Collaborative Testing Services, Inc
FORENSIC TESTING PROGRAM

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

Computer Hard Drive - Windows Analysis
Test No. 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:

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

Question ***Manufacturer's Response***

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Manufacturer's Information, continued

Question ***Manufacturer's Response***

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

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

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

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

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

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

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

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

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

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

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

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

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

Manufacturer's Information, continued

Question ***Manufacturer's Response***

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

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

30 **Provide the name of the file contained within the encrypted file in a user’s “Documents” directory.**
cookbook.pdf

Manufacturer's Information, continued

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

Question ***Manufacturer's Response***

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

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

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

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

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

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

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

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

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

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

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

Summary Comments

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

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

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

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

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

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

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 Response: 51945f35b4b3e59a4a802195bce4efff

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
BXTTXP-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
HAVVCD-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	3d57dbf15f0918b0e7ba53598b85950
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:

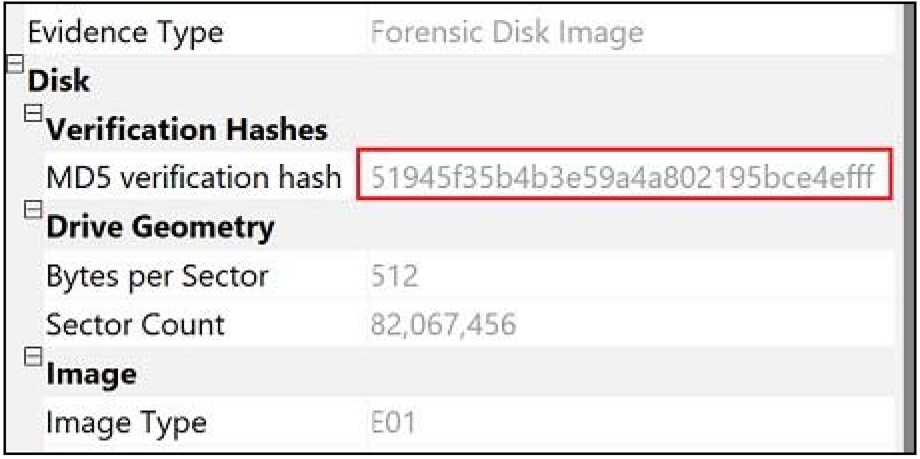
51945f35b4b3e59a4a802195bce4efff

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



Evidence Type   Forensic Disk Image

⊟ Disk

⊟ Verification Hashes

MD5 verification hash   51945f35b4b3e59a4a802195bce4efff

⊟ Drive Geometry

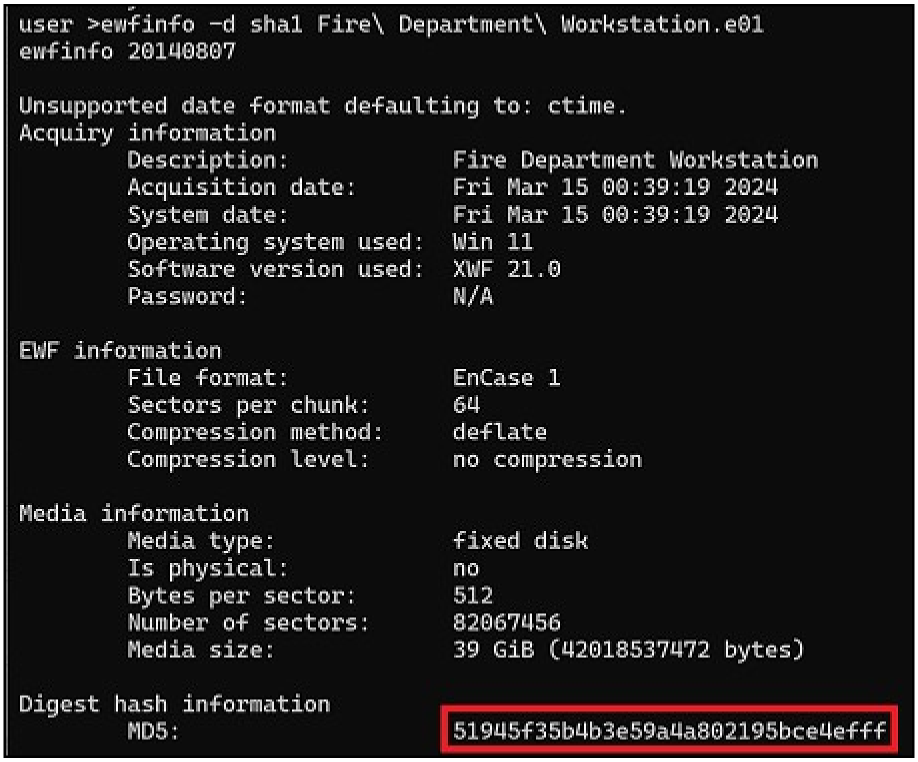
Bytes per Sector   512

Sector Count   82,067,456

⊟ Image

Image Type   E01

ewfinfo view of Fire Department Workstation.e01 stored verification hash



```
user >ewfinfo -d sha1 Fire\ Department\ Workstation.e01
ewfinfo 20140807

Unsupported date format defaulting to: ctime.
Acquiry information
        Description:            Fire Department Workstation
        Acquisition date:       Fri Mar 15 00:39:19 2024
        System date:            Fri Mar 15 00:39:19 2024
        Operating system used:  Win 11
        Software version used:  XWF 21.0
        Password:               N/A

EWF information
        File format:            EnCase 1
        Sectors per chunk:      64
        Compression method:     deflate
        Compression level:      no compression

Media information
        Media type:             fixed disk
        Is physical:            no
        Bytes per sector:       512
        Number of sectors:      82067456
        Media size:             39 GiB (42018537472 bytes)

Digest hash information
        MD5:                    51945f35b4b3e59a4a802195bce4efff
```

Other Responses:

Twenty-three (15%) participants reported the MD5 hash of the container file, 3d57dbf15f09181b0e7ba53598b85950, not the stored verification hash of the provided image.