Collaborative Testing Services, Inc
FORENSIC TESTING PROGRAM

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

Computer Hard Drive - Windows Analysis
Test No. 20-5561/2 Summary Report

Participants were provided with data yielded from an extraction of a Windows 10 Computer Hard Drive. Additionally, participants in the 5562 test also received a physical USB drive. Examiners were asked to analyze the sample material and answer scenario based questions utilizing their own tools and methods. Data were returned from 49 participants, 24 of which also returned results associated with the physical USB. These results are compiled in the following tables:

Report Contents: Page

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

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

Manufacturer's Information

The Computer Hard Drive – Windows Analysis test consisted of evidence data acquired from a Windows 10 computer. The extracted data was provided in a DD 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 20-5562: 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, based upon a counterfeit money operation was created to generate user data on a Windows Hard Drive. The execution of the scripted crime took place from February 9, 2020 to March 1, 2020. 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 20-5562.

A flat-file (DD, or .001) physical image of the 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 compressed and uploaded to the CTS portal for participants to download. MD5 and SHA1 digests (cryptographic checksums, or 'hashes') were calculated for the compressed data and provided to participants to enable validation of successful download of the files. An MD5 digest for the uncompressed DD image was provided to participants to enable validation of successful decompression of the compressed image.

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
Over the previous several weeks, numerous counterfeit $20 and $50 dollar bills have been discovered by local banks in cash deposits from local convenience stores. The town police department posted a notice on social media for businesses to look out for the fake bills. On March 1, 2020, a cashier at the Main Street Kwik-E-Mart thought something felt odd about a $20 bill he was given by a customer who purchased only a cup of coffee. He observed the customer drive away in a dark colored sedan and noted the license plate. The cashier called the police department and when interviewed by detectives provided a description of the customer and the vehicle, the license plate number, and surrendered the suspect $20 bill.

Examination of the $20 bill determined it to be an ink-jet printer produced counterfeit similar to those previously discovered. The police department interviewed the registered owner of the sedan, James Mitchell, who matched the description given by the cashier. Mitchell admitted he "may have printed some 'play money' for a poker night" but denied having passed any "for real".

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

Manufacturer's Information, continued

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

1 The provided archive CHD 20-5561-2.zip contains a raw image acquired from the hard drive in the subject's computer. The MD5 digest (hash) of the image when extracted from the archive is 3D6B6B19ED716C56ECA37D7684A4C466. Provide the SHA256 hash value of the extracted image.
B94AB48828C519ADD80F57354E1E8188221AE5E44CD880CCAC4D7B6ED582A4DD

2 Provide the SHA256 hash for the file with the MD5 hash of 3C8F6D9AF84A6DB132077C6BDCC69BBC.
A2115F2F9FA32D899C5E911E85CD973730B53F032E97BFA5A4519B5114292A76

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

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?
james.mitchell.40@outlook.com

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
02/10/2020 01:18:41 AM (UTC)

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
03/01/2020 07:24:38 PM (UTC)

8 Provide the user name of the account created by the user.
james

9 What is the SID of the user account created by the user?
S-1-5-21-4282868925-760505910-2700774193-1001

10 What is the configured time zone?
Pacific Standard Time

11** What was the name (Volume Label) of the LAST drive mounted on this computer?
ResponseTools

12 Provide the name of the MOST RECENTLY viewed video file?
SNL-Celebrity Jeopardy- Buck 1.mpg

13 What is the name of the file the user unsuccessfully attempted to print?
20_back.xcf

14 What networking device did the user attach via USB?
Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter

Manufacturer's Information, continued

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

15 Identify an anti-forensics application executed by the user?
Ccleaner, Eraser or SDelete

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

17 What IP address was assigned by this network?
10.21.6.146

18 What program did the responding/seizing examiner execute?
FTK Imager

19 From what URL was the file with SHA1 3de75af054fed96e39568bad6edfdbc452d2cda4 downloaded?
https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download

20 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
03/01/2020 06:45:09 PM

21 What is the volume serial number for the file system on the system partition?
2C2E-5168, 68512E2C or 402C2E602C2E5168

22 What is the original (pre-deletion) name of the file in the user's Recycle Bin?
20_front.xcf

23 What was the path to the location of the file (file reference in question #22) prior to being sent to the Recycle Bin?
C:\Users\james\Documents\

24 On what date and time was the file (file referenced in question #22) deleted? Provide your response in UTC + 00:00 using the following format: MM/DD/YYYY HH:MM AM/PM
03/01/2020 04:06:46 PM (UTC)

25 What is the default application for opening this type of file (file referenced in question #22)?
C:\Program Files\GIMP 2\bin\gimp-2.10.exe, GIMP 2, or GIMP

26 What is the name of the encrypted file found in C:\Users\james\Documents?
vfpr6npaqea12.jpg

27 What email application was installed by the user?
Mozilla Thunderbird

28 What third party encryption application was executed by the user?
Veracrypt

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

Manufacturer's Information, continued

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

29** On what date and time was this third party encryption application LAST executed? Provide your in the UTC + 00:00 using the following format: MM/DD/YYYY HH:MM:SS AM/PM
02/28/2020 06:09:01 AM (UTC)

30 Provide the FIRST term searched using Google Chrome on this device.
torproject

31 What darkweb (darknet) site did the user bookmark?
dreadditevelidot.onion

32 What web browser was used to download openoffice?
Microsoft edge

33** From the information in prefetch, how many times was Tor.exe executed? Provide a NUMERIC response (e.g. 1, 2, 3).
4

34 Who LAST modified 000051.xls?
richburg_r

35 Who is the Author of 004583.doc?
Celal Konor

36 What is the name of the file that contains the word "ohtaguchi"?
003555.txt

37 Provide the name of the (active) file containing the word "playmoney" where the letters a,o,e have been replaced with arbitrary characters.
lorem.text

38 What is the literal spelling of the word found in Question #37?
pl@ym0n3y

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

Manufacturer's Information, continued

Removable Media Analysis: *USB Drive*
Test No. 20-5562

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

39** What is the SHA-256 hash for the device?
2b1fb19de0da5f1358437c4be80a6e0f01fbbe8a6ada79b0ae24473c8e8b44fd

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

41 What is the volume serial number?
CA9F-D08C

42 What is the name (Volume Label)?
BLACK2G

43 What is the file system (include version) for this device?
NTFS 3.1

44 What color is the animal in the file with SHA1 Hash b5fe34cd8d978d2e3c97835eb9128ad3c72edd9d?
Black

45 What does the difference in creation and last written times indicate about the 4stq6uu5w4j41.jpg file?
The creation date for this file is after the modified (last written date) meaning it was copied there from another volume.

46 What is the name of the file with header 0x 00 00 00 01 42 75 64 31?
.DS_Store

47 What does the presence of this file (file referenced in question #46) indicate?
File created by OS X (Apple) (device was used in a Mac)

48 Who is the Author of 000124.doc?
Becky Allee

49 In unallocated space on this device is a photo of a grey and white cat with a blue toy. What is the SHA1 hash of this file?
866c4b57882276e2e473f3ad8c364d92a890cebd

50 What is the name of the file that contains the word "convallis"?
lorem.text

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 in DD file format, and a series of questions related to the extracted data. Additionally, participants enrolled in the 20-5562: Computer Hard Drive – Windows & Removable Media Storage Analysis test also received a physical USB drive. These participants were also 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 49 participants returned results for the 5561 Computer Hard Drive - Windows Analysis test. Of the 38 total questions, three questions did not reach a consensus response. These three questions were found in the following three categories of analysis: Registry, Application and Prefetch.

Of the participants enrolled in the 5562 Removable Media Storage Analysis test, 24 returned results. One of the twelve questions did not reach a consensus response. This question asked for the SHA256 hash for the USB device. Of the inconsistent responses, one participant reported a truncated version of the expected hash response and two others provided the SHA1 hash value instead of the SHA256 hash value.

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.

Digital Evidence Responses

TABLE 1

Question 1 - Hashing / File Integrity

Question 1: The provided archive CHD 20-5561-2.zip contains a raw image acquired from the hard drive in the subject's computer. The MD5 digest (hash) of the image when extracted from the archive is 3D6B6B19ED716C56ECA37D7684A4C466. Provide the SHA256 hash value of the extracted image.

Manufacturer's Expected Response: B94AB48828C519ADD80F57354E1E8188221AE5E44CD880CCAC4D7B6ED582A4DD

WebCode-Test	Response
2ZQE6A-5561	B94AB48828C519ADD80F57354E1E8188221AE5E44CD880CCAC4D7B6ED582A4DD
4XFB84-5561	b94ab48828c519add80f57354e1e8188221ae5e44cd880ccac4d7b6ed582a4dd
64W7NX-5562	B94AB48828C519ADD80F57354E1E8188221AE5E44CD880CCAC4D7B6ED582A4DD
6U9F26-5561	B94AB48828C519ADD80F57354E1E8188221AE5E44CD880CCAC4D7B6ED582A4DD
6ZF77W-5562	b94ab48828c519add80f57354e1e8188221ae5e44cd880ccac4d7b6ed582a4dd
7K2ZUX-5562	B94AB48828C519ADD80F57354E1E8188221AE5E44CD880CCAC4D7B6ED582A4DD
7M9E24-5561	B94AB48828C519ADD80F57354E1E8188221AE5E44CD880CCAC4D7B6ED582A4DD
8Q3VR3-5562	B94AB48828C519ADD80F57354E1E8188221AE5E44CD880CCAC4D7B6ED582A4DD
9ENXLY-5561	b94ab48828c519add80f57354e1e8188221ae5e44cd880ccac4d7b6ed582a4dd
ABKKEY-5561	b94ab48828c519add80f57354e1e8188221ae5e44cd880ccac4d7b6ed582a4dd
AQCK6Y-5561	B94AB48828C519ADD80F57354E1E8188221AE5E44CD880CCAC4D7B6ED582A4DD
BJTE9R-5562	B94AB48828C519ADD80F57354E1E8188221AE5E44CD880CCAC4D7B6ED582A4DD
C8D7KQ-5561	b94ab48828c519add80f57354e1e8188221ae5e44cd880ccac4d7b6ed582a4dd
CCTE9P-5562	b94ab48828c519add80f57354e1e8188221ae5e44cd880ccac4d7b6ed582a4dd
CKXLNP-5561	B94AB48828C519ADD80F57354E1E8188221AE5E44CD880CCAC4D7B6ED582A4DD
CPXWKP-5562	b94ab48828c519add80f57354e1e8188221ae5e44cd880ccac4d7b6ed582a4dd
DGFL7P-5562	b94ab48828c519add80f57354e1e8188221ae5e44cd880ccac4d7b6ed582a4dd
DX4YHV-5561	b94ab48828c519add80f57354e1e8188221ae5e44cd880ccac4d7b6ed582a4dd
EQHHC7-5562	B94AB48828C519ADD80F57354E1E8188221AE5E44CD880CCAC4D7B6ED582A4DD
ETQDAP-5562	B94AB48828C519ADD80F57354E1E8188221AE5E44CD880CCAC4D7B6ED582A4DD
HG3KCP-5561	B94AB48828C519ADD80F57354E1E8188221AE5E44CD880CCAC4D7BED582A4DD
HHBXTQ-5562	b94ab48828c519add80f57354e1e8188221ae5e44cd880ccac4d7b6ed582a4dd

TABLE 1

Question 1 - Hashing / File Integrity

WebCode-Test	Response
J6MAYJ-5561	B94AB48828C519ADD80F57354E1E8188221AE5E44CD880CCAC4D7B6ED582A4DD
KH3VVH-5562	B94AB48828C519ADD80F57354E1E8188221AE5E44CD880CCAC4D7B6ED582A4DD
MTJYGM-5562	B94AB48828C519ADD80F57354E1E8188221AE5E44CD880CCAC4D7B6ED582A4DD
NF4QTK-5562	B94AB48828C519ADD80F57354E1E8188221AE5E44CD880CCAC4D7B6ED582A4DD
NZEF7H-5561	b94ab48828c519add80f57354e1e8188221ae5e44cd880ccac4d7b6ed582a4dd
P6M4JK-5562	b94ab48828c519add80f57354e1e8188221ae5e44cd880ccac4d7b6ed582a4dd
P8TN8K-5561	B94AB48828C519ADD80F57354E1E8188221AE5E44CD880CCAC4D7B6ED582A4DD
P92YZG-5562	b94ab48828c519add80f57354e1e8188221ae5e44cd880ccac4d7b6ed582a4dd
PZ7VVK-5561	d8b4e2fecaaf8f837ad7041c6314df8c3b2aba066c33a0448b6b6e788bd8a2dd
Q7RBYH-5562	fab90d80a2dc3c1960c56c5466d2c54af097df50
QAQLVH-5561	B94AB48828C519ADD80F57354E1E8188221AE5E44CD880CCAC4D7B6ED582A4DD
QFHW6F-5561	B94AB48828C519ADD80F57354E1E8188221AE5E44CD880CCAC4D7B6ED582A4DD
QZQWEG-5561	B94AB48828C519ADD80F57354E1E8188221AE5E44CD880CCAC4D7B6ED582A4DD
R7BE8H-5562	7K4Q3AFC3Q6BSYGFNRKGNUWFJLYJPX2Q
TANE4A-5561	B94AB48828C519ADD80F57354E1E8188221AE5E44CD880CCAC4D7B6ED582A4DD
TEV68F-5561	b94ab48828c519add80f57354e1e8188221ae5e44cd880ccac4d7b6ed582a4dd
TXBE8F-5561	B94AB48828C519ADD80F57354E1E8188221AE5E44CD880CCAC4D7B6ED582A4DD
U3ZBAC-5562	B94AB48828C519ADD80F57354E1E8188221AE5E44CD880CCAC4D7B6ED582A4DD
VBBWX7-5562	b94ab48828c519add80f57354e1e8188221ae5e44cd880ccac4d7b6ed582a4dd
VZACVE-5562	b94ab48828c519add80f57354e1e8188221ae5e44cd880ccac4d7b6ed582a4dd
W2ZUC7-5562	The SHA256 value of the extracted raw image is b94ab48828c519add80f57354e1e8188221ae5e44cd880ccac4d7b6ed582a4dd. I have used hashmyfiles tool to find the SHA256 value.
WVD6QB-5561	B94AB48828C519ADD80F57354E1E8188221AE5E44CD880CCAC4D7B6ED582A4DD
XGCTUC-5561	b94ab48828c519add80f57354e1e8188221ae5e44cd880ccac4d7b6ed582a4dd
Y78Z2B-5561	B94AB48828C519ADD80F57354E1E8188221AE5E44CD880CCAC4D7B6ED582A4DD
YCA984-5562	B94AB48828C519ADD80F57354E1E8188221AE5E44CD880CCAC4D7B6ED582A4DD

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 1 - Hashing / File Integrity

WebCode-Test	Response
Z4WK8A-5562	B94AB48828C519ADD80F57354E1E8188221AE5E44CD880CCAC4D7B6ED582A4DD
Z6A992-5561	b94ab48828c519add80f57354e1e8188221ae5e44cd880ccac4d7b6ed582a4dd

Question 1: The provided archive CHD 20-5561-2.zip contains a raw image acquired from the hard drive in the subject's computer. The MD5 digest (hash) of the image when extracted from the archive is 3D6B6B19ED716C56ECA37D7684A4C466. Provide the SHA256 hash value of the extracted image.

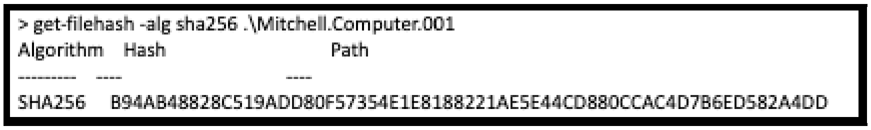
Consensus Result: B94AB48828C519ADD80F57354E1E8188221AE5E44CD880CCAC4D7B6ED582A4DD

Expected Response Explanation:

The hash can be calculated with any reliable hashing tool. Windows powershell contains a native cmdlet for hashing.

Expected Response Illustration:

Windows Powershell hashing of forensic image:



```
> get-filehash -alg sha256 .\Mitchell.Computer.001
Algorithm   Hash                                Path
---------   ----                                ----
SHA256      B94AB48828C519ADD80F57354E1E8188221AE5E44CD880CCAC4D7B6ED582A4DD
```

TABLE 1

Question 2 - Hashing / File Integrity

Question 2: Provide the SHA256 hash for the file with the MD5 hash of 3C8F6D9AF84A6DB132077C6BDCC69BBC.

Manufacturer's Expected Response: A2115F2F9FA32D899C5E911E85CD973730B53F032E97BFA5A4519B5114292A76

WebCode-Test	Response
2ZQE6A-5561	A2115F2F9FA32D899C5E911E85CD973730B53F032E97BFA5A4519B5114292A76
4XFB84-5561	a2115f2f9fa32d899c5e911e85cd973730b53f032e97bfa5a4519b5114292a76
64W7NX-5562	A2115F2F9FA32D899C5E911E85CD973730B53F032E97BFA5A4519B5114292A76
6U9F26-5561	a2115f2f9fa32d899c5e911e85cd973730b53f032e97bfa5a4519b5114292a76
6ZF77W-5562	a2115f2f9fa32d899c5e911e85cd973730b53f032e97bfa5a4519b5114292a76
7K2ZUX-5562	a2115f2f9fa32d899c5e911e85cd973730b53f032e97bfa5a4519b5114292a76
7M9E24-5561	A2115F2F9FA32D899C5E911E85CD973730B53F032E97BFA5A4519B5114292A76
8Q3VR3-5562	A2115F2F9FA32D899C5E911E85CD973730B53F032E97BFA5A4519B5114292A76
9ENXLY-5561	a2115f2f9fa32d899c5e911e85cd973730b53f032e97bfa5a4519b5114292a76
ABKKEY-5561	a2115f2f9fa32d899c5e911e85cd973730b53f032e97bfa5a4519b5114292a76
AQCK6Y-5561	A2115F2F9FA32D899C5E911E85CD973730B53F032E97BFA5A4519B5114292A76
BJTE9R-5562	a2115f2f9fa32d899c5e911e85cd973730b53f032e97bfa5a4519b5114292a76
C8D7KQ-5561	396b8c3f058f8e7090f28ab6ff10b3c5a97a685b478bf257fa8470ae89e60bcb
CCTE9P-5562	a2115f2f9fa32d899c5e911e85cd973730b53f032e97bfa5a4519b5114292a76
CKXLNP-5561	a2115f2f9fa32d899c5e911e85cd973730b53f032e97bfa5a4519b5114292a76
CPXWKP-5562	a2115f2f9fa32d899c5e911e85cd973730b53f032e97bfa5a4519b5114292a76
DGFL7P-5562	The sha-256 is a2115f2f9fa32d899c5e911e85cd973730b53f032e97bfa5a4519b5114292a76
DX4YHV-5561	a2115f2f9fa32d899c5e911e85cd973730b53f032e97bfa5a4519b5114292a76
EQHHC7-5562	A2115F2F9FA32D899C5E911E85CD973730B53F032E97BFA5A4519B5114292A76
ETQDAP-5562	A2115F2F9FA32D899C5E911E85CD973730B53F032E97BFA5A4519B5114292A76
HG3KCP-5561	A2115F2F9FA32D899C5E911E85CD973730B53F032E97BFA5A4519B5114292A76
HHBXTQ-5562	a2115f2f9fa32d899c5e911e85cd973730b53f032e97bfa5a4519b5114292a76
J6MAYJ-5561	A2115F2F9FA32D899C5E911E85CD973730B53F032E97BFA5A4519B5114292A76

TABLE 1

Question 2 - Hashing / File Integrity

WebCode-Test	Response
KH3VVH-5562	A2115F2F9FA32D899C5E911E85CD973730B53F032E97BFA5A4519B5114292A76
MTJYGM-5562	A2115F2F9FA32D899C5E911E85CD973730B53F032E97BFA5A4519B5114292A76
NF4QTK-5562	A2115F2F9FA32D899C5E911E85CD973730B53F032E97BFA5A4519B5114292A76
NZEF7H-5561	a2115f2f9fa32d899c5e911e85cd973730b53f032e97bfa5a4519b5114292a76
P6M4JK-5562	a2115f2f9fa32d899c5e911e85cd973730b53f032e97bfa5a4519b5114292a76
P8TN8K-5561	A2115F2F9FA32D899C5E911E85CD973730B53F032E97BFA5A4519B5114292A76
P92YZG-5562	a2115f2f9fa32d899c5e911e85cd973730b53f032e97bfa5a4519b5114292a76
PZ7VVK-5561	396b8c3f058f8e7090f28ab6ff10b3c5a97a685b478bf257fa8470ae89e60bcb
Q7RBYH-5562	32d005b04e58fbd745ecd92a1fe34cf6b3ec50bf
QAQLVH-5561	a2115f2f9fa32d899c5e911e85cd973730b53f032e97bfa5a4519b5114292a76
QFHW6F-5561	A2115F2F9FA32D899C5E911E85CD973730B53F032E97BFA5A4519B5114292A76
QZQWEG-5561	A2115F2F9FA32D899C5E911E85CD973730B53F032E97BFA5A4519B5114292A76
R7BE8H-5562	32d005b04e58fbd745ecd92a1fe34cf6b3ec50bf
TANE4A-5561	A2115F2F9FA32D899C5E911E85CD973730B53F032E97BFA5A4519B5114292A76
TEV68F-5561	a2115f2f9fa32d899c5e911e85cd973730b53f032e97bfa5a4519b5114292a76
TXBE8F-5561	A2115F2F9FA32D899C5E911E85CD973730B53F032E97BFA5A4519B5114292A76
U3ZBAC-5562	A2115F2F9FA32D899C5E911E85CD973730B53F032E97BFA5A4519B5114292A76
VBBWX7-5562	a2115f2f9fa32d899c5e911e85cd973730b53f032e97bfa5a4519b5114292a76
VZACVE-5562	a2115f2f9fa32d899c5e911e85cd973730b53f032e97bfa5a4519b5114292a76
W2ZUC7-5562	The SHA256 value of 3C8F6D9AF84A6DB132077C6BDCC69BBC is a2115f2f9fa32d899c5e911e85cd973730b53f032e97bfa5a4519b5114292a76. I have used the Axiom forensics tool and parsed the raw image in it. When searched for the file with this MD5, I am able to see the jpeg file. I have exported the file and used hashmyfiles tool to calculate the SHA256 hash.
WVD6QB-5561	A2115F2F9FA32D899C5E911E85CD973730B53F032E97BFA5A4519B5114292A76
XGCTUC-5561	a2115f2f9fa32d899c5e911e85cd973730b53f032e97bfa5a4519b5114292a76
Y78Z2B-5561	A2115F2F9FA32D899C5E911E85CD973730B53F032E97BFA5A4519B5114292A76
YCA984-5562	A2115F2F9FA32D899C5E911E85CD973730B53F032E97BFA5A4519B5114292A76
Z4WK8A-5562	A2115F2F9FA32D899C5E911E85CD973730B53F032E97BFA5A4519B5114292A76

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 2 - Hashing / File Integrity

WebCode-Test	Response
Z6A992-5561	a2115f2f9fa32d899c5e911e85cd973730b53f032e97bfa5a4519b5114292a76

Question 2: Provide the SHA256 hash for the file with the MD5 hash of 3C8F6D9AF84A6DB132077C6BDCC69BBC.

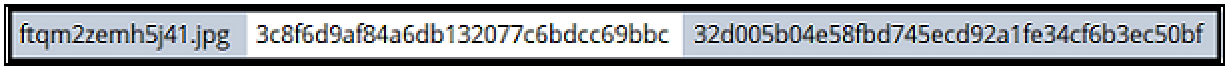
Consensus Result: A2115F2F9FA32D899C5E911E85CD973730B53F032E97BFA5A4519B5114292A76

Expected Response Explanation:

Computing the MD5 hash values for all files and searching for the provide MD5 hash value discovers C:/Users/james/Documents/ftqm2zemh5j41.jpg. Any reliable hashing tool can calculate a SHA256 hash value of this file.

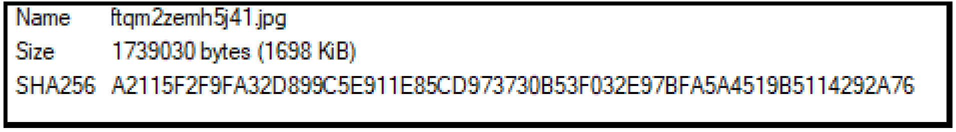
Expected Response Illustration:

EnCase view of MD5 file hash information:



ftqm2zemh5j41.jpg	3c8f6d9af84a6db132077c6bdcc69bbc	32d005b04e58fbd745ecd92a1fe34cf6b3ec50bf

7zip hashing utility output:



```
Name     ftqm2zemh5j41.jpg
Size     1739030 bytes (1698 KiB)
SHA256   A2115F2F9FA32D899C5E911E85CD973730B53F032E97BFA5A4519B5114292A76
```

TABLE 1

Question 3 - Disk Analysis

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

Manufacturer's Expected Response: 2

WebCode-Test	Response
2ZQE6A-5561	2
4XFB84-5561	2
64W7NX-5562	2
6U9F26-5561	2
6ZF77W-5562	2
7K2ZUX-5562	2
7M9E24-5561	2
8Q3VR3-5562	2
9ENXLY-5561	2
ABKKEY-5561	2
AQCK6Y-5561	2
BJTE9R-5562	2
C8D7KQ-5561	2
CCTE9P-5562	2
CKXLNP-5561	2
CPXWKP-5562	2
DGFL7P-5562	2
DX4YHV-5561	2
EQHHC7-5562	2
ETQDAP-5562	2
HG3KCP-5561	2
HHBXTQ-5562	2
J6MAYJ-5561	2
KH3VVH-5562	2

TABLE 1

Question 3 - Disk Analysis

WebCode-Test	Response
MTJYGM-5562	2
NF4QTK-5562	2
NZEF7H-5561	2
P6M4JK-5562	2
P8TN8K-5561	2
P92YZG-5562	2
PZ7VVK-5561	2
Q7RBYH-5562	2
QAQLVH-5561	2
QFHW6F-5561	2
QZQWEG-5561	2
R7BE8H-5562	2
TANE4A-5561	2
TEV68F-5561	2
TXBE8F-5561	2
U3ZBAC-5562	2
VBBWX7-5562	2
VZACVE-5562	2
W2ZUC7-5562	I have mounted the image using Axiom forensics tool, i am able to see that there are 2 partitions, one is System reserved and the other is OS partition.
WVD6QB-5561	2
XGCTUC-5561	2
Y78Z2B-5561	2
YCA984-5562	2
Z4WK8A-5562	2
Z6A992-5561	2 (two)

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

TABLE 1

Question 3 - Disk Analysis

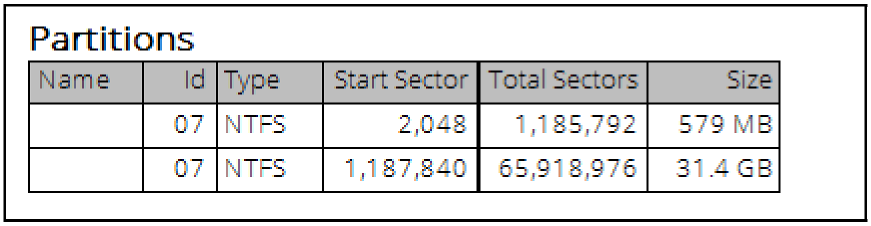
Consensus Result: 2

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:

Partition Table:



Partitions

Name	Id	Type	Start Sector	Total Sectors	Size
	07	NTFS	2,048	1,185,792	579 MB
	07	NTFS	1,187,840	65,918,976	31.4 GB

TABLE 1

Question 4 - Operating System / Registry Analysis

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

Manufacturer's Expected Response: Windows 10 Home

WebCode-Test	Response
2ZQE6A-5561	Windows 10 Home (Core) 1903 (upgrade from ver. 6.3 (Windows 8.1))
4XFB84-5561	Windows 10 Home(1903) version 6.3
64W7NX-5562	Windows 10 Home (1903)
6U9F26-5561	Microsoft Windows 10 Home (1903), Version 6.3
6ZF77W-5562	Microsoft Windows 10 Home Product Version: Multiprocessor Free 6.3.18362.19h1_release.190318-1202
7K2ZUX-5562	Windows 10 Home. Core, Ver 6.3
7M9E24-5561	Windows 10 Home, 6.3, 18362
8Q3VR3-5562	Windows 10 Home (version 6.3)(1903)
9ENXLY-5561	Windows 10 Home; Version 6.3
ABKKEY-5561	Windows 10 Home 6.3
AQCK6Y-5561	Windows 10 Home
BJTE9R-5562	Product Name: Windows 10 Home (Version 10.0.18362.657), Edition ID: Core Current Version: 6.3, Release Id: 1903, Current Major Version: 10, Current Minor Version: 0, Current Build: 18362, UBR: 657
C8D7KQ-5561	windows 10 Home x64
CCTE9P-5562	Windows 10; Edition : Home; Version: Core; Version Number: 6.3; Build number: 18362
CKXLNP-5561	Windows 10 Home
CPXWKP-5562	Windows 10 version 6.3 Home Edition
DGFL7P-5562	The operating system installed according to the registry \Windows\System32\config\SOFTWARE\Microsoft\Windows NT\CurrentVersion. Windows 10 Home (1903) version 6.3
DX4YHV-5561	Windows 10 Home (1903), Version 6.3
EQHHC7-5562	Windows 10 Home (1903)
ETQDAP-5562	OS : Windows 10 Home(Version : 6.3)
HG3KCP-5561	wINDOWS 10 hOM,E (1903) vERSION 6.3
HHBXTQ-5562	Microsoft Windows 10 Home (1903) v6.3
J6MAYJ-5561	Windows 10 Home (1903), Version 6.3, Build Number 18362

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 4 - Operating System / Registry Analysis

WebCode-Test	Response
KH3VVH-5562	Windows 10 Home 6.3 Version
MTJYGM-5562	Windows 10 Home
NF4QTK-5562	Windows 10 Home 6.3
NZEF7H-5561	Windows 10 Home (1903 Build 18362 v6.3 Core)
P6M4JK-5562	Microsoft Windows 10 Home (CurrentBuild: 18362, ProductId: 00326-10854-19213-AA838, CurrentVersion: 6.3)
P8TN8K-5561	Windows 10 Home (1903) Version 6.3
P92YZG-5562	Windows 10 Home – build 18362 – Internal version 6.3
PZ7VVK-5561	Windows 10 (1903) 6.3
Q7RBYH-5562	Windows 10 Home (6.3) Build Number 18362
QAQLVH-5561	Windows 10 Home
QFHW6F-5561	Windows 10 Home, Release ID 1903
QZQWEG-5561	Windows 10 Home version 6.3 (Build 18362)
R7BE8H-5562	Windows 10 Home (1903) Core (18362)
TANE4A-5561	Windows 10 Home
TEV68F-5561	Windows 10 Home , Version 6.3
TXBE8F-5561	WINDOWS 10 HOME
U3ZBAC-5562	Windows 10 Home 6.3
VBBWX7-5562	Windows 10 Home (1903) Ver 6.3
VZACVE-5562	Windows 10 Home , Version 6.3
W2ZUC7-5562	I have processed the image using Axiom forensics tool and with the help of operating system artifacts i am able to find the operating system details as Windows 10 Home (1903) version 6.3 – 64 bit.
WVD6QB-5561	Windows 10 Home Edition (Release 1903) version 6.3
XGCTUC-5561	Windows 10 Home (1903) version 6.3
Y78Z2B-5561	Windows 10 Home (1903) Version 6.3
YCA984-5562	Windows 10 Home (1903)
Z4WK8A-5562	Windows 10 Home
Z6A992-5561	Windows 10 Home, Version: 6.3

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 4 - Operating System / Registry Analysis

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

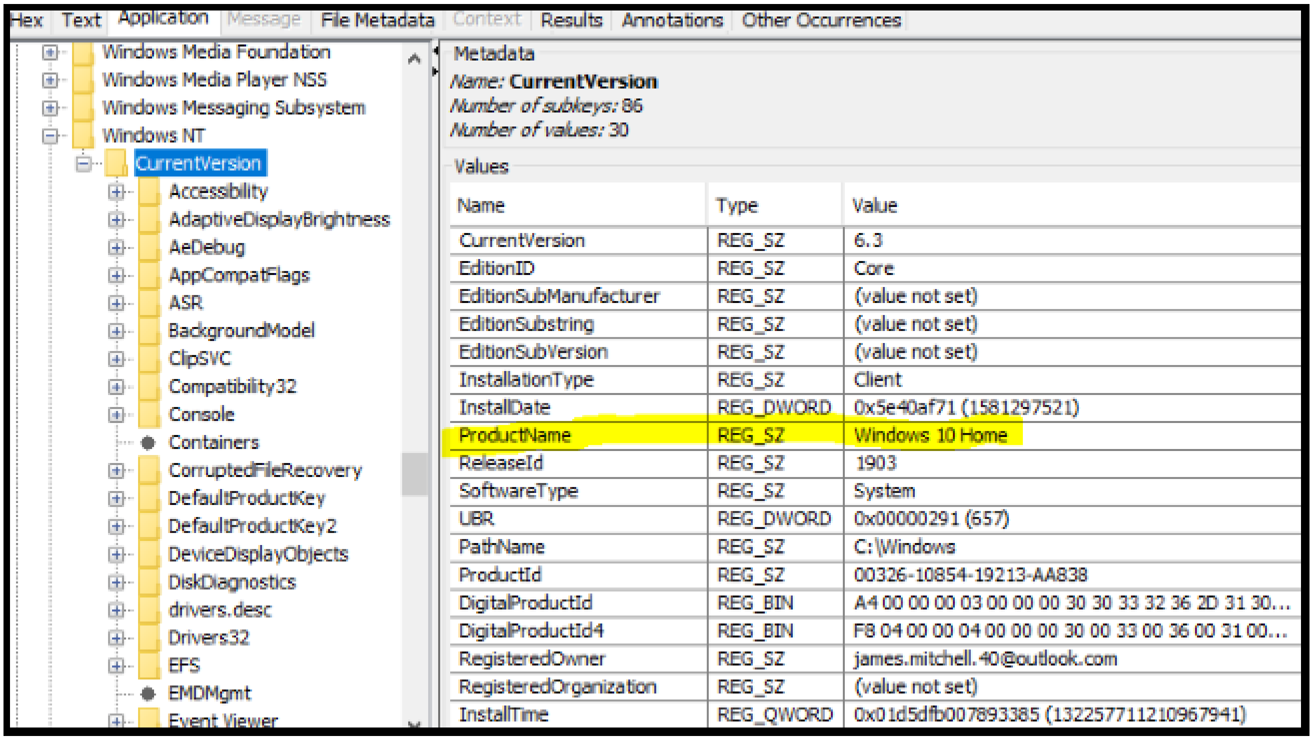
Consensus Result: Windows 10 Home

Expected Response Explanation:

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

Expected Response Illustration:

OS Metadata:



- Windows Media Foundation
- Windows Media Player NSS
- Windows Messaging Subsystem
- Windows NT
  - CurrentVersion
    - Accessibility
    - AdaptiveDisplayBrightness
    - AeDebug
    - AppCompatFlags
    - ASR
    - BackgroundModel
    - ClipSVC
    - Compatibility32
    - Console
    - Containers
    - CorruptedFileRecovery
    - DefaultProductKey
    - DefaultProductKey2
    - DeviceDisplayObjects
    - DiskDiagnostics
    - drivers.desc
    - Drivers32
    - EFS
    - EMDMgmt
    - Event Viewer

Metadata

Name: **CurrentVersion**
Number of subkeys: 86
Number of values: 30

Values

Name	Type	Value
CurrentVersion	REG_SZ	6.3
EditionID	REG_SZ	Core
EditionSubManufacturer	REG_SZ	(value not set)
EditionSubstring	REG_SZ	(value not set)
EditionSubVersion	REG_SZ	(value not set)
InstallationType	REG_SZ	Client
InstallDate	REG_DWORD	0x5e40af71 (1581297521)
ProductName	REG_SZ	Windows 10 Home
ReleaseId	REG_SZ	1903
SoftwareType	REG_SZ	System
UBR	REG_DWORD	0x00000291 (657)
PathName	REG_SZ	C:\Windows
ProductId	REG_SZ	00326-10854-19213-AA838
DigitalProductId	REG_BIN	A4 00 00 00 03 00 00 00 30 30 33 32 36 2D 31 30...
DigitalProductId4	REG_BIN	F8 04 00 00 04 00 00 00 30 00 33 00 36 00 31 00...
RegisteredOwner	REG_SZ	james.mitchell.40@outlook.com
RegisteredOrganization	REG_SZ	(value not set)
InstallTime	REG_QWORD	0x01d5dfb007893385 (132257711210967941)

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 5 - Operating System / Registry Analysis

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

Manufacturer's Expected Response: james.mitchell.40@outlook.com

WebCode-Test	Response
2ZQE6A-5561	james.mitchell.40@outlook.com
4XFB84-5561	james.mitchell.40@outlook.com
64W7NX-5562	james.mitchell.40@outlook.com
6U9F26-5561	james.mitchell.40@outlook.com
6ZF77W-5562	james.mitchell.40@outlook.com
7K2ZUX-5562	james.mitchell.40@outlook.com
7M9E24-5561	james.mitchell.40@outlook.com
8Q3VR3-5562	james.mitchell.40@outlook.com
9ENXLY-5561	James Mitchell - james.mitchell.40@outlook.com
ABKKEY-5561	james.mitchell.40@outlook.com
AQCK6Y-5561	james.mitchell.40@outlook.com
BJTE9R-5562	james.mitchell.40@outlook.com
C8D7KQ-5561	james.mitchell.40@outlook.com
CCTE9P-5562	james.mitchell.40@outlook.com
CKXLNP-5561	james.mitchell.40@outlook.com
CPXWKP-5562	James.mitchell.40@outlook.com
DGFL7P-5562	The registered owner according to the registry Windows\System32\config\SOFTWARE\Microsoft\Windows NT\CurrentVersion. james.mitchell.40@outlook.com
DX4YHV-5561	james.mitchell.40@outlook.com
EQHHC7-5562	james.mitchell.40@outlook.com
ETQDAP-5562	james.mitchell.40@outlook.com
HG3KCP-5561	jAME.mITCHELL.40@oUTLOCK.COM
HHBXTQ-5562	james.mitchell.40@outlook.com
J6MAYJ-5561	james.mitchell.40@outlook.com
KH3VVH-5562	james.mitchell.40@outlook.com

TABLE 1

Question 5 - Operating System / Registry Analysis

WebCode-Test	Response
MTJYGM-5562	james.mitchell.40@outlook.com
NF4QTK-5562	james.mitchell.40@outlook.com
NZEF7H-5561	james.mitchell.40@outlook.com
P6M4JK-5562	james.mitchell.40@outlook.com
P8TN8K-5561	james.mitchell.40@outlook.com
P92YZG-5562	james.mitchell.40@outlook.com
PZ7VVK-5561	james.mitchell.40@outlook.com
Q7RBYH-5562	james.mitchell.40@outlook.com
QAQLVH-5561	james.mitchell.40@outlook.com
QFHW6F-5561	james.mitchell.40@outlook.com
QZQWEG-5561	james.mitchell.40@outlook.com
R7BE8H-5562	james.mitchell.40@outlook.com
TANE4A-5561	james.mitchell.40@outlook.com
TEV68F-5561	james.mitchell.40@outlook.com
TXBE8F-5561	james.mitchell.40@outlook.com
U3ZBAC-5562	james.mitchell.40@outlook.com
VBBWX7-5562	james.mitchell.40@outlook.com
VZACVE-5562	james.mitchell.40@outlook.com
W2ZUC7-5562	I have processed the image using Axiom forensics tool and with operating system artifacts I can see the owner details as james.mitchell.40@outlook.com
WVD6QB-5561	james.mitchell.40@outlook.com
XGCTUC-5561	james.mitchell.40@outlook.com
Y78Z2B-5561	james.mitchell.40@outlook.com
YCA984-5562	james.mitchell.40@outlook.com
Z4WK8A-5562	james.mitchell.40@outlook.com
Z6A992-5561	james.mitchell.40@outlook.com

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

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 5 - Operating System / Registry Analysis

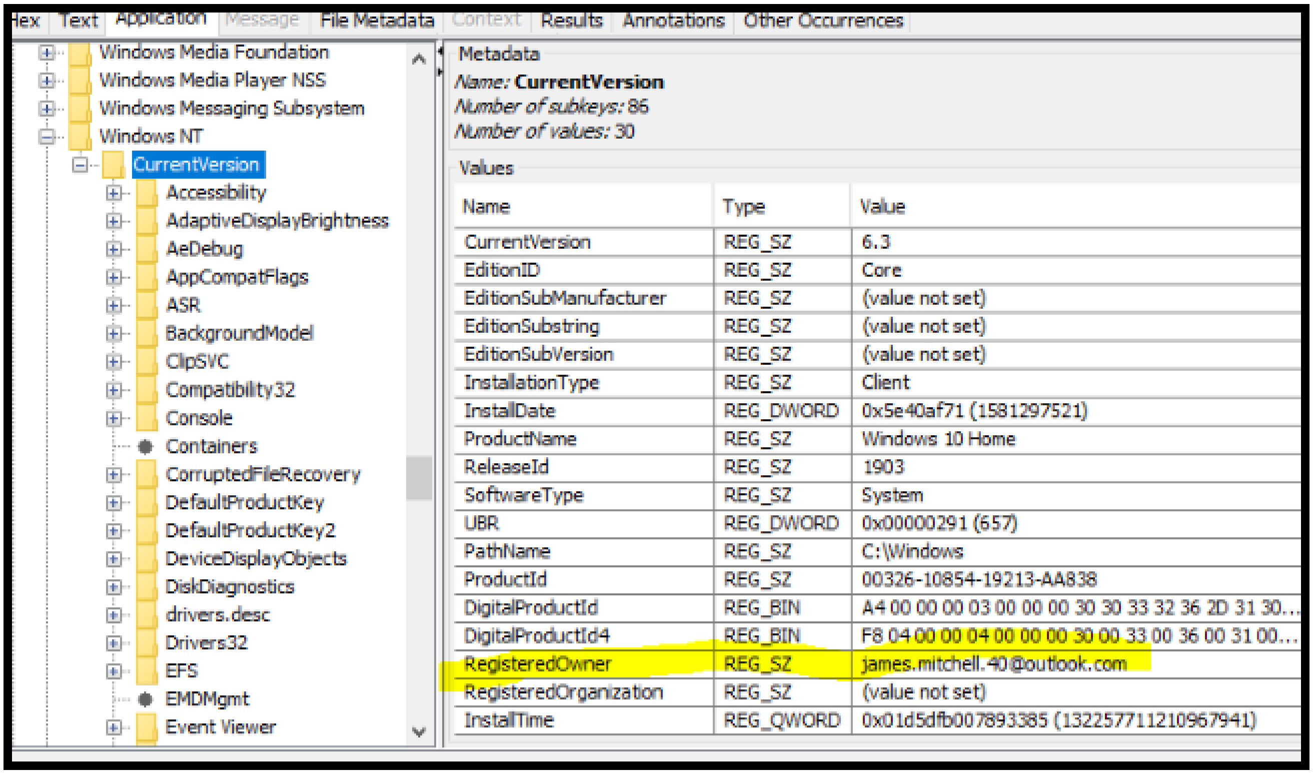
Consensus Result: james.mitchell.40@outlook.com

Expected Response Explanation:

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

Expected Response Illustration:

OS Metadata:



Metadata

Name: **CurrentVersion**

Number of subkeys: 86

Number of values: 30

Values

Name	Type	Value
CurrentVersion	REG_SZ	6.3
EditionID	REG_SZ	Core
EditionSubManufacturer	REG_SZ	(value not set)
EditionSubstring	REG_SZ	(value not set)
EditionSubVersion	REG_SZ	(value not set)
InstallationType	REG_SZ	Client
InstallDate	REG_DWORD	0x5e40af71 (1581297521)
ProductName	REG_SZ	Windows 10 Home
ReleaseId	REG_SZ	1903
SoftwareType	REG_SZ	System
UBR	REG_DWORD	0x00000291 (657)
PathName	REG_SZ	C:\Windows
ProductId	REG_SZ	00326-10854-19213-AA838
DigitalProductId	REG_BIN	A4 00 00 00 03 00 00 00 30 30 33 32 36 2D 31 30...
DigitalProductId4	REG_BIN	F8 04 00 00 04 00 00 00 30 00 33 00 36 00 31 00...
RegisteredOwner	REG_SZ	james.mitchell.40@outlook.com
RegisteredOrganization	REG_SZ	(value not set)
InstallTime	REG_QWORD	0x01d5dfb007893385 (132257711210967941)

TABLE 1

Question 6 - Operating System / Registry Analysis

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: 02/10/2020 01:18:41 AM (UTC)

WebCode-Test	Response
2ZQE6A-5561	02/10/2020 01:18:41 AM
4XFB84-5561	2/10/2020 01:18:41 AM
64W7NX-5562	02/10/2020 01:18:41
6U9F26-5561	2/10/2020 1:18:41 AM
6ZF77W-5562	02/10/2020 01:18:41 AM
7K2ZUX-5562	02/10/2020 01:18:41 AM
7M9E24-5561	02/10/2020 01:18:41 PM
8Q3VR3-5562	02/10/2020 01:18:41 AM
9ENXLY-5561	2/10/2020 1:18:41 AM
ABKKEY-5561	02/10/2020 01:18:41 AM
AQCK6Y-5561	02/10/2020 01:18:41 AM
BJTE9R-5562	02/10/2020 01:18:41 AM (UTC + 00:00)
C8D7KQ-5561	02/10/2020 01:18:41 AM
CCTE9P-5562	2/10/2020 1:18:41 AM UTC
CKXLNP-5561	02/10/2020 01:18:41 AM
CPXWKP-5562	02/10/2020 01:18:41 AM
DGFL7P-5562	The operating system was installed according to the registry \Windows\System32\config\SOFTWARE\Microsoft\Windows NT\CurrentVersion. 2/10/2020 1:18:41 AM UTC
DX4YHV-5561	02/10/2020 01:18:41 AM
EQHHC7-5562	10/02/2020 01:18:41
ETQDAP-5562	02/10/2020 01:18:41 AM
HG3KCP-5561	2/10/2020 01:18:41 AM
HHBXTQ-5562	02/10/2020 01:18:41 AM
J6MAYJ-5561	02/10/2020 1:18:41 AM

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 6 - Operating System / Registry Analysis

WebCode-Test	Response
KH3VVH-5562	02/10/2020 01:18:41 AM
MTJYGM-5562	02/10/2020 01:18:41 AM
NF4QTK-5562	02/10/2020 01:18:41 AM
NZEF7H-5561	02/10/2020 01:18:41 AM
P6M4JK-5562	02/10/2020 01:18:41 AM
P8TN8K-5561	02/10/2020 01:18:41 AM
P92YZG-5562	02/10/2020 1:18:41 AM
PZ7VVK-5561	02/10/2020 01:18:41 AM
Q7RBYH-5562	02/10/2020 01:18:41 AM
QAQLVH-5561	02/10/2020 01:18:41 AM
QFHW6F-5561	02/10/2020 01:18:41 AM
QZQWEG-5561	02/10/2020 01:18:41 AM (UTC)
R7BE8H-5562	02/10/2020 1:18:41
TANE4A-5561	6. 02/10/2020 01:18:41 AM
TEV68F-5561	02/10/2020 01:18:41 AM
TXBE8F-5561	02/10/2020 01:18:41 AM
U3ZBAC-5562	02/10/20 01:18:41
VBBWX7-5562	02/10/2020 01:18:41 AM
VZACVE-5562	02/10/2020 01:18:41 AM
W2ZUC7-5562	By the converting the registry key value under HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\InstallDate with the help of Dcode tool, I can see that the original installation date as 02/10/2020 01:18:41 AM UTC
WVD6QB-5561	02/10/2020 01:18:41 AM
XGCTUC-5561	02/10/2020 01:18:41 AM
Y78Z2B-5561	02/10/2020 01:18:41 AM
YCA984-5562	02/10/2020 01:18:41 AM
Z4WK8A-5562	02/10/2020 01:18:41 AM

TABLE 1

Question 6 - Operating System / Registry Analysis

WebCode-Test	Response
Z6A992-5561	02/10/2020 01:18:41 AM

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

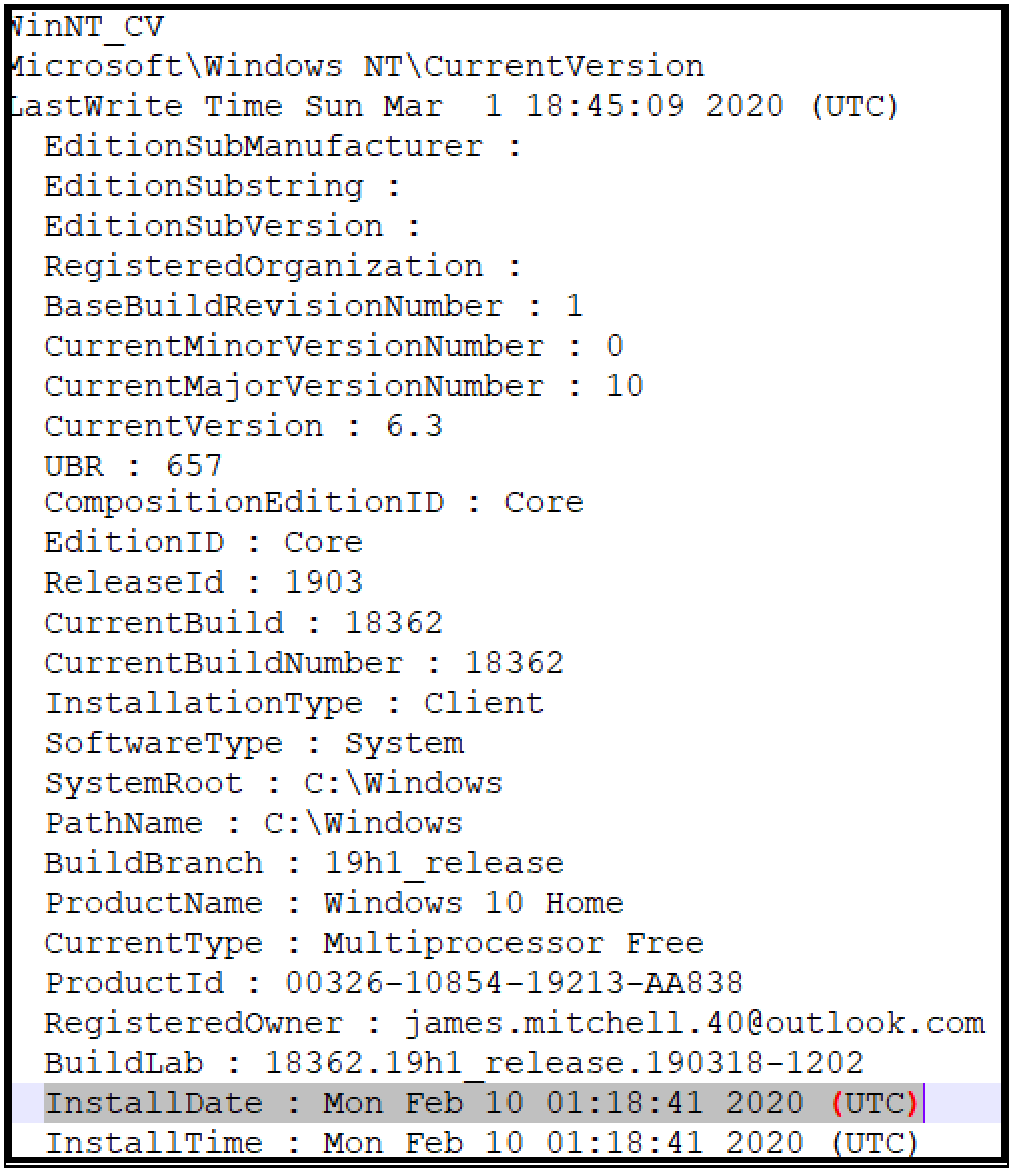
Consensus Result: 02/10/2020 01:18:41 AM (UTC) and all formatting styles which represent the same information.

Expected Response Explanation:

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

Expected Response Illustration:

RegRipper Parsed SOFTWARE registry key:



```
WinNT_CV
Microsoft\Windows NT\CurrentVersion
LastWrite Time Sun Mar  1 18:45:09 2020 (UTC)
  EditionSubManufacturer :
  EditionSubstring :
  EditionSubVersion :
  RegisteredOrganization :
  BaseBuildRevisionNumber : 1
  CurrentMinorVersionNumber : 0
  CurrentMajorVersionNumber : 10
  CurrentVersion : 6.3
  UBR : 657
  CompositionEditionID : Core
  EditionID : Core
  ReleaseId : 1903
  CurrentBuild : 18362
  CurrentBuildNumber : 18362
  InstallationType : Client
  SoftwareType : System
  SystemRoot : C:\Windows
  PathName : C:\Windows
  BuildBranch : 19h1_release
  ProductName : Windows 10 Home
  CurrentType : Multiprocessor Free
  ProductId : 00326-10854-19213-AA838
  RegisteredOwner : james.mitchell.40@outlook.com
  BuildLab : 18362.19h1_release.190318-1202
  InstallDate : Mon Feb 10 01:18:41 2020 (UTC)
  InstallTime : Mon Feb 10 01:18:41 2020 (UTC)
```

TABLE 1

Question 7 - Operating System / Registry Analysis

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: 03/01/2020 07:24:38 PM (UTC)

WebCode-Test	Response
2ZQE6A-5561	03/01/2020 07:24:38 PM
4XFB84-5561	03/01/2020 07:24:38 PM
64W7NX-5562	03/01/2020 19:24:38 PM
6U9F26-5561	3/1/2020 7:24:38 PM
6ZF77W-5562	03/01/2020 07:24:38 PM
7K2ZUX-5562	02/10/2020 01:18:41 AM
7M9E24-5561	03/01/2020 07:24:38 PM
8Q3VR3-5562	03/01/2020 07:24:38 PM
9ENXLY-5561	3/1/2020 07:24:38 PM (19:24:38) UTC
ABKKEY-5561	03/01/2020 07:24:38 PM
AQCK6Y-5561	03/01/2020 07:24:38 PM
BJTE9R-5562	03/01/2020 07:24:38 PM (UTC + 00:00)
C8D7KQ-5561	03/01/2020 19:24:38 PM
CCTE9P-5562	3/1/2020 7:24:38 PM UTC
CKXLNP-5561	03/01/2020 07:24:34 PM
CPXWKP-5562	03/01/2020 07:24:38 PM
DGFL7P-5562	The computer was last shutdown according to the registry \Windows\System32\config\SOFTWARE\Microsoft\Windows NT\CurrentVersion. 3/1/2020 7:24:38 PM UTC
DX4YHV-5561	03/01/2020 07:24:38 PM
EQHHC7-5562	01/03/2020 19:24:38
ETQDAP-5562	03/01/2020 07:24:38 PM
HG3KCP-5561	03/01/2020 07:24:38 PM
HHBXTQ-5562	03/01/2020 07:24:38 PM
J6MAYJ-5561	03/01/2020 19:24:38 PM

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 7 - Operating System / Registry Analysis

WebCode-Test	Response
KH3VVH-5562	03/01/2020 07:24:38 PM
MTJYGM-5562	03/01/2020 07:24:38 PM
NF4QTK-5562	03/01/2020 07:24:38 PM
NZEF7H-5561	03/01/2020 07:24:38 PM
P6M4JK-5562	03/01/2020 07:24:38 PM
P8TN8K-5561	03/01/2020 7:24:38 PM
P92YZG-5562	03/01/2020 7:24:38 PM
PZ7VVK-5561	03/01/2020 07:24:38 PM
Q7RBYH-5562	03/01/2020 19:24:38 PM
QAQLVH-5561	03/01/2020 07:24:38 PM
QFHW6F-5561	03/01/2020 07:24:38 PM
QZQWEG-5561	03/01/2020 07:24:38 PM (UTC)
R7BE8H-5562	03/01/2020 19:24:38
TANE4A-5561	03/01/2020 07:24:38 PM
TEV68F-5561	03/01/2020 7:24:38 PM
TXBE8F-5561	03/1/2020 7:24:38pm-0600
U3ZBAC-5562	03/01/20 19:24:38
VBBWX7-5562	03/01/2020 07:24:38 PM
VZACVE-5562	03/01/2020 7:24:38 PM
W2ZUC7-5562	Using Axiom forensics tool I can see that the last shutdown gracefully was on 03/01/2020 07:24:38 PM UTC. I have also validated the time to be correct from the reg key HKLM\SYSTEM\CurrentControlSet\Control\Windows\ and converted the value of ShutdownTime using Dcode tool.
WVD6QB-5561	03/01/2020 07:24:38 PM
XGCTUC-5561	03/01/2020 07:24:38 PM
Y78Z2B-5561	03/01/2020 07:24:38 PM
YCA984-5562	03/01/2020 07:24:38 PM
Z4WK8A-5562	03/01/2020 07:24:38 PM

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 7 - Operating System / Registry Analysis

WebCode-Test	Response
Z6A992-5561	03/01/2020 07:24:38 PM

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

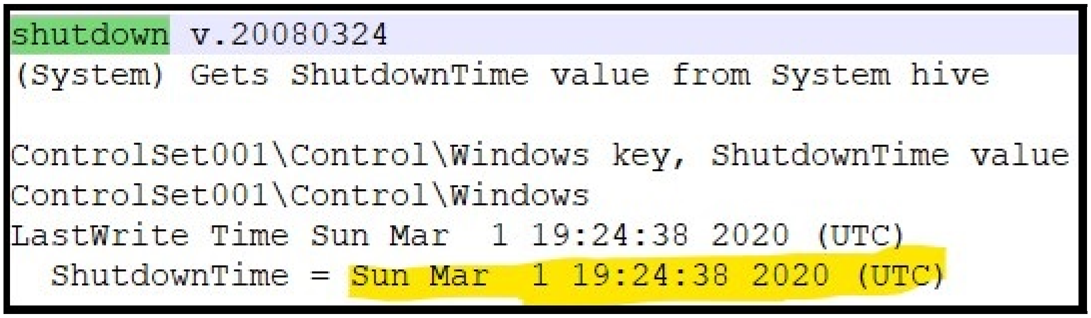
Consensus Result: 03/01/2020 07:24:38 PM (UTC) and all formatting styles which represent the same information.

Expected Response Explanation:

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

Expected Response Illustration:

RegRipper Parsed SYSTEM registry key:



```
shutdown v.20080324
(System) Gets ShutdownTime value from System hive

ControlSet001\Control\Windows key, ShutdownTime value
ControlSet001\Control\Windows
LastWrite Time Sun Mar  1 19:24:38 2020 (UTC)
  ShutdownTime = Sun Mar  1 19:24:38 2020 (UTC)
```

TABLE 1

Question 8 - Operating System / Registry Analysis

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

Manufacturer's Expected Response: james

WebCode-Test	Response
2ZQE6A-5561	james
4XFB84-5561	james
64W7NX-5562	James
6U9F26-5561	james
6ZF77W-5562	james
7K2ZUX-5562	james
7M9E24-5561	James
8Q3VR3-5562	james
9ENXLY-5561	james
ABKKEY-5561	james
AQCK6Y-5561	james
BJTE9R-5562	james
C8D7KQ-5561	james
CCTE9P-5562	james
CKXLNP-5561	james
CPXWKP-5562	james
DGFL7P-5562	the user account created is called james according to the registry \Windows\System32\config\SAM\Domains\Account\Users\000003E9
DX4YHV-5561	james
EQHHC7-5562	james
ETQDAP-5562	james
HG3KCP-5561	James
HHBXTQ-5562	james
J6MAYJ-5561	james
KH3VVH-5562	james

TABLE 1

Question 8 - Operating System / Registry Analysis

WebCode-Test	Response
MTJYGM-5562	james
NF4QTK-5562	james
NZEF7H-5561	james
P6M4JK-5562	james
P8TN8K-5561	james
P92YZG-5562	james
PZ7VVK-5561	james
Q7RBYH-5562	james
QAQLVH-5561	james
QFHW6F-5561	james
QZQWEG-5561	james
R7BE8H-5562	James
TANE4A-5561	james
TEV68F-5561	james
TXBE8F-5561	james
U3ZBAC-5562	james
VBBWX7-5562	james
VZACVE-5562	james
W2ZUC7-5562	The answer is james. I have processed the image using Axiom forensics tool and with 'user accounts' artifact I am able to find the user account created by the user as 'james'
WVD6QB-5561	james
XGCTUC-5561	james
Y78Z2B-5561	james
YCA984-5562	james
Z4WK8A-5562	james
Z6A992-5561	james

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

TABLE 1

Question 8 - Operating System / Registry Analysis

Consensus Result: james

Expected Response Explanation:

There is only one user-created account on this device. Information about user (and system) accounts is found in the System Accounts Manager registry hive at C:\Windows\System32\Config\SAM: and can be parsed with most forensic suites or a standalone tool like regripper or RegistryExplorer.

Expected Response Illustration:

System Accounts Manager registry hive:

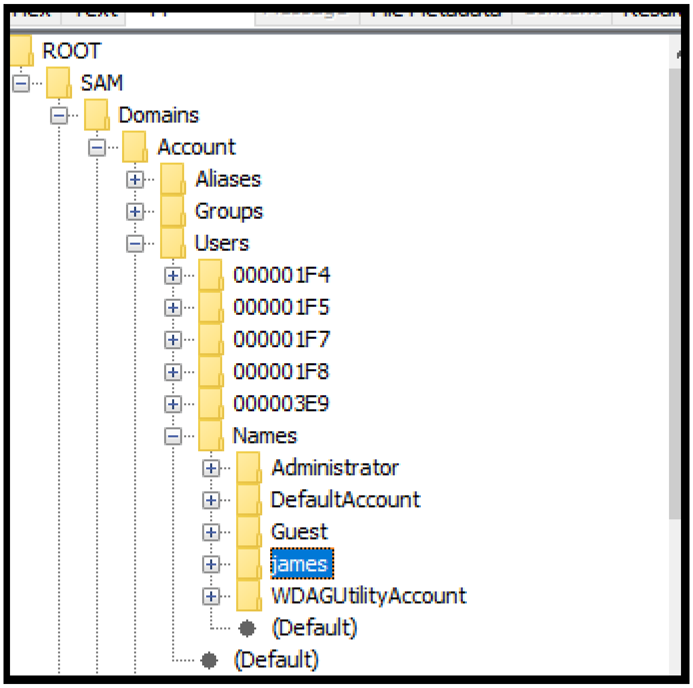


TABLE 1

Question 9 - Operating System / Registry Analysis

Question 9: What is the SID of the user account created by the user?

Manufacturer's Expected Response: S-1-5-21-4282868925-760505910-2700774193-1001

WebCode-Test	Response
2ZQE6A-5561	S-1-5-21-4282868925-760505910-2700774193-1001
4XFB84-5561	S-1-5-21-4282868925-760505910-2700774193-1001
64W7NX-5562	S-1-5-21-4282868925-760505910-2700774193-1001
6U9F26-5561	S-1-5-21-4282868925-760505910-2700774193-1001
6ZF77W-5562	S-1-5-21-4282868925-760505910-2700774193-1001
7K2ZUX-5562	S-1-5-21-4282868925-760505910-2700774193-1001
7M9E24-5561	S-1-5-21-4282868925-760505910-2700774193-1001
8Q3VR3-5562	S-1-5-21-4282868925-760505910-2700774193-1001
9ENXLY-5561	S-1-21-4282868925-760505910-2700774193-1001
ABKKEY-5561	S-1-5-21-4282868925-760505910-2700774193-1001
AQCK6Y-5561	S-1-5-21-4282868925-760505910-2700774193-1001
BJTE9R-5562	S-1-5-21-4282868925-760505910-2700774193-1001
C8D7KQ-5561	S-1-5-21-4282868925-760505910-2700774193-1001
CCTE9P-5562	S-1-5-21-4282868925-760505910-2700774193-1001
CKXLNP-5561	S-1-5-21-4282868925-760505910-2700774193-1001
CPXWKP-5562	S-1-5-21-4282868925-760505910-2700774193-1001
DGFL7P-5562	the SID of the account james according to the registry \Windows\System32\config\SAM\Domains\Account\Users\000003E9. S-1-5-21-4282868925-760505910-2700774193-1001
DX4YHV-5561	S-1-5-21-4282868925-760505910-2700774193-1001
EQHHC7-5562	S-1-5-21-4282868925-760505910-2700774193-1001
ETQDAP-5562	S-1-5-21-4282868925-760505910-2700774193-1001
HG3KCP-5561	S-1-5-21-4282868925-760505910-27007741-93-1001
HHBXTQ-5562	S-1-5-21-4282868925-760505910-2700774193-1001
J6MAYJ-5561	S-1-5-21-4282868925-760505910-2700774193-1001

TABLE 1

Question 9 - Operating System / Registry Analysis

WebCode-Test	Response
KH3VVH-5562	S-1-5-21-4282868925-760505910-2700774193-1001
MTJYGM-5562	S-1-5-21-4282868925-760505910-2700774193-1001
NF4QTK-5562	S-1-5-21-4282868925-760505910-2700774193-1001
NZEF7H-5561	S-1-5-21-4282868925-760505910-2700774193-1001
P6M4JK-5562	S-1-5-21-4282868925-760505910-2700774193-1001
P8TN8K-5561	S-1-5-21-4282868925-760505910-2700774193-1001
P92YZG-5562	S-1-5-21-4282868925-760505910-2700774193-1001
PZ7VVK-5561	S-1-5-21-4282868925-760505910-2700774193-1001
Q7RBYH-5562	S-1-5-21-4282868925-760505910-2700774193-1001
QAQLVH-5561	S-1-5-21-4282868925-760505910-2700774193-1001
QFHW6F-5561	S-1-5-21-4282868925-760505910-2700774193-1001
QZQWEG-5561	S-1-5-21-4282868925-760505910-2700774193-1001
R7BE8H-5562	S-1-5-21-4282868925-760505910-2700774193-1001
TANE4A-5561	S-1-5-21-4282868925-760505910-2700774193-1001
TEV68F-5561	S-1-5-21-4282868925-760505910-2700774193-1001
TXBE8F-5561	1001
U3ZBAC-5562	S-1-5-21-4282868925-760505910-2700774193-1001
VBBWX7-5562	S-1-5-21-4282868925-760505910-2700774193-1001
VZACVE-5562	S-1-5-21-4282868925-760505910-2700774193-1001
W2ZUC7-5562	The answer is S-1-5-21-4282868925-760505910-2700774193-1001. I have processed the image using Axiom forensics tool and with 'user accounts' artifact I am able to find the SID of the user as S-1-5-21-4282868925-760505910-2700774193-1001
WVD6QB-5561	S-1-5-21-4282868925-760505910-2700774193-1001
XGCTUC-5561	S-1-5-21-4282868925-760505910-2700774193-1001
Y78Z2B-5561	S-1-5-21-4282868925-760505910-2700774193-1001
YCA984-5562	S-1-5-21-4282868925-760505910-2700774193-1001
Z4WK8A-5562	S-1-5-21-4282868925-760505910-2700774193-1001

TABLE 1

Question 9 - Operating System / Registry Analysis

WebCode-Test	Response
Z6A992-5561	S-1-5-21-4282868925-760505910-2700774193-1001

Question 9: What is the SID of the user account created by the user?

Consensus Result: S-1-5-21-4282868925-760505910-2700774193-1001

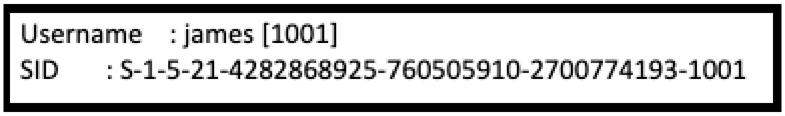
Expected Response Explanation:

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

Username : james [1001]
SID : S-1-5-21-4282868925-760505910-2700774193-1001

Expected Response Illustration:

RegRipper Parsed SAM registry key:



```
Username   : james [1001]
SID      : S-1-5-21-4282868925-760505910-2700774193-1001
```

TABLE 1

Question 10 - Operating System / Registry Analysis

Question 10: What is the configured time zone?

Manufacturer's Expected Response: Pacific Standard Time

WebCode-Test	Response
2ZQE6A-5561	Pacific Standard Time (PST)
4XFB84-5561	Pacific Standard Time
64W7NX-5562	Pacific Standard Time
6U9F26-5561	Pacific Standard Time (UTC-08:00)
6ZF77W-5562	Pacific Standard Time
7K2ZUX-5562	Pacific Standard Time
7M9E24-5561	Pacific
8Q3VR3-5562	(UTC-08:00) Pacific Time (US & Canada)
9ENXLY-5561	Pacific Standard Time
ABKKEY-5561	Pacific Standard Time
AQCK6Y-5561	Pacific Standard Time
BJTE9R-5562	Pacific Standard Time
C8D7KQ-5561	Pacific Standard Time
CCTE9P-5562	(UTC-08:00) Pacific Time (US & Canada)
CKXLNP-5561	(UTC-08:00) Pacific Time (US & Canada)
CPXWKP-5562	(UTC-08:00) Pacific Time (US & Canada)
DGFL7P-5562	the timezone according to the registry is Pacific Standard Time
DX4YHV-5561	Pacific Standard Time
EQHHC7-5562	Pacific Standard Time
ETQDAP-5562	(UTC-08:00) Pacific Time (US & Canada)
HG3KCP-5561	Pacific Standard Time
HHBXTQ-5562	Pacific Standard Time
J6MAYJ-5561	Pacific Standard Time
KH3VVH-5562	(UTC-08:00) Pacific Time (US & Canada)

TABLE 1

Question 10 - Operating System / Registry Analysis

WebCode-Test	Response
MTJYGM-5562	Pacific Standard Time
NF4QTK-5562	Pacific Time (PST)
NZEF7H-5561	Pacific Time (UTC -08:00), Bias/Offset: -480
P6M4JK-5562	Pacific Standard Time
P8TN8K-5561	Pacific
P92YZG-5562	Pacific Standard Time (UTC -8:00)
PZ7VVK-5561	Pacific Standard Time
Q7RBYH-5562	Pacific Standard Time
QAQLVH-5561	Pacific Standard Time
QFHW6F-5561	Pacific Standard Time
QZQWEG-5561	Pacific Standard Time
R7BE8H-5562	Pacific Standard Time
TANE4A-5561	UTC-08:00 Pacific Standard Time
TEV68F-5561	(UTC-08:00) Pacific Time (US & Canada)
TXBE8F-5561	PACIFIC STANDARD TIME
U3ZBAC-5562	Pacific Time
VBBWX7-5562	(UTC-08:00) Pacific Time (US & Canada)
VZACVE-5562	(UTC-08:00) Pacific Time (US & Canada)
W2ZUC7-5562	The answer is Pacific Standard Time. I have processed the image using Axiom forensics tool and with the help of 'Timezone Information' artifact I am able to find that the machine is configured with Pacific Standard Time time zone and daylight time zone is Pacific daylight time
WVD6QB-5561	Pacific Standard Time
XGCTUC-5561	Pacific Standard Time with daylight savings
Y78Z2B-5561	(UTC-08:00) Pacific Time (US & Canada)
YCA984-5562	Pacific Standard Time
Z4WK8A-5562	(UTC-08:00) Pacific Time (US & Canada)
Z6A992-5561	Pacific Standard Time

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 10 - Operating System / Registry Analysis

Question 10: What is the configured time zone?

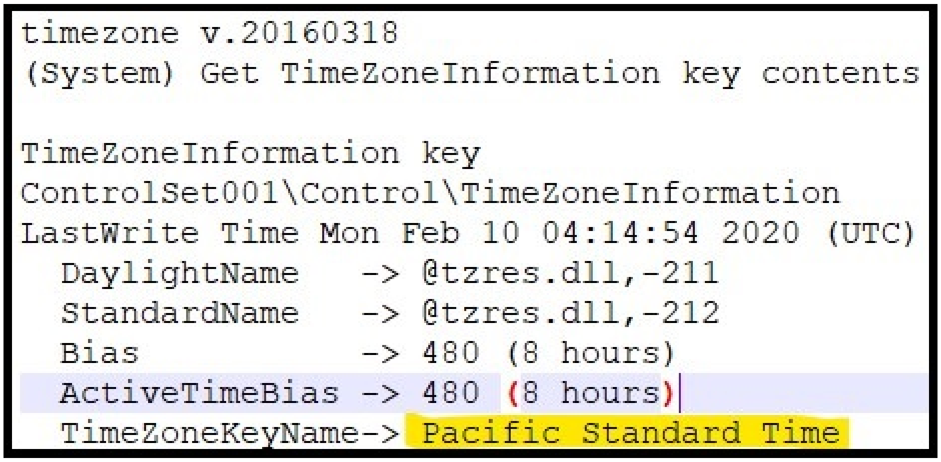
Consensus Result: Pacific Standard Time

Expected Response Explanation:

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

Expected Response Illustration:

System registry hive:



```
timezone v.20160318
(System) Get TimeZoneInformation key contents

TimeZoneInformation key
ControlSet001\Control\TimeZoneInformation
LastWrite Time Mon Feb 10 04:14:54 2020 (UTC)
  DaylightName   -> @tzres.dll,-211
  StandardName   -> @tzres.dll,-212
  Bias           -> 480 (8 hours)
  ActiveTimeBias -> 480 (8 hours)
  TimeZoneKeyName-> Pacific Standard Time
```

TABLE 1

Question 11 - Operating System / Registry Analysis

Question 11: What was the name (Volume Label) of the LAST drive mounted on this computer?

Manufacturer's Expected Response: ResponseTools

** Inconsistencies not highlighted; No consensus achieved **

WebCode-Test	Response
2ZQE6A-5561	ResponseTools
4XFB84-5561	Samsung portable SSD T1 USB Device
64W7NX-5562	ResponseTools
6U9F26-5561	VBOX HARDDISK - This drive contained 2 partitions and the C:\ drive (not named) was the last to be mounted.
6ZF77W-5562	ResponseTools
7K2ZUX-5562	VeraCryptVolumeV
7M9E24-5561	VeraCryptVolumeV
8Q3VR3-5562	ResponseTools
9ENXLY-5561	[Participant did not return results for this question.]
ABKKEY-5561	ResponseTools
AQCK6Y-5561	VeracryptVolumeV
BJTE9R-5562	Response Tools
C8D7KQ-5561	Samsung Portable SSD T1 USB Device S25JNAAGB17529N_____&0
CCTE9P-5562	ResponseTools
CKXLNP-5561	PURP1G
CPXWKP-5562	ResponseTools
DGFL7P-5562	The volume label of the last drive mounted to this computer was RESPONSE TOOLS which was found in the registry \SOFTWARE\Microsoft\Windows Portable Devices. The last connection date was 2020-03-01 17:54:04
DX4YHV-5561	PURP1G
EQHHC7-5562	PERP1G
ETQDAP-5562	PURP1G
HG3KCP-5561	Samsung Portable SSD T1 USB Drive
HHBXTQ-5562	ResponseTools
J6MAYJ-5561	F
KH3VVH-5562	PURP1G

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 11 - Operating System / Registry Analysis

WebCode-Test	Response ** Inconsistencies not highlighted; No consensus achieved **
MTJYGM-5562	VeracryptVolumeV
NF4QTK-5562	VeraCryptVolumeV
NZEF7H-5561	PURP1G
P6M4JK-5562	"ResponseTools"
P8TN8K-5561	VeraCryptVolumeV
P92YZG-5562	ResponseTools
PZ7VVK-5561	Samsung Portable SSD T1 USB device
Q7RBYH-5562	PURP1G
QAQLVH-5561	ResponseTools
QFHW6F-5561	Response Tools
QZQWEG-5561	ResponseTools
R7BE8H-5562	E:\ (Samsung Portable SSD T1 USB Device)
TANE4A-5561	ResponseTools
TEV68F-5561	20200301\
TXBE8F-5561	PURP1G
U3ZBAC-5562	VeraCryptVolumeV
VBBWX7-5562	ResponseTools
VZACVE-5562	20200301
W2ZUC7-5562	The answer is 'ResponseTools'. Based on the registry value SOFTWARE\Microsoft\Windows Portable Devices\Devices, the last mounted device volume label is 'ResponseTools'
WVD6QB-5561	ResponseTools
XGCTUC-5561	PURP1G
Y78Z2B-5561	E:\
YCA984-5562	ResponseTools
Z4WK8A-5562	PURP1G
Z6A992-5561	ResponseTools

Question 11: What was the name (Volume Label) of the LAST drive mounted on this computer?

TABLE 1

Question 11 - Operating System / Registry Analysis

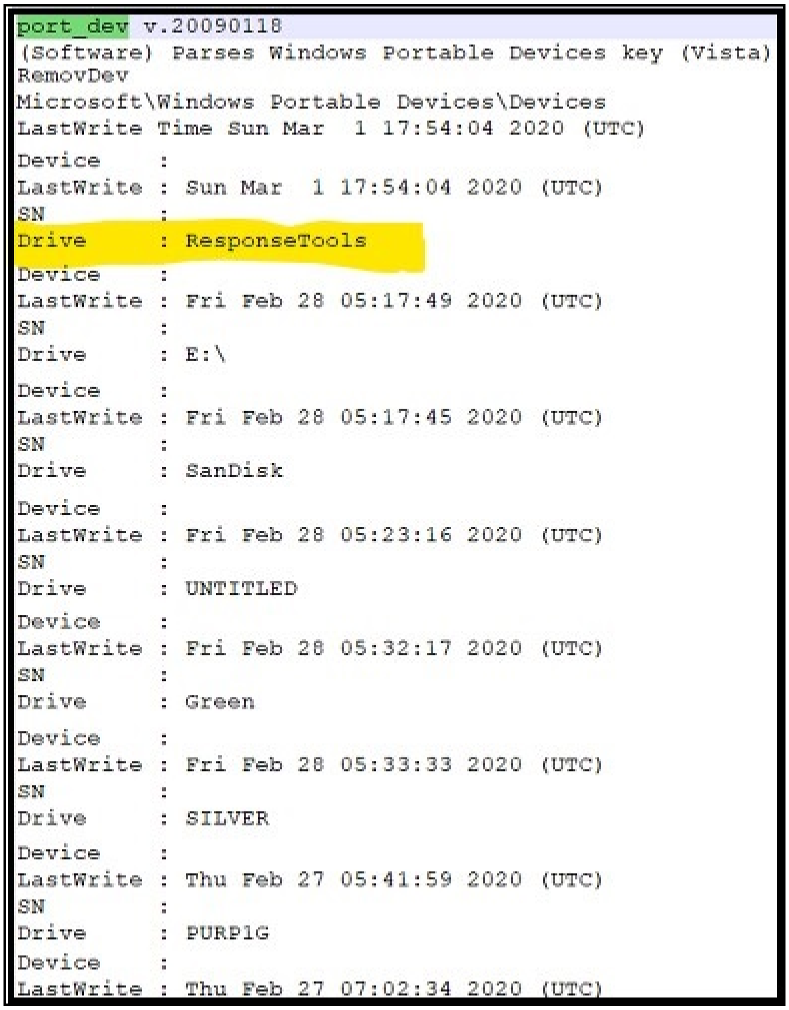
Consensus Result: A consensus was not achieved. The objective of this question was to have the examiner identify the location where mount times are stored and report which volume label was the last drive to be mounted to the computer.

Expected Response Explanation:

Information about mounted devices and last mount times can be found in the software registry hive at C:\windows\system32\config\software:port_dev (removedev) and can be parsed with most forensic suites or a standalone tool like reg-ripper or RegistryExplorer. Only 43% of particpants reported the expected response. Another 21% reported "PURP1G" and 15% reported "VeraCryptVolumeV". For the response of "VeraCryptVolumeV", participants may have been interpreting the last write time for the System:Mounted devices registry key as the last mounted time for the first device listed in that key.

Expected Response Illustration:

Software registry hive:



```
port_dev v.20090118
(Software) Parses Windows Portable Devices key (Vista)
RemovDev
Microsoft\Windows Portable Devices\Devices
LastWrite Time Sun Mar  1 17:54:04 2020 (UTC)
Device    :
LastWrite : Sun Mar  1 17:54:04 2020 (UTC)
SN        :
Drive     : ResponseTools
Device    :
LastWrite : Fri Feb 28 05:17:49 2020 (UTC)
SN        :
Drive     : E:\
Device    :
LastWrite : Fri Feb 28 05:17:45 2020 (UTC)
SN        :
Drive     : SanDisk
Device    :
LastWrite : Fri Feb 28 05:23:16 2020 (UTC)
SN        :
Drive     : UNTITLED
Device    :
LastWrite : Fri Feb 28 05:32:17 2020 (UTC)
SN        :
Drive     : Green
Device    :
LastWrite : Fri Feb 28 05:33:33 2020 (UTC)
SN        :
Drive     : SILVER
Device    :
LastWrite : Thu Feb 27 05:41:59 2020 (UTC)
SN        :
Drive     : PURP1G
Device    :
LastWrite : Thu Feb 27 07:02:34 2020 (UTC)
```

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 12 - Operating System / Registry Analysis

Question 12: Provide the name of the MOST RECENTLY viewed video file?

Manufacturer's Expected Response: SNL-Celebrity Jeopardy- Buck 1.mpg

WebCode-Test	Response
2ZQE6A-5561	SNL-Celebrity Jeopardy- Buck 1.mpg
4XFB84-5561	Skype Incoming-Video-Available.m4a
64W7NX-5562	SNL-Celebrity Jeopardy- Buck 1.mpg
6U9F26-5561	Skype_Incoming_Video_Available.m4a
6ZF77W-5562	SNL-Celebrity Jeopardy- Buck 1.mpg
7K2ZUX-5562	SNL-Celebrity Jeopardy- Buck 1.mpg
7M9E24-5561	Skype_Incoming_Video_Available.m4a or SNL-Celebrity Jeopardy- Buck 1.mpg Comments at the end
8Q3VR3-5562	SNL-Celebrity Jeopardy- Buck 1.mpg
9ENXLY-5561	SNL –Celebrity Jeopardy – Buck 1.mpg
ABKKEY-5561	SNL-Celebrity Jeopardy- Buck 1.mpg
AQCK6Y-5561	SNL-Celebrity Jeopardy- Buck 1.mpg
BJTE9R-5562	SNL-Celebrity Jeopardy- Buck 1.mpg
C8D7KQ-5561	SNL-Celebrity Jeopardy- Buck 1.mpg
CCTE9P-5562	SNL-Celebrity Jeopardy- Buck 1.mpg
CKXLNP-5561	SNL-Celebrity Jeopardy- Buck 1.mpg
CPXWKP-5562	SNL-Celebrity Jeopardy- Buck 1.mpg
DGFL7P-5562	The most recently viewed video file was SNL-Celebrity Jeopardy- Buck 1.mpg according recentdocs registry key in the NTUSER.DAT for the account james located in NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.mpg
DX4YHV-5561	SNL-Celebrity Jeopardy- Buck 1.mpg
EQHHC7-5562	SNL-Celebrity Jeopardy- Buck 1.mpg 01/03/2020 15:48
ETQDAP-5562	SNL-Celebrity Jeopardy- Buck 1.mpg
HG3KCP-5561	Skype_Incoming_Video_Availabe.M4a
HHBXTQ-5562	SNL-Celebrity Jeopardy- Buck 1.mpg
J6MAYJ-5561	SNL-Celebrity Jeopardy- Buck 1.mpg

TABLE 1

Question 12 - Operating System / Registry Analysis

WebCode-Test	Response
KH3VVH-5562	SNL-Celebrity Jeopardy- Buck 1.mpg
MTJYGM-5562	SNL-Celebrity Jeopardy- Buck 1.mpg
NF4QTK-5562	SNL-Celebrity Jeopardy- Buck 1.mpg
NZEF7H-5561	SNL-Celebrity Jeopardy- Buck 1.mpg
P6M4JK-5562	“SNL-Celebrity Jeopardy- Buck 1.mpg ” maybe the answer that this test is suggesting but question clarity is needed. – Although, certain MS Windows MOST RECENTLY USED (MRU) registry keys shows “SNL-Celebrity Jeopardy- Buck 1.mpg” (Full path=E:/Documents/Videos/) as the most recently USED mpg, the “SNL-Celebrity Jeopardy- Buck 1.mpg” that is on thumpdrive is an audio mpg file not a video mpg file. The last accessed actual video file by ACCESS time was “edrcalibration.mkv” (Full path= Windows/servicing/LCU/Package_for_RollupFix~31bf3856ad364e35~amd64~~18362.657.1.7/amd64_microsoft-windows-i..ntrolpanel.appxmain_31bf3856ad364e35_10.0.18362.628_none_70aeb1de288e9915/f/edrcalibration.mkv), but ACCESS time does not equate to viewed. ACCESS times can be changed (and frequently are changed) by various services (anti-virus, windows search indexer, other OS services, etc…) or by the User. Also, some websites may contain video that is partially downloaded like the last accessed video file by ACCESS time in web cache which was “f_000474” (Full path= Users/james/AppData/Local/Google/Chrome/User Data/Default/Cache/f_000474), which is an actual video file.
P8TN8K-5561	SNL-CelebrityJeopardy-Buck1.mpg 3/1/2020 3:48:30 PM
P92YZG-5562	SNL-Celebrity Jeopardy- Buck 1.mpg
PZ7VVK-5561	Skype_Incoming_Video_Available.m4a
Q7RBYH-5562	SNL-Celebrity Jeopardy- Buck 1.mpg
QAQLVH-5561	SNL-Celebrity Jeopardy- Buck 1.mpg
QFHW6F-5561	SNL-Celebrity Jeopardy- Buck 1.mpg
QZQWEG-5561	SNL-Celebrity Jeopardy- Buck 1.mpg
R7BE8H-5562	edrcalibration.mkv
TANE4A-5561	SNL-Celebrity Jeopardy- Buck 1.mpg
TEV68F-5561	WHATSNEW_MTVCON.mp4
TXBE8F-5561	SNL-Celebrity Jeopardy-Buck 1.MPG
U3ZBAC-5562	SNL-Celebrity Jeopardy- Buck 1.mpg
VBBWX7-5562	SNL-Celebrity Jeopardy- Buck 1.mpg
VZACVE-5562	WHATSNEW_MTVCON.mp4
W2ZUC7-5562	The answer is 'SNL-Celebrity Jeopardy- Buck 1.mpg'. Based on the registry key of MRU, NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\ OpenSavePIDlMRU, I see that the most recently viewed video file is 'SNL-Celebrity Jeopardy- Buck 1.mpg'
WVD6QB-5561	SNL-Celebrity Jeopardy- Buck 1.mpg

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 12 - Operating System / Registry Analysis

WebCode-Test	Response
XGCTUC-5561	SNL-Celebrity Jeopardy- Buck 1.mpg
Y78Z2B-5561	SNL-Celebrity Jeopardy- Buck 1.mpg
YCA984-5562	SNL-Celebrity Jeopardy- Buck 1.mpg
Z4WK8A-5562	SNL-Celebrity Jeopardy- Buck 1.mpg
Z6A992-5561	Celebrity Jeopardy – Buck 1.mpg

Question 12: Provide the name of the MOST RECENTLY viewed video file?

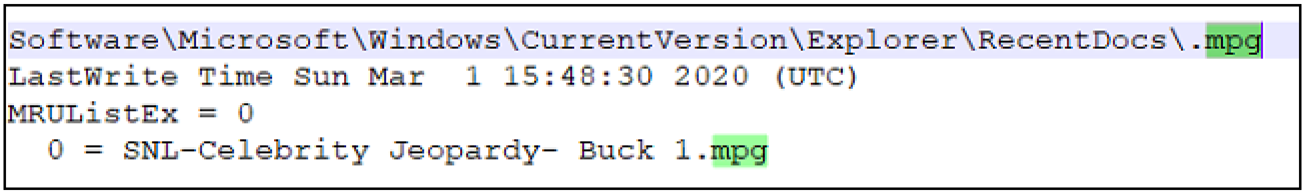
Consensus Result: SNL-Celebrity Jeopardy- Buck 1.mpg

Expected Response Explanation:

Information about recently viewed files can be found in a user's NTUSER.DAT registry hive at C:\users\james\NTUSER.DAT:Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.mpg.

Expected Response Illustration:

NTUSER.DAT registry hive:



```
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.mpg
LastWrite Time Sun Mar  1 15:48:30 2020 (UTC)
MRUListEx = 0
  0 = SNL-Celebrity Jeopardy- Buck 1.mpg
```

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 13 - Operating System / Registry Analysis

Question 13: What is the name of the file the user unsuccessfully attempted to print?

Manufacturer's Expected Response: 20_back.xcf

WebCode-Test	Response
2ZQE6A-5561	20_back.xcf
4XFB84-5561	20_back.xcf
64W7NX-5562	Embedded 001.png
6U9F26-5561	20_back.xcf
6ZF77W-5562	Print Document
7K2ZUX-5562	Print document
7M9E24-5561	20_back.xcf
8Q3VR3-5562	20_back.xcf
9ENXLY-5561	20_back.xcf
ABKKEY-5561	20_back.xcf
AQCK6Y-5561	Print Document 01/03/2020 03:34
BJTE9R-5562	20_back.xcf
C8D7KQ-5561	00004.SPL
CCTE9P-5562	20_back.xcf
CKXLNP-5561	20_back.xcf
CPXWKP-5562	20_back.xcf
DGFL7P-5562	There are SPL and SHD files in the /Windows/System32/spool/PRINTERS/ called 00004.SPL and 00004.SHD. The presence of these files indicate that the print job may have not have printed successfully. The SHD file indicates the file 20_back.xcf may have been attempted to be printed. james 20_back.xcf HP248C0C (HP ENVY 4520 series) HP ENVY 4520 series
DX4YHV-5561	Print Document
EQHHC7-5562	20_back.xcf
ETQDAP-5562	20_back.xcf
HG3KCP-5561	20_back.xcf
HHBXTQ-5562	20_back.xcf
J6MAYJ-5561	james

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 13 - Operating System / Registry Analysis

WebCode-Test	Response
KH3VVH-5562	20_back.xcf
MTJYGM-5562	Print Document
NF4QTK-5562	20_back.xcf
NZEF7H-5561	20_back.xcf
P6M4JK-5562	20_back.xcf
P8TN8K-5561	20_back.xcf
P92YZG-5562	20_back.xcf
PZ7VVK-5561	20_back.xcf
Q7RBYH-5562	20_back.xcf
QAQLVH-5561	20_back.xcf
QFHW6F-5561	jamesjames20_back.xcf
QZQWEG-5561	20_back.xcf
R7BE8H-5562	20_back.xcf
TANE4A-5561	20_back.xcf
TEV68F-5561	“Print Document” that is Param1 because “Allow job name in event logs” policy is disabled.
TXBE8F-5561	US20-back.jpg
U3ZBAC-5562	20_back.xcf
VBBWX7-5562	20_back.xcf
VZACVE-5562	“Print Document” that is Param1 because “Allow job name in event logs” policy is disabled.
W2ZUC7-5562	The answer is '20_back.xcf'. Under the file system path \Windows\System32\spool\PRINTERS\ I see the shadow file as 00004.SHD. I have extracted the file and opened in HxD editor where i can see that the file the user unsuccessfully attempted to print is '20_back.xcf'
WVD6QB-5561	20_back.xcf
XGCTUC-5561	Print Document
Y78Z2B-5561	20_back.xcf
YCA984-5562	20_back.xcf
Z4WK8A-5562	20_back.xcf

TABLE 1

Question 13 - Operating System / Registry Analysis

WebCode-Test	Response
Z6A992-5561	20_back.xcf

Question 13: What is the name of the file the user unsuccessfully attempted to print?

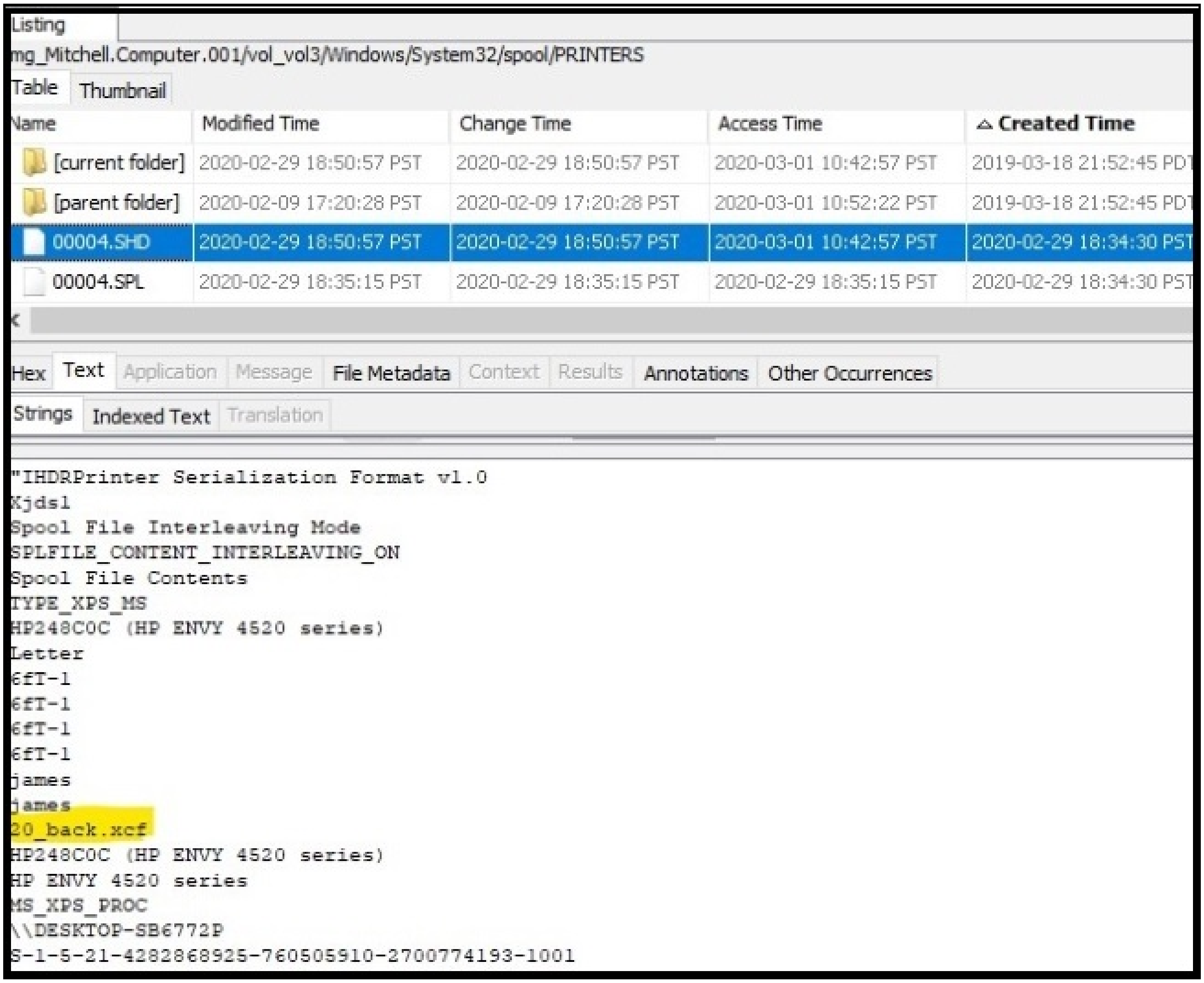
Consensus Result: 20_back.xcf

Expected Response Explanation:

The Windows print spooling process causes the creation of shadow (.SHD) and spool files in C:\windows\system32\spool\PRINTERS\ for each print job. When a print job is successful, both files are deleted. When a job fails, they are not. There is only one such pair of files on the subject image. The shadow file C:\windows\system32\spool\PRINTERS\00004.SHD contains the name of file that was attempted to be printed.

Expected Response Illustration:

Contents of 00004.SHD:



mg_Mitchell.Computer.001/vol_vol3/Windows/System32/spool/PRINTERS

Name	Modified Time	Change Time	Access Time	Created Time
[current folder]	2020-02-29 18:50:57 PST	2020-02-29 18:50:57 PST	2020-03-01 10:42:57 PST	2019-03-18 21:52:45 PDT
[parent folder]	2020-02-09 17:20:28 PST	2020-02-09 17:20:28 PST	2020-03-01 10:52:22 PST	2019-03-18 21:52:45 PDT
00004.SHD	2020-02-29 18:50:57 PST	2020-02-29 18:50:57 PST	2020-03-01 10:42:57 PST	2020-02-29 18:34:30 PST
00004.SPL	2020-02-29 18:35:15 PST	2020-02-29 18:35:15 PST	2020-02-29 18:35:15 PST	2020-02-29 18:34:30 PST

```
"IHDRPrinter Serialization Format v1.0
Kjdsl
Spool File Interleaving Mode
SPLFILE_CONTENT_INTERLEAVING_ON
Spool File Contents
TYPE_XPS_MS
HP248C0C (HP ENVY 4520 series)
Letter
6fT-1
6fT-1
6fT-1
6fT-1
james
james
20_back.xcf
HP248C0C (HP ENVY 4520 series)
HP ENVY 4520 series
MS_XPS_PROC
\\DESKTOP-SB6772P
S-1-5-21-4282868925-760505910-2700774193-1001
```

Other Responses:

"Print Document" was reported by eight participants (17%). This response may have been derived from the event logs but is not a means to identify the name of an unsuccessfully printed file.

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 14 - Operating System / Registry Analysis

Question 14: What networking device did the user attach via USB?

Manufacturer's Expected Response: Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter

WebCode-Test	Response
2ZQE6A-5561	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
4XFB84-5561	Realtex RTL8188EU Wireless LAN802.11n
64W7NX-5562	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
6U9F26-5561	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
6ZF77W-5562	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
7K2ZUX-5562	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
7M9E24-5561	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
8Q3VR3-5562	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
9ENXLY-5561	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
ABKKEY-5561	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
AQCK6Y-5561	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
BJTE9R-5562	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
C8D7KQ-5561	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
CCTE9P-5562	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
CKXLNP-5561	VBOX
CPXWKP-5562	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
DGFL7P-5562	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter according to the registry \Windows\System32\config\SYSTEM
DX4YHV-5561	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
EQHHC7-5562	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter (wireless dongle)
ETQDAP-5562	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
HG3KCP-5561	Realtek RTL8188EU Wireless Lan 802.ln USB 2.0 Network Adapter
HHBXTQ-5562	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
J6MAYJ-5561	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
KH3VVH-5562	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 14 - Operating System / Registry Analysis

WebCode-Test	Response
MTJYGM-5562	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
NF4QTK-5562	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
NZEF7H-5561	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
P6M4JK-5562	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
P8TN8K-5561	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
P92YZG-5562	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
PZ7VVK-5561	Realtek RTL8188EU wireless LAN
Q7RBYH-5562	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
QAQLVH-5561	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
QFHW6F-5561	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
QZQWEG-5561	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
R7BE8H-5562	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
TANE4A-5561	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
TEV68F-5561	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
TXBE8F-5561	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
U3ZBAC-5562	ROOT_HUB30
VBBWX7-5562	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
VZACVE-5562	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
W2ZUC7-5562	The answer is Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter. With the help of Axiom forensic tool (USB devices artifact), I am able to see that the user had connected Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter device via USB (also confirmed this through the registry location – SYSTEM\ControlSet001\Enum\USB\VID_0BDA&PID_8179\00E04C0001)
WVD6QB-5561	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
XGCTUC-5561	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
Y78Z2B-5561	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
YCA984-5562	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
Z4WK8A-5562	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
Z6A992-5561	Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network adapter

TABLE 1

Question 14 - Operating System / Registry Analysis

Question 14: What networking device did the user attach via USB?

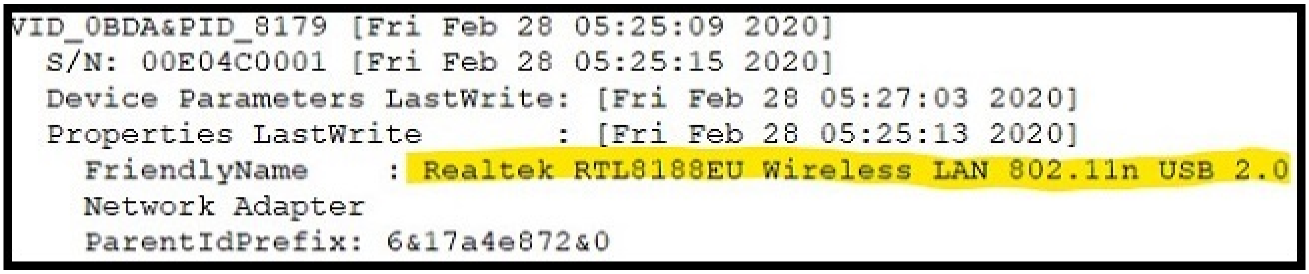
Consensus Result: Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter and all formatting styles which represent the same information. Slight variations of the expected result were disregarded and not considered outliers, if they were easily identified as spelling errors.

Expected Response Explanation:

Information about attached USB devices can be found in the Windows System registry hive at C:\Windows\System32\Config\SYSTEM:ControlSet001\Enum\USB. This key contained only one entry identifying a networking device.

Expected Response Illustration:

RegRipper Parsed SYSTEM registry key:



```
VID_0BDA&PID_8179 [Fri Feb 28 05:25:09 2020]
  S/N: 00E04C0001 [Fri Feb 28 05:25:15 2020]
  Device Parameters LastWrite: [Fri Feb 28 05:27:03 2020]
  Properties LastWrite       : [Fri Feb 28 05:25:13 2020]
    FriendlyName    : Realtek RTL8188EU Wireless LAN 802.11n USB 2.0
    Network Adapter
    ParentIdPrefix: 6&17a4e872&0
```

TABLE 1

Question 15 - Operating System / Registry Analysis

Question 15: Identify an anti-forensics application executed by the user?

Manufacturer's Expected Response: Ccleaner, Eraser or SDelete

WebCode-Test	Response
2ZQE6A-5561	CCleaner / ccPortable (PortableApps)
4XFB84-5561	VeraCrypt Portable 1.2.4
64W7NX-5562	CCleaner64.exe
6U9F26-5561	ccleaner64.exe
6ZF77W-5562	Eraser
7K2ZUX-5562	Eraser.exe
7M9E24-5561	CCleaner64.exe
8Q3VR3-5562	CCLEANER64.EXE
9ENXLY-5561	Eraser.exe
ABKKEY-5561	Tor.exe
AQCK6Y-5561	CCLEANER
BJTE9R-5562	VeraCrypt (from userassist of james); Eraser (from prefetch files); CCleaner64 (from prefetch files)
C8D7KQ-5561	Tor.exe and Veracrypt
CCTE9P-5562	VeraCrypt.exe; tor.exe; SDELETE64.EXE
CKXLNP-5561	CCleaner
CPXWKP-5562	Eraser
DGFL7P-5562	the user james executed ccleaner from E:\PortableApps\ccPortable\App\CCleaner\CCleaner64.exe according to the user registry. \Users\james\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count
DX4YHV-5561	VeraCrypt.exe
EQHHC7-5562	Veracrypt.exe and tor.exe
ETQDAP-5562	ERASER
HG3KCP-5561	Veracrypt
HHBXTQ-5562	CCLEANER64.EXE (E:\PortableApps\ccPortable\App\CCleaner\CCleaner64.exe); SDELETE64.EXE (C:\Users\james\Downloads\SDelete\sdelete64.exe); ERASERPORTABLE.EXE/ERASER.EXE (E:\PortablesApps\EraserPortable\App\eraser\Eraser.exe)

TABLE 1

Question 15 - Operating System / Registry Analysis

WebCode-Test	Response
J6MAYJ-5561	VeraCrypt.exe and tor.exe
KH3VVH-5562	SDELETE
MTJYGM-5562	CCLEANER
NF4QTK-5562	CCleaner64.exe
NZEF7H-5561	Eraser.exe
P6M4JK-5562	sdelete64.exe
P8TN8K-5561	CCleaner64
P92YZG-5562	Eraser Portable
PZ7VVK-5561	Veracrypt.exe
Q7RBYH-5562	ERASER.EXE
QAQLVH-5561	Eraser.exe
QFHW6F-5561	CCLEANER64.EXE
QZQWEG-5561	Ccleaner (ccleaner64.exe)
R7BE8H-5562	VeraCrypt
TANE4A-5561	SDelete
TEV68F-5561	Ccleaner
TXBE8F-5561	CCLeaner
U3ZBAC-5562	Eraser.exe
VBBWX7-5562	Eraser.exe
VZACVE-5562	Ccleaner
W2ZUC7-5562	The answers are Sdelete64.exe, Tor.exe, Ccleaner64.exe, Eraser.exe. Based on the program execution artifacts UserAssist, Shimcache and Prefetch (artifacts in Axiom forensics tool) I have observed the above anti-forensics applications executed by the user. All these tools can be categorized under anti-forensics applications.
WVD6QB-5561	CCleaner (CCleaner64.exe)
XGCTUC-5561	VeraCrypt.exe
Y78Z2B-5561	CCleaner
YCA984-5562	Eraser

TABLE 1

Question 15 - Operating System / Registry Analysis

WebCode-Test	Response
Z4WK8A-5562	Eraser.exe (other anti-forensics applications identified: CCleaner.exe, CCleaner64.exe, veraCrypt.exe, Sdelete64.exe)
Z6A992-5561	CCleaner, VeraCrypt

Question 15: Identify an anti-forensics application executed by the user?

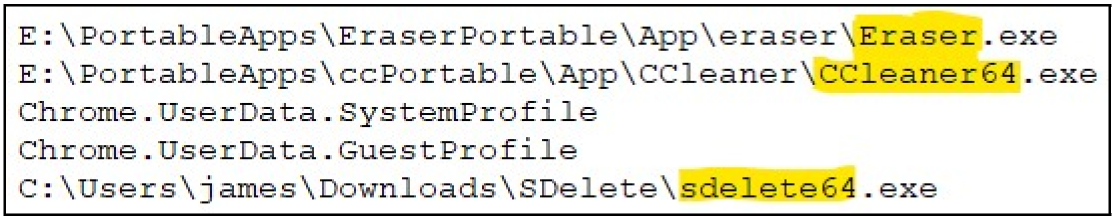
Consensus Result: Ccleaner, Eraser or SDelete

Expected Response Explanation:

Information about executed applications can be found in many places on a Windows computer including prefetch files and within the registry. There are a number of entries in these artifacts for applications which could be considered "Anti-Forensics", or intended to remove artifacts of user activity typically sought in forensic analysis: e.g. C:\users\james\NTUSER.DAT:Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist

Expected Response Illustration:

RegRipper Parsed (james) NTUSER.DAT registry key:



```
E:\PortableApps\EraserPortable\App\eraser\Eraser.exe
E:\PortableApps\ccPortable\App\CCleaner\CCleaner64.exe
Chrome.UserData.SystemProfile
Chrome.UserData.GuestProfile
C:\Users\james\Downloads\SDelete\sdelete64.exe
```

Other Responses:

Thirteen participants reported the encryption program "Veracrypt.exe", four of which also reported at least one of the expected responses. The distinction being that an anti-forensics application is used to remove artifacts of user activity sought during forensic analysis. Whereas, an encryption program is a general privacy application.

TABLE 1

Question 16 - Operating System / Registry Analysis

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

Manufacturer's Expected Response: attwifi

WebCode-Test	Response
2ZQE6A-5561	attwifi
4XFB84-5561	attwifi
64W7NX-5562	attwifi
6U9F26-5561	attwifi
6ZF77W-5562	attwifi
7K2ZUX-5562	Attwifi
7M9E24-5561	attwifi
8Q3VR3-5562	attwifi
9ENXLY-5561	attwifi
ABKKEY-5561	attwifi
AQCK6Y-5561	attwifi
BJTE9R-5562	attwifi
C8D7KQ-5561	attwifi
CCTE9P-5562	attwifi
CKXLNP-5561	Network
CPXWKP-5562	attwifi
DGFL7P-5562	the name of the last wireless network was called Network with a profile name attwifi Last Connected on 2020-02-27 21:27:57 PM PST (or 4:27:57 AM UTC) according to the registry \Windows\System32\config\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkList\Signatures\Unmanaged\
DX4YHV-5561	attwifi
EQHHC7-5562	attwifi
ETQDAP-5562	attwifi
HG3KCP-5561	Att Wifi
HHBXTQ-5562	attwifi
J6MAYJ-5561	attwifi

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 16 - Operating System / Registry Analysis

WebCode-Test	Response
KH3VVH-5562	attwifi
MTJYGM-5562	attwifi
NF4QTK-5562	attwifi
NZEF7H-5561	attwifi
P6M4JK-5562	attwifi
P8TN8K-5561	attwifi
P92YZG-5562	attwifi
PZ7VVK-5561	ATT wifi
Q7RBYH-5562	attwifi
QAQLVH-5561	attwifi
QFHW6F-5561	attwifi
QZQWEG-5561	attwifi
R7BE8H-5562	Attwifi
TANE4A-5561	attwifi
TEV68F-5561	attwifi
TXBE8F-5561	attwifi
U3ZBAC-5562	attwifi
VBBWX7-5562	attwifi
VZACVE-5562	attwifi
W2ZUC7-5562	The answer is attwifi. From the Axiom forensics tool, 'Network Profiles' artifact there are 3 wifi profiles the machine is connected to and based on the timestamp the last wireless network the machine is connected to is 'attwifi'. Validated and confirmed this with the event ID 8001 associated with the Provider Name="Microsoft-Windows-WLAN-AutoConfig" and with the registry value SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged
WVD6QB-5561	attwifi
XGCTUC-5561	attwifi
Y78Z2B-5561	attwifi
YCA984-5562	attwifi

TABLE 1

Question 16 - Operating System / Registry Analysis

WebCode-Test	Response
Z4WK8A-5562	attwifi
Z6A992-5561	attwifi

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

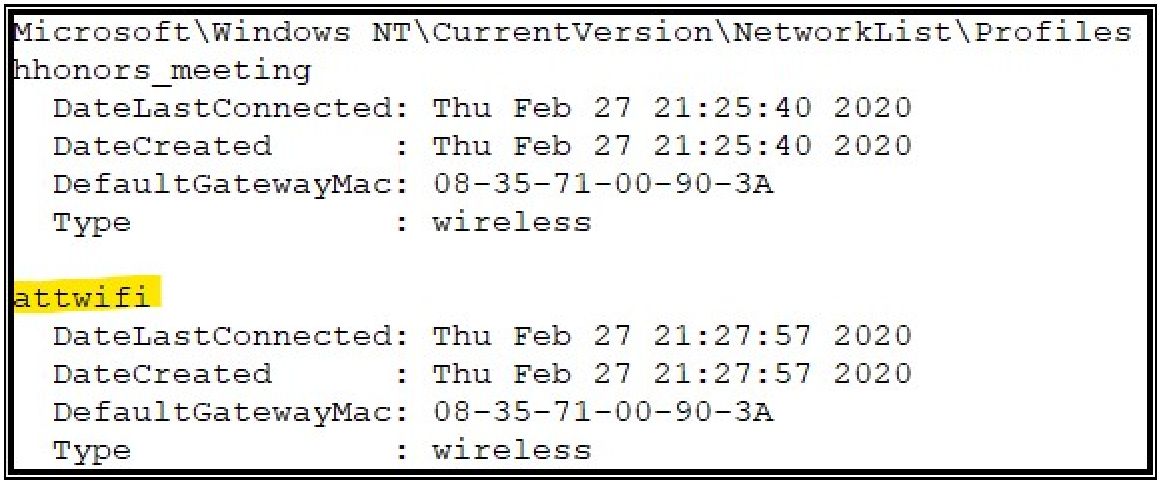
Consensus Result: attwifi

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 attwifi.

Expected Response Illustration:

Windows Software registry hive:



```
Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles
hhonors_meeting
  DateLastConnected: Thu Feb 27 21:25:40 2020
  DateCreated      : Thu Feb 27 21:25:40 2020
  DefaultGatewayMac: 08-35-71-00-90-3A
  Type             : wireless

attwifi
  DateLastConnected: Thu Feb 27 21:27:57 2020
  DateCreated      : Thu Feb 27 21:27:57 2020
  DefaultGatewayMac: 08-35-71-00-90-3A
  Type             : wireless
```

TABLE 1

Question 17 - Operating System / Registry Analysis

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

Manufacturer's Expected Response: 10.21.6.146

WebCode-Test	Response
2ZQE6A-5561	10.21.6.146
4XFB84-5561	10.21.6.146
64W7NX-5562	10.21.6.146
6U9F26-5561	10.21.6.146
6ZF77W-5562	10.21.6.146
7K2ZUX-5562	10.21.6.146
7M9E24-5561	10.21.6.146
8Q3VR3-5562	10.30.8.133
9ENXLY-5561	10.21.6.146
ABKKEY-5561	10.21.6.146
AQCK6Y-5561	10.21.6.146
BJTE9R-5562	10.21.6.146
C8D7KQ-5561	10.21.6.146
CCTE9P-5562	10.21.6.146
CKXLNP-5561	10.21.6.146
CPXWKP-5562	10.21.6.146
DGFL7P-5562	192.228.79.201 according to the registry Microsoft\Windows NT\CurrentVersion\NetworkList
DX4YHV-5561	10.21.6.146
EQHHC7-5562	IPv4 10.21.6.146 --- DNS Domain hil-seaukht.sea.wayport.net
ETQDAP-5562	10.21.6.146
HG3KCP-5561	10.21.6.146
HHBXTQ-5562	10.21.6.146
J6MAYJ-5561	10.21.6.146
KH3VVH-5562	10.21.6.146

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 17 - Operating System / Registry Analysis

WebCode-Test	Response
MTJYGM-5562	10.21.6.146
NF4QTK-5562	10.21.6.146
NZEF7H-5561	10.21.6.146
P6M4JK-5562	10.21.6.146
P8TN8K-5561	10.21.6.146
P92YZG-5562	10.21.6.146
PZ7VVK-5561	10.21.6.146
Q7RBYH-5562	08-35-71-00-90-3A
QAQLVH-5561	10.21.6.146
QFHW6F-5561	10.21.6.146
QZQWEG-5561	10.21.6.146
R7BE8H-5562	10.21.6.146
TANE4A-5561	10.21.6.146
TEV68F-5561	10.21.6.146
TXBE8F-5561	10.0.18362.657
U3ZBAC-5562	10.21.6.146
VBBWX7-5562	10.21.6.146
VZACVE-5562	10.21.6.146
W2ZUC7-5562	The answer is 10.21.6.146. Based on the registry key - HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards the GUID of the interface is {88F2E9AA-6123-482C-95C3-3FD04AAF619D} and with this information and the registry key HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{88F2E9AA-6123-482C-95C3-3FD04AAF619D} the last assigned IP address is 10.21.6.146
WVD6QB-5561	10.21.6.146
XGCTUC-5561	10.21.6.146
Y78Z2B-5561	10.21.6.146
YCA984-5562	10.21.6.146
Z4WK8A-5562	10.21.6.146

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 17 - Operating System / Registry Analysis

WebCode-Test	Response
Z6A992-5561	10.21.6.146

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

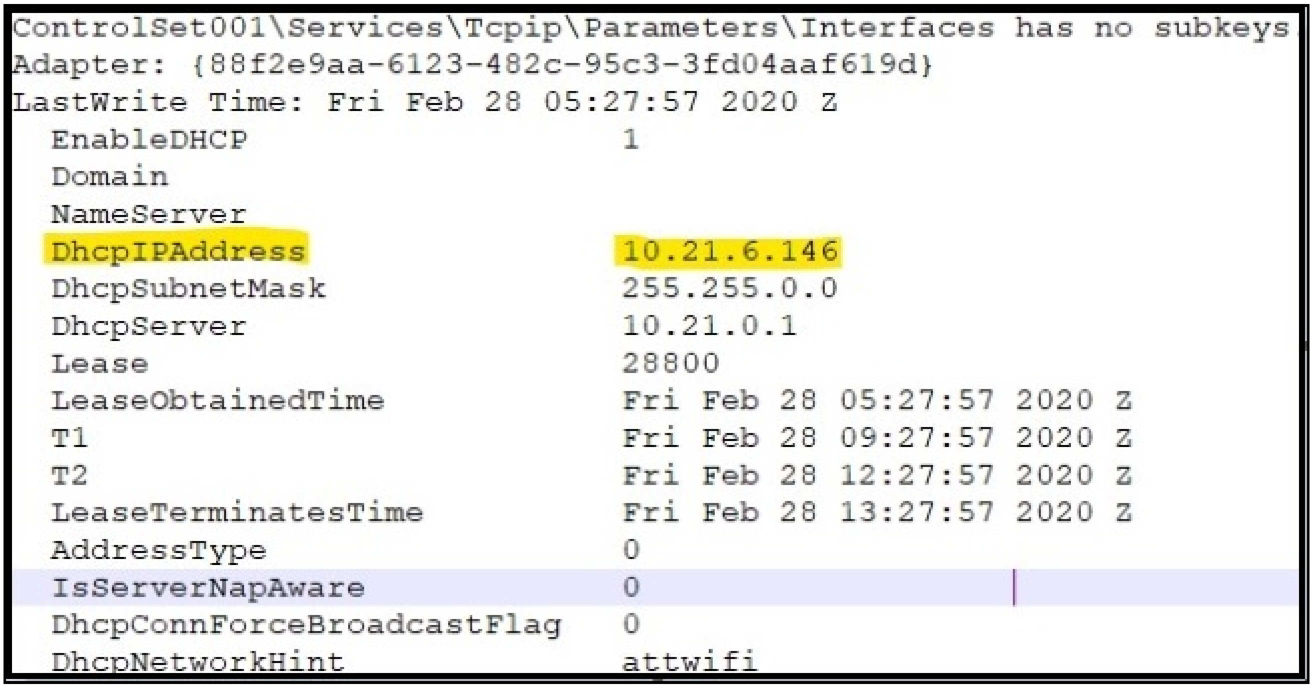
Consensus Result: 10.21.6.146

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:

Windows System registry hive:



```
ControlSet001\Services\Tcpip\Parameters\Interfaces has no subkeys
Adapter: {88f2e9aa-6123-482c-95c3-3fd04aaf619d}
LastWrite Time: Fri Feb 28 05:27:57 2020 Z
  EnableDHCP                  1
  Domain
  NameServer
  DhcpIPAddress               10.21.6.146
  DhcpSubnetMask              255.255.0.0
  DhcpServer                  10.21.0.1
  Lease                       28800
  LeaseObtainedTime           Fri Feb 28 05:27:57 2020 Z
  T1                          Fri Feb 28 09:27:57 2020 Z
  T2                          Fri Feb 28 12:27:57 2020 Z
  LeaseTerminatesTime         Fri Feb 28 13:27:57 2020 Z
  AddressType                 0
  IsServerNapAware            0
  DhcpConnForceBroadcastFlag  0
  DhcpNetworkHint             attwifi
```

TABLE 1

Question 18 - Operating System / Registry Analysis

Question 18: What program did the responding/seizing examiner execute?

Manufacturer's Expected Response: FTK Imager

WebCode-Test	Response
2ZQE6A-5561	FTK Imager (Lite 3.1.1)
4XFB84-5561	Imager_Lite 3.1.1\FTKImager
64W7NX-5562	FTK Imager.exe
6U9F26-5561	FTK Imager Lite (e:\Imager_Lite_3.1.1\FTK Imager.exe)
6ZF77W-5562	FTK Imager
7K2ZUX-5562	FTK Imager
7M9E24-5561	FTK Imager
8Q3VR3-5562	FTK Imager.exe
9ENXLY-5561	FTK Imager.EXE
ABKKEY-5561	FTK Imager.exe
AQCK6Y-5561	FTK Imager
BJTE9R-5562	FTK Imager.exe
C8D7KQ-5561	FTK Imager.exe
CCTE9P-5562	FTK IMAGER.EXE
CKXLNP-5561	FTK IMAGER
CPXWKP-5562	FTK Imager Lite 3.1
DGFL7P-5562	the program executed was ftk imager from E:\Imager_Lite_3.1.1\FTK Imager.exe according to the user registry Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA }\Count
DX4YHV-5561	FTK Imager.exe
EQHHC7-5562	This is dependent on when the device was seized, no time has been provided however, FTK Imager.exe was run at 01/03/2020 18:18:25, thunderbird.exe was run at 01/03/2020 17:18:21 and CCleaner64.exe was run at 01/03/2020 16:58:38.
ETQDAP-5562	FTK IMAGER.EXE
HG3KCP-5561	FTK Imager Imagerlite 3.1.1
HHBXTQ-5562	FTK Imager.exe (E:\Imager_Lite_3.1.1\FTK Imager.exe)
J6MAYJ-5561	FTK Imager

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 18 - Operating System / Registry Analysis

WebCode-Test	Response
KH3VVH-5562	FTK IMAGER.EXE
MTJYGM-5562	FTK Imager
NF4QTK-5562	FTK Imager.exe
NZEF7H-5561	FTK Imager.exe
P6M4JK-5562	"FTK IMAGER.EXE"
P8TN8K-5561	FTK Imager.exe
P92YZG-5562	FTK Imager
PZ7VVK-5561	FTK Imager Lite 3.11
Q7RBYH-5562	FTK Imager.exe
QAQLVH-5561	FTK Imager
QFHW6F-5561	FTK IMAGER.EXE
QZQWEG-5561	FTK Imager (E:\Imager_Lite_3.1.1\FTK Imager.exe)
R7BE8H-5562	FTK Imager
TANE4A-5561	FTK Imager Lite
TEV68F-5561	FTK Imager
TXBE8F-5561	Imager_Lite_3.1.1\FTK Imager.exe
U3ZBAC-5562	Imager_Lite_3.1.1\FTK Imager.exe
VBBWX7-5562	FTK Imager.exe
VZACVE-5562	FTK Imager
W2ZUC7-5562	I have processed the image using Axiom forensics tool and with prefetch data, i can see that the the examiner executed FTKImager program.
WVD6QB-5561	Imager_Lite_3.1.1 (FTK Imager.exe)
XGCTUC-5561	FTK Imager.exe
Y78Z2B-5561	FTK Imager.exe
YCA984-5562	FTK Imager
Z4WK8A-5562	FTK Imager

TABLE 1

Question 18 - Operating System / Registry Analysis

WebCode-Test	Response
Z6A992-5561	FTK Imager

Question 18: What program did the responding/seizing examiner execute?

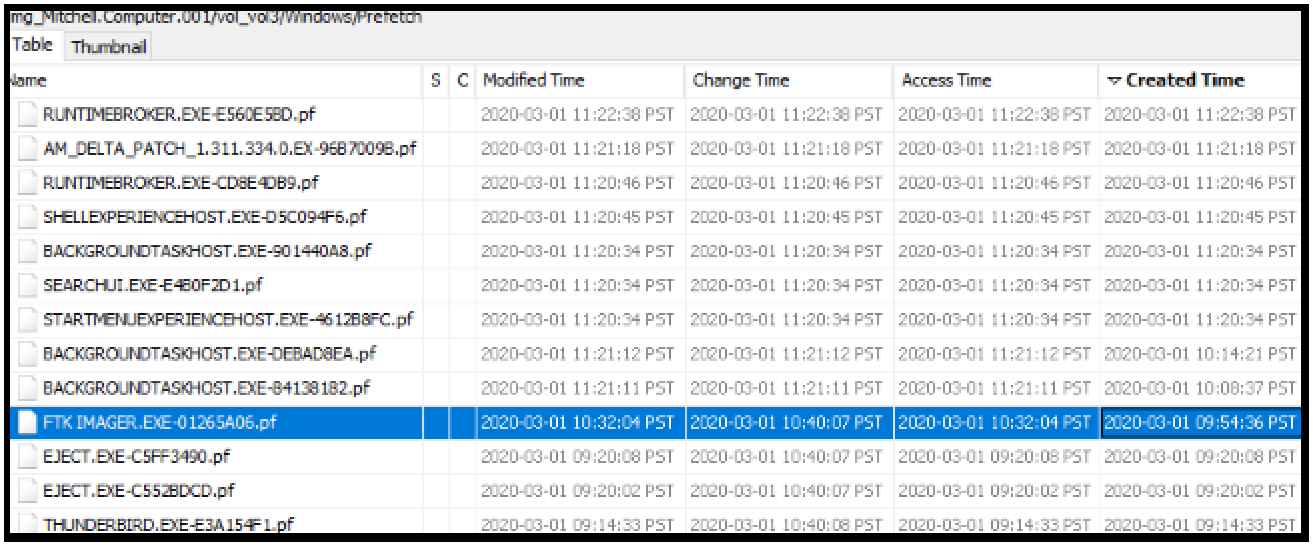
Consensus Result: FTK Imager

Expected Response Explanation:

Presumably, a responding/seizing examiner would be the last person to interact with the computer prior to and during the acquisition. It is common for an examiner to mount external media and execute forensic applications to preview or acquire data from a seized running computer prior to shutdown. A review of the files in C:\Windows\prefetch indicates that among the last programs executed prior to shutdown was FTKIMAGER.exe. Analysis of the prefetch file shows a last run time of what is seen in the second image.The NTUSER.DAT registry hive for the user at C:\users\james\NTUSER.DAT:Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist also contains a record of the program execution.

Expected Response Illustration:

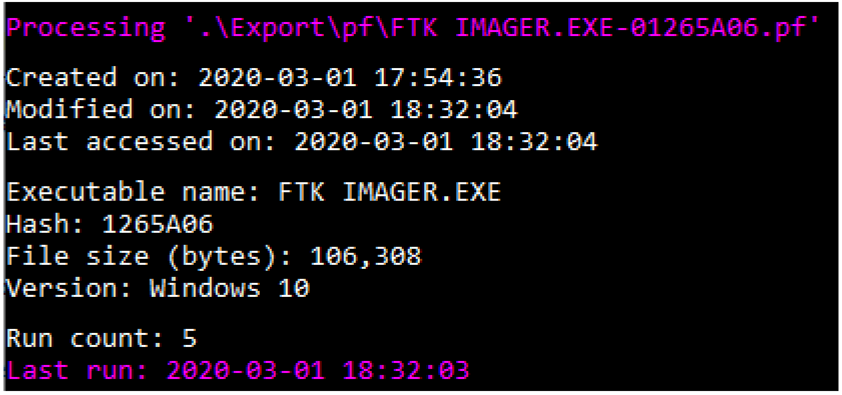
Prefetch:



mg_Mitchell.Computer.001/vol_vol3/Windows/Prefetch

Name	S	C	Modified Time	Change Time	Access Time	▿ Created Time
RUNTIMEBROKER.EXE-E560E58D.pf			2020-03-01 11:22:38 PST	2020-03-01 11:22:38 PST	2020-03-01 11:22:38 PST	2020-03-01 11:22:38 PST
AM_DELTA_PATCH_1.311.334.0.EX-96B70098.pf			2020-03-01 11:21:18 PST	2020-03-01 11:21:18 PST	2020-03-01 11:21:18 PST	2020-03-01 11:21:18 PST
RUNTIMEBROKER.EXE-CD8E4DB9.pf			2020-03-01 11:20:46 PST	2020-03-01 11:20:46 PST	2020-03-01 11:20:46 PST	2020-03-01 11:20:46 PST
SHELLEXPERIENCEHOST.EXE-D5C094F6.pf			2020-03-01 11:20:45 PST	2020-03-01 11:20:45 PST	2020-03-01 11:20:45 PST	2020-03-01 11:20:45 PST
BACKGROUNDTASKHOST.EXE-901440A8.pf			2020-03-01 11:20:34 PST	2020-03-01 11:20:34 PST	2020-03-01 11:20:34 PST	2020-03-01 11:20:34 PST
SEARCHUI.EXE-E4B0F2D1.pf			2020-03-01 11:20:34 PST	2020-03-01 11:20:34 PST	2020-03-01 11:20:34 PST	2020-03-01 11:20:34 PST
STARTMENUEXPERIENCEHOST.EXE-4612B8FC.pf			2020-03-01 11:20:34 PST	2020-03-01 11:20:34 PST	2020-03-01 11:20:34 PST	2020-03-01 11:20:34 PST
BACKGROUNDTASKHOST.EXE-DEBAD8EA.pf			2020-03-01 11:21:12 PST	2020-03-01 11:21:12 PST	2020-03-01 11:21:12 PST	2020-03-01 10:14:21 PST
BACKGROUNDTASKHOST.EXE-84138182.pf			2020-03-01 11:21:11 PST	2020-03-01 11:21:11 PST	2020-03-01 11:21:11 PST	2020-03-01 10:08:37 PST
FTK IMAGER.EXE-01265A06.pf			2020-03-01 10:32:04 PST	2020-03-01 10:40:07 PST	2020-03-01 10:32:04 PST	2020-03-01 09:54:36 PST
EJECT.EXE-C5FF3490.pf			2020-03-01 09:20:08 PST	2020-03-01 10:40:07 PST	2020-03-01 09:20:08 PST	2020-03-01 09:20:08 PST
EJECT.EXE-C552BDCD.pf			2020-03-01 09:20:02 PST	2020-03-01 10:40:07 PST	2020-03-01 09:20:02 PST	2020-03-01 09:20:02 PST
THUNDERBIRD.EXE-E3A154F1.pf			2020-03-01 09:14:33 PST	2020-03-01 10:40:08 PST	2020-03-01 09:14:33 PST	2020-03-01 09:14:33 PST

PECmd parsed FTK IMAGER.EXE-01265A06.pf prefetch file:



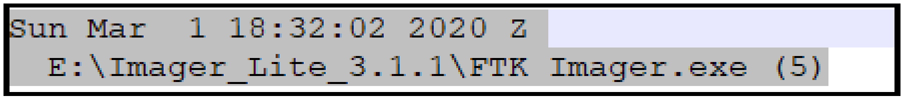
```
Processing '.\Export\pf\FTK IMAGER.EXE-01265A06.pf'

Created on: 2020-03-01 17:54:36
Modified on: 2020-03-01 18:32:04
Last accessed on: 2020-03-01 18:32:04

Executable name: FTK IMAGER.EXE
Hash: 1265A06
File size (bytes): 106,308
Version: Windows 10

Run count: 5
Last run: 2020-03-01 18:32:03
```

NTUSER.DAT registry hive:



```
Sun Mar  1 18:32:02 2020 Z
  E:\Imager_Lite_3.1.1\FTK Imager.exe (5)
```

TABLE 1

Question 19 - Event Log Analysis / Filesystem Analysis

Question 19: From what URL was the file with SHA1 3de75af054fed96e39568bad6edfdbc452d2cda4 downloaded?

Manufacturer's Expected Response: https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download

WebCode-Test	Response
2ZQE6A-5561	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
4XFB84-5561	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
64W7NX-5562	File Not Found / Hash Does not exist in case
6U9F26-5561	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
6ZF77W-5562	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
7K2ZUX-5562	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
7M9E24-5561	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
8Q3VR3-5562	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
9ENXLY-5561	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
ABKKEY-5561	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
AQCK6Y-5561	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
BJTE9R-5562	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
C8D7KQ-5561	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
CCTE9P-5562	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
CKXLNP-5561	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
CPXWKP-5562	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download

DGFL7P-5562	New100back.jpg located in \Users\james\Downloads\New100back.jpg\Zone.Identifier.
	The alternate data stream found in FTK imager for the file shows a zone identifier of 3 which indicates it was downloaded from https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download using Google Chrome found in the internet history \Users\james\AppData\Local\Google\Chrome\User Data\Default\History
	[ZoneTransfer]
	ZoneId=3
	ReferrerUrl=https://en.wikipedia.org/
	HostUrl=https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download

DX4YHV-5561	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
EQHHC7-5562	https://en.wikipedia.org/wiki/Federal_Reserve_Note#/media/File:New100back.jpg
ETQDAP-5562	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 19 - Event Log Analysis / Filesystem Analysis

WebCode-Test	Response
HG3KCP-5561	Https://upload.wikimedia.org/wikepedia/cpmmpms/b/b7/New100buck.jpg?download
HHBXTQ-5562	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
J6MAYJ-5561	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
KH3VVH-5562	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
MTJYGM-5562	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
NF4QTK-5562	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
NZEF7H-5561	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
P6M4JK-5562	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
P8TN8K-5561	https://en.wikipedia.org/ HostUrl=https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
P92YZG-5562	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
PZ7VVK-5561	https://upload.wikimedic.org/wikipedia/commons/b/b7/new100black.jpg?
Q7RBYH-5562	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
QAQLVH-5561	Https://upload.Wikimedia.org/Wikimedia/commons/b/b7/New100back.jpg?download
QFHW6F-5561	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
QZQWEG-5561	Url=https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
R7BE8H-5562	Reviewed all downloads made in browsers, in addition to all files present in said evidence, none are found with the SHA1 described.
TANE4A-5561	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
TEV68F-5561	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
TXBE8F-5561	https://en.wikipedia.org/
U3ZBAC-5562	https://en.wikipedia.org/wiki/Federal_Reserve_Note#/media/File:New100back.jpg
VBBWX7-5562	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
VZACVE-5562	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
W2ZUC7-5562	The answer is h t t p s :/ / upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download Using FTKImager I am able to export hash listing of all files on the partition and this hash matched with the zone identifier at 'Users\james\Downloads\New100back.jpg\Zone.Identifier' and then searching for the New100back.jpg file name in Axiom we are able to identify that the file got downloaded from the above mentioned URL based on web history artifact.
WVD6QB-5561	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download

TABLE 1

Question 19 - Event Log Analysis / Filesystem Analysis

WebCode-Test	Response
XGCTUC-5561	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
Y78Z2B-5561	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
YCA984-5562	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
Z4WK8A-5562	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
Z6A992-5561	https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download

Question 19: From what URL was the file with SHA1 3de75af054fed96e39568bad6edfdbc452d2cda4 downloaded?

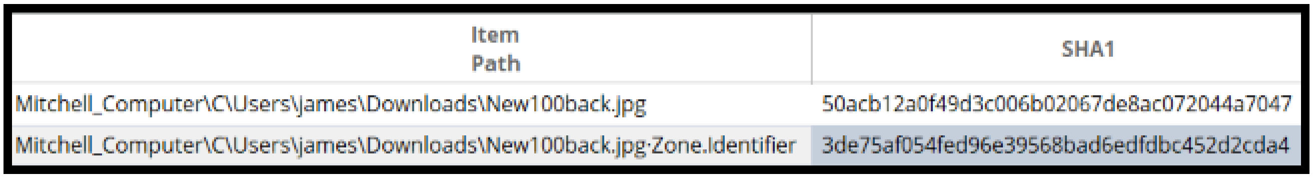
Consensus Result: https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download and all formatting styles which represent the same information. Slight variations of the expected result were disregarded and not considered outliers, if they were easily identified as spelling errors.

Expected Response Explanation:

Finding this file requires a tool that is aware of NTFS Alternate Data Streams (ADS) and will calculate SHA1 for those file objects. Calculating SHA1 hashes for all files, sorting by hash value, and looking for the above hash will find the ADS for C:\Users\james\Downloads\New100back.jpg·Zone.Identifier. The contents of this file show the URL hosting this file, from where it was downloaded.

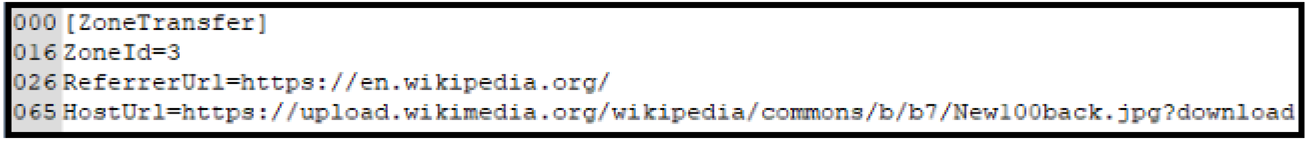
Expected Response Illustration:

EnCase file listing:



Item Path	SHA1
Mitchell_Computer\C\Users\james\Downloads\New100back.jpg	50acb12a0f49d3c006b02067de8ac072044a7047
Mitchell_Computer\C\Users\james\Downloads\New100back.jpg·Zone.Identifier	3de75af054fed96e39568bad6edfdbc452d2cda4

Contents of New100back.jpg·Zone.Identifier:



```
000 [ZoneTransfer]
016 ZoneId=3
026 ReferrerUrl=https://en.wikipedia.org/
065 HostUrl=https://upload.wikimedia.org/wikipedia/commons/b/b7/New100back.jpg?download
```

TABLE 1

Question 20 - Event Log Analysis / Filesystem Analysis

Question 20: 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: 03/01/2020 06:45:09 PM

WebCode-Test	Response
2ZQE6A-5561	03/01/2020 06:45:09 PM
4XFB84-5561	03/01/2020 02:45:09 PM
64W7NX-5562	03/01/2020 18:45:09 PM
6U9F26-5561	2020-03-01 18:45:09 PM
6ZF77W-5562	03/01/2020 06:45:09 PM
7K2ZUX-5562	03/01/2020 07:45:09 PM
7M9E24-5561	03/01/2020 06:45:09 PM
8Q3VR3-5562	03/01/2020 06:45:09 PM
9ENXLY-5561	3/1/2020 7:24:32 PM (19:24:32) UTC
ABKKEY-5561	03/01/2020 09:38:49 PM
AQCK6Y-5561	03/01/2020 07:45:09 PM
BJTE9R-5562	03/01/2020 06:45:09 PM
C8D7KQ-5561	[Participant did not return results for this question.]
CCTE9P-5562	3/1/2020 6:45:09 PM UTC
CKXLNP-5561	03/01/2020 06:45:09 PM
CPXWKP-5562	03/01/2020 06:45:09 PM
DGFL7P-5562	the last login for the account james was 3/1/2020 7:24:31 PM UTC according to the last modified time of the account's NTUSER.DAT
DX4YHV-5561	03/01/2020 06:45:09 PM
EQHHC7-5562	01/03/2020 18:45:09
ETQDAP-5562	03/01/2020 06:45:09 PM
HG3KCP-5561	03/01/2020 06:47:46 PM
HHBXTQ-5562	Last screen unlock (type 7) was at 03/01/20 06:45:09 PM. Last interactive logon (type 2) was at 02/10/20 01:39:13 AM
J6MAYJ-5561	02/10/2020 1:33:46 AM

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 20 - Event Log Analysis / Filesystem Analysis

WebCode-Test	Response
KH3VVH-5562	03/01/2020 06:45:09 PM
MTJYGM-5562	03/01/2020 07:45:09 PM
NF4QTK-5562	3/1/2020 06:45:09 PM
NZEF7H-5561	03/01/2020 6:45:09 PM
P6M4JK-5562	03/01/2020 06:45:09 PM
P8TN8K-5561	03/01/2020 06:45:09 PM
P92YZG-5562	03/02/2020 5:45:09 AM
PZ7VVK-5561	03/01/2020 06:47:46 PM
Q7RBYH-5562	03/01/2020 18:45:09 PM
QAQLVH-5561	03/01/2020 09:38:49PM
QFHW6F-5561	03/01/2020 18:45:09 PM
QZQWEG-5561	03/01/2020 06:45:09 PM (UTC)
R7BE8H-5562	james.mitchell.40@outlook.com; 03/01/2020 18:45:09
TANE4A-5561	03/01/2020 01:51:16 AM
TEV68F-5561	03/01/2020 06:45:09 PM
TXBE8F-5561	03/01/2020 06:45:09 PM UTC +00:00
U3ZBAC-5562	02/10/20 01:33:46
VBBWX7-5562	3/1/2020 7:24:18 PM
VZACVE-5562	03/01/2020 06:45:09 PM
W2ZUC7-5562	The answer is 3/1/2020 7:24:18 PM UTC. Based on the registry 'SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI' last update time can be considered as last login which is 3/1/2020 7:24:18 PM UTC
WVD6QB-5561	03/01/2020 06:45:09 PM
XGCTUC-5561	03/01/2020 06:45:09 PM
Y78Z2B-5561	03/01/2020 06:45:09 PM
YCA984-5562	03/01/2020 06:45:09 PM
Z4WK8A-5562	03/01/2020 06:45:09 PM

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 20 - Event Log Analysis / Filesystem Analysis

WebCode-Test	Response
Z6A992-5561	03/01/2020 06:45:09 PM (Event ID: 4624)

Question 20: 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

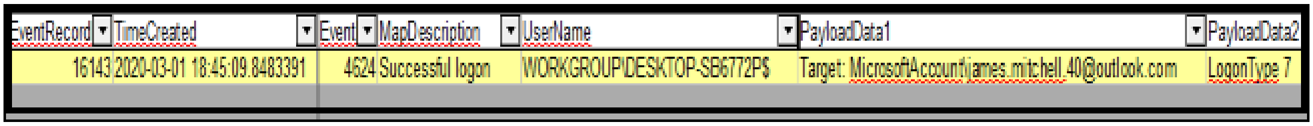
Consensus Result: 03/01/2020 06:45:09 PM and all formatting styles which represent the same information. In addition, the same date with the times of 02:45:09 PM and 07:45:09 PM which represents the different time zones were also accepted.

Expected Response Explanation:

In this installation of Windows 10, the default login authentication mechanism was set as a PIN code instead of a password. PIN logins don't get logged to the SAM hive as password logins do in other versions and editions of Windows. The Windows security event log at C:\Windows\System32\winevt\Logs\Security.evtx contains records for those logins. Filtering this log for EventID 4624 ("An account was successfully logged on") , and for payload data containing "james", the latest record is a Type 7 Logon (Screen unlock) at 03/01/2020 18:45:09 PM UTC+0.

Expected Response Illustration:

Windows Security event log:



EventRecord	TimeCreated	Event	MapDescription	UserName	PayloadData1	PayloadData2
16143	2020-03-01 18:45:09.8483391	4624	Successful logon	WORKGROUP\DESKTOP-SB6772P$	Target: MicrosoftAccount\james.mitchell.40@outlook.com	LogonType 7

TABLE 1

Question 21 - Event Log Analysis / Filesystem Analysis

Question 21: What is the volume serial number for the file system on the system partition?

Manufacturer's Expected Response: 2C2E-5168, 68512E2C or 402C2E602C2E5168

WebCode-Test	Response
2ZQE6A-5561	68512E2C
4XFB84-5561	2C2E-5168
64W7NX-5562	402C2E602C2E5168
6U9F26-5561	402C2E602C2E5168
6ZF77W-5562	2C2E-5168
7K2ZUX-5562	2C2E-5168
7M9E24-5561	2C2E-5168
8Q3VR3-5562	2C2E-5168
9ENXLY-5561	2C2E-5168
ABKKEY-5561	2C2E-5168
AQCK6Y-5561	0x68512E2C
BJTE9R-5562	2C2E-5168
C8D7KQ-5561	2C2E-5168
CCTE9P-5562	Volume Serial Number = 8C2D-CE1B; Full Volume Serial Number = A28C2DFE8C2DCE1B
CKXLNP-5561	2C2E-5168
CPXWKP-5562	8C2D-CE1B
DGFL7P-5562	8C2D-CE1B
DX4YHV-5561	2C2E-5168
EQHHC7-5562	Volume Serial Number: 2C2E-5168 --- Full Volume Serial Number: 402C2E602C2E5168
ETQDAP-5562	Serial No.: 68512E2C (hex); Serial No.: 2C2E5168 (hex, rev); Serial No.: 741233000 (dec, rev)
HG3KCP-5561	2C2E-5168
HHBXTQ-5562	2C2E-5168
J6MAYJ-5561	8C2D-CE1B
KH3VVH-5562	2C2E-5168

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 21 - Event Log Analysis / Filesystem Analysis

WebCode-Test	Response
MTJYGM-5562	0x68512E2C
NF4QTK-5562	2C2E-5168
NZEF7H-5561	2C2E-5168
P6M4JK-5562	2C2E-5168
P8TN8K-5561	2C2E-5168
P92YZG-5562	402C2E602C2E5168
PZ7VVK-5561	2C2E-5168
Q7RBYH-5562	2C2E-5168
QAQLVH-5561	2C2E-5168
QFHW6F-5561	2C2E5168
QZQWEG-5561	2C2E-5168
R7BE8H-5562	Serial Number: 2C2E-5168; Full Serial Number: 402C2E602C2E5168
TANE4A-5561	2C2E-5168
TEV68F-5561	2C2E-5168
TXBE8F-5561	2C2E-5168
U3ZBAC-5562	8C2D-CE1B
VBBWX7-5562	2C2E-5168
VZACVE-5562	2C2E-5168
W2ZUC7-5562	The answer is 2C2E-5168. Based on the 'File System Information' artifact in Axiom forensics tool I see that this data as 2C2E-5168
WVD6QB-5561	2C2E-5168
XGCTUC-5561	2C2E-5168
Y78Z2B-5561	402C2E602C2E5168
YCA984-5562	2C2E5168
Z4WK8A-5562	2C2E-5168
Z6A992-5561	2C2E-5168

Question 21: What is the volume serial number for the file system on the system partition?

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 21 - Event Log Analysis / Filesystem Analysis

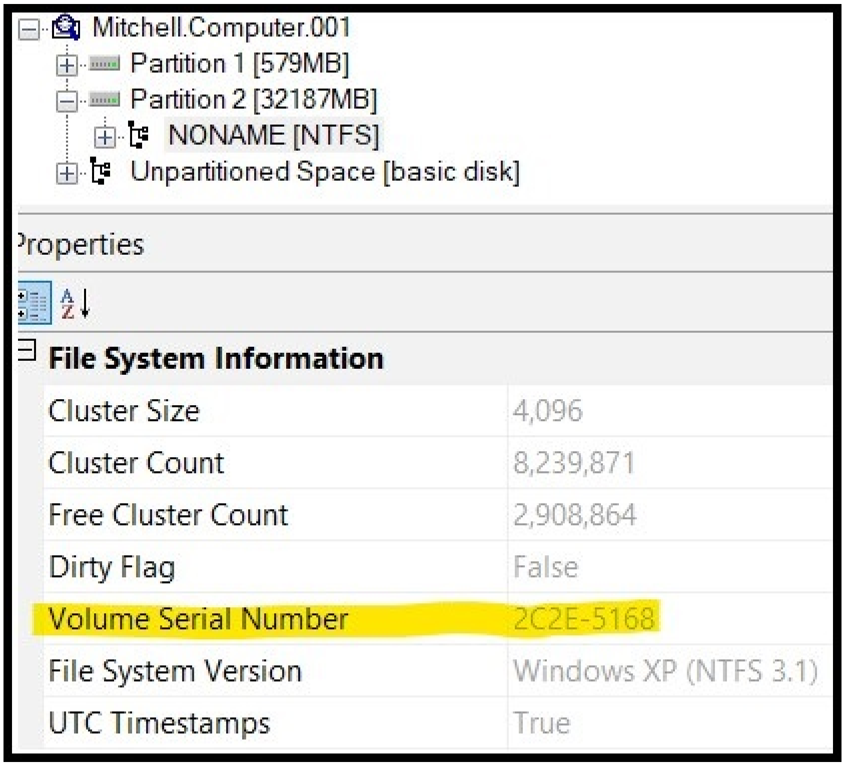
Consensus Result: 2C2E-5168, 68512E2C (hex) and the full volume serial number of 402C2E602C2E5168 was also accepted.

Expected Response Explanation:

The volume serial number is parsed and reported by most forensic tools.

Expected Response Illustration:

FTK Imager view of device information:



Mitchell.Computer.001
Partition 1 [579MB]
Partition 2 [32187MB]
NONAME [NTFS]
Unpartitioned Space [basic disk]

Properties

File System Information

Cluster Size	4,096
Cluster Count	8,239,871
Free Cluster Count	2,908,864
Dirty Flag	False
Volume Serial Number	2C2E-5168
File System Version	Windows XP (NTFS 3.1)
UTC Timestamps	True

TABLE 1

Question 22 - Event Log Analysis / Filesystem Analysis

Question 22: What is the original (pre-deletion) name of the file in the user's Recycle Bin?

Manufacturer's Expected Response: 20_front.xcf

WebCode-Test	Response
2ZQE6A-5561	20_front.xcf
4XFB84-5561	20_front3.xcf
64W7NX-5562	20_front.xcf
6U9F26-5561	20_front.xcf 20_front3.xcf
6ZF77W-5562	20_front.xcf; 20_front3.xcf
7K2ZUX-5562	20_front.xcf
7M9E24-5561	20_front.xcf
8Q3VR3-5562	20_front.xcf
9ENXLY-5561	20_front.xcf
ABKKEY-5561	20_front.xcf
AQCK6Y-5561	20_front.xcf
BJTE9R-5562	20_front.xcf
C8D7KQ-5561	20_front.xcf
CCTE9P-5562	20_front.xcf
CKXLNP-5561	20_front.xcf
CPXWKP-5562	20_front.xcf
DGFL7P-5562	20_front.xcf
DX4YHV-5561	20_front.xcf
EQHHC7-5562	20_front.xcf
ETQDAP-5562	20_front.xcf
HG3KCP-5561	20_Front.xcf
HHBXTQ-5562	20_front.xcf; 20_front3.xcf
J6MAYJ-5561	20_front.xcf
KH3VVH-5562	20_front.xcf

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 22 - Event Log Analysis / Filesystem Analysis

WebCode-Test	Response
MTJYGM-5562	20_front.xcf
NF4QTK-5562	20_front.xcf
NZEF7H-5561	20_front.xcf
P6M4JK-5562	20_front.xcf & 20_front3.xcf
P8TN8K-5561	20_front.xcf and 20_front3.xcf
P92YZG-5562	20_front.xcf
PZ7VVK-5561	20_front.xcf
Q7RBYH-5562	20_front.xcf
QAQLVH-5561	20_front.xcf
QFHW6F-5561	20_front.xcf
QZQWEG-5561	20_front.xcf
R7BE8H-5562	20_front3.xcf
TANE4A-5561	20_front.xcf
TEV68F-5561	$RUKNIK0.xcf -------- 20_front.xcf $RV82MQE.xcf -------- 20_front3.xcf both files were found in the Recycle Bin
TXBE8F-5561	20_front.xcf
U3ZBAC-5562	20_front3.xcf
VBBWX7-5562	20_front.xcf
VZACVE-5562	$RUKNIK0.xcf -------- 20_front.xcf $RV82MQE.xcf -------- 20_front3.xcf both files were found in Recycle Bin
W2ZUC7-5562	The answer is 20_front.xcf. I have parsed the raw image in Autopsy and under the Recycle Bin artifacts, i see original pre-deletion name of the file as 20_front.xcf
WVD6QB-5561	20_front.xcf
XGCTUC-5561	20_front.xcf
Y78Z2B-5561	20_front.xcf
YCA984-5562	20_front.xcf
Z4WK8A-5562	20_front.xcf
Z6A992-5561	1. 20_front.xcf 2. 20_front3.xcf

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 22 - Event Log Analysis / Filesystem Analysis

Question 22: What is the original (pre-deletion) name of the file in the user's Recycle Bin?

Consensus Result: 20_front.xcf

Expected Response Explanation:

Every user on a system has a folder in C:\$Recycle.Bin named for their Security Identifier, or SID. In this case, the user james' SID is S-1-5-21-4282868925-760505910-2700774193-1001. Within that folder are 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, $IUKNIK0.xcf, and $RUKNIK0.xcf, respectively. $IUKNIK0.xcf contains the files original name, 20_front.xcf.

Other Responses:

Eleven participants reported "20_front3.xcf", eight of these also reported the expected response. There are two $I files in the recycle bin, only one $IUKNIK0.xcf (containing the metadata for 20_front.xcf), has a corresponding $R file, $RUKNIK0.xcf with content. The other file present in the Recycle Bin, I$V82MQE.xcf, associated with "20_front3.xcf" does not have a corresponding $R file which indicates that although this file was once in the Recycle Bin, it is no longer present. When a file is restored from the Recycle Bin the $R file disappears but the $I file remains.

TABLE 1

Question 23 - Event Log Analysis / Filesystem Analysis

Question 23: What was the path to the location of the file (file reference in question #22) prior to being sent to the Recycle Bin?

Manufacturer's Expected Response: C:\Users\james\Documents\

WebCode-Test	Response
2ZQE6A-5561	C:\Users\james\Documents\
4XFB84-5561	c:\users\james\documents\20_front.xcf
64W7NX-5562	C:\Users\james\Documents\20_front.xcf
6U9F26-5561	C:\Users\james\Documents\
6ZF77W-5562	C:\Users\james\Documents
7K2ZUX-5562	\Users\james\Documents\
7M9E24-5561	C:\Users\james\Documents\20_front.xcf
8Q3VR3-5562	C:\Users\james\Documents\
9ENXLY-5561	C:\Users\james\Documents\20_front.xcf
ABKKEY-5561	C:\Users\james\Documents\20_front.xcf
AQCK6Y-5561	C:\Users\james\Documents\
BJTE9R-5562	C:\Users\james\Documents\20_front.xcf
C8D7KQ-5561	C:\Users\james\Documents\20_front.xcf
CCTE9P-5562	C:\Users\james\Documents\20_front.xcf
CKXLNP-5561	C:\Users\james\Documents\
CPXWKP-5562	C:\Users\james\Documents\20_front.xcf
DGFL7P-5562	C:\Users\james\Documents\20_front.xcf
DX4YHV-5561	C:\Users\james\Documents\20_front.xcf
EQHHC7-5562	C:\Users\james\Documents\
ETQDAP-5562	C:\Users\james\Documents\20_front.xcf
HG3KCP-5561	\users\james\documents\20_front.xcf
HHBXTQ-5562	C:\Users\james\Documents\20_front.xcf C:\Users\james\Documents\20_front3.xcf
J6MAYJ-5561	C:\Users\james\Documents\20_front.xcf

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 23 - Event Log Analysis / Filesystem Analysis

WebCode-Test	Response
KH3VVH-5562	C:\Users\james\Documents
MTJYGM-5562	C:\Users\james\Documents\
NF4QTK-5562	C:\Users\james\Documents\
NZEF7H-5561	C:\Users\james\Documents\20_front.xcf
P6M4JK-5562	C:\Users\james\Documents
P8TN8K-5561	C:\Users\james\Documents\20_front.xcf and C:\Users\james\Documents\20_front3.xcf
P92YZG-5562	C:\Users\james\Documents\
PZ7VVK-5561	C:\users\james\documents\20_front.xcf
Q7RBYH-5562	C:\Users\james\Documents\20_front.xcf
QAQLVH-5561	C:\Users\james\Documents
QFHW6F-5561	C:\Users\james\Documents
QZQWEG-5561	C:\Users\james\Documents\
R7BE8H-5562	C:\Users\james\Documents\20_front3.xcf
TANE4A-5561	C:\Users\james\Documents\
TEV68F-5561	C:\Users\james\Documents\20_front.xcf C:\Users\james\Documents\20_front3.xcf
TXBE8F-5561	C:\Users\james\Documents\20_front.xcf
U3ZBAC-5562	C:\Users\james\Documents\20_front3.xcf
VBBWX7-5562	C:\Users\james\Documents\20_front.xcf
VZACVE-5562	C:\Users\james\Documents\20_front.xcf C:\Users\james\Documents\20_front3.xcf
W2ZUC7-5562	The answer is C:\Users\james\Documents\. From the parsed raw image data in Autopsy under Recycle Bin artifacts, i see that the path to the location of the file as C:\Users\james\Documents\
WVD6QB-5561	C:\Users\james\Documents\20_front.xcf
XGCTUC-5561	C:\Users\james\Documents\20_front.xcf
Y78Z2B-5561	\Users\james\Documents\
YCA984-5562	C:\Users\james\Documents\20_front.xcf
Z4WK8A-5562	C:\Users\james\Documents\20_front.xcf
Z6A992-5561	1. C:\Users\james\Documents\20_front.xcf 2. C:\Users\james\Documents\20_front3.xcf

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 23 - Event Log Analysis / Filesystem Analysis

Question 23: What was the path to the location of the file (file reference in question #22) prior to being sent to the Recycle Bin?

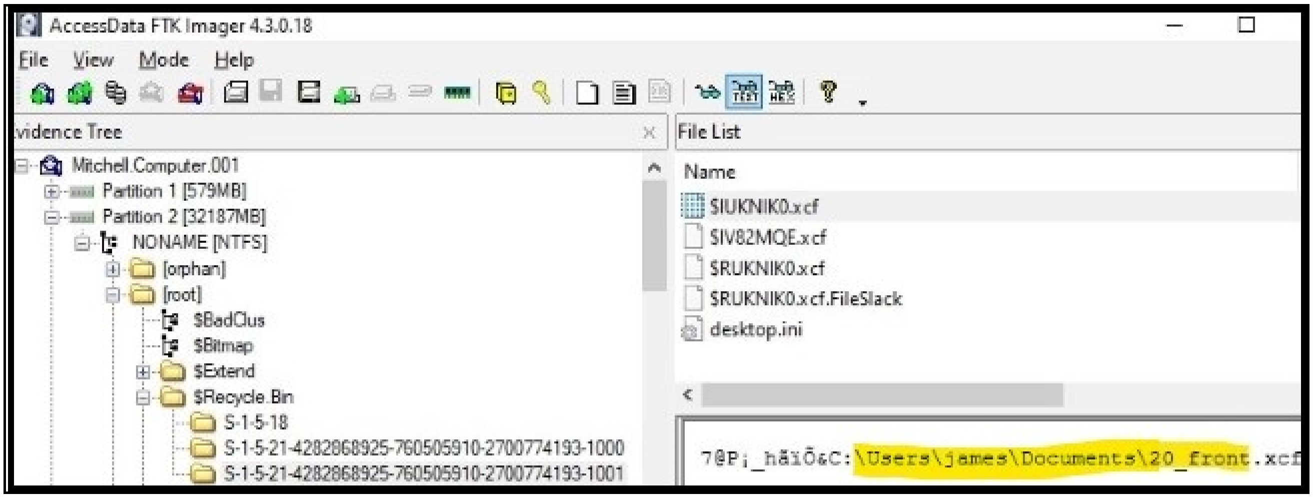
Consensus Result: C:\Users\james\Documents\. This path regardless of the file name was accepted.

Expected Response Explanation:

The file's original path can be found within the user's SID folder in the $IUKNIK0.xcf file. See question 22.

Expected Response Illustration:

Recycle Bin:



```
Mitchell.Computer.001
  Partition 1 [579MB]
  Partition 2 [32187MB]
    NONAME [NTFS]
      [orphan]
      [root]
        $BadClus
        $Bitmap
        $Extend
        $Recycle.Bin
          S-1-5-18
          S-1-5-21-4282868925-760505910-2700774193-1000
          S-1-5-21-4282868925-760505910-2700774193-1001
```

```
$IUKNIK0.xcf
$IV82MQE.xcf
$RUKNIK0.xcf
$RUKNIK0.xcf.FileSlack
desktop.ini
```

```
7@P¡_hãïÕ&C:\Users\james\Documents\20_front.xcf
```

TABLE 1

Question 24 - Event Log Analysis / Filesystem Analysis

Question 24: On what date and time was the file (file referenced in question #22) deleted? Provide your response in UTC + 00:00 using the following format: MM/DD/YYYY HH:MM AM/PM

Manufacturer's Expected Response: 03/01/2020 04:06:46 PM (UTC)

WebCode-Test	Response
2ZQE6A-5561	03/01/2020 04:06 PM
4XFB84-5561	03/01/2020 04:06:46 PM
64W7NX-5562	03/01/2020 16:06:46
6U9F26-5561	20_front.xcf 3/1/2020 4:06:46 PM 20_front3.xcf 3/1/2020 4:02:26 PM
6ZF77W-5562	File 20_front.xcf 03/01/2020 04:06:46 PM File 20_front3.xcf 03/01/2020 04:02:26 PM
7K2ZUX-5562	03/01/2020 04:06:46 PM
7M9E24-5561	03/01/2020 04:06:46 PM
8Q3VR3-5562	03/01/2020 04:06 PM
9ENXLY-5561	3/1/2020 4:06:46 PM
ABKKEY-5561	03/01/2020 04:06:46 PM
AQCK6Y-5561	03/01/2020 04:06:46 PM
BJTE9R-5562	03/01/2020 04:06 PM (UTC + 00:00)
C8D7KQ-5561	03/01/2020 04:06:46 PM
CCTE9P-5562	3/1/2020 4:06:46 PM UTC
CKXLNP-5561	03/01/2020 04:06 PM
CPXWKP-5562	03/01/2020 04:06:46 PM
DGFL7P-5562	3/1/2020 4:06:46 PM UTC
DX4YHV-5561	03/01/2020 04:06:46 PM
EQHHC7-5562	01/03/2020 16:06:46
ETQDAP-5562	03/01/20 04:06:46 PM
HG3KCP-5561	03/01/2020 04:06:46 PM
HHBXTQ-5562	20_front.xcf = 03/01/20 04:06:46 PM 20_front3.xcf = 03/01/20 04:02:26 PM
J6MAYJ-5561	03/01/2020 4:06:46 PM

TABLE 1

Question 24 - Event Log Analysis / Filesystem Analysis

WebCode-Test	Response
KH3VVH-5562	03/01/2020 04:06:46 PM
MTJYGM-5562	03/01/2020 04:06:46 PM
NF4QTK-5562	03/01/2020 04:06 PM
NZEF7H-5561	03/01/2020 4:06:46 PM
P6M4JK-5562	03/01/2020 4:06:46 PM & 03/01/2020 4:02:26 PM
P8TN8K-5561	03/01/2020 04:06 PM
P92YZG-5562	03/01/2020 4:06:46 PM
PZ7VVK-5561	03/01/2020 4:06:46 PM
Q7RBYH-5562	03/01/2020 16:06 PM
QAQLVH-5561	03/01/2020 04:06:46PM
QFHW6F-5561	03/01/2020 16:02:26 AM
QZQWEG-5561	03/01/2020 04:06:46 PM (UTC)
R7BE8H-5562	03/01/2020 16:02:26
TANE4A-5561	03/01/2020 04:06 PM
TEV68F-5561	20_front.xcf ------------- 3/1/2020 4:06:46 PM 20_front3.xcf -------------3/1/2020 4:02:26 PM
TXBE8F-5561	03-01-2020 04:06:46 pm
U3ZBAC-5562	03/01/20 16:02:26
VBBWX7-5562	3/1/2020 4:06:46 PM
VZACVE-5562	20_front.xcf ------------- 3/1/2020 4:06:46 PM 20_front3.xcf -------------3/1/2020 4:02:26 PM
W2ZUC7-5562	The answer is 03/01/2020 16:06:46 PM UTC. From the parsed raw image data in Autopsy under Recycle Bin artifacts, i see that the date and time was the file deleted was 03/01/2020 16:06:46 PM UTC
WVD6QB-5561	03/01/2020 04:06:46 PM
XGCTUC-5561	03/01/2020 04:06:46 PM
Y78Z2B-5561	03/01/2020 04:06:46 PM
YCA984-5562	03.01.2020 04:06:46 PM
Z4WK8A-5562	03/01/2020 04:06 PM
Z6A992-5561	1. 20_front.xcf deleted on 03/01/2020 04:06:46 PM 1. 20_front3.xcf deleted on 03/01/2020 04:02:26 PM

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 24 - Event Log Analysis / Filesystem Analysis

Question 24: On what date and time was the file (file referenced in question #22) deleted? Provide your response in UTC + 00:00 using the following format: MM/DD/YYYY HH:MM AM/PM

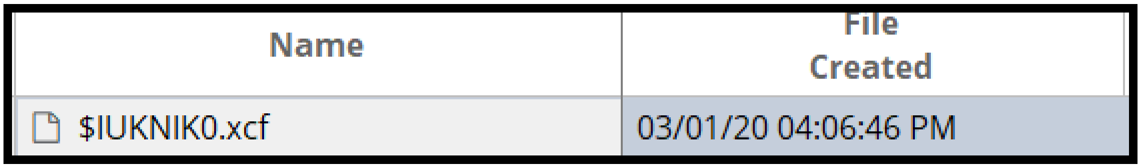
Consensus Result: 03/01/2020 04:06:46 PM (UTC)

Expected Response Explanation:

The creation date and time for the $I file, $IUKNIK0.xcf, indicates the time the file was sent to the recycler (deleted).

Expected Response Illustration:

EnCase view of file metadata:



Name	File Created
$IUKNIK0.xcf	03/01/20 04:06:46 PM

Other Responses:

Ten participants reported the date and time associated with the file "20_front3.xcf" which is the response they reported in question# 22. Seven of these also reported the expected date and time associated with "20_front.xcf", the expected response for question# 22.

TABLE 1

Question 25 - Operating System / File Analysis

Question 25: What is the default application for opening this type of file (file referenced in question #22)?

Manufacturer's Expected Response: C:\Program Files\GIMP 2\bin\gimp-2.10.exe, GIMP 2, or GIMP

WebCode-Test	Response
2ZQE6A-5561	GIMP 2.10.14
4XFB84-5561	Gimp 2.10.14
64W7NX-5562	GIMP
6U9F26-5561	Gimp 2
6ZF77W-5562	gimp-2.10
7K2ZUX-5562	GIMP
7M9E24-5561	Gimp
8Q3VR3-5562	GIMP 2.10.14
9ENXLY-5561	Gimp.exe
ABKKEY-5561	GIMP 2
AQCK6Y-5561	GIMP2
BJTE9R-5562	GIMP
C8D7KQ-5561	GIMP 2.10.14
CCTE9P-5562	GNU Image Manipulation Program (GIMP) Filename : gimp-2.10.exe
CKXLNP-5561	GIMP
CPXWKP-5562	Gimp
DGFL7P-5562	GIMP 2.10.14 according to the registry SOFTWARE\Classes\GIMP2.xcf
DX4YHV-5561	GIMP
EQHHC7-5562	gimp-2.10.exe
ETQDAP-5562	Quick Access
HG3KCP-5561	Gimp 2.10.exe
HHBXTQ-5562	GIMP
J6MAYJ-5561	GIMP 2.10.14

TABLE 1

Question 25 - Operating System / File Analysis

WebCode-Test	Response
KH3VVH-5562	gimp 2.10
MTJYGM-5562	GIMP2
NF4QTK-5562	Gimp
NZEF7H-5561	C:\Program Files\GIMP 2\bin\gimp-2.10.exe
P6M4JK-5562	gimp-2.10
P8TN8K-5561	Gimp
P92YZG-5562	GIMP - GNU Image Manipulation Program
PZ7VVK-5561	gimp-2.10.exe
Q7RBYH-5562	Not set in Registry; xcf file opened using GIMP
QAQLVH-5561	GIMP 2
QFHW6F-5561	Gimp 2.10
QZQWEG-5561	GIMP 2.10.14
R7BE8H-5562	GIMP
TANE4A-5561	GIMP (GNU Image Manipulation Program)
TEV68F-5561	gimp-2.10.exe
TXBE8F-5561	GIMP
U3ZBAC-5562	Quick Access
VBBWX7-5562	GIMP-2.10.EXE
VZACVE-5562	gimp-2.10.exe
W2ZUC7-5562	The answer is gimp-2.10.exe. I have processed the image using Axiom forensics tool and with the help of 'File Associations' artifact, i see that to open .xcf file, the default application is gimp-2.10.exe
WVD6QB-5561	GIMP (version 2.10.14)
XGCTUC-5561	GIMP
Y78Z2B-5561	GIMP
YCA984-5562	GIMP
Z4WK8A-5562	GIMP 2.10.14
Z6A992-5561	Gimp

TABLE 1

Question 25 - Operating System / File Analysis

Question 25: What is the default application for opening this type of file (file referenced in question #22)?

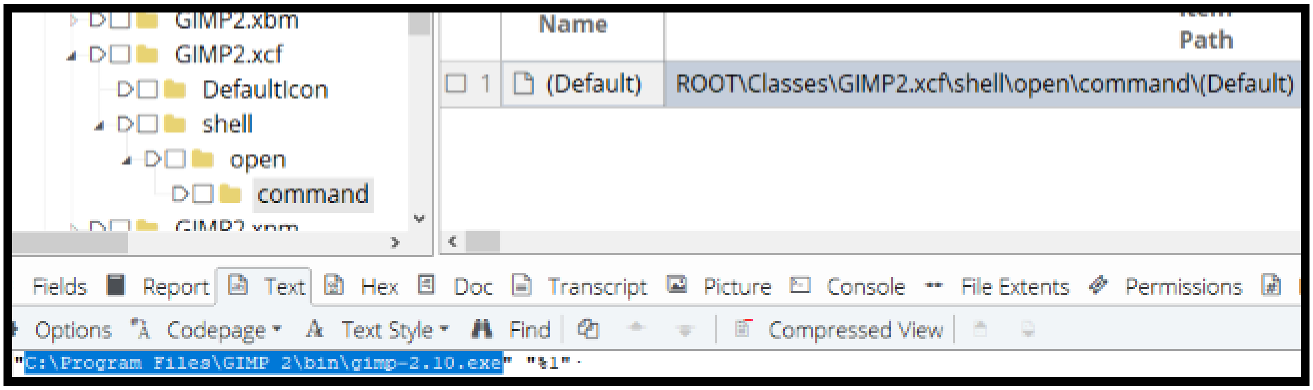
<u>Consensus Result:</u> C:\Program Files\GIMP 2\bin\gimp-2.10.exe, GIMP 2, or GIMP

<u>Expected Response Explanation</u>:

Windows stores settings for default applications (by file extension) in the SOFTWARE registry hive: C:\Windows\System32\Config\SOFTWARE: Classes\.xcf contains a pointer to ROOT(C:\Windows\System32\Config\SOFTWARE:)\Classes\.xcf\OpenWithProgids\GIMP2.xcf. C:\Windows\System32\Config\SOFTWARE:Classes\GIMP2.xcf\shell\open\command identifies the executable for opening .xcf files as C:\Program Files\GIMP 2\bin\gimp-2.10.exe.

<u>Expected Response Illustration:</u>

Software registry hive:



	Name	Path
□ 1	(Default)	ROOT\Classes\GIMP2.xcf\shell\open\command\(Default)

```
"C:\Program Files\GIMP 2\bin\gimp-2.10.exe" "%1"·
```

TABLE 1

Question 26 - Operating System / File Analysis

Question 26: What is the name of the encrypted file found in C:\Users\james\Documents?

Manufacturer's Expected Response: vfpr6npaqea12.jpg

WebCode-Test	Response
2ZQE6A-5561	vfpr6npaqea12.jpg
4XFB84-5561	vfpr6npaqea12.jpg
64W7NX-5562	vfpr6npaqea12.jpg
6U9F26-5561	vfpr6npaqea12.jpg
6ZF77W-5562	vfpr6npaqea12.jpg
7K2ZUX-5562	vfpr6npaqea12.jpg
7M9E24-5561	vfpr6npaqea12.jpg
8Q3VR3-5562	vfpr6npaqea12.jpg
9ENXLY-5561	vfpr6npaqea12.jpg
ABKKEY-5561	vfpr6npaqea12.jpg
AQCK6Y-5561	vfpr6npaqea12.jpg
BJTE9R-5562	vfpr6npaqea12.jpg
C8D7KQ-5561	vfpr6npaqea12.jpg
CCTE9P-5562	vfpr6npaqea12.jpg
CKXLNP-5561	vfpr6npaqea12.jpg
CPXWKP-5562	000029.pdf
DGFL7P-5562	The encrypted file is 20_front2.xcf
DX4YHV-5561	vfpr6npaqea12.jpg
EQHHC7-5562	vfpr6npaqea12.jpg
ETQDAP-5562	vfpr6npaqea12.jpg
HG3KCP-5561	vfpr6npaqea12.jpg
HHBXTQ-5562	vfpr6npaqea12.jpg
J6MAYJ-5561	vfpr6npaqea12.jpg
KH3VVH-5562	vfpr6npaqea12.jpg

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 26 - Operating System / File Analysis

WebCode-Test	Response
MTJYGM-5562	vfpr6npaqea12.jpg
NF4QTK-5562	vfpr6npaqea12.jpg
NZEF7H-5561	vfpr6npaqea12.jpg
P6M4JK-5562	vfpr6npaqea12.jpg
P8TN8K-5561	vfpr6npaqea12.jpg
P92YZG-5562	vfpr6npaqea12.jpg
PZ7VVK-5561	vfpr6npagea12.jpg
Q7RBYH-5562	vfpr6npaqea12.jpg
QAQLVH-5561	vfpr6npaqea12.jpg
QFHW6F-5561	vfpr6npaqea12.jpg
QZQWEG-5561	vfpr6npaqea12.jpg
R7BE8H-5562	vfpr6npaqea12.jpg
TANE4A-5561	vfpr6npaqea12.jpg
TEV68F-5561	vfpr6npaqea12.jpg
TXBE8F-5561	vfpr6npaqea12.jpg
U3ZBAC-5562	vfpr6npaqea12.jpg
VBBWX7-5562	vfpr6npaqea12.jpg
VZACVE-5562	vfpr6npaqea12.jpg
W2ZUC7-5562	The answer is vfpr6npaqea12.jpg. From the Axiom 'encrypted files' artifact we can see that the encrypted file is vfpr6npaqea12.jpg and the file type as 'Encrypted Container'. Also validated and confirmed this by reviewing that the header of the file and it is not JPEG.
WVD6QB-5561	vfpr6npaqea12.jpg
XGCTUC-5561	vfpr6npaqea12.jpg
Y78Z2B-5561	vfpr6npaqea12.jpg
YCA984-5562	vfpr6npaqea12.jpg
Z4WK8A-5562	vfpr6npaqea12.jpg
Z6A992-5561	vfpr6npaqea12.jpg

TABLE 1

Question 26 - Operating System / File Analysis

Question 26: What is the name of the encrypted file found in C:\Users\james\Documents?

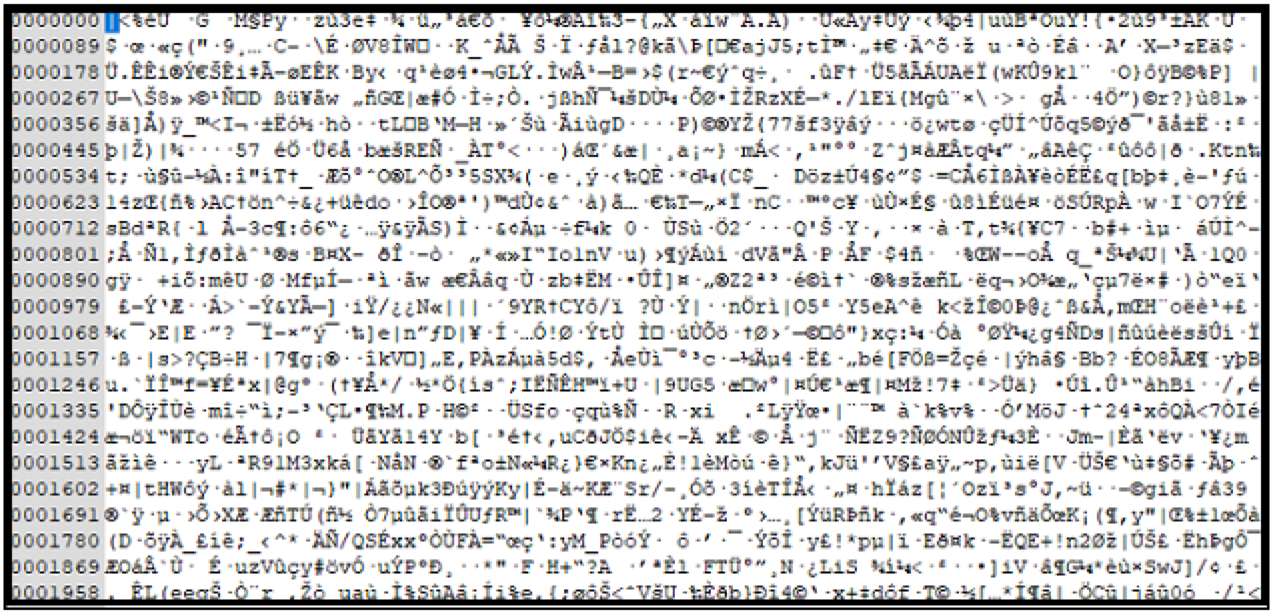
<u>Consensus Result:</u> "vfpr6npaqea12.jpg" and any slight variation, if they were easily identified as a spelling error.

<u>Expected Response Explanation</u>:

Within C:\Users\james\Documents there are only five files which have file signatures that do not correlate with their file extensions. All but one of these are easily readable by the associated application (Excel, Acrobat), or their content is readable in a text or hex editor. The content of vfpr6npaqea12.jpg, a purported jpeg image, does not include the typical jpeg headers or other content normally found in a jpg image. The appearingly random nature of this data is suggestive of encryption. The last modified date of this file is within 5 minutes of the last execution of Veracrypt.

<u>Expected Response Illustration:</u>

Encrypted contents of vfpr6npaqea12.jpg:



```
0000000 <‰èU ·G ·M$Py··zù3e‡·¼·ü„'ä€õ· ¥ö¼®AI‰3-{„X·äIw¨A.A)··U«Ay‡Uy·<¾þ‡|uùB*OuY!{•2û9'±AK·U·
0000089 $·œ·«ç("·9,…·C-·\É·ØV8ÎWD··K_^ÅÃ Š·Ï·ƒå1?@kã\Þ[D€ajJ5;tÌ™·„‡€·Ä^õ·ž u·²ò·Éâ··A'·X—³zEä$·
0000178 Ù.ÊÊi®Ÿ€ŠÊi‡Ã-øEÊK·By‹·q¹èø4•¬GLÝ.ÌwÅ¹—B=›$(r~€ý˜q÷,· .ûF†·Ù5ãÃÂUAëÏ(wKÛ9k1¨ ·O}óÿB©%P] |
0000267 U—\Š8»›©¹ÑDD ßü¥ãw „ñGE|æ‡Ó·Ì÷;Ò.·jßhÑ¯¼šDÙ¼·Õø•ÎŽRzXÉ—*./1Eï(Mgû¨×\·>· gÅ··4Ö")©r?}ù8l»·
0000356 šä]Å)ÿ_™<I¬·±Ëó¼·hò··tLDB'M—H·»´Šù·ÃiùgD····P)©®YŽ(77šf3ÿâý···ö¿wtø·çÙÍ^Ûõq5©ýð¯'ãå±Ë·:²·
0000445 þ|Ž)|¾····57 éÖ·Ü6å·bæšREÑ·_ÀT°<···)áŒ´&æ|·,a¡~}·mÁ<·,¹"°°·Z^j¤åÆÂtq¼"·„åAêÇ·²ûôõ|ð·.Ktn‰
0000534 t;·ù§û—½Å:î"iT†_·Æõ°^O®L^Õ³³5SX¾(·e·,ý·<‰QÈ·*d¼(C$_· Döz±Û4§¢"$·=CÅ6ÌßÀ¥èòÉËËq[bþ‡,è—'ƒú·
0000623 14zŒ(ñ‰›AC†ön^÷&¿+ûêdo·›ÎO®*')™dÙ¢&^·à)ã…·€‰T—„×Ï·nC··™°c¥·ùÙ×É§·û8iÉüé¤·öSÚRpÀ·w·I`O7ÝÉ·
0000712 sBd²R{·1 Å-3c¶:ô6"¿·…ÿ&ÿÃS)İ··&¢Åµ·÷f¼k 0· ÙSù·Ö2´···Q'Š·Y·,··×·à·T,t¾(¥C7··b‡+·ìµ· áÛÌ^—
0000801 ;Å·Ñ1,ÌƒõÌà^¹®s·B¤X- ðÎ·-ò· „*«»I"IolnV·u)›¶ýÁûi·dVã"Å·P·ÅF·$4ñ· ·‰ŒW--oÅ q_*Š¼¼U|'Ã·1Q0·
0000890 gÿ· +iõ:mêU·Ø·MfµÍ—·ªì·ãw æ€Åâq·Ù·zb‡ËM·•ÛÎ]¤·„®Z2²³·é©i†`·®%sžæñL·ëq¬›O¾æ„'çµ7ë×‡·)ò"eï'
0000979 £-Ý'Æ··Á>`-Ý&YÃ—]·iŸ/¿¿N«|||·´9YR†CYô/ì ?Ù·Ý|··nÖri|O5²·Y5eA^ê k<žÎ©0Þ@¿^ß&Å,mŒH¨oëè¹+£·
0001068 ¾‹¯›E|E·"? ¯Ï-×"ý¯·‰]e|n"ƒD|¥·Í·…Ó!Ø·ÝtÙ ÌD·úÙÕö·†Ø›´—©Dô"}xç:¼·Óà °ØŸ¼¿g4ÑDs|ñûúèësšÛi·Ï
0001157 ·ß·|s>?ÇB÷H·|7¶g¡®··ìkVD]„E,PÀzÁµà5d$,·ÅeÙi¯°³c·—½Åµ4·Ë£·„bé[FÖß=Žçé·|ýhá$·Bb?·ÉO8ÃÆ¶·ýþB
0001246 u.`ÏÎ™f=¥É*x|@g°·(†¥Å*/·½*Ö{is^;IÊÑÊH™i+U·|9UG5·æDw°|¤Û€¹æ¶|¤Mž!7‡··²>Üä} •Úi.Û¹"âhBi··/,é
0001335 'DÔÿÎÜè·mi÷"ì;-³'ÇL•¶‰M.P·H©²··ÜSfo·çqù‰Ñ··R·xi .²LÿŸœ•|¨¯™ à`k‰v‰··Ó'MöJ·†^24ªxôQÀ<7ÒIé
0001424 æ¬öl"WTo·éÅ†ô¡O ²· ÜãYã14Y·b[·*é†‹,uCðJÖ$iè‹-Ã xÊ·©·Å·j¨·ÑEZ9?ÑØÓNÛžƒ¼3È··Jm-|Èã'èv··'¥¿m
0001513 ãžiê···yL·ªR91M3xká[·NåN·®`fªo±N«¼R¿}€×Kn¿„Ë!lèMòú·ê}",kJü''V§£aÿ„~p,ùië[V·ÜŠ€'ù‡§õ‡·Ãþ·^
0001602 +¤|tHWóý·àl|¬#*|¬)"|ÁãõµK3ÐúÿýKy|É-ã~KÆ¨Sr/-,Óõ·3ièTÎÅ‹·„¤·hÏáz[¦´OzÏ³s°J,~ü··—®giã·ƒâ39
0001691 ®`ÿ·µ·›Ő›XÆ·ÆñTÚ(ñ½ Ò7µûãiÏÛUƒR™|`¾P'¶·rË…2·YÉ-ž·°›…,[ÝüRÞñk·,«q"é¬O‰vñäŐœK¡(¶,y"|Œ‰±lœÕà
0001780 (D·õÿÀ_£iê;_‹^*·ÀÑ/QSÉxx°ÒÙFÀ="œç':yM_PòóÝ· ô·'·¯·ÝõÎ·y£!*pµ|ï·Eð¤k·—ËQE+!n2Øž|ÚŠ£·ÈhÞgÕ¯
0001869 ÆOáÅ`Ù· É·uzVûçy‡övÓ·uÝP°Ð,··*"·F·H+"?A ·'*È1·FTÜ°",N·¿LiS ¾i¼‹·²···•]iV·â¶G¼*èù×SwJ]/¢·£·
0001958 , ÊL(eeqŠ·Ò¨r ,Žò uaù·Ì‰SûAâ;Ïi‰e,{;øôŠ<^VšU·‰È8b}Ði4©'·x+‡dôf·T®·½[…*Í¶ã|·ÒCû|jáû0ó ·/¹<
```

TABLE 1

Question 27 - Application / Web Browser Analysis

Question 27: What email application was installed by the user?

Manufacturer's Expected Response: Mozilla Thunderbird

WebCode-Test	Response
2ZQE6A-5561	Mozilla Thunderbird
4XFB84-5561	Mozilla Thunderbird 68.5.0(x86en-GB)
64W7NX-5562	Thunderbird
6U9F26-5561	Mozilla Thunderbird
6ZF77W-5562	Thunderbird
7K2ZUX-5562	Mozilla Thunderbird
7M9E24-5561	Mozilla Thunderbird
8Q3VR3-5562	Mozilla Thunderbird 68.5.0 (x86 en-GB)
9ENXLY-5561	Mozilla Thunderbird
ABKKEY-5561	Mozilla Thunderbird
AQCK6Y-5561	Thunderbird
BJTE9R-5562	Mozilla Thunderbird 68.5.0 (x86 en-GB)
C8D7KQ-5561	Mozilla THunderbird 68.5.0
CCTE9P-5562	Mozilla Thunderbird 68.5.0 (x86 en-GB)
CKXLNP-5561	Mozilla Thunderbird
CPXWKP-5562	Thunderbird
DGFL7P-5562	Mozilla Thunderbird
DX4YHV-5561	Thunderbird
EQHHC7-5562	Mozilla Thunderbird
ETQDAP-5562	thunderbird.exe
HG3KCP-5561	Mozilla Thunderbird 68.5.0
HHBXTQ-5562	Mozilla Thunderbird
J6MAYJ-5561	Mozilla Thunderbird 68.5.0
KH3VVH-5562	Mozilla thunderbird

TABLE 1

Question 27 - Application / Web Browser Analysis

WebCode-Test	Response
MTJYGM-5562	Thunderbird
NF4QTK-5562	Mozilla Thunderbird 68.5.0
NZEF7H-5561	Mozilla Thunderbird
P6M4JK-5562	THUNDERBIRD
P8TN8K-5561	Mozilla Thunderbird 68.5.0 (x86 en-GB)
P92YZG-5562	Mozilla Thundebird 68.5.0 (x86 en-GB)
PZ7VVK-5561	Mozilla Thunderbird 6.8.30
Q7RBYH-5562	Mozilla Thunderbird 68.5.0 (x86 en-GB)
QAQLVH-5561	Thunderbird
QFHW6F-5561	Mozilla Thunderbird 68.5.0
QZQWEG-5561	Mozilla Thunderbird
R7BE8H-5562	Mozilla Thunderbird 68.5.0
TANE4A-5561	Mozilla Thunderbird
TEV68F-5561	Mozilla Thunderbird 68.5.0
TXBE8F-5561	Thunderbird
U3ZBAC-5562	Mozilla Thunderbird 68.5.0
VBBWX7-5562	Mozilla Thunderbird 68.5.0 (x86 en-GB) v.68.5.0
VZACVE-5562	ThunderBird Portable
W2ZUC7-5562	The answer is Mozilla Thunderbird 68.5.0. Based on the Axiom data 'Installed Programs' artifact we can see that the email application installed by the user is Mozilla Thunderbird 68.5.0.
WVD6QB-5561	Mozilla Thunderbird (version 68.5.0)
XGCTUC-5561	Thunderbird
Y78Z2B-5561	Mozilla Thunderbird
YCA984-5562	Mozilla Thunderbird
Z4WK8A-5562	Mozilla Thunderbird 68.5.0 (x86 en-GB)
Z6A992-5561	Thunderbird

Question 27: What email application was installed by the user?

TABLE 1

Question 27 - Application / Web Browser Analysis

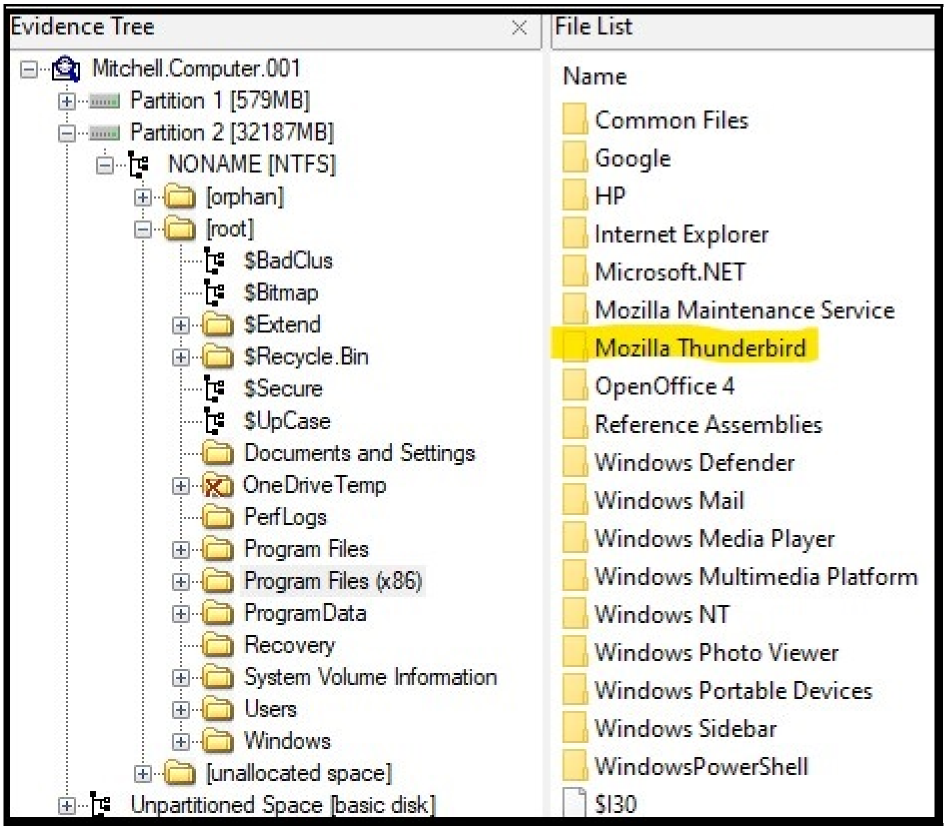
Consensus Result: Mozilla Thunderbird and any slight variation, if they were easily identified as a spelling error.

Expected Response Explanation:

The review of C:\Program Files and C:\Program Files (x86) identifies only two email-related software programs: The default install of Windows Mail, and "Mozilla Thunderbird".

Expected Response Illustration:

FTK Imager directory listing:



```
Evidence Tree
Mitchell.Computer.001
  Partition 1 [579MB]
  Partition 2 [32187MB]
    NONAME [NTFS]
      [orphan]
      [root]
        $BadClus
        $Bitmap
        $Extend
        $Recycle.Bin
        $Secure
        $UpCase
        Documents and Settings
        OneDriveTemp
        PerfLogs
        Program Files
        Program Files (x86)
        ProgramData
        Recovery
        System Volume Information
        Users
        Windows
      [unallocated space]
  Unpartitioned Space [basic disk]
```

```
File List
Name
Common Files
Google
HP
Internet Explorer
Microsoft.NET
Mozilla Maintenance Service
Mozilla Thunderbird
OpenOffice 4
Reference Assemblies
Windows Defender
Windows Mail
Windows Media Player
Windows Multimedia Platform
Windows NT
Windows Photo Viewer
Windows Portable Devices
Windows Sidebar
WindowsPowerShell
$I30
```

TABLE 1

Question 28 - Application / Web Browser Analysis

Question 28: What third party encryption application was executed by the user?

Manufacturer's Expected Response: Veracrypt

WebCode-Test	Response
2ZQE6A-5561	VeraCrypt Portable
4XFB84-5561	Veracrypt
64W7NX-5562	Veracrypt
6U9F26-5561	VeraCrypt
6ZF77W-5562	Veracrypt
7K2ZUX-5562	Veracrypt
7M9E24-5561	Veracrypt.exe
8Q3VR3-5562	VeraCrypt.exe
9ENXLY-5561	Veracrypt.exe
ABKKEY-5561	VeraCrypt
AQCK6Y-5561	VERACRYPT
BJTE9R-5562	VeraCrypt.exe
C8D7KQ-5561	VeraCyrpt
CCTE9P-5562	VeraCrypt.exe
CKXLNP-5561	VeraCrypt
CPXWKP-5562	Veracrypt
DGFL7P-5562	C:\Users\james\Downloads\VC\VeraCrypt.exe C:\Users\james\Downloads\VeraCrypt Portable 1.24-Update4.exe
DX4YHV-5561	Veracrypt
EQHHC7-5562	Veracrypt
ETQDAP-5562	VERACRYPT.EXE
HG3KCP-5561	Veracrypt
HHBXTQ-5562	VERACRYPT.EXE
J6MAYJ-5561	VeraCrypt.exe
KH3VVH-5562	VERACRYPT

TABLE 1

Question 28 - Application / Web Browser Analysis

WebCode-Test	Response
MTJYGM-5562	VERACRYPT
NF4QTK-5562	Veracrypt
NZEF7H-5561	Veracrypt.exe
P6M4JK-5562	Veracrypt
P8TN8K-5561	Veracrypt
P92YZG-5562	VeraCrypt
PZ7VVK-5561	veracrypt.exe
Q7RBYH-5562	VeraCrypt.exe
QAQLVH-5561	Veracrypt
QFHW6F-5561	Veracrypt
QZQWEG-5561	Veracrypt
R7BE8H-5562	VeraCrypt
TANE4A-5561	VeraCrypt
TEV68F-5561	VeraCrypt.exe
TXBE8F-5561	VeraCrypt
U3ZBAC-5562	VeraCrypt
VBBWX7-5562	VeraCrypt.exe
VZACVE-5562	VeraCrypt.exe
W2ZUC7-5562	The answer is VeraCrypt. Based on the program execution artifacts UserAssist, Shimcache and Prefetch and parsing data using Axiom artifacts we see that third party encryption application executed by the user is VeraCrypt.
WVD6QB-5561	Veracrypt (Veracrypt.exe)
XGCTUC-5561	Veracrypt
Y78Z2B-5561	VeraCrypt
YCA984-5562	Veracrypt
Z4WK8A-5562	VeraCrypt.exe
Z6A992-5561	VeraCrypt

Question 28: What third party encryption application was executed by the user?

Question 28 - Application / Web Browser Analysis

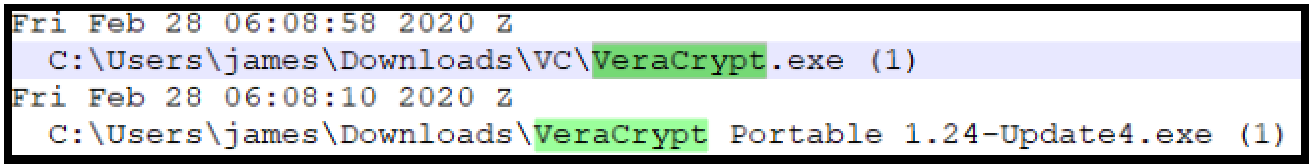
Consensus Result: "Veracrypt" and any slight variation, if they were easily identified as a spelling error.

Expected Response Explanation:

Windows records executions of most programs in the SYSTEM registry at C:\Windows\System32\Config\SYSTEM:ControlSet001\Control\Session Manager\AppCompatCache reviewing this key's contents discovers several records of execution of C:\Users\james\Downloads\VC\VeraCrypt.exe. User james' NTUSER.DAT registry hive contains records VeraCrypt execution at C:\users\james\NTUSER.DAT:Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist.

Expected Response Illustration:

RegRipper Parsed (james') NTUSER.DAT registry key:



```
Fri Feb 28 06:08:58 2020 Z
  C:\Users\james\Downloads\VC\VeraCrypt.exe (1)
Fri Feb 28 06:08:10 2020 Z
  C:\Users\james\Downloads\VeraCrypt Portable 1.24-Update4.exe (1)
```

TABLE 1

Question 29 - Application / Web Browser Analysis

Question 29: On what date and time was this third party encryption application LAST executed? Provide your in the UTC + 00:00 using the following format: MM/DD/YYYY HH:MM:SS AM/PM

Manufacturer's Expected Response: 02/28/2020 06:09:01 AM (UTC)

** Inconsistencies not highlighted; No consensus achieved **

WebCode-Test	Response
2ZQE6A-5561	02/28/2020 06:09:01 AM
4XFB84-5561	02/28/2020 06:08:58 AM
64W7NX-5562	02/28/2020 06:08:58
6U9F26-5561	2/28/2020 6:09:01 AM
6ZF77W-5562	02/28/2020 06:09:01 AM
7K2ZUX-5562	02/28/2020 06:09:01 AM
7M9E24-5561	02/28/2020 06:09:01 AM
8Q3VR3-5562	02/28/2020 06:08:58 AM
9ENXLY-5561	2/28/2020 6:09:18 AM
ABKKEY-5561	02/28/2020 06:09:01 AM
AQCK6Y-5561	02/28/2020 06:09:01 AM
BJTE9R-5562	02/28/2020 06:09:01 AM (UTC + 00:00)
C8D7KQ-5561	03/01/2020 15:56:37 PM
CCTE9P-5562	2/28/2020 6:09:01 AM UTC
CKXLNP-5561	02/28/2020 06:17:18 AM
CPXWKP-5562	Veracrypt.exe was executed at 02/28/2020 06:09:01 AM Veracrypt Format.exe was executed at 02/28/2020 06:17:18 AM
DGFL7P-5562	the latest run date was 2/28/2020 6:08:58 AM UTC for the encryption application located in C:\Users\james\Downloads\VC\VeraCrypt.exe
DX4YHV-5561	03/01/2020 03:56:37 PM
EQHHC7-5562	Last Accessed Time: 01/03/2020 15:56:37 – Last time VeraCrypt.exe file opened: 01/03/2020 16:01:45
ETQDAP-5562	28/02/2020 06:09:01 AM
HG3KCP-5561	02/28/2020 06:08:58 AM
HHBXTQ-5562	02/28/20 06:09:01 AM
J6MAYJ-5561	02/28/2020 6:09:01 AM

TABLE 1

Question 29 - Application / Web Browser Analysis

WebCode-Test	Response ** Inconsistencies not highlighted; No consensus achieved **
KH3VVH-5562	02/28/2020 06:09:01 AM
MTJYGM-5562	02/28/2020 06:09:01 AM
NF4QTK-5562	02/28/2020 06:09:01 AM
NZEF7H-5561	2/28/2020 6:09:01 AM
P6M4JK-5562	02/28/2020 06:09:01 AM
P8TN8K-5561	02/28/2020 06:24:00 AM
P92YZG-5562	02/28/2020 6:09:01 AM
PZ7VVK-5561	02/28/2020 6:08:58 AM
Q7RBYH-5562	02/28/2020 06:09:01 (from Prefetch)
QAQLVH-5561	02/28/2020 06:09:01 AM
QFHW6F-5561	02/28/2020 06:08:58 AM
QZQWEG-5561	02/28/2020 06:09:01 AM (UTC)
R7BE8H-5562	03/01/2020 15:56:37
TANE4A-5561	02/28/2020 06:09:01 AM
TEV68F-5561	03/01/2020 3:56:37 PM
TXBE8F-5561	03/01/2020 03:56:37 pm UTC +00:00
U3ZBAC-5562	3/01/2020 15:56:37
VBBWX7-5562	2/28/2020 6:08:58 AM
VZACVE-5562	3/1/2020 3:56:37 PM
W2ZUC7-5562	The answer is 2/28/2020 6:08:37 AM UTC. By parsing the Shimcache artifact in Axiom I see that the last updated date and time as 2/28/2020 6:08:37 AM UTC for the veracrypt which is when the application last executed.
WVD6QB-5561	02/28/2020 06:09:01 AM
XGCTUC-5561	03/01/2020 03:56:37 PM
Y78Z2B-5561	02/28/2020 06:14:32 AM
YCA984-5562	02/28/2020 06:09:01 AM
Z4WK8A-5562	02/28/2020 06:08:58 AM
Z6A992-5561	02/28/2020 06:09:03 AM

TABLE 1

Question 29 - Application / Web Browser Analysis

Question 29: On what date and time was this third party encryption application LAST executed? Provide your in the UTC + 00:00 using the following format: MM/DD/YYYY HH:MM:SS AM/PM

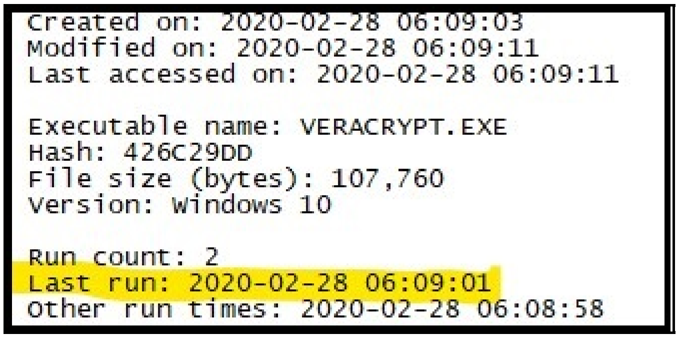
Consensus Result: A consensus was not achieved. Although 81% reported the expected date, only 50% reported the expected time. The objective was to identify VeraCrypt as the third party encryption application and locate the last time this program was executed.

Expected Response Explanation:

Windows Prefetch data contains records of execution of the VeraCrypt program in C:\Windows\Prefetch\ VERACRYPT.EXE-426C29DD.pf. Parsing this file with a prefetch analysis tool shows what is captured in the image provided below.

Expected Response Illustration:

PECmd parsed VERACRYPT.EXE-426C29DD.pf prefetch file:



```
Created on: 2020-02-28 06:09:03
Modified on: 2020-02-28 06:09:11
Last accessed on: 2020-02-28 06:09:11

Executable name: VERACRYPT.EXE
Hash: 426C29DD
File size (bytes): 107,760
Version: Windows 10

Run count: 2
Last run: 2020-02-28 06:09:01
Other run times: 2020-02-28 06:08:58
```

TABLE 1

Question 30 - Application / Web Browser Analysis

Question 30: Provide the FIRST term searched using Google Chrome on this device.

Manufacturer's Expected Response: torproject

WebCode-Test	Response
2ZQE6A-5561	torproject
4XFB84-5561	torproject
64W7NX-5562	torproject
6U9F26-5561	torproject
6ZF77W-5562	torproject
7K2ZUX-5562	Torproject
7M9E24-5561	Torproject
8Q3VR3-5562	Torproject
9ENXLY-5561	torproject
ABKKEY-5561	torproject
AQCK6Y-5561	torproject
BJTE9R-5562	torproject
C8D7KQ-5561	torproject
CCTE9P-5562	torproject
CKXLNP-5561	torproject
CPXWKP-5562	torproject
DGFL7P-5562	the first search term is "torproject" on 2/10/2020 1:58:13 AM UTC in the user account james chrome history \Users\james\AppData\Local\Google\Chrome\User Data\Default\History
DX4YHV-5561	torproject
EQHHC7-5562	Tor project
ETQDAP-5562	torproject
HG3KCP-5561	Tor Project
HHBXTQ-5562	torproject
J6MAYJ-5561	high res us money scans
KH3VVH-5562	torproject

TABLE 1

Question 30 - Application / Web Browser Analysis

WebCode-Test	Response
MTJYGM-5562	torproject
NF4QTK-5562	torproject
NZEF7H-5561	torproject
P6M4JK-5562	torproject
P8TN8K-5561	torproject
P92YZG-5562	torproject
PZ7VVK-5561	torproject
Q7RBYH-5562	torproject
QAQLVH-5561	torproject
QFHW6F-5561	torproject
QZQWEG-5561	torproject
R7BE8H-5562	us dollar
TANE4A-5561	torproject
TEV68F-5561	torproject
TXBE8F-5561	torproject
U3ZBAC-5562	toroproject
VBBWX7-5562	torproject
VZACVE-5562	torproject
W2ZUC7-5562	The answer is Torproject. By parsing the raw image using Axiom, the 'Google searches' artifact provide these details. By sorting by time, I see that the first term searched using google chrome on this device is Torproject.
WVD6QB-5561	torproject
XGCTUC-5561	torproject
Y78Z2B-5561	torproject
YCA984-5562	torproject
Z4WK8A-5562	torproject
Z6A992-5561	torproject

Question 30: Provide the FIRST term searched using Google Chrome on this device.

TABLE 1

Question 30 - Application / Web Browser Analysis

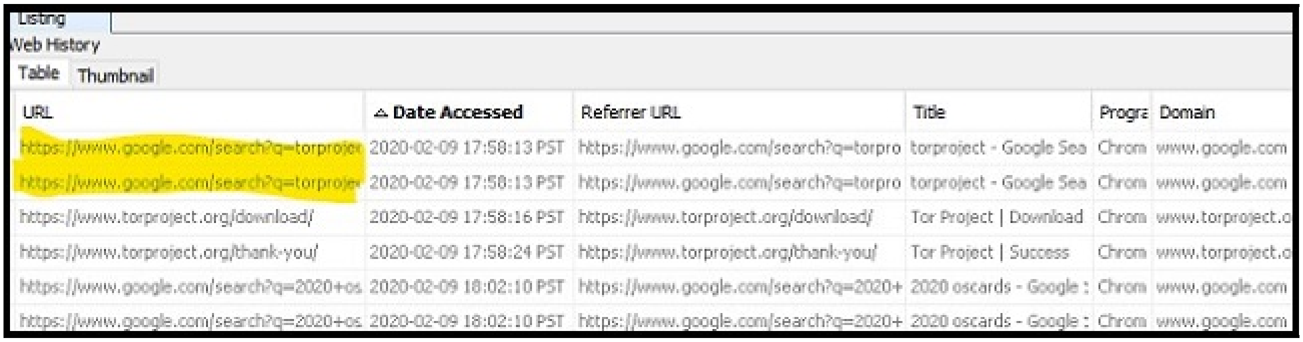
Consensus Result: "Torproject" and any slight variation, if they were easily identified as a spelling error.

Expected Response Explanation:

The Google Chrome internet browser history for '"james" is stored in an SQLite database at C:/Users/james/AppData/Local/Google/Chrome/User Data/Default/History. Parsing this database shows the first entry to be a Google search for "torproject".

Expected Response Illustration:

Autopsy parsed internet browser history:



URL	⚠ Date Accessed	Referrer URL	Title	Progra	Domain
https://www.google.com/search?q=torprojec	2020-02-09 17:58:13 PST	https://www.google.com/search?q=torpro	torproject - Google Sea	Chrom	www.google.com
https://www.google.com/search?q=torprojec	2020-02-09 17:58:13 PST	https://www.google.com/search?q=torpro	torproject - Google Sea	Chrom	www.google.com
https://www.torproject.org/download/	2020-02-09 17:58:16 PST	https://www.torproject.org/download/	Tor Project | Download	Chrom	www.torproject.o
https://www.torproject.org/thank-you/	2020-02-09 17:58:24 PST	https://www.torproject.org/thank-you/	Tor Project | Success	Chrom	www.torproject.o
https://www.google.com/search?q=2020+os	2020-02-09 18:02:10 PST	https://www.google.com/search?q=2020+	2020 oscards - Google :	Chrom	www.google.com
https://www.google.com/search?q=2020+os	2020-02-09 18:02:10 PST	https://www.google.com/search?q=2020+	2020 oscards - Google :	Chrom	www.google.com

TABLE 1

Question 31 - Application / Web Browser Analysis

Question 31: What darkweb (darknet) site did the user bookmark?

Manufacturer's Expected Response: dreadditevelidot.onion

WebCode-Test	Response
2ZQE6A-5561	http://dreadditevelidot.onion
4XFB84-5561	https://dreadditevelidot.onion/d/counterfeiting
64W7NX-5562	http://dreadditevelidot.onion
6U9F26-5561	dreadditevelidot.onion
6ZF77W-5562	http://dreadditevelidot.onion
7K2ZUX-5562	http://dreadditevelidot.onion/d/Counterfeiting
7M9E24-5561	http://dreadditevelidot.onion.com
8Q3VR3-5562	http://dreadditevelidot.onion
9ENXLY-5561	http://dreadditevelidot.onion/d/Counterfeiting
ABKKEY-5561	http://dreadditevelidot.onion/post/2fb1a799ff8680f6/#c-381319d3fd33495a0a and http://dreadditevelidot.onion/d/Counterfeiting
AQCK6Y-5561	http://dreadditevelidot.onion
BJTE9R-5562	http://dreadditevelidot.onion/d/Counterfeiting, http://dreadditevelidot.onion/post/2fb1a799ff8680f6/#c-381319d3fd33495a0a
C8D7KQ-5561	http://dreadditevelidot.onion/d/Counterfeiting
CCTE9P-5562	http://dreadditevelidot.onion. I found below two URLs bookmarked in Mozila Firefox browser: http://dreadditevelidot.onion/d/Counterfeiting http://dreadditevelidot.onion/post/2fb1a799ff8680f6/#c-381319d3fd33495a0a
CKXLNP-5561	http://dreadditevelidot.onion/d/Counterfeiting
CPXWKP-5562	dreadditevelidot.onion
DGFL7P-5562	the following site http://dreadditevelidot.onion/post/2fb1a799ff8680f6/#c-381319d3fd33495a0a was found bookmarked in the user account james FireFox history located in Users\james\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\places.sqlite
DX4YHV-5561	http://dreadditevelidot.onion
EQHHC7-5562	http://dreadditevelidot.onion/post/2fb1a799ff8680f6/#c-381319d3fd33495a0a and http://dreadditevelidot.onion/d/Counterfeiting
ETQDAP-5562	http://dreadditevelidot.onion/d/Counterfeiting http://dreadditevelidot.onion/post/2fb1a799ff8680f6/#c-381319d3fd33495a0a
HG3KCP-5561	Dreadditevelidot.onion
HHBXTQ-5562	http://dreadditevelidot.onion/post/2fb1a799ff8680f6/#c-381319d3fd33495a0a http://dreadditevelidot.onion/d/Counterfeiting
J6MAYJ-5561	http://dreadditevelidot.onion/d/Counterfeiting and http://dreadditevelidot.onion/post/2fb1a799ff8680f6/#c-381319d3fd33495a0a

TABLE 1

Question 31 - Application / Web Browser Analysis

WebCode-Test	Response
KH3VVH-5562	http://dreadditevelidot.onion/post/2fb1a799ff8680f6/#c-381319d3fd33495a0a http://dreadditevelidot.onion/Counterfeiting
MTJYGM-5562	http://dreadditevelidot.onion
NF4QTK-5562	http://dreadditevelidot.onion/
NZEF7H-5561	http://dreadditevelidot.onion
P6M4JK-5562	dreadditevelidot.onion
P8TN8K-5561	http://dreadditevelidot.onion/d/Counterfeiting and http://dreadditevelidot.onion/post/2fb1a799ff8680f6/#c-381319d3fd33495a0a
P92YZG-5562	http://dreadditevelidot.onion/d/Counterfeiting
PZ7VVK-5561	dreadditevelidot.onion
Q7RBYH-5562	http://dreadditevelidot.onion/d/Counterfeiting
QAQLVH-5561	http://dreadditevelidot.onion/post/2fb1a799ff86080f6/#c-381319d3fd33495a0a http://dreadditevelidot.onion/d/Counterfeiting
QFHW6F-5561	http://dreadditevelidot.onion
QZQWEG-5561	dreadditevelidot.onion
R7BE8H-5562	http://dreadditevelidot.onion/Counterfeiting
TANE4A-5561	http://dreadditevelidot.onion
TEV68F-5561	http://dreadditevelidot.onion
TXBE8F-5561	http://dreadditevelidot.onion/d/Counterfeiting
U3ZBAC-5562	Best paper to use for counterfeit USD? : /d/Forgeries – Dread
VBBWX7-5562	http://dreadditevelidot.onion/post/2fb1a799ff8680f6/#c-381319d3fd33495a0a
VZACVE-5562	http://dreadditevelidot.onion/post/2fb1a799ff8680f6/#c-381319d3fd33495a0a
W2ZUC7-5562	The answer is H t t p : / / dreadditevelidot.onion/post/2fb1a799ff8680f6/#c-381319d3fd33495a0a. I got this information from 'Firefox Bookmarks' under 'Web related' artifacts in Axiom forensic tool.
WVD6QB-5561	http://dreadditevelidot.onion
XGCTUC-5561	http://dreadditevelidot.onion
Y78Z2B-5561	http://dreadditevelidot.onion/d/Counterfeiting
YCA984-5562	http://dreadditevelidot.onion
Z4WK8A-5562	http://dreadditevelidot.onion

TABLE 1

Question 31 - Application / Web Browser Analysis

WebCode-Test	Response
Z6A992-5561	http://dreadditevelidot.onion/d/Counterfeiting

Question 31: What darkweb (darknet) site did the user bookmark?

Consensus Result: dreadditevelidot.onion

Expected Response Explanation:

The user installed the Tor Browser darkweb browser in his downloads directory. Tor Browser stores browsing history and bookmarks to an SQLite database at C:/Users/james/Desktop/Tor Browser/Browser/TorBrowser/Data/Browser/profile.default/places.sqlite. The moz_bookmarks and moz_places tables in this database store factory and user added bookmarks. These tables contain bookmarks for two pages on the Dread forum site (a Reddit-like dark web discussion forum) at http://dreadditevelidot.onion/. Darkweb sites are identified by the top level domain (TLD) of .onion.

Expected Response Illustration:

Moz_places table:

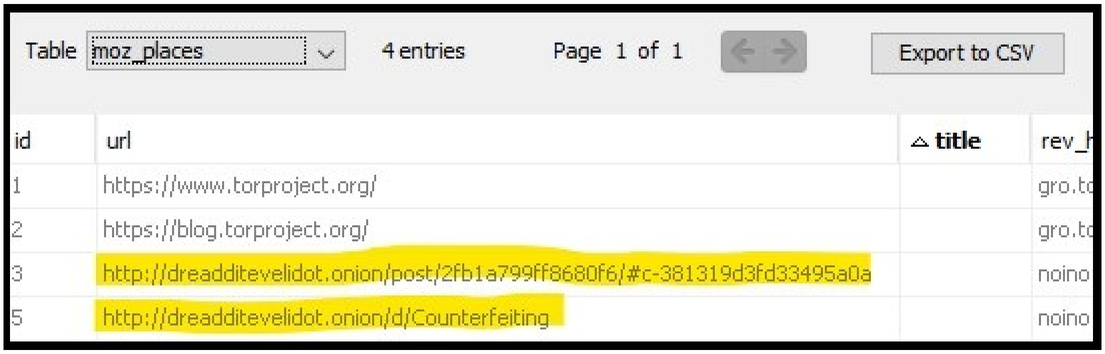


Table moz_places 4 entries Page 1 of 1

id	url	△ title	rev_h
1	https://www.torproject.org/		gro.to
2	https://blog.torproject.org/		gro.to
3	http://dreadditevelidot.onion/post/2fb1a799ff8680f6/#c-381319d3fd33495a0a		noino
5	http://dreadditevelidot.onion/d/Counterfeiting		noino

TABLE 1

Question 32 - Application / Web Browser Analysis

Question 32: What web browser was used to download openoffice?

Manufacturer's Expected Response: Microsoft edge

WebCode-Test	Response
2ZQE6A-5561	Microsoft Edge
4XFB84-5561	Edge/Internet Explorer
64W7NX-5562	Internet Explorer
6U9F26-5561	Microsoft Edge
6ZF77W-5562	Microsoft Edge
7K2ZUX-5562	Internet Explorer 10-11
7M9E24-5561	Microsoft Edge
8Q3VR3-5562	Microsoft Edge
9ENXLY-5561	Edge/Internet Explorer
ABKKEY-5561	Edge
AQCK6Y-5561	Microsoft Edge
BJTE9R-5562	Internet Explorer
C8D7KQ-5561	Internet Explorer
CCTE9P-5562	Microsoft Edge
CKXLNP-5561	Internet Explorer
CPXWKP-5562	Microsoft Edge
DGFL7P-5562	Microsoft Edge located in \Users\james\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat
DX4YHV-5561	Edge/Internet Explorer 10-11
EQHHC7-5562	Edge/Internet Explorer
ETQDAP-5562	Microsoft Edge
HG3KCP-5561	Edge/Internet Explorer 10
HHBXTQ-5562	Microsoft Edge
J6MAYJ-5561	Edge/InternetExplorer 10-11
KH3VVH-5562	Microsoft Edge

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 32 - Application / Web Browser Analysis

WebCode-Test	Response
MTJYGM-5562	Microsoft Edge
NF4QTK-5562	Microsoft Edge
NZEF7H-5561	Microsoft Edge
P6M4JK-5562	Microsoft Edge
P8TN8K-5561	Microsoft Edge/Internet Explorer
P92YZG-5562	Internet Explorer
PZ7VVK-5561	Edge/Internet Explorer 10
Q7RBYH-5562	Microsoft Edge
QAQLVH-5561	Edge
QFHW6F-5561	Edge/Internet Explorer
QZQWEG-5561	Microsoft Edge
R7BE8H-5562	Edge/Internet Explorer 10-11
TANE4A-5561	Microsoft Edge
TEV68F-5561	Microsoft Edge browser
TXBE8F-5561	www.bing.com
U3ZBAC-5562	MicrosoftEdge
VBBWX7-5562	Microsoft Edge Browser
VZACVE-5562	Microsoft Edge browse
W2ZUC7-5562	The answer is Edge browser. I got this information from 'Edge/Internet Explorer 10-11 Downloads' under 'Web related' artifacts in Axiom where the openoffice is downloaded from sourceforge website using Edge browser.
WVD6QB-5561	Microsoft Edge
XGCTUC-5561	Edge
Y78Z2B-5561	Microsoft Edge
YCA984-5562	Microsoft Edge
Z4WK8A-5562	Microsoft Edge
Z6A992-5561	Internet Explorer

Question 32: What web browser was used to download openoffice?

TABLE 1

Question 32 - Application / Web Browser Analysis

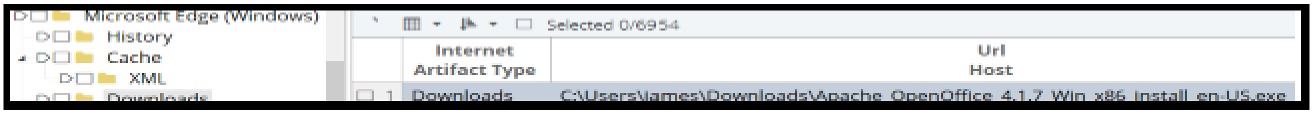
Consensus Result: Microsoft edge

Expected Response Explanation:

To determine what web browser was used to download openoffice, one would view James' Microsoft internet browsing history file at C\Users\james\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat which contains a download record for the URL of the openoffice installer, C:\Users\james\Downloads\Apache_OpenOffice_4.1.7_Win_x86_install_en-US.exe and the record indicates Microsoft Edge as the browser.

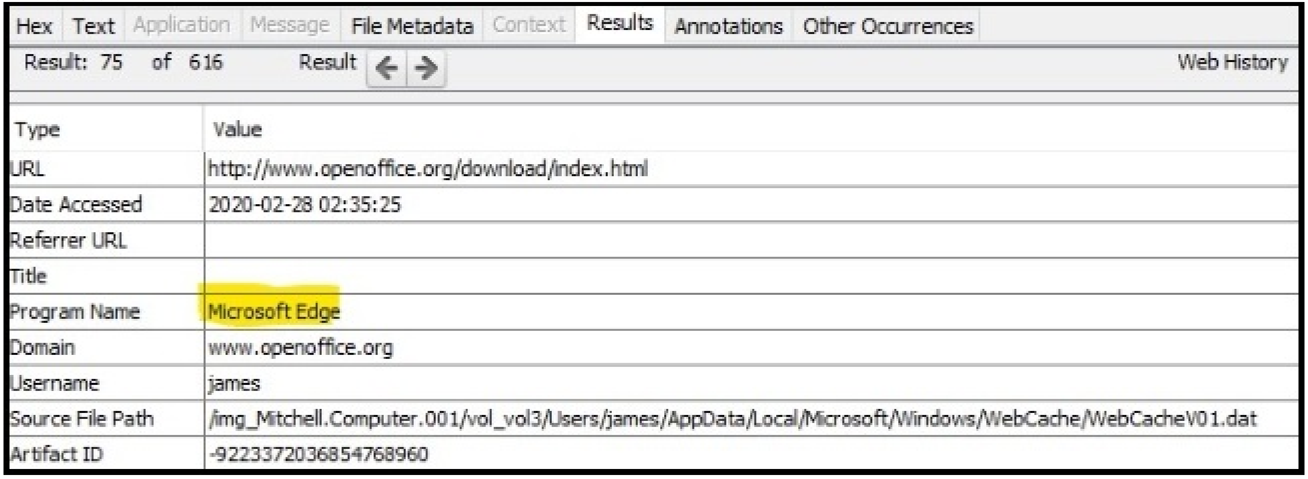
Expected Response Illustration:

EnCase parsed Edge "Downloads" records from WebcacheV01.dat:



	Internet Artifact Type	Url Host
1	Downloads	C:\Users\james\Downloads\Apache_OpenOffice_4.1.7_Win_x86_install_en-US.exe

Autopsy parsed Edge "Downloads" records from WebcacheV01.dat:



Type	Value
URL	http://www.openoffice.org/download/index.html
Date Accessed	2020-02-28 02:35:25
Referrer URL	
Title	
Program Name	Microsoft Edge
Domain	www.openoffice.org
Username	james
Source File Path	/img_Mitchell.Computer.001/vol_vol3/Users/james/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat
Artifact ID	-9223372036854768960

TABLE 1

Question 33 - Operating System / Prefetch Analysis

Question 33: From the information in prefetch, how many times was Tor.exe executed? Provide a NUMERIC response (e.g. 1, 2, 3).

Manufacturer's Expected Response: 4

WebCode-Test	Response	** Inconsistencies not highlighted; No consensus achieved **
2ZQE6A-5561	4	
4XFB84-5561	4	
64W7NX-5562	0	
6U9F26-5561	0	
6ZF77W-5562	4	
7K2ZUX-5562	0 (zero)	
7M9E24-5561	4	
8Q3VR3-5562	4	
9ENXLY-5561	0	
ABKKEY-5561	4	
AQCK6Y-5561	4	
BJTE9R-5562	0	
C8D7KQ-5561	1	
CCTE9P-5562	4	
CKXLNP-5561	0	
CPXWKP-5562	0	
DGFL7P-5562	4	
DX4YHV-5561	4	
EQHHC7-5562	1	
ETQDAP-5562	4	
HG3KCP-5561	4	
HHBXTQ-5562	4	
J6MAYJ-5561	8	

TABLE 1

Question 33 - Operating System / Prefetch Analysis

WebCode-Test	Response ** Inconsistencies not highlighted; No consensus achieved **
KH3VVH-5562	4
MTJYGM-5562	4
NF4QTK-5562	4
NZEF7H-5561	4
P6M4JK-5562	0
P8TN8K-5561	4
P92YZG-5562	4
PZ7VVK-5561	4
Q7RBYH-5562	0
QAQLVH-5561	4
QFHW6F-5561	4
QZQWEG-5561	4
R7BE8H-5562	1. 02/15/2020 13:48:17
TANE4A-5561	0
TEV68F-5561	8
TXBE8F-5561	3
U3ZBAC-5562	0
VBBWX7-5562	4
VZACVE-5562	8
W2ZUC7-5562	The answer is 4. I have exported the Tor prefetch file and by parsing it using Eric Zimmerman's PEcmd, I see that the file was ran 4 times.
WVD6QB-5561	4
XGCTUC-5561	4
Y78Z2B-5561	4
YCA984-5562	4
Z4WK8A-5562	4
Z6A992-5561	4 (four)

TABLE 1

Question 33 - Operating System / Prefetch Analysis

Question 33: From the information in prefetch, how many times was Tor.exe executed? Provide a NUMERIC response (e.g. 1, 2, 3).

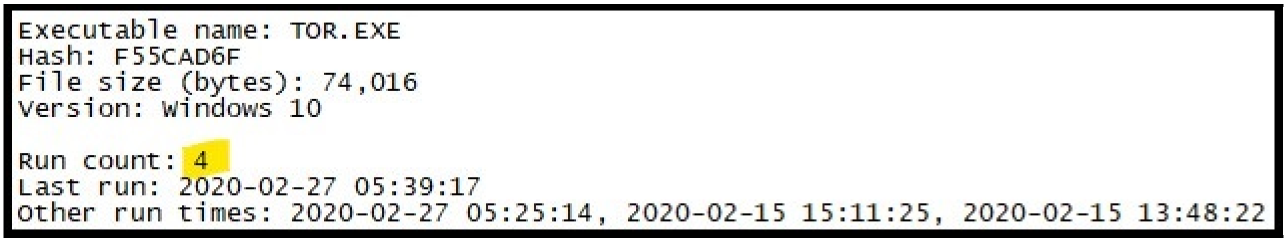
Consensus Result: A consensus was not achieved. Although the majority of participants reported the expected response of "4", eleven other participants reported the response of zero (0). The objective of this question was to view the prefetch files for Tor.exe and determine how many times this program was executed.

Expected Response Explanation:

C:\Windows\Prefetch contains one prefetch file for Tor.exe, TOR.EXE-F55CAD6F.pf. Parsing this file determines the run count to be 4.

Expected Response Illustration:

PECmd parsed TOR.EXE-F55CAD6F.pf prefetch file:



```
Executable name: TOR.EXE
Hash: F55CAD6F
File size (bytes): 74,016
Version: Windows 10

Run count: 4
Last run: 2020-02-27 05:39:17
Other run times: 2020-02-27 05:25:14, 2020-02-15 15:11:25, 2020-02-15 13:48:22
```

TABLE 1

Question 34 - Document Metadata Analysis

Question 34: Who LAST modified 000051.xls?

Manufacturer's Expected Response: richburg_r

WebCode-Test	Response
2ZQE6A-5561	richburg_r
4XFB84-5561	richburg_r
64W7NX-5562	richburg_r
6U9F26-5561	richburg_r
6ZF77W-5562	richburg_r
7K2ZUX-5562	richburg_r
7M9E24-5561	richburg_r
8Q3VR3-5562	richburg_r
9ENXLY-5561	richburg_r
ABKKEY-5561	richburg_r
AQCK6Y-5561	richburg_r
BJTE9R-5562	richburg_r
C8D7KQ-5561	richburg_r
CCTE9P-5562	richburg_r
CKXLNP-5561	richburg_r
CPXWKP-5562	richburg_r
DGFL7P-5562	the last author was richburg_r located in the metadata of the file located in \Users\james\Documents\000051.xls
DX4YHV-5561	richburg_r
EQHHC7-5562	richburg_r
ETQDAP-5562	richburg_r
HG3KCP-5561	richburg_r
HHBXTQ-5562	richburg_r
J6MAYJ-5561	richburg_r
KH3VVH-5562	richburg_r

TABLE 1

Question 34 - Document Metadata Analysis	
WebCode-Test	**Response**
MTJYGM-5562	richburg_r
NF4QTK-5562	richburg_r
NZEF7H-5561	richburg_r
P6M4JK-5562	richburg_r
P8TN8K-5561	richburg_r
P92YZG-5562	richburg_r
PZ7VVK-5561	richburg_r
Q7RBYH-5562	richburg_r
QAQLVH-5561	richburg_r
QFHW6F-5561	richburg_r
QZQWEG-5561	richburg_r
R7BE8H-5562	richburg_r
TANE4A-5561	richburg_r
TEV68F-5561	Richburg_r
TXBE8F-5561	richburg_r
U3ZBAC-5562	richburg_r
VBBWX7-5562	richburg_r
VZACVE-5562	Richburg_r
W2ZUC7-5562	The answer is richburg_r. I have searched for the file name 000051.xls in Axiom forensics tool which provided the information of the file which has last author modified as richburg_r
WVD6QB-5561	richburg_r
XGCTUC-5561	richburg_r
Y78Z2B-5561	richburg_r
YCA984-5562	richburg_r
Z4WK8A-5562	richburg_r
Z6A992-5561	richburg_r

Question 34: Who LAST modified 000051.xls?

TABLE 1

Question 34 - Document Metadata Analysis

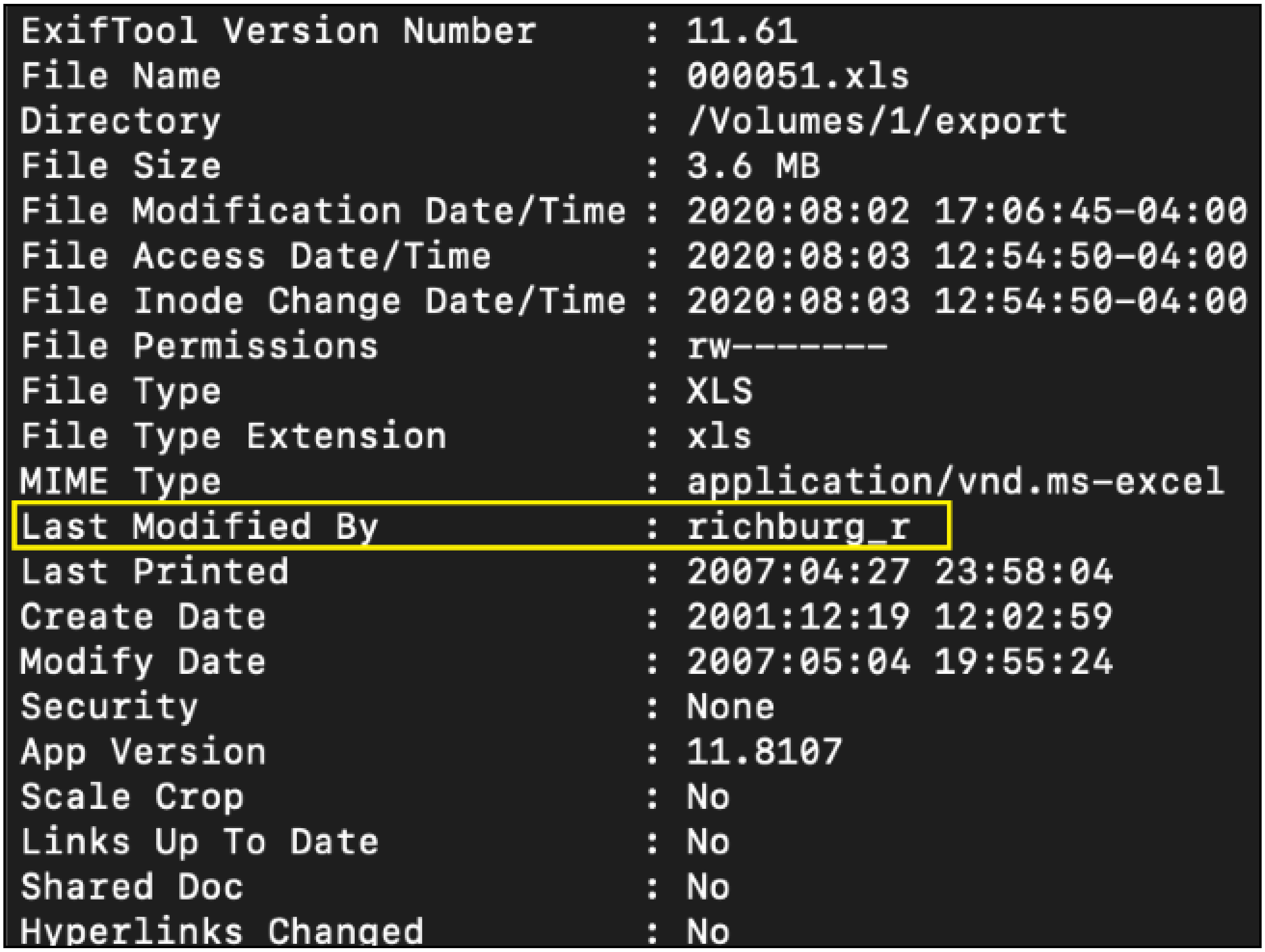
Consensus Result: richburg_r

Expected Response Explanation:

Parsing the metadata from 000051.xls show the “Last Modified By” field lists “richburg_r”. Microsoft Excel will also show this under the info section under the file tab.

Expected Response Illustration:

Metadata:

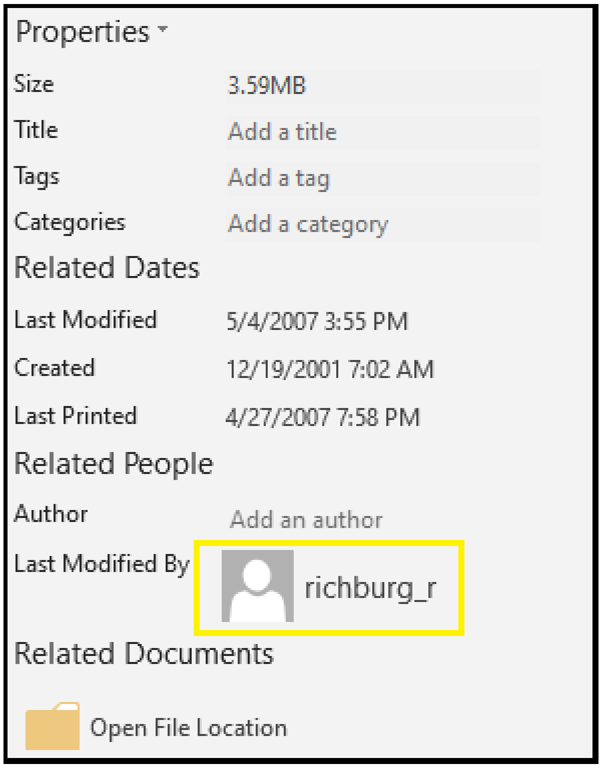


```
ExifTool Version Number      : 11.61
File Name                    : 000051.xls
Directory                    : /Volumes/1/export
File Size                    : 3.6 MB
File Modification Date/Time : 2020:08:02 17:06:45-04:00
File Access Date/Time        : 2020:08:03 12:54:50-04:00
File Inode Change Date/Time : 2020:08:03 12:54:50-04:00
File Permissions             : rw-------
File Type                    : XLS
File Type Extension          : xls
MIME Type                    : application/vnd.ms-excel
Last Modified By             : richburg_r
Last Printed                 : 2007:04:27 23:58:04
Create Date                  : 2001:12:19 12:02:59
Modify Date                  : 2007:05:04 19:55:24
Security                     : None
App Version                  : 11.8107
Scale Crop                   : No
Links Up To Date             : No
Shared Doc                   : No
Hyperlinks Changed           : No
```

TABLE 1

Question 34 - Document Metadata Analysis

Excel Info tab:



Properties ▾

Size	3.59MB
Title	Add a title
Tags	Add a tag
Categories	Add a category

Related Dates

Last Modified	5/4/2007 3:55 PM
Created	12/19/2001 7:02 AM
Last Printed	4/27/2007 7:58 PM

Related People

Author	Add an author
Last Modified By	richburg_r

Related Documents

TABLE 1

Question 35 - Document Metadata Analysis

Question 35: Who is the Author of 004583.doc?

Manufacturer's Expected Response: Celal Konor

WebCode-Test	Response
2ZQE6A-5561	Celal Konor
4XFB84-5561	Celal Konor
64W7NX-5562	Celal Konor
6U9F26-5561	Celal Konor
6ZF77W-5562	Celal Konor
7K2ZUX-5562	Celal Konor
7M9E24-5561	rabel
8Q3VR3-5562	Celal Konor
9ENXLY-5561	Celal Konor
ABKKEY-5561	Celal Konor
AQCK6Y-5561	Celal Konor
BJTE9R-5562	Celal Konor
C8D7KQ-5561	celal konor
CCTE9P-5562	Celal Konor
CKXLNP-5561	Celal Konor
CPXWKP-5562	Celal Konor
DGFL7P-5562	The author of the document is Celal Konor and the last author was rabel found in the metadata of the file located in \Users\james\Documents\004583.doc
DX4YHV-5561	Celal Konor
EQHHC7-5562	Celal Konor
ETQDAP-5562	Celal Konor
HG3KCP-5561	Celal Konor
HHBXTQ-5562	Celal Konor
J6MAYJ-5561	Celal Konor
KH3VVH-5562	Celal Konor

TABLE 1

Question 35 - Document Metadata Analysis

WebCode-Test	Response
MTJYGM-5562	Celal Konor
NF4QTK-5562	rabel
NZEF7H-5561	Celal Konor
P6M4JK-5562	"Celal Konor"
P8TN8K-5561	rabel
P92YZG-5562	Celal Konor
PZ7VVK-5561	Celal Konor
Q7RBYH-5562	Celal Konor
QAQLVH-5561	Celal Konor
QFHW6F-5561	Celal Konor
QZQWEG-5561	Celal Konor
R7BE8H-5562	Celal Konor
TANE4A-5561	Celal Konor
TEV68F-5561	Celal Konor
TXBE8F-5561	Celal Konor
U3ZBAC-5562	Celal Konor
VBBWX7-5562	Celal Konor
VZACVE-5562	Celal Konor
W2ZUC7-5562	The answer is Celal Konor. I have searched for the file name 004583.doc in Axiom forensics tool which provided the information of the file which has author as Celal Konor
WVD6QB-5561	Celal Konor
XGCTUC-5561	Celal Konor
Y78Z2B-5561	Celal Konor
YCA984-5562	Celal Konor
Z4WK8A-5562	Celal Konor
Z6A992-5561	Celal Konor

Question 35: Who is the Author of 004583.doc?

TABLE 1

Question 35 - Document Metadata Analysis

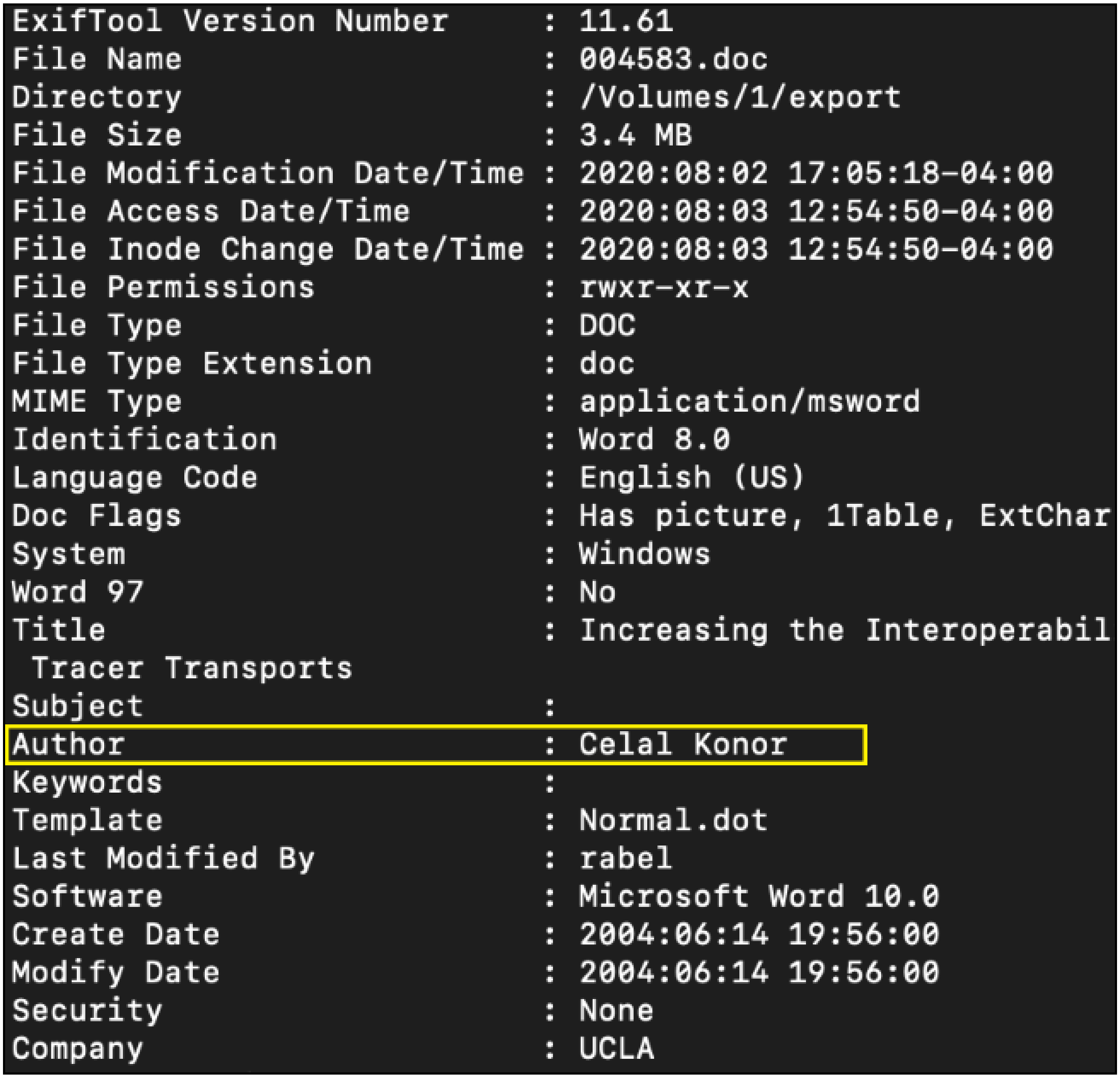
Consensus Result: Celal Konor

Expected Response Explanation:

Parsing the metadata from 004583.doc indicates the author as “Celal Konor”. Windows Explorer can also parse this data.

Expected Response Illustration:

Metadata:

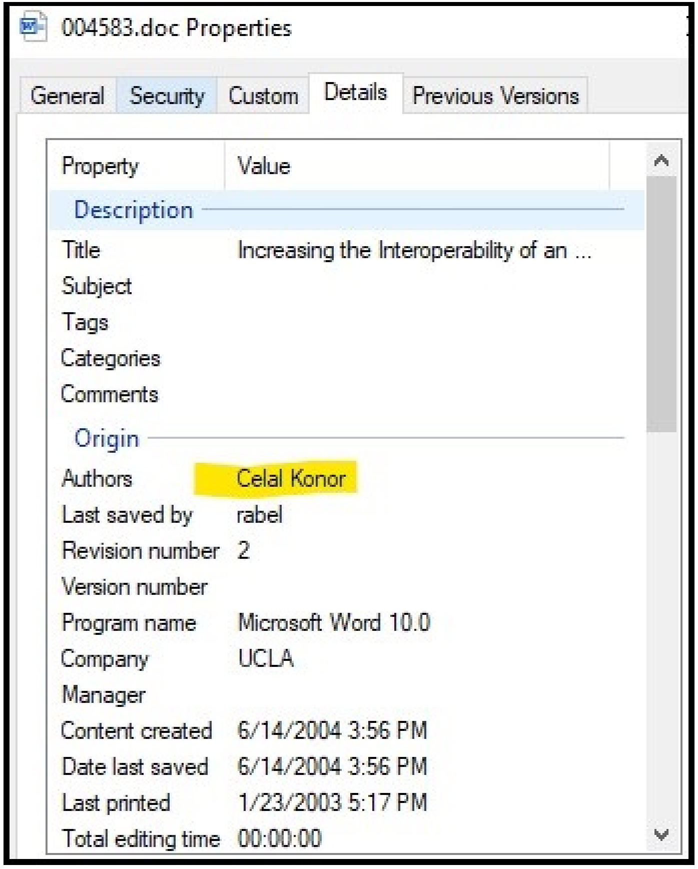


```
ExifTool Version Number         : 11.61
File Name                       : 004583.doc
Directory                       : /Volumes/1/export
File Size                       : 3.4 MB
File Modification Date/Time     : 2020:08:02 17:05:18-04:00
File Access Date/Time           : 2020:08:03 12:54:50-04:00
File Inode Change Date/Time     : 2020:08:03 12:54:50-04:00
File Permissions                : rwxr-xr-x
File Type                       : DOC
File Type Extension             : doc
MIME Type                       : application/msword
Identification                  : Word 8.0
Language Code                   : English (US)
Doc Flags                       : Has picture, 1Table, ExtChar
System                          : Windows
Word 97                         : No
Title                           : Increasing the Interoperabil
 Tracer Transports
Subject                         :
Author                          : Celal Konor
Keywords                        :
Template                        : Normal.dot
Last Modified By                : rabel
Software                        : Microsoft Word 10.0
Create Date                     : 2004:06:14 19:56:00
Modify Date                     : 2004:06:14 19:56:00
Security                        : None
Company                         : UCLA
```

TABLE 1

Question 35 - Document Metadata Analysis

Windows Explorer:



004583.doc Properties

Property	Value
Description	
Title	Increasing the Interoperability of an ...
Subject	
Tags	
Categories	
Comments	
Origin	
Authors	Celal Konor
Last saved by	rabel
Revision number	2
Version number	
Program name	Microsoft Word 10.0
Company	UCLA
Manager	
Content created	6/14/2004 3:56 PM
Date last saved	6/14/2004 3:56 PM
Last printed	1/23/2003 5:17 PM
Total editing time	00:00:00

TABLE 1

Question 36 - Keyword / Expression Searching

Question 36: What is the name of the file that contains the word "ohtaguchi"?

Manufacturer's Expected Response: 003555.txt

WebCode-Test	Response
2ZQE6A-5561	003555.text
4XFB84-5561	003555.txt
64W7NX-5562	003555.text
6U9F26-5561	003555.text
6ZF77W-5562	003555.text
7K2ZUX-5562	003555.txt
7M9E24-5561	003555.text
8Q3VR3-5562	003555.text
9ENXLY-5561	003555.text
ABKKEY-5561	003555.text
AQCK6Y-5561	003555.text
BJTE9R-5562	003555.text
C8D7KQ-5561	003555.text
CCTE9P-5562	003555.text
CKXLNP-5561	003555.text
CPXWKP-5562	003555.text
DGFL7P-5562	003555.txt
DX4YHV-5561	003555.text
EQHHC7-5562	003555.txt
ETQDAP-5562	003555.text
HG3KCP-5561	003555.text
HHBXTQ-5562	\Users\james\Documents\003555.text
J6MAYJ-5561	003555.text
KH3VVH-5562	003555.text

TABLE 1

Question 36 - Keyword / Expression Searching

WebCode-Test	Response
MTJYGM-5562	003555.text
NF4QTK-5562	003555.text
NZEF7H-5561	003555.text
P6M4JK-5562	003555.text
P8TN8K-5561	003555.text
P92YZG-5562	003555.text
PZ7VVK-5561	003555.text
Q7RBYH-5562	003555.text
QAQLVH-5561	003555.text
QFHW6F-5561	003555.text
QZQWEG-5561	003555.text
R7BE8H-5562	003555.text
TANE4A-5561	003555.text
TEV68F-5561	003555.text
TXBE8F-5561	003555.TEXT
U3ZBAC-5562	003555.text
VBBWX7-5562	003555.text
VZACVE-5562	003555.text
W2ZUC7-5562	The answer is 003555.text. I have search in Axiom with the word 'ohtaguchi' which provided the result of the file name as 003555.text
WVD6QB-5561	003555.text
XGCTUC-5561	003555.text
Y78Z2B-5561	003555.text
YCA984-5562	003555.text
Z4WK8A-5562	003555.text
Z6A992-5561	003555.text

Question 36: What is the name of the file that contains the word "ohtaguchi"?

TABLE 1

Question 36 - Keyword / Expression Searching

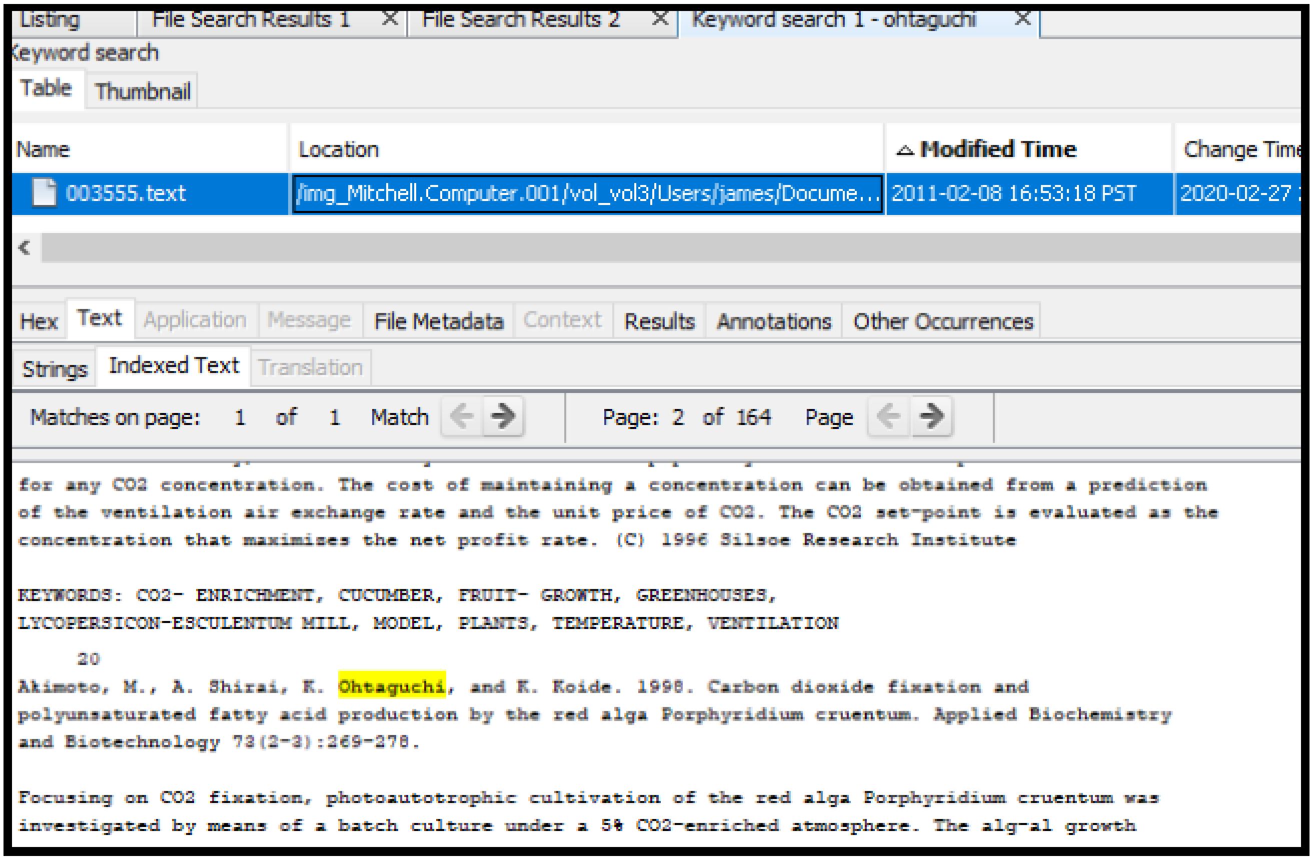
Consensus Result: 003555.text and 003555.txt

Expected Response Explanation:

A simple keyword search will find the file where this word is located, C:\Users\james\Documents\003555.txt.

Expected Response Illustration:

Keyword Search:



Name	Location	Modified Time	Change Time
003555.text	/img_Mitchell.Computer.001/vol_vol3/Users/james/Docume…	2011-02-08 16:53:18 PST	2020-02-27

Matches on page: 1 of 1 Match Page: 2 of 164 Page

```
for any CO2 concentration. The cost of maintaining a concentration can be obtained from a prediction
of the ventilation air exchange rate and the unit price of CO2. The CO2 set-point is evaluated as the
concentration that maximizes the net profit rate. (C) 1996 Silsoe Research Institute

KEYWORDS: CO2- ENRICHMENT, CUCUMBER, FRUIT- GROWTH, GREENHOUSES,
LYCOPERSICON-ESCULENTUM MILL, MODEL, PLANTS, TEMPERATURE, VENTILATION

    20
Akimoto, M., A. Shirai, K. Ohtaguchi, and K. Koide. 1998. Carbon dioxide fixation and
polyunsaturated fatty acid production by the red alga Porphyridium cruentum. Applied Biochemistry
and Biotechnology 73(2-3):269-278.

Focusing on CO2 fixation, photoautotrophic cultivation of the red alga Porphyridium cruentum was
investigated by means of a batch culture under a 5% CO2-enriched atmosphere. The alg-al growth
```

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 37 - Keyword / Expression Searching

Question 37: Provide the name of the (active) file containing the word "playmoney" where the letters a,o,e have been replaced with arbitrary characters.

Manufacturer's Expected Response: lorem.text

WebCode-Test	Response
2ZQE6A-5561	lorem.text
4XFB84-5561	lorem.txt
64W7NX-5562	lorem.text
6U9F26-5561	lorem.text
6ZF77W-5562	lorem.text
7K2ZUX-5562	March 2008 E-audiobook Titles and Authors
7M9E24-5561	Lorem.text
8Q3VR3-5562	lorem.text
9ENXLY-5561	Lorem.text
ABKKEY-5561	lorem.text
AQCK6Y-5561	lorem.text
BJTE9R-5562	lorem.text
C8D7KQ-5561	[Participant did not return results for this question.]
CCTE9P-5562	lorem.text
CKXLNP-5561	lorem.text
CPXWKP-5562	Lorem.text
DGFL7P-5562	The file lorem.txt contained a variation spelling of "playmoney" spelled pl@ym0n3y located in C:\Users\james\Documents\lorem.txt
DX4YHV-5561	lorem.text
EQHHC7-5562	Lorem.text
ETQDAP-5562	lorem.text
HG3KCP-5561	lorem.text
HHBXTQ-5562	\Users\james\Documents\lorem.text
J6MAYJ-5561	lorem.text

TABLE 1

Question 37 - Keyword / Expression Searching

WebCode-Test	Response
KH3VVH-5562	lorem.text
MTJYGM-5562	lorem.text
NF4QTK-5562	lorem.text
NZEF7H-5561	lorem.text
P6M4JK-5562	lorem.text
P8TN8K-5561	lorem.text
P92YZG-5562	lorem.text
PZ7VVK-5561	lorem.txt
Q7RBYH-5562	lorem.text
QAQLVH-5561	lorem.text
QFHW6F-5561	lorem.text
QZQWEG-5561	lorem.text
R7BE8H-5562	lorem.text
TANE4A-5561	pagefile.sys
TEV68F-5561	lorem.text
TXBE8F-5561	lorem.text
U3ZBAC-5562	lorem. Text
VBBWX7-5562	lorem.txt
VZACVE-5562	lorem.text
W2ZUC7-5562	The answer is lorem.text. Using Axiom forensics tool, we are able to search using regex (as \bpl.ym.n.y\b) and got the result as lorem.text
WVD6QB-5561	lorem.text
XGCTUC-5561	lorem.text
Y78Z2B-5561	lorem.text
YCA984-5562	lorem.text
Z4WK8A-5562	lorem.text
Z6A992-5561	lorem.text

TABLE 1

Question 37 - Keyword / Expression Searching

Question 37: Provide the name of the (active) file containing the word "playmoney" where the letters a,o,e have been replaced with arbitrary characters.

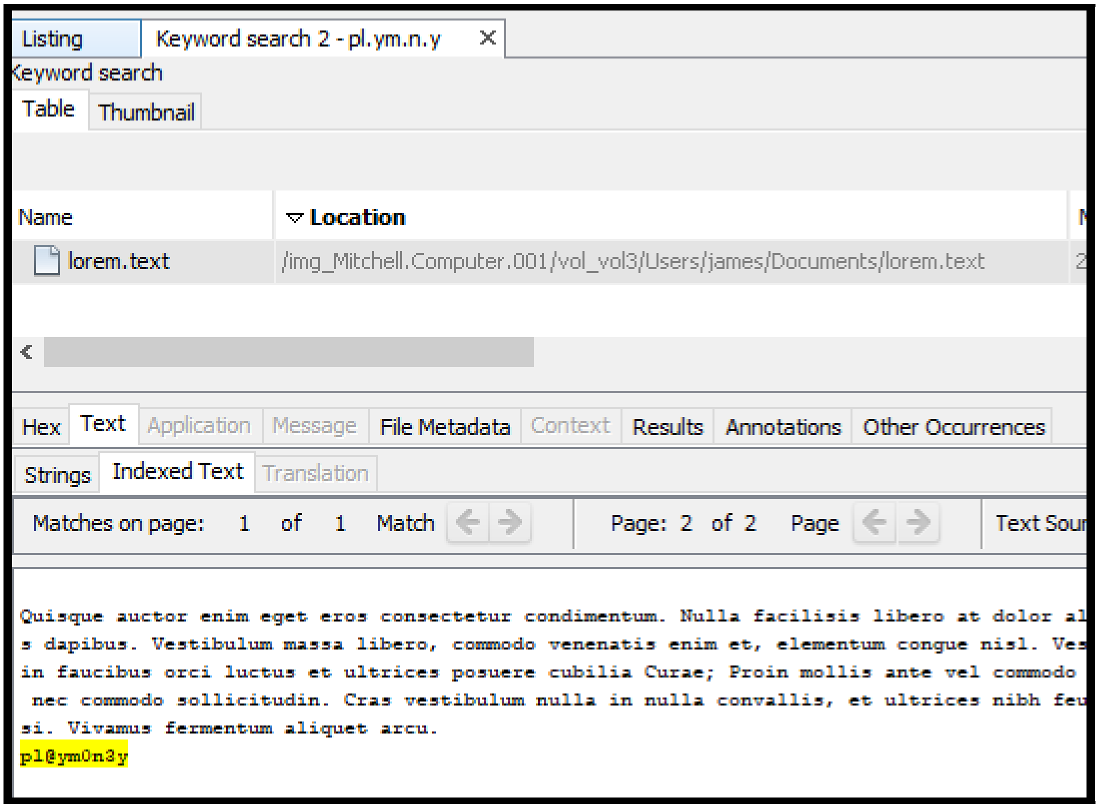
Consensus Result: lorem.text

Expected Response Explanation:

A regular expression built by replacing a, o, and e, with the wildcard ".", i.e. "pl.ym.n.y" will hit on the targeted term in C:\Users\james\Documents\lorem.text.

Expected Response Illustration:

Keyword Search:



Name	Location
lorem.text	/img_Mitchell.Computer.001/vol_vol3/Users/james/Documents/lorem.text

Matches on page: 1 of 1 Match

Page: 2 of 2 Page

```
Quisque auctor enim eget eros consectetur condimentum. Nulla facilisis libero at dolor al
s dapibus. Vestibulum massa libero, commodo venenatis enim et, elementum congue nisl. Ves
in faucibus orci luctus et ultrices posuere cubilia Curae; Proin mollis ante vel commodo
 nec commodo sollicitudin. Cras vestibulum nulla in nulla convallis, et ultrices nibh feu
si. Vivamus fermentum aliquet arcu.
pl@ym0n3y
```

TABLE 1

Question 38 - Keyword / Expression Searching

Question 38: What is the literal spelling of the word found in Question #37?

Manufacturer's Expected Response: pl@ym0n3y

WebCode-Test	Response
2ZQE6A-5561	pl@ym0n3y
4XFB84-5561	pl@ym0n3y
64W7NX-5562	pl@ym0n3y
6U9F26-5561	pl@ym0n3y
6ZF77W-5562	pl@ym0n3y
7K2ZUX-5562	Play money
7M9E24-5561	pl@ym0n3y
8Q3VR3-5562	pl@ym0n3y
9ENXLY-5561	pl@ym0n3y
ABKKEY-5561	pl@ym0n3y
AQCK6Y-5561	pl@ym0n3y
BJTE9R-5562	pl@ym0n3y
C8D7KQ-5561	[Participant did not return results for this question.]
CCTE9P-5562	pl@ym0n3y
CKXLNP-5561	pl@ym0n3y
CPXWKP-5562	pl@ym0n3y
DGFL7P-5562	pl@ym0n3y
DX4YHV-5561	pl@ym0n3y
EQHHC7-5562	pl@ym0n3y
ETQDAP-5562	pl@ym0n3y
HG3KCP-5561	pl@ym0n3y
HHBXTQ-5562	pl@ym0n3y
J6MAYJ-5561	pl@ym0n3y
KH3VVH-5562	pl@ym0n3y

TABLE 1

Question 38 - Keyword / Expression Searching

WebCode-Test	Response
MTJYGM-5562	pl@ym0n3y
NF4QTK-5562	pl@ym0n3y
NZEF7H-5561	pl@ym0n3y
P6M4JK-5562	pl@ym0n3y
P8TN8K-5561	pl@ym0n3y
P92YZG-5562	pl@ym0n3y
PZ7VVK-5561	pl@ym0n3y
Q7RBYH-5562	pl@ym0n3y
QAQLVH-5561	pl@ym0n3y
QFHW6F-5561	pl@ym0n3y
QZQWEG-5561	pl@ym0n3y
R7BE8H-5562	pl@ym0ney
TANE4A-5561	playMiniY
TEV68F-5561	pl@ym0n3y
TXBE8F-5561	pl@ym0n3y
U3ZBAC-5562	pl@ym0n3y
VBBWX7-5562	pl@ym0n3y
VZACVE-5562	pl@ym0n3y
W2ZUC7-5562	The answer is 'pl@ym0n3y'. Using Axiom forensics tool, we are able to search using the regex (as \bpl.ym.n.y\b) and got the answer of question 37 as lorem.text. In that file we see the word as pl@ym0n3y.
WVD6QB-5561	pl@ym0n3y
XGCTUC-5561	pl@ym0n3y
Y78Z2B-5561	pl@ym0n3y
YCA984-5562	pl@ym0n3y
Z4WK8A-5562	pl@ym0n3y
Z6A992-5561	pl@ym0n3y

Question 38: What is the literal spelling of the word found in Question #37?

TABLE 1

Question 38 - Keyword / Expression Searching

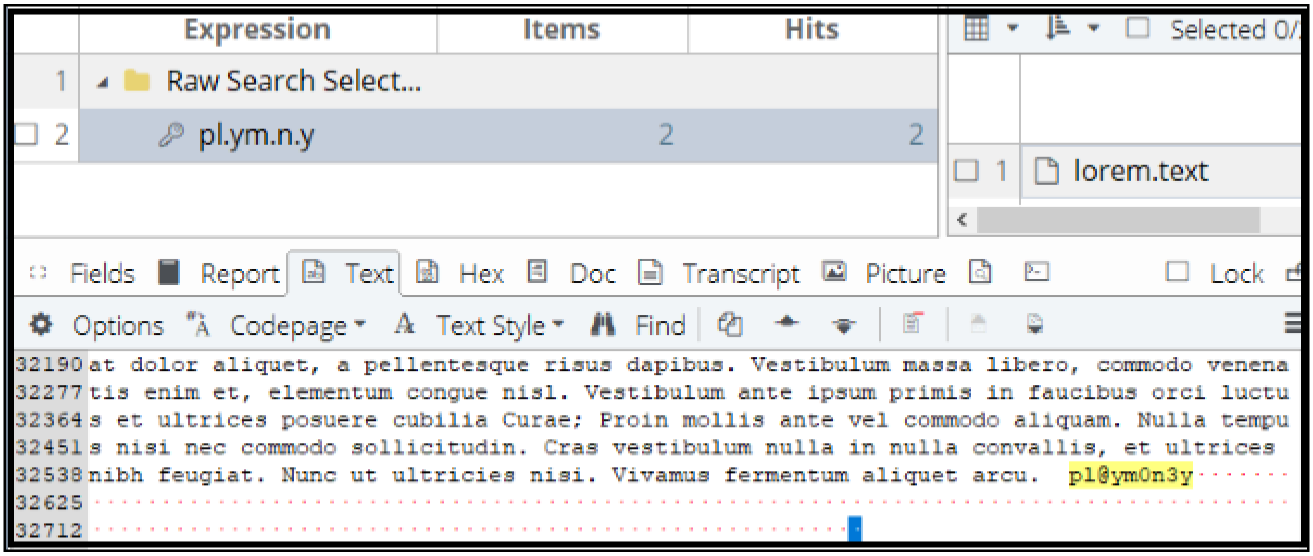
Consensus Result: pl@ym0n3y

Expected Response Explanation:

A regular expression built by replacing a, o, and e, with the wildcard ".", i.e. "pl.ym.n.y" will hit on the targeted term in C:\Users\james\Documents\lorem.text.

Expected Response Illustration:

Contents of lorem.txt showing highlighted keyword:



	Expression	Items	Hits
1	Raw Search Select...		
□ 2	pl.ym.n.y	2	2

□ 1	lorem.text

```
32190 at dolor aliquet, a pellentesque risus dapibus. Vestibulum massa libero, commodo venena
32277 tis enim et, elementum congue nisl. Vestibulum ante ipsum primis in faucibus orci luctu
32364 s et ultrices posuere cubilia Curae; Proin mollis ante vel commodo aliquam. Nulla tempu
32451 s nisi nec commodo sollicitudin. Cras vestibulum nulla in nulla convallis, et ultrices
32538 nibh feugiat. Nunc ut ultricies nisi. Vivamus fermentum aliquet arcu.  pl@ym0n3y······
32625 ········································································
32712 ·······························································
```

TABLE 1

Question 39 - Removable Media 20-5562

Question 39: What is the SHA-256 hash for the device?

Manufacturer's Expected Response: 2b1fb19de0da5f1358437c4be80a6e0f01fbbe8a6ada79b0ae24473c8e8b44fd

WebCode-Test	Response	** Inconsistencies not highlighted; No consensus achieved **
64W7NX-5562	2b1fb19de0da5f1358437c4be80a6e0f01fbbe8a6ada79b0ae24	
6ZF77W-5562	2b1fb19de0da5f1358437c4be80a6e0f01fbbe8a6ada79b0ae24473c8e8b44fd	
7K2ZUX-5562	6E9D7B35C3E12A3C17B55B6E9F13629C95B25D0DBA7FD26C9BAEA698D505E771	
8Q3VR3-5562	2B1FB19DE0DA5F1358437C4BE80A6E0F01FBBE8A6ADA79B0AE24473C8E8B44FD	
BJTE9R-5562	2B1FB19DE0DA5F1358437C4BE80A6E0F01FBBE8A6ADA79B0AE24473C8E8B44FD	
CCTE9P-5562	293e7f3b3f68a76df4d6df5cc8375dd1e0586987db5efcc7b8f65d7131c40424	
CPXWKP-5562	2b1fb19de0da5f1358437c4be80a6e0f01fbbe8a6ada79b0ae24473c8e8b44fd	
DGFL7P-5562	The usb drive was connected to the Tableau Forensic write blocker and hash was calculated using FEX Imager the SHA-256 was 2b1fb19de0da5f1358437c4be80a6e0f01fbbe8a6ada79b0ae24473c8e8b44fd. A raw dd image was created using FEX Imager. The raw image hash after the imaging completed was 2b1fb19de0da5f1358437c4be80a6e0f01fbbe8a6ada79b0ae24473c8e8b44fd which matched the calculated hash of the original evidence thus the integrity of the original evidence was maintained and no data was changed.	
EQHHC7-5562	2B1FB19DE0DA5F1358437C4BE80A6E0F01FBBE8A6ADA79B0AE24473C8E8B44FD	
ETQDAP-5562	2B1FB19DE0DA5F1358437C4BE80A6E0F01FBBE8A6ADA79B0AE24473C8E8B44FD	
HHBXTQ-5562	2b1fb19de0da5f1358437c4be80a6e0f01fbbe8a6ada79b0ae24473c8e8b44fd	
KH3VVH-5562	2B1FB19DE0DA5F1358437C4BE80A6E0F01FBBE8A6ADA79B0AE24473C8E8B44FD	
MTJYGM-5562	2B1FB19DE0DA5F1358437C4BE80A6E0F01FBBE8A6ADA79B0AE24473C8E8B44FD	
NF4QTK-5562	2B1FB19DE0DA5F1358437C4BE80A6E0F01FBBE8A6ADA79B0AE24473C8E8B44FD	
P6M4JK-5562	2b1fb19de0da5f1358437c4be80a6e0f01fbbe8a6ada79b0ae24473c8e8b44fd	
P92YZG-5562	2b1fb19de0da5f1358437c4be80a6e0f01fbbe8a6ada79b0ae24473c8e8b44fd	
Q7RBYH-5562	2a0f39123b4c19c1ab198ab0636bbeb829649e4d	
R7BE8H-5562	2a0f39123b4c19c1ab198ab0636bbeb829649e4d	
U3ZBAC-5562	8C1EA70677CC28105702EE576B27D3DC321661B45A3C3B2A3219E974F7BBB785	
VBBWX7-5562	2b1fb19de0da5f1358437c4be80a6e0f01fbbe8a6ada79b0ae24473c8e8b44fd	
VZACVE-5562	2b1fb19de0da5f1358437c4be80a6e0f01fbbe8a6ada79b0ae24473c8e8b44fd	
W2ZUC7-5562	The answer is 7c49e65e0a7adba24b989d8f4ab8877cb157d68833781e2cca30d2b69dd81dbb. I have used write blocker and mounted the USB evidence. Then I have imaged the USB evidence and calculated the SHA256 hash using the hashmyfiles tool.	

TABLE 1

Question 39 - Removable Media 20-5562

WebCode-Test	Response ** Inconsistencies not highlighted; No consensus achieved **
YCA984-5562	2B1FB19DE0DA5F1358437C4BE80A6E0F01FBBE8A6ADA79B0AE24473C8E8B44FD
Z4WK8A-5562	2B1FB19DE0DA5F1358437C4BE80A6E0F01FBBE8A6ADA79B0AE24473C8E8B44FD

Question 39: What is the SHA-256 hash for the device?

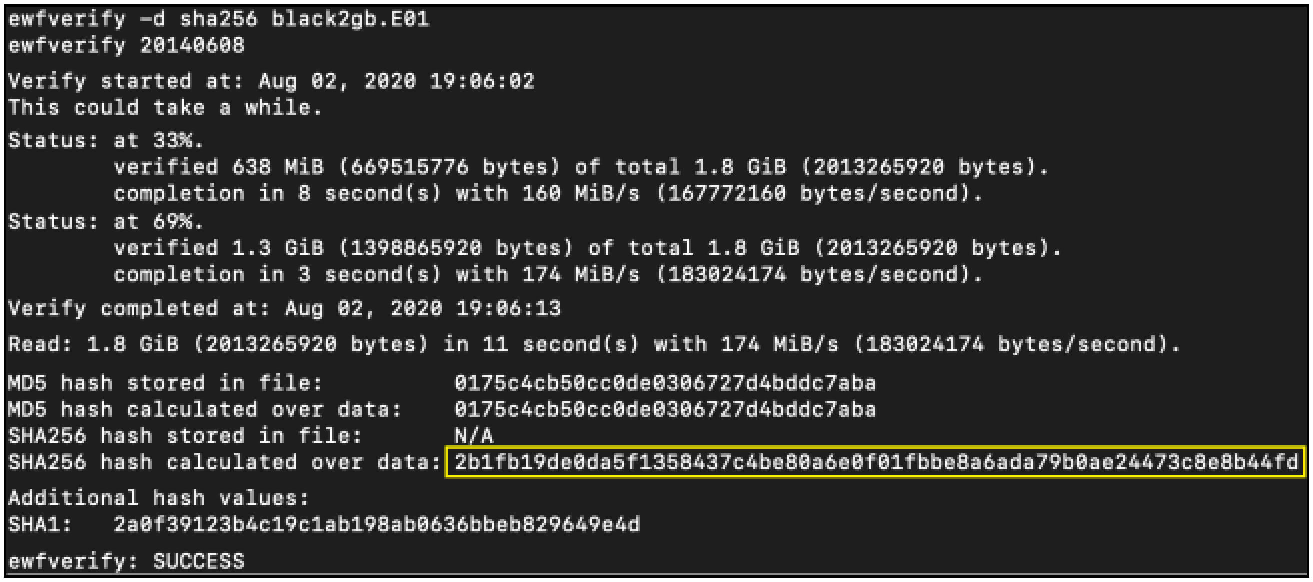
Consensus Result: A consensus was not achieved. Only 71% of participants reported the expected response. The objective was to run a hashing algorithm on the USB device.

Expected Response Explanation:

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

Expected Response Illustration:

Hashing Algorithm:



```
ewfverify -d sha256 black2gb.E01
ewfverify 20140608

Verify started at: Aug 02, 2020 19:06:02
This could take a while.

Status: at 33%.
        verified 638 MiB (669515776 bytes) of total 1.8 GiB (2013265920 bytes).
        completion in 8 second(s) with 160 MiB/s (167772160 bytes/second).
Status: at 69%.
        verified 1.3 GiB (1398865920 bytes) of total 1.8 GiB (2013265920 bytes).
        completion in 3 second(s) with 174 MiB/s (183024174 bytes/second).

Verify completed at: Aug 02, 2020 19:06:13

Read: 1.8 GiB (2013265920 bytes) in 11 second(s) with 174 MiB/s (183024174 bytes/second).

MD5 hash stored in file:          0175c4cb50cc0de0306727d4bddc7aba
MD5 hash calculated over data:    0175c4cb50cc0de0306727d4bddc7aba
SHA256 hash stored in file:       N/A
SHA256 hash calculated over data: 2b1fb19de0da5f1358437c4be80a6e0f01fbbe8a6ada79b0ae24473c8e8b44fd

Additional hash values:
SHA1:   2a0f39123b4c19c1ab198ab0636bbeb829649e4d

ewfverify: SUCCESS
```

TABLE 1

Question 40 - Removable Media 20-5562

Question 40: How many partitions are on the device? Provide a NUMERIC response (e.g. 1, 2, 3).

Manufacturer's Expected Response: 1

WebCode-Test	Response
64W7NX-5562	1
6ZF77W-5562	1
7K2ZUX-5562	1
8Q3VR3-5562	1
BJTE9R-5562	1
CCTE9P-5562	1
CPXWKP-5562	1
DGFL7P-5562	1
EQHHC7-5562	1
ETQDAP-5562	1
HHBXTQ-5562	1
KH3VVH-5562	1
MTJYGM-5562	1
NF4QTK-5562	1
P6M4JK-5562	1
P92YZG-5562	1
Q7RBYH-5562	1
R7BE8H-5562	1
U3ZBAC-5562	1
VBBWX7-5562	1
VZACVE-5562	1
W2ZUC7-5562	The answer is 1. Once the USB evidence has been imaged, I have parsed it using Axiom forensics tool which provided the details of the partition.
YCA984-5562	1
Z4WK8A-5562	1

TABLE 1

Question 40 - Removable Media 20-5562

Question 40: How many partitions are on the device? Provide a NUMERIC response (e.g. 1, 2, 3).

Consensus Result: 1

Expected Response Explanation:

The number of device partitions can be determined by reviewing the partition table with most forensic suites or imaging tools. This drive is not partitioned (it has only one partition which includes the volume boot record and the filesystem).

Expected Response Illustration:

FTK Imager view of device information:

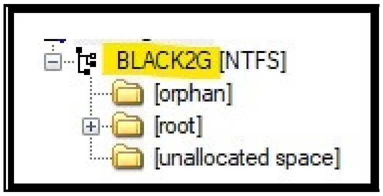


TABLE 1

Question 41 - Removable Media 20-5562

Question 41: What is the volume serial number?

Manufacturer's Expected Response: CA9F-D08C

WebCode-Test	Response
64W7NX-5562	38CAA018CA9FD08C
6ZF77W-5562	CA9F-D08C
7K2ZUX-5562	CA9F-D08C
8Q3VR3-5562	CA9F-D08C
BJTE9R-5562	CA9F-D08C
CCTE9P-5562	Volume Serial Number: CA9F-D08C Full Volume Serial Number: 38CAA018CA9FD08C
CPXWKP-5562	CA9F-D08C
DGFL7P-5562	CA9F-D08C
EQHHC7-5562	Volume Serial Number, CA9FD08C – Full Volume Serial number, 38CAA018CA9FD08C
ETQDAP-5562	Serial No.: 8CD09FCA (hex) Serial No.: CA9FD08C (hex, rev) Serial No.: 3399471244 (dec, rev)
HHBXTQ-5562	CA9FD08C
KH3VVH-5562	CA9F-D08C
MTJYGM-5562	0x8CD09FCA
NF4QTK-5562	CA9F-D08C
P6M4JK-5562	CA9F-D08C
P92YZG-5562	38CAA018CA9FD08C
Q7RBYH-5562	CA9F-D08C
R7BE8H-5562	CA9F-D08C
U3ZBAC-5562	CA9F-D08C
VBBWX7-5562	CA9F-D08C
VZACVE-5562	CA9F-D08C
W2ZUC7-5562	The volume serial number is CA9F-D08C, based on the 'File System Information' artifact in Axiom forensics tool.
YCA984-5562	CA9FD08C

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 41 - Removable Media 20-5562

WebCode-Test	Response
Z4WK8A-5562	CA9F-D08C

Question 41: What is the volume serial number?

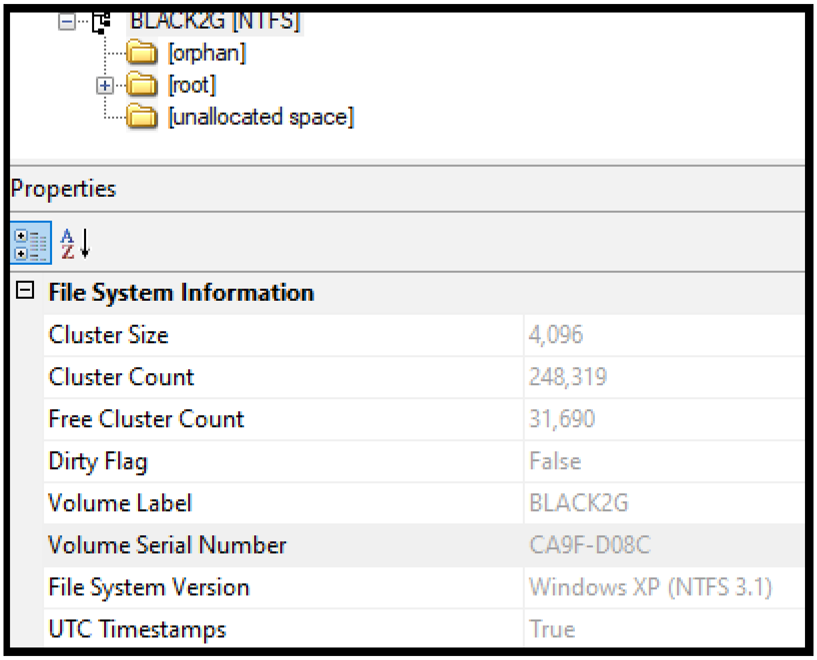
Consensus Result: CA9F-D08C and the full volume serial number of 38CAA018CA9FD08C was also accepted.

Expected Response Explanation:

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

Expected Response Illustration:

FTK Imager view of device information:



File System Information

Cluster Size	4,096
Cluster Count	248,319
Free Cluster Count	31,690
Dirty Flag	False
Volume Label	BLACK2G
Volume Serial Number	CA9F-D08C
File System Version	Windows XP (NTFS 3.1)
UTC Timestamps	True

TABLE 1

Question 42 - Removable Media 20-5562

Question 42: What is the name (Volume Label)?

Manufacturer's Expected Response: BLACK2G

WebCode-Test	Response
64W7NX-5562	BLACK2G
6ZF77W-5562	BLACK2G
7K2ZUX-5562	BLACK2G
8Q3VR3-5562	BLACK2G
BJTE9R-5562	BLACK2G
CCTE9P-5562	BLACK2G
CPXWKP-5562	BLACK2G
DGFL7P-5562	BLACK2G
EQHHC7-5562	4BLACK2G
ETQDAP-5562	BLACK2G
HHBXTQ-5562	BLACK2G
KH3VVH-5562	BLACK2G
MTJYGM-5562	BLACK2G
NF4QTK-5562	BLACK2G
P6M4JK-5562	Black2G
P92YZG-5562	BLACK2G
Q7RBYH-5562	BLACK2G
R7BE8H-5562	BLACK2G
U3ZBAC-5562	BLACK2G
VBBWX7-5562	BLACK2G
VZACVE-5562	BLACK2G
W2ZUC7-5562	The answer is BLACK2G, based on the 'File System Information' artifact in Axiom forensics tool.
YCA984-5562	BLACK2G
Z4WK8A-5562	BLACK2G

TABLE 1

Question 42 - Removable Media 20-5562

Question 42: What is the name (Volume Label)?

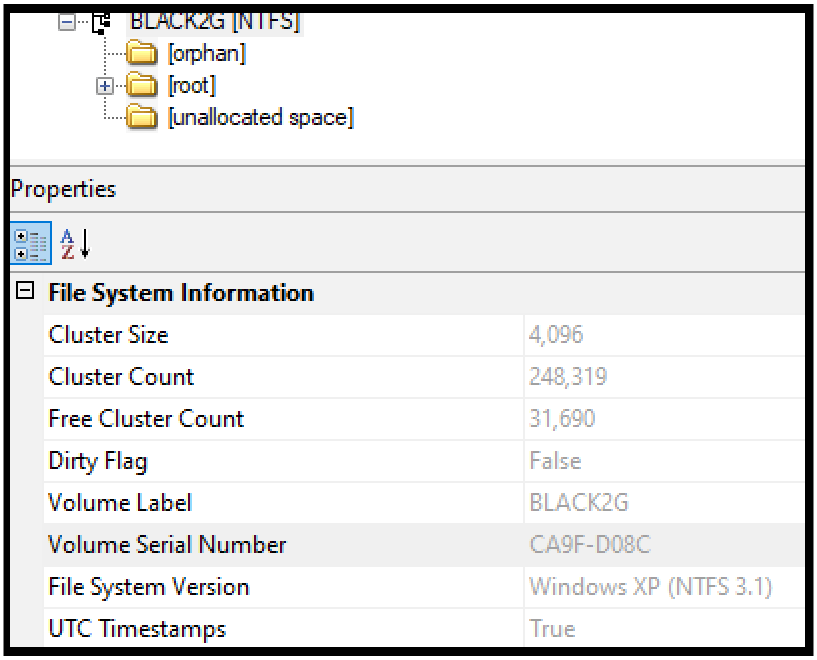
Consensus Result: BLACK2G

Expected Response Explanation:

Most forensic tools will parse and display the volume label value. It can also be listed by the operating system for a mounted drive.

Expected Response Illustration:

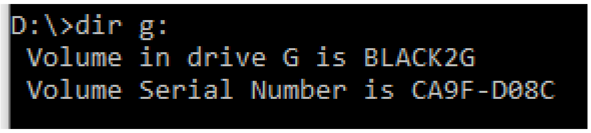
FTK Imager view of device information:



File System Information

Cluster Size	4,096
Cluster Count	248,319
Free Cluster Count	31,690
Dirty Flag	False
Volume Label	BLACK2G
Volume Serial Number	CA9F-D08C
File System Version	Windows XP (NTFS 3.1)
UTC Timestamps	True

Windows Cmd view of volume information:



```
D:\>dir g:
 Volume in drive G is BLACK2G
 Volume Serial Number is CA9F-D08C
```

TABLE 1

Question 43 - Removable Media 20-5562

Question 43: What is the file system (include version) for this device?

Manufacturer's Expected Response: NTFS 3.1

WebCode-Test	Response
64W7NX-5562	Microsoft NTFS
6ZF77W-5562	NTFS version 3.1
7K2ZUX-5562	NTFS version 3.1. x
8Q3VR3-5562	NTFS 3.1
BJTE9R-5562	NTFS 3.1
CCTE9P-5562	Microsoft NTFS
CPXWKP-5562	NTFS 3.1

DGFL7P-5562	The filesystem is NTFS version 3.1. The forensic image was mounted read only in FTK Imager as logical drive F: and the following command was ran fsutil fsinfo ntfsinfo F:
	C:\WINDOWS\system32>fsutil fsinfo ntfsinfo F:
	NTFS Volume Serial Number : 0x38caa018ca9fd08c; NTFS Version: 3.1; LFS Version: 1.1; Total Sectors: 1,986,559 (970.0 MB); Total Clusters: 248,319 (970.0 MB); Free Clusters: 28,991 (113.2 MB); Total Reserved Clusters : 0 (0.0 KB); Reserved For Storage Reserve : 0 (0.0 KB); Bytes Per Sector: 512; Bytes Per Physical Sector : 512; Bytes Per Cluster : 4096; Bytes Per FileRecord Segment: 1024; Clusters Per FileRecord Segment : 0; Mft Valid Data Length : 3.75 MB; Mft Start Lcn : 0x0000000000014355; Mft2 Start Lcn : 0x0000000000000002; Mft Zone Start : 0x0000000000000000; Mft Zone End : 0x0000000000000000; MFT Zone Size : 0.00 KB; Max Device Trim Extent Count : 0;
	Max Device Trim Byte Count : 0; Max Volume Trim Extent Count : 62; Max Volume Trim Byte Count : 0x40000000;

EQHHC7-5562	Microsoft NTFS
ETQDAP-5562	NTFS 3.1
HHBXTQ-5562	NTFS 3.1
KH3VVH-5562	NTFS 3.1
MTJYGM-5562	NTFS version: 3.1
NF4QTK-5562	NTFS
P6M4JK-5562	NTFS 3.1
P92YZG-5562	NTFS – version 3.1
Q7RBYH-5562	Windows XP (NTFS 3.1)
R7BE8H-5562	Microsoft NTFS [Drivers Information NTFS 3.1 (80)]
U3ZBAC-5562	NTFS 3.1

TABLE 1

Question 43 - Removable Media 20-5562

WebCode-Test	Response
VBBWX7-5562	NTFS version: 3.1
VZACVE-5562	Microsoft NTFS 3.1
W2ZUC7-5562	The answer is Microsoft NTFS 3.1 (version 3.1 since XP), based on the 'File System Information' artifact in Axiom forensics tool.
YCA984-5562	NTFS v3.1
Z4WK8A-5562	NTFS 3.1

Question 43: What is the file system (include version) for this device?

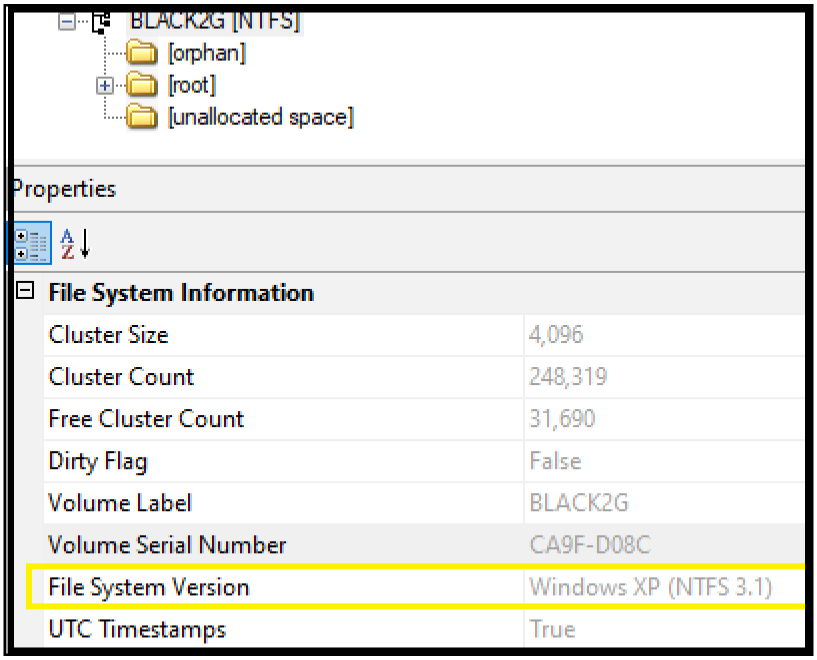
Consensus Result: NTFS 3.1. Four participants reported "NTFS" but neglected to include the version.

Expected Response Explanation:

The file system and version is parsed by some forensic tools and can be displayed by Windows for a mounted drive.

Expected Response Illustration:

FTK Imager view of volume information



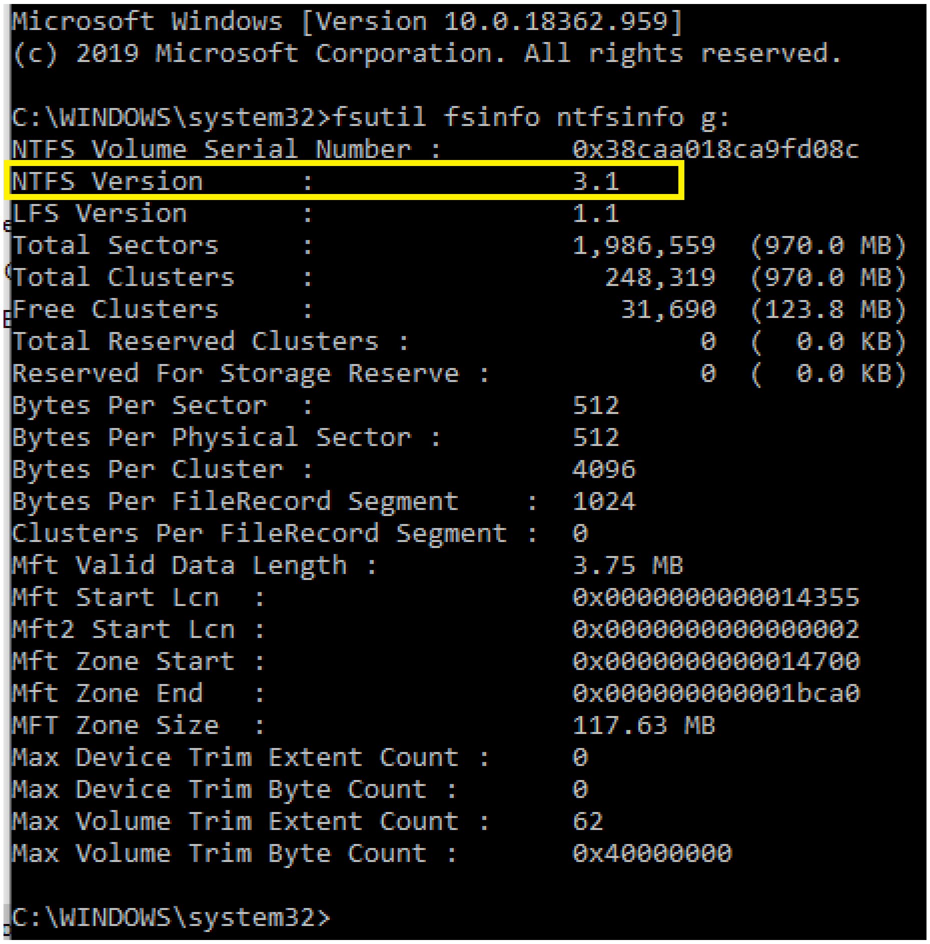
File System Information

Cluster Size	4,096
Cluster Count	248,319
Free Cluster Count	31,690
Dirty Flag	False
Volume Label	BLACK2G
Volume Serial Number	CA9F-D08C
File System Version	Windows XP (NTFS 3.1)
UTC Timestamps	True

TABLE 1

Question 43 - Removable Media 20-5562

Windows fsutil view of volume information:



```
Microsoft Windows [Version 10.0.18362.959]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>fsutil fsinfo ntfsinfo g:
NTFS Volume Serial Number :        0x38caa018ca9fd08c
NTFS Version      :                3.1
LFS Version       :                1.1
Total Sectors     :                1,986,559  (970.0 MB)
Total Clusters    :                  248,319  (970.0 MB)
Free Clusters     :                   31,690  (123.8 MB)
Total Reserved Clusters :                  0  (  0.0 KB)
Reserved For Storage Reserve :             0  (  0.0 KB)
Bytes Per Sector  :                512
Bytes Per Physical Sector :        512
Bytes Per Cluster :                4096
Bytes Per FileRecord Segment    :  1024
Clusters Per FileRecord Segment :  0
Mft Valid Data Length :            3.75 MB
Mft Start Lcn  :                   0x0000000000014355
Mft2 Start Lcn :                   0x0000000000000002
Mft Zone Start :                   0x0000000000014700
Mft Zone End   :                   0x000000000001bca0
MFT Zone Size  :                   117.63 MB
Max Device Trim Extent Count :     0
Max Device Trim Byte Count :       0
Max Volume Trim Extent Count :     62
Max Volume Trim Byte Count :       0x40000000

C:\WINDOWS\system32>
```

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 44 - Removable Media 20-5562

Question 44: What color is the animal in the file with SHA1 Hash b5fe34cd8d978d2e3c97835eb9128ad3c72edd9d?

Manufacturer's Expected Response: Black

WebCode-Test	Response
64W7NX-5562	Black
6ZF77W-5562	Black
7K2ZUX-5562	Black
8Q3VR3-5562	Black
BJTE9R-5562	Black
CCTE9P-5562	Black
CPXWKP-5562	Black
DGFL7P-5562	brown in the file called rur0b9lxe1k41.jpg
EQHHC7-5562	Black Cat
ETQDAP-5562	Black
HHBXTQ-5562	Black
KH3VVH-5562	black
MTJYGM-5562	black
NF4QTK-5562	black
P6M4JK-5562	black
P92YZG-5562	Black
Q7RBYH-5562	Black
R7BE8H-5562	Black (Cat)
U3ZBAC-5562	black
VBBWX7-5562	BLACK
VZACVE-5562	Black
W2ZUC7-5562	The colour of cat is black, i have searched in Axiom with the above SHA1 hash and got the picture file which has black cat.
YCA984-5562	Black

TABLE 1

Question 44 - Removable Media 20-5562

WebCode-Test	Response
Z4WK8A-5562	Black

Question 44: What color is the animal in the file with SHA1 Hash b5fe34cd8d978d2e3c97835eb9128ad3c72edd9d?

Consensus Result: Black

Expected Response Explanation:

Calculating SHA1 hashes for all files, sorting, and searching for the above value identifies C:\Users\james\Documents\Pictures\rur0b9lxe1k41.jpg, which contains the below image of a black cat.

Expected Response Illustration:

Image content:

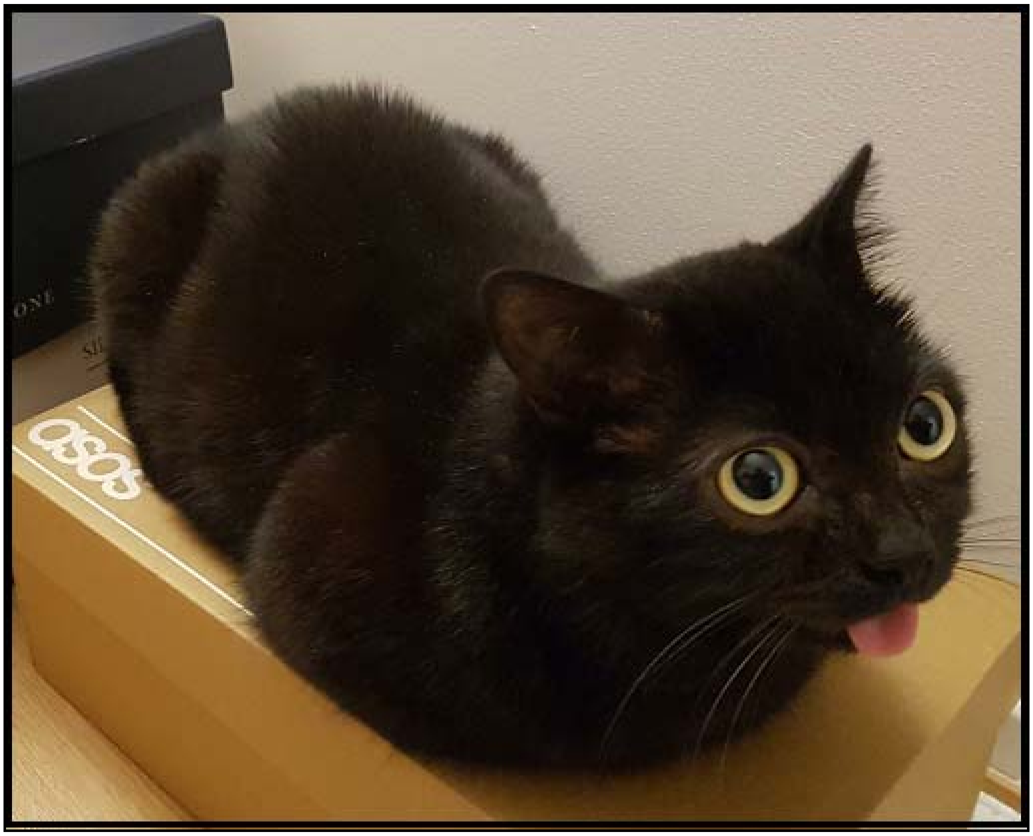


TABLE 1

Question 45 - Removable Media 20-5562

Question 45: What does the difference in creation and last written times indicate about the 4stq6uu5w4j41.jpg file?

Manufacturer's Expected Response: The creation date for this file is after the modified (last written date) meaning it was copied there from another volume.

WebCode-Test	Response
64W7NX-5562	The file was potentially created on another device and then 'copied' to this device.
6ZF77W-5562	It indicates that this file was created in some other place (in a computer) and then it was copied to the actual location.
7K2ZUX-5562	Changed MFT File record
8Q3VR3-5562	The file was created or edited on while stored on another physical storage device and then later copied to the flash drive.
BJTE9R-5562	File was copied to USB
CCTE9P-5562	the file 4stq6uu5w4j41.jpg was later opened on 3/1/2020 4:26:04 PM UTC.
CPXWKP-5562	The file was copied from another drive.
DGFL7P-5562	The file last modified time is 2/25/2020 8:59:31 PM is before the creation time 3/1/2020 4:26:28 PM which indicates the file was copied onto the thumb drive.
EQHHC7-5562	Modified is before created so potentially moved from another location.
ETQDAP-5562	This file was copied from another system.
HHBXTQ-5562	It suggests that the file was copied to the device on 3/1/20 from another device. The last written date of 2/25/20 quite possibly indicates that the creation date on the device from which the file was copied to the examined device was 2/25/20.
KH3VVH-5562	The 4stq6uu5w4j41.jpg file is a new file created by file-copying. Thus, the 4stq6uu5w4j41.jpg file preserves the last written time of its original file. However, the creation time was newly generated when its original file was copied to the location where the 4stq6uu5w4j41.jpg now exists.
MTJYGM-5562	The file was copied on the device from another one.
NF4QTK-5562	This file was created somewhere else, and copied over to this thumb drive.
P6M4JK-5562	The file create date and time was 2020-03-01 16:26:28 UTC and the file modification date and time was 2020-02-25 20:59:31 UTC. (Also, EXIF data for this image was corrupt, missing or never created.) The creation date/time indicates when it was created in its location and that this file was moved after its last written date/time.
P92YZG-5562	Likely copied to the USB from another device as Creation time is newer than Modified.
Q7RBYH-5562	File last written before it was created on this volume, indicates copied from another source.
R7BE8H-5562	That has been copied (creating a new file on creation date, but keeping the previous ones of last access and last writing)
U3ZBAC-5562	File was saved onto Thumb drive.
VBBWX7-5562	File was copied
VZACVE-5562	it was copied from another source and the modification was done prior the existence in this drive

TABLE 1

Question 45 - Removable Media 20-5562

WebCode-Test	Response
W2ZUC7-5562	This means that the file 4stq6uu5w4j41.jpg was copied to the USB. This is because when the picture got copied to the USB, the timestamp was captured as creation time as per the Windows time rules on the file system and it is NOT abnormal that the last written time is older than the creation time.
YCA984-5562	The file was copied from a different volume.
Z4WK8A-5562	The file was copied from the other device to this one.

Question 45: What does the difference in creation and last written times indicate about the 4stq6uu5w4j41.jpg file?

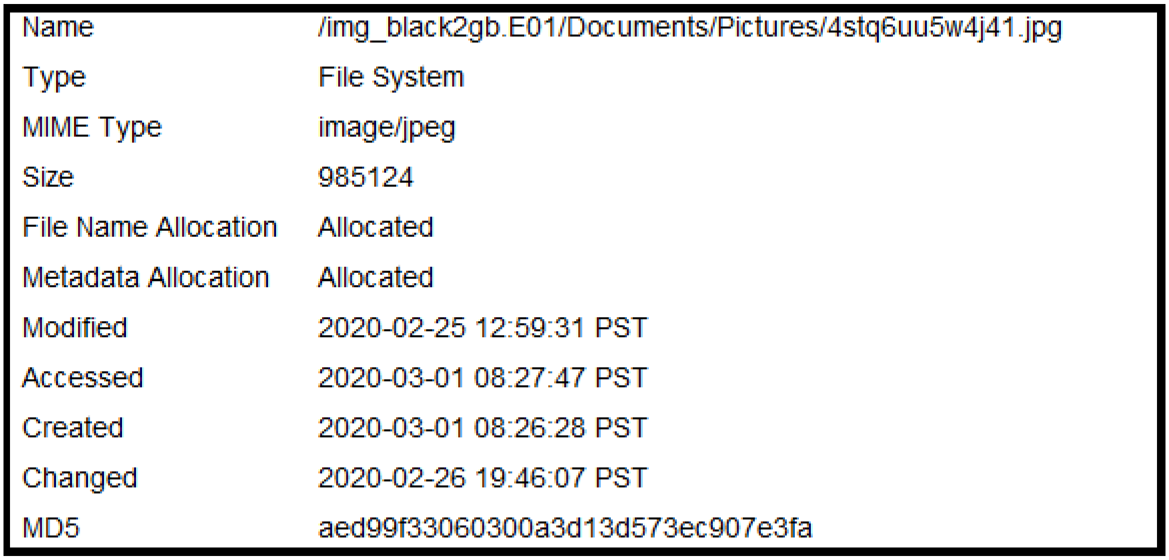
Consensus Result: The creation date for this file is after the modified date (last written date) meaning it was copied there from another volume.

Expected Response Explanation:

Having a creation date for a file that is after the modified date (last written date) indicates that the file was created in a different volume and then copied to this location.

Expected Response Illustration:

Autopsy view of 4stq6uu5w4j41.jpg metadata



Name	/img_black2gb.E01/Documents/Pictures/4stq6uu5w4j41.jpg
Type	File System
MIME Type	image/jpeg
Size	985124
File Name Allocation	Allocated
Metadata Allocation	Allocated
Modified	2020-02-25 12:59:31 PST
Accessed	2020-03-01 08:27:47 PST
Created	2020-03-01 08:26:28 PST
Changed	2020-02-26 19:46:07 PST
MD5	aed99f33060300a3d13d573ec907e3fa

TABLE 1

Question 46 - Removable Media 20-5562

Question 46: What is the name of the file with header 0x 00 00 00 01 42 75 64 31?

Manufacturer's Expected Response: .DS_Store

WebCode-Test	Response
64W7NX-5562	.DS_Store
6ZF77W-5562	.DS_Store
7K2ZUX-5562	.DS_Store
8Q3VR3-5562	.DS_Store
BJTE9R-5562	.DS_Store
CCTE9P-5562	.DS_Store
CPXWKP-5562	.DS_Store
DGFL7P-5562	Bud1
EQHHC7-5562	.DS_Store
ETQDAP-5562	.DS_Store
HHBXTQ-5562	\Documents\.DS_Store
KH3VVH-5562	.DS_Store
MTJYGM-5562	.DS_Store
NF4QTK-5562	.DS_Store
P6M4JK-5562	.DS_Store
P92YZG-5562	.DS_Store
Q7RBYH-5562	.DS_Store
R7BE8H-5562	.DS_Store
U3ZBAC-5562	.DS_Store
VBBWX7-5562	.DS_Store
VZACVE-5562	.Ds_store
W2ZUC7-5562	The answer is .DS_Store. Using Autopsy, we are able to search the hex pattern which matched with the file /Documents/.DS_Store.
YCA984-5562	.DS_Store
Z4WK8A-5562	.DS_Store

TABLE 1

Question 46 - Removable Media 20-5562

Question 46: What is the name of the file with header 0x 00 00 00 01 42 75 64 31?

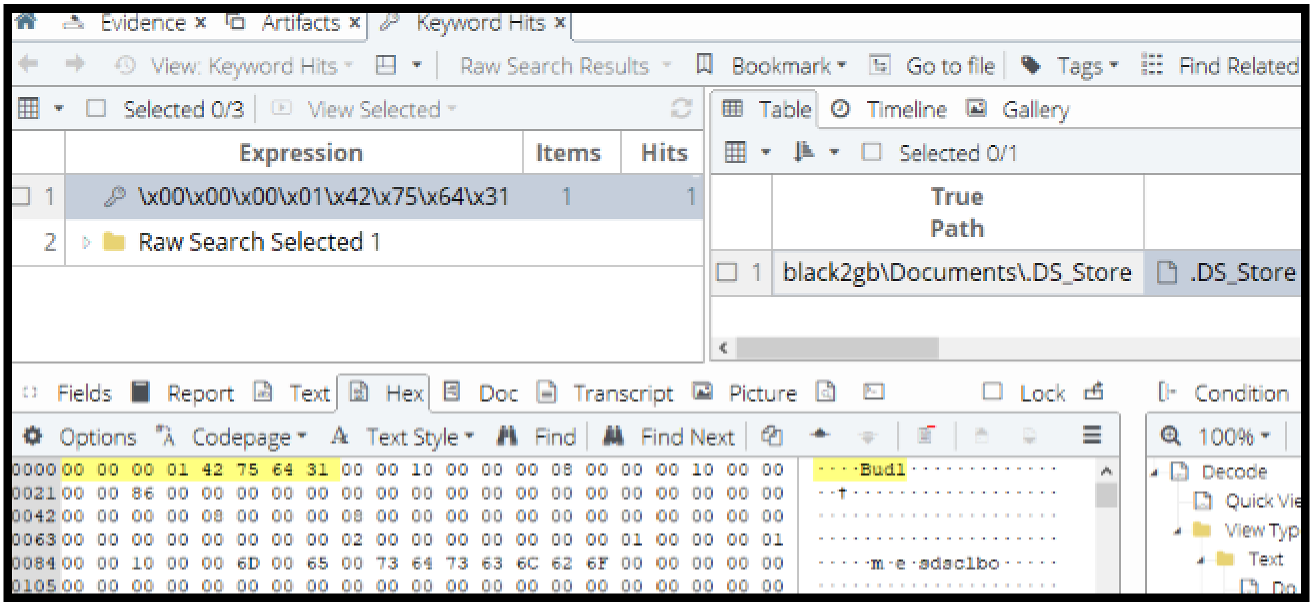
Consensus Result: .DS_Store

Expected Response Explanation:

This file is discovered using a keyword search for the hex value listed in the question. Converting the text header to ASCII and searching for that keyword (Bud1) will also discover \Documents\.DS_Store.

Expected Response Illustration:

Keyword Search:



	Expression	Items	Hits
☐ 1	\x00\x00\x00\x01\x42\x75\x64\x31	1	1
2	Raw Search Selected 1		

	True Path	
☐ 1	black2gb\Documents\.DS_Store	.DS_Store

```
0000 00 00 00 01 42 75 64 31 00 00 10 00 00 00 08 00 00 00 10 00 00   ····Bud1··············
0021 00 00 86 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ··†···················
0042 00 00 00 00 08 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00   ······················
0063 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 01   ······················
0084 00 00 10 00 00 6D 00 65 00 73 64 73 63 6C 62 6F 00 00 00 00 00   ·····m·e·sdsclbo······
0105 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ······················
```

TABLE 1

Question 47 - Removable Media 20-5562

Question 47: What does the presence of this file (file referenced in question #46) indicate?

Manufacturer's Expected Response: File created by OS X (Apple) (device was used in a Mac)

WebCode-Test	Response
64W7NX-5562	That a folder may have been copied from a Mac to this device.
6ZF77W-5562	.DS_Store is a metadata file, it indicates that the pendrive has been mounted and used in a MacOS operative system. The file is created by Finder.
7K2ZUX-5562	Removable media was attached to computer with the Mac Operating System.
8Q3VR3-5562	The flash drive had been inserted in an Apple computer and the volume had been mounted by the operating system of the Apple computer.
BJTE9R-5562	.DS_Store is a proprietary Mac/OSX system file that holds attributes/meta-data about the folder it resides in. The presence of this file indicate that the user may have copied it along with some data (which was originally created on a Mac/OSX file system).
CCTE9P-5562	The presence of .DS_Store file indicates that the USB was previously plugged in to MaC and used on it before connecting to a Windows machine. .DS_Store files are used by Mac OS X to store folder specific metadata information. They are created in every folder that Mac OS X Finder accesses, even network volumes and external devices. Folder level customizations are stored in the DS_Store file, things like custom icons, icon placement, icon size, window placement, list views, custom background pictures or colors, etc. DS_Store files are intended to be unobtrusive, which is why they have a . in front of their name, which indicates to UNIX file systems that the file is invisible.
CPXWKP-5562	The drive was connected to a computer running MacOS.
DGFL7P-5562	file referenced is .DS_Store which indicates the thumb drive may have been connected to a Apple computer
EQHHC7-5562	Plugged into a Mac at some point
ETQDAP-5562	It has been connected to the mac OS system.
HHBXTQ-5562	The presence of the \Documents\.DS_Store file suggests that the \Documents\ folder on the examined device was once accessed via Finder on a system running Mac OS X.
KH3VVH-5562	The presence of DS_STORE file can indicate that this USB storing .DS_Store has been inserted to a Mac OS X system. Mac OS X keeps track of custom attributes of the containing folder such as indexing, trash bins, folder positions etc. on every drive connected to a Mac OS X, by creating these files.
MTJYGM-5562	The device was connected to a macOS operating system
NF4QTK-5562	This USB was attached to an Apple Computer, and the Apple Computer also had software that allowed it to write to an NTFS partition.
P6M4JK-5562	.DS_Store files are theoretically created in every folder that Mac OS program “Finder” accesses. At some point in time (most likely at or before 2020-03-02 01:05:11 UTC), this flash drive was either plugged into a device running MAC OS X or this file was copied onto this flash drive (and the file was previously generated from another device running MAC OS X).
P92YZG-5562	It is likely the USB has been previously plugged into an Apple device.
Q7RBYH-5562	USB has been connected to a computer running Mac OSX operating system
R7BE8H-5562	On the MacOS system .DS_Store stores the custom attributes of the folder containing it. So, being on a Pendrive, which makes us think, that it has been on connected at some point on a macOS system
U3ZBAC-5562	Device was plugged into a Mac

TABLE 1

Question 47 - Removable Media 20-5562

WebCode-Test	Response
VBBWX7-5562	That the USB drive was connected at-least once to a machine running Apple Mac OS operating system.
VZACVE-5562	user file metadata are saved in this file.Metadata of the files in a folder are stored in this file.
W2ZUC7-5562	This USB evidence might be connected to a MAC machine earlier and so this file is created on the USB device. The .DS_Store (Desktop Services Store) is a file that stores custom attributes of its containing folder, such as the position of icons or the choice of a background image. It is created and maintained by the Finder application (MAC OS) in every folder, and has functions similar to the file desktop.ini in Microsoft Windows.
YCA984-5562	The folder containing ".DS_STORE" file was accessed from MAC operating system.
Z4WK8A-5562	This device was used on Mac OS.

Question 47: What does the presence of this file (file referenced in question #46) indicate?

Consensus Result: File created by OS X (Apple) (device was used in a Mac)

Expected Response Explanation:

The presence of .DS_Store files are created by macOS operating systems in directories of mounted volumes to store attributes of folders (directories).

TABLE 1

Question 48 - Removable Media 20-5562

Question 48: Who is the Author of 000124.doc?

Manufacturer's Expected Response: Becky Allee

WebCode-Test	Response
64W7NX-5562	Becky Allee
6ZF77W-5562	Becky Allee
7K2ZUX-5562	Becky Allee
8Q3VR3-5562	Becky Allee
BJTE9R-5562	Becky Allee
CCTE9P-5562	Becky Allee
CPXWKP-5562	Becky Allee
DGFL7P-5562	according to the metadata of the document the original author was Becky Allee and the last author was NOAA-CSC
EQHHC7-5562	Author - Becky Allee, Last Author - NOAA-CSC
ETQDAP-5562	Becky Allee
HHBXTQ-5562	Becky Allee
KH3VVH-5562	Becky Allee
MTJYGM-5562	Becky Allee
NF4QTK-5562	Becky Allee
P6M4JK-5562	"Becky Allee"
P92YZG-5562	Becky Allee
Q7RBYH-5562	Becky Allee
R7BE8H-5562	Author: Becky Allee last author: NOAA-CSC
U3ZBAC-5562	Becky Allee
VBBWX7-5562	Becky Allee
VZACVE-5562	Becky Allee
W2ZUC7-5562	The answer is Becky Allee. We are able to search the filename in Axiom and the resulted file says that the author of the document is Becky Allee.
YCA984-5562	Becky Allee
Z4WK8A-5562	Becky Allee

TABLE 1

Question 48 - Removable Media 20-5562

Question 48: Who is the Author of 000124.doc?

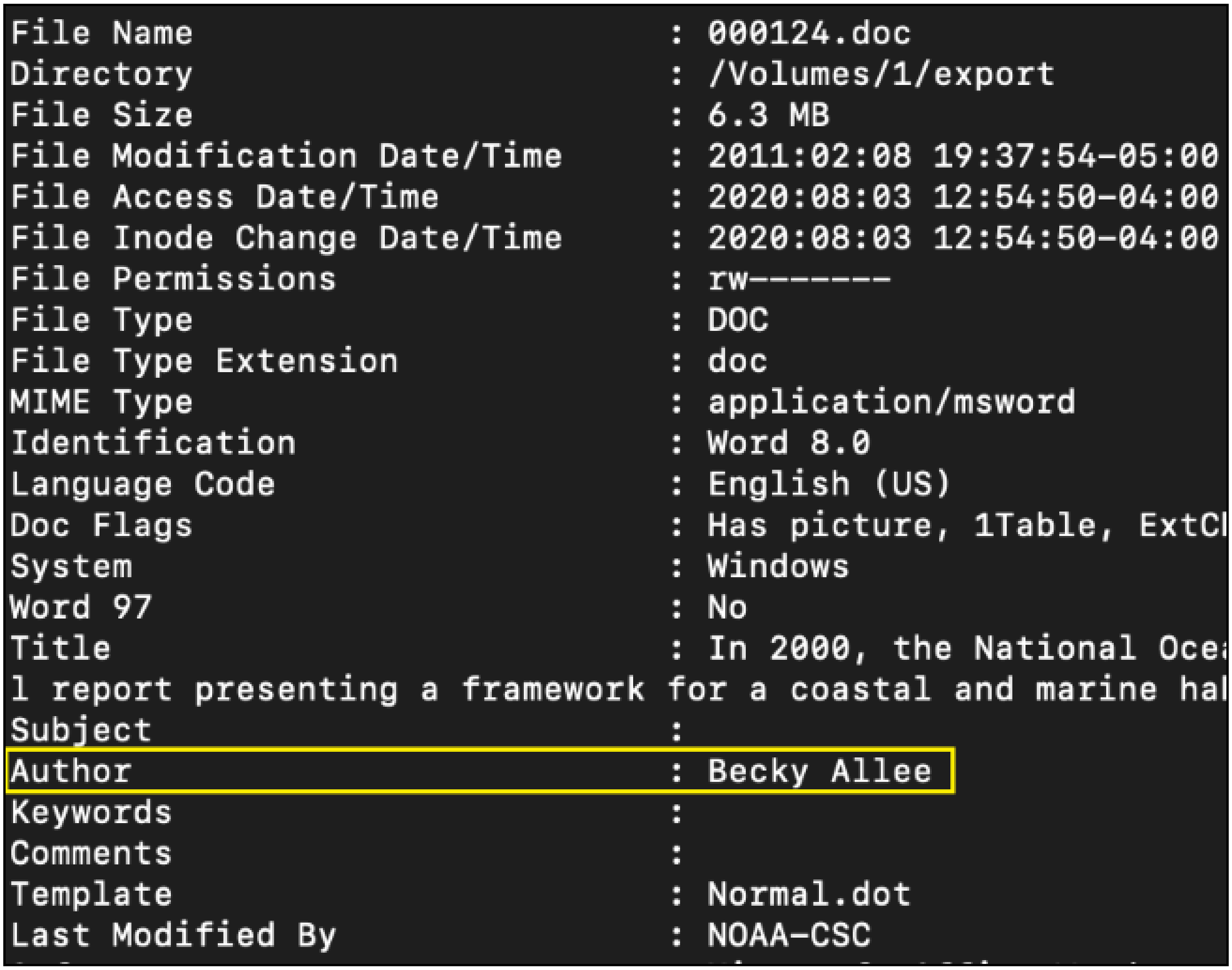
Consensus Result: Becky Allee

Expected Response Explanation:

Word document metadata can be parsed as shown in the provided image.

Expected Response Illustration:

Word document metadata:



```
File Name                       : 000124.doc
Directory                       : /Volumes/1/export
File Size                       : 6.3 MB
File Modification Date/Time     : 2011:02:08 19:37:54-05:00
File Access Date/Time           : 2020:08:03 12:54:50-04:00
File Inode Change Date/Time     : 2020:08:03 12:54:50-04:00
File Permissions                : rw-------
File Type                       : DOC
File Type Extension             : doc
MIME Type                       : application/msword
Identification                  : Word 8.0
Language Code                   : English (US)
Doc Flags                       : Has picture, 1Table, ExtCl
System                          : Windows
Word 97                         : No
Title                           : In 2000, the National Ocea
l report presenting a framework for a coastal and marine hal
Subject                         :
Author                          : Becky Allee
Keywords                        :
Comments                        :
Template                        : Normal.dot
Last Modified By                : NOAA-CSC
```

TABLE 1

Question 49 - Removable Media 20-5562

Question 49: In unallocated space on this device is a photo of a grey and white cat with a blue toy. What is the SHA1 hash of this file?

Manufacturer's Expected Response: 866c4b57882276e2e473f3ad8c364d92a890cebd

WebCode-Test	Response
64W7NX-5562	866C4B57882276E2E473F3AD8C364D92A890CEBD
6ZF77W-5562	866c4b57882276e2e473f3ad8c364d92a890cebd
7K2ZUX-5562	adac26902f8c097ba4c2d1c2cafb46c99ba40369
8Q3VR3-5562	866c4b57882276e2e473f3ad8c364d92a890cebd
BJTE9R-5562	866c4b57882276e2e473f3ad8c364d92a890cebd
CCTE9P-5562	adac26902f8c097ba4c2d1c2cafb46c99ba40369
CPXWKP-5562	866c4b57882276e2e473f3ad8c364d92a890cebd
DGFL7P-5562	the photo name is f0244288.jpg which was carved from unallocated space using Autopsy 4. The SHA1 is 866c4b57882276e2e473f3ad8c364d92a890cebd
EQHHC7-5562	866c4b57882276e2e473f3ad8c364d92a890cebd
ETQDAP-5562	866c4b57882276e2e473f3ad8c364d92a890cebd
HHBXTQ-5562	866c4b57882276e2e473f3ad8c364d92a890cebd
KH3VVH-5562	866C4B57882276E2E473F3AD8C364D92A890CEBD
MTJYGM-5562	866C4B57882276E2E473F3AD8C364D92A890CEBD
NF4QTK-5562	866c4b57882276e2e473f3ad8c364d92a890cebd
P6M4JK-5562	866c4b57882276e2e473f3ad8c364d92a890cebd
P92YZG-5562	866c4b57882276e2e473f3ad8c364d92a890cebd
Q7RBYH-5562	866c4b57882276e2e473f3ad8c364d92a890cebd
R7BE8H-5562	866c4b57882276e2e473f3ad8c364d92a890cebd
U3ZBAC-5562	866C4B57882276E2E473F3AD8C364D92A890CEBD
VBBWX7-5562	866C4B57882276E2E473F3AD8C364D92A890CEBD
VZACVE-5562	866c4b57882276e2e473f3ad8c364d92a890cebd
W2ZUC7-5562	The answer is 866c4b57882276e2e473f3ad8c364d92a890cebd. We are able to parse the unallocated file system in Autopsy and when checked in the pictures carved from the unallocated space, we see the picture as described in the question and the hash value is 866c4b57882276e2e473f3ad8c364d92a890cebd.
YCA984-5562	866C4B57882276E2E473F3AD8C364D92A890CEBD

Revised September 04, 2020. Reissuance due to removal of highlighting of a specific response for Question #21.

TABLE 1

Question 49 - Removable Media 20-5562

WebCode-Test	Response
Z4WK8A-5562	866C4B57882276E2E473F3AD8C364D92A890CEBD

Question 49: In unallocated space on this device is a photo of a grey and white cat with a blue toy. What is the SHA1 hash of this file?

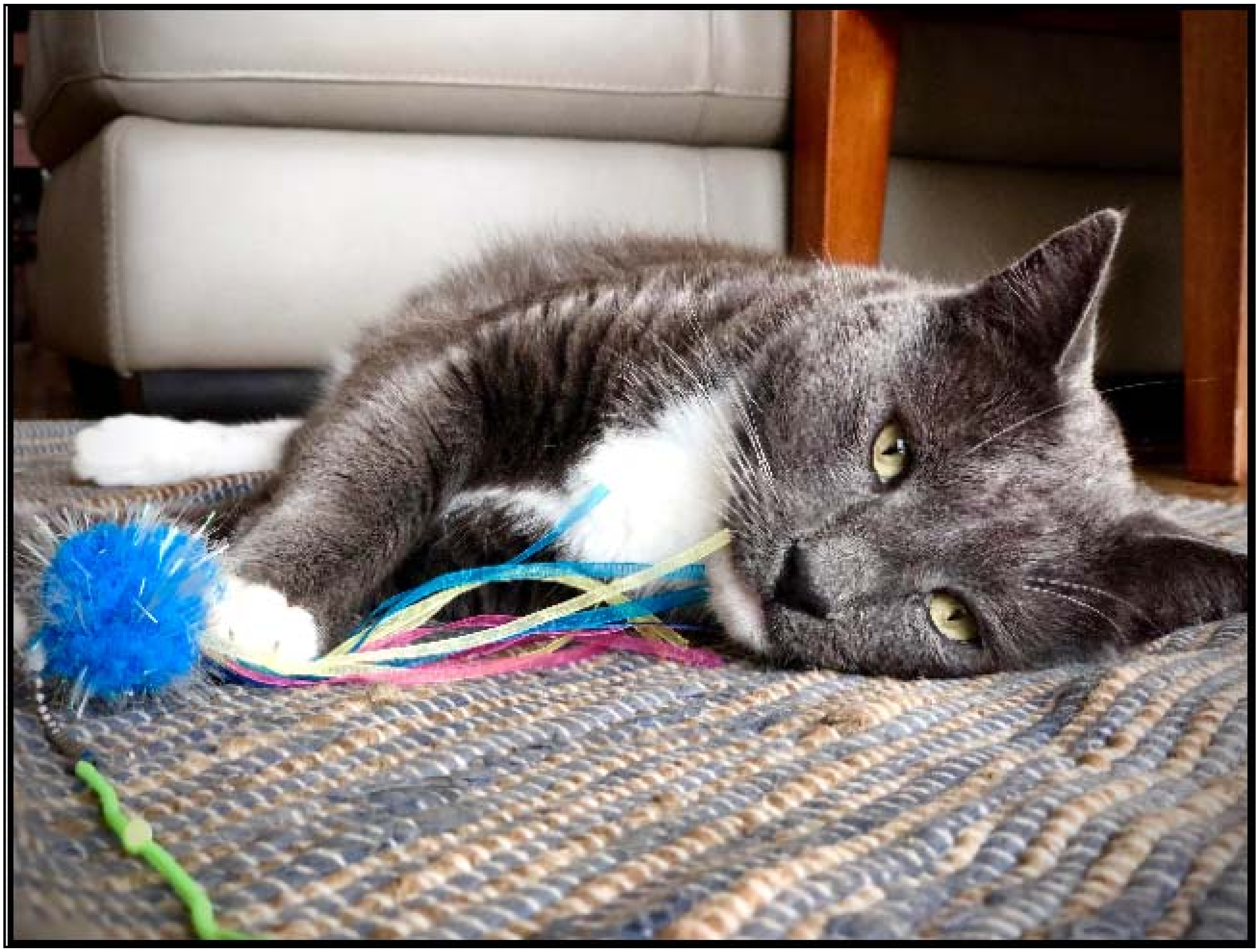
Consensus Result: 866c4b57882276e2e473f3ad8c364d92a890cebd

Expected Response Explanation:

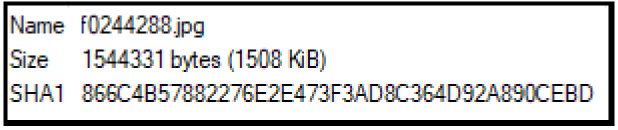
Any forensic file carving utility can be used to carve photo files from the unallocated space on the usb device. Reviewing the carved files will locate the described photo.

Expected Response Illustration:

Image content:



Autopsy view of metadata for the carved file:



Name	f0244288.jpg
Size	1544331 bytes (1508 KiB)
SHA1	866C4B57882276E2E473F3AD8C364D92A890CEBD

TABLE 1

Question 50 - Removable Media 20-5562

Question 50: What is the name of the file that contains the word "convallis"?

Manufacturer's Expected Response: lorem.text

WebCode-Test	Response
64W7NX-5562	lorem.text
6ZF77W-5562	lorem.text
7K2ZUX-5562	lorem.txt
8Q3VR3-5562	lorem.text
BJTE9R-5562	lorem.text
CCTE9P-5562	lorem.text
CPXWKP-5562	lorem.text
DGFL7P-5562	A keyword search using the word convallis revealed the document lorem.txt containing this word located in Location /Documents/Pictures/lorem.text
EQHHC7-5562	Lorem.text
ETQDAP-5562	lorem.text
HHBXTQ-5562	\Documents\Pictures\lorem.text
KH3VVH-5562	lorem.text
MTJYGM-5562	lorem.text
NF4QTK-5562	lorem.text
P6M4JK-5562	lorem.text
P92YZG-5562	lorem.text
Q7RBYH-5562	lorem.text
R7BE8H-5562	Lorem.text
U3ZBAC-5562	lorem.text
VBBWX7-5562	lorem.txt
VZACVE-5562	lorem.text
W2ZUC7-5562	The answer is lorem.text. Using Axiom forensics tool we are able to search for the keyword and we see that the name of the file where this keyword is mentioned is lorem.text
YCA984-5562	lorem.text
Z4WK8A-5562	lorem.text

TABLE 1

Question 50 - Removable Media 20-5562

Question 50: What is the name of the file that contains the word "convallis"?

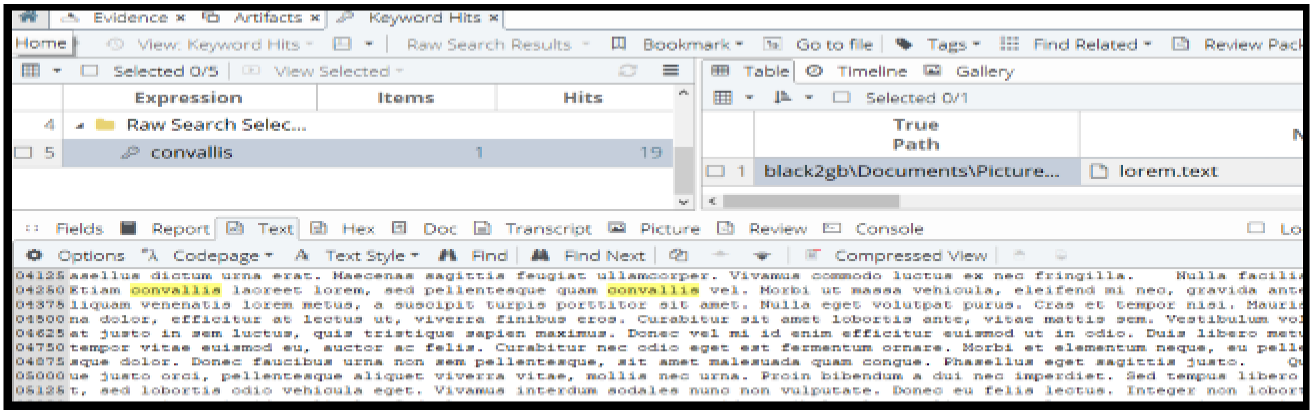
Consensus Result: lorem.text

Expected Response Explanation:

A keyword search identifies the target file at the following path \Documents\Pictures\lorem.text.

Expected Response Illustration:

Keyword Search:



	Expression	Items	Hits
4	Raw Search Selec...		
5	convallis	1	19

	True Path	N
1	black2gb\Documents\Picture...	lorem.text

```
04125 asellus dictum urna erat. Maecenas sagittis feugiat ullamcorper. Vivamus commodo luctus ex nec fringilla.    Nulla facili
04250 Etiam convallis laoreet lorem, sed pellentesque quam convallis vel. Morbi ut massa vehicula, eleifend mi nec, gravida ante
04375 liquam venenatis lorem metus, a suscipit turpis porttitor sit amet. Nulla eget volutpat purus. Cras et tempor nisi. Mauri
04500 na dolor, efficitur at lectus ut, viverra finibus eros. Curabitur sit amet lobortis ante, vitae mattis sem. Vestibulum vo
04625 at justo in sem luctus, quis tristique sapien maximus. Donec vel mi id enim efficitur euismod ut in odio. Duis libero met
04750 tempor vitae euismod eu, auctor ac felis. Curabitur nec odio eget est fermentum ornare. Morbi et elementum neque, eu pell
04875 sque dolor. Donec faucibus urna non sem pellentesque, sit amet malesuada quam congue. Phasellus eget sagittis justo.    Q
05000 ue justo orci, pellentesque aliquet viverra vitae, mollis nec urna. Proin bibendum a dui nec imperdiet. Sed tempus libero
05125 t, sed lobortis odio vehicula eget. Vivamus interdum sodales nunc non vulputate. Donec eu felis lectus. Integer non lobor
```

Additional Comments

TABLE 2

WebCode	Additional Comments
2ZQE6A-5561	Question 19: "From what URL was the file with SHA1 3de75af054fed96e39568bad6edfdbc452d2cda4 downloaded?" shouldn't use the word "file" as the data used to answer the question is a file's alternate data stream and isn't actually a file itself. Some software tools will represent this data as a file in order to make the information more accessibly. The process to determine the answer shouldn't be dependent on using the tool that was used to build the test. Question 31: "What darkweb (darknet) site did the user bookmark?" shouldn't use the the word "site" as technically two (2) sites were bookmarked, but they both were from the same host/domain (which I assume is the answer that is being sought).
6U9F26-5561	Questions 22 and 24 have 2 answers (2 files in the james' Recycle Bin). The questions only asked for a singular answer but I answered with data about both files. Question 11 is incorrectly worded: drives are not mounted - file systems contained on partitions are mounted. The last drive to contain a partition to be mounted was VBOX HARDDISK. This drive contained 2 partitions and the C:\ drive (not named) was the last to be mounted.
6ZF77W-5562	In questions 22 and 24 in the Recycle Bin there are 2 files, for that in the answers we provided the times for each file.
7M9E24-5561	Question 12: Looking at video files in Axiom and sorting by last accessed, a file associated with Skype video shows the last accessed. However, looking at locally access files and folders and sorting by last accessed, the SNL Jeopardy file is the most recent video file that was accessed.
9ENXLY-5561	#11 not in laboratory scope
DGFL7P-5562	44. I am colored blind it looks brown. 3.there are two partitions - system reserved with a sector count 1,185,792 and the second partition with no volume label with a sector count of 65,918,976. The two partitions together equal the total sectors of 67,108,864. Alot of the questions seem to reference incorrectly an example "What is the literal spelling of the word found in Question #38? " I think it meant to say what was found in question 37.
P92YZG-5562	Q21 & Q41 - The volume serial number provided is the full 8-byte value in hex as little endian.
QAQLVH-5561	The questions about antiforensic programs and the recycling bin were more difficult than they should have been. Having multiple tools to process in makes it easier but some tools will report multiple files for the recycle bin and the antiforensic tools could be TOR but it doesnt have to be.
R7BE8H-5562	The answers obtained towards the questions that had been raised. A encrypted container in the evidence There are no aspects of interest to review in what at the level technician is concerned. Note the location of an encrypted container located in the file name "Vfpr6npaqea12.jpg", which is only accessible by password, this being "pl@ym0n3y". Once this encrypted container is accessed, we can find ourselves in it with a file of text, named as “answer.txt” and that presents the following text: “, so long, and thanks for all the fish 42”.
TANE4A-5561	Because we are not native English speakers, the last question is not clear for us. We hope you will consider it.

TABLE 2

WebCode	Additional Comments
TXBE8F-5561	Question 7, 8, 20, 22 are poorly worded.
U3ZBAC-5562	Some of the questions had answers that required written answers instead of copying the text directly from the analysis tool. I have missed questions in the past because a letter was capitalized but not in the text of the analysis tool.

-End of Report-
(Appendix may follow)