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. 22-5561/2 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 95 participants, 43 of which also returned results associated with the physical USB. These results are compiled in the following tables:

Report Contents:

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. The extracted data was provided in a 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 22-5562: 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 homicide case was created to generate user data on a Windows Hard Drive. The execution of the test production took place within the following date range, 1 February 2022 – 6 March 2022. 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 22-5562.

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 participants to download. MD5 digest (cryptographic checksums, or 'hashes') was calculated for the compressed data and provided to participants to enable validation of a successful download of the files.

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: libewf 20170703, EnCase 8.11, Autopsy 4.19.3, Exiftool 12.05, Registry Explorer 1.6.0.0, Windows 10.0.19044 and included utilities (CMD, Powershell 5.1.19041, EventViewer), EvtxExplorer 0.6.5.0, RegRipper 3.9, FTKimager 4.5.0.3, PECmd 1.5.0.0, HxD 2.4.0.0. CTS does not endorse any particular tools.

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

SCENARIO PROVIDED TO PARTICIPANTS
You have been assigned to conduct computer forensic analysis in support of a homicide investigation. The victim was discovered deceased in their home by apparent strangulation. The Medical Examiner’s report estimates the victim died sometime between 10 P.M. and midnight (EST), March 5th, 2022. Subsequent investigation by the local police department identified Alex Andersen as a person of interest in the investigation.
You are being provided with:
-a copy of the forensic image acquired from a computer found in the victim's apartment and
-a USB flash storage device surrendered by Andersen during an interview by police (5562 only)
You have appropriate legal authority to examine the device for evidence related to the suspected homicide and perform analysis to answer the following questions (5561).
You have appropriate legal authority to examine both devices for evidence related to the suspected homicide (5562 only).
Perform analysis of the data on these devices to answer the following questions. The USB device should be handled as an item of original seized evidence provided to your lab for acquisition and analysis (5562 only).

Manufacturer's Information, continued

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

1 **Provide the Stored Acquisition SHA-1 Hash for the provided image, 22.5561.E01.**
a7b250cb09fcd6e5e362fcbc268ec6df12dbd418

2 **How many partitions are on the hard drive (device imaged as 22-5561.E01)? Provide a NUMERIC response.**
2

3 **What is the hostname for this computer?**
DESKTOP-RNO1O54

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?**
Jessie Jenkins

6 **When was the operating system installed? Provide your response in UTC+0, using the date/time picker to select the date and time (24-hour).**
2022-02-02 05:31

7 **When was the computer LAST shutdown gracefully? Provide your response in UTC+0, using the date/time picker to select the date and time (24-hour).**
2022-03-06 05:12

8 **Provide the username of the LAST user account created on the system.**
chris

9 **What is the Security ID (SID) of the registered owner's user account?**
S-1-5-21-3501254099-4204809888-2000606956-1002

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

11 **Provide the SHA 1 hash value for the jpeg (.jpg) file captured with a DJI XT2 camera.**
03be76ca62406c58e4778f1afac61ce02fe63cbe

12 **What search terms did the Jessie Jenkins user search for (FIRST) on google.com on 02/10/2022 at 21:31:07 (UTC-05:00)?**
local meetups in reston

13 **Provide the path and filename of the file containing the term "Micrathene".**
C:\Users\Jessie Jenkins\Documents\Book1.xlsx

14 **What event was scheduled to occur at the location user Jessie Jenkins searched for directions to on 02/24/2022 21:11:51 (UTC-05:00)?**
Mardis Gras Masquerade Party (Meetup) at Rebel Taco in Washington, DC

15 **What was the name of the wireless network to which the computer was connected?**
JenkinsHome

16 **What IP address was assigned by this network?**
192.168.3.121

Manufacturer's Information, continued

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

17 **From whom (provide name and email address) did Jessie Jenkins receive an email on 02/26/2022 17:39 (UTC-05:00)?**
Name: Alex Andersen
Email: alwaysalexandersen@gmail.com

18 **Where and when did Jessie ultimately agree to meet the person from the response for question 17?**
Where: Founding Farmers Reston
When: 2022-03-05 20:00

19** **According to the Windows Event Logs, what comment was given for the computer shutdown on 2/25/22 3:29 AM (UTC+0)?**
time for bed

20 **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 picker to select the date and time (24-hour).**
Date & Time: 2022-03-06 05:07
User Account: Jessie Jenkins

21 **How many failed logins immediately preceded the successful one in question 20? Provide a NUMERIC response.**
6

22 **How many times was the Electrum program executed (not the installer)? Provide a NUMERIC response.**
6

23 **What is the original (pre-deletion) path and name of $IBB0QWJ.doc (found in the user Jessie Jenkins' Recycle Bin)?**
C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc

24 **What is the file TYPE for the file with SHA-1 hash 61cf7b3e81a6276e1ae5953fcf09f1e99f5bea78?**
File Type: Portable Network Graphic or PNG

25** **What is the $FILE_NAME Attribute created date and time for PoorFairJaguar.html? Provide your response in UTC+0, using the date/time picker to select the date and time (24-hour).**
2022-02-20 18:55 (UTC+0)

26 **What does the HostUrl for PXL_20211121_130028206.jpg indicate about its source?**
Downloaded from the Internet as a mail-attachment

27 **What email client and version did the administrator install?**
Mozilla Thunderbird (x64 en-US) v.91.6

28 **What is the file status of C:\Users\Jessie Jenkins\Pictures\132p61j53ai81.jpg?**
Deleted, not overwritten

29 **Who is listed as the author of AliveTroubledSalmon.doc?**
vhamocbrewsp

30 **What is the name of the file that contains a string consisting of two letters, five numbers, "CW", and four numbers (e.g., AA12345CW1234)?**
CheerfulSuperDonkey.text

Manufacturer's Information, continued

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

31 **Who has the U.S. phone number beginning in "57" and ending in "57"? What is the full phone number?**
Who: Jessie Jenkins
Phone Number: (571) 302-4357

32 **For the photo that was sent to Jesse [Jessie] Jenkins from John Jenkins, provide the name of the file and the GPS coordinates where the photo was taken. Provide your response in the format: ##.#### N/S, ##.#### E/W**
18.3626 N, 64.7298 W and other versions representing the same information

Manufacturer's Information, continued

Removable Media Analysis: *USB Drive*
Test No. 22-5562

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

33** **Provide the SHA256 hash for the USB device.**
D7C4034A6A0EB86785B61EAFF1869CBDA440B01FAD959EBF8A1FE89384327D12

34** **How many ACTIVE partitions are on the device? Provide a NUMERIC response.**
1

35 **What is the volume serial number of the NTFS partition (The first 4 bytes (little endian)) as it would be reported/displayed by Windows?**
2469-CE18

36 **What is the name (Volume Label) of the NTFS Partition?**
New Volume

37 **What text is visible in the photo file containing six cats/kittens?**
LMAO

38 **What is the file TYPE of the file with SHA-1 hash 613cd9e96da949694014ccf77e63005cb99d7d49?**
JPEG, JPG or JFIF

39** **Provide the SHA256 hash of the file named default_wallet (not default_wallet.backup).**
20649e413c8dbe9f2248dbf6cc74eb39f9489ec17d7e4004f4df69c7e8e10848

40 **On what date and time was the file default_wallet created on the USB media? Provide your response in GMT, using the date/time picker to select the date and time (24-hour).**
2022-03-06 05:11 GMT

41 **In unallocated space on the NTFS partition on this device is a deleted photo of a mallard duck. What text is visible in the image?**
platyrhynchos

42 **What is the file TYPE for the file with Created Time = 2017-12-20 14:23:53 GMT?**
JPEG, JPG or JFIF

43 **Who is the owner of default_wallet.backup?**
Jessie Jenkins

44** **Place the following events in the order in which they occurred (report each letter in order separated by a comma, e.g. A,B,C,D,E):**
A. the creation of the file referenced in USB question 40
B. scheduled meeting referenced in question 18
C. failed logins referenced in question 21
D. the last execution of the program referenced in question 22
E. approximate time of victim's death as provided by the medical examiner
B,E,C,D,A

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, and a series of questions related to the extracted data. Additionally, participants enrolled in the 22-5562: 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 95 participants returned results for the 5561 Computer Hard Drive - Windows Analysis test. Of the 32 total questions, two questions did not reach a consensus response. These questions dealt with the following topics: providing the comment given for the computer shutdown on a specified date and time and providing the creation date and time for the $FILE_NAME attribute for PoorFairJaquar.html.

Of the participants enrolled in the 5562 Removable Media Storage Analysis test, 43 returned results. Four of the twelve questions did not achieve a consensus response. Topics for these four questions include: providing SHA256 hash of USB device, providing the quantity of active partitions on the device, providing SHA256 hash of a specific file and placing events in chronological order.

The Digital Forensics field is increasing in complexity with a variety of tools to choose from; this directly affects the ability to determine clear consensus responses. Therefore, for this test, participants are encouraged to follow their laboratory's policies and procedures when evaluating their responses to these proficiency test questions.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 1 - Examination Questions

Question 1: Provide the Stored Acquisition SHA-1 Hash for the provided image, 22.5561.E01.

Manufacturer's Expected Response: a7b250cb09fcd6e5e362fcbc268ec6df12dbd418

WebCode Test	Response
2GYK6H-5562	A7B250CB09FCD6E5E362FCBC268EC6DF12DBD418
37HZM7-5561	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
3ERMDL-5562	A7B250CB09FCD6E5E362FCBC268EC6DF12DBD418
3J2MUJ-5561	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
3W8X27-5561	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
4ELR7K-5562	1AC729C981DFAE5668F12DE30BEFC9937FDD12EF
6GRCUL-5562	A7B250CB09FCD6E5E362FCBC268EC6DF12DBD418
6XRJND-5562	A7B250CB09FCD6E5E362FCBC268EC6DF12DBD418
7CPVTB-5561	1ac729c981dfae5668f12de30befc9937fdd12ef See Additional Comments on Page 3
8PW7XC-5562	A7B250CB09FCD6E5E362FCBC268EC6DF12DBD418
8YYJXD-5562	The SHA-1 Hash for the provided image file is (a7b250cb09fcd6e5e362fcbc268ec6df12dbd418). Below the FTK images showing the images verifies results.
8ZU2ZE-5562	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
98A6KL-5561	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
9WRPDD-5562	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
9ZBF4H-5561	1AC729C981DFAE5668F12DE30BEFC9937FDD12EF
A7BERC-5562	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
ARP7Q6-5561	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
B6WATE-5561	A7B250CB09FCD6E5E362FCBC268EC6DF12DBD418
B9WHYA-5561	SHA-1 Base 16 - 1AC729C981DFAE5668F12DE30BEFC9937FDD12EF

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 1 - Examination Questions	
WebCode Test	**Response**
BN9WG8-5562	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
BVR2DE-5562	A7B250CB09FCD6E5E362FCBC268EC6DF12DBD418
BYPLFC-5562	1ac729c981dfae5668f12de30befc9937fdd12ef
CMTYN8-5561	A7B250CB09FCD6E5E362FCBC268EC6DF12DBD418
CN44V6-5561	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
DHRBK7-5562	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
E7WKY6-5561	A7B250CB09FCD6E5E362FCBC268EC6DF12DBD418
E7XH9Z-5561	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
EAWU6Z-5561	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
EREXP8-5561	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
EX67D8-5562	A7B250CB09FCD6E5E362FCBC268EC6DF12DBD418
EZEWXB-5561	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
F2G9Z3-5562	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
F8L898-5562	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
FGDPP2-5562	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
FL36D9-5562	02B408BDB0717C1DC17E287D213B449B4EE9CD1F9489E78DD6A2829728BCE730
FVTQJ7-5562	A7B250CB09FCD6E5E362FCBC268EC6DF12DBD418
FXXHAY-5561	9885cb57c4db34926b1bbe95015bdbebc3705563
G8GC37-5561	A7B250CB09FCD6E5E362FCBC268EC6DF12DBD418
GCTZYW-5561	1AC729C981DFAE5668F12DE30BEFC9937FDD12EF
GFWVHY-5561	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 1 - Examination Questions	
WebCode Test	**Response**
GLX6QD-5562	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
GR9ZT2-5561	1ac729c981dfae5668f12de30befc9937fdd12ef
HDM36C-5561	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
HDM9G8-5561	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
HEVFPY-5561	A7B250CB09FCD6E5E362FCBC268EC6DF12DBD418
HPTDCY-5561	Sha-1 Base16 is 1AC729C981DFAE5668F12DE30BEFC9937FDD12EF; base 32 is DLDSTSMB36XFM2HRFXRQX36JSN752EXP
HWZPPY-5562	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
HX9YL3-5562	1AC729C981DFAE5668F12DE30BEFC9937FDD12EF
JEDQ2D-5562	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
JQ84YN-5561	1AC729C981DFAE5668F12DE30BEFC9937FDD12EF
K4BTM4-5561	1AC729C981DFAE5668F12DE30BEFC9937FDD12EF
K9GN9W-5561	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
KA2332-5562	A7B250CB09FCD6E5E362FCBC268EC6DF12DBD418
KDZDY2-5561	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
LTKL96-5562	Hash (SHA1) A7B250CB09FCD6E5E362FCBC268EC6DF12DBD418
LYVGBT-5561	9885cb57c4db34926b1bbe95015bdbebc3705563
MW334U-5561	A7B250CB09FCD6E5E362FCBC268EC6DF12DBD418
PPRVBV-5561	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
PPUJUU-5561	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
PQ9R3V-5561	1ac729c981dfae5668f12de30befc9937fdd12ef
PRHXH6-5562	A7B250CB09FCD6E5E362FCBC268EC6DF12DBD418

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 1 - Examination Questions	
WebCode Test	**Response**
PTTY3H-5562	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
PV4KAY-5561	stored SHA-1: a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
PZAFUR-5562	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
Q8PGRF-5561	A7B250CB09FCD6E5E362FCBC268EC6DF12DBD418
QKG3YW-5562	A7B250CB09FCD6E5E362FCBC268EC6DF12DBD418
QLMMJQ-5561	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
QQ3XWU-5561	A7B250CB09FCD6E5E362FCBC268EC6DF12DBD418
QVYKR4-5562	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
R8KDG3-5562	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
RFWD9R-5562	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
RNVVQP-5561	Hash (SHA-1): A7B250CB09FCD6E5E362FCBC268EC6DF12DBD418
T4JR6P-5562	A7B250CB09FCD6E5E362FCBC268EC6DF12DBD418
TA98UW-5561	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
TE2AXW-5561	1ac729c981dfae5668f12de30befc9937fdd12ef
TWHDG3-5561	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
URL94P-5562	1AC729C981DFAE5668F12DE30BEFC9937FDD12EF
VKGWHC-5561	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
VRFDXN-5561	1ac729c981dfae5668f12de30befc9937fdd12ef
VU4RLY-5562	a7b250cb09fd6e5e362fcbc268ec6df12dbd418
WB6WLF-5561	9885cb57c4db34926b1bbe95015bdbebc3705563
WRDQDP-5562	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 1 - Examination Questions	
WebCode Test	**Response**
WXJKCR-5562	A7B250CB09FCD6E5E362FCBC268EC6DF12DBD418
X7U2JR-5561	A7B250CB09FCD6E5E362FCBC268EC6DF12DBD418
XB3L8N-5562	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
XGEEHM-5561	1ac729c981dfae5668f12de30befc9937fdd12ef
Y4WCCF-5561	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
YDMVRA-5562	[Participant did not return results for this question.]
YE4XXP-5561	a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
YL2H7J-5562	A7B250CB09FCD6E5E362FCBC268EC6DF12DBD418
YLG7ZJ-5562	1AC729C981DFAE5668F12DE30BEFC9937FDD12EF
ZD74EJ-5561	The SHA-1 Hash for the provided image file is (a7b250cb09fcd6e5e362fcbc268ec6df12dbd418). Below the FTK images showing the images verifies results.
ZDHVAK-5562	A7B250CB09FCD6E5E362FCBC268EC6DF12DBD418
ZG7AXV-5561	1ac729c981dfae5668f12de30befc9937fdd12ef
ZLZ4XH-5561	A7B250CB09FCD6E5E362FCBC268EC6DF12DBD418

Question 1: Provide the Stored Acquisition SHA-1 Hash for the provided image, 22.5561.E01.

Consensus Result:

a7b250cb09fcd6e5e362fcbc268ec6df12dbd418

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.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 1 - Examination Questions

Expected Response Illustration:

ewfinfo (LIbewf) parse of 22-5561.E01 metadata

```
$ewfinfo -m 22-5561.E01
ewfinfo 20170703

EWF information
        File format:            EnCase 7
        Sectors per chunk:      64
        Error granularity:      64
        Compression method:     deflate
        Compression level:      best compression
        Set identifier:         fecd37cd-f0bb-b748-9ce3-b9cca3ad02a3

Media information
        Media type:             fixed disk
        Is physical:            yes
        Bytes per sector:       512
        Number of sectors:      62914560
        Media size:             30 GiB (32212254720 bytes)

Digest hash information
        MD5:                    8d3d62bfc411a03e6718c170ab25d8ce
        SHA1:                   a7b250cb09fcd6e5e362fcbc268ec6df12dbd418
```

Other Responses:

Another 19% of participants reported the SHA1 hash (1ac729c981dfae5668f12de30befc9937fdd12ef) of the 22-5561.E01 file, not the stored verification hash of the evidence data it contains.

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 22-5561.E01)? Provide a NUMERIC response.

Manufacturer's Expected Response: 2

WebCode Test	Response
2GYK6H-5562	2
37HZM7-5561	2
3ERMDL-5562	2
3J2MUJ-5561	2
3W8X27-5561	2
4ELR7K-5562	2
6GRCUL-5562	2
6XRJND-5562	2
7CPVTB-5561	2
8PW7XC-5562	2
8YYJXD-5562	2
8ZU2ZE-5562	2
98A6KL-5561	2
9WRPDD-5562	2
9ZBF4H-5561	2
A7BERC-5562	2
ARP7Q6-5561	2
B6WATE-5561	2
B9WHYA-5561	2

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 2 - Examination Questions	
WebCode Test	**Response**
BN9WG8-5562	2
BVR2DE-5562	2
BYPLFC-5562	2
CMTYN8-5561	2
CN44V6-5561	2
DHRBK7-5562	[Participant did not return results for this question.]
E7WKY6-5561	2
E7XH9Z-5561	2
EAWU6Z-5561	2
EREXP8-5561	2
EX67D8-5562	2
EZEWXB-5561	2
F2G9Z3-5562	2
F8L898-5562	2
FGDPP2-5562	02
FL36D9-5562	2
FVTQJ7-5562	2
FXXHAY-5561	2
G8GC37-5561	2
GCTZYW-5561	2
GFWVHY-5561	2

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 2 - Examination Questions	
WebCode Test	**Response**
GLX6QD-5562	2
GR9ZT2-5561	2
HDM36C-5561	2
HDM9G8-5561	2
HEVFPY-5561	2
HPTDCY-5561	2
HWZPPY-5562	2
HX9YL3-5562	2
JEDQ2D-5562	2
JQ84YN-5561	2
K4BTM4-5561	2
K9GN9W-5561	2
KA2332-5562	2
KDZDY2-5561	2
LTKL96-5562	2
LYVGBT-5561	2
MW334U-5561	2
PPRVBV-5561	2
PPUJUU-5561	2
PQ9R3V-5561	2
PRHXH6-5562	2

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 2 - Examination Questions	
WebCode Test	**Response**
PTTY3H-5562	2
PV4KAY-5561	2
PZAFUR-5562	2
Q8PGRF-5561	2
QKG3YW-5562	2
QLMMJQ-5561	2
QQ3XWU-5561	2
QVYKR4-5562	2
R8KDG3-5562	2
RFWD9R-5562	2
RNVVQP-5561	2
T4JR6P-5562	2
TA98UW-5561	2
TE2AXW-5561	2
TWHDG3-5561	2
URL94P-5562	2
VKGWHC-5561	2
VRFDXN-5561	2
VU4RLY-5562	2
WB6WLF-5561	2
WRDQDP-5562	2

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 2 - Examination Questions	
WebCode Test	**Response**
WXJKCR-5562	2
X7U2JR-5561	2
XB3L8N-5562	2
XGEEHM-5561	2
Y4WCCF-5561	2
YDMVRA-5562	[Participant did not return results for this question.]
YE4XXP-5561	2
YL2H7J-5562	2
YLG7ZJ-5562	2
ZD74EJ-5561	2
ZDHVAK-5562	2
ZG7AXV-5561	2
ZLZ4XH-5561	2

Question 2: How many partitions are on the hard drive (device imaged as 22-5561.E01)? Provide a NUMERIC response.

Consensus Result:

2

Expected Response Explanation:

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

Expected Response Illustration:

EnCase Report of Drive Geometry

Partitions

Name	Id	Type	Start Sector	Total Sectors	Size
	07	NTFS	2,048	102,400	50 MB
	07	NTFS	104,448	62,808,064	29.9 GB

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 2 - Examination Questions

fdisk parse of image partition table

```
$fdisk -l /media/image/ewf1
Disk /media/image/ewf1: 30 GiB, 32212254720 bytes, 62914560 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x0e30d349

Device              Boot  Start      End  Sectors Size Id Type
/media/image/ewf1p1 *      2048   104447   102400  50M  7 HPFS/NTFS/exFAT
/media/image/ewf1p2      104448 62912511 62808064  30G  7 HPFS/NTFS/exFAT
```

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3 - Examination Questions

Question 3: What is the hostname for this computer?

Manufacturer's Expected Response: DESKTOP-RNO1O54

WebCode Test	Response
2GYK6H-5562	DESKTOP-RNO1O54
37HZM7-5561	DESKTOP-RNO1O54
3ERMDL-5562	DESKTOP-RNO1O54
3J2MUJ-5561	DESKTOP-RNO1O54
3W8X27-5561	DESKTOP-RN01054
4ELR7K-5562	DESKTOP-RNO1O54
6GRCUL-5562	DESKTOP-RNO1O54
6XRJND-5562	DESKTOP-RNO1O54
7CPVTB-5561	DESKTOP-RNO1O54
8PW7XC-5562	DESKTOP-RNO1O54
8YYJXD-5562	Jessie Jenkins
8ZU2ZE-5562	DESKTOP-RO1O54
98A6KL-5561	DESKTOP-RNO1O54
9WRPDD-5562	DESKTOP-RNO1O54
9ZBF4H-5561	Jessie Jenkins
A7BERC-5562	DESKTOP-RNO1O54
ARP7Q6-5561	DESKTOP-RNO1054
B6WATE-5561	DESKTOP-RNO1O54
B9WHYA-5561	DESKTOP-RNO1O54

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3 - Examination Questions	
WebCode Test	**Response**
BN9WG8-5562	DESKTOP-RNO1O54
BVR2DE-5562	DESKTOP-RNO1O54
BYPLFC-5562	DESKTOP-RNO1O54
CMTYN8-5561	DESKTOP-RNO1O54
CN44V6-5561	DESKTOP-RNO1O54
DHRBK7-5562	DESKTOP-RNO1O54
E7WKY6-5561	DESKTOP-RNO1O54
E7XH9Z-5561	DESKTOP-RNO1O54
EAWU6Z-5561	DESKTOP-RNO1O54
EREXP8-5561	DESKTOP-RN01054
EX67D8-5562	DESKTOP-RNO1O54
EZEWXB-5561	DESKTOP-RNO1O54
F2G9Z3-5562	DESKTOP-RNO1O54
F8L898-5562	DESKTOP-RNO1O54
FGDPP2-5562	DESKTOP-RNO1O54
FL36D9-5562	DESKTOP-PNO154
FVTQJ7-5562	DESKTOP-RNO1O54
FXXHAY-5561	DESKTOP-RN01054
G8GC37-5561	DESKTOP-RNO1O54
GCTZYW-5561	DESKTOP-RNO1O54
GFWVHY-5561	DESKTOP-RN01054

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3 - Examination Questions	
WebCode Test	**Response**
GLX6QD-5562	DESKTOP-RNO1O54
GR9ZT2-5561	DESKTOP-RNO1O54
HDM36C-5561	DESKTOP-RNO1054
HDM9G8-5561	DESKTOP-RNO1O54
HEVFPY-5561	DESKTOP-RNO1O54
HPTDCY-5561	DESKTOP-RNO1O54
HWZPPY-5562	DESKTOP-RNO1O54
HX9YL3-5562	DESKTOP-RNO1O54
JEDQ2D-5562	DESKTOP-RNO1O54
JQ84YN-5561	DESKTOP-RNO1O54
K4BTM4-5561	DESKTOP-RNO1O54
K9GN9W-5561	DESKTOP-RNO1O54
KA2332-5562	DESKTOP-RNO1O54
KDZDY2-5561	JenkinsHome
LTKL96-5562	DESKTOP-RNO1O54
LYVGBT-5561	Desktop-RNO1054
MW334U-5561	DESKTOP-RNO1O54
PPRVBV-5561	DESKTOP-RNO1O54
PPUJUU-5561	DESKTOP-RNO1O54
PQ9R3V-5561	DESKTOP-RNO1O54
PRHXH6-5562	DESKTOP-RNO1O54

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3 - Examination Questions	
WebCode Test	**Response**
PTTY3H-5562	DESKTOP-RNO1O54
PV4KAY-5561	DESKTOP-RNO1O54
PZAFUR-5562	DESKTOP-RNO1O54
Q8PGRF-5561	DESKTOP-RNO 1054
QKG3YW-5562	DESKTOP-RNO1O54
QLMMJQ-5561	DESKTOP-RNO1O54
QQ3XWU-5561	DESKTOP-RNO1O54
QVYKR4-5562	DESKTOP-RN01054
R8KDG3-5562	DESKTOP-RNO1O54
RFWD9R-5562	DESKTOP-RNO1O54
RNVVQP-5561	DESKTOP-RNO1O54
T4JR6P-5562	DESKTOP-RNO1O54
TA98UW-5561	DESKTOP-RNO1O54
TE2AXW-5561	DESKTOP-RNO1O54
TWHDG3-5561	DESKTOP-RNO1O54
URL94P-5562	DESKTOP-RNO1O54
VKGWHC-5561	DESKTOP-RNO1O54
VRFDXN-5561	VictimComputer
VU4RLY-5562	DESKTOP-RN01054
WB6WLF-5561	DESKTOP-RNO1054
WRDQDP-5562	DESKTOP-RNO1O54

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3 - Examination Questions	
WebCode Test	**Response**
WXJKCR-5562	DESKTOP-RNO1O54
X7U2JR-5561	DESKTOP-RNO1O54
XB3L8N-5562	DESKTOP-RNO1O54
XGEEHM-5561	DESKTOP-RNO1O54
Y4WCCF-5561	DESKTOP-RNO1O54
YDMVRA-5562	[Participant did not return results for this question.]
YE4XXP-5561	DESKTOP-RNO1O54
YL2H7J-5562	DESKTOP-RNO1O54
YLG7ZJ-5562	DESKTOP-RN01054
ZD74EJ-5561	Jessie Jenkins
ZDHVAK-5562	DESKTOP-RNO1O54
ZG7AXV-5561	DESKTOP-RNO1O54
ZLZ4XH-5561	DESKTOP-RNO1O54

Question 3: What is the hostname for this computer?

Consensus Result:

DESKTOP-RNO1O54

Expected Response Explanation:

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

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3 - Examination Questions

Expected Response Illustration:

Registry Explorer view of computer name registry key

Values

	Value Name	Value Type	Data
	ABC	ABC	ABC
	(default)	RegSz	mnmsrvc
▶	ComputerNa...	RegSz	DESKTOP-RNO1O54

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
2GYK6H-5562	Windows 10 Home
37HZM7-5561	Windows 10 Home. Build Number=19044. Version=2009.
3ERMDL-5562	Windows 10 Home Edition Version 6.3
3J2MUJ-5561	Windows 10 Home (2009), Version 6.3
3W8X27-5561	Windows 10 Home Version 6.3
4ELR7K-5562	Windows 10 Home (2009) 6.3 Core
6GRCUL-5562	Windows 10 Home 21H2
6XRJND-5562	Windows 10 Home
7CPVTB-5561	Windows 10 Home version 6.3 (19041.vb_release.191206-1406)
8PW7XC-5562	Windows 10 Home version 21H2
8YYJXD-5562	Windows 10 Home (2009), version number (603) core
8ZU2ZE-5562	Windows 10 Home (2009) v 6.3
98A6KL-5561	Windows 10 Home 6.3 (19044)
9WRPDD-5562	Windows 10 Home (2009), número de versión 6.3
9ZBF4H-5561	Windows 10 Home (2009) Version Number: 6.3 Operating system version: Core Build Number: 19044
A7BERC-5562	Windows 10 Home (2009) version 6.3 build number 19044
ARP7Q6-5561	Windows 10 Home (version: 6.3 edition: Core)
B6WATE-5561	Windows 10 Home Edition Version 6.3
B9WHYA-5561	Windows 10 Home, Version 6.3

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4 - Examination Questions	
WebCode Test	**Response**
BN9WG8-5562	Windows 10 Home, Version :- 6.3, Build Number :- 19044
BVR2DE-5562	Windows 10 Home, Version 6.3
BYPLFC-5562	Microsoft Windows 10 Home (2009) version 6.3
CMTYN8-5561	Windows 10 Home, version 6.3, build 19044
CN44V6-5561	6.3 Windows 10 Home
DHRBK7-5562	Windows 10 Home (2019) v6.3
E7WKY6-5561	Windows 10 Home
E7XH9Z-5561	Windows 10 Home 6.3 Core
EAWU6Z-5561	Windows 10 Home (2009) version 6.3 and Core edition
EREXP8-5561	Windows 10 Home
EX67D8-5562	Windows 10 Home (2009) 6.3
EZEWXB-5561	Windows 10 Home (2009) Version: 6.3
F2G9Z3-5562	Windows 10 Home (2009) Version 6.3 19044
F8L898-5562	Windows 10 Home (2009) / Version 6.3 / Build 19044
FGDPP2-5562	Windows 10 Home
FL36D9-5562	Windows 10 Home (2009) Version 6.3
FVTQJ7-5562	Windows 10 Home, Version: 6.3, Edition: Core, Build: 19044
FXXHAY-5561	Windows 10 Home 2009
G8GC37-5561	Windows 10 Home 19044
GCTZYW-5561	Windows 10 Home (2009) v.6.3
GFWVHY-5561	Windows 10 Home (2009) Version 6.3 Build Number 19044

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4 - Examination Questions	
WebCode Test	**Response**
GLX6QD-5562	Windows 10 Home Edition
GR9ZT2-5561	Windows 10 Home
HDM36C-5561	Windows 10 Home Edition
HDM9G8-5561	Windows 10 Home (2009) version 6.3
HEVFPY-5561	Windows 10 Home version 6.3 (2009)
HPTDCY-5561	Windows 10 Home version-6.3 build-19044
HWZPPY-5562	Windows 10 Home Version 6.3 Core 21H2
HX9YL3-5562	Windows 10 Home (2009) Version Number 6.3
JEDQ2D-5562	Windows 10 Home
JQ84YN-5561	Windows 10 Home (2009) Version 6.3
K4BTM4-5561	Windows 10 Home (2009)
K9GN9W-5561	Windows 10 Home 2009 version 6.3
KA2332-5562	Windows 10 Home
KDZDY2-5561	Windows 10 Home
LTKL96-5562	Windows 10 Home (2009), version 6.3
LYVGBT-5561	Windows 10 Home (2009)
MW334U-5561	Windows 10 Home 2009 6.3
PPRVBV-5561	Windows 10 Home (2009) Version 6.3
PPUJUU-5561	Windows 10 Home (2009) 6.3
PQ9R3V-5561	Windows 10 Home (2009) v 6.3
PRHXH6-5562	Windows 10 Home

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4 - Examination Questions	
WebCode Test	**Response**
PTTY3H-5562	Windows 10 Home
PV4KAY-5561	Windows 10 Home (2009), version 6.3
PZAFUR-5562	Windows 10 Home (2009), version 6.3
Q8PGRF-5561	Windows 10 Home edition, version 21H2
QKG3YW-5562	Windows 10 Home (2009) Version 6.3 and Build 19044
QLMMJQ-5561	Windows 10 Home Version: 6.3
QQ3XWU-5561	Windows 10 Home
QVYKR4-5562	Windows 10 Home
R8KDG3-5562	Windows 10 Home v21H1
RFWD9R-5562	Windows 10 Home, version 6.3
RNVVQP-5561	Windows 10 Home (version 20H2)
T4JR6P-5562	Windows 10 Home (2009) Versión 6.3
TA98UW-5561	Windows 10 Home
TE2AXW-5561	Windows 10 Home
TWHDG3-5561	Windows 10 Home
URL94P-5562	Windows 10 Home version 6.3 Build number 19044
VKGWHC-5561	Windows 10 Home Edition (Version 6.3)
VRFDXN-5561	Windows 10 Home 6.3
VU4RLY-5562	Windows 10 Home(2009) Version 6.3
WB6WLF-5561	Windows 10 Home (2009) ver. 6.3
WRDQDP-5562	Microsoft Windows 10 Home

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4 - Examination Questions	
WebCode Test	**Response**
WXJKCR-5562	Windows 10 Home (2009) Core, version 6.3
X7U2JR-5561	Windows 10 Home version 6.3
XB3L8N-5562	Windows 10 Home
XGEEHM-5561	Windows 10 Home (2009) v6.3
Y4WCCF-5561	Windows 10 Home 21H2
YDMVRA-5562	[Participant did not return results for this question.]
YE4XXP-5561	Windows 10 Home (2009), version 6.3
YL2H7J-5562	Windows 10 (Edition Home) (Version 19044)
YLG7ZJ-5562	Windows 10 Home (2009) 6.3
ZD74EJ-5561	Windows 10 Home (2009), version number (603) core
ZDHVAK-5562	Windows 10 Home, version 6.3, build 19044
ZG7AXV-5561	Windows 10 Home v6.3 Core Edition
ZLZ4XH-5561	Windows 10 Home

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

Consensus Result:

Windows 10 Home

Expected Response Explanation:

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

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4 - Examination Questions

Expected Response Illustration:

Registry Explorer view showing Windows version and edition in the Software registry hive

Values

Value Name	Value Type	Data
InstallationType	RegSz	Client
InstallDate	RegDword	1643779866
ProductName	RegSz	Windows 10 Home
ReleaseId	RegSz	2009
SoftwareType	RegSz	System
UBR	RegDword	1526

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: Jessie Jenkins

WebCode Test	Response
2GYK6H-5562	Jessie Jenkins
37HZM7-5561	Jessie Jenkins
3ERMDL-5562	Jessie Jenkins
3J2MUJ-5561	Jessie Jenkins
3W8X27-5561	Jessie Jenkins
4ELR7K-5562	Jessie Jenkins
6GRCUL-5562	Jessie Jenkins
6XRJND-5562	Jessie Jenkins
7CPVTB-5561	Jessie Jenkins
8PW7XC-5562	Jessie Jenkins
8YYJXD-5562	Jessie Jenkins
8ZU2ZE-5562	Jessie Jenkins
98A6KL-5561	Jessie Jenkins
9WRPDD-5562	Jessie Jenkins
9ZBF4H-5561	Jessie Jenkins
A7BERC-5562	Jessie Jenkins
ARP7Q6-5561	Jessie Jenkins
B6WATE-5561	Jessie Jenkins
B9WHYA-5561	Jessie Jenkins

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 5 - Examination Questions	
WebCode Test	**Response**
BN9WG8-5562	Jessie Jenkins
BVR2DE-5562	Jessie Jenkins
BYPLFC-5562	Jessie Jenkins
CMTYN8-5561	Jessie Jenkins
CN44V6-5561	Jessie Jenkins
DHRBK7-5562	Jessie Jenkins
E7WKY6-5561	Jessie Jenkins
E7XH9Z-5561	Jessie Jenkins
EAWU6Z-5561	Jessie Jenkins
EREXP8-5561	Jessie Jenkins
EX67D8-5562	Jessie Jenkins
EZEWXB-5561	Jessie Jenkins
F2G9Z3-5562	Jessie Jenkins
F8L898-5562	Jessie Jenkins
FGDPP2-5562	Jessie Jenkins
FL36D9-5562	Jessi Jenkins
FVTQJ7-5562	Jessie Jenkins
FXXHAY-5561	Jessie Jenkins
G8GC37-5561	Jessie Jenkins
GCTZYW-5561	Jessie Jenkins
GFWVHY-5561	Jesse Jenkins

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 5 - Examination Questions	
WebCode Test	**Response**
GLX6QD-5562	Jessie Jenkins
GR9ZT2-5561	Jessie Jenkins
HDM36C-5561	Jessie Jenkins
HDM9G8-5561	Jessie Jenkins
HEVFPY-5561	Jessie Jenkins
HPTDCY-5561	Jessie Jenkins
HWZPPY-5562	Jessie Jenkins
HX9YL3-5562	Jessie Jenkins
JEDQ2D-5562	Jessie Jenkins
JQ84YN-5561	Jessie Jenkins
K4BTM4-5561	Jessie Jenkins
K9GN9W-5561	Jessie Jenkins
KA2332-5562	Jessie Jenkins
KDZDY2-5561	Jessie Jenkins
LTKL96-5562	Jessie Jenkins
LYVGBT-5561	Jessie Jenkins
MW334U-5561	Jessie Jenkins
PPRVBV-5561	Jessie Jenkins
PPUJUU-5561	Jessie Jenkins
PQ9R3V-5561	Jessie Jenkins
PRHXH6-5562	Jessie Jenkins

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 5 - Examination Questions	
WebCode Test	**Response**
PTTY3H-5562	Jessie Jenkins
PV4KAY-5561	Jessie Jenkins
PZAFUR-5562	Jessie Jenkins
Q8PGRF-5561	Jessie Jenkins
QKG3YW-5562	Jessie Jenkins
QLMMJQ-5561	Jessie Jenkins
QQ3XWU-5561	Jessie Jenkins
QVYKR4-5562	Jessie JENKINS
R8KDG3-5562	Jessie Jenkins
RFWD9R-5562	Jessie Jenkins
RNVVQP-5561	Jessie Jenkins
T4JR6P-5562	Jessie Jenkins
TA98UW-5561	Jessie Jenkins
TE2AXW-5561	Jessie Jenkins
TWHDG3-5561	Jessie Jenkins
URL94P-5562	Jessie Jenkins
VKGWHC-5561	Jessie Jenkins
VRFDXN-5561	Jessie Jenkins
VU4RLY-5562	Jessie Jenkins
WB6WLF-5561	Jessie Jenkins
WRDQDP-5562	Jessie Jenkins

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 5 - Examination Questions	
WebCode Test	**Response**
WXJKCR-5562	Jessie Jenkins
X7U2JR-5561	Jessie Jenkins
XB3L8N-5562	Jessie Jenkins
XGEEHM-5561	Jessie Jenkins
Y4WCCF-5561	Jessie Jenkins
YDMVRA-5562	[Participant did not return results for this question.]
YE4XXP-5561	Jessie Jenkins
YL2H7J-5562	Jessie Jenkins
YLG7ZJ-5562	Jessie Jenkins
ZD74EJ-5561	Jessie Jenkins
ZDHVAK-5562	Jessie Jenkins
ZG7AXV-5561	Jessie Jenkins
ZLZ4XH-5561	Jessie Jenkins

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

Consensus Result:

Jessie Jenkins

Expected Response Explanation:

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

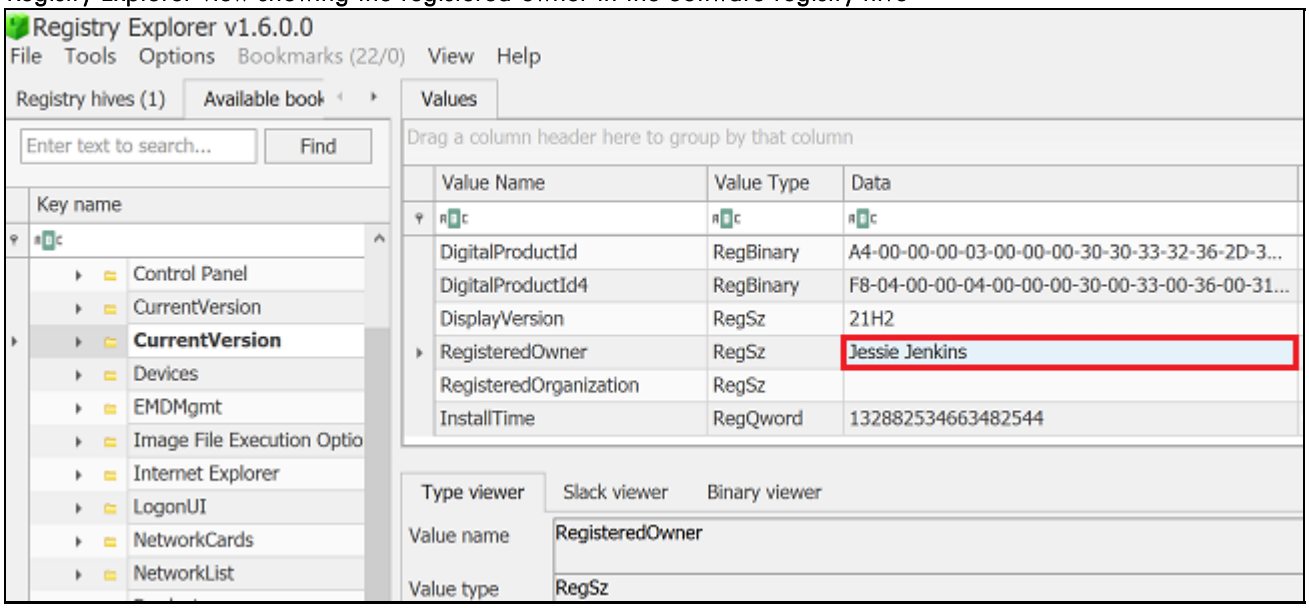
Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 5 - Examination Questions

Expected Response Illustration:

Registry Explorer view showing the registered owner in the Software registry hive



Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6 - Examination Questions

Question 6: When was the operating system installed? Provide your response in UTC+0, using the date/time picker to select the date and time (24-hour).

Manufacturer's Expected Response: 2022-02-02 05:31

WebCode Test	Response
2GYK6H-5562	2022-02-02 05:31
37HZM7-5561	2022-02-02 05:31
3ERMDL-5562	2022-02-02 05:31
3J2MUJ-5561	2022-02-02 05:31
3W8X27-5561	2022-02-02 05:31
4ELR7K-5562	2022-02-02 05:31
6GRCUL-5562	2022-02-02 05:31
6XRJND-5562	2022-02-02 05:31
7CPVTB-5561	2022-02-02 05:31
8PW7XC-5562	2022-02-02 05:31
8YYJXD-5562	2022-02-02 05:31
8ZU2ZE-5562	2022-02-02 05:31
98A6KL-5561	2022-02-02 05:31
9WRPDD-5562	2022-02-02 05:31
9ZBF4H-5561	2022-02-02 05:31
A7BERC-5562	2022-02-02 05:31
ARP7Q6-5561	2022-02-02 05:31
B6WATE-5561	2022-02-02 05:31
B9WHYA-5561	2022-02-02 05:31

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6 - Examination Questions	
WebCode Test	**Response**
BN9WG8-5562	2022-02-02 05:31
BVR2DE-5562	2022-02-02 05:31
BYPLFC-5562	2022-02-02 05:31
CMTYN8-5561	2022-02-02 05:31
CN44V6-5561	2022-02-02 05:31
DHRBK7-5562	2022-02-02 05:31
E7WKY6-5561	2022-02-02 05:31
E7XH9Z-5561	2022-02-02 05:31
EAWU6Z-5561	2022-02-22 05:31
EREXP8-5561	2022-02-02 05:31
EX67D8-5562	2022-02-02 05:31
EZEWXB-5561	2022-02-02 05:31
F2G9Z3-5562	2022-02-02 05:31
F8L898-5562	2022-02-02 05:31
FGDPP2-5562	2022-02-02 05:31
FL36D9-5562	2022-02-02 05:31
FVTQJ7-5562	2022-02-02 05:31
FXXHAY-5561	2022-02-02 05:31
G8GC37-5561	2022-02-02 05:31
GCTZYW-5561	2022-02-02 05:31
GFWVHY-5561	2022-02-02 05:31

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6 - Examination Questions	
WebCode Test	**Response**
GLX6QD-5562	2022-02-02 05:31
GR9ZT2-5561	2022-02-02 05:31
HDM36C-5561	2022-02-02 05:31
HDM9G8-5561	2022-02-02 05:31
HEVFPY-5561	2022-02-02 05:31
HPTDCY-5561	2022-02-02 05:31
HWZPPY-5562	2022-02-02 05:31
HX9YL3-5562	2022-02-02 05:31
JEDQ2D-5562	2022-02-02 05:31
JQ84YN-5561	2022-02-02 05:31
K4BTM4-5561	2022-02-02 05:31
K9GN9W-5561	2022-02-02 05:31
KA2332-5562	2022-02-02 05:31
KDZDY2-5561	2022-02-02 05:31
LTKL96-5562	2022-02-02 05:31
LYVGBT-5561	2022-02-02 05:31
MW334U-5561	2022-02-02 05:31
PPRVBV-5561	2022-02-02 05:31
PPUJUU-5561	2022-02-02 05:31
PQ9R3V-5561	2022-02-02 05:31
PRHXH6-5562	2022-02-02 05:31

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6 - Examination Questions	
WebCode Test	**Response**
PTTY3H-5562	2022-02-02 05:31
PV4KAY-5561	2022-02-02 05:31
PZAFUR-5562	2022-02-02 05:31
Q8PGRF-5561	2022-02-02 05:31
QKG3YW-5562	2022-02-02 05:31
QLMMJQ-5561	2022-02-02 05:31
QQ3XWU-5561	2022-02-02 05:31
QVYKR4-5562	2022-02-02 05:31
R8KDG3-5562	2022-02-02 05:31
RFWD9R-5562	2022-02-02 05:31
RNVVQP-5561	2022-02-02 05:31
T4JR6P-5562	2022-02-02 05:31
TA98UW-5561	2022-02-02 05:31
TE2AXW-5561	2022-02-02 05:31
TWHDG3-5561	2022-02-02 05:31
URL94P-5562	2022-02-02 05:31
VKGWHC-5561	2022-02-02 05:31
VRFDXN-5561	2022-02-02 05:31
VU4RLY-5562	2022-02-02 05:31
WB6WLF-5561	2022-02-02 05:31
WRDQDP-5562	2022-02-02 05:31

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6 - Examination Questions	
WebCode Test	**Response**
WXJKCR-5562	2022-02-02 05:31
X7U2JR-5561	2022-02-02 05:31
XB3L8N-5562	2022-02-02 05:31
XGEEHM-5561	2022-02-02 05:31
Y4WCCF-5561	2022-02-02 05:31
YDMVRA-5562	[Participant did not return results for this question.]
YE4XXP-5561	2022-02-02 05:31
YL2H7J-5562	2022-02-02 05:31
YLG7ZJ-5562	2022-02-02 05:31
ZD74EJ-5561	2022-02-02 05:31
ZDHVAK-5562	2022-02-02 05:31
ZG7AXV-5561	2019-07-12 09:03
ZLZ4XH-5561	2022-02-02 05:31

Question 6: When was the operating system installed? Provide your response in UTC+0, using the date/time picker to select the date and time (24-hour).

Consensus Result:

2022-02-02 05:31

Expected Response Explanation:

This information is found in the Windows Software registry at C:\Windows\System32\Config\Software: Microsoft\Windows NT\CurrentVersion: InstallDate (or InstallTime)

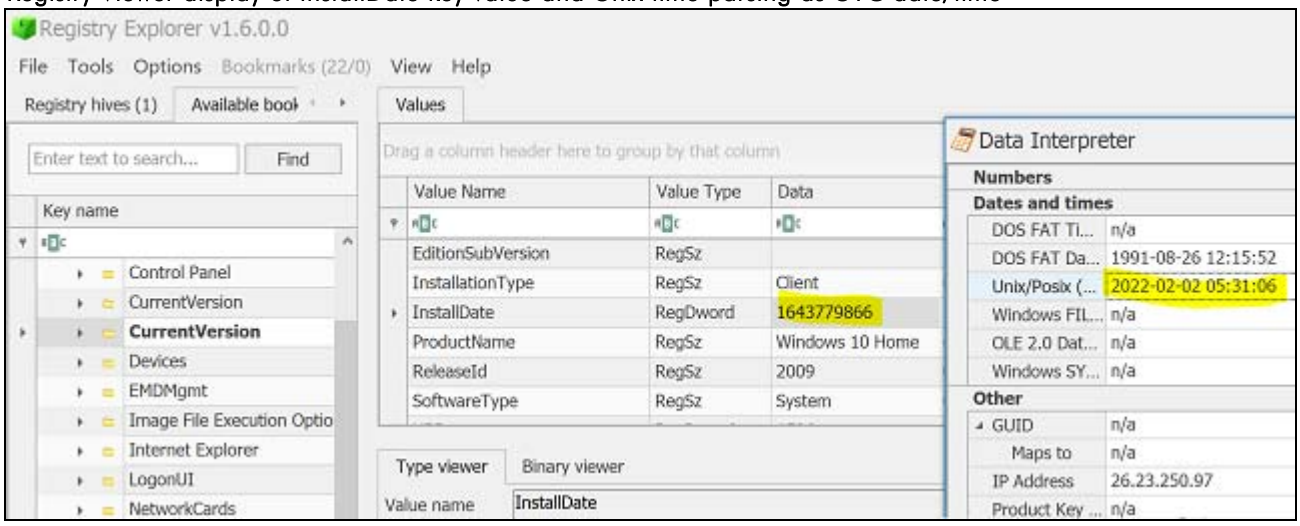
Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6 - Examination Questions

Expected Response Illustration:

Registry Viewer display of InstallDate key value and Unix time parsing as UTC date/time



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 picker to select the date and time (24-hour).

Manufacturer's Expected Response: 2022-03-06 05:12

WebCode Test	Response
2GYK6H-5562	2022-03-06 05:12
37HZM7-5561	2022-03-06 05:12
3ERMDL-5562	2022-03-06 05:12
3J2MUJ-5561	2022-03-06 05:12
3W8X27-5561	2022-03-06 05:12
4ELR7K-5562	2022-03-06 05:12
6GRCUL-5562	2022-03-06 05:12
6XRJND-5562	2022-03-06 05:12
7CPVTB-5561	2022-03-06 05:12
8PW7XC-5562	2022-03-06 05:12
8YYJXD-5562	2022-03-06 05:12
8ZU2ZE-5562	2022-03-06 05:12
98A6KL-5561	2022-03-06 05:12
9WRPDD-5562	2022-03-06 05:12
9ZBF4H-5561	2022-03-06 05:12
A7BERC-5562	2022-03-06 05:12
ARP7Q6-5561	2022-03-06 05:12
B6WATE-5561	2022-03-06 05:12
B9WHYA-5561	2022-03-06 05:12

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7 - Examination Questions	
WebCode Test	**Response**
BN9WG8-5562	2022-03-06 05:12
BVR2DE-5562	2022-03-06 05:12
BYPLFC-5562	2022-03-06 05:12
CMTYN8-5561	2022-03-06 05:12
CN44V6-5561	2022-03-06 05:12
DHRBK7-5562	2022-03-06 05:12
E7WKY6-5561	2022-03-06 05:12
E7XH9Z-5561	2022-03-06 05:12
EAWU6Z-5561	2022-03-06 05:12
EREXP8-5561	2022-03-06 05:12
EX67D8-5562	2022-03-06 05:12
EZEWXB-5561	2022-03-06 05:12
F2G9Z3-5562	2022-03-06 05:12
F8L898-5562	2022-03-06 05:12
FGDPP2-5562	2022-03-06 05:12
FL36D9-5562	2022-03-06 05:12
FVTQJ7-5562	2022-03-06 05:12
FXXHAY-5561	2022-03-06 05:29
G8GC37-5561	2022-03-06 05:12
GCTZYW-5561	2022-03-06 05:12
GFWVHY-5561	2022-03-06 05:12

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7 - Examination Questions	
WebCode Test	**Response**
GLX6QD-5562	2022-03-06 05:12
GR9ZT2-5561	2022-03-06 05:12
HDM36C-5561	2022-03-05 05:12
HDM9G8-5561	2022-03-06 05:12
HEVFPY-5561	2022-03-06 05:12
HPTDCY-5561	2022-03-06 05:12
HWZPPY-5562	2022-03-06 05:12
HX9YL3-5562	2022-03-06 05:12
JEDQ2D-5562	2022-03-06 05:12
JQ84YN-5561	2022-03-06 05:12
K4BTM4-5561	2022-03-06 05:12
K9GN9W-5561	2022-03-06 05:12
KA2332-5562	2022-03-06 05:12
KDZDY2-5561	2022-03-06 05:12
LTKL96-5562	2022-03-06 05:12
LYVGBT-5561	2022-03-06 05:12
MW334U-5561	2022-03-06 05:12
PPRVBV-5561	2022-03-06 05:12
PPUJUU-5561	2022-03-06 05:12
PQ9R3V-5561	2022-03-06 05:12
PRHXH6-5562	2022-03-06 05:12

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7 - Examination Questions	
WebCode Test	**Response**
PTTY3H-5562	2022-03-06 05:12
PV4KAY-5561	2022-03-06 05:12
PZAFUR-5562	2022-03-06 05:12
Q8PGRF-5561	2022-03-06 05:12
QKG3YW-5562	2022-03-06 05:12
QLMMJQ-5561	2022-03-06 05:12
QQ3XWU-5561	2022-03-06 05:12
QVYKR4-5562	2022-03-06 05:12
R8KDG3-5562	2022-03-06 05:12
RFWD9R-5562	2022-03-06 05:12
RNVVQP-5561	2022-03-06 05:12
T4JR6P-5562	2022-03-06 05:12
TA98UW-5561	2022-03-06 05:12
TE2AXW-5561	2022-03-06 05:12
TWHDG3-5561	2022-03-06 05:12
URL94P-5562	2022-03-06 05:12
VKGWHC-5561	2022-03-06 05:12
VRFDXN-5561	2022-03-06 05:12
VU4RLY-5562	2022-03-06 05:12
WB6WLF-5561	2022-03-06 05:12
WRDQDP-5562	2022-03-06 05:12

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7 - Examination Questions	
WebCode Test	**Response**
WXJKCR-5562	2022-03-06 05:12
X7U2JR-5561	2022-03-06 05:12
XB3L8N-5562	2022-03-06 05:12
XGEEHM-5561	2022-03-06 05:12
Y4WCCF-5561	2022-03-06 05:12
YDMVRA-5562	[Participant did not return results for this question.]
YE4XXP-5561	2022-03-06 05:12
YL2H7J-5562	2022-03-06 05:12
YLG7ZJ-5562	2022-03-06 05:12
ZD74EJ-5561	2022-03-06 05:12
ZDHVAK-5562	2022-03-06 05:12
ZG7AXV-5561	2022-03-06 05:12
ZLZ4XH-5561	2022-03-06 05:12

Question 7: When was the computer LAST shutdown gracefully? Provide your response in UTC+0, using the date/time picker to select the date and time (24-hour).

Consensus Result:

2022-03-06 05:12

Expected Response Explanation:

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

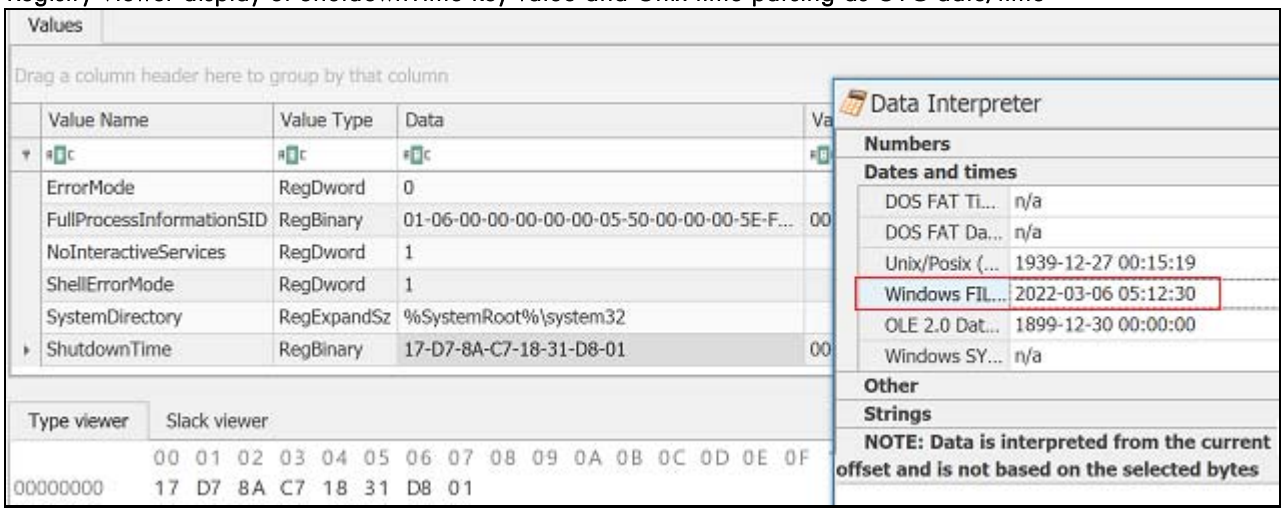
Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7 - Examination Questions

Expected Response Illustration:

Registry Viewer display of ShutdownTime key value and Unix time parsing as UTC date/time



Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 8 - Examination Questions

Question 8: Provide the username of the LAST user account created on the system.

Manufacturer's Expected Response: chris

WebCode Test	Response
2GYK6H-5562	chris
37HZM7-5561	chris
3ERMDL-5562	Jessie Jenkins
3J2MUJ-5561	chris
3W8X27-5561	Chris
4ELR7K-5562	Sam
6GRCUL-5562	chris
6XRJND-5562	Sam
7CPVTB-5561	Jessie Jenkins 2/17/2022 1:14:03 UTC (SAM)
8PW7XC-5562	chris
8YYJXD-5562	The answer is “Sam”. I have processed the image file using Axiom forensics tool and with user accounts artifact I am able to find the last user account created on the system.
8ZU2ZE-5562	Sam
98A6KL-5561	chris
9WRPDD-5562	Chris
9ZBF4H-5561	chris
A7BERC-5562	Sam
ARP7Q6-5561	chris
B6WATE-5561	Jessie Jenkins
B9WHYA-5561	chris

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 8 - Examination Questions	
WebCode Test	**Response**
BN9WG8-5562	Chris
BVR2DE-5562	Jessie Jenkins
BYPLFC-5562	chris
CMTYN8-5561	chris
CN44V6-5561	chris
DHRBK7-5562	chris
E7WKY6-5561	chris
E7XH9Z-5561	chris
EAWU6Z-5561	chris
EREXP8-5561	Chris
EX67D8-5562	chris
EZEWXB-5561	Chris
F2G9Z3-5562	chris
F8L898-5562	Chris
FGDPP2-5562	chris
FL36D9-5562	chris
FVTQJ7-5562	chris
FXXHAY-5561	Chris
G8GC37-5561	chris
GCTZYW-5561	chris
GFWVHY-5561	Chris

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 8 - Examination Questions	
WebCode Test	**Response**
GLX6QD-5562	chris
GR9ZT2-5561	Jessie Jenkins
HDM36C-5561	chris
HDM9G8-5561	chris
HEVFPY-5561	chris
HPTDCY-5561	chris
HWZPPY-5562	chris
HX9YL3-5562	chris
JEDQ2D-5562	chris
JQ84YN-5561	chris
K4BTM4-5561	Sam
K9GN9W-5561	chris
KA2332-5562	chris
KDZDY2-5561	Sam
LTKL96-5562	chris
LYVGBT-5561	Chris
MW334U-5561	Chris
PPRVBV-5561	chris
PPUJUU-5561	chris
PQ9R3V-5561	chris
PRHXH6-5562	Sam

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 8 - Examination Questions	
WebCode Test	**Response**
PTTY3H-5562	chris
PV4KAY-5561	Sam
PZAFUR-5562	Chris
Q8PGRF-5561	Sam
QKG3YW-5562	Sam
QLMMJQ-5561	chris
QQ3XWU-5561	chris
QVYKR4-5562	Sam
R8KDG3-5562	chris
RFWD9R-5562	chris
RNVVQP-5561	chris
T4JR6P-5562	Chris
TA98UW-5561	chris
TE2AXW-5561	chris
TWHDG3-5561	Jessie Jenkins
URL94P-5562	Chris
VKGWHC-5561	chris
VRFDXN-5561	Jessie Jenkins
VU4RLY-5562	chris
WB6WLF-5561	Chris
WRDQDP-5562	chris

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 8 - Examination Questions	
WebCode Test	**Response**
WXJKCR-5562	chris
X7U2JR-5561	Jessie Jenkins
XB3L8N-5562	chris
XGEEHM-5561	chris
Y4WCCF-5561	chris
YDMVRA-5562	[Participant did not return results for this question.]
YE4XXP-5561	chris
YL2H7J-5562	Chris
YLG7ZJ-5562	Jessie Jenkins
ZD74EJ-5561	The answer is “Sam”. I have processed the image file using Axiom forensics tool and with user accounts artifact I am able to find the last user account created on the system.
ZDHVAK-5562	chris
ZG7AXV-5561	Sam
ZLZ4XH-5561	Chris

Question 8: Provide the username of the LAST user account created on the system.

Consensus Result:

chris

Expected Response Explanation:

There are five user-created accounts on this system. 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. Accounts are assigned with a sequential numerical security ID (SID) when created.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 8 - Examination Questions

Expected Response Illustration:

EnCase Processor View of User Accounts

S-1-5-21-3501254099-4204809888-2000606956-1000	defaultuser0	S-1-5-21-3501254099-4204809888-2000606956-1000
Jessie Jenkins	Jessie Jenkins	S-1-5-21-3501254099-4204809888-2000606956-1002
mom	mom	S-1-5-21-3501254099-4204809888-2000606956-1003
dad	dad	S-1-5-21-3501254099-4204809888-2000606956-1004
Sam	Sam	S-1-5-21-3501254099-4204809888-2000606956-1005
chris	chris	S-1-5-21-3501254099-4204809888-2000606956-1006
Administrator	Administrator	S-1-5-21-3501254099-4204809888-2000606956-500
DefaultAccount	DefaultAccount	S-1-5-21-3501254099-4204809888-2000606956-503

Other Responses:

Another 17.9% of participants reported "Sam" as the username of the last user account created on the system. Based on the SID value, this was the second to last account created. This may be due to participants using the creation time of the user's profile folder. This represents the order the accounts were first logged in to and not the best indicator of the creation order of accounts.

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-1-5-21-3501254099-4204809888-2000606956-1002

WebCode Test	Response
2GYK6H-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
37HZM7-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
3ERMDL-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
3J2MUJ-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
3W8X27-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
4ELR7K-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
6GRCUL-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
6XRJND-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
7CPVTB-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
8PW7XC-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
8YYJXD-5562	S-1-5-21-3501254099-4204809888-2000606956-1002.
8ZU2ZE-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
98A6KL-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
9WRPDD-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
9ZBF4H-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
A7BERC-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
ARP7Q6-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
B6WATE-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
B9WHYA-5561	S-1-5-21-3501254099-4204809888-2000606956-1002

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 9 - Examination Questions	
WebCode Test	**Response**
BN9WG8-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
BVR2DE-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
BYPLFC-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
CMTYN8-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
CN44V6-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
DHRBK7-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
E7WKY6-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
E7XH9Z-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
EAWU6Z-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
EREXP8-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
EX67D8-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
EZEWXB-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
F2G9Z3-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
F8L898-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
FGDPP2-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
FL36D9-5562	S-1-5-21-3501254099-4204809888-20000606956-1002
FVTQJ7-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
FXXHAY-5561	S-1-5-21-350125
G8GC37-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
GCTZYW-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
GFWVHY-5561	S-1-5-21-3501254099-4204809888-2000606956-1002

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 9 - Examination Questions	
WebCode Test	**Response**
GLX6QD-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
GR9ZT2-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
HDM36C-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
HDM9G8-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
HEVFPY-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
HPTDCY-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
HWZPPY-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
HX9YL3-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
JEDQ2D-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
JQ84YN-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
K4BTM4-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
K9GN9W-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
KA2332-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
KDZDY2-5561	S-1-5-21-3501254099-4204809888-2000606956-1005
LTKL96-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
LYVGBT-5561	S-1-5-21-3501254099-4204809888-200606956-1002
MW334U-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
PPRVBV-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
PPUJUU-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
PQ9R3V-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
PRHXH6-5562	S-1-5-21-3501254099-4204809888-2000606956-1002

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 9 - Examination Questions	
WebCode Test	**Response**
PTTY3H-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
PV4KAY-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
PZAFUR-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
Q8PGRF-5561	1002
QKG3YW-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
QLMMJQ-5561	S-1-5-21-3501254099-4204809888-20000606956-1002
QQ3XWU-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
QVYKR4-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
R8KDG3-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
RFWD9R-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
RNVVQP-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
T4JR6P-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
TA98UW-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
TE2AXW-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
TWHDG3-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
URL94P-5562	1002
VKGWHC-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
VRFDXN-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
VU4RLY-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
WB6WLF-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
WRDQDP-5562	S-1-5-21-3501254099-4204809888-2000606956-1002

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 9 - Examination Questions

WebCode Test	Response
WXJKCR-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
X7U2JR-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
XB3L8N-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
XGEEHM-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
Y4WCCF-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
YDMVRA-5562	[Participant did not return results for this question.]
YE4XXP-5561	S-1-5-21-3501254099-4204809888-2000606956-1006
YL2H7J-5562	S-1-5-21-3501254099-4204809888-2000606956-1006
YLG7ZJ-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
ZD74EJ-5561	S-1-5-21-3501254099-4204809888-2000606956-1002.
ZDHVAK-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
ZG7AXV-5561	S-1-5-21-3501254099-4204809888-2000606956-1002
ZLZ4XH-5561	S-1-5-21-3501254099-4204809888-2000606956-1002

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

Consensus Result:

S-1-5-21-3501254099-4204809888-2000606956-1002

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

S-1-5-21-3501254099-4204809888-2000606956-1000	defaultuser0	S-1-5-21-3501254099-4204809888-2000606956-1000
Jessie Jenkins	Jessie Jenkins	S-1-5-21-3501254099-4204809888-2000606956-1002
mom	mom	S-1-5-21-3501254099-4204809888-2000606956-1003
dad	dad	S-1-5-21-3501254099-4204809888-2000606956-1004
Sam	Sam	S-1-5-21-3501254099-4204809888-2000606956-1005
chris	chris	S-1-5-21-3501254099-4204809888-2000606956-1006

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
2GYK6H-5562	Eastern Standard Time
37HZM7-5561	Eastern Standard Time (UTC-05:00)
3ERMDL-5562	Eastern Standard time
3J2MUJ-5561	Eastern Standard Time (UTC-05:00)
3W8X27-5561	Eastern Standard Time
4ELR7K-5562	Eastern Time
6GRCUL-5562	Eastern Standard Time
6XRJND-5562	Eastern Standard Time
7CPVTB-5561	Eastern Standard Time, Daylight time active
8PW7XC-5562	(UTC-05:00) Eastern Time (US & Canada)
8YYJXD-5562	The configured time zone for the device is Eastern Standard Time ((UTC-05:00) Eastern Time (US & Canada)
8ZU2ZE-5562	Eastern Standard Time
98A6KL-5561	Eastern Standard Time(UTC -05:00)
9WRPDD-5562	Eastern Standard Time. (UTC-05:00) Eastern Time (US & Canada)
9ZBF4H-5561	Eastern Standard Time
A7BERC-5562	Eastern Standard Time
ARP7Q6-5561	Eastern Standard Time
B6WATE-5561	Eastern Standard time
B9WHYA-5561	Eastern Time

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 10 - Examination Questions	
WebCode Test	**Response**
BN9WG8-5562	Eastern Standard Time
BVR2DE-5562	Eastern Standard time
BYPLFC-5562	(UTC-05:00) Eastern Time (US & Canada)
CMTYN8-5561	Eastern Standard Time
CN44V6-5561	Eastern Standard Time
DHRBK7-5562	Eastern Standard Time (UTC-5)
E7WKY6-5561	Eastern Standard Time
E7XH9Z-5561	Eastern Standard Time
EAWU6Z-5561	Eastern Standard Time (Active Time Bias: 300 with DaylightBias of -60 and DaylightName: @tzres.dll -111)
EREXP8-5561	Eastern Standard Time
EX67D8-5562	Eastern Standard Time
EZEWXB-5561	Eastern Standard Time
F2G9Z3-5562	Eastern Standard Time (Current timezone offset -300 minutes)
F8L898-5562	Eastern Standard Time UTC-05:00 (US & Canada)
FGDPP2-5562	Eastern Standard Time
FL36D9-5562	Eastern Standard Time
FVTQJ7-5562	Eastern Standard Time (UTC -5)
FXXHAY-5561	Eastern Standard Time
G8GC37-5561	Eastern Standard Time
GCTZYW-5561	Eastern Standard Time
GFWVHY-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**
GLX6QD-5562	Eastern Daylight Time
GR9ZT2-5561	Eastern Standard Time
HDM36C-5561	Eastern Daylight Time
HDM9G8-5561	Eastern Standard Time
HEVFPY-5561	Eastern Standard Time
HPTDCY-5561	Eastern
HWZPPY-5562	Eastern Standard Time
HX9YL3-5562	Eastern Time Zone
JEDQ2D-5562	Eastern
JQ84YN-5561	Eastern Standard Time
K4BTM4-5561	Eastern Standard Time
K9GN9W-5561	Eastern Standard Time (UTC-05:00) with daylight saving or Eastern Daylight Time
KA2332-5562	Eastern Standard Time
KDZDY2-5561	UTC-05:00
LTKL96-5562	Eastern Standard Time
LYVGBT-5561	Eastern Standard Time
MW334U-5561	Eastern Standard Time
PPRVBV-5561	Eastern Standard Time (UTC -5:00)
PPUJUU-5561	(UTC-05:00) Eastern Standard Time (US & Canada)
PQ9R3V-5561	UTC-05:00 Eastern Standard Time (US & Canada)
PRHXH6-5562	Eastern Standard Time

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 10 - Examination Questions	
WebCode Test	**Response**
PTTY3H-5562	Eastern Standard Time
PV4KAY-5561	(UTC-05:00) Eastern Time (US & Canada)
PZAFUR-5562	Eastern Standard Time
Q8PGRF-5561	Eastern Standard Time
QKG3YW-5562	Eastern Standard Time
QLMMJQ-5561	Eastern Standard Time
QQ3XWU-5561	Eastern Standard Time
QVYKR4-5562	(UTC -05:00) Eastern Time (US & Canada)
R8KDG3-5562	Eastern Standard Time
RFWD9R-5562	Eastern Standard Time
RNVVQP-5561	Time zone: Eastern Standard Time
T4JR6P-5562	Eastern Standard Time (UTC-5)
TA98UW-5561	Eastern Standard Time
TE2AXW-5561	Eastern Standard Time (EST)
TWHDG3-5561	(UTC-05:00) Eastern Time (US & Canada)
URL94P-5562	Eastern Standard Time
VKGWHC-5561	Eastern Standard Time (EST)
VRFDXN-5561	Easter Standar Time (US&Canada) (UTC-5:00)
VU4RLY-5562	Eastern Standard Time
WB6WLF-5561	Eastern Standard Time
WRDQDP-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**
WXJKCR-5562	Eastern Standard Time
X7U2JR-5561	Eastern Standard time
XB3L8N-5562	Eastern Standard Time
XGEEHM-5561	Eastern Standard Time
Y4WCCF-5561	UTC-05:00
YDMVRA-5562	[Participant did not return results for this question.]
YE4XXP-5561	Eastern Standard Time
YL2H7J-5562	Eastern Standard Time
YLG7ZJ-5562	Eastern Standard Time
ZD74EJ-5561	The configured time zone for the device is Eastern Standard Time ((UTC-05:00) Eastern Time (US & Canada)
ZDHVAK-5562	Eastern Standard Time
ZG7AXV-5561	Eastern Standard Time
ZLZ4XH-5561	Eastern Standard Time

Question 10: What is the configured time zone?

Consensus Result:

Eastern Standard Time, or UTC-5 and other variations representing the Eastern time zone.

Expected Response Explanation:

Time zone setting information is found in the Windows 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.

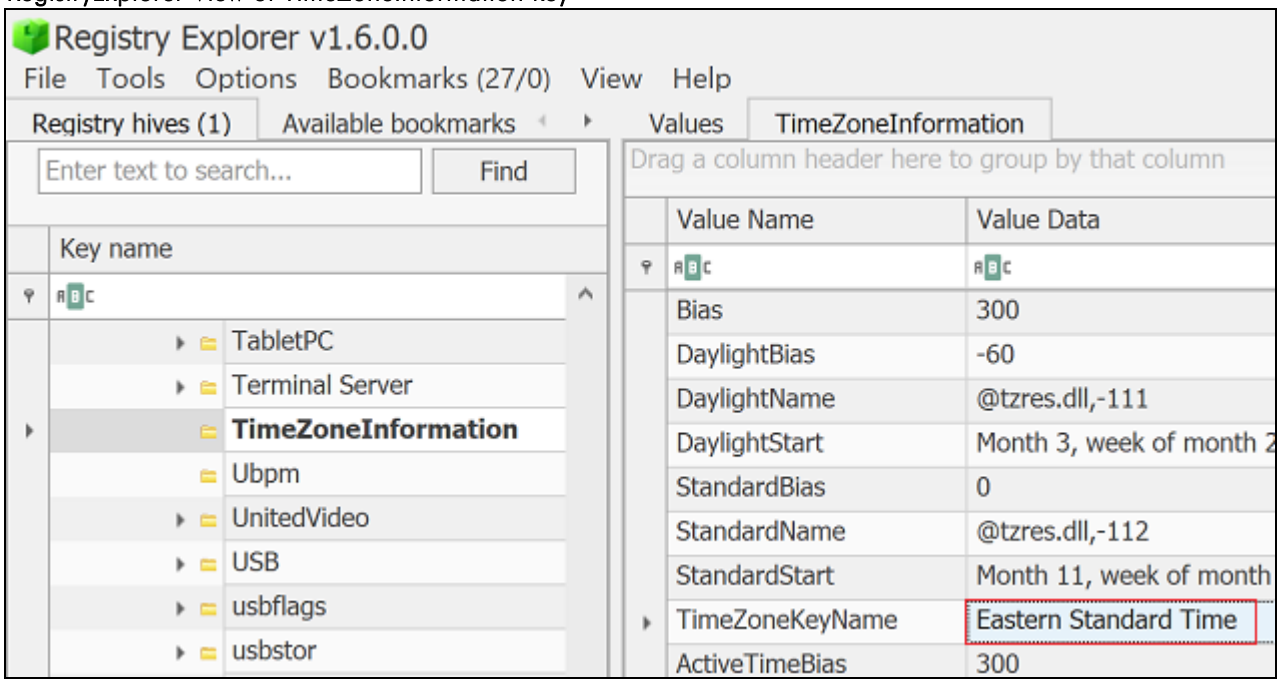
Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 10 - Examination Questions

Expected Response Illustration:

RegistryExplorer View of TimeZoneInformation key



Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 11 - Examination Questions

Question 11: Provide the SHA 1 hash value for the jpeg (.jpg) file captured with a DJI XT2 camera.

Manufacturer's Expected Response: 03be76ca62406c58e4778f1afac61ce02fe63cbe

WebCode Test	Response
2GYK6H-5562	03BE76CA62406C58E4778F1AFAC61CE02FE63CBE
37HZM7-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe
3ERMDL-5562	03BE76CA62406C58E4778F1AFAC61CE02FE63CBE
3J2MUJ-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe
3W8X27-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe
4ELR7K-5562	03be76ca62406c58e4778f1afac61ce02fe63cbe
6GRCUL-5562	03BE76CA62406C58E4778F1AFAC61CE02FE63CBE
6XRJND-5562	03BE76CA62406C58E4778F1AFAC61CE02FE63CBE
7CPVTB-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe
8PW7XC-5562	03be76ca62406c58e4778f1afac61ce02fe63cbe
8YYJXD-5562	03be76ca62406c58e4778f1afac61ce02fe63cbe
8ZU2ZE-5562	03be76ca62406c58e4778f1afac61ce02fe63cbe
98A6KL-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe
9WRPDD-5562	03be76ca62406c58e4778f1afac61ce02fe63cbe
9ZBF4H-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe
A7BERC-5562	03be76ca62406c58e4778f1afac61ce02fe63cbe
ARP7Q6-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe
B6WATE-5561	03BE76CA62406C58E4778F1AFAC61CE02FE63CBE
B9WHYA-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 11 - Examination Questions	
WebCode Test	**Response**
BN9WG8-5562	03BE76CA62406C58E4778F1AFAC61CE02FE63CBE
BVR2DE-5562	03BE76CA62406C58E4778F1AFAC61CE02FE63CBE
BYPLFC-5562	03be76ca62406c58e4778f1afac61ce02fe63cbe
CMTYN8-5561	03BE76CA62406C58E4778F1AFAC61CE02FE63CBE
CN44V6-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe
DHRBK7-5562	03be76ca62406c58e4778f1afac61ce02fe63cbe
E7WKY6-5561	03BE76CA62406C58E4778F1AFAC61CE02FE63CBE
E7XH9Z-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe
EAWU6Z-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe
EREXP8-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe
EX67D8-5562	03be76ca62406c58e4778f1afac61ce02fe63cbe
EZEWXB-5561	03Be76ca62406c58e4778f1afac61ce02fe63cbe
F2G9Z3-5562	03be76ca62406c58e4778f1afac61ce02fe63cbe
F8L898-5562	03be76ca62406c58e4778f1afac61ce02fe63cbe
FGDPP2-5562	03be76ca62406c58e4778f1afac61ce02fe63cbe
FL36D9-5562	03be76ca62406c58e4778f1afac61ce02fe63cbe
FVTQJ7-5562	03BE76CA62406C58E4778F1AFAC61CE02FE63CBE
FXXHAY-5561	03BE76CA62406C58E4778F1AFAC61CE02FE63CBE
G8GC37-5561	03BE76CA62406C58E4778F1AFAC61CE02FE63CBE
GCTZYW-5561	03BE76CA62406C58E4778F1AFAC61CE02FE63CBE
GFWVHY-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 11 - Examination Questions	
WebCode Test	**Response**
GLX6QD-5562	03be76ca62406c58e4778f1afac61ce02fe63cbe
GR9ZT2-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe
HDM36C-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe
HDM9G8-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe
HEVFPY-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe
HPTDCY-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe
HWZPPY-5562	03be76ca62406c58e4778f1afac61ce02fe63cbe
HX9YL3-5562	03be76ca62406c58e4778f1afac61ce02fe63cbe
JEDQ2D-5562	03be76ca62406c58e4778f1afac61ce02fe63cbe
JQ84YN-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe
K4BTM4-5561	03BE76CA62406C58E4778F1AFAC61CE02FE63CBE
K9GN9W-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe
KA2332-5562	03BE76CA62406C58E4778F1AFAC61CE02FE63CBE
KDZDY2-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe
LTKL96-5562	Photo1.jpg
LYVGBT-5561	03BE76CA62406C58E4778F1AFAC61CE02FE63CBE
MW334U-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe
PPRVBV-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe
PPUJUU-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe
PQ9R3V-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe
PRHXH6-5562	03BE76CA62406C58E4778F1AFAC61CE02FE63CBE

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 11 - Examination Questions	
WebCode Test	**Response**
PTTY3H-5562	03be76ca62406c58e4778f1afac61ce02fe63cbe
PV4KAY-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe
PZAFUR-5562	03BE76CA62406C58E4778F1AFAC61CE02FE63CBE
Q8PGRF-5561	03BE76CA62406C58E4778F1AFAC61CE02FE63CBE
QKG3YW-5562	03BE76CA62406C58E4778F1AFAC61CE02FE63CBE
QLMMJQ-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe
QQ3XWU-5561	03BE76CA62406C58E4778F1AFAC61CE02FE63CBE
QVYKR4-5562	03BE76CA62406C58E4778F1AFAC61CE02FE63CBE
R8KDG3-5562	03BE76CA62406C58E4778F1AFAC61CE02FE63CBE
RFWD9R-5562	03BE76CA62406C58E4778F1AFAC61CE02FE63CBE
RNVVQP-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe
T4JR6P-5562	03be76ca62406c58e4778f1afac61ce02fe63cbe
TA98UW-5561	03BE76CA62406C58E4778F1AFAC61CE02FE63CBE
TE2AXW-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe
TWHDG3-5561	FILE NAME : Photo1.jpg SHA1 : 03be76ca62406c58e4778f1afac61ce02fe63cbe
URL94P-5562	03be76ca62406c58e4778f1afac61ce02fe63cbe
VKGWHC-5561	03BE76CA62406C58E4778F1AFAC61CE02FE63CBE
VRFDXN-5561	Photo1.jpg 03be76ca62406c58e4778f1afac61ce02fe63cbe
VU4RLY-5562	03be76ca62406c58e4778f1afac61ce02fe63cbe
WB6WLF-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe
WRDQDP-5562	03be76ca62406c58e4778f1afac61ce02fe63cbe

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 11 - Examination Questions	
WebCode Test	**Response**
WXJKCR-5562	03be76ca62406c58e4778f1afac61ce02fe63cbe
X7U2JR-5561	03BE76CA62406C58E4778F1AFAC61CE02FE63CBE
XB3L8N-5562	03BE76CA62406C58E4778F1AFAC61CE02FE63CBE
XGEEHM-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe
Y4WCCF-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe
YDMVRA-5562	[Participant did not return results for this question.]
YE4XXP-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe
YL2H7J-5562	03BE76CA62406C58E4778F1AFAC61CE02FE63CBE
YLG7ZJ-5562	03be76ca62406c58e4778f1afac61ce02fe63cbe
ZD74EJ-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe
ZDHVAK-5562	03BE76CA62406C58E4778F1AFAC61CE02FE63CBE
ZG7AXV-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe
ZLZ4XH-5561	03be76ca62406c58e4778f1afac61ce02fe63cbe

Question 11: Provide the SHA 1 hash value for the jpeg (.jpg) file captured with a DJI XT2 camera.

Consensus Result:

03be76ca62406c58e4778f1afac61ce02fe63cbe

Expected Response Explanation:

Camera capture information is often embedded as EXIF text in jpeg files. Some forensic tools index this kind of metadata. In this case, the subject photo can be found with a simple keyword search of jpeg files for the camera and model number.

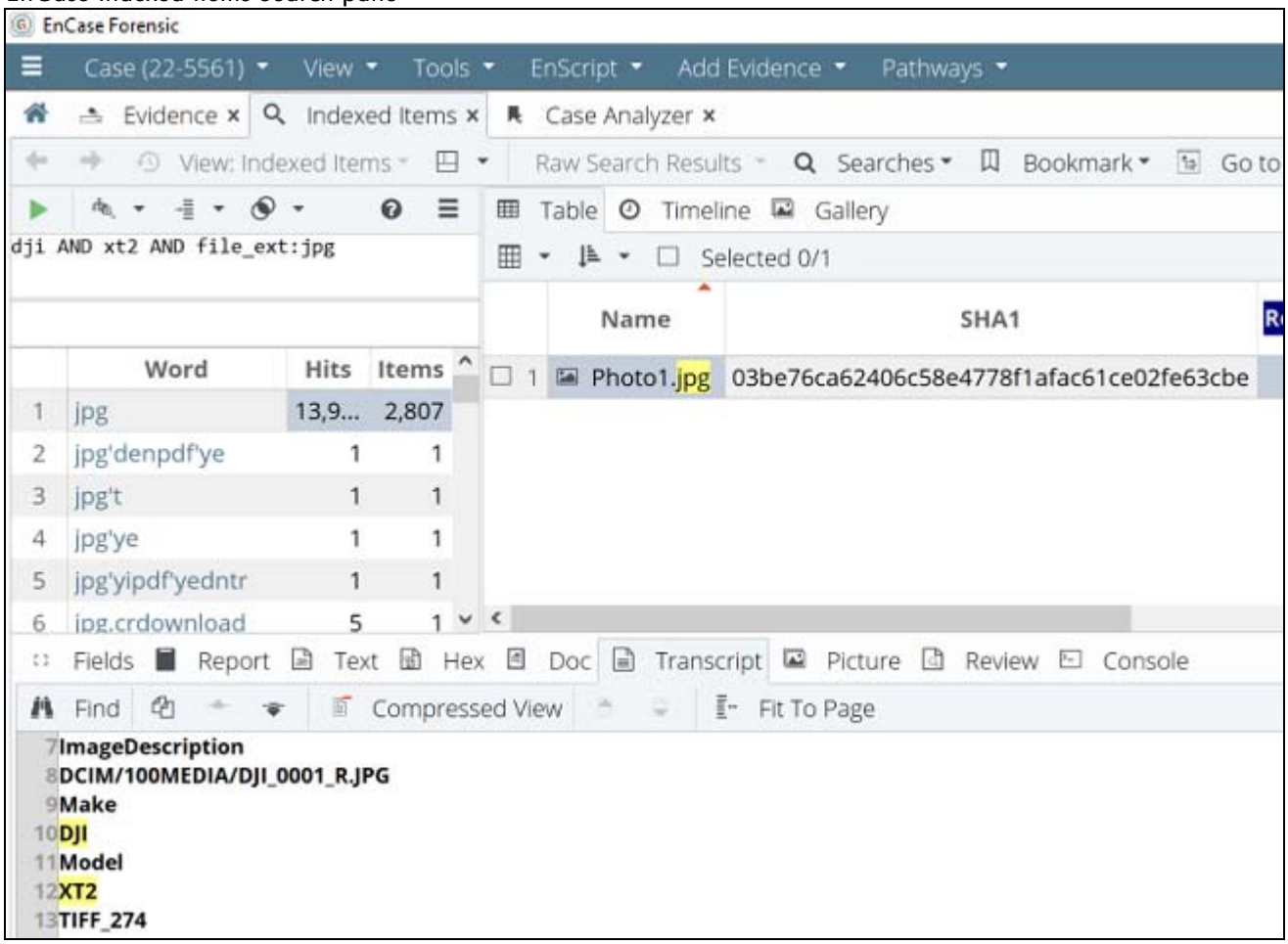
Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 11 - Examination Questions

Expected Response Illustration:

EnCase Indexed Items Search pane



Autopsy EXIF Metadata pane

Path	Device Model	▵ Device Make
/img_VictimComputer.E01/vol_vol3/Users/dad/Desktop/Photo1.jpg	XT2	DJI

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12 - Examination Questions

Question 12: What search terms did the Jessie Jenkins user search for (FIRST) on google.com on 02/10/2022 at 21:31:07 (UTC-05:00)?

Manufacturer's Expected Response: local meetups in reston

WebCode Test	Response
2GYK6H-5562	local meetups in reston
37HZM7-5561	local meetups in reston
3ERMDL-5562	local meetups in reston
3J2MUJ-5561	local meetups in reston
3W8X27-5561	Local meetups in Reston
4ELR7K-5562	local meetups in reston
6GRCUL-5562	local meetups in reston
6XRJND-5562	local meet-ups in Reston
7CPVTB-5561	local meetups in reston https://www.google.com/search?q=local+meetups+in+reston&rlz=1C1CHBF_enUS992&oq=local+meetups+in+reston&aqs=chrome..69i57j33i22i29i30.5016j0j7&sourceid=chrome&ie=UTF-8
8PW7XC-5562	local meetups in reston
8YYJXD-5562	“local meetups in reston”
8ZU2ZE-5562	adfont
98A6KL-5561	local meetups in reston
9WRPDD-5562	local meetups in reston
9ZBF4H-5561	local meetups in reston
A7BERC-5562	local meetups in reston
ARP7Q6-5561	local meetups in reston
B6WATE-5561	local meetups in reston

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12 - Examination Questions	
WebCode Test	**Response**
B9WHYA-5561	local meetups in reston
BN9WG8-5562	local meetups in reston
BVR2DE-5562	local meetups in reston
BYPLFC-5562	local meetups in reston
CMTYN8-5561	local meetups in reston
CN44V6-5561	local meetups in reston
DHRBK7-5562	local meetups in reston
E7WKY6-5561	local meetups in reston
E7XH9Z-5561	local meetups in reston
EAWU6Z-5561	local meetups in reston
EREXP8-5561	local meetups in reston
EX67D8-5562	local meetups in reston
EZEWXB-5561	local meetups in reston
F2G9Z3-5562	local meetups in reston
F8L898-5562	local meetups in Reston
FGDPP2-5562	local meetups in reston
FL36D9-5562	Local meetups in reston
FVTQJ7-5562	local meetups in reston
FXXHAY-5561	Local meetups in Reston
G8GC37-5561	local meetups in reston
GCTZYW-5561	adfontes

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12 - Examination Questions	
WebCode Test	**Response**
GFWVHY-5561	local meetups in reston
GLX6QD-5562	local meetups in reston
GR9ZT2-5561	Local meetups in reston
HDM36C-5561	local meetups in person
HDM9G8-5561	local meetups in reston
HEVFPY-5561	Local meetups in reston
HPTDCY-5561	local meetups in reston
HWZPPY-5562	local meetups in reston
HX9YL3-5562	local meetups in reston
JEDQ2D-5562	local meetups in reston
JQ84YN-5561	local meetups in reston
K4BTM4-5561	local meetups in reston
K9GN9W-5561	local meetups in reston
KA2332-5562	local meetups in reston
KDZDY2-5561	local meetups in reston
LTKL96-5562	local meetups in reston
LYVGBT-5561	Local Meetups in Reston
MW334U-5561	Local meetups in reston
PPRVBV-5561	local meetups in reston
PPUJUU-5561	local meetups in reston
PQ9R3V-5561	Local meetups in Reston

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12 - Examination Questions	
WebCode Test	**Response**
PRHXH6-5562	local meetups in reston
PTTY3H-5562	local meetups in reston
PV4KAY-5561	local meetups in reston
PZAFUR-5562	Local meetups in Reston
Q8PGRF-5561	local meetups in reston
QKG3YW-5562	“local meetups in reston”
QLMMJQ-5561	local meetups in reston
QQ3XWU-5561	local meetups in reston
QVYKR4-5562	local meetups in reston (11/02/2022 02:31:07hrs UTC+0)
R8KDG3-5562	local meetups in reston
RFWD9R-5562	local meetups in reston
RNVVQP-5561	local meetups in reston
T4JR6P-5562	local meetups in reston
TA98UW-5561	local meetups in reston
TE2AXW-5561	local meetups in reston
TWHDG3-5561	local meetups in reston
URL94P-5562	local meetups in reston
VKGWHC-5561	local meetups in reston
VRFDXN-5561	local meetups in reston
VU4RLY-5562	local meetups in reston
WB6WLF-5561	local meetups in reston

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12 - Examination Questions	
WebCode Test	**Response**
WRDQDP-5562	local meetups in reston
WXJKCR-5562	local meetups in reston
X7U2JR-5561	local meetups in reston
XB3L8N-5562	local meetups in reston
XGEEHM-5561	local meetups in reston
Y4WCCF-5561	local meetups in reston
YDMVRA-5562	[Participant did not return results for this question.]
YE4XXP-5561	local meetups in reston
YL2H7J-5562	local meetups in reston
YLG7ZJ-5562	local meetups in reston
ZD74EJ-5561	“local meetups in reston”
ZDHVAK-5562	local meetups in reston
ZG7AXV-5561	Local meetups in reston
ZLZ4XH-5561	Local meetups in reston

Question 12: What search terms did the Jessie Jenkins user search for (FIRST) on google.com on 02/10/2022 at 21:31:07 (UTC-05:00)?

Consensus Result:

local meetups in reston

Expected Response Explanation:

This search was executed using the Chrome browser. Chrome history events for this user are stored in C:\Users\Jessie Jenkins\AppData\Local\Google\Chrome\User Data\Default\History.

Expected Response Illustration:

EnCase table view of internet browser history record

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13 - Examination Questions

Question 13: Provide the path and filename of the file containing the term "Micrathene".

Manufacturer's Expected Response: C:\Users\Jessie Jenkins\Documents\Book1.xlsx

WebCode Test	Response
2GYK6H-5562	\Users\Jessie Jenkins\Documents\Book1.xlsx
37HZM7-5561	C:\Users\Jessie Jenkins\Documents\Book1.xlsx
3ERMDL-5562	Path : /Users/Jessie Jenkins/Documents/Book1.xlsx Filename : Book1.xlsx
3J2MUJ-5561	Path: Partition 2 (Microsoft NTFS, 29.95 GB)\Users\Jessie Jenkins\Documents\Book1.xlsx Filename: Book1.xlsx
3W8X27-5561	Users/Jessie Jenkins/Documents/Book1.xlsx
4ELR7K-5562	Users\Jessie Jenkins\Documents\Book1.xlsx
6GRCUL-5562	\Users\Jessie Jenkins\Documents\Book1.xlsx
6XRJND-5562	\Users\Jessie Jenkins\Documents\Book1.xlsx
7CPVTB-5561	Path: Partition 2 (Microsoft NTFS, 29.95 GB)\Users\Jessie Jenkins\Documents\Book1.xlsx Filename: Book1.xlsx
8PW7XC-5562	\Users\Jessie Jenkins\Documents\Book1.xlsx
8YYJXD-5562	D\Users\Jessie Jenkins\Documents\Book1.xlsx
8ZU2ZE-5562	\Users\Jessie Jenkins\Documents\Book1.xlsx
98A6KL-5561	C:\Users\Jessie Jenkins\Documents\Book1.xlsx
9WRPDD-5562	Users\Jessie Jenkins\Documents\Book1.xlsx
9ZBF4H-5561	Path: Partition 2 (Microsoft NTFS, 29.95 GB)\Users\Jessie Jenkins\Documents\Book1.xlsx FileName: Book1.xlsx
A7BERC-5562	\Users\Jessie Jenkins\Documents\Book1.xlsx Book1.xlsx
ARP7Q6-5561	VictimComputer\D\Users\Jessie Jenkins\Documents\Book1.xlsx Filename - Book1.xlsx
B6WATE-5561	Path : /Users/Jessie Jenkins/Documents/Book1.xlsx Filename : Book1.xlsx
B9WHYA-5561	\Users\Jessie Jenkins\Documents\Book1.xlsx

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13 - Examination Questions	
WebCode Test	**Response**
BN9WG8-5562	Path:- User\Jessie Jenkins\Documents\Book1.xlsx File Name:-Book1.xlsx
BVR2DE-5562	Path /Users/Jessie Jenkins/Documents/Book1.xlsx Filename: Book1.xlsx
BYPLFC-5562	C:\Users\Jessie Jenkins\Documents\Book1.xlsx
CMTYN8-5561	\Users\Jessie Jenkins\Documents\Book1.xlsx
CN44V6-5561	Users\Jessie Jenkins\Documents\Book1.xlsx
DHRBK7-5562	C:\Users\Jessie Jenkins\Documents\Book1.xlsx
E7WKY6-5561	\Users\Jessie Jenkins\Documents\Book1.xlsx
E7XH9Z-5561	\Users\Jessie Jenkins\Documents\Book1.xlsx, Book1.xlsx
EAWU6Z-5561	The file path is: <root>\Users\Jessie Jenkins\Documents\ and the filename is “Book1.xlsx”.
EREXP8-5561	C:\Users\Jessie Jenkins\Documents\Book1.xlsx
EX67D8-5562	Users\Jessie Jenkins\Documents\Book1.xlsx
EZEWXB-5561	22-5561.E01-Partition 2 (Microsoft NTFS, 29.95 GB)\Users\Jessie Jenkins\Documents\Book1.xlxs
F2G9Z3-5562	\Users\Jessue Jenkins\Documents\Book1.xlsx
F8L898-5562	Users\Jessie Jenkins\Documents\Book1.xlsx
FGDPP2-5562	Path: Partition 2/NONAME [NTFS]/[root]/Users/Jessie Jenkins/Documents/Book1.xlsx, File Name: Book1.xlsx
FL36D9-5562	Users\Jessie Jenkins\Documents\Book1.xlsx
FVTQJ7-5562	\Users\Jessie Jenkins\Documents\Book1.xlsx
FXXHAY-5561	C:\Users\Jessie Jenkins\Documents\Book1.xlsx
G8GC37-5561	\Users\Jessie Jenkins\Documents\Book1.xlsx
GCTZYW-5561	\Users\Jessie Jenkins\Documents\Book1.xlsx
GFWVHY-5561	\root\Users\Jessie Jenkins\Documents\Book1.xlsx

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13 - Examination Questions	
WebCode Test	**Response**
GLX6QD-5562	22-5561.E01\Partition @ 104448\Root\Users\Jessie Jenkins\Documents\Book1.xlsx
GR9ZT2-5561	\Users\Jessie Jenkins\Documents\Book1.xlsx
HDM36C-5561	22-5561.E01\Partition @ 104448\Root\Users\Jessie Jenkins\Documents\Book1.xlsx\
HDM9G8-5561	Users\Jessie Jenkins\Documents\Book1.xlsx
HEVFPY-5561	\Users\Jessie Jenkins\Documents\Book1.xlsx\xl\sharedStrings.xml
HPTDCY-5561	\Users\Jessie Jenkins\Documents\Book1.xlsx
HWZPPY-5562	\Users\Jessie Jenkins\Documents\Book1.xlsx
HX9YL3-5562	\Users\Jessie Jenkins\Documents\Book1.xlsx
JEDQ2D-5562	\Users\Jessie Jenkins\Documents\Book1.xlsx
JQ84YN-5561	22-5561.E01 - Partition 2 (Microsoft NTFS, 29.95 GB)\Users\Jessie Jenkins\Documents\Book1.xlsx Book1.xlsx
K4BTM4-5561	\Users\Jessie Jenkins\Documents\Book1.xlsx
K9GN9W-5561	Path – 22-5561.E01 - Partition 2 (Microsoft NTFS, 29.95 GB)\Users\Jessie Jenkins\Documents\Book1.xlsx OR Users\Jessie Jenkins\Documents\Book1.xlsx OR 22-5561.E01/Partition 2/NONAME [NTFS]/[root]/Users/Jessie Jenkins/Documents/Book1.xlsx Filename – Book1.xlsx
KA2332-5562	\Users\Jessie Jenkins\Documents\Book1.xlsx
KDZDY2-5561	C:\Users\Jessie Jenkins\Documents\Book1.xlsx
LTKL96-5562	Partition 2 (Microsoft NTFS, 29.95 GB)\Users\Jessie Jenkins\Documents\Book1.xlsx
LYVGBT-5561	C:\Users\Jessie Jenkins\Documents\Book1.xlsx
MW334U-5561	\Users\Jessie Jenkins\Documents\Book1.xlsx
PPRVBV-5561	Path: root\Users\Jessie Jenkins\Documents\Book1.xlsx Filename: Book1.xlsx
PPUJUU-5561	C:\Users\Jessie Jenkins\Documents\Book1.xlsx
PQ9R3V-5561	Users\Jessie Jenkins\Documents\Book1.xlsx

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13 - Examination Questions	
WebCode Test	**Response**
PRHXH6-5562	\Users\Jessie Jenkins\Documents\Book1.xlsx
PTTY3H-5562	C:\Users\Jessie Jenkins\Documents\Book1.xlsx
PV4KAY-5561	Users\Jessie Jenkins\Documents\Book1.xlsx
PZAFUR-5562	Partition 2\Users\Jessie Jenkins\Documents\Book1.xlsx
Q8PGRF-5561	path = \Users\Jessie Jenkins\Documents; filename = Book1.xlsx
QKG3YW-5562	Partition 2\Users\Jessie Jenkins\Documents\Book1.xlsx
QLMMJQ-5561	Users\Jessie Jenkins\Documents\Book1.xlsx
QQ3XWU-5561	C:\Users\Jessie Jenkins\Documents\Book1.xlsx
QVYKR4-5562	Users\Jessie Jenkins\Documents\Book1.xlsx
R8KDG3-5562	Partition2: \\Users\Jessie Jenkins\Documents\Book1.xlsx
RFWD9R-5562	22-5561.E01\Partition 2\NONAME [NTFS]\[root]\Users\Jessie Jenkins\Documents\Book1.xlsx
RNVVQP-5561	\Users\Jessie Jenkins\Documents\Book1.xlsx (Operating System Partition)
T4JR6P-5562	\Users\Jessie Jenkins\Documents\Book1.xlsx
TA98UW-5561	C:\Users\Jessie Jenkins\Documents\Book1.xlsx
TE2AXW-5561	22-5561.E01/Partition 2/NONAME [NTFS]/[root]/Users/Jessie Jenkins/Documents/Book1.xlsx
TWHDG3-5561	Path : C:\Users\Jessie Jenkins\Documents\ File Name : Book1.xlsx
URL94P-5562	C:\Users\Jessie\Jenkins\Documents\Book1.xlsx
VKGWHC-5561	C:\Users\Jessie Jenkins\Documents\Book1.xlsx
VRFDXN-5561	VictimComputer\D\Users\Jessie Jenkins\Documents\Book1.xlsx
VU4RLY-5562	Book1.xlsx \users\jessie jenkins\Documents
WB6WLF-5561	C:\Users\Jessie Jenkins\Documents\Book1.xlsx Book1.xlsx

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13 - Examination Questions	
WebCode Test	**Response**
WRDQDP-5562	C:/Users/Jessie Jenkins/Documents/Book1.xlsx
WXJKCR-5562	Users\Jessie Jenkins\Documents\Book1.xlsx, Book1.xlsx
X7U2JR-5561	Path : /Users/Jessie Jenkins/Documents/Book1.xlsx Filename : Book1.xlsx
XB3L8N-5562	Users\Jessie Jenkins\Documents\Book1.xlsx
XGEEHM-5561	Users\Jessie Jenkins\Documents\Book1.xlsx
Y4WCCF-5561	C:\Users\Jessie Jenkins\Documents\Book1.xlsx
YDMVRA-5562	[Participant did not return results for this question.]
YE4XXP-5561	22-5561.E01 - Partition 2 (Microsoft NTFS, 29.95 GB)\Users\Jessie Jenkins\Documents\Book1.xlsx
YL2H7J-5562	22-5561\Partition 2\Users\Jessie Jenkins\Documents\Book1.xlsx
YLG7ZJ-5562	Path:22-5561.E01 - Partition 2 (Microsoft NTFS, 29.95 GB)\Users\Jessie Jenkins\Documents\Book1.xlsx Filename: Book1.xlsx
ZD74EJ-5561	D\Users\Jessie Jenkins\Documents\Book1.xlsx
ZDHVAK-5562	\Users\Jessie Jenkins\Documents\Book1.xlsx
ZG7AXV-5561	Users/Jessie Jenkins/Documents/Book1.xlsx
ZLZ4XH-5561	\Users\Jessie Jenkins\Documents\Book1.xlsx

Question 13: Provide the path and filename of the file containing the term "Micrathene".

Consensus Result:

C:\Users\Jessie Jenkins\Documents\Book1.xlsx

Expected Response Explanation:

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

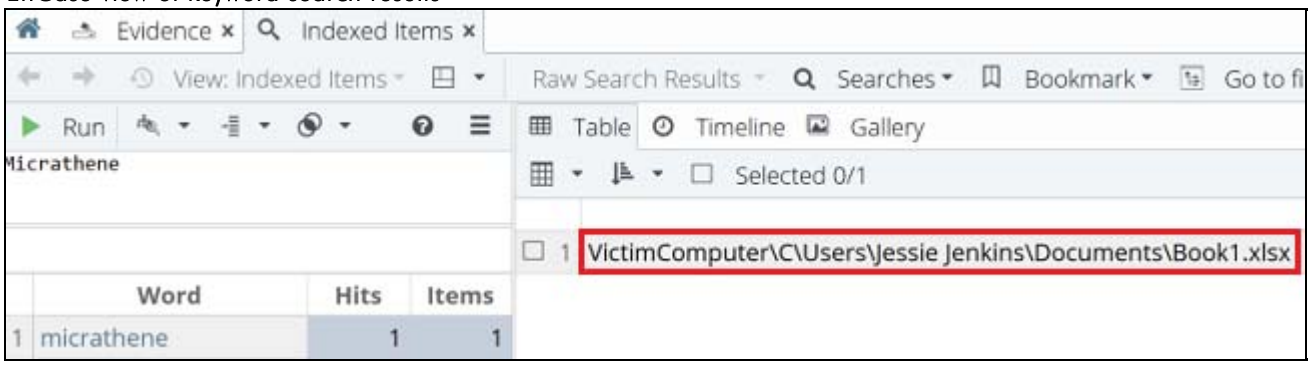
Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13 - Examination Questions

Expected Response Illustration:

EnCase view of keyword search results



Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 14 - Examination Questions

Question 14: What event was scheduled to occur at the location user Jessie Jenkins searched for directions to on 02/24/2022 21:11:51 (UTC-05:00)?

Manufacturer's Expected Response: Mardis Gras Masquerade Party (Meetup) at Rebel Taco in Washington, DC

WebCode Test	Response
2GYK6H-5562	Mardis Gras Masquerade Party
37HZM7-5561	Mardi Gras Masquerade Party. Scheduled to occur Friday, February 25, 2022 10:00 PM, ET Rebel Taco 1214 U St NW Washington, DC 20009.
3ERMDL-5562	Mardis Gras Masquerade Party
3J2MUJ-5561	Mardis Gras Masquerade Party
3W8X27-5561	Mardi Gras Masquerade Party at Rebel Taco
4ELR7K-5562	Mardis Gras Masquerade Party
6GRCUL-5562	Mardis Gras Masquerade Party
6XRJND-5562	EDM pop-up Party
7CPVTB-5561	Event: Mardis Gras Masquerade Party Location: Rebel Taco 1214 U St NW · Washington, DC
8PW7XC-5562	Mardis Gras Masquarade Party
8YYJXD-5562	Rebel Taco 1214 U St NW · Washington, DC - Google Search - 2/25/2022 2:11:51 AM
8ZU2ZE-5562	Mardis Gras Masquerade Party
98A6KL-5561	Mardis Gras Masquerade Party
9WRPDD-5562	Mardis Gras Masquerade Party. Rebel Taco 1214 U St NW · Washington, DC
9ZBF4H-5561	Mardis Gras Masquerade Party
A7BERC-5562	Rebel Taco 1214 U St NW · Washington, DC
ARP7Q6-5561	Mardis Gras Masquerade Party
B6WATE-5561	Mardis Gras Masquerade Party
B9WHYA-5561	Mardis Gras Masquerade Party

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 14 - Examination Questions	
WebCode Test	**Response**
BN9WG8-5562	Mardis Gras Masquerade Party at rebel taco
BVR2DE-5562	Mardis Gras Masquerade Party
BYPLFC-5562	Mardis Gras Masquerade Party
CMTYN8-5561	Mardi Gras Masquerade Party
CN44V6-5561	Mardis Gras Masquerade Party
DHRBK7-5562	Mardis Gras Masquerade Party
E7WKY6-5561	Mardis Gras Masquerade Party
E7XH9Z-5561	Mardi Gras Masquerade Party
EAWU6Z-5561	The event was the “Mardis Gras Masquerade Party” to take place at “Rebel Taco” at 1214 U St. NW in Washington DC.
EREXP8-5561	Mardis Gras Masquerade Party Meetup
EX67D8-5562	Mardis Gras Masquerade Party
EZEWXB-5561	Mardis Gras Masquerade Party
F2G9Z3-5562	Mardis Gras Masquerade Party
F8L898-5562	Mardis Gras Masquerade Party
FGDPP2-5562	Mardis Gras Masquerade Party
FL36D9-5562	Mardis Gras masquerade Party
FVTQJ7-5562	Mardis Gras Masquerade Party
FXXHAY-5561	Mardi Gras Masquerade Party Meetup
G8GC37-5561	Mardis Gras Masquerade Party at Rebel Taco 1214 U St NW · Washington, DC 20009
GCTZYW-5561	Mardi Gras Masquerade Party
GFWVHY-5561	Martis Gras Masquerade Party

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 14 - Examination Questions	
WebCode Test	**Response**
GLX6QD-5562	Mardis Gras Masquerade Party
GR9ZT2-5561	Mardi Gras Masquerade Party
HDM36C-5561	Mardis Gras Masquerade Party
HDM9G8-5561	NoVa Singles Mardis Gras Masquerade Party
HEVFPY-5561	Mardis Gras Masquerade Party
HPTDCY-5561	Mardis Gras Masquerade Party - Meetup
HWZPPY-5562	Mardis Gras Masquerade Party
HX9YL3-5562	Mardi Gras Masquerade Party
JEDQ2D-5562	Rebel Taco 1214 U St NW · Washington, DC
JQ84YN-5561	Mardis Gras Masquerade Party
K4BTM4-5561	Mardis Gras Masquerade Party
K9GN9W-5561	Mardi Gras Masquerade Party
KA2332-5562	Mardis Gras Masquerade Party
KDZDY2-5561	Mardis Gras Masquerade Party
LTKL96-5562	Rebel Taco 1214 U St NW · Washington, DC
LYVGBT-5561	Mardi Gras Masquerade Party Meet Up
MW334U-5561	Mardis Gras Masquerade Party
PPRVBV-5561	Mardis Gras Masquerade Party Meetup
PPUJUU-5561	Mardis Gras Masquerade Party
PQ9R3V-5561	Mardis Gras Masquerade Party
PRHXH6-5562	Mardis Gras Masquerade Party

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 14 - Examination Questions	
WebCode Test	**Response**
PTTY3H-5562	Mardis Gras Masquerade Party
PV4KAY-5561	NoVa Singles Mardis Gras Masquerade Party | Meetup | Friday, February 25, 2022 10PM ET | Rebel Taco
PZAFUR-5562	Mardis Gras Masquerade Party, Search: Location: Rebel Taco, 1214 U St NW, Washington DC
Q8PGRF-5561	Mardi Gras Masquerade Party (location = Rebel Taco 1214 U St NW, Washington, DC)
QKG3YW-5562	Mardis Gras Masquerade Party
QLMMJQ-5561	Mardis Gras Masquerade Party
QQ3XWU-5561	Mardis Gras Masquerade Party
QVYKR4-5562	'Mardis Gras Masquerade Party' at Rebel Taco arranged through website Meetup.com Map search on 25/02/2022 02:11:51hrs (UTC+0) was for Rebel Taco, Washington DC
R8KDG3-5562	Mardis Gras Masquerade Party
RFWD9R-5562	Rebel Taco 1214 U St NW · Washington, DC
RNVVQP-5561	"Mardis Gras Masquerade Party"
T4JR6P-5562	Mardis Gras Masquerade Party
TA98UW-5561	Mardis Gras Masquerade Party
TE2AXW-5561	Mardis Gras Masquerade Party
TWHDG3-5561	Jessie Jenkins is supposed to meet at rebel taco's house.
URL94P-5562	Rebel Taco 1214 U St NW washington DC. Event Mardi Gras Masquerade Party Friday 25th February
VKGWHC-5561	Mardis Gras Masquerade Party
VRFDXN-5561	Rebel Taco 1214 U StNW- Washington DC. Mexican restaurant.
VU4RLY-5562	Mardi Gras Masquerade Party
WB6WLF-5561	Mardis Gras Masquerade Party | Meetup
WRDQDP-5562	Rebel Taco 1214 U St NW · Washington, DC

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 14 - Examination Questions	
WebCode Test	**Response**
WXJKCR-5562	Mardis Gras Masquerade Party on the 25th Feb 2022 or Friday Rooftop Social 4th March 2022 or Friday Meetup 18th March 2022
X7U2JR-5561	Mardis Gras Masquerade Party
XB3L8N-5562	Mardis Gras Masquerade Party
XGEEHM-5561	Mardis Gras Masquerade Party
Y4WCCF-5561	Mardis Gras Masquerade Party
YDMVRA-5562	[Participant did not return results for this question.]
YE4XXP-5561	Mardis Gras Masquerade Party
YL2H7J-5562	Mardis Gras Masquerade Party
YLG7ZJ-5562	Mardis Gras Masquerade Party
ZD74EJ-5561	Rebel Taco 1214 U St NW · Washington, DC - Google Search - 2/25/2022 2:11:51 AM
ZDHVAK-5562	Mardi Gras Masquerade Party
ZG7AXV-5561	Mardi Gras Masquerade Party at Rebel Taco
ZLZ4XH-5561	Mardis Gras Masquerade Party

Question 14: What event was scheduled to occur at the location user Jessie Jenkins searched for directions to on 02/24/2022 21:11:51 (UTC-05:00)?

Consensus Result:

Mardis Gras Masquerade Party (Meetup) at Rebel Taco

Expected Response Explanation:

At 02/24/2022 21:11:51 (-5:00 Eastern Standard Time) user Jessie Jenkins searched Google maps for directions to Rebel Taco in Washington DC. Keyword searching for Rebel Taco across the device finds artifacts in internet history records and emails referencing the meetup for Mardis Gras Masquerade Party (Meetup) at Rebel Taco in Washington, DC.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

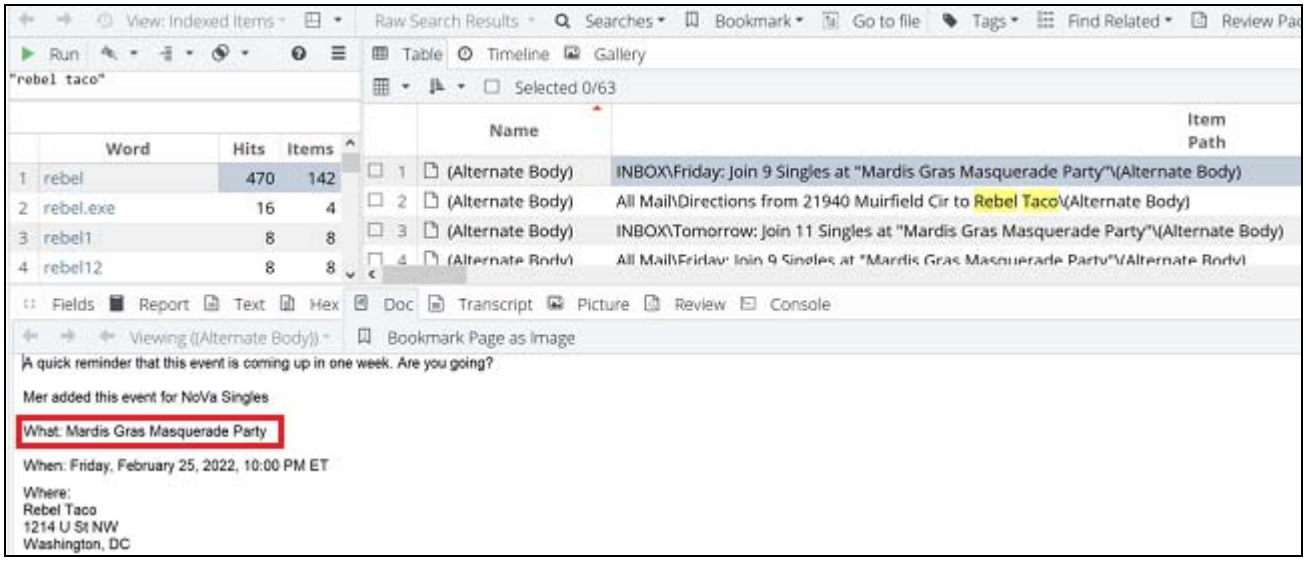
Question 14 - Examination Questions

Expected Response Illustration:

EnCase Table View of Internet History Records

Internet Artifact Type	Record Last Accessed	Url Name
History	02/24/2022 21:10:49 ...	https://mail.google.com/mail/u/0/#inbox/FMfcgzGmvBrxfhmdbcmbWLZnVFkRHBSH
History	02/24/2022 21:11:05 ...	http://meet.meetup.com/ls/click?upn=yBf4llw5PeaY7leriFwBBkipzLsJ7uXZdea5ZSOL1NLj-2FlOBe...
History	02/24/2022 21:11:05 ...	https://www.meetup.com/__ms355463778/novasingles/events/wsvkjlydcdblc/?refund_policy=tr...
History	02/24/2022 21:11:05 ...	https://www.google.com/url?q=http://meet.meetup.com/ls/click?upn%3DyBf4llw5PeaY7leriFwB...
History	02/24/2022 21:11:06 ...	https://www.meetup.com/novasingles/events/wsvkjlydcdblc/?refund_policy=true&rv=md2&_xtd...
History	02/24/2022 21:11:06 ...	https://www.meetup.com/novasingles/events/wsvkjlydcdblc/?refund_policy=true&rv=md2&_xtd...
History	02/24/2022 21:11:51 ...	https://www.google.com/search?q=Rebel+Taco+1214+U+St+NW+%C2%B7+Washington%2C+DC...
History	02/24/2022 21:11:51 ...	https://www.google.com/search?q=Rebel+Taco+1214+U+St+NW+%C2%B7+Washington%2C+DC...

EnCase View of email message re Mardi Gras Party



Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15 - Examination Questions

Question 15: What was the name of the wireless network to which the computer was connected?

Manufacturer's Expected Response: JenkinsHome

WebCode Test	Response
2GYK6H-5562	JenkinsHome
37HZM7-5561	JenkinsHome
3ERMDL-5562	JenkinsHome
3J2MUJ-5561	JenkinsHome
3W8X27-5561	JenkinsHome
4ELR7K-5562	JenkinsHome
6GRCUL-5562	JenkinsHome
6XRJND-5562	JenkinsHome
7CPVTB-5561	JenkinsHome Software/Microsoft/WindowsNT/CurrentVersion/NetworkList/Profiles
8PW7XC-5562	JenkinsHome
8YYJXD-5562	JenkinsHome
8ZU2ZE-5562	JenkninsHome
98A6KL-5561	JenkinsHome
9WRPDD-5562	JenkinsHome
9ZBF4H-5561	JenkinsHome
A7BERC-5562	JenkinsHome
ARP7Q6-5561	JenkinsHome
B6WATE-5561	JenkinsHome
B9WHYA-5561	JenkinsHome

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15 - Examination Questions	
WebCode Test	**Response**
BN9WG8-5562	JenkinsHome
BVR2DE-5562	JenkinsHome
BYPLFC-5562	JenkinsHome
CMTYN8-5561	JenkinsHome
CN44V6-5561	JenkinsHome
DHRBK7-5562	JenkinsHome
E7WKY6-5561	JenkinsHome
E7XH9Z-5561	JenkinsHome
EAWU6Z-5561	JenkinsHome
EREXP8-5561	Jenkins Home
EX67D8-5562	JenkinsHome
EZEWXB-5561	JenkinsHome
F2G9Z3-5562	JenkinsHome
F8L898-5562	JenkinsHome
FGDPP2-5562	JenkinsHome
FL36D9-5562	JenkinsHome
FVTQJ7-5562	JenkinsHome
FXXHAY-5561	JenkinsHome
G8GC37-5561	JenkinsHome
GCTZYW-5561	JenkinsHome
GFWVHY-5561	JenkinsHome

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15 - Examination Questions	
WebCode Test	**Response**
GLX6QD-5562	JenkinsHome
GR9ZT2-5561	Jenkins Home
HDM36C-5561	JenkinsHome
HDM9G8-5561	JenkinsHome
HEVFPY-5561	JenkinsHome
HPTDCY-5561	JenkinsHome
HWZPPY-5562	JenkinsHome
HX9YL3-5562	JenkinsHome
JEDQ2D-5562	JenkinsHome
JQ84YN-5561	JenkinsHome
K4BTM4-5561	JenkinsHome
K9GN9W-5561	JenkinsHome
KA2332-5562	JenkinsHome
KDZDY2-5561	JenkinsHome
LTKL96-5562	JenkinsHome
LYVGBT-5561	Jenkins Home
MW334U-5561	JenkinsHome
PPRVBV-5561	JenkinsHome
PPUJUU-5561	JenkinsHome
PQ9R3V-5561	JenkinsHome
PRHXH6-5562	JenkinsHome

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15 - Examination Questions	
WebCode Test	**Response**
PTTY3H-5562	JenkinsHome
PV4KAY-5561	JenkinsHome
PZAFUR-5562	JenkinsHome
Q8PGRF-5561	JenkinsHome
QKG3YW-5562	JenkinsHome
QLMMJQ-5561	JenkinsHome
QQ3XWU-5561	JenkinsHome
QVYKR4-5562	JenkinsHome
R8KDG3-5562	JenkinsHome
RFWD9R-5562	JenkinsHome
RNVVQP-5561	JenkinsHome
T4JR6P-5562	JenkinsHome
TA98UW-5561	JenkinsHome
TE2AXW-5561	JenkinsHome
TWHDG3-5561	JenkinsHome
URL94P-5562	JenkinsHome
VKGWHC-5561	JenkinsHome
VRFDXN-5561	JenkinsHome
VU4RLY-5562	JENKINSHOME
WB6WLF-5561	JenkinsHome
WRDQDP-5562	JenkinsHome

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15 - Examination Questions	
WebCode Test	**Response**
WXJKCR-5562	JenkinsHome
X7U2JR-5561	JenkinsHome
XB3L8N-5562	JenkinsHome
XGEEHM-5561	JenkinsHome
Y4WCCF-5561	JenkinsHome
YDMVRA-5562	[Participant did not return results for this question.]
YE4XXP-5561	JenkinsHome
YL2H7J-5562	JenkinsHome
YLG7ZJ-5562	JenkinsHome
ZD74EJ-5561	JenkinsHome
ZDHVAK-5562	JenkinsHome
ZG7AXV-5561	JenkinsHome
ZLZ4XH-5561	JenkinsHome

Question 15: What was the name of the wireless network to which the computer was connected?

Consensus Result:

JenkinsHome

Expected Response Explanation:

Information about wireless network connections can be found in the Windows Software registry hive at C:\Windows\System32\Config\Software:Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles. There is only one wireless network listed.

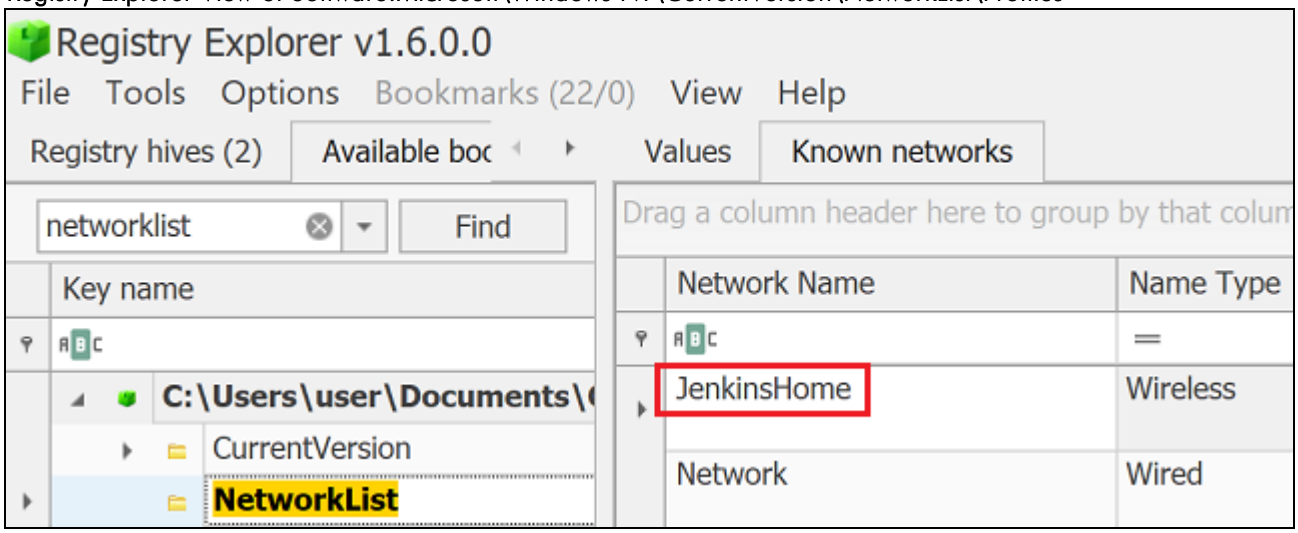
Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15 - Examination Questions

Expected Response Illustration:

Registry Explorer View of Software:Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles



Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16 - Examination Questions

Question 16: What IP address was assigned by this network?

Manufacturer's Expected Response: 192.168.3.121

WebCode Test	Response
2GYK6H-5562	192.168.3.121
37HZM7-5561	192.168.3.121
3ERMDL-5562	192.168.3.121
3J2MUJ-5561	192.168.3.121
3W8X27-5561	192.168.3.121
4ELR7K-5562	192.168.3.121
6GRCUL-5562	192.168.3.121
6XRJND-5562	192.168.3.121
7CPVTB-5561	192.168.3.121
8PW7XC-5562	192.168.3.121
8YYJXD-5562	192.168.3.121
8ZU2ZE-5562	192.168.3.121
98A6KL-5561	192.168.3.121
9WRPDD-5562	192.168.3.121
9ZBF4H-5561	192.168.3.121
A7BERC-5562	192.168.3.121
ARP7Q6-5561	192.168.3.121
B6WATE-5561	192.168.3.121
B9WHYA-5561	192.168.3.121

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16 - Examination Questions	
WebCode Test	**Response**
BN9WG8-5562	192.168.3.121
BVR2DE-5562	192.168.3.121
BYPLFC-5562	192.168.3.121
CMTYN8-5561	192.168.3.121
CN44V6-5561	192.168.3.121
DHRBK7-5562	192.168.3.121
E7WKY6-5561	192.168.3.121
E7XH9Z-5561	192.168.3.121
EAWU6Z-5561	192.168.3.121
EREXP8-5561	192.168.3.121
EX67D8-5562	192.168.3.121
EZEWXB-5561	192.168.3.121
F2G9Z3-5562	192.168.3.121
F8L898-5562	192.168.3.121
FGDPP2-5562	192.168.3.121
FL36D9-5562	30:5A:3A:C3:2E:E0
FVTQJ7-5562	192.168.3.121
FXXHAY-5561	192.168.3.121
G8GC37-5561	192.168.3.121
GCTZYW-5561	192.168.3.121
GFWVHY-5561	192.168.3.121

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16 - Examination Questions	
WebCode Test	**Response**
GLX6QD-5562	192.168.3.121
GR9ZT2-5561	192.168.3.121
HDM36C-5561	192.168.3.121
HDM9G8-5561	192.168.3.121
HEVFPY-5561	192.168.3.121
HPTDCY-5561	192.168.3.121
HWZPPY-5562	192.168.3.121
HX9YL3-5562	192.168.3.121
JEDQ2D-5562	192.168.3.121
JQ84YN-5561	192.168.3.121
K4BTM4-5561	192.168.3.121
K9GN9W-5561	192.168.3.121
KA2332-5562	192.168.3.121
KDZDY2-5561	192.168.3.121
LTKL96-5562	192.168.3.121
LYVGBT-5561	192.168.3.121
MW334U-5561	192.168.3.121
PPRVBV-5561	192.168.3.121
PPUJUU-5561	192.168.3.121
PQ9R3V-5561	192.168.3.121
PRHXH6-5562	192.168.3.121

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16 - Examination Questions	
WebCode Test	**Response**
PTTY3H-5562	192.168.3.121
PV4KAY-5561	192.168.3.121
PZAFUR-5562	192.168.3.121
Q8PGRF-5561	192.168.3.121
QKG3YW-5562	192.168.3.1
QLMMJQ-5561	192.168.3.121
QQ3XWU-5561	192.168.3.121
QVYKR4-5562	192.168.3.121
R8KDG3-5562	192.168.3.121
RFWD9R-5562	192.228.79.201
RNVVQP-5561	192.168.3.121
T4JR6P-5562	192.168.3.121
TA98UW-5561	192.168.3.121
TE2AXW-5561	192.168.3.121
TWHDG3-5561	192.168.3.121
URL94P-5562	192.168.3.121
VKGWHC-5561	192.168.3.121
VRFDXN-5561	192.168.3.121
VU4RLY-5562	192.168.3.1
WB6WLF-5561	192.168.3.121
WRDQDP-5562	192.168.3.121

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16 - Examination Questions	
WebCode Test	**Response**
WXJKCR-5562	192.168.3.121
X7U2JR-5561	192.168.3.121
XB3L8N-5562	192.168.3.121
XGEEHM-5561	192.168.3.121
Y4WCCF-5561	192.168.3.121
YDMVRA-5562	[Participant did not return results for this question.]
YE4XXP-5561	192.168.3.121
YL2H7J-5562	192.168.3.121
YLG7ZJ-5562	192.168.3.121
ZD74EJ-5561	192.168.3.121
ZDHVAK-5562	192.168.3.121
ZG7AXV-5561	192.168.3.121
ZLZ4XH-5561	192.168.3.121

Question 16: What IP address was assigned by this network?

Consensus Result:

192.168.3.121

Expected Response Explanation:

Information about network addresses can be found in the Windows SYSTEM registry hive at C:\Windows\System32\Config\SYSTEM:ControlSet001\Services\Tcpip\Parameters\Interfaces. Only keys for wireless interfaces will have a value for DhcpNetworkHint. There is only one IR address.

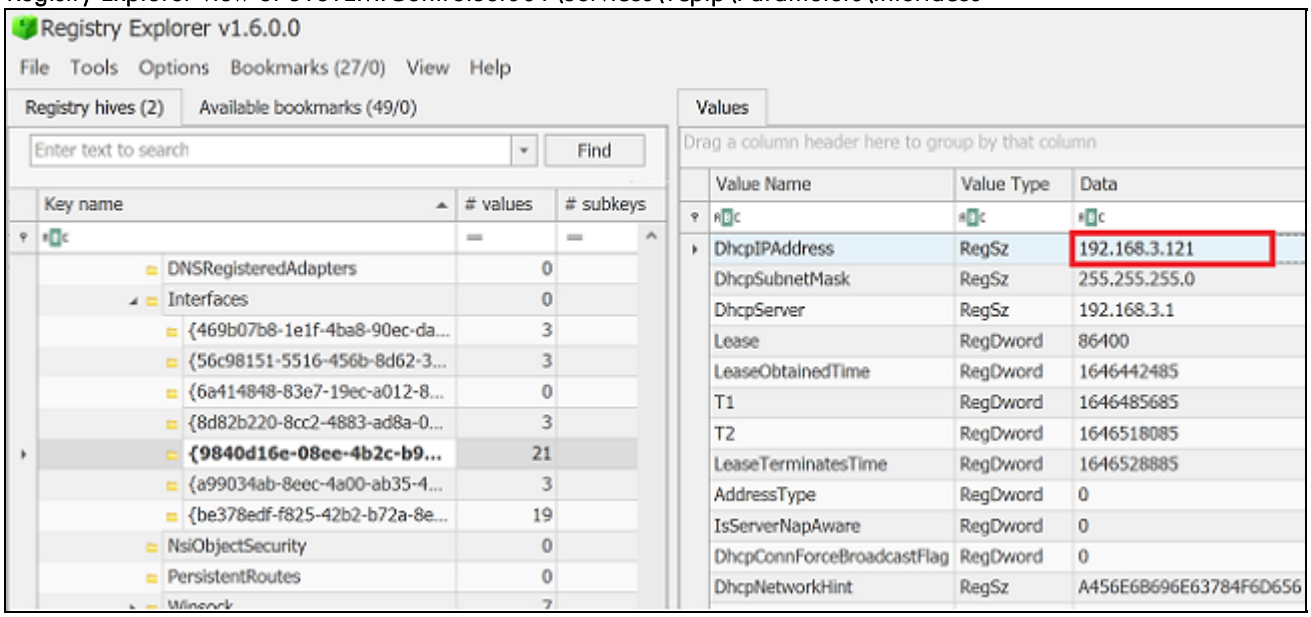
Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16 - Examination Questions

Expected Response Illustration:

Registry Explorer view of SYSTEM:ControlSet001\Services\Tcpip\Parameters\Interfaces



Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17 - Examination Questions

Question 17: From whom (provide name and email address) did Jessie Jenkins receive an email on 02/26/2022 17:39 (UTC-05:00)?

Manufacturer's Expected Response: Name: Alex Andersen
Email: alwaysalexandersen@gmail.com

WebCode Test	Response
2GYK6H-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
37HZM7-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
3ERMDL-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
3J2MUJ-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
3W8X27-5561	Name: Alex Anderson, Email: alwaysalexanderson@gmail.com
4ELR7K-5562	Name: Alex Anderson, Email: alwaysalexanderson@gmail.com
6GRCUL-5562	Name: Alex Anderson, Email: alwaysalexandersen@gmail.com
6XRJND-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
7CPVTB-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
8PW7XC-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
8YYJXD-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
8ZU2ZE-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
98A6KL-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
9WRPDD-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
9ZBF4H-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
A7BERC-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
ARP7Q6-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
B6WATE-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
B9WHYA-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17 - Examination Questions	
WebCode Test	**Response**
BN9WG8-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
BVR2DE-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
BYPLFC-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
CMTYN8-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
CN44V6-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
DHRBK7-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
E7WKY6-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
E7XH9Z-5561	Name: Alex Anderson, Email: alwaysalexanderson@gmail.com
EAWU6Z-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
EREXP8-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
EX67D8-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
EZEWXB-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
F2G9Z3-5562	Name: Alex Anderson, Email: alwaysalexanderson@gmail.com
F8L898-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
FGDPP2-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
FL36D9-5562	Name: Alex Andresen, Email: alwaysalexandersen@gmail.com
FVTQJ7-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
FXXHAY-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
G8GC37-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
GCTZYW-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17 - Examination Questions	
WebCode Test	**Response**
GFWVHY-5561	Name: Alex Anderson, Email: Alwaysalexandersen@gmail.com
GLX6QD-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
GR9ZT2-5561	Name: Alex Anderson, Email: alwaysalexanderson@gmail.com
HDM36C-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
HDM9G8-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
HEVFPY-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
HPTDCY-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
HWZPPY-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
HX9YL3-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
JEDQ2D-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
JQ84YN-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
K4BTM4-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
K9GN9W-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
KA2332-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
KDZDY2-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
LTKL96-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
LYVGBT-5561	Name: Alex Anderson, Email: alwaysalexanderson@gmail.com
MW334U-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
PPRVBV-5561	Name: Alex Andersen, Email: Alwaysalexandersen@gmail.com
PPUJUU-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
PQ9R3V-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17 - Examination Questions	
WebCode Test	**Response**
PRHXH6-5562	Name: Alex Anderson, Email: alwaysalexanderson@gmail.com
PTTY3H-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
PV4KAY-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
PZAFUR-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
Q8PGRF-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
QKG3YW-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
QLMMJQ-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
QQ3XWU-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
QVYKR4-5562	Name: Alex Andersen 26/02/22 22:39hrs (UTC+0), Email: alwaysalexandersen@gmail.com
R8KDG3-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
RFWD9R-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
RNVVQP-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
T4JR6P-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
TA98UW-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
TE2AXW-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
TWHDG3-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
URL94P-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
VKGWHC-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
VRFDXN-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
VU4RLY-5562	Name: ALEX ANDERSON, Email: alwaysalexanderson@gmail.com
WB6WLF-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17 - Examination Questions	
WebCode Test	**Response**
WRDQDP-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
WXJKCR-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
X7U2JR-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
XB3L8N-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
XGEEHM-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
Y4WCCF-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
YDMVRA-5562	[Participant did not return results for this question.]
YE4XXP-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
YL2H7J-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
YLG7ZJ-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
ZD74EJ-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
ZDHVAK-5562	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
ZG7AXV-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com
ZLZ4XH-5561	Name: Alex Andersen, Email: alwaysalexandersen@gmail.com

Question 17: From whom (provide name and email address) did Jessie Jenkins receive an email on 02/26/2022 17:39 (UTC-05:00)?

Consensus Result:

Name: Alex Andersen
Email: alwaysalexandersen@gmail.com

Expected Response Explanation:

Email files on this computer are stored in C:\Users\Jessie Jenkins\AppData\Roaming\Thunderbird\Profiles\1uql4331.default-release\ImapMail\imap.gmail.com\INBOX. A review of the contents of the Inbox by date and time finds the relevant message.

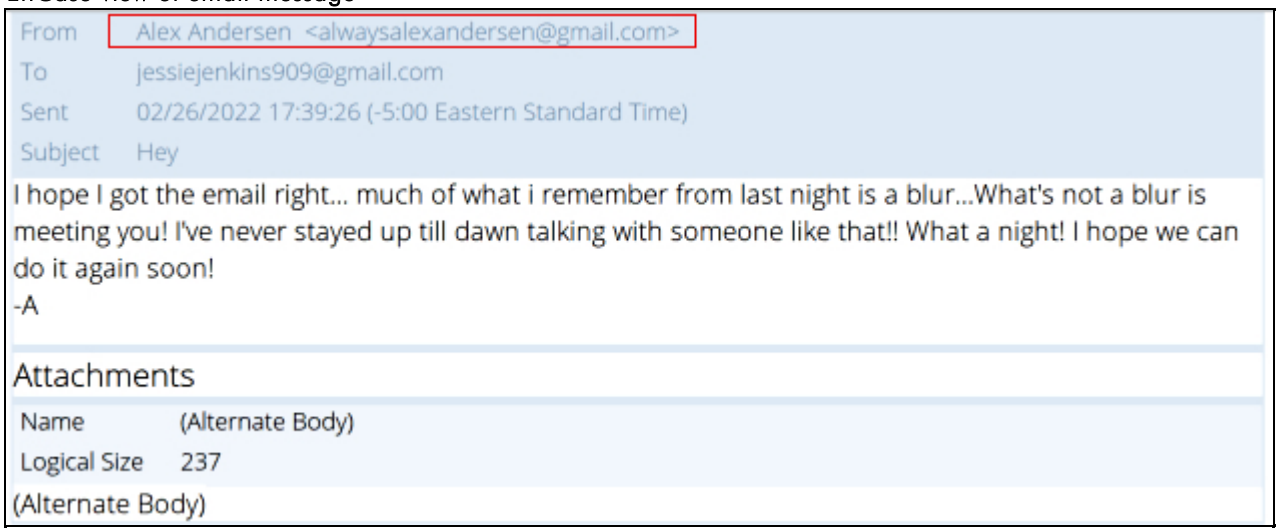
Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17 - Examination Questions

Expected Response Illustration:

EnCase view of email message



Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18 - Examination Questions

Question 18: Where and when did Jessie ultimately agree to meet the person from the response for question 17?

Manufacturer's Expected Response: Where: Founding Farmers Reston
When: 2022-03-05 20:00

WebCode Test	Response
2GYK6H-5562	Where: founding farmers reston station, When: 2022-05-03 20:00
37HZM7-5561	Where: Founding Farmers Restaurant, Reston VA, When: 2022-03-05 20:00
3ERMDL-5562	Where: Founding Farmers https://www.wearefoundingfarmers.com/location/reston/, When: 2022-03-05 20:00
3J2MUJ-5561	Where: Founding Farmers, When: 2022-03-05 20:00
3W8X27-5561	Where: We are Founding Fathers, When: 2022-05-03 20:00
4ELR7K-5562	Where: founding farmers, When: 2022-03-05 20:00
6GRCUL-5562	Where: Founding Farmers Reston Station, When: 2022-03-05 20:00
6XRJND-5562	Where: Founding Farmers, When: 2022-03-05 20:00
7CPVTB-5561	Where: Founding Farmers Reston Station https://www.wearefoundingfarmers.com/location/reston/, When: 2022-03-05 20:00
8PW7XC-5562	Where: "Founding Farmers Reston Station", 1904 RESTON METRO PLAZA, RESTON, VA 20190, When: 2022-03-05 20:00
8YYJXD-5562	Where: https://www.wearefoundingfarmers.com/location/reston/, When: 2022-03-05 00:00
8ZU2ZE-5562	Where: Founding Farmers Resteraunt, When: 2022-03-06 20:00
98A6KL-5561	Where: founding farmers Reston Station, When: 2022-03-05 05:38
9WRPDD-5562	Where: Cita para Cenar en Founding Farmers, When: 2022-03-05 20:00
9ZBF4H-5561	Where: Founding Farmers Reston Station, When: 2022-03-04 08:00
A7BERC-5562	Where: Founding Farmers Reston Station (https://www.wearefoundingfarmers.com/location/reston), When: 2022-03-05 20:00
ARP7Q6-5561	Where: Founding Farmers Restaurant, When: 2022-03-05 20:00
B6WATE-5561	Where: Founding Farmers https://www.wearefoundingfarmers.com/location/reston/, When: 2022-03-05 20:00

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18 - Examination Questions	
WebCode Test	**Response**
B9WHYA-5561	Where: Founding Farmers, When: 2022-03-05 20:00
BN9WG8-5562	Where: www.wearefoundingfarmers.com - restaurant, reston, When: 2022-03-05 20:00
BVR2DE-5562	Where: Founding Farmers https://www.wearefoundingfarmers.com/location/reston/, When: 2022-03-03 20:00
BYPLFC-5562	Where: 1904 Reston Metro Plaza, Reston, VA 20190 from web site https://www.wearefoundingfarmers.com/location/reston/, When: 2022-03-05 20:00
CMTYN8-5561	Where: Founding Farmers Reston, When: 2022-03-05 20:00
CN44V6-5561	Where: Founding Farmers Reston, When: 2022-03-05 20:00
DHRBK7-5562	Where: Founding Farmers Reston (Reston Station Restaurant), When: 2022-03-05 20:00
E7WKY6-5561	Where: founding farmers reston station, When: 2022-05-03 20:00
E7XH9Z-5561	Where: Founding Farmers Restaurant 3/5/2022 20:00 (UTC-05:00), When: 2022-03-05 20:00
EAWU6Z-5561	Where: Founding Farmers Restaurant in Reston, When: 2022-03-05 20:00
EREXP8-5561	Where: Founding Farmers in Reston, VA, When: 2022-03-05 20:00
EX67D8-5562	Where: Founding Farmers in Reston, VA, When: 2022-03-05 20:00
EZEWXB-5561	Where: Founding Farmers Reston Station, When: 2022-03-04 00:00
F2G9Z3-5562	Where: Founding Farmers Reston Station - 1904 Reston Metro Plaza Drive, Reston, VA 20190, United States, When: 2022-03-05 20:00
F8L898-5562	Where: Founding Farmers Reston Station, 1904 RESTON METRO PLAZA, RESTON, VA 20190, When: 2022-03-05 20:00
FGDPP2-5562	Where: Founding Farmers Reston Station, When: 2022-03-05 20:00
FL36D9-5562	Where: We are Founding farmers, Reston, When: 2022-03-05 08:00
FVTQJ7-5562	Where: Founding Farmers Reston Station 1904 Reston Metro Plaza Drive, Reston, VA 20190, United States, When: 2022-05-03 20:00
FXXHAY-5561	Where: Founding Farmers reston, When: 2022-03-05 00:00
G8GC37-5561	Where: Founding Farmers URL: https://www.wearefoundingfarmers.com/location/reston/, When: 2022-03-05 20:00

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18 - Examination Questions	
WebCode Test	**Response**
GCTZYW-5561	Where: Founding Farmers (Reston, VA), When: 2022-03-05 20:00
GFWVHY-5561	Where: Founding Farmers, When: 2022-03-05 20:00
GLX6QD-5562	Where: Founding Farmers Reston Station, When: 2022-03-05 20:00
GR9ZT2-5561	Where: Founding Farmers in Reston, When: 2022-03-04 20:00
HDM36C-5561	Where: Founding Farmers Reston Station, When: 2022-03-05 20:00
HDM9G8-5561	Where: Founding Farmers Reston Station, 1904 RESTON METRO PLAZA, RESTON, VA 20190, When: 2022-03-15 20:00
HEVFPY-5561	Where: Founding Farmers, When: 2022-03-05 20:00
HPTDCY-5561	Where: Founding Farmers Reston Station (https://www.wearefoundingfarmers.com/location/reston/), When: 2022-03-05 20:00
HWZPPY-5562	Where: Founding Farmers Reston Station, When: 2022-03-05 20:00
HX9YL3-5562	Where: Founding Farmers, When: 2022-03-05 20:00
JEDQ2D-5562	Where: https://www.wearefoundingfarmers.com/location/reston/, When: 2022-03-05 20:00
JQ84YN-5561	Where: Founding Farmers, When: 2022-03-05 20:00
K4BTM4-5561	Where: A restaraunt in Reston, When: 2022-03-05 20:00
K9GN9W-5561	Where: Founding Farmers, When: 2022-03-05 20:00
KA2332-5562	Where: We Are founding farmers, When: 2022-03-05 20:00
KDZDY2-5561	Where: Founding Farmers at Reston, When: 2022-03-05 20:00
LTKL96-5562	Where: https://www.wearefoundingfarmers.com/location/reston/, When: 2022-03-05 20:00
LYVGBT-5561	Where: Founding Farmers Reston, When: 2022-03-05 20:00
MW334U-5561	Where: Founding Farmers Restaurant, When: 2022-03-05 20:00
PPRVBV-5561	Where: Founding Farmers Reston Station, When: 2022-03-05 20:00
PPUJUU-5561	Where: Founding Farmers Reston Station, When: 2022-03-05 20:00

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18 - Examination Questions	
WebCode Test	**Response**
PQ9R3V-5561	Where: Founding Farmers, When: 2022-03-05 20:00
PRHXH6-5562	Where: Reston Station Restaurant, When: 2022-03-05 20:00
PTTY3H-5562	Where: Founding Farmers Reston Station, When: 2022-03-05 20:00
PV4KAY-5561	Where: Founding Farmers Restaurant/Reston Station/1904 Reston Metro Plaza Drive, Reston, VA 20190, When: 2022-03-05 20:00
PZAFUR-5562	Where: Founding Farmers Reston Station Restaurant, 1904 Reston Metro Plaza, Reston, VA 20190, When: 2022-03-05 20:00
Q8PGRF-5561	Where: Founding Farmers Reston Station, 1904 Reston Metro Plaza, Reston, VA 20190 USA, When: 2022-03-05 20:00
QKG3YW-5562	Where: we are founding farmers in reston, When: 2022-03-05 20:00
QLMMJQ-5561	Where: Founding Farmers Reston Station, When: 2022-03-05 20:00
QQ3XWU-5561	Where: Founding Farmers Reston Station, When: 2022-03-05 20:00
QVYKR4-5562	Where: 'We are Founding Fathers' at Reston, When: 2022-03-05 20:00
R8KDG3-5562	Where: Founding Farmers Restaurant, When: 2022-03-05 20:00
RFWD9R-5562	Where: Founding Farmers, Reston VA, When: 2022-03-04
RNVVQP-5561	Where: FOUNDING FARMERS (Restaurant) RESTON STATION, 1904 RESTON METRO PLAZA, RESTON, VA 20190, When: 2022-03-05 20:00
T4JR6P-5562	Where: The restaurant “Foundig Farmers”, When: 2022-03-05 20:00
TA98UW-5561	Where: Founding Farmers Reston Station 1904 Reston Metro Plaza Drive, Reston, VA 20190, When: 2022-03-05 20:00
TE2AXW-5561	Where: Founding Farmers Reston Station, When: 2022-03-05 20:00
TWHDG3-5561	Where: https://www.wearefoundingfarmers.com/location/reston/, When: 2022-02-28 20:36
URL94P-5562	Where: Founding Farmers Restaurant Reston, When: 2022-03-04 00:00
VKGWHC-5561	Where: Founding Farmers Reston (Reston Station Restaurant), When: 2022-03-05 20:00
VRFDXN-5561	Where: FoundingFarmer Reston Station Restaurant Lunch&Dinner Menu, When: 2022-03-05 20:00

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18 - Examination Questions	
WebCode Test	**Response**
VU4RLY-5562	Where: Wearefoundingfarmers.com/location/reston, When: 2022-03-05 00:00
WB6WLF-5561	Where: we are founding farmers, When: 2022-03-05 20:00
WRDQDP-5562	Where: Founding Farmers Reston from https://www.wearefoundingfarmers.com/location/reston/, When: 2022-03-06 01:00
WXJKCR-5562	Where: We Are Founding Farmers, Reston, When: 2022-03-05 20:00
X7U2JR-5561	Where: Founding Farmers https://www.wearefoundingfarmers.com/location/reston/, When: 2022-03-05 20:00
XB3L8N-5562	Where: Founding Farmers Reston Station 1904 Reston Metro Plaza Drive, Reston, VA 20190, When: 2022-03-05 20:00
XGEEHM-5561	Where: Founding Farmers, When: 2022-03-05 08:00
Y4WCCF-5561	Where: Founding Farmers Reston Station, When: 2022-03-06 01:00
YDMVRA-5562	[Participant did not return results for this question.]
YE4XXP-5561	Where: Founding Farmers, When: 2022-03-05 20:00
YL2H7J-5562	Where: Founding Farmers (1904 RESTON METRO PLAZA, RESTON, VA 20190)., When: 2022-03-05 20:00
YLG7ZJ-5562	Where: We are founding farmers, When: 2022-03-05 20:00
ZD74EJ-5561	Where: https://www.wearefoundingfarmers.com/location/reston/, When: 2022-03-05 08:00
ZDHVAK-5562	Where: Founding Farmers Reston, When: 2022-03-05 20:00
ZG7AXV-5561	Where: Founding Farmers restaurant, When: 2022-03-05 20:00
ZLZ4XH-5561	Where: https://www.wearefoundingfarmers.com/location/reston/, When: 2022-03-05 20:00

Question 18: Where and when did Jessie ultimately agree to meet the person from the response for question 17?

Consensus Result:

Where: Founding Farmers Reston
When: 2022-03-05 20:00

Expected Response Explanation:

Email files on this computer are stored in C:\Users\Jessie Jenkins\AppData\Roaming\Thunderbird\Profiles\1uql4331.default-release\ImapMail\imap.gmail.com\. Following the message thread between Alex Andersen and Jessie Jenkins finds the relevant last message and the agreement to meet at Founding Farmers Reston on March 5, 2022 at 20:00 (8:00 pm).

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18 - Examination Questions

Expected Response Illustration:

EnCase view of email message

From Alex Andersen <alwaysalexandersen@gmail.com>
To Jessie Jenkins <jessiejenkins909@gmail.com>
Sent 03/05/2022 17:38:52 (-5:00 Eastern Standard Time)
Subject Re: Hey

i'm so sorry (i'll explain why i had to cance). yes. we're on. i'll meet you there at 8.

On Sat, Mar 5, 2022 at 5:36 PM Jessie Jenkins <jessiejenkins909@gmail.com [mailto:jessiejenkins909@gmail.com] > wrote:

are we on for tonight or are you gonna cancel again. 10s don't get left on 'read'

On 2/28/2022 8:38 PM, Alex Andersen wrote:
k i'll call you :)

On Mon, Feb 28, 2022 at 8:37 PM Jessie Jenkins <jessiejenkins909@gmail.com [mailto:jessiejenkins909@gmail.com] > wrote:

(571) 302-4357 ;)
On 2/28/2022 8:37 PM, Alex Andersen wrote:
ok. that sounds fun. i'll make a reservation. what's your mobile number?

On Mon, Feb 28, 2022 at 8:36 PM Jessie Jenkins <jessiejenkins909@gmail.com [mailto:jessiejenkins909@gmail.com] > wrote:

lol. how about a nice dinner out?
like

https://www.wearefoundingfarmers.com/location/reston/ [https://www.wearefoundingfarmers.com/location/reston/]

On 2/28/2022 8:34 PM, Alex Andersen wrote:
hmmmm your place? friday?

On Sun, Feb 27, 2022 at 6:04 PM Jessie Jenkins <jessiejenkins909@gmail.com [mailto:jessiejenkins909@gmail.com] > wrote:
It was great meeting you too!
I'd love to get together again.
Pick a place?

On Sat, Feb 26, 2022 at 5:39 PM Alex Andersen <alwaysalexandersen@gmail.com [mailto:alwaysalexandersen@gmail.com] > wrote:

I hope I got the email right... much of what i remember from last night is a blur... What's not a blur is meeting you! I've never stayed up till dawn talking with someone like that!! What a night! I hope we can do it again soon!
-A

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 19 - Examination Questions

Question 19: According to the Windows Event Logs, what comment was given for the computer shutdown on 2/25/22 3:29 AM (UTC+0)?

Manufacturer's Expected Response: time for bed

WebCode Test	Response ** Inconsistencies not highlighted; No consensus achieved **
2GYK6H-5562	time for bed
37HZM7-5561	time for bed
3ERMDL-5562	time for bed
3J2MUJ-5561	time for bed
3W8X27-5561	time for bed
4ELR7K-5562	time for bed
6GRCUL-5562	The kernel power manager has initiated a shutdown transition
6XRJND-5562	remotely
7CPVTB-5561	The event logging service has shut down. Event ID 1100 "Service shutdown"
8PW7XC-5562	time for bed
8YYJXD-5562	The operating system is shutting down.
8ZU2ZE-5562	time for bed
98A6KL-5561	time for bed
9WRPDD-5562	Cierre de sesión de escritorio remoto exitoso
9ZBF4H-5561	The operating system is shutting down.
A7BERC-5562	The operating system is shutting down. Event ID 13
ARP7Q6-5561	time for bed
B6WATE-5561	time for bed
B9WHYA-5561	time for bed

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 **
BN9WG8-5562	109 - The kernel power manager has initiated a shut down 13 - The operating system is shutting down	
BVR2DE-5562	time for bed	
BYPLFC-5562	The kernel power manager has initiated a shutdown transition.	
CMTYN8-5561	time for bed	
CN44V6-5561	time for bed	
DHRBK7-5562	The operating system is shutting down.	
E7WKY6-5561	time for bed	
E7XH9Z-5561	time for bed	
EAWU6Z-5561	time for bed	
EREXP8-5561	time for bed	
EX67D8-5562	time for bed	
EZEWXB-5561	time for bed	
F2G9Z3-5562	Group Policy received Preshutdown notification from Service Control Manager	
F8L898-5562	Time for bed	
FGDPP2-5562	time for bed	
FL36D9-5562	User initiated logoff	
FVTQJ7-5562	time for bed	
FXXHAY-5561	User Initiated Log Off	
G8GC37-5561	Time for bed	
GCTZYW-5561	Successfully scheduled Software Protection service for re-start at 2122-02-01T03:29:16Z. Reason: RulesEngine.	
GFWVHY-5561	Time for bed.	

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 **
GLX6QD-5562	time for bed	
GR9ZT2-5561	The operating system is shutting down.	
HDM36C-5561	time for bed	
HDM9G8-5561	time for bed	
HEVFPY-5561	time for bed	
HPTDCY-5561	time for bed	
HWZPPY-5562	time for bed	
HX9YL3-5562	time for bed	
JEDQ2D-5562	The operating system is shutting down	
JQ84YN-5561	According to Microsoft Event Viewer- the event properties read: The operating system is shutting down at system time 2022-02-25T03:29:57.197741900Z. i consider this a 'comment' by the definition of the word: a piece of specially tagged explanatory text within (a program) to assist other users.	
K4BTM4-5561	The operating system is shutting down.	
K9GN9W-5561	time for bed	
KA2332-5562	time for bed	
KDZDY2-5561	time for bed	
LTKL96-5562	time for bed	
LYVGBT-5561	User Initiated Log Off	
MW334U-5561	time for bed	
PPRVBV-5561	time for bed	
PPUJUU-5561	time for bed	
PQ9R3V-5561	time for bed	

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 **
PRHXH6-5562	time for bed	
PTTY3H-5562	time for bed	
PV4KAY-5561	User-initiated logoff. Name="TargetUserSid">S-1-5-21-3501254099-4204809888-2000606956-1002 Name=User Name>Jessie Jenkins	
PZAFUR-5562	User Initiated Logoff	
Q8PGRF-5561	time for bed	
QKG3YW-5562	The kernel power manager has initiated a shutdown transition	
QLMMJQ-5561	Time for Bed	
QQ3XWU-5561	time for bed	
QVYKR4-5562	The operating system is shutting down.	
R8KDG3-5562	time for bed	
RFWD9R-5562	time for bed	
RNVVQP-5561	time for bed	
T4JR6P-5562	time for bed (event 2607)	
TA98UW-5561	"No title for this reason could be found (<Data Name=""param1"">C:\Windows\system32\shutdown.exe (DESKTOP-RNO1O54)</Data> <Data Name=""param2"">DESKTOP-RNO1O54</Data> <Data Name=""param3"">No title for this reason could be found</Data> <Data Name=""param4"">0x800000ff</Data> <Data Name=""param5"">shutdown</Data> <Data Name=""param6"">time for bed</Data> <Data Name=""param7"">DESKTOP-RNO1O54\Jessie Jenkins</Data>)"	
TE2AXW-5561	time for bed	
TWHDG3-5561	This event is written when an application causes the system to restart, or when the user initiates a restart or shutdown by clicking Start or pressing CTRL+ALT+DELETE, and then clicking Shut Down.	
URL94P-5562	The kernel power manager has initiated a shutdown transition	
VKGWHC-5561	time for bed	
VRFDXN-5561	time for bed	

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 **
VU4RLY-5562	20:00:00 Saturday 5th March 2022	
WB6WLF-5561	User initiated logoff	
WRDQDP-5562	time for bed	
WXJKCR-5562	The operating system is shutting down.	
X7U2JR-5561	time for bed	
XB3L8N-5562	"No title for this reason could be found (<Data Name=""param1"">C:\Windows\system32\shutdown.exe (DESKTOP-RNO1O54)</Data> <Data Name=""param2"">DESKTOP-RNO1O54</Data> <Data Name=""param3"">No title for this reason could be found</Data> <Data Name=""param4"">0x800000ff</Data> <Data Name=""param5"">shutdown</Data> <Data Name=""param6"">time for bed</Data> <Data Name=""param7"">DESKTOP-RNO1O54\Jessie Jenkins</Data>)"	
XGEEHM-5561	The operating system is shutting down.	
Y4WCCF-5561	time for bed	
YDMVRA-5562	[Participant did not return results for this question.]	
YE4XXP-5561	The operating system is shutting down.	
YL2H7J-5562	User initiated logoff	
YLG7ZJ-5562	The Event log service was stopped	
ZD74EJ-5561	The operating system is shutting down.	
ZDHVAK-5562	time for bed	
ZG7AXV-5561	time for bed	
ZLZ4XH-5561	time for bed	

Question 19: According to the Windows Event Logs, what comment was given for the computer shutdown on 2/25/22 3:29 AM (UTC+0)?

Consensus Result:

While a majority of participants reported the expected response of "time for bed," a consensus was not achieved. Another 20% of participants reported "The operating system is shutting down."

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

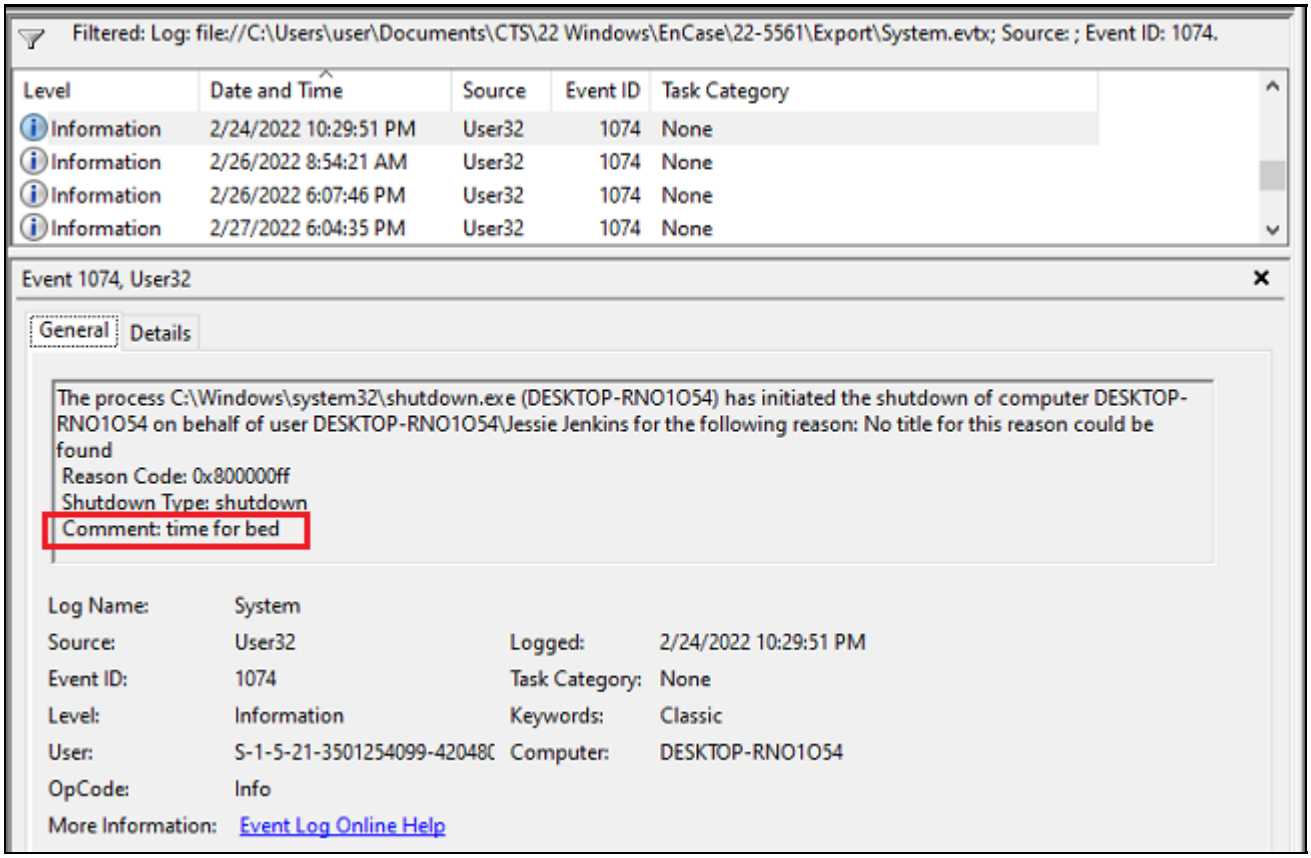
Question 19 - Examination Questions

Expected Response Explanation:

Records of shutdown events are stored in the Windows System Event Log at C:\Windows\System32\winevt\Logs\System.evtx. Parsing this file with Windows event viewer or an appropriate forensic tool, filtering by event ID 1074 and searching for the event on 2/25/22 3:29 AM (UTC) finds the record containing the comment "time for bed."

Expected Response Illustration:

Windows Event Viewer view of shutdown event with comment



Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20 - Examination Questions

Question 20: 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 picker to select the date and time (24-hour).

Manufacturer's Expected Response: Date & Time: 2022-03-06 05:07
User Account: Jessie Jenkins

WebCode Test	Response
2GYK6H-5562	Date and Time: 2022-03-06 05:07, User Account: 1002 Jessie Jenkins
37HZM7-5561	Date and Time: 2022-03-06 05:07, User Account: Jesse Jenkins
3ERMDL-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
3J2MUJ-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
3W8X27-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
4ELR7K-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
6GRCUL-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
6XRJND-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
7CPVTB-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
8PW7XC-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
8YYJXD-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
8ZU2ZE-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
98A6KL-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
9WRPDD-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
9ZBF4H-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
A7BERC-5562	Date and Time: 2022-03-07 05:07, User Account: Jessie Jenkins
ARP7Q6-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
B6WATE-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20 - Examination Questions	
WebCode Test	**Response**
B9WHYA-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
BN9WG8-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
BVR2DE-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
BYPLFC-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins, S-1-5-21-3501254099-4204809888-2000606956-1002
CMTYN8-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins (user ID 1002)
CN44V6-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
DHRBK7-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
E7WKY6-5561	Date and Time: 2022-03-06 05:07, User Account: 1002 Jessie Jenkins
E7XH9Z-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
EAWU6Z-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
EREXP8-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
EX67D8-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
EZEWXB-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
F2G9Z3-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
F8L898-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
FGDPP2-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
FL36D9-5562	Date and Time: 2022-03-06 05:07, User Account: Jessi Jenkins
FVTQJ7-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins (S-1-5-21-3501254099-4204809888-2000606956-1002)
FXXHAY-5561	Date and Time: 2022-03-06 05:12, User Account: Jessie Jenkins
G8GC37-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
GCTZYW-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20 - Examination Questions	
WebCode Test	**Response**
GFWVHY-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
GLX6QD-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
GR9ZT2-5561	Date and Time: 2022-06-06 05:07, User Account: Jesse Jenkins
HDM36C-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
HDM9G8-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
HEVFPY-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
HPTDCY-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
HWZPPY-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
HX9YL3-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
JEDQ2D-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
JQ84YN-5561	Date and Time: 2022-03-05 23:12, User Account: Jessie Jenkins
K4BTM4-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
K9GN9W-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
KA2332-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
KDZDY2-5561	Date and Time: 2022-02-06 05:07, User Account: Jessie Jenkins
LTKL96-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
LYVGBT-5561	Date and Time: 2022-03-06 05:12, User Account: Jessie Jenkins
MW334U-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
PPRVBV-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
PPUJUU-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20 - Examination Questions	
WebCode Test	**Response**
PQ9R3V-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
PRHXH6-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
PTTY3H-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
PV4KAY-5561	Date and Time: 2022-03-06 05:12, User Account: S-1-5-18 SYSTEM
PZAFUR-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
Q8PGRF-5561	Date and Time: 2022-03-06 05:07, User Account: 1002 (Jessie Jenkins)
QKG3YW-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
QLMMJQ-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
QQ3XWU-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
QVYKR4-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie JENKINS
R8KDG3-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
RFWD9R-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
RNVVQP-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
T4JR6P-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
TA98UW-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
TE2AXW-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
TWHDG3-5561	Date and Time: 2022-03-06 19:07, User Account: Jessie Jenkins
URL94P-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
VKGWHC-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
VRFDXN-5561	Date and Time: 2022-03-06 05:12, User Account: S-1-5-18 Systemprofile
VU4RLY-5562	Date and Time: 2022-03-06 05:07, User Account: jessie jenkins

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20 - Examination Questions	
WebCode Test	**Response**
WB6WLF-5561	Date and Time: 2022-03-06 05:12, User Account: S-1-5-21-3501254099-4204809888-2000606956-1002 Jessie Jenkins
WRDQDP-5562	Date and Time: 2022-03-06 05:05:26.9 UTC, User Account: Jessie Jenkins
WXJKCR-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
X7U2JR-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
XB3L8N-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
XGEEHM-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
Y4WCCF-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
YDMVRA-5562	[Participant did not return results for this question.]
YE4XXP-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
YL2H7J-5562	Date and Time: 2022-03-06 05:12, User Account: Jessie Jenkins
YLG7ZJ-5562	Date and Time: 2022-03-06 05:07, User Account: .\Jessie Jenkins
ZD74EJ-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
ZDHVAK-5562	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins (user ID 1002)
ZG7AXV-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins
ZLZ4XH-5561	Date and Time: 2022-03-06 05:07, User Account: Jessie Jenkins

Question 20: 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 picker to select the date and time (24-hour).

Consensus Result:

Date & Time: 2022-03-06 05:07
User Account: Jessie Jenkins

Expected Response Explanation:

Records of logon 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 logon type 2 will show the last successful logon and the target user account. The last login date for a user is also recorded in the System Accounts Manager registry hive.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20 - Examination Questions

Expected Response Illustration:

Evtx Explorer Parse of Security.evtx

TimeCreated	EventId	MapDescription	PayloadData1	PayloadData2	PayloadData3
2022-03-06T05:06:16	4625	Failed logon	Target: DESKTOP-RNO1O54\Jessie Jenkins	LogonType 2	FailureReason: user name is correct but the password is wrong
2022-03-06T05:06:20	4625	Failed logon	Target: DESKTOP-RNO1O54\Jessie Jenkins	LogonType 2	FailureReason: user name is correct but the password is wrong
2022-03-06T05:06:25	4625	Failed logon	Target: DESKTOP-RNO1O54\Jessie Jenkins	LogonType 2	FailureReason: user name is correct but the password is wrong
2022-03-06T05:06:28	4625	Failed logon	Target: DESKTOP-RNO1O54\Jessie Jenkins	LogonType 2	FailureReason: user name is correct but the password is wrong
2022-03-06T05:06:48	4625	Failed logon	Target: DESKTOP-RNO1O54\Jessie Jenkins	LogonType 2	FailureReason: user name is correct but the password is wrong
2022-03-06T05:06:54	4625	Failed logon	Target: DESKTOP-RNO1O54\Jessie Jenkins	LogonType 2	FailureReason: user name is correct but the password is wrong
2022-03-06T05:07:35	4624	Successful logon	Target: DESKTOP-RNO1O54\Jessie Jenkins	LogonType 2	LogonId: 0x116A34

RegRipper view of SAM hive login data for Jessie Jenkins

```
Username        : Jessie Jenkins [1002]
Full Name       :
User Comment    :
Account Type    :
Account Created : 2022-02-02 05:39:49Z
Name            :
Password Hint   : same
Last Login Date : 2022-03-06 05:07:34Z
Pwd Reset Date  : 2022-02-17 01:14:03Z
Pwd Fail Date   : 2022-03-06 05:06:53Z
Login Count     : 59
Embedded RID    : 1002
```

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21 - Examination Questions

Question 21: How many failed logins immediately preceded the successful one in question 20? Provide a NUMERIC response.

Manufacturer's Expected Response: 6

WebCode Test	Response
2GYK6H-5562	6
37HZM7-5561	1
3ERMDL-5562	6
3J2MUJ-5561	6
3W8X27-5561	6
4ELR7K-5562	6
6GRCUL-5562	1
6XRJND-5562	6
7CPVTB-5561	6
8PW7XC-5562	6
8YYJXD-5562	6
8ZU2ZE-5562	1
98A6KL-5561	6
9WRPDD-5562	6
9ZBF4H-5561	59
A7BERC-5562	6
ARP7Q6-5561	6
B6WATE-5561	6
B9WHYA-5561	6

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21 - Examination Questions	
WebCode Test	**Response**
BN9WG8-5562	6
BVR2DE-5562	6
BYPLFC-5562	6
CMTYN8-5561	6
CN44V6-5561	6
DHRBK7-5562	[Participant did not return results for this question.]
E7WKY6-5561	6
E7XH9Z-5561	6
EAWU6Z-5561	6
EREXP8-5561	6
EX67D8-5562	6
EZEWXB-5561	1
F2G9Z3-5562	1
F8L898-5562	6
FGDPP2-5562	06
FL36D9-5562	[Participant did not return results for this question.]
FVTQJ7-5562	6
FXXHAY-5561	1
G8GC37-5561	6
GCTZYW-5561	6
GFWVHY-5561	6

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21 - Examination Questions	
WebCode Test	**Response**
GLX6QD-5562	6
GR9ZT2-5561	0
HDM36C-5561	6
HDM9G8-5561	6
HEVFPY-5561	6
HPTDCY-5561	6
HWZPPY-5562	6
HX9YL3-5562	6
JEDQ2D-5562	6
JQ84YN-5561	6
K4BTM4-5561	1
K9GN9W-5561	6
KA2332-5562	6
KDZDY2-5561	1
LTKL96-5562	6
LYVGBT-5561	1
MW334U-5561	6
PPRVBV-5561	6
PPUJUU-5561	6
PQ9R3V-5561	1
PRHXH6-5562	6

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21 - Examination Questions	
WebCode Test	**Response**
PTTY3H-5562	6
PV4KAY-5561	0
PZAFUR-5562	6
Q8PGRF-5561	6
QKG3YW-5562	2
QLMMJQ-5561	6
QQ3XWU-5561	6
QVYKR4-5562	16
R8KDG3-5562	6
RFWD9R-5562	6
RNVVQP-5561	6
T4JR6P-5562	6
TA98UW-5561	59
TE2AXW-5561	6
TWHDG3-5561	6
URL94P-5562	1
VKGWHC-5561	6
VRFDXN-5561	6
VU4RLY-5562	6
WB6WLF-5561	5
WRDQDP-5562	4

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21 - Examination Questions	
WebCode Test	**Response**
WXJKCR-5562	6
X7U2JR-5561	6
XB3L8N-5562	59
XGEEHM-5561	1
Y4WCCF-5561	6
YDMVRA-5562	[Participant did not return results for this question.]
YE4XXP-5561	6
YL2H7J-5562	6
YLG7ZJ-5562	6
ZD74EJ-5561	6
ZDHVAK-5562	6
ZG7AXV-5561	6
ZLZ4XH-5561	6

Question 21: How many failed logins immediately preceded the successful one in question 20? Provide a NUMERIC response.

Consensus Result:

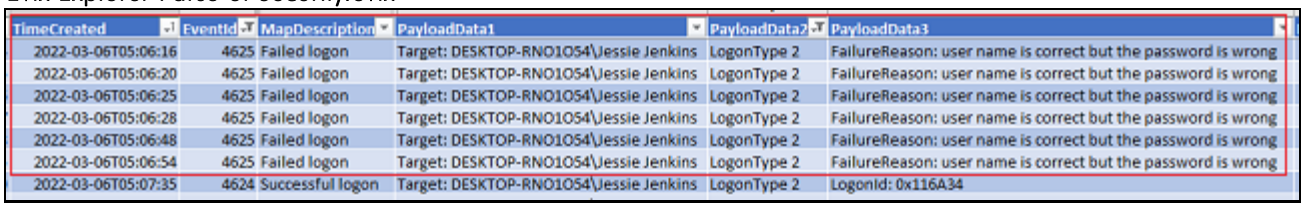
6

Expected Response Explanation:

Records of logon 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 IDs 4624 and 4625, and logon type 2 will show the last successful logon and target user account as well as the preceding failed logins.

Expected Response Illustration:

Evtx Explorer Parse of Security.evtx



TimeCreated	EventId	MapDescription	PayloadData1	PayloadData2	PayloadData3
2022-03-06T05:06:16	4625	Failed logon	Target: DESKTOP-RNO1O54\Jessie Jenkins	LogonType 2	FailureReason: user name is correct but the password is wrong
2022-03-06T05:06:20	4625	Failed logon	Target: DESKTOP-RNO1O54\Jessie Jenkins	LogonType 2	FailureReason: user name is correct but the password is wrong
2022-03-06T05:06:25	4625	Failed logon	Target: DESKTOP-RNO1O54\Jessie Jenkins	LogonType 2	FailureReason: user name is correct but the password is wrong
2022-03-06T05:06:28	4625	Failed logon	Target: DESKTOP-RNO1O54\Jessie Jenkins	LogonType 2	FailureReason: user name is correct but the password is wrong
2022-03-06T05:06:48	4625	Failed logon	Target: DESKTOP-RNO1O54\Jessie Jenkins	LogonType 2	FailureReason: user name is correct but the password is wrong
2022-03-06T05:06:54	4625	Failed logon	Target: DESKTOP-RNO1O54\Jessie Jenkins	LogonType 2	FailureReason: user name is correct but the password is wrong
2022-03-06T05:07:35	4624	Successful logon	Target: DESKTOP-RNO1O54\Jessie Jenkins	LogonType 2	LogonId: 0x116A34

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22 - Examination Questions

Question 22: How many times was the Electrum program executed (not the installer)? Provide a NUMERIC response.

Manufacturer's Expected Response: 6

WebCode Test	Response
2GYK6H-5562	6
37HZM7-5561	6
3ERMDL-5562	6
3J2MUJ-5561	6
3W8X27-5561	6
4ELR7K-5562	6
6GRCUL-5562	6
6XRJND-5562	6
7CPVTB-5561	6
8PW7XC-5562	6
8YYJXD-5562	12
8ZU2ZE-5562	6
98A6KL-5561	6
9WRPDD-5562	6
9ZBF4H-5561	6
A7BERC-5562	6
ARP7Q6-5561	6
B6WATE-5561	6
B9WHYA-5561	6

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22 - Examination Questions	
WebCode Test	**Response**
BN9WG8-5562	6
BVR2DE-5562	6
BYPLFC-5562	4
CMTYN8-5561	6
CN44V6-5561	6
DHRBK7-5562	[Participant did not return results for this question.]
E7WKY6-5561	6
E7XH9Z-5561	6
EAWU6Z-5561	6
EREXP8-5561	6
EX67D8-5562	6
EZEWXB-5561	6
F2G9Z3-5562	6
F8L898-5562	6
FGDPP2-5562	04
FL36D9-5562	6
FVTQJ7-5562	6
FXXHAY-5561	6
G8GC37-5561	6
GCTZYW-5561	6
GFWVHY-5561	6

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22 - Examination Questions	
WebCode Test	**Response**
GLX6QD-5562	6
GR9ZT2-5561	6
HDM36C-5561	6
HDM9G8-5561	6
HEVFPY-5561	11
HPTDCY-5561	6
HWZPPY-5562	6
HX9YL3-5562	6
JEDQ2D-5562	4
JQ84YN-5561	6
K4BTM4-5561	3
K9GN9W-5561	6
KA2332-5562	6
KDZDY2-5561	1
LTKL96-5562	11
LYVGBT-5561	6
MW334U-5561	11
PPRVBV-5561	6
PPUJUU-5561	6
PQ9R3V-5561	6
PRHXH6-5562	6

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22 - Examination Questions	
WebCode Test	**Response**
PTTY3H-5562	6
PV4KAY-5561	6
PZAFUR-5562	6
Q8PGRF-5561	6
QKG3YW-5562	6
QLMMJQ-5561	6
QQ3XWU-5561	6
QVYKR4-5562	6
R8KDG3-5562	6
RFWD9R-5562	6
RNVVQP-5561	6
T4JR6P-5562	6
TA98UW-5561	6
TE2AXW-5561	6
TWHDG3-5561	11
URL94P-5562	6
VKGWHC-5561	6
VRFDXN-5561	6
VU4RLY-5562	6
WB6WLF-5561	6
WRDQDP-5562	6

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22 - Examination Questions	
WebCode Test	**Response**
WXJKCR-5562	6
X7U2JR-5561	6
XB3L8N-5562	6
XGEEHM-5561	6
Y4WCCF-5561	6
YDMVRA-5562	[Participant did not return results for this question.]
YE4XXP-5561	6
YL2H7J-5562	6
YLG7ZJ-5562	6
ZD74EJ-5561	12
ZDHVAK-5562	6
ZG7AXV-5561	6
ZLZ4XH-5561	11

Question 22: How many times was the Electrum program executed (not the installer)? Provide a NUMERIC response.

Consensus Result:

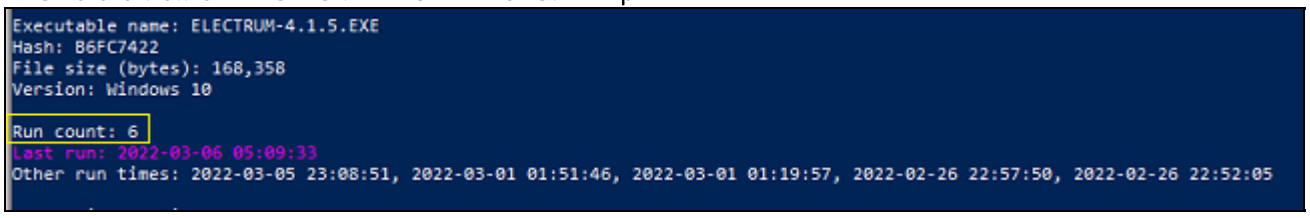
6

Expected Response Explanation:

Prefetch analysis is used to determine program execution details. There is one prefetch file for ELECTRUM-4.1.5.EXE in C:\Windows\Prefetch\ELECTRUM-4.1.5.EXE-B6FC7422.pf. Analysis of this file with PECmd (Prefetch Explorer Cmd) or the PFDump EnScript for EnCase indicates ELECTRUM-4.1.5.EXE was executed 6 times.

Expected Response Illustration:

PECmd.exe view of ELECTRUM-4.1.5.EXE-B6FC7422.pf



Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22 - Examination Questions

EnScript view of ELECTRUM-4.1.5.EXE-B6FC7422.pf

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23 - Examination Questions

Question 23: What is the original (pre-deletion) path and name of $IBB0QWJ.doc (found in the user Jessie Jenkins' Recycle Bin)?

Manufacturer's Expected Response: C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc

WebCode Test	Response
2GYK6H-5562	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
37HZM7-5561	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
3ERMDL-5562	Path: C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc Name: AmusedWearyQuetzal.doc
3J2MUJ-5561	Path: C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc Filename: AmusedWearyQuetzal
3W8X27-5561	c:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
4ELR7K-5562	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
6GRCUL-5562	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
6XRJND-5562	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
7CPVTB-5561	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
8PW7XC-5562	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
8YYJXD-5562	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc.
8ZU2ZE-5562	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
98A6KL-5561	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
9WRPDD-5562	AmusedWearyQuetzal.doc
9ZBF4H-5561	OriginalPath: C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc OriginalName: AmusedWearyQuetzal.doc
A7BERC-5562	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc AmusedWearyQuetzal.doc
ARP7Q6-5561	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
B6WATE-5561	Path: C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc Name: AmusedWearyQuetzal.doc
B9WHYA-5561	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23 - Examination Questions	
WebCode Test	**Response**
BN9WG8-5562	Path :- C:\Users\Jessie Jenkins\Documents\AmusedWearyuetzal.doc Name:- AmusedWearyuetzal.doc
BVR2DE-5562	Path: C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc / Name: AmusedWearyQuetzal.doc
BYPLFC-5562	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
CMTYN8-5561	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
CN44V6-5561	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
DHRBK7-5562	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
E7WKY6-5561	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
E7XH9Z-5561	\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
EAWU6Z-5561	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
EREXP8-5561	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
EX67D8-5562	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
EZEWXB-5561	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
F2G9Z3-5562	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
F8L898-5562	C\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
FGDPP2-5562	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
FL36D9-5562	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
FVTQJ7-5562	\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
FXXHAY-5561	C:\Users\Jessie Jenkins\Documents\AmusedwearyQuetzal.doc
G8GC37-5561	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
GCTZYW-5561	C:\Users\Jesse Jenkins\Documents\AmusedWearyQuetzal.doc
GFWVHY-5561	\root\users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23 - Examination Questions	
WebCode Test	**Response**
GLX6QD-5562	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
GR9ZT2-5561	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
HDM36C-5561	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
HDM9G8-5561	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
HEVFPY-5561	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
HPTDCY-5561	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
HWZPPY-5562	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
HX9YL3-5562	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
JEDQ2D-5562	\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
JQ84YN-5561	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
K4BTM4-5561	AmusedWearyQuetzal.doc
K9GN9W-5561	Path – C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc Name – AmusedWearyQuetzal.doc
KA2332-5562	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
KDZDY2-5561	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
LTKL96-5562	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
LYVGBT-5561	C:\Users\Jessie Jenkins\Documents\AmusedwearyQuetzal.doc
MW334U-5561	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
PPRVBV-5561	root\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
PPUJUU-5561	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
PQ9R3V-5561	C:\\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc; \AmusedWearyQuetzal.doc
PRHXH6-5562	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23 - Examination Questions	
WebCode Test	**Response**
PTTY3H-5562	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
PV4KAY-5561	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
PZAFUR-5562	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
Q8PGRF-5561	path = C:\Users\Jessie Jenkins\Documents; name = AmusedWearyQuetzal.doc
QKG3YW-5562	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
QLMMJQ-5561	\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
QQ3XWU-5561	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
QVYKR4-5562	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
R8KDG3-5562	Partition 2 \\Users\Jessie Jenkins\Documents\AmusedWearQuetzal.doc
RFWD9R-5562	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
RNVVQP-5561	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
T4JR6P-5562	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
TA98UW-5561	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
TE2AXW-5561	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
TWHDG3-5561	PATH : C:\Users\Jessie Jenkins\Documents\ FILE NAEM : AmusedWearyQuetzal.doc
URL94P-5562	C:\Users\jessie Jenkins\Documents\AmusedWearyQuetzal.doc
VKGWHC-5561	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
VRFDXN-5561	D:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
VU4RLY-5562	c:\users\jessie jenkins\desktop\New Folder(2)\S-1-5-2-3501254099-4204809888-2000606956-1002$IBB0QWJ.DOC
WB6WLF-5561	C:\Users\Jessie Jenkins\Jessie Jenkins\Documents\AmusedWearyQuaetzal.doc
WRDQDP-5562	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23 - Examination Questions

WebCode Test	Response
WXJKCR-5562	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc, AmusedWearyQuetzal.doc
X7U2JR-5561	Path: C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc Name: AmusedWearyQuetzal.doc
XB3L8N-5562	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
XGEEHM-5561	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
Y4WCCF-5561	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
YDMVRA-5562	[Participant did not return results for this question.]
YE4XXP-5561	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
YL2H7J-5562	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
YLG7ZJ-5562	Path: C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc Name: AmusedWearyQuetzal.doc
ZD74EJ-5561	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc.
ZDHVAK-5562	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
ZG7AXV-5561	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc
ZLZ4XH-5561	C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc

Question 23: What is the original (pre-deletion) path and name of $IBB0QWJ.doc (found in the user Jessie Jenkins' Recycle Bin)?

Consensus Result:

C:\Users\Jessie Jenkins\Documents\AmusedWearyQuetzal.doc

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 Jessie Jenkins' SID is S-1-5-21-3501254099-4204809888-2000606956-1002. 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.

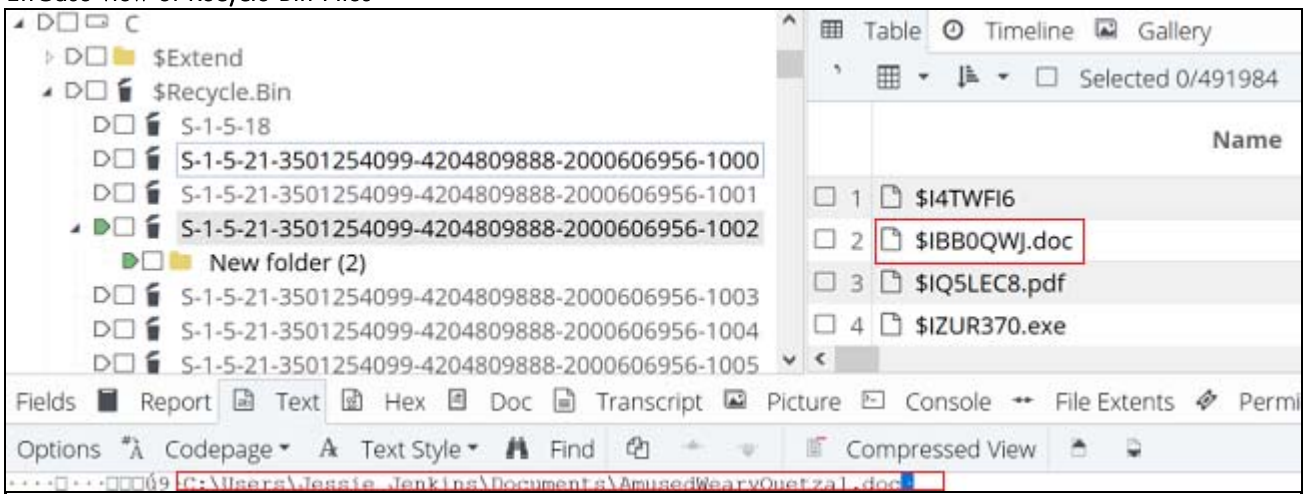
Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23 - Examination Questions

Expected Response Illustration:

EnCase view of Recycle Bin Files



Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions

Question 24: What is the file TYPE for the file with SHA-1 hash 61cf7b3e81a6276e1ae5953fcf09f1e99f5bea78?

Manufacturer's Expected Response: File Type: Portable Network Graphic or PNG

WebCode Test	Response
2GYK6H-5562	File TYPE: PNG, How did you determine the file TYPE?: 0x89504E47 (PNG signature)
37HZM7-5561	File TYPE: png, How did you determine the file TYPE?: Signature analysis
3ERMDL-5562	File TYPE: Picture (Image), How did you determine the file TYPE?: ? From the file extension, which is JPG (find it in the Meta data which is given by the tool that I'm using)
3J2MUJ-5561	File TYPE: .PNG (Portable Network Graphic), How did you determine the file TYPE?: Looked at the hex and Signature Analysis
3W8X27-5561	File TYPE: PNG, How did you determine the file TYPE?: Hex values from the file header
4ELR7K-5562	File TYPE: PNG, How did you determine the file TYPE?: File Header
6GRCUL-5562	File TYPE: PNG, How did you determine the file TYPE?: File header signature
6XRJND-5562	File TYPE: PNG, How did you determine the file TYPE?: hex header / type mismatch
7CPVTB-5561	File TYPE: .JPG, How did you determine the file TYPE?: Using AXIOM, conducted a keyword search for the SHA value
8PW7XC-5562	File TYPE: PNG image, How did you determine the file TYPE?: by File Header
8YYJXD-5562	File TYPE: jpg, How did you determine the file TYPE?: File Header: FF D8 FF
8ZU2ZE-5562	File TYPE: PNG, How did you determine the file TYPE?: File Header 89 50 4E 47 0D 0A 1A 0A following mismatch
98A6KL-5561	File TYPE: Portable Network Graphic (PNG), How did you determine the file TYPE?: Confirmed by file signature, Header : 89 50 4E 47 0D 0A 1A 0A / Footer: 49 45 4E 44 AE 42 60 82
9WRPDD-5562	File TYPE: .png, How did you determine the file TYPE?: Por la cabecera del archivo (89 50 4E 47)
9ZBF4H-5561	File TYPE: png, How did you determine the file TYPE?: File Header
A7BERC-5562	File TYPE: PNG (portable Network Graphic), How did you determine the file TYPE?: Signature Analysis 89 50 4E 47
ARP7Q6-5561	File TYPE: .PNG, How did you determine the file TYPE?: Found the file and examined the header information of the file

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions	
WebCode Test	**Response**
B6WATE-5561	File TYPE: Picture (Image), How did you determine the file TYPE?: From the file extension, which is JPG (find it in the Meta data which is given by the tool that I'm using)
B9WHYA-5561	File TYPE: PNG, How did you determine the file TYPE?: From the HEX
BN9WG8-5562	File TYPE: PNG, How did you determine the file TYPE?: Looked at the file header
BVR2DE-5562	File TYPE: Picture (Image), How did you determine the file TYPE?: From the file extension, which is JPG (find it in the Meta data which is given by the tool that I'm using)
BYPLFC-5562	File TYPE: .png, How did you determine the file TYPE?: Viewed the Hex for the file header ie 89 50 4E
CMTYN8-5561	File TYPE: .png, How did you determine the file TYPE?: 1. Observed file signature in hex viewer. 2. Used X-Ways Forensics and verified file types in Refine Volume Snapshot
CN44V6-5561	File TYPE: PNG, How did you determine the file TYPE?: File header
DHRBK7-5562	File TYPE: PNG, How did you determine the file TYPE?: We look at the file signature (header information) to determine the file type.
E7WKY6-5561	File TYPE: PNG, How did you determine the file TYPE?: 0x89504E47 (PNG signature)
E7XH9Z-5561	File TYPE: PNG picture, How did you determine the file TYPE?: the file header
EAWU6Z-5561	File TYPE: .png, How did you determine the file TYPE?: Looking at the first 4 bytes of the file header (89 50 4E 47)
EREXP8-5561	File TYPE: .PNG, How did you determine the file TYPE?: hex file header, and software listed file type as .png also
EX67D8-5562	File TYPE: .png, How did you determine the file TYPE?: The header of the file: 0x 89 50 4E 47 0D 0A 1A 0A
EZEWXB-5561	File TYPE: PNG, How did you determine the file TYPE?: Reviewed the HEX. The file signature and ASCII indicated that it was a PNG file.
F2G9Z3-5562	File TYPE: .PNG, How did you determine the file TYPE?: File header is 89 50 4e 47 which is the file header for .png files
F8L898-5562	File TYPE: .PNG, How did you determine the file TYPE?: Ran file signature analysis over the file. Checked the hexadecimal of the file header.
FGDPP2-5562	File TYPE: PNG, How did you determine the file TYPE?: File Header / Signature
FL36D9-5562	File TYPE: .PNG, How did you determine the file TYPE?: Searched on SHA-1 and view hex of file.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions	
WebCode Test	**Response**
FVTQJ7-5562	File TYPE: png, How did you determine the file TYPE?: Identified the file signature (89 50 4E 47 0D 0A 1A 0A) for png using the hex viewer
FXXHAY-5561	File TYPE: PNG, How did you determine the file TYPE?: File header
G8GC37-5561	File TYPE: PNG, How did you determine the file TYPE?: File signature mismatch, the header was parsed, header mismatch for JPG. File name is LockScreen___3840_2160_notdimmed.jpg but header for file in hex is '%PNG'.
GCTZYW-5561	File TYPE: PNG image, How did you determine the file TYPE?: Header shows PNG signature
GFWVHY-5561	File TYPE: png, How did you determine the file TYPE?: checked the file header in HEX
GLX6QD-5562	File TYPE: Image, How did you determine the file TYPE?: Signature Analysis
GR9ZT2-5561	File TYPE: PNG, How did you determine the file TYPE?: The file header is 0x89504E47 which in ASCII is PNG
HDM36C-5561	File TYPE: Image, How did you determine the file TYPE?: signature analysis
HDM9G8-5561	File TYPE: PNG image file, How did you determine the file TYPE?: Reviewed file in a hex viewer and noted first 8 bytes were 89 50 4E 47 0D 0A 1A 0A, which is the file signature of a PNG file.
HEVFPY-5561	File TYPE: .PNG, How did you determine the file TYPE?: File Header
HPTDCY-5561	File TYPE: PNG (Portable Network Graphic), How did you determine the file TYPE?: Hex Code - 0x89504e47
HWZPPY-5562	File TYPE: PNG, How did you determine the file TYPE?: File header information
HX9YL3-5562	File TYPE: .PNG, How did you determine the file TYPE?: Reviewing the hex for the file, the header showed .PNG.
JEDQ2D-5562	File TYPE: displayed as .jpg - header indicates a .png file (.PNG), How did you determine the file TYPE?: examination of HEX data associated with the file
JQ84YN-5561	File TYPE: JPEG, How did you determine the file TYPE?: its a .jpg file extension and that is associated with the JPEG file type…
K4BTM4-5561	File TYPE: PNG, How did you determine the file TYPE?: Looking at the header in the HEX viewer
K9GN9W-5561	File TYPE: PNG, How did you determine the file TYPE?: Looked at the properties of the file and looked at the file in hex view.
KA2332-5562	File TYPE: .PNG, How did you determine the file TYPE?: The file signature is for PNG
KDZDY2-5561	File TYPE: Picture, How did you determine the file TYPE?: By file name, content and extension

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions

WebCode Test	Response
LTKL96-5562	File TYPE: .PNG, How did you determine the file TYPE?: File signature
LYVGBT-5561	File TYPE: PNG, How did you determine the file TYPE?: file header
MW334U-5561	File TYPE: PNG, How did you determine the file TYPE?: File Header
PPRVBV-5561	File TYPE: PNG, How did you determine the file TYPE?: File Header
PPUJUU-5561	File TYPE: PNG, How did you determine the file TYPE?: The file signature of this file is PNG.
PQ9R3V-5561	File TYPE: PNG, How did you determine the file TYPE?: opened in Note Pad and looked at header
PRHXH6-5562	File TYPE: PNG, How did you determine the file TYPE?: Checked the header of the file which showed 'PNG'
PTTY3H-5562	File TYPE: PNG, How did you determine the file TYPE?: File's header corresponding to a PNG file: 0x89 50 4e 47 0d 0a 1a 0a
PV4KAY-5561	File TYPE: .PNG (Portable Network Graphic), How did you determine the file TYPE?: File has .png extension and 8-byte file signature: 89 50 4E 47 0D 0A 1A 0A
PZAFUR-5562	File TYPE: Portable Network Graphic, How did you determine the file TYPE?: Signature Analysis
Q8PGRF-5561	File TYPE: png, How did you determine the file TYPE?: The file header starts : 0x 89 50 4E 47 (in ASCII, 0x 50 4E 47 displays as PNG)
QKG3YW-5562	File TYPE: PNG, How did you determine the file TYPE?: Viewing the header of the file, the header for a PNG file is ‰PNG
QLMMJQ-5561	File TYPE: PNG, How did you determine the file TYPE?: file header
QQ3XWU-5561	File TYPE: PNG, How did you determine the file TYPE?: File Signature
QVYKR4-5562	File TYPE: image file [Defined in HEX as .png], How did you determine the file TYPE?: Defined in HEX as .png (Portable Network Graphic)
R8KDG3-5562	File TYPE: Picture (.png), How did you determine the file TYPE?: file signature analysis (mismatch detected)
RFWD9R-5562	File TYPE: PNG, How did you determine the file TYPE?: For the file signature (0x89504E470D)
RNVVQP-5561	File TYPE: Portable network graphics (PNG) file, How did you determine the file TYPE?: Examination of file signature
T4JR6P-5562	File TYPE: png image, How did you determine the file TYPE?: Viewing the file header (89 50 4E 47) in hexadecimal

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions	
WebCode Test	**Response**
TA98UW-5561	File TYPE: PNG, How did you determine the file TYPE?: JPG Signature(Header): FF D8 FF E0(E8) Signature(Foot): FF D9 but this picture's signature(Header): 89 50 4E 47 0D 0A 1A 0A Signature(Footer): 49 45 4E 44 AE 42 60 82. This signature means PNG
TE2AXW-5561	File TYPE: PNG, How did you determine the file TYPE?: HEX signature is 89 50 4E 47
TWHDG3-5561	File TYPE: Portable Network Graphic, How did you determine the file TYPE?: Picture, jpg
URL94P-5562	File TYPE: .png, How did you determine the file TYPE?: File Header x89 x50 x4E x47
VKGWHC-5561	File TYPE: PNG (Portable Network Graphics File), How did you determine the file TYPE?: File type was determined by the file header (89 50 4E 47).
VRFDXN-5561	File TYPE: Picture .jpg, How did you determine the file TYPE?: When I was checking and I was finding the SHA-1 I found the file and file type.
VU4RLY-5562	File TYPE: JPEG Image file, How did you determine the file TYPE?: Analysis software identified file, or could have used file header within the file itself
WB6WLF-5561	File TYPE: .png, How did you determine the file TYPE?: File header. Hex is 50 4E 47
WRDQDP-5562	File TYPE: PNG, How did you determine the file TYPE?: Utilizing a digital forensic program's category type then verifying it using a program which determine file type by three sets of tests, performed in this order: filesystem tests, magic tests (/usr/share/misc/magic.mgc){which includes file signature matches}, and language tests.
WXJKCR-5562	File TYPE: PNG, How did you determine the file TYPE?: X-Ways type column, checked header in Hex viewer (‰PNG)
X7U2JR-5561	File TYPE: Picture (Image), How did you determine the file TYPE?: From the file extension, which is JPG (find it in the Meta data which is given by the tool that I'm using)
XB3L8N-5562	File TYPE: PNG, How did you determine the file TYPE?: JPG Signature(Header): FF D8 FF E0(E8) Signature(Foot): FF D9 but this picture's signature(Header): 89 50 4E 47 0D 0A 1A 0A Signature(Footer): 49 45 4E 44 AE 42 60 82. This signature means PNG
XGEEHM-5561	File TYPE: PNG, How did you determine the file TYPE?: I viewed the file in a hex viewer and determined the file type based on its file header.
Y4WCCF-5561	File TYPE: Portable Network Graphics, How did you determine the file TYPE?: Signature Analysis
YDMVRA-5562	[Participant did not return results for this question.]
YE4XXP-5561	File TYPE: PNG, How did you determine the file TYPE?: The header is 89 50 4E 47 0D 0A 1A 0A.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions	
WebCode Test	**Response**
YL2H7J-5562	File TYPE: .png, How did you determine the file TYPE?: File header was 89504E470D0A1A0A0000000D and file footer was 49454E44 (These headers relates to .png file types)
YLG7ZJ-5562	File TYPE: image, How did you determine the file TYPE?: File extension .jpg
ZD74EJ-5561	File TYPE: jpg, How did you determine the file TYPE?: File Header: FF D8 FF
ZDHVAK-5562	File TYPE: .png, How did you determine the file TYPE?: 1. Observed file signature in hex viewer. 2. Used X-Ways Forensics and verified file types in Refine Volume Snapshot
ZG7AXV-5561	File TYPE: PNG, How did you determine the file TYPE?: Although the file extension is shown as .jpg, the file header in hex is actually that of a .png file (89 50 4e)
ZLZ4XH-5561	File TYPE: PNG, How did you determine the file TYPE?: File signature

Question 24: What is the file TYPE for the file with SHA-1 hash 61cf7b3e81a6276e1ae5953fcf09f1e99f5bea78?

Consensus Result:

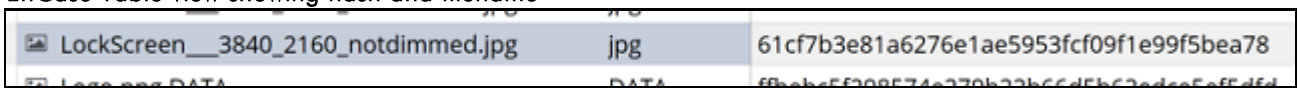
File Type: Portable Network Graphic or PNG

Expected Response Explanation:

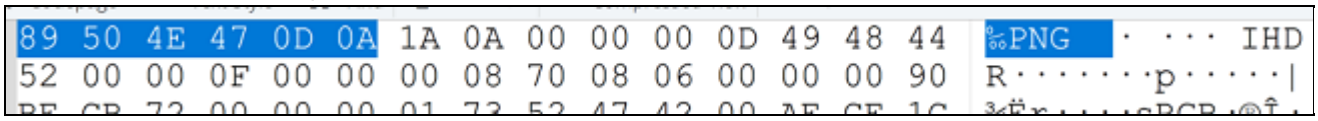
The file can be located with a sorted list of SHA-1 hashes for all files on the device. The file is named LockScreen___3840_2160_notdimmed.jpg as a "Joint Photographic Experts Group" (jpeg) image format file. However, internally it has the 89 50 4E 47 0D 0A (%PNG) header of Portable Network Graphic file.

Expected Response Illustration:

EnCase Table view showing hash and filename



EnCase Hex view showing file header



Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions

LockScreen___3840_2160_notdimmed.jpg

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25 - Examination Questions

Question 25: What is the $FILE_NAME Attribute created date and time for PoorFairJaguar.html? Provide your response in UTC+0, using the date/time picker to select the date and time (24-hour).

Manufacturer's Expected Response: 2022-02-20 18:55 (UTC+0)

WebCode Test	Response	** Inconsistencies not highlighted; No consensus achieved **
2GYK6H-5562	2018-01-15 22:42	
37HZM7-5561	2022-02-20 18:55	
3ERMDL-5562	2018-01-15 22:42	
3J2MUJ-5561	2018-01-15 22:42	
3W8X27-5561	2022-02-20 18:55	
4ELR7K-5562	2018-01-15 22:42	
6GRCUL-5562	2022-01-15 22:42	
6XRJND-5562	2022-02-20 18:55	
7CPVTB-5561	2022-02-20 18:59	
8PW7XC-5562	2022-02-20 18:55	
8YYJXD-5562	2018-01-16 02:42	
8ZU2ZE-5562	2018-01-15 17:42	
98A6KL-5561	2022-02-20 18:55	
9WRPDD-5562	2018-01-15 23:42	
9ZBF4H-5561	2022-02-20 18:55	
A7BERC-5562	2018-01-15 22:42	
ARP7Q6-5561	2022-02-20 14:55	
B6WATE-5561	2018-01-15 22:42	
B9WHYA-5561	2022-02-20 18:55	

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25 - Examination Questions		
WebCode Test	**Response**	** Inconsistencies not highlighted; No consensus achieved **
BN9WG8-5562	2022-02-20 18:55	
BVR2DE-5562	2018-01-15 22:42	
BYPLFC-5562	2022-02-02 05:39	
CMTYN8-5561	2022-02-20 18:55	
CN44V6-5561	2022-02-20 18:55	
DHRBK7-5562	2022-02-20 18:55	
E7WKY6-5561	2018-01-15 22:42	
E7XH9Z-5561	2022-02-20 14:55	
EAWU6Z-5561	2022-02-20 18:55	
EREXP8-5561	2022-02-20 18:55	
EX67D8-5562	2022-02-20 18:55	
EZEWXB-5561	2022-02-20 18:55	
F2G9Z3-5562	2018-01-15 22:42	
F8L898-5562	2022-02-20 18:55	
FGDPP2-5562	2022-02-20 18:55	
FL36D9-5562	[Participant did not return results for this question.]	
FVTQJ7-5562	2022-02-20 18:55	
FXXHAY-5561	2018-01-15 10:42	
G8GC37-5561	2018-01-15 22:42	
GCTZYW-5561	2022-02-20 18:55	
GFWVHY-5561	2022-02-20 18:55	

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25 - Examination Questions		
WebCode Test	**Response**	** Inconsistencies not highlighted; No consensus achieved **
GLX6QD-5562	2022-02-20 18:55	
GR9ZT2-5561	2022-02-20 18:55	
HDM36C-5561	2022-02-20 18:55	
HDM9G8-5561	2022-02-20 08:55	
HEVFPY-5561	2022-02-20 18:55	
HPTDCY-5561	2022-02-20 18:55	
HWZPPY-5562	2022-02-20 18:55	
HX9YL3-5562	2022-02-20 18:55	
JEDQ2D-5562	2022-02-02 05:13	
JQ84YN-5561	2022-02-20 18:55	
K4BTM4-5561	2022-02-20 18:55	
K9GN9W-5561	2018-01-15 22:42	
KA2332-5562	2022-02-20 18:55	
KDZDY2-5561	2022-02-20 18:55	
LTKL96-5562	2022-02-20 18:55	
LYVGBT-5561	2018-01-15 10:42	
MW334U-5561	2022-02-20 18:55	
PPRVBV-5561	2022-02-20 18:55	
PPUJUU-5561	2022-02-20 18:55	
PQ9R3V-5561	2018-01-15 22:42	
PRHXH6-5562	2022-02-20 18:55	

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25 - Examination Questions		
WebCode Test	**Response**	** Inconsistencies not highlighted; No consensus achieved **
PTTY3H-5562	2022-02-20 18:55	
PV4KAY-5561	2022-02-20 18:55	
PZAFUR-5562	2018-01-15 16:42	
Q8PGRF-5561	2022-02-20 18:55	
QKG3YW-5562	2022-02-20 18:55	
QLMMJQ-5561	2022-02-20 23:35	
QQ3XWU-5561	2022-02-20 18:55	
QVYKR4-5562	2018-01-15 22:42	
R8KDG3-5562	2018-01-15 22:42	
RFWD9R-5562	2018-01-15 22:42	
RNVVQP-5561	2022-02-20 18:55	
T4JR6P-5562	2018-01-15 23:42	
TA98UW-5561	2018-01-15 22:42	
TE2AXW-5561	2022-02-20 18:55	
TWHDG3-5561	2018-01-16 12:42	
URL94P-5562	2022-02-20 18:55	
VKGWHC-5561	2022-02-20 18:55	
VRFDXN-5561	2022-02-20 19:55	
VU4RLY-5562	2022-02-20 18:55	
WB6WLF-5561	2018-01-15 22:42	
WRDQDP-5562	2022-02-20 18:55	

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25 - Examination Questions		
WebCode Test	**Response**	** Inconsistencies not highlighted; No consensus achieved **
WXJKCR-5562	2022-02-20 18:55	
X7U2JR-5561	2018-01-15 22:42	
XB3L8N-5562	2018-01-15 22:42	
XGEEHM-5561	2018-01-15 22:42	
Y4WCCF-5561	2022-02-20 18:55	
YDMVRA-5562	[Participant did not return results for this question.]	
YE4XXP-5561	2022-02-20 18:55	
YL2H7J-5562	2018-01-15 22:49	
YLG7ZJ-5562	2018-01-15 22:42	
ZD74EJ-5561	2018-01-16 02:42	
ZDHVAK-5562	2022-02-20 18:55	
ZG7AXV-5561	2022-02-20 18:55	
ZLZ4XH-5561	2022-02-20 18:55	

Question 25: What is the $FILE_NAME Attribute created date and time for PoorFairJaguar.html? Provide your response in UTC+0, using the date/time picker to select the date and time (24-hour).

Consensus Result:

While a majority of participants (61%) reported the expected date and time from the $FILE_NAME attribute, 2022-02-20 18:55, a consensus was not achieved. Another 32% of participants reported the $STANDARD_INFORMATION attribute value of 2018-01-15 22:42.

Expected Response Explanation:

NTFS tracks file times via both the $STANDARD_INFORMATION attribute and the $FILE_NAME attribute. The windows operating system only displays the $STANDARD_INFORMATION attribute file times which are easily manipulated. In this case, the file created time was “stomped” to make it look older than it is (2018-01-15 22:42:49). The $FILE_NAME attribute contains the true time the file was created on this volume.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25 - Examination Questions

Expected Response Illustration:

Autopsy / Sleuth Kit view of NTFS metadata for PoorFairJaguar.html

```
from The Sleuth Kit istat Tool:
MFT Entry Header Values:
Entry: 303846 Sequence: 1
$LogFile Sequence Number: 743432112
Allocated File
Links: 2
$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 1772 (S-1-5-21-3501254099-4204809888-2000606956-1002)
Last User Journal Update Sequence Number: 295346176
Created: 2018-01-15 17:42:49.147916800 (Eastern Standard Time)
File Modified: 2018-11-26 02:32:39.170508800 (Eastern Standard Time)
MFT Modified: 2022-02-20 13:59:02.103062200 (Eastern Standard Time)
Accessed: 2022-02-20 14:01:52.852908400 (Eastern Standard Time)
$FILE_NAME Attribute Values:
Flags: Archive
Name: PoorFairJaguar.html
Parent MFT Entry: 102284 Sequence: 1
Allocated Size: 20480 Actual Size: 0
Created: 2022-02-20 13:55:38.296100700 (Eastern Standard Time)
File Modified: 2022-02-20 13:55:38.296100700 (Eastern Standard Time)
MFT Modified: 2022-02-20 13:55:38.296100700 (Eastern Standard Time)
Accessed: 2022-02-20 13:55:38.296100700 (Eastern Standard Time)
```


Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26 - Examination Questions

Question 26: What does the HostUrl for PXL_20211121_130028206.jpg indicate about its source?

Manufacturer's Expected Response: Downloaded from the Internet as a mail-attachment

WebCode Test	Response
2GYK6H-5562	mail attachment with sender john jenkins johnqjenkins1955@gmail.com
37HZM7-5561	That the file was received as an email attachment downloaded from the Internet.
3ERMDL-5562	It's an email attachment
3J2MUJ-5561	Source is a Google Pixel 5. It was emailed to Jessie Jenkins and downloaded/saved.
3W8X27-5561	Associated with Gmail
4ELR7K-5562	Arrived on email
6GRCUL-5562	Downloaded from an email.
6XRJND-5562	Google mail attachment
7CPVTB-5561	the JPG is from the Internet / ZoneId=3
8PW7XC-5562	Downloaded attachment from e-mail
8YYJXD-5562	HostUrl=https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=82db7f646a&attid=0.1&permmsgid=msg-f:1726420540029
8ZU2ZE-5562	It was downloaded from an empty page i.e. something internal as opposed to from the internet. This image looks to have been downloaded from email.
98A6KL-5561	Attachments in google mail(HostURL in PXL_20211121_130028206.jpg:Zone.Identifier)
9WRPDD-5562	Que es un fichero adjunto de correo. https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=82db7f646a&attid=0
9ZBF4H-5561	https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=82db7f646a&attid=0.1&permmsgid=msg-f:1726420540029497770&th=17f57a558d6571aa&view=att&disp=safe&realattid=f_l0d5k36h0
A7BERC-5562	mail attachments
ARP7Q6-5561	The picture is part of a gmail email as an attachment
B6WATE-5561	It's an email attachment
B9WHYA-5561	It was downloaded from an email attachment online

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26 - Examination Questions	
WebCode Test	**Response**
BN9WG8-5562	email attachment
BVR2DE-5562	It's an email attachment.
BYPLFC-5562	john jenkins <johnqjenkins1955@gmail.com>
CMTYN8-5561	It indicates the source was Google mail
CN44V6-5561	email attachment
DHRBK7-5562	HostUrl: https://mail-attachment.googleusercontent.com / It is indicate that sent to Jessie Jenkins from john jenkins on e-mail.
E7WKY6-5561	mail attachment with sender john jenkins johnqjenkins1955@gmail.com
E7XH9Z-5561	email attachment
EAWU6Z-5561	The host URL indicates that the image was downloaded from the inbox of a Google mail account.
EREXP8-5561	It was received via email attachment from google
EX67D8-5562	That it was downloaded from the internet
EZEWXB-5561	The HostUrl indicates that this image was downloaded from an email containing this item as an attachment.
F2G9Z3-5562	It has been received via email
F8L898-5562	Mail attachment
FGDPP2-5562	Email Attachment
FL36D9-5562	Taken by a Google Pixel 5 and received form email address john jenkins1955@gmail.com
FVTQJ7-5562	Located the zone.identifier. Identified that the file was downloaded from Gmail with the use of the Zone ID.
FXXHAY-5561	Email Attachment
G8GC37-5561	The file is an email attachment which was received via Jessie Jenkins Gmail account from sender johnqjenkins1955@gmail.com on 05/03/2022 01:15:17 (UTC). The subject of the email is 'pic' and the body of the email is 'check this photo out. such a neat pattern'. The file was saved to the following path C:\Users\Jessie Jenkins\Downloads \PXL_20211121_130028206.jpg
GCTZYW-5561	Picture was downloaded using Chrome bowser from gmail account. (jessiejenkins909@gmail.com)

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26 - Examination Questions

WebCode Test	Response
GFWVHY-5561	Email attachment from John Jenkins
GLX6QD-5562	Email Attachment
GR9ZT2-5561	It's an email attachment
HDM36C-5561	Email attachment
HDM9G8-5561	Source of file is an email from Google or Gmail.
HEVFPY-5561	From a gmail account
HPTDCY-5561	Downloaded from the internet from a mail-attachment
HWZPPY-5562	The file is an apparent email attachment.
HX9YL3-5562	That the file was downloaded from an email attachment.
JEDQ2D-5562	downloaded from an email attachment
JQ84YN-5561	HostUrl=https://mail-attachment.googleusercontent.com/attachment/u/0/ an attachment that arrives via email
K4BTM4-5561	ZoneID is 3, so it was downloaded from the Internet, and the source is a mail attachment from a gmail account.
K9GN9W-5561	The source was a Google Pixel 5. It was emailed to Jessie Jenkins, from John Jenkins. Then it was downloaded and saved.
KA2332-5562	Indicates it was an email attachment
KDZDY2-5561	Google mail
LTKL96-5562	Indicate time of taken picture in UTC 00 time zone.
LYVGBT-5561	email attachment
MW334U-5561	Gmail account
PPRVBV-5561	The photo came from an email attachment.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26 - Examination Questions	
WebCode Test	**Response**
PPUJUU-5561	https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=82db7f646a&attid=0.1&permmsgid=msg-f:1726420540029497770&th=17f57a558d6571aa&view=att&disp=safe&realattid=f_l0d5k36h0&saddbat=ANGjdJ_naljkTuVJ7Vid-Q2LrNDc7fmOYncDpFsqkT4As8_30X5oJKmou9Qrj5k5RrlZ9tXfC7skNZ9M7qqo88Se3PlwWdEm6spvifoj7Q2u2gcUWWKmO7RlX1vdrvdn2Rv4OduTf4GfPo4KYWJrX1RvRxRLS8XCcM5GmXygx-i7PhcUmuPNcTsT5_xZ0vftc4rUO3tJq0yDF7IIC5Wnm2khh73vLSPe13tl_-1lHw1U1UghqBnSy8J2otPzbxjwe9-q9VoKA6UdEdPcIGsenM2iXGiN8esfgQyyBGF8U-sB--WpmAqbSHM3PVLocvQfs6YDxjOhVAlkvuJKO4HerpxHnKhCAf77gDdGABFrlHuPuXNdC2XPZNw68nrg6GrpG6LI-IHlzcrApaXboOuw1vY5XavHSXvdIFQ_9oe1Z88Y83Z4AOp2BgR0X9yL5DM-iEbbF5vzEPUb_ykURETUVTgvkOl4W38JNcpgauJT5IP2OVtvTjuajskDQA2nnQO-hIKw6EPG_KTsw-Mvk9mE96vj-4ocme1aq4GOvwg4i47ybFIsWvaCzjCeqy01Ys5MQFbhtFz1ctmaJL2knb-tWTuX4wDrVDrufwK06ftSvLiOVcwgR-f8zQVT07EgoWXNMmAcPz6crwdqEwL6dOjQrSwDIjSe30hjxlv_np34BB5Onk6RzDdOJob_Qh0vKms; The file was downloaded from Gmail attachments.
PQ9R3V-5561	from a Google User
PRHXH6-5562	The HostUrl information indicates that the file is an email attachment from a Google account.
PTTY3H-5562	This file was downloaded from the inbox of a Gmail account (Webmail)
PV4KAY-5561	Chrome download file, email attachment from John Jenkins to Jessie Jenkins (Gmail Inbox).
PZAFUR-5562	Taken by Google Pixel 5, Camera on British Virgin Islands
Q8PGRF-5561	Source = email attachment (HostUrl = https://mail-attachment.googleusercontent.com/attachment...)
QKG3YW-5562	It is an attachment present within an email from a google mail account
QLMMJQ-5561	Attachment download from Google (GMAIL)
QQ3XWU-5561	It was downloaded from the Internet via an email attachment.
QVYKR4-5562	The image attachment was accessed via Google Chrome.
R8KDG3-5562	That the file has been received as an email attachment from a Gmail account. HostUrl=https://mail-attachment.googleusercontent.com/attachment/u/0/
RFWD9R-5562	That is an attachment of an email from John Jenkins the day before her death.
RNVVQP-5561	Gmail Email attachment

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26 - Examination Questions	
WebCode Test	**Response**
T4JR6P-5562	https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=82db7f646a&attid=0.1&permmsgid=msgf:1726420540029497770&th=17f57a558d6571aa&view=att&disp=safe&realattid=f_l0d5k36h0&saddbat=ANGjdJ_naIjkTuVJ7Vid-Q2LrNDc7fmOYncDpFsqkT4As8_30X5oJKmou9Qrj5k5RrlZ9tXfC7skNZ9M7qqo88Se3PIwWdEm6spvifoj7Q2u2gcUWWKmO7RlX1vdrvdn2Rv4OduTf4GfPo4KYWJrX1RvRxRLS8XCcM5GmXygx-i7PhcUmuPNcTsT5_xZ0vftc4rUO3tJq0yDF7IIC5Wnm2khh73vLSPe13tI_-1lHw1U1UghqBnSy8J2otPzbxjwe9-q9VoKA6UdEdPclGsenM2iXGiN8esfgQyyBGF8U-sB--WpmAqbSHM3PVLocvQfs6YDxjOhVAlkvuJKO4HerpxHnKhCAf77gDdGABFrlHuPuXNdC2XPZNw68nrg6GrpG6Ll-lHlzcrApaXboOuw1vY5XavHSXvdIFQ_9oe1Z88Y83Z4AOp2BgR0X9yL5DMiEbbF5vzEPUb_ykURETUVTgvkOl4W38JNcpgauJT5lP2OVtvTjuajskDQA2nnQO-hlKw6EPG_KTsw-Mvk9mE96vj-4ocme1aq4GOvwg4i47ybFlsWvaCzjCeqy01Ys5MQFbhtFz1ctmaJL2knb-tWTuX4wDrVDrufwK06ftSvLiOVcwgRf8zQVT07EgoWXNMmAcPz6crwdqEwL6dOjQrSwDljSe30hjxlv_ np34BB5Onk6RzDdOJob_Qh0vKms
TA98UW-5561	https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=82db7f646a&attid=0.1&permmsgid=msg-f:1726420540029497770&th=17f57a558d6571aa&view=att&disp=safe&realattid=f_l0d5k36h0&saddbat=ANGjdJ_naIjkTuVJ7Vid-Q2LrNDc7fmOYncDpFsqkT4As8_30X5oJKmou9Qrj5k5RrlZ9tXfC7skNZ9M7qqo88Se3PIwWdEm6spvifoj7Q2u2gcUWWKmO7RlX1vdrvdn2Rv4OduTf4GfPo4KYWJrX1RvRxRLS8XCcM5GmXygx-i7PhcUmuPNcTsT5_xZ0vftc4rUO3tJq0yDF7IIC5Wnm2khh73vLSPe13tI_-1lHw1U1UghqBnSy8J2otPzbxjwe9-q9VoKA6UdEdPclGsenM2iXGiN8esfgQyyBGF8U-sB--WpmAqbSHM3PVLocvQfs6YDxjOhVAlkvuJKO4HerpxHnKhCAf77gDdGABFrlHuPuXNdC2XPZNw68nrg6GrpG6Ll-lHlzcrApaXboOuw1vY5XavHSXvdIFQ_9oe1Z88Y83Z4AOp2BgR0X9yL5DM-iEbbF5vzEPUb_ykURETUVTgvkOl4W38JNcpgauJT5lP2OVtvTjuajskDQA2nnQO-hlKw6EPG_KTsw-Mvk9mE96vj-4ocme1aq4GOvwg4i47ybFlsWvaCzjCeqy01Ys5MQFbhtFz1ctmaJL2knb-tWTuX4wDrVDrufwK06ftSvLiOVcwgR-f8zQVT07EgoWXNMmAcPz6crwdqEwL6dOjQrSwDljSe30hjxlv_np34BB5Onk6RzDdOJob_Qh0vKms
TE2AXW-5561	The file is received as attachment by gmail
TWHDG3-5561	HostUrl=https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=82db7f646a&attid=0.1&permmsgid=msg-f:1726420540029497770&th=17f57a558d6571aa&view=att&disp=safe&realattid=f_l0d5k36h0&saddbat=ANGjdJ_naIjkTuVJ7Vid-Q2LrNDc7fmOYncDpFsqkT4As8_30X5oJKmou9Qrj5k5RrlZ9tXfC7skNZ9M7qqo88Se3PIwWdEm6spvifoj7Q2u2gcUWWKmO7RlX1vdrvdn2Rv4OduTf4GfPo4KYWJrX1RvRxRLS8XCcM5GmXygx-i7PhcUmuPNcTsT5_xZ0vftc4rUO3tJq0yDF7IIC5Wnm2khh73vLSPe13tI_-1lHw1U1UghqBnSy8J2otPzbxjwe9-q9VoKA6UdEdPclGsenM2iXGiN8esfgQyyBGF8U-sB--WpmAqbSHM3PVLocvQfs6YDxjOhVAlkvuJKO4HerpxHnKhCAf77gDdGABFrlHuPuXNdC2XPZNw68nrg6GrpG6Ll-lHlzcrApaXboOuw1vY5XavHSXvdIFQ_9oe1Z88Y83Z4AOp2BgR0X9yL5DM-iEbbF5vzEPUb_ykURETUVTgvkOl4W38JNcpgauJT5lP2OVtvTjuajskDQA2nnQO-hlKw6EPG_KTsw-Mvk9mE96vj-4ocme1aq4GOvwg4i47ybFlsWvaCzjCeqy01Ys5MQFbhtFz1ctmaJL2knb-tWTuX4wDrVDrufwK06ftSvLiOVcwgR-f8zQVT07EgoWXNMmAcPz6crwdqEwL6dOjQrSwDljSe30hjxlv_np34BB5Onk6RzDdOJob_Qh0vKms
URL94P-5562	email attachment
VKGWHC-5561	The Zone.Identifier (ZoneID=3) for the file "PXL_20211121_130028206.jpg" indicated that the file been downloaded from Google Mail (https://mail-attachment.googleusercontent.com/attachment/).
VRFDXN-5561	It was sended by email from johnqjenkins1955@gmail.com to jessiejenkins909@gmail.com
VU4RLY-5562	Downloaded using Google Chrome

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26 - Examination Questions

WebCode Test	Response
WB6WLF-5561	An attachment to a gmail email.
WRDQDP-5562	The source HostURL for PXL_20211121_130028206.jpg indicates that it was from a google user's mail. (HostUrl=https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=82db7f646a&…)
WXJKCR-5562	It is/was a google mail attachment (HostUrl=https://mail-attachment.googleusercontent.com/attachment/u/0/)
X7U2JR-5561	It's an email attachment.
XB3L8N-5562	https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=82db7f646a&attid=0.1&permmsgid=msg-f:1726420540029497770&th=17f57a558d6571aa&view=att&disp=safe&realattid=f_l0d5k36h0&saddbat=ANGjdJ_naljkTuVJ7Vid-Q2LrNDc7fmOYncDpFsqkT4As8_30X5oJKmou9Qrj5k5RrlZ9tXfC7skNZ9M7qqo88Se3PlwWdEm6spvifoj7Q2u2gcUWWKmO7RlX1vdrvdn2Rv4OduTf4GfPo4KYWJrX1RvRxRLS8XCcM5GmXygx-i7PhcUmuPNcTsT5_xZ0vftc4rUO3tJq0yDF7IIC5Wnm2khh73vLSPe13tl_-1lHw1U1UghqBnSy8J2otPzbxjwe9-q9VoKA6UdEdPcIGsenM2iXGiN8esfgQyyBGF8U-sB--WpmAqbSHM3PVLocvQfs6YDxjOhVAlkvuJKO4HerpxHnKhCAf77gDdGABFrlHuPuXNdC2XPZNw68nrg6GrpG6LI-IHlzcrApaXboOuw1vY5XavHSXvdIFQ_9oe1Z88Y83Z4AOp2BgR0X9yL5DM-iEbbF5vzEPUb_ykURETUVTgvkOl4W38JNcpgauJT5IP2OVtvTjuajskDQA2nnQO-hIKw6EPG_KTsw-Mvk9mE96vj-4ocme1aq4GOvwg4i47ybFIsWvaCzjCeqy01Ys5MQFbhtFz1ctmaJL2knb-tWTuX4wDrVDrufwK06ftSvLiOVcwgR-f8zQVT07EgoWXNMmAcPz6crwdqEwL6dOjQrSwDIjSe30hjxlv_np34BB5Onk6RzDdOJob_Qh0vKms
XGEEHM-5561	The picture was downloaded
Y4WCCF-5561	The source of the file was an email attachment
YDMVRA-5562	[Participant did not return results for this question.]
YE4XXP-5561	https://mail.google.com/mail/u/0/#inbox/FMfcgzGmvLRqPkhMQgkKVGpnqsvnsHhL
YL2H7J-5562	Google Pixel 5
YLG7ZJ-5562	It was downloaded from the internet/email attachment
ZD74EJ-5561	HostUrl=https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=82db7f646a&attid=0.1&permmsgid=msg-f:1726420540029
ZDHVAK-5562	It indicates the source was Google mail
ZG7AXV-5561	It indicates the file originated as an attachment from a Google Mail account email
ZLZ4XH-5561	email using google

Question 26: What does the HostUrl for PXL_20211121_130028206.jpg indicate about its source?

Consensus Result:

Downloaded from the Internet as a mail-attachment and variations representing the same information.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26 - Examination Questions

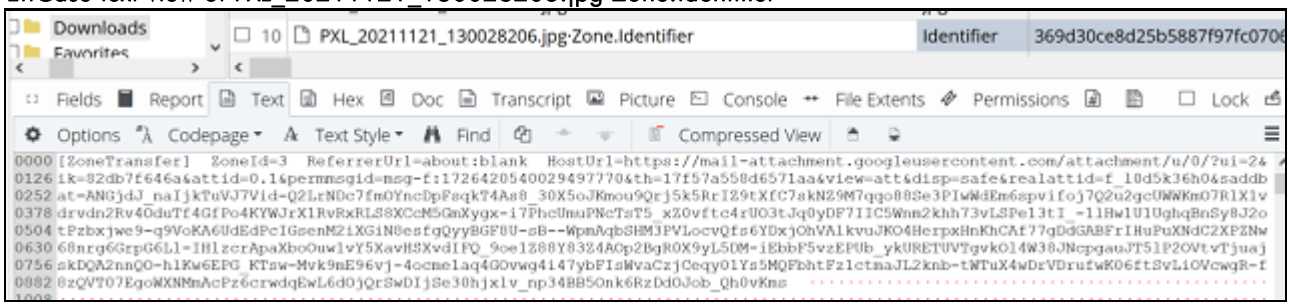
Expected Response Explanation:

PXL_20211121_130028206.jpg is in user Jessie Jenkins' downloads directory. The file has alternate data stream PXL_20211121_130028206.jpg:Zone.Identifier which contains information about the source of the file. In this case ZoneId=3 meaning it was downloaded from the internet (vs. a local network).

PXL_20211121_130028206.jpg:Zone.Identifier also includes information about the HostUrl, in this case HostUrl=https://mail-attachment.googleusercontent.com/attachment…

Expected Response Illustration:

EnCase text view of PXL_20211121_130028206.jpg:Zone.Identifier



Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27 - Examination Questions

Question 27: What email client and version did the administrator install?

Manufacturer's Expected Response: Mozilla Thunderbird (x64 en-US) v.91.6

WebCode Test	Response
2GYK6H-5562	Thunderbird 91.6.0
37HZM7-5561	Mozilla Thunderbird (x64 en-US) version 91.6.1
3ERMDL-5562	Mozilla Thunderbird Version (91.6.1)
3J2MUJ-5561	Thunderbird, version 91.6.0
3W8X27-5561	Thunderbird 91.6.1
4ELR7K-5562	Microsoft OneDrive 22.022.0130.0001
6GRCUL-5562	Mozilla Thunderbird (x64 en-US) version 91.6.1
6XRJND-5562	Thunderbird 91.6.1
7CPVTB-5561	Mozilla Thunderbird v91.6.0.
8PW7XC-5562	Mozilla Thunderbird, version 91.6.1
8YYJXD-5562	The Email client is Mozilla Thunderbird, Version 91.6.1
8ZU2ZE-5562	Mozilla Thunderbird 91.6.1
98A6KL-5561	Thunderbird 91.6.0
9WRPDD-5562	Mozilla Thunderbird (x64 en-US). Versión 91.6.1
9ZBF4H-5561	Mozilla Thunderbird_Version 91.6.1
A7BERC-5562	Mozilla Thunderbird (x64 en-US) 91.6.1
ARP7Q6-5561	Mozilla Thunderbird 91.6.1
B6WATE-5561	Mozilla Thunderbird Version (91.6.1)
B9WHYA-5561	Mozzila Thunderbird 91.6.0

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27 - Examination Questions	
WebCode Test	**Response**
BN9WG8-5562	Mozilla Thunderbird version 91.6.1
BVR2DE-5562	Mozilla Thunderbird / Version (91.6.1)
BYPLFC-5562	Thunderbird Version 91.6.1
CMTYN8-5561	Mozilla Thunderbird 91.6.0 (updated to 91.6.1)
CN44V6-5561	Thunderbird 91.6.0
DHRBK7-5562	Mozilla Thunderbird (x64 en-US) v91.6.1
E7WKY6-5561	Thunderbird 91.6.0
E7XH9Z-5561	Mozilla Thunderbird 91.6.1
EAWU6Z-5561	Mozilla Thunderbird Version 91.6.0
EREXP8-5561	Mozilla Thunderbird v.91.6.1
EX67D8-5562	Mozilla Thunderbird v. 91.6.1
EZEWXB-5561	Mozilla Thunderbird 91.6.0
F2G9Z3-5562	Mozilla Thunderbird version 91.6.1
F8L898-5562	Thunderbird. Version 91.6.1
FGDPP2-5562	Mozila Thunderbird(x64 en-US) version 91.6.1
FL36D9-5562	[Participant did not return results for this question.]
FVTQJ7-5562	Mozilla Thunderbird 91.6.0
FXXHAY-5561	Mozilla Thunderbird 91.6.1
G8GC37-5561	Mozilla Thunderbird 91.6.1
GCTZYW-5561	Mozilla Thunderbird Version: 91.6.1
GFWVHY-5561	Thunderbird 91.6.0

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27 - Examination Questions	
WebCode Test	**Response**
GLX6QD-5562	Mozilla Thunderbird v91.6.0
GR9ZT2-5561	Mozilla Thunderbird, 91.6.1
HDM36C-5561	Mozilla Thunderbird v91.6.0
HDM9G8-5561	Mozilla Thunderbird version 91.6.1
HEVFPY-5561	Mozilla Thunderbird (x64 en-US) version 91.6.1
HPTDCY-5561	Mozilla Thunderbird 64bit, version 91.6.0 was installed, current version is 91.6.1.
HWZPPY-5562	Mozilla Thunderbird Version 91.6.0
HX9YL3-5562	Mozilla Thunderbird v91.6.0
JEDQ2D-5562	Mozilla Thunderbird - 91.6.1
JQ84YN-5561	Mozilla Thunderbird 91.6.0 is the version that is in the Downloads folder for Jessie Jenkins (part of the Administrators group) but version 91.6.1 is installed. The Mozilla Maintenance Service is installed which allows for automated updates (which updated according to the Registry entry -- on 3/5/2022 1:18:55AM (UTC+0:00). This update could have been installed without the need for the user to begin the process. According to the AmCache Program Entries the install date for version 91.6.0 is 2/17/2022.
K4BTM4-5561	Mozilla Thunderbird 91.6.0
K9GN9W-5561	Thunderbird 91.6.0
KA2332-5562	Thunderbird version 91.6.0
KDZDY2-5561	Mozilla Thunderbird 91.6.1
LTKL96-5562	Mozzila Thunderbird, version 91.6.1.
LYVGBT-5561	Mozilla Thunderbird 91.6.1
MW334U-5561	Mozilla Thunderbird 91.6.1
PPRVBV-5561	Mozilla Thunderbird v.91.6.1
PPUJUU-5561	Mozilla Thunderbird (x64 en-US) 91.6.1
PQ9R3V-5561	Thunderbird v 91.6.0

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27 - Examination Questions	
WebCode Test	**Response**
PRHXH6-5562	Mozilla Thunderbird version 91.6.1
PTTY3H-5562	Thunderbird 91.6.0
PV4KAY-5561	Mozilla Thunderbird (x64 en-US), version 91.6.1
PZAFUR-5562	Mozilla Thunderbird (x64 EN-US)
Q8PGRF-5561	Mozilla Thunderbird, version 91.6.0
QKG3YW-5562	Mozilla Thunderbird v91.6.1
QLMMJQ-5561	Mozilla Thunderbird Ver. 91.6.1
QQ3XWU-5561	Mozilla Thunderbird, 91.6.0
QVYKR4-5562	Mozilla Thunderbird v 91.6.1
R8KDG3-5562	Mozilla Thunderbird (x64 en-US) v91.6.1
RFWD9R-5562	Mozilla Thunderbird, version 91.6.1
RNVVQP-5561	Mozilla Thunderbird (x64 en-US) Version 91.6.1
T4JR6P-5562	Mozilla Thunderbird (x64 en-US) version 91.6.1
TA98UW-5561	Thunderbird 91.6.0
TE2AXW-5561	Mozilla Thunderbird 91.6.1
TWHDG3-5561	Mozilla Thunderbird (x64 en-US) / 91.6.1
URL94P-5562	thunderbird setup version 91.6.0. Software hive Registry displays Thunderbird upgraded to version 91.6.1
VKGWHC-5561	Mozilla Thunderbird (version 91.6.0)
VRFDXN-5561	Mozilla Thumderbird(x64eu-us)91.6.0
VU4RLY-5562	Mozeilla Thunderbird 91.6.1
WB6WLF-5561	Mozilla Thunderbird (x64 en-US) 91.6.1

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27 - Examination Questions	
WebCode Test	**Response**
WRDQDP-5562	Mozilla Thunderbird (x64 en-US) v.91.6.1
WXJKCR-5562	Thunderbird 91.6.1
X7U2JR-5561	Mozilla Thunderbird Version (91.6.1)
XB3L8N-5562	Thunderbird 91.6.0
XGEEHM-5561	Mozilla Thunderbird (x64 en-US) v91.6.1
Y4WCCF-5561	Thunderbird v91.6.0
YDMVRA-5562	[Participant did not return results for this question.]
YE4XXP-5561	Mozilla Thunderbird (x64 en-US), version 91.6.1
YL2H7J-5562	Mozilla Thunderbird
YLG7ZJ-5562	Mozilla Thunderbird version 91.6.1
ZD74EJ-5561	The Email client is Mozilla Thunderbird, Version 91.6.1
ZDHVAK-5562	Mozilla Thunderbird 91.6.0 (updated to 91.6.1)
ZG7AXV-5561	Mozilla Thunderbird v91.6.0
ZLZ4XH-5561	Mozilla Thunderbird 91.6.1

Question 27: What email client and version did the administrator install?

Consensus Result:

Mozilla Thunderbird v.91.6

Expected Response Explanation:

Installed applications are recorded in the Software registry hive in the Microsoft\Windows\CurrentVersion\Uninstall key.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27 - Examination Questions

Expected Response Illustration:

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

```
uninstall v.20200525
(Software, NTUSER.DAT) Gets contents of Uninstall keys from Software, NTUSER.DAT hives

Uninstall
Microsoft\Windows\CurrentVersion\Uninstall

2022-03-05 01:18:55Z
  Mozilla Thunderbird (x64 en-US) v.91.6.1
```


Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28 - Examination Questions

Question 28: What is the file status of C:\Users\Jessie Jenkins\Pictures\132p61j53ai81.jpg?

Manufacturer's Expected Response: Deleted, not overwritten

WebCode Test	Response
2GYK6H-5562	previously existing (deleted)
37HZM7-5561	"Item from deleted sources" "… no longer exists from the point of view of the file system". 132p61j53ai81.jpg has the status of deleted and can't be viewed by the user of the device without required software.
3ERMDL-5562	DELETED
3J2MUJ-5561	Deleted
3W8X27-5561	Deleted
4ELR7K-5562	deleted
6GRCUL-5562	deleted
6XRJND-5562	previously existing, data not necessarily intact
7CPVTB-5561	Deleted
8PW7XC-5562	Deleted
8YYJXD-5562	Items from deleted sources
8ZU2ZE-5562	Deleted
98A6KL-5561	Deleted
9WRPDD-5562	Eliminado
9ZBF4H-5561	Deleted
A7BERC-5562	Deleted
ARP7Q6-5561	Deleted
B6WATE-5561	DELETED
B9WHYA-5561	Deleted

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28 - Examination Questions	
WebCode Test	**Response**
BN9WG8-5562	File is deleted
BVR2DE-5562	DELETED
BYPLFC-5562	Deleted
CMTYN8-5561	Deleted
CN44V6-5561	Deleted
DHRBK7-5562	That file has been deleted.
E7WKY6-5561	previously existing (deleted)
E7XH9Z-5561	deleted
EAWU6Z-5561	It is a deleted file.
EREXP8-5561	deleted
EX67D8-5562	Previously existing (deleted)
EZEWXB-5561	Deleted
F2G9Z3-5562	deleted
F8L898-5562	Deleted
FGDPP2-5562	Deleted File
FL36D9-5562	Deleted
FVTQJ7-5562	Deleted/ Previously existing.
FXXHAY-5561	Deleted
G8GC37-5561	deleted (but recoverable)
GCTZYW-5561	Deleted
GFWVHY-5561	Deleted

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28 - Examination Questions	
WebCode Test	**Response**
GLX6QD-5562	Deleted
GR9ZT2-5561	Deleted
HDM36C-5561	Deleted
HDM9G8-5561	deleted
HEVFPY-5561	Unallocated
HPTDCY-5561	Deleted File, with archive flag
HWZPPY-5562	Deleted
HX9YL3-5562	Deleted
JEDQ2D-5562	\Users\Jessie Jenkins\Pictures\132p61j53ai81.jpg - downloaded from https://i.redd.it/132p61j53ai81.jpg and saved in the pictures folder
JQ84YN-5561	forensic software reports this as a deleted file
K4BTM4-5561	prev. existing, data not necessarily intact
K9GN9W-5561	Deleted
KA2332-5562	Previously existing (deleted file)
KDZDY2-5561	Deleted
LTKL96-5562	File is deleted.
LYVGBT-5561	deleted
MW334U-5561	Unallocated
PPRVBV-5561	It's deleted
PPUJUU-5561	Deleted
PQ9R3V-5561	Deleted
PRHXH6-5562	Deleted

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28 - Examination Questions	
WebCode Test	**Response**
PTTY3H-5562	Deleted File
PV4KAY-5561	Deleted file recovered from file slack.
PZAFUR-5562	Deleted
Q8PGRF-5561	previously existing (e.g., deleted), data not necessarily intact
QKG3YW-5562	It is previously existing, and data may not be intact
QLMMJQ-5561	deleted
QQ3XWU-5561	Previously Existing
QVYKR4-5562	Deleted.
R8KDG3-5562	Previously existing, data not necessarily intact
RFWD9R-5562	Deleted
RNVVQP-5561	Deleted, no indication that the data, or part of the data, has been overwritten
T4JR6P-5562	deleted
TA98UW-5561	Deleted
TE2AXW-5561	Deleted
TWHDG3-5561	File, Deleted, Archive
URL94P-5562	deleted
VKGWHC-5561	Deleted
VRFDXN-5561	Deleted. Picture deleted 17/02/2022 01:53:33
VU4RLY-5562	File status is deleted
WB6WLF-5561	Deleted
WRDQDP-5562	DELETED (Unallocated)

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28 - Examination Questions

WebCode Test	Response
WXJKCR-5562	Previously existing
X7U2JR-5561	DELETED
XB3L8N-5562	Deleted
XGEEHM-5561	Deleted
Y4WCCF-5561	Deleted
YDMVRA-5562	[Participant did not return results for this question.]
YE4XXP-5561	Deleted
YL2H7J-5562	Deleted/Previously existing
YLG7ZJ-5562	Deleted
ZD74EJ-5561	Items from deleted sources
ZDHVAK-5562	Deleted
ZG7AXV-5561	Deleted
ZLZ4XH-5561	Unallocated

Question 28: What is the file status of C:\Users\Jessie Jenkins\Pictures\132p61j53ai81.jpg?

Consensus Result:

Deleted

Expected Response Explanation:

This file was deleted, and the Master File Table (MFT) entry marked for reuse, but neither the file nor the MFT entry have been overwritten so the file contents and metadata in the MFT are still available for review.

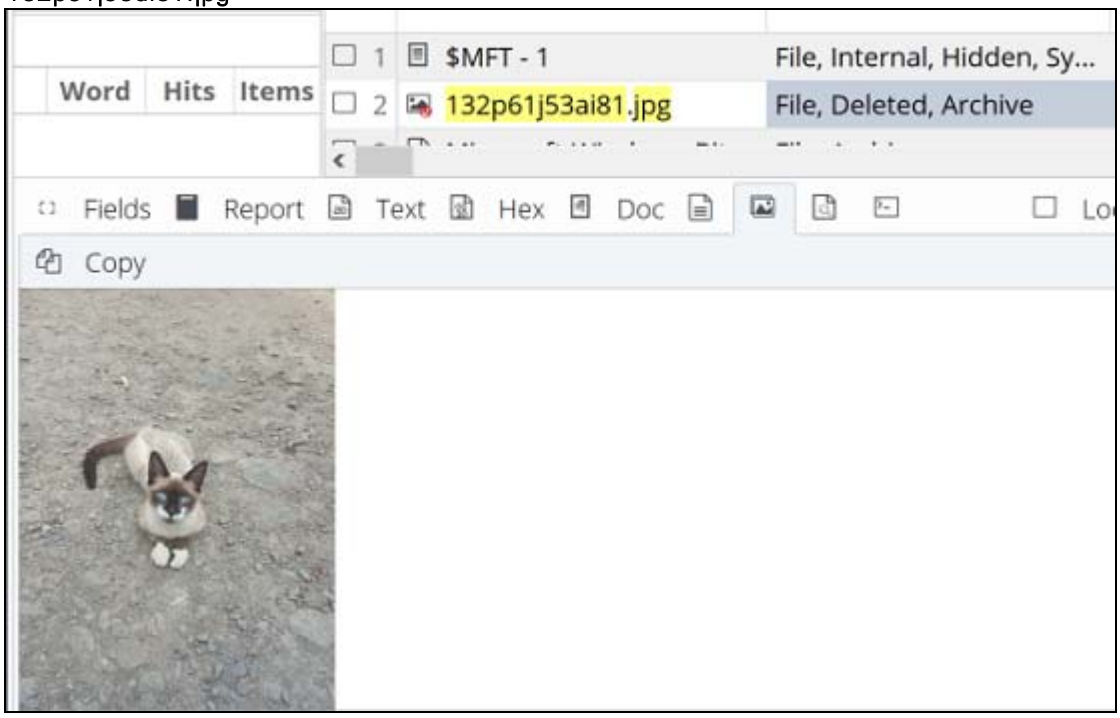
Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28 - Examination Questions

Expected Response Illustration:

132p61j53ai81.jpg



Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 29 - Examination Questions

Question 29: Who is listed as the author of AliveTroubledSalmon.doc?

Manufacturer's Expected Response: vhamocbrewsp

WebCode Test	Response
2GYK6H-5562	vhamocbrewsp
37HZM7-5561	vhamocbrewsp
3ERMDL-5562	vhamocbrewsp
3J2MUJ-5561	vhamocbrewsp
3W8X27-5561	vhamocbrewsp
4ELR7K-5562	vhamocbrewsp
6GRCUL-5562	vhamocbrewsp
6XRJND-5562	vhamocbrewsp
7CPVTB-5561	vhamocbrewsp
8PW7XC-5562	Vhamocbrewsp
8YYJXD-5562	The answer is “vhamocbrewsp “. I have searched for the file name AliveTroubledSalmon.doc in Axiom forensics tools which provided the information of the file which has author as vhamocbrewsp.
8ZU2ZE-5562	vhamocbrewsp
98A6KL-5561	vhamocbrewsp
9WRPDD-5562	vhamocbrewsp
9ZBF4H-5561	vhamocbrewsp
A7BERC-5562	vhamocbrewsp
ARP7Q6-5561	vhamocbrewsp
B6WATE-5561	vhamocbrewsp
B9WHYA-5561	vhamocbrewsp

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 29 - Examination Questions	
WebCode Test	**Response**
BN9WG8-5562	vhamocbrewsp
BVR2DE-5562	vhamocbrewsp
BYPLFC-5562	vhamocbrewsp
CMTYN8-5561	vhamocbrewsp
CN44V6-5561	vhamocbrewsp
DHRBK7-5562	vhamocbrewsp
E7WKY6-5561	vhamocbrewsp
E7XH9Z-5561	vhamocbrewsp
EAWU6Z-5561	vhamocbrewsp
EREXP8-5561	VHAMOCBREWSP
EX67D8-5562	vhamocbrewsp
EZEWXB-5561	Vhamocbrewsp
F2G9Z3-5562	vhamocbrewsp
F8L898-5562	Vhamocbrewsp
FGDPP2-5562	vhamocbrewsp
FL36D9-5562	vhamocbrewsp
FVTQJ7-5562	vhamocbrewsp
FXXHAY-5561	Vhamocbrewsp Department of Veteran Affairs
G8GC37-5561	vhamocbrewsp
GCTZYW-5561	vhamocbrewsp
GFWVHY-5561	vhamocbrewsp

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 29 - Examination Questions	
WebCode Test	**Response**
GLX6QD-5562	vhamocbrewsp
GR9ZT2-5561	vhamocbrewsp
HDM36C-5561	vhamocbrewsp
HDM9G8-5561	vhamocbrewsp
HEVFPY-5561	vhamocbrewsp
HPTDCY-5561	vhamocbrewsp
HWZPPY-5562	vhamocbrewsp
HX9YL3-5562	vhamocbrewsp
JEDQ2D-5562	vhamocbrewsp
JQ84YN-5561	vhamocbrewsp
K4BTM4-5561	vhamocbrewsp
K9GN9W-5561	vhamocbrewsp
KA2332-5562	vhamocbrewsp
KDZDY2-5561	vhamocbrewsp
LTKL96-5562	vhamocbrewsp
LYVGBT-5561	VHAMOCBREWSP department of adminstration- veteran affairs
MW334U-5561	Vhamocbrewsp
PPRVBV-5561	vhamocbrewsp
PPUJUU-5561	vhamocbrewsp
PQ9R3V-5561	vhamocbrewsp
PRHXH6-5562	vhamocbrewsp

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 29 - Examination Questions	
WebCode Test	**Response**
PTTY3H-5562	vhamocbrewsp
PV4KAY-5561	vhamocbrewsp, Dept. of Veterans Affairs
PZAFUR-5562	vhamocbrewsp
Q8PGRF-5561	vhamocbrewsp
QKG3YW-5562	vhamocbrewsp
QLMMJQ-5561	vhamcbrewsp
QQ3XWU-5561	vhamocbrewsp
QVYKR4-5562	'vhamocbrewsp'
R8KDG3-5562	vhamocbrewsp
RFWD9R-5562	vhamocbrewsp
RNVVQP-5561	vhamocbrewsp
T4JR6P-5562	vhamocbrewsp
TA98UW-5561	vhamocbrewsp
TE2AXW-5561	vhamocbrewsp
TWHDG3-5561	vhamocbrewsp
URL94P-5562	vhamocbrewsp
VKGWHC-5561	vhamocbrewsp
VRFDXN-5561	whamocbrewsp
VU4RLY-5562	vhamocbrewsp
WB6WLF-5561	vhamocbrewsp Dept of Veterans Affairs
WRDQDP-5562	vhamocbrewsp

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 29 - Examination Questions	
WebCode Test	**Response**
WXJKCR-5562	vhamocbrewsp
X7U2JR-5561	vhamocbrewsp
XB3L8N-5562	vhamocbrewsp
XGEEHM-5561	vhamocbrewsp
Y4WCCF-5561	vhamocbrewsp
YDMVRA-5562	[Participant did not return results for this question.]
YE4XXP-5561	vhamocbrewsp
YL2H7J-5562	Jessie Jenkins
YLG7ZJ-5562	vhamocbrewsp
ZD74EJ-5561	The answer is “vhamocbrewsp “. I have searched for the file name AliveTroubledSalmon.doc in Axiom forensics tools which provided the information of the file which has author as vhamocbrewsp.
ZDHVAK-5562	vhamocbrewsp
ZG7AXV-5561	vhamocbrewsp
ZLZ4XH-5561	Vhamocbrewsp

Question 29: Who is listed as the author of AliveTroubledSalmon.doc?

Consensus Result:

vhamocbrewsp

Expected Response Explanation:

Microsoft Office document metadata can be viewed with a tool such as Exiftool, or by opening with the native office application.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 29 - Examination Questions

Expected Response Illustration:

Exiftool parsing of metadata for AliveTroubledSalmon.doc

```
ExifTool Version Number       : 12.05
File Name                     : AliveTroubledSalmon.doc
Directory                     : C:/Users/user/Documents/CTS/22 Windows/Autopsy/22-5561/Export
File Size                     : 158 kB
File Modification Date/Time   : 2022:03:08 10:16:29-05:00
File Access Date/Time         : 2022:03:08 10:16:59-05:00
File Creation Date/Time       : 2022:03:08 10:16:29-05:00
File Permissions              : rw-rw-rw-
File Type                     : DOC
File Type Extension           : doc
MIME Type                     : application/msword
Identification                : Word 8.0
Language Code                 : English (US)
Doc Flags                     : Has picture, 1Table, ExtChar
System                        : Windows
Word 97                       : No
Title                         : Section 9 - Education, Training and Exercises
Subject                       :
Author                        : vhamocbrewsp
Keywords                      :
```

Microsoft Word display of information for AliveTroubledSalmon.doc

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 30 - Examination Questions

Question 30: What is the name of the file that contains a string consisting of two letters, five numbers, "CW", and four numbers (e.g., AA12345CW1234)?

Manufacturer's Expected Response: CheerfulSuperDonkey.text

WebCode Test	Response
2GYK6H-5562	CheerfulSuperDonkey.text
37HZM7-5561	CheerfulSuperDonkey.text
3ERMDL-5562	CheerfulSuperDonkey.text
3J2MUJ-5561	CheerfulSuperDonkey.text
3W8X27-5561	CheerfulSuperDonkey.text
4ELR7K-5562	CheerfulSuperDonkey.text
6GRCUL-5562	CheerfulSuperDonkey.text
6XRJND-5562	\Users\Jessie Jenkins\Documents\CheerfulSuperDonkey.text
7CPVTB-5561	CheerfulSuperDonkey.text
8PW7XC-5562	CheerfulSuperDonkey.text
8YYJXD-5562	Cheerfulsuperdonkey.text
8ZU2ZE-5562	cheerfulsuperdonkey.text
98A6KL-5561	CheerfulSuperDonkey.text
9WRPDD-5562	CheerfulSuperDonkey.text. (EA23456CW4448)
9ZBF4H-5561	CheerfulSuperDonkey.text
A7BERC-5562	CheerfulSuperDonkey.text
ARP7Q6-5561	CheerfulSuperDonkey.text
B6WATE-5561	CheerfulSuperDonkey.text
B9WHYA-5561	CheerfulSuperDonkey.text

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 30 - Examination Questions	
WebCode Test	**Response**
BN9WG8-5562	CheerfulSuperDonkey.txt
BVR2DE-5562	EA23456CW4488 / CheerfulSuperDonkey.text
BYPLFC-5562	CheerfulSuperDonkey.text
CMTYN8-5561	CheerfulSuperDonkey.text
CN44V6-5561	CheerfulSuperDonkey.text
DHRBK7-5562	CheerfulSuperDonkey.text
E7WKY6-5561	CheerfulSuperDonkey.text
E7XH9Z-5561	CheerfulSuperDonkey.text
EAWU6Z-5561	CheerfulSuperDonkey.text
EREXP8-5561	cheerfulsuperdonkey.text
EX67D8-5562	Unable to find
EZEWXB-5561	CheerfulSuperDonkey.text
F2G9Z3-5562	CheerfulSuperDonkey.text
F8L898-5562	CheerfulSuperDonkey
FGDPP2-5562	CheerfulSuperDonkey.text
FL36D9-5562	[Participant did not return results for this question.]
FVTQJ7-5562	CheerfulSuperDonkey.text
FXXHAY-5561	CheerfulSuperDonkey.text
G8GC37-5561	CheerfulSuperDonkey.text
GCTZYW-5561	CheerfulSuperDonkey.text
GFWVHY-5561	CheerfulSuperDonkey.text

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 30 - Examination Questions	
WebCode Test	**Response**
GLX6QD-5562	CheerfulSuperDonkey.text
GR9ZT2-5561	CheerfulSuperDonkey.text
HDM36C-5561	CheerfulSuperDonkey.text
HDM9G8-5561	CheerfulSuperDonkey.text
HEVFPY-5561	CheerfulSuperDonkey.text
HPTDCY-5561	CheerfulSuperDonkey.text - Text (EA23456CW4448)
HWZPPY-5562	CheerfulSuperDonkey.text
HX9YL3-5562	CheerfulSuperDonkey.text
JEDQ2D-5562	Users\Jessie Jenkins\Documents\CheerfulSuperDonkey.text
JQ84YN-5561	CheerfulSuperDonkey.text
K4BTM4-5561	CheerfulSuperDonkey.text
K9GN9W-5561	CheerfulSuperDonkey.text
KA2332-5562	CheerfulSuperDonkey.text
KDZDY2-5561	CheerfulSuperDonkey.text
LTKL96-5562	[Participant did not return results for this question.]
LYVGBT-5561	cheerfulsuperdonkey.txt
MW334U-5561	CheerfulSuperDonkey.text
PPRVBV-5561	CheerfulSuperDonkey.text
PPUJUU-5561	CheerfulSuperDonkey.text
PQ9R3V-5561	CheerfulSuperDonkey.text
PRHXH6-5562	CheerfulSuperDonkey.txt

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 30 - Examination Questions	
WebCode Test	**Response**
PTTY3H-5562	CheerfulSuperDonkey.text
PV4KAY-5561	CheerfulSuperDonkey.text
PZAFUR-5562	Cheerfulsuperdonkey.text
Q8PGRF-5561	CheerfulSuperDonkey.text
QKG3YW-5562	CheerfulSuperDonkey
QLMMJQ-5561	CheerfulSuperDonkey.text
QQ3XWU-5561	CheerfulSuperDonkey.text
QVYKR4-5562	CheerfulSuperDonkey.text
R8KDG3-5562	CheerfulSuperDonkey.text
RFWD9R-5562	EA23456CW4448
RNVVQP-5561	CheerfulSuperDonkey.text
T4JR6P-5562	cheerfulsuperdonkey.text
TA98UW-5561	CheerfulSuperDonkey.text
TE2AXW-5561	CheerfulSuperDonkey.text
TWHDG3-5561	CheerfulSuperDonkey.text
URL94P-5562	CheerfulSuperDonkey.text EA23456CW4448
VKGWHC-5561	CheerfulSuperDonkey.text
VRFDXN-5561	CheerfulSuperDonkey.text D:\Users\Jessie Jekins\documents\CheerfulSuperDonkey.text "EA23456CW4448"
VU4RLY-5562	cheerfulsuperdonkey.text
WB6WLF-5561	CheerfulSuperDonkey.text

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 30 - Examination Questions	
WebCode Test	**Response**
WRDQDP-5562	C:/Users/Jessie Jenkins/Documents/CheerfulSuperDonkey.text
WXJKCR-5562	CheerfulSuperDonkey.text (EA23456CW4448)
X7U2JR-5561	CheerfulSuperDonkey.text
XB3L8N-5562	CheerfulSuperDonkey.text
XGEEHM-5561	CheerfulSuperDonkey.text
Y4WCCF-5561	CheerfulSuperDonkey.text
YDMVRA-5562	[Participant did not return results for this question.]
YE4XXP-5561	CheerfulSuperDonkey.text
YL2H7J-5562	CheerfulSuperDonkey.text
YLG7ZJ-5562	[Participant did not return results for this question.]
ZD74EJ-5561	Cheerfulsuperdonkey.text
ZDHVAK-5562	CheerfulSuperDonkey.text
ZG7AXV-5561	CheerfulSuperDonkey.text
ZLZ4XH-5561	CheerfulSuperDonkey.text

Question 30: What is the name of the file that contains a string consisting of two letters, five numbers, "CW", and four numbers (e.g., AA12345CW1234)?

Consensus Result:

CheerfulSuperDonkey.text

Expected Response Explanation:

The answer to this question is easiest to find by using a regular expression to search for the structured data, the expression: [a-z]{2,2}[0-9]{5,5}CW[0-9]{4,4} will find occurrences of the string consisting of two letters, five numbers, CW, and four letters, EA23456CW4448.

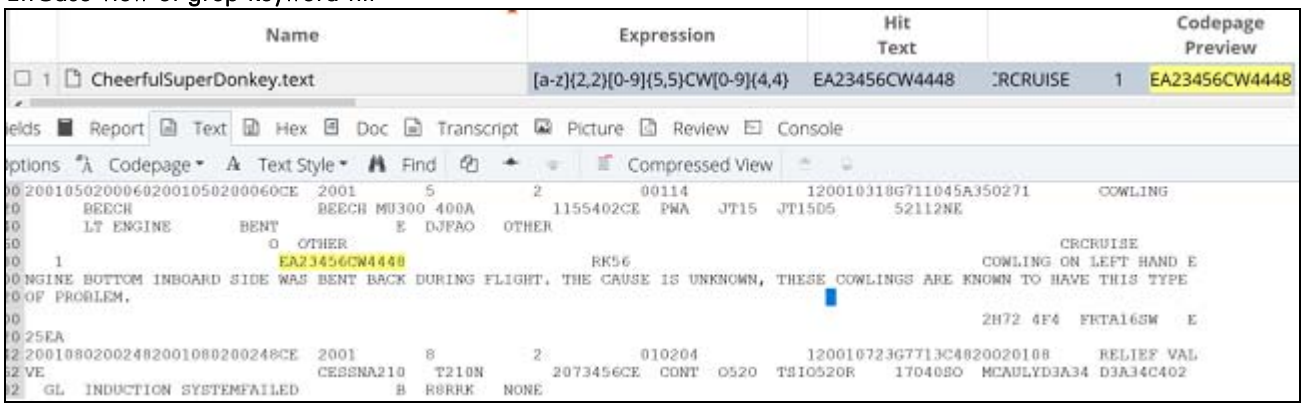
Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

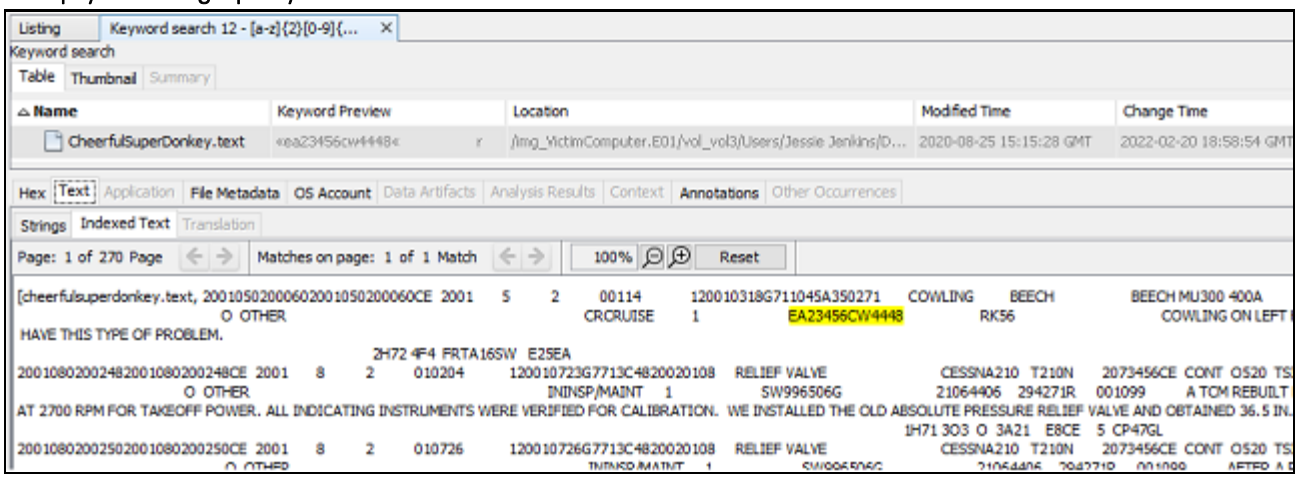
Question 30 - Examination Questions

Expected Response Illustration:

EnCase view of grep keyword hit



Autopsy view of grep keyword hit



Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 31 - Examination Questions

Question 31: Who has the U.S. phone number beginning in "57" and ending in "57"? What is the full phone number?

Manufacturer's Expected Response: Who: Jessie Jenkins
Phone Number: (571) 302-4357

WebCode Test	Response
2GYK6H-5562	Who: Jessie Jenkins, Phone Number: (571) 302-4357
37HZM7-5561	Who: Jesse Jenkins, Phone Number: 5713024357
3ERMDL-5562	Who: Jessie Jenkins, Phone Number: (571) 302-4357
3J2MUJ-5561	Who: Jessie Jenkins, Phone Number: (571) 302-4357
3W8X27-5561	Who: Jessie Jenkins, Phone Number: (571) 302 4357
4ELR7K-5562	Who: Jessie Jenkins, Phone Number: (571)302-4357
6GRCUL-5562	Who: Jessie Jenkins, Phone Number: (571) 302-4357
6XRJND-5562	Who: Jessie Jenkins, Phone Number: 571 302 4357
7CPVTB-5561	Who: Jessie Jenkins, Phone Number: (571) 302-4357
8PW7XC-5562	Who: Jessie Jenkins, Phone Number: (571) 302-4357
8YYJXD-5562	Who: Jessie Jenkins {jessiejenkins909@gmail.com}, Phone Number: (571)302-4357
8ZU2ZE-5562	Who: Jessie Jenkins (jessiejenkins909@gmail.com), Phone Number: (571) 302-4357
98A6KL-5561	Who: Jessie Jenkins, Phone Number: (571) 302-4357
9WRPDD-5562	Who: Jessie Jenkins, Phone Number: (571) 302-4357
9ZBF4H-5561	Who: Jessie Jenkins, Phone Number: (571) 302-4357
A7BERC-5562	Who: Jessie Jenkins, Phone Number: (571) 302-4357
ARP7Q6-5561	Who: Jessie Jenkins, Phone Number: (571) 302-4357
B6WATE-5561	Who: Jessie Jenkins, Phone Number: (571) 302-4357
B9WHYA-5561	Who: Jessie Jenkins, Phone Number: (571) 302-4357

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 31 - Examination Questions	
WebCode Test	**Response**
BN9WG8-5562	Who: Jessie Jenkins, Phone Number: (571) 302-4357
BVR2DE-5562	Who: Jessie Jenkins, Phone Number: (571) 302-4357
BYPLFC-5562	Who: Jessie Jenkins, Phone Number: (571) 302-4357
CMTYN8-5561	Who: Jessie Jenkins, Phone Number: (571) 302-4357
CN44V6-5561	Who: Jessie Jenkins, Phone Number: 5713024357
DHRBK7-5562	Who: Jessie Jenkins, Phone Number: (571) 302-4357
E7WKY6-5561	Who: Jessie Jenkins, Phone Number: (571) 302-4357
E7XH9Z-5561	Who: Jessie Jenkins, Phone Number: (571) 302-4357
EAWU6Z-5561	Who: Jessie Jenkins, Phone Number: (571) 302-4357
EREXP8-5561	Who: Jessie Jenkins, Phone Number: 571-302-4357
EX67D8-5562	Who: Jessie Jenkins, Phone Number: 571-302-4357
EZEWXB-5561	Who: Jessie Jenkins, Phone Number: (571) 302-4357
F2G9Z3-5562	[Participant did not return results for this question.]
F8L898-5562	Who: Jessie Jenkins, Phone Number: (571) 302-4357
FGDPP2-5562	Who: Jessie Jenkins, Phone Number: (571) 302-4357
FL36D9-5562	[Participant did not return results for this question.]
FVTQJ7-5562	Who: Jessie Jenkins, Phone Number: (571) 302-4357
FXXHAY-5561	Who: Jessie Jenkins, Phone Number: 571-303-4357
G8GC37-5561	Who: Jessie Jenkins, Phone Number: (571) 302-4357
GCTZYW-5561	Who: Jessie Jenkins, Phone Number: (571) 302-4357
GFWVHY-5561	Who: Jessie Jenkins, Phone Number: (571) 302-4357

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 31 - Examination Questions	
WebCode Test	**Response**
GLX6QD-5562	Who: Jessie Jenkins, Phone Number: (571) 302-4357
GR9ZT2-5561	Who: Jessie Jenkins, Phone Number: 571-302-4357
HDM36C-5561	Who: Jessie Jenkins, Phone Number: (571) 302-4357
HDM9G8-5561	Who: Jessie Jenkins, Phone Number: (571) 302-4357
HEVFPY-5561	Who: Alex Anderson, Phone Number: 5713024357
HPTDCY-5561	Who: Jesse Jenkins, Phone Number: (571) 302-4357
HWZPPY-5562	Who: Jessie Jenkins, Phone Number: (571) 302-4357
HX9YL3-5562	Who: Jessie Jenkins, Phone Number: (571) 302-4357
JEDQ2D-5562	Who: Jessie Jenkins, Phone Number: (571) 302-4357
JQ84YN-5561	Who: Jessie Jenkins, Phone Number: (571) 302-4357
K4BTM4-5561	Who: Jessie Jenkins, Phone Number: (571) 302-4357
K9GN9W-5561	Who: Jessie Jenkins, Phone Number: (571) 302-4357
KA2332-5562	Who: Jessie Jenkins, Phone Number: (571) 302-4357
KDZDY2-5561	[Participant did not return results for this question.]
LTKL96-5562	[Participant did not return results for this question.]
LYVGBT-5561	Who: Jessie Jenkins, Phone Number: (571) 302-4357
MW334U-5561	Who: Alex Anderson, Phone Number: 5713024357
PPRVBV-5561	Who: Jessie Jenkins, Phone Number: 571-302-4357
PPUJUU-5561	Who: Jessie Jenkins; Ms. Yvette Alvarez, Phone Number: (571) 302-4357; 718-573-4857
PQ9R3V-5561	Who: Jessie Jenkins, Phone Number: (571)302-4357

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 31 - Examination Questions	
WebCode Test	**Response**
PRHXH6-5562	Who: Jessie Jenkins, Phone Number: (571) 302-4357
PTTY3H-5562	Who: Jessie Jenkins, Phone Number: (571) 302-4357
PV4KAY-5561	Who: Jessie Jenkins, Phone Number: 571-302-4357
PZAFUR-5562	Who: Jessie Jenkins, Phone Number: (571) 302-4357
Q8PGRF-5561	Who: Jessie Jenkins, Phone Number: (571) 302-4357
QKG3YW-5562	Who: Jessie Jenkins, Phone Number: (571) 302-4357
QLMMJQ-5561	Who: Jessie Jenkins, Phone Number: (571) 302-4357
QQ3XWU-5561	Who: Jessie Jenkins, Phone Number: (571) 302-4357
QVYKR4-5562	Who: Jessie JENKINS, Phone Number: (571) 302 4357
R8KDG3-5562	Who: Jessie Jenkins, Phone Number: (571) 302-4357
RFWD9R-5562	Who: Jessie Jenkins, Phone Number: (571) 302-4357
RNVVQP-5561	Who: Jessie Jenkins, Phone Number: (571) 302-4357
T4JR6P-5562	Who: Jessie Jenkins, Phone Number: (571) 302-4357
TA98UW-5561	Who: Jessie Jenkins, Phone Number: (571) 302-4357
TE2AXW-5561	Who: Jessie Jenkins, Phone Number: (571) 302-4357
TWHDG3-5561	Who: Jessie Jenkins, Phone Number: (571) 302-4357
URL94P-5562	Who: Jessie Jenkins, Phone Number: 571 302-4357
VKGWHC-5561	Who: Jessie Jenkins, Phone Number: 571-302-4357
VRFDXN-5561	Who: Jessiejenkins909@gmail.com, Phone Number: (571)302-4357
VU4RLY-5562	Who: jessie jenkins, Phone Number: (571) 302-4357 (located within an email)
WB6WLF-5561	Who: Jessie Jenkins, Phone Number: 571-302-4357

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 31 - Examination Questions

WebCode Test	Response
WRDQDP-5562	Who: Jessie Jenkins, Phone Number: (571) 302-4357
WXJKCR-5562	Who: Jessie Jenkins, Phone Number: (571) 302-4357
X7U2JR-5561	Who: Jessie Jenkins, Phone Number: (571) 302-4357
XB3L8N-5562	Who: Jessie Jenkins, Phone Number: (571) 302-4357
XGEEHM-5561	Who: Jessie Jenkins, Phone Number: (571)302-4357
Y4WCCF-5561	Who: Jessie Jenkins, Phone Number: (571) 302-4357
YDMVRA-5562	[Participant did not return results for this question.]
YE4XXP-5561	Who: Jessie Jenkins, Phone Number: (571) 302-4357
YL2H7J-5562	Who: Jessie Jenkins, Phone Number: (571) 302-4357
YLG7ZJ-5562	Who: Jessie Jenkins, Phone Number: (571) 302-4357
ZD74EJ-5561	Who: Jessie Jenkins {jessiejenkins909@gmail.com}, Phone Number: (571)302-4357
ZDHVAK-5562	Who: Jessie Jenkins, Phone Number: (571) 302-4357
ZG7AXV-5561	Who: Jessie Jenkins, Phone Number: (571) 302-4357
ZLZ4XH-5561	Who: Alex Anderson, Phone Number: 5713024357

Question 31: Who has the U.S. phone number beginning in "57" and ending in "57"? What is the full phone number?

Consensus Result:

Who: Jessie Jenkins
Phone Number: (571) 302-4357

Expected Response Explanation:

Most forensic analysis suites include generic regular expressions for finding phone numbers (e.g., [0-9]{3,3}[)]?[\-\ \.][0-9]{3,3}[\-\ \.][0-9]{4,4}). Searching with this expression will find hits in thousands of files. Altering the expression to search specifically for phone numbers beginning and ending in "57" (e.g. 57[0-9][)]?[\-\ \.] [0-9]{3,3}[\-\ \.][0-9]{2,2}57) returns only about 10 files, all related to an email message sent from Jessie Jenkins to Alex Andersen wherein she provides her phone number (571) 302-4357.

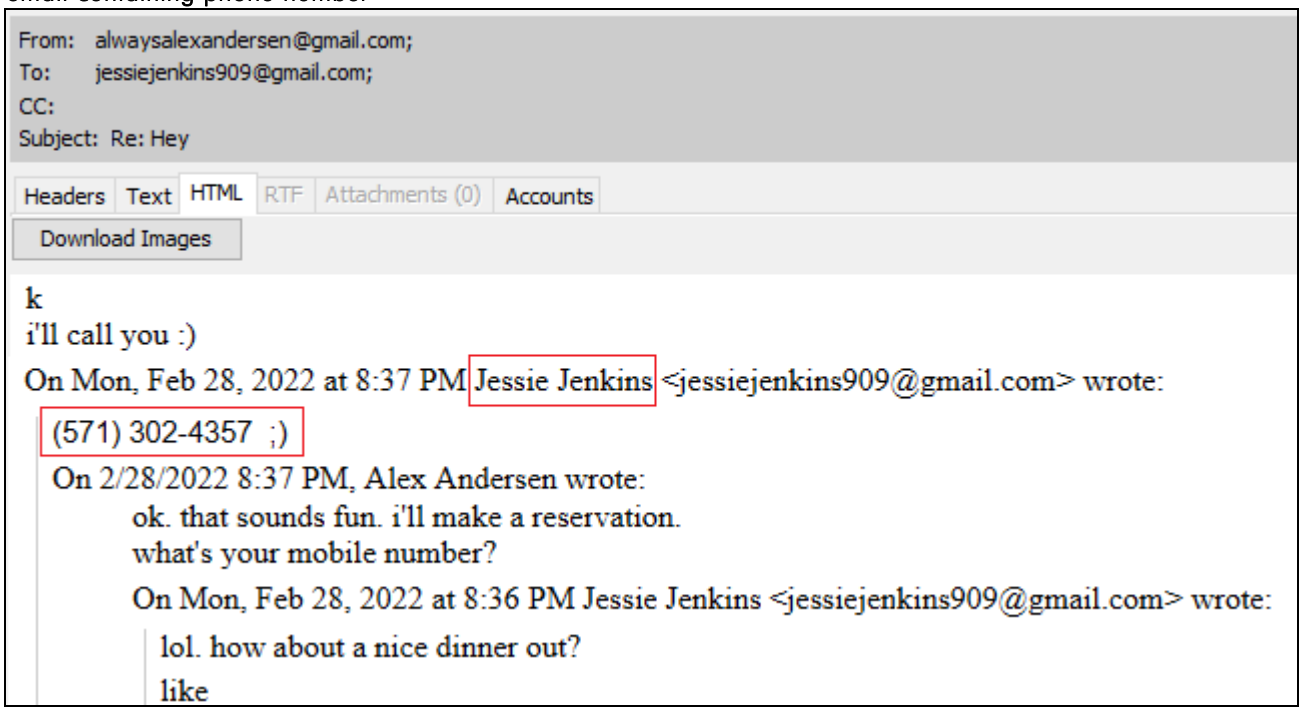
Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 31 - Examination Questions

Expected Response Illustration:

email containing phone number



Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 32 - Examination Questions

Question 32: For the photo that was sent to Jesse [Jessie] Jenkins from John Jenkins, provide the name of the file and the GPS coordinates where the photo was taken. Provide your response in the format: ##.#### N/S, ##.#### E/W

Manufacturer's Expected Response: 18.3626 N, 64.7298 W and other versions representing the same information

WebCode Test	Response
2GYK6H-5562	18.3626472 N 64.729805555555556W
37HZM7-5561	18.3626 N, 64.7298 W
3ERMDL-5562	PXL_20211121_130028206.jpg N 18.3626 W -64.7298
3J2MUJ-5561	File Name: PXL_20211121_130028206.jpg GPS coordinates: 18.362647 N, 64.729806 W
3W8X27-5561	18.3626 N, 64.7298 W
4ELR7K-5562	18.362647, -64.729806
6GRCUL-5562	PXL_20211121_130028206.jpg 18.3626 N/S, -64.7298 E/W
6XRJND-5562	PXL_20211121_130028206.jpg 18.3626, -64.7298
7CPVTB-5561	32 PXL_20211121_130028206.jpg 18.362647 N, -64.729806 W
8PW7XC-5562	PXL_20211121_130028206.jpg, 18.362647 N, 64.729806 W
8YYJXD-5562	The file name is PXL_20211121_130028206.jpg GPS position: 18°21'45.53" N, 64°43'47.3" W
8ZU2ZE-5562	PXL_20211121_130028206.jpg 18.36265 N, 64.72981 W
98A6KL-5561	18.3626 N 64.7298 W
9WRPDD-5562	18°21'45.53" N , 64°43'47.3" W
9ZBF4H-5561	GPSLongitude: -64.729806 West GPSLatitude: 18.362647 North
A7BERC-5562	18.214553 N 64.43473 W
ARP7Q6-5561	18.3626 N -64.7298 W
B6WATE-5561	PXL_20211121_130028206.jpg N 18.3626 W -64.7298

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 32 - Examination Questions	
WebCode Test	**Response**
B9WHYA-5561	PXL_20211121_130028206.jpg, 18.3626 N, 64.7298 W
BN9WG8-5562	PXL_20211121_130028206.jpg -64.729806 N 18.362647 W
BVR2DE-5562	PXL_20211121_130028206.jpg N 18.3626 W -64.7298
BYPLFC-5562	PXL_20211121_130028206.jpg GPS: 18.3626 North 64.7298 West
CMTYN8-5561	PXL_20211121_130028206.jpg 18.36264 N, 64.72980 W
CN44V6-5561	PXL_20211121_130028206.jpg 18.3626 N, 64.7298 W
DHRBK7-5562	"PXL_20211121_130028206.jpg" "18°21'45 N, 64°43'47 W"
E7WKY6-5561	18.3626472 N 64.72980555555556W
E7XH9Z-5561	18.3626 N, -64.7298 W
EAWU6Z-5561	The name of the file is PXL_20211121_130028206.jpg and GPS coordinates are 18.362647 N, 64.729806 W (18.362647, -64.729806)
EREXP8-5561	-64.7298 N/S, 18.3626 E/W
EX67D8-5562	18.3625 N, 64.7297 W
EZEWXB-5561	PXL_20211121_130028206.jpg 18 21 45.529999 N, 64 43 47.299999 W
F2G9Z3-5562	18.362647 N, -64.729806 W
F8L898-5562	PXL_202111121_130028206.jpg 18.3626 N/S, -64.7298 E/W (also displayed as 18" 21' 45N, 64" 43' 47W)
FGDPP2-5562	Latitude: 18.3626 N, Longitude: 64.7298 W
FL36D9-5562	PXL_20211121_130028206.jpg 18.362647 N/S, -64.729806 E/W
FVTQJ7-5562	Filename: PXL_20211121_130028206.jpg GPS Coordinates: 18.362647 N, -64.729806 W
FXXHAY-5561	PXL_20211121_130028206.jpg 18.362647 N -64.729806 W
G8GC37-5561	PXL_20211121_130028206.jpg 18.362647 N, -64.729806 W
GCTZYW-5561	18.36264 N, -64.72980 W

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 32 - Examination Questions	
WebCode Test	**Response**
GFWVHY-5561	PXL_20211121_130028206.jpg, 18.3626 N, 64.7298 W
GLX6QD-5562	PXL_20211121_130028206.jpg 18.3626 N/S, -64.7298 E/W
GR9ZT2-5561	18.3626472 N, 64.7298055 W
HDM36C-5561	PXL_20211121_130028206.jpg 18.3626 N/S, -64.7298 E/W
HDM9G8-5561	PXL_20211121_130028206.jpg 18.3626 N, 64.7298 W
HEVFPY-5561	PXL_20211121_130028206.jpg 18.362647 N, 64.729806 W
HPTDCY-5561	PXL_20211121_130028206.jpg 18.3626 N, 64.7298 W
HWZPPY-5562	PXL_20211121_130028206.jpg, 18.3626 N, 64.7298 W
HX9YL3-5562	PXL_20211121_130028206.jpg and 18.3626 N, 64.7298 W
JEDQ2D-5562	PXL_20211121_130028206.jpg 18°21'45.53" N - 64°43'47.3" W
JQ84YN-5561	PXL_20211121_130028206.jpg 18.3626 N/S, -64.7298 E/W
K4BTM4-5561	PXL_20211121_130028206.jpg 18.3626472222 - -64.7298055556
K9GN9W-5561	PXL_20211121_130028206.jpg 18.362647 N, 64.729806 W
KA2332-5562	PXL_20211121_130028206.jpg 18.362647 N/S, 64.729806 E/W
KDZDY2-5561	-64.7298 N/S, 18.3626 E/W
LTKL96-5562	[Participant did not return results for this question.]
LYVGBT-5561	PXL_20211121_1300282206.jpg
MW334U-5561	PXL_20211121_130028206.jpg 18.362647 N, 64.729806 W
PPRVBV-5561	PXL_20211121_130028206.jpg 18.362647 N, 64.729806 W
PPUJUU-5561	name:PXL_20211121_130028206.jpg; GPS:18.3626 N, 64.7298 W
PQ9R3V-5561	PXL_20211121_130028206.JPG; 64.72980555555556 N/S, 18.36264722222222 E/W

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 32 - Examination Questions	
WebCode Test	**Response**
PRHXH6-5562	PXL_20211121_130028206.jpg 18.36264,-64.72980
PTTY3H-5562	18.36265 N, 64.72980 W
PV4KAY-5561	PXL_20211121_130028206.jpg 18.3626 N, 64.7298 W
PZAFUR-5562	PXL_20211121_130028206.jpg; GPS: 18.2145 N, 64.4347 W
Q8PGRF-5561	name = PXL_20211121_130028206.jpg; Geolocation = 18.36264, -64.72980
QKG3YW-5562	18.3626 N/S, 64.7298 E/W
QLMMJQ-5561	Name: PXL_20211121_130028206.jpg GPS: 18.362647 N 28.63 W
QQ3XWU-5561	PXL_20211121_130028206.jpg, 18.3626 N, 64.7298 W
QVYKR4-5562	PXL_20211121_130028206.jpg 18.3626472222222 N, 64.7298055555556 W
R8KDG3-5562	18.36264 N/S, -64.72980 E/W
RFWD9R-5562	PXL_20211121_130028206.jpg; 18.3626 N, 64.7298 W
RNVVQP-5561	18.3626 N, 64.7298 W
T4JR6P-5562	18.362647 N, 64.729806 W
TA98UW-5561	18.3626, 64.7298
TE2AXW-5561	18.362647 N, 64.729806 W
TWHDG3-5561	Name : PXL_20211121_130028206.jpg GPS : 18°21’45.53”N/S , 64°43’47.3”E/W
URL94P-5562	18.2145 N/S 64.4347 E/W
VKGWHC-5561	PXL_20211121_130028206.jpg: 18.3626 N, 64.7298 W
VRFDXN-5561	18.3626 N -64.7298 W United States Virgin Islands
VU4RLY-5562	18 deg 21' 45.5" N 64 deg 43' 47.30" W
WB6WLF-5561	PXL_20211121_130028206.jpg GPSLongitude: -64.729806 GPSLatitude: 18.362647

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 32 - Examination Questions	
WebCode Test	**Response**
WRDQDP-5562	PXL_20211121_130028206.jpg, 18.36265 N, 64.7298 W
WXJKCR-5562	PXL_20211121_130028206.jpg 18.2145.53 N, 64.4347.3 W
X7U2JR-5561	PXL_20211121_130028206.jpg N 18.3626 W -64.7298
XB3L8N-5562	18.3626, 64.7298
XGEEHM-5561	45.5300 N, 47.3000 W
Y4WCCF-5561	PXL_20211121_130028206.jpg 18.3626 N, 64.7298 W
YDMVRA-5562	[Participant did not return results for this question.]
YE4XXP-5561	18.3626 N, 64.7298 W
YL2H7J-5562	18 deg 21' 45.53" N, 64 deg 43' 47.30" W (Converted Lat 18.362647 - Long -64.729806)
YLG7ZJ-5562	PXL_20211121_130028206.jpg 18.214553 N 64.43473 W
ZD74EJ-5561	The file name is PXL_20211121_130028206.jpg GPS position: 18°21'45.53" N, 64°43'47.3" W
ZDHVAK-5562	PXL_20211121_130028206.jpg 18.36264 N, 64.72980 W
ZG7AXV-5561	PXL_20211121_130028206.jpg; 18.362639, -64.729806
ZLZ4XH-5561	PXL_20211121_130028206.jpg 18.362647 N, 64.729806 W

Question 32: For the photo that was sent to Jesse [Jessie] Jenkins from John Jenkins, provide the name of the file and the GPS coordinates where the photo was taken. Provide your response in the format: ##.#### N/S, ##.#### E/W

Consensus Result:

18.3626 N, 64.7698 W and other versions representing the same information. Although, the file name was also requested in this question, 27% of participants did not report this information therefore consensus was determined based solely on GPS coordinates.

Expected Response Explanation:

On March 4, 2022, Jessie Jenkins received an email from John Jenkins containing an attached photo, PXL_20211121_130028206.jpg. Parsing this file with a tool like Exiftool will reveal the embedded GPS EXIF metadata.

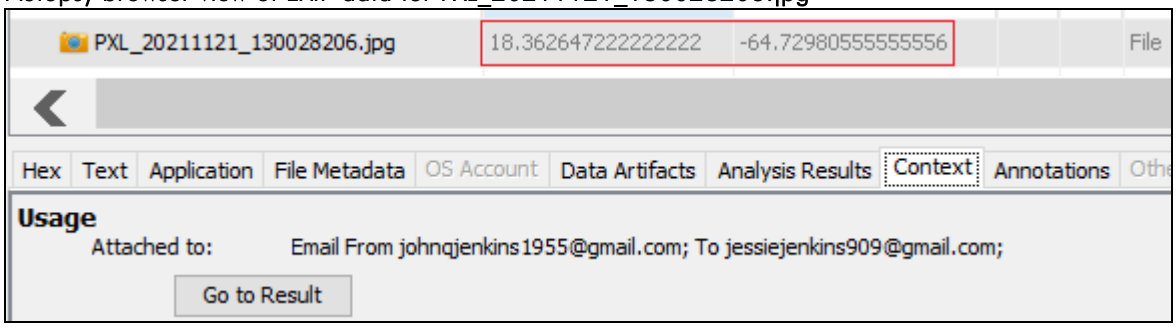
Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

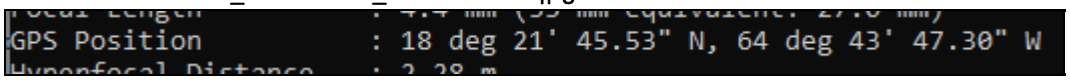
Question 32 - Examination Questions

Expected Response Illustration:

Autopsy browser view of EXIF data for PXL_20211121_130028206.jpg



Exiftool view of PXL_20211121_130028206.jpg



Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 33 - Removable Media 22-5562

Question 33: Provide the SHA256 hash for the USB device.

Manufacturer's Expected Response: D7C4034A6A0EB86785B61EAFF1869CBDA440B01FAD959EBF8A1FE89384327D12

WebCode Test	Response ** Inconsistencies not highlighted; No consensus achieved **
2GYK6H-5562	d7c4034a6a0eb86785b61eaff1869cbda440b01fad959ebf8a1fe89384327d12
3ERMDL-5562	698EB400D0436D8546AC8845AC6C8027133E4C45FE82E9EFB6E4FB9819B80F2D
4ELR7K-5562	222CB05BE57CB79AFBC42797ADD1EFDB6CD2FC54C70A012778FA15F2952E3BCA
6GRCUL-5562	d7c4034a6a0eb86785b61eaff1869cbda440b01fad959ebf8a1fe89384327d12
6XRJND-5562	D7C4034A6A0EB86785B61EAFF1869CBDA440B01FAD959EBF8A1FE89384327D12
8PW7XC-5562	D7C4034A6A0EB86785B61EAFF1869CBDA440B01FAD959EBF8A1FE89384327D12
8YYJXD-5562	5957b58bce2e575d862a1787433330806cec2f70b84aad816f07405f3a5b3565
8ZU2ZE-5562	D7C4034A6A0EB86785B61EAFF1869CBDA440B01FAD959EBF8A1FE89384327D12
9WRPDD-5562	d7c4034a6a0eb86785b61eaff1869cbda440b01fad959ebf8a1fe89384327d12
A7BERC-5562	D7C4034A6A0EB86785B61EAFF1869CBDA440B01FAD959EBF8A1FE89384327D12
BN9WG8-5562	D7C4034A6A0EB86785B61EAFF1869CBDA440B01FAD959EBF8A1FE89384327D12
BVR2DE-5562	698EB400D0436D8546AC8845AC6C8027133E4C45FE82E9EFB6E4FB9819B80F2D
BYPLFC-5562	778559d20966e9fe1abd8db22e656e63d9e6d7035e82b905fbcae3709420a4bd
DHRBK7-5562	d7c4034a6a0eb86785b61eaff1869cbda440b01fad959ebf8a1fe89384327d12
EX67D8-5562	d7c4034a6a0eb86785b61eaff1869cbda440b01fad959ebf8a1fe89384327d12
F2G9Z3-5562	d7c4034a6a0eb86785b61eaff1869cbda440b01fad959ebf8a1fe89384327d12
F8L898-5562	D7C4034A6A0EB86785B61EAFF1869CBDA440B01FAD959EBF8A1FE89384327D12
FGDPP2-5562	d7c4034a6a0eb86785b61eaff1869cbda440b01fad959ebf8a1fe89384327d12
FL36D9-5562	c7d4e22386d105d8a4c707a75392b4b933d43684e2068d0238084bf8be3fc19e

Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 33 - Removable Media 22-5562		
WebCode Test	**Response**	** Inconsistencies not highlighted; No consensus achieved **
FVTQJ7-5562	D7C4034A6A0EB86785B61EAFF1869CBDA440B01FAD959EBF8A1FE89384327D12	
GLX6QD-5562	d7c4034a6a0eb86785b61eaff1869cbda440b01fad959ebf8a1fe89384327d12	
HWZPPY-5562	d7c4034a6a0eb86785b61eaff1869cbda440b01fad959ebf8a1fe89384327d12	
HX9YL3-5562	1E057345261DF727754588F5994B4EF2F032CF6F22E463BE0B5CE5D9B0A3A281	
JEDQ2D-5562	D7C4034A6A0EB86785B61EAFF1869CBDA440B01FAD959EBF8A1FE89384327D12	
KA2332-5562	C89FADEEE568B3C9F475C5ED2597B468B09C41743FCD68987F96D125D1A10257	
LTKL96-5562	SHA256: D7C4034A6A0EB86785B61EAFF1869CBDA440B01FAD959EBF8A1FE89384327D12	
PRHXH6-5562	We do not capture the SHA256 hash for devices that we image. We capture the SHA1 and MD5 hashes.	
PTTY3H-5562	d7c4034a6a0eb86785b61eaff1869cbda440b01fad959ebf8a1fe89384327d12	
PZAFUR-5562	74B10D67F95F380E3138C74704113093331191641FA1DEDB7DCF2724CF138347	
QKG3YW-5562	ee01 0683 abe2 7680 db63 4fd1 aa00 aea4 9382 0ef0 57c1 dee7 d528 fa55 f123 d85c	
QVYKR4-5562	532405FD1A7DC69491231ADB3566E2A091C0829E5BA39302AF505C6932210C8A	
R8KDG3-5562	D7C4034A6A0EB86785B61EAFF1869CBDA440B01FAD959EBF8A1FE89384327D12	
RFWD9R-5562	D7C4034A6A0EB86785B61EAFF1869CBDA440B01FAD959EBF8A1FE89384327D12	
T4JR6P-5562	d7c4034a6a0eb86785b61eaff1869cbda440b01fad959ebf8a1fe89384327d12	
URL94P-5562	EFF95E55FE634C21D3C564B4ABDC2E3EAA8A7E96BBF9F19D6DEC0C430C655715	
VU4RLY-5562	60741d61add2e1e1f4f1448dd6648ecd9f8c8879	
WRDQDP-5562	d7c4034a6a0eb86785b61eaff1869cbda440b01fad959ebf8a1fe89384327d12	
WXJKCR-5562	D7C4034A6A0EB86785B61EAFF1869CBDA440B01FAD959EBF8A1FE89384327D12	
XB3L8N-5562	D7C4034A6A0EB86785B61EAFF1869CBDA440B01FAD959EBF8A1FE89384327D12	
YDMVRA-5562	5fd75e91b2521dfc35dcae91cde2a74fb21851bb7cb741a9aa790fadebed9ee4	

Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 33 - Removable Media 22-5562		
WebCode Test	**Response**	** Inconsistencies not highlighted; No consensus achieved **
YL2H7J-5562	D7C4034A6A0EB86785B61EAFF1869CBDA440B01FAD959EBF8A1FE89384327D12	
YLG7ZJ-5562	fec6 3953 a903 a3c2 07ea 0216 609d 6538 23a5 e748 e35f 1aa4 b5d6 19fe 736a e5f9	
ZDHVAK-5562	D7C4034A6A0EB86785B61EAFF1869CBDA440B01FAD959EBF8A1FE89384327D12	

Question 33: Provide the SHA256 hash for the USB device.

Consensus Result:

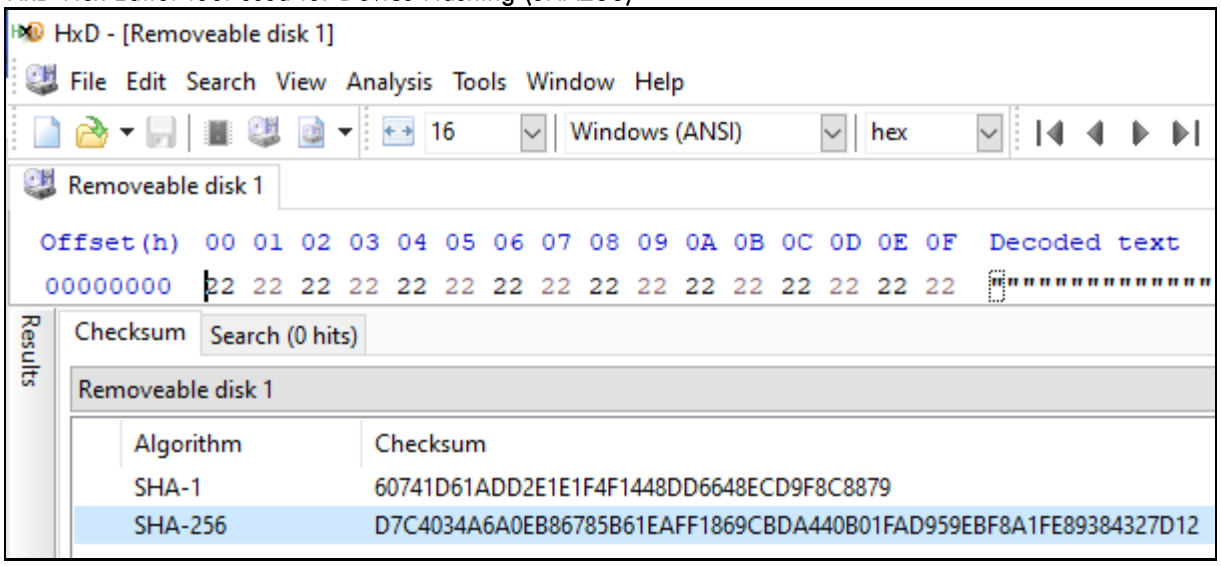
While the majority of participants (67%) reported the expected SHA256 hash of d7c4034a6a0eb86785b61eaff1869cbda440b01fad959ebf8a1fe89384327d12, a concensus was not achieved for this question.

Expected Response Explanation:

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

Expected Response Illustration:

HxD Hex Editor tool used for Device Hashing (SHA256)



Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 34 - Removable Media 22-5562

Question 34: How many ACTIVE partitions are on the device? Provide a NUMERIC response.

Manufacturer's Expected Response: 1

WebCode Test	Response	** Inconsistencies not highlighted; No consensus achieved **
2GYK6H-5562	1	
3ERMDL-5562	2	
4ELR7K-5562	2	
6GRCUL-5562	1	
6XRJND-5562	1	
8PW7XC-5562	1	
8YYJXD-5562	2	
8ZU2ZE-5562	1	
9WRPDD-5562	1	
A7BERC-5562	1	
BN9WG8-5562	0	
BVR2DE-5562	2	
BYPLFC-5562	1	
DHRBK7-5562	[Participant did not return results for this question.]	
EX67D8-5562	1	
F2G9Z3-5562	1	
F8L898-5562	1	
FGDPP2-5562	0	
FL36D9-5562	1	

Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 34 - Removable Media 22-5562		
WebCode Test	**Response**	** Inconsistencies not highlighted; No consensus achieved **
FVTQJ7-5562	1	
GLX6QD-5562	1	
HWZPPY-5562	0	
HX9YL3-5562	1	
JEDQ2D-5562	1	
KA2332-5562	1	
LTKL96-5562	1	
PRHXH6-5562	1	
PTTY3H-5562	1	
PZAFUR-5562	2	
QKG3YW-5562	2	
QVYKR4-5562	2	
R8KDG3-5562	1	
RFWD9R-5562	1	
T4JR6P-5562	2	
URL94P-5562	2	
VU4RLY-5562	1	
WRDQDP-5562	1	
WXJKCR-5562	1	
XB3L8N-5562	1	
YDMVRA-5562	[Participant did not return results for this question.]	

Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 34 - Removable Media 22-5562		
WebCode Test	**Response**	** Inconsistencies not highlighted; No consensus achieved **
YL2H7J-5562	2	
YLG7ZJ-5562	1	
ZDHVAK-5562	0	

Question 34: How many ACTIVE partitions are on the device? Provide a NUMERIC response.

Consensus Result:

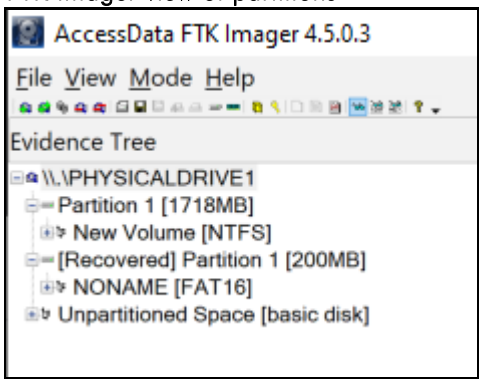
While a majority of participants (66%) reported the expected response of "1", a consensus was not achieved. Another 24% of participants reported "2" for the number of active partitions. One of the device's partitions was deleted, therefore no longer active.

Expected Response Explanation:

The number of device partitions can be determined by reviewing the partition table with most forensic suites or imaging tools. This device has two partitions, but one has been deleted.

Expected Response Illustration:

FTK Imager view of partitions



EnCase Report of Drive Geometry

Partitions

Name	Id	Type	Start Sector	Total Sectors	Size
	07	NTFS	128	3,518,464	1.7 GB

Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 35 - Removable Media 22-5562

Question 35: What is the volume serial number of the NTFS partition (The first 4 bytes (little endian)) as it would be reported/displayed by Windows?

Manufacturer's Expected Response: 2469-CE18

WebCode Test	Response
2GYK6H-5562	2469CE18
3ERMDL-5562	1E9A
4ELR7K-5562	18 CE 69 24
6GRCUL-5562	2469
6XRJND-5562	2469CE18
8PW7XC-5562	2469-CE18
8YYJXD-5562	2469-CE18
8ZU2ZE-5562	2469-CE18
9WRPDD-5562	2469-CE18
A7BERC-5562	24 69 CE 18
BN9WG8-5562	2469-CE18
BVR2DE-5562	1E9A
BYPLFC-5562	2469CE18
DHRBK7-5562	2469CE18
EX67D8-5562	2469CE18
F2G9Z3-5562	2469CE18
F8L898-5562	2469-CE18
FGDPP2-5562	2469-CE18
FL36D9-5562	[Participant did not return results for this question.]

Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 35 - Removable Media 22-5562	
WebCode Test	**Response**
FVTQJ7-5562	2469CE18
GLX6QD-5562	2469-CE18
HWZPPY-5562	2469CE18
HX9YL3-5562	2469CE18
JEDQ2D-5562	18 CE 69 24
KA2332-5562	24 69 CE 18
LTKL96-5562	2469-CE18
PRHXH6-5562	2469
PTTY3H-5562	2469-CE18
PZAFUR-5562	2469-CE18
QKG3YW-5562	5C 24 69 F0
QVYKR4-5562	2469CE18
R8KDG3-5562	2469-CE18
RFWD9R-5562	2469-CE18
T4JR6P-5562	24 69 CE 18
URL94P-5562	2469-CE18
VU4RLY-5562	2469CE18
WRDQDP-5562	2469-CE18
WXJKCR-5562	2469
XB3L8N-5562	2469-CE18
YDMVRA-5562	[Participant did not return results for this question.]

Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 35 - Removable Media 22-5562	
WebCode Test	**Response**
YL2H7J-5562	2469CE18
YLG7ZJ-5562	24 69 CE 18
ZDHVAK-5562	35AF-FF00

Question 35: What is the volume serial number of the NTFS partition (The first 4 bytes (little endian)) as it would be reported/displayed by Windows?

Consensus Result:

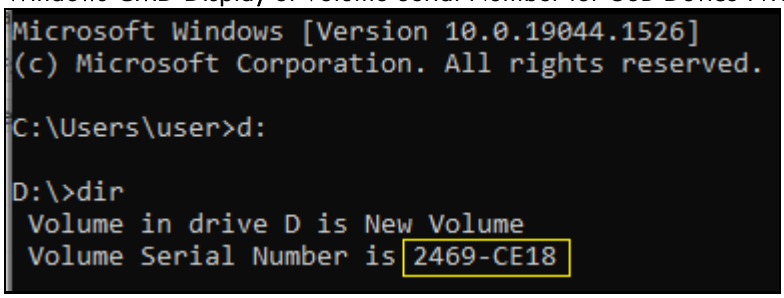
2469-CE18

Expected Response Explanation:

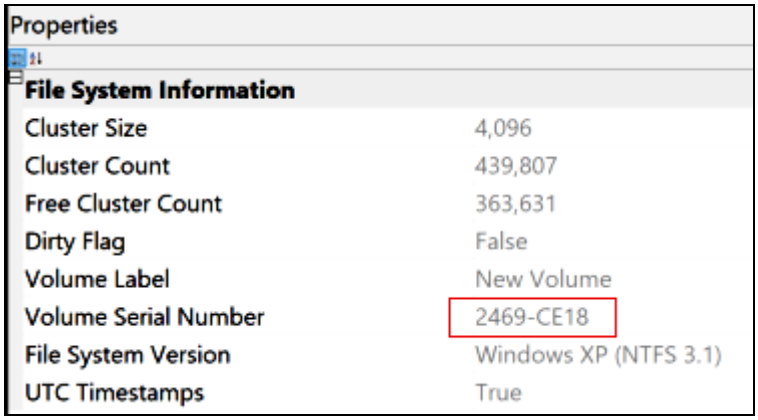
Most forensic tools will parse and display the volume serial number value. It can also be displayed by the operating system for a mounted volume.

Expected Response Illustration:

Windows CMD Display of Volume Serial Number for USB Device NTFS Partition



FTK Imager Display of Volume Serial Number for USB Device NTFS Partition



Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 36 - Removable Media 22-5562

Question 36: What is the name (Volume Label) of the NTFS Partition?

Manufacturer's Expected Response: New Volume

WebCode Test	Response
2GYK6H-5562	New Volume
3ERMDL-5562	New Volume
4ELR7K-5562	New Volume
6GRCUL-5562	New Volume
6XRJND-5562	New Volume
8PW7XC-5562	New Volume
8YYJXD-5562	New Volume
8ZU2ZE-5562	New Volume
9WRPDD-5562	New Volume
A7BERC-5562	NEW Volume
BN9WG8-5562	New Volume
BVR2DE-5562	New Volume
BYPLFC-5562	New Volume
DHRBK7-5562	New Volume
EX67D8-5562	New Volume
F2G9Z3-5562	New Volume
F8L898-5562	New Volume
FGDPP2-5562	New Volume
FL36D9-5562	New Volume

Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 36 - Removable Media 22-5562	
WebCode Test	**Response**
FVTQJ7-5562	New Volume
GLX6QD-5562	New Volume
HWZPPY-5562	New Volume
HX9YL3-5562	New Volume
JEDQ2D-5562	New Volume
KA2332-5562	New Volume
LTKL96-5562	New Volume
PRHXH6-5562	New Volume
PTTY3H-5562	New Volume
PZAFUR-5562	New Volume
QKG3YW-5562	New Volume
QVYKR4-5562	New Volume
R8KDG3-5562	New Volume
RFWD9R-5562	New Volume
T4JR6P-5562	New Volume
URL94P-5562	New Volume
VU4RLY-5562	New Volume
WRDQDP-5562	New Volume
WXJKCR-5562	New Volume
XB3L8N-5562	New Volume
YDMVRA-5562	[Participant did not return results for this question.]

Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 36 - Removable Media 22-5562	
WebCode Test	**Response**
YL2H7J-5562	New Volume
YLG7ZJ-5562	New Volume
ZDHVAK-5562	New Volume

Question 36: What is the name (Volume Label) of the NTFS Partition?

Consensus Result:

New Volume

Expected Response Explanation:

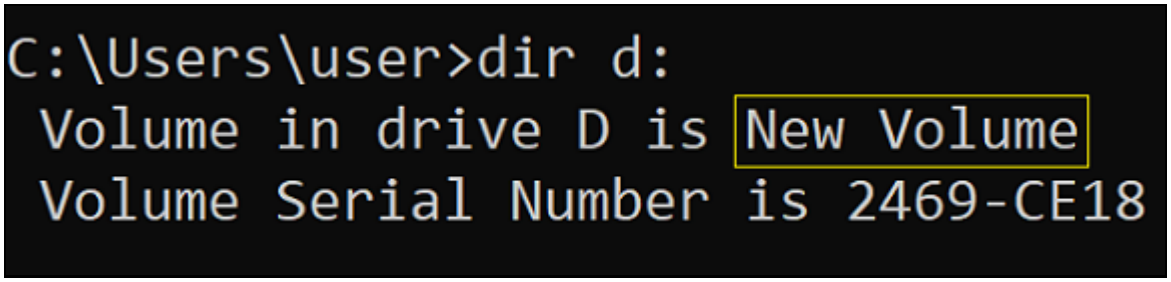
NTFS volumes can have a name. The Windows operating system will display this, as well as many forensic tools.

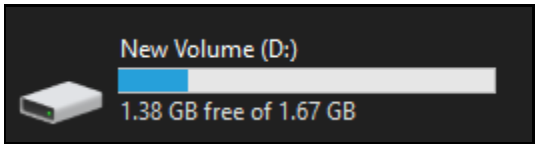
Expected Response Illustration:

EnCase drive information report

Volume	
File System	NTFS
Sectors per cluster	8
Bytes per sector	512
Total Sectors	3,518,464
Total Capacity	1,801,449,472 Bytes (1.7 GB)
Total Clusters	439,807
Unallocated	1,489,432,576 Bytes (1.4 GB)
Free Clusters	363,631
Allocated	312,016,896 Bytes (297.6 MB)
Volume Name	New Volume
Volume Offset	128
Drive Type	Fixed

Windows CMD and Explorer Display of Volume name for USB Device NTFS Partition





Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 37 - Removable Media 22-5562

Question 37: What text is visible in the photo file containing six cats/kittens?

Manufacturer's Expected Response: LMAO

WebCode Test	Response
2GYK6H-5562	LMAO
3ERMDL-5562	LMAO
4ELR7K-5562	LMAO
6GRCUL-5562	LMAO
6XRJND-5562	LMAO
8PW7XC-5562	LMAO
8YYJXD-5562	the text is (LMAO)
8ZU2ZE-5562	LMAO
9WRPDD-5562	LMAO
A7BERC-5562	LAMO
BN9WG8-5562	LMAO
BVR2DE-5562	LMAO
BYPLFC-5562	LMAO
DHRBK7-5562	LMAO
EX67D8-5562	LMAO
F2G9Z3-5562	LMAO
F8L898-5562	LMAO
FGDPP2-5562	LMAO
FL36D9-5562	LMAO

Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 37 - Removable Media 22-5562	
WebCode Test	**Response**
FVTQJ7-5562	LMAO
GLX6QD-5562	LMAO
HWZPPY-5562	LMAO
HX9YL3-5562	LMAO
JEDQ2D-5562	LMAO
KA2332-5562	LMAO
LTKL96-5562	LMAO
PRHXH6-5562	LMAO
PTTY3H-5562	LMAO
PZAFUR-5562	Das Otterhaus Http:// Blog Kohan - Studio.com/
QKG3YW-5562	LMAO
QVYKR4-5562	LMAO
R8KDG3-5562	LMAO
RFWD9R-5562	LMAO
T4JR6P-5562	LMAO
URL94P-5562	LMAO
VU4RLY-5562	LMAO
WRDQDP-5562	LMAO
WXJKCR-5562	LMAO
XB3L8N-5562	LMAO
YDMVRA-5562	[Participant did not return results for this question.]

Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 37 - Removable Media 22-5562	
WebCode Test	**Response**
YL2H7J-5562	LMAO
YLG7ZJ-5562	LMAO
ZDHVAK-5562	LMAO

Question 37: What text is visible in the photo file containing six cats/kittens?

Consensus Result:

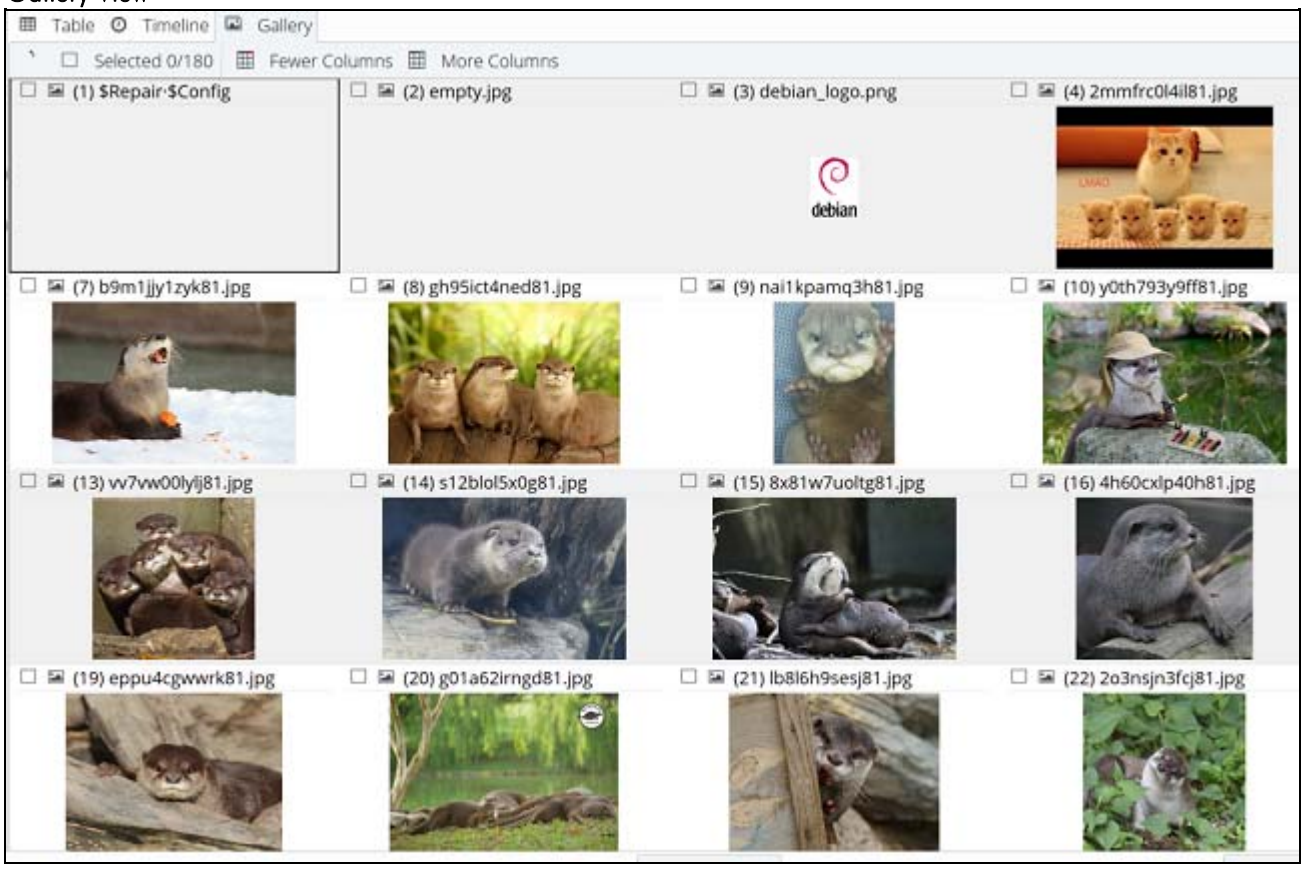
LMAO

Expected Response Explanation:

There is one jpeg (.jpg) file on the device containing an image of six cats. It is on the deleted partition. To find this file, the partition must be recovered or the unused disk space carved.

Expected Response Illustration:

Gallery View



Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 37 - Removable Media 22-5562

2mmfrc0l4il81.jpg

Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 38 - Removable Media 22-5562

Question 38: What is the file TYPE of the file with SHA-1 hash 613cd9e96da949694014ccf77e63005cb99d7d49?

Manufacturer's Expected Response: JPEG, JPG or JFIF

WebCode Test	Response
2GYK6H-5562	File TYPE: JPEG, How did you determine the file TYPE?: FFD8FFE0 (jpg signature)
3ERMDL-5562	File TYPE: Picture (Image), How did you determine the file TYPE?: From the file extension, which is JPG (find it in the Meta data which was given by the tool that I'm using)
4ELR7K-5562	File TYPE: JPG, How did you determine the file TYPE?: File Header
6GRCUL-5562	File TYPE: JPEG, How did you determine the file TYPE?: File header signature
6XRJND-5562	File TYPE: jpg, How did you determine the file TYPE?: extension mismatch detected (not a .sys file)
8PW7XC-5562	File TYPE: JPG image, How did you determine the file TYPE?: By File Header and Footer
8YYJXD-5562	File TYPE: Jpg, How did you determine the file TYPE?: File Header: FF D8 FF
8ZU2ZE-5562	File TYPE: JPG, How did you determine the file TYPE?: File header FF D8 FF following missmatch
9WRPDD-5562	File TYPE: Archivo de imagen (JFIF), How did you determine the file TYPE?: Por la cabecera del archivo. (4A 46 49 46)
A7BERC-5562	File TYPE: jpg, JPEG, How did you determine the file TYPE?: Signature Analysis FF D8 FF
BN9WG8-5562	File TYPE: JPG, How did you determine the file TYPE?: Looked at the file header
BVR2DE-5562	File TYPE: Picture (Image), How did you determine the file TYPE?: From the file extension, which is JPG (find it in the Meta data which was given by the tool that I'm using)
BYPLFC-5562	File TYPE: JPEG, How did you determine the file TYPE?: looking at the file header in HEX ie ÿØÿà..JFIF
DHRBK7-5562	File TYPE: JPG, How did you determine the file TYPE?: We look at the file signature (header information) to determine the file type.
EX67D8-5562	File TYPE: .jpeg/.jfif, How did you determine the file TYPE?: The header of the file: 0x FF D8 FF E0 00 10 4A 46 49 46 00
F2G9Z3-5562	File TYPE: .JPG, How did you determine the file TYPE?: file header is FF D8 FF E0 (JPG file header)
F8L898-5562	File TYPE: .JPG, How did you determine the file TYPE?: Ran file signature analysis over the file. Checked the hexadecimal of the file header.

Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 38 - Removable Media 22-5562	
WebCode Test	**Response**
FGDPP2-5562	File TYPE: JPEG, How did you determine the file TYPE?: File Header / Signature
FL36D9-5562	File TYPE: JPEG, How did you determine the file TYPE?: View file source and view hex – File header
FVTQJ7-5562	File TYPE: JFIF, How did you determine the file TYPE?: Identified the file header FF D8 FF E0 00 10 4A 46 in the hex viewer
GLX6QD-5562	File TYPE: Image, How did you determine the file TYPE?: Signature Analysis
HWZPPY-5562	File TYPE: JPEG Image Standard, How did you determine the file TYPE?: File header information & EnCase display of file type
HX9YL3-5562	File TYPE: JPEG, How did you determine the file TYPE?: Viewing the hex header, 0xFFD8FFE0, was observed which indicates it is a JPEG file.
JEDQ2D-5562	File TYPE: displayed as .sys but is in fact a .jpg, How did you determine the file TYPE?: examination of the HEX data in the file header = ÿØÿà
KA2332-5562	File TYPE: JPG, How did you determine the file TYPE?: The file signature is for JPG
LTKL96-5562	File TYPE: jpg, How did you determine the file TYPE?: File signature JFIF (0xFFD8FFE000).
PRHXH6-5562	File TYPE: JPEG picture file, How did you determine the file TYPE?: X-Ways v19.8 SR-13 indicates that the type status of the file is a mismatch. The file type is shown as 'jpg' yet the file extension is 'sys'. File header also shows YOYA JFIF' which confirms that the file is a JPG file. Viewing the file also shows that it is a jpg file of an otter lying on its back.
PTTY3H-5562	File TYPE: JPEG, How did you determine the file TYPE?: File's header corresponding to a JPEG file: 0xFF D8 FF
PZAFUR-5562	File TYPE: JPEG Image Standard - Filename: 230d3seoaff81.sys, How did you determine the file TYPE?: Signature Analysis
QKG3YW-5562	File TYPE: jpg, How did you determine the file TYPE?: Looked at the header for the file which was the header for a 'jpg' file, FF D8 FF E0
QVYKR4-5562	File TYPE: image file, How did you determine the file TYPE?: Defined in HEX as 'yoya JFIF' - this is an image file.
R8KDG3-5562	File TYPE: Picture (.jpg), How did you determine the file TYPE?: file signature analysis (mismatch detected)
RFWD9R-5562	File TYPE: JPEG, How did you determine the file TYPE?: For the file signature (0xFFD8FFE000104A46494600)
T4JR6P-5562	File TYPE: jpeg image, How did you determine the file TYPE?: Reading the File Header (FF D8 FF E0)
URL94P-5562	File TYPE: .jpg, How did you determine the file TYPE?: File Header Hex xFF xD8 xFF xE0
VU4RLY-5562	File TYPE: JPEG, How did you determine the file TYPE?: File header contains FF D8 FF, denotes start of jpeg

Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 38 - Removable Media 22-5562	
WebCode Test	**Response**
WRDQDP-5562	File TYPE: JPEG, How did you determine the file TYPE?: Utilizing a digital forensic program's category type then verifying it using a program which determine file type by three sets of tests, performed in this order: filesystem tests, magic tests (/usr/share/misc/magic.mgc){which includes file signature matches}, and language tests.
WXJKCR-5562	File TYPE: jpg, How did you determine the file TYPE?: Type column in X-Ways, checked header
XB3L8N-5562	File TYPE: JPG, How did you determine the file TYPE?: This File's Signature(Header) is FF D8 FF E0 (Signature(Footer): FF D9). This Signature means JPG
YDMVRA-5562	[Participant did not return results for this question.]
YL2H7J-5562	File TYPE: .jpg, How did you determine the file TYPE?: File header was FFD8 and file footer was FFD9 (These headers relates to .jpg file types)
YLG7ZJ-5562	File TYPE: image, How did you determine the file TYPE?: file signature in hex is FF D8 FF E0
ZDHVAK-5562	File TYPE: .jpg, How did you determine the file TYPE?: Viewed file signature in hex = FFD8FFE0

Question 38: What is the file TYPE of the file with SHA-1 hash 613cd9e96da949694014ccf77e63005cb99d7d49?

Consensus Result:

JPEG, JPG or JFIF

Expected Response Explanation:

The file with hash 613cd9e96da949694014ccf77e63005cb99d7d49 is z30d3swoaff81.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 FF D8 FF E0 00 10 4A 46 49 46 (ÿØÿà··JFIF), the identifier for a jpeg file.

Expected Response Illustration:

EnCase table and view panes showing hash, name, and filetype for z30d3swoaff81.sys

SHA1	Name	File Type
613cd9e96da949694014ccf77e63005cb99d7d49	z30d3swoaff81.sys	JPEG Image Standard

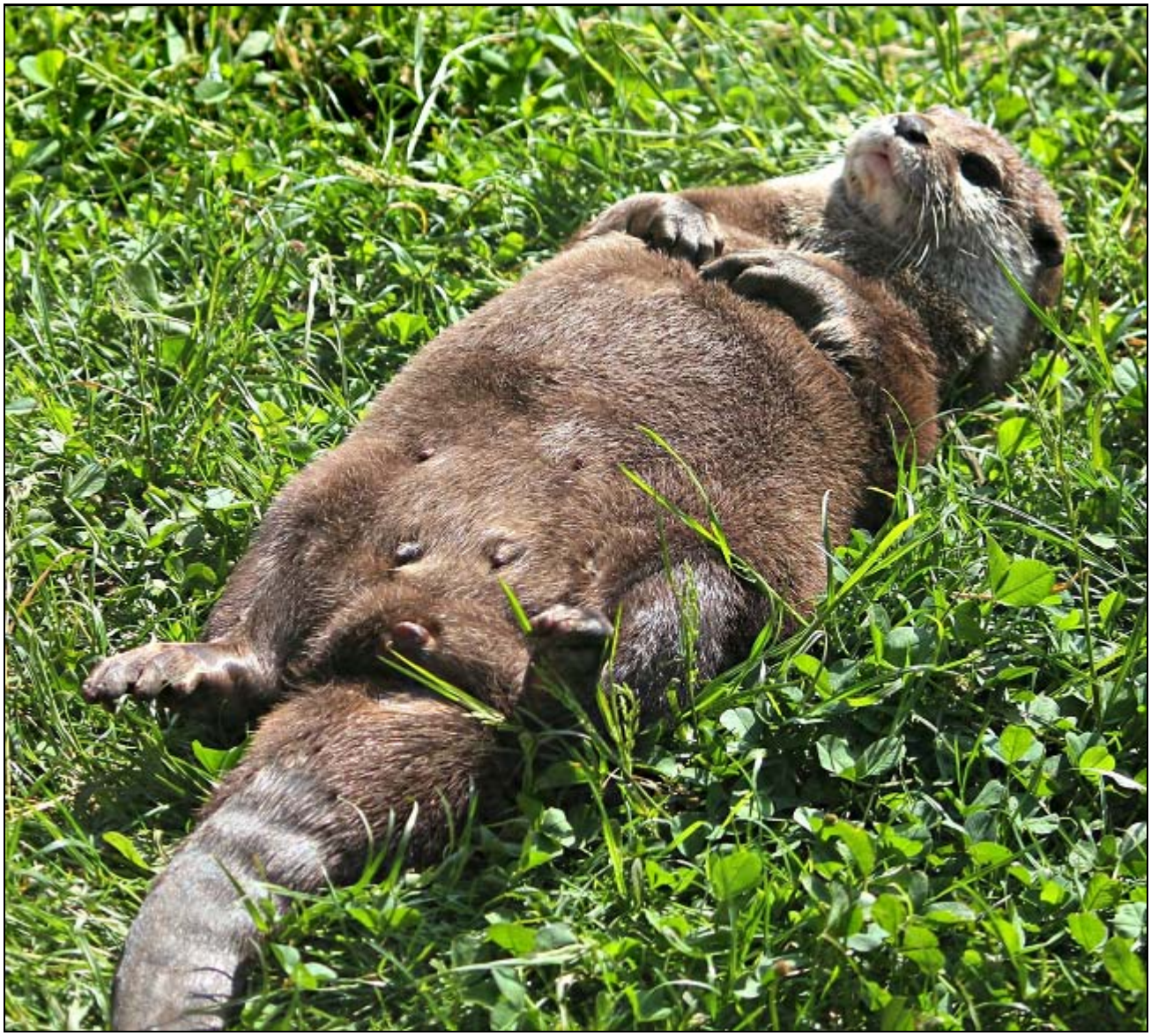
Hex view of z30d3swoaff81.sys header

Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 38 - Removable Media 22-5562

z30d3swoaff81.sys



Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 39 - Removable Media 22-5562

Question 39: Provide the SHA256 hash of the file named default_wallet (not default_wallet.backup).

Manufacturer's Expected Response: 20649e413c8dbe9f2248dbf6cc74eb39f9489ec17d7e4004f4df69c7e8e10848

WebCode Test	Response ** Inconsistencies not highlighted; No consensus achieved **
2GYK6H-5562	20649e413c8dbe9f2248dbf6cc74eb39f9489ec17d7e4004f4df69c7e8e10848
3ERMDL-5562	20649E413C8DBE9F2248DBF6CC74EB39F9489EC17D7E4004F4DF69C7E8E10848
4ELR7K-5562	EAD7C2B57778F90AF8114C133A572A6B405729D2AA30CFDFA6D4713BF874825D
6GRCUL-5562	20649E413C8DBE9F2248DBF6CC74EB39F9489EC17D7E4004F4DF69C7E8E10848
6XRJND-5562	20649E413C8DBE9F2248DBF6CC74EB39F9489EC17D7E4004F4DF69C7E8E10848
8PW7XC-5562	20649E413C8DBE9F2248DBF6CC74EB39F9489EC17D7E4004F4DF69C7E8E10848
8YYJXD-5562	a134f088af259f797cd795187f5a8a6c8cf64718926ca2608104ef05caa9bde6
8ZU2ZE-5562	01f2e0966873b4cf54a89eea4b951a15bf91b9316374919ee51511e7d90418ca
9WRPDD-5562	20649e413c8dbe9f2248dbf6cc74eb39f9489ec17d7e4004f4df69c7e8e10848
A7BERC-5562	20649E413C8DBE9F2248DBF6CC74EB39F9489EC17D7E4004F4DF69C7E8E10848
BN9WG8-5562	01f2e0966873b4cf54a89eea4b951a15bf91b9316374919ee51511e7d90418ca
BVR2DE-5562	20649E413C8DBE9F2248DBF6CC74EB39F9489EC17D7E4004F4DF69C7E8E10848
BYPLFC-5562	20649e413c8dbe9f2248dbf6cc74eb39f9489ec17d7e4004f4df69c7e8e10848
DHRBK7-5562	879d92683784d45287211c089746393c95dd5e6056ab49b6e62f162f6ce71ff8
EX67D8-5562	20649e413c8dbe9f2248dbf6cc74eb39f9489ec17d7e4004f4df69c7e8e10848
F2G9Z3-5562	01f2e0966873b4c54a89eea4b951a15bf91b9316374919ee51511e7d90418ca
F8L898-5562	There are two files bearing the name 'default_wallet' – one on the USB device and one on the supplied forensic image: SHA-256 for file on USB stick - 20649e413c8dbe9f2248dbf6cc74eb39f9489ec17d7e4004f4df69c7e8e10848 SHA-256 for file on E01 - 01f2e0966873b4cf54a89eea4b951a15bf91b9316374919ee51511e7d90418ca
FGDPP2-5562	20649e413c8dbe9f2248dbf6cc74eb39f9489ec17d7e4004f4df69c7e8e10848

Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 39 - Removable Media 22-5562		
WebCode Test	**Response**	** Inconsistencies not highlighted; No consensus achieved **
FL36D9-5562	20649E413C8DBE9F2248DBF6CC74EB39F9489EC17D7E4004F4DF69C7E8E10848	
FVTQJ7-5562	20649E413C8DBE9F2248DBF6CC74EB39F9489EC17D7E4004F4DF69C7E8E10848	
GLX6QD-5562	File name not found on the USB media. Named file is present on the computer with the SHA256 Hash of - 01f2e0966873b4cf54a89eea4b951a15bf91b9316374919ee51511e7d90418ca	
HWZPPY-5562	20649e413c8dbe9f2248dbf6cc74eb39f9489ec17d7e4004f4df69c7e8e10848	
HX9YL3-5562	20649e413c8dbe9f2248dbf6cc74eb39f9489ec17d7e4004f4df69c7e8e10848	
JEDQ2D-5562	6BCA3E8F386C9929BE7278BE078FB9B54C9FC62431431C9311466AFBC6754357	
KA2332-5562	20649E413C8DBE9F2248DBF6CC74EB39F9489EC17D7E4004F4DF69C7E8E10848	
LTKL96-5562	SHA256: 20649E413C8DBE9F2248DBF6CC74EB39F9489EC17D7E4004F4DF69C7E8E10848	
PRHXH6-5562	20649E413C8DBE9F2248DBF6CC74EB39F9489EC17D7E4004F4DF69C7E8E10848	
PTTY3H-5562	20649e413c8dbe9f2248dbf6cc74eb39f9489ec17d7e4004f4df69c7e8e10848	
PZAFUR-5562	A134F088AF259F797CD795187F5A8A6C8CF64718926CA2608104EF05CAA9BDE6	
QKG3YW-5562	20649e413c8dbe9f2248dbf6cc74eb39f9489ec17d7e4004f4df69c7e8e10848	
QVYKR4-5562	20649E413C8DBE9F2248DBF6CC74EB39F9489EC17D7E4004F4DF69C7E8E10848	
R8KDG3-5562	20649E413C8DBE9F2248DBF6CC74EB39F9489EC17D7E4004F4DF69C7E8E10848	
RFWD9R-5562	20649e413c8dbe9f2248dbf6cc74eb39f9489ec17d7e4004f4df69c7e8e10848	
T4JR6P-5562	20649E413C8DBE9F2248DBF6CC74EB39F9489EC17D7E4004F4DF69C7E8E10848	
URL94P-5562	20649E413C8DBE9F2248DBF6CC74EB39F9489EC17D7E4004F4DF69C7E8E10848	
VU4RLY-5562	01f2e0966873b4cf54a89eea4b951a15bf91b9316374919ee51511e7d90418ca	
WRDQDP-5562	20649e413c8dbe9f2248dbf6cc74eb39f9489ec17d7e4004f4df69c7e8e10848	
WXJKCR-5562	20649E413C8DBE9F2248DBF6CC74EB39F9489EC17D7E4004F4DF69C7E8E10848	
XB3L8N-5562	20649E413C8DBE9F2248DBF6CC74EB39F9489EC17D7E4004F4DF69C7E8E10848	

Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 39 - Removable Media 22-5562		
WebCode Test	**Response**	** Inconsistencies not highlighted; No consensus achieved **
YDMVRA-5562	[Participant did not return results for this question.]	
YL2H7J-5562	a134f088af259f797cd795187f5a8a6c8cf64718926ca2608104ef05caa9bde6	
YLG7ZJ-5562	01f2e0966873b4cf54a89eea4b951a15bf91b9316374919ee51511e7d90418ca	
ZDHVAK-5562	20649E413C8DBE9F2248DBF6CC74EB39F9489EC17D7E4004F4DF69C7E8E10848	

Question 39: Provide the SHA256 hash of the file named default_wallet (not default_wallet.backup).

Consensus Result:

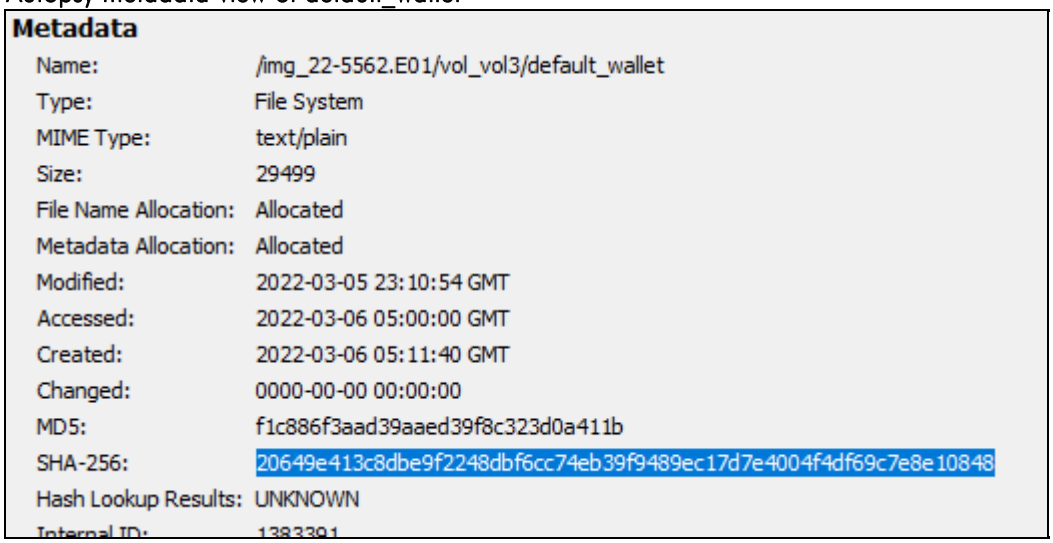
While a majority of participants (71%) reported the expected SHA256 hash of 20649e413c8dbe9f2248dbf6cc74eb39f9489ec17d7e4004f4df69c7e8e10848, a consensus was not achieved. Another 14% of participants reported the hash of a different version of the file which was found on the computer image not the USB.

Expected Response Explanation:

The file default_wallet was stored on the deleted FAT16 partition on the USB. To find and recover the file requires first recovering the partition, then hashing the file. Some forensic suites automate this process.

Expected Response Illustration:

Autopsy metadata view of default_wallet



Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 40 - Removable Media 22-5562

Question 40: On what date and time was the file default_wallet created on the USB media? Provide your response in GMT, using the date/time picker to select the date and time (24-hour).

Manufacturer's Expected Response: 2022-03-06 05:11 GMT

WebCode Test	Response
2GYK6H-5562	2022-03-06 05:11
3ERMDL-5562	2022-03-06 00:11
4ELR7K-5562	2022-03-06 05:11
6GRCUL-5562	2022-03-06 05:11
6XRJND-5562	2022-03-06 00:11
8PW7XC-5562	2022-03-06 05:11
8YYJXD-5562	2022-03-06 05:11
8ZU2ZE-5562	2022-03-06 05:11
9WRPDD-5562	2022-03-06 00:11
A7BERC-5562	2022-03-06 00:11
BN9WG8-5562	2022-03-06 00:11
BVR2DE-5562	2022-03-06 00:11
BYPLFC-5562	2022-03-06 05:11
DHRBK7-5562	2022-03-06 00:11
EX67D8-5562	2022-03-06 00:11
F2G9Z3-5562	2022-03-06 05:11
F8L898-5562	2022-03-06 05:11
FGDPP2-5562	2022-03-05 19:11
FL36D9-5562	2022-03-06 00:11

Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 40 - Removable Media 22-5562	
WebCode Test	**Response**
FVTQJ7-5562	2022-03-06 05:11
GLX6QD-5562	2022-03-06 05:11
HWZPPY-5562	2022-03-06 00:11
HX9YL3-5562	2022-03-06 05:11
JEDQ2D-5562	2022-03-06 05:11
KA2332-5562	2022-03-06 00:11
LTKL96-5562	2022-03-06 05:11
PRHXH6-5562	2022-03-06 05:11
PTTY3H-5562	2022-03-06 05:11
PZAFUR-5562	2022-03-06 05:11
QKG3YW-5562	2022-03-06 00:11
QVYKR4-5562	2022-03-06 05:11
R8KDG3-5562	2022-03-06 00:11
RFWD9R-5562	2022-03-06 00:11
T4JR6P-5562	2022-03-05 23:11
URL94P-5562	2022-03-06 00:11
VU4RLY-5562	[Participant did not return results for this question.]
WRDQDP-5562	2022-03-06 05:11
WXJKCR-5562	2022-03-06 05:11
XB3L8N-5562	2022-03-06 00:11
YDMVRA-5562	[Participant did not return results for this question.]

Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 40 - Removable Media 22-5562	
WebCode Test	**Response**
YL2H7J-5562	2022-03-05 22:11
YLG7ZJ-5562	2022-03-06 05:11
ZDHVAK-5562	2022-03-06 00:11

Question 40: On what date and time was the file default_wallet created on the USB media? Provide your response in GMT, using the date/time picker to select the date and time (24-hour).

Consensus Result:

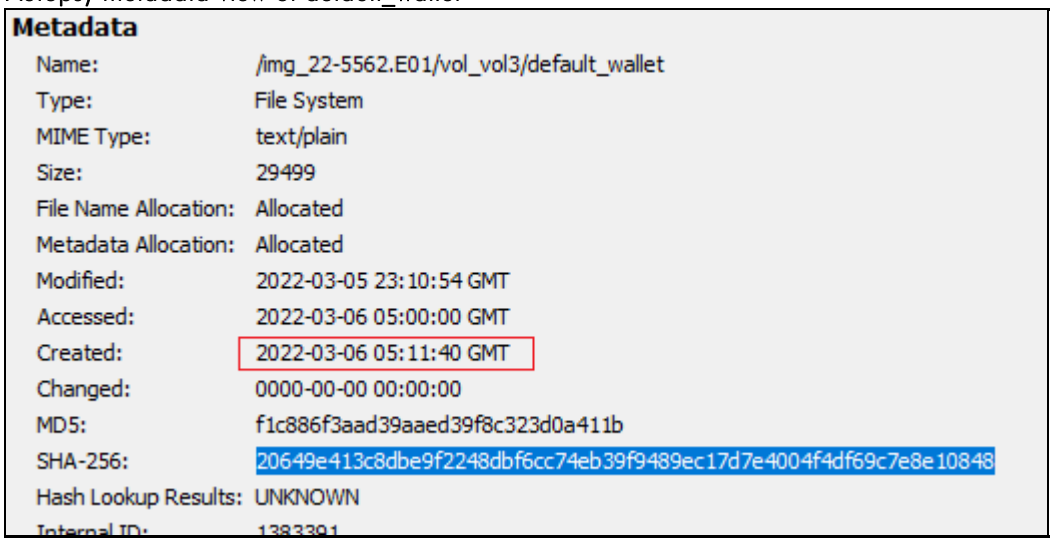
2022-03-06 05:11 GMT as well as the local time zone of the device.

Expected Response Explanation:

The file default_wallet was stored on the deleted FAT16 partition on the USB. To find and recover the file metadata requires first recovering the partition, then viewing the file system MAC times.

Expected Response Illustration:

Autopsy metadata view of default_wallet



Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 41 - Removable Media 22-5562

Question 41: In unallocated space on the NTFS partition on this device is a deleted photo of a mallard duck. What text is visible in the image?

Manufacturer's Expected Response: platyrhynchos

WebCode Test	Response
2GYK6H-5562	platyrhynchos
3ERMDL-5562	platyrhynchos
4ELR7K-5562	platyrhynchos
6GRCUL-5562	platyrhynchos
6XRJND-5562	platyrthynchos
8PW7XC-5562	platyrhynchos
8YYJXD-5562	Platyrhynchos
8ZU2ZE-5562	platyrhynchos
9WRPDD-5562	platyrhynchos
A7BERC-5562	platyrhynchos
BN9WG8-5562	platyrhynchos
BVR2DE-5562	platyrhynchos
BYPLFC-5562	platyrhynchos
DHRBK7-5562	platyrhynchos
EX67D8-5562	platyrhynchos
F2G9Z3-5562	platyrhynchos
F8L898-5562	Platyrhynchos
FGDPP2-5562	platyrhynchos
FL36D9-5562	platyrhynchos

Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 41 - Removable Media 22-5562	
WebCode Test	**Response**
FVTQJ7-5562	platyrhynchos
GLX6QD-5562	platyrhynchos
HWZPPY-5562	platyrhynchos
HX9YL3-5562	platyrhynchos
JEDQ2D-5562	platyrhynchos
KA2332-5562	platyrhynchos
LTKL96-5562	platyrhynchos
PRHXH6-5562	platyrhynchos
PTTY3H-5562	platyrhynchos
PZAFUR-5562	platyrhynchos
QKG3YW-5562	platyrhynchos
QVYKR4-5562	platyrhynchos
R8KDG3-5562	platyrhynchos
RFWD9R-5562	platyrhynchos
T4JR6P-5562	platyrhynchos
URL94P-5562	platyrhynchos
VU4RLY-5562	platyrhynchos
WRDQDP-5562	platyrhynchos
WXJKCR-5562	platyrhynchos
XB3L8N-5562	platyrhynchos
YDMVRA-5562	[Participant did not return results for this question.]

Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 41 - Removable Media 22-5562	
WebCode Test	**Response**
YL2H7J-5562	platyrhynchos
YLG7ZJ-5562	platyrhynchos
ZDHVAK-5562	platyrhyncos

Question 41: In unallocated space on the NTFS partition on this device is a deleted photo of a mallard duck. What text is visible in the image?

Consensus Result:

platyrhynchos

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:

deleted jpg file recovered from unallocated space

Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 42 - Removable Media 22-5562

Question 42: What is the file TYPE for the file with Created Time = 2017-12-20 14:23:53 GMT?

Manufacturer's Expected Response: JPEG, JPG or JFIF

WebCode Test	Response
2GYK6H-5562	File TYPE: JPEG, How did you determine the file TYPE?: FFD8FFE0 (jpg signature)
3ERMDL-5562	File TYPE: Picture (Image), How did you determine the file TYPE?: By file content extension and entropy test score was 0.9944 which was suspicious
4ELR7K-5562	File TYPE: JPG, How did you determine the file TYPE?: File Header
6GRCUL-5562	File TYPE: JPG, How did you determine the file TYPE?: File header signature
6XRJND-5562	File TYPE: jpg, How did you determine the file TYPE?: yoya hex header and there is file type mismatch found in X-Ways
8PW7XC-5562	File TYPE: JPG image, How did you determine the file TYPE?: By File Header and Footer
8YYJXD-5562	File TYPE: jpg, How did you determine the file TYPE?: File Header: FF D8 FF
8ZU2ZE-5562	File TYPE: JPG, How did you determine the file TYPE?: File header FF D8 FF following missmatch
9WRPDD-5562	File TYPE: Archivo de imagen (Exif), How did you determine the file TYPE?: Por la cabecera del archivo. (45 78 69 66)
A7BERC-5562	File TYPE: JPG, JPEG, How did you determine the file TYPE?: signature FF D8 FF and exif
BN9WG8-5562	File TYPE: JPEG, How did you determine the file TYPE?: Looked at the file header
BVR2DE-5562	File TYPE: Picture (Image), How did you determine the file TYPE?: By file content extension and entropy test score was 0.9944 which was suspicious.
BYPLFC-5562	File TYPE: JPEG, How did you determine the file TYPE?: HEX of file header ie ÿØÿàK&Exif
DHRBK7-5562	File TYPE: JPG, How did you determine the file TYPE?: We look at the file signature (header information) to determine the file type.
EX67D8-5562	File TYPE: .jpg, How did you determine the file TYPE?: The header of the file: 0xFF D8 FF E1
F2G9Z3-5562	File TYPE: JPG, How did you determine the file TYPE?: File header is FF D8 FF E1 which is JPG (Exif)
F8L898-5562	File TYPE: .JPG, How did you determine the file TYPE?: Ran file signature analysis over the file. Checked the hexadecimal of the file header.

Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 42 - Removable Media 22-5562	
WebCode Test	**Response**
FGDPP2-5562	File TYPE: JPEG EXIF, How did you determine the file TYPE?: File Header / Signature
FL36D9-5562	File TYPE: JPEG, How did you determine the file TYPE?: View file source and view hex – File header.
FVTQJ7-5562	File TYPE: Exif, How did you determine the file TYPE?: By identifying the File header of the file in hex
GLX6QD-5562	File TYPE: Image, How did you determine the file TYPE?: Signature Analysis
HWZPPY-5562	File TYPE: JPEG Image Non-Standard, How did you determine the file TYPE?: File header information & EnCase display of file type
HX9YL3-5562	File TYPE: JPEG, How did you determine the file TYPE?: Viewing the hex header, 0xFFD8FFE1, was observed which indicates it is a JPEG file.
JEDQ2D-5562	File TYPE: file is displayed as a .mp3 file but is in fact a .jpg displaying a photo of a circuit board, How did you determine the file TYPE?: examination of the HEX file header information - ÿØÿá
KA2332-5562	File TYPE: JPG, How did you determine the file TYPE?: The file signature is for JPG
LTKL96-5562	File TYPE: .jpg, How did you determine the file TYPE?: File signature
PRHXH6-5562	File TYPE: JPEG picture file, How did you determine the file TYPE?: X-Ways v19.8 SR-13 indicates that the type status of the file is a mismatch. The file type is shown as 'jpg' yet the file extension is 'mp3'. File header also shows YOYA JFIF' which confirms that the file is a JPG file. Viewing the file also shows that it is a jpg file of circuit board.
PTTY3H-5562	File TYPE: JPEG, How did you determine the file TYPE?: File's header corresponding to a JPEG file: 0xFF D8 FF
PZAFUR-5562	File TYPE: JPEG Image Non Standard, How did you determine the file TYPE?: Signature Analysis
QKG3YW-5562	File TYPE: jpg, How did you determine the file TYPE?: By looking at the header of the file
QVYKR4-5562	File TYPE: image file, How did you determine the file TYPE?: Defined in HEX as 'yoya K&Exif MM' - this is an image file with multi-media
R8KDG3-5562	File TYPE: Picture (.jpg), How did you determine the file TYPE?: file signature analysis (mismatch detected)
RFWD9R-5562	File TYPE: JPEG EXIF, How did you determine the file TYPE?: For the file signature (0xFFD8FFE1)
T4JR6P-5562	File TYPE: EXIF jpg image, How did you determine the file TYPE?: Reading the File Header (FF D8 FF E1)
URL94P-5562	File TYPE: .jpg, How did you determine the file TYPE?: File Header Hex xFF xD8 xFF xE1
VU4RLY-5562	File TYPE: jpeg (although extension states mp3), How did you determine the file TYPE?: Examination of file header

Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 42 - Removable Media 22-5562	
WebCode Test	**Response**
WRDQDP-5562	File TYPE: JPEG, How did you determine the file TYPE?: Utilizing a digital forensic program's category type then verifying it using a program which determine file type by three sets of tests, performed in this order: filesystem tests, magic tests (/usr/share/misc/magic.mgc) {which includes file signature matches}, and language tests.
WXJKCR-5562	File TYPE: jpg, How did you determine the file TYPE?: Type column in X-Ways, checked header
XB3L8N-5562	File TYPE: JPG, How did you determine the file TYPE?: This File's Signature(Header) is FF D8 FF E1 (Signature(Footer): FF D9). This Signature means JPG. And When you change the extension of this file to jpg, you can see it properly.
YDMVRA-5562	[Participant did not return results for this question.]
YL2H7J-5562	File TYPE: .jpg, How did you determine the file TYPE?: File header was FFD8 and file footer was FFD9 (These headers relates to .jpg file types)
YLG7ZJ-5562	File TYPE: mp3, How did you determine the file TYPE?: FF D8 FF E1 Hex file signature
ZDHVAK-5562	File TYPE: .jpg, How did you determine the file TYPE?: Viewed file signature in hex = FFD8FFE1

Question 42: What is the file TYPE for the file with Created Time = 2017-12-20 14:23:53 GMT?

Consensus Result:

JPEG, JPG or JFIF

Expected Response Explanation:

The file with hash 613cd9e96da949694014ccf77e63005cb99d7d49 is z30d3swoaff81.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 FF D8 FF E0 00 10 4A 46 49 46 (ÿØÿà··JFIF), the identifier for a jpeg file.

Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 42 - Removable Media 22-5562

Expected Response Illustration:

IMG_20200827_231612.mp3

Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 43 - Removable Media 22-5562

Question 43: Who is the owner of default_wallet.backup?

Manufacturer's Expected Response: Jessie Jenkins

WebCode Test	Response
2GYK6H-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
3ERMDL-5562	Jessie Jenkins
4ELR7K-5562	Jessie Jenkins
6GRCUL-5562	S-1-5-21-3501254099-4204809888-2000606956-1002 Jessie Jenkins
6XRJND-5562	Jessie Jenkins
8PW7XC-5562	S-1-5-21-3501254099-4204809888-2000606956-1002 (Jessie Jenkins)
8YYJXD-5562	d18a119e
8ZU2ZE-5562	Jessie Jenkins
9WRPDD-5562	Jessie Jenkins
A7BERC-5562	Jessie Jenkins
BN9WG8-5562	Jessie Jenkins
BVR2DE-5562	Jessie Jenkins
BYPLFC-5562	Jessie Jenkins S-1-5-21-3501254099-4204809888-2000606956-1002
DHRBK7-5562	Jessie Jenkins
EX67D8-5562	Unable to locate
F2G9Z3-5562	Jessie Jenkins
F8L898-5562	Jessie Jenkins
FGDPP2-5562	Jessie Jenkins
FL36D9-5562	[Participant did not return results for this question.]

Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 43 - Removable Media 22-5562	
WebCode Test	**Response**
FVTQJ7-5562	Jessi Jenkins
GLX6QD-5562	Jessie Jenkins
HWZPPY-5562	Jessie Jenkins
HX9YL3-5562	Jessie Jenkins
JEDQ2D-5562	22-5561.E01 - Partition 2 (Microsoft NTFS, 29.95 GB)\Users\Jessie Jenkins\Documents\New Directory\default_wallet.backup
KA2332-5562	S-1-5-21-3501254099-4204809888-2000606956-1002 (Jessie Jenkins)
LTKL96-5562	Jessie Jenkins
PRHXH6-5562	Jessie Jenkins
PTTY3H-5562	Jessie Jenkins (S-1-5-21-3501254099-4204809888-2000606956-1002)
PZAFUR-5562	Jessie Jenkins
QKG3YW-5562	'S-1-5-21-3501254099-4204809888-2000606956-1002' this SID matches the registered owner, 'Jessie Jenkins', of the operating system found on exhibit '22-5561'
QVYKR4-5562	S-1-5-21-3501254099-4204809888-2000606956-1002
R8KDG3-5562	Jessie Jenkins (S-1-5-21-3501254099-4204809888-2000606956-1002)
RFWD9R-5562	Jessie Jenkins
T4JR6P-5562	Jessie Jenkins
URL94P-5562	Jessie Jenkins
VU4RLY-5562	S-1-5-21-30501254099-4204809888-2000606956-1002 (jessie jenkins)
WRDQDP-5562	Jessie Jenkins (S-1-5-21-3501254099-4204809888-2000606956-1002)
WXJKCR-5562	Jessie Jenkins
XB3L8N-5562	Jessie Jenkins
YDMVRA-5562	[Participant did not return results for this question.]

Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 43 - Removable Media 22-5562	
WebCode Test	**Response**
YL2H7J-5562	Jessie Jenkins
YLG7ZJ-5562	SID (S-1-5-21-3501254099-4204809888-2000606956-1002) Jesse Jenkins
ZDHVAK-5562	Jessie Jenkins

Question 43: Who is the owner of default_wallet.backup?

Consensus Result:

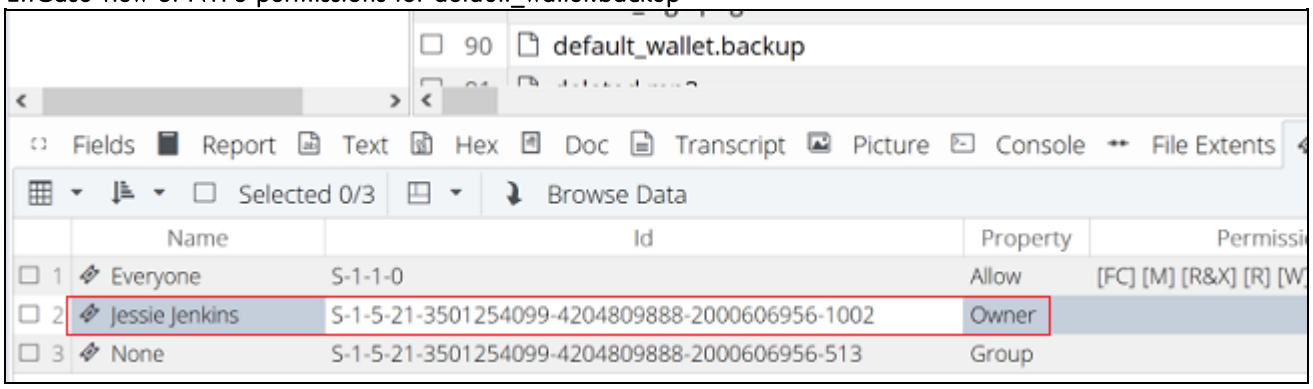
Jessie Jenkins as well as S-1-5-21-3501254099-4204809888-2000606956-1002

Expected Response Explanation:

The NTFS filesystem permissions on the USB device lists Jessie Jenkins with SID S-1-5-21-3501254099-4204809888-2000606956-1002, as the owner of this file.

Expected Response Illustration:

EnCase view of NTFS permissions for default_wallet.backup



Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 44 - Removable Media 22-5562

Question 44: Place the following events in the order in which they occurred (report each letter in order separated by a comma, e.g. A,B,C,D,E):
A. the creation of the file referenced in USB question 40
B. scheduled meeting referenced in question 18
C. failed logins referenced in question 21
D. the last execution of the program referenced in question 22
E. approximate time of victim's death as provided by the medical examiner

Manufacturer's Expected Response: B,E,C,D,A

WebCode Test	Response	** Inconsistencies not highlighted; No consensus achieved **
2GYK6H-5562	B > E > C > D > A	
3ERMDL-5562	B,E,A,C,D	
4ELR7K-5562	B,E,C,D,A	
6GRCUL-5562	B,E,C,D,A	
6XRJND-5562	B,E,A,C,D	
8PW7XC-5562	B,E,C,D,A	
8YYJXD-5562	C,B,D,A,E	
8ZU2ZE-5562	B,E,C,D,A	
9WRPDD-5562	B,E,A,C,D	
A7BERC-5562	B,E,A,C,D	
BN9WG8-5562	B,E.C,D,A	
BVR2DE-5562	B,E,A,C,D	
BYPLFC-5562	B,E,C,D,A	
DHRBK7-5562	B,E,C,D,A	
EX67D8-5562	F,C,A,D,E,B	
F2G9Z3-5562	B,E,C,D,A	

Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 44 - Removable Media 22-5562		
WebCode Test	**Response**	** Inconsistencies not highlighted; No consensus achieved **
F8L898-5562	B,E,C,D,A,	
FGDPP2-5562	A,B,E,C,D	
FL36D9-5562	D,B,E,A,C	
FVTQJ7-5562	B,E,C,D,A	
GLX6QD-5562	C,B,E,D,A	
HWZPPY-5562	A,B,E,C,D	
HX9YL3-5562	B,E,C,D,A	
JEDQ2D-5562	B,E,C,D,A	
KA2332-5562	B,A,E,C,D	
LTKL96-5562	B,C,D,A,E	
PRHXH6-5562	B,E,C,D,A	
PTTY3H-5562	B,E,C,D,A	
PZAFUR-5562	B,E,C,D,A	
QKG3YW-5562	A,B,E,C,D	
QVYKR4-5562	B,E,C,D,A	
R8KDG3-5562	B,E,C,D,A	
RFWD9R-5562	B,A,E,C,D	
T4JR6P-5562	B,A,E,C,D	
URL94P-5562	B,E,A,C,D	
VU4RLY-5562	[Participant did not return results for this question.]	
WRDQDP-5562	B,E,C,D,A	

Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 44 - Removable Media 22-5562		
WebCode Test	**Response**	** Inconsistencies not highlighted; No consensus achieved **
WXJKCR-5562	B,E,C,D,A	
XB3L8N-5562	B,E,A,C,D	
YDMVRA-5562	[Participant did not return results for this question.]	
YL2H7J-5562	ABECD	
YLG7ZJ-5562	D,B,E,C,A	
ZDHVAK-5562	A,B,E,C,D	

Question 44: Place the following events in the order in which they occurred (report each letter in order separated by a comma, e.g. A,B,C,D,E):
A. the creation of the file referenced in USB question 40
B. scheduled meeting referenced in question 18
C. failed logins referenced in question 21
D. the last execution of the program referenced in question 22
E. approximate time of victim's death as provided by the medical examiner

Consensus Result:

A consensus response was not achieved for this question. The expected response, "B,E,C,D,A" was reported by 47% of participants. The second most common response was "B,E,A,C,D" at 17%.

Expected Response Explanation:

Reviewing the above events as listed:
A. The creation of the file referenced in question 40: default_wallet was stored on the deleted FAT16 partition on the USB. To find and recover the file metadata requires first recovering the partition, then viewing the file system MAC times. Once recovered, the file system meta data for that file shows it was created 2022-03-06 05:11:40 UTC.
B. The meeting referenced in question 18 was arranged via email message between the victim and Andersen, and scheduled for 8 P.M. EST, Saturday, March 5, 2022; 2022-03-06 01:00:00 UTC.
C. Question 21 references failed logins prior to successful login referenced in question 20. Windows Security Event Logs show the last successful user login to this computer 2022-03-06 05:07:35 UTC.
D. According to Windows prefetch records, Electrum was last executed 2022-03-06 05:09:33 UTC.
E. Per the test instructions: the Medical Examiner's report estimates the victim died sometime between 10 P.M. and midnight (EST), March 5th. i.e. before 2022-03-06 05:00:00 UTC.

Converting all times to UTC and placing in order:
1. B. 2022-03-06 01:00:00 UTC scheduled meeting referenced in question 19
2. E. 2022-03-06 05:00:00 UTC approximate time of victim's death per the medical examiner
3. C. 2022-03-06 05:07:35 UTC failed/successful logins referenced in question 22
4. D. 2022-03-06 05:09:33 UTC the last execution of the program referenced in question 23
5. A. 2022-03-06 05:11:40 UTC the creation of the file referenced in USB question

Additional Comments

TABLE 3

WebCode Test	Additional Comments
3W8X27-5561	FTK imager used to verify stored SHA-1 hash of image. Integrity of downloaded image checked using HashCheck shell extension
7CPVTB-5561	When I added just the E01 file, I obtained the following MD5 and SHA1 values for the file: MD5: 8d3d62bfc411a03e6718c170ab25d8ce SHA1: a7b250cb09fcd6e5e362fcbc268ec6df12dbd418 When I added the folder contacting the E01 file, I obtained the following MD5 and SHA1 values: MD5: 6b9817826df193eee61011f72128aeb9 SHA1: 1ac729c981dfae5668f12de30befc9937fdd12ef
A7BERC-5562	thank you~!!
F8L898-5562	After the estimated time of death the deceased account was accessed, and the bitcoin application was activated. Qu 39 - There are two files bearing the name 'default_wallet' – one on the USB device and one on the supplied forensic image. It was not clear in the questions which hash value was required.
FGDPP2-5562	Question 18: The provided date and time answer is in EST. From Question 33 onward up to 44 have been considered belonging to USB storage device.
GLX6QD-5562	Is there an error with Question 39 & 40? as the file cannot be found on the USB media? Answers provided for these questions are reflective of the file located on the computer instead
HPTDCY-5561	Question 1 - This is an ongoing problem with the CTS - It always asks for Sha-1 values, but NEVER states if it wants base16 or base32. As a proficiency test, I would think that you do not want to confuse your testers and would be more clear in the answers you want. Or don't use Sha-1, which has two common base's. Question 19 - You switch to UTC time zone. The rest of the exam was in EDT, so to switch feels like an intentional move to confuse the test taker. Question 21 - There are six entries for Code 4625, which is a failed login attempt. Question 32 - In your question, you ask for the picture which involves user "Jesse Jenkins". There is no such user. There is a "Jessie" Jenkins, which I assume you are asking about. This type of clerical error (which I assume is what it is), can be very misleading if you are trying to trick the reader or not. Especially when a spelling error on our part will result in a 'non-conformance' marking. This proficiency test is used by our department for certification purposes. When an answer is found incorrect/non-conforming, then we must pause all case work until justifications can be made. Spelling mistakes in questions therefore can have a profound effect on an examiners being able to continue casework.

TABLE 3

WebCode Test	Additional Comments
HWZPPY-5562	PART 1: Three questions related to file TYPE. File TYPE may have multiple interpretations. Does this mean the File Type flags within the Standard Information attribute (File TYPE according to IACIS), file Type according to Windows interpretation of the file extension (file TYPE displayed in Windows file properties), the file type as interpreted by the examiner using file header information (JPEG, PNG, picture, movie), or file type as displayed in EnCase (or other tool) (JPEG Standard Format, etc.)? This set of questions should be better worded to ensure you are receiving a consistent response from participants. PART 2: Also, one question asks about the number of ACTIVE partitions. Active, in computer terms, means "bootable". Active in layman's terms, may mean active for the user to access. Depending on interpretation, the answer will be different.
HX9YL3-5562	Q1 - Doesn't specify which SHA hash type. Q34 - Question is vague. There is one active partition/present without recovery, another partition (FAT16) was recovered from physical sector 3518592.
JQ84YN-5561	Some questions such as 21 have poorly defined time frames (immediately preceding) but are asking for a specific number response. The wording of the questions added to the confusion for several questions- the question asking about the name of the file containing a string with 2 letters, 5 numbers, "CW", and 4 numbers comes to mind. I read it as what i was looking for was the name of a file that contained that string. Spent 2 days working on it. maybe "there is a file whose contents contain a string with blah-blah-blah...- what is the name of that file?" When i read #26 I try to determine what the question wants me to respond with, and I feel that when I'm putting it in my own words(as opposed to answers with definite correct responses) there's a very good chance i'm misinterpreting the question. I would much prefer if questions were limited to categorical answers. The answer to 24B could be "I remember learning that in a class one time..." I may be the only person who has this problem(if so, my apologies) but i've been trained and conditioned to answer the question i'm asked and when there is any ambiguity to the question, i struggle. Question number 27, perhaps is straightforward to some, but based on the considerations I've had to account for when answering questions like this in the past, needs to clarified. I think i understand what the test is asking for as far as my response, but I could be reading it wrong and answering a different question than the one the provider is asking. i probably went overboard on this, but i'm an over-thinker. My honest answer to this question initially was, "I can't answer this question. I wasn't there when the email client was installed." I know the question probably means the Administrator Account, but the question says, "Administrator". To me- that means the physical person. the same as the court question i get sometimes, "Who was at the keyboard?" - Me: "I can't speak to that. I wasn't there at the time in question." Also- i called tuesday 6/21/2022 for clarification on a few questions, however the person who wrote the test was out of town on vacation.

TABLE 3

WebCode Test	Additional Comments
PPUJUU-5561	The questions of this test were very well organized. Thank you very much for your excellent job! But there are several questions, which meaning was not clearly understood, therefore caused problems in the process of answering. In question 26, the specific reference to "source" could not be accurately understood. This results in a number of possible answers to it. It can be the sender's name, an email address, the photo device, or the download address, etc. This makes us quite unsure which answer to fill in. In question 31, it was not certain if the answer to this question includes the area code. As a result, two numbers were found. One of which was a 10-digit number with the first two and last two digits being "57", and the other was a number with the first two and last two digits being "57" after the first three area codes were removed. Thank you very much. Best wishes.
PZAFUR-5562	[For Question #22, participant's full response was "Application run count = 6 - Jessie Jenkins - Electrum 4.1.5.exe"; For Question #34, participant's full response was "2 (1 Recovered)"]
QQ3XWU-5561	Question 18 could have multiple answers based on the examiner's interpretation of the word "ultimately". The two individuals discussed a couple of different options to begin with and ultimately decided on a restaurant for a date without a time. Then, the second individual did not show up to the agreed-upon time and they ultimately rescheduled to a later date with a slightly ambiguous time. The question could be more clear. Additionally, Question 32 appears to have misspelled the victim's name as "Jesse Jenkins".
QVYKR4-5562	No additional comments.
RFWD9R-5562	During the examination of the Removable Media, I noticed that the questions do not match with what I'm looking in the USB. The USB device only shows one FAT16 partition and the rest was blank. Thinking that maybe that was the challenge, I try everything to find for something else. After analyzed the hex, I could confirm that the USB don't have anything and the file system is FAT16, I contacted QA with the issue. The QA Manager contacted CTS, which the customer service was poor and the person never accept that the USB sent was incorrect, they agreed to send another USB and give an extension. After the new USB arrives, I could confirm that the first USB was incorrect based on hashes and content. I would suggest a better quality control and a better customer service.
RNWQP-5561	Searches can be affected by cultural differences in how dates and telephone numbers are presented in different countries.

TABLE 3

WebCode Test	Additional Comments
WRDQDP-5562	Question #4 - in addition to "Microsoft Windows 10 Home" the "CurrentVersion" is 6.3, the "DisplayVersion" is 21H2, the "EditionID" is Core and the CurrentBuild is 19044. Question #20 - In the System.evtx file the last successful login (Winlogon 7001) was at 03/06/2022 05:05:26.9 UTC. The Security.evtx "Special Logon:4672: Special privileges assigned to new logon" at 3/6/2022 5:07:34 UTC is a security event when someone who is already logged on runs a command as administrator (or in some cases any server or applications accounts logging on as a batch job (scheduled task) or system service.) If this includes these security events as logins then the answer is "3/6/2022 5:07:34 UTC". Question #21 - 4 (if within that second of the Security.evtx) {Event record IDs 12784, 12785, 12794 and 12811} 1 (if literally each Security.evt entry) {Event record ID 12811} Also, if the answer for #20 is "3/6/2022 5:07:34 UTC" because the the "Special Logon" then #21 is equal to 1. Question #25 - Since the question explicitly stated "$FILE_NAME" I provided the MFT $FILE_NAME Attribute for created date and time of 02/20/2022 18:55:38 UTC versus the common MFT $Standard_Information Attribute for created date and time of 01/15/2018 22:42:49 UTC for C:\Users\Jessie Jenkins\Documents\PoorFairJaguar.html. Question #43 - The Flash drive Owner of : 2022-CTS-FLASH01.E01/Partition 1/New Volume [NTFS]/ [root]/default_wallet.backup With MD5: f41be80190c87a1af749f0b404547c3c Is: S-1-5-21-3501254099-4204809888-2000606956-1002) which is the username: Jessie Jenkins (only because we have the computer)
XB3L8N-5562	default_wallet is 00:11 default_wallet.backup is 05:11 The context is B-E-C-D-A, but it's not a backup file.
Y4WCCF-5561	Assuming terms "version" and "edition" in Question 4 refer to "10" and "Home" found within the ProductName string. But there is some ambiguity here as the term "version" could instead be interpreted to refer to either the observed CurrentVersion value (6.3) or the DisplayVersion value (21H2) under the CurrentVersion subkey. Similarly, the term "edition" could instead be interpreted to refer to the observed EditionID value (Core). Wording chosen for Question 18 provokes response ambiguity both with the "where" (meeting venue) and the "when" (meeting date and time). The where could connote the facility name (e.g. Founding Farmers, Founding Farmers Reston, and/or Founding Farmers Reston Station), street address, website address, or description (e.g. "a nice dinner out"). And the when could be provided in either local (UTC-05:00) or UTC+0 date and time. UTC+0 was chosen since all the other Questions referencing date and time values request responses in this format. The term "immediately" used in Question 21 was expected to describe a timeframe as short as a few seconds (or even milliseconds). Since there were no unsuccessful logon attempt events logged within this timeframe, "0" could also be considered a defensible response. No response input format was provided for Question 24 and Question 26. The "short answer" concept could cause response consensus conflicts due to syntax variation. The date/time picker also does not allow for the selection of seconds (only hours and minutes) which could cause response consensus conflicts due to rounding.

TABLE 3

WebCode Test	Additional Comments
YL2H7J-5562	Question 19 - The term 'Comment' was not helpful as there were several event descriptions during the time provided (Which did not include 'seconds'). The first event description during the time period provided was the 'User generated logoff', which I have provided as the answer. Question 31 - This question assumes the investigator knows the makeup of a US based phone number. A pattern (Similar to that provided in question 30) would have been helpful.
ZLZ4XH-5561	Some of the questions, in my opinion, are beyond the scope of a proficiency test.

-End of Report-
(Appendix may follow)