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. 19-5561/2 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 33 participants, 15 of which also returned results associated with the physical USB. These results are compiled in the following tables:

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 an E01 file format. Participants were asked to examine the extracted data as it relates to a simulated scenario utilizing their own software and methods.

All participants enrolled in the 19-5562: 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:
A scripted scenario, based upon a murder case was created to generate user data on a Windows Hard Drive. The execution of the scripted crime took place from January 7, 2019 to January 17, 2019. 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 19-5562.

The data from the evidence hard drive was acquired through a physical extraction. The data was processed and analyzed using commercial and open source forensic tools. Following sample validation, the E01 files were compressed and uploaded to the CTS portal for participants to download. MD5 and SHA-1 algorithms were run on the compressed folder to generate unique hash values to allow participants to validate the successful download of the files.

The USB drive was duplicated using forensic hardware.

SAMPLE VALIDATION/VERIFICATION:
The validation stage consisted of the examination of the extracted data utilizing various software tools to ensure the expected results could be achieved. All the USB drives were validated by comparing the cryptographic hash functions.

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
Police are investigating a case involving the murder of a 70-yr old female. The victim's daughter is the primary suspect in this investigation. Police have collected multiple pieces of evidence from the suspect's house. You are being tasked with analyzing a forensic image of a computer. Using your own tools and methodologies, analyze the files to determine if they have any relevance to the investigation.

Manufacturer's Information, continued

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

1 Provide the MD5 hash value of the decompressed imaged drive.
905D67240D48D52C4EA290E7E8885DE2

2 What operating system was installed on the device?
Windows 10 Education

3 When was the operating system installed? Provide the answer in the UTC + 00:00 using the following format: MM/DD/YYYY HH:MM:SS AM/PM.
01/11/2019 03:02:34 PM

4 When was the device last shut down? Provide the answer in the UTC + 00:00 using the following format: MM/DD/YYYY HH:MM:SS AM/PM.
01/17/2019 07:34:22 PM

5 Provide the user name of the two accounts created by the user. Do not include Guest Account and Default Account
Morgan Chen, Kids

6 What is the set time zone on the device?
(UTC-05:00) Eastern Time (US & Canada)

7 When did the primary user last login to their account? Provide the answer in the UTC + 00:00 using the following format: MM/DD/YYYY HH:MM:SS AM/PM.
01/17/2019 01:26:04 PM

8 How many times did the primary user log into this computer?
Seven (7)

9 Provide the password hint for Morgan Chen's account.
last

10 What is the assigned IP address of the subject computer?
192.168.189.132

11 How many files are in the Recycle Bin?
Two (2)

12 Provide the name of the most recently viewed document. (pdf, xls, docx, rtf)
Julie_Chen - LastWill.docx

13 What feature of Windows records execution of programs (and their parameters) to speed up the application's start up process?
Prefetch

14 How many pages were bookmarked on Chrome?
Four (4)

Manufacturer's Information, continued

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

15 Provide the last term searched using Google Chrome on this device?
probate process in new jersey

16 What email application was used to send and receive emails?
Thunderbird or Mozilla Thunderbird

17 What is the Gmail email address associated to the primary user on this device?
chenmorgan01@gmail.com

18 An email was sent to "Laurelmurray63@gmail.com" on 01/14/2019 at 01:19 PM. Provide the subject of that email.
Hey Girl

19 What is the primary user's physical (home) address? Provide the Building number, Street Name, City, and State
16925 Shaw Road, Trenton, New Jersey

20** When was "notepad.exe" last executed? Provide the answer in the UTC + 00:00 using the following format: MM/DD/YYYY HH:MM:SS AM/PM.
01/14/2019 08:15:39 PM

21 How many times was "mspaint.exe" executed?
Seven (7)

22 Was the Skype Application executed on this computer?
Yes

23 What type (CD, USB, SD Card, Optical drive) of device was last mounted as E: drive?
USB

24 How many USB devices were mounted to this computer?
Two (2)

25** Provide the serial number associated with USB named "Give Away 2018".
0DCDD820

26** Provide the last write time for device named "Give Away 2018". Provide the answer in the UTC + 00:00 using the following format: MM/DD/YYYY HH:MM:SS AM/PM.
01/14/2019 08:09:45 PM

27 What drive letter was assigned to the last mounted USB drive?
E:

28 What is the install date and time of the last mounted device? Provide the answer in the UTC + 00:00 using the following format: MM/DD/YYYY HH:MM:SS AM/PM.
01/15/2019 03:02:54 PM

Manufacturer's Information, continued

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

29** Provide the manufacturer's name of the last mounted device.
Alcor Micro Corp.

30 What is the MD5 of the imaged drive?
303ef526fce62837655577dedc17b376

31 What file system(s) is utilized on this drive?
FAT16

32** What is the vendor ID?
058f

33** What is the product ID?
6387

34 How many JPG images were stored in the "Family Pictures" folder?
Eight (8)

35 Were the images found in the "Family Pictures" folder accessed using the computer hard drive? Yes/No
Yes

36 Provide the volume label of the device.
Recipe's

37** When was the file "Julie_Chen - LastWill.docx" last modified? Provide the answer in the UTC + 00:00 using the following format: MM/DD/YYYY HH:MM:SS AM/PM.
01/11/2019 08:58:00 PM

38 Based on your investigation, does this device have any connection with the computer hard drive evidence? Yes/No
Yes

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 E01 file format, and a series of questions related to the extracted data. Additionally, participants enrolled in the 19-5562: 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 33 participants returned results for the 5561 Computer Hard Drive - Windows Analysis test. Of the 29 total questions, four questions did not reach a consensus response. These four questions were found in the following two skill sets: Applications and External Media.

Of the participants enrolled in the 5592 Removable Media Storage Analysis test, 15 returned results. Three of the eight questions did not reach a consensus response.

Notably, a portion of inconsistent responses across the collection of questions may have been due to typographical errors and others were due to not answering the question in the requested format.

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 the proficiency test questions.

Digital Evidence Responses

TABLE 1

Question: 1 Category: Authentication

Question 1: Provide the MD5 hash value of the decompressed imaged drive.

Manufacturer's Expected Response: 905D67240D48D52C4EA290E7E8885DE2

WebCode	Response
32LYBW-5562	905D67240D48D52C4EA290E7E8885DE2
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	905d67240d48d52c4ea290e7e8885de2
682GJP-5562	905d67240d48d52c4ea290e7e8885de2
6Z4RZY-5561	905d67240d48d52c4ea290e7e8885de2
9LB7BM-5562	905d67240d48d52c4ea290e7e8885de2
AP6K9W-5562	905d67240d48d52c4ea290e7e8885de2
C97GKM-5561	905D67240D48D52C4EA290E7E8885DE2
CMBD4P-5561	905d67240d48d52c4ea290e7e8885de2
CPHTCG-5561	905D67240D48D52C4EA290E7E8885DE2
D9NRUF-5562	905D67240D48D52C4EA290E7E8885DE2
EP84ZE-5562	905D67240D48D52C4EA290E7E8885DE2
H6CDEC-5561	363e8d4aa10ddd172c958ae0fc5c4bfc
J3ZUA9-5561	905d67240d48d52c4ea290e7e8885de2
JLWJ4G-5562	905D67240D48D52C4EA290E7E8885DE2
K3E3B9-5561	905d67240d48d52c4ea290e7e8885de2
L6WGE9-5561	905d67240d48d52c4ea290e7e8885de2
MUUH6E-5561	905d67240d48d52c4ea290e7e8885de2
NBXF34-5561	905d67240d48d52c4ea290e78885de2
NFT79E-5562	MD5 : 905D67240D48D52C4EA290E7E8885DE2
NMCAFG-5561	905d67240d48d52c4ea290e7e8885de2
Q2K3Y6-5562	905d67240d48d52c4ea290e7e8885de2
QL9NG8-5561	905D67240D48D52C4EA290E7E8885DE2
QVYAM6-5562	905d67240d48d52c4ea290e7e8885de2

TABLE 1

Question: 1 **Category: Authentication**

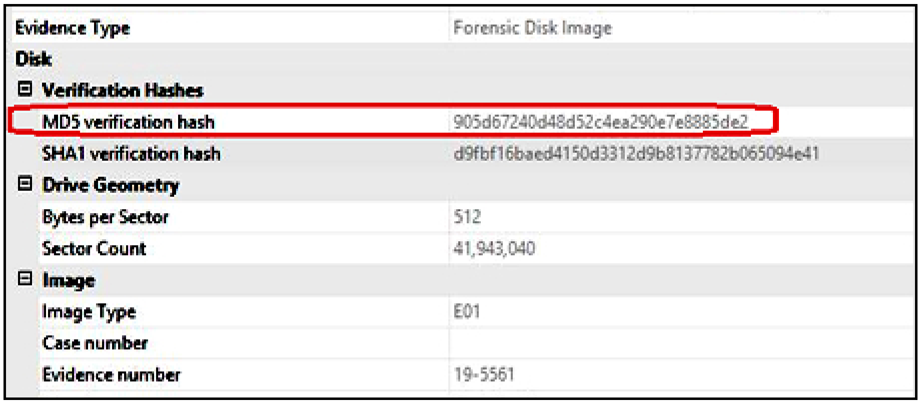
WebCode	Response
RTPJX2-5561	905d67240d48d52c4ea290e7e8885de2
V292YY-5561	905d6720d48d52c4ea290e7e8885de2
WJ4UKW-5561	MD5 - 905d67240d48d52c4ea290e7e8885de2. SHA1 - d9fbf16baed4150d3312d9b8137782b065094e41
X4PZAY-5562	905d67240d48d52c4ea290e7e8885de2
XDC2Q9-5561	905d67240d48d52c4ea290e7e8885de2
XE36GV-5561	905d67240d48d52c4ea290e7e8885de2
YN48YX-5562	905d67240d48d52c4ea290e7e8885de2
YUVEG7-5561	905d67240d48d52c4ea290e7e8885de2
ZMBJCV-5562	905d67240d48d52c4ea290e7e8885de2

Question 1: Provide the MD5 hash value of the decompressed imaged drive.

Consensus Result: 905D67240D48D52C4EA290E7E8885DE2

Expected Response Explanation:
This hash value can be calculated using a forensic tool.

Screen Shot:
MD5 Hash Value:



Evidence Type	Forensic Disk Image
Disk	
⊟ Verification Hashes	
MD5 verification hash	905d67240d48d52c4ea290e7e8885de2
SHA1 verification hash	d9fbf16baed4150d3312d9b8137782b065094e41
⊟ Drive Geometry	
Bytes per Sector	512
Sector Count	41,943,040
⊟ Image	
Image Type	E01
Case number	
Evidence number	19-5561

TABLE 1

Question: 2	Category: System

Question 2: What operating system was installed on the device?

Manufacturer's Expected Response: Windows 10 Education

WebCode	Response
32LYBW-5562	Windows 10 Education
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	Windows 10 Education
682GJP-5562	Windows 10 Education
6Z4RZY-5561	Windows 10 Education, version 6.3
9LB7BM-5562	Windows 10 Education
AP6K9W-5562	Windows 10 Education V6.3
C97GKM-5561	Windows 10 Education
CMBD4P-5561	Windows 10 Education
CPHTCG-5561	Windows 10 Education
D9NRUF-5562	Windows 10 Education
EP84ZE-5562	Windows 10 Education
H6CDEC-5561	Windows 10 Education
J3ZUA9-5561	Windows 10 Education
JLWJ4G-5562	Windows 10 Education 10.0.15063 N/A Build 15063
K3E3B9-5561	Windows 10 Education 6.3 compilación 15063. (“Windows\System32\config\SOFTWARE”)
L6WGE9-5561	Windows 10 Education
MUUH6E-5561	Windows 10 Education
NBXF34-5561	Windows 10 Education
NFT79E-5562	Windows 10 Education
NMCAFG-5561	Windows 10 Education
Q2K3Y6-5562	Windows 10 Education
QL9NG8-5561	Windows 10 Education
QVYAM6-5562	Windows 10 Education
RTPJX2-5561	Windows 10 Education

TABLE 1

Question: 2	Category: System
WebCode	**Response**
V292YY-5561	Windows 10 Education version 6.3 build 15063
WJ4UKW-5561	Windows 10 Education
X4PZAY-5562	Windows 10 Education
XDC2Q9-5561	Windows 10 Education
XE36GV-5561	Windows 10 Educational, Build 15603
YN48YX-5562	Windows 10 Education
YUVEG7-5561	Windows 10 Education
ZMBJCV-5562	Windows 10 Education build 15063

Question 2: What operating system was installed on the device?

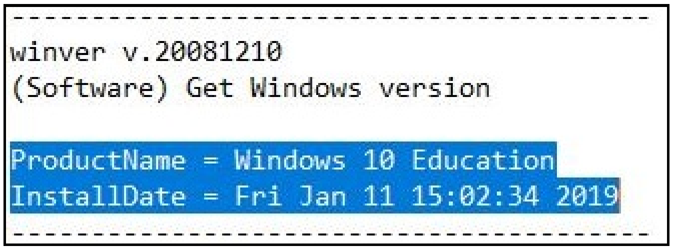
Consensus Result: Windows 10 Education

Expected Response Explanation:

Information regarding the operating system installed on this device is found in the Software registry hive at the following location: C:\Windows\system32\config\SOFTWARE: \Microsoft\Windows NT\CurrentVersion

Screen Shot:

OS Version:



```
----------------------------------------
winver v.20081210
(Software) Get Windows version

ProductName = Windows 10 Education
InstallDate = Fri Jan 11 15:02:34 2019
----------------------------------------
```

TABLE 1

Question: 3	Category: System

Question 3: When was the operating system installed? Provide the answer in the UTC + 00:00 using the following format: MM/DD/YYYY HH:MM:SS AM/PM.

Manufacturer's Expected Response: 01/11/2019 03:02:34 PM

WebCode	Response
32LYBW-5562	1/11/2019 3:02:34 PM
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	01/11/2019 03:02:34 PM
682GJP-5562	01/11/2019 03:02:34 PM
6Z4RZY-5561	01/11/2019 03:02:34 PM
9LB7BM-5562	01/11/2019 03:02:34 PM
AP6K9W-5562	01/11/2019 15:02:34 +1:00
C97GKM-5561	01/11/2019 03:02:34 PM
CMBD4P-5561	11/01/2019 03:02:34 PM
CPHTCG-5561	01/11/2019 03:02:34 PM
D9NRUF-5562	01/11/2019 03:02:34 PM
EP84ZE-5562	01/11/2019 15:02:34 UTC
H6CDEC-5561	1/11/2019 15:02:34
J3ZUA9-5561	01/11/2019 03:02:34 PM
JLWJ4G-5562	01/11/2019 03:02:34 PM
K3E3B9-5561	01/11/2019 03:02:34 PM (“Windows\System32\config\SOFTWARE”)
L6WGE9-5561	01/11/2019 03:02:34 PM
MUUH6E-5561	01/11/2019 03:02:34 PM
NBXF34-5561	01/11/2019 03:02:34 PM
NFT79E-5562	01/11/2019 15:02:34 PM
NMCAFG-5561	01/11/2019 03:02:34 PM
Q2K3Y6-5562	01/11/2019 10:02:34 AM
QL9NG8-5561	01/11/2019 03:02:34 PM
QVYAM6-5562	01/11/2019 15:02:34
RTPJX2-5561	01/11/2019 03:02:34 PM

TABLE 1

Question: 3	Category: System
WebCode	**Response**
V292YY-5561	01/11/2019 03:02:34 PM UTC
WJ4UKW-5561	01/11/2019 15:02:34 PM UTC
X4PZAY-5562	01/11/2019 3:02:34 PM
XDC2Q9-5561	01/11/2019 03:02:34 PM
XE36GV-5561	01/11/2019 3:02:34 PM
YN48YX-5562	1/11/2019 3:02:34 PM
YUVEG7-5561	01/11/2019 03:02:34 PM.
ZMBJCV-5562	01/12/2019 01:02:34 AM

Question 3: When was the operating system installed? Provide the answer in the UTC + 00:00 using the following format: MM/DD/YYYY HH:MM:SS AM/PM.

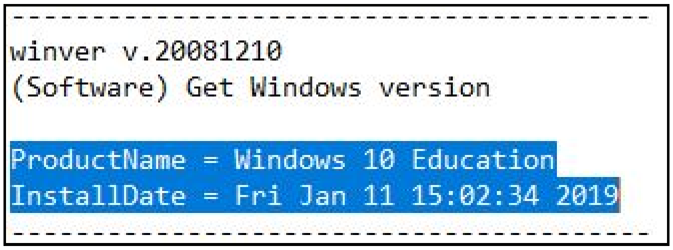
Consensus Result: 01/11/2019 03:02:34 PM

Expected Response Explanation:

Information regarding when the operating system was installed on this device is found in the Software registry hive at the following location: C:\Windows\system32\config\SOFTWARE: \Microsoft\Windows NT\CurrentVersion

Screen Shot:

OS Install Date:



```
----------------------------------------
winver v.20081210
(Software) Get Windows version

ProductName = Windows 10 Education
InstallDate = Fri Jan 11 15:02:34 2019
----------------------------------------
```

TABLE 1

Question: 4	Category: System

Question 4: When was the device last shut down? Provide the answer in the UTC + 00:00 using the following format: MM/DD/YYYY HH:MM:SS AM/PM.

Manufacturer's Expected Response: 01/17/2019 07:34:22 PM

WebCode	Response
32LYBW-5562	1/17/2019 7:34:22 PM
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	01/17/2019 07:34:22 PM
682GJP-5562	01/17/2019 07:34:22 PM
6Z4RZY-5561	01/17/2019 07:34:22 PM
9LB7BM-5562	01/17/2019 07:34:22 PM
AP6K9W-5562	01/17/2019 19:34:22 +1:00
C97GKM-5561	01/17/2019 07:34:22 PM
CMBD4P-5561	01/17/2019 07:34:22 PM
CPHTCG-5561	01/17/2019 07:34:22 PM
D9NRUF-5562	01/17/2019 07:34:22 PM
EP84ZE-5562	01/17/2019 19:34:22 UTC
H6CDEC-5561	1/17/2019 19:34:22
J3ZUA9-5561	01/17/2019 07:34:22 PM
JLWJ4G-5562	01/17/2019 07:34:22 PM
K3E3B9-5561	01/17/2019 07:34:22 PM ("Windows\System32\config\SOFTWARE")
L6WGE9-5561	01/17/2019 07:34:22 PM
MUUH6E-5561	01/17/2019 07:34:22 PM
NBXF34-5561	01/17/2019 07:34:22 PM
NFT79E-5562	01/18/2019 01:30:22
NMCAFG-5561	01/17/2019 07:34:22 PM
Q2K3Y6-5562	01/17/2019 02:34:22 PM
QL9NG8-5561	01/17/2019 07:34:22 PM
QVYAM6-5562	01/17/2019 19:34:22
RTPJX2-5561	01/17/2019 07:34:22 PM

TABLE 1

Question: 4 **Category: System**

WebCode	Response
V292YY-5561	01/17/2019 07:34:22 PM UTC
WJ4UKW-5561	01/17/2019 19:34:22 PM UTC
X4PZAY-5562	1/17/2019 7:34:22 PM
XDC2Q9-5561	01/17/2019 07:34:22 PM
XE36GV-5561	01/17/2019 7:34:22 PM
YN48YX-5562	1/17/2019 7:34:22 PM
YUVEG7-5561	01/17/2019 07:34:22 PM.
ZMBJCV-5562	01/18/2019 05:34:22 AM

Question 4: When was the device last shut down? Provide the answer in the UTC + 00:00 using the following format: MM/DD/YYYY HH:MM:SS AM/PM.

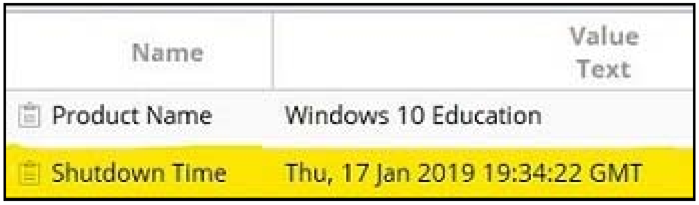
Consensus Result: 01/17/2019 07:34:22 PM

Expected Response Explanation:

Information regarding the last shutdown date and time can be sourced from the Software registry hive at the following location: CurrentControlSet\Control\Windows Shutdown time

Screen Shot:

Device Shutdown Date/Time:



Name	Value Text
Product Name	Windows 10 Education
Shutdown Time	Thu, 17 Jan 2019 19:34:22 GMT

TABLE 1

Question: 5	Category: System

Question 5: Provide the user name of the two accounts created by the user. Do not include Guest Account and Default Account

Manufacturer's Expected Response: Morgan Chen, Kids

WebCode	Response
32LYBW-5562	Morgan Chen Kids
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	Morgan Chen Kids
682GJP-5562	Kids, Morgan Chen
6Z4RZY-5561	Morgan , Kids
9LB7BM-5562	Kids, Morgan Chen
AP6K9W-5562	Kids Morgan Chen
C97GKM-5561	Morgan Chen Kids
CMBD4P-5561	Morgan Chen Kids
CPHTCG-5561	Kids and Morgan Chen
D9NRUF-5562	Morgan Chen Kids
EP84ZE-5562	Morgan Chen, Kids
H6CDEC-5561	Kids, Morgan Chen
J3ZUA9-5561	Kids Morgan Chen
JLWJ4G-5562	Morgan Chen, Kids
K3E3B9-5561	Morgan Chen y Kids. (“Windows\System32\config\SAM”)
L6WGE9-5561	Kids Morgan Chen
MUUH6E-5561	Kids, Morgan Chen
NBXF34-5561	Kids Morgan Chen
NFT79E-5562	"Kids" & "Morgan Chen"
NMCAFG-5561	Morgan Chen Kids
Q2K3Y6-5562	1) Morgan Chen; 2) Kids
QL9NG8-5561	Kids, Morgan Chen
QVYAM6-5562	Morgan Chen and Kids
RTPJX2-5561	Morgan Chen, Kids

TABLE 1

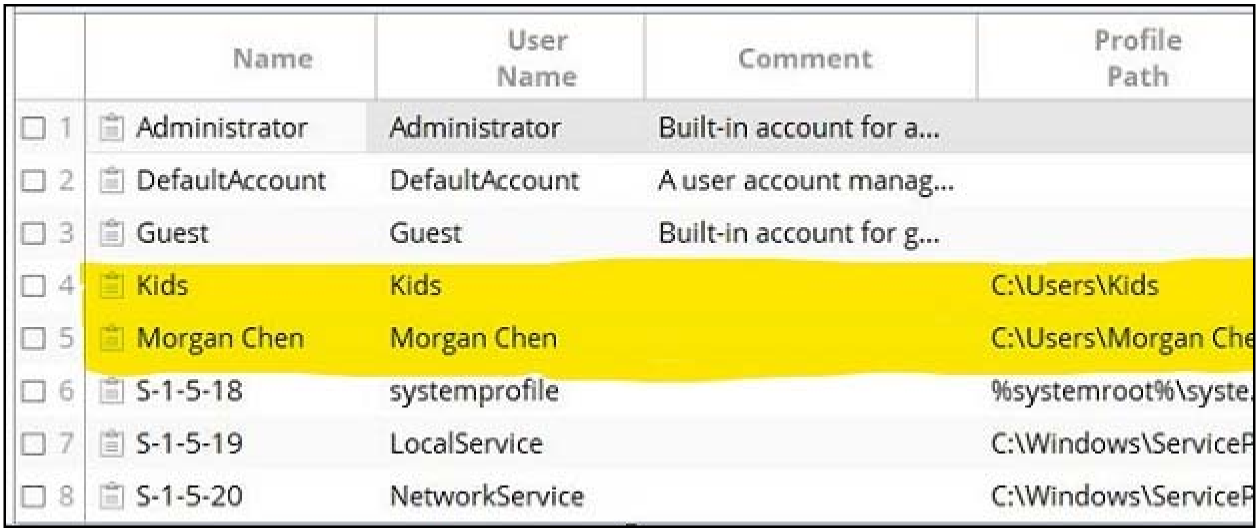
Question: 5	Category: System
WebCode	**Response**
V292YY-5561	Morgan Chen (RID 1000) Kids (RID 1001)
WJ4UKW-5561	Morgan Chen, Kids
X4PZAY-5562	Morgan Chen Kids
XDC2Q9-5561	Kids Morgan Chen
XE36GV-5561	Morgan Chen Kids
YN48YX-5562	Morgan Chen Kids
YUVEG7-5561	Kids, Morgan Chen
ZMBJCV-5562	"Morgan Chen", "Kids"

Question 5: Provide the user name of the two accounts created by the user. Do not include Guest Account and Default Account

Consensus Result: Morgan Chen, Kids

Expected Response Explanation:
Information regarding the user names of the accounts created by the user can be sourced from the Security Accounts Manager (SAM) registry hive at \Windows\System32\Config\.

Screen Shot:
User Accounts:



	Name	User Name	Comment	Profile Path
□ 1	Administrator	Administrator	Built-in account for a...	
□ 2	DefaultAccount	DefaultAccount	A user account manag...	
□ 3	Guest	Guest	Built-in account for g...	
□ 4	Kids	Kids		C:\Users\Kids
□ 5	Morgan Chen	Morgan Chen		C:\Users\Morgan Che
□ 6	S-1-5-18	systemprofile		%systemroot%\syste
□ 7	S-1-5-19	LocalService		C:\Windows\ServiceP
□ 8	S-1-5-20	NetworkService		C:\Windows\ServiceP

TABLE 1

Question: 6	Category: System

Question 6: What is the set time zone on the device?

Manufacturer's Expected Response: (UTC-05:00) Eastern Time (US & Canada)

WebCode	Response
32LYBW-5562	Eastern Standard Time
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	Eastern Standard Time (UTC + 05:00)
682GJP-5562	Eastern Standard Time
6Z4RZY-5561	(UTC-05:00) Eastern Time (US & Canada)
9LB7BM-5562	Eastern Standard Time
AP6K9W-5562	Eastern Standard Time
C97GKM-5561	Eastern Standard Time
CMBD4P-5561	Eastern Standart Time
CPHTCG-5561	Eastern Standard Time (UTC -05)
D9NRUF-5562	Eastern Standard Time (UTC -5)
EP84ZE-5562	Eastern Standard Time
H6CDEC-5561	Eastern Standard
J3ZUA9-5561	Eastern Standard Time
JLWJ4G-5562	(UTC-05:00) Eastern Time (US & Canada)
K3E3B9-5561	Eastern Daylight Time. (Current Desviation -300 minutes, "Windows\System32\config\SYSTEM")
L6WGE9-5561	Eastern Standard Time
MUUH6E-5561	Eastern Standard Time
NBXF34-5561	Eastern Standard Time
NFT79E-5562	Eastern Standard Time .
NMCAFG-5561	(UTC-05:00) Eastern Time (US & Canada)
Q2K3Y6-5562	Eastern Standard Time
QL9NG8-5561	(UTC-05:00) Eastern Time (US & Canada)
QVYAM6-5562	Eastern Standard Time.
RTPJX2-5561	Eastern Standard Time

TABLE 1

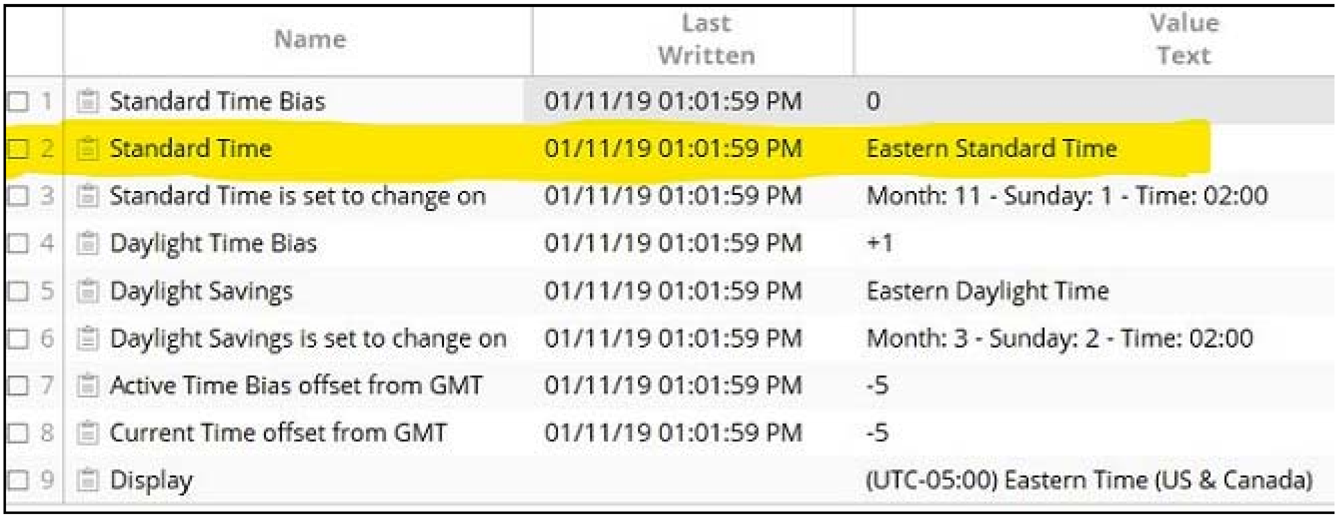
Question: 6	Category: System
WebCode	**Response**
V292YY-5561	Eastern Time (-5 UTC) Daylight Savings was enabled, but not currently active
WJ4UKW-5561	Eastern Standard Time
X4PZAY-5562	Eastern Standard Time
XDC2Q9-5561	Eastern Standard Time
XE36GV-5561	Eastern Standard Time
YN48YX-5562	Eastern Standard Time
YUVEG7-5561	Eastern Standard Time
ZMBJCV-5562	Eastern Standard Time

Question 6: What is the set time zone on the device?

Consensus Result: (UTC-05:00) Eastern Time (US & Canada)

Expected Response Explanation:
Information regarding the time zone set on the device can be sourced from the System registry hive at the following location:
ControlSet001\Control\TimeZoneInformation

Screen Shot:
Time Zone of Device:



	Name	Last Written	Value Text
☐ 1	Standard Time Bias	01/11/19 01:01:59 PM	0
☐ 2	Standard Time	01/11/19 01:01:59 PM	Eastern Standard Time
☐ 3	Standard Time is set to change on	01/11/19 01:01:59 PM	Month: 11 - Sunday: 1 - Time: 02:00
☐ 4	Daylight Time Bias	01/11/19 01:01:59 PM	+1
☐ 5	Daylight Savings	01/11/19 01:01:59 PM	Eastern Daylight Time
☐ 6	Daylight Savings is set to change on	01/11/19 01:01:59 PM	Month: 3 - Sunday: 2 - Time: 02:00
☐ 7	Active Time Bias offset from GMT	01/11/19 01:01:59 PM	-5
☐ 8	Current Time offset from GMT	01/11/19 01:01:59 PM	-5
☐ 9	Display		(UTC-05:00) Eastern Time (US & Canada)

TABLE 1

Question: 7 **Category: System**

Question 7: When did the primary user last login to their account? Provide the answer in the UTC + 00:00 using the following format: MM/DD/YYYY HH:MM:SS AM/PM.

Manufacturer's Expected Response: 01/17/2019 01:26:04 PM

WebCode	Response
32LYBW-5562	10/17/2019 1:26:04 PM
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	01/17/2019 01:26:04 PM
682GJP-5562	01/17/2019 01:26:04 PM
6Z4RZY-5561	01/17/2019 01:26:04 PM
9LB7BM-5562	01/17/2019 01:26:04 PM
AP6K9W-5562	01/17/2019 13:26:04 +1:00
C97GKM-5561	01/17/2019 01:26:04 PM
CMBD4P-5561	01/17/2019 01:26:04 PM
CPHTCG-5561	01/17/2019 01:26:04 PM
D9NRUF-5562	01/17/2019 01:26:04 PM
EP84ZE-5562	01/17/2019 13:26:04 UTC
H6CDEC-5561	01/17/19 13:26:04
J3ZUA9-5561	01/17/2019 01:26:04 PM
JLWJ4G-5562	01/17/2019 01:26:04 PM
K3E3B9-5561	01/17/2019 01:26:04. PM (“Windows\System32\config\SAM”)
L6WGE9-5561	01/17/2019 01:26:04 PM
MUUH6E-5561	01/17/2019 01:26:04 PM
NBXF34-5561	01/17/2019 01:26:04 PM
NFT79E-5562	01/17/2019 13:26:04 PM
NMCAFG-5561	01/17/2019 01:26:04 PM
Q2K3Y6-5562	01/17/2019 08:26:04 AM
QL9NG8-5561	01/17/2019 01:26:04 PM
QVYAM6-5562	1/17/2019 13:26:04 PM
RTPJX2-5561	01/17/2019 1:26:04 PM

TABLE 1

Question: 7	Category: System
WebCode	**Response**
V292YY-5561	01/17/2019 01:26:04 PM UTC
WJ4UKW-5561	01/17/2019 13:26:04 PM UTC
X4PZAY-5562	01/17/2019 1:26:04 PM
XDC2Q9-5561	01/17/2019 01:26:04 PM
XE36GV-5561	01/17/2019 1:26:04 PM
YN48YX-5562	1/17/2019 1:26:04 PM
YUVEG7-5561	01/17/19 01:26:04 PM.
ZMBJCV-5562	01/17/2019 11:26:04 PM

Question 7: When did the primary user last login to their account? Provide the answer in the UTC + 00:00 using the following format: MM/DD/YYYY HH:MM:SS AM/PM.

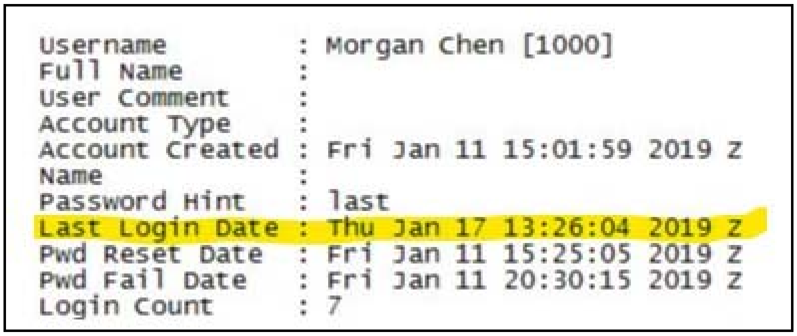
Consensus Result: 01/17/2019 01:26:04 PM

Expected Response Explanation:

Information regarding the primary user's last login date/time can be sourced from the Security Accounts Manager (SAM) registry hive.

Screen Shot:

User File:



```
Username        : Morgan Chen [1000]
Full Name       :
User Comment    :
Account Type    :
Account Created : Fri Jan 11 15:01:59 2019 Z
Name            :
Password Hint   : last
Last Login Date : Thu Jan 17 13:26:04 2019 Z
Pwd Reset Date  : Fri Jan 11 15:25:05 2019 Z
Pwd Fail Date   : Fri Jan 11 20:30:15 2019 Z
Login Count     : 7
```

TABLE 1

Question: 8	Category: System

Question 8: How many times did the primary user log into this computer?

Manufacturer's Expected Response: Seven (7)

WebCode	Response
32LYBW-5562	7
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	Seven (07) times
682GJP-5562	7
6Z4RZY-5561	7
9LB7BM-5562	7
AP6K9W-5562	7
C97GKM-5561	7
CMBD4P-5561	7
CPHTCG-5561	7
D9NRUF-5562	7
EP84ZE-5562	7
H6CDEC-5561	7
J3ZUA9-5561	7
JLWJ4G-5562	7
K3E3B9-5561	7 times (“Windows\System32\config\SAM”).
L6WGE9-5561	7
MUUH6E-5561	7
NBXF34-5561	7
NFT79E-5562	7
NMCAFG-5561	Seven (7)
Q2K3Y6-5562	7
QL9NG8-5561	6
QVYAM6-5562	7
RTPJX2-5561	7

TABLE 1

Question: 8 **Category: System**

WebCode	Response
V292YY-5561	7
WJ4UKW-5561	7
X4PZAY-5562	7
XDC2Q9-5561	7
XE36GV-5561	Seven
YN48YX-5562	7
YUVEG7-5561	7 Times
ZMBJCV-5562	7

Question 8: How many times did the primary user log into this computer?

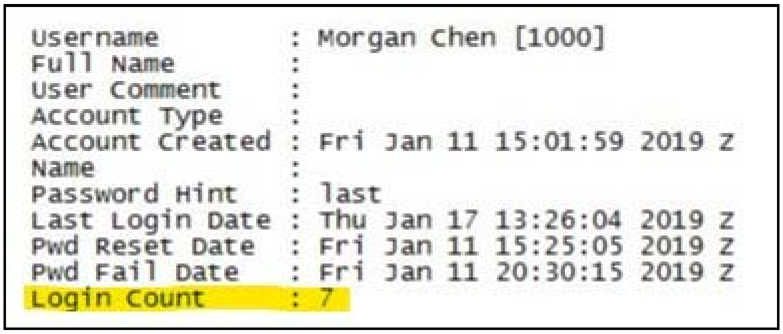
Consensus Result: Seven (7)

Expected Response Explanation:

Information regarding the number of times the primary user has logged onto this computer can be sourced from the Security Accounts Manager (SAM) registry hive.

Screen Shot:

User File:



```
Username        : Morgan Chen [1000]
Full Name       :
User Comment    :
Account Type    :
Account Created : Fri Jan 11 15:01:59 2019 Z
Name            :
Password Hint   : last
Last Login Date : Thu Jan 17 13:26:04 2019 Z
Pwd Reset Date  : Fri Jan 11 15:25:05 2019 Z
Pwd Fail Date   : Fri Jan 11 20:30:15 2019 Z
Login Count     : 7
```

TABLE 1

Question: 9	Category: System

Question 9: Provide the password hint for Morgan Chen's account.

Manufacturer's Expected Response: last

WebCode	Response
32LYBW-5562	last
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	last
682GJP-5562	last
6Z4RZY-5561	last
9LB7BM-5562	last
AP6K9W-5562	Last
C97GKM-5561	last
CMBD4P-5561	last
CPHTCG-5561	last
D9NRUF-5562	Last
EP84ZE-5562	last
H6CDEC-5561	last
J3ZUA9-5561	last
JLWJ4G-5562	last
K3E3B9-5561	last (“Windows\System32\config\SAM”)
L6WGE9-5561	last
MUUH6E-5561	last
NBXF34-5561	last
NFT79E-5562	" Last "
NMCAFG-5561	last
Q2K3Y6-5562	last
QL9NG8-5561	last
QVYAM6-5562	last
RTPJX2-5561	last

TABLE 1

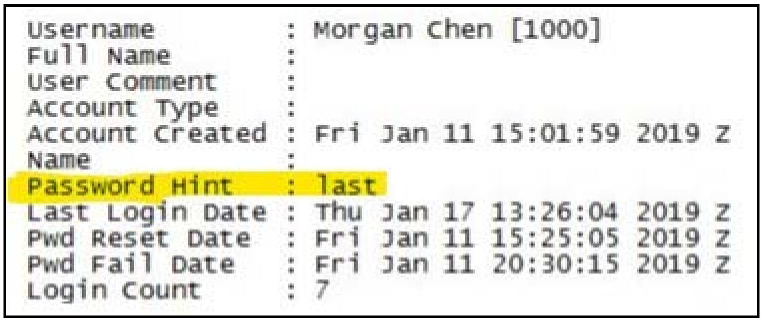
Question: 9	Category: System
WebCode	**Response**
V292YY-5561	last
WJ4UKW-5561	last
X4PZAY-5562	last
XDC2Q9-5561	last
XE36GV-5561	last
YN48YX-5562	last
YUVEG7-5561	last
ZMBJCV-5562	"last"

Question 9: Provide the password hint for Morgan Chen's account.

Consensus Result: last

Expected Response Explanation:
Information regarding the password hint for Morgan Chen's account can be sourced from the Security Accounts Manager (SAM) registry hive.

Screen Shot:
User File:



```
Username         : Morgan Chen [1000]
Full Name        :
User Comment     :
Account Type     :
Account Created  : Fri Jan 11 15:01:59 2019 Z
Name             :
Password Hint    : last
Last Login Date  : Thu Jan 17 13:26:04 2019 Z
Pwd Reset Date   : Fri Jan 11 15:25:05 2019 Z
Pwd Fail Date    : Fri Jan 11 20:30:15 2019 Z
Login Count      : 7
```

TABLE 1

Question: 10	Category: System

Question 10: What is the assigned IP address of the subject computer?

Manufacturer's Expected Response: 192.168.189.132

WebCode	Response
32LYBW-5562	192.168.189.132
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	192.168.189.132
682GJP-5562	192.168.189.132
6Z4RZY-5561	192.168.189.132
9LB7BM-5562	192.168.189.132
AP6K9W-5562	192.168.189.132
C97GKM-5561	192.168.189.132
CMBD4P-5561	192.168.189.2
CPHTCG-5561	192.168.189.132
D9NRUF-5562	192.168.189.132
EP84ZE-5562	192.168.189.132
H6CDEC-5561	192.168.189.2
J3ZUA9-5561	192.168.189.132
JLWJ4G-5562	192.168.189.132
K3E3B9-5561	192.168.189.132 ("Windows\System32\config\SYSTEM"
L6WGE9-5561	192.168.189.132
MUUH6E-5561	192.168.189.132
NBXF34-5561	192.168.189.132
NFT79E-5562	192.168.189.132
NMCAFG-5561	192.168.189.132
Q2K3Y6-5562	192.168.189.132
QL9NG8-5561	192.168.189.132
QVYAM6-5562	192.168.132
RTPJX2-5561	192.168.189.132

TABLE 1

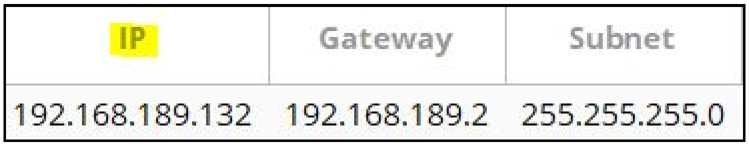
Question: 10	Category: System
WebCode	**Response**
V292YY-5561	192.168.189.132
WJ4UKW-5561	192.168.189.132
X4PZAY-5562	192.168.189.132
XDC2Q9-5561	192.168.189.132
XE36GV-5561	192.168.189.132
YN48YX-5562	192.168.189.132
YUVEG7-5561	192.228.79.201
ZMBJCV-5562	192.168.189.132

Question 10: What is the assigned IP address of the subject computer?

Consensus Result: 192.168.189.132

Expected Response Explanation:
Information regarding the IP address assigned to this computer can be sourced from the System hive at the following location: ControlSet001\Services\Tcpip\Parameters\

Screen Shot:
Parameters:



IP	Gateway	Subnet
192.168.189.132	192.168.189.2	255.255.255.0

TABLE 1

Question: 11	Category: System

Question 11: How many files are in the Recycle Bin?

Manufacturer's Expected Response: Two (2)

WebCode	Response
32LYBW-5562	2
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	Two (02) Files
682GJP-5562	2
6Z4RZY-5561	2
9LB7BM-5562	2
AP6K9W-5562	2
C97GKM-5561	2
CMBD4P-5561	6 files
CPHTCG-5561	2
D9NRUF-5562	2 text (1x RTF 1x .txt) files (And additionally 2x desktop.ini and 2x $xxx recycler files)
EP84ZE-5562	5, including the desktop.ini file for SID 1000 (Morgan Chen), just the desktop.ini file in SID 1001 (Kids)
H6CDEC-5561	2
J3ZUA9-5561	2
JLWJ4G-5562	2
K3E3B9-5561	2 files are in the Recycle Bin. “Olivia Letters.txt” y “Absence Note.rtf”. Both from the Morgan Chen's Desktop
L6WGE9-5561	7
MUUH6E-5561	2
NBXF34-5561	2
NFT79E-5562	two files
NMCAFG-5561	Two (2)
Q2K3Y6-5562	4
QL9NG8-5561	2
QVYAM6-5562	The SID ending with 1000 has seven files and the SID ending with 1001 has the destop .ini. If you looking for Morgan Chen, actual document that is deleted gets start with $R therefore the answer is 11 files.
RTPJX2-5561	2

TABLE 1

Question: 11 **Category: System**

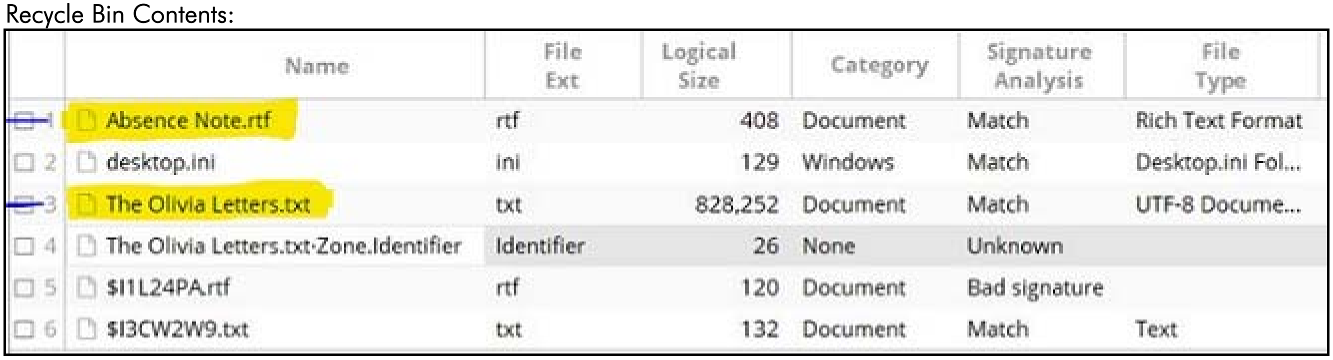
WebCode	Response
V292YY-5561	2 user deleted files If system files are also included there are 7 files, which included both deleted documents ($R1L24PA.rtf and $R3CW2W9.txt), the information files associated with each deleted document ($I1L24PA.rtf and $I3CW2W9.txt), two initialization files (desktop.ini), and one alternate datastream file (zone.Identifier).
WJ4UKW-5561	2
X4PZAY-5562	2
XDC2Q9-5561	2
XE36GV-5561	Two
YN48YX-5562	2
YUVEG7-5561	2 files
ZMBJCV-5562	5

Question 11: How many files are in the Recycle Bin?

Consensus Result: Two (2)

Expected Response Explanation:
The intention of this question was to have participants report only the files deleted by the user. This information is found in the recycle bin folder.

Screen Shot:
Recycle Bin Contents:



	Name	File Ext	Logical Size	Category	Signature Analysis	File Type
☑ 1	Absence Note.rtf	rtf	408	Document	Match	Rich Text Format
□ 2	desktop.ini	ini	129	Windows	Match	Desktop.ini Fol...
☑ 3	The Olivia Letters.txt	txt	828,252	Document	Match	UTF-8 Docume...
□ 4	The Olivia Letters.txt·Zone.Identifier	Identifier	26	None	Unknown	
□ 5	$I1L24PA.rtf	rtf	120	Document	Bad signature	
□ 6	$I3CW2W9.txt	txt	132	Document	Match	Text

Other Responses:
Six participants reported a value greater than two (2). Some participants included I$ files and desktop.ini files as part of their count.

TABLE 1

Question: 12 **Category: System**

Question 12: Provide the name of the most recently viewed document. (pdf, xls, docx, rtf)

Manufacturer's Expected Response: Julie_Chen - LastWill.docx

WebCode	Response
32LYBW-5562	Julie_Chen - LastWill.docx
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	Julie_Chen - LastWill.docx
682GJP-5562	Julie_Chen - LastWill.docx
6Z4RZY-5561	Gmail - Finalized Will.pdf
9LB7BM-5562	Julie_Chen - LastWill.docx
AP6K9W-5562	Julie_chen-last will.docx
C97GKM-5561	Julie_Chen - LastWill.docx
CMBD4P-5561	Julie Chen Last Will.docx
CPHTCG-5561	Julie_Chen - LastWill.docx
D9NRUF-5562	Julie_Chen - LastWill.docx
EP84ZE-5562	decimals.pdf, Julie_Chen - LastWill.docx, Absence Note.rtf
H6CDEC-5561	PDF - decimals, XLS - MsoIrmProtector, DOCX - Julie_Chen - LastWill, RTF - Absence Note
J3ZUA9-5561	Julie_Chen - LastWill.docx
JLWJ4G-5562	Julie_Chen - LastWill.docx
K3E3B9-5561	“Julie_Chen -LastWill.docx”, “Abscense Note.rtf”, “decimals.pdf”. (“\Users\Morgan Chen\NTUSER.dat”)
L6WGE9-5561	Julie_Chen - LastWill.docx
MUUH6E-5561	Julie_Chen - LastWill.docx
NBXF34-5561	Julie_Chen - LastWill.docx
NFT79E-5562	« Julie_Chen - LastWill.docx "
NMCAFG-5561	Julie_Chen - LastWill.docx
Q2K3Y6-5562	Julie_Chen - LastWill.docx
QL9NG8-5561	Julie_Chen - LastWill.docx
QVYAM6-5562	Julie_Chen - Last Will
RTPJX2-5561	Julie_Chen - LastWill.docx

TABLE 1

Question: 12 **Category: System**

WebCode	Response
V292YY-5561	Julie_Chen - Lastwill.docx
WJ4UKW-5561	Julie_Chen - LastWill.docx
X4PZAY-5562	Julie_Chen - LastWill.docx
XDC2Q9-5561	Julie_Chen - Last Will.docx
XE36GV-5561	Julie_Chen - LastWill.docx
YN48YX-5562	Julie_Chen - LastWill.docx
YUVEG7-5561	decimals.pdf, Julie_Chen - LastWill.docx, Absense Note.rtf
ZMBJCV-5562	"Julie_Chen - LastWill.docx"

Question 12: Provide the name of the most recently viewed document. (pdf, xls, docx, rtf)

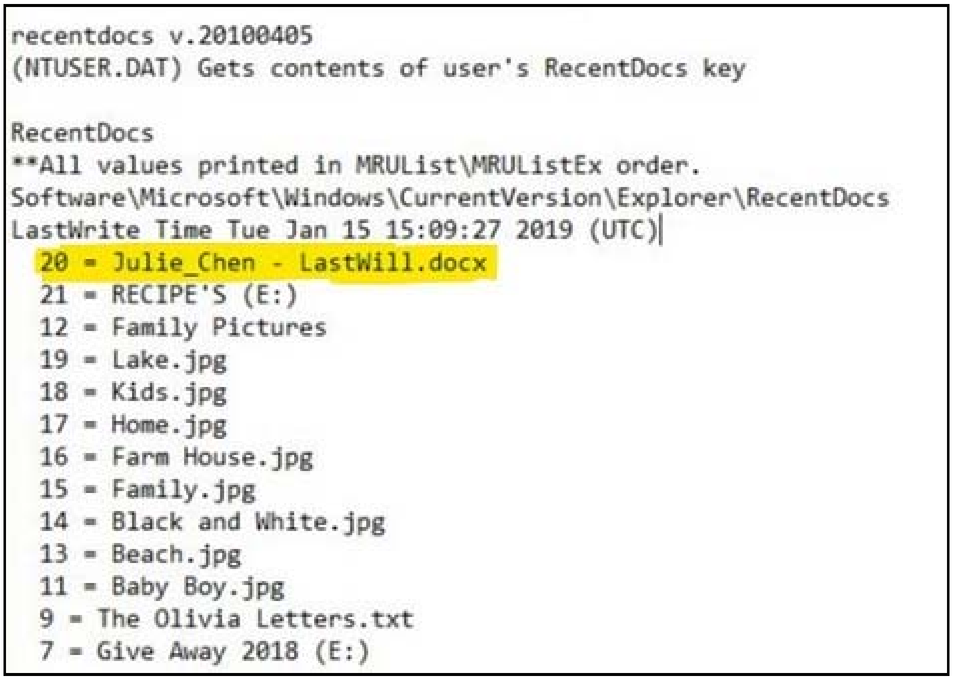
Consensus Result: Julie_Chen - LastWill.docx

Expected Response Explanation:

Information regarding the name of the most recently viewed document can be found at the following location: C:\Users\Morgan Chen\NTUSER.DAT\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.docx

Screen Shot:

Recent Docs:



```
recentdocs v.20100405
(NTUSER.DAT) Gets contents of user's RecentDocs key

RecentDocs
**All values printed in MRUList\MRUListEx order.
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
LastWrite Time Tue Jan 15 15:09:27 2019 (UTC)
  20 = Julie_Chen - LastWill.docx
  21 = RECIPE'S (E:)
  12 = Family Pictures
  19 = Lake.jpg
  18 = Kids.jpg
  17 = Home.jpg
  16 = Farm House.jpg
  15 = Family.jpg
  14 = Black and White.jpg
  13 = Beach.jpg
  11 = Baby Boy.jpg
  9 = The Olivia Letters.txt
  7 = Give Away 2018 (E:)
```

TABLE 1

Question: 13	Category: System

Question 13: What feature of Windows records execution of programs (and their parameters) to speed up the application's start up process?

Manufacturer's Expected Response: Prefetch

WebCode	Response
32LYBW-5562	Prefetch
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	Prefetch
682GJP-5562	UserAssist
6Z4RZY-5561	Prefetch Files
9LB7BM-5562	Prefetch
AP6K9W-5562	Prefetch, as default it's only available for boot prefetching
C97GKM-5561	Prefetch
CMBD4P-5561	Prefetch
CPHTCG-5561	Prefetch
D9NRUF-5562	Prefetch
EP84ZE-5562	Prefetch
H6CDEC-5561	Prefetch
J3ZUA9-5561	Prefetch
JLWJ4G-5562	Windows Prefetch
K3E3B9-5561	The feature of windows that records execution of programas to speed up the application's start up process is: Prefecth.
L6WGE9-5561	Superfetch
MUUH6E-5561	Prefetch Files
NBXF34-5561	Prefetch
NFT79E-5562	The startup manager
NMCAFG-5561	prefetch
Q2K3Y6-5562	Jump Lists
QL9NG8-5561	Prefetch File
QVYAM6-5562	Prefetch Files. It records the loading order of files and then maps that info for retrieval the next time the file is loaded. Prefetch enhances the speed of loading by storing the order of pages ahead of time in memory; hence the name Prefetch.

TABLE 1

Question: 13	Category: System
WebCode	**Response**
RTPJX2-5561	Prefetch
V292YY-5561	Prefetch
WJ4UKW-5561	Prefetch files
X4PZAY-5562	Prefetch
XDC2Q9-5561	Prefetch
XE36GV-5561	Prefetch
YN48YX-5562	Prefetch
YUVEG7-5561	Startup
ZMBJCV-5562	Prefetch

Question 13: What feature of Windows records execution of programs (and their parameters) to speed up the application's start up process?

Consensus Result: Prefetch

Expected Response Explanation:
The prefetch files are found within the prefetch folder at C:\Windows\Prefetch

TABLE 1

Question: 14	Category: Application

Question 14: How many pages were bookmarked on Chrome?

Manufacturer's Expected Response: Four (4)

WebCode	Response
32LYBW-5562	4
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	Four (04) pages
682GJP-5562	4
6Z4RZY-5561	4
9LB7BM-5562	4
AP6K9W-5562	4
C97GKM-5561	4
CMBD4P-5561	4
CPHTCG-5561	4
D9NRUF-5562	4
EP84ZE-5562	4
H6CDEC-5561	4
J3ZUA9-5561	4
JLWJ4G-5562	4
K3E3B9-5561	4 pages were bookmarked: www.cnn.com, www.buzzfeed.com, www.facebook.com, www.pinterest.com
L6WGE9-5561	0
MUUH6E-5561	4
NBXF34-5561	4
NFT79E-5562	4
NMCAFG-5561	Four (4)
Q2K3Y6-5562	4
QL9NG8-5561	4
QVYAM6-5562	Eight
RTPJX2-5561	4

TABLE 1

Question: 14 **Category: Application**

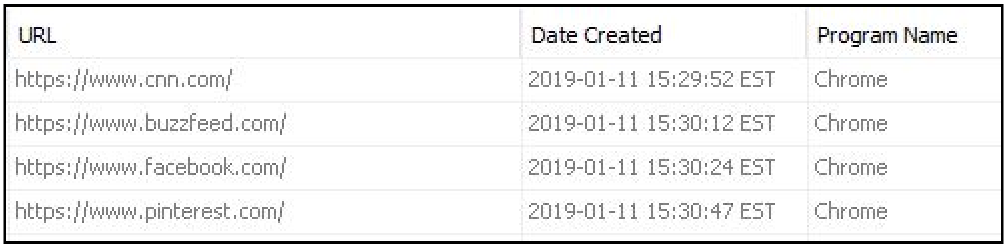
WebCode	Response
V292YY-5561	4
WJ4UKW-5561	4
X4PZAY-5562	4
XDC2Q9-5561	4
XE36GV-5561	Four
YN48YX-5562	4
YUVEG7-5561	4 pages
ZMBJCV-5562	4

Question 14: How many pages were bookmarked on Chrome?

Consensus Result: Four (4)

Expected Response Explanation:
Information regarding the pages bookmarked on Chrome can be found at the following location: C:\Users\Morgan Chen\AppData\Local\Google\Chrome\UserData\Default\Bookmarks

Screen Shot:
Chrome Bookmarks:



URL	Date Created	Program Name
https://www.cnn.com/	2019-01-11 15:29:52 EST	Chrome
https://www.buzzfeed.com/	2019-01-11 15:30:12 EST	Chrome
https://www.facebook.com/	2019-01-11 15:30:24 EST	Chrome
https://www.pinterest.com/	2019-01-11 15:30:47 EST	Chrome

TABLE 1

Question: 15	Category: Application

Question 15: Provide the last term searched using Google Chrome on this device?

Manufacturer's Expected Response: probate process in new jersey

WebCode	Response
32LYBW-5562	probate process in new jersey
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	probate process in new jersey
682GJP-5562	probate process in new jersey
6Z4RZY-5561	probate process in new jersey
9LB7BM-5562	probate process in new jersey
AP6K9W-5562	Probate Process in New Jersey
C97GKM-5561	probate process in new jersey
CMBD4P-5561	Probate process in New Jersey
CPHTCG-5561	probate process in new jersey
D9NRUF-5562	probate process in new jersey
EP84ZE-5562	"probate process in new jersey"
H6CDEC-5561	probate process in new jersey
J3ZUA9-5561	probate process in new jersey
JLWJ4G-5562	probate process in new jersey
K3E3B9-5561	Probate process in new jersey. It was searched on 01/15/2019 17:16:56
L6WGE9-5561	probate process in new jersey
MUUH6E-5561	probate process in new jersey
NBXF34-5561	probate process in new jersey
NFT79E-5562	“navy credit union”
NMCAFG-5561	probate process in new jersey
Q2K3Y6-5562	probate process in new jersey
QL9NG8-5561	probate process in new jersey
QVYAM6-5562	NAVY credit union
RTPJX2-5561	probate process in new jersey

TABLE 1

Question: 15 **Category: Application**

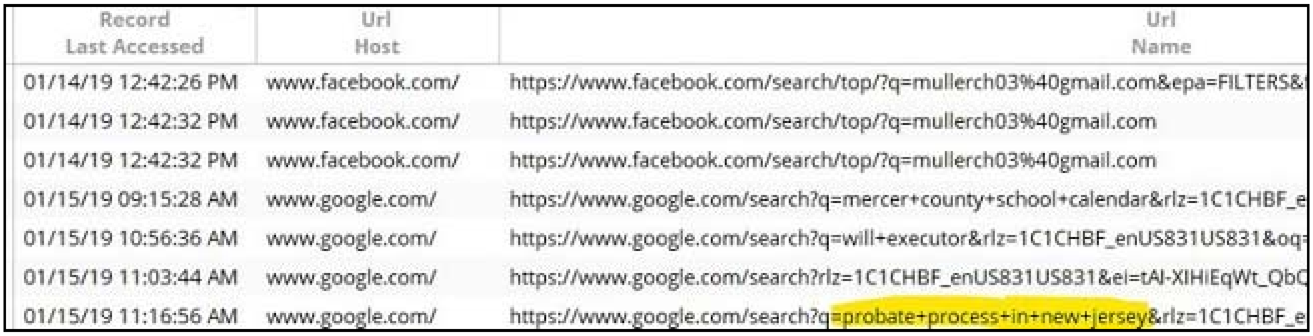
WebCode	Response
V292YY-5561	probate process in new jersey
WJ4UKW-5561	probate process in new jersey
X4PZAY-5562	probate process in new jersey
XDC2Q9-5561	probate process in New Jersey
XE36GV-5561	probate process in new jersey
YN48YX-5562	probate process in new jersey
YUVEG7-5561	probate process in new jersey - Google Search
ZMBJCV-5562	"probate process in new jersey"

Question 15: Provide the last term searched using Google Chrome on this device?

Consensus Result: probate process in new jersey

Expected Response Explanation:
Information regarding the last term searched using Google Chrome can be found at the following location: C:\Users\Morgan Chen\AppData\Local\Google\Chrome\UserData\Default\History

Screen Shot:
Searched Terms:



Record Last Accessed	Url Host	Url Name
01/14/19 12:42:26 PM	www.facebook.com/	https://www.facebook.com/search/top/?q=mullerch03%40gmail.com&epa=FILTERS&
01/14/19 12:42:32 PM	www.facebook.com/	https://www.facebook.com/search/top/?q=mullerch03%40gmail.com
01/14/19 12:42:32 PM	www.facebook.com/	https://www.facebook.com/search/top/?q=mullerch03%40gmail.com
01/15/19 09:15:28 AM	www.google.com/	https://www.google.com/search?q=mercer+county+school+calendar&rlz=1C1CHBF_e
01/15/19 10:56:36 AM	www.google.com/	https://www.google.com/search?q=will+executor&rlz=1C1CHBF_enUS831US831&oq
01/15/19 11:03:44 AM	www.google.com/	https://www.google.com/search?rlz=1C1CHBF_enUS831US831&ei=tAl-XIHiEqWt_QbC
01/15/19 11:16:56 AM	www.google.com/	https://www.google.com/search?q=probate+process+in+new+jersey&rlz=1C1CHBF_e

TABLE 1

Question: 16	Category: Application

Question 16: What email application was used to send and receive emails?

Manufacturer's Expected Response: Thunderbird or Mozilla Thunderbird

WebCode	Response
32LYBW-5562	Mozilla Thunderbird
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	Mozilla Thunderbird
682GJP-5562	Mozilla Thunderbird
6Z4RZY-5561	Mozilla Thunderbird
9LB7BM-5562	Thunderbird
AP6K9W-5562	Gmail
C97GKM-5561	Mozilla Thunderbird
CMBD4P-5561	Mozilla Thunderbird
CPHTCG-5561	Thunderbird
D9NRUF-5562	Thunderbird
EP84ZE-5562	Thunderbird
H6CDEC-5561	Thunderbird
J3ZUA9-5561	Thunderbird
JLWJ4G-5562	Mozilla Thunderbird
K3E3B9-5561	Thunderbird. Installed on ("\Program File (x86)\").
L6WGE9-5561	Mozilla Thunderbird
MUUH6E-5561	Mozilla Thunderbird
NBXF34-5561	Thunderbird
NFT79E-5562	Thunderbird
NMCAFG-5561	Mozilla Thunderbird 60.4.0 (x86 en-US)
Q2K3Y6-5562	MBox
QL9NG8-5561	Mozilla Thunderbird
QVYAM6-5562	Gmail
RTPJX2-5561	Thunderbird

TABLE 1

Question: 16 **Category: Application**

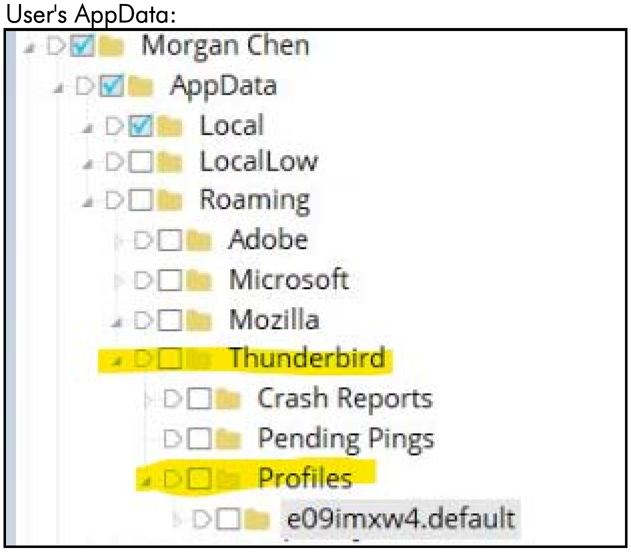
WebCode	Response
V292YY-5561	Thunderbird
WJ4UKW-5561	gmail
X4PZAY-5562	Mozilla Thunderbird
XDC2Q9-5561	Thunderbird
XE36GV-5561	Thunderbird
YN48YX-5562	Thunderbird
YUVEG7-5561	Gmail application
ZMBJCV-5562	Mozilla Thunderbird 60.4.0

Question 16: What email application was used to send and receive emails?

Consensus Result: Thunderbird or Mozilla Thunderbird

Expected Response Explanation:
Information regarding the email application used to send and receive emails can be found at the following location: C:\Users\Morgan Chen\AppData\Roaming\Thunderbird\Profiles

Screen Shot:
User's AppData:



```
☑ Morgan Chen
  ☑ AppData
    ☑ Local
    □ LocalLow
    □ Roaming
      □ Adobe
      □ Microsoft
      □ Mozilla
      □ Thunderbird
        □ Crash Reports
        □ Pending Pings
        □ Profiles
          □ e09imxw4.default
```

TABLE 1

Question: 17 **Category: Application**

Question 17: What is the Gmail email address associated to the primary user on this device?

Manufacturer's Expected Response: chenmorgan01@gmail.com

WebCode	Response
32LYBW-5562	chenmorgan01@gmail.com
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	chenmorgan01@gmail.com
682GJP-5562	chenmorgan01@gmail.com
6Z4RZY-5561	Mozilla Thunderbird
9LB7BM-5562	chenmorgan01@gmail.com
AP6K9W-5562	chenmorgan01@gmail.com
C97GKM-5561	chenmorgan01@gmail.com
CMBD4P-5561	chenmorgan01@gmail.com
CPHTCG-5561	chenmorgan01@gmail.com
D9NRUF-5562	Chenmorgan01@gmail.com
EP84ZE-5562	chenmorgan01@gmail.com
H6CDEC-5561	chenmorgan01@gmail.com
J3ZUA9-5561	chenmorgan01@gmail.com
JLWJ4G-5562	chenmorgan01@gmail.com
K3E3B9-5561	chenmorgan01@gmail.com obtained from ("\Users\Morgan Chen\AppData\Roaming\Thunderbird\Profiles\")
L6WGE9-5561	chenmorgan01@gmail.com
MUUH6E-5561	chenmorgan01@gmail.com
NBXF34-5561	chenmorgan01@gmail.com
NFT79E-5562	« chenmorgan01@gmail.com »
NMCAFG-5561	chenmorgan01@gmail.com
Q2K3Y6-5562	chenmorgan01@gmail.com
QL9NG8-5561	chenmorgan01@gmail.com
QVYAM6-5562	chenmorgan01@gmail.com
RTPJX2-5561	chenmorgan01@gmail.com

TABLE 1

Question: 17	Category: Application
WebCode	**Response**
V292YY-5561	chenmorgan01@gmail.com
WJ4UKW-5561	chenmorgan01@gmail.com
X4PZAY-5562	chenmorgan01@gmail.com
XDC2Q9-5561	chenmorgan01@gmail.com
XE36GV-5561	chenmorgan01@gmail.com
YN48YX-5562	chenmorgan01@gmail.com
YUVEG7-5561	chenmorgan01@gmail.com
ZMBJCV-5562	"chenmorgan01@gmail.com"

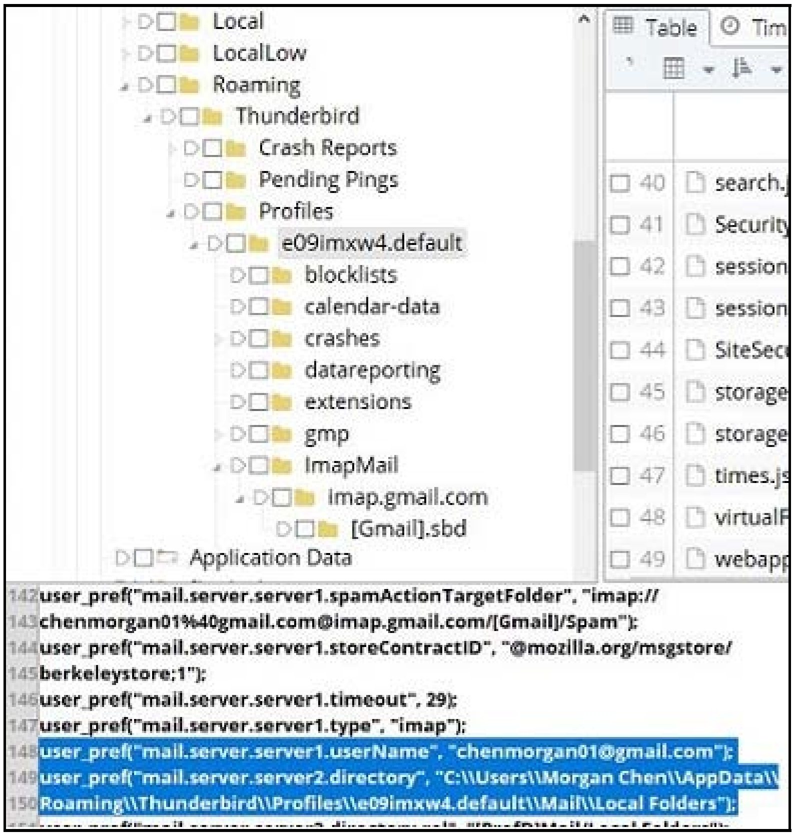
Question 17: What is the Gmail email address associated to the primary user on this device?

Consensus Result: chenmorgan01@gmail.com

Expected Response Explanation:
Information regarding the Gmail email address associated with the primary user on this device can be found at the following location: C:\Users\Morgan Chen\AppData\Roaming\Thunderbird\Profiles\e09imxw4.default\pref.js

Screen Shot:

Preferences:



```
user_pref("mail.server.server1.spamActionTargetFolder", "imap://
chenmorgan01%40gmail.com@imap.gmail.com/[Gmail]/Spam");
user_pref("mail.server.server1.storeContractID", "@mozilla.org/msgstore/
berkeleystore;1");
user_pref("mail.server.server1.timeout", 29);
user_pref("mail.server.server1.type", "imap");
user_pref("mail.server.server1.userName", "chenmorgan01@gmail.com");
user_pref("mail.server.server2.directory", "C:\\Users\\Morgan Chen\\AppData\\
Roaming\\Thunderbird\\Profiles\\e09imxw4.default\\Mail\\Local Folders");
```

TABLE 1

Question: 18 Category: Application

Question 18: An email was sent to "Laurelmurray63@gmail.com" on 01/14/2019 at 01:19 PM. Provide the subject of that email.

Manufacturer's Expected Response: Hey Girl

WebCode	Response
32LYBW-5562	Hey Girl
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	Hey Girl
682GJP-5562	Hey Girl
6Z4RZY-5561	Hey Girl
9LB7BM-5562	Hey Girl
AP6K9W-5562	Hey Girl
C97GKM-5561	Hey Girl
CMBD4P-5561	Hey Girl
CPHTCG-5561	Hey Girl
D9NRUF-5562	Hey Girl
EP84ZE-5562	Hey Girl
H6CDEC-5561	Hey Girl
J3ZUA9-5561	Hey Girl
JLWJ4G-5562	Hey Girl
K3E3B9-5561	Hey Girl. obtained from (“\Users\Morgan Chen\AppData\Roaming\Thunderbird\Profiles\e09imxw4.default\ImapMail\imap.gmail.com\[G mail].sbd\Sent Mail”).
L6WGE9-5561	Hey Girl
MUUH6E-5561	Hey Girl
NBXF34-5561	Hey Girl
NFT79E-5562	« Hey Girl »
NMCAFG-5561	Hey Girl
Q2K3Y6-5562	Hey Girl
QL9NG8-5561	Hey Girl
QVYAM6-5562	Hey Girl

TABLE 1

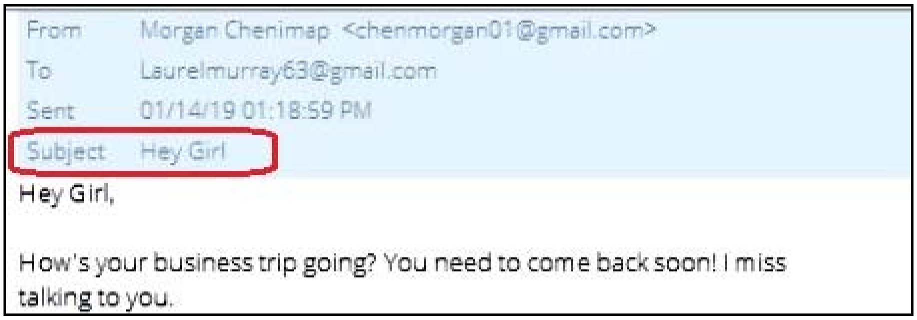
Question: 18	Category: Application
WebCode	**Response**
RTPJX2-5561	Hey Girl
V292YY-5561	Hey Girl
WJ4UKW-5561	Hey Girl
X4PZAY-5562	Hey Girl
XDC2Q9-5561	Hey Girl
XE36GV-5561	Hey Girl
YN48YX-5562	Hey Girl
YUVEG7-5561	Hey Girl
ZMBJCV-5562	"Hey Girl"

Question 18: An email was sent to "Laurelmurray63@gmail.com" on 01/14/2019 at 01:19 PM. Provide the subject of that email.

Consensus Result: Hey Girl

Expected Response Explanation:
Information regarding the subject of a sent email can be found at the following location: C:\Users\Morgan Chen\AppData\Roaming\Thunderbird\Profiles\e09imxw4.default\ImapMail\imap.gmail.com\[Gmail].sbd\All Mail

Screen Shot:
Email:



From Morgan Chenimap <chenmorgan01@gmail.com>
To Laurelmurray63@gmail.com
Sent 01/14/19 01:18:59 PM
Subject Hey Girl

Hey Girl,

How's your business trip going? You need to come back soon! I miss talking to you.

TABLE 1

Question: 19	Category: Application

Question 19: What is the primary user's physical (home) address? Provide the Building number, Street Name, City, and State

Manufacturer's Expected Response: 16925 Shaw Road, Trenton, New Jersey

WebCode	Response
32LYBW-5562	16925 Shaw Road, Trenton, New Jersey 08666
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	16925 Shaw Road, Trenton, New Jersey 08666
682GJP-5562	16925 Shaw Road, Trenton, New Jersey 08666
6Z4RZY-5561	16925 Shaw Road, Trenton, New Jersey 08666
9LB7BM-5562	16925 Shaw Road, Trenton, New Jersey
AP6K9W-5562	16925 Shaw Road, Trenton, New Jersey, 08666
C97GKM-5561	16925 Shaw Road, Trenton, New Jersey 08666
CMBD4P-5561	16925 Shaw Road, Trenton, New Jersey 08666
CPHTCG-5561	16925 Shaw Road, Trenton, New Jersey 08666
D9NRUF-5562	16925 Shaw Road, Trenton, New Jersey 08666
EP84ZE-5562	16925 Shaw Road, Trenton, New Jersey 08666
H6CDEC-5561	Morgan Chen 16925 Shaw Road Trenton New Jersey 08666 - Morgan Chen is a user account; however, you can not say who physically used that account.
J3ZUA9-5561	16925 Shaw Road, Trenton, New Jersey
JLWJ4G-5562	16925 Shaw Road, Trenton, New Jersey 08666
K3E3B9-5561	"16925 Shaw Road, Trenton, New Jersey, 08666" obtained from reviewing the "User\Morgan Chen\Desktop\Julie_Chen – LastWill.docx"
L6WGE9-5561	2415 Grover Place, Trenton, New Jersey 08666
MUUH6E-5561	16925, Shaw Road, Trenton, New Jersey
NBXF34-5561	16925 Shaw Road, Trenton, New Jersey
NFT79E-5562	16925 Shaw Road, Trenton, New Jersey 08666.
NMCAFG-5561	16925 Shaw Road, Trenton, New Jersey
Q2K3Y6-5562	16925 Shaw Road, Trenton, New Jersey 08666
QL9NG8-5561	16925 Shaw Road, Trenton, New Jersey 08666
QVYAM6-5562	16925 Shaw Road, Trenton, New Jersey 08666
RTPJX2-5561	16925 Shaw Road, Trenton, New Jersey

TABLE 1

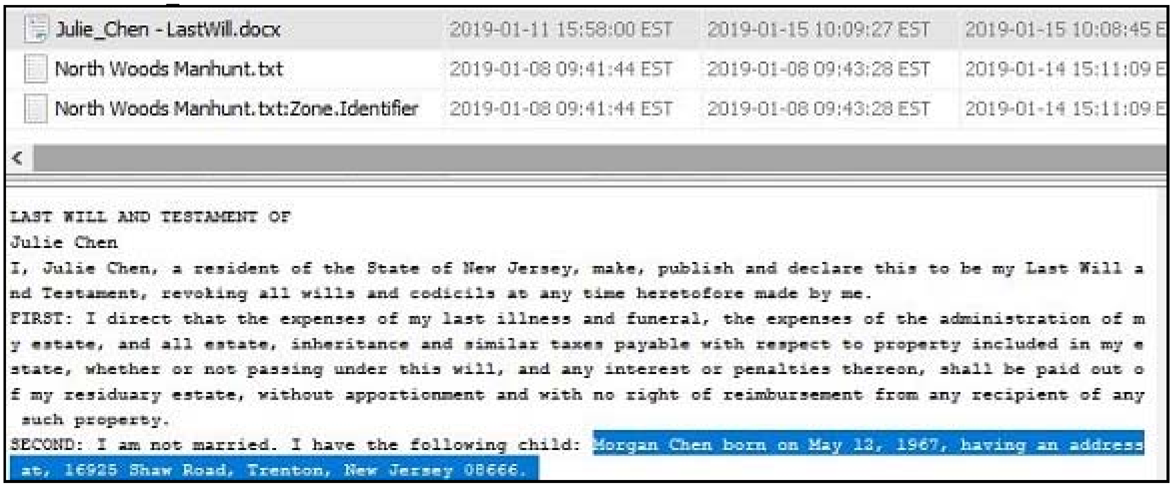
Question: 19	Category: Application
WebCode	**Response**
V292YY-5561	16925 Shaw Road, Trenton, New Jersey 08666
WJ4UKW-5561	16925 Shaw Road, Trenton, New Jersey 08666
X4PZAY-5562	16925 Shaw Road, Trenton, New Jersey 08666
XDC2Q9-5561	16925 Shaw Road, Trenton, New Jersey
XE36GV-5561	16925 Shaw Road, Trenton, NJ 08666
YN48YX-5562	16925 Shaw Road, Trenton, New Jersey 08666
YUVEG7-5561	16925 Shaw Road, Trenton, New Jersey 08666
ZMBJCV-5562	"16925 Shaw Road, Trenton, New Jersey 08666"

Question 19: What is the primary user's physical (home) address? Provide the Building number, Street Name, City, and State

Consensus Result: 16925 Shaw Road, Trenton, New Jersey 08666

Expected Response Explanation:
The primary user's physical address can be sourced from the body of text within the document titled "Julie_Chen - LastWill.docx".

Screen Shot:
Text from "Julie_Chen - LastWill.docx":



```
Julie_Chen - LastWill.docx                   2019-01-11 15:58:00 EST   2019-01-15 10:09:27 EST   2019-01-15 10:08:45 E
North Woods Manhunt.txt                      2019-01-08 09:41:44 EST   2019-01-08 09:43:28 EST   2019-01-14 15:11:09 E
North Woods Manhunt.txt:Zone.Identifier      2019-01-08 09:41:44 EST   2019-01-08 09:43:28 EST   2019-01-14 15:11:09 E
```

```
LAST WILL AND TESTAMENT OF
Julie Chen
I, Julie Chen, a resident of the State of New Jersey, make, publish and declare this to be my Last Will a
nd Testament, revoking all wills and codicils at any time heretofore made by me.
FIRST: I direct that the expenses of my last illness and funeral, the expenses of the administration of m
y estate, and all estate, inheritance and similar taxes payable with respect to property included in my e
state, whether or not passing under this will, and any interest or penalties thereon, shall be paid out o
f my residuary estate, without apportionment and with no right of reimbursement from any recipient of any
 such property.
SECOND: I am not married. I have the following child: Morgan Chen born on May 12, 1967, having an address
 at, 16925 Shaw Road, Trenton, New Jersey 08666.
```

TABLE 1

Question: 20 Category: Application

Question 20: When was "notepad.exe" last executed? Provide the answer in the UTC + 00:00 using the following format: MM/DD/YYYY HH:MM:SS AM/PM.

Manufacturer's Expected Response: 01/14/2019 08:15:39 PM

WebCode	Response	** Inconsistencies not highlighted; No consensus achieved **
32LYBW-5562	1/14/2019 8:15:39 PM	
3VUW4Q-5562	[Participant did not return results for this question.]	
4RQFAT-5562	01/14/2019 08:36:09 PM (by user "Kids")	
682GJP-5562	01/14/2019 08:15:39 PM	
6Z4RZY-5561	01/17/2019 06:50:32 PM	
9LB7BM-5562	01/14/2019 08:15:39 PM	
AP6K9W-5562	01/14/2019 20:15:39 +1:00	
C97GKM-5561	01/14/2019 08:15:39 PM	
CMBD4P-5561	01/14/2019 08:36:09 PM	
CPHTCG-5561	01/14/2019 08:36:09 PM	
D9NRUF-5562	01/14/2019 08:15:39 PM	
EP84ZE-5562	01/14/2019 20:15:39 UTC	
H6CDEC-5561	03/18/2017 20:58:25 UTC	
J3ZUA9-5561	01/14/2019 08:36:09 PM	
JLWJ4G-5562	01/14/2019 08:36:09 PM	
K3E3B9-5561	01/14/2019 08:15:39 PM (“Windows\Prefetch\NOTEPAD.EXE-C5670914.pf”)	
L6WGE9-5561	01/14/2019 09:15:39 PM	
MUUH6E-5561	01/14/2019 08:36:09 PM	
NBXF34-5561	01/14/2019 08:36:09 PM	
NFT79E-5562	01/14/2019 20:36:09 PM.	
NMCAFG-5561	01/14/2019 08:36:09 PM	
Q2K3Y6-5562	1/14/2019 03:15:39 PM	
QL9NG8-5561	01/14/2019 08:36:09 PM	
QVYAM6-5562	03/18/2017 20:58:58 PM	
RTPJX2-5561	1/14/2019 8:36:09 PM	

TABLE 1

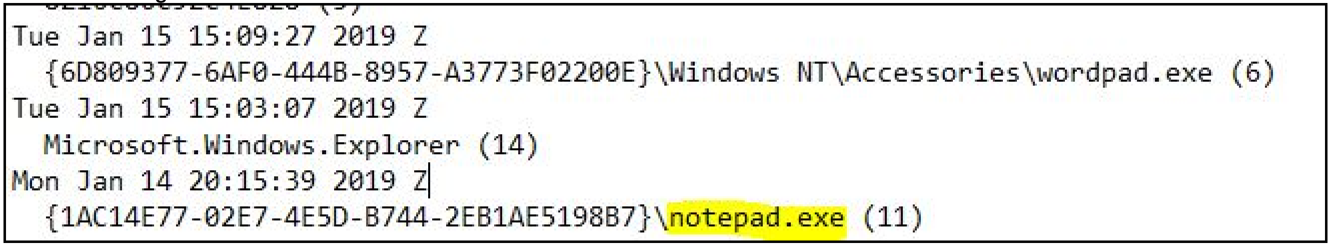
Question: 20	Category: Application
WebCode	**Response** ** Inconsistencies not highlighted; No consensus achieved **
V292YY-5561	01/14/2019 08:36:09 PM UTC for Kids user account. 01/14/2019 08:15:39 PM UTC for Morgan Chen user account
WJ4UKW-5561	01/14/2019 08:15:40 PM UTC
X4PZAY-5562	01/14/2019 8:15:39 PM
XDC2Q9-5561	01/14/2019 08:11:00 PM
XE36GV-5561	01/14/2019 8:15:39 PM
YN48YX-5562	1/14/2019 8:15:39 PM
YUVEG7-5561	01/14/19 08:15:39 PM.
ZMBJCV-5562	01/14/2019 08:15:39 PM

Question 20: When was "notepad.exe" last executed? Provide the answer in the UTC + 00:00 using the following format: MM/DD/YYYY HH:MM:SS AM/PM.

Consensus Result: A consensus was not achieved. Approximately 42% of participants reported the expected date and time of 01/14/2019, 08:15:39 PM.

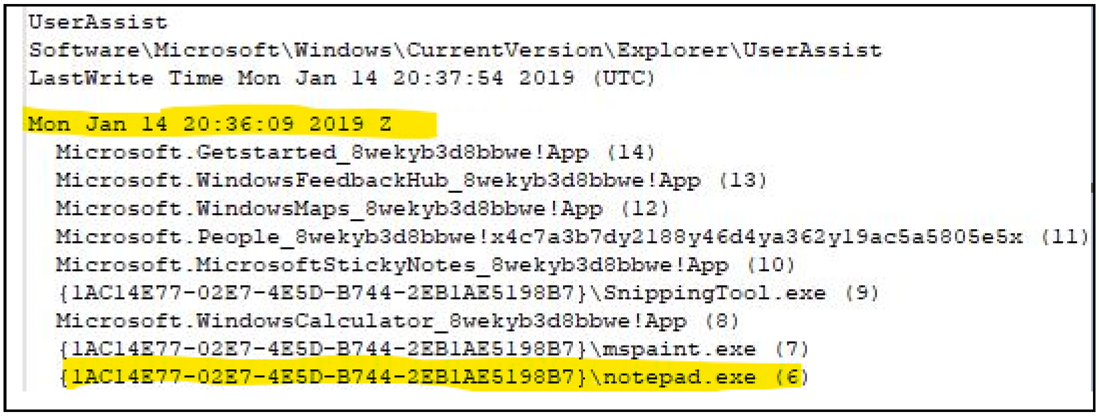
Expected Response Explanation:
Information regarding the date/time "notepad.exe" last executed can be found at the following location:
C:\Users\Morgan Chen\NTUSER.DAT

Screen Shot:
C:\Users\Morgan Chen\NTUSER.DAT:



```
Tue Jan 15 15:09:27 2019 Z
  {6D809377-6AF0-444B-8957-A3773F02200E}\Windows NT\Accessories\wordpad.exe (6)
Tue Jan 15 15:03:07 2019 Z
  Microsoft.Windows.Explorer (14)
Mon Jan 14 20:15:39 2019 Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\notepad.exe (11)
```

Other Responses:
Some participants (35%) reported the expected date but a time of 08:36:09 PM. Two participants mentioned that this time was related to the Kids user account.
C:\Users\Kids\NTUSER.DAT:



```
UserAssist
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
LastWrite Time Mon Jan 14 20:37:54 2019 (UTC)

Mon Jan 14 20:36:09 2019 Z
  Microsoft.Getstarted_8wekyb3d8bbwe!App (14)
  Microsoft.WindowsFeedbackHub_8wekyb3d8bbwe!App (13)
  Microsoft.WindowsMaps_8wekyb3d8bbwe!App (12)
  Microsoft.People_8wekyb3d8bbwe!x4c7a3b7dy2188y46d4ya362y19ac5a5805e5x (11)
  Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe!App (10)
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\SnippingTool.exe (9)
  Microsoft.WindowsCalculator_8wekyb3d8bbwe!App (8)
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\mspaint.exe (7)
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\notepad.exe (6)
```

TABLE 1

Question: 21 Category: Application

Question 21: How many times was "mspaint.exe" executed?

Manufacturer's Expected Response: Seven (7)

WebCode	Response
32LYBW-5562	7
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	Morgan Chen Seven (07) times Kids Seven (07) Times
682GJP-5562	0
6Z4RZY-5561	4
9LB7BM-5562	14
AP6K9W-5562	7 by both users
C97GKM-5561	7
CMBD4P-5561	7
CPHTCG-5561	14
D9NRUF-5562	0
EP84ZE-5562	7 times by user "Kids", 7 times by user "Morgan Chen"
H6CDEC-5561	0
J3ZUA9-5561	14
JLWJ4G-5562	14
K3E3B9-5561	7 times. It is found on the NTUSER.DAT, from accocunts "Morgan Chen" y "Kids", On the hive we find the Count ("Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CDACE2-4F4F-9178-9926F41749EA}\Count")
L6WGE9-5561	14
MUUH6E-5561	7
NBXF34-5561	14
NFT79E-5562	14
NMCAFG-5561	Fourteen (14)
Q2K3Y6-5562	7
QL9NG8-5561	14(Morgan Chen 7, Kids 7)
QVYAM6-5562	Four times
RTPJX2-5561	14

TABLE 1

Question: 21 **Category: Application**

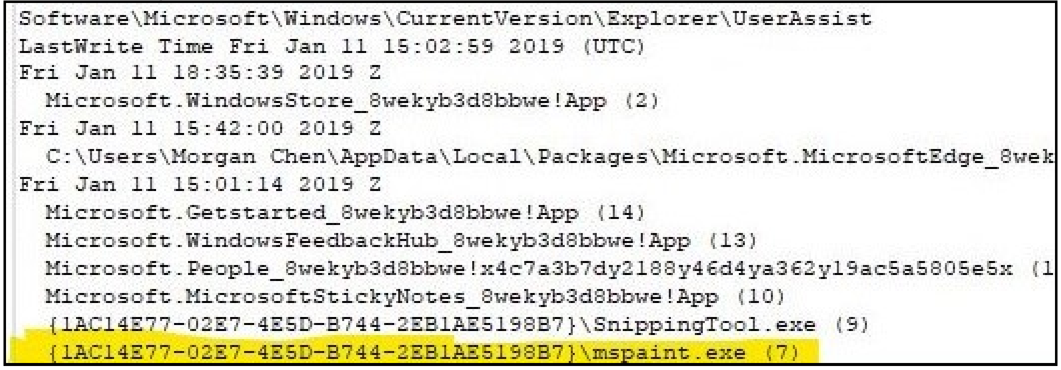
WebCode	Response
V292YY-5561	14 (7 times for each for the user accounts of Morgan Chen and Kids)
WJ4UKW-5561	Total of 14 - 7: Kids, 7: Morgan Chen
X4PZAY-5562	7
XDC2Q9-5561	14
XE36GV-5561	Zero
YN48YX-5562	7
YUVEG7-5561	7 times
ZMBJCV-5562	0

Question 21: How many times was "mspaint.exe" executed?

Consensus Result: Seven (7) and/or Fourteen (14)

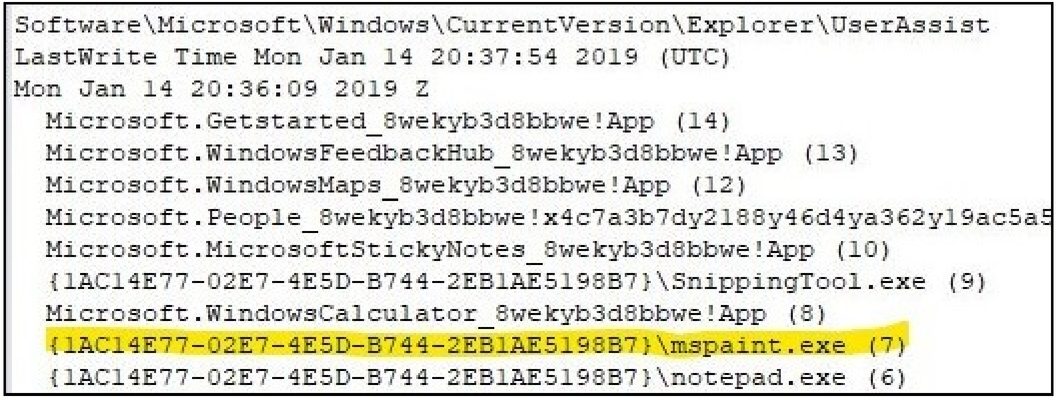
Expected Response Explanation:
The expected response was seven (7), however due to the ambiguity of the question participants did not know which user account to target. The response of fourteen (14) was also accepted for the total count from the two user accounts. Information regarding the number of times "mspaint.exe" was executed can be found at the following location: C:\Users\Morgan Chen\NTUSER.DAT and C:\Users\Kids\NTUSER.DAT.

Screen Shot:
C:\Users\Morgan Chen\NTUSER.DAT:



```
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
LastWrite Time Fri Jan 11 15:02:59 2019 (UTC)
Fri Jan 11 18:35:39 2019 Z
  Microsoft.WindowsStore_8wekyb3d8bbwe!App (2)
Fri Jan 11 15:42:00 2019 Z
  C:\Users\Morgan Chen\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wek
Fri Jan 11 15:01:14 2019 Z
  Microsoft.Getstarted_8wekyb3d8bbwe!App (14)
  Microsoft.WindowsFeedbackHub_8wekyb3d8bbwe!App (13)
  Microsoft.People_8wekyb3d8bbwe!x4c7a3b7dy2188y46d4ya362y19ac5a5805e5x (1
  Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe!App (10)
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\SnippingTool.exe (9)
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\mspaint.exe (7)
```

C:\Users\Kids\NTUSER.DAT:



```
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
LastWrite Time Mon Jan 14 20:37:54 2019 (UTC)
Mon Jan 14 20:36:09 2019 Z
  Microsoft.Getstarted_8wekyb3d8bbwe!App (14)
  Microsoft.WindowsFeedbackHub_8wekyb3d8bbwe!App (13)
  Microsoft.WindowsMaps_8wekyb3d8bbwe!App (12)
  Microsoft.People_8wekyb3d8bbwe!x4c7a3b7dy2188y46d4ya362y19ac5a5
  Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe!App (10)
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\SnippingTool.exe (9)
  Microsoft.WindowsCalculator_8wekyb3d8bbwe!App (8)
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\mspaint.exe (7)
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\notepad.exe (6)
```

TABLE 1

Question: 22	Category: Application

Question 22: Was the Skype Application executed on this computer?

Manufacturer's Expected Response: Yes

WebCode	Response
32LYBW-5562	yes
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	Yes
682GJP-5562	Yes
6Z4RZY-5561	Yes
9LB7BM-5562	Yes
AP6K9W-5562	Yes
C97GKM-5561	yes
CMBD4P-5561	yes
CPHTCG-5561	Yes
D9NRUF-5562	Yes
EP84ZE-5562	Yes
H6CDEC-5561	yes
J3ZUA9-5561	Yes
JLWJ4G-5562	Yes
K3E3B9-5561	Yes, 4 times. ("Windows\Prefetch\SKYPEAPP.EXE-3055373E.pf")
L6WGE9-5561	Yes
MUUH6E-5561	Yes
NBXF34-5561	Yes
NFT79E-5562	Yes
NMCAFG-5561	yes
Q2K3Y6-5562	Yes
QL9NG8-5561	Yes
QVYAM6-5562	Yes
RTPJX2-5561	Yes

TABLE 1

Question: 22 **Category: Application**

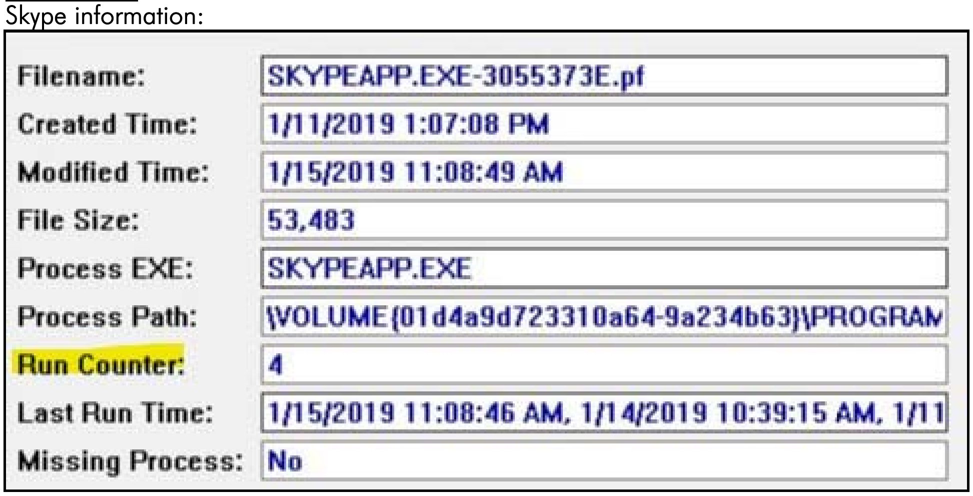
WebCode	Response
V292YY-5561	Yes, prefetch evidence for SKYPEAPP.EXE indicated 4 separate run times, as well as 3 UserAssist entries for Microsoft.SkypeApp_kzf8qxf38zg5c!App
WJ4UKW-5561	Yes - Run count: 4 (SKYPEAPP.EXE)
X4PZAY-5562	Yes
XDC2Q9-5561	Yes
XE36GV-5561	Yes
YN48YX-5562	Yes
YUVEG7-5561	Yes
ZMBJCV-5562	Yes

Question 22: Was the Skype Application executed on this computer?

Consensus Result: Yes

Expected Response Explanation:
Information regarding whether the Skype application was executed can be found at the following location:
C:\Windows\Prefetch

Screen Shot:
Skype information:



Filename:	SKYPEAPP.EXE-3055373E.pf
Created Time:	1/11/2019 1:07:08 PM
Modified Time:	1/15/2019 11:08:49 AM
File Size:	53,483
Process EXE:	SKYPEAPP.EXE
Process Path:	\VOLUME{01d4a9d723310a64-9a234b63}\PROGRAM
Run Counter:	4
Last Run Time:	1/15/2019 11:08:46 AM, 1/14/2019 10:39:15 AM, 1/11
Missing Process:	No

TABLE 1

Question: 23	Category: External Media

Question 23: What type (CD, USB, SD Card, Optical drive) of device was last mounted as E: drive?

Manufacturer's Expected Response: USB

WebCode	Response
32LYBW-5562	USB
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	USB
682GJP-5562	USB
6Z4RZY-5561	Generic Flash Disk USB Device
9LB7BM-5562	USB
AP6K9W-5562	USB
C97GKM-5561	USB
CMBD4P-5561	USB
CPHTCG-5561	USB
D9NRUF-5562	USB
EP84ZE-5562	USB Storage device
H6CDEC-5561	USB
J3ZUA9-5561	USB
JLWJ4G-5562	USB
K3E3B9-5561	Generic Flash Disk USB Device. ("Windows\System32\config\SYSTEM") – ("Windows\INF\setupapidev.log")
L6WGE9-5561	USB
MUUH6E-5561	USB
NBXF34-5561	USB
NFT79E-5562	USB device
NMCAFG-5561	USB
Q2K3Y6-5562	USB
QL9NG8-5561	USB
QVYAM6-5562	USB
RTPJX2-5561	USB

TABLE 1

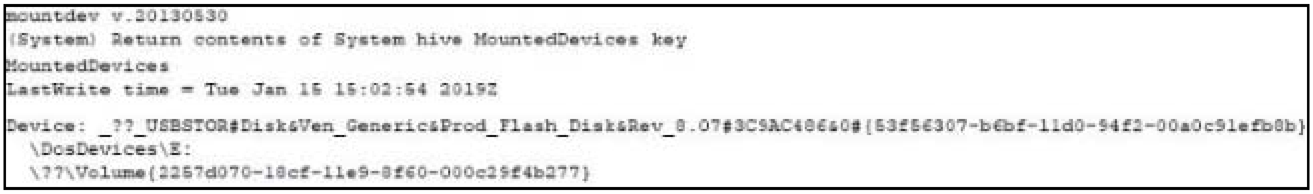
Question: 23	Category: External Media
WebCode	**Response**
V292YY-5561	USB Drive
WJ4UKW-5561	USB
X4PZAY-5562	USB
XDC2Q9-5561	USB
XE36GV-5561	A USB device.
YN48YX-5562	USB
YUVEG7-5561	USB
ZMBJCV-5562	USB

Question 23: What type (CD, USB, SD Card, Optical drive) of device was last mounted as E: drive?

Consensus Result: USB

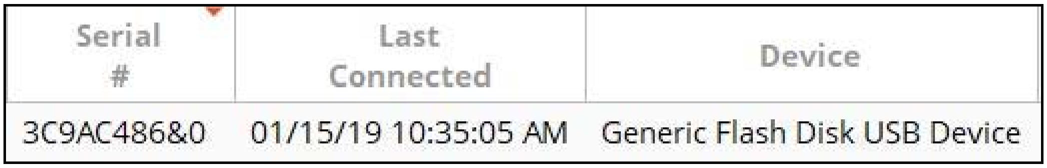
Expected Response Explanation:
Information regarding what type of device was last mounted to the E: drive can be sourced from the System registry hive within the MountedDevices subkey.

Screen Shot:
Mounted Devices:



```
mountdev v.20130530
(System) Return contents of System hive MountedDevices key
MountedDevices
LastWrite time = Tue Jan 15 15:02:54 2019Z

Device: _??_USBSTOR#Disk&Ven_Generic&Prod_Flash_Disk&Rev_8.07#3C9AC486&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
  \DosDevices\E:
  \??\Volume{2257d070-18cf-11e9-8f60-000c29f4b277}
```



Serial #	Last Connected	Device
3C9AC486&0	01/15/19 10:35:05 AM	Generic Flash Disk USB Device

TABLE 1

Question: 24	Category: External Media

Question 24: How many USB devices were mounted to this computer?

Manufacturer's Expected Response: Two (2)

WebCode	Response
32LYBW-5562	2
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	Two (02) devices
682GJP-5562	2
6Z4RZY-5561	2
9LB7BM-5562	2
AP6K9W-5562	11
C97GKM-5561	2
CMBD4P-5561	2
CPHTCG-5561	2
D9NRUF-5562	2
EP84ZE-5562	2 USB Storage devices, 1 USB hub, 1 USB Composite device, 2 USB Input devices. The 2 USB storage devices were mounted (given drive letters) previously.
H6CDEC-5561	1
J3ZUA9-5561	2
JLWJ4G-5562	2
K3E3B9-5561	2. (“Windows\System32\config\SYSTEM”) – (“Windows\INF\setupapidev.log”).
L6WGE9-5561	2
MUUH6E-5561	2
NBXF34-5561	2
NFT79E-5562	2
NMCAFG-5561	Two (2)
Q2K3Y6-5562	2
QL9NG8-5561	2
QVYAM6-5562	12
RTPJX2-5561	2

TABLE 1

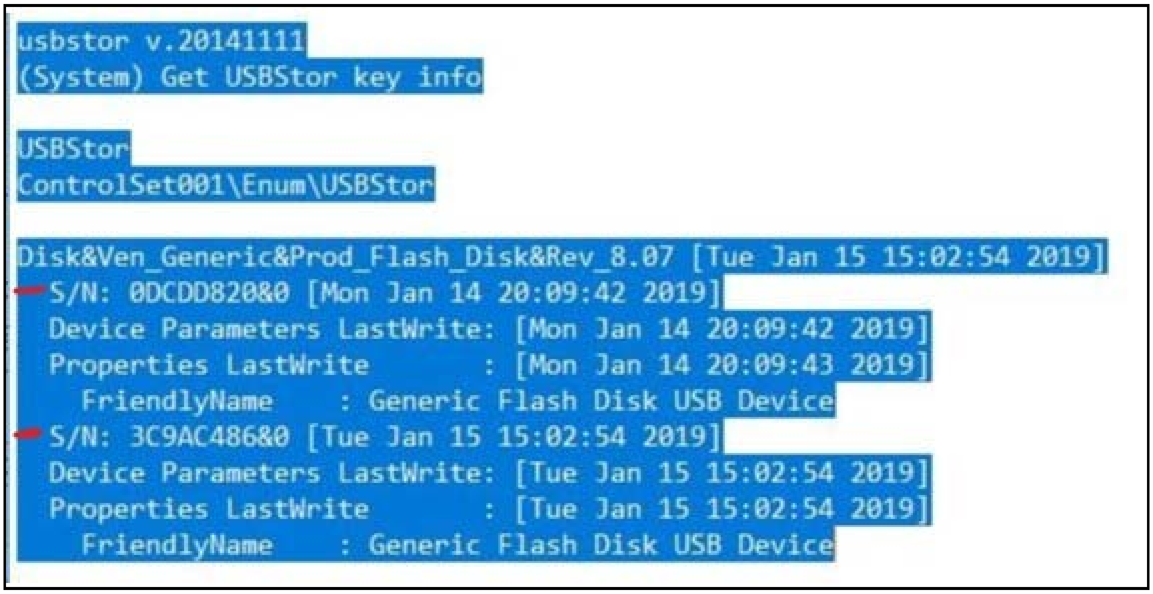
Question: 24	Category: External Media
WebCode	**Response**
V292YY-5561	2
WJ4UKW-5561	2 - USB storage devices
X4PZAY-5562	2
XDC2Q9-5561	2
XE36GV-5561	Two
YN48YX-5562	2
YUVEG7-5561	2 Devices
ZMBJCV-5562	2

Question 24: How many USB devices were mounted to this computer?

Consensus Result: Two (2)

Expected Response Explanation:
Information regarding how many USB devices were mounted to this computer can be sourced from the System registry hive within the USBSTOR subkey.

Screen Shot:
USBSTOR:



```
usbstor v.20141111
(System) Get USBStor key info

USBStor
ControlSet001\Enum\USBStor

Disk&Ven_Generic&Prod_Flash_Disk&Rev_8.07 [Tue Jan 15 15:02:54 2019]
  S/N: 0DCDD820&0 [Mon Jan 14 20:09:42 2019]
  Device Parameters LastWrite: [Mon Jan 14 20:09:42 2019]
  Properties LastWrite       : [Mon Jan 14 20:09:43 2019]
    FriendlyName     : Generic Flash Disk USB Device
  S/N: 3C9AC486&0 [Tue Jan 15 15:02:54 2019]
  Device Parameters LastWrite: [Tue Jan 15 15:02:54 2019]
  Properties LastWrite       : [Tue Jan 15 15:02:54 2019]
    FriendlyName     : Generic Flash Disk USB Device
```

TABLE 1

Question: 25 Category: External Media

Question 25: Provide the serial number associated with USB named "Give Away 2018".

Manufacturer's Expected Response: 0DCDD820

WebCode	Response ** Inconsistencies not highlighted; No consensus achieved **
32LYBW-5562	584FC79D
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	0DCDD820
682GJP-5562	0DCDD820
6Z4RZY-5561	584FC79D
9LB7BM-5562	0DCDD820
AP6K9W-5562	3c9ac486&0
C97GKM-5561	584FC79D
CMBD4P-5561	3c9ac486&0
CPHTCG-5561	0DCDD820&0
D9NRUF-5562	0DCDD820
EP84ZE-5562	0DCDD820&0
H6CDEC-5561	1a38be56
J3ZUA9-5561	0dcdd820
JLWJ4G-5562	584F-C79D
K3E3B9-5561	3C9AC486&0. (“Windows\System32\config\SYSTEM”) – (“Windows\INF\setupapidev.log”)
L6WGE9-5561	3C9AC486&0
MUUH6E-5561	0DCDD820
NBXF34-5561	0DCDD820
NFT79E-5562	0DCDD820&0
NMCAFG-5561	0DCDD820
Q2K3Y6-5562	584FC79D
QL9NG8-5561	0DCDD820&0
QVYAM6-5562	I did not fine the named "Give Away 2018" however I found ODCDD820
RTPJX2-5561	0DCDD820

TABLE 1

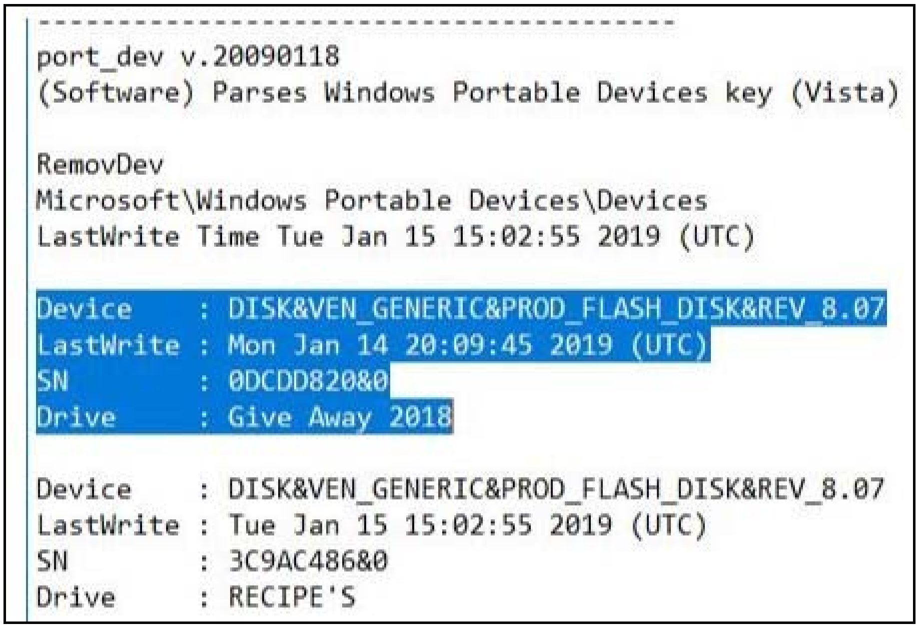
Question: 25	Category: External Media
WebCode	**Response** ** Inconsistencies not highlighted; No consensus achieved **
V292YY-5561	Volume serial number - 584fc79d. USB serial number - 0dcdd820
WJ4UKW-5561	0DCDD820
X4PZAY-5562	584FC79D
XDC2Q9-5561	584FC79D
XE36GV-5561	0DCDD820
YN48YX-5562	584FC79D
YUVEG7-5561	0DCDD820
ZMBJCV-5562	0DCDD820

Question 25: Provide the serial number associated with USB named "Give Away 2018".

Consensus Result: A consensus response was not achieved. The objective was to identify and report the USB serial number for "Give Away 2018". The expected response was 0DCDD820.

Expected Response Explanation:
A non-consensus majority of participants reported the expected response. Information regarding the serial number associated with the USB named "Give Away 2018" can be found in the Software registry hive.

Screen Shot:
Devices:



```
----------------------------------------
port_dev v.20090118
(Software) Parses Windows Portable Devices key (Vista)

RemovDev
Microsoft\Windows Portable Devices\Devices
LastWrite Time Tue Jan 15 15:02:55 2019 (UTC)

Device    : DISK&VEN_GENERIC&PROD_FLASH_DISK&REV_8.07
LastWrite : Mon Jan 14 20:09:45 2019 (UTC)
SN        : 0DCDD820&0
Drive     : Give Away 2018

Device    : DISK&VEN_GENERIC&PROD_FLASH_DISK&REV_8.07
LastWrite : Tue Jan 15 15:02:55 2019 (UTC)
SN        : 3C9AC486&0
Drive     : RECIPE'S
```

Other Responses:
Eight participants reported the serial number 584FC79D; one additional participant identified this serial number as the volume serial number.

TABLE 1

Question: 26 **Category: External Media**

Question 26: Provide the last write time for device named "Give Away 2018". Provide the answer in the UTC + 00:00 using the following format: MM/DD/YYYY HH:MM:SS AM/PM.

Manufacturer's Expected Response: 01/14/2019 08:09:45 PM

WebCode	**Response** ** Inconsistencies not highlighted; No consensus achieved **
32LYBW-5562	1/14/2019 6:14:13 PM
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	01/14/2019 08:09:42 PM
682GJP-5562	01/14/2019 08:09:14 PM
6Z4RZY-5561	01/14/2019 08:12:28 PM (UTC +00:00)
9LB7BM-5562	01/14/2019 08:09:42 PM
AP6K9W-5562	01/08/2019 14:42:50 +1:00
C97GKM-5561	01/14/2019 06:14:13 PM
CMBD4P-5561	01/15/2019 03:35:05 PM
CPHTCG-5561	01/14/2019 06:14:13 PM
D9NRUF-5562	01/14/2019 08:09:42 PM
EP84ZE-5562	01/14/2019 20:09:42 UTC
H6CDEC-5561	01/15/2019 03:05:22 PM
J3ZUA9-5561	01/14/2019 08:15:09 PM
JLWJ4G-5562	01/14/2019 06:14:13 PM
K3E3B9-5561	01/14/2019 08:15:06 PM. ("\Windows\System32\config\"), it has been found by its serial number
L6WGE9-5561	01/14/2019 08:14:13 PM
MUUH6E-5561	01/14/2019 08:15:06 PM
NBXF34-5561	01/14/2019 08:15:09 PM
NFT79E-5562	01/14/2019 21:12:17
NMCAFG-5561	01/14/2019 08:15:06 PM
Q2K3Y6-5562	01/14/2019 3:12:28 PM
QL9NG8-5561	01/14/2019 06:14:13 PM
QVYAM6-5562	I am unable to provide the answer due to my answer to question 25. 01/14/2019 20:09:42
RTPJX2-5561	01/14/2019 08:15:06 PM

TABLE 1

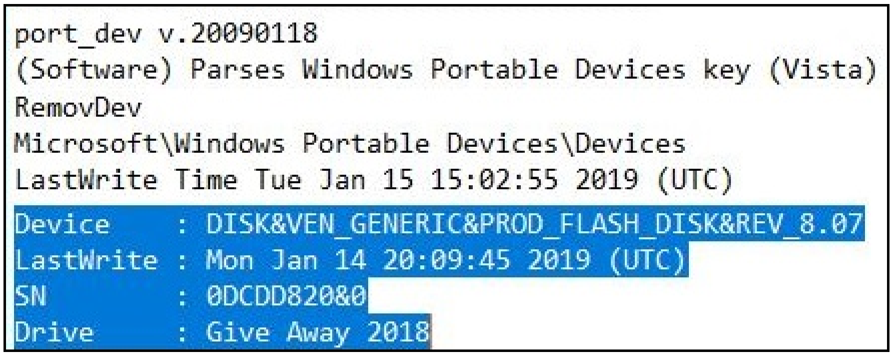
Question: 26	Category: External Media
WebCode	**Response** ** Inconsistencies not highlighted; No consensus achieved **
V292YY-5561	Last removal date and time - 01/14/2019 08:15:09 PM UTC
WJ4UKW-5561	FTK Registry Viewer displays 01/14/2019 20:09:45 PM UTC
X4PZAY-5562	1/15/2019 3:43:30 PM
XDC2Q9-5561	01/14/2019 06:14:13 PM
XE36GV-5561	01/14/2019 8:15:06 (last connection date/time)
YN48YX-5562	1/15/2019 3:43:30 PM
YUVEG7-5561	01/14/2019 08:09:42 PM.
ZMBJCV-5562	01/15/2019 03:05:22 PM

Question 26: Provide the last write time for device named "Give Away 2018". Provide the answer in the UTC + 00:00 using the following format: MM/DD/YYYY HH:MM:SS AM/PM.

Consensus Result: A consensus response was not achieved. The objective was to identify the last write time of the USB device "Give Away 2018". The expected response was 01/14/2019, 08:09:45 PM.

Expected Response Explanation:
Information regarding the last write time for the device named "Give Away 2018" can be found in the Software registry hive at the following location: Software\Microsoft\Windows Portable Devices\Devices.

Screen Shot:
Devices:

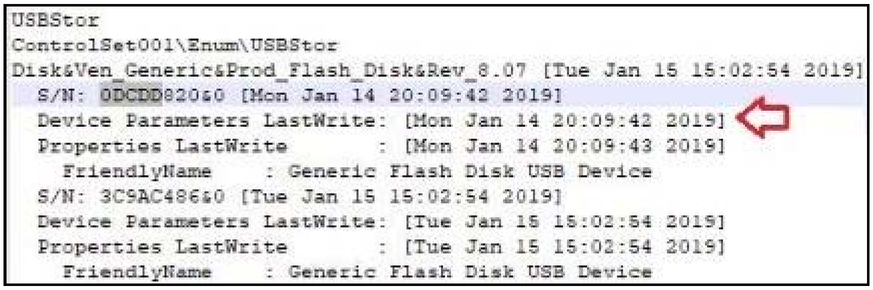


```
port_dev v.20090118
(Software) Parses Windows Portable Devices key (Vista)
RemovDev
Microsoft\Windows Portable Devices\Devices
LastWrite Time Tue Jan 15 15:02:55 2019 (UTC)

Device    : DISK&VEN_GENERIC&PROD_FLASH_DISK&REV_8.07
LastWrite : Mon Jan 14 20:09:45 2019 (UTC)
SN        : 0DCDD820&0
Drive     : Give Away 2018
```

Other Responses:
Six participants reported the expected date but the time of 08:09:42 PM which is associated with the device parameters last write time.

Device Parameters LastWrite:



```
USBStor
ControlSet001\Enum\USBStor
Disk&Ven_Generic&Prod_Flash_Disk&Rev_8.07 [Tue Jan 15 15:02:54 2019]
  S/N: 0DCDD820&0 [Mon Jan 14 20:09:42 2019]
  Device Parameters LastWrite: [Mon Jan 14 20:09:42 2019]
  Properties LastWrite        : [Mon Jan 14 20:09:43 2019]
    FriendlyName    : Generic Flash Disk USB Device
  S/N: 3C9AC486&0 [Tue Jan 15 15:02:54 2019]
  Device Parameters LastWrite: [Tue Jan 15 15:02:54 2019]
  Properties LastWrite        : [Tue Jan 15 15:02:54 2019]
    FriendlyName    : Generic Flash Disk USB Device
```

TABLE 1

Question: 27	Category: External Media

Question 27: What drive letter was assigned to the last mounted USB drive?

Manufacturer's Expected Response: E:

WebCode	Response
32LYBW-5562	E
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	E
682GJP-5562	E
6Z4RZY-5561	E
9LB7BM-5562	E
AP6K9W-5562	E
C97GKM-5561	E
CMBD4P-5561	E
CPHTCG-5561	E:
D9NRUF-5562	E
EP84ZE-5562	E:
H6CDEC-5561	E:
J3ZUA9-5561	E:
JLWJ4G-5562	E
K3E3B9-5561	E. (“Windows\System32\config\SYSTEM”) – (“Windows\INF\setupapidev.log”)
L6WGE9-5561	E
MUUH6E-5561	E:
NBXF34-5561	E:
NFT79E-5562	E :
NMCAFG-5561	E
Q2K3Y6-5562	E
QL9NG8-5561	E
QVYAM6-5562	E
RTPJX2-5561	E:

TABLE 1

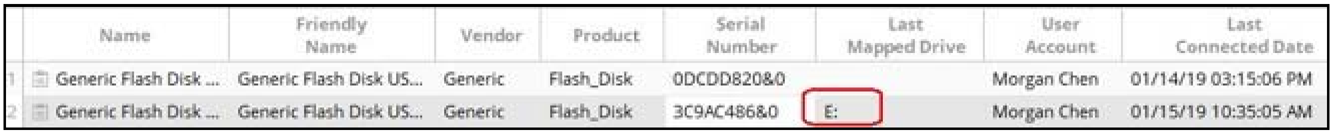
Question: 27	Category: External Media
WebCode	**Response**
V292YY-5561	E
WJ4UKW-5561	E:
X4PZAY-5562	E
XDC2Q9-5561	E
XE36GV-5561	E:\
YN48YX-5562	E
YUVEG7-5561	letter E
ZMBJCV-5562	"E"

Question 27: What drive letter was assigned to the last mounted USB drive?

Consensus Result: E:

Expected Response Explanation:
Information regarding what drive was assigned to the last mounted USB device can be sourced from the System registry hive within the MountedDevices subkey.

Screen Shot:
Mounted Devices:



	Name	Friendly Name	Vendor	Product	Serial Number	Last Mapped Drive	User Account	Last Connected Date
1	Generic Flash Disk ...	Generic Flash Disk US...	Generic	Flash_Disk	0DCDD820&0		Morgan Chen	01/14/19 03:15:06 PM
2	Generic Flash Disk ...	Generic Flash Disk US...	Generic	Flash_Disk	3C9AC486&0	E:	Morgan Chen	01/15/19 10:35:05 AM

TABLE 1

Question: 28	Category: External Media

Question 28: What is the install date and time of the last mounted device? Provide the answer in the UTC + 00:00 using the following format: MM/DD/YYYY HH:MM:SS AM/PM.

Manufacturer's Expected Response: 01/15/2019 03:02:54 PM

WebCode	Response
32LYBW-5562	1/15/2019 3:02:54 PM
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	01/15/2019 03:02:54 PM
682GJP-5562	01/15/2019 03:02:55 PM
6Z4RZY-5561	01/15/2019 03:02:54 PM
9LB7BM-5562	01/15/2019 03:02:54 PM
AP6K9W-5562	01/15/2019 15:02:54 +1:00
C97GKM-5561	01/15/2019 03:02:54 PM
CMBD4P-5561	01/15/2019 03:02:54 PM
CPHTCG-5561	01/15/2019 03:02:54 PM
D9NRUF-5562	01/15/2019 03:02:54 PM
EP84ZE-5562	01/15/2019 15:02:54 UTC
H6CDEC-5561	1/15/2019 03:02:54 PM
J3ZUA9-5561	01/15/2019 03:02:54 PM
JLWJ4G-5562	01/15/2019 03:02:54 PM
K3E3B9-5561	Install date 01/15/2019 03:02:54 PM, last mounted device date 01/15/2019 03:35:05 PM. ("Windows\System32\config\SYSTEM") – ("Windows\INF\setupapidev.log").
L6WGE9-5561	01/05/19 03:35:05 PM
MUUH6E-5561	01/15/2019 03:02:54 PM
NBXF34-5561	01/15/2019 03:02:54 PM
NFT79E-5562	01/15/2019 15:02:54 PM
NMCAFG-5561	01/15/2019 03:02:54 PM
Q2K3Y6-5562	01/15/2019 10:02:54 AM
QL9NG8-5561	01/15/2019 03:02:54
QVYAM6-5562	1/15/2019 15:02:54 PM
RTPJX2-5561	01/15/2019 03:02:54 PM

TABLE 1

Question: 28 **Category: External Media**

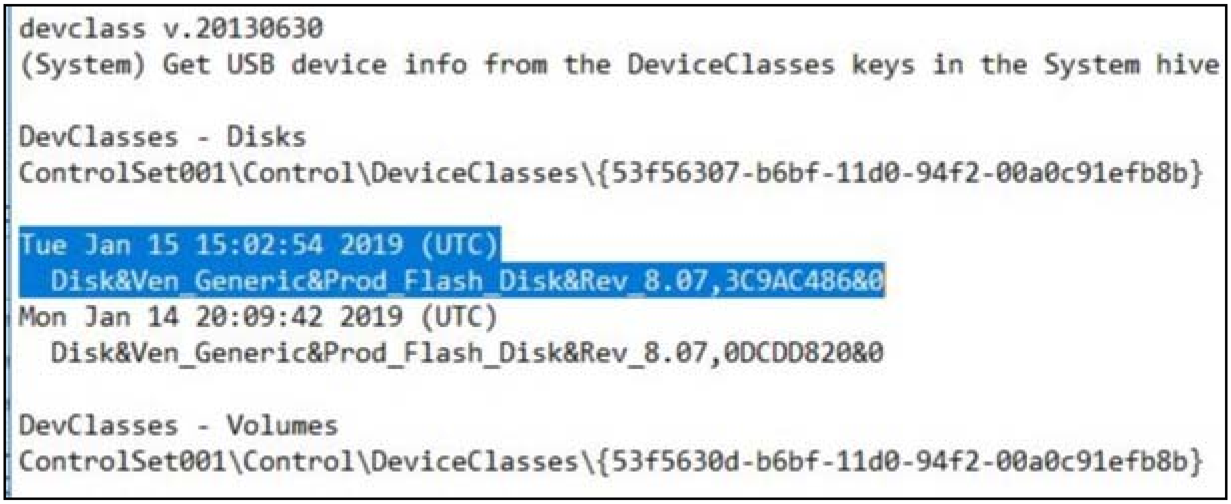
WebCode	Response
V292YY-5561	01/15/2019 03:02:54 PM UTC
WJ4UKW-5561	01/15/2019 15:02:54 PM UTC
X4PZAY-5562	1/15/2019 3:02:54 PM
XDC2Q9-5561	01/15/2019 15:35:05 PM
XE36GV-5561	01/15/2019 10:02:54 AM
YN48YX-5562	1/15/2019 3:02:54 PM
YUVEG7-5561	01/15/2019 03:02:54 PM.
ZMBJCV-5562	01/15/2019 03:02:54 PM

Question 28: What is the install date and time of the last mounted device? Provide the answer in the UTC + 00:00 using the following format: MM/DD/YYYY HH:MM:SS AM/PM.

Consensus Result: 01/15/2019 03:02:54 PM

Expected Response Explanation:
Information regarding the install date/time of the last mounted device can be sourced from the System registry hive within the DeviceClasses subkey.

Screen Shot:
Device Classes:



```
devclass v.20130630
(System) Get USB device info from the DeviceClasses keys in the System hive

DevClasses - Disks
ControlSet001\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

Tue Jan 15 15:02:54 2019 (UTC)
  Disk&Ven_Generic&Prod_Flash_Disk&Rev_8.07,3C9AC486&0
Mon Jan 14 20:09:42 2019 (UTC)
  Disk&Ven_Generic&Prod_Flash_Disk&Rev_8.07,0DCDD820&0

DevClasses - Volumes
ControlSet001\Control\DeviceClasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
```

TABLE 1

Question: 29 **Category: External Media**

Question 29: Provide the manufacturer's name of the last mounted device.

Manufacturer's Expected Response: Alcor Micro Corp.

WebCode	Response ** Inconsistencies not highlighted; No consensus achieved **
32LYBW-5562	Generic
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	Generic
682GJP-5562	Generic
6Z4RZY-5561	Alcor Micro Corp.
9LB7BM-5562	Alcor Micro Corp.
AP6K9W-5562	Generic Flash Disk USB Device
C97GKM-5561	Generic
CMBD4P-5561	Standard disk drives
CPHTCG-5561	Generic
D9NRUF-5562	Alcor Micro Corp
EP84ZE-5562	Generic
H6CDEC-5561	Generic Device (no manufacturer)
J3ZUA9-5561	Generic
JLWJ4G-5562	Generic
K3E3B9-5561	Genmanufacturer. (“Windows\System32\config\SYSTEM”) – (“Windows\INF\setupapidev.log”)
L6WGE9-5561	Generic Flash Disk USB Device
MUUH6E-5561	Generic
NBXF34-5561	Generic
NFT79E-5562	Standard USB HUB
NMCAFG-5561	Alcor Micro Corp.
Q2K3Y6-5562	Generic Mfg Compatible USB storage Device
QL9NG8-5561	Standard disk drives
QVYAM6-5562	Standard disk drive
RTPJX2-5561	Generic

TABLE 1

Question: 29 **Category: External Media**

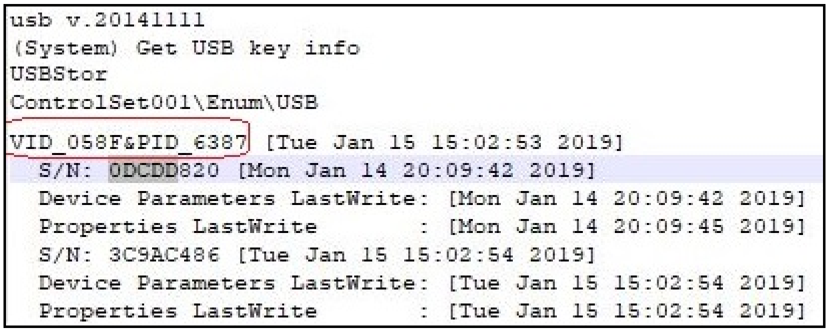
WebCode	Response ** Inconsistencies not highlighted; No consensus achieved **
V292YY-5561	Vendor ID - VID_058F. Product ID - PID_6387. Vendor ID lookup - Alcor Micro Corp. Product ID lookup - Flash Drive Windows indicates the USB device is a generic flash drive, and uses the friendly name of "Generic Flash Disk USB Device"
WJ4UKW-5561	generic manufacturer
X4PZAY-5562	Standard disk drives
XDC2Q9-5561	Generic
XE36GV-5561	Generic
YN48YX-5562	Standard disk drives
YUVEG7-5561	Generic
ZMBJCV-5562	"Alcor Micro, Corp."

Question 29: Provide the manufacturer's name of the last mounted device.

Consensus Result: A consensus was not achieved. The objective of this question was to use the Vendor ID to search the internet for the manufacturer of the device. The expected response was Alcor Micro Corp.

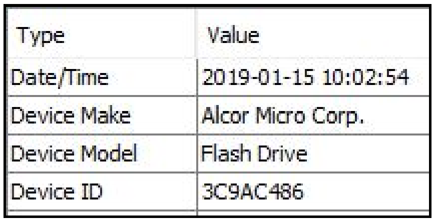
Expected Response Explanation:
The manufacturer's name can be obtained using the Vendor ID 058f and searching the internet for the manufacturer associated with this Vendor ID.

Screen Shot:
USBSTOR:



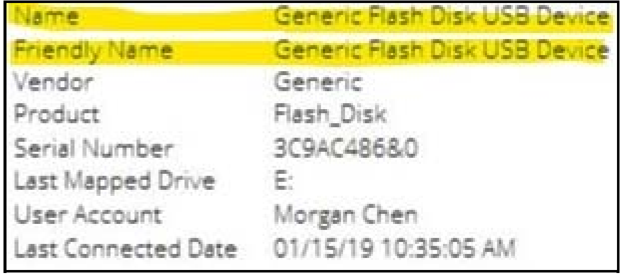
```
usb v.20141111
(System) Get USB key info
USBStor
ControlSet001\Enum\USB
VID_058F&PID_6387 [Tue Jan 15 15:02:53 2019]
  S/N: 0DCDD820 [Mon Jan 14 20:09:42 2019]
  Device Parameters LastWrite: [Mon Jan 14 20:09:42 2019]
  Properties LastWrite       : [Mon Jan 14 20:09:45 2019]
  S/N: 3C9AC486 [Tue Jan 15 15:02:54 2019]
  Device Parameters LastWrite: [Tue Jan 15 15:02:54 2019]
  Properties LastWrite       : [Tue Jan 15 15:02:54 2019]
```

Internet Search:



Type	Value
Date/Time	2019-01-15 10:02:54
Device Make	Alcor Micro Corp.
Device Model	Flash Drive
Device ID	3C9AC486

Other Responses:
A majority of participants reported Generic as the manufacturer's name.



Name	Generic Flash Disk USB Device
Friendly Name	Generic Flash Disk USB Device
Vendor	Generic
Product	Flash_Disk
Serial Number	3C9AC486&0
Last Mapped Drive	E:
User Account	Morgan Chen
Last Connected Date	01/15/19 10:35:05 AM

TABLE 1

Question: 30 Category: Removable Media 19-5562

Question 30: What is the MD5 of the imaged drive?

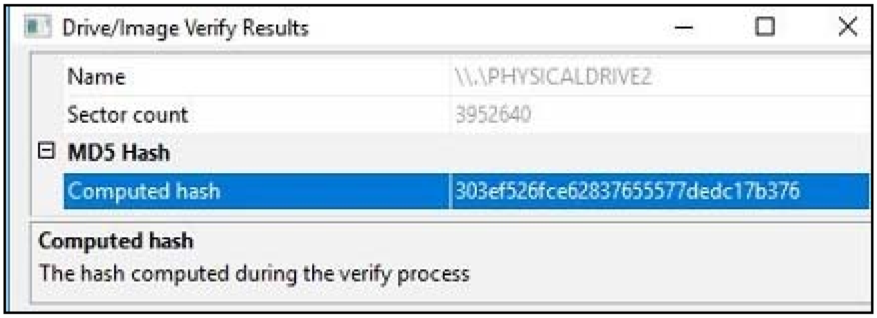
Manufacturer's Expected Response: 303ef526fce62837655577dedc17b376

WebCode	Response
32LYBW-5562	C30D54185823F53464ACADCF59F19239
3VUW4Q-5562	303ef526fce62837655577dedc17b376
4RQFAT-5562	303ef526fce62837655577dedc17b376
682GJP-5562	303ef526fce62837655577dedc17b376
9LB7BM-5562	303ef526fce62837655577dedc17b376
AP6K9W-5562	303efj26fce62837655577dedc17b376
D9NRUF-5562	30BAB5A372D48C82E8597559677BDAD9. NOTE: Thumb drive received suspected to be faulty/beginning to fail. Hash changes every time the drive is re-imaged or hashed (connected via verified writeblocking device). Hash above is from the first image taken. Image verified successfully. X-Ways reports inconsistent read error when accessing the thumb drive.
EP84ZE-5562	303EF526FCE62837655577DEDC17B376
JLWJ4G-5562	303EF526FCE62837655577DEDC17B376
NFT79E-5562	MD5: 303ef526fce62837655577dedc17b376
Q2K3Y6-5562	303ef526fce62837655577dedc17b376
QVYAM6-5562	303ef526fce62837655577dedc17b376
X4PZAY-5562	303EF526FCE62837655577DEDC17B376
YN48YX-5562	303ef526fce62837655577dedc17b376
ZMBJCV-5562	303ef526fce62837655577dedc17b376

Consensus Result: 303ef526fce62837655577dedc17b376

Expected Response Explanation:
This hash value can be calculated using a forensic tool.

Screen Shot:
MD5 Hash Value:



Drive/Image Verify Results

Name	\\.\PHYSICALDRIVE2
Sector count	3952640
⊟ MD5 Hash	
Computed hash	303ef526fce62837655577dedc17b376

Computed hash
The hash computed during the verify process

TABLE 1

Question: 31	Category: Removable Media 19-5562

Question 31: What file system(s) is utilized on this drive?

Manufacturer's Expected Response: FAT16

WebCode	Response
32LYBW-5562	FAT16
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	FAT16
682GJP-5562	FAT16
9LB7BM-5562	FAT16
AP6K9W-5562	Microsoft FAT 16
D9NRUF-5562	FAT16
EP84ZE-5562	FAT16
JLWJ4G-5562	FAT16
NFT79E-5562	FAT16
Q2K3Y6-5562	FAT16
QVYAM6-5562	FAT16
X4PZAY-5562	FAT16
YN48YX-5562	FAT16
ZMBJCV-5562	FAT16

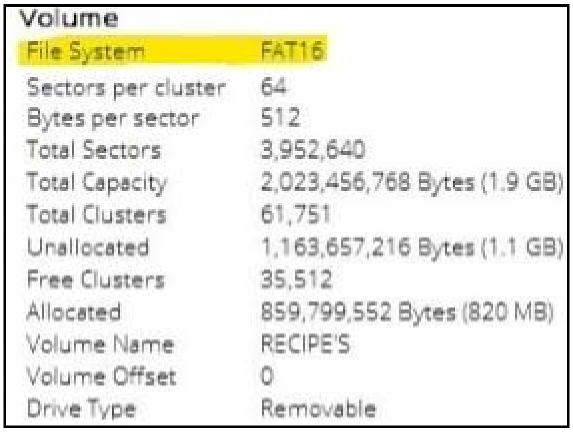
Consensus Result: FAT16

Expected Response Explanation:

Information regarding the file system utilized on this drive can be found as an encoded value in a partition table for the device.

Screen Shot:

Device Partition:



Volume

File System	FAT16
Sectors per cluster	64
Bytes per sector	512
Total Sectors	3,952,640
Total Capacity	2,023,456,768 Bytes (1.9 GB)
Total Clusters	61,751
Unallocated	1,163,657,216 Bytes (1.1 GB)
Free Clusters	35,512
Allocated	859,799,552 Bytes (820 MB)
Volume Name	RECIPE'S
Volume Offset	0
Drive Type	Removable

TABLE 1

Question: 32 **Category: Removable Media 19-5562**

Question 32: What is the vendor ID?

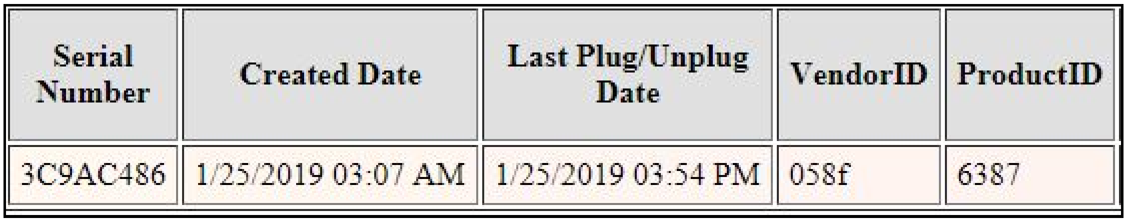
Manufacturer's Expected Response: 058f

WebCode	Response	** Inconsistencies not highlighted; No consensus achieved **
32LYBW-5562	Generic	
3VUW4Q-5562	[Participant did not return results for this question.]	
4RQFAT-5562	058f	
682GJP-5562	58F	
9LB7BM-5562	058F	
AP6K9W-5562	$DISKWIPE	
D9NRUF-5562	058F	
EP84ZE-5562	058F	
JLWJ4G-5562	058F	
NFT79E-5562	058F	
Q2K3Y6-5562	058F	
QVYAM6-5562	058F	
X4PZAY-5562	13D7	
YN48YX-5562	13D7	
ZMBJCV-5562	058F	

Consensus Result: A consensus response was not achieved. The objective was to identify and report the vendor ID for the USB. A majority of participants reported the expected response of 058f.

Expected Response Explanation:
Information regarding the vendor ID is located in the System registry hive in the USBSTOR subkey.

Screen Shot:
USBSTOR:



Serial Number	Created Date	Last Plug/Unplug Date	VendorID	ProductID
3C9AC486	1/25/2019 03:07 AM	1/25/2019 03:54 PM	058f	6387

TABLE 1

Question: 33 Category: Removable Media 19-5562

Question 33: What is the product ID?

Manufacturer's Expected Response: 6387

** Inconsistencies not highlighted; No consensus achieved **

WebCode	Response
32LYBW-5562	Flash_Disk
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	6387
682GJP-5562	6387
9LB7BM-5562	6387
AP6K9W-5562	-
D9NRUF-5562	9380
EP84ZE-5562	6387
JLWJ4G-5562	6387
NFT79E-5562	6387
Q2K3Y6-5562	6387
QVYAM6-5562	3687
X4PZAY-5562	0014
YN48YX-5562	0014
ZMBJCV-5562	6387

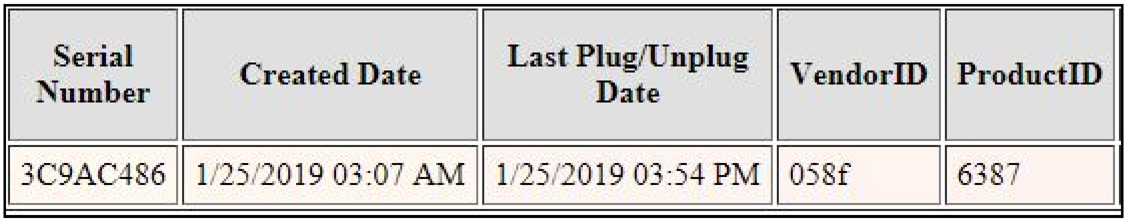
Consensus Result: A consensus result was not achieved. The objective of this question was to identify the product ID for the USB titled "Recipe's". A majority of participants reported the expected response of 6387.

Expected Response Explanation:

Information regarding the product ID of the removable media is located in the System registry hive in the USBSTOR subkey.

Screen Shot:

USBSTOR:



Serial Number	Created Date	Last Plug/Unplug Date	VendorID	ProductID
3C9AC486	1/25/2019 03:07 AM	1/25/2019 03:54 PM	058f	6387

TABLE 1

Question: 34 Category: Removable Media 19-5562

Question 34: How many JPG images were stored in the "Family Pictures" folder?

Manufacturer's Expected Response: Eight (8)

WebCode	Response
32LYBW-5562	8
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	Eight (08)
682GJP-5562	8
9LB7BM-5562	8
AP6K9W-5562	9
D9NRUF-5562	8
EP84ZE-5562	8 Jpgs, 8 Thumbnails
JLWJ4G-5562	8
NFT79E-5562	8
Q2K3Y6-5562	8
QVYAM6-5562	Eight
X4PZAY-5562	8
YN48YX-5562	8
ZMBJCV-5562	8

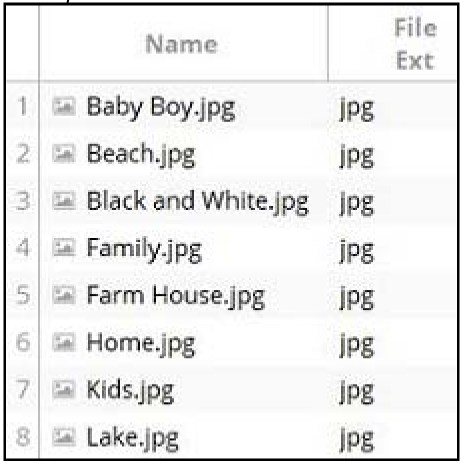
Consensus Result: Eight (8)

Expected Response Explanation:

Information regarding how many jpg images were stored in the "Family Pictures" folder can be found within the Removable Media folder, under the Family Pictures folder.

Screen Shot:

Family Pictures Folder:



	Name	File Ext
1	Baby Boy.jpg	jpg
2	Beach.jpg	jpg
3	Black and White.jpg	jpg
4	Family.jpg	jpg
5	Farm House.jpg	jpg
6	Home.jpg	jpg
7	Kids.jpg	jpg
8	Lake.jpg	jpg

TABLE 1

Question: 35	Category: Removable Media 19-5562

Question 35: Were the images found in the "Family Pictures" folder accessed using the computer hard drive? Yes/No

Manufacturer's Expected Response: Yes

WebCode	Response
32LYBW-5562	Yes
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	Yes
682GJP-5562	Yes
9LB7BM-5562	Yes
AP6K9W-5562	no
D9NRUF-5562	Yes
EP84ZE-5562	Yes
JLWJ4G-5562	Yes
NFT79E-5562	Yes
Q2K3Y6-5562	Yes
QVYAM6-5562	Yes
X4PZAY-5562	Yes
YN48YX-5562	Yes
ZMBJCV-5562	Yes

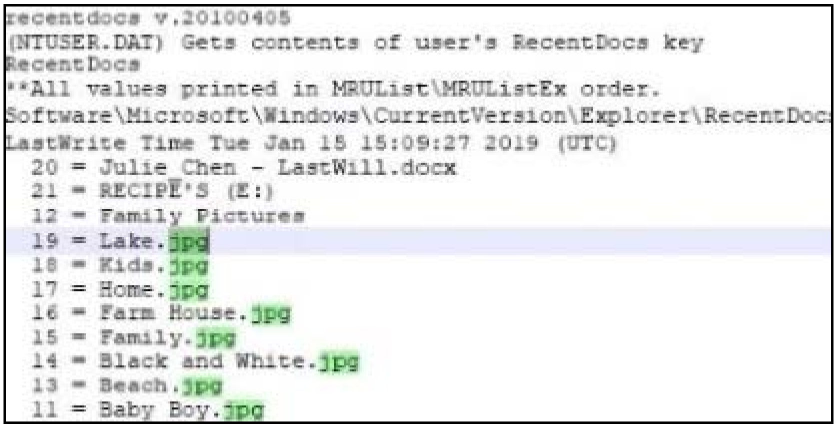
Consensus Result: Yes

Expected Response Explanation:

Information regarding images within the "Family Pictures" folder can be found at the following location:
C:\Users\Morgan Chen\NTUSER.DAT\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

Screen Shot:

Recent Docs:



```
recentdocs v.20100405
(NTUSER.DAT) Gets contents of user's RecentDocs key
RecentDocs
**All values printed in MRUList\MRUListEx order.
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDoc
LastWrite Time Tue Jan 15 15:09:27 2019 (UTC)
  20 = Julie Chen - LastWill.docx
  21 = RECIPE'S (E:)
  12 = Family Pictures
  19 = Lake.jpg
  18 = Kids.jpg
  17 = Home.jpg
  16 = Farm House.jpg
  15 = Family.jpg
  14 = Black and White.jpg
  13 = Beach.jpg
  11 = Baby Boy.jpg
```

TABLE 1

Question: 36 Category: Removable Media 19-5562

Question 36: Provide the volume label of the device.

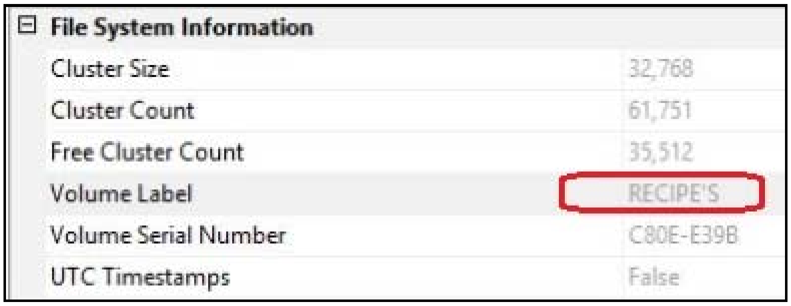
Manufacturer's Expected Response: Recipe's

WebCode	Response
32LYBW-5562	RECIPE'S
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	RECIPE’S
682GJP-5562	RECIPE'S
9LB7BM-5562	RECIPE'S
AP6K9W-5562	GENERIC
D9NRUF-5562	RECIPE'S
EP84ZE-5562	RECIPE'S
JLWJ4G-5562	RECIPE'S
NFT79E-5562	RECIPE'S
Q2K3Y6-5562	E
QVYAM6-5562	RECIPE'S
X4PZAY-5562	RECIPE'S
YN48YX-5562	RECIPE'S
ZMBJCV-5562	RECIPE'S

Consensus Result: Recipe's

Expected Response Explanation:
Information regarding the volume label of the device can be found at the following location:
Software\Microsoft\Windows Portable Devices\Devices

Screen Shot:
Device Information:



⊟ File System Information

Cluster Size	32,768
Cluster Count	61,751
Free Cluster Count	35,512
Volume Label	RECIPE'S
Volume Serial Number	C80E-E39B
UTC Timestamps	False

TABLE 1

Question: 37 Category: Removable Media 19-5562

Question 37: When was the file "Julie_Chen - LastWill.docx" last modified? Provide the answer in the UTC + 00:00 using the following format: MM/DD/YYYY HH:MM:SS AM/PM.

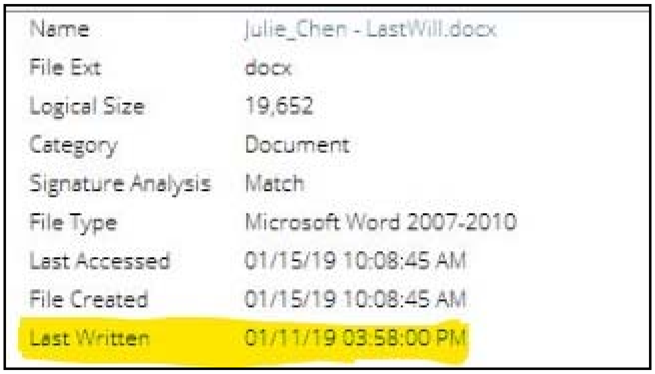
Manufacturer's Expected Response: 01/11/2019 08:58:00 PM

WebCode	Response ** Inconsistencies not highlighted; No consensus achieved **
32LYBW-5562	1/11/2019 3:58:00 PM
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	01/11/2019 10:58:00 AM
682GJP-5562	01/11/2019 08:57:00 PM
9LB7BM-5562	01/11/2019 08:57:00 PM
AP6K9W-5562	01/11/2019 15:58 +1:00
D9NRUF-5562	01/11/2019 08:58:00 PM NOTE: Internal modified d/t metadata from the .docx file is 01/11/2019 08:57:00 PM
EP84ZE-5562	01/11/2019 20:58:00 UTC (01/11/2019 15:58:00 local time), if file was modified in EST. FAT file system does not track time zones. Same last modified date exists on copy of file located on desktop of computer image file.
JLWJ4G-5562	01/11/2019 08:58:00 PM
NFT79E-5562	01/11/2019 14:58:00 PM
Q2K3Y6-5562	01/11/2019 03:58:00 PM
QVYAM6-5562	01/11/2019 20:58:00 PM
X4PZAY-5562	1/11/2019 9:58:00 PM
YN48YX-5562	1/11/2019 9:58:00 PM
ZMBJCV-5562	01/11/2019 05:58:00 AM

Consensus Result: A consensus result was not achieved. The objective was to provide the last modified date and time for the specified document in UTC+00:00. The date was consistent for all participants and the majority of participants reported 58 minutes 00 seconds but the hours varied. The expected response was 01/11/2019 08:58:00PM.

Expected Response Explanation:
Information regarding when the specified file was last modified can be found at the following location:
C:\Users\Morgan Chen\Desktop\Julie_Chen - LastWill.docx

Screen Shot:
Document Information:



Name	Julie_Chen - LastWill.docx
File Ext	docx
Logical Size	19,652
Category	Document
Signature Analysis	Match
File Type	Microsoft Word 2007-2010
Last Accessed	01/15/19 10:08:45 AM
File Created	01/15/19 10:08:45 AM
Last Written	01/11/19 03:58:00 PM

TABLE 1

Question: 38 **Category: Removable Media 19-5562**

Question 38: Based on your investigation, does this device have any connection with the computer hard drive evidence? Yes/No

Manufacturer's Expected Response: Yes

WebCode	Response
32LYBW-5562	Yes
3VUW4Q-5562	[Participant did not return results for this question.]
4RQFAT-5562	Yes
682GJP-5562	Yes
9LB7BM-5562	No
AP6K9W-5562	Yes
D9NRUF-5562	Yes
EP84ZE-5562	Yes
JLWJ4G-5562	Yes
NFT79E-5562	Yes
Q2K3Y6-5562	Yes
QVYAM6-5562	Yes
X4PZAY-5562	Yes
YN48YX-5562	Yes
ZMBJCV-5562	Yes

Consensus Result: Yes

Expected Response Explanation:
This USB device is connected to the computer hard drive evidence.

Additional Comments

TABLE 2

WebCode	Additional Comments
3VUW4Q	Only the creation of a forensic image from the USB was performed. MD5 submitted.
D9NRUF	As stated previously,the thumb drive received suspected to be faulty/beginning to fail. It is possible some of my findings may have been impacted (particularly the hash).
J3ZUA9	Question 26 is a weird wording and doesn't give enough information for what a "last write time" for a thumb drive would be applicable here. Last time the USB was inserted or removed versus actually accessing, changing, and saving a file on it.
JLWJ4G	Some of the questions are ambiguous.
K3E3B9	Very interesting and useful
NBXF34	Question 26 was unclear as to what 'last write time' is referring to. Does that mean the last time a file was accessed/created on the USB or the last time the USB was accessed on the computer.
NMCAFG	regarding question number 26 and due to the language difference: if "the last write time" means "last mounted time" then the answer is the one provided previously. if "the last write time" means "key properties last written time" then the answer is the following: 01/14/2019 08:09:42 PM.
QVYAM6	I did not fine the named "Give Away 2018". I also believe it depend on the Forensic use during the time or imaging can determine some answer. For question 11, I used AXIOM to exam recyle bin, there were only two files, then I used FTK, my go to tool to verify and I saw 11 files. Over all it was a good time.
RTPJX2	Due to the fact the questions are reduced to a tenth of a second it makes it difficult to know what date you want. It depends on where you pull the information from. It took me a great deal of time to try and guess what date/ time you wanted. I spent far more time trying to decipher where the most likely place the test creator pulled the information from and not where all the artifacts for the event would be found. On question 11 "How many files are in the Recycle Bin?" I have to guess if you want how many files are allocated to the Recycle Bin or how many user deleted files are in the Recycle Bin. On question 25 the device has two serial numbers associated with it. The device and volume serial number. 50/50 change I can guess what the test takes is considering associated with. On Question 26 "Provide the last write time for the device named "Give Away 2018". What do you mean by the last write time? Is this the last write to the registry, link file, Windows Log or but maybe you are talking about the last removal time at 8:15:09, last insertion 08:09:42 of or maybe the WPDBUSENUM key of 8:09:45. Maybe the Mount Points key of 08:15:06. On Question 28 what do you mean by mounted device? Is this a mounted storage device or other device like a USB hub? I selected USB storage device. Maybe the Windows install for the last USB that started on 1/15/19 at 3:02:54 and ended at 3:02:55? Maybe the last removal for this device at 3:43:30?

TABLE 2

WebCode	Additional Comments
V292YY	The test overall does a good job of satisfying proficiency for a digital examiner for Windows based computers. I would like to see questions better worded that there is less confusion to the intent rather than what may actually be present. For example, question #4 asked about the last shutdown of the computer; however, the proper way to ask the question would be the last known good shutdown, as an improper power loss will shutdown the computer, but not update the registry key appropriately. Additional questions that could use better clarification include #7, #8, #11, #21, and #25, which all lack an amount of specificity or make assumptions about the data based on the wording. So either more information should be established in the scenario or the questions should be better phrased.

-End of Report-
(Appendix may follow)