



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

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

	<u>Page</u>
<u>Manufacturer's Information</u>	<u>2</u>
<u>Summary Comments</u>	<u>8</u>
<u>Table 1: Computer Hard Drive - Windows Analysis Results</u>	<u>9</u>
<u>Table 2: Removable Media Analysis Results</u>	<u>268</u>
<u>Table 3: Additional Comments</u>	<u>303</u>

Available in the 5562 version of the report.

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

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

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

Manufacturer's Information

The Computer Hard Drive – Windows Analysis test consisted of evidence data acquired from a computer running Windows 11 Pro. The extracted data was provided in an E01 file format. Participants were asked to examine the extracted data as it relates to a simulated scenario utilizing their own software and methods.

All participants enrolled in the 24-5562: Computer Hard Drive – Windows & Removable Media Storage Analysis test received an additional component, a physical USB drive shipped in a sealed manila envelope. These participants were also asked to perform evidence acquisition, extraction, and analysis.

SAMPLE PREPARATION/VALIDATION

A scripted scenario discussing a case related to a series of suspicious fires and confirmed arsons was created to generate user data on a Windows Hard Drive. The execution of the test production took place within the following date range, 14 February 2024 and 15 March 2024. Multiple system and third-party applications were used to perform activities and generate the intended artifacts. A USB device was used to add user activity on the computer and onto the removable media storage device provided to participants enrolled in 24-5562.

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

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

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

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

Manufacturer's Information, continued

SCENARIO PROVIDED TO PARTICIPANTS

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

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

You are being provided with:

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

Manufacturer's Information, continued

<u>Question</u>	<u>Manufacturer's Response</u>
1	<u>Provide the stored verification [acquisition] hash MD5 hash for the provided image, Fire Department Workstation.e01.</u> <i>51945f35b4b3e59a4a802195bce4eff</i>
2	<u>Compute and provide the SHA-1 hash of the acquired data in the provided image, Fire Department Workstation.e01.</u> <i>d894343e8d005219c49226fee4b6fe2e9f5cc3b5</i>
3	<u>What is the hostname (Computer Name) for this computer?</u> <i>COMPANY-13</i>
4	<u>What operating system (include version, edition, and Display Version) was installed on this computer?</u> <i>Windows 10, Pro, 23H2; or Windows 11 Pro, 23H2</i>
5	<u>To what domain was this computer joined?</u> <i>EmergencyServices.Winchestertonfieldville.org</i>
6	<u>What warning banner / legal notice text was displayed to users at the Windows logon screen? Provide the first two sentences of the warning.</u> <i>This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.</i>
7	<u>What time zone was this computer configured to display? (Provide answer as name, e.g., Mountain Daylight Time)</u> <i>Pacific Time</i>
8	<u>Provide the SSID (network name) of the Wi-Fi hotspot to which this computer was connected.</u> <i>Winchestertonfieldville_Fire</i>
9	<u>Provide the user account name for the owner of C:\New folder\New Text Document.txt.</u> <i>smcnamara</i>
10	<u>Provide the filesystem attributes for C:\New folder\New Text Document.txt.</u> <i>Hidden, Read-Only, Archive</i>
11	<u>What user remotely logged on to this computer via Remote Desktop Protocol (RDP)?</u> <i>tgavin</i>
12	<u>What was the IP address (of the other computer) from which a user (from question #11) remotely logged on to this computer via Remote Desktop Protocol (RDP)?</u> <i>10.0.2.15</i>
13	<u>Provide the name and path of the active (not deleted) file containing the keyword "flammulated"?</u> <i>C:\Users\mohalloran\Pictures\DSC_0921.jpg</i>
14	<u>What text appears in the desktop background photo for user kshea?</u> <i>Sleep 'til you're hungry, eat 'til you're sleepy.</i>

Manufacturer's Information, continued

<u>Question</u>	<u>Manufacturer's Response</u>
15 <u>Who is listed as the author of the document with SHA1 hash 0C67015E256CF9B9030DAA0E517B161DC95EA0F0?</u>	<i>James Moore</i>
16 <u>Provide the hostname (computer name) for the computer on which the file agency_admin_guide_2004.pdf was located.</u>	<i>FIRE-DC01</i>
17 <u>What terms did user gmontag search on Google in the Chrome browser, March 9, 2024?</u>	<i>bulk chemicals</i>
18 <u>For the email message containing the keyword "trychtichlorate", provide the sender's email address.</u>	<i>ronaldbartel@fireman.net</i>
19 <u>What term was searched for on YouTube at 2024-03-14 01:45:01 UTC by the then currently logged on user?</u>	<i>bleve</i>
20 <u>What phone number in the format (NNN)NNN-NNNN appears in the file with SHA1 hash 961FF684E4097CE52C475FB7F249D01EE9DC2BF2?</u>	<i>(571)434-1925</i>
21 <u>What was the original (pre-deletion) path of crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf? Provide both the path and filename.</u>	<i>C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf</i>
22 <u>Describe the filetype and content of the file with created date March 9, 2024 21:56:33 UTC+0.</u>	<i>FileType: mp4 file Content file description: A video of a person igniting a flammable gas in a large bottle. Dancing man at the end of the video (Rick Astley's music video or Rick-Rolled).</i>
23 <u>According to Windows prefetch, how many times was the calculator app executed?</u>	<i>Once (1)</i>
24 <u>According to Windows prefetch, from what directory was the Adobe Acrobat Reader application installer, AcroRdrDC2300820555 en US.exe, executed?</u>	<i>C:\temp\</i>
25 <u>In unallocated space on the subject volume is a picture file containing red text, "Make Your Own Focaccia." Provide the five words that immediately follow, "Make Your Own Focaccia."</u>	<i>A cooking workshop for all</i>
26 <u>Provide the username for the user who searched for "thermite recipie" [sic].</u>	<i>gmontag</i>
27 <u>According to the user jbeatty's NTUSER.DAT file, what other user's documents folder did they access?</u>	<i>gmontag</i>

Manufacturer's Information, continued

<u>Question</u>	<u>Manufacturer's Response</u>
28	<u>Provide the filetype (MIME Type) for the file with SHA256 hash</u> <u>67a6fa82325141eaca921ca7a64fe6e6cafb6fb86bd3ba278ccced0d6925986d.</u> <i>SQLite or SQLite 3 (Database)</i>
29	<u>Provide the path and filename of the encrypted file in one of the user's "Documents" directory.</u> <i>C:\Users\jbeatty\Documents\book.zip</i>
30	<u>Provide the name of the file contained within the encrypted file in a user's "Documents" directory.</u> <i>cookbook.pdf</i>

Manufacturer's Information, continued

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

<u>Question</u>	<u>Manufacturer's Response</u>
31 ** <u>Provide the SHA256 hash of the provided USB flash storage device.</u>	<i>47C41270C819C675B48EE47CF664733997F8FA04ED430C448E42D3F9CD8EB4A4</i>
32 ** <u>What filesystem is on the second partition (in sector order) on this device?</u>	<i>NTFS</i>
33 ** <u>What is the full path (partition name\parent directory\file) for 1m3r1xbw8wzb1.jpg?</u>	<i>\filez\New folder\1m3r1xbw8wzb1.jpg</i>
34 <u>On the device is a photo of a pair of otters (<i>Lontra canadensis</i>) standing together on a white background. Provide the green text that appears in the image.</u>	<i>2024 CTS 001</i>
35 <u>Provide the filetype (MIME Type) for the file with SHA256 hash f0445b8916474b7cb177d50ffafb646e25dab0b6c5e5ba14089443d84589c42.</u>	<i>GIF image or GIF87a</i>
36 <u>What user account is the owner of all the non-system files on the NTFS partition on this device?</u>	<i>S-1-5-21-2298470282-2867887670-580413564-1119, or jbeatty</i>
37 <u>On this device is a photo of a red onion on a wooden cutting board containing black text on a white background. Provide the text in the image.</u>	<i>DOUBLE ZIPPED</i>
38 <u>Provide the filename and path for the file that contains the keyword methylbenzene, where all the vowels have been replaced with numbers, e.g. m3th3lb3nz3n3 (but not necessarily 3s, could be any number or different numbers)</u>	<i>\Untitled\206969.doc</i>
39 <u>Who is listed as the author of Fire-fighting-Training-Manual.pdf?</u>	<i>Rui Vieito</i>
40 <u>On the device is a graphic file containing the text "2024 cts 004" (without quotes) on a red banner. Provide the text color and a description of the image content.</u>	<i>Text color: green text, Image content description: building on fire</i>
41 <u>Provide the URL contained in the file created on 11/07/23 (November 7, 2023) 17:12:31 UTC.</u>	<i>https://nij.ojp.gov/topics/articles/guide-investigating-fire-and-arson</i>

Summary Comments

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

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

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

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

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

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

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 MD5 hash for the provided image, Fire Department Workstation.e01.

Manufacturer's 51945f35b4b3e59a4a802195bce4efff

Response:

WebCode Test	Response
28NKRK-5561	51945f35b4b3e59a4a802195bce4efff
2BXEJB-5561	51945f35b4b3e59a4a802195bce4efff
2EUC34-5562	51945f35b4b3e59a4a802195bce4efff
2UJN7X-5562	51945F35B4B3E59A4A802195BCE4EFFF
2XN36N-5561	51945f35b4b3e59a4a802195bce4efff
36GUPN-5561	51945f35b4b3e59a4a802195bce4efff
3CH2GJ-5562	[Participant did not return results for this question.]
3DBUC3-5561	51945f35b4b3e59a4a802195bce4efff
3K9LKW-5561	51945f35b4b3e59a4a802195bce4efff
3LM236-5561	51945f35b4b3e59a4a802195bce4efff
483YXK-5561	51945f35b4b3e59a4a802195bce4efff
49DVEJ-5561	51945f35b4b3e59a4a802195bce4efff
4K6LX2-5561	51945f35b4b3e59a4a802195bc343fff
4L6CCW-5562	51945F35B4B3E59A4A802195BCE4EFFF
4P6N9W-5561	51945f35b4b3e59a4a802195bce4efff
4THJUL-5562	[Participant did not return results for this question.]
4XXRHK-5561	51945f35b4b3e59a4a802195bce4efff
4Z77PR-5561	51945F35B4B3E59A4A802195BCE4EFFF
6KNFKX-5561	51945f35b4b3e59a4a802195bce4efff
6RLGDW-5561	51945f35b4b3e59a4a802195bce4efff

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 1 - Examination Questions	
WebCode Test	Response
78YYBQ-5561	3d57dbf15f09181b0e7ba53598b85950
7M6APW-5561	51945f35b4b3e59a4a802195bce4efff
7WAG6W-5561	51945f35b4b3e59a4a802195bce4efff
7WV3RK-5561	51945F35B4B3E59A4A802195BCE4EFFF
8ED4K3-5562	The correct answer is 51945f35b4b3e59a4a802195bce4efff, but this is only the actual data is calculated. When metadata is included in the calculation, the result is 3d57dbf15f09181b0e7ba53598b85950.
8LRYCP-5561	51945f35b4b3e59a4a802195bce4efff
8P8Q2X-5561	3D57DBF15F09181B0E7BA53598B85950
8RFV4L-5561	51945f35b4b3e59a4a802195bce4efff
8W78WW-5562	51945f35b4b3e59a4a802195bce4efff
98N78Y-5561	Acquisition MD5 51945f35b4b3e59a4a802195bce4efff
9J6THK-5561	51945f35b4b3e59a4a802195bce4efff
9QMRX6-5561	51945f35b4b3e59a4a802195bce4efff
9XFKVP-5562	51945F35B4B3E59A4A802195BCE4EFFF2
AN93XR-5561	3d57dbf15f09181b0e7ba53598b85950
AXDBED-5562	51945f35b4b3e59a4a802195bce4efff
AXFVBT-5561	3D57DBF15F09181B0E7BA53598B85950
B2ACZR-5562	51945f35b4b3e59a4a802195bce4efff
BA4FBG-5561	51945F35B4B3E59A4A802195BCE4EFFF
BPGNBK-5562	51945f35b4b3e59a4a802195bce4efff
BVMG7F-5561	51945f35b4b3e59a4a802195bce4efff
BXTTTP-5561	51945f35b4b3e59a4a802195bce4efff
CCXUMK-5561	51945f35b4b3e59a4a802195bce4efff

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 1 - Examination Questions	
WebCode Test	Response
CPQ4TQ-5561	51945F35B4B3E59A4A802195BCE4EFFF
D3A9ER-5561	51945f35b4b3e59a4a802195bce4efff
D3MR2K-5561	51945f35b4b3e59a4a802195bce4efff
D7C7PK-5562	3D57DBF15F09181B0E7BA53598B85950
D8QG3R-5561	51945f35b4b3e59a4a802195bce4efff
DCKG7E-5561	3d57dbf15f09181b0e7ba53598b85950
DKUYDR-5561	3D57DBF15F09181B0E7BA53598B85950
DKVPRL-5562	51945f35b4b3e59a4a802195bce4efff
DPA82Q-5561	51945f35b4b3e59a4a802195bce4efff
DTN8XH-5562	51945F35B4B3E59A4A802195BCE4EFFF
DXKMTK-5561	3d57dbf15f09181b0e7ba53598b85950
EJD6CG-5561	51945f35b4b3e59a4a802195bce4efff
EJK3WT-5561	3D57DBF15F09181B0E7BA53598B85950
EMTM9G-5561	51945f35b4b3e59a4a802195bce4efff
F3TPTL-5561	3d57dbf15f09181b0e7ba53598b85950
F7NG2H-5561	3d57dbf15f09181b0e7ba53598b85950
FG6CVN-5561	MD5: 51945f35b4b3e59a4a802195bce4efff
FT8J39-5561	51945f35b4b3e59a4a802195bce4efff
G6U6KA-5561	51945F35B4B3E59A4A802195BCE4EFFF
G9BD99-5561	51945f35b4b3e59a4a802195bce4efff
G9PQLK-5561	51945F35B4B3E59A4A802195BCE4EFFF
GALGEK-5562	51945f35b4b3e59a4a802195bce4efff

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 1 - Examination Questions	
WebCode Test	Response
GMPPAG-5561	51945F35B4B3E59A4A802195BCE4EFFF
H3X34J-5561	51945f35b4b3e59a4a802195bce4efff
HAWCD-5562	51945f35b4b3e59a4a802195bce4efff
HFM3VL-5562	[Participant did not return results for this question.]
HGE2AK-5561	51945f35b4b3e59a4a802195bce4efff
HMQYPK-5561	51945f35b4b3e59a4a802195bce4efff
HTB6DE-5562	51945F35B4B3E59A4A802195BCE4EFFF
HVJ3Y9-5561	51945f35b4b3e59a4a802195bce4efff
HYHLVF-5561	3d57dbf15f09181b0e7ba53598b85950
J3FCTE-5561	3d57dbf15f09181b0e7ba53598b85950
J49DM9-5561	51945f35b4b3e59a4a802195bce4efff
JFURCD-5561	51945f35b4b3e59a4a802195bce4efff
JPAH22-5562	51945f35b4b3e59a4a802195bce4efff
JXAZDE-5561	51945f35b4b3e59a4a802195bce4efff
JXHVGK-5561	51945f35b4b3e59a4a802195bce4efff
K3WXT8-5562	3d57dbf15f09181b0e7ba53598b85950
KA94ED-5562	51945f35b4b3e59a4a802195bce4efff
KCQD3T-5561	51945F35B4B3E59A4A802195BCE4EFFF
KMHPR4-5561	51945f35b4b3e59a4a802195bce4efff
LBJ6ZC-5562	51945f35b4b3e59a4a802195bce4efff
LMDLPD-5561	51945F35B4B3E59A4A802195BCE4EFFF
LRM3Y2-5562	51945f35b4b3e59a4a802195bce4efff

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 1 - Examination Questions	
WebCode Test	Response
LWKE3D-5561	51945f35b4b3e59a4a802195bce4efff
MCQ8YF-5561	3d57dbf15f09181b0e7ba53598b85950
MD8AY2-5561	51945f35b4b3e59a4a802195bce4efff
MK6QJE-5561	3d57dbf15f09181b0e7ba53598b85950
MR47EE-5562	51945f35b4b3e59a4a802195bce4efff
MV6A9L-5561	51945f35b4b3e59a4a802195bce4efff
N9Q2B2-5562	51945F35B4B3E59A4A802195BCE4EFFF
NH83FA-5562	51945F35B4B3E59A4A802195BCE4EFFF
NNQD78-5561	51945f35b4b3e59a4a802195bce4efff
NPUPBF-5562	51945f35b4b3e59a4a802195bce4efff
NQ7BB3-5561	51945f35b4b3e59a4a802195bce4efff
P3EHK8-5562	51945f35b4b3e59a4a802195bce4efff
P3ER7C-5561	51945f35b4b3e59a4a802195bce4efff
P6NMZG-5561	3d57dbf15f09181b0e7ba53598b85950
PE6G4X-5561	51945f35b4b3e59a4a802195bce4efff
PYKJC4-5561	51945f35b4b3e59a4a802195bce4efff
Q4ZTN7-5562	51945f35b4b3e59a4a802195bce4efff
Q73JRN-5561	51945f35b4b3e59a4a802195bce4efff
RBARA4-5561	51945f35b4b3e59a4a802195bce4efff
RE7DZL-5561	51945f35b4b3e59a4a802195bce4efff
RUTBQ8-5561	51945f35b4b3e59a4a802195bce4efff
RY7A78-5561	51945f35b4b3e59a4a802195bce4efff

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 1 - Examination Questions	
WebCode Test	Response
RZKKZ7-5562	51945F35B4B3E59A4A802195BCE4EFFF
T9UAE6-5561	51945f35b4b3e59a4a802195bce4efff
TH2XG4-5562	51945F35B4B3E59A4A802195BCE4EFFF
TTGXLB-5561	51945f35b4b3e59a4a802195bce4efff
U8973A-5561	51945f35b4b3e59a4a802195bce4efff
UEQLM7-5561	3d57dbf15f09181b0e7ba53598b85950
UEWNPX-5561	3d57dbf15f09181b0e7ba53598b85950
UGNM4W-5561	51945F35B4B3E59A4A802195BCE4EFFF
ULHG2X-5561	3d57dbf15f09181b0e7ba53598b85950
UPTW39-5562	51945f35b4b3e59a4a802195bce4efff
UUA6Q9-5561	51945f35b4b3e59a4a802195bce4efff
UZQMYA-5562	51945f35b4b3e59a4a802195bce4efff
V66XC6-5562	3d57dbf15f09181b0e7ba53598b85950
V82HUJ-5561	51945f35b4b3e5ca4a802195bce4efff
VXLE96-5561	51945f35b4b3e59a4a802195bce4efff
VYTW7Z-5561	51945f35b4b3e59a4a802195bce4efff
W447WA-5561	51945f35b4b3e59a4a802195bce4efff
WB84Q8-5561	51945f35b4b3e59a4a802195bce4efff
WBPY99-5561	51945f35b4b3e59a4a802195bce4efff
WFVT36-5561	51945f35b4b3e59a4a802195bce4efff
WH6VY2-5561	3d57dbf15f09181b0e7ba53598b85950
WL2PNP-5561	51945f35b4b3e59a4a802195bce4efff

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 1 - Examination Questions	
WebCode Test	Response
WL4AK7-5562	51945F35B4B3E59A4A802195BCE4EFFF
WQGWCP-5562	51945f35b4b3e59a4a802195bce4efff
X2AZR3-5561	51945f35b4b3e59a4a802195bce4efff
X3NFAB-5561	51945f35b4b3e59a4a802195bce4efff
X62GKW-5561	51945f35b4b3e59a4a802195bce4efff
X84MXA-5561	51945f35b4b3e59a4a802195bce4efff
XDQM3P-5561	51945f35b4b3e59a4a802195bce4efff
XDT8Y6-5562	51945f35b4b3e59a4a802195bce4efff
XLP32A-5562	51945f35b4b3e59a4a802195bce4efff
XQXJAX-5561	51945f35b4b3e59a4a802195bce4efff
Y2PJCZ-5561	3D57DBF15F09181B0E7BA53598B85950
Y8WZT2-5561	51945f35b4b3e59a4a802195bce4efff
YZK9WX-5561	51945f35b4b3e59a4a802195bce4efff
Z4GR62-5562	51945f35b4b3e59a4a802195bce4efff
Z4PAVK-5561	51945f35b4b3e59a4a802195bce4efff
ZBUQRZ-5561	51945f35b4b3e59a4a802195bce4efff
ZEU2MZ-5562	51945F35B4B3E59A4A802195BCE4EFFF
ZF7RW4-5561	51945f35b4b3e59a4a802195bce4efff
ZN4C6R-5561	51945f35b4b3e59a4a802195bce4efff
ZQ4URL-5562	3d57dbf15f09181b0e7ba53598b85950
ZU7QJ2-5561	51945f35b4b3e59a4a802195bce4efff
ZWABN2-5562	51945F35B4B3E59A4A802195BCE4EFFF

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 MD5 hash for the provided image, Fire Department Workstation.e01.

Consensus Result:

51945f35b4b3e59a4a802195bce4eff

Manufacturer's Response Explanation:

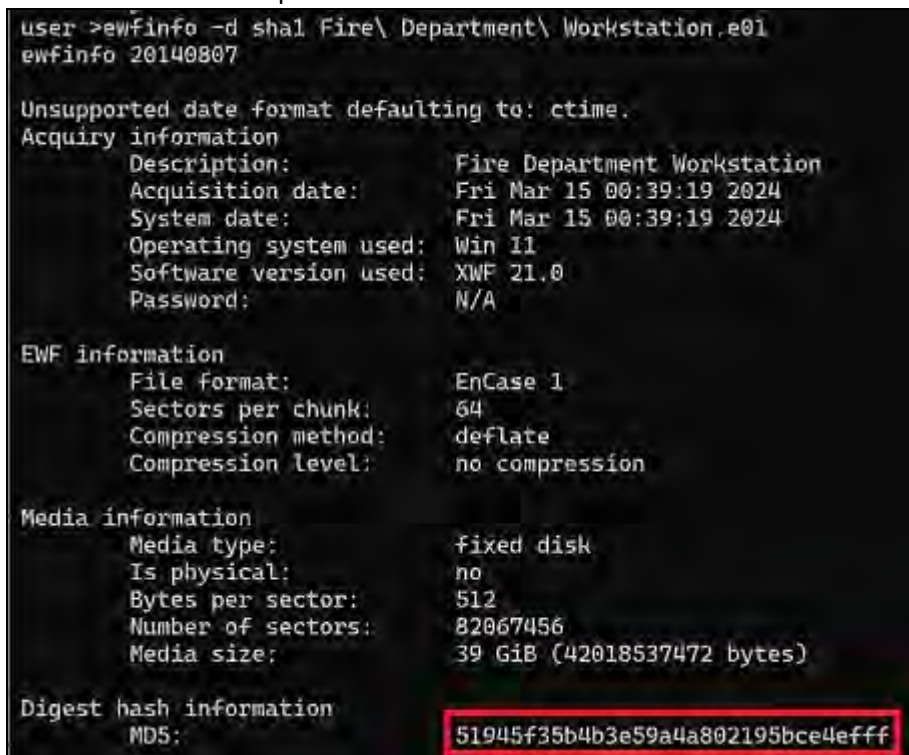
The verification hash is embedded in the .E01 (EWF) forensic container file by the acquisition tool. Forensic tools that support the Expert Witness Format (EWF) will parse and display this information.

Manufacturer's Response Illustration:

FTK Imager view of Fire Department Workstation.e01 stored verification hash



ewfinfo view of Fire Department Workstation.e01 stored verification hash



Other Responses:

Twenty-three (15%) participants reported the MD5 hash of the container file, 3d57dbf15f09181b0e7ba53598b85950, 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: Compute and provide the SHA-1 hash of the acquired data in the provided image, Fire Department Workstation.e01.

Manufacturer's d894343e8d005219c49226fee4b6fe2e9f5cc3b5

Response:

WebCode Test	Response
28NKRK-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
2BXEJB-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
2EUC34-5562	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
2UJN7X-5562	D894343E8D005219C49226FEE4B6FE2E9F5CC3B5
2XN36N-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
36GUPN-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
3CH2GJ-5562	[Participant did not return results for this question.]
3DBUC3-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
3K9LKW-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
3LM236-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
483YXK-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
49DVEJ-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
4K6LX2-5561	d894343e8d005219c49226f334b6fe2e9f5cc3b5
4L6CCW-5562	D894343E8D005219C49226FEE4B6FE2E9F5CC3B5
4P6N9W-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
4THJUL-5562	[Participant did not return results for this question.]
4XXRHK-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
4Z77PR-5561	D894343E8D005219C49226FEE4B6FE2E9F5CC3B5
6KNFKX-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
6RLGDW-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 2 - Examination Questions	
WebCode Test	Response
78YYBQ-5561	3c012264004c9d49d636b43662572672a59ca9a6
7M6APW-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
7WAG6W-5561	3c012264004c9d49d636b43662572672a59ca9a6
7WV3RK-5561	D894343E8D005219C49226FEE4B6FE2E9F5CC3B5
8ED4K3-5562	The correct answer is d894343e8d005219c49226fee4b6fe2e9f5cc3b5, but this is only the actual data is calculated. When metadata is included in the calculation, the result is 3c012264004c9d49d636b43662572672a59ca9a6
8LRYCP-5561	D894343E8D005219C49226FEE4B6FE2E9F5CC3B5
8P8Q2X-5561	3c012264004c9d49d636b43662572672a59ca9a6
8RFV4L-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
8W78WW-5562	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
98N78Y-5561	3c012264004c9d49d636b43662572672a59ca9a6
9J6THK-5561	D894343E8D005219C49226FEE4B6FE2E9F5CC3B5
9QMRX6-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
9XFKVP-5562	D894343E8D005219C49226FEE4B6FE2E9F5CC3B5
AN93XR-5561	3c012264004c9d49d636b43662572672a59ca9a6
AXDBED-5562	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
AXFVBT-5561	3C012264004C9D49D636B43662572672A59CA9A6
B2ACZR-5562	D894343e8d005219c49226fee4b6fe2e9f5cc3b5
BA4FBG-5561	D894343E8D005219C49226FEE4B6FE2E9F5CC3B5
BPGNBK-5562	D894343E8D005219C49226FEE4B6FE2E9F5CC3B5
BVMG7F-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
BXTTXP-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
CCXUMK-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 2 - Examination Questions	
WebCode Test	Response
CPQ4TQ-5561	3C012264004C9D49D636B4366257267A59CA9A6
D3A9ER-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
D3MR2K-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
D7C7PK-5562	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
D8QG3R-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
DCKG7E-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
DKUYDR-5561	3C012264004C9D49D636B43662572672A59CA9A6
DKVPR-5562	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
DPA82Q-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
DTN8XH-5562	3d57dbf15f09181b0e7ba53598b85950
DXKMTK-5561	3c012264004c9d49d636b43662572672a59ca9a6
EJD6CG-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
EJK3WT-5561	3C012264004C9D49D636B43662572672A59CA9A6
EMTM9G-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
F3TPTL-5561	3c012264004c9d49d636b43662572672a59ca9a6
F7NG2H-5561	3c012264004c9d49d636b43662572672a59ca9a6
FG6CVN-5561	SHA-1 : d894343e8d005219c49226fee4b6fe2e9f5cc3b5
FT8J39-5561	D894343E8D005219C49226FEE4B6FE2E9F5CCB5
G6U6KA-5561	D894343E8D005219C49226FEE4B6FE2E9F5CC3B5
G9BD99-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
G9PQLK-5561	D894343E8D005219C49226FEE4B6FE2E9F5CC3B5
GALGEK-5562	d894343e8d005219c49226fee4b6fe2e9f5cc3b5

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 2 - Examination Questions	
WebCode Test	Response
GMPPAG-5561	D894343E8D005219C49226FEE4B6FE2E9F5CC3B5
H3X34J-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
HAVCD-5562	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
HFM3VL-5562	[Participant did not return results for this question.]
HGE2AK-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
HMQYPK-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
HTB6DE-5562	D894343E8D005219C49226FEE4B6FE2E9F5CC3B5
HVJ3Y9-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
HYHLVF-5561	3c012264004c9d49d636b43662572672a59ca9a6
J3FCTE-5561	3c012264004c9d49d636b43662572672a59ca9a6
J49DM9-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
JFURCD-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
JPAH22-5562	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
JXAZDE-5561	3c012264004c9d49d636b43662572672a59ca9a6
JXHVGK-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
K3WXT8-5562	3c012264004c9d49d636b43662572672a59ca9a6
KA94ED-5562	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
KCQD3T-5561	D894343E8D005219C49226FEE4B6FE2E9F5CC3B5
KMHPR4-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
LBJ6ZC-5562	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
LMDLPD-5561	D894343E8D005219C49226FEE4B6FE2E9F5CC3B5
LRM3Y2-5562	d894343e8d005219c49226fee4b6fe2e9f5cc3b5

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 2 - Examination Questions	
WebCode Test	Response
LWKE3D-5561	3c012264004c9d49d636b43662572672a59ca9a6
MCQ8YF-5561	3c012264004c9d49d636b43662572672a59ca9a6
MD8AY2-5561	D894343E8D005219C49226FEE4B6FE2E9F5CC3B5
MK6QJE-5561	3c012264004c9d49d636b43662572672a59ca9a6
MR47EE-5562	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
MV6A9L-5561	d894343e8d005219c49226fee4b6fe2e9f5cc
N9Q2B2-5562	D894343E8D005219C49226FEE4B6FE2E9F5CC3B5
NH83FA-5562	D894343E8D005219C49226FEE4B6FE2E9F5CC3B5
NNQD78-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
NPUPBF-5562	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
NQ7BB3-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
P3EHK8-5562	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
P3ER7C-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
P6NMZG-5561	3C012264004C9D49D636B43662572672A59CA9A6
PE6G4X-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
PYKJC4-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
Q4ZTN7-5562	D894343E8D005219C49226FEE4B6FE2E9F5CC3B5
Q73JRN-5561	D894343E8D005219C49226FEE4B6FE2E9F5CC3B5
RBARA4-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
RE7DZL-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
RUTBQ8-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
RY7A78-5561	3C012264004C9D49D636B43662572672A59CA9A6

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 2 - Examination Questions	
WebCode Test	Response
RZKKZ7-5562	D894343E8D005219C49226FEE4B6FE2E9F5CC3B5
T9UAE6-5561	D894343E8D005219C49226FEE4B6FE2E9F5CC3B5
TH2XG4-5562	D894343E8D005219C49226FEE4B6FE2E9F5CC3B5
TTGXLB-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
U8973A-5561	3c012264004c9d49d636b43662572672a59ca9a6
UEQLM7-5561	3c012264004c9d49d636b43662572672a59ca9a6
UEWNPX-5561	3c012264004c9d49d636b43662572672a59ca9a6
UGNM4W-5561	D894343E8D005219C49226FEE4B6FE2E9F5CC3B5
ULHG2X-5561	3c012264004c9d636b43662572672a59ca9a6
UPTW39-5562	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
UUA6Q9-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
UZQMYA-5562	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
V66XC6-5562	3c012264004c9d49d636b43662572672a59ca9a6
V82HUJ-5561	D894343E8D005219C49226FEE4B6FE2E9F5CC3B5
VXLE96-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
VYTW7Z-5561	3c012264004c9d49d636b43662572672a59ca9a6
W447WA-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
WB84Q8-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
WBPY99-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
WFVT36-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
WH6VY2-5561	3c012264004c9d49d636b43662572672a59ca9a6
WL2PNP-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 2 - Examination Questions	
WebCode Test	Response
WL4AK7-5562	D894343E8D005219C49226FEE4B6FE2E9F5CC3B5
WQGWCP-5562	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
X2AZR3-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
X3NFAB-5561	D894343E8D005219C49226FEE4B6FE2E9F5CC3B5
X62GKW-5561	D894343E8D005219C49226FEE4B6FE2E9F5CC3B5
X84MXA-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
XDQM3P-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
XDT8Y6-5562	SHA1 160bit - D894343E8D005219C49226FEE4B6FE2E9F5CC3B5
XLP32A-5562	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
XQXJAX-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
Y2PJCZ-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
Y8WZT2-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
YZK9WX-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
Z4GR62-5562	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
Z4PAVK-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
ZBUQRZ-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
ZEU2MZ-5562	D894343E8D005219C49226FEE4B6FE2E9F5CC3B5
ZF7RW4-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
ZN4C6R-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
ZQ4URL-5562	3c012264004c9d49d636b43662572672a59ca9a6
ZU7QJ2-5561	d894343e8d005219c49226fee4b6fe2e9f5cc3b5
ZWABN2-5562	D894343E8D005219C49226FEE4B6FE2E9F5CC3B5

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 2 - Examination Questions

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

Consensus Result:

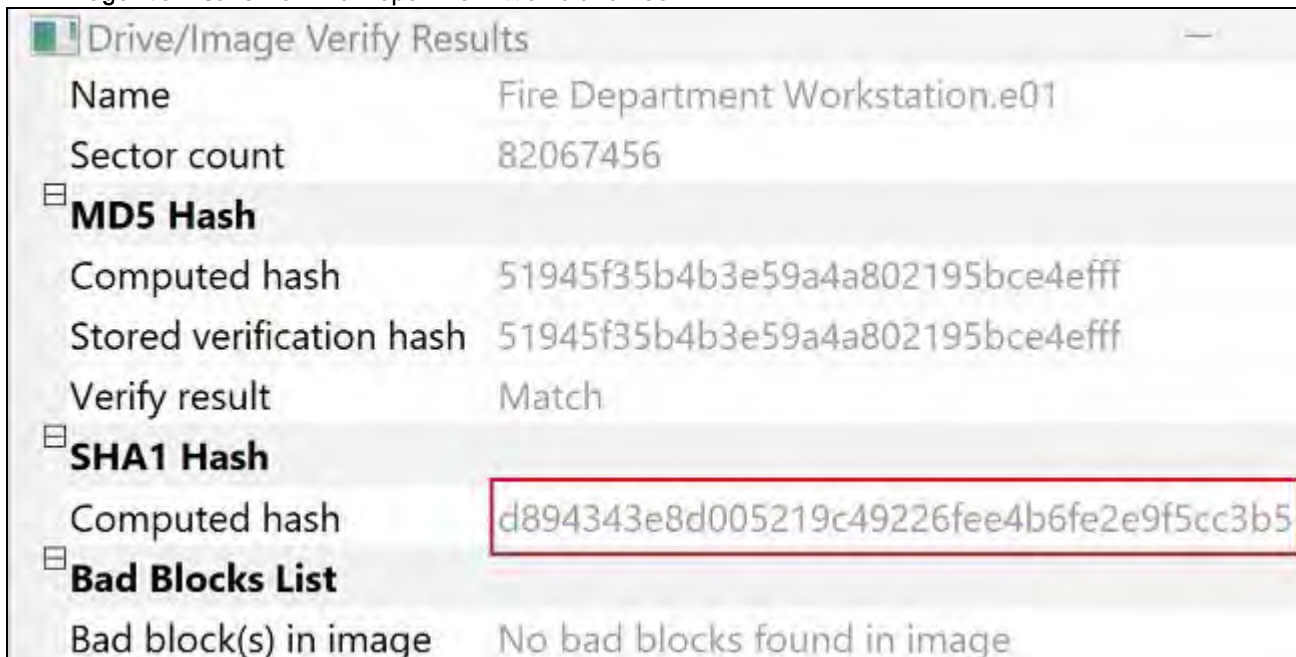
d894343e8d005219c49226fee4b6fe2e9f5cc3b5

Manufacturer's Response Explanation:

Forensic tools that support the Expert Witness Format (EWF) can calculate this hash.

Manufacturer's Response Illustration:

FTK Imager verification of Fire Department Workstation.e01



ewfverify verification of Fire Department Workstation.e01

```
Read: 39 GiB (42018537472 bytes) in 6 minute(s) and 20 second(s)
with 105 MiB/s (110575098 bytes/second).
MD5 hash stored in file:      51945f35b4b3e59a4a802195bce4efff
MD5 hash calculated over data: 51945f35b4b3e59a4a802195bce4efff
SHA1 hash stored in file:     N/A
SHA1 hash calculated over data: d894343e8d005219c49226fee4b6fe2e9f5cc3b5
ewfverify: SUCCESS
```

Other Responses:

Twenty-seven (18%) participants reported the SHA-1 hash of the container file, 3c012264004c9d49d636b43662572672a59ca9a6, not the computed hash of the provided image.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3 - Examination Questions

Question 3: What is the hostname (Computer Name) for this computer?

Manufacturer's COMPANY-13

Response:

WebCode Test	Response
28NKRK-5561	Company-13
2BXEJB-5561	COMPANY-13
2EUC34-5562	COMPANY-13
2UJN7X-5562	Company-13
2XN36N-5561	Company-13
36GUPN-5561	COMPANY-13
3CH2GJ-5562	[Participant did not return results for this question.]
3DBUC3-5561	Company-13
3K9LKW-5561	COMPANY-13
3LM236-5561	COMPANY-13
483YXK-5561	COMPANY-13
49DVEJ-5561	COMPANY-13
4K6LX2-5561	COMPUTER-13
4L6CCW-5562	COMPANY-13
4P6N9W-5561	COMPANY 13
4THJUL-5562	[Participant did not return results for this question.]
4XXRHK-5561	COMPANY-13
4Z77PR-5561	COMPANY-13
6KNFKX-5561	Company-13
6RLGDW-5561	COMPANY-13 (Company-13)
78YYBQ-5561	COMPANY-13

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3 - Examination Questions	
WebCode Test	Response
7M6APW-5561	COMPANY-13
7WAG6W-5561	Company-13
7WV3RK-5561	COMPANY-13
8ED4K3-5562	COMPANY-13
8LRYCP-5561	COMPANY-13
8P8Q2X-5561	Company-13
8RFV4L-5561	COMPANY-13
8W78WW-5562	COMPANY-13
98N78Y-5561	COMPANY-13
9J6THK-5561	Company-13
9QMRX6-5561	COMPANY-13
9XFKVP-5562	Company-13
AN93XR-5561	Company-13
AXDBED-5562	COMPANY-13
AXFVBT-5561	Company 13
B2ACZR-5562	COMPANY-13
BA4FBG-5561	COMPANY-13
BPGNBK-5562	COMPANY-13
BVMG7F-5561	COMPANY-13
BXTTXP-5561	COMPANY-13
CCXUMK-5561	COMPANY-13
CPQ4TQ-5561	COMPANY-13

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3 - Examination Questions	
WebCode Test	Response
D3A9ER-5561	COMPANY-13
D3MR2K-5561	COMPANY-13
D7C7PK-5562	Company-13
D8QG3R-5561	COMPANY-13
DCKG7E-5561	COMPANY-13
DKUYDR-5561	COMPANY-13
DKVPRL-5562	COMPANY-13
DPA82Q-5561	COMPANY-13
DTN8XH-5562	COMPANY-13
DXKMTK-5561	COMPANY-13
EJD6CG-5561	COMPANY-13
EJK3WT-5561	COMPANY-13
EMTM9G-5561	COMPANY-13
F3TPTL-5561	COMPANY-13
F7NG2H-5561	COMPANY-13
FG6CVN-5561	COMPANY-13
FT8J39-5561	COMPANY-13
G6U6KA-5561	COMPANY-13
G9BD99-5561	COMPANY-13
G9PQLK-5561	COMPANY-13
GALGEK-5562	COMPANY-13
GMPPAG-5561	COMPANY-13

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3 - Examination Questions	
WebCode Test	Response
H3X34J-5561	COMPANY-13
HAVVCD-5562	COMPANY-13
HFM3VL-5562	[Participant did not return results for this question.]
HGE2AK-5561	COMPANY-13
HMQYPK-5561	COMPANY-13
HTB6DE-5562	Company-13
HVJ3Y9-5561	Company-13
HYHLVF-5561	Company - 13
J3FCTE-5561	COMPANY-13
J49DM9-5561	COMPANY-13
JFURCD-5561	COMPANY-13
JPAH22-5562	Company-13
JXAZDE-5561	COMPANY-13
JXHVGK-5561	COMPANY-13
K3WXT8-5562	COMPANY-13
KA94ED-5562	COMPANY-13
KCQD3T-5561	COMPANY-13
KMHPR4-5561	COMPANY-13
LBJ6ZC-5562	COMPANY-13
LMDLPD-5561	Company-13
LRM3Y2-5562	Company-13
LWKE3D-5561	COMPANY 13

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3 - Examination Questions	
WebCode Test	Response
MCQ8YF-5561	COMPANY-13
MD8AY2-5561	Company-13
MK6QJE-5561	COMPANY-13
MR47EE-5562	COMPANY-13
MV6A9L-5561	COMPANY-13
N9Q2B2-5562	COMPANY-13
NH83FA-5562	Company-13
NNQD78-5561	COMPANY-13
NPUPBF-5562	COMPANY-13
NQ7BB3-5561	COMPANY-13
P3EHK8-5562	COMPANY-13
P3ER7C-5561	COMPANY-13
P6NMZG-5561	COMPANY-13
PE6G4X-5561	COMPANY-13
PYKJC4-5561	Company-13
Q4ZTN7-5562	COMPANY-13
Q73JRN-5561	COMPANY 13
RBARA4-5561	COMPANY-13
RE7DZL-5561	COMPANY-13
RUTBQ8-5561	COMPANY-13
RY7A78-5561	COMPANY-13
RZKKZ7-5562	COMPANY-13

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3 - Examination Questions	
WebCode Test	Response
T9UAE6-5561	Company-13
TH2XG4-5562	Not in scope
TTGXLB-5561	Company-13
U8973A-5561	COMPANY-13
UEQLM7-5561	COMPANY-13
UEWNPX-5561	COMPANY-13
UGNM4W-5561	Company-13
ULHG2X-5561	COMPANY-13
UPTW39-5562	COMPANY-13
UUA6Q9-5561	COMPANY-13
UZQMYA-5562	COMPANY-13
V66XC6-5562	COMPANY-13
V82HUJ-5561	Company-13
VXLE96-5561	company-13
VYTW7Z-5561	COMPANY-13
W447WA-5561	COMPANY-13
WB84Q8-5561	COMPANY-13
WBPY99-5561	COMPANY-13
WFVT36-5561	COMPANY-13
WH6VY2-5561	COMPANY-13
WL2PNP-5561	COMPANY-13
WL4AK7-5562	COMPANY-13

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3 - Examination Questions	
WebCode Test	Response
WQGWCP-5562	Company 13
X2AZR3-5561	Company-13
X3NFAB-5561	COMPANY-13
X62GKW-5561	Company-13
X84MXA-5561	COMPANY-13
XDQM3P-5561	COMPANY-13
XDT8Y6-5562	COMPANY-13
XLP32A-5562	COMPANY-13
XQXJAX-5561	COMPANY-13
Y2PJCZ-5561	Company-13
Y8WZT2-5561	COMPANY-13
YZK9WX-5561	COMPANY-13
Z4GR62-5562	COMPANY-13
Z4PAVK-5561	COMPANY-13
ZBUQRZ-5561	COMPANY-13
ZEU2MZ-5562	COMPANY-13
ZF7RW4-5561	COMPANY-13
ZN4C6R-5561	COMPANY-13
ZQ4URL-5562	COMPANY-13
ZU7QJ2-5561	COMPANY-13
ZWABN2-5562	COMPANY-13

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 3 - Examination Questions

Question 3: What is the hostname (Computer Name) for this computer?

Consensus Result:

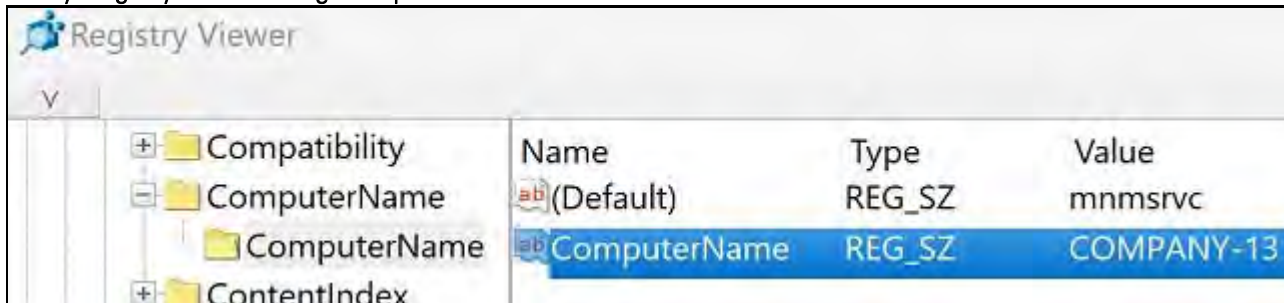
COMPANY-13

Manufacturer's Response Explanation:

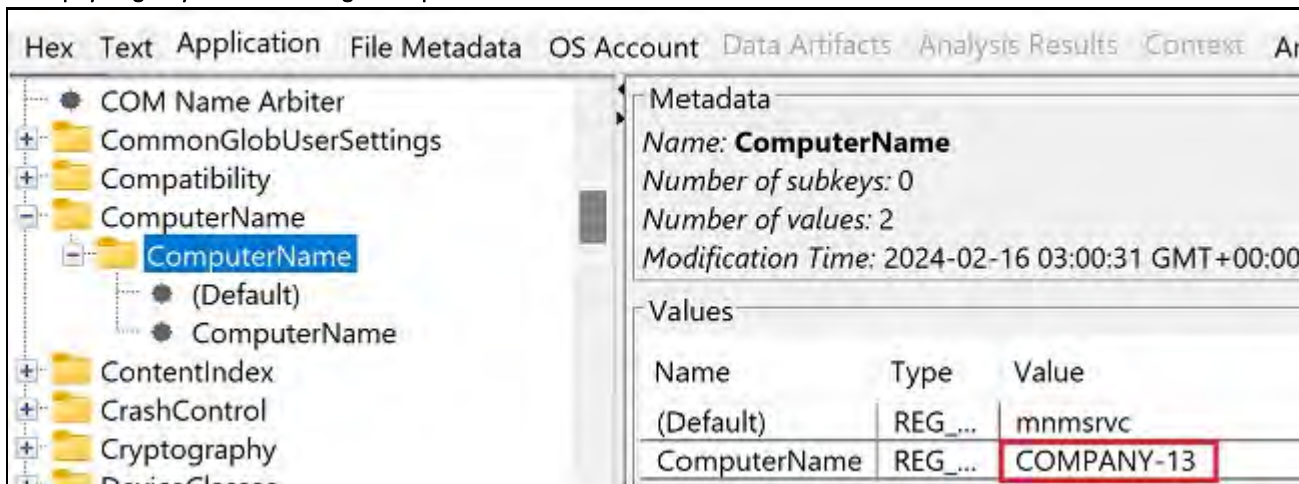
Windows Computer Name information is stored in the Windows System registry at ControlSet001\Control\ComputerName\ComputerName.

Manufacturer's Response Illustration:

X-ways registry view showing Computer Name information



Autopsy registry view showing Computer Name information



Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4 - Examination Questions

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

Manufacturer's Windows 10, Pro, 23H2; or Windows 11 Pro, 23H2

Response:

WebCode Test	Response
28NKRK-5561	Windows 11 Professional (2009), 6.3.
2BXEJB-5561	Axiom v8.2.0-Windows 11 Professional (2009), version 6.3, build 22631 / EnCase v23.4-Windows 10 Pro (2009), version 6.3, build 22631
2EUC34-5562	Windows 11 Professional, Ver 6.3 , Build: 22631
2UJN7X-5562	Windows 11 Professional (2009) v6.3
2XN36N-5561	Windows 10 Pro (Edition ID: Professional Display Version: 23H2)
36GUPN-5561	Windows 11 Professional (2009) 6.3 23H2
3CH2GJ-5562	[Participant did not return results for this question.]
3DBUC3-5561	Windows 23H2 Build 22631, Professional, Windows 11
3K9LKW-5561	Windows 11 Professional (23H2) Version 6.3 Build Number: 22631
3LM236-5561	Windows 11 Professional (2009)
483YXK-5561	Windows 11 Professional, 23H2
49DVEJ-5561	Windows 10 Pro 22631.3296
4K6LX2-5561	Windows 10 Professional edition, version 6.3, display version 23H2
4L6CCW-5562	Windows 11 (6.3 Professional 23H2)
4P6N9W-5561	Windows 10 Pro
4THJUL-5562	[Participant did not return results for this question.]
4XXRHK-5561	Installed OS: Windows 11 Professional (2009) Version: 6.3 Edition: Professional Display Version: 23H2
4Z77PR-5561	Windows 11 Professional 23H2
6KNFKX-5561	Windows 10 Professional, Display version = 23H2
6RLGDW-5561	Windows 11 Professional (2009) 22631 6.3

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4 - Examination Questions	
WebCode Test	Response
78YYBQ-5561	Windows 11 Professional 2009 Version 6.3
7M6APW-5561	Windows 11 Professional (2009), Current Version: 6.3, Display Version: 23H2
7WAG6W-5561	Windows 10 Pro, version 6.3, Display Version 23H2
7WV3RK-5561	Windows 11 Professional (2009), Version 6.3
8ED4K3-5562	include version: 6.3, edition: Windows 11 Professional, Display Version: 23H2
8LRYCP-5561	Windows 10, Pro, 23H2
8P8Q2X-5561	Windows 10 Pro Enterprise, installed 2/16/2-24 02:57:17 UTC
8RFV4L-5561	Windows 11 Professional 6.3
8W78WW-5562	Windows 11 Professional (2009) Version 6.3 Build number 22631
98N78Y-5561	Operating System Windows 11 Professional (2009) Version Number 6.3
9J6THK-5561	Windows 11 Professional (2009) Version 6.3
9QMRX6-5561	Windows 11 Professional 23H2
9XFKVP-5562	Windows 11 Professional (2009) 6.3
AN93XR-5561	Windows 11 Professional (2009) Version 6.3
AXDBED-5562	Windows 11 v10.0.22631 Professional 23H2
AXFVBT-5561	Windows 10 Pro
B2ACZR-5562	Windows 11 Professional
BA4FBG-5561	Windows 11 Professional (2009), version 6.3
BPGNBK-5562	Productname: Windows 10 pro, Edition: Professional, Currentversion: 6.3, Displayversion: 23H2
BVMG7F-5561	Windows Professional 11 (2009) Version 6.3
BXTTYP-5561	Windows 11 Professional (2009) 6.3
CCXUMK-5561	Windows 11 Professional (2000), Build Number 22631, Version 6.3

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4 - Examination Questions	
WebCode Test	Response
CPQ4TQ-5561	Windows 10 Pro, Enterprise, 23H2
D3A9ER-5561	Windows 10 Pro, Release ID 2009, Version 6.3, Display Version 23H2,
D3MR2K-5561	Windows 10 Pro, Version: 6.3, Edition: Professional, Display Version: 23H2
D7C7PK-5562	Windows 11 Professional (2009) v6.3, OS version = Professional, Build number = 22631, Product ID = 00330-80847-16684-AA181
D8QG3R-5561	Microsoft Windows 10 Professional Edition, Release ID: 2009
DCKG7E-5561	Windows 10 Professional 23H2
DKUYDR-5561	Windows 10 Professional, Display Version 23H2
DKVPRL-5562	Microsoft Windows 10 Professional 23H2
DPA82Q-5561	Windows 11 Professional (2009), Version 6.3, Build number 22631
DTN8XH-5562	Windows 11 Professional (2009) Version 6.3 Build number 22631 Display Version 23H2
DXKMTK-5561	Windows 11 Professional (2009) Version 6.3
EJD6CG-5561	Windows 11 Professional (2009)
EJK3WT-5561	Windows 10 Professional, v6.3 (23H2)
EMTM9G-5561	Windows 11 Professional (version 6.3 build number 22631)
F3TPTL-5561	Windows 11 Professional (2009), 6.3
F7NG2H-5561	Windows 11 Professional (2009) version number 6.3
FG6CVN-5561	Windows 11 Professional (2009) Version 6.3 Build 22631
FT8J39-5561	OS - Windows 11 Professional (2009), Version - 6.3, Edition - Professional, Display Version - 23H2
G6U6KA-5561	Windows 11 Professional (build 22631), version 6.3, 23H2
G9BD99-5561	Windows 11, Professional, 23H2 ("Current Version" listed in the registry is 6.3)
G9PQLK-5561	Windows 11 Professional (2009) version 6.3
GALGEK-5562	Windows 11 Professional (2009), Version 6.3, 23H2

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4 - Examination Questions	
WebCode Test	Response
GMPPAG-5561	Windows 11 Professional (2009) 6.3
H3X34J-5561	Windows 11 Professional, Version: 23H2, Build 22631, Release ID: 2009
HAVCD-5562	Windows 11 Professional (2009) v6.3 23H2
HFM3VL-5562	[Participant did not return results for this question.]
HGE2AK-5561	Windows 11 Professional, 23H2
HMQYPK-5561	Windows 11, Version 6.3, Edition Professional, Display Version 23H2
HTB6DE-5562	v6.3
HVJ3Y9-5561	Windows 11 Professional (2009) 6.3, Display Version 23H2
HYHLVF-5561	Windows 11 Professional (2009) 6.3
J3FCTE-5561	Windows 10 Pro
J49DM9-5561	Windows 10 Pro (2009 v6.3) Build 22621, however it had been upgraded to Windows 11 Pro (23H2)
JFURCD-5561	Windows 11 Professional (2009); Version 6.3; Build# 22631
JPAH22-5562	Windows 11 Professional 23H2 Build 22631
JXAZDE-5561	Microsoft Windows 10 Professional, Display Version 23H2,build number 22631
JXHVGK-5561	Windows 11 Professional (2009) Version 6.3
K3WXT8-5562	Windows 11 Professional (2009), ver.# 6.3
KA94ED-5562	Windows 11 Professional (2009) Version 6.3 compilation 22631
KCQD3T-5561	Windows 11; Version - 6.3; Edition - Professional; Display Version - 23H2
KMHPR4-5561	Windows 11, Professional edition, Version 6.3, Display version 23H2
LBJ6ZC-5562	Windows 11 Professional, 6.3, 23H2
LMDLPD-5561	Windows 10 Pro, current version 6.3 Edition Professional, Display version 23H2
LRM3Y2-5562	Windows 11 Professional (2009), 6.3.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4 - Examination Questions	
WebCode Test	Response
LWKE3D-5561	Windows 10 Pro 6.3
MCQ8YF-5561	Windows 11, Professional (2009), 6.3
MD8AY2-5561	Windows 11; 6.3; Professional; Display Version 23H2
MK6QJE-5561	Windows 11 Professional (2009), Version 6.3
MR47EE-5562	WINDOWS 11 PROFESSIONAL (2009) 6.3
MV6A9L-5561	Windows 11 Professional (2009)
N9Q2B2-5562	Windows 10 Professional 23H2
NH83FA-5562	OS: Windows 11 Professional 2009, Version No.: 6.3, Installed/Updated Date/Time: 16/02/2024 02:57:17, Product Key: 3MHG2-FDNH4-B7487-6PQKG-3V66T, Displayed Comp Name: Company-13, Build Number: 22631, Product ID: 00330-80847-16684-AA181
NNQD78-5561	Windows 11 Professional (2009) 6.3 Build 22631
NPUPBF-5562	Windows 11 Professional (2009), Version 6.3, Build number 22631
NQ7BB3-5561	Windows 11 Professional Version: 6.3 Edition: Professional Display Version: 23H2
P3EHK8-5562	Windows 11 Pro, 2009, 23H2, 6.3
P3ER7C-5561	Product name: Windows 10 Pro; Display version: 23H2; CompositionEditionID: Enterprise
P6NMZG-5561	Windows 11 Professional (2009), v6.3, build22631
PE6G4X-5561	Windows 11 Professional (2009), 6.3
PYKJC4-5561	Windows 11 Professional (2009)
Q4ZTN7-5562	Windows 10, Pro, 23H2
Q73JRN-5561	Windows 10 Professional Edition v6.3, Display Version 23H2
RBARA4-5561	Windows 11 Professional (2009), Build Number 22631, Display Version 6.3
RE7DZL-5561	Version: 6.3 Windows 11 Professional (2009) 23H2
RUTBQ8-5561	Windows 10 Pro (Display Version 23H2)
RY7A78-5561	Windows 10 Professional, version: 6.3, Display Version: 23H2

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4 - Examination Questions	
WebCode Test	Response
RZKKZ7-5562	Windows 11 Professional (2009) 6.3
T9UAE6-5561	Windows 11 Pro 23H2
TH2XG4-5562	Not in scope
TTGXLB-5561	OS: Windows 11, Edition: professional, Version: 6.3, Display Version: 23H2
U8973A-5561	Windows 10 Pro 6.3
UEQLM7-5561	Microsoft NTFS, Microsoft Windows 11 Professional (2009), Version 6.3, Build number 22631
UEWNPX-5561	Windows 11 Professional (2009) version 6.3
UGNM4W-5561	Windows 11 Pro, 6.3, Professional, 23H2
ULHG2X-5561	Windows 11 Professional (2009) ver. 6.3
UPTW39-5562	Windows 11 Professional, Ver 6.3 , Build: 22631
UUA6Q9-5561	Windows 11 Professional, 6.3, Build 22631, 23H2
UZQMYA-5562	OS Windows 11 Professional Version 6.3, Display Version 23H2.
V66XC6-5562	Windows, Version 6.3, Edition Professional, Display Version 23H2
V82HUJ-5561	Windows Pro 10 Version 6.3 (22361)
VXLE96-5561	OS: Microsoft Windows, Display Version: Windows 10 Pro version 2009, Build number 22631
YTW7Z-5561	Windows 11 Professional (2009)
W447WA-5561	Windows 11 Professional (2009) v. 6.3 build 22631
WB84Q8-5561	Windows 11 Professional, Ver 6.3 , Build: 22631
WBPY99-5561	Operating System: Windows 11 Pro (2009), Version: 6.3, Display Version: 23H2
WFVT36-5561	Windows 11 Professional (2009) Version Number 6.3 Build Number 22631
WH6VY2-5561	Windows 11 Professional (2009) Version Number 6.3
WL2PNP-5561	Windows 10 Professional , Version 6.3, edition: Professional, Display Version 23H2, Build Number 22631 .

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4 - Examination Questions	
WebCode Test	Response
WL4AK7-5562	Windows 11 Professional (2009) version 6.3
WQGWCP-5562	Windows 11 Professional 23H2
X2AZR3-5561	Windows 10 Pro 6.3
X3NFAB-5561	Windows 11 Professional (2009), version 6.3, build number: 22631
X62GKW-5561	Windows 11 Pro (Build 22631) Display Version: 23H2
X84MXA-5561	Version: 6.3 (Build 22631) Edition: Windows 10 Pro (Professional) Display Version: 23H2
XDQM3P-5561	Windows 11 Professional / Version 6.3 / 23H2
XDT8Y6-5562	Windows 11 Professional (2209), v6.3, build 22631, display version 23H2 - Note that it displayed Windows 10 in registry despite being a Windows 11 build#.
XLP32A-5562	Windows 10 Pro 22631, 23H2(DisplayVersion)
XQXJAX-5561	Operating System – Windows 11 Version – 6.3 Edition – Professional Display Version – 23H2 Build - 22631
Y2PJCZ-5561	Windows 11 Professional, 6.3, 23H2, Build number 22631
Y8WZT2-5561	Windows 11 version 6.3, Professional, 23H2
YZK9WX-5561	Windows 11 Professional (2009), Build Number 22631, Display Version 6.3
Z4GR62-5562	Microsoft Windows 11 Professional (DisplayVersion=23H2, CurrentVersion=6.3) **SEE Additional Comments**
Z4PAVK-5561	Windows 10 Pro, version 6.3, Enterprise, 23H2
ZBUQRZ-5561	Windows 11 Professional (2009), version 6.3
ZEU2MZ-5562	Windows 10 Pro 23H2
ZF7RW4-5561	Windows 10 Pro (64-bit) , Version:23H2 , Build: 22631
ZN4C6R-5561	Windows 11 Professional (2009) version 6.3
ZQ4URL-5562	Windows 11 Professional (2009) Version Number 6.3 Build Number 22631 Display Version 23H2
ZU7QJ2-5561	Windows 10 Pro (Professional) 23H2
ZWABN2-5562	Windows 11 Professional 6.3 23H2

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 4 - Examination Questions

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

Consensus Result:

Windows 10 Pro or 11 Pro. Due to the low quantity of participants reporting the display version, 23H2, this component was excluded.

Manufacturer's Response Explanation:

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.

Manufacturer's Response Illustration:

Autopsy registry view showing Windows version and edition in the Software registry hive

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other																														
<div style="display: flex;"> <div style="width: 30%; border-right: 1px solid #ccc; padding-right: 5px;"> <ul style="list-style-type: none"> Windows Media Player NSS Windows Messaging Subsystem Windows NT <ul style="list-style-type: none"> <li style="background-color: #e0e0e0;">CurrentVersion Windows Photo Viewer Windows Portable Devices Windows Script Host Windows Search Windows Security Health WindowsMitigation WindowsRuntime WindowsSelfHost WindowsUpdate Wisp WlanSvc Wlpassvc Wow64 </div> <div style="width: 70%; padding-left: 5px;"> <p>Metadata</p> <p>Name: CurrentVersion Number of subkeys: 96 Number of values: 32 Modification Time: 2024-03-14 03:01:20 GMT+00:00</p> <hr/> <p>Values</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>DisplayVersion</td> <td>REG_SZ</td> <td style="border: 1px solid red;">23H2</td> </tr> <tr> <td>EditionID</td> <td>REG_SZ</td> <td>Professional</td> </tr> <tr> <td>EditionSubManufacturer</td> <td>REG_SZ</td> <td>(value not set)</td> </tr> <tr> <td>EditionSubstring</td> <td>REG_SZ</td> <td>(value not set)</td> </tr> <tr> <td>EditionSubVersion</td> <td>REG_SZ</td> <td>(value not set)</td> </tr> <tr> <td>InstallationType</td> <td>REG_SZ</td> <td>Client</td> </tr> <tr> <td>InstallDate</td> <td>REG_DWOR...</td> <td>0x65cecf0d (1708052237)</td> </tr> <tr> <td>ProductName</td> <td>REG_SZ</td> <td style="border: 1px solid red;">Windows 10 Pro</td> </tr> <tr> <td>Releaseld</td> <td>REG_SZ</td> <td>2009</td> </tr> </tbody> </table> </div> </div>										Name	Type	Value	DisplayVersion	REG_SZ	23H2	EditionID	REG_SZ	Professional	EditionSubManufacturer	REG_SZ	(value not set)	EditionSubstring	REG_SZ	(value not set)	EditionSubVersion	REG_SZ	(value not set)	InstallationType	REG_SZ	Client	InstallDate	REG_DWOR...	0x65cecf0d (1708052237)	ProductName	REG_SZ	Windows 10 Pro	Releaseld	REG_SZ	2009
Name	Type	Value																																					
DisplayVersion	REG_SZ	23H2																																					
EditionID	REG_SZ	Professional																																					
EditionSubManufacturer	REG_SZ	(value not set)																																					
EditionSubstring	REG_SZ	(value not set)																																					
EditionSubVersion	REG_SZ	(value not set)																																					
InstallationType	REG_SZ	Client																																					
InstallDate	REG_DWOR...	0x65cecf0d (1708052237)																																					
ProductName	REG_SZ	Windows 10 Pro																																					
Releaseld	REG_SZ	2009																																					

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

Name	Type	Value
CurrentBuildNumber	REG_SZ	22631
CurrentMajorVersionNumber	REG_DWORD	0x0000000A (10)
CurrentMinorVersionNumber	REG_DWORD	0x00000000 (0)
CurrentType	REG_SZ	Multiprocessor Free
CurrentVersion	REG_SZ	6.3
DisplayVersion	REG_SZ	23H2
EditionID	REG_SZ	Professional
EditionSubManufacturer	REG_SZ	
EditionSubstring	REG_SZ	
EditionSubVersion	REG_SZ	
InstallationType	REG_SZ	Client
InstallDate	REG_DWORD	0x65CECF0D (1708052237)
ProductName	REG_SZ	Windows 10 Pro

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 5 - Examination Questions

Question 5: To what domain was this computer joined?

Manufacturer's EmergencyServices.Winchestertonfieldville.org

Response:

WebCode Test	Response
28NKRK- 5561	EmergencyServices.Winchestertonfieldville.org
2BXEJB- 5561	EmergencyServices.Winchestertonfieldville.org
2EUC34- 5562	EmergencyServices.Winchestertonfieldville.org
2UJN7X- 5562	EmergencyServices.Winchestertonfieldville.org
2XN36N- 5561	EmergencyServices.Winchestertonfieldville.org
36GUPN- 5561	EmergencyServices.Winchestertonfieldville.org
3CH2GJ- 5562	[Participant did not return results for this question.]
3DBUC3- 5561	EmergencyServices.Winchestertonfieldville.org
3K9LKW- 5561	EMERGENCYSERVIC
3LM236- 5561	EmergencyServices.Winchestertonfieldville.org
483YXK- 5561	EmergencyServices.Winchestertonfieldville.org
49DVEJ- 5561	EmergencyServices.Winchestertonfieldville.org
4K6LX2- 5561	EmergencyServices.Winchestertonfieldville.org
4L6CCW- 5562	EmergencyServices.Winchestertonfieldville.org
4P6N9W- 5561	EmergencyServices.Winchestertonfieldville.org
4THJUL- 5562	[Participant did not return results for this question.]
4XXRHK- 5561	EmergencyServices.Winchestertonfieldville.org
4Z77PR- 5561	EmergencyServices.Winchestertonfieldville.org
6KNFKX- 5561	EmergencyServices.Winchestertonfieldville.org
6RLGDW- 5561	EmergencyServices.Winchestertonfieldville.org
78YYBQ- 5561	EmergencyServices.Winchestertonfieldville.org

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 5 - Examination Questions	
WebCode Test	Response
7M6APW-5561	EmergencyServices.Winchestertonfieldville.org
7WAG6W-5561	EmergencyServices.Winchestertonfieldville.org
7WV3RK-5561	EmergencyServices.Winchestertonfieldville.org
8ED4K3-5562	EmergencyServices.Winchestertonfieldville.org
8LRYCP-5561	EmergencyServices.Winchestertonfieldville.org
8P8Q2X-5561	EmergencyServices.Winchestertonfieldville.org
8RFV4L-5561	EmergencyServices.Winchestertonfieldville.org
8W78WW-5562	EmergencyServices.Winchestertonfieldville.org
98N78Y-5561	EmergencyServices.Winchestertonfieldville.org
9J6THK-5561	EmergencyServices.Winchestertonfieldville.org
9QMRX6-5561	EmergencyServices.Winchestertonfieldville.org
9XFKVP-5562	EMERGENCYSERVIC EmergencyServices.Winchestertonfieldville.org
AN93XR-5561	EMERGENCYSERVIC
AXDBED-5562	EmergencyServices.Winchestertonfieldville.org
AXFVBT-5561	EmergencyServices.Winchestertonfieldville.org
B2ACZR-5562	EmergencyServices.Winchestertonfieldville.org
BA4FBG-5561	EmergencyServices.Winchestertonfieldville.org
BPGNBK-5562	EmergencyServices.Winchestertonfieldville.org
BVMG7F-5561	EmergencyServices.Winchestertonfieldville.org
BXTTTP-5561	EmergencyServices.Winchestertonfieldville.org
CCXUMK-5561	EmergencyServices.Winchestertonfieldville.org
CPQ4TQ-5561	EmergencyServices.Winchestertonfieldville.org

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 5 - Examination Questions	
WebCode Test	Response
D3A9ER-5561	EmergencyServices.Winchestertonfieldville.org
D3MR2K-5561	EmergencyServices.Winchestertonfieldville.org
D7C7PK-5562	EmergencyServices.Winchestertonfieldville.org
D8QG3R-5561	EmergencyServices.Winchestertonfieldville.org
DCKG7E-5561	EMERGENCYSERVICES.WINCHESTERTONFIELDVILLE.ORG
DKUYDR-5561	EmergencyServicesWinchestertonfieldville.org
DKVPRL-5562	EmergencyServices.Winchestertonfieldville.org
DPA82Q-5561	EmergencyServices.Winchestertonfieldville.org
DTN8XH-5562	EmergencyServices.Winchestertonfieldville.org
DXKMTK-5561	EmergencyServices.Winchestertonfieldville.org
EJD6CG-5561	EmergencyServices.Winchestertonfieldville.org
EJK3WT-5561	EmergencyServices.Winchestertonfieldville.org
EMTM9G-5561	EmergencyServices.Winchestertonfieldville.org
F3TPTL-5561	EmergencyServices.Winchestertonfieldville.org
F7NG2H-5561	EmergencyServices.Winchestertonfieldville.org
FG6CVN-5561	EmergencyServices.Winchestertonfieldville.org
FT8J39-5561	EmergencyServices.Winchestertonfieldville.org
G6U6KA-5561	EmergencyServices.Winchestertonfieldville.org
G9BD99-5561	EmergencyServices.Winchestertonfieldville.org
G9PQLK-5561	EmergencyServices.Winchestertonfieldville.org
GALGEK-5562	EmergencyServices.Winchestertonfieldville.org
GMPPAG-5561	EmergencyServices.Winchestertonfieldville.org

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 5 - Examination Questions	
WebCode Test	Response
H3X34J-5561	EmergencyServices.Winchestertonfieldville.org
HAVVCD-5562	EmergencyServices.Winchestertonfieldville.org
HFM3VL-5562	[Participant did not return results for this question.]
HGE2AK-5561	EmergencyServices.Winchestertonfieldville.org
HMQYPK-5561	EmergencyServices.Winchestertonfieldville.org
HTB6DE-5562	EmergencyServices.Winchestertonfieldville.org
HVJ3Y9-5561	EmergencyServices.Winchestertonfieldville.org
HYHLVF-5561	EmergencyServices.Winchestertonfieldville.org
J3FCTE-5561	EmergencyServices.Winchestertonfieldville.org
J49DM9-5561	EmergencyServices.Winchestertonfieldville.org
JFURCD-5561	EmergencyServices.Winchestertonfieldville.org
JPAH22-5562	EmergencyServices.Winchestertonfieldville.org
JXAZDE-5561	EmergencyServices.Winchestertonfieldville.org
JXHVGK-5561	EmergencyServices.Winchestertonfieldville.org
K3WXT8-5562	EmergencyServices.Winchestertonfieldville.org
KA94ED-5562	EmergencyServices.Winchestertonfieldville.org
KCQD3T-5561	EmergencyServices.Winchestertonfieldville.org
KMHPR4-5561	EmergencyServices.Winchestertonfieldville.org
LBJ6ZC-5562	EmergencyServices.Winchestertonfieldville.org
LMDLPD-5561	EMERGENCYSERVICE
LRM3Y2-5562	EmergencyServices.Winchestertonfieldville.org
LWKE3D-5561	Winchestertonfieldville_Fire

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 5 - Examination Questions	
WebCode Test	Response
MCQ8YF-5561	EmergencyServices.Winchestertonfieldville.org
MD8AY2-5561	EmergencyServices.Winchestertonfieldville.org
MK6QJE-5561	EmergencyServices.Winchestertonfieldville.org
MR47EE-5562	EmergencyServices.Winchestertonfieldville.org
MV6A9L-5561	EMERGENCYSERVIC
N9Q2B2-5562	EmergencyServices.Winchestertonfieldville.org (EMERGENCYSERVIC)
NH83FA-5562	EmergencyServices.Winchestertonfieldville.org (EMERGENCYSERVIC)
NNQD78-5561	EmergencyServices.Winchestertonfieldville.org
NPUPBF-5562	EmergencyServices.Winchestertonfieldville.org
NQ7BB3-5561	EmergencyServices.Winchestertonfieldville.org
P3EHK8-5562	EmergencyServices.Winchestertonfieldville.org
P3ER7C-5561	EmergencyServices.Winchestertonfieldville.org
P6NMZG-5561	EmergencyServices.Winchestertonfieldville.org
PE6G4X-5561	EmergencyServices.Winchestertonfieldville.org
PYKJC4-5561	EmergencyServices.Winchestertonfieldville.org
Q4ZTN7-5562	EmergencyServices.Winchestertonfieldville.org
Q73JRN-5561	EmergencyServicesWinchestertonfieldville.org
RBARA4-5561	EmergencyServices.Winchestertonfieldville.org
RE7DZL-5561	EmergencyServices.Winchestertonfieldville.org
RUTBQ8-5561	EmergencyServices.Winchestertonfieldville.org
RY7A78-5561	Winchestertonfieldville_Fire
RZKKZ7-5562	EmergencyServices.Winchestertonfieldville.org

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 5 - Examination Questions	
WebCode Test	Response
T9UAE6-5561	EmergencyServices.Winchestertonfieldville.org
TH2XG4-5562	Not in scope
TTGXLB-5561	EmergencyServices.Winchestertonfieldville.org
U8973A-5561	Emergency Services.Winchestertonfieldville.org
UEQLM7-5561	EmergencyServices.Winchestertonfieldville.org
UEWNPX-5561	EmergencyServices.Winchestertonfieldville.org
UGNM4W-5561	EmergencyServices.Winchestertonfieldville.org
ULHG2X-5561	EmergencyServices.Winchestertonfieldville.org
UPTW39-5562	EmergencyServices.Winchestertonfieldville.org
UUA6Q9-5561	EmergencyServices.Winchestertonfieldville.org
UZQMYA-5562	EmergencyServices.Winchestertonfieldville.org
V66XC6-5562	EmergencyServices.Winchestertonfieldville.org
V82HUJ-5561	EmergencyServices.Winchestertonfieldville.org
VXLE96-5561	EmergencyServices.Winchestertonfieldville.org
VYTW7Z-5561	EmergencyServices.Winchestertonfieldville.org
W447WA-5561	Emergency Services
WB84Q8-5561	EmergencyServices.Winchestertonfieldville.org
WBPY99-5561	EmergencyServices.Winchestertonfieldville.org
WFVT36-5561	EmergencyServices.Winchestertonfieldville.org domain
WH6VY2-5561	EmergencyServices.Winchestertonfieldville.org
WL2PNP-5561	EmergencyServices.Winchestertonfieldville.org
WL4AK7-5562	EmergencyServices.Winchestertonfieldville.org

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 5 - Examination Questions	
WebCode Test	Response
WQGWCP-5562	EmergencyServices.Winchestertonfieldville.org
X2AZR3-5561	EMERGENCYSERVIC
X3NFAB-5561	EmergencyServices.Winchestertonfieldville.org
X62GKW-5561	EmergencyServices.Winchestertonfieldville.org / EMERGENCYSERVIC
X84MXA-5561	EmergencyServices.Winchestertonfieldville.org
XDQM3P-5561	EmergencyServices.Winchestertonfieldville.org
XDT8Y6-5562	EmergencyServices.Winchestertonfieldville.org
XLP32A-5562	EmergencyServices.Winchestertonfieldville.org
XQXJAX-5561	EmergencyServices.Winchestertonfieldville.org
Y2PJCZ-5561	EmergencyServices.Winchestertonfieldville.org
Y8WZT2-5561	EmergencyServices.Winchestertonfieldville.org
YZK9WX-5561	EmergencyServices.Winchestertonfieldville.org
Z4GR62-5562	EMERGENCYSERVIC **SEE Additional Comments**
Z4PAVK-5561	CN=COMPANY-13,CN=Computers,DC=EmergencyServices,DC=Winchestertonfieldville,DC=org
ZBUQRZ-5561	Ian
ZEU2MZ-5562	EmergencyServices.Winchestertonfieldville.org
ZF7RW4-5561	EmergencyServices.Winchestertonfieldville.org
ZN4C6R-5561	EmergencyServices.Winchestertonfieldville.org
ZQ4URL-5562	EmergencyServices.Winchestertonfieldville.org
ZU7QJ2-5561	EmergencyServices.Winchestertonfieldville.org
ZWABN2-5562	EmergencyServices.Winchestertonfieldville.org

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 5 - Examination Questions

Question 5: To what domain was this computer joined?

Consensus Result:

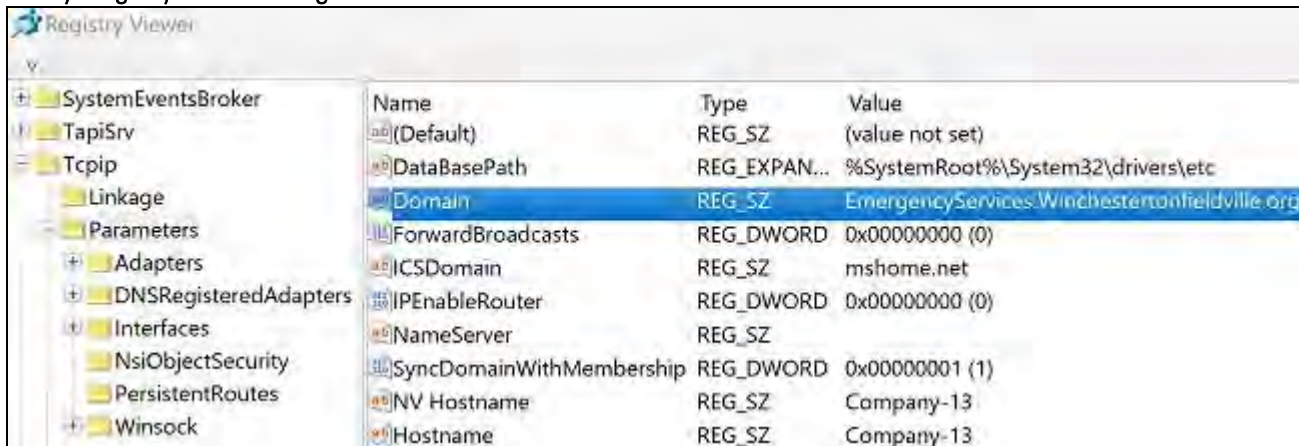
EmergencyServices.Winchestertonfieldville.org and slight variations if it was easily determined to be a typographical error.

Manufacturer's Response Explanation:

Windows domain membership system information is found in the System registry at C:\Windows\System32\Config\System: \CurrentControlSet\Services\Tcpip\Parameters\Domain.

Manufacturer's Response Illustration:

X-rays registry view showing domain information



Autopsy registry view showing domain information



Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6 - Examination Questions

Question 6: What warning banner / legal notice text was displayed to users at the Windows logon screen? Provide the first two sentences of the warning.

Manufacturer's Response: This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.

WebCode Test	Response
28NKRK-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
2BXEJB-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
2EUC34-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
2UJN7X-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
2XN36N-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
36GUPN-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
3CH2GJ-5562	[Participant did not return results for this question.]
3DBUC3-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
3K9LKW-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
3LM236-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only. All data contained on department computer systems is owned by the department and all use may be monitored, intercepted, recorded, read, copied, or captured in any manner, and disclosed in any manner. Users have no expectation of privacy on this system!
483YXK-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
49DVEJ-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
4K6LX2-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
4L6CCW-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
4P6N9W-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
4THJUL-5562	[Participant did not return results for this question.]
4XXRHK-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
4Z77PR-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
6KNFKX-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6 - Examination Questions	
WebCode Test	Response
6RLGDW-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
78YYBQ-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
7M6APW-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
7WAG6W-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
7WV3RK-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
8ED4K3-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
8LRYCP-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
8P8Q2X-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
8RFV4L-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
8W78WW-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
98N78Y-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
9J6THK-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
9QMRX6-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
9XFKVP-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
AN93XR-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
AXBED-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
AXFVBT-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only. All data contained on department computer systems is owned by the department and all use may be monitored, intercepted, recorded, read, copied, or captured in any manner, and disclosed in any manner.
B2ACZR-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonville municipal computer systems are provided for official use only.
BA4FBG-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
BPGNBK-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
BVMG7F-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
BXTTXP-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6 - Examination Questions	
WebCode Test	Response
CCXUMK-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
CPQ4TQ-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
D3A9ER-5561	****WARNING**** This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only. All data contained on department computer systems is owned by the department and all use may be monitored, intercepted, recorded, read, copied, or captured in any manner, and disclosed in any manner. Users have no expectation of privacy on this system!..
D3MR2K-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
D7C7PK-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
D8QG3R-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
DCKG7E-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
DKUYDR-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
DKVPR-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
DPA82Q-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
DTN8XH-5562	****WARNING*** This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only. All data contained on department computer systems is owned by the department and all use may be monitored, intercepted, recorded, read, copied, or captured in any manner, and disclosed in any manner. Users have no expectation of privacy on this system!" Whether "****WARNING****" counts as a sentence is debatable. Also, whilst I have included the paragraph above, technically, the two sentences are, 1: This is a Winchestertonfieldville municipal computer system. And, 2: Winchestertonfieldville municipal computer systems are provided for official use only.
DXKMTK-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
EJD6CG-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
EJK3WT-5561	"This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only. All data contained on department computer systems is owned by the department and all use may be monitored, intercepted, recorded, read, copied, or captured in any manner, and disclosed in any manner."
EMTM9G-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
F3TPTL-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
F7NG2H-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
FG6CVN-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
FT8J39-5561	Banner - ****WARNING*** Legal Notice - This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6 - Examination Questions	
WebCode Test	Response
G6U6KA-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
G9BD99-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
G9PQLK-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
GALGEK-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
GMPPAG-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
H3X34J-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
HAVCD-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
HFM3VL-5562	[Participant did not return results for this question.]
HGE2AK-5561	"This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only."
HMQYPK-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only. All data contained on department computer systems is owned by the department and all use may be monitored, intercepted, recorded, read, copied, or captured in any manner, and disclosed in any manner. Users have no expectation of privacy on this system!
HTB6DE-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
HVJ3Y9-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
HYHLVF-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
J3FCTE-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
J49DM9-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
JFURCD-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
JPAH22-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
JXAZDE-5561	This is Wincherstertonfieldville municipal computer system. Wincherstertonfieldville municipal computer systems are provided for official use only.
JXHV GK-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
K3WXT8-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
KA94ED-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
KCQD3T-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6 - Examination Questions	
WebCode Test	Response
KMHPR4-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
LBJ6ZC-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
LMDLPD-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
LRM3Y2-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
LWKE3D-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
MCQ8YF-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
MD8AY2-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
MK6QJE-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only. All data contained on department computer systems is owned by the department and all use may be monitored, intercepted, recorded, read, copied, or captured in any manner, and disclosed in any manner. Users have no expectation of privacy on this system!
MR47EE-5562	"This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only".
MV6A9L-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
N9Q2B2-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
NH83FA-5562	This is a Winchestertonville municipal computer system. Winchestertonville municipal computer systems are provided for official use only.
NNQD78-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
NPUPBF-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
NQ7BB3-5561	"This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only."
P3EHK8-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
P3ER7C-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
P6NMZG-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only. All data contained on department computer systems is owned by the department and all use may be monitored, intercepted, recorded, read, copied, or captured in any manner, and disclosed in any manner. Users have no expectation of privacy on this system!
PE6G4X-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
PYKJC4-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
Q4ZTN7-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6 - Examination Questions	
WebCode Test	Response
Q73JRN-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
RBARA4-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
RE7DZL-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
RUTBQ8-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
RY7A78-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
RZKKZ7-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
T9UAE6-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
TH2XG4-5562	Not in scope
TTGXLB-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
U8973A-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
UEQLM7-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
UEWNPX-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
UGNM4W-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
ULHG2X-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only. All data contained on department computer systems is owned by the department and all use may be monitored, intercepted, recorded, read, copied, or captured in any manner, and disclosed in any manner.
UPTW39-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
UUA6Q9-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
UZQMYA-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
V66XC6-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
V82HUJ-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
VXLE96-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
VYTW7Z-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only. All data contained on department computer systems is owned by the department and all use may be monitored, intercepted, recorded, read, copied, or captured in any manner, and disclosed in any manner. Users have no expectation of privacy on this system!

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6 - Examination Questions	
WebCode Test	Response
W447WA-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
WB84Q8-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
WBPY99-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
WFVT36-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
WH6VY2-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
WL2PNP-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
WL4AK7-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
WQGWCPC-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
X2AZR3-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
X3NFAB-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
X62GKW-5561	****WARNING*** This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only. All data contained on department computer systems is owned by the department and all use may be monitored, intercepted, recorded, read, copied, or captured in any manner, and disclosed in any manner. Users have no expectation of privacy on this system!
X84MXA-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
XDQM3P-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
XDT8Y6-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
XLP32A-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
XQXJAX-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
Y2PJCZ-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
Y8WZT2-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
YZK9WX-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
Z4GR62-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
Z4PAVK-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
ZBUQRZ-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6 - Examination Questions	
WebCode Test	Response
ZEU2MZ-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
ZF7RW4-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
ZN4C6R-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
ZQ4URL-5562	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
ZU7QJ2-5561	This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only.
ZWABN2-5562	****WARNING***

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6 - Examination Questions

Question 6: What warning banner / legal notice text was displayed to users at the Windows logon screen? Provide the first two sentences of the warning.

Consensus Result:

"This is a Winchestertonfieldville municipal computer system. Winchestertonfieldville municipal computer systems are provided for official use only." Any slight variation of this response was disregarded as an outlier if it was easily determined to be a typographical error or additional text from the notice.

Manufacturer's Response Explanation:

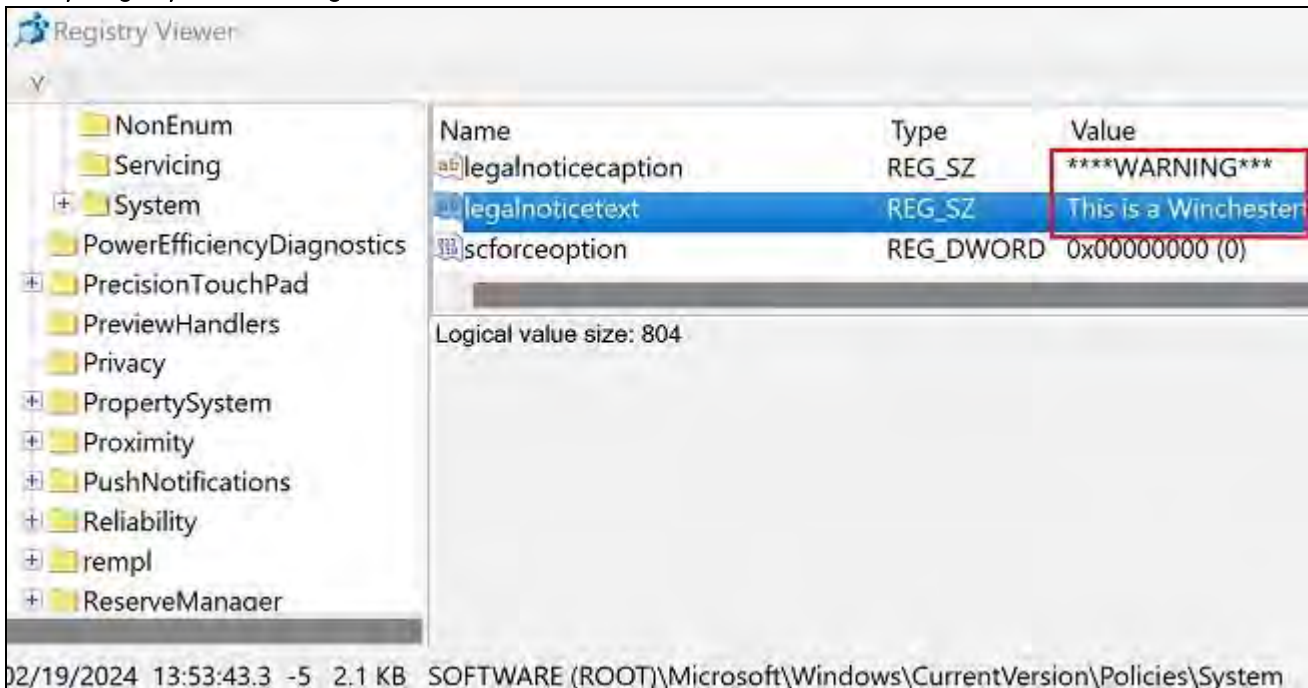
Windows warning banner and legal notice text is stored in the SOFTWARE registry at C:\Windows\System32\Config\SOFTWARE: \Microsoft\Windows\CurrentVersion\Policies\System\legalnoticecaption and legalnoticetext.

Manufacturer's Response Illustration:

logon screenshot



X-ways registry view showing domain information



Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 6 - Examination Questions

Autopsy registry view showing legal notice information

The screenshot shows the Windows Registry Editor interface. The left pane displays a tree view of the registry, with the 'System' key expanded under 'Policies'. The right pane shows the 'Values' section for the 'System' key, listing several registry values. Two values are highlighted in blue: 'legalnoticecaption' and 'legalnoticetext'.

Metadata		
Name: System		
Number of subkeys: 2		
Number of values: 21		
Modification Time: 2024-02-19 18:53:43 GMT+00:00		
Values		
Name	Type	Value
SupportFullTrustStartupTasks	REG_DWOR...	0x00000001 (1)
SupportUwpStartupTasks	REG_DWOR...	0x00000001 (1)
ValidateAdminCodeSignatures	REG_DWOR...	0x00000000 (0)
dontdisplaylastusername	REG_DWOR...	0x00000000 (0)
legalnoticecaption	REG_SZ	****WARNING***
legalnoticetext	REG_SZ	This is a Winchest
scforceoption	REG_DWOR...	0x00000000 (0)

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7 - Examination Questions

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

Manufacturer's Pacific Time

Response:

WebCode Test	Response
28NKRK-5561	Pacific Standard Time
2BXEJB-5561	Pacific Standard Time
2EUC34-5562	Winchestertonfieldville_Fire
2UJN7X-5562	Pacific Standard Time
2XN36N-5561	Pacific Standard Time
36GUPN-5561	Pacific Daylight Time
3CH2GJ-5562	[Participant did not return results for this question.]
3DBUC3-5561	Pacific Standard Time
3K9LKW-5561	Pacific Standard Time
3LM236-5561	Pacific Standard Time
483YXK-5561	Pacific Daylight Time
49DVEJ-5561	Pacific Standard Time
4K6LX2-5561	Pacific Daylight Time
4L6CCW-5562	Pacific Standard Time
4P6N9W-5561	Pacific Standard Time
4THJUL-5562	[Participant did not return results for this question.]
4XXRHK-5561	Pacific Daylight Time (-7 hrs (0x01A4))
4Z77PR-5561	Pacific Daylight Time
6KNFKX-5561	Pacific Standard Time
6RLGDW-5561	Pacific Daylight Time (-420)

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7 - Examination Questions	
WebCode Test	Response
78YYBQ-5561	Pacific Daylight Time
7M6APW-5561	Pacific Standard Time
7WAG6W-5561	Pacific Standard Time
7WV3RK-5561	Pacific Standard Time
8ED4K3-5562	Pacific Standard Time
8LRYCP-5561	Pacific Standard Time
8P8Q2X-5561	Pacific Standard Time
8RFV4L-5561	Pacific Standard Time
8W78WW-5562	Pacific Daylight Time
98N78Y-5561	Pacific Standard Time
9J6THK-5561	Pacific Standard Time
9QMRX6-5561	Pacific Daylight Time
9XFKVP-5562	Pacific Standard Time
AN93XR-5561	Pacific Standard Time
AXDBED-5562	Pacific Daylight Time
AXFVBT-5561	America/New York (Eastern Standard time)
B2ACZR-5562	Pacific Standard Time
BA4FBG-5561	Pacific Standard Time
BPGNBK-5562	(UTC-08:00) Pacific Time (US & Canada)
BVMG7F-5561	Pacific Standard Time
BXTTYP-5561	Pacific Daylight Time
CCXUMK-5561	Pacific Daylight Time

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7 - Examination Questions	
WebCode Test	Response
CPQ4TQ-5561	Pacific Standard Time
D3A9ER-5561	Pacific Standard Time
D3MR2K-5561	Pacific Standard Time
D7C7PK-5562	Pacific Standard Time (UTC-08:00) Pacific Time (US & Canada)
D8QG3R-5561	Pacific Standard Time
DCKG7E-5561	Pacific Standard Time
DKUYDR-5561	Pacific Standard Time
DKVPRL-5562	Pacific Standard Time
DPA82Q-5561	Pacific Standard Time
DTN8XH-5562	Pacific Daylight Time
DXKMTK-5561	Pacific Standard Time
EJD6CG-5561	Pacific Standard Time
EJK3WT-5561	Pacific Standard time
EMTM9G-5561	Pacific Standard Time
F3TPTL-5561	Pacific Standard Time
F7NG2H-5561	Pacific Standard Time
FG6CVN-5561	Pacific Standard Time
FT8J39-5561	Pacific Standard Time
G6U6KA-5561	Pacific Daylight Time
G9BD99-5561	Pacific Daylight Time
G9PQLK-5561	Pacific Standard Time
GALGEK-5562	Pacific Standard Time

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7 - Examination Questions	
WebCode Test	Response
GMPPAG-5561	Pacific Daylight Time
H3X34J-5561	Pacific Standard Time
HAWCD-5562	Pacific Standard Time
HFM3VL-5562	[Participant did not return results for this question.]
HGE2AK-5561	Pacific Daylight Time
HMQYPK-5561	Pacific Standard Time
HTB6DE-5562	Pacific Daylight Time
HVJ3Y9-5561	Pacific Daylight Time
HYHLVF-5561	Pacific Standard Time
J3FCTE-5561	Pacific Daylight Time
J49DM9-5561	Pacific Standard Time
JFURCD-5561	Pacific Daylight Time
JPAH22-5562	Pacific Standard Time
JXAZDE-5561	Pacific Standard Time
JXHV GK-5561	Pacific Daylight Time
K3WXT8-5562	Pacific Standard Time
KA94ED-5562	(UTC-08:00) Pacific Time (US & Canada)
KCQD3T-5561	Pacific Standard Time
KMHPR4-5561	Pacific Time
LBJ6ZC-5562	Pacific Daylight Time (PDT/PST)
LMDLPD-5561	Pacific Daylight Time
LRM3Y2-5562	Pacific Standard Time

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7 - Examination Questions	
WebCode Test	Response
LWKE3D-5561	Pacific Standard Time
MCQ8YF-5561	Pacific Standard Time
MD8AY2-5561	Pacific Standard Time
MK6QJE-5561	Pacific Standard Time
MR47EE-5562	Pacific Daylight Time (Pacific Standard Time)
MV6A9L-5561	Pacific Daylight Time
N9Q2B2-5562	Pacific Standard Time
NH83FA-5562	Pacific Daylight Time
NNQD78-5561	Pacific Daylight Time
NPUPBF-5562	Pacific Standard Time
NQ7BB3-5561	Pacific Standard Time
P3EHK8-5562	Pacific Standard Time
P3ER7C-5561	Pacific Standard Time
P6NMZG-5561	Pacific Standard Time
PE6G4X-5561	Pacific Standard Time, -420
PYKJC4-5561	Pacific Standard Time
Q4ZTN7-5562	Pacific Standard Time
Q73JRN-5561	Pacific Standard Time
RBARA4-5561	Pacific Daylight Time
RE7DZL-5561	Pacific Daylight Time
RUTBQ8-5561	Pacific Standard Time
RY7A78-5561	Pacific Standard Time

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7 - Examination Questions	
WebCode Test	Response
RZKKZ7-5562	Pacific Daylight Time
T9UAE6-5561	Pacific Daylight Time
TH2XG4-5562	Not in scope
TTGXLB-5561	(UTC-08:00) Pacific Time (US & Canada)
U8973A-5561	Pacific Daylight Time
UEQLM7-5561	Pacific StandardTime
UEWNPX-5561	Pacific Daylight Time
UGNM4W-5561	Pacific Standard Time
ULHG2X-5561	Pacific Daylight Time
UPTW39-5562	Pacific Standard Time
UUA6Q9-5561	Pacific Standard Time
UZQMYA-5562	Pacific Standard Time
V66XC6-5562	Pacific Standard Time
V82HUJ-5561	Pacific Standard Time
VXLE96-5561	Pacific Standard Time
VYTW7Z-5561	Pacific Standard Time
W447WA-5561	Pacific Standard Time
WB84Q8-5561	Winchestertonfieldville_Fire
WBPY99-5561	(UTC-08:00) Pacific Time (US & Canada)
WFVT36-5561	Pacific Daylight Time
WH6VY2-5561	Pacific Standard Time
WL2PNP-5561	Pacific Standard Time

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7 - Examination Questions	
WebCode Test	Response
WL4AK7-5562	Pacific Standard Time
WQGWCP-5562	Pacific Standard Time
X2AZR3-5561	Pacific Standard Time
X3NFAB-5561	Pacific Daylight Time
X62GKW-5561	Pacific Standard Time
X84MXA-5561	Pacific Standard Time
XDQM3P-5561	Pacific Standard Time
XDT8Y6-5562	Pacific Standard Time - This is in the registry with the key "Current offset (-8)". All forenisc tools just report it as "Pacific Time". Registry "TimeZoneInformation" key also shows Pacific Standard Time.
XLP32A-5562	Pacific Standard Time(US&Canada)
XQXJAX-5561	Pacific Standard Time
Y2PJCZ-5561	Pacific Daylight Time
Y8WZT2-5561	Pacific Standard Time
YZK9WX-5561	Pacific Daylight Time
Z4GR62-5562	Pacific Standard Time
Z4PAVK-5561	Pacific Standard Time
ZBUQRZ-5561	Pacific Daylight Time
ZEU2MZ-5562	Pacific Standard Time
ZF7RW4-5561	Pacific Standard Time
ZN4C6R-5561	Pacific Standard Time
ZQ4URL-5562	(UTC-08:00) Pacific Time (US & Canada)
ZU7QJ2-5561	Pacific Daylight Time
ZWABN2-5562	Pacific Daylight Time

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 7 - Examination Questions

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

Consensus Result:

Pacific Time and any variations representing similar information.

Manufacturer's Response Explanation:

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

Manufacturer's Response Illustration:

X-rays registry view showing time zone information

Name	Type	Value
(Default)	REG_SZ	(value not set)
Bias	REG_DWORD	0x000001E0 (480)
DaylightBias	REG_DWORD	0xFFFFF4 (4294967236)
DaylightName	REG_SZ	@tzres.dll,-211
DaylightStart	REG_BINARY	00 00 03 00 02 00 02 00 0
StandardBias	REG_DWORD	0x00000000 (0)
StandardName	REG_SZ	@tzres.dll,-212
StandardStart	REG_BINARY	00 00 0B 00 01 00 02 00 0
TimezoneKeyName	REG_SZ	Pacific Standard Time
DynamicDaylightTimeDisabled	REG_DWORD	0x00000000 (0)
ActiveTimeBias	REG_DWORD	0x000001A4 (420)

Autopsy registry view showing time zone information

Name	Type	Value
DaylightBias	REG_DWORD	0xfffffc4 (4294967236)
DaylightName	REG_SZ	@tzres.dll,-211
DaylightStart	REG_BIN	00 00 03 00 02 00 02 00 0
StandardBias	REG_DWORD	0x00000000 (0)
StandardName	REG_SZ	@tzres.dll,-212
StandardStart	REG_BIN	00 00 0B 00 01 00 02 00 0
TimezoneKeyName	REG_SZ	Pacific Standard Time
DynamicDaylightTimeDisabled	REG_DWORD	0x00000000 (0)

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 8 - Examination Questions

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

Manufacturer's Winchestertonfieldville_Fire

Response:

WebCode Test	Response
28NKRK-5561	Winchestertonfieldville_Fire
2BXEJB-5561	Winchestertonfieldville_Fire
2EUC34-5562	Pacific Standard Time
2UJN7X-5562	Winchestertonfieldville_Fire
2XN36N-5561	Winchestertonfieldville_Fire
36GUPN-5561	Winchestertonfieldville_Fire
3CH2GJ-5562	[Participant did not return results for this question.]
3DBUC3-5561	Winchestertonfieldville_Fire
3K9LKW-5561	Winchestertonfieldville_Fire
3LM236-5561	Winchestertonfieldville_Fire
483YXK-5561	Winchestertonfieldville_Fire
49DVEJ-5561	Winchestertonfieldville_Fire
4K6LX2-5561	Winchestertonfieldville_Fire
4L6CCW-5562	00:C1:40:50:03:49 (Winchestertonfieldville_Fire)
4P6N9W-5561	Winchestertonfieldville_Fire
4THJUL-5562	[Participant did not return results for this question.]
4XXRHK-5561	Winchestertonfieldville_Fire
4Z77PR-5561	Winchestertonfieldville_Fire
6KNFKX-5561	Winchestertonfieldville_Fire
6RLGDW-5561	Winchestertonfieldville_Fire

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 8 - Examination Questions	
WebCode Test	Response
78YYBQ-5561	Winchestertonfieldville_Fire
7M6APW-5561	Winchestertonfieldville_Fire
7WAG6W-5561	Winchestertonfieldville_fire
7WV3RK-5561	Winchestertonfieldville_Fire
8ED4K3-5562	Winchestertonfieldville_Fire
8LRYCP-5561	Winchestertonfieldville_Fire
8P8Q2X-5561	Winchestertonfieldville_Fire
8RFV4L-5561	Winchestertonfieldville_Fire
8W78WW-5562	Winchestertonfieldville_Fire
98N78Y-5561	Winchestertonfieldville_Fire
9J6THK-5561	Winchestertonfieldville_Fire
9QMRX6-5561	Winchestertonfieldville_Fire
9XFKVP-5562	Winchestertonfieldville_Fire
AN93XR-5561	Winchestertonfieldville_Fire
AXDBED-5562	Winchestertonfieldville_Fire
AXFVBT-5561	Winchestertonfieldville_Fire
B2ACZR-5562	Winchestertonfieldville_Fire
BA4FBG-5561	Winchestertonfieldville_Fire
BPGNBK-5562	SSID: Winchestertonfieldville_Fire, BSSID: 5E:36:C2:BD:C3:98
BVMG7F-5561	Winchestertonfieldville_Fire
BXTTTP-5561	Winchestertonfieldville_Fire
CCXUMK-5561	Winchestertonfieldville_Fire

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 8 - Examination Questions	
WebCode Test	Response
CPQ4TQ-5561	Winchestertonville_Fire
D3A9ER-5561	Winchestertonfieldville_Fire
D3MR2K-5561	Winchestertonfieldville_Fire
D7C7PK-5562	Provider name: Microsoft-Windows-SMBCClient
D8QG3R-5561	Winchestertonfieldville_Fire
DCKG7E-5561	Winchestertonfieldville_Fire
DKUYDR-5561	Winchestertonfieldville_Fire
DKVPRL-5562	Winchestertonfieldville_Fire
DPA82Q-5561	Winchestertonfieldville_Fire
DTN8XH-5562	Winchestertonfieldville_Fire / 00:C1:40:50:03:49
DXKMTK-5561	Winchestertonfieldville_Fire
EJD6CG-5561	Winchestertonfieldville_Fire
EJK3WT-5561	Winchestertonfieldville_Fire
EMTM9G-5561	Winchestertonfieldville_Fire
F3TPTL-5561	Winchestertonfieldville_Fire
F7NG2H-5561	Winchestertonfieldville_Fire
FG6CVN-5561	Winchestertonfieldville_Fire
FT8J39-5561	Winchestertonfieldville_Fire
G6U6KA-5561	Winchestertonfieldville_Fire
G9BD99-5561	Winchestertonfieldville_Fire
G9PQLK-5561	00:C1:40:50:03:49 (Winchestertonfieldville_Fire)
GALGEK-5562	Winchestertonfieldville_Fire

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 8 - Examination Questions	
WebCode Test	Response
GMPPAG-5561	Winchestertonfieldville_Fire
H3X34J-5561	Winchestertonfieldville_Fire
HAWCD-5562	Winchestertonfieldville_Fire
HFM3VL-5562	[Participant did not return results for this question.]
HGE2AK-5561	Winchestertonfieldville_Fire
HMQYPK-5561	Winchestertonfieldville_Fire
HTB6DE-5562	Winchestertonfieldville_Fire
HVJ3Y9-5561	Winchestertonfieldville_Fire
HYHLVF-5561	Winchestertonfieldville_Fire
J3FCTE-5561	Winchestertonfieldville_Fire
J49DM9-5561	Winchestertonfieldville_Fire
JFURCD-5561	Winchestertonfieldville_Fire
JPAH22-5562	Winchestertonfieldville_Fire
JXAZDE-5561	Winchestertonfieldville_Fire
JXHV GK-5561	Winchestertonfieldville_Fire
K3WXT8-5562	Winchestertonfieldville_Fire
KA94ED-5562	Winchestertonfieldville_Fire
KCQD3T-5561	Winchestertonfieldville_Fire
KMHPR4-5561	Winchestertonfieldville_Fire
LBJ6ZC-5562	5E 36 BD D8 AF B1
LMDLPD-5561	BSSID = 00:C1:40:50:03:49, SSID = Winchestertonfieldville_Fire
LRM3Y2-5562	Winchestertonfieldville_Fire

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 8 - Examination Questions	
WebCode Test	Response
LWKE3D-5561	Winchestertonfieldville_Fire
MCQ8YF-5561	Winchestertonfieldville_Fire
MD8AY2-5561	Winchestertonfieldville_Fire
MK6QJE-5561	Winchestertonfieldville_Fire
MR47EE-5562	Winchestertonfieldville_Fire (00:C1:40:50:03:49)
MV6A9L-5561	Winchestertonfieldville_Fire
N9Q2B2-5562	Winchestertonfieldville_Fire
NH83FA-5562	Winchestertonfieldville_Fire
NNQD78-5561	Winchestertonfieldville_Fire
NPUPBF-5562	Winchestertonfieldville_Fire
NQ7BB3-5561	Winchestertonfieldville_Fire
P3EHK8-5562	Winchestertonfieldville_Fire
P3ER7C-5561	Winchestertonfieldville_Fire
P6NMZG-5561	Winchestertonfieldville_Fire
PE6G4X-5561	Winchestertonfieldville_Fire
PYKJC4-5561	Winchestertonfieldville_Fire
Q4ZTN7-5562	Winchestertonfieldville_Fire
Q73JRN-5561	Winchestertonfieldville_Fire
RBARA4-5561	Winchestertonfieldville_Fire
RE7DZL-5561	Winchestertonfieldville_Fire
RUTBQ8-5561	Winchestertonfieldville_Fire
RY7A78-5561	Winchestertonfieldville_Fire

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 8 - Examination Questions	
WebCode Test	Response
RZKKZ7-5562	Winchestertonfieldville_Fire
T9UAE6-5561	Winchestertonfieldville_Fire
TH2XG4-5562	Not in scope
TTGXLB-5561	Winchestertonfieldville_Fire
U8973A-5561	{3B1007C4-2D37-4C88-9ADD-3DDA6AF5B4F8
UEQLM7-5561	Winchestertonfieldville_Fire
UEWNPX-5561	Winchestertonfieldville_Fire
UGNM4W-5561	Winchestertonfieldville_Fire
ULHG2X-5561	Winchestertonfieldville_Fire
UPTW39-5562	Winchestertonfieldville_Fire
UUA6Q9-5561	Winchestertonfieldville_Fire
UZQMYA-5562	Winchestertonfieldville_Fire
V66XC6-5562	Winchestertonfieldville_Fire
V82HUJ-5561	Winchestertonfieldville_Fire
VXLE96-5561	Winchestertonfieldville_Fire
VYTW7Z-5561	Winchestertonfieldville_Fire
W447WA-5561	Winchestertonfieldville_Fire
WB84Q8-5561	Pacific Standard Time
WBPY99-5561	Winchestertonfiledville_Fire
WFVT36-5561	Winchestertonfieldville_Fire
WH6VY2-5561	Winchestertonfieldville_Fire
WL2PNP-5561	Winchestertonfieldville_Fire

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 8 - Examination Questions	
WebCode Test	Response
WL4AK7-5562	Winchestertonfieldville_Fire
WQGWCP-5562	Winchestertonfieldville_Fire
X2AZR3-5561	Winchestertonfieldville-Fire
X3NFAB-5561	Winchestertonfieldville_Fire
X62GKW-5561	Winchestertonfieldville_Fire
X84MXA-5561	Winchestertonfieldville_Fire
XDQM3P-5561	Winchestertonfieldville_Fire
XDT8Y6-5562	Winchestertonfieldville_Fire
XLP32A-5562	Winchestertonfieldville_Fire
XQXJAX-5561	The registry indicates this computer was connected to at least 4 wireless access points 1.Winchesteronfieldville_Fire 2.Network 2 3.Network 4. EmergencyServices.Winchestertonfieldville.org SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles
Y2PJCZ-5561	Winchestertonfieldville_Fire
Y8WZT2-5561	Winchestertonfieldville_Fire
YZK9WX-5561	Winchestertonfieldville_Fire
Z4GR62-5562	Winchestertonfieldville_Fire
Z4PAVK-5561	Network, Network 2, EmergencyServices.Winchestertonfieldville.org, Unidentified network, Winchestertonfieldville_Fire
ZBUQRZ-5561	Winchestertonfieldville_Fire
ZEU2MZ-5562	Winchestertonfieldville_Fire
ZF7RW4-5561	Winchestertonfieldville_Fire
ZN4C6R-5561	Winchestertonfieldville_Fire
ZQ4URL-5562	Winchestertonfieldville_Fire
ZU7QJ2-5561	Winchestertonfieldville_Fire
ZWABN2-5562	Winchestertonfieldville_Fire

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 8 - Examination Questions

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

Consensus Result:

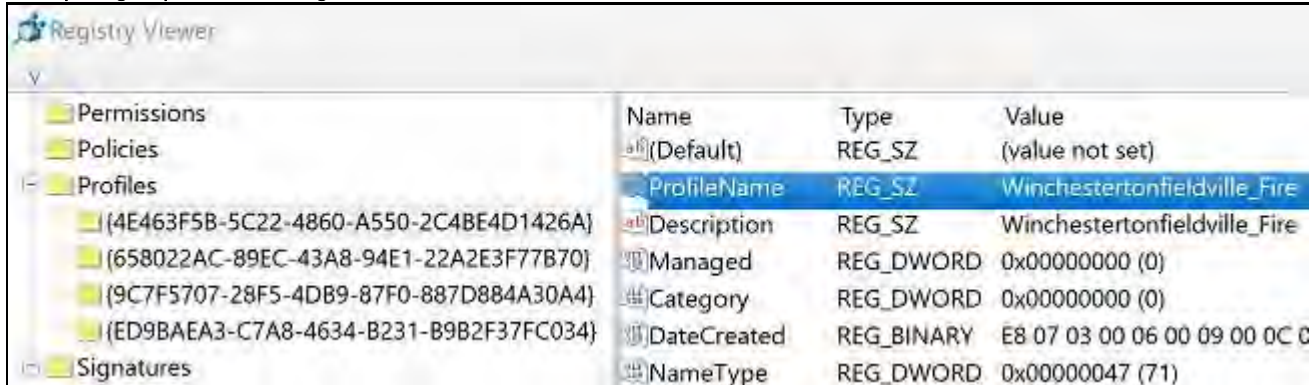
Winchestertonfieldville_Fire and slight variations if it was easily determined to be a typographical error.

Manufacturer's Response Explanation:

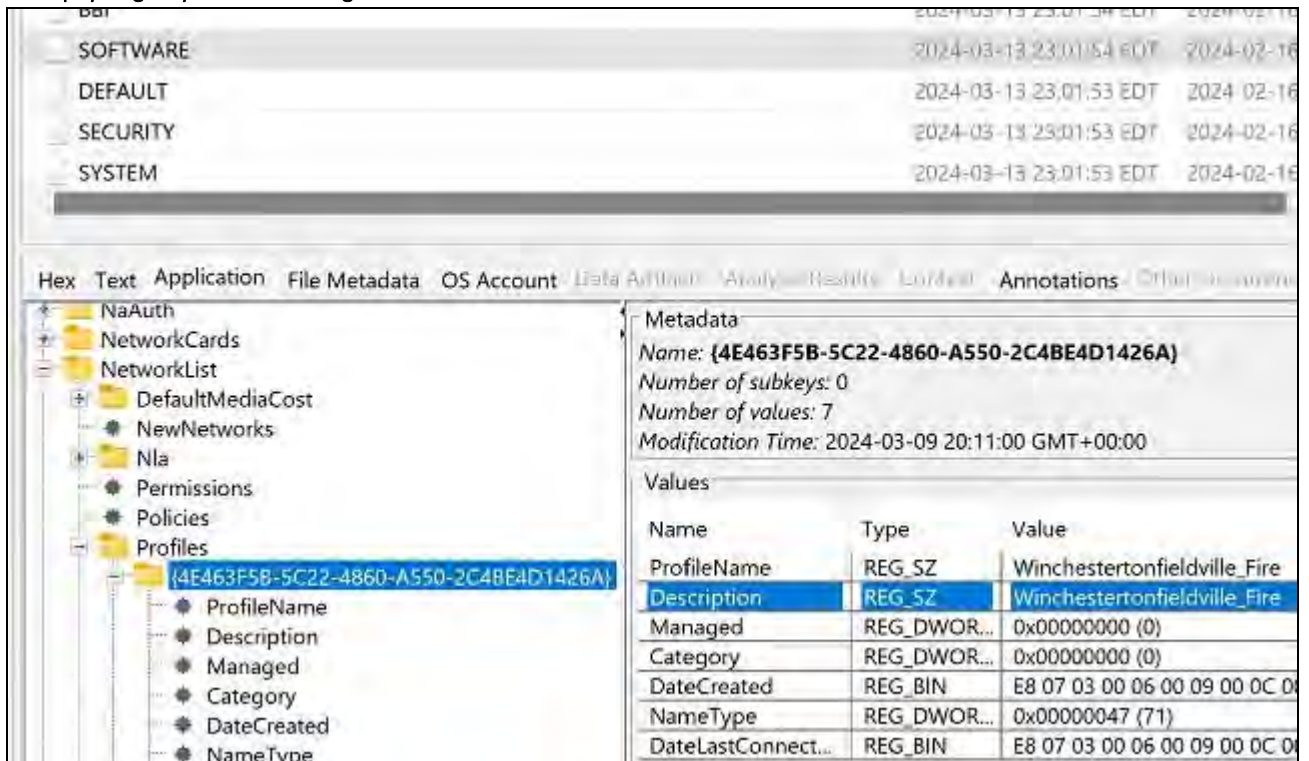
Windows network connection settings information is found in the SYSTEM registry hive at
 C:\Windows\System32\Config\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\.

Manufacturer's Response Illustration:

X-ways registry view showing network information



Autopsy registry view showing network information



Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 9 - Examination Questions

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

Manufacturer's smcnamara

Response:

WebCode Test	Response
28NKRK-5561	smcnamara
2BXEJB-5561	smcnamara
2EUC34-5562	smcnamara
2UJN7X-5562	smcnamara
2XN36N-5561	smcnamara
36GUPN-5561	smcnamara
3CH2GJ-5562	[Participant did not return results for this question.]
3DBUC3-5561	smcnamara
3K9LKW-5561	smcnamara
3LM236-5561	Smcnamara
483YXK-5561	smcnamara
49DVEJ-5561	smcnamara
4K6LX2-5561	smcnamara
4L6CCW-5562	smcnamara
4P6N9W-5561	smcnamara
4THJUL-5562	[Participant did not return results for this question.]
4XXRHK-5561	smcnamara
4Z77PR-5561	smcnamara
6KNFKX-5561	smcnamara
6RLGDW-5561	smcnamara
78YYBQ-5561	jmorrison

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 9 - Examination Questions	
WebCode Test	Response
7M6APW-5561	smcnamara
7WAG6W-5561	Smcnamara
7WV3RK-5561	smcnamara
8ED4K3-5562	smcnamara
8LRYCP-5561	Smcnamara
8P8Q2X-5561	smcnamara
8RFV4L-5561	smcnamara
8W78WW-5562	smcnamara
98N78Y-5561	smcnamara
9J6THK-5561	smcnamara
9QMRX6-5561	smcnamara
9XFKVP-5562	smcnamara
AN93XR-5561	smcnamara
AXDBED-5562	jmorrison
AXFVBT-5561	smcnamara
B2ACZR-5562	smcnamara
BA4FBG-5561	smcnamara
BPGNBK-5562	smcnamara
BVMG7F-5561	smcnamara
BXTTXP-5561	smcnamara
CCXUMK-5561	smcnamara
CPQ4TQ-5561	smcnamara

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 9 - Examination Questions	
WebCode Test	Response
D3A9ER-5561	smcnamara
D3MR2K-5561	smcnamara
D7C7PK-5562	S-1-5-21-2298470282-2867887670-580413564-1112 = Domain User = C:\Users\smcnamara. User = smcnamara
D8QG3R-5561	Unknown
DCKG7E-5561	smcnamara
DKUYDR-5561	Smcnamara
DKVPRL-5562	smcnamara
DPA82Q-5561	smcnamara (7538 (S-1-5-21-2298470282-2867887670-580413564-1112))
DTN8XH-5562	smcnamara
DXKMTK-5561	smcnamara
EJD6CG-5561	smcnamara
EJK3WT-5561	smcnamara
EMTM9G-5561	smcnamara
F3TPTL-5561	smcnamara
F7NG2H-5561	smcnamara
FG6CVN-5561	Smcnamara
FT8J39-5561	smcnamara
G6U6KA-5561	smcnamara
G9BD99-5561	smcnamara
G9PQLK-5561	Smcnamara
GALGEK-5562	smcnamara
GMPPAG-5561	smcnamara

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 9 - Examination Questions	
WebCode Test	Response
H3X34J-5561	smcnamara
HAWCD-5562	smcnamara
HFM3VL-5562	[Participant did not return results for this question.]
HGE2AK-5561	smcnamara
HMQYPK-5561	smcnamara
HTB6DE-5562	smcnamara
HVJ3Y9-5561	Smcnamara
HYHLVF-5561	smcnamara
J3FCTE-5561	smcnamara
J49DM9-5561	smcnamara
JFURCD-5561	smcnamara
JPAH22-5562	smcnamara
JXAZDE-5561	smcnamara
JXHV GK-5561	smcnamara
K3WXT8-5562	smcnamara
KA94ED-5562	smcnamara
KCQD3T-5561	smcnamara
KMHPR4-5561	smcnamara
LBJ6ZC-5562	smcnamara
LMDLPD-5561	smcnamara
LRM3Y2-5562	smcnamara
LWKE3D-5561	smcnamara

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 9 - Examination Questions	
WebCode Test	Response
MCQ8YF-5561	smcnamara
MD8AY2-5561	smcnamara
MK6QJE-5561	smcnamara
MR47EE-5562	smcnamara
MV6A9L-5561	smcnamara
N9Q2B2-5562	smcnamara
NH83FA-5562	smcnamara
NNQD78-5561	smcnamara
NPUPBF-5562	smcnamara (7538 (S-1-5-21-2298470282-2867887670-580413564-1112))
NQ7BB3-5561	1112 "smcnamara"
P3EHK8-5562	smcnamara
P3ER7C-5561	smcnamara
P6NMZG-5561	smcnamara
PE6G4X-5561	smcnamara
PYKJC4-5561	smcnamara
Q4ZTN7-5562	Smcnamara
Q73JRN-5561	smcnamara
RBARA4-5561	smcnamara
RE7DZL-5561	smcnamara
RUTBQ8-5561	smcnamara
RY7A78-5561	smcnamara
RZKKZ7-5562	smcnamara

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 9 - Examination Questions	
WebCode Test	Response
T9UAE6-5561	smcnamara
TH2XG4-5562	Not in scope
TTGXLB-5561	smcnamara
U8973A-5561	jmorrison
UEQLM7-5561	jmorrison
UEWNPX-5561	smcnamara
UGNM4W-5561	smcnamara
ULHG2X-5561	smcnamara
UPTW39-5562	smcnamara
UUA6Q9-5561	smcnamara
UZQMYA-5562	smcnamara
V66XC6-5562	smcnamara
V82HUJ-5561	smcnamara
VXLE96-5561	smcnamara
VYTW7Z-5561	smcnamara
W447WA-5561	smcnamera
WB84Q8-5561	smcnamara
WBPY99-5561	smcnamara
WFVT36-5561	smcnamara
WH6VY2-5561	smcnamara
WL2PNP-5561	smcnamara
WL4AK7-5562	smcnamara

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 9 - Examination Questions	
WebCode Test	Response
WQGWCP-5562	Smcnamara
X2AZR3-5561	smcnamara
X3NFAB-5561	smcnamara
X62GKW-5561	smcnamara
X84MXA-5561	smcnamara
XDQM3P-5561	smcnamara
XDT8Y6-5562	smcnamara - SS, User SID/RID - S-1-5-21-2298470282-2867887670-580413564-1112
XLP32A-5562	Administrators
XQXJAX-5561	smcnamara
Y2PJCZ-5561	smcnamara
Y8WZT2-5561	smcnamara
YZK9WX-5561	smcnamara
Z4GR62-5562	smcnamara
Z4PAVK-5561	smcnamara
ZBUQRZ-5561	smcnamara
ZEU2MZ-5562	smcnamara
ZF7RW4-5561	smcnamara
ZN4C6R-5561	smcnamara
ZQ4URL-5562	smcnamara
ZU7QJ2-5561	smcnamara
ZWABN2-5562	smcnamara

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 9 - Examination Questions

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

Consensus Result:

smcnamara and slight variations if it was easily determined to be a typographical error.

Manufacturer's Response Explanation:

File ownership is a feature of the filesystem. NTFS filesystem metadata identifies the owner of the file by security identifier (SID) as S-1-5-21-2298470282-2867887670-580413564-1112. Names and local profile information for domain users is stored in the Windows SOFTWARE registry at C:\Windows\System32\Config\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList.

Manufacturer's Response Illustration:

X-ways New Text Document.txt file detail information

Full path	\New folder\New Text Document.txt
Parent name	New folder
Size	8 B
Created	Friday, March 8, 2024 22:04:53.8 -5
Modified	Friday, March 8, 2024 22:07:30.4 -5
Record changed	Friday, March 8, 2024 22:10:12.6 -5
Accessed	Friday, March 8, 2024 22:09:55.7 -5
Attr.	HRAI
1st sector	61,307,220
FS offset	74EF2A800
ID	218098
Int. ID	263056
Int. parent	264618
Unique ID	0-263056
Unique ID as GUID	00040390-0000-4000-BEB2511C1B3E9FE6
Owner	S-1-5-21-2298470282-2867887670-580413564-1112

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 9 - Examination Questions

Autopsy New Text Document.txt file detail information

Yimg_Fire Department Workstation.e01/New folder

Table Thumbnail Summary	S	C	O	MD	Modified Time
[parent folder]					2024-03-13 22:46:02 EDT
New Text Document.txt					2024-03-08 22:07:30 EST
[current folder]					2024-03-08 22:04:53 EST

Hex Text Application File Metadata OS Account Data Artifacts Ana

Basic Properties

Login:

Full Name:

Address: S-1-5-21-2298470282-2867887670-580413564-1112

X-Ways view of SOFTWARE:Microsoft\Windows NT\CurrentVersion\ProfileList

Name	Type	Value
(Default)	REG_SZ	(value not set)
ProfileImagePath	REG_EXPAN...	C:\User\asmcnamara
Flags	REG_DWORD	0x00000000 (0)
FullProfile	REG_DWORD	0x00000001 (1)
State	REG_DWORD	0x00000000 (0)
Sid	REG_BINARY	01 05 00 00 00 00 00
Guid	REG_SZ	{ac6dbb9b-4f6e-42a3
LocalProfileLoadTimeLow	REG_DWORD	0xC2E4AF47 (3269766
LocalProfileLoadTimeHigh	REG_DWORD	0x01DA71CD (310931
ProfileAttemptedProfileDownloa...	REG_DWORD	0x00000000 (0)
ProfileAttemptedProfileDownloa...	REG_DWORD	0x00000000 (0)
ProfileLoadTimeLow	REG_DWORD	0x00000000 (0)

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 10 - Examination Questions

Question 10: Provide the filesystem attributes for C:\New folder\New Text Document.txt.

Manufacturer's Hidden, Read-Only, Archive

Response:

WebCode Test	Response
28NKRK-5561	Hidden: True, System: False, Read-only: True, Archive: True
2BXEJB-5561	Archive, Hidden, Readonly
2EUC34-5562	Archive, Hidden, Read Only
2UJN7X-5562	HRAI (Hidden, Read-Only, Archived-Indexed)
2XN36N-5561	Hidden, Read Only, Archive
36GUPN-5561	ReadOnly, Hidden, Archive
3CH2GJ-5562	[Participant did not return results for this question.]
3DBUC3-5561	Hidden: True, System: False, Read Only: True, Archive: True
3K9LKW-5561	ReadOnly, Hidden, Archive
3LM236-5561	Readonly, Hidden, Archive
483YXK-5561	Read only, Hidden, Archive
49DVEJ-5561	ReadOnly, Hidden, Archive
4K6LX2-5561	Hidden, Read-Only, Archive
4L6CCW-5562	IHRA
4P6N9W-5561	Hidden, Read Only, Archive
4THJUL-5562	[Participant did not return results for this question.]
4XXRHK-5561	File, Hidden, Read Only, Archive
4Z77PR-5561	ReadOnly, Hidden, Archive
6KNFKX-5561	read only, hidden, archive
6RLGDW-5561	ReadOnly, Hidden, Archive
78YYBQ-5561	dinictis

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 10 - Examination Questions	
WebCode Test	Response
7M6APW-5561	ReadOnly, Hidden, Archive
7WAG6W-5561	HRAI: Hidden, Read-Only, Archive, Not Content Indexed
7WV3RK-5561	ReadOnly, Hidden, Archive
8ED4K3-5562	The file attributes are ReadOnly, Hidden, and Archive, but if you're asking about all other attributes, here they are: File name: New Text Document.txt, Artifact type: Text Documents, Created Date/Time: 2024-03-09 AM 3:04:53, Last Accessed Date/Time: 2024-03-09 AM 3:09:55, Last Modified Date/Time: 2024-03-09 AM 3:07:30, MFT Modified Date/Time: 2024-03-09 AM 3:10:12, Size (bytes): 8, Security ID: 7538(S-1-5-21-2298470282-2867887670-580413564-1112), Additionally, if you are asking about the filesystem where the file exists, it is NTFS.
8LRYCP-5561	Read Only, Hidden, Archive
8P8Q2X-5561	Hidden, Read Only, Archive
8RFV4L-5561	archive, notcontentindexed
8W78WW-5562	ReadOnly, Hidden, Archive
98N78Y-5561	FILE_ATTRIBUTE_ARCHIVE
9J6THK-5561	ReadOnly, Hidden, Archive
9QMRX6-5561	ReadOnly, Hidden, Archive
9XFKVP-5562	Modified 09/03/2024 03:07:30:000, Accessed 09/03/2024 03:09:55:000, Created 09/03/2024 03:04:353:000, Item iD 3487, MD5/Sha1 Hahses
AN93XR-5561	ReadOnly, Hidden, Archive
AXDBED-5562	Archive
AXFVBT-5561	Text (attribute)
B2ACZR-5562	Readonly, Hidden, Archive
BA4FBG-5561	Read Only, Hidden, Archive.
BPGNBK-5562	ReadOnly, Hidden, Ready to archive
BVMG7F-5561	Archive, NotContentIndexed
BXTTXP-5561	ReadOnly, Hidden, Archive
CCXUMK-5561	archive, hidden, and read-only

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 10 - Examination Questions	
WebCode Test	Response
CPQ4TQ-5561	Hidden, Read Only, Archive
D3A9ER-5561	Date Accessed 3/9/2024 3:09:55 AM, File Size 8, Physical Size 8, Hidden - True, System - False, Read Only - True, Archive - True,
D3MR2K-5561	ReadOnly, Hidden, Archive
D7C7PK-5562	ReadOnly, Hidden, Archive, Times: C - 09/03/2024 03:04:53:814, A - 09/03/2024 03:09:55:705, M - 09/03/2024 03:07:30:455, MFT Mod-09/03/2024 03:10:12:650, MFT Record 218098, ParentMFT 219662, Sec ID 7538, 8 bytes md5 hash givenrs
D8QG3R-5561	Path: Fire%20Department%20Workstation-001.e01\Root\New folder\. Modified: 09/03/2024 03:07:30. Created: 09/03/2024 03:04:53. Accessed. 09/03/2024 03:09:55. Is Deleted: No. Sector: 61307220. Logical Size: 8. Physical Size: 8
DCKG7E-5561	Not content indexed, hidden, read-only, archived
DKUYDR-5561	ReadOnly, Hidden, Archive
DKVPRL-5562	Hidden, Read only, Archive, non-System
DPA82Q-5561	ReadOnly, Hidden, Archive
DTN8XH-5562	Read Only, Hidden, Archive
DXKMTK-5561	ReadOnly, Hidden, Archive
EJD6CG-5561	ReadOnly, Hidden, Archive
EJK3WT-5561	Read-only; Hidden; Archive
EMTM9G-5561	Hidden
F3TPTL-5561	ReadOnly, Hidden, Archive
F7NG2H-5561	Archive, NotContentIndexed
FG6CVN-5561	Hidden, Read Only and Archive
FT8J39-5561	File, Hidden, Read Only, Archive
G6U6KA-5561	ReadOnly, Hidden, Archive
G9BD99-5561	ReadOnly, Hidden, Archive
G9PQLK-5561	Read Only, Hidden, Archive

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 10 - Examination Questions	
WebCode Test	Response
GALGEK-5562	Read Only, Hidden, Archive
GMPPAG-5561	ReadOnly, Hidden, Archive
H3X34J-5561	ReadOnly, Hidden, Archive
HAVCD-5562	ReadOnly, Hidden, Archive
HFM3VL-5562	[Participant did not return results for this question.]
HGE2AK-5561	HRAI (Hidden, read only, to be archived, not content indexed), Filename: New Text Document.txt, Short filename: NEWTEX~1.TXT, Path: C:\New Folder\New Text Document.txt, Size: 8 B, Resident, MFT Record Number: 218098, Created Date: 2024-03-09 03:04:53 UTC, Accessed Date: 2024-03-09 03:09:55 UTC, Modified Date: 2024-03-09 03:07:30 UTC,
HMQYPK-5561	ReadOnly, Hidden, Archive
HTB6DE-5562	HRAI (ReadOnly, Hidden, Archive)
HVJ3Y9-5561	ReadOnly, Hidden, Archive
HYHLVF-5561	Read only, Hidden, Archive
J3FCTE-5561	Last Modified date/Time: 09/03/2024 3:07:30.000 AM, Last Accessed Date/Time: 09/03/2024 3:09:55.000 AM, Created date/Time: 09/03/2024 3:04:53.000 AM MD5: cfe35ec8e0456aa2330948f4c0563953
J49DM9-5561	Archive, Hidden, Read-Only.
JFURCD-5561	ReadOnly, Hidden, Archive
JPAH22-5562	File, Hidden, Read Only
JXAZDE-5561	Created: 2024-03-09 06:04:53, File Modified: 2024-03-09 06:07:30, MFT modified: 2024-03-09 06:10:12,
JXHV GK-5561	ReadOnly, Hidden, Archive
K3WXT8-5562	ReadOnly, Hidden, Archive
KA94ED-5562	ReadOnly, Hidden, Archive
KCQD3T-5561	ReadOnly, Hidden, Archive
KMHPR4-5561	Read Only, Hidden, Archive
LBJ6ZC-5562	ReadOnly, Hidden, Archive
LMDLPD-5561	File name: New Text Document.txt size: 8 Byte created date/time: 9/3/2024 3:04:53 AM Accessed date/time: 9/3/2024 3:09:55 AM Modified date/time: 9/3/2024 3:07:30 AM Filesystem: NTFS

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 10 - Examination Questions	
WebCode Test	Response
LRM3Y2-5562	Hidden: True, System: False, Read-only: True, Archive: True
LWKE3D-5561	ReadOnly, Hidden, Archive
MCQ8YF-5561	Hidden, Read Only, Archive
MD8AY2-5561	File, Hidden, Read Only, Archive
MK6QJE-5561	Read Only, Hidden, Archive
MR47EE-5562	ReadOnly, Hidden, Archive
MV6A9L-5561	FILE_ARCHIVE
N9Q2B2-5562	Read only, Hidden, Archive
NH83FA-5562	Name: New Text Document.txt, Extension .txt, Type Plain Text Document, Size 8B, Created Date 09/03/2024 03:04:53, 1st Sector 61, 307, 220, FS offset 74EF2A800, UID as GUID 00040390-0005-4000-BCCEBA485D178D59, Owner S-1-5-21-2298470282-2867887670-580413564-1112
NNQD78-5561	hidden, readonly, archive
NPUPBF-5562	ReadOnly, Hidden, Archive
NQ7BB3-5561	Hidden, Read Only, Archive
P3EHK8-5562	ReadOnly, Hidden, Archive
P3ER7C-5561	Hidden: True; Read only: True; Archive: True; System: False; Date Created: 3/8/2024 03:04:53 UTC; Date Accessed: 3/8/2024 03:09:55 UTC; Date Modified: 3/8/2024 03:07:30 UTC; Physical and Logical size: 8 bytes; File Type: 7 bit text
P6NMZG-5561	ReadOnly, Hidden, Archive
PE6G4X-5561	ReadOnly, Hidden, Archive
PYKJC4-5561	ReadOnly, Hidden, Archive
Q4ZTN7-5562	Read Only, Hidden, Archive
Q73JRN-5561	Hidden, File, Read Only, Archive
RBARA4-5561	Hidden, Read Only, Archive
RE7DZL-5561	ReadOnly, Hidden, Archive

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 10 - Examination Questions	
WebCode Test	Response
RUTBQ8-5561	IT's a Hidden, Archive and a read only file
RY7A78-5561	Hidden (H), Read-Only (R), Archive (A)
RZKKZ7-5562	ReadOnly, Hidden, Archive
T9UAE6-5561	Hidden, Read Only, Archive, Not content indexed
TH2XG4-5562	Not in scope
TTGXLB-5561	File, Hidden, Read Only, Archive
U8973A-5561	File, Hidden, Read only, Archive
UEQLM7-5561	ReadOnly, Hidden, Archive
UEWNPX-5561	ReadOnly, Hidden, Archive
UGNM4W-5561	H – Hidden, R – Read-only, A – to be archived
ULHG2X-5561	Read Only, Hidden, Archive
UPTW39-5562	Archive, Hidden, Read Only
UUA6Q9-5561	File, ReadOnly, Hidden, Archive
UZQMYA-5562	File, Hidden, Read-only, Archive
V66XC6-5562	ReadOnly, Hidden, Archive
V82HUJ-5561	File, Hidden, Read Only, Archive
VXLE96-5561	Archive, , Hidden, Read only
VYTW7Z-5561	[Participant did not return results for this question.]
W447WA-5561	ReadOnly, Hidden, Archive
WB84Q8-5561	Archive, Hidden, Read Only
WBPY99-5561	ReadOnly, Hidden, Archive
WFVT36-5561	ReadOnly, Hidden, Archive

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 10 - Examination Questions	
WebCode Test	Response
WH6VY2-5561	Archive, ReadOnly, Hidden
WL2PNP-5561	ReadOnly, Hidden, Archive
WL4AK7-5562	ReadOnly, Hidden, Archive
WQGWCP-5562	File, Hidden, Read Only, Archive
X2AZR3-5561	Read Only, Hidden, Archive
X3NFAB-5561	ReadOnly, Hidden, Archive
X62GKW-5561	Hidden, Read-only, Archive
X84MXA-5561	Type: File System MIME Type: text/plain Size: 8 bytes File Name Allocation: Allocated Metadata Allocation: Allocated Timestamps: - Created: 2024-03-08 19:04:53 PST - Modified: 2024-03-08 19:07:30 PST - Accessed: 2024-03-08 19:09:55 PST - Changed: 2024-03-08 19:10:12 PST Hashes: - MD5: cfe35ec8e0456aa2330948f4c0563953 - SHA-256: 914bc708cf234018084c0c950350acd0205bbeb1255d89c97e34b6600b8c0984 MFT Entry Header Values: - Entry: 218098 - Sequence: 5 - \$LogFile Sequence Number: 1159404195 - Allocated File: Yes - Links: 2 \$STANDARD_INFORMATION Attribute Values: - Flags: Read Only, Hidden, Archive - Owner ID: 0 - Security ID: 7538 (S-1-5-21-2298470282-2867887670-580413564-1112) - Last User Journal Update Sequence Number: 217797944 - Created: 2024-03-09 04:04:53.814641000 (Central European Standard Time) - File Modified: 2024-03-09 04:07:30.455493800 (Central European Standard Time) - MFT Modified: 2024-03-09 04:10:12.650496200 (Central European Standard Time) - Accessed: 2024-03-09 04:09:55.705890300 (Central European Standard Time) \$FILE_NAME Attribute Values: - Flags: Archive - Name: NEWTEX~1.TXT - Parent MFT Entry: 219662 Sequence: 4 - Allocated Size: 0 - Actual Size: 0 - Created: 2024-03-09 04:04:53.814641000 (Central European Standard Time) - File Modified: 2024-03-09 04:04:53.814641000 (Central European Standard Time) - MFT Modified: 2024-03-09 04:04:53.814641000 (Central European Standard Time) - Accessed: 2024-03-09 04:04:53.814641000 (Central European Standard Time) \$OBJECT_ID Attribute Values: - Object Id: e5dfcef3-ddc0-11ee-aa39-08002794be6a Attributes: - Type: \$STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72 - Type: \$FILE_NAME (48-3) Name: N/A Resident size: 90 - Type: \$FILE_NAME (48-2) Name: N/A Resident size: 108 - Type: \$OBJECT_ID (64-4) Name: N/A Resident size: 16 - Type: \$DATA (128-1) Name: N/A Resident size: 8; Encrypted: False, Compressed: False, Actual File: True; Hidden: True; Read Only: True; Archive: True
XDQM3P-5561	ReadOnly, Hidden, Archive
XDT8Y6-5562	File, Hidden, Read Only, Archive
XLP32A-5562	ReadOnly, Hidden, Archive / Path: "C:\New folder\New Text Document.txt", size: 8, MACTIME: 2024.3.9.03:07:30(M) 03:09:55(A) 03:04:53(C)
XQXJAX-5561	Read Only, Hidden, Archive
Y2PJCZ-5561	ReadOnly, Hidden, Archive, not compressed, actual file (not clear which attributes are sought in question)
Y8WZT2-5561	Hidden, Read Only, Archive
YZK9WX-5561	ReadOnly, Hidden, Archive

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 10 - Examination Questions	
WebCode Test	Response
Z4GR62-5562	Hidden: True, System: False, Read Only: True, Archive: True, MTF #: 219662, MTF Date Change: 3/9/2024 3:04:53 AM, Resident: True, Offline: False, Sparse: False, Temp: False, Owner SID: S-1-5-21-2298470282-2867887670-580413564-1112 **SEE Additional Comments**
Z4PAVK-5561	Hidden, Read Only, Archive
ZBUQRZ-5561	Read Only, Hidden, Archive
ZEU2MZ-5562	Read Only, Hidden, Archive
ZF7RW4-5561	Archive, Hidden, Read Only
ZN4C6R-5561	ReadOnly, Hidden, Archive
ZQ4URL-5562	ReadOnly, Hidden, Archive
ZU7QJ2-5561	read only, hidden, archive
ZWABN2-5562	ReadOnly, Hidden, Archive

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 10 - Examination Questions

Question 10: Provide the filesystem attributes for C:\New folder\New Text Document.txt.

Consensus Result:

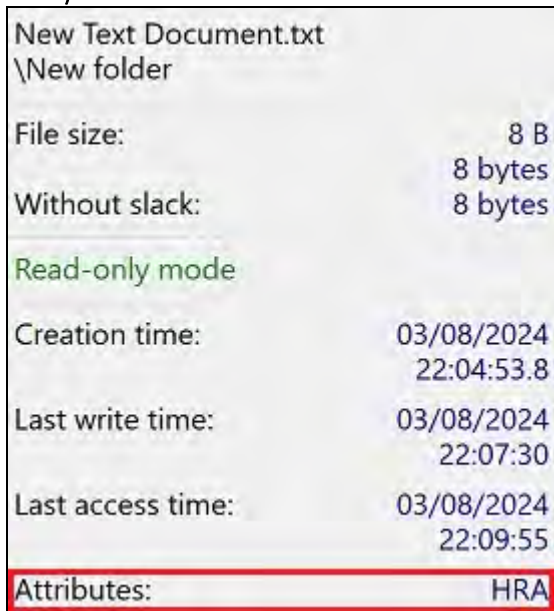
Hidden, Read-Only, Archive

Manufacturer's Response Explanation:

NTFS filesystem metadata includes flags for the attributes above.

Manufacturer's Response Illustration:

X-ways New Text Document.txt file detail information



New Text Document.txt
 \New folder

File size: 8 B
 8 bytes

Without slack: 8 bytes

Read-only mode

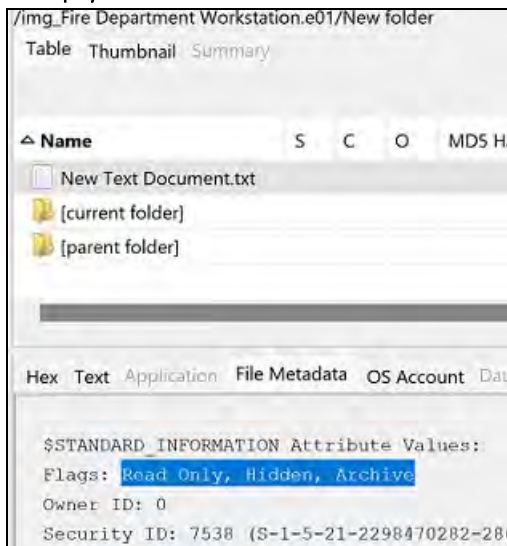
Creation time: 03/08/2024
 22:04:53.8

Last write time: 03/08/2024
 22:07:30

Last access time: 03/08/2024
 22:09:55

Attributes: HRA

Autopsy New Text Document.txt file detail information



/img_Fire Department Workstation.e01/New folder

Table Thumbnail Summary

▲ Name S C O MDS H

New Text Document.txt

[current folder]

[parent folder]

Hex Text Application File Metadata OS Account Data

\$STANDARD_INFORMATION Attribute Values:
 Flags: Read Only, Hidden, Archive
 Owner ID: 0
 Security ID: 7538 (S-1-5-21-2298470282-28)

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 11 - Examination Questions

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

Manufacturer's tgavin

Response:

WebCode Test	Response
28NKRK- 5561	tgavin
2BXEJB- 5561	tgavin
2EUC34- 5562	tgavin
2UJN7X- 5562	tgavin
2XN36N- 5561	tgavin
36GUPN- 5561	tgavin
3CH2GJ- 5562	[Participant did not return results for this question.]
3DBUC3- 5561	tgavin
3K9LKW- 5561	tgavin
3LM236- 5561	Tgavin
483YXK- 5561	tgavin
49DVEJ- 5561	tgavin
4K6LX2- 5561	tgavin
4L6CCW- 5562	tgavin
4P6N9W- 5561	tgavin
4THJUL- 5562	[Participant did not return results for this question.]
4XXRHK- 5561	tgavin
4Z77PR- 5561	tgavin
6KNFKX- 5561	tgavin
6RLGDW- 5561	tgavin
78YYBQ- 5561	tgavin

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 11 - Examination Questions	
WebCode Test	Response
7M6APW-5561	Tgavin
7WAG6W-5561	smcnamara
7WV3RK-5561	tgavin
8ED4K3-5562	tgavin
8LRYCP-5561	tgavin
8P8Q2X-5561	Tgavin
8RFV4L-5561	tgavin
8W78WW-5562	tgavin
98N78Y-5561	tgavin
9J6THK-5561	tgavin
9QMRX6-5561	tgavin
9XFKVP-5562	tgavin user id: S-1-5-20
AN93XR-5561	tgavin
AXDBED-5562	tgavin
AXFVBT-5561	tgavin
B2ACZR-5562	tgavin
BA4FBG-5561	tgavin
BPGNBK-5562	tgavin
BVMG7F-5561	COMPANY-13\$
BXTTXP-5561	tgavin
CCXUMK-5561	tgavin
CPQ4TQ-5561	tgavin

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 11 - Examination Questions	
WebCode Test	Response
D3A9ER-5561	tgavin
D3MR2K-5561	tgavin
D7C7PK-5562	tgavin TargetUserSid">S-1-5-21-2298470282-2867887670-580413564-1108</Data><Data Name="TargetUserName">tgavin</
D8QG3R-5561	tgavin
DCKG7E-5561	tgavin
DKUYDR-5561	Tgavin
DKVPRL-5562	tgavin
DPA82Q-5561	EMERGENCYSERVIC\tgavin
DTN8XH-5562	tgavin
DXKMTK-5561	tgavin
EJD6CG-5561	tgavin
EJK3WT-5561	tgavin
EMTM9G-5561	tgavin
F3TPTL-5561	tgavin
F7NG2H-5561	tgavin
FG6CVN-5561	tgavin
FT8J39-5561	tgavin
G6U6KA-5561	tgavin
G9BD99-5561	tgavin
G9PQLK-5561	tgavin
GALGEK-5562	tgavin
GMPPAG-5561	tgavin

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 11 - Examination Questions	
WebCode Test	Response
H3X34J-5561	tgavin
HAVVCD-5562	tgavin
HFM3VL-5562	[Participant did not return results for this question.]
HGE2AK-5561	tgavin
HMQYPK-5561	tgavin
HTB6DE-5562	tgavin
HVJ3Y9-5561	tgavin
HYHLVF-5561	tgavin
J3FCTE-5561	tgavin
J49DM9-5561	tgavin
JFURCD-5561	tgavin
JPAH22-5562	tgavin
JXAZDE-5561	jbeatty
JXHV GK-5561	tgavin
K3WXT8-5562	tgavin
KA94ED-5562	tgavin
KCQD3T-5561	tgavin
KMHPR4-5561	tgavin
LBJ6ZC-5562	tgavin
LMDLPD-5561	tgavin
LRM3Y2-5562	tgavin
LWKE3D-5561	tgavin

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 11 - Examination Questions	
WebCode Test	Response
MCQ8YF-5561	tgavin
MD8AY2-5561	tgavin
MK6QJE-5561	tgavin
MR47EE-5562	tgavin
MV6A9L-5561	tgavin
N9Q2B2-5562	tgavin
NH83FA-5562	tgavin
NNQD78-5561	tgavin
NPUPBF-5562	EMERGENCYSERVIC\tgavin
NQ7BB3-5561	"tgavin"
P3EHK8-5562	tgavin
P3ER7C-5561	tgavin
P6NMZG-5561	tgavin
PE6G4X-5561	tgavin
PYKJC4-5561	tgavin
Q4ZTN7-5562	tgavin
Q73JRN-5561	tgavin
RBARA4-5561	tgavin
RE7DZL-5561	tgavin
RUTBQ8-5561	Tgavin
RY7A78-5561	tgavin
RZKKZ7-5562	tgavin

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 11 - Examination Questions	
WebCode Test	Response
T9UAE6-5561	tgavin
TH2XG4-5562	Not in scope
TTGXLB-5561	tgavin
U8973A-5561	tgavin
UEQLM7-5561	tgavin
UEWNPX-5561	tgavin
UGNM4W-5561	tgavin
ULHG2X-5561	tgavin
UPTW39-5562	tgavin
UUA6Q9-5561	tgavin
UZQMYA-5562	tgavin
V66XC6-5562	tgavin
V82HUJ-5561	tgavin
VXLE96-5561	tgavin
VYTW7Z-5561	tgavin
W447WA-5561	tgavin
WB84Q8-5561	tgavin
WBPY99-5561	tgavin
WFVT36-5561	tgavin
WH6VY2-5561	tgavin
WL2PNP-5561	tgavin
WL4AK7-5562	tgavin

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 11 - Examination Questions	
WebCode Test	Response
WQGWCP-5562	tgavin
X2AZR3-5561	tgavin
X3NFAB-5561	tgavin
X62GKW-5561	tgavin
X84MXA-5561	tgavin
XDQM3P-5561	tgavin
XDT8Y6-5562	tgavin
XLP32A-5562	tgavin
XQXJAX-5561	tgavin
Y2PJCZ-5561	tgavin
Y8WZT2-5561	tgavin
YZK9WX-5561	tgavin
Z4GR62-5562	tgavin
Z4PAVK-5561	tgavin
ZBUQRZ-5561	tgavin
ZEU2MZ-5562	tgavin
ZF7RW4-5561	tgavin
ZN4C6R-5561	tgavin
ZQ4URL-5562	tgavin
ZU7QJ2-5561	tgavin
ZWABN2-5562	tgavin

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 11 - Examination Questions

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

Consensus Result:

tgavin

Manufacturer's Response Explanation:

Remote logon information can be found in the Windows Event logs, specifically, Microsoft-Windows-TerminalServices-RemoteConnectionManager Operational.evtx.

Manufacturer's Response Illustration:

Windows Event Viewer - Microsoft-Windows-TerminalServices-RemoteConnectionManager Operational.evtx

The screenshot displays the Windows Event Viewer interface for the log 'Microsoft-Windows-TerminalServices-RemoteConnectionManager\Operational'. It shows a list of events with the following details:

Level	Date and Time	Source	Event ID	Task Category
Information	3/13/2024 12:31:24 AM	TerminalServices-RemoteConnectionM...	20523	None
Information	3/13/2024 12:31:24 AM	TerminalServices-RemoteConnectionM...	263	None
Information	3/9/2024 4:03:54 PM	TerminalServices-RemoteConnectionM...	1149	None

The details for Event 1149 are expanded, showing the following information:

- Event Name: Event 1149, TerminalServices-RemoteConnectionManager
- General tab selected.
- Remote Desktop Services: User authentication succeeded:
- User: **tgavin** (highlighted with a red box)
- Domain: EMERGENCYSERVICE
- Source Network Address: 10.0.2.15

Additional event details are listed below:

- Log Name: Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational
- Source: TerminalServices-RemoteCo
- Logged: 3/9/2024 4:03:54 PM
- Event ID: 1149
- Task Category: None
- Level: Information
- Keywords:
- User: NETWORK SERVICE
- Computer: Company-13.EmergencyServices.Winchestertonfieldville.org
- OpCode: Info
- More Information: [Event Log Online Help](#)

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12 - Examination Questions

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

Manufacturer's 10.0.2.15

Response:

WebCode Test	Response
28NKRK-5561	10.0.2.15
2BXEJB-5561	10.0.2.15
2EUC34-5562	10.0.2.15
2UJN7X-5562	10.0.2.15
2XN36N-5561	10.0.2.15
36GUPN-5561	10.0.2.15
3CH2GJ-5562	[Participant did not return results for this question.]
3DBUC3-5561	10.0.2.15
3K9LKW-5561	10.0.2.15
3LM236-5561	10.0.2.15
483YXK-5561	10.0.2.15
49DVEJ-5561	10.0.2.15
4K6LX2-5561	10.0.2.15
4L6CCW-5562	10.0.2.15
4P6N9W-5561	10.0.2.15
4THJUL-5562	[Participant did not return results for this question.]
4XXRHK-5561	10.0.2.15
4Z77PR-5561	10.0.2.15
6KNFKX-5561	10.0.2.15
6RLGDW-5561	10.0.2.15

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12 - Examination Questions	
WebCode Test	Response
78YYBQ-5561	10.0.2.15
7M6APW-5561	10.0.2.15
7WAG6W-5561	10.0.2.15
7WV3RK-5561	10.0.2.15
8ED4K3-5562	10.0.2.15
8LRYCP-5561	10.0.2.15
8P8Q2X-5561	10.0.2.15
8RFV4L-5561	10.0.2.15
8W78WW-5562	10.0.2.15
98N78Y-5561	10.0.2.15
9J6THK-5561	10.0.2.15
9QMRX6-5561	10.0.2.15
9XFKVP-5562	10.0.2.15
AN93XR-5561	10.0.2.15
AXDBED-5562	10.0.2.15
AXFVBT-5561	10.0.2.15
B2ACZR-5562	10.0.2.15
BA4FBG-5561	10.0.2.15
BPGNBK-5562	10.0.2.15
BVMG7F-5561	10.0.2.15
BXTTTP-5561	10.0.2.15
CCXUMK-5561	10.0.2.15

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12 - Examination Questions	
WebCode Test	Response
CPQ4TQ-5561	10.0.2.15
D3A9ER-5561	10.0.2.15
D3MR2K-5561	10.0.2.15
D7C7PK-5562	Origin IP address: 10.0.2.15
D8QG3R-5561	10.0.2.15
DCKG7E-5561	10.0.2.15
DKUYDR-5561	10.0.2.15
DKVPRL-5562	10.0.2.15
DPA82Q-5561	10.0.2.15
DTN8XH-5562	10.0.2.15
DXKMTK-5561	10.0.2.15
EJD6CG-5561	10.0.2.15
EJK3WT-5561	10.0.2.15
EMTM9G-5561	10.0.2.15
F3TPTL-5561	10.0.2.15
F7NG2H-5561	10.0.2.15
FG6CVN-5561	10.0.2.15
FT8J39-5561	10.0.2.15
G6U6KA-5561	10.0.2.15
G9BD99-5561	10.0.2.15
G9PQLK-5561	10.0.2.15
GALGEK-5562	10.0.2.15

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12 - Examination Questions	
WebCode Test	Response
GMPPAG-5561	10.0.2.15
H3X34J-5561	10.0.2.15
HAWCD-5562	10.0.2.15
HFM3VL-5562	[Participant did not return results for this question.]
HGE2AK-5561	10.0.2.15
HMQYPK-5561	10.0.2.15
HTB6DE-5562	10.0.2.15
HVJ3Y9-5561	10.0.2.15
HYHLVF-5561	10.0.2.15
J3FCTE-5561	10.0.2.15
J49DM9-5561	10.0.2.15
JFURCD-5561	10.0.2.15
JPAH22-5562	10.0.2.15
JXAZDE-5561	00:C1:40:50:03:49
JXHV GK-5561	10.0.2.15
K3WXT8-5562	10.0.2.15
KA94ED-5562	10.0.2.15
KCQD3T-5561	10.0.2.15
KM HPR4-5561	10.0.2.15
LBJ6ZC-5562	10.0.2.15
LMDLPD-5561	10.0.2.15
LRM3Y2-5562	10.0.2.15

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12 - Examination Questions	
WebCode Test	Response
LWKE3D-5561	10.0.2.15
MCQ8YF-5561	10.0.2.15
MD8AY2-5561	10.0.2.15
MK6QJE-5561	10.0.2.15
MR47EE-5562	10.0.2.15
MV6A9L-5561	10.0.2.15
N9Q2B2-5562	10.0.2.15
NH83FA-5562	10.0.2.15
NNQD78-5561	10.0.2.15
NPUPBF-5562	10.0.2.15
NQ7BB3-5561	10.0.2.15
P3EHK8-5562	10.0.2.15
P3ER7C-5561	10.0.2.15
P6NMZG-5561	10.0.2.15
PE6G4X-5561	10.0.2.15
PYKJC4-5561	10.0.2.15
Q4ZTN7-5562	10.0.2.15
Q73JRN-5561	Source Network Address: 10.0.2.15
RBARA4-5561	10.0.2.15
RE7DZL-5561	10.0.2.15
RUTBQ8-5561	10.0.2.15
RY7A78-5561	10.0.2.15

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12 - Examination Questions	
WebCode Test	Response
RZKKZ7-5562	10.0.2.15
T9UAE6-5561	10.0.2.15
TH2XG4-5562	Not in scope
TTGXLB-5561	10.0.2.15
U8973A-5561	10.0.2.15
UEQLM7-5561	10.0.2.15
UEWNPX-5561	10.0.2.15
UGNM4W-5561	10.0.2.15
ULHG2X-5561	10.0.2.15
UPTW39-5562	10.0.2.15
UUA6Q9-5561	10.0.2.15
UZQMYA-5562	10.02.15
V66XC6-5562	10.0.2.15
V82HUJ-5561	10.0.2.15
VXLE96-5561	10.0.2.15
VYTW7Z-5561	10.0.2.15
W447WA-5561	10.0.2.15
WB84Q8-5561	10.0.2.15
WBPY99-5561	10.0.2.15
WFVT36-5561	10.0.2.15
WH6VY2-5561	10.0.2.15
WL2PNP-5561	10.0.2.15

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12 - Examination Questions	
WebCode Test	Response
WL4AK7-5562	10.0.2.15
WQGWCP-5562	10.0.2.15
X2AZR3-5561	10.0.2.15
X3NFAB-5561	10.0.2.15
X62GKW-5561	10.0.2.7
X84MXA-5561	10.0.2.15
XDQM3P-5561	10.0.2.15
XDT8Y6-5562	10.0.2.15
XLP32A-5562	10.0.2.15
XQXJAX-5561	10.0.2.15
Y2PJCZ-5561	10.0.2.15
Y8WZT2-5561	10.0.2.15
YZK9WX-5561	10.0.2.15
Z4GR62-5562	10.0.2.15
Z4PAVK-5561	10.0.2.15
ZBUQRZ-5561	10.0.2.15
ZEU2MZ-5562	10.0.2.15
ZF7RW4-5561	10.0.2.15
ZN4C6R-5561	10.0.2.15
ZQ4URL-5562	10.0.2.15
ZU7QJ2-5561	10.0.2.15
ZWABN2-5562	10.0.2.15

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 12 - Examination Questions

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

Consensus Result:

10.0.2.15

Manufacturer's Response Explanation:

Remote logon information can be found in the Windows Event logs, specifically, Microsoft-Windows-TerminalServices-RemoteConnectionManager Operational.evtx.

Manufacturer's Response Illustration:

Windows Event Viewer - Microsoft-Windows-TerminalServices-RemoteConnectionManager Operational.evtx

The screenshot shows the Windows Event Viewer interface for the log 'Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational'. A table lists three events, with the third event (ID 1149) selected. The details for event 1149 are shown below, including the message 'Remote Desktop Services: User authentication succeeded:' and the 'Source Network Address' field, which is highlighted with a red box and contains the IP address 10.0.2.15. Other details include the user 'tgavin', domain 'EMERGENCYSERVIC', and log name 'Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational'.

Level	Date and Time	Source	Event ID	Task Category
Info	3/13/2024 12:31:24 AM	TerminalServices-RemoteConnectionM...	20523	None
Info	3/13/2024 12:31:24 AM	TerminalServices-RemoteConnectionM...	263	None
Info	3/9/2024 4:03:54 PM	TerminalServices-RemoteConnectionM...	1149	None

Event 1149, TerminalServices-RemoteConnectionManager

General Details

Remote Desktop Services: User authentication succeeded:

User: tgavin
 Domain: EMERGENCYSERVIC
 Source Network Address: 10.0.2.15

Log Name: Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational
 Source: TerminalServices-RemoteCo Logged: 3/9/2024 4:03:54 PM
 Event ID: 1149 Task Category: None
 Level: Information Keywords:
 User: NETWORK SERVICE Computer: Company-13.EmergencyServices.Winchestertonfiel
 OpCode: Info
 More Information: [Event Log Online Help](#)

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13 - Examination Questions

Question 13: Provide the name and path of the active (not deleted) file containing the keyword "flammulated"?

Manufacturer's Response: C:\Users\mohalloran\Pictures\DSC_0921.jpg

Response:

WebCode Test	Response
28NKRK-5561	\Users\mohalloran\Pictures\DSC_0921.jpg
2BXEJB-5561	Fire Department Workstation\Users\mohalloran\Pictures\DSC_0921.jpg
2EUC34-5562	C:\Users\mohalloran\Pictures\DSC_0921.jpg
2UJN7X-5562	\Users\mohalloran\Pictures\DSC_0921.jpg
2XN36N-5561	C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.db
36GUPN-5561	\Users\mohalloran\Pictures\DSC_0921.jpg Also \ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.db
3CH2GJ-5562	[Participant did not return results for this question.]
3DBUC3-5561	[root]/Users/mohalloran/Pictures/DSC_0921.jpg
3K9LKW-5561	Fire Department Workstation-001.e01\NONAME [NTFS]\[root]\Users\mohalloran\Pictures\DSC_0921.jpg
3LM236-5561	/Fire Department Workstation 001/Fire%20Department%20Workstation-1/[Unnamed Disk Image]/[Unnamed Partition]/[File System Users/mohalloran/Pictures/ DSC_0921.jpg
483YXK-5561	C:\Users\mohalloran\Pictures\DSC_0921.jpg
49DVEJ-5561	\Users\mohalloran\Pictures\DSC_0921.jpg
4K6LX2-5561	\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.db
4L6CCW-5562	\Users\mohalloran\Pictures\DSC_0921.jpg
4P6N9W-5561	Fire%20Department%20Workstation-001.e01\NONAME [NTFS]/ [root]/ProgramData/Microsoft/Search/Data/Applications/Windows/Windows.db
4THJUL-5562	[Participant did not return results for this question.]
4XXRHK-5561	C:\Users\mohalloran\Pictures\DSC_0921.jpg and C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.db
4Z77PR-5561	ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.db Keyword also identified in EXIF of \Users\mohalloran\Pictures\DSC_0921.jpg
6KNFKX-5561	C:\Users\mohalloran\Pictures\DSC_0921.jpg
6RLGDW-5561	\Users\mohalloran\Pictures\DSC_0921.jpg

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13 - Examination Questions	
WebCode Test	Response
78YYBQ-5561	\Users\mohalloran\Pictures\DSC_0921.jpg
7M6APW-5561	[root]\Users\mohalloran\Pictures\DSC_0921.jpg
7WAG6W-5561	Users\mohalloran\Pictures\DSC_0921.jpg
7WV3RK-5561	Users\mohalloran\Pictures\DSC_0921.jpg DSC_0921.jpg
8ED4K3-5562	File name: windows.db, File path: C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.db
8LRYCP-5561	Users\mohalloran\Pictures\DSC_0921.jpg
8P8Q2X-5561	Fire%20Department%20Workstation-001.e01/NONAME [NTFS]/ [root]/Users/mohalloran/Pictures/DSC_0921.jpg
8RFV4L-5561	C:\Users\rbliss\Desktop\firetruck.jpg
8W78WW-5562	\Users\mohalloran\Pictures\DSC_0921.jpg
98N78Y-5561	Users\mohalloran\Pictures\DSC_0921.jpg DSC_0921.jpg
9J6THK-5561	C:\Users\mohalloran\Pictures\DSC_0921.jpg
9QMRX6-5561	C:\Users\mohalloran\Pictures\DSC_0921.jpg
9XFKVP-5562	Filepath: Fire20Workstation-001.E01 - Entire Disk (Microsoft NTFS, 39.13 GB)\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.db Filename: Windows.db
AN93XR-5561	\Users\mohalloran\Pictures\DSC_921.jpg
AXDBED-5562	C:\Users\mohalloran\Pictures\DSC_0921.jpg
AXFVBT-5561	/img_Fire%20Department%20Workstation-001.e01/Users/mohalloran/Pictures/DSC_0921.jpg
B2ACZR-5562	\Users\mohalloran\Pictures\DSC_0921.jpg
BA4FBG-5561	C:\Users\mohalloran\Pictures\DSC_0921.jpg DSC_0921.jpg
BPGNBK-5562	/Users/mohalloran/Pictures/DSC_0921.jpg
BVMG7F-5561	Users/mohalloran/Pictures/DSC_0921.jpg
BXTTXP-5561	Users\mohalloran\Pictures\DSC_0921.jpg
CCXUMK-5561	Fire_20Department_20Workstation-001.e01\Root\Users\mohalloran\Pictures\DSC_0921.jpg

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13 - Examination Questions	
WebCode Test	Response
CPQ4TQ-5561	\Users\mohalloran\Pictures\DSC_0921.jpg
D3A9ER-5561	Fire%20Department%20Workstation-001.e01/NONAME [NTFS]/[root]/Users/mohalloran/Pictures/DSC_0921.jpg , File Name: DSC_0921.jpg
D3MR2K-5561	Name: DSC_0921.jpg, Path: Fire20Workstation-001.e01/NONAME [NTFS]/[root]/Users/mohalloran/Pictures/DSC_0921.jpg
D7C7PK-5562	\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.db Windows.db
D8QG3R-5561	Path:Fire%20Department%20Workstation-001.e01\Root\Users\mohalloran\Pictures\ Filename: DSC_0921.jpg
DCKG7E-5561	\Users\mohalloran\Pictures\DSC_0921.jpg
DKUYDR-5561	C:\Users\mohalloran\Pictures\close-up-portrait-of-heroic-fireman-in-protective-suit-and-red-helmet-holds-saved-cat-in-his-arms-firefighter-in-fire-fighting-operation-photo.jpg
DKVPRL-5562	/Users/mohalloran/Pictures/DSC_0921.jpg
DPA82Q-5561	\Users\mohalloran\Pictures\DSC_0921.jpg DSC_0921.jpeg
DTN8XH-5562	File path: \ProgramData\Microsoft\Search\Data\Applications\Windows\ Name : Windows.db
DXKMTK-5561	Users\mohalloran\Pictures\DSC_0921.jpg
EJD6CG-5561	Fire%20Department%20Workstation-001.E01 - Entire Disk (Microsoft NTFS, 39.13 GB)\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.db
EJK3WT-5561	/Users/mohalloran/Pictures/DSC_0921.jpg
EMTM9G-5561	Users\mohalloran\Pictures\DSC_0921.jpg and DSC_0921.jpg
F3TPTL-5561	Users/mohalloran/Pictures/DSC_0921.jpg
F7NG2H-5561	\$Recycle.Bin\S-1-5-21-2298470282-2867887670-580413564-1117\\$RCZUXP4.jpg \$RCZUXP4.jpg
FG6CVN-5561	Path: Fire%20Department%20Workstation-001.e01/NONAME [NTFS]/[root]/Users/mohalloran/Pictures/DSC_0921.jpg Name: DSC_0921.jpg
FT8J39-5561	Fire Department Workstation\Users\mohalloran\Pictures\DSC_0921.jpg
G6U6KA-5561	\Users\mohalloran\Pictures\DSC_0921.jpg
G9BD99-5561	C:\Users\mohalloran\Pictures\DSC_0921.jpg DSC_0921.jpg
G9PQLK-5561	\Users\mohalloran\Pictures\DSC_0921.jpg

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13 - Examination Questions	
WebCode Test	Response
GALGEK-5562	Users\mohalloran\Pictures\DSC_0921.jpg
GMPPAG-5561	C:/Users/mohalloran/Pictures/DSC_0921.jpg
H3X34J-5561	\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.db
HAVVCD-5562	C:\Users\mohalloran\Pictures\DSC_0921.jpg
HFM3VL-5562	[Participant did not return results for this question.]
HGE2AK-5561	Path: C:/Users/mohalloran/Pictures/DSC_0921.jpg Name: DSC_0921.jpg
HMQYPK-5561	\\Users\mohalloran\Pictures\DSC_0921.jpg
HTB6DE-5562	\Users\mohalloran\Pictures DSC_0921.jpg
HVJ3Y9-5561	C:\Users\mohalloran\Pictures\DSC_0921.jpg
HYHLVF-5561	\$Recycle.Bin\S-1-5-21-2298470282-2867887670-580413564-1117\RCZUXP4.jpg \$RCZUXP4.jpg
J3FCTE-5561	Path: Workstation\Users\mohalloran\DSC_0921.jpg. Name: DSC_0921.jpg
J49DM9-5561	C:\Users\mohalloran\Pictures\DSC_0921.jpg
JFURCD-5561	\Users\mohalloran\Pictures\DSC_0921.jpg
JPAH22-5562	C:\Users\mohalloran\Pictures\DSC_0921.jpg
JXAZDE-5561	/Users/mohalloran/Pictures/DSC_0921.jpg DSC_0921.JPG
JXHV GK-5561	root/ProgramData/Microsoft/Search/Data/Applications/Windows/Windows.db
K3WXT8-5562	Users/mohalloran/Pictures/DSC_0921.jpg
KA94ED-5562	/Users/mohalloran/Pictures/DSC_0921.jpg
KCQD3T-5561	C:\Users\mohalloran\Pictures\ DSC_0921.jpg
KMHPR4-5561	Fire Department Workstation\Users\mohalloran\Pictures\DSC_0921.jpg
LBJ6ZC-5562	/NONAME [NTFS]/[root]/Users/mohalloran/Pictures/DSC_0921.jpg DSC_0921.jpg
LMDLPD-5561	Fire Department Workstation\Users\mohalloran\Pictures\DSC_0921.jpg

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13 - Examination Questions	
WebCode Test	Response
LRM3Y2-5562	\Users\mohalloran\Pictures\DSC_0921.jpg
LWKE3D-5561	C:\Users\mohalloran\Pictures\DSC_0921.jpg
MCQ8YF-5561	[root]\ProgramData\Microsoft\Search\Data\applications\Windows\Windows.db
MD8AY2-5561	Users\mohalloran\Pictures\DSC_0921.jpg
MK6QJE-5561	\Users\mohalloran\Pictures\DSC_0921.jpg
MR47EE-5562	C:\Users\mohalloran\Pictures\DSC_0921.jpg
MV6A9L-5561	Users/mohalloran/Pictures/DSC_0921.jpg
N9Q2B2-5562	C:\Users\mohalloran\Pictures\DSC_0921.jpg
NH83FA-5562	Filepath: \Users\mohalloran\Pictures Name: DSC_0921.jpg
NNQD78-5561	C:\Users\mohalloran\Pictures\DSC_0921.jpg
NPUPBF-5562	\Users\mohalloran\Pictures\DSC_0921.jpg DSC_0921.jpeg
NQ7BB3-5561	\users\mohalloran\pictures\DSC_0921.jpg
P3EHK8-5562	\Users\mohalloran\Pictures\DSC_0921.jpg
P3ER7C-5561	/root/Users/mohalloran/Pictures/DSC.0921.jpg
P6NMZG-5561	/Root/ProgramData/Microsoft/Search/Data/Applications/Windows/Windows.db
PE6G4X-5561	Users\mohalloran\Pictures\ DSC_0921.jpg
PYKJC4-5561	C:\Users\mohalloran\Pictures\close-up-portrait-of-heroic-fireman-in-protective-suit-and-red-helmet-holds-saved-cat-in-his-arms-firefighter-in-fire-fighting-operation-photo.jpg
Q4ZTN7-5562	Users\mohalloran\Pictures\DSC_0921.jpg
Q73JRN-5561	c:\users\mohalloran\pictures\DSC_0921.jpg
RBARA4-5561	[root]\Users\mohalloran\Pictures\DSC_0921.jpg
RE7DZL-5561	Users\mohalloran\Pictures\DSC_0921.jpg
RUTBQ8-5561	Path: /Users/mohalloran/Pictures/DSC_0921.jpg Name: DSC_0921.jpg

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13 - Examination Questions	
WebCode Test	Response
RY7A78-5561	Users\mohalloran\Pictures\DSC_0921.jpg
RZKKZ7-5562	C:/Users/mohalloran/Pictures/DSC_0921.jpg
T9UAE6-5561	C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.db
TH2XG4-5562	\Users\mohalloran\Pictures\DSC_0921.jpg
TTGXLB-5561	Fire Department Workstation\Users\mohalloran\Pictures\DSC_0921.jpg
U8973A-5561	Workstation\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.db
UEQLM7-5561	C:\Users\mohalloran\Pictures\DSC_0921.jpg
UEWNPX-5561	\Users\mohalloran\Pictures\n-photo.jpg
UGNM4W-5561	\Users\mohalloran\Pictures\DSC_0921.jpg
ULHG2X-5561	C:\Users\mohalloran\Pictures\close-up-portrait-of-heroic-fireman-in-protective-suit-and-red-helmet-holds-saved-cat-in-his-arms-firefighter-in-fire-fighting-operation-photo.jpg
UPTW39-5562	C:\Users\mohalloran\Pictures\DSC_0921.jpg
UUA6Q9-5561	Fire Department Workstation\Users\mohalloran\Pictures\DSC_0921.jpg
UZQMYA-5562	Fire Department Workstation\Users\Mohalloran\Pictures\DSC_0921.JPG
V66XC6-5562	C:\Users\mohalloran\Pictures\DSC_0921.jpg DSC_0921.jpg
V82HUJ-5561	Fire Department Workstation\Users\mohalloran\Pictures\DSC_0921.jpg
VXLE96-5561	Path: C:\Users\mohalloran\Pictures\DSC_0921.jpg (Fire20Workstation-001:\Users\mohalloran\Pictures\DSC_0921.jpg) FileName: DSC_0921.jpg
VYTW7Z-5561	[Participant did not return results for this question.]
W447WA-5561	root\users\mohalloran\pictures\DSC_0921.jpg
WB84Q8-5561	C:\Users\mohalloran\Pictures\DSC_0921.jpg
WBPY99-5561	C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.db
WFVT36-5561	C:\Users\mohalloran\Pictures\DSC_0921.jpg
WH6VY2-5561	\$Recycle.Bin\S-1-5-21-2298470282-2867887670-580413564-1117\RCZUXP4.jpg \$RCZUXP4.jpg

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13 - Examination Questions	
WebCode Test	Response
WL2PNP-5561	C:\Users\mohalloran\pictures\DSC_0921.jpg C:\Users\rbliss\Desktop\firetruck..jpg
WL4AK7-5562	Users\mohalloran\Pictures\DSC_0921.jpg (I think this is the 'correct' answer, but X-rays located two more hits in a database file as follows: \ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.db)
WQGWCPC-5562	Path: Users\mohalloran\Pictures\DSC_0921.jpg Name: DSC_0921.jpg
X2AZR3-5561	\Users\mohalloran\Pictures\DSC_0921.jpg DSC_0921.jpg
X3NFAB-5561	path: C:\Users\mohalloran\Pictures\DSC_0921.jpg filename: DSC_0921.jpg
X62GKW-5561	\Users\mohalloran\Pictures\DSC_0921.jpg
X84MXA-5561	DSC_0921.jpg
XDQM3P-5561	\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.db
XDT8Y6-5562	Fire Department Workstation\Users\mohalloran\Pictures\DSC_0921.jpg
XLP32A-5562	C:\Users\rbliss\Desktop\firetruck..jpg
XQXJAX-5561	Users\mohalloran\Pictures\DSC_0921.jpg
Y2PJCZ-5561	/ProgramData/Microsoft/Search/Data/Applications/Windows/Windows.db Windows.db
Y8WZT2-5561	C:/Users/mohalloran/Pictures/DSC_0921.jpg
YZK9WX-5561	Fire20Workstation-001.e01\Root\Users\mohalloran\Pictures\DSC_0921.jpg
Z4GR62-5562	C:/Users/mohalloran/Pictures/DSC_0921.jpg and C:/ProgramData/Microsoft/Search/Data/Applications/Windows/Windows.db **SEE Additional Comments**
Z4PAVK-5561	Fire Department Workstation\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.db
ZBUQRZ-5561	/img_Fire_20Department_20Workstation-001.e01/Users/mohalloran/Pictures/DSC_0921.jpg
ZEU2MZ-5562	/Users/mohalloran/Pictures/DSC_0921.jpg DSC_0921.jpg
ZF7RW4-5561	C:\Users\mohalloran\Pictures\DSC_0921.jpg
ZN4C6R-5561	\Users\mohalloran\Pictures\DSC_0921.jpg
ZQ4URL-5562	Path: ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.db Name : Windows.db
ZU7QJ2-5561	root\Users\mohalloran\Pictures\DSC_0921.jpg

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13 - Examination Questions	
WebCode Test	Response
ZWABN2- 5562	\Users\mohalloran\Pictures\DSC_0921.jpg

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 13 - Examination Questions

Question 13: Provide the name and path of the active (not deleted) file containing the keyword "flamulated"?

Consensus Result:

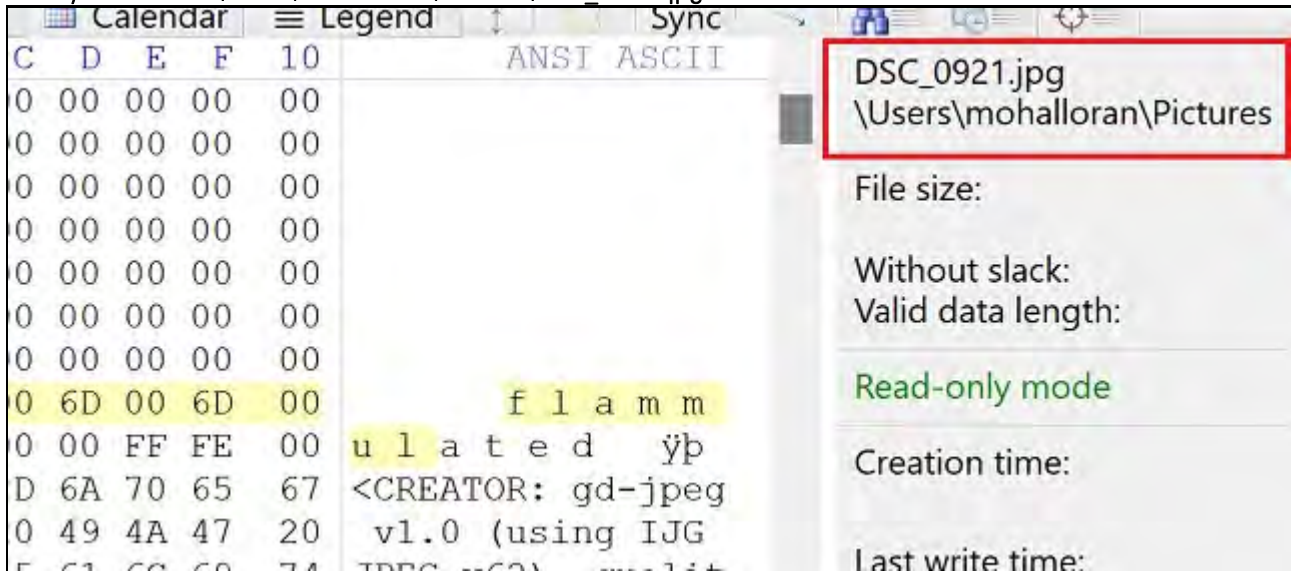
C:\Users\mohalloran\Pictures\DSC_0921.jpg. The response of \ProgramData\Microsoft\Search\Data\Applications\Windows\ was also accepted as it appears that Windows indexed "flamulated" and it ended up in the search index.

Manufacturer's Response Explanation:

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

Manufacturer's Response Illustration:

X-Ways view of C:\Users\mohalloran\Pictures\DSC_0921.jpg



Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 14 - Examination Questions

Question 14: What text appears in the desktop background photo for user kshea?

Manufacturer's Sleep 'til you're hungry, eat 'til you're sleepy.

Response:

WebCode Test	Response
28NKRK-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
2BXEJB-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
2EUC34-5562	sleep 'til you're hungry – eat 'til you're sleepy
2UJN7X-5562	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan
2XN36N-5561	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan
36GUPN-5561	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan quotefancy
3CH2GJ-5562	[Participant did not return results for this question.]
3DBUC3-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
3K9LKW-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
3LM236-5561	Sleep 'til you're hungry, eat 'til you're sleepy
483YXK-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
49DVEJ-5561	Sleep 'til you're hungry. eat 'til you're sleepy.
4K6LX2-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
4L6CCW-5562	Sleep 'til you're hungry, eat 'til you're sleepy
4P6N9W-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
4THJUL-5562	[Participant did not return results for this question.]
4XXRHK-5561	Sleep 'til you're hungry. Eat 'til you're sleepy. Niall Horan quotefancy
4Z77PR-5561	Sleep 'til you're hungry, eat 'til you're sleepy Niall Horan quotefancy
6KNFKX-5561	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan "quotefancy
6RLGDW-5561	"Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan quotefancy"
78YYBQ-5561	Sleep 'til you're hungry, eat 'til you're sleepy.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 14 - Examination Questions	
WebCode Test	Response
7M6APW-5561	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan quotefancy
7WAG6W-5561	Sleep 'til you're hungry, eat 'til you're sleepy
7WV3RK-5561	Sleep `til you're hungry, eat `til you're sleepy.
8ED4K3-5562	Sleep 'til you're hungry, eat 'll you're sleepy.
8LRYCP-5561	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan
8P8Q2X-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
8RFV4L-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
8W78VW-5562	Sleep 'til you're hungry. eat 'til you're sleepy. Niall Horan quotefancy
98N78Y-5561	Sleep til you're hungry, eat 'til you're sleepy
9J6THK-5561	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan
9QMRX6-5561	Sleep 'till you're hungry, eat 'till you're sleepy
9XFKVP-5562	Sleep 'til you're hungry, eat 'til you're sleepy.
AN93XR-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
AXDBED-5562	Sleep 'till you're hungry, eat 'till you're sleepy. Niall Horan. "quotefancy
AXFVBT-5561	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan
B2ACZR-5562	Sleep 'til you're hungry, eat 'til you're sleepy
BA4FBG-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
BPGNBK-5562	Sleep 'til you're hungry, eat 'til you're sleepy
BVMG7F-5561	Sleep 'til you're hungry, eat 'til you're sleepy
BXTTTP-5561	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan
CCXUMK-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
CPQ4TQ-5561	Sleep 'til you're hungry, eat 'till you're sleepy.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 14 - Examination Questions	
WebCode Test	Response
D3A9ER-5561	Sleep til you're hungry, eat 'til you're sleepy
D3MR2K-5561	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan "quotefancy
D7C7PK-5562	Sleep 'til you're hungry, eat 'til you're sleepy.
D8QG3R-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
DCKG7E-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
DKUYDR-5561	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan
DKVPRL-5562	Sleep 'til you're hungry, eat 'til you're sleepy
DPA82Q-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
DTN8XH-5562	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan "quotefancy
DXKMTK-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
EJD6CG-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
EJK3WT-5561	Sleep 'til you're hungry, eat 'til you're sleepy. – Niall Horan
EMTM9G-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
F3TPTL-5561	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan
F7NG2H-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
FG6CVN-5561	Sleep 'til you're hungry, Eat 'til you're sleepy.
FT8J39-5561	Sleep 'til you're hungry, eat 'til you're sleepy. - Niall Horan quotefancy
G6U6KA-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
G9BD99-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
G9PQLK-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
GALGEK-5562	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Howran
GMPPAG-5561	Sleep'tilyou'rehungry, eat'tilyou'resleepy. Niall Horan "quotefancy

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 14 - Examination Questions	
WebCode Test	Response
H3X34J-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
HAVVCD-5562	Sleep 'til you're hungry, eat 'til you're sleepy
HFM3VL-5562	[Participant did not return results for this question.]
HGE2AK-5561	"Sleep 'till you're hungry, eat 'til you're sleepy."
HMQYPK-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
HTB6DE-5562	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan. quotefancy
HVJ3Y9-5561	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan "quotefancy
HYHLVF-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
J3FCTE-5561	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan
J49DM9-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
JFURCD-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
JPAH22-5562	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan
JXAZDE-5561	Sleep 'til you're hungry, eat 'til you're sleepy
JXHV GK-5561	Sleep 'til you're hungry, eat 'till you're sleepy.
K3WXT8-5562	Sleep 'til you're hungry, eat 'til you're sleepy.
KA94ED-5562	Sleep til your're hungry, eat til you're sleepy
KCQD3T-5561	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan
KMHPR4-5561	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan quotefancy
LBJ6ZC-5562	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan
LMDLPD-5561	Sleep 'til you're hungry, eat 'til you're sleepy
LRM3Y2-5562	Sleep 'til you're hungry, eat 'til you're sleepy.
LWKE3D-5561	Sleep 'til you're hungry, eat 'til you're sleepy -Niall Horan

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 14 - Examination Questions	
WebCode Test	Response
MCQ8YF-5561	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan
MD8AY2-5561	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan "quotefancy
MK6QJE-5561	Sleep 'til you're hungry, eat 'til you're sleepy
MR47EE-5562	Sleep 'til you're hungry, eat 'til you're sleepy
MV6A9L-5561	Sleep til you're hungry, eat til you're sleepy
N9Q2B2-5562	Sleep 'til you're hungry, eat 'til you're sleepy.
NH83FA-5562	Sleep 'til you're hungry, eat 'til you're sleepy.
NNQD78-5561	sleep 'til you're hungry, eat 'till you're sleepy
NPUPBF-5562	Sleep 'til you're hungry, eat 'til you're sleepy.
NQ7BB3-5561	"Sleep 'till you're hungry, eat 'til you're sleepy. Niall Horan quotefancy"
P3EHK8-5562	Sleep 'til you're hungry, eat 'til you're sleepy.
P3ER7C-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
P6NMZG-5561	Sleep 'til you're hungry, eat 'til you're sleepy. Nial Horan
PE6G4X-5561	"Sleep 'til you're hungry, eat 'til you're sleepy"
PYKJC4-5561	Sleep 'til your're hungry, eat 'til you're sleepy.
Q4ZTN7-5562	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan
Q73JRN-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
RBARA4-5561	"Sleep 'til you're hungry, eat 'til you're sleepy."
RE7DZL-5561	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan "quotefancy
RUTBQ8-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
RY7A78-5561	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan
RZKKZ7-5562	Sleep'tilyou'rehungry, eat'tilyou'resleepy. Niall Horan "quotefancy

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 14 - Examination Questions	
WebCode Test	Response
T9UAE6-5561	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan quotefancy
TH2XG4-5562	Not in scope
TTGXLB-5561	Sleep 'til you're hungry, eat 'til you're sleepy
U8973A-5561	Sleep 'til you're hungry, eat 'til you're sleepy
UEQLM7-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
UEWNPX-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
UGNM4W-5561	Sleep 'til you're hungry, Eat 'til you're sleepy. Niall Horan "quotefancy
ULHG2X-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
UPTW39-5562	sleep 'til you're hungry – eat 'til you're sleepy
UUA6Q9-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
UZQMYA-5562	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan
V66XC6-5562	Sleep 'til you're hungry, eat 'til you're sleepy
V82HUJ-5561	Sleep 'til you're hungry. eat 'til you're sleepy.
VXLE96-5561	sleep 'til you're hungry, eat 'til you're sleepy.
VYTW7Z-5561	Sleep 'til you're hungry, eat 'til you're sleepy
W447WA-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
WB84Q8-5561	sleep 'til you're hungry – eat 'til you're sleepy
WBPY99-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
WFVT36-5561	Sleep 'til you're hungry, Eat 'til you're sleepy. Niall Horan "quoterfancy
WH6VY2-5561	Sleep 'til you're hungry, eat 'til you're sleepy. - Niall Horan
WL2PNP-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
WL4AK7-5562	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 14 - Examination Questions	
WebCode Test	Response
WQGWCP-5562	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan
X2AZR3-5561	Sleep 'til you're hungry, eat 'til you're sleepy
X3NFAB-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
X62GKW-5561	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan
X84MXA-5561	Sleep 'till you're hungry, eat 'til you're sleepy. Nial Horan
XDQM3P-5561	Sleep 'til you're hungry, eat 'til you're sleepy – Niall Horan
XDT8Y6-5562	Sleep 'til you're hungry, eat 'til you're sleepy. - Niall Horan
XLP32A-5562	Sleep 'til you're hungry, eat 'til you're sleepy.
XQXJAX-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
Y2PJCZ-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
Y8WZT2-5561	Sleep 'til you're hungry, eat 'til you're sleepy
YZK9WX-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
Z4GR62-5562	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan "quotefancy
Z4PAVK-5561	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan QuoteFancy
ZBUQRZ-5561	Sleep 'til you're hungry, eat 'til you're sleepy
ZEU2MZ-5562	Sleep 'til you're hungry, eat 'til you're sleepy. Niall Horan
ZF7RW4-5561	sleep 'til you're hungry – eat 'til you're sleepy
ZN4C6R-5561	Sleep 'til you're hungry, eat 'til you're sleepy.
ZQ4URL-5562	Sleep 'till you're hungry, eat 'til you're sleepy.
ZU7QJ2-5561	Sleep 'til you're hungry, eat 'til you're sleep. Niall Horan "quotefancy
ZWABN2-5562	Sleep 'til you're hungry, eat 'til you're sleepy

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 14 - Examination Questions

Question 14: What text appears in the desktop background photo for user kshea?

Consensus Result:

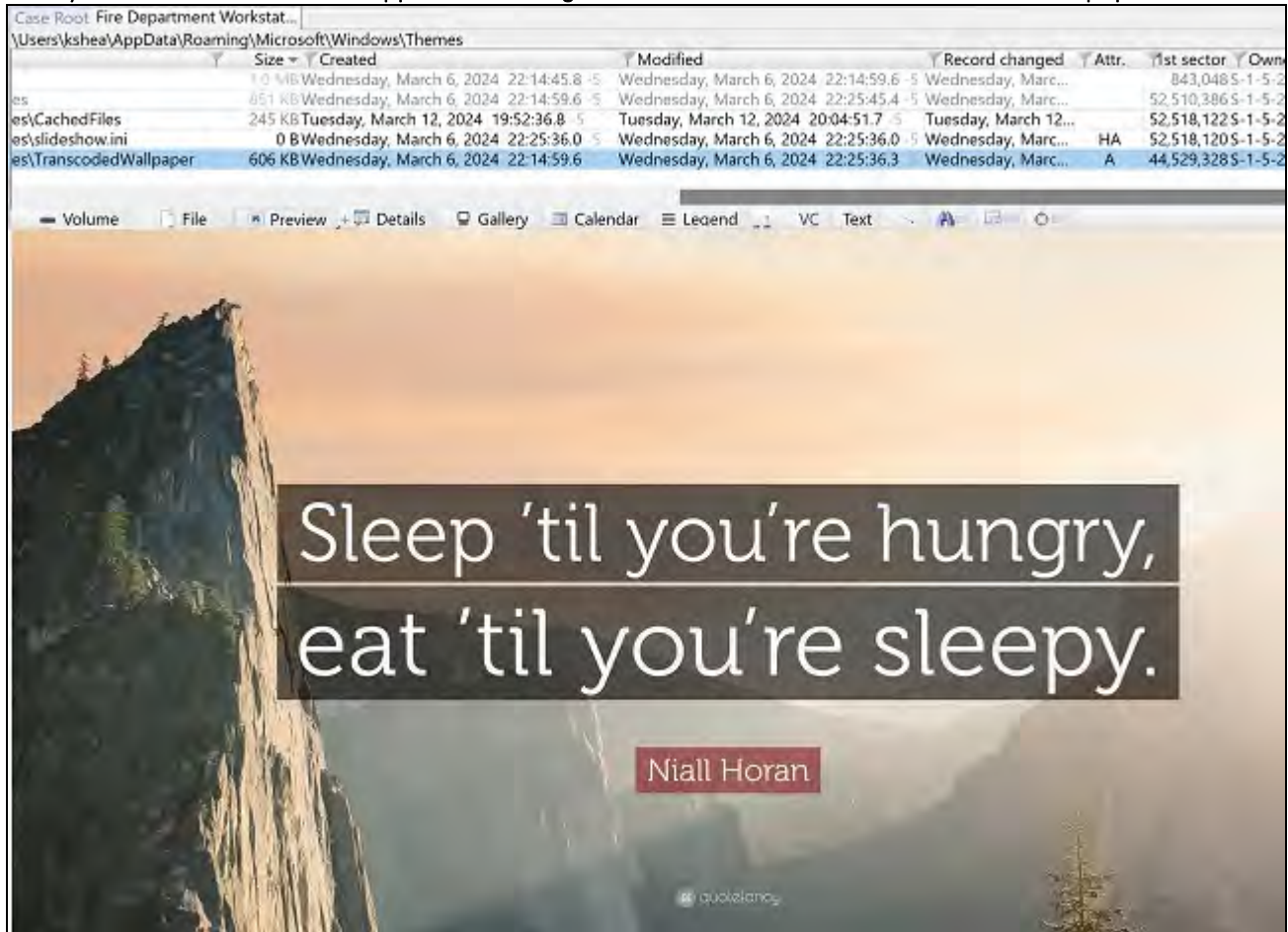
"Sleep 'til you're hungry, eat 'til you're sleepy." and any slight variations of this response, if it was easily determined to be a formatting issue.

Manufacturer's Response Explanation:

User's desktop background images are stored in \Users\<>username>\AppData\Roaming\Microsoft\Windows\Themes\TranscodedWallpaper

Manufacturer's Response Illustration:

X-Ways view of C:\Users\kshea\AppData\Roaming\Microsoft\Windows\Themes\TranscodedWallpaper



Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15 - Examination Questions

Question 15: Who is listed as the author of the document with SHA1 hash 0C67015E256CF9B9030DAA0E517B161DC95EA0F0?

Manufacturer's James Moore

Response:

WebCode Test	Response
28NKRK-5561	James Moore
2BXEJB-5561	James Moore
2EUC34-5562	James Moore
2UJN7X-5562	James Moore
2XN36N-5561	James Moore
36GUPN-5561	James Moore
3CH2GJ-5562	[Participant did not return results for this question.]
3DBUC3-5561	James Moore
3K9LKW-5561	James Moore
3LM236-5561	James Moore
483YXK-5561	James Moore
49DVEJ-5561	James Moore
4K6LX2-5561	James Moore
4L6CCW-5562	James Moore
4P6N9W-5561	James Moore
4THJUL-5562	[Participant did not return results for this question.]
4XXRHK-5561	James Moore
4Z77PR-5561	James Moore
6KNFKX-5561	James Moore
6RLGDW-5561	James Moore

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15 - Examination Questions	
WebCode Test	Response
78YYBQ-5561	James Moore
7M6APW-5561	James Moore
7WAG6W-5561	James Moore
7WV3RK-5561	James Moore
8ED4K3-5562	James Moore
8LRYCP-5561	James Moore
8P8Q2X-5561	James Moore
8RFV4L-5561	James Moore
8W78WW-5562	James Moore
98N78Y-5561	James Moore
9J6THK-5561	James Moore
9QMRX6-5561	James Moore
9XFKVP-5562	James Moore
AN93XR-5561	James Moore
AXDBED-5562	James Moore
AXFVBT-5561	James Moore
B2ACZR-5562	James Moore
BA4FBG-5561	James Moore
BPGNBK-5562	James Moore
BVMG7F-5561	James Moore
BXTTYP-5561	James Moore
CCXUMK-5561	James Moore

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15 - Examination Questions	
WebCode Test	Response
CPQ4TQ-5561	James Moore
D3A9ER-5561	James Moore
D3MR2K-5561	James Moore
D7C7PK-5562	Author: James Moore
D8QG3R-5561	James Moore
DCKG7E-5561	James Moore
DKUYDR-5561	James Moore
DKVPRL-5562	James Moore
DPA82Q-5561	James Moore
DTN8XH-5562	James Moore
DXKMTK-5561	James Moore
EJD6CG-5561	James Moore
EJK3WT-5561	James Moore
EMTM9G-5561	James Moore
F3TPTL-5561	James Moore
F7NG2H-5561	James Moore
FG6CVN-5561	James Moore
FT8J39-5561	James Moore
G6U6KA-5561	James Moore
G9BD99-5561	James Moore
G9PQLK-5561	James Moore. Document is stored on the user account 'kshea'
GALGEK-5562	James Moore

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15 - Examination Questions	
WebCode Test	Response
GMPPAG-5561	James Moore
H3X34J-5561	James Moore
HAWCD-5562	James Moore
HFM3VL-5562	[Participant did not return results for this question.]
HGE2AK-5561	James Moore
HMQYPK-5561	James Moore
HTB6DE-5562	James Moore
HVJ3Y9-5561	James Moore
HYHLVF-5561	James Moore
J3FCTE-5561	James Moore
J49DM9-5561	James Moore
JFURCD-5561	James Moore
JPAH22-5562	James Moore
JXAZDE-5561	James Moore
JXHV GK-5561	James Moore
K3WXT8-5562	James Moore
KA94ED-5562	James Moore
KCQD3T-5561	James Moore
KMHPR4-5561	James Moore
LBJ6ZC-5562	James Moore
LMDLPD-5561	James Moore
LRM3Y2-5562	James Moore

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15 - Examination Questions	
WebCode Test	Response
LWKE3D-5561	James Moore
MCQ8YF-5561	James Moore
MD8AY2-5561	James Moore
MK6QJE-5561	James Moore
MR47EE-5562	James Moore
MV6A9L-5561	James Moore
N9Q2B2-5562	James Moore
NH83FA-5562	James Moore
NNQD78-5561	James Moore
NPUPBF-5562	James Moore
NQ7BB3-5561	James Moore
P3EHK8-5562	James Moore
P3ER7C-5561	James Moore
P6NMZG-5561	James Moore
PE6G4X-5561	James Moore
PYKJC4-5561	James Moore
Q4ZTN7-5562	James Moore
Q73JRN-5561	James Moore
RBARA4-5561	James Moore
RE7DZL-5561	James Moore
RUTBQ8-5561	James Moore
RY7A78-5561	James Moore

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15 - Examination Questions	
WebCode Test	Response
RZKKZ7-5562	James Moore
T9UAE6-5561	James Moore
TH2XG4-5562	James Moore
TTGXLB-5561	James Moore
U8973A-5561	JAMES MOORE
UEQLM7-5561	James Moore
UEWNPX-5561	James Moore
UGNM4W-5561	James Moore
ULHG2X-5561	James Moore
UPTW39-5562	James Moore
UUA6Q9-5561	James Moore
UZQMYA-5562	James Moore
V66XC6-5562	James Moore
V82HUJ-5561	James Moore
VXLE96-5561	James Moore
VYTW7Z-5561	[Participant did not return results for this question.]
W447WA-5561	James Moore
WB84Q8-5561	James Moore
WBPY99-5561	James Moore
WFVT36-5561	James Moore
WH6VY2-5561	James Moore
WL2PNP-5561	James Moore

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15 - Examination Questions	
WebCode Test	Response
WL4AK7-5562	James Moore
WQGWCP-5562	James Moore
X2AZR3-5561	James Moore
X3NFAB-5561	James Moore
X62GKW-5561	James Moore
X84MXA-5561	James Moore
XDQM3P-5561	James Moore
XDT8Y6-5562	James Moore
XLP32A-5562	James Moore
XQXJAX-5561	James Moore
Y2PJCZ-5561	James Moore
Y8WZT2-5561	James Moore
YZK9WX-5561	James Moore
Z4GR62-5562	James Moore
Z4PAVK-5561	James Moore
ZBUQRZ-5561	James Moore
ZEU2MZ-5562	James Moore
ZF7RW4-5561	James Moore
ZN4C6R-5561	James Moore
ZQ4URL-5562	James Moore
ZU7QJ2-5561	James Moore
ZWABN2-5562	James Moore

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 15 - Examination Questions

Question 15: Who is listed as the author of the document with SHA1 hash 0C67015E256CF9B9030DAA0E517B161DC95EA0F0?

Consensus Result:

James Moore

Manufacturer's Response Explanation:

C:\Users\kshea\Documents\my-favorite-thin-crisp-chocolate-chip-cookies-recipe.docx has the above SHA1 hash. Microsoft "Word" format documents contain metadata fields including one identifying the author.

Manufacturer's Response Illustration:

Windows Explorer view of my-favorite-thin-crisp-chocolate-chip-cookies-recipe.docx details

The screenshot shows the 'Details' pane of a Windows Explorer window. The file name is 'my-favorite-thin-crisp-chocolate-chip-cookies-recipe.docx'. The 'General' tab is selected. The 'Property' and 'Value' columns are visible. The 'Authors' property is highlighted with a red box and contains the value 'James Moore'. Other properties include 'Last saved by' (James Moore), 'Revision number 2', 'Version number', 'Program name' (Microsoft Office Word), 'Company', 'Manager', 'Content created' (8/4/2017 12:16 PM), 'Date last saved' (8/6/2017 1:47 PM), 'Last printed', and 'Total editing time' (01:49:00). A link at the bottom says 'Remove Properties and Personal Information'.

Property	Value
Description	
Origin	
Authors	James Moore
Last saved by	James Moore
Revision number	2
Version number	
Program name	Microsoft Office Word
Company	
Manager	
Content created	8/4/2017 12:16 PM
Date last saved	8/6/2017 1:47 PM
Last printed	
Total editing time	01:49:00
Content	

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16 - Examination Questions

Question 16: Provide the hostname (computer name) for the computer on which the file `agency_admin_guide_2004.pdf` was located.

Manufacturer's FIRE-DC01

Response:

WebCode Test	Response
28NKRK-5561	FIRE-DC01
2BXEJB-5561	FIRE-DC01\fire drive
2EUC34-5562	FIRE-DC01
2UJN7X-5562	FIRE-DC01
2XN36N-5561	FIRE-DC01
36GUPN-5561	FIRE-DC01
3CH2GJ-5562	[Participant did not return results for this question.]
3DBUC3-5561	FIRE-DC01
3K9LKW-5561	FIRE-DC01
3LM236-5561	fire-dc01
483YXK-5561	FIRE-DC01
49DVEJ-5561	FIRE-DC01
4K6LX2-5561	FIRE-DC01
4L6CCW-5562	\\FIRE-DC01\
4P6N9W-5561	Fire-dc01
4THJUL-5562	[Participant did not return results for this question.]
4XXRHK-5561	FIRE-DC01
4Z77PR-5561	fire-dc01
6KNFKX-5561	FIRE-DC01
6RLGDW-5561	\\FIRE-DC01\

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16 - Examination Questions	
WebCode Test	Response
78YYBQ-5561	fire-dc01
7M6APW-5561	Fire-dc01
7WAG6W-5561	fire-dc01
7WV3RK-5561	Fire-dc01
8ED4K3-5562	fire-dc01
8LRYCP-5561	FIRE-DC01
8P8Q2X-5561	Fire-DC01
8RFV4L-5561	FIRE-DC01
8W78WW-5562	fire-dc01
98N78Y-5561	FIRE-DC01
9J6THK-5561	fire-dc01
9QMRX6-5561	FIRE-DC01
9XFKVP-5562	fire-dc01
AN93XR-5561	FIRE-DC01
AXDBED-5562	FIRE-DC01
AXFVBT-5561	FIRE-DC01
B2ACZR-5562	Fire-dc01
BA4FBG-5561	fire-dc01
BPGNBK-5562	FIRE-DC01
BVMG7F-5561	FIRE-DC01
BXTTYP-5561	FIRE-DC01
CCXUMK-5561	fire-dc01

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16 - Examination Questions	
WebCode Test	Response
CPQ4TQ-5561	FIRE-DC01
D3A9ER-5561	FIRE-DC01
D3MR2K-5561	fire-dc01
D7C7PK-5562	Net Bios Name: fire-dc01
D8QG3R-5561	FIRE-DC01
DCKG7E-5561	FIRE-DC01
DKUYDR-5561	FIRE-DC01
DKVPRL-5562	FIRE-DC01
DPA82Q-5561	FIRE-DC01
DTN8XH-5562	fire-dc01
DXKMTK-5561	FIRE-DC01
EJD6CG-5561	FIRE-DC01
EJK3WT-5561	fire-dc01
EMTM9G-5561	FIRE-DC01
F3TPTL-5561	fire-dc01
F7NG2H-5561	fire-dc01
FG6CVN-5561	fire-dc01
FT8J39-5561	FIRE-DC01
G6U6KA-5561	fire-dc01
G9BD99-5561	FIRE-DC01
G9PQLK-5561	fire-dc01
GALGEK-5562	FIRE-DC01

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16 - Examination Questions	
WebCode Test	Response
GMPPAG-5561	FIRE-DC01
H3X34J-5561	fire-dc01
HAWCD-5562	FIRE-DC01
HFM3VL-5562	[Participant did not return results for this question.]
HGE2AK-5561	FIRE-DC01
HMQYPK-5561	fire-dc01
HTB6DE-5562	FIRE-DC01
HVJ3Y9-5561	Fire-DC01
HYHLVF-5561	fire-dc01
J3FCTE-5561	\\FIRE-DC01\fire drive\agency_admin_guide_2004.pdf, pathi: Users\rbliss\Desktop\agency_admin_guide_2004 - Shortcut.lnk
J49DM9-5561	FIRE-DC01
JFURCD-5561	\\FIRE-DC01\
JPAH22-5562	FIRE-DC01
JXAZDE-5561	FIRE-DC01
JXHV GK-5561	FIRE-DC01
K3WXT8-5562	FIRE-DC01
KA94ED-5562	\\FIRE-DC01\fire drive\agency_admin_guide_2004.pdf
KCQD3T-5561	FIRE-DC01
KMHPR4-5561	fire-dc01
LBJ6ZC-5562	FIRE-DC01
LMDLPD-5561	fire-dc01
LRM3Y2-5562	FIRE-DC01

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16 - Examination Questions	
WebCode Test	Response
LWKE3D-5561	fire-dc01
MCQ8YF-5561	FIRE-DC01
MD8AY2-5561	fire-dc01
MK6QJE-5561	fire_dc01
MR47EE-5562	\\FIRE-DC01\fire drive
MV6A9L-5561	FIRE-DC01
N9Q2B2-5562	FIRE-DC01
NH83FA-5562	FIRE-DC01
NNQD78-5561	fire-dc01
NPUPBF-5562	FIRE-DC01
NQ7BB3-5561	FIRE-DC01
P3EHK8-5562	FIRE-DC01
P3ER7C-5561	\\FIRE-DC01\firedrive\
P6NMZG-5561	FIRE-DC01
PE6G4X-5561	FIRE-DC01
PYKJC4-5561	FIRE-DC01
Q4ZTN7-5562	FIRE-DC01
Q73JRN-5561	FIRE-DC01
RBARA4-5561	\\FIRE-DC01\
RE7DZL-5561	FIRE-DC01
RUTBQ8-5561	FIRE-DC01
RY7A78-5561	FIRE-DC01

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16 - Examination Questions	
WebCode Test	Response
RZKKZ7-5562	FIRE-DC01
T9UAE6-5561	FIRE-DC01
TH2XG4-5562	Not in scope
TTGXLB-5561	FIRE-DC01
U8973A-5561	FIRE-DC01
UEQLM7-5561	\\FIRE-DC01\fire drive
UEWNPX-5561	fire-dc01
UGNM4W-5561	fire-dc01
ULHG2X-5561	FIRE-DC01
UPTW39-5562	FIRE-DC01
UUA6Q9-5561	FIRE-DC01
UZQMYA-5562	FIRE-DC01
V66XC6-5562	FIRE-DC01
V82HUJ-5561	FIRE-DC01
VXLE96-5561	fire-dc01
VYTW7Z-5561	fire-dc01
W447WA-5561	FIRE-DC01
WB84Q8-5561	FIRE-DC01
WBPY99-5561	FIRE-DC01
WFVT36-5561	FIRE-DC01
WH6VY2-5561	fire-dc01
WL2PNP-5561	FIRE-DC01

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16 - Examination Questions	
WebCode Test	Response
WL4AK7-5562	fire-dc01
WQGWCP-5562	FIRE-DC01
X2AZR3-5561	FIRE-DC01
X3NFAB-5561	FIRE-DC01
X62GKW-5561	\\FIRE-DC01
X84MXA-5561	FIRE-DC01
XDQM3P-5561	FIRE-DC01
XDT8Y6-5562	FIRE-DC01
XLP32A-5562	rbliss
XQXJAX-5561	fire-dc01
Y2PJCZ-5561	Fire-dc01
Y8WZT2-5561	FIRE-DC01
YZK9WX-5561	FIRE-DC01
Z4GR62-5562	FIRE-DC01
Z4PAVK-5561	FIRE-DC01
ZBUQRZ-5561	FIRE-DC01
ZEU2MZ-5562	FIRE-DC01
ZF7RW4-5561	FIRE-DC01
ZN4C6R-5561	FIRE-DC01
ZQ4URL-5562	fire-dc01
ZU7QJ2-5561	fire-dc01
ZWABN2-5562	fire-dc01

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 16 - Examination Questions

Question 16: Provide the hostname (computer name) for the computer on which the file `agency_admin_guide_2004.pdf` was located.

Consensus Result:

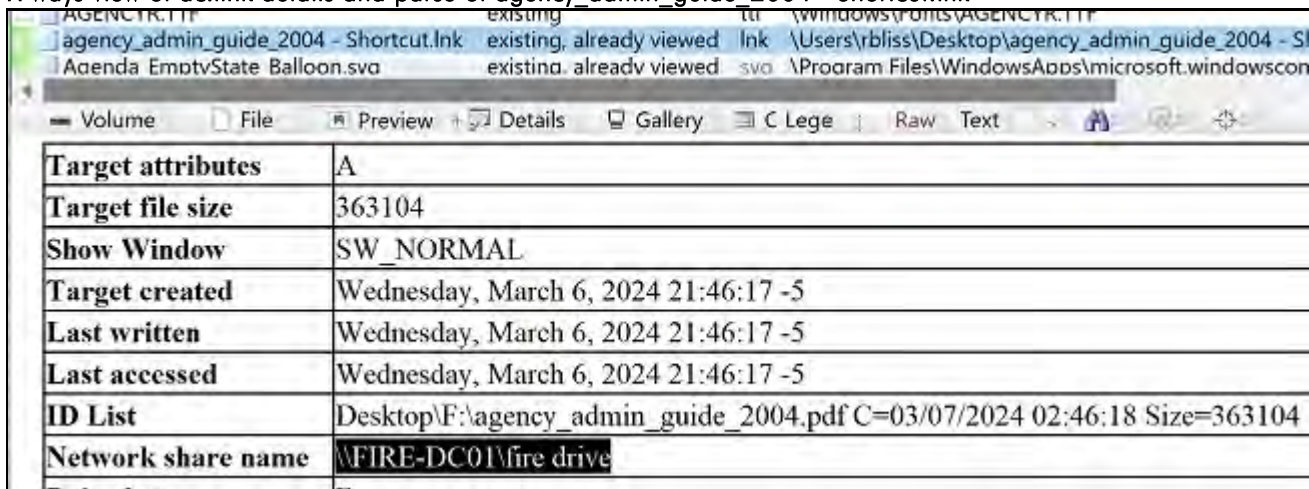
FIRE-DC01

Manufacturer's Response Explanation:

Links to recently opened files are created in users' `~\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. Searching for the filename across the subject computer discovers this link file, `agency_admin_guide_2004 - Shortcut.lnk`. The contents of the link file show the location of the file to be on a network share, `\\FIRE-DC01\fire drive`.

Manufacturer's Response Illustration:

X-ways view of `ac.link` details and parse of `agency_admin_guide_2004 - Shortcut.lnk`



Target attributes	A
Target file size	363104
Show Window	SW_NORMAL
Target created	Wednesday, March 6, 2024 21:46:17 -5
Last written	Wednesday, March 6, 2024 21:46:17 -5
Last accessed	Wednesday, March 6, 2024 21:46:17 -5
ID List	Desktop\F:\agency_admin_guide_2004.pdf C=03/07/2024 02:46:18 Size=363104
Network share name	\\FIRE-DC01\fire drive

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17 - Examination Questions

Question 17: What terms did user gmontag search on Google in the Chrome browser, March 9, 2024?

Manufacturer's bulk chemicals

Response:

WebCode Test	Response
28NKRK-5561	bulk Chemicals
2BXEJB-5561	bulk chemicals
2EUC34-5562	Bulk Chemicals
2UJN7X-5562	bulk chemicals
2XN36N-5561	bulk chemicals
36GUPN-5561	bulk chemicals
3CH2GJ-5562	[Participant did not return results for this question.]
3DBUC3-5561	bulk chemicals
3K9LKW-5561	bulk chemicals
3LM236-5561	Bulk chemicals
483YXK-5561	bulk chemicals
49DVEJ-5561	bulk chemicals
4K6LX2-5561	"bulk chemicals"
4L6CCW-5562	bulk chemicals
4P6N9W-5561	acetone+VS+isopropyl+alcohol
4THJUL-5562	[Participant did not return results for this question.]
4XXRHK-5561	bulk chemicals
4Z77PR-5561	bulk chemicals
6KNFKX-5561	bulk chemicals
6RLGDW-5561	bulk chemicals

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17 - Examination Questions	
WebCode Test	Response
78YYBQ-5561	bulk chemicals
7M6APW-5561	"bulk chemicals"
7WAG6W-5561	"thermite recipe", "acetone", "acetone vs isopropyl alcohol"
7WV3RK-5561	bulk chemicals
8ED4K3-5562	bulk chemicals
8LRYCP-5561	Bulk chemicals
8P8Q2X-5561	Bulk Chemicals
8RFV4L-5561	bulk chemicals
8W78WW-5562	bulk chemicals
98N78Y-5561	bulk chemicals
9J6THK-5561	Bulk Chemicals
9QMRX6-5561	bulk chemicals
9XFKVP-5562	Bulk chemicals
AN93XR-5561	bulk chemicals
AXDBED-5562	bulk chemicals
AXFVBT-5561	Bulk chemicals
B2ACZR-5562	Bulk Chemicals
BA4FBG-5561	bulk chemicals
BPGNBK-5562	bulk chemicals
BVMG7F-5561	bulk chemicals
BXTTYP-5561	bulk chemicals
CCXUMK-5561	bulk chemicals

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17 - Examination Questions	
WebCode Test	Response
CPQ4TQ-5561	bulk chemicals
D3A9ER-5561	"bulk chemicals"
D3MR2K-5561	bulk chemicals
D7C7PK-5562	bulk chemicals
D8QG3R-5561	bulk chemicals
DCKG7E-5561	bulk chemicals
DKUYDR-5561	bulk chemicals
DKVPRL-5562	bulk chemicals
DPA82Q-5561	bulk chemicals
DTN8XH-5562	bulk chemicals
DXKMTK-5561	bulk chemicals
EJD6CG-5561	bulk chemicals
EJK3WT-5561	bulk chemicals
EMTM9G-5561	bulk chemicals
F3TPTL-5561	bulk chemicals
F7NG2H-5561	bulk chemicals
FG6CVN-5561	bulk chemicals
FT8J39-5561	bulk chemicals
G6U6KA-5561	bulk chemicals
G9BD99-5561	bulk chemicals
G9PQLK-5561	bulk chemicals
GALGEK-5562	bulk chemicals

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17 - Examination Questions	
WebCode Test	Response
GMPPAG-5561	bulk chemicals
H3X34J-5561	bulk chemicals
HAWCD-5562	bulk chemicals
HFM3VL-5562	[Participant did not return results for this question.]
HGE2AK-5561	"bulk" + "chemicals"
HMQYPK-5561	bulk chemicals
HTB6DE-5562	bulk chemicals
HVJ3Y9-5561	Bulk chemicals
HYHLVF-5561	Bulk chemicals
J3FCTE-5561	bulk chemicals
J49DM9-5561	bulk chemicals
JFURCD-5561	bulk chemicals
JPAH22-5562	bulk chemicals
JXAZDE-5561	bulk chemicals
JXHV GK-5561	bulk chemicals
K3WXT8-5562	bulk chemicals
KA94ED-5562	bulk chemicals
KCQD3T-5561	bulk chemicals
KMHPR4-5561	bulk chemicals
LBJ6ZC-5562	bulk chemicals
LMDLPD-5561	bulk chemicals
LRM3Y2-5562	bulk Chemicals

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17 - Examination Questions	
WebCode Test	Response
LWKE3D-5561	bulk chemicals
MCQ8YF-5561	bulk chemicals
MD8AY2-5561	bulk chemicals
MK6QJE-5561	bulk chemicals
MR47EE-5562	bulk chemicals
MV6A9L-5561	bulk chemicals
N9Q2B2-5562	bulk chemicals
NH83FA-5562	Bulk chemicals
NNQD78-5561	bulk chemicals
NPUPBF-5562	bulk chemicals
NQ7BB3-5561	Two instances of the term "bulk chemicals"
P3EHK8-5562	bulk chemicals
P3ER7C-5561	bulk + chemicals
P6NMZG-5561	bulk chemicals
PE6G4X-5561	Bulk chemicals
PYKJC4-5561	bulk chemicals
Q4ZTN7-5562	Bulk chemicals
Q73JRN-5561	Bulk Chemicals
RBARA4-5561	bulk chemicals
RE7DZL-5561	bulk chemicals
RUTBQ8-5561	bulk chemicals
RY7A78-5561	bulk chemicals

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17 - Examination Questions	
WebCode Test	Response
RZKKZ7-5562	bulk chemicals
T9UAE6-5561	bulk chemicals
TH2XG4-5562	Not in scope
TTGXLB-5561	bulk chemicals
U8973A-5561	bulk chemicals
UEQLM7-5561	bulk chemicals
UEWNPX-5561	bulk chemicals
UGNM4W-5561	bulk chemicals
ULHG2X-5561	bulk chemicals
UPTW39-5562	Bulk Chemicals
UUA6Q9-5561	bulk chemicals
UZQMYA-5562	bulk chemicals
V66XC6-5562	Bulk Chemicals
V82HUJ-5561	bulk chemicals
VXLE96-5561	acetone, thermite recipe, acetone vs isopropyl alcohol, bulk chemicals
VYTW7Z-5561	bulk chemicals
W447WA-5561	bulk chemicals
WB84Q8-5561	Bulk Chemicals
WBPY99-5561	bulk chemicals
WFVT36-5561	bulk chemicals
WH6VY2-5561	bulk chemicals
WL2PNP-5561	bulk chemicals

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17 - Examination Questions	
WebCode Test	Response
WL4AK7-5562	bulk chemicals
WQGWCP-5562	bulk chemicals
X2AZR3-5561	bulk chemicals
X3NFAB-5561	bulk chemicals
X62GKW-5561	bulk chemicals
X84MXA-5561	"bulk chemicals"
XDQM3P-5561	bulk chemicals
XDT8Y6-5562	bulk chemicals
XLP32A-5562	bulk chemicals
XQXJAX-5561	bulk chemicals
Y2PJCZ-5561	bulk chemicals
Y8WZT2-5561	bulk chemicals
YZK9WX-5561	bulk chemicals
Z4GR62-5562	bulk chemicals
Z4PAVK-5561	bulk chemicals
ZBUQRZ-5561	bulk chemicals
ZEU2MZ-5562	bulk chemicals
ZF7RW4-5561	Bulk Chemicals
ZN4C6R-5561	bulk chemicals
ZQ4URL-5562	bulk chemicals
ZU7QJ2-5561	bulk chemicals
ZWABN2-5562	bulk chemicals

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 17 - Examination Questions

Question 17: What terms did user gmontag search on Google in the Chrome browser, March 9, 2024?

Consensus Result:

bulk chemicals

Manufacturer's Response Explanation:

Chrome browser history for a user is stored in a SQLite database in C:\Users\

Manufacturer's Response Illustration:

X-ways parse of C:\Users\gmontag\AppData\Local\Google\Chrome\User Data\Default\History

Id	Time	Title	URL
1	03/09/2024 17:02:26.45	bulk chemicals - Google Search	https://www.google.com/search?q=bulk+chemicals&rlz=1C1CHBF_enUS1100&oq=bulk+chemicals&gs_lcrp=EgZjaHJvbWUyBggAEEUY
2	03/09/2024 17:02:27.3	bulk chemicals - Google	https://www.google.com/search?q=bulk+chemicals&rlz=1C1CHBF_enUS1100&oq=bulk

EnCase parse of C:\Users\gmontag\AppData\Local\Google\Chrome\User Data\Default\History

True Path	Record Last Accessed	URL
n\Users\gmontag\AppData\Local\Packages\DuckDuckGo.D...	03/09/24 05:01:51 PM	https://en.wikipedia.org/wiki/Acetone
n\Users\gmontag\AppData\Local\Google\Chrome\User Dat...	03/09/24 05:02:27 PM	https://www.google.com/search?q=bulk+chemicals&
n\Users\gmontag\AppData\Local\Google\Chrome\User Dat...	03/09/24 05:02:27 PM	https://www.google.com/search?q=bulk+chemicals&
n\Users\gmontag\AppData\Local\Google\Chrome\User Dat...	03/09/24 05:02:27 PM	https://www.google.com/search?q=bulk+chemicals&

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18 - Examination Questions

Question 18: For the email message containing the keyword "trychtichlorate", provide the sender's email address.

Manufacturer's ronaldbartel@fireman.net

Response:

WebCode Test	Response
28NKRK-5561	ronaldbartel@fireman.net
2BXEJB-5561	ronaldbartel@fireman.net
2EUC34-5562	ronaldbartel@fireman.net
2UJN7X-5562	ronaldbartel@fireman.net
2XN36N-5561	ronaldbartel@fireman.net
36GUPN-5561	ronaldbartel@fireman.net
3CH2GJ-5562	[Participant did not return results for this question.]
3DBUC3-5561	ronaldbartel@fireman.net
3K9LKW-5561	ronaldbartel@fireman.net
3LM236-5561	Ronald Bartel <ronaldbartel@fireman.net>
483YXK-5561	ronaldbartel@fireman.net
49DVEJ-5561	ronaldbartel@fireman.net
4K6LX2-5561	ronaldbartel@fireman.net
4L6CCW-5562	ronaldbartel@fireman.net
4P6N9W-5561	ronaldbartel@fireman.net
4THJUL-5562	[Participant did not return results for this question.]
4XXRHK-5561	ronaldbartel@fireman.net
4Z77PR-5561	ronaldbartel@fireman.net
6KNFKX-5561	ronaldbartel@fireman.net
6RLGDW-5561	Ronald Bartel <ronaldbartel@fireman.net>

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18 - Examination Questions	
WebCode Test	Response
78YYBQ-5561	ronaldbartel@fireman.net
7M6APW-5561	ronaldbartel@fireman.net
7WAG6W-5561	Ronaldbartel@fireman.net
7WV3RK-5561	ronaldbartel@fireman.net
8ED4K3-5562	ronaldbartel@fireman.net
8LRYCP-5561	Ronaldbartel@fireman.net
8P8Q2X-5561	Ronald Bartel <ronaldbartel@fireman.net>
8RFV4L-5561	ronaldbartel@fireman.net
8W78WW-5562	ronaldbartel@fireman.net
98N78Y-5561	ronaldbartel@fireman.net
9J6THK-5561	ronaldbartel@fireman.net
9QMRX6-5561	ronaldbartel@fireman.net
9XFKVP-5562	Ronald Bartel ronaldbartel@fireman.net
AN93XR-5561	ronaldbartel@fireman.net
AXDBED-5562	ronaldbartel@fireman.net
AXFVBT-5561	ronaldbartel@fireman.net
B2ACZR-5562	ronaldbartel@fireman.net
BA4FBG-5561	ronaldbartel@fireman.net
BPGNBK-5562	ronaldbartel@fireman.net
BVMG7F-5561	ronaldbartel@fireman.net
BXTTTP-5561	ronaldbartel@fireman.net
CCXUMK-5561	ronaldbartel@fireman.net

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18 - Examination Questions	
WebCode Test	Response
CPQ4TQ-5561	ronaldbartel@fireman.net
D3A9ER-5561	ronaldbartel@fireman.net
D3MR2K-5561	ronaldbartel@fireman.net
D7C7PK-5562	Ronald Bartel" <ronaldbartel@fireman.net
D8QG3R-5561	ronaldbartel@fireman.net
DCKG7E-5561	ronaldbartel@fireman.net
DKUYDR-5561	ronaldbartel@fireman.net
DKVPRL-5562	ronaldbartel@fireman.net
DPA82Q-5561	Ronald Bartel <ronaldbartel@fireman.net>
DTN8XH-5562	ronaldbartel@fireman.net
DXKMTK-5561	ronaldbartel@fireman.net
EJD6CG-5561	ronaldbartel@fireman.net
EJK3WT-5561	ronaldbartel@fireman.net
EMTM9G-5561	ronaldbartel@fireman.net
F3TPTL-5561	ronaldbartel@fireman.net
F7NG2H-5561	ronaldbartel@fireman.net
FG6CVN-5561	ronaldbartel@fireman.net
FT8J39-5561	ronaldbartel@fireman.net
G6U6KA-5561	ronaldbartel@fireman.net
G9BD99-5561	ronaldbartel@fireman.net
G9PQLK-5561	"Ronald Bartel" <ronaldbartel@fireman.net>
GALGEK-5562	ronaldbartel@fireman.net

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18 - Examination Questions	
WebCode Test	Response
GMPPAG-5561	ronaldbartel@fireman.net
H3X34J-5561	ronaldbartel@fireman.net
HAWCD-5562	ronaldbartel@fireman.net
HFM3VL-5562	[Participant did not return results for this question.]
HGE2AK-5561	ronaldbartel@fireman.net
HMQYPK-5561	ronaldbartel@fireman.net
HTB6DE-5562	ronaldbartel@fireman.net
HVJ3Y9-5561	ronaldbartel@fireman.net
HYHLVF-5561	ronaldbartel@fireman.net
J3FCTE-5561	Ronald Bortel ronaldbartel@firwman.net is called trychtichlorate
J49DM9-5561	ronaldbartel@fireman.net
JFURCD-5561	ronaldbartel@fireman.net
JPAH22-5562	ronaldbartel@fireman.net
JXAZDE-5561	guy.montag@winchestertonfieldville.org
JXHV GK-5561	ronaldbartel@fireman.net
K3WXT8-5562	ronaldbartel@fireman.net
KA94ED-5562	ronaldbartel@fireman.net
KCQD3T-5561	ronaldbartel@fireman.net
KMHPR4-5561	ronaldbartel@fireman.net
LBJ6ZC-5562	ronaldbartel@fireman.net
LMDLPD-5561	ronaldbartel@fireman.net
LRM3Y2-5562	ronaldbartel@fireman.net

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18 - Examination Questions	
WebCode Test	Response
LWKE3D-5561	ronaldbartel@fireman.net
MCQ8YF-5561	ronaldbartel@fireman.net
MD8AY2-5561	ronaldbartel@fireman.net
MK6QJE-5561	ronaldbartel@fireman.net
MR47EE-5562	ronaldbartel@fireman.net
MV6A9L-5561	ronaldbartel@fireman.net ???
N9Q2B2-5562	ronaldbartel@fireman.net
NH83FA-5562	ronaldbartel@fireman.net
NNQD78-5561	ronaldbartel@fireman.net
NPUPBF-5562	Ronald Bartel <ronaldbartel@fireman.net>
NQ7BB3-5561	ronaldbartel@fireman.net
P3EHK8-5562	ronaldbartel@fireman.net
P3ER7C-5561	ronaldbartel@fireman.net
P6NMZG-5561	UNABLE TO IDENTIFY EMAIL WITH THIS DATA
PE6G4X-5561	ronaldbartel@fireman.net
PYKJC4-5561	gmontag@winchestertonfieldville.org
Q4ZTN7-5562	Ronaldbartel@fireman.net
Q73JRN-5561	Ronald Bartel <RonalsBartel@fireman.net>
RBARA4-5561	ronaldbartel@fireman.net
RE7DZL-5561	ronaldbartel@fireman.net
RUTBQ8-5561	ronaldbartel@fireman.net
RY7A78-5561	ronaldbartel@fireman.net

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18 - Examination Questions	
WebCode Test	Response
RZKKZ7-5562	ronaldbartel@fireman.net
T9UAE6-5561	ronaldbartel@fireman.net
TH2XG4-5562	Not in scope
TTGXLB-5561	ronaldbartel@fireman.net
U8973A-5561	ronaldbartel@fireman.net
UEQLM7-5561	ronaldbartel@fireman.net
UEWNPX-5561	ronaldbartel@fireman.net
UGNM4W-5561	ronaldbartel@fireman.net
ULHG2X-5561	ronaldbartel@fireman.net
UPTW39-5562	guys.montage@winchestertonfieldville.org
UUA6Q9-5561	ronaldbartel@fireman.net
UZQMYA-5562	ronaldbartel@fireman.net
V66XC6-5562	ronaldbartel@fireman.net
V82HUJ-5561	ronaldbartel@fireman.net
VXLE96-5561	gmontag@winchestertonfieldville.org
VYTW7Z-5561	ronaldbartel@fireman.net
W447WA-5561	ronaldbartel@fireman.net
WB84Q8-5561	ronaldbartel@fireman.net
WBPY99-5561	ronaldbartel@fireman.net
WFVT36-5561	ronaldbartel@fireman.net
WH6VY2-5561	ronaldbartel@fireman.net
WL2PNP-5561	ronaldbartel@fireman.net

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 18 - Examination Questions	
WebCode Test	Response
WL4AK7-5562	ronaldbartel@fireman.net
WQGWCP-5562	ronaldbartel@fireman.net
X2AZR3-5561	ronaldbartel@fireman.net
X3NFAB-5561	ronaldbartel@fireman.net
X62GKW-5561	ronaldbartel@fireman.net
X84MXA-5561	ronaldbartel@fireman.net
XDQM3P-5561	ronaldbartel@fireman.net
XDT8Y6-5562	ronaldbartel@fireman.net
XLP32A-5562	Ronald Bartel <ronaldbartel@fireman.net>
XQXJAX-5561	ronaldbartel@fireman.net
Y2PJCZ-5561	ronaldbartel@fireman.net
Y8WZT2-5561	ronaldbartel@fireman.net
YZK9WX-5561	ronaldbartel@fireman.net
Z4GR62-5562	ronaldbartel@fireman.net
Z4PAVK-5561	ronaldbartel@fireman.net
ZBUQRZ-5561	ronaldbartel@fireman.net
ZEU2MZ-5562	ronaldbartel@fireman.net
ZF7RW4-5561	guys.montage@winchesters.org
ZN4C6R-5561	ronaldbartel@fireman.net
ZQ4URL-5562	ronaldbartel@fireman.net
ZU7QJ2-5561	ronaldbartel@fireman.net
ZWABN2-5562	ronaldbartel@fireman.net

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 19 - Examination Questions

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

Manufacturer's bleve

Response:

WebCode Test	Response
28NKRK-5561	bleve
2BXEJB-5561	bleve
2EUC34-5562	bleve
2UJN7X-5562	bleve
2XN36N-5561	bleve
36GUPN-5561	bleve
3CH2GJ-5562	[Participant did not return results for this question.]
3DBUC3-5561	bleve
3K9LKW-5561	bleve
3LM236-5561	Bleve
483YXK-5561	bleve
49DVEJ-5561	bleve
4K6LX2-5561	bleve
4L6CCW-5562	bleve
4P6N9W-5561	bleve
4THJUL-5562	[Participant did not return results for this question.]
4XXRHK-5561	bleve
4Z77PR-5561	bleve
6KNFKX-5561	bleve
6RLGDW-5561	bleve

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 19 - Examination Questions	
WebCode Test	Response
78YYBQ-5561	bleve
7M6APW-5561	bleve
7WAG6W-5561	Bleve
7WV3RK-5561	bleve
8ED4K3-5562	bleve
8LRYCP-5561	bleve
8P8Q2X-5561	Bleve
8RFV4L-5561	bleve
8W78WW-5562	bleve
98N78Y-5561	bleve
9J6THK-5561	bleve
9QMRX6-5561	bleve
9XFKVP-5562	bleve
AN93XR-5561	bleve
AXDBED-5562	bleve
AXFVBT-5561	bleve 20
B2ACZR-5562	Searched term: Bleve – User: mohalloran
BA4FBG-5561	bleve
BPGNBK-5562	bleve
BVMG7F-5561	bleve
BXTTYP-5561	bleve
CCXUMK-5561	bleve

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 19 - Examination Questions	
WebCode Test	Response
CPQ4TQ-5561	bleve
D3A9ER-5561	bleve
D3MR2K-5561	bleve
D7C7PK-5562	bleve
D8QG3R-5561	bleve
DCKG7E-5561	bleve
DKUYDR-5561	bleve
DKVPRL-5562	bleve
DPA82Q-5561	bleve
DTN8XH-5562	bleve
DXKMTK-5561	bleve
EJD6CG-5561	bleve
EJK3WT-5561	Bleve
EMTM9G-5561	bleve
F3TPTL-5561	bleve
F7NG2H-5561	bleve
FG6CVN-5561	bleve
FT8J39-5561	bleve
G6U6KA-5561	bleve
G9BD99-5561	bleve
G9PQLK-5561	bleve
GALGEK-5562	bleve

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 19 - Examination Questions	
WebCode Test	Response
GMPPAG-5561	bleve
H3X34J-5561	bleve
HAWCD-5562	bleve
HFM3VL-5562	[Participant did not return results for this question.]
HGE2AK-5561	bleve
HMQYPK-5561	bleve
HTB6DE-5562	bleve
HVJ3Y9-5561	bleve
HYHLVF-5561	bleve
J3FCTE-5561	bleve
J49DM9-5561	bleve
JFURCD-5561	bleve
JPAH22-5562	bleve
JXAZDE-5561	bleve
JXHV GK-5561	bleve
K3WXT8-5562	bleve
KA94ED-5562	bleve
KCQD3T-5561	bleve
KMHPR4-5561	bleve
LBJ6ZC-5562	bleve
LMDLPD-5561	Search on Youtube = bleve. User = mohalloran
LRM3Y2-5562	bleve

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 19 - Examination Questions	
WebCode Test	Response
LWKE3D-5561	bleve
MCQ8YF-5561	bleve
MD8AY2-5561	bleve
MK6QJE-5561	bleve
MR47EE-5562	bleve
MV6A9L-5561	bleve
N9Q2B2-5562	bleve
NH83FA-5562	bleve
NNQD78-5561	bleve
NPUPBF-5562	bleve
NQ7BB3-5561	"bleve"
P3EHK8-5562	bleve
P3ER7C-5561	bleve
P6NMZG-5561	bleve
PE6G4X-5561	bleve
PYKJC4-5561	bleve
Q4ZTN7-5562	bleve
Q73JRN-5561	bleve
RBARA4-5561	bleve
RE7DZL-5561	bleve
RUTBQ8-5561	bleve
RY7A78-5561	bleve

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 19 - Examination Questions	
WebCode Test	Response
RZKKZ7-5562	bleve
T9UAE6-5561	bleve
TH2XG4-5562	Not in scope
TTGXLB-5561	bleve
U8973A-5561	bleve
UEQLM7-5561	thermite recipe
UEWNPX-5561	bleve
UGNM4W-5561	bleve
ULHG2X-5561	bleve
UPTW39-5562	bleve
UUA6Q9-5561	bleve
UZQMYA-5562	bleve
V66XC6-5562	bleve and the user was mohalloran
V82HUJ-5561	bleve
VXLE96-5561	bleve
VYTW7Z-5561	bleve
W447WA-5561	bleve
WB84Q8-5561	bleve
WBPY99-5561	bleve
WFVT36-5561	Bleve
WH6VY2-5561	bleve
WL2PNP-5561	bleve

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 19 - Examination Questions	
WebCode Test	Response
WL4AK7-5562	bleve
WQGWCP-5562	bleve
X2AZR3-5561	bleve
X3NFAB-5561	bleve
X62GKW-5561	bleve (User: mohalloran)
X84MXA-5561	bleve
XDQM3P-5561	bleve
XDT8Y6-5562	bleve
XLP32A-5562	bleve
XQXJAX-5561	bleve
Y2PJCZ-5561	bleve
Y8WZT2-5561	bleve
YZK9WX-5561	bleve
Z4GR62-5562	bleve
Z4PAVK-5561	fire impact on tanks
ZBUQRZ-5561	bleve
ZEU2MZ-5562	bleve
ZF7RW4-5561	bleve
ZN4C6R-5561	bleve
ZQ4URL-5562	bleve
ZU7QJ2-5561	bleve
ZWABN2-5562	bleve

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 19 - Examination Questions

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

Consensus Result:

bleve

Manufacturer's Response Explanation:

Timeline analysis of internet history activity will show YouTube visits at the specified date and time, including the search for the term "bleve."

Manufacturer's Response Illustration:

Autopsy view of internet history records

Web History

Source Name	S	C	O	URL	▲ Date Accessed
History		0		https://www.youtube.com/watch?v=CoFVEsSGVGM	2024-03-14 01:43:53 UTC
History		0		https://www.youtube.com/results?search_query=bleve	2024-03-14 01:45:01 UTC
History		0		https://www.youtube.com/results?search_query=bleve	2024-03-14 01:45:01 UTC

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context

Result: 3 of 27 Result ← →

Visit Details

Title: bleve - YouTube
 Username: Default
 Date Accessed: 2024-03-14 01:45:01 UTC
 Domain: youtube.com
 URL: https://www.youtube.com/results?search_query=bleve

EnCase view of internet history records

Record Last Accessed	Url Name
03/13/24 09:45:01 PM (-4:00 ...	https://www.youtube.com/results?search_query=bleve
03/13/24 09:45:01 PM (-4:00 ...	https://www.youtube.com/results?search_query=bleve
03/13/24 09:45:01 PM (-4:00 ...	https://www.youtube.com/results?search_query=bleve
03/13/24 09:45:01 PM (-4:00 ...	https://www.youtube.com/results?search_query=bleve

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20 - Examination Questions

Question 20: What phone number in the format (NNN)NNN-NNNN appears in the file with SHA1 hash 961FF684E4097CE52C475FB7F249D01EE9DC2BF2?

Manufacturer's (571)434-1925

Response:

WebCode Test	Response
28NKRK-5561	(571)434-1925
2BXEJB-5561	(571)434-1925
2EUC34-5562	(571) 434-1925
2UJN7X-5562	(571)434-1925
2XN36N-5561	(571)434-1925
36GUPN-5561	(571)434-1925
3CH2GJ-5562	[Participant did not return results for this question.]
3DBUC3-5561	(571)434-1925
3K9LKW-5561	(571) 434-1925
3LM236-5561	(571)434-1925
483YXK-5561	(571)434-1925
49DVEJ-5561	(571)434-1925
4K6LX2-5561	(571)434-1925
4L6CCW-5562	(571)434-1925
4P6N9W-5561	(571)434-1925
4THJUL-5562	[Participant did not return results for this question.]
4XXRHK-5561	(571)434-1925
4Z77PR-5561	(571)434-1925
6KNFKX-5561	(571)434-1925

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20 - Examination Questions	
WebCode Test	Response
6RLGDW-5561	(571)434-1925
78YYBQ-5561	(571)434-1925
7M6APW-5561	(571)434-1925
7WAG6W-5561	(571)434-1925
7WV3RK-5561	(571)434-1925
8ED4K3-5562	(571)434-1925
8LRYCP-5561	(571)434-1925
8P8Q2X-5561	(571)434-1925
8RFV4L-5561	(571)434-1925
8W78WW-5562	(571)434-1925
98N78Y-5561	(571)434-1925
9J6THK-5561	(571)434-1925
9QMRX6-5561	(571)434-1925
9XFKVP-5562	(571)434-1925
AN93XR-5561	(571)434-1925
AXDBED-5562	(571)434-1925
AXFVBT-5561	The file with the above listed hash is numbers.txt the phone number is (573)434-1925
B2ACZR-5562	(571) 434-1925
BA4FBG-5561	(571)434-1925
BPGNBK-5562	(571)434-1925
BVMG7F-5561	(571)434-1925

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20 - Examination Questions	
WebCode Test	Response
BXTTXP-5561	(571)434-1925
CCXUMK-5561	(571)434-1925
CPQ4TQ-5561	(571)434-1925
D3A9ER-5561	(571)434-1925
D3MR2K-5561	(571)434-1925
D7C7PK-5562	Regular expression: \\(\\d{3}\\)\\d{3}-\\d{4} phone number: (571)434-1925
D8QG3R-5561	(571)434-1925
DCKG7E-5561	(571)434-1925
DKUYDR-5561	(571)434-1925
DKVPRL-5562	(571)434-1925
DPA82Q-5561	(571)434-1925
DTN8XH-5562	(571)434-1925
DXKMTK-5561	(571)-434-1925
EJD6CG-5561	(571)434-1925
EJK3WT-5561	(571)434-1925
EMTM9G-5561	(571)434-1925
F3TPTL-5561	(571)434-1925
F7NG2H-5561	(571)434-1925
FG6CVN-5561	(571) 434-1925
FT8J39-5561	(571)434-1925
G6U6KA-5561	(571)434-1925

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20 - Examination Questions	
WebCode Test	Response
G9BD99-5561	(571)434-1925
G9PQLK-5561	(571)434-1925
GALGEK-5562	(571)434-1925
GMPPAG-5561	(571)434-1925
H3X34J-5561	(571)434-1925
HAVVCD-5562	(571)434-1925
HFM3VL-5562	[Participant did not return results for this question.]
HGE2AK-5561	(571)434-1925
HMQYPK-5561	(571)434-1925
HTB6DE-5562	(571)434-1925
HVJ3Y9-5561	(571)434-1925
HYHLVF-5561	(571)-434-1925
J3FCTE-5561	(571)434-1925
J49DM9-5561	(571)434-1925
JFURCD-5561	(571)434-1925
JPAH22-5562	(571)434-1925
JXAZDE-5561	725-770-9122
JXHV GK-5561	(571)434-1925
K3WXT8-5562	(571)434-1925
KA94ED-5562	(571)434-1925
KCQD3T-5561	(571)434-1925

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20 - Examination Questions	
WebCode Test	Response
KMHPR4-5561	(571)434-1925
LBJ6ZC-5562	(571)434-1925
LMDLPD-5561	(571)434-1925
LRM3Y2-5562	(571)434-1925
LWKE3D-5561	(571)434-1925
MCQ8YF-5561	(571)434-1925
MD8AY2-5561	(571)434-1925
MK6QJE-5561	(571)434-1925
MR47EE-5562	(571)434-1925
MV6A9L-5561	(571)434-1925
N9Q2B2-5562	(571)434-1925
NH83FA-5562	(571) 434-1925
NNQD78-5561	(571)434-1925
NPUPBF-5562	(571)434-1925
NQ7BB3-5561	Phone number: (571)434-1925 File is "numbers.txt"
P3EHK8-5562	(571)434-1925
P3ER7C-5561	(571)434-1925
P6NMZG-5561	(571)434-1925
PE6G4X-5561	(571)434-1925
PYKJC4-5561	(571)434-1925
Q4ZTN7-5562	(571)434-1925

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20 - Examination Questions	
WebCode Test	Response
Q73JRN-5561	(571)434-1925
RBARA4-5561	(571)434-1925
RE7DZL-5561	(571)434-1925
RUTBQ8-5561	(571)434-1925
RY7A78-5561	(571)434-1925
RZKKZ7-5562	(571)434-1925
T9UAE6-5561	(571)434-1925
TH2XG4-5562	(571)434-1925
TTGXLB-5561	(571)434-1925
U8973A-5561	(571)434-1925
UEQLM7-5561	(571)434-1925
UEWNPX-5561	(571)434-1925
UGNM4W-5561	(571)434-1925
ULHG2X-5561	(571)434-1925
UPTW39-5562	(571) 434-1925
UUA6Q9-5561	(571)434-1925
UZQMYA-5562	(571)434-1925
V66XC6-5562	(571)434-1925
V82HUJ-5561	(571)434-1925
VXLE96-5561	(571)434-1925
VYTW7Z-5561	[Participant did not return results for this question.]

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20 - Examination Questions	
WebCode Test	Response
W447WA-5561	(571)434-1925
WB84Q8-5561	(571) 434-1925
WBPY99-5561	(571)434-1925
WFVT36-5561	(571)434-1925
WH6VY2-5561	(571)434-1925
WL2PNP-5561	(571)434-1925
WL4AK7-5562	(571)434-1925
WQGWCP-5562	(571)434-1925
X2AZR3-5561	(571)434-1925
X3NFAB-5561	(571)434-1925
X62GKW-5561	(571)434-1925
X84MXA-5561	(571)434-1925
XDQM3P-5561	(571)434-1925
XDT8Y6-5562	(571)434-1925
XLP32A-5562	(571)434-1925
XQXJAX-5561	(571)434-1925
Y2PJCZ-5561	(571)434-1925
Y8WZT2-5561	(571)434-1925
YZK9WX-5561	(571)434-1925
Z4GR62-5562	(571)434-1925
Z4PAVK-5561	(571)434-1925

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20 - Examination Questions	
WebCode Test	Response
ZBUQRZ-5561	(571)434-1925
ZEU2MZ-5562	(571)434-1925
ZF7RW4-5561	(571)434-1925
ZN4C6R-5561	(571)434-1925
ZQ4URL-5562	(571)434-1925
ZU7QJ2-5561	(571)434-1925
ZWABN2-5562	YES (571)434-1925

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 20 - Examination Questions

Question 20: What phone number in the format (NNN)NNN-NNNN appears in the file with SHA1 hash 961FF684E4097CE52C475FB7F249D01EE9DC2BF2?

Consensus Result:

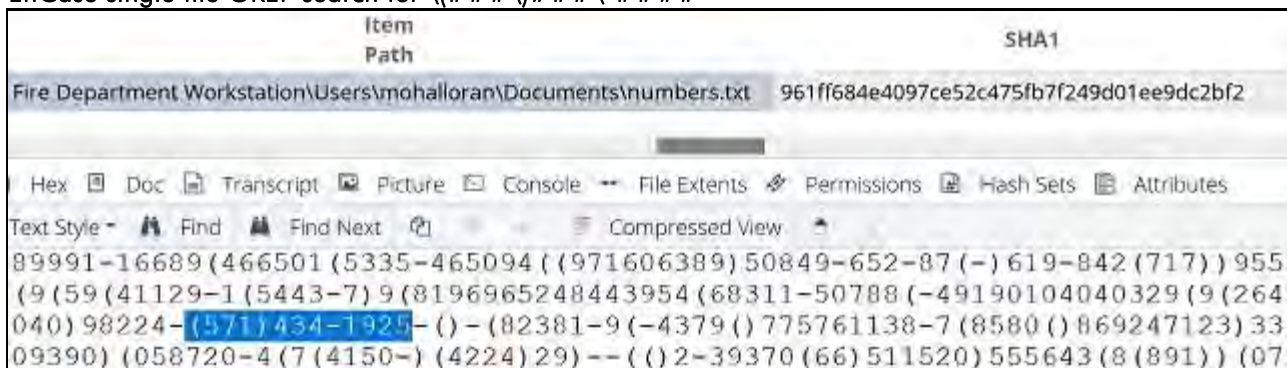
(571)434-1925

Manufacturer's Response Explanation:

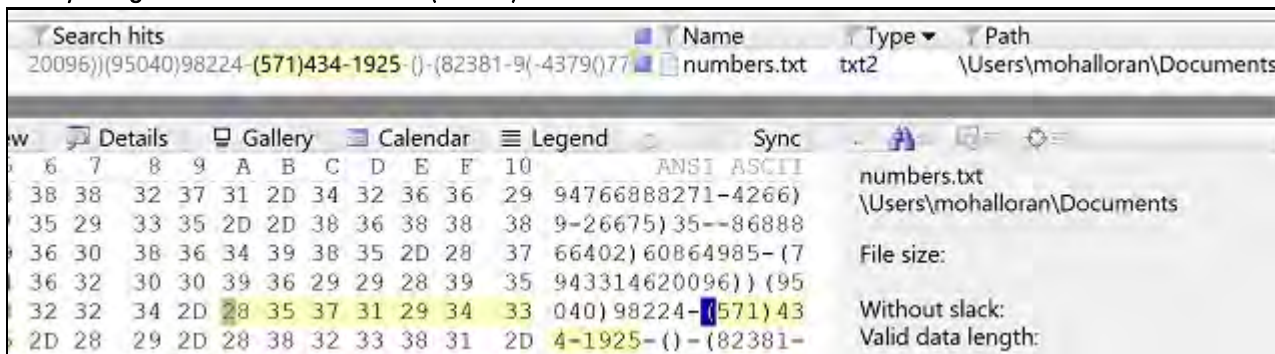
C:\Users\mohalloran\Documents\numbers.txt has the specified SHA1 hash. Searching the file with a simple regular expression such as `\(\d{3}\)\(\d{3}\)\(\d{3}\)` or `\(###\)###\-####` will locate the above phone number.

Manufacturer's Response Illustration:

EnCase single file GREP search for `\(###\)###\-####`



X-rays single file GREP search for `\(###\)###\-####`



Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21 - Examination Questions

Question 21: What was the original (pre-deletion) path of `crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf`? Provide both the path and filename.

Manufacturer's Response: C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf

Response: pdf

WebCode Test	Response
28NKRK-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
2BXEJB-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b97.pdf
2EUC34-5562	C:/Users/kshea/Documents/crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
2UJN7X-5562	\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf \$ION3HTM.pdf and \$RON3HTM.pdf
2XN36N-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
36GUPN-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
3CH2GJ-5562	[Participant did not return results for this question.]
3DBUC3-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
3K9LKW-5561	\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
3LM236-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
483YXK-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
49DVEJ-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
4K6LX2-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
4L6CCW-5562	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
4P6N9W-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
4THJUL-5562	[Participant did not return results for this question.]
4XXRHK-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
4Z77PR-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
6KNFKX-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21 - Examination Questions	
WebCode Test	Response
6RLGDW-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
78YYBQ-5561	\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
7M6APW-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
7WAG6W-5561	c:\users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
7WV3RK-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
8ED4K3-5562	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
8LRYCP-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf File Name: Crispy Ranch Pork Chops 5f771bea76d6a959777b2c98-5335b973
8P8Q2X-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
8RFV4L-5561	C:\Users\kshea\Documents\Crispy-ranch-pork-chops-5f771bea76d6a95977762c98-5335b973.pdf
8W78WW-5562	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
98N78Y-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
9J6THK-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
9QMRX6-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
9XFKVP-5562	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
AN93XR-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
AXDBED-5562	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
AXFVBT-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
B2ACZR-5562	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
BA4FBG-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
BPGNBK-5562	\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
BVMG7F-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21 - Examination Questions	
WebCode Test	Response
BXTTXP-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
CCXUMK-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
CPQ4TQ-5561	\Users\kshea\Documents\crispy-ranch-pork-chops-5F771BEA76D6A959777B2C98-5335B973.pdf
D3A9ER-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
D3MR2K-5561	Path: C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf, Filename: crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
D7C7PK-5562	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
D8QG3R-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
DCKG7E-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
DKUYDR-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
DKVPR-5562	/Users/kshea/Documents/crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
DPA82Q-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
DTN8XH-5562	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
DXKMTK-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
EJD6CG-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
EJK3WT-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
EMTM9G-5561	Users\kshea\documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf / File name: crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
F3TPTL-5561	Original Path - C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf Original Filename - crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
F7NG2H-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf, crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
FG6CVN-5561	Filename: spy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf Path: C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
FT8J39-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
G6U6KA-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21 - Examination Questions	
WebCode Test	Response
G9BD99-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
G9PQLK-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
GALGEK-5562	\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
GMPPAG-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
H3X34J-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
HAVCD-5562	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
HFM3VL-5562	[Participant did not return results for this question.]
HGE2AK-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
HMQYPK-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
HTB6DE-5562	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
HVJ3Y9-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
HYHLVF-5561	crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
J3FCTE-5561	Path:\Users\kshea\Documents\crispy-ranch-pork-chops- 5f771bea76d6a959777b2c98-5335b973.pdf, Filename: \$I0N3HTM.pdf
J49DM9-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
JFURCD-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
JPAH22-5562	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
JXAZDE-5561	c:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
JXHVGK-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
K3WXT8-5562	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
KA94ED-5562	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
KCQD3T-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21 - Examination Questions	
WebCode Test	Response
KMHPR4-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
LBJ6ZC-5562	C:\Users\kshea\Documents\ , crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
LMDLPD-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
LRM3Y2-5562	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
LWKE3D-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
MCQ8YF-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
MD8AY2-5561	\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf; crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
MK6QJE-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
MR47EE-5562	C:\Users\kshea\Documentos\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
MV6A9L-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
N9Q2B2-5562	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
NH83FA-5562	\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
NNQD78-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
NPUPBF-5562	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
NQ7BB3-5561	File: crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf Path: C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
P3EHK8-5562	\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
P3ER7C-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b93.pdf
P6NMZG-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
PE6G4X-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf; crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
PYKJC4-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
Q4ZTN7-5562	Path: A) C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pd File Name: Crispy Ranch Pork Chops 5f771bea76d6a959777b2c98-5335b973

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21 - Examination Questions	
WebCode Test	Response
Q73JRN-5561	c:\users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b97.pdf
RBARA4-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
RE7DZL-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
RUTBQ8-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
RY7A78-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
RZKKZ7-5562	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
T9UAE6-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
TH2XG4-5562	Not in scope
TTGXLB-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c985335b973.pdf
U8973A-5561	FireDepartametWorkstation/Users/KSHEA/Documents/crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
UEQLM7-5561	C:\Users\kshea\Documents\
UEWNPX-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
UGNM4W-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
ULHG2X-5561	\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
UPTW39-5562	C:/Users/kshea/Documents/crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
UUA6Q9-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
UZQMYA-5562	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
V66XC6-5562	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
V82HUJ-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
VXLE96-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
VYTW7Z-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21 - Examination Questions	
WebCode Test	Response
W447WA-5561	root\users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
WB84Q8-5561	C:/Users/kshea/Documents/crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
WBPY99-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
WFVT36-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
WH6VY2-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
WL2PNP-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
WL4AK7-5562	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
WQGWCP-5562	Path: Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf, Filename: crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
X2AZR3-5561	\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
X3NFAB-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
X62GKW-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
X84MXA-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
XDQM3P-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
XDT8Y6-5562	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
XLP32A-5562	\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
XQXJAX-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
Y2PJCZ-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
Y8WZT2-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
YZK9WX-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
Z4GR62-5562	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
Z4PAVK-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21 - Examination Questions	
WebCode Test	Response
ZBUQRZ-5561	/img_Fire_20Department_20Workstation-001.e01/Users/kshea/Documents/crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
ZEU2MZ-5562	crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
ZF7RW4-5561	C:/Users/kshea/Documents/crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
ZN4C6R-5561	\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
ZQ4URL-5562	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
ZU7QJ2-5561	C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf
ZWABN2-5562	\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 21 - Examination Questions

Question 21: What was the original (pre-deletion) path of `crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf`? Provide both the path and filename.

Consensus Result:

C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf and variations representing similar information or easily determined to be a typographical error.

Manufacturer's Response Explanation:

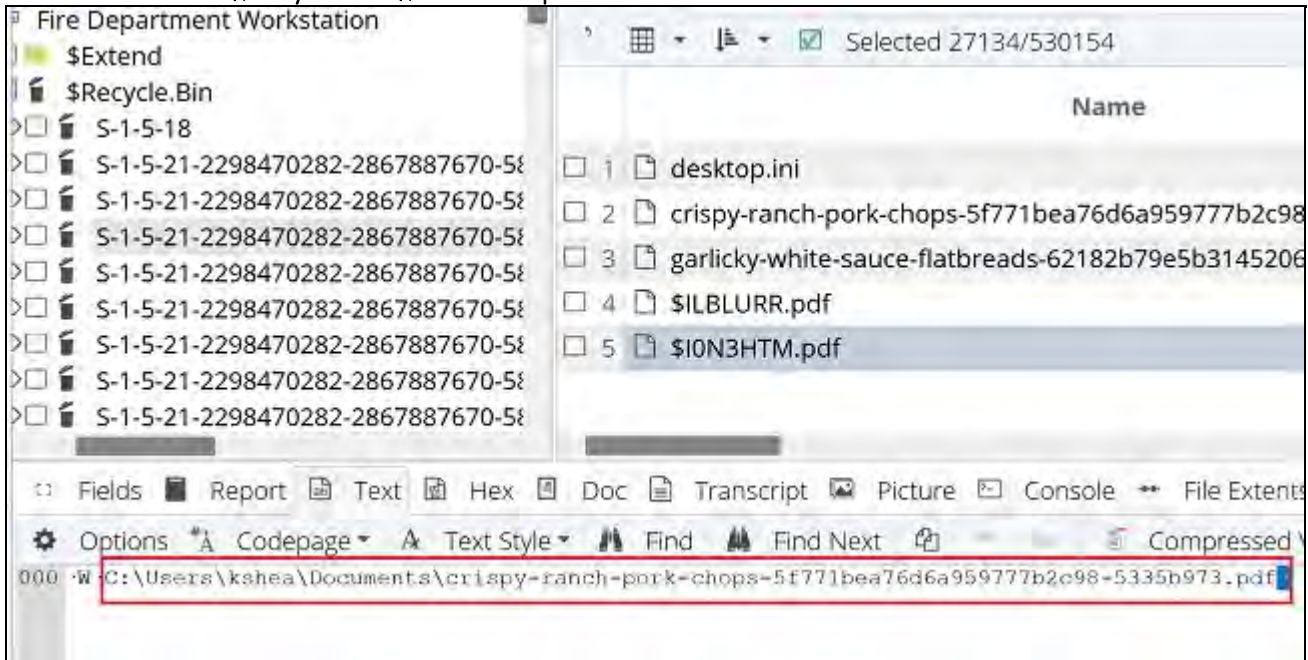
Every user on a Windows system has a folder in C:\\$Recycle.Bin named with their Security Identifier, or SID. Within that folder are a pair of files for each recycled file. One, beginning with \$I, which contains the metadata for the recycled file including its pre-deletion path and name, and another, beginning with \$R, containing the file's content. `crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf` is currently in

C:\\$Recycle.Bin\S-1-5-21-2298470282-2867887670-580413564-1109\ \$RON3HTM.pdf. Its Recycle Bin companion \$I file, C:\\$Recycle.Bin\S-1-5-21-2298470282-2867887670-580413564-1109\ \$ION3HTM.pdf contains the original path

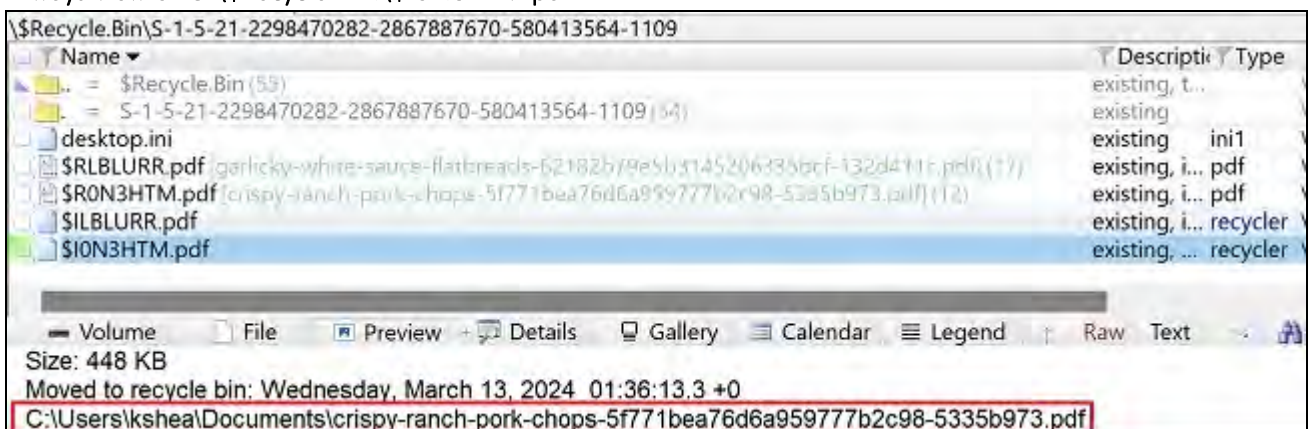
C:\Users\kshea\Documents\crispy-ranch-pork-chops-5f771bea76d6a959777b2c98-5335b973.pdf.

Manufacturer's Response Illustration:

EnCase view of C:\\$Recycle.BIN\\$ION3HTM.pdf



X-ways view of C:\\$Recycle.BIN\\$ION3HTM.pdf



Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22 - Examination Questions

Question 22: Describe the filetype and content of the file with created date March 9, 2024 21:56:33 UTC+0.

Manufacturer's FileType: mp4 file

Response: Content file description: A video of a person igniting a flammable gas in a large bottle. Dancing man at the end of the video (Rick Astley's music video or Rick-Rolled).

WebCode Test	Response
28NKRK-5561	Filetype: .MP4, Content file description: Video of volatile gas explosion
2BXEJB-5561	Filetype: MPEG-4 Video, Content file description: large glass bottle (whoosh bottle) is lit with a lighter, gas lights up, and then some music with a guy dancing
2EUC34-5562	Filetype: Video/MP4 , Content file description: volatile gas explosion
2UJN7X-5562	Filetype: .mp4, Content file description: An mp4 file called "volatile gas explosion.mp4" 14 seconds long showing a plastic bottle filled with fire for 9 seconds, followed by a video of Rick Astley Never Going to Give You Up from 9 seconds to the end of the video.
2XN36N-5561	Filetype: .mp4 Video File, Content file description: The content of the video depicted a flame in a bottle, which later transitions to the Rick Astley video for "Never Gonna Give You Up".
36GUPN-5561	Filetype: .mp4, Content file description: video of gas being lit and burned inside glass bottle, then rick rolled
3CH2GJ-5562	[Participant did not return results for this question.]
3DBUC3-5561	Filetype: mp4, Content file description: A video of a flammable gas being set on fire in a five gallon jug followed by a video of Rick Astley dancing in the music video never going to give you up
3K9LKW-5561	Filetype: MP4, Content file description: Someone lit a large glass bottle and a chain reaction happened within the bottle and then the video cuts to a music video of Rick Astley performing "Never Gonna Give You Up."
3LM236-5561	Filetype: MP4 video file, Content file description: a video file contains recording of volatile gas explosion
483YXK-5561	Filetype: Video (mp4), Content file description: explosion inside a glass jar followed by an excerpt of a music video
49DVEJ-5561	Filetype: mp4, Content file description: A man dances after gas is released from glass.
4K6LX2-5561	Filetype: Video (MP4, H.264 encoded), Content file description: Video depicting a flammable gas contained in a jar being ignited, leading into a Rickroll video clip.
4L6CCW-5562	Filetype: mp4 (video file), Content file description: video of someone putting a flame in a gaz in a bottle. RickRoll at the end
4P6N9W-5561	Filetype: MPEG 4.0 Video, Content file description: volatile gas explosion inside glass bottle
4THJUL-5562	[Participant did not return results for this question.]

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22 - Examination Questions	
WebCode Test	Response
4XXRHK-5561	Filetype: .mp4 video, Content file description: Video showing someone lighting gas in a bottle and then a male dancing.
4Z77PR-5561	Filetype: mp4, Content file description: Whoosh bottle demonstration rickroll
6KNFKX-5561	Filetype: MP4, Content file description: The content is a video of someone lighting a fire in a glass jar and then transitions into a Rick Astley music video
6RLGDW-5561	Filetype: MP4 video file, Content file description: Named "volatile gas explosion.mp4" of a flame inside a bottle and ending with a music soundtrack. Located in \Users\gmontag\Videos\
78YYBQ-5561	Filetype: .mp4, Content file description: volatile gas explosion.mp4 – A video of a lighter being used to put a flame inside a large glass bottle. The flame moved towards the bottom of the bottle and small explosions are heard. A male's voice is heard in the background. The video then switches to a male subject dancing and singing.
7M6APW-5561	Filetype: MPEG 4.0 Video titled "volatile gas explosion.mp4", Content file description: a volatile gas explosion inside of a five gallon glass tube that segways into a Rick Astley music video for "Never Gonna Give You Up."
7WAG6W-5561	Filetype: MP4 file type, file name is "Volatile Gas Explosion.mp4", Content file description: Video shows someone lighting a fire that goes into a flask and a red-headed singer/dancer
7WV3RK-5561	Filetype: .mp4, Content file description: Short video called volatile gas explosion in which a substance is lit on fire within a glass bottle and then the video cuts to Rick Astley's "never gonna give you up" song.
8ED4K3-5562	Filetype: mp4, Content file description: The first part of the video shows volatile gas in a bottle catching fire, and the latter part features a man dancing to an upbeat song.
8LRYCP-5561	Filetype: MPEG 4.0 Video, Content file description: It shows a video of a jug being lit up by a lighter then it cuts into a man dancing.
8P8Q2X-5561	Filetype: .mp4, Content file description: volatile gas explosion.mp4
8RFV4L-5561	Filetype: .mp4, Content file description: Video of a fire in a bottle followed by a guy dancing to never gonna give you up.
8W78WW-5562	Filetype: MP4 (Video file), Content file description: (volatile gas explosion.mp4) The video was about 14 seconds in duration which showed a bottle at the beginning of the video and a man dancing to music at the end of the video.
98N78Y-5561	Filetype: .mp4, Content file description: show a video of a man who puts fire in the bottle and ends with a song
9J6THK-5561	Filetype: .mp4, Content file description: A video showing volatile gas explosion with a music video.
9QMRX6-5561	Filetype: .mp4 (MP4 file format), Content file description: The chemical experiment of volatile gas in a bottle was processed, and then a part of a music video with a man dancing was played.
9XFKVP-5562	Filetype: File Name: volatile gas explosion.mp4 Filetype: .mp4, Content file description: The contents of a transparent bottle is lit on fire, it is then switched to Rich Astley

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22 - Examination Questions	
WebCode Test	Response
AN93XR-5561	Filetype: .mp4 video, Content file description: Volatile gas explosion within a glass jar edited with a Rick Astley music video at the end.
AXDBED-5562	Filetype: .mp4, Content file description: a science experiment turns into a Rick-roll.
AXFVBT-5561	Filetype: .mp4, Content file description: volatile gas explosion in a glass jar. Then I got Rick Rolled.
B2ACZR-5562	Filetype: MP4, Content file description: Volatile gas explosion
BA4FBG-5561	Filetype: .mp4, Content file description: A video depicting a gas being lit on fire inside a jug. The video then cuts to a portion of Rick Astley's 'Never Gonna Give You Up' music video.
BPGNBK-5562	Filetype: video/mp4, Content file description: EXPLOSION IN BOTTLE FOLLOWED BY RICK ASHLEY
BVMG7F-5561	Filetype: .mp4, Content file description: clips of water jug, a man's foot, and a man singing
BXTTXP-5561	Filetype: MP4, Content file description: whoosh bottle and music video compilation
CCXUMK-5561	Filetype: volatile gas explosion.mp4, Content file description: rick roll video that starts /w a glass jar with volatile gas inside that is lit on fire.
CPQ4TQ-5561	Filetype: MPEG 4.0, Content file description: video
D3A9ER-5561	Filetype: MPEG 4.0 Video, extension .mp4, Content file description: File name - volatile gas explosion. Video file depicting a fire event occurring in a large water jug.
D3MR2K-5561	Filetype: MPEG 4.0 Video, Content file description: The video appears to be of someone lighting a bottle on fire to make a "whoosh bottle" per the audio. Then it appears the Rick Astley – Never Gonna Give You Up music video begins to play.
D7C7PK-5562	Filetype: volatile gas explosion.mp4, Video file (.mp4) , Content file description: volatile gas explosion.mp4, flame used to ignite the contents of a large bottle, then it cuts to Rick Astley dancing
D8QG3R-5561	Filetype: MP4, Video, Content file description: volatile gas explosion followed by Rick Astley
DCKG7E-5561	Filetype: mp4, Content file description: Video of a large clear jar full of clear combustible gas. Gas is lit and segues into a Rick roll session.
DKUYDR-5561	Filetype: Mp4, Content file description: Volatile gas explosion
DKVPRL-5562	Filetype: MPEG 4.0 Video, Content file description: Woosh bottle demonstration with a Rickroll
DPA82Q-5561	Filetype: .mp4 Video file, Content file description: volatile gas explosion followed by part of rick Astley video
DTN8XH-5562	Filetype: mp4 video file, Content file description: A fourteen second (14s) video of a flammable substance igniting within a jar which is then replaced with an excerpt of 1987 pop classic "Never Gonna Give You Up" sung by the legend that is Rick Astley, and written and produced by Stock, Aitken, and Waterman.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22 - Examination Questions	
WebCode Test	Response
DXKMTK-5561	Filetype: Video file - .mp4, Content file description: gas explosion in a glass bottle with a clip of Never gonna give you up by rick astley music video at the end
EJD6CG-5561	Filetype: MP4 Video, Content file description: Video of volatile gas explosion and after that video of singer.
EJK3WT-5561	Filetype: MPEG-4 Video File, Content file description: Volatile gas explosion.mp4
EMTM9G-5561	Filetype: MPEG 4.0 Video, Content file description: video file titled volatile gas explosion: Fire inside of glass bottle and music/dance video
F3TPTL-5561	Filetype: .mp4, Content file description: volatile gas explosion in a glass jar with a music clip at the end of the video
F7NG2H-5561	Filetype: Video, Content file description: Gas explosion/Rick Astley
FG6CVN-5561	Filetype: Video (.mp4), Content file description: volatile gas explosion.mp4 Flame being put to large clear water container followed by male dancing (Never going to give you up tune lol)
FT8J39-5561	Filetype: MPEG-4 Video, Content file description: Video starting out with igniting gas in a container and turns into a rick roll video
G6U6KA-5561	Filetype: Mp4 video file, Content file description: A video of Flames in a bottle that turns into a rickroll
G9BD99-5561	Filetype: MPEG-4 Video, Content file description: video of man speaking and lighting the top of a bottle and then a man with red hair starts dancing to a song
G9PQLK-5561	Filetype: mp4, Content file description: Video showing a volatile gas explosion inside a whoosh glass bottle, with a man dancing at the end.
GALGEK-5562	Filetype: .mp4, Content file description: video of lighting gas in a large water bottle, guy dancing
GMPPAG-5561	Filetype: MPEG 4.0 Video, Content file description: The begining of the video shows a chemical experience (gas explosion in a bottle) then at the end it shows someone dancing.
H3X34J-5561	Filetype: MP4 Video, Content file description: fire in a bottle + rick roll
HAVCD-5562	Filetype: Video/mp4, Content file description: Funny video about the sound made by burning the gas in the bottle. (Rick Astley - Never Gonna Give You Up)
HFM3VL-5562	[Participant did not return results for this question.]
HGE2AK-5561	Filetype: MP4 (video), Content file description: Video of fire burning in a jar + the start of a "Rick Roll" clip.
HMQYPK-5561	Filetype: .mp4, Content file description: This file was an .mp4 (video) file. The video is 14 seconds in duration. A male voice is heard saying "All right, we are going to try this here whoosh bottle". A clear bottle observed, and its contents being ignited. The sounds of explosions are heard which then the audio and video transitions to the well-known "Never Gonna Give You Up" by Rick Astley song.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22 - Examination Questions	
WebCode Test	Response
HTB6DE-5562	Filetype: MP4 video file, Content file description: 14 second colour video beginning with gas being ignited in a jar. At 8 seconds the video switches to a music video of Rick Astley.
HVJ3Y9-5561	Filetype: .mp4 Content, Content file description: Video clip containing fire in a glass jug and a snippet of Rick Astley music video
HYHLVF-5561	Filetype: video, Content file description: Volatile gas explosion
J3FCTE-5561	Filetype: Filetype: mp4, Content file description: Chemical experiment (fire in a bottle conatinner), and the same video continues with a musical clip.
J49DM9-5561	Filetype: Video\MP4, Content file description: gas fire into rick roll
JFURCD-5561	Filetype: .mp4 video, Content file description: Video of a flaming jug into a RickRoll
JPAH22-5562	Filetype: MPEG-4 Video, Content file description: starts as an experiment on explosive gas, ends as a joke "Rick rolled" with Never Gonna Give You Up song by Rick Astley
JXAZDE-5561	Filetype: video/mp4 MPEG 4.0 Video, Content file description: A 14 seconds video of someone lighting a flame at the mouth of a glass bottle, and a flame lowering to the bottle. The video ends with a song titled 'Never Gonna Give You up' by Rick Astley.
JXHV GK-5561	Filetype: .mp4, Content file description: Contains video of a volatile gas explosion with a Rick Roll at the end.
K3WXT8-5562	Filetype: .mp4 video file, Content file description: Video of a clear gas being lighted inside large glass bottle. Red headed man dancing at the end of the video.
KA94ED-5562	Filetype: mp4, Content file description: A bottle with gas and Rick Astley videoclip
KCQD3T-5561	Filetype: .mp4 video file, Content file description: video of gas contained within a glass jar being ignited then rick astley singing/playing
KMHPR4-5561	Filetype: .mp4 video, Content file description: Flame inside of a glass bottle ending with Rick Astley clip
LBJ6ZC-5562	Filetype: MPEG 4.0 Video, Content file description: The video starts with a POV shot where someone is lighting a bottle with a lighter. The person says something similar to "let's try to hear some wush bottle." As the bottle is lit, a fire starts, making a "bhabha" sound, the video then transitions to some retro music video where a man is seen dancing.
LMDLPD-5561	Filetype: Video file .mp4 , Content file description: Filename = volatile gas explosion.mp4
LRM3Y2-5562	Filetype: .MP4, Content file description: Video of volatile gas explosion
LWKE3D-5561	Filetype: MP4, Content file description: Gas inside of a jug is ignited leading into the music video for Rick Astley's "Never Gonna Give you Up"
MCQ8YF-5561	Filetype: mp4, Content file description: volitale gas explosion in empty water jug followed by a Rick Astley clip (Rick Roll)

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22 - Examination Questions	
WebCode Test	Response
MD8AY2-5561	Filetype: .mp4/video, Content file description: gas igniting that cuts to music video
MK6QJE-5561	Filetype: MPEG 4.0 Video, Content file description: Gas ignited and explodes inside a glass jar then a music video of Rick Ashley plays.
MR47EE-5562	Filetype: mp4 (video: volatile gas explosion.mp4), Content file description: Gas explosion
MV6A9L-5561	Filetype: mp4, Content file description: Gas is being ignited inside a glass bottle then a Rickroll.
N9Q2B2-5562	Filetype: MP4 Video file, Content file description: We see someone lighting a fire in a glass bottle, causing a transition between the sound of firecrackers and Rick Astley's music video - Never Gonna Give You Up.
NH83FA-5562	Filetype: Filetype: MP4, Content file description: Video – volatile gas explosion (video is a few seconds depicting gas being ignited in a glass bottle.....before Rick Astley video starts).
NNQD78-5561	Filetype: mp4, Content file description: video of fire in a bottle and rick roll
NPUPBF-5562	Filetype: .mp4 Video file, Content file description: volatile gas explosion followed by part of rick Astley video
NQ7BB3-5561	Filetype: mp4 video file, Content file description: A rick rolled video. The presenter and recorder uses a lighter to ignite what appears to be a gaseous substance within a glass flask. Then the video cuts to Rick Astley's music video for "Never Gonna give you up" and him dancing in front of microphone.
P3EHK8-5562	Filetype: mp4, Content file description: volatile gas explosion with rickroll
P3ER7C-5561	Filetype: MPEG 4.0 video, Content file description: Video of gas explosion/flames in a "whoosh" bottle and 80's song video
P6NMZG-5561	Filetype: Video file, Content file description: Rick Roll; starts with a volatile gas explosion which merges into Rick Astley - Never Gonna Give You Up (Music Video)
PE6G4X-5561	Filetype: mp4, Content file description: Rick-rolled volatile gas explosion
PYKJC4-5561	Filetype: .mp4, Content file description: Video of gas being lit on fire inside a plastic jug.
Q4ZTN7-5562	Filetype: MPEG 4.0 Video, Content file description: It shows a video of a jug being lit up by a lighter then it cuts into a man dancing.
Q73JRN-5561	Filetype: .mp4 Advanced Audio Coding, Content file description: Bush bottle containing gas lit with lighter and Rick Astley singing "Never gonna give you up"
RBARA4-5561	Filetype: .mp4 file format, which is a video file type, Content file description: Some type of flammable material contained in a glass jug is lit on fire before transitioning into a male dancing to a song (Rickrolling meme).
RE7DZL-5561	Filetype: video/mp4, Content file description: blurry video of fire igniting gas in a glass bottle and then a Rick Roll.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22 - Examination Questions	
WebCode Test	Response
RUTBQ8-5561	Filetype: Video (mp4), Content file description: Experiment of volatile gas explosion were man light a fire in a bottle ended by man dancing
RY7A78-5561	Filetype: mp4, Content file description: Explosion inside a glass jar/ Music video
RZKKZ7-5562	Filetype: MPEG 4.0 Video, Content file description: The begining of the video shows a chemical experience (gas explosion in a bottle) then at the end it shows someone dancing.
T9UAE6-5561	Filetype: MP4 video, Content file description: Video of someone setting fire to some gasses in a bottle, which then cuts to a video of Rick Astley (commonly referred to as 'rick-rolled')
TH2XG4-5562	Filetype: mp4, Content file description: Combustion of some gas followed by a man dancing to music
TTGXLB-5561	Filetype: MPEG-4 Video, Content file description: A man is dancing to a song in front of a microphone after a volatile gas explosion test scene.
U8973A-5561	Filetype: MPEG-4, Content file description: VIDEO
UEQLM7-5561	Filetype: mp4 (video file), Content file description: The video shows a volatile gas explosion and then starts into a music video
UEWNPX-5561	Filetype: .mp4, Content file description: volatile gas explosion
UGNM4W-5561	Filetype: Mp4 - mpeg 4 video, Content file description: Video of volatile gas explosion (in glass jar)
ULHG2X-5561	Filetype: mp4, Content file description: Glass bottle flame lite above then white male singing and dancing
UPTW39-5562	Filetype: Video/MP4 , Content file description: A large bottle filled with flammable gases that ignited (volatile gas explosion) and other sense with the music and dance show.
UUA6Q9-5561	Filetype: MP4 which is a movie file, Content file description: A video of someone holding a lighter to a bottle, causing a flame. The video then switches to Rick Roll.
UZQMYA-5562	Filetype: .mp4, Content file description: Video of unknown gas being lit in a glass container, followed by Rick Astley music video for Never gonna give you up
V66XC6-5562	Filetype: volatile gas explosion.mp4 , Content file description: Video of a bottle with fire and a music video
V82HUJ-5561	Filetype: MPEG-4 Video, Content file description: A video of someone lighting some type of gaseous compound in a large glass container. The vapors ignite and send a bluish flame down and then up the inside of the container. This clip is followed by a red-haired male dancing in front of a microphone.
VXLE96-5561	Filetype: Filetype: Videos, Content file description: volatile gas explosion and a man is dancing behind microphone.
VYTW7Z-5561	Filetype: mp4, Content file description:

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22 - Examination Questions	
WebCode Test	Response
W447WA-5561	Filetype: .mp4 (multimedia file storage format used for storing video), Content file description: volatile gas explosion
WB84Q8-5561	Filetype: Video/MP4 , Content file description: volatile gas explosion
WBPY99-5561	Filetype: .mp4 video file, Content file description: Video of gas in a bottle burning followed by a singer at a microphone.
WFVT36-5561	Filetype: MP4 Video, Content file description: The content starts out with a glass bottle with some sort of fuel in it being set on fire then video turns into a music video with a white male with red hair dancing in front of a microphone.
WH6VY2-5561	Filetype: .mp4 (Video), Content file description: volatile gas explosion.mp4 this is a video of someone lighting a flame in a glass jug then a music video popping up.
WL2PNP-5561	Filetype: .mp4, Content file description: The video depicts a volatile gas explosion, where a person ignites a lighter near a gas-air mixture, causing an explosion. The video concludes with scenes of music and people dancing.
WL4AK7-5562	Filetype: .mp4 video, Content file description: starts with a video of a combusting gas in a glass bottle and ends with a clip from never gonna give you up by rick astley
WQGWCP-5562	Filetype: MPEG-4 Video, Content file description: A video of a science experiment that turns into Rick Astley
X2AZR3-5561	Filetype: mp4, Content file description: ****ing Rick Roll
X3NFAB-5561	Filetype: MP4 video file, Content file description: Volatile gas explosion with Rick Ashley music song and dance.
X62GKW-5561	Filetype: MP4 video, Content file description: The video shows a 'whoosh' bottle being lit and then a clip from Rick Astley's Never Gonna Give You Up.
X84MXA-5561	Filetype: MP4, Content file description: Some kind of chemical experiment + "rickrolling"
XDQM3P-5561	Filetype: MPEG 4.0 Video / .MP4, Content file description: the video of burning gas in a bottle continues with video music
XDT8Y6-5562	Filetype: This is a video file with the .mp4 format. , Content file description: This video is of a water container with some sort of gas inside, being lit. As the video follows the fire in the bottle, it changes over to Rick Aston's "Never gonna give you up" video, commonly referred to as a "Rick Roll".
XLP32A-5562	Filetype: mp4, Content file description: In the video, he said, "We'll try this fuel whoosh bottle." Then Setting fire to the opening of the glass bottle causes flames to fall down and an explosion to occur, and changes to show a man dancing and singing.
XQXJAX-5561	Filetype: .mp4 video file, Content file description: Out of scope for reporting for our purposes. We would provide the file but would not provide a description of the file.
Y2PJCZ-5561	Filetype: .mp4 video file, Content file description: some type of gas burning inside a glass jar followed by a man singing at a microphone

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22 - Examination Questions	
WebCode Test	Response
Y8WZT2-5561	Filetype: Video/mp4, Content file description: The video starts with a volatile gas explosion in a glass bottle and then cuts to a man dancing
YZK9WX-5561	Filetype: volatile gas explosion.mp4 is the file in question. This file is a .mp4 or a video file type., Content file description: This is a video depicting a clear container containing a blueish flame moving from top to bottom after a lit lighter is introduced to the opening. "Never Gonna Give You Up" by Rick Astley immediately plays following this.
Z4GR62-5562	Filetype: MPEG 4.0 Video, Content file description: It appears to be gas "swoosh" bottle video for approximately 9 seconds then into a "dancing video clip of 1987 hit song "Never Gonna Give You Up" performed by Rick Astley (this is AKA Rickrolling)" for approximately 5 seconds, Total duration: 14.33 seconds, bitrate: 433 kb/s, Video: h264, Audio: aac/mp4a 44100 Hz, stereo.
Z4PAVK-5561	Filetype: ISO Base Media File (MPEG-4) v1, Content file description: Flame up in a bottle...then Rick rolled.
ZBUQRZ-5561	Filetype: video, Content file description: volatile gas explosion
ZEU2MZ-5562	Filetype: mp4, Content file description: a fire ignited in something looks like a bottle or a jug, and then a man appears dancing.
ZF7RW4-5561	Filetype: Video/MP4, Content file description: volatile gas explosion
ZN4C6R-5561	Filetype: .mp4, Content file description: video of ignited gas in glass container, followed by Rick Astley music video
ZQ4URL-5562	Filetype: Media file (video, with extension .mp4), Content file description: The video shows the ignition of gas in a glass bottle and ends with a music video (rickroll).
ZU7QJ2-5561	Filetype: filetype .mp4 or ISO base media file (video), Content file description: The content of the file was a video with sound. The video appears to depict an unknown individual apply an ignition source to the mouth of a clear in color jar. What appears to be a blue in color fire is then observed inside the jug. The video then changes to depict an unidentified individual with red in color hair moving around the screen while music plays. The audio and video is consistent with a music video for the song "Never Gonna Give You Up" by artist Rick Astley.
ZWABN2-5562	Filetype: mp4, Content file description: The bottle is lit on fire, the gas explodes and goes down, and the man is dancing.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 22 - Examination Questions

Question 22: Describe the filetype and content of the file with created date March 9, 2024 21:56:33 UTC+0.

Consensus Result:

FileType: mp4 file

Content file description: A video of a person igniting a flammable gas in a large bottle. Dancing man at the end of the video (Rick Astley's music video or Rick-Rolled). Variations of this description were also accepted.

Manufacturer's Response Explanation:

Viewing all the files on the volume and sorting by creation date will discover volatile gas explosion.mp4.

Manufacturer's Response Illustration:

X-ways directory browser

and subdirectories	407,59			
Descripti	Type	Full path	Size	Created
existing	xml	\Users\gmontag\AppData\Local\Microsoft\Office\SolutionPackages\caa3...	2.0 KB	Saturday, March 9, 2024 21:54:08.5
existing, ...	mp4	\Users\gmontag\Videos\volatile gas explosion.mp4	759 KB	Saturday, March 9, 2024 21:56:33.7
existing		\Users\gmontag\AppData\Local\Packages\DuckDuckGo.DesktopBrowser.	94.6 KB	Saturday, March 9, 2024 21:59:22.2
existing	service...	\Users\gmontag\AppData\Local\Packages\DuckDuckGo.DesktopBrowser.	252 B	Saturday, March 9, 2024 21:59:22.2

X-ways view of C:\\$Recycle.BIN\IION3HTM.pdf

Item Path	File Created
Fire Department Workstation\Users\gmontag\AppData\Local\Microsoft\Office\Sc	03/09/24 04:54:08 PM (-5:00 Easter
Fire Department Workstation\Users\gmontag\Videos\volatile gas explosion.mp4	03/09/24 04:56:33 PM (-5:00 Easter
Fire Department Workstation\Users\gmontag\AppData\Local\Packages\DuckDuc	03/09/24 04:59:22 PM (-5:00 Easter



Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23 - Examination Questions

Question 23: According to Windows prefetch, how many times was the calculator app executed?

Manufacturer's Once (1)

Response:

WebCode Test	Response
28NKRK-5561	1
2BXEJB-5561	1
2EUC34-5562	118 Times
2UJN7X-5562	One
2XN36N-5561	1
36GUPN-5561	Once
3CH2GJ-5562	[Participant did not return results for this question.]
3DBUC3-5561	1
3K9LKW-5561	1
3LM236-5561	1 time
483YXK-5561	one (1)
49DVEJ-5561	1
4K6LX2-5561	1
4L6CCW-5562	1
4P6N9W-5561	1
4THJUL-5562	[Participant did not return results for this question.]
4XXRHK-5561	1
4Z77PR-5561	1
6KNFKX-5561	7
6RLGDW-5561	1

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23 - Examination Questions	
WebCode Test	Response
78YYBQ-5561	1
7M6APW-5561	per prefetch, calculatorapp.exe was executed 1 time.
7WAG6W-5561	1
7WV3RK-5561	1
8ED4K3-5562	1
8LRYCP-5561	1
8P8Q2X-5561	1
8RFV4L-5561	1
8W78WW-5562	1
98N78Y-5561	1
9J6THK-5561	1
9QMRX6-5561	1
9XFKVP-5562	1
AN93XR-5561	7
AXDBED-5562	1
AXFVBT-5561	Once
B2ACZR-5562	118
BA4FBG-5561	1
BPGNBK-5562	1 time
BVMG7F-5561	1
BXTTXP-5561	1

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23 - Examination Questions	
WebCode Test	Response
CCXUMK-5561	1
CPQ4TQ-5561	1
D3A9ER-5561	11
D3MR2K-5561	1
D7C7PK-5562	1
D8QG3R-5561	1
DCKG7E-5561	1
DKUYDR-5561	One
DKVPRL-5562	7 times
DPA82Q-5561	1
DTN8XH-5562	Executed one (1) time
DXKMTK-5561	1
EJD6CG-5561	1
EJK3WT-5561	1 time
EMTM9G-5561	1
F3TPTL-5561	1
F7NG2H-5561	1
FG6CVN-5561	1
FT8J39-5561	1
G6U6KA-5561	1
G9BD99-5561	1

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23 - Examination Questions	
WebCode Test	Response
G9PQLK-5561	1
GALGEK-5562	1
GMPPAG-5561	1
H3X34J-5561	1
HAWCD-5562	1
HFM3VL-5562	[Participant did not return results for this question.]
HGE2AK-5561	7
HMQYPK-5561	1
HTB6DE-5562	1
HVJ3Y9-5561	1 time
HYHLVF-5561	1
J3FCTE-5561	1
J49DM9-5561	1
JFURCD-5561	1
JPAH22-5562	1
JXAZDE-5561	7
JXHV GK-5561	1
K3WXT8-5562	1
KA94ED-5562	1
KCQD3T-5561	1
KMHPR4-5561	1

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23 - Examination Questions	
WebCode Test	Response
LBJ6ZC-5562	One (01)
LMDLPD-5561	1
LRM3Y2-5562	1
LWKE3D-5561	1
MCQ8YF-5561	1
MD8AY2-5561	1
MK6QJE-5561	1
MR47EE-5562	1 (one)
MV6A9L-5561	1
N9Q2B2-5562	1
NH83FA-5562	Once [1]
NNQD78-5561	1
NPUPBF-5562	1
NQ7BB3-5561	Executed 1 time
P3EHK8-5562	1
P3ER7C-5561	Once
P6NMZG-5561	1
PE6G4X-5561	1
PYKJC4-5561	1
Q4ZTN7-5562	1
Q73JRN-5561	1

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23 - Examination Questions	
WebCode Test	Response
RBARA4-5561	1
RE7DZL-5561	1
RUTBQ8-5561	1 time
RY7A78-5561	1
RZKKZ7-5562	1
T9UAE6-5561	1
TH2XG4-5562	Not in scope
TTGXLB-5561	1
U8973A-5561	1
UEQLM7-5561	1
UEWNPX-5561	1
UGNM4W-5561	Once
ULHG2X-5561	1
UPTW39-5562	118 Times
UUA6Q9-5561	1
UZQMYA-5562	1 time
V66XC6-5562	1
V82HUJ-5561	1
VXLE96-5561	1
VYTW7Z-5561	1
W447WA-5561	1

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23 - Examination Questions	
WebCode Test	Response
WB84Q8-5561	118 Times
WBPY99-5561	One time
WFVT36-5561	Once
WH6VY2-5561	1
WL2PNP-5561	1
WL4AK7-5562	1
WQGWCP-5562	7
X2AZR3-5561	1
X3NFAB-5561	1
X62GKW-5561	1
X84MXA-5561	1
XDQM3P-5561	1
XDT8Y6-5562	1 - The CalculatorApp was run one time, on 3/14/2024.
XLP32A-5562	7
XQXJAX-5561	1
Y2PJCZ-5561	1
Y8WZT2-5561	118
YZK9WX-5561	1
Z4GR62-5562	1
Z4PAVK-5561	1
ZBUQRZ-5561	1

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23 - Examination Questions	
WebCode Test	Response
ZEU2MZ-5562	1
ZF7RW4-5561	118 Times
ZN4C6R-5561	1
ZQ4URL-5562	1
ZU7QJ2-5561	1
ZWABN2-5562	1

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 23 - Examination Questions

Question 23: According to Windows prefetch, how many times was the calculator app executed?

Consensus Result:

1 (once)

Manufacturer's Response Explanation:

There is one prefetch file for CALCULATORAPP.EXE in C:\Windows\Prefetch. Analysis of this file with a reliable tool can parse the contained data, which includes the "run count" or number of times the program has been executed.

Manufacturer's Response Illustration:

X-Ways parse of CALCULATORAPP.EXE-089D935A.pf

The screenshot shows the X-Ways Forensics interface. At the top, a list of files is displayed with columns for file name, status, and path. The file 'CALCULATORAPP.EXE-089D935A.pf' is selected. Below the list, a detailed view of the selected file is shown, including a table with the following data:

Prefetch	
Name	CALCULATORAPP.EXE
Last Run	Thursday, March 14, 2024 02:08:26 +0
Run Count	1

Below this table is another table with columns for Time (ms), Name, and Path.

PECmd.exe parse of CALCULATORAPP.EXE-089D935A.pf

```

Command line: -f C:\temp\CALCULATORAPP.EXE-089D935A.pf
Warning: Administrator privileges not found!
Keywords: temp, tmp

Processing C:\temp\CALCULATORAPP.EXE-089D935A.pf
Created on: 2024-03-20 03:11:12
Modified on: 2024-03-14 02:08:36
Last accessed on: 2024-03-20 03:12:47

Executable name: CALCULATORAPP.EXE
Hash: 89D935A
File size (bytes): 130,852
Version: Windows 10 or Windows 11
Run count: 1
Last run: 2024-03-14 02:08:26

```

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions

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

Manufacturer's C:\temp\

Response:

WebCode Test	Response
28NKRK-5561	1
2BXEJB-5561	TEMP
2EUC34-5562	C:\ temp\AcroRdrDC2300820555_en_US.exe
2UJN7X-5562	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\ACRORDRDC2300820555_EN_US.EXE
2XN36N-5561	C:\
36GUPN-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\ACRORDRDC2300820555_EN_US.EXE
3CH2GJ-5562	[Participant did not return results for this question.]
3DBUC3-5561	[root]/TEMP/ACRORDRDC2300820555_EN_US.EXE
3K9LKW-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\ACRORDRDC2300820555_EN_US.EXE
3LM236-5561	C:\TEMP
483YXK-5561	temp
49DVEJ-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP
4K6LX2-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP
4L6CCW-5562	\TEMP\
4P6N9W-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP
4THJUL-5562	[Participant did not return results for this question.]
4XXRHK-5561	C:\Temp
4Z77PR-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\
6KNFKX-5561	C:\temp\

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions	
WebCode Test	Response
6RLGDW-5561	\TEMP\
78YYBQ-5561	temp
7M6APW-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP
7WAG6W-5561	\temp
7WV3RK-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\
8ED4K3-5562	VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\ACRORDRDC23008_0555_EN_US.EXE
8LRYCP-5561	Program Files (x86)
8P8Q2X-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\ACRORDRDC2300820555_EN_US.EXE
8RFV4L-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP
8W78WW-5562	\TEMP\
98N78Y-5561	C:\temp\AcroRdrDC2300820555_en_US.exe
9J6THK-5561	Temporary
9QMRX6-5561	C:\temp
9XFKVP-5562	Temp
AN93XR-5561	C:\temp\
AXDBED-5562	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\ACRORDRDC2300820555_EN_US.exe
AXFVBT-5561	\TEMP
B2ACZR-5562	C:\temp\AcroRdrDC2300820555_en_US.exe
BA4FBG-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP
BPGNBK-5562	\temp
BVMG7F-5561	VOLUME {01da609bdb9b99bd-32dbb012}

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions	
WebCode Test	Response
BXTTXP-5561	TEMP
CCXUMK-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\ACRORDRDC2300820555_EN_US.EXE
CPQ4TQ-5561	\\VOLUME{01DA609BDB9B99BD-32DBB012}\TEMP
D3A9ER-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\ACRORDRDC2300820555_EN_US.EXE
D3MR2K-5561	TEMP
D7C7PK-5562	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\ACRORDRDC2300820555_EN_US.EXE
D8QG3R-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\ACRORDRDC2300820555_EN_US.EXE
DCKG7E-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\
DKUYDR-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\ACRORDRDC2300820555_EN_US.EXE
DKVPRL-5562	/temp
DPA82Q-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\
DTN8XH-5562	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\ACRORDRDC2300820555_EN_US.EXE
DXKMTK-5561	C:\temp
EJD6CG-5561	TEMP
EJK3WT-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\ACRORDRDC2300820555_EN_US.EXE
EMTM9G-5561	temp
F3TPL-5561	temp
F7NG2H-5561	C:\temp
FG6CVN-5561	Temp
FT8J39-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\
G6U6KA-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions	
WebCode Test	Response
G9BD99-5561	TEMP
G9PQLK-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP (C:\temp)
GALGEK-5562	TEMP
GMPPAG-5561	C:\temp\
H3X34J-5561	C:\temp
HAVVCD-5562	C:/temp
HFM3VL-5562	[Participant did not return results for this question.]
HGE2AK-5561	\temp
HMQYPK-5561	\\temp\
HTB6DE-5562	\TEMP
HVJ3Y9-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\ACRORDRDC2300820555_EN_US.EXE
HYHLVF-5561	TEMP
J3FCTE-5561	C:\temp
J49DM9-5561	C:\Windows\Temp\
JFURCD-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\
JPAH22-5562	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP
JXAZDE-5561	TEMP
JXHV GK-5561	TEMP
K3WXT8-5562	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\ACRORDRDC2300820555_EN_US.EXE
KA94ED-5562	/TEMP
KCQD3T-5561	\temp\

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions	
WebCode Test	Response
KMHPR4-5561	TEMP
LBJ6ZC-5562	\\TEMP\ACRORDRDC2300820555_EN_US.EXE
LMDLPD-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\ACRORDRDC2300820555_EN_US.EXE
LRM3Y2-5562	1
LWKE3D-5561	TEMP
MCQ8YF-5561	TEMP
MD8AY2-5561	\\temp\
MK6QJE-5561	\\VOLUME {01da609bdb9b99db-32dbb012}\TEMP
MR47EE-5562	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\AcroRdrDC2300820555_en_US.exe
MV6A9L-5561	temp
N9Q2B2-5562	\\TEMP\
NH83FA-5562	TEMP
NNQD78-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\ACRORDRDC2300820555_EN_US.EXE
NPUPBF-5562	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\
NQ7BB3-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP
P3EHK8-5562	temp
P3ER7C-5561	\\TEMP
P6NMZG-5561	\\TEMP\
PE6G4X-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\ACRORDRDC2300820555_EN_US.EXE
PYKJC4-5561	\\VOLUME{01da609bdb9b99bd-dbb012}\TEMP
Q4ZTN7-5562	Program Files (x86)

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions	
WebCode Test	Response
Q73JRN-5561	\temp
RBARA4-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\ACRORDRDC2300820555_EN_US.EXE
RE7DZL-5561	TEMP
RUTBQ8-5561	TEMP Directory
RY7A78-5561	TEMP
RZKKZ7-5562	C:\temp\
T9UAE6-5561	C:\TEMP\
TH2XG4-5562	Not in scope
TTGXLB-5561	C:/TEMP
U8973A-5561	/TEMP
UEQLM7-5561	\TEMP\
UEWNPX-5561	C:\TEMP\
UGNM4W-5561	\temp
ULHG2X-5561	C:\TEMP\
UPTW39-5562	C:\ temp\AcroRdrDC2300820555_en_US.exe
UUA6Q9-5561	TEMP
UZQMYA-5562	\\DEVICE\HARDDISKVOLUME3\TEMP\ACRORDRDC2300820555_EN_US.EXE
V66XC6-5562	VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\ACRORDRDC2300820555_EN_US.EXE
V82HUJ-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\ACRORDRDC2300820555_EN_US.EXE
VXLE96-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\ACRORDRDC2300820555_EN_US.EXE
VYTW7Z-5561	\TEMP\ACRORDRDC2300820555_EN_US.EXE

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions	
WebCode Test	Response
W447WA-5561	C:\temp\
WB84Q8-5561	C:\temp\AcroRdrDC2300820555_en_US.exe
WBPY99-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\ACRORDRDC2300820555_EN_US.EXE
WFVT36-5561	TEMP
WH6VY2-5561	c:\temp\
WL2PNP-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\PROGRAM FILES (X86)\COMMON FILES\ADOBE\READER\TEMP\17761\
WL4AK7-5562	\\VOLUME{01da609bdb9b99bd-32dbb012}
WQGWCP-5562	Temp
X2AZR3-5561	temp
X3NFAB-5561	C:\TEMP\ACRORDRDC2300820555_EN_US.EXE
X62GKW-5561	\temp\
X84MXA-5561	.\TEMP folder
XDQM3P-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\ACRORDRDC2300820555_EN_US.EXE
XDT8Y6-5562	\\TEMP\ACRORDRDC2300820555_EN_US.EXE (The Temp Directory)
XLP32A-5562	C:\temp
XQXJAX-5561	C:\temp
Y2PJCZ-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP (filename: ACRORDRDC2300820555_EN_US.EXE)
Y8WZT2-5561	TEMP
YZK9WX-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\ACRORDRDC2300820555_EN_US.EXE
Z4GR62-5562	C:\temp
Z4PAVK-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\ACRORDRDC2300820555_EN_US.EXE

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions	
WebCode Test	Response
ZBUQRZ-5561	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\
ZEU2MZ-5562	temp
ZF7RW4-5561	C:\ temp\AcroRdrDC2300820555_en_US.exe
ZN4C6R-5561	\TEMP
ZQ4URL-5562	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\
ZU7QJ2-5561	\root\temp
ZWABN2-5562	\\VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\ACRORDRDC2300820555_EN_US.EXE

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 24 - Examination Questions

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

Consensus Result:

C:\temp\ and any variations representing similar information.

Manufacturer's Response Explanation:

There is one prefetch file for AcroRdrDC2300820555_en_US.exe in C:\Windows\Prefetch. Analysis of this file with a reliable tool can parse the contained data, which includes the path of files referenced by the program when executed, including itself.

Manufacturer's Response Illustration:

X-Ways parse of ACRORDRDC2300820555_EN_US.EXE-6594D80D.pf

Name	Description	Type	Full path
..	Windows (130.244)	existing, ...	\Windows
.	Prefetch (329)	existing	\Windows\Prefetch
ACRORDRDC2300820555_EN_US.EXE-6594D80D.pf	existing, ...	pf	\Windows\Prefetch\ACRORDRDC2300820555_EN_US.EXE-6594D80D.pf
ADNOTIFICATIONMANAGER.EXE-E7F9E8B8.pf	existing	pf	\Windows\Prefetch\ADNOTIFICATIONMANAGER.EXE-E7F9E8B8.pf
ADOBEARM.EXE-F9223367.pf	existing	pf	\Windows\Prefetch\ADOBEARM.EXE-F9223367.pf

Volume	File	Full path
118	KERNEL32.DLL	\WINDOWS\SYSWOW64\KERNEL32.DLL
189	USER32.DLL	\WINDOWS\SYSTEM32\USER32.DLL
190	WOW64CPU.DLL	\WINDOWS\SYSTEM32\WOW64CPU.DLL
196	NTDLL.DLL	\WINDOWS\SYSWOW64\NTDLL.DLL
304	ACRORDRDC2300820555_EN_US.EXE	\TEMP\ACRORDRDC2300820555_EN_US.EXE
14862	KERNELBASE.DLL	\WINDOWS\SYSWOW64\KERNELBASE.DLL
15008	LOCALE.NLS	\WINDOWS\SYSTEM32\LOCALE.NLS

PECmd.exe parse of ACRORDRDC2300820555_EN_US.EXE-6594D80D.pf showing execution directory

```

11: \VOLUME{01da609bdb9b99bd-32dbb012}\WINDOWS\SYSTEM32\WOW64CPU.DLL
12: \VOLUME{01da609bdb9b99bd-32dbb012}\WINDOWS\SYSWOW64\NTDLL.DLL
13: \VOLUME{01da609bdb9b99bd-32dbb012}\TEMP\ACRORDRDC2300820555_EN_US.EXE (Executable: True)
14: \VOLUME{01da609bdb9b99bd-32dbb012}\WINDOWS\SYSWOW64\KERNELBASE.DLL
15: \VOLUME{01da609bdb9b99bd-32dbb012}\WINDOWS\SYSTEM32\LOCALE.NLS

```

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 picture file containing red text, "Make Your Own Focaccia." Provide the five words that immediately follow, "Make Your Own Focaccia."

Manufacturer's A cooking workshop for all

Response:

WebCode Test	Response
28NKRK-5561	A cooking workshop for all
2BXEJB-5561	A cooking workshop for all
2EUC34-5562	A Cooking Workshop For Al
2UJN7X-5562	A cooking workshop for all
2XN36N-5561	A cooking workshop for all
36GUPN-5561	A cooking workshop for all
3CH2GJ-5562	[Participant did not return results for this question.]
3DBUC3-5561	A cooking workshop for all
3K9LKW-5561	A cooking workshop for all
3LM236-5561	A cooking workshop for all
483YXK-5561	A cooking workshop for all
49DVEJ-5561	Make Your Own Focaccia
4K6LX2-5561	A cooking workshop for all
4L6CCW-5562	a cooking workshop for all
4P6N9W-5561	A cooking workshop for all
4THJUL-5562	[Participant did not return results for this question.]
4XXRHK-5561	A cooking workshop for all
4Z77PR-5561	A cooking workshop for all
6KNFKX-5561	A cooking workshop for all

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25 - Examination Questions	
WebCode Test	Response
6RLGDW-5561	"A cooking workshop for all"
78YYBQ-5561	A cooking workshop for all
7M6APW-5561	"A cooking workshop for all"
7WAG6W-5561	A cooking workshop for all
7WV3RK-5561	A cooking workshop for all
8ED4K3-5562	A cooking workshop for all
8LRYCP-5561	A cooking workshop for all
8P8Q2X-5561	A cooking workshop for all
8RFV4L-5561	A cooking workshop for all
8W78WW-5562	A cooking workshop for all
98N78Y-5561	a cooking workshop for all
9J6THK-5561	A cooking workshop for all
9QMRX6-5561	A cooking workshop for all
9XFKVP-5562	A cooking workshop for all
AN93XR-5561	A cooking workshop for all
AXDBED-5562	A cooking workshop for all
AXFVBT-5561	A cooking workshop for all.
B2ACZR-5562	A cooking workshop for all
BA4FBG-5561	A cooking workshop for all
BPGNBK-5562	A cooking workshop for all
BVMG7F-5561	A cooking workshop for all

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25 - Examination Questions	
WebCode Test	Response
BXTTXP-5561	A cooking workshop for all
CCXUMK-5561	A cooking workshop for all
CPQ4TQ-5561	A cooking workshop for all
D3A9ER-5561	[Participant did not return results for this question.]
D3MR2K-5561	A cooking workshop for all
D7C7PK-5562	A cooking workshop for all
D8QG3R-5561	A cooking workshop for all
DCKG7E-5561	A Cooking Workshop For All
DKUYDR-5561	A cooking workshop for all
DKVPRL-5562	A cooking workshop for all
DPA82Q-5561	A cooking workshop for all
DTN8XH-5562	"A cooking workshop for all"
DXKMTK-5561	A cooking workshop for all
EJD6CG-5561	A cooking workshop for all
EJK3WT-5561	A cooking workshop for all
EMTM9G-5561	"A cooking workshop for all"
F3TPL-5561	A cooking workshop for all
F7NG2H-5561	A cooking workshop for all
FG6CVN-5561	A cooking workshop for all
FT8J39-5561	A cooking workshop for all
G6U6KA-5561	A cooking workshop for all

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25 - Examination Questions	
WebCode Test	Response
G9BD99-5561	A cooking workshop for all
G9PQLK-5561	A cooking workshop for all
GALGEK-5562	A cooking workshop for all
GMPPAG-5561	A cooking workshop for all
H3X34J-5561	A cooking workshop for all
HAVVCD-5562	A cooking workshop for all
HFM3VL-5562	[Participant did not return results for this question.]
HGE2AK-5561	"A cooking workshop for all"
HMQYPK-5561	A cooking workshop for all
HTB6DE-5562	A cooking workshop for all
HVJ3Y9-5561	A cooking workshop for all
HYHLVF-5561	A cooking workshop for all
J3FCTE-5561	A cooking workshop for all
J49DM9-5561	A cooking workshop for all
JFURCD-5561	A cooking workshop for all
JPAH22-5562	A cooking workshop for all
JXAZDE-5561	A cooking workshop for all
JXHV GK-5561	A cooking workshop for all
K3WXT8-5562	A cooking workshop for all
KA94ED-5562	A cooking workshop for all
KCQD3T-5561	A cooking workshop for all

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25 - Examination Questions	
WebCode Test	Response
KMHPR4-5561	A cooking workshop for all
LBJ6ZC-5562	A cooking workshop for all
LMDLPD-5561	A cooking workshop for all
LRM3Y2-5562	A cooking workshop for all
LWKE3D-5561	A cooking workshop for all
MCQ8YF-5561	A cooking workshop for all
MD8AY2-5561	A cooking workshop for all
MK6QJE-5561	A cooking workshop for all
MR47EE-5562	"A cooking workshop for all"
MV6A9L-5561	A cooking workshop for all
N9Q2B2-5562	A cooking workshop for all
NH83FA-5562	A cooking workshop for all
NNQD78-5561	a cooking workshop for all
NPUPBF-5562	A cooking workshop for all
NQ7BB3-5561	"A cooking workshop for all"
P3EHK8-5562	A cooking workshop for all
P3ER7C-5561	A cooking workshop for all
P6NMZG-5561	A cooking workshop for all
PE6G4X-5561	A cooking workshop for all
PYKJC4-5561	A cooking workshop for all
Q4ZTN7-5562	A cooking workshop for all

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25 - Examination Questions	
WebCode Test	Response
Q73JRN-5561	A cooking workshop for all
RBARA4-5561	"A cooking workshop for all"
RE7DZL-5561	A cooking workshop for all
RUTBQ8-5561	A cooking workshop for all
RY7A78-5561	A cooking workshop for all
RZKKZ7-5562	A cooking workshop for all
T9UAE6-5561	A cooking workshop for all
TH2XG4-5562	Not in scope
TTGXLB-5561	A cooking workshop for all
U8973A-5561	A cooking workshop for all
UEQLM7-5561	A cooking workshop for all
UEWNPX-5561	A cooking workshop for all
UGNM4W-5561	A cooking workshop for all
ULHG2X-5561	A cooking workshop for all
UPTW39-5562	A Cooking Workshop For All
UUA6Q9-5561	A cooking workshop for all
UZQMYA-5562	A cooking workshop for all
V66XC6-5562	A cooking workshop for all
V82HUJ-5561	A cooking workshop for all
VXLE96-5561	A cooking workshop for all
VYTW7Z-5561	[Participant did not return results for this question.]

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25 - Examination Questions	
WebCode Test	Response
W447WA-5561	A cooking workshop for all
WB84Q8-5561	A Cooking Workshop For Al
WBPY99-5561	A cooking workshop for all
WFVT36-5561	A cooking workshop for all
WH6VY2-5561	A cooking workshop for all
WL2PNP-5561	A cooking workshop for all
WL4AK7-5562	A cooking workshop for all
WQGWCP-5562	A cooking workshop for all
X2AZR3-5561	A cooking workshop for all
X3NFAB-5561	A cooking workshop for all
X62GKW-5561	A cooking workshop for all
X84MXA-5561	A cooking workshop for all
XDQM3P-5561	A cooking workshop for all
XDT8Y6-5562	A cooking workshop for all
XLP32A-5562	A cooking workshop for all
XQXJAX-5561	A cooking workshop for all
Y2PJCZ-5561	A cooking workshop for all
Y8WZT2-5561	A cooking workshop for all
YZK9WX-5561	A cooking workshop for all
Z4GR62-5562	A cooking workshop for all
Z4PAVK-5561	A cooking workshop for all

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25 - Examination Questions	
WebCode Test	Response
ZBUQRZ-5561	A cooking workshop for all
ZEU2MZ-5562	A cooking workshop for all
ZF7RW4-5561	A Cooking Workshop For All
ZN4C6R-5561	A cooking workshop for all
ZQ4URL-5562	A cooking workshop for all
ZU7QJ2-5561	A cooking workshop for all
ZWABN2-5562	A cooking workshop for all

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 picture file containing red text, "Make Your Own Focaccia." Provide the five words that immediately follow, "Make Your Own Focaccia."

Consensus Result:

"A cooking workshop for all" and any slight variation of this response, if it was easily determined to be a formatting issue.

Manufacturer's Response Explanation:

A reliable file recovery or file carving tool can find deleted files in unallocated space. The purpose of this question was to carve for deleted picture files and review graphic content.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 25 - Examination Questions

Manufacturer's Response Illustration:

X-Ways carved file

	000094 (Photoshop Web 75).jpg	carved fr...	jpg	\Path unknown\Carved files\000094 (Phot
	000096.png	carved fr...	png	\Path unknown\Carved files\000096.png
	000097.png	carved fr...	png	\Path unknown\Carved files\000097.png
	000098 (Standard 75).jpg	carved fr...	jpg	\Path unknown\Carved files\000098 (Stan
	000100.pna	carved fr...	pna	\Path unknown\Carved files\000100.pna

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

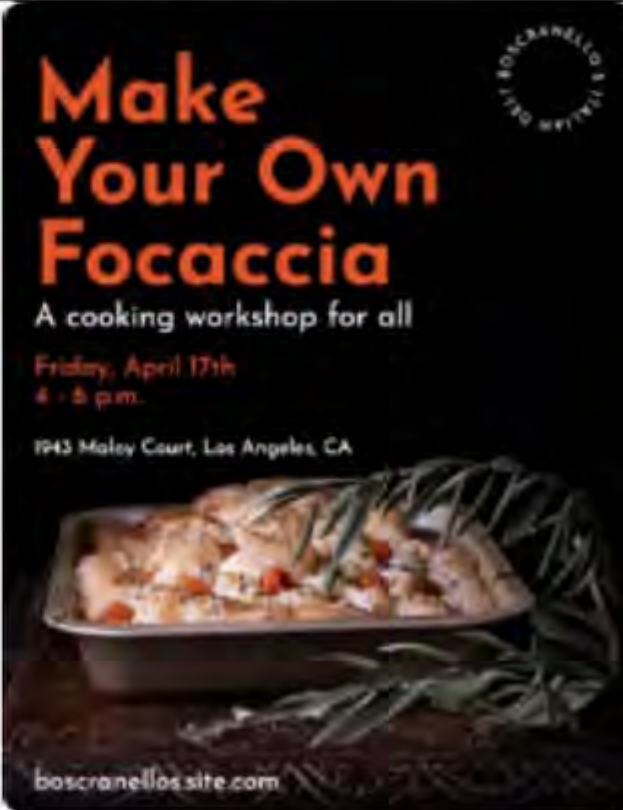
Question 25 - Examination Questions

Autopsy carved file

Name	S	C	O	MDS Hash	Modified Time	Change Time
f0008960_shtransform_dll	0			8287cbd7db5a6749da988a5ab180c5d6	0000-00-00 00:00:00	0000-00-00 00:00:00
f0008968.png	0			346e6e0605afa726a849a1d8ee084fba	0000-00-00 00:00:00	0000-00-00 00:00:00
f0009217.h	0			aff951c0dd2c62fe011de50544b7b20a	0000-00-00 00:00:00	0000-00-00 00:00:00

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrence

0° 171% Reset



The image shows a thumbnail of a poster for a cooking workshop. The poster has a black background with orange and white text. The main title is 'Make Your Own Focaccia' in large orange letters. Below it, in white, is 'A cooking workshop for all'. The date and time are 'Friday, April 17th 4 - 5 p.m.' and the location is '1943 Maloy Court, Los Angeles, CA'. At the bottom, there is a photo of a focaccia bread in a pan, garnished with olive branches. The website 'boscranellosite.com' is at the bottom left. A circular logo with 'BOSCRANELLOSITE.COM' is in the top right corner.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26 - Examination Questions

Question 26: Provide the username for the user who searched for "thermite recipie" [sic].

Manufacturer's gmontag

Response:

WebCode Test	Response
28NKRK- 5561	gmontag
2BXEJB- 5561	gmontag
2EUC34- 5562	Gmontag
2UJN7X- 5562	gmontag
2XN36N- 5561	gmontag
36GUPN- 5561	gmontag
3CH2GJ- 5562	[Participant did not return results for this question.]
3DBUC3- 5561	gmontag
3K9LKW- 5561	gmontag
3LM236- 5561	gmontag
483YXK- 5561	gmontag
49DVEJ- 5561	gmontag
4K6LX2- 5561	gmontag
4L6CCW- 5562	gmontag
4P6N9W- 5561	gmontag
4THJUL- 5562	[Participant did not return results for this question.]
4XXRHK- 5561	gmontag
4Z77PR- 5561	gmontag
6KNFKX- 5561	gmontag
6RLGDW- 5561	gmontag

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26 - Examination Questions	
WebCode Test	Response
78YYBQ-5561	gmontag
7M6APW-5561	gmontag
7WAG6W-5561	gmontag
7WV3RK-5561	gmontag
8ED4K3-5562	gmontag
8LRYCP-5561	gmontag
8P8Q2X-5561	Gmontag
8RFV4L-5561	gmontag
8W78WW-5562	gmontag
98N78Y-5561	gmontag
9J6THK-5561	gmontag
9QMRX6-5561	gmontag
9XFKVP-5562	gmontag
AN93XR-5561	gmontag
AXDBED-5562	gmontag
AXFVBT-5561	gmontag
B2ACZR-5562	Gmontag
BA4FBG-5561	gmontag
BPGNBK-5562	gmontag
BVMG7F-5561	gmontag
BXTTXP-5561	gmontag

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26 - Examination Questions	
WebCode Test	Response
CCXUMK-5561	gmontag
CPQ4TQ-5561	gmontag
D3A9ER-5561	gmontag
D3MR2K-5561	gmontag
D7C7PK-5562	gmontag
D8QG3R-5561	gmontag
DCKG7E-5561	gmontag
DKUYDR-5561	gmontag
DKVPRL-5562	gmontag
DPA82Q-5561	gmontag
DTN8XH-5562	gmontag
DXKMTK-5561	gmontag
EJD6CG-5561	gmontag
EJK3WT-5561	Gmontag
EMTM9G-5561	gmontag
F3TPTL-5561	gmontag
F7NG2H-5561	gmontag
FG6CVN-5561	gmontag
FT8J39-5561	gmontag
G6U6KA-5561	gmontag
G9BD99-5561	gmontag

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26 - Examination Questions	
WebCode Test	Response
G9PQLK-5561	gmontag
GALGEK-5562	gmontag
GMPPAG-5561	gmontag
H3X34J-5561	gmontag
HAWCD-5562	gmontag
HFM3VL-5562	[Participant did not return results for this question.]
HGE2AK-5561	gmontag
HMQYPK-5561	gmontag
HTB6DE-5562	gmontag
HVJ3Y9-5561	gmontag
HYHLVF-5561	gmontag
J3FCTE-5561	Users/gmontag
J49DM9-5561	gmontag
JFURCD-5561	gmontag
JPAH22-5562	gmontag
JXAZDE-5561	gmontag
JXHV GK-5561	gmontag
K3WXT8-5562	gmontag
KA94ED-5562	gmontag
KCQD3T-5561	gmontag
KMHPR4-5561	gmontag

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26 - Examination Questions	
WebCode Test	Response
LBJ6ZC-5562	gmontag
LMDLPD-5561	gmontag
LRM3Y2-5562	gmontag
LWKE3D-5561	gmontag
MCQ8YF-5561	gmontag
MD8AY2-5561	gmontag
MK6QJE-5561	gmontag
MR47EE-5562	gmontag
MV6A9L-5561	gmontag
N9Q2B2-5562	gmontag
NH83FA-5562	Filename: book.zip Filepath: \Users\jbeatty\Documents
NNQD78-5561	gmontag
NPUPBF-5562	gmontag
NQ7BB3-5561	User "gmontag"
P3EHK8-5562	gmontag
P3ER7C-5561	gmontag
P6NMZG-5561	gmontag
PE6G4X-5561	gmontag
PYKJC4-5561	gmontag
Q4ZTN7-5562	gmontag
Q73JRN-5561	gmontag

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26 - Examination Questions	
WebCode Test	Response
RBARA4-5561	gmontag
RE7DZL-5561	gmontag
RUTBQ8-5561	gmontag
RY7A78-5561	gmontag
RZKKZ7-5562	gmontag
T9UAE6-5561	gmontag
TH2XG4-5562	Not in scope
TTGXLB-5561	gmontag
U8973A-5561	gmontag
UEQLM7-5561	gmontag
UEWNPX-5561	gmontag
UGNM4W-5561	gmontag
ULHG2X-5561	gmontag
UPTW39-5562	Gmontag
UUA6Q9-5561	gmontag
UZQMYA-5562	gmontag
V66XC6-5562	gmontag
V82HUJ-5561	gmontag
VXLE96-5561	gmontag
VYTW7Z-5561	gmontag
W447WA-5561	gmontag

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26 - Examination Questions	
WebCode Test	Response
WB84Q8-5561	Gmontag
WBPY99-5561	gmontag
WFVT36-5561	username gmontag
WH6VY2-5561	gmontag
WL2PNP-5561	gmontag
WL4AK7-5562	gmontag
WQGWCP-5562	Gmontag
X2AZR3-5561	gmontag
X3NFAB-5561	gmontag
X62GKW-5561	gmontag
X84MXA-5561	gmontag
XDQM3P-5561	gmontag
XDT8Y6-5562	gmontag
XLP32A-5562	gmontag
XQXJAX-5561	gmontag
Y2PJCZ-5561	gmontag
Y8WZT2-5561	gmontag
YZK9WX-5561	gmontag
Z4GR62-5562	gmontag
Z4PAVK-5561	gmontag
ZBUQRZ-5561	gmontag

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26 - Examination Questions	
WebCode Test	Response
ZEU2MZ-5562	gmontag
ZF7RW4-5561	Gmontag
ZN4C6R-5561	gmontag
ZQ4URL-5562	gmontag
ZU7QJ2-5561	gmontag
ZWABN2-5562	gmontag

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 26 - Examination Questions

Question 26: Provide the username for the user who searched for "thermite recipe" [sic].

Consensus Result:

gmontag

Manufacturer's Response Explanation:

User gmontag used the DuckDuckGo privacy browser to search duckduckgo.com for "thermite recipe". Duck Duck Go browser records are stored in C:\Users\gmontag\AppData\Local\Packages\DuckDuckGo.DesktopBrowser_ya2fgkz3nks94\LocalState\EBWebView\Default\ History.

Manufacturer's Response Illustration:

EnCase parse of DuckDuckGo History

True Path	Internet Artifact Type	Record Last Accessed	Uri Name
n\Users\gmontag\AppData\Local\Packages\DuckDuckGo.Desktop...	History	03/09/24 04:42...	https://duckduckgo.com/?q=thermite+recipie
n\Users\gmontag\AppData\Local\Packages\DuckDuckGo.Desktop...	Keyword Search	03/09/24 04:42...	https://duckduckgo.com/?q=thermite+recipie
n\Users\gmontag\AppData\Local\Packages\DuckDuckGo.Desktop...	History	03/09/24 04:42...	https://duckduckgo.com/?q=thermite+recipie
n\Users\gmontag\AppData\Local\Packages\DuckDuckGo.Desktop...	History	03/09/24 04:42...	https://duckduckgo.com/?q=thermite+recipie

Autopsy parse of DuckDuckGo History

id	url	title	visits
21	https://en.wikipedia.org/wiki/Acetone	Acetone - Wikipedia	2
22	https://duckduckgo.com/?q=thermite+recipie	thermite recipe at DuckDuckGo	1
23	https://duckduckgo.com/?q=thermite+recipie&atb=v420-1gl	thermite recipe at DuckDuckGo	2
24	https://duckduckgo.com/?q=thermite+recipie&atb=v420-1gl&ia=web	thermite recipe at DuckDuckGo	2
25	https://duckduckgo.com/?q=thermite+recipie&atb=v420-1gl&iax=videos...	thermite recipe at DuckDuckGo	1
26	https://www.youtube.com/watch?v=IMCw1cbKzNM#ddg-play	How to Make Thermite - YouTube	2
27	https://www.youtube.com/watch?v=RiF73l4PjyY	Make Thermite (and testing various iron	1

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27 - Examination Questions

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

Manufacturer's gmontag

Response:

WebCode Test	Response
28NKRK-5561	gmontag
2BXEJB-5561	gmontag
2EUC34-5562	C:\Users\gmontag\Documents
2UJN7X-5562	kshea
2XN36N-5561	gmontag
36GUPN-5561	gmontag
3CH2GJ-5562	[Participant did not return results for this question.]
3DBUC3-5561	gmontag
3K9LKW-5561	gmontag
3LM236-5561	Documents, OneDrive, Downloads, Desktop
483YXK-5561	gmontag
49DVEJ-5561	C:\Users\gmontag\Documents\Document.rtf
4K6LX2-5561	gmontag
4L6CCW-5562	gmontag
4P6N9W-5561	Pictures
4THJUL-5562	[Participant did not return results for this question.]
4XXRHK-5561	gmontag
4Z77PR-5561	gmontag
6KNFKX-5561	gmontag

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27 - Examination Questions	
WebCode Test	Response
6RLGDW-5561	gmontag
78YYBQ-5561	gmontag
7M6APW-5561	gmontag
7WAG6W-5561	Documents, FireDrive(F:), User Data, Pictures
7WV3RK-5561	gmontag
8ED4K3-5562	gmontag
8LRYCP-5561	gmontag
8P8Q2X-5561	Gmontag
8RFV4L-5561	gmontag
8W78WW-5562	C:\Users\gmontag\Documents\
98N78Y-5561	Fire-fighting-Training-Manual.pdf basic-scba-instructor-manual-rev-10-21-13-1.pdf
9J6THK-5561	gmontag
9QMRX6-5561	gmontag
9XFKVP-5562	gmontag
AN93XR-5561	C:\Users\gmontag\Documents\Document.rtf
AXDBED-5562	gmontag
AXFVBT-5561	gmontag
B2ACZR-5562	User: C:\Users\gmontag\Documents\
BA4FBG-5561	gmontag
BPGNBK-5562	\Users\gmontag\Documents
BVMG7F-5561	gmontag

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27 - Examination Questions	
WebCode Test	Response
BXTTXP-5561	gmontag
CCXUMK-5561	gmontag
CPQ4TQ-5561	gmontag
D3A9ER-5561	\Users\gmontag\Documents
D3MR2K-5561	gmontag
D7C7PK-5562	hives\jbeatty\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\ Gmontag = Users\gmontag\Documents\Document.rtf
D8QG3R-5561	gmontag
DCKG7E-5561	gmontag
DKUYDR-5561	gmontag
DKVPRL-5562	gmontag
DPA82Q-5561	gmontag
DTN8XH-5562	gmontag
DXKMTK-5561	gmontag
EJD6CG-5561	gmontag
EJK3WT-5561	Gmontag, Document.rtf
EMTM9G-5561	gmontag
F3TPTL-5561	gmontag
F7NG2H-5561	gmontag
FG6CVN-5561	gmontag
FT8J39-5561	gmontag
G6U6KA-5561	gmontag

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27 - Examination Questions	
WebCode Test	Response
G9BD99-5561	gmontag
G9PQLK-5561	gmontag
GALGEK-5562	gmontag
GMPPAG-5561	C:\Users\gmontag\Documents
H3X34J-5561	gmontag
HAVVCD-5562	C:\Users\gmontag\Documents\
HFM3VL-5562	[Participant did not return results for this question.]
HGE2AK-5561	gmontag
HMQYPK-5561	c:\Users\gmontag\Documents\
HTB6DE-5562	gmontag
HVJ3Y9-5561	gmontag
HYHLVF-5561	gmontag
J3FCTE-5561	My Computer\C:\Users\gmontag\Documens\DocumentsRTF.
J49DM9-5561	gmontag
JFURCD-5561	gmontag
JPAH22-5562	gmontag
JXAZDE-5561	gmontag
JXHVGK-5561	gmontag
K3WXT8-5562	gmontag
KA94ED-5562	C:\Users\gmontag\Documents\
KCQD3T-5561	gmontag

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27 - Examination Questions	
WebCode Test	Response
KMHPR4-5561	gmontag
LBJ6ZC-5562	gmontag
LMDLPD-5561	montag documents folder
LRM3Y2-5562	gmontag
LWKE3D-5561	gmontag
MCQ8YF-5561	gmontag
MD8AY2-5561	gmontag
MK6QJE-5561	C:\Users\gmontag\Documents\Document.rtf
MR47EE-5562	gmontag
MV6A9L-5561	gmontag
N9Q2B2-5562	gmontag
NH83FA-5562	gmontag (C:\Users\gmontag\Documents\Document.rtf)
NNQD78-5561	gmontag
NPUPBF-5562	gmontag
NQ7BB3-5561	Accessed "Document.rtf" from user gmontag's document folder
P3EHK8-5562	gmontag\Documents
P3ER7C-5561	gmontag
P6NMZG-5561	C:\Users\gmontag\Documents
PE6G4X-5561	gmontag
PYKJC4-5561	gmontag
Q4ZTN7-5562	gmontag

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27 - Examination Questions	
WebCode Test	Response
Q73JRN-5561	gmontag
RBARA4-5561	gmontag
RE7DZL-5561	gmontag
RUTBQ8-5561	gmontag
RY7A78-5561	gmontag
RZKKZ7-5562	C:\Users\gmontag\Documents
T9UAE6-5561	gmontag
TH2XG4-5562	Not in scope
TTGXLB-5561	gmontag
U8973A-5561	FireDepartametWorkstation/Users/gmontag/Documents/Document.rtf
UEQLM7-5561	gmontag
UEWNPX-5561	gmontag
UGNM4W-5561	gmontag
ULHG2X-5561	gmontag
UPTW39-5562	C:\Users\gmontag\Documents\
UUA6Q9-5561	gmontag
UZQMYA-5562	gmontag
V66XC6-5562	gmontag
V82HUJ-5561	C:\Users\gmontag\Documents\Document.rtf
VXLE96-5561	C:\Users\gmontag\Documents\Document.rtf
VYTW7Z-5561	[Participant did not return results for this question.]

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27 - Examination Questions	
WebCode Test	Response
W447WA-5561	gmontag
WB84Q8-5561	C:\Users\gmontag\Documents
WBPY99-5561	gmontag
WFVT36-5561	C:\Users\gmontag\Documents
WH6VY2-5561	gmontag
WL2PNP-5561	gmontag documents folder
WL4AK7-5562	gmontag
WQGWCP-5562	Gmontag
X2AZR3-5561	gmontag
X3NFAB-5561	file: Document.rtf user folder accessed "Documents" path: C:\Users\gmontag\Documents\Document.rtf
X62GKW-5561	gmontag
X84MXA-5561	Documents, Pictures, User Data
XDQM3P-5561	C:\Users\gmontag\Documents\Document.rtf
XDT8Y6-5562	C:\Users\gmontag\documents - specifically the document.rtf file. The user "gmontag" is the answer.
XLP32A-5562	Document.rtf
XQXJAX-5561	gmontag
Y2PJCZ-5561	gmontag
Y8WZT2-5561	gmontag
YZK9WX-5561	gmontag
Z4GR62-5562	gmontag
Z4PAVK-5561	gmontag

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27 - Examination Questions	
WebCode Test	Response
ZBUQRZ-5561	gmontag
ZEU2MZ-5562	gmontag
ZF7RW4-5561	C:\Users\gmontag\Documents\
ZN4C6R-5561	gmontag
ZQ4URL-5562	Document.rtf, belonging to the user gmontag, which is located at the path: C:\Users\gmontag\Documents\Document.rtf
ZU7QJ2-5561	gmontag
ZWABN2-5562	My Computer (Computer)\C:\Users\gmontag\Documents gmontag

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 27 - Examination Questions

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

Consensus Result:

gmontag and variations representing similar information.

Manufacturer's Response Explanation:

A review of the NTUSER.DAT user registry hive for the jbeatty account can identify most recently used (MRU) files and paths.

Manufacturer's Response Illustration:

RegRipper parse of jbeatty NTUSER.DAT

```

LastVisitedPidlMRU
LastWrite time: 2024-03-13 00:43:34Z
Note: All value names are listed in MRUListEx order.

  PickerHost.exe - My Documents
  chrome.exe - My Computer\C:\Users\jbeatty\AppData\Local\Google\Chrome\User Data
  {B5E83989-4076-4ED0-A33E-9B8E9870B07F} - My Computer\C:\Users\gmontag\Documents

OpenSavePidlMRU
LastWrite time: 2024-03-13 00:43:34Z
OpenSavePidlMRU\*
LastWrite Time: Wed Mar 13 00:43:34 2024
Note: All value names are listed in MRUListEx order.

  My Documents\beatty.jpg
  My Computer\C:\Users\jbeatty\AppData\Local\Google\Chrome\User Data\ac
  My Computer\C:\Users\gmontag\Documents\Document.rtf

```

Registry Explorer parse of jbeatty NTUSER.DAT

Type viewer	Slack viewer	Binary viewer
Value name	File1	
Value type	RegSz	
Value	C:\Users\gmontag\Documents\Document.rtf	
Raw value	43-00-3A-00-5C-00-55-00-73-00-65-00-72-00-73-00-5C-00-67-00-6D-00-6F-00	
oftware\Microsoft\Windows\CurrentVersion\Applets\Wordpad\Recent File List		
jbeatty.NTUSER.DAT Last write: 2024-03-11 04:09:06 1 of 1 values shown (100.00%)		

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28 - Examination Questions

Question 28: Provide the filetype (MIME Type) for the file with SHA256 hash 67a6fa82325141eaca921ca7a64fe6e6cafb6fb86bd3ba278ccced0d6925986d.

Manufacturer's SQLite or SQLite 3 (Database)

Response:

WebCode Test	Response
28NKRK-5561	.txt
2BXEJB-5561	back up file / back up copy of a file
2EUC34-5562	application/x-sqlite3
2UJN7X-5562	Database/bak (sqlitedb)
2XN36N-5561	SQLite Database
36GUPN-5561	.bak backup file for an sqlite database
3CH2GJ-5562	[Participant did not return results for this question.]
3DBUC3-5561	text/plain
3K9LKW-5561	SQLITE
3LM236-5561	SQLite Database file
483YXK-5561	application/x-sqlite3
49DVEJ-5561	Filename : store.bak, Filetype : backup file
4K6LX2-5561	SQLite database
4L6CCW-5562	sqlite database
4P6N9W-5561	SQLITE Database
4THJUL-5562	[Participant did not return results for this question.]
4XXRHK-5561	The file store.bak is a backup file for a SQLite database
4Z77PR-5561	SQLite 3 database
6KNFKX-5561	SQLite database

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28 - Examination Questions	
WebCode Test	Response
6RLGDW-5561	ProgramData\USOPrivate\UpdateStore\store.bak - Extension is ".bak" - file header appears to be "SQLite format 3" (opens as SQLite database)
78YYBQ-5561	application/octet-stream
7M6APW-5561	that specific hash is related to a file named "store.bak," a SQLITE Database
7WAG6W-5561	sqlitedb
7WV3RK-5561	.bak
8ED4K3-5562	SQLite Database(application/x-sqlite3)
8LRYCP-5561	SQLITE Database file - .bak
8P8Q2X-5561	.bak
8RFV4L-5561	.bak
8W78WW-5562	sqlitedb
98N78Y-5561	.mp4
9J6THK-5561	Application/x-sqlite3
9QMRX6-5561	application/x-sqlite3
9XFKVP-5562	Bak
AN93XR-5561	SQL Database (Backup File)
AXDBED-5562	Backup file
AXFVBT-5561	x-sqlite-3
B2ACZR-5562	application/x-sqlite3
BA4FBG-5561	.bak
BPGNBK-5562	application/x-sqlite3
BVMG7F-5561	.bak

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28 - Examination Questions	
WebCode Test	Response
BXTTXP-5561	application/x-sqlite3
CCXUMK-5561	SQLite 3
CPQ4TQ-5561	application/octet-stream
D3A9ER-5561	store.bak, backup/SQLite DB, Application/octet-stream
D3MR2K-5561	SQLITE Database (SQLite format 3)
D7C7PK-5562	Filename: store.bak MIME type: bak
D8QG3R-5561	SQLite Database
DCKG7E-5561	.bak file which is a SQLite database file.
DKUYDR-5561	.bak
DKVPRL-5562	SQLITE Database
DPA82Q-5561	.bak sqlitedb
DTN8XH-5562	SQLite database
DXKMTK-5561	Application
EJD6CG-5561	SQLITE Database
EJK3WT-5561	SQLite database
EMTM9G-5561	SQLite Database
F3TPTL-5561	[Participant did not return results for this question.]
F7NG2H-5561	Video
FG6CVN-5561	File Type: SQLITE Database File Name: store.bak
FT8J39-5561	store.bak - file type - SQLite, SQLite database 3, sqlitedb
G6U6KA-5561	SQLite database

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28 - Examination Questions	
WebCode Test	Response
G9BD99-5561	SQLite
G9PQLK-5561	Sqlite db backup file (.bak)
GALGEK-5562	application/xsqlite3 .bak file
GMPPAG-5561	SQLITE Database
H3X34J-5561	application/x-sqlite3
HAVVCD-5562	application/x-sqlite3
HFM3VL-5562	[Participant did not return results for this question.]
HGE2AK-5561	SQLITE DATABASE (MIME Type = "application/octet-stream")
HMQYPK-5561	Database File / SQLite Format 3
HTB6DE-5562	SQLite 3 (application/vnd.sqlite3)
HVJ3Y9-5561	SQL Server Database Backup File
HYHLVF-5561	File not found
J3FCTE-5561	Name:/img_Fire%20Department%20Workstation-001.e01/ProgramData/USOPrivate/UpdateStore/store.bak, Type: File System, MIME Type: application/x-sqlite3, MD5: ecaded9d6d2888292402cd4e231eda29, SHA-256:67a6fa82325141eaca921ca7a64fe6e6cafb6fb86bd3ba278ccced0d6925986d
J49DM9-5561	application\x-sqlite3
JFURCD-5561	application/vnd.sqlite3 (.bak file for sqlite database)
JPAH22-5562	Application/x-sqlite3
JXAZDE-5561	SQLITE Database application/x-sqlite3
JXHV GK-5561	application/octet-stream
K3WXT8-5562	.bak file extension. Used to signify a back up copy of a file.
KA94ED-5562	application/x-sqlite3
KCQD3T-5561	SQLite format 3

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28 - Examination Questions	
WebCode Test	Response
KMHPR4-5561	SQLite
LBJ6ZC-5562	SQLITE Database
LMDLPD-5561	file extension = .bak. file name = store.bak
LRM3Y2-5562	.txt
LWKE3D-5561	SQLite Database
MCQ8YF-5561	application/octet-stream
MD8AY2-5561	SQLite Database
MK6QJE-5561	SQLite Database
MR47EE-5562	SQLITE Format 3 (53 51 4C 69) (store.bak)
MV6A9L-5561	SQLITE Database store.bak
N9Q2B2-5562	SQLite database (application/vnd.sqlite3)
NH83FA-5562	sqlitedb
NNQD78-5561	SQLite 3
NPUPBF-5562	.bak sqlitedb
NQ7BB3-5561	This hash is for the file "store.bak", which is a SQLite database file. \ProgramData\USOPrivate\UpdateStore\store.bak
P3EHK8-5562	application/x-sqlite3
P3ER7C-5561	SQLITE Database
P6NMZG-5561	application/x-sqlite3
PE6G4X-5561	.bak
PYKJC4-5561	.bak
Q4ZTN7-5562	SQLITE Database file - .bak

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28 - Examination Questions	
WebCode Test	Response
Q73JRN-5561	.bak
RBARA4-5561	SQLite 3 (file is store.bak)
RE7DZL-5561	application/x-sqlite3
RUTBQ8-5561	SQLITE Database (.bak)
RY7A78-5561	SQLITE Database
RZKKZ7-5562	SQLITE Database
T9UAE6-5561	application/vnd.sqlite3
TH2XG4-5562	application/vnd.sqlite3
TTGXLB-5561	application/octet-stream
U8973A-5561	SQL Server Database Backup file store.bak
UEQLM7-5561	store.bak (Sqlite database)
UEWNPX-5561	[Participant did not return results for this question.]
UGNM4W-5561	sqlitedb
ULHG2X-5561	.doc
UPTW39-5562	application/x-sqlite3
UUA6Q9-5561	SQLite Database
UZQMYA-5562	SQL
V66XC6-5562	Application/ X-sqlite 3
V82HUJ-5561	SQLite
VXLE96-5561	application/x-sqlite3
VYTW7Z-5561	[Participant did not return results for this question.]

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28 - Examination Questions	
WebCode Test	Response
W447WA-5561	.bak (backup file for SQL database [store.db])
WB84Q8-5561	application/x-sqlite3
WBPY99-5561	.bak (back-up copy of an SQLITE database file)
WFVT36-5561	Filetype SQLite format 3 (Application/x-sqlite3 or Application/vnd.sqlite3)
WH6VY2-5561	Website
WL2PNP-5561	application/x-sqlite3
WL4AK7-5562	.bak - a SQLite 3.x db
WQGWCP-5562	Application/x-sqlite3
X2AZR3-5561	sqlitedb
X3NFAB-5561	store.bak SQLite (application/octet-stream)
X62GKW-5561	SQLite
X84MXA-5561	MIME Type: application/x-sqlite3
XDQM3P-5561	SQLITE Database / .bak
XDT8Y6-5562	SQLite database file, filename "store.bak"
XLP32A-5562	store.bak(backup file, SQLite)
XQXJAX-5561	This is a SQLite database file which appears to be a backup file
Y2PJCZ-5561	SQLITE Database
Y8WZT2-5561	application/x-sqlite3
YZK9WX-5561	application/vnd.sqlite3
Z4GR62-5562	SQLite database 3.x (application/vnd.sqlite3 also known as the deprecated application/x-sqlite3) **SEE Additional Comments**
Z4PAVK-5561	SQLite

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28 - Examination Questions	
WebCode Test	Response
ZBUQRZ-5561	application/x-sqlite3
ZEU2MZ-5562	SQLITE bak
ZF7RW4-5561	application/x-sqlite3
ZN4C6R-5561	application/x-sqlite3
ZQ4URL-5562	x-sqlite3
ZU7QJ2-5561	application/x-sqlite3
ZWABN2-5562	bak SQLITE backup file

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 28 - Examination Questions

Question 28: Provide the filetype (MIME Type) for the file with SHA256 hash 67a6fa82325141eaca921ca7a64fe6e6cafb6fb86bd3ba278ccced0d6925986d.

Consensus Result:

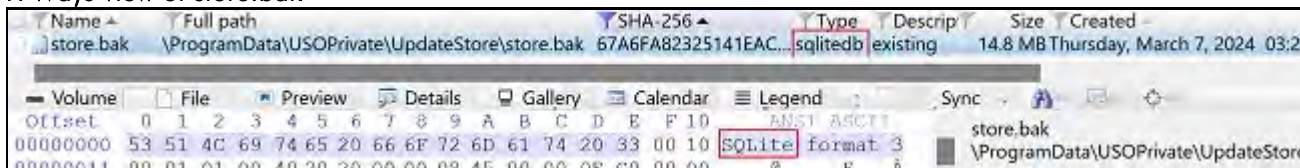
SQLite and variations representing similar information.

Manufacturer's Response Explanation:

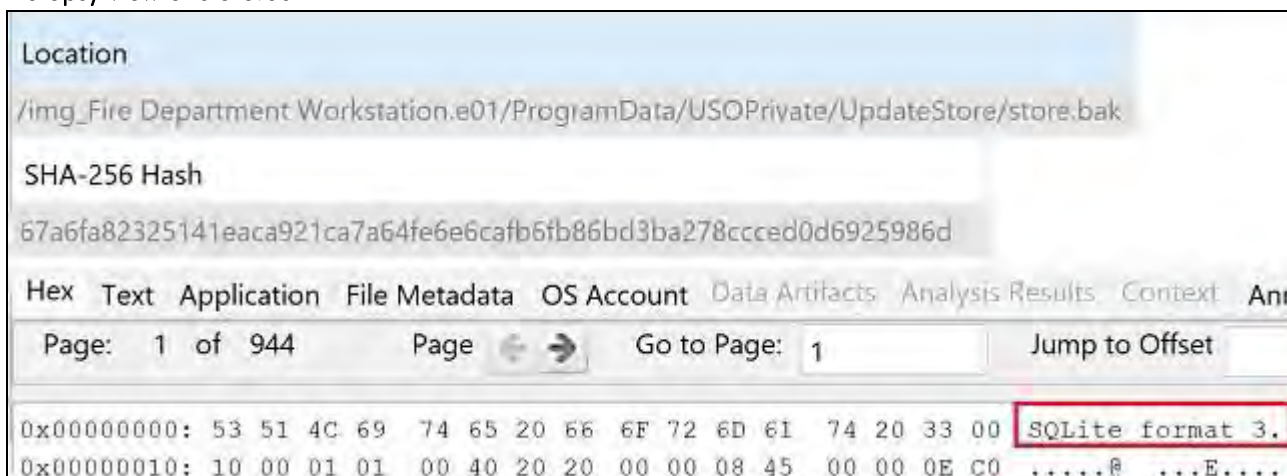
C:\ProgramData\USOPrivate\UpdateStore\store.bak has the SHA256 hash specified in the question. This file has a .bak extension (backup file) which was mentioned by 40 participants; however, its internal file signature (header) identifies it as an SQLite database. The purpose of this question was to prompt the participant to identify the type of file by its contents, not solely by its filename.

Manufacturer's Response Illustration:

X-Ways view of store.bak



Autopsy view of store.bak



Other Responses:

16 participants responded ".bak" or "backup." The .bak file extension is not the file type itself.

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 29 - Examination Questions

Question 29: Provide the path and filename of the encrypted file in one of the user's "Documents" directory.

Manufacturer's C:\Users\jbeatty\Documents\book.zip

Response:

WebCode Test	Response
28NKRK-5561	Users\jbeatty\Documents\book.zip
2BXEJB-5561	\Fire Department Workstation\Users\jbeatty\Documents\book.zip
2EUC34-5562	C:\Users\jbeatty\Documents\book.zip
2UJN7X-5562	2 files identified - Users\jbeatty\Documents\book.zip and \Users\mboone\Documents\f_6310.1_arson_and_explosives_training_request_for_non-atf_employees.pdf
2XN36N-5561	C:\Users\jbeatty\Documents\book.zip
36GUPN-5561	\Users\jbeatty\Documents\book.zip
3CH2GJ-5562	[Participant did not return results for this question.]
3DBUC3-5561	[root]/Users/jbeatty/Documents/book.zip
3K9LKW-5561	Fire Department Workstation-001.e01/NONAME [NTFS]/[root]/Users/jbeatty/Documents/book.zip
3LM236-5561	\jbeatty\Documents\book.zip
483YXK-5561	C:\Users\jbeatty\Documents\book.zip
49DVEJ-5561	[root]\Users\jbeatty\Documents\book.zip
4K6LX2-5561	\Users\jbeatty\Documents\book.zip
4L6CCW-5562	\User\jbeatty\Documents\book.zip
4P6N9W-5561	/img_Fire%20Department%20Workstation-001.e01/Users/jbeatty/Documents/book.zip
4THJUL-5562	[Participant did not return results for this question.]
4XXRHK-5561	Fire Department Workstation\Users\jbeatty\Documents\book.zip
4Z77PR-5561	Users\jbeatty\Documents\book.zip
6KNFKX-5561	C:\Users\jbeatty\Documents\book.zip

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 29 - Examination Questions	
WebCode Test	Response
6RLGDW-5561	\Users\jbeatty\Documents\book.zip
78YYBQ-5561	\Users\jbeatty\Documents\book.zip
7M6APW-5561	[root]\Users\jbeatty\Documents\book.zip
7WAG6W-5561	users\jbeatty\Documents\book.zip
7WV3RK-5561	\Users\jbeatty\Documents\book.zip
8ED4K3-5562	C:\Users\jbeatty\Documents\book.zip
8LRYCP-5561	Users/jbeatty/Documents/book.zip
8P8Q2X-5561	Fire%20Department%20Workstation-001.e01/NONAME [NTFS]/[root]/Users/jbeatty/Documents/book.zip
8RFV4L-5561	Users\mboone\Documents\f_6310_1_arson_and_explosives_training_request_for_non_atf_employees.pdf
8W78WW-5562	\Users\jbeatty\Documents\book.zip
98N78Y-5561	\Users\jbeatty\Documents\book.zip book.zip
9J6THK-5561	\Users\jbeatty\Documents\book.zip\cookbook.pdf
9QMRX6-5561	C:\Users\jbeatty\Documents\book.zip
9XFKVP-5562	Path- Fire20Workstation-001.E01 - Entire Disk (Microsoft NTFS, 39.13 GB)\Users\jbeatty\Documents\book.zip Filename: book.zip
AN93XR-5561	/Users/jbeatty/Documents/books.zip
AXDBED-5562	C:\Users\jbeatty\Documents\book.zip
AXFVBT-5561	/Users/jbeatty/Documents/book.zip
B2ACZR-5562	Users\jbeatty\Documents\book.zip
BA4FBG-5561	\Users\jbeatty\Documents\book.zip
BPGNBK-5562	\Users\jbeatty\Documents\book.zip
BVMG7F-5561	Fire%20Department%20Workstation-001.E01-Entire Disk (Microsoft NTFS, 39.13 GB)\Users\jbeatty\Documents\book.zip

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 29 - Examination Questions	
WebCode Test	Response
BXTTXP-5561	Users\jbeatty\Documents\book.zip
CCXUMK-5561	Fire_20Department_20Workstation-001.e01\Root\Users\jbeatty\Documents\book.zip
CPQ4TQ-5561	\Users\jbeatty\Documents\book.zip
D3A9ER-5561	Users\jbeatty\Documents\book.zip, book.zip
D3MR2K-5561	Path: Fire20Workstation-001.e01\NONAME [NTFS]/[root]/Users/jbeatty/Documents/book.zip, Filename: book.zip
D7C7PK-5562	Filepath: \Users\jbeatty\Documents\book.zip Filename: book.zip
D8QG3R-5561	Fire%20Department%20Workstation-001.e01\Root\Users\jbeatty\Documents\book.zip
DCKG7E-5561	\Users\jbeatty\Documents\book.zip
DKUYDR-5561	C:\Users\jbeatty\Documents\book.zip
DKVPRL-5562	/Users/jbeatty/Documents/book.zip
DPA82Q-5561	\Users\jbeatty\Documents\book.zip
DTN8XH-5562	Users\jbeatty\Documents\book.zip
DXKMTK-5561	Fire%20Department%20Workstation-001.E01 - Entire Disk (Microsoft NTFS, 39.13 GB)\Users\jbeatty\Documents\book.zip
EJD6CG-5561	Fire%20Department%20Workstation-001.E01 - Entire Disk (Microsoft NTFS, 39.13 GB)\Users\jbeatty\Documents\book.zip
EJK3WT-5561	[File System Root]/Users/jbeatty/Documents/book.zip Book.zip
EMTM9G-5561	\Users\jbeatty\Documents\book.zip
F3TPTL-5561	Users\mboone\Documents\f_6310._1_arson_and_explosives_training_request_for_non-atf_employees.pdf
F7NG2H-5561	Fire%20Department%20Workstation-001.E01 - Entire Disk (Microsoft NTFS, 39.13 GB)\Users\jbeatty\Documents\book.zip book.zip
FG6CVN-5561	File Path: Fire%20Department%20Workstation-001.E01 - Entire Disk (Microsoft NTFS, 39.13 GB)\Users\jbeatty\Documents\book.zip File Name: book.zip
FT8J39-5561	Fire Department Workstation\Users\jbeatty\Documents\book.zip
G6U6KA-5561	\Users\jbeatty\Documents\book.zip

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 29 - Examination Questions	
WebCode Test	Response
G9BD99-5561	Users\jbeatty\Documents\book.zip
G9PQLK-5561	\Users\jbeatty\Documents\book.zip
GALGEK-5562	Users\jbeatty\Documents\book.zip
GMPPAG-5561	C:\Users\jbeatty\Documents\book.zip
H3X34J-5561	\Users\jbeatty\Documents\book.zip
HAVCD-5562	C:\Users\jbeatty\Documents\book.zip
HFM3VL-5562	[Participant did not return results for this question.]
HGE2AK-5561	Path: C:/Users/jbeatty/Documents/book.zip Name: book.zip
HMQYPK-5561	\\Users\jbeatty\Documents\book.zip
HTB6DE-5562	\Users\jbeatty\Documents\book.zip
HVJ3Y9-5561	Fire%20Department%20Workstation-001.E01 - Entire Disk (Microsoft NTFS, 39.13 GB)\Users\jbeatty\Documents\book.zip
HYHLVF-5561	Fire%20Department%20Workstation-001.E01 - Entire Disk (Microsoft NTFS, 39.13 GB)\Users\jbeatty\Documents\book.zip\cookbook.pdf
J3FCTE-5561	/img_Fire%20Department%20Workstation001.e01/Users/jbeatty/Documents/book.zip
J49DM9-5561	C:\Users\jbeatty\Documents\book.zip
JFURCD-5561	\Users\jbeatty\Documents\book.zip
JPAH22-5562	C:\Users\jbeatty\Documents\book.zip
JXAZDE-5561	/img_Fire%20Department%20Workstation-001(1).e01/Users/jbeatty/Documents/book.zip
JXHVGK-5561	roof\Users\jbeatty\Documents\book.zip
K3WXT8-5562	Users/jbeatty/Documents/book.zip/cookbook.pdf
KA94ED-5562	\Users\jbeatty\Documents\book.zip
KCQD3T-5561	C:\Users\jbeatty\Documents\book.zip

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 29 - Examination Questions	
WebCode Test	Response
KMHPR4-5561	\Users\jbeatty\Documents\book.zip
LBJ6ZC-5562	Fire%20Department%20Workstation-001.E01 - Entire Disk (Microsoft NTFS, 39.13 GB)\Users\jbeatty\Documents\book.zip, book.zip
LMDLPD-5561	Users\mboone\Documents\f_6310._1_arson_and_explosives_training_request_for_non-atf_employees.pdf
LRM3Y2-5562	Users\jbeatty\Documents\book.zip
LWKE3D-5561	Fire%20Department%20Workstation-001.E01 - Entire Disk (Microsoft NTFS, 39.13 GB)\Users\jbeatty\Documents\book.zip
MCQ8YF-5561	[root]\Users\jbeatty\Documents\book.zip
MD8AY2-5561	Users\jbeatty\Documents\book.zip; book.zip
MK6QJE-5561	C:\Users\jbeatty\Documents\book.zip
MR47EE-5562	\Users\jbeatty\Documents\book.zip
MV6A9L-5561	Users/jbeatty/Documents/book.zip
N9Q2B2-5562	C:\Users\jbeatty\Documents\book.zip
NH83FA-5562	Filepath: \Users\jbeatty\Documents Filename: book.zip
NNQD78-5561	Users\jbeatty\Documents\book.zip
NPUPBF-5562	\Users\jbeatty\Documents\book.zip
NQ7BB3-5561	Users\jbeatty\Documents\book.zip
P3EHK8-5562	/Users/jbeatty/Documents/book.zip
P3ER7C-5561	/root/Users/jbeatty/Documents/book.zip
P6NMZG-5561	\Users\jbeatty\Documents\book.zip
PE6G4X-5561	Fire%20Department%20Workstation-001.E01 - Entire Disk (Microsoft NTFS, 39.13 GB)\Users\jbeatty\Documents\book.zip, book.zip
PYKJC4-5561	\User\Documents\book.zip
Q4ZTN7-5562	Users/jbeatty/Documents/book.zip

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 29 - Examination Questions	
WebCode Test	Response
Q73JRN-5561	users\jbeatty\Documents\book.zip
RBARA4-5561	/[root]/Users/jbeatty/Documents/book.zip
RE7DZL-5561	Fire%20Department%20Workstation-001.E01 - Entire Disk (Microsoft NTFS, 39.13 GB)\Users\jbeatty\Documents\book.zip
RUTBQ8-5561	Users/jbeatty/Documents/book.zip
RY7A78-5561	Users\jbeatty\Documents\book.zip
RZKKZ7-5562	C:\Users\jbeatty\Documents\book.zip
T9UAE6-5561	C:\Users\jbeatty\Documents\book.zip
TH2XG4-5562	Not in scope
TTGXLB-5561	C:\Users\jbeatty\Documents\book.zip
U8973A-5561	FireDepartametWorkstation/Users/jbeatty/Documents/book.zip
UEQLM7-5561	C:\Users\jbeatty\Documents\books.zip
UEWNPX-5561	\Users\jbeatty\Documents\book.zip
UGNM4W-5561	\Users\jbeatty\Documents\book.zip
ULHG2X-5561	Users\jbeatty\Documents\book.zip
UPTW39-5562	C:\Users\jbeatty\Documents\book.zip
UUA6Q9-5561	\Users\jbeatty\Documents\book.zip
UZQMYA-5562	Users\jbeatty\Documents\book.zip
V66XC6-5562	Users/Jbeatty/Documents/Book.zip/
V82HUJ-5561	Fire Department Workstation\Users\jbeatty\Documents folder\book.zip
VXLE96-5561	C:/Users/jbeatty/Documents/book.zip or /img_Fire20Workstation-001.e01/Users/jbeatty/Documents/book.zip
VYTW7Z-5561	[Participant did not return results for this question.]

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 29 - Examination Questions	
WebCode Test	Response
W447WA-5561	users\jbeatty\Documents\book.zip
WB84Q8-5561	C:\Users\jbeatty\Documents\book.zip
WBPY99-5561	Fire%20Department%20Workstation-001.E01 - Entire Disk (Microsoft NTFS, 39.13 GB)\Users\mboone\Documents\f_6310._1_arson_and_explosives_training_request_for_non-atf_employees.pdf
WFVT36-5561	C:\Users\jbeatty\Documents\book.zip
WH6VY2-5561	Fire%20Department%20Workstation-001.E01\Entire Disk (Microsoft NTFS, 39.13 GB)\Users\jbeatty\Documents\book.zip
WL2PNP-5561	/Users/jbeatty/Documents/book.zip
WL4AK7-5562	\Users\jbeatty\Documents\book.zip
WQGWCP-5562	Path: Users\jbeatty\Documents\book.zip Filename: book.zip
X2AZR3-5561	\Users\jbeatty\Documents\book.zip
X3NFAB-5561	path: C:\Users\jbeatty\Documents\book.zip filename: book.zip
X62GKW-5561	\Users\jbeatty\Documents\book.zip
X84MXA-5561	Path: /Users/jbeatty/Documents/book.zip
XDQM3P-5561	C:\Users\jbeatty\Documents\book.zip
XDT8Y6-5562	\\Users\jbeatty\Documents\book.zip
XLP32A-5562	\Users\jbeatty\Documents\book.zip
XQXJAX-5561	Users\mboone\Documents\f_6310._1_arson_and_explosives_training_request_for_non-atf_employees.pdf f_6310._1_arson_and_explosives_training_request_for_non-atf_employees.pdf
Y2PJCZ-5561	/Users/jbeatty/Documents/book.zip cookbook.pdf
Y8WZT2-5561	Users/jbeatty/Documents/book.zip
YZK9WX-5561	Fire20Workstation-001.e01\Root\Users\jbeatty\Documents\book.zip
Z4GR62-5562	C:\Users\jbeatty\Documents\book.zip
Z4PAVK-5561	Fire Department Workstation\Users\jbeatty\Documents\book.zip

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 29 - Examination Questions	
WebCode Test	Response
ZBUQRZ-5561	/img_Fire_20Department_20Workstation-001.e01/Users/jbeatty/Documents/book.zip
ZEU2MZ-5562	/Users/jbeatty/Documents/book.zip book.zip
ZF7RW4-5561	Users\jbeatty\Documents\book.zip
ZN4C6R-5561	\Users\jbeatty\Documents\book.zip
ZQ4URL-5562	Users\jbeatty\Documents\book.zip
ZU7QJ2-5561	\root\Users\jbeatty\Documents\book.zip
ZWABN2-5562	\Users\jbeatty\Documents\book.zip

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 29 - Examination Questions

Question 29: Provide the path and filename of the encrypted file in one of the user's "Documents" directory.

Consensus Result:

C:\Users\jbeatty\Documents\book.zip and variations representing similar information.

Manufacturer's Response Explanation:

This file is discoverable by listing all files, filtering the path to contain "Documents", and sorting by entropy. Opening this file with an archive utility will prompt the user for a password.

Manufacturer's Response Illustration:

Encase table view showing book.zip

	Entropy	Item Path
<input type="checkbox"/> 1	7.9972084	Fire Department Workstation\Users\jbeatty\Documents\book.zip
<input type="checkbox"/> 2	7.9699547	Fire Department Workstation\Users\kshea\Documents\chicken-scallopini-5d8e2203db
<input type="checkbox"/> 3	7.8834309	Fire De
<input type="checkbox"/> 4	7.8357736	Fire De
<input type="checkbox"/> 5	7.8341948	Fire De
<input type="checkbox"/> 6	7.8312057	Fire De
<input type="checkbox"/> 7	7.8000148	Fire De
<input type="checkbox"/> 8	7.7888835	Fire De

View File Structure

This file has a "ZIP" signature. Continue parsing?

Password

A

OK Cancel

Fields Report

View Type Find

1 cookbook.pdf
218,319,020
33/12/2024 8:24 PM

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 30 - Examination Questions

Question 30: Provide the name of the file contained within the encrypted file in a user's "Documents" directory.

Manufacturer's cookbook.pdf

Response:

WebCode Test	Response
28NKRK-5561	cookbook.pdf
2BXEJB-5561	cookbook.pdf
2EUC34-5562	cookbook.pdf
2UJN7X-5562	Cookbook.pdf
2XN36N-5561	cookbook.pdf
36GUPN-5561	cookbook.pdf
3CH2GJ-5562	[Participant did not return results for this question.]
3DBUC3-5561	cookbook.pdf
3K9LKW-5561	cookbook.pdf
3LM236-5561	Cookbook.pdf
483YXK-5561	cookbook.pdf
49DVEJ-5561	cookbook.pdf
4K6LX2-5561	cookbook.pdf
4L6CCW-5562	cookbook.pdf
4P6N9W-5561	cookbook.pdf
4THJUL-5562	[Participant did not return results for this question.]
4XXRHK-5561	cookbook.pdf
4Z77PR-5561	cookbook.pdf
6KNFKX-5561	cookbook.pdf

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 30 - Examination Questions	
WebCode Test	Response
6RLGDW-5561	cookbook.pdf
78YYBQ-5561	cookbook.pdf
7M6APW-5561	cookbook.pdf
7WAG6W-5561	cookbook.pdf
7WV3RK-5561	cookbook.pdf
8ED4K3-5562	cookbook.pdf
8LRYCP-5561	Cookbook.pdf
8P8Q2X-5561	Fire%20Department%20Workstation-001.e01/NONAME [NTFS]/[root]/Users/[beatty/Documents/book.zip»cookbook.pdf
8RFV4L-5561	cookbook.pdf
8W78WW-5562	cookbook.pdf
98N78Y-5561	cookbook.pdf
9J6THK-5561	cookbook.pdf
9QMRX6-5561	cookbook.pdf
9XFKVP-5562	Cookbook.pdf
AN93XR-5561	cookbook.pdf
AXDBED-5562	cookbook.pdf
AXFVBT-5561	The Anarchist Cookbook
B2ACZR-5562	cookbook.pdf
BA4FBG-5561	cookbook.pdf
BPGNBK-5562	cookbook.pdf
BVMG7F-5561	cookbook.pdf

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 30 - Examination Questions	
WebCode Test	Response
BXTTXP-5561	cookbook.pdf
CCXUMK-5561	cookbook.pdf
CPQ4TQ-5561	cookbook.pdf
D3A9ER-5561	cookbook.pdf
D3MR2K-5561	cookbook.pdf
D7C7PK-5562	\\Users\jbeatty\Documents\book.zip\cookbook.pdf
D8QG3R-5561	cookbook.pdf
DCKG7E-5561	cookbook.pdf
DKUYDR-5561	Cookbook.pdf
DKVPRL-5562	cookbook.pdf
DPA82Q-5561	cookbook.pdf
DTN8XH-5562	cookbook.pdf
DXKMTK-5561	cookbook.pdf
EJD6CG-5561	cookbook.pdf
EJK3WT-5561	Cookbook.pdf
EMTM9G-5561	cookbook
F3TPL-5561	f_6310._1_arson_and_explosives_training_request_for_non-atf_employees.pdf
F7NG2H-5561	cookbook.pdf
FG6CVN-5561	file name: cookbook.pdf
FT8J39-5561	cookbook.pdf
G6U6KA-5561	cookbook.pdf

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 30 - Examination Questions	
WebCode Test	Response
G9BD99-5561	cookbook.pdf
G9PQLK-5561	cookbook.pdf
GALGEK-5562	cookbook.pdf
GMPPAG-5561	cookbook.pdf
H3X34J-5561	cookbook.pdf
HAVVCD-5562	cookbook.pdf
HFM3VL-5562	[Participant did not return results for this question.]
HGE2AK-5561	cookbook.pdf
HMQYPK-5561	cookbook.pdf
HTB6DE-5562	cookbook.pdf
HVJ3Y9-5561	cookbook.pdf
HYHLVF-5561	Cookbook.pdf
J3FCTE-5561	cookbook.pdf
J49DM9-5561	cookbook.pdf
JFURCD-5561	cookbook.pdf
JPAH22-5562	cookbook.pdf
JXAZDE-5561	cookbook.pdf
JXHVGK-5561	cookbook.pdf
K3WXT8-5562	cookbook.pdf
KA94ED-5562	Cookbook.pdf
KCQD3T-5561	cookbook.pdf

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 30 - Examination Questions	
WebCode Test	Response
KMHPR4-5561	cookbook.pdf
LBJ6ZC-5562	cookbook.pdf
LMDLPD-5561	f_6310._1_arson_and_explosives_training_request_for_non-atf_employees.pdf
LRM3Y2-5562	cookbook.pdf
LWKE3D-5561	Cookbook.pdf
MCQ8YF-5561	cookbook.pdf
MD8AY2-5561	cookbook.pdf
MK6QJE-5561	cookbook.pdf
MR47EE-5562	Cookbook.pdf
MV6A9L-5561	cookbook.pdf
N9Q2B2-5562	cookbook.pdf
NH83FA-5562	Cookbook.pdf
NNQD78-5561	cookbook.pdf
NPUPBF-5562	cookbook.pdf
NQ7BB3-5561	cookbook.pdf
P3EHK8-5562	cookbook.pdf
P3ER7C-5561	cookbook.pdf
P6NMZG-5561	cookbook.pdf
PE6G4X-5561	Cookbook.pdf
PYKJC4-5561	cookbook.pdf
Q4ZTN7-5562	Cookbook.pdf

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 30 - Examination Questions	
WebCode Test	Response
Q73JRN-5561	cookbook.pdf
RBARA4-5561	cookbook.pdf
RE7DZL-5561	cookbook.pdf
RUTBQ8-5561	cookbook.pdf
RY7A78-5561	cookbook.pdf
RZKKZ7-5562	cookbook.pdf
T9UAE6-5561	cookbook.pdf
TH2XG4-5562	Not in scope
TTGXLB-5561	Cookbook.pdf
U8973A-5561	cookbook.pdf
UEQLM7-5561	cookbook.pdf
UEWNPX-5561	Cookbook.pdf
UGNM4W-5561	cookbook.pdf
ULHG2X-5561	cookbook.pdf
UPTW39-5562	cookbook.pdf
UUA6Q9-5561	cookbook.pdf
UZQMYA-5562	cookbook.pdf
V66XC6-5562	cookbook.pdf
V82HUJ-5561	cookbook.pdf
VXLE96-5561	cookbook.pdf
VYTW7Z-5561	[Participant did not return results for this question.]

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 30 - Examination Questions	
WebCode Test	Response
W447WA-5561	cookbook.pdf
WB84Q8-5561	cookbook.pdf
WBPY99-5561	f_6310._1_arson_and_explosives_training_request_for_non-atf_employees.pdf
WFVT36-5561	cookbook.pdf
WH6VY2-5561	cookbook.pdf
WL2PNP-5561	cookbook.pdf
WL4AK7-5562	cookbook.pdf
WQGWCP-5562	cookbook.pdf
X2AZR3-5561	cookbook.pdf
X3NFAB-5561	cookbook.pdf
X62GKW-5561	cookbook.pdf
X84MXA-5561	cookbook.pdf
XDQM3P-5561	cookbook.pdf
XDT8Y6-5562	cookbook.pdf
XLP32A-5562	cookbook.pdf
XQXJAX-5561	cookbook.pdf
Y2PJCZ-5561	Cookbook.pdf
Y8WZT2-5561	cookbook.pdf
YZK9WX-5561	cookbook.pdf
Z4GR62-5562	cookbook.pdf
Z4PAVK-5561	cookbook.pdf

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 30 - Examination Questions	
WebCode Test	Response
ZBUQRZ-5561	cookbook.pdf
ZEU2MZ-5562	cookbook.pdf
ZF7RW4-5561	cookbook.pdf
ZN4C6R-5561	cookbook.pdf
ZQ4URL-5562	cookbook.pdf
ZU7QJ2-5561	cookbook.pdf
ZWABN2-5562	coobook.pdf

Computer Hard Drive - Windows Analysis Results

TABLE 1: Computer Hard Drive - Windows Analysis Results

Question 30 - Examination Questions

Question 30: Provide the name of the file contained within the encrypted file in a user's "Documents" directory.

Consensus Result:

cookbook.pdf

Manufacturer's Response Explanation:

The filenames of files contained within encrypted zip archives are stored in plaintext and are readable without decrypting the file.

Manufacturer's Response Illustration:

Encase table view showing book.zip

	Entropy	Item Path
<input type="checkbox"/> 1	7.9972084	Fire Department Workstation\Users\jbeatty\Documents\book.zip
<input type="checkbox"/> 2	7.9699547	Fire Department Workstation\Users\kshea\Documents\chicken-scallopi-5c
<input type="checkbox"/> 3	7.8834309	Fire Depar
<input type="checkbox"/> 4	7.8357736	Fire Depar
<input type="checkbox"/> 5	7.8341948	Fire Depar
<input type="checkbox"/> 6	7.8312057	Fire Depar
<input type="checkbox"/> 7	7.8000148	Fire Depar
<input type="checkbox"/> 8	7.7000000	Fire Depar

View File Structure

This file has a "ZIP" signature. Continue parsing?

Password

A

OK Cancel

Fields Report T

View Type Find

cookbook.pdf

18,319,020

3/12/2024 8:24 PM

Additional Comments

TABLE 3

WebCode Test	Additional Comments
2UJN7X- 5562	Question 33, no answer was identified
3CH2GJ- 5562	33) We are unable to locate "1m3r1xbw8wzb1.jpg" with our current tools. 38) All of the instances we found had special characters that replaced the vowels but the last vowel had not been altered.
6RLGDW- 5561	The wording of question 2 is confusing. The SHA1 of the entire E01 file is already provided in the exam instructions, so I'm assuming the question is asking for the internal E01 data (that's what I provided). The wording of question 9 is confusing. What is meant by the "owner" of a text file? Text files do not have metadata or owners, and the file is stored at the root of C:\. I'm assuming the question is asking who may have created and/or accessed the file? I went off a LNK file in the smcnamara user folder. The wording of question 28 is also confusing. What is meant by "filetype (MIME Type)"? Several possible answers, and .bak files are usually proprietary filetypes.
98N78Y- 5561	I was unable to boot the image on VM because the system was corrupted which would help me to find some answers.
CPQ4TQ- 5561	Question #4- Axiom reported the OS as Windows 11 (it was parsed correctly in the File System view). Questions #29/#30- Axiom had one (1) exception and would not process cookbook.pdf. It noted cookbook.pdf was present and the file path showing it came from book.zip. FTK Lab correctly processed book.zip as an encrypted file.
DKVPRL- 5562	Regarding question 11: Windows terminal services event log event description fields are misleading. The user tgavin has never actually remotely logged in to the computer, he only attempted to. EventID 1149 (which was found) is not necessarily a successful login, it just means the client is connected for an RDP login attempt. An actual successful authentication is EventID 4624, which however was not found in the log file.
DTN8XH- 5562	Notes from the colleague who did Imaging / Processing:- There were no notes on the imaging process of the computer or photos of the exhibit. The image created wasn't a physical image of the computer, there was no explanation of why this was done and what data might have been missed as a consequence. Notes from the Investigator - Thank you for the other pics.
EMTM9G- 5561	Thank you for your time.
F3TPL- 5561	Question #28- Magnet Axiom did not generate Sha256 values. Ingested the file into Autopsy and could not locate the file with the provided hash.
HFM3VL- 5562	33).What is the full path (partition name\parent directory\file) for 1m3r1xbw8wzb1.jpg? Cannot locate this file on the E01 forensic image of the USB drive. Performed several keyword searches with different configurations and permutations in anticipation that it has been erroneously spelt - no matching results found - possibly an error with this question?

TABLE 3

WebCode Test	Additional Comments
HGE2AK-5561	<p>Question 10 is a bit vague regarding which specific attributes the test is looking for. There are several different types of NTFS "file attributes" so I included the Standard Information attributes listed and main File Name attributes.</p> <p>Question 25 is misleading because two PNG files (img_flyers.png & img_flyers@2x.png) exist on the volume in allocated space which match the exact description. I was able to find a duplicate of "img_flyers@2x.png" in unallocated space by carving, however I'm not sure that doing so was really necessary to answer the question. Unless I missed a different picture saying "Make your own focaccia" in red text somewhere.</p> <p>Question 28 was confusing because the file in question (store.bak) is a SQL Database backup file, which doesn't have its own MIME type. You would just use "application/octet-stream".</p>
J3FCTE-5561	<p>According to Windows prefetch, how many times was the calculator app executed? I have a comment on this question: The program Magnet Axioma Version 8.2.0.40565 and Cellebrite Inseyst Physical Analyzer Versioni 10.2.101.352 gave us the results that the calculator is executed only once (1), While Autopsy and Forensic Explorer give us the result that the calculator is executed seven (7) times.</p>
LBJ6ZC-5562	<p>Question 4: In the Registry, it shows Windows 10; however, the build number 23H2 indicates Windows 11. Question 25: Forensic tools did not find this particular text in the unallocated space of the subject volume, however, picture containing this text was found in: /Program Files/Adobe/Acrobat DC/Acrobat/WebResources/Resource0/static/js/plugins/aicuc/images/themeless_Reader/img_flyers@2x.png. Question 32: Some forensic tools found remnants of a FAT32 volume called "STUFF" If we count this volume, the second volume would be NTFS. However, since this space was categorized as unallocated, the second volume, based on sector order, is exFAT.</p>
MCQ8YF-5561	<p>Please be aware that some questions provided have ambiguous, broad, or less than specific answers that could lead to a wide variance of responses.</p> <p>Some examples include: 14 - there are multiple possible responses to include: quote, quote + author, quote + author + other text, 22- this is a very broad 2 part question in which somewhat open ended responses are likely</p>
MR47EE-5562	<p>It is very difficult to interpret the statements without a properly translation into our mother language. It is very easy to get confused and to give a wrong answer due to a bad interpretation of the real purpose of the question.</p>
P6NMZG-5561	<p>For question [18] "For the email message containing the keyword "trychtichlorate", provide the sender's email address." I was unable to identify any keywords with this phrase. For question [8] the original question i had was "Provide the BSSID (network name) of the Wi-Fi hotspot to which this computer was connected.", when answering the question that appeared to have changed to "Provide the SSID (network name) of the Wi-Fi hotspot to which this computer was connected." - this change had not been made clear.</p>
V66XC6-5562	<p>Question 33 - I Searched for the file and the file name in hex (31 00 6D 00 33 00 72) and located it at sector 8368. The volume is a FAT32 volume that is not recognized. Possible directory name of STUFF which is located in a sector near the file.</p>
YTW7Z-5561	<p>Had two hours time to do :/</p>

TABLE 3

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

TABLE 3

WebCode Test	Additional Comments
Z4GR62-5562	<p>4) The operating system registry values show the following: ProductName: Windows 10 Pro, EditionID: Professional, CurrentVersion: 6.3, DisplayVersion: 23H2. The Windows 11 2023 Update (also known as version 23H2 and codenamed "Sun Valley 3") is the second update to Windows 11. Windows 11 is the first time Microsoft release a new version of windows but continues to use the previous "ProductName" (Windows 10 Pro) value in the registry. 5) The MS Domain Controller that the computer has joined is "EMERGENCYSERVIC" but the full qualified domain name is "EmergencyServices.Winchestertonfieldville.org." 10) Note the term "filesystem attributes" can have different meaning depending on ones training, the digital forensic tool(s) used, or even the interpretation of the word attributes. For an example this file on an NTFS file system contains "General attributes", "DOS attributes", "Date and time attributes {classic Modify/Access/Create}", "NTFS attributes" and "NTFS access control attributes". My answer for this question used the "DOS attributes" and the "NTFS attributes" if any of the additional attributes were needed, I can provide them. 13) There are three file containing the keyword "flammulated"? two are active the third is in the Recycle Bin.</p> <ul style="list-style-type: none"> - ProgramData/Microsoft/Search/Data/Applications/Windows/Windows. - Users/mohalloran/Pictures/DSC_0921.jpg. - \$Recycle.Bin/S-1-5-21-2298470282-2867887670-580413564-1117/\$RCZUXP4.jpg. <p>28) I provided both "filetype" ("MIME Type"). The MIME Type follows the format of https://www.iana.org/assignments/media-types/media-types.xhtml. https://www.iana.org/assignments/media-types/application/vnd.sqlite3. Also please note the FILE EXTENSION was .bak for this SQLite database backup.</p> <p>35) I provided both "filetype" ("MIME Type"). The MIME Type follows the format of https://www.iana.org/assignments/media-types/media-types.xhtml. Also please note the FILE EXTENSION was .txt for this GIF image file. 36) The SID for jbeatty is S-1-5-21-2298470282-2867887670-580413564-1119. 38) thumb-cts24-5562.E01\Partition 1\filez [NTFS]\[root]\206969.doc. *In other words the root directory of the thumb drive on Partition 1 which was formatted NTFS*</p>
ZQ4URL-5562	<p>Our lab didn't receive USB flash drive for this test. In Q13, answer is also located in Recycle bin, path and filename: \ \$Recycle.Bin\S-1-5-21-2298470282-2867887670-580413564-1117/\$RCZUXP4.jpg</p>
ZU7QJ2-5561	<p>The opportunity to attach a report of findings in this space would be appreciated.</p>
ZWABN2-5562	<p>Thank you!!</p>

-End of Report-
(Appendix may follow)