UNIVERSITY OF THE WEST of SCOTLAND
UWS | London Campus

Digital Forensic Analysis Logbook

Case Number: 001548

Submitted to

Dr Manesh Thankappan,

By

Ilyas Zyat

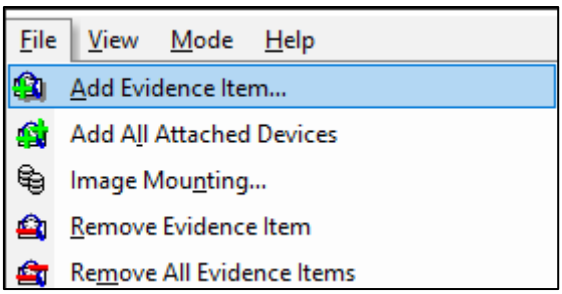
B01794768

July 2025

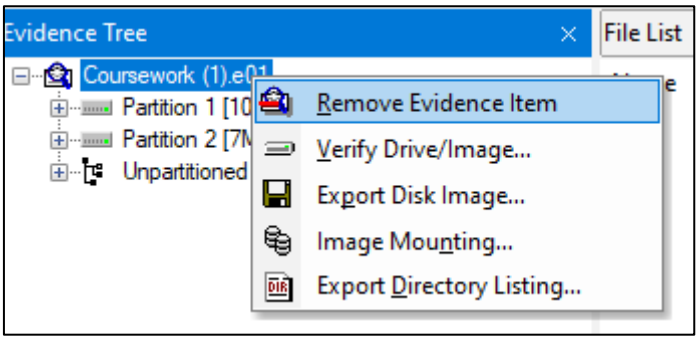
Date	**7/13/2025**	**Location**	*img_Coursework.e01*
Time	**09:43 AM**		
Evidence Description	*1. What is an image hash? Does the acquisition and verification hash match?*		

Answer: An image hash is a cryptographic fingerprint of a file, used to ensure that the data has not been altered. Using FTK Imager's "Verify Drive/Image" function, I verified the MD5 and SHA1 hash values of the Coursework.e01 forensic image. The computed hash and the stored verification hash both matched, confirming the image has not been tampered with and is forensically sound. MD5 and SHA1 are different algorithms that produce different hash values. FTK Imager successfully matched the computed and stored hashes for both algorithms, confirming the image's integrity.

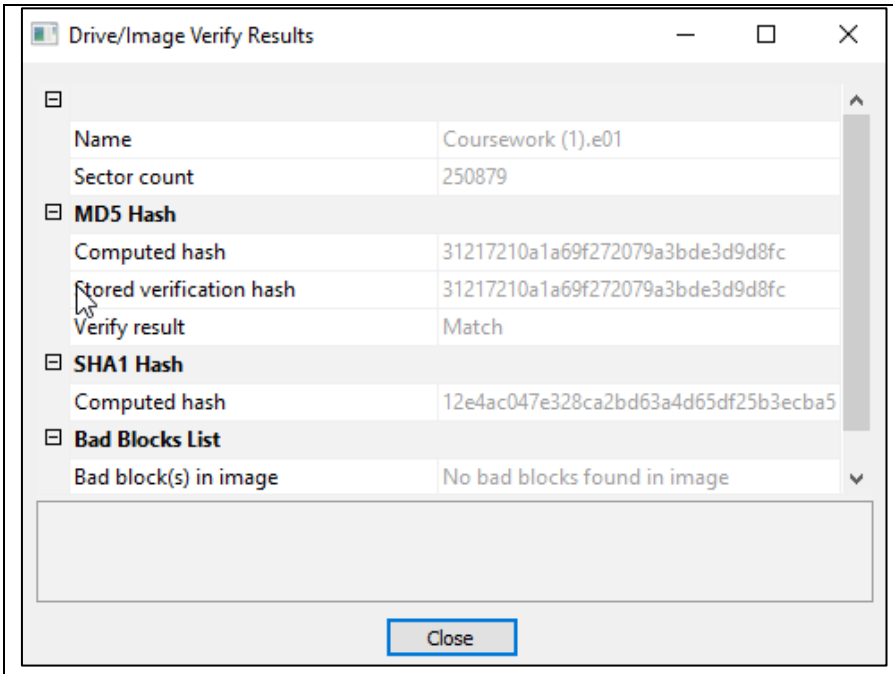
Comments and Screenshot:



Adding the image file to hash analysis



Launching the Drive/Image verification

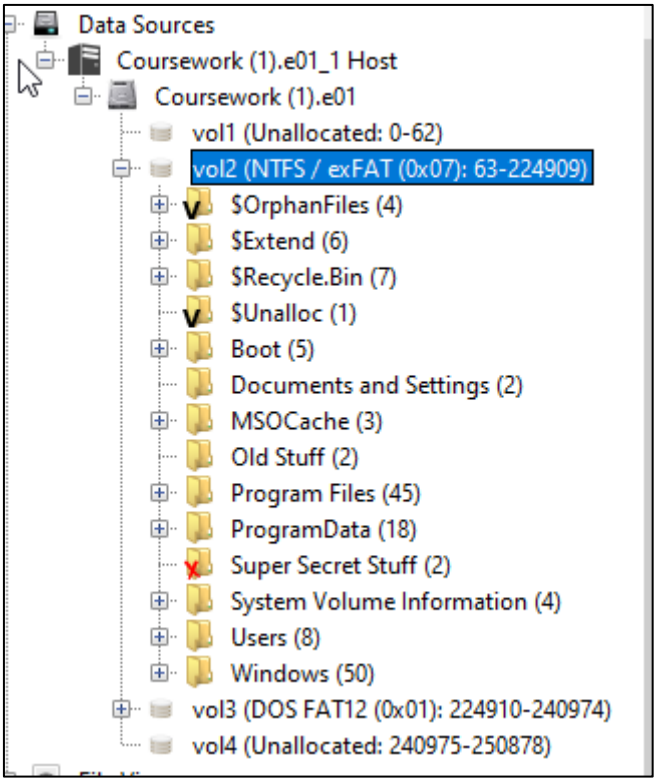


Drive/Image verification results with the MD5 and SHA1 Hash values

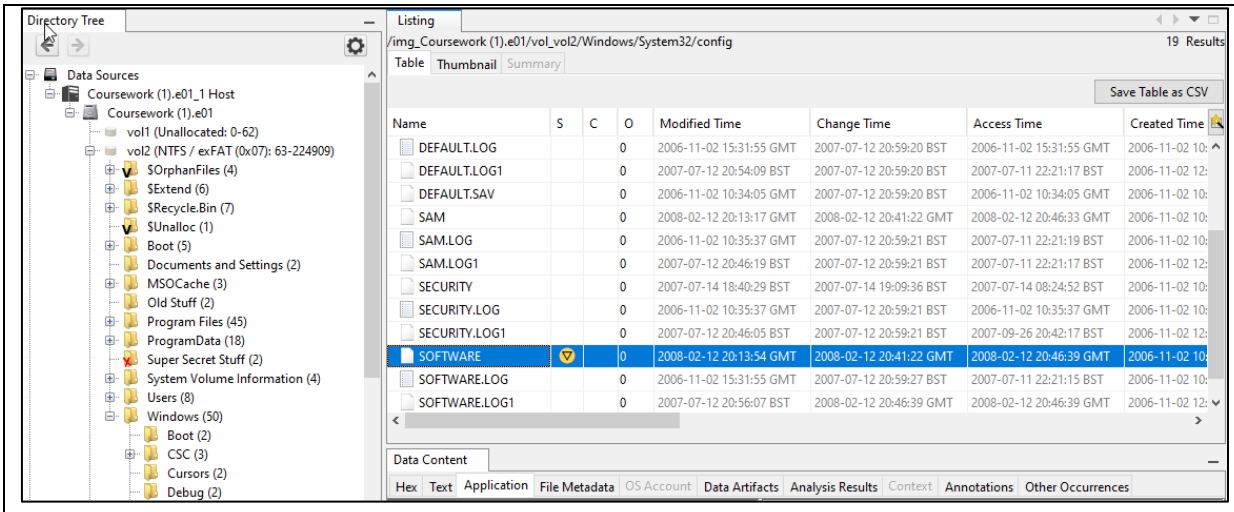
Date	**7/13/2025**	**Location**	*img_Coursework.e01*\vol_vol2\Windows\System32\config\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\
Time	**09:30 AM**		
Evidence Description	*2. What operating system was used on the computer?*		

Answer: The operating system installed on the suspect's machine was identified using the SOFTWARE registry hive. By analysing the key SOFTWARE/Microsoft/Windows NT/CurrentVersion in AccessData Registry Viewer, the ProductName value was found to be Windows Vista (TM) Ultimate. This confirms the system was running a Windows Vista OS.

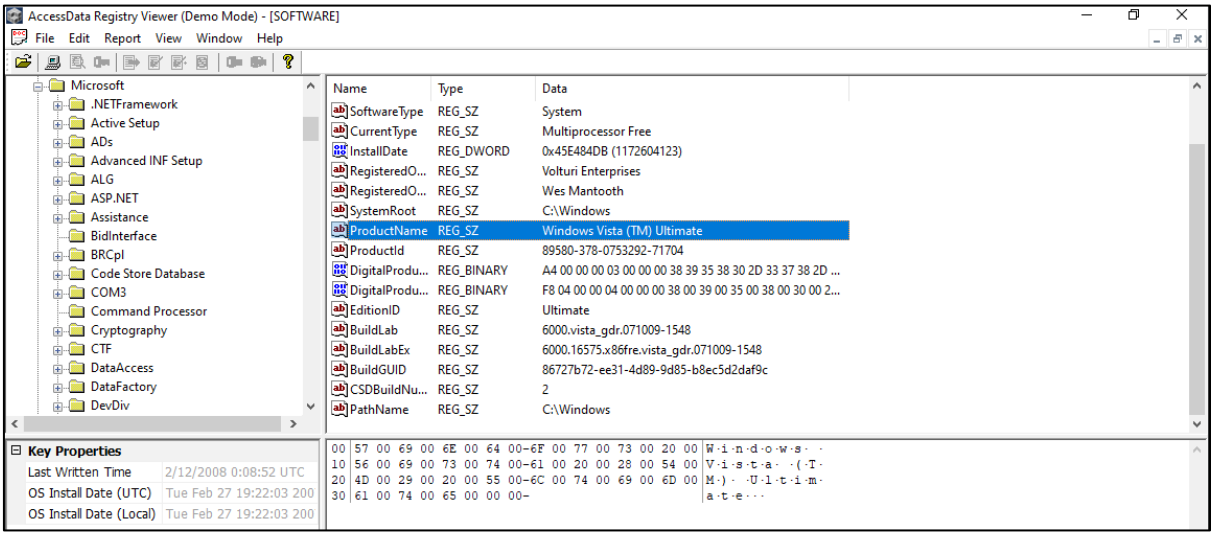
Comments and Screenshot:



Navigating to vol2 folder



Extracting the SOFTWARE file for Registry Viewer analysis



Finding the operating system version on ProductName file

Date	**7/13/2025**	**Location**	*/img_Coursework.e01/*vol_vol2/Windows/System32/config/ SOFTWARE/Microsoft/WindowsNT/CurrentVersion/
Time	**09:45 AM**		
Evidence Description	*3. When was the installation date?*		

Answer: The operating system installation date was identified using the SOFTWARE registry hive, specifically under the key: SOFTWARE/Microsoft/WindowsNT/CurrentVersion. The Install Date value was stored as a Unix timestamp (1172604123) and was automatically decoded by Access Data Registry Viewer. According to the decoded value, the OS was installed on Tuesday, 27 February 2007 at 19:22:03 UTC.

Comments and Screenshot:

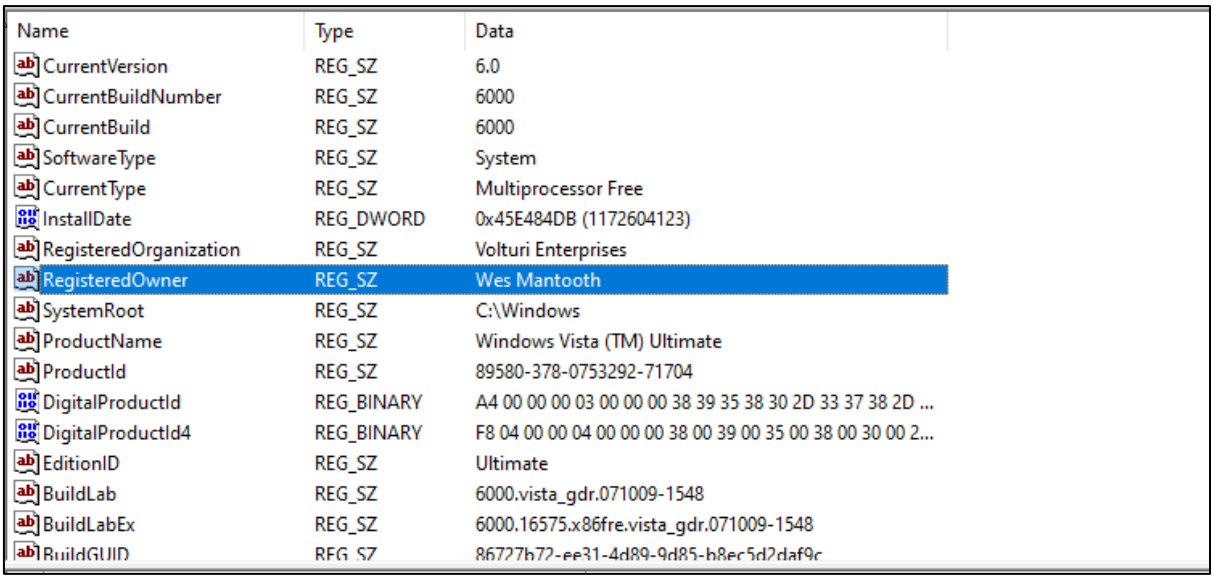
Key Properties	
Last Written Time	2/12/2008 0:08:52 UTC
OS Install Date (UTC)	Tue Feb 27 19:22:03 2007
OS Install Date (Local)	Tue Feb 27 19:22:03 2007

Installation date information

Date	**7/13/2025**	**Location**	*/img_Coursework.e01/*vol_vol2/Windows/System32/config/ SOFTWARE/Microsoft/WindowsNT/CurrentVersion/
Time	**10:00 AM**		
Evidence Description	*4. Who is the registered owner?*		

Answer: The registered owner of the computer was found in the SOFTWARE hive, under the key SOFTWARE/Microsoft/Windows NT/CurrentVersion. The value of RegisteredOwner is Wes Mantooth, which confirms the system was registered under the name of the suspect.

Comments and Screenshot:



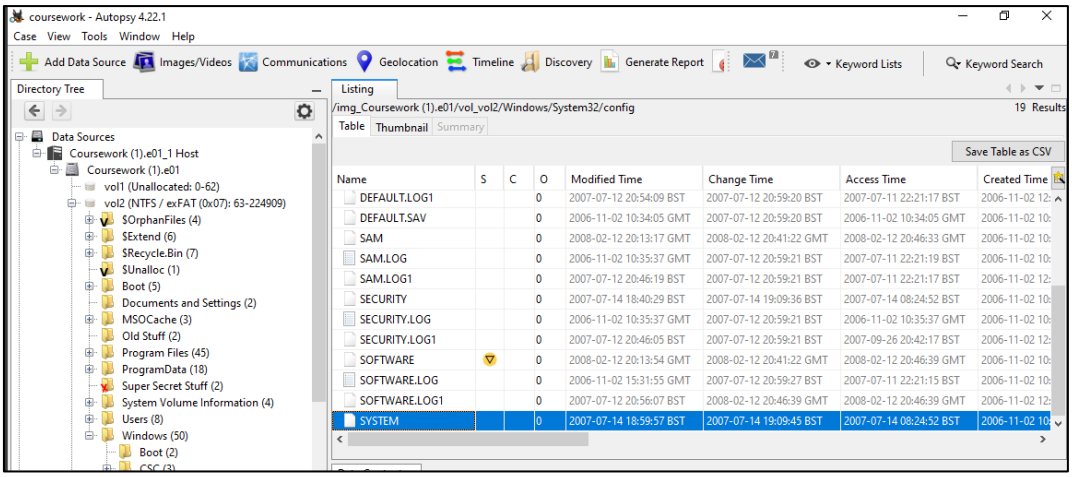
Name	Type	Data
CurrentVersion	REG_SZ	6.0
CurrentBuildNumber	REG_SZ	6000
CurrentBuild	REG_SZ	6000
SoftwareType	REG_SZ	System
CurrentType	REG_SZ	Multiprocessor Free
InstallDate	REG_DWORD	0x45E484DB (1172604123)
RegisteredOrganization	REG_SZ	Volturi Enterprises
RegisteredOwner	REG_SZ	Wes Mantooth
SystemRoot	REG_SZ	C:\Windows
ProductName	REG_SZ	Windows Vista (TM) Ultimate
ProductId	REG_SZ	89580-378-0753292-71704
DigitalProductId	REG_BINARY	A4 00 00 00 03 00 00 00 38 39 35 38 30 2D 33 37 38 2D ...
DigitalProductId4	REG_BINARY	F8 04 00 00 04 00 00 00 38 00 39 00 35 00 38 00 30 00 2...
EditionID	REG_SZ	Ultimate
BuildLab	REG_SZ	6000.vista_gdr.071009-1548
BuildLabEx	REG_SZ	6000.16575.x86fre.vista_gdr.071009-1548
BuildGUID	REG_SZ	86727b72-ee31-4d89-9d85-b8ec5d2daf9c

Registered Owner as Wes Mantooth

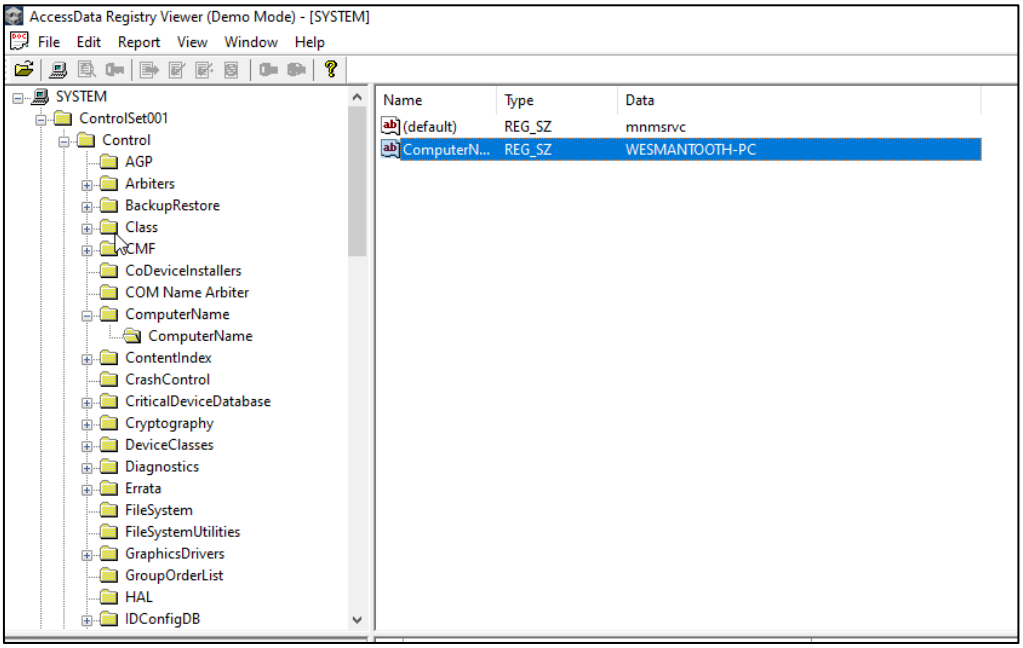
Date	**7/13/2025**	**Location**	*/img_Coursework.e01*/vol_vol2/Windows/System32/config/ SYSTEM/ControlSet001/Control/ComputerName/ComputerName
Time	**10:20 AM**		
Evidence Description	*5. What is the computer account name?*		

Answer: The computer account name was retrieved from the SYSTEM registry hive. Specifically, under the key: ControlSet001/Control/ComputerName/ComputerName, the ComputerName value was identified as WESMANTOOTH-PC. This confirms the hostname of the suspect's machine.

Comments and Screenshot:



Extracting the SYSTEM file for Registry Viewer analysis

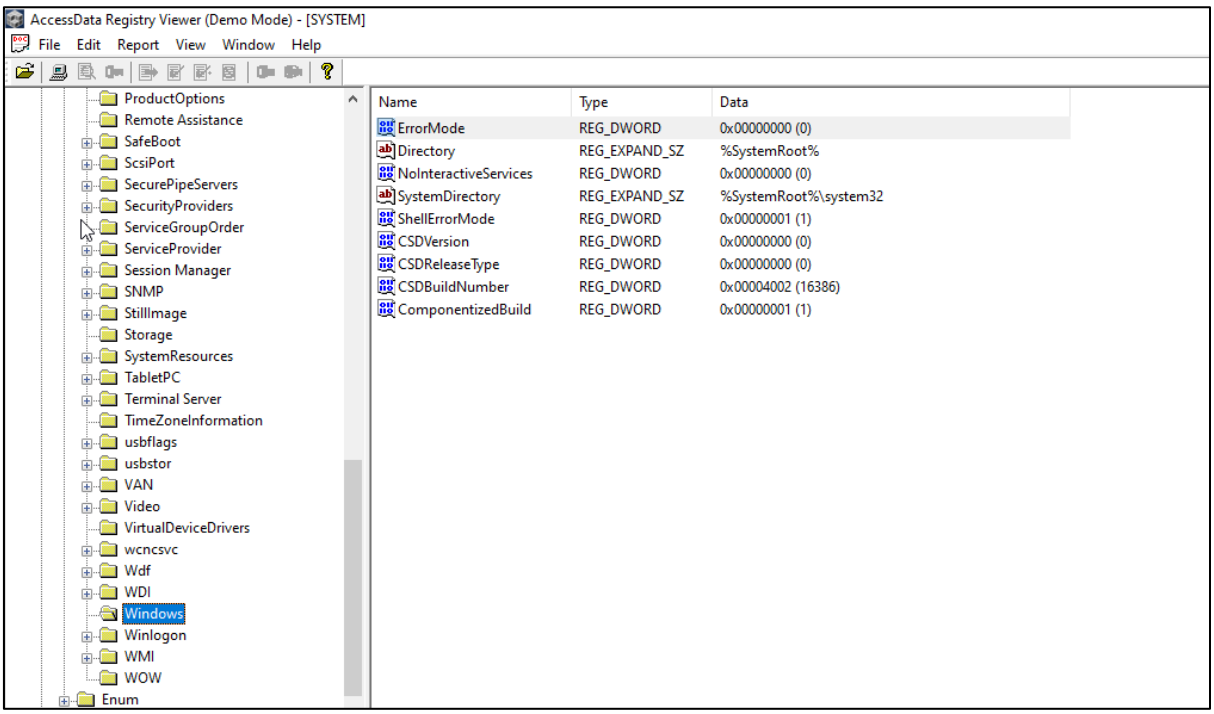


Finding the computer account name WESMANTOOTH-PC

Date	**7/13/2025**	**Location**	*/img_Coursework.e01/*vol_vol2/Windows/System32/config/SYSTEM/ControlSet001/Control/Windows
Time	**11:03 AM**		
Evidence Description	*6. When was the last recorded computer shutdown date/time?*		

Answer: The last shutdown time is typically stored in the SYSTEM hive under the key: ControlSet001/Control/Windows, value: ShutdownTime. However, upon inspecting both ControlSet001 and ControlSet003 in AccessData Registry Viewer, the ShutdownTime value was not present. This suggests that the system either did not shut down properly or the value was not recorded on this version of Windows. Therefore, the last shutdown time could not be conclusively determined from the registry.

Comments and Screenshot:

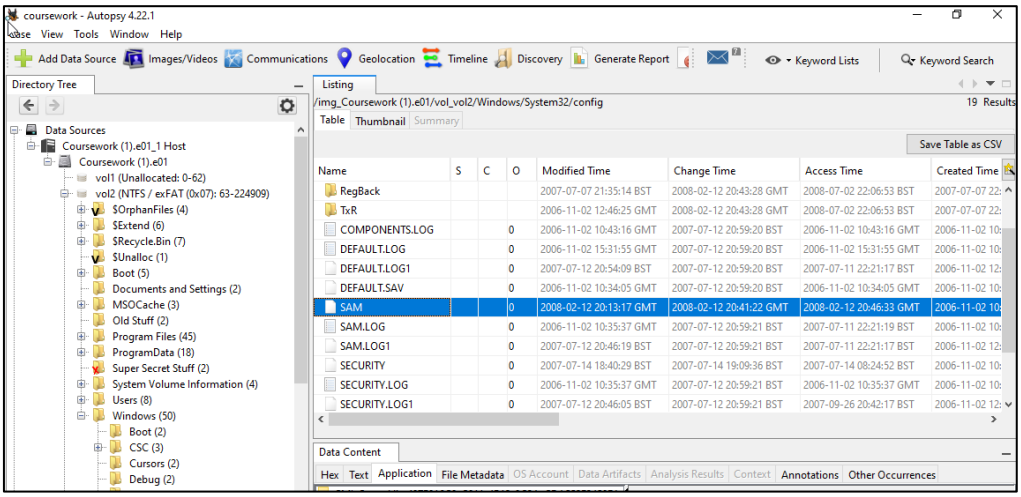


Shutdown file not found

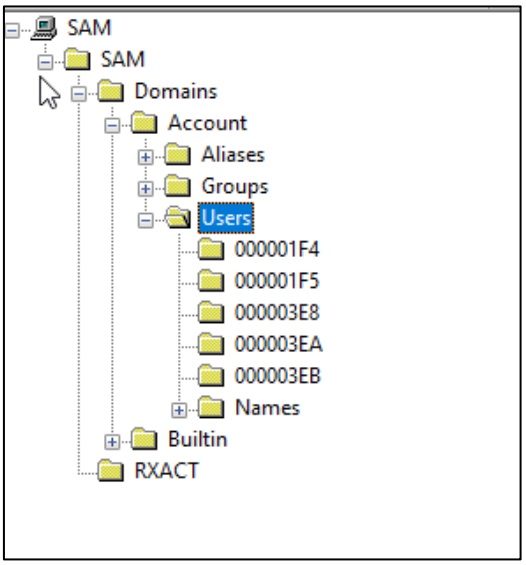
Date	**7/13/2025**	**Location**	*/img_Coursework.e01/*vol_vol2/Windows/System32/config/ SAM/Domains/Account/Users
Time	**11:18 AM**		
Evidence Description	*7. How many accounts are registered (total number)?*		

Answer: The total number of registered user accounts on the system was found under the key: SAM/Domains/Account/Users. There are 5 subkeys representing user or built-in accounts: 000001F4, 000001F5, 000003E8, 000003EA, and 000003EB. The Names folder is not a user account but a mapping container, so it was excluded from the count. Therefore, the total number of registered accounts is 5.

Comments and Screenshot:



Extracting the SAM file for Registry Viewer analysis

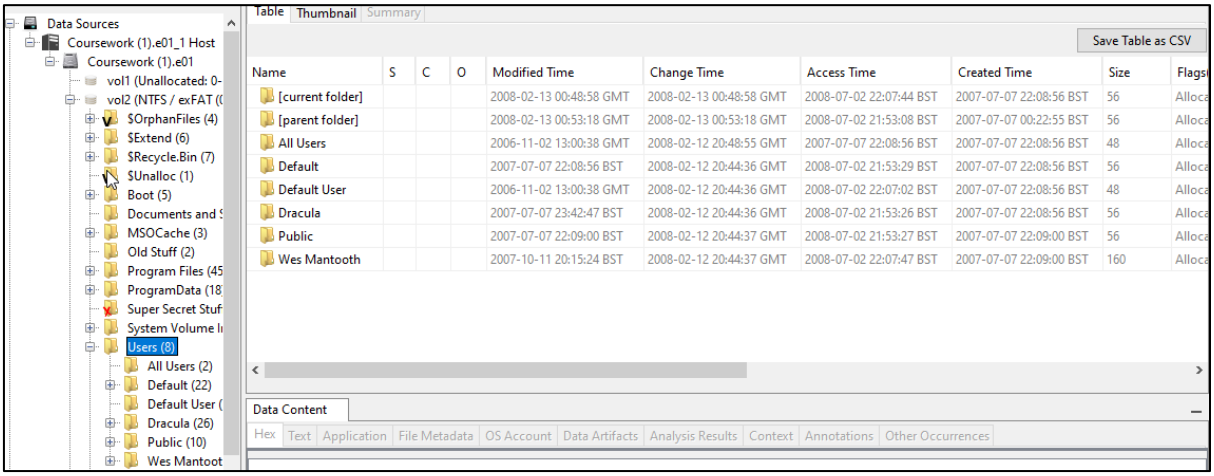


Number of registered accounts discovered

Date	**7/13/2025**	**Location**	*/img_Coursework.e01/*vol_vol2/Windows/Users
Time	**11:36 AM**		
Evidence Description	*8. What is the name of the user account that uses the computer the most?*		

Answer: The user account that uses the computer the most was determined by analyzing the metadata of user profile folders under C:\Users using Autopsy. The “Wes Mantooth” folder had the largest size (160) and the most recent access timestamp (2008-07-02 22:07:47 BST). Based on this evidence, it is concluded that Wes Mantooth is the primary and most active user of the computer.

Comments and Screenshot:



List of the users with the most used one

Date	**7/13/2025**	**Location**	*/img_Coursework.e01/*vol_vol2/Windows/Users
Time	**11:53 AM**		
Evidence Description	*9. Who was the last user who entered the computer?*		

Answer: The last user who logged into the computer was identified by examining the access timestamps of profile folders in C:\Users via Autopsy. The folder Wes Mantooth had the most recent access time: 2008-07-02 22:07:47 BST, which indicates that Wes Mantooth was the last user to log into the system.

Comments and Screenshot:

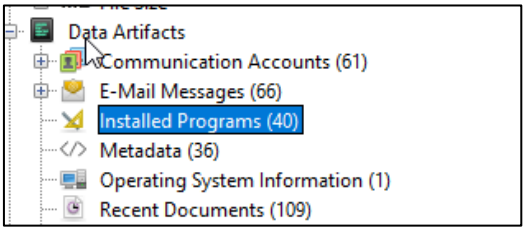
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
[current folder]				2008-02-13 00:48:58 GMT	2008-02-13 00:48:58 GMT	2008-07-02 22:07:44 BST	2007-07-07 22:08:56 BST
[parent folder]				2008-02-13 00:53:18 GMT	2008-02-13 00:53:18 GMT	2008-07-02 21:53:08 BST	2007-07-07 00:22:55 BST
All Users				2006-11-02 13:00:38 GMT	2008-02-12 20:48:55 GMT	2007-07-07 22:08:56 BST	2007-07-07 22:08:56 BST
Default				2007-07-07 22:08:56 BST	2008-02-12 20:44:36 GMT	2008-07-02 21:53:29 BST	2007-07-07 22:08:56 BST
Default User				2006-11-02 13:00:38 GMT	2008-02-12 20:44:36 GMT	2008-07-02 22:07:02 BST	2007-07-07 22:08:56 BST
Dracula				2007-07-07 23:42:47 BST	2008-02-12 20:44:36 GMT	2008-07-02 21:53:26 BST	2007-07-07 22:08:56 BST
Public				2007-07-07 22:09:00 BST	2008-02-12 20:44:37 GMT	2008-07-02 21:53:27 BST	2007-07-07 22:09:00 BST
Wes Mantooth				2007-10-11 20:15:24 BST	2008-02-12 20:44:37 GMT	2008-07-02 22:07:47 BST	2007-07-07 22:09:00 BST

Finding the most recent user entering the computer

Date	7/13/2025	Location	*Data Artifacts/Installed Programs*
Time	**12:09 PM**		
Evidence Description	*10. Find installed programs that may be used for criminal activity (e.g. hacking, phishing, unauthorized access or etc.).*		

Answer: Several installed programs were identified that may be related to criminal activity. This analysis was conducted through Autopsy's Installed Programs artifact: FileZilla, an FTP client that can be used to transfer or exfiltrate data from the system. VNC Free Edition 4.1.2, a remote desktop software that allows full control of the system from a remote device, potentially enabling unauthorized access. TrueCrypt, a disk encryption tool often used to hide evidence or store illicit data securely. P2P Networking, a peer-to-peer communication software that may be used to share illegal content or bypass standard file monitoring. These programs may be legitimate in some contexts, but in a forensic investigation, they warrant further analysis and correlation with other evidence.

Comments and Screenshot:



Navigating to the Installed Programs folder on Data Artifacts

Source Name	S	C	O	Program Name	Date/Time	Data Source
SOFTWARE			0	WebEx	2007-10-10 10:12:40 BST	Coursework (1).e01
SOFTWARE			0	FileZilla (remove only)	2007-06-24 00:23:53 BST	Coursework (1).e01
SOFTWARE			0	Microsoft Office Standard Edition 2003 v.11.0.5614.0	2007-04-17 23:25:28 BST	Coursework (1).e01
SOFTWARE			0	RTC Client API v1.2 v.1.2.0000	2007-04-17 21:43:27 BST	Coursework (1).e01
SOFTWARE			0	AccessData DNA 3 Worker v.3.3	2007-04-17 19:58:46 BST	Coursework (1).e01
SOFTWARE			0	AccessData Registry Viewer v.1.5	2007-04-14 00:01:22 BST	Coursework (1).e01
SOFTWARE			0	QuickTime	2007-04-13 23:36:51 BST	Coursework (1).e01
SOFTWARE			0	Adobe Reader 8 v.8.0.0	2007-04-12 23:26:59 BST	Coursework (1).e01
SOFTWARE			0	VNC Free Edition 4.1.2 v.4.1.2	2007-04-11 17:24:00 BST	Coursework (1).e01
SOFTWARE			0	TrueCrypt	2007-04-11 01:37:31 BST	Coursework (1).e01
SOFTWARE			0	Mozilla Firefox (2.0.0.3) v.2.0.0.3 (en-US)	2007-04-10 17:55:21 BST	Coursework (1).e01
SOFTWARE			0	AccessData FTK Imager v.2.5.1	2007-02-27 23:14:26 GMT	Coursework (1).e01

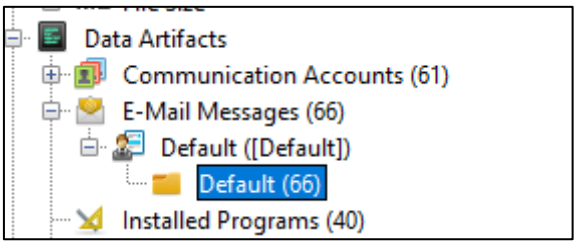
Source Name	S	C	O	Program Name	Date/Time	Data Source
SOFTWARE			0	BestCrypt 8.0	2007-02-27 23:08:21 GMT	Coursework (1).e01
SOFTWARE			0	P2P Networking	2007-02-27 23:03:51 GMT	Coursework (1).e01
SOFTWARE			0	AOL Uninstaller (Choose which Products to Remove)	2007-02-27 20:57:42 GMT	Coursework (1).e01
SOFTWARE			0	Yahoo! Browser Services	2007-02-27 20:28:40 GMT	Coursework (1).e01
SOFTWARE			0	Yahoo! Install Manager	2007-02-27 20:28:40 GMT	Coursework (1).e01
SOFTWARE			0	Yahoo! Internet Mail	2007-02-27 20:28:36 GMT	Coursework (1).e01
SOFTWARE			0	Yahoo! Toolbar	2007-02-27 20:28:31 GMT	Coursework (1).e01
SOFTWARE			0	Yahoo! Toolbar	2007-02-27 20:28:29 GMT	Coursework (1).e01
SOFTWARE			0	Yahoo! Messenger	2007-02-27 20:28:14 GMT	Coursework (1).e01
SOFTWARE			0	WinRAR archiver	2007-02-27 20:01:25 GMT	Coursework (1).e01
SOFTWARE			0	Trillian	2007-02-27 19:39:25 GMT	Coursework (1).e01
SOFTWARE			0	Windows Live Messenger v.8.1.0178.00	2007-02-27 19:29:18 GMT	Coursework (1).e01

List of all the programs and some suspicious one

Date	**7/13/2025**	**Location**	*Data Artifacts/Email Messages/Top of Personal Folders*
Time	**12:24 PM**		
Evidence Description	*11. Which email is used by Wes Mantooth and others?*		

Answer: The email address used by Wes Mantooth was identified by analysing the "E-Mail Messages" artifact in Autopsy. Multiple messages were found sent from: dollarhyde86@comcast.net, confirming that this was his primary email address in use.

Comments and Screenshot:



Navigating to the emails found

Data Source	E-Mail From	Date Received	Message (Plaintext)
Coursework (1).e01			
Coursework (1).e01	dollarhyde86@comcast.net <dollarhyde86@comcast....	2007-06-20 18:50:35 BST	This is an e-mail message s
Coursework (1).e01	Outlook 2003 Team <olteam@microsoft.com>	2007-06-20 18:25:36 BST	Thank you for using Micros
Coursework (1).e01	John Washer <chkwasher@comcast.net>	2007-06-20 18:56:25 BST	Dude! You been laying a li
Coursework (1).e01	John Washer <chkwasher@comcast.net>	2007-06-20 19:01:59 BST	Very nice... forget percripti
Coursework (1).e01	John Washer <chkwasher@comcast.net>	2007-06-20 19:09:34 BST	So.. how are you going to g
Coursework (1).e01	Rasco Badguy <txkidd@swbell.net>	2007-08-01 20:09:08 BST	Guys, Been working on a le
Coursework (1).e01	Wes Mantooth <dollarhyde86@comcast.net>	2007-06-21 19:00:00 BST	Sorry man. I have been a l
Coursework (1).e01	Wes Mantooth <dollarhyde86@comcast.net>	2007-06-21 22:06:00 BST	Your crazy! You are going
Coursework (1).e01	Wes Mantooth <dollarhyde86@comcast.net>	2007-06-22 00:26:00 BST	It works EXACTLY the same
Coursework (1).e01	Wes Mantooth <dollarhyde86@comcast.net>	2007-06-22 00:05:08 BST	
Coursework (1).e01	Wes Mantooth <dollarhyde86@comcast.net>	2007-06-22 00:05:50 BST	
Coursework (1).e01			Innovative technologies to
Coursework (1).e01			New Zealand's premier pha
Coursework (1).e01			
Coursework (1).e01			Proper credentialing enable
Coursework (1).e01			The Collecting and Process
Coursework (1).e01			
Coursework (1).e01			
Coursework (1).e01			Texas Star Pharmacy3033 W
Coursework (1).e01	Wes Mantooth <dollarhyde86@comcast.net>	2007-06-22 00:25:47 BST	
Coursework (1).e01	Wes Mantooth <dollarhyde86@comcast.net>	2007-06-21 23:38:32 BST	Excellent source for checks
Coursework (1).e01	Wes Mantooth <dollarhyde86@comcast.net>	2007-06-21 23:42:55 BST	

List of emails with the one belonging to Wes Mantooth

Date	7/13/2025	Location	*Data Artifacts/Web History*
Time	**12:47 PM**		
Evidence Description	12. What websites was the Wes Mantooth accessing?		

Answer: The web browsing activity for Wes Mantooth was analysed using the Web History artifact in Autopsy. By filtering entries by the Username column, all URLs accessed by Wes were extracted. Numerous visits were made on 2007-07-12 between 23:13 and 23:17 BST, with content largely focused on:

- Drug-related content, including searches for methamphetamine and access to: www.totse.com and www.neonjoint.com
- Fraud/Scam research, including topics on ATM card skimmers and scam warnings: snopes.com
- Hacking content: physorg.com, casalemedia.com, images.google.com, imageshack.us

Comments and Screenshot:

URL	Date Accessed	Program Name	Domain	Username
http://www.physorg.com/physorg.rss	2007-07-12 23:16:22 BST	Internet Explorer Analyzer	physorg.com	Wes Mantooth
http://images.google.com/images?q=check+washing...	2007-07-12 23:17:30 BST	Internet Explorer Analyzer	google.com	Wes Mantooth
file/Business%20Ideas/Camera.bmp	2007-07-12 23:15:11 BST	Internet Explorer Analyzer		Wes Mantooth
http://b.casalemedia.com/V2/44508/86958/index.html...	2007-07-12 23:15:00 BST	Internet Explorer Analyzer	casalemedia.com	Wes Mantooth
http://www.totse.com/en/drugs/speedy_drugs/howto...	2007-07-12 23:16:04 BST	Internet Explorer Analyzer	totse.com	Wes Mantooth
http://www.totse.com/totse.rss	2007-07-12 23:16:04 BST	Internet Explorer Analyzer	totse.com	Wes Mantooth
file/Business%20Ideas/Guts.bmp	2007-07-12 23:14:53 BST	Internet Explorer Analyzer		Wes Mantooth
http://www.google.com/search?hl=en&q=making+...	2007-07-12 23:16:33 BST	Internet Explorer Analyzer	google.com	Wes Mantooth
http://images.google.com/images?um=1&tab=wi&hl...	2007-07-12 23:17:08 BST	Internet Explorer Analyzer	google.com	Wes Mantooth
http://images.google.com/images?um=1&tab=wi&hl...	2007-07-12 23:15:24 BST	Internet Explorer Analyzer	google.com	Wes Mantooth
http://www.sccja.org/images/csid_meth1.jpg	2007-07-12 23:17:02 BST	Internet Explorer Analyzer	sccja.org	Wes Mantooth
file/Business%20Ideas/untitled.bmp	2007-07-12 23:14:17 BST	Internet Explorer Analyzer		Wes Mantooth
http://www.google.com/search?hl=en&q=atm+card...	2007-07-12 23:15:34 BST	Internet Explorer Analyzer	google.com	Wes Mantooth
http://images.google.com/images?q=making+meth...	2007-07-12 23:17:06 BST	Internet Explorer Analyzer	google.com	Wes Mantooth
http://images.google.com/images?svnum=10&um=1...	2007-07-12 23:17:36 BST	Internet Explorer Analyzer	google.com	Wes Mantooth
http://img376.imageshack.us/img376/8880/washingis...	2007-07-12 23:17:44 BST	Internet Explorer Analyzer	imageshack.us	Wes Mantooth
http://www.physorg.com/news99637614.html	2007-07-12 23:16:23 BST	Internet Explorer Analyzer	physorg.com	Wes Mantooth
http://www.snopes.com/fraud/atm/atmcamera.asp	2007-07-12 23:13:19 BST	Internet Explorer Analyzer	snopes.com	Wes Mantooth
http://www.neonjoint.com/drug_recipes/chapter3.html	2007-07-12 23:15:52 BST	Internet Explorer Analyzer	neonjoint.com	Wes Mantooth
http//www.sccja.org/images/csid_meth1.jpg&imgref...	2007-07-12 23:17:06 BST	Internet Explorer Analyzer		Wes Mantooth
http://images.google.com/images?q=making+meth...	2007-07-12 23:17:06 BST	Internet Explorer Analyzer	google.com	Wes Mantooth
http://www.google.com/search?hl=en&q=atm+card...	2007-07-12 23:15:34 BST	Internet Explorer Analyzer	google.com	Wes Mantooth
http://images.google.com/images?q=check+washing...	2007-07-12 23:17:35 BST	Internet Explorer Analyzer	google.com	Wes Mantooth

http://images.google.com/images?q=check+washing...	2007-07-12 23:17:30 BST	Internet Explorer Analyzer	google.com	Wes Mantooth
img376.imageshack.us	2007-07-12 23:17:44 BST	Internet Explorer Analyzer	imageshack.us	Wes Mantooth
http://www.snopes.com/fraud/atm/atmcamera.asp	2007-07-12 23:13:19 BST	Internet Explorer Analyzer	snopes.com	Wes Mantooth
http://b.casalemedia.com/V2/44508/86958/index.html...	2007-07-12 23:15:00 BST	Internet Explorer Analyzer	casalemedia.com	Wes Mantooth
www.neonjoint.com	2007-07-12 23:15:52 BST	Internet Explorer Analyzer	neonjoint.com	Wes Mantooth
images.google.com	2007-07-12 23:15:24 BST	Internet Explorer Analyzer	google.com	Wes Mantooth
http://images.google.com/images?svnum=10&um=1...	2007-07-12 23:17:36 BST	Internet Explorer Analyzer	google.com	Wes Mantooth
http://img376.imageshack.us/img376/8880/washingis...	2007-07-12 23:17:44 BST	Internet Explorer Analyzer	imageshack.us	Wes Mantooth
http://images.google.com/images?q=making+meth...	2007-07-12 23:17:06 BST	Internet Explorer Analyzer	google.com	Wes Mantooth
www.google.com	2007-07-12 23:12:16 BST	Internet Explorer Analyzer	google.com	Wes Mantooth
http//www.sccja.org/images/csid_meth1.jpg&imgref...	2007-07-12 23:17:06 BST	Internet Explorer Analyzer		Wes Mantooth
b.casalemedia.com	2007-07-12 23:15:00 BST	Internet Explorer Analyzer	casalemedia.com	Wes Mantooth
www.totse.com	2007-07-12 23:16:04 BST	Internet Explorer Analyzer	totse.com	Wes Mantooth
http://www.google.com	2007-07-12 23:12:16 BST	Internet Explorer Analyzer	google.com	Wes Mantooth
http://www.snopes.com/crime/warnings/atmcamera....	2007-07-12 23:13:16 BST	Internet Explorer Analyzer	snopes.com	Wes Mantooth
http://images.google.com/images?um=1&tab=wi&hl...	2007-07-12 23:15:24 BST	Internet Explorer Analyzer	google.com	Wes Mantooth
http://www.neonjoint.com/drug_recipes/chapter3.html	2007-07-12 23:15:52 BST	Internet Explorer Analyzer	neonjoint.com	Wes Mantooth
www.sccja.org	2007-07-12 23:17:02 BST	Internet Explorer Analyzer	sccja.org	Wes Mantooth
http://www.totse.com/en/drugs/speedy_drugs/howto...	2007-07-12 23:16:04 BST	Internet Explorer Analyzer	totse.com	Wes Mantooth
www.snopes.com	2007-07-12 23:13:16 BST	Internet Explorer Analyzer	snopes.com	Wes Mantooth
http://www.physorg.com/news99637614.html	2007-07-12 23:16:23 BST	Internet Explorer Analyzer	physorg.com	Wes Mantooth

List of accessed websites by Wes Mantooth

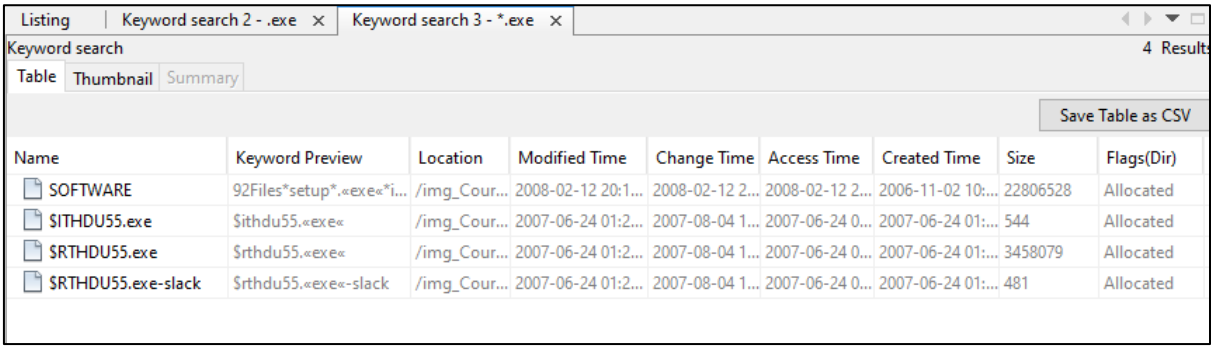
Date	**7/13/2025**	**Location**	*Keyword search "*.exe" files*
Time	**01:05 PM**		
Evidence Description	13. How many executables files were used? And are these files really deleted? Or files are there in the recycle bin?		

Answer: Yes, several .exe files were located, including some that appear to have been deleted.

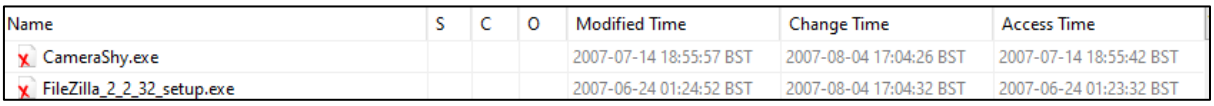
- Found executables include: SRTHDU55.exe (created: 2007-06-24, allocated), FileZilla_2_2_32_setup.exe (created: 2007-06-24, deleted), CameraShy.exe (created: 2007-07-14, deleted)
- Deleted executables are indicated with a red "X" and located through keyword search and within unallocated space/slack.

These suggest potential software installs or usage, including possibly suspicious ones like CameraShy.exe.

Comments and Screenshot:



Found allocated executable files

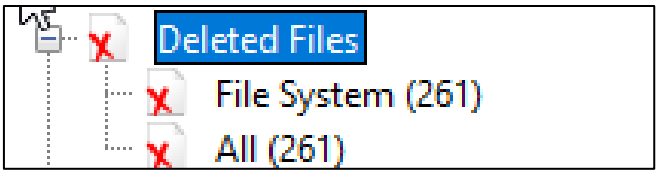


Found deleted files

Date	**7/13/2025**	**Location**	*File Views/Deleted Files/File System*
Time	**01:19 PM**		
Evidence Description	14. How many files are reported to be deleted by the file system?		

Answer: 261 files. These were found under Views > File Types > Deleted Files > File System (261) in Autopsy, indicating they are reported as deleted by the file system

Comments and Screenshot:



Number of the deleted files by the file system

Date	**7/13/2025**	**Location**	*Data Artifacts/Installed Programs*
Time	**01:38 PM**		
Evidence Description	15. Is encryption software installed on the Coursework computer?		

Answer: Yes, encryption software was installed on the Coursework computer. This is evidenced by the presence of TrueCrypt and BestCrypt 8.0 in the list of installed programs found within the SOFTWARE registry hive in Autopsy. Both applications are known for providing file and disk encryption capabilities.

Comments and Screenshot:

SOFTWARE	0	TrueCrypt	2007-04-11 01:37:31 BST	Coursework (1).e01
SOFTWARE	0	Mozilla Firefox (2.0.0.3) v.2.0.0.3 (en-US)	2007-04-10 17:55:21 BST	Coursework (1).e01
SOFTWARE	0	AccessData FTK Imager v.2.5.1	2007-02-27 23:14:26 GMT	Coursework (1).e01
SOFTWARE	0	BestCrypt 8.0	2007-02-27 23:08:21 GMT	Coursework (1).e01

Found encryption software installed on the computer

Date	7/13/2025	Location	*Data Artifacts/Web History*
Time	**01:57 PM**		
Evidence Description	16. What is the most visited internet domain and how many times it has been visited?		

Answer: The most visited internet domain is google.com, which appears over 20 times in the web history records. This was identified through the "Web History" section in Autopsy by reviewing and counting the entries in the Domain column.

Additional Observations (Forensic Relevance): While google.com is the most visited by frequency, other domains raise investigative interest: truecrypt.org, indicates interaction with encryption software totse.com, known for hosting controversial or illicit content. physorg.com and snopes.com are legitimate sites but may reflect the user's interests. These domains provide more meaningful insight into the suspect's activities than simple visit counts.

Comments and Screenshot:

URL	Date Accessed	Program Name	Domain	Username
http://www.physorg.com/physorg.rss	2007-07-12 23:16:22 BST	Internet Explorer Analyzer	physorg.com	Wes Mantooth
http://images.google.com/images?q=check+washing...	2007-07-12 23:17:30 BST	Internet Explorer Analyzer	google.com	Wes Mantooth
file/Business%20Ideas/Camera.bmp	2007-07-12 23:15:11 BST	Internet Explorer Analyzer		Wes Mantooth
http://b.casalemedia.com/V2/44508/86958/index.html...	2007-07-12 23:15:00 BST	Internet Explorer Analyzer	casalemedia.com	Wes Mantooth
http://www.totse.com/en/drugs/speedy_drugs/howto...	2007-07-12 23:16:04 BST	Internet Explorer Analyzer	totse.com	Wes Mantooth
http://www.totse.com/totse.rss	2007-07-12 23:16:04 BST	Internet Explorer Analyzer	totse.com	Wes Mantooth
file/Business%20Ideas/Guts.bmp	2007-07-12 23:14:53 BST	Internet Explorer Analyzer		Wes Mantooth
http://www.google.com/search?hl=en&q=making+...	2007-07-12 23:16:33 BST	Internet Explorer Analyzer	google.com	Wes Mantooth
http://images.google.com/images?um=1&tab=wi&hl...	2007-07-12 23:17:08 BST	Internet Explorer Analyzer	google.com	Wes Mantooth
http://images.google.com/images?um=1&tab=wi&hl...	2007-07-12 23:15:24 BST	Internet Explorer Analyzer	google.com	Wes Mantooth
http://www.sccja.org/images/csid_meth1.jpg	2007-07-12 23:17:02 BST	Internet Explorer Analyzer	sccja.org	Wes Mantooth
file/Business%20Ideas/untitled.bmp	2007-07-12 23:14:17 BST	Internet Explorer Analyzer		Wes Mantooth
http://www.google.com/search?hl=en&q=atm+card...	2007-07-12 23:15:34 BST	Internet Explorer Analyzer	google.com	Wes Mantooth
http://images.google.com/images?q=making+meth...	2007-07-12 23:17:06 BST	Internet Explorer Analyzer	google.com	Wes Mantooth
http://images.google.com/images?svnum=10&um=1...	2007-07-12 23:17:36 BST	Internet Explorer Analyzer	google.com	Wes Mantooth
http://img376.imageshack.us/img376/8880/washingis...	2007-07-12 23:17:44 BST	Internet Explorer Analyzer	imageshack.us	Wes Mantooth
http://www.physorg.com/news99637614.html	2007-07-12 23:16:23 BST	Internet Explorer Analyzer	physorg.com	Wes Mantooth
http://www.snopes.com/fraud/atm/atmcamera.asp	2007-07-12 23:13:19 BST	Internet Explorer Analyzer	snopes.com	Wes Mantooth
http://www.neonjoint.com/drug_recipes/chapter3.html	2007-07-12 23:15:52 BST	Internet Explorer Analyzer	neonjoint.com	Wes Mantooth
http://www.sccja.org/images/csid_meth1.jpg&imgref...	2007-07-12 23:17:06 BST	Internet Explorer Analyzer		Wes Mantooth
http://images.google.com/images?q=making+meth...	2007-07-12 23:17:06 BST	Internet Explorer Analyzer	google.com	Wes Mantooth
http://www.google.com/search?hl=en&q=atm+card...	2007-07-12 23:15:34 BST	Internet Explorer Analyzer	google.com	Wes Mantooth
http://images.google.com/images?q=check+washing...	2007-07-12 23:17:35 BST	Internet Explorer Analyzer	google.com	Wes Mantooth

URL	Date Accessed	Program Name	Domain	Username
http://images.google.com/images?q=check+washing...	2007-07-12 23:17:30 BST	Internet Explorer Analyzer	google.com	Wes Mantooth
img376.imageshack.us	2007-07-12 23:17:44 BST	Internet Explorer Analyzer	imageshack.us	Wes Mantooth
http://www.snopes.com/fraud/atm/atmcamera.asp	2007-07-12 23:13:19 BST	Internet Explorer Analyzer	snopes.com	Wes Mantooth
http://b.casalemedia.com/V2/44508/86958/index.html...	2007-07-12 23:15:00 BST	Internet Explorer Analyzer	casalemedia.com	Wes Mantooth
www.neonjoint.com	2007-07-12 23:15:52 BST	Internet Explorer Analyzer	neonjoint.com	Wes Mantooth
images.google.com	2007-07-12 23:15:24 BST	Internet Explorer Analyzer	google.com	Wes Mantooth
http://images.google.com/images?svnum=10&um=1...	2007-07-12 23:17:36 BST	Internet Explorer Analyzer	google.com	Wes Mantooth
http://img376.imageshack.us/img376/8880/washingis...	2007-07-12 23:17:44 BST	Internet Explorer Analyzer	imageshack.us	Wes Mantooth
http://images.google.com/images?q=making+meth...	2007-07-12 23:17:06 BST	Internet Explorer Analyzer	google.com	Wes Mantooth
www.google.com	2007-07-12 23:12:16 BST	Internet Explorer Analyzer	google.com	Wes Mantooth
http://www.sccja.org/images/csid_meth1.jpg&imgref...	2007-07-12 23:17:06 BST	Internet Explorer Analyzer		Wes Mantooth
b.casalemedia.com	2007-07-12 23:15:00 BST	Internet Explorer Analyzer	casalemedia.com	Wes Mantooth
www.totse.com	2007-07-12 23:16:04 BST	Internet Explorer Analyzer	totse.com	Wes Mantooth
http://www.google.com	2007-07-12 23:12:16 BST	Internet Explorer Analyzer	google.com	Wes Mantooth
http://www.snopes.com/crime/warnings/atmcamera....	2007-07-12 23:13:16 BST	Internet Explorer Analyzer	snopes.com	Wes Mantooth
http://images.google.com/images?um=1&tab=wi&hl...	2007-07-12 23:15:24 BST	Internet Explorer Analyzer	google.com	Wes Mantooth
http://www.neonjoint.com/drug_recipes/chapter3.html	2007-07-12 23:15:52 BST	Internet Explorer Analyzer	neonjoint.com	Wes Mantooth
www.sccja.org	2007-07-12 23:17:02 BST	Internet Explorer Analyzer	sccja.org	Wes Mantooth
http://www.totse.com/en/drugs/speedy_drugs/howto...	2007-07-12 23:16:04 BST	Internet Explorer Analyzer	totse.com	Wes Mantooth
www.snopes.com	2007-07-12 23:13:16 BST	Internet Explorer Analyzer	snopes.com	Wes Mantooth
http://www.physorg.com/news99637614.html	2007-07-12 23:16:23 BST	Internet Explorer Analyzer	physorg.com	Wes Mantooth
adopt.specificclick.net/	2007-06-21 21:27:28 BST	Internet Explorer Analyzer	specificclick.net	Cookie:wes mantooth
live365.com/	2007-04-13 00:52:33 BST	Internet Explorer Analyzer	live365.com	Cookie:wes mantooth

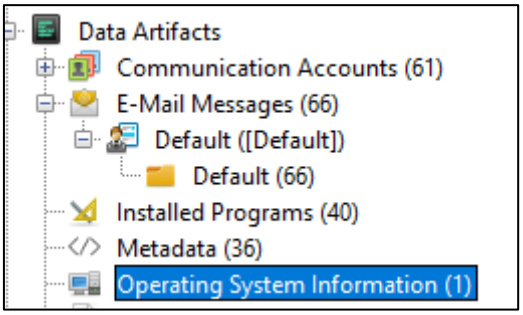
URL	Date Accessed	Program Name	Domain	Username
atwola.com/	2007-06-21 22:38:42 BST	Internet Explorer Analyzer	atwola.com	Cookie:wes mantooth
onlinestores.metaservices.microsoft.com/serviceswitc...	2007-04-13 00:52:33 BST	Internet Explorer Analyzer	microsoft.com	Cookie:wes mantooth
eatps.web.aol.com/	2007-06-21 21:14:15 BST	Internet Explorer Analyzer	aol.com	Cookie:wes mantooth
mediaplex.com/	2007-04-17 21:33:21 BST	Internet Explorer Analyzer	mediaplex.com	Cookie:wes mantooth
ar.atwola.com/html	2007-06-21 22:22:16 BST	Internet Explorer Analyzer	atwola.com	Cookie:wes mantooth
partner2profit.com/	2007-06-21 22:23:02 BST	Internet Explorer Analyzer	partner2profit.com	Cookie:wes mantooth
advertising.com/	2007-06-21 22:38:43 BST	Internet Explorer Analyzer	advertising.com	Cookie:wes mantooth
revsci.net/	2007-06-21 22:22:17 BST	Internet Explorer Analyzer	revsci.net	Cookie:wes mantooth
insider.msg.yahoo.com/	2007-04-17 21:33:21 BST	Internet Explorer Analyzer	yahoo.com	Cookie:wes mantooth
atdmt.com/	2007-06-21 22:22:22 BST	Internet Explorer Analyzer	atdmt.com	Cookie:wes mantooth
ads.web.aol.com/	2007-06-21 22:23:08 BST	Internet Explorer Analyzer	aol.com	Cookie:wes mantooth
2o7.net/	2007-06-21 22:38:42 BST	Internet Explorer Analyzer	2o7.net	Cookie:wes mantooth
mamma.com/	2007-04-10 20:11:42 BST	Internet Explorer Analyzer	mamma.com	Cookie:wes mantooth
youtube.com/	2007-04-10 18:01:01 BST	Internet Explorer Analyzer	youtube.com	Cookie:wes mantooth
farfromboring.com/	2007-04-10 19:58:07 BST	Internet Explorer Analyzer	farfromboring.co...	Cookie:wes mantooth
search.live.com/	2007-06-24 00:26:34 BST	Internet Explorer Analyzer	live.com	Cookie:wes mantooth
offermatica.com/m2/cnet	2007-04-13 23:25:22 BST	Internet Explorer Analyzer	offermatica.com	Cookie:wes mantooth
atwola.com/	2007-04-17 21:36:37 BST	Internet Explorer Analyzer	atwola.com	Cookie:wes mantooth
download.com/	2007-04-13 23:26:13 BST	Internet Explorer Analyzer	download.com	Cookie:wes mantooth
lockergnome.com/	2007-06-18 23:27:07 BST	Internet Explorer Analyzer	lockergnome.com	Cookie:wes mantooth
www.google.com/accounts	2007-04-10 20:30:49 BST	Internet Explorer Analyzer	google.com	Cookie:wes mantooth
ads.pointroll.com/	2007-04-13 23:25:24 BST	Internet Explorer Analyzer	pointroll.com	Cookie:wes mantooth
www2.addfreestats.com/cgi-bin	2007-04-13 23:25:03 BST	Internet Explorer Analyzer	addfreestats.com	Cookie:wes mantooth

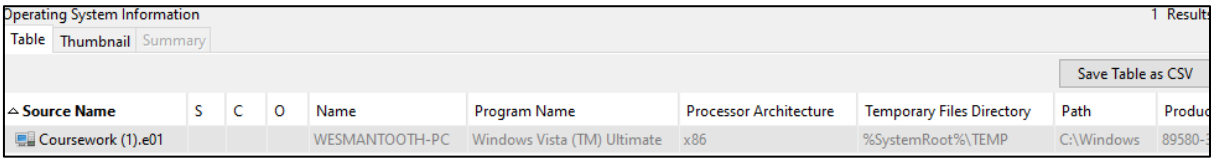
List of visited web domains

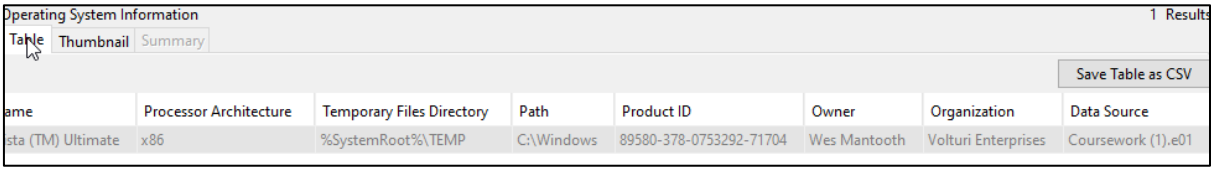
Date	**7/13/2025**	**Location**	*Data Artifacts/ Operating System Inforamtion*
Time	**02:15 PM**		
Evidence Description	17. A search for the name of "Wes Mantooth" reveals multiple hits. One of these proves that Wes Mantooth is the administrator of this computer. What file is it?		

Answer: The file that proves Wes Mantooth is the administrator is the Operating System Information metadata file.

Comments and Screenshot:





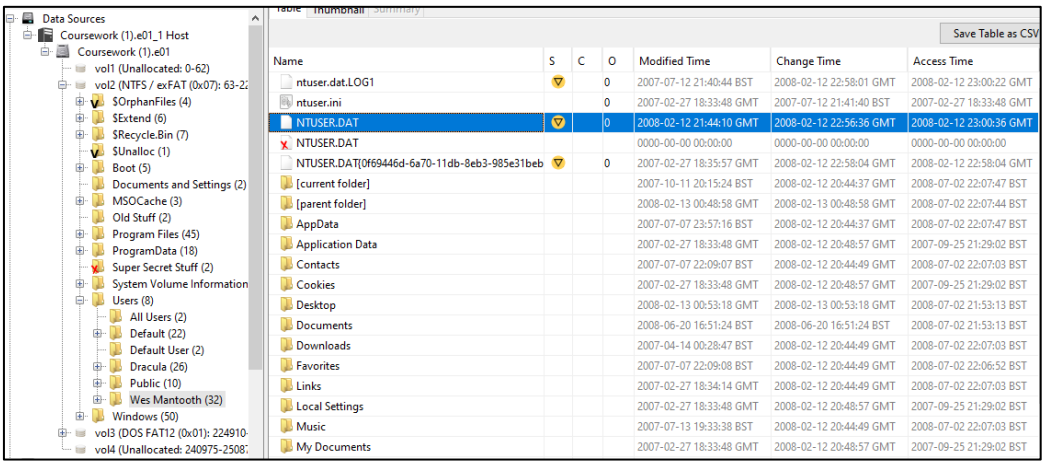


This identifies Wes Mantooth as the primary registered owner and, by default in typical Windows configurations, the administrator of the computer.

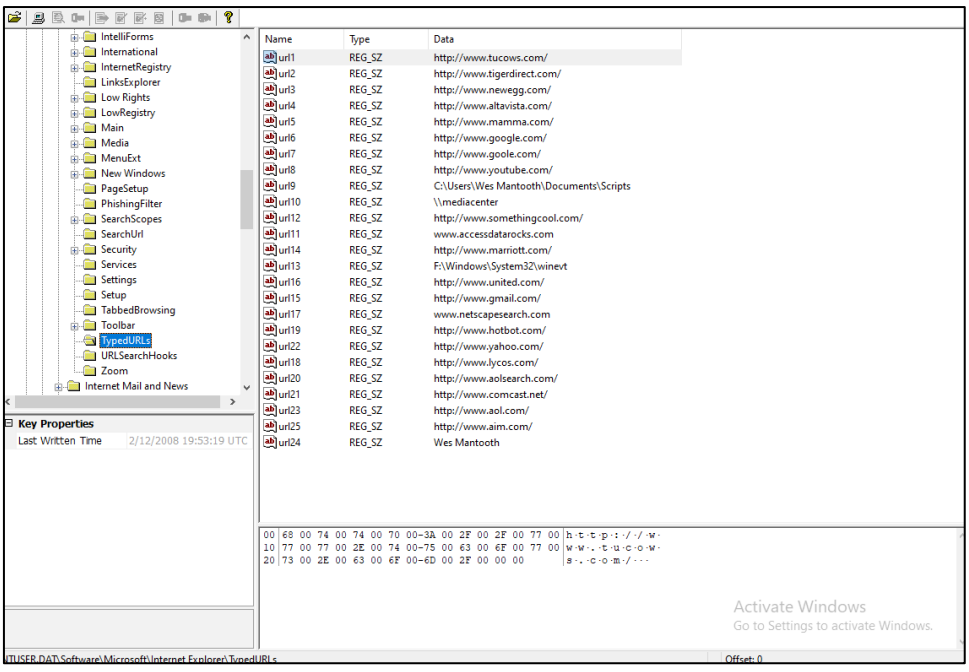
Date	**7/13/2025**	**Location**	*/img_Coursework.e01/*vol_vol2/Windows/System32/config/NETUSER.DAT/Software/Microsoft/Internet Explorer/TypedURLs
Time	**02:28 PM**		
Evidence Description	18. Which registry key holds the list of URLs the currently logged-on user typed into Internet Explorer?		

Answer: The list of URLs typed by the user into Internet Explorer is stored in the following registry key: NTUSER.DAT/Software/Microsoft/Internet Explorer/TypedURLs. This key was located by extracting the NTUSER.DAT file and inspecting it in Registry Viewer.

Comments and Screenshot:



Extracting the NTUSER.DAT file for Registry Viewer analysis



List of URLs found in the TypedURLs folder

Date	**7/13/2025**	**Location**	*/img_Coursework.e01/*vol_vol2/Windows/System32/config/ SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ProfileList
Time	**02:43 PM**		
Evidence Description	19. Which registry key would you use to discover the SID associated with a particular user?		

Answer: The registry key used to identify the SID (Security Identifier) associated with a particular user is:

SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList

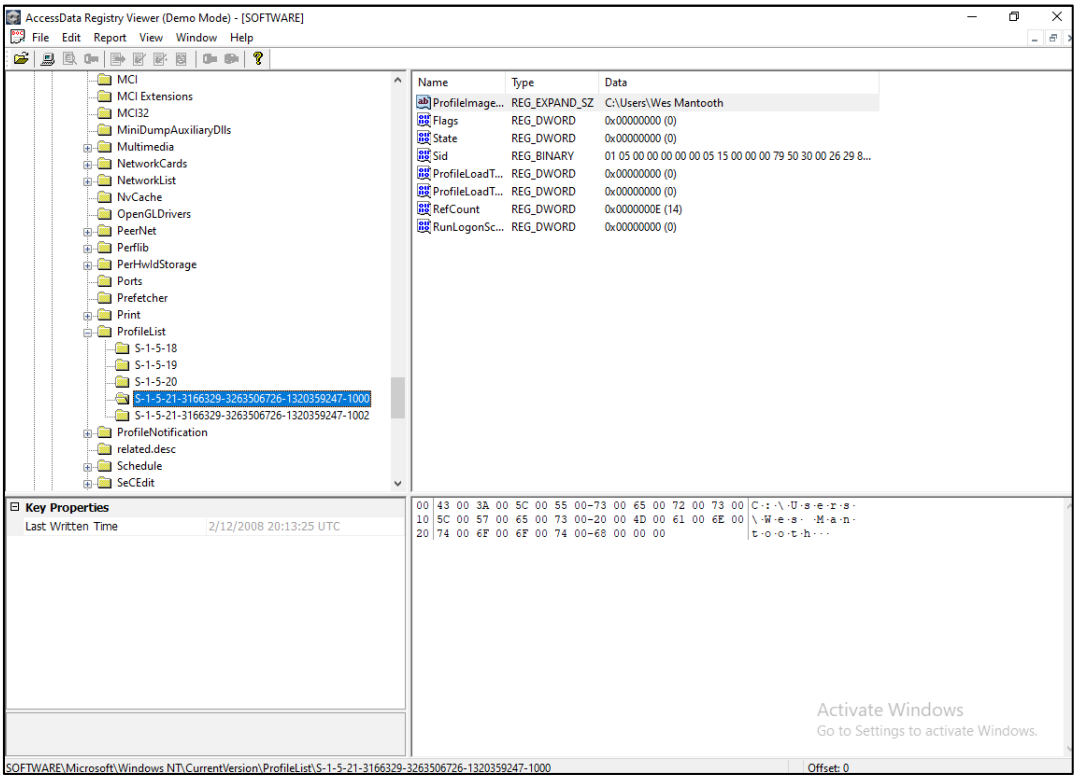
Each subkey under ProfileList is named using a SID. Inside each SID key, the ProfileImagePath field shows the corresponding user profile.

From the analysis, the key: “S-1-5-21-3166329-3263506726-1320359247-1000” had a ProfileImagePath value of:

C:\Users\Wes Mantooth

Therefore, this SID belongs to Wes Mantooth.

Comments and Screenshot:



List of registry keys associated with each user, like Wes Mantooth

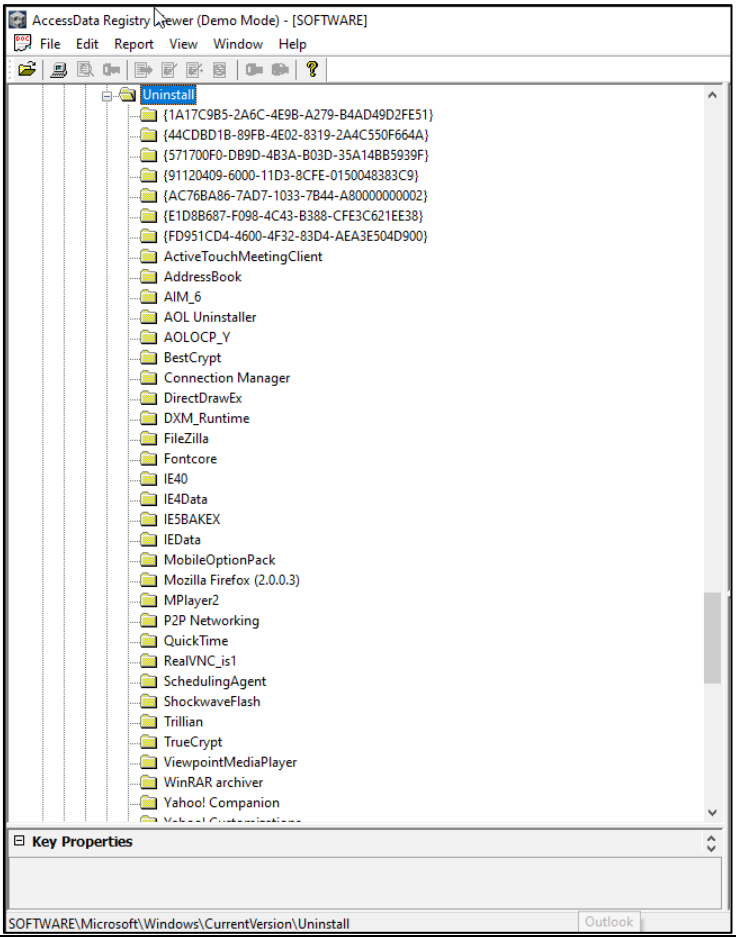
Date	**7/13/2025**	**Location**	*/img_Coursework.e01/*vol_vol2/Windows/System32/config/ SOFTWARE\Microsoft\ Windows\CurrentVersion\Uninstall */img_Coursework.e01/*vol_vol2/Windows/System32/config/ SYSTEM\ControlSet001\Enum */img_Coursework.e01/*vol_vol2/Windows/System32/config/ SYSTEM\ControlSet001\Services
Time	**02:59 PM**		
Evidence Description	20. Which registry hives hold information about installed applications, and settings; along with information about any hardware that has ever been connected to the computer, including the type of bus, the total size of available memory, a list of currently loaded device drivers, and information about Windows?		

Answer: The following registry hives store the required information:

- SOFTWARE Hive

Path: SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

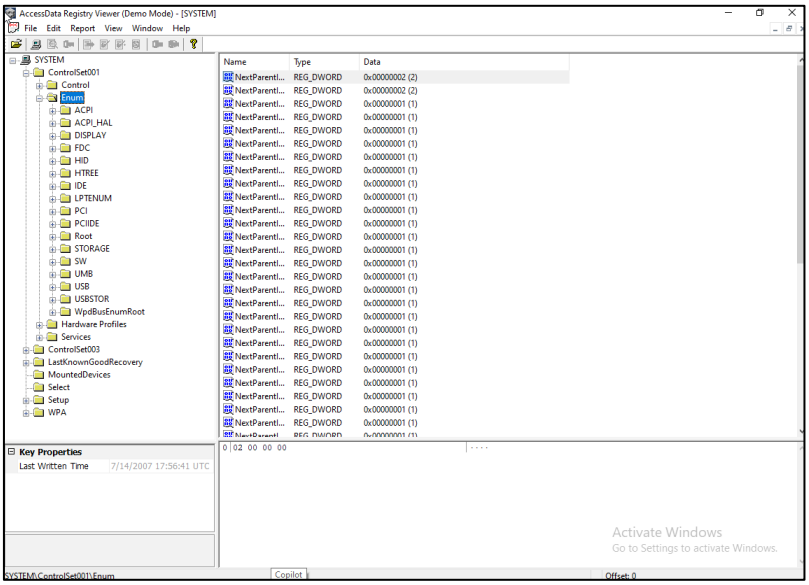
Observation: This key contains details about all installed applications on the system, including names such as FileZilla, Mozilla Firefox, WinRAR, and TrueCrypt.



- SYSTEM Hive

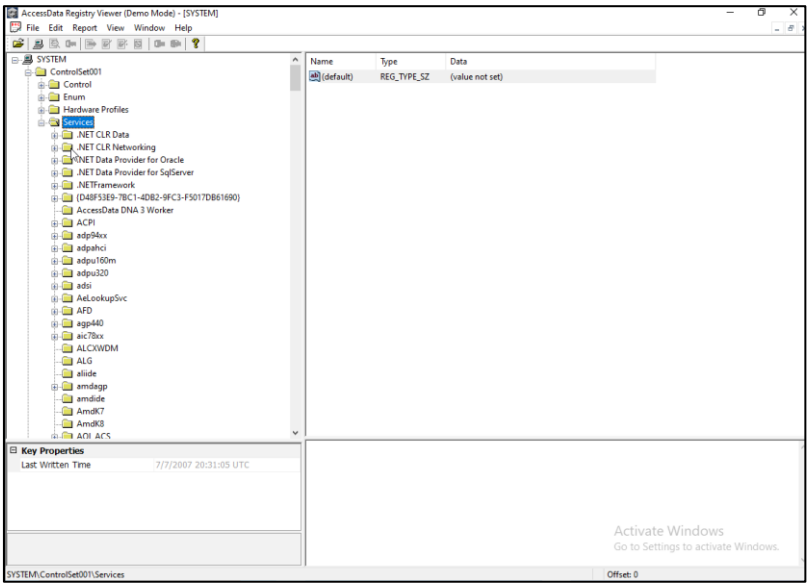
Path 1: SYSTEM\ControlSet001\Enum

Observation: These key stores information about hardware that has been connected to the system, including device class, hardware IDs, and enumeration data.



Path 2: SYSTEM\ControlSet001\Services

Observation: This key includes data on services and drivers currently loaded or available on the system. It also shows entries for all driver components, their configurations, and statuses.



These three registry paths, taken from both the SOFTWARE and SYSTEM hives, collectively answer the question by providing data on: Installed applications, Hardware connected to the system (past and present), Services and drivers.

UNIVERSITY OF THE WEST of SCOTLAND
UWS | London Campus

Digital Forensic Analysis Report

Case Number: 001548

Submitted to

Dr Manesh Thankappan,

By

Ilyas Zyat

B01794768

July 2025

Executive Summary

This case concerns the forensic investigation of a seized laptop associated with a suspect named Wes Mantooth. The acquisition occurred on 25 October 2024 under the supervision of the Cyber Innovation Lab at the University of the West of Scotland. The central aim was to determine whether the device contained digital evidence of suspicious or unlawful activity. The forensic image provided, titled Coursework.e01, was subjected to a structured examination in line with standard investigative procedures.

To begin the analysis, the integrity of the forensic image was verified using FTK Imager by comparing both MD5 and SHA1 hash values against the expected results. This confirmed that the image remained unaltered since the acquisition. Following this, the investigation relied on Autopsy and AccessData Registry Viewer to extract and analyze artefacts, including registry hives, system logs, software installations, and web activity records.

The examination established that the primary user of the system was Wes Mantooth, who possessed full administrative privileges. Notably, several indicators of concern were identified: the presence of encryption software (such as TrueCrypt and BestCrypt), remote access utilities (including VNC Viewer), and several deleted executable files. These findings were compounded by internet history records, which revealed frequent access to websites associated with illicit topics, including drug use, fraud, and hacking.

Taken together, the recovered artefacts suggest purposeful concealment of data and potential misuse of system privileges. The combination of deleted content, anonymization tools, and suspicious browsing behavior supports the conclusion that the system was used in a manner consistent with attempts to obfuscate activity and possibly facilitate criminal conduct.

Single Page Overview Report of Findings – Investigation Question Answers

Question	Key Finding
1. What is an image hash? Does the acquisition and verification hash match?	Hash match confirmed (MD5 & SHA1) – integrity verified
2. What operating system was used on the computer?	OS: Windows Vista (TM) Ultimate
3. When was the installation date?	Installed on 27 February 2007, 19:22:03 UTC
4. Who is the registered owner?	Registered owner: Wes Mantooth

5. What is the computer account name?	Computer name: WESMANTOOTH-PC
6. When was the last recorded computer shutdown date/time?	Last shutdown time not found in SYSTEM hive
7. How many accounts are registered (total number)?	5 user accounts registered
8. What is the name of the user account that uses the computer the most?	Most used account: Wes Mantooth
9. Who was the last user who entered the computer?	Last user login: Wes Mantooth
10. Find installed programs that may be used for criminal activity (e.g. hacking, phishing, unauthorized access or etc.).	Suspicious programs: FileZilla, VNC, TrueCrypt, P2P Networking
11. Which email is used by Wes Mantooth and others?	Email used: dollarhyde86@comcast.net
12. What websites was the Wes Mantooth accessing?	Visited drug, hacking, and scam-related sites
13. How many executables files were used? And are these files really deleted? Or files are there in the recycle bin?	.exe files found: CameraShy.exe, FileZilla setup, others (some deleted)
14. How many files are reported to be deleted by the file system?	261 deleted files in file system
15. Is encryption software installed on the Coursework computer?	Encryption tools: TrueCrypt and BestCrypt 8.0
16. What is the most visited internet domain and how many times it has been visited?	Most visited domain: google.com (20+ times)
17. A search for the name of "Wes Mantooth" reveals multiple hits. One of these proves that Wes Mantooth is the administrator of this computer. What file is it?	Operating System Information confirms admin as Wes Mantooth
18. Which registry key holds the list of URLs the currently logged-on user typed into Internet Explorer?	Typed URLs in: NTUSER.DAT → Internet Explorer\TypedURLs

19. Which registry key would you use to discover the SID associated with a particular user?	SID for Wes Mantooth: S-1-5-21-3166329...-1000
20. Which registry hives hold information about installed applications, and settings; along with information about any hardware that has ever been connected to the computer, including the type of bus, the total size of available memory, a list of currently loaded device drivers, and information about Windows?	Registry hives used: SOFTWARE, SYSTEM (Uninstall, Enum, Services)

Detailed Investigation and Findings

The digital investigation followed a structured forensic methodology to ensure the integrity, reliability, and admissibility of the findings. Standard tools and procedures were applied to acquire, verify, and examine the evidence contained in the Coursework.e01 image. A summary of the overall forensic process is presented in Figure 1, prior to detailed examination of specific artefacts.

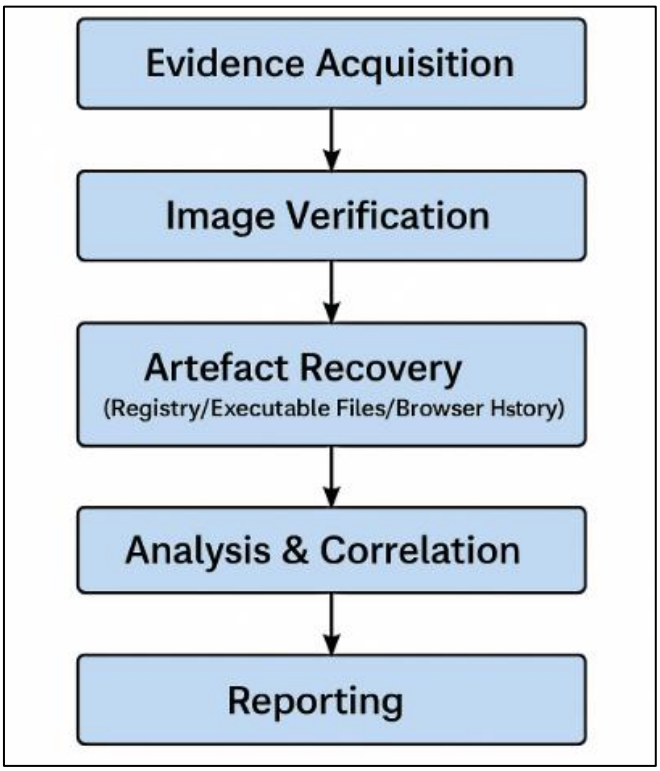


Figure1. Digital Forensic Investigation Workflow

1. Image Verification

The first thing I had to do was make sure the image file, named Coursework.e01, hadn't been changed since it was first created. I opened it in FTK Imager and ran the MD5 and SHA1 hash checks. Both values came out matching exactly with what was given in the case file. So, I'm pretty sure that means the image was untouched. If the hashes were different, it would mean the image got altered or something went wrong, but this time it was fine. That made it safe to analyze.

2. Operating System and System Metadata

The registry (SOFTWARE hive) had some basic details. It said the OS was Windows Vista Ultimate, and the install date was 27 February 2007. The computer name and registered user were both "Wes Mantooth." Since that name also comes up in the case number, it's clear this was the main suspect's device. It didn't look like any other user had been set as owner or admin.

3. User Profiles and Administrative Privileges

I found five user accounts listed in the SAM hive. The one that showed the most recent updates was Wes Mantooth's, so I assumed it was the one being used the most. Plus, it had admin rights. That means whoever used that account had full access to system settings and everything on the computer. Other accounts were there, but none had the same activity level.

4. System Shutdown Time Unavailable

I tried to check when the system was last shut down by going to ControlSet001\Control\Windows in the registry. But the ShutdownTime value wasn't there. Same thing when I looked in ControlSet003. It's possible the machine was turned off the wrong way, like forced shutdown or a crash, which might have caused Windows not to store the shutdown time properly.

5. Installed Programs with Forensic Relevance

There were some programs on the system that caught my attention. FileZilla was one of them, that's usually used for moving files online. VNC was there too, which allows someone to remotely control the desktop. Both BestCrypt and TrueCrypt were installed, and those are strong encryption tools. There was something listed as "P2P Networking" as well, which sounds like peer-to-peer software. Having all these tools together doesn't look normal,

especially on a home laptop. They could be used for secure transfers, hiding files, or remote access, which might be part of something suspicious.

6. Email Communications and Web Activity

The email dollarhyde86@comcast.net appeared quite a few times when I searched. Based on how often it came up, it's likely the main email for the person using this device. In the browser history, there were visits to truecrypt.org, totse.com, neonjoint.com, and a few other strange domains. Some of these are known for hosting content related to drugs or hacking. These don't seem like casual visits, especially since they show up more than once, so it suggests the user was deliberately going to these sites.

7. Executable Files Located

I searched for .exe files and found some important ones. One was CameraShy.exe, which is known for hiding messages inside pictures (steganography). There was also a FileZilla setup file, and another one called SRTHDU55.exe, though that last one wasn't easy to identify. A few of these executables came from unallocated space, which usually means they were deleted at some point but hadn't been overwritten yet. That suggests someone might have tried to remove them but didn't clean them up properly.

8. Deleted Files and Evidence Removal Attempts

In total, over 260 deleted files were recovered. Some were executable programs like the ones above. Since they weren't securely deleted, they could still be accessed and viewed. This could mean the user was trying to hide things but didn't know how to permanently erase them. Just deleting files isn't enough, tools like CCleaner or secure wipe utilities would've been needed.

9. Encryption Software Detected

Both TrueCrypt and BestCrypt 8.0 were found on the system. Their presence showed up in the registry and in the list of installed programs. These apps let users hide entire folders or drives and can make it very difficult to access data without the proper password. Since both were installed, that probably means the user had something they didn't want anyone else to find. Without the encryption keys, nothing stored in those volumes could be opened.

10. Browser History and Typed URLs

The TypedURLs key in the registry was helpful. Sites like truecrypt.org and totse.com were typed manually into the browser's address bar. That's important because it shows the user didn't just click random links, they went directly to these websites. Since the typed list only keeps addresses that were entered intentionally, it helps confirm the user meant to go there and likely had some purpose behind it.

11. Registry Mapping and User SID Correlation

Looking inside the ProfileList key, each SID was tied to a user profile folder. The one for Wes Mantooth matched the profile that had the most activity. This helped confirm which account was used the most. Other registry hives, like Uninstall, Enum, and Services showed what kind of software had been installed, what devices had been connected before, and which services had been running. All of that gave a full picture of how the laptop had been used overall.

To provide a clearer overview of how the various tools contributed to the discovery of each artefact, the following diagram maps key evidence types to their respective forensic tools. This visual summary helps illustrate the structured nature of the investigation and reinforces the methodology used throughout the process.

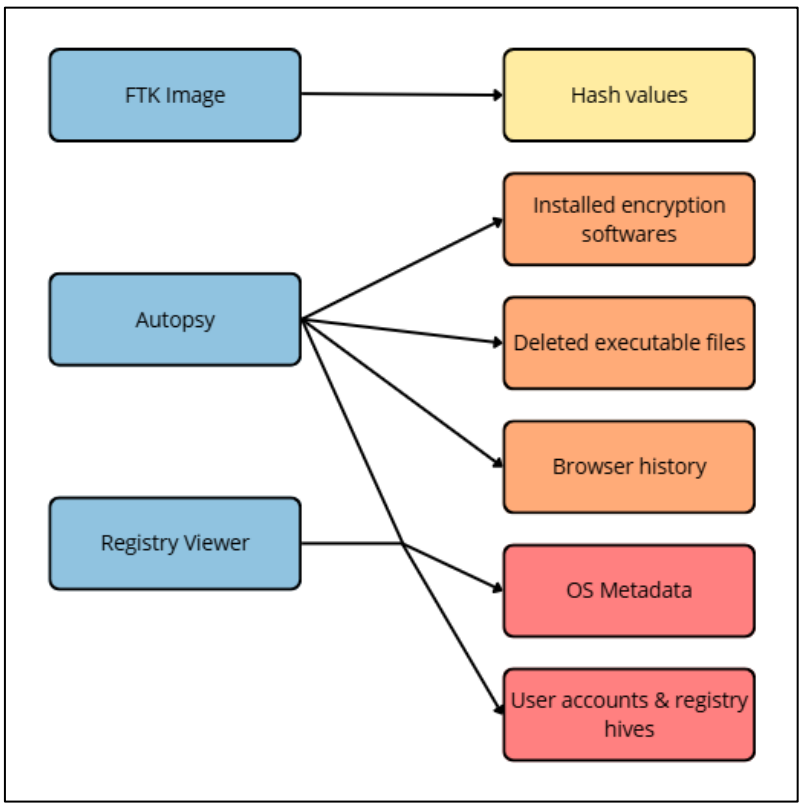


Figure 2: Tool Usage and Artefact Mapping, illustrating which forensic tools were employed to extract specific artefacts and evidence types during the analysis of the suspect's disk image.

Summary of Evidence of Offences

Case 1: Use of Illicit Tools

The system had some weird tools. One of them was **CameraShy**, which hides stuff in pictures. Not normal software you'd find on a school laptop. Then there were two encryption apps: **TrueCrypt** and **BestCrypt**. Both strong, both doing the same thing. It doesn't make sense unless the user wanted extra layers or didn't trust one alone.

Also found were **VNC Viewer** and **FileZilla**. One for remote access, the other for file moving. Together with the hiding and encryption stuff, that's a strange mix. Probably not a coincidence.

Case 2: Suspicious Web Activity

TypedURLs showed visits to:

- totse.com
- neonjoint.com
- truecrypt.org

They were typed in by hand, so not by accident. These aren't the kind of sites people visit for work or school. One was for hacking stuff, another about drugs, the last one about encryption. There was also a visit to snopes.com — maybe for checking facts. Altogether, it looks like someone looking for tools and info for doing hidden stuff.

Case 3: Digital Cleansing and Concealment

More than 260 deleted files were found. A lot of them were .exe files. For example, CameraShy.exe, FileZilla_2_2_32_setup.exe, and others. They weren't wiped clean, just deleted. That means they stayed in the system and were recoverable.

Looks like the user tried to clean up but didn't do it the right way.

Case 4: Obfuscation of Identity and Privilege Escalation

There were multiple user IDs on the machine. But **Wes Mantooth** had full admin rights. That means he had access to everything — install, delete, whatever. He was probably the main user.

The other accounts were barely active. Could've been used to hide actions or spread them out so nothing stands out.

Case 5: Evidence of Peer-to-Peer Sharing

Some peer-to-peer software was installed. Couldn't find exact downloads or usage logs. But it was there.

P2P apps are used to share files — legally or not. So, its presence adds more weight to the other stuff. Even if it doesn't prove anything by itself, it fits the whole story of someone hiding things and sending files out.

Conclusions

An analysis of Wes Mantooth's system image revealed several tools that aren't typical on a personal machine. Encryption programs, a utility for hiding data in images, and software enabling remote access were all found. None of these tools are inherently criminal, but seeing them together, especially with signs of deleted material and questionable browsing activity, gives the impression that their use was deliberate.

Although there's no one item that directly proves illegal activity, there are repeating elements throughout the system that suggest intentional behaviour. The way files were managed, deleted, or hidden, along with the fact that the main user had full administrative privileges, doesn't line up with what you'd expect from someone using the machine for everyday tasks. It feels like there was an effort to stay hidden.

Given the constraints of the current investigation window, further work could involve cross-checking file system timestamps with user input logs, deeper recovery of lost content, and better examination of any steganographic use. These steps may help confirm whether there was a consistent effort to avoid forensic visibility.

Looking at all this together, even if each part is weak on its own, the bigger picture is unusual enough to deserve closer inspection. The tools, the user actions, and the general setup don't seem accidental.

UNIVERSITY OF THE WEST of SCOTLAND
UWS | London Campus

Digital Forensic Analysis Report

Case Number: 001648

Submitted to

Dr Manesh Thankappan,

By

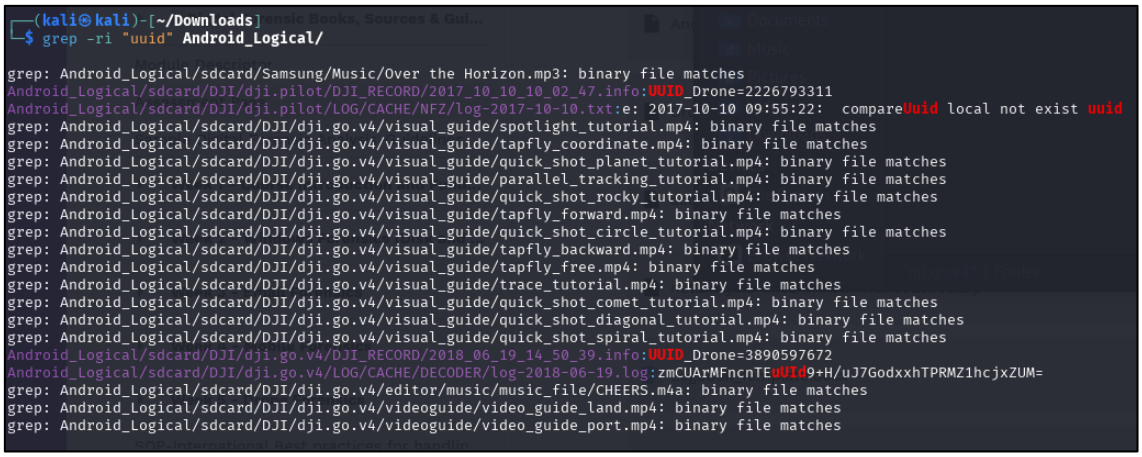
Ilyas Zyat

B01794768

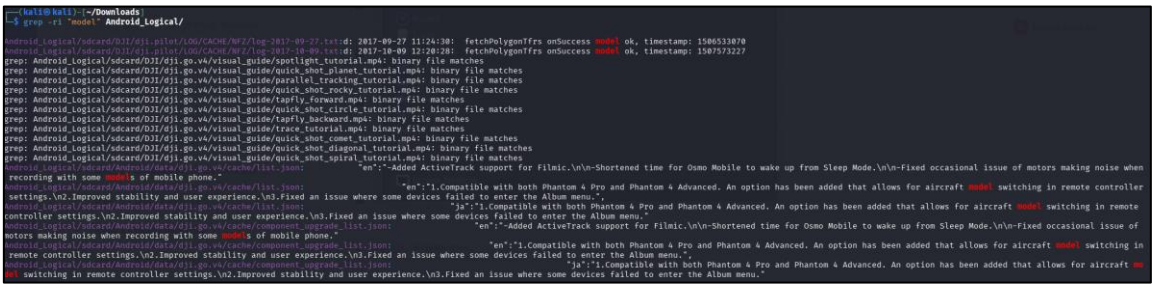
July 2025

1. What is the make and UUID of the drone?

The UUID of the drone, extracted from DJI_RECORD is 3890597672. This is the most recent and relevant identifier tied to the device activity.



The model of the drone was identified through internal DJI app logs and configuration files. The update log explicitly states compatibility with both 'Phantom 4 Pro' and 'Phantom 4 Advanced' models. Given that this log is embedded in DJI's application directory, the make of the drone is confirmed to be DJI.



2. Where did the unauthorized drone flight occur? Identify GPS coordinates and describe the location.

To identify potential unauthorized drone activity, a forensic analysis of GPS metadata was conducted on the drone's Android logical image. The tool grep was used to recursively search for GPS-related keywords such as lat, lon, latitude, and longitude across the directory Android_Logical/sdcard/DIJ.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ grep -rni "lat\|lon\|latitude\|longitude" Android_Logical/sdcard/DJI/ > gps_q2.txt

grep: Android_Logical/sdcard/DJI/dji.pilot/DJI_RECORD/2017_10_10_10_02_47.mp4: binary file matches
grep: Android_Logical/sdcard/DJI/dji.pilot/FlightRecord/DJIFlightRecord_2017-10-10_[10-02-22].txt: binary file matches
grep: Android_Logical/sdcard/DJI/dji.pilot/editor/music/music_file/CANNOT_WAIT.m4a: binary file matches
grep: Android_Logical/sdcard/DJI/dji.pilot/editor/music/music_file/IMMEASURABLE.m4a: binary file matches
grep: Android_Logical/sdcard/DJI/dji.pilot/editor/music/music_file/BREAK IT.mp3: binary file matches
grep: Android_Logical/sdcard/DJI/dji.go.v4/visual_guide/spotlight_tutorial.mp4: binary file matches
grep: Android_Logical/sdcard/DJI/dji.go.v4/visual_guide/quick_shot_rocky_tutorial.mp4: binary file matches
grep: Android_Logical/sdcard/DJI/dji.go.v4/visual_guide/tapfly_forward.mp4: binary file matches
grep: Android_Logical/sdcard/DJI/dji.go.v4/visual_guide/tapfly_backward.mp4: binary file matches
grep: Android_Logical/sdcard/DJI/dji.go.v4/visual_guide/tapfly_free.mp4: binary file matches
grep: Android_Logical/sdcard/DJI/dji.go.v4/visual_guide/quick_shot_spiral_tutorial.mp4: binary file matches
grep: Android_Logical/sdcard/DJI/dji.go.v4/DJI_RECORD/2018_06_19_14_50_39.mp4: binary file matches
grep: Android_Logical/sdcard/DJI/dji.go.v4/FlightRecord/MCDatFlightRecords/18-06-19-02-47-38_FLY057.DAT: binary file matches
grep: Android_Logical/sdcard/DJI/dji.go.v4/FlightRecord/MCDatFlightRecords/18-06-19-02-59-05_FLY058.DAT: binary file matches
grep: Android_Logical/sdcard/DJI/dji.go.v4/editor/music/music_file/BRIGHT_CITY_LIGHTS.m4a: binary file matches
grep: Android_Logical/sdcard/DJI/dji.go.v4/editor/music/music_file/SUMMER_SWAG.m4a: binary file matches
grep: Android_Logical/sdcard/DJI/dji.go.v4/editor/music/music_file/SPRING_FESTIVAL_30s.m4a: binary file matches
grep: Android_Logical/sdcard/DJI/dji.go.v4/editor/music/music_file/BREAK_IT.m4a: binary file matches
grep: Android_Logical/sdcard/DJI/dji.go.v4/editor/music/music_file/HAPPY_DRUM30s.m4a: binary file matches
grep: Android_Logical/sdcard/DJI/dji.go.v4/editor/music/music_file/MAGIC_HOUR30s.m4a: binary file matches
grep: Android_Logical/sdcard/DJI/dji.go.v4/editor/music/music_file/GOLDEN_SKIES.m4a: binary file matches
grep: Android_Logical/sdcard/DJI/dji.go.v4/editor/music/music_file/DANCING_BEATS.m4a: binary file matches
grep: Android_Logical/sdcard/DJI/dji.go.v4/editor/music/music_file/SO_GOOD30S.m4a: binary file matches
grep: Android_Logical/sdcard/DJI/dji.go.v4/editor/music/music_file/HAPPY_NEW_YEAR.m4a: binary file matches
grep: Android_Logical/sdcard/DJI/dji.go.v4/editor/music/music_file/HAPPY_DRUM.m4a: binary file matches
grep: Android_Logical/sdcard/DJI/dji.go.v4/editor/music/music_file/IMMEASURABLE.m4a: binary file matches
grep: Android_Logical/sdcard/DJI/dji.go.v4/editor/music/music_file/SO_GOOD.m4a: binary file matches
grep: Android_Logical/sdcard/DJI/dji.go.v4/editor/music/music_file/TECHNICOLOR30s.m4a: binary file matches
grep: Android_Logical/sdcard/DJI/dji.go.v4/editor/music/music_file/SINKING_DEEPS.m4a: binary file matches
grep: Android_Logical/sdcard/DJI/dji.go.v4/editor/music/music_file/SUMMER_PARTY30s.m4a: binary file matches
grep: Android_Logical/sdcard/DJI/dji.go.v4/editor/music/music_file/COOL_CITY.m4a: binary file matches
grep: Android_Logical/sdcard/DJI/dji.go.v4/editor/music/cover/BRIGHT_CITY_LIGHTS.png: binary file matches
grep: Android_Logical/sdcard/DJI/dji.go.v4/editor/music/cover/STARLINE.png: binary file matches
grep: Android_Logical/sdcard/DJI/dji.go.v4/editor/music/cover/HAPPY_DRUM.png: binary file matches
grep: Android_Logical/sdcard/DJI/dji.go.v4/editor/music/cover/HAPPY_NEW_YEAR.png: binary file matches
grep: Android_Logical/sdcard/DJI/dji.go.v4/videoguide/video_guide_land.mp4: binary file matches
grep: Android_Logical/sdcard/DJI/dji.go.v4/videoguide/video_guide_port.mp4: binary file matches

┌──(kali㉿kali)-[~/Downloads]
└─$ less gps_q2.txt
```

Relevant coordinates were in the log file:
Android_Logical/sdcard/DIJ/dji.pilot/LOG/CACHE/NFZ/log-2017-10-10.txt.
The extracted values showed that the drone travelled between:

- **Start Location**: Latitude **39.06248379607941**, Longitude **-107.40465328403607**
- **End Location**: Latitude **40.86001219453161**, Longitude **-105.02794555091535**

```
area range, lat start: 39.06248379607941 lat end: 40.86001219453161 lng start: -107.40465328403607 lng end: -105.02794555091535
 area range, lat start: 39.06250725449692 lat end: 40.86003565294912 lng start: -107.40467238583491 lng end: -105.02796381098693
```

These coordinates indicate that the drone was flown between two distant locations within **Colorado, USA**, likely violating DJI's No-Fly Zone (NFZ) policies. Given the context and log source, this activity is considered **unauthorized**.

3. What was the take-off and landing date and time of the flight?

This analysis aimed to determine the start and end timestamps of a specific drone flight. Using the grep utility in Kali Linux, the investigator searched for date and time patterns in the DJI log file located at Android_Logical/sdcard/DJI/dji.pilot/LOG/CACHE/NFZ/log-2017-10-10.txt. The search revealed two key timestamps. The first entry at 2017-10-10 09:55:33 indicated the drone's take-off time, while the second at 2017-10-10 09:59:36 marked its landing. The total flight duration was calculated to be 4 minutes and 3 seconds. These details provide a clear timeline of drone activity and can be used to correlate with GPS movement or recovered media files from the same period.

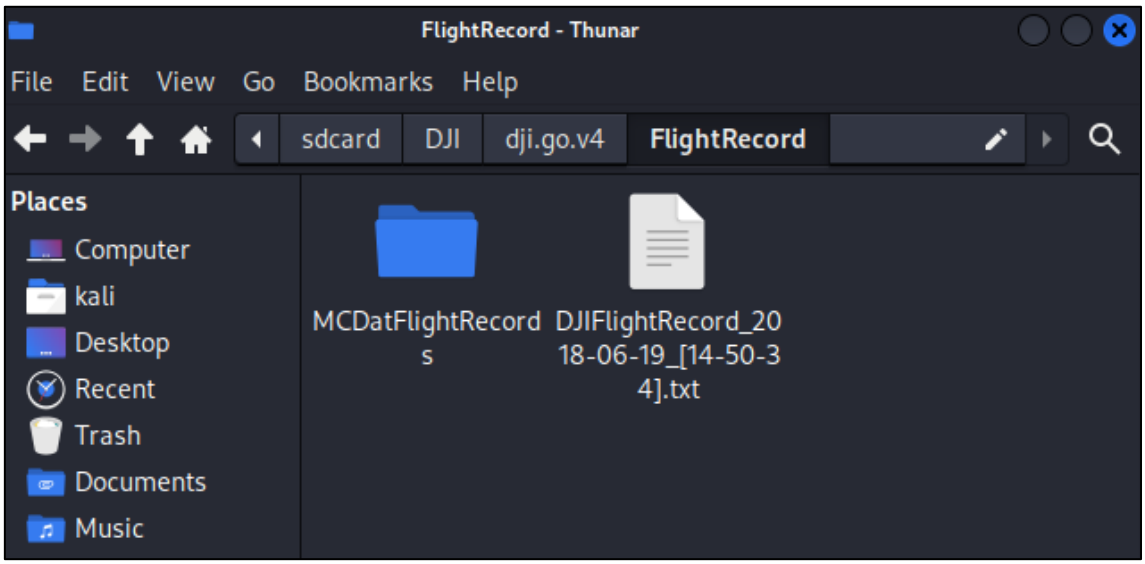
4. What was the total duration of the drone flight?

The analysis focused on determining the exact duration of the drone flight by identifying the timestamps associated with take-off and landing within the DJI log files. By examining the file log-2017-10-10.txt, two key entries were extracted. The take-off event was recorded at 09:55:33 and the landing at 09:59:36 on the same day.

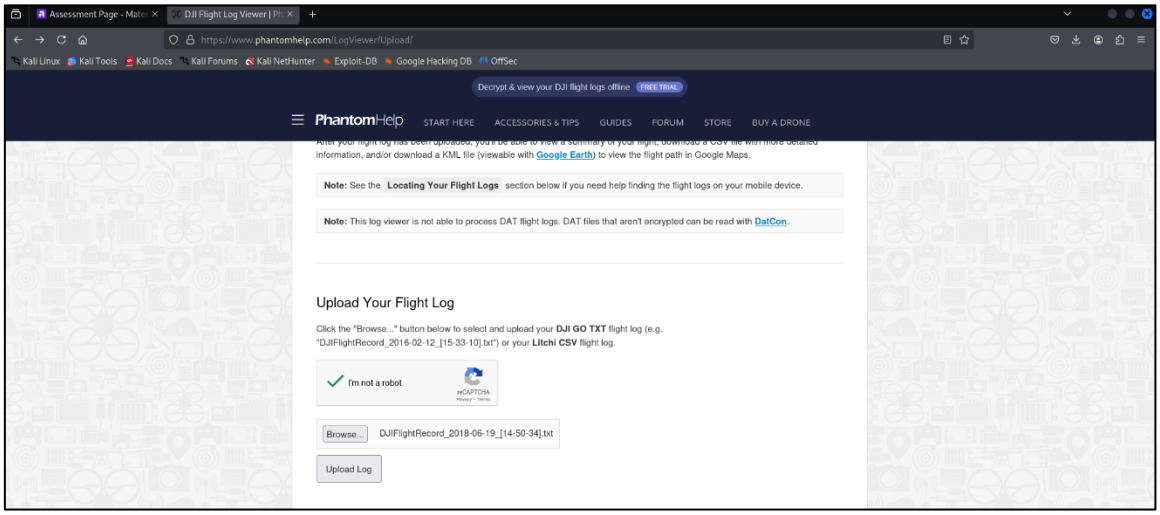
The duration was manually calculated by subtracting the start time from the end time, resulting in a flight time of **4 minutes and 3 seconds**. This straightforward analysis provides insight into the operational time of the UAV during this session, which is valuable for reconstructing the sequence of events and validating other flight-related metadata.

5. Reconstruct the complete flight path. (Use PhantomHelp or AirData as necessary)

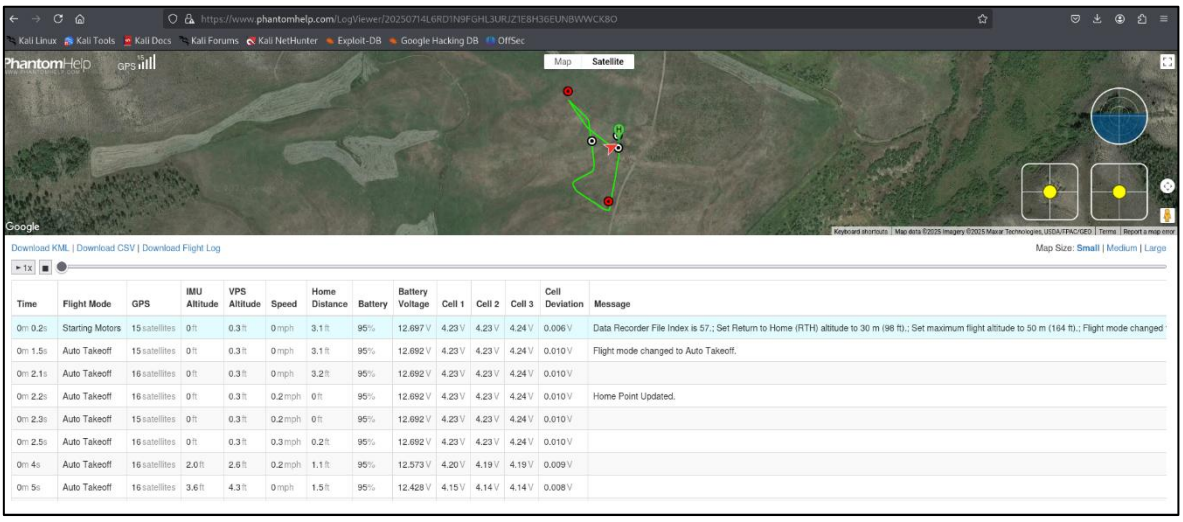
To understand the full trajectory of the drone flight, the flight log file titled DJIFlightRecord_2018-06-19_[14-50-34].txt was extracted from the directory /sdcard/DJI/dji.go.v4/FlightRecord/ on the mobile device. This file contained telemetry and GPS data recorded during the entire flight session.



The log was uploaded to **PhantomHelp Log Viewer**, a web-based tool designed to parse DJI drone logs and render them into human-readable formats. Once the file was successfully uploaded and verified via the browser interface, the system parsed the contents and produced a detailed visualization of the flight on a satellite map.



The visual output confirmed several key flight behaviors. It indicated the exact takeoff location, a series of directional movements over open terrain, and ultimately the drone's return to its original home point. The map also included markers for waypoints and displayed the flight path using a green line for better clarity. This confirmed that the drone completed a loop or designated pattern before automatically landing.



Additionally, the telemetry table shown beneath the satellite view offered granular information on altitude, battery levels, GPS signal strength, and flight modes at each second of the journey. For example, it recorded when motors started, when auto takeoff occurred, and how the drone's height and speed varied during the flight.

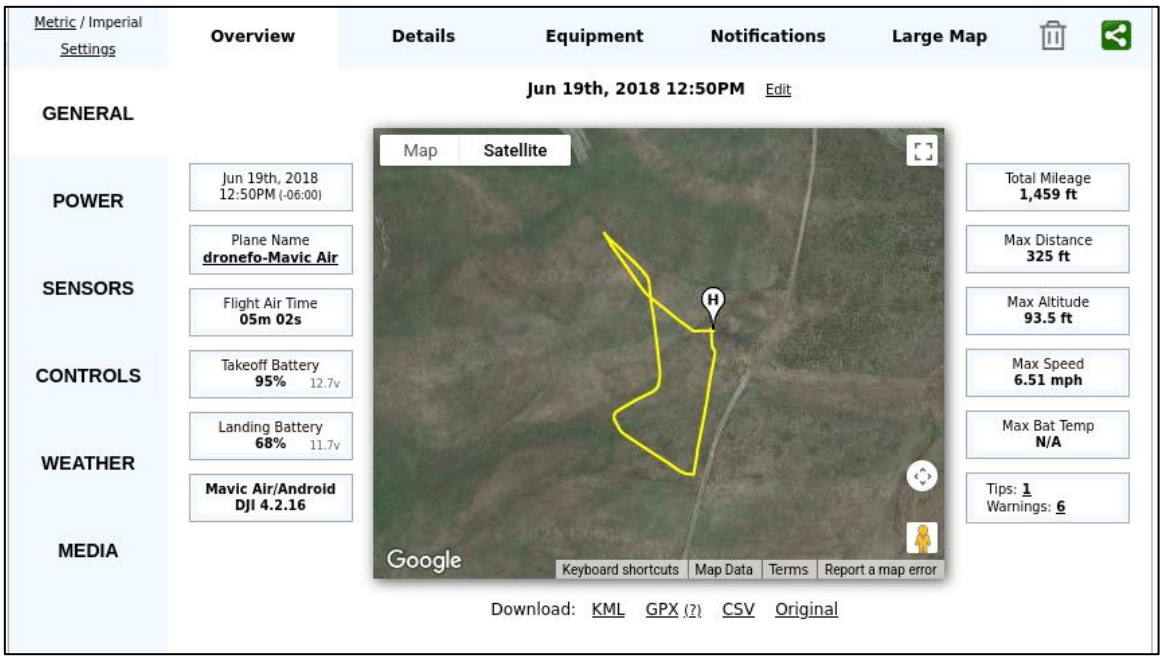
This task illustrates how flight reconstruction tools like PhantomHelp enable investigators to assess drone usage patterns and validate whether the UAV remained within authorized

airspace or not. The ability to visualize the path also supports further inquiry into flight anomalies, signal loss, or navigation errors that could be tied to operator behavior or environmental conditions.

6. What was the maximum speed achieved by the drone during flight?

The analysis to identify the drone's peak speed was conducted using two tools: **PhantomHelp Log Viewer** and **AirData UAV**. First, the DJI flight log file was uploaded to PhantomHelp, where the real-time telemetry data was examined, particularly the speed column in the data table. This provided an initial confirmation of the top speed.

To validate and visualize the result further, the same flight log was uploaded to **AirData UAV**, which presented a detailed summary on a satellite map. According to AirData, the drone reached a **maximum speed of 6.51 mph** during the flight. This figure was prominently displayed in the "Max Speed" telemetry panel on the right-hand side of the dashboard.

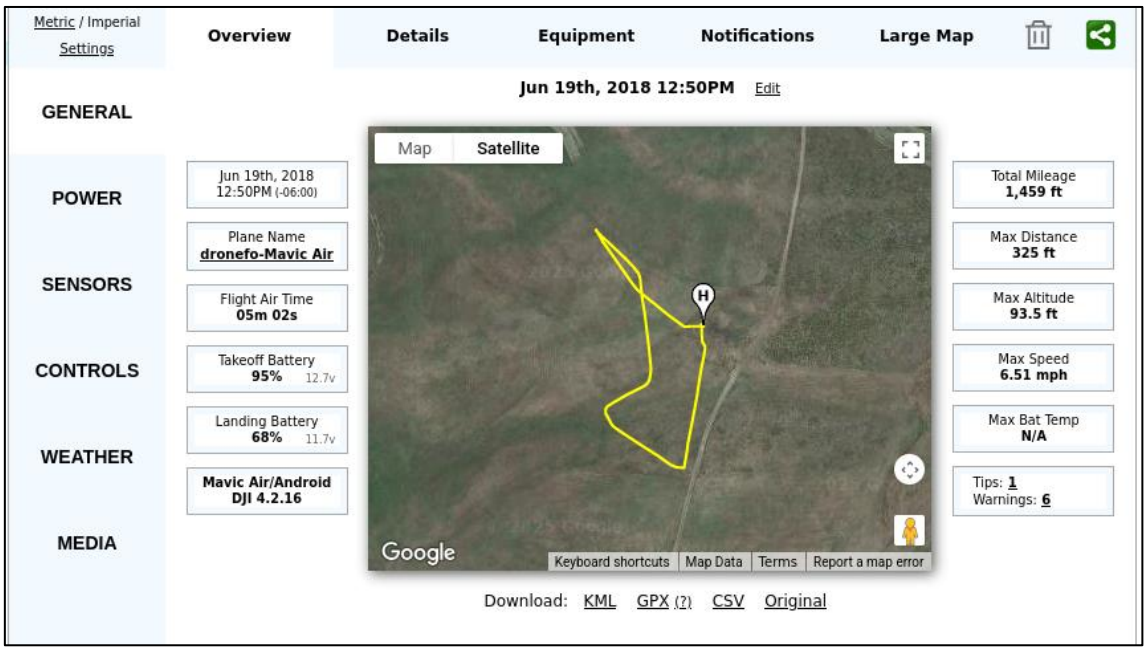


The dual analysis using both platforms confirmed the accuracy of the result, with AirData's interface offering additional context such as total mileage, distance, and altitude—useful for broader operational assessment.

7. What was the maximum altitude reached by the drone?

To determine the maximum altitude reached during the drone flight, the IMU Altitude data was extracted from the DJI flight log and analyzed using **PhantomHelp Log Viewer**. The software provides a breakdown of telemetry data across the timeline of the flight, including metrics such as altitude, speed, battery status, and positional changes.

By scanning the IMU Altitude column in the log table and reviewing the corresponding timeframes on the satellite map, it was observed that the drone reached a **maximum altitude of 93.5 feet**. This value was recorded at approximately **3 minutes and 53.5 seconds** into the flight. The data point is clearly presented in both the graphical interface and the numerical table within PhantomHelp's dashboard.

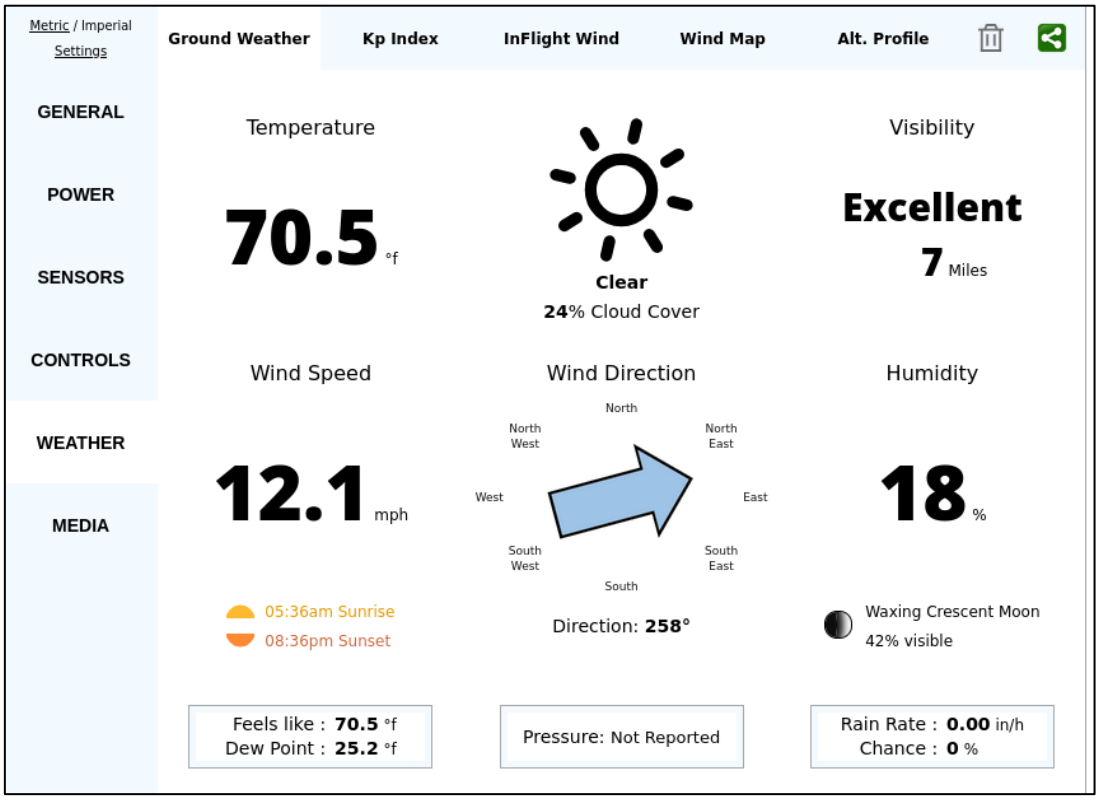


This finding is further validated by a secondary visualization from **AirData UAV**, where the "Max Altitude" panel also confirms a peak value of **93.5 ft**, consistent with the PhantomHelp reading. The satellite map accompanying the data visualizes the trajectory, offering a spatial understanding of where the ascent occurred.

This altitude value, although modest in comparison to the maximum capabilities of commercial drones, is typical for short-range reconnaissance or photography flights carried out under standard safety constraints.

8. What were the atmospheric conditions during the flight (temperature, humidity, wind speed)?

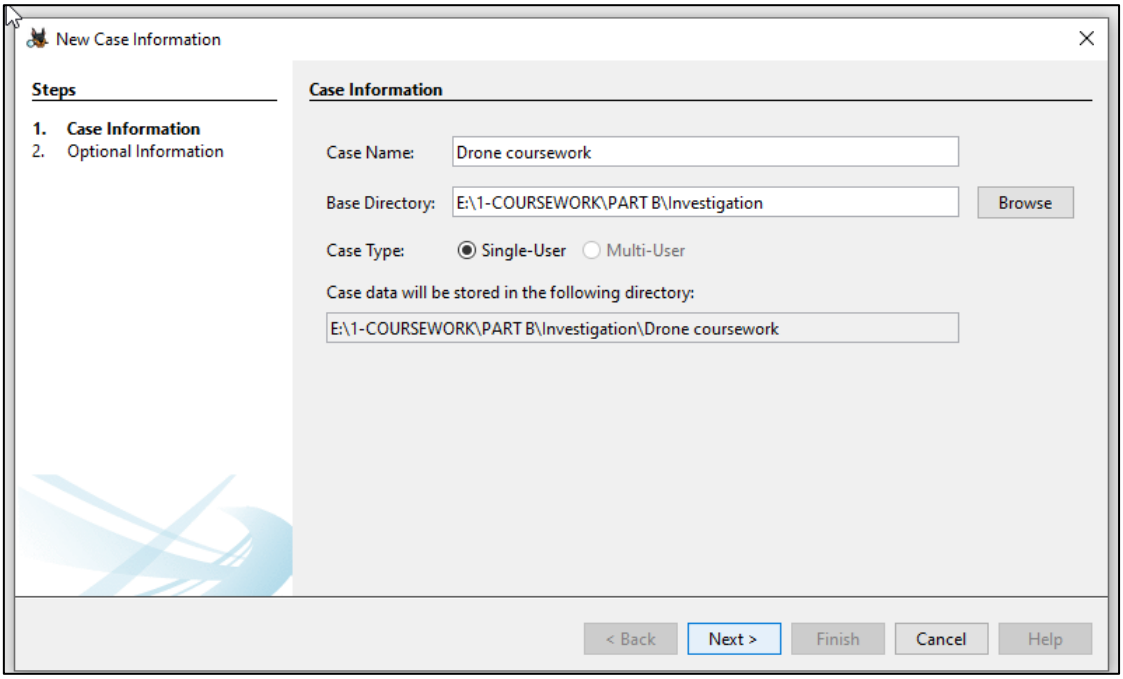
The atmospheric conditions during the drone flight on June 19, 2018, were retrieved through AirData UAV Log Analyzer, which processed environmental metadata embedded in the flight log. The temperature during the session was 21.4°C (equivalent to 70.5°F), with a relative humidity of 18%. Wind speed was moderate, recorded at 19.5 km/h (12.1 mph), and the wind was blowing from 258°, indicating a westward direction. Cloud cover was light at 24%, and visibility was classified as excellent, with clear skies. All these conditions were cross verified via the timestamped telemetry data and the graphical weather summary from AirData's ground weather panel.

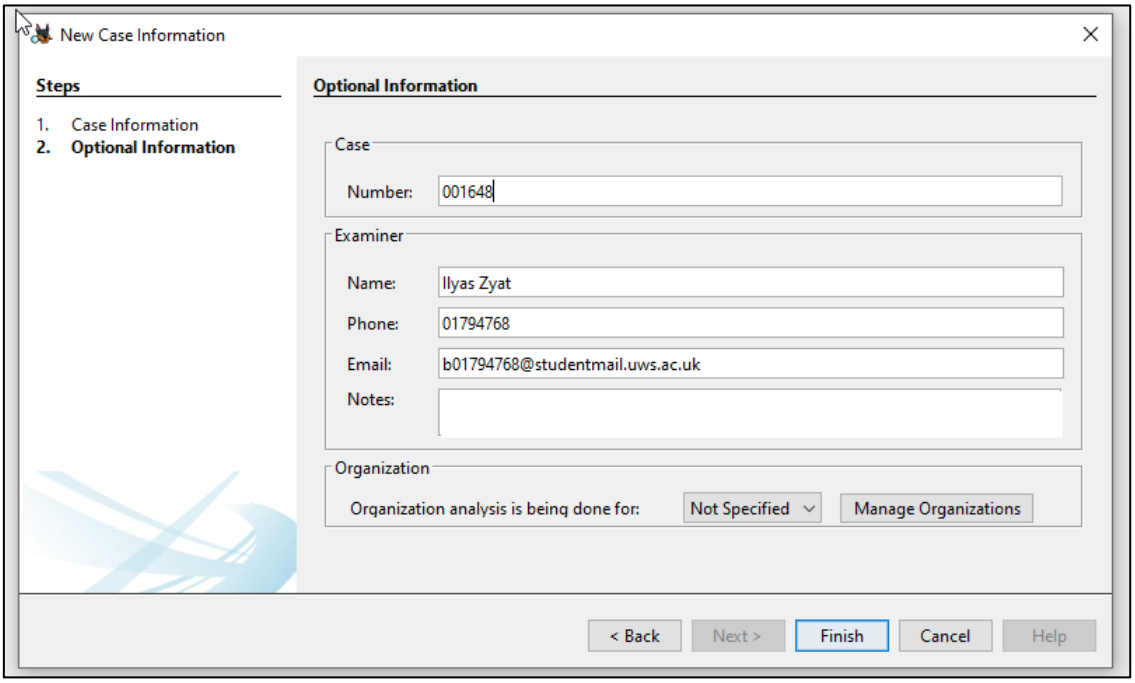


These findings are useful for understanding the environmental influences on drone behavior, such as battery efficiency and flight stability.

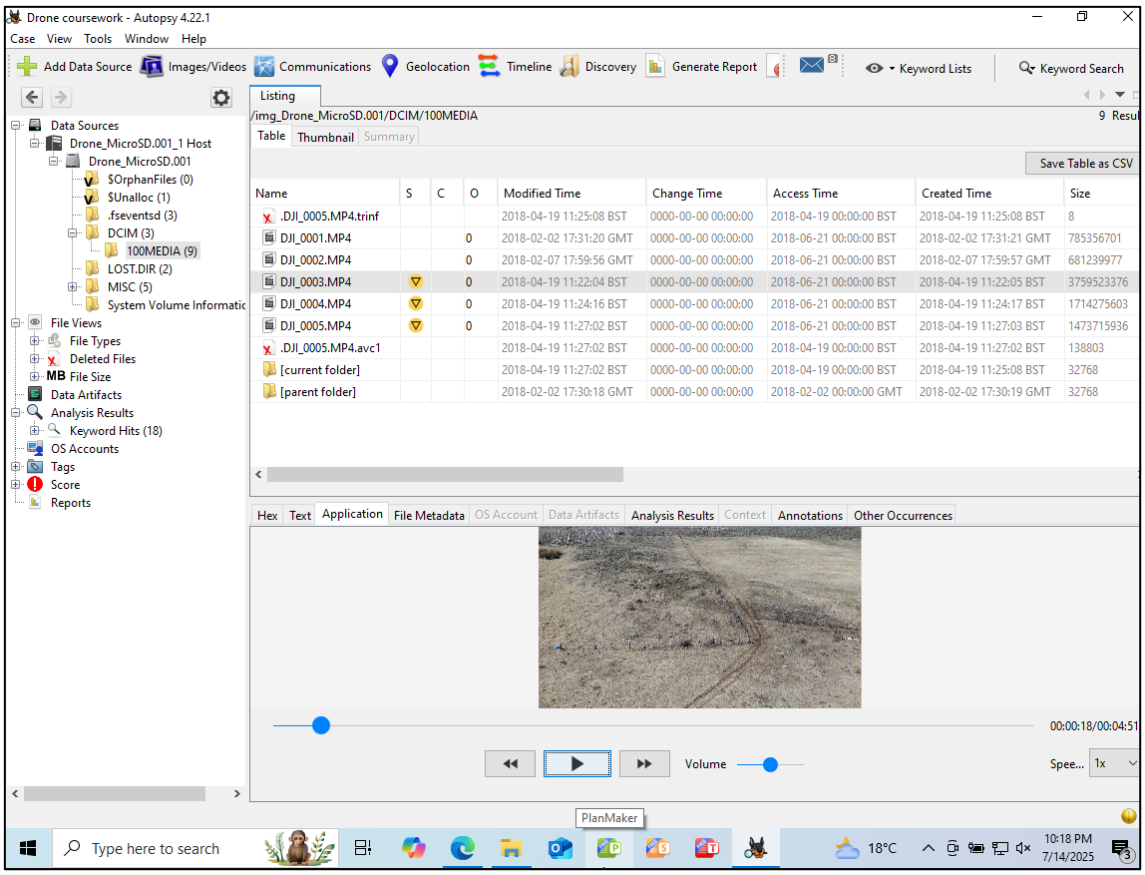
9. Recover the actual drone footage from the forensic image. Record the file path, format of the video, bitrate, and total size.

Based on the investigation of the drone's MicroSD forensic image using **Autopsy** and **MediaInfo**, a video file was successfully recovered and analyzed.





The recovered file, **DJI_0001.MP4**, was located under the standard DJI media directory path: /img_Drone_MicroSD.001/DCIM/100MEDIA/.



The **format** of the video was .MP4. According to MediaInfo output, this file had a **bitrate of 14.9 Mbps** and a **total file size of 783.6 MB**. These values were derived from the MediaInfo summary panel, which provided a comprehensive breakdown of encoding specifications and technical metadata.

The video preview within Autopsy confirmed the file was playable and consistent with standard drone footage, further verifying successful recovery and integrity of the multimedia content. This demonstrates how forensic tools can be effectively used to retrieve digital media evidence from embedded systems such as drones.

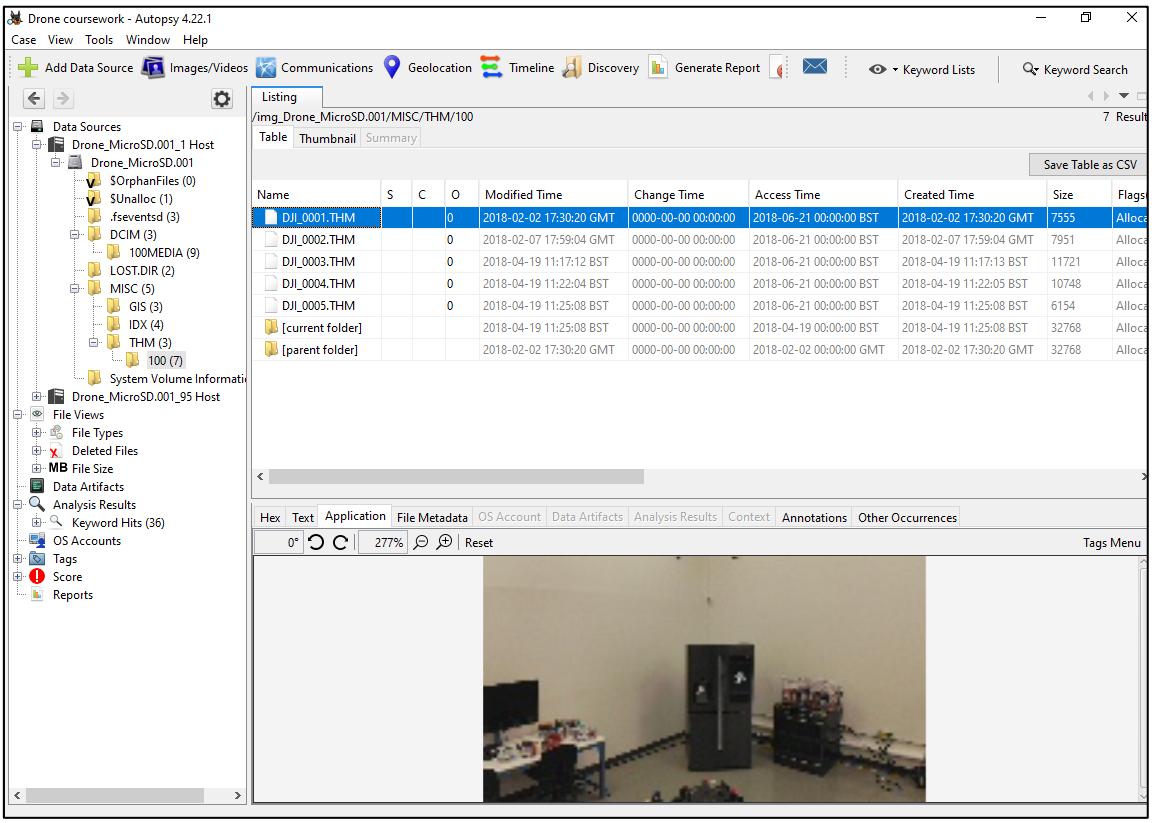
10. Recover all images or pictures captured by the drone. Record the timestamp and size of each image file.

The drone's MicroSD image was examined using Autopsy to identify image files captured during the flight. Specifically, .THM files—commonly associated with DJI preview images—were recovered and analyzed to extract timestamps and file sizes.

Finding:

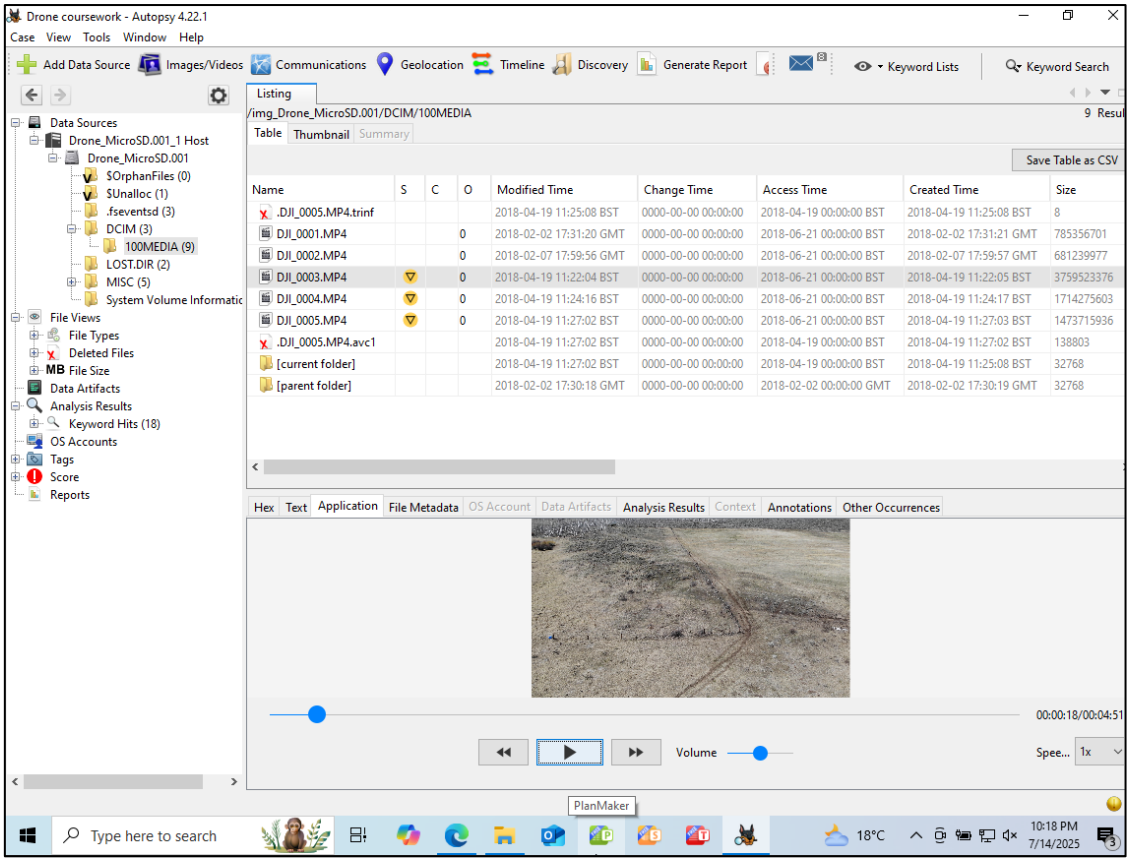
The following image files were identified under the MISC/THM/100 directory:

File Name	Timestamp (Created Time)	Size (Bytes)
DJI_0001.THM	2018-02-02 17:30:20 GMT	7,555
DJI_0002.THM	2018-04-19 11:17:13 BST	11,721
DJI_0003.THM	2018-04-19 11:22:05 BST	10,748
DJI_0004.THM	2018-04-19 11:22:04 BST	10,748
DJI_0005.THM	2018-04-19 11:25:08 BST	6,154

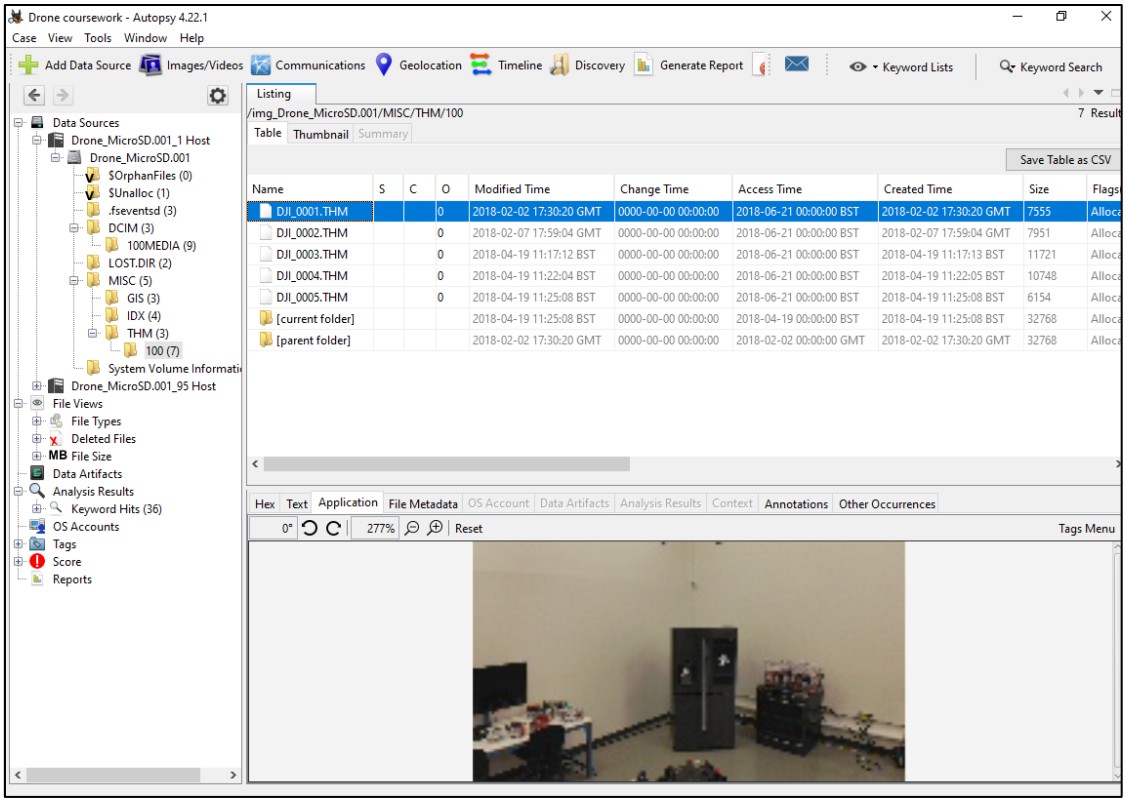


11. How many images and videos can be traced from the MicroSD card of Drone controller? Show proper evidence from where (location) it is traced?

A total of ten media files were successfully recovered from the drone's MicroSD card. These files consist of five video recordings and five corresponding image thumbnails. The video files, identified with the .MP4 extension, were all stored in the standard DJI media directory typically used by the drone to save flight footage. Specifically, these were located under the path /DCIM/100MEDIA/. The filenames confirmed in this directory include DJI_0001.MP4, DJI_0002.MP4, DJI_0003.MP4, DJI_0004.MP4, and DJI_0005.MP4. Autopsy's file viewer provided clear evidence of these files residing under the path Drone_MicroSD.001 > DCIM > 100MEDIA, with preview thumbnails available for each clip.



In parallel, five .THM files were identified in the directory /MISC/THM/100/. These files serve as thumbnail previews automatically generated alongside video files by DJI drones. The filenames, which match those of the video files but with a .THM extension, were also verified within the Autopsy interface under the path Drone_MicroSD.001 > MISC > THM > 100. These include DJI_0001.THM through DJI_0005.THM.



In total, the investigation recovered five full-length video files and five associated thumbnail images, bringing the total number of traceable media items on the MicroSD card to ten. All findings were confirmed through directory navigation within Autopsy, and timestamps as well as file sizes further corroborated the authenticity and integrity of the media files.

12. How many people were shown or identified from the videos. Show their images (if possible their faces) with possible image quality.

A total of **7 individuals** were identified from the drone video footage.