Computer Hard Drive - Windows Analysis
Test No. 25-5561/2 Summary Report

Each participant received data extracted from a Windows 11 Pro computer hard drive, while those in test 5562 also received a physical USB drive and were asked to analyze the material and answer questions using their own tools and methods. Data, associated with questions #1-28, were returned from 130 participants, 61 of whom also returned results associated with the USB. These results are compiled in the following tables:

Manufacturer's Information

The Computer Hard Drive – Windows Analysis test (5561/5562) consisted of evidence data, provided in an E01 file format, and acquired from a computer running Windows 11 Pro. 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 Computer Hard Drive – Windows & Removable Media Storage Analysis (5562) test received a physical USB drive as an additional component. These participants were also asked to perform evidence acquisition, extraction, and analysis.

SAMPLE PREPARATION/VALIDATION
A scripted scenario was created and used to generate user data on a Windows Hard Drive. The execution of the test production took place within the following date range, 17 February 2025 and 4 March 2025. 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 test 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. A MD5 digest (cryptographic checksum, or 'hash') was 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: X-Ways Forensics 21.4, FTK Imager 4.5.0.3, Autopsy 4.21.0, EnCase 22.3.0.124, ExifTool 12.65, RegRipper 3.0, 7-Zip 24.09, HxD 2.5.0.0, PECmd 1.6.0.0, Registry Explorer 2.1.0.0, DB Browser 3.12.2, FileAlyzer 2.0.5.57, and GIMP 2.10. 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

Dana DeResident, seeking a new home, found an online listing for an attractive rental property. After online contact and discussion with the listing agent, DeResident signed a contract to lease the property, paid the deposit and first month's rent to the listing agent, and received a key-code to access the property.

When DeResident tried to access the property, her access code did not work. She subsequently contacted the property manager who advised her the 'listing agent' she had communicated with was not affiliated with the property. DeResident filed a report with the local police department who opened an investigation.

Using information provided by the online listing service and internet service provider, police investigators identified an address associated with the account used to post the online listing. The police agency local to that address used this information to obtain and execute a search warrant for evidence related to this fraud.

In accordance with the issued warrant, investigators seized the computer which has been provided to you (the participant) for analysis.
You have appropriate legal authority to examine the computer (5561/5562) and one USB flash media device (5562) for evidence related to the investigation and perform analysis of the data on the device(s) to answer the following questions.

Manufacturer's Information, continued

Question   _Manufacturer's Response_

1   **Provide the stored verification [acquisition] hash, SHA-1, for the provided image, 25-5561.E01, within the container. Do not provide the hash of the container file itself as this is already provided to you on the front page of the data entry form to verify the download. Transfer the hash carefully.**
    7A0311AD60A8E2686A5DFF06E509A76E1D6C215B

2   **What is the hostname (Computer Name) for this computer?**
    DESKTOP-P8SVDMN

3   **What operating system (include version and edition) was installed on this computer? (e.g. "Windows 7, Home")**
    Windows 10, Pro; or Windows 11, Pro

4   **Who is listed as the "registered owner" for this installation of Windows?**
    thomas

5   **List the non-built-in user account(s) (name(s)) on this computer.**
    thomas
    Martha

6   **What time zone was this computer configured to display? Provide answer as name (e.g. Atlantic Time).**
    US Mountain Standard Time

7   **Provide the BSSID (network name) of the Wi-Fi hotspot MAC Address 16-E4-C2-A6-28-95.**
    zion

8 **   **Provide the filetype (file format) for the file containing the keyword "Otuscommersoni".**
    SQLite or SQLite 3 (Database)

9   **For the file created 02/26/2025 (February 26, 2025) 20:44:21 (subject computer's local time), provide the source (host URL) of this file, according to its metadata.**
    https://ar.rdcpix.com , or
    _https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp_

10 **According to Windows Prefetch, what application was executed at 03/03/2025 (March 3, 2025) 16:28:57 (subject computer's local time)?**
    REALTOR.EXE

11   **From what path (include the drive letter) was the application identified in question 10 executed?**
    G:\apps\realtor.exe, or
    G:\apps

12 **A Windows registry key value contains the following enciphered text: P:\Hfref\gubznf\Qbjaybnqf\ariretbaantvirlbhhc.rkr. What is the deciphered value (text)?**
    C:\Users\thomas\Downloads\nevergonnagiveyouup.exe

Manufacturer's Information, continued

Question   *Manufacturer's Response*

13   **Provide the filetype (file format) for C: \Users\thomas\text.txt.**
Microsoft Portable Executable; or
Windows Executable; or
DOS Executable, or
Application

14   **Provide the filename for the MP3 recently opened by user thomas.**
groovy-ambient-funk-201745.mp3

15   **What terms did the user search for with the Edge browser, 02/19/25 (February 19, 2025) 20:10:21 (subject computer's local time)?**
"philadelphia houses for rent"

16   **What 3rd party (non-Microsoft) email client was installed and in use on the subject computer?**
Mozilla Thunderbird

17   **Provide the text in the file named "the answer to question 17".**
"Never gonna give you up"

18   **What email address was the installed (non-Microsoft) email client configured to use?**
leslielessor@gmail.com

19   **What email address sent the email with sent date/time of 02/27/25 (February 27, 2025) 19:34:34 (subject computer's local time)?**
danaderesident@gmail.com

20   **Provide the original (pre-deletion) path of philly_2.pdf.**
C:\Users\thomas\Desktop\philly_2.pdf

21   **When was C:\Users\thomas\Desktop\Microsoft Edge.lnk deleted? Provide date and time with offset of device configured local time, using the date/time (24-hour) picker which presents the date/time in the following format: YYYY-MM-DD HH:MM.**
2025-03-02 10:01

22   **Provide the cross-streets for the closest intersection to the GPS coordinates embedded in the photograph taken with an Olympus Stylus 1 digital camera.**
Woodshire Dr. and Gentry Dr.

23   **Describe the contents of cat.xcf?**
An image of an old cat "cougar.jpg", and a red bordered image of a kitten, "kitten.jpg"

24   **Find the file containing the string "realestateagent" where each of the vowels have been replaced with one of the following characters ~!@#$%^&*(). Provide the PATH and FILENAME, and the RESULTANT STRING.**
Path & Filename: C: \Users\thomas\Documents\Realestateagent.txt
*Resultant string: r~@l#st@t#&g*nt*

25   **In unallocated space on the subject volume is a photograph (picture file) of an alligator with a green border, containing white text beginning with "CTS", provide the complete text visible in the picture.**
CTS2025-A1.1

Manufacturer's Information, continued

Question   ***Manufacturer's Response***

26   **At what time did the user thomas first log in on 02/24/2025 (February 24, 2025) (UTC time)? Provide your answer in UTC time, using this format: HH:MM.**
      02:28

27   **Who is listed as the author of the spreadsheet document containing the keywords "philly", "Wilmington", and "phoenix"?**
      Leslie Lessor

28   **Provide the names of the files the user accessed from the H:\k\ directory.**
      1852232766.jpg, 778494116.jpg

Manufacturer's Information, continued

Removable Media Analysis: *USB Storage Device*
Test No. 25-5562

Question   ***Manufacturer's Response***

29 **Provide a physical description of the provided evidence item, as well as the unique Identifier written in marker.**
Responses will vary but should include the CTS assigned number (written on the device), and a description of a black USB stick flash media storage device with silver cover, etc.

30 **Provide the SHA256 hash of the provided USB flash storage device. Transfer the hash carefully.**
CCC57620030E10D90E77F50D23E5A1AC51EFFC4C9D834F39194C247EDBC2822C

31 **Identify the filesystem on each partition on this device. Provide partition number, filesystem, and volume name/label for all partitions.**
1. *exFat, [unnamed / NONAME]*
2. *NTFS, "NTFS"*
3. *FAT32, "SMALL"*
4. *NTFS, "misc"*

32 **What is the full path (partition name\parent directory\file) for the picture file which lists "Collaborative" as the Creator/Author?**
[Partition1 NONAME]\50 E. Ramblewood St..jpeg

33 **On the device is a purple-bordered photo of a black dog running on a beach. Provide the text that appears in the image.**
CTS2025-D25

34 **Provide the filetype (file format) for the file with SHA256 hash DD8F4F698DDEEA89BEEAF02ECD61453DB7E00947B6E488CE8E4ABEDA33B4FA28.**
Text file

35 **Provide the Windows Security Identifier (SID) of the user account that is the owner of files in the "k" directory.**
S-1-5-21-3142915031-3623484693-281401572-1001

36 **Provide the username corresponding with the SID identified in question 35.**
thomas

37 **Provide the file header (file signature, in ASCII) of the file containing the keyword "arcseconds".**
SIMPLE

38 **Provide the title (not the filename) of the document authored by David McGuirk.**
NOAA GEO-IDE Plan

39 **What artifact suggests this device was forensically sanitized prior to use?**
The observation that the free space had been overwritten with a recognizable pattern: collaborative-testing.com_collaborative-testing.com…

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 25-5562: Computer Hard Drive – Windows & Removable Media Storage Analysis test received a physical USB drive. These participants were asked to analyze various digital artifacts including: image details, settings, external media, native and third-party applications, communications, and web browser history. Refer to the Manufacturer's Information for preparation details.

A total of 130 participants returned results for the 5561 Computer Hard Drive - Windows Analysis test (questions #1-28). Of the 28 total questions, one did not reach a consensus response. Question #8 asked for the filetype for the file containing the word "Otuscommersoni". Approximately 73.8% of responding participants reported the Manufacturer's response, whereas 22.3% reported '.sys' and other variations of this response.

A total of 61 participants returned results for the 5562 Removable Media Storage Analysis test (questions #29-41). All questions reached consensus.

A 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.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 1 - Examination Questions

Question 1: Provide the stored verification [acquisition] hash, SHA-1, for the provided image, 25-5561.E01, within the container. Do not provide the hash of the container file itself as this is already provided to you on the front page of the data entry form to verify the download. Transfer the hash carefully.

Manufacturer's Response: 7A0311AD60A8E2686A5DFF06E509A76E1D6C215B

WebCode Test	Response
24VY4B-5561	7A0311AD60A8E2686A5DFF06E509A76E1D6C215B
24WLMH-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
2RG9U9-5562	ECE302C7A12DD53B2E8AF15E82DB4692D5A19AC8
2U4TZC-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
349ZFC-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
3BYPCG-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
3GDA68-5561	ece302c7a12dd53b2e8af15e82db4692d5a19ac8
3J4DXE-5562	ece302c7a12dd53b2e8af15e82db4692d5a19ac8
3PA7TA-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
4FFFK9-5561	7A0311AD60A8E2686A5DFF06E509A76E1D6C215B
4RN848-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
4ZJ2KE-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
63LLN6-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
673VQB-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
6PJ238-5561	ece302c7a12dd53b2e8af15e82db4692d5a19ac8
7CQT46-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
7PVVH8-5561	7A0311AD60A8E2686A5DFF06E509A76E1D6C215B
8FPDKA-5562	7A0311AD60A8E2686A5DFF06E509A76E1D6C215B
8KE4Q6-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 1 - Examination Questions	
WebCode Test	**Response**
8TBZD8-5562	7A0311AD60A8E2686A5DFF06E509A76E1D6C215B
8WNN47-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
A444U7-5562	SHA1: ece302c7a12dd53b2e8af15e82db4692d5a19ac8
AEKNE3-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
AFF7G6-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
AUY2L3-5562	7A0311AD60A8E2686A5DFF06E509A76E1D6C215B
AXDN7Y-5561	ece302c7a12dd53b2e8af15e82db4692d5a19ac8
B7LHX8-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
B8ELJ2-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
BEGRX4-5562	7A0311AD60A8E2686A5DFF06E509A76E1D6C215B
BTXP36-5562	ECE302C7A12DD53B2E8AF15E82DB4692D5A19AC8 (SHA1 base 16)
CDHZN3-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
CTEYRY-5562	ECE302C7A12DD53B2E8AF15E82DB4692D5A19AC8
CWHMF2-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
DB9AYY-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
DJLBA2-5562	ECE302C7A12DD53B2E8AF15E82DB4692D5A19AC8
DPCKJZ-5561	ECE302C7A12DD53B2E8AF15E82DB4692D5A19AC8
E6FEQZ-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
EYTN7P-5562	ece302c7a12dd53b2e8af15e82db4692d5a19ac8
F4KDZ3-5562	ECE302C7A12DD53B2E8AF15E82DB4692D5A19AC8
FJ22JX-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
FMYKLW-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 1 - Examination Questions	
WebCode Test	**Response**
GA6R7K-5561	BB12EEDC594224738D3C1FB20FACD4BBA1103ADD103F15EF6B64CAA0B0C5EC57
GA8D2Z-5562	7A0311AD60A8E2686A5DFF06E509A76E1D6C215B
GJP4GX-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
GPH4VT-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
GQUT6W-5561	7A0311AD60A8E2686A5DFF06E509A76E1D6C215B
GTHERT-5562	SHA1 : 7a0311ad60a8e2686a5dff06e509a76e1d6c215b
GTZ73X-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
HEX8ER-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
HF9WVJ-5561	ece302c7a12dd53b2e8af15e82db4692d5a19ac8
HFCE3U-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
HXUD8T-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
HYZ6QT-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
J2L9YQ-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
J7HNUT-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
JGEWDV-5562	SHA1: 7A0311AD60A8E2686A5DFF06E509A76E1D6C215B
JYYMCV-5561	7A0311AD60A8E2686A5DFF06E509A76E1D6C215B
JZU7EW-5561	7A0311AD60A8E2686A5DFF06E509A76E1D6C215B
K2HYQQ-5561	7A0311AD60A8E2686A5DFF06E509A76E1D6C215B
K7CZKT-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
KA8UHU-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
KYBNNV-5562	The stored verification hash value for the 25-5561.E01 image is as follows: 7a0311ad60a8e2686a5dff06e509a76e1d6c215b
L7QRBN-5561	7A0311AD60A8E2686A5DFF06E509A76E1D6C215B

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 1 - Examination Questions	
WebCode Test	**Response**
LACBFT-5562	7A0311AD60A8E2686A5DFF06E509A76E1D6C215B, ece302c7a12dd53b2e8af15e82db4692d5a19ac8
LKDRCP-5561	7A0311AD60A8E2686A5DFF06E509A76E1D6C215B
LMYFNP-5561	ECE302C7A12DD53B2E8AF15E82DB4692D5A19AC8
LN7VWF-5562	BB12EEDC594224738D3C1FB20FACD4BBA1103ADD103F15EF6B64CAA0B0C5EC57
LRRKGT-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
LUECCW-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
LYJAEX-5561	711c8c1D07fac0f60406167b19c1e5fd
M2VAHU-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
MD7R7R-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
MGM8JP-5561	7A0311AD60A8E2686A5DFF06E509A76E1D6C215B
ML4AQV-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
MQXA6Q-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
MR7JXN-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
MRTR8R-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
MV6VTN-5562	7A0311AD60A8E2686A5DFF06E509A76E1D6C215B
NJQ8AP-5561	ece302c7a12dd53b2e8af15e82db4692d5a19ac8
NK3WJT-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
PAF6NN-5561	ece302c7a12dd53b2e8af15e82db4692d5a19ac8
PPBH8Q-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
PQH2LD-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
PZAD6L-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
Q2Z3GD-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 1 - Examination Questions	
WebCode Test	**Response**
QCLZQR-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
QEMD4J-5561	EO1 Hash - ECE302C7A12DD53B2E8AF15E82DB4692D5A19AC8
QH4FBN-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
QT7QQQ-5561	ECE302C7A12DD53B2E8AF15E82DB4692D5A19AC8
QWAN2J-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b (used FTK Imager to calculate hash)
QYVDDJ-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
R86XKL-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
RBJUPN-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
REKXEP-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
RR9ZXG-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
T8JQPN-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
T8LHLB-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
TGQH3P-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
THHLMJ-5562	7A0311AD60A8E2686A5DFF06E509A76E1D6C215B
TRHDUP-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
TVPPWK-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
TZXUNK-5561	ECE302C7A12DD53B2E8AF15E82DB4692D5A19AC8
U3GARK-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
U4CRUL-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
UGJTDH-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
UT9WBG-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
V63DZH-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 1 - Examination Questions	
WebCode Test	**Response**
VJJLKL-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
VLV2EM-5561	Md5: 82fcff911fff27899f5035e454862356 - sha-1: 385ab346d1c46069196a501abaff0b798531008b
VYH7LJ-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
W7CX8H-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
W9FNCC-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
WH87QK-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
WKE9TJ-5562	7A0311AD60A8E2686A5DFF06E509A76E1D6C215B
WRVWDD-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
WVD7FJ-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
X9VFGE-5562	SHA1: 7a0311ad60a8e2686a5dff06e509a76e1d6c215b
XDUKGE-5562	7A0311AD60A8E2686A5DFF06E509A76E1D6C215B
XFRBFD-5561	7A0311AD60A8E2686A5DFF06E509A76E1D6C215B
XGRD6G-5562	e0eaa25e75ff6facab1c85896758d473
XMC987-5562	ece302c7a12dd53b2e8af15e82db4692d5a19ac8
XY6VCG-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
Y36EXF-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
YVMR6B-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
YVR6WD-5561	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
Z8XMWF-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
ZBE3BE-5561	SHA-1: 7a0311ad60a8e2686a5dff06e509a76e1d6c215b
ZNK3ZC-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b
ZRL9H3-5562	385ab346d1c46069196a501abaff0b798531008b

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 1 - Examination Questions	
WebCode Test	**Response**
ZZUWEA-5562	7a0311ad60a8e2686a5dff06e509a76e1d6c215b

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 1 - Examination Questions

Question 1: Provide the stored verification [acquisition] hash, SHA-1, for the provided image, 25-5561.E01, within the container. Do not provide the hash of the container file itself as this is already provided to you on the front page of the data entry form to verify the download. Transfer the hash carefully.

Consensus Result:

7A0311AD60A8E2686A5DFF06E509A76E1D6C215B

Manufacturer's Response Explanation:

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

Manufacturer's Response Illustration:

X-Ways view of 25-5561.E01 stored verification hash

EnCase view of 25-5561.E01 stored verification hash

```
1    Name      Laptop Computer SN:Z1ON0101
10   Acquisition MD5 e0eaa25e75ff6facab1c85896758d473
11   Verification MD5    e0eaa25e75ff6facab1c85896758d473
12   Acquisition SHA1    7a0311ad60a8e2686a5dff06e509a76e1d6c215b
13   Verification SHA1   7a0311ad60a8e2686a5dff06e509a76e1d6c215b
```

Other Responses:

A total of 20 (15%) participants reported the MD5 hash of the container file, ece302c7a12dd53b2e8af15e82db4692d5a19ac8, not the stored verification hash of the provided image.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 2 - Examination Questions

Question 2: What is the hostname (Computer Name) for this computer?

Manufacturer's
Response: DESKTOP-P8SVDMN

WebCode Test	Response
24VY4B-5561	DESKTOP-P8SVDMN
24WLMH-5561	DESKTOP-P8SVDMN
2RG9U9-5562	DESKTOP-P8SVDMN
2U4TZC-5561	DESKTOP-P8SVDMN
349ZFC-5562	DESKTOP-P8SVDMN
3BYPCG-5561	DESKTOP-P8SVDMN
3GDA68-5561	DESKTOP-P8SVDMN
3J4DXE-5562	DESKTOP-P8SVDMN
3PA7TA-5561	DESKTOP-P8SVDMN
4FFFK9-5561	DESKTOP-P8SVDMN
4RN848-5561	DESKTOP-P8SVDMN
4ZJ2KE-5562	DESKTOP-P8SVDMN
63LLN6-5561	DESKTOP-P8SVDMN
673VQB-5562	DESKTOP-P8SVDMN
6PJ238-5561	DESKTOP-P8SVDMN
7CQT46-5561	DESKTOP-P8SVDMN
7PVVH8-5561	DESKTOP-P8SVDMN
8FPDKA-5562	DESKTOP-P8SVDMN
8KE4Q6-5561	DESKTOP-P8SVDMN
8TBZD8-5562	Not in scope.
8WNN47-5562	DESKTOP-P8SVDMN

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 2 - Examination Questions	
WebCode Test	**Response**
A444U7-5562	DESKTOP-P8SVDMN
AEKNE3-5561	DESKTOP-P8SVDMN
AFF7G6-5561	DESKTOP-P8SVDMN
AUY2L3-5562	DESKTOP-P8SVDMN
AXDN7Y-5561	DESKTOP-P8SVDMN
B7LHX8-5561	DESKTOP-P8SVDMN
B8ELJ2-5561	DESKTOP-P8SVDMN
BEGRX4-5562	DESKTOP-P8SVDMN
BTXP36-5562	DESKTOP-P8SVDMN
CDHZN3-5561	DESKTOP-P8SVDMN
CTEYRY-5562	DESKTOP-P8SVDMN
CWHMF2-5561	DESKTOP-P8SVDMN
DB9AYY-5561	DESKTOP-P8SVDMN
DJLBA2-5562	DESKTOP-P8SVDMN
DPCKJZ-5561	DESKTOP-P8SVDMN
E6FEQZ-5562	DESKTOP-P8SVDMN
EYTN7P-5562	DESKTOP-P8SVDMN
F4KDZ3-5562	DESKTOP-P8SVDMN
FJ22JX-5562	DESKTOP-P8SVDMN
FMYKLW-5561	DESKTOP-P8SVDMN
GA6R7K-5561	DESKTOP-P8SVDMN
GA8D2Z-5562	DESKTOP-P8SVDMN

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 2 - Examination Questions	
WebCode Test	**Response**
GJP4GX-5562	DESKTOP-P8SVDMN
GPH4VT-5561	DESKTOP-P8SVDMN
GQUT6W-5561	DESKTOP-P8SVDMN
GTHERT-5562	DESKTOP-P8SVDMN
GTZ73X-5562	DESKTOP-P8SVDMN
HEX8ER-5562	DESKTOP-P8SVDMN
HF9WVJ-5561	DESKTOP-P8SVDMN
HFCE3U-5561	DESKTOP-P8SVDMN
HXUD8T-5562	DESKTOP-P8SVDMN
HYZ6QT-5562	DESKTOP-P8SVDMN
J2L9YQ-5561	DESKTOP-P8SVDMN
J7HNUT-5561	DESKTOP-P8SVDMN
JGEWDV-5562	DESKTOP-P8SVDMN
JYYMCV-5561	DESKTOP-P8SVDMN
JZU7EW-5561	DESKTOP-P8SVDMN
K2HYQQ-5561	DESKTOP-P8SVDMN
K7CZKT-5562	DESKTOP-P8SVDMN
KA8UHU-5562	DESKTOP-P8SVDMN
KYBNNV-5562	The computer name for this machine is DESKTOP-P8SVDMN
L7QRBN-5561	DESKTOP-P8SVDMN
LACBFT-5562	DESKTOP-P8SVDMN
LKDRCP-5561	DESKTOP-P8SVDMN

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 2 - Examination Questions	
WebCode Test	**Response**
LMYFNP-5561	DESKTOP-P8SVDMN
LN7VWF-5562	DESKTOP-P8SVDMN
LRRKGT-5562	DESKTOP-P8SVDMN
LUECCW-5561	DESKTOP-P8SVDMN
LYJAEX-5561	DESKTOP-P8SVDMN
M2VAHU-5562	DESKTOP-P8SVDMN
MD7R7R-5562	DESKTOP-P8SVDMN
MGM8JP-5561	DESKTOP-P8SVDMN
ML4AQV-5561	DESKTOP-P8SVDMN
MQXA6Q-5562	DESKTOP-P8SVDMN
MR7JXN-5561	DESKTOP-P8SVDMN
MRTR8R-5561	DESKTOP-P8SVDMN
MV6VTN-5562	DESKTOP-P8SVDMN
NJQ8AP-5561	DESKTOP-P8SVDMN
NK3WJT-5561	DESKTOP-P8SVDMN
PAF6NN-5561	DESKTOP-P8SVDMN
PPBH8Q-5561	DESKTOP-P8SVDMN
PQH2LD-5561	DESKTOP-P8SVDMN
PZAD6L-5561	DESKTOP-P8SVDMN
Q2Z3GD-5562	DESKTOP-P8SVDMN
QCLZQR-5562	DESKTOP-P8SVDMN
QEMD4J-5561	DESKTOP-P8SVDMN

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 2 - Examination Questions	
WebCode Test	**Response**
QH4FBN-5562	DESKTOP-P8SVDMN
QT7QQQ-5561	DESKTOP-P8SVDMN
QWAN2J-5561	DESKTOP-P8SVDMN
QYVDDJ-5561	DESKTOP-P8SVDMN
R86XKL-5561	DESKTOP-P8SVDMN
RBJUPN-5561	DESKTOP-P8SVDMN
REKXEP-5561	DESKTOP-P8SVDMN
RR9ZXG-5561	DESKTOP-P8SVDMN
T8JQPN-5562	DESKTOP-P8SVDMN
T8LHLB-5561	DESKTOP-P8SVDMN
TGQH3P-5561	DESKTOP-P8SVDMN
THHLMJ-5562	DESKTOP-P8SVDMN
TRHDUP-5562	DESKTOP-P8SVDMN
TVPPWK-5562	DESKTOP-P8SVDMN
TZXUNK-5561	DESKTOP-P8SVDMN
U3GARK-5562	DESKTOP-P8SVDMN
U4CRUL-5562	DESKTOP-P8SVDMN
UGJTDH-5561	DESKTOP-P8SVDMN
UT9WBG-5562	DESKTOP-P8SVDMN
V63DZH-5562	DESKTOP-P8SVDMN
VJJLKL-5562	DESKTOP-P8SVDMN
VLV2EM-5561	Thomas

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 2 - Examination Questions	
WebCode Test	**Response**
VYH7LJ-5561	DESKTOP-P8SVDMN
W7CX8H-5562	DESKTOP-P8SVDMN
W9FNCC-5561	DESKTOP-P8SVDMN
WH87QK-5562	DESKTOP-P8SVDMN
WKE9TJ-5562	DESKTOP-P8SVDMN
WRVWDD-5561	DESKTOP-P8SVDMN
WVD7FJ-5562	Desktop-P8SVDMN
X9VFGE-5562	Laptop Computer SN:Z1ON0101
XDUKGE-5562	DESKTOP-P8SVDMN
XFRBFD-5561	DESKTOP-P8SVDMN
XGRD6G-5562	DESKTOP-P8SVDMN
XMC987-5562	DESKTOP-P8SVDMN
XY6VCG-5562	DESKTOP-P8SVDMN
Y36EXF-5561	DESKTOP-P8SVDMN
YVMR6B-5561	DESKTOP-P8SVDMN
YVR6WD-5561	DESKTOP-P8SVDMN
Z8XMWF-5562	DESKTOP-P8SVDMN
ZBE3BE-5561	DESKTOP-P8SVDMN
ZNK3ZC-5562	DESKTOP-P8SVDMN
ZRL9H3-5562	DESKTOP-P8SVDMN
ZZUWEA-5562	DESKTOP-P8SVDMN

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 2 - Examination Questions

Question 2: What is the hostname (Computer Name) for this computer?
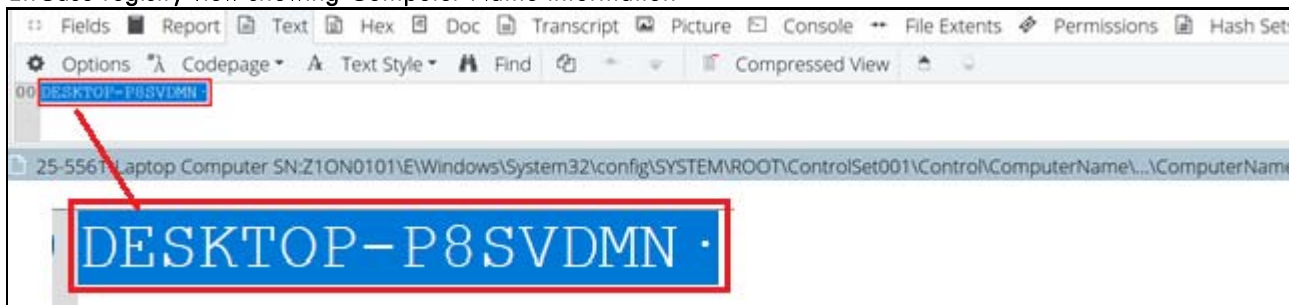
Consensus Result:

DESKTOP-P8SVDMN

Manufacturer's Response Explanation:

Windows Computer Name information is stored in the Windows System registry at ControlSet001\Control\ComputerName\ComputerName.

Manufacturer's Response Illustration:

EnCase registry view showing Computer Name information

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3 - Examination Questions

Question 3: What operating system (include version and edition) was installed on this computer? (e.g. "Windows 7, Home")

<u>Manufacturer's Response:</u>   Windows 10, Pro; or Windows 11, Pro

WebCode Test	Response
24VY4B-5561	Windows 11 Professional v. 6.3
24WLMH-5561	Windows 11 Professional (2009) ver 6.3
2RG9U9-5562	Windows 11 Professional (2009) v6.3 Build 22631
2U4TZC-5561	Windows 11 Professional
349ZFC-5562	Windows 10 Pro (professional)
3BYPCG-5561	Windows 11 Professional (2009)
3GDA68-5561	Windows 11 Professional (2009) Version 6.3
3J4DXE-5562	Windows 11, Professional, version: 6.3
3PA7TA-5561	Windows 11, Professional
4FFFK9-5561	Windows 11, Professional
4RN848-5561	Windows 10 Pro
4ZJ2KE-5562	Windows 10 Pro
63LLN6-5561	Windows 11 Professional version 6.3
673VQB-5562	Windows 11, Professional (2009), UPDATED FROM WINDOWS 10
6PJ238-5561	Windows 11, Professional
7CQT46-5561	Windows 11 Professional (2009)
7PVVH8-5561	Windows 11 Professional (2009)
8FPDKA-5562	Windows 11 Professional (2009) Version Number 6.3
8KE4Q6-5561	Windows 11, Pro 22631 (23H2)
8TBZD8-5562	Not in scope.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3 - Examination Questions	
WebCode Test	**Response**
8WNN47-5562	Windows 11, Professional
A444U7-5562	Windows 11 Professional (2009) v.6.3
AEKNE3-5561	Windows 11 Professional
AFF7G6-5561	Windows 11 Professional (2009) version 6.3 build 22631
AUY2L3-5562	Windows 11 Professional (2009), version 6.3, build 22631
AXDN7Y-5561	Windows 10 Pro, Professional
B7LHX8-5561	Windows 11 Professional (2009)
B8ELJ2-5561	Windows 11 Professional
BEGRX4-5562	Windows 11, Professional
BTXP36-5562	Windows 10 Pro, Upgraded to Windows 11 Pro.
CDHZN3-5561	Windows 11 Professional
CTEYRY-5562	Windows 11, Professional
CWHMF2-5561	Windows 11 Professional
DB9AYY-5561	Windows 11, Professional
DJLBA2-5562	Windows 10, Professional
DPCKJZ-5561	Windows 11, Professional
E6FEQZ-5562	Windows 11 Professional (2009) Version 6.3 Build Number 22631
EYTN7P-5562	Windows 11 Professional (2009) 6.3
F4KDZ3-5562	Windows 10 Pro
FJ22JX-5562	Windows 11 Professional (2009), Version 6.3, Build: 22631
FMYKLW-5561	Windows 10 Pro (Edition: Professional, Version: 6.3)
GA6R7K-5561	Windows 10 Pro

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3 - Examination Questions	
WebCode Test	**Response**
GA8D2Z-5562	Windows 11 Pro 6.3
GJP4GX-5562	Windows 11 Professional
GPH4VT-5561	Windows 11, Professional or Windows 10, Professional
GQUT6W-5561	Windows 11 Professional (2009), Version 6.3, Build: 22631
GTHERT-5562	Windows 11 Professional (2009) version 6.3
GTZ73X-5562	Windows 11 Professional
HEX8ER-5562	Windows 11, Professional
HF9WVJ-5561	Windows 11, Professional
HFCE3U-5561	Windows 11, Professional, Version 6.3
HXUD8T-5562	Windows 11, Professional
HYZ6QT-5562	Windows 11, Professional, Version: 6.3, 23H2, Build:22631
J2L9YQ-5561	Windows 11 Professional (2009) / Version: 6.3
J7HNUT-5561	Windows 11 Professional (2009)
JGEWDV-5562	Windows 11 Pro, 23H2
JYYMCV-5561	Windows 11 Professional (2009), version 6.3
JZU7EW-5561	Windows 11 Pro
K2HYQQ-5561	Windows 11 Pro
K7CZKT-5562	Windows 11 Professional (2009) OS Version: 6.3 (Build 22631)
KA8UHU-5562	Windows 11, Professional
KYBNNV-5562	The operating system on the computer is Windows 11 Professional
L7QRBN-5561	Windows 11 Professional
LACBFT-5562	Windows 11, Professional

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3 - Examination Questions	
WebCode Test	**Response**
LKDRCP-5561	Windows 11 Pro
LMYFNP-5561	Windows 11 Professional, 6.3
LN7VWF-5562	Windows 10 Pro
LRRKGT-5562	Windows 10 Professional Enterprise Edition version 6.3
LUECCW-5561	Windows 10 Pro
LYJAEX-5561	Windows 10 Pro
M2VAHU-5562	"Windows 11 Professional (2009)"
MD7R7R-5562	Windows 10, Pro
MGM8JP-5561	Windows 11 Professional (2009) Version 6.3
ML4AQV-5561	Windows 10 Pro
MQXA6Q-5562	Windows 11, Professional
MR7JXN-5561	The registry key ProductName indicates Windows 10 Pro however when interpretting the build number it is Windows 11 so Windows 11 Professional Version 6.3 Build Number 22631; Please see additional comments.
MRTR8R-5561	Windows 11 Professional (2009) version 6.3 build 22631
MV6VTN-5562	Windows 11 Professional, version 6.3 (Referencing registry entries: 'CurrentBuild' - 22631, and 'DisplayVersion' - 23H2). See Comments
NJQ8AP-5561	Windows 11 Professional (2009), Version 6.3
NK3WJT-5561	Windows 10 Pro version 6.3
PAF6NN-5561	Windows 11 Professional (2009), Version 6.3
PPBH8Q-5561	Windows 11 Professional; Version 6.3 Professional Edition; Build 22631; Display Version 23H2 (Registry shows as Windows 10 Pro but 23H2 was not released for Windows 10).
PQH2LD-5561	Windows 11 Professional
PZAD6L-5561	Windows 11 Pro
Q2Z3GD-5562	Windows 11, Professional
QCLZQR-5562	Windows 10 Pro version 6.3 or Windows 11 Professional version 6.3

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3 - Examination Questions	
WebCode Test	**Response**
QEMD4J-5561	Windows 11 Pro, v6.3, build 22631 *Note, the OS reports it as Windows 10, but build 22631 is actually Windows 11.
QH4FBN-5562	Windows 11 Professional (2009)
QT7QQQ-5561	Windows 11 Professional (2009) v6.3
QWAN2J-5561	Windows 11 Professional (2009) Version 6.3, Build Number 22631
QYVDDJ-5561	Windows 11 Professional
R86XKL-5561	Windows 11 Professional
RBJUPN-5561	Windows 11 Professional, Version 6.3
REKXEP-5561	Windows 11 Professional (2009)
RR9ZXG-5561	Windows 11 Professional (2009), version 6.3 build 22631
T8JQPN-5562	Windows 11 Professional, Version 23H2, 22631.4890
T8LHLB-5561	Windows 11, Professional (6.3)
TGQH3P-5561	Windows 10 Pro (Professional) version 6.3
THHLMJ-5562	Windows 11 Professional Build 22631
TRHDUP-5562	Windows 11 Professional (2009)
TVPPWK-5562	Windows 11 Professional 22631
TZXUNK-5561	Windows 11 Professional (2009) ver.6.3
U3GARK-5562	Windows 10 Professional (2009); build: 22631; Version Number: 6.3
U4CRUL-5562	Windows 11 Professional (2009), Version 6.3, Build 22631
UGJTDH-5561	Windows 11 Professional (2009)
UT9WBG-5562	Windows 11 Professional, Version 2009 (Build 22631)
V63DZH-5562	Windows 10 Pro 22631, Display version 23H2
VJJLKL-5562	Windows 11 Professional version 6.3, Windows Pro 10, and Windows Enterprise version 6.3

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3 - Examination Questions	
WebCode Test	**Response**
VLV2EM-5561	Windows 11 Professional (2009)
VYH7LJ-5561	Windows 11 Version 6.3 Professional Edition
W7CX8H-5562	Windows 11, Enterprise (which is a rebranded Windows 10, Pro)
W9FNCC-5561	Windows 11 Professional (2009) , version 6.3 Build 22631
WH87QK-5562	Windows 10 Pro version 6.3 or Windows 11 Professional (2009) version 6.3
WKE9TJ-5562	Windows 11 Professional (2009)
WRVWDD-5561	Windows 11 Professional Version 6.3
WVD7FJ-5562	Windows 11 Professional (2009)
X9VFGE-5562	Windows 10 Pro
XDUKGE-5562	Windows 11, Professional
XFRBFD-5561	Windows 11 Pro
XGRD6G-5562	Windows 10 Professional Version 6.3; Updated to Windows 11 Professional Version 6.3
XMC987-5562	Version: Windows 10 Pro , Edition: Professional
XY6VCG-5562	Windows 11 Professional (2009)
Y36EXF-5561	Windows 11, Professional (2009), version 6.3
YVMR6B-5561	Windows 11 Professional
YVR6WD-5561	Windows 11 Professional
Z8XMWF-5562	Windows 10 Professional (2009)
ZBE3BE-5561	Windows 11 Professional (2009), version 6.3
ZNK3ZC-5562	Windows 11 Pro (2009) v6.3 23H2
ZRL9H3-5562	Windows 11 Professional (2009)
ZZUWEA-5562	Windows 11 Professional (2009)

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3 - Examination Questions

Question 3: What operating system (include version and edition) was installed on this computer? (e.g. "Windows 7, Home")

<u>Consensus Result:</u>

Windows 10, Pro; or Windows 11, Pro

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

Windows operating system information is found in the registry at C:\Windows\System32\Config\Software: Microsoft\Windows NT\CurrentVersion: ProductName. Windows 11 was installed on this computer, however, registry keys report this as Windows 10. The Display version, 23H2, is Windows 11.

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

RegRipper registry view showing Windows version and edition from the Software registry hive

```
winver v.20200525
(Software) Get Windows version & build info

ProductName              Windows 10 Pro
ReleaseID                2009
BuildLab                 22621.ni_release.220506-1250
BuildLabEx               22621.1.amd64fre.ni_release.220506-1250
CompositionEditionID     Enterprise
RegisteredOrganization
RegisteredOwner          thomas
UBR                      4890
InstallDate              2024-03-15 03:29:26Z
InstallTime              2024-03-15 03:29:26Z
UBR                      4890
```

X-Ways registry view showing Windows version and edition in the Software registry hive

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4 - Examination Questions

Question 4: Who is listed as the "registered owner" for this installation of Windows?

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

WebCode Test	Response
24VY4B-5561	thomas
24WLMH-5561	thomas
2RG9U9-5562	thomas
2U4TZC-5561	thomas
349ZFC-5562	thomas
3BYPCG-5561	thomas
3GDA68-5561	thomas
3J4DXE-5562	thomas
3PA7TA-5561	thomas
4FFFK9-5561	thomas
4RN848-5561	thomas
4ZJ2KE-5562	thomas
63LLN6-5561	thomas
673VQB-5562	thomas
6PJ238-5561	Thomas
7CQT46-5561	thomas
7PVVH8-5561	thomas
8FPDKA-5562	thomas
8KE4Q6-5561	thomas
8TBZD8-5562	Not in scope.
8WNN47-5562	thomas

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4 - Examination Questions	
WebCode Test	**Response**
A444U7-5562	Thomas
AEKNE3-5561	thomas
AFF7G6-5561	thomas
AUY2L3-5562	thomas
AXDN7Y-5561	thomas
B7LHX8-5561	Thomas
B8ELJ2-5561	thomas
BEGRX4-5562	Thomas
BTXP36-5562	Thomas
CDHZN3-5561	thomas
CTEYRY-5562	thomas
CWHMF2-5561	thomas
DB9AYY-5561	Thomas
DJLBA2-5562	thomas
DPCKJZ-5561	Thomas
E6FEQZ-5562	thomas
EYTN7P-5562	thomas
F4KDZ3-5562	thomas
FJ22JX-5562	thomas
FMYKLW-5561	thomas
GA6R7K-5561	thomas
GA8D2Z-5562	Thomas

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4 - Examination Questions	
WebCode Test	**Response**
GJP4GX-5562	thomas
GPH4VT-5561	thomas
GQUT6W-5561	thomas
GTHERT-5562	thomas
GTZ73X-5562	thomas
HEX8ER-5562	thomas
HF9WVJ-5561	thomas
HFCE3U-5561	thomas
HXUD8T-5562	thomas
HYZ6QT-5562	thomas
J2L9YQ-5561	thomas
J7HNUT-5561	thomas
JGEWDV-5562	thomas
JYYMCV-5561	thomas
JZU7EW-5561	thomas
K2HYQQ-5561	thomas
K7CZKT-5562	thomas
KA8UHU-5562	thomas
KYBNNV-5562	The registered owner for this Windows installation is "thomas"
L7QRBN-5561	thomas
LACBFT-5562	thomas
LKDRCP-5561	thomas

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4 - Examination Questions	
WebCode Test	**Response**
LMYFNP-5561	thomas
LN7VWF-5562	thomas
LRRKGT-5562	thomas
LUECCW-5561	thomas
LYJAEX-5561	thomas
M2VAHU-5562	thomas
MD7R7R-5562	thomas
MGM8JP-5561	thomas
ML4AQV-5561	thomas
MQXA6Q-5562	thomas
MR7JXN-5561	thomas
MRTR8R-5561	thomas
MV6VTN-5562	thomas
NJQ8AP-5561	thomas
NK3WJT-5561	thomas
PAF6NN-5561	thomas
PPBH8Q-5561	thomas
PQH2LD-5561	thomas
PZAD6L-5561	thomas
Q2Z3GD-5562	thomas
QCLZQR-5562	thomas
QEMD4J-5561	thomas

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4 - Examination Questions	
WebCode Test	**Response**
QH4FBN-5562	thomas
QT7QQQ-5561	thomas
QWAN2J-5561	thomas
QYVDDJ-5561	thomas
R86XKL-5561	thomas
RBJUPN-5561	thomas
REKXEP-5561	thomas
RR9ZXG-5561	thomas
T8JQPN-5562	thomas
T8LHLB-5561	thomas
TGQH3P-5561	thomas
THHLMJ-5562	Leslie (Name of registered person = Thomas)
TRHDUP-5562	thomas
TVPPWK-5562	thomas
TZXUNK-5561	thomas
U3GARK-5562	Thomas
U4CRUL-5562	Thomas
UGJTDH-5561	thomas
UT9WBG-5562	thomas
V63DZH-5562	thomas
VJJLKL-5562	thomas
VLV2EM-5561	thomas

Copyright ©2025 CTS, Inc

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4 - Examination Questions	
WebCode Test	**Response**
VYH7LJ-5561	thomas
W7CX8H-5562	thomas
W9FNCC-5561	thomas
WH87QK-5562	thomas
WKE9TJ-5562	thomas
WRVWDD-5561	thomas
WVD7FJ-5562	thomas
X9VFGE-5562	thomas
XDUKGE-5562	thomas
XFRBFD-5561	thomas
XGRD6G-5562	thomas
XMC987-5562	thomas
XY6VCG-5562	Thomas
Y36EXF-5561	thomas
YVMR6B-5561	Thomas
YVR6WD-5561	thomas
Z8XMWF-5562	thomas
ZBE3BE-5561	thomas
ZNK3ZC-5562	thomas
ZRL9H3-5562	thomas
ZZUWEA-5562	thomas

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4 - Examination Questions

Question 4: Who is listed as the "registered owner" for this installation of Windows?
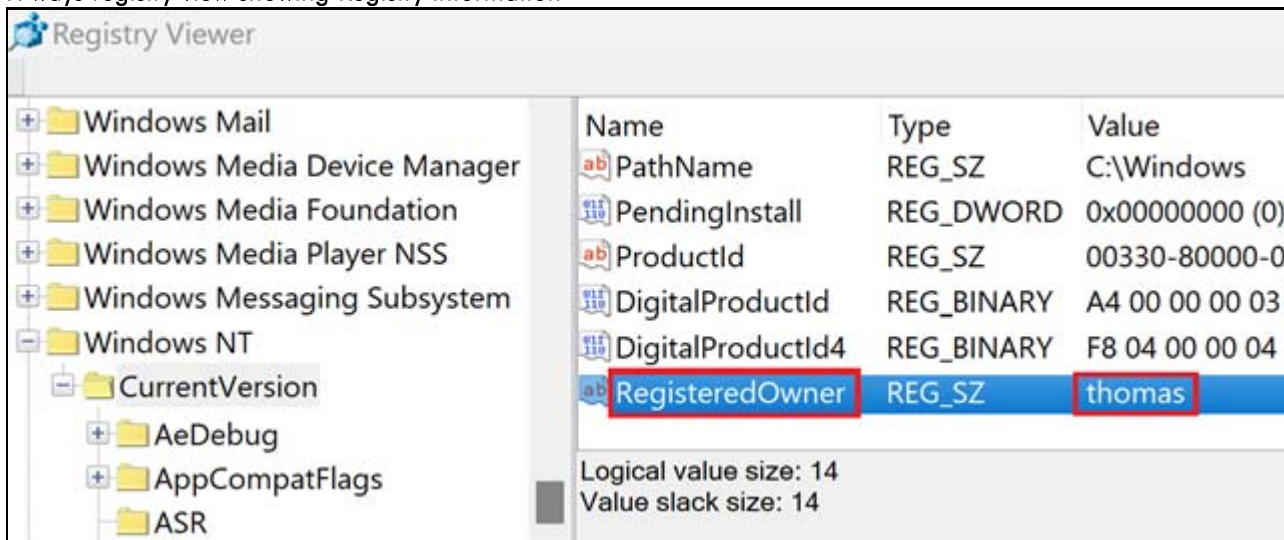
Consensus Result:

thomas

Manufacturer's Response Explanation:

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

Manufacturer's Response Illustration:

X-ways registry view showing Registry information

RegRipper registry view showing RegisteredOwner information

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 5 - Examination Questions

Question 5: List the non-built-in user account(s) (name(s)) on this computer.

Manufacturer's
Response:
thomas
Martha

WebCode Test	Response
24VY4B-5561	Martha and thomas
24WLMH-5561	thomas, Martha
2RG9U9-5562	thomas and Martha
2U4TZC-5561	Thomas (1001) Martha (1002)
349ZFC-5562	thomas, Martha, DefaultAccount, WDAGUtilityAcccount
3BYPCG-5561	thomas; Martha
3GDA68-5561	thomas, Martha
3J4DXE-5562	Martha, thomas
3PA7TA-5561	thomas, Martha
4FFFK9-5561	thomas, martha
4RN848-5561	users: Thomas, Martha,
4ZJ2KE-5562	thomas, Martha
63LLN6-5561	thomas; Martha
673VQB-5562	user: thomas & martha/default: DefaultAccount, Administrator, Guest, & WDAGUtilityAccount
6PJ238-5561	thomas; Martha
7CQT46-5561	Martha, Thomas
7PVVH8-5561	thomas; Martha – (user has yet to login for the first time)
8FPDKA-5562	thomas, Martha
8KE4Q6-5561	"thomas", "Martha"
8TBZD8-5562	Not in scope.
8WNN47-5562	thomas, Martha

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 5 - Examination Questions	
WebCode Test	**Response**
A444U7-5562	2 (Martha, thomas)
AEKNE3-5561	thomas, Martha
AFF7G6-5561	"thomas" (1001), "Martha" (1002)
AUY2L3-5562	Thomas and Martha
AXDN7Y-5561	Martha, thomas
B7LHX8-5561	thomas and Martha
B8ELJ2-5561	thomas; Martha
BEGRX4-5562	Thomas(1001), Martha (1002)
BTXP36-5562	Thomas and Marta
CDHZN3-5561	thomas and Martha
CTEYRY-5562	Martha, thomas
CWHMF2-5561	thomas, Martha
DB9AYY-5561	Thomas Martha Administrator Guests DefaultAccount WDAGUtilityAccount
DJLBA2-5562	Martha, Administrator, Guest, WDAGUtilityAccount, DefaultAccount, Default
DPCKJZ-5561	thomas, Martha
E6FEQZ-5562	thomas and Martha
EYTN7P-5562	thomas, Administrator, Guest, DefaultAccount, WDAGUtilityAccount, Martha
F4KDZ3-5562	Martha, Thomas
FJ22JX-5562	thomas (1001), Martha (1002)
FMYKLW-5561	thomas, Martha
GA6R7K-5561	Martha
GA8D2Z-5562	Thomas, Martha

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

WebCode Test	Response
GJP4GX-5562	thomas, Martha
GPH4VT-5561	thomas Martha
GQUT6W-5561	thomas, Martha
GTHERT-5562	thomas and Martha
GTZ73X-5562	thomas, Martha
HEX8ER-5562	Martha, thomas
HF9WVJ-5561	Thomas, Martha
HFCE3U-5561	thomas and Martha
HXUD8T-5562	thomas, Martha
HYZ6QT-5562	thomas, Martha
J2L9YQ-5561	thomas; Martha
J7HNUT-5561	Martha, thomas
JGEWDV-5562	thomas & Martha
JYYMCV-5561	Thomas, Administrator, Guest, DefaultAccount, WDAGUtilityAccount, Martha
JZU7EW-5561	thomas, Martha
K2HYQQ-5561	thomas, Martha
K7CZKT-5562	thomas, Martha
KA8UHU-5562	thomas , Martha
KYBNNV-5562	The non-built-in user accounts on this computer is "thomas" and "Martha".
L7QRBN-5561	thomas, Martha
LACBFT-5562	thomas, Martha
LKDRCP-5561	thomas, Martha

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 5 - Examination Questions	
WebCode Test	**Response**
LMYFNP-5561	thomas and Martha
LN7VWF-5562	Martha,
LRRKGT-5562	thomas, Martha
LUECCW-5561	Martha and thomas
LYJAEX-5561	martha & thomas
M2VAHU-5562	Martha, thomas
MD7R7R-5562	thomas, Martha
MGM8JP-5561	thomas Martha
ML4AQV-5561	Martha and thomas
MQXA6Q-5562	Thomas, Martha
MR7JXN-5561	Martha ; thomas
MRTR8R-5561	thomas, Martha
MV6VTN-5562	Martha, thomas
NJQ8AP-5561	Martha, Administrator, Guest, DefaultAccount, WDAGUtilityAccount, thomas
NK3WJT-5561	Martha, Thomas
PAF6NN-5561	thomas, Administrator, Guest, DefaultAccount, WDAGUtilityAccount, Martha
PPBH8Q-5561	Martha, thomas
PQH2LD-5561	thomas, Martha
PZAD6L-5561	Thomas, Martha
Q2Z3GD-5562	thomas, Martha
QCLZQR-5562	thomas, Martha
QEMD4J-5561	"Martha" and "thomas" are the two active accounts.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

WebCode Test	Response
QH4FBN-5562	thomas, Martha
QT7QQQ-5561	Martha WDAGUtilityAccount DefaultAccount
QWAN2J-5561	thomas, Martha, WDAGUtilityAccount, DefaultAccount (the Administrator and Guest are created by default during the OS installation)
QYVDDJ-5561	thomas, Martha, DefaultAccount, WDAGUtilityAccount
R86XKL-5561	thomas, Martha
RBJUPN-5561	Martha, thomas
REKXEP-5561	thomas, Martha
RR9ZXG-5561	thomas, Martha
T8JQPN-5562	Martha, thomas
T8LHLB-5561	Martha, thomas
TGQH3P-5561	thomas, Martha
THHLMJ-5562	Thomas Martha
TRHDUP-5562	Martha, thomas
TVPPWK-5562	thomas, martha
TZXUNK-5561	thomas, Martha
U3GARK-5562	Thomas, Martha, Guest, Default, and WDAGUtilityAccount. Typically, the last three are built in users; however, forensic tools identified them as local users.
U4CRUL-5562	Thomas, Martha
UGJTDH-5561	thomas ; Martha
UT9WBG-5562	thomas, Martha
V63DZH-5562	thomas, Martha
VJJLKL-5562	thomas and Martha
VLV2EM-5561	Martha - Thomas

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

WebCode Test	Response
VYH7LJ-5561	Martha, thomas
W7CX8H-5562	thomas, Martha
W9FNCC-5561	thomas, Martha
WH87QK-5562	thomas and Martha
WKE9TJ-5562	thomas, Martha
WRVWDD-5561	thomas, Martha
WVD7FJ-5562	thomas, Martha
X9VFGE-5562	02 accounts (Martha and Thomas).
XDUKGE-5562	"thomas" and "Martha"
XFRBFD-5561	thomas – active user account Martha – created, viable, but no evidence of logins or user profile.
XGRD6G-5562	User Created: thomas, Martha; Default: Administrator, Guest, Default, DefaultAccount, WDAGUtilityAccount
XMC987-5562	Martha, Thomas, WDAGUtilityAccount, DefaultAccount, Guest and Administrator
XY6VCG-5562	Martha, Thomas
Y36EXF-5561	thomas, Martha
YVMR6B-5561	Martha, Thomas
YVR6WD-5561	thomas & Martha
Z8XMWF-5562	Martha & thomas
ZBE3BE-5561	Thomas, Martha
ZNK3ZC-5562	thomas, Martha
ZRL9H3-5562	thomas, Administrator, Guest, DefaultAccount, WDAGUtilityAccount, Martha
ZZUWEA-5562	Martha

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 5 - Examination Questions

Question 5: List the non-built-in user account(s) (name(s)) on this computer.
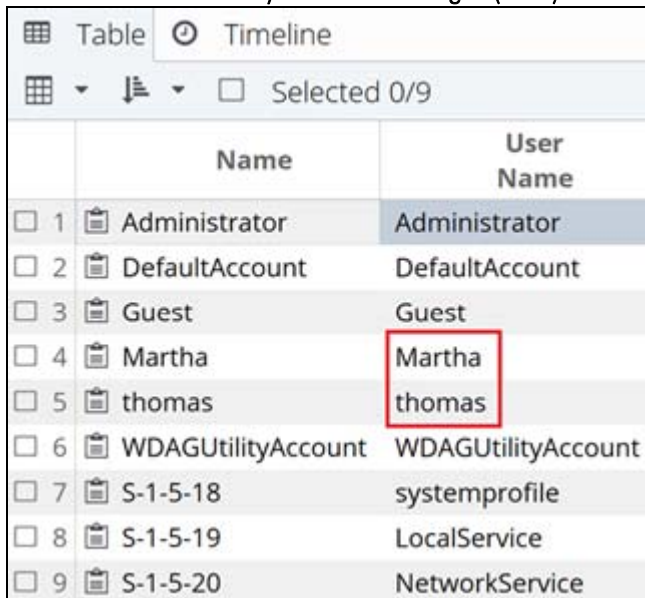
Consensus Result:

thomas
Martha

Manufacturer's Response Explanation:

User account information is stored in the Windows Security Account Manager (SAM) registry hive at C:\Windows\System32\Config\SAM:Domains\Account\Users\Names.
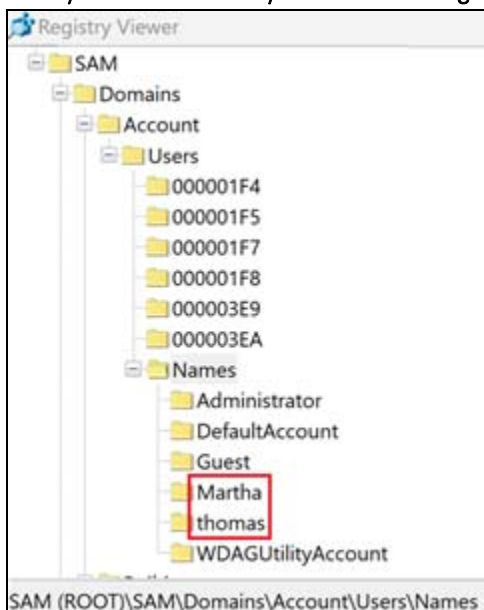
Manufacturer's Response Illustration:

EnCase view of Security Account Manager (SAM) hive

X-ways view of Security Account Manager (SAM) hive

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6 - Examination Questions

Question 6: What time zone was this computer configured to display? Provide answer as name (e.g. Atlantic Time).

<u>Manufacturer's Response:</u> US Mountain Standard Time

WebCode Test	Response
24VY4B-5561	US Mountain Standard Time, (UTC-07:00) Arizona
24WLMH-5561	US Mountain Standard Time
2RG9U9-5562	US Mountain Standard Time
2U4TZC-5561	US Mountain Standard Time (UTC -7:00) Arizona.
349ZFC-5562	Mountain Standard Time
3BYPCG-5561	US Mountain Time Zone
3GDA68-5561	(UTC-07:00) Arizona, Timezone name: US Mountain Standard Time
3J4DXE-5562	US Mountain Standard Time
3PA7TA-5561	Arizona
4FFFK9-5561	US Mountain Standard Time
4RN848-5561	(UTC-07:00) Arizona
4ZJ2KE-5562	US Mountain Standard Time
63LLN6-5561	Mountain Time
673VQB-5562	US Mountain Standard Time
6PJ238-5561	Arizona
7CQT46-5561	US Mountain Standard Time
7PVVH8-5561	US Mountain Standard Time
8FPDKA-5562	US Mountain Standard Time
8KE4Q6-5561	US Mountain Time
8TBZD8-5562	Not in scope.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6 - Examination Questions	
WebCode Test	**Response**
8WNN47-5562	US Mountain Standard Time
A444U7-5562	US Mountain Standard Time
AEKNE3-5561	Arizona (US Mountain Standard Time)
AFF7G6-5561	US Mountain Standard Time
AUY2L3-5562	US Mountain Standard Time
AXDN7Y-5561	US Mountain Standard Time
B7LHX8-5561	US Moutnain Standard Time
B8ELJ2-5561	US Mountain Standard Time
BEGRX4-5562	US Mountain Standard Time
BTXP36-5562	Mountain Standard Time
CDHZN3-5561	US Mountain Standard Time
CTEYRY-5562	Arizona Time
CWHMF2-5561	US Mountain Standard Time
DB9AYY-5561	Arizona Time
DJLBA2-5562	US Mountain Daylight Time
DPCKJZ-5561	US Mountain Standard Time
E6FEQZ-5562	US Mountain Standard Time
EYTN7P-5562	US Mountain Standard Time ((UTC-07:00) Arizona)
F4KDZ3-5562	Mountain Standard
FJ22JX-5562	US Mountain Standard Time
FMYKLW-5561	US Mountain Standard Time
GA6R7K-5561	US Mountain Standard Time

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6 - Examination Questions	
WebCode Test	**Response**
GA8D2Z-5562	US Mountain Standard Time
GJP4GX-5562	US Mountain Standard Time
GPH4VT-5561	US Mountain Standard Time
GQUT6W-5561	US Mountain Standard Time
GTHERT-5562	US Moutnain Standard Time
GTZ73X-5562	Mountain Time
HEX8ER-5562	Arizona Time
HF9WVJ-5561	US Mountain Standard Time
HFCE3U-5561	US Mountain Standard Time, Arizona
HXUD8T-5562	US Mountain Standard Time
HYZ6QT-5562	US Mountain Standard Time
J2L9YQ-5561	US Mountain Standard Time
J7HNUT-5561	US Mountain Time (Also Axiom says the Time Zone Display is Arizona)
JGEWDV-5562	US Mountain Standard Time ([UTC-07:00] Arizona)
JYYMCV-5561	Mountain Time
JZU7EW-5561	US Mountain Standard Time
K2HYQQ-5561	US Mountain Standard Time
K7CZKT-5562	(UTC-07:00) Arizona
KA8UHU-5562	US Mountain Standard Time
KYBNNV-5562	The time zone for this computer was set at Mountain Time (Arizona).
L7QRBN-5561	US Mountain Standard Time
LACBFT-5562	US Mountain Standard Time

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6 - Examination Questions	
WebCode Test	**Response**
LKDRCP-5561	Mountain Standard Time
LMYFNP-5561	US Mountain Standard Time
LN7VWF-5562	US Mountain Standard Time
LRRKGT-5562	Mountain Time
LUECCW-5561	Mountain Standard Time
LYJAEX-5561	US MOUNTAIN STANDARD TIME
M2VAHU-5562	US Mountain Standard Time
MD7R7R-5562	US Mountain Standard Time
MGM8JP-5561	US Mountain Standard Time
ML4AQV-5561	US Mountain Standard Time
MQXA6Q-5562	US Mountain Standard Time
MR7JXN-5561	US Mountain Standard Time
MRTR8R-5561	US Mountain Time
MV6VTN-5562	Mountain Standard Time
NJQ8AP-5561	US Mountain Standard Time
NK3WJT-5561	US Mountain Standard Time
PAF6NN-5561	US Mountain Standard Time
PPBH8Q-5561	US Mountain Standard Time
PQH2LD-5561	(UTC-07:00) Arizona
PZAD6L-5561	US Mountain Standard Time
Q2Z3GD-5562	US Mountain Standard Time
QCLZQR-5562	Mountain Time

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6 - Examination Questions	
WebCode Test	**Response**
QEMD4J-5561	US Mountain Time - specifically Arizona
QH4FBN-5562	Mountain Standard Time
QT7QQQ-5561	US Mountain Standard Time
QWAN2J-5561	US Mountain Standard Time
QYVDDJ-5561	US Mountain Standard Time UTC -7 Arizona
R86XKL-5561	Arizona
RBJUPN-5561	US Mountain Standard Time
REKXEP-5561	US Mountain Standard Time
RR9ZXG-5561	(UTC-07:00) Arizona
T8JQPN-5562	US Mountain Standard Time
T8LHLB-5561	Mountain Standard Time
TGQH3P-5561	US Mountain Standard Time
THHLMJ-5562	US Mountain Standard Time
TRHDUP-5562	Mountain Standard Time
TVPPWK-5562	US Mountain Time
TZXUNK-5561	US Mountain Standard Time
U3GARK-5562	US Mountain Standard Time
U4CRUL-5562	US Mountain Standard Time
UGJTDH-5561	US Mountain Standard Time
UT9WBG-5562	US Mountain Standard Time (UTC-7:00), Arizona
V63DZH-5562	US Mountain Standard Time(UTC-7)
VJJLKL-5562	US Mountain Standard Time with Daylight Savings

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6 - Examination Questions	
WebCode Test	**Response**
VLV2EM-5561	Arizona -US Mountain Standard Time
VYH7LJ-5561	US Mountain Standard Time
W7CX8H-5562	US Mountain Standard Time
W9FNCC-5561	US Mountain Standard Time (Arizona Time)
WH87QK-5562	Mountain Time
WKE9TJ-5562	US Mountain Standard Time
WRVWDD-5561	Mountain Time
WVD7FJ-5562	Mountain Standard Time
X9VFGE-5562	(UTC -07:00) Arizona
XDUKGE-5562	US Mountain Standard Time
XFRBFD-5561	US Mountain Standard Time
XGRD6G-5562	US Mountain Time
XMC987-5562	US Mountain Standard Time
XY6VCG-5562	US Mountain Standard Time, (UTC-07:00) Arizona
Y36EXF-5561	Mountain Time
YVMR6B-5561	US Mountain Standard Time
YVR6WD-5561	US Mountain Standard Time
Z8XMWF-5562	Mountain Time
ZBE3BE-5561	Mountain Time
ZNK3ZC-5562	US Mountain Standard Time
ZRL9H3-5562	US Mountain Standard Time
ZZUWEA-5562	US Mountain Standard Time

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6 - Examination Questions

Question 6: What time zone was this computer configured to display? Provide answer as name (e.g. Atlantic Time).

<u>Consensus Result:</u>

US Mountain Standard Time and/or (UTC -07:00) Arizona

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

Windows time zone setting information is found in the SYSTEM registry hive at C:\Windows\System32\Config\SYSTEM:ControlSet001\Control\TimeZoneInformation.

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

X-ways registry view showing time zone information

EnCase view showing time zone information

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7 - Examination Questions

Question 7: Provide the BSSID (network name) of the Wi-Fi hotspot MAC Address 16-E4-C2-A6-28-95.

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

WebCode Test	Response
24VY4B-5561	zion
24WLMH-5561	zion
2RG9U9-5562	zion
2U4TZC-5561	zion
349ZFC-5562	zion
3BYPCG-5561	The network name is "zion"
3GDA68-5561	zion
3J4DXE-5562	zion
3PA7TA-5561	zion
4FFFK9-5561	zion
4RN848-5561	zion
4ZJ2KE-5562	zion
63LLN6-5561	zion
673VQB-5562	Zion
6PJ238-5561	zion
7CQT46-5561	zion
7PVVH8-5561	zion
8FPDKA-5562	zion
8KE4Q6-5561	"zion"
8TBZD8-5562	Not in scope.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7 - Examination Questions	
WebCode Test	**Response**
8WNN47-5562	zion
A444U7-5562	Zion
AEKNE3-5561	zion
AFF7G6-5561	zion
AUY2L3-5562	16-E4-C2-A6-28-95
AXDN7Y-5561	zion
B7LHX8-5561	zion
B8ELJ2-5561	zion
BEGRX4-5562	Zion
BTXP36-5562	Zion
CDHZN3-5561	zion
CTEYRY-5562	zion
CWHMF2-5561	zion
DB9AYY-5561	zion
DJLBA2-5562	zion
DPCKJZ-5561	zion
E6FEQZ-5562	Zion
EYTN7P-5562	zion
F4KDZ3-5562	Zion
FJ22JX-5562	zion
FMYKLW-5561	zion
GA6R7K-5561	zion

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7 - Examination Questions	
WebCode Test	**Response**
GA8D2Z-5562	zion
GJP4GX-5562	zion
GPH4VT-5561	zion
GQUT6W-5561	zion
GTHERT-5562	zion
GTZ73X-5562	zion
HEX8ER-5562	zion
HF9WVJ-5561	zion
HFCE3U-5561	zion
HXUD8T-5562	zion
HYZ6QT-5562	zion
J2L9YQ-5561	We think the most likely answer is "zion", but "RCMP Surveillance Moose", "Acadia" and "Shenandoah" are also possible.
J7HNUT-5561	zion
JGEWDV-5562	zion
JYYMCV-5561	zion
JZU7EW-5561	zino
K2HYQQ-5561	zion
K7CZKT-5562	zion
KA8UHU-5562	zion
KYBNNV-5562	The BSSID of the Wi-Fi hotspot with the MAC address of 16-E4-C2-A6-28-95 is "zion".
L7QRBN-5561	zion
LACBFT-5562	zion

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7 - Examination Questions	
WebCode Test	**Response**
LKDRCP-5561	zion
LMYFNP-5561	zion
LN7VWF-5562	zion
LRRKGT-5562	Zion
LUECCW-5561	zion
LYJAEX-5561	zion
M2VAHU-5562	zion
MD7R7R-5562	zion
MGM8JP-5561	* Not in scope of agency exam
ML4AQV-5561	zion
MQXA6Q-5562	16:E4:C2:A6:28:95 (Zion)
MR7JXN-5561	zion
MRTR8R-5561	Zion
MV6VTN-5562	zion
NJQ8AP-5561	zion
NK3WJT-5561	zion
PAF6NN-5561	zion
PPBH8Q-5561	zion
PQH2LD-5561	zion
PZAD6L-5561	zion
Q2Z3GD-5562	zion
QCLZQR-5562	zion

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7 - Examination Questions	
WebCode Test	**Response**
QEMD4J-5561	zion
QH4FBN-5562	zion
QT7QQQ-5561	RCMP Surveillance Moose
QWAN2J-5561	zion
QYVDDJ-5561	zion
R86XKL-5561	zion
RBJUPN-5561	zion
REKXEP-5561	zion
RR9ZXG-5561	zion
T8JQPN-5562	zion
T8LHLB-5561	zion
TGQH3P-5561	zion
THHLMJ-5562	zion
TRHDUP-5562	Zion
TVPPWK-5562	zion
TZXUNK-5561	zion
U3GARK-5562	Zion
U4CRUL-5562	zion
UGJTDH-5561	zion
UT9WBG-5562	ZION
V63DZH-5562	zion
VJJLKL-5562	zion

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7 - Examination Questions	
WebCode Test	**Response**
VLV2EM-5561	WpadDecisionTime
VYH7LJ-5561	zion
W7CX8H-5562	zion
W9FNCC-5561	zion
WH87QK-5562	zion
WKE9TJ-5562	zion
WRVWDD-5561	zion
WVD7FJ-5562	zion
X9VFGE-5562	zion
XDUKGE-5562	zion
XFRBFD-5561	zion
XGRD6G-5562	zion
XMC987-5562	zion
XY6VCG-5562	zion
Y36EXF-5561	zion
YVMR6B-5561	Zion
YVR6WD-5561	zion
Z8XMWF-5562	Zion
ZBE3BE-5561	zion
ZNK3ZC-5562	zion
ZRL9H3-5562	[Participant did not return results for this question.]
ZZUWEA-5562	Realtek 8821CU Wireless LAN 802.11ac USB NIC

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7 - Examination Questions

Question 7: Provide the BSSID (network name) of the Wi-Fi hotspot MAC Address 16-E4-C2-A6-28-95.

Consensus Result:

zion

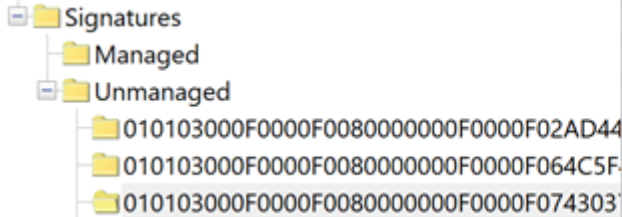Manufacturer's Response Explanation:

Windows network connection settings information is found in the SYSTEM registry hive at C:\Windows\System32\Config\ SOFTWARE:Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged.

Manufacturer's Response Illustration:

X-ways registry view showing network information

RegRipper registry view showing network information for the zion network

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 8 - Examination Questions

Question 8: Provide the filetype (file format) for the file containing the keyword "Otuscommersoni".

Manufacturer's   SQLite or SQLite 3 (Database)
Response:

WebCode Test	Response ** Inconsistencies not highlighted; No consensus achieved **
24VY4B-5561	SQLite Database
24WLMH-5561	SQLite Database, application/x-sqlite3
2RG9U9-5562	SQLite
2U4TZC-5561	sys/ SQLite database.
349ZFC-5562	SQL Database
3BYPCG-5561	SQLite database file
3GDA68-5561	SQLite format
3J4DXE-5562	SQLite3
3PA7TA-5561	SQLite
4FFFK9-5561	SQLite database
4RN848-5561	application/x-sqlite3
4ZJ2KE-5562	SQLite Database
63LLN6-5561	.sys
673VQB-5562	SQLite format
6PJ238-5561	Filetype: Database file "SQLite"
7CQT46-5561	.sys
7PVVH8-5561	.sys
8FPDKA-5562	SQLite format 3
8KE4Q6-5561	SQLite3 database file
8TBZD8-5562	SQLite format 3
8WNN47-5562	SQLite

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

	Question 8 - Examination Questions
WebCode Test	**Response** ** Inconsistencies not highlighted; No consensus achieved **
A444U7-5562	[Participant did not return results for this question.]
AEKNE3-5561	SQLite format 3
AFF7G6-5561	SQLite format 3
AUY2L3-5562	Sqlitedb
AXDN7Y-5561	.sys
B7LHX8-5561	.sys
B8ELJ2-5561	SQLite table
BEGRX4-5562	SQLite Format 3 OS System file (.sys)
BTXP36-5562	.HTML
CDHZN3-5561	SQLite
CTEYRY-5562	SQLite Database
CWHMF2-5561	SQLite 3
DB9AYY-5561	SQLite Database
DJLBA2-5562	SQLite Database
DPCKJZ-5561	SQLite database file
E6FEQZ-5562	SQLITE database
EYTN7P-5562	.sys (localskelscratch.sys)
F4KDZ3-5562	SQLite Format 3
FJ22JX-5562	sqlite format 3
FMYKLW-5561	.sys
GA6R7K-5561	.sys
GA8D2Z-5562	Sqlite

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

	Question 8 - Examination Questions	
WebCode Test	**Response**	** Inconsistencies not highlighted; No consensus achieved **
GJP4GX-5562	.sys	
GPH4VT-5561	SQLite	
GQUT6W-5561	sqlite3	
GTHERT-5562	.sys	
GTZ73X-5562	SqLite Database (.sys)	
HEX8ER-5562	SQLite	
HF9WVJ-5561	SQLite	
HFCE3U-5561	SQLite format 3	
HXUD8T-5562	SQLite format 3	
HYZ6QT-5562	SQLITE Database (.sys)	
J2L9YQ-5561	SQLITE Database	
J7HNUT-5561	SQLite format 3	
JGEWDV-5562	SQLite 3.x database	
JYYMCV-5561	File System (.sys); SQLite3 database	
JZU7EW-5561	sys	
K2HYQQ-5561	sqlitedb	
K7CZKT-5562	SQLITE Database (localskelscratch.sys)	
KA8UHU-5562	sqlite database	
KYBNNV-5562	The filetype that contains the keyword "Otuscommersoni" is system file for Windows machines. The file name localskelscratch.sys.	
L7QRBN-5561	SQLite Database	
LACBFT-5562	SQLite	
LKDRCP-5561	SQLite 3	

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

WebCode Test	Response
Question 8 - Examination Questions	
** Inconsistencies not highlighted; No consensus achieved **	
LMYFNP-5561	SQLite
LN7VWF-5562	.sys
LRRKGT-5562	HTML
LUECCW-5561	SQLite Database
LYJAEX-5561	The hit for "Otuscommersoni" comes from a file named localskelscratch.sys, so the file's format is a Windows kernel-mode driver: File type: SYS (Windows system driver
M2VAHU-5562	sys
MD7R7R-5562	SQLite Database
MGM8JP-5561	* Not in scope of agency exam
ML4AQV-5561	SQLITE Database
MQXA6Q-5562	system file
MR7JXN-5561	SQLite database file
MRTR8R-5561	SQLite format 3
MV6VTN-5562	SQLite
NJQ8AP-5561	localskelscratch.sys the file with the signature of .sys which is a sqlite database
NK3WJT-5561	SQLite format 3
PAF6NN-5561	The file is localskelscratch.sys, with an extension of .sys. However, the file signature of 0x53 51 4C 69 74 65 20 66 6F 72 6D 61 74 20 33 is indicative of a SQLite Database.
PPBH8Q-5561	SQLite
PQH2LD-5561	SQLite format 3
PZAD6L-5561	.sys
Q2Z3GD-5562	sqlite3
QCLZQR-5562	SQLite
QEMD4J-5561	SQLite database file, filename localskelscratch.sys

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 8 - Examination Questions	
WebCode Test	**Response** — ** Inconsistencies not highlighted; No consensus achieved **
QH4FBN-5562	sys
QT7QQQ-5561	.sys
QWAN2J-5561	.sys file but the header is SQLite format 3
QYVDDJ-5561	SQLite format 3
R86XKL-5561	SQLite
RBJUPN-5561	.sys file extension, the file header indicates it is SQLite format
REKXEP-5561	SQLite database file
RR9ZXG-5561	localskelscratch.sys
T8JQPN-5562	SQLite database
T8LHLB-5561	A SQLite 3 database file
TGQH3P-5561	SQL
THHLMJ-5562	SQLite db
TRHDUP-5562	SQLite file format
TVPPWK-5562	SQlite 3
TZXUNK-5561	localskelscratch.sys
U3GARK-5562	.sys
U4CRUL-5562	SQLite Database
UGJTDH-5561	SQLite format 3
UT9WBG-5562	.sys
V63DZH-5562	sqlite db file(filename: localskelscratch.sys)
VJJLKL-5562	SQLITE Database
VLV2EM-5561	sys

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

WebCode Test	Response ** ** Inconsistencies not highlighted; No consensus achieved **
VYH7LJ-5561	SQLite database
W7CX8H-5562	sqlite3 database file
W9FNCC-5561	SQLite format 3
WH87QK-5562	SQLite Database or SQLite or SQLite 3 (Database)
WKE9TJ-5562	SQLite Database
WRVWDD-5561	.sys file (SQLite format 3)
WVD7FJ-5562	System file (.sys)
X9VFGE-5562	.SQLite
XDUKGE-5562	SQLite format 3
XFRBFD-5561	SQLite 3.x database
XGRD6G-5562	SQLite (localskelscratch.sys)
XMC987-5562	.SYS file
XY6VCG-5562	.sys - system
Y36EXF-5561	application/x-sqlite3, File System
YVMR6B-5561	SQLite Database file
YVR6WD-5561	SQLite format 3
Z8XMWF-5562	A ".sys" file filename: localskelscratch.sys
ZBE3BE-5561	File is showing as a .SYS file however the file Header shows it as a SQlite Database.
ZNK3ZC-5562	SQLite
ZRL9H3-5562	[Participant did not return results for this question.]
ZZUWEA-5562	.sys

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 8 - Examination Questions

Question 8: Provide the filetype (file format) for the file containing the keyword "Otuscommersoni".

Consensus Result:

A consensus was not achieved. The intent of this question was for participants to provide the filetype (file format) for the file containing the keyword "Otuscommersoni". Approximately 73.8% of responding participants reported the Manufacturer's response, whereas 22.3% reported the file extension '.sys' and other variations of this response.

Manufacturer's Response Explanation:

The keyword in this question is found in \Users\thomas\AppData\Local\Microsoft\Edge\User Data\Default\Continuous Migration\Logs\localskelscratch.sys. This file has a .sys extension, however its internal file signature (header) identifies it as an SQLite database.

Manufacturer's Response Illustration:

X-Ways view of localskelscratch.sys
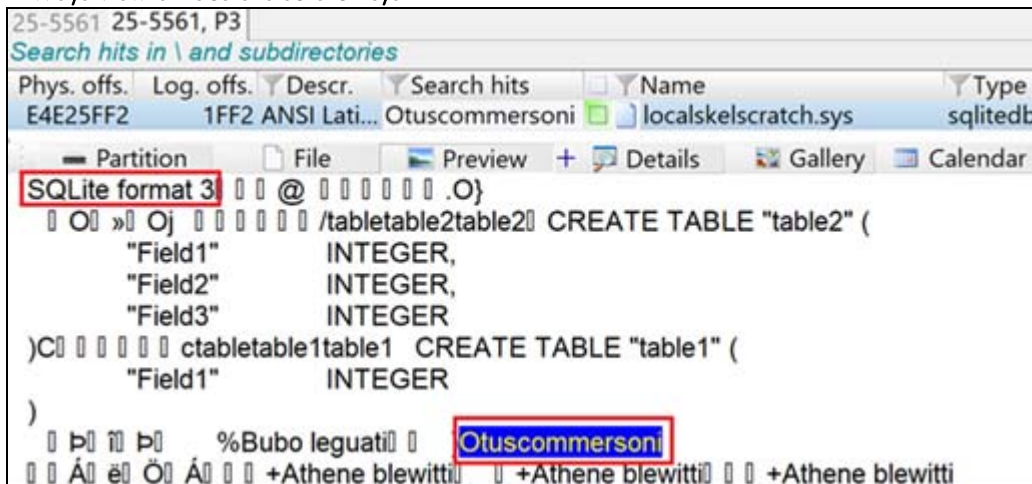
EnCase view of localskelscratch.sys

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 9 - Examination Questions

Question 9: For the file created 02/26/2025 (February 26, 2025) 20:44:21 (subject computer's local time), provide the source (host URL) of this file, according to its metadata.

Manufacturer's Response: https://ar.rdcpix.com , or
https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp

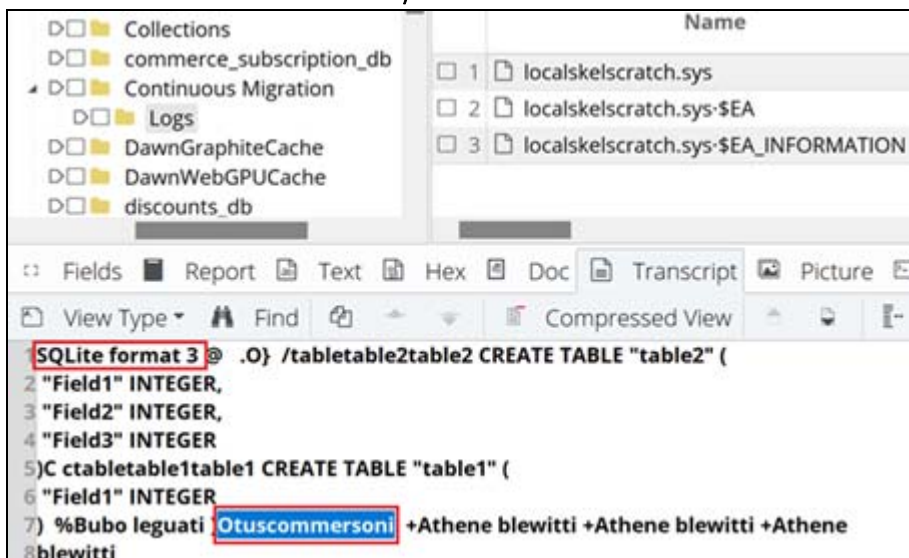| WebCode Test	Response
24VY4B-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
24WLMH-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
2RG9U9-5562	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f114334632rd-w2048_h1536.webp
2U4TZC-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e-f3263582073rd-w2048_h1536.webp
349ZFC-5562	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
3BYPCG-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
3GDA68-5561	HostUrl=https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
3J4DXE-5562	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
3PA7TA-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
4FFFK9-5561	https://ar.rdcpix.com (or https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp)
4RN848-5561	C:\Users\thomas\Downloads\b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
4ZJ2KE-5562	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
63LLN6-5561	https://ar.rdcpix.com/
673VQB-5562	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp / referrer URL: https://www.realtor.com/
6PJ238-5561	https://ar.rdcpix.com/
7CQT46-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f114334632rd-w2048_h1536.webp
7PVVH8-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
8FPDKA-5562	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
8KE4Q6-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.web
8TBZD8-5562	Not in scope.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 9 - Examination Questions	
WebCode Test	**Response**
8WNN47-5562	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f2390008254rd-w2048_h1536.webp
A444U7-5562	[Participant did not return results for this question.]
AEKNE3-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
AFF7G6-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
AUY2L3-5562	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
AXDN7Y-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
B7LHX8-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
B8ELJ2-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
BEGRX4-5562	//www.realtor.com/
BTXP36-5562	Realtor.com
CDHZN3-5561	https://www.realtor.com/
CTEYRY-5562	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f114334632rd-w2048_h1536.webp
CWHMF2-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
DB9AYY-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
DJLBA2-5562	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
DPCKJZ-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f114334632rd-w2048_h1536.webp
E6FEQZ-5562	HostUrl=https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
EYTN7P-5562	https://ar.rdcpix.com
F4KDZ3-5562	file:///C:/Users/thomas/Downloads/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
FJ22JX-5562	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
FMYKLW-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
GA6R7K-5561	[Participant did not return results for this question.]

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

WebCode Test	Response
Question 9 - Examination Questions	
GA8D2Z-5562	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
GJP4GX-5562	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f2390008254rd-w2048_h1536.webp
GPH4VT-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
GQUT6W-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
GTHERT-5562	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
GTZ73X-5562	www.realtor.com
HEX8ER-5562	https://ar.rdcpix.com
HF9WVJ-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
HFCE3U-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
HXUD8T-5562	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
HYZ6QT-5562	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
J2L9YQ-5561	25-5561-001.E01 - Partition 3 (Microsoft NTFS, 24.13 GB)\Users\thomas\Downloads\b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
J7HNUT-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
JGEWDV-5562	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
JYYMCV-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f2774552687rd-w2048_h1536.webp
JZU7EW-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
K2HYQQ-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
K7CZKT-5562	C:\Users\thomas\Downloads\b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
KA8UHU-5562	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
KYBNNV-5562	The host URL of this file appears to be https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp, and the item downloaded was b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
L7QRBN-5561	https://www.realtor.com
LACBFT-5562	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 9 - Examination Questions	
WebCode Test	**Response**
LKDRCP-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
LMYFNP-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
LN7VWF-5562	[Participant did not return results for this question.]
LRRKGT-5562	HostUrl=https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
LUECCW-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
LYJAEX-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f114334632rd-w2048_h1536.webp https://www.realtor.com/rentals/details/45-Boynton-Ave-SE-Unit-504_Atlanta_GA_30315_M96955-55878
M2VAHU-5562	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
MD7R7R-5562	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
MGM8JP-5561	* Not in scope of agency exam
ML4AQV-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
MQXA6Q-5562	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
MR7JXN-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
MRTR8R-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
MV6VTN-5562	https://ar.rdcpix.com
NJQ8AP-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
NK3WJT-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
PAF6NN-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
PPBH8Q-5561	https://ar.rdcpix.com/
PQH2LD-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
PZAD6L-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f114334632rd-w2048_h1536.webp
Q2Z3GD-5562	https://ar.rdcpix.com/ b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
QCLZQR-5562	Host URL: https://ar.rdcpix.com/ Full source URL: https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 9 - Examination Questions	
WebCode Test	**Response**
QEMD4J-5561	https://ar.rdcpix.com/ is the host URL, - Full URL is https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f521514396rd-w2048_h1536.webp
QH4FBN-5562	from realtor.com https://ar.rdcpix.com/b28004.....h1536.webp (there's no way in hell I'm writing this whole thing out, you know I found the right URL)
QT7QQQ-5561	file:///C:/Users/thomas/Downloads/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
QWAN2J-5561	https://ar.rdcpix.com
QYVDDJ-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
R86XKL-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
RBJUPN-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
REKXEP-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
RR9ZXG-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
T8JQPN-5562	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
T8LHLB-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f114334632rd-w2048_h1536.webp
TGQH3P-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
THHLMJ-5562	https://ar.rdcpix.com (https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f2774552687rd-w2048_h1536.webp)
TRHDUP-5562	thomas@file:///C:/Users/thomas/Downloads/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
TVPPWK-5562	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
TZXUNK-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f2774552687rd-w2048_h1536.webp
U3GARK-5562	https://www.realtor.com/
U4CRUL-5562	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
UGJTDH-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
UT9WBG-5562	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
V63DZH-5562	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
VJJLKL-5562	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 9 - Examination Questions	
WebCode Test	**Response**
VLV2EM-5561	https://www.realtor.com/
VYH7LJ-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
W7CX8H-5562	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
W9FNCC-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
WH87QK-5562	https://ar.rdcpix.com/ or https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
WKE9TJ-5562	https://ar.rdcpix.com
WRVWDD-5561	file:///C:/Users/thomas/Downloads/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
WVD7FJ-5562	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
X9VFGE-5562	https://ar.rdcpix.com
XDUKGE-5562	https://ar.rdcpix.com/
XFRBFD-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
XGRD6G-5562	ReferrerUrl: https://www.realtor.com/; HostUrl: https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
XMC987-5562	http://www.eme.l
XY6VCG-5562	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
Y36EXF-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
YVMR6B-5561	www.realtor.com
YVR6WD-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
Z8XMWF-5562	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
ZBE3BE-5561	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
ZNK3ZC-5562	https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
ZRL9H3-5562	[Participant did not return results for this question.]
ZZUWEA-5562	https://ar.rdcpix.com

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 9 - Examination Questions

Question 9: For the file created 02/26/2025 (February 26, 2025) 20:44:21 (subject computer's local time), provide the source (host URL) of this file, according to its metadata.

Consensus Result:

https://ar.rdcpix.com , or
https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp

Manufacturer's Response Explanation:

C:\Users\thomas\AppData\Roaming\Microsoft\Windows\Recent\b28004b34e92e8ff1d7971947f230e72c-f32635 82073rd-w2048_h1536.webp was created (downloaded) at the specified time. Files downloaded from the internet are tagged with information regarding their source, which is stored in an alternate data stream of the file, in this case, ~… h1536.webp:Zone.Identifier

Manufacturer's Response Illustration:

EnCase b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp:Zone.Identifier detail
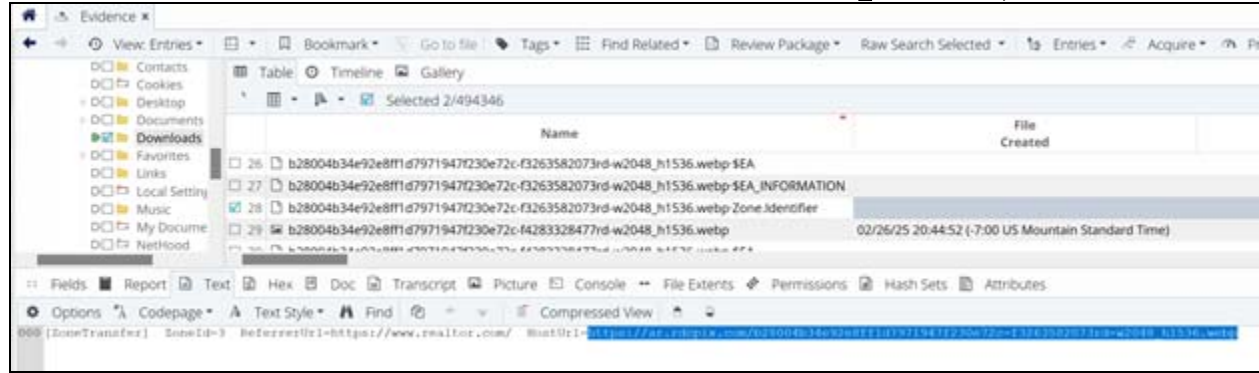
X-Ways view of

Full path	\Users\thomas\Downloads\b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp
Parent name	Downloads
Child objects	EA
Size	59.4 KB (60,868)
Created	02/26/2025 20:44:21 -7
Modified	02/26/2025 20:44:22 -7
Modified²	02/26/2025 20:44:22 -7
Record changed	03/04/2025 17:17:43 -7
Record changed²	02/26/2025 20:44:22 -7
Accessed	03/02/2025 07:52:14 -7
MD5	33033987B14CDB0D8EB1A9552DD80873
SHA-256	BEBACB218727F9B390D5BFDBA9EA0CB2C8CCE88900CF9FB105EBD1DB85E5F13C
Labels	ZoneId=3
Metadata	ZoneId=3 ReferrerUrl=https://www.realtor.com/ HostUrl=https://ar.rdcpix.com/b28004b34e92e8ff1d7971947f230e72c-f3263582073rd-w2048_h1536.webp

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 10 - Examination Questions

Question 10: According to Windows Prefetch, what application was executed at 03/03/2025 (March 3, 2025) 16:28:57 (subject computer's local time)?

<u>Manufacturer's</u>   REALTOR.EXE
<u>Response:</u>

WebCode Test	Response
24VY4B-5561	REALTOR.EXE
24WLMH-5561	REALTOR.EXE
2RG9U9-5562	REALTOR.EXE
2U4TZC-5561	realtor.exe
349ZFC-5562	Realtor.exe
3BYPCG-5561	REALTOR.EXE
3GDA68-5561	REALTOR.EXE
3J4DXE-5562	REALTOR.EXE
3PA7TA-5561	REALTOR.EXE
4FFFK9-5561	REALTOR.EXE
4RN848-5561	realtor.exe
4ZJ2KE-5562	REALTOR.EXE
63LLN6-5561	REALTOR.EXE
673VQB-5562	REALTOR.EXE
6PJ238-5561	REALTOR.EXE
7CQT46-5561	REALTOR.EXE
7PVVH8-5561	REALTOR.EXE
8FPDKA-5562	realtor.exe
8KE4Q6-5561	realtor.exe
8TBZD8-5562	Not in scope.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 10 - Examination Questions	
WebCode Test	**Response**
8WNN47-5562	REALTOR.EXE
A444U7-5562	Realtor.exe
AEKNE3-5561	REALTOR.EXE
AFF7G6-5561	REALTOR.EXE
AUY2L3-5562	REALTOR.EXE
AXDN7Y-5561	REALTOR.EXE
B7LHX8-5561	realtor.exe
B8ELJ2-5561	realtor.exe
BEGRX4-5562	REALTOR.EXE
BTXP36-5562	Realtor.exe
CDHZN3-5561	REALTOR.EXE
CTEYRY-5562	REALTOR.EXE
CWHMF2-5561	REALTOR.EXE
DB9AYY-5561	REALTOR.EXE
DJLBA2-5562	REALTOR.EXE
DPCKJZ-5561	REALTOR.EXE
E6FEQZ-5562	REALTOR.EXE
EYTN7P-5562	Realtor.exe
F4KDZ3-5562	calculatorapp.exe
FJ22JX-5562	REALTOR.EXE
FMYKLW-5561	realtor.exe
GA6R7K-5561	Realtor.exe Runtimebroker.exe

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 10 - Examination Questions	
WebCode Test	**Response**
GA8D2Z-5562	REALTOR.EXE
GJP4GX-5562	REALTOR.EXE
GPH4VT-5561	REALTOR.EXE
GQUT6W-5561	REALTOR.EXE
GTHERT-5562	realtor.exe
GTZ73X-5562	Realtor.exe
HEX8ER-5562	REALTOR.EXE
HF9WVJ-5561	realtor.exe
HFCE3U-5561	REALTOR.EXE
HXUD8T-5562	realtor.exe
HYZ6QT-5562	REALTOR.EXE (File Description: Windows Calculator)
J2L9YQ-5561	REALTOR.EXE
J7HNUT-5561	REALTOR.EXE
JGEWDV-5562	REALTOR.EXE
JYYMCV-5561	REALTOR.EXE
JZU7EW-5561	REALTOR.exe
K2HYQQ-5561	REALTOR.EXE
K7CZKT-5562	Calculator app
KA8UHU-5562	REALTOR.EXE
KYBNNV-5562	According the Windows Prefetch, the application Realtor.exe was executed at 3/3/2025 at 16:28:57.
L7QRBN-5561	realtor.exe
LACBFT-5562	REALTOR.EXE

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 10 - Examination Questions	
WebCode Test	**Response**
LKDRCP-5561	REALTOR.EXE
LMYFNP-5561	Realtor.exe
LN7VWF-5562	Realtor.exe Runtimebroker.exe
LRRKGT-5562	Realtor.exe
LUECCW-5561	Realtor.exe
LYJAEX-5561	app
M2VAHU-5562	REALTOR.EXE
MD7R7R-5562	Realtor.exe
MGM8JP-5561	* Not in scope of agency exam
ML4AQV-5561	Realtor.exe
MQXA6Q-5562	svchost.exe
MR7JXN-5561	REALTOR.exe
MRTR8R-5561	Realtor.exe
MV6VTN-5562	REALTOR.exe
NJQ8AP-5561	REALTOR.EXE
NK3WJT-5561	Realtor.exe
PAF6NN-5561	REALTOR.EXE
PPBH8Q-5561	REALTOR.EXE
PQH2LD-5561	REALTOR.EXE
PZAD6L-5561	REALTOR.EXE
Q2Z3GD-5562	REALTOR.EXE
QCLZQR-5562	REALTOR.EXE

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 10 - Examination Questions	
WebCode Test	**Response**
QEMD4J-5561	REALTOR.EXE
QH4FBN-5562	realtor.exe
QT7QQQ-5561	REALTOR.EXE-6BF69CC5.pf
QWAN2J-5561	REALTOR.EXE
QYVDDJ-5561	REALTOR.EXE
R86XKL-5561	Realtor.exe
RBJUPN-5561	realtor.exe
REKXEP-5561	REALTOR.EXE
RR9ZXG-5561	REALTOR.exe
T8JQPN-5562	REALTOR.EXE, CALCULATORAPP.EXE, RUNTIMEBROKER.EXE
T8LHLB-5561	Realtor.exe
TGQH3P-5561	REALTOR.EXE
THHLMJ-5562	REALTOR.exe
TRHDUP-5562	REALTOR.EXE
TVPPWK-5562	REALTOR.EXE
TZXUNK-5561	REALTOR.EXE
U3GARK-5562	REALTOR.EXE
U4CRUL-5562	REALTOR.EXE
UGJTDH-5561	REALTOR.EXE
UT9WBG-5562	REALTOR.EXE
V63DZH-5562	REALTOR.exe
VJJLKL-5562	REALTOR.EXE

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 10 - Examination Questions	
WebCode Test	**Response**
VLV2EM-5561	REALTOR.EXE
VYH7LJ-5561	Realtor.exe
W7CX8H-5562	REALTOR.EXE
W9FNCC-5561	REALTOR.EXE
WH87QK-5562	REALTOR.EXE
WKE9TJ-5562	realtor.exe
WRVWDD-5561	REALTOR.EXE
WVD7FJ-5562	Realtor.exe
X9VFGE-5562	REALTOR.EXE-6BF69CC5.pf
XDUKGE-5562	realtor.exe
XFRBFD-5561	realtor.exe
XGRD6G-5562	REALTOR.EXE
XMC987-5562	RUNTIMEBROKER.EXE
XY6VCG-5562	REALTOR.EXE
Y36EXF-5561	REALTOR.EXE
YVMR6B-5561	REALTOR.EXE
YVR6WD-5561	REALTOR.EXE
Z8XMWF-5562	Realtor.exe
ZBE3BE-5561	REALTOR.EXE
ZNK3ZC-5562	REALTOR.EXE
ZRL9H3-5562	[Participant did not return results for this question.]
ZZUWEA-5562	REALTOR.EXE

Computer Hard Drive - Windows Analysis Results
TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 10 - Examination Questions

Question 10: According to Windows Prefetch, what application was executed at 03/03/2025 (March 3, 2025) 16:28:57 (subject computer's local time)?

Consensus Result:

REALTOR.EXE

Manufacturer's Response Explanation:

There is one prefetch file, REALTOR.EXE-6BF69CC5.pf, in C:\Windows\Prefetch, with this created time. Analysis of this file with a reliable tool confirms this execution time.

Manufacturer's Response Illustration:

X-Ways view of C:\Windows\Prefetch\REALTOR.EXE-6BF69CC5.pf

PECmd.exe parse of REALTOR.EXE-6BF69CC5.pf (UTC)

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 11 - Examination Questions

Question 11: From what path (include the drive letter) was the application identified in question 10 executed?

Manufacturer's Response:　　　G:\apps\realtor.exe, or
　　　　　　　　　　　　　　　G:\apps\

WebCode Test	Response
24VY4B-5561	G:\apps\realtor.exe
24WLMH-5561	G:\apps\realtor.exe
2RG9U9-5562	G:\apps\realtor.exe
2U4TZC-5561	G:\apps\realtor.exe
349ZFC-5562	G:\apps\realtor.exe
3BYPCG-5561	G:\APPS\
3GDA68-5561	G:\apps\realtor.exe
3J4DXE-5562	C:\Windows\Prefetch\REALTOR.EXE-6BF69CC5.pf
3PA7TA-5561	G:\APPS\REALTOR.EXE
4FFFK9-5561	G:\apps\
4RN848-5561	G:\apps\realtor.exe
4ZJ2KE-5562	G:\APPS\REALTOR.EXE
63LLN6-5561	G:\apps
673VQB-5562	G:\apps\realtor.exe
6PJ238-5561	G:\apps\realtor.exe
7CQT46-5561	G:\APPS\Realtor.exe
7PVVH8-5561	G:\apps\
8FPDKA-5562	G:\apps
8KE4Q6-5561	G:\apps\realtor.exe
8TBZD8-5562	Not in scope.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 11 - Examination Questions	
WebCode Test	**Response**
8WNN47-5562	G:\apps\realtor.exe
A444U7-5562	G:\apps\realtor.exe
AEKNE3-5561	G:\apps\realtor.exe
AFF7G6-5561	G:\apps\realtor.exe
AUY2L3-5562	G:\APPS\REALTOR.EXE
AXDN7Y-5561	G:\apps\realtor.exe
B7LHX8-5561	G:\apps\realtor.exe
B8ELJ2-5561	G:\apps\realtor.exe
BEGRX4-5562	G:\APPS\REALTOR.EXE
BTXP36-5562	G:\apps\realtor.exe
CDHZN3-5561	G:\apps\realtor.exe
CTEYRY-5562	G:\APPS\REALTOR.EXE
CWHMF2-5561	C:\APPS\REALTOR.EXE
DB9AYY-5561	G:\apps\realtor.exe
DJLBA2-5562	G:\apps\realtor.exe
DPCKJZ-5561	G:\apps\realtor.exe
E6FEQZ-5562	G:\apps\realtor.exe
EYTN7P-5562	G:\APPS\REALTOR.EXE
F4KDZ3-5562	\VOLUME{01da76a407bb52d6-f207cad7}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.WINDOWSCALCULATOR_11.2411.1.0_X64__8WEKYB3D8BBWE\CALCULATORAPP.EXE
FJ22JX-5562	G:\apps\realtor.exe
FMYKLW-5561	G:\apps\
GA6R7K-5561	25-5561-001.E01\Basic data partition (EFI 3)\Root\Windows\Prefetch\

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 11 - Examination Questions	
WebCode Test	**Response**
GA8D2Z-5562	G:\apps\realtor.exe
GJP4GX-5562	G:\apps\realtor.exe
GPH4VT-5561	G:\apps\realtor.exe
GQUT6W-5561	G:\apps\realtor.exe
GTHERT-5562	G:\apps\realtor.exe
GTZ73X-5562	G:\apps\realtor.exe
HEX8ER-5562	G:\apps\realtor.exe
HF9WVJ-5561	G:\apps\realtor.exe
HFCE3U-5561	G:\apps\realtor.exe
HXUD8T-5562	G:\apps\realtor.exe
HYZ6QT-5562	G:\apps\realtor.exe
J2L9YQ-5561	G:\apps\realtor.exe
J7HNUT-5561	G:\apps\realtor.exe
JGEWDV-5562	G:\apps
JYYMCV-5561	G:\apps\realtor.exe
JZU7EW-5561	G:\apps
K2HYQQ-5561	G:\apps\realtor.exe
K7CZKT-5562	C:\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.WINDOWSCALCULATOR_11.2411.1.0_X64__8WEKYB3D8BBWE\CALCULATORAPP.EXE
KA8UHU-5562	G:\APPS\
KYBNNV-5562	The path the application was executed from was E:\apps\Realtor.exe. The thumb drive was mounted as the E: drive.
L7QRBN-5561	G:\apps\realtor.exe
LACBFT-5562	G:\apps\realtor.exe

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 11 - Examination Questions	
WebCode Test	**Response**
LKDRCP-5561	G:\apps\realtor.exe
LMYFNP-5561	G:\apps\realtor.exe
LN7VWF-5562	25-5561-001.E01\Basic data partition (EFI 3)\Root\Windows\Prefetch\
LRRKGT-5562	G:\apps\realtor.exe
LUECCW-5561	G:\apps\realtor.exe
LYJAEX-5561	G
M2VAHU-5562	G:\apps\realtor.exe
MD7R7R-5562	G:\apps\realtor.exe
MGM8JP-5561	G:\apps\realtor.exe
ML4AQV-5561	G:\apps\realtor.exe
MQXA6Q-5562	C:\WINDOWS\SYSTEM32\
MR7JXN-5561	G:\apps\realtor.exe
MRTR8R-5561	G:\APPS\REALTOR.EXE
MV6VTN-5562	G:\apps\realtor.exe
NJQ8AP-5561	G:\apps\realtor.exe
NK3WJT-5561	G:\APPS\REALTOR.EXE
PAF6NN-5561	G:\apps\realtor.exe
PPBH8Q-5561	G:\apps\realtor.exe
PQH2LD-5561	G:\apps\realtor.exe
PZAD6L-5561	G:\apps\realtor.exe
Q2Z3GD-5562	G:\apps\realtor.exe
QCLZQR-5562	G:\apps\realtor.exe

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

WebCode Test	Response
QEMD4J-5561	G:\APPS\REALTOR.EXE
QH4FBN-5562	G:\apps\realtor.exe
QT7QQQ-5561	Windows\Prefetch\REALTOR.EXE-6BF69CC5.pf
QWAN2J-5561	G:\apps\realtor.exe
QYVDDJ-5561	G:\APPS\REALTOR.EXE
R86XKL-5561	G:\apps\
RBJUPN-5561	G:\apps\realtor.exe
REKXEP-5561	G:\apps\realtor.exe
RR9ZXG-5561	G:\apps\realtor.exe
T8JQPN-5562	REALTOR.EXE = <USB>\APPS\ ; CALCULATORAPP.EXE = C:\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.WINDOWSCALCULATOR_11.2411.1.0_X64__8WEKYB3D8BBWE\ ; RUNTIMEBROKER.EXE = C:\WINDOWS\SYSTEM32\
T8LHLB-5561	G:\apps\realtor.exe
TGQH3P-5561	G:\apps\realtor.exe
THHLMJ-5562	G:\apps\realtor.exe
TRHDUP-5562	E: \VOLUME{0000000000000000- a2ae62d7}\APPS\REALTOR.EXE (USB Path partition 3)
TVPPWK-5562	G:\apps\realtor.exe
TZXUNK-5561	G:\apps\realtor.exe
U3GARK-5562	G:\apps\realtor.exe
U4CRUL-5562	G:\APPS\REALTOR.EXE which was found within User Assist and having the Last Run date and time in question 10.
UGJTDH-5561	G:\APPS\REALTOR.EXE
UT9WBG-5562	C:\APPS\REALTOR.EXE
V63DZH-5562	G:\APPS\REALTOR.EXE
VJJLKL-5562	G:\apps\realtor.exe

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

WebCode Test	Response
VLV2EM-5561	G:\apps\realtor.exe
VYH7LJ-5561	G:\Apps\Realtor.exe
W7CX8H-5562	G:\apps
W9FNCC-5561	G:\apps\realtor.exe
WH87QK-5562	G:\apps\realtor.exe
WKE9TJ-5562	G:\apps
WRVWDD-5561	G:\apps\realtor.exe
WVD7FJ-5562	G:\apps\realtor.exe
X9VFGE-5562	E\Windows\Prefetch\thomas
XDUKGE-5562	G:\apps
XFRBFD-5561	G:\apps\realtor.exe
XGRD6G-5562	G:\apps\realtor.exe
XMC987-5562	VOLUME{01da76a407bb52d6-f207cad7}\WINDOWS\SYSTEM32\RUNTIMEBROKER.EXE
XY6VCG-5562	G:\apps
Y36EXF-5561	G:\apps\realtor.exe
YVMR6B-5561	G:\apps\realtor.exe
YVR6WD-5561	G:\apps\realtor.exe
Z8XMWF-5562	E:\APPS\REALTOR.EXE
ZBE3BE-5561	G:\apps\realtor.exe
ZNK3ZC-5562	G:\APPS\REALTOR.EXE
ZRL9H3-5562	[Participant did not return results for this question.]
ZZUWEA-5562	E:/apps

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 11 - Examination Questions

Question 11: From what path (include the drive letter) was the application identified in question 10 executed?

Consensus Result:

G:\apps\realtor.exe, or
G:\apps\

Manufacturer's Response Explanation:

Many sources exist for this information. Execution path information is available in Prefetch data but does not include the resolved drive letter for the volume. Program execution information is also available in users' registry hives, NTUSER.DAT.

Manufacturer's Response Illustration:

RegRipper parse of User Assist Key from Thomas\NTUSER.DAT
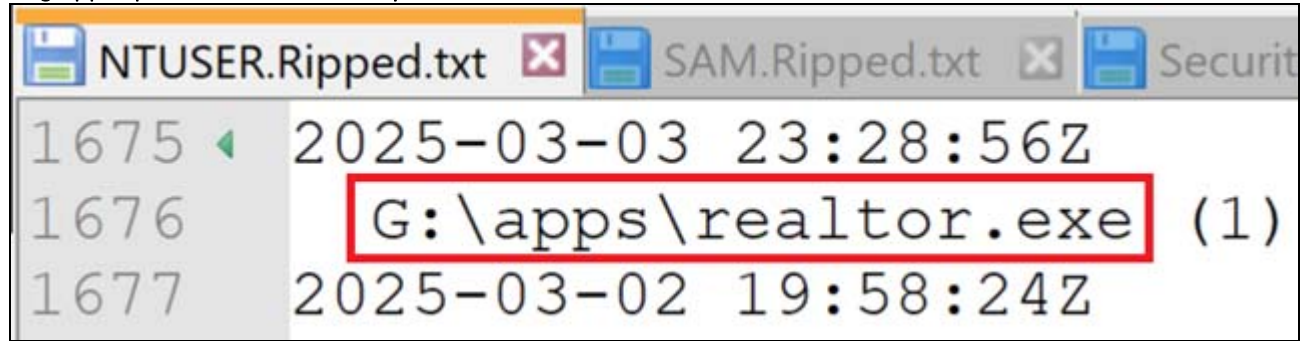
Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12 - Examination Questions

Question 12: A Windows registry key value contains the following enciphered text: P:\Hfref\gubznf\Qbjaybnqf\ariretbaantvirlbhhc.rkr. What is the deciphered value (text)?

<u>Manufacturer's Response:</u>   C:\Users\thomas\Downloads\nevergonnagiveyouup.exe

WebCode Test	Response
24VY4B-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
24WLMH-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
2RG9U9-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
2U4TZC-5561	P:\Users\thomas\Downloads\nevergonnagiveyouup.exe
349ZFC-5562	Rot13
3BYPCG-5561	nevergonnagiveyouup.exe
3GDA68-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
3J4DXE-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
3PA7TA-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
4FFFK9-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
4RN848-5561	Users\thomas\Downloads\nevergonnagiveyouup.exe
4ZJ2KE-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
63LLN6-5561	Users\thomas\Downloads\nevergonnagiveyouup
673VQB-5562	C:\Users\Thomas\Downloads\nevergonnagiveyouup.exe
6PJ238-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
7CQT46-5561	C:\Users\Thomas\Downloads\nevertongativeyouup.exe
7PVVH8-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
8FPDKA-5562	C:\Users\thomas\Downloads\nevergonnnagiveyouup.exe
8KE4Q6-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
8TBZD8-5562	Not in scope.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12 - Examination Questions	
WebCode Test	**Response**
8WNN47-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
A444U7-5562	[Participant did not return results for this question.]
AEKNE3-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
AFF7G6-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
AUY2L3-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
AXDN7Y-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
B7LHX8-5561	C:\users\thomas\Downloads\nevergonnagiveyouup.exe
B8ELJ2-5561	P:\Users\thomas\Downloads\nevergonnagiveyouup.exe
BEGRX4-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
BTXP36-5562	c:\users\Thomas\downloads\nevergonnagiveyouup.exe
CDHZN3-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
CTEYRY-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
CWHMF2-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
DB9AYY-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe.
DJLBA2-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
DPCKJZ-5561	Users\thomas\Downloads\nevergonnagiveyouup.exe
E6FEQZ-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
EYTN7P-5562	C:\Users\thomas\Downloads\nevergotactivateyouup.exe
F4KDZ3-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe.
FJ22JX-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
FMYKLW-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
GA6R7K-5561	[Participant did not return results for this question.]

(88)

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

WebCode Test	Response
GA8D2Z-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
GJP4GX-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
GPH4VT-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
GQUT6W-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
GTHERT-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
GTZ73X-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
HEX8ER-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
HF9WVJ-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
HFCE3U-5561	C:\users\thomas\downloads\nevergonnagiveyouup.exe
HXUD8T-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
HYZ6QT-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
J2L9YQ-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
J7HNUT-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
JGEWDV-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
JYYMCV-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
JZU7EW-5561	C:\Users\thomas\Downloads\nevergoneagainyouup.exe
K2HYQQ-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
K7CZKT-5562	P:\Users\thomas\Downloads\nevergonnagiveyouup.exe
KA8UHU-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
KYBNNV-5562	The deciphered value of the given text is C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
L7QRBN-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
LACBFT-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12 - Examination Questions	
WebCode Test	**Response**
LKDRCP-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
LMYFNP-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
LN7VWF-5562	[Participant did not return results for this question.]
LRRKGT-5562	P:\Users\thomas\Downloads\nevergoingtogiveyouup.exe
LUECCW-5561	Users\thomas\Downloads\nevergonnagiveyouup.exe
LYJAEX-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
M2VAHU-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
MD7R7R-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
MGM8JP-5561	* Not in scope of agency exam
ML4AQV-5561	Users\thomas\Downloads\nevergonnagiveyouup.exe
MQXA6Q-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
MR7JXN-5561	c:\users\thomas\downloads\nevergonnagiveyouup.exe
MRTR8R-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
MV6VTN-5562	P:\Users\thomas\Downloads\nevergonnagiveyouup
NJQ8AP-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
NK3WJT-5561	C:\users\thomas\downloads\nevergonnagiveyouup.exe
PAF6NN-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
PPBH8Q-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
PQH2LD-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
PZAD6L-5561	C:\Users\thomas\Downloads\nevergoingnagiveyouup.exe
Q2Z3GD-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
QCLZQR-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12 - Examination Questions	
WebCode Test	**Response**
QEMD4J-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
QH4FBN-5562	C:\Users\thomas\downloads\nevergonnagiveyouup.exe
QT7QQQ-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
QWAN2J-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
QYVDDJ-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
R86XKL-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
RBJUPN-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
REKXEP-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
RR9ZXG-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
T8JQPN-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
T8LHLB-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
TGQH3P-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
THHLMJ-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.rkr
TRHDUP-5562	\Users\thomas\Downloads\nevergonnagiveyouup.exe
TVPPWK-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
TZXUNK-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe.
U3GARK-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
U4CRUL-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
UGJTDH-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
UT9WBG-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
V63DZH-5562	C:\Users\thomas\Downloads\nevergonnegiveyouup.exe
VJJLKL-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12 - Examination Questions	
WebCode Test	**Response**
VLV2EM-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
VYH7LJ-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
W7CX8H-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
W9FNCC-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
WH87QK-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
WKE9TJ-5562	nevergonnagiveyouup.exe
WRVWDD-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
WVD7FJ-5562	\Users\thomas\Downloads\nevergonnagiveyouup.exe
X9VFGE-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
XDUKGE-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
XFRBFD-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
XGRD6G-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
XMC987-5562	Nevergonnagiveyouup
XY6VCG-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe.
Y36EXF-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
YVMR6B-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
YVR6WD-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
Z8XMWF-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
ZBE3BE-5561	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
ZNK3ZC-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
ZRL9H3-5562	[Participant did not return results for this question.]
ZZUWEA-5562	C:\Users\Downloads\nevergonnagiveyouup.exe

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12 - Examination Questions

Question 12: A Windows registry key value contains the following enciphered text: P:\Hfref\gubznf\Qbjaybnqf\ariretbaantvirlbhhc.rkr. What is the deciphered value (text)?
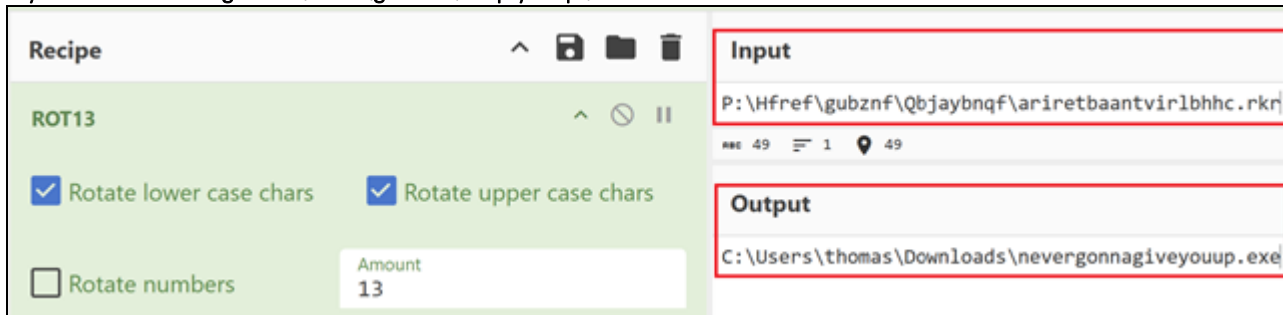
<u>Consensus Result:</u>

C:\Users\thomas\Downloads\nevergonnagiveyouup.exe

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

Information in the Windows registries is often stored as ROT13 enciphered values.

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

Cyberchef decoding of P:\Hfref\gubznf\Qbjaybnqf\ariretbaantvirlbhhc.rkr

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13 - Examination Questions

Question 13: Provide the filetype (file format) for C: \Users\thomas\text.txt.

Manufacturer's Response: Microsoft Portable Executable; or
Windows Executable; or
DOS Executable, or
Application

WebCode Test	Response
24VY4B-5561	DOS Executable
24WLMH-5561	DOS Executable, application
2RG9U9-5562	MS DOS executable
2U4TZC-5561	Exe
349ZFC-5562	.exe (executable)
3BYPCG-5561	Windows Portable Executable (.exe)
3GDA68-5561	Windows Executable, header shows as MZ
3J4DXE-5562	binary, executable
3PA7TA-5561	DOS Executable
4FFFK9-5561	Executable (EXE) program
4RN848-5561	exe file
4ZJ2KE-5562	Windows Executable
63LLN6-5561	Executable
673VQB-5562	Mz - DOS executable
6PJ238-5561	DOS MZ executable format
7CQT46-5561	.exe
7PVVH8-5561	.exe (DOS MZ executable)
8FPDKA-5562	executable (exe)
8KE4Q6-5561	This file is an executable file renamed with the "txt" file extension.
8TBZD8-5562	EXE

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13 - Examination Questions	
WebCode Test	**Response**
8WNN47-5562	EXE
A444U7-5562	Ejecutable (.exe)
AEKNE3-5561	MS-DOS executable
AFF7G6-5561	EXE/DLL
AUY2L3-5562	exe
AXDN7Y-5561	Executable File
B7LHX8-5561	PE32+
B8ELJ2-5561	EXE
BEGRX4-5562	EXE
BTXP36-5562	.exe
CDHZN3-5561	ZAP
CTEYRY-5562	executable file
CWHMF2-5561	Windows Executable
DB9AYY-5561	Executable
DJLBA2-5562	Executable (.exe)
DPCKJZ-5561	Windows Executable File (.exe)
E6FEQZ-5562	Executable
EYTN7P-5562	.exe (executable)
F4KDZ3-5562	Windows PE
FJ22JX-5562	EXE/DLL
FMYKLW-5561	.exe
GA6R7K-5561	Application - EXE/DLL

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13 - Examination Questions	
WebCode Test	**Response**
GA8D2Z-5562	executable
GJP4GX-5562	.zap ZoneAlam data file
GPH4VT-5561	DOS Executable
GQUT6W-5561	exe
GTHERT-5562	PE32+
GTZ73X-5562	.exe
HEX8ER-5562	DOS Executable
HF9WVJ-5561	DOS Executable
HFCE3U-5561	A DOS executable file
HXUD8T-5562	PE(Portable Executable) File
HYZ6QT-5562	Executable File (.exe)
J2L9YQ-5561	EXE
J7HNUT-5561	MZ (executable file format)
JGEWDV-5562	Windows Portable Executable
JYYMCV-5561	.exe (Win64 EXE)
JZU7EW-5561	exe
K2HYQQ-5561	exe
K7CZKT-5562	Text document
KA8UHU-5562	executable (.exe)
KYBNNV-5562	The actual file format for the file at path C:\Users\thomas\text.txt is an executable file as the signature has an "MZ" value.
L7QRBN-5561	DOS MZ Executable
LACBFT-5562	ZAP ZoneAlarm data file

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13 - Examination Questions	
WebCode Test	**Response**
LKDRCP-5561	Windows Executable, EXE
LMYFNP-5561	MS DOS executable
LN7VWF-5562	Application - EXE/DLL
LRRKGT-5562	Exe
LUECCW-5561	Executable
LYJAEX-5561	application/x-msdownload - File System
M2VAHU-5562	PE32+
MD7R7R-5562	executable
MGM8JP-5561	* Not in scope of agency exam
ML4AQV-5561	EXE
MQXA6Q-5562	ZoneAlam data file
MR7JXN-5561	Windows/DOS executable file
MRTR8R-5561	EXE/DLL
MV6VTN-5562	MZ, DOS executable file in Windows
NJQ8AP-5561	The file type is a MZ file. A .MZ file is a portable executable file for DOS systems.
NK3WJT-5561	.EXE
PAF6NN-5561	MS DOS executable. File type is MZ. Based on the file signature, could be a DLL, COM or EXE file.
PPBH8Q-5561	DOS MZ executable
PQH2LD-5561	DOS MZ executable
PZAD6L-5561	.exe
Q2Z3GD-5562	exe
QCLZQR-5562	ZAP or ZoneAlam data file. Multiple file types contain the first 2 or 8 bytes of this file signature, so there could be multiple answers to this question based on where you believe the file signature ends. The ZAP signature contains all of the bytes listed in the hex.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13 - Examination Questions	
WebCode Test	**Response**
QEMD4J-5561	MS DOS Executable - Header "MZ"
QH4FBN-5562	exe
QT7QQQ-5561	Plain Text File
QWAN2J-5561	executable (exe)
QYVDDJ-5561	EXE
R86XKL-5561	Executable for Windows Write
RBJUPN-5561	.ZAP file (ZoneAlarm data file)
REKXEP-5561	portable executable (PE) file format
RR9ZXG-5561	Text document, txt
T8JQPN-5562	Windows Executable
T8LHLB-5561	An executable file
TGQH3P-5561	MZ File (.EXE)
THHLMJ-5562	Windows Executable (MZ)
TRHDUP-5562	EXE
TVPPWK-5562	executable
TZXUNK-5561	.exe
U3GARK-5562	.txt
U4CRUL-5562	Windows Executable
UGJTDH-5561	MZ hex header, DOS Executable file
UT9WBG-5562	Ejecutable .exe
V63DZH-5562	PE type(exe File)
VJJLKL-5562	EXE or Executable

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

WebCode Test	Response
VLV2EM-5561	txt
VYH7LJ-5561	executable application
W7CX8H-5562	PE32+ executable (GUI) x86-64, for MS Windows
W9FNCC-5561	MZ Portable Executable (PE) file format
WH87QK-5562	DOS Executable or EXE or Executable or ZAP or ZoneAlarm
WKE9TJ-5562	Windows/DOS Executable
WRVWDD-5561	.exe
WVD7FJ-5562	Text Document
X9VFGE-5562	DOS executable (.exe)
XDUKGE-5562	DOS MZ executable
XFRBFD-5561	Windows Executable (.exe), sub-type pe-format (portable exe)
XGRD6G-5562	MZ (file signature) – Windows DOS executable file
XMC987-5562	text/plain
XY6VCG-5562	.Exe – Executable
Y36EXF-5561	application/x-msdownload, Win64 EXE
YVMR6B-5561	DOS executable file
YVR6WD-5561	WINDOWS EXECUTABLE
Z8XMWF-5562	An executable file
ZBE3BE-5561	.exe (DOS MZ executable format)
ZNK3ZC-5562	Application (EXE/DLL)
ZRL9H3-5562	.txt
ZZUWEA-5562	DOS MZ Executable

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13 - Examination Questions

Question 13: Provide the filetype (file format) for C: \Users\thomas\text.txt.

Consensus Result:

Microsoft Portable Executable; or
Windows Executable; or
DOS Executable, or
Application

Manufacturer's Response Explanation:

Inspection of the contents of C: \Users\thomas\text.txt shows its file header as 45 5A, or MZ, indicating a DOS executable filetype.

Manufacturer's Response Illustration:

X-Ways view of text.text

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 14 - Examination Questions

Question 14: Provide the filename for the MP3 recently opened by user thomas.

Manufacturer's
Response: groovy-ambient-funk-201745.mp3

WebCode Test	Response
24VY4B-5561	groovy-ambient-funk-201745.mp3
24WLMH-5561	groovy-ambient-funk-201745.mp3
2RG9U9-5562	groovy-ambient-funk-201745.mp3
2U4TZC-5561	groovy-ambient-funk-201745.mp3
349ZFC-5562	groovy-ambient-funk-201745.mp3
3BYPCG-5561	groovy-ambient-funk-201745.mp3
3GDA68-5561	groovy-ambient-funk-201745.mp3
3J4DXE-5562	groovy-ambient-funk-201745.mp3
3PA7TA-5561	groovy-ambient-funk-201745.mp3
4FFFK9-5561	groovy-ambient-funk-201745.mp3
4RN848-5561	groovy-ambient-funk-201745.mp3
4ZJ2KE-5562	groovy-ambient-funk-201745.mp3
63LLN6-5561	groovy-ambient-funk-201745.mp3
673VQB-5562	Groovy-ambient-funk-201745.mp3
6PJ238-5561	groovy-ambient-funk-201745.mp3
7CQT46-5561	groovy-ambient-funk-201745.mp3
7PVVH8-5561	groovy-ambient-funk-201745.mp3
8FPDKA-5562	groovy-ambient-funk-201745.mp3
8KE4Q6-5561	" groovy-ambient-funk-201745.mp3"
8TBZD8-5562	Not in scope.
8WNN47-5562	groovy-ambient-funk-201745.mp3

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 14 - Examination Questions	
WebCode Test	**Response**
A444U7-5562	groovy-ambient-funk-201745.mp3
AEKNE3-5561	groovy-ambient-funk-201745.mp3
AFF7G6-5561	groovy-ambient-funk-201745.mp3
AUY2L3-5562	groovy-ambient-funk-201745.mp3
AXDN7Y-5561	groovy-ambient-funk-201745.mp3
B7LHX8-5561	groovy-ambient-funk-201745
B8ELJ2-5561	groovy-ambient-funk-201745.mp3
BEGRX4-5562	groovy-ambient-funk-201745.mp3
BTXP36-5562	AchievementUnlocked.mp3
CDHZN3-5561	groovy-ambient-funk-201745.mp3
CTEYRY-5562	groovy-ambient-funk-201745.mp3
CWHMF2-5561	groovy-ambient-funk-201745.mp3
DB9AYY-5561	groovy-ambient-funk-201745.mp3
DJLBA2-5562	groovy-ambient-funk-201745.mp3
DPCKJZ-5561	groovy-ambient-funk-201745.mp3
E6FEQZ-5562	groovy-ambient-funk-201745.mp3
EYTN7P-5562	groovy-ambient-funk-201745.mp3
F4KDZ3-5562	Message_Notification_SetA_v14_v2.mp3
FJ22JX-5562	groovy-ambient-funk-201745.mp3
FMYKLW-5561	groovy-ambient-funk-201745.mp3
GA6R7K-5561	groovy-ambient-funk-201745.mp3
GA8D2Z-5562	groovy-ambient-funk-201745.mp3

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 14 - Examination Questions	
WebCode Test	**Response**
GJP4GX-5562	groovy-ambient-funk-201745.mp3
GPH4VT-5561	groovy-ambient-funk-201745.mp3
GQUT6W-5561	groovy-ambient-funk-201745.mp3
GTHERT-5562	groovy-ambient-funk-201745
GTZ73X-5562	groovy-ambient-funk-201745.mp3
HEX8ER-5562	groovy-ambient-funk-201745.mp3
HF9WVJ-5561	Message_Notification_SetA_v14_v2.mp3
HFCE3U-5561	groovy-ambient-funk-201745.mp3
HXUD8T-5562	groovy-ambient-funk-201745.mp3
HYZ6QT-5562	groovy-ambient-funk-201745.mp3
J2L9YQ-5561	groovy-ambient-funk-201745.mp3
J7HNUT-5561	groovy-ambient-funk-201745.mp3
JGEWDV-5562	groovy-ambient-funk-201745.mp3
JYYMCV-5561	groovy-ambient-funk-201745.mp3
JZU7EW-5561	groovy-ambient-funk-201745.mp3
K2HYQQ-5561	groovy-ambient-funk-201745.mp3
K7CZKT-5562	F:\groovy-ambient-funk-201745.mp3
KA8UHU-5562	groovy-ambient-funk-201745.mp3
KYBNNV-5562	The filename for the MP3 that was recently opened by the thomas user is groovy-ambient-funk-201745.mp3.
L7QRBN-5561	groovy-ambient-funk-201745.mp3
LACBFT-5562	groovy-ambient-funk-201745.mp3
LKDRCP-5561	groovy-ambient-funk-201745.mp3

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

WebCode Test	Response
LMYFNP-5561	groovy-ambient-funk-201745.mp3
LN7VWF-5562	groovy-ambient-funk-201745.mp3
LRRKGT-5562	groovy-ambient-funk-201745.mp3
LUECCW-5561	groovy-ambient-funk-201745.mp3
LYJAEX-5561	F:\groovy-ambient-funk-201745.mp3
M2VAHU-5562	groovy-ambient-funk-201745
MD7R7R-5562	groovy-ambient-funk-201745.mp3
MGM8JP-5561	groovy-ambient-funk-201745.mp3
ML4AQV-5561	groovy-ambient-funk-201745.mp3
MQXA6Q-5562	groovy-ambient-funk-201745.mp3
MR7JXN-5561	groovy-ambient-funk-201745.mp3
MRTR8R-5561	groovy-ambient-funk-201745
MV6VTN-5562	Message_Notification_SetA_v14_v2.mp3
NJQ8AP-5561	groovy-ambient-funk-201745.mp3.lnk
NK3WJT-5561	groovy-ambient-funk-201745.mp3
PAF6NN-5561	F:\groovy-ambient-funk-201745.mp3
PPBH8Q-5561	groovy-ambient-funk-201745.mp3
PQH2LD-5561	groovy-ambient-funk-201745.mp3
PZAD6L-5561	groovy-ambient-funk-201745.mp3
Q2Z3GD-5562	F:\groovy-ambient-funk-201745.mp3
QCLZQR-5562	groovy-ambient-funk-201745.mp3
QEMD4J-5561	groovy-ambient-funk-201745.mp3

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 14 - Examination Questions	
WebCode Test	**Response**
QH4FBN-5562	Message_Notification_SetA_v14_v2.mp3
QT7QQQ-5561	groovy-ambient-funk-201745.mp3
QWAN2J-5561	groovy-ambient-funk-201745.mp3
QYVDDJ-5561	groovy-ambient-funk-201745.mp3
R86XKL-5561	groovy-ambient-funk-201745.mp3
RBJUPN-5561	groovy-ambient-funk-201745.mp3
REKXEP-5561	groovy-ambient-funk-201745.mp3
RR9ZXG-5561	groovy-ambient-funk-201745.mp3
T8JQPN-5562	groovy-ambient-funk-201745.mp3
T8LHLB-5561	groovy-ambient-funk-201745.mp3
TGQH3P-5561	groovy-ambient-funk-201745.mp3
THHLMJ-5562	AchievementUnlocked.mp3
TRHDUP-5562	groovy-ambient-funk-201745.mp3
TVPPWK-5562	groovy-ambient-funk-201745.mp3
TZXUNK-5561	Message_Notification_SetA_v14_v2.mp3
U3GARK-5562	F:\groovy-ambient-funk-201745.mp3
U4CRUL-5562	groovy-ambient-funk-201745.mp3
UGJTDH-5561	groovy-ambient-funk-201745.mp3
UT9WBG-5562	groovy-ambient-funk-201745.mp3
V63DZH-5562	groovy-ambient-funk-201745.mp3
VJJLKL-5562	groovy-ambient-funk-201745.mp3
VLV2EM-5561	groovy-ambient-funk-201745.mp3

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 14 - Examination Questions	
WebCode Test	**Response**
VYH7LJ-5561	groovy-ambient-funk-201745.mp3
W7CX8H-5562	groovy-ambient-funk-201745.mp3
W9FNCC-5561	groovy-ambient-funk-201745.mp3
WH87QK-5562	groovy-ambient-funk-201745.mp3
WKE9TJ-5562	groovy-ambient-funk-201745.mp3
WRVWDD-5561	groovy-ambient-funk-201745.mp3
WVD7FJ-5562	groovy-ambient-funk-201745.mp3
X9VFGE-5562	groovy-ambient-funk-201745.mp3
XDUKGE-5562	groovy-ambient-funk-201745.mp3
XFRBFD-5561	groovy-ambient-funk-201745.mp3
XGRD6G-5562	groovy-ambient-funk-201745.mp3
XMC987-5562	groovy-ambient-funk-201745.mp3
XY6VCG-5562	groovy-ambient-funk-201745.mp3
Y36EXF-5561	groovy-ambient-funk-201745.mp3
YVMR6B-5561	file:///F:/groovy-ambient-funk-201745.mp3
YVR6WD-5561	groovy-ambient-funk-201745.mp3
Z8XMWF-5562	groovy-ambient-funk-201745.mp3
ZBE3BE-5561	groovy-ambient-funk-201745.mp3
ZNK3ZC-5562	groovy-ambient-funk-201745.mp3
ZRL9H3-5562	groovy-ambient-funk-2017-45.mp3
ZZUWEA-5562	Groovy-ambient-funk-201745

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 14 - Examination Questions

Question 14: Provide the filename for the MP3 recently opened by user thomas.

Consensus Result:

groovy-ambient-funk-201745.mp3

Manufacturer's Response Explanation:

Links to recently opened files are created in the user's AppData\Roaming\Microsoft\Windows\Recent directory. These "link files" bear the name of the opened file but have a .lnk extension. The .lnk files contain data including the path to the opened file. Recently used files are also listed in the user's NTUSER.DAT registry file.

Manufacturer's Response Illustration:

X-ways view of lnk file details and parse of target file path

RegRipper parse of \Users\thomas\NTUSER.DAT:

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15 - Examination Questions

Question 15: What terms did the user search for with the Edge browser, 02/19/25 (February 19, 2025) 20:10:21 (subject computer's local time)?

<u>Manufacturer's</u> "philadelphia houses for rent"
<u>Response:</u>

WebCode Test	Response
24VY4B-5561	philadelphia houses for rent
24WLMH-5561	philadelphia houses for rent
2RG9U9-5562	philadelphia houses for rent
2U4TZC-5561	Philadelphia houses for rent
349ZFC-5562	philadelphia houses for rent
3BYPCG-5561	"philadelphia houses for rent"
3GDA68-5561	philadelphia houses for rent
3J4DXE-5562	philadelphia houses for rent
3PA7TA-5561	philadelphia houses for rent
4FFFK9-5561	philadelphia houses for rent
4RN848-5561	philadelphia houses for rent
4ZJ2KE-5562	philadelphia houses for rent
63LLN6-5561	philadelphia houses for rent
673VQB-5562	Philadelphia houses for rent
6PJ238-5561	philadelphia houses for rent
7CQT46-5561	philadelphia houses for rent
7PVVH8-5561	philadelphia houses for rent
8FPDKA-5562	philadelphia houses for rent, philadelphia houses for sale
8KE4Q6-5561	"philadelphia houses for rent"

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15 - Examination Questions	
WebCode Test	**Response**
8TBZD8-5562	Not in scope.
8WNN47-5562	philadelphia houses for rent
A444U7-5562	philadelphia houses for rent
AEKNE3-5561	philadelphia houses for rent
AFF7G6-5561	philadelphia houses for rent
AUY2L3-5562	philadelphia houses for rent
AXDN7Y-5561	philadelphia houses for rent
B7LHX8-5561	Philadelphia houses for rent
B8ELJ2-5561	philadelphia houses for rent
BEGRX4-5562	philadelphia houses for rent
BTXP36-5562	Philadelphia houses for rent
CDHZN3-5561	philadelphia houses for rent
CTEYRY-5562	philadelphia houses for rent
CWHMF2-5561	philadelphia houses for rent
DB9AYY-5561	philadelphia houses for rent
DJLBA2-5562	philadelphia houses for rent
DPCKJZ-5561	philadelphia houses for rent
E6FEQZ-5562	philadelphia houses for rent
EYTN7P-5562	philadelphia houses for rent
F4KDZ3-5562	Philadelphia houses for rent
FJ22JX-5562	philadelphia houses for rent

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15 - Examination Questions	
WebCode Test	**Response**
FMYKLW-5561	philadelphia houses for rent
GA6R7K-5561	philadelphia houses for rent
GA8D2Z-5562	philadelphia houses for rent
GJP4GX-5562	philadelphia houses for rent
GPH4VT-5561	Philadelphia houses for rent
GQUT6W-5561	philadelphia houses for rent
GTHERT-5562	philadelphia houses for rent
GTZ73X-5562	philadelphia houses for rent
HEX8ER-5562	philadelphia houses for rent
HF9WVJ-5561	philadelphia houses for rent
HFCE3U-5561	philadelphia houses for rent
HXUD8T-5562	philadelphia houses for rent
HYZ6QT-5562	philadelphia houses for rent
J2L9YQ-5561	philadelphia houses for rent; philadelphia houses for sale
J7HNUT-5561	philadelphia houses for rent
JGEWDV-5562	philadelphia houses for rent
JYYMCV-5561	philadelphia houses for rent
JZU7EW-5561	philadelphia houses for rent
K2HYQQ-5561	philadelphia houses for rent
K7CZKT-5562	philadelphia houses for rent
KA8UHU-5562	philadelphia houses for rent

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15 - Examination Questions	
WebCode Test	**Response**
KYBNNV-5562	The user searched for "philadelphia houses for rent" with Edge browser on February 19, 2025.
L7QRBN-5561	philadelphia houses for rent
LACBFT-5562	philadelphia houses for rent
LKDRCP-5561	philadelphia houses for rent
LMYFNP-5561	philadelphia houses for rent
LN7VWF-5562	philadelphia houses for rent
LRRKGT-5562	Philadelphia houses for rent / Philadelphia houses for sale
LUECCW-5561	philadelphia houses for rent
LYJAEX-5561	philadelphia houses for rent
M2VAHU-5562	philadelphia houses for rent
MD7R7R-5562	Philadelphia houses for rent
MGM8JP-5561	philadelphia houses for rent
ML4AQV-5561	philadelphia houses for rent
MQXA6Q-5562	philadelphia houses for rent
MR7JXN-5561	Philadelphia houses for rent
MRTR8R-5561	philadelphia houses for rent
MV6VTN-5562	Philadelphia houses for rent
NJQ8AP-5561	philadelphia houses for rent
NK3WJT-5561	philadelphia houses for rent
PAF6NN-5561	philadelphia houses for rent
PPBH8Q-5561	philadelphia houses for rent

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15 - Examination Questions	
WebCode Test	**Response**
PQH2LD-5561	philadelphia houses for rent
PZAD6L-5561	philadelphia houses for rent
Q2Z3GD-5562	philadelphia houses for sale
QCLZQR-5562	philadelphia houses for rent
QEMD4J-5561	philadelphia houses for rent
QH4FBN-5562	philadelphia houses for rent
QT7QQQ-5561	philadelphia houses for rent
QWAN2J-5561	philadelphia houses for rent
QYVDDJ-5561	philadelphia houses for rent
R86XKL-5561	Philadelphia houses for rent
RBJUPN-5561	philadelphia houses for rent
REKXEP-5561	philadelphia houses for rent
RR9ZXG-5561	philadelphia houses for rent
T8JQPN-5562	philadelphia houses for rent
T8LHLB-5561	philadelphia houses for rent
TGQH3P-5561	philadelphia houses for rent
THHLMJ-5562	Philadelphia houses for rent
TRHDUP-5562	philadelphia houses for rent
TVPPWK-5562	philadelphia houses for rent
TZXUNK-5561	philadelphia houses for rent
U3GARK-5562	Philadelphia houses for rent

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15 - Examination Questions	
WebCode Test	**Response**
U4CRUL-5562	'philadelphia houses for rent'
UGJTDH-5561	philadelphia houses for rent
UT9WBG-5562	philadelphia houses for rent - philadelphia houses for sale
V63DZH-5562	philadelphia houses for rent
VJJLKL-5562	philadelphia houses for rent
VLV2EM-5561	Philadelphia houses for rent
VYH7LJ-5561	philadelphia houses for rent
W7CX8H-5562	philadelphia houses for rent
W9FNCC-5561	philadelphia houses for rent
WH87QK-5562	philadelphia houses for rent
WKE9TJ-5562	philadelphia houses for rent
WRVWDD-5561	philadelphia houses for rent
WVD7FJ-5562	philadelphia houses for rent
X9VFGE-5562	philadelphia houses for rent
XDUKGE-5562	philadelphia houses for rent
XFRBFD-5561	philadelphia houses for rent
XGRD6G-5562	philadelphia houses for rent
XMC987-5562	philadelphia houses for rent
XY6VCG-5562	philadelphia houses for rent
Y36EXF-5561	philadelphia houses for rent
YVMR6B-5561	philadelphia houses for rent

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15 - Examination Questions	
WebCode Test	**Response**
YVR6WD-5561	philadelphia houses for rent
Z8XMWF-5562	Philadelphia houses for rent
ZBE3BE-5561	philadelphia houses for rent
ZNK3ZC-5562	philadelphia houses for rent
ZRL9H3-5562	[Participant did not return results for this question.]
ZZUWEA-5562	Philadelphia houses for rent

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15 - Examination Questions

Question 15: What terms did the user search for with the Edge browser, 02/19/25 (February 19, 2025) 20:10:21 (subject computer's local time)?

Consensus Result:

"philadelphia houses for rent"

Manufacturer's Response Explanation:

Edge browser history for each user is stored in an SQLite database in 25-5561\Laptop Computer Laptop Computer C:\Users\thomas\AppData\Local\Microsoft\Edge\User Data\Default\History.

Manufacturer's Response Illustration:

EnCase parse of C:\Users\thomas\AppData\Local\Microsoft\Edge\User Data\Default\History

True Path	Record Last Accessed	Url Name
Users\thomas\AppData\Local\Microsoft\Edge\User Data\Default\...	02/19/25 20:08:21 (-7:00 ...	https://www.bing.com/search?pglt=2083&q=ipchicken&cvid=620da29a03094...
Users\thomas\AppData\Local\Microsoft\Edge\User Data\Default\...	02/19/25 20:10:21 (-7:00 ...	https://www.bing.com/search?pglt=2083&q=philadelphia+houses+for+rent&...
Users\thomas\AppData\Local\Microsoft\Edge\User Data\Default\...	02/23/25 18:50:35 (-7:00 ...	https://www.bing.com/search?q=philadelphia%20houses%20for%20sale&qs...

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16 - Examination Questions

Question 16: What 3rd party (non-Microsoft) email client was installed and in use on the subject computer?

<u>Manufacturer's Response:</u> Mozilla Thunderbird

WebCode Test	Response
24VY4B-5561	Mozilla Thunderbird (x64 en-US)
24WLMH-5561	Mozilla Thunderbird
2RG9U9-5562	Mozilla Thunderbird
2U4TZC-5561	Mozilla thunderbird
349ZFC-5562	Mozilla thunderbird
3BYPCG-5561	Mozilla Thunderbird (x64 en-US)
3GDA68-5561	Mozilla Thunderbird
3J4DXE-5562	Mozilla Thunderbird
3PA7TA-5561	Mozilla Thunderbird
4FFFK9-5561	Thunderbird
4RN848-5561	Moxilla Thunderbird
4ZJ2KE-5562	Mozilla Thunderbird
63LLN6-5561	Mozilla Thunderbird
673VQB-5562	Mozilla Thunderbird
6PJ238-5561	Thunderbird
7CQT46-5561	Mozilla Thunderbird
7PVVH8-5561	Mozilla Thunderbird
8FPDKA-5562	Thunderbird
8KE4Q6-5561	Mozilla Thunderbird

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16 - Examination Questions	
WebCode Test	**Response**
8TBZD8-5562	Not in scope.
8WNN47-5562	Mozilla Thunderbird
A444U7-5562	Thunderbird
AEKNE3-5561	Mozilla Thunderbird
AFF7G6-5561	Mozilla Thunderbird (x64 en-US)
AUY2L3-5562	Mozilla Thunderbird (x64 en-US)
AXDN7Y-5561	Mozilla Thunderbird
B7LHX8-5561	Mozilla thunderbird (x64 en-US)
B8ELJ2-5561	Mozilla Thunderbird
BEGRX4-5562	Mozilla Thunderbird
BTXP36-5562	mozilla thunderbird
CDHZN3-5561	Mozilla Thunderbird
CTEYRY-5562	Mozilla Thunderbird (x64 en-US)
CWHMF2-5561	Thunderbird
DB9AYY-5561	Mozilla Thunderbird
DJLBA2-5562	Mozilla Thunderbird
DPCKJZ-5561	Mozilla Thunderbird
E6FEQZ-5562	Mozilla Thunderbird
EYTN7P-5562	Mozilla Thunderbird (x64 en-US)
F4KDZ3-5562	Thunderbird
FJ22JX-5562	Mozilla Thunderbird

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16 - Examination Questions	
WebCode Test	**Response**
FMYKLW-5561	Mozilla Thunderbird (version 128.7.1)
GA6R7K-5561	Thunderbird
GA8D2Z-5562	Mozilla Thunderbird
GJP4GX-5562	Mozilla Thunderbird
GPH4VT-5561	Mozzilla Thunderbird
GQUT6W-5561	Mozilla Thunderbird (x64 en-US)
GTHERT-5562	Mozilla thunderbird (x64 en-US)
GTZ73X-5562	Mozilla Thunderbird
HEX8ER-5562	Thunderbird
HF9WVJ-5561	Mozilla Thunderbird (x64 en-US)
HFCE3U-5561	Mozilla Thunderbird
HXUD8T-5562	Mozilla Thunderbird (x64 en-US)
HYZ6QT-5562	Mozilla Thunderbird
J2L9YQ-5561	Mozilla Thunderbird (x64 en-US)
J7HNUT-5561	Mozilla Thunderbird
JGEWDV-5562	Mozilla Thunderbird
JYYMCV-5561	Mozilla Thunderbird
JZU7EW-5561	Mozilla Thunderbird x64 128.7.1
K2HYQQ-5561	Mozilla Thunderbird 128.7.1 (x64 en-US)
K7CZKT-5562	Mozilla Thunderbird
KA8UHU-5562	Thunderbird

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16 - Examination Questions	
WebCode Test	**Response**
KYBNNV-5562	Thunderbird was installed on the subject computer.
L7QRBN-5561	Thunderbird
LACBFT-5562	Mozilla Thunderbird
LKDRCP-5561	Mozilla Thunderbird
LMYFNP-5561	Mozilla Thunderbird
LN7VWF-5562	Thunderbird
LRRKGT-5562	Thunderbird
LUECCW-5561	Mozilla Thunderbird (x64 en-US)
LYJAEX-5561	Mozilla Thunderbird (x64 en-US) v.128.7.1
M2VAHU-5562	Mozilla Thunderbird
MD7R7R-5562	Mozilla Thunderbird
MGM8JP-5561	Thunderbird
ML4AQV-5561	Mozilla Thunderbird (x64 en-US)
MQXA6Q-5562	Thunderbird
MR7JXN-5561	Mozilla Thunderbird
MRTR8R-5561	Thunderbird
MV6VTN-5562	Mozilla Thunderbird
NJQ8AP-5561	Mozilla Thunderbird (x64 en-US)
NK3WJT-5561	Mozilla Thunderbird
PAF6NN-5561	Mozilla Thunderbird
PPBH8Q-5561	Mozilla Thunderbird

(119)

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

WebCode Test	Response
PQH2LD-5561	Mozilla Thunderbird (x64 en-US)
PZAD6L-5561	Mozilla Thunderbird
Q2Z3GD-5562	Mozilla Thunderbird
QCLZQR-5562	Mozilla Thunderbird
QEMD4J-5561	Thunderbird by Mozilla
QH4FBN-5562	Mozilla Thunderbird
QT7QQQ-5561	Thunderbird
QWAN2J-5561	Thunderbird
QYVDDJ-5561	Mozilla Thunderbird (x64 en-US)
R86XKL-5561	Mozilla Thunderbird
RBJUPN-5561	Mozilla Thunderbird
REKXEP-5561	Mozilla Thunderbird
RR9ZXG-5561	WhatsAppDesktop, Clipchamp, 7zip 24.09 (x64), Mozilla Firefox (x64-en-US), Mozilla Thunderbird (x64 en-US), Mozilla Maintenance Service, Oracle VM VirtualBox Guest Additions 7.0.14, WinDirStat, OpenOffice 4.1.15
T8JQPN-5562	Mozilla Thunderbird
T8LHLB-5561	Thunderbird (Mozilla), known as MBOX
TGQH3P-5561	Mozilla Thunderbird
THHLMJ-5562	Mozilla Thunderbird
TRHDUP-5562	Mozilla Thunderbird
TVPPWK-5562	Thunderbird
TZXUNK-5561	leslielessor@gmail.com
U3GARK-5562	Thunderbird

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16 - Examination Questions	
WebCode Test	**Response**
U4CRUL-5562	Mozilla Thunderbird
UGJTDH-5561	Thunderbird
UT9WBG-5562	Mozilla Thunderbird
V63DZH-5562	Mozilla Thunderbird
VJJLKL-5562	Mozilla Thunderbird
VLV2EM-5561	Mozilla Thunderbird
VYH7LJ-5561	Mozilla Thunderbird
W7CX8H-5562	Mozilla Thunderbird
W9FNCC-5561	Mozilla Thunderbird (x64 en-US)
WH87QK-5562	Mozilla Thunderbird
WKE9TJ-5562	Mozilla Thunderbird
WRVWDD-5561	Mozilla Thunderbird
WVD7FJ-5562	Mozilla Thunderbird
X9VFGE-5562	Mozilla Thunderbird
XDUKGE-5562	Mozilla Thunderbird (x64 en-US)
XFRBFD-5561	Mozilla Thunderbird (X64 en-US)
XGRD6G-5562	Mozilla Thunderbird
XMC987-5562	Thunderbird
XY6VCG-5562	Mozilla Thunderbird
Y36EXF-5561	Mozilla Thunderbird
YVMR6B-5561	Mozilla Thunderbird (x64 en-US)

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16 - Examination Questions	
WebCode Test	**Response**
YVR6WD-5561	Mozilla Thunderbird
Z8XMWF-5562	Thunderbird
ZBE3BE-5561	Mozilla Thunderbird
ZNK3ZC-5562	Mozilla Thunderbird (x64 en-US)
ZRL9H3-5562	MBOX Emails
ZZUWEA-5562	Thunderbird

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16 - Examination Questions

Question 16: What 3rd party (non-Microsoft) email client was installed and in use on the subject computer?

Consensus Result:

Mozilla Thunderbird

Manufacturer's Response Explanation:

Many locations on the Windows operating system indicate installed applications. Reviewing the folders in C:\Program Files for executable programs will discover C:\Program Files\Mozilla Thunderbird\thunderbird.exe. The SOFTWARE registry hive also contains a list of 'Uninstall Keys" showing installed programs at C:\Windows\System32\Config\Software: Microsoft\Windows\CurrentVersion\Uninstall.

Manufacturer's Response Illustration:

EnCase list of installed software

RegRipper parse of C:\Windows\System32\Config\Software: Microsoft\Windows\CurrentVersion\Uninstall

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17 - Examination Questions

Question 17: Provide the text in the file named "the answer to question 17".

Manufacturer's "Never gonna give you up"
Response:

WebCode Test	Response
24VY4B-5561	Never gonna give you up
24WLMH-5561	Never gonna give you up
2RG9U9-5562	Never gonna give you up
2U4TZC-5561	[Participant did not return results for this question.]
349ZFC-5562	password
3BYPCG-5561	Never gonna give you up
3GDA68-5561	zip.zip\the answer to question 17 - \Users\thomas\AppData\Local\Microsoft\zip.zip\the answer to question 17
3J4DXE-5562	Never gonna give you up
3PA7TA-5561	Never gonna give you up
4FFFK9-5561	Never gonna give you up
4RN848-5561	Never gonna give you up
4ZJ2KE-5562	Never gonna give you up
63LLN6-5561	Never gonna give you up
673VQB-5562	Never gonna give you up
6PJ238-5561	Never gonna give you up
7CQT46-5561	Never gonna give you up
7PVVH8-5561	Never gonna give you up
8FPDKA-5562	Never gonna give you up
8KE4Q6-5561	"Never gonna give you up"
8TBZD8-5562	Not in scope.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17 - Examination Questions	
WebCode Test	**Response**
8WNN47-5562	Never gonna give you up
A444U7-5562	Never gonna give you up
AEKNE3-5561	Never gonna give you up
AFF7G6-5561	"Never gonna give you up"
AUY2L3-5562	Never gonna give you up
AXDN7Y-5561	Never gonna give you up
B7LHX8-5561	Never gonna give you up
B8ELJ2-5561	Never gonna give you up
BEGRX4-5562	Never gonna give you up
BTXP36-5562	never gonna give you up
CDHZN3-5561	Never gonna give you up
CTEYRY-5562	Never gonna give you up
CWHMF2-5561	Never gonna give you up
DB9AYY-5561	Never gonna give you up
DJLBA2-5562	Never gonna give you up
DPCKJZ-5561	Never gonna give you up
E6FEQZ-5562	Never gonna give you up
EYTN7P-5562	Never gonna give you up
F4KDZ3-5562	never gonna give you up
FJ22JX-5562	Never gonna give you up
FMYKLW-5561	Never gonna give you up

(125)

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17 - Examination Questions	
WebCode Test	**Response**
GA6R7K-5561	File is password protected -
GA8D2Z-5562	never gonna give you up
GJP4GX-5562	File is contained in zip.zip and is password protected.
GPH4VT-5561	Never gonna give you up
GQUT6W-5561	Never gonna give you up
GTHERT-5562	Never gonna give you up
GTZ73X-5562	Never gonna give you up
HEX8ER-5562	Never gonna give you up
HF9WVJ-5561	Never gonna give you up
HFCE3U-5561	Never gonna give you up
HXUD8T-5562	Never gonna give you up
HYZ6QT-5562	Never gonna give you up
J2L9YQ-5561	Never gonna give you up
J7HNUT-5561	Never gonna give you up
JGEWDV-5562	Never gonna give you up
JYYMCV-5561	Never gonna give you up
JZU7EW-5561	Never gonna give you up
K2HYQQ-5561	Never gonna give you up
K7CZKT-5562	Never gonna give you up
KA8UHU-5562	Never gonna give you up
KYBNNV-5562	The file named "the answer to question 17" appears to be encrypted.

(126)

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17 - Examination Questions	
WebCode Test	**Response**
L7QRBN-5561	Never gonna give you up
LACBFT-5562	Never gonna give you up
LKDRCP-5561	Never gonna give you up
LMYFNP-5561	Never gonna give you up
LN7VWF-5562	File is password protected -
LRRKGT-5562	Never gonna give you up
LUECCW-5561	Never gonna give you up
LYJAEX-5561	Never gonna give you up
M2VAHU-5562	Never gonna give you up
MD7R7R-5562	Never gonna give you up
MGM8JP-5561	* Not in scope of agency exam
ML4AQV-5561	Never gonna give you up
MQXA6Q-5562	Never gonna give you up
MR7JXN-5561	Never gonna give you up
MRTR8R-5561	Never gonna give you up
MV6VTN-5562	Unable to answer.
NJQ8AP-5561	password
NK3WJT-5561	never gonna give you up
PAF6NN-5561	Never gonna give you up
PPBH8Q-5561	Never gonna give you up
PQH2LD-5561	Never gonna give you up

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17 - Examination Questions	
WebCode Test	**Response**
PZAD6L-5561	Never gonna give you up
Q2Z3GD-5562	Never gonna give you up
QCLZQR-5562	Never gonna give you up
QEMD4J-5561	Never gonna give you up
QH4FBN-5562	never gonna give you up
QT7QQQ-5561	Never gonna give you up
QWAN2J-5561	Never gonna give you up
QYVDDJ-5561	Never gonna give you up
R86XKL-5561	Never gonna give you up
RBJUPN-5561	Never gonna give you up
REKXEP-5561	Never gonna give you up
RR9ZXG-5561	Never gonna give you up
T8JQPN-5562	Never gonna give you up
T8LHLB-5561	"Never gonna give you up"
TGQH3P-5561	Never gonna give you up
THHLMJ-5562	Never gonna give you up
TRHDUP-5562	Never gonna give you up
TVPPWK-5562	Never gonna give you up
TZXUNK-5561	Never gonna give you up
U3GARK-5562	"Never gonna give you up"
U4CRUL-5562	The words shown on a picture is "Never gonna give you up"

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17 - Examination Questions	
WebCode Test	**Response**
UGJTDH-5561	Never gonna give you up
UT9WBG-5562	Never gonna give you up
V63DZH-5562	Never gonna give you up
VJJLKL-5562	Never gonna give you up
VLV2EM-5561	Never Gonne give you up
VYH7LJ-5561	Never gonna give you up
W7CX8H-5562	Never gonna give you up
W9FNCC-5561	Never gonna give you up
WH87QK-5562	Never gonna give you up
WKE9TJ-5562	never gonna give you up
WRVWDD-5561	Never gonna give you up
WVD7FJ-5562	Never gonna give you up
X9VFGE-5562	Never gonna give you up
XDUKGE-5562	Never gonna give you up
XFRBFD-5561	"Never gonna give you up"
XGRD6G-5562	Never gonna give you up
XMC987-5562	Never gonna give you up
XY6VCG-5562	Never gonna give you up
Y36EXF-5561	Never gonna give you up
YVMR6B-5561	Never gonna give you up
YVR6WD-5561	Never gonna give you up

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17 - Examination Questions	
WebCode Test	**Response**
Z8XMWF-5562	Never gonna give you up
ZBE3BE-5561	Never gonna give you up
ZNK3ZC-5562	Never gonna give you up
ZRL9H3-5562	zip file unable to decode text
ZZUWEA-5562	Never gonna give you up

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17 - Examination Questions

Question 17: Provide the text in the file named "the answer to question 17".

Consensus Result:

"Never gonna give you up"

Manufacturer's Response Explanation:

"The answer to question 17" is a file within the encrypted zip archive,
C:\Users\thomas\AppData\Local\Microsoft\zip.zip.
Because the internal directories of encrypted zip files are not encrypted, this filename can be found with a simple keyword search even though the contents of the file cannot be read until decrypted. Once found, the zip file password can be cracked using most forensic suites or cracking tools. The simple password, "password" is easily guessed. Once extracted, "the answer to question 17" file does not have a file extension. The participant must view it in a hex or text editor to inspect the file header and determine its type. The file header is FF D8 FF DB, indicating it is a jpeg image file. Viewing this file shows the contained text to be, "Never gonna give you up".

Manufacturer's Response Illustration:

X-ways keyword search hit for "question 17"

7zip password encryption
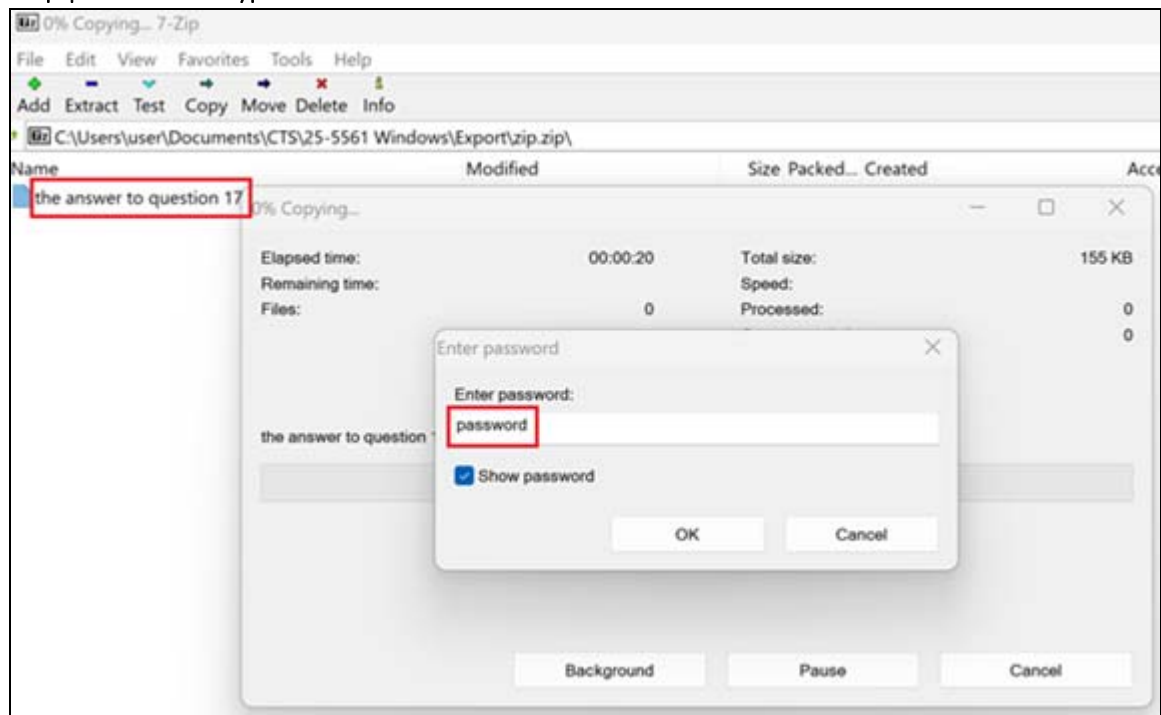
Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17 - Examination Questions

HxD view of "the answer to question 17"

the answer to question 17.jpg

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18 - Examination Questions

Question 18: What email address was the installed (non-Microsoft) email client configured to use?

<u>Manufacturer's</u> leslielessor@gmail.com
<u>Response:</u>

WebCode Test	Response
24VY4B-5561	leslielessor@gmail.com
24WLMH-5561	leslielessor@gmail.com
2RG9U9-5562	leslielessor@gmail.com
2U4TZC-5561	leslielessor@gmail.com
349ZFC-5562	leslielessor@gmail.com
3BYPCG-5561	leslielessor@gmail.com
3GDA68-5561	leslielessor@gmail.com
3J4DXE-5562	leslietlessor@realtyagent.com
3PA7TA-5561	leslielessor@gmail.com
4FFFK9-5561	leslielessor@gmail.com
4RN848-5561	leslielessor@gmail.com
4ZJ2KE-5562	leslielessor@gmail.com
63LLN6-5561	leslielessor@gmail.com
673VQB-5562	leslielessor@gmail.com
6PJ238-5561	leslielessor@gmail.com
7CQT46-5561	leslielessor@gmail.com
7PVVH8-5561	leslielessor@gmail.com
8FPDKA-5562	leslielessor@gmail.com
8KE4Q6-5561	leslielessor@gmail.com
8TBZD8-5562	Not in scope.

(133)

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18 - Examination Questions	
WebCode Test	**Response**
8WNN47-5562	leslielessor@gmail.com
A444U7-5562	leslielessor@gmail.com
AEKNE3-5561	leslielessor@gmail.com
AFF7G6-5561	leslielessor@gmail.com
AUY2L3-5562	leslielessor@gmail.com
AXDN7Y-5561	Leslie Lessor <leslielessor@gmail.com>
B7LHX8-5561	leslielessor@gmail.com
B8ELJ2-5561	leslielessor@gmail.com
BEGRX4-5562	leslielessor@gmail.com
BTXP36-5562	leslielessor@gmail.com
CDHZN3-5561	leslielessor@gmail.com
CTEYRY-5562	leslielessor@gmail.com
CWHMF2-5561	leslielessor@gmail.com
DB9AYY-5561	leslielessor@gmail.com
DJLBA2-5562	leslielessor@gmail.com
DPCKJZ-5561	leslielessor@gmail.com
E6FEQZ-5562	leslielessor@gmail.com
EYTN7P-5562	leslielessor@gmail.com
F4KDZ3-5562	leslielessor@gmail.com
FJ22JX-5562	leslielessor@gmail.com
FMYKLW-5561	leslielessor@gmail.com

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18 - Examination Questions	
WebCode Test	**Response**
GA6R7K-5561	[Participant did not return results for this question.]
GA8D2Z-5562	leslielessor@gmail.com
GJP4GX-5562	leslielessor@gmail.com
GPH4VT-5561	leslielessor@gmail.com
GQUT6W-5561	leslielessor@gmail.com
GTHERT-5562	leslielessor@gmail.com
GTZ73X-5562	leslielessor@gmail.com
HEX8ER-5562	leslielessor@gmail.com
HF9WVJ-5561	leslielessor@gmail.com
HFCE3U-5561	leslielessor@gmail.com
HXUD8T-5562	leslielessor@gmail.com
HYZ6QT-5562	leslielessor@gmail.com
J2L9YQ-5561	leslielessor@gmail.com
J7HNUT-5561	leslielessor@gmail.com
JGEWDV-5562	leslielessor@gmail.com
JYYMCV-5561	leslielessor@gmail.com
JZU7EW-5561	leslielessor@gmail.com
K2HYQQ-5561	leslielessor@gmail.com
K7CZKT-5562	leslielessor@gmail.com
KA8UHU-5562	leslielessor@gmail.com
KYBNNV-5562	The email address that Thunderbird was configured to use was leslielessor@gmail.com.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18 - Examination Questions	
WebCode Test	**Response**
L7QRBN-5561	leslielessor@gmail.com
LACBFT-5562	leslielessor@gmail.com
LKDRCP-5561	leslielessor@gmail.com
LMYFNP-5561	leslielessor@gmail.com
LN7VWF-5562	[Participant did not return results for this question.]
LRRKGT-5562	leslielessor@gmail.com
LUECCW-5561	danaderesident@gmail.com
LYJAEX-5561	leslielessor@gmail.com
M2VAHU-5562	leslielessor@gmail.com
MD7R7R-5562	leslielessor@gmail.com
MGM8JP-5561	leslielessor@gmail.com
ML4AQV-5561	danaderesident@gmail.com
MQXA6Q-5562	leslielessor@gmail.com
MR7JXN-5561	leslielessor@gmail.com
MRTR8R-5561	leslielessor@gmail.com
MV6VTN-5562	leslielessor@gmail.com
NJQ8AP-5561	leslielessor@gmail.com
NK3WJT-5561	leslielessor@gmail.com
PAF6NN-5561	leslielessor@gmail.com
PPBH8Q-5561	leslielessor@gmail.com
PQH2LD-5561	leslielessor@gmail.com

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18 - Examination Questions	
WebCode Test	**Response**
PZAD6L-5561	leslielessor@gmail.com
Q2Z3GD-5562	leslielessor@gmail.com
QCLZQR-5562	leslielessor@gmail.com
QEMD4J-5561	leslielessor@gmail.com
QH4FBN-5562	leslielessor@gmail.com
QT7QQQ-5561	leslielessor@gmail.com
QWAN2J-5561	leslielessor@gmail.com
QYVDDJ-5561	leslielessor@gmail.com
R86XKL-5561	leslielessor@gmail.com
RBJUPN-5561	leslielessor@gmail.com
REKXEP-5561	leslielessor@gmail.com
RR9ZXG-5561	leslietlessor@realtyagent.com
T8JQPN-5562	leslielessor@gmail.com
T8LHLB-5561	leslielessor@gmail.com
TGQH3P-5561	leslielessor@gmail.com
THHLMJ-5562	leslielessor@gmail.com
TRHDUP-5562	leslielessor@gmail.com
TVPPWK-5562	leslielessor@gmail.com
TZXUNK-5561	leslielessor@gmail.com
U3GARK-5562	leslielessor@gmail.com
U4CRUL-5562	leslielessor@gmail.com

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18 - Examination Questions	
WebCode Test	**Response**
UGJTDH-5561	leslielessor@gmail.com
UT9WBG-5562	leslielessor@gmail.com
V63DZH-5562	leslielessor@gmail.com
VJJLKL-5562	leslielessor@gmail.com
VLV2EM-5561	leslielessor@gmail.com
VYH7LJ-5561	leslielessor@gmail.com
W7CX8H-5562	leslielessor@gmail.com
W9FNCC-5561	leslielessor@gmail.com
WH87QK-5562	leslielessor@gmail.com
WKE9TJ-5562	leslielessor@gmail.com
WRVWDD-5561	leslielessor@gmail.com
WVD7FJ-5562	leslielessor@gmail.com
X9VFGE-5562	leslielessor@gmail.com
XDUKGE-5562	leslielessor@gmail.com
XFRBFD-5561	leslielessor@gmail.com
XGRD6G-5562	leslielessor@gmail.com
XMC987-5562	leslielessor@gmail.com
XY6VCG-5562	leslielessor@gmail.com
Y36EXF-5561	leslielessor@gmail.com
YVMR6B-5561	leslielessor@gmail.com
YVR6WD-5561	leslielessor@gmail.com

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18 - Examination Questions	
WebCode Test	**Response**
Z8XMWF-5562	leslielessor@gmail.com
ZBE3BE-5561	leslielessor@gmail.com
ZNK3ZC-5562	leslielessor@gmail.com
ZRL9H3-5562	leslielessor@gmail.com
ZZUWEA-5562	leslielessor@gmail.com

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18 - Examination Questions

Question 18: What email address was the installed (non-Microsoft) email client configured to use?

<u>Consensus Result:</u>

leslielessor@gmail.com

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

Configuration information for the Thunderbird email client is stored in
\Users\thomas\AppData\Roaming\Thunderbird\Profiles\x7zy6eh1.default-esr\prefs.js.

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

RegRipper parse of Mozilla User Preferences from prefs.js

```
1  ▶    // Mozilla User Preferences
81 ◀    user_pref("mail.identity.id1.useremail", "leslielessor@gmail.com");
82      user_pref("mail.identity.id1.valid", true);
83      user_pref("mail.nstmp_cleanup_completed", true);
84      user_pref("mail.rights.version", 1);
85      user_pref("mail.root.imap",
```

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 19 - Examination Questions

Question 19: What email address sent the email with sent date/time of 02/27/25 (February 27, 2025) 19:34:34 (subject computer's local time)?

<u>Manufacturer's</u> danaderesident@gmail.com
<u>Response:</u>

WebCode Test	Response
24VY4B-5561	danaderesident@gmail.com
24WLMH-5561	danaderesident@gmail.com
2RG9U9-5562	danaderesident@gmail.com
2U4TZC-5561	danaderesident@gmail.com
349ZFC-5562	danaderesident@gmail.com
3BYPCG-5561	danaderesident@gmail.com
3GDA68-5561	danaderesident@gmail.com
3J4DXE-5562	danaderesident@gmail.com
3PA7TA-5561	danaderesident@gmail.com
4FFFK9-5561	danaderesident@gmail.com
4RN848-5561	From: Dana DeResident danaderesident@gmail.com Sent: 27-Feb-25 19:34:34. To: Leslie Lessor leslielessor@gmail.com
4ZJ2KE-5562	danaderesident@gmail.com
63LLN6-5561	danaderesident@gmail.com
673VQB-5562	danaderesident@gmail.com
6PJ238-5561	danaderesident@gmail.com
7CQT46-5561	DanaDeresident@gmail.com
7PVVH8-5561	danaderesident@gmail.com
8FPDKA-5562	danaderesident@gmail.com
8KE4Q6-5561	danaderesident@gmail.com

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 19 - Examination Questions	
WebCode Test	**Response**
8TBZD8-5562	Not in scope.
8WNN47-5562	danaderesident@gmail.com
A444U7-5562	danaderesident@gmail.com
AEKNE3-5561	danaderesident@gmail.com
AFF7G6-5561	danaderesident@gmail.com
AUY2L3-5562	danaderesident@gmail.com
AXDN7Y-5561	Dana DeResident <danaderesident@gmail.com>
B7LHX8-5561	danaderesident@gmail.com
B8ELJ2-5561	danaderesident@gmail.com
BEGRX4-5562	danaderesident@gmail.com
BTXP36-5562	danaderesident@gmail.com
CDHZN3-5561	danaderesident@gmail.com
CTEYRY-5562	danaderesident@gmail.com
CWHMF2-5561	danaderesident@gmail.com
DB9AYY-5561	danaderesident@gmail.com
DJLBA2-5562	danaderesident@gmail.com
DPCKJZ-5561	danaderesident@gmail.com
E6FEQZ-5562	danaderesident@gmail.com
EYTN7P-5562	danaderesident@gmail.com
F4KDZ3-5562	danaderesident@gmail.com
FJ22JX-5562	danaderesident@gmail.com

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

WebCode Test	Response
FMYKLW-5561	danaderesident@gmail.com
GA6R7K-5561	[Participant did not return results for this question.]
GA8D2Z-5562	danaderesident@gmail.com
GJP4GX-5562	danaderesident@gmail.com
GPH4VT-5561	danaderesident@gmail.com
GQUT6W-5561	danaderesident@gmail.com
GTHERT-5562	danaderesident@gmail.com
GTZ73X-5562	danaderesident@gmail.com
HEX8ER-5562	danaderesident@gmail.com
HF9WVJ-5561	danaderesident@gmail.com
HFCE3U-5561	danaderesident@gmail.com
HXUD8T-5562	danaderesident@gmail.com
HYZ6QT-5562	danaderesident@gmail.com
J2L9YQ-5561	danaderesident@gmail.com
J7HNUT-5561	Dana DeResident <danaderesident@gmail.com>
JGEWDV-5562	danaderesident@gmail.com
JYYMCV-5561	danaderesident@gmail.com
JZU7EW-5561	danaderesident@gmail.com
K2HYQQ-5561	danaderesident@gmail.com
K7CZKT-5562	danaderesident@gmail.com
KA8UHU-5562	danaderesident@gmail.com

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 19 - Examination Questions	
WebCode Test	**Response**
KYBNNV-5562	The email address that was sent the email with the specified sent date/time was danaderesident@gmail.com.
L7QRBN-5561	danaderesident@gmail.com
LACBFT-5562	danaderesident@gmail.com
LKDRCP-5561	danaderesident@gmail.com
LMYFNP-5561	danaderesident@gmail.com
LN7VWF-5562	[Participant did not return results for this question.]
LRRKGT-5562	danaderesident@gmail.com
LUECCW-5561	danaderesident@gmail.com
LYJAEX-5561	danaderesident@gmail.com
M2VAHU-5562	danaderesident@gmail.com
MD7R7R-5562	danaderesident@gmail.com
MGM8JP-5561	danaresident@gmail.com
ML4AQV-5561	Dana DeResident <danaderesident@gmail.com>
MQXA6Q-5562	danaderesident@gmail.com
MR7JXN-5561	danaderesident@gmail.com
MRTR8R-5561	danaderesident@gmail.com
MV6VTN-5562	danaderesident@gmail.com
NJQ8AP-5561	danaderesident@gmail.com
NK3WJT-5561	danaderesident@gmail.com
PAF6NN-5561	danaderesident@gmail.com
PPBH8Q-5561	danaderesident@gmail.com

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 19 - Examination Questions	
WebCode Test	**Response**
PQH2LD-5561	danaderesident@gmail.com
PZAD6L-5561	danaderesident@gmail.com
Q2Z3GD-5562	danaderesident@gmail.com
QCLZQR-5562	danaderesident@gmail.com
QEMD4J-5561	danaderesident@gmail.com
QH4FBN-5562	danaderesident@gmail.com
QT7QQQ-5561	danaderesident@gmail.com
QWAN2J-5561	danaderesident@gmail.com
QYVDDJ-5561	danaderesident@gmail.com
R86XKL-5561	danaderesident@gmail.com
RBJUPN-5561	danaderesident@gmail.com
REKXEP-5561	danaderesident@gmail.com
RR9ZXG-5561	danaderesident@gmail.com
T8JQPN-5562	dataderesident@gmail.com
T8LHLB-5561	danaderesident@gmail.com
TGQH3P-5561	danaderesident@gmail.com
THHLMJ-5562	danaderesident@gmail.com
TRHDUP-5562	danaderesident@gmail.com
TVPPWK-5562	danaderesident@gmail.com
TZXUNK-5561	danaderesident@gmail.com
U3GARK-5562	Dana DeResident (danaderesident@gmail.com)

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 19 - Examination Questions	
WebCode Test	**Response**
U4CRUL-5562	danaderesident@gmail.com
UGJTDH-5561	danaderesident@gmail.com
UT9WBG-5562	danaderesident@gmail.com
V63DZH-5562	Dana DeResident <danaderesident@gmail.com>
VJJLKL-5562	danaderesident@gmail.com
VLV2EM-5561	danaderesident@gmail.com
VYH7LJ-5561	danaderesident@gmail.com
W7CX8H-5562	danaderesident@gmail.com
W9FNCC-5561	danaderesident@gmail.com
WH87QK-5562	danaderesident@gmail.com
WKE9TJ-5562	danaderesident@gmail.com
WRVWDD-5561	danaderesident@gmail.com
WVD7FJ-5562	leslielessor@gmail.com
X9VFGE-5562	danaderesident@gmail.com
XDUKGE-5562	danaderesident@gmail.com
XFRBFD-5561	danaderesident@gmail.com
XGRD6G-5562	danaderesident@gmail.com
XMC987-5562	danaderesident@gmail.com
XY6VCG-5562	danaderesident@gmail.com
Y36EXF-5561	danaderesident@gmail.com
YVMR6B-5561	danaderesident@gmail.com

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 19 - Examination Questions	
WebCode Test	**Response**
YVR6WD-5561	danaderesident@gmail.com
Z8XMWF-5562	danaderesident@gmail.com
ZBE3BE-5561	danaderesident@gmail.com
ZNK3ZC-5562	danaderesident@gmail.com
ZRL9H3-5562	no-reply@accounts.google.com
ZZUWEA-5562	danaderesident@gmail.com

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 19 - Examination Questions

Question 19: What email address sent the email with sent date/time of 02/27/25 (February 27, 2025) 19:34:34 (subject computer's local time)?

Consensus Result:

danaderesident@gmail.com

Manufacturer's Response Explanation:

Mozilla IMAP email data is stored in
C:\Users\thomas\AppData\Roaming\Thunderbird\Profiles\x7zy6eh1.default-esr\ImapMail\imap.gmail.com.msf.

Manufacturer's Response Illustration:
EnCase view of Re: NOW AVAILABLE NE PHILLY! email message
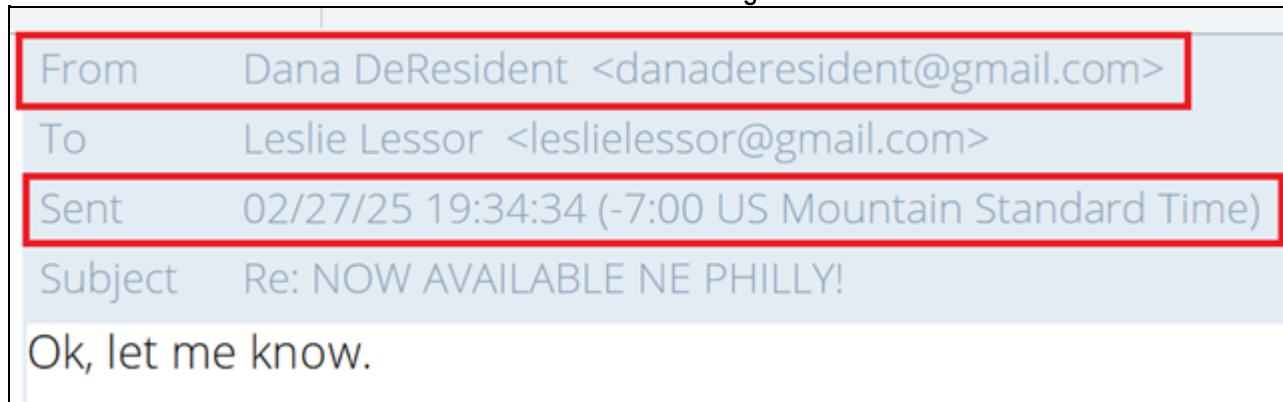
From	Dana DeResident <danaderesident@gmail.com>
To	Leslie Lessor <leslielessor@gmail.com>
Sent	02/27/25 19:34:34 (-7:00 US Mountain Standard Time)
Subject	Re: NOW AVAILABLE NE PHILLY!

Ok, let me know.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20 - Examination Questions

Question 20: Provide the original (pre-deletion) path of philly_2.pdf.

<u>Manufacturer's Response:</u> C:\Users\thomas\Desktop\philly_2.pdf

WebCode Test	Response
24VY4B-5561	C:\Users\thomas\Desktop\philly_2.pdf
24WLMH-5561	C:\Users\thomas\Desktop\philly_2.pdf
2RG9U9-5562	C:\Users\thomas\Desktop\philly_2.pdf
2U4TZC-5561	C:\Users\thomas\Desktop\philly_2.pdf
349ZFC-5562	C:\Users\thomas\Desktop\philly_2.pdf
3BYPCG-5561	C:\Users\thomas\Desktop\philly_2.pdf
3GDA68-5561	C:\Users\thomas\Desktop\philly_2.pdf
3J4DXE-5562	C:\Users\thomas\Desktop\philly_2.pdf
3PA7TA-5561	C:\Users\thomas\Desktop\philly_2.pdf
4FFFK9-5561	C:\Users\thomas\Desktop\philly_2.pdf
4RN848-5561	C:\Users\thomas\Desktop\philly_2.pdf
4ZJ2KE-5562	C:\Users\thomas\Desktop\philly_2.pdf
63LLN6-5561	C:\Users\thomas\Desktop
673VQB-5562	C:\Users\thomas\Desktop\philly_2.pdf
6PJ238-5561	C:\Users\thomas\Desktop\philly_2.pdf
7CQT46-5561	C:\Users\thomas\Desktop\philly_2.pdf
7PVVH8-5561	C:\Users\thomas\Desktop\philly_2.pdf
8FPDKA-5562	C:\Users\thomas\Desktop
8KE4Q6-5561	C:\Users\thomas\Desktop\philly_2.pdf
8TBZD8-5562	Not in scope.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

WebCode Test	Response
8WNN47-5562	C:\Users\thomas\Desktop\philly_2.pdf
A444U7-5562	C:\Users\thomas\Desktop\philly_2.pdf
AEKNE3-5561	C:\Users\thomas\Desktop\philly_2.pdf
AFF7G6-5561	C:\Users\thomas\Desktop\philly_2.pdf
AUY2L3-5562	C:\Users\thomas\Desktop\philly_2.pdf
AXDN7Y-5561	C:\Users\thomas\Desktop\philly_2.pdf
B7LHX8-5561	C:\users\thomas\desktop\philly_2.pdf
B8ELJ2-5561	C:\Users\thomas\Desktop\philly_2.pdf
BEGRX4-5562	C:\Users\thomas\Desktop\philly_2.pdf
BTXP36-5562	users\thomas\desktop
CDHZN3-5561	C:\Users\thomas\Desktop\philly_2.pdf
CTEYRY-5562	C:\Users\thomas\Desktop\philly_2.pdf
CWHMF2-5561	C:\Users\thomas\Desktop
DB9AYY-5561	C:\Users\thomas\Desktop\philly_2.pdf
DJLBA2-5562	C:\Users\thomas\Desktop\philly_2.pdf
DPCKJZ-5561	C:\Users\thomas\Desktop\philly_2.pdf
E6FEQZ-5562	C:\Users\thomas\Desktop\philly_2.pdf
EYTN7P-5562	C:\Users\thomas\Desktop\philly_2.pdf
F4KDZ3-5562	C:/Users/thomas/Desktop/philly_2.pdf
FJ22JX-5562	C:\Users\thomas\Desktop\philly_2.pdf
FMYKLW-5561	C:\Users\thomas\Desktop\philly_2.pdf

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20 - Examination Questions	
WebCode Test	**Response**
GA6R7K-5561	25-5561-001.E01\Basic data partition (EFI 3)\Root\Users\thomas\AppData\Roaming\Microsoft\Windows\Recent\
GA8D2Z-5562	C:\Users\thomas\Desktop\philly_2.pdf
GJP4GX-5562	C:\Users\thomas\Desktop\philly_2.pdf
GPH4VT-5561	C:\Users\thomas\Desktop\philly_2.pdf
GQUT6W-5561	C:\Users\thomas\Desktop\philly_2.pdf
GTHERT-5562	C:\Users\thomas\Desktop\philly_2.pdf
GTZ73X-5562	C:\Users\thomas\Desktop\philly_2.pdf
HEX8ER-5562	C:\Users\thomas\Desktop\philly_2.pdf
HF9WVJ-5561	C:\Users\thomas\Desktop\philly_2.pdf
HFCE3U-5561	C:\Users\thomas\Desktop\philly_2.pdf
HXUD8T-5562	C:\Users\thomas\Desktop\philly_2.pdf
HYZ6QT-5562	C:\Users\thomas\Desktop\philly_2.pdf
J2L9YQ-5561	C:\Users\thomas\Desktop\philly_2.pdf
J7HNUT-5561	C:\Users\thomas\Desktop\philly_2.pdf
JGEWDV-5562	C:\Users\thomas\Desktop\philly_2.pdf
JYYMCV-5561	C:\Users\thomas\Desktop\philly_2.pdf
JZU7EW-5561	C:\Users\thomas\Desktop
K2HYQQ-5561	C:\Users\thomas\Desktop\philly_2.pdf
K7CZKT-5562	C:\Users\thomas\Desktop\philly_2.pdf
KA8UHU-5562	C:\Users\thomas\Desktop
KYBNNV-5562	The original path of philly_2.pdf was C:\Users\thomas\Desktop\philly_2.pdf.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

WebCode Test	Response
L7QRBN-5561	C:\Users\thomas\Desktop\philly_2.pdf
LACBFT-5562	C:\Users\thomas\Desktop\philly_2.pdf
LKDRCP-5561	C:\Users\thomas\Desktop\philly_2.pdf
LMYFNP-5561	C:\Users\thomas\Desktop\philly_2.pdf
LN7VWF-5562	25-5561-001.E01\Basic data partition (EFI 3)\Root\Users\thomas\AppData\Roaming\Microsoft\Windows\Recent\
LRRKGT-5562	C:\Users\thomas\Desktop\philly_2.pdf
LUECCW-5561	C:\Users\thomas\Desktop\philly_2.pdf
LYJAEX-5561	C:\Users\thomas\Desktop\philly_2.pdf
M2VAHU-5562	C:\Users\thomas\Desktop\philly_2.pdf
MD7R7R-5562	C:\Users\thomas\Desktop\philly_2.pdf
MGM8JP-5561	C:\Users\thomas\Desktop\philly_2.pdf
ML4AQV-5561	C:\Users\thomas\Desktop\philly_2.pdf
MQXA6Q-5562	C:\Users\thomas\Desktop\
MR7JXN-5561	C:\Users\thomas\Desktop\philiy_2.pdf
MRTR8R-5561	C:\Users\thomas\Desktop\philly_2.pdf
MV6VTN-5562	c:\users\thomas\Desktop\philly_2.pdf
NJQ8AP-5561	C:\Users\thomas\Desktop\philly_2.pdf
NK3WJT-5561	C:\Users\thomas\Desktop\philly_2.pdf
PAF6NN-5561	C:\Users\thomas\Desktop\philly_2.pdf
PPBH8Q-5561	C:\Users\thomas\Desktop\philly_2.pdf
PQH2LD-5561	C:\Users\thomas\Desktop\philly_2.pdf

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20 - Examination Questions	
WebCode Test	**Response**
PZAD6L-5561	C:\Users\thomas\Desktop\philly_2.pdf
Q2Z3GD-5562	C:\Users\thomas\Desktop\philly_2.pdf
QCLZQR-5562	C:\Users\thomas\Desktop\philly_2.pdf
QEMD4J-5561	C:\Users\thomas\Desktop\philly_2.pdf
QH4FBN-5562	C:\Users\thomas\Desktop\philly_2.pdf
QT7QQQ-5561	\Users\thomas\Desktop\philly_2.pdf
QWAN2J-5561	C:\Users\thomas\Desktop\philly_2.pdf
QYVDDJ-5561	C:\Users\thomas\Desktop\philly_2.pdf
R86XKL-5561	C:\Users\thomas\Desktop\philly_2.pdf
RBJUPN-5561	C:\Users\thomas\Desktop\philly_2.pdf
REKXEP-5561	C:\Users\thomas\Desktop\philly_2.pdf
RR9ZXG-5561	c:\Users\thomas\Desktop
T8JQPN-5562	C:\Users\thomas\Desktop\philly_2.pdf
T8LHLB-5561	C:\Users\thomas\Desktop\philly_2.pdf
TGQH3P-5561	C:\Users\thomas\Desktop\philly_2.pdf
THHLMJ-5562	C:\Users\thomas\Desktop\philly_2.pdf
TRHDUP-5562	C:\Users\thomas\Desktop
TVPPWK-5562	C:\Users\thomas\Desktop\philly_2.pdf
TZXUNK-5561	C:\Users\thomas\Desktop\philly_2.pdf
U3GARK-5562	C:\Users\thomas\Desktop\philly_2.pdf
U4CRUL-5562	C:\Users\thomas\Desktop\philly_2.pdf

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20 - Examination Questions	
WebCode Test	**Response**
UGJTDH-5561	C:\Users\thomas\Desktop\philly_2.pdf
UT9WBG-5562	C:\Users\thomas\Desktop\philly_2.pdf
V63DZH-5562	C:\Users\thomas\Desktop\philly_2.pdf
VJJLKL-5562	C:\Users\thomas\Desktop\philly_2.pdf
VLV2EM-5561	C:\Users\thomas\Desktop\philly_2.pdf
VYH7LJ-5561	C:\Users\thomas\Desktop\philly_2.pdf
W7CX8H-5562	C:\Users\thomas\Desktop\philly_2.pdf
W9FNCC-5561	C:\Users\thomas\Desktop\philly_2.pdf
WH87QK-5562	C:\Users\thomas\Desktop\philly_2.pdf
WKE9TJ-5562	C:\Users\thomas\Desktop\philly_2.pdf
WRVWDD-5561	C:\Users\thomas\Desktop\philly_2.pdf
WVD7FJ-5562	C:\Users\thomas\Desktop\philly_2.pdf
X9VFGE-5562	C:\Users\thomas\Desktop\philly_2.pdf
XDUKGE-5562	C:\Users\thomas\Desktop\philly_2.pdf
XFRBFD-5561	C:\Users\thomas\Desktop\philly_2.pdf
XGRD6G-5562	C:\Users\thomas\Desktop\philly_2.pdf
XMC987-5562	C:\Users\thomas\Desktop\philly_2.pdf
XY6VCG-5562	C:\Users\thomas\Desktop\philly_2.pdf
Y36EXF-5561	C:\Users\thomas\Desktop\philly_2.pdf
YVMR6B-5561	C:\Users\thomas\Desktop\philly_2.pdf
YVR6WD-5561	C:\Users\thomas\Desktop\philly_2.pdf

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20 - Examination Questions	
WebCode Test	**Response**
Z8XMWF-5562	C:\Users\thomas\Desktop\philly_2.pdf
ZBE3BE-5561	C:\Users\thomas\Desktop\philly_2.pdf
ZNK3ZC-5562	C:\Users\thomas\Desktop\philly_2.pdf
ZRL9H3-5562	C:\Users\thomas\Desktop\
ZZUWEA-5562	C:\Users\thomas\Desktop\

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20 - Examination Questions

Question 20: Provide the original (pre-deletion) path of philly_2.pdf.

<u>Consensus Result:</u>

C:\Users\thomas\Desktop\philly_2.pdf

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

Every user on a Windows system has a folder in C:\$Recycle.Bin named with their Security Identifier, or SID. Within that folder are a pair of files for each recycled file. One, beginning with $I, which contains the metadata for the recycled file including its pre-deletion path and name, and another, beginning with $R, containing the file's content. philly_2.pdf is currently in
C : \$Recycle.Bin\S-1-5-21-3142915031-3623484693-281401572-1001\$R9S0XCM.pdf.

Its Recycle Bin companion $I file, C: \$Recycle.Bin\S-1-5-21-3142915031-3623484693-281401572-1001\ $I9S0XCM.pdf contains the original path C:\Users\thomas\Desktop\philly_2.pdf.

<u>Manufacturer's Response Illustration:</u>
X-Ways view of C:\$Recycle.BIN\$I9S0XCM.pdf

\$Recycle.Bin\S-1-5-21-3142915031-3623484693-281401572-1001	
Name ▲	Created
.. = $Recycle.Bin (18)	05/06/2022 22:24:50 -7
. = S-1-5-21-3142915031-3623484693-281401572-1001 (17)	02/17/2025 10:09:18 -7
$RLNEAC9 (12)	02/22/2025 10:55:14 -7
$I9S0XCM.pdf	03/02/2025 10:01:15 -7
$I9SPQGE.lnk	03/02/2025 10:01:20 -7
$R9S0XCM.pdf [philly_2.pdf]	03/02/2025 10:00:16 -7
$R9SPQGE.lnk [Microsoft Edge.lnk]	02/17/2025 10:08:04 -7
desktop.ini	02/17/2025 10:09:18 -7

— Partition   File   Preview   + Details   Gallery   Calendar

Size: 736 KB
Moved to recycle bin: 03/02/2025 10:01:15 -7
C:\Users\thomas\Desktop\philly_2.pdf

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21 - Examination Questions

Question 21: When was C:\Users\thomas\Desktop\Microsoft Edge.lnk deleted? Provide date and time with offset of device configured local time, using the date/time (24-hour) picker which presents the date/time in the following format: YYYY-MM-DD HH:MM.

Manufacturer's Response: 2025-03-02 10:01

WebCode Test	Response
24VY4B-5561	2025-03-02 10:01
24WLMH-5561	2025-03-02 10:01
2RG9U9-5562	2025-03-02 10:01
2U4TZC-5561	2025-03-02 10:01
349ZFC-5562	2025-03-02 10:01
3BYPCG-5561	2025-03-02 10:01
3GDA68-5561	2025-03-02 10:01
3J4DXE-5562	2025-02-03 10:01
3PA7TA-5561	2025-03-02 10:01
4FFFK9-5561	2025-03-02 10:01
4RN848-5561	2025-03-02 10:01
4ZJ2KE-5562	2025-03-02 10:01
63LLN6-5561	2025-03-02 10:01
673VQB-5562	2025-03-02 10:01
6PJ238-5561	2025-03-02 10:01
7CQT46-5561	2025-03-02 10:01
7PVVH8-5561	2025-03-02 10:01
8FPDKA-5562	2025-03-02 10:01
8KE4Q6-5561	2025-03-02 10:01

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21 - Examination Questions	
WebCode Test	**Response**
8TBZD8-5562	Not in scope.
8WNN47-5562	2025-03-02 10:01
A444U7-5562	2025-03-02 10:01
AEKNE3-5561	2025-03-02 10:01
AFF7G6-5561	2025-03-02 10:01
AUY2L3-5562	2025-03-02 10:01
AXDN7Y-5561	2025-03-02 10:01
B7LHX8-5561	2025-03-02 10:01
B8ELJ2-5561	2025-03-03 00:01
BEGRX4-5562	2025-03-02 10:01
BTXP36-5562	2025-03-02 05:01
CDHZN3-5561	2025-03-02 10:01
CTEYRY-5562	2025-03-02 10:01
CWHMF2-5561	2025-03-02 10:01
DB9AYY-5561	2025-03-02 10:01
DJLBA2-5562	2025-03-02 10:01
DPCKJZ-5561	2025-03-02 10:01
E6FEQZ-5562	2025-03-02 10:01
EYTN7P-5562	2025-03-02 10:01
F4KDZ3-5562	2025-03-02 11:01
FJ22JX-5562	2025-03-02 10:01

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21 - Examination Questions	
WebCode Test	**Response**
FMYKLW-5561	2025-03-02 10:01
GA6R7K-5561	2025-02-23 19:21
GA8D2Z-5562	2025-03-02 10:01
GJP4GX-5562	2025-03-02 10:01
GPH4VT-5561	2025-03-02 10:01
GQUT6W-5561	2025-03-02 10:01
GTHERT-5562	2025-03-02 10:01
GTZ73X-5562	2025-03-02 10:01
HEX8ER-5562	2025-03-02 10:01
HF9WVJ-5561	2025-03-02 10:01
HFCE3U-5561	2025-03-02 10:01
HXUD8T-5562	2025-03-02 10:01
HYZ6QT-5562	2025-03-02 10:01
J2L9YQ-5561	2025-03-02 10:01
J7HNUT-5561	2025-03-02 10:01
JGEWDV-5562	2025-03-02 10:01
JYYMCV-5561	2025-03-02 10:01
JZU7EW-5561	2025-03-02 10:01
K2HYQQ-5561	2025-03-02 10:01
K7CZKT-5562	2025-03-02 10:01
KA8UHU-5562	2025-03-02 10:01

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21 - Examination Questions	
WebCode Test	**Response**
KYBNNV-5562	2025-03-02 10:01
L7QRBN-5561	2025-03-02 10:01
LACBFT-5562	2025-03-02 10:01
LKDRCP-5561	2025-03-02 10:01
LMYFNP-5561	2025-03-02 10:01
LN7VWF-5562	[Participant did not return results for this question.]
LRRKGT-5562	2025-03-02 10:01
LUECCW-5561	2025-03-02 10:01
LYJAEX-5561	2025-03-02 10:01
M2VAHU-5562	2025-03-02 10:01
MD7R7R-5562	2025-03-02 10:01
MGM8JP-5561	2025-03-02 10:01
ML4AQV-5561	2025-03-02 10:01
MQXA6Q-5562	2025-03-02 10:01
MR7JXN-5561	2025-03-02 10:01
MRTR8R-5561	2025-03-02 10:01
MV6VTN-5562	2025-03-02 17:01
NJQ8AP-5561	2025-03-02 10:01
NK3WJT-5561	2025-03-02 10:01
PAF6NN-5561	2025-03-02 10:01
PPBH8Q-5561	2025-03-02 10:01

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21 - Examination Questions	
WebCode Test	**Response**
PQH2LD-5561	2025-03-02 10:01
PZAD6L-5561	2025-03-02 10:01
Q2Z3GD-5562	2025-03-02 10:01
QCLZQR-5562	2025-03-02 10:01
QEMD4J-5561	2025-03-02 10:01
QH4FBN-5562	2025-03-02 10:01
QT7QQQ-5561	2025-03-02 10:01
QWAN2J-5561	2025-03-02 10:01
QYVDDJ-5561	2025-03-02 10:01
R86XKL-5561	2025-03-02 10:01
RBJUPN-5561	2025-03-02 10:01
REKXEP-5561	2025-03-02 10:01
RR9ZXG-5561	2025-03-02 10:01
T8JQPN-5562	2025-02-17 17:08
T8LHLB-5561	2025-03-02 10:01
TGQH3P-5561	2025-03-02 10:01
THHLMJ-5562	2025-03-02 10:01
TRHDUP-5562	2025-03-02 10:01 (UTC -7)
TVPPWK-5562	2025-03-02 10:01
TZXUNK-5561	2025-03-02 10:01
U3GARK-5562	2025-03-02 10:01

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21 - Examination Questions	
WebCode Test	**Response**
U4CRUL-5562	2025-03-02 10:01
UGJTDH-5561	2025-03-02 10:01
UT9WBG-5562	2025-03-02 10:01
V63DZH-5562	2025-03-02 10:01
VJJLKL-5562	2025-03-02 10:01
VLV2EM-5561	2025-03-02 10:01
VYH7LJ-5561	2025-03-02 10:01
W7CX8H-5562	2025-03-02 10:01
W9FNCC-5561	2025-03-02 10:01
WH87QK-5562	2025-03-02 10:01
WKE9TJ-5562	2025-03-02 10:01
WRVWDD-5561	2025-03-02 10:01
WVD7FJ-5562	2025-03-02 17:01
X9VFGE-5562	2025-02-24 07:18
XDUKGE-5562	2025-03-02 10:01
XFRBFD-5561	2025-03-02 10:01
XGRD6G-5562	2025-02-03 10:01
XMC987-5562	2025-03-02 17:01
XY6VCG-5562	2025-03-02 10:01
Y36EXF-5561	2025-03-02 10:01
YVMR6B-5561	2025-03-02 10:01

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21 - Examination Questions	
WebCode Test	**Response**
YVR6WD-5561	2025-03-02 10:01
Z8XMWF-5562	2025-03-02 10:01
ZBE3BE-5561	2025-03-02 10:01
ZNK3ZC-5562	2025-03-02 10:01
ZRL9H3-5562	2025-03-02 17:01
ZZUWEA-5562	2025-03-02 10:01

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21 - Examination Questions

Question 21: When was C:\Users\thomas\Desktop\Microsoft Edge.lnk deleted? Provide date and time with offset of device configured local time, using the date/time (24-hour) picker which presents the date/time in the following format: YYYY-MM-DD HH:MM.

<u>Consensus Result:</u>

2025-03-02 10:01

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

Every user on a Windows system has a folder in C:\$Recycle.Bin named with their Security Identifier, or SID. Within that folder are a pair of files for each recycled file. One, beginning with $I, which contains the metadata for the recycled file including its pre-deletion path and name, and another, beginning with $R, containing the file's content. The created date of these files indicates the date they were deleted.

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

X-Ways view of C:\$Recycle.BIN\$I9SPQGE.lnk

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22 - Examination Questions

Question 22: Provide the cross-streets for the closest intersection to the GPS coordinates embedded in the photograph taken with an Olympus Stylus 1 digital camera.

<u>Manufacturer's</u> Woodshire Dr. and Gentry Dr.
<u>Response:</u>

WebCode Test	Response
24VY4B-5561	Woodshire Dr. and Gentry Dr.
24WLMH-5561	Woodshire Dr and Gentry Dr
2RG9U9-5562	Gentry Drive and Woodshire Drive
2U4TZC-5561	39.0261, -77.406
349ZFC-5562	Woodshire Dr and Gentry Dr
3BYPCG-5561	Woodshire Dr and Gentry Dr
3GDA68-5561	Woodshire Dr. and Gentry Dr.
3J4DXE-5562	Woodshire Dr, Gentry Dr
3PA7TA-5561	Woodshire Dr and Gentry Dr
4FFFK9-5561	Gentry Dr. & Woodshire Dr.
4RN848-5561	21331 Gentry Dr, Sterling, VA 20166, United States, intersect with Woodshire Dr street; 2HGV+CJJ Dulles Town Center, Virginia, USA
4ZJ2KE-5562	Woodshire Drive / Gentry Drive
63LLN6-5561	Woodshire Dr / Gentry Dr
673VQB-5562	Gentry Dr & Woodshire Dr
6PJ238-5561	N 39.0261238, W 77.4055602 – crossstreets (Woodshire DR.-Gentry Dr.)
7CQT46-5561	Gentry Dr/Woodshire Dr
7PVVH8-5561	Woodshire Dr, Gentry Dr
8FPDKA-5562	Gentry and Woodshire
8KE4Q6-5561	Woodshire Dr and Gentry Dr

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

WebCode Test	Response
8TBZD8-5562	Woodshire Dr, Gentry Dr
8WNN47-5562	Woodshire Drive, Gentry Drive
A444U7-5562	Woodshire Dr / Gentry Dr
AEKNE3-5561	Woodshire Dr, Gentry Dr
AFF7G6-5561	Woodshire Drive / Gentry Drive
AUY2L3-5562	Woodshire Drive and Gentry Drive
AXDN7Y-5561	Woodshire Drive, Gentry Drive
B7LHX8-5561	WOODSHIRE Drive and Gentry Drive
B8ELJ2-5561	Gentry Drive
BEGRX4-5562	Woodshire Dr. \ Gentry Dr.
BTXP36-5562	Pulaski Highway and Loreley Road/Days Cove Road.
CDHZN3-5561	Woodshire Dr and Gentry Dr
CTEYRY-5562	Woodshire Dr and Gentry Dr
CWHMF2-5561	Woodshire Dr / Gentry Dr
DB9AYY-5561	Woodshire Dr and Gentry Dr
DJLBA2-5562	Gentry Drive and Woodshire Drive
DPCKJZ-5561	Woodshire Dr, Genty Dr
E6FEQZ-5562	Woodshire Drive and Gentry Drive
EYTN7P-5562	Woodshire Dr, Gentry Dr (Sterling – Virginia)
F4KDZ3-5562	Woodshire Drive and Gentry Drive
FJ22JX-5562	Woodshire Drive / Gentry Drive, Sterling, VA

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22 - Examination Questions	
WebCode Test	**Response**
FMYKLW-5561	Woodshire Dr. & Gentry Dr.
GA6R7K-5561	The Long and Lat show a Desert in China, however the image is of Brighton Pier.
GA8D2Z-5562	Woodshire Dr & Gentry Dr
GJP4GX-5562	Woodshire Drive & Gentry Drive
GPH4VT-5561	Woodshire Drive and Gentry Drive
GQUT6W-5561	Woodshire Drive / Gentry Drive
GTHERT-5562	Woodshire Drive and Gentry Drive
GTZ73X-5562	Gentry Dr., Woodshire Dr.
HEX8ER-5562	Woodshire Dr, Gentry Dr
HF9WVJ-5561	Woodshire Dr and Gentry Dr
HFCE3U-5561	Woodshire Drive and Gentry Drive
HXUD8T-5562	Gentry Dr
HYZ6QT-5562	Woodshire Dr & Gentry Dr
J2L9YQ-5561	Gentry Dr& Woodshire Dr
J7HNUT-5561	Gentry Drive and Woodshire Drive
JGEWDV-5562	Gentry Dr and Woodshire Dr
JYYMCV-5561	Woodshire Dr & Gentry Dr
JZU7EW-5561	Gentry Dr, Woodshire Dr
K2HYQQ-5561	Woodshire Drive, Gentry Drive
K7CZKT-5562	Woodshire Drive / Gentry Drive
KA8UHU-5562	Woodshire Dr. and Gentry Dr.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22 - Examination Questions	
WebCode Test	**Response**
KYBNNV-5562	The closest intersection to the provided GPS coordinates embedded in the photograph is Woodshire Road and Gentry Drive in Dulles Town Center, VA.
L7QRBN-5561	Woodshire Dr. & Gentry Dr.
LACBFT-5562	Gentry Dr, Woodshire Dr
LKDRCP-5561	Woodshire Dr, Gentry Dr
LMYFNP-5561	Woodshire Dr and Gentry Dr
LN7VWF-5562	The Long and Lat show a Desert in China, however the image is of Brighton Pier.
LRRKGT-5562	Woodshire Dr / Gentry Dr in Sterling Virginia
LUECCW-5561	Gentry Drive and Woodshire Drive
LYJAEX-5561	Loudoun County Parkway & George Washington Boulevard
M2VAHU-5562	Woodshire Drive and Gentry Drive
MD7R7R-5562	Woodshire Dr and Gentry Dr
MGM8JP-5561	* Not in scope of agency exam
ML4AQV-5561	Gentry Drive and Woodshire Drive
MQXA6Q-5562	Gentry Drive, Woodshire Drive
MR7JXN-5561	Woodshire Drive and Gentry Drive
MRTR8R-5561	Woodshire Dr / Gentry Dr
MV6VTN-5562	Woodshire Drive and Gentry Drive
NJQ8AP-5561	Gentry Dr and Woodshire Dr
NK3WJT-5561	Woodshire Dr and Gentry Dr
PAF6NN-5561	Woodshire Dr and Gentry Dr
PPBH8Q-5561	Woodshire Dr. and Gentry Dr.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22 - Examination Questions	
WebCode Test	**Response**
PQH2LD-5561	Woodshire Drive & Gentry Drive
PZAD6L-5561	Gentry Dr/Woodshire Dr
Q2Z3GD-5562	Woodshire Dr, Gentry Dr
QCLZQR-5562	Woodshire Dr and Gentry Dr
QEMD4J-5561	Gentry Dr and Woodshire Dr
QH4FBN-5562	Gentry & Woodshire
QT7QQQ-5561	Woodshire Drive and Gentry Drive
QWAN2J-5561	Gentry Drive & Woodshire Drive
QYVDDJ-5561	Woodshire Dr, Gentry Dr
R86XKL-5561	Woodshire Dr and Gentry Dr
RBJUPN-5561	Gentry Drive & Woodshire Drive
REKXEP-5561	Woodshire Drive and Gentry Drive
RR9ZXG-5561	Woodshire Dr. & Gentry Dr.
T8JQPN-5562	Woodshire Dr and Gentry Dr
T8LHLB-5561	Woodshire Drive and Gentrey Drive
TGQH3P-5561	Woodshire Dr / Gentry Dr
THHLMJ-5562	Woodshire Drive and Gentry Drive (Sterling Virginia)
TRHDUP-5562	Woodshire Dr. and Gentry Dr.
TVPPWK-5562	Woodshire Drive / Gentry Drive
TZXUNK-5561	Woodsire Dr.
U3GARK-5562	Nearest major cross street is a Round-a-bout. Streets are Old Steine, Marine Parade, Madeira Dr, and Kingsway (A259)

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22 - Examination Questions	
WebCode Test	**Response**
U4CRUL-5562	Woodshire Drive and Gentry Drive
UGJTDH-5561	Woodshire Dr and Gentry Dr, Dulles Town Center, Virginia
UT9WBG-5562	Woodshire Dr - Gentry Dr
V63DZH-5562	The closest intersection to the GPS coordinates (39.026072, -77.405972) is Woodshire Drive and Gentry Drive.
VJJLKL-5562	Woodshire Dr and Gentry Dr
VLV2EM-5561	MD 17 (Burkittsville Road) and MD 180 (Old Frederick Road)
VYH7LJ-5561	Gentry Dr and Woodshire Dr
W7CX8H-5562	Woodshire Drive / Gentry Drive
W9FNCC-5561	Woodshire Drive and Gentry Drive
WH87QK-5562	Woodshire Dr and Gentry Dr
WKE9TJ-5562	Woodshire Dr, Gentry Dr
WRVWDD-5561	Woodshire Dr / Gentry Dr
WVD7FJ-5562	Gentry Drive and Woodshire Drive
X9VFGE-5562	Woodshire Dr y Gentry Dr
XDUKGE-5562	Woodshire Drive and Cascades Parkway
XFRBFD-5561	Junction Woodshire Drive and Gentry Drive, Sterling Va
XGRD6G-5562	Woodshire Drive and Gentry Drive (Sterling, VA – Lat. 39.0261; Long. -77.406)
XMC987-5562	Woodshire drive + Gentry Drive
XY6VCG-5562	Gentry Drive and Woodshire Drive
Y36EXF-5561	Woodshire Dr and Gentry Dr
YVMR6B-5561	Woodshire Dr and Gentry Dr

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22 - Examination Questions	
WebCode Test	**Response**
YVR6WD-5561	Woodshire Dr and Gentry Dr
Z8XMWF-5562	Woodshire Drive & Gentry Drive
ZBE3BE-5561	Woodshire Drive and Gentry Drive
ZNK3ZC-5562	Woodshire Dr - Gentry Dr
ZRL9H3-5562	[Participant did not return results for this question.]
ZZUWEA-5562	Woodshire Drive & Gentry Drive

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22 - Examination Questions

Question 22: Provide the cross-streets for the closest intersection to the GPS coordinates embedded in the photograph taken with an Olympus Stylus 1 digital camera.

<u>Consensus Result:</u>

Woodshire Dr. and Gentry Dr.
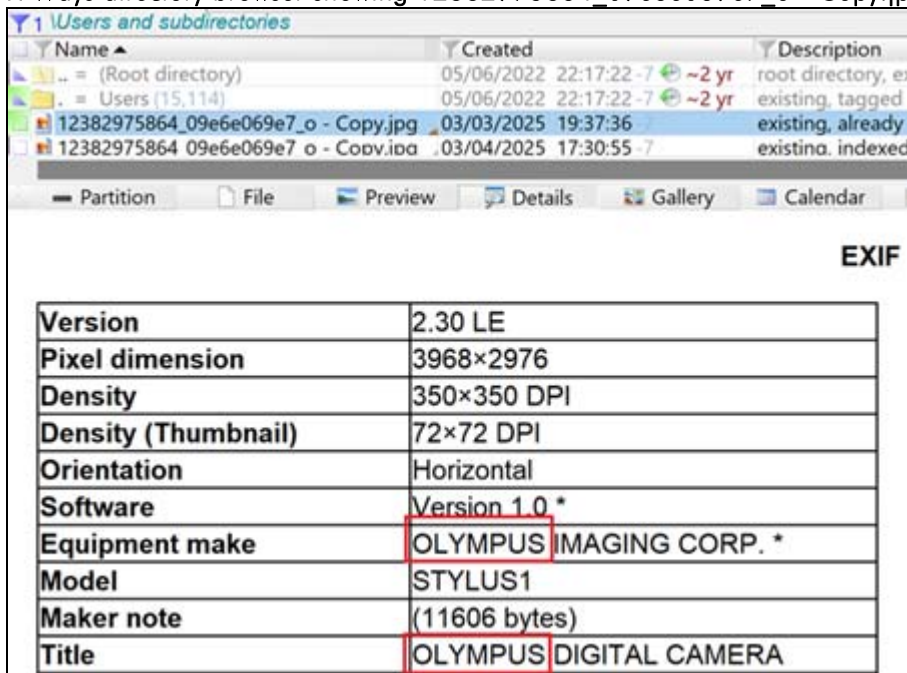
<u>Manufacturer's Response Explanation</u>:

Searching for "Olympus" within photo EXIF metadata will discover
C: \Users\thomas\OneDrive\12382975864_09e6e069e7_o - Copy.jpg. Review of the EXIF metadata within this file finds the following GPS coordinates: 39°01'33.9"N 77°24'21.5"W. Querying those coordinates in a mapping utility will discover the closest intersection.

<u>Manufacturer's Response Illustration:</u>
X-Ways directory browser showing 12382975864_09e6e069e7_o - Copy.jpg EXIF data

X-Ways directory browser showing 12382975864_09e6e069e7_o - Copy.jpg EXIF data

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22 - Examination Questions

Exiftool Parse of 12382975864_09e6e069e7_o - Copy.jpg location data

```
GPS Latitude : 39 deg 1' 33.86" N
GPS Longitude: 77 deg 24' 21.50" W
```

Google Maps view of 39°01'33.9"N 77°24'21.5"W
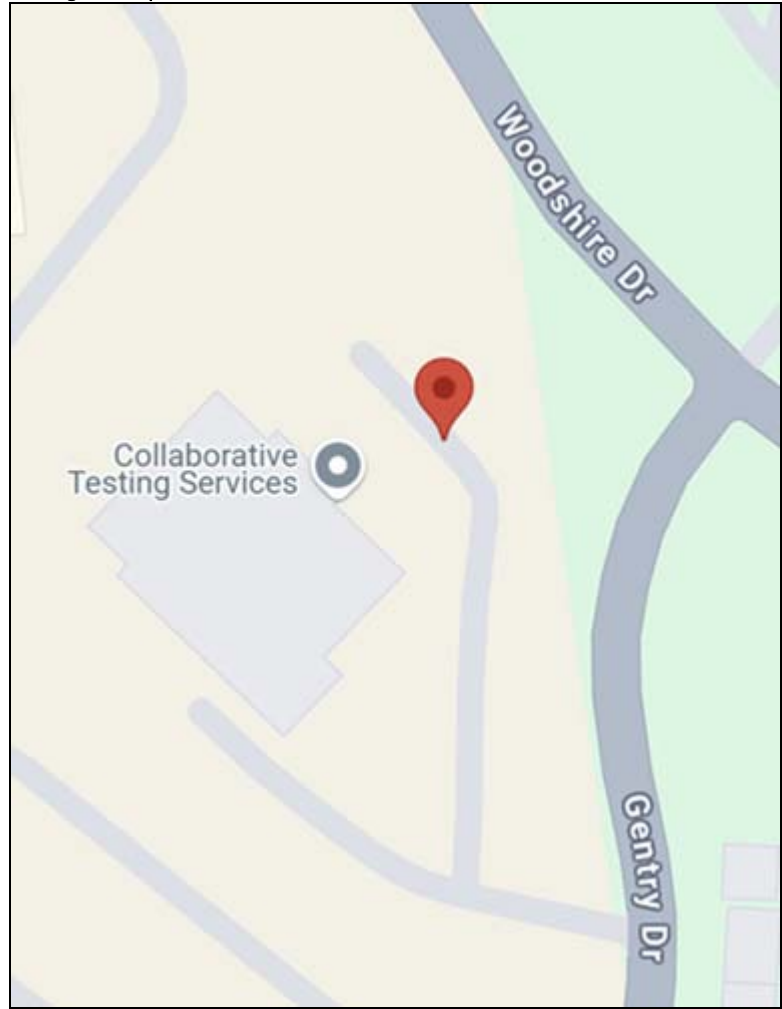
Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23 - Examination Questions

Question 23: Describe the contents of cat.xcf?

<u>Manufacturer's Response:</u> An image of an old cat "cougar.jpg", and a red bordered image of a kitten, "kitten.jpg"

WebCode Test	Response
24VY4B-5561	An image of what appears to be a cougar overlaying another image of what appears to be a kitten.
24WLMH-5561	image of mountain lion
2RG9U9-5562	This is a multilayer image of a large brown cat (Florida Panther or Eastern Cougar) and white/light brown kitten with a red border.
2U4TZC-5561	A picture of a puma
349ZFC-5562	Cougar
3BYPCG-5561	GIMP file with the image of a Cougar animal
3GDA68-5561	The system time was changed. Based on artifact UsnJrnl and Windows Event Logs/System Events
3J4DXE-5562	big cat - puma
3PA7TA-5561	The image contains two layers, one in the foreground labeled cougar and contained an image of a cougar. A second layer was labeled kitten and contained an image of a kitten.
4FFFK9-5561	Layered image consisting of two jpg images: cougar.jpg and kitten.jpg (depicting a cougar and a kitten, respectively)
4RN848-5561	First Image A large wild cat, most likely a cougar (also called mountain lion or puma). Close-up of the face, particularly the eyes and nose. Second Image: A light gray or cream-colored kitten with blue eyes. Lying on its back on a soft white textured surface (like a blanket), looking toward the camera with paws slightly raised. Surrounded by a thick red frame.
4ZJ2KE-5562	A picture of a cougar overlayed on a picture of a kitten
63LLN6-5561	GIMP file. Cougar with strange eyes and a kitten when filters are turned on/off.
673VQB-5562	Image of a Florida panther/cougar
6PJ238-5561	The image features a close-up of a puma or pantera (felidae family). Its face is prominently displayed, with sharp focus on its eyes, ears, and whiskers. The eyes appear cloudy.
7CQT46-5561	Its a picture of a cat looks like a lion possibly
7PVVH8-5561	2 still images layered. Couger.jpg showing an orange cougar with glossy eyes and kitten.jpg showing a grey kitten.
8FPDKA-5562	Mountain lion with creepy eyes
8KE4Q6-5561	This is a photo that contains two layers, the first layer is a picture of a cougar "cougar.jpg". The second layer is a picture of a kitten, "kitten.jpg".

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23 - Examination Questions	
WebCode Test	**Response**
8TBZD8-5562	"cat.xcf" contains two images in separate layers: "cougar.jpg" and "kitten.jpg"
8WNN47-5562	cougar
A444U7-5562	The .xcf file contains two layers. cougar.jpg y Kitten.jpg
AEKNE3-5561	Multilayer picture depicting a Cougar or Mountain Lion and a Kitten
AFF7G6-5561	Image of a cougar overlaid over another image of a kitten with a red border
AUY2L3-5562	Cougar
AXDN7Y-5561	The image shows a large feline, likely a cougar or mountain lion, with tawny brown fur, distinctive ears and strange eyes.
B7LHX8-5561	Cougar and kitten
B8ELJ2-5561	the picture of a cougar
BEGRX4-5562	GIMP photo editor native file format displaying or tracking the changes/r layers, colors being made to the image cougar.jpg (similar to a Photoshop PSD file)
BTXP36-5562	Picture of a cougar.
CDHZN3-5561	kitten.jpg and cougar.jpg
CTEYRY-5562	It's a project GIMP which contain two pictures: the first one "cougar.jpg" represent a Florida Panther, and the second one "kitten.jpg" represent a kitten.
CWHMF2-5561	Photo of a Cheetah with grey eyes, second layer has a kitten with red border
DB9AYY-5561	Close up image of a cougar
DJLBA2-5562	There are two JPGs in this file. cougar.jpg and kitten.jpg
DPCKJZ-5561	Two layer image of a picture of cougar and kitten
E6FEQZ-5562	an image of a cougar staring in the direction of a camera lens
EYTN7P-5562	Puma head with white eyes, blurred background
F4KDZ3-5562	The face of a mountain lion
FJ22JX-5562	This file contains two images a mountain lion and a kitten. Both images are stored as layers which can be viewed in GIMP.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23 - Examination Questions	
WebCode Test	**Response**
FMYKLW-5561	Picture of a mountain lion
GA6R7K-5561	it is a picture of a light coloured cat laying on its back. Its back legs are crossed and it is laying on a white carpet.
GA8D2Z-5562	It is a multi-layered image, with one layer being a kitten and the other being a cougar.
GJP4GX-5562	Mountain lion
GPH4VT-5561	The file cat.xcf contains a main image of a cougar in the foreground and another layer with kitten.jpg, which is partially hidden. The composition shows the cougar with a dark background and focus on its face
GQUT6W-5561	image of a kitten with a red border and a predatory cat
GTHERT-5562	Cougar and kitten
GTZ73X-5562	Picture of a Tiger/Large Cat
HEX8ER-5562	The file "cat.xcf" is a GIMP XCF file that contains two image layers. Both layers are visible and use the Normal blend mode. The top layer is named "Cougar.jpg," and the bottom layer is named "kitten.jpg."
HF9WVJ-5561	The file cat.xcf consists of two layers. The first layer, cougar.jpg, is a photo of a cougar staring straight ahead. The second layer, kitten.jpg, is a photo of a cat lying on a blanket. The layers are overlapped, and since the first layer is opaque, it covers the second layer, making it usually invisible.
HFCE3U-5561	File is an image file that contains two layers named: "cougar.jpg" and "kitten.jpg". When the user toggles the eye button in the layer tree the user can view the other images underneath the first one.
HXUD8T-5562	There are two overlapping layers: one is cougar.jpg and the other is kitten.jpg. When cougar.jpg is made invisible, kitten.jpg becomes visible.
HYZ6QT-5562	An XCF file containing two layers couger.jpg (a mountain lion with cloudy eyes) and kitten.jpg (a cat lying on its back)
J2L9YQ-5561	A picture of cougar
J7HNUT-5561	2 layer image. One is of a courgar with cloudy eyes and the other layer is of a kitten.
JGEWDV-5562	Blind cougar
JYYMCV-5561	It's a photo of a cougar (.jpg)
JZU7EW-5561	Cougar (first layer) and kitten (second layer)
K2HYQQ-5561	cougar and kitten
K7CZKT-5562	A picture of a kitten behind a picture of a cougar
KA8UHU-5562	This is a proprietary file used by the program Gimp; it is the edited version of a photograph file (possibly cougar.jpg) that depicts a cougar

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23 - Examination Questions	
WebCode Test	**Response**
KYBNNV-5562	When viewing the contents of cat.xcf in a hex editor, the file appears to be related to the image editing software GIMP. When I opened up cat.xcf in GIMP it appears to be a Mountain Lion.
L7QRBN-5561	A graphic of a mountain lion focused on the head. Gimp type of graphic file.
LACBFT-5562	Mountain lion
LKDRCP-5561	GIMP's XCF version 11 project file. The project contains the image, kitten.jpg
LMYFNP-5561	GIMP multilayer picture of a cougar (big cat) and kitten.
LN7VWF-5562	it is a picture of a light coloured cat laying on its back. Its back legs are crossed and it is laying on a white carpet.
LRRKGT-5562	The head of a female lion with glassy eyes
LUECCW-5561	A two-layer image consisting of Cougar.jpg and Kitten.jpg
LYJAEX-5561	it is a project file from photo editing and layering software, when I open this file, I see animal resembling a puma or lion in yellowish-brown tones with a face visible in the foreground and misty eyes.
M2VAHU-5562	The File contain two layers that has the file name cougar.jpg and kitten.jpg
MD7R7R-5562	Mountain lion with gray eyes
MGM8JP-5561	Image of cougar
ML4AQV-5561	Two layer image Cougar.jpg Kitten.jpg with red boarder.
MQXA6Q-5562	A Florida Panther or North American Cougar stalking his next meal off in the distance waiting for his chance to ponce and enjoy the fresh meat off them bones.
MR7JXN-5561	The file is a GNU Image Manipulation Program (GIMP) eXperimental Computing Facility (XCF) iimage file and contains two image files: couger.jpg which contains a picture of a cougar and kitten.jpg which contains a picture of a white kitten with a red boarder.
MRTR8R-5561	image of a cougar layered with an image of a kitten with a red border
MV6VTN-5562	Animal in picture appears to be a predatory feline, such as a Cougar. Noted original filename in GIMP image metadata to be 'cougar.jpg'.
NJQ8AP-5561	a photo of some type of large wildcat
NK3WJT-5561	cougar.jpg and kitten.jpg
PAF6NN-5561	Photo of a large cat
PPBH8Q-5561	Panther/Mountain Lion (interpretation is outside the scope of the lab)

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23 - Examination Questions	
WebCode Test	**Response**
PQH2LD-5561	The file named cat.xcf consists of two image layers in JPG format: the first layer, named 'cougar.jpg', features a cougar; the second layer, named 'kitten.jpg', depicts a kitten lying down.
PZAD6L-5561	A picture of the head and partial body of a wild cat, possibly a panther
Q2Z3GD-5562	Two layers, top one is a picture of a cougar. Behind it a kitten playing with a string.
QCLZQR-5562	A cougar
QEMD4J-5561	A large predator cat with a yellow box around its head. Further invesitigation found that there was a second layer (image) which shows a white kitten on its back.
QH4FBN-5562	A mountain lion/cougar/puma or whatever your preference is to describe the large cat native to the Americas; the animal appears to be blind judging by the clouded appearance of the eyes and the absence of an iris/pupil; the eyes themselves are a mix of blue/gray/green; the picture is a closeup of the animals face and was taken with a very high quality camera judging by the fact that individual whiskers can be easily identified and enumerated; the animals ears are perked up as if in response to something, perhaps the reacting to the sound of the cameraman's lens opening and closing, which might be disturbing the the cat as, again, it appears to be blind; the wrinkles atop the head may also indicate a feeling of concern for the animal. I don't know, that might be a stretch, all I know is that my forehead tends to wrinkle like that when I get concerned. I hope this sufficiently answers the "describe the contents" question, and if this was more than you needed, maybe ask something simpler like "What is pictured here?"
QT7QQQ-5561	Image of gray and white kitten laying on back. Red rectangle around photo.
QWAN2J-5561	picture of a mountain lion and a separate picture of cat behind it (used GIMP software to open)
QYVDDJ-5561	2 pictures, one is cougar.jpg,the other one is kitten.jpg.
R86XKL-5561	It is a picture of a Cougar
RBJUPN-5561	GIMP layered image of a mountain lion and kitten with file names "kitten.jpg" and "cougar.jpg"
REKXEP-5561	Cat.xcf depicts a large tan in color cat, visually similar to a Florida panther or a cougar. The eyes of the cat appear hazy. The image resembles one posted by user Caleb Falkenhagen on the site pexels, titled 'Cougar in Close Up.'
RR9ZXG-5561	Mountain lion
T8JQPN-5562	A tiger
T8LHLB-5561	The file contains two images, cougar.jpg and kitten.jpg, overlapping. The GIMP application is used for photoshopping images and other media.
TGQH3P-5561	A Picture of a big Cat. (cougar) and Kitten lay down
THHLMJ-5562	An image of a big cat (possibly a cougar /mountain lion.) It has tawny/brown fur, white fur around the mouth and eyes and large rounded ears.
TRHDUP-5562	Cat\Cougar with clouded eyes

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23 - Examination Questions	
WebCode Test	**Response**
TVPPWK-5562	GIMP files containing two layers, one with a cougar and another with a kitten with a red border.
TZXUNK-5561	There are two files with the extension .jpg. The file named kiiten.jpg is hidden in another file named cougar.jpg
U3GARK-5562	Gimp file: Cougar.jpg layered on top of kitten.jpg
U4CRUL-5562	XCF is the native file format for an image editing program, which is similar to Photoshop, called GIMP. The file stores all data related to an image, its layers, channels, paths, transparency, and guides which allows for non-destructive editing. Specifically in this file, there is reference to cougar.jpg and kitten.jpg within the hex code.
UGJTDH-5561	two layer GIMP image, one layer is labeled "cougar" with a picture of a cougar/mountain lion type wild feline, the other layer is a picture of a kitten on it's back with a red border around the image
UT9WBG-5562	An image of a big cat with strangers eyes.
V63DZH-5562	The file cat.xcf is a GIMP image file, as indicated by its MIME type image/x-xcf.
VJJLKL-5562	A cougar's face
VLV2EM-5561	there are two layers kitten and cougar
VYH7LJ-5561	it is a picture of a mountain lion
W7CX8H-5562	A GIMP image containing two layers: cougar.jpg (a photo of a cougar) and kitten.jpg (a photo of a kitten)
W9FNCC-5561	Cougar or Puma
WH87QK-5562	A cougar
WKE9TJ-5562	The cat.xcf file contains a "cougar.jpg" picture overlayed on a "kitten.jpg" picture
WRVWDD-5561	It is a picture of a mountain lion with foggy eyes that is overlayed on picture of a kitten with a red border.
WVD7FJ-5562	gimp file
X9VFGE-5562	It seems to be an illustration of a wild animal (Puma).
XDUKGE-5562	The file contains two images layered on each other. On the bottom is an image of kitten on a rug (kitten.jpg) and on the top is a close-up photograph of a cougar's head (cougar.jpg).
XFRBFD-5561	A close-up image of a cougar
XGRD6G-5562	Florida Panther / cougar
XMC987-5562	Source file: Windows.db Source file size:15.6 MB Name: cat.xcf Full path: C:\Users\thomas\Pictures\cat.xcf Type: . xcf Size: 50.1 MB Folder: Pictures

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23 - Examination Questions	
WebCode Test	**Response**
XY6VCG-5562	cat.xcf is a image file where the first and third pages are of what appears to be a mountain lion. The second page is of a cat surrounded by a red border.
Y36EXF-5561	Photograph of a cougar, close-up of its face.
YVMR6B-5561	A layered image in GIMP file format. Cougar.jpg and Kitten.jpg. kitten.jpg has a red border which is common to simulate CSAM in a training environment.
YVR6WD-5561	a layered image with a big cat on one layer and a small cat on the other layer
Z8XMWF-5562	A picture of a cougar.
ZBE3BE-5561	Close up photo of a cougar.
ZNK3ZC-5562	A multi-layered image file with a kitten picture with a red frame in the background and a cougar picture in the foreground.
ZRL9H3-5562	[Participant did not return results for this question.]
ZZUWEA-5562	It contains an image of a lioness, created by the jpg's of 'cougar' and kitten'

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23 - Examination Questions

Question 23: Describe the contents of cat.xcf?

<u>Consensus Result:</u>

An image of an old cat "cougar.jpg", and a red bordered image of a kitten, "kitten.jpg"

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

cat.xcf is a GIMP image file. GIMP, The GNU Image Manipulation Program, is a free and open-source photo editing application like Photoshop. Opening the file with its associated application allows viewing its contents, two images, stacked in layers. one layer containing an image of an old cat, "cougar.jpg", and one layer containing a red bordered image of a kitten, "kitten.jpg".

<u>Manufacturer's Response Illustration:</u>
GIMP: cat.xcf
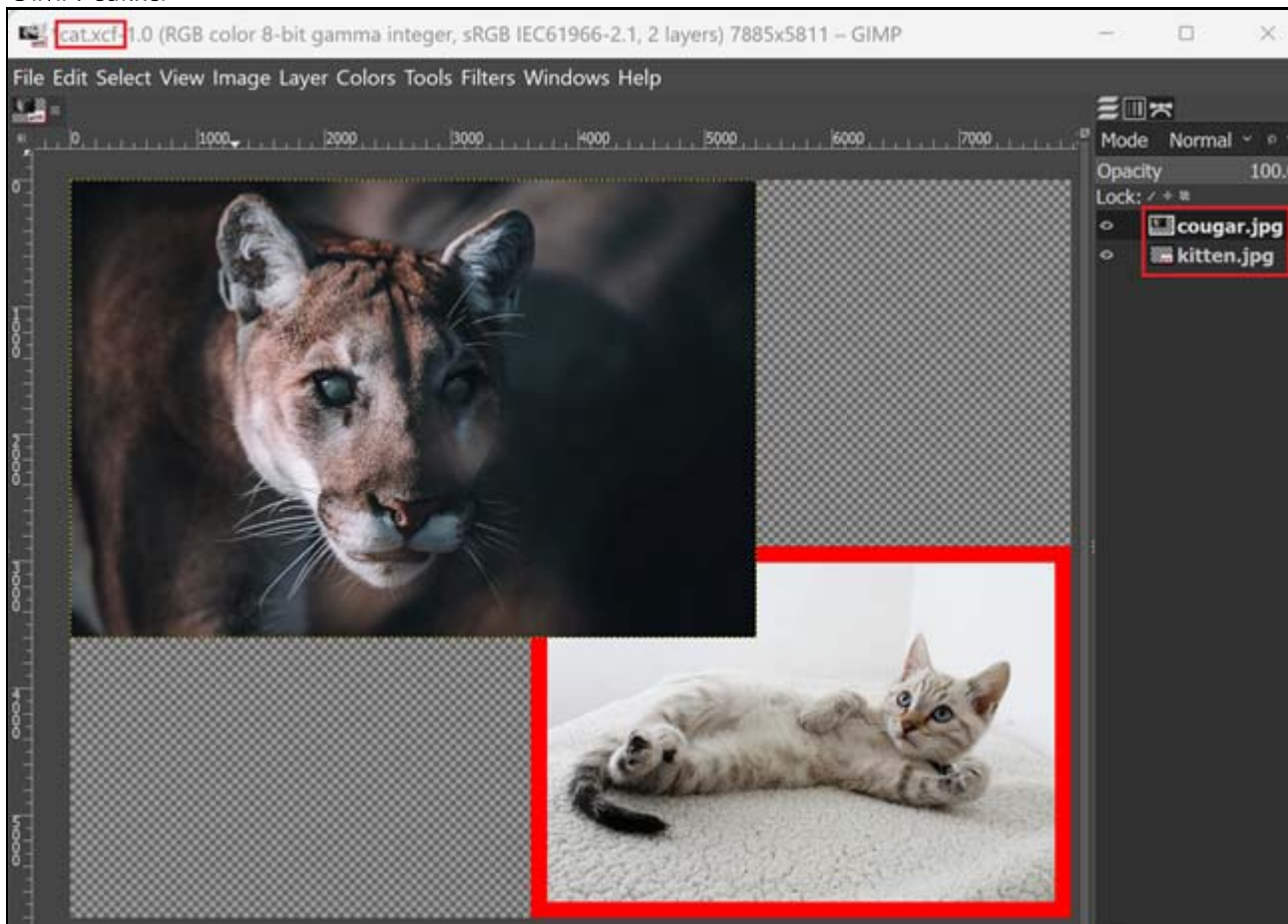
Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions

Question 24: Find the file containing the string "realestateagent" where each of the vowels have been replaced with one of the following characters ~!@#$%^&*(). Provide the PATH and FILENAME, and the RESULTANT STRING.

<u>Manufacturer's</u> Path & Filename: C: \Users\thomas\Documents\Realestateagent.txt
<u>Response:</u>　　　　Resultant string: r~@l#st@t#&g*nt

WebCode Test	Response
24VY4B-5561	Realestateagent.txt, C:\Users\thomas\Documents\Realestateagent.txt Resultant string: r~@l#st@t#&g*nt
24WLMH-5561	Users/thomas/Documents/Realestateagent.txt Resultant string: r~@l#st@t#&g*nt
2RG9U9-5562	PATH = \Users\thomas\Documents\ FILENAME = Realestateagent.txt RESULTANT STRING = r~@l#st@t#&g*nt
2U4TZC-5561	C\Users\thomas\Documents\Realestateagent.txt. Realestateagent
349ZFC-5562	r~@l#st@t#&g*nt
3BYPCG-5561	PATH: C:/Users/thomas/Documents/ FILENAME: Realestateagent.txt STRING: r~@l#st@t#&g*nt
3GDA68-5561	Users\thomas\Documents\Realestateagent.txt Resultant string: r~@l#st@t#&g*nt
3J4DXE-5562	PATH: Partition 3\Users\thomas\Documents\Realestateagent.txt, FILENAME: Realestateagent.txt, RESULTANT STRING: r~@l#st@t#&g*nt
3PA7TA-5561	C\Users\thomas\Documents\Realestateagent.txt, Resultant string: r~@l#st@t#&g*nt
4FFFK9-5561	PATH: \Users\thomas\Documents FILENAME: Realestateagent.txt STRING: r~@l#st@t#&g*nt
4RN848-5561	Path is: Users\thomas\Documents\Realestateagent.txt and RESULTANT STRING is: r~@l#st@t#&g*nt
4ZJ2KE-5562	Path & filename: Partition 3/NONAME [NTFS]/[root]/Users/thomas/Documents/Realestateagent.txt ; Resultant string: r~@l#st@t#&g*nt
63LLN6-5561	Users\thomas\Documents\ Realestateagent.txt Resultant string: r~@l#st@t#&g*nt
673VQB-5562	C:\Users\thomas\Documents\Realestateagent.txt; Resultant string: r~@l#st@t#&g*nt
6PJ238-5561	Path- Partition3(C):\\Users\thomas\Documents; Filename- Realestateagent.txt; Resultant String- r~@l#st@t#&g*nt
7CQT46-5561	Users\thomas\Documents\Realestateagent.txt, Resultant string: r~@l#st@t#&g*nt
7PVVH8-5561	File Path: \Users\thomas\Documents\Realestateagent.txt - String: r~@l#st@t#&g*nt

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions	
WebCode Test	**Response**
8FPDKA-5562	\Users\thomas\Documents\Realestateagent.txt; Resultant string: r~@l#st@t#&g*nt
8KE4Q6-5561	\Users\thomas\Documents\Realestateagent.txt String: "r~@l#st@t#&g*nt"
8TBZD8-5562	Not in scope.
8WNN47-5562	C\Users\thomas\Documents\Realestateagent.txt, Realestateagent.txt, Resultant string: r~@l#st@t#&g*nt
A444U7-5562	Users\thomas\Documents\Realestateagent.txt Resultant string: rOdlPst\t:egTnt
AEKNE3-5561	C:\Users\thomas\Documents\Realestateagent.txt, Resultant string: r~@l#st@t#&g*nt
AFF7G6-5561	\root\Users\thomas\Documents\Realestateagent.txt, Resultant string: r~@l#st@t#&g*nt
AUY2L3-5562	PATH: Users\thomas\Documents\Realestateagent.txt FILENAME: Realestateagent.txt RESULTANT STRING: r~@l#st@t#&g*nt
AXDN7Y-5561	PATH: Users\thomas\Documents\Realestateagent.txt, FileName: Realestateagent.txt, RESULTANT STRING: r~@l#st@t#&g*nt
B7LHX8-5561	users\thomas\documents\realestateagent.txt
B8ELJ2-5561	C:\Users\thomas\Documents\Realestateagent.txt; Resultant string: r~@l#st@t#&g*nt
BEGRX4-5562	Resultant string: r~@l#st@t#&g*nt
BTXP36-5562	users\thomas\documents\realestateagent.txt
CDHZN3-5561	Basic data partition (3)/NONAME [NTFS]/[root]/Users/thomas/Documents/Realestateagent.txt Resultant string: r~@l#st@t#&g*nt
CTEYRY-5562	Path and filename: Partition 3\Users\thomas\Documents\Realestateagent.txt the resultant string: r~@l#st@t#&g*nt
CWHMF2-5561	C:\Users\thomas\Documents\ Realestateagent.txt Resultant string: r~@l#st@t#&g*nt
DB9AYY-5561	\Users\thomas\Documents\Realestateagent.txt Resultant string: r~@l#st@t#&g*nt
DJLBA2-5562	25-5561-001.E01/Basic data partition (3)/NONAME [NTFS]/ [root]/Users/thomas/Documents/Realestateagent.txt and Realestateagent.txt
DPCKJZ-5561	Users\thomas\Documents\Realestateagent.txt Resultant string: r@l!st#t%g ⌃ nt

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

WebCode Test	Response
E6FEQZ-5562	: Path: 25-5561-001.E01 - Partition 3 (Microsoft NTFS, 24.13 GB)\Users\thomas\Documents\Realestateagent.txt Filename: Realestateagent.txt Resultant string: r~@l#st@t#&g*nt
EYTN7P-5562	Path : C:\Users\thomas\Documents\Realestateagent.txt, Filename : Realestateagent.txt, Resultant string : r~@l#st@t#&g*nt
F4KDZ3-5562	/vol_vol6/Users/thomas/Documents/Realestateagent.txt FILENAME=Realestateagent.txt STRING= r~@l#st@t#&g*nt
FJ22JX-5562	25-5561-001.E01\Basic data partition (EFI 3)\Root\Users\thomas\Documents\Realestateagent.txt, Resultant string: r~@l#st@t#&g*nt
FMYKLW-5561	PATH/FILENAME: C:\Users\thomas\Documents\Realestateagent.txt RESULTANT STRING: r~@l#st@t#&g*nt
GA6R7K-5561	25-5561-001.E01\Basic data partition (EFI 3)\Root\Users\thomas\Documents\Realestateagent.txt
GA8D2Z-5562	\Users\thomas\Documents\Realestateagent.txt Resultant string: r~@l#st@t#&g*nt
GJP4GX-5562	Basic data partition (3)/NONAME [NTFS]/[root]/Users/thomas/Documents/Realestateagent.txt Resultant string: "r~@l#st@t#&g*nt"
GPH4VT-5561	PATH: C:\Users\thomas\Documents\Realestateagent.txt FILENAME: Realestateagent.txt RESULT STRING: r~@l#st@t#&g*nt
GQUT6W-5561	C:\Users\thomas\Documents\Realestateagent.txt; string: r~@l#st@t#&g*nt
GTHERT-5562	file name : Realestateagent.txt , Path: Users\thomas\Documents\Realestateagent.txt Resultant string: r~@l#st@t#&g*nt
GTZ73X-5562	C:\Users\thomas\Documents\Realestateagent.txt, Resultant string: r~@l#st@t#&g*nt
HEX8ER-5562	C:\Users\thomas\Documents\Realestateagent.txt , Realestateagent.txt , Resultant string: r~@l#st@t#&g*nt
HF9WVJ-5561	PATH: C:\Users\thomas\Documents\Realestateagent.txt | FILENAME: Realestateagent.txt | RESULTANT STRING: r~@l#st@t#&g*nt
HFCE3U-5561	Users\thomas\Documents\Realestateagent.txt, Resultant string: r~@l#st@t#&g*nt
HXUD8T-5562	C:\Users\thomas\Documents\Realestateagent.txt, Resultant string: r~@l#st@t#&g*nt
HYZ6QT-5562	Path: /Basic data partition (3)/NONAME [NTFS]/[root]/Users/thomas/Documents/Realestateagent.txt, File name: Realestateagent.txt, Resultant String: r~@l#st@t#&g*nt

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions	
WebCode Test	**Response**
J2L9YQ-5561	Path: 25-5561-001.E01 - Partition 3 (Microsoft NTFS, 24.13 GB)\Users\thomas\Documents\Realestateagent.txt; Filename: Realestateagent.txt; Resultant String: r~@l#st@t#&g*nt
J7HNUT-5561	25-5561-001.E01 - Partition 3 (Microsoft NTFS, 24.13 GB)\Users\thomas\Documents\Realestateagent.txt, Realestateagent.txt, Resultant string: r~@l#st@t#&g*nt
JGEWDV-5562	C:\Users\thomas\Documents\Realestateagent.txt | Resultant string: r~@l#st@t#&g*nt
JYYMCV-5561	C:\Users\thomas\Documents\Realestateagent.txt, Realestateagent.txt, Resultant string: r~@l#st@t#&g*nt
JZU7EW-5561	C:\Users\thomas\Documents\Realestateagent.txt Resultant string: r~@l#st@t#&g*nt
K2HYQQ-5561	\Users\thomas\Documents\Realestateagent.txt, Realestateagent.txt, Resultant string: r~@l#st@t#&g*nt
K7CZKT-5562	(3)/NONAME [NTFS]/[root]/Users/thomas/Documents/Realestateagent.txt Resultant string: (r~@l#st@t#&g*nt)
KA8UHU-5562	PATH: Users\thomas\Documents FILENAME: Realestateagent.txt RESULTANT STRING: r~@l#st@t#&g*nt
KYBNNV-5562	The path and file name of the of specific file is C:\Users\thomas\Documents\Realestateagent.txt and the resulting string is r~@l#st@t#&g*nt.
L7QRBN-5561	Users/thomas/Documents/Realestateagent.txt , Resultant string: r~@l#st@t#&g*nt
LACBFT-5562	\Users\thomas\Documents\Realestateagent.txt Resultant string: r~@l#st@t#&g*nt
LKDRCP-5561	C:\Users\thomas\Documents\Realestateagent.txt, Resultant string: r~@l#st@t#&g*nt
LMYFNP-5561	\Users\thomas\Documents\Realestateagent.txt, Resultant string: r~@l#st@t#&g*nt
LN7VWF-5562	25-5561-001.E01\Basic data partition (EFI 3)\Root\Users\thomas\Documents\Realestateagent.txt
LRRKGT-5562	Users\thomas\Documents\Realestateagent.txt
LUECCW-5561	\Users\thomas\Documents\Realestateagent.txt
LYJAEX-5561	PATH C/Users/thomas/Documents/Realestateagent.txt, FILENAME Realestateagent.txt, RESULTANT STRING r:glAstvtR6g^nt
M2VAHU-5562	Users\thomas\Documents\Realestateagent.txt and Realestateagent and Resultant string: the r~@l#st@t#&g*nt
MD7R7R-5562	\Users\thomas\Documents\Realestateagent.txt, Realestateagent.txt

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions	
WebCode Test	**Response**
MGM8JP-5561	* Not in scope of agency exam
ML4AQV-5561	\Users\thomas\Documents\Realestateagent.txt Resultant string: r~@l#st@t#&g*nt
MQXA6Q-5562	C:\Users\thomas\Documents\ and Realestateagent.txt, and Resultant string: r~@l#st@t#&g*nt
MR7JXN-5561	C:\Users\thomas\Documents\Realestateagent.txt ; Resultant string: r~@l#st@t#&g*nt
MRTR8R-5561	\root\Users\thomas\Documents\Realestateagent.txt Resultant string: r~@l#st@t#&g*nt
MV6VTN-5562	c:\users\thomas\Documents\Realestateagent.txt STRING: 'r~@l#st@t#&g*nt'
NJQ8AP-5561	C:\Users\thomas\Documents\Realestateagent.txt Resultant string: r~@l#st@t#&g*nt
NK3WJT-5561	C:\users\thomas\documents\realestateagent.txt Resultant string: r~@l#st@t#&g*nt
PAF6NN-5561	Path: C:\Users\thomas\Documents\Realestateagent.txt String: r~@l#st@t#&g*nt
PPBH8Q-5561	Path: 25-5561-001.E01/Basic data partition (3)/NONAME [NTFS]/ [root]/Users/thomas/Documents/Realestateagent.txt Filename: Realestateagent.txt Resultant string: r~@l#st@t#&g*nt
PQH2LD-5561	C\Users\thomas\Documents\Realestateagent.txt (PATH), Realestateagent.txt (FILENAME), r~@l#st@t#&g*nt (RESULTANT STRING)
PZAD6L-5561	C:\Users\thomas\Documents\Realestateagent.txt; Resultant string: r~@l#st@t#&g*nt
Q2Z3GD-5562	PATH and FILENAME: Users\thomas\Documents\Realestateagent.txt RESULTANT STRING: r~@l#st@t#&g*nt
QCLZQR-5562	Path: Partition 3 (Microsoft NTFS, 24.13 GB)\Users\thomas\Documents\Realestateagent.txt Filename: Realestateagent.txt String: r~@l#st@t#&g*nt
QEMD4J-5561	string is r~@l#st@t#&g*nt - path is \\Users\thomas\Documents\Realestateagent.txt
QH4FBN-5562	C:\Users\thomas\Documents\realestateagent.txt
QT7QQQ-5561	/img_25-5561-001.E01/vol_vol6/Users/thomas/Documents/Realestateagent.txt Resultant string: r~@l#st@t#&g*nt
QWAN2J-5561	The path/filename is Users\thomas\Documents\Realestateagent.txt Resultant string: r~@l#st@t#&g*nt
QYVDDJ-5561	PATH: C:\Users\thomas\Documents FILENAME: Realestateagent.txt RESULTANT STRING: r~@l#st@t#&g*nt

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions	
WebCode Test	**Response**
R86XKL-5561	C:\Users\thomas\Documents\Realestateagent.txt, Resultant string: r~@l#st@t#&g*nt
RBJUPN-5561	C:\Users\thomas\Documents\Realestateagent.txt, Resultant string: r~@l#st@t#&g*nt
REKXEP-5561	25-5561-001.E01 - Partition 3 (Microsoft NTFS, 24.13 GB)\Users\thomas\Documents\Realestateagent.txt, Resultant string: r~@l#st@t#&g*nt
RR9ZXG-5561	c:\Users\thomas\Documents\Realestateagent.txt
T8JQPN-5562	C:\Users\thomas\Documents\Realestateagent.txt ; Resultant string: r~@l#st@t#&g*nt
T8LHLB-5561	r~@l#st@t#&g*nt
TGQH3P-5561	25-5561-001.E01\Basic data partition (EFI 3)\Root\Users\thomas\Documents\Realestateagent.txt; Realestateagent.txt; r~@l#st@t#&g*nt
THHLMJ-5562	Path = \Users\thomas\Documents\Realestateagent.txt, Filename = Realestateagent.txt, esultant String = r~@l#st@t#&g*nt
TRHDUP-5562	\Users\thomas\Documents\Realestateagent.txt; RESULTANT STRING = r~@l#st@t#&g*nt
TVPPWK-5562	C:\Users\thomas\Documents\Realestateagent.txt, Resultant string: r~@l#st@t#&g*nt
TZXUNK-5561	Users\thomas\Documents\Realestateagent.txt
U3GARK-5562	(path C:\users\Thomas\Documents\Realestateagent.txt.) Resultant string: R~@l#st@t#&g*nt
U4CRUL-5562	Path: 25-5561-001.E01\Basic data partition (3)\NONAME [NTFS]\[root]\Users\thomas\Documents\Realestateagent.txt; Filename: Realestateagent.txt; Resultant String: r~@l#st@t#&g*nt
UGJTDH-5561	Filename: Realestateagent.txt ; Path: \Users\thomas\Documents\Realestateagent.txt Resultant String: r~@l#st@t#&g*nt
UT9WBG-5562	Path: Users\thomas\Documents\Realestateagent.txt / String: r~@l#st@t#&g*nt
V63DZH-5562	Path: Users\thomas\Documents\Realestateagent.txt Filename: Realestateagent.txt Resultant String: r:glAstvtR6g ⌃ nt
VJJLKL-5562	Path – Partition 3 (Microsoft NTFS, 24.13 GB)\Users\thomas\Documents\Realestateagent.txt or C:\ Users\thomas\Documents\Realestateagent.txt, Filename – Realestateagent.txt, Resultant String – r~@l#st@t#&g*nt
VLV2EM-5561	Users\thomas\Documents\Realestateagent.txt , Resultant string: r~@l#st@t#&g*nt

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions	
WebCode Test	**Response**
VYH7LJ-5561	PATH= C:\Users\thomas\Documents\Realestateagent.txt FILENAME= Realestateagent.txt RESULTANT STRING= r~@l#st@t#&g*nt
W7CX8H-5562	C:\Users\thomas\Documents\Realestateagent.txt, RESULTANT STRING: r~@l#st@t#&g*nt
W9FNCC-5561	25-5561-001.E01 - Partition 3 (Microsoft NTFS, 24.13 GB)\Users\thomas\Documents\, Realestateagent.txt, Resultant string: r~@l#st@t#&g*nt
WH87QK-5562	PATH: 25-5561-001.E01 - Partition 3 (Microsoft NTFS, 24.13 GB)\Users\thomas\Documents\Realestateagent.txt or C:\ Users\thomas\Documents\Realestateagent.txt, FILENAME: Realestateagent.txt, RESULTANT STRING: r~@l#st@t#&g*nt
WKE9TJ-5562	PATH and FILENAME: C:\Users\thomas\Documents\Realestateagent.txt; RESULTANT STRING: r~@l#st@t#&g*nt
WRVWDD-5561	\Users\thomas\Documents\Realestateagent.txt String - r~@l#st@t#&g*nt
WVD7FJ-5562	\Users\thomas\Documents\Realestateagent.txt , Realestateagent.txt, Resultant string: r~@l#st@t#&g*nt
X9VFGE-5562	thomas
XDUKGE-5562	PATH = C:\Users\thomas\Documents FILENAME = Realestateagent.txt RESULTANT STRING = r~@l#st@t#&g*nt
XFRBFD-5561	Path: \Users\thomas\Documents\ Filename: Realestateagent.txt Resultant String: r~@l#st@t#&g*nt
XGRD6G-5562	C:\Users\thomas\Documents\Realestateagent.txt; Resultant string: r~@l#st@t#&g*nt
XMC987-5562	ProgramData/Microsoft/Search/Data/Applications/Windows/Windows-gather.db
XY6VCG-5562	Users\thomas\Documents\Realestateagent.txt - String: r~@l#st@t#&g*nt
Y36EXF-5561	C:\Users\thomas\Documents\Realestateagent.txt, Realestateagent.txt, Resultant string: r~@l#st@t#&g*nt
YVMR6B-5561	\Users\thomas\Documents\Realestateagent.txt Resultant string: r~@l#st@t#&g*nt
YVR6WD-5561	\Users\thomas\Documents\Realestateagent.txt Resultant string: r~@l#st@t#&g*nt
Z8XMWF-5562	Realestateagent.txt, C:\Users\thomas\Documents\Realestateagent.txt
ZBE3BE-5561	C:\Users\thomas\Documents\Realestateagent.txt , Realestateagent.txt , Resultant string: r~@l#st@t#&g*nt

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions	
WebCode Test	**Response**
ZNK3ZC-5562	C:\Users\thomas\Documents\Realestateagent.txt Resultant string: r~@l#st@t#&g*nt
ZRL9H3-5562	Partition 3\Users\thomas\Documents\Realestateagent.txt
ZZUWEA-5562	Not sure

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions

Question 24: Find the file containing the string "realestateagent" where each of the vowels have been replaced with one of the following characters ~!@#$%^&*(). Provide the PATH and FILENAME, and the RESULTANT STRING.

<u>Consensus Result:</u>

Path & Filename: C: \Users\thomas\Documents\Realestateagent.txt
Resultant string: r~@l#st@t#&g*nt

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

Regular expressions are useful for searching for patterns and specific wildcards. Here, the set of special characters, ~!@#$%^&*() can be described by the expression [~!@\#$%^&*()].

Building the search term by replacing all the vowels in realestateagent yields, r[~!@\#$%^&*()][~!@\#$%^&*()]l[~!@\#$%^&*()]st[~!@\#$%^&*()]t[~!@\#$%^&*()][~!@\#$%^&*()]g[~!@\#$%^&*()]nt

Searching the media for this expression will discover the string, r~@l#st@t#&g*nt with the following path: C: \Users\thomas\Documents\Realestateagent.txt.

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

X-Ways search for r[~!@\#$%^&*()][~!@\#$%^&*()]l[~!@\#$%^&*()]st[~!@\#$%^&*()]t[~!@\#$%^&*()][~!@\#$%^&*()]g[~!@\#$%^&*()]nt
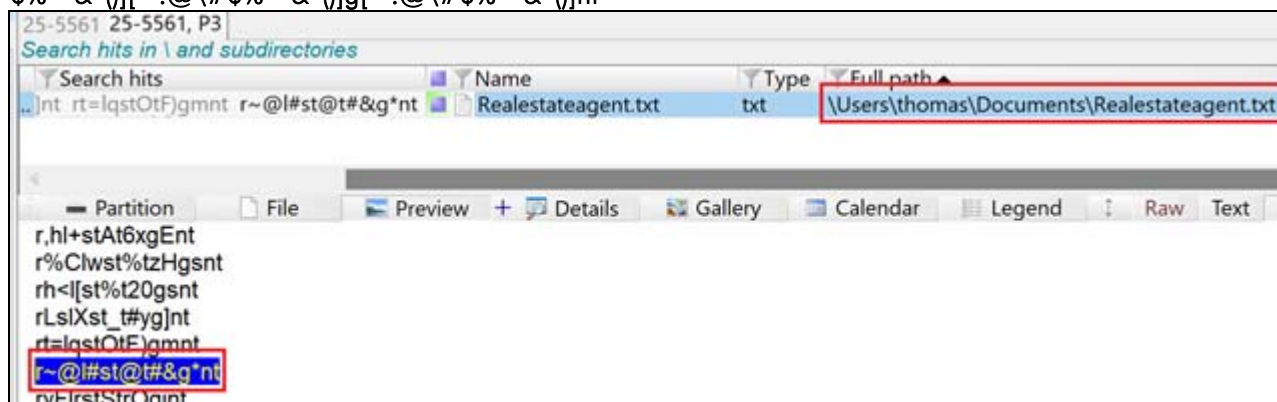
Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25 - Examination Questions

Question 25: In unallocated space on the subject volume is a photograph (picture file) of an alligator with a green border, containing white text beginning with "CTS", provide the complete text visible in the picture.

<u>Manufacturer's Response:</u> CTS2025-A1.1

WebCode Test	Response
24VY4B-5561	CTS2025-A1.1
24WLMH-5561	CTS2025-A1.1
2RG9U9-5562	CTS2025-A1.1
2U4TZC-5561	2025-A1.1
349ZFC-5562	CTS2025-A1.1
3BYPCG-5561	CTS2025-A1.1
3GDA68-5561	CTS2025-A1.1
3J4DXE-5562	CTS2025-A1.1
3PA7TA-5561	CTS2025-A1.1
4FFFK9-5561	CTS2025-A1.1
4RN848-5561	CTS2025-A1.1
4ZJ2KE-5562	CTS2025-A1.1
63LLN6-5561	CTS2025-A1.1
673VQB-5562	CTS2025-A1.1
6PJ238-5561	CTS2025-A1.1
7CQT46-5561	CTS2025-A1.1
7PVVH8-5561	CTS2025-A1.1
8FPDKA-5562	CTS2025-A1.1
8KE4Q6-5561	CTS2025-A1.1

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25 - Examination Questions	
WebCode Test	**Response**
8TBZD8-5562	Not in scope.
8WNN47-5562	CTS2025-A1.1
A444U7-5562	CTS2025-A1.1
AEKNE3-5561	CTS2025-A1.1
AFF7G6-5561	CTS2025-A1.1
AUY2L3-5562	CTS2025-A1.1
AXDN7Y-5561	CTS2025-A1.1
B7LHX8-5561	CTS2025-A1.1 – Carved 'jpg' file 0x02224728.jpg
B8ELJ2-5561	CTS2025-A1.1
BEGRX4-5562	CTS2025-A1.1
BTXP36-5562	CTS2025-A1.1
CDHZN3-5561	CTS2025-A1.1
CTEYRY-5562	CTS2025-A1.1
CWHMF2-5561	CTS2025-A1.1
DB9AYY-5561	CTS2025-A1.1
DJLBA2-5562	CTS2025-A1.1
DPCKJZ-5561	CTS2025-A1.1
E6FEQZ-5562	CTS2025-A1.1
EYTN7P-5562	CTS2025-A1.1
F4KDZ3-5562	CTS2025-A1.1
FJ22JX-5562	CTS2025-A1.1

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

	Question 25 - Examination Questions
WebCode Test	**Response**
FMYKLW-5561	CTS2025-A1.1
GA6R7K-5561	[Participant did not return results for this question.]
GA8D2Z-5562	CTS2025-A1.1
GJP4GX-5562	CTS2025-A1.1
GPH4VT-5561	CTS2025-A1.1
GQUT6W-5561	CTS2025-A1.1
GTHERT-5562	CTS2025-A1.1 – Carved 'jpg' file 0x02224728.jpg
GTZ73X-5562	CTS2025-A1.1
HEX8ER-5562	CTS2025-A1.1
HF9WVJ-5561	CTS2025-A1.1
HFCE3U-5561	CTS2025-A1.1
HXUD8T-5562	CTS2025-A1.1
HYZ6QT-5562	CTS2025-A1.1
J2L9YQ-5561	CTS2025-A1.1
J7HNUT-5561	CTS2025-A1.1
JGEWDV-5562	CTS2025-A1.1
JYYMCV-5561	CTS2025-A1.1
JZU7EW-5561	CTS2025-A1.1
K2HYQQ-5561	CTS2025-A1.1
K7CZKT-5562	CTS2025-A1.1
KA8UHU-5562	CTS2025-A1.1

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25 - Examination Questions	
WebCode Test	**Response**
KYBNNV-5562	The complete text within the photograph is "CTS2025-A1.1"
L7QRBN-5561	CTS2025-A1.1
LACBFT-5562	CTS2025-A1.1
LKDRCP-5561	CTS2025-A1.1
LMYFNP-5561	CTS2025-A1.1
LN7VWF-5562	[Participant did not return results for this question.]
LRRKGT-5562	CTS2025-A1.1
LUECCW-5561	CTS2025-A1.1
LYJAEX-5561	CTS2025-A1.1
M2VAHU-5562	CTS2025-A1.1
MD7R7R-5562	CTS2025-A1.1
MGM8JP-5561	CTS2025-A1.1
ML4AQV-5561	CTS2025-A1.1
MQXA6Q-5562	CTS2025-A1.1
MR7JXN-5561	CTS2025-A1.1
MRTR8R-5561	CTS2025-A1.1
MV6VTN-5562	CTS2025-A1.1
NJQ8AP-5561	CTS2025-A1.1
NK3WJT-5561	CTS2025-A1.1
PAF6NN-5561	CTS2025-A1.1
PPBH8Q-5561	CTS2025-A1.1

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25 - Examination Questions	
WebCode Test	**Response**
PQH2LD-5561	CTS2025-A1.1
PZAD6L-5561	CTS2025-A1.1
Q2Z3GD-5562	CTS2025-A1.1
QCLZQR-5562	CTS2025-A1.1
QEMD4J-5561	CTS2025-A1.1
QH4FBN-5562	CTS2025-A1.1
QT7QQQ-5561	CTS2025-A1.1
QWAN2J-5561	CTS2025-A1.1
QYVDDJ-5561	CTS2025-A1.1
R86XKL-5561	CTS2025-A1.1
RBJUPN-5561	CTS2025-A1.1
REKXEP-5561	CTS2025-A1.1
RR9ZXG-5561	CTS29250A1.1
T8JQPN-5562	CTS2025-A1.1
T8LHLB-5561	CTS2025-A1.1
TGQH3P-5561	CTS2025-A1.1
THHLMJ-5562	CTS2025-A1.1
TRHDUP-5562	CTS2025-A1.1
TVPPWK-5562	CTS2025-a1.1
TZXUNK-5561	CTS 2025-A1.1
U3GARK-5562	CTS2025-A1.1

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25 - Examination Questions	
WebCode Test	**Response**
U4CRUL-5562	CTS2025-A1.1
UGJTDH-5561	CTS2025-A1.1
UT9WBG-5562	CTS2025-A1.1
V63DZH-5562	CTS2025-A1.1
VJJLKL-5562	CTS2025-A1.1
VLV2EM-5561	CTS2025-A1.1
VYH7LJ-5561	CTS2025-A1.1
W7CX8H-5562	CTS2025-A1.1
W9FNCC-5561	CTS2025-A1.1
WH87QK-5562	CTS2025-A1.1
WKE9TJ-5562	CTS2025-A1.1
WRVWDD-5561	CTS2025-A1.1
WVD7FJ-5562	CTS2025-A1.1
X9VFGE-5562	12382975864_09e6e069e7_o.jpg
XDUKGE-5562	CTS2025-A1.1
XFRBFD-5561	CTS2025-A1.1
XGRD6G-5562	CTS2025-A1.1
XMC987-5562	CTS2025-A1.1
XY6VCG-5562	CTS2025-A1.1
Y36EXF-5561	CTS2025-A1.1
YVMR6B-5561	CTS2025-A1.1

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25 - Examination Questions	
WebCode Test	**Response**
YVR6WD-5561	CTS2025-A1.1
Z8XMWF-5562	CTS2025-A1.1
ZBE3BE-5561	CTS2025-A1.1
ZNK3ZC-5562	CTS2025-A1.1
ZRL9H3-5562	[Participant did not return results for this question.]
ZZUWEA-5562	CTS2025-A1.1

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25 - Examination Questions

Question 25: In unallocated space on the subject volume is a photograph (picture file) of an alligator with a green border, containing white text beginning with "CTS", provide the complete text visible in the picture.

<u>Consensus Result:</u>

CTS2025-A1.1

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

A reliable file recovery or file carving tool can find deleted files in unallocated space.

<u>Manufacturer's Response Illustration:</u>
X-Ways carved file

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26 - Examination Questions

Question 26: At what time did the user thomas first log in on 02/24/2025 (February 24, 2025) (UTC time)? Provide your answer in UTC time, using this format: HH:MM.

<u>Manufacturer's Response:</u> 02:28

WebCode Test	Response
24VY4B-5561	02:28
24WLMH-5561	02:28
2RG9U9-5562	02:28
2U4TZC-5561	02:28
349ZFC-5562	02:28 Successful
3BYPCG-5561	01:49 (UTC+0)
3GDA68-5561	02/24/2025 02:28
3J4DXE-5562	01:49
3PA7TA-5561	02:28
4FFFK9-5561	02:28
4RN848-5561	24-Feb-25 01:49:07
4ZJ2KE-5562	02:28
63LLN6-5561	02:28 UTC
673VQB-5562	02:28
6PJ238-5561	02:28
7CQT46-5561	01:49
7PVVH8-5561	02:28
8FPDKA-5562	02:28
8KE4Q6-5561	04:28 AM 02/24/25 UTC Time

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26 - Examination Questions	
WebCode Test	**Response**
8TBZD8-5562	Not in scope.
8WNN47-5562	02:28
A444U7-5562	02:28 UTC
AEKNE3-5561	02:28
AFF7G6-5561	02:28
AUY2L3-5562	01:49
AXDN7Y-5561	02:28
B7LHX8-5561	01:49
B8ELJ2-5561	02:28
BEGRX4-5562	02:28
BTXP36-5562	03:01
CDHZN3-5561	02:28
CTEYRY-5562	01:49
CWHMF2-5561	02:28
DB9AYY-5561	02:28
DJLBA2-5562	02:28
DPCKJZ-5561	02:28
E6FEQZ-5562	02:28
EYTN7P-5562	02:28
F4KDZ3-5562	Did not log in
FJ22JX-5562	02:28

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26 - Examination Questions	
WebCode Test	**Response**
FMYKLW-5561	2/24/2025 02:28
GA6R7K-5561	[Participant did not return results for this question.]
GA8D2Z-5562	02:28
GJP4GX-5562	02:28
GPH4VT-5561	02:28
GQUT6W-5561	02:28
GTHERT-5562	01:49
GTZ73X-5562	02:28
HEX8ER-5562	02:28
HF9WVJ-5561	02:28
HFCE3U-5561	02:28
HXUD8T-5562	02:28
HYZ6QT-5562	02:28 UTC
J2L9YQ-5561	02:28
J7HNUT-5561	02:28
JGEWDV-5562	02:28
JYYMCV-5561	02:28
JZU7EW-5561	02:28
K2HYQQ-5561	02:28
K7CZKT-5562	02:28
KA8UHU-5562	02:28

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26 - Examination Questions	
WebCode Test	**Response**
KYBNNV-5562	It appears that the user account "thomas" first logged on to the computer on 02/24/2025 at 02:28:05.
L7QRBN-5561	02:28
LACBFT-5562	02:28
LKDRCP-5561	02:28
LMYFNP-5561	02:28
LN7VWF-5562	[Participant did not return results for this question.]
LRRKGT-5562	02:28
LUECCW-5561	02:28
LYJAEX-5561	2025-02-24 01:49:07 UTC
M2VAHU-5562	01:49
MD7R7R-5562	02:28
MGM8JP-5561	02:28
ML4AQV-5561	02:28
MQXA6Q-5562	02:28
MR7JXN-5561	02:28 UTC
MRTR8R-5561	02:28
MV6VTN-5562	09:28 UTC
NJQ8AP-5561	02:28
NK3WJT-5561	02:28
PAF6NN-5561	02:28
PPBH8Q-5561	02:28

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

WebCode Test	Response
PQH2LD-5561	02:28
PZAD6L-5561	1:49 AM
Q2Z3GD-5562	02:28
QCLZQR-5562	02:28
QEMD4J-5561	02:28
QH4FBN-5562	02:27
QT7QQQ-5561	01:28
QWAN2J-5561	02:28
QYVDDJ-5561	02:27
R86XKL-5561	01:49
RBJUPN-5561	01:49
REKXEP-5561	02:28 AM
RR9ZXG-5561	02:28
T8JQPN-5562	17:07
T8LHLB-5561	02:27
TGQH3P-5561	2:28:05 AM
THHLMJ-5562	01:49 (UTC+0:00)
TRHDUP-5562	02:28
TVPPWK-5562	02:28
TZXUNK-5561	1:49
U3GARK-5562	09:28

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26 - Examination Questions	
WebCode Test	**Response**
U4CRUL-5562	02:28
UGJTDH-5561	02:28
UT9WBG-5562	02:27 UTC 0
V63DZH-5562	02:28(UTC 0)
VJJLKL-5562	02:28
VLV2EM-5561	02:28
VYH7LJ-5561	02:28
W7CX8H-5562	02:28
W9FNCC-5561	02:28
WH87QK-5562	02:28
WKE9TJ-5562	02:28
WRVWDD-5561	02:28
WVD7FJ-5562	02:28
X9VFGE-5562	2025-02-24 07:18
XDUKGE-5562	02:28
XFRBFD-5561	02:28 note: failed login attempt at 02:27
XGRD6G-5562	02:28
XMC987-5562	02:28 (UTC+0)
XY6VCG-5562	02:28
Y36EXF-5561	02:28
YVMR6B-5561	02:28

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26 - Examination Questions	
WebCode Test	**Response**
YVR6WD-5561	02:28
Z8XMWF-5562	02:28 UTC
ZBE3BE-5561	02:28
ZNK3ZC-5562	02:28
ZRL9H3-5562	01:49
ZZUWEA-5562	01:49

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26 - Examination Questions

Question 26: At what time did the user thomas first log in on 02/24/2025 (February 24, 2025) (UTC time)? Provide your answer in UTC time, using this format: HH:MM.

Consensus Result:

02:28

Manufacturer's Response Explanation:

User login events are stored in C: \Windows\System32\winevt\Logs\Security.evtx. EventID 4624 corresponds to successful login events.

Manufacturer's Response Illustration:

Windows Event Viewer

Other Responses:

A total of 17 (13%) participants reported 01:49. There are security event records associated with the thomas account at that time, but they are background processes, NOT a log in.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27 - Examination Questions

Question 27: Who is listed as the author of the spreadsheet document containing the keywords "philly", "Wilmington", and "phoenix"?

<u>Manufacturer's</u> Leslie Lessor
<u>Response:</u>

WebCode Test	Response
24VY4B-5561	Leslie Lessor
24WLMH-5561	Leslie Lessor
2RG9U9-5562	Leslie Lessor
2U4TZC-5561	Leslie Lessor
349ZFC-5562	Leslie Lessor
3BYPCG-5561	Leslie Lessor
3GDA68-5561	Leslie Lessor
3J4DXE-5562	Leslie Lessor
3PA7TA-5561	Leslie Lessor
4FFFK9-5561	Leslie Lessor
4RN848-5561	Leslie Lessor
4ZJ2KE-5562	Leslie Lessor
63LLN6-5561	Leslie Lessor
673VQB-5562	Leslie Lessor
6PJ238-5561	Leslie Lessor
7CQT46-5561	Leslie Lessor
7PVVH8-5561	Leslie Lessor
8FPDKA-5562	Leslie Lessor
8KE4Q6-5561	Leslie Lessor

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27 - Examination Questions	
WebCode Test	**Response**
8TBZD8-5562	Leslie Lessor
8WNN47-5562	Leslie Lessor
A444U7-5562	Leslie Lessor
AEKNE3-5561	Leslie Lessor
AFF7G6-5561	Leslie Lessor
AUY2L3-5562	Leslie Lessor
AXDN7Y-5561	Leslie Lessor
B7LHX8-5561	Leslie Lessor
B8ELJ2-5561	Leslie Lessor
BEGRX4-5562	Leslie Lessor
BTXP36-5562	Thomas
CDHZN3-5561	Leslie Lessor
CTEYRY-5562	Leslie Lessor
CWHMF2-5561	Leslie Lessor
DB9AYY-5561	Leslie Lessor
DJLBA2-5562	Leslie Lessor
DPCKJZ-5561	Leslie Lessor
E6FEQZ-5562	Leslie Lessor
EYTN7P-5562	Leslie Lessor
F4KDZ3-5562	Thomas
FJ22JX-5562	Leslie Lessor

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27 - Examination Questions	
WebCode Test	**Response**
FMYKLW-5561	Leslie Lessor
GA6R7K-5561	You should have changed me, Jennifer
GA8D2Z-5562	Leslie Lessor
GJP4GX-5562	Leslie Lessor
GPH4VT-5561	Leslie Lessor
GQUT6W-5561	Leslie Lessor
GTHERT-5562	Leslie Lessor
GTZ73X-5562	Leslie Lessor
HEX8ER-5562	Leslie Lessor
HF9WVJ-5561	Leslie Lessor
HFCE3U-5561	Leslie Lessor
HXUD8T-5562	Leslie Lessor
HYZ6QT-5562	Leslie Lessor
J2L9YQ-5561	Leslie Lessor
J7HNUT-5561	Leslie Lessor
JGEWDV-5562	Leslie Lessor
JYYMCV-5561	Leslie Lessor
JZU7EW-5561	Leslie Lessor
K2HYQQ-5561	Leslie Lessor
K7CZKT-5562	Leslie Lessor
KA8UHU-5562	Leslie Lessor

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27 - Examination Questions	
WebCode Test	**Response**
KYBNNV-5562	The author of the spreadsheet "Untitled 2.ods" has Leslie Lessor as the author.
L7QRBN-5561	Leslie Lessor
LACBFT-5562	Leslie Lessor
LKDRCP-5561	Leslie Lessor
LMYFNP-5561	Leslie Lessor
LN7VWF-5562	You should have changed me, Jennifer
LRRKGT-5562	Leslie Lessor
LUECCW-5561	Leslie Lessor
LYJAEX-5561	Leslie Lessor
M2VAHU-5562	Leslie Lessor
MD7R7R-5562	Leslie Lessor
MGM8JP-5561	Leslie Lessor
ML4AQV-5561	Leslie Lessor
MQXA6Q-5562	Leslie Lessor
MR7JXN-5561	Leslie Lessor
MRTR8R-5561	Leslie Lessor
MV6VTN-5562	Leslie Lessor
NJQ8AP-5561	Leslie Lessor
NK3WJT-5561	Leslie Lessor
PAF6NN-5561	Leslie Lessor
PPBH8Q-5561	Leslie Lessor

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27 - Examination Questions	
WebCode Test	**Response**
PQH2LD-5561	Leslie Lessor
PZAD6L-5561	Leslie Lessor
Q2Z3GD-5562	Leslie Lessor
QCLZQR-5562	Leslie Lessor
QEMD4J-5561	Leslie Lessor
QH4FBN-5562	You should have changed me, Jennifer
QT7QQQ-5561	Leslie Lessor
QWAN2J-5561	Leslie Lessor
QYVDDJ-5561	Leslie Lessor
R86XKL-5561	Leslie Lessor
RBJUPN-5561	Leslie Lessor
REKXEP-5561	Leslie Lessor
RR9ZXG-5561	Leslie Lessor
T8JQPN-5562	Leslie Lessor
T8LHLB-5561	Leslie Lessor
TGQH3P-5561	Leslie Lessor
THHLMJ-5562	Leslie Lessor
TRHDUP-5562	Leslie Lessor
TVPPWK-5562	Leslie Lessor
TZXUNK-5561	Leslie Lessor
U3GARK-5562	Leslie Lessor

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27 - Examination Questions	
WebCode Test	**Response**
U4CRUL-5562	Leslie Lessor
UGJTDH-5561	Leslie Lessor
UT9WBG-5562	Leslie Lessor
V63DZH-5562	Leslie Lessor
VJJLKL-5562	Leslie Lessor
VLV2EM-5561	Leslie Lessor
VYH7LJ-5561	Leslie Lessor
W7CX8H-5562	Leslie Lessor
W9FNCC-5561	Leslie Lessor
WH87QK-5562	Leslie Lessor
WKE9TJ-5562	Leslie Lessor
WRVWDD-5561	Leslie Lessor
WVD7FJ-5562	Leslie Lessor
X9VFGE-5562	file.xls
XDUKGE-5562	Leslie Lessor
XFRBFD-5561	Leslie Lessor
XGRD6G-5562	Leslie Lessor
XMC987-5562	Leslie Lessor
XY6VCG-5562	Leslie Lessor
Y36EXF-5561	Leslie Lessor
YVMR6B-5561	Leslie Lessor

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27 - Examination Questions	
WebCode Test	**Response**
YVR6WD-5561	Leslie Lessor
Z8XMWF-5562	Leslie Lessor
ZBE3BE-5561	Leslie Lessor
ZNK3ZC-5562	Leslie Lessor
ZRL9H3-5562	leslie lessor
ZZUWEA-5562	Leslie Lessor

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27 - Examination Questions

Question 27: Who is listed as the author of the spreadsheet document containing the keywords "philly", "Wilmington", and "phoenix"?

<u>Consensus Result:</u>

Leslie Lessor

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

Searching for the provided keywords and/or filtering for spreadsheet files discovers
C: \Users\thomas\Documents\Untitled 2.ods, an OpenOffice Calc spreadsheet. Reviewing the metadata in that file with OpenOffice Calc or MS Excel shows the authorship information.

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

X-Ways view of Untitled 2.ods

MS Excel display of Untitled 2.ods file information

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28 - Examination Questions

Question 28: Provide the names of the files the user accessed from the H:\k\ directory.

Manufacturer's Response: 1852232766.jpg, 778494116.jpg

WebCode Test	Response
24VY4B-5561	1852232766.jpg and 778494116.jpg
24WLMH-5561	1852232766.jpg, 778494116.jpg
2RG9U9-5562	778494116.jpg and 1852232766.jpg
2U4TZC-5561	1852232766.jpg and 778494116.jpg.
349ZFC-5562	H:\k\778494116.jpg and H:\k\1852232766.jpg
3BYPCG-5561	H:\k\1852232766.jpg H:\k\778494116.jpg
3GDA68-5561	H:\k\778494116.jpg, H:\k\1852232766.jpg
3J4DXE-5562	1852232766.jpg, 778494116.jpg
3PA7TA-5561	1852232766.jpg, 778494116.jpg
4FFFK9-5561	1852232766.jpg, 778494116.jpg
4RN848-5561	H:\k\1852232766.jpg, H:\k\778494116.jpg
4ZJ2KE-5562	1852232766.jpg ; 778494116.jpg
63LLN6-5561	1852232766.jpg; 778494116.jpg
673VQB-5562	1852232766.jpg; 778494116.jpg
6PJ238-5561	778494116.jpg; 1852232766.jpg
7CQT46-5561	H:\k\1852232766.jpg, H:\k\778494116.jpg
7PVVH8-5561	1852232766.jpg; 778494116.jpg
8FPDKA-5562	1852232766.jpg, 778494116.jpg
8KE4Q6-5561	778494116.jpg 1852232766.jpg
8TBZD8-5562	Not in scope.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28 - Examination Questions	
WebCode Test	**Response**
8WNN47-5562	778494116.jpg, 1852232766.jpg
A444U7-5562	778494116.jpg and 1852232766.jpg
AEKNE3-5561	1852232766.jpg, 778494116.jpg
AFF7G6-5561	778494116.jpg and 1852232766.jpg
AUY2L3-5562	1852232766.jpg and 778494116.jpg
AXDN7Y-5561	1852232766.jpg, 778494116.jpg
B7LHX8-5561	1852232766 and 778494116
B8ELJ2-5561	1852232766.jpg; 778494116.jpg
BEGRX4-5562	1852232766.jpg, 778494116.jpg
BTXP36-5562	778494116.jpg (3 times), 1852232766.jpg (3 times).
CDHZN3-5561	778494116.jpg 1852232766.jpg 1852232766.jpg
CTEYRY-5562	1852232766.jpg, 778494116.jpg
CWHMF2-5561	1852232766.jpg, 778494116.jpg
DB9AYY-5561	778494116.jpg 1852232766.jpg
DJLBA2-5562	1852232766.jpg and 778494116.jpg
DPCKJZ-5561	778494116.jpg & 1852232766.jpg
E6FEQZ-5562	94116.jpg and 1852232766.jpg
EYTN7P-5562	1852232766.jpg, 778494116.jpg
F4KDZ3-5562	1852232766.jpg and 778494116.jpg
FJ22JX-5562	H:\k\1852232766.jpg, H:\k\778494116.jpg
FMYKLW-5561	1852232766.jpg, 778494116.jpg

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28 - Examination Questions	
WebCode Test	**Response**
GA6R7K-5561	[Participant did not return results for this question.]
GA8D2Z-5562	778494116.jpg and 1852232766.jpg
GJP4GX-5562	1852232766.jpg & 778494116.jpg
GPH4VT-5561	1852232766.jpg and 778494116.jpg
GQUT6W-5561	778494116.jpg, 1852232766.jpg
GTHERT-5562	H:\k\778494116.jpg , H:\k\1852232766.jpg
GTZ73X-5562	1852232766.jpg, 778494116.jpg
HEX8ER-5562	1852232766.jpg, 778494116.jpg
HF9WVJ-5561	778494116.jpg, 1852232766.jpg
HFCE3U-5561	1852232766.jpg and 778494116.jpg
HXUD8T-5562	1852232766.jpg, 778494116.jpg
HYZ6QT-5562	1852232766.jpg, 778494116.jpg
J2L9YQ-5561	1852232766.jpg; 778494116.jpg
J7HNUT-5561	778494116.jpg, 1852232766.jpg
JGEWDV-5562	778494116.jpg & 1852232766.jpg
JYYMCV-5561	778494116.jpg, 1852232766.jpg
JZU7EW-5561	1852232766.jpg 778494116.jpg
K2HYQQ-5561	778494116.jpg, 1852232766.jpg
K7CZKT-5562	1852232766.jpg, 778494116.jpg
KA8UHU-5562	1852232766.jpg, 778494116.jpg
KYBNNV-5562	It appears that the user accessed 778494166.jpg and 1852232766.jpg.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28 - Examination Questions	
WebCode Test	**Response**
L7QRBN-5561	778494116.jpg , 1852232766.jpg
LACBFT-5562	1852232766.jpg, 778494116.jpg
LKDRCP-5561	1852232766.jpg, 778494116.jpg
LMYFNP-5561	778494116.jpg, 1852232766.jpg
LN7VWF-5562	[Participant did not return results for this question.]
LRRKGT-5562	778494116.jpg , 1852232766.jpg
LUECCW-5561	1852232766.jpg, 778494116.jpg
LYJAEX-5561	1852232766.jpg, 778494116.jpg
M2VAHU-5562	1852232766, 778494116
MD7R7R-5562	778494116.jpg, 1852232766.jpg
MGM8JP-5561	1852232766.jpg 778494116.jpg
ML4AQV-5561	H:\k\1852232766.jpg H:\k\778494116.jpg
MQXA6Q-5562	778494116.jpg, 1852232766.jpg
MR7JXN-5561	1852232766.jpg ; 778494116.jpg
MRTR8R-5561	778494116.jpg and 1852232766.jpg
MV6VTN-5562	1852232766.jpg, 778494116.jpg
NJQ8AP-5561	1852232766.jpg, 778494116.jpg
NK3WJT-5561	1852232766.jpg 778494116.jpg
PAF6NN-5561	1852232766.jpg, 778494116.jpg
PPBH8Q-5561	1852232766.jpg and 778494116.jpg
PQH2LD-5561	778494116.jpg & 1852232766.jpg

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28 - Examination Questions	
WebCode Test	**Response**
PZAD6L-5561	A. 778494116.jpg, 1852232766.jpg
Q2Z3GD-5562	H:/k/1852232766.jpg, H:/k/778494116.jpg
QCLZQR-5562	778494116.jpg and 1852232766.jpg
QEMD4J-5561	1852232766.jpg, 778494116.jpg
QH4FBN-5562	778494116.jpg; 1852232766.jpg
QT7QQQ-5561	H:\k\778494116.jpg H:\k\1852232766.jpg
QWAN2J-5561	1852232766.jpg & 778494116.jpg
QYVDDJ-5561	1852232766.jpg, 778494116.jpg
R86XKL-5561	1852232766.jpg, 778494116.jpg
RBJUPN-5561	1852232766.jpg, 778494116.jpg
REKXEP-5561	778494116.jpg, 1852232766.jpg
RR9ZXG-5561	H:\k\1852232766.jpg, H:\k\778494116.jpg
T8JQPN-5562	1852232766.jpg, 778494116.jpg
T8LHLB-5561	1852232766.jpg, 778494116.jpg
TGQH3P-5561	1852232766.jpg 778494116.jpg
THHLMJ-5562	1852232766.jpg 778494116.jpg
TRHDUP-5562	1852232766.jpg, 778494116.jpg
TVPPWK-5562	1852232766.jpg, 778494116.jpg
TZXUNK-5561	778494116.jpg, 1852232766.jpg
U3GARK-5562	H:\k\778494116.jpg and H:\k\1852232766.jpg
U4CRUL-5562	778494116.jpg and 1852232766.jpg

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28 - Examination Questions	
WebCode Test	**Response**
UGJTDH-5561	H:\k\1852232766.jpg ; H:\k\778494116.jpg
UT9WBG-5562	1852232766.jpg / 778494116.jpg
V63DZH-5562	778494116.jpg, 1852232766.jpg
VJJLKL-5562	1852232766.jpg and 778494116.jpg
VLV2EM-5561	$MFT - k.lnk
VYH7LJ-5561	1852232766.jpg, 778494116.jpg
W7CX8H-5562	778494116.jpg and 1852232766.jpg (the following files have been accessed, but are assumed to not have been user accessed: 461652889.jpg and 676878980.jpg)
W9FNCC-5561	1852232766.jpg, 778494116.jpg
WH87QK-5562	1852232766.jpg and 778494116.jpg
WKE9TJ-5562	778494116.jpg, 1852232766.jpg
WRVWDD-5561	1852232766.jpg, 778494116.jpg
WVD7FJ-5562	778494116.jpg and 1852232766.jpg
X9VFGE-5562	1852232766.jpg and 778494116.jpg
XDUKGE-5562	1852232766.jpg and 778494116.jpg
XFRBFD-5561	1852232766.jpg and 778494116.jpg
XGRD6G-5562	778494116.jpg, 1852232766.jpg
XMC987-5562	H:\k\1852232766.jpg H:\k\778494116.jpg
XY6VCG-5562	778494116.jpg, 1852232766.jpg, 778494116.jpg, 1852232766.jpg
Y36EXF-5561	778494116.jpg, 1852232766.jpg
YVMR6B-5561	H:\k\1852232766.jpg, H:\k\778494116.jpg
YVR6WD-5561	778494116.jpg & 1852232766.jpg

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

	Question 28 - Examination Questions
WebCode Test	**Response**
Z8XMWF-5562	1852232766.jpg & 778494116.jpg
ZBE3BE-5561	778494116.jpg, 1852232766.jpg
ZNK3ZC-5562	1852232766.jpg 778494116.jpg
ZRL9H3-5562	778494116.jpg, 1852232766.jpg
ZZUWEA-5562	1852232766.jpg & 778494116.jpg

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28 - Examination Questions

Question 28: Provide the names of the files the user accessed from the H:\k\ directory.

<u>Consensus Result:</u>

1852232766.jpg, 778494116.jpg

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

When a user opens a file, Windows creates a lnk file in the user's "Recent" directory. A search of these files for relevant path information (i.e., "H:\k\") will identify files opened from that path.

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

X-Ways Parse of C:\Users\thomas\AppData\Roaming\Microsoft\Windows\Recent\778494116.jpg.lnk

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28 - Examination Questions

X-Ways Parse of C:\Users\thomas\AppData\Roaming\Microsoft\Windows\Recent\1852232766.jpg.lnk

Target attributes	A
Target file size	906818
Show Window	SW_NORMAL
Target created	02/20/2022 18:36:59 -7
Last written	09/02/2023 13:45:53 -7
Last accessed	03/02/2025 13:01:06 -7
ID List	Desktop\H:\k\ C=06/28/2022 23:59:20 M=01/23/2023 01:46:16 A=03/02/2025 1852232766 M=09/02/2023 20:45:54 A=06/17/2022 Size=906818
Volume type	Removable
Volume serial	0x5EADB852
Volume name	misc
Local path	H:\k\1852232766.jpg
Working directory	H:\k
Known Folder Tracking	false
Host name	desktop-p8svdmn
Volume ID	{00000000-0000-0000-0000-000000000000}
Object ID	{48037844-F4AF-11EF-A341-080027575D1A}
MAC Address	08 00 27 57 5D 1A
Timestamp	02/26/2025 21:05:13 -5, Seq: 9025

H:\k\1852232766.jpg

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 29 - Removable Media 25-5562

Question 29: Provide a physical description of the provided evidence item, as well as the unique Identifier written in marker.

Manufacturer's Response: Responses will vary but should include the CTS assigned number (written on the device), and a description of a black USB stick flash media storage device with silver cover, etc.

WebCode Test	Response
2RG9U9-5562	This was a black and silver USB drive. The USB drive was black with a silver hinged cover. A white sticker was attached bearing "CTS Test 25-5562". On hinged area of the USB drive in silver marker was "09" with an underline.
349ZFC-5562	Silver/Black Tonpha 4 Gigabyte USB flash drive, labeled CTS Test 25-5562; with 52 writing in silver marker
3J4DXE-5562	description: pendrive USB, identifier: 25-5562
4ZJ2KE-5562	It's a black and silver colored pendrive, with the number 63 handwritten on it with a silver marker.
673VQB-5562	Black and Silver USB drive with a white sticker labeled "CTS Test 25-5562" and a silver, hand-written, "17" and checkmark
8FPDKA-5562	Black and silver, 4GB foldable USB device, CTS Test 25-5562, hand written number "23" and a "check" (or "v") character
8TBZD8-5562	A black USB drive containing the markings "CTS Test" "25-5562" printed on a label, "66", and a tick written in white marker.
8WNN47-5562	25-5562
A444U7-5562	USB stick with a white label reading 'CTS Test 25-5562' and marked with a grey marker '70'
AUY2L3-5562	A black USB flash drive with a silver cover. The identifier written in marker is "74"
BEGRX4-5562	Black and Silver Swivel close USB 2.0 with CTS Test 25-5565 printed on a sticker and a Checkmark with initials in silver marker
BTXP36-5562	TONPHA USB 2.0 Classic/ S/N - 0000ECC0300085104/CTS TEST 25-5562/51 Black with silver handle.
CTEYRY-5562	A black USB flash drive written on it the number 74 and a tick, the Drive has a metallic swivel cover, with a white attached label including the text CTS Test 25-5562.
DJLBA2-5562	A black USB labeled CTS Test 25-5562, 19 with a check mark written in silver sharpie
E6FEQZ-5562	Black TONPHA USB 2.0 Classic 4 GB USB Flash Drive, Labeled CTS Test 25-5562, Flash drive has the number "60" written on it in silver marker
EYTN7P-5562	A black and silver USB stick with a white label with the inscription "CTS Test 25-5562"
F4KDZ3-5562	Black Universal Serial Bus drive with a label on it with typed words of "CTS Test" and underneath those words are tyoed "25-5562"
FJ22JX-5562	SILVER AND BLACK 4 GB THUMB DRIVE WITH THE NUMBER "44" WRITTEN ON IT IN SILVER LETTERING.
GA8D2Z-5562	USB flash drive with a mention on sticker : "CTS Test 25-5562" (G5/45/GS/4S)
GJP4GX-5562	USB Flash drive, Flip-open style with black plastic body and silver metal cover. Marked with a printed label "CTS Test 25-556" and silver marker markings "21" underlined.

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 29 - Removable Media 25-5562	
WebCode Test	**Response**
GTHERT-5562	paper bag that contains: Black and silver USB flash drive / written in white color 35
GTZ73X-5562	Black and Grey USB Thumb drive labeled "CTS Test 25-5562"
HEX8ER-5562	USB flash memory with gray/black color, "68" and check mark on the top right written in marker, Label "CTS Test 25-5562"
HXUD8T-5562	Physical Description: The evidence item is a black swivel-type USB flash drive with a silver-colored cover. The USB connector appears to be black. Unique Identifier: The number "46" is written on the device in marker.
HYZ6QT-5562	A USB drive labelled as "CTS TEST 25-5562" with hand marking "G1" and tick mark.
JGEWDV-5562	Silver and black , swivel, USB 2.0 Flash Drive, Label w/ "CTS Test 25-5562", Written in silver marker "05" and checkmark
K7CZKT-5562	Black USB Flash Drive with label "CTS Test 25-5562" and '13' written in silver marker
KA8UHU-5562	Black and silver USB Flash Drive with a white label that reads "CTS Test 25-5562"; the number 54 is written in silver marker on the front of the drive
KYBNNV-5562	The provided evidence item is a grey and black USB 2.0 thumb drive. There is a printed label containing the "CTS Test 25-5562". Additionally, there is a "22" written in white marker on the black hinge of the evidence item.
LACBFT-5562	Black USB thumb drive with silver casing, labelled "CTS Test 25-5562", "75" written in marker
LN7VWF-5562	Black and grey USB stick., CTS TEST 25-5562. There identifer is 79 - it also has a silver Tick on it.
LRRKGT-5562	black and silver, TONPHA USB Flash Drive, Serial Number: 24070120441799262221929, labeled CTS Test 25-5562, from within a sealed envelope with red evidence tape and the initials CTS
M2VAHU-5562	Black USB flash drive, CTS on the evidence container and 25 on the USB drive.
MD7R7R-5562	Black and silver USB thumb drive. Contains a sticker on it with the following information: CTS Test 25-5562 Also has the number 12, 21, or 17 and a check mark in silver
MQXA6Q-5562	Black in color with a silver rotating cover with what appears to be a check mark and a "03" and a sticker labeled CTS Test 25-5562
MV6VTN-5562	Black and silver USB 'thumbdrive' with white label showing 'CTS Test 25-5562' in black text. Written in silver-colored marker appears to be '04' along with what appears to be a silver-colored checkmark.
Q2Z3GD-5562	Black/Gray USB. Sticky paper marked "CTS Test 25-5562" and "45" written in marker.
QCLZQR-5562	A black and silver flash drive with a white sticker on it that reads "CTS Test 25-5562". The unique identifier(s) written in marker are the number 25 and a checkmark.
QH4FBN-5562	Black USB drive with gray cover; "CTS Test 25-5562"; unique ID 20
T8JQPN-5562	Black and silver USB thumb drive labeled "CTS Test" "25-5562" silver marker labeled "11 2"
THHLMJ-5562	Black and silver USB with a white label with the following 'CTS Test 25-5562' affixed to the silver part. The number '78' has been written in silver marker on the same side of the USB as the white label. There is a silver tick (in marker) also visible on the bottom part of the USB.
TRHDUP-5562	Black/Silver USB flash drive printed label CTS 25-5562 with 24 and a check-mark written in silver marker.

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 29 - Removable Media 25-5562	
WebCode Test	**Response**
TVPPWK-5562	Black and silver drive with CTS Test 25-5562 sticker
U3GARK-5562	UIN: 25-5562; Make: Tonpha 2.0 Classic USB Device; Size: 3.8GB. The number 30 appears to be written in marker on the device.
U4CRUL-5562	On the front of a small orange envelope, there is a white label placed toward the top with black typed writing: "2025 CTS Forensic Testing Program, TEST NO. 25-5562: COMPUTER HARD DRIVE- WINDOWS & REMOVABLE MEDIA ANALYSIS, Sample Pack: HDRM." Just below this label is a yellow label with black typed writing: "Please note this test has two parts: Part I is on the CTS Portal. Part II (USB) is enclosed here. TREAT USB AS EVIDENCE!" On the rear of the envelope, the flap is sealed with red and black evidence tape and has the letters "CTS" hand written across the bottom of the tape with black marker. Within the envelope is a small clear plastic bag with a black and silver generic thumb drive inside. On the silver portion of one side of the thumb drive, there is a white label with black typed writing: "CTS Test 25-5562". On the black part of the same side of the thumb drive as the white label is what appears to be the number 14 and a checkmark hand written with a silver marker.
UT9WBG-5562	Gray and black pendrive with inscription "CTS Test 25-5562"
V63DZH-5562	The provided evidence item is a silver and black USB flash drive with a swivel metal cover. A white label affixed to the metal cover reads "CTS Test 25-5562." Additionally, the number "71" is written in marker inside the circular indentation on the swivel cover.
VJJLKL-5562	Black and silver USB flash drive with a label "CTS Test 25-5562" and some markings with a silver marker
W7CX8H-5562	Black USB-stick without visible brand, containing a sticker with the text "CTS Test 25-5562" and the number "64" and "v" written with a silver marker.
WH87QK-5562	Silver and black USB thumb drive with a white label and in black letters "CTS Test 25-5562". The thumb drive also had some illegible silver markings on the device.
WKE9TJ-5562	Black and silver USB thumb drive. Labeled CTS Test 25-5562. The number "56" (Possible Unique ID) and a "checkmark" is written on the device in silver marker.
WVD7FJ-5562	Black and Silver USB Flash Drive, Printed label reads "CTS Test 25-5562"; written on the USB in silver marker is 53 and what appears to be a check mark
X9VFGE-5562	USB memory with a black plastic casing and a silver rotating metal cap. It has a type A USB connector. No visible manufacturer markings. Unique identifier: CTS Test 25-5562, with the number 72 written in marker.
XDUKGE-5562	The item is a black unbranded US flash drive inside a tape-sealed envelope with writing in silver pen on the black body that appears to be a checkmark and an underlined number 10; there is a printed label that reads as "CTS Test 25-5562".
XGRD6G-5562	Black and Silver USB flash drive with a white label containing the text "CTS Test 25-5562", as well as the number "58" and a check mark written in silver.
XMC987-5562	CTS Test 25-5562
XY6VCG-5562	Received one unbranded black USB device with grey swivel guard. The device was marked with the number "52" and a checkmark in grey marker. A label was affixed with the unique identifier "CTS Test 25-5562".
Z8XMWF-5562	Black/Gray USB Drive with a white sticker label reading "CTS Test 25-5562" and the checkmark symbol and the number "55" or letters "SS" written in gray marker on the device.
ZNK3ZC-5562	A black flash drive with a rotating metal cover around it. Unique Identifier written in marker is 34.
ZRL9H3-5562	Black and silver USB, labelled CTS Test 25-5562. Unique identifier is 77

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 29 - Removable Media 25-5562	
WebCode Test	**Response**
ZZUWEA-5562	USB in a sealed clear bag within a yellow envelope, sealed with possible 'EVIDENCE' tape, 'DENCE' is only visible. A white label on the front on the envelope with the following: 2025 CTS Forensic Testing Program TEST NO. 25-5562 COMPUTER HARD DRIVE- WINDOWS & REMOVABLE MEDIA ANALYSIS Sample Pack: HDRM A yellow label on the front with the following: Please note this test has two parts: Part I is on the CTS Portal. Part II (USB) is enclosed here. TREAT USB AS EVIDENCE CTS written in black marker, partially on the tape and envelope

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 29 - Removable Media 25-5562

Question 29: Provide a physical description of the provided evidence item, as well as the unique Identifier written in marker.

Consensus Result:

Responses include the CTS assigned number (written on the device), and a description of a black USB stick flash media storage device with silver cover, etc.

Manufacturer's Response Explanation:

The response serves as validation that the participant has considered a process for tracking intake of items of physical digital evidence.

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 30 - Removable Media 25-5562

Question 30: Provide the SHA256 hash of the provided USB flash storage device. Transfer the hash carefully.

Manufacturer's Response: CCC57620030E10D90E77F50D23E5A1AC51EFFC4C9D834F39194C247EDBC2822C

WebCode Test	Response
2RG9U9-5562	CCC57620030E10D90E77F50D23E5A1AC51EFFC4C9D834F39194C247EDBC2822C
349ZFC-5562	ccc5 7620 030e 10d9 0e77 f50d 23e5 a1ac 51ef fc4c 9d83 4f39 194c 247e dbc2 822c
3J4DXE-5562	5EC468F9831055B9C31F907C74B64C25D8B953123229FF7502AF3DE94E64AF06
4ZJ2KE-5562	ccc57620030e10d90e77f50d23e5a1ac51effc4c9d834f39194c247edbc2822c
673VQB-5562	CCC57620030E10D90E77F50D23E5A1AC51EFFC4C9D834F39194C247EDBC2822C
8FPDKA-5562	CCC57620030E10D90E77F50D23E5A1AC51EFFC4C9D834F39194C247EDBC2822C
8TBZD8-5562	CCC57620030E10D90E77F50D23E5A1AC51EFFC4C9D834F39194C247EDBC2822C
8WNN47-5562	CCC57620030E10D90E77F50D23E5A1AC51EFFC4C9D834F39194C247EDBC2822C
A444U7-5562	[Participant did not return results for this question.]
AUY2L3-5562	CCC57620030E10D90E77F50D23E5A1AC51EFFC4C9D834F39194C247EDBC2822C
BEGRX4-5562	CCC57620030E10D90E77F50D23E5A1AC51EFFC4C9D834F39194C247EDBC2822C
BTXP36-5562	CF7F4706DD9942A6727BDC7EE1BAAD2EDCC85957810C7DD9F481723865CF4078
CTEYRY-5562	CCC57620030E10D90E77F50D23E5A1AC51EFFC4C9D834F39194C247EDBC2822C
DJLBA2-5562	CCC57620030E10D90E77F50D23E5A1AC51EFFC4C9D834F39194C247EDBC2822C
E6FEQZ-5562	ccc5 7620 030e 10d9 0e77 f50d 23e5 a1ac 51ef fc4c 9d83 4f39 194c 247e dbc2 822c
EYTN7P-5562	CCC57620030E10D90E77F50D23E5A1AC51EFFC4C9D834F39194C247EDBC2822C
F4KDZ3-5562	f5f52cb1f607bbbacfee1196f711c6dfa95c863081f10ff17e3934b686f4edfb
FJ22JX-5562	ccc57620030e10d90e77f50d23e5a1ac51effc4c9d834f39194c247edbc2822c
GA8D2Z-5562	CCC57620030E10D90E77F50D23E5A1AC51EFFC4C9D834F39194C247EDBC2822C
GJP4GX-5562	ccc5 7620 030e 10d9 0e77 f50d 23e5 a1ac 51ef fc4c 9d83 4f39 194c 247e dbc2 822c

(229)

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 30 - Removable Media 25-5562	
WebCode Test	**Response**
GTHERT-5562	149e91000b4a3a18cbc6b0bee836ace01a1d17d7fb05bc0cab7da487b34ef596
GTZ73X-5562	DAD75ADA184EA3F079016ED520BC0644F01017E3CC4E6FF566F3E7FE47CD613B
HEX8ER-5562	ccc57620030e10d90e77f50d23e5a1ac51effc4c9d834f39194c247edbc2822c
HXUD8T-5562	ccc5 7620 030e 10d9 0e77 f50d 23e5 a1ac 51ef fc4c 9d83 4f39 194c 247e dbc2 822c
HYZ6QT-5562	CCC57620030E10D90E77F50D23E5A1AC51EFFC4C9D834F39194C247EDBC2822C
JGEWDV-5562	SHA256: CCC57620030E10D90E77F50D23E5A1AC51EFFC4C9D834F39194C247EDBC2822C
K7CZKT-5562	8C78F3B3B310D5D32FC37D2793538B0D1E5435DF43C3DF944DC2356EA4927C9F
KA8UHU-5562	CCC57620030E10D90E77F50D23E5A1AC51EFFC4C9D834F39194C247EDBC2822C
KYBNNV-5562	The SHA256 hash value for the USB stick is CCC57620030E10D90E77F50D23E5A1AC51EFFC4C9D834F39194C247EDBC2822C
LACBFT-5562	63863aa6c0ffccda9a0b8dd3ed3c5d23dbc17749926c1b978681cd34f257d669
LN7VWF-5562	04b2bc3bad854176191bef933e4a72a0ef88c02e86e609952a16d151957d1935
LRRKGT-5562	ccc5 7620 030e 10d9 0e77 f50d 23e5 a1ac 51ef fc4c 9d83 4f39 194c 247e dbc2 822c
M2VAHU-5562	ccc57620030e10d90e77f50d23e5a1ac51effc4c9d834f39194c247edbc2822c
MD7R7R-5562	CCC57620030E10D90E77F50D23E5A1AC51EFFC4C9D834F39194C247EDBC2822C
MQXA6Q-5562	ccc57620030e10d90e77f50d23e5a1ac51effc4c9d834f39194c247edbc2822c
MV6VTN-5562	ccc57620030e10d90e77f50d23e5a1ac51effc4c9d834f39194c247edbc2822c
Q2Z3GD-5562	ccc57620030e10d90e77f50d23e5a1ac51effc4c9d834f39194c247edbc2822c
QCLZQR-5562	ccc57620030e10d90e77f50d23e5a1ac51effc4c9d834f39194c247edbc2822c
QH4FBN-5562	ccc576200e10d90e77f50d23e5a1ac51effc4c9d834f39194c247edbc2882c
T8JQPN-5562	CCC57620030E10D90E77F50D23E5A1AC51EFFC4C9D834F39194C247EDBC2822C
THHLMJ-5562	CCC57620030E10D90E77F50D23E5A1AC51EFFC4C9D834F39194C247EDBC2822C
TRHDUP-5562	CCC57620030E10D90E77F50D23E5A1AC51EFFC4C9D834F39194C247EDBC2822C

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 30 - Removable Media 25-5562	
WebCode Test	**Response**
TVPPWK-5562	SHA256: CCC57620030E10D90E77F50D23E5A1AC51EFFC4C9D834F39194C247EDBC2822C
U3GARK-5562	CCC57620030E10D90E77F50D23E5A1AC51EFFC4C9D834F39194C247EDBC2822C
U4CRUL-5562	Using my TX1, I hashed the provided thumb drive and received the SHA256 value of: ccc5 7620 030e 10d9 0e77 f50d 23e5 a1ac 51ef fc4c 9d83 4f39 194c 247e dbc2 822c
UT9WBG-5562	ccc57620030e10d90e77f50d23e5a1ac51effc4c9d834f39194c247edbc2822c
V63DZH-5562	E44B49FB4DEDE1D9CCAB75FF53ED882A206E6E6BEBF4FFE43A2E37564274D486(USB),B45B94592566705F0F9F9AC58DD640D9DBEC25EAE5D3761C31A386048123D5BC(raw file)
VJJLKL-5562	ccc57620030e10d90e77f50d23e5a1ac51effc4c9d834f39194c247edbc2822c
W7CX8H-5562	ccc57620030e10d90e77f50d23e5a1ac51effc4c9d834f39194c247edbc2822c
WH87QK-5562	ccc57620030e10d90e77f50d23e5a1ac51effc4c9d834f39194c247edbc2822c
WKE9TJ-5562	CCC57620030E10D90E77F50D23E5A1AC51EFFC4C9D834F39194C247EDBC2822C
WVD7FJ-5562	CCC57620030E10D90E77F50D23E5A1AC51EFFC4C9D834F39194C247EDBC2822C
X9VFGE-5562	SHA256 Hash: ccc57620030e10d90e77f50d23e5a1ac51effc4c9d834f39194c247edbc2822c
XDUKGE-5562	CCC57620030E10D90E77F50D23E5A1AC51EFFC4C9D834F39194C247EDBC2822C
XGRD6G-5562	CCC57620030E10D90E77F50D23E5A1AC51EFFC4C9D834F39194C247EDBC2822C
XMC987-5562	58cca50e51b740bba9d8cfb32748117706947c269251304cb7079705fd76f814
XY6VCG-5562	CCC57620030E10D90E77F50D23E5A1AC51EFFC4C9D834F39194C247EDBC2822C
Z8XMWF-5562	ccc5 7620 030e 10d9 0e77 f50d 23e5 a1ac 51ef fc4c 9d83 4f39 194c 247e dbc2 822c
ZNK3ZC-5562	c9fbbe17bcdd0ecb72cc44a92d3b36612d0626f79863fd6379efb29c8edf197b (A different hash comes out every time.)
ZRL9H3-5562	5f402d3f77a1b3436c366928c5428983705c0097c06e756ebc8186ce66fd0169
ZZUWEA-5562	ccc57620030e10d90e77f50d23e5a1ac51effc4c9d834f39194c247edbc2822c

Removable Media Analysis Results
TABLE 2: Removable Media Analysis Results

Question 30 - Removable Media 25-5562

Question 30: Provide the SHA256 hash of the provided USB flash storage device. Transfer the hash carefully.

Consensus Result:

CCC57620030E10D90E77F50D23E5A1AC51EFFC4C9D834F39194C247EDBC2822C

Manufacturer's Response Explanation:

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

Manufacturer's Response Illustration:

X-Ways USB Device SHA256 hash

```
 1   03/09/2025, 22:08:00
 2 ▸ X-Ways Forensics BYOD 21.4 SR-1 x64
12 ◂ Source: Removable storage 3
13   Sectors 0-7864319
14
15   Model: TONPHA USB 2.0 Classic
16   Serial No.: 1502141613383306403119
17   Firmware Rev.: 5.00
18   Bus: USB
19
20 ▸ Total capacity: 4,026,531,840 bytes = 3.8 GB
58 ◂ Hash of source data: 2BA17083E92897E00F59FF6C81C3EA52  (MD5)
59   Hash of source data: CCC57620030E10D90E77F50D23E5A1AC51EFFC4C9D834F39194C247EDBC2822C (SHA-256)
60
```

Logicube Talon USB Device SHA256 hash

```
<VerifyInfo>
    <Drive Result="Pass" LogicalSectSz="512" LBA="7864320" HashType="SHA-256"
Hash='ccc57620030e10d90e77f50d23e5a1ac51effc4c9d834f39194c247edbc2822c'
ExpectedHash="ccc57620030e10d90e77f50d23e5a1ac51effc4c9d834f39194c247edbc2822c"
</VerifyInfo>
```

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 31 - Removable Media 25-5562

Question 31: Identify the filesystem on each partition on this device. Provide partition number, filesystem, and volume name/label for all partitions.

Manufacturer's Response:
1. exFat, [unnamed / NONAME]
2. NTFS, "NTFS"
3. FAT32, "SMALL"
4. NTFS, "misc"

WebCode Test	Response
2RG9U9-5562	Partition 1, exFAT, NONAME and Partition 2, NTFS, NTFS and Partition 3, FAT32, SMALL and Partition 4, NTFS, misc
349ZFC-5562	Partition 1: EXFAT ; NONAME | Partition 2: NTFS ; NTFS | Partition 3: FAT32 ; SMALL | Partition 4: NTFS ; misc
3J4DXE-5562	(Partition 1, exFAT, NONAME); (Partition 2, NTFS, NTFS); (Partition 3, FAT32, SMALL); (Partition 4, NTFS, misc); Unpartitioned space
4ZJ2KE-5562	Partition: 1, filesystem, exFAT, volume label: (n/a) ; Partition: 2, filesystem: NTFS, volume label: NTFS ; Partition: 3, filesystem: FAT32, volume label: SMALL ; Partition: 4, filesystem: NTFS, volume label: misc
673VQB-5562	1) exFat/"NONAME" 2) NTFS/"NTFS" 3) FAT32/"SMALL" 4) NTFS/"misc"
8FPDKA-5562	Partition 1, exFAT, (none); Partition 2, NTFS, NTFS; Partition 3, FAT32, SMALL; Partition 4, NTFS, misc
8TBZD8-5562	Not in scope.
8WNN47-5562	Partition 1, exFAT, <Null>, Partition 2, NTFS, NTFS, Partition 3, FAT32, SMALL, Partition 4, NTFS, misc
A444U7-5562	Partition 1 exFAT " " (NONAME), Partition 2 NTFS NTFS, Partition 3 Fat32 SMALL, Partition 4 NTFS misc
AUY2L3-5562	Partition 1, exFAT, no volume name. Partition 2, NTFS, NTFS. Partition 3, FAT32, SMALL. Partition 4, NTFS, misc
BEGRX4-5562	Partition 1 (NONAME exFAT]), Partition 2 (NTFS [NTFS]), Partition 3 (SMALL [FAT32]), Partition 4 (misc [NTFS])

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 31 - Removable Media 25-5562	
WebCode Test	**Response**
BTXP36-5562	P1=exFAT - 'NONAME'; P2=NTFS - 'NTFS'; P3=FAT32 - 'SMALL'; P4=NTFS - 'misc'.
CTEYRY-5562	PARTITION 1, exFAT, ; PARTITION 2, NTFS, NTFS; PARTITION 3, FAT32, SMALL; PARTITION 4, NTFS, misc.
DJLBA2-5562	Partition 1 exFAT NO NAME (F:) | Partition 2, NTFS NTFS (H:) | Partition 3, FAT32, SMALL (J:) | Partition 4, NTFS misc (K:)
E6FEQZ-5562	Partition 1 File Name: NONAME File system: exFAT Partition 2 File Name: NTFS File system: NTFS Partition 3 File Name: SMALL File system: FAT32 Partition 4 File Name: misc File system: NTFS
EYTN7P-5562	Partition 1 (Filesystem: exFAT, Volume name: NONAME), Partition 2 (Filesystem: NTFS, Volume name: NTFS), Partition 3 (Filesystem: FAT32, Volume name: SMALL), Partition 4 (Filesystem: NTFS, Volume name: misc).
F4KDZ3-5562	Partition 1 (D) exFAT, Partition 2 H:NTFS(NTFS) Partition 3 I:SMALL(FAt32) Partition 4 J:misc(NTFS)
FJ22JX-5562	Partition 1 @ 128 Filesystem is EXFAT, name/label is NONAME, Partition 2 @ 3764352 Filesystem is NTFS volume name/label is NTFS, Partition 3 @ 5812352 filesystem is FAT32 volume name/label is SMALL, Partition 4 @ 6842368 filesystem is NTFS and volume name/label is misc.
GA8D2Z-5562	Partition n°1 exFAT <No name>, Partition n°2 NTFS Name:NTFS Partition n°3 FAT32 Name:SMALL, Partition n°4 NTFS Name:misc, lost Partiition: ExFAT, no name
GJP4GX-5562	Partition 1, exFAT, No Label – Partition 2, NTFS, NTFS – Partition 3, FAT32, SMALL – Partition 4, NTFS, misc
GTHERT-5562	(1,2,3,4), (ExFAT,NTFS ,FAT32,NTFS), and (Unlabeled Volume,NTFS,SMALL,misc)
GTZ73X-5562	1. NONAME (exFAT) 2. NTFS (NTFS) 3. SMALL (FAT32) 4. misc (NTFS)
HEX8ER-5562	Partition 1, filesystem: exFat, volume name/label: - Partition 2, filesystem: NTFS, volume name/label: NTFS Partition 3, filesystem: FAT32, volume name/label: SMALL Partition 4, filesystem: NTFS, volume name/label: misc

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 31 - Removable Media 25-5562	
WebCode Test	**Response**
HXUD8T-5562	A total of four partitions were found. • Partition 1 has a file system format of exFAT and does not have a volume label. • Partition 2 has a file system format of NTFS and its volume label is "NTFS." • Partition 3 has a file system format of FAT32 and its volume label is "SMALL." • Partition 4 has a file system format of NTFS and its volume label is "misc."
HYZ6QT-5562	[Partition 1, exFAT, (NONAME)], [Partition 2, NTFS, NTFS], [Partition 3, FAT32, SMALL], [Partition 4, NTFS, misc], The remnants of another partition were recovered [Partition 5, exFAT, (NONAME)]
JGEWDV-5562	Partition 1: File System = exFAT; Volume Name/Label = N/A | Partition 2: File System = NTFS; Volume Name/Label = "NTFS" | Partition 3: File System = FAT32; Volume Name/Label = "SMALL" | Partition 4: File System = NTFS; Volume Name/Label = "misc"
K7CZKT-5562	Partition 1: exFat 'no name' Partition 2: NTFS, NTFS Partition 3: FAT32, SMALL Partition 4: RAW 'no name'
KA8UHU-5562	Partition 1 exFAT (no name); Partition 2 NTFS "NTFS"; Partition 3 FAT32 "SMALL"; Partition 4 NTFS "misc"
KYBNNV-5562	Partition 1 has exFAT as the file system and the volume label is "NONAME". Partition 2 has NTFS files system and the volume label is NTFS. Partition 3 has FAT32 file system and a volume label of "SMALL". Partition 4 has NTFS file system and a volume label of "misc".
LACBFT-5562	Partition 1: exFAT, no name, Partition 2: Microsoft NTFS, name: NTFS, Partition 3: Microsoft FAT32, name: SMALL, Partition 4: Microsoft NTFS, name: misc
LN7VWF-5562	(D:) - exFAT 1.79GB - NFTS (G:) NTFS 1000MB - SMALL (H:) 500MB FAT32 - misc (J:) 498MB NTFS
LRRKGT-5562	Partition 1 exfat NONAME, Partition 2 NTFS NTFS, Partition 3 FAT32 Small , Partition 4 NTFS misc
M2VAHU-5562	(1,2,3,4), (ExFAT,NTFS ,FAT32,NTFS), and (Unlabeled Volume,NTFS,SMALL,misc)
MD7R7R-5562	Partition 1, exFAT, NONAME, Partition 2, NTFS, NTFS, Partition 3, FAT32, SMALL, Partition 4, NTFS, misc
MQXA6Q-5562	Partition1, exFAT, HAS NO VOLUME\PARTITION NAME; Partition 2, NTFS, NTFS; Partition 3, FAT32, SMALL; Partition 4, NTFS, misc

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 31 - Removable Media 25-5562	
WebCode Test	**Response**
MV6VTN-5562	Partition 1, exFAT, NO NAME; Partition 2, NTFS, NTFS; Partition 3, FAT32, SMALL; Partition 4, NTFS, misc
Q2Z3GD-5562	Partition 1: exFAT, no volume name ; Partition 2: NTFS, "NTFS" ; Partition 3: FAT32, "SMALL", Partition 4: NTFS, "misc"
QCLZQR-5562	Partition 1-exFAT-no name, Partition 2-Microsoft NTFS-NTFS. Partition 3-Microsoft FAT32-SMALL, Partition 4-Microsoft NTFS-misc
QH4FBN-5562	1 (F, exFAT), 2 (H, NTFS); 3 (I, FAT32); 4 (J, NTFS)
T8JQPN-5562	1 - exFAT - "NONAME" ; 2 - NTFS - "NTFS" ; 3 - NTFS - "SMALL" ; 4 - NTFS - "misc"
THHLMJ-5562	Partition 1: exFAT, Partition 2: NTFS + NTSF, Partition 3: FAT32 + SMALL, Partition 4: NTFS + misc
TRHDUP-5562	Partition 1, [exFAT], NONAME; Partition 2, [NTFS], NTFS; Partition 3,[FAT32], SMALL; Partition 4, [NTFS], misc.
TVPPWK-5562	Partition 1: ExFAT NONAME; Partition 2: NTFS NTFS; Partition 3: FAT32 SMALL; Partition 4: NTFS small
U3GARK-5562	Partition 1\NONAME [exFAT]; Partition 2\NTFS[NTFS]; Partition 3\SMALL[FAT32]; Partition 4\misc[NTFS]
U4CRUL-5562	Partition 1 is an EXFAT filesystem and its volume name is NONAME. Partition 2 is an NTFS filesystem and its volume name is NTFS. Partition 3 is a FAT32 filesystem and its volume name is SMALL. Partition 4 is an NTFS filesystem and its volume name is misc.
UT9WBG-5562	Partition 1: exFAT, No Volume name / Partition 2: NTFS, Volume name: NTFS / Partition 3: FAT32, Volume name: SMALL / Partition 4: NTFS, Volume name: misc
V63DZH-5562	Partition1: exFAT, NONAME, Partition2: NTFS, NTFS, Partition3: FAT32, SMALL, Partition4: NTFS, misc

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 31 - Removable Media 25-5562	
WebCode Test	**Response**
VJJLKL-5562	Partition 1 – exFAT – no name, Partition 2 – NTFS – NTFS, Partition 3 - FAT32 – SMALL, Partition 4 – NTFS – misc
W7CX8H-5562	Part. Nr. 1: Filesystem=exFAT, name/label=<empty> ; Part. Nr. 2: Filesystem=NTFS, name/label=NTFS ; Part. Nr. 3: Filesystem=FAT32, name/label=SMALL ; Part. Nr. 4: Filesystem=NTFS, name/label=misc
WH87QK-5562	Partition 1 - exFAT - No Name, Partition 2 - NTFS - NTFS, Partition 3 - FAT32 - SMALL, Partition 4 - NTFS - misc
WKE9TJ-5562	Partition #: 1, Filesystem: exFAT, Volume Name/Label: ; Partition #: 2, Filesystem: NTFS, Volume Name/Label: NTFS; Partition #: 3, Filesystem: FAT32, Volume Name/Label: SMALL; Partition #: 4, Filesystem: NTFS, Volume Name/Label: misc
WVD7FJ-5562	Partition 1 filesystem: exFAT, volume name: NONAME, Partition 2 filesystem: NTFS, volume name: NTFS, Partition 3 filesystem: FAT32, volume name: SMALL, Partition 4 filesystem: NTFS, volume name: misc
X9VFGE-5562	C:\Users\thomas\Desktop\philly_2.pdf
XDUKGE-5562	Partition 1 is formatted as exFAT with no label; Partition 2 is formatted as NTFS with "NTFS" as the label; Partition 3 is formatted as FAT32 with "SMALL" as the label; Parition 4 is formatted as NTFS with "misc" as the label
XGRD6G-5562	Partition 1; NONAME (exFAT), Partition 2; NTFS (NTFS), Partition 3; SMALL (FAT32) , Partition 4; misc (NFTS)
XMC987-5562	partition number:04, file system: exFAT, NTFS, FAT32 & NTFS volume name/ label for all partitions: MBR Partition 1/Unlabeled EXFAT Partition, MBR Partition 2/Unlabeled NTFS Partition, MBR Partition 3/NO NAME & MBR Partition 4/Unlabeled NTFS Partition
XY6VCG-5562	Partition 1: exFAT, NONAME, Partition 2: NTFS, NTFS Partition 3: FAT32, SMALL Partition 4: NTFS, misc
Z8XMWF-5562	(Partition 1, exFAT, NONAME), (Partition 2, NTFS, NTFS), (Partition 3, FAT32, SMALL), (Partition 4, NTFS, misc)
ZNK3ZC-5562	1- Partition @ 128 ExFAT No Name, 2- Partition @ 3764352 NTFS NTFS, 3- Partition @ 5812351 NTFS No Name, 4- Partition @ 5812352 FAT32 SMALL, 5- Partition @ 6842368 NTFS misc

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 31 - Removable Media 25-5562	
WebCode Test	**Response**
ZRL9H3-5562	Partition 1 (exFAT), Partition 2 (NTFS)'NTFS', Partition 3 (FAT32) 'SMALL', Partition 4 (NTFS) 'misc'
ZZUWEA-5562	C/No name/EXFAT, D/NTFS/NTFS, E/SMALL/FAT32, F/misc/NTFS

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 31: Identify the filesystem on each partition on this device. Provide partition number, filesystem, and volume name/label for all partitions.

Consensus Result:

1. exFat, [unnamed / NONAME]
2. NTFS, "NTFS"
3. FAT32, "SMALL"
4. NTFS, "misc"
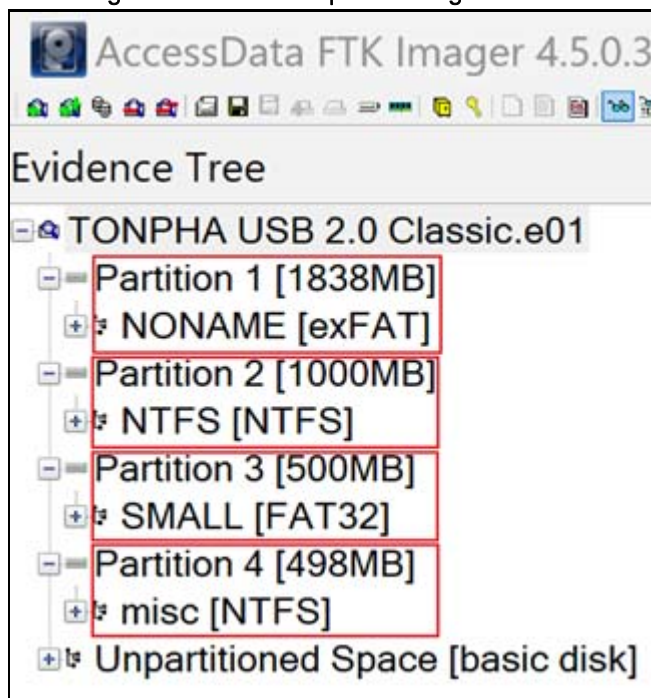
Manufacturer's Response Explanation:

There are four partitions on this device.

Manufacturer's Response Illustration:

X-Ways view of device partitioning

Name	Description	Type	Full path
Carved files	virtual (for examination purposes)		\Carved files
Start sectors	virtual (for examination purposes)		\Start sectors
Partition 1 (G:)	partition, existing	exFAT	\Partition 1 (G:)
Partition 2 (H:)	partition, existing	NTFS	\Partition 2 (H:)
Partition 3 (I:)	partition, existing	FAT32	\Partition 3 (I:)
Unpartitioned space	virtual (for examination purposes)		\Unpartitioned space
Partition 4 (J:)	partition, existing	NTFS	\Partition 4 (J:)
Unpartitionable space	virtual (for examination purposes)		\Unpartitionable space

25-5561 TONPHA USB 2.0 Classic
Partitioning style: MBR

FTK Imager view of device partitioning

AccessData FTK Imager 4.5.0.3

Evidence Tree

TONPHA USB 2.0 Classic.e01
- Partition 1 [1838MB]
  - NONAME [exFAT]
- Partition 2 [1000MB]
  - NTFS [NTFS]
- Partition 3 [500MB]
  - SMALL [FAT32]
- Partition 4 [498MB]
  - misc [NTFS]
- Unpartitioned Space [basic disk]

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 31 - Removable Media 25-5562

Windows view of device partitioning

Disk 3
Basic
3.75 GB
Read Only

(E:)	NTFS (G:)	SMALL (H:)	misc (I:)
1.79 GB exFAT	1000 MB NTFS	500 MB FAT32	498 MB NTFS
Healthy (Primary Pa	Healthy (Primary F	Healthy (Primar	Healthy (Priman

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 32 - Removable Media 25-5562

Question 32: What is the full path (partition name\parent directory\file) for the picture file which lists "Collaborative" as the Creator/Author?

Manufacturer's Response: [Partition1 NONAME]\50 E. Ramblewood St..jpeg

WebCode Test	Response
2RG9U9-5562	Partition 1 Unallocated\50 E. Ramblewood St..jpeg
349ZFC-5562	USB Thumb Drive.E01/Partition 1/NONAME [exFAT]/[root]/50 E. Ramblewood St..jpeg
3J4DXE-5562	Partition 1\50 E. Ramblewood St..jpeg
4ZJ2KE-5562	/Partition 1/NONAME [exFAT]/[root]/50 E. Ramblewood St..jpeg
673VQB-5562	NONAME\50 E. Ramblewood St..jpeg
8FPDKA-5562	[Partition 1]\ 50 E. Ramblewood St..jpeg
8TBZD8-5562	Not in scope.
8WNN47-5562	Patition1\50 E. Ramblewood St..jpeg
A444U7-5562	Partition 1 [1838MB]\NONAME [exFAT]\[root]\50 E. Ramblewood St..jpeg
AUY2L3-5562	\50 E. Ramblewood St..jpeg
BEGRX4-5562	NONAME\[root]\50 E. Ramblewood St..jpeg
BTXP36-5562	Partition 1\NONAME\exFAT\root\50 E. Ramblewood St.jpeg
CTEYRY-5562	Partition 1\[root]\50 E. Ramblewood St..jpeg
DJLBA2-5562	Partition 1/NONAME [exFAT]/[root]/50 E. Ramblewood St..jpeg
E6FEQZ-5562	CTS_USB_2025.E01/Partition 1/NONAME [exFAT]/[root]/50 E. Ramblewood St..jpeg
EYTN7P-5562	Partition 1(Noname)/50 E. Ramblewood St..jpeg
F4KDZ3-5562	vol_vol2/50 E. Ramblewood St..jpeg
FJ22JX-5562	USB1-CTS25-5562.E01\Partition @ 128\Root\50 E. Ramblewood St..jpeg
GA8D2Z-5562	Partition 1 \50 E. Ramblewood St..jpeg
GJP4GX-5562	Thumbdrive.E01\Partition 1\NONAME [exFAT]\[root]\50 E. Ramblewood St..jpeg

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 32 - Removable Media 25-5562	
WebCode Test	**Response**
GTHERT-5562	Partition 1exFAT\50 E. Ramblewood St..jpeg
GTZ73X-5562	NONAME\root\50 E. Ramblewood St..jpeg
HEX8ER-5562	Partition 1 (no name)\50 E. Ramblewood St..jpeg
HXUD8T-5562	partition 1\50 E. Ramblewood St..jpeg (The partition does not have a specific name, but it is the first in order. Additionally, there is no parent directory — the file is located directly in the root of the partition.)
HYZ6QT-5562	/Partition 1/NONAME [exFAT]/[root]/50 E. Ramblewood St..jpeg
JGEWDV-5562	Partition 1\50 E. Ramblewood St..jpeg
K7CZKT-5562	NONAME\[root]\50 E. Ramblewood St..jpeg
KA8UHU-5562	Partition 1\[Root]\50 E. Ramblewood St..jpeg
KYBNNV-5562	The full path of the picture file is NONAME\root\50 E. Ramblewood ST..jpeg
LACBFT-5562	P1\50 E. Ramblewood St..jpeg
LN7VWF-5562	image.Ex01\Partition @ 128\Root\50 E. Ramblewood St..jpeg
LRRKGT-5562	/Partition 1/NONAME [Exfat]/[root]/50 E. Ramblewood st..jpeg
M2VAHU-5562	Partition 1(Unlabeled Volume)\50 E. Ramblewood St..jpeg
MD7R7R-5562	Partition 1\50 E. Ramblewood St..jpeg
MQXA6Q-5562	50 E. Ramblewood St..jpeg
MV6VTN-5562	Partition 1 (NO NAME)\50 E. Ramblewood St..jpeg
Q2Z3GD-5562	Partition 1\50 E. Ramblewood St..jpeg
QCLZQR-5562	Partition 1/NONAME [exFAT]/[root]/50 E. Ramblewood St..jpeg
QH4FBN-5562	Partition 1(exFAT 1.79GB)\50 E. Ramblewood St.jpg
T8JQPN-5562	"NONAME"\50 E. Ramblewood St..jpeg
THHLMJ-5562	Partition 1\50 E.Ramblewood St..jpeg
TRHDUP-5562	Partition 1/NONAME [exFAT]/[root]/50 E. Ramblewood St..jpeg

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 32 - Removable Media 25-5562	
WebCode Test	**Response**
TVPPWK-5562	Partition 1\NONAME [exFAT]\[root]\50 E. Ramblewood St..jpeg
U3GARK-5562	Partition1\NONAME[exFAT]\[root]\50 E. Ramblewood St.jpeg
U4CRUL-5562	NONAME\[root]\50 E. Ramblewood St..jpeg
UT9WBG-5562	Partition 3/Users/thomas/Documents/
V63DZH-5562	NONAME:\50 E. Ramblewood St..jpeg, Partition 1/50 E. Ramblewood St..jpeg
VJJLKL-5562	Partition 1/NONAME [exFAT]/[root]/50 E. Ramblewood St..jpeg
W7CX8H-5562	[PARTITION 1: <no name>][root][50 E. Ramblewood St..jpeg]
WH87QK-5562	Partition 1/NONAME [exFAT]/[root]/50 E. Ramblewood St..jpeg
WKE9TJ-5562	Partition 1\NONAME [exFAT]\[root]\50 E. Ramblewood St..jpeg (Partition 1\50 E. Ramblewood St..jpeg)
WVD7FJ-5562	Partition 1\50 E. Ramblewood St..jpeg
X9VFGE-5562	C:\Users\thomas\Downloads\nevergonnagiveyouup.exe
XDUKGE-5562	[Partition 1]\[root]\50 E. Ramblewood St..jpeg
XGRD6G-5562	Partition 1\NONAME [exFAT]\[root]\50 E. Ramblewood St..jpg
XMC987-5562	E:\ 50 E. Ramblewood St..jpeg
XY6VCG-5562	Partition 1: NONAME\50 E. Ramblewood St..jpeg
Z8XMWF-5562	Partition 1/NONAME [exFAT]/[root]/50 E. Ramblewood St..jpeg
ZNK3ZC-5562	\Partition @ 128\Root\50 E. Ramblewood St..jpeg
ZRL9H3-5562	Partion 1\50 E. Ramblewood St..jpeg
ZZUWEA-5562	C:\50 E. Ramblewood St..jpeg

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 32 - Removable Media 25-5562

Question 32: What is the full path (partition name\parent directory\file) for the picture file which lists "Collaborative" as the Creator/Author?

Consensus Result:

[Partition1 NONAME]\50 E. Ramblewood St..jpeg

Manufacturer's Response Explanation:

This value is contained in the EXIF metadata for the jpg image file and can be searched and parsed with most forensic tools.

Manufacturer's Response Illustration:

X-Ways file information

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 33 - Removable Media 25-5562

Question 33: On the device is a purple-bordered photo of a black dog running on a beach. Provide the text that appears in the image.

<u>Manufacturer's Response:</u>   CTS2025-D25

WebCode Test	Response
2RG9U9-5562	CTS2025-D25
349ZFC-5562	CTS2025-D25
3J4DXE-5562	CTS2025-D25
4ZJ2KE-5562	CTS2025-D25
673VQB-5562	CTS2025-D25
8FPDKA-5562	CTS2025-D25
8TBZD8-5562	CTS2025-D25
8WNN47-5562	CTS2025-D25
A444U7-5562	CTS2025-D25
AUY2L3-5562	CTS2025-D25
BEGRX4-5562	CTS2025-D25
BTXP36-5562	CTS2025-D25
CTEYRY-5562	CTS2025-D25
DJLBA2-5562	CTS2025-D25
E6FEQZ-5562	CTS2025-D25
EYTN7P-5562	CTS2025-D25
F4KDZ3-5562	CTS2025-D25
FJ22JX-5562	CTS2025-D25
GA8D2Z-5562	CTS2025-D25
GJP4GX-5562	CTS2025-D25

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

WebCode Test	Response
GTHERT-5562	CTS2025-D25
GTZ73X-5562	CTS2025-D25
HEX8ER-5562	CTS2025-D25
HXUD8T-5562	CTS2025-D25
HYZ6QT-5562	CTS2025-D25
JGEWDV-5562	CTS2025-D25
K7CZKT-5562	CTS2025-D25
KA8UHU-5562	CTS2025-D25
KYBNNV-5562	The text that on the provided image is "CTS2025-D25".
LACBFT-5562	CTS2025-D25
LN7VWF-5562	[Participant did not return results for this question.]
LRRKGT-5562	CTS2025-D25
M2VAHU-5562	CTS2025-D25
MD7R7R-5562	CTS2025-D25
MQXA6Q-5562	CTS2025-D25
MV6VTN-5562	CTS2025-D25
Q2Z3GD-5562	CTS2025-D25
QCLZQR-5562	CTS2025-D25
QH4FBN-5562	CTS2025-D25
T8JQPN-5562	CTS2025-D25
THHLMJ-5562	CTS2025-D25
TRHDUP-5562	CTS2025-D25

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 33 - Removable Media 25-5562	
WebCode Test	**Response**
TVPPWK-5562	CTS2025-D25
U3GARK-5562	CTS2025-D25
U4CRUL-5562	CTS2025-D25
UT9WBG-5562	CTS2025-D25
V63DZH-5562	CTS2025-D25
VJJLKL-5562	CTS2025-D25
W7CX8H-5562	CTS2025-D25
WH87QK-5562	CTS2025-D25
WKE9TJ-5562	CTS2025-D25
WVD7FJ-5562	CTS2025-D25
X9VFGE-5562	cat.xcf
XDUKGE-5562	CTS2025-D25
XGRD6G-5562	CTS2025-D25
XMC987-5562	Every single day
XY6VCG-5562	CTS2025-D25
Z8XMWF-5562	CTS2025-D25
ZNK3ZC-5562	CTS2025-D25
ZRL9H3-5562	CTS2025-D25
ZZUWEA-5562	CTS2025-D25

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 33 - Removable Media 25-5562

Question 33: On the device is a purple-bordered photo of a black dog running on a beach. Provide the text that appears in the image.
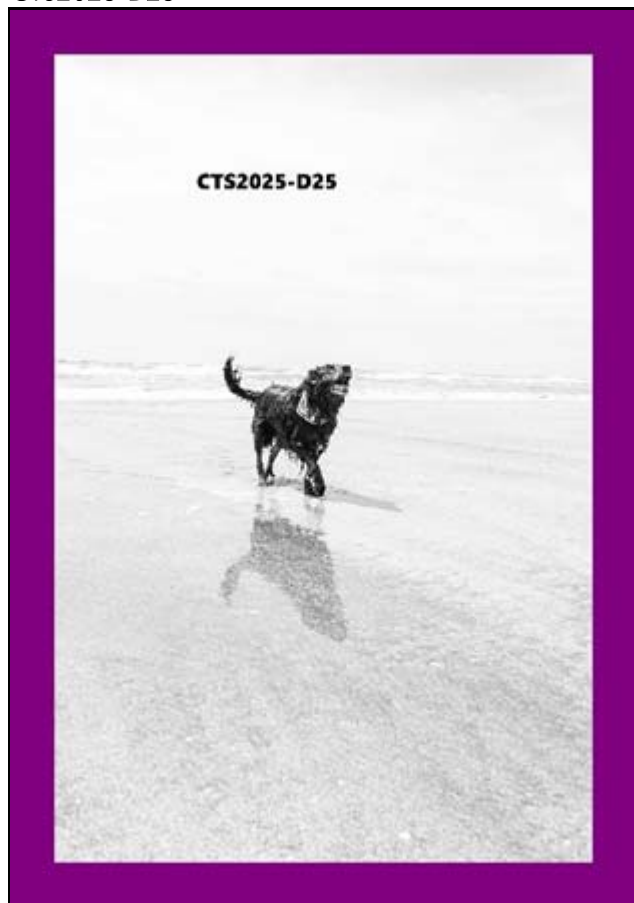
Consensus Result:

CTS2025-D25

Manufacturer's Response Explanation:

This photo was deleted and left in unallocated space. A forensic file recovery (carving) tool will recover files from unallocated space.

Manufacturer's Response Illustration:

CTS2025-D25

CTS2025-D25

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 34 - Removable Media 25-5562

Question 34: Provide the filetype (file format) for the file with SHA256 hash DD8F4F698DDEEA89BEEAF02ECD61453DB7E00947B6E488CE8E4ABEDA33B4FA28.

<u>Manufacturer's Response:</u>   Text file

WebCode Test	Response
2RG9U9-5562	Raw Text/Plain Text
349ZFC-5562	7 bit text
3J4DXE-5562	text/plain
4ZJ2KE-5562	7 bit text format
673VQB-5562	7bit text
8FPDKA-5562	Text
8TBZD8-5562	ASCII
8WNN47-5562	Text
A444U7-5562	plain text file, Unformatted text file.
AUY2L3-5562	ascii
BEGRX4-5562	Raw ASCII Text/Placeholder file (7-bit-text)
BTXP36-5562	7 bit text
CTEYRY-5562	7 bit text
DJLBA2-5562	7 bit file
E6FEQZ-5562	7 bit text
EYTN7P-5562	TXT (plain text)
F4KDZ3-5562	Plain text
FJ22JX-5562	Text File
GA8D2Z-5562	text file
GJP4GX-5562	TXT

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 34 - Removable Media 25-5562	
WebCode Test	**Response**
GTHERT-5562	.txt
GTZ73X-5562	.txt
HEX8ER-5562	Plain text
HXUD8T-5562	text/plain
HYZ6QT-5562	Plain Text (.txt)
JGEWDV-5562	text/plain
K7CZKT-5562	A file with this hash value was not located on the supplied USB Flash Drive
KA8UHU-5562	ascii
KYBNNV-5562	The file with the provided SHA256 hash value appears to be a text file.
LACBFT-5562	Text file
LN7VWF-5562	[Participant did not return results for this question.]
LRRKGT-5562	Text File
M2VAHU-5562	.txt
MD7R7R-5562	text file
MQXA6Q-5562	Plain text
MV6VTN-5562	None, basic 'text' file. Text only with generic text: 'Lorum ipsum.....'
Q2Z3GD-5562	txt
QCLZQR-5562	plain text
QH4FBN-5562	ascii
T8JQPN-5562	raw text
THHLMJ-5562	7-bit ASCII (Plain Text)
TRHDUP-5562	Plain text 7-bit ASCII

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 34 - Removable Media 25-5562	
WebCode Test	**Response**
TVPPWK-5562	text file
U3GARK-5562	7 bit text (\ Partition 4\misc [NTFS]\[root]\k\file)
U4CRUL-5562	7-bit text
UT9WBG-5562	.txt (plain text)
V63DZH-5562	The file is a plain text file (.txt).
VJJLKL-5562	7 bit text
W7CX8H-5562	text/plain; charset='ascii'
WH87QK-5562	plain text file
WKE9TJ-5562	7-bit text
WVD7FJ-5562	7 bit text
X9VFGE-5562	file.txt
XDUKGE-5562	Plain Text
XGRD6G-5562	7 bit text
XMC987-5562	E:\50 E.Ramblewood St..jpeg
XY6VCG-5562	Ascii
Z8XMWF-5562	A regular file named "file" that contains Latin text in relation to "Lorem ipsum".
ZNK3ZC-5562	Text
ZRL9H3-5562	ascii , plain text
ZZUWEA-5562	Document

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 34 - Removable Media 25-5562

Question 34: Provide the filetype (file format) for the file with SHA256 hash DD8F4F698DDEEA89BEEAF02ECD61453DB7E00947B6E488CE8E4ABEDA33B4FA28.
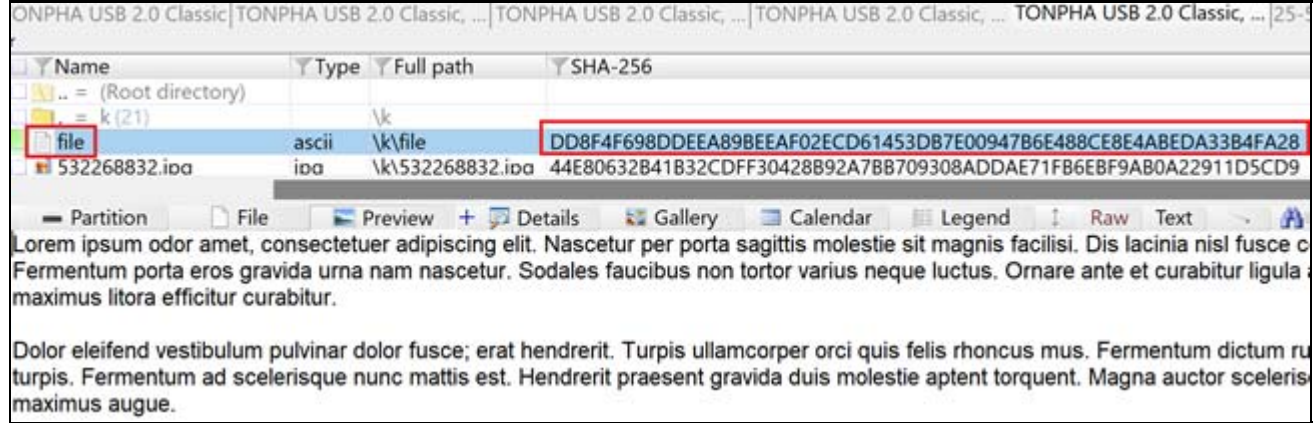
<u>Consensus Result:</u>

Text file

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

The specified hash identifies [Partition4, misc]\file. This file has no extension but contains ascii encoded readable text.

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

X-Ways view of [Partition4, misc]\file

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 35 - Removable Media 25-5562

Question 35: Provide the Windows Security Identifier (SID) of the user account that is the owner of files in the "k" directory.

<u>Manufacturer's Response:</u> S-1-5-21-3142915031-3623484693-281401572-1001

WebCode Test	Response
2RG9U9-5562	S-1-5-21-3142915031-3623484693-281401572-1001
349ZFC-5562	S-1-5-21-3142915031-3623484693-281401572-1001
3J4DXE-5562	S-1-5-21-3190731067-2237959463-3261579367-1001
4ZJ2KE-5562	S-1-5-21-3142915031-3623484693-281401572-1001
673VQB-5562	S-1-5-21-3142915031-3623484693-281401572-1001
8FPDKA-5562	S-1-5-21-3142915031-3623484693-281401572-1001
8TBZD8-5562	Not in scope.
8WNN47-5562	S-1-5-21-3142915031-3623484693-281401572-1001
A444U7-5562	S-1-5-21-3142915031-3623484693-281401572-1001
AUY2L3-5562	S-1-5-21-3142915031-3623484693-281401572-1001
BEGRX4-5562	S-1-5-21
BTXP36-5562	S-1-5-21-3190731067-2237959463-3261579367-1001
CTEYRY-5562	S-1-5-21-3142915031-3623484693-281401572-1001
DJLBA2-5562	S-1-5-21-3142915031-3623484693-281401572-1001
E6FEQZ-5562	S-1-5-21-3142915031-3623484693-281401572-1001
EYTN7P-5562	S-1-5-21-3142915031-3623484693-281401572-1001
F4KDZ3-5562	S-1-5-21-3142915031-3623484693-281401572 with a RID of 1001
FJ22JX-5562	S-1-5-21-3142915031-3623484693-281401572-1001
GA8D2Z-5562	S-1-5-21-3142915031-3623484693-281401572-1001
GJP4GX-5562	S-1-5-21-3142915031-3623484693-281401572-1001

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 35 - Removable Media 25-5562
WebCode Test	**Response**
GTHERT-5562	S-1-5-21-3142915031-3623484693-281401572-1001
GTZ73X-5562	S-1-5-21-3142915031-3623484693-281401572-1001
HEX8ER-5562	S-1-5-21-3142915031-3623484693-281401572-1001
HXUD8T-5562	S-1-5-21-3142915031-3623484693-281401572-1001
HYZ6QT-5562	S-1-5-21-3142915031-3623484693-281401572-1001
JGEWDV-5562	S-1-5-21-3142915031-3623484693-281401572-1001
K7CZKT-5562	S-1-5-21-3142915031-3623484693-281401572-1001
KA8UHU-5562	S-1-5-21-3142915031-3623484693-281401572-1001
KYBNNV-5562	The Windows SID of the user account that is the owner of the files in the "k" directory is S-1-5-21-3142915031-3623484693-281401572-1001
LACBFT-5562	S-1-5-21-3142915031-3623484693-281401572-1001
LN7VWF-5562	S-1-5-21-3142915031-3623484693-281401572-1001
LRRKGT-5562	268 (S-1-5-21-3142915031-3623484693-281401572-1001)
M2VAHU-5562	S-1-5-21-3142915031-3623484693-281401572-1001
MD7R7R-5562	S-1-5-21-3142915031-3623484693-281401572-1001
MQXA6Q-5562	268 (S-1-5-21-3142915031-3623484693-281401572-1001)
MV6VTN-5562	S-1-5-21-31429-15031-3623484693-281401572-1001
Q2Z3GD-5562	S-1-5-21-3142915031-3623484693-281401572-1001
QCLZQR-5562	S-1-5-21-314291531-3623484693-281401572-1001
QH4FBN-5562	268 (S-1-5 .... 1001)
T8JQPN-5562	S-1-5-21-3142915031-3623484693-281401572-1001
THHLMJ-5562	S-1-5-21-3142915031-3623484693-281401572-1001
TRHDUP-5562	S-1-5-21-3142915031-3623484693-281401572-1001

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 35 - Removable Media 25-5562	
WebCode Test	**Response**
TVPPWK-5562	S-1-5-21-3142915031-3623484693-281401572-1001
U3GARK-5562	S-1-5-21-3142915031-3623484693-281401572-1001
U4CRUL-5562	S-1-5-21-3142915031-3623484693-281401572-1001
UT9WBG-5562	S-1-5-21-3190731067-2237959463-3261579367-1001
V63DZH-5562	S-1-5-21-3190731067-2237959463-3261579367-1001
VJJLKL-5562	S-1-5-21-3142915031-3623484693-281401572-1001
W7CX8H-5562	S-1-5-21-3142915031-3623484693-281401572-1001
WH87QK-5562	S-1-5-21-3142915031-3623484693-281401572-1001
WKE9TJ-5562	S-1-5-21-3142915031-3623484693-281401572-1001
WVD7FJ-5562	S-1-5-21-3190731067-2237959463-3261579367-1001
X9VFGE-5562	S-1-5-21-3142915031-3623484693-281401572-1001
XDUKGE-5562	S-1-5-21-3142915031-3623484693-281401572-1001
XGRD6G-5562	S-1-5-21-3142915031-3623484693-281401572-1001
XMC987-5562	S-1-5-21-3623811015-3361044348-30300820-1001
XY6VCG-5562	S-1-5-21-3142915031-3623484693-281401572-1001
Z8XMWF-5562	S-1-5-21-3142915031-3623484693-281401572-1001
ZNK3ZC-5562	S-1-5-21-3142915031-3623484693-281401572-1001
ZRL9H3-5562	S-1-5-21-3190731067-2237959463-3261579367-1001
ZZUWEA-5562	S-1-5-21-3142915031-3623484693-281401572-1001

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 35 - Removable Media 25-5562

Question 35: Provide the Windows Security Identifier (SID) of the user account that is the owner of files in the "k" directory.

<u>Consensus Result:</u>

S-1-5-21-3142915031-3623484693-281401572-1001

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

NTFS file permissions often follow files copied to removable media. The Security Identifier (SID) for these files, S-1-5-21-3142915031-3623484693-281401572-1001, identifies the owner account and domain (or computer).

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

X-Ways view of NTFS partition files with ownership information

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 36 - Removable Media 25-5562

Question 36: Provide the username corresponding with the SID identified in question 35.

Manufacturer's Response: thomas

WebCode Test	Response
2RG9U9-5562	thomas
349ZFC-5562	thomas
3J4DXE-5562	thomas
4ZJ2KE-5562	thomas
673VQB-5562	Thomas
8FPDKA-5562	thomas
8TBZD8-5562	Not in scope.
8WNN47-5562	thomas
A444U7-5562	thomas
AUY2L3-5562	thomas
BEGRX4-5562	Thomas
BTXP36-5562	Thomas
CTEYRY-5562	thomas
DJLBA2-5562	thomas
E6FEQZ-5562	thomas
EYTN7P-5562	thomas
F4KDZ3-5562	thomas
FJ22JX-5562	thomas
GA8D2Z-5562	thomas
GJP4GX-5562	thomas
GTHERT-5562	thomas

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 36 - Removable Media 25-5562	
WebCode Test	**Response**
GTZ73X-5562	thomas
HEX8ER-5562	thomas
HXUD8T-5562	thomas
HYZ6QT-5562	thomas
JGEWDV-5562	thomas
K7CZKT-5562	thomas
KA8UHU-5562	thomas
KYBNNV-5562	The user account that has the SID from question 35 is "thomas".
LACBFT-5562	thomas
LN7VWF-5562	thomas
LRRKGT-5562	thomas
M2VAHU-5562	thomas
MD7R7R-5562	thomas
MQXA6Q-5562	thomas
MV6VTN-5562	thomas
Q2Z3GD-5562	thomas
QCLZQR-5562	thomas
QH4FBN-5562	thomas
T8JQPN-5562	thomas
THHLMJ-5562	Thomas
TRHDUP-5562	thomas
TVPPWK-5562	thomas

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 36 - Removable Media 25-5562	
WebCode Test	**Response**
U3GARK-5562	Thomas
U4CRUL-5562	thomas
UT9WBG-5562	Thomas
V63DZH-5562	thomas
VJJLKL-5562	thomas
W7CX8H-5562	thomas
WH87QK-5562	thomas
WKE9TJ-5562	thomas
WVD7FJ-5562	thomas
X9VFGE-5562	thomas
XDUKGE-5562	thomas
XGRD6G-5562	thomas
XMC987-5562	zion
XY6VCG-5562	Thomas
Z8XMWF-5562	thomas
ZNK3ZC-5562	thomas
ZRL9H3-5562	k
ZZUWEA-5562	thomas

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 36 - Removable Media 25-5562

Question 36: Provide the username corresponding with the SID identified in question 35.

<u>Consensus Result:</u>

thomas

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

NTFS file permissions often follow files copied to removable media. The Security Identifier (SID) for these files, S-1-5-21-3142915031-3623484693-281401572-1001, identifies the owner's account and domain (or computer). In this case, it is possible to match this SID with the one recovered from files on the 25-5561-001.E01 evidence file.

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

RegRipper Parse of the SAM registry hive from 25-5561 showing thomas' SID

```
   NTUSER.Ripped.txt    SAM.Ripped.txt    Security.Ripped.txt    Software.Ripped.txt    System.Ripped.txt
70  Username      : thomas [1001]
71  SID           : S-1-5-21-3142915031-3623484693-281401572-1001
72  Full Name     :
```

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 37 - Removable Media 25-5562

Question 37: Provide the file header (file signature, in ASCII) of the file containing the keyword "arcseconds".

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

WebCode Test	Response
2RG9U9-5562	Header of "CmnD". This was recovered from the file named "icudtl.dat" which was located at "\E\Windows\Globalization\ICU\" (File Offset 23548462) . This path location was within the provided .E01 of the computer and not the USB.
349ZFC-5562	53494D504C4520203D2020202020202020202020202020202020202020202054202F205772697474656E2062792049444C3A202053756E205365702032312031383A32303A30322032303033202020202020 ; SIMPLE = T / Written by IDL: Sun Sep 21 18:20:02 2003
3J4DXE-5562	SIMPLE
4ZJ2KE-5562	SIMPLE = T / Written by IDL: Sun Sep 21 18:20:02 2003
673VQB-5562	SIMPLE
8FPDKA-5562	The header hex is "1F 8B." I can't input the value in ASCII because 1F is not printable in ASCII.
8TBZD8-5562	SIMPLE = T
8WNN47-5562	1F 8B 08
A444U7-5562	[Participant did not return results for this question.]
AUY2L3-5562	SIMPLE = T / Written by IDL: Sun Sep 21 18:20:02 2003 BIT
BEGRX4-5562	..U' (icudtl.dat 25-5561-001.E01),, "SIMPLE" (trac_171_a0_20030916_080907.fts CTS2025-USB.E01)
BTXP36-5562	53 49 4D 50 4C 45 - SIMPLE
CTEYRY-5562	SIMPLE = T
DJLBA2-5562	SIMPLE
E6FEQZ-5562	SIMPLE = T / Written by IDL: Sun Sep 21 18:20:02 2003
EYTN7P-5562	SIMPLE
F4KDZ3-5562	SIMPLE as in a FITS file format
FJ22JX-5562	SIMPLE =
GA8D2Z-5562	SIMPLE

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 37 - Removable Media 25-5562	
WebCode Test	**Response**
GJP4GX-5562	SIMPLE
GTHERT-5562	SIMPLE = T / Written by IDL: Sun Sep 21 18:20:02 2003
GTZ73X-5562	SIMPLE
HEX8ER-5562	SIMPLE = T
HXUD8T-5562	SIMPLE = T /
HYZ6QT-5562	SIMPLE = T
JGEWDV-5562	SIMPLE
K7CZKT-5562	SIMPLE
KA8UHU-5562	SIMPLE
KYBNNV-5562	The file header in ASCII for the file containing "Arcseconds" is "SIMPLE".
LACBFT-5562	53 49 4D 50 4C 45 20 20
LN7VWF-5562	9000DA271400000000000200436D6E4401000000030000020436F707972696967687420284329 2032
LRRKGT-5562	SIMPLE = T
M2VAHU-5562	SIMPLE = T / Written by IDL: Sun Sep 21 18:20:02 2003
MD7R7R-5562	SIMPLE = T
MQXA6Q-5562	SIMPLE = T
MV6VTN-5562	SIMPLE, 53 49 4D 50 4C 45, '.FTS' file
Q2Z3GD-5562	SIMPLE = T
QCLZQR-5562	SIMPLE
QH4FBN-5562	SIMPLE
T8JQPN-5562	SIMPLE
THHLMJ-5562	SIMPLE = T / Written by IDL: Sun Sep 21 18:20:02 2003

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 37 - Removable Media 25-5562	
WebCode Test	**Response**
TRHDUP-5562	SIMPLE =
TVPPWK-5562	SIMPLE
U3GARK-5562	Simple (53 49 4D 50 4C 45)
U4CRUL-5562	SIMPLE
UT9WBG-5562	ResB
V63DZH-5562	"SIMPLE "(53 49 4D 50 4C 45 20 20)
VJJLKL-5562	SIMPLE
W7CX8H-5562	SIMPLE
WH87QK-5562	SIMPLE
WKE9TJ-5562	SIMPLE
WVD7FJ-5562	SIMPLE
X9VFGE-5562	12382975864_09e6e069e7_o.jpg
XDUKGE-5562	SIMPLE
XGRD6G-5562	SIMPLE
XMC987-5562	Simple
XY6VCG-5562	SIMPLE
Z8XMWF-5562	SIMPLE
ZNK3ZC-5562	SIMPLE = T
ZRL9H3-5562	SIMPLE = T / Written by IDL: Sun Sep 21 18:20:02 2003
ZZUWEA-5562	Not sure

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 37 - Removable Media 25-5562

Question 37: Provide the file header (file signature, in ASCII) of the file containing the keyword "arcseconds".
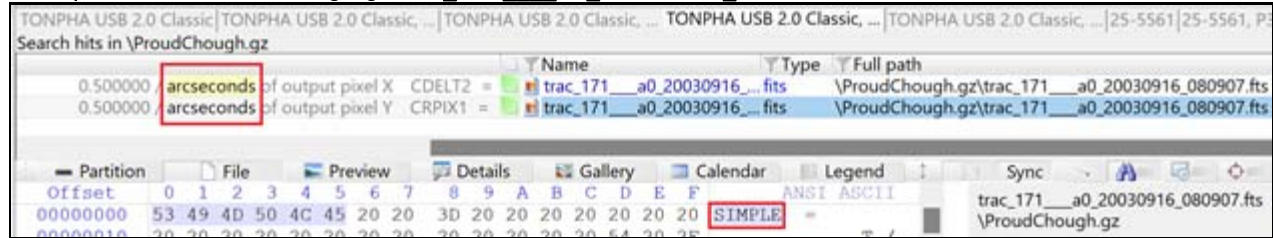
Consensus Result:

SIMPLE

Manufacturer's Response Explanation:

The keyword "arcseconds" is found in trac_171____a0_20030916_080907.fts, a file inside the compressed gzip archive ProudChough.gz on the first partition.

Manufacturer's Response Illustration:

X-Ways view of \ProudChough.gz\trac_171____a0_20030916_080907.fts

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 38 - Removable Media 25-5562

Question 38: Provide the title (not the filename) of the document authored by David McGuirk.

<u>Manufacturer's</u>   NOAA GEO-IDE Plan
<u>Response</u>:

WebCode Test	Response
2RG9U9-5562	NOAA GEO-IDE Plan
349ZFC-5562	NOAA Global Earth Observation Integrated Data Environment (GEO-IDE)
3J4DXE-5562	NOAA GEO-IDE Plan
4ZJ2KE-5562	NOAA GEO-IDE Plan
673VQB-5562	NOAA Global Earth Observation Integrated Data Environment (GEO-IDE)
8FPDKA-5562	NOAA Global Earth Observation Integrated Data Environment (GEO-IDE)
8TBZD8-5562	NOAA GEO-IDE Plan
8WNN47-5562	NOAA GEO-IDE Plan
A444U7-5562	NOAA Global Earth Observation Integrated Data Environment (GEO-IDE)
AUY2L3-5562	NOAA Global Earth Observation Integrated Data Environment (GEO-IDE)
BEGRX4-5562	NOAA Global Earth Observation Integrated Data Environment (GEO-IDE)
BTXP36-5562	NOAA GLOBAL EARTH OBSERVATION INTEGRATED DATA ENVIRONMENT (GEO-IDE) PLAN
CTEYRY-5562	NOAA GEO-IDE Plan
DJLBA2-5562	NOAA GEO-IDE Plan
E6FEQZ-5562	NOAA Global Earth Observation Integrated Data Environment (GEO-IDE) ---DRAFT--- Version 2.6 13 March 2006
EYTN7P-5562	NOAA Global Earth Observation Integrated Data Environment (GEO-IDE)
F4KDZ3-5562	ExpensiveMink.doc
FJ22JX-5562	NOAA GEO-IDE Plan
GA8D2Z-5562	NOAA GEO-IDE Plan
GJP4GX-5562	NOAA Global Earth Observation Integrated Data Environment (GEO-IDE)
GTHERT-5562	NOAA GEO-IDE Plan

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 38 - Removable Media 25-5562	
WebCode Test	**Response**
GTZ73X-5562	NOAA GEO-IDE Plan
HEX8ER-5562	NOAA GEO-IDE Plan
HXUD8T-5562	NOAA GEO-IDE Plan
HYZ6QT-5562	NOAA GEO-IDE Plan
JGEWDV-5562	NOAA GEO-IDE Plan
K7CZKT-5562	NOAA GEO-IDE Plan
KA8UHU-5562	NOAA Global Earth Observation Integrated Data Environment (GEO-IDE) (NOTE: Metadata title is "NOAA GEO-IDE Plan")
KYBNNV-5562	The provided title of the document authored by David McGuirk is "NOAA Global Earth Observation Integrated Data Environment (GEO-IDE) --DRAFT-- version 2.6 13 March 2006"
LACBFT-5562	NOAA GEO-IDE Plan
LN7VWF-5562	NOAA Global Earth Observation Intergrated Data Environment (GEO-IDE)
LRRKGT-5562	NOAA Global Earth Observation Integrated Data Enviroment (GEO-IDE) Draft Version 2.6
M2VAHU-5562	NOAA GEO-IDE Plan
MD7R7R-5562	NOAA Global Earth Observation Integrated Data Environment (GEO-IDE)
MQXA6Q-5562	NOAA GEO-IDE Plan
MV6VTN-5562	NOAA Global Earth Observatory Integrated Data Environment
Q2Z3GD-5562	NOAA GEO-IDE Plan
QCLZQR-5562	NOAA GEO-IDE Plan
QH4FBN-5562	NOAA GEO-IDE Plan
T8JQPN-5562	NOAA GEO-IDE Plan
THHLMJ-5562	NOAA, Global Earth Observation, Integrated Data Environment (GEO-IDE)
TRHDUP-5562	NOAA GEO-IDE Plan
TVPPWK-5562	NOAA GEO-IDE Plan

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 38 - Removable Media 25-5562	
WebCode Test	**Response**
U3GARK-5562	NOAA Global Earth Observation Integrated Data Environment (GEO-IDE) Plan
U4CRUL-5562	NOAA GEO-IDE Plan
UT9WBG-5562	NOAA Global Earth Observation Integrated Data Environment (GEO-IDE) ---DRAFT--- Version 2.6 13 March 2006
V63DZH-5562	NOAA GEO-IDE Plan (ExpensiveMink.doc)
VJJLKL-5562	NOAA GEO-IDE Plan
W7CX8H-5562	From the metadata of the file: 'NOAA GEO-IDE Plan' ; From the title page of the file: 'NOAA Global Earth Observation Integrated Data Environment (GEO-IDE)'
WH87QK-5562	NOAA GEO-IDE Plan
WKE9TJ-5562	NOAA GEO-IDE Plan
WVD7FJ-5562	NOAA GEO-IDE Plan
X9VFGE-5562	philly_2.pdf
XDUKGE-5562	NOAA GEO-IDE Plan
XGRD6G-5562	NOAA Global Earth Observation Integrated Data Environment (GEO-IDE)
XMC987-5562	NOAA GEO-IDE Plan
XY6VCG-5562	NOAA GEO-IDE Plan
Z8XMWF-5562	NOAA GEO-IDE Plan
ZNK3ZC-5562	NOAA GEO-IDE Plan
ZRL9H3-5562	NOAA GEO_IDE Plan
ZZUWEA-5562	NOAA GEO-IDE Plan

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 38 - Removable Media 25-5562

Question 38: Provide the title (not the filename) of the document authored by David McGuirk.

Consensus Result:

NOAA GEO-IDE Plan

Manufacturer's Response Explanation:

Microsoft Word Documents enable the annotation of metadata with tags including author and title. Many forensic tools parse these values and enable searching for them.

Manufacturer's Response Illustration:

X-Ways view of ExpensiveMink.doc metadata

Summary Information

OS	Win32 5.1
Title	NOAA GEO-IDE Plan
Subject	
Author	David McGuirk
Keywords	
Comments	
Template	Normal.dot
Last saved by	david.mcguirk
Version	3
Application	Microsoft Office Word

Word properties pane

Properties ˅

Size	3.91MB
Pages	64
Words	23048
Total Editing Time	34 Minutes
Title	NOAA GEO-IDE Plan
Tags	Add a tag
Comments	Add comments

Related People

Author   DM David McGuirk

Add an author

Last Modified By   D david.mcguirk

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 39 - Removable Media 25-5562

Question 39: What artifact suggests this device was forensically sanitized prior to use?

Manufacturer's Response: The observation that the free space had been overwritten with a recognizable pattern: collaborative-testing.com_collaborative-testing.com…

WebCode Test	Response
2RG9U9-5562	Reviewing different locations within the USB it was observed that a repeating uniform pattern of "_collaborative-testing.com_" was used to fill in space. This suggests that a tool was used to overwrite unallocated space and existing data with no remnants of deleted files or fragmented data.
349ZFC-5562	Known pattern in the Unpartitioned space ; collaborative-testing.com_ and Repeat
3J4DXE-5562	The device was foresically sanitized prior to use, because in unpartitioned space there is the text "collaborative-testing.com".
4ZJ2KE-5562	Unallocated spaces are filled with infinitely repeating strings of "_collaborative-testing.com_"
673VQB-5562	The unpartitioned space has "collaborative-testing.com" repetitively listed in hex view
8FPDKA-5562	Free space and unallocated space is wiped with the same string pattern (collaborative-testing.com_)
8TBZD8-5562	Not in scope.
8WNN47-5562	All Slack or Free space on the USB device is filled with the repeating pattern 'collaborative-testing.com_'.
A444U7-5562	[Participant did not return results for this question.]
AUY2L3-5562	All the free space has been overwritten with colabrative-testing.com_
BEGRX4-5562	All Unallocated/slack space over written with "collaborative-testing.com_" repeating.
BTXP36-5562	The presence of free space or unallocated space.
CTEYRY-5562	The unallocated space on the device was overwritten with a pattern: collaborative-testing.com_
DJLBA2-5562	$LogFile
E6FEQZ-5562	Unallocated and Unpartitioned Space (collaborative-testing.com_ repeating throughout)
EYTN7P-5562	Artifact: Unallocated Space
F4KDZ3-5562	Same repeated ASCII / Hex in unallocated areas = example collaborative-testing.com_collaborative-testing.com_etc.
FJ22JX-5562	If the unpartitioned space on the disk is examined with a hex editor or FTK Imager the repeated characters of "collaborative-testing.com_" can be seen all through the unpartitioned/unallocated space.
GA8D2Z-5562	unnalocated space is filled with " collaborativetesting.com_"
GJP4GX-5562	All unallocated space is stomped on with the same text in repeat "collaborative-testing.com_"

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 39 - Removable Media 25-5562	
WebCode Test	**Response**
GTHERT-5562	windows installation date 2024/03/15, and some files were created before the installation date
GTZ73X-5562	Unpartitioned Space is filled with Hex values translating to collaborative-testing.com_ repeated until the end of the drive.
HEX8ER-5562	The clearest artifact is the repeated ASCII marker _collaborative-testing.com_ overwriting every Unused Disk Area, Unallocated Cluster—including sectors 0–127—indicating the drive was forensically sanitized with a signature-wipe (writing that pattern across the media) before use.
HXUD8T-5562	When performing a wiping, random values or consistent patterns may be found in unallocated space. This phenomenon has been observed in unallocated space on USB devices, indicating that the device was initialized (wiped) with the string collaborative-testing.com_ prior to use.
HYZ6QT-5562	The presence of string at the empty spaces of drive "collaborative-testing.com_ (HEX: 636F6C6C61626F7261746976652D74657374696E672E636F6D5F)" indicates that the device was forensically sanitized prior to use.
JGEWDV-5562	Device unallocated and partition free space are filled with "collaborative-testing.com_"
K7CZKT-5562	Partition 3 (Microsoft NTFS, 24.13 GB)\Windows\Panther\setupact.log
KA8UHU-5562	The free and unallocated space are overwritten with the values "collaborative-testing.com"
KYBNNV-5562	The artifact that suggests that this devices was forensically sanitized prior to use is that the unpartitioned and unallocated space on the device has the repeated known characters of "collaborative-testing.com_".
LACBFT-5562	UninterestedToad.ps contains 0s and Fs in a pattern that resembles data that has been wiped
LN7VWF-5562	[Participant did not return results for this question.]
LRRKGT-5562	The unallocated space is overwritten with a pattern. _collaborative-testing.com
M2VAHU-5562	ProudChough.gz
MD7R7R-5562	When reviewing the data within the physical disk, a known ASCII code "collaborative-testing.com" repeats itself in in areas which have not been overwritten by other data.
MQXA6Q-5562	The repetitive known hex written to the unused portions of the drive shows that it was wiped with a known pattern proving that it was a controlled sanitize.
MV6VTN-5562	Repeating 'collaborative-testing.com' and repeating zeroes through 'Unallocated' or Unpartitioned Space.
Q2Z3GD-5562	Unused areas overwritten with "collaborative-testing.com_"
QCLZQR-5562	The unallocated space is overwritten with a pattern, collaborative-testing.com_
QH4FBN-5562	unused sectors show known pattern (collaborative-testing.com_) typical in a forensic wiping process
T8JQPN-5562	Unallocated space has the text "collaborative-testing.com_" repeated throughout the disk. Allocated data appears to have overwritten it.
THHLMJ-5562	Looking at the Hex within the Disk view on X-Ways the following string 'collaborative-testing.com' is repeated continuously until data on the disk is present. After the end of the data present, the string restarts.

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 39 - Removable Media 25-5562	
WebCode Test	**Response**
TRHDUP-5562	Unallocated space was overwritten with the following repetitive pattern: "_collaborative-testing.com_collaborative-testing.com_..........."
TVPPWK-5562	_collaborative-testing.com in all unallocated space
U3GARK-5562	The unallocated space for each partition were found to contain a known pattern, suggesting a secure wipe prior to current usage
U4CRUL-5562	Unallocated space before, between, and after partitions contain the text "collaborative-testing.com_" over and over again. A way to wipe the content of a storage device would be to write all 0's across it but the 0's can be replaced by any other pattern of information such as "collaborative-testing.com_" and have the same effect.
UT9WBG-5562	$LogFile with identical timestamps 23/02/2025 10:25:24 UTC -7
V63DZH-5562	Repetitive and structured data (collaborative-testing.com) filling multiple sectors indicates the device was likely forensically wiped using custom data.
VJJLKL-5562	The unpartitioned space shows a logical size of 0 Bytes. Also, the unpartitioned space is showing a specific pattern "collaborative-testing.com_".
W7CX8H-5562	The raw data contains a repeating string ("collaborative-testing.com_") in the unpartitioned area of the device
WH87QK-5562	Unallocated Space or Unpartitioned Space. When you forensically sanitize a device you can overwrite every bit on the device with a known value/pattern. All unallocated and unpartitioned space on this device (in each partition) was overwritten with a pattern of : collaborative-testing.com_.
WKE9TJ-5562	Unpartitioned Space. Custom wipe pattern is written to sectors: "collaborative-testing.com_"
WVD7FJ-5562	The unallocated space on the USB drive is formatted in a pattern with "collaborative-testing.com_" repeated over and over
X9VFGE-5562	REALTOR.EXE-6BF69CC5.pf
XDUKGE-5562	The repeating ASCII text "collaborative-testing.com_" appears to have been used to wipe the drive since it is present throughout the drive and in sectors that are not part of the file system such as the first physical sectors on the drive.
XGRD6G-5562	collaborative-testing.com_ is written to unallocated space during the wiping process.
XMC987-5562	There is no artifact suggesting that this device was forensically sanitized prior to use, as data was found on the device. Additionally, there is no indication of free space being overwritten, nor were any traces of wiping tools such as DBAN, CCleaner, or SDelete identified.
XY6VCG-5562	The unallocated space and free space on the USB was written with "collaborative-testing.com" repeated.
Z8XMWF-5562	It appears within the hex of all the ".FileSlack" and "unallocated Space" files via Hex containing a series of 0s at the beginning then the repeating string "collaborative-testing.com" after.
ZNK3ZC-5562	The fact that the entire flash drive is filled with "collaborative-testing.com_" is an artifact.
ZRL9H3-5562	Realtor.exe
ZZUWEA-5562	Not sure

Removable Media Analysis Results

TABLE 2: Removable Media Analysis Results

Question 39 - Removable Media 25-5562

Question 39: What artifact suggests this device was forensically sanitized prior to use?

Consensus Result:

Free space has been overwritten with a recognizable pattern: collaborative-testing.com_collaborative-testing.com…

Manufacturer's Response Explanation:

Windows executable files, identified by their file header, "MZ" are compound files which often contain other files. Contained within realtor.exe are several 'resources', including "version.txt."

Manufacturer's Response Illustration:

free space on the device

Additional Comments

TABLE 3

WebCode Test	Additional Comments
24WLMH-5561	I thought the term file format was a bit odd. I believe in past tests, the term used was "mime type" which was clearer.
349ZFC-5562	Thank you very much for your time and assistance. Have a great week!
3GDA68-5561	Question 17, not sure if the question was the text inside the zip file, zip.zip\the answer to question 17 \Users\thomas\AppData\Local\Microsoft\zip.zip\the answer to question 17
4FFFK9-5561	For question 10, there were a couple of additional applications with matching run timestamps noted in the Prefetch files: CALCULATORAPP.EXE and RUNTIMEBROKER.EXE. However, the REALTOR.EXE app appeared to be the only one launched from a different volume.
673VQB-5562	Question(s) 10/11 - multiple applications were executed within that time so it was difficult to determine which one was correct. Question 22 - The pier in the picture is located in London, not the exif coordinates. The coordinates do not reflect what is showing in the picture.
7CQT46-5561	On Question 3 it is reported Windows 10 in the registry but it is actually Windows 11. The reason being Windows did not update the particular entries in the registry when updating to Windows 11, such as product name, etc., then it will still be reported as Windows 10. Microsoft is still listing the OS under the windows 10 numerical series: "10.0.22631", which I believe it is actually Windows 11, 23H2. It's by design for compatibility issues so that a ton of software doesn't stop installing because it thinks that Windows 11 is an unsupported operating system
8FPDKA-5562	#1: Question 37 didn't seem possible to answer as written. #2: Much of this test seemed directed to people with significant experience in the the Windows platform and with significant Windows-specific training (through some place like SANS.) I don't know if that is fair or a valid way to measure competence, even if I personally think anyone calling themselves a forensic examiner SHOULD be able to answer those questions. Some of the questions were directed at reasonably obscure concepts.
8TBZD8-5562	Q21 was not in scope for this test.
8WNN47-5562	I had difficulty understanding the question. I hope future questions will be worded more clearly. I sincerely enjoyed participating and hope for a positive result. Questions : 22, 23, 31, 37, 39.
CTEYRY-5562	Regarding to the answer of question 31: there are 04 partitions, and the partition 1 has no name/label. Regarding to the answer of question 38: according to metadata of the file, the title was "NOAA GEO-IDE Plan", and while opening the file it shows on the first page the title "NOAA Global Earth Observation Integrated Data Environment (GEO-IDE)"

TABLE 3

WebCode Test	Additional Comments
DB9AYY-5561	Expanded answer for Question 5: List the non-built-in user account(s) (name(s)) on this computer. Thomas Martha Administrator Guests DefaultAccount WDAGUtilityAccount Axiom lists the type of account as either Built-in or Local User. Thomas and Martha are user created accounts (RID 1001 and 1002). These are certainly considered "non-built-in" accounts. Administrator, Guest, DefaultAccount, and WDAGUtilityAccount are also identified by Axiom as Local User accounts (RID 500, 501, 503, and 504) These accounts are created by default during the Windows installation (meaning they are arguably "built-in"). After rereading the question carefully, I interpreted the desired response as, provide a list of all accounts that are labeled "Local User" as opposed to the "Built-in" identifier even though Administrator, Guest, DefaultAccount, and WDAGUtilityAccount are part of the Windows installation process as opposed to the accounts identified by Axiom as "Built-in" SID S-1-5-18, SID S-1-5-19 and SID S-1-5-20.
EYTN7P-5562	Question 10: timestamp show 4 apps were executed, differences in milliseconds: Realtor.exe, Caluclatorapp.exe, Scvhost.exe, Runtimebroker.exe.
GPH4VT-5561	COMMENTS ABOUT QUESTIONS: 3. The forensic tools used interpret differently the operative system data. Magnet Axiom identified as Windows 11, while EnCase and Autopsy showed the register value as Windows 10 Professional. 22. This question is a bit ambiguous due to the difference in cultures and linguistics. In our country is not common to use the term "cross-streets", the way that is used in USA. Usually we reference intersections or corners by their name, without identify transversal streets. This difference generated confusion about the information that we needed to give (address, full intersection or the perpendicular street). The EXIF metadata gave latitude 39.026072 and longitude -77.405972 that made reference to the following address: 21331 Gentry Drive, Sterling, Virginia, USA.
HYZ6QT-5562	Regarding Question 38: The metadata of the office document shows the title to be : NOAA GEO-IDE Plan, However the content of the first(title) page of the document is as follows: "NOAA Global Earth Observation Integrated Data Environment (GEO-IDE)"
J7HNUT-5561	Question 7 again uses BSSID for the Network Name. question 1 references the image file 25-5561.E01, but the image file is 25-5561-001.E01. #3 version is also listed in software as 6.3.
K7CZKT-5562	Please note that the supplied USB Flash Drive was malfunctioning at the time of receipt. While treating the USB Flash Drive as original evidence, the use of a write-blocker, TX1 and Tableau Forensic USB 3.0 Bridge (T8u), was unsuccessful. As a last resort, I bypassed the write-blocker and was able to recover two separate images. On May 28, 2025, I was able to obtain an image using FTK Imager. On June 24, 2025, I was able to obtain an image using X-ways. The MD5 hash value did not match between the separate image files. I have notified [Name] on June 30, 2025 via email of this issue.
LACBFT-5562	For question 1, two hash values have been provided. The first is the hash of the data as reported by XWays, the second is the hash of the E01 file as calculated by HashMyFiles. For question 22, the cross streets have been provided for the junction closest to the point of the coordinates. [Laboratory] is based in [Country] and we believe there are language differences in terms of the word 'intersection'.

TABLE 3

WebCode Test	Additional Comments
ML4AQV-5561	1: Which software analysis tool(s) did you utilize to take this test? AccessData® Passwprd Recovery Toolkit® v8.2.1 Build 971 Cellebrite Insyetes_PA v10.5.0.1027 Exterro® Forensic Toolkit® 8.2.0.596 Exterro® Registry Viewer® 2.3.1.14 Magnet AXION V 9.0.0.43519 2: Are the skill sets appropriate for this type of test? Yes 3: What components/skills can be added to improve this test? 4: Does the quality of the data meet your lab's standards for testing? If not, where is it lacking? Yes 5: How long did it take you to complete this test? Over four days - approximately 20 hours 6: Are there any questions on this test that should be revised? If yes, please provide the question number and your suggested revision.
MR7JXN-5561	Question #3 needs clarification since there is a known quirk of Windows 11 and what is reported in the registry. The quirk being that there is a difference between what is reported by the registry key and what is accurately interpreted by all the registry keys. Based on how the question is phrased I'm not sure what CTS is looking for as their answer. If the question is just asking what is reported in the key value 'SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName' then the answer would be Windows 10 Pro. However, if CTS is looking for us to interpret the information for the actual operating system installed then the 'BuildNumber' key would also need to be used to help determine the operating system as Windows 11 Pro. I think the question can be seen as a trick question and needs to be more specific to specify if CTS is looking for the operating system installed according to the registry value 'ProductName' or if all the key values in 'SOFTWARE\Microsoft\Windows NT\CurrentVersion\' need to be interpreted to determine the operating system installed. For this reason, I reported both operating systems in my answer.
MV6VTN-5562	RE: Question #3. One forensic tool listed 'Windows 11 Pro' as the operating system, but also had Windows 10 Pro in the ProductName registry field. This tool specifically displayed, "Windows 11 Pro (2009)". The ReleaseId field, showing 2009 is possibly a deprecated registry entry but needs confirmation/research to determine if this field is causing a false positive effect with listing of the Operating System Name. The other forensic tool referenced 'Windows 10 Pro' under ProductName but both tools referenced CurrentBuild as 22631, and DisplayVersion as 23H2, both of which are associated with Windows 11, not Windows 10 although additional research would be helpful. Accordingly, this question creates some issues and highlights some disparity in Microsoft's versioning for Windows 10 and 11. Multiple discussion forums discussing the versioning/build issues were noted. RE: Question #17. Located encrypted archive 'Zip.zip'. Was unable to locate or brute-force password to open the file.
NK3WJT-5561	Please keep these tests as realistic and germane to the investigation as possible. We are a Police Department. The Owl photos and Rick Astley easter eggs are distracting and borderline condescending. More importantly, please do not switch back and forth between local and UTC time. That is never encountered in real casework and is confusing for a purpose unknown.
PZAD6L-5561	For #3 Axiom showed Windows 11 pro, however, EnCase shows Windows 10 pro build 22621. Research shows that it's due to a design choice to maintain application compatibility.

TABLE 3

WebCode Test	Additional Comments
QCLZQR-5562	Question 3: Two answers were located for this question and both were provided. Question 9: Clarification was requested on what needed to be provided, either the full source URL or only the website portion (host). We were told either would be acceptable and both were provided. Question 13: Fourteen file types contain the first 2, 8, or 14 bytes of the requested file. There could be multiple answers to this question depending on where you believe the file signature ends. Question 10: Clarification was requested on this question and we were provided with the answer: "Report the application executed closest to, but not before,16:28:57.000." The file executed at 16:28:57.050 was provided, although other files were executed at 16:28:57.
QEMD4J-5561	The time zone inconsistencies (UTC for some questions, local time for others) is inconsistant. Switching time zones for questions seems to be trickery to try and get people to answer wrong.
QH4FBN-5562	I said this last year and I'll say it again this year, stop making us hand jam long answers like full SHA256 strings or ridiculous file paths. Either make it a multiple choice answer or give us the option to provide a shortened answer, like the first and last five digits of the hash or what not.
REKXEP-5561	Question 21 seems to request the answer be reported in the device local time. The use of offset is unclear - should I have reported the offset in minutes/hours? Other questions asked for local time in plain language. Question 25 references a photo of an alligator. The large reptile depicted appears to be a crocodile based on snout shape and lack of webbing at the toes. This led me to question whether I identified the correct photo, or if there was an image of an alligator on the drive that I missed.
U3GARK-5562	The answer for question 21 was confusing as for the offset. I submitted the device time as it was Mountain Standard Time but if you were asking for UTC, it would be the same date with the time of 17:01.
UGJTDH-5561	for question 10 - the calculator app also appeared to be executed at the requested time for question 28 - the files listed were reported multiple times
WH87QK-5562	Question 3: CTS was contacted in regards to how to answer this question as two answers were located for this question and both were provided. Question 5: The question states non-built in users however CTS was contacted and they stated to only list those accounts that are created by individual users. Question 9: CTS was contacted to determine how much of the URL was needed to provide for the answer (full URL of the file (including file name) or just the website that ends in .com. Both were provided. Question 10: CTS was contacted to determine how to answer this question as three applications were executed at this time. CTS responded "Report the application executed closest to, but not before,16:28:57.000." Question 13: There are several filetypes with this file header therefore there could be multiple answers depending on how many bytes you interpret as the file signature. Multiple answers were provided as that is what we would do in casework and is approved by our policies and procedures. Question 34: CTS was contacted as the filetype is not reported by our forensic software program but deductively reasoning you could say it is a plain text file or 7 bit file. Overall, I provided multiple answers on several questions as deemed necessary. We contacted CTS for guidance on some of the questions. Our policies and procedures at our laboratory allows for this. In casework we would give all the data and they determine which is relevant to their case.

TABLE 3

WebCode Test	Additional Comments
YVR6WD-5561	Question 10). According to Windows Prefetch, what application was executed at 03/03/2025 (March 3, 2025) 16:28:57 (subject computer's local time)? CALCULATORAPP.EXE and RUNTIMEBROKER.EXE have the same execution date and time as REALTOR.EXE
ZZUWEA-5562	If this was to be used in future, it would be best to choose a 'similar' [Country] based case, rather than an American real-estate fraud job. Some of the American terminology used in the question, do make it difficult slightly with their wordings. The majority of work consists and reporting on IIoC cases and to tailor a case based on this would be better. In the course I have completed they use animals, such as cats to reflect IIoC. With this case in particular, we would not go into as much detail, which the questions require. Most of them I have no had experience with in my day to day, so they have been answered as best as possible. If this was to be used in the future, it would have be tweaked, especially for new starters. A more 'challenging' one could then be introduced. I do fell like they would benefit the unit, and it made a change to my workday, compared to the demand I am currently faced with.

-End of Report-
(Appendix may follow)