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 & Removable Media Analysis Test No. 21-5561/2 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 120 participants, 38 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 21-5562: 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 financial fraud 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, 25 January 2021 – 10 March 2021. 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 21-5562.

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 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.

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
Gordon Jamerson is the victim of financial fraud.

Jamerson received an unsolicited direct message on Instagram from “Samantha”, who alleged she was an account manager with a firm that specializes in binary trading options. After lengthy conversation Samantha convinced Gordon to send her money to invest in her fund. Gordon was unable to withdraw his “earnings,” became suspicious, and reported the activity to police.

Information provided by Instagram pursuant to a subpoena identified the Internet Protocol addresses used to access “Samantha’s” Instagram account. Information provided by Comcast, the ISP controlling those IP addresses, led investigators to “Samantha’s” residence where they seized a laptop computer pursuant to a search warrant for evidence of fraud and identity theft.

The seized laptop has been submitted for forensic examination to find evidence of the alleged fraud and links to the true identity of the laptop’s owner.

You are being tasked with analyzing a forensic image of a computer and a USB using your own tools and methodologies.

Manufacturer's Information, continued

Question	Manufacturer's Expected Response
1	**Provide the (Stored Verification) SHA-1 Hash for the provided image, 21-5561.E01.** *62868241dc672c662be2e2d14b1fb0e3f46520d4*
2	**How many partitions are on the device imaged as 21-5561.E01?** *Two (2)*
3	**What is the volume serial number for the filesystem on the system partition? (Report the first 4 bytes (little endian) as it would be reported/displayed by Windows)** *F617-480A and/or 3A16-DAAE*
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?** *susie*
6	**When was the operating system installed? Provide the answer in UTC + 00:00 using the following format: MM/DD/YYYY HH:MM:SS AM/PM.** *02/18/2021 22:45:51 PM*
7	**When was the device LAST shutdown gracefully? Provide the answer in UTC + 00:00 using the following format: MM/DD/YYYY HH:MM:SS AM/PM.** *03/10/2021 02:45:33 AM*
8	**Provide the username of the account created by the user.** *susie*
9	**What is the Security ID (SID) of the user account created by the user?** *S-1-5-21-1943064195-990424342-2473957490-1001*
10	**What is the configured time zone?** *W. Central Africa Standard Time, or UTC-1*
11	**Provide the name for the paired Bluetooth device with MAC address 98:d3:71:fd:9a:2a.** *BEARODACTYL*
12**	**According to the last write times on the associated registry keys, what was the volume label (name) of the LAST mounted volume on a portable storage (USB) device?** *stuff*
13	**In unallocated space on this device is a JPEG photograph of an opossum carrying joeys (baby opossums). What is the SHA1 hash of this file?** *13d5240c84a2f9dcafbce49ed0a63527adcd16fa*
14	**Provide the path and filename of the file containing the term "typhimiurium".** *C:\Users\susie\Documents\003464.xls*
15**	**What (non-encryption related) anti-forensics application did the user execute?** *Please refer to the section labeled "Consensus Result" for this specific question for more information.*

Manufacturer's Information, continued

Question	Manufacturer's Expected Response
16	**What was the name of the LAST wireless network to which the computer was connected?** *RCMP Surveillance Moose*
17	**What IP address was assigned by this network?** *192.168.40.37*
18	**What encryption program did the user execute?** *VeraCrypt, Or Veracrypt-X64, or VeraCrypt Setup 1.24-Update7.exe*
19	**The encrypted volume was mounted to what drive letter?** *V*
20	**What directory containing photos did the user access on the mounted volume referenced in Question 19?** *V:\kittehs*
21**	**From what volume serial number was the encryption program referenced in question #18 executed?** *4a0c3885 and/or f617480a*
22	**When did the user LAST login to the user's account (account referenced in questions: #8, #9)? Provide your response in UTC + 00:00 using the following format: MM/DD/YYYY HH:MM:SS AM/PM** *03/10/2021 02:38:42 AM*
23**	**How many times was NOTEPAD.EXE executed?** *Please refer to the section labeled "Consensus Result" for this specific question for more information.*
24	**What is the original (pre-deletion) path and name of $I9JOSIO.jpg (found in the user's Recycle Bin)?** *C:\Users\susie\Documents\004854.jpg*
25	**What date and time was the file 004651.pdf deleted? Provide your response in UTC + 00:00 using the following format: MM/DD/YYYYHH:MM:SS AM/PM** *03/07/2021 03:33:23 AM*
26	**Provide the first six bytes of the file with SHA1 hash 383d4c012ac7c550699c3908c57f7ad00b98ecbe.** *47 49 46 38 37 61, or GIF87a*
27	**From what host URL was the file Watcher_Generic.zip downloaded?** *https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip*
28	**What website did the user visit at 03/01/2021 01:55:08 (UTC+00:00)?** *www.farmersonly.com*
29	**What email address is the Google Chrome browser configured to use to sign into Google?** *robertapeal67@gmail.com*
30	**With what software was the file 000536.jpg modified?** *Adobe Photoshop 7.0*

Manufacturer's Information, continued

Question	*Manufacturer's Expected Response*

31 **Who is listed as the author of 850248.xls?**

Toni Timberman

32 **What file(s) contains the words "Fraud" and "Pack" separated by another word?**

C:\Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\bookmarkbackups\bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4 and/or Computer\C:\Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\places.sqlite-wal

33 **What email address was the user-installed email client successfully configured to access (send and receive messages)?**

robertapeal67@gmail.com

34** **With what (other party) email address did the user send and receive emails with encrypted content or attachments?**

francismilligan599@gmail.com

35** **What is the default program for opening .docx document files?**

OpenOffice Writer or swriter.exe

36 **Provide the 10 byte (ASCII) string beginning at Physical Sector 5236523, Sector Offset 67.**

good work!

37 **The SHA1 hash for the USB device is F3C33632CD03525ECC4B07362AC5196DA5F02262. Provide the SHA256 hash for the USB device.**

EE010683ABE27680DB634FD1AA00AEA493820EF057C1DEE7D528FA55F123D85C

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

2

Manufacturer's Information, continued

Removable Media Analysis: *USB Drive*
Test No. 21-5562

Question	*Manufacturer's Expected Response*

39 **What is the volume serial number of the NTFS partition (The first 4 bytes (little endian) as it would be reported/displayed by Windows)?**
4A0C-3885

40 **What is the name (Volume Label) of the NTFS Partition?**
stuff

41 **What number is visible in the file with SHA1 hash 6b5fc1a4273ff607974492ce6c40a34db1e6ec69?**
64

42** **What do the differences in the filesystem metadata between lscg16kho8i61.jpg and lscg16kho8i61 - Copy.jpg indicate?**
The copy was created on a different computer than the original.

43 **What is the name of the file in the root directory of the NTFS volume with header 89 50 4E 47?**
850785.png

44 **Who is the author of 850009.xls?**
shuga001

45 **In unallocated space on this device is a deleted photo of a black kitten with blue eyes. What is the SHA1 hash of this file?**
3843fe118e1f55cc4d3d7f8cede8f3aeb2793e00

46 **What indications, if any, suggest this device was "sterilized" prior to use?**
The unallocated space on the device was overwritten with a pattern, "CTS_FORENSICS_"

47 **What are the GPS coordinates where PA020033.JPG was captured? Provide your answer in the format: DD MM' SS.SS" N/S, DD MM' SS.SS"E/W.**
38°49'10.22" N, 76°12'58.40" W

48 **What is the name of the file containing the word "glucuronasyltransferase"?**
850952.doc

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 21-5562: 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 120 participants returned results for the 5561 Computer Hard Drive - Windows Analysis test. Of the 36 total questions, six questions did not reach a consensus response. These questions dealt with topics such as identifying the following: the volume label of the last mounted volume on USB, the anti-forensic application executed, the volume serial number that executed Veracrypt, the run count for notepad.exe and the email address the user sent and received email with encrypted content.

Of the participants enrolled in the 5562 Removable Media Storage Analysis test, 38 returned results. One of the twelve questions did not reach a consensus response. This question asked examiners to described the meaning behind the differences between filesystem metadata between two jpgs.

We realize that the Digital Forensics field is increasing in complexity and there are generally not many clearly-defined answers. Similarly, for this test, participants should 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

Question 1: Provide the (Stored Verification) SHA-1 Hash for the provided image, 21-5561.E01.

Manufacturer's Expected Response:
62868241dc672c662be2e2d14b1fb0e3f46520d4

WebCode - Test	Response
23UJ67-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
29JUMG-5562	62868241dc672c662be2e2d14b1fb0e3f46520d4
2YBWJR-5562	62868241dc672c662be2e2d14b1fb0e3f46520d4
3B7V4P-5561	06053c89de1b83d5eaead561bd3a6174a7f68488
3RC2CZ-5561	The SHA-1 hash value for the provided 21-5561.E01 image is 62868241dc672c662be2e2d14b1fb0e3f46520d4.
44372B-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
4A86BF-5561	06053C89DE1B83D5EAEAD561BD3A6174A7F68488
4UEFFJ-5561	Acquisition SHA1 62868241dc672c662be2e2d14b1fb0e3f46520d; Verification SHA1 62868241dc672c662be2e2d14b1fb0e3f46520d4
66CHBZ-5561	SHA-1: 62868241dc672c662be2e2d14b1fb0e3f46520d4
67H6N6-5562	62868241dc672c662be2e2d14b1fb0e3f46520d4
6G29KN-5562	62868241dc672c662be2e2d14b1fb0e3f46520d4
6LBUJ2-5561	62868241DC672C662BE2E2D14B1FB0E3F46520D4
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
6ZD7FZ-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
7A2A6E-5561	62868241DC672C662BE2E2D14B1FB0E3F46520D4
7FMAEZ-5562	3dd605cd2c0b034367c62b550ee19770
7W9P7F-5562	62868241dc672c662be2e2d14b1fb0e3f46520d4
89LGKW-5561	SHA1 verification hash 62868241dc672c662be2e2d14b1fb0e3f46520d4
89NM2E-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
8UH9ME-5562	06053c89de1b83d5eaead561bd3a6174a7f68488
8YVWFY-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 1	
WebCode - Test	**Response**
93AL3L-5562	62868241dc672c662be2e2d14b1fb0e3f46520d4
9ARR2D-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
9GULT8-5562	62868241dc672c662be2e2d14b1fb0e3f46520d4
9V6AXV-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
A8KGFG-5561	62868241DC672C662BE2E2D14B1FB0E3F46520D4
AK9F96-5561	62868241DC672C662BE2E2D14B1FB0E3F46520D4
AQYVXC-5562	62868241DC672C662BE2E2D14B1FB0E3F46520D4
AV4RGC-5562	62868241dc672c662be2e2d14b1fb0e3f46520d4
BGJGLT-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
BKPYQG-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
BMT8ZD-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
BR6KUT-5562	62868241DC672C662BE2E2D14B1FB0E3F46520D4
BWZC2P-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
CBTGPD-5562	62868241dc672c662be2e2d14b1fb0e3f46520d4
CMHKPW-5561	06053C89DE1B83D5EAEAD561BD3A6174A7F68488
CPRZ8G-5561	62868241DC672C662BE2E2D14B1FB0E3F46520D4
CQ9KB9-5562	62868241dc672c662be2e2d14b1fb0e3f46520d4
CQJQ7N-5561	SHA1 - 62868241dc672c662be2e2d14b1fb0e3f46520d4
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
E43HU2-5561	62868241DC672C662BE2E2D14B1FB0E3F46520D4
E7BXK2-5561	62868241DC672C662BE2E2D14B1FB0E3F46520D4
EELYM9-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
F2UYKR-5561	SHA-1 of the image is 62868241dc672c662be2e2d14b1fb0e3f46520d4

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 1	
WebCode - Test	**Response**
FFG39B-5562	62868241dc672c662be2e2d14b1fb0e3f46520d4
FJWWP9-5562	06053c89de1b83d5eaead561bd3a6174a7f68488
FP3BPR-5562	62868241dc672c662be2e2d14b1fb0e3f46520d4
FTFDBN-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
G9A37K-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
GGKE74-5561	62868241DC672C662BE2E2D14B1FB0E3F46520D4
GU9W29-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
GZY7B8-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
H949ZJ-5561	3dd605cd2c0b034367c62b550ee19770
HEBY4P-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
HYFCYH-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
J3U2M6-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
J3XR9B-5561	Stored digest: 62868241dc672c662be2e2d14b1fb0e3f46520d4; Computed digest: 62868241dc672c662be2e2d14b1fb0e3f46520d4
JF4GTB-5562	62868241dc672c662be2e2d14b1fb0e3f46520d4
JJJA4W-5562	62868241DC672C662BE2E2D14B1FB0E3F46520D4
JMJLZW-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
JU4NYL-5561	62868241DC672C662BE2E2D14B1FB0E3F46520D4
K6Z7V8-5562	62868241dc672c662be2e2d14b1fb0e3f46520d4
KE3C4M-5561	06053c89de1b83d5eaead561bd3a6174a7f68488
KH3MYM-5562	62868241dc672c662be2e2d14b1fb0e3f46520d4
KT78B9-5562	62868241DC672C662BE2E2D14B1FB0E3F46520D4
KW3EPY-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
L9D7RX-5562	62868241dc672c662be2e2d14b1fb0e3f46520d4
LCV3Z2-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 1	
WebCode - Test	**Response**
LEERBL-5562	62868241dc672c662be2ed14b1fb0e3f46520d4
LPY8P3-5561	06053c89de1b83d5eaead561bd3a6174a7f68488
LRRLAT-5562	62868241dc672c662be2e2d14b1fb0e3f46520d4
LXXGTT-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
M98EB2-5562	62868241DC672C662BE2E2D14B1FB0E3F46520D4
MWHHA4-5562	06053c89de1b83d5eaead561bd3a6174a7f68488
MYJKY6-5562	06053c89de1b83d5eaead561bd3a6174a7f68488
N66VNU-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
NFQ2KX-5562	62868241dc672c662be2e2d14b1fb0e3f46520d4
NPAH8D-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
NRJXPX-5561	SHA-1 Hash: 06053C89DE1B83D5EAEAD561BD3A6174A7F68488
NTAT4D-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
NUKNP6-5562	06053c89de1b83d5eaead561bd3a6174a7f68488
PBBNHP-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
PBQMFZ-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
PTA4GV-5562	62868241dc672c662be2e2d14b1fb0e3f46520d4
QP2MPV-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
R36ZB9-5561	06053c89de1b83d5eaead561bd3a6174a7f68488
RAQR4V-5562	62868241dc672c662be2e2d14b1fb0e3f46520d4
RFUVTT-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
RGQL4V-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
RK6QRB-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
RXCADP-5561	Verification SHA1: 62868241DC672C662BE2E2D14B1FB0E3F46520D4
T8F7TZ-5562	62868241dc672c662be2e2d14b1fb0e3f46520d4

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 1	
WebCode - Test	**Response**
TCA8P9-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
TDLF3U-5561	06053C89DE1B83D5EAEAD561BD3A6174A7F68488
TFMD29-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
TMAWNW-5561	06053C89DE1B83D5EAEAD561BD3A6174A7F68488
U298Q9-5561	62868241DC672C662BE2E2D14B1FB0E3F46520D4
U964DC-5562	62868241dc672c662be2e2d14b1fb0e3f46520d4
UWTR4N-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
V23CK9-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
V96U7R-5561	06053c89de1b83d5eaead561bd3a6174a7f68488
VFHDED-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
WHMDWP-5561	06053C89DE1B83D5EAEAD561BD3A6174A7F68488
WLLU9J-5561	62868241DC672C662BE2E2D14B1FB0E3F46520D4
WRR3GT-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
WW4B2Q-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
X436QC-5562	62868241dc672c662be2e2d14b1fb0e3f46520d4
X4L22Q-5562	62868241dc672c662be2e2d14b1fb0e3f46520d4
XCDUFN-5561	62868241DC672C662BE2E2D14B1FB0E3F46520D4
XHHHQN-5561	06053C89DE1B83D5EAEAD561BD3A6174A7F68488
XUR36B-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
Y2ANWU-5561	62868241DC672C662BE2E2D14B1FB0E3F46520D4
YQTYXP-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
YXADZU-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
YYKJVA-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4
ZGHWCN-5561	62868241dc672c662be2e2d14b1fb0e3f46520d4

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 1	
WebCode - Test	**Response**
ZM6UW6-5561	62868241DC672C662BE2E2D14B1FB0E3F46520D4
ZTBFTE-5561	62868241DC672C662BE2E2D14B1FB0E3F46520D4

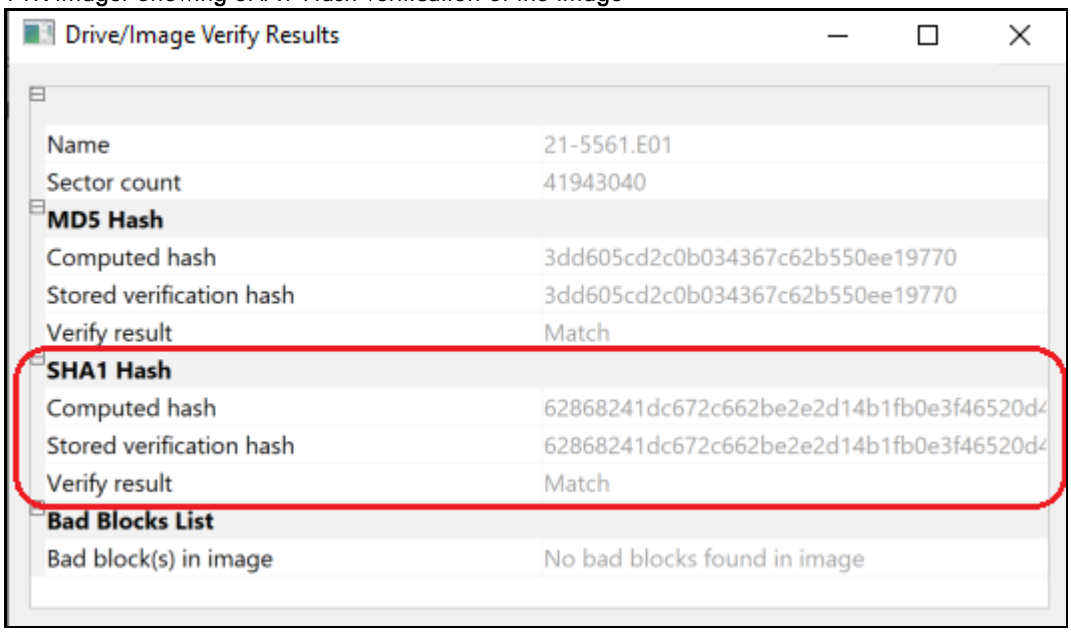
Question 1: Provide the (Stored Verification) SHA-1 Hash for the provided image, 21-5561.E01.

Consensus Result:
62868241dc672c662be2e2d14b1fb0e3f46520d4

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

Expected Response Illustration:

FTK Imager Showing SHA1 Hash verification of the image



Other Responses:
Seventeen participants reported the SHA-1 hash of the 21-5561.E01 file and not the stored verification hash.

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 2

Question 2: How many partitions are on the device imaged as 21-5561.E01?

Manufacturer's Expected Response:

Two (2)

WebCode - Test	Response
23UJ67-5561	2
29JUMG-5562	2
2YBWJR-5562	2
3B7V4P-5561	2
3RC2CZ-5561	There are 2 partition on 21-5561.E01. One partition is a System Reserve partition. Another partition is where the operating system is installed.
44372B-5561	2
4A86BF-5561	Partition 1 NTFS, (System Reserved) 579MB Partition 2, NTFS, 19,43GB
4UEFFJ-5561	2 partitions
66CHBZ-5561	2 Partitions
67H6N6-5562	2
6G29KN-5562	2
6LBUJ2-5561	Two partitions
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	2
6ZD7FZ-5561	2
7A2A6E-5561	2
7FMAEZ-5562	2
7W9P7F-5562	2
89LGKW-5561	Partition 1 System Reserved [NTFS] Partition 2 NONAME [NTFS]
89NM2E-5561	TWO (2)
8UH9ME-5562	Two partitions - 1st is the system reserved, 2nd is the data partition
8YVWFY-5561	2 - 1x Boot Partition - 1x User OS Partition
93AL3L-5562	2

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 2	
WebCode - Test	**Response**
9ARR2D-5561	2
9GULT8-5562	2
9V6AXV-5561	2
A8KGFG-5561	2 partitions (third partition is unallocated/unused space)
AK9F96-5561	2
AQYVXC-5562	2 partitions are present on the device imaged as 21-5561.E01.
AV4RGC-5562	2 (two) partitions
BGJGLT-5561	2 Partitions
BKPYQG-5561	Two Partitions
BMT8ZD-5561	2
BR6KUT-5562	2
BWZC2P-5561	2
CBTGPD-5562	2
CMHKPW-5561	2
CPRZ8G-5561	2
CQ9KB9-5562	Two
CQJQ7N-5561	2 partitions and 1 unpartitioned (unallocated) space. Partition 1 (579MB) / Partition 2 (19899MB) / Unpartitioned Unallocated Space).
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	2
E43HU2-5561	2
E7BXK2-5561	2
EELYM9-5561	Two (2)
F2UYKR-5561	There is only 1 partition in the given device image.
FFG39B-5562	2

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 2	
WebCode - Test	**Response**
FJWWP9-5562	2
FP3BPR-5562	2
FTFDBN-5561	2
G9A37K-5561	2
GGKE74-5561	2
GU9W29-5561	two
GZY7B8-5561	(2) two
H949ZJ-5561	2
HEBY4P-5561	2 partitions
HYFCYH-5561	Two
J3U2M6-5561	2
J3XR9B-5561	2
JF4GTB-5562	2
JJJA4W-5562	2
JMJLZW-5561	2
JU4NYL-5561	2 Partitions
K6Z7V8-5562	2
KE3C4M-5561	2
KH3MYM-5562	2
KT78B9-5562	2
KW3EPY-5561	Two
L9D7RX-5562	Two (02) partitions
LCV3Z2-5561	2
LEERBL-5562	2

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 2	
WebCode - Test	**Response**
LPY8P3-5561	2 partitions and 1 unpartitioned
LRRLAT-5562	2
LXXGTT-5561	2
M98EB2-5562	2
MWHHA4-5562	2
MYJKY6-5562	2
N66VNU-5561	Two
NFQ2KX-5562	2
NPAH8D-5561	2 partitions
NRJXPX-5561	2 partitions
NTAT4D-5561	Two (2)
NUKNP6-5562	2
PBBNHP-5561	2
PBQMFZ-5561	Two partitions: System Recovery: Partition 1, NTFS System Reserved 579MB; Windows File System: Partition 2, NTFS NONAME 19899MB
PTA4GV-5562	02
QP2MPV-5561	2 partitions
R36ZB9-5561	Two
RAQR4V-5562	2
RFUVTT-5561	Two (2)
RGQL4V-5561	2
RK6QRB-5561	2
RXCADP-5561	2 partitions (and an unpartitioned space entry)
T8F7TZ-5562	Two (2)
TCA8P9-5561	Two (2) Partitions (System Reserved [NTFS] and NONAME [NTFS])

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 2	
WebCode - Test	**Response**
TDLF3U-5561	2
TFMD29-5561	2
TMAWNW-5561	2
U298Q9-5561	2
U964DC-5562	2
UWTR4N-5561	2
V23CK9-5561	2
V96U7R-5561	2
VFHDED-5561	2
WHMDWP-5561	2
WLLU9J-5561	2
WRR3GT-5561	2
WW4B2Q-5561	2
X436QC-5562	Two (2)
X4L22Q-5562	2
XCDUFN-5561	2
XHHHQN-5561	2
XUR36B-5561	Two (2)
Y2ANWU-5561	2
YQTYXP-5561	Two
YXADZU-5561	2
YYKJVA-5561	2
ZGHWCN-5561	Two (2)
ZM6UW6-5561	2

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 2	
WebCode - Test	**Response**
ZTBFTE-5561	2

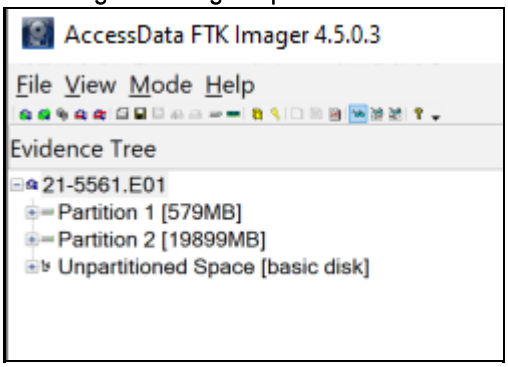
Question 2: How many partitions are on the device imaged as 21-5561.E01?

Consensus Result:
Two (2)

Expected Response Explanation:
The number of device partitions can be determined by reviewing the partition table. Most forensic suites and imaging tools can be used to identify this information.

Expected Response Illustration:

FTK Imager showing the partitions on the drive image.



EnCase Report of Drive Geometry

Partitions

Name	Id	Type	Start Sector	Total Sectors	Size
	07	NTFS	2,048	1,185,792	579 MB
	07	NTFS	1,187,840	40,753,152	19.4 GB

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3

Question 3: What is the volume serial number for the filesystem on the system partition? (Report the first 4 bytes (little endian) as it would be reported/displayed by Windows)

Manufacturer's Expected Response:

F617-480A and/or 3A16-DAAE

WebCode - Test	Response
23UJ67-5561	F617-480A
29JUMG-5562	F617-480A
2YBWJR-5562	0x3A16DAAE
3B7V4P-5561	F617-480A
3RC2CZ-5561	Reporting the first 4 bytes in little endian: 2C F6 17 7E. The volume serial number found is 0X0A 48 17 F6 7E 17 F6 2C.
44372B-5561	F617480A
4A86BF-5561	3A 16 DA AE
4UEFFJ-5561	F617
66CHBZ-5561	Little Endian as windows would see it (0A48-17F6)
67H6N6-5562	F617480A
6G29KN-5562	0x 3A 16 DA AE
6LBUJ2-5561	F617-480A
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	F617-480A
6ZD7FZ-5561	F617480A
7A2A6E-5561	F617480A
7FMAEZ-5562	3A16-DAAE
7W9P7F-5562	3A16-DAAE
89LGKW-5561	F617-480A
89NM2E-5561	F617480A
8UH9ME-5562	F617480A
8YVWFY-5561	0A4817F6

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3	
WebCode - Test	**Response**
93AL3L-5562	3A16-DAAE
9ARR2D-5561	F6 17 48 0A
9GULT8-5562	F617
9V6AXV-5561	F617-480A
A8KGFG-5561	DA AE
AK9F96-5561	F617-480A
AQYVXC-5562	3A16DAAE
AV4RGC-5562	F617480A
BGJGLT-5561	F617-480A
BKPYQG-5561	3A16
BMT8ZD-5561	F617-480A
BR6KUT-5562	F617-480A
BWZC2P-5561	3A16DAAE
CBTGPD-5562	F617480A
CMHKPW-5561	F617-480A
CPRZ8G-5561	3A16DAAE
CQ9KB9-5562	3A16
CQJQ7N-5561	Volume serial number – F617-480A
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	F6 17 48 0A
E43HU2-5561	F617-480A
E7BXK2-5561	F617-480A
EELYM9-5561	F617480A
F2UYKR-5561	1187

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3	
WebCode - Test	**Response**
FFG39B-5562	3A16-DAAE
FJWWP9-5562	F617480A
FP3BPR-5562	3A 16 DA AE
FTFDBN-5561	F617-480A
G9A37K-5561	F617-480A
GGKE74-5561	F617480A
GU9W29-5561	F617-480A 0A48 (little endian)
GZY7B8-5561	F617480A
H949ZJ-5561	F617-480A
HEBY4P-5561	3A16-DAAE
HYFCYH-5561	F617-480A
J3U2M6-5561	F617480A
J3XR9B-5561	3A16-DAAE
JF4GTB-5562	F617480A
JJJA4W-5562	F617-480A
JMJLZW-5561	F617
JU4NYL-5561	3A16
K6Z7V8-5562	3A16DAAE
KE3C4M-5561	3A16-DAAE
KH3MYM-5562	F617 480A
KT78B9-5562	F617480A
KW3EPY-5561	F617480A
L9D7RX-5562	F617480A
LCV3Z2-5561	F617-480A

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3	
WebCode - Test	**Response**
LEERBL-5562	3A16DAAE
LPY8P3-5561	3a 16 da ae
LRRLAT-5562	F617-480A
LXXGTT-5561	3A16DAAE
M98EB2-5562	0A4817F6
MWHHA4-5562	F617480A
MYJKY6-5562	F617480A
N66VNU-5561	F617-480A
NFQ2KX-5562	0A4817F6
NPAH8D-5561	F617-480A 0A 48 17 F6
NRJXPX-5561	F617-480A is the volume serial number. The first 4 bytes in little endian are 0A4817F6.
NTAT4D-5561	Partition 1 - System Reserved (Volume Serial Number = 3A16-DAAE) Partition 2 - NONAME [NTFS] (Volume Serial Number = F617-480A)
NUKNP6-5562	F617-480A
PBBNHP-5561	3A16DAAE
PBQMFZ-5561	F617480A
PTA4GV-5562	3A16-DAAE (System Reserved Partition)
QP2MPV-5561	F617480A
R36ZB9-5561	F617-480A
RAQR4V-5562	3A16DAAE
RFUVTT-5561	F617480A
RGQL4V-5561	F617480A
RK6QRB-5561	F617480A
RXCADP-5561	f617480a
T8F7TZ-5562	F617480A

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3	
WebCode - Test	**Response**
TCA8P9-5561	F617
TDLF3U-5561	3A16DAAE
TFMD29-5561	F617
TMAWNW-5561	1187840-41940991
U298Q9-5561	0A48-17F6
U964DC-5562	System Reserved Partition = 00 00 C1 00 (Serial Number - 3A16-DAAE) C Drive Partition = 00 0C 00 00 (Serial Number - F617-480A)
UWTR4N-5561	3A16-DAAE
V23CK9-5561	F617480A
V96U7R-5561	3A16DAAE
VFHDED-5561	0A 48 17 F6
WHMDWP-5561	F617-480A
WLLU9J-5561	F617-480A
WRR3GT-5561	F6 17 48 0A
WW4B2Q-5561	F617-480A
X436QC-5562	2C F6 17 7E
X4L22Q-5562	2C F6 17 7E - full serial number (64 bit) F6 17 48 0A - serial number (32 bit)
XCDUFN-5561	F617-480A
XHHHQN-5561	F617
XUR36B-5561	2C F6 17 7E
Y2ANWU-5561	Since Windows NT 3.1 Microsoft have defined this as the “System Reserved” Partition, containing the Boot loader. 3A16-DAAE NTFS
YQTYXP-5561	F617-480A (32bit) 2CF6-177E (64 bit)
YXADZU-5561	F617-480A
YYKJVA-5561	F617480A
ZGHWCN-5561	F6 14 48 0A

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3	
WebCode - Test	**Response**
ZM6UW6-5561	F617-480A
ZTBFTE-5561	3A16DAAE

Question 3: What is the volume serial number for the filesystem on the system partition? (Report the first 4 bytes (little endian) as it would be reported/displayed by Windows)

Consensus Result:

F617-480A and/or 3A16-DAAE.

Participants who reported the volume serial number in big endian 0A4817F6 were also included as part of the consensus.

Expected Response Explanation:

The volume serial number is parsed and reported by most forensic tools or can be viewed natively from Windows for a mounted filesystem. In most cases (not specific to MS Windows), "system partition" refers to the partition on which the operating system is installed. Microsoft calls this the "Windows Partition" and refers to the "EFI Partition" as the "System Partition" or "System Reserved Partition". Because of this ambiguity, both F617-480A (the Windows System Partition) and 3A16-DAAE (the system reserved partition) were accepted.

Expected Response Illustration:

FTK Imager view of information for the System Partition

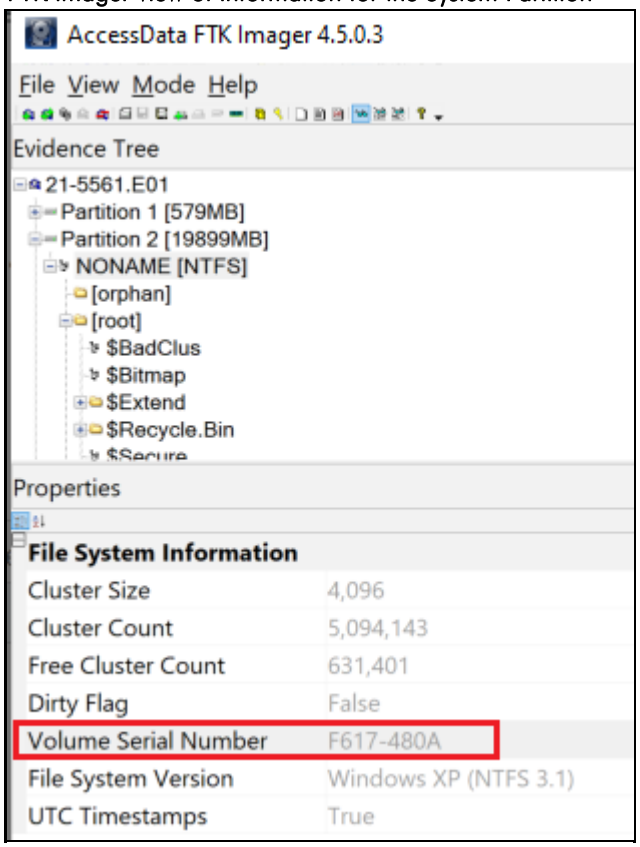
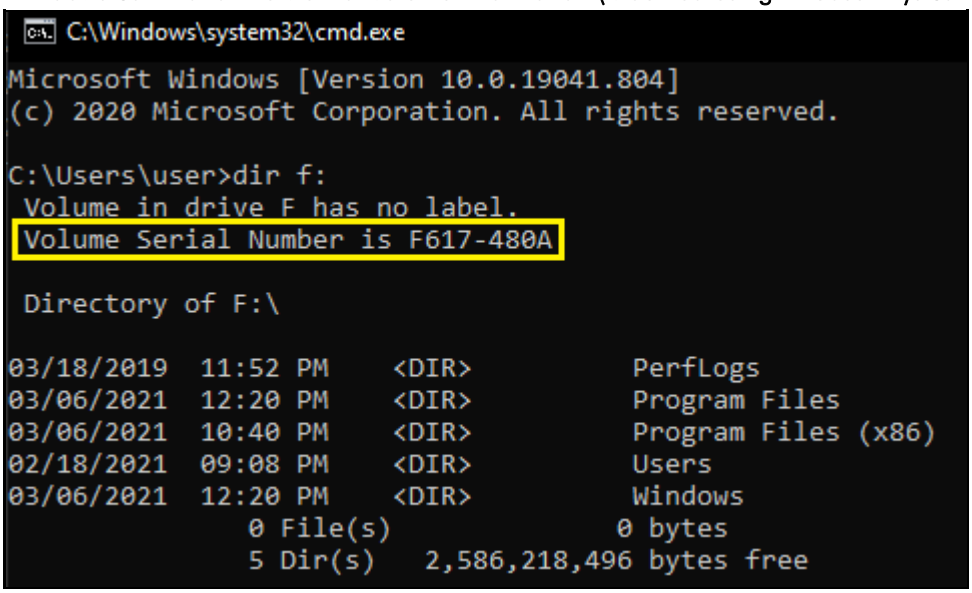


TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3

Windows command line view of volume information (Mounted using EnCase Physical Disk Emulator)



FTK Imager view of Volume Serial Number of System Reserved Partition

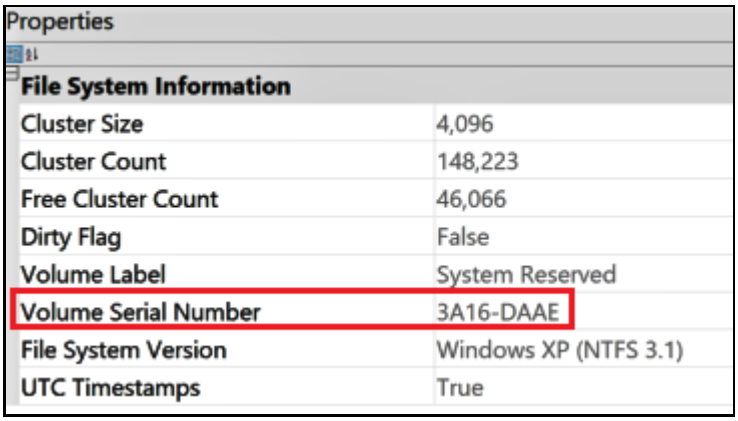


TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4

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

Manufacturer's Expected Response:

Windows 10 Home

WebCode - Test	Response
23UJ67-5561	Windows 10 Home Core Build 18362
29JUMG-5562	Sistema operativo: Windows 10 Home (1903) Número de versión: 6.3 Número de compilación: 18362
2YBWJR-5562	Windows 10 Home V6.3 Build 18362
3B7V4P-5561	Windows 10 Home
3RC2CZ-5561	The operating system installed on the computer is Windows 10 Home with a 1903 release ID.
44372B-5561	Windows 10 Home 1903
4A86BF-5561	Windows 10 Home Version 6.3, compilation 18362
4UEFFJ-5561	Windows 10 Version: 6.3 Edition: Home
66CHBZ-5561	Windows 10 Home, Version 6.3, Build Number 18362
67H6N6-5562	Windows 10 Home (1903) 6.3
6G29KN-5562	Windows 10 Home Version 6.3
6LBUJ2-5561	Windows 10 Home 64bit build 18362
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	Windows 10 Home
6ZD7FZ-5561	Windows 10 Home version 6.3 Core Edition
7A2A6E-5561	Windows 10 Home
7FMAEZ-5562	Windows 10 Home (1903) v.6.3
7W9P7F-5562	Windows 10 Home Edition: Core Version: 6.3
89LGKW-5561	Windows 10 Home Version Number 6.3
89NM2E-5561	Windows 10 Home
8UH9ME-5562	Windows 10 Home (1903) version 6.3
8YVWFY-5561	Windows 10 Home (1903) v6.3

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4	
WebCode - Test	**Response**
93AL3L-5562	Windows 10 Home (1093) Version 6.3 Build 18362
9ARR2D-5561	Windows 10 Home version 6.3
9GULT8-5562	Windows 10 Home
9V6AXV-5561	Windows 10 Home (1903)
A8KGFG-5561	Windows 10 Home 1903 Current build: 18362
AK9F96-5561	Windows 10 Home 1903 10.0.18362.30
AQYVXC-5562	Windows 10 Home (1903), Version 6.3, Build 18362
AV4RGC-5562	Windows 10 Home (1903) v6.3
BGJGLT-5561	Windows 10 Home V 6.3
BKPYQG-5561	Windows 10 Home 1903
BMT8ZD-5561	Windows 10 Home (1903) version 6.3
BR6KUT-5562	Windows 10 Home (1903) – 6.3
BWZC2P-5561	Windows 10 Home Edition Version 1903
CBTGPD-5562	Windows 10 Home (1903) Core v6.3 build 18362
CMHKPW-5561	Windows 10 Home version 1903 and 18362 edition
CPRZ8G-5561	Windows 10 Home 1903
CQ9KB9-5562	Windows 10 Home (1903) version 6.3
CQJQ7N-5561	Operating system – Windows 10 Home
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	Windows 10 Home Ver 6.3
E43HU2-5561	Windows 10 Home 1903
E7BXK2-5561	Windows 10 Home
EELYM9-5561	Windows 10 Home (1903) 6.3
F2UYKR-5561	Windows 10 Home

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4	
WebCode - Test	**Response**
FFG39B-5562	Windows 10 Home (19h1_release, build 18362)
FJWWP9-5562	Windows 10 Home Version:6.3
FP3BPR-5562	Windows 10 Home (Version 6.3 / Core edition)
FTFDBN-5561	Windows 10 Home
G9A37K-5561	Windows 10 Home (Version 1903)
GGKE74-5561	Windows 10 Home
GU9W29-5561	Windows 10 Home (6.3.18362)
GZY7B8-5561	Windows 10 Home (1903) V. 6.3
H949ZJ-5561	Windows 10 Home 1903
HEBY4P-5561	Windows 10 Home Core V 6.3
HYFCYH-5561	Windows 10 Home Edition version 1903 build 18362
J3U2M6-5561	Windows 10 Home (1903) 6.3
J3XR9B-5561	Windows 10 Home 1903
JF4GTB-5562	Windows 10 Home version 6.3
JJJA4W-5562	Windows 10 Home
JMJLZW-5561	Windows 10 Home
JU4NYL-5561	Windows 10 Home (1903) 6.3
K6Z7V8-5562	Windows 10 Home (1903) v6.3
KE3C4M-5561	Windows 10 Home (1903) versio 6.3
KH3MYM-5562	Windows 10 Home, Version 6.3
KT78B9-5562	Windows 10 Home, version number:6.3
KW3EPY-5561	Product Name: Windows 10 Home Current version: 6.3 EditionID: Core
L9D7RX-5562	Windows 10 Home (1903) version 6.3
LCV3Z2-5561	Windows 10 Home version 1903

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4	
WebCode - Test	**Response**
LEERBL-5562	Windows 10 Home (1903) Core Version 6.3 Build Number 18362
LPY8P3-5561	Windows 10 (1903) version 6.3
LRRLAT-5562	Windows 10 Home version 6.3; build number 18362
LXXGTT-5561	Windows 10 Home
M98EB2-5562	Windows 10 Home (1903) version 6.3
MWHHA4-5562	Windows 10 Home (1903) Version 6.3
MYJKY6-5562	Windows 10 Home
N66VNU-5561	Windows 10 Home
NFQ2KX-5562	Windows 10 Home (1903) Multiprocessor Free 6.3.18362.19h1_release.190318-1202
NPAH8D-5561	Windows 10 Home
NRJXPX-5561	Windows 10 Home version 6.3
NTAT4D-5561	Windows 10 Home (version 6.3)
NUKNP6-5562	Windows 10 Home (1903), version 6.3
PBBNHP-5561	Windows 10 Home (1903) Version 6.3
PBQMFZ-5561	Windows 10 Home 6.3
PTA4GV-5562	Windows 10 Home (Version: 10.0.18362.30, edition: Core)
QP2MPV-5561	Windows 10 Home (1903) version 6. 3 build 18362
R36ZB9-5561	Windows 10 Home (1903) Version 6.3
RAQR4V-5562	Windows 10 Home (1903)
RFUVTT-5561	Windows 10 Home (1903) 6.3
RGQL4V-5561	Windows 10 Home (1903 v6.3 build 18632)
RK6QRB-5561	Windows 10 Home Version 1903 Build 18362
RXCADP-5561	Windows 10 Home (1903); version number: 6.3
T8F7TZ-5562	Windows 10 Home (1903) 6.3

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4	
WebCode - Test	**Response**
TCA8P9-5561	Windows 10 Home (1903), Build Number 18362
TDLF3U-5561	Windows 10 (1903) Version 6.3
TFMD29-5561	Windows 10 Home
TMAWNW-5561	Windows 10 Home (1903)
U298Q9-5561	Windows 10 Home Version 6.3
U964DC-5562	Windows 10 Home version 6.3 build 18362
UWTR4N-5561	Windows 10 Home (1903) Version 6.3
V23CK9-5561	Windows 10 Home version 6.3
V96U7R-5561	Windows 10 Home (1903) version 6.3
VFHDED-5561	Windows 10 Home version 1903
WHMDWP-5561	Windows 10 Home (1903), Version 6.3
WLLU9J-5561	version 1903, edition : “may 2019 update” , Windows 10 Home release 19h1
WRR3GT-5561	Windows 10 Home (1903) version 6.3 Build 18362
WW4B2Q-5561	Windows 10 Home (1903) v6.3
X436QC-5562	Windows 10 (Home Edition)
X4L22Q-5562	Windows 10 Home 6.3
XCDUFN-5561	Windows 10 Home
XHHHQN-5561	Windows 10 Home (1903) 6.3 Build18362
XUR36B-5561	Microsoft Windows 10 (Home Edition)
Y2ANWU-5561	Windows 10 Home (1903) version 6.3
YQTYXP-5561	Windows 10 Home; Version 6.3 Build 18362
YXADZU-5561	Windows 10 Home
YYKJVA-5561	Windows 10 Home (1903) 6.3
ZGHWCN-5561	Windows 10 Home (1903) Version 6.3

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4	
WebCode - Test	**Response**
ZM6UW6-5561	Windows 10 Home
ZTBFTE-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 hive at C:\Windows\System32\Config\Software: Microsoft\Windows NT\CurrentVersion: ProductName.

Expected Response Illustration:

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

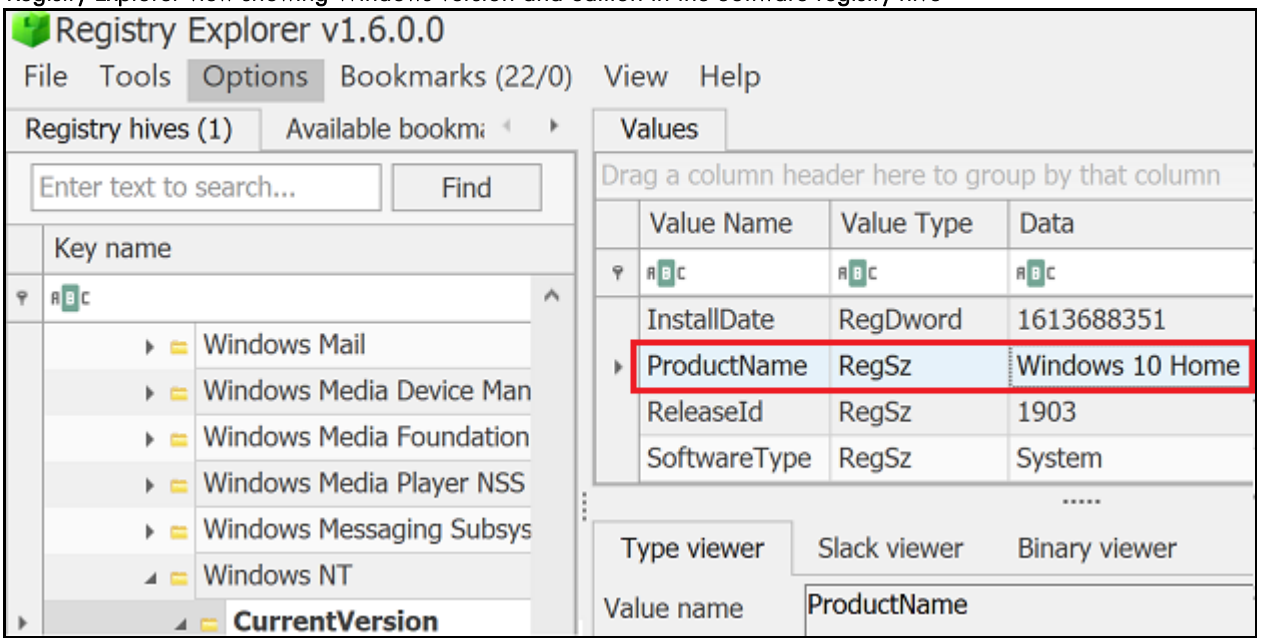


TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 5

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

Manufacturer's Expected Response:

susie

WebCode - Test	Response
23UJ67-5561	susie
29JUMG-5562	susie
2YBWJR-5562	susie
3B7V4P-5561	susie
3RC2CZ-5561	The registered owner of the installed operating system is "susie".
44372B-5561	susie
4A86BF-5561	Susie
4UEFFJ-5561	Susie
66CHBZ-5561	Registered Owner of OS - susie
67H6N6-5562	susie
6G29KN-5562	susie
6LBUJ2-5561	susie
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	susie
6ZD7FZ-5561	susie
7A2A6E-5561	susie
7FMAEZ-5562	susie
7W9P7F-5562	susie
89LGKW-5561	susie
89NM2E-5561	susie
8UH9ME-5562	susie
8YVWFY-5561	susie
93AL3L-5562	susie

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 5	
WebCode - Test	**Response**
9ARR2D-5561	susie
9GULT8-5562	susie
9V6AXV-5561	susie
A8KGFG-5561	Susie
AK9F96-5561	susie
AQYVXC-5562	susie
AV4RGC-5562	susie
BGJGLT-5561	susie
BKPYQG-5561	susie
BMT8ZD-5561	susie
BR6KUT-5562	susie
BWZC2P-5561	susie
CBTGPD-5562	susie
CMHKPW-5561	susie
CPRZ8G-5561	susie
CQ9KB9-5562	susie
CQJQ7N-5561	Registered owner of this operating system installation – “susie”
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	susie
E43HU2-5561	susie
E7BXK2-5561	susie
EELYM9-5561	susie
F2UYKR-5561	The registered owner of the system is susie.
FFG39B-5562	susie

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 5	
WebCode - Test	**Response**
FJWWP9-5562	Susie
FP3BPR-5562	susie
FTFDBN-5561	susie
G9A37K-5561	susie
GGKE74-5561	susie
GU9W29-5561	Susie
GZY7B8-5561	Susie
H949ZJ-5561	susie
HEBY4P-5561	susie
HYFCYH-5561	susie
J3U2M6-5561	susie
J3XR9B-5561	susie
JF4GTB-5562	susie
JJJA4W-5562	susie
JMJLZW-5561	susie
JU4NYL-5561	susie
K6Z7V8-5562	susie
KE3C4M-5561	susie
KH3MYM-5562	susie
KT78B9-5562	susie
KW3EPY-5561	RegisteredOwner: susie
L9D7RX-5562	susie
LCV3Z2-5561	susie
LEERBL-5562	Susie

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 5	
WebCode - Test	**Response**
LPY8P3-5561	susie
LRRLAT-5562	susie
LXXGTT-5561	susie
M98EB2-5562	susie
MWHHA4-5562	susie
MYJKY6-5562	susie
N66VNU-5561	susie
NFQ2KX-5562	susie
NPAH8D-5561	susie
NRJXPX-5561	susie
NTAT4D-5561	susie
NUKNP6-5562	susie
PBBNHP-5561	susie
PBQMFZ-5561	Susie
PTA4GV-5562	susie
QP2MPV-5561	susie
R36ZB9-5561	susie
RAQR4V-5562	susie
RFUVTT-5561	susie
RGQL4V-5561	susie
RK6QRB-5561	susie
RXCADP-5561	susie
T8F7TZ-5562	susie
TCA8P9-5561	susie

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 5	
WebCode - Test	**Response**
TDLF3U-5561	Susie
TFMD29-5561	susie
TMAWNW-5561	susie
U298Q9-5561	susie
U964DC-5562	susie
UWTR4N-5561	susie
V23CK9-5561	susie
V96U7R-5561	susie
VFHDED-5561	susie
WHMDWP-5561	susie
WLLU9J-5561	susie
WRR3GT-5561	susie
WW4B2Q-5561	susie
X436QC-5562	susie
X4L22Q-5562	susie
XCDUFN-5561	susie
XHHHQN-5561	susie
XUR36B-5561	susie
Y2ANWU-5561	“susie”
YQTYXP-5561	susie
YXADZU-5561	susie
YYKJVA-5561	susie
ZGHWCN-5561	susie
ZM6UW6-5561	susie

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 5	
WebCode - Test	**Response**
ZTBFTE-5561	susie

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

Consensus Result:

susie

Expected Response Explanation:

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

Expected Response Illustration:

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

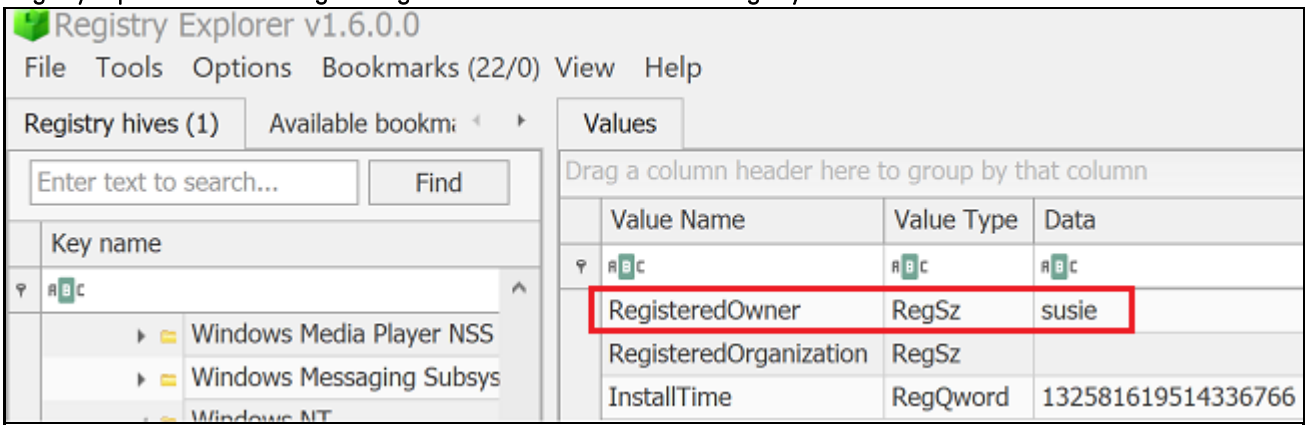


TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6

Question 6: When was the operating system installed? Provide the answer in UTC + 00:00 using the following format: MM/DD/YYYY HH:MM:SS AM/PM.

Manufacturer's Expected Response:
02/18/2021 22:45:51 PM

WebCode - Test	Response
23UJ67-5561	02/18/2021 11:45:51 PM AM
29JUMG-5562	02/18/2021 22:45:51
2YBWJR-5562	02/18/2021 10:45:51 PM
3B7V4P-5561	02/18/2021 22:45:51 PM
3RC2CZ-5561	The operating system was installed on 02/18/2021 22:45:51 PM UTC.
44372B-5561	02/18/2021 10:45:51 PM
4A86BF-5561	02/18/2021 10:45:51 PM
4UEFFJ-5561	2/18/2021 10:45:51 PM
66CHBZ-5561	Install Date – UTC 02/18/2021 22:45:51 PM
67H6N6-5562	02/18/2021 10:45:51 PM
6G29KN-5562	02/18/2021 10:45:51 PM
6LBUJ2-5561	02/18/2021 10:45:51 PM
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	02/18/2021 10:45:51 PM
6ZD7FZ-5561	02/18/2021 10:45:51 PM
7A2A6E-5561	02/18/2021 10:45:51 PM
7FMAEZ-5562	02/18/2021 22:45:51 PM
7W9P7F-5562	02/18/2021 10:45:51 PM
89LGKW-5561	02/18/2021 10:45:2021 PM
89NM2E-5561	02/18/2021 10:45:51 PM(UTC + 00:00)
8UH9ME-5562	02/18/2021 10:45:51 PM
8YVWFY-5561	02/18/2021 10:45:51 PM (18th February 2021 - 22:45:51)

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6	
WebCode - Test	**Response**
93AL3L-5562	2/18/2021 10:45:51 PM
9ARR2D-5561	02/18/2021 22:45:51 PM
9GULT8-5562	02/18/2021 10:45:51 PM
9V6AXV-5561	2/18/2021 10:45:51 PM
A8KGFG-5561	18/02/2021 22:45:51 PM +0
AK9F96-5561	02/18/2021 10:45:51 PM
AQYVXC-5562	Thu Feb 18 22:45:51 2021
AV4RGC-5562	02.18.2021 10:45:51 PM
BGJGLT-5561	02/18/2021 10:45:51 PM GMT
BKPYQG-5561	02/18/2021 10:45:51 PM
BMT8ZD-5561	02/18/2021 10:45:51 PM
BR6KUT-5562	02/18/2021 10:45:51 PM
BWZC2P-5561	02/18/2021 22:45:51 UTC
CBTGPD-5562	02/18/2021 10:45:51 PM
CMHKPW-5561	02/18/2021 10:45:51 PM
CPRZ8G-5561	02/18/2021 10:45:51 PM
CQ9KB9-5562	02/18/2021 10:45:51 PM
CQJQ7N-5561	Operating system installed – 02/18/2021 10:45:51 PM (22:45:51) UTC
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	02/18/2021 10:45:51 PM
E43HU2-5561	02/18/2021 10:45:51 PM
E7BXK2-5561	02/18/2021 10:45:51 PM UTC+0
EELYM9-5561	02/18/2021 10:45:51 PM
F2UYKR-5561	The operating system was installed on 02/21/2021 01:52:03 AM.

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6

WebCode - Test	Response
FFG39B-5562	02/18/2021 10:45:51 PM
FJWWP9-5562	02/18/2021 22:45:51
FP3BPR-5562	02-18-2021 10:45:51 PM UTC +00:00
FTFDBN-5561	02/18/2021 10:45:51 PM
G9A37K-5561	Registry shows installation time as 02/18/2021 10:45:51 PM, however this may also reflect a Windows update. The creation of system folders, typically created when Windows is installed, reflects the date of 3/19/2019 around 4:37:21 AM. This includes the Windows, Users, ProgramData folders and the Root directory.
GGKE74-5561	02/18/2021 10:45:51 PM
GU9W29-5561	02/18/2021 10:45:51 PM
GZY7B8-5561	02/18/2021 10:45:51 PM
H949ZJ-5561	02/18/2021 22:45:51 UTC
HEBY4P-5561	02/18/2021 10:45:51 PM UTC
HYFCYH-5561	02/18/2021 22:45:51 PM
J3U2M6-5561	2/18/2021 10:45:51 PM
J3XR9B-5561	Thursday, February 18, 2021 at 10:45:51 PM Greenwich Mean Time
JF4GTB-5562	02/18/2021 10:45:51 PM
JJJA4W-5562	02/18/2021 10:45:51 PM
JMJLZW-5561	02/18/2021 10:45:51 PM
JU4NYL-5561	02/18/2021 22:45:51 PM (18th February 2021 - 10:45:51 PM)
K6Z7V8-5562	02/18/2021 22:45:51 PM
KE3C4M-5561	02/18/2021 10:45:51 PM
KH3MYM-5562	02/18/2021 10:45:51 PM
KT78B9-5562	02/18/2021 10:45:51 PM GMT
KW3EPY-5561	02/18/2021 10:45:51 PM
L9D7RX-5562	02/18/2021 10:45:51 PM
LCV3Z2-5561	02/18/2021 10:45:51 PM UTC + 00:00

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6	
WebCode - Test	**Response**
LEERBL-5562	02/18/2021 10:45:51 PM
LPY8P3-5561	02/18/2021 10:45:51 AM
LRRLAT-5562	02/18/2021 22:45:51 PM
LXXGTT-5561	02/18/2021 10:45:51 PM
M98EB2-5562	02/18/2021 22:45:51 pm
MWHHA4-5562	02/18/2021 22:45:51 PM
MYJKY6-5562	02/18/2021 22:45:51 PM
N66VNU-5561	02/18/2021 10:45:51 PM
NFQ2KX-5562	02/18/2021 10:45:51 PM
NPAH8D-5561	02/18/2021 22:45:51
NRJXPX-5561	02/18/2021 22:45:51 PM
NTAT4D-5561	02/18/2021 22:45:51 UTC = 02/18/2021 10:45:51 PM
NUKNP6-5562	02/18/2021 21:45:51 PM
PBBNHP-5561	02/18/2021 10:45:51 PM
PBQMFZ-5561	2/18/2021 10:45:51 PM
PTA4GV-5562	02/18/2021 10:45:51 PM
QP2MPV-5561	02/18/2021 10:45:51 PM
R36ZB9-5561	02/18/2021 10:45:51 PM
RAQR4V-5562	02/18/2021 10:45:51 PM
RFUVTT-5561	02/18/2021 22:45:51 PM
RGQL4V-5561	02/18/2021 10:45:51 PM
RK6QRB-5561	02/18/2021 10:45:51 PM
RXCADP-5561	02/18/2021 22:45:51 PM
T8F7TZ-5562	02/18/2021 22:45:51 PM

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6	
WebCode - Test	**Response**
TCA8P9-5561	02/18/2021 10:45:51 PM
TDLF3U-5561	02/18/2021 10:45:51 AM
TFMD29-5561	02/18/2021 10:45:51 PM
TMAWNW-5561	02.18.2021 09:45:51 PM
U298Q9-5561	02/28/2021 10:45:51 PM UTC
U964DC-5562	02/18/2021 22:45:51 PM
UWTR4N-5561	02/18/2021 10:45:51 PM
V23CK9-5561	02/18/2021 10:45:51 AM
V96U7R-5561	02/18/2021 10:45:51 PM
VFHDED-5561	02/18/2021 22:45:51 (10:45:51 PM)
WHMDWP-5561	02/18/2021 10:45:51 PM
WLLU9J-5561	02/18/2021 10:45:51 PM UTC
WRR3GT-5561	02/18/2021 10:45:51 PM
WW4B2Q-5561	02/18/2021 10:45:51 PM
X436QC-5562	02/18/2021 10:45:51 PM
X4L22Q-5562	02/18/2021 10:45:51 PM
XCDUFN-5561	02/18/2021 10:45:51 PM
XHHHQN-5561	02/18/2021 10:45:51 PM
XUR36B-5561	02/18/2021 10:45:51 PM
Y2ANWU-5561	02/18/2021 22:45:51 PM
YQTYXP-5561	02/18/2021 22:45:51
YXADZU-5561	02/18/2021 22:45:51 PM
YYKJVA-5561	02/18/2021 10:45:51 PM
ZGHWCN-5561	02/18/2021 10:45:51 PM

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6

WebCode - Test	Response
ZM6UW6-5561	02/18/2021 10:45:51 PM
ZTBFTE-5561	02/18/2021 10:45:51 PM

Question 6: When was the operating system installed? Provide the answer in UTC + 00:00 using the following format: MM/DD/YYYY HH:MM:SS AM/PM.

Consensus Result:

02/18/2021 22:45:51 PM and all formatting styles including different time zones which represent the same information.

Expected Response Explanation:

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

Expected Response Illustration:

Registry Viewer display of InstallTime key value and FILETIME parsing as UTC date/time

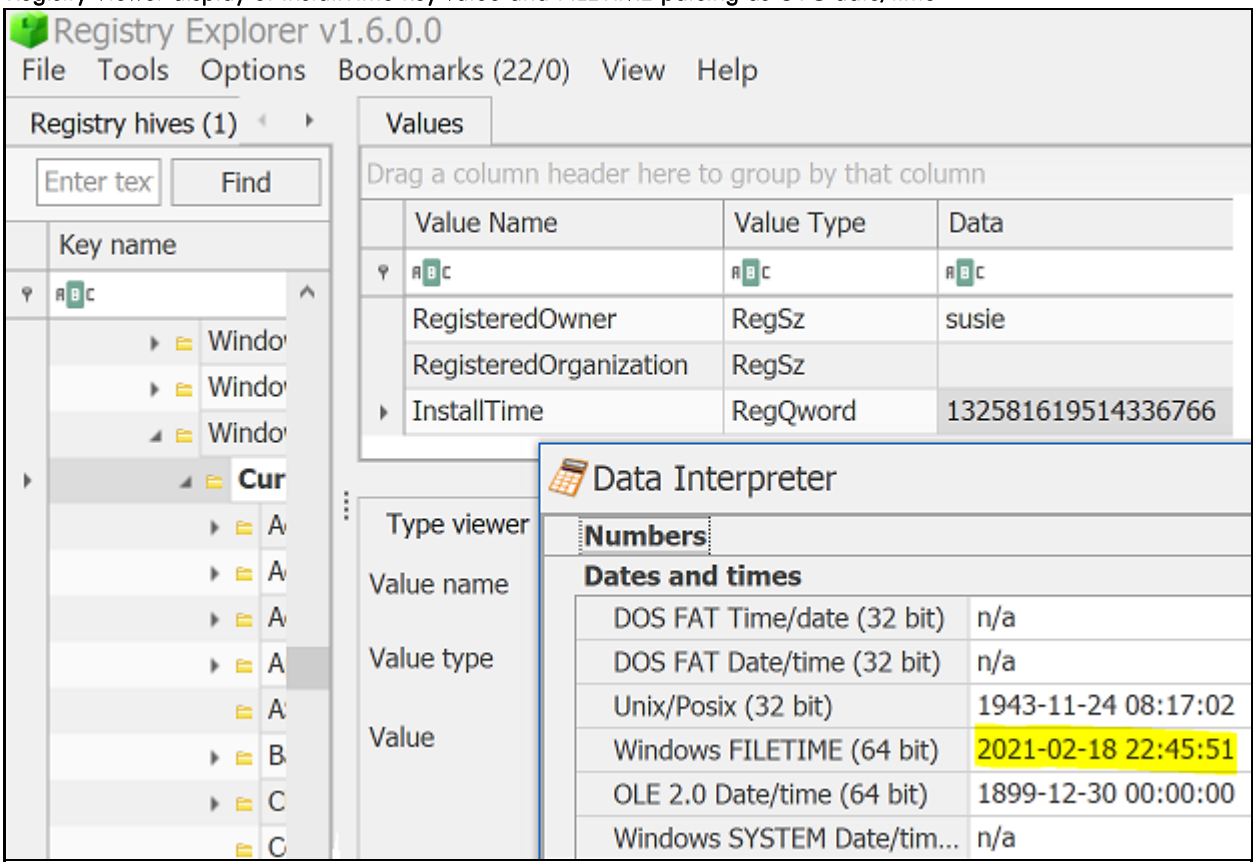


TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6

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

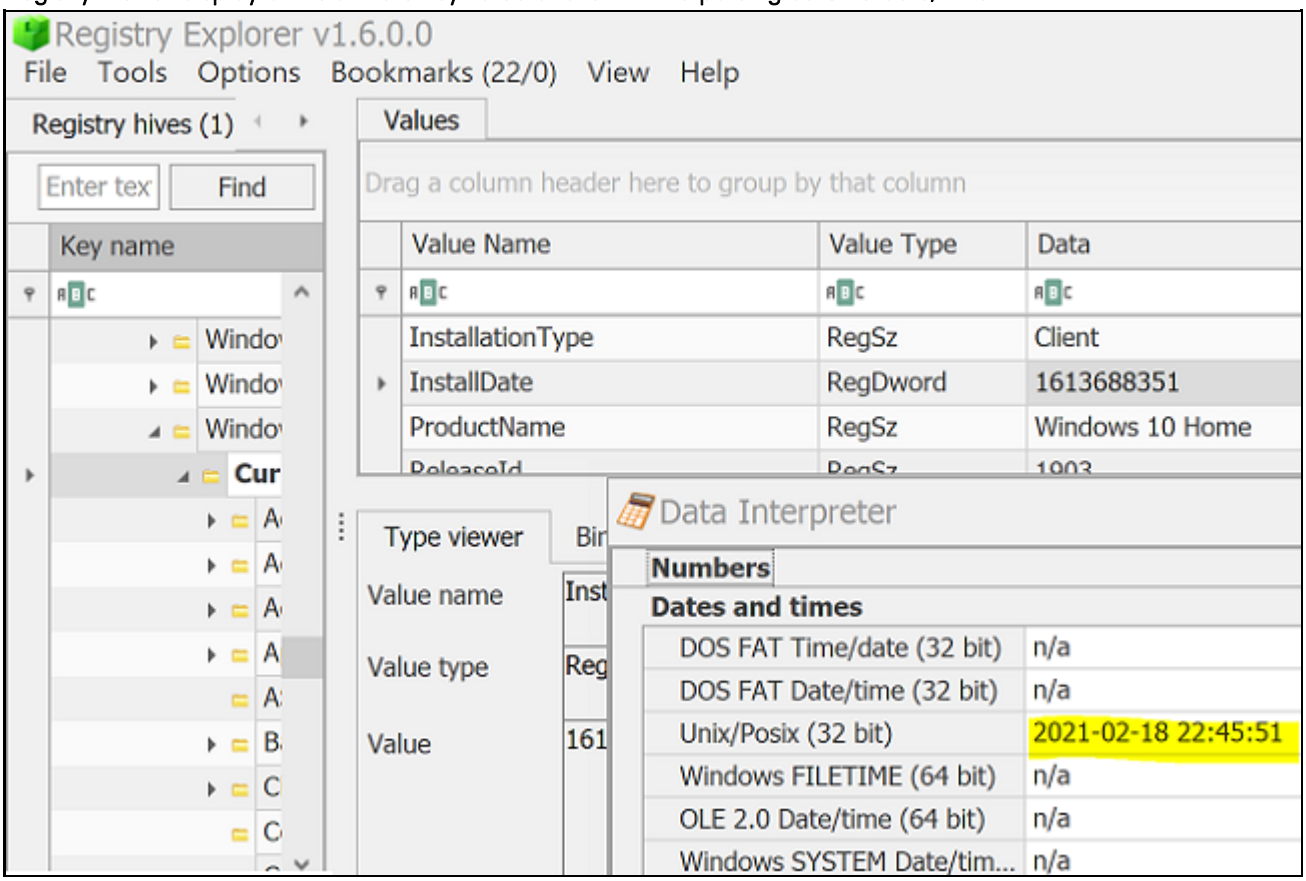


TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7

Question 7: When was the device LAST shutdown gracefully? Provide the answer in UTC + 00:00 using the following format: MM/DD/YYYY HH:MM:SS AM/PM.

Manufacturer's Expected Response:
03/10/2021 02:45:33 AM

WebCode - Test	Response
23UJ67-5561	03/10/2021 02:45:33 AM
29JUMG-5562	03/10/2021 2:45:33
2YBWJR-5562	03/10/2021 02:45:33 AM
3B7V4P-5561	03/10/2021 02:45:33 AM
3RC2CZ-5561	The device was last gracefully shutdown on 03/10/2021 02:45:33 AM UTC.
44372B-5561	03/10/2021 02:45:33 AM
4A86BF-5561	03/10/2021 02:45:33 AM
4UEFFJ-5561	3/10/2021 2:45:33 AM
66CHBZ-5561	Device last shutdown – UTC 03/10/2021 02:45:31 AM
67H6N6-5562	03/10/2021 02:45:33 AM
6G29KN-5562	03/10/2021 02:45:33 AM
6LBUJ2-5561	03/10/2021 02:45:32 AM
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	03/10/2021 02:45:33 AM
6ZD7FZ-5561	03/10/2021 02:45:33 AM
7A2A6E-5561	03/10/2021 02:45:31 AM
7FMAEZ-5562	03/10/2021 02:45:33 AM
7W9P7F-5562	03/10/2021 02:45:33 AM
89LGKW-5561	03/10/2021 02:45:33 AM
89NM2E-5561	03/10/2021 02:45:33 AM(UTC + 00:00)
8UH9ME-5562	03/10/2021 02:45:33 AM
8YVWFY-5561	03/10/2021 02:45:33 AM (10th March 2021 - 02:45:33)

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7	
WebCode - Test	**Response**
93AL3L-5562	3/10/2021 2:45:33 AM
9ARR2D-5561	03/10/2021 02:45:33 AM
9GULT8-5562	03/10/2021 2:45:33 AM UTC
9V6AXV-5561	3/10/2021 2:45:33 AM
A8KGFG-5561	10/03/2021 02:45:33 AM +0
AK9F96-5561	03/10/2021 02:45:32 AM
AQYVXC-5562	10/03/2021 02:45:33 UTC
AV4RGC-5562	03.10.2021 02:45:33 AM
BGJGLT-5561	03/10/2021 02:45:33 AM GMT
BKPYQG-5561	03/10/2021 2:45:33 AM
BMT8ZD-5561	03/10/2021 02:45:33 AM
BR6KUT-5562	03/10/2021 02:45:33 AM
BWZC2P-5561	03/10/2021 02:45:33 UTC
CBTGPD-5562	03/10/2021 02:45:33 AM
CMHKPW-5561	03/10/2021 2:45:33 AM
CPRZ8G-5561	03/10/2021 02:45:33 AM
CQ9KB9-5562	03/10/2021 02:45:33 AM
CQJQ7N-5561	Last graceful shutdown – 03/10/2021 02:45:33 AM (02:45:33) UTC
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	03/10/2021 02:45:33 AM
E43HU2-5561	03/10/2021 02:45:33 AM
E7BXK2-5561	03/10/2021 02:45:33 AM UTC+0
EELYM9-5561	03/10/2021 02:45:33 AM
F2UYKR-5561	The last graceful shutdown was on 03/10/2021 02:45:33 AM.

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7	
WebCode - Test	**Response**
FFG39B-5562	03/10/2021 02:45:33 AM
FJWWP9-5562	03/10/2021 02:45:33
FP3BPR-5562	The device was last shutdown gracefully on 03-10-2021 02:45:33 AM UTC +00:00
FTFDBN-5561	03/10/2021 02:45:33 AM
G9A37K-5561	03/10/2021 02:45:33 AM
GGKE74-5561	03/10/2021 02:45:31 AM
GU9W29-5561	03/10/2021 02:45:33 AM
GZY7B8-5561	03/10/2021 02:45:33 AM
H949ZJ-5561	03/10/2021 2:45:33 UTC
HEBY4P-5561	03/10/2021 02:45:33 AM UTC
HYFCYH-5561	03/10/2021 02:45:31 AM
J3U2M6-5561	3/10/2021 2:45:33 AM
J3XR9B-5561	Wednesday, March 10, 2021 at 2:45:33 AM Greenwich Mean Time
JF4GTB-5562	03/10/2021 02:45:33 AM
JJJA4W-5562	03/10/2021 02:45:33 AM
JMJLZW-5561	03/10/2021 02:45:33 AM
JU4NYL-5561	03/10/2021 02:45:33 AM (10th March 2021 - 02:45:33 AM)
K6Z7V8-5562	03/10/2021 02:45:33 AM
KE3C4M-5561	03/10/2021 2:45:33 AM
KH3MYM-5562	03/10/2021 02:45:33 AM
KT78B9-5562	03/10/2021 02:45:33 AM
KW3EPY-5561	03/10/2021 02:24:33 AM
L9D7RX-5562	03/10/2021 02:45:32 AM
LCV3Z2-5561	03/10/2021 02:45:33 AM UTC + 00:00

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7	
WebCode - Test	**Response**
LEERBL-5562	03/10/2021 02:45:33 AM
LPY8P3-5561	3/10/2021 02:45:33 AM
LRRLAT-5562	03/10/2021 02:45:33 AM
LXXGTT-5561	03/10/2021 02:45:33 AM
M98EB2-5562	03/10/2021 02:45:33 am
MWHHA4-5562	03/10/2021 02:45:33 AM
MYJKY6-5562	03/10/2021 02:45:33 AM
N66VNU-5561	03/10/2021 02:45:33 AM
NFQ2KX-5562	03/10/2021 02:45:33 AM
NPAH8D-5561	03/10/2021 02:45:31
NRJXPX-5561	3/10/2021 02:45:33 AM
NTAT4D-5561	03/10/2021 02:45:33 UTC = 03/10/2021 02:45:33 AM
NUKNP6-5562	03/10/2021 01:45:33 AM
PBBNHP-5561	03/10/2021 02:45:33 AM
PBQMFZ-5561	03/10/2021 2:45:33 AM
PTA4GV-5562	03/10/2021 02:45:33 AM
QP2MPV-5561	03/10/2021 02:45:33 AM
R36ZB9-5561	03/10/2021 02:45:33 AM
RAQR4V-5562	03/10/2021 02:45:33 AM
RFUVTT-5561	03/10/2021 02:45:33 AM
RGQL4V-5561	03/10/2021 02:45:33 AM
RK6QRB-5561	03/10/2021 02:45:33 AM
RXCADP-5561	03/10/2021 02:45:33 AM
T8F7TZ-5562	03/10/2021 02:45:33 AM

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7	
WebCode - Test	**Response**
TCA8P9-5561	03/10/2021 02:45:33 AM
TDLF3U-5561	03/10/2021 02:45:33 AM
TFMD29-5561	03/10/2021 02:45:33 AM
TMAWNW-5561	2021 01:45:33 AM
U298Q9-5561	03/10/2021 02:45 AM UTC
U964DC-5562	03/10/2021 02:45:33 AM
UWTR4N-5561	03/10/2021 02:45:33 AM
V23CK9-5561	03/10/2021 02:45:31 AM
V96U7R-5561	03/10/10/2021 02:45:33 AM
VFHDED-5561	03/10/2021 02:45:33 UTC (02:45:33 AM)
WHMDWP-5561	03/10/2021 02:45:33 AM
WLLU9J-5561	Last shutdown: 03/10/2021 2:45:33 AM UTC
WRR3GT-5561	03/10/2021 2:45:33 AM
WW4B2Q-5561	03/10/2021 02:45:33 AM
X436QC-5562	03/10/2021 02:45:33 AM
X4L22Q-5562	03/10/2021 02:45:33 AM
XCDUFN-5561	03/10/2021 02:45:33 AM
XHHHQN-5561	03/10/2021 02:45:33 AM
XUR36B-5561	03/10/2021 02:45:33 AM
Y2ANWU-5561	03/10/2021 02:45:33 AM
YQTYXP-5561	03/10/2021 02:45:33
YXADZU-5561	03/10/2021 02:45:32 AM
YYKJVA-5561	03/10/2021 02:45:33 AM
ZGHWCN-5561	03/10/2021 02:45:33 AM

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7

WebCode - Test	Response
ZM6UW6-5561	03/10/2021 02:45:33 AM
ZTBFTE-5561	03/10/2021 02:45:33 AM

Question 7: When was the device LAST shutdown gracefully? Provide the answer in UTC + 00:00 using the following format: MM/DD/YYYY HH:MM:SS AM/PM.

Consensus Result:

03/10/2021 02:45:33 AM and all formatting styles including different time zones which represent the same information. Although, milliseconds were requested in this question they were disregarded as part of participants' responses.

Expected Response Explanation:

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

Expected Response Illustration:

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

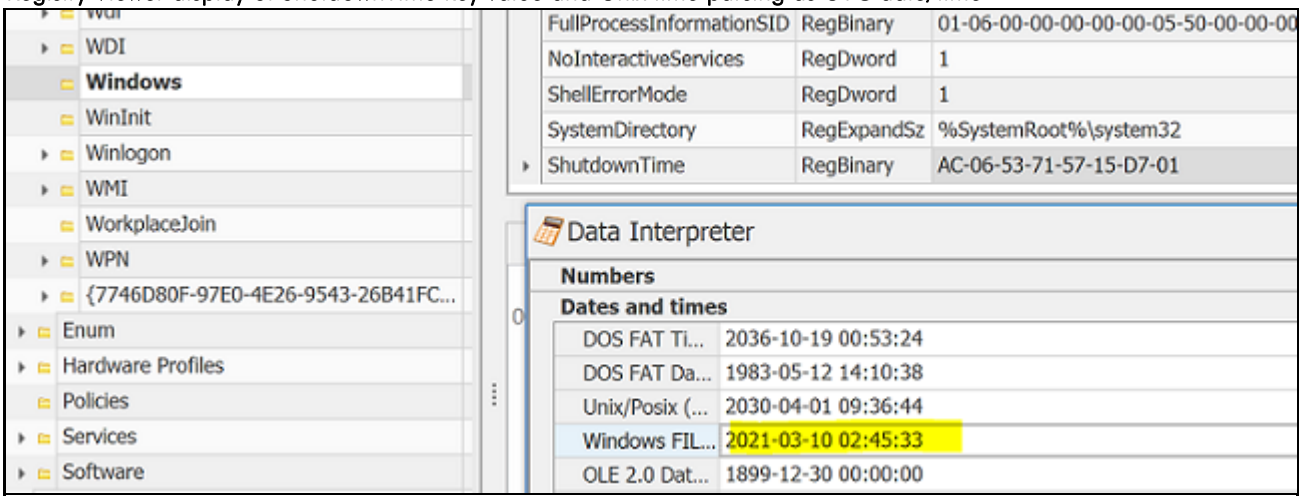


TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 8

Question 8: Provide the username of the account created by the user.

Manufacturer's Expected Response:

susie

WebCode - Test	Response
23UJ67-5561	susie
29JUMG-5562	susie
2YBWJR-5562	susie
3B7V4P-5561	susie
3RC2CZ-5561	The username of the account created by the a user is "susie".
44372B-5561	susie
4A86BF-5561	Susie
4UEFFJ-5561	susie
66CHBZ-5561	User name created by user - susie
67H6N6-5562	susie
6G29KN-5562	susie
6LBUJ2-5561	susie
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	susie
6ZD7FZ-5561	susie
7A2A6E-5561	susie
7FMAEZ-5562	susie
7W9P7F-5562	susie
89LGKW-5561	susie
89NM2E-5561	susie
8UH9ME-5562	susie
8YVWFY-5561	susie
93AL3L-5562	susie

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 8

WebCode - Test	Response
9ARR2D-5561	susie
9GULT8-5562	susie
9V6AXV-5561	susie
A8KGFG-5561	Susie
AK9F96-5561	susie
AQYVXC-5562	susie
AV4RGC-5562	susie
BGJGLT-5561	susie
BKPYQG-5561	susie
BMT8ZD-5561	susie
BR6KUT-5562	susie
BWZC2P-5561	susie
CBTGPD-5562	susie
CMHKPW-5561	susie
CPRZ8G-5561	susie
CQ9KB9-5562	susie
CQJQ7N-5561	Username of account created by the user – “susie”
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	susie
E43HU2-5561	susie
E7BXK2-5561	susie
EELYM9-5561	susie
F2UYKR-5561	Username of the account is robertapeal67@gmail.com
FFG39B-5562	Samantha

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 8	
WebCode - Test	**Response**
FJWWP9-5562	susie
FP3BPR-5562	susie
FTFDBN-5561	susie
G9A37K-5561	susie
GGKE74-5561	susie
GU9W29-5561	Susie
GZY7B8-5561	Susie
H949ZJ-5561	susie
HEBY4P-5561	susie
HYFCYH-5561	susie
J3U2M6-5561	susie
J3XR9B-5561	Susie
JF4GTB-5562	susie
JJJA4W-5562	susie
JMJLZW-5561	susie
JU4NYL-5561	susie
K6Z7V8-5562	susie
KE3C4M-5561	susie
KH3MYM-5562	susie
KT78B9-5562	susie
KW3EPY-5561	susie
L9D7RX-5562	susie
LCV3Z2-5561	susie
LEERBL-5562	Susie

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 8	
WebCode - Test	**Response**
LPY8P3-5561	susie
LRRLAT-5562	susie
LXXGTT-5561	susie
M98EB2-5562	susie
MWHHA4-5562	susie
MYJKY6-5562	susie
N66VNU-5561	susie
NFQ2KX-5562	susie
NPAH8D-5561	susie
NRJXPX-5561	susie
NTAT4D-5561	susie
NUKNP6-5562	susie
PBBNHP-5561	susie
PBQMFZ-5561	Susie
PTA4GV-5562	susie
QP2MPV-5561	susie
R36ZB9-5561	susie
RAQR4V-5562	susie
RFUVTT-5561	susie
RGQL4V-5561	susie
RK6QRB-5561	susie
RXCADP-5561	susie
T8F7TZ-5562	susie
TCA8P9-5561	susie

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 8	
WebCode - Test	**Response**
TDLF3U-5561	Susie
TFMD29-5561	susie
TMAWNW-5561	Susie
U298Q9-5561	susie
U964DC-5562	susie
UWTR4N-5561	susie
V23CK9-5561	susie
V96U7R-5561	susie
VFHDED-5561	susie
WHMDWP-5561	susie
WLLU9J-5561	susie
WRR3GT-5561	susie
WW4B2Q-5561	susie
X436QC-5562	susie
X4L22Q-5562	susie
XCDUFN-5561	susie
XHHHQN-5561	susie
XUR36B-5561	susie
Y2ANWU-5561	susie
YQTYXP-5561	susie
YXADZU-5561	susie
YYKJVA-5561	susie
ZGHWCN-5561	susie
ZM6UW6-5561	susie

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 8	
WebCode - Test	**Response**
ZTBFTE-5561	susie

Question 8: Provide the username of the account created by the user.

Consensus Result:

susie

Expected Response Explanation:

There is only one user-created account on this device. Information about user (and system) accounts is found in the Windows System Accounts Manager (SAM) 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

	User Name	Comment	Security ID	Group ID	Profile Path
1	Administrator	Built-in account for administering the comp...	S-1-5-21-1943064195-990424342-2473957490-500	513	
2	DefaultAccount	A user account managed by the system.	S-1-5-21-1943064195-990424342-2473957490-503	513	
3	Guest	Built-in account for guest access to the com...		513	
4	susie		S-1-5-21-1943064195-990424342-2473957490-1001	513	C:\Users\susie
5	WDAGUtilityAccount	A user account managed and used by the s...	S-1-0-0-0-0-0-0	513	
6	systemprofile		S-1-5-18		%systemroot%\syste...
7	LocalService		S-1-5-19		%systemroot%\Servic...
8	NetworkService		S-1-5-20		%systemroot%\Servic...

RegRipper View of SAM Hive Entry for "Susie"

```
Username        : susie [1001]
Full Name       :
User Comment    :
Account Type    :
Account Created : 2021-02-19 02:03:12Z
Name            :
Last Login Date : 2021-03-10 02:38:42Z
Pwd Reset Date  : 2021-02-19 02:03:18Z
Pwd Fail Date   : 2021-03-08 02:44:16Z
Login Count     : 12
Embedded RID    : 1001
  --> Password does not expire
  --> Password not required
  --> Normal user account
```

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 9

Question 9: What is the Security ID (SID) of the user account created by the user?

Manufacturer's Expected Response:

S-1-5-21-1943064195-990424342-2473957490-1001

WebCode - Test	Response
23UJ67-5561	S-1-5-21-1943064195-990424342-2473957490-1001
29JUMG-5562	S-1-5-21-1943064195-990424342-2473957490-1001
2YBWJR-5562	S-1-5-21-1943064195-990424342-2473957490-1001
3B7V4P-5561	S-1-5-21-1943064195-990424342-2473957490-1001
3RC2CZ-5561	The SID for the "susie" user account is S-1-5-21-1943064195-990424342-2473957490-1001 (1001).
44372B-5561	S-1-5-21-1943064195-990424342-2473957490-1001
4A86BF-5561	S-1-5-21-1943064195-990424342-2473957490-1001
4UEFFJ-5561	S-1-5-21-1943064195-990424342-2473957490-1001
66CHBZ-5561	S-1-5-21-1943064195-990424342-2473957490-1001
67H6N6-5562	S-1-5-21-1943064195-990424342-2473957490-1001
6G29KN-5562	S-1-5-21-1943064195-990424342-2473957490-1001
6LBUJ2-5561	S-1-5-21-1943064195-990424342-2473957490-1001
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	S-1-5-21-1943064195-990424342-2473957490-1001
6ZD7FZ-5561	S-1-5-21-1943064195-990424342-2473957490-1001
7A2A6E-5561	S-1-5-21-1943064195-990424342-2473957490-1001
7FMAEZ-5562	S-1-5-21-1943064195-990424342-2473957490-1001
7W9P7F-5562	S-1-5-21-1943064195-990424342-2473957490-1001
89LGKW-5561	1001
89NM2E-5561	S-1-5-21-1943064195-990424342-2473957490-1001
8UH9ME-5562	S-1-5-21-1943064195-990424342-2473957490-1001
8YVWFY-5561	S-1-5-21-1943064195-990424342-2473957490-1001
93AL3L-5562	S-1-5-21-1943064195-990424342-2473957490-1001

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 9	
WebCode - Test	**Response**
9ARR2D-5561	S-1-5-21-1943064195-990424342-2473957490-1001
9GULT8-5562	S-1-5-21-1943064195-990424342-2473957490-1001
9V6AXV-5561	S-1-5-21-1943064195-990424342-2473957490-1001
A8KGFG-5561	S-1-15-21 S-1-5-21-1943064195-990424342-2473957490-1001
AK9F96-5561	S-1-5-21-1943064195-990424342-2473957490-1001
AQYVXC-5562	S-1-5-21-1943064195-990424342-2473957490-1001
AV4RGC-5562	S-1-5-21-1943064195-990424342-2473957490-1001
BGJGLT-5561	S-1-5-21-1943064195-990424342-2473957490-1001
BKPYQG-5561	S-1-5-21-1943064195-990424342-2473957490-1001
BMT8ZD-5561	S-1-5-21-1943064195-990424342-2473957490-1001
BR6KUT-5562	S-1-5-21-1943064195-990424342-2473957490-1001
BWZC2P-5561	S-1-5-21-1943064195-990424342-2473957490-1001
CBTGPD-5562	S-1-5-21-1943064195-990424342-2473957490-1001
CMHKPW-5561	S-1-5-21-1943064195-990424342-2473957490-1001
CPRZ8G-5561	S-1-5-21-1943064195-990424342-2473957490-1001
CQ9KB9-5562	S-1-5-21-1943064195-990424342-2473957490-1001
CQJQ7N-5561	Security ID (SID) of user account – S-1-5-21-1943064195-990424342-2473957490-1001
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	S-1-5-21-1943064195-990424342-2473957490-1001
E43HU2-5561	S-1-5-21-1943064195-990424342-2473957490-1001
E7BXK2-5561	S-1-5-21-1943064195-990424342-2473957490-1001
EELYM9-5561	S-1-5-21-1943064195-990424342-2473957490-1001
F2UYKR-5561	S-1-5-21-1943064195-990424342-2473957490-1001
FFG39B-5562	S-1-5-21-1943064195-990424342-2473957490-1001

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 9	
WebCode - Test	**Response**
FJWWP9-5562	S-1-5-21-1943064195-990424342-2473957490-1001
FP3BPR-5562	S-1-5-21-1943064195-990424342-2473957490-1001
FTFDBN-5561	S-1-5-21-1943064195-990424342-2473957490-1001
G9A37K-5561	S-1-5-21-1943064195-990424342-2473957490-1001
GGKE74-5561	S-1-5-21-1943064195-990424342-2473957490-1001
GU9W29-5561	000003E9
GZY7B8-5561	S-1-5-21-1943064195-990424342-2473957490-1001
H949ZJ-5561	1001
HEBY4P-5561	S-1-5-21-1943064195-990424342-2473957490-1001
HYFCYH-5561	S-1-5-21-1943064195-990424342-2473957490-1001
J3U2M6-5561	S-1-5-21-1943064195-990424342-2473957490-1001
J3XR9B-5561	S-1-5-21-1943064195-990424342-2473957490-1001
JF4GTB-5562	S-1-5-21-1943064195-990424342-2473957490-1001
JJJA4W-5562	S-1-5-21-1943064195-990424342-2473957490-1001
JMJLZW-5561	S-1-5-21-1943064195-990424342-2473957490-1001 (0x03E9)
JU4NYL-5561	S-1-5-21-1943064195-990424342-2473957490-1001
K6Z7V8-5562	S-1-5-21-1943064195-990424342-2473957490-1001
KE3C4M-5561	S-1-5-21-1943064195-990424342-2473957490-1001
KH3MYM-5562	S-1-5-21-1943064195-990424342-2473957490-1001
KT78B9-5562	S-1-5-21-1943064195-990424342-2473957490-1001
KW3EPY-5561	S-1-5-21-1943064195-990424342-2473957490-1001
L9D7RX-5562	S-1-5-21-1943064195-990424342-2473957490-1001
LCV3Z2-5561	S-1-5-21-1943064195-990424342-2473957490-1001
LEERBL-5562	S-1-5-21-1943064195-990424342-2473957490-1001

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 9	
WebCode - Test	**Response**
LPY8P3-5561	S-1-5-21-1943064195-990424342-2473957490-1001
LRRLAT-5562	S-1-5-21-1943064195-990424342-2473957490-1001
LXXGTT-5561	S-1-5-21-1943064195-990424342-2473957490-1001
M98EB2-5562	S-1-5-21-1943064195-990424342-2473957490-1001
MWHHA4-5562	S-1-5-21-1943064195-990424342-2473957490-1001
MYJKY6-5562	S-1-5-21-1943064195-990424342-2473957490-1001
N66VNU-5561	S-1-5-21-1943064195-990424342-2473957490-1001
NFQ2KX-5562	S-1-5-21-1943064195-990424342-2473957490-1001
NPAH8D-5561	S-1-5-21-1943064195-990424342-2473957490-1001
NRJXPX-5561	S-1-5-21-1943064195-990424342-2473957490-1001
NTAT4D-5561	S-1-5-21-1943064195-990424342-2473957490-1001
NUKNP6-5562	S-1-5-21-1943064195-990424342-2473957490-1001
PBBNHP-5561	S-1-5-21-1943064195-990424342-2473957490-1001
PBQMFZ-5561	S-1-5-21-1943064195-990424342-2473957490-1001
PTA4GV-5562	S-1-5-21-1943064195-990424342-2473957490-1001
QP2MPV-5561	S-1-5-21-1943064195-990424342-2473957490-1001
R36ZB9-5561	S-1-5-21-1943064195-990424342-2473957490-1001
RAQR4V-5562	S-1-5-21-1943064195-990424342-2473957490-1001
RFUVTT-5561	S-1-5-21-1943064195-990424342-2473957490-1001
RGQL4V-5561	S-1-5-21-1943064195-990424342-2473957490-1001
RK6QRB-5561	S-1-5-21-1943064195-990424342-2473957490-1001
RXCADP-5561	S-1-5-21-1943064195-990424342-2473957490-1001
T8F7TZ-5562	S-1-5-21-1943064195-990424342-2473957490-1001
TCA8P9-5561	S-1-5-21-1943064195-990424342-2473957490-1001

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 9

WebCode - Test	Response
TDLF3U-5561	S-1-5-21-1943064195-990424342-2473957490-1001
TFMD29-5561	S-1-5-21-1943064195-990424342-2473957490-1001
TMAWNW-5561	S-1-5-21-1943064195-990424342-2473957490-1001
U298Q9-5561	1001
U964DC-5562	S-1-5-21-1943064195-990424342-2473957490-1001
UWTR4N-5561	S-1-5-21-1943064195-990424342-2473957490-1001
V23CK9-5561	s-1-5-21-1943064195-990424342-2473957490-1001
V96U7R-5561	S-1-5-21-1943064195-990424342-2473957490-1001
VFHDED-5561	S-1-5-21-1943064195-990424342-2473957490-1001
WHMDWP-5561	S-1-5-21-1943064195-990424342-2473957490-1001
WLLU9J-5561	[Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-1943064195-990424342-2473957490-1001 Registry_Key_Write_Time="2021/03/10 02:45:31 UTC" "ProfileImagePath"="C:\Users\susie
WRR3GT-5561	S-1-5-21-1943064195-990424342-2473957490-1001
WW4B2Q-5561	S-1-5-21-1943064195-990424342-2473957490-1001
X436QC-5562	S-1-5-21-1943064195-990424342-2473957490-1001
X4L22Q-5562	S-1-5-21-1943064195-990424342-2473957490-1001
XCDUFN-5561	S-1-5-21-1943064195-990424342-2473957490-1001
XHHHQN-5561	S-1-5-21-1943064195-990424342-2473957490-1001
XUR36B-5561	S-1-5-21-1943064195-990424342-2473957490-1001
Y2ANWU-5561	S-1-5-21-1943064195-990424342-2473957490-1001
YQTYXP-5561	S-1-5-21-1943064195-990424342-2473957490 with a user RID of 1001
YXADZU-5561	S-1-5-21-1943064195-990424342-2473957490-1001
YYKJVA-5561	S-1-5-21-1943064195-990424342-2473957490-1001
ZGHWCN-5561	S-1-5-21-1943064195-990424342-2473957490-1001
ZM6UW6-5561	S-1-5-21-1943064195-990424342-2473957490-1001

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 9

WebCode - Test	Response
ZTBFTE-5561	S-1-5-21-1943064195-990424342-2473957490-1001

Question 9: What is the Security ID (SID) of the user account created by the user?

Consensus Result:
S-1-5-21-1943064195-990424342-2473957490-1001

Expected Response Explanation:

Information about user (and system) accounts is found in the Windows System Accounts Manager (SAM) 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

	User Name	Comment	Security ID	Group ID	Profile Path
1	Administrator	Built-in account for administering the comp...	S-1-5-21-1943064195-990424342-2473957490-500	513	
2	DefaultAccount	A user account managed by the system.	S-1-5-21-1943064195-990424342-2473957490-503	513	
3	Guest	Built-in account for guest access to the com...		513	
4	susie		S-1-5-21-1943064195-990424342-2473957490-1001	513	C:\Users\susie
5	WDAGUtilityAccount	A user account managed and used by the s...	S-1-0-0-0-0-0-0	513	
6	systemprofile		S-1-5-18		%systemroot%\syste...
7	LocalService		S-1-5-19		%systemroot%\Servic...
8	NetworkService		S-1-5-20		%systemroot%\Servic...

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 10

Question 10: What is the configured time zone?

Manufacturer's Expected Response:

W. Central Africa Standard Time, or UTC-1

WebCode - Test	Response
23UJ67-5561	W. Central Africa Standard Time
29JUMG-5562	W. Central Africa Standard Time (UTC+01:00) West Central Africa
2YBWJR-5562	W. Central Africa Standard Time
3B7V4P-5561	W. Central Africa Standard Time
3RC2CZ-5561	The configured time zone for the device is W. Central Africa Standard Time.
44372B-5561	West Central Africa (UTC+01:00)
4A86BF-5561	West Central Africa (UTC+01:00)
4UEFFJ-5561	(UTC+01:00) West Central Africa
66CHBZ-5561	West Central Africa Standard Time
67H6N6-5562	(UTC+01:00) West Central Africa
6G29KN-5562	West Central Africa Standard Time
6LBUJ2-5561	W. Central Africa Standard Time, (UTC+01:00) West Central Africa
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	W. Central Africa Standard Time
6ZD7FZ-5561	W. Central Africa Standard Time
7A2A6E-5561	W. Central Africa Standard Time
7FMAEZ-5562	W. Central Africa Standard Time (UTC+01:00)
7W9P7F-5562	W. Central Africa Daylight Time
89LGKW-5561	W. Central Africa Standard Time
89NM2E-5561	West Central Africa(UTC+01:00)
8UH9ME-5562	W. Central Africa Standard Time
8YVWFY-5561	W. Central Africa Standard Time
93AL3L-5562	W. Central Africa Standard Time

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 10	
WebCode - Test	**Response**
9ARR2D-5561	W. Central Africa Standard Time
9GULT8-5562	W. Central Africa Standard Time
9V6AXV-5561	W. Central Africa Standard Time
A8KGFG-5561	W. Central Africa Standard Time
AK9F96-5561	(UTC+01:00) West Central Africa
AQYVXC-5562	W. Central Africa Standard Time
AV4RGC-5562	West Central Africa Standard time
BGJGLT-5561	W. Central Africa (UTC+1)
BKPYQG-5561	W. Central Africa Standard Time
BMT8ZD-5561	W. Central Africa Standard Time
BR6KUT-5562	W. Central Africa Standard Time
BWZC2P-5561	W. Central Africa Standard Time
CBTGPD-5562	W. Central Africa Standard Time
CMHKPW-5561	(UTC+01:00) West Central Africa
CPRZ8G-5561	W. Central Africa Standard Time
CQ9KB9-5562	W. Central Africa Standard Time
CQJQ7N-5561	Configured time zone – West Central Africa Standard Time
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	West Central Africa Standard Time
E43HU2-5561	W. Central Africa Standard Time
E7BXK2-5561	W. Central Africa Standard Time
EELYM9-5561	(UTC+01:00) West Central Africa
F2UYKR-5561	The configured time zone is of W Central Africa Standard Time.
FFG39B-5562	W. Central Africa Standard Time

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 10	
WebCode - Test	**Response**
FJWWP9-5562	W. Central Africa Standard Time
FP3BPR-5562	W.Central Africa Standard Time (UTC+01:00)
FTFDBN-5561	W. Central Africa Standard Time
G9A37K-5561	W. Central Africa Standard Time
GGKE74-5561	W. Central Africa Standard Time
GU9W29-5561	W. Central Africa Standard Time
GZY7B8-5561	W.Central Africa Standard Time Current Timezone Offset (Minutes) 60
H949ZJ-5561	W. Central Africa Standard Time
HEBY4P-5561	W. Central Africa Standard Time
HYFCYH-5561	W. Central Africa Standard Time (UTC+1)
J3U2M6-5561	(UTC+01:00) West Central Africa
J3XR9B-5561	W. Central Africa Standard Time
JF4GTB-5562	W. Central Africa Standard Time
JJJA4W-5562	W. Central Africa Standard Time
JMJLZW-5561	W. Central Africa Standard Time
JU4NYL-5561	W. Central Africa Standard Time
K6Z7V8-5562	W. Central Africa Daylight Time
KE3C4M-5561	(UTC+01:00) West Central Africa
KH3MYM-5562	W.Central Africa
KT78B9-5562	West Central Africa Standard Time
KW3EPY-5561	W. Central Africa Standard Time
L9D7RX-5562	W. Central Africa Standard Time
LCV3Z2-5561	W. Central Africa Standard Time
LEERBL-5562	West Central Africa Time

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 10	
WebCode - Test	**Response**
LPY8P3-5561	W. Central Africa Daylight Time
LRRLAT-5562	W. Central Africa Standard Time
LXXGTT-5561	W. Central Africa Standard Time
M98EB2-5562	W. Central Africa Standard Time
MWHHA4-5562	W. Central Africa Standard Time
MYJKY6-5562	W. Central Africa Standard Time
N66VNU-5561	"W. Central Africa Standard Time" (UTC+01:00)
NFQ2KX-5562	(UTC+01:00) West Central Africa
NPAH8D-5561	W. Central Africa Standard Time
NRJXPX-5561	West Central Africa Standard Time
NTAT4D-5561	W. Central Africa Daylight Time
NUKNP6-5562	UTC +01:00 West Central Aafrica
PBBNHP-5561	W. Central Africa Standard Time (UTC+1)
PBQMFZ-5561	System time set to W Central Africa time +1:00
PTA4GV-5562	W. Central Africa Standard Time
QP2MPV-5561	(UTC+01:00) West Central Africa
R36ZB9-5561	W. Central Africa Standard Time
RAQR4V-5562	(UTC+01:00) West Central Africa
RFUVTT-5561	W. Central Africa Daylight Time
RGQL4V-5561	UTC+01:00 West Central Africa Standard Time
RK6QRB-5561	W. Central Africa Standard Time (UTC+1:00)
RXCADP-5561	(UTC+01:00) West Central Africa
T8F7TZ-5562	W. Central Africa Daylight Time
TCA8P9-5561	W. Central Africa Standard Time

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 10	
WebCode - Test	**Response**
TDLF3U-5561	W. Central Africa Daylight Time
TFMD29-5561	W.Central Africa Standard Time
TMAWNW-5561	(UTC+01:00) West Central Africa
U298Q9-5561	W. Central Africa Standard Time
U964DC-5562	(UTC+01:00) West Central Africa
UWTR4N-5561	W. Central Africa Standard Time
V23CK9-5561	West Central Africa Standard Time
V96U7R-5561	W. Central Africa Standard Time
VFHDED-5561	W. Central Africa Standard Time
WHMDWP-5561	W. Central Africa Standard Time
WLLU9J-5561	W. Central Africa Standard
WRR3GT-5561	W. Central Africa Standard Time (UTC+01:00)
WW4B2Q-5561	(UTC+01:00) West Central Africa
X436QC-5562	W. Central Africa Standard Time
X4L22Q-5562	W. Central Africa Standard Time
XCDUFN-5561	W. Central Africa Standard Time
XHHHQN-5561	W. Central Africa Standard Time (UTC +01:00) West Central Africa
XUR36B-5561	W.Central Africa Standard Time
Y2ANWU-5561	West Central African Time +60 minutes
YQTYXP-5561	W. Central Africa (UTC+01:00)
YXADZU-5561	W. Central Africa Standard Time
YYKJVA-5561	(UTC+01:00) West Central Africa
ZGHWCN-5561	West Central Africa Standard Time
ZM6UW6-5561	W. Central Africa Standard Time

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 10	
WebCode - Test	**Response**
ZTBFTE-5561	W. Central Africa Standard Time

Question 10: What is the configured time zone?

Consensus Result:

W. Central Africa Standard Time and all formatting styles which represent the same information.

Expected Response Explanation:

The 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.

Expected Response Illustration:

RegistryExplorer View of TimeZoneInformation key

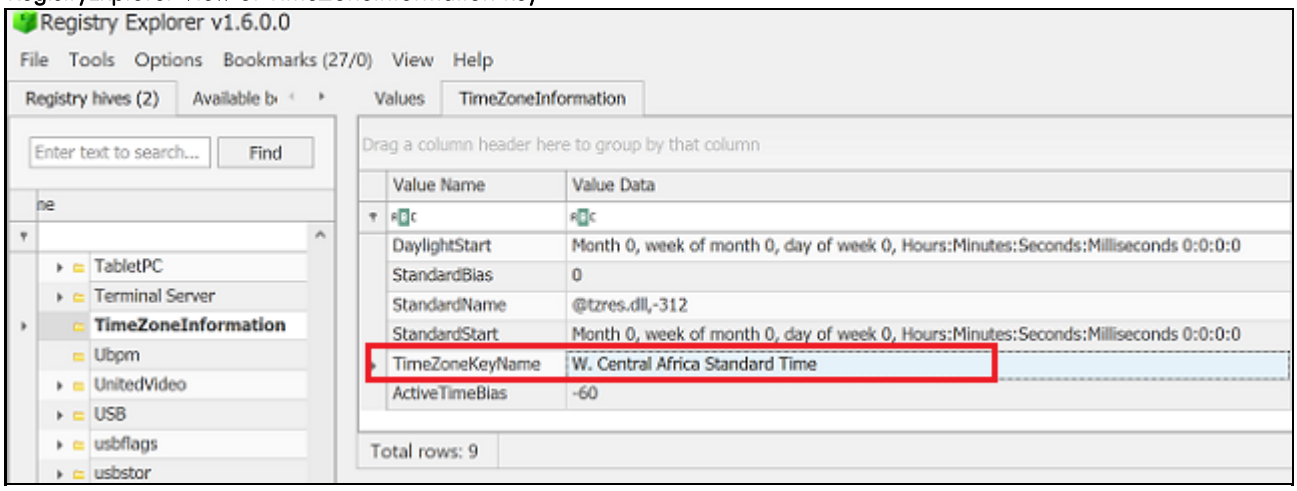


TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 11

Question 11: Provide the name for the paired Bluetooth device with MAC address 98:d3:71:fd:9a:2a.

Manufacturer's Expected Response:

BEARODACTYL

WebCode - Test	Response
23UJ67-5561	BEARODACTYL
29JUMG-5562	ASUS USB-BT400, con número de serie 5CF370A29417, ID: VID_0B05&PID_17CB
2YBWJR-5562	The [Laboratory] does not include this information on the report and is outside the scope of our normal reporting procedures
3B7V4P-5561	BEARODACTYL
3RC2CZ-5561	The name of the paired Bluetooth device with the MAC address of 98:d3:71:fd:9a:2a is Bluetooth Device (Personal Area Network).
44372B-5561	BEARODACTYL
4A86BF-5561	BTHUSB
4UEFFJ-5561	BTHUSB
66CHBZ-5561	BEARODACTYL
67H6N6-5562	BTHUSB
6G29KN-5562	This question is outside the scope of a normal examination at the [Laboratory] and would not be reported under normal circumstances.
6LBUJ2-5561	BEARODACTYL
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	BEARODACTYL
6ZD7FZ-5561	BEARODATYL
7A2A6E-5561	BEARODACTYL
7FMAEZ-5562	BTHUSB
7W9P7F-5562	BEARODACTYL
89LGKW-5561	BEARODACTYL
89NM2E-5561	BEARODACTYL
8UH9ME-5562	Bearodactyl
8YVWFY-5561	BEARODACTYL
93AL3L-5562	[Participant did not return results for this question.]

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 11	
WebCode - Test	**Response**
9ARR2D-5561	BEARODACTYL
9GULT8-5562	Bearodactyl
9V6AXV-5561	BTHUSB
A8KGFG-5561	BEARODACTYL
AK9F96-5561	BEARODACTYL
AQYVXC-5562	BEARODACTYL
AV4RGC-5562	BEARODACTYL
BGJGLT-5561	Bearodactyl
BKPYQG-5561	BTHUSB
BMT8ZD-5561	BEARODACTYL
BR6KUT-5562	BEARODACTYL
BWZC2P-5561	BEARODACTYL
CBTGPD-5562	BEARODACTYL
CMHKPW-5561	BEARODACTYL
CPRZ8G-5561	BEARODACTYL
CQ9KB9-5562	BTHUSB
CQJQ7N-5561	Provider name for Bluetooth device with MAC address 98:d3:71:fd:9a:2a - BTHUSB
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	BEARODACTYL
E43HU2-5561	BEARODACTYL
E7BXK2-5561	BEARODACTYL
EELYM9-5561	BEARODACTYL
F2UYKR-5561	The name of the Bluetooth device is Bearodactyl.
FFG39B-5562	Standard Serial over Bluetooth

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 11	
WebCode - Test	**Response**
FJWWP9-5562	BTHUSB
FP3BPR-5562	BEARODACTYL
FTFDBN-5561	BEARODACYTYL
G9A37K-5561	BEARODACTYL
GGKE74-5561	BEARODACTYL
GU9W29-5561	Bearodactyl
GZY7B8-5561	BEARODACTYL
H949ZJ-5561	BEARODACTYL
HEBY4P-5561	BEARODACTYL
HYFCYH-5561	BEARODACTYL
J3U2M6-5561	BEARODACTYL
J3XR9B-5561	BTHUSB
JF4GTB-5562	BEARODACTYL.
JJJA4W-5562	BEARODACTYL
JMJLZW-5561	BEARODACTYL
JU4NYL-5561	BTHUSB
K6Z7V8-5562	DUCKEXMACHINA
KE3C4M-5561	BEARODACTYL
KH3MYM-5562	RFCOMM
KT78B9-5562	BEARODACTYL
KW3EPY-5561	BEARODACTYL
L9D7RX-5562	BEARODACTYL
LCV3Z2-5561	BEARODACTYL
LEERBL-5562	BEARODACTYL

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 11	
WebCode - Test	**Response**
LPY8P3-5561	BEARODACTYL
LRRLAT-5562	BTHUSB
LXXGTT-5561	Bearodactyl
M98EB2-5562	BEARODACTYL
MWHHA4-5562	BTHUSB
MYJKY6-5562	BTHUSB
N66VNU-5561	BEARODACTYL
NFQ2KX-5562	BEARODACTYL
NPAH8D-5561	Bearodactyl
NRJXPX-5561	Bearodactyl
NTAT4D-5561	BEARODACTYL
NUKNP6-5562	Desktop Computer
PBBNHP-5561	BEARODACTYL
PBQMFZ-5561	The friendly name is BEARODACTYL. As viewed within the System Registry Hive at the path: ROOT\ControlSet001\Enum\BTHENUM\Dev_98D371FD9A2A\7&4f6eb3f&0&BluetoothDevice_98D371FD9A2A
PTA4GV-5562	BEARODACTYL
QP2MPV-5561	BEARODACTYL
R36ZB9-5561	BTH USB
RAQR4V-5562	Bearodactyl
RFUVTT-5561	BTHENUM
RGQL4V-5561	BEARODACTYL
RK6QRB-5561	BEARODACTYL
RXCADP-5561	BEARODACTYL
T8F7TZ-5562	BTHENUM
TCA8P9-5561	BEARODACTYL

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 11	
WebCode - Test	**Response**
TDLF3U-5561	BEARODACTYL
TFMD29-5561	BEARODACTYL
TMAWNW-5561	BTHUSB
U298Q9-5561	BEARODACTYL
U964DC-5562	Bearodactyl
UWTR4N-5561	BEARODACTYL
V23CK9-5561	BEARODACTYL
V96U7R-5561	BEARODACTYL
VFHDED-5561	BTHENUM
WHMDWP-5561	BEARODACTYL
WLLU9J-5561	BEARODACTYL
WRR3GT-5561	Bearodactyl
WW4B2Q-5561	BEARODACTYL
X436QC-5562	BEARODACTYL
X4L22Q-5562	BEARODACTYL
XCDUFN-5561	BEARODACTYL
XHHHQN-5561	BEARODACTYL
XUR36B-5561	BEARODACTYL
Y2ANWU-5561	BEARODACTYL
YQTYXP-5561	Friendly name - BEARODACTYL Provider name - BTHUSB
YXADZU-5561	BEARODACTYL
YYKJVA-5561	BTHUSB
ZGHWCN-5561	BEARODACTYL
ZM6UW6-5561	BEARODACTYL

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 11	
WebCode - Test	**Response**
ZTBFTE-5561	BEARODACTYL

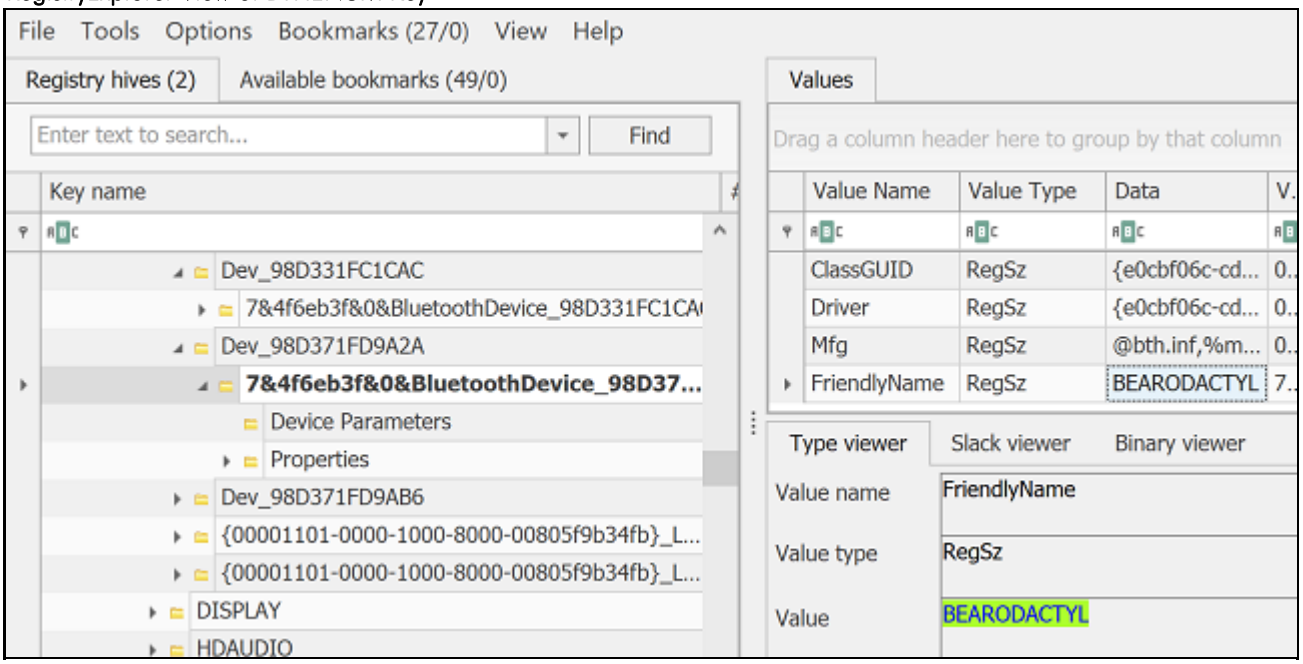
Question 11: Provide the name for the paired Bluetooth device with MAC address 98:d3:71:fd:9a:2a.

Consensus Result:
BEARODACTYL and any slight variation, if they were easily identified as a spelling error.

Expected Response Explanation:
Information about connected Bluetooth devices is found in the Windows SYSTEM registry hive at C:\Windows\System32\Config\SYSTEM: ControlSet001\Enum\BTHENUM and in SYSTEM: ControlSet001\services\BTHPORT\Parameters\Devices.

Expected Response Illustration:

RegistryExplorer View of BTHENUM Key



RegRipper view of BTHPORT key

```
bthport v.20200517
(System) Gets Bluetooth-connected devices from System hive

ControlSet001\services\BTHPORT\Parameters\Devices
LastWrite: 2021-03-06 18:27:40Z
Device Unique ID: 98d371fd9a2a
Name            : BEARODACTYL
LastSeen        : 2021-03-06 19:35:36Z
LastConnected   : 2021-03-06 19:27:48Z
```

Other Responses:
Seventeen participants reported "BTHUSB" which would apply to any/all USB bluetooth adapters, not the one specified in this question.

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12

Question 12: According to the last write times on the associated registry keys, what was the volume label (name) of the LAST mounted volume on a portable storage (USB) device?

Manufacturer's Expected Response:

stuff

WebCode - Test	Response ** Inconsistencies not highlighted; No consensus achieved **
23UJ67-5561	stuff
29JUMG-5562	Stuff
2YBWJR-5562	The [Laboratory] does not include this information on the report and is outside the scope of our normal reporting procedures
3B7V4P-5561	General UDisk USB Device
3RC2CZ-5561	The volume label last mounted USB portable storage device is "Generic UDisk USB Device". But there was a volume name of "stuff"
44372B-5561	stuff
4A86BF-5561	VBOX HARDDISK
4UEFFJ-5561	#USBSTOR#Disk&Ven_[VenderName]&Prod_[ProductName]&Rev_PMAP (the syntax) Disk&Ven_Apple&Prod_iPod&Rev_1.62 3/4/2021 1:23:12AM Disk&Ven_Lexar&Prod_CFUDMASD&Rev_1000 3/4/2021 1:20:17AM Last mounted volume: VID_148F&PID_7601 802.11n USB Wireless LAN Card
66CHBZ-5561	General UDisk USB Device
67H6N6-5562	stuff
6G29KN-5562	This question is outside the scope of a normal examination at the [Laboratory] and would not be reported under normal circumstances.
6LBUJ2-5561	stuff
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	stuff
6ZD7FZ-5561	Stuff
7A2A6E-5561	stuff
7FMAEZ-5562	Stuff
7W9P7F-5562	General UDisk USB Device
89LGKW-5561	JOHNS IPOD - Last Connected 03/04/2021 01:23:12 AM
89NM2E-5561	stuff
8UH9ME-5562	stuff

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12	
WebCode - Test	**Response** ** Inconsistencies not highlighted; No consensus achieved **
8YVWFY-5561	stuff
93AL3L-5562	[Participant did not return results for this question.]
9ARR2D-5561	General UDisk USB Device
9GULT8-5562	General UDisk USB Device
9V6AXV-5561	Apple iPod USB Device
A8KGFG-5561	USB Device: General UDisk USB Device – USB 6&1526ad36&0&_&0 Volume: Disk&Ven_General&Prod_UDisk&Rev_5.00 {c33383a2-7d23-11eb-80e9-08002732dc0f}
AK9F96-5561	General UDisk USB Device
AQYVXC-5562	stuff
AV4RGC-5562	stuff
BGJGLT-5561	stuff
BKPYQG-5561	General UDisk USB Device
BMT8ZD-5561	stuff
BR6KUT-5562	stuff
BWZC2P-5561	stuff
CBTGPD-5562	stuff
CMHKPW-5561	F:
CPRZ8G-5561	stuff
CQ9KB9-5562	Apple iPod USB Device
CQJQ7N-5561	Volume label (name) of the last mounted volume on a portable storage (USB) device – Lexar CFUDMASD USB Device
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	General UDisk USB Device
E43HU2-5561	stuff
E7BXK2-5561	stuff
EELYM9-5561	stuff

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12

WebCode - Test	Response ** Inconsistencies not highlighted; No consensus achieved **
F2UYKR-5561	not found
FFG39B-5562	stuff
FJWWP9-5562	07/03/2021 03:01:04
FP3BPR-5562	The volume label for the last mounted USB device was shown as 'stuff'
FTFDBN-5561	stuff
G9A37K-5561	stuff
GGKE74-5561	stuff
GU9W29-5561	Apple iPod USB Device
GZY7B8-5561	Stuff
H949ZJ-5561	stuff
HEBY4P-5561	VeraCryptVolumeV
HYFCYH-5561	General UDisk USB Device
J3U2M6-5561	stuff
J3XR9B-5561	General UDisk USB Device
JF4GTB-5562	General UDisk USB Device
JJJA4W-5562	stuff (the USB drive is General Udisk USB Device)
JMJLZW-5561	General UDisk USB Device
JU4NYL-5561	stuff
K6Z7V8-5562	General UDisk USB Device
KE3C4M-5561	stuff
KH3MYM-5562	UDisk
KT78B9-5562	stuff
KW3EPY-5561	General UDisk USB Device
L9D7RX-5562	Stuff

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12

WebCode - Test	Response ** Inconsistencies not highlighted; No consensus achieved **
LCV3Z2-5561	stuff
LEERBL-5562	stuff
LPY8P3-5561	General UDisk USB Device
LRRLAT-5562	stuff
LXXGTT-5561	General UDisk USB Device
M98EB2-5562	stuff
MWHHA4-5562	Lexar CFUDMASD USB Device
MYJKY6-5562	General UDisk USB Device
N66VNU-5561	Volume label was “stuff” (E:\) (Device name was “General UDisk USB Device”)
NFQ2KX-5562	General UDisk USB Device
NPAH8D-5561	General UDisk USB Device
NRJXPX-5561	General UDisk USB Drive
NTAT4D-5561	Based on review of the Windows Portable Devices and USBSTOR Registry keys, it is determined that the Volume Label of the LAST mounted volume on a portable storage device is stuff.
NUKNP6-5562	E:\ stuff
PBBNHP-5561	General UDisk USB Device
PBQMFZ-5561	Volume name: stuff Volume SN: 4A0C3885 According to USBSTOR last connected USB device was 03/07/2021 03:01:04 AM
PTA4GV-5562	stuff
QP2MPV-5561	General UDisk USB Device
R36ZB9-5561	General UDisk USB Device
RAQR4V-5562	General UDISK USB Device
RFUVTT-5561	stuff
RGQL4V-5561	General UDisk USB Device
RK6QRB-5561	stuff
RXCADP-5561	if you consider UDISK a USB device - STUFF otherwise- JOHNS IPOD

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12	
WebCode - Test	**Response** ** Inconsistencies not highlighted; No consensus achieved **
T8F7TZ-5562	stuff
TCA8P9-5561	General UDisk USB Device
TDLF3U-5561	General UDisk USB Device
TFMD29-5561	General UDisk USB Device
TMAWNW-5561	DataTraveler 1GB/2GB Pen Drive
U298Q9-5561	stuff
U964DC-5562	Volume label (name) = stuff
UWTR4N-5561	stuff
V23CK9-5561	stuff
V96U7R-5561	General UDisk USB Device
VFHDED-5561	General UDisk USB Device {c333839a-7d23-11eb-80e9-08002732dc0f}
WHMDWP-5561	General UDisk USB Device
WLLU9J-5561	stuff
WRR3GT-5561	General UDisk USB Device
WW4B2Q-5561	stuff
X436QC-5562	stuff
X4L22Q-5562	General UDisk USB Device
XCDUFN-5561	VeraCryptVolumeV
XHHHQN-5561	stuff
XUR36B-5561	stuff
Y2ANWU-5561	E:\Stuff Disk&Ven_General&Prod_UDisk&Rev_5.00, Last Written 2021-03-07 03:01:04 +00:00
YQTYXP-5561	General UDisk USB Device
YXADZU-5561	DATA
YYKJVA-5561	stuff

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12

WebCode - Test	Response ** Inconsistencies not highlighted; No consensus achieved **
ZGHWCN-5561	General UDisk USB Device
ZM6UW6-5561	stuff
ZTBFTE-5561	"stuff" is what would have displayed in Windows Explorer when the USB device was connected. However, it is hard to know for certain what is being looked for here. Within the SYSTEM hive, WPDBUSENUM has the following information: FriendlyName = "stuff"; FriendlyName = ":\"; DeviceDesc = "UDisk" USBSTOR has the following information: Key Label = "Disk&Ven_General&Prod_UDisk&Rv_5.00"; FriendlyName = "General UDisk USB Device"

Question 12: According to the last write times on the associated registry keys, what was the volume label (name) of the LAST mounted volume on a portable storage (USB) device?

Consensus Result:

The objective of this question was for the examiner to provide the volume label (name) of the filesystem on the device. While the majority (55%) reported the expected response of "stuff", a consensus was not achieved for this question. Another 32% of participants reported "Udisk USB Device" which is the friendly name for the hardware USB device.

Expected Response Explanation:

The volume label (name) can be found in the Windows SOFTWARE registry hive in two places: the VolumeInfoCache from Windows Search key and the Windows Portable Devices key contents. Either can be parsed with a registry tool like RegRipper or Registry Explorer.

Expected Response Illustration:

RegRipper view of VolumeInfoCache from Windows Search key

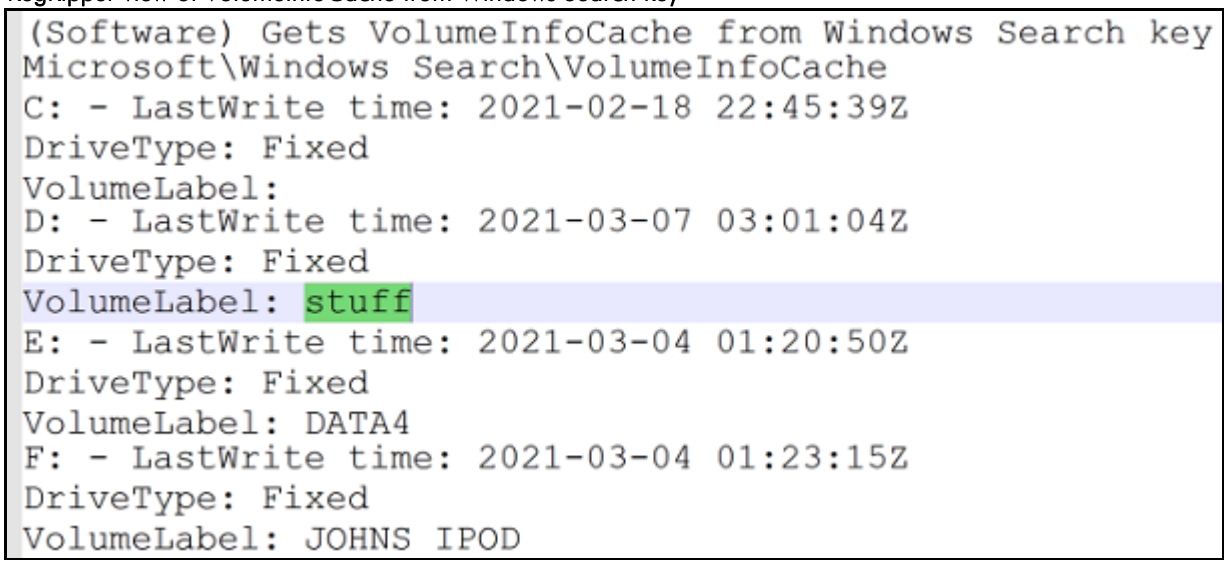


TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12

Registry Explorer view of Windows Portable Devices Keys

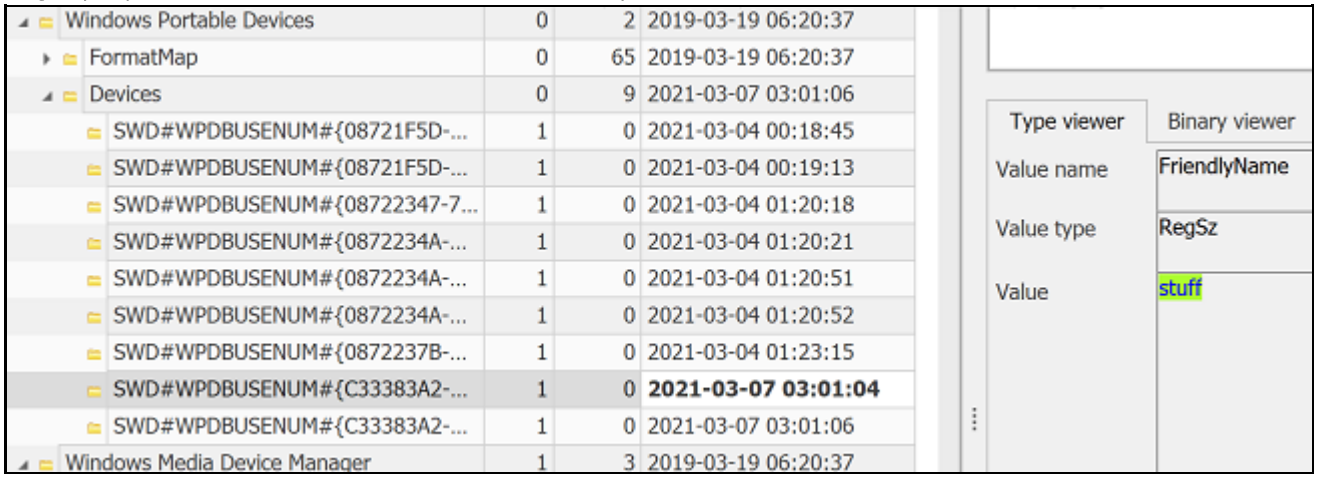


TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13

Question 13: In unallocated space on this device is a JPEG photograph of an opossum carrying joeys (baby opossums). What is the SHA1 hash of this file?

Manufacturer's Expected Response:

13d5240c84a2f9dcafbce49ed0a63527adcd16fa

WebCode - Test	Response
23UJ67-5561	572d3fc67d555a9110b37bb1941180f88b69d39d
29JUMG-5562	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
2YBWJR-5562	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
3B7V4P-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
3RC2CZ-5561	The SHA1 hash value for the JPEG photo of the opossum is 13d5240c84a2f9dcafbce49ed0a63527adcd16fa.
44372B-5561	13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA
4A86BF-5561	13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA
4UEFFJ-5561	SHA1 Hash: 13d5240c84a2f9dcafbce49ed0a63527adcd16fa
66CHBZ-5561	SHA1 - 13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA
67H6N6-5562	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
6G29KN-5562	13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA
6LBUJ2-5561	13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
6ZD7FZ-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
7A2A6E-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
7FMAEZ-5562	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
7W9P7F-5562	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
89LGKW-5561	SHA1 Hash 13d5240c84a2f9dcafbce49ed0a63527adcd16fa
89NM2E-5561	13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA
8UH9ME-5562	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
8YVWFY-5561	13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13

WebCode - Test	Response
93AL3L-5562	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
9ARR2D-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
9GULT8-5562	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
9V6AXV-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
A8KGFG-5561	13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA
AK9F96-5561	13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA
AQYVXC-5562	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
AV4RGC-5562	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
BGJGLT-5561	13d5240c84a2f9dcafbce49ed0a63527abcd16fa
BKPYQG-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
BMT8ZD-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
BR6KUT-5562	13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA
BWZC2P-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
CBTGPD-5562	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
CMHKPW-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
CPRZ8G-5561	13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA
CQ9KB9-5562	13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA
CQJQ7N-5561	JPEG photograph of an opossum carrying joeys (baby opossums) SHA1 hash - 13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
E43HU2-5561	13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA
E7BXK2-5561	13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA
EELYM9-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
F2UYKR-5561	No such file was found.

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13	
WebCode - Test	**Response**
FFG39B-5562	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
FJWWP9-5562	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
FP3BPR-5562	13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA
FTFDBN-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
G9A37K-5561	13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA
GGKE74-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
GU9W29-5561	13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA
GZY7B8-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
H949ZJ-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
HEBY4P-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
HYFCYH-5561	13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA
J3U2M6-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
J3XR9B-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
JF4GTB-5562	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
JJJA4W-5562	13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA
JMJLZW-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
JU4NYL-5561	13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA
K6Z7V8-5562	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
KE3C4M-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
KH3MYM-5562	13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA
KT78B9-5562	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
KW3EPY-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
L9D7RX-5562	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
LCV3Z2-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13	
WebCode - Test	**Response**
LEERBL-5562	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
LPY8P3-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
LRRLAT-5562	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
LXXGTT-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
M98EB2-5562	13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA
MWHHA4-5562	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
MYJKY6-5562	A48B4F70E6C1D049AC77CBD5FC144ADB672D666C
N66VNU-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
NFQ2KX-5562	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
NPAH8D-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
NRJXPX-5561	13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA
NTAT4D-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
NUKNP6-5562	A48B4F70E6C1D049AC77CBD5FC144ADB672D666C
PBBNHP-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
PBQMFZ-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa Physical Sector 35860593
PTA4GV-5562	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
QP2MPV-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
R36ZB9-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
RAQR4V-5562	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
RFUVTT-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
RGQL4V-5561	13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA
RK6QRB-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
RXCADP-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
T8F7TZ-5562	13d5240c84a2f9dcafbce49ed0a63527adcd16fa

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13	
WebCode - Test	**Response**
TCA8P9-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
TDLF3U-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
TFMD29-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
TMAWNW-5561	[Participant did not return results for this question.]
U298Q9-5561	13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA
U964DC-5562	13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA
UWTR4N-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
V23CK9-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
V96U7R-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
VFHDED-5561	Hash Tool v1.0 - Report created: 06/03/2021 12:07 PM sha1 (Carved [5083].jpeg) = 13d5240c84a2f9dcafbce49ed0a63527adcd16fa
WHMDWP-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
WLLU9J-5561	13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA
WRR3GT-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
WW4B2Q-5561	13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA
X436QC-5562	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
X4L22Q-5562	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
XCDUFN-5561	13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA
XHHHQN-5561	13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA
XUR36B-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
Y2ANWU-5561	13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA
YQTYXP-5561	13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA
YXADZU-5561	13D5240C84A2F9DCAFBCE49ED0A63527ADCD16FA
YYKJVA-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
ZGHWCN-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13

WebCode - Test	Response
ZM6UW6-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa
ZTBFTE-5561	13d5240c84a2f9dcafbce49ed0a63527adcd16fa

Question 13: In unallocated space on this device is a JPEG photograph of an opossum carrying joeys (baby opossums). What is the SHA1 hash of this file?

Consensus Result:
13d5240c84a2f9dcafbce49ed0a63527adcd16fa

Expected Response Explanation:
Deleted files can be recovered from unallocated space with a carving utility such as PhotoRec, with a forensic tool like EnCase, or manually by searching unallocated clusters for the jpeg header, FF D8 FF E0 and the footer FF D9.

Expected Response Illustration:

EnCase table view of carved image showing SHA1 Hash

Name	SHA1
00011555_Unallocated Clusters_FO-632124379_PS-35860593+475.jpg	13d5240c84a2f9dcafbce49ed0a63527adcd16fa

Content of carved file

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 14

Question 14: Provide the path and filename of the file containing the term "typhimiurium".

Manufacturer's Expected Response:

C:\Users\susie\Documents\003464.xls

WebCode - Test	Response
23UJ67-5561	[Root]/Users/susie/Documents/003464.xls
29JUMG-5562	21-5561.E01 - Partition 2 (Microsoft NTFS, 19,43 GB)\Users\susie\Documents\003464.xls
2YBWJR-5562	003464.xls
3B7V4P-5561	C:/Users/susie/Documents/003464.xls
3RC2CZ-5561	There is an Excel spreadsheet that contains the term "typhimiurium". The following is the path and file name of the file: 21-5561.E01\Partition 2\root\Users\susie\Documents\003463.xls
44372B-5561	C:\Users\susie\Documents\003464.xls
4A86BF-5561	\USERS\SUSIE\DOCUMENTS\003464.XLS
4UEFFJ-5561	Path: Computer\D\Users\susie\Documents\003464.xls File Name: 003464.xls
66CHBZ-5561	Computer\D\Users\susie\Documents\003464.xls
67H6N6-5562	\Users\susie\Documents\003464.xls
6G29KN-5562	Name=003464.xls Path=Partition 2 (Microsoft NTFS, 19.43 GB)\Users\susie\Documents\003464.xls
6LBUJ2-5561	path: Partition2:\Users\susie\Documents filename: 003464.xls
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	/Users/susie/Documents/003464.xls
6ZD7FZ-5561	Users/susie/Documents/003464.xls
7A2A6E-5561	/Users/susie/Documents/003464.xls
7FMAEZ-5562	C:\Users\susie\Documents\003464.xls
7W9P7F-5562	Users\susie\Documents\003464.xls
89LGKW-5561	Path: 21-5561.E01/Partition 2/NONAME [NTFS]/[root]/Users/susie/Documents/003464.xls Filename: 003464.xls
89NM2E-5561	\Users\susie\Documents\003464.xls
8UH9ME-5562	\Users\susie\Documents\003464.xls
8YVWFY-5561	\Users\susie\Documents\003464.xls
93AL3L-5562	21-5561.E01 - Partition 2 (Microsoft NTFS, 19.43 GB)\Users\susie\Documents\003464.xls

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 14

WebCode - Test	Response
9ARR2D-5561	C:\Users/susie/Documents/003464.xls
9GULT8-5562	21-5561.E01/Partition 2/NONAME [NTFS]/[root]/Users/susie/Documents/003464.xls
9V6AXV-5561	\Users\susie\Documents\003464.xls
A8KGFG-5561	Users\susie\Documents 003464.xls
AK9F96-5561	C:\Users\susie\Documents\003464.xls
AQYVXC-5562	21-5561.E01 - Partition 2 (Microsoft NTFS, 19.43 GB)\Users\susie\Documents\003464.xls
AV4RGC-5562	\Partition @ 1187840\Root\Users\susie\Documents\003464.xls
BGJGLT-5561	users\susie\documents\003464.xls
BKPYQG-5561	Path: /Evidence 1/21-5561.E01/[Unnamed Disk Image]/[Unnamed Partition]/[File System Root]/Users/susie/Documents File Name: 003464.xls
BMT8ZD-5561	C:\Users\susie\Documents\003464.xls
BR6KUT-5562	C:\Users\susie\Documents\003464.xls
BWZC2P-5561	21-5561.E01/Partition 2/NONAME [NTFS]/[root]/Users/susie/Documents/003464.xls
CBTGPD-5562	Users\susie\Documents\003464.xls
CMHKPW-5561	\Users\susie\Documents\003464.xls
CPRZ8G-5561	\Users\susie\Documents\003464.xls
CQ9KB9-5562	\Users\Susie\Documents\003464.xls
CQJQ7N-5561	Path and filename of the file containing the term “typhimiurium” – Path (21-5561.E01\Partition 2\NONAME [NTFS]\[root]\Users\susie\Documents\003464.xls / File name “003464.xls”
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	Partition2 \users\susie\documents\003464.xls
E43HU2-5561	\Users\susie\Documents\003464.xls
E7BXK2-5561	\Users\susie\Documents\003464.xls
EELYM9-5561	Partition 2 (Microsoft NTFS, 19.43 GB)\Users\susie\Documents\003464.xls
F2UYKR-5561	The name of the file is 003464.xls and path of the file is partition2/users/Susie/Documents/003464.xls
FFG39B-5562	C:\Users\susie\Documents\003464.xls

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 14	
WebCode - Test	**Response**
FJWWP9-5562	21-5561.E01 - Partition 2 (Microsoft NTFS, 19.43 GB)\Users\susie\Documents\003464.xls
FP3BPR-5562	003464.xls
FTFDBN-5561	21-5561.E01/Partition 2/NONAME [NTFS]/[root]/Users/susie/Documents/003464.xls
G9A37K-5561	\Users\susie\Documents\003464.xls
GGKE74-5561	Users\susie\Documents\003464.xls
GU9W29-5561	Users\susie\Documents\003464.xls
GZY7B8-5561	21-5561.E01-Partition 2 (Microsoft NTFS, 19.43 GB)\Users\susie\Documents\003464.XLS
H949ZJ-5561	21-5561.e01/Partition 2/NONAME [NTFS]/[root]/Users/susie/Documents/003464.xls
HEBY4P-5561	21-5561.E01/Partition 2/NONAME [NTFS]/[root]/Users/susie/Documents/003464.xls
HYFCYH-5561	\Users\susie\Documents\003464.xls
J3U2M6-5561	Partition 2 (Microsoft NTFS, 19.43 GB)\Users\susie\Documents\003464.xls
J3XR9B-5561	/Evidence 1/21-5561.E01/[Unnamed Disk Image]/[Unnamed Partition]/[File System Root]/Users/susie/Documents 003464.xls
JF4GTB-5562	\Users\susie\Documents\003464.xls
JJJA4W-5562	\Users\susie\Documents\003464.xls
JMJLZW-5561	D:\users\susie\Documents\003464.xls
JU4NYL-5561	\Users\susie\Documents\003464.xls
K6Z7V8-5562	Partition 2 (Microsoft NTFS, 19.43 GB)\Users\susie\Documents\003464.xls
KE3C4M-5561	Path = Partition 2 (Microsoft NTFS, 19.43 GB)\Users\susie\Documents\ Filename = 003464.xls
KH3MYM-5562	D\Users\susie\Documents\003464.xls
KT78B9-5562	\Users\susie\Documents\003464.xls
KW3EPY-5561	Partition 2 (Microsoft NTFS, 19.43 GB)\Users\susie\Documents\003464.xls
L9D7RX-5562	21-5561.E01/Partition 2/NONAME [NTFS]/[root]/Users/susie/Documents/003464.xls
LCV3Z2-5561	C:\Users\susie\Documents\003464.xls
LEERBL-5562	\Users\Susie\Documents\Documents\003464.xls

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 14

WebCode - Test	Response
LPY8P3-5561	Users\susie\Documents\003464.xls 003464.xls
LRRLAT-5562	Computer\D\Users\susie\Documents\003464.xls
LXXGTT-5561	21-5561.E01/Partition 2/NONAME [NTFS]/[root]/Users/susie/Documents/003464.xls
M98EB2-5562	\Users\susie\Documents\003464.xls
MWHHA4-5562	Users\susie\Documents\003464.xls
MYJKY6-5562	003464.xls \Users\susie\Documents
N66VNU-5561	C:/Users/Susie/Documents/003464.xls
NFQ2KX-5562	Partition 2 (Microsoft NTFS, 19.43 GB)\Users\susie\Documents\003464.xls
NPAH8D-5561	21-5561.E01/Partition 2/NONAME [NTFS]/[root]/Users/susie/Documents/003464.xls 003464.xls
NRJXPX-5561	Partition 2/NONAME [NTFS]/[root]/Users/susie/Documents/003464.xls
NTAT4D-5561	21-5561.E01/Partition 2/NONAME [NTFS]/[root]/Users/susie/Documents/003464.xls
NUKNP6-5562	003464.xls
PBBNHP-5561	21-5561.e01 - Partition 2\Users\susie\Documents\003464.xls
PBQMFZ-5561	File name: 003464.xls Partition 2 (Microsoft NTFS, 19.43 GB)\Users\susie\Documents\003464.xls
PTA4GV-5562	Name: 003464.xls Path: Partition 2/[root]/Users/Susie/Documents/003464.xls
QP2MPV-5561	Path: \Users\susie\Documents\003464.xls Filename: 003464.xls
R36ZB9-5561	21-5561.E01/Partition 2/NONAME [NTFS]/[root]/users/susie/Documents/003464.xls NAME: 003464.xls
RAQR4V-5562	Users\susie\Documents\003464.xls
RFUVTT-5561	Users\susie\Documents\003464.xls
RGQL4V-5561	Users\susie\Documents\003464.xls
RK6QRB-5561	21-5561.E01/Partition 2/NONAME [NTFS]/[root]/Users/susie/Documents/003464.xls
RXCADP-5561	21-5561.E01 - Partition 2 (Microsoft NTFS, 19.43 GB)\Users\susie\Documents\003464.xls , 003464.xls
T8F7TZ-5562	Users\susie\Documents\003464.xls
TCA8P9-5561	Path: 21-5561.E01/Partition 2/NONAME [NTFS]/[root]/Users/susie/Documents/003464.xls Filename: 003464

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 14	
WebCode - Test	**Response**
TDLF3U-5561	Users\susie\Documents\003464.xls 003464.xls
TFMD29-5561	\Users\susie\Documents\003464.xls
TMAWNW-5561	Users\susie\Documents\003464.xls
U298Q9-5561	Partition2/NONAME[NTFS]/root/Users/susie/Documents/003464.xls
U964DC-5562	C\Users\susie\Documents\003464.xls - Filename - 003464.xls
UWTR4N-5561	\Users\susie\Documents\003464.xls
V23CK9-5561	C:\Users\susie\Documents\003646.xls
V96U7R-5561	C:\Users\susie\Documents\003464.xls
VFHDED-5561	003464.xls [NTFS]/[root]/Users/susie/Documents/003464.xls
WHMDWP-5561	The path of the file : 21-5561.E01/Partition 2/NONAME [NTFS]/[root]/Users/susie/Documents/003464.xls The filename of the file : 003464.xls
WLLU9J-5561	\Users\susie\Documents\003464.xls
WRR3GT-5561	Path: \Users\suzie\Documents\003464.xls Filename: 003464.xls
WW4B2Q-5561	C:\Users\susie\Documents\003464.xls
X436QC-5562	C:\Users\susie\Documents\003464.xls
X4L22Q-5562	\Users\susie\Documents\003464.xls
XCDUFN-5561	\Users\susie\Documents\003464.xls
XHHHQN-5561	Partition 2\Users\susie\Documents\003464.xls
XUR36B-5561	C:\Users\susie\Documents\003464.xls
Y2ANWU-5561	21-5561.E01 - Partition 2 (Microsoft NTFS, 19.43 GB) \Users\susie\Documents\003464.xls
YQTYXP-5561	ROOT\Users\susie\Documents\003464.xls
YXADZU-5561	/Users/susie/Documents/003464.xls
YYKJVA-5561	\Users\susie\Documents\003464.xls
ZGHWCN-5561	\\Users\susie\Documents\003464.xls
ZM6UW6-5561	21-5561.E01\Partition 2\NONAME [NTFS]\[root]\Users\susie\Documents\003464.xls 003464.xls

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 14	
WebCode - Test	**Response**
ZTBFTE-5561	\Users\susie\Documents\003464.xls

Question 14: Provide the path and filename of the file containing the term "typhimiurium".

Consensus Result:

C:\Users\susie\Documents\003464.xls and all formatting styles which represent the same information.

Expected Response Explanation:

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

Expected Response Illustration:

EnCase view of keyword search results.

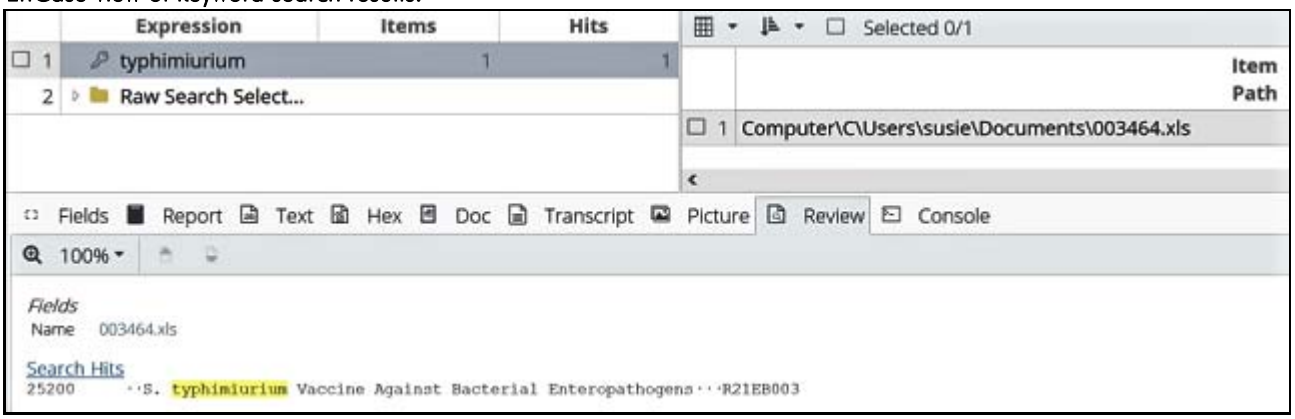


TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15

Question 15: What (non-encryption related) anti-forensics application did the user execute?

Manufacturer's Expected Response:

Please refer to the section labeled "Consensus Result" for this specific question for more information.

WebCode - Test	Response ** Inconsistencies not highlighted; No consensus achieved **
23UJ67-5561	Tor.exe
29JUMG-5562	Tor
2YBWJR-5562	Tor.exe
3B7V4P-5561	TOR BROWSER
3RC2CZ-5561	Another anti-forensics application that the user executed was Tor.exe
44372B-5561	Tor Browser
4A86BF-5561	Tor Browser
4UEFFJ-5561	tor.exe
66CHBZ-5561	Cleanmgr
67H6N6-5562	sdelete64.exe
6G29KN-5562	Tor.exe
6LBUJ2-5561	sd.exe
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	VirtualBox
6ZD7FZ-5561	sDelete
7A2A6E-5561	Tor browser
7FMAEZ-5562	SDelete64.exe
7W9P7F-5562	Tor.exe
89LGKW-5561	tor.exe
89NM2E-5561	Tor Browser
8UH9ME-5562	tor.exe
8YVWFY-5561	TOR Browser
93AL3L-5562	TOR.exe

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15

WebCode - Test	Response ** Inconsistencies not highlighted; No consensus achieved **
9ARR2D-5561	This question is too broad. There are many programs installed that could be used for anti-forensics or to aid in anti-forensics, but the most common program seen that has been executed was CLEANMGR.EXE.
9GULT8-5562	TOR.exe
9V6AXV-5561	Tor Browser
A8KGFG-5561	Tor Browser
AK9F96-5561	sd.exe
AQYVXC-5562	Tor.exe
AV4RGC-5562	Disk Cleanup (cleanmgr.exe)
BGJGLT-5561	Tor-Browser
BKPYQG-5561	Sdelete64.exe
BMT8ZD-5561	Tor Browser
BR6KUT-5562	sdelete64.exe
BWZC2P-5561	Tor
CBTGPD-5562	TOR Browser (tor.exe)
CMHKPW-5561	CLEANMGR.EXE, sdelete64.exe, defrag.exe, LOCKAPP.EXE
CPRZ8G-5561	tor.exe
CQ9KB9-5562	Tor.exe
CQJQ7N-5561	Anti-forensic (non-encryption related) application that the user executed – gpgconf.exe
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	Cleanmgr.exe
E43HU2-5561	Tor Browser
E7BXK2-5561	Tor.exe
EELYM9-5561	sd.exe
F2UYKR-5561	Tor Browser was used by the user probably to hide the data being accessed.
FFG39B-5562	cleanmgr.exe

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15

WebCode - Test	Response ** Inconsistencies not highlighted; No consensus achieved **
FJWWP9-5562	gpg
FP3BPR-5562	The user executed the anti-forensic tool 'SD.exe'. TOR is present however prefetch analysis shows that TOR.EXE has not been ran
FTFDBN-5561	Tor Browser
G9A37K-5561	Tor, Disk Cleanup Tool (Cleanmgr.exe), and SDelete (SD.exe).
GGKE74-5561	Tor Browser
GU9W29-5561	Tor.exe
GZY7B8-5561	SD.EXE
H949ZJ-5561	GPG
HEBY4P-5561	VBoxWindowsAdditions-AMD64.exe
HYFCYH-5561	TOR
J3U2M6-5561	sd.exe
J3XR9B-5561	SD.exe Sdelete64.exe On desktop and on prefetch
JF4GTB-5562	tor.exe
JJJA4W-5562	Tor.exe
JMJLZW-5561	TOR.exe
JU4NYL-5561	Tor Browser
K6Z7V8-5562	VirtualBox
KE3C4M-5561	Tor Browser
KH3MYM-5562	CLEANMGR
KT78B9-5562	Tor Browser
KW3EPY-5561	Tor Browser, the executable is 'Tor.exe' (TOR = The Onion Router)
L9D7RX-5562	Disk Cleanup (cleanmgr.exe)
LCV3Z2-5561	sd.exe
LEERBL-5562	tor.exe

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15

WebCode - Test	Response ** Inconsistencies not highlighted; No consensus achieved **
LPY8P3-5561	cleanmgr.exe
LRRLAT-5562	Tor browser
LXXGTT-5561	tor.exe
M98EB2-5562	TOR.EXE
MWHHA4-5562	tor.exe
MYJKY6-5562	tor.exe
N66VNU-5561	SD.EXE {sdelete} (sdelete64.exe by Sysinternals - www.sysinternals.com)
NFQ2KX-5562	gpg.exe
NPAH8D-5561	Tor Firefox
NRJXPX-5561	cleanmgr.exe
NTAT4D-5561	Tor.exe
NUKNP6-5562	tor.exe
PBBNHP-5561	TOR.EXE
PBQMFZ-5561	Sd.exe is command line program named SDelete aka secure delete. This file was exported from the image file and executed. Found to be SDelete v2.04 with a valid Microsoft certificate. There is a record of this program being executed eight (8) times based on the Prefetch files. \VOLUME{01d70660173e4f97-f617480a}\USERS\SUSIE\DESKTOP\SD.EXE Last Run: 3/7/2021 3:49:38 AM First Run: 3/7/2021 3:28:52 AM
PTA4GV-5562	Disk Cleanup (Cleanmgr.exe) sd.exe Tor browser
QP2MPV-5561	tor.exe
R36ZB9-5561	tor.exe (TOR)
RAQR4V-5562	Tor
RFUVTT-5561	tor
RGQL4V-5561	Tor.exe
RK6QRB-5561	Tor Browser
RXCADP-5561	Tor.exe

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15

WebCode - Test	Response ** Inconsistencies not highlighted; No consensus achieved **
T8F7TZ-5562	tor
TCA8P9-5561	SDEL.EXE (also known as SD.EXE) which is a command line function that can be used by a computer's user to delete files in a similar manner as CCleaner. It was also noted that TOR.EXE was used.
TDLF3U-5561	cleanmgr.exe
TFMD29-5561	sdelete64.exe
TMAWNW-5561	Tor browser
U298Q9-5561	cleanmgr.exe
U964DC-5562	Tor Browser
UWTR4N-5561	C:\Users\susie\Desktop\Tor Browser\Browser\firefox.exe (Tor)
V23CK9-5561	Tor Browser
V96U7R-5561	cleanmgr.exe
VFHDED-5561	SDelete.exe
WHMDWP-5561	sdelete64.exe
WLLU9J-5561	There are two: sdelete.exe and Cleanmgr.exe
WRR3GT-5561	Tor
WW4B2Q-5561	SDelete v2.04 - Secure file delete C:\Users\susie\Desktop\sd.exe
X436QC-5562	TOR.exe
X4L22Q-5562	Tor.exe
XCDUFN-5561	sdelete64.exe
XHHHQN-5561	SDelete/Tor Browser
XUR36B-5561	TOR.exe
Y2ANWU-5561	Tor
YQTYXP-5561	Tor.exe
YXADZU-5561	TOR.EXE
YYKJVA-5561	sdelete64.exe

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15	
WebCode - Test	**Response** ** Inconsistencies not highlighted; No consensus achieved **
ZGHWCN-5561	Tor.exe
ZM6UW6-5561	Tor Browser
ZTBFTE-5561	sdelete64.exe (SysInternals sdelete) The user also executed tor.exe, which is arguably an anti-forensics tool.

Question 15: What (non-encryption related) anti-forensics application did the user execute?

Consensus Result:

After a full review of participants' responses, this question was deemed to not be of value to the proficiency test. No expected response is being provided.

Expected Response Explanation:

Participants' results have been presented, however due to the question being found to be of no value, no expected response nor discussion on achieving that response is being provided.

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16

Question 16: What was the name of the LAST wireless network to which the computer was connected?

Manufacturer's Expected Response:

RCMP Surveillance Moose

WebCode - Test	Response
23UJ67-5561	"RCMP Surveillance Moose"
29JUMG-5562	RCMP Surveillance Moose
2YBWJR-5562	RCMP Surveillance Moose
3B7V4P-5561	RCMP Surveillance Moose
3RC2CZ-5561	The last wireless network is named "RCMP Surveillance Moose".
44372B-5561	RCMP Surveillance Moose
4A86BF-5561	RCMP Surveillance Moose
4UEFFJ-5561	RCMP Surveillance Moose
66CHBZ-5561	Wi-Fi
67H6N6-5562	RCMP Surveillance Moose
6G29KN-5562	RCMP Surveillance Moose
6LBUJ2-5561	RCMP Surveillance Moose
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	Network
6ZD7FZ-5561	RCMP Surveillance Moose
7A2A6E-5561	RCMP Surveillance Moose
7FMAEZ-5562	RCMP Surveillance Moose
7W9P7F-5562	Network
89LGKW-5561	RCMP Surveillance Moose
89NM2E-5561	RCMP Surveillance Moose
8UH9ME-5562	RCMP Surveillance Moose
8YVWFY-5561	RCMP Surveillance Moose
93AL3L-5562	RCMP Surveillance Moose

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16	
WebCode - Test	**Response**
9ARR2D-5561	Skynet
9GULT8-5562	RCMP Surveillance Moose
9V6AXV-5561	RCMP Surveillance Moose
A8KGFG-5561	Network
AK9F96-5561	RCMP Surveillance Moose
AQYVXC-5562	RCMP Surveillance Moose, 06/03/2021 18:11:11 (Local time)
AV4RGC-5562	RCMP Surveillance Moose
BGJGLT-5561	RCMP Surveillance Moose
BKPYQG-5561	RCMP Surveillance Moose
BMT8ZD-5561	RCMP Surveillance Moose
BR6KUT-5562	RCMP Surveillance Moose
BWZC2P-5561	RCMP Surveillance Moose
CBTGPD-5562	RCMP Surveillance Moose
CMHKPW-5561	RCMP Surveillance Moose
CPRZ8G-5561	RCMP Surveillance Moose
CQ9KB9-5562	RCMP Surveillance Moose
CQJQ7N-5561	Name of last wireless network the computer was connected to – "Network"
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	RCMP Surveillance Moose
E43HU2-5561	RCMP Surveillance Moose
E7BXK2-5561	RCMP Surveillance Moose
EELYM9-5561	RCMP Surveillance Moose

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16

WebCode - Test	Response
F2UYKR-5561	WLAN AutoConfig service has successfully connected to a wireless network. Network Adapter: 802.11n USB Wireless LAN Card Interface GUID: {173ee097-33c8-488e-a6bb-d3505caf2957} Connection Mode: Connection to a secure network without a profile Profile Name: RCMP Surveillance Moose SSID: RCMP Surveillance Moose BSS Type: Infrastructure PHY Type: 802.11n Authentication: WPA2-Personal Encryption: AES-CCMP 802.1x Enabled: No Hidden: false
FFG39B-5562	Network
FJWWP9-5562	RCMP Surveillance Moose
FP3BPR-5562	Network
FTFDBN-5561	RCMP Surveillance Moose
G9A37K-5561	RCMP Surveillance Moose 3/6/2021 18:11:11
GGKE74-5561	RCMP Surveillance Moose
GU9W29-5561	RCMP Surveillance Moose
GZY7B8-5561	RCMP Surveillance Moose
H949ZJ-5561	RCMP Surveillance Moose
HEBY4P-5561	802.11n USB Wireless LAN Card
HYFCYH-5561	RCMP Surveillance Moose
J3U2M6-5561	RCMP Surveillance Moose
J3XR9B-5561	RCMP Surveillance Moose
JF4GTB-5562	RCMP Surveillance Moose
JJJA4W-5562	RCMP Surveillance Moose
JMJLZW-5561	RCMP Surveillance Moose
JU4NYL-5561	RCMP Surveillance Moose
K6Z7V8-5562	RCMP Surveillance Moose
KE3C4M-5561	RCMP Surveillance Moose

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16	
WebCode - Test	**Response**
KH3MYM-5562	RCMP Surveillance Moose
KT78B9-5562	RCMP Surveillance Moose
KW3EPY-5561	RCMP Surveillance Moose
L9D7RX-5562	RCMP Surveillance Moose
LCV3Z2-5561	RCMP Surveillance Moose
LEERBL-5562	RCMP Surveillance Moose
LPY8P3-5561	skynet
LRRLAT-5562	RCMP Surveillance Moose
LXXGTT-5561	RCMP Surveillance Moose
M98EB2-5562	RCMP Surveillance Moose
MWHHA4-5562	Skynet
MYJKY6-5562	RCMP Surveillance Moose
N66VNU-5561	“RCMP Surveillance Moose”
NFQ2KX-5562	RCMP Surveillance Moose
NPAH8D-5561	RCMP Surveillance Moose
NRJXPX-5561	Network
NTAT4D-5561	RCMP Surveillance Moose
NUKNP6-5562	Skynet
PBBNHP-5561	RCMP Surveillance Moose
PBQMFZ-5561	RCMP Surveillance Moose- 3/6/2021 6:11:11 PM
PTA4GV-5562	RCMP Surveillance Moose
QP2MPV-5561	RCMP Surveillance Moose
R36ZB9-5561	RCMP Surveillance Moose
RAQR4V-5562	RCMP Surveillance Moose

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16	
WebCode - Test	**Response**
RFUVTT-5561	RCMP Surveillance Moose
RGQL4V-5561	RCMP Surveillance Moose
RK6QRB-5561	RCMP Surveillance Moose
RXCADP-5561	RCMP Surveillance Moose
T8F7TZ-5562	RCMP Surveillance Moose
TCA8P9-5561	RCMP Surveillance Moose
TDLF3U-5561	RCMP Surveillance Moose
TFMD29-5561	RCMP Surveillance Moose
TMAWNW-5561	Network
U298Q9-5561	RCMP Surveillance Moose
U964DC-5562	Skynet
UWTR4N-5561	RCMP Surveillance Moose
V23CK9-5561	RCMP Surveillance Moose
V96U7R-5561	RCMP Surveillance Moose
VFHDED-5561	Network Last Connect Ft 3/10/2021 08:38:36 UTC
WHMDWP-5561	Network
WLLU9J-5561	RCMP Surveillance Moose
WRR3GT-5561	RCMP Surveillance Moose
WW4B2Q-5561	RCMP Surveillance Moose (password: nopassword@$)
X436QC-5562	RCMP Surveillance Moose
X4L22Q-5562	RCMP Surveillance Moose
XCDUFN-5561	RCMP Surveillance Moose
XHHHQN-5561	RCMP Surveillance Moose
XUR36B-5561	RCMP Surveillance Moose

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16	
WebCode - Test	**Response**
Y2ANWU-5561	RCMP Surveillance Moose
YQTYXP-5561	RCMP Surveillance Moose
YXADZU-5561	RCMP Surveillance Moose
YYKJVA-5561	RCMP Surveillance Moose
ZGHWCN-5561	RCMP Surveillance Moose
ZM6UW6-5561	Network
ZTBFTE-5561	RCMP Surveillance Moose

Question 16: What was the name of the LAST wireless network to which the computer was connected?

Consensus Result:
RCMP Surveillance Moose

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. The wireless network with the latest "DateLastConnected" value is "RCMP Surveillance Moose".

Expected Response Illustration:

RegRipper View of Software:Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles

```
Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles
Network
  Key LastWrite     : 2021-03-06 17:06:25Z
  DateLastConnected: 2021-03-06 18:06:25
  DateCreated       : 2021-02-18 17:45:09
  DefaultGatewayMac: 52-54-00-12-35-02
  Type              : wired
RCMP Surveillance Moose
  Key LastWrite     : 2021-03-06 17:11:11Z
  DateLastConnected: 2021-03-06 18:11:11
  DateCreated       : 2021-03-06 18:11:11
  DefaultGatewayMac: C2-B5-4F-BC-2A-6C
  Type              : wireless
Skynet
  Key LastWrite     : 2021-03-06 17:09:06Z
  DateLastConnected: 2021-03-06 18:09:06
  DateCreated       : 2021-03-06 18:09:06
  DefaultGatewayMac: 30-5A-3A-C3-2E-E1
  Type              : wireless
```


TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17

Question 17: What IP address was assigned by this network?

Manufacturer's Expected Response:

192.168.40.37

WebCode - Test	Response
23UJ67-5561	192.168.40.37
29JUMG-5562	192.168.40.37
2YBWJR-5562	192.168.40.37
3B7V4P-5561	192.168.40.37
3RC2CZ-5561	The IP address that was assigned by this network was 192.168.40.37
44372B-5561	192.168.40.37
4A86BF-5561	192.168.40.37
4UEFFJ-5561	192.168.40.37
66CHBZ-5561	192.168.40.37
67H6N6-5562	192.168.40.37
6G29KN-5562	192.168.40.37
6LBUJ2-5561	192.168.40.37
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	192.168.40.37
6ZD7FZ-5561	192.168.40.37
7A2A6E-5561	192.168.40.37
7FMAEZ-5562	192.168.40.37
7W9P7F-5562	192.168.40.37
89LGKW-5561	192.168.40.37
89NM2E-5561	192.168.40.37
8UH9ME-5562	192.168.40.37 I did my best to answer this one, but we don't normally identify IP addresses in our unit. If a case gets that complicated that we're tracking down user's IP addresses we call a special team outside of our agency for help.
8YVWFY-5561	192.168.40.37

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17	
WebCode - Test	**Response**
93AL3L-5562	192.168.40.37
9ARR2D-5561	192.168.40.37
9GULT8-5562	192.168.40.37
9V6AXV-5561	192.168.40.37
A8KGFG-5561	10.0.2.15
AK9F96-5561	192.168.40.37
AQYVXC-5562	SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{173ee097-33c8-488e-a6bb-d3505caf2957} - 192.168.40.37
AV4RGC-5562	192.168.40.37
BGJGLT-5561	192.168.40.37
BKPYQG-5561	192.168.101.121
BMT8ZD-5561	192.168.40.37
BR6KUT-5562	192.168.40.37
BWZC2P-5561	192.168.40.37
CBTGPD-5562	192.168.40.37
CMHKPW-5561	192.168.40.37
CPRZ8G-5561	192.168.40.37
CQ9KB9-5562	192.168.40.37
CQJQ7N-5561	IP address assigned by this network – "10.0.2.15"
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	192.168.40.37
E43HU2-5561	192.168.40.37
E7BXK2-5561	192.168.40.37
EELYM9-5561	192.168.40.37
F2UYKR-5561	192.168.40.37 was the DHCP IP Address assigned.

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17	
WebCode - Test	**Response**
FFG39B-5562	192.168.40.37
FJWWP9-5562	192.168.40.37
FP3BPR-5562	The IP address assigned by the network 'Network' was 10.0.2.15
FTFDBN-5561	192.168.40.37
G9A37K-5561	192.168.40.37
GGKE74-5561	192.168.40.37
GU9W29-5561	192.168.40.37
GZY7B8-5561	192.168.40.37
H949ZJ-5561	192.168.40.37
HEBY4P-5561	192.168.40.37
HYFCYH-5561	192.168.40.37
J3U2M6-5561	192.168.40.37
J3XR9B-5561	192.168.40.37
JF4GTB-5562	192.168.40.37
JJJA4W-5562	192.168.40.37
JMJLZW-5561	192.168.40.37
JU4NYL-5561	192.168.40.37
K6Z7V8-5562	192.168.40.37
KE3C4M-5561	192.168.40.37
KH3MYM-5562	192.168.40.37
KT78B9-5562	192.168.40.37
KW3EPY-5561	192.168.40.37
L9D7RX-5562	192.168.40.37
LCV3Z2-5561	192.168.40.37

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17	
WebCode - Test	**Response**
LEERBL-5562	192.168.101.121
LPY8P3-5561	192.168.40.37
LRRLAT-5562	192.168.40.37
LXXGTT-5561	192.168.40.37
M98EB2-5562	192.168.40.37
MWHHA4-5562	192.168.40.37
MYJKY6-5562	192.168.40.37
N66VNU-5561	192.168.40.37
NFQ2KX-5562	192.168.40.37
NPAH8D-5561	192.168.40.37
NRJXPX-5561	192.168.40.37
NTAT4D-5561	192.168.40.37
NUKNP6-5562	192.168.101.1
PBBNHP-5561	192.168.40.37
PBQMFZ-5561	192.168.40.37
PTA4GV-5562	192.168.40.37
QP2MPV-5561	192.168.40.37
R36ZB9-5561	192.168.40.37
RAQR4V-5562	192.168.40.37
RFUVTT-5561	192.168.40.37
RGQL4V-5561	192.168.40.37
RK6QRB-5561	192.168.40.37
RXCADP-5561	192.168.40.37
T8F7TZ-5562	192.168.40.37

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17	
WebCode - Test	**Response**
TCA8P9-5561	192.168.40.37
TDLF3U-5561	192.168.40.37
TFMD29-5561	192.168.40.37
TMAWNW-5561	192.168.101.121
U298Q9-5561	192.168.40.37
U964DC-5562	192.168.40.37
UWTR4N-5561	192.168.40.37
V23CK9-5561	192.168.40.37
V96U7R-5561	192.168.40.37
VFHDED-5561	IP Address 10.0.2.15 Subnet Mask 255.255.255.0 Gateway 10.0.2.2
WHMDWP-5561	10.0.2.15
WLLU9J-5561	192.168.40.37
WRR3GT-5561	192.168.40.37
WW4B2Q-5561	192.168.40.37
X436QC-5562	192.168.40.37
X4L22Q-5562	192.168.40.37
XCDUFN-5561	192.168.40.37
XHHHQN-5561	192.168.40.37
XUR36B-5561	192.168.40.37
Y2ANWU-5561	Initially 192.168.101.121 – Saturday 6th March 2021 17:09:05, which was nearly immediately terminated, and then became 192.168.40.37 – Saturday 6th March 2021 17:11:11, which was terminated at Saturday 6th March 2021 18:11:10
YQTYXP-5561	192.168.40.37
YXADZU-5561	192.168.40.37
YYKJVA-5561	192.168.40.37

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17	
WebCode - Test	**Response**
ZGHWCN-5561	192.168.40.37
ZM6UW6-5561	10.0.2.15
ZTBFTE-5561	192.168.40.37

Question 17: What IP address was assigned by this network?

Consensus Result:
192.168.40.37

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

Expected Response Illustration:

RegRipper view of SYSTEM:ControlSet001\Services\Tcpip\Parameters\Interfaces

```
nic2 v.20200525
(System) Gets NIC info from System hive

Adapter: {173ee097-33c8-488e-a6bb-d3505caf2957}
LastWrite Time: 2021-03-06 17:11:11Z
  EnableDHCP                    1
  Domain
  NameServer
  DhcpIPAddress                 192.168.40.37
  DhcpSubnetMask                255.255.255.0
  DhcpServer                    192.168.40.150
  Lease                         3599
  LeaseObtainedTime             2021-03-06 17:11:11Z
  T1                            2021-03-06 17:41:10Z
  T2                            2021-03-06 18:03:40Z
  LeaseTerminatesTime           2021-03-06 18:11:10Z
  AddressType                   0
  IsServerNapAware              0
  DhcpConnForceBroadcastFlag    0
  DhcpNetworkHint               RCMP Surveillance Moose
```


TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18

Question 18: What encryption program did the user execute?

Manufacturer's Expected Response:

VeraCrypt, Or Veracrypt-X64, or VeraCrypt Setup 1.24-Update7.exe

WebCode - Test	Response
23UJ67-5561	gpg (Gnu Privacy Guard)and VeraCrypt
29JUMG-5562	Veracrypt
2YBWJR-5562	Veracypt
3B7V4P-5561	VERACRYPT
3RC2CZ-5561	The encryption program the user executed was "Veracrypt".
44372B-5561	VeraCrypt
4A86BF-5561	Veracrypt
4UEFFJ-5561	gpg.exe
66CHBZ-5561	VeraCrypt -x64
67H6N6-5562	VeraCrypt-x64.exe
6G29KN-5562	VeraCrypt
6LBUJ2-5561	VeraCrypt
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	Veracrypt
6ZD7FZ-5561	veracrypt
7A2A6E-5561	veracrypt
7FMAEZ-5562	Veracrypt.exe
7W9P7F-5562	VeraCrypt-x64.exe
89LGKW-5561	VeraCrypt Gpg4win\bin\kleopatra.exe Protonmail can be used to encrypt emails GNU Privacy Guard (App Installed) Gpg4Win (App Installed)
89NM2E-5561	VeraCrypt
8UH9ME-5562	Veracrypt

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18

WebCode - Test	Response
8YVWFY-5561	Veracrypt
93AL3L-5562	VeraCrypt-x64.exe
9ARR2D-5561	Veracrypt
9GULT8-5562	GPG.exe
9V6AXV-5561	VeraCrypt
A8KGFG-5561	Kleopatra
AK9F96-5561	VeraCrypt
AQYVXC-5562	gpg4win-3.1.15
AV4RGC-5562	VeraCrypt
BGJGLT-5561	Vera Crypt
BKPYQG-5561	VeraCrypt-x64.exe
BMT8ZD-5561	Veracrypt (veracrypt-x64.exe)
BR6KUT-5562	VeraCrypt-x64.exe
BWZC2P-5561	VeraCrypt
CBTGPD-5562	VeraCrypt (veracrypt-x64.exe)
CMHKPW-5561	VERACRYPT-X64.EXE, GPG.EXE, GPG4WIN-3.1.15.EXE
CPRZ8G-5561	VeraCrypt, GNU Privacy Guard, and Gpg4win
CQ9KB9-5562	Veracrypt
CQJQ7N-5561	Encryption program that the user executed – VeraCrypt.exe
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	VeraCrypt
E43HU2-5561	VeraCrypt (GPG, Kleopatra)
E7BXK2-5561	veracrypt
EELYM9-5561	VeraCrypt-x64.exe

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18

WebCode - Test	Response
F2UYKR-5561	VeraCrypt was used by the user.
FFG39B-5562	Veracrypt
FJWWP9-5562	VeraCrypt
FP3BPR-5562	Veracrypt
FTFDBN-5561	VeraCrypt
G9A37K-5561	GPG.exe and Veracrypt-X64.exe
GGKE74-5561	VeraCrypt
GU9W29-5561	Veracrypt-x64.exe
GZY7B8-5561	Veracrypt
H949ZJ-5561	Veracrypt
HEBY4P-5561	Gpg4win-3.1.15
HYFCYH-5561	VERACRYPT-X64.EXE
J3U2M6-5561	VeraCrypt
J3XR9B-5561	VeraCrypt-x64.exe
JF4GTB-5562	VeraCrypt-x64.exe
JJJA4W-5562	veracrypt
JMJLZW-5561	GPG.exe
JU4NYL-5561	VERACRYPT
K6Z7V8-5562	VERACRYPT-X64.EXE
KE3C4M-5561	VeraCrypt
KH3MYM-5562	GPG
KT78B9-5562	GPG (Kleopatra.exe), Veracrypt-x64.exe
KW3EPY-5561	VeraCrypt-x64.exe
L9D7RX-5562	VeraCrypt-x64.exe

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18	
WebCode - Test	**Response**
LCV3Z2-5561	VeraCrypt-x64.exe
LEERBL-5562	Veracrypt-x64.exe Veracrypt
LPY8P3-5561	Veracrypt
LRRLAT-5562	VeraCrypt
LXXGTT-5561	Veracrypt
M98EB2-5562	Veracrypt
MWHHA4-5562	VeraCrypt
MYJKY6-5562	gpg.exe
N66VNU-5561	D:\VeraCrypt\VeraCrypt-x64.exe
NFQ2KX-5562	D:\VeraCrypt\VeraCrypt-x64.exe
NPAH8D-5561	VeraCrypt
NRJXPX-5561	Vera Crypt
NTAT4D-5561	Veracrypt.exe
NUKNP6-5562	Kleopatra
PBBNHP-5561	VeraCrypt
PBQMFZ-5561	The GPG4WIN encryption suite is installed on the system: C:\Program Files (x86)\Gpg4win along with C:\Program Files (x86)\GnuPG\bin\gpg.exe GPG.exe last executed 03/04/2021 12:11:12 AM according to the Prefetch file Kleopatra was last executed 3/4/2021 12:02:36AM Kleopatra is the front-end GUI and cert manager for the encryption program GnUPG (GPG.exe) Veracrypt-X64.exe last executed 03/07/2021 03:29:55 AM
PTA4GV-5562	VeraCrypt.exe
QP2MPV-5561	Veracrypt & gpg
R36ZB9-5561	Veracrypt
RAQR4V-5562	Veracrypt
RFUVTT-5561	Veracrypt
RGQL4V-5561	Gpg.exe and veracrypt-X64.exe
RK6QRB-5561	VeraCrypt

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18

WebCode - Test	Response
RXCADP-5561	GPG.EXE
T8F7TZ-5562	Veracrypt
TCA8P9-5561	Veracrypt
TDLF3U-5561	Veracrypt
TFMD29-5561	Veracrypt
TMAWNW-5561	gpg4Win
U298Q9-5561	Veracrypt.exe
U964DC-5562	Veracrypt
UWTR4N-5561	VeraCrypt
V23CK9-5561	Veracrypt
V96U7R-5561	VeraCrypt
VFHDED-5561	VeraCrypt-x64.exe
WHMDWP-5561	gpg.exe, tor.exe and VERACRYPT-X64.EXE
WLLU9J-5561	VERACRYPT-X64.EXE
WRR3GT-5561	Veracrypt and GPG
WW4B2Q-5561	VeraCrypt
X436QC-5562	VeraCrypt
X4L22Q-5562	VeraCrypt
XCDUFN-5561	VeraCrypt
XHHHQN-5561	Gpg4win, VeraCrypt
XUR36B-5561	VeraCrypt-x64.exe
Y2ANWU-5561	VeraCrypt was ran as VERACRYPT-X64.exe from a D:\ drive Gpg.exe
YQTYXP-5561	Veracrypt was used to attach a volume. Artifacts located in the Windows Defender log also show Gpg4win being installed and uninstalled.
YXADZU-5561	VERACRYPT-X64.exe / Veracrypt

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18

WebCode - Test	Response
YYKJVA-5561	VeraCrypt-x64.exe
ZGHWCN-5561	VeraCrypt
ZM6UW6-5561	Veracrypt
ZTBFTE-5561	VERACRYPT-X64.EXE

Question 18: What encryption program did the user execute?

Consensus Result:

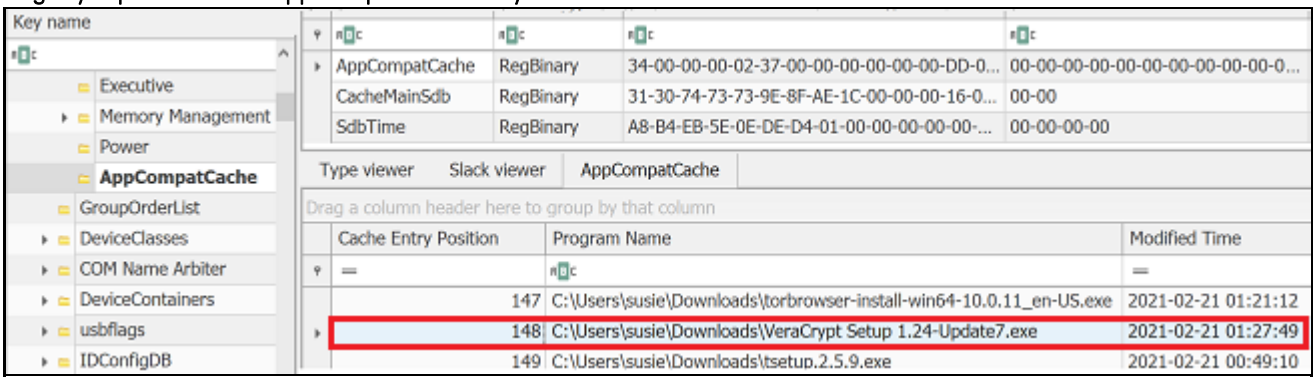
VeraCrypt and all formatting styles which represent the same information. In addition, GPG and Kleopatra were also accepted.

Expected Response Explanation:

Records of execution of the Veracrypt program can be found in AppCompcatCache data in the SYSTEM registry hive and in Windows prefetch files.

Expected Response Illustration:

Registry Explorer view of AppCompcatCache key



EnCase view of Veracrypt Prefetch file

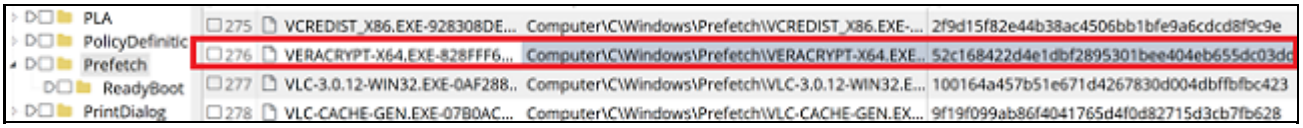


TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 19

Question 19: The encrypted volume was mounted to what drive letter?

Manufacturer's Expected Response:

V

WebCode - Test	Response
23UJ67-5561	V:
29JUMG-5562	V:\
2YBWJR-5562	V
3B7V4P-5561	V:
3RC2CZ-5561	It appears that the encrypted volume was mounted as letter "V".
44372B-5561	V:\
4A86BF-5561	V:\
4UEFFJ-5561	V
66CHBZ-5561	Drive Letter V
67H6N6-5562	V
6G29KN-5562	V
6LBUJ2-5561	V:
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	E:
6ZD7FZ-5561	v
7A2A6E-5561	V
7FMAEZ-5562	V:
7W9P7F-5562	V:
89LGKW-5561	V:\
89NM2E-5561	V:
8UH9ME-5562	V:
8YVWFY-5561	V:\
93AL3L-5562	V

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 19	
WebCode - Test	**Response**
9ARR2D-5561	V:
9GULT8-5562	V:
9V6AXV-5561	V:
A8KGFG-5561	\:V ??\Volume{c33383fd-7d23-11eb-80e9-08002732dc0f}: VeraCryptVolumeV
AK9F96-5561	V
AQYVXC-5562	V:\
AV4RGC-5562	V
BGJGLT-5561	Veracrypt Volume V
BKPYQG-5561	D:\
BMT8ZD-5561	V:\
BR6KUT-5562	V:
BWZC2P-5561	V:
CBTGPD-5562	V
CMHKPW-5561	D: and E:
CPRZ8G-5561	V:
CQ9KB9-5562	V:\
CQJQ7N-5561	Encrypted volume was mounted to – Drive letter "V"
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	V
E43HU2-5561	V
E7BXK2-5561	V
EELYM9-5561	V:
F2UYKR-5561	By default, it is mounted on drive Z.
FFG39B-5562	V:

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 19	
WebCode - Test	**Response**
FJWWP9-5562	General UDisk USB Device - V
FP3BPR-5562	V:\
FTFDBN-5561	V
G9A37K-5561	V:\
GGKE74-5561	V
GU9W29-5561	V
GZY7B8-5561	V:
H949ZJ-5561	V:
HEBY4P-5561	D:\\
HYFCYH-5561	V:
J3U2M6-5561	V
J3XR9B-5561	VeraCryptVolumeV
JF4GTB-5562	V:
JJJA4W-5562	V
JMJLZW-5561	V
JU4NYL-5561	V:\
K6Z7V8-5562	V
KE3C4M-5561	V:\
KH3MYM-5562	V:\
KT78B9-5562	V: (Veracrypt)
KW3EPY-5561	V
L9D7RX-5562	V
LCV3Z2-5561	V:\
LEERBL-5562	V:\

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 19

WebCode - Test	Response
LPY8P3-5561	V
LRRLAT-5562	V:\\
LXXGTT-5561	V
M98EB2-5562	V:
MWHHA4-5562	V:
MYJKY6-5562	V:
N66VNU-5561	V:
NFQ2KX-5562	V:\
NPAH8D-5561	Drive letter D. is the removable device thats has Veracrypt on it. Drive letter V. is the encrypted volume.
NRJXPX-5561	V:
NTAT4D-5561	Based on the Windows Registry and the additional Operating System artifacts, it is determined that Veracrypt was located on a device that was connected to the system and assigned drive letter D:\. The encrypted volume was mounted as drive letter V:\.
NUKNP6-5562	V:\
PBBNHP-5561	V:
PBQMFZ-5561	V:\
PTA4GV-5562	V
QP2MPV-5561	V:
R36ZB9-5561	Vercacrypt Volume - Drive Letter (V:)
RAQR4V-5562	V
RFUVTT-5561	V
RGQL4V-5561	V:\
RK6QRB-5561	V:
RXCADP-5561	V
T8F7TZ-5562	V
TCA8P9-5561	V:\

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 19	
WebCode - Test	**Response**
TDLF3U-5561	V
TFMD29-5561	V:\
TMAWNW-5561	[Participant did not return results for this question.]
U298Q9-5561	V:\
U964DC-5562	V
UWTR4N-5561	V:
V23CK9-5561	V:\
V96U7R-5561	V: Veracrypt
VFHDED-5561	V:
WHMDWP-5561	V
WLLU9J-5561	\DosDevices\E: then to V:
WRR3GT-5561	V:
WW4B2Q-5561	V:\
X436QC-5562	V
X4L22Q-5562	V
XCDUFN-5561	V
XHHHQN-5561	V
XUR36B-5561	V:
Y2ANWU-5561	File.gpg E:\ ?
YQTYXP-5561	V
YXADZU-5561	V
YYKJVA-5561	V
ZGHWCN-5561	V
ZM6UW6-5561	V:\

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 19

WebCode - Test	Response
ZTBFTE-5561	V:\

Question 19: The encrypted volume was mounted to what drive letter?

Consensus Result:

V

Expected Response Explanation:

The Window SYSTEM registry hive contains records of mounted devices including one for device Volume{c33383fd-7d23-11eb-80e9-08002732dc0f} as "VeraCryptVolumeV".

Expected Response Illustration:

Registry Explorer view of mounted devices key

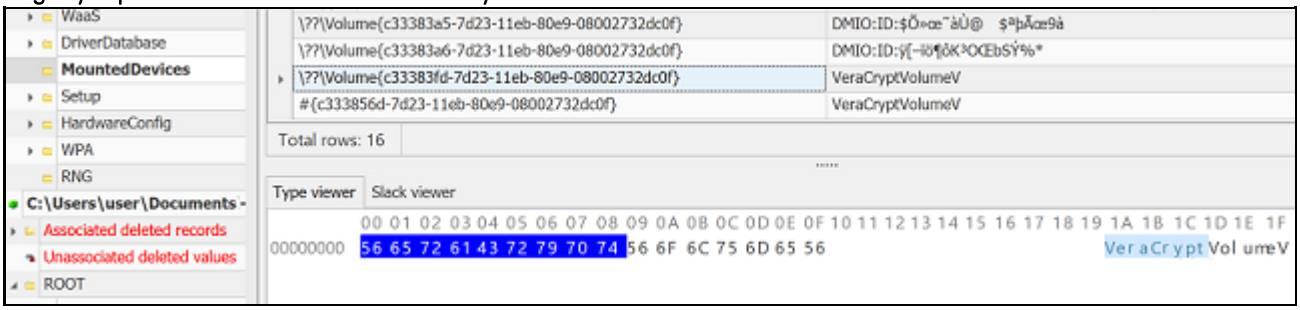


TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20

Question 20: What directory containing photos did the user access on the mounted volume referenced in Question 19?

Manufacturer's Expected Response:

V:\kittehs\

WebCode - Test	Response
23UJ67-5561	kittehs
29JUMG-5562	V:\kittehs\
2YBWJR-5562	Kittehs
3B7V4P-5561	kittehs
3RC2CZ-5561	It appears to be a folder named "kittehs" of the mounted Volume.
44372B-5561	V:\kittehs\
4A86BF-5561	V:\kittehs
4UEFFJ-5561	V:\kittehs\
66CHBZ-5561	kittehs
67H6N6-5562	kittehs
6G29KN-5562	kittehs
6LBUJ2-5561	V:\kittehs\
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	Kittehs
6ZD7FZ-5561	Kittehs
7A2A6E-5561	kittehs
7FMAEZ-5562	V:\kittehs
7W9P7F-5562	kittehs
89LGKW-5561	V:\kittehs
89NM2E-5561	V:\kittehs
8UH9ME-5562	V:\kittehs
8YVWFY-5561	V:\kittehs\

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20

WebCode - Test	Response
93AL3L-5562	V:\kittehs\
9ARR2D-5561	V:/kittehs/
9GULT8-5562	kittehs
9V6AXV-5561	kittehs
A8KGFG-5561	V:\kittehs\
AK9F96-5561	kittehs
AQYVXC-5562	V:\kittehs
AV4RGC-5562	V:\kittehs\
BGJGLT-5561	Kittehs
BKPYQG-5561	\Device\VeraCryptVolumeV\kittehs\
BMT8ZD-5561	V:\kittehs\
BR6KUT-5562	kittehs
BWZC2P-5561	kittehs
CBTGPD-5562	kittehs
CMHKPW-5561	D:\
CPRZ8G-5561	kittehs
CQ9KB9-5562	kittehs
CQJQ7N-5561	Directory containing photos that the user accessed on the mounted volume referenced in Question 19 – "kittehs"
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	kittehs
E43HU2-5561	kittehs
E7BXK2-5561	V:\kittehs
EELYM9-5561	V:\kittehs\
F2UYKR-5561	Directory not found

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20	
WebCode - Test	**Response**
FFG39B-5562	kittehs
FJWWP9-5562	file:///V:/kittehs/
FP3BPR-5562	The folder on the volume mounted at V:\ which contained a series of jpeg images was called 'kittehs'
FTFDBN-5561	kittehs
G9A37K-5561	Kittehs
GGKE74-5561	kittehs
GU9W29-5561	V:\kittehs
GZY7B8-5561	V:\kittehs\
H949ZJ-5561	Kittehs
HEBY4P-5561	Stuff
HYFCYH-5561	kittehs
J3U2M6-5561	V:\kittehs\
J3XR9B-5561	\Device\VeraCryptVolumeV\kittehs\
JF4GTB-5562	kittehs
JJJA4W-5562	V:\kittehs
JMJLZW-5561	Kittehs
JU4NYL-5561	V:\kittehs
K6Z7V8-5562	V:\kittehs
KE3C4M-5561	V:\kittehs\
KH3MYM-5562	kittehs
KT78B9-5562	V:\kittehs
KW3EPY-5561	V:\kittehs\
L9D7RX-5562	Kittehs
LCV3Z2-5561	kittehs

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20

WebCode - Test	Response
LEERBL-5562	V:\Kittehs\
LPY8P3-5561	V:\kittehs\14mq9b8cogk61.jpg
LRRLAT-5562	kittehs
LXXGTT-5561	kittehs
M98EB2-5562	kittehs
MWHHA4-5562	'Kittens'
MYJKY6-5562	kittehs
N66VNU-5561	Kittehs
NFQ2KX-5562	V:\kittehs\
NPAH8D-5561	kittehs
NRJXPX-5561	V:\kittehs
NTAT4D-5561	Based on Operating System artifacts, specifically Link (LNK) files and Jump Lists, it was determined that the directory containing photos (.jpg files) is named kittehs and that the .jpg files were opened with the Microsoft Photos application.
NUKNP6-5562	kittehs
PBBNHP-5561	kittehs
PBQMFZ-5561	V:\kittehs
PTA4GV-5562	kittehs
QP2MPV-5561	V:\kittehs\
R36ZB9-5561	V:\kittehs
RAQR4V-5562	V:\Kittehs
RFUVTT-5561	kittehs
RGQL4V-5561	V:\kittehs\
RK6QRB-5561	kittehs
RXCADP-5561	kittehs
T8F7TZ-5562	kittehs

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20	
WebCode - Test	**Response**
TCA8P9-5561	kittehs
TDLF3U-5561	v:\kittehs\
TFMD29-5561	V:\kittehs
TMAWNW-5561	[Participant did not return results for this question.]
U298Q9-5561	Kittehs
U964DC-5562	kittehs
UWTR4N-5561	\kittehs\
V23CK9-5561	V:\kittehs
V96U7R-5561	V:kittehs
VFHDED-5561	V:\kittehs
WHMDWP-5561	kittehs
WLLU9J-5561	Kittehs
WRR3GT-5561	kittehs
WW4B2Q-5561	V:\kittehs\
X436QC-5562	kittehs
X4L22Q-5562	V:\kittehs
XCDUFN-5561	kittehs
XHHHQN-5561	V:\kittehs\
XUR36B-5561	kittehs
Y2ANWU-5561	-Unanswered-
YQTYXP-5561	kittehs
YXADZU-5561	kittehs
YYKJVA-5561	kittehs
ZGHWCN-5561	V:\kittehs\

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20

WebCode - Test	Response
ZM6UW6-5561	Kittehs
ZTBFTE-5561	V:\kittehs\

Question 20: What directory containing photos did the user access on the mounted volume referenced in Question 19?

Consensus Result:
V:\kittehs\

Expected Response Explanation:
Records of file access through Windows Explorer are recorded in C:\Users\susie\AppData\Local\Microsoft\Windows\WebCache\Internet Explorer (Windows)\History\Daily\WebCacheV01.dat and can be viewed with any tool capable of parsing that file.

Expected Response Illustration:

EnCase view of Internet History

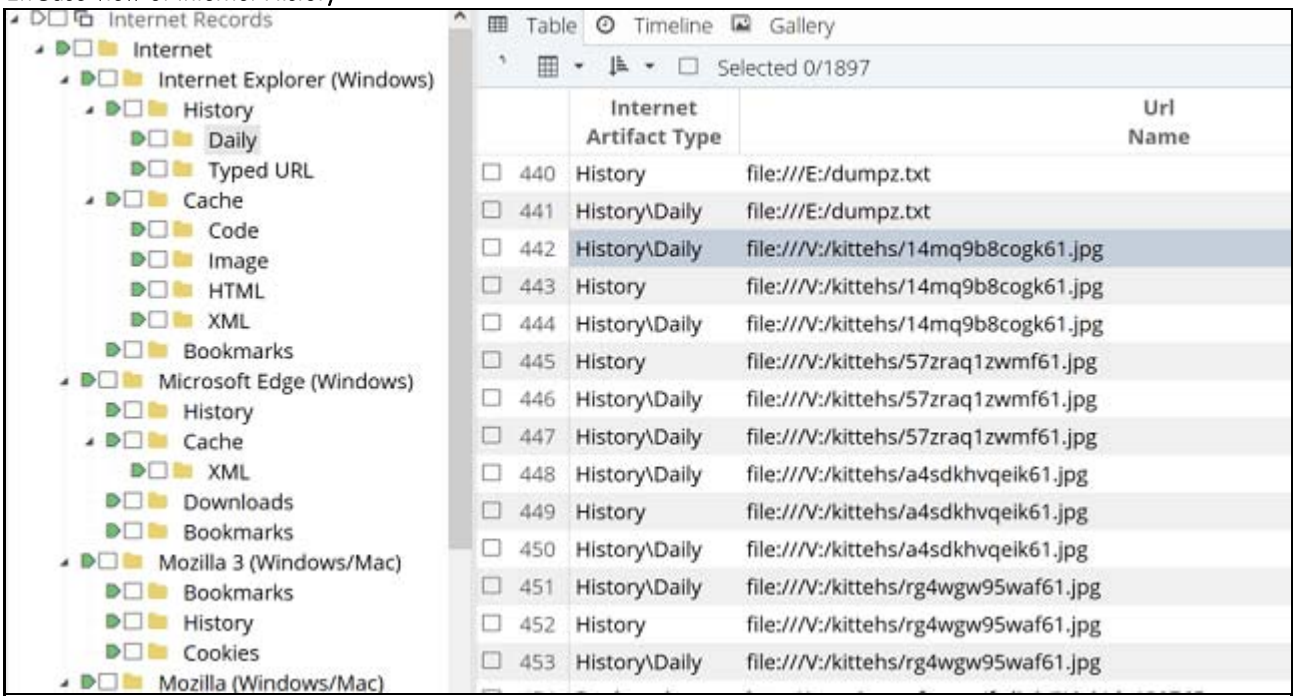


TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21

Question 21: From what volume serial number was the encryption program referenced in question #18 executed?

Manufacturer's Expected Response:

4a0c3885 and/or f617480a

WebCode - Test	Response ** Inconsistencies not highlighted; No consensus achieved **
23UJ67-5561	8E233CC8
29JUMG-5562	4A0C-3885
2YBWJR-5562	0x4A0C3885
3B7V4P-5561	01d712f80aa59b38-4a0c3885
3RC2CZ-5561	The volume serial number of the Veracrypt mounted volume or the V drive is 8E233CC8.
44372B-5561	8E233CC8
4A86BF-5561	4A0C3885
4UEFFJ-5561	8E233CC8
66CHBZ-5561	2384673992
67H6N6-5562	4A0C3885
6G29KN-5562	4a0c3885
6LBUJ2-5561	4A0C-3885
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	C333856D-7D23-11EB-80E9-08002732DC0F
6ZD7FZ-5561	4A0C3885
7A2A6E-5561	4A0C3885
7FMAEZ-5562	4A0C-3885
7W9P7F-5562	2384673992
89LGKW-5561	D:\VeraCrypt
89NM2E-5561	8E233CC8
8UH9ME-5562	4A0C3885
8YVWFY-5561	4A0C3885
93AL3L-5562	4A0C3885

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21

WebCode - Test	Response ** Inconsistencies not highlighted; No consensus achieved **
9ARR2D-5561	[Participant did not return results for this question.]
9GULT8-5562	8E233CC8
9V6AXV-5561	F617-480A
A8KGFG-5561	0A4817F6
AK9F96-5561	4A0C-3885
AQYVXC-5562	F617480A
AV4RGC-5562	4A0C3885
BGJGLT-5561	c33383fd-7d23-11eb-80e9-08002732dc0f
BKPYQG-5561	RegistryValue SIGN.MEDIA=D596882 VeraCrypt\VeraCrypt-x64.exe: File Path: D:\VeraCrypt\VeraCrypt-x64.exe DMIO:ID:$Õ»àÙ@ $ºþÃ9à
BMT8ZD-5561	4A0C-3885
BR6KUT-5562	8E23-3CC8
BWZC2P-5561	4A0C-3885
CBTGPD-5562	4A0C3885
CMHKPW-5561	4A0C-3885
CPRZ8G-5561	4A0C3885
CQ9KB9-5562	8E233CC8
CQJQ7N-5561	Volume serial number that the encryption program referenced in Question 18 executed – F617-480A
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	4A0C3885
E43HU2-5561	4A0C-3885
E7BXK2-5561	4A0C3885
EELYM9-5561	4A0C3885
F2UYKR-5561	file not found
FFG39B-5562	4A0C3885

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21

WebCode - Test	Response ** Inconsistencies not highlighted; No consensus achieved **
FJWWP9-5562	6&1526ad36&0&_&0
FP3BPR-5562	The VSN of the volume where VeraCrypt was executed from was 4A 0C 38 85
FTFDBN-5561	1242314885
G9A37K-5561	8E233CC8
GGKE74-5561	4A0C3885
GU9W29-5561	01d712f80aa59b38-4a0c3885
GZY7B8-5561	4A0C3885
H949ZJ-5561	8E233CC8
HEBY4P-5561	F617-480A
HYFCYH-5561	8E23-3CC8
J3U2M6-5561	4A0C3885
J3XR9B-5561	RegistryValue SIGN.MEDIA=D596882 VeraCrypt\VeraCrypt-x64.exe: File Path: D:\VeraCrypt\VeraCrypt-x64.exe DMIO:ID:$Õ»àÙ@$ºþÃ9à
JF4GTB-5562	4A0C3885
JJJA4W-5562	4A0C3885
JMJLZW-5561	8E233CC8
JU4NYL-5561	0A4817F6 (01d70660173e4f97-f617480a) (C:\)
K6Z7V8-5562	4a0c3885
KE3C4M-5561	3A13-1D02
KH3MYM-5562	F617480A
KT78B9-5562	VeraCrypt 4a0c3885, Kleopatra f617480a
KW3EPY-5561	4A0C3885
L9D7RX-5562	01d712f80aa59b38-4a0c3885
LCV3Z2-5561	4A0C-3885
LEERBL-5562	5&12c8f4c0&0&2

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21	
WebCode - Test	**Response** ** Inconsistencies not highlighted; No consensus achieved **
LPY8P3-5561	#{c333856d-7d23-11eb-80e9-08002732dc0f}
LRRLAT-5562	4a0c3885 (Matches VSN for 21-5562)
LXXGTT-5561	c33383fd-7d23-11eb-80e9-08002732dc0f
M98EB2-5562	4A0C3885
MWHHA4-5562	4A0C3885
MYJKY6-5562	8E233CC8
N66VNU-5561	4A0C-3885 is the serial number of the D: when D:\VeraCrypt\VeraCrypt-x64.exe was executed. (Also, the volume serial number of the encrypted drive V: was 8E23-3CC8)
NFQ2KX-5562	4A0C-3885
NPAH8D-5561	2384673992 for volume V. 4A0C3885 for volume D.
NRJXPX-5561	8E23-3CC8
NTAT4D-5561	Based on the fact that a new Volume Serial Number is created by Windows each time the device is formatted and the dates of use, the device had a Volume Serial Number of the D:\ volume is 4A0C3885.
NUKNP6-5562	4A0C-3885
PBBNHP-5561	c333856d-7d23-11eb-80e9-08002732dc0f
PBQMFZ-5561	GPG from Volume SN: f617480a Veracrypt from Volume: 4a0c3885 \VOLUME{01d70660173e4f97-f617480a}\PROGRAM FILES (X86)\GNUPG\BIN\GPG.EXE \VOLUME{01d712f80aa59b38-4a0c3885}\VERACRYPT\VERACRYPT-X64.EXE
PTA4GV-5562	4A0C-3885
QP2MPV-5561	Veracrypt: 4A0C3885 gpg: F617480A
R36ZB9-5561	4a0c 3885
RAQR4V-5562	4A0C3885
RFUVTT-5561	4A0C3885
RGQL4V-5561	Gpg.exe was executed from volume s/n F617480A Veracrypt-X64.exe was executed from volume s/n 4A0C3885
RK6QRB-5561	8E233CC8
RXCADP-5561	f617480a (reported similar to #3)
T8F7TZ-5562	4A0C3885

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21

WebCode - Test	Response ** Inconsistencies not highlighted; No consensus achieved **
TCA8P9-5561	4A0C3885
TDLF3U-5561	#{c333856d-7d23-11eb-80e9-08002732dc0f}
TFMD29-5561	c33383fd-7d23-11eb-80e9-08002732dc0f
TMAWNW-5561	[Participant did not return results for this question.]
U298Q9-5561	8E233CC8
U964DC-5562	4A0C-3885
UWTR4N-5561	4A0C3885
V23CK9-5561	4A0C3885
V96U7R-5561	#c333856d-7d23-11eb-80e9-08002732dc0f
VFHDED-5561	{08721f5d-7a47-11eb-80e7-08002732dc0f}
WHMDWP-5561	4A0C3885
WLLU9J-5561	4a0c3885
WRR3GT-5561	4A 0C 38 85 (Veracrypt) F6 17 48 0A (GPG)
WW4B2Q-5561	8E233CC8
X436QC-5562	4A0C3885
X4L22Q-5562	8E233CC8
XCDUFN-5561	4A0C3885
XHHHQN-5561	4a0c3885
XUR36B-5561	4A0C3885
Y2ANWU-5561	01d712f80aa59b38-4a0c3885
YQTYXP-5561	8E233CC8
YXADZU-5561	4A0C3885
YYKJVA-5561	4A0C3885
ZGHWCN-5561	8E233CC8

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21

WebCode - Test	Response	** Inconsistencies not highlighted; No consensus achieved **
ZM6UW6-5561	4A0C-3885	
ZTBFTE-5561	4A0C3885	

Question 21: From what volume serial number was the encryption program referenced in question #18 executed?

Consensus Result:

A consensus for this question was not achieved. The objective of the question was for the examiner to identify the volume serial number where VeraCrypt was executed from. Only 61% of participants reported the expected response of "4A0C3885" or "F617480A". Another 18% of participants reported "8E233CC8", the serial number for the volume mounted by Veracrypt and 7% reported "33383fd-7d23-11eb-80e9-08002732dc0f" the guid for the volume mounted by Veracrypt.

Expected Response Explanation:

Program execution details can be recovered from the related Window Prefetch file, in this case, C:\Windows\Prefetch\VERACRYPT-X64.EXE-828FFF6B.pf and parsed with a tool like EnCase Prefetch Parser or Prefetch Explorer (PECmd.exe).

Expected Response Illustration:

PECmd view of VERACRYPT-X64.EXE-828FFF6B.pf

```
005: \VOLUME{01d70660173e4f97-f617480a}\WINDOWS\APPPATCH\SYSMAIN.SDB
006: \VOLUME{01d712f80aa59b38-4a0c3885}\VERACRYPT\VERACRYPT-X64.EXE
007: \VOLUME{01d70660173e4f97-f617480a}\WINDOWS\SYSTEM32\USER32.DLL
```

EnCase PFDump EnScript view of VERACRYPT-X64.EXE-828FFF6B.pf

PECmd view of GPG.EXE-6065ABF5.pf

```
007: \VOLUME{01d70660173e4f97-f617480a}\WINDOWS\SYSWOW64\NTDLL.DLL
008: \VOLUME{01d70660173e4f97-f617480a}\PROGRAM FILES (X86)\GNUPG\BIN\GPG.EXE
009: \VOLUME{01d70660173e4f97-f617480a}\WINDOWS\SYSWOW64\KERNELBASE.DLL
```

KLEOPATRA.EXE-86D5E0B1.pf

```
007: \VOLUME{01d70660173e4f97-f617480a}\WINDOWS\SYSWOW64\NTDLL.DLL
008: \VOLUME{01d70660173e4f97-f617480a}\PROGRAM FILES (X86)\GPG4WIN\BIN\KLEOPATRA.EXE
009: \VOLUME{01d70660173e4f97-f617480a}\WINDOWS\SYSWOW64\KERNELBASE.DLL
```


TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22

Question 22: When did the user LAST login to the user's account (account referenced in questions: #8, #9)? Provide your response in UTC + 00:00 using the following format: MM/DD/YYYY HH:MM:SS AM/PM

Manufacturer's Expected Response:
03/10/2021 02:38:42 AM

WebCode - Test	Response
23UJ67-5561	03/10/2021 02:38:42 AM
29JUMG-5562	03/10/2021 02:38:42 AM
2YBWJR-5562	03/10/2021 02:38:42 AM
3B7V4P-5561	03/10/2021 02:38:42 AM
3RC2CZ-5561	The last login by user account susie was on 03/10/2021 02:38:42 AM UTC.
44372B-5561	03/10/2021 02:38:42 AM
4A86BF-5561	03/10/2021 02:38:42 AM
4UEFFJ-5561	Last Login: 03/10/2021 02:38:42 AM
66CHBZ-5561	03/10/2021 02:38:42 AM UTC
67H6N6-5562	03/10/2021 02:38:42 AM
6G29KN-5562	03/10/2021 02:38:42 AM
6LBUJ2-5561	03/10/2021 02:38:42 AM
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	03/10/2021 02:38:42 AM
6ZD7FZ-5561	3/10/2021 02:38:42 AM
7A2A6E-5561	03/10/2021 02:38:42 AM
7FMAEZ-5562	03/10/2021 02:38:42 AM
7W9P7F-5562	03/10/2021 02:38:42 AM
89LGKW-5561	03/10/2021 02:38:42 AM
89NM2E-5561	03/10/2021 02:38:42 AM
8UH9ME-5562	03/10/2021 02:38:42 AM
8YVWFY-5561	03/10/2021 02:38:42 AM (10th March 2021 - 02:38:42)

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22

WebCode - Test	Response
93AL3L-5562	3/10/2021 2:38:42 AM
9ARR2D-5561	03/10/2021 02:38:42 AM
9GULT8-5562	03/10/2021 02:38:42 AM
9V6AXV-5561	3/10/2021 2:38:42 AM
A8KGFG-5561	10/03/2021 02:38:42 AM
AK9F96-5561	03/10/2021 02:38:42 AM
AQYVXC-5562	10/03/2021 02:38:42 +0 AM, (or US Format: 03/10/2021 02:38:42 +0 AM)
AV4RGC-5562	03.10.2021 02:38:42 AM
BGJGLT-5561	03/10/2021 02:38:42 AM
BKPYQG-5561	03/10/2021 2:38:42 AM
BMT8ZD-5561	03/10/2021 02:38:42 AM
BR6KUT-5562	03/10/2021 02:38:42 AM
BWZC2P-5561	03/10/2021 02:38:42 UTC
CBTGPD-5562	03/10/2021 02:38:42 AM
CMHKPW-5561	03/10/2021 02:38:42 AM
CPRZ8G-5561	3/10/2021 2:38:42 AM
CQ9KB9-5562	03/10/2021 02:38:42 AM
CQJQ7N-5561	Last login to the user's account (referenced in Questions 8 & 9) – 03/10/2021 02:38:42 AM (02:38:42) UTC
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	03/10/2021 02:38:42 AM
E43HU2-5561	03/10/2021 02:38:42 AM
E7BXK2-5561	03/10/2021 02:38:42 AM
EELYM9-5561	03/10/2021 02:38:42 AM
F2UYKR-5561	The last login was on 03/04/2021 12:06:54 AM.

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22

WebCode - Test	Response
FFG39B-5562	03/10/2021 02:38:42 AM
FJWWP9-5562	03/10/2021 02:38:42 AM
FP3BPR-5562	The user last logged into the 'susie' user account on 03-10-2021 02:38:42 AM UTC+ 00:00
FTFDBN-5561	03/10/2021 02:38:42 AM
G9A37K-5561	03/10/2021 02:38:42 AM
GGKE74-5561	03/10/2021 02:38:42 AM
GU9W29-5561	03/10/2021 02:38 AM
GZY7B8-5561	3/10/2021/ 2:38:42 AM
H949ZJ-5561	03/10/2021 2:38:42 UTC
HEBY4P-5561	03/10/2021 02:38:42 AM
HYFCYH-5561	03/10/2021 2:38:42 AM
J3U2M6-5561	3/10/2021 2:38:42 AM
J3XR9B-5561	03/10/2021 2:38:42 AM
JF4GTB-5562	03/10/2021 02:38:42 AM
JJJA4W-5562	03/10/2021 02:38:42 AM
JMJLZW-5561	03/10/2021 02:38:42 AM
JU4NYL-5561	03/10/2021 02:38:42 AM (10th March 2021 - 02:38:42)
K6Z7V8-5562	03/10/2021 02:38:42 AM
KE3C4M-5561	03/10/2021 02:38:42 AM
KH3MYM-5562	03/10/2021 02:38:42 AM
KT78B9-5562	03/10/2021 02:38:42 AM
KW3EPY-5561	03/10/2021 02:38:42 AM
L9D7RX-5562	03/10/2021 02:43:10 AM
LCV3Z2-5561	03/10/2021 02:38:42 AM UTC + 00:00

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22	
WebCode - Test	**Response**
LEERBL-5562	03/10/2021 01:38:42 AM
LPY8P3-5561	03/10/2021 02:38:42 AM
LRRLAT-5562	03/10/2021 02:38:42 AM
LXXGTT-5561	03/10/2021 02:38:42 AM
M98EB2-5562	03/10/2021 02:38:42 am
MWHHA4-5562	03/10/2021 02:38:42 AM
MYJKY6-5562	03/10/2021 02:38:42 AM
N66VNU-5561	03/10/2021 02:38:42 AM
NFQ2KX-5562	03.10.2021 02:38:42 AM
NPAH8D-5561	03/10/2021 02:38:42
NRJXPX-5561	03/10/2021 02:38:42 AM
NTAT4D-5561	03/10/2021 02:38:42 UTC = 03/10/2021 02:38:42 AM
NUKNP6-5562	03/10/2021 01:38:42 AM
PBBNHP-5561	03/10/2021 02:38:42 AM
PBQMFZ-5561	User Susie last logged in: 03/10/2021 02:38:42 AM
PTA4GV-5562	03/10/2021 2:38:42 AM
QP2MPV-5561	03/10/2021 02:38:42 AM
R36ZB9-5561	03/10/2021 02:38:42 AM
RAQR4V-5562	03/10/2021 02:38:42 AM
RFUVTT-5561	03/10/2021 02:38:42 AM
RGQL4V-5561	03/10/2021 02:38:42 AM
RK6QRB-5561	3/10/2021 02:38:42 AM
RXCADP-5561	03/10/2021 02:38:42 AM
T8F7TZ-5562	03/10/2021 02:38:42 AM

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22	
WebCode - Test	**Response**
TCA8P9-5561	3/10/2021 02:38:42 AM
TDLF3U-5561	03/10/2021 02:38:42 AM
TFMD29-5561	03/10/2021 02:38:42 AM
TMAWNW-5561	03.10.2021 02.38.42 AM
U298Q9-5561	03/10/2021 02:38 AM
U964DC-5562	03/10/2021 02:38:42 AM
UWTR4N-5561	03/10/2021 02:38:42 AM
V23CK9-5561	03/10/2021 02:38:42 AM
V96U7R-5561	03/10/2021 02:38:42 AM
VFHDED-5561	03/10/2021 02:38:42 AM
WHMDWP-5561	03/10/2021 02:38:42 AM
WLLU9J-5561	03/10/2021 02:38:42 AM UTC
WRR3GT-5561	03/10/2021 02:38:42 AM
WW4B2Q-5561	03/10/2021 02:38:42 AM
X436QC-5562	03/10/2021 02:38:42 AM
X4L22Q-5562	3/10/2021 02:38:42 AM
XCDUFN-5561	03/10/2021 02:38:42 AM
XHHHQN-5561	03/10/2021 02:38:42 AM
XUR36B-5561	03/10/2021 02:38:42 AM
Y2ANWU-5561	03/10/2021 02:38:42 AM
YQTYXP-5561	03/10/21 02:38:42 UTC
YXADZU-5561	03/10/2021 02:38:42 AM
YYKJVA-5561	03/10/2021 02:38:42 AM
ZGHWCN-5561	3/10/2021 02:38:42 AM

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22	
WebCode - Test	**Response**
ZM6UW6-5561	03/10/2021 02:38:42 AM
ZTBFTE-5561	03/10/2021 02:38:42 AM

Question 22: When did the user LAST login to the user's account (account referenced in questions: #8, #9)? Provide your response in UTC + 00:00 using the following format: MM/DD/YYYY HH:MM:SS AM/PM

Consensus Result:

03/10/2021 02:38:42 AM and all formatting styles including different time zones which represent the same information.

Expected Response Explanation:

The last login date for a user is recorded in the System Accounts Manager (SAM) registry hive.

Expected Response Illustration:

RegRipper view of SAM hive login data for susie

```
Username        : susie [1001]
Full Name       :
User Comment    :
Account Type    :
Account Created : 2021-02-19 02:03:12Z
Name            :
Last Login Date : 2021-03-10 02:38:42Z
Pwd Reset Date  : 2021-02-19 02:03:18Z
Pwd Fail Date   : 2021-03-08 02:44:16Z
Login Count     : 12
Embedded RID    : 1001
  --> Password does not expire
  --> Password not required
  --> Normal user account
```


TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23

Question 23: How many times was NOTEPAD.EXE executed?

Manufacturer's Expected Response:

Please refer to the section labeled "Consensus Result" for this specific question for more information.

WebCode - Test	Response ** Inconsistencies not highlighted; No consensus achieved **
23UJ67-5561	3
29JUMG-5562	8
2YBWJR-5562	The [Laboratory] does not include this information on the report and is outside the scope of our normal reporting procedures
3B7V4P-5561	8
3RC2CZ-5561	NOTEPAD.EXE was executed 3 times.
44372B-5561	14
4A86BF-5561	14
4UEFFJ-5561	3 times
66CHBZ-5561	14
67H6N6-5562	6
6G29KN-5562	This question is outside the scope of a normal examination and would not be reported under normal circumstances.
6LBUJ2-5561	14
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	5
6ZD7FZ-5561	3
7A2A6E-5561	15
7FMAEZ-5562	14
7W9P7F-5562	6
89LGKW-5561	3
89NM2E-5561	8
8UH9ME-5562	8
8YVWFY-5561	14 - by user susie. NTUSER.DAT
93AL3L-5562	[Participant did not return results for this question.]

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23

WebCode - Test	Response ** Inconsistencies not highlighted; No consensus achieved **
9ARR2D-5561	8
9GULT8-5562	14
9V6AXV-5561	3
A8KGFG-5561	8
AK9F96-5561	8
AQYVXC-5562	Application Run Count: 14 Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count
AV4RGC-5562	8
BGJGLT-5561	3
BKPYQG-5561	14
BMT8ZD-5561	8
BR6KUT-5562	14
BWZC2P-5561	3
CBTGPD-5562	8
CMHKPW-5561	8
CPRZ8G-5561	8
CQ9KB9-5562	14
CQJQ7N-5561	NOTEPAD.EXE was executed – 5 times
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	8 times
E43HU2-5561	8
E7BXK2-5561	14
EELYM9-5561	14
F2UYKR-5561	It was executed 8 times.
FFG39B-5562	3

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23

WebCode - Test	Response ** Inconsistencies not highlighted; No consensus achieved **
FJWWP9-5562	14
FP3BPR-5562	Notepad.exe has been ran 3 times
FTFDBN-5561	3
G9A37K-5561	NOTEPAD.EXE was executed at least 8 times. Exact execution count cannot be determined, as each artifact recorded a different number of executions with varying/overlapping date/times (UserAssist shows 14, while prefetch recorded 8, for example). The 8 confirmed executions were determined by creating a timeline of the dates/times recorded by seperate program execution artifacts. This timeline found 8 consistent execution records.
GGKE74-5561	15
GU9W29-5561	15
GZY7B8-5561	14
H949ZJ-5561	3
HEBY4P-5561	14
HYFCYH-5561	8
J3U2M6-5561	14
J3XR9B-5561	14
JF4GTB-5562	14
JJJA4W-5562	14
JMJLZW-5561	14
JU4NYL-5561	14
K6Z7V8-5562	14
KE3C4M-5561	14
KH3MYM-5562	3
KT78B9-5562	14
KW3EPY-5561	8
L9D7RX-5562	14
LCV3Z2-5561	14 (not sufficiently trained to answer conclusively - 8 in Prefetch, 14 in UserAssist)

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23

WebCode - Test	Response ** Inconsistencies not highlighted; No consensus achieved **
LEERBL-5562	14
LPY8P3-5561	8
LRRLAT-5562	3
LXXGTT-5561	8
M98EB2-5562	Userassist states 14 times, Prefetch says 8 times
MWHHA4-5562	14
MYJKY6-5562	8
N66VNU-5561	Three
NFQ2KX-5562	14
NPAH8D-5561	From checking Prefetch files, it was opened 3 times. From checking User Assist, it was opened 14 times.
NRJXPX-5561	14
NTAT4D-5561	A review of the Prefetech artifacts indicates that the Notepad program was run three (3) times. A review of the Link (LNK) files indicates that six (6) different files were opened with the Notepad program, which is supported by the UserAssist artifacts. The UserAssist artifacts, which are user specific, also indicates that the Notepad program was run a total of fourteen (14) times.
NUKNP6-5562	8
PBBNHP-5561	8
PBQMFZ-5561	It appears it was executed 14 Times. The User Assist shows it was executed 14 times, with a last run date that matches the last run timestamp from the prefetch file. The Prefetch file shows an execution of 8 times
PTA4GV-5562	14
QP2MPV-5561	14
R36ZB9-5561	Three
RAQR4V-5562	8
RFUVTT-5561	Three (3)
RGQL4V-5561	14
RK6QRB-5561	3
RXCADP-5561	8

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23

WebCode - Test	Response ** Inconsistencies not highlighted; No consensus achieved **
T8F7TZ-5562	Three (3)
TCA8P9-5561	3 times (based on Prefetch file)
TDLF3U-5561	8
TFMD29-5561	8
TMAWNW-5561	8
U298Q9-5561	6
U964DC-5562	8
UWTR4N-5561	3
V23CK9-5561	14
V96U7R-5561	8
VFHDED-5561	3
WHMDWP-5561	3
WLLU9J-5561	8
WRR3GT-5561	14
WW4B2Q-5561	8
X436QC-5562	UserAssist records fourteen (14) Prefetch records eight (8)
X4L22Q-5562	14
XCDUFN-5561	14
XHHHQN-5561	8
XUR36B-5561	UserAssist records fourteen (14) executions Windows Prefetch records eight (8) executions
Y2ANWU-5561	3
YQTYXP-5561	14 - 0x0E
YXADZU-5561	8
YYKJVA-5561	6

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23	
WebCode - Test	**Response** ** Inconsistencies not highlighted; No consensus achieved **
ZGHWCN-5561	14
ZM6UW6-5561	3
ZTBFTE-5561	3, based on the run count in Windows prefetch.

Question 23: How many times was NOTEPAD.EXE executed?

Consensus Result:

Based on the inconsistency found in certain artifacts, this question was determined to be of little value for this dataset. No expected response is being provided.

Expected Response Explanation:

Participants' results have been presented, however due to inconsistencies with certain artifacts, no expected response nor discussion on achieving that response is being provided.

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24

Question 24: What is the original (pre-deletion) path and name of $I9JOSIO.jpg (found in the user's Recycle Bin)?

Manufacturer's Expected Response:

C:\Users\susie\Documents\004854.jpg

WebCode - Test	Response
23UJ67-5561	C:\Users\susie\Documents\004854.jpg
29JUMG-5562	C:\Users\susie\Documents\004854.jpg
2YBWJR-5562	\users\susie\Documents\004854.jpg
3B7V4P-5561	C:\Users\susie\Documents\004854.jpg
3RC2CZ-5561	The original name of $I9JOSIO.jpg is 004854.jpg. The original file path is C:\Users\susie\Documents\004854.jpg.
44372B-5561	C:\Users\susie\Documents\004854.jpg
4A86BF-5561	C:\Users\susie\Documents\004854.jpg
4UEFFJ-5561	original (pre-deletion) path and CS: C:\Users\susie\Documents\004854.jpg
66CHBZ-5561	$I9JOSIO was originally named 004854.jpg and original path was C:\Users\susie\Documents\004854.jpg
67H6N6-5562	C:\Users\susie\Documents\004854.jpg
6G29KN-5562	C:\Users\susie\Documents\004854.jpg
6LBUJ2-5561	C:\Users\susie\Documents\004854.jpg
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	C:\Users\susie\Documents\004854.jpg
6ZD7FZ-5561	C:\Users\susie\Documents\004854.jpg
7A2A6E-5561	C:\Users\susie\Documents\004854.jpg
7FMAEZ-5562	C:\Users\susie\Documents and 004854.jpg
7W9P7F-5562	C:\Users\susie\Documents\004854.jpg
89LGKW-5561	Original Path C:\Users\susie\Documents\004854.jpg File Name: 004854.jpg Cryptic Name: $R9JOSIO.jpg
89NM2E-5561	C:\Users\susie\Documents\004854.jpg
8UH9ME-5562	C:\Users\susie\Documents\004854.jpg
8YVWFY-5561	C:\Users\susie\Documents\004854.jpg

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24

WebCode - Test	Response
93AL3L-5562	C:\Users\susie\Documents\004854.jpg
9ARR2D-5561	C:\Users\susie\Documents
9GULT8-5562	C:\Users\susie\Documents\004854.jpg
9V6AXV-5561	C:\Users\susie\Documents\004854.jpg
A8KGFG-5561	filepath: C:\Users\susie\Documents filename: 004854.jpg
AK9F96-5561	C:\Users\susie\Documents\004854.jpg
AQYVXC-5562	\Users\susie\Documents\004854.jpg
AV4RGC-5562	C:\Users\susie\Documents\004854.jpg
BGJGLT-5561	C:\users\susie\documents\004854.jpg
BKPYQG-5561	C:\Users\susie\Documents\004854.jpg
BMT8ZD-5561	C:\Users\susie\Documents\004854.jpg
BR6KUT-5562	C:\Users\susie\Documents\004854.jpg
BWZC2P-5561	C:\Users\susie\Documents\004854.jpg
CBTGPD-5562	C:\Users\susie\Documents\004854.jpg
CMHKPW-5561	C:\Users\susie\Documents\004854.jpg
CPRZ8G-5561	C:\Users\susie\Documents\004854.jpg
CQ9KB9-5562	Name - 004854.jpg Original Path - C:\Users\susie\Documents
CQJQ7N-5561	Original (pre-deletion) path and name of "$19JOSIO.jpg" (found in the user's Recycle Bin) – Path \Users\susie\Documents\004854.jpg / File name "004854.jpg"
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	\Users\susie\Documents\004854.jpg
E43HU2-5561	C:\Users\susie\Documents\004854.jpg
E7BXK2-5561	C:\Users\susie\Documents\004854.jpg
EELYM9-5561	C:\Users\susie\Documents\004854.jpg
F2UYKR-5561	Name of the file was 004854.jpg and the original path was C:\users\susie\Documents

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24	
WebCode - Test	**Response**
FFG39B-5562	C:\Users\susie\Documents\004854.jpg
FJWWP9-5562	C:\Users\susie\Documents\004854.jpg
FP3BPR-5562	C:\Users\susie\Documents. The original file name was 004854.jpg
FTFDBN-5561	C:\Users\susie\Documents\004854.jpg
G9A37K-5561	C:\Users\susie\Documents\004854.jpg
GGKE74-5561	C:\Users\susie\Documents\004854.jpg
GU9W29-5561	C:\Users\susie\Documents\004854.jpg
GZY7B8-5561	C:\Users\susie\Documents\004854.jpg
H949ZJ-5561	C:\Users\susie\Documents\004854.jpg
HEBY4P-5561	C:\Users\susie\Documents\004854.jpg
HYFCYH-5561	C:\Users\susie\Documents\004854.jpg
J3U2M6-5561	C:\Users\susie\Documents\004854.jpg
J3XR9B-5561	C:\Users\susie\Documents\004854.jpg
JF4GTB-5562	C:\Users\susie\Documents\004854.jpg
JJJA4W-5562	C:\Users\susie\Documents\004854.jpg
JMJLZW-5561	C:\users\susie\Documents\004854.jpg
JU4NYL-5561	\Users\susie\Documents\004854.jpg
K6Z7V8-5562	C:\Users\susie\Documents\004854.jpg
KE3C4M-5561	004854.jpg C:\Users\susie\Documents\004854.jpg
KH3MYM-5562	C:\Users\susie\Documents\004854.jpg
KT78B9-5562	C:\Users\susie\Documents\004854.jpg
KW3EPY-5561	C:\Users\susie\Documents\004854.jpg
L9D7RX-5562	C:\Users\susie\Documents\004854.jpg
LCV3Z2-5561	C:\Users\susie\Documents\004854.jpg

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24	
WebCode - Test	**Response**
LEERBL-5562	C:\Users\Susie\Documents\004854.jpg
LPY8P3-5561	C:\Users\susie\Documents\004854.jpg
LRRLAT-5562	C:\Users\susie\Documents\004854.jpg
LXXGTT-5561	C:\Users\susie\Documents\004854.jpg
M98EB2-5562	C:\Users\susie\Documents\004854.jpg, 004854.jpg
MWHHA4-5562	C:\Users\susie\Documents\004854.jpg
MYJKY6-5562	C:\Users\susie\Documents 004854.jpg
N66VNU-5561	C:\Users\susie\Documents\004854.jpg
NFQ2KX-5562	C:\Users\susie\Documents\004854.jpg
NPAH8D-5561	C:\Users\susie\Documents\004854.jpg
NRJXPX-5561	C:\Users\susie\Documents\004854.jpg
NTAT4D-5561	C:\Users\susie\Documents\004854.jpg
NUKNP6-5562	004854.jpg C:\Users\susie\Documents\
PBBNHP-5561	C:\Users\susie\Documents\004854.jpg
PBQMFZ-5561	C:\Users\susie\Documents\ File Name: 004854.jpg
PTA4GV-5562	Path: C:\Users\susie\Documents\004854.jpg Name: 004854.jpg
QP2MPV-5561	C:\Users\susie\Documents\004854.jpg
R36ZB9-5561	C:\Users\susie\Documents\004854.jpg
RAQR4V-5562	C:\Users\susie\Documents\004854.jpg
RFUVTT-5561	Users\susie\Documents\004854.jpg
RGQL4V-5561	\Users\susie\Documents\004854.jpg
RK6QRB-5561	C:\Users\susie\Documents\004854.jpg
RXCADP-5561	C:\Users\susie\Documents\004854.jpg
T8F7TZ-5562	Users\susie\Documents\004854.jpg

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24

WebCode - Test	Response
TCA8P9-5561	File Path: C:\Users\susie\Documents\004854.jpg File Name: 004854
TDLF3U-5561	Users/susie/Documents/004854.jpg
TFMD29-5561	C:\Users\susie\Documents\004854.jpg
TMAWNW-5561	Path: C:\Users\susie\Documents\ Name: 004854.jpg
U298Q9-5561	C:\Users\susie\Documents\004854.jpg
U964DC-5562	C\Users\susie\Documents\004854.jpg - Filename - 004854.jpg
UWTR4N-5561	C:\Users\susie\Documents\004854.jpg
V23CK9-5561	c:\Users\susie\Documents\004854.jpg
V96U7R-5561	c:\Users\susie\Documents\004854.jpg
VFHDED-5561	C:\Users\susie\Documents\004854.jpg
WHMDWP-5561	The original (pre-deletion) path : C:\Users\susie\Documents\004854.jpg The original (pre-deletion) name : 004854.jpg
WLLU9J-5561	\Users\susie\Documents\004854.jpg
WRR3GT-5561	C:\Users\susie\Documents\004854.jpg
WW4B2Q-5561	C:\Users\susie\Documents\004854.jpg
X436QC-5562	C:\Users\susie\Documents\004854.jpg
X4L22Q-5562	\Users\susie\Documents\004854.jpg
XCDUFN-5561	C:\Users\susie\Documents\004854.jpg
XHHHQN-5561	C:\Users\susie\Documents\004854.jpg
XUR36B-5561	C:\Users\susie\Documents\004854.jpg
Y2ANWU-5561	004854.jpg
YQTYXP-5561	c:\Users\susie\Douments\004854.jpg
YXADZU-5561	C:\Users\susie\Documents\004854.jpg
YYKJVA-5561	C:\Users\susie\Documents\004854.jpg
ZGHWCN-5561	C:\Users\susie\Documents\004854.jpg

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24	
WebCode - Test	**Response**
ZM6UW6-5561	C:\users\susie\Documents\004854.jpg
ZTBFTE-5561	C:\Users\susie\Documents\004854.jpg

Question 24: What is the original (pre-deletion) path and name of $I9JOSIO.jpg (found in the user's Recycle Bin)?

Consensus Result:

C:\Users\susie\Documents\004854.jpg and all formatting styles which represent the same information.

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 susie's SID is S-1-5-21-1943064195-990424342-2473957490-1001. 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; in this case, however, the recycle bin was emptied after the above file was recycled so there is no corresponding $R file.

Expected Response Illustration:

FTK Imager view of Recycle Bin Files

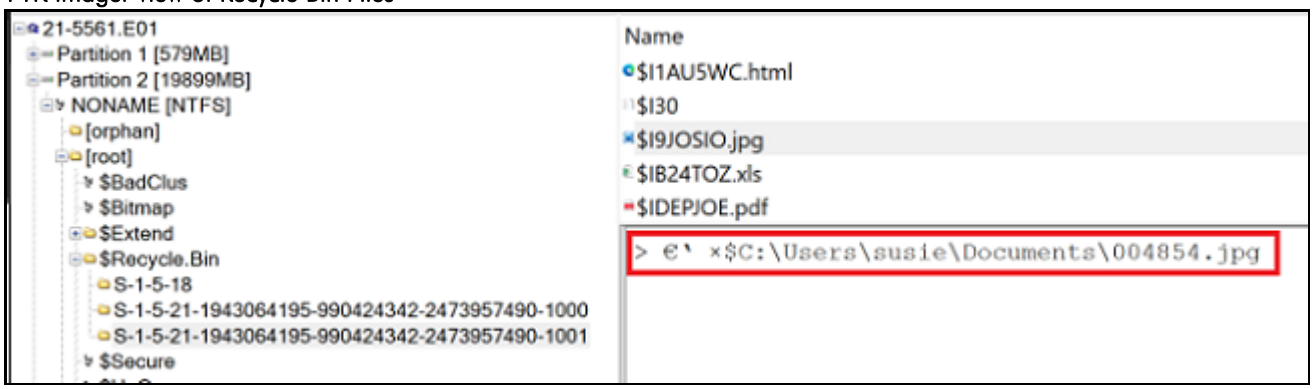


TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25

Question 25: What date and time was the file 004651.pdf deleted? Provide your response in UTC + 00:00 using the following format: MM/DD/YYYYHH:MM:SS AM/PM

Manufacturer's Expected Response:
03/07/2021 03:33:23 AM

WebCode - Test	Response
23UJ67-5561	03/07/2021 03:33:23 AM
29JUMG-5562	03/07/2021 03:33:23 AM
2YBWJR-5562	03/07/2021:03:33:23 AM
3B7V4P-5561	03/07/2021 03:33:23 AM
3RC2CZ-5561	The file was deleted on 03/07/2021 at 03:33:22 AM UTC.
44372B-5561	03/07/2021 03:33:23 AM
4A86BF-5561	03/07/2021 03:33:23 AM
4UEFFJ-5561	3/7/2021 3:33:23 AM
66CHBZ-5561	03/07/2021 04:33:23 AM UTC
67H6N6-5562	03/07/2021 03:18:11 AM
6G29KN-5562	03/07/2021 03:33:23 AM
6LBUJ2-5561	03/07/2021 03:33:23 AM
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	03/07/2021 03:33:23 AM
6ZD7FZ-5561	3/7/2021 3:33:23 AM
7A2A6E-5561	03/07/2021 03:33:23 AM
7FMAEZ-5562	03/07/2021 03:33:23 AM
7W9P7F-5562	03/07/2021 03:33:23 AM
89LGKW-5561	03/07/2021 03:33:23 AM
89NM2E-5561	03/07/2021 03:33:23 AM
8UH9ME-5562	03/07/2021 03:33:23 AM
8YVWFY-5561	03/07/2021 03:33:23 AM (07th March 2021 - 03:33:23)

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25

WebCode - Test	Response
93AL3L-5562	3/7/2021 3:33:23 AM
9ARR2D-5561	03/07/2021 03:33:23 AM
9GULT8-5562	03/07/2021 03:33:23 AM
9V6AXV-5561	3/7/2021 3:33:23 AM
A8KGFG-5561	07/03/2021 03:33:23 AM
AK9F96-5561	03/07/2021 03:33:23 AM
AQYVXC-5562	07/03/2021 03:33:23 +0
AV4RGC-5562	03.07.2021 03:33:23 AM
BGJGLT-5561	03/07/2021 03:33:23 AM
BKPYQG-5561	03/07/2021 3:33:23 AM
BMT8ZD-5561	03/07/2021 03:33:23 AM
BR6KUT-5562	03/07/2021 03:33:23 AM
BWZC2P-5561	03/07/2021 03:33:23 UTC
CBTGPD-5562	03/07/2021 03:33:23 AM
CMHKPW-5561	03/07/2021 3:33:23 AM
CPRZ8G-5561	3/7/2021 3:33:23 AM
CQ9KB9-5562	03/07/2021 03:33:23 AM
CQJQ7N-5561	Date and time file 004651.pdf was deleted – 03/08/2021 11:22:34 PM (23:22:34) UTC
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	03/07/2021 03:33:23 AM
E43HU2-5561	03/07/2021 03:33:23 AM
E7BXK2-5561	03/07/2021 03:33:23 AM
EELYM9-5561	03/7/2021 03:33:23 AM
F2UYKR-5561	The file was deleted on 03/07/2021 12:48:11 AM.

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25	
WebCode - Test	**Response**
FFG39B-5562	03/07/2021 03:33:23 AM
FJWWP9-5562	03/07/2021 03:33:23 AM
FP3BPR-5562	03-07-2021 at 03:33:23 AM UTC +00:00
FTFDBN-5561	03/07/2021 03:33:23 AM
G9A37K-5561	03/07/2021 03:33:23 AM
GGKE74-5561	03/7/2021 03:33:23 AM
GU9W29-5561	03/07/2021 03:33 AM
GZY7B8-5561	3/7/2021 3:33:23 AM
H949ZJ-5561	03/07/2021 03:33:23 UTC
HEBY4P-5561	03/06/2021 10:33:23 PM
HYFCYH-5561	03/07/2021 03:33:23 AM
J3U2M6-5561	3/7/2021 3:33:23 AM
J3XR9B-5561	Sunday, March 7, 2021 at 3:33:23 AM Greenwich Mean Time
JF4GTB-5562	3/7/2021 4:33:23 AM
JJJA4W-5562	03/07/2021 03:33:23
JMJLZW-5561	03-07-2021 03:33:23 AM
JU4NYL-5561	03/07/2021 03:18:11 (7th March 2021 - 03:18:11)
K6Z7V8-5562	03/07/2021 03:33:23 AM
KE3C4M-5561	03/07/2021 03:33:23 AM
KH3MYM-5562	03/07/2021 03:33:23 AM
KT78B9-5562	03/07/2021 03:33:23 AM
KW3EPY-5561	03/07/2021 03:33:23 AM
L9D7RX-5562	03/07/2021 03:33:23 AM
LCV3Z2-5561	03/07/2021 03:33:23 AM UTC + 00:00

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25	
WebCode - Test	**Response**
LEERBL-5562	03/07/2021 02:33:23 AM
LPY8P3-5561	03/07/2021 03:33:23 AM
LRRLAT-5562	03/07/2021 03:33:23 AM
LXXGTT-5561	03/07/2021 03:33:23 AM
M98EB2-5562	03/07/2021 03:33:23 am
MWHHA4-5562	03/07/2021 03:33:23 AM
MYJKY6-5562	03/07/2021 03:33:23 AM
N66VNU-5561	03/07/2021 03:33:23 AM
NFQ2KX-5562	03/07/2021 03:33:23 AM
NPAH8D-5561	03/06/2021 10:33:23 PM 03/07/2021 03:33:23 AM UTC
NRJXPX-5561	03/07/2021 03:33:23 AM
NTAT4D-5561	03/07/2021 03:33:23 UTC = 03/07/2021 03:33:23 AM
NUKNP6-5562	03/07/2021 02:33:23 AM
PBBNHP-5561	03/07/2021 03:33:23 AM
PBQMFZ-5561	3/7/2021 3:33:23 AM
PTA4GV-5562	03/07/2021 03:33:23 AM
QP2MPV-5561	03/07/2021 03:33:23 AM
R36ZB9-5561	03/07/2021 03:33:23 AM
RAQR4V-5562	03/07/2021 03:33:23 AM
RFUVTT-5561	03/07/2021 03:33:23 AM
RGQL4V-5561	03/07/2021 03:33:23 AM
RK6QRB-5561	03/07/2021 03:33:23 AM
RXCADP-5561	03/07/2021 03:33:23 AM
T8F7TZ-5562	03/07/2021 03:33:23 AM

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25	
WebCode - Test	**Response**
TCA8P9-5561	3/7/2021 3:33:23 AM
TDLF3U-5561	03/07/2021 4:33:23 AM
TFMD29-5561	03/07/2021 03:33:23 AM
TMAWNW-5561	7.3.2021 3.33.23 AM
U298Q9-5561	03/07/2021 03:33:23 AM
U964DC-5562	03/07/2021 03:33:23 AM
UWTR4N-5561	03/07/2021 03:33:23 AM
V23CK9-5561	03/07/2021 03:33:23 AM
V96U7R-5561	03/07/2021 03:33:23 AM
VFHDED-5561	03/07/2021 03:33:23 AM
WHMDWP-5561	03/07/2021 03:33:23 AM
WLLU9J-5561	03/07/2021 03:03:36 AM UTC
WRR3GT-5561	03/07/2021 03:33:23 AM
WW4B2Q-5561	03/07/2021 03:33:23 AM
X436QC-5562	03/07/2021 03:33:23 AM
X4L22Q-5562	03/07/2021 03:33:23 AM
XCDUFN-5561	03/07/2021 03:33:23 AM
XHHHQN-5561	03/07/2021 03:33:23 AM
XUR36B-5561	03/07/2021 03:33:23 AM
Y2ANWU-5561	07/03/2021 03:33:23 AM
YQTYXP-5561	03/07/21 03:33:23
YXADZU-5561	03/07/2021 03:33:23 AM
YYKJVA-5561	03/07/2021 03:18:11 AM
ZGHWCN-5561	03/07/2021 03:33:23 AM

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25

WebCode - Test	Response
ZM6UW6-5561	03/07/2021 03:33:23 AM
ZTBFTE-5561	03/07/2021 03:33:23 AM

Question 25: What date and time was the file 004651.pdf deleted? Provide your response in UTC + 00:00 using the following format: MM/DD/YYYYHH:MM:SS AM/PM

Consensus Result:

03/07/2021 03:33:23 AM and all formatting styles including different time zones which represent the same information.

Expected Response Explanation:

The Recycle Bin file containing the metadata for 004651.pdf is $IN2E11F.pdf. The modified and created dates for the corresponding $RN2E11F.pdf file indicate the deletion date.

Expected Response Illustration:

FTK Imager view of Recycle Bin Files

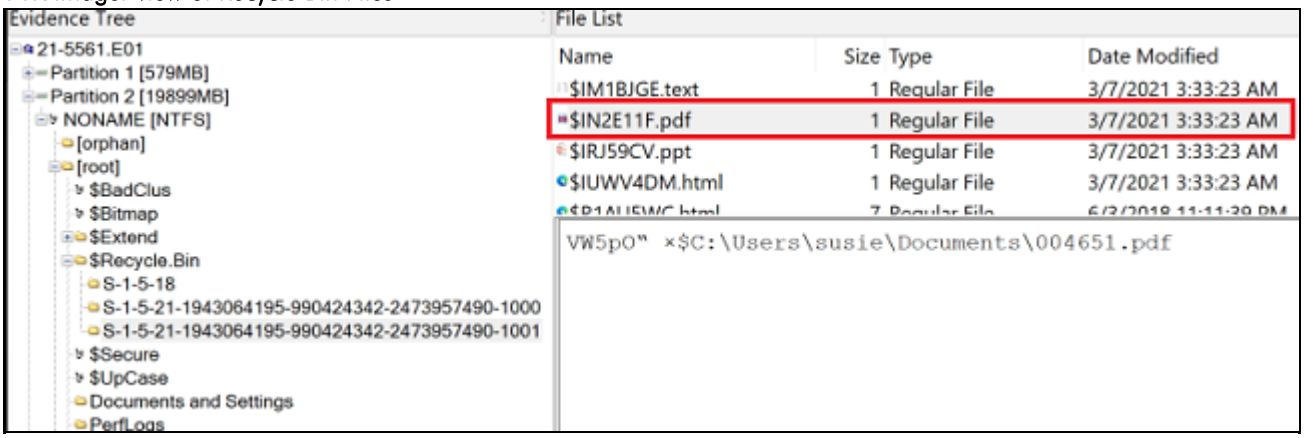


TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26

Question 26: Provide the first six bytes of the file with SHA1 hash 383d4c012ac7c550699c3908c57f7ad00b98ecbe.

Manufacturer's Expected Response:

47 49 46 38 37 61, or GIF87a

WebCode - Test	Response
23UJ67-5561	GIF87a
29JUMG-5562	47 49 46 38 37 61 Computer\D\Users\susie\Documents\000519.gif
2YBWJR-5562	0x47 49 46 38 37 61
3B7V4P-5561	47 49 46 38 37 61
3RC2CZ-5561	The first six bytes of the file are 0x47 49 46 38 37 61
44372B-5561	GIF87a
4A86BF-5561	47 49 46 38 37 61
4UEFFJ-5561	47 49 46 38 37 61
66CHBZ-5561	47 49 46 38 37 61 (Hex), GIF87a (ASCII)
67H6N6-5562	47 49 46 38 37 61(GIF87a)
6G29KN-5562	0x 47 49 46 38 37 61
6LBUJ2-5561	hex:47 49 46 38 37 61, ascii: GIF87a
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	47 49 46
6ZD7FZ-5561	474946383761
7A2A6E-5561	0x47 0x49 0x46 0x38 0x37 0x61
7FMAEZ-5562	47 49 46 38 37 61
7W9P7F-5562	47 49 46 38 37 61
89LGKW-5561	47 49 46 38 37 61
89NM2E-5561	GIF87a
8UH9ME-5562	0x 47 49 46 38 37 61
8YVWFY-5561	GIF87a 47 49 46 38 37 61

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26

WebCode - Test	Response
93AL3L-5562	47 49 46 38 37 61
9ARR2D-5561	47 49 46 38 37 61
9GULT8-5562	474946383761
9V6AXV-5561	47 49 46 38 37 61
A8KGFG-5561	47 49 46 38 37 61
AK9F96-5561	474946383761
AQYVXC-5562	47 49 46 38 37 61, GIF87a
AV4RGC-5562	GIF87a 47 49 46 38 37 61
BGJGLT-5561	47 49 46
BKPYQG-5561	25 50 44 46 2D 31
BMT8ZD-5561	47 49 46 38 37 61
BR6KUT-5562	47 49 46 38 37 61
BWZC2P-5561	47 49 46 38 37 61
CBTGPD-5562	47 49 46 38 37 61
CMHKPW-5561	47 49 46
CPRZ8G-5561	47 49 46 38 37 61
CQ9KB9-5562	47 49 46 38 37 61
CQJQ7N-5561	First six bytes of the file with SHA1 hash 383d4c012ac7c550699c3908c57f7ad00b98ecbe – 47 49 46
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	47 49 46 38 37 61
E43HU2-5561	47 49 46 38 37 61
E7BXK2-5561	0x47 0x49 0x46 0x38 0x37 0x61
EELYM9-5561	47 49 46 38 37 61 GIF87a
F2UYKR-5561	The first six bytes of the file were found to be 47 49 46. Thus, indicating the file is a gif.

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26

WebCode - Test	Response
FFG39B-5562	47 49 46 38 37 61
FJWWP9-5562	47 49 46 38 37 61
FP3BPR-5562	47 49 46 38 37 61
FTFDBN-5561	474946383761
G9A37K-5561	47 49 46 38 37 61
GGKE74-5561	47 49 46 38 37 61
GU9W29-5561	47 49 46 38 37 61
GZY7B8-5561	47 49 46 38 37 61
H949ZJ-5561	474946383761
HEBY4P-5561	47 49 46 38 37 61
HYFCYH-5561	47 49 46 38 37 61 (GIF87a)
J3U2M6-5561	47 49 46 38 37 61
J3XR9B-5561	25 50 44 46 2D 31
JF4GTB-5562	47 49 46 38 37 61
JJJA4W-5562	0x47 0x49 0x46 0x38 0x37 0x61
JMJLZW-5561	0x 47 49 46 38 37 61
JU4NYL-5561	474946383761 (GIF87a)
K6Z7V8-5562	47 49 46 38 37 61
KE3C4M-5561	47 49 46 38 37 61
KH3MYM-5562	47 49 46 38 37 61
KT78B9-5562	47 49 46 38 37 61 (GIF87a)
KW3EPY-5561	47 49 46 38 37 61 (HEX), ASCII “GIF87a”
L9D7RX-5562	474946383761 (or GIF87a)
LCV3Z2-5561	47 49 46 38 37 61

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26	
WebCode - Test	**Response**
LEERBL-5562	47 49 46 38 37 61
LPY8P3-5561	47 49 46 38 37 61
LRRLAT-5562	47 49 46 38 37 61
LXXGTT-5561	474946383761
M98EB2-5562	474946383761 (GIF87a)
MWHHA4-5562	47 49 46
MYJKY6-5562	47 49 46 38 37 61
N66VNU-5561	47 49 46 38 37 61 (GIF87a)
NFQ2KX-5562	474946383761
NPAH8D-5561	47 49 46 38 37 61
NRJXPX-5561	47 49 46 38 37 61
NTAT4D-5561	47 49 46 38 37 61 (GIF87a) -- 000519.gif
NUKNP6-5562	0x47 0x49 0x46 0x38 0x37 0x61
PBBNHP-5561	47 49 46 38 37 61
PBQMFZ-5561	ASCII:GIF87a HEX: 47 49 46 38 37 61
PTA4GV-5562	474946383761 (values in hexadecimal)
QP2MPV-5561	HEX: 47 49 46 38 37 61 ASCII: GIF87a
R36ZB9-5561	47 49 46 38 37 61
RAQR4V-5562	47 49 46 38 37 61
RFUVTT-5561	47 49 46 38 37 61
RGQL4V-5561	HEX: 47 49 46 38 37 61 ASCII: GIF87a
RK6QRB-5561	GIF87a
RXCADP-5561	47 49 46 38 37 61
T8F7TZ-5562	47 49 46 38 37 61

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26	
WebCode - Test	**Response**
TCA8P9-5561	GIF87a (47 49 46 38 37 61)
TDLF3U-5561	474946383761
TFMD29-5561	Hex: 47 49 46 38 37 61 ASCII: GIF87a
TMAWNW-5561	00111000 00111101 01001100 00000001 00101010 11000111
U298Q9-5561	47 49 46 38 37 61
U964DC-5562	47 49 46 38 37 61
UWTR4N-5561	GIF87a
V23CK9-5561	47 49 46 38 37 61
V96U7R-5561	47 49 46 38 37 61
VFHDED-5561	47 49 46 38 37 61 GIF87a
WHMDWP-5561	47 49 46 38 37 61(Hex),GIF87a(ASCII)
WLLU9J-5561	Hex--47 49 46 38 37 61
WRR3GT-5561	GIF87a (47 49 46 38 37 61)
WW4B2Q-5561	47 49 46 38 37 61
X436QC-5562	47 49 46 38 37 61
X4L22Q-5562	47 49 46 38 37 61
XCDUFN-5561	47 49 46 38 37 61 84
XHHHQN-5561	GIF87a (0x474946383761)
XUR36B-5561	47 49 46 38 37 61
Y2ANWU-5561	47 49 46 38 37 61 GIF87a
YQTYXP-5561	47 49 46 38 37 61
YXADZU-5561	0x47494638
YYKJVA-5561	47 49 46 38 37 61(GIF87a)
ZGHWCN-5561	47 49 46 38 37 61

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26

WebCode - Test	Response
ZM6UW6-5561	0x474946383761
ZTBFTE-5561	GIF87a (47 49 46 38 37 61)

Question 26: Provide the first six bytes of the file with SHA1 hash 383d4c012ac7c550699c3908c57f7ad00b98ecbe.

Consensus Result:
47 49 46 38 37 61, or GIF87a

Expected Response Explanation:
This file can be located with a sorted list of SHA1 hashes for all files on the device. The first several bytes of a file generally contain header information that identifies the file type.

Expected Response Illustration:

Contents of 000519.gif

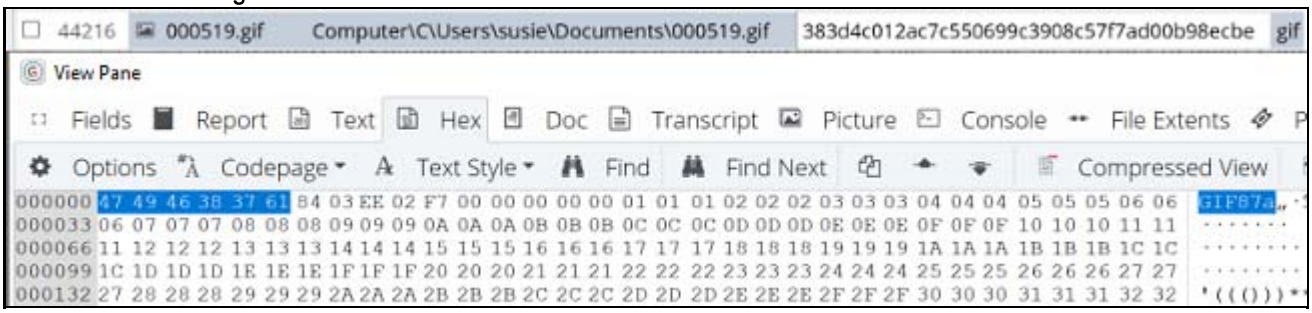


TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27

Question 27: From what host URL was the file Watcher_Generic.zip downloaded?

Manufacturer's Expected Response:

https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip

WebCode - Test	Response
23UJ67-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
29JUMG-5562	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
2YBWJR-5562	https://www.downloads.netgear.com/files/aircard/
3B7V4P-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
3RC2CZ-5561	The host URL where Watcher_Gneric.zip was downloaded from was "https://www.netgear.com/files/aircard/Watcher_Generic.zip".
44372B-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
4A86BF-5561	https://www.downloads.netgear.com (https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip)
4UEFFJ-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
66CHBZ-5561	www.netgear.com
67H6N6-5562	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
6G29KN-5562	https://www.downloads.netgear.com/files/aircard/
6LBUJ2-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	www.downloads.netgear.com
6ZD7FZ-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
7A2A6E-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
7FMAEZ-5562	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
7W9P7F-5562	https://www.netgear.com
89LGKW-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
89NM2E-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
8UH9ME-5562	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
8YVWFY-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
93AL3L-5562	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27

WebCode - Test	Response
9ARR2D-5561	www.downloads.netgear.com
9GULT8-5562	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
9V6AXV-5561	https://www.downloads.netgear.com/files/aircard/
A8KGFG-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
AK9F96-5561	www.downloads.netgear.com
AQYVXC-5562	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
AV4RGC-5562	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
BGJGLT-5561	www.downloads.netgear.com
BKPYQG-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
BMT8ZD-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
BR6KUT-5562	https://www.downloads.netgear.com/files/aircard/
BWZC2P-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
CBTGPD-5562	https://www.downloads.netgear.com/files/aircard/
CMHKPW-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
CPRZ8G-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
CQ9KB9-5562	www.downloads.netgear.com
CQJQ7N-5561	Host URL that file Watcher_Generic.zip was downloaded – www.downloads.netgear.com
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	https://www.downloads.netgear.com/files/aircard
E43HU2-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
E7BXK2-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
EELYM9-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
F2UYKR-5561	The download link of the file was found to be https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
FFG39B-5562	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27

WebCode - Test	Response
FJWWP9-5562	https://www.downloads.netgear.com/files/aircard/
FP3BPR-5562	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
FTFDBN-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
G9A37K-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
GGKE74-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
GU9W29-5561	https://www.downloads.netgear.com
GZY7B8-5561	https://www.downloads.netgear.com/files/aircard/Watcher Generic.zip
H949ZJ-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
HEBY4P-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
HYFCYH-5561	https://www.netgear.com
J3U2M6-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
J3XR9B-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
JF4GTB-5562	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
JJJA4W-5562	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
JMJLZW-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
JU4NYL-5561	https://www.downloads.netgear.com/files/aircard/
K6Z7V8-5562	https://www.downloads.netgear.com/files/aircard/
KE3C4M-5561	https://www.downloads.netgear.com/files/aircard/
KH3MYM-5562	www.downloads.netgear.com/files/aircard/
KT78B9-5562	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
KW3EPY-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
L9D7RX-5562	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
LCV3Z2-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
LEERBL-5562	www.downloads.netgear.com/files/aircard/watcher_Generic.zip

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27

WebCode - Test	Response
LPY8P3-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
LRRLAT-5562	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
LXXGTT-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
M98EB2-5562	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
MWHHA4-5562	https://www.downloads.ntegear.com/files/aircard/
MYJKY6-5562	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
N66VNU-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
NFQ2KX-5562	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
NPAH8D-5561	https://www.netgear.com https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
NRJXPX-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip (HTTPS://WWW.NETGEAR.COM)
NTAT4D-5561	https://www.netgear.com https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
NUKNP6-5562	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
PBBNHP-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
PBQMFZ-5561	https://www.downloads.netgear.com/
PTA4GV-5562	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
QP2MPV-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
R36ZB9-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
RAQR4V-5562	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
RFUVTT-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
RGQL4V-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
RK6QRB-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
RXCADP-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
T8F7TZ-5562	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
TCA8P9-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27

WebCode - Test	Response
TDLF3U-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
TFMD29-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
TMAWNW-5561	https://www.downloads.netgear.com/files/aircard/
U298Q9-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
U964DC-5562	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
UWTR4N-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
V23CK9-5561	https://www.donloads.netgear.com/files/aircard/
V96U7R-5561	https://www.downloads.netgear.com/files/aircard/watcher_Generic.zip
VFHDED-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
WHMDWP-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
WLLU9J-5561	HostUrl=https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
WRR3GT-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
WW4B2Q-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
X436QC-5562	www.netgear.com (https://www.netgear.com/support/product/AirCard%20313U%20(ATT).aspx#Watcher_generic_B3507.msi)
X4L22Q-5562	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
XCDUFN-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
XHHHQN-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
XUR36B-5561	www.netgear.com (https://www.netgear.com/support/product/AirCard%20313U%20(ATT).aspx#Watcher_generic_B3507.msi%20)
Y2ANWU-5561	downloads.netgear.com
YQTYXP-5561	https://www.downloads.netgear.com/files/aircard/
YXADZU-5561	www.downloads.netgear.com
YYKJVA-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
ZGHWCN-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip
ZM6UW6-5561	https://www.netgear.com/support/product/AirCard 313U

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27	
WebCode - Test	**Response**
ZTBFTE-5561	https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip

Question 27: From what host URL was the file Watcher_Generic.zip downloaded?

Consensus Result:
https://www.downloads.netgear.com/files/aircard/Watcher_Generic.zip

Expected Response Explanation:
Finding this file requires a tool that is aware of NTFS Alternate Data Streams (ADS). The subject file has an alternate data stream, Watcher_Generic.zip·Zone.Identifier. The contents of this file show the URL hosting this file, from where it was downloaded.

Expected Response Illustration:

EnCase view of Watcher_Generic.zip·Zone.Identifier

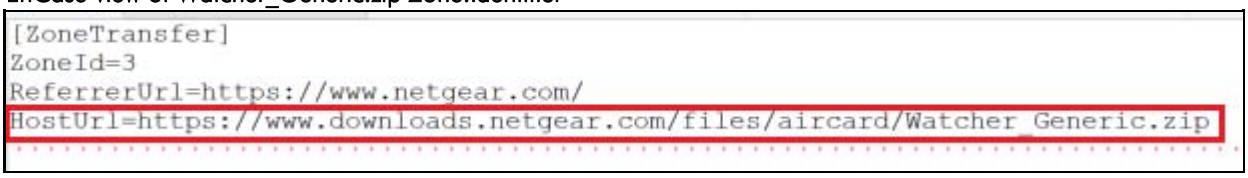


TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28

Question 28: What website did the user visit at 03/01/2021 01:55:08 (UTC+00:00)?

Manufacturer's Expected Response:

www.farmersonly.com

WebCode - Test	Response
23UJ67-5561	FarmersOnly.com
29JUMG-5562	https://www.farmersonly.com/my-photos?just_registered=1
2YBWJR-5562	https://www.farmersonly.com/my-photos?just_registered=1
3B7V4P-5561	www.farmersonly.com
3RC2CZ-5561	The user visited www.farmersonly.com on 3/01/2021 at 01:55:08 UTC.
44372B-5561	https://www.farmersonly.com/
4A86BF-5561	https://www.farmersonly.com
4UEFFJ-5561	https://www.farmersonly.com/?sig=43df905a8c331ecb1c7df8094db843fdada281bcdd542b399c8108045ae9964a https://www.farmersonly.com/my-photos?just_registered=1
66CHBZ-5561	www.farmersonly.com
67H6N6-5562	www.farmersonly.com
6G29KN-5562	https://www.farmersonly.com
6LBUJ2-5561	https://www.farmersonly.com/
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	www.farmersonly.com
6ZD7FZ-5561	www.farmersonly.com
7A2A6E-5561	www.farmersonly.com
7FMAEZ-5562	https:\\www.farmersonly.com
7W9P7F-5562	https://www.farmersonly.com
89LGKW-5561	https://www.farmersonly.com/my-photos?just registered=1
89NM2E-5561	www.farmersonly.com (https://www.farmersonly.com/?sig=43df905a8c331ecb1c7df8094db843fdada281bcdd542b399c8108045ae9964a)
8UH9ME-5562	Farmers Only / https://www.farmersonly.com/my-photos?just_registered=1

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28

WebCode - Test	Response
8YVWFY-5561	https://www.farmersonly.com/?sig=43df905a8c331ecb1c7df8094db843fdada281bcdd542b399c8108045ae9964a https://www.farmersonly.com/my-photos?just_registered=1
93AL3L-5562	https://www.farmersonly.com/
9ARR2D-5561	FarmersOnly.com
9GULT8-5562	https://www.farmersonly.com
9V6AXV-5561	FarmersOnly.com
A8KGFG-5561	FarmersOnly.com URL: https://www.farmersonly.com/?sig=43df905a8c331ecb1c7df8094db843fdada281bcdd542b399c8108045ae9964a
AK9F96-5561	farmersonly.com
AQYVXC-5562	https://www.farmersonly.com
AV4RGC-5562	https://www.farmersonly.com
BGJGLT-5561	www.farmersonly.com
BKPYQG-5561	https://www.farmersonly.com/my-photos?just_registered=1
BMT8ZD-5561	FarmersOnly.com (www.farmersonly.com)
BR6KUT-5562	https://www.farmersonly.com/my-photos?just_registered=1
BWZC2P-5561	https://www.farmersonly.com
CBTGPD-5562	https://www.farmersonly.com/
CMHKPW-5561	https://www.farmersonly.com/
CPRZ8G-5561	www.farmersonly.com
CQ9KB9-5562	www.farmersonly.com
CQJQ7N-5561	Website the user visited at 03/01/2021 01:55:08 (UTC+00:00) – www.FarmersOnly.com
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	www.farmersonly.com
E43HU2-5561	https://www.farmersonly.com
E7BXK2-5561	https://www.farmersonly.com

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28

WebCode - Test	Response
EELYM9-5561	www.farmersonly.com
F2UYKR-5561	At the given time the website accessed was farmsonly.com
FFG39B-5562	FarmersOnly.com
FJWWP9-5562	FarmersOnly.com
FP3BPR-5562	www.farmersonly.com
FTFDBN-5561	http://www.farmersonly.com/
G9A37K-5561	www.farmersonly.com
GGKE74-5561	www.farmersonly.com
GU9W29-5561	Farmersonly.com
GZY7B8-5561	www.farmersonly.com
H949ZJ-5561	https://www.farmersonly.com/?sig=43df905a8c331ecb1c7df8094db843fdada281bcdd542b399c8108045ae9964a
HEBY4P-5561	FarmersOnly.com
HYFCYH-5561	https://www.farmersonly.com
J3U2M6-5561	www.farmersonly.com
J3XR9B-5561	https://www.farmersonly.com/my-photos?just_registered=1
JF4GTB-5562	www.farmersonly.com
JJJA4W-5562	https://www.farmersonly.com
JMJLZW-5561	https://www.farmersonly.com/my-photos?just_registered=1 (https://www.farmersonly.com)
JU4NYL-5561	www.farmersonly.com
K6Z7V8-5562	FarmersOnly.com
KE3C4M-5561	https://www.farmersonly.com
KH3MYM-5562	www.farmersonly.com
KT78B9-5562	https://www.farmersonly.com
KW3EPY-5561	https://www.farmersonly.com

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28

WebCode - Test	Response
L9D7RX-5562	https://www.farmersonly.com/
LCV3Z2-5561	www.farmersonly.com
LEERBL-5562	www.farmersonly.com
LPY8P3-5561	FarmersOnly.com
LRRLAT-5562	https://www.farmersonly.com/my-photos?just_registered=1
LXXGTT-5561	FarmersOnly.com
M98EB2-5562	https://www.farmersonly.com/
MWHHA4-5562	https://www.farmersonly.com/my-photos?just_registered=1
MYJKY6-5562	https://www.farmersonly.com/?sig=43df905a8c331ecb1c7df8094db843fdada281bcdd542b399c8108045ae9964a
N66VNU-5561	https://www.farmersonly.com
NFQ2KX-5562	https://www.farmersonly.com/?sig=43df905a8c331ecb1c7df8094db843fdada281bcdd542b399c8108045ae9964a
NPAH8D-5561	www.farmersonly.com
NRJXPX-5561	FarmersOnly.com
NTAT4D-5561	https://www.farmersonly.com
NUKNP6-5562	https://www.farmersonly.com/?sig=43df905a8c331ecb1c7df8094db843fdada281bcdd542b399c8108045ae9964a
PBBNHP-5561	farmersonly.com
PBQMFZ-5561	https://www.farmersonly.com/
PTA4GV-5562	https://www.farmersonly.com
QP2MPV-5561	www.FarmersOnly.com
R36ZB9-5561	FarmersOnly.com
RAQR4V-5562	https://www.farmersonly.com/?sig=43df905a8c331ecb1c7df8094db843fdada281bcdd542b399c8108045ae9964a
RFUVTT-5561	https://www.farmersonly.com/
RGQL4V-5561	www.farmersonly.com
RK6QRB-5561	https://www.farmersonly.com/?sig=43df905a8c331ecb1c7df8094db843fdada281bcdd542b399c8108045ae9964a

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28

WebCode - Test	Response
RXCADP-5561	FarmersOnly.com
T8F7TZ-5562	https://www.farmersonly.com/
TCA8P9-5561	farmersonly.com Initially: https://www.farmersonly.com/?sig=43df905a8c331ecb1c7df8094db843fdada281bcdd542b399c8108045ae9964a Then: https://www.farmersonly.com/my-photos?just_registered=1
TDLF3U-5561	https://farmersonly.com
TFMD29-5561	www.farmersonly.com
TMAWNW-5561	FarmersOnly.com
U298Q9-5561	WWW.FarmersOnly.com
U964DC-5562	FarmersOnly.com
UWTR4N-5561	https://www.farmersonly.com/
V23CK9-5561	FarmersOnly.com
V96U7R-5561	https://www.farmersonly.com/
VFHDED-5561	https://www.farmersonly.com/ 03/01/2021 01:55:08 AM (01/03/2021 06:55:08 AM UTC)
WHMDWP-5561	FarmersOnly.com
WLLU9J-5561	www.farmersonly.com
WRR3GT-5561	FarmersOnly.com
WW4B2Q-5561	https://www.farmersonly.com
X436QC-5562	www.farmersonly.com
X4L22Q-5562	https://www.farmersonly.com/my-photos?just_registered=1
XCDUFN-5561	FarmersOnly.com
XHHHQN-5561	FarmersOnly.com
XUR36B-5561	www.farmersonly.com
Y2ANWU-5561	Farmersonly.com
YQTYXP-5561	https://www.farmersonly.com/my-photos?just_registered=1

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28

WebCode - Test	Response
YXADZU-5561	farmersonly.com
YYKJVA-5561	www.farmersonly.com
ZGHWCN-5561	https://www.farmersonly.com/my-photos?just_registered=1
ZM6UW6-5561	www.farmersonly.com
ZTBFTE-5561	FarmersOnly.com (https://www.farmersonly.com/my-photos?just_registered=1)

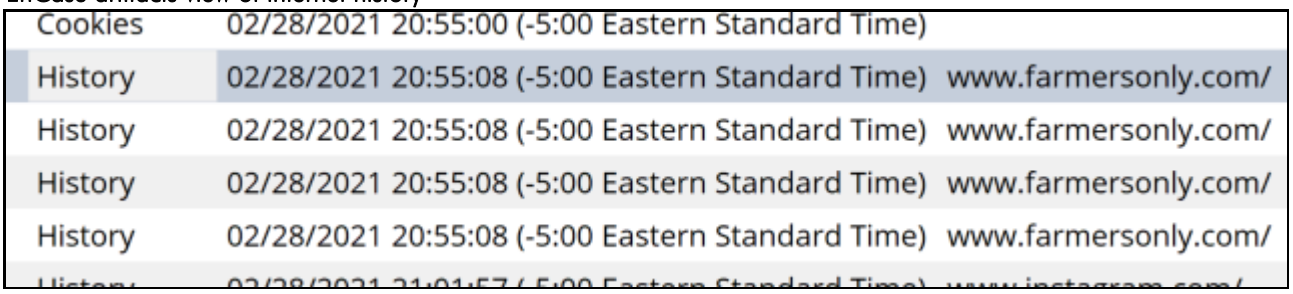
Question 28: What website did the user visit at 03/01/2021 01:55:08 (UTC+00:00)?

Consensus Result:
www.farmersonly.com

Expected Response Explanation:
The user visited this site with the Chrome browser. Parsing the history files for all the installed browsers, sorting by record access time, and seeking this date/time (adjusting for offset) will show the record for this visit.

Expected Response Illustration:

EnCase artifacts view of internet history



Cookies	02/28/2021 20:55:00 (-5:00 Eastern Standard Time)	
History	02/28/2021 20:55:08 (-5:00 Eastern Standard Time)	www.farmersonly.com/
History	02/28/2021 20:55:08 (-5:00 Eastern Standard Time)	www.farmersonly.com/
History	02/28/2021 20:55:08 (-5:00 Eastern Standard Time)	www.farmersonly.com/
History	02/28/2021 20:55:08 (-5:00 Eastern Standard Time)	www.farmersonly.com/

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 29

Question 29: What email address is the Google Chrome browser configured to use to sign into Google?

Manufacturer's Expected Response:

robertapeal67@gmail.com

WebCode - Test	Response
23UJ67-5561	robertapeal67@gmail.com
29JUMG-5562	robertapeal67@gmail.com
2YBWJR-5562	robertapeal67@gmail.com
3B7V4P-5561	robertapeal67@gmail.com
3RC2CZ-5561	The email address used in Google Chrome to sign into Google was "robertapeal67@gmail.com".
44372B-5561	robertapeal67@gmail.com
4A86BF-5561	robertapeal67@gmail.com
4UEFFJ-5561	robertapeal67@gmail.com
66CHBZ-5561	robertapeal67@gmail.com
67H6N6-5562	robertapeal67@gmail.com
6G29KN-5562	robertapeal67@gmail.com
6LBUJ2-5561	robertapeal67@gmail.com
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	robertapeal67@gmail.com
6ZD7FZ-5561	robertapeal67@gmail.com
7A2A6E-5561	robertapeal67@gmail.com
7FMAEZ-5562	robertapeal76@gmail.com
7W9P7F-5562	robertapeal67@gmail.com
89LGKW-5561	robertapeal67@gmail.com
89NM2E-5561	robertapeal67@gmail.com
8UH9ME-5562	robertapeal67@gmail.com
8YVWFY-5561	robertapeal67@gmail.com
93AL3L-5562	robertapeal67@gmail.com

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 29

WebCode - Test	Response
9ARR2D-5561	robertapeal67@gmail.com
9GULT8-5562	robertapeal67@gmail.com
9V6AXV-5561	robertapeal67@gmail.com
A8KGFG-5561	robertapeal67@gmail.com
AK9F96-5561	robertapeal67@gmail.com
AQYVXC-5562	robertapeal67@gmail.com - Users\susie\AppData\Local\Google\Chrome\User Data\Default\Login Data
AV4RGC-5562	robertapeal67@gmail.com
BGJGLT-5561	robertapearl67@gmail.com
BKPYQG-5561	robertapeal67@gmail.com
BMT8ZD-5561	robertapeal67@gmail.com
BR6KUT-5562	robertapeal67@gmail.com
BWZC2P-5561	robertapeal67@gmail.com
CBTGPD-5562	robertapeal67@gmail.com
CMHKPW-5561	robertapeal67@gmail.com
CPRZ8G-5561	robertapeal67@gmail.com
CQ9KB9-5562	robertapeal67@gmail.com
CQJQ7N-5561	Email address that Google Chrome browser is configured to sign into Google – robertapeal67@gmail.com
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	robertapeal67@gmail.com
E43HU2-5561	robertapeal67@gmail.com
E7BXK2-5561	robertapeal67@gmail.com
EELYM9-5561	robertapeal67@gmail.com
F2UYKR-5561	robertapeal67@gmail.com
FFG39B-5562	robertapeal67@gmail.com

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 29	
WebCode - Test	**Response**
FJWWP9-5562	robertapeal67@gmail.com
FP3BPR-5562	robertapeal67@gmail.com
FTFDBN-5561	robertapeal67@gmail.com
G9A37K-5561	Robertapeal67@gmail.com
GGKE74-5561	robertapeal67@gmail.com
GU9W29-5561	robertapeal67@gmail.com
GZY7B8-5561	Robertapeal67@gmail.com
H949ZJ-5561	robertapeal67@gmail.com
HEBY4P-5561	robertapeal67@gmail.com
HYFCYH-5561	robertapeal67@gmail.com
J3U2M6-5561	robertapeal67@gmail.com
J3XR9B-5561	robertapeal67@gmail.com
JF4GTB-5562	robertapeal67@gmail.com
JJJA4W-5562	robertapeal67@gmail.com
JMJLZW-5561	robertapeal67@gmail.com
JU4NYL-5561	robertapeal67@gmail.com
K6Z7V8-5562	robertapeal67@gmail.com
KE3C4M-5561	robertapeal67@gmail.com
KH3MYM-5562	robertapeal67@gmail.com
KT78B9-5562	robertapeal67@gmail.com
KW3EPY-5561	robertapeal67@gmail.com
L9D7RX-5562	[Participant did not return results for this question.]
LCV3Z2-5561	robertapeal67@gmail.com
LEERBL-5562	robertapeal67@gmail.com

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 29	
WebCode - Test	**Response**
LPY8P3-5561	robertapeal67@gmail.com
LRRLAT-5562	robertapeal67@gmail.com
LXXGTT-5561	robertapeal67@gmail.com
M98EB2-5562	robertapeal67@gmail.com
MWHHA4-5562	robertapeal67@gmail.com
MYJKY6-5562	robertapeal67@gmail.com
N66VNU-5561	robertapeal672@gmail.com
NFQ2KX-5562	robertapeal67@gmail.com
NPAH8D-5561	robertapeal67@gmail.com
NRJXPX-5561	Robertapeal67@gmail.com
NTAT4D-5561	robertapeal67@gmail.com
NUKNP6-5562	robertapeal67@gmail.com
PBBNHP-5561	robertapeal67@gmail.com
PBQMFZ-5561	robertapeal67@gmail.com based on Chrome saved Login
PTA4GV-5562	robertapeal67@gmail.com
QP2MPV-5561	robertapeal67@gmail.com
R36ZB9-5561	robertapeal67@gmail.com
RAQR4V-5562	robertapeal67@gmail.com
RFUVTT-5561	robertapeal67@gmail.com
RGQL4V-5561	robertapeal67@gmail.com
RK6QRB-5561	robertapeal67@gmail.com
RXCADP-5561	robertapeal67@gmail.com
T8F7TZ-5562	robertapeal67@gmail.com
TCA8P9-5561	robertapeal67@gmail.com

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 29	
WebCode - Test	**Response**
TDLF3U-5561	Robertapeal67@gmail.com
TFMD29-5561	robertapeal67@gmail.com
TMAWNW-5561	robertapeal67@gmail.com
U298Q9-5561	Robertapeal67@gmail.com
U964DC-5562	robertapeal67@gmail.com
UWTR4N-5561	robertapeal67@gmail.com
V23CK9-5561	robertapeal67@gmail.com
V96U7R-5561	robertapeal67@gmail.com
VFHDED-5561	robertapeal67@gmail.com
WHMDWP-5561	robertapeal67@gmail.com
WLLU9J-5561	robertapeal67@gmail.com
WRR3GT-5561	robertapeal67@gmail.com
WW4B2Q-5561	robertapeal67@gmail.com
X436QC-5562	robertapeal67@gmail.com
X4L22Q-5562	robertapeal672@gmail.com
XCDUFN-5561	robertapeal67@gmail.com
XHHHQN-5561	robertapeal67@gmail.com
XUR36B-5561	robertapeal67@gmail.com
Y2ANWU-5561	robertapeal67@gmail.com
YQTYXP-5561	robertapeal67@gmail.com
YXADZU-5561	robertapeal67@gmail.com
YYKJVA-5561	robertapeal67@gmail.com
ZGHWCN-5561	robertapeal67@gmail.com
ZM6UW6-5561	robertapeal67@gmail.com

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 29	
WebCode - Test	**Response**
ZTBFTE-5561	robertapeal67@gmail.com

Question 29: What email address is the Google Chrome browser configured to use to sign into Google?

Consensus Result:
robertapeal67@gmail.com

Expected Response Explanation:
Google Chrome browser configuration information is stored in C:\Users\susie\AppData\Local\Google\Chrome\User Data\Default\Preferences.

Expected Response Illustration:

Json view of C:\Users\susie\AppData\Local\Google\Chrome\User Data\Default\Preferences.


```
{
    "account_id_migration_state": 2,
    "account_info": [
        {
            "account_id": "100668971676865529021",
            "email": "robertapeal67@gmail.com",
            "full_name": "Roberta Peal",
            "gaia": "100668971676865529021",
            "given_name": "Roberta",
            "hd": "NO_HOSTED_DOMAIN",
            "is_child_account": false,
            "is_under_advanced_protection": false,
```


TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 30

Question 30: With what software was the file 000536.jpg modified?

Manufacturer's Expected Response:

Adobe Photoshop 7.0

WebCode - Test	Response
23UJ67-5561	Adobe Photoshop 7.0
29JUMG-5562	Adobe Photoshop 7.0
2YBWJR-5562	Adobe Photoshop 7.0
3B7V4P-5561	Adobe Photoshop 7.0
3RC2CZ-5561	The 000536.jpg file was modified by Adobe PhotoShop 7.0.
44372B-5561	Adobe Photoshop 7.0
4A86BF-5561	Adobe Photoshop 7.0
4UEFFJ-5561	Adobe Photoshop 7.0
66CHBZ-5561	Adobe Photoshop 7.0
67H6N6-5562	powershell
6G29KN-5562	Adobe Photoshop 7.0
6LBUJ2-5561	Adobe Photoshop 7.0
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	Adobe Photoshop 7.0
6ZD7FZ-5561	Adobe Photoshop 7.0
7A2A6E-5561	Adobe Photoshop 7.0
7FMAEZ-5562	Adobe Photoshop 7.0
7W9P7F-5562	Adobe Photoshop 7.0
89LGKW-5561	Adobe Photoshop 7.047
89NM2E-5561	Adobe Photoshop 7.0
8UH9ME-5562	Adobe Photoshop 7.0
8YVWFY-5561	Adobe Photoshop v7.0
93AL3L-5562	Adobe Photoshop 7.0

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 30	
WebCode - Test	**Response**
9ARR2D-5561	Adobe Photoshop
9GULT8-5562	Adobe Photoshop 7.0
9V6AXV-5561	Adobe Photoshop 7.0
A8KGFG-5561	Adobe Photoshop 7.0
AK9F96-5561	Adobe Photoshop 7.0
AQYVXC-5562	Adobe Photoshop 7.0
AV4RGC-5562	Adobe Photoshop 7.0
BGJGLT-5561	Adobe Photoshop
BKPYQG-5561	Adobe Photoshop 7.0
BMT8ZD-5561	Adobe Photoshop 7.0
BR6KUT-5562	Adobe Photoshop 7.0
BWZC2P-5561	Adobe Photoshop 7.0
CBTGPD-5562	Adobe Photoshop 7.0
CMHKPW-5561	Adobe Photoshop 7.0
CPRZ8G-5561	Adobe Photoshop 7.0
CQ9KB9-5562	Adobe Photoshop 7.0
CQJQ7N-5561	000536.jpg was modified with – Adobe Photoshop 7.0
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	Adobe Photoshop 7.0
E43HU2-5561	Adobe Photoshop
E7BXK2-5561	Adobe Photoshop 7.0
EELYM9-5561	Adobe Photoshop 7.0
F2UYKR-5561	Adobe Photoshop 7.0 was used to modify the said image.
FFG39B-5562	Adobe Photoshop 7.0

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 30	
WebCode - Test	**Response**
FJWWP9-5562	Adobe Photoshop 7.0
FP3BPR-5562	The file 00536.jpg was modified with Adobe Photoshop 7.0
FTFDBN-5561	Adobe Photoshop
G9A37K-5561	Adobe Photoshop 7.0
GGKE74-5561	Adobe photoshop 7.0
GU9W29-5561	Adobe Photoshop 7.0
GZY7B8-5561	Adobe Photoshop 7.0
H949ZJ-5561	Adobe Photoshop 7.0
HEBY4P-5561	Adobe Photoshop 7.0
HYFCYH-5561	Adobe Photoshop 7.0
J3U2M6-5561	Adobe Photoshop 7.0
J3XR9B-5561	Adobe Photoshop 7.0
JF4GTB-5562	Adobe Photoshop 7.0
JJJA4W-5562	Adobe Photoshop 7.0
JMJLZW-5561	Adobe Photoshop 7.0
JU4NYL-5561	Adobe photoshop 7
K6Z7V8-5562	Adobe Photoshop 7.0
KE3C4M-5561	Adobe Photoshop 7.0
KH3MYM-5562	Adobe Photoshop
KT78B9-5562	Adobe Photoshop 7
KW3EPY-5561	Adobe Photoshop 7.0
L9D7RX-5562	Adobe Photoshop 7.0
LCV3Z2-5561	Adobe Photoshop 7.0
LEERBL-5562	Adobe Photoshop 7.0

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 30	
WebCode - Test	**Response**
LPY8P3-5561	Adobe Photoshop 7.0
LRRLAT-5562	Adobe Photoshop 7.0
LXXGTT-5561	Adobe Photoshop 7.0
M98EB2-5562	Adobe Photoshop 7.0
MWHHA4-5562	Adobe Photoshop 7.0
MYJKY6-5562	Adobe Photoshop
N66VNU-5561	Adobe Photoshop 7.0
NFQ2KX-5562	Adobe Photoshop 7.0
NPAH8D-5561	Adobe Photoshop 7.0
NRJXPX-5561	Adobe Photoshop 7.0
NTAT4D-5561	Adobe Photoshop 7.0
NUKNP6-5562	Adobe Photoshop 7.0
PBBNHP-5561	Adobe Photoshop 7.0
PBQMFZ-5561	Adobe Photoshop 7.0 8/12/2005 2:57:21 PM
PTA4GV-5562	Adobe Photoshop 7.0
QP2MPV-5561	Adobe Photoshop 7.0
R36ZB9-5561	Adobe Photoshop 7.0
RAQR4V-5562	Adobe Photoshop 7.0
RFUVTT-5561	Adobe Photoshop 7.0
RGQL4V-5561	Adobe Photoshop 7.0
RK6QRB-5561	Adobe Photoshop 7.0
RXCADP-5561	Adobe Photoshop
T8F7TZ-5562	Adobe Photoshop 7.0
TCA8P9-5561	Adobe Photoshop 7.0

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 30	
WebCode - Test	**Response**
TDLF3U-5561	Adobe Photoshop 7.0
TFMD29-5561	Adobe Photoshop 7.0
TMAWNW-5561	Adobe Photoshop 7.0
U298Q9-5561	Adobe Photoshop 7.0
U964DC-5562	Adobe Photoshop 7.0
UWTR4N-5561	Adobe Photoshop 7.0
V23CK9-5561	Adobe Photoshop 7.0
V96U7R-5561	Adobe Photoshop 7.0
VFHDED-5561	Adobe Photoshop 7.0
WHMDWP-5561	Adobe Photoshop 7.0
WLLU9J-5561	Adobe Photoshop
WRR3GT-5561	Adobe Photoshop 7.0
WW4B2Q-5561	Adobe Photoshop 7.0
X436QC-5562	Adobe Photoshop 7.0
X4L22Q-5562	Adobe Photoshop 7.0
XCDUFN-5561	Adobe Photoshop 7.0
XHHHQN-5561	Adobe Photoshop 7.0
XUR36B-5561	Adobe Photoshop 7.0
Y2ANWU-5561	Adobe Photoshop 7.0
YQTYXP-5561	Adobe Photoshop 7.0
YXADZU-5561	Photoshop
YYKJVA-5561	powershell
ZGHWCN-5561	Adobe Photoshop 7.0
ZM6UW6-5561	Adobe Photoshop 7.0

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 30	
WebCode - Test	**Response**
ZTBFTE-5561	Adobe Photoshop 7.0

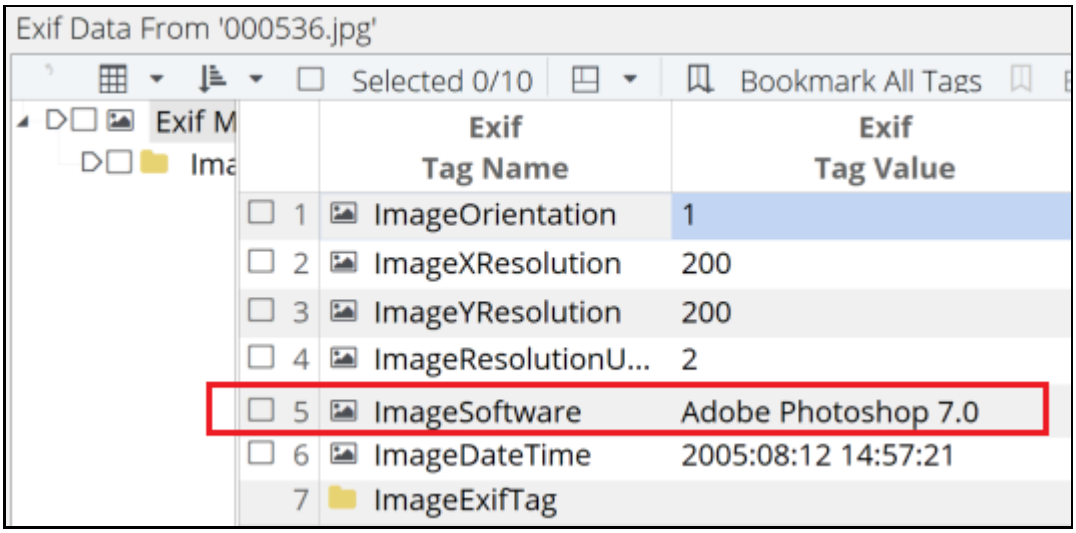
Question 30: With what software was the file 000536.jpg modified?

Consensus Result:
Adobe Photoshop 7.0

Expected Response Explanation:
This information is contained in the EXIF metadata embedded in the file and can be parsed with many tools.

Expected Response Illustration:

EnCase Exif data view



Exiftool data view

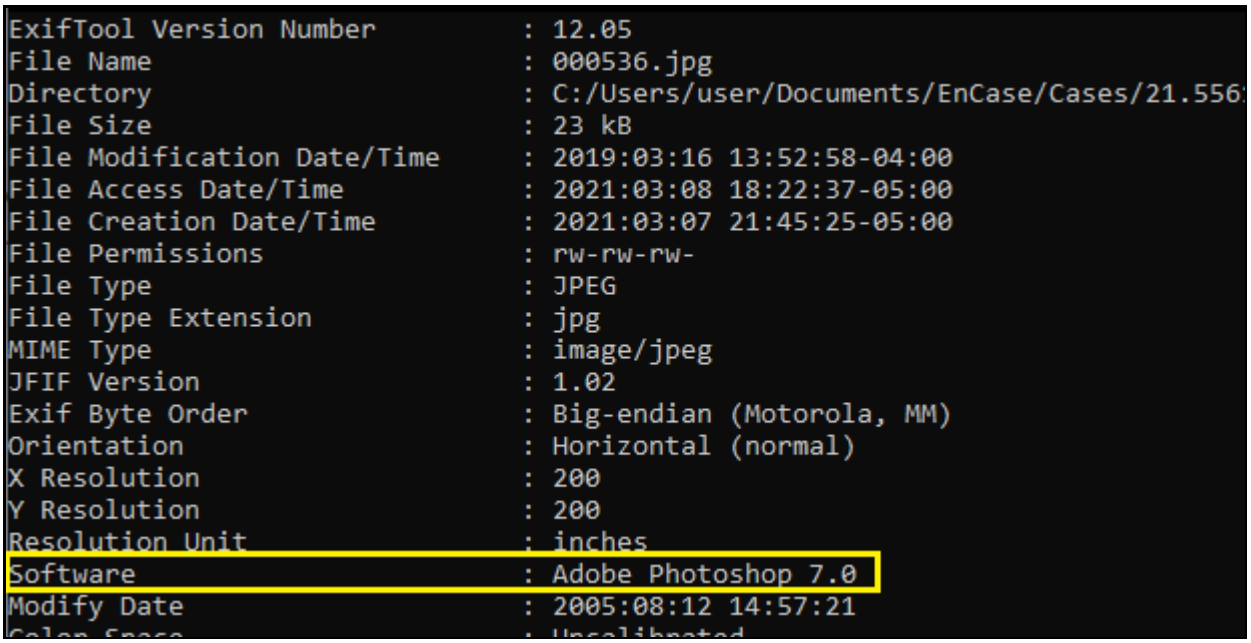


TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 31

Question 31: Who is listed as the author of 850248.xls?

Manufacturer's Expected Response:

Toni Timberman

WebCode - Test	Response
23UJ67-5561	Toni Timberman
29JUMG-5562	Authors :Toni Timberman. Last Author: FRP9899
2YBWJR-5562	Toni Timberman
3B7V4P-5561	Toni Timberman
3RC2CZ-5561	Toni Timberman is listed as the author of 850248.xls.
44372B-5561	Toni Timberman
4A86BF-5561	Toni Timberman
4UEFFJ-5561	Authors: Toni Timberman Last Author: FRP9899
66CHBZ-5561	Toni Timberman
67H6N6-5562	Toni Timberman
6G29KN-5562	Toni Timberman
6LBUJ2-5561	Toni Timberman
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	Toni Timberman
6ZD7FZ-5561	Toni Timberman
7A2A6E-5561	Toni Timberman
7FMAEZ-5562	Toni Timberman
7W9P7F-5562	Toni Timberman
89LGKW-5561	Toni Timberman
89NM2E-5561	Toni Timberman
8UH9ME-5562	Toni Timberman
8YVWFY-5561	Toni Timberman
93AL3L-5562	Toni Timberman

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 31	
WebCode - Test	**Response**
9ARR2D-5561	Toni Timberman
9GULT8-5562	Toni Timberman
9V6AXV-5561	Toni Timberman
A8KGFG-5561	Toni Timberman
AK9F96-5561	Toni Timberman
AQYVXC-5562	Toni Timberman
AV4RGC-5562	Toni Timberman
BGJGLT-5561	Toni Timberman
BKPYQG-5561	Toni Timberman
BMT8ZD-5561	Toni Timberman
BR6KUT-5562	Toni Timberman
BWZC2P-5561	Toni Timberman
CBTGPD-5562	Toni Timberman
CMHKPW-5561	Toni Timberman
CPRZ8G-5561	Toni Timberman
CQ9KB9-5562	Toni Timberman
CQJQ7N-5561	Listed author of file 850248.xls – "susie"
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	Toni Timberman
E43HU2-5561	Toni Timberman
E7BXK2-5561	Toni Timberman
EELYM9-5561	Toni Timberman
F2UYKR-5561	Toni Timberman is the author of the file.
FFG39B-5562	Toni Timberman

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 31

WebCode - Test	Response
FJWWP9-5562	Toni Timberman
FP3BPR-5562	The author of the of the file named 850248.xls is shown as Toni Timberman
FTFDBN-5561	Toni Timberman
G9A37K-5561	Toni Timberman
GGKE74-5561	Toni Timberman
GU9W29-5561	Toni Timberman
GZY7B8-5561	Toni Timberman
H949ZJ-5561	Toni Timberman
HEBY4P-5561	Toni Timberman
HYFCYH-5561	Toni Timberman
J3U2M6-5561	Toni Timberman
J3XR9B-5561	Author: Toni Timberman Last Author FRP9899
JF4GTB-5562	Toni Timberman
JJJA4W-5562	Toni Timberman
JMJLZW-5561	Toni Timberman
JU4NYL-5561	Toni Timberman
K6Z7V8-5562	Toni Timberman
KE3C4M-5561	Toni Timberman
KH3MYM-5562	Toni Timberman
KT78B9-5562	Toni Timberman
KW3EPY-5561	Toni Timberman
L9D7RX-5562	Toni Timberman
LCV3Z2-5561	Toni Timberman
LEERBL-5562	Toni Timberman

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 31	
WebCode - Test	**Response**
LPY8P3-5561	Toni Timberman
LRRLAT-5562	Toni Timberman
LXXGTT-5561	Toni Timberman
M98EB2-5562	Toni Timberman
MWHHA4-5562	Toni Timberman
MYJKY6-5562	Toni Timberman
N66VNU-5561	Toni Timberman
NFQ2KX-5562	Toni Timberman & FRP9899
NPAH8D-5561	Toni Timberman
NRJXPX-5561	Toni Timberman
NTAT4D-5561	Toni Timberman
NUKNP6-5562	Toni Timberman
PBBNHP-5561	Toni Timberman
PBQMFZ-5561	Author: Toni Timberman
PTA4GV-5562	Toni Timberman
QP2MPV-5561	Toni Timberman
R36ZB9-5561	Toni Timberman
RAQR4V-5562	Toni Timberman
RFUVTT-5561	Toni Timberman
RGQL4V-5561	Toni Timberman
RK6QRB-5561	Toni Timberman
RXCADP-5561	Toni Timberman
T8F7TZ-5562	Toni Timberman
TCA8P9-5561	Toni Timberman

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 31	
WebCode - Test	**Response**
TDLF3U-5561	Toni Timberman
TFMD29-5561	Toni Timberman
TMAWNW-5561	Toni Timberman
U298Q9-5561	Toni Timberman
U964DC-5562	Toni Timberman
UWTR4N-5561	Toni Timberman
V23CK9-5561	Toni Timberman
V96U7R-5561	Toni Timberman
VFHDED-5561	Toni Timberman
WHMDWP-5561	Toni Timberman
WLLU9J-5561	Toni Timberman
WRR3GT-5561	Toni Timberman
WW4B2Q-5561	Toni Timberman
X436QC-5562	Toni Timberman
X4L22Q-5562	Toni Timberman
XCDUFN-5561	Toni Timberman
XHHHQN-5561	Toni Timberman
XUR36B-5561	Toni Timberman
Y2ANWU-5561	Toni Timberman
YQTYXP-5561	Toni Timberman
YXADZU-5561	Toni Timberman
YYKJVA-5561	Toni Timberman
ZGHWCN-5561	Toni Timberman
ZM6UW6-5561	Tim Timberman

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 31	
WebCode - Test	**Response**
ZTBFTE-5561	Toni Timberman

Question 31: Who is listed as the author of 850248.xls?

Consensus Result:
Toni Timberman

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

Expected Response Illustration:

Exiftool parsing of metadata for 850248.xls

```
ExifTool Version Number      : 12.05
File Name                    : 850248.xls
Directory                    : C:/Users/user/Documents/EnCase/Cases/21.5561.1/Temp
File Size                    : 166 kB
File Modification Date/Time  : 2030:08:26 16:42:45-04:00
File Access Date/Time        : 2021:03:06 22:06:08-05:00
File Creation Date/Time      : 2021:03:06 22:06:08-05:00
File Permissions             : rw-rw-rw-
File Type                    : XLS
File Type Extension          : xls
MIME Type                    : application/vnd.ms-excel
Author                       : Toni Timberman
Last Modified By             : FRP9899
Software                     : Microsoft Excel
```

Microsoft Excel display of information for 850248.xls

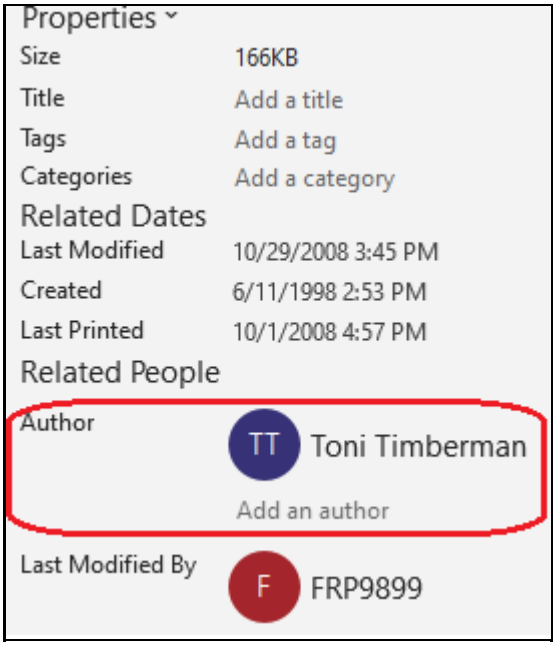


TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 32

Question 32: What file(s) contains the words "Fraud" and "Pack" separated by another word?

Manufacturer's Expected Response:

C:\Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\bookmarkbackups\bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4 and/or
Computer\C:\Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\places.sqlite-wal

WebCode - Test	Response
23UJ67-5561	"bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4" and "places.sqlite"
29JUMG-5562	World Market: The Ultimate Fraud Tutorial Pack (2450+ Tutorials)
2YBWJR-5562	places.sqlite and places.sqlite-wal
3B7V4P-5561	places.sqlite-wal bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4
3RC2CZ-5561	I found TorBrowser artifacts that contain content about Fraud Tutorial Pack. I found a TorBrowser places.sqlite-wal (SQLite Write ahead log) file that was parsed into an HTML file that contained content about Fraud Tutorial Pack. I also found a TorBrowser bookmark artifact containing Fraud Tutorial Pack content.
44372B-5561	places.sqlite-wal bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4
4A86BF-5561	World Market: The Ultimate Fraud Tutorial Pack (2450+ Tutorials)
4UEFFJ-5561	000126.doc; 002683.doc; 002686.doc; 000226.text; 001752.text; 002287.text; 002294.text; 002603.text; 000405.xls World Market: The Ultimate Fraud Tutorial Pack
66CHBZ-5561	Files containing "Fraud (Tutorial) Pack": a. bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4 b. places.sqlite-wa
67H6N6-5562	001677.PDF; us_tv_and_film.txt; 001359.pdf; 002686.doc; 002683.doc; 000405.xls
6G29KN-5562	places.sqlite places.sqlite-wal
6LBUJ2-5561	bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	places.sqlite-wal bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4
6ZD7FZ-5561	Places.sqlite places.sqlite-wal bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4
7A2A6E-5561	places.sqlite
7FMAEZ-5562	http://worldps45uh3rhedmx7g3jgjf3vw52wkvvcastfm46fzrpwoc7f33lid.onion/listing/9825 World Market: The Ultimate Fraud Tutorial Pack (2450+ Tutorials)
7W9P7F-5562	places.sqlite
89LGKW-5561	Tor Browser/bookmarkbackups/bookmarks-2021-03-06_9 -- Ultimate Fraud Tutorial Pack (2450+ Tutorials) https://blog.torproject.org World Market: The Ultimate Fraud Tutorial Pack (2450+ Tutorials)
89NM2E-5561	bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4 places.sqlite-wal

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 32

WebCode - Test	Response
8UH9ME-5562	A bookmark item artifact with the url of: http://worldps45uh3rhedmx7g3jgjf3vw52wkvvcastfm46fzrpwoc7f33lid.onion/listing/9825 and a title of: World Market: The Ultimate Fraud Tutorial Pack (2450+ Tutorials)
8YVWFY-5561	\Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\places.sqlite-wal \Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\bookmarkbackups\bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4
93AL3L-5562	21-5561.E01 - Partition 2 (Microsoft NTFS, 19.43 GB)\Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\places.sqlite World Market: The Ultimate Fraud Tutorial Pack (2450+ Tutorials) This question would be outside our normal lab policies or what is reported to customers unless specifically requested or needed for the examination.
9ARR2D-5561	Two (2) HTML documents, One (1) Sqlite database, and one (1) JSON file bookmark_id_0000010.html bookmarks-2021-03-06_9_LdYTkJ0lDLGwYkFgrdHlA==.jsonlz4 places.sqlite-wal rows_0000000_0000009.html
9GULT8-5562	bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4 places.sqlite-wal
9V6AXV-5561	\Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\places.sqlite – Firefox Bookmarks for - World Market: The Ultimate Fraud Tutorial Pack (2450+ Tutorials) at http://worldps45uh3rhedmx7g3jgjf3vw52wkvvcastfm46fzrpwoc7f33lid.onion/listing/9825
A8KGFG-5561	places.sqlite-wal bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4
AK9F96-5561	C:\Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\bookmarkbackups\bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4 and C:\Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\places.sqlite-wal
AQYVXC-5562	places.sqlite-wal (http://worldps45uh3rhedmx7g3jgjf3vw52wkvvcastfm46fzrpwoc7f33lid.onion/listing/9825) bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4 \Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\bookmarkbackups\bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4
AV4RGC-5562	bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4 places.sqlite
BGJGLT-5561	bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4 places.sqlite-wal
BKPYQG-5561	None Conclusion.
BMT8ZD-5561	bookmark_id_0000010.html bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4 places.sqlite-wal rows_0000000_0000009.html
BR6KUT-5562	Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\places.sqlite
BWZC2P-5561	bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4 places.sqlite-wal
CBTGPD-5562	places.sqlite located at file path Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\places.sqlite
CMHKPW-5561	places.sqlite
CPRZ8G-5561	places.sqlite-wal, bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 32

WebCode - Test	Response
CQ9KB9-5562	URL - http://worldps45uh3rhedmx7g3jgjf3vw52wkvvcastfm46fzrpwoc7f33lid.onion/listing/9825 Title - World Market: The Ultimate Fraud Tutorial Pack
CQJQ7N-5561	File that contains the works “Fraud” and “Pack” – The Ultimate Fraud Tutorial Pack
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	places.sqlite Bookmark Item: http://worldps45uh3rhedmx7g3jgjf3vw52wkvvcastfm46fzrpwoc7f33lid.onion/listing/9825
E43HU2-5561	places.sqlite-wal bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4
E7BXK2-5561	\Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\places.sqlite-wal \Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\bookmarkbackups\bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4
EELYM9-5561	places.sqlite
F2UYKR-5561	No such files found.
FFG39B-5562	places.sqlite-wal AND bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4
FJWWP9-5562	World Market: The Ultimate Fraud Tutorial Pack (2450+ Tutorials)
FP3BPR-5562	The files containing the words “Fraud” and “Pack” separated by one word are: a. bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4 b. places.sqlite-wal Both of these files reside in the Tor Browser directory on the users’ desktop.
FTFDBN-5561	bookmark_id_0000010.html
G9A37K-5561	places.sqlite-wal and bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4
GGKE74-5561	places.sqlite
GU9W29-5561	[ROOT]\Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\places.sqlite
GZY7B8-5561	Places.sqlite
H949ZJ-5561	[Participant did not return results for this question.]
HEBY4P-5561	places.sqlite-wal bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4
HYFCYH-5561	places.sqlite-wal bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4
J3U2M6-5561	places.sqlite
J3XR9B-5561	2
JF4GTB-5562	Firefox bookmark in a sqlite database /Users/susie/Desktop/Tor Browser/Browser/TorBrowser/Data/Browser/profile.default/places.sqlite-wal

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 32

WebCode - Test	Response
JJJA4W-5562	\Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\places.sqlite-wal \Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\bookmarkbackups\bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4
JMJLZW-5561	The Ultimate Fraud Tutorial Pack (2450+ Tutorials), bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4
JU4NYL-5561	\Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\places.sqlite-wal \Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\bookmarkbackups\bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4
K6Z7V8-5562	Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\places.sqlite-wal Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\bookmarkbackups\bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4
KE3C4M-5561	places.sqlite
KH3MYM-5562	Web Page Titled World Market: The Ultimate Fraud Tutorial Pack
KT78B9-5562	C:\Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\places.sqlite
KW3EPY-5561	bookmark title located inside the places.sqlite file. Path: Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\places.sqlite
L9D7RX-5562	bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4 places.sqlite-wal places.sqlite
LCV3Z2-5561	bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4 places.sqlite-wal places.sqlite
LEERBL-5562	\Users\Susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\places.sqlite
LPY8P3-5561	World Market: The Ultimate Fraud Tutorial Pack (2450+ Tutorials)
LRRLAT-5562	I. bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4 II. paces.sqlite-wal
LXXGTT-5561	places.sqlite
M98EB2-5562	TorBrowser\Data\Browser\profile.default\places.sqlite (Tor Browser Bookmark - World Market: The Ultimate Fraud Tutorial Pack (2450+ Tutorials) bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4
MWHHA4-5562	Firefox Bookmark titled "World Market: The Ultimate Fraud Tutorial Pack 2450+ Tutorials)
MYJKY6-5562	places.sqlite-wal bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4
N66VNU-5561	There are three files that matched: bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4, places.sqlite, places.sqlite-wal {path for all three files were in /Users/susie/Desktop/Tor Browser/Browser/TorBrowser/Data/Browser/profile.default/ or /Users/susie/Desktop/Tor Browser/Browser/TorBrowser/Data/Browser/profile.default/bookmarkbackups/}
NFQ2KX-5562	places.sqlite

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 32

WebCode - Test	Response
NPAH8D-5561	File name Carved [163653].MPEG found at path 21-5561.E01/Partition 2/NONAME [NTFS]/[root]/Users/susie/Desktop/Tor Browser/Browser/TorBrowser/Data/Browser/profile.default/places.sqlite-wal/Carved [163653].MPEG file name bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4 found at path jsonlz4 21-5561.E01/Partition 2/NONAME [NTFS]/[root]/Users/susie/Desktop/Tor Browser/Browser/TorBrowser/Data/Browser/profile.default/bookmarkbackups/bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4
NRJXPX-5561	Users/Susie/Desktop/Tor Browser/Browser/TorBrowser/Data/Browser/profile.default/places.sqlite>>Firefox Places>>bookmark_id_0000010.html Users/Susie/Desktop/Tor Browser/Browser/TorBrowser/Data/Browser/profile.default/places.sqlite/SQLite Database/tables/moz_bookmarks/rows_0000000_0000009.html
NTAT4D-5561	bookmark_id_0000010.html bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4 (bookmark backups) places.sqlite-wal rows_0000000_0000009.html
NUKNP6-5562	us_tv_and_film.txt
PBBNHP-5561	places.sqlite
PBQMFZ-5561	The database file for the torbrowser named places.sqlite, contains a bookmarked webpage titled "World Market: The Ultimate Fraud Tutorial Pack (2450+ Tutorials") http://worldps45uh3rhedmx7g3jgjf3vw52wkvvcastfm46fzrpwoc7f33lid.onion/listing/9825 Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\places.sqlite
PTA4GV-5562	bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4 places.sqlite-wal
QP2MPV-5561	\Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\places.sqlite \Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\bookmarkbackups\bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4
R36ZB9-5561	Regarding "Fraud Tutorial Pack", Documents contains one file (HTML). Internet/ Chat Files contains one file (Bookmarks). Unknown Types contains two files (Unknown).
RAQR4V-5562	Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\places.sqlite
RFUVTT-5561	World Market The Ultimate Fraud Tutorial Pack (2450+ Tutorials)
RGQL4V-5561	bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4 places.sqlite-wal
RK6QRB-5561	21-5561.E01/Partition 2/NONAME [NTFS]/[root]/Users/susie/Desktop/Tor Browser/Browser/TorBrowser/Data/Browser/profile.default/bookmarkbackups/bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4 21-5561.E01/Partition 2/NONAME [NTFS]/[root]/Users/susie/Desktop/Tor Browser/Browser/TorBrowser/Data/Browser/profile.default/places.sqlite-wal
RXCADP-5561	A keyword hit pointed to a bookmark to the URL http://worldps45uh3rhedmx7g3jgjf3vw52wkvvcastfm46fzrpwoc7f33lid.onion/listing/9825 software indicated that the title was: World Market: The Ultimate Fraud Tutorial Pack (2450+ Tutorials) There were also 2 Keyword Snippets that were hits for the search I performed with the expression Fraud.{1,100}Pack however they appeared to be references to the above listed URL bookmark. bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4 also places.sqlite-wal
T8F7TZ-5562	World Market The Ultimate Fraud Tutorial Pack (2450+ Tutorials)
TCA8P9-5561	21-5561.E01/Partition 2/NONAME [NTFS]/[root]/Users/susie/Desktop/Tor Browser/Browser/TorBrowser/Data/Browser/profile.default/places.sqlite/SQLite Database/tables/moz_bookmarks/rows_0000000_0000009.html "World Market: The Ultimate Fraud Tutorial Pack (2450+ Tutorials)"
TDLF3U-5561	World Market: The Ultimate Fraud Tutorial Pack (2450+ Tutorials)

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 32

WebCode - Test	Response
TFMD29-5561	places.sqlite-wal bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4
TMAWNW-5561	Bookmark Item "World Market: The Ultimate Fraud Tutorial Pack (2450+ Tutorials)"
U298Q9-5561	Bookmarks-2021-03-06_9_LdYTkjJ0lDLwYkFgrdHlA==.jsonlz4 Places.sqlite-wal
U964DC-5562	"Fraud Tutorial Pack" found in the files: places.sqlite-wal and bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4.
UWTR4N-5561	\Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\places.sqlite
V23CK9-5561	World Market: The Ultimate Fraud Tutorial Pack (2450+ Tutorials) - Bookmark found at C:\Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Broswer\default.profile\places.sqlite
V96U7R-5561	http://worldps45uh3rhedmx7g3jgjf3vw52wkvvcastfm46fzrpwoc7f33lid.onion/listing/9825 World Market: The Ultimate Fraud Tutorial Pack (2450+ Tutorials)
VFHDED-5561	places.sqlite-wal bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4
WHMDWP-5561	bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4 places.sqlite-wal
WLLU9J-5561	#1- I:\Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default \bookmarkbackups\bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4 #2. I:\Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\places.sqlite-wal
WRR3GT-5561	Places.sqlite bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4
WW4B2Q-5561	C:\Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\bookmarkbackups\bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4 C:\Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\places.sqlite-wal
X436QC-5562	bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4 places.sqlite-wa
X4L22Q-5562	World Market: The Ultimate Fraud Tutorial Pack (2450+ Tutorials)
XCDUFN-5561	places.sqlite-wal bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4
XHHHQN-5561	places.sqlite-wal, bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4
XUR36B-5561	bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4 places.sqlite-wal
Y2ANWU-5561	"Fraud ([aA-zZ]+){1}Pack" only returns a web link
YQTYXP-5561	\Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\places.sqlite This is sqlite database which points to the URL http://worldps45uh3rhedmx7g3jgjf3vw52wkvvcastfm46fzrpwoc7f33lid.onion/listing/9825 which has a website title of World Market: The Ultimate Fraud Tutorial Pack (2450+ Tutorials)
YXADZU-5561	bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4 places.sqlite-wal
YYKJVA-5561	001677.PDF, us_tv_and_film.txt, 001359.pdf, 002686.doc, 002683.doc, 000405.xls
ZGHWCN-5561	\Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\places.sqlite
ZM6UW6-5561	bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4 places.sqlite-wal

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 32

WebCode - Test	Response
ZTBFTE-5561	\Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\places.sqlite Bookmark titled "World Market: The Ultimate Fraud Tutorial Pack (2450+ Tutorials)"

Question 32: What file(s) contains the words "Fraud" and "Pack" separated by another word?

Consensus Result:

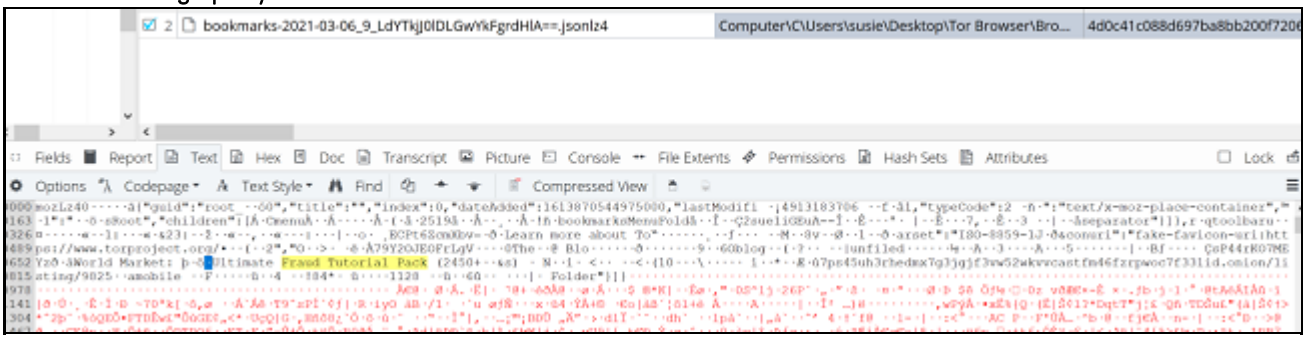
C:\Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\bookmarkbackups\bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4 and/or Computer\C:\Users\susie\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\places.sqlite-wal

Expected Response Explanation:

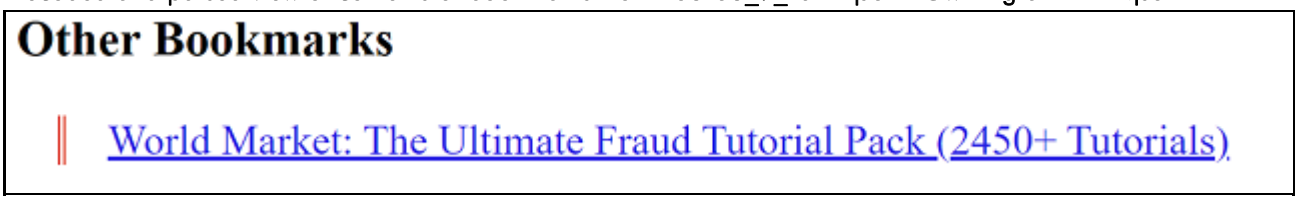
This file contains a backup of sites bookmarked in the Tor browser (or is the SQLite database write ahead log for the Tor browser history log). The string sought in the above question, "Ultimate Fraud Tutorial Pack", can be found using a regular expression search like "Fraud \w{5,10} Pack" or "Fraud [a-z|A-Z]{5,20} Pack" depending on the implementation of grep command used by the analyst or their tool. When decoded, this file contains an HTML list of Tor Browser bookmarks including one for a listing on the Darknet Market, "World Market" for "The Ultimate Fraud Tutorial Pack (2450+ Tutorials)

Expected Response Illustration:

EnCase view of grep keyword hit



Decoded and parsed view of contents of bookmarks-2021-03-06_9_LdYTkjJ0lDLGwYkFgrdHlA==.jsonlz4



Other Responses:

Twenty-one participants reported a relevant artifact (e.g. bookmark "World Market: The Ultimate Fraud Tutorial Pack (2450+ Tutorials)") but did not identify the files.

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 33

Question 33: What email address was the user-installed email client successfully configured to access (send and receive messages)?

Manufacturer's Expected Response:

robertapeal67@gmail.com

WebCode - Test	Response
23UJ67-5561	robertapeal67@gmail.com
29JUMG-5562	robertapeal67@gmail.com
2YBWJR-5562	robertapeal67@gmail.com
3B7V4P-5561	robertapeal67@gmail.com
3RC2CZ-5561	The robertapeal67@gmail.com email address was successfully configured within the Thunderbird email client.
44372B-5561	robertapeal67@gmail.com
4A86BF-5561	robertapeal67@gmail.com
4UEFFJ-5561	robertapeal67@gmail.com
66CHBZ-5561	robertapeal67@gmail.com
67H6N6-5562	robertapeal67@protonmail.com
6G29KN-5562	robertapeal67@gmail.com
6LBUJ2-5561	robertapeal67@gmail.com
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	robertapeal67@gmail.com
6ZD7FZ-5561	robertapeal67@gmail.com
7A2A6E-5561	robertapeal67@gmail.com
7FMAEZ-5562	robertapeal67@gmail.com
7W9P7F-5562	robertapeal67@gmail.com
89LGKW-5561	live.thunderbird.net/autoconfig/v1.1/gmail.com robertapeal67@gmail.com
89NM2E-5561	robertapeal67@gmail.com
8UH9ME-5562	robertapeal67@gmail.com
8YVWFY-5561	robertapeal67@gmail.com

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 33

WebCode - Test	Response
93AL3L-5562	robertapeal67@gmail.com - Thunderbird
9ARR2D-5561	The email client used was Thunderbird. The email address was robertapeal67@protonmail.com. This email address was found in the "mbd2ydcb" profile.
9GULT8-5562	robertapeal67@gmail.com
9V6AXV-5561	robertapeal67@gmail.com
A8KGFG-5561	Mozilla Thunderbird: robertapeal67@gmail.com
AK9F96-5561	robertapeal67@gmail.com
AQYVXC-5562	robertapeal67@gmail.com
AV4RGC-5562	robertapeal67@gmail.com
BGJGLT-5561	robertapearl67@gmail.com
BKPYQG-5561	robertapeal67@gmail.com
BMT8ZD-5561	robertapeal67@gmail.com
BR6KUT-5562	robertapeal67@gmail.com
BWZC2P-5561	robertapeal67@gmail.com
CBTGPD-5562	robertapeal67@gmail.com
CMHKPW-5561	robertapeal67@gmail.com
CPRZ8G-5561	robertapeal67@gmail.com
CQ9KB9-5562	robertapeal67@gmail.com
CQJQ7N-5561	Email address the user-installed email client successfully configured to access (send and receive messages) – robertapeal67@gmail.com
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	robertapeal67@gmail.com
E43HU2-5561	robertapeal67@gmail.com
E7BXK2-5561	robertapeal67@gmail.com
EELYM9-5561	robertapeal67@gmail.com
F2UYKR-5561	The email id robertapeal67@gmail.com was configured on Thunderbird.

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 33

WebCode - Test	Response
FFG39B-5562	robertapeal67@gmail.com
FJWWP9-5562	robertapeal67@protonmail.com
FP3BPR-5562	robertapeal67@gmail.com
FTFDBN-5561	robertapeal67@gmail.com
G9A37K-5561	Robertapeal67@gmail.com
GGKE74-5561	robertapeal67@gmail.com
GU9W29-5561	robertapeal67@gmail.com
GZY7B8-5561	Robertapeal67@gmail.com
H949ZJ-5561	robertapeal67@gmail.com
HEBY4P-5561	robertapeal67@gmail.com
HYFCYH-5561	robertapeal67@gmail.com
J3U2M6-5561	robertapeal67@gmail.com
J3XR9B-5561	robertapeal67@gmail.com
JF4GTB-5562	robertapeal67@gmail.com
JJJA4W-5562	robertapeal67@gmail.com
JMJLZW-5561	robertapeal67@gmail.com (Mozilla Thunderbird)
JU4NYL-5561	robertapeal67@gmail.com
K6Z7V8-5562	robertapeal67@gmail.com
KE3C4M-5561	robertapeal67@gmail.com
KH3MYM-5562	robertapeal67@protonmail.com
KT78B9-5562	robertapeal67@.gmail.com
KW3EPY-5561	robertapeal67@gmail.com
L9D7RX-5562	[Participant did not return results for this question.]
LCV3Z2-5561	robertapeal67@gmail.com

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 33

WebCode - Test	Response
LEERBL-5562	robertapeal67@gmail.com
LPY8P3-5561	robertapeal67@gmail.com
LRRLAT-5562	robertapeal67@gmail.com
LXXGTT-5561	robertapeal67@gmail.com
M98EB2-5562	robertapeal67@gmail.com
MWHHA4-5562	robertapeal67@gmail.com, francismilligan599@gmail.com, robertapeel@protonmail.com
MYJKY6-5562	robertapeal67@gmail.com
N66VNU-5561	robertapeal67@gmail.com
NFQ2KX-5562	collections@irs.gov.go
NPAH8D-5561	robertapeal67@gmail.com
NRJXPX-5561	Robertapeal67@gmail.com
NTAT4D-5561	An email was located indicating that Mozilla Thunderbird was granted access to your Gmail Account: robertapeal67@gmail.com
NUKNP6-5562	benjerry@protonmail.com
PBBNHP-5561	robertapeal67@gmail.com
PBQMFZ-5561	robertapeal67@gmail.com Thunderbird email client
PTA4GV-5562	robertapeal67@gmail.com
QP2MPV-5561	robertapeal67@gmail.com
R36ZB9-5561	robertapeal67@gmail.com
RAQR4V-5562	robertapeal67@protonmail.com
RFUVTT-5561	robertapeal67@protonmail.com
RGQL4V-5561	robertapeal67@gmail.com
RK6QRB-5561	robertapeal67@gmail.com
RXCADP-5561	robertapeal67@gmail.com
T8F7TZ-5562	robertapeal67@protonmail.com

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 33

WebCode - Test	Response
TCA8P9-5561	collections@irs.gov
TDLF3U-5561	Roberttapeal67@gmail.com
TFMD29-5561	robertapeal67@gmail.com
TMAWNW-5561	robertapeal67@gmail.com
U298Q9-5561	Mozilla Thunderbird Email
U964DC-5562	robertapeal67@gmail.com
UWTR4N-5561	robertapeal67@gmail.com
V23CK9-5561	robertapeal67@gmail.com
V96U7R-5561	robertapeal67@gmail.com
VFHDED-5561	robertapeal67@gmail.com
WHMDWP-5561	robertapeal67@gmail.com
WLLU9J-5561	Robertapeal67@gmail.com using mozilla thunderbird ldap in gmail
WRR3GT-5561	Robertapeal67@gmail.com
WW4B2Q-5561	robertapeal67@gmail.com
X436QC-5562	robertapeal67@gmail.com
X4L22Q-5562	robertapeal67@gmail.com
XCDUFN-5561	robertapeal67@gmail.com
XHHHQN-5561	robertapeal67@gmail.com
XUR36B-5561	robertapeal67@gmail.com
Y2ANWU-5561	robertapeal67@gmail.com
YQTYXP-5561	robertapeal67@gmail.com - Installed through Thunderbird.
YXADZU-5561	robertapeal67@gmail.com
YYKJVA-5561	robertapeal67@protonmail.com
ZGHWCN-5561	robertapeal67@gmail.com via the Thunderbird application

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 33

WebCode - Test	Response
ZM6UW6-5561	robertapeal67@gmail.com
ZTBFTE-5561	robertapeal67@gmail.com

Question 33: What email address was the user-installed email client successfully configured to access (send and receive messages)?

Consensus Result:
robertapeal67@gmail.com

Expected Response Explanation:
Mozilla Thunderbird, the user installed email client stores its configuration information in numerous files, including email messages, within the user's AppData directory. This user's (susie) active Thunderbird profile is located at C:\Users\susie\AppData\Roaming\Thunderbird\Profiles\mbd2ydcb.default-release\
The username information in the logins.json settings file used by Thunderbird is encrypted and unviewable without special tools. However, this data appears in plain text in other files such as folderTree.json shown below, which lists the accounts. A review of the contents of the INBOX and Sent Mail folders finds messages sent from and received by the account above.

Expected Response Illustration:

Contents of Thunderbird folderTree.json

```
{
    "open": {
        "all": [
            "mailbox://nobody@Local%20Folders",
            "mailbox://nobody@Local%20Folders/Unsent%20Messages",
            "mailbox://nobody@Local%20Folders/Trash",
            "imap://robertapeal67%40gmail.com@imap.gmail.com/INBOX",
            "imap://robertapeal67%40gmail.com@imap.gmail.com/[Gmail]",
            "imap://collections%40irs.go@.irs.go"
        ]
    },
    "colors": {}
}
```

Email message sent by the email client from the robertapeal67@gmail.com account

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 34

Question 34: With what (other party) email address did the user send and receive emails with encrypted content or attachments?

Manufacturer's Expected Response:
francismilligan599@gmail.com

WebCode - Test	Response ** Inconsistencies not highlighted; No consensus achieved **
23UJ67-5561	Francis Milligan <francismilligan599@gmail.com>
29JUMG-5562	robertapeal67@protonmail.com
2YBWJR-5562	francismilligan599@gmail.com
3B7V4P-5561	robertapeal67@protonmail.com
3RC2CZ-5561	The other email address that the user sent and received emails with encrypted contents and attachments is robertapeal67@protonmail.com.
44372B-5561	robertapeal67@protonmail.com
4A86BF-5561	francismilligan599@gmail.com
4UEFFJ-5561	robertapeal67@protonmail.com
66CHBZ-5561	Francismilligan599@gmail.com
67H6N6-5562	robertapeal67@gmail.com
6G29KN-5562	francismilligan599@gmail.com
6LBUJ2-5561	francismilligan599@gmail.com
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	francismilligan599@gmail.com
6ZD7FZ-5561	francismilligan599@gmail.com
7A2A6E-5561	robertapeal67@protonmail.com
7FMAEZ-5562	francismilligan599@gmail.com
7W9P7F-5562	robertapeal67@protonmail.com
89LGKW-5561	Protonmail robertapeal67@protonmail.com Internet Email robertapeal67@gmail.com (Attachment contained .asc file used by Pretty Good Privacy (PGP))
89NM2E-5561	robertapeal67@protonmail.com
8UH9ME-5562	robertapeal67@protonmail.com
8YVWFY-5561	francismilligan599@gmail.com

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 34

WebCode - Test	Response ** Inconsistencies not highlighted; No consensus achieved **
93AL3L-5562	Francis Milligan <francismilligan599@gmail.com>
9ARR2D-5561	Emails were sent to Francis Milligan from Roberta Peal
9GULT8-5562	francismilligan599@gmail.com
9V6AXV-5561	francismilligan599@gmail.com
A8KGFG-5561	francismilligan599@gmail.com
AK9F96-5561	francismilligan599@gmail.com
AQYVXC-5562	Francis Milligan <francismilligan599@gmail.com>
AV4RGC-5562	robertapeal67@protonmail.com
BGJGLT-5561	robertapearl@protonmail.com
BKPYQG-5561	francismilligan599@gmail.com
BMT8ZD-5561	francismilligan599@gmail.com
BR6KUT-5562	francismilligan599@gmail.com
BWZC2P-5561	francismilligan599@gmail.com
CBTGPD-5562	francismilligan599@gmail.com and robertapeal67@protonmail.com
CMHKPW-5561	robertapeal67@protonmail.com
CPRZ8G-5561	francismilligan599@gmail.com
CQ9KB9-5562	francismilligan599@gmail.com
CQJQ7N-5561	Email address (other party) the user sent and received emails with encrypted content or attachments – Francis Milligan francismilligan599@gmail.com
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	francismilligan599@gmail.com
E43HU2-5561	francismilligan599@gmail.com
E7BXK2-5561	robertapeal67@protonmail.com
EELYM9-5561	francismilligan599@gmail.com
F2UYKR-5561	Emails with encrypted content were exchanged with francismilligan599@gmail.com

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 34

WebCode - Test	Response ** Inconsistencies not highlighted; No consensus achieved **
FFG39B-5562	francismilligan599@gmail.com
FJWWP9-5562	Proton Mail
FP3BPR-5562	francismilligan599@gmail.com
FTFDBN-5561	francismilligan599@gmail.com
G9A37K-5561	Francis Milligan <francismilligan599@gmail.com>
GGKE74-5561	robertapeal67@protonmail.com
GU9W29-5561	francismilligan599@gmail.com
GZY7B8-5561	Francismilligan599@gmail.com
H949ZJ-5561	robertapeal67@protonmail.com
HEBY4P-5561	robertapeal67@protonmail.com
HYFCYH-5561	francismilligan599@gmail.com
J3U2M6-5561	francismilligan599@gmail.com
J3XR9B-5561	francismilligan599@gmail.com
JF4GTB-5562	francismilligan599@gmail.com
JJJA4W-5562	robertapeal67@protonmail.com
JMJLZW-5561	francismilligan599@gmail.com
JU4NYL-5561	robertapeal67@protonmail.com
K6Z7V8-5562	francismilligan599@gmail.com
KE3C4M-5561	francismilligan599@gmail.com
KH3MYM-5562	francismilligan599@gmail.com
KT78B9-5562	Francis Milligan francismilligan599@gmail.com, robertapeal67@protonmail.com
KW3EPY-5561	1) Received from: francismilligan599@gmail.com and 2) Send to: robertapeal67@protonmail.com
L9D7RX-5562	[Participant did not return results for this question.]
LCV3Z2-5561	francismilligan599@gmail.com

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 34

WebCode - Test	Response ** Inconsistencies not highlighted; No consensus achieved **
LEERBL-5562	francismilligan599@gmail.com Also communication with robertapeal67@protonmail.com
LPY8P3-5561	francismilligan599@gmail.com
LRRLAT-5562	francismilligan599@gmail.com
LXXGTT-5561	francismilligan599@gmail.com
M98EB2-5562	francismilligan599@gmail.com, robertapeal67@protonmail.com
MWHHA4-5562	francesmilligan599@gmail.com
MYJKY6-5562	robertapeal67@protonmail.com
N66VNU-5561	Francis Milligan <francismilligan599@gmail.com>
NFQ2KX-5562	robertapeal67@gmail.com
NPAH8D-5561	francismilligan599@gmail.com robertapeal67@protonmail.com
NRJXPX-5561	Francismilligan599@gmail.com
NTAT4D-5561	Email communication was located that contained encrypted messages and attachments between Roberta Peal - robertapeal67@gmail.com and Francis Milligan - francismilligan599@gmail.com.
NUKNP6-5562	francismilligan599@gmail.com
PBBNHP-5561	francismilligan599@gmail.com
PBQMFZ-5561	francismilligan599@gmail.com
PTA4GV-5562	francismilligan559@gmail.com
QP2MPV-5561	francismilligan599@gmail.com
R36ZB9-5561	robertapeal67@protonmail.com
RAQR4V-5562	FrancisMilligan599@gmail.com
RFUVTT-5561	francismilligan599@gmail.com
RGQL4V-5561	francismilligan599@gmail.com
RK6QRB-5561	francismilligan599@gmail.com
RXCADP-5561	francismilligan599@gmail.com
T8F7TZ-5562	francismilligan599@gmail.com

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 34	
WebCode - Test	**Response** ** Inconsistencies not highlighted; No consensus achieved **
TCA8P9-5561	robertapeal67@gmail.com
TDLF3U-5561	fransicmilligan599@gmail.com
TFMD29-5561	francismilligan599@gmail.com
TMAWNW-5561	robertapeal67@protonmail.com
U298Q9-5561	Francismilligan599@gmail.com
U964DC-5562	Francis Milligan <francismiligan599@gmail.com>
UWTR4N-5561	Francis Milligan <francismilligan599@gmail.com>
V23CK9-5561	robertapeal67@protonmail.com
V96U7R-5561	francismilligan599@gmail.com
VFHDED-5561	robertapeal67@protonmail.com
WHMDWP-5561	francismilligan599@gmail.com
WLLU9J-5561	Francismilligan599@gmail.com
WRR3GT-5561	Francismilligan599@gmail.com
WW4B2Q-5561	francismilligan599@gmail.com
X436QC-5562	francismilligan599@gmail.com
X4L22Q-5562	francismilligan599@gmail.com
XCDUFN-5561	francismilligan599@gmail.com
XHHHQN-5561	francismilligan599@gmail.com
XUR36B-5561	francismilligan599@gmail.com
Y2ANWU-5561	francismilligan599@gmail.com
YQTYXP-5561	francismilligan599@gmail.com
YXADZU-5561	francismilligan599@gmail.com
YYKJVA-5561	robertapeal67@gmail.com
ZGHWCN-5561	Francis Milligan <francismilligan599@gmail.com>

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 34	
WebCode - Test	**Response** ** Inconsistencies not highlighted; No consensus achieved **
ZM6UW6-5561	robertapeal67@protonmail.com
ZTBFTE-5561	francismilligan599@gmail.com

Question 34: With what (other party) email address did the user send and receive emails with encrypted content or attachments?

Consensus Result:

A consensus for this question was not achieved. The objective of the question was for the examiner to identify the email address belonging to the other party in which the user sent and received emails with encrypted content. The majority of participants (73%) reported the expected email address. Another 20% of participants reported the user's email address.

Expected Response Explanation:

The Thunderbird INBOX contains an email with Subject, "the info you requested" with an attachment, "file.gpg". The extension gpg is used for files encrypted with GNU Privacy Guard, a free cryptographic software suite. Presumably, this attachment would be encrypted with the recipient's public key (it is in this case) and if the recipient's private key were recoverable from their computer (also true here), and the password protecting that key could be broken, the contents of this file could be determined.

Expected Response Illustration:

EnCase report view of message with encrypted attachment

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 34

View of encrypted content in file.gpg

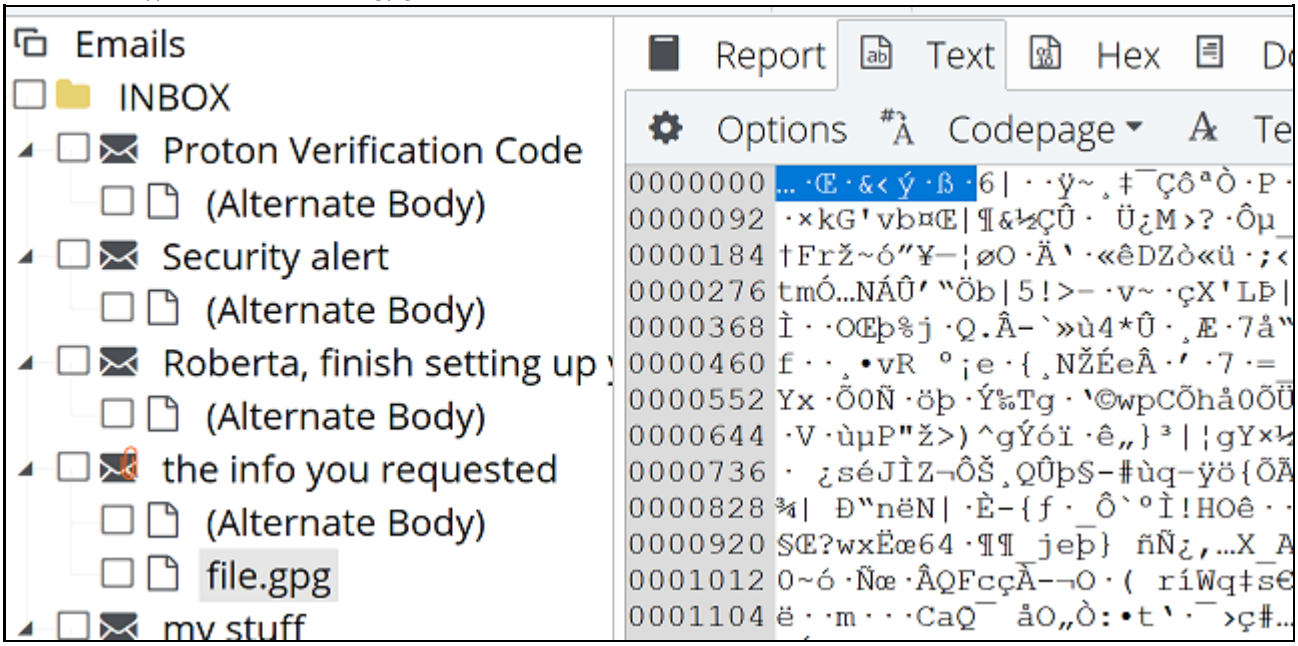


TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 35

Question 35: What is the default program for opening .docx document files?

Manufacturer's Expected Response:

OpenOffice Writer or swriter.exe

WebCode - Test	Response ** Inconsistencies not highlighted; No consensus achieved **
23UJ67-5561	WordPad.exe
29JUMG-5562	OpenOffice 4 (swriter.exe)
2YBWJR-5562	OpenOffice
3B7V4P-5561	WordPad
3RC2CZ-5561	It appears that the default program used to open .docx files is WordPad.exe
44372B-5561	OpenOffice
4A86BF-5561	Open Office Writer
4UEFFJ-5561	OpenOffice (swriter.exe) [wordpad.exe was the default on 2019]
66CHBZ-5561	Microsoft Office Word
67H6N6-5562	OpenOffice.Docx
6G29KN-5562	OpenOffice
6LBUJ2-5561	OpenOffice
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	Open Office
6ZD7FZ-5561	Open Office Writer
7A2A6E-5561	OpenOffice
7FMAEZ-5562	Open Office
7W9P7F-5562	wordpad.exe
89LGKW-5561	OpenWithProgids OpenOffice.docx OpenOffice 4.1.9
89NM2E-5561	OpenOffice
8UH9ME-5562	OpenOffice
8YVWFY-5561	WORDPAD.EXE
93AL3L-5562	Open Office

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 35

WebCode - Test	Response ** Inconsistencies not highlighted; No consensus achieved **
9ARR2D-5561	OpenOffice
9GULT8-5562	WordPad.exe
9V6AXV-5561	wordpad.exe
A8KGFG-5561	Open Office
AK9F96-5561	OpenOffice Writer
AQYVXC-5562	Open Office (Writer)
AV4RGC-5562	OpenOffice 4.1.9
BGJGLT-5561	Wordpad.exe
BKPYQG-5561	OpenOffice
BMT8ZD-5561	OpenOffice 4.1.9 (swriter.exe)
BR6KUT-5562	a: soffice.bin
BWZC2P-5561	Open Office
CBTGPD-5562	OpenOffice
CMHKPW-5561	OPENOFFICE
CPRZ8G-5561	Open Office
CQ9KB9-5562	WORDPAD.EXE
CQJQ7N-5561	Default program opening .docx document files – Microsoft Word 2016 XML
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	OpenOffice.Docx
E43HU2-5561	OpenOffice Writer "C:\Program Files (x86)\OpenOffice 4\program\swriter.exe"
E7BXK2-5561	OpenOffice
EELYM9-5561	OpenOffice 4
F2UYKR-5561	To open .docx files default program set was Open office.
FFG39B-5562	Open Office

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 35	
WebCode - Test	**Response** ** Inconsistencies not highlighted; No consensus achieved **
FJWWP9-5562	Microsoft Office Word
FP3BPR-5562	The default program for opening .docx files is OpenOffice
FTFDBN-5561	OpenOffice.Docx
G9A37K-5561	OpenOffice 4
GGKE74-5561	OpenOffice
GU9W29-5561	Wordpad.exe
GZY7B8-5561	Open office 4
H949ZJ-5561	Open Office
HEBY4P-5561	OpenOffice 4.1.9
HYFCYH-5561	WordPad.exe
J3U2M6-5561	Open office
J3XR9B-5561	Openoffice
JF4GTB-5562	soffice.bin Open Office
JJJA4W-5562	OpenOffice
JMJLZW-5561	OpendOffice.Docx
JU4NYL-5561	OpenOfficer.org Writer
K6Z7V8-5562	WORDPAD.EXE
KE3C4M-5561	OpenOffice4 / swriter.exe
KH3MYM-5562	Apache Open Office
KT78B9-5562	OpenOffice
KW3EPY-5561	Wordpad
L9D7RX-5562	OpenOffice
LCV3Z2-5561	swriter.exe (OpenOffice Writer)
LEERBL-5562	Open Office Writer

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 35

WebCode - Test	Response ** Inconsistencies not highlighted; No consensus achieved **
LPY8P3-5561	OpenOffice.exe
LRRLAT-5562	Soffice.bin
LXXGTT-5561	OpenOffice
M98EB2-5562	Wordpad.exe
MWHHA4-5562	swriter.exe
MYJKY6-5562	Open Office
N66VNU-5561	Default program for opening .docx is WORDPAD (and the default "open-with" listed program when using MS windows explorer is OpenOffice 4.1.9)
NFQ2KX-5562	OpenOffice 4
NPAH8D-5561	Office 4
NRJXPX-5561	WordPad.exe
NTAT4D-5561	Open Office 4
NUKNP6-5562	OpenOffice 4.1.9805
PBBNHP-5561	WordPad.exe
PBQMFZ-5561	OpenOffice 4.1.9
PTA4GV-5562	OpenOffice
QP2MPV-5561	Open Office (soffice.bin)
R36ZB9-5561	OpenOffice (OpenOffice.docx)
RAQR4V-5562	Open Office
RFUVTT-5561	OpenOffice 4\program\\swriter.exe
RGQL4V-5561	Open Office (soffice.bin)
RK6QRB-5561	soffice.bin (LibreOffice)
RXCADP-5561	OpenOffice
T8F7TZ-5562	OpenOffice 4\program\\swriter.exe
TCA8P9-5561	Apache Open Office 4.1.9 - OpenOffice Writer

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 35	
WebCode - Test	**Response** ** Inconsistencies not highlighted; No consensus achieved **
TDLF3U-5561	OpenOffice
TFMD29-5561	C:\Program Files (x86)\OpenOffice 4\program\swriter.exe
TMAWNW-5561	Wordpad.exe
U298Q9-5561	OpenOffice/swriter.exe
U964DC-5562	OpenOffice (Version 4.1.9 Installed)
UWTR4N-5561	WORDPAD.EXE
V23CK9-5561	WordPad.exe
V96U7R-5561	Open Office
VFHDED-5561	Apache OpenOffice Writer
WHMDWP-5561	WORDPAD.EXE
WLLU9J-5561	OpenOffice
WRR3GT-5561	Openoffice (soffice.bin)
WW4B2Q-5561	Apache OpenOffice 4.1.9
X436QC-5562	Open Office
X4L22Q-5562	WORDPAD.EXE
XCDUFN-5561	OpenOffice.Docx
XHHHQN-5561	OpenOffice Writer
XUR36B-5561	Open Office
Y2ANWU-5561	Wordpad.exe
YQTYXP-5561	Wordpad.exe
YXADZU-5561	OpenOffice
YYKJVA-5561	OpenOffice.Docx
ZGHWCN-5561	WORDPAD.EXE
ZM6UW6-5561	OpenOffice

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 35	
WebCode - Test	**Response** ** Inconsistencies not highlighted; No consensus achieved **
ZTBFTE-5561	Wordpad.exe

Question 35: What is the default program for opening .docx document files?

Consensus Result:

A consensus was not achieved for this question. The objective of the question was for the examiner to identify the default program for opening docx. document files on this computer. The majority of participants (73%) reported the expected response. Another 20% reported "WordPad.exe" which is the normal Windows setting but on this computer it was changed to swriter when Open Office was installed.

Expected Response Explanation:

Windows stores settings for default applications (by file extension) in the SOFTWARE registry hive: SOFTWARE: Classes\.dotx\OpenWithProgids\ which specifies OpenOffice.Docx. SOFTWARE: Classes\OpenOffice.Docx\shell\open\command identifies the executable for opening .docx files as "C:\Program Files (x86)\OpenOffice 4\program\\swriter.exe"

Expected Response Illustration:

Registry Explorer view of SOFTWARE: Classes\OpenOffice.Docx\shell\open\command

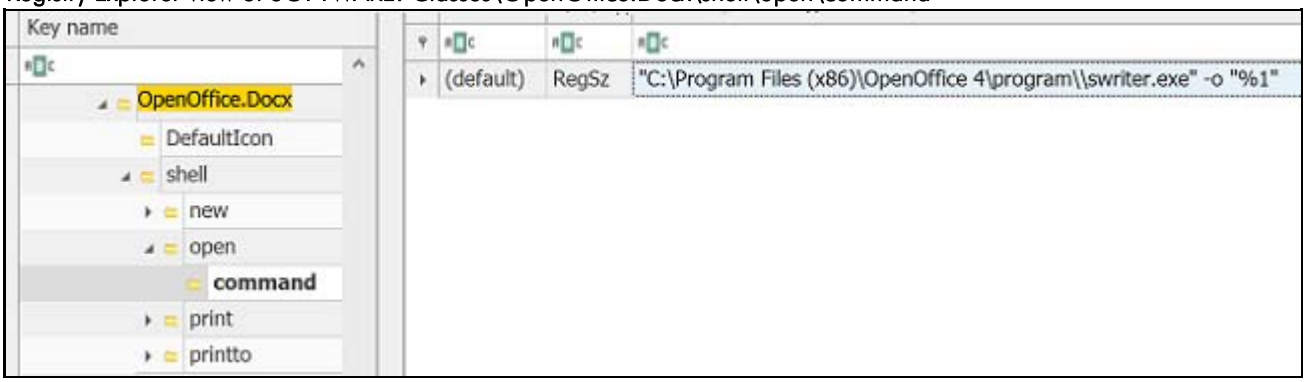


TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 36

Question 36: Provide the 10 byte (ASCII) string beginning at Physical Sector 5236523, Sector Offset 67.

Manufacturer's Expected Response:

good work!

WebCode - Test	Response
23UJ67-5561	good work!
29JUMG-5562	good work! (67 6F 6F 64 20 77 6F 72 6B 21)
2YBWJR-5562	good work!
3B7V4P-5561	good work!
3RC2CZ-5561	The 10 bytes in ASCII at Physical Sector 5236523, Sector Offset 67 is good work!
44372B-5561	good work!
4A86BF-5561	good work!
4UEFFJ-5561	67 6F 6F 64 20 77 6F 72 6B 21
66CHBZ-5561	good work!
67H6N6-5562	good work!
6G29KN-5562	good work!
6LBUJ2-5561	good work!
6N3QEM-5562	[Participant did not return results for this question.]
6RMHKX-5561	get you to
6ZD7FZ-5561	good work!
7A2A6E-5561	good.work!
7FMAEZ-5562	good work!
7W9P7F-5562	uld just g
89LGKW-5561	good work!
89NM2E-5561	good work!
8UH9ME-5562	253-773-5
8YVWFY-5561	good work!
93AL3L-5562	good work!

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 36

WebCode - Test	Response
9ARR2D-5561	[Participant did not return results for this question.]
9GULT8-5562	good work!
9V6AXV-5561	good work! (676F6F6420776F726B21)
A8KGFG-5561	Good work!
AK9F96-5561	good work!
AQYVXC-5562	676F6F6420776F726B21 - good work!
AV4RGC-5562	good work!
BGJGLT-5561	good work!
BKPYQG-5561	0A 0A 28 67 6F 6F 64 20 77 6F
BMT8ZD-5561	good work!
BR6KUT-5562	good work!
BWZC2P-5561	good work!
CBTGPD-5562	good work!
CMHKPW-5561	good work!
CPRZ8G-5561	good work!
CQ9KB9-5562	67 6f 6f 64 20 77 6f 72 6b 21 (good work!)
CQJQ7N-5561	10 byte (ASCII) string beginning at Physical Sector 5236523, Sector Offset 67 – 75 6C 64 20 6A 75 73 74 20 67
CZCW7G-5562	[Participant did not return results for this question.]
DBQ9Y6-5561	good work!
E43HU2-5561	good work!
E7BXK2-5561	good work!
EELYM9-5561	good work!
F2UYKR-5561	DE 37 0F 6F 42 18 9A EC
FFG39B-5562	(good work

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 36	
WebCode - Test	**Response**
FJWWP9-5562	good work!
FP3BPR-5562	The 10 byte ASCII string at PS 5236523 SO 67 reads “good work!”
FTFDBN-5561	good
G9A37K-5561	good work!
GGKE74-5561	good.work!
GU9W29-5561	good work!
GZY7B8-5561	Good work!
H949ZJ-5561	m Ø Zoà ˜
HEBY4P-5561	20 32 35 33 2D 37 37 33 2D 35
HYFCYH-5561	253-773-5
J3U2M6-5561	good work!
J3XR9B-5561	0A 0A 28 67 6F 6F 64 20 77 6F
JF4GTB-5562	good work!
JJJA4W-5562	good work!
JMJLZW-5561	Good Work!
JU4NYL-5561	good work!
K6Z7V8-5562	good work!
KE3C4M-5561	good work!
KH3MYM-5562	good work!
KT78B9-5562	67 6F 6F 64 20 77 6F 72 6B 21 / good work!
KW3EPY-5561	good work!
L9D7RX-5562	good work!
LCV3Z2-5561	good work!
LEERBL-5562	good work!

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 36

WebCode - Test	Response
LPY8P3-5561	good work!
LRRLAT-5562	good work!
LXXGTT-5561	good work!
M98EB2-5562	good work!
MWHHA4-5562	good work!
MYJKY6-5562	good work!
N66VNU-5561	“good work!”
NFQ2KX-5562	66 FF 76 08 68 00 00 68 00 7C
NPAH8D-5561	Good work!
NRJXPX-5561	good work!
NTAT4D-5561	Starting at Sector Offset 68, the ASCII sting is goodwork!
NUKNP6-5562	h7##¬4uŞqé
PBBNHP-5561	good work!
PBQMFZ-5561	"good work!"
PTA4GV-5562	good work!
QP2MPV-5561	good work!
R36ZB9-5561	67 6F 6F 64 20 77 6F 72 6B 21
RAQR4V-5562	good work!
RFUVTT-5561	67 6F 6F 64 20 77 6F 72 6B 21
RGQL4V-5561	good work!
RK6QRB-5561	good work!
RXCADP-5561	good work!
T8F7TZ-5562	67 6F 6F 64 20 77 6F 72 6B 21
TCA8P9-5561	good work!

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 36

WebCode - Test	Response
TDLF3U-5561	good work!
TFMD29-5561	good work!
TMAWNW-5561	[Participant did not return results for this question.]
U298Q9-5561	good work!
U964DC-5562	good work!
UWTR4N-5561	good work!
V23CK9-5561	good work!
V96U7R-5561	good work!
VFHDED-5561	73 95 A3 BE DF 72 D0 05 40 F5
WHMDWP-5561	good work!
WLLU9J-5561	good work!
WRR3GT-5561	Good work!
WW4B2Q-5561	good work!
X436QC-5562	good work!
X4L22Q-5562	good work!
XCDUFN-5561	good work!
XHHHQN-5561	good work!
XUR36B-5561	good work!
Y2ANWU-5561	good work!
YQTYXP-5561	good work! - (HEX 67 6F 6F 64 20 77 6F 72 6B 21)
YXADZU-5561	good work!
YYKJVA-5561	good work!
ZGHWCN-5561	good work! - 676F6F6420776F726B21
ZM6UW6-5561	good work!

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 36	
WebCode - Test	**Response**
ZTBFTE-5561	good work!

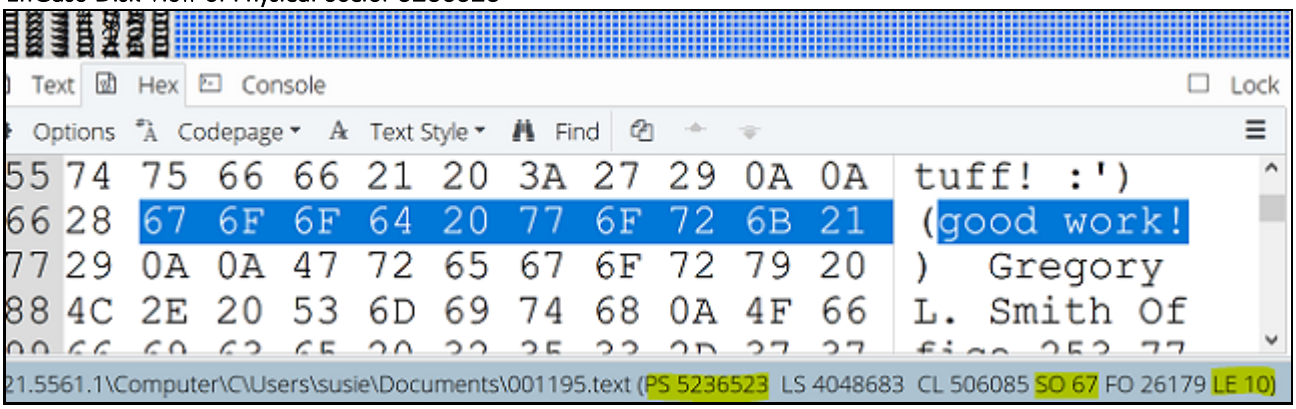
Question 36: Provide the 10 byte (ASCII) string beginning at Physical Sector 5236523, Sector Offset 67.

Consensus Result:
good work!

Expected Response Explanation:
A forensic tool with a disk view function will allow an analyst to navigate to a particular sector and offset.

Expected Response Illustration:

EnCase Disk View of Physical Sector 5236523



Removable Media Device Results

TABLE 2: Removable Media Device Results

Question 37

Question 37: The SHA1 hash for the USB device is F3C33632CD03525ECC4B07362AC5196DA5F02262. Provide the SHA256 hash for the USB device.

Manufacturer's Expected Response:
EE010683ABE27680DB634FD1AA00AEA493820EF057C1DEE7D528FA55F123D85C

WebCode - Test	Response
29JUMG-5562	EE010683ABE27680DB634FD1AA00AEA493820EF057C1DEE7D528FA55F123D85C
2YBWJR-5562	At the time this test was issued, there was not an approved tool for use to provide this data.
67H6N6-5562	[Participant did not return results for this question.]
6G29KN-5562	This question is outside the scope of a normal examination at the [Laboratory] and would not be reported under normal circumstances. I'm familiar with forensic software programs that are capable of generating SHA256 hash values for digital media (e.g. Forensic Explorer and OSForensics) and I am capable of generating a SHA256 hash value for the USB device, but it isn't normal lab practice to generate SHA256 hash values for digital media submitted to the lab. Forensic Explorer is approved for use at the [Laboratory], but we don't typically use it to generate SHA256 hash values. Therefore, I am not providing an answer to this question.
6N3QEM-5562	ee010683abe27680db634fd1aa00aea493820ef057c1dee7d528fa55f123d85c
7FMAEZ-5562	EE010683ABE27680DB634FD1AA00AEA493820EF057C1DEE7D528FA55F123D85C
7W9P7F-5562	EE010683ABE27680DB634FD1AA00AEA493820EF057C1DEE7D528FA55F123D85C
8UH9ME-5562	EE010683ABE27680DB634FD1AA00AEA493820EF057C1DEE7D528FA55F123D85C
93AL3L-5562	[Participant did not return results for this question.]
9GULT8-5562	EE010683ABE27680DB634FD1AA00AEA493820EF057C1DEE7D528FA55F123D85C
AQYVXC-5562	EE010683ABE27680DB634FD1AA00AEA493820EF057C1DEE7D528FA55F123D85C
AV4RGC-5562	ee010683abe27680db634fd1aa00aea493820ef057c1dee7d528fa55f123d85c
BR6KUT-5562	EE010683ABE27680DB634FD1AA00AEA493820EF057C1DEE7D528FA55F123D85C
CBTGPD-5562	EE010683ABE27680DB634FD1AA00AEA493820EF057C1DEE7D528FA55F123D85C
CQ9KB9-5562	EE010683ABE27680DB634FD1AA00AEA493820EF057C1DEE7D528FA55F123D85C
CZCW7G-5562	ee010683abe27680db634fd1aa00aea493820ef057c1dee7d528fa55f123d85c
FFG39B-5562	ee01 0683 abe2 7680 db63 4fd1 aa00 aea4 9382 0ef0 57c1 dee7 d528 fa55 f123 d85c
FJWWP9-5562	[Participant did not return results for this question.]
FP3BPR-5562	EE010683ABE27680DB634FD1AA00AEA493820EF057C1DEE7D528FA55F123D85C
JF4GTB-5562	ee010683abe27680db634fd1aa00aea493820ef057c1dee7d528fa55f123d85c

TABLE 2: Removable Media Device Results

Question 37	
WebCode - Test	**Response**
JJJA4W-5562	EE010683ABE27680DB634FD1AA00AEA493820EF057C1DEE7D528FA55F123D85C
K6Z7V8-5562	EE010683ABE27680DB634FD1AA00AEA493820EF057C1DEE7D528FA55F123D85C
KH3MYM-5562	EE010683ABE27680DB634FD1AA00AEA493820EF057C1DEE7D528FA55F123D85C
KT78B9-5562	ee010683abe27680db634fd1aa00aea493820ef057c1dee7d528fa55f123d85c
L9D7RX-5562	ee010683abe27680db634fd1aa00aea493820ef057c1dee7d528fa55f123d85c
LEERBL-5562	SHA1 hash did not match that shown on this question.
LRRLAT-5562	ee010683abe27680db634fd1aa00aea493820ef057c1dee7d528fa55f123d85c
M98EB2-5562	EE010683ABE27680DB634FD1AA00AEA493820EF057C1DEE7D528FA55F123D85C
MWHHA4-5562	EE010683ABE27680DB634FD1AA00AEA493820EF057C1DEE7D528FA55F123D85C
MYJKY6-5562	EE010683ABE27680DB634FD1AA00AEA493820EF057C1DEE7D528FA55F123D85C
NFQ2KX-5562	EE010683ABE27680DB634FD1AA00AEA493820EF057C1DEE7D528FA55F123D85C
NUKNP6-5562	99F17261FA644AC7665321CBDEF7C0879387C766DA56B784BBCC60DED02F99F0
PTA4GV-5562	ee010683abe27680db634fd1aa00aea493820ef057c1dee7d528fa55f123d85c
RAQR4V-5562	EE010683ABE27680DB634FD1AA00AEA493820EF057C1DEE7D528FA55F123D85C
T8F7TZ-5562	20E5856E0BB8FF08E57F1C3554BEFC41236811E8AD521B12AB92B1ACA465CFF8
U964DC-5562	91533431a4dc0b2da06659f45708eb93ddfe8c7d441815a024e6554806a121a0
X436QC-5562	9B51243F97864480FD97D598CD0100DA3BE81C748B730F2EC1F822EA7C5A3E91
X4L22Q-5562	ee010683abe27680db634fd1aa00aea493820ef057c1dee7d528fa55f123d85c

Question 37: The SHA1 hash for the USB device is F3C33632CD03525ECC4B07362AC5196DA5F02262. Provide the SHA256 hash for the USB device.

Consensus Result:
EE010683ABE27680DB634FD1AA00AEA493820EF057C1DEE7D528FA55F123D85C

Expected Response Explanation:
Attaching the USB device to a computer with either hardware or software write blocking and hashing provides the correct hash value.

TABLE 2: Removable Media Device Results

Question 37

Expected Response Illustration:

HxD Hex Editor tool used for Device Hashing (SHA256)

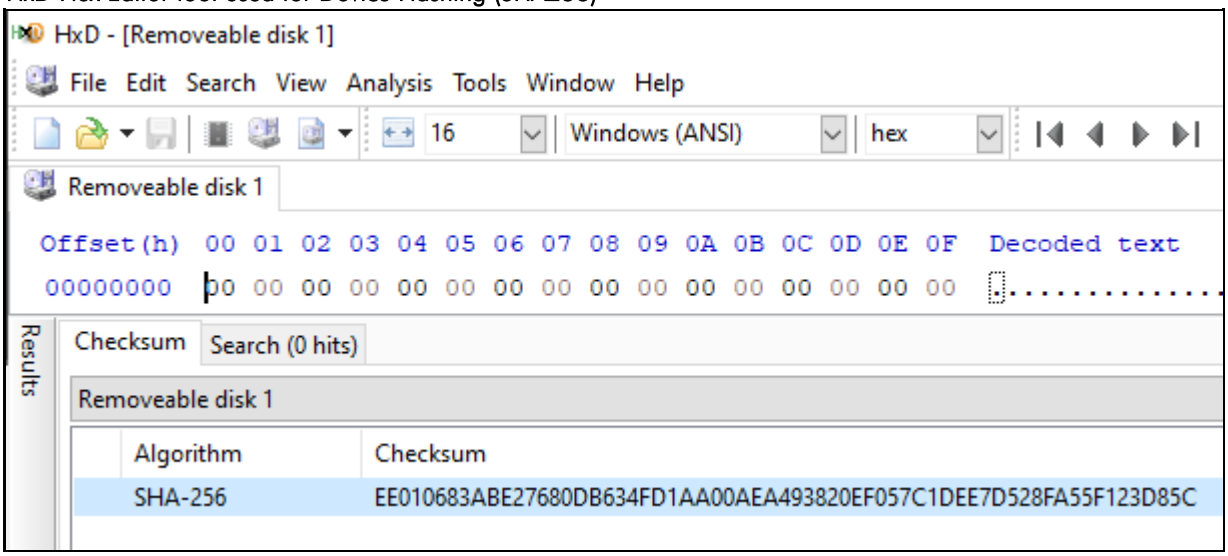


TABLE 2: Removable Media Device Results

Question 38

Question 38: How many partitions are on the USB device? Provide a NUMERIC response (e.g., 1, 2, 3).

Manufacturer's Expected Response:

2

WebCode - Test	Response
29JUMG-5562	2. One of them is encrypted
2YBWJR-5562	2
67H6N6-5562	2
6G29KN-5562	2
6N3QEM-5562	2
7FMAEZ-5562	2
7W9P7F-5562	2
8UH9ME-5562	2
93AL3L-5562	2
9GULT8-5562	2
AQYVXC-5562	2
AV4RGC-5562	2
BR6KUT-5562	2
CBTGPD-5562	2
CQ9KB9-5562	2
CZCW7G-5562	2
FFG39B-5562	2
FJWWP9-5562	2
FP3BPR-5562	2
JF4GTB-5562	2
JJJA4W-5562	2
K6Z7V8-5562	2
KH3MYM-5562	2

TABLE 2: Removable Media Device Results

Question 38

WebCode - Test	Response
KT78B9-5562	2
L9D7RX-5562	Two (02) partitions
LEERBL-5562	2
LRRLAT-5562	2
M98EB2-5562	2
MWHHA4-5562	2
MYJKY6-5562	2
NFQ2KX-5562	2
NUKNP6-5562	2
PTA4GV-5562	02
RAQR4V-5562	2
T8F7TZ-5562	2
U964DC-5562	2
X436QC-5562	1
X4L22Q-5562	2

Question 38: How many partitions are on the USB device? Provide a NUMERIC response (e.g., 1, 2, 3).

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:

FTK Imager view of partitions

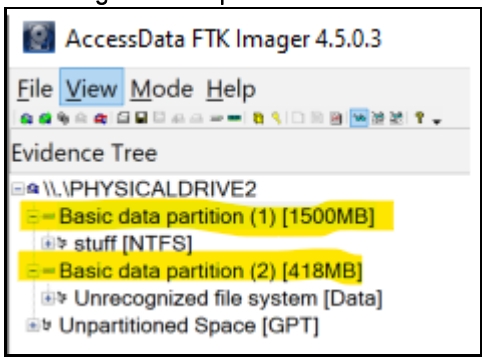


TABLE 2: Removable Media Device Results

Question 38

EnCase Report of Drive Geometry

Partitions

Name	Id	Type	Start Sector	Total Sectors	Size
Basic data partition	07	NTFS	128	3,072,000	1.5 GB
Basic data partition	07	NTFS	3,072,128	856,064	418 MB

TABLE 2: Removable Media Device Results

Question 39

Question 39: 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:

4A0C-3885

WebCode - Test	Response
29JUMG-5562	4A0C3885
2YBWJR-5562	0x4A0C3885
67H6N6-5562	4A0C3885
6G29KN-5562	0x 4A 0C 38 85
6N3QEM-5562	4A0C
7FMAEZ-5562	4A0C-3885
7W9P7F-5562	4A0C-3885
8UH9ME-5562	4A0C3885
93AL3L-5562	4A0C-3885
9GULT8-5562	4A0C
AQYVXC-5562	4A0C3885
AV4RGC-5562	4A0C3885
BR6KUT-5562	4A0C-3885
CBTGPD-5562	4A0C3885
CQ9KB9-5562	4A0C
CZCW7G-5562	4A0C
FFG39B-5562	4A0C-3885
FJWWP9-5562	4A0C3885 - EB 52 90 4E
FP3BPR-5562	4A 0C 38 85
JF4GTB-5562	4A0C3885
JJJA4W-5562	4A0C3885
K6Z7V8-5562	4A0C3885

TABLE 2: Removable Media Device Results

Question 39	
WebCode - Test	**Response**
KH3MYM-5562	480C-3885
KT78B9-5562	4A0C3885
L9D7RX-5562	4A0C3885
LEERBL-5562	4A 0C 38 85
LRRLAT-5562	4A0C-3885
M98EB2-5562	85380C4A
MWHHA4-5562	4A0C3885
MYJKY6-5562	4A0C3885
NFQ2KX-5562	85380C4A (4A0C3885)
NUKNP6-5562	4A0C-3885
PTA4GV-5562	4A0C-3885
RAQR4V-5562	4A0C3885
T8F7TZ-5562	4A0C3885
U964DC-5562	00 01 F4 00 - Volume Serial Number = 4A0C-3885
X436QC-5562	82 4A 0C 45
X4L22Q-5562	4A0C3885 – volume serial

Question 39: 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:

4A0C-3885

Participants who reported the volume serial number in big endian 85380C4A were also included as part of the consensus.

Expected Response Explanation:

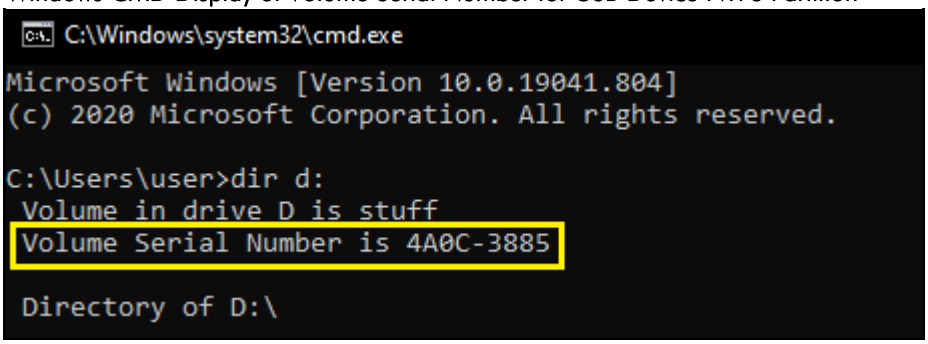
Most forensic tools will parse and display the volume serial number value. It can also be displayed by the operating system for a mounted volume.

TABLE 2: Removable Media Device Results

Question 39

Expected Response Illustration:

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



EnCase Display of Volume Serial Number for USB Device NTFS Partition

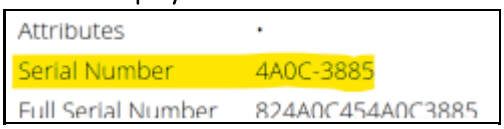


TABLE 2: Removable Media Device Results

Question 40

Question 40: What is the name (Volume Label) of the NTFS Partition?

Manufacturer's Expected Response:

stuff

WebCode - Test	Response
29JUMG-5562	stuff
2YBWJR-5562	stuff
67H6N6-5562	stuff
6G29KN-5562	stuff
6N3QEM-5562	stuff
7FMAEZ-5562	Stuff
7W9P7F-5562	stuff
8UH9ME-5562	stuff
93AL3L-5562	stuff
9GULT8-5562	stuff
AQYVXC-5562	stuff
AV4RGC-5562	stuff
BR6KUT-5562	stuff
CBTGPD-5562	stuff
CQ9KB9-5562	Stuff
CZCW7G-5562	stuff
FFG39B-5562	stuff
FJWWP9-5562	stuff
FP3BPR-5562	stuff
JF4GTB-5562	stuff
JJJA4W-5562	stuff
K6Z7V8-5562	stuff
KH3MYM-5562	stuff

TABLE 2: Removable Media Device Results

Question 40	
WebCode - Test	**Response**
KT78B9-5562	stuff
L9D7RX-5562	stuff
LEERBL-5562	stuff
LRRLAT-5562	stuff
M98EB2-5562	stuff
MWHHA4-5562	Stuff
MYJKY6-5562	stuff
NFQ2KX-5562	stuff
NUKNP6-5562	stuff
PTA4GV-5562	stuff
RAQR4V-5562	stuff
T8F7TZ-5562	stuff
U964DC-5562	stuff
X436QC-5562	stuff
X4L22Q-5562	Stuff

Question 40: What is the name (Volume Label) of the NTFS Partition?

Consensus Result:
stuff

Expected Response Explanation:
NTFS volumes can have a name. The Windows operating system as well as many other forensic tools will display the name.

TABLE 2: Removable Media Device Results

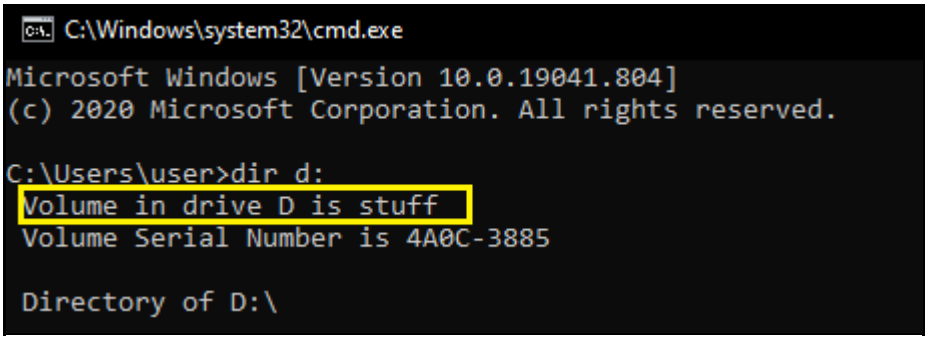
Question 40

Expected Response Illustration:

EnCase drive information report

Volume	
File System	NTFS
Sectors per cluster	8
Bytes per sector	512
Total Sectors	3,072,000
Total Capacity	1,572,859,904 Bytes (1.5 GB)
Total Clusters	383,999
Unallocated	605,437,952 Bytes (577.4 MB)
Free Clusters	147,812
Allocated	967,421,952 Bytes (922.6 MB)
Volume Name	stuff
Volume Offset	128
Drive Type	Fixed

Windows CMD Display of Volume name for USB Device NTFS Partition



Explorer Display of Volume name USB Device NTFS Partition

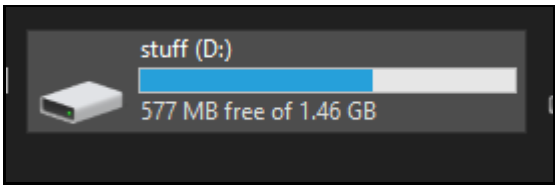


TABLE 2: Removable Media Device Results

Question 41

Question 41: What number is visible in the file with SHA1 hash 6b5fc1a4273ff607974492ce6c40a34db1e6ec69?

Manufacturer's Expected Response:

64

WebCode - Test	Response
29JUMG-5562	64. El número 64 es visualizado cuando se reproduce el fichero PA100163.MOV.
2YBWJR-5562	64
67H6N6-5562	64
6G29KN-5562	64
6N3QEM-5562	64
7FMAEZ-5562	64
7W9P7F-5562	64
8UH9ME-5562	64
93AL3L-5562	64 - on the red buoy in the water
9GULT8-5562	64
AQYVXC-5562	64
AV4RGC-5562	64
BR6KUT-5562	64
CBTGPD-5562	64
CQ9KB9-5562	61
CZCW7G-5562	64
FFG39B-5562	64
FJWWP9-5562	64
FP3BPR-5562	64
JF4GTB-5562	64
JJJA4W-5562	64
K6Z7V8-5562	100163

TABLE 2: Removable Media Device Results

Question 41	
WebCode - Test	**Response**
KH3MYM-5562	64
KT78B9-5562	64
L9D7RX-5562	64
LEERBL-5562	64
LRRLAT-5562	64
M98EB2-5562	64
MWHHA4-5562	64
MYJKY6-5562	64
NFQ2KX-5562	64
NUKNP6-5562	64
PTA4GV-5562	64
RAQR4V-5562	64
T8F7TZ-5562	64
U964DC-5562	64
X436QC-5562	64
X4L22Q-5562	64

Question 41: What number is visible in the file with SHA1 hash 6b5fc1a4273ff607974492ce6c40a34db1e6ec69?

Consensus Result:
64

Expected Response Explanation:
There is one file on the device with the given hash, PA100163.MOV, a QuickTime movie file in the root directory of the NTFS partition. Viewing this video in a media player shows the view from a sailboat approaching a channel marker. At approximately 45 seconds into the video, the number 64 becomes visible on the marker.

TABLE 2: Removable Media Device Results

Question 41

Expected Response Illustration:

Encase table pane showing filename and SHA1 Hash

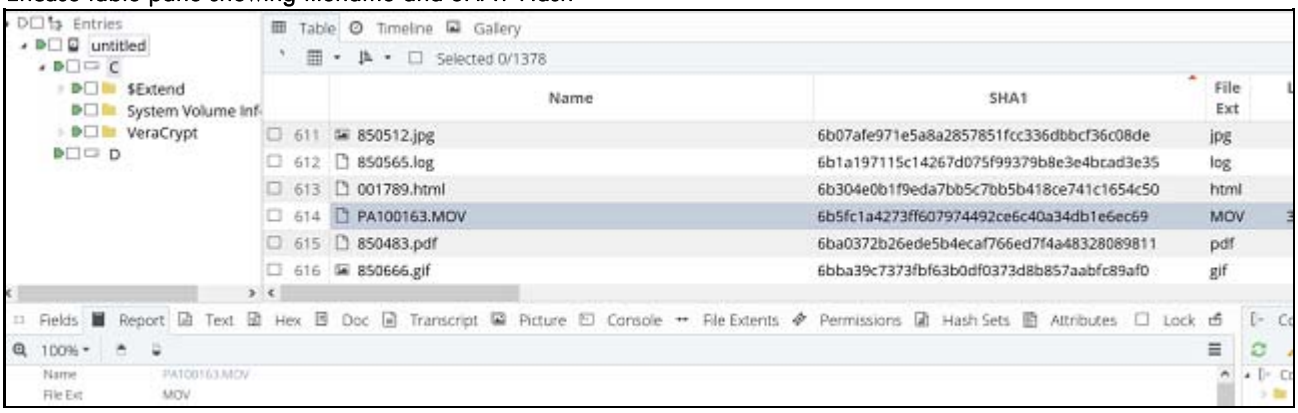


Image captured from movie displayed in Windows Movies & TV

TABLE 2: Removable Media Device Results

Question 42

Question 42: What do the differences in the filesystem metadata between lscg16kho8i61.jpg and lscg16kho8i61 - Copy.jpg indicate?

Manufacturer's Expected Response:

The copy was created on a different computer than the original.

WebCode - Test	Response ** Inconsistencies not highlighted; No consensus achieved **
29JUMG-5562	Los metadatos referidos a las fechas de Modificación, Acceso y Creación son diferentes. En las fechas de acceso y creación, podemos apreciar como el último acceso de "lscg16kho8i61.jpg" coincide prácticamente con los valores de acceso y creación de "lscg16kho8i61 - Copy.jpg". Con lo que vemos la coincidencia de que dicha copia se realizó y renombró automáticamente el 08/03/2021 3:15:39. "lscg16kho8i61.jpg": creacion: 07/03/2021 3:05:28 | acceso: 08/03/2021 3:15:35 | modificacion: 14/02/2019 1:11:30. "lscg16kho8i61 - Copy.jpg": creacion: 08/03/2021 3:15:39 | acceso: 08/03/2021 3:15:39 | modificacion: 14/02/2019 1:11:30
2YBWJR-5562	The [Laboratory] does not include this information on the report and is outside the scope of our normal reporting procedures
67H6N6-5562	created time: lscg16kho8i61.jpg-2021-03-07 03:05:28 / lscg16kho8i61 - Copy.jpg - 201-03-08 03:15:39
6G29KN-5562	The differences in the file system metadata indicate an exact copy of the file named “lscg16kho8i61.jpg” was created on Item 1 approximately one (1) day after the original file was saved to the device, as the entry modified data precedes the file creation date by approximately 24 hours for the file named “lscg16kho8i61 - Copy.jpg”. The files are exact copies as their MD5 and SHA hash values are identical. The file “lscg16kho8i61.jpg” appear to have been copied to the device from another location, as the modified date precedes the created date by over 2 years.
6N3QEM-5562	The created time of the files is different. The file lscg16kho8i61.jpg is created on 07/03/2021 07:05:28 (2021-03-07 03:05:28 UTC) and the file lscg16kho8i61 - Copy.jpg is created on 08/03/2021 07:15:39 (2021-03-08 03:15:39 UTC).
7FMAEZ-5562	User has changed the Date / Time on the system
7W9P7F-5562	The copy was created the next day
8UH9ME-5562	lscg16kho8i61.jpg is a symlink file created on the drive first, lscg16kho8i61 - Copy.jpg is an active file created the next day
93AL3L-5562	[Participant did not return results for this question.]
9GULT8-5562	The user made a copy of the file in the same directory; differences are only in the file name and file system’s metadata.
AQYVXC-5562	That lscg16kho8i61.jpg was original file downloaded and saved from Reddit on 07/03/2021 03:05:28. The same file was then accessed at 08/03/2021 03:15:35 to create a copy of the same file 'lscg16kho8i61 - Copy.jpg' which was created at 08/03/2021 03:15:39 and no longer shows reddit as the source
AV4RGC-5562	Created times are different. (lscg16kho8i61.jpg 03.7.2021 03:05:28) (lscg16kho8i61 - Copy.jpg 03.8.2021 03:15:39)
BR6KUT-5562	That this image is evidentially the same with matching hashes, size and dimensions. The only differences are the dates (and names) indicating this image was copied using the operating system. (i.e. copy and paste with Windows OS appending – copy to end). Last Modified = same. Created = more recent in copy. Last Accessed = more recent in copy.
CBTGPD-5562	That the copy was made a day after the original file was created
CQ9KB9-5562	That the original jpeg has been copied into the same location the following day.
CZCW7G-5562	The created time of the files is different the file lscg16kho8i61.jpg is created on 07/03/2021 07:05:28 (2021-03-07 03:05:28 UTC) and the file lscg16kho8i61 - Copy.jpg is created on 08/03/2021 07:15:39 (2021-03-08 03:15:39 UTC)

TABLE 2: Removable Media Device Results

Question 42

WebCode - Test	Response ** Inconsistencies not highlighted; No consensus achieved **
FFG39B-5562	file "lscg16kho8i61.jpg" was copied creating "lscg16kho8i61 - Copy.jpg" at 03/08/2021 03:15:39 AM UTC +0 (8th March 2021)
FJWWP9-5562	File lscg16kho8i61 – Copy.jpeg is a copy of file lscg16kho8i61.jpg and was created 08/03/2021 03:15:39
FP3BPR-5562	The differences between the files lscg16kho8i61.jpg and lscg16kho8i61 - Copy.jpg indicate that the file has been copied from a domain connected computer to the USB device. The difference in file system metadata between the files lscg16kho8i61.jpg and lscg16kho8i61 - Copy.jpg show that the file named lscg16kho8i61 - Copy.jpg has permissions set that allow access to domain users. The file named lscg16kho8i61.jpg has permissions set that allow access for a user named susie. The copy jpg file was created on the USB device on 08.03.2021 and the lscg16kho8i61.jpg file was created on the computer on 09.03.2021 indicating that the USB device has been used to copy a file from a domain connected computer and then that file was transferred to the standalone computer with the user account susie present. Further analysis shows that a 3rd file bearing the name lscg16kho8i61.jpg was located on the USB device and this file was created on 07.03.2021; lscg16kho8i61.jpg (from USB Stick) | Created: 07.03.2021 lscg16kho8i61 - Copy.jpg (From USB Stick) | Created: 08.03.2021 lscg16kho8i61.jpg (From Computer) | Created: 09.09.2020 Conclusion therefore that this file existed on the computer first, it was then copied to the USB stick and then copied to a domain connected computer before being copied back to the USB stick.
JF4GTB-5562	A copy of the file lscg16kho8i61.jpg was created on 3/7/2021
JJJA4W-5562	One is a copy of the other
K6Z7V8-5562	lscg16kho8i61.jpg was created on 03/07/2021 03:05:28 and copied to the same location on 03/08/2021 03:15:39 and renamed to lscg16kho8i61 - Copy.jpg
KH3MYM-5562	Object identifiers are present on the original but not on the copy
KT78B9-5562	lscg16kho8i61.jpg: Created Date/Time 07.03.2021 04:05:28; Last Accesed Date/Time 08.03.2021 04:15:35 lscg16kho8i61 - Copy.jpg: Created Date/Time 08.03.2021 04:15:39; Last Accesed Date/Time 08.03.2021 04:15:39
L9D7RX-5562	The differences in Dates/Times indicate that the “lscg16kho8i61 - Copy.jpg” file was created by the copy and paste operations of the “lscg16kho8i61.jpg” file at the same place
LEERBL-5562	That lscg16kho8i61.jpg was copied at 03/08/2021 03:15:39
LRRLAT-5562	‘lscg16kho8i61 - Copy.jpg’ was created at 03:15 on 08-Mar-2021, as ‘lscg16kho8i61.jpg’ was already in existence (created 03:05 on 07-Mar-2021) it had to be renamed to avoid two files with the same name.
M98EB2-5562	It was copied around 24 hours later
MWHHA4-5562	A copy of the file was made in the same location just over 24hrs after originally being created on the device in that same location.
MYJKY6-5562	An exact copy of lscg16kho8i61.jpg was created and stored within the same directory at 04:15 on 08/03/2021. The filename was automatically assigned by the system as a 'copy'.
NFQ2KX-5562	just have been made a copy without opening
NUKNP6-5562	Different "File Creation" and "File Read" dates and times.
PTA4GV-5562	lscg16kho8i61.jpg was created on (03/07/2021) and lscg16kho8i61 - Copy.jpg was created as a copy of lscg16kho8i61.jpg on (03/08/2021).
RAQR4V-5562	The file was copied on 08/03/2021 03:15:39
T8F7TZ-5562	The attributes are different in that the SID is different and no owner shown indicating that the picture has been on another computer.

TABLE 2: Removable Media Device Results

Question 42	
WebCode - Test	**Response** ** Inconsistencies not highlighted; No consensus achieved **
U964DC-5562	The difference between the two files is the file created time. The copy was created a day later than the original. This means that the file was copied and pasted creating a new MFT record for the copied file. The filename also has the addition of "- Copy.jpg" when the file is pasted into the same volume/folder as the original.
X436QC-5562	The naming convention indicates file 'lscg16kho8i61.jpg' has been copied and pasted back into the same folder, hence the inclusion of the text ' - Copy' in its filename. The 'lscg16kho8i61.jpg' has a created date of 03/07/2021 whereas the 'lscg16kho8i61 - Copy.jpg' has a creation date of 03/08/2021.
X4L22Q-5562	Hashes are the same so the information within the image was not changed. lscg16kho8i61.jpg was created first and on 3/8/2021, it was accessed in order to created lscg16kho8i61 - Copy.jpg. The last accessed date for lscg16kho8i61.jpg matches the created date for lscg16kho8i61 - Copy.jpg.

Question 42: What do the differences in the filesystem metadata between lscg16kho8i61.jpg and lscg16kho8i61 - Copy.jpg indicate?

Consensus Result:

A consensus was not achieved for this question. The objective of this question was for the examiner to draw conclusions from the metadata.

Expected Response Explanation:

The NTFS permissions show the owner of the files as:
lscg16kho8i61.jpg S-1-5-21-1943064195-990424342-2473957490-1001; and
lscg16kho8i61 - Copy.jpg S-1-5-21-3190731067-2237959463-3261579367-1001
The differing machine identifiers (highlighted below) indicate the files were created by different computers. lscg16kho8i61.jpg was created by the user (susie) on the 21-5561 subject computer. The 'copy' was created by a user on another computer.

Expected Response Illustration:

EnCase table and view panes showing permissions metadata for lscg16kho8i61.jpg and lscg16kho8i61 - Copy.jpg

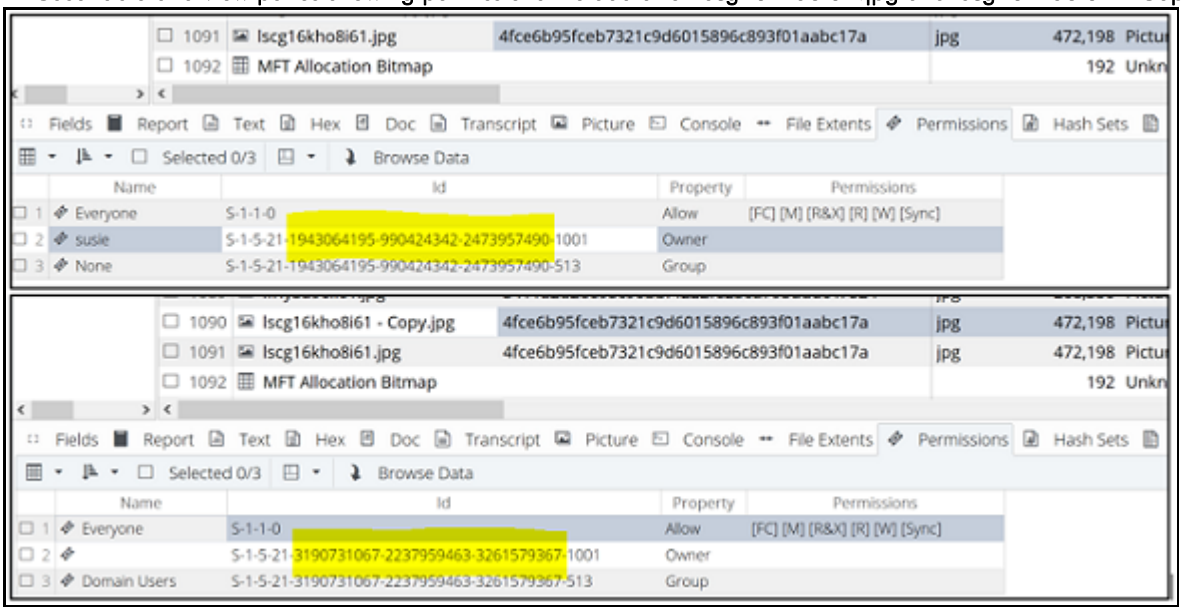


TABLE 2: Removable Media Device Results

Question 42

Autopsy table showing permissions metadata for lscg16kho8i61.jpg and lscg16kho8i61- Copy.jpg

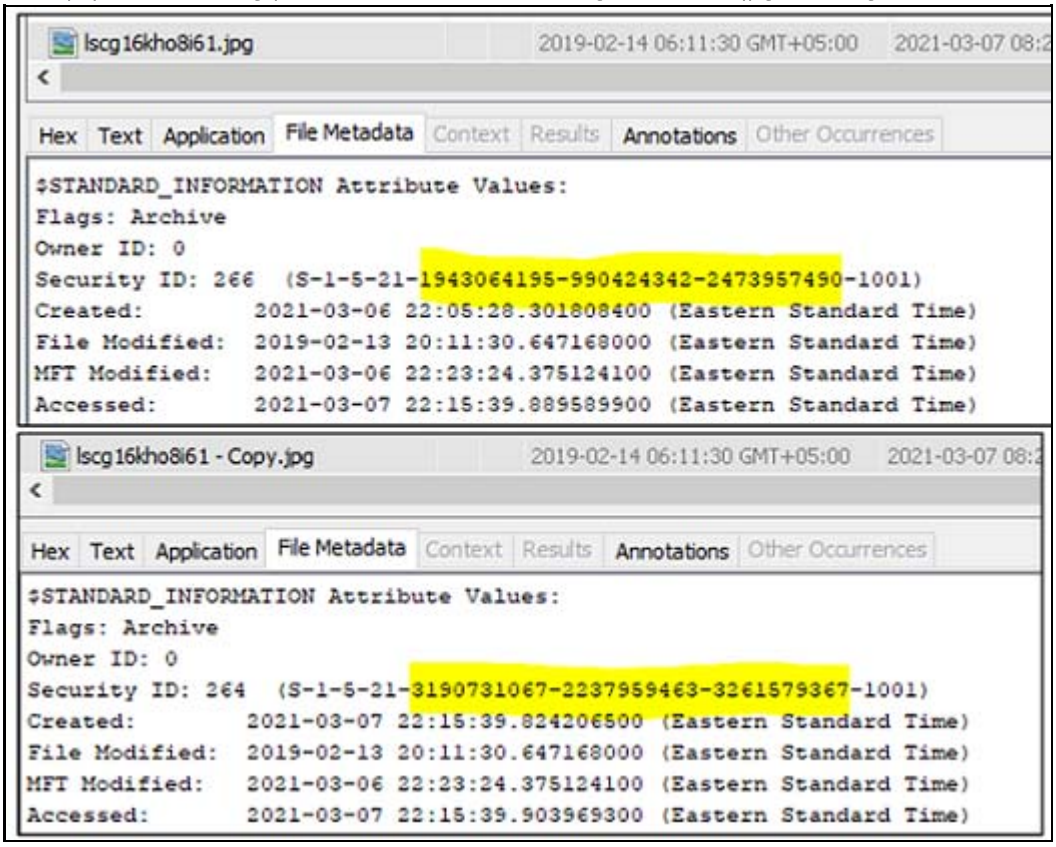


TABLE 2: Removable Media Device Results

Question 43

Question 43: What is the name of the file in the root directory of the NTFS volume with header 89 50 4E 47?

Manufacturer's Expected Response:

850785.png

WebCode - Test	Response
29JUMG-5562	bank_30x30.png (C\VeraCrypt\docs\html\en\bank_30x30.png)
2YBWJR-5562	850785.png
67H6N6-5562	850785.png
6G29KN-5562	850785.png
6N3QEM-5562	850785.png
7FMAEZ-5562	850785.png
7W9P7F-5562	850785.png
8UH9ME-5562	850785.jpg
93AL3L-5562	This file is a png.file 850785.png
9GULT8-5562	850785.png
AQYVXC-5562	850785.png
AV4RGC-5562	850785.png
BR6KUT-5562	850785.png
CBTGPD-5562	850785.png
CQ9KB9-5562	850785.png
CZCW7G-5562	850785.png
FFG39B-5562	850785.png
FJWWP9-5562	850785.png
FP3BPR-5562	850785.png
JF4GTB-5562	850785.PNG
JJJA4W-5562	850785.png
K6Z7V8-5562	850785.png
KH3MYM-5562	850785.png

TABLE 2: Removable Media Device Results

Question 43	
WebCode - Test	**Response**
KT78B9-5562	850785.png
L9D7RX-5562	850785.png
LEERBL-5562	850785.png
LRRLAT-5562	850785.png
M98EB2-5562	bank_30x30.png
MWHHA4-5562	850785.png
MYJKY6-5562	850785.png
NFQ2KX-5562	bank_30x30.png
NUKNP6-5562	850785.png
PTA4GV-5562	850785.png
RAQR4V-5562	850785.png
T8F7TZ-5562	850785.png
U964DC-5562	850785.png
X436QC-5562	850785.png
X4L22Q-5562	850785.png

Question 43: What is the name of the file in the root directory of the NTFS volume with header 89 50 4E 47?

Consensus Result:
850785.png

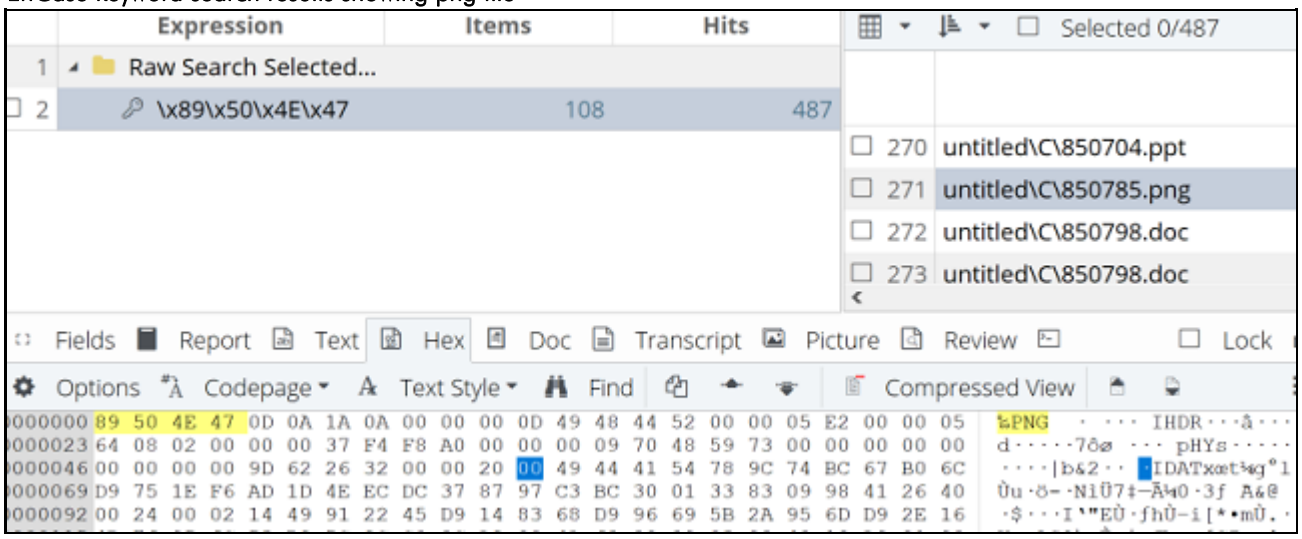
Expected Response Explanation:
89 50 4E 47 is the header for a Portable Network Graphic (.png) file. A keyword search for this hex value will find one .png file, 850785.png in the root directory.

TABLE 2: Removable Media Device Results

Question 43

Expected Response Illustration:

EnCase keyword search results showing png file



Autopsy hex view of 850785.png

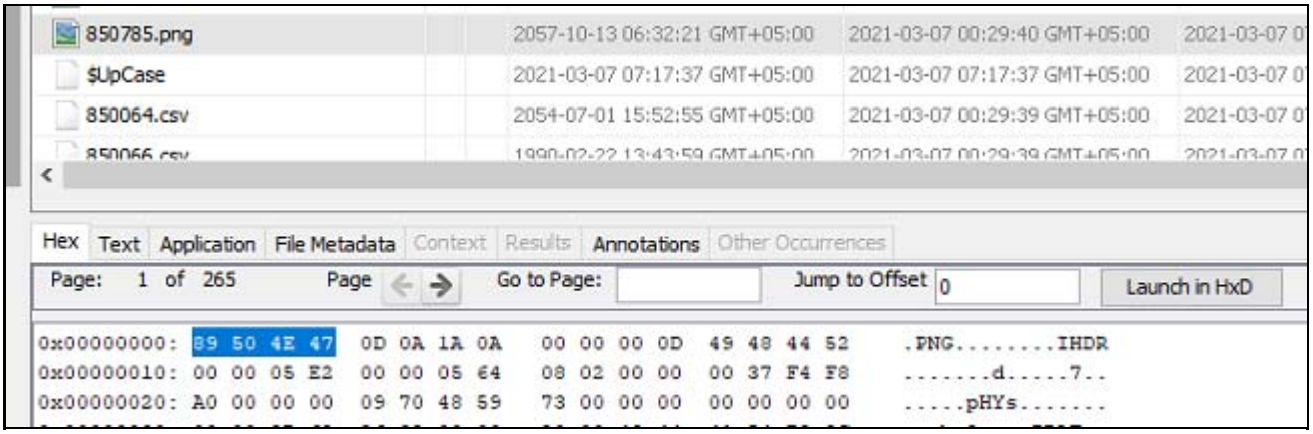


TABLE 2: Removable Media Device Results

Question 44

Question 44: Who is the author of 850009.xls?

Manufacturer's Expected Response:

shuga001

WebCode - Test	Response
29JUMG-5562	Authors : shuga001. Last Author: malon315.
2YBWJR-5562	shuga001
67H6N6-5562	shuga001
6G29KN-5562	shuga001
6N3QEM-5562	shuga001
7FMAEZ-5562	shuga001
7W9P7F-5562	shuga001
8UH9ME-5562	shuga001
93AL3L-5562	shuga001
9GULT8-5562	shuga001
AQYVXC-5562	shuga001
AV4RGC-5562	shuga001
BR6KUT-5562	shuga001
CBTGPD-5562	Original author: shuga001, last modified by: malon315
CQ9KB9-5562	shuga001
CZCW7G-5562	shuga001
FFG39B-5562	shuga001
FJWWP9-5562	shuga001
FP3BPR-5562	The author of 850009.xls was shown as 'shuga001' however the last author was shown as 'malon315'
JF4GTB-5562	shuga001
JJJA4W-5562	shuga001
K6Z7V8-5562	shuga001. Last author malon315
KH3MYM-5562	shuga001

TABLE 2: Removable Media Device Results

Question 44	
WebCode - Test	**Response**
KT78B9-5562	shuga001
L9D7RX-5562	shuga001
LEERBL-5562	shuga001 Last author malon315
LRRLAT-5562	shuga001
M98EB2-5562	shuga001
MWHHA4-5562	Shuga001
MYJKY6-5562	shuga001
NFQ2KX-5562	shuga001 & malon315 (last author)
NUKNP6-5562	shuga001
PTA4GV-5562	shuga001
RAQR4V-5562	shuga001
T8F7TZ-5562	shuga001 - Last Author malon315
U964DC-5562	shuga001
X436QC-5562	shuga001
X4L22Q-5562	shuga001

Question 44: Who is the author of 850009.xls?

Consensus Result:
shuga001

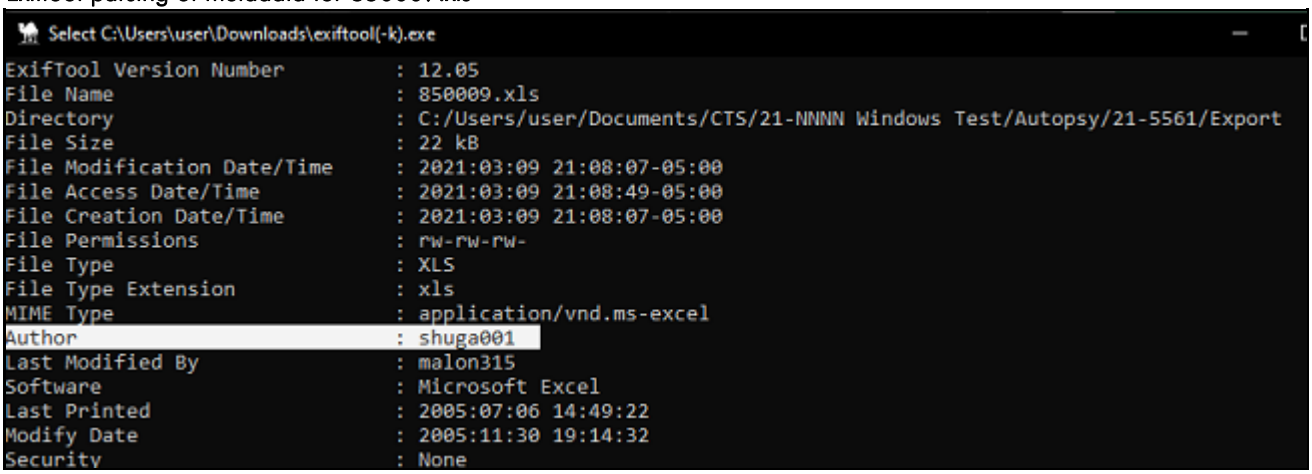
Expected Response Explanation:
Microsoft Office document metadata can be viewed with a tool such as Exiftool or by opening with the native office application.

TABLE 2: Removable Media Device Results

Question 44

Expected Response Illustration:

Exiftool parsing of metadata for 850009.xls



Microsoft Excel display of information for 850009.xls

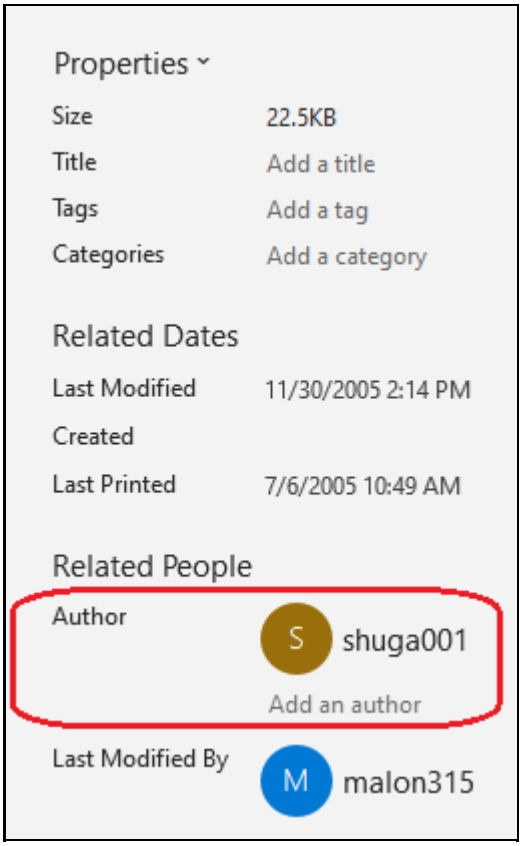


TABLE 2: Removable Media Device Results

Question 45

Question 45: In unallocated space on this device is a deleted photo of a black kitten with blue eyes. What is the SHA1 hash of this file?

Manufacturer's Expected Response:

3843fe118e1f55cc4d3d7f8cede8f3aeb2793e00

WebCode - Test	Response
29JUMG-5562	3843fe118e1f55cc4d3d7f8cede8f3aeb2793e00
2YBWJR-5562	3843fe118e1f55cc4d3d7f8cede8f3aeb2793e00
67H6N6-5562	3843fe118e1f55cc4d3d7f8cede8f3aeb2793e00
6G29KN-5562	3843fe118e1f55cc4d3d7f8cede8f3aeb2793e00
6N3QEM-5562	3843fe118e1f55cc4d3d7f8cede8f3aeb2793e00
7FMAEZ-5562	3843fe118e1f55cc4d3d7f8cede8f3aeb2793e00
7W9P7F-5562	3843fe118e1f55cc43d37f8cede8f3aeb2793e00
8UH9ME-5562	3843fe118e1f55cc4d3d7f8cede8f3aeb2793e00
93AL3L-5562	3843fe118e1f55cc4d3d7f8cede8f3aeb2793e00
9GULT8-5562	3843fe118e1f55cc4d3d7f8cede8f3aeb2793e00
AQYVXC-5562	3843FE118E1F55CC4D3D7F8CEDE8F3AEB2793E00
AV4RGC-5562	3843fe118e1f55cc4d3d7f8cede8f3aeb2793e00
BR6KUT-5562	3843FE118E1F55CC4D3D7F8CEDE8F3AEB2793E00
CBTGPD-5562	3843fe118e1f55cc4d3d7f8cede8f3aeb2793e00
CQ9KB9-5562	3843FE118E1F55CC4D3D7F8CEDE8F3AEB2793E00
CZCW7G-5562	3843fe118e1f55cc4d3d7f8cede8f3aeb2793e00
FFG39B-5562	3843fe118e1f55cc4d3d7f8cede8f3aeb2793e00
FJWWP9-5562	3843fe118e1f55cc4d3d7f8cede8f3aeb2793e00
FP3BPR-5562	3843FE118E1F55CC4D3D7F8CEDE8F3AEB2793E00
JF4GTB-5562	3843fe118e1f55cc4d3d7f8cede8f3aeb2793e00
JJJA4W-5562	3843FE118E1F55CC4D3D7F8CEDE8F3AEB2793E00
K6Z7V8-5562	3843fe118e1f55cc4d3d7f8cede8f3aeb2793e00

TABLE 2: Removable Media Device Results

Question 45	
WebCode - Test	**Response**
KH3MYM-5562	3843FE118E1F55CC4D3D7F8CEDE8F3AEB2793E00
KT78B9-5562	3843fe118e1f55cc4d3d7f8cede8f3aeb2793e00
L9D7RX-5562	3843fe118e1f55cc4d3d7f8cede8f3aeb2793e00
LEERBL-5562	3843fe118e1f55cc4d3d7f8cede8f3aeb2793e00
LRRLAT-5562	3843fe118e1f55cc4d3d7f8cede8f3aeb2793e00
M98EB2-5562	3843FE118E1F55CC4D3D7F8CEDE8F3AEB2793E00
MWHHA4-5562	3843fe118e1f55cc4d3d7f8cede8f3aeb2793e00
MYJKY6-5562	3843FE118E1F55CC4D3D7F8CEDE8F3AEB2793E00
NFQ2KX-5562	3843fe118e1f55cc4d3d7f8cede8f3aeb2793e00
NUKNP6-5562	1C80BBAC0AC5AF952A0D0AA2A39BD86C3BAE4204
PTA4GV-5562	3843fe118e1f55cc4d3d7f8cede8f3aeb2793e00
RAQR4V-5562	3843fe118e1f55cc4d3d7f8cede8f3aeb2793e00
T8F7TZ-5562	3843fe118e1f55cc4d3d7f8cede8f3aeb2793e00
U964DC-5562	3843FE118E1F55CC4D3D7F8CEDE8F3AEB2793E00
X436QC-5562	3843fe118e1f55cc4d3d7f8cede8f3aeb2793e00
X4L22Q-5562	3843fe118e1f55cc4d3d7f8cede8f3aeb2793e00

Question 45: In unallocated space on this device is a deleted photo of a black kitten with blue eyes. What is the SHA1 hash of this file?

Consensus Result:
3843fe118e1f55cc4d3d7f8cede8f3aeb2793e00

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. Use of a hashing utility may be required to calculate the SHA1 digest of the recovered file.

TABLE 2: Removable Media Device Results

Question 45

Expected Response Illustration:

deleted jpg file recovered from unallocated space

7zip checksum utility SHA1 output for recovered file

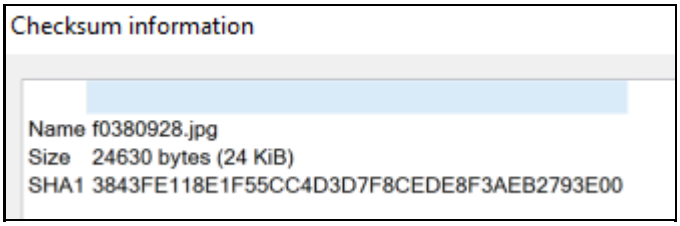


TABLE 2: Removable Media Device Results

Question 46

Question 46: What indications, if any, suggest this device was "sterilized" prior to use?

Manufacturer's Expected Response:

The unallocated space on the device was overwritten with a pattern, "CTS_FORENSICS_"

WebCode - Test	Response
29JUMG-5562	Existe un patron que se repite en ciertas partes de la imagen con valor 4354535F464F52454E534943535F (CTS_FORENSICS_), lo cual parece indicar que al dispositivo se le practicó un borrado seguro (wipe) estableciendo ese patrón repetido para el borrado.
2YBWJR-5562	Evidence of manually overwriting data in the file system partition where data such as "CTS_FORENSICS" would normally not exist.
67H6N6-5562	The "CTS_FORENSICS_" pattern was continuously written in the unallocated area.
6G29KN-5562	Portions of the free/unallocated space of both of the partitions located on the device had been overwritten with "FORENSICS_CTS_" repeatedly, which would not typically exist on a piece of media unless someone intentionally overwrote and/or sterilized the media with that custom data.
6N3QEM-5562	The device has a partition with hex value "CTS_FORENSICS" which means it has been over written and sterilized.
7FMAEZ-5562	On 07/03/2021 at 02:17 a link file is created to D:\Stuff – Removable Drive. Immediately after this the NTFS file structure is created on the device indicating the drive was probably formatted before use and to 'sterilize' it.
7W9P7F-5562	File system slack space is written with "CTS_FORENSICS"
8UH9ME-5562	The unallocated/slack space is filled with the characters CTS_FORENSICS_
93AL3L-5562	The repeated characters of CTS_FORENSICS on the drive in both partitions and also un-partitioned space.
9GULT8-5562	Unallocated space in the NTFS partition shows a predetermined pattern: CTS_FORENSICS.
AQYVXC-5562	CTS_FORENSICS was identified when viewing portions of the device in hex view which is indicative of the device being wiped/sterilized before use.
AV4RGC-5562	This device may have been sterilized with "sdelete64.exe"
BR6KUT-5562	Both Free Space and Volume slack have been overwritten with the repetitive bytes forming the words "CTS_FORENSICS_". The program previously mentioned sdelete64.exe is also capable of wiping in such a manner.
CBTGPD-5562	Some of the disc has been overwritten with the value 'CTS_FORENSICS_'
CQ9KB9-5562	There are no indications of the device being sanitized.
CZCW7G-5562	The device has a partition with hex value "CTS_FORENSICS" which means it has been over written and sterilized.
FFG39B-5562	sdelete64.exe is present on the USB. The program securely deletes files by overwriting their data and the MFT
FJWWP9-5562	All carved items refer to current user, no trace of any other user accounts.
FP3BPR-5562	The unallocated space of the USB device is populated with a repeating pattern of text which reads "CTS_FORENSICS". This is an indication that the device was populated with this string prior to use and therefore "sterilized"
JF4GTB-5562	The unallocated space has a repetitive hex sequence which indicates sterilization
JJJA4W-5562	The free space is filled with a text that repeats itself

TABLE 2: Removable Media Device Results

Question 46	
WebCode - Test	**Response**
K6Z7V8-5562	$Logfile contains records of file deletions (file.bin, 57zraq1zwmf61.jpg, fptxtzw3ipk61.jpg, 6w8w8kl2u1i61.jpg, a4sdkhvqeik61.jpg, baby_kitteh - Copy.jpg and keepers).
KH3MYM-5562	Unallocated space showing _CTS_FORENSICS_
KT78B9-5562	FreeSpace Filled with pattern CTS_FORENSICS_
L9D7RX-5562	Almost all the content of the unallocated space (free space) of the device is occupied by the string "CTS_FORENSICS_" which suggests that the device was "sterilized" prior to use
LEERBL-5562	Repetition of pattern in Hex 43 54 53 5F 46 4F 52 45 4E 53 49 43 53 5F
LRRLAT-5562	$Logfile shows File named 'file.bin' has been created and deleted; five '.jpg' files also shown as deleted. These match names with shortcuts on computer to V:\\.
M98EB2-5562	Hex has been overwritten with 'CTS_FORENSICS' in order to destroy data
MWHHA4-5562	No data prior to 7th March 2021. Sys Folder created on 7th March 2021.
MYJKY6-5562	Sectors appear to have been overwritten with CTS_FORENSICS
NFQ2KX-5562	Presence of text: FORENSICS_CTS_ in unallocated space, could be indicator
NUKNP6-5562	Existing and execution of sdelete.exe software, files in unallocated space contains values "CTS TEST" sentence
PTA4GV-5562	Yes. It was sterilized using string "FORENSICS_CTS_" prior to use.
RAQR4V-5562	Unused space on the disk is populated with repeating characters CTS_FORENSICS_
T8F7TZ-5562	Appears that the device was sterilised/wiped as there are sectors that have been overwritten with CTS_FORENSICS
U964DC-5562	An executable file called "sdelete64.exe" is present on the volume of the USB. sdelete64.exe is a utility program which allows a user to delete files, folders or directories. A 418MB volume is present on the USB only containing Unallocated Space. Within the hex of this unallocated space has multiple ASCII repeats of the term "CTS_FORENSIC". This suggests this volume was deleted and the USB was sterilized before use.
X436QC-5562	Most of unallocated is filled with 'CTS_FORENSICS_', all file slack is zeroed and there is a copy of the secure deletion application SDelete v2.04 present.
X4L22Q-5562	Unallocated space at the end of partitions read all 0's or CTS_FORENSICS

Question 46: What indications, if any, suggest this device was "sterilized" prior to use?

Consensus Result:

The unallocated space on the device was overwritten with a pattern, "CTS_FORENSICS_".

Expected Response Explanation:

Storage devices usually ship from manufacturers with empty space containing zeros or hex FF. The source device for this test was completely overwritten with the above pattern before partitioning and formatting.

TABLE 2: Removable Media Device Results

Question 46

Expected Response Illustration:

EnCase view of unallocated clusters

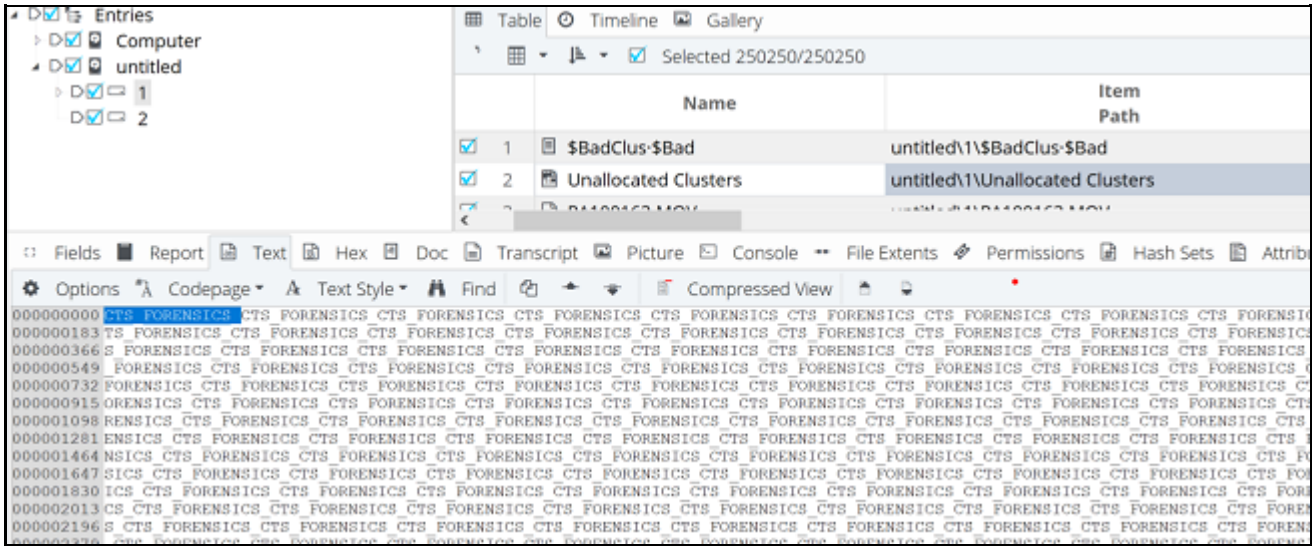


TABLE 2: Removable Media Device Results

Question 47

Question 47: What are the GPS coordinates where PA020033.JPG was captured? Provide your answer in the format: DD MM' SS.SS" N/S, DD MM' SS.SS"E/W.

Manufacturer's Expected Response:
38°49'10.22" N, 76°12'58.40" W

WebCode - Test	Response
29JUMG-5562	Latitud: 38°49'10.23" North, Longitud: 76°12'58.4" West
2YBWJR-5562	38 49 10.23" N, 76 12 58.40"W
67H6N6-5562	38 49' 10.22" N, 76 12'58.40"W
6G29KN-5562	38°49'10.23" N, 76°12'58.40" W
6N3QEM-5562	40:45:36N 73:59:2.4W
7FMAEZ-5562	02/10 38°49'10.23" North, 02/10 76°12'58.4" West
7W9P7F-5562	38 49'10.22" N, 76 12'58.40" W
8UH9ME-5562	38 49'10.23" N, 76 12'58.4" W
93AL3L-5562	38°49'10.23" North \ 76°12'58.4" West
9GULT8-5562	38 49 10.2252 N, 76 12 58.3992 W
AQYVXC-5562	38°49'10.22" N, 76°12'58.40" W
AV4RGC-5562	76°12'58.4"N/S , 38°49'10.23" E/W
BR6KUT-5562	38°49'10.23" N, 76°12'58.4" W
CBTGPD-5562	38°49'10.23" N, 76°12'58.4" W
CQ9KB9-5562	38 49' 10.22" N, 76 12' 58.40" W
CZCW7G-5562	40:45:36N 73:59:2.4W
FFG39B-5562	38°49'10.22" N, 76°12'58.4" W
FJWWP9-5562	38°49'10.23", 76°12'58.4"
FP3BPR-5562	The GPS coordinates stored within the file PA020033.JPG are 38 49' 10.23" North/South , 76 12' 58.4" East/West
JF4GTB-5562	38 49'10.224" N, 76 12' 58.398" W
JJJA4W-5562	38°49'10,224" N, 76°12'58,398" W
K6Z7V8-5562	38°49'10.23" N, 76°12'58.4" W

TABLE 2: Removable Media Device Results

Question 47	
WebCode - Test	**Response**
KH3MYM-5562	-76° 12' 58.41 S 38° 19' 10.23 E
KT78B9-5562	38°49'10.23" N, 76°12'58.4" W
L9D7RX-5562	38 49' 10.23" N, 76 12' 58.4" W
LEERBL-5562	38 49' 10.23 N, 76 12' 58.4 W
LRRLAT-5562	38°49' N, 76°12' W
M98EB2-5562	38°49'10.23" N, 76°12'58.4" W
MWHHA4-5562	38 49' 10.23 N, 76 12 58.4 W
MYJKY6-5562	38 49' 10.22" N, 76 12' 58.40" W
NFQ2KX-5562	38°49'10.23" North, 76°12'58.4" West
NUKNP6-5562	38°49'10.2"N, 76°12'58.4"W
PTA4GV-5562	38°49'10.2240" North, 76°12'58.3980" West
RAQR4V-5562	LAT: 38°49'10.23" (North), Long: 76°12'58.4" (West)
T8F7TZ-5562	38°49'10.23" N, 76°12'58.4" W
U964DC-5562	38 49' 10.22"N, 76 12' 58.39"W
X436QC-5562	38 49' 10.22N 76 12' 58.39W
X4L22Q-5562	38°49'10.23" N, 76°12'58.4" W

Question 47: What are the GPS coordinates where PA020033.JPG was captured? Provide your answer in the format: DD MM' SS.SS" N/S, DD MM' SS.SS"E/W.

Consensus Result:

38°49'10.22" N, 76°12'58.40" W and slight variations representing the same location.

Expected Response Explanation:

The camera used to capture this photo embedded GPS location data as EXIF metadata within the file. This information can be parsed with many tools.

Expected Response Illustration:

Exiftool view of GPS Position Exif Tag

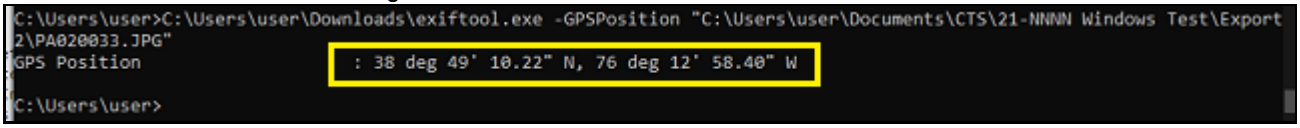


TABLE 2: Removable Media Device Results

Question 48

Question 48: What is the name of the file containing the word "glucuronasyltransferase"?

Manufacturer's Expected Response:

850952.doc

WebCode - Test	Response
29JUMG-5562	850952.doc (21-5562.E01 - Partition 1 (Microsoft NTFS, 1,46 GB) stuff\850952.doc)
2YBWJR-5562	850952.doc
67H6N6-5562	850952.doc
6G29KN-5562	850952.doc
6N3QEM-5562	850952.doc
7FMAEZ-5562	850952.doc
7W9P7F-5562	850952.doc
8UH9ME-5562	850952.doc
93AL3L-5562	850952.doc
9GULT8-5562	850952.doc
AQYVXC-5562	850952.doc
AV4RGC-5562	850952.doc
BR6KUT-5562	850952.doc
CBTGPD-5562	850952.doc
CQ9KB9-5562	850952.doc
CZCW7G-5562	850952.doc
FFG39B-5562	850952.doc
FJWWP9-5562	850952.doc
FP3BPR-5562	850952.doc
JF4GTB-5562	850952.doc
JJJA4W-5562	850952.doc
K6Z7V8-5562	850952.doc
KH3MYM-5562	850952.doc

TABLE 2: Removable Media Device Results

Question 48

WebCode - Test	Response
KT78B9-5562	850952.doc
L9D7RX-5562	850952.doc
LEERBL-5562	850952.doc
LRRLAT-5562	850952.doc
M98EB2-5562	850952.doc
MWHHA4-5562	850952.doc
MYJKY6-5562	850952.doc
NFQ2KX-5562	850952.doc
NUKNP6-5562	[Participant did not return results for this question.]
PTA4GV-5562	850952.doc
RAQR4V-5562	850952.doc
T8F7TZ-5562	850952.doc
U964DC-5562	850952.doc
X436QC-5562	850952.doc
X4L22Q-5562	850952.doc

Question 48: What is the name of the file containing the word "glucuronasyltransferase"?

Consensus Result:
850952.doc

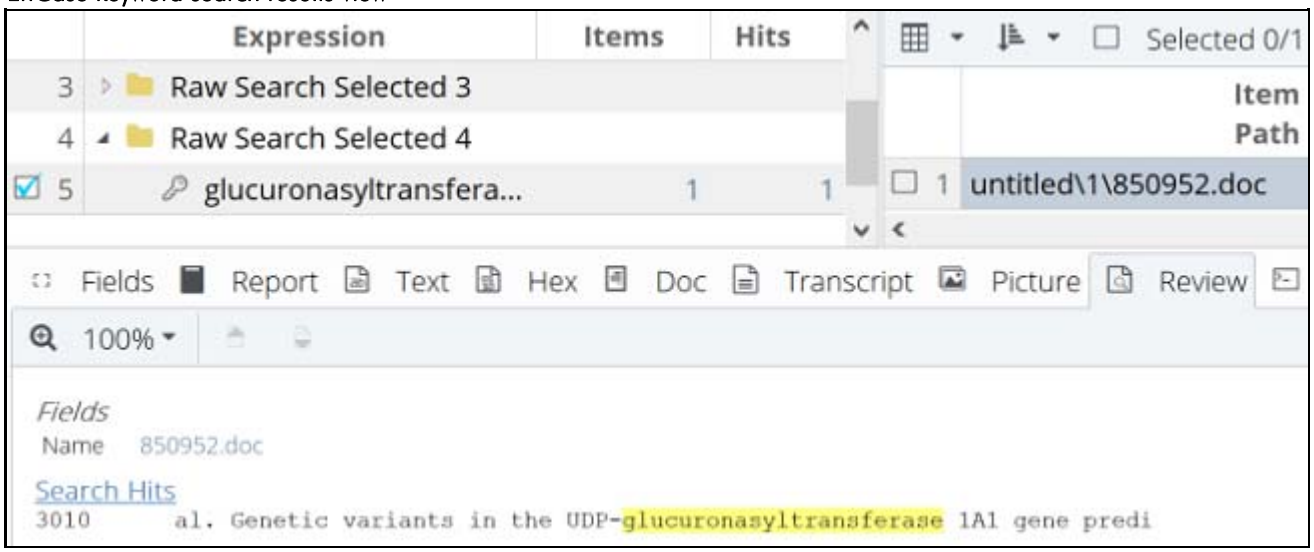
Expected Response Explanation:
A keyword search with any tool capable of expanding compound files will locate this term.

TABLE 2: Removable Media Device Results

Question 48

Expected Response Illustration:

EnCase keyword search results view



Additional Comments

TABLE 3

WebCode	Additional Comments
67H6N6-5562	Regarding question 37, When the USB arrived at the company, it was inserted into the PC for a USB virus scan according to the company import procedure. And the hash value is changed. The tester received an email saying that the USB will be arriving soon, but the exact date is not known, and it should be marked as USB packaging for testing only to bring it into the company.
8UH9ME-5562	I'm not sure if I just answered a bunch of questions wrong, but there were a lot of repeat answers/similar questions asked in this test. I just think some more variety would be helpful.
93AL3L-5562	The lab did not authorize the use of a SHA 256 tool when this examination was assigned. There are several questions that based on lab policies and procedure would not be answered. : Questions 11, 12, 23, 37, 42. There are several questions that would be outside of the normal data released to our customers unless specifically requested or needed for the examination but answers were provided for these questions: 3, 17, 18, 21, 26, 28, 32, 35, 36, 39, 43. For a PT test this seems a lot more in-depth than a normal PT for our laboratory. This would probably be fine for a deep dive comp test for a new examiner.
9ARR2D-5561	Q21: This information is not provided or obtained because this is of no value to customers; therefore, it is not performed/tested in this laboratory. Q36: This question is not tested at the laboratory because it is not consistent with the information/work product provided back to the laboratory customers.
CQJQ7N-5561	MD5 hash value that was provided for .E01 file is wrong. I computed the .E01 file and the MD5 hash value that my forensic tool provided is (3dd605cd2c0b034367c62b550ee19770).
FP3BPR-5562	Some of the questions are ambiguous as to their target, for example. Q40 reads "What is the name (Volume Label) of the NTFS Partition? Between the 2 evidence files, there are 4 partitions, 3 of which are NTFS format. Context is assumed in this instance to refer to the USB stick, as the preceding questions have mentioned this device.The time / date information questions are not posed for an international participant list. All times are provided in US Time format (MM-DD-YYYY). A more suitable approach to cater for all would be to use an ISO format time of YYYY-MM-DD. To pose a question regarding an expected "indication" is not suitable for a forensic process. Whilst an indication may lead the investigator to further lines of enquiry, this would not be evidenced by the practitioner. The questions posed regarding volume serial numbers are misleading. The author requests the data to be displayed in little endian "as would be by Windows". Whilst the raw data is stored as little endian, Windows reports the volume serial number, in command prompt, in Big Endian. The questions, as a whole, do not represent forensic challenges and processes which are encountered on a routine basis. A heavy bias toward 'academic' forensics was implied, rather than 'real world' forensics.
KW3EPY-5561	Q#9: The Relative Identifier (RID) for user account susie is: 1001. Q#25: This is the date when the file was re-allocated to the recycle.bin.
L9D7RX-5562	Questions 29, 33, 34 are not in the scope of our laboratory's examination because the laboratory is not specialized in email-related artifacts analysis and does not have the necessary tools for email artifacts analysis.

TABLE 3

WebCode	Additional Comments
LCV3Z2-5561	Question 23 about the number of times Notepad.exe was executed was unknown given my current training. Because UserAssist run counts increasing 3 times was possible based on how the program was executed (as Administrator from the Start menu) messed up my current understanding of UserAssist run counts. https://pdfs.semanticscholar.org/b12c/6cd1c6d1f1d2a24bcb0a5fa1e71449700d38.pdf Application auditing was not enabled in the suspect disk image. UsnJrnl tracking of .pf creation/modifications times fell within the prefetch 8 and UserAssist 14 count times for notepad execution.
LEERBL-5562	Question 37 couldn't be answered as the SHA1 hash did not match. The instructions were not, in my opinion clear enough with regards to the USB stick, and where the image of the hard drive could be found. Therefor the USB was mounted not through a write blocker and it is possible changes were made, affecting the hash. Lab procedures would always be to use write blocker on evidence, it wass not clear to me when I received the package that it was evidence. This could be made clear on the packaging of the USB and advise to mount through write blocker.
LRRLAT-5562	Noted the presence of the word document 'opossum.docx' has title 'Password Document' and has single word 'Didelphis' and an image. Media 21-5562-M1 has an encrypted partition. Email attachment 'file.gpg' of probable relevance. Unable to open either using password and/or '. asc' key files.
LXXGTT-5561	For Question 35, I listed the default program for susie's account specifically.
PBBNHP-5561	(Question 35) I provided the default docx app from the System registry file, but noticed a different one is listed under the user's NTUSER.dat registry file
RXCADP-5561	Confused why the scenario has no bearing on the test. Any questions I thought to ask were addressed quickly.
TFMD29-5561	Some of the questions have some degree of subjectivity and there is some measure of doubt about the "most correct" sourcing of an answer. That is, the context suggests that the "correct" answer is found in one place, but an equally "correct" (and different) answer might be found somewhere else. Example: Question 23 "How many times was NOTEPAD.EXE executed?" I put the answer as "8" because that's the additive number of the times in the prefetch record. However, the prefetch record also lists the "application run count" as "3." I personally think the additive approach is a more authoritative number, but prefetch has its charms. Likewise, I spent a lot of time trying to make sure I didn't get the wrong answer by simply misunderstanding what the correct answer format was Example: Question 26 "Provide the first six bytes of the file with SHA1 hash 383d4c012ac7c550699c3908c57f7ad00b98ecbe." I wasn't sure if it was more appropriate to answer in Hex or ASCII.

TABLE 3

WebCode	Additional Comments
XCDUFN-5561	I am not entirely sure of what program the developer of the test was thinking of when creating question 15 “What (non-encryption related) anti-forensics application did the user execute?” I looked through multiple areas where artifacts are created when programs are executed. Locations such as UserAssist, Windows 10 Timeline, Jump Lists, Prefetch, Shimcache, etc… I did some general internet searches on executables that I was unfamiliar with and eliminated stock programs. I considered selecting some of the other more obvious programs such as Cipher or TOR but these certainly have elements of encryption. After locating sdelete64.exe on the users’s desktop I completed a keyword search with a few different forensic programs and found some supporting evidence that application was executed (although not as much as I would like to see). Given the location, the keyword search results, the Shimcache artifact, and the notion that sdelete could be used to securely overwrite files I decided that was the intention of the question.
YQTYXP-5561	Question 1 - You use the word "stored verification". I believe you mean the image acquisition (as opposed to the E01 file hash). This is worded very poorly. Question 3 - You ask for the Volume serial number, but you don't add if you want it in 32bit or 64bit. When looking at raw hex code, 32 bit uses offset 0x68 while 64-bit uses offset 0x72. EnCase, Axiom and X-ways confirm this. This question is again worded very poorly. When you say the first four bytes as displayed by "Windows", do you mean in 32 bit? Question 11 does not identify which name you are looking for. The provider name (as reported by forensic tools) shows BTHUSB. But if you do a deep dive into the registry, the following key: SYSTEM\ROOT\ControlSet001\Enum\BTHENUM\Dev_98D371FD9A2A\7&4f6eb3f&0&BluetoothDevice_98D371FD9A2A\Properties\{a35996ab-11cf-4935-8b61-a6761081ecdf}\000C\(Default) idntifies the device friendly name as as BEARODACTYL.
YYKJVA-5561	For question 15, Question 15 asks the use of anti-forensic applications. The usage history of tor browser is found on the user's pc. Because tor browser can be used without leaving any web history, it can be a kind of anti-forensic application.
ZTBFTE-5561	Regarding question #3, there is some inconsistency about what a "system partition" is. Broadly, it is defined as the partition on which the operating system resides. However, Microsoft itself defines it as a separate partition that contains, among other things, the boot code and Windows recovery environment for Windows 10 (see: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/hard-drives-and-partitions). As the examined image comes from a Windows 10 system, I provided the volume serial number for the "System Recovery" partition (partition 1) as this contains the boot code and Windows RE.

-End of Report-
(Appendix may follow)

