Computer Hard Drive - Windows Analysis
Test No. 24-5561/2 Summary Report

Participants were provided with data yielded from an extraction of a Windows 11 Pro Computer Hard Drive. Additionally, participants in the 5562 test received a physical USB drive. Examiners were asked to analyze the sample material and answer questions utilizing their own tools and methods. Data were returned from 152 participants, 42 of which also returned results associated with the physical USB. These results are compiled in the following tables:

← Available in the 5561 version of the report.

10/2/2024 - Due to technical issues related to Hurricane Helene, this report was unable to be posted in its entirety. Results for the 5561(Table 1) and 5562(Table 2) tests have been split at this time. The reports will be returned to their original merged form once the technical issues are resolved.

Manufacturer's Information

The Computer Hard Drive – Windows Analysis test consisted of evidence data acquired from a computer running Windows 11 Pro. 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 24-5562: Computer Hard Drive – Windows & Removable Media Storage Analysis test received an additional component, a physical USB drive shipped in a sealed manila envelope. These participants were also asked to perform evidence acquisition, extraction, and analysis.

SAMPLE PREPARATION/VALIDATION
A scripted scenario discussing a case related to a series of suspicious fires and confirmed arsons was created to generate user data on a Windows Hard Drive. The execution of the test production took place within the following date range, 14 February 2024 and 15 March 2024. 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 24-5562.

Data from the subject computer's hard drive was acquired and analyzed using commercial and open-source industry standard forensic tools. Following sample validation, the image was uploaded to the CTS Portal for download by test participants. MD5 and SHA1 digests (cryptographic checksum, or 'hash') were calculated for the compressed data and provided to participants to enable validation of a successful download of the file(s).

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

VERIFICATION: Predistribution results were consistent with each other and the manufacturer's preparation information. The combination of internal test validation and the responses received from predistribution testing structured the final questions utilized in this test. The following list of tools were utilized in the validation of this test: Autopsy 4.21.0, EnCase 22.3.0.124, FTK Imager 4.5.0.3, RegRipper 3.0, ExifTool 12.65, PECmd 1.6.0.0, HxD 2.5.0.0, 7-Zip 23.01, ewfverify 20140807, and X-Ways Forensics 21.0. CTS does not endorse any particular tools.

PLEASE NOTE: Questions marked with asterisks (**) did not show a clear consensus during preliminary review of the participant's responses. Further information is present in the summary comments and accompanying relevant questions throughout the report.

Manufacturer's Information, continued

SCENARIO PROVIDED TO PARTICIPANTS

State police are investigating a series of suspicious fires and confirmed arsons they believe are related. A tipster indicated they suspected Michael O'Halloran might be responsible. O'Halloran is a volunteer at the Winchestertonfieldville fire station. The tipster advised they often see O'Halloran watching fire related videos on the company computer and he acted odd when asked about it.

The police obtained authorization from the county IT administrator to seize the computer and examine it for information related to the investigation. You have appropriate legal authority to examine this device for evidence related to the arson investigation (5561). You have appropriate legal authority to examine both devices for evidence related to the arson investigation (5562). The USB device should be handled as an item of original evidence provided to your lab for acquisition and analysis (5562).

You are being provided with:
- a copy of the forensic image acquired by the police of the computer seized from the fire station, and
- the USB flash storage device discovered by investigators at the scene of one of the fires (5562 only)

Manufacturer's Information, continued

Question   *Manufacturer's Response*

1 **Provide the stored verification [acquisition] hash MD5 hash for the provided image, Fire Department Workstation.e01.**
51945f35b4b3e59a4a802195bce4efff

---

2 **Compute and provide the SHA-1 hash of the acquired data in the provided image, Fire Department Workstation.e01.**
d894343e8d005219c49226fee4b6fe2e9f5cc3b5

---

3 **What is the hostname (Computer Name) for this computer?**
COMPANY-13

---

4 **What operating system (include version, edition, and Display Version) was installed on this computer?**
Windows 10, Pro, 23H2; or Windows 11 Pro, 23H2

---

5 **To what domain was this computer joined?**
EmergencyServices.Winchestertonfieldville.org

---

6 **What warning banner / legal notice text was displayed to users at the Windows logon screen? Provide the first two sentences of the warning.**
This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.

---

7 **What time zone was this computer configured to display? (Provide answer as name, e.g., Mountain Daylight Time)**
Pacific Time

---

8 **Provide the SSID (network name) of the Wi-Fi hotspot to which this computer was connected.**
Winchestertonfieldville_Fire

---

9 **Provide the user account name for the owner of C:\New folder\New Text Document.txt.**
smcnamara

---

10 **Provide the filesystem attributes for C:\New folder\New Text Document.txt.**
Hidden, Read-Only, Archive

---

11 **What user remotely logged on to this computer via Remote Desktop Protocol (RDP)?**
tgavin

---

12 **What was the IP address (of the other computer) from which a user (from question #11) remotely logged on to this computer via Remote Desktop Protocol (RDP)?**
10.0.2.15

---

13 **Provide the name and path of the active (not deleted) file containing the keyword "flammulated"?**
C:\Users\mohalloran\Pictures\DSC_0921.jpg

---

14 **What text appears in the desktop background photo for user kshea?**
Sleep 'til you're hungry, eat 'til you're sleepy.

Manufacturer's Information, continued

Question   *Manufacturer's Response*

15 **Who is listed as the author of the document with SHA1 hash 0C67015E256CF9B9030DAA0E517B161DC95EA0F0?**
James Moore

16 **Provide the hostname (computer name) for the computer on which the file agency_admin_guide_2004.pdf was located.**
FIRE-DC01

17 **What terms did user gmontag search on Google in the Chrome browser, March 9, 2024?**
bulk chemicals

18 **For the email message containing the keyword "trychtichlorate", provide the sender's email address.**
ronaldbartel@fireman.net

19 **What term was searched for on YouTube at 2024-03-14 01:45:01 UTC by the then currently logged on user?**
bleve

20 **What phone number in the format (NNN)NNN-NNNN appears in the file with SHA1 hash 961FF684E4097CE52C475FB7F249D01EE9DC2BF2?**
(571)434-1925

21 **What was the original (pre-deletion) path of crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf? Provide both the path and filename.**
C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf

22 **Describe the filetype and content of the file with created date March 9, 2024 21:56:33 UTC+0.**
FileType: mp4 file
Content file description: A video of a person igniting a flammable gas in a large bottle. Dancing man at the end of the video (Rick Astley's music video or Rick-Rolled).

23 **According to Windows prefetch, how many times was the calculator app executed?**
Once (1)

24 **According to Windows prefetch, from what directory was the Adobe Acrobat Reader application installer, AcroRdrDC2300820555_en_US.exe, executed?**
C:\temp

25 **In unallocated space on the subject volume is a picture file containing red text, "Make Your Own Focaccia." Provide the five words that immediately follow, "Make Your Own Focaccia."**
A cooking workshop for all

26 **Provide the username for the user who searched for "thermite recipie" [sic].**
gmontag

27 **According to the user jbeatty's NTUSER.DAT file, what other user's documents folder did they access?**
gmontag

Manufacturer's Information, continued

Question   *Manufacturer's Response*

28   **Provide the filetype (MIME Type) for the file with SHA256 hash 67a6fa82325141eaca921ca7a64fe6e6cafb6fb86bd3ba278ccced0d6925986d.**
SQLite or SQLite 3 (Database)

29   **Provide the path and filename of the encrypted file in one of the user's "Documents" directory.**
C:\Users\jbeatty\Documents\book.zip

30   **Provide the name of the file contained within the encrypted file in a user's "Documents" directory.**
cookbook.pdf

Manufacturer's Information, continued

Removable Media Analysis: *USB Storage Device*
Test No. 24-5562

Question   ***Manufacturer's Response***

31 ** **Provide the SHA256 hash of the provided USB flash storage device.**
47C41270C819C675B48EE47CF664733997F8FA04ED430C448E42D3F9CD8EB4A4

32 ** **What filesystem is on the second partition (in sector order) on this device?**
NTFS

33 ** **What is the full path (partition name\parent directory\file) for 1m3r1xbw8wzb1.jpg?**
\filez\New folder\1m3r1xbw8wzb1.jpg

34 **On the device is a photo of a pair of otters (Lontra canadensis) standing together on a white background. Provide the green text that appears in the image.**
2024 CTS 001

35 **Provide the filetype (MIME Type) for the file with SHA256 hash f0445b8916474b7cb177d50fffafb646e25dab0b6c5e5ba14089443d84589c42.**
GIF image or GIF87a

36 **What user account is the owner of all the non-system files on the NTFS partition on this device?**
S-1-5-21-2298470282-2867887670-580413564-1119, or
jbeatty

37 **On this device is a photo of a red onion on a wooden cutting board containing black text on a white background. Provide the text in the image.**
DOUBLE ZIPPED

38 **Provide the filename and path for the file that contains the keyword methylbenzene, where all the vowels have been replaced with numbers, e.g. m3th3lb3nz3n3 (but not necessarily 3s, could be any number or different numbers)**
\Untitled\206969.doc

39 **Who is listed as the author of Fire-fighting-Training-Manual.pdf?**
Rui Vieito

40 **On the device is a graphic file containing the text "2024 cts 004" (without quotes) on a red banner. Provide the text color and a description of the image content.**
Text color: green text,
Image content description: building on fire

41 **Provide the URL contained in the file created on 11/07/23 (November 7, 2023) 17:12:31 UTC.**
https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson

Summary Comments

This test was designed to allow participants to assess their proficiency in analyzing digital artifacts using their own tools and methods. Participants were provided with a scripted scenario, the data extracted from a computer hard drive running Windows 11 Pro, and a series of questions related to the extracted data. Additionally, participants enrolled in the 24-5562: Computer Hard Drive – Windows & Removable Media Storage Analysis test received a physical USB drive. These participants were asked to perform evidence acquisition, extraction, and analysis. Refer to the Manufacturer's Information for preparation details.

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

A total of 152 participants returned results for the 5561 Computer Hard Drive - Windows Analysis test (questions #1-30). All questions reached consensus.

A total of 42 participants returned results for the 5562 Removable Media Storage Analysis test (questions #31-41). Of the 11 total questions, three did not reach a consensus response, questions #31, #32 and #33. Question #31 asked for the SHA256 hash of the provided USB flash storage device. The majority of participants reported the Manufacturer's response, two reported abbreviated versions of this hash and the remaining 14 reported different hashes. Question #32 asked for the filesystem on the second partition (in sector order) on the USB device. The majority of participants reported "exFAT" instead of the Manufacturer's response of "NTFS." Question #33 asked for the full path (partition name\parent directory\file) for 1m3r1xbw8wzb1.jpg. The majority of participants reported the Manufacturer's response, the remaining participants did not report a path or reported that they were unable to locate the .jpg.

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

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

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 31 - Removable Media 24-5562

Question 31: Provide the SHA256 hash of the provided USB flash storage device.

<u>Manufacturer's Response:</u> 47C41270C819C675B48EE47CF664733997F8FA04ED430C448E42D3F9CD8EB4A4

WebCode Test	Response
	** Inconsistencies not highlighted; No consensus achieved **
2EUC34-5562	3d5eb95269c2bb9fcac4473c8ae99b637c6db34f77fc7e909b7d6716fe58260f
2UJN7X-5562	f739 8ba7 dcf9 1179 3c98 d427 1d06 0a19 aa40 b05a
3CH2GJ-5562	D27B9AE022C7D7C3574F4C64CF03996C2512C5CE19F3633B36704AC39D0A6BB9
4L6CCW-5562	47C41270C819C675B48EE47CF664733997F8FA04ED430C448E42D3F9CD8EB4A4
4THJUL-5562	47C41270C819C675B48EE47CF664733997F8FA04ED430C448E42D3F9CD8EB4A4
8ED4K3-5562	47c41270c819c675b48ee47cf664733997f8fa04ed43
8W78WW-5562	47C41270C819C675B48EE47CF664733997F8FA04ED430C448E42D3F9CD8EB4A4
9XFKVP-5562	47c41270c819c675b48...c448e42d3f9cd8eb4a4
AXDBED-5562	47C41270C819C675B48EE47CF664733997F8FA04ED430C448E42D3F9CD8EB4A4
B2ACZR-5562	3d5eb95269c2bb9fcac4473c8ae99b637c6db34f77fc7e909b7d6716fe58260f
BPGNBK-5562	47c41270c819c675b48ee47cf664733997f8fa04ed430c448e42d3f9cd8eb4a4
D7C7PK-5562	ED4B5C90BEC6AAC858B1E1CD587159672D236E6322806CD16CEB63AE0946292E
DKVPRL-5562	47c41270c819c675b48ee47cf664733997f8fa04ed430c448e42d3f9cd8eb4a4
DTN8XH-5562	47C41270C819C675B48EE47CF664733997F8FA04ED430C448E42D3F9CD8EB4A4
GALGEK-5562	be73d7bd2f76cbf4f894b458dd1d5ec5ba31b62663573b7d5a4b0f8afe85eb73
HAVVCD-5562	47c41270c819c675b48ee47cf664733997f8fa04ed430c448e42d3f9cd8eb4a4
HFM3VL-5562	47c41270c819c675b48ee47cf664733997f8fa04ed430c448e42d3f9cd8eb4a4
HTB6DE-5562	47C41270C819C675B48EE47CF664733997F8FA04ED430C448E42D3F9CD8EB4A4
JPAH22-5562	47c41270c819c675b48ee47cf664733997f8fa04ed430c448e42d3f9cd8eb4a4
K3WXT8-5562	8871BAF808FFD4BACA1A4222109A7F0B49E9EE2A4E47C2AA30510AB0F40EC193
KA94ED-5562	a9d8d97413b9aadb0ab33b5ffd03cd30bec3bcd7ce95baa5b80dbe49a11a8a0c

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 31 - Removable Media 24-5562	
WebCode Test / **Response**	** Inconsistencies not highlighted; No consensus achieved **

WebCode Test	Response
LBJ6ZC-5562	47c41270c819c675b48ee47cf664733997f8fa04ed430c448e42d3f9cd8eb4a4
LRM3Y2-5562	1e0e9cabcb2d06f634dabc43ce6dd0d3e58358f10d882319cbc0bac0e83f9a47
MR47EE-5562	47c41270c819c675b48ee47cf664733997f8fa04ed430c448e42d3f9cd8eb4a4
N9Q2B2-5562	47C41270C819C675B48EE47CF664733997F8FA04ED430C448E42D3F9CD8EB4A4
NH83FA-5562	47C41270C819C675B48EE47CF664733997F8FA04ED430C448E42D3F9CD8EB4A4
NPUPBF-5562	47C41270C819C675B48EE47CF664733997F8FA04ED430C448E42D3F9CD8EB4A4
P3EHK8-5562	47C41270C819C675B48EE47CF664733997F8FA04ED430C448E42D3F9CD8EB4A4
Q4ZTN7-5562	7C10C2516F7F1817135B6E669AE8ACEE8F902B27199C146383D87EF9E1626BAB
RZKKZ7-5562	47C41270C819C675B48EE47CF664733997F8FA04ED430C448E42D3F9CD8EB4A4
TH2XG4-5562	47C41270C819C675B48EE47CF664733997F8FA04ED430C448E42D3F9CD8EB4A4
UPTW39-5562	3d5eb95269c2bb9fcac4473c8ae99b637c6db34f77fc7e909b7d6716fe58260f
UZQMYA-5562	47c41270c819c675b48ee47cf664733997f8fa04ed430c448e42d3f9cd8eb4a4
V66XC6-5562	6831ec4704f6fca0eb6102f952f578b8bf4cd817a512225895d99d1870517781. E01 image
WL4AK7-5562	47C41270C819C675B48EE47CF664733997F8FA04ED430C448E42D3F9CD8EB4A4
WQGWCP-5562	47c41270c819c675b48ee47cf664733997f8fa04ed430c448e42d3f9cd8eb4a4
XDT8Y6-5562	47C41270C819C675B48EE47CF664733997F8FA04ED430C448E42D3F9CD8EB4A4
XLP32A-5562	097514f62f0f9271420c0fd556d6a9f4130aeabd61a795919a5c4cad71af4108
Z4GR62-5562	47c41270c819c675b48ee47cf664733997f8fa04ed430c448e42d3f9cd8eb4a4
ZEU2MZ-5562	47C41270C819C675B48EE47CF664733997F8FA04ED430C448E42D3F9CD8EB4A4
ZQ4URL-5562	939f30c1edbdb381ad585b03a50cd645048f901f09191124e142aab1cd1660e5
ZWABN2-5562	5DE61F37690435B1BBA0B8C96BE326105ADF97A485F0FDFF5613277D9B1D66EC

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 31 - Removable Media 24-5562

Question 31: Provide the SHA256 hash of the provided USB flash storage device.
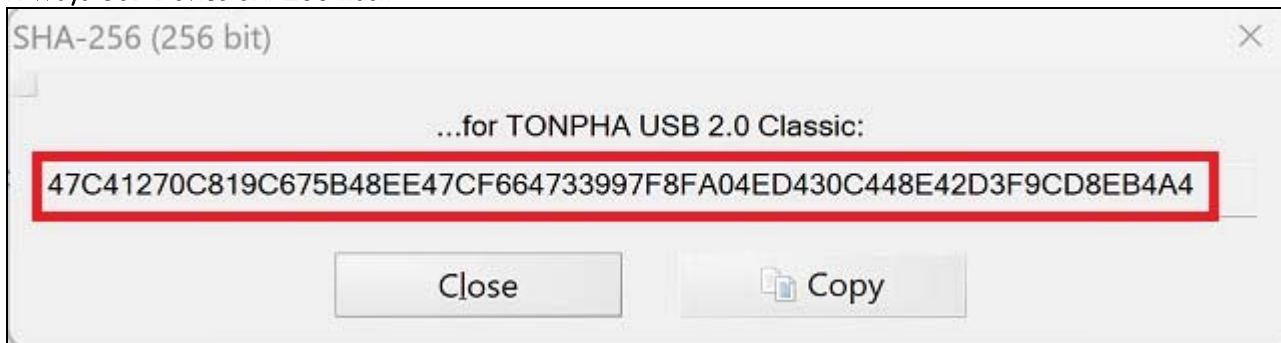
<u>Consensus Result:</u>

A consensus was not achieved for this question. The majority of participants (61%) reported the SHA256 listed as the Manufacturer's response. Two other participants reported a similar hash to the MI but were missing characters. Approximately 14 other hashes were reported by participants. The purpose of this question was to have participants use a reliable write-blocking method to read and hash data from a USB mass storage device.

<u>Manufacturer's Response Explanation:</u>

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

<u>Manufacturer's Response Illustration:</u>

X-Ways USB Device SHA256 hash

SHA-256 (256 bit)

...for TONPHA USB 2.0 Classic:

47C41270C819C675B48EE47CF664733997F8FA04ED430C448E42D3F9CD8EB4A4

Close   Copy

Logicube Talon USB Device SHA256 hash

Verify Information

Drive 1

Bay:	USB_S1
LBA Count:	7864320
Sector Size:	512
Hash Type:	SHA-256
Hash:	47c41270c819c675b48ee47cf664733997f8fa04ed430c448e42d3f9cd8eb4a4
Expected Hash:	47c41270c819c675b48ee47cf664733997f8fa04ed430c448e42d3f9cd8eb4a4
Result:	Pass

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 32 - Removable Media 24-5562

Question 32: What filesystem is on the second partition (in sector order) on this device?

Manufacturer's Response: NTFS

WebCode Test	Response	** Inconsistencies not highlighted; No consensus achieved **
2EUC34-5562	exFAT	
2UJN7X-5562	exFAT	
3CH2GJ-5562	exFAT	
4L6CCW-5562	exFAT	
4THJUL-5562	NTFS	
8ED4K3-5562	If the invisible FAT32 partition at sector 128 of the physical location of the USB is considered the first partition, the second partition is NTFS. If NTFS is considered the first partition instead of the invisible FAT32, then exFAT becomes the second partition.	
8W78WW-5562	exFAT	
9XFKVP-5562	ExFAT	
AXDBED-5562	exFAT	
B2ACZR-5562	exFAT	
BPGNBK-5562	exFat	
D7C7PK-5562	exFAT	
DKVPRL-5562	exFAT	
DTN8XH-5562	exFAT	
GALGEK-5562	exFAT	
HAVVCD-5562	exFAT	
HFM3VL-5562	ExFat	
HTB6DE-5562	exFAT	
JPAH22-5562	NTFS	
K3WXT8-5562	exFAT	
KA94ED-5562	ex-FAT	

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 32 - Removable Media 24-5562	
WebCode Test **Response**	** Inconsistencies not highlighted; No consensus achieved **
LBJ6ZC-5562	exFAT
LRM3Y2-5562	exFAT
MR47EE-5562	exFAT
N9Q2B2-5562	exFAT considering the Master Partition Table, NTFS if we consider the previously existing FAT32 partition
NH83FA-5562	exFAT
NPUPBF-5562	exFAT
P3EHK8-5562	NTFS
Q4ZTN7-5562	ExFat
RZKKZ7-5562	NTFS
TH2XG4-5562	exFAT
UPTW39-5562	exFAT
UZQMYA-5562	NTFS
V66XC6-5562	ExFAT
WL4AK7-5562	exFAT
WQGWCP-5562	NTFS
XDT8Y6-5562	NTFS - After recovering the deleted Fat32 partition, NTFS becomes the second partition. Prior to recovery, exFat is partition 2.
XLP32A-5562	exFAT
Z4GR62-5562	exFAT
ZEU2MZ-5562	exfat
ZQ4URL-5562	exFAT
ZWABN2-5562	exFAT

Removable Media Analysis Results
TABLE 2: Removable Media Analysis Results

Question 32 - Removable Media 24-5562

Question 32: What filesystem is on the second partition (in sector order) on this device?

<u>Consensus Result:</u>

A consensus was not achieved for this question. The majority of participants (76.2%) reported "exFAT" as the second partition instead of "NTFS" which was reported by 21.4% of participants. The purpose of this question was for participants to apply best practices and review drive partitioning to account for all space on the subject drive prior to further processing. This step would discover indications of a deleted partition on the drive. This deleted partition, FAT32, is before the two extant partitions (therefore it is the first partition when sorted in sector order) which would make the second partition NTFS.

<u>Manufacturer's Response Explanation</u>:

There are three partitions on this device. The first partition, formatted as FAT32, was deleted. The second partition was formatted NTFS, and the third, exFAT.

<u>Manufacturer's Response Illustration:</u>

X-Ways view of device partitioning

Name	Full path	Type	Description	1st secto	Size
Partition 3	\Partition 3	FAT32	partition, not referenced in partition table	128	1.0 GB
Partition 1	\Partition 1	NTFS	partition, existing	2,097,280	1.0 GB
Partition 2	\Partition 2	exFAT	partition, existing	4,194,432	1.7 GB
Partition gap	\Partition gap		virtual (for examination purposes)	7,860,352	1.0 MB
Unpartitionable space	\Unpartitionable space		virtual (for examination purposes)	7,862,400	960 KB

EnCase view of device partitioning showing recovered partition

	Item Path	Physical Sector
1	24-5562\Unused Disk Area	1
2	24-5562\STUFF	8,320
3	24-5562\filez	2,097,568
4	24-5562\Untitled [exFAT]	4,195,200

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 33 - Removable Media 24-5562

Question 33: What is the full path (partition name\parent directory\file) for 1m3r1xbw8wzb1.jpg?

Manufacturer's
Response:
\filez\New folder\1m3r1xbw8wzb1.jpg

WebCode Test	Response	** Inconsistencies not highlighted; No consensus achieved **
2EUC34-5562	C:\New folder\1m3r1xbw8wzb1.jpg	
2UJN7X-5562	[Participant did not return results for this question.]	
3CH2GJ-5562	[Participant did not return results for this question.]	
4L6CCW-5562	STUFF\New folder\1m3r1xbw8wzb1.jpg	
4THJUL-5562	(FAT32) STUFF : \New folder\1m3r1xbw8wzb1.jpg	
8ED4K3-5562	STUFF\New folder\1m3r1xbw8wzb1.jpg	
8W78WW-5562	Unused Disk Area	
9XFKVP-5562	(no answer given)	
AXDBED-5562	STUFF\New folder\1m3r1xbw8wzb1.jpg	
B2ACZR-5562	C:\New folder\1m3r1xbw8wzb1.jpg	
BPGNBK-5562	\Stuff\New folder\1m3r1xbw8wzb1.jpg	
D7C7PK-5562	xxx	
DKVPRL-5562	[Partition 3]/New Folder/1m3r1xbw8wzb1.jpg	
DTN8XH-5562	The full file path not found, but reference to it found on unpartitioned space on the USB (Offset 4,284,641)	
GALGEK-5562	File not found	
HAVVCD-5562	Free Space\New folder\	
HFM3VL-5562	This file cannot be located on the forensic image	
HTB6DE-5562	\Unpartitioned space	
JPAH22-5562	STUFF\New folder\1m3r1xbw8wzb1.jpg	
K3WXT8-5562	/img_CTS.E01/vol_vol2/1.zip/2.zip/56	
KA94ED-5562	STUFF\New Folder\1m3r1xbw8wzb1.jpg	

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 33 - Removable Media 24-5562	
WebCode Test **Response**	** Inconsistencies not highlighted; No consensus achieved **
LBJ6ZC-5562	No file with such name was identified by any of the available forensic tools.
LRM3Y2-5562	Unpartitioned space [Disk Space] and 0000001
MR47EE-5562	STUFF\root\NewFolder\1m3r1xbw8wzb1.jpg
N9Q2B2-5562	STUFF\New folder\1m3r1xbw8wzb1.jpg
NH83FA-5562	Unable to locate file
NPUPBF-5562	Unable to find this file with Encase 24.2, X-ways or Axiom. searched for filename and by HEX values.
P3EHK8-5562	/stuff/New folder/1m3r1xbw8wzb1.jpg
Q4ZTN7-5562	Not applicable
RZKKZ7-5562	STUFF\New Folder\1m3r1xbw8wzb1.jpg
TH2XG4-5562	Not in scope
UPTW39-5562	C:\New folder\1m3r1xbw8wzb1.jpg
UZQMYA-5562	STUFF\New Folder\1m3r1xbw8wzb1.jpg
V66XC6-5562	Unable to find
WL4AK7-5562	STUFF\New folder\1m3r1xbw8wzb1.jpg
WQGWCP-5562	STUFF\New folder\1m3r1xbw8wzb1.jpg
XDT8Y6-5562	\\STUFF\New folder\1m3r1xbw8wzb1.jpg
XLP32A-5562	G:\New folder\1m3r1xbw8wzb1.jpg
Z4GR62-5562	Unable to locate the file "1m3r1xbw8wzb1.jpg".
ZEU2MZ-5562	N/A
ZQ4URL-5562	[Participant did not return results for this question.]
ZWABN2-5562	STUFF\NEW folder\1m3r1xbw8wzb1.jpg

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 33 - Removable Media 24-5562

Question 33: What is the full path (partition name\parent directory\file) for 1m3r1xbw8wzb1.jpg?

<u>Consensus Result:</u>

A consensus was not achieved for this question. The majority of participants (65%) reported the Manufacturer's response. The purpose of this question was twofold: discovering and recovering the deleted partition, and then searching for and identifying files by filename.

<u>Manufacturer's Response Explanation:</u>

1m3r1xbw8wzb1.jpg was on the deleted FAT32 partition. Recovering the partition before carving will restore the FAT32 filesystem and enable discovery of this artifact.

<u>Manufacturer's Response Illustration:</u>

X-ways file information

Name	1m3r1xbw8wzb1.jpg
Existent	✗
Full path	\New folder\1m3r1xbw8wzb1.jpg
Ext.	jpg

EnCase file information

		Name	Item Path
☐	4	_87OJSY.PNG	24-5562\filez\New folder_87OJSY.PNG
☐	5	1m3r1xbw8wzb1.jpg	24-5562\filez\New folder\1m3r1xbw8wzb1.jpg
☐	6	4g5wmssgaqyb1.jpg	24-5562\filez\New folder\4g5wmssgaqyb1.jpg

Entries
- 24-5562
  - filez
    - .Spotlight-V100
    - New folder
      - _
    - System Volume I
  - Untitled
  - exFAT

Table Timeline Gallery
Selected 0/1172

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 33 - Removable Media 24-5562

EnCase view of [USB Root]\["STUFF" partition]\New folder\1m3r1xbw8wzb1.jpg

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 34 - Removable Media 24-5562

Question 34: On the device is a photo of a pair of otters (Lontra canadensis) standing together on a white background. Provide the green text that appears in the image.

<u>Manufacturer's</u>   2024 CTS 001
<u>Response:</u>

WebCode Test	Response
2EUC34-5562	2024 CTS 001
2UJN7X-5562	2024 CTS 001
3CH2GJ-5562	2024 CTS 001
4L6CCW-5562	2024 CTS 001
4THJUL-5562	2024 CTS 001
8ED4K3-5562	2024 CTS 001
8W78WW-5562	2024 CTS 001
9XFKVP-5562	2024 CTS 001
AXDBED-5562	2024 CTS 001
B2ACZR-5562	2024 CTS 001
BPGNBK-5562	2024 CTS 001
D7C7PK-5562	2024 CTS 001
DKVPRL-5562	2024 CTS 001
DTN8XH-5562	2024 CTS 001
GALGEK-5562	2024 CTS 001
HAVVCD-5562	2024 CTS 001
HFM3VL-5562	2024 CTS 001
HTB6DE-5562	2024 CTS 001
JPAH22-5562	2024 CTS 001
K3WXT8-5562	2024 CTS 001

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 34 - Removable Media 24-5562	
WebCode Test	**Response**
KA94ED-5562	2024 CTS 001
LBJ6ZC-5562	2024 CTS 001
LRM3Y2-5562	2024 CTS 001
MR47EE-5562	2024 CTS 001
N9Q2B2-5562	2024 CTS 001
NH83FA-5562	2024 CTS 001
NPUPBF-5562	2024 CTS 001
P3EHK8-5562	2024 CTS 001
Q4ZTN7-5562	2024 CTS 001
RZKKZ7-5562	2024 CTS 001
TH2XG4-5562	2024 CTS 001
UPTW39-5562	2024 CTS 001
UZQMYA-5562	2024 CTS 001
V66XC6-5562	2024 CTS 001
WL4AK7-5562	2024 CTS 001
WQGWCP-5562	2024 CTS 001
XDT8Y6-5562	2024 CTS 001
XLP32A-5562	2024 CTS 001
Z4GR62-5562	2024 CTS 001
ZEU2MZ-5562	2024 CTS 001
ZQ4URL-5562	2024 CTS 001
ZWABN2-5562	2024 CTS 001

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 34 - Removable Media 24-5562

Question 34: On the device is a photo of a pair of otters (Lontra canadensis) standing together on a white background. Provide the green text that appears in the image.

Consensus Result:

2024 CTS 001

Manufacturer's Response Explanation:

The photo was on the deleted partition. The image can be located by recovering the partition. Alternatively, the image could be carved from unallocated space, if the partition was not recovered.

Manufacturer's Response Illustration:

2024 CTS 001

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 35 - Removable Media 24-5562

Question 35: Provide the filetype (MIME Type) for the file with SHA256 hash f0445b8916474b7cb177d50fffafb646e25dab0b6c5e5ba14089443d84589c42.

<u>Manufacturer's</u>   GIF image or GIF87a
<u>Response:</u>

WebCode Test	Response
2EUC34-5562	image/gif
2UJN7X-5562	Image/gif
3CH2GJ-5562	image/gif
4L6CCW-5562	Graphic Interchange Format gif
4THJUL-5562	gif
8ED4K3-5562	image/gif
8W78WW-5562	GIF file
9XFKVP-5562	gif
AXDBED-5562	.txt
B2ACZR-5562	image/gif
BPGNBK-5562	image/gif
D7C7PK-5562	Filename: 206610.txt MIME Type: gif
DKVPRL-5562	GIF (Graphics Interchange Format)
DTN8XH-5562	.gif (image/gif) - a file type mismatch
GALGEK-5562	image/gif
HAVVCD-5562	image/gif
HFM3VL-5562	Graphics
HTB6DE-5562	GIF (image/gif)
JPAH22-5562	image/gif
K3WXT8-5562	image/gif

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

WebCode Test	Response
Question 35 - Removable Media 24-5562	
KA94ED-5562	image/Gif
LBJ6ZC-5562	GIF
LRM3Y2-5562	.txt
MR47EE-5562	GIF (47 49 46) (206610.txt)
N9Q2B2-5562	image/gif
NH83FA-5562	.gif
NPUPBF-5562	.txt (206610.txt)
P3EHK8-5562	image/gif
Q4ZTN7-5562	GIF
RZKKZ7-5562	GIF
TH2XG4-5562	image/gif
UPTW39-5562	image/gif
UZQMYA-5562	.GIF
V66XC6-5562	Image/gif
WL4AK7-5562	.gif - Graphic Interchange Format
WQGWCP-5562	image/gif
XDT8Y6-5562	This is an image file, GIF header. File name is 206610.txt
XLP32A-5562	filetype: gif(image file) filename: 206610.txt comment: This file extension is txt, but the hex value is a gif value(47 49 46 38 37 61), so it looks a bad signature
Z4GR62-5562	GIF image data (image/gif) **SEE Additional Comments**
ZEU2MZ-5562	GIF
ZQ4URL-5562	image/gif
ZWABN2-5562	gif, pictures

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 35: Provide the filetype (MIME Type) for the file with SHA256 hash f0445b8916474b7cb177d50fffafb646e25dab0b6c5e5ba14089443d84589c42.
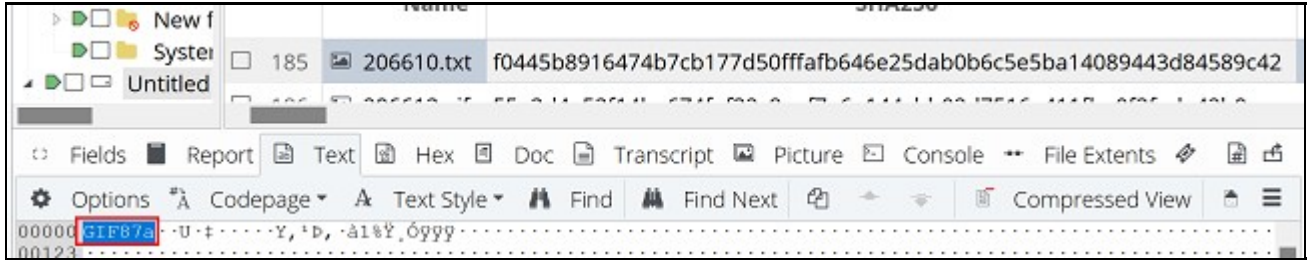
<u>Consensus Result:</u>

GIF image and variations representing similar information.

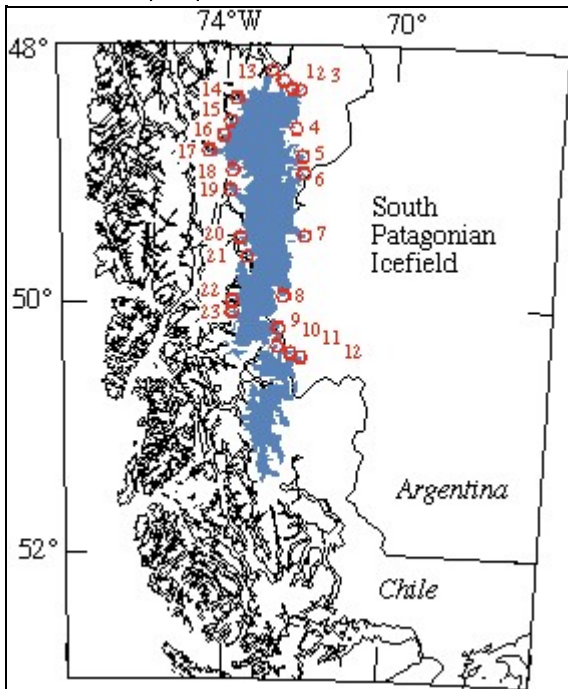<u>Manufacturer's Response Explanation</u>:

The specified hash identifies \Untitled\206610.txt. This file has a .txt extension; however, the internal file extension identifies it as a GIF image file.

<u>Manufacturer's Response Illustration:</u>

EnCase view of 206610.txt

206610.txt (GIF)

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 36 - Removable Media 24-5562

Question 36: What user account is the owner of all the non-system files on the NTFS partition on this device?

Manufacturer's Response: S-1-5-21-2298470282-2867887670-580413564-1119, or jbeatty

WebCode Test	Response
2EUC34-5562	jbeatty
2UJN7X-5562	jbeatty
3CH2GJ-5562	filez
4L6CCW-5562	jbeatty
4THJUL-5562	jbeatty
8ED4K3-5562	jbeatty
8W78WW-5562	jbeatty
9XFKVP-5562	S-1-5-21-2298470282-2867887670-580413564-1119 - jbeatty
AXDBED-5562	jbeatty
B2ACZR-5562	jbeatty
BPGNBK-5562	jbeatty, (S-1-5-21-2298470282-2867887670-580413564-1119)
D7C7PK-5562	Owner: S-1-5-21-2298470282-2867887670-580413564-1119 = jbeatty
DKVPRL-5562	jbeatty
DTN8XH-5562	jbeatty (SID S-1-5-21-2298470282-2867887670-580413564-1119
GALGEK-5562	jbeatty
HAVVCD-5562	jbeatty
HFM3VL-5562	jbeatty
HTB6DE-5562	jbeatty
JPAH22-5562	jbeatty
K3WXT8-5562	jbeatty

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 36 - Removable Media 24-5562	
WebCode Test	**Response**
KA94ED-5562	S-1-5-21-2298470282-2867887670-580413564-1119 jbeatty
LBJ6ZC-5562	jbeatty
LRM3Y2-5562	jbeatty
MR47EE-5562	jbeatty
N9Q2B2-5562	jbeatty
NH83FA-5562	jbeatty
NPUPBF-5562	Owner S-1-5-21-2298470282-2867887670-580413564-1119 - from Computer image ID is jbeatty
P3EHK8-5562	jbeatty
Q4ZTN7-5562	jbeatty
RZKKZ7-5562	jbeatty
TH2XG4-5562	Not in scope
UPTW39-5562	jbeatty
UZQMYA-5562	jbeatty
V66XC6-5562	lmcburney
WL4AK7-5562	Everyone
WQGWCP-5562	jbeatty
XDT8Y6-5562	JBeatty - SID - S-1-5-21-2298470282-2867887670-580413564-1119
XLP32A-5562	COMPANY-13
Z4GR62-5562	jbeatty **SEE Additional Comments**
ZEU2MZ-5562	jbeatty
ZQ4URL-5562	jbeatty
ZWABN2-5562	jbeatty

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 36 - Removable Media 24-5562

Question 36: What user account is the owner of all the non-system files on the NTFS partition on this device?

Consensus Result:

jbeatty and S-1-5-21-2298470282-2867887670-580413564-1119

**Manufacturer's Response Explanation:**

NTFS file permissions often follow files copied to removable media. The Security Identifier (SID) for these files, S-1-5-21-2298470282-2867887670-580413564-1119, identifies the owning account and domain, jbeatty.EmergencyServices.Winchestertonfieldville.org.

Manufacturer's Response Illustration:

X-ways view of NTFS partition files with ownership information
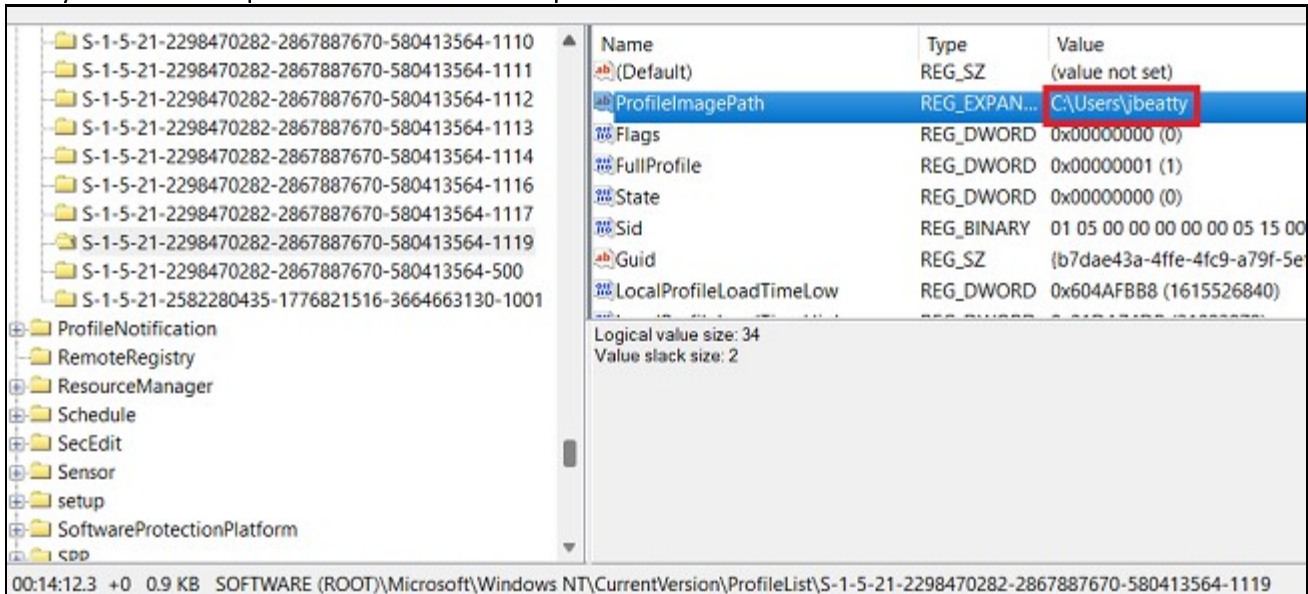
FTK Imager view of NTFS partition files with ownership information
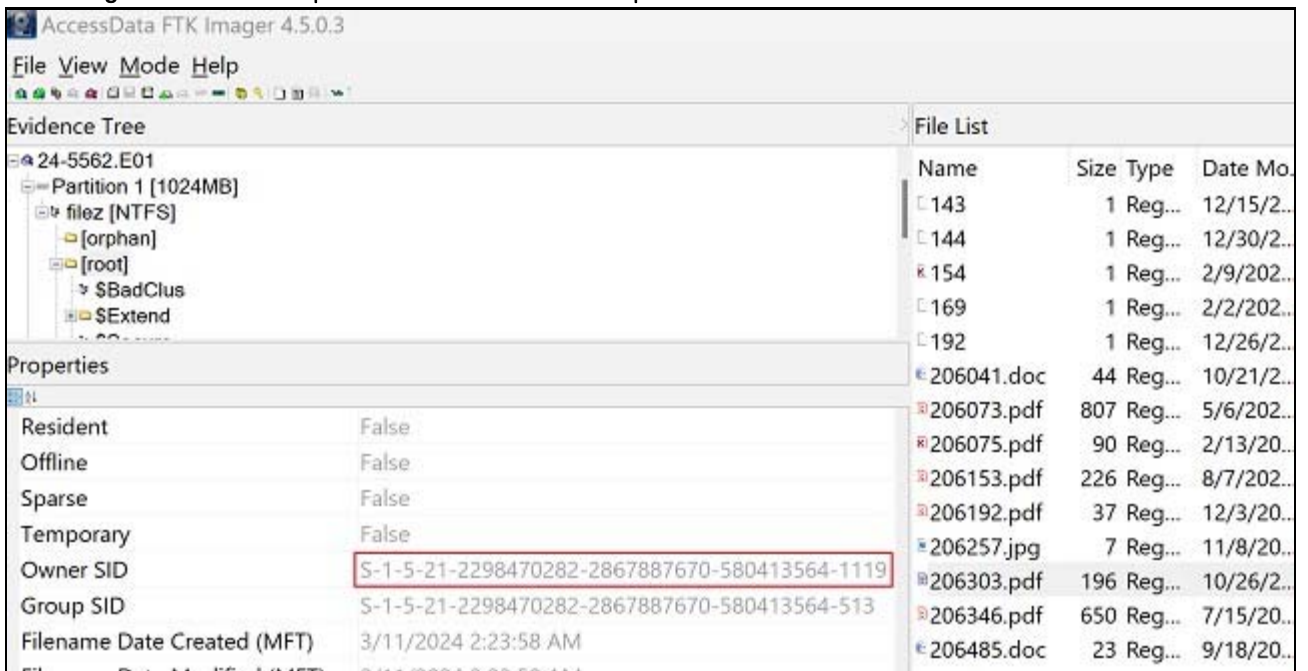
Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 37 - Removable Media 24-5562

Question 37: On this device is a photo of a red onion on a wooden cutting board containing black text on a white background. Provide the text in the image.

<u>Manufacturer's Response:</u>   DOUBLE ZIPPED

WebCode Test	Response
2EUC34-5562	Double Zipped
2UJN7X-5562	Double Zipped
3CH2GJ-5562	DOUBLE ZIPPED
4L6CCW-5562	DOUBLE ZIPPED
4THJUL-5562	DOUBLE ZIPPED
8ED4K3-5562	DOUBLE ZIPPED
8W78WW-5562	DOUBLE ZIPPED
9XFKVP-5562	Double zipped
AXDBED-5562	DOUBLE ZIPPED
B2ACZR-5562	Double Zipped
BPGNBK-5562	DOUBLE ZIPPED
D7C7PK-5562	DOUBLE ZIPPED
DKVPRL-5562	DOUBLE ZIPPED
DTN8XH-5562	DOUBLE ZIPPED (which is ironic, as the file was double zipped)
GALGEK-5562	DOUBLE ZIPPED
HAVVCD-5562	DOUBLE ZIPPED
HFM3VL-5562	DOUBLE ZIPPED
HTB6DE-5562	DOUBLE ZIPPED
JPAH22-5562	DOUBLE ZIPPED
K3WXT8-5562	DOUBLE ZIPPED

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 37 - Removable Media 24-5562	
WebCode Test	**Response**
KA94ED-5562	DOUBLE ZIPPED
LBJ6ZC-5562	DOUBLE ZIPPED
LRM3Y2-5562	DOUBLE ZIPPED
MR47EE-5562	DOUBLE ZIPPED
N9Q2B2-5562	DOUBLE ZIPPED
NH83FA-5562	DOUBLE ZIPPED
NPUPBF-5562	DOUBLE ZIPPED
P3EHK8-5562	DOUBLE ZIPPED
Q4ZTN7-5562	DOUBLE ZIPPED
RZKKZ7-5562	DOUBLE ZIPPED
TH2XG4-5562	DOUBLE ZIPPED
UPTW39-5562	Double Zipped
UZQMYA-5562	DOUBLE ZIPPED
V66XC6-5562	DOUBLE ZIPPED
WL4AK7-5562	DOUBLE ZIPPED
WQGWCP-5562	DOUBLE ZIPPED
XDT8Y6-5562	Double Zipped
XLP32A-5562	DOUBLE ZIPPED
Z4GR62-5562	DOUBLE ZIPPED
ZEU2MZ-5562	DOUBLE ZIPPED
ZQ4URL-5562	DOUBLE ZIPPED
ZWABN2-5562	DOUBLE ZIPPED

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 37: On this device is a photo of a red onion on a wooden cutting board containing black text on a white background. Provide the text in the image.
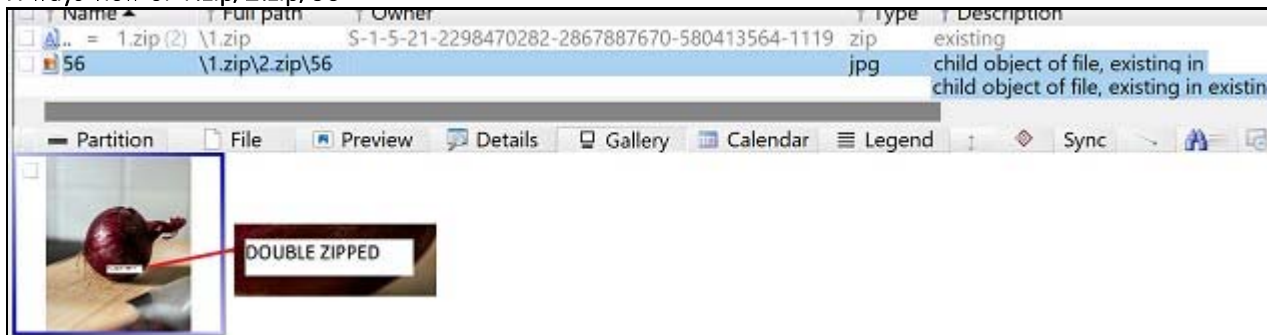
<u>Consensus Result:</u>

DOUBLE ZIPPED

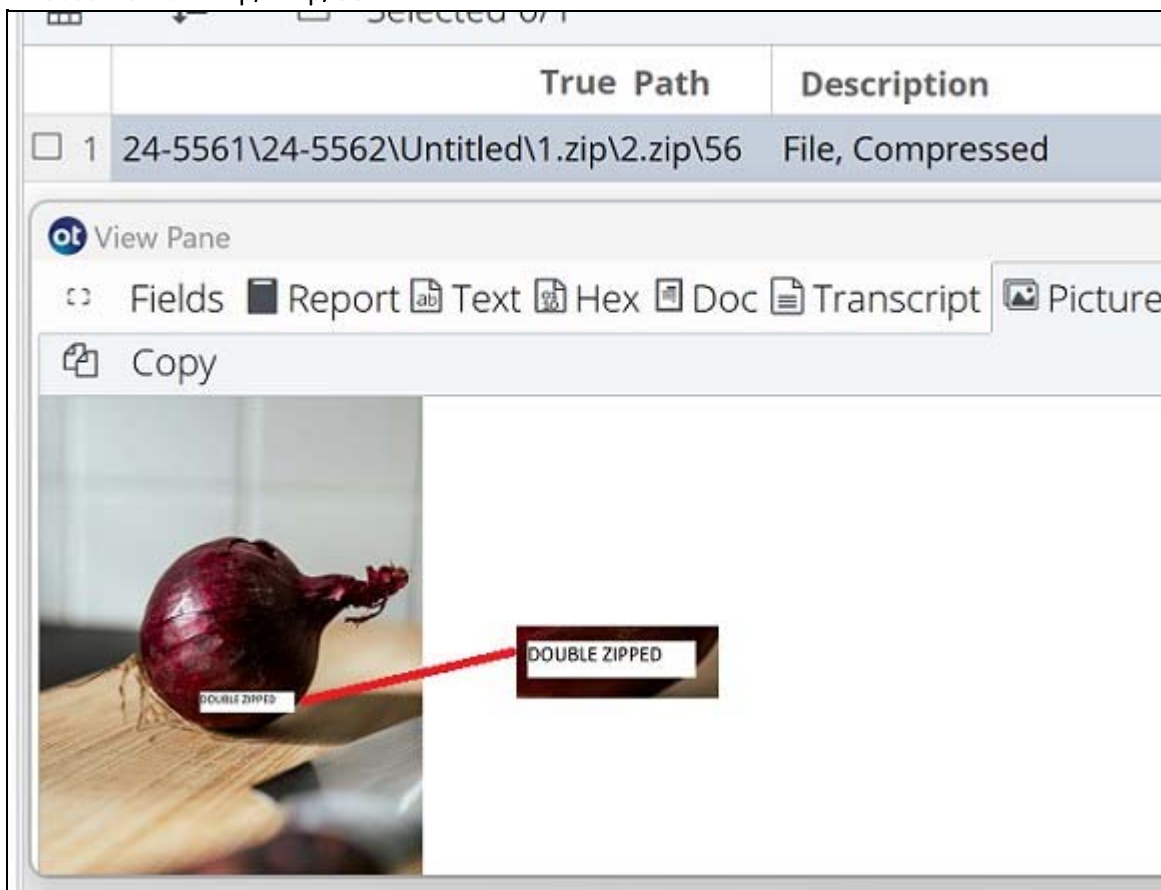<u>Manufacturer's Response Explanation</u>:

The image file, named "56" is found within a zip archive, 2.zip, itself inside a .zip archive, 1.zip. Expansion of compound files and file signature analysis are necessary to discover this file.

<u>Manufacturer's Response Illustration:</u>

X-ways view of 1.zip/2.zip/56

EnCase view of 1.zip/2.zip/56

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 38 - Removable Media 24-5562

Question 38: Provide the filename and path for the file that contains the keyword methylbenzene, where all the vowels have been replaced with numbers, e.g. m3th3lb3nz3n3 (but not necessarily 3s, could be any number or different numbers)

Manufacturer's Response: \Untitled\206969.doc

WebCode Test	Response
2EUC34-5562	D:\206969.doc
2UJN7X-5562	filez\206969.doc
3CH2GJ-5562	[Participant did not return results for this question.]
4L6CCW-5562	\206969.doc
4THJUL-5562	\206969.doc
8ED4K3-5562	filename: 206969.doc, path: filez\206969.doc
8W78WW-5562	(Partition 1)\206969.doc
9XFKVP-5562	Filename: 206973.html
AXDBED-5562	filez\206969.doc
B2ACZR-5562	D:\206969.doc
BPGNBK-5562	\206969.doc
D7C7PK-5562	m$thylb%nz^ne found in free space and files with no extension such as 518 stored on the root of the drive
DKVPRL-5562	[NTFS]/[root]/206969.doc
DTN8XH-5562	Partition 1 (Microsoft NTFS, 1 GB) filez (root directory)\206969.doc
GALGEK-5562	vol_vol2/206969.doc
HAVVCD-5562	\Partition @ 2097280\Root\206969.doc
HFM3VL-5562	Unable to locate this file
HTB6DE-5562	(Partition 1) filez\206969.doc
JPAH22-5562	filez\206969.doc
K3WXT8-5562	/img_CTS.E01/vol_vol2/206969.doc

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

WebCode Test	Response
Question 38 - Removable Media 24-5562	
KA94ED-5562	/img_CtsPEN.001/vol_vol2/206969.doc -> m0th9lb8nz7n6
LBJ6ZC-5562	206969.doc, Partition 1\filez [NTFS]\[root]\206969.doc
LRM3Y2-5562	filez\206969.doc
MR47EE-5562	filez\root\206969.doc (m0th9lb9nz7n6)
N9Q2B2-5562	\206969.doc
NH83FA-5562	Filename: 206973.html Filepath: DM-01\Partition 1\filez\206973.html
NPUPBF-5562	\206969.doc
P3EHK8-5562	/img_pendrive_3A25AAF5.E01/vol_vol2/206969.doc
Q4ZTN7-5562	206969.doc
RZKKZ7-5562	filez\206969.doc
TH2XG4-5562	filez[NTFS]/[root]/206969.doc
UPTW39-5562	D:\206969.doc
UZQMYA-5562	C:\206969.doc (Root of NTFS partition)
V66XC6-5562	M0th9lb8nz7n6 filez/206969.doc
WL4AK7-5562	Partition 1 (NTFS) filez\206969.doc
WQGWCP-5562	Filename: 206969.doc, Path: filez\206969.doc
XDT8Y6-5562	\\FILEZ\206969.doc
XLP32A-5562	Partition 1 (Microsoft NTFS, 1 GB) filez [G:\]\206969.doc
Z4GR62-5562	thumb-cts24-5562.E01\Partition 1\filez [NTFS]\[root]\206969.doc **SEE Additional Comments**
ZEU2MZ-5562	206969.doc /filez [NTFS]/[root]/206969.doc
ZQ4URL-5562	filez/206969.doc
ZWABN2-5562	d(untitled):\ 1~1000

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 38 - Removable Media 24-5562

Question 38: Provide the filename and path for the file that contains the keyword methylbenzene, where all the vowels have been replaced with numbers, e.g. m3th3lb3nz3n3 (but not necessarily 3s, could be any number or different numbers)

Consensus Result:

filez\206969.doc and variations representing similar information.

Manufacturer's Response Explanation:

Searching this device with a simple regular expression such as m#th#lb#nz#n# will locate the file.

Manufacturer's Response Illustration:

EnCase GREP keyword hit in \Untitled\206969.doc

X-ways keyword hit in \206969.doc

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 39 - Removable Media 24-5562

Question 39: Who is listed as the author of Fire-fighting-Training-Manual.pdf?

Manufacturer's
Response: Rui Vieito

WebCode Test	Response
2EUC34-5562	Rui Vieito
2UJN7X-5562	Rui Vieito
3CH2GJ-5562	Rui Vieito
4L6CCW-5562	Rui Vieito
4THJUL-5562	Rui Vieito
8ED4K3-5562	Rui Vieito
8W78WW-5562	Rui Vieito
9XFKVP-5562	Rui Vieito
AXDBED-5562	Rui Vieito
B2ACZR-5562	Rui Vieito
BPGNBK-5562	Rui Vieito
D7C7PK-5562	Rui Vieito
DKVPRL-5562	Rui Vieito
DTN8XH-5562	Rui Vieito
GALGEK-5562	Rui Vieito
HAVVCD-5562	Rui Vieito
HFM3VL-5562	Rui Vieito
HTB6DE-5562	Rui Vieito
JPAH22-5562	Rui Vieito
K3WXT8-5562	Rui Vieito
KA94ED-5562	Rui Vieito

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 39 - Removable Media 24-5562	
WebCode Test	**Response**
LBJ6ZC-5562	Rui Vieito
LRM3Y2-5562	Rui Vieito
MR47EE-5562	Rui Vieito
N9Q2B2-5562	Rui Vieito
NH83FA-5562	Rui Vieito
NPUPBF-5562	Rui Vieito
P3EHK8-5562	Rui Vieito
Q4ZTN7-5562	Rui Vieito
RZKKZ7-5562	Rui Vieito
TH2XG4-5562	Rui Vieito
UPTW39-5562	Rui Vieito
UZQMYA-5562	Rui Vieito
V66XC6-5562	Rui Vieito
WL4AK7-5562	Rui Vieito
WQGWCP-5562	Rui Vieito
XDT8Y6-5562	Rui Vieito
XLP32A-5562	Rui Manuel da Torre Vieito Sérgio Alexandre Neves Guimarães
Z4GR62-5562	Rui Vieito
ZEU2MZ-5562	Rui Manuel da Torre Vieito Sérgio Alexander Neves Guimarães
ZQ4URL-5562	Rui Vieito
ZWABN2-5562	Rui Vieito

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 39 - Removable Media 24-5562

Question 39: Who is listed as the author of Fire-fighting-Training-Manual.pdf?

Consensus Result:

Rui Vieito

Manufacturer's Response Explanation:

Portable Documents (PDFs) can contain metadata fields including "Author." These properties can be viewed.

Manufacturer's Response Illustration:

X-ways view of Fire-fighting-Training-Manual.pdf metadata

Modification	11/25/2008 23:16:52.0 +0
Creation	11/25/2008 23:16:52.0 +0
Title	Microsoft Word - Fire-fighting-Training-Manual
Creator	PScript5.dll Version 5.2
Producer	Acrobat Distiller 6.0 (Windows)
Author	Rui Vieito
Pages	27
Width	842
Height	595
Generator signature	9D348FBE (Adobe PDF Library/Distiller 5-7 W)

Chrome properties pane

Document properties

File name:	Fire-fighting-Training-Manual.pdf
File size:	694 KB
Title:	Microsoft Word - Fire-fighting-Training-Manual
Author:	Rui Vieito
Subject:	-
Keywords:	-
Created:	11/25/08, 6:16:52 PM
Modified:	11/25/08, 6:16:52 PM
Application:	PScript5.dll Version 5.2
PDF producer:	Acrobat Distiller 6.0 (Windows)
PDF version:	1.4
Page count:	27
Page size:	8.26 × 11.69 in (portrait)
Fast web view:	Yes

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 40 - Removable Media 24-5562

Question 40: On the device is a graphic file containing the text "2024 cts 004" (without quotes) on a red banner. Provide the text color and a description of the image content.

Manufacturer's
Response:
Text color: green text,
Image content description: building on fire

WebCode Test	Response
2EUC34-5562	Text color: Green, Image content description: House On Fire
2UJN7X-5562	Text color: Green, Image content description: House on Fire with a Man wearing glasses seen in the bottom half and a crane on the left-hand side of the image.
3CH2GJ-5562	Text color: Green, Image content description: A burning Building
4L6CCW-5562	Text color: green, Image content description: a house on fire
4THJUL-5562	Text color: green, Image content description: House fire
8ED4K3-5562	Text color: green, Image content description: It is an image of a house on fire.
8W78WW-5562	Text color: green, Image content description: It showed fire at a house and a person outside the house
9XFKVP-5562	Text color: Green, Image content description: A house if on fire on a grey day. There is a red square box with green writing on it stating 2024 cts 004
AXDBED-5562	Text color: Green, Image content description: The roof of a house on fire
B2ACZR-5562	Text color: Green, Image content description: Wooden House On Fire!
BPGNBK-5562	Text color: green, Image content description: house on fire
D7C7PK-5562	Text color: Green, Image content description: A house with the roof on fire. Wooden fence across the foreground and a man, side on in, just behind the fence in the bottom centre of the picture. Trees, crane and overhead cables to the right of the picture. There is a red square box with green writing across the image stating "2024 cts 004".
DKVPRL-5562	Text color: Green text on red foreground, Image content description: Burning roof of a house, jets of water trying to quench it
DTN8XH-5562	Text color: Green, Image content description: A house with a burning rooftop.
GALGEK-5562	Text color: Green, Image content description: roof of building on fire
HAVVCD-5562	Text color: Green, Image content description: A burning roof
HFM3VL-5562	Text color: Green, Image content description: house on fire
HTB6DE-5562	Text color: Green, Image content description: House roof on fire

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 40 - Removable Media 24-5562	
WebCode Test	**Response**
JPAH22-5562	Text color: Green text, Image content description: Burning building
K3WXT8-5562	Text color: green, Image content description: Image of a house on fire. Fire truck ladder up in the air next to the fire.
KA94ED-5562	Text color: Green, Image content description: A house burning
LBJ6ZC-5562	Text color: Green, Image content description: a house on fire with fire truck and a man seen from side.
LRM3Y2-5562	Text color: Green, Image content description: House/Building is on fire.
MR47EE-5562	Text color: Green, Image content description: A house burning through the roof and also appears a man with a green jacket
N9Q2B2-5562	Text color: green, Image content description: A house on fire
NH83FA-5562	Text color: Green, Image content description: House on Fire
NPUPBF-5562	Text color: Green, Image content description: Building on Fire
P3EHK8-5562	Text color: green, Image content description: roof fire
Q4ZTN7-5562	Text color: Green, Image content description: Image of a house on fire with the text "2024 cts 004" in green color in a red banner.
RZKKZ7-5562	Text color: Green, Image content description: An image shows ahouse on firewith flames and smoke. Firefightersappear to be on scene.
TH2XG4-5562	Text color: Green, Image content description: Photograph of a burning structure/premises
UPTW39-5562	Text color: Green, Image content description: House On Fire
UZQMYA-5562	Text color: Green, Image content description: File shows a building on fire with a person in the foreground wearing a green hoodie and glasses
V66XC6-5562	Text color: green, Image content description: building on fire
WL4AK7-5562	Text color: green, Image content description: a building on fire with a fire truck ladder next to it
WQGWCP-5562	Text color: Green, Image content description: Burning building with fire and smoke and one man infront of the building
XDT8Y6-5562	Text color: green, Image content description: House on Fire
XLP32A-5562	Text color: green, Image content description: There is a man in the house in front and the house in the back is on fire.
Z4GR62-5562	Text color: Green, Image content description: It appears to be the top part of a house/building on fire and bottom middle of the picture appears to be a possible male wearing glasses and a hooded green shirt. {no additional information such as metadata (like EXIF data/gps/etc…)}

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 40 - Removable Media 24-5562	
WebCode Test	**Response**
ZEU2MZ-5562	Text color: green, Image content description: Building on fire and smoke
ZQ4URL-5562	Text color: Green, Image content description: House on fire
ZWABN2-5562	Text color: green, Image content description: The house is on fire

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 40 - Removable Media 24-5562

Question 40: On the device is a graphic file containing the text "2024 cts 004" (without quotes) on a red banner. Provide the text color and a description of the image content.

<u>Consensus Result:</u>

Text color: green text,

Image content description: building on fire and variations describing similar information.

<u>Manufacturer's Response Explanation:</u>

Manual review of images found on the device can find this image. Scanning images with optical character recognition tools to find the text can expedite the discovery of the image.

<u>Manufacturer's Response Illustration:</u>

s8dmvbrryku41.jpg

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 41 - Removable Media 24-5562

Question 41: Provide the URL contained in the file created on 11/07/23 (November 7, 2023) 17:12:31 UTC.

Manufacturer's Response: https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson

WebCode Test	Response
2EUC34-5562	fire investigator guide.url
2UJN7X-5562	https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson
3CH2GJ-5562	fire investigator guide.url
4L6CCW-5562	https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson
4THJUL-5562	https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson
8ED4K3-5562	https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson
8W78WW-5562	https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson
9XFKVP-5562	https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson
AXDBED-5562	https://nij.ojp.gov/topics/articles/guide-investgating-fire-and-arson
B2ACZR-5562	fire investigator guide.url
BPGNBK-5562	https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson
D7C7PK-5562	Nothing identified for the date provided but the following URL identified within file "SUPA_Chap_11.ppt": http://investigation.discovery.com/videos/solved-secrets-and-bombs.html
DKVPRL-5562	https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson
DTN8XH-5562	A house with a burning rooftop.
GALGEK-5562	Https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson
HAVVCD-5562	https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson
HFM3VL-5562	https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson
HTB6DE-5562	https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson
JPAH22-5562	https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson
K3WXT8-5562	https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 41 - Removable Media 24-5562	
WebCode Test	**Response**
KA94ED-5562	URL=https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson fire investigator guide.url
LBJ6ZC-5562	https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson
LRM3Y2-5562	https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson
MR47EE-5562	https://nij.ojp.gov/topics/articles/guide-investigatin-fire-and-arson
N9Q2B2-5562	https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson
NH83FA-5562	https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson
NPUPBF-5562	URL=https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson
P3EHK8-5562	https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson
Q4ZTN7-5562	https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson
RZKKZ7-5562	https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson
TH2XG4-5562	https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson
UPTW39-5562	fire investigator guide.url
UZQMYA-5562	URL in file from 07/11/2023: *https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson
V66XC6-5562	https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson
WL4AK7-5562	https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson
WQGWCP-5562	https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson
XDT8Y6-5562	https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson
XLP32A-5562	https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson
Z4GR62-5562	https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson
ZEU2MZ-5562	https://nij.ojp.gov/topics/articles/guide-investigatin-fire-and-arson
ZQ4URL-5562	https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson
ZWABN2-5562	https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson

Removable Media Analysis Results
TABLE 2: Removable Media Analysis Results

Question 41 - Removable Media 24-5562

Question 41: Provide the URL contained in the file created on 11/07/23 (November 7, 2023) 17:12:31 UTC.

Consensus Result:

https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson

Manufacturer's Response Explanation:

Listing all files on the device and sorting by creation date will locate \exFAT\fire investigator guide.url. This file is a link file containing the above url.

Manufacturer's Response Illustration:

X-ways view of fire investigator guide.url

Additional Comments

TABLE 3

WebCode Test	Additional Comments
2UJN7X-5562	Question 33, no answer was identified
3CH2GJ-5562	33) We are unable to locate "1m3r1xbw8wzb1.jpg" with our current tools. 38) All of the instances we found had special characters that replaced the vowels but the last vowel had not been altered.
6RLGDW-5561	The wording of question 2 is confusing. The SHA1 of the entire E01 file is already provided in the exam instructions, so I'm assuming the question is asking for the internal E01 data (that's what I provided). The wording of question 9 is confusing. What is meant by the "owner" of a text file? Text files do not have metadata or owners, and the file is stored at the root of C:\. I'm assuming the question is asking who may have created and/or accessed the file? I went off a LNK file in the smcnamara user folder. The wording of question 28 is also confusing. What is meant by "filetype (MIME Type)"? Several possible answers, and .bak files are usually proprietary filetypes.
98N78Y-5561	I was unable to boot the image on VM because the system was corrupted which would help me to find some answers.
CPQ4TQ-5561	Question #4- Axiom reported the OS as Windows 11 (it was parsed correctly in the File System view). Questions #29/#30- Axiom had one (1) exception and would not process cookbook.pdf. It noted cookbook.pdf was present and the file path showing it came from book.zip. FTK Lab correctly processed book.zip as an encrypted file.
DKVPRL-5562	Regarding question 11: Windows terminal services event log event description fields are misleading. The user tgavin has never actually remotely logged in to the computer, he only attempted to. EventID 1149 (which was found) is not necessarily a successful login, it just means the client is connected for an RDP login attempt. An actual successful authentication is EventID 4624, which however was not found in the log file.
DTN8XH-5562	Notes from the colleague who did Imaging / Processing:- There were no notes on the imaging process of the computer or photos of the exhibit. The image created wasn't a physical image of the computer, there was no explanation of why this was done and what data might have been missed as a consequence. Notes from the Investigator - Thank you for the otter pics.
EMTM9G-5561	Thank you for your time.
F3TPTL-5561	Question #28- Magnet Axiom did not generate Sha256 values. Ingested the file into Autopsy and could not locate the file with the provided hash.
HFM3VL-5562	33).What is the full path (partition name\parent directory\file) for 1m3r1xbw8wzb1.jpg? Cannot locate this file on the E01 forensic image of the USB drive. Performed several keyword searches with different configurations and permutations in anticipation that it has been erroneously spelt - no matching results found - possibly an error with this question?

TABLE 3

WebCode Test	Additional Comments
HGE2AK-5561	Question 10 is a bit vague regarding which specific attributes the test is looking for. There are several different types of NTFS "file attributes" so I included the Standard Information attributes listed and main File Name attributes. Question 25 is misleading because two PNG files (Img_flyers.png & img_flyers@2x.png) exist on the volume in allocated space which match the exact description. I was able to find a duplicate of "img_flyers@2x.png" in unallocated space by carving, however I'm not sure that doing so was really necessary to answer the question. Unless I missed a different picture saying "Make your own focaccia" in red text somewhere. Question 28 was confusing because the file in question (store.bak) is a SQL Database backup file, which doesn't have its own MIME type. You would just use "application/octet-stream".
J3FCTE-5561	According to Windows prefetch, how many times was the calculator app executed? I have a comment on this question: The program Magnet Axioma Version 8.2.0.40565 and Cellebrite Inseyest Physical Analyzer Versioni 10.2.101.352 gave us the results that the calculator is executed only once (1), While Autopsy and Forensic Explorer give us the result that the calculator is executed seven (7) times.
LBJ6ZC-5562	Question 4: In the Registry, it shows Windows 10; however, the build number 23H2 indicates Windows 11. Question 25: Forensic tools did not find this particular text in the unallocated space of the subject volume, however, picture containing this text was found in: /Program Files/Adobe/Acrobat DC/Acrobat/WebResources/Resource0/static/js/plugins/aicuc/images/themeless_Reader/img _flyers@2x.png. Question 32: Some forensic tools found remnants of a FAT32 volume called "STUFF" If we count this volume, the second volume would be NTFS. However, since this space was categorized as unallocated, the second volume, based on sector order, is exFAT.
MCQ8YF-5561	Please be aware that some questions provided have ambiguous, broad, or less than specific answers that could lead to a wide variance of responses. Some examples include: 14 - there are multiple possible responses to include: quote, quote + author, quote + author + other text, 22- this is a very broad 2 part question in which somewhat open ended responses are likely
MR47EE-5562	It is very difficult to interpret the statements without a properly translation into our mother language. It is very easy to get confused and to give a wrong answer due to a bad interpretation of the real purpose of the question.
P6NMZG-5561	For question [18] "For the email message containing the keyword "trychtichlorate", provide the sender's email address." I was unable to identify any keywords with this phrase. For question [8] the original question i had was "Provide the BSSID (network name) of the Wi-Fi hotspot to which this computer was connected.", when answering the question that appeared to have changed to "Provide the SSID (network name) of the Wi-Fi hotspot to which this computer was connected." - this change had not been made clear.
V66XC6-5562	Question 33 - I Searched for the file and the file name in hex (31 00 6D 00 33 00 72) and located it at sector 8368. The volume is a FAT32 volume that is not recognized. Possible directory name of STUFF which is located in a sector near the file.
VYTW7Z-5561	Had two hours time to do :/

TABLE 3

WebCode Test	Additional Comments
WBPY99-5561	Question 18 was a tough one. I had to use two forensic tools to find the word trychtichlorate. I only located partial files. The email address I used in the answer was next to the word - essentially at the end of a partial email - so I answered with that email address, but I did not have a full header. If I was doing a real examination, I would feel compelled to qualify my answer that I was not 100% sure that was the sender of the email since the full email header was not present.
X84MXA-5561	In question number 27 it is not clear the meaning of words "other" user's documents and "they" access.
XDT8Y6-5562	Question 2 - As previously discussed with CTS directly - SHA-1 uses multiple algorithms, Base 16 and Base32, or 160-bit. CTS did not spedify which version to use. Question 7 - This question is again unclear. A better question would be to "what offset is the timezone set at?". Or what timezone with bias is the computer set in. The computer is set to Pacific Time. Pacific Time is celebrated by much of the west coast, except Arizona. Arizona doesn't take BIAS into effect. Therefore they just refer to it as Pacific Time all year. Question 18 - This question involves having to parse the store.vol file for Windows App Mail. In all my research, I was able to identify this file as an ESEDB file. Using ESEDB file viewer, the data in this file is, specifically the messages tab, not readable. I needed to download a paid software tool called OSForensics in order to view it. EnCase and Axiom was unable to parse it. Reseach also showed that Autopsy is unable to properly parse store.vol files (although I didn't independantly verify this). I am curious to know what tools the creators of this exam expected uses to use to find this information, as I stuggled very much with this question. In question #40 - There is a spelling mistake. The word context is spelled "contect".
Y2PJCZ-5561	I would request more clear direction in some of the questions. For example, asking the examiner to provide file system attributes for a specific file is too general. When you look at file properties, there are several different categories of attributes that could be provided. Other issues: question 25 refers to a file in unallocated space. I located this file in allocated space. Questions 29 and 30 appear to be somewhat duplicative. Question 2 appears to require the examiner to understand the difference between a tool that hashes a container only versus a tool that can compute the hash of the data contained in a container. However, I cannot say this for certain because I think the question is worded somewhat strangely/vaguely. I would recommend reviewing the questions for clarity before publishing them on the test. As the examiner, it is not enjoyable trying to discern the meaning of the question and second guessing your own interpretation of the question's meaning.

TABLE 3

WebCode Test	Additional Comments
Z4GR62-5562	4) The operating system registry values show the following: ProductName: Windows 10 Pro, EditionID: Professional, CurrentVersion: 6.3, DisplayVersion: 23H2. The Windows 11 2023 Update (also known as version 23H2 and codenamed "Sun Valley 3") is the second update to Windows 11. Windows 11 is the first time Microsoft release a new version of windows but continues to use the previous "ProductName" (Windows 10 Pro) value in the registry. 5) The MS Domain Controller that the computer has joined is "EMERGENCYSERVIC" but the full qualified domain name is "EmergencyServices.Winchestertonfieldville.org." 10) Note the term "filesystem attributes" can have different meaning depending on ones training, the digital forensic tool(s) used, or even the interpretation of the word attributes. For an example this file on an NTFS file system contains "General attributes", "DOS attributes", "Date and time attributes {classic Modify/Access/Create}", "NTFS attributes" and "NTFS access control attributes". My answer for this question used the "DOS attributes" and the "NTFS attributes" if any of the additional attributes were needed, I can provide them. 13) There are three file containing the keyword "flammulated"? two are active the third is in the Recycle Bin. - ProgramData/Microsoft/Search/Data/Applications/Windows/Windows. - Users/mohalloran/Pictures/DSC_0921.jpg. - $Recycle.Bin/S-1-5-21-2298470282-2867887670-580413564-1117/$RCZUXP4.jpg. 28) I provided both "filetype" ("MIME Type"). The MIME Type follows the format of https://www.iana.org/assignments/media-types/media-types.xhtml. https://www.iana.org/assignments/media-types/application/vnd.sqlite3. Also please note the FILE EXTENSION was .bak for this SQLite database backup. 35) I provided both "filetype" ("MIME Type"). The MIME Type follows the format of https://www.iana.org/assignments/media-types/media-types.xhtml. Also please note the FILE EXTENSION was .txt for this GIF image file. 36) The SID for jbeatty is S-1-5-21-2298470282-2867887670-580413564-1119. 38) thumb-cts24-5562.E01\Partition 1\filez [NTFS]\[root]\206969.doc. *In other words the root directory of the thumb drive on Partition 1 which was formatted NTFS*
ZQ4URL-5562	Our lab didn't recieve USB flash drive for this test. In Q13, answer is also located in Recycle bin, path and filename: \$Recycle.Bin\S-1-5-21-2298470282-2867887670-580413564-1117\$RCZUXP4.jpg
ZU7QJ2-5561	The opportunity to attach a report of findings in this space would be appreciated.
ZWABN2-5562	Thank you!!

-End of Report-
(Appendix may follow)