles/0jug9sv4.default-release/ImapMail/mail.privateemail.com/Sent-1
INBOX.msf	/img_23-5561..E01/vol_vol3/Users/David Lightman/AppData/Roaming/Thunderbird/Profiles/0jug9sv4.default-release/ImapMail/mail.privateemail.com/INBOX.msf

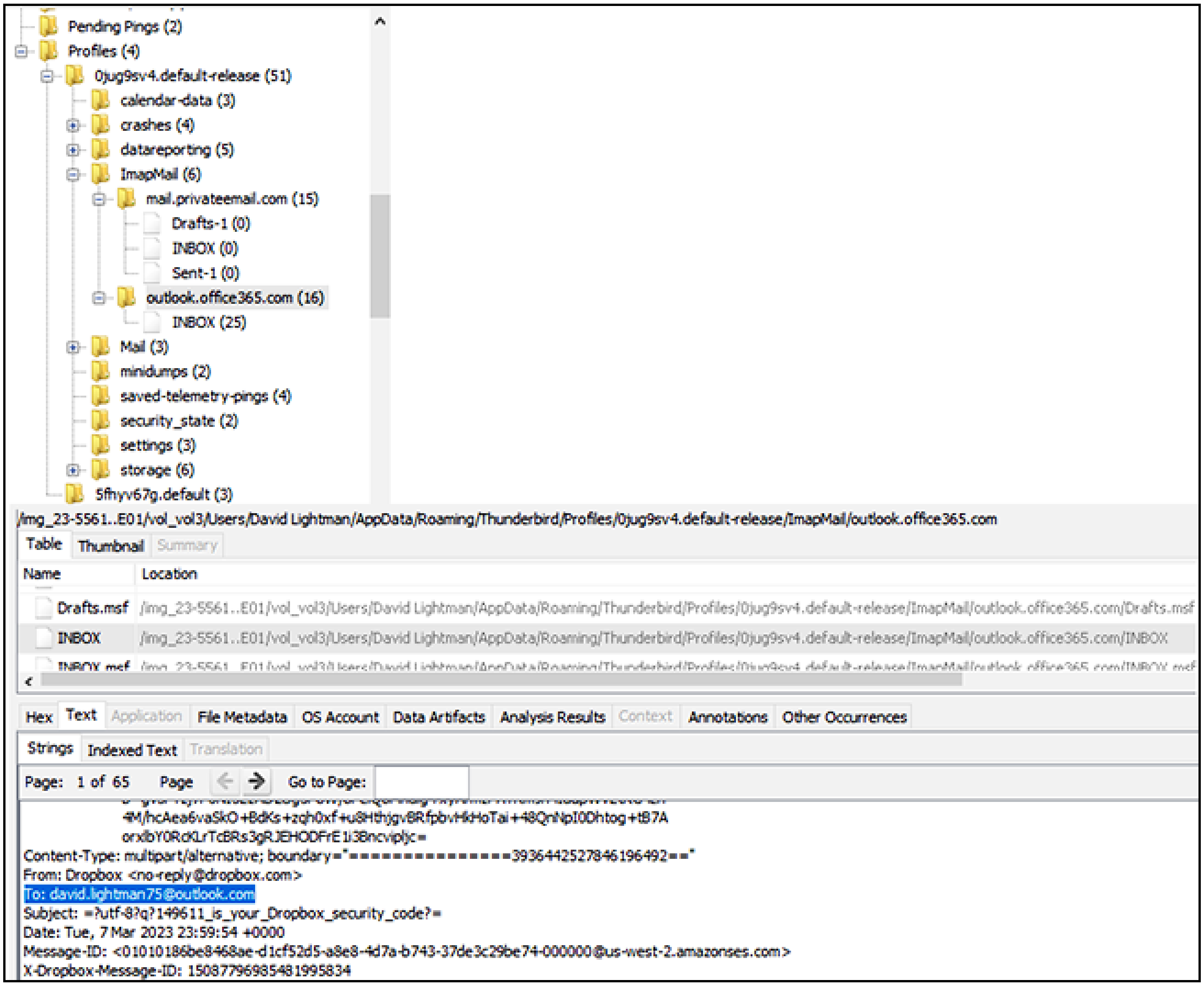
```
From - Tue Feb 28 21:32:32 2023
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
Date: Tue, 28 Feb 2023 20:25:12 -0500 (EST)
From: "admin@st.clotildes.institute admin@st.clotildes.institute"
 <admin@clotildes.institute>
To: "jennymack16@outlook.com" <jennymack16@outlook.com>
Message-ID: <456851128.698660.1677633912427@privateemail.com>
Subject: test message
MIME-Version: 1.0
```

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions

IMAP folder containing messages to David.lightman75@outlook.com



/img_23-5561..E01/vol_vol3/Users/David Lightman/AppData/Roaming/Thunderbird/Profiles/0jug9sv4.default-release/ImapMail/outlook.office365.com

Name	Location
Drafts.msf	/img_23-5561..E01/vol_vol3/Users/David Lightman/AppData/Roaming/Thunderbird/Profiles/0jug9sv4.default-release/ImapMail/outlook.office365.com/Drafts.msf
INBOX	/img_23-5561..E01/vol_vol3/Users/David Lightman/AppData/Roaming/Thunderbird/Profiles/0jug9sv4.default-release/ImapMail/outlook.office365.com/INBOX
INBOX.msf	/img_23-5561..E01/vol_vol3/Users/David Lightman/AppData/Roaming/Thunderbird/Profiles/0jug9sv4.default-release/ImapMail/outlook.office365.com/INBOX.msf

```
        4M/hcAea6vaSkO+BdKs+zqh0xf+u8HthjgvBRfpbvHkHoTai+48QnNpI0Dhtog+tB7A
        orxlbY0RdKLrTcBRs3gRJEHODFrE1i38ncviplјc=
Content-Type: multipart/alternative; boundary="===============3936442527846196492=="
From: Dropbox <no-reply@dropbox.com>
To: david.lightman75@outlook.com
Subject: =?utf-8?q?149611_is_your_Dropbox_security_code?=
Date: Tue, 7 Mar 2023 23:59:54 +0000
Message-ID: <01010186be8468ae-d1cf52d5-a8e8-4d7a-b743-37de3c29be74-000000@us-west-2.amazonses.com>
X-Dropbox-Message-ID: 1508779698548199583 4
```

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25 - Examination Questions

Question 25: Provide the email address of the person with whom user David Lightman communicated with about changing grades.

Manufacturer's Expected Response: Email Address: jennymack16@outlook.com
Name of Person: Jennifer Mack

WebCode Test	Response
2A9WQN-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
2P2VAR-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
2PJFNF-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
2VQ8RL-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
2ZFN6X-5561	Email Address: jennymack16@outlook.com , Name of Person: Jennifer Mack
3CDK6E-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
3DPEPK-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
3M9X4P-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
42BM2N-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
48GFVJ-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
4U7ZP2-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
649HZ6-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
68RW46-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
6DZZCR-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
6MKCN6-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
6Q2RXW-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
6Q4JPC-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
6QKH3A-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
6TR3NP-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25 - Examination Questions

WebCode Test	Response
72ZUTD-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
78PAK7-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
7JUP4F-5561	Email Address: jennymack16@stclotildes.institute, Name of Person: jenny mack
7PQ8PM-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
7XZLMH-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
82VWX9-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
83AEYT-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
8CB97J-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
8LJ9TK-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
96TUNQ-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
98ZV8C-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
99QBZK-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
9AJ8JM-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
9J9Q8U-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
A8QHYB-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
A8VQBZ-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
ABK3AJ-5561	Email Address: NOT IN SCOPE, Name of Person: NOT IN SCOPE
ACTERK-5561	Email Address: Not in Scope, Name of Person: Not in Scope
ADYU2Y-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
AKG6BT-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
AM94QQ-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25 - Examination Questions

WebCode Test	Response
BFKZWF-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
BQRG78-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
C4LMC9-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
C897D8-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
CF2CBE-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
CKAXYB-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
CP6N6M-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
D7PUVD-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
DB6AM4-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
DGVH9K-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
DXVP3C-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
E2RHRZ-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
E4ZNBG-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
EV7HHF-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
F3JVRX-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
FZVEJB-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
G973T4-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
GJ39KG-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
GYTEQP-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
HQVXJW-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
HUFQTD-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25 - Examination Questions

WebCode Test	Response
HW2LD2-5562	[Participant did not return results for this question.]
J84AQF-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
JE9W33-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
JGBUAC-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
JJDU63-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
JL32PY-5562	Email Address: jennymack16@outlook.com, Name of Person: Jenny Mack
JLRZA6-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
JPKFX7-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
KR28JR-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
KR4V3R-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
KXRBW6-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
KZVDDT-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
LDKC3B-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
M9HYHY-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
MF4Q7B-5561	Email Address: jennymack16@outlook.com, Name of Person: Jenny Mack
MF8B24-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
NADTWE-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
NE7TEF-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
NTANM4-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
NTZJR4-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
P3ACZC-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25 - Examination Questions

WebCode Test	Response
P79FU7-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
P8ZNUA-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
PFEMA7-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
PFVN93-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
PLGGK2-5561	Email Address: jennymack16@outlook.com, Name of Person: Jenifer Mack
PPMYM4-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
PTKDEZ-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
PUTRGY-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
PWJXV6-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
Q2CFQV-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
Q33NQX-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
Q3RHY2-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
QMR3Q2-5561	Email Address: Jennymack16@outlook.com, Name of Person: Jennifer Mack
QRJAR3-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
QTHAXU-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
RAK67E-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
RBBDCA-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
RGH4EF-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
RRMUMV-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
RRXTDK-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
RV3JKZ-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25 - Examination Questions

WebCode Test	Response
TC4JAF-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
TCGEBD-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
TEPC2R-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
TKFNZV-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
TNEXBT-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
TVF9MD-5562	Email Address: Jennymack16@outlook.com, Name of Person: Jannifer Mack
TX22EP-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
U3RQC6-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
UKBK6E-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
URA8XZ-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
UVZCUQ-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
V4KY4K-5562	Email Address: <jennymack16@outlook.com>, Name of Person: Jennifer Mack
VCE6WL-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
VJH9N7-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
VTZR3B-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
VWB8V-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
WC9E49-5561	Email Address: Jennymack16@outlook.com, Name of Person: Jennifer Mack
WD8DHB-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
WK4CUH-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
WNN64Y-5561	Email Address: Jennymack16@outlook.com, Name of Person: Jennifer Mack
WX2YKZ-5561	Email Address: Not currently within scope of the lab., Name of Person: Not currently within scope of the lab.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25 - Examination Questions

WebCode Test	Response
WZGLVL-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
XA2A8Z-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
XEVDXV-5561	Email Address: Not in scope, Name of Person: Not in scope
XJ99G2-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
XQ9B22-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
XVDHZK-5562	[Participant did not return results for this question.]
XWDAB7-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
XX78KX-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
Y63G92-5562	Email Address: jennymack16@outlook.com, Name of Person: Jenny mack
YDJQ3P-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
YPNENR-5562	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack
ZPR26J-5561	Email Address: jennymack16@outlook.com, Name of Person: Jennifer Mack

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25 - Examination Questions

Question 25: Provide the email address of the person with whom user David Lightman communicated with about changing grades.

Consensus Result:

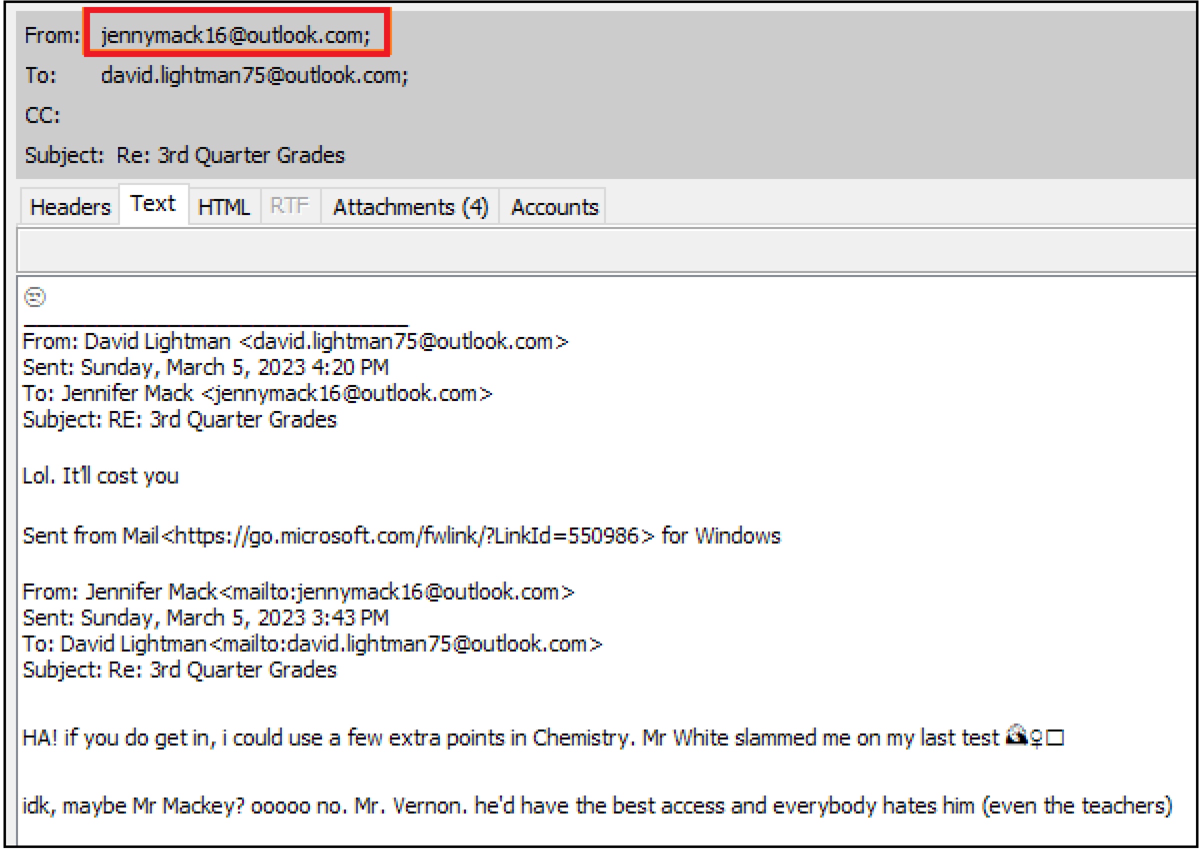
Email Address: jennymack16@outlook.com
Name of Person: Jennifer Mack

Expected Response Explanation:

Within the Thunderbird IMAP email for david.lightman75@outlook.com is an email thread between David Lightman and Jennifer Mack in which they discuss changing grades.

Expected Response Illustration:

Autopsy view of email message



From: jennymack16@outlook.com;
To: david.lightman75@outlook.com;
CC:
Subject: Re: 3rd Quarter Grades

😒

From: David Lightman <david.lightman75@outlook.com>
Sent: Sunday, March 5, 2023 4:20 PM
To: Jennifer Mack <jennymack16@outlook.com>
Subject: RE: 3rd Quarter Grades

Lol. It'll cost you

Sent from Mail<https://go.microsoft.com/fwlink/?LinkId=550986> for Windows

From: Jennifer Mack<mailto:jennymack16@outlook.com>
Sent: Sunday, March 5, 2023 3:43 PM
To: David Lightman<mailto:david.lightman75@outlook.com>
Subject: Re: 3rd Quarter Grades

HA! if you do get in, i could use a few extra points in Chemistry. Mr White slammed me on my last test 🤦♀□

idk, maybe Mr Mackey? ooooo no. Mr. Vernon. he'd have the best access and everybody hates him (even the teachers)

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26 - Examination Questions

Question 26: To what email address was an email message sent containing “Expired Password - Reset Required” in the subject?

Manufacturer's Expected Response: stephen.falken@stclotildes.institute

WebCode Test	Response
2A9WQN-5561	stephen.falken@stclotildes.institute
2P2VAR-5561	stephen.falken@stclotildes.institute
2PJFNF-5562	admin@clotildes.institute
2VQ8RL-5562	stephen.falken@stclotildes.institute
2ZFN6X-5561	Stephen.falken@stclotildes.institute
3CDK6E-5562	stephen.falken@stclotildes.institute
3DPEPK-5561	stephen.falken@stclotildes.institute
3M9X4P-5561	stephen.falken@stclotildes.institute
42BM2N-5561	stephen.falken@stclotildes.institute
48GFVJ-5561	stephen.falken@stclotildes.institute
4U7ZP2-5562	stephen.falken@stclotildes.institute
649HZ6-5561	stephen.falken@stclotildes.institute
68RW46-5562	stephen.falken@stclotildes.institute
6DZZCR-5561	stephen.falken@stclotildes.institute
6MKCN6-5562	stephen.falken@stclotildes.institute
6Q2RXW-5562	stephen.falken@stclotildes.institute
6Q4JPC-5561	stephen.falken@stclotildes.institute
6QKH3A-5562	stephen.falken@stclotildes.institute
6TR3NP-5561	stephen.falken@stclotildes.institute

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26 - Examination Questions

WebCode Test	Response
72ZUTD-5561	stephen.falken@stclotildes.institute
78PAK7-5562	stephen.falken@stclotildes.institute
7JUP4F-5561	stephen.falken@stclotildes.institute
7PQ8PM-5562	stephen.falken@stclotildes.institute
7XZLMH-5562	stephen.falken@stclotildes.institute
82VWX9-5562	stephen.falken@stclotildes.institute
83AEYT-5562	stephen.falken@stclotildes.institute
8CB97J-5561	stephen.falken@stclotildes.institute
8LJ9TK-5561	stephen.falken@stclotildes.institute
96TUNQ-5561	stephen.falken@stclotildes.institute
98ZV8C-5561	stephen.falken@stclotildes.institute
99QBZK-5562	Stephen.falken@stclotildes.institute
9AJ8JM-5561	stephen.falken@stclotildes.institute
9J9Q8U-5562	stephen.falken@stclotildes.institute
A8QHYB-5562	stephen.falken@stclotildes.institute
A8VQBZ-5561	stephen.falken@stclotildes.institute
ABK3AJ-5561	NOT IN SCOPE
ACTERK-5561	Not in Scope
ADYU2Y-5562	stephen.falken@stclotildes.institute
AKG6BT-5562	stephen.falken@stclotildes.institute
AM94QQ-5561	stephen.falken@stclotildes.institute

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26 - Examination Questions

WebCode Test	Response
BFKZWF-5562	stephen.falken@stclotildes.institute
BQRG78-5561	stephen.falken@stclotildes.institute
C4LMC9-5562	stephen.falken@stclotildes.institute
C897D8-5561	stephen.falken@stclotildes.institute
CF2CBE-5562	stephen.falken@stclotildes.institute
CKAXYB-5561	stephen.falken@stclotildes.institute
CP6N6M-5561	stephen.falken@stclotildes.institute
D7PUVD-5561	stephen.falken@stclotildes.institute
DB6AM4-5561	stephen.falken@stclotildes.institute
DGVH9K-5561	stephen.falken@stclotildes.institute
DXVP3C-5562	stephen.falken@stclotildes.institute
E2RHRZ-5562	stephen.falken@stclotildes.institute
E4ZNBG-5561	stephen.falken@stclotildes.institute
EV7HHF-5561	stephen.falken@stclotildes.institute
F3JVRX-5561	Stephen.falken@stclotildes.Institute
FZVEJB-5561	stephen.falken@stclotildes.institute
G973T4-5561	stephen.falken@stclotildes.institute
GJ39KG-5561	stephen.falken@stclotildes.institute
GYTEQP-5561	stephen.falken@stclotildes.institute
HQVXJW-5561	admin@clotildes.institute
HUFQTD-5561	stephen.falken@stclotildes.institute

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26 - Examination Questions

WebCode Test	Response
HW2LD2-5562	[Participant did not return results for this question.]
J84AQF-5562	stephen.falken@stclotildes.institute
JE9W33-5561	stephen.falken@stclotildes.institute
JGBUAC-5562	stephen.falken@stclotildes.institue
JJDU63-5561	stephen.falken@stclotildes.institute
JL32PY-5562	stephen.falken@stclotildes.institute
JLRZA6-5561	stephen.falken@stclotildes.institute
JPKFX7-5561	stephen.falken@stclotildes.institute
KR28JR-5562	Stephen.falken@stclotildes.institute
KR4V3R-5561	stephen.falken@stclotildes.institute
KXRBW6-5562	stephen.falken@stclotildes.institute
KZVDDT-5561	stephen.falken@stclotildes.institute
LDKC3B-5561	stephen.falken@stclotildes.insitute
M9HYHY-5561	stephen.falken@stclotildes.institute
MF4Q7B-5561	RosarioSIS (admin@clotildes.institute)
MF8B24-5561	stephen.falken@stclotildes.institute
NADTWE-5561	stephen.falken@stclotildes.institute
NE7TEF-5562	stephen.falken@stclotildes.institute
NTANM4-5561	stephen.falken@stclotildes.institute
NTZJR4-5561	stephen.falken@stclotildes.institute
P3ACZC-5561	stephen.falken@stclotildes.institute

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26 - Examination Questions

WebCode Test	Response
P79FU7-5561	stephen.falken@stclotildes.institute
P8ZNUA-5561	stephen.falken@stclotildes.institute
PFEMA7-5562	stephen.falken@stclotildes.institute
PFVN93-5561	stephen.falkin@stclotildes.institute
PLGGK2-5561	stephen.falken@stclotildes.institute
PPMYM4-5562	stephen.falken@stclotildes.institute
PTKDEZ-5562	stephen.falken@stclotildes.institute
PUTRGY-5561	stephen.falken@stclotildes.institute
PWJXV6-5561	stephen.falken@stclotildes.institute
Q2CFQV-5561	admin@clotildes.institute
Q33NQX-5561	stephen.falken@stclotildes.institute
Q3RHY2-5561	stephen.falken@stclotildes.institute
QMR3Q2-5561	david.lightman75@outlook.com
QRJAR3-5561	stephen.falken@stclotildes.institute
QTHAXU-5561	stephen.falken@stclotildes.institute
RAK67E-5562	stephen.falken@stclotildes.institute
RBBDCA-5562	stephen.falken@stclotildes.institute
RGH4EF-5562	stephen.falken@stclotildes.institute
RRMUMV-5561	stephen.falken@stclotildes.institute
RRXTDK-5562	stephen.falken@stclotildes.institute
RV3JKZ-5561	stephen.falken@stclotildes.institute

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26 - Examination Questions

WebCode Test	Response
TC4JAF-5562	stephen.falken@stclotildes.institute
TCGEBD-5561	stephen.falken@stclotildes.institute
TEPC2R-5562	stephen.falken@stclotildes.institute
TKFNZV-5561	stephen.falken@stclotildes.institute
TNEXBT-5561	stephen.falken@stclotildes.institute
TVF9MD-5562	Stephen.falken@stclotildes.institute
TX22EP-5561	admin@clotildes.institute
U3RQC6-5561	stephen.falken@stclotildes.institute
UKBK6E-5561	admin@clotildes.institute
URA8XZ-5561	stephen.falken@stclotildes.institute
UVZCUQ-5562	stephen.falken@stclotildes.institute
V4KY4K-5562	"stephen.falken@stclotildes.institute"
VCE6WL-5561	stephen.falken@stclotildes.institute
VJH9N7-5561	stephen.falken@stclotildes.institute
VTZR3B-5561	stephen.falken@stclotildes.institute
VVVB8V-5561	stephen.falken@stclotildes.institute
WC9E49-5561	David.lightman75@outlook.com
WD8DHB-5561	stephen.falken@stclotildes.institute
WK4CUH-5561	stephen.falken@stclotildes.institute
WNN64Y-5561	stephen.falken@stclotildes.institute
WX2YKZ-5561	Not currently within scope of the lab.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26 - Examination Questions

WebCode Test	Response
WZGLVL-5562	stephen.falken@stclotildes.institute
XA2A8Z-5562	stephen.falken@stclotildes.institute
XEVDXV-5561	Not in scope
XJ99G2-5562	stephen.falken@stclotildes.institute
XQ9B22-5561	stephen.falken@stclotildes.institute
XVDHZK-5562	[Participant did not return results for this question.]
XWDAB7-5561	stephen.falken@stclotildes.institute
XX78KX-5561	stephen.falken@stclotildes.institute
Y63G92-5562	stephen.falken@stclotildes.institute
YDJQ3P-5561	stephen.falken@stclotildes.institute
YPNENR-5562	stephen.falken@stclotildes.institute
ZPR26J-5561	stephen.falken@stclotildes.institute

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26 - Examination Questions

Question 26: To what email address was an email message sent containing “Expired Password - Reset Required” in the subject?

Consensus Result:

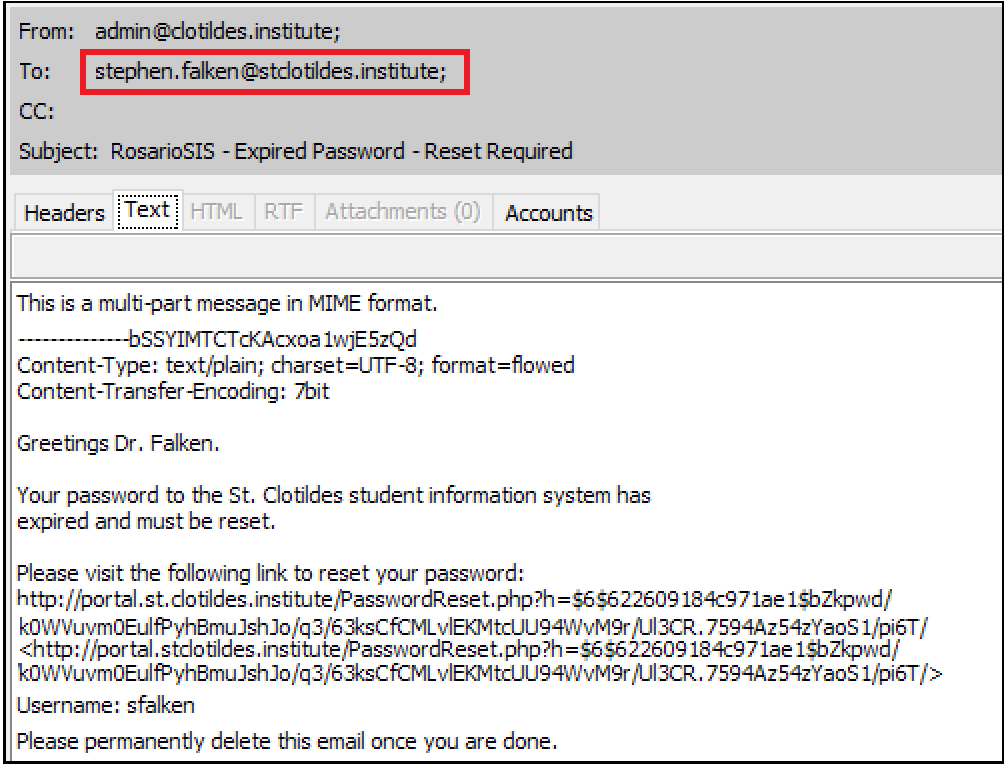
stephen.falken@stclotildes.institute

Expected Response Explanation:

Within the Thunderbird IMAP email for admin@clotildes.institute is a sent message addressed to stephen.falken@stclotildes.institute with the subject "RosarioSIS - Expired Password - Reset Required."

Expected Response Illustration:

Autopsy view of grep email message



From: admin@clotildes.institute;
To: stephen.falken@stclotildes.institute;
CC:
Subject: RosarioSIS - Expired Password - Reset Required

```
This is a multi-part message in MIME format.
--------------bSSYIMTCTcKAcxoa1wjE5zQd
Content-Type: text/plain; charset=UTF-8; format=flowed
Content-Transfer-Encoding: 7bit

Greetings Dr. Falken.

Your password to the St. Clotildes student information system has
expired and must be reset.

Please visit the following link to reset your password:
http://portal.st.clotildes.institute/PasswordReset.php?h=$6$622609184c971ae1$bZkpwd/
k0WVuvm0EulfPyhBmuJshJo/q3/63ksCfCMLvlEKMtcUU94WvM9r/Ul3CR.7594Az54zYaoS1/pi6T/
<http://portal.stclotildes.institute/PasswordReset.php?h=$6$622609184c971ae1$bZkpwd/
k0WVuvm0EulfPyhBmuJshJo/q3/63ksCfCMLvlEKMtcUU94WvM9r/Ul3CR.7594Az54zYaoS1/pi6T/>
Username: sfalken
Please permanently delete this email once you are done.
```

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27 - Examination Questions

Question 27: In the image, there are several red bordered jpeg image files of animals. Locate one of these photos and provide the black font text that appears in the photo.

Manufacturer's Expected Response: 2023A, 2023R or 2023T

WebCode Test	Response
2A9WQN-5561	2023T
2P2VAR-5561	2023R
2PJFNF-5562	2023R 2023T
2VQ8RL-5562	2023R and 2023T
2ZFN6X-5561	2023R
3CDK6E-5562	2023R
3DPEPK-5561	2023R
3M9X4P-5561	20237
42BM2N-5561	2023R
48GFVJ-5561	2023R
4U7ZP2-5562	2023R
649HZ6-5561	2023T
68RW46-5562	2023R
6DZZCR-5561	2023R
6MKCN6-5562	2023A, 2023R, 2023T
6Q2RXW-5562	2023T
6Q4JPC-5561	2023R
6QKH3A-5562	2023T
6TR3NP-5561	2023R

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27 - Examination Questions

WebCode Test	Response
72ZUTD-5561	2023R
78PAK7-5562	2023T
7JUP4F-5561	20023T
7PQ8PM-5562	2023R
7XZLMH-5562	2023T
82VWX9-5562	2023R
83AEYT-5562	2023T
8CB97J-5561	2023T
8LJ9TK-5561	2023T
96TUNQ-5561	2023T
98ZV8C-5561	2023R
99QBZK-5562	2023R
9AJ8JM-5561	2023R
9J9Q8U-5562	2023T
A8QHYB-5562	2023R
A8VQBZ-5561	2023R
ABK3AJ-5561	NOT IN SCOPE
ACTERK-5561	Not in Scope
ADYU2Y-5562	2023R
AKG6BT-5562	2023T
AM94QQ-5561	2023R

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27 - Examination Questions

WebCode Test	Response
BFKZWF-5562	2023T
BQRG78-5561	2023R
C4LMC9-5562	2023T or 2023R
C897D8-5561	2023R
CF2CBE-5562	2023T , \Users\27560950478_f166261959_o.jpg
CKAXYB-5561	2023R
CP6N6M-5561	2023R / 2023T
D7PUVD-5561	2023R, 2023T
DB6AM4-5561	2023T, 2023R
DGVH9K-5561	2023T
DXVP3C-5562	2023A
E2RHRZ-5562	2023T
E4ZNBG-5561	2023T
EV7HHF-5561	2023T
F3JVRX-5561	2023T, 2023R
FZVEJB-5561	2023R
G973T4-5561	2023T
GJ39KG-5561	2023T
GYTEQP-5561	2023R
HQVXJW-5561	2023R
HUFQTD-5561	2023R

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27 - Examination Questions

WebCode Test	Response
HW2LD2-5562	[Participant did not return results for this question.]
J84AQF-5562	2023A
JE9W33-5561	2023T
JGBUAC-5562	2023R
JJDU63-5561	2023R
JL32PY-5562	2023T, 2023R, 2023A
JLRZA6-5561	2023R
JPKFX7-5561	2023R
KR28JR-5562	2023T
KR4V3R-5561	2023R
KXRBW6-5562	2023R, 2023T
KZVDDT-5561	2023T / 2023R
LDKC3B-5561	2023T
M9HYHY-5561	2023T
MF4Q7B-5561	2023T
MF8B24-5561	2023R
NADTWE-5561	2023R
NE7TEF-5562	2023A 2023T 2023R
NTANM4-5561	2023R
NTZJR4-5561	2023R
P3ACZC-5561	2023R

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27 - Examination Questions

WebCode Test	Response
P79FU7-5561	2023T
P8ZNUA-5561	2023R
PFEMA7-5562	2023R
PFVN93-5561	2023T
PLGGK2-5561	2023T
PPMYM4-5562	2023T
PTKDEZ-5562	2023R
PUTRGY-5561	2023R
PWJXV6-5561	2023T
Q2CFQV-5561	2023T,2023R
Q33NQX-5561	\Users\27560950478_f166261959_o.jpg,2023T
Q3RHY2-5561	2023R
QMR3Q2-5561	2023T
QRJAR3-5561	2023T
QTHAXU-5561	2023R
RAK67E-5562	2023T
RBBDCA-5562	2023T
RGH4EF-5562	2023A
RRMUMV-5561	2023T
RRXTDK-5562	2023T (27560950478_f166261959_o.jpg)
RV3JKZ-5561	2023T

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27 - Examination Questions

WebCode Test	Response
TC4JAF-5562	2023R
TCGEBD-5561	2023T 2023R
TEPC2R-5562	2023R
TKFNZV-5561	2023R
TNEXBT-5561	2023T
TVF9MD-5562	2023R
TX22EP-5561	2023T, 2023R
U3RQC6-5561	2023T
UKBK6E-5561	27560950478_f166261959_o.jpg / 2023T
URA8XZ-5561	2023T - \Users\27560950478_f166261959_o.jpg
UVZCUQ-5562	2023T
V4KY4K-5562	"2023T" "2023R" or "2023A"
VCE6WL-5561	2023T
VJH9N7-5561	2023T
VTZR3B-5561	2023R
VVVB8V-5561	2023R
WC9E49-5561	2023T
WD8DHB-5561	2023R
WK4CUH-5561	2023T
WNN64Y-5561	2023T
WX2YKZ-5561	Not currently within scope of the lab.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27 - Examination Questions

WebCode Test	Response
WZGLVL-5562	2023A, 2023R, 2023T
XA2A8Z-5562	2023R
XEVDXV-5561	Not in scope
XJ99G2-5562	2023T
XQ9B22-5561	2023T
XVDHZK-5562	[Participant did not return results for this question.]
XWDAB7-5561	2023T
XX78KX-5561	2023T
Y63G92-5562	2023T
YDJQ3P-5561	2023A
YPNENR-5562	2023T
ZPR26J-5561	2023R

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27 - Examination Questions

Question 27: In the image, there are several red bordered jpeg image files of animals. Locate one of these photos and provide the black font text that appears in the photo.

Consensus Result:

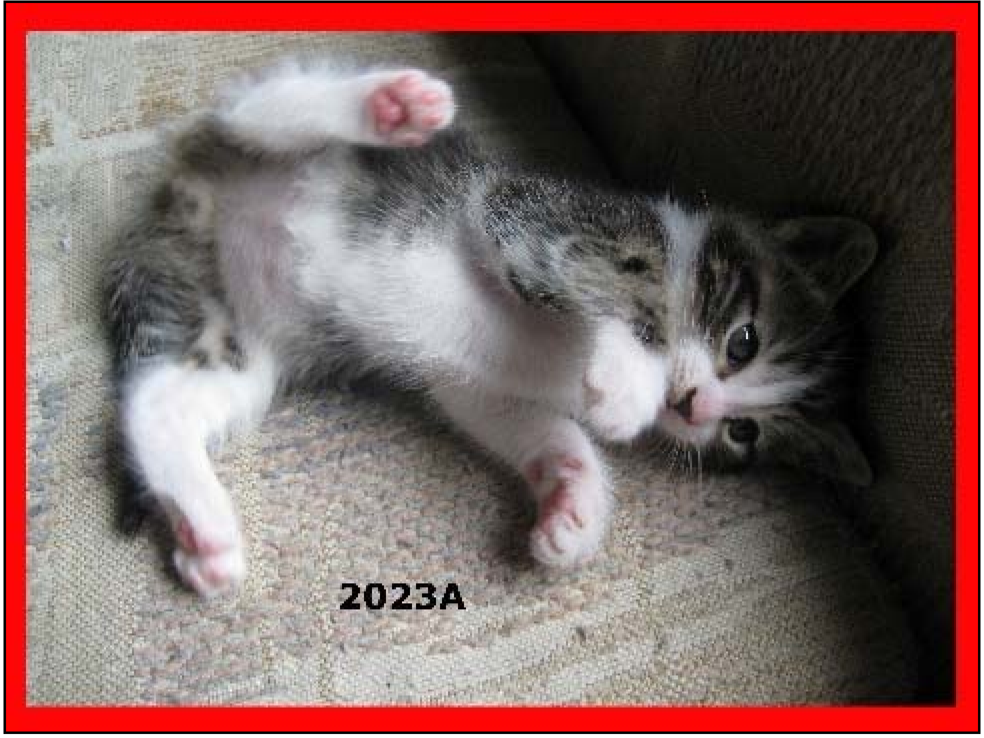
2023A, 2023R or 2023T

Expected Response Explanation:

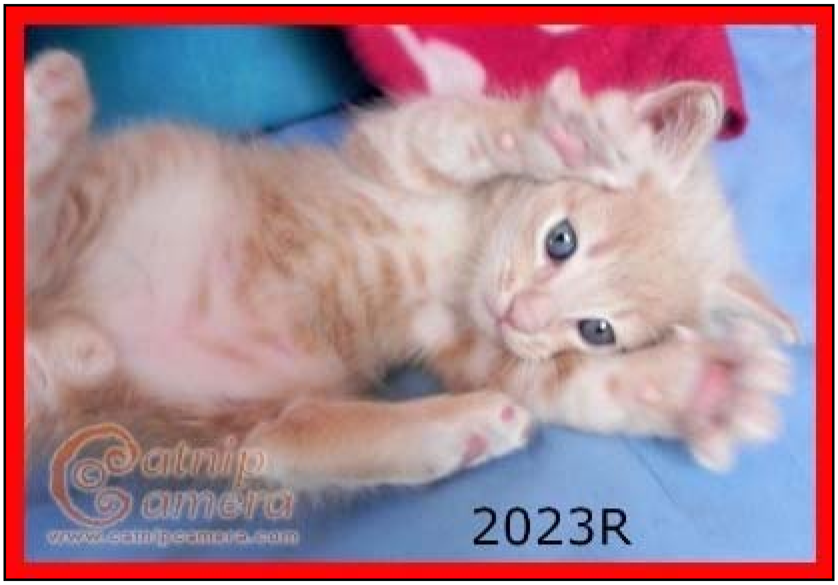
Reviewing the images in gallery view will reveal the files described in the question.

Expected Response Illustration:

Red bordered image 2023A



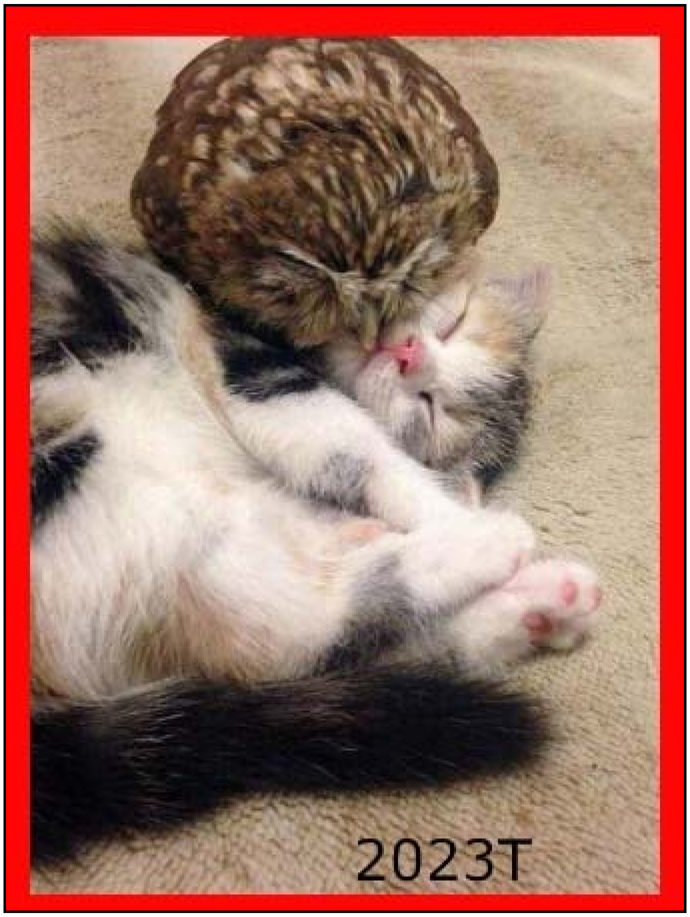
Red bordered image 2023R



Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27 - Examination Questions
Red bordered image 2023T



Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28 - Examination Questions

Question 28: Provide the GPS coordinates where the photo racetrack.jpg was taken. Provide your response in the format ##.##### (Indicate directionality as N or S), ##.##### (Indicate directionality as E or W).

Manufacturer's Expected Response: 39.2421 N, 77.9732 W and varying formats that represent the same location.

WebCode Test	Response
2A9WQN-5561	39.242108 N, -77.973289 W
2P2VAR-5561	39.242108 N, -77.973289 W
2PJFNF-5562	N 39.1431 W 77.5823
2VQ8RL-5562	GPS Latitude 39°14'31.59" (N), GPS Longitude 77°58'23.84" (W)
2ZFN6X-5561	39.2421, -77.9733
3CDK6E-5562	N 39.242108 W 77.973289
3DPEPK-5561	39.242108 N, 77.973289 W
3M9X4P-5561	39.24210 N -77.97328 W
42BM2N-5561	39.1431 N, 77.5823 W
48GFVJ-5561	39.24210 N, 77.97328 W
4U7ZP2-5562	39.242108333333334; -77.97328888888889
649HZ6-5561	39.24210 N, -77.97328 W
68RW46-5562	N 39.24211, W 77.97329
6DZZCR-5561	39.1431.59N , 77.5823.84W
6MKCN6-5562	39.242108(N), -77.973289(W)
6Q2RXW-5562	39.24210 N, 77.97328 W
6Q4JPC-5561	39.143159 N, 77.582384 W
6QKH3A-5562	39.2421 N, -77.9733 W

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28 - Examination Questions

WebCode Test	Response
6TR3NP-5561	39°14'31.59" N 77°58'23.84" W
72ZUTD-5561	39.24210 N 77.97328 W (to nearest 5 decimal places)
78PAK7-5562	39.242108 N, 77.973289 W
7JUP4F-5561	39.2421 N, -77.9733 W
7PQ8PM-5562	GPSLatitude: 39.242108 (North), GPSLongitude: 77.973289 (West)
7XZLMH-5562	39.24210 N, -77.97329W
82VWX9-5562	N 39.143159 W 77.582384
83AEYT-5562	39.24210 N, 77.97328 W
8CB97J-5561	39.24211 N, -77.97329 W
8LJ9TK-5561	39.24211 N, 77.97329 W
96TUNQ-5561	Latitude: 39.242108 / Longitude: -77.973289
98ZV8C-5561	39.24210 N, 77.97328 W
99QBZK-5562	39.24210 N, -77.97328 W
9AJ8JM-5561	39.143159 N, 77.582383 W
9J9Q8U-5562	39.2421 N, -77.9733 W
A8QHYB-5562	39.242108 N, 77.973289 W
A8VQBZ-5561	North 39.242108, West -77.973289
ABK3AJ-5561	NOT IN SCOPE
ACTERK-5561	Not in Scope
ADYU2Y-5562	39.242108 N, -77.973289 W
AKG6BT-5562	39 deg 14' 31.59" N, 77 deg 58' 23.84" W (39°14'31.59"(N), 77°58'23.84"(W))

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28 - Examination Questions

WebCode Test	Response
AM94QQ-5561	39.2421 N, -77.9733 W
BFKZWF-5562	39.24211 N , 77.97329 W
BQRG78-5561	39.242108 N, 77.973289 W
C4LMC9-5562	39.24210 N 77.97328 W
C897D8-5561	39.24210 N, -77.97328 W
CF2CBE-5562	Latitude: 39.2421 N , Longitude: 77.9733 W
CKAXYB-5561	39.242108 N 77.973289 W
CP6N6M-5561	39.242108°N and -77.973289°W
D7PUVD-5561	N 39.242108, W -77.973289
DB6AM4-5561	39.24210 N, 77.97328 W
DGVH9K-5561	39.2421 N, 77.9732 W
DXVP3C-5562	39.24210 N, 77.97328 W
E2RHRZ-5562	N 39.242108 , W -77.973289
E4ZNBG-5561	39.24210 N, 77.97328 W
EV7HHF-5561	39.24210 N, -77.97328 W
F3JVRX-5561	39.242108 (N), -77.973289 (W)
FZVEJB-5561	39.242108 N, -77.973289 W
G973T4-5561	Latitude: 39.24211 N Longitude: 77.97329 W
GJ39KG-5561	N 39°14'31.59" - W 77°58'23.84"
GYTEQP-5561	39.242108 N, -77.973289 W
HQVXJW-5561	39.24211(N), 77.97328(W)

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28 - Examination Questions

WebCode Test	Response
HUFQTD-5561	39.24210 -77.97328
HW2LD2-5562	[Participant did not return results for this question.]
J84AQF-5562	39° 14' 31,59" N 77° 58' 23,84" W
JE9W33-5561	39.24210 N, 77.97328 W
JGBUAC-5562	Latitude: N 39.242108 Longitude: W 77.973289
JJDU63-5561	39.2421 (N), -77.9733 (W)
JL32PY-5562	39.24194N 77.97305W
JLRZA6-5561	39.24210 N, -77.97328 W
JPKFX7-5561	39.242108N -77.973289W
KR28JR-5562	39.242108 N, 77.973289 W
KR4V3R-5561	39.24211 N, 77.97329 W
KXRBW6-5562	N 39.242108, W -77.973289
KZVDDT-5561	39.24210 N, -77.97328 W
LDKC3B-5561	N 39.2421083, E -76.02671111111111
M9HYHY-5561	39.2421 N , 77.9732 W
MF4Q7B-5561	GPSLatitude: 39.242108; GPSLongitude: -77.973289
MF8B24-5561	39.24210 North -77.97328 West
NADTWE-5561	39.14315 N, 77.58238 W
NE7TEF-5562	39.242108(N), -77.973289(W)
NTANM4-5561	39°14'31.59" N, -77°58'23.84" W
NTZJR4-5561	39.242108 N -77.973289 W

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28 - Examination Questions

WebCode Test	Response
P3ACZC-5561	39.143159 N -77.582384 W
P79FU7-5561	Latitude 39.24210 N, Longitude -77.97328 W
P8ZNUA-5561	39.24210833 N 77.97328889 W
PFEMA7-5562	39.24210 N, 77.97328 W
PFVN93-5561	39.2421N, -77.9733W
PLGGK2-5561	39.1431 N, 77.5823 W
PPMYM4-5562	Latitude 39.24210 N, Longitude 77.97328 W
PTKDEZ-5562	39.242108 N, 77.973289 W.
PUTRGY-5561	39.24211 N , 77.97329 W
PWJXV6-5561	39.242108 N, 77.973289 W
Q2CFQV-5561	39.24210 N,77.97328 W
Q33NQX-5561	39.24210N,77.97328W
Q3RHY2-5561	39.1431 N, 77.5823 W
QMR3Q2-5561	N 1°0'1.00", W 1°0'1.00"
QRJAR3-5561	39.242108 N, 77.973289 W
QTHAXU-5561	39.24210 N, 77.97330 W
RAK67E-5562	39.242108 N 77.973289 W
RBBDCA-5562	Latitude (N/S): 39.242108 Longitude (E/W): -77.973289
RGH4EF-5562	N-39.242108, W-77.973289
RRMUMV-5561	39.242108 N 77.973289 W
RRXTDK-5562	39.24210 N, 77.97328 W

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28 - Examination Questions

WebCode Test	Response
RV3JKZ-5561	Latitude: 39.24211 N Longitude: 77.97329 W
TC4JAF-5562	39.2421 N -77.9732 W
TCGEBD-5561	39°14'31.59" North 77°58'23.84" West
TEPC2R-5562	39.2421 N , 77.9732 W
TKFNZV-5561	39.2421 N , 77.9732 W
TNEXBT-5561	39° 14' 31.59" N 77° 58' 23.84" W
TVF9MD-5562	39' 14.3159 N, 77' 58.2384 W
TX22EP-5561	39.24210(N), 77.97328(W)
U3RQC6-5561	39.242108 N, -77.973289 W
UKBK6E-5561	31.5899 / 23.8400
URA8XZ-5561	Latitude 39.24210 N, Longitude -77.97328 W
UVZCUQ-5562	39.24211 N, 77.97329 W
V4KY4K-5562	39°14'31.59"N 77°58'23.84" W
VCE6WL-5561	Longitude: -77.97328 W and Latitude: 39.24210 N (Latitude: 39.242108333333334 N Longitude: -77.97328888888889 W)
VJH9N7-5561	39.24210 N, 77.97328 W
VTZR3B-5561	39.242108 N, -77.973289 W
VVVB8V-5561	39.24210 N -77.97328 W
WC9E49-5561	39.24210N,-77.97328W
WD8DHB-5561	39.242108 N, 77.973289 W
WK4CUH-5561	39.2421 N, -77.9732 W
WNN64Y-5561	39.242108 N; -77.973289 W

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28 - Examination Questions

WebCode Test	Response
WX2YKZ-5561	Not currently within scope of the lab.
WZGLVL-5562	39,24211N, 77,97329W
XA2A8Z-5562	39.242108 N , -77.973289 W
XEVDXV-5561	Not in scope
XJ99G2-5562	Latitude 39.24210 - North & Longitude 77.97328 – West
XQ9B22-5561	39.24211° N, 77.97329° W
XVDHZK-5562	[Participant did not return results for this question.]
XWDAB7-5561	39.242108 N, 77.973289 W
XX78KX-5561	39.24210 N -77.97328 W
Y63G92-5562	GPS LatitudeRef - N GPSLatitude - 39 14 31.59 (39.242108) GPSLongitudeRef - W GPSLongitude - 77 58 23.84 (77.973289)
YDJQ3P-5561	39.24210 N, 77.97328 W
YPNENR-5562	Latitude: 39.2421 N Longitude: 77.9733 W
ZPR26J-5561	North 39.2421 , West -77.9732

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28 - Examination Questions

Question 28: Provide the GPS coordinates where the photo racetrack.jpg was taken. Provide your response in the format ##.##### (Indicate directionality as N or S), ##.##### (Indicate directionality as E or W).

Consensus Result:

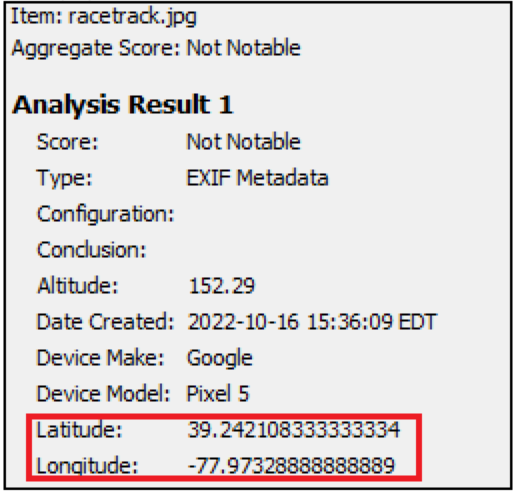
39.2421 N, 77.9732 W and varying formats that represent the same location.

Expected Response Explanation:

The photo racetrack.jpg is stored in C:\Users\David Lightman\Pictures\Camera Roll\. Parsing this file with a tool like ExifTool will reveal the embedded GPS EXIF metadata.

Expected Response Illustration:

Autopsy browser view of EXIF data for racetrack.jpg

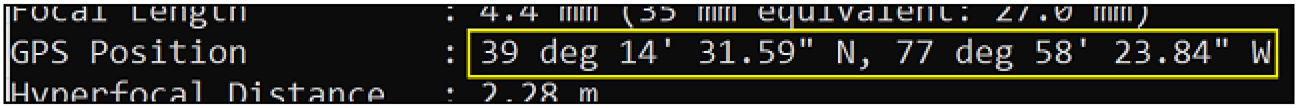


Item: racetrack.jpg
Aggregate Score: Not Notable

Analysis Result 1

Score:	Not Notable
Type:	EXIF Metadata
Configuration:	
Conclusion:	
Altitude:	152.29
Date Created:	2022-10-16 15:36:09 EDT
Device Make:	Google
Device Model:	Pixel 5
Latitude:	39.242108333333334
Longitude:	-77.97328888888889

ExifTool view of racetrack.jpg



```
Focal Length                    : 4.4 mm (35 mm equivalent: 27.0 mm)
GPS Position                    : 39 deg 14' 31.59" N, 77 deg 58' 23.84" W
Hyperfocal Distance             : 2.28 m
```

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 29 - Examination Questions

Question 29: In unallocated space on the "C" (second) partition on the computer hard drive is a deleted jpeg image of a black and white F-18 aircraft with "NASA" on the tail flying in a dark blue sky. The MD5 hash of this file is ce47fda2b3b78478a9c0610ca859bcda. Provide the SHA1 hash of this file.

Manufacturer's Expected Response: 28A7CA82C03C0C6F686E05DC951BC78A7679334B

WebCode Test	Response
2A9WQN-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
2P2VAR-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
2PJFNF-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
2VQ8RL-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
2ZFN6X-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
3CDK6E-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
3DPEPK-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
3M9X4P-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
42BM2N-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
48GFVJ-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
4U7ZP2-5562	424B37AE2CA853BBF76031D076AAEBAABFC382BF
649HZ6-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
68RW46-5562	28a7 ca82 c03c 0c6f 686e 05dc 951b c78a 7679 334b
6DZZCR-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
6MKCN6-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
6Q2RXW-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
6Q4JPC-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
6QKH3A-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 29 - Examination Questions

WebCode Test	Response
6TR3NP-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
72ZUTD-5561	424B37AE2CA853BBF76031D076AAEBAABFC382BF (Note this was locate via a manual image search on S21 LASERi-X due to the provided MD5 not being present on our processed X-Ways)
78PAK7-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
7JUP4F-5561	fct4vawahqgg62d0ax0jkg6hrj3hsm2l
7PQ8PM-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
7XZLMH-5562	28A7CA82C03C0C6F686E05DC951BC78A7679334B
82VWX9-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
83AEYT-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
8CB97J-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
8LJ9TK-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
96TUNQ-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
98ZV8C-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
99QBZK-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
9AJ8JM-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
9J9Q8U-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
A8QHYB-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
A8VQBZ-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
ABK3AJ-5561	NOT IN SCOPE
ACTERK-5561	Not in Scope
ADYU2Y-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
AKG6BT-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 29 - Examination Questions

WebCode Test	Response
AM94QQ-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
BFKZWF-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
BQRG78-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
C4LMC9-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
C897D8-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
CF2CBE-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
CKAXYB-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
CP6N6M-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
D7PUVD-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
DB6AM4-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
DGVH9K-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
DXVP3C-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
E2RHRZ-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
E4ZNBG-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
EV7HHF-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
F3JVRX-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
FZVEJB-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
G973T4-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
GJ39KG-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
GYTEQP-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
HQVXJW-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 29 - Examination Questions

WebCode Test	Response
HUFQTD-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
HW2LD2-5562	[Participant did not return results for this question.]
J84AQF-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
JE9W33-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
JGBUAC-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
JJDU63-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
JL32PY-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
JLRZA6-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
JPKFX7-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
KR28JR-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
KR4V3R-5561	28A7CA82C03C0C6F686E05DC951BC78A7679334B
KXRBW6-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
KZVDDT-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
LDKC3B-5561	28A7CA82C03C0C6F686E05DC951BC78A7679334B
M9HYHY-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
MF4Q7B-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
MF8B24-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
NADTWE-5561	28A7CA82C03C0C6F686E05DC951BC78A7679334B
NE7TEF-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
NTANM4-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
NTZJR4-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 29 - Examination Questions

WebCode Test	Response
P3ACZC-5561	28a7ca82c03c0c6f686e05dc951bc78a76793
P79FU7-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
P8ZNUA-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
PFEMA7-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
PFVN93-5561	28A7CA82C03C0C6F686E05DC951BC78A7679334B
PLGGK2-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
PPMYM4-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
PTKDEZ-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
PUTRGY-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
PWJXV6-5561	28a7ca82c03c0cbf686e05dc951bc78a7679334b
Q2CFQV-5561	28A7CA82C03C0C6F686E05DC951BC78A7679334B
Q33NQX-5561	28A7CA82C03C0C6F686E05DC951BC78A7679334B
Q3RHY2-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
QMR3Q2-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
QRJAR3-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
QTHAXU-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
RAK67E-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
RBBDCA-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
RGH4EF-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
RRMUMV-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
RRXTDK-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 29 - Examination Questions

WebCode Test	Response
RV3JKZ-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
TC4JAF-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
TCGEBD-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
TEPC2R-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
TKFNZV-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
TNEXBT-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
TVF9MD-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
TX22EP-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
U3RQC6-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
UKBK6E-5561	4aeedb21681e7ad29e3a7324a39d489c (MD5) , 8fbd2b95d6bfce0479316b1d94427fa0f2114c81 (SHA-1)
URA8XZ-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
UVZCUQ-5562	28A7CA82C03C0C6F686E05DC951BC78A7679334B
V4KY4K-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
VCE6WL-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
VJH9N7-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
VTZR3B-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
VVVB8V-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
WC9E49-5561	424b37ae2ca853bbf76031d076aaebaabfc382bf
WD8DHB-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
WK4CUH-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
WNN64Y-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 29 - Examination Questions

WebCode Test	Response
WX2YKZ-5561	Not currently within scope of the lab.
WZGLVL-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
XA2A8Z-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
XEVDXV-5561	Not in scope
XJ99G2-5562	424B37AE2CA853BBF76031D076AAEBAABFC382BF
XQ9B22-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
XVDHZK-5562	[Participant did not return results for this question.]
XWDAB7-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
XX78KX-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
Y63G92-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
YDJQ3P-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b
YPNENR-5562	28a7ca82c03c0c6f686e05dc951bc78a7679334b
ZPR26J-5561	28a7ca82c03c0c6f686e05dc951bc78a7679334b

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 29 - Examination Questions

Question 29: In unallocated space on the "C" (second) partition on the computer hard drive is a deleted jpeg image of a black and white F-18 aircraft with "NASA" on the tail flying in a dark blue sky. The MD5 hash of this file is ce47fda2b3b78478a9c0610ca859bcda. Provide the SHA1 hash of this file.

Consensus Result:

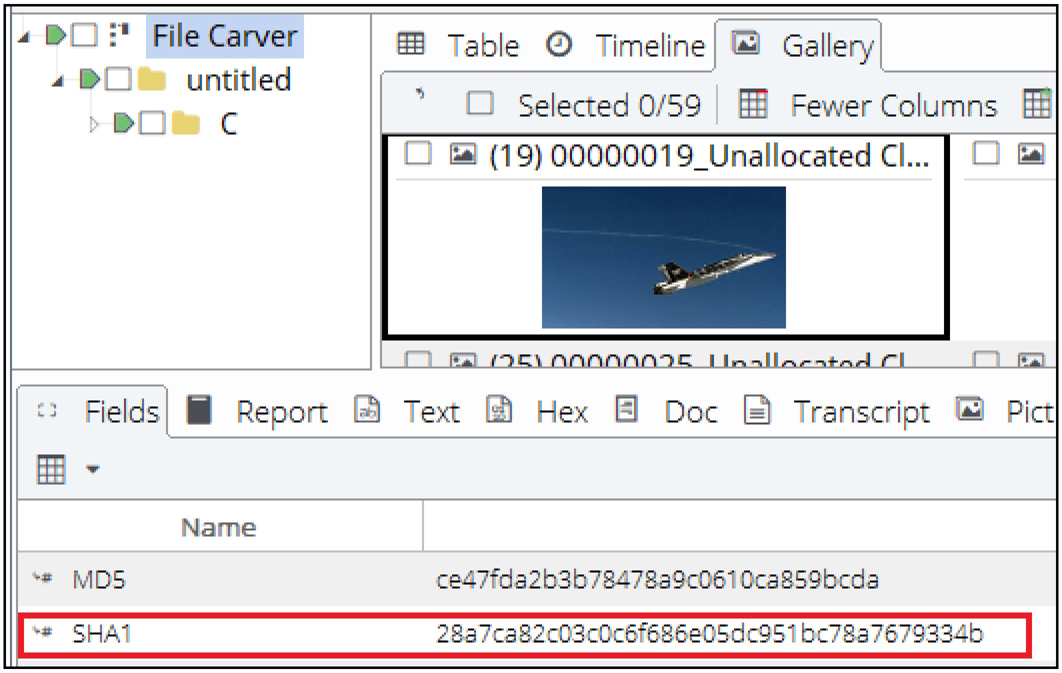
28A7CA82C03C0C6F686E05DC951BC78A7679334B

Expected Response Explanation:

A reliable file recovery or file tool can find deleted files in unallocated space.

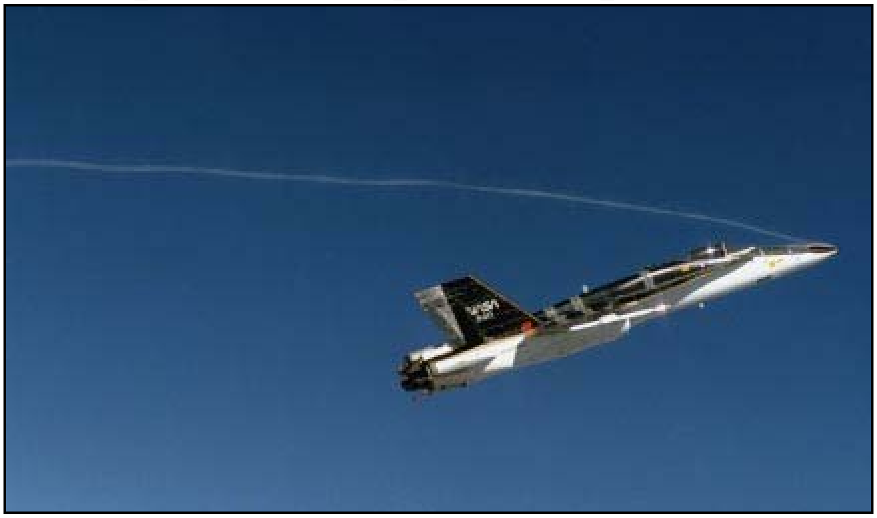
Expected Response Illustration:

EnCase File Carver



Name	
MD5	ce47fda2b3b78478a9c0610ca859bcda
SHA1	28a7ca82c03c0c6f686e05dc951bc78a7679334b

00000055_Unallocated Clusters_FO-232856670_PS-2767734+94.jpg



Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 30 - Examination Questions

Question 30: In unallocated space on the "C" (second) partition on the computer hard drive is a deleted jpeg image of four owls standing on the ground. The MD5 hash of this file is 8f3faa6a67485cd264a74c33e70808d8. Provide the SHA-1 hash of this file.

Manufacturer's Expected Response: E90E098A1A3BCB853FE255E6820B0084B1381048

WebCode Test	Response
2A9WQN-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
2P2VAR-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
2PJFNF-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
2VQ8RL-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
2ZFN6X-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
3CDK6E-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
3DPEPK-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
3M9X4P-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
42BM2N-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
48GFVJ-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
4U7ZP2-5562	E90E098A1A3BCB853FE255E6820B0084B1381048
649HZ6-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
68RW46-5562	e90e 098a 1a3b cb85 3fe2 55e6 820b 0084 b138 1048
6DZZCR-5561	No such MD5 exists; I found a picture that matches the visual description but it has a different MD5 than what is provided in the question
6MKCN6-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
6Q2RXW-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
6Q4JPC-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
6QKH3A-5562	e90e098a1a3bcb853fe255e6820b0084b1381048

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 30 - Examination Questions

WebCode Test	Response
6TR3NP-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
72ZUTD-5561	DED11C1E265E09564DA84AE2750567CB54B77389 (Note this was locate via a manual image search on S21 LASERi-X due to the provided MD5 not being present on our processed X-Ways)
78PAK7-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
7JUP4F-5561	only the carved thumbnail was observed
7PQ8PM-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
7XZLMH-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
82VWX9-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
83AEYT-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
8CB97J-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
8LJ9TK-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
96TUNQ-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
98ZV8C-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
99QBZK-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
9AJ8JM-5561	d7ea6f3c765e7d2a6ded42b3520666237e976dd0
9J9Q8U-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
A8QHYB-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
A8VQBZ-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
ABK3AJ-5561	NOT IN SCOPE
ACTERK-5561	Not in Scope
ADYU2Y-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
AKG6BT-5562	e90e098a1a3bcb853fe255e6820b0084b1381048

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 30 - Examination Questions

WebCode Test	Response
AM94QQ-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
BFKZWF-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
BQRG78-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
C4LMC9-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
C897D8-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
CF2CBE-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
CKAXYB-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
CP6N6M-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
D7PUVD-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
DB6AM4-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
DGVH9K-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
DXVP3C-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
E2RHRZ-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
E4ZNBG-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
EV7HHF-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
F3JVRX-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
FZVEJB-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
G973T4-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
GJ39KG-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
GYTEQP-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
HQVXJW-5561	e90e098a1a3bcb853fe255e6820b0084b1381048

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 30 - Examination Questions

WebCode Test	Response
HUFQTD-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
HW2LD2-5562	[Participant did not return results for this question.]
J84AQF-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
JE9W33-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
JGBUAC-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
JJDU63-5561	d7ea6f3c765e7d2a6ded42b3520666237e976dd0
JL32PY-5562	E90E098A1A3BCB853FE255E6820B0084B1381048
JLRZA6-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
JPKFX7-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
KR28JR-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
KR4V3R-5561	E90E098A1A3BCB853FE255E6820B0084B1381048
KXRBW6-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
KZVDDT-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
LDKC3B-5561	E90E098A1A3BCB853FE255E6820B0084B1381048
M9HYHY-5561	d7ea6f3c765e7d2a6ded42b3520666237e976dd0
MF4Q7B-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
MF8B24-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
NADTWE-5561	E90E098A1A3BCB853FE255E6820B0084B1381048
NE7TEF-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
NTANM4-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
NTZJR4-5561	e90e098a1a3bcb853fe255e6820b0084b1381048

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 30 - Examination Questions

WebCode Test	Response
P3ACZC-5561	E90E098A1A3BCB853FE255E6820B0084B1381048
P79FU7-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
P8ZNUA-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
PFEMA7-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
PFVN93-5561	d7ea6f3c765e7d2a6ded42b352066237e96dd0
PLGGK2-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
PPMYM4-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
PTKDEZ-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
PUTRGY-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
PWJXV6-5561	e90e098ala3bcb853fe255e6820b0084b1381084
Q2CFQV-5561	E90E098A1A3BCB853FE255E6820B0084B1381048
Q33NQX-5561	E90E098A1A3BCB853FE255E6820B0084B1381048
Q3RHY2-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
QMR3Q2-5561	not match(has a different MD 5 hash)
QRJAR3-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
QTHAXU-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
RAK67E-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
RBBDCA-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
RGH4EF-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
RRMUMV-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
RRXTDK-5562	e90e098a1a3bcb853fe255e6820b0084b1381048

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 30 - Examination Questions

WebCode Test	Response
RV3JKZ-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
TC4JAF-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
TCGEBD-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
TEPC2R-5562	d7ea6f3c765e7d2a6ded42b3520666237e976dd0
TKFNZV-5561	d7ea6f3c765e7d2a6ded42b3520666237e976dd0
TNEXBT-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
TVF9MD-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
TX22EP-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
U3RQC6-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
UKBK6E-5561	857301f22fed0feb44d8c7a22b3bf94a (MD5) , a95cff1d030f17730176e82787e09ed4e70dc008 (SHA-1)
URA8XZ-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
UVZCUQ-5562	E90E098A1A3BCB853FE255E6820B0084B1381048
V4KY4K-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
VCE6WL-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
VJH9N7-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
VTZR3B-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
VVVB8V-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
WC9E49-5561	b66a87d51b0eabafd5e87ee7e3aba30b364ef9c4
WD8DHB-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
WK4CUH-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
WNN64Y-5561	e90e098a1a3bcb853fe255e6820b0084b1381048

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 30 - Examination Questions

WebCode Test	Response
WX2YKZ-5561	Not currently within scope of the lab.
WZGLVL-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
XA2A8Z-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
XEVDXV-5561	Not in scope
XJ99G2-5562	B66A87D51B0EABAFD5E87EE7E3ABA30B364EF9C4
XQ9B22-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
XVDHZK-5562	[Participant did not return results for this question.]
XWDAB7-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
XX78KX-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
Y63G92-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
YDJQ3P-5561	e90e098a1a3bcb853fe255e6820b0084b1381048
YPNENR-5562	e90e098a1a3bcb853fe255e6820b0084b1381048
ZPR26J-5561	e90e098a1a3bcb853fe255e6820b0084b1381048

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 30 - Examination Questions

Question 30: In unallocated space on the “C” (second) partition on the computer hard drive is a deleted jpeg image of four owls standing on the ground. The MD5 hash of this file is 8f3faa6a67485cd264a74c33e70808d8. Provide the SHA-1 hash of this file.

Consensus Result:

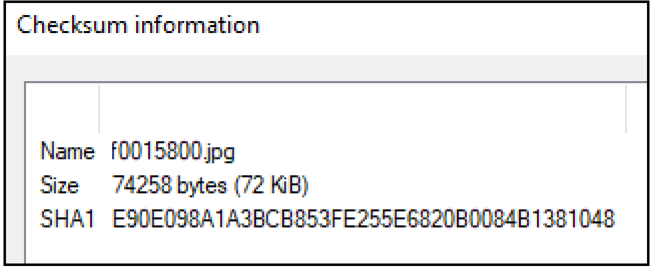
E90E098A1A3BCB853FE255E6820B0084B1381048

Expected Response Explanation:

A reliable file recovery or file tool can find deleted files in unallocated space.

Expected Response Illustration:

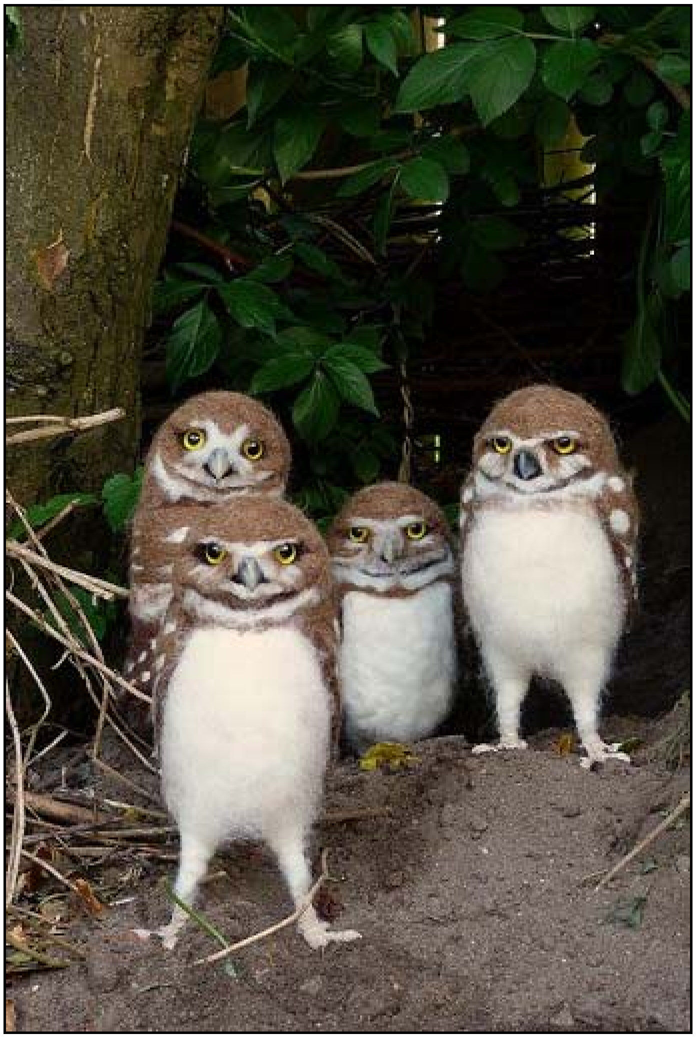
Checksum information via 7Zip



Checksum information

Name	f0015800.jpg
Size	74258 bytes (72 KiB)
SHA1	E90E098A1A3BCB853FE255E6820B0084B1381048

img_offset='8089600'

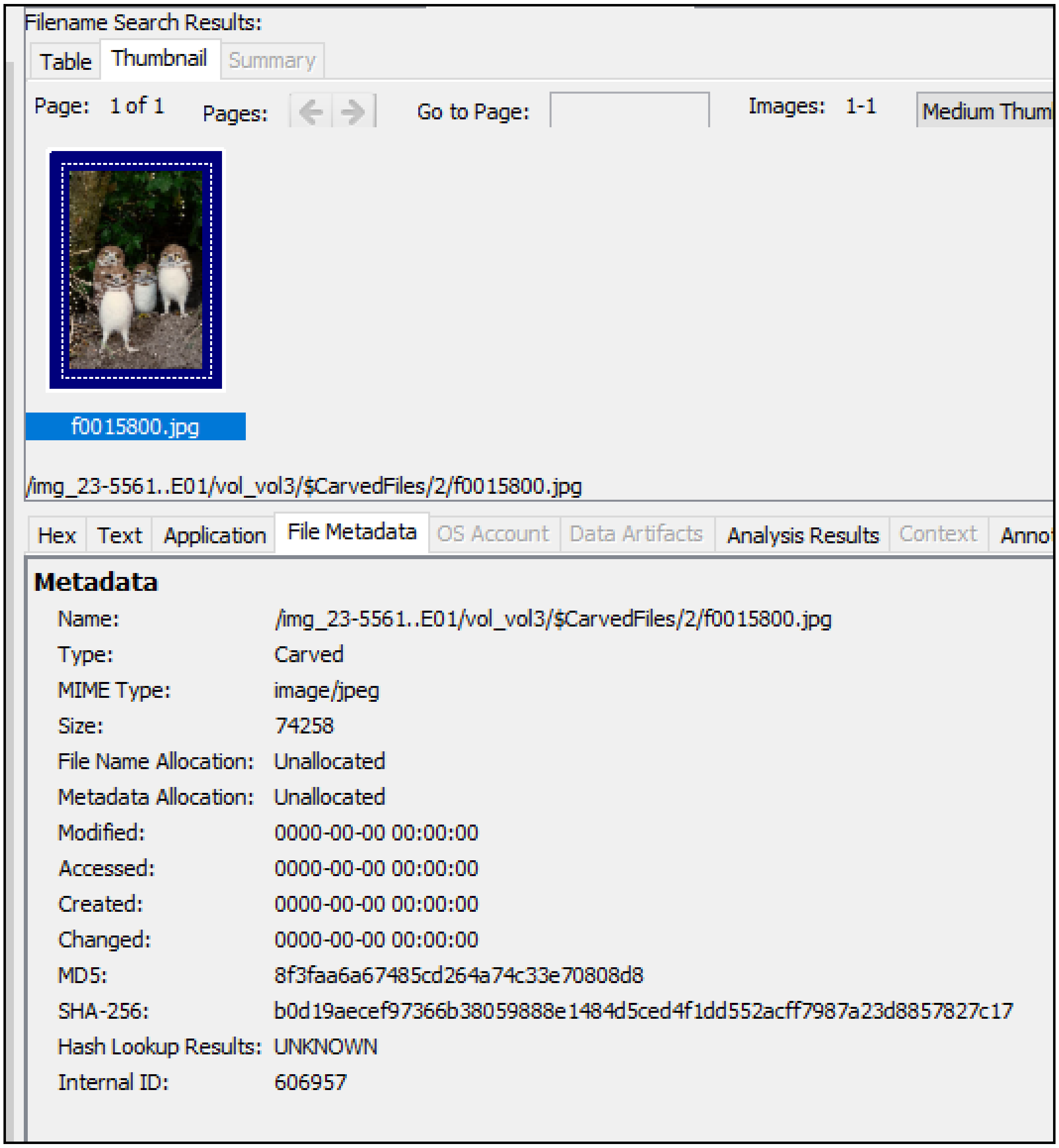


Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 30 - Examination Questions

Autopsy view of carved owl image



/img_23-5561..E01/vol_vol3/$CarvedFiles/2/f0015800.jpg

Metadata

Name:	/img_23-5561..E01/vol_vol3/$CarvedFiles/2/f0015800.jpg
Type:	Carved
MIME Type:	image/jpeg
Size:	74258
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	0000-00-00 00:00:00
Accessed:	0000-00-00 00:00:00
Created:	0000-00-00 00:00:00
Changed:	0000-00-00 00:00:00
MD5:	8f3faa6a67485cd264a74c33e70808d8
SHA-256:	b0d19aecef97366b38059888e1484d5ced4f1dd552acff7987a23d8857827c17
Hash Lookup Results:	UNKNOWN
Internal ID:	606957

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 31 - Examination Questions

Question 31: Locate the keyword that begins “Iera”, continues 6 letters, and ends “nae”. Provide the word and location (path and filename) where it is found. Please note, the keyword starts with a capital letter "I" like in the word 'India'. (e.g., ill, +6 letters, + ion, = illustration)

Manufacturer's Expected Response:	Word: Ieraglaucinae, Location: C:\Windows\System32\config\SOFTWARE:family\subfamily , OR C:\Windows\System32\config\SOFTWARE.log

WebCode Test	Response
2A9WQN-5561	Word: Ieraglaucinae, Location (path and filename): Windows/System32/config/SOFTWARE/family/subfamily
2P2VAR-5561	Word: Ieraglaucinae, Location (path and filename): 23-5561.LE01 - Partition 2 (Microsoft NTFS, 29.95 GB)\Windows\System32\config\SOFTWARE
2PJFNF-5562	Word: Ieraglaucinae, Location (path and filename): untitled\D\Windows\System32\config\SOFTWARE
2VQ8RL-5562	Word: Ieraglaucinae, Location (path and filename): Windows\System32\config\SOFTWARE.LOG1
2ZFN6X-5561	Word: Ieraglaucinae, Location (path and filename): /partition 2/NONAME [NTFS]/root]/Windows/System32/config/SOFTWARE.LOG1 - SOFTWARE.LOG1
3CDK6E-5562	Word: Ieraglaucinae, Location (path and filename): \Windows\System32\Config\Software
3DPEPK-5561	Word: Ieraglaucinae, Location (path and filename): C:\Windows\System32\config\Software
3M9X4P-5561	Word: Ieraglaucinae, Location (path and filename): \Windows\System32\config\SOFTWARE.LOG1
42BM2N-5561	Word: Ieraglaucinae, Location (path and filename): C:\windows\system32\config\software.Log1
48GFVJ-5561	Word: Ieraglaucinae, Location (path and filename): /Windows/System32/config/SOFTWARE
4U7ZP2-5562	Word: Ieraglaucinae, Location (path and filename): /Windows/System32/config/SOFTWARE.LOG1
649HZ6-5561	Word: Ieraglaucinae, Location (path and filename): Windows/System32/config/SOFTWARE
68RW46-5562	Word: Ieraglaucinae, Location (path and filename): Partition 2 (Microsoft NTFS, 29.95 GB)/Windows/System32/config/SOFTWARE/family/subfamily
6DZZCR-5561	Word: Ieraglaucinae, Location (path and filename): /Windows/System32/Config/Software
6MKCN6-5562	Word: Ieraglaucinae, Location (path and filename): Windows\System32\config\SOFTWARE\NTRegistry\ROOT\family\subfamily
6Q2RXW-5562	Word: Ieraglaucinae , Location (path and filename): Path: /Partition2/NONAME[NTFS]/[root]/Windows/System32/config/SOFTWARE, filename: SOFTWARE

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 31 - Examination Questions

WebCode Test	Response
6Q4JPC-5561	Word: leraglaucinae, Location (path and filename): 23-5561.E01 - Partition 2 (Microsoft NTFS, 29.95 GB)\Windows\System32\config\SOFTWARE.LOG1
6QKH3A-5562	Word: leraglaucinae, Location (path and filename): Windows\System32\config\SOFTWARE.LOG1
6TR3NP-5561	Word: leraglaucinae, Location (path and filename): Partition 2\Windows\System32\config\SOFTWARE.LOG1 (also in SOFTWARE)
72ZUTD-5561	Word: N/K, Location (path and filename): N/K
78PAK7-5562	Word: leraglaucinae, Location (path and filename): C:\Windows\System32\config\SOFTWARE\ROOT\family\subfamily
7JUP4F-5561	Word: lerglaucinae, Location (path and filename): root\windows\system32\config\software.log1
7PQ8PM-5562	Word: leraglaucinae, Location (path and filename): \Windows\System32\config\SOFTWARE.LOG1
7XZLMH-5562	Word: leraglaucinae, Location (path and filename): The word was found in two different locations: '\Windows\System32\config\SOFTWARE.reg' and '\Windows\System32\config\SOFTWARE.LOG1'
82VWX9-5562	Word: leraglaucinae, Location (path and filename): \Windows\System32\config\SOFTWARE
83AEYT-5562	Word: leraglaucinae, Location (path and filename): C:\Windows\System32\config\SOFTWARE\family\subfamily
8CB97J-5561	Word: leraglaucinae, Location (path and filename): Windows/System32/config/SOFTWARE
8LJ9TK-5561	Word: leraglaucinae, Location (path and filename): C:\Windows\System32\config\SOFTWARE.LOG1
96TUNQ-5561	Word: leraglaucinae , Location (path and filename): 23-5561.E01/Partition 2/NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE and 23-5561.E01/Partition 2/NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE.LOG1
98ZV8C-5561	Word: leraglaucinae, Location (path and filename): C:\Windows\System32\config\SOFTWARE\family\subfamily
99QBZK-5562	Word: ieraglaucinae, Location (path and filename): untitled\D\Windows\System32\config\SOFTWARE.LOG1
9AJ8JM-5561	Word: leraglaucinae, Location (path and filename): 23-5561.E01/Partition 2/NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE>>family>>subfamily
9J9Q8U-5562	Word: leraglaucinae, Location (path and filename): Windows\System32\config\SOFTWARE\family\subfamily
A8QHYB-5562	Word: leraglaucinae, Location (path and filename): 23-5561.E01 - Partition 2 (Microsoft NTFS, 29.95 GB)\Windows\System32\config\SOFTWARE
A8VQBZ-5561	Word: leraglaucinae, Location (path and filename): C:\Windows\System32\config\SOFTWARE

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 31 - Examination Questions

WebCode Test	Response
ABK3AJ-5561	Word: NOT IN SCOPE, Location (path and filename): NOT IN SCOPE
ACTERK-5561	Word: Not in Scope, Location (path and filename): Not in Scope
ADYU2Y-5562	Word: Tried the following regular expression, however no keyword matching the above question was found., Location (path and filename): \bIera\w+(?:\w+){1,6}?nae\b
AKG6BT-5562	Word: Ieraglaucinae, Location (path and filename): root\Windows\System32\config\SOFTWARE (Software registry hive)
AM94QQ-5561	Word: Ieraglaucinae, Location (path and filename): \Windows\System32\config\SOFTWARE
BFKZWF-5562	Word: Ieraglaucinae, Location (path and filename): Windows\System32\config\SOFTWARE.LOG1
BQRG78-5561	Word: Ieraglaucinae, Location (path and filename): [root]/Windows/System32/config/SOFTWARE»family»subfamily
C4LMC9-5562	Word: Ieraglaucinae, Location (path and filename): /Windows/System32/config/SOFTWARE
C897D8-5561	Word: Ierapetranae, Location (path and filename): /Users/David Lightman/Documents/SoreEnthusiasticElephant/CruelFierceWren.pdf
CF2CBE-5562	Word: Ieraglaucinae, Location (path and filename): Windows\System32\config\SOFTWARE.LOG1
CKAXYB-5561	Word: Ieraglaucinae, Location (path and filename): [root]/Windows/System32/config/SOFTWARE
CP6N6M-5561	Word: Ieraglaucinae, Location (path and filename): Windows/System32/config/SOFTWARE
D7PUVD-5561	Word: Ieraglaucinae, Location (path and filename): \Windows\system32\config\SOFTWARE - Regkey SOFTWARE\family
DB6AM4-5561	Word: Ieraglaucinae, Location (path and filename): C:\Windows\System32\config\SYSTEM
DGVH9K-5561	Word: Ieraglaucinae, Location (path and filename): C:\Windows\System32\config\SOFTWARE (registry Hive), within the registry hive, the path is Root\family\subfamily - Additionally, it is also found in the SOFTWARE.LOG1 file.
DXVP3C-5562	Word: Ieraglaucinae, Location (path and filename): \Windows\System32\Config\SOFTWARE.LOG1
E2RHRZ-5562	Word: Ieraglaucinae, Location (path and filename): \Windows\System32\config\SOFTWARE
E4ZNBG-5561	Word: Ieraglaucinae, Location (path and filename): \Windows\System32\config\SOFTWARE\ROOT\family\subfamily
EV7HHF-5561	Word: Ieraglaucinae, Location (path and filename): /Windows/System32/config/SOFTWARE
F3JVRX-5561	Word: Ieraglaucinae, Location (path and filename): C:/Windows/System32/config/SOFTWARE

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 31 - Examination Questions

WebCode Test	Response
FZVEJB-5561	Word: leraglaucinae, Location (path and filename): \Windows\System32\config\SOFTWARE
G973T4-5561	Word: leraglaucinae, Location (path and filename): Windows\System32\config\SOFTWARE.LOG1
GJ39KG-5561	[Participant did not return results for this question.]
GYTEQP-5561	Word: Unable to find, Location (path and filename): Unable to find
HQVXJW-5561	Word: leraglaucinae, Location (path and filename): C:\Windows\System32\config\SOFTWARE.LOG1
HUFQTD-5561	Word: leraglaucinae, Location (path and filename): C:\Windows\System32\config\SOFTWARE (hive -> family)
HW2LD2-5562	[Participant did not return results for this question.]
J84AQF-5562	Word: leraglaucinae, Location (path and filename): C:\Windows\System32\config\software.log
JE9W33-5561	Word: leraglaucinae, Location (path and filename): C\Windows\System32\config\SOFTWARE\ROOT\family\subfamily
JGBUAC-5562	Word: leraglaucinae, Location (path and filename): File Path: Partition 2 - \Windows\System32\config\SOFTWARE\family Also there are positive hits in the following; File Path: Partition 2 - \Windows\System32\config\SOFTWARE.LOG1
JJDU63-5561	Word: leraglaucinae, Location (path and filename): /Windows/System32/config/SOFTWARE
JL32PY-5562	Word: Leraglaucinae, Location (path and filename): C:/windows/system32/config/software
JLRZA6-5561	Word: leraglaucinae, Location (path and filename): Windows\System32\config\SOFTWARE.LOG1
JPKFX7-5561	Word: leraglancinae, Location (path and filename): c:/windows/system32/config/software/.log1
KR28JR-5562	Word: leraglaucinae, Location (path and filename): C:\Windows\System32\config\SOFTWARE\SOFTWARE\ROOT\family\subfamily
KR4V3R-5561	Word: leraglaucinae, Location (path and filename): Partition 2 [C:]\Windows\System32\config\SOFTWARE > \family\subfamily
KXRBW6-5562	Word: leraglaucinae, Location (path and filename): \Windows\system32\config\SOFTWARE - Regkey SOFTWARE\family
KZVDDT-5561	Word: leraglaucinae, Location (path and filename): C\Windows\System32\config\SOFTWARE\family
LDKC3B-5561	Word: leraglaucinae, Location (path and filename): Windows/System32/config/SOFTWARE
M9HYHY-5561	Word: leraglaucinae, Location (path and filename): Windows/System32/config/SOFTWARE.LOG1
MF4Q7B-5561	Word: leraglaucinae, Location (path and filename): Partition 2/NONAME [NTFS]/[root]/Windows/System32/Config/SOFTWARE

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 31 - Examination Questions

WebCode Test	Response
MF8B24-5561	Word: leraglaucinae, Location (path and filename): Windows\System32\config\SOFTWARE
NADTWE-5561	Word: leraglaucinae, Location (path and filename): \Windows\System32\config\SOFTWARE.LOG1
NE7TEF-5562	Word: leraglaucinae, Location (path and filename): D:\Windows\System32\config\SOFTWARE
NTANM4-5561	Word: leraglaucinae, Location (path and filename): Windows\System32\config\SOFTWARE
NTZJR4-5561	Word: leraglaucinae, Location (path and filename): Root\Windows\System32\Config\SOFTWARE
P3ACZC-5561	Word: leraglaucinae, Location (path and filename): C:/Windows/System32/config/Software/family
P79FU7-5561	Word: leraglaucinae, Location (path and filename): /Windows/System32/config/SOFTWARE
P8ZNUA-5561	Word: leraglaucinae, Location (path and filename): C:\Windows\System32\config\SOFTWARE\family\subfamily
PFEMA7-5562	Word: leraglaucinae, Location (path and filename): /Windows/System32/config/SOFTWARE/ROOT/family/subfamily
PFVN93-5561	Word: leraglaucinae, Location (path and filename): C:\Windows\System32\config\SOFTWARE.LOG1; SOFTWARE.LOG1
PLGGK2-5561	Word: leraglaucinae, Location (path and filename): /Windows/System32/Config/SOFTWARE
PPMYM4-5562	Word: leraglaucinae, Location (path and filename): untitled\D\Windows\System32\config\SOFTWARE
PTKDEZ-5562	Word: leraglaucinae, Location (path and filename): Windows\System32\config\SOFTWARE
PUTRGY-5561	Word: leraglaucinae, Location (path and filename): Windows\System32\config\SOFTWARE.LOG1
PWJXV6-5561	Word: leraglaucinae, Location (path and filename): Windows/system32/config/SOFTWARE.LOG1
Q2CFQV-5561	Word: leraglaucinae, Location (path and filename): C:\Windows\System32\config\SOFTWARE,C:\Windows\System32\config\SOFTWARE.LOG1
Q33NQX-5561	Word: leraglaucinae, Location (path and filename): \Windows\System32\config\SOFTWARE, \Windows\System32\config\SOFTWARE.LOG1
Q3RHY2-5561	Word: leraglaucinae, Location (path and filename): c:\Windows\System32\config\Software\family
QMR3Q2-5561	Word: leraglaucinae, Location (path and filename): D\Windows\System32\config\SOFTWARE
QRJAR3-5561	Word: leraglaucinae, Location (path and filename): /Windows/System32/config/SOFTWARE

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 31 - Examination Questions

WebCode Test	Response
QTHAXU-5561	Word: leraglaucinae, Location (path and filename): /Windows/System32/config/SOFTWARE.LOG1
RAK67E-5562	Word: leraglaucinae, Location (path and filename): Windows\System32\config\SOFTWARE
RBBDCA-5562	Word: leraglaucinae, Location (path and filename): SOFTWARE Registry Hive (\Windows\System32\config). Also present 16 times in SOFTWARE.LOG1 (\Windows\System32\config).
RGH4EF-5562	Word: leraglaucinae, Location (path and filename): File location #1: C\Windows\System32\config\SOFTWARE File location #2: C\Windows\System32\config\SOFTWARE.LOG1
RRMUMV-5561	Word: leraglaucinae , Location (path and filename): 23-5561.E01\Partition @ 104448\Root\Windows\System32\config\SOFTWARE\family\subfamily
RRXTDK-5562	Word: leraglaucinae, Location (path and filename): Windows/System32/config/SOFTWARE AND Windows/System32/config/SOFTWARE.LOG1
RV3JKZ-5561	Word: leraglaucinae, Location (path and filename): Windows\System32\config\SOFTWARE.LOG1
TC4JAF-5562	Word: leraglaucinae, Location (path and filename): Path: C:\Windows\System32\config\ Filename: SOFTWARE
TCGEBD-5561	Word: leraglaucinae, Location (path and filename): C:\Windows\System32\config\SOFTWARE
TEPC2R-5562	Word: leraglaucinae, Location (path and filename): /Windows/System32/config/SOFTWARE.LOG1
TKFNZV-5561	Word: leraglaucinae, Location (path and filename): /Windows/System32/config/SOFTWARE.LOG1
TNEXBT-5561	Word: leraglaucinae, Location (path and filename): \Windows\System32\config\SOFTWARE.LOG1
TVF9MD-5562	Word: leraglaucinae, Location (path and filename): \Windows\System32\config\SOFTWARE
TX22EP-5561	Word: leraglaucinae, Location (path and filename): C:/Windows/System32/config/SOFTWARE
U3RQC6-5561	Word: leraglaucinae, Location (path and filename): C:\Windows\System32\config\SOFTWARE, Adobe Acrobat
UKBK6E-5561	Word: nae, Location (path and filename): \Users\David Lightman\Documents\FragileShinyJellyfish\JoyousSillyHedgehog.dat
URA8XZ-5561	Word: leraglaucinae, Location (path and filename): untitled\D\Windows\System32\config\SOFTWARE
UVZCUQ-5562	Word: leraglaucinae, Location (path and filename): \Windows\System32\config\SOFTWARE
V4KY4K-5562	Word: leraglaucinae, Location (path and filename): Users\David Lightman\AppData\Local\Google\Chrome\User Data\ZxcvbnData\3\us_tv_and_film.txt

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 31 - Examination Questions

WebCode Test	Response
VCE6WL-5561	Word: leraglaucinae, Location (path and filename): 23-5561.E01/Partition 2/NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE and in the log with the path 23-5561.E01/Partition 2/NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE.LOG1
VJH9N7-5561	Word: leraglaucinae, Location (path and filename): \Windows\System32\config\SOFTWARE (There is a file named "SOFTWARE.LOG1" in the file location \Windows\System32\config\ which also contains the keyword "leraglaucinae".)
VTZR3B-5561	Word: leraglaucinae, Location (path and filename): untitled\D\Windows\System32\config\SOFTWARE\ family\subfamily
VVVB8V-5561	Word: leraglaucinae, Location (path and filename): \Windows\System32\config\SOFTWARE
WC9E49-5561	[Participant did not return results for this question.]
WD8DHB-5561	Word: leraglaucinae, Location (path and filename): C:\Windows\System32\config\SOFTWARE
WK4CUH-5561	Word: leraglaucinae, Location (path and filename): C:\Windows\System32\config\SOFTWARE (registry file, in the /family/subfamily key) and C:\Windows\System32\config\SOFTWARE.log1
WNN64Y-5561	Word: leraglaucinae, Location (path and filename): Windows\System32\config\SOFTWARE\family (HKLM\SOFTWARE\family)
WX2YKZ-5561	Word: Not currently within scope of the lab., Location (path and filename): Not currently within scope of the lab.
WZGLVL-5562	Word: leraglaucinae, Location (path and filename): Windows\System32\config\SOFTWARE.LOG1
XA2A8Z-5562	Word: leraglaucinae, Location (path and filename): 23-5561.E01 - Partition 2 (Microsoft NTFS, 29.95 GB)\Windows\System32\config\SOFTWARE.LOG1
XEVDXV-5561	Word: Not in scope, Location (path and filename): Not in scope
XJ99G2-5562	Word: leraglaucinae, Location (path and filename): \Windows\System32\config\SOFTWARE\family-subfamily
XQ9B22-5561	Word: leraglaucinae, Location (path and filename): 23-5561.e01\Partition 2\NONAME [NTFS]\[root]\Windows\System32\config\SOFTWARE
XVDHZK-5562	[Participant did not return results for this question.]
XWDAB7-5561	Word: leraglaucinae, Location (path and filename): C:\Windows\System32\config\SOFTWARE (family:subfamily)
XX78KX-5561	Word: leraglaucinae, Location (path and filename): 23-5561.E01/Partition 2/NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE.LOG1
Y63G92-5562	Word: leraglaucinae, Location (path and filename): Windows\system32\config\SOFTWARE.LOG1 file

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 31 - Examination Questions

WebCode Test	Response
YDJQ3P-5561	Word: leraglaucinae, Location (path and filename): \Windows\System32\Config\SOFTWARE.LOG1
YPNENR-5562	Word: leraglaucinae, Location (path and filename): Windows\System32\config\SOFTWARE.LOG1
ZPR26J-5561	Word: leraglaucinae, Location (path and filename): C:\Windows\System32\config\SOFTWARE

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 31 - Examination Questions

Question 31: Locate the keyword that begins "Iera", continues 6 letters, and ends "nae". Provide the word and location (path and filename) where it is found. Please note, the keyword starts with a capital letter "I" like in the word 'India'. (e.g., ill, +6 letters, + ion, = illustration)

Consensus Result:

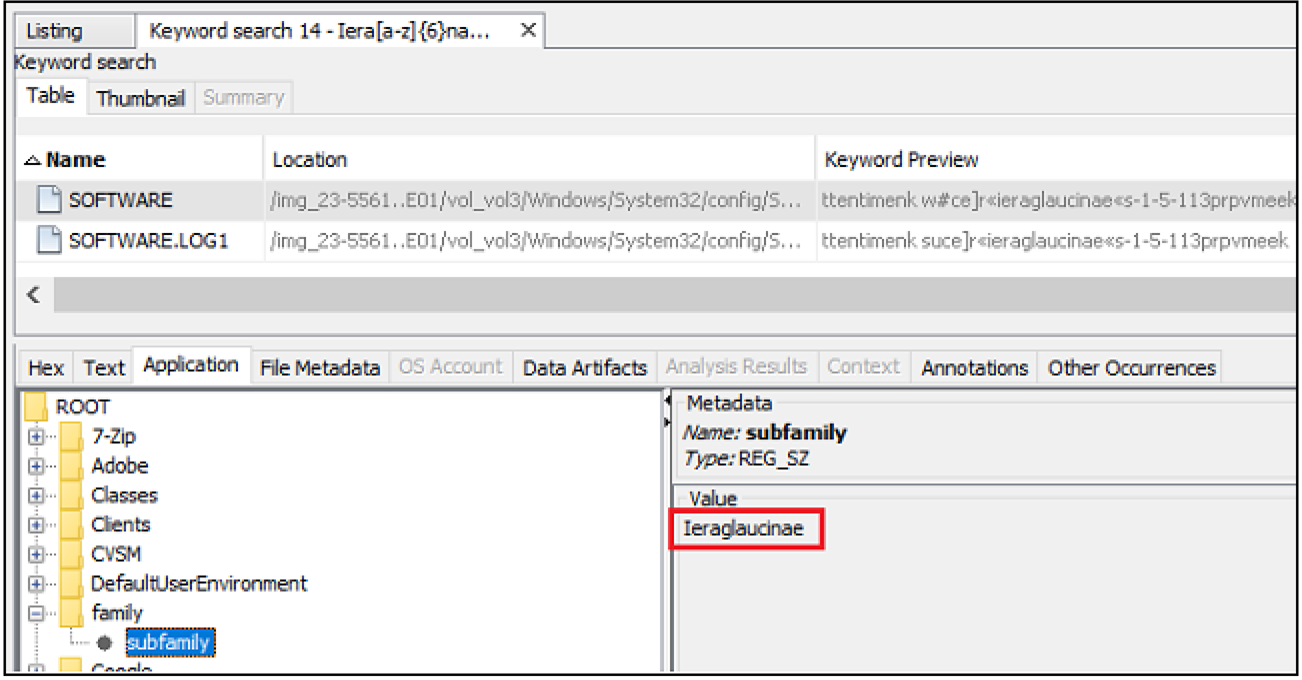
Word: Ieraglaucinae and any slight variation easily identified as a spelling error,
Location: C:\Windows\System32\config\SOFTWARE:family\subfamily , OR
C:\Windows\System32\config\SOFTWARE.log

Expected Response Explanation:

This keyword can be found with a regular expression, i.e. Iera[a-z]{6}nae , or simply, Iera......nae
This value is stored in the SOFTWARE registry key \family\subfamily. It also appears in the log file for the SOFTWARE hive.

Expected Response Illustration:

Autopsy view of C:\Windows\System32\config\SOFTWARE:family\subfamily

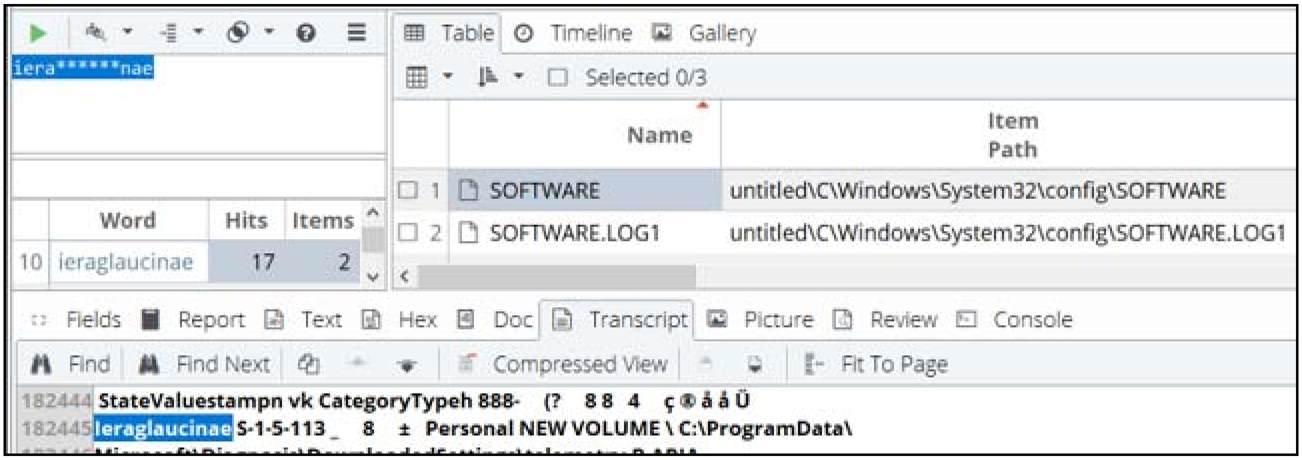


Name	Location	Keyword Preview
SOFTWARE	/img_23-5561..E01/vol_vol3/Windows/System32/config/S...	ttentimenk w#ce]r«ieraglaucinae«s-1-5-113prpvmeek
SOFTWARE.LOG1	/img_23-5561..E01/vol_vol3/Windows/System32/config/S...	ttentimenk suce]r«ieraglaucinae«s-1-5-113prpvmeek

Metadata
Name: **subfamily**
Type: REG_SZ

Value
Ieraglaucinae

EnCase view of C:\Windows\System32\config\SOFTWARE



	Word	Hits	Items
10	ieraglaucinae	17	2

	Name	Item Path
□ 1	SOFTWARE	untitled\C\Windows\System32\config\SOFTWARE
□ 2	SOFTWARE.LOG1	untitled\C\Windows\System32\config\SOFTWARE.LOG1

```
182444 StateValuestampn vk CategoryTypeh 888-   (?   8 8  4   ç ® å å Ü
182445 Ieraglaucinae S-1-5-113 _   8   ±  Personal NEW VOLUME \ C:\ProgramData\
```

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 32 - Examination Questions

Question 32: According to user David Lightman's registry hive 'most recently used' records, what "Rich Text File" did he open?

Manufacturer's Expected Response: superpostiion.rtf

WebCode Test	Response
2A9WQN-5561	superpostiion.rtf
2P2VAR-5561	superpostiion.rtf
2PJFNF-5562	superpostiion.rtf
2VQ8RL-5562	superpostiion.rtf
2ZFN6X-5561	superposition.rtf
3CDK6E-5562	superpostiion.rtf
3DPEPK-5561	Superpostiion.rtf
3M9X4P-5561	superposition.rtf
42BM2N-5561	C:\Users\David Lightman\Documents\superpostiion.rtf
48GFVJ-5561	superpostiion.rtf
4U7ZP2-5562	superpostiion.rtf
649HZ6-5561	superpostiion.rtf
68RW46-5562	superpostiion.rtf
6DZZCR-5561	Superpostiion.rtf
6MKCN6-5562	superpostiion.rtf
6Q2RXW-5562	superpostiion.rtf
6Q4JPC-5561	Superposition.rtf
6QKH3A-5562	superpostiion.rtf
6TR3NP-5561	My Computer (Computer)\d3162b92-9365-467a-956b-92703aca08af\superpostiion.rtf

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 32 - Examination Questions

WebCode Test	Response
72ZUTD-5561	superpostiion.rtf
78PAK7-5562	superpostiion.rtf
7JUP4F-5561	superpostiion.rtf
7PQ8PM-5562	superpostiion.rtf
7XZLMH-5562	superpostiion.rtf
82VWX9-5562	superpostiion.rtf
83AEYT-5562	superpostiion.rtf
8CB97J-5561	superpostiion.rtf
8LJ9TK-5561	superpostiion.rtf
96TUNQ-5561	superpostiion.rtf
98ZV8C-5561	superpostiion.rtf
99QBZK-5562	superpostiion.rtf
9AJ8JM-5561	superposition.rtf
9J9Q8U-5562	superpostiion.rtf
A8QHYB-5562	superpostiion.rtf
A8VQBZ-5561	superpostiion.rtf
ABK3AJ-5561	NOT IN SCOPE
ACTERK-5561	Not in Scope
ADYU2Y-5562	superpostiion.rtf
AKG6BT-5562	superpostiion.rtf
AM94QQ-5561	superpostiion.rtf

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 32 - Examination Questions

WebCode Test	Response
BFKZWF-5562	Superpostiion.rtf
BQRG78-5561	superpostiion.rtf
C4LMC9-5562	/Users/David Lightman/Documents/superpostiion.rtf
C897D8-5561	superpostiion.rtf
CF2CBE-5562	superpostiion.rtf
CKAXYB-5561	superpostiion.rtf
CP6N6M-5561	superpostiion.rtf
D7PUVD-5561	superpostiion.rtf
DB6AM4-5561	superposition.rtf
DGVH9K-5561	superpostiion.rtf
DXVP3C-5562	superposition.rtf
E2RHRZ-5562	superpostiion.rtf
E4ZNBG-5561	superpostiion.rtf
EV7HHF-5561	superpostiion.rtf
F3JVRX-5561	superposition.rtf
FZVEJB-5561	superposition.rtf
G973T4-5561	Superpostiion.rtf
GJ39KG-5561	superpostiion.rtf
GYTEQP-5561	superpostiion.rtf
HQVXJW-5561	superpostiion.rtf
HUFQTD-5561	superpostiion.rtf

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 32 - Examination Questions

WebCode Test	Response
HW2LD2-5562	[Participant did not return results for this question.]
J84AQF-5562	superpostiion.rtf
JE9W33-5561	superpostiion.rtf
JGBUAC-5562	superpostiion.rtf
JJDU63-5561	superpostiion.rtf
JL32PY-5562	superpostiion.rtf
JLRZA6-5561	superpostiion.rtf
JPKFX7-5561	superpostiion.rtf
KR28JR-5562	superpostiion.rtf
KR4V3R-5561	superpostiion.rtf
KXRBW6-5562	superpostiion.rtf
KZVDDT-5561	superpostiion.rtf
LDKC3B-5561	superposition.rtf
M9HYHY-5561	superpostiion.rtf
MF4Q7B-5561	superpostiion.rtf
MF8B24-5561	superpostiion.rtf
NADTWE-5561	superposition.rtf
NE7TEF-5562	superpostiion.rtf
NTANM4-5561	superpostiion.rtf
NTZJR4-5561	superpostiion.rtf
P3ACZC-5561	superposition.rtf

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 32 - Examination Questions

WebCode Test	Response
P79FU7-5561	superpostiion.rtf
P8ZNUA-5561	superpostiion.rtf
PFEMA7-5562	superpostiion.rtf
PFVN93-5561	superposition.rtf
PLGGK2-5561	superpostiion.rtf
PPMYM4-5562	Superposition.rtf
PTKDEZ-5562	superpostiion.rtf
PUTRGY-5561	Superpostiion.rtf
PWJXV6-5561	Superpostiion.rtf
Q2CFQV-5561	C:\Users\David Lightman\Documents\superpostiion.rtf
Q33NQX-5561	superpostiion.rtf
Q3RHY2-5561	superpostiion.rtf
QMR3Q2-5561	Superposition.rtf
QRJAR3-5561	superpostiion.rtf
QTHAXU-5561	superpostiion.rtf
RAK67E-5562	superpostiion.rtf
RBBDCA-5562	superpostiion.rtf
RGH4EF-5562	superpostiion.rtf
RRMUMV-5561	superpostiion.rtf
RRXTDK-5562	superpostiion.rtf
RV3JKZ-5561	Superpostiion.rtf

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 32 - Examination Questions

WebCode Test	Response
TC4JAF-5562	superpostiion.rtf
TCGEBD-5561	superpostiion.rtf
TEPC2R-5562	superpostiion.rtf
TKFNZV-5561	superpostiion.rtf
TNEXBT-5561	superpositiion.rtf
TVF9MD-5562	superpostiion.rtf
TX22EP-5561	superpostiion.rtf
U3RQC6-5561	Superposition.rtf
UKBK6E-5561	My Computer\Documents\superpostiion.rtf
URA8XZ-5561	superpostiion.rtf
UVZCUQ-5562	superpostiion.rtf
V4KY4K-5562	superpostiion.rtf
VCE6WL-5561	superpostiion.rtf
VJH9N7-5561	superpostiion.rtf
VTZR3B-5561	superpostiion.rtf
VVVB8V-5561	superpostiion.rtf
WC9E49-5561	Superpostiion.rtf
WD8DHB-5561	superpostiion.rtf
WK4CUH-5561	superpostiion.rtf
WNN64Y-5561	superpostiion.rtf
WX2YKZ-5561	Not currently within scope of the lab.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 32 - Examination Questions

WebCode Test	Response
WZGLVL-5562	superpostiion.rtf
XA2A8Z-5562	superpostiion.rtf
XEVDXV-5561	Not in scope
XJ99G2-5562	superpostiion.rtf
XQ9B22-5561	Superposition.rtf
XVDHZK-5562	[Participant did not return results for this question.]
XWDAB7-5561	superpostiion.rtf
XX78KX-5561	superpostiion.rtf
Y63G92-5562	superpostiion.rtf
YDJQ3P-5561	superposition.rtf
YPNENR-5562	Superpostiion.rtf
ZPR26J-5561	superpostiion.rtf

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 32 - Examination Questions

Question 32: According to user David Lightman's registry hive 'most recently used' records, what "Rich Text File" did he open?

Consensus Result:

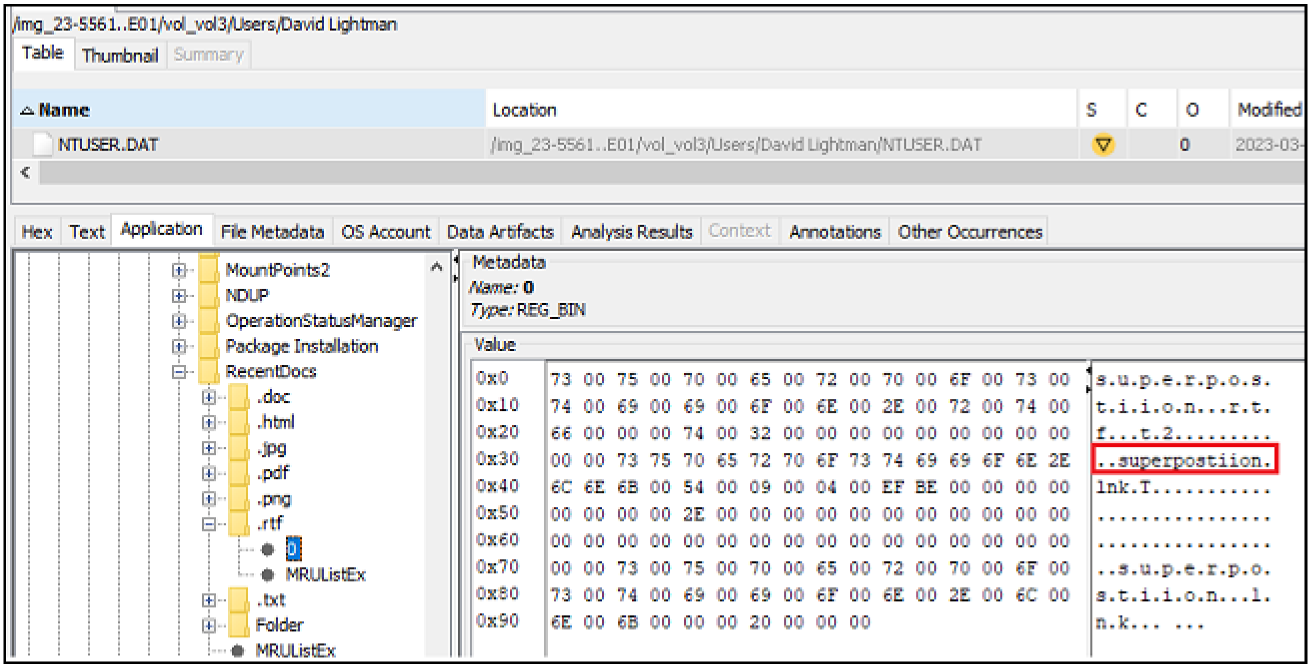
"superpostiion.rtf" and slight variations.

Expected Response Explanation:

A user's NTUSER.DAT registry hive contains a record of used files most recent opened with Windows explorer at NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs.

Expected Response Illustration:

Autopsy view of C:\Users\David Lightman\NTUSER.DAT: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs



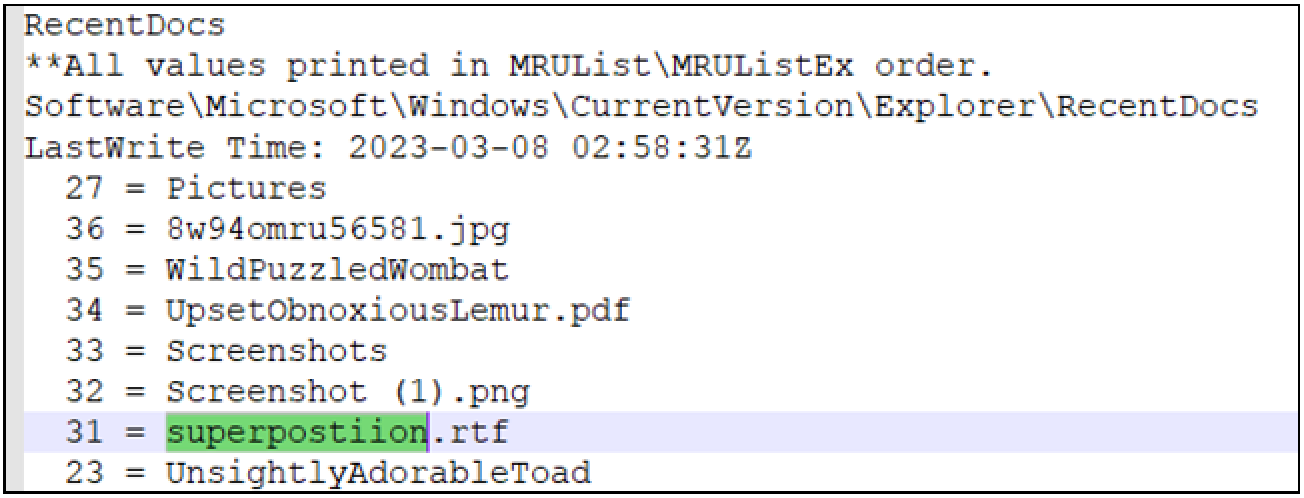
Name	Location	S	C	O	Modified
NTUSER.DAT	/img_23-5561..E01/vol_vol3/Users/David Lightman/NTUSER.DAT	▽		0	2023-03-

Metadata
Name: **0**
Type: REG_BIN

Value

```
0x0   73 00 75 00 70 00 65 00 72 00 70 00 6F 00 73 00   s.u.p.e.r.p.o.s.
0x10  74 00 69 00 69 00 6F 00 6E 00 2E 00 72 00 74 00   t.i.i.o.n...r.t.
0x20  66 00 00 00 74 00 32 00 00 00 00 00 00 00 00 00   f...t.2.........
0x30  00 00 73 75 70 65 72 70 6F 73 74 69 69 6F 6E 2E   ..superpostiion.
0x40  6C 6E 6B 00 54 00 09 00 04 00 EF BE 00 00 00 00   lnk.T...........
0x50  00 00 00 00 2E 00 00 00 00 00 00 00 00 00 00 00   ................
0x60  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x70  00 00 73 00 75 00 70 00 65 00 72 00 70 00 6F 00   ..s.u.p.e.r.p.o.
0x80  73 00 74 00 69 00 69 00 6F 00 6E 00 2E 00 6C 00   s.t.i.i.o.n...l.
0x90  6E 00 6B 00 00 00 20 00 00 00                     n.k... ...
```

RegRipper parse of C:\Users\David Lightman\NTUSER.DAT: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs



```
RecentDocs
**All values printed in MRUList\MRUListEx order.
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
LastWrite Time: 2023-03-08 02:58:31Z
  27 = Pictures
  36 = 8w94omru56581.jpg
  35 = WildPuzzledWombat
  34 = UpsetObnoxiousLemur.pdf
  33 = Screenshots
  32 = Screenshot (1).png
  31 = superpostiion.rtf
  23 = UnsightlyAdorableToad
```

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 33 - Examination Questions

Question 33: According to the data IN the associated prefetch file, when was NOTEPAD.exe LAST executed? Provide your response in UTC+0, using the date/time (24-hour) picker which presents the date in the following format: YYYY-MM-DD.

Manufacturer's Expected Response: 2023-03-08 00:21

WebCode Test	Response
2A9WQN-5561	2023-03-08 00:21
2P2VAR-5561	2023-03-08 00:21
2PJFNF-5562	2023-03-08 00:21
2VQ8RL-5562	2023-03-08 00:21
2ZFN6X-5561	2023-03-08 00:21
3CDK6E-5562	2023-03-08 00:21
3DPEPK-5561	2023-03-08 00:21
3M9X4P-5561	2023-03-08 00:21
42BM2N-5561	2023-03-08 00:21
48GFVJ-5561	2023-03-08 00:21
4U7ZP2-5562	2023-03-08 00:21
649HZ6-5561	2023-03-08 00:21
68RW46-5562	2023-03-08 00:21
6DZZCR-5561	2023-03-08 00:21
6MKCN6-5562	2023-03-08 00:21
6Q2RXW-5562	2023-03-08 00:21
6Q4JPC-5561	2023-03-08 12:21
6QKH3A-5562	2023-03-08 00:21

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 33 - Examination Questions

WebCode Test	Response
6TR3NP-5561	2023-03-08 00:21
72ZUTD-5561	2023-03-08 00:21
78PAK7-5562	2023-03-08 00:21
7JUP4F-5561	2023-03-08 00:21
7PQ8PM-5562	2023-03-08 00:21
7XZLMH-5562	2023-03-08 00:21
82VWX9-5562	2023-03-08 00:21
83AEYT-5562	2023-03-08 00:21
8CB97J-5561	2023-03-08 00:21
8LJ9TK-5561	2023-03-08 00:21
96TUNQ-5561	2023-03-08 00:21
98ZV8C-5561	2023-03-08 00:21
99QBZK-5562	2023-03-23 00:21
9AJ8JM-5561	2023-03-08 00:21
9J9Q8U-5562	2023-03-07 23:21
A8QHYB-5562	2023-03-08 00:21
A8VQBZ-5561	2023-03-08 00:21
ABK3AJ-5561	[Participant did not return results for this question.]
ACTERK-5561	[Participant did not return results for this question.]
ADYU2Y-5562	2023-03-08 00:21
AKG6BT-5562	2023-03-08 00:21

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 33 - Examination Questions

WebCode Test	Response
AM94QQ-5561	2023-03-08 00:21
BFKZWF-5562	2023-03-08 00:21
BQRG78-5561	2023-03-08 00:21
C4LMC9-5562	2023-03-08 00:21
C897D8-5561	2023-03-08 00:21
CF2CBE-5562	2023-03-08 00:21
CKAXYB-5561	2023-03-08 00:21
CP6N6M-5561	2023-03-08 00:21
D7PUVD-5561	2023-03-08 05:21
DB6AM4-5561	2023-03-08 00:21
DGVH9K-5561	2023-03-07 12:21
DXVP3C-5562	2023-03-08 00:21
E2RHRZ-5562	2023-03-08 00:21
E4ZNBG-5561	2023-03-08 00:21
EV7HHF-5561	2023-03-08 00:21
F3JVRX-5561	2023-03-08 00:21
FZVEJB-5561	2023-03-08 00:21
G973T4-5561	2023-06-23 00:21
GJ39KG-5561	2023-03-08 12:21
GYTEQP-5561	2023-03-08 00:21
HQVXJW-5561	2023-03-08 00:21

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 33 - Examination Questions

WebCode Test	Response
HUFQTD-5561	2023-03-08 00:21
HW2LD2-5562	[Participant did not return results for this question.]
J84AQF-5562	2023-03-08 05:21
JE9W33-5561	2023-03-08 00:21
JGBUAC-5562	2023-03-08 21:16
JJDU63-5561	2023-03-08 12:21
JL32PY-5562	2023-03-08 00:21
JLRZA6-5561	2023-03-08 00:21
JPKFX7-5561	2023-03-08 01:21
KR28JR-5562	2023-03-08 00:21
KR4V3R-5561	2023-03-08 00:21
KXRBW6-5562	2023-03-08 05:21
KZVDDT-5561	2023-03-08 00:21
LDKC3B-5561	2023-03-07 14:32
M9HYHY-5561	2023-03-08 00:21
MF4Q7B-5561	2023-03-08 12:21
MF8B24-5561	2023-03-08 00:21
NADTWE-5561	2023-03-08 00:21
NE7TEF-5562	2023-03-08 00:21
NTANM4-5561	2023-03-08 00:21
NTZJR4-5561	2023-03-08 00:21

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 33 - Examination Questions

WebCode Test	Response
P3ACZC-5561	2023-03-08 00:21
P79FU7-5561	2023-03-08 21:16
P8ZNUA-5561	2023-03-08 12:21
PFEMA7-5562	2023-03-08 00:21
PFVN93-5561	2023-03-08 00:21
PLGGK2-5561	2023-03-08 05:21
PPMYM4-5562	2022-03-08 00:21
PTKDEZ-5562	2023-03-08 00:21
PUTRGY-5561	2023-03-08 00:21
PWJXV6-5561	2023-03-08 00:21
Q2CFQV-5561	2023-03-08 21:16
Q33NQX-5561	2023-03-08 00:21
Q3RHY2-5561	2023-03-08 00:21
QMR3Q2-5561	2023-03-08 00:20
QRJAR3-5561	2023-03-08 00:21
QTHAXU-5561	2023-03-08 00:21
RAK67E-5562	2023-03-08 00:21
RBBDCA-5562	2023-05-08 00:21
RGH4EF-5562	2023-03-08 00:21
RRMUMV-5561	2023-03-08 00:21
RRXTDK-5562	2023-03-08 00:21

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 33 - Examination Questions

WebCode Test	Response
RV3JKZ-5561	2023-03-08 00:21
TC4JAF-5562	2023-03-08 00:21
TCGEBD-5561	2023-03-08 12:21
TEPC2R-5562	2023-03-08 00:21
TKFNZV-5561	2023-03-08 00:21
TNEXBT-5561	2023-03-08 00:21
TVF9MD-5562	2023-03-08 00:21
TX22EP-5561	2023-03-08 00:21
U3RQC6-5561	2023-03-08 00:21
UKBK6E-5561	2023-03-08 09:21
URA8XZ-5561	2023-03-08 00:21
UVZCUQ-5562	2023-03-08 00:21
V4KY4K-5562	2023-03-08 00:21
VCE6WL-5561	2023-03-08 00:21
VJH9N7-5561	2023-03-08 00:21
VTZR3B-5561	2023-03-08 00:21
VVVB8V-5561	2023-03-08 00:21
WC9E49-5561	2023-03-08 00:21
WD8DHB-5561	2023-03-08 00:21
WK4CUH-5561	2023-03-08 00:21
WNN64Y-5561	2023-03-08 00:21

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 33 - Examination Questions

WebCode Test	Response
WX2YKZ-5561	[Participant did not return results for this question.]
WZGLVL-5562	2023-03-08 00:21
XA2A8Z-5562	2023-03-08 12:21
XEVDXV-5561	[Participant did not return results for this question.]
XJ99G2-5562	2023-03-08 00:21
XQ9B22-5561	2023-03-08 00:21
XVDHZK-5562	[Participant did not return results for this question.]
XWDAB7-5561	2023-03-08 00:21
XX78KX-5561	2023-03-08 12:21
Y63G92-5562	2023/03/08 00.21
YDJQ3P-5561	2023-03-08 00:21
YPNENR-5562	2023-03-08 00:21
ZPR26J-5561	2023-03-08 00:21

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 33 - Examination Questions

Question 33: According to the data IN the associated prefetch file, when was NOTEPAD.exe LAST executed? Provide your response in UTC+0, using the date/time (24-hour) picker which presents the date in the following format: YYYY-MM-DD.

Consensus Result:

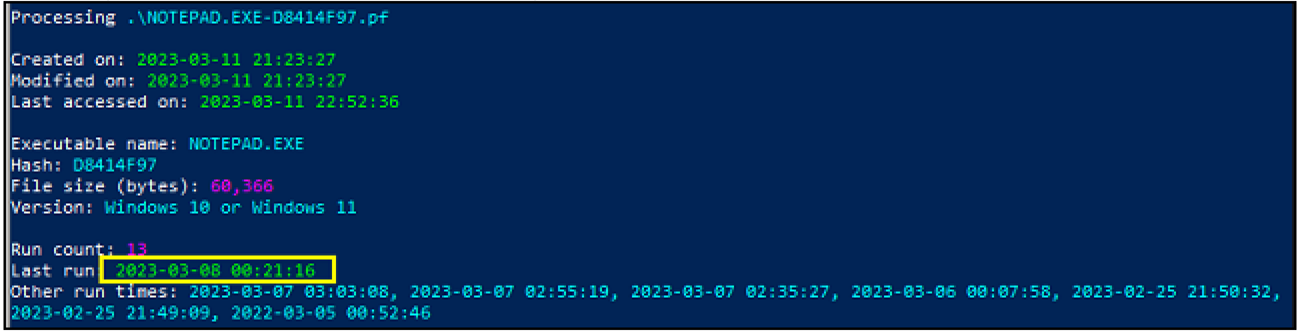
2023-03-08 00:21

Expected Response Explanation:

Prefetch analysis is used to determine program execution details. There is one prefetch file for NOTEPAD.EXE in C:\Windows\Prefetch, NOTEPAD.EXE-D8414F97.pf. Analysis of this file with PECmd (Prefetch Explorer Cmd) or the PFDump EnScript for EnCase indicates NOTEPAD.EXE was last executed 2023-03-08 00:21:16.

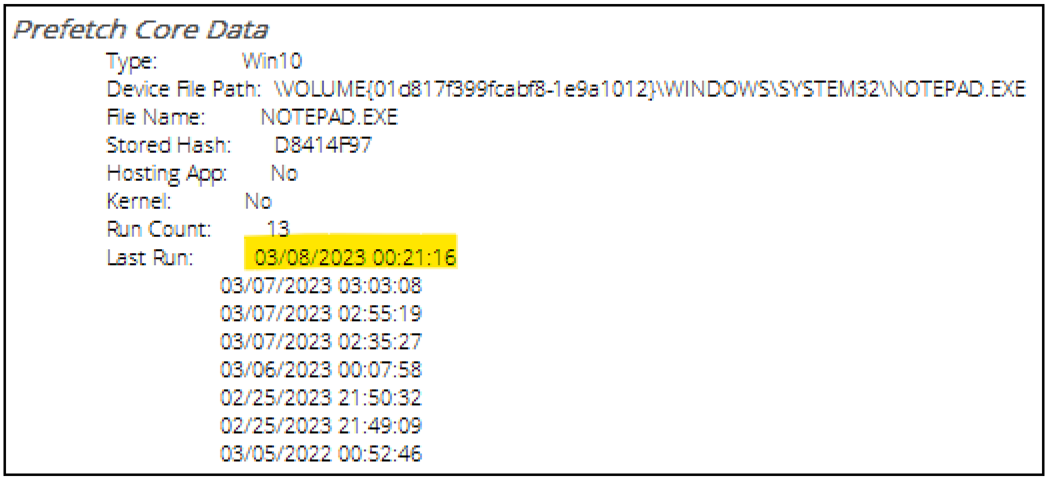
Expected Response Illustration:

PECMD parse of NOTEPAD.EXE-D8414F97.pf



```
Processing .\NOTEPAD.EXE-D8414F97.pf

Created on: 2023-03-11 21:23:27
Modified on: 2023-03-11 21:23:27
Last accessed on: 2023-03-11 22:52:36

Executable name: NOTEPAD.EXE
Hash: D8414F97
File size (bytes): 60,366
Version: Windows 10 or Windows 11

Run count: 13
Last run: 2023-03-08 00:21:16
Other run times: 2023-03-07 03:03:08, 2023-03-07 02:55:19, 2023-03-07 02:35:27, 2023-03-06 00:07:58, 2023-02-25 21:50:32,
2023-02-25 21:49:09, 2022-03-05 00:52:46
```

PFDump EnScript for EnCase



```
Prefetch Core Data
        Type:           Win10
        Device File Path:  \VOLUME{01d817f399fcabf8-1e9a1012}\WINDOWS\SYSTEM32\NOTEPAD.EXE
        File Name:        NOTEPAD.EXE
        Stored Hash:      D8414F97
        Hosting App:      No
        Kernel:          No
        Run Count:        13
        Last Run:        03/08/2023 00:21:16
                    03/07/2023 03:03:08
                    03/07/2023 02:55:19
                    03/07/2023 02:35:27
                    03/06/2023 00:07:58
                    02/25/2023 21:50:32
                    02/25/2023 21:49:09
                    03/05/2022 00:52:46
```

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 34 - Removable Media 23-5562

Question 34: Provide the SHA256 hash for the USB device.

Manufacturer's Expected Response: 6B5C8BD30A01B303A968D88F467192BF0CD4D21659E95D8A0A38D667E1B31AB2

WebCode Test	Response
2PJFNF-5562	6B5C8BD30A01B303A968D88F467192BF0CD4D21659E95D8A0A38D667E1B31AB2
2VQ8RL-5562	6b5c8bd30a01b303a968d88f467192bf0cd4d21659e95d8a0a38d667e1b31ab2
3CDK6E-5562	64D00826424895EC5A8D508CE1B3E4391C60B4A4EEE3F274AEE02C07605E1257
4U7ZP2-5562	6b5c8bd30a01b303a968d88f467192bf0cd4d21659e95d8a0a38d667e1b31ab2
68RW46-5562	6b5c 8bd3 0a01 b303 a968 d88f 4671 92bf 0cd4 d216 59e9 5d8a 0a38 d667 e1b3 1ab2
6MKCN6-5562	733C4E207C967BFE41A8BE1D4ECDE82D6FD1D42B3793F9C9FA65D7310F5883D1
6Q2RXW-5562	6b5c8bd30a01b303a968d88f467192bf0cd4d21659e95d8a0a38d667e1b31ab2
6QKH3A-5562	c57d3766173db2fac472e27015cac2cee8331ea4d5f84f297d6c8b151bab03f4
78PAK7-5562	6b5c8bd30a01b303a968d88f467192bf0cd4d21659e95d8a0a38d667e1b31ab2
7PQ8PM-5562	6B5C8BD30A01B303A968D88F467192BF0CD4D21659E95D8A0A38D667E1B31AB2
7XZLMH-5562	6B5C8BD30A01B303A968D88F467192BF0CD4D21659E95D8A0A38D667E1B31AB2
82VWX9-5562	E2B873FC1FA842167DB03A2AE3AD2E4854573936861191 20C4CAB58B93AACD42
83AEYT-5562	6b5c8 bd30a01b303a968d88f467192bf0cd4d21659e95d8a0a38d667e1b31ab2
99QBZK-5562	6B5C8BD30A01B303A968D88F467192BF0CD4D21659E95D8A0A38D667E1B31AB2
9J9Q8U-5562	6b5c 8bd3 0a01 b303 a968 d88f 4671 92bf 0cd4 d216 59e9 5d8a 0a38 d667 e1b3 1ab2
A8QHYB-5562	6B5C8BD30A01B303A968D88F467192BF0CD4D21659E95D8A0A38D667E1B31AB2
ADYU2Y-5562	6B5C8BD30A01B303A968D88F467192BF0CD4D21659E95D8A0A38D667E1B31AB2 (decompressed image file) 2CE62D4BDF8C37C334EFF3D852644BB9B4E664BC4CB154E808AC275A092487C1 (compressed image file)
AKG6BT-5562	6B5C8BD30A01B303A968D88F467192BF0CD4D21659E95D8A0A38D667E1B31AB2
BFKZWF-5562	6b5c8bd30a01b303a968d88f467192bf0cd4d21659e95d8a0a38d667e1b31ab2
C4LMC9-5562	6B5C8BD30A01B303A968D88F467192BF0CD4D21659E95D8A0A38D667E1B31AB2

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 34 - Removable Media 23-5562

WebCode Test	Response
CF2CBE-5562	6b5c8bd30a01b303a968d88f467192bf0cd4d21659e95d8a0a38d667e1b31ab2
DXVP3C-5562	9c64e1fd0d570c5d7231439314a1ebff08f6f3c88bcfb21088ddcacfa4993558
E2RHRZ-5562	6B5C8BD30A01B303A968D88F467192BF0CD4D21659E95D8A0A38D667E1B31AB2
HW2LD2-5562	159F436CF591C14E449EDDDACED9AB730DE6334611D3741255F65B7D924F070A
J84AQF-5562	6b5c8bd30a01b303a968d88f467192bf0cd4d21659e95d8a0a38d667e1b31ab2
JGBUAC-5562	4a97379a2c56a0cf8fc1c97573b22ae7b63d1715a2066636a70a1adcb45c5bd5
JL32PY-5562	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
KR28JR-5562	6b5c8bd30a01b303a968d88f467192bf0cd4d21659e95d8a0a38d667e1b31ab2
KXRBW6-5562	6b5c 8bd3 0a01 b303 a968 d88f 4671 92bf 0cd4 d216 59e9 5d8a 0a38 d667 e1b3 1ab2
NE7TEF-5562	C8A69629133BCD43AA629198E50FFAF8D8006BBD3D6610061812FA20484E2241
PFEMA7-5562	6b5c8bd30a01b303a968d88f467192bf0cd4d21659e95d8a0a38d667e1b31ab2
PPMYM4-5562	6b5c8bd30a01b303a968d88f467192bf0cd4d21659e95d8a0a38d667e1b31ab2
PTKDEZ-5562	6b5c8bd30a01b303a968d88f467192bf0cd4d21659e95d8a0a38d667e1b31ab2
RAK67E-5562	6B5C8BD30A01B303A968D88F467192BF0CD4D21659E95D8A0A38D667E1B31AB2
RBBDCA-5562	6B5C8BD30A01B303A968D88F467192BF0CD4D21659E95D8A0A38D667E1B31AB2
RGH4EF-5562	6b5c8bd30a01b303a968d88f467192bf0cd4d21659e95d8a0a38d667e1b31ab2
RRXTDK-5562	6b5c8bd30a01b303a968d88f467192bf0cd4d21659e95d8a0a38d667e1b31ab2
TC4JAF-5562	6b5c8bd30a01b303a968d88f467192bf0cd4d21659e95d8a0a38d667e1b31ab2
TEPC2R-5562	159F436CF591C14E449EDDDACED9AB730DE6334611D3741255F65B7D924F070A
TVF9MD-5562	B7AA87244ADA7FCDCB7120663170594DEA038D435C5BB4C60E154A5A0A8F45E0
UVZCUQ-5562	6B5C8BD30A01B303A968D88F467192BF0CD4D21659E95D8A0A38D667E1B31AB2
V4KY4K-5562	6b5c8bd30a01b303a968d88f467192bf0cd4d21659e95d8a0a38d667e1b31ab2

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 34 - Removable Media 23-5562

WebCode Test	Response
WZGLVL-5562	6b5c8bd30a01b303a968d88f467192bf0cd4d21659e95d8a0a38d667e1b31ab2
XA2A8Z-5562	6B5C8BD30A01B303A968D88F467192BF0CD4D21659E95D8A0A38D667E1B31AB2
XJ99G2-5562	6B5C8BD30A01B303A968D88F467192BF0CD4D21659E95D8A0A38D667E1B31AB2
XVDHZK-5562	6B5C8BD30A01B303A968D88F467192BF0CD4D21659E95D8A0A38D667E1B31AB2
Y63G92-5562	6B5C8BD30A01B303A968D88F467192BF0CD4D21659E95D8A0A38D667E1B31AB2
YPNENR-5562	6b5c8bd30a01b303a968d88f467192bf0cd4d21659e95d8a0a38d667e1b31ab2

Question 34: Provide the SHA256 hash for the USB device.

Consensus Result:

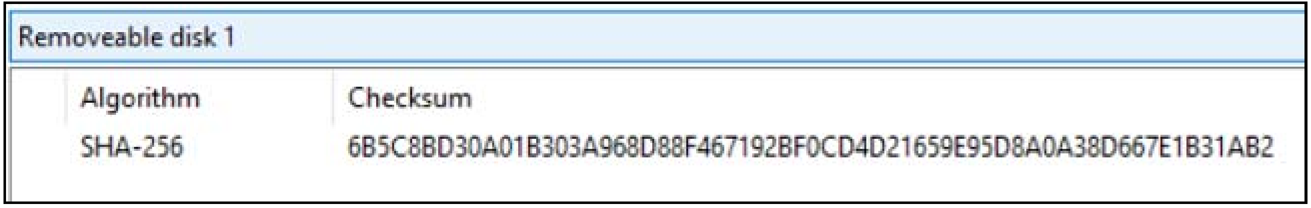
6B5C8BD30A01B303A968D88F467192BF0CD4D21659E95D8A0A38D667E1B31AB2

Expected Response Explanation:

Attaching the USB device to a computer with write blocking and hashing provides the expected hash value.

Expected Response Illustration:

HxD Hex Editor tool used for Device Hashing (SHA256)



Removeable disk 1

Algorithm	Checksum
SHA-256	6B5C8BD30A01B303A968D88F467192BF0CD4D21659E95D8A0A38D667E1B31AB2

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 35 - Removable Media 23-5562

Question 35: How many active partitions are on the device? Provide a NUMERIC response (e.g., 1, 2, 3).

Manufacturer's Expected Response: 3

WebCode Test	Response
2PJFNF-5562	3
2VQ8RL-5562	3
3CDK6E-5562	3
4U7ZP2-5562	3
68RW46-5562	3
6MKCN6-5562	3
6Q2RXW-5562	3
6QKH3A-5562	3
78PAK7-5562	3
7PQ8PM-5562	3
7XZLMH-5562	3
82VWX9-5562	3
83AEYT-5562	3
99QBZK-5562	1
9J9Q8U-5562	3
A8QHYB-5562	3
ADYU2Y-5562	3
AKG6BT-5562	3
BFKZWF-5562	3
C4LMC9-5562	3

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 35 - Removable Media 23-5562

WebCode Test	Response
CF2CBE-5562	3
DXVP3C-5562	3
E2RHRZ-5562	3
HW2LD2-5562	3
J84AQF-5562	3
JGBUAC-5562	3
JL32PY-5562	3
KR28JR-5562	3
KXRBW6-5562	3
NE7TEF-5562	3
PFEMA7-5562	3
PPMYM4-5562	3
PTKDEZ-5562	3
RAK67E-5562	3
RBBDCA-5562	3
RGH4EF-5562	3
RRXTDK-5562	3
TC4JAF-5562	3
TEPC2R-5562	3
TVF9MD-5562	3
UVZCUQ-5562	0
V4KY4K-5562	3

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 35 - Removable Media 23-5562

WebCode Test	Response
WZGLVL-5562	0
XA2A8Z-5562	3
XJ99G2-5562	3
XVDHZK-5562	3
Y63G92-5562	3
YPNENR-5562	3

Question 35: How many active partitions are on the device? Provide a NUMERIC response (e.g., 1, 2, 3).

Consensus Result:

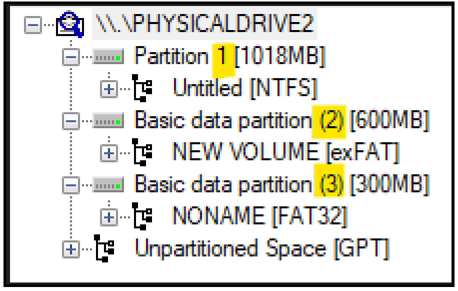
3

Expected Response Explanation:

The number of device partitions can be determined by reviewing the partition table with most forensic suites or imaging tools.

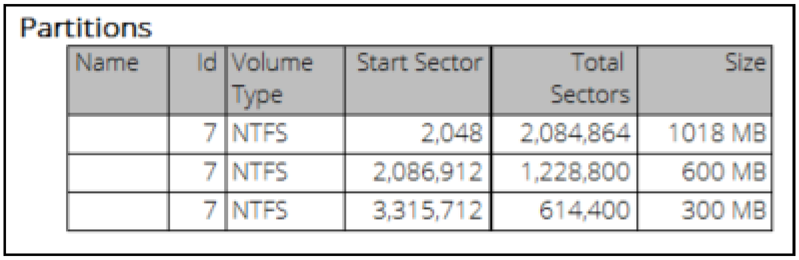
Expected Response Illustration:

FTK Imager view of partitions



```
\\.\PHYSICALDRIVE2
  Partition 1 [1018MB]
    Untitled [NTFS]
  Basic data partition (2) [600MB]
    NEW VOLUME [exFAT]
  Basic data partition (3) [300MB]
    NONAME [FAT32]
  Unpartitioned Space [GPT]
```

EnCase Report of Drive Geometry



Partitions

Name	Id	Volume Type	Start Sector	Total Sectors	Size
	7	NTFS	2,048	2,084,864	1018 MB
	7	NTFS	2,086,912	1,228,800	600 MB
	7	NTFS	3,315,712	614,400	300 MB

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 36 - Removable Media 23-5562

Question 36: What type of filesystem is on the second partition (named "NEW VOLUME")?

Manufacturer's Expected Response: exFAT

WebCode Test	Response
2PJFNF-5562	exfat
2VQ8RL-5562	exFAT
3CDK6E-5562	exFAT
4U7ZP2-5562	exFAT
68RW46-5562	exFAT
6MKCN6-5562	exfat
6Q2RXW-5562	exFAT
6QKH3A-5562	exFAT
78PAK7-5562	exFAT
7PQ8PM-5562	exFAT
7XZLMH-5562	exFAT
82VWX9-5562	exFAT
83AEYT-5562	exFAT
99QBZK-5562	exFAT
9J9Q8U-5562	exFAT
A8QHYB-5562	exFAT
ADYU2Y-5562	exFAT
AKG6BT-5562	exFat
BFKZWF-5562	exFAT
C4LMC9-5562	exFAT
CF2CBE-5562	exFAT

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 36 - Removable Media 23-5562

WebCode Test	Response
DXVP3C-5562	exFAT
E2RHRZ-5562	exFAT
HW2LD2-5562	exFAT
J84AQF-5562	exFAT
JGBUAC-5562	exFAT
JL32PY-5562	exFAT
KR28JR-5562	exFAT
KXRBW6-5562	exFAT
NE7TEF-5562	exFAT
PFEMA7-5562	NTFS
PPMYM4-5562	exFAT
PTKDEZ-5562	exFAT
RAK67E-5562	exFAT
RBBDCA-5562	exFAT
RGH4EF-5562	exFAT
RRXTDK-5562	exFAT
TC4JAF-5562	exFAT
TEPC2R-5562	exFAT
TVF9MD-5562	EXFAT
UVZCUQ-5562	exFAT
V4KY4K-5562	exFAT
WZGLVL-5562	exFAT

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 36 - Removable Media 23-5562

WebCode Test	Response
XA2A8Z-5562	exFAT
XJ99G2-5562	exFAT
XVDHZK-5562	exFAT
Y63G92-5562	Ex-Fat
YPNENR-5562	exFAT

Question 36: What type of filesystem is on the second partition (named "NEW VOLUME")?

Consensus Result:

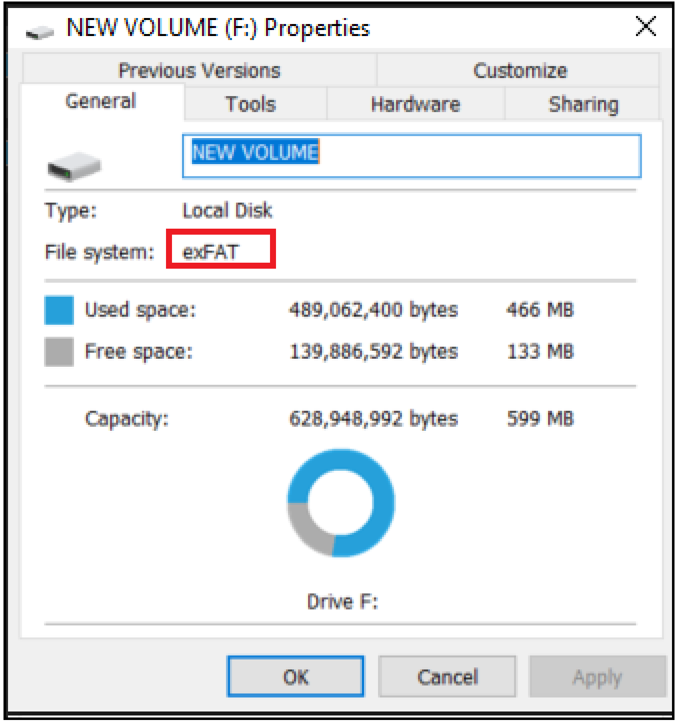
exFAT

Expected Response Explanation:

This partition is formatted with an exFAT Filesystem.

Expected Response Illustration:

Windows Drive Properties



NEW VOLUME

Type: Local Disk

File system: exFAT

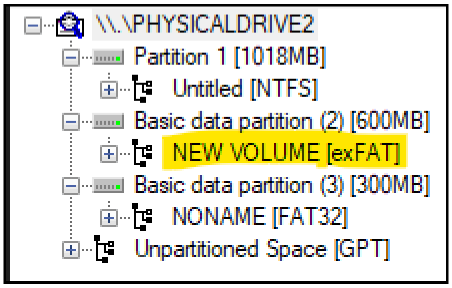
Used space:	489,062,400 bytes	466 MB
Free space:	139,886,592 bytes	133 MB
Capacity:	628,948,992 bytes	599 MB

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 36 - Removable Media 23-5562

FTK Imager view of partitions



```
\\.\PHYSICALDRIVE2
    Partition 1 [1018MB]
        Untitled [NTFS]
    Basic data partition (2) [600MB]
        NEW VOLUME [exFAT]
    Basic data partition (3) [300MB]
        NONAME [FAT32]
    Unpartitioned Space [GPT]
```

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 37 - Removable Media 23-5562

Question 37: What is the parent directory for ItchyBlackKoala.xls?

Manufacturer's Expected Response: DarkFierceLocust

WebCode Test	Response
2PJFNF-5562	DarkFierceLocust
2VQ8RL-5562	DarkFierceLocust
3CDK6E-5562	DarkFierceLocust
4U7ZP2-5562	DarkFierceLocust
68RW46-5562	DarkFierceLocust
6MKCN6-5562	DarkFierceLocust
6Q2RXW-5562	DarkFierceLocust
6QKH3A-5562	Partition 3 (Microsoft FAT32, 300 MB) NO NAME\DarkFierceLocust\ItchyBlackKoala.xls
78PAK7-5562	DarkFierceLocust
7PQ8PM-5562	DarkFierceLocust
7XZLMH-5562	DarkFierceLocust
82VWX9-5562	Parent directory is DarkFierceLocust
83AEYT-5562	DarkFierceLocust
99QBZK-5562	DarkFierceLocust
9J9Q8U-5562	DarkFierceLocust
A8QHYB-5562	DarkFierceLocust
ADYU2Y-5562	\DarkFierceLocust
AKG6BT-5562	DarkFierceLocust
BFKZWF-5562	DarkFierceLocust
C4LMC9-5562	DarkFierceLocust
CF2CBE-5562	DarkFierceLocust

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 37 - Removable Media 23-5562

WebCode Test	Response
DXVP3C-5562	DarkFierceLocust
E2RHRZ-5562	DarkFierceLocust
HW2LD2-5562	DarkFierceLocust
J84AQF-5562	\DarkFierceLocust\
JGBUAC-5562	DarkFierceLocust
JL32PY-5562	DarkFierceLocust
KR28JR-5562	DarkFierceLocust
KXRBW6-5562	\DarkFierceLocust\
NE7TEF-5562	DarkFierceLocust
PFEMA7-5562	DarkFierceLocust
PPMYM4-5562	DarkFierceLocust
PTKDEZ-5562	DarkFierceLocust
RAK67E-5562	DarkFierceLocust
RBBDCA-5562	DarkFierceLocust
RGH4EF-5562	\DarkFierceLocust\
RRXTDK-5562	DarkFierceLocust
TC4JAF-5562	DarkFierceLocust
TEPC2R-5562	DarkFierceLocust/ItchyBlackKoala.xls
TVF9MD-5562	\DarkFierceLocust\
UVZCUQ-5562	DarkFierceLocust
V4KY4K-5562	\DarkFierceLocust\
WZGLVL-5562	DarkFierceLocust

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 37 - Removable Media 23-5562

WebCode Test	Response
XA2A8Z-5562	DarkFierceLocust
XJ99G2-5562	\DarkFierceLocust
XVDHZK-5562	DarkFierceLocust
Y63G92-5562	DarkFierceLocust
YPNENR-5562	DarkFierceLocust

Question 37: What is the parent directory for ItchyBlackKoala.xls?

Consensus Result:

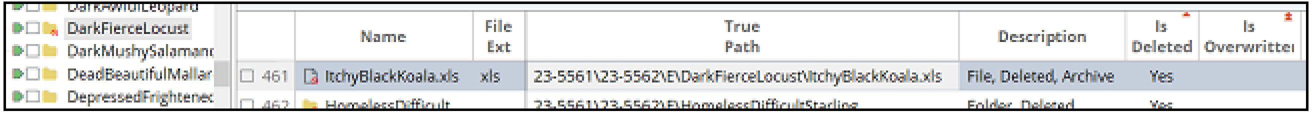
DarkFierceLocust

Expected Response Explanation:

ItchyBlackKoala.xls and its parent directory DarkFierceLocust are both deleted, but not overwritten. Their entries in the NTFS Master File Table have not yet been overwritten so they are still readable by forensic tools which will show the files (and directory) as having been deleted but still readable from the volume.

Expected Response Illustration:

EnCase table view of \DarkFierceLocust\ItchyBlackKoala.xls



DarkAwfulLeopard
DarkFierceLocust
DarkMushySalamanc
DeadBeautifulMallar
DepressedFrightenec

	Name	File Ext	True Path	Description	Is Deleted	Is Overwritter
461	ItchyBlackKoala.xls	xls	23-5561\23-5562\E\DarkFierceLocust\ItchyBlackKoala.xls	File, Deleted, Archive	Yes	
462	HomelessDifficult		23-5561\23-5562\E\HomelessDifficultStarling	Folder, Deleted	Yes	

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 38 - Removable Media 23-5562

Question 38: What is the filetype of the file with SHA-1 hash 9b810eb160adcb2cabac5aa318b36ea34244e281?

Manufacturer's Expected Response: 7-zip file

** Inconsistencies not highlighted; No consensus achieved **

WebCode Test	Response
2PJFNF-5562	sys
2VQ8RL-5562	sys
3CDK6E-5562	This SHA1 value not found
4U7ZP2-5562	system page file
68RW46-5562	7-Zip
6MKCN6-5562	7zip
6Q2RXW-5562	7-Zip
6QKH3A-5562	7Zip
78PAK7-5562	7-zip
7PQ8PM-5562	7Zip
7XZLMH-5562	7z
82VWX9-5562	7-Zip
83AEYT-5562	7Zip
99QBZK-5562	File has a .7z header with a .SYS file extention
9J9Q8U-5562	.sys 7zip file
A8QHYB-5562	application/x-7z-compressed
ADYU2Y-5562	7Zip
AKG6BT-5562	The file is "pagefile.sys", this is a (.sys) system file and is used by Windows as part of the memory (RAM) management on a windows system
BFKZWF-5562	7Zip
C4LMC9-5562	7z

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 38 - Removable Media 23-5562

** Inconsistencies not highlighted; No consensus achieved **

WebCode Test	Response
CF2CBE-5562	7Zip
DXVP3C-5562	.sys = system
E2RHRZ-5562	7Zip
HW2LD2-5562	.sys (system file)
J84AQF-5562	pagefile.sys
JGBUAC-5562	7Zip
JL32PY-5562	7z compressed
KR28JR-5562	7-zip
KXRBW6-5562	pagefile.sys
NE7TEF-5562	7zip
PFEMA7-5562	7Zip
PPMYM4-5562	Archive/7Zip
PTKDEZ-5562	7Zip
RAK67E-5562	7Zip
RBBDCA-5562	sys (pagefile.sys)
RGH4EF-5562	7-Zip file
RRXTDK-5562	7z application/x-7z-compressed
TC4JAF-5562	7zip
TEPC2R-5562	.sys system file
TVF9MD-5562	7Zip
UVZCUQ-5562	7-Zip
V4KY4K-5562	(File system, compressed) *.sys – [pagefile.sys]

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 38 - Removable Media 23-5562

** Inconsistencies not highlighted; No consensus achieved **

WebCode Test	Response
WZGLVL-5562	7Zip
XA2A8Z-5562	7ZIP
XJ99G2-5562	7z
XVDHZK-5562	File System
Y63G92-5562	7-Zip file containing a pagefile.sys file
YPNENR-5562	7Zip

Question 38: What is the filetype of the file with SHA-1 hash 9b810eb160adcb2cabac5aa318b36ea34244e281?

Consensus Result:

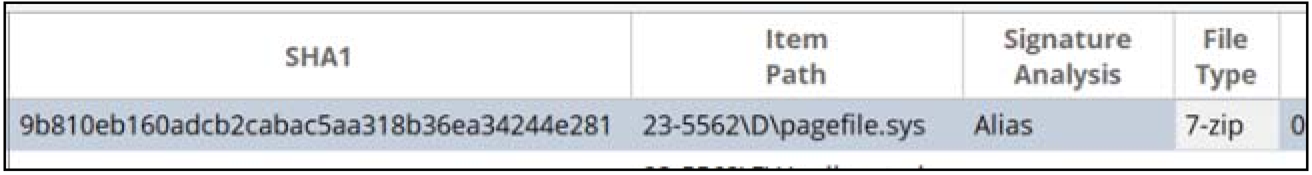
No consensus was achieved for this question. The majority of participants (74%) reported the expected response, 7-zip. However, 11 participants reported that the filetype was a sys file. The intent of this question was for the participant to identify the filetype by the file header or contents of the file, not its filename extension, which can be misleading.

Expected Response Explanation:

The file with hash 9b810eb160adcb2cabac5aa318b36ea34244e281 is pagefile.sys. The extension of this file suggests it is a system file, however inspection of the file header, shows the first 10 bytes to be 37 7A BC AF (7z¼), the identifier for a 7-zip file.

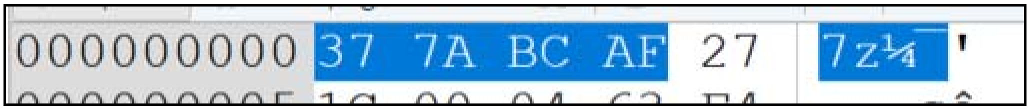
Expected Response Illustration:

EnCase table and view panes showing hash, name, and filetype for pagefile.sys



SHA1	Item Path	Signature Analysis	File Type
9b810eb160adcb2cabac5aa318b36ea34244e281	23-5562\D\pagefile.sys	Alias	7-zip

Hex view of pagefile.sys header



```
000000000 37 7A BC AF 27   7z¼ '
```

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 39 - Removable Media 23-5562

Question 39: In unallocated space on the USB flash drive is a jpeg photo file of a white rock on a black background. The SHA-1 hash of this file is 446b6fe695c878b6651d58378acc9a2503d50048 Provide the MD5 hash of this file.

Manufacturer's Expected Response: 73BB4AE1D3C52A8B2B371D5CB059D145

WebCode Test	Response
2PJFNF-5562	73bb4ae1d3c52a8b2b371d5cb059d145
2VQ8RL-5562	73bb4ae1d3c52a8b2b371d5cb059d145
3CDK6E-5562	73bb4ae1d3c52a8b2b371d5cb059d145
4U7ZP2-5562	C315DBE0590608189453E160E3B592C0
68RW46-5562	73bb 4ae1 d3c5 2a8b 2b37 1d5c b059 d145
6MKCN6-5562	73bb4ae1d3c52a8b2b371d5cb059d145
6Q2RXW-5562	73bb4ae1d3c52a8b2b371d5cb059d145
6QKH3A-5562	73bb4ae1d3c52a8b2b371d5cb059d145
78PAK7-5562	73bb4ae1d3c52a8b2b371d5cb059d145
7PQ8PM-5562	73bb4ae1d3c52a8b2b371d5cb059d145
7XZLMH-5562	73BB4AE1D3C52A8B2B371D5CB059D145
82VWX9-5562	73bb4ae1d3c52a8b2b371d5cb059d145
83AEYT-5562	73bb4ae1d3c52a8b2b371d5cb059d145
99QBZK-5562	73bb4ae1d3c52a8b2b371d5cb059d145
9J9Q8U-5562	73bb4ae1d3c52a8b2b371d5cb059d145
A8QHYB-5562	73bb4ae1d3c52a8b2b371d5cb059d145
ADYU2Y-5562	73bb4ae1d3c52a8b2b371d5cb059d145
AKG6BT-5562	73bb4ae1d3c52a8b2b371d5cb059d145
BFKZWF-5562	73bb4ae1d3c52a8b2b371d5cb059d145
C4LMC9-5562	73bb4ae1d3c52a8b2b371d5cb059d145

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 39 - Removable Media 23-5562

WebCode Test	Response
CF2CBE-5562	73bb4ae1d3c52a8b2b371d5cb059d145
DXVP3C-5562	73bb4ae1d3c52a8b2b371d5cb059d145
E2RHRZ-5562	73bb4ae1d3c52a8b2b371d5cb059d145
HW2LD2-5562	73BB4AE1D3C52A8B2B371D5CB059D145
J84AQF-5562	73bb4ae1d3c52a8b2b371d5cb059d145
JGBUAC-5562	73bb4ae1d3c52a8b2b371d5cb059d145
JL32PY-5562	73BB4AE1D3C52A8B2B371D5CB059D145
KR28JR-5562	73bb4ae1d3c52a8b2b371d5cb059d145
KXRBW6-5562	73bb4ae1d3c52a8b2b371d5cb059d145
NE7TEF-5562	73bb4ae1d3c52a8b2b371d5cb059d145
PFEMA7-5562	73bb4ae1d3c52a8b2b371d5cb059d145
PPMYM4-5562	73bb4ae1d3c52a8b2b371d5cb059d145
PTKDEZ-5562	73bb4ae1d3c52a8b2b371d5cb059d145
RAK67E-5562	73bb4ae1d3c52a8b2b371d5cb059d145
RBBDCA-5562	73bb4ae1d3c52a8b2b371d5cb059d145
RGH4EF-5562	73bb4ae1d3c52a8b2b371d5cb059d145
RRXTDK-5562	73BB4AE1D3C52A8B2B371D5CB059D145
TC4JAF-5562	73bb4ae1d3c52a8b2b371d5cb059d145
TEPC2R-5562	73bb4ae1d3c52a8b2b371d5cb059d145
TVF9MD-5562	73bb4ae1d3c52a8b2b371d5cb059d145
UVZCUQ-5562	73BB4AE1D3C52A8B2B371D5CB059D145
V4KY4K-5562	73bb4ae1d3c52a8b2b371d5cb059d145

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 39 - Removable Media 23-5562

WebCode Test	Response
WZGLVL-5562	73bb4ae1d3c52a8b2b371d5cb059d145
XA2A8Z-5562	73bb4ae1d3c52a8b2b371d5cb059d145
XJ99G2-5562	06D30D40149AE3542BC09C5E0C0A5DD8
XVDHZK-5562	73bb4ae1d3c52a8b2b371d5cb059d145
Y63G92-5562	73bb4ae1d3c52a8b2b371d5cb059d145
YPNENR-5562	73bb4ae1d3c52a8b2b371d5cb059d145

Question 39: In unallocated space on the USB flash drive is a jpeg photo file of a white rock on a black background. The SHA-1 hash of this file is 446b6fe695c878b6651d58378acc9a2503d50048. Provide the MD5 hash of this file.

Consensus Result:

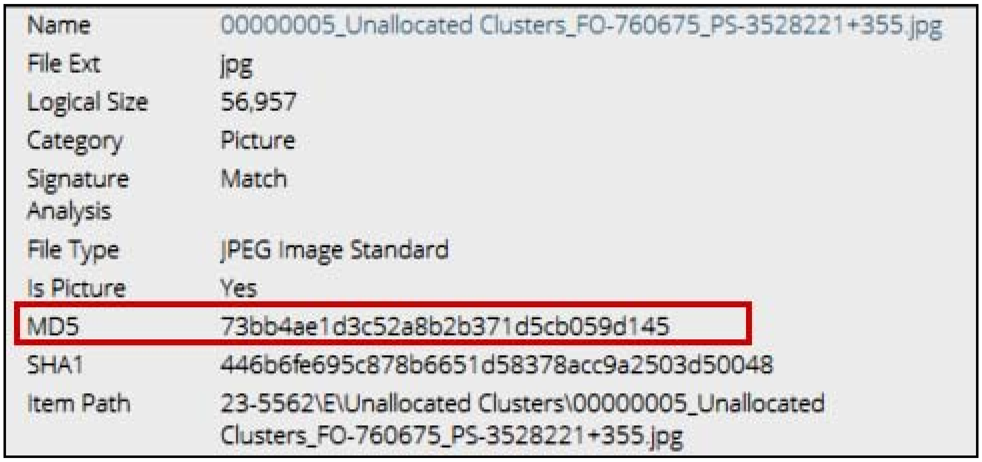
73BB4AE1D3C52A8B2B371D5CB059D145

Expected Response Explanation:

Any forensic file carving utility can be used to carve photo files from the unallocated space on the USB device. Reviewing the carved files will locate the described photo.

Expected Response Illustration:

EnCase carved file information



Name	00000005_Unallocated Clusters_FO-760675_PS-3528221+355.jpg
File Ext	jpg
Logical Size	56,957
Category	Picture
Signature Analysis	Match
File Type	JPEG Image Standard
Is Picture	Yes
MD5	73bb4ae1d3c52a8b2b371d5cb059d145
SHA1	446b6fe695c878b6651d58378acc9a2503d50048
Item Path	23-5562\E\Unallocated Clusters\00000005_Unallocated Clusters_FO-760675_PS-3528221+355.jpg

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 39 - Removable Media 23-5562
00000005_Unallocated Clusters_FO-760675_PS-3528221+355.jpg

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 40 - Removable Media 23-5562

Question 40: A directory of files was created on the USB on 7 March 2023 (2023-03-07) at 02:28:38 (UTC+0). Provide the name of the directory.

Manufacturer's Expected Response: spoof reset page

WebCode Test	Response
2PJFNF-5562	spoof reset page
2VQ8RL-5562	spoof reset page
3CDK6E-5562	spoof reset page
4U7ZP2-5562	spoof reset page
68RW46-5562	spoof reset page
6MKCN6-5562	spoof reset page
6Q2RXW-5562	spoof reset page
6QKH3A-5562	Spoof reset page
78PAK7-5562	spoof reset page
7PQ8PM-5562	spoof reset page
7XZLMH-5562	spoof reset page
82VWX9-5562	spoof reset page
83AEYT-5562	spoof reset page
99QBZK-5562	Spoof reset page
9J9Q8U-5562	Password help _ Reset your password_files
A8QHYB-5562	spoof reset page
ADYU2Y-5562	\spoof reset page
AKG6BT-5562	Spoof reset page
BFKZWF-5562	spoof reset page
C4LMC9-5562	spoof reset page

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 40 - Removable Media 23-5562

WebCode Test	Response
CF2CBE-5562	spoof reset page
DXVP3C-5562	G:\spoof reset page
E2RHRZ-5562	Spoof reset page
HW2LD2-5562	spoof reset page
J84AQF-5562	System Volume Information
JGBUAC-5562	G:\spoof reset page
JL32PY-5562	spoof reset page
KR28JR-5562	spoof reset page
KXRBW6-5562	spoof reset page
NE7TEF-5562	spoof reset page
PFEMA7-5562	spoof reset page
PPMYM4-5562	Untitled
PTKDEZ-5562	spoof reset page
RAK67E-5562	Spoof Reset Page
RBBDCA-5562	spoof reset page
RGH4EF-5562	\spoof reset page
RRXTDK-5562	spoof reset page
TC4JAF-5562	spoof reset page
TEPC2R-5562	spoof reset page
TVF9MD-5562	spoof reset page
UVZCUQ-5562	spoof reset page
V4KY4K-5562	\spoof reset page\

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 40 - Removable Media 23-5562

WebCode Test	Response
WZGLVL-5562	spoof reset page
XA2A8Z-5562	G:\spoof reset page
XJ99G2-5562	spoof reset page
XVDHZK-5562	[Participant did not return results for this question.]
Y63G92-5562	spoof reset page
YPNENR-5562	spoof reset page

Question 40: A directory of files was created on the USB on 7 March 2023 (2023-03-07) at 02:28:38 (UTC+0). Provide the name of the directory.

Consensus Result:

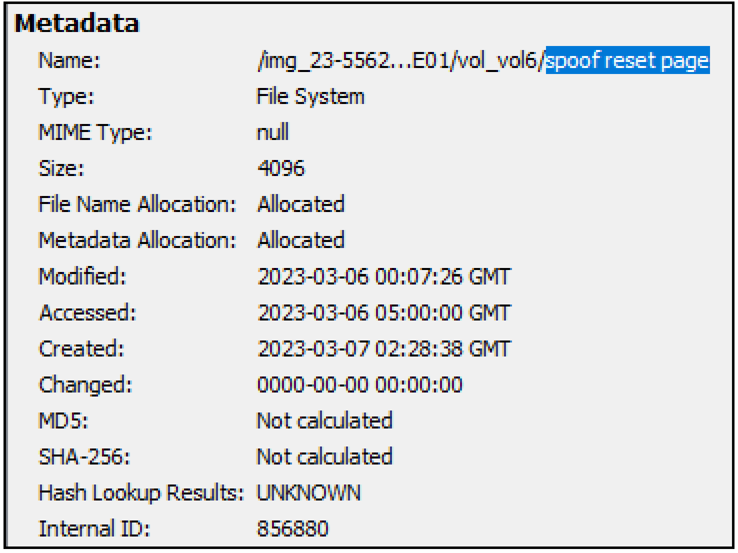
spoof reset page

Expected Response Explanation:

The "spoof reset page" directory (and contained files) was created on the FAT32 volume at 2023-03-07 02:28:38 (UTC+0).

Expected Response Illustration:

Autopsy metadata view of spoof reset page



Metadata

Name:	/img_23-5562...E01/vol_vol6/spoof reset page
Type:	File System
MIME Type:	null
Size:	4096
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-03-06 00:07:26 GMT
Accessed:	2023-03-06 05:00:00 GMT
Created:	2023-03-07 02:28:38 GMT
Changed:	0000-00-00 00:00:00
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup Results:	UNKNOWN
Internal ID:	856880

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 41 - Removable Media 23-5562

Question 41: Compare the “Created” and “Modified” timestamps of the directory and files referenced in question 40. What do the relative “Created” and “Modified” timestamps indicate about the files’ placement on the USB?

Manufacturer's Expected Response: "They were copied from another volume" and variations of this text providing a similar description.

WebCode Test	Response
2PJFNF-5562	Modified 2023-03-06 AM12:07:26 Created 2023-03-07 AM 2:28:38
2VQ8RL-5562	The spoof reset page folder and files are not the original because the modified date is earlier than the created date. This means that the file has been copied to a USB drive.
3CDK6E-5562	The files were created prior to the folder they are now resident within
4U7ZP2-5562	The files in the "spoof reset page" directory were modified on a computer the night before, and then copied/pasted to the USB stick.
68RW46-5562	Created: 06/03/2023 21:28:38 (UTC+5) Modified: 05/03/2023 19:07:26 (UTC+5). The created timestamp shows when the file has been created on the filesystem. Transfering it to/from FS1 (e.g. laptop) to FS2 (e.g. USB) changes the created time to the date and time is has been moved, but leaves the modified timestamp unchanged. The modified timestamp is when the internals of the file (i.e. the content) has been changed. Due to this, the created time can be of a later date than the modified time.
6MKCN6-5562	When copying a folder to USB, the creation time is changed, and when saving a file in the folder, the change time is changed.
6Q2RXW-5562	The fact that the "Created" timestamp is later than the "Modified" timestamp suggests that the files and directory were copied to the USB drive at a later date.
6QKH3A-5562	File was created in a separate location, then copied onto the USB. Gives new creation date, inherits original modified date and time.
78PAK7-5562	The items were copied to the USB from another data source, and were not modified after being written to the USB
7PQ8PM-5562	The created and modified timestamps indicate that the directory and files were created on a different device and than placed on the USB.
7XZLMH-5562	The modified dates predate the created dates, indicating that the directory and the files it contains were created elsewhere and subsequently copied to this location.
82VWX9-5562	The files were originally created on 2023-03-05 and copied to the USB on 2023-03-06 21:28:38. This is due to all the creation dates being the same for all files, while the modified dates are different.
83AEYT-5562	The creation date for the directory and files referenced in question 40 is after the modified (last written date) meaning they were copied there from another volume.
99QBZK-5562	The file creation date is after the last written date. As the last write is before the creation date this may signify that the folder was created on a separate device and then transferred to the USB device, possibly a result of changing from the original file system to FAT32.
9J9Q8U-5562	The modifed time is the original creation time of the folder/file. The "Created" time is when is was placed on the USB per FAT32 protocol.
A8QHYB-5562	The directory and files were copied onto the USB.
ADYU2Y-5562	The created and modified timestamps indicate that the folder was copied to the USB where the modified timestamp has been inherited from the original folder/files.
AKG6BT-5562	The file was “last modified” before it was created, this suggests that the file was copied to the USB. The file created is the time/date it was created on the USB. The time/date modified is inherited from the file modified date/time of the original file

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 41 - Removable Media 23-5562

WebCode Test	Response
BFKZWF-5562	the items existed on the hard drive on 3/6/2023 in David Lightman Downloads folder, and copied to the USB drive on 3/7/2023 at the mentioned time.
C4LMC9-5562	They were copy-pasted from another system
CF2CBE-5562	The directory has been copied from the hard drive to the USB, hence the modified date (6/3/2023) is a day earlier than the created date (7/3/2023)
DXVP3C-5562	It was created on a different device, then placed onto the USB
E2RHRZ-5562	Created: 07/03/2023 02:28:38, Modified: 06/03/2023 00:07:26 : A modified timestamp before the created timestamps indicates the file is not the original and has been possibly copied from another device onto the USB.
HW2LD2-5562	Date Created is the time the file was created / opened / moved on the USB, whereas the Date Modified is time content of a file was last modified/changed.
J84AQF-5562	That have been modified
JGBUAC-5562	The pre existing folder on the computer that has been last modified on 06/03/2023 and then created on 07/03/2023. This was transferred to the USB. Hence why the created date and time is after the modified date and time.
JL32PY-5562	It could have something to do with the way the files are processed, where the Modified time is left to the time where the contents of the file changed, but the Created time is when the file in the new location was created. That is usual with copied files, when you copy a file the file's created date becomes the modified date and the current date(when the file is copied) becomes the created date.
KR28JR-5562	Files creation dates later than last modified, indicates the full folder was written to the USB on creation date and has not been subsequently modified.
KXRBW6-5562	The files have been pasted from the USB to the machine but were created elsewhere as all the created timestamps are the same
NE7TEF-5562	Copied to USB the Directory.
PFEMA7-5562	The modified timestamp is before the created timestamp, which indicates the directory and files were created on a different drive, then placed on the USB drive. The directory/files maintained the original modified timestamp, but the created timestamp is when the directory/file was created on the drive.
PPMYM4-5562	They are created in the USB itself not copied.
PTKDEZ-5562	This indicates that the directory and files are likely copied from elsewhere.
RAK67E-5562	It indicates that the folder was created on another device and copied to the USB stick
RBBDCA-5562	They have been copied to the USB (Modified dates/times are older than Created dates/times and Created dates/times are identical)
RGH4EF-5562	The folder and its content have been moved from another location (device or partition) from where they may have been first created
RRXTDK-5562	It indicates that the files were created on other computer/device and later copied into the USB drive.
TC4JAF-5562	Directory and files was copied to the USB on 6 March 2023 at 21:28:38. Therefore "Modified Time" is older than "Created Time".

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 41 - Removable Media 23-5562

WebCode Test	Response
TEPC2R-5562	Date Created is the time the file was created / opened / moved on the USB, whereas the Date Modified is time content of a file was last modified/changed.
TVF9MD-5562	The files were in another location before being on the USB/in their current location.
UVZCUQ-5562	Modified date and time precede the Created date and time - most likely the files were copied onto the USB
V4KY4K-5562	That the files have been copied from the computer and were also created previously
WZGLVL-5562	"Modified" is older than "Created" - directory may have been copied from another location/drive
XA2A8Z-5562	Created time is when the data was copied to the USB device. The modified time is the timestamp from the original exhibit of Davids-Laptop
XJ99G2-5562	The difference in the created and modified timestamps of the directory indicate that the files in question appear to have been modified prior to being copied onto the USB drive.
XVDHZK-5562	[Participant did not return results for this question.]
Y63G92-5562	It would appear that the files contained in the folder were originally created on different device and the entire folder was copied onto the USB at the time stated in question 40
YPNENR-5562	The directory and files were copied to USB drive

Question 41: Compare the “Created” and “Modified” timestamps of the directory and files referenced in question 40. What do the relative “Created” and “Modified” timestamps indicate about the files’ placement on the USB?

Consensus Result:

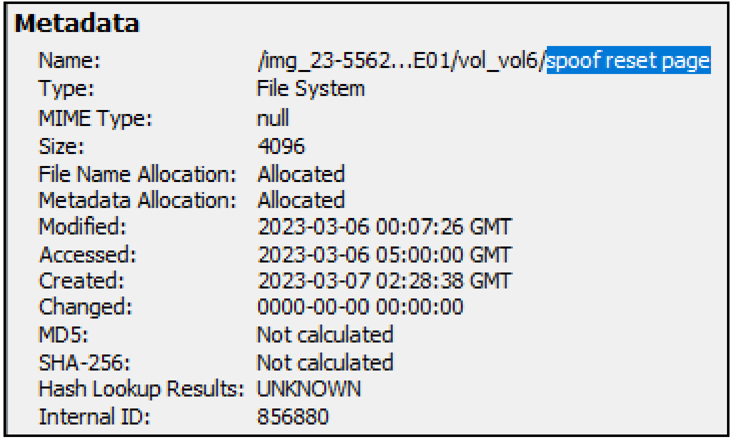
"They were copied from another volume" and variations of this text providing a similar description.

Expected Response Explanation:

When files are copied from one volume to another, they are given new created times but the modified times are not updated. Therefore, they will have created times AFTER their last modification times. This indicates they were created on a different storage device then copied to their current location.

Expected Response Illustration:

Autopsy metadata view of spoof reset page



Metadata

Name:	/img_23-5562...E01/vol_vol6/spoof reset page
Type:	File System
MIME Type:	null
Size:	4096
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-03-06 00:07:26 GMT
Accessed:	2023-03-06 05:00:00 GMT
Created:	2023-03-07 02:28:38 GMT
Changed:	0000-00-00 00:00:00
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup Results:	UNKNOWN
Internal ID:	856880

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 42 - Removable Media 23-5562

Question 42: Provide the URL contained in the file with SHA-1 hash 9f2271430d2cd6d897024ee589e8c9db192d8af2.

Manufacturer's Expected Response: http://portal.st.clotildes.institute/PasswordReset.php

WebCode Test	Response
2PJFNF-5562	http://portal.st.clotildes.institute/PasswordReset.php?h=$6$622609184c971ae1$bZkpwd/k0WVuvm0EulfPyhBmuJshJo/q3/63ksCfCMLvlEKMtcUU94WvM9r/Ul3CR.7594Az54zYaoS1/pi6T/
2VQ8RL-5562	http://portal.st.clotildes.institute/PasswordReset.php?h=$6$622609184c971ae1$bZkpwd/k0WVuvm0EulfPyhBmuJshJo/q3/63ksCfCMLvlEKMtcUU94WvM9r/Ul3CR.7594Az54zYaoS1/pi6T/
3CDK6E-5562	http://portal.st.clotildes.institute/PasswordReset.php
4U7ZP2-5562	http://portal.st.clotildes.institute/PasswordReset.php
68RW46-5562	http://portal.st.clotildes.institute/PasswordReset.php
6MKCN6-5562	http://portal.st.clotildes.institute/PasswordReset.php
6Q2RXW-5562	http://portal.st.clotildes.institute/PasswordReset.php?h=$6$622609184c971ae1$bZkpwd/k0WVuvm0EulfPyhBmuJshJo/q3/63ksCfCMLvlEKMtcUU94WvM9r/Ul3CR.7594Az54zYaoS1/pi6T/
6QKH3A-5562	url=(0162) http://portal.st.clotildes.institute/PasswordReset.php?h=$6$622609184c971ae1$bZkpwd/k0WVuvm0EulfPyhBmuJshJo/q3/
78PAK7-5562	http://portal.st.clotildes.institute/PasswordReset.php
7PQ8PM-5562	http://portal.st.clotildes.institute/PasswordReset.php?h=$6$622609184c971ae1$bZkpwd/k0WVuvm0EulfPyhBmuJshJo/q3/63ksCfCMLvlEKMtcUU94WvM9r/Ul3CR.7594Az54zYaoS1/pi6T/
7XZLMH-5562	http://portal.st.clotildes.institute/PasswordReset.php?h=$6$622609184c971ae1$bZkpwd/k0WVuvm0EulfPyhBmuJshJo/q3/63ksCfCMLvlEKMtcUU94WvM9r/Ul3CR.7594Az54zYaoS1/pi6T/
82VWX9-5562	http://portal.st.clotildes.institute/PasswordReset.php?h=$6$622609184c971ae1$bZkpwd/k0WVuvm0EulfPyhBmuJshJo/q3/63ksCfCMLvlEKMtcUU94WvM9r/Ul3CR.7594Az54zYaoS1/pi6T/
83AEYT-5562	http://portal.st.clotildes.institute/PasswordReset.php?h=$6$622609184c971ae1$bZkpwd/k0WVuvm0EulfPyhBmuJshJo/q3/63ksCfCMLvlEKMtcUU94WvM9r/Ul3CR.7594Az54zYaoS1/pi6T/
99QBZK-5562	http://portal.st.clotildes.institute/PasswordReset.php?h=$6$622609184c971ae1$bZkpwd/k0WVuvm0EulfPyhBmuJshJo/q3/63ksCfCMLvlEKMtcUU94WvM9r/Ul3CR.7594Az54zYaoS1/pi6T/
9J9Q8U-5562	Password help _ Reset your password.html
A8QHYB-5562	http://portal.st.clotildes.institute/PasswordReset.php
ADYU2Y-5562	http://portal.st.clotildes.institute/PasswordReset.php?h=$6$622609184c971ae1$bZkpwd/k0WVuvm0EulfPyhBmuJshJo/q3/63ksCfCMLvlEKMtcUU94WvM9r/Ul3CR.7594Az54zYaoS1/pi6T/
AKG6BT-5562	http://portal.st.clotildes.institute/PasswordReset.php
BFKZWF-5562	http://portal.st.clotildes.institute/PasswordReset.php
C4LMC9-5562	http://portal.st.clotildes.institute/PasswordReset.php?h=$6$622609184c971ae1$bZkpwd/k0WVuvm0EulfPyhBmuJshJo/q3/

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 42 - Removable Media 23-5562

WebCode Test	Response
CF2CBE-5562	http://portal.st.clotildes.institute/PasswordReset.php?h=$6$622609184c971ae1$bZkpwd/k0WVuvm0EulfPyhBmuJshJo/q3/63ksCfCMLvlEKMtcUU94WvM9r/Ul3CR.7594Az54zYaoS1/pi6T/
DXVP3C-5562	http://portal.st.clotildes.institute/PasswordReset.php
E2RHRZ-5562	http://portal.st.clotildes.institute/PasswordReset.php?h=$6$622609184c971ae1$bZkpwd/k0WVuvm0EulfPyhBmuJshJo/q3/63ksCfCMLvlEKMtcUU94WvM9r/Ul3CR.7594Az54zYaoS1/pi6T/
HW2LD2-5562	Password help _ Reset your password.html - http://portal.st.clotildes.institute/PasswordReset.php?h=$6$622609184c971ae1$bZkpwd/k0WVuvm0EulfPyhBmuJshJo/q3/63ksCfCMLvlEKMtcUU94WvM9r/Ul3CR.7594Az54zYaoS1/pi6T/
J84AQF-5562	http://portal.st.clotildes.institute/PasswordReset.php?h=$6$622609184c971ae1$bZkpwd/k0WVuvm0EulfPyhBmuJshJo/q3/63ksCfCMLvlEKMtcUU94WvM9r/Ul3CR.7594Az54zYaoS1/pi6T/
JGBUAC-5562	http://portal.st.clotildes.institute/PasswordReset.php?h=$6$622609184c971ae1$bZkpwd/k0WVuvm0EulfPyhBmuJshJo/q3/63ksCfCMLvlEKMtcUU94WvM9r/Ul3CR.7594Az54zYaoS1/pi6T/
JL32PY-5562	http://portal.st.clotildes.institute/PasswordReset.php?h=$6$622609184c971ae1$bZkpwd/k0WVuvm0EulfPyhBmuJshJo/q3/63ksCfCMLvlEKMtcUU94WvM9r/Ul3CR.7594Az54zYaoS1/pi6T/
KR28JR-5562	http://portal.st.clotildes.institute/PasswordReset.php
KXRBW6-5562	http://portal.st.clotildes.institute/PasswordReset.php
NE7TEF-5562	http://portal.st.clotildes.institute/PasswordReset.php
PFEMA7-5562	http://portal.st.clotildes.institute/PasswordReset.php?h=$6$622609184c971ae1$bZkpwd/k0WVuvm0EulfPyhBmuJshJo/q3/63ksCfCMLvlEKMtcUU94WvM9r/Ul3CR.7594Az54zYaoS1/pi6T/
PPMYM4-5562	http://portal.st.clotildes.institute/PasswordReset.php?h=$6$622609184c971ae1$bZkpwd/k0WVuvm0EulfPyhBmuJshJo/q3/63ksCfCMLvlEKMtcUU94WvM9r/Ul3CR.7594Az54zYaoS1/pi6T/
PTKDEZ-5562	http://portal.st.clotildes.institute/PasswordReset.php?h=$6$622609184c971ae1$bZkpwd/k0WVuvm0EulfPyhBmuJshJo/q3/63ksCfCMLvlEKMtcUU94WvM9r/Ul3CR.7594Az54zYaoS1/pi6T/
RAK67E-5562	http://portal.st.clotildes.institute/PasswordReset.php?h=$6$622609184c971ae1$bZkpwd/k0WVuvm0EulfPyhBmuJshJo/q3/63ksCfCMLvlEKMtcUU94WvM9r/Ul3CR.7594Az54zYaoS1/pi6T/
RBBDCA-5562	http://portal.st.clotildes.institute/PasswordReset.php?h=$6$622609184c971ae1$bZkpwd/k0WVuvm0EulfPyhBmuJshJo/q3/63ksCfCMLvlEKMtcUU94WvM9r/Ul3CR.7594Az54zYaoS1/pi6T/
RGH4EF-5562	http://portal.st.clotildes.institute/PasswordReset.php?h=$6$622609184c971ae1$bZkpwd/k0WVuvm0EulfPyhBmuJshJo/q3/63ksCfCMLvlEKMtcUU94WvM9r/Ul3CR.7594Az54zYaoS1/pi6T/
RRXTDK-5562	url=index.php?modfunc=logout&reason=javascript&token=979c03782f542775f1fe977c95d8c9d1
TC4JAF-5562	http://portal.st.clotildes.institute/PasswordReset.php
TEPC2R-5562	http://portal.st.clotildes.institute/PasswordReset.php?h=$6$622609184c971ae1$bZkpwd/k0WVuvm0EulfPyhBmuJshJo/q3/63ksCfCMLvlEKMtcUU94WvM9r/Ul3CR.7594Az54zYaoS1/pi6T/
TVF9MD-5562	http://portal.st.clotildes.institute/PasswordReset.php
UVZCUQ-5562	http://portal.st.clotildes.institute/PasswordReset.php?h=$6$622609184c971ae1$bZkpwd/k0WVuvm0EulfPyhBmuJshJo/q3/63ksCfCMLvlEKMtcUU94WvM9r/Ul3CR.7594Az54zYaoS1/pi6T/
V4KY4K-5562	http://portal.st.clotildes.institute/PasswordReset.php?h=$6$622609184c971ae1$bZkpwd/k0WVuvm0EulfPyhBmuJshJo/q3/63ksCfCMLvlEKMtcUU94WvM9r/Ul3CR.7594Az54zYaoS1/pi6T/

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 42 - Removable Media 23-5562

WebCode Test	Response
WZGLVL-5562	http://portal.st.clotildes.institute/PasswordReset.php?h=$6$622609184c971ae1$bZkpwd/k0WVuvm0EulfPyhBmuJshJo/q3/63ksCfCMLvlEKMtcUU94WvM9r/Ul3CR.7594Az54zYaoS1/pi6T/
XA2A8Z-5562	http://portal.st.clotildes.institute/PasswordReset.php
XJ99G2-5562	http://portal.st.clotildes.institute
XVDHZK-5562	[Participant did not return results for this question.]
Y63G92-5562	http://portal.st.clotildes.institute/PasswordReset.php?h=
YPNENR-5562	http://portal.st.clotildes.institute/PasswordReset.php?

Question 42: Provide the URL contained in the file with SHA-1 hash 9f2271430d2cd6d897024ee589e8c9db192d8af2.

Consensus Result:

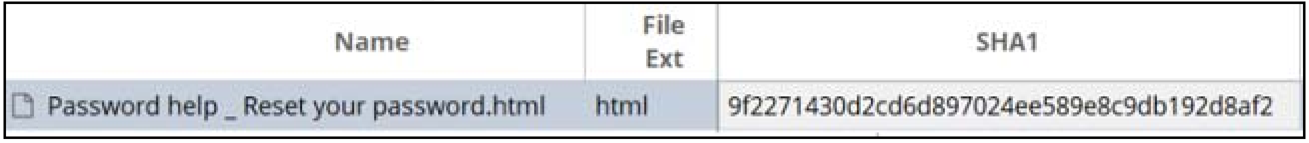
http://portal.st.clotildes.institute/PasswordReset.php and variations representing the same information.

Expected Response Explanation:

Password help _ Reset your password.html has the above SHA1 hash. The second line of the file contains the URL http://portal.st.clotildes.institute/PasswordReset.php.

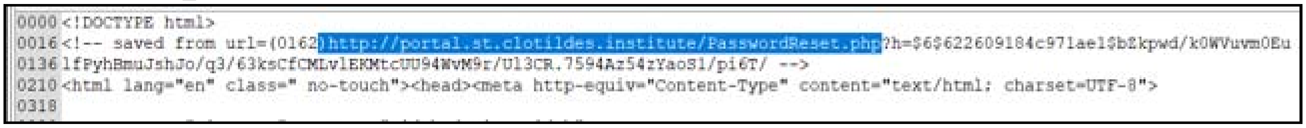
Expected Response Illustration:

EnCase table view of Password help _ Reset your password.html



Name	File Ext	SHA1
Password help _ Reset your password.html	html	9f2271430d2cd6d897024ee589e8c9db192d8af2

Password help _ Reset your password.html



```
0000 <!DOCTYPE html>
0016 <!-- saved from url=(0162)http://portal.st.clotildes.institute/PasswordReset.php?h=$6$622609184c971ae1$bZkpwd/k0WVuvm0Eu
0136 lfPyhBmuJshJo/q3/63ksCfCMLvlEKMtcUU94WvM9r/Ul3CR.7594Az54zYaoS1/pi6T/ -->
0210 <html lang="en" class=" no-touch"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
0318
```

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 43 - Removable Media 23-5562

Question 43: Provide the SHA256 hash of GracefulGrievingUrchin.rar?

Manufacturer's Expected Response: B53E2BE6204E0645558D79333BFD17AFF33DE31E06E178C6CF243BB175EFDA98

WebCode Test	Response
2PJFNF-5562	b53e2be6204e0645558d79333bfd17aff33de31e06e178c6cf243bb175efda98
2VQ8RL-5562	b53e2be6204e0645558d79333bfd17aff33de31e06e178c6cf243bb175efda98
3CDK6E-5562	B53E2BE6204E0645558D79333BFD17AFF33DE31E06E178C6CF243BB175EFDA98
4U7ZP2-5562	b53e2be6204e0645558d79333bfd17aff33de31e06e178c6cf243bb175efda98
68RW46-5562	b53e 2be6 204e 0645 558d 7933 3bfd 17af f33d e31e 06e1 78c6 cf24 3bb1 75ef da98
6MKCN6-5562	b53e2be6204e0645558d79333bfd17aff33de31e06e178c6cf243bb175efda98
6Q2RXW-5562	b53e2be6204e0645558d79333bfd17aff33de31e06e178c6cf243bb175efda98
6QKH3A-5562	b53e2be6204e0645558d79333bfd17aff33de31e06e178c6cf243bb175efda98
78PAK7-5562	b53e2be6204e0645558d79333bfd17aff33de31e06e178c6cf243bb175efda98
7PQ8PM-5562	b53e2be6204e0645558d79333bfd17aff33de31e06e178c6cf243bb175efda98
7XZLMH-5562	B53E2BE6204E0645558D79333BFD17AFF33DE31E06E178C6CF243BB175EFDA98
82VWX9-5562	B53E2BE6204E0645558D79333BFD17AFF33DE31E06E178C6CF243BB175EFDA98
83AEYT-5562	b53e2be6204e0645558d79333bfd17aff33de31e06e178c6cf243bb175efda98
99QBZK-5562	B53E2BE6204E0645558D79333BFD17AFF33DE31E06E178C6CF243BB175EFDA98
9J9Q8U-5562	b53e2be6204e0645558d79333bfd17aff33de31e06e178c6cf243bb175efda98
A8QHYB-5562	B53E2BE6204E0645558D79333BFD17AFF33DE31E06E178C6CF243BB175EFDA98
ADYU2Y-5562	b53e2be6204e0645558d79333bfd17aff33de31e06e178c6cf243bb175efda98
AKG6BT-5562	b53e2be6204e0645558d79333bfd17aff33de31e06e178c6cf243bb175efda98
BFKZWF-5562	b53e2be6204e0645558d79333bfd17aff33de31e06e178c6cf243bb175efda98
C4LMC9-5562	B53E2BE6204E0645558D79333BFD17AFF33DE31E06E178C6CF243BB175EFDA98
CF2CBE-5562	b53e2be6204e0645558d79333bfd17aff33de31e06e178c6cf243bb175efda98

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 43 - Removable Media 23-5562

WebCode Test	Response
DXVP3C-5562	b53e2be6204e0645558d79333bfd17aff33de31e06e178c6cf243bb175efda98
E2RHRZ-5562	B53E2BE6204E0645558D79333BFD17AFF33DE31E06E178C6CF243BB175EFDA98
HW2LD2-5562	B53E2BE6204E0645558D79333BFD17AFF33DE31E06E178C6CF243BB175EFDA98
J84AQF-5562	b53e2be6204e0645558d79333bfd17aff33de31e06e178c6cf243bb175efda98
JGBUAC-5562	b53e2be6204e0645558d79333bfd17aff33de31e06e178c6cf24bb175efda98
JL32PY-5562	B53E2BE6204E0645558D79333BFD17AFF33DE31E06E178C6CF243BB175EFDA98
KR28JR-5562	b53e2be6204e0645558d79333bfd17aff33de31e06e178c6cf243bb175efda98
KXRBW6-5562	B53E2BE6204E0645558D79333BFD17AFF33DE31E06E178C6CF243BB175EFDA98
NE7TEF-5562	B53E2BE6204E0645558D79333BFD17AFF33DE31E06E178C6CF243BB175EFDA98
PFEMA7-5562	b53e2be6204e0645558d79333bfd17aff33de31e06e178c6cf243bb175efda98
PPMYM4-5562	b53e2be6204e0645558d79333bfd17aff33de31e06e178c6cf243bb175efda98
PTKDEZ-5562	b53e2be6204e0645558d79333bfd17aff33de31e06e178c6cf243bb175efda98
RAK67E-5562	B53E2BE6204E0645558D79333BFD17AFF33DE31E06E178C6CF243BB175EFDA98
RBBDCA-5562	B53E2BE6204E0645558D79333BFD17AFF33DE31E06E178C6CF243BB175EFDA98
RGH4EF-5562	B53E2BE6204E0645558D79333BFD17AFF33DE31E06E178C6CF243BB175EFDA98
RRXTDK-5562	B53E2BE6204E0645558D79333BFD17AFF33DE31E06E178C6CF243BB175EFDA98
TC4JAF-5562	b53e2be6204e0645558d79333bfd17aff33de31e06e178c6cf243bb175efda98
TEPC2R-5562	b53e2be6204e0645558d79333bfd17aff33de31e06e178c6cf243bb175efda98
TVF9MD-5562	B53E2BE6204E0645558D79333BFD17AFF33DE31E06E178C6CF243BB175EFDA98
UVZCUQ-5562	B53E2BE6204E0645558D79333BFD17AFF33DE31E06E178C6CF243BB175EFDA98
V4KY4K-5562	b53e2be6204e0645558d79333bfd17aff33de31e06e178c6cf243bb175efda98
WZGLVL-5562	b53e2be6204e0645558d79333bfd17aff33de31e06e178c6cf243bb175efda98

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 43 - Removable Media 23-5562

WebCode Test	Response
XA2A8Z-5562	b53e2be6204e0645558d79333bfd17aff33de31e06e178c6cf243bb175efda98
XJ99G2-5562	B53E2BE6204E0645558D79333BFD17AFF33DE31E06E178C6CF243BB175EFDA98
XVDHZK-5562	b53e2be6204e0645558d79333bfd17aff33de31e06e178c6cf243bb175efda98
Y63G92-5562	B53E2BE6204E0645558D79333BFD17AFF33DE31E06E178C6CF243BB175EFDA98
YPNENR-5562	b53e2be6204e0645558d79333bfd17aff33de31e06e178c6cf243bb175efda98

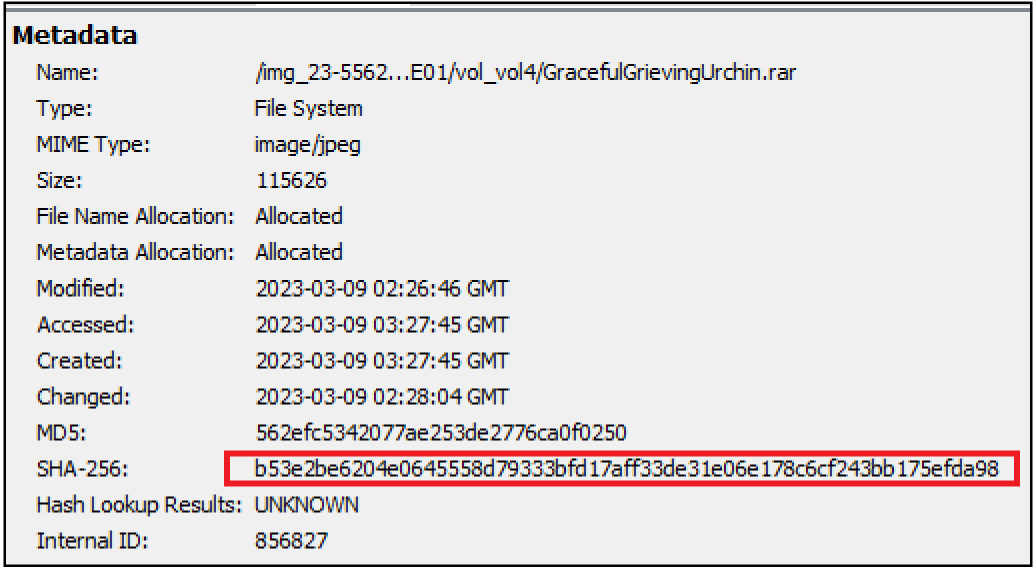
Question 43: Provide the SHA256 hash of GracefulGrievingUrchin.rar?

Consensus Result:
B53E2BE6204E0645558D79333BFD17AFF33DE31E06E178C6CF243BB175EFDA98

Expected Response Explanation:
SHA256 hashes can be computed with any reliable hashing tool.

Expected Response Illustration:

Autopsy metadata view for GracefulGrievingUrchin.rar



Metadata

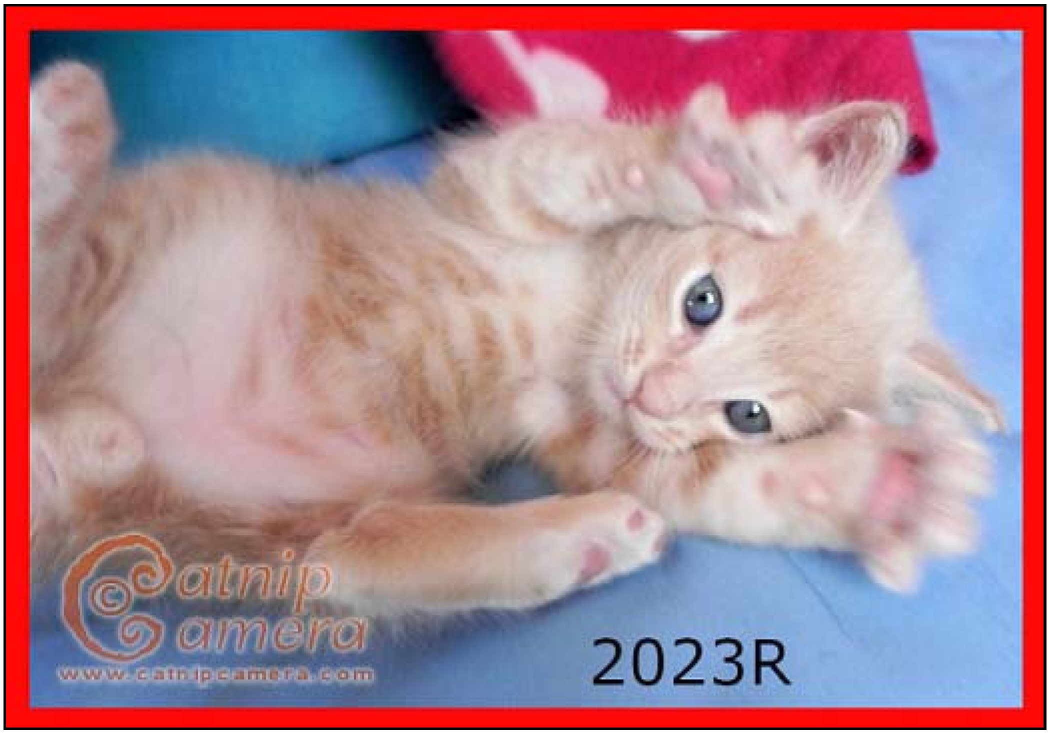
Name:	/img_23-5562...E01/vol_vol4/GracefulGrievingUrchin.rar
Type:	File System
MIME Type:	image/jpeg
Size:	115626
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-03-09 02:26:46 GMT
Accessed:	2023-03-09 03:27:45 GMT
Created:	2023-03-09 03:27:45 GMT
Changed:	2023-03-09 02:28:04 GMT
MD5:	562efc5342077ae253de2776ca0f0250
SHA-256:	b53e2be6204e0645558d79333bfd17aff33de31e06e178c6cf243bb175efda98
Hash Lookup Results:	UNKNOWN
Internal ID:	856827

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 43 - Removable Media 23-5562

GracefulGrievingUrchin.rar



Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 44 - Removable Media 23-5562

Question 44: What is the filetype (MIME) of GracefulGrievingUrchin.rar?

Manufacturer's Expected Response: jpeg (or jpg) image file

WebCode Test	Response
2PJFNF-5562	JPG
2VQ8RL-5562	image/jpeg
3CDK6E-5562	image/jpeg
4U7ZP2-5562	image/jpeg
68RW46-5562	image/jpeg
6MKCN6-5562	jpeg
6Q2RXW-5562	JPEG EXIF
6QKH3A-5562	image/jpeg
78PAK7-5562	image/jpeg
7PQ8PM-5562	image/jpeg
7XZLMH-5562	JPEG/JFIF
82VWX9-5562	JPEG file (image/jpeg)
83AEYT-5562	image/jpeg
99QBZK-5562	JPG
9J9Q8U-5562	image/jpeg as a .rar
A8QHYB-5562	image/jpeg
ADYU2Y-5562	jpg
AKG6BT-5562	Jpeg image
BFKZWF-5562	image/jpeg
C4LMC9-5562	JPG
CF2CBE-5562	Image\JPEG

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 44 - Removable Media 23-5562

WebCode Test	Response
DXVP3C-5562	.jpg = JPEG
E2RHRZ-5562	JPEG
HW2LD2-5562	JPEG (EXIF)
J84AQF-5562	JPG
JGBUAC-5562	.rar - Archive
JL32PY-5562	jpg
KR28JR-5562	image/jpeg
KXRBW6-5562	The file is shown with the .rar extension but the file is actually a .jpg
NE7TEF-5562	jpeg
PFEMA7-5562	Picture, JPEG Image Standard
PPMYM4-5562	Image\JPEG
PTKDEZ-5562	image/jpeg
RAK67E-5562	Image/jpeg
RBBDCA-5562	JPG (Image)
RGH4EF-5562	JPEG
RRXTDK-5562	image/jpeg
TC4JAF-5562	image/jpeg
TEPC2R-5562	JPEG EXIF
TVF9MD-5562	JPEG
UVZCUQ-5562	image/jpeg
V4KY4K-5562	(File Image) *.jpg [FF D8 FF EO ..]
WZGLVL-5562	image/jpeg

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 44 - Removable Media 23-5562

WebCode Test	Response
XA2A8Z-5562	JPG
XJ99G2-5562	Image/jpg
XVDHZK-5562	image/jpeg
Y63G92-5562	ÿØÿà jiff (image file)
YPNENR-5562	image/jpeg

Question 44: What is the filetype (MIME) of GracefulGrievingUrchin.rar?

Consensus Result:

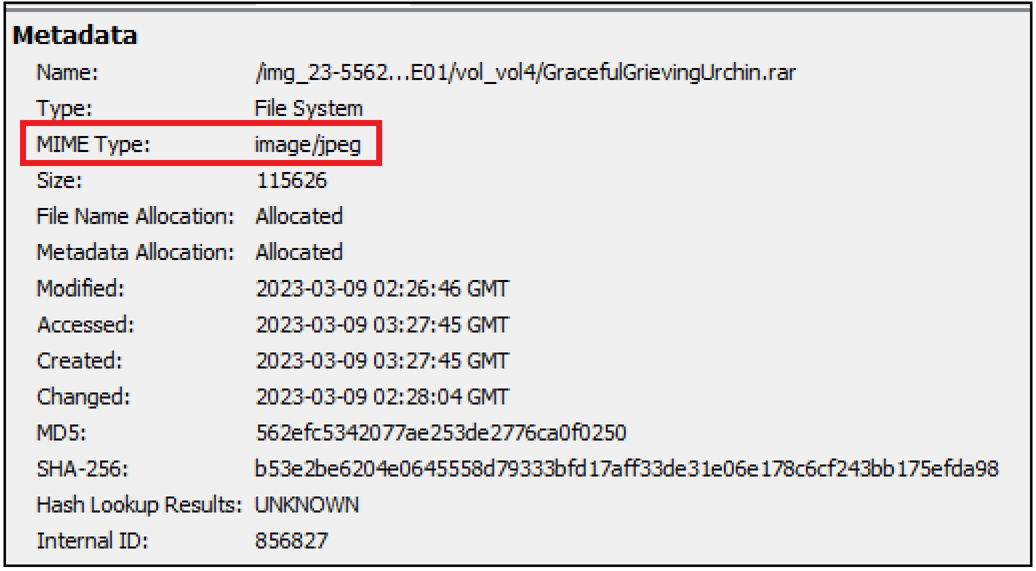
JPEG or image/jpeg

Expected Response Explanation:

GracefulGrievingUrchin.rar is a jpeg photograph file containing an image of a kitten. Its file extension has been changed to .rar so it will not be displayed as an image by Windows or by a forensic tool if file signatures analysis has not been performed. However, the file signature contained in the first 10 bytes of the file, FF D8 FF E0 00 10 4A 46 indicates it is a jpeg image.

Expected Response Illustration:

Autopsy metadata view for GracefulGrievingUrchin.rar



Metadata

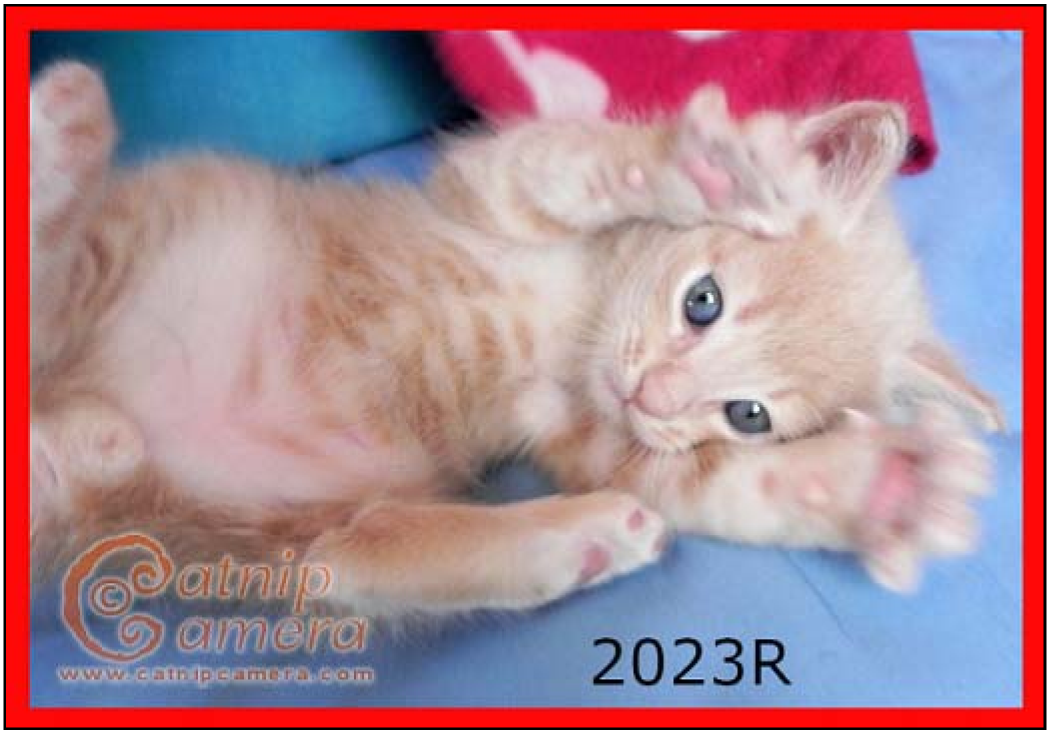
```
Name:                  /img_23-5562...E01/vol_vol4/GracefulGrievingUrchin.rar
Type:                  File System
MIME Type:             image/jpeg
Size:                  115626
File Name Allocation:  Allocated
Metadata Allocation:   Allocated
Modified:              2023-03-09 02:26:46 GMT
Accessed:              2023-03-09 03:27:45 GMT
Created:               2023-03-09 03:27:45 GMT
Changed:               2023-03-09 02:28:04 GMT
MD5:                   562efc5342077ae253de2776ca0f0250
SHA-256:               b53e2be6204e0645558d79333bfd17aff33de31e06e178c6cf243bb175efda98
Hash Lookup Results:   UNKNOWN
Internal ID:           856827
```

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 44 - Removable Media 23-5562

GracefulGrievingUrchin.rar



Additional Comments

TABLE 3

WebCode Test	Additional Comments
2PJFNF-5562	Enacase 22.1
3M9X4P-5561	Question 6: difficult to understand what you actually want here. This questions needs to be reworded. Question 12: your timestamp doesn't match anything exact here. Either say "approximately" for the time or double check the timestamp you put in the question. Question 15: Up to this point, you've had us bounce from UTC to local time and back again. Here, you don't indicate any timezone at all. Not cool. Be consistent.
4U7ZP2-5562	For question 29, it is stated that the image provided is the only one that meets the description indicated in the statement, however, it maintains an MD5 hash value different from that indicated in the statement. For question 39, it is stated that the image provided is the only one that meets the description indicated in the statement, however, it maintains a SHA1 hash value different from that indicated in the statement.
68RW46-5562	Q27: Two other (unique) files are found which meet the criteria. The black font in these images spell out: 2023T, 2023A
6DZZCR-5561	A couple of these questions contained incorrect information about the files in within the question. This made the test take much longer because I spent a lot of time verifying I couldn't find files with particular attributes or specific timestamps.
6Q2RXW-5562	There is ambiguity in question 35. It can be answered in two ways. If we consider the active partition as "The partition that has marked active" then the answer would be "0" (zero). However, as per previous year's test (22-5562) manufacturer's summary, present non-deleted partitions were considered as active. If same principle is followed, answer would be "3" (three).
6TR3NP-5561	Thank you!
72ZUTD-5561	I was unable to locate the images requested in questions 29 and 30 using the supplied MD5. I had to manually locate the pictures using S21 as the MD5 values did not match any files on our processed X-Ways. I was unable to locate the keyword and file in question 31.
7JUP4F-5561	Sha 1 32bit calculations used. suggest using sha-256 as a secondary, not sha1 which can be two different algorithms for a 16bit/32bit equation. The "4 owl" picture was not found, a thumbnail was recovered but not used as it was a different MD5. question 29 and 30 wording should not include the term unallocated, not universal term and the data is technically still in allocated space, so its a confusing question forcing people to look in the literal unallocated sections instead of the file being anywhere on the hard drive until it is overwritten (allocated space). its best to refer to the point of the question as "deleted file"
83AEYT-5562	1. Regarding the question 24: The answer to this question was based on the folders and files located on «/Users/David Lightman/AppData/Roaming/Thunderbird/Profiles/0jug9sv4.default-release/ImapMail/» that were created when the two email accounts were configured in the user installed IMAP email client for user David Lightman. Indeed, the file “folderTree.json” is showing only one email which is “admin@clotildes.institute”, this can be explained by the effect that the second email “david.lightman75@outlook.com” was deleted. 2. Regarding the question 27: Another alternative answer for this question is:2023R

TABLE 3

WebCode Test	Additional Comments
98ZV8C-5561	The user of the device account David Lightman was apparently created a spear-fishing email for stephen.falken@stclotildes.institute, to alter other person's grades for financial gain.
99QBZK-5562	Qu 35) Active was taken to mean bootable (1 Active bootable partition, but 3 Partitions in total). It is unknown if this is what the question was asking.
9J9Q8U-5562	Tools Used: FTK Imager 4.2.0.13 Magnet Axiom v6.11.0.34807 TX1 #19: This question is confusing because the user is clearly Mark which is in the file path. But the owner of the file (before it was deleted) was David. So I'd be more specific here about what it is you want to see. This is especially true if a machine is determining if these questions are right or wrong. If a human is reading and then deciding the accuracy of the answers, then they may be able to tell what the test-taker is trying to explain. #31: I spent 1 1\2 hours on this question. To me, it is not within the scope of a proficient examiner. This should be reserved for an expert examiner. This answer was within the registry but, based on the question, the examiner would not know to look there. Maybe give it some context, as in, "(check the registry)" or something to that nature. Less than 1% of intrusions that I've worked involve a sophisticated attacker who adds/hides things in the registry. Additionally, this questions asks for "word and location (path and filename) where it is found". This is a registry data entry. To me there really isn't a file path for this. It's not a URL necessarily. It's just a data entry into the registry. Not sure I even got this sub-question correct. #32: the rtf file is "Superpostiion" but the document itself is about superposition. Just an observation. Not sure if this was by design or not. #34 and #43: Even though it's better to use, not a lot of tools use SHA-256. Magnet Axiom or FTK does not hash in this format. If a test-taker only has access to these tools, he/she would not be able to answer these questions. I don't think it's a fair assumption that they have these tools yet. I had to use a TX1 just to get the answer for the USB SHA-256.
ABK3AJ-5561	Currently, there is no analysis being conducted on the data collected from computers during examinations at this lab. The evidence is being imaged, a portable case is being created using Axiom, and the information obtained is returned to the investigating agency. No further testing is being conducted at this time.
ACTERK-5561	Currently, no analysis is being conducted on the data collected from computers during examinations at this lab. The evidence is imaged, a portable case is created using Axiom, and the information obtained is returned to the investigating agency. No further testing is being conducted at this time.
CKAXYB-5561	Hardware: Exam 9: Custom built Corsair desktop computer. Windows 10 Pro v21H2, OS Build: 19044.1706, BCFSU# 02021022514191970398. Software: AccessData® FTK Imager v4.7.1.2, AccessData® Forensic Toolkit® v7.6.0.618, AccessData® Registry Viewer v2.0.0, Magnet Forensics® AXIOM Process v7.2.0.36145, Magnet Forensics® AXIOM Examine v7.2.0.36145, WinHex 20.8, TeraCopy v3.9.2
DGVH9K-5561	1. When asking for SHA-1 hashes, you need to clarify Base 16 or Base 32. This is an ongoing problem with the CTS exams. 21. What is a "regular" file - There are lots of System files which are regular files? There are several "Alias" files which also come back as images. There is one .txt file. The .sys files have the oldest dates, but there are over 10 of them with the same date/time, including these 6: FW_7662.bin, Patch_7662.bin, amdgpio2.sys, amdi2c.sys, bcmfn2.sys. This question is very poorly written.
E4ZNBG-5561	Questions 21/22 were too vague/ambiguous.

TABLE 3

WebCode Test	Additional Comments
EV7HHF-5561	Multiple questions are tools specific. The results are based on how the tool gets to a result, processes the information for interpretation, etc... For a proficiency exam these questions should be based on the scientific principles not a specific tool. Answers should be just as efficiently located without the tool that was used to build the exam. Most of the questions follow this direction but they're a few that the tool that was used to build the exam is almost "needed" to get to the answer.
JGBUAC-5562	FTK Imager produces different MD5 and SHA1 due to including the CRC check in an E01. This means it will be different from HashCalc because HashCalc will look at the file as a whole including the CRC check. Some of the date and times I have provided need changing too. For example, TT:TT:TT is the format I used. However, the format required is TT:TT. The answers will only contain the first and second part of the time.
JJDU63-5561	The MD5 hash in question 30 was nowhere to be found in the image.
KR4V3R-5561	For future questions requesting GPS coordinates in decimal format (e.g. question 28), please specify if you want the value rounded.
NE7TEF-5562	Have a nice day
P8ZNUA-5561	question 12 regarding the whatsapp message transfer states 7:56 for the time sent. It was 7:55. Please advise.
PFEMA7-5562	Questions 21 and 22 were very unclear. What is a "regular" file is an ambiguous question. The answer I placed in 21 and 22, wincatyawn.sys, is what I believe the CTS is looking for but it does not fit the entire question. They specify that it should not be hidden, deleted, alias, etc. This would technically make wincatyawn.sys an alias file, however every other file aside from a text file is a system or bin file and makes no sense as an answer.
PFVN93-5561	For question 10, the configured time zone was eastern standard time with daylight savings enabled starting the second Sunday of March. The date of the last shutdown was prior to the second Sunday of March. For question 30, I located a jpeg matching the description of the image provided, but was unable to locate the MD5 provided. I carved, opened compressed files, searched for the MD5, and manually reviewed the unallocated space, but could not locate it. I provided the SHA1 for the jpeg matching the description provided in question 30.
QRJAR3-5561	The MD5 hash listed on the scenario page (e249654cc0fbef3ecfb40cd7302a79e2) did not match the stored hash of the 23-5561.E01 file I downloaded. [MD5] Computed hash: 723b38249ecdc873485e89909219504b. Image hash: 723b38249ecdc873485e89909219504b. Verify result: Match. [SHA1] Computed hash: b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1. Image hash: b5d7dda9b578e937f1ade6f90c13cfbbf7cad8f1. Verify result: Match.
QTHAXU-5561	Answer #15 is not being shown completely in the view of previous form. I include the answer here for reference: Difference is among the first characters of the URLs: http://portal.stclotildes.institute/ and http://portal.st.clotildes.institute/. Specifically: st.clotides and stclotildes.

TABLE 3

WebCode Test	Additional Comments
V4KY4K-5562	It is recommendable in the future that translations be made for other languages due to the complexity of technical English when it comes to interpreting what is being asked exactly, since sometimes it is not easy to specify an answer due to the difficulty of the translation and how precise it is. It must be the work of computer forensics
WC9E49-5561	#26 - email subject is wrong.
WD8DHB-5561	The PT should be more difficult.
WX2YKZ-5561	Currently, there is no analysis being conducted on the data collected from computers during examinations at this lab. The evidence is being imaged, a portable case is being created using Axiom, and the information obtained is returned to the investigating agency. No further testing is being conducted at this time.
XA2A8Z-5562	Would be more engaging and realistic if the questions related directly to the scenario, Digital Forensic work is usually followed with a report which is designed to prove a point. Would be nice to bring all of the evidence together to prove or disprove a case.
XEVDXV-5561	Currently, there is no analysis being conducted on the data collected from computers during examinations at this lab. The evidence is being imaged, a portable case is being created using Axiom , and the information obtained is returned to the investigating agency. No further testing is being conducted at this time.
XJ99G2-5562	Please note that we have had email communication with [CTS Employee] regarding issues around the cryptographic hashes. The provided hash values for question 1, 29, 30 and 39 did not correspond to the the hash values generated on our side.
XVDHZK-5562	We were only looking for scoring in the acquisition of storage media. Our acquisition tools were unable to locate the files referenced in questions 40, 41 and 42.

-End of Report-
(Appendix may follow)