ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
Τμήμα Πληροφορικής

Εργασία Μαθήματος ***Digital Forensics***

Αρ. Άσκησης – Τίτλος Ασκησης	***Final Exam Assignment***
Όνομα φοιτητή – Αρ. Μητρώου	Ανδριανόπουλος Βασίλειος - ΜΠΚΕΔ2303
Ημερομηνία παράδοσης	06-05-2024

Εκφώνηση της άσκησης

Analyze the digital evidence and answer the following questions. Proper explanation of the analysis and screenshots must be included. Always include timestamps (UTC), when applicable.

1. What file is of crucial importance when we want to acquire volatile evidence from a Windows pc which is in hibernation state and why? How would you convert this file into a memory dump with volatility framework?

2. Is the integrity of the evidence preserved? If you were responsible for acquiring the evidence, how would you ensure that the evidence is admissible in a court of law?

3. If you had to examine evidence (both non-volatile and volatile) from a vmware VM, which files would you need?

4. From the forensic image evidence, what is the timezone setting?

5. What is the computer name?

6. What are the partitions of the image? Which is the partition which contains the operating system files?

7. What is the installed OS and when was it installed? (OS type, version info, install date)

8. List all accounts in OS, except the system accounts. The suspect is the last user to logon into PC. Who is the suspect user?

9. When was the last recorded shutdown date/time (in UTC)?

10. Provide the information of network interface(s) with a DHCP assigned IP address.

11. List all applications installed after 23/3/2015.

12. Review the event logs and list all suspect user logon and logoff events after 22/03/2015.

13. List all files that were opened with a browser. Include the user, the path, the source file and the timestamp.

14. List all suspect user keywords that were used at the search bar in Windows Explorer.

15. What is the IP address of a shared network drive accessed by the suspect user? List all directories that were traversed by the suspect in that network drive.

16. List all recent files that were opened by the suspect in the shared network drive.

17. Which deleted executables last accessed on 25/03/2015 show that the suspect user tried to erase data from the system?

18. Were these executables executed on the system? How many times? Provide all available evidence.

19. Check the suspect users' autoruns. What suspicious executable can you find? What did he intend to do?

20. What e-mail account did the suspect user use? How did the suspect user exfiltrate information to “spy”?.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

1 Question 1

What file is of crucial importance when we want to acquire volatile evidence from a Windows pc which is in hibernation state and why? How would you convert this file into a memory dump with volatility framework?

1.1 Answer

When acquiring volatile evidence from a Windows PC that is in a hibernation state, one of the crucial files is the hiberfil.sys file. This file is of utmost importance because it contains the contents of the system's memory (RAM) at the time the system was hibernated. Therefore, it can provide valuable insights into the state of the system, including running processes, open files, network connections, and other volatile data.

To convert the hiberfil.sys file into a memory dump using the Volatility framework, you would follow these steps:

Acquire the hiberfil.sys file: Locate and extract the hiberfil.sys file from the Windows system's file system. This file is typically located in the root directory of the system drive (e.g., C:\hiberfil.sys).

Use Volatility to analyze the hiberfil.sys file: Volatility is a powerful open-source framework for analyzing volatile memory dumps. You would use Volatility to analyze the hiberfil.sys file and extract the memory dump.

Identify the profile: Before analyzing the hiberfil.sys file with Volatility, you need to determine the profile of the Windows system from which the hibernation file was obtained. This information is crucial for Volatility to interpret the memory dump correctly.

Convert the hiberfil.sys file: Once you have identified the profile, you can use the volatility command-line tool to convert the hiberfil.sys file into a memory dump. The command typically looks like this:

volatility -f hiberfil.sys --profile=PROFILE_NAME imagecopy -O output.raw

Replace hiberfil.sys with the path to your hiberfil.sys file, PROFILE_NAME with the profile of the Windows system, and output.raw with the desired name for the output memory dump file.

Analyze the memory dump: Once you have converted the hiberfil.sys file into a memory dump, you can analyze it further using Volatility or other forensic tools to extract valuable information such as running processes, network connections, registry keys, and more.

By converting the hiberfil.sys file into a memory dump, you can effectively analyze the volatile memory of a Windows system even when it is in a hibernation state, providing valuable insights for digital forensics investigations.

2 Question 2

Is the integrity of the evidence preserved? If you were responsible for acquiring the evidence, how would you ensure that the evidence is admissible in a court of law?

2.1 Answer

Preserving the integrity of evidence is paramount in digital forensics, especially when the evidence may be presented in a court of law. Here's how I would ensure the integrity of the evidence and make it admissible:

1. **Chain of Custody**

   Establish and maintain a clear chain of custody for the evidence from the moment it is acquired until it is presented in court. Document every step of the process, including who handled the evidence, when, and for what purpose.

2. **Forensic Imaging**

   Use forensic imaging tools and techniques to create a bitwise copy of the original evidence. This ensures that the original evidence remains intact and unaltered during the investigation process.

3. **Write-Blocking**

   Utilize write-blocking hardware or software to prevent any modifications to the original evidence during the acquisition process. This ensures that the evidence remains in its original state and cannot be tampered with.

4. **Documentation**

   Document the acquisition process thoroughly, including the tools and techniques used, any changes made to the system during acquisition, and any observations or anomalies encountered.

5. **Checksums and Hashing**

   Calculate checksums or cryptographic hashes of the acquired evidence before and after acquisition. This allows for verification of the integrity of the evidence and detection of any alterations.

6. **Validation and Verification**

   Validate the integrity of the acquired evidence through independent verification methods, such as comparing hashes or conducting integrity checks with trusted tools.

7. **Expert Testimony**

   Prepare expert testimony to explain the acquisition process, the steps taken to preserve the integrity of the evidence, and the validity of the findings. This helps establish the credibility of the evidence in court.

8. **Compliance with Standards**

   Ensure that the acquisition process complies with industry standards and best practices, as well as any legal requirements or guidelines applicable in the jurisdiction where the evidence may be presented.

3 Question 3

If you had to examine evidence (both non-volatile and volatile) from a vmware VM, which files would you need?

3.1 Answer

When examining evidence from a VMware virtual machine (VM), you would typically need both non-volatile and volatile data to conduct a comprehensive forensic analysis. Here's a breakdown of the types of files you would need:

Non-Volatile Data

1. Virtual Disk File (VMDK): This file contains the virtual hard disk of the VM, including the operating system, applications, and user data. It's crucial for extracting file system artifacts, registry hives, logs, and other persistent data.
2. Snapshot Files (if applicable): If snapshots of the VM were taken, you would need the snapshot files to analyze the state of the VM at different points in time. These files capture changes made to the VM's disk over time and can provide valuable insights into system activity and configuration changes.
3. VM Configuration File (VMX): The VMX file contains the configuration settings of the VM, including hardware specifications, virtual device configurations, and other settings. It can help reconstruct the VM environment and ensure accurate analysis.
4. Log Files: VMware produces various log files that record VM events, errors, and other activities. Analyzing these log files can provide context and assist in understanding the behavior of the VM.

Volatile Data

1. Memory Dump: Acquiring a memory dump (also known as a RAM image) of the running VM is essential for capturing volatile data such as running processes, network connections, open files, and system state. Analyzing the memory dump can provide real-time insights into the VM's activity at the time of acquisition.
2. Network Traffic Capture (if applicable): If the VM was connected to a network, capturing network traffic can help identify communication patterns, malicious activities, and interactions with external systems.
3. Registry and Process Information: While technically non-volatile, extracting registry hives and process information from the VM's memory dump can provide insights into system configuration, user activity, and running processes.

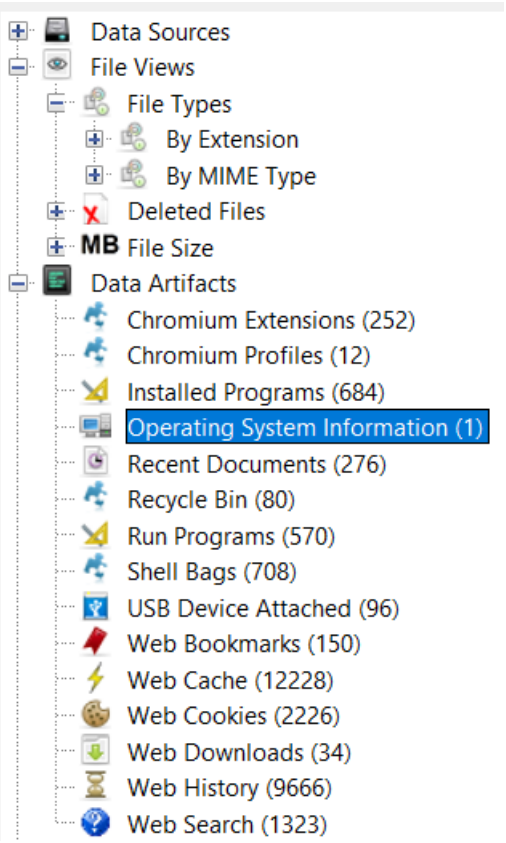
By collecting both non-volatile and volatile data from the VMware VM, forensic examiners can conduct a thorough analysis to reconstruct events, identify artifacts, and uncover evidence relevant to the investigation.

4 Question 4

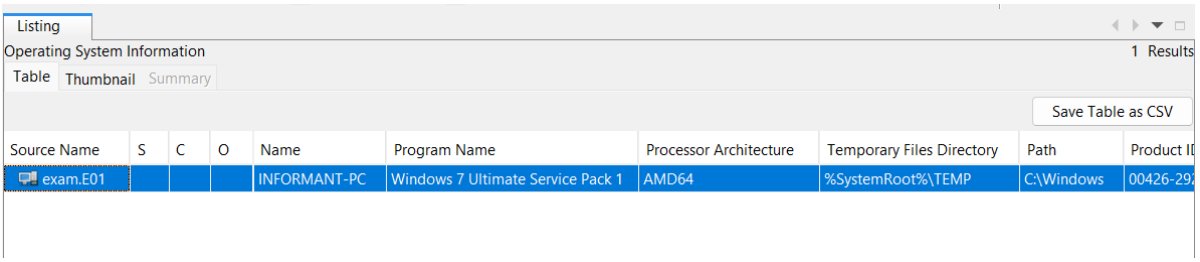
From the forensic image evidence, what is the timezone setting?

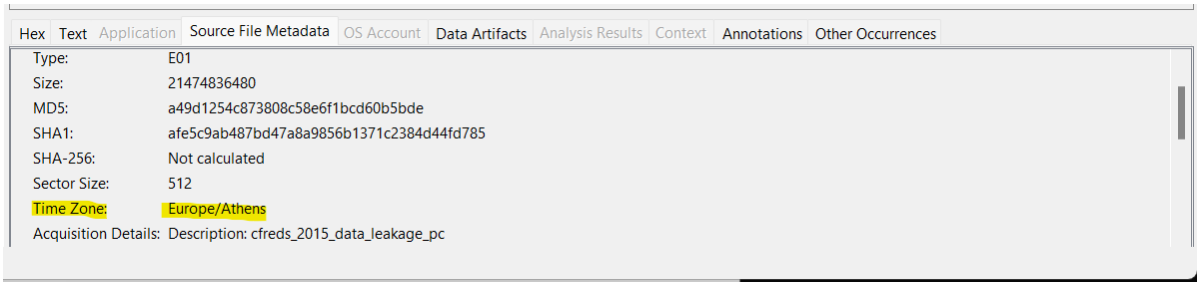
4.1 Answer

From the Operating System Information section on the Data Artifacts tab we can find the time zone setting first selecting the source name of the operating system and then viewing the file metadata.



Εικόνα 1. Παράδειγμα εικόνας με αριθμημένη λεζάντα





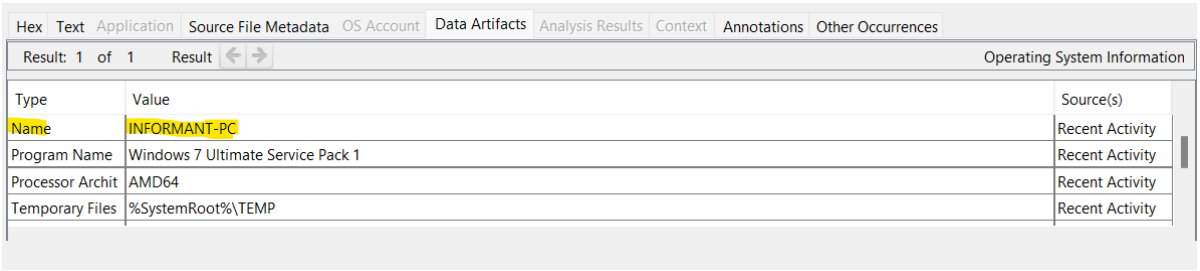
So the awsner is ***Europe/Athens***

5 Question 5

What is the computer name?

5.1 Answer

From the same window as before we can go to the Data Artifacts tab and view the computer name.



So the answer is **INFORMANT-PC**

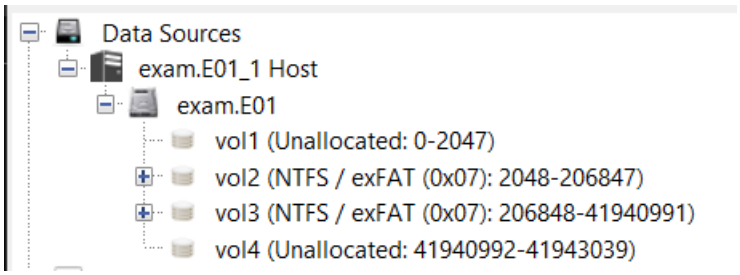
6 Question 6

What are the partitions of the image? Which is the partition which contains the operating system files?

6.1 Answer

From the Operating System Information section on the Data Artifacts tab we can find the time zone setting first selecting the source name of the operating system and then viewing the file metadata.

From the Data Sources section under the exam.E01_1 Host on the exam.01 section are located 4 partitions.



How do we know on which partition are located the operation system files?

To identify which partition contains the operating system files, you can look for specific clues:

Volume Label and Size

Sometimes, the volume label (like “Windows,” “System Reserved”) and the size of the partition can give us a clue. The OS partition is typically larger than others reserved for system recovery or other utilities.

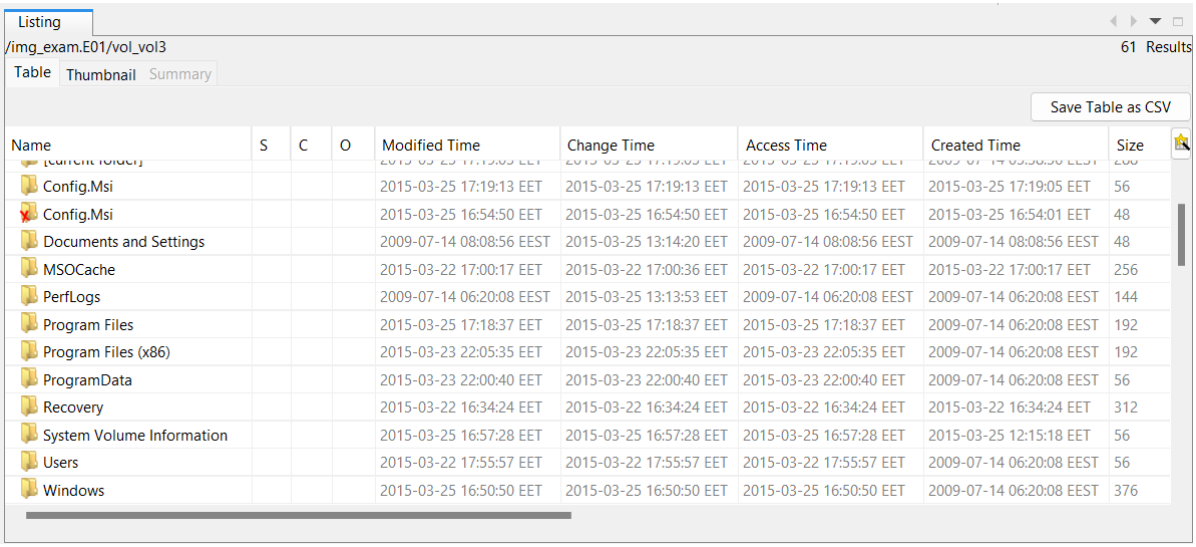
File System Type

Partitions with file systems like NTFS for Windows, or EXT4 for Linux, are more likely to contain the operating system, depending on the OS in question.

Content Inspection

We can browse the files in each partition. The presence of certain directories and files (like Windows\System32) can indicate an operating system partition.

Looking on the partition's extensions we will see that vol3 is NTFS and checking the Listing section we see all the Windows File Systems.



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
Config.Msi				2015-03-25 17:19:13 EET	2015-03-25 17:19:13 EET	2015-03-25 17:19:13 EET	2015-03-25 17:19:05 EET	56
Config.Msi				2015-03-25 16:54:50 EET	2015-03-25 16:54:50 EET	2015-03-25 16:54:50 EET	2015-03-25 16:54:01 EET	48
Documents and Settings				2009-07-14 08:08:56 EEST	2015-03-25 13:14:20 EET	2009-07-14 08:08:56 EEST	2009-07-14 08:08:56 EEST	48
MSOCache				2015-03-22 17:00:17 EET	2015-03-22 17:00:36 EET	2015-03-22 17:00:17 EET	2015-03-22 17:00:17 EET	256
PerfLogs				2009-07-14 06:20:08 EEST	2015-03-25 13:13:53 EET	2009-07-14 06:20:08 EEST	2009-07-14 06:20:08 EEST	144
Program Files				2015-03-25 17:18:37 EET	2015-03-25 17:18:37 EET	2015-03-25 17:18:37 EET	2009-07-14 06:20:08 EEST	192
Program Files (x86)				2015-03-23 22:05:35 EET	2015-03-23 22:05:35 EET	2015-03-23 22:05:35 EET	2009-07-14 06:20:08 EEST	192
ProgramData				2015-03-23 22:00:40 EET	2015-03-23 22:00:40 EET	2015-03-23 22:00:40 EET	2009-07-14 06:20:08 EEST	56
Recovery				2015-03-22 16:34:24 EET	2015-03-22 16:34:24 EET	2015-03-22 16:34:24 EET	2015-03-22 16:34:24 EET	312
System Volume Information				2015-03-25 16:57:28 EET	2015-03-25 16:57:28 EET	2015-03-25 16:57:28 EET	2015-03-25 12:15:18 EET	56
Users				2015-03-22 17:55:57 EET	2015-03-22 17:55:57 EET	2015-03-22 17:55:57 EET	2009-07-14 06:20:08 EEST	56
Windows				2015-03-25 16:50:50 EET	2015-03-25 16:50:50 EET	2015-03-25 16:50:50 EET	2009-07-14 06:20:08 EEST	376

So the answer is vol3 partition.

7 Question 7

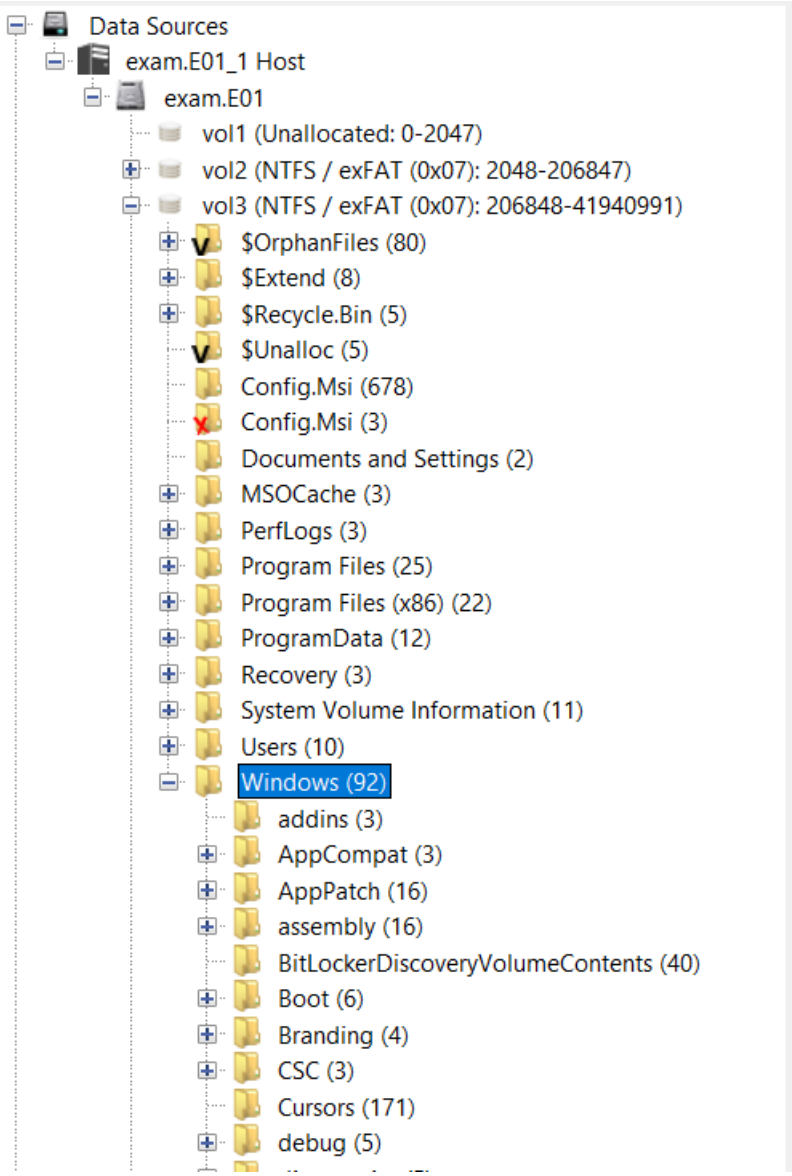
What is the installed OS and when was it installed? (OS type, version info, install date)

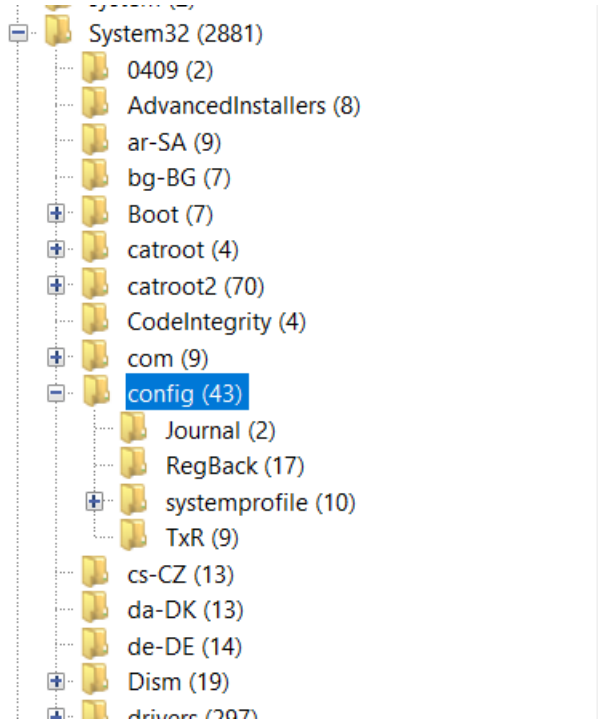
7.1 Answer

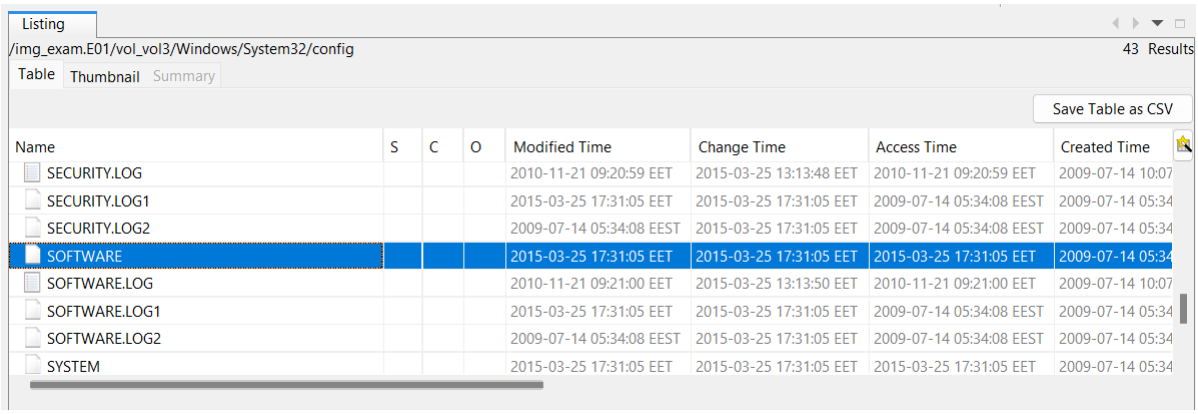
The answer is behind the Windows Registry. (Firstly we checked under the Operating System Information section but we only found the OS version and not the installation date)

Where can we locate the Windows Registry of the Image?

We go to the operating system files (vol3) and under Windows/System32/config path we find the key file like 'SOFTWARE', 'SYSTEM' etc.

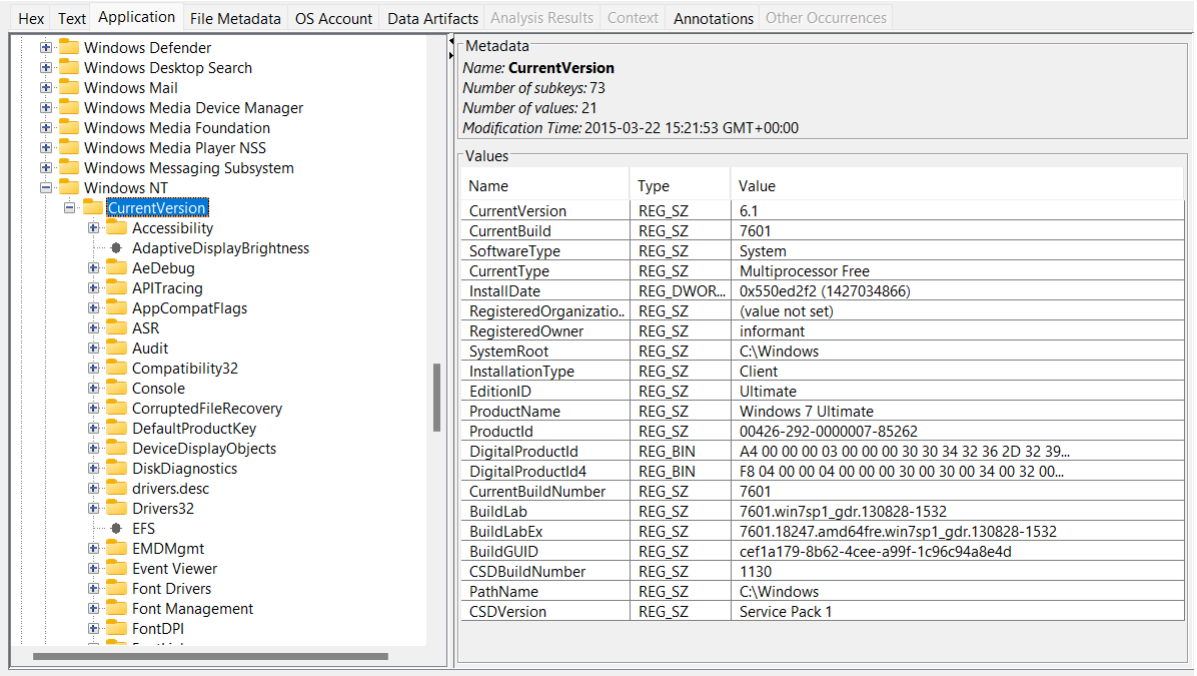






We click on ‘SOFTWARE’ and we navigate to Microsoft/Windows NT/CurrentVersion

And then from there we see all the necessary information that we want



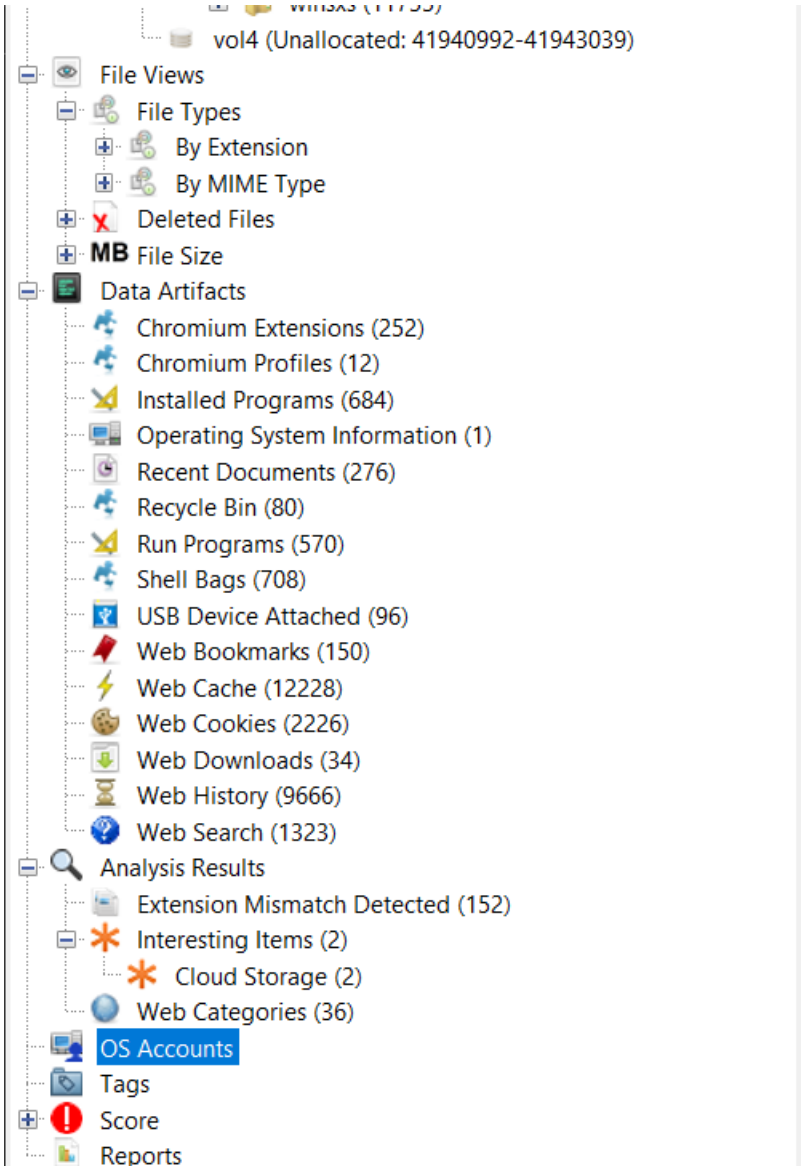
We see that the installed OS is Windows 7 Ultimate, installed on 2015-03-22 15:21:06 (under InstallDate row we see 1427034866 that are in seconds).

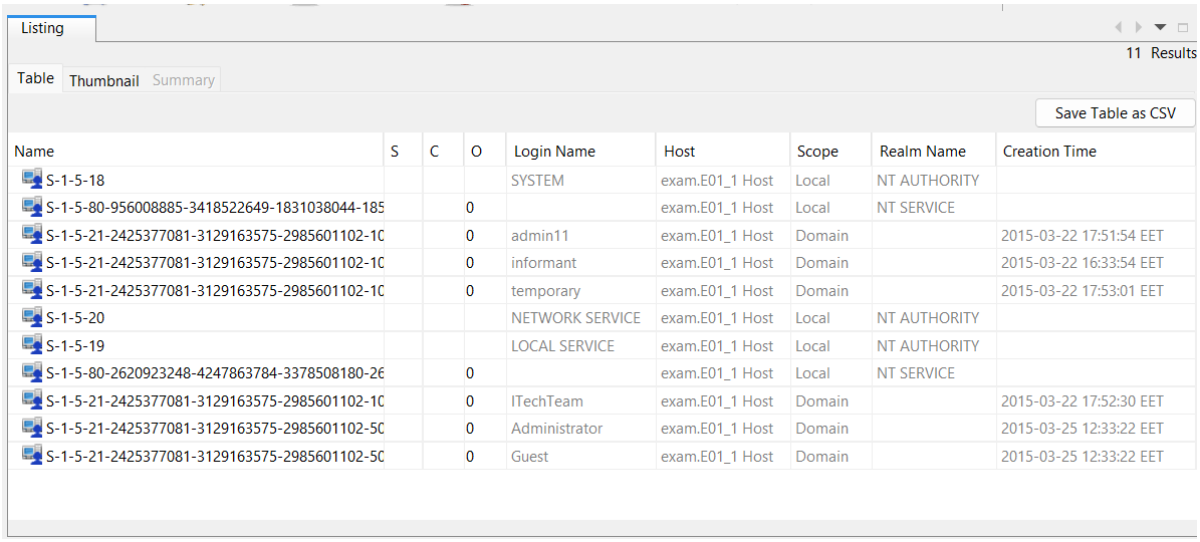
8 Question 7

List all accounts in OS, except the system accounts. The suspect is the last user to logon into PC. Who is the suspect user?

8.1 Answer

Firstly, we navigate to OS Account Section to list all the registered users of the system.


vol4 (Unallocated: 41940992-41943039)
File Views
File Types
By Extension
By MIME Type
Deleted Files
File Size
Data Artifacts
Chromium Extensions (252)
Chromium Profiles (12)
Installed Programs (684)
Operating System Information (1)
Recent Documents (276)
Recycle Bin (80)
Run Programs (570)
Shell Bags (708)
USB Device Attached (96)
Web Bookmarks (150)
Web Cache (12228)
Web Cookies (2226)
Web Downloads (34)
Web History (9666)
Web Search (1323)
Analysis Results
Extension Mismatch Detected (152)
Interesting Items (2)
Cloud Storage (2)
Web Categories (36)
OS Accounts
Tags
Score
Reports



Listing

11 Results

Table | Thumbnail | Summary

Save Table as CSV

Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-5-18				SYSTEM	exam.E01_1 Host	Local	NT AUTHORITY	
S-1-5-80-956008885-3418522649-1831038044-185			0		exam.E01_1 Host	Local	NT SERVICE	
S-1-5-21-2425377081-3129163575-2985601102-1C			0	admin11	exam.E01_1 Host	Domain		2015-03-22 17:51:54 EET
S-1-5-21-2425377081-3129163575-2985601102-1C			0	informant	exam.E01_1 Host	Domain		2015-03-22 16:33:54 EET
S-1-5-21-2425377081-3129163575-2985601102-1C			0	temporary	exam.E01_1 Host	Domain		2015-03-22 17:53:01 EET
S-1-5-20				NETWORK SERVICE	exam.E01_1 Host	Local	NT AUTHORITY	
S-1-5-19				LOCAL SERVICE	exam.E01_1 Host	Local	NT AUTHORITY	
S-1-5-80-2620923248-4247863784-3378508180-26			0		exam.E01_1 Host	Local	NT SERVICE	
S-1-5-21-2425377081-3129163575-2985601102-1C			0	ITechTeam	exam.E01_1 Host	Domain		2015-03-22 17:52:30 EET
S-1-5-21-2425377081-3129163575-2985601102-5C			0	Administrator	exam.E01_1 Host	Domain		2015-03-25 12:33:22 EET
S-1-5-21-2425377081-3129163575-2985601102-5C			0	Guest	exam.E01_1 Host	Domain		2015-03-25 12:33:22 EET

In the list provided, the system accounts can be identified based on the well-known Security Identifiers (SIDs) and their typical associated descriptions. Here are the system accounts from the list:

S-1-5-18

Account Name: SYSTEM

Authority: NT AUTHORITY

This SID is for the System account, a service account that is used by the operating system.

S-1-5-20

Account Name: NETWORK SERVICE

Authority: NT AUTHORITY

This SID represents the Network Service account, which is used by service processes run by the system that communicate with other computers on the network.

S-1-5-19

Account Name: LOCAL SERVICE

Authority: NT AUTHORITY

This SID represents the Local Service account, which has fewer privileges on the system and presents anonymous credentials on the network.

S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464 and S-1-5-80-2620923248-4247863784-3378508180-2659151310-2535246811 (the empty ones)

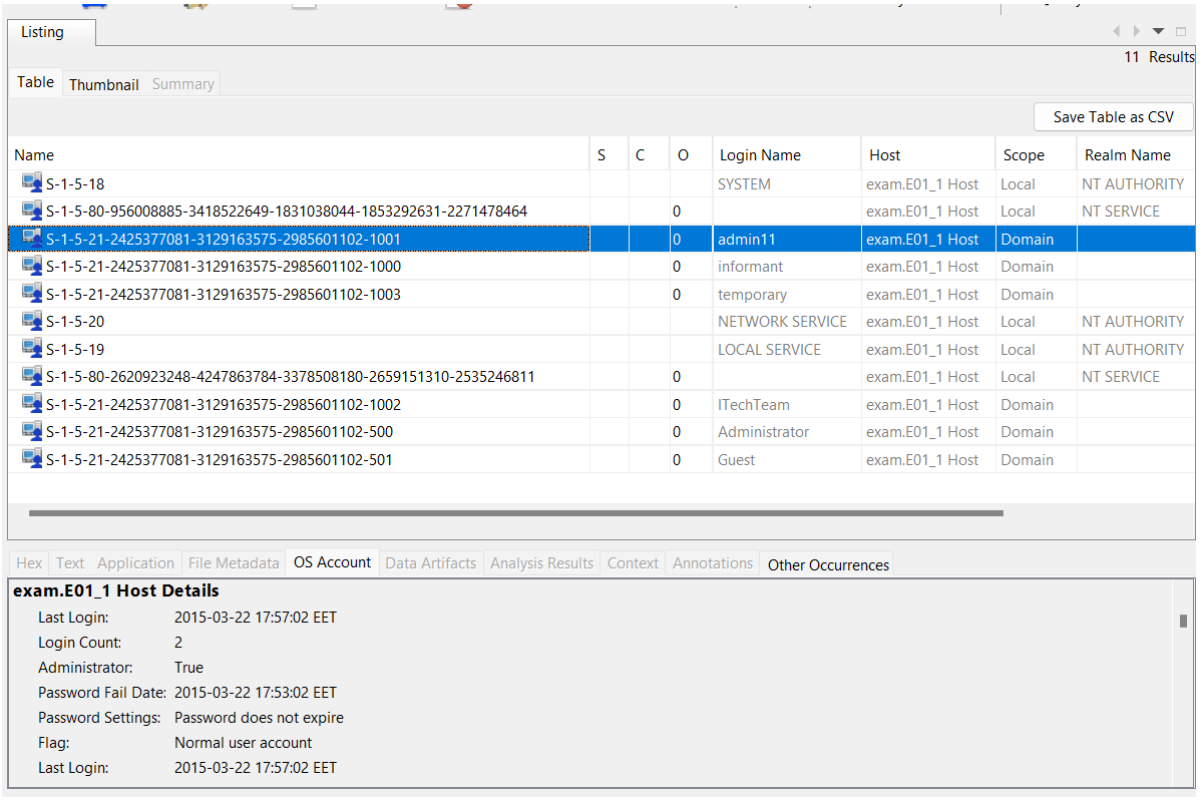
Account Type: NT SERVICE

These SIDs are part of the Service Account range (S-1-5-80). They are used by services and service applications installed on the system.

The remaining SIDs that start with S-1-5-21 typically represent user accounts in a domain or local user accounts, including:

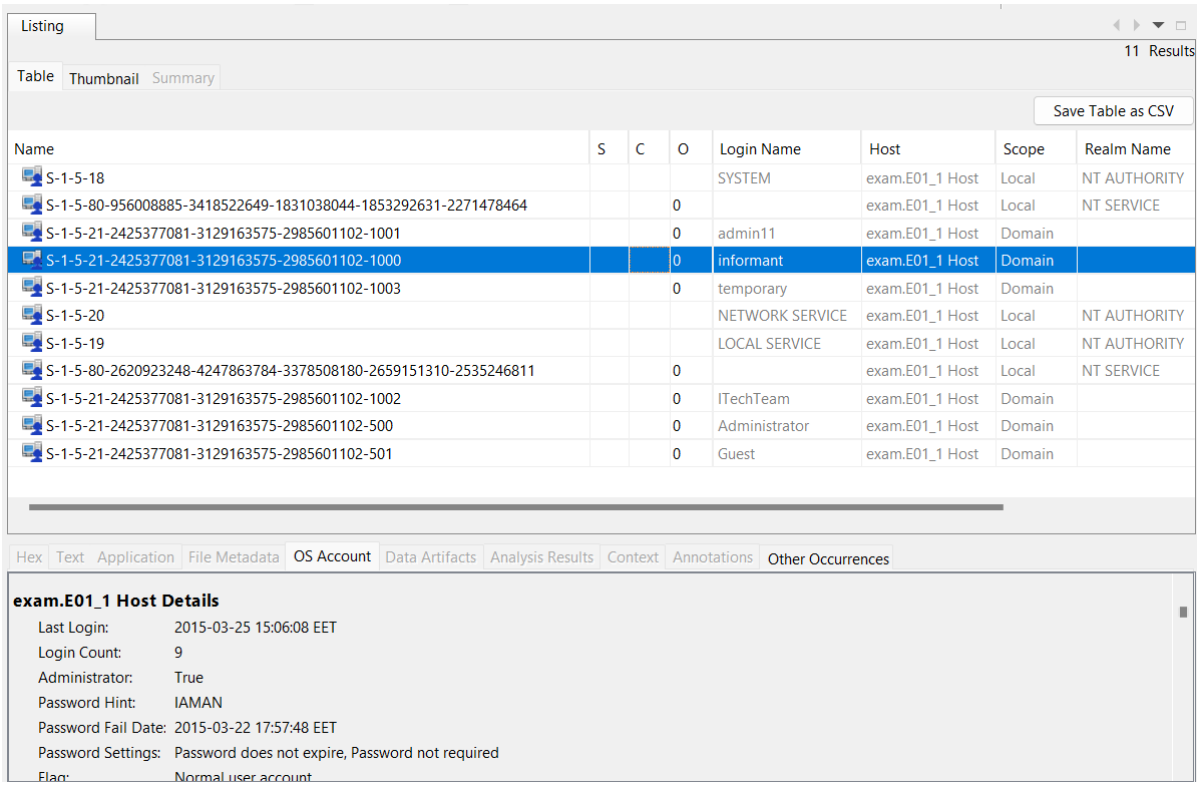
- admin11
- informant
- temporary
- ITechTeam

Based on the list of users to find the suspect (i.e., the last user to log on to the PC), we need to look at the last Login timestamps associated with each account that is located in the OS Account Tab:

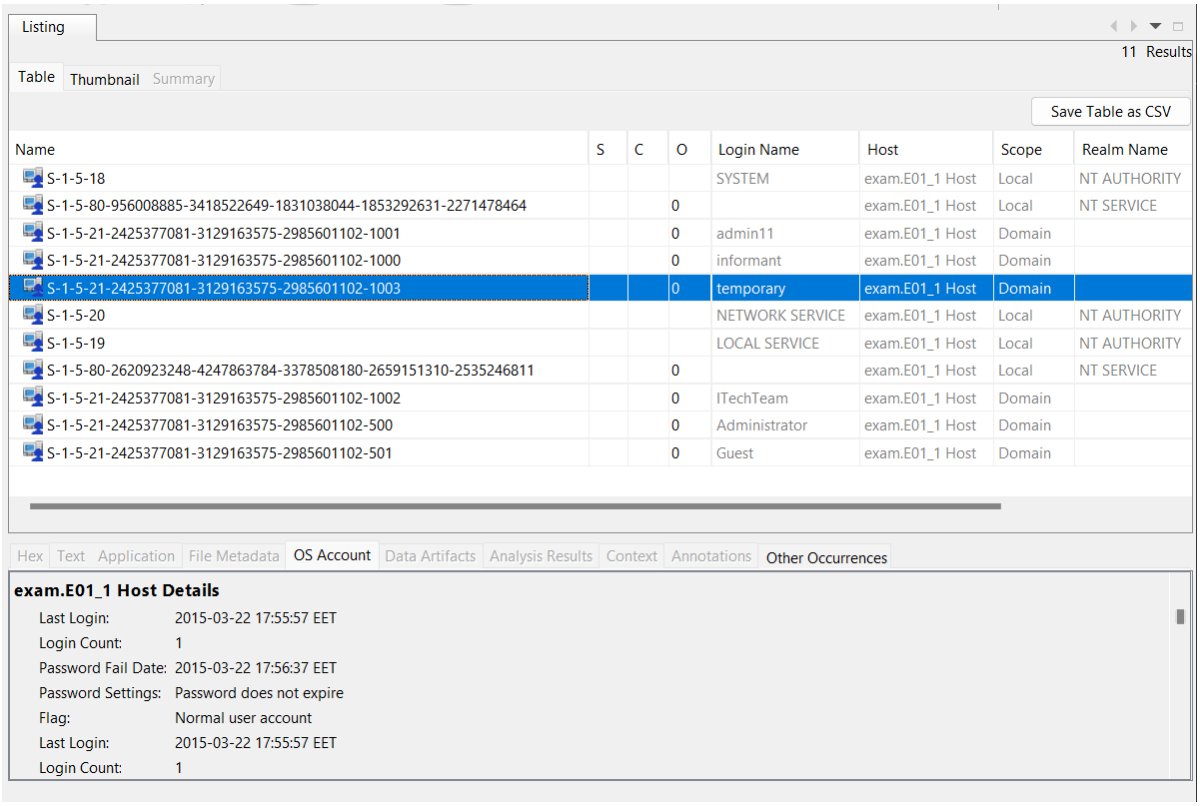


Here are the relevant entries with their logon times:

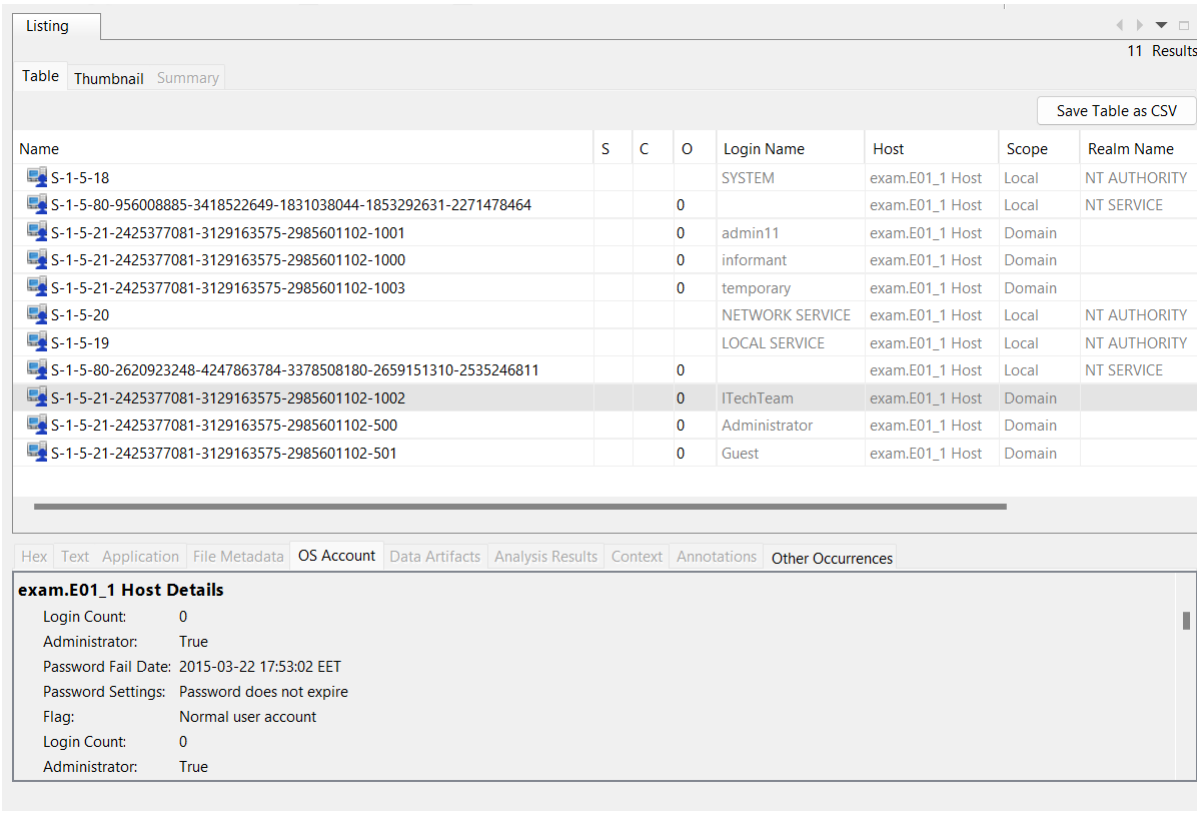
admin11: Logged on at 2015-03-22 17:57:02 EET



informant: Logged on at 2015-03-25 15:06:08 EET



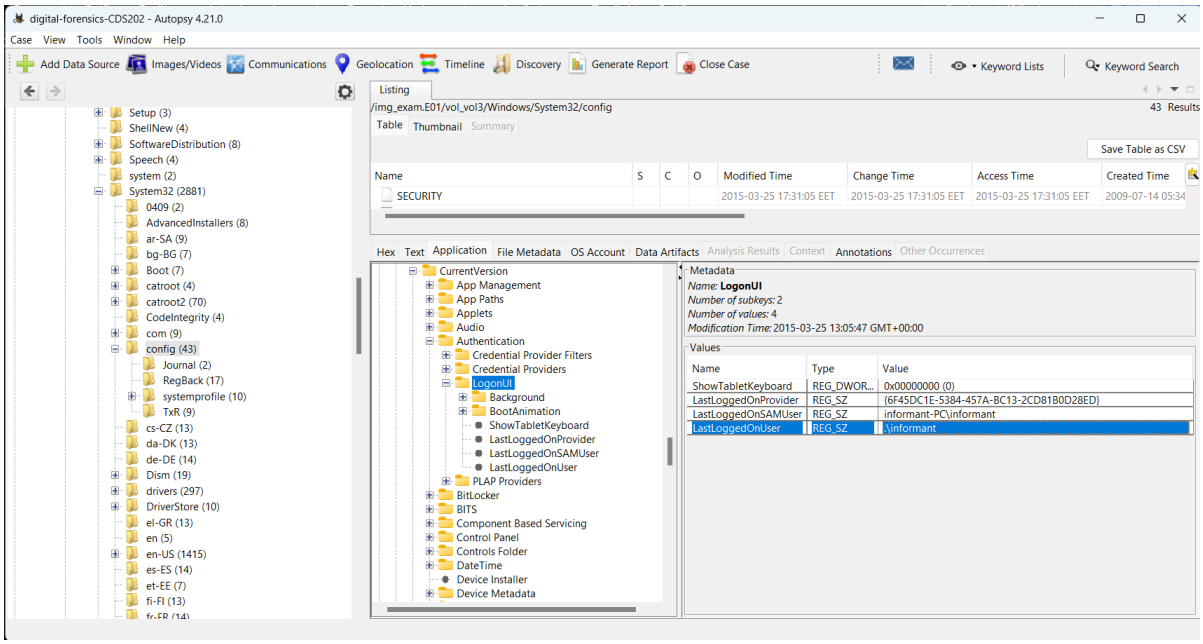
temporary: Logged on at 2015-03-22 17:55:57 EET



ITechTeam: Never logon

From the above list, the informant user have logon timestamp of 2015-03-25 15:06:08 EET, which are the most recent.

We can confirm that by looking at the register files on Windows/System32/config under the SOFTWARE key file and navigating to Microsoft/Windows/CurrentVersion/Authentication/LogonUI



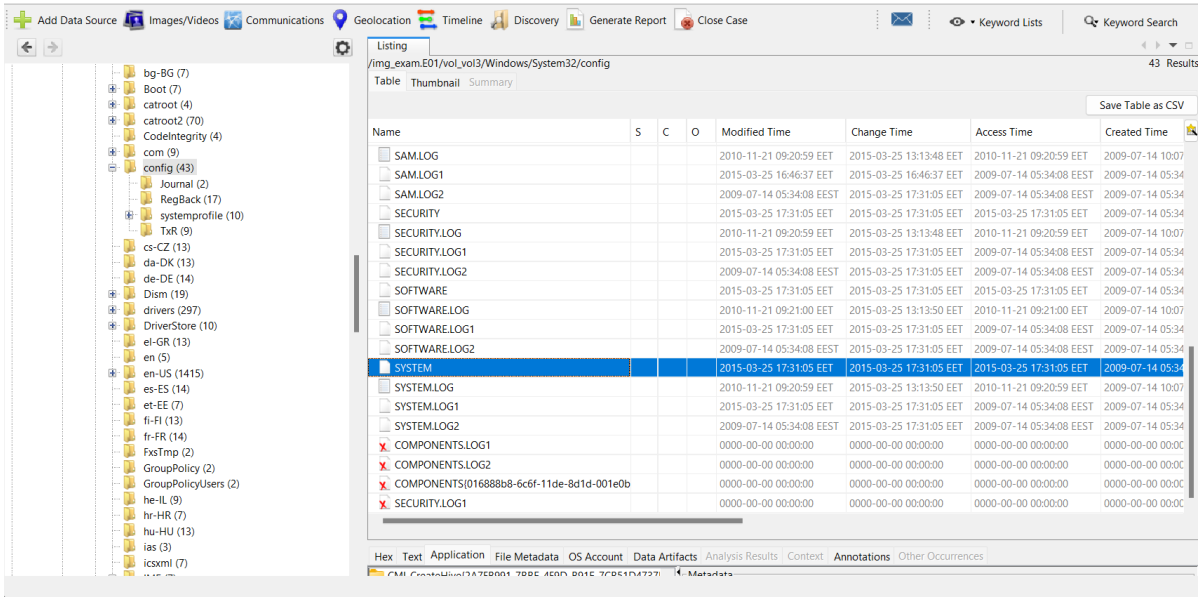
So the suspect user is informant.

9 Question 9

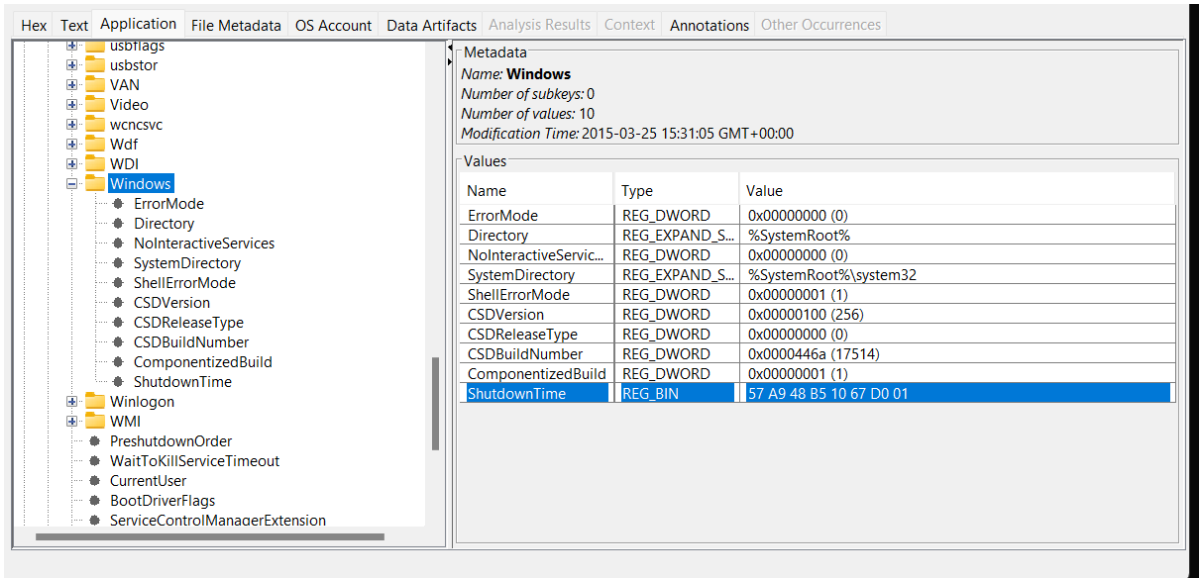
When was the last recorded shutdown date/time (in UTC)?

9.1 Answer

Firstly, we navigate to Windows/System32/config and we find the key file SYSTEM.



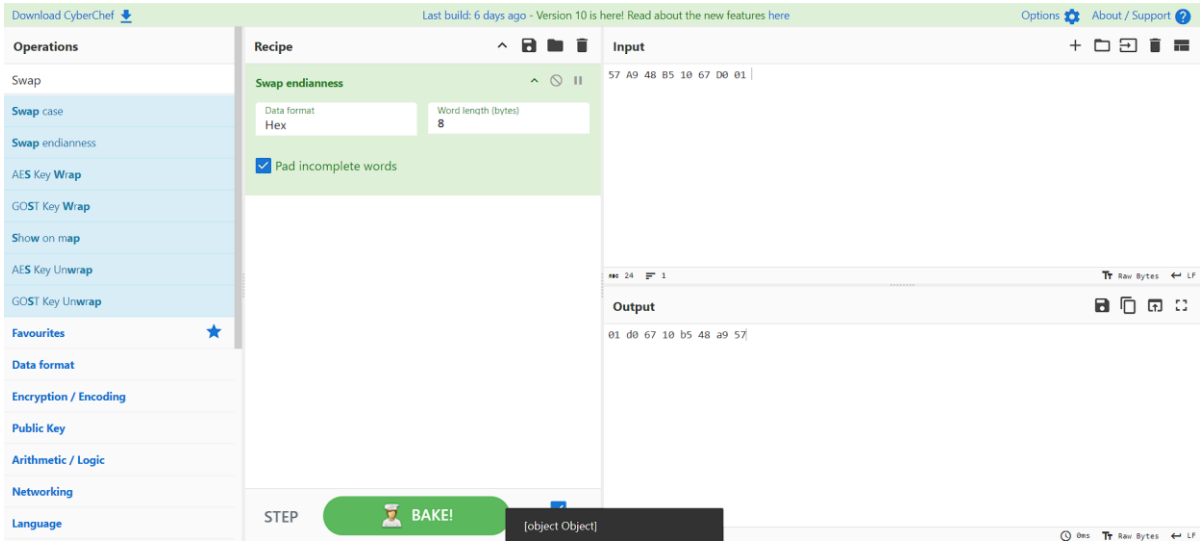
Then, we navigate from the Application tab to Controlset001/Control/Windows and we locate the ShutdownTime



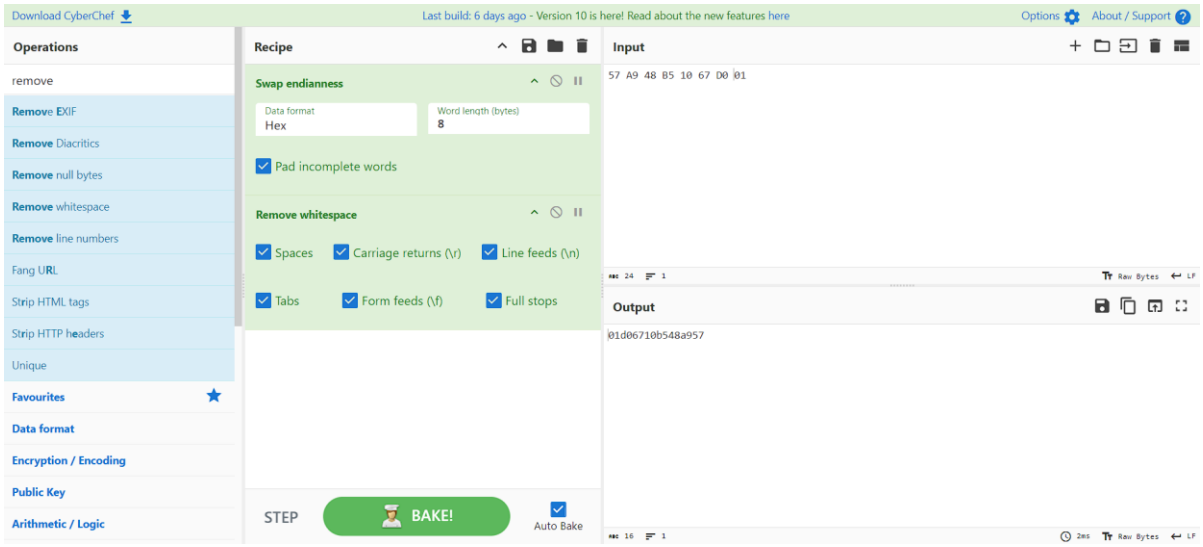
The value of the shutdowntime is ***57 A9 48 B5 10 67 D0 01*** wich is not in a human redable format.

We go to Cyberchef (a github project) and create our recipe to decode this value.

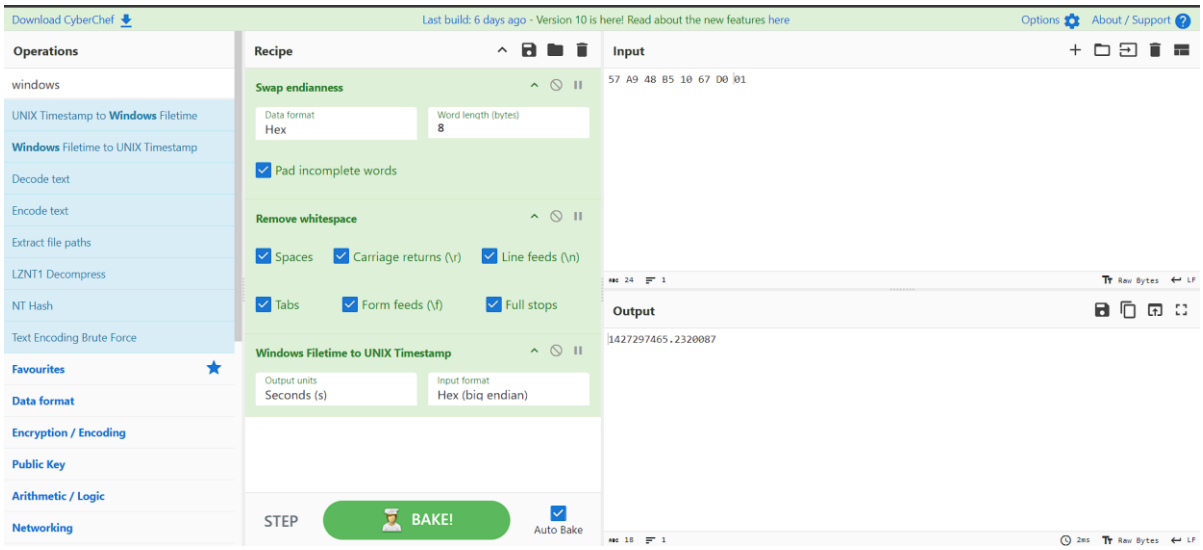
We use **Swap Endianness recipe** with 8 byte world length



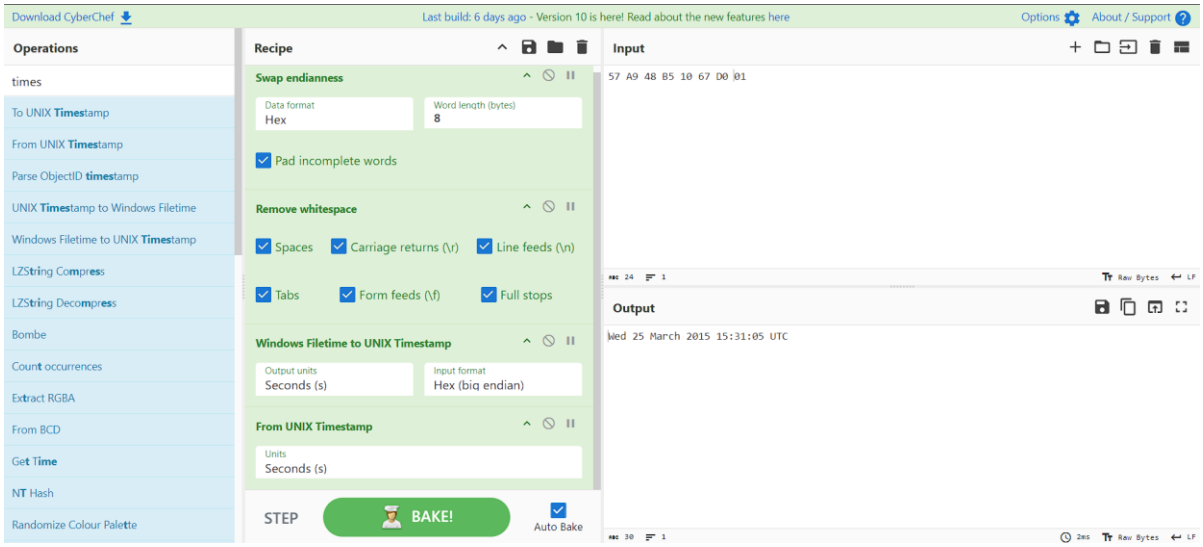
Then we add **Remove Whitespace module** to our recipe.



Then we add **Windows Filetime to UNIX Timestamp** to convert the filetime to UNIX Timestamp (with hex input)



And finally we convert this to date using **From UNIX Timestamp**



So the anwser is that the last Shutdown Time was 25/03/2015 15:31:05 UTC.

10 Question 10

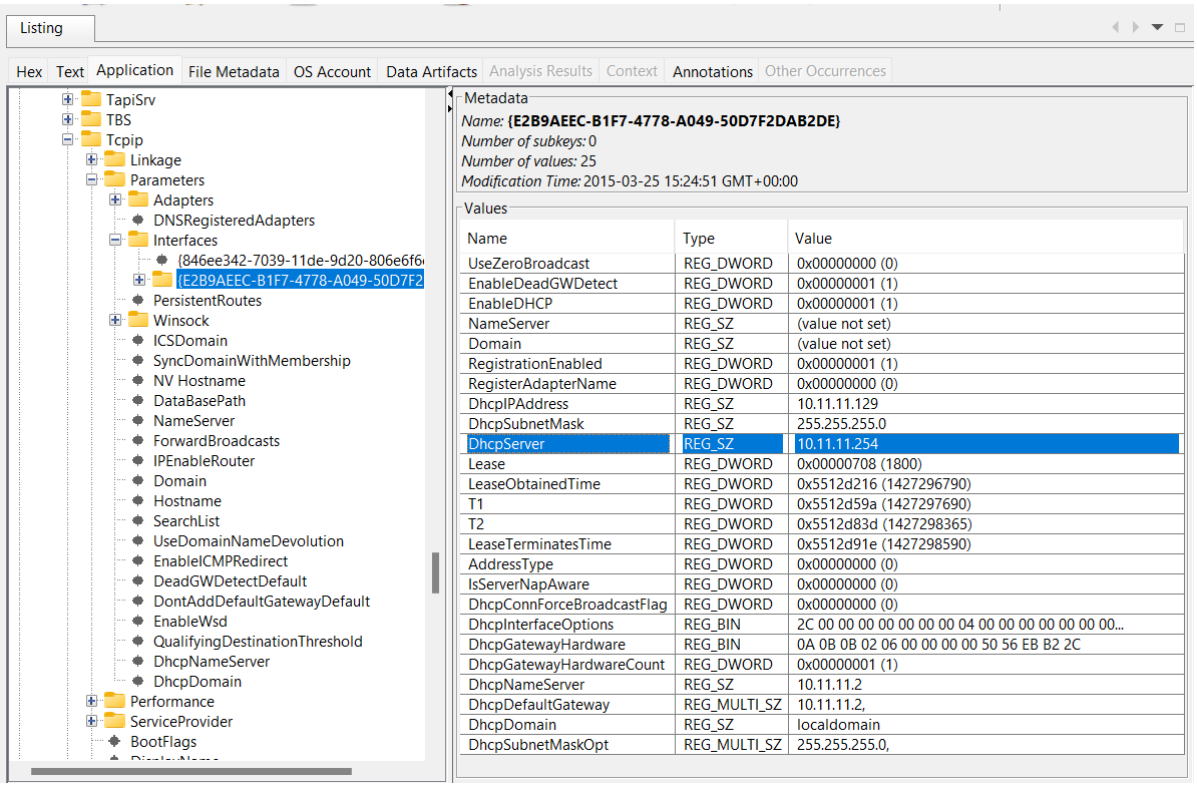
Provide the information of network interface(s) with a DHCP assigned IP address.

10.1 Answer

Again we navigate to Windows/System32/config and we find the key file SYSTEM.

Then, we navigate to ControlSet001/services/Tcpip/parameters/interfaces and we check each interface folder.

Here, we have only one



On EnableDHCP we see the entry is set to 0x00000001 (1), indicating that DHCP is enabled on this interface.

On DhcpIPAddress we see that the DHCP assigned IP address for this interface is 10.11.11.129.

On DhcpSubnetMask the subnet mask assigned by DHCP is 255.255.255.0.

On DhcpServer the DHCP server that assigned the IP address is 10.11.11.254.

On DhcpNameServer the DNS server provided by DHCP is 10.11.11.2.

On DhcpDefaultGateway the default gateway provided by DHCP is 10.11.11.2.

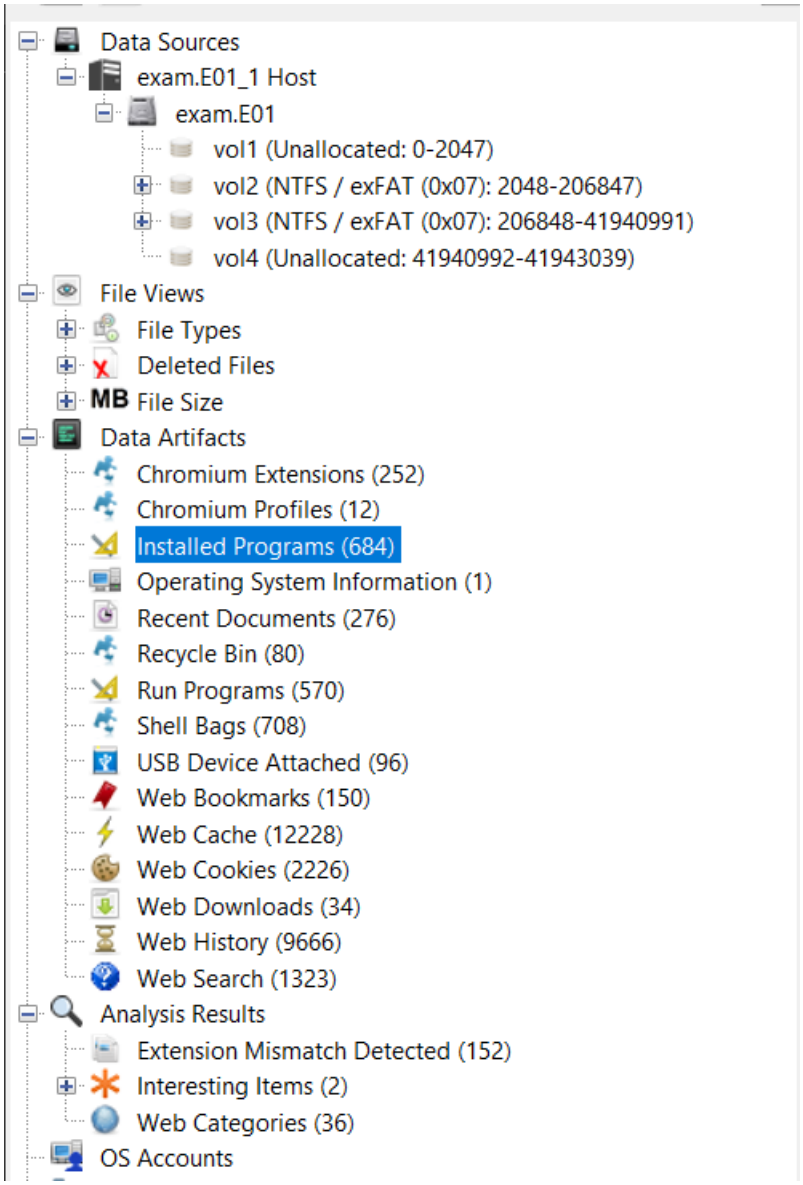
On DhcpDomain the domain name provided by DHCP is localdomain.

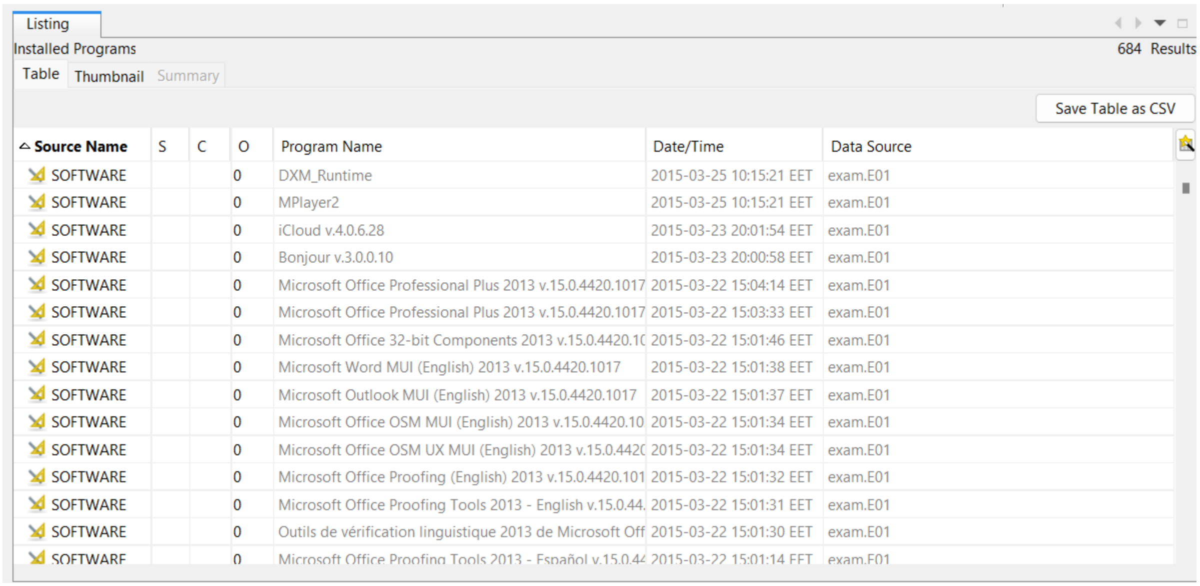
11 Question 11

List all applications installed after 23/3/2015.

11.1 Answer

From the Installed Programs section, we can list all the installed programs.

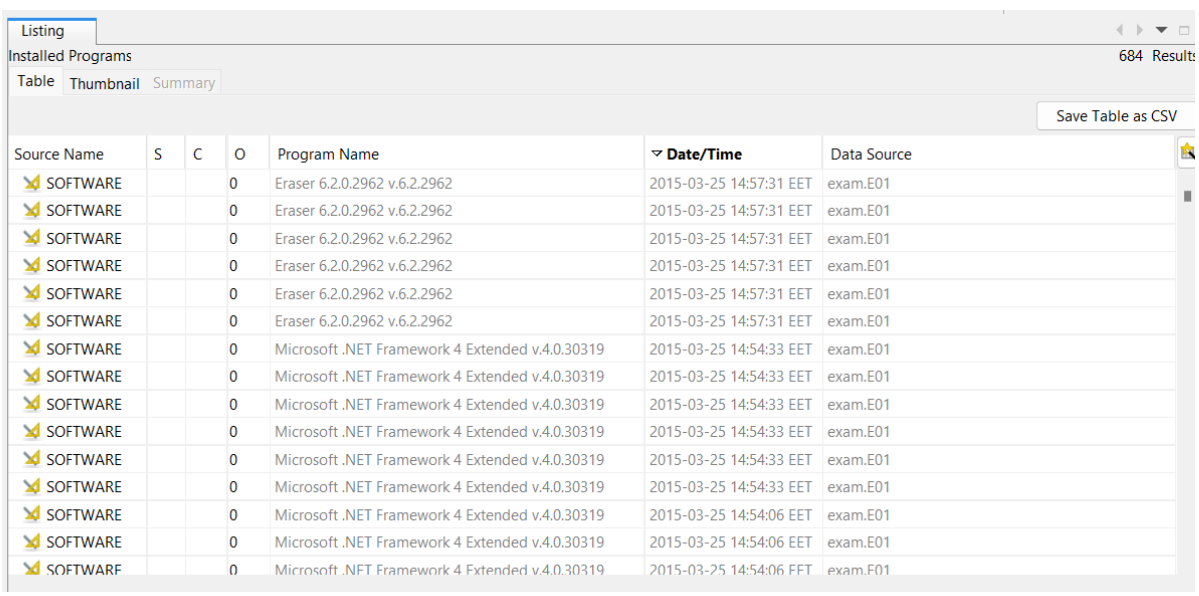

Data Sources
exam.E01_1 Host
exam.E01
vol1 (Unallocated: 0-2047)
vol2 (NTFS / exFAT (0x07): 2048-206847)
vol3 (NTFS / exFAT (0x07): 206848-41940991)
vol4 (Unallocated: 41940992-41943039)
File Views
File Types
Deleted Files
MB File Size
Data Artifacts
Chromium Extensions (252)
Chromium Profiles (12)
Installed Programs (684)
Operating System Information (1)
Recent Documents (276)
Recycle Bin (80)
Run Programs (570)
Shell Bags (708)
USB Device Attached (96)
Web Bookmarks (150)
Web Cache (12228)
Web Cookies (2226)
Web Downloads (34)
Web History (9666)
Web Search (1323)
Analysis Results
Extension Mismatch Detected (152)
Interesting Items (2)
Web Categories (36)
OS Accounts



Listing
Installed Programs — 684 Results
Table | Thumbnail | Summary
Save Table as CSV

Source Name	S	C	O	Program Name	Date/Time	Data Source
SOFTWARE			0	DXM_Runtime	2015-03-25 10:15:21 EET	exam.E01
SOFTWARE			0	MPlayer2	2015-03-25 10:15:21 EET	exam.E01
SOFTWARE			0	iCloud v.4.0.6.28	2015-03-23 20:01:54 EET	exam.E01
SOFTWARE			0	Bonjour v.3.0.0.10	2015-03-23 20:00:58 EET	exam.E01
SOFTWARE			0	Microsoft Office Professional Plus 2013 v.15.0.4420.1017	2015-03-22 15:04:14 EET	exam.E01
SOFTWARE			0	Microsoft Office Professional Plus 2013 v.15.0.4420.1017	2015-03-22 15:03:33 EET	exam.E01
SOFTWARE			0	Microsoft Office 32-bit Components 2013 v.15.0.4420.1(	2015-03-22 15:01:46 EET	exam.E01
SOFTWARE			0	Microsoft Word MUI (English) 2013 v.15.0.4420.1017	2015-03-22 15:01:38 EET	exam.E01
SOFTWARE			0	Microsoft Outlook MUI (English) 2013 v.15.0.4420.1017	2015-03-22 15:01:37 EET	exam.E01
SOFTWARE			0	Microsoft Office OSM MUI (English) 2013 v.15.0.4420.10	2015-03-22 15:01:34 EET	exam.E01
SOFTWARE			0	Microsoft Office OSM UX MUI (English) 2013 v.15.0.442(	2015-03-22 15:01:34 EET	exam.E01
SOFTWARE			0	Microsoft Office Proofing (English) 2013 v.15.0.4420.101	2015-03-22 15:01:32 EET	exam.E01
SOFTWARE			0	Microsoft Office Proofing Tools 2013 - English v.15.0.44.	2015-03-22 15:01:31 EET	exam.E01
SOFTWARE			0	Outils de vérification linguistique 2013 de Microsoft Off	2015-03-22 15:01:30 EET	exam.E01
SOFTWARE			0	Microsoft Office Proofing Tools 2013 - Español v.15.0.44	2015-03-22 15:01:14 EET	exam.E01

To find the installed programs after 23/03/2015, we click on Date/Time column option to classify the programs based on their installation date.



Listing
Installed Programs — 684 Results
Table | Thumbnail | Summary
Save Table as CSV

Source Name	S	C	O	Program Name	Date/Time	Data Source
SOFTWARE			0	Eraser 6.2.0.2962 v.6.2.2962	2015-03-25 14:57:31 EET	exam.E01
SOFTWARE			0	Eraser 6.2.0.2962 v.6.2.2962	2015-03-25 14:57:31 EET	exam.E01
SOFTWARE			0	Eraser 6.2.0.2962 v.6.2.2962	2015-03-25 14:57:31 EET	exam.E01
SOFTWARE			0	Eraser 6.2.0.2962 v.6.2.2962	2015-03-25 14:57:31 EET	exam.E01
SOFTWARE			0	Eraser 6.2.0.2962 v.6.2.2962	2015-03-25 14:57:31 EET	exam.E01
SOFTWARE			0	Eraser 6.2.0.2962 v.6.2.2962	2015-03-25 14:57:31 EET	exam.E01
SOFTWARE			0	Microsoft .NET Framework 4 Extended v.4.0.30319	2015-03-25 14:54:33 EET	exam.E01
SOFTWARE			0	Microsoft .NET Framework 4 Extended v.4.0.30319	2015-03-25 14:54:33 EET	exam.E01
SOFTWARE			0	Microsoft .NET Framework 4 Extended v.4.0.30319	2015-03-25 14:54:33 EET	exam.E01
SOFTWARE			0	Microsoft .NET Framework 4 Extended v.4.0.30319	2015-03-25 14:54:33 EET	exam.E01
SOFTWARE			0	Microsoft .NET Framework 4 Extended v.4.0.30319	2015-03-25 14:54:33 EET	exam.E01
SOFTWARE			0	Microsoft .NET Framework 4 Extended v.4.0.30319	2015-03-25 14:54:33 EET	exam.E01
SOFTWARE			0	Microsoft .NET Framework 4 Extended v.4.0.30319	2015-03-25 14:54:06 EET	exam.E01
SOFTWARE			0	Microsoft .NET Framework 4 Extended v.4.0.30319	2015-03-25 14:54:06 EET	exam.E01
SOFTWARE			0	Microsoft .NET Framework 4 Extended v.4.0.30319	2015-03-25 14:54:06 EET	exam.E01

So the installed programs after 23/03/2015 are

1. Eraser 6.2.0.2962 v.6.2.2962 installed on 2015-03-25 14:57:31 EET
2. Microsoft .NET Framework 4 Extended v.4.0.30319 installed on 2015-03-25 14:54:33 EET

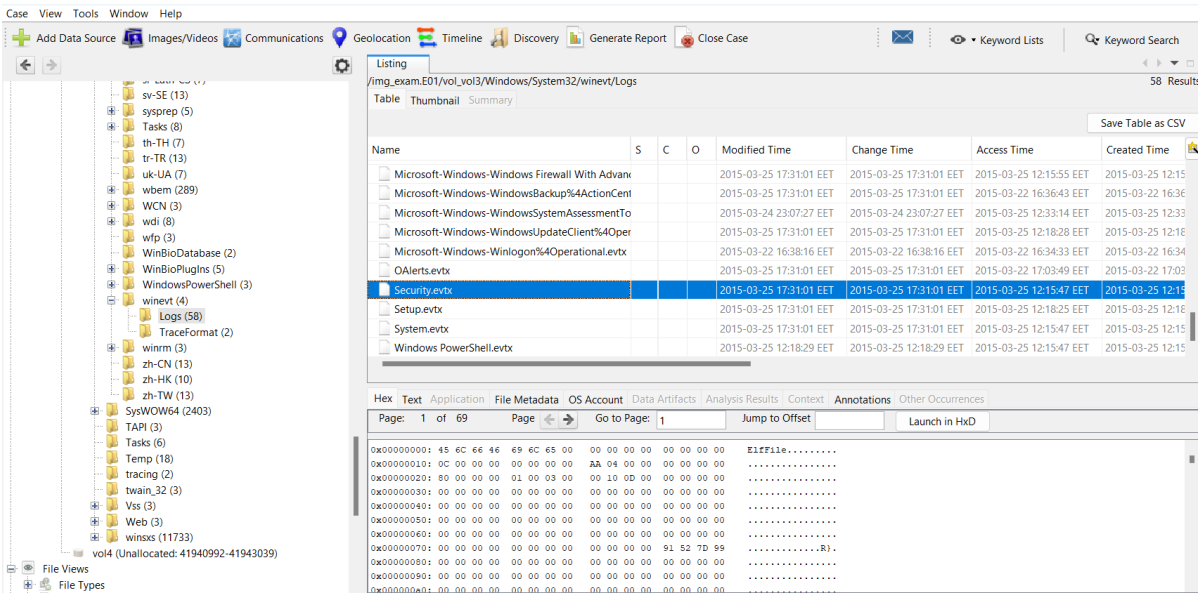
3. Microsoft .NET Framework 4 Client Profile v.4.0.30319 installed on 2015-03-25 14:52:06 EET
4. DXM_Runtime installed on 2015-03-25 10:15:21 EET
5. MPlayer2 installed on 2015-03-25 10:15:21 EET

12 Question 12

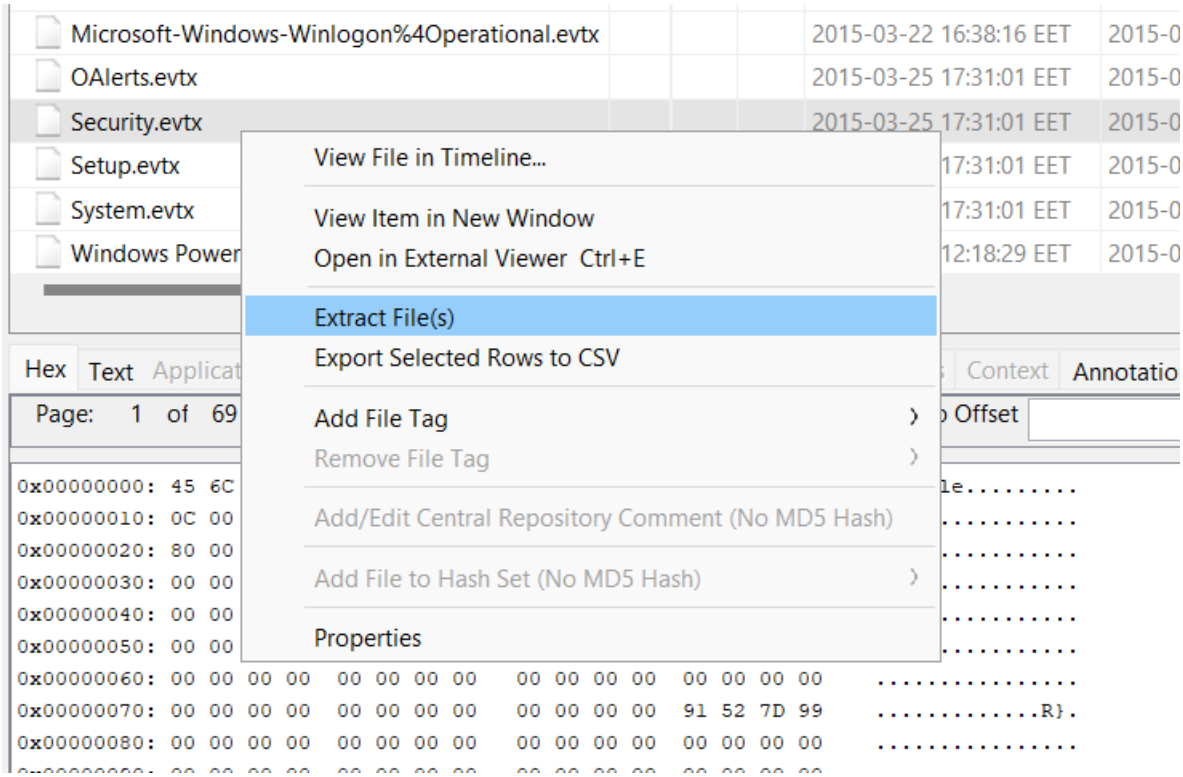
Review the event logs and list all suspect user logon and logoff events after 22/03/2015.

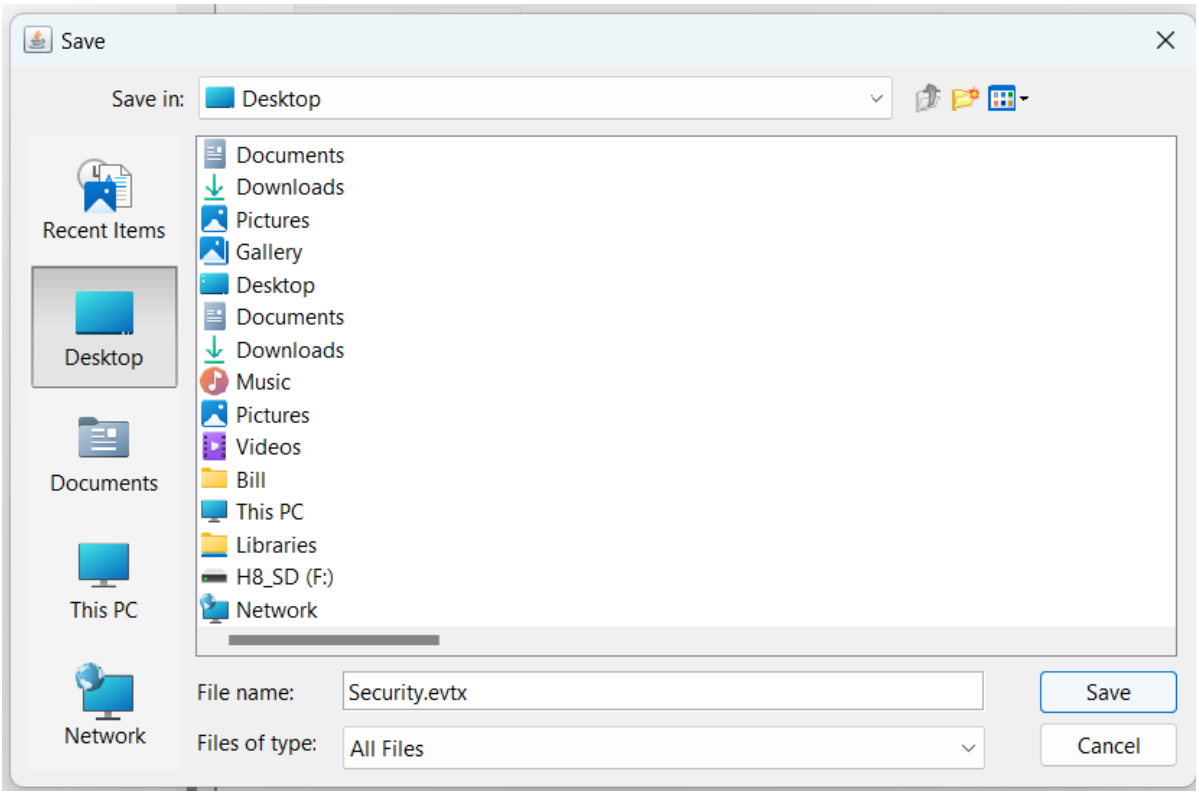
12.1 Answer

Firstly we navigate to Windows/System32/winevt/Logs and look for files such as Security.evtx, which records security-related events like logon and logoff activities.



We extract these files from the image to analyze them. Let's extract the file to our Desktop directory.


Microsoft-Windows-Winlogon%4Operational.evtx
2015-03-22 16:38:16 EET
OAlerts.evtx
2015-03-25 17:31:01 EET
Security.evtx
2015-03-25 17:31:01 EET
Setup.evtx
System.evtx
Windows Power
View File in Timeline...
View Item in New Window
Open in External Viewer Ctrl+E
Extract File(s)
Export Selected Rows to CSV
Add File Tag
Remove File Tag
Add/Edit Central Repository Comment (No MD5 Hash)
Add File to Hash Set (No MD5 Hash)
Properties
Hex
Text
Context
Annotatio
Page: 1 of 69
Offset
0x00000000: 45 6C
0x00000010: 0C 00
0x00000020: 80 00
0x00000030: 00 00
0x00000040: 00 00
0x00000050: 00 00
0x00000060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x00000070: 00 00 00 00 00 00 00 00 00 00 00 00 91 52 7D 99
0x00000080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00


Save
Save in:
Desktop
Recent Items
Desktop
Documents
This PC
Network
Documents
Downloads
Pictures
Gallery
Desktop
Documents
Downloads
Music
Pictures
Videos
Bill
This PC
Libraries
H8_SD (F:)
Network
File name:
Security.evtx
Files of type:
All Files
Save
Cancel

Now, we can use a tool capable of reading .evtx files.

There are several tools available for this:

- Built-in Windows Event Viewer: Great for Windows systems. We can simply use the Event Viewer to open and review the .evtx files.
- Third-party Tools: Tools like LogParser, Event Log Explorer, or third-party forensic tools that can interpret .evtx files might offer more advanced analysis options, such as filtering specific event IDs, times, and other relevant attributes.

For our purposes, we will use Built-in Windows Event Viewer.

We will focus on Relevant Event IDs: For user logon and logoff tracking and we will filter the events using specific IDs:

4624: An account was successfully logged on.

4608: System is starting up.

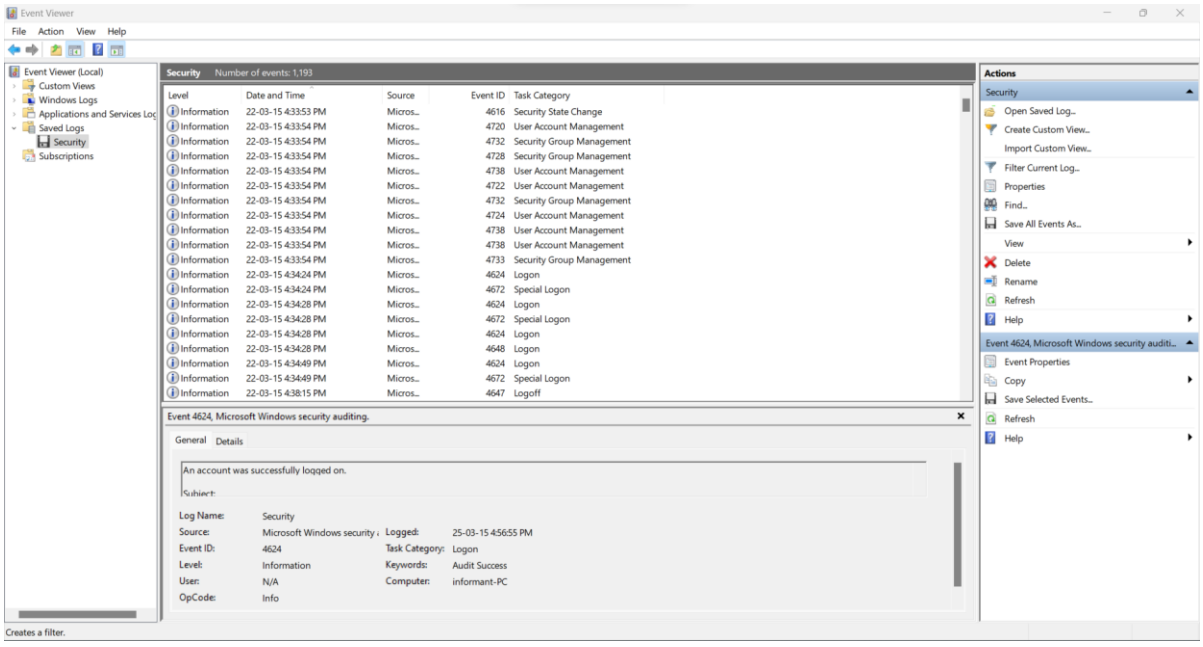
4637: An account was logged off.

1100: System is shuting down.

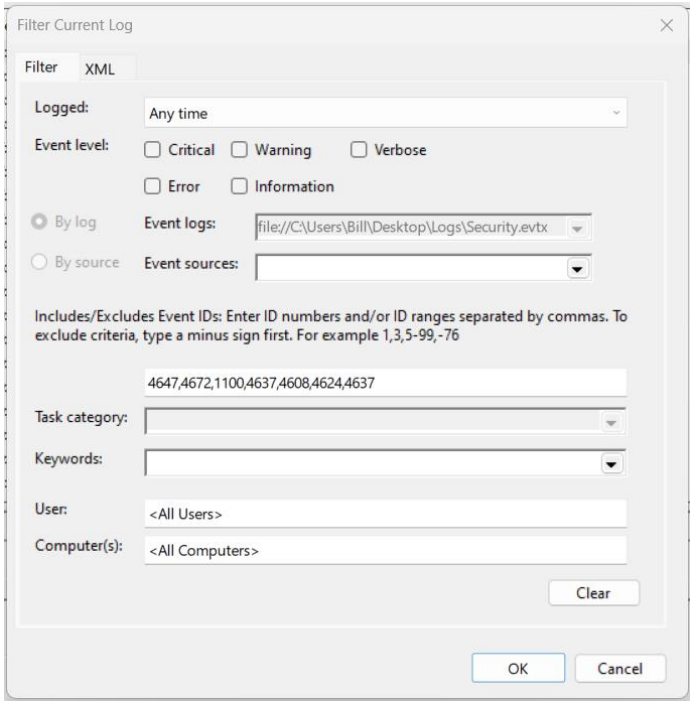
4672: Special privileges assigned to new logon.

4647: User initiated logoff.

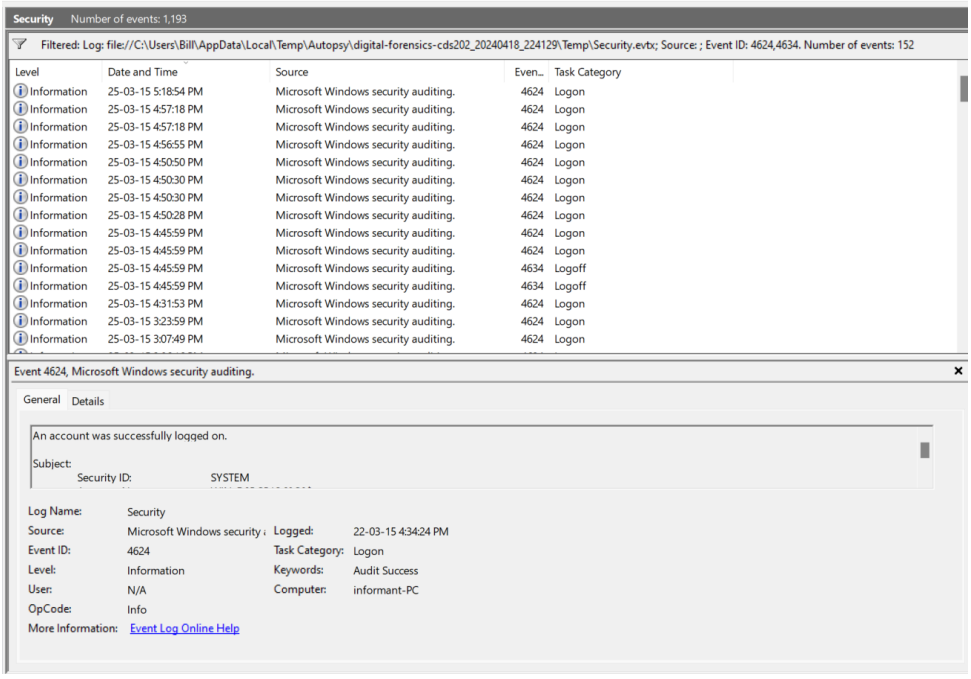
We will use the above ids.



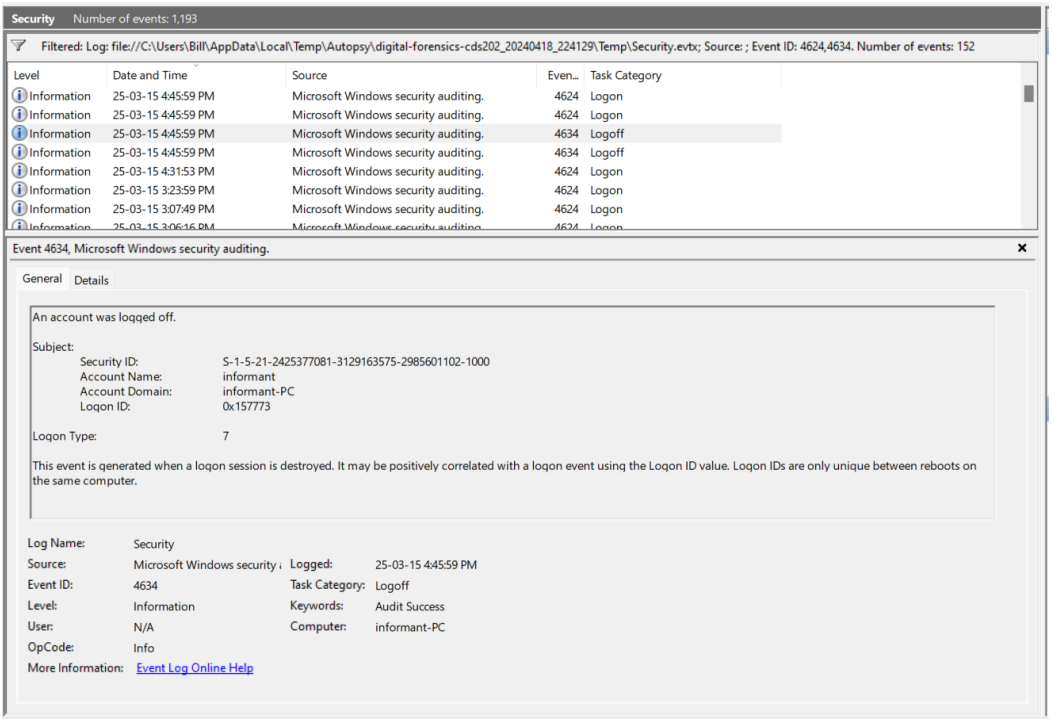
Now, we can create a custom filter for current log, entering the above ids.



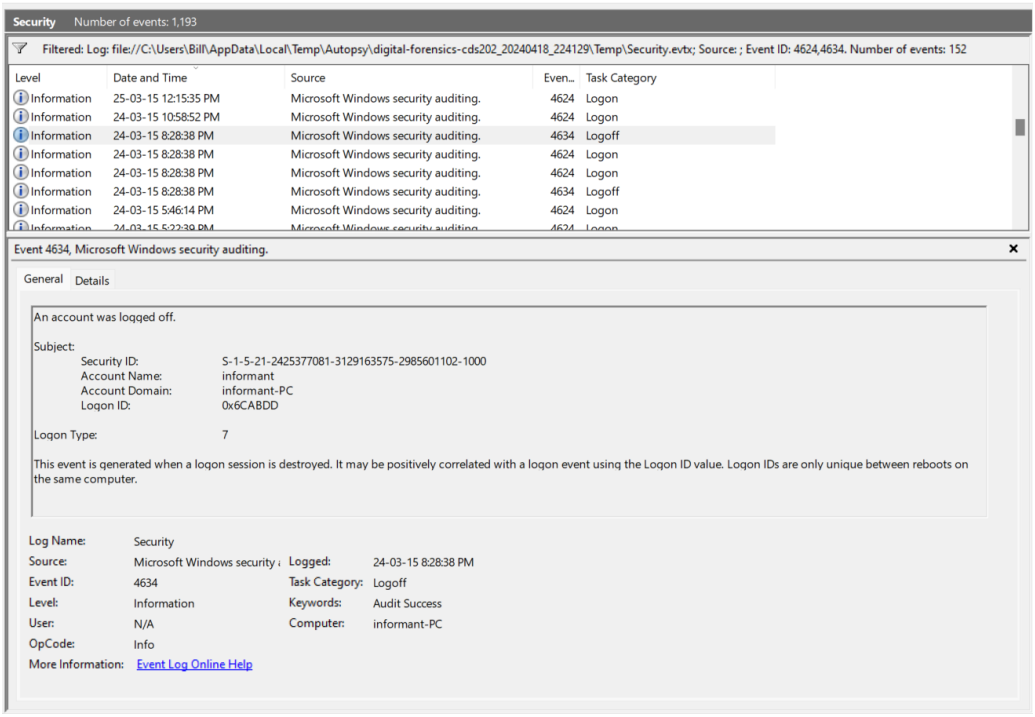
We classifly base on date.



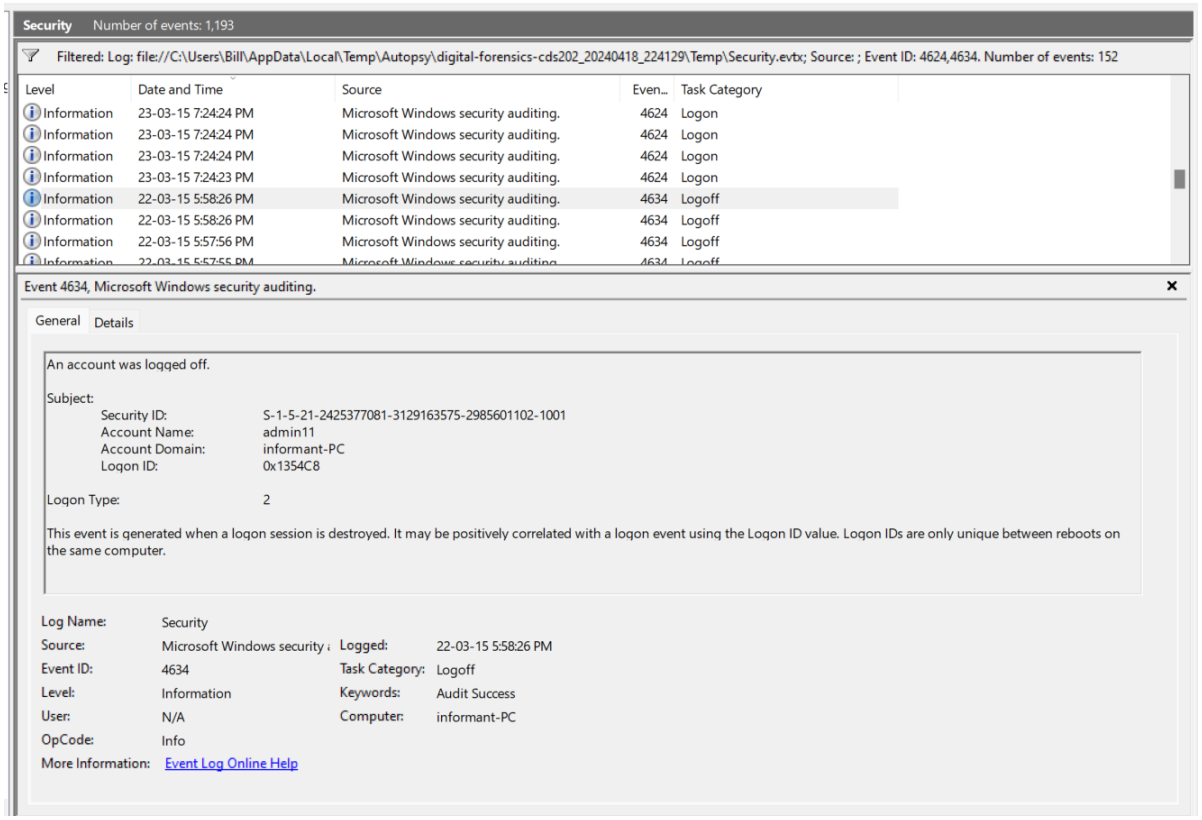
We see that the most recest user from user's list that logged on was informant



The second recent was informant again



Then we have 'admin11', who logged on on March 22, 2022, but we can not include that user because we are out of the given timeline.



So, the only suspect is informant.

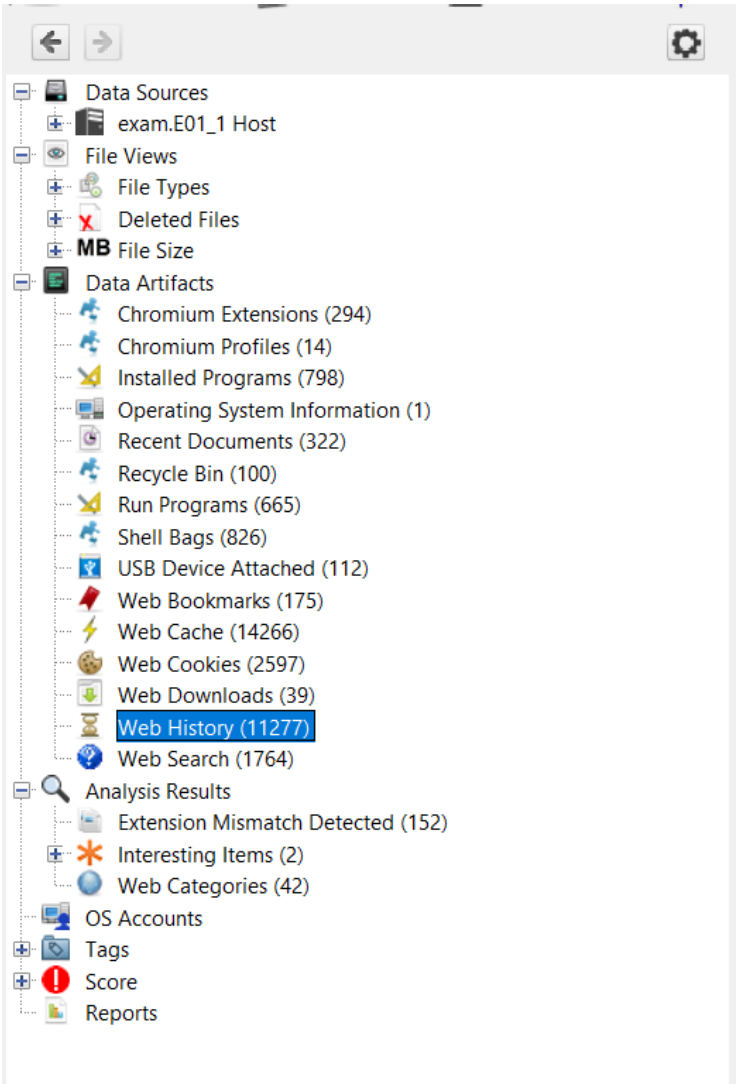
13 Question 13

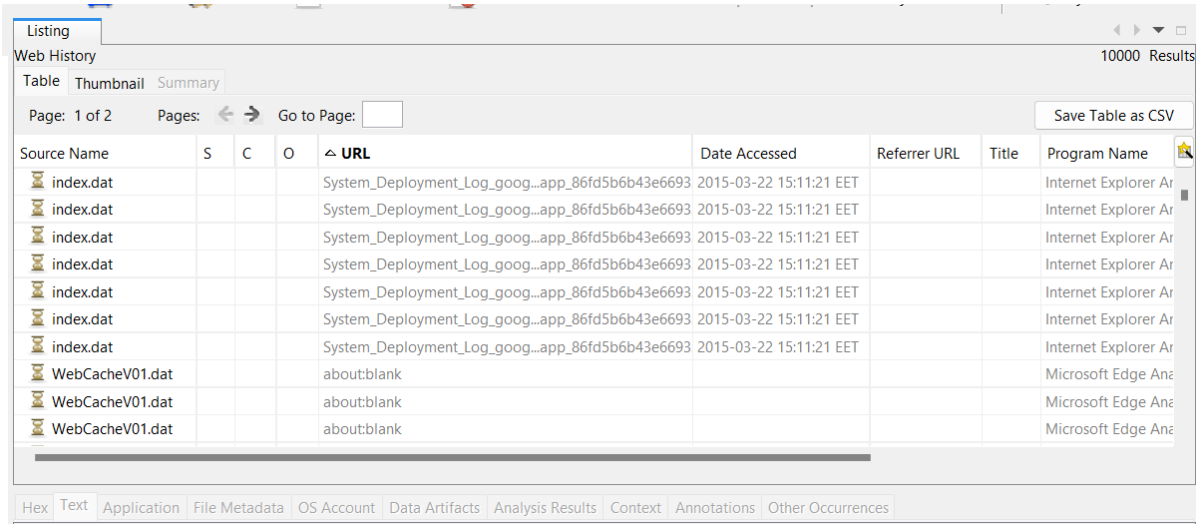
List all files that were opened with a browser. Include the user, the path, the source file and the timestamp.

13.1 Answer

To list all files that were opened with a browser, we can look at the web history and check for local urls entries.

We navigate to Web History Tab and we classify the list by URL.

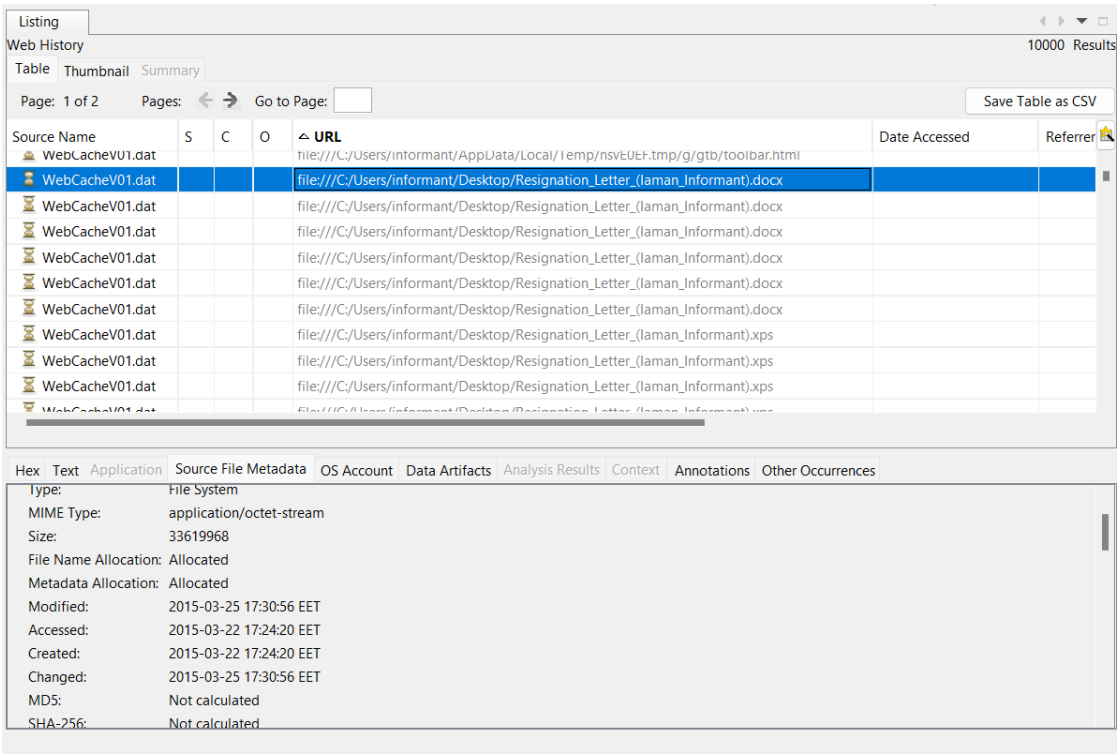

Data Sources
exam.E01_1 Host
File Views
File Types
Deleted Files
MB File Size
Data Artifacts
Chromium Extensions (294)
Chromium Profiles (14)
Installed Programs (798)
Operating System Information (1)
Recent Documents (322)
Recycle Bin (100)
Run Programs (665)
Shell Bags (826)
USB Device Attached (112)
Web Bookmarks (175)
Web Cache (14266)
Web Cookies (2597)
Web Downloads (39)
Web History (11277)
Web Search (1764)
Analysis Results
Extension Mismatch Detected (152)
Interesting Items (2)
Web Categories (42)
OS Accounts
Tags
Score
Reports

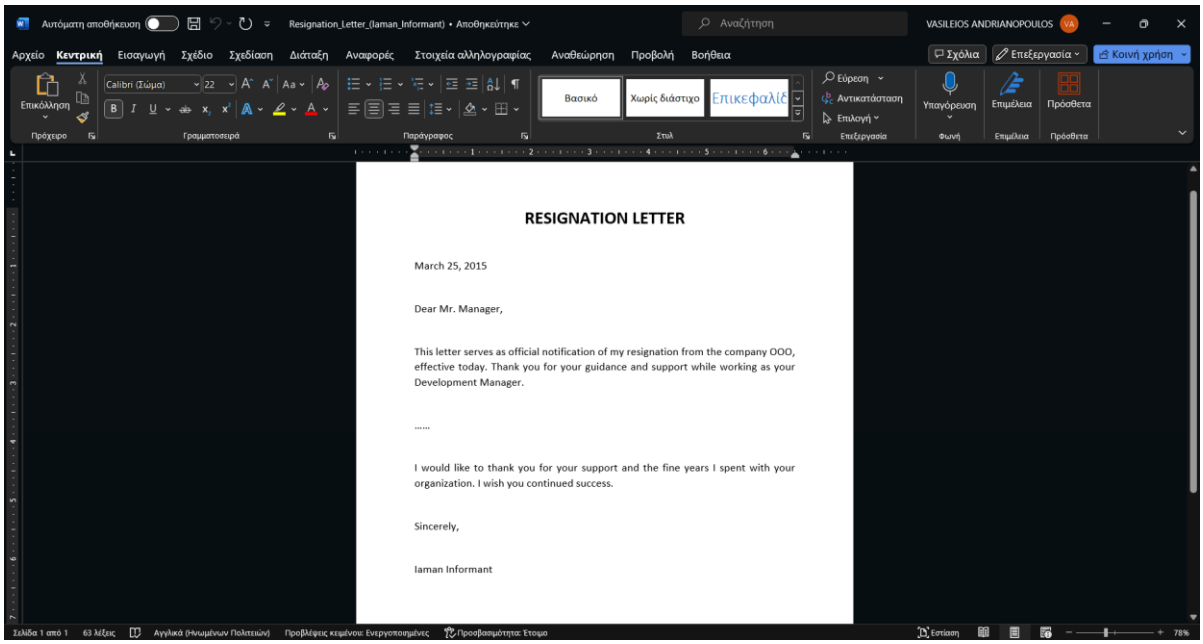

Listing
Web History
10000 Results
Table
Thumbnail
Summary
Page: 1 of 2
Pages:
Go to Page:
Save Table as CSV
Source Name
S
C
O
URL
Date Accessed
Referrer URL
Title
Program Name
index.dat
System_Deployment_Log_goog...app_86fd5b6b43e6693
2015-03-22 15:11:21 EET
Internet Explorer Ar
WebCacheV01.dat
about:blank
Microsoft Edge Ana
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences

Then we can find the entries like “file://”

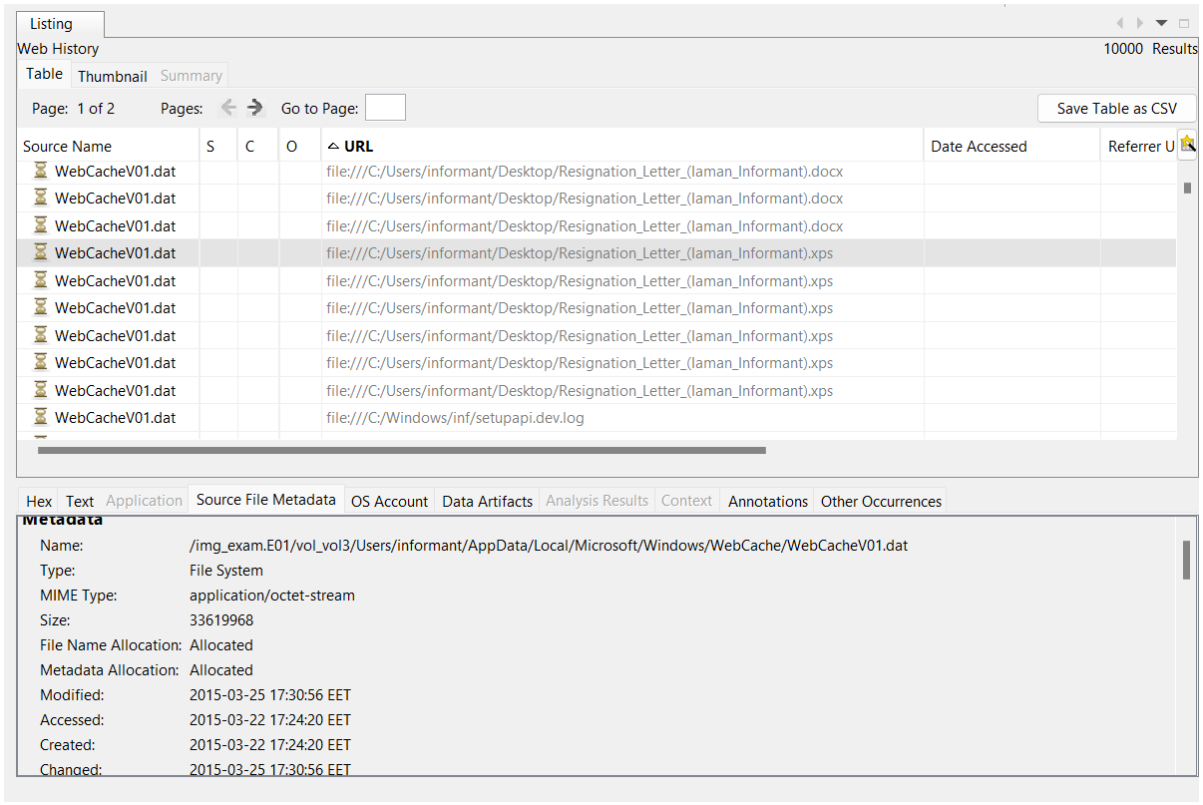
First we have the doc file Resignation_Letter_(laman_informant).docx that was created at 22-03-22 17:30:56 EET, and changed at 25-03-2015 17:30:56 EET.

The filepath is C:/Users/informant/Desktop and we can simple create a backup of the file to our own system





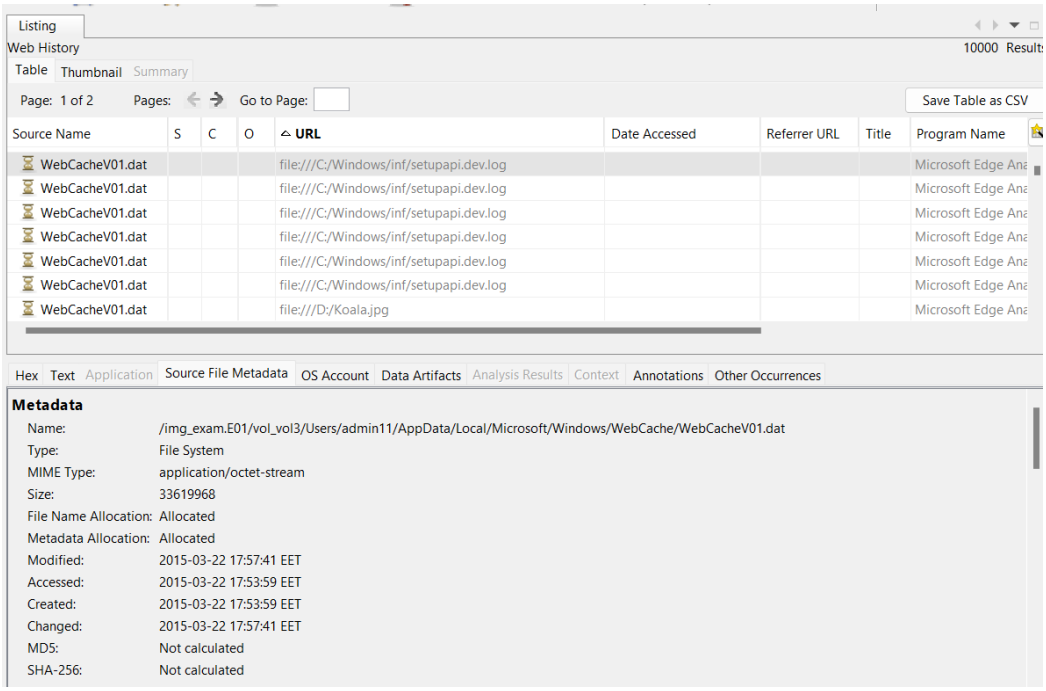
Then we have the file Resignation_Letter_(laman_informant).xps that is located on Desktop and created at 22-03-2015 17:24:20 and modified at 25-03-2015 17:30:56



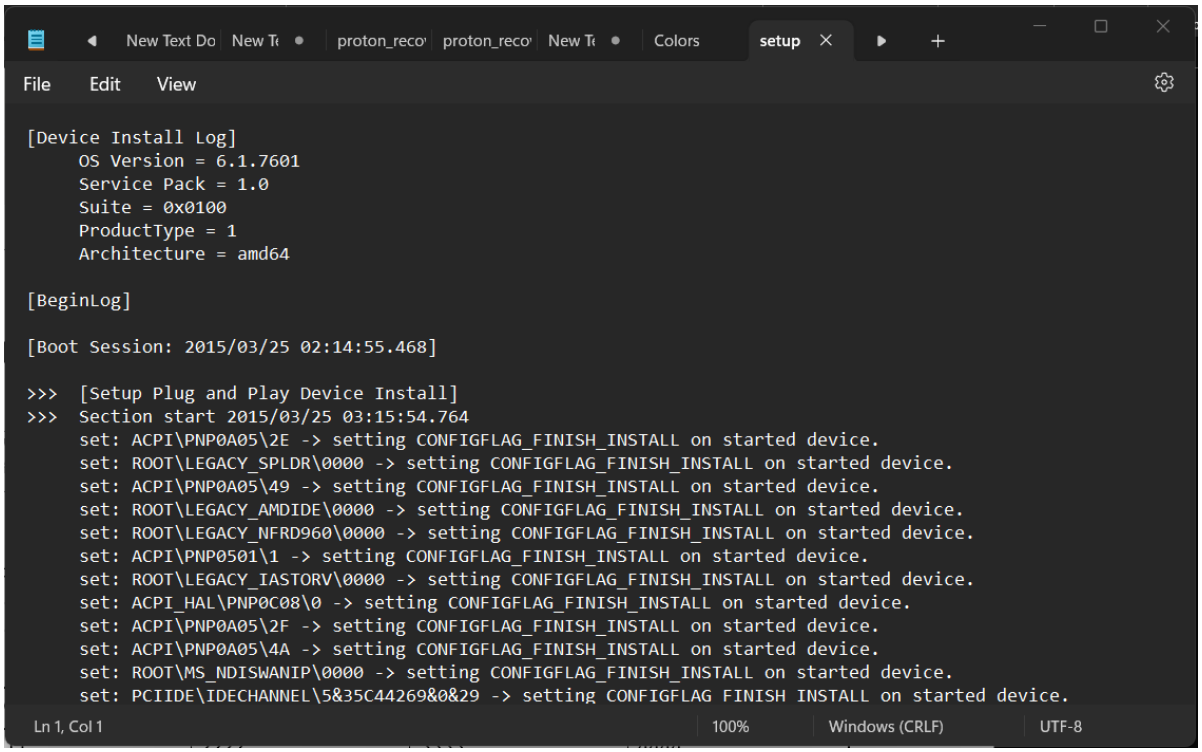
We can navigate to informant's Dektop folder

Then admin11 opened a file called setupapi.dev.log wich is located on C:/Windows/int

The file created at 22-03-2015 17:53:59 EET and modified at 22-03-2015 17:57:41 EET.

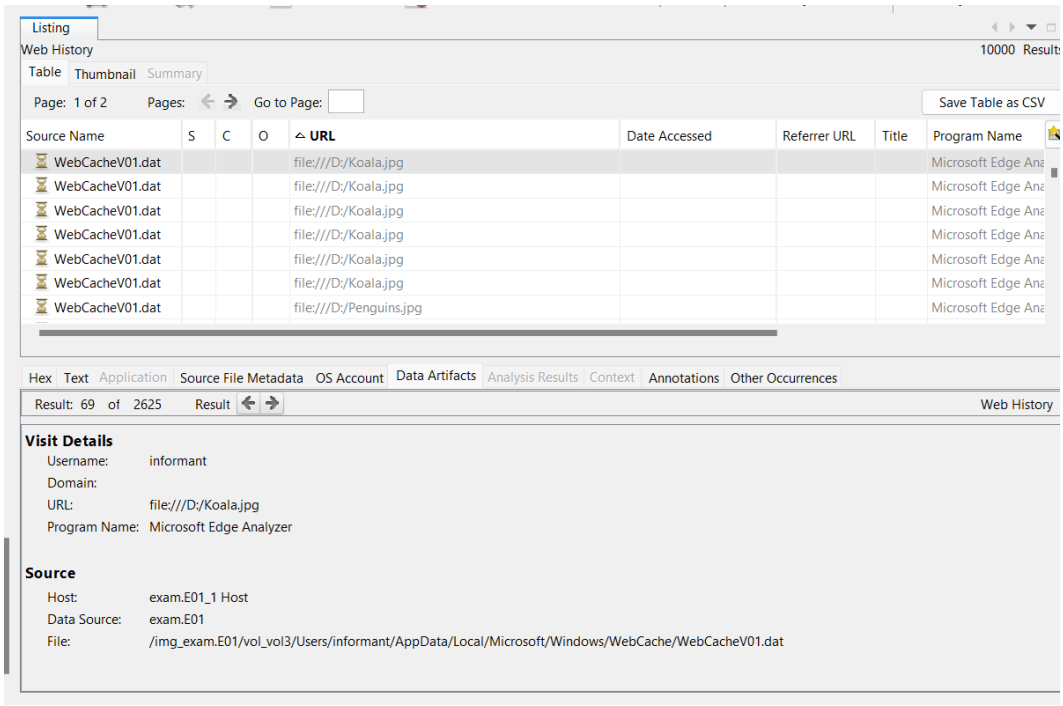


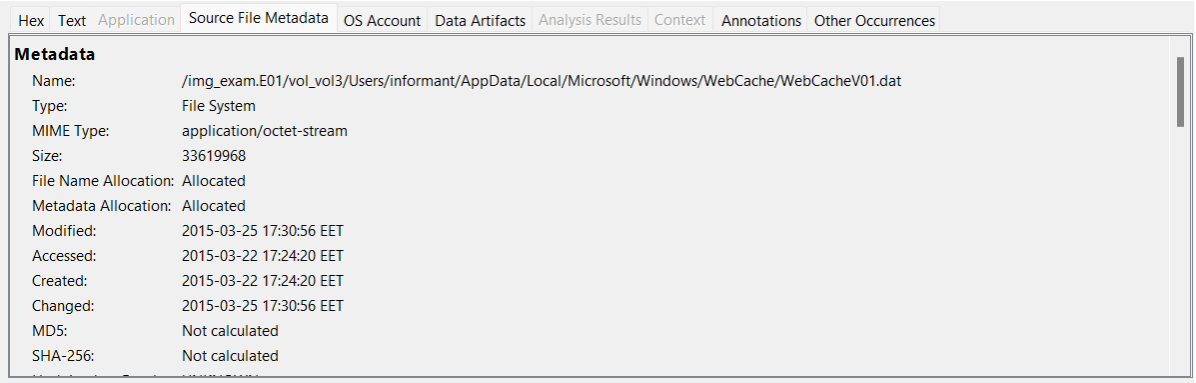
We can navigate to that folder and view the file with a simple txt editor.



Then, informant viewed a koalla picture file that is located on D partition.

This file was created at 22-03-2015 17:30:56 EET.





We continue the same and finally we have the following table

File Name	File Path	Owner	Accessed
Resignation_Letter_(laman_Informant).docx	C:/Users/informant/Desktop/Resignation_Letter_(laman_Informant).docx	informant	2015-03-22 17:24:20 EET
setupapi.dev.log	C:/Windows/inf/setupapi.dev.log	admin11	2015-03-22 17:53:59 EET
Koala.jpg	D:/Koala.jpg	Informant	2015-03-22 17:24:20 EET
Penguins.jpg	D:/Penguins.jp	Informant	2015-03-22 17:24:20 EET
Tulips.jpg	D:/Tulips.jpg	Informant	2015-03-22 17:24:20 EET
winter_whether_advisory.zip	D:/de/winter_whether_advisory.zip	Informant	2015-03-22 17:24:20 EET
[secret_project]_design_concept.ppt	E:/RM#1/Secret%20Project%20Data/design/[secret_project]_design_concept.ppt	informant	2015-03-22 17:24:20 EET
[secret_project]_proposal.docx	E:/RM#1/Secret%20Project%20Data/proposal/[secret_project]_proposal.docx	informant	2015-03-22 17:24:20 EET

[secret_project]_final_meeting.pptx	V:/Secret%20Project%20Data/final/[secret_project]_final_meeting.pptx	informant	2015-03-22 17:24:20 EET
(secret_project)_pricing_decision.xls	10.11.11.128/secured_drive/Secret%20Project%20Data/pricing%20decision/(secret_project)_pricing_decision.xlsx	informant	2015-03-22 17:24:20 EET
toolbar.html	C:/Users/informant/AppData/Local/Temp/nsvE0EF.tmp/g/gtb/toolbar.html	informant	2015-03-22 17:24:20 EET

Table 1. List of the files that were open from browser

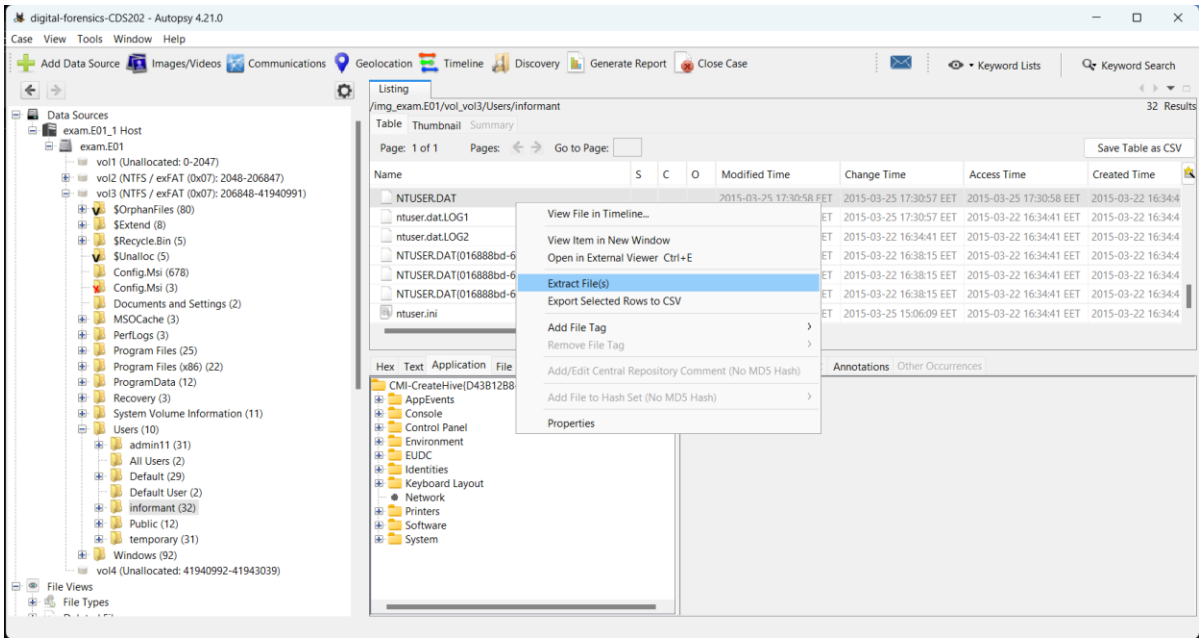
14 Question 14

List all suspect user keywords that were used at the search bar in Windows Explorer.

14.1 Answer

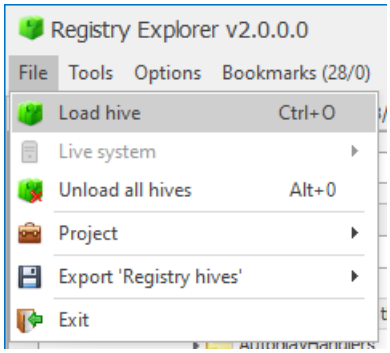
The suspect user is informant and to list all the keywords that searched in Windows Explorer search bar we have to locate ntuser.dat file.

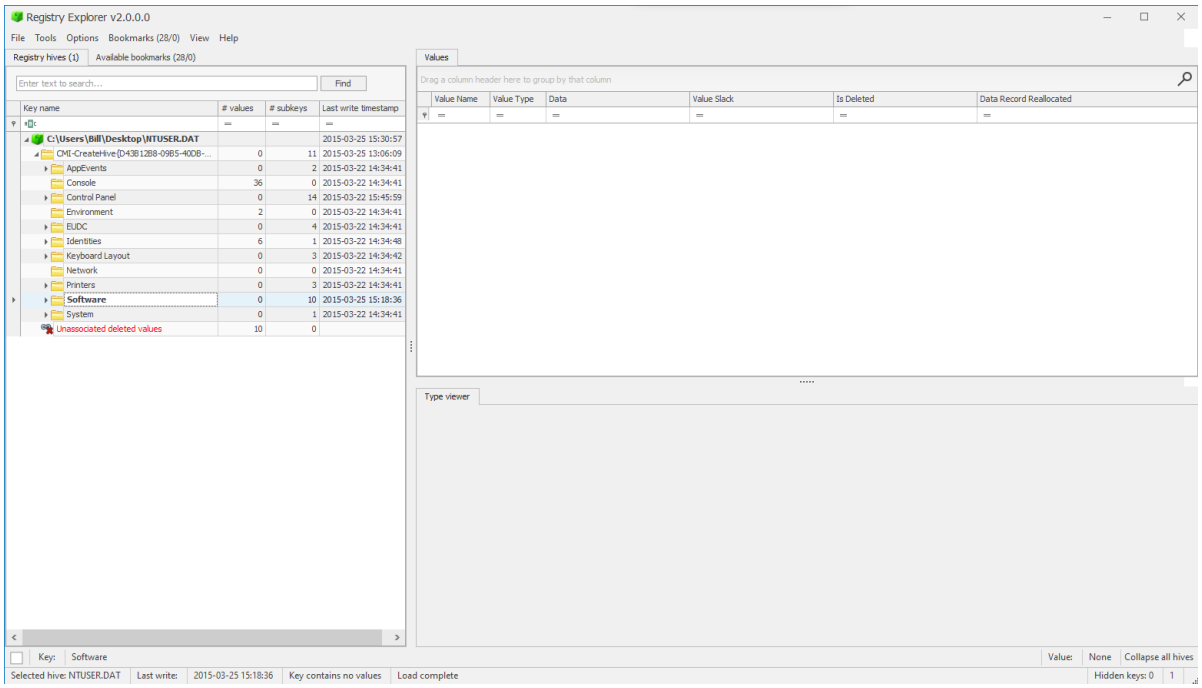
We navigate to Users/informant and we export ntuser.dat file to our pc.



We want to read it with a third-party application such as Eric Zimmerman's Registry Explorer.

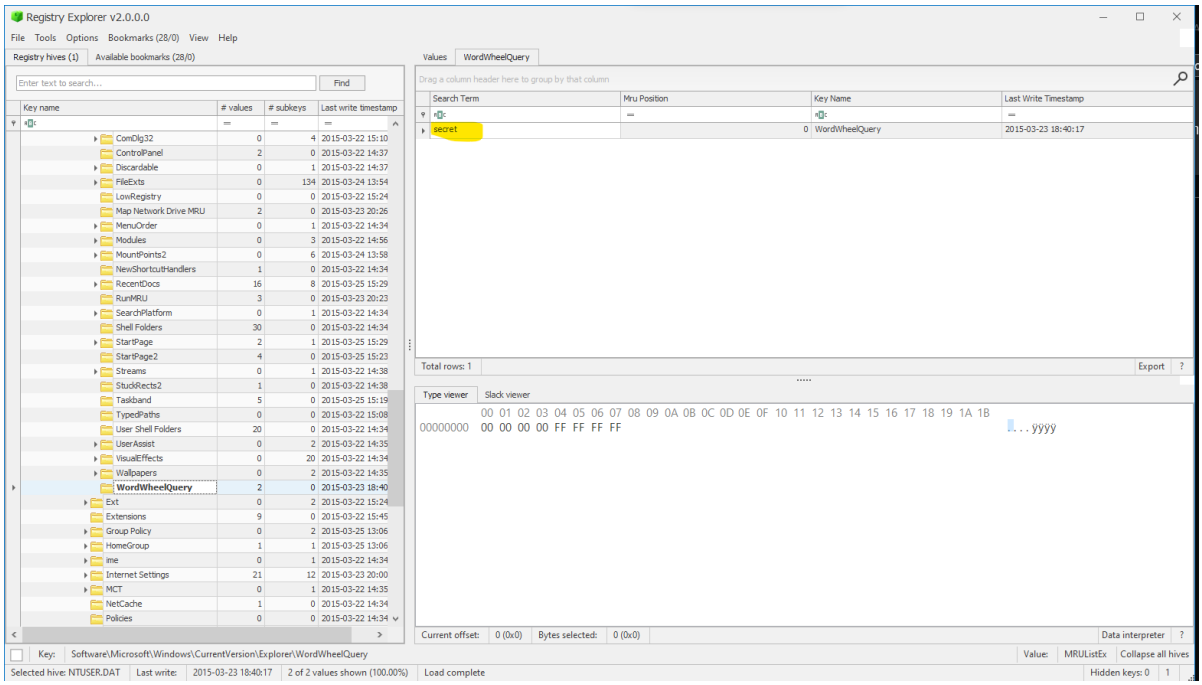
We launch Registry Explorer and we load the file.





Then, we navigate to Software/Microsot/Windows/Currentversion/Explorer/WordWheelQuery

And we see that the word that was searched was secret



15 Question 15

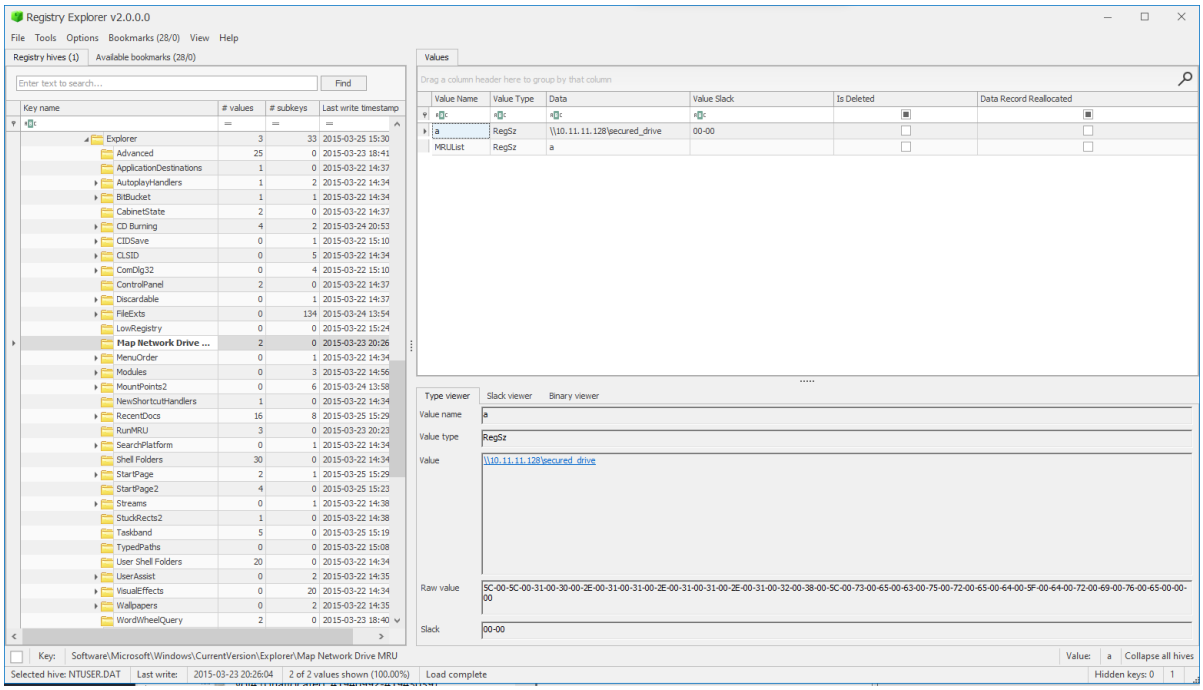
What is the IP address of a shared network drive accessed by the suspect user? List all directories that were traversed by the suspect in that network drive.

15.1 Answer

The suspect user is informant and to find the IP address of a shared network drive we have to locate ntuser.dat file.

We can use the previous exported ntuser.dat file that we imported to Eric Zimmerman's Registry Explorer.

We navigate to Software/Microsot/Windows/Currentversion/Explorer/Map Network Drive MRU



Here, we can see that the ip is 10.11.11.128

16 Question 16

What is the IP address of a shared network drive accessed by the suspect user? List all directories that were traversed by the suspect in that network drive.

16.1 Answer

To track the files recently opened by informant on a shared network drive, we would investigate specific directories and registry entries on his computer because:

- Recent and Office Recent Directories (*.lnk files): These contain shortcuts to the most recently accessed files and folders, including those on network drives. They reveal which files were opened and their original locations.
- AutomaticDestinations and CustomDestinations: These folders store lists of files opened by applications, maintained by Windows. Analyzing these can provide a history of accessed documents, including network files.
- Registry Entries (File MRU): Entries such as those for Excel and PowerPoint in the Windows Registry track the most recently used documents by these applications, showing paths to accessed documents on network drives.

So we will search here,

\User\informant\AppData\Roaming\Microsoft\Windows\Recent*.lnk

\User\informant\AppData\Roaming\Microsoft\Office\Recent*.lnk

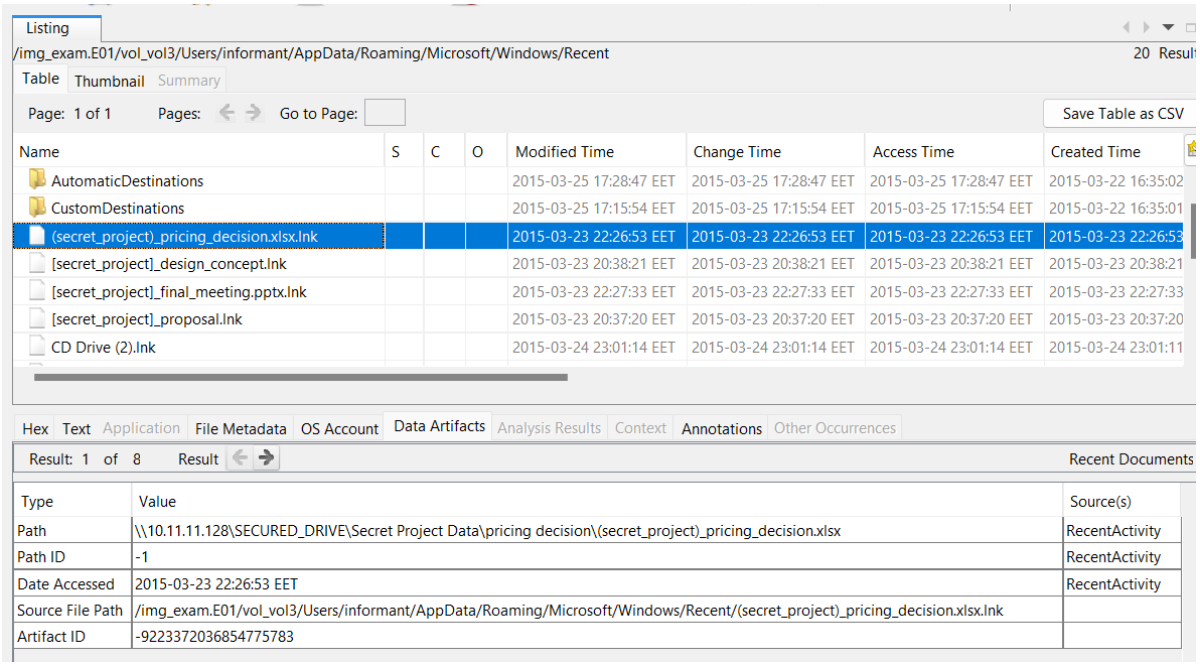
\User\informant\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

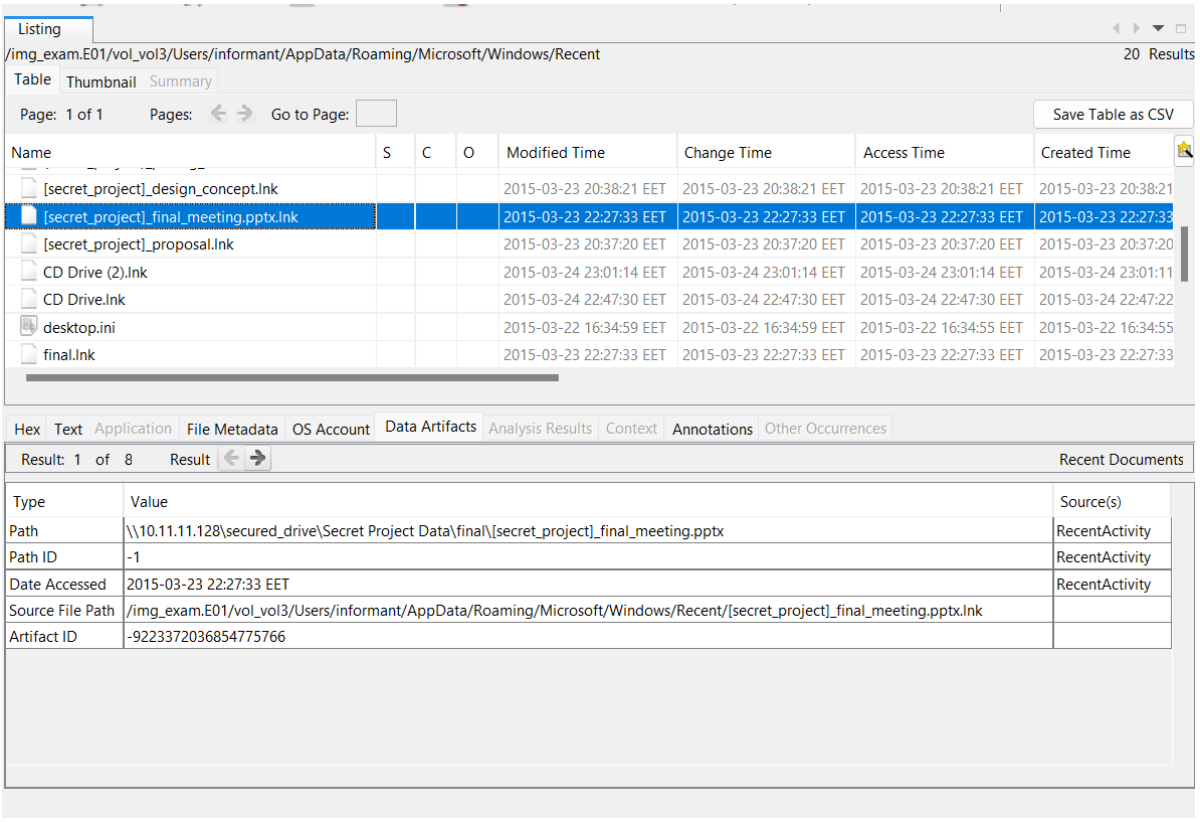
\User\informant\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations

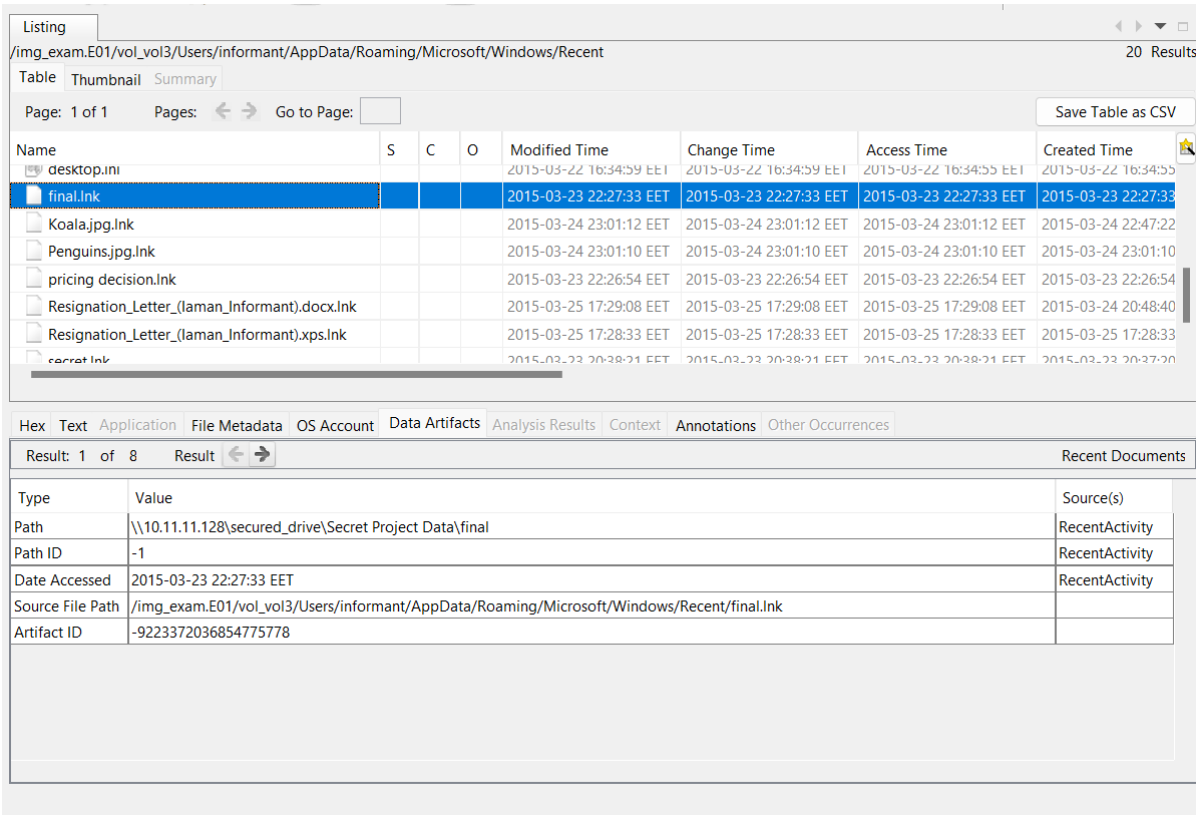
HKU\informant\Software\Microsoft\Office\15.0\Excel\File MRU

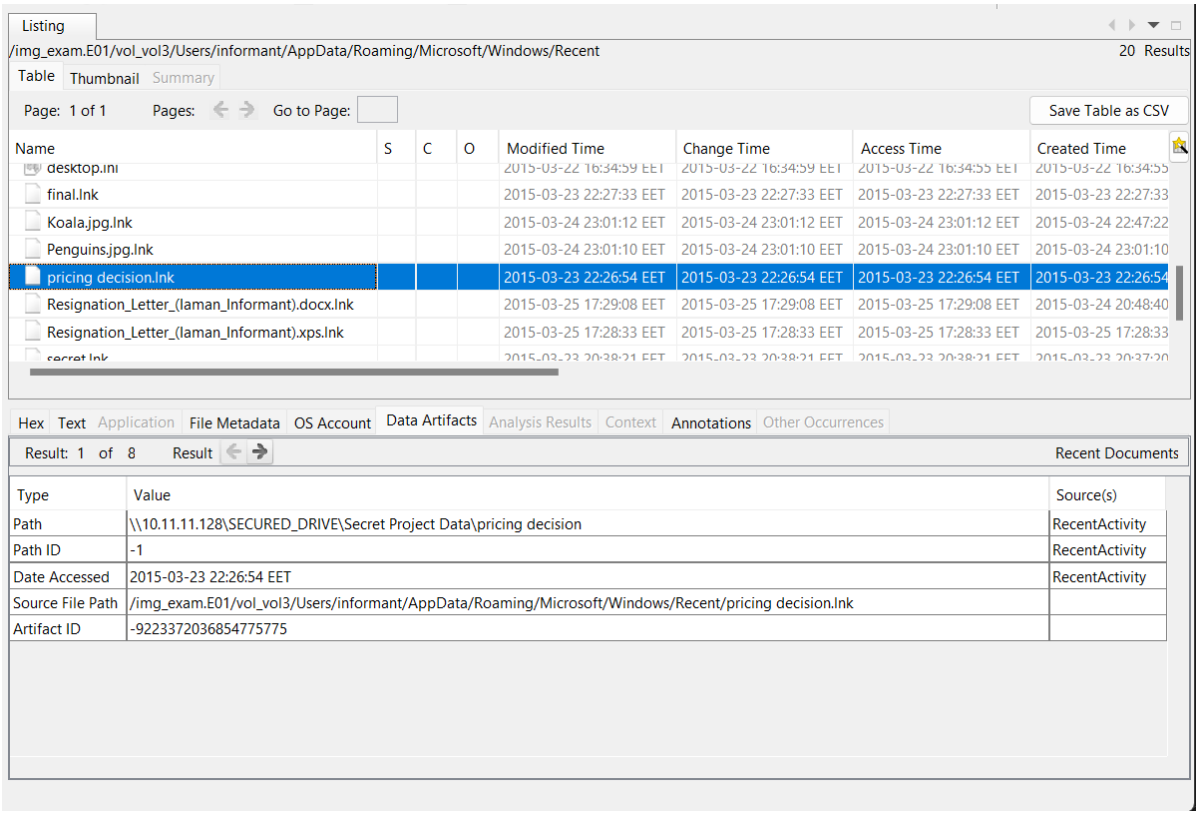
HKU\informant\Software\Microsoft\Office\15.0\PowerPoint\File MRU

On \User\informant\AppData\Roaming\Microsoft\Windows\Recent path

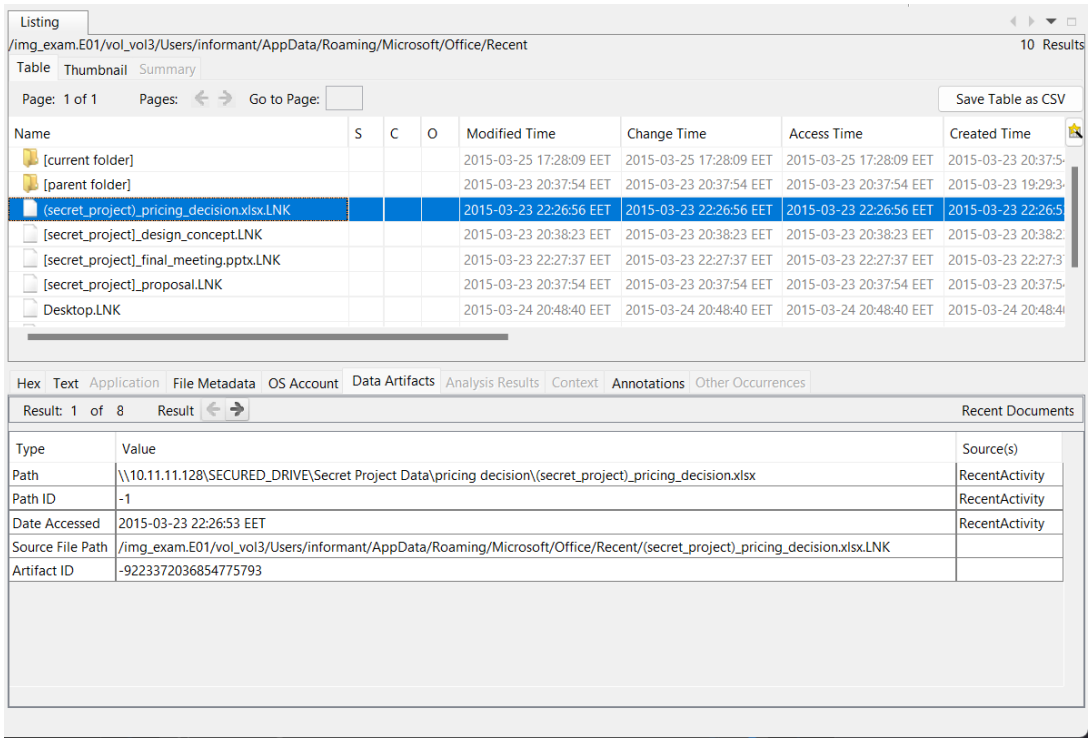


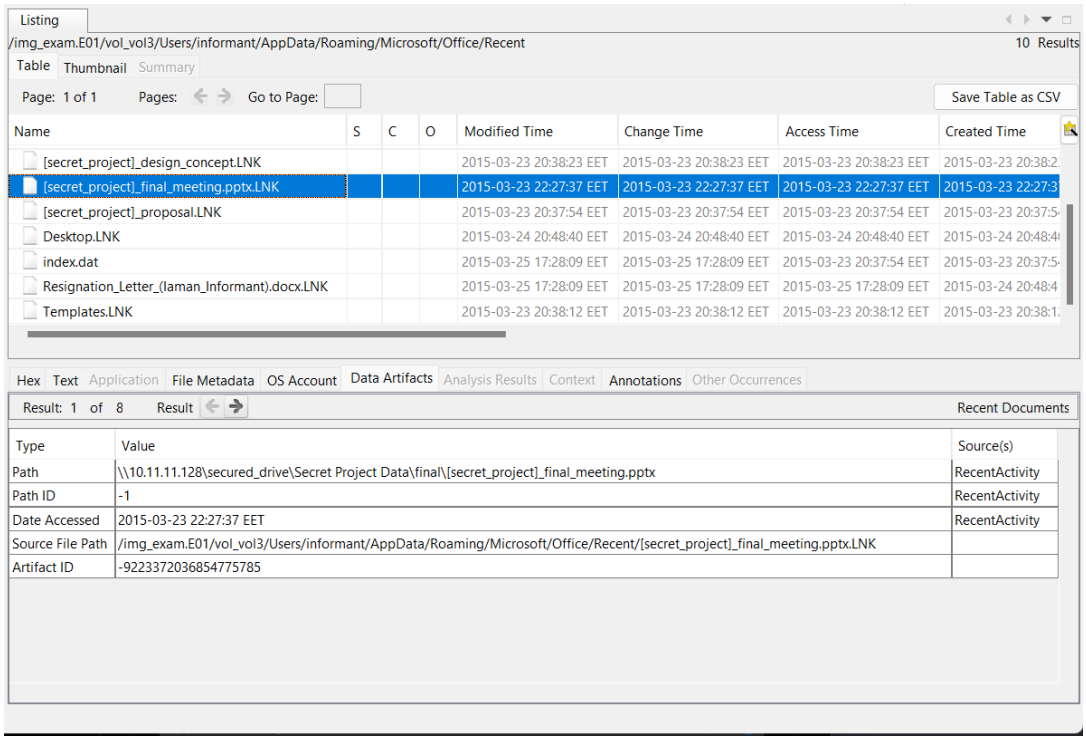



Listing
/img_exam.E01/vol_vol3/Users/informant/AppData/Roaming/Microsoft/Windows/Recent
20 Results
Table Thumbnail Summary
Page: 1 of 1 Pages: Go to Page:
Save Table as CSV
Name S C O Modified Time Change Time Access Time Created Time
final.lnk 2015-03-23 22:27:33 EET 2015-03-23 22:27:33 EET 2015-03-23 22:27:33 EET 2015-03-23 22:27:33
Koala.jpg.lnk 2015-03-24 23:01:12 EET 2015-03-24 23:01:12 EET 2015-03-24 23:01:12 EET 2015-03-24 22:47:22
Penguins.jpg.lnk 2015-03-24 23:01:10 EET 2015-03-24 23:01:10 EET 2015-03-24 23:01:10 EET 2015-03-24 23:01:10
pricing decision.lnk 2015-03-23 22:26:54 EET 2015-03-23 22:26:54 EET 2015-03-23 22:26:54 EET 2015-03-23 22:26:54
Resignation_Letter_(Iaman_Informant).docx.lnk 2015-03-25 17:29:08 EET 2015-03-25 17:29:08 EET 2015-03-25 17:29:08 EET 2015-03-24 20:48:40
Resignation_Letter_(Iaman_Informant).xps.lnk 2015-03-25 17:28:33 EET 2015-03-25 17:28:33 EET 2015-03-25 17:28:33 EET 2015-03-25 17:28:33
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Result: 1 of 8 Result
Recent Documents
Type Value Source(s)
Path \\10.11.11.128\secured_drive\Secret Project Data\final RecentActivity
Path ID -1 RecentActivity
Date Accessed 2015-03-23 22:27:33 EET RecentActivity
Source File Path /img_exam.E01/vol_vol3/Users/informant/AppData/Roaming/Microsoft/Windows/Recent/final.lnk
Artifact ID -9223372036854775778


Listing
/img_exam.E01/vol_vol3/Users/informant/AppData/Roaming/Microsoft/Windows/Recent
20 Results
Table Thumbnail Summary
Page: 1 of 1 Pages: Go to Page:
Save Table as CSV
Name S C O Modified Time Change Time Access Time Created Time
final.lnk 2015-03-23 22:27:33 EET 2015-03-23 22:27:33 EET 2015-03-23 22:27:33 EET 2015-03-23 22:27:33
Koala.jpg.lnk 2015-03-24 23:01:12 EET 2015-03-24 23:01:12 EET 2015-03-24 23:01:12 EET 2015-03-24 22:47:22
Penguins.jpg.lnk 2015-03-24 23:01:10 EET 2015-03-24 23:01:10 EET 2015-03-24 23:01:10 EET 2015-03-24 23:01:10
pricing decision.lnk 2015-03-23 22:26:54 EET 2015-03-23 22:26:54 EET 2015-03-23 22:26:54 EET 2015-03-23 22:26:54
Resignation_Letter_(Iaman_Informant).docx.lnk 2015-03-25 17:29:08 EET 2015-03-25 17:29:08 EET 2015-03-25 17:29:08 EET 2015-03-24 20:48:40
Resignation_Letter_(Iaman_Informant).xps.lnk 2015-03-25 17:28:33 EET 2015-03-25 17:28:33 EET 2015-03-25 17:28:33 EET 2015-03-25 17:28:33
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Result: 1 of 8 Result
Recent Documents
Type Value Source(s)
Path \\10.11.11.128\SECURED_DRIVE\Secret Project Data\pricing decision RecentActivity
Path ID -1 RecentActivity
Date Accessed 2015-03-23 22:26:54 EET RecentActivity
Source File Path /img_exam.E01/vol_vol3/Users/informant/AppData/Roaming/Microsoft/Windows/Recent/pricing decision.lnk
Artifact ID -9223372036854775775

On \User\informant\AppData\Roaming\Microsoft\Office\Recent*.lnk path

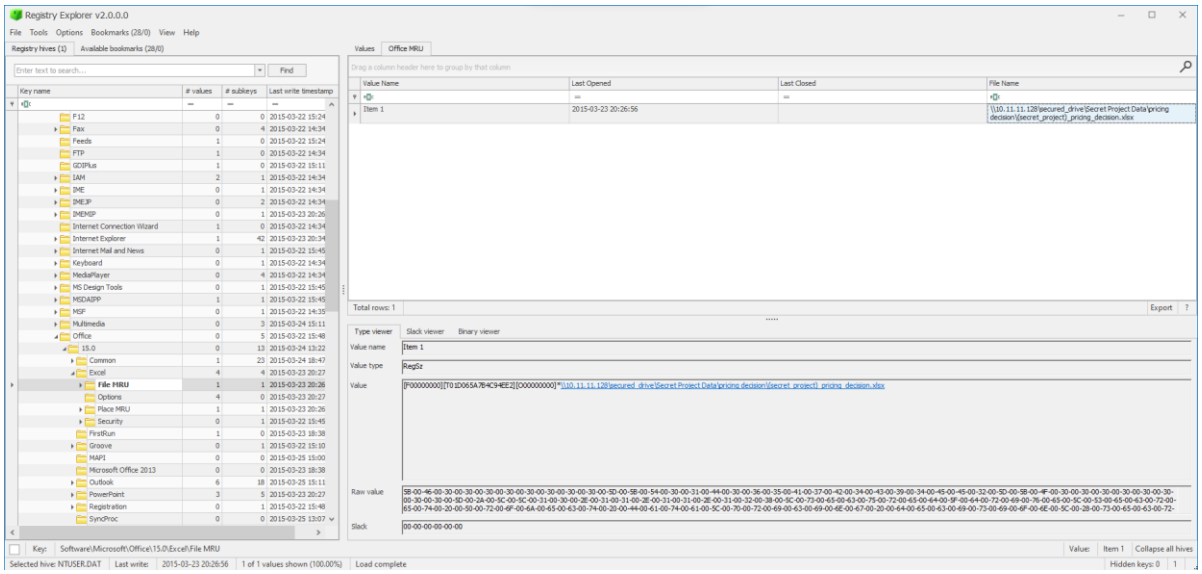




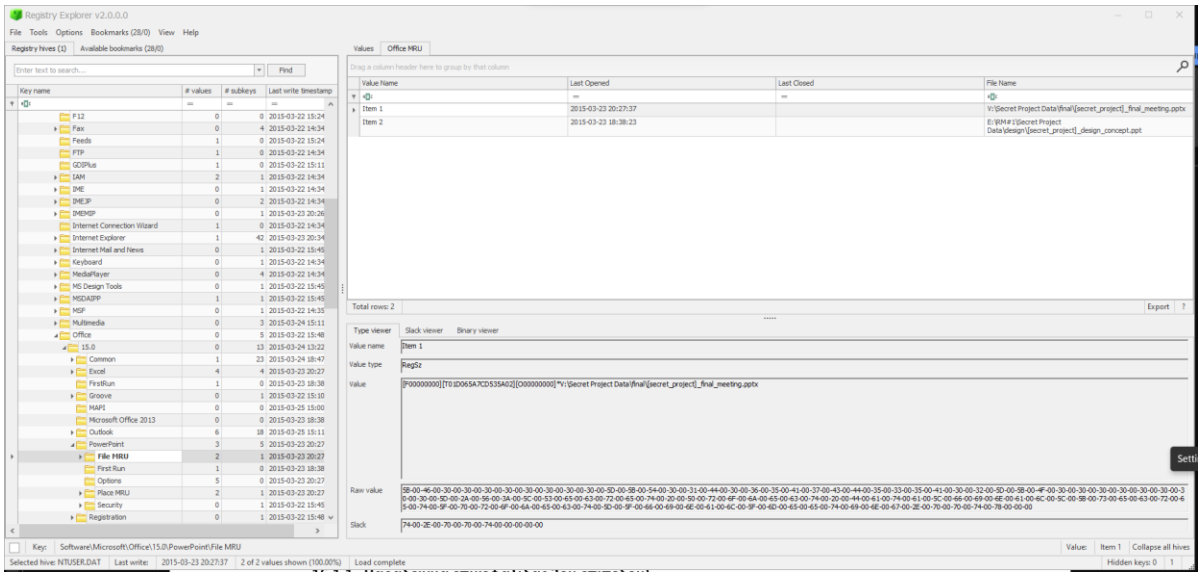
On \User\informant\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations path there's nothing relative to network shared drive.

On \User\informant\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations path there's nothing relative to network shared drive.

On HKU\informant\Software\Microsoft\Office\15.0\Excel\File MRU we can find the xlsx file



And on HKU\informant\Software\Microsoft\Office\15.0\PowerPoint\File MRU we can find the 2 following files

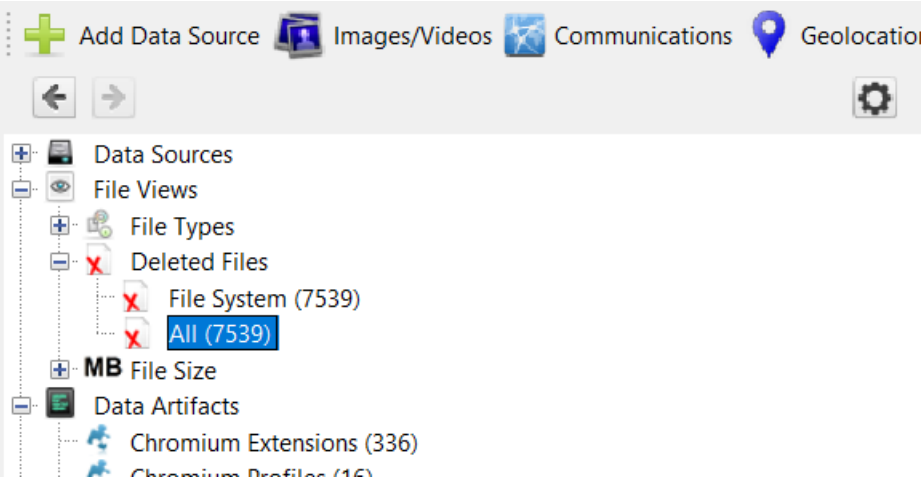


17 Question 17

Which deleted executables last accessed on 25/03/2015 show that the suspect user tried to erase data from the system?

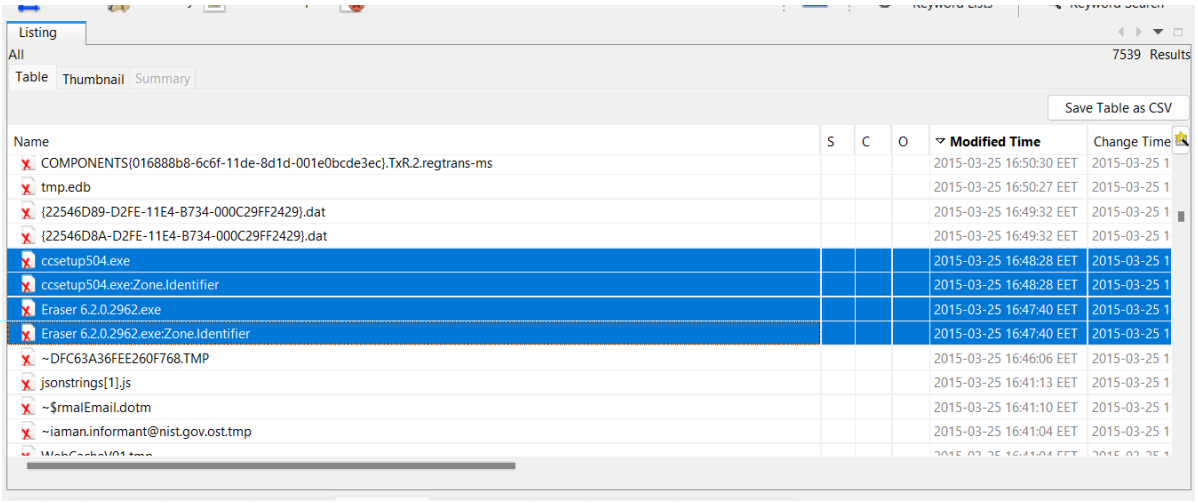
17.1 Answer

From Deleted Filed section on Autopsy, we can easily find all the deleted executables that last accessed on 25/03/2015.



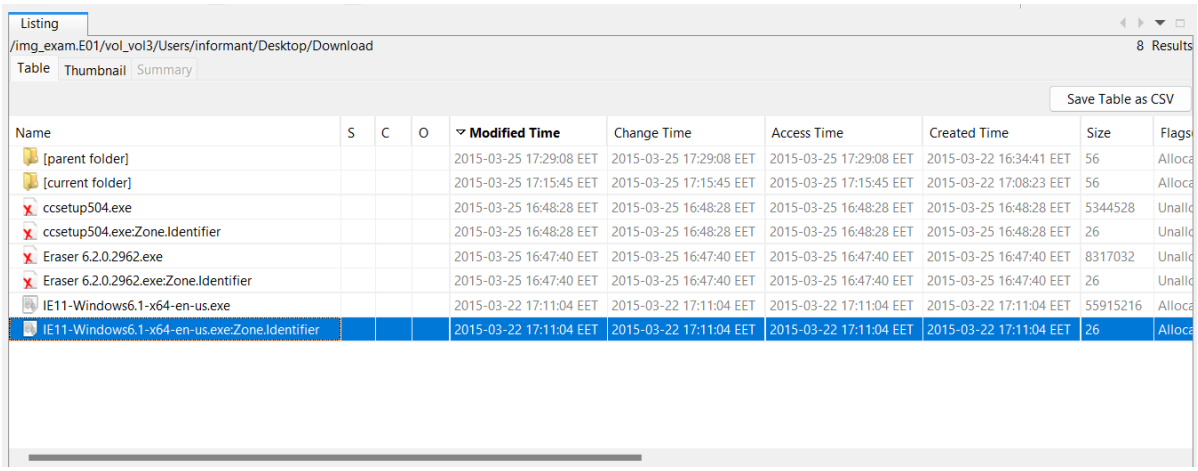
We sort the list by Modified Date and we start finding the .exe extension files that was accessed by informant and seems suspicious.

We find 2 files.



ccsetup504.exe and Eraser 6.2.0.2963.exe

We can also locate those deleted files to informant's download folder



CCleaner and Eraser are not inherently anti-forensics tools; however, they can be misused for such purposes. Here's why they could be considered as potentially aiding anti-forensic activities:

1. File Deletion: Both CCleaner and Eraser have features that allow users to securely delete files from their systems. While these features are intended for legitimate purposes such as maintaining privacy or securely erasing sensitive data, they can also be misused to deliberately erase incriminating evidence or cover one's tracks.

2. Data Overwriting: Eraser, in particular, is known for its ability to securely overwrite deleted files to prevent their recovery using forensic techniques. While this feature can be useful for protecting sensitive information from unauthorized access, it can also hinder forensic investigations by making it more difficult or impossible to recover deleted files.
3. Evidence Destruction: When used with the intention of destroying evidence, CCleaner and Eraser can effectively erase digital footprints, making it harder for forensic analysts to reconstruct the activities of a user on a system. This deliberate destruction of evidence can impede investigations into criminal activities or misconduct.
4. Automated Cleaning: CCleaner offers automated cleaning features that allow users to schedule regular cleanings of their systems. While this can help improve system performance and free up disk space, it can also automatically remove potentially relevant forensic evidence without the user's knowledge or intent.

18 Question 18

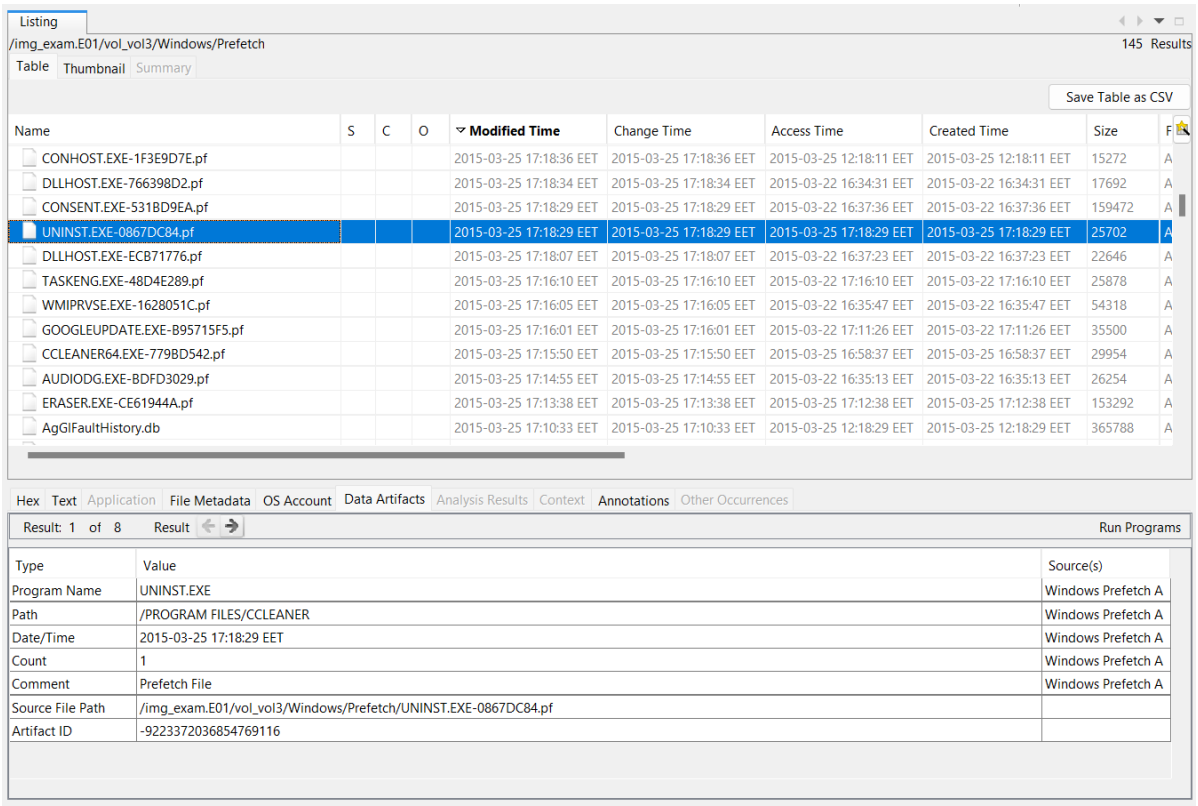
Were these executables executed on the system? How many times? Provide all available evidence.

18.1 Answer

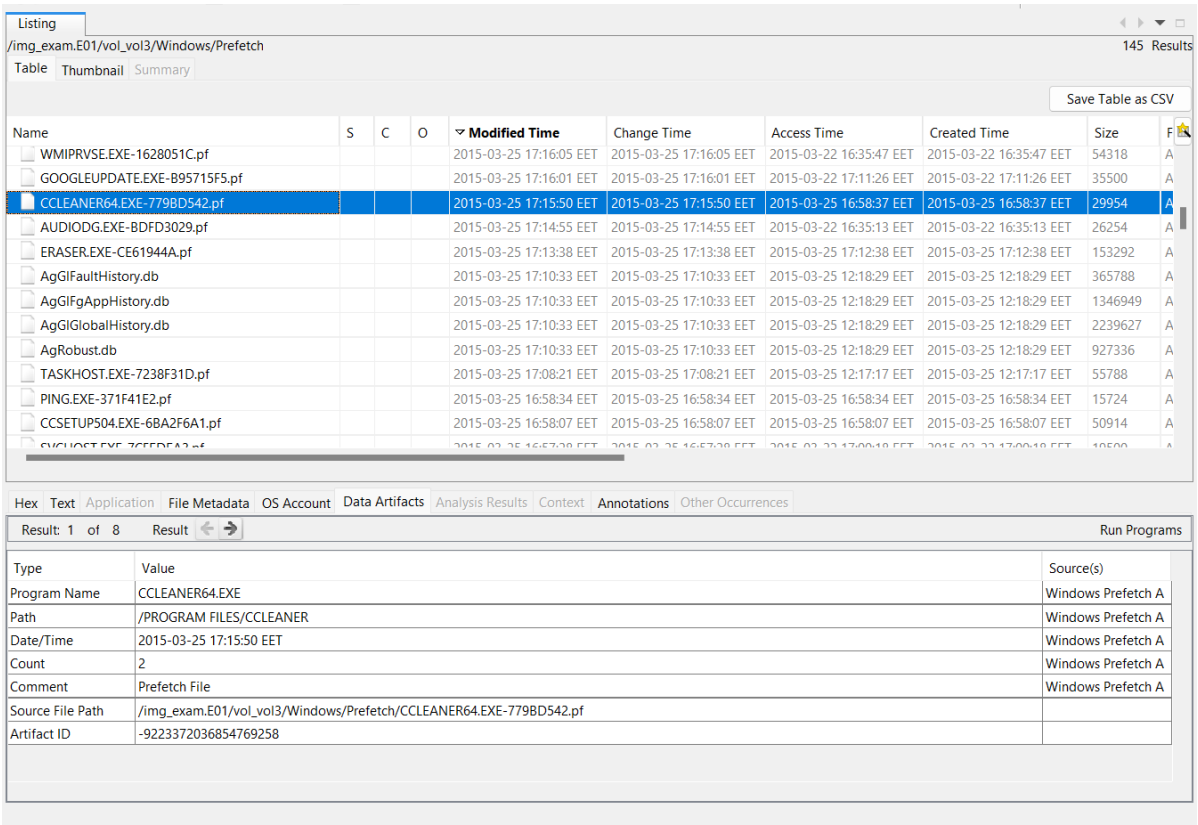
We navigate to Windows/Prefetch and we start looking at *.pf files.

There we can find diagnostic Information. The data stored in prefetch files can provide valuable diagnostic information for system administrators and forensic analysts. Knowing how often an application has been launched can help identify patterns of usage or detect unusual behavior on a system.

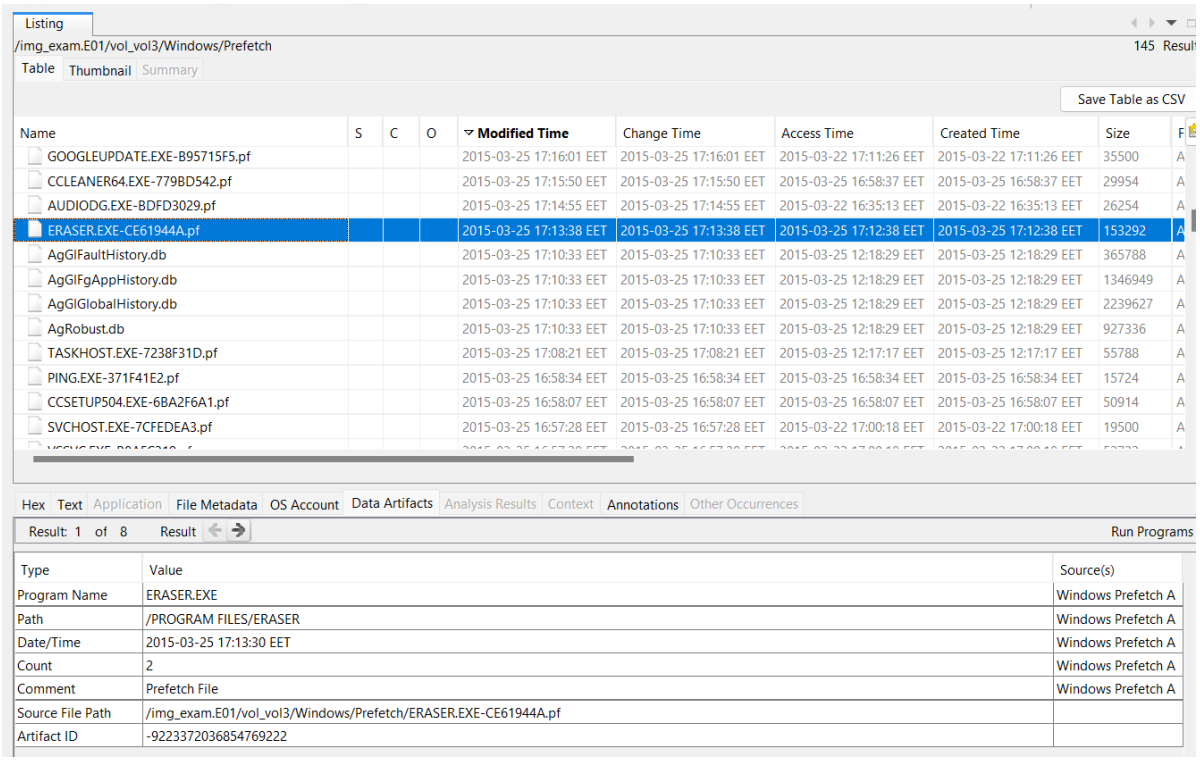
We found that ccleaner program run only once


Listing
/img_exam.E01/vol_vol3/Windows/Prefetch
145 Results
Table Thumbnail Summary
Save Table as CSV
Name S C O Modified Time Change Time Access Time Created Time Size
CONHOST.EXE-1F3E9D7E.pf 2015-03-25 17:18:36 EET 2015-03-25 17:18:36 EET 2015-03-25 12:18:11 EET 2015-03-25 12:18:11 EET 15272
DLLHOST.EXE-766398D2.pf 2015-03-25 17:18:34 EET 2015-03-25 17:18:34 EET 2015-03-22 16:34:31 EET 2015-03-22 16:34:31 EET 17692
CONSENT.EXE-531BD9EA.pf 2015-03-25 17:18:29 EET 2015-03-25 17:18:29 EET 2015-03-22 16:37:36 EET 2015-03-22 16:37:36 EET 159472
UNINST.EXE-0867DC84.pf 2015-03-25 17:18:29 EET 2015-03-25 17:18:29 EET 2015-03-25 17:18:29 EET 2015-03-25 17:18:29 EET 25702
DLLHOST.EXE-ECB71776.pf 2015-03-25 17:18:07 EET 2015-03-25 17:18:07 EET 2015-03-22 16:37:23 EET 2015-03-22 16:37:23 EET 22646
TASKENG.EXE-48D4E289.pf 2015-03-25 17:16:10 EET 2015-03-25 17:16:10 EET 2015-03-22 17:16:10 EET 2015-03-22 17:16:10 EET 25878
WMIPRVSE.EXE-1628051C.pf 2015-03-25 17:16:05 EET 2015-03-25 17:16:05 EET 2015-03-22 16:35:47 EET 2015-03-22 16:35:47 EET 54318
GOOGLEUPDATE.EXE-B95715F5.pf 2015-03-25 17:16:01 EET 2015-03-25 17:16:01 EET 2015-03-22 17:11:26 EET 2015-03-22 17:11:26 EET 35500
CCLEANER64.EXE-779BD542.pf 2015-03-25 17:15:50 EET 2015-03-25 17:15:50 EET 2015-03-25 16:58:37 EET 2015-03-25 16:58:37 EET 29954
AUDIODG.EXE-BDFD3029.pf 2015-03-25 17:14:55 EET 2015-03-25 17:14:55 EET 2015-03-22 16:35:13 EET 2015-03-22 16:35:13 EET 26254
ERASER.EXE-CE61944A.pf 2015-03-25 17:13:38 EET 2015-03-25 17:13:38 EET 2015-03-25 17:12:38 EET 2015-03-25 17:12:38 EET 153292
AgGlFaultHistory.db 2015-03-25 17:10:33 EET 2015-03-25 17:10:33 EET 2015-03-25 12:18:29 EET 2015-03-25 12:18:29 EET 365788
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Result: 1 of 8 Result
Run Programs
Type Value Source(s)
Program Name UNINST.EXE Windows Prefetch A
Path /PROGRAM FILES/CCLEANER Windows Prefetch A
Date/Time 2015-03-25 17:18:29 EET Windows Prefetch A
Count 1 Windows Prefetch A
Comment Prefetch File Windows Prefetch A
Source File Path /img_exam.E01/vol_vol3/Windows/Prefetch/UNINST.EXE-0867DC84.pf
Artifact ID -9223372036854769116

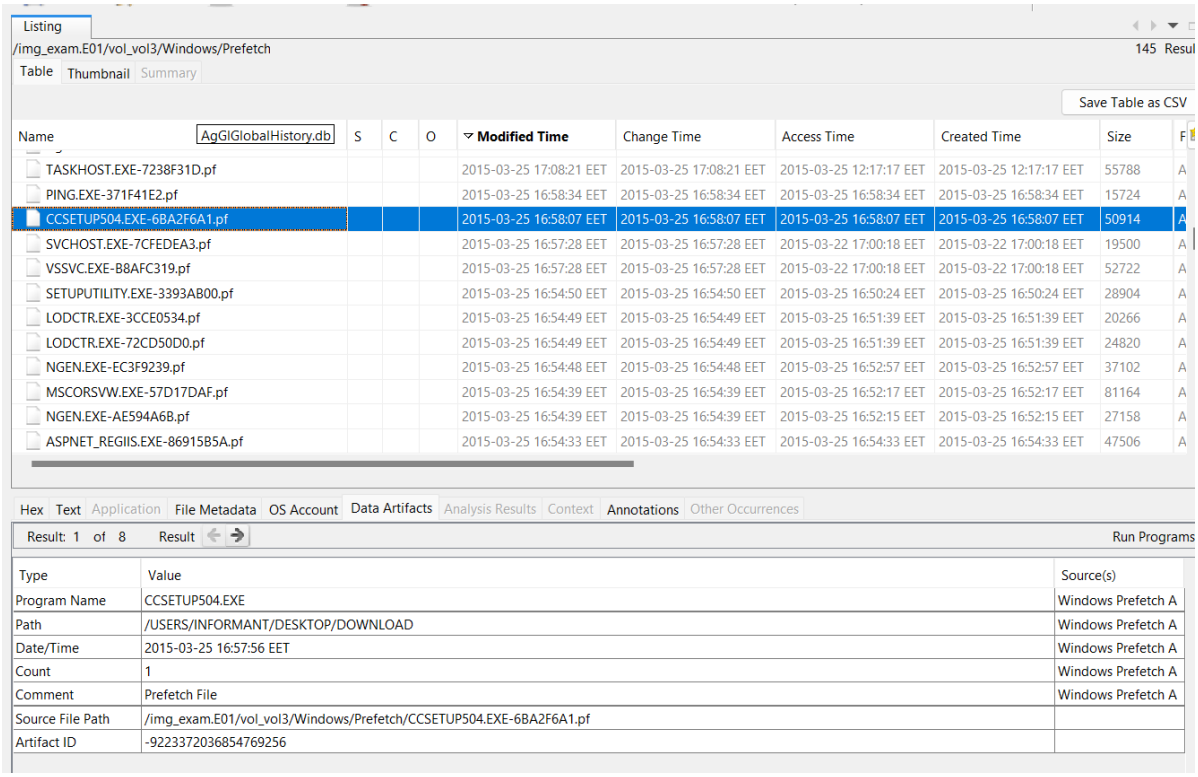
Then twice


Listing
/img_exam.E01/vol_vol3/Windows/Prefetch
145 Results
Table Thumbnail Summary
Save Table as CSV
Name S C O Modified Time Change Time Access Time Created Time Size
WMIPRVSE.EXE-1628051C.pf 2015-03-25 17:16:05 EET 2015-03-25 17:16:05 EET 2015-03-22 16:35:47 EET 2015-03-22 16:35:47 EET 54318
GOOGLEUPDATE.EXE-B95715F5.pf 2015-03-25 17:16:01 EET 2015-03-25 17:16:01 EET 2015-03-22 17:11:26 EET 2015-03-22 17:11:26 EET 35500
CCLEANER64.EXE-779BD542.pf 2015-03-25 17:15:50 EET 2015-03-25 17:15:50 EET 2015-03-25 16:58:37 EET 2015-03-25 16:58:37 EET 29954
AUDIODG.EXE-BDFD3029.pf 2015-03-25 17:14:55 EET 2015-03-25 17:14:55 EET 2015-03-22 16:35:13 EET 2015-03-22 16:35:13 EET 26254
ERASER.EXE-CE61944A.pf 2015-03-25 17:13:38 EET 2015-03-25 17:13:38 EET 2015-03-25 17:12:38 EET 2015-03-25 17:12:38 EET 153292
AgGlFaultHistory.db 2015-03-25 17:10:33 EET 2015-03-25 17:10:33 EET 2015-03-25 12:18:29 EET 2015-03-25 12:18:29 EET 365788
AgGlFgAppHistory.db 2015-03-25 17:10:33 EET 2015-03-25 17:10:33 EET 2015-03-25 12:18:29 EET 2015-03-25 12:18:29 EET 1346949
AgGlGlobalHistory.db 2015-03-25 17:10:33 EET 2015-03-25 17:10:33 EET 2015-03-25 12:18:29 EET 2015-03-25 12:18:29 EET 2239627
AgRobust.db 2015-03-25 17:10:33 EET 2015-03-25 17:10:33 EET 2015-03-25 12:18:29 EET 2015-03-25 12:18:29 EET 927336
TASKHOST.EXE-7238F31D.pf 2015-03-25 17:08:21 EET 2015-03-25 17:08:21 EET 2015-03-25 12:17:17 EET 2015-03-25 12:17:17 EET 55788
PING.EXE-371F41E2.pf 2015-03-25 16:58:34 EET 2015-03-25 16:58:34 EET 2015-03-25 16:58:34 EET 2015-03-25 16:58:34 EET 15724
CCSETUP504.EXE-6BA2F6A1.pf 2015-03-25 16:58:07 EET 2015-03-25 16:58:07 EET 2015-03-25 16:58:07 EET 2015-03-25 16:58:07 EET 50914
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Result: 1 of 8 Result
Run Programs
Type Value Source(s)
Program Name CCLEANER64.EXE Windows Prefetch A
Path /PROGRAM FILES/CCLEANER Windows Prefetch A
Date/Time 2015-03-25 17:15:50 EET Windows Prefetch A
Count 2 Windows Prefetch A
Comment Prefetch File Windows Prefetch A
Source File Path /img_exam.E01/vol_vol3/Windows/Prefetch/CCLEANER64.EXE-779BD542.pf
Artifact ID -9223372036854769258

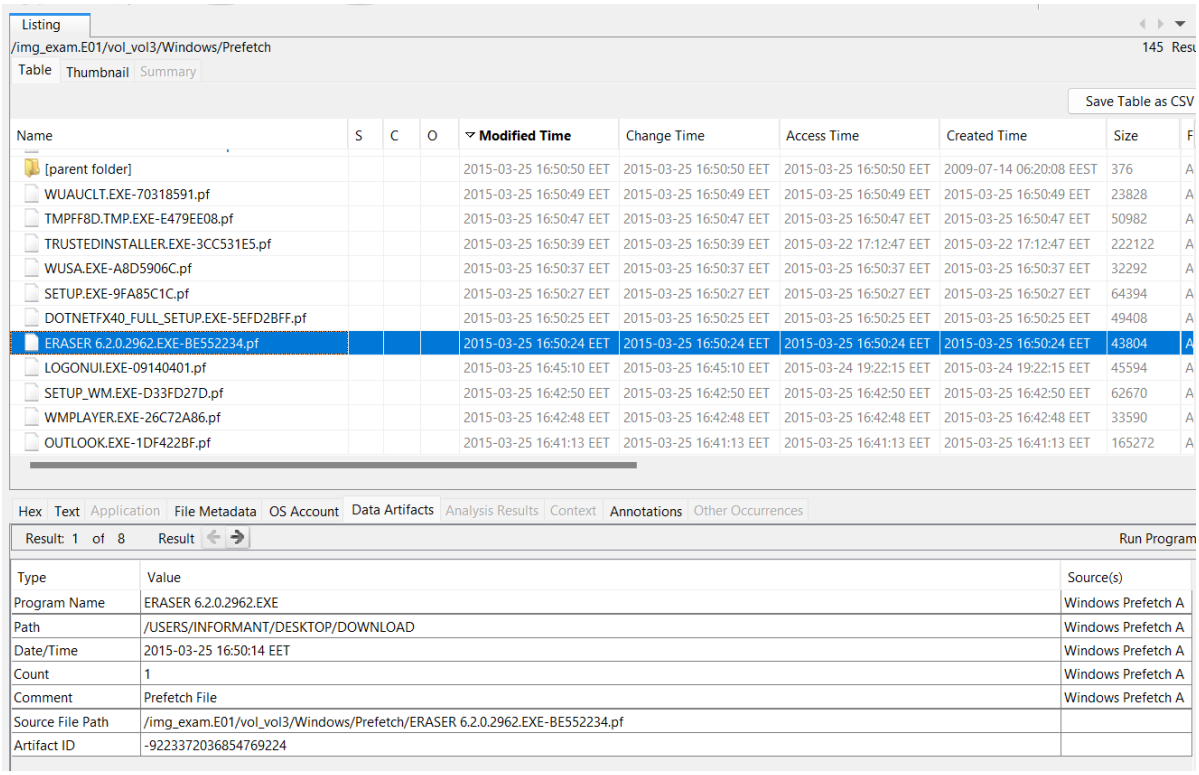
Eraser
twice



Ccleaner setup only once


Listing
/img_exam.E01/vol_vol3/Windows/Prefetch
145 Resul
Table Thumbnail Summary
Save Table as CSV
Name AgGlGlobalHistory.db S C O Modified Time Change Time Access Time Created Time Size F
TASKHOST.EXE-7238F31D.pf 2015-03-25 17:08:21 EET 2015-03-25 17:08:21 EET 2015-03-25 12:17:17 EET 2015-03-25 12:17:17 EET 55788 A
PING.EXE-371F41E2.pf 2015-03-25 16:58:34 EET 2015-03-25 16:58:34 EET 2015-03-25 16:58:34 EET 2015-03-25 16:58:34 EET 15724 A
CCSETUP504.EXE-6BA2F6A1.pf 2015-03-25 16:58:07 EET 2015-03-25 16:58:07 EET 2015-03-25 16:58:07 EET 2015-03-25 16:58:07 EET 50914 A
SVCHOST.EXE-7CFEDEA3.pf 2015-03-25 16:57:28 EET 2015-03-25 16:57:28 EET 2015-03-22 17:00:18 EET 2015-03-22 17:00:18 EET 19500 A
VSSVC.EXE-B8AFC319.pf 2015-03-25 16:57:28 EET 2015-03-25 16:57:28 EET 2015-03-22 17:00:18 EET 2015-03-22 17:00:18 EET 52722 A
SETUPUTILITY.EXE-3393AB00.pf 2015-03-25 16:54:50 EET 2015-03-25 16:54:50 EET 2015-03-25 16:50:24 EET 2015-03-25 16:50:24 EET 28904 A
LODCTR.EXE-3CCE0534.pf 2015-03-25 16:54:49 EET 2015-03-25 16:54:49 EET 2015-03-25 16:51:39 EET 2015-03-25 16:51:39 EET 20266 A
LODCTR.EXE-72CD50D0.pf 2015-03-25 16:54:49 EET 2015-03-25 16:54:49 EET 2015-03-25 16:51:39 EET 2015-03-25 16:51:39 EET 24820 A
NGEN.EXE-EC3F9239.pf 2015-03-25 16:54:48 EET 2015-03-25 16:54:48 EET 2015-03-25 16:52:57 EET 2015-03-25 16:52:57 EET 37102 A
MSCORSVW.EXE-57D17DAF.pf 2015-03-25 16:54:39 EET 2015-03-25 16:54:39 EET 2015-03-25 16:52:17 EET 2015-03-25 16:52:17 EET 81164 A
NGEN.EXE-AE594A6B.pf 2015-03-25 16:54:39 EET 2015-03-25 16:54:39 EET 2015-03-25 16:52:15 EET 2015-03-25 16:52:15 EET 27158 A
ASPNET_REGIIS.EXE-86915B5A.pf 2015-03-25 16:54:33 EET 2015-03-25 16:54:33 EET 2015-03-25 16:54:33 EET 2015-03-25 16:54:33 EET 47506 A
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Result: 1 of 8 Result
Run Programs
Type Value Source(s)
Program Name CCSETUP504.EXE Windows Prefetch A
Path /USERS/INFORMANT/DESKTOP/DOWNLOAD Windows Prefetch A
Date/Time 2015-03-25 16:57:56 EET Windows Prefetch A
Count 1 Windows Prefetch A
Comment Prefetch File Windows Prefetch A
Source File Path /img_exam.E01/vol_vol3/Windows/Prefetch/CCSETUP504.EXE-6BA2F6A1.pf
Artifact ID -9223372036854769256

Eraser once

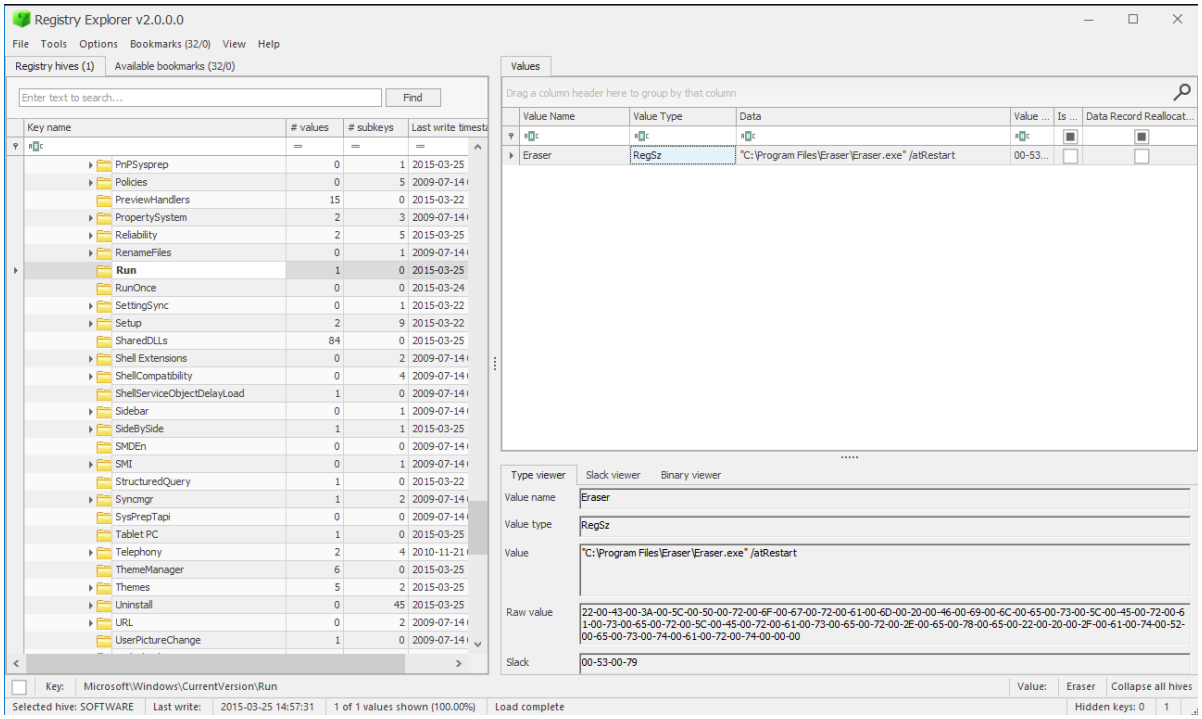

Listing
/img_exam.E01/vol_vol3/Windows/Prefetch
145 Resu
Table Thumbnail Summary
Save Table as CSV
Name S C O Modified Time Change Time Access Time Created Time Size F
[parent folder] 2015-03-25 16:50:50 EET 2015-03-25 16:50:50 EET 2015-03-25 16:50:50 EET 2009-07-14 06:20:08 EEST 376 A
WUAUCLT.EXE-70318591.pf 2015-03-25 16:50:49 EET 2015-03-25 16:50:49 EET 2015-03-25 16:50:49 EET 2015-03-25 16:50:49 EET 23828 A
TMPFF8D.TMP.EXE-E479EE08.pf 2015-03-25 16:50:47 EET 2015-03-25 16:50:47 EET 2015-03-25 16:50:47 EET 2015-03-25 16:50:47 EET 50982 A
TRUSTEDINSTALLER.EXE-3CC531E5.pf 2015-03-25 16:50:39 EET 2015-03-25 16:50:39 EET 2015-03-22 17:12:47 EET 2015-03-22 17:12:47 EET 222122 A
WUSA.EXE-A8D5906C.pf 2015-03-25 16:50:37 EET 2015-03-25 16:50:37 EET 2015-03-25 16:50:37 EET 2015-03-25 16:50:37 EET 32292 A
SETUP.EXE-9FA85C1C.pf 2015-03-25 16:50:27 EET 2015-03-25 16:50:27 EET 2015-03-25 16:50:27 EET 2015-03-25 16:50:27 EET 64394 A
DOTNETFX40_FULL_SETUP.EXE-5EFD2BFF.pf 2015-03-25 16:50:25 EET 2015-03-25 16:50:25 EET 2015-03-25 16:50:25 EET 2015-03-25 16:50:25 EET 49408 A
ERASER 6.2.0.2962.EXE-BE552234.pf 2015-03-25 16:50:24 EET 2015-03-25 16:50:24 EET 2015-03-25 16:50:24 EET 2015-03-25 16:50:24 EET 43804 A
LOGONUI.EXE-09140401.pf 2015-03-25 16:45:10 EET 2015-03-25 16:45:10 EET 2015-03-24 19:22:15 EET 2015-03-24 19:22:15 EET 45594 A
SETUP_WM.EXE-D33FD27D.pf 2015-03-25 16:42:50 EET 2015-03-25 16:42:50 EET 2015-03-25 16:42:50 EET 2015-03-25 16:42:50 EET 62670 A
WMPLAYER.EXE-26C72A86.pf 2015-03-25 16:42:48 EET 2015-03-25 16:42:48 EET 2015-03-25 16:42:48 EET 2015-03-25 16:42:48 EET 33590 A
OUTLOOK.EXE-1DF422BF.pf 2015-03-25 16:41:13 EET 2015-03-25 16:41:13 EET 2015-03-25 16:41:13 EET 2015-03-25 16:41:13 EET 165272 A
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Result: 1 of 8 Result
Run Program
Type Value Source(s)
Program Name ERASER 6.2.0.2962.EXE Windows Prefetch A
Path /USERS/INFORMANT/DESKTOP/DOWNLOAD Windows Prefetch A
Date/Time 2015-03-25 16:50:14 EET Windows Prefetch A
Count 1 Windows Prefetch A
Comment Prefetch File Windows Prefetch A
Source File Path /img_exam.E01/vol_vol3/Windows/Prefetch/ERASER 6.2.0.2962.EXE-BE552234.pf
Artifact ID -9223372036854769224

19 Question 19

Check the suspect users' autoruns. What suspicious executable can you find? What did he intend to do?

19.1 Answer

Upon investigating the suspect users' autoruns, we discovered the suspicious executable named "eraser.exe" in the registry run folder. It appears that the suspect intended to prevent the execution of this program on every system, implying a deliberate attempt to conceal its activities.

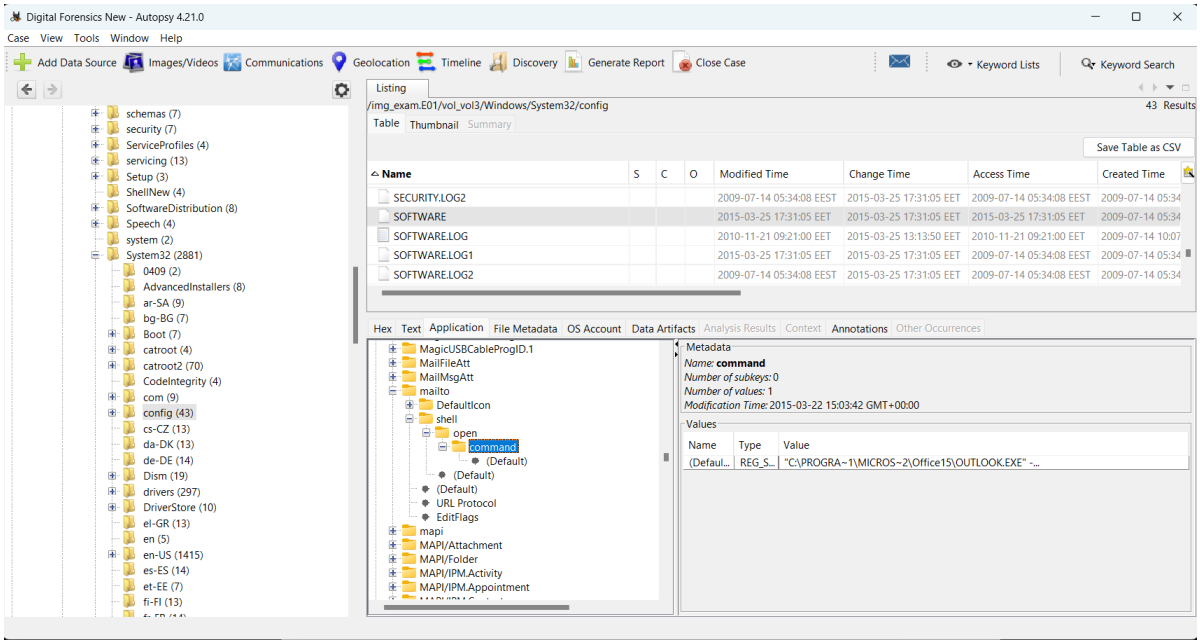


20 Question 20

What e-mail account did the suspect user use? How did the suspect user exfiltrate information to “spy”??

20.1 Answer

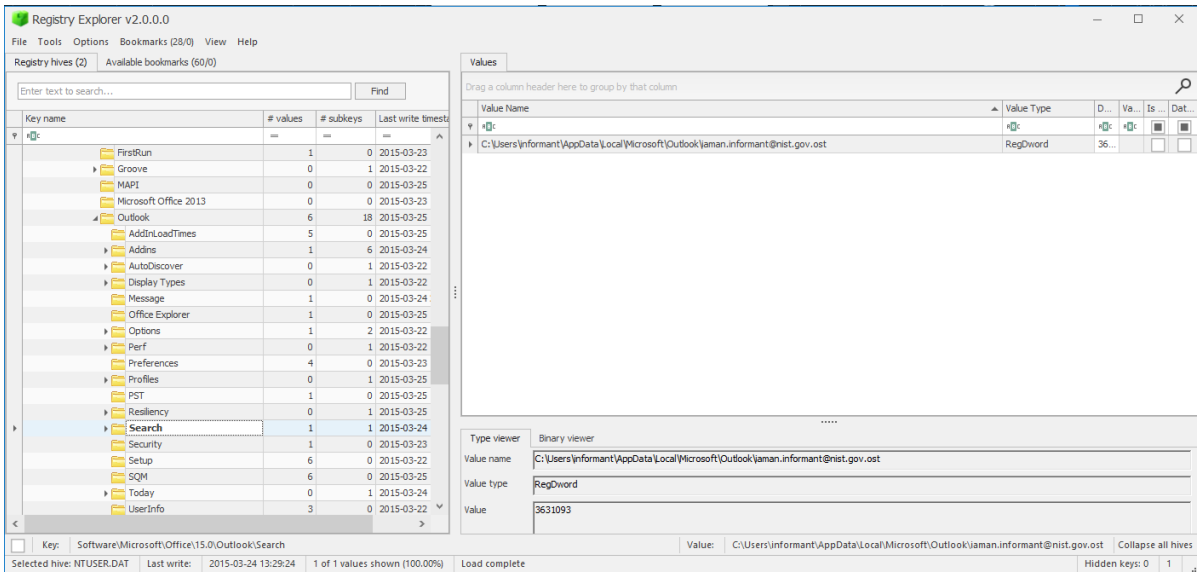
Firstly, we navigate to HKLM\SOFTWARE\Classes\mailto\shell\open\command to see the application was used for e-mail communication



From the values table we can see that the application that was used was outlook.exe

So, where is the e-mail that was user located?

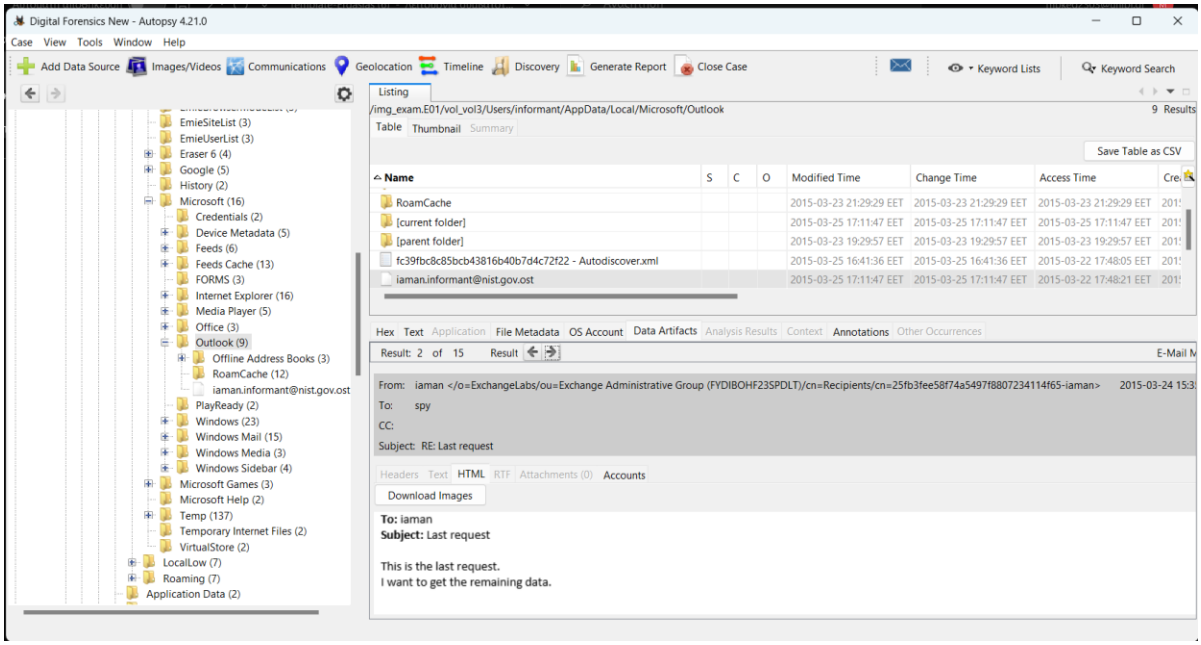
We navigate again to NTUSER file and we open it with Registry Explorer. Then we navigate to Software\Microsoft\Office\15.0\Outlook\Search



Here we can see that the email that was used was iaman.informant@nist.gov.ost

Let's find the contents of the email convertations of informant (suspect user)

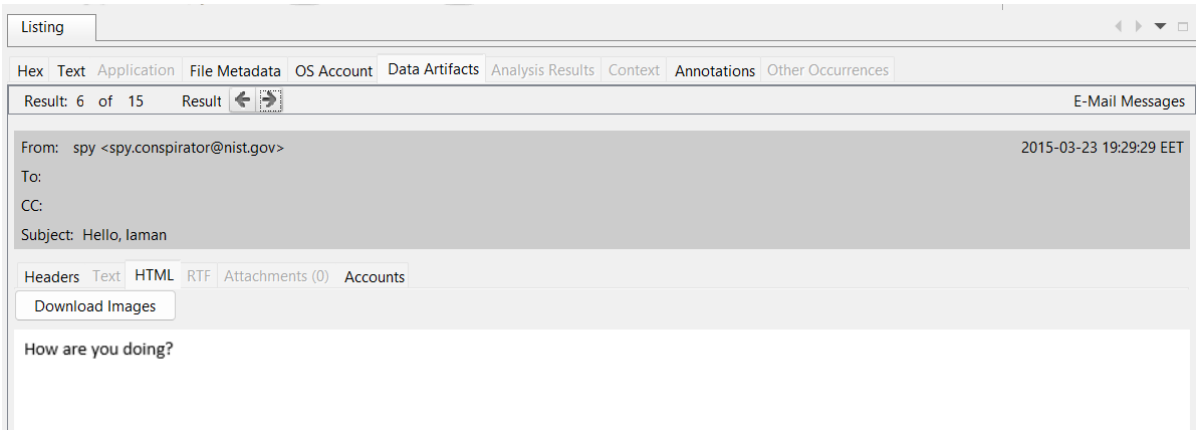
We navigate to vol3/Users/informant/Appdata/local/Microsoft/Outlook and we find the .ost file.



Now, we can view the contents of the emails on the HTML or we can export the .ost file and preview it on a .ost viewer application.

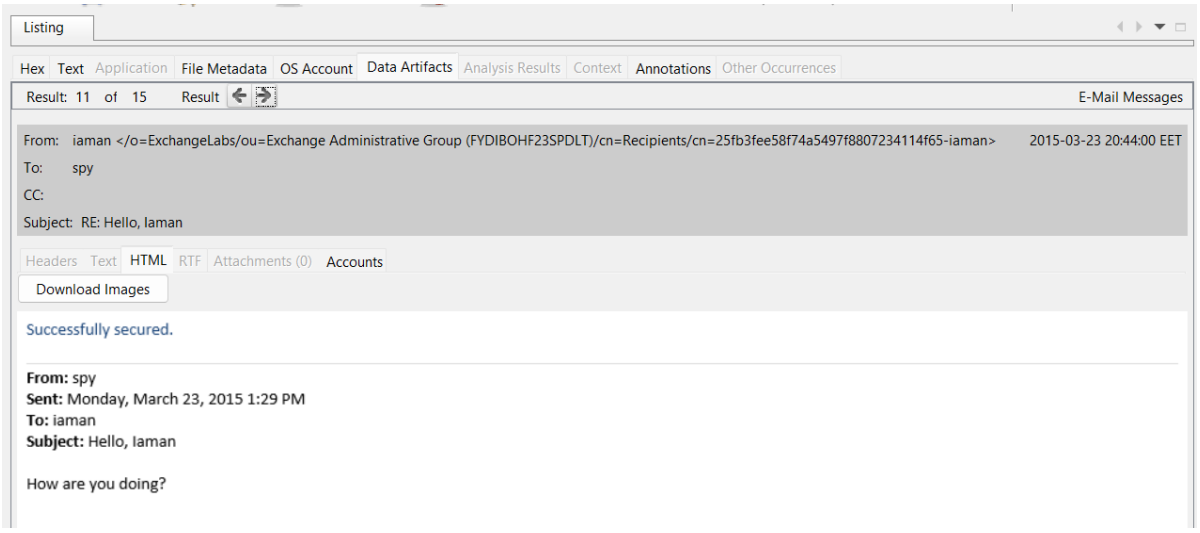
1. Initial Contact (March 23, 2015):

Spy initiates contact with iaman, asking how they are doing.



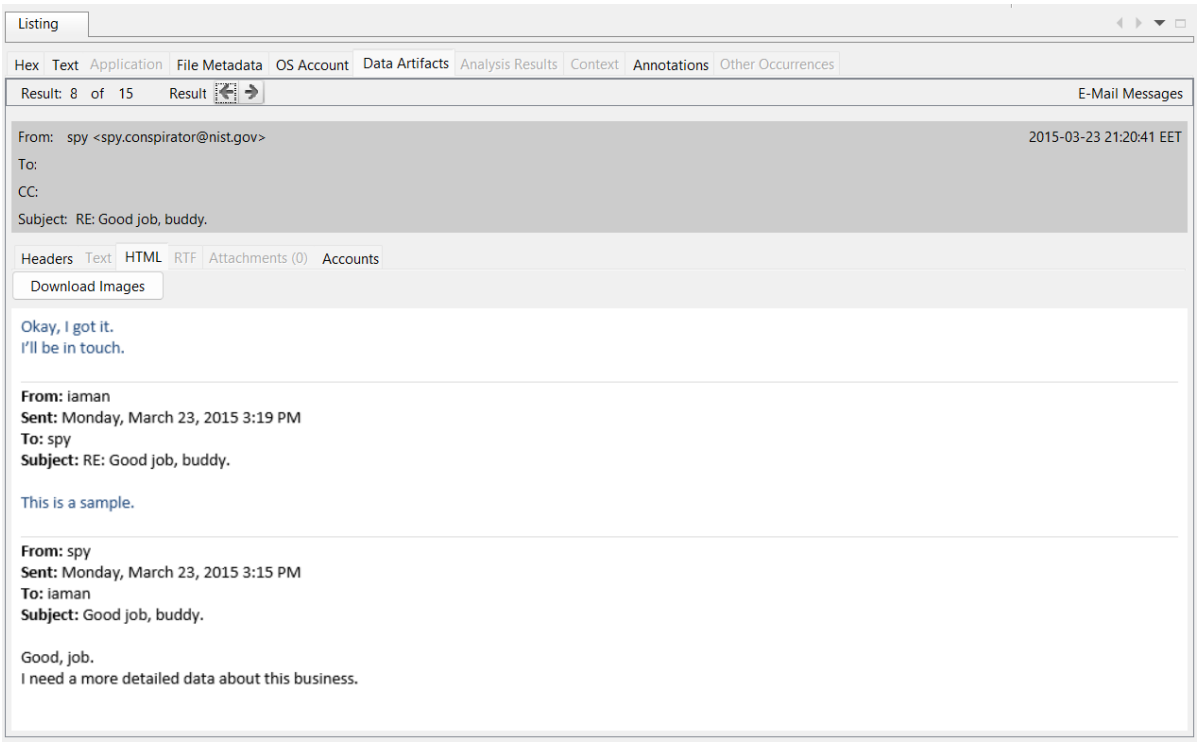
2. Acknowledgment of Success (March 23, 2015):

Iaman responds, confirming successful completion of a task.



3. Request for Detailed Data (March 23, 2015):

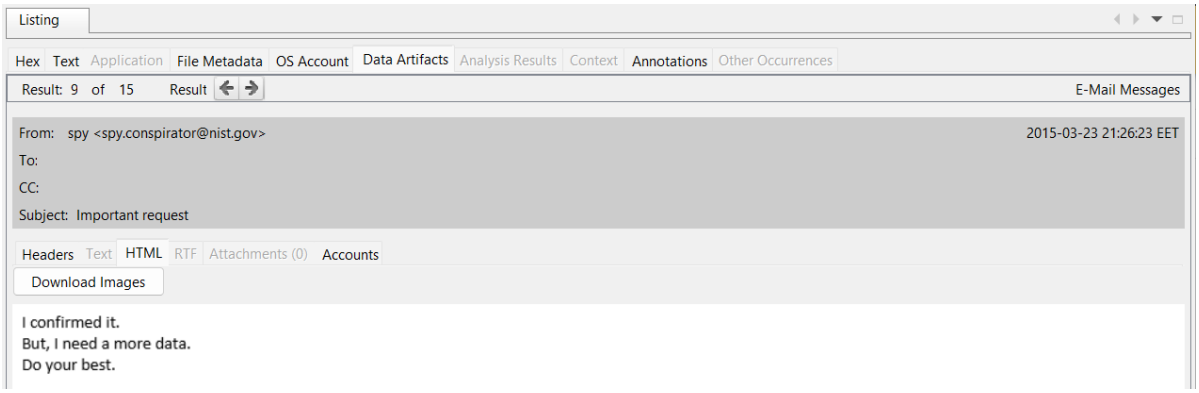
Spy acknowledges the success but requests more detailed data about the business.

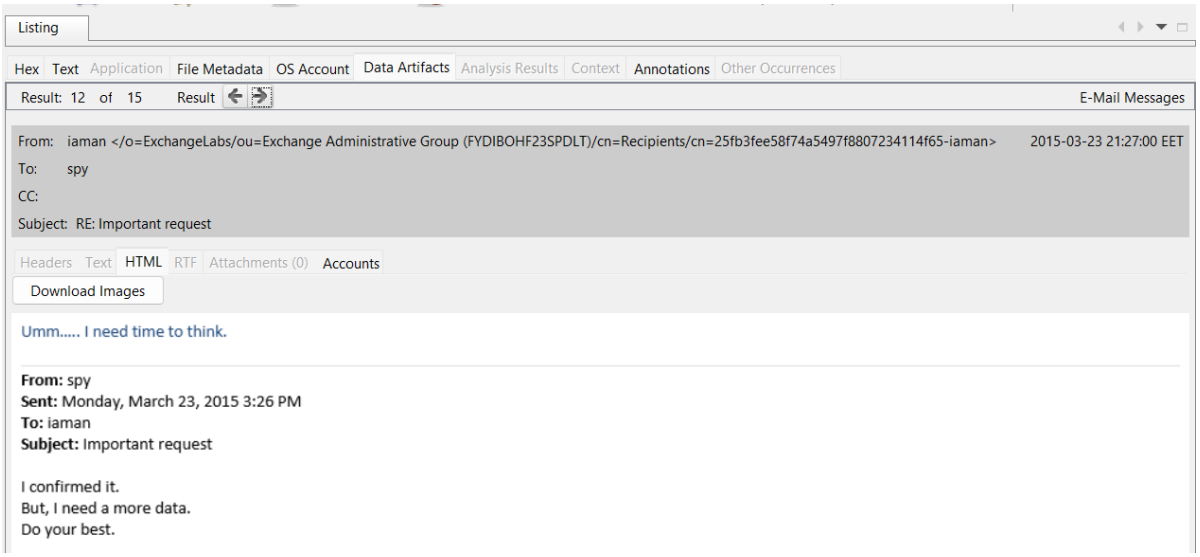


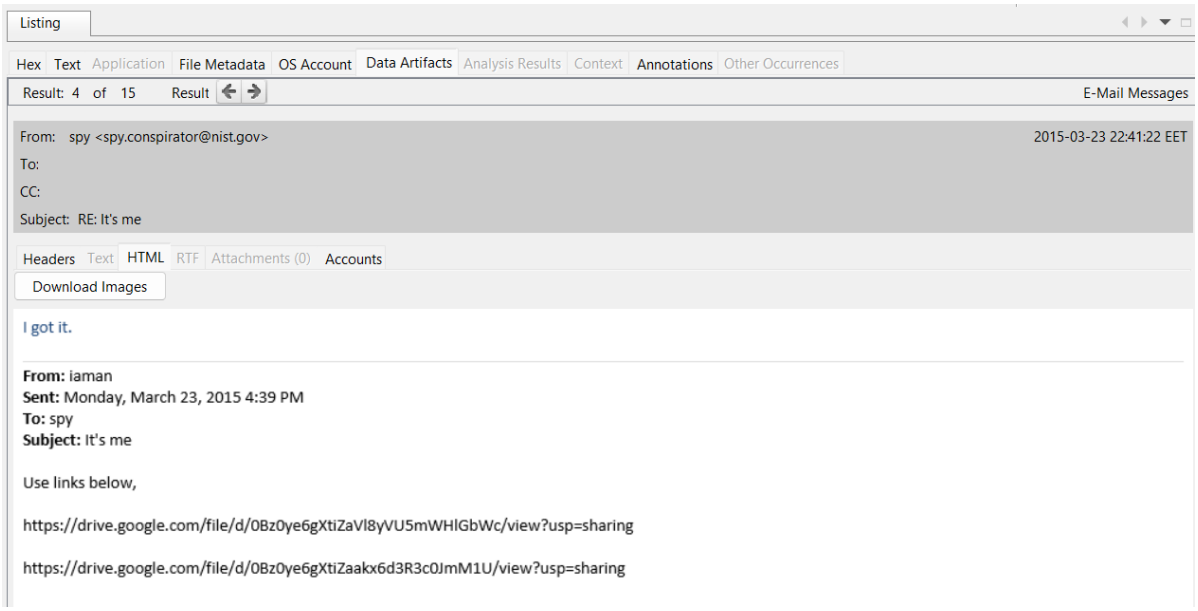
4. Further Communication (March 23, 2015):

Spy sends another message reiterating the need for detailed data.

Iaman responds, indicating that they will provide more detailed data.

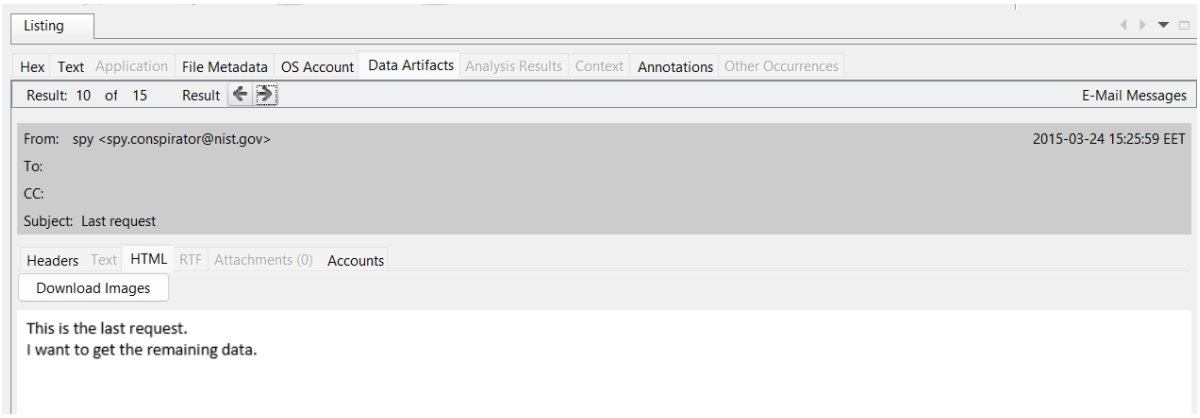



Listing
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Result: 12 of 15 Result
E-Mail Messages
From: iaman </o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=25fb3fee58f74a5497f8807234114f65-iaman> 2015-03-23 21:27:00 EET
To: spy
CC:
Subject: RE: Important request
Headers Text HTML RTF Attachments (0) Accounts
Download Images
Umm..... I need time to think.
From: spy
Sent: Monday, March 23, 2015 3:26 PM
To: iaman
Subject: Important request
I confirmed it.
But, I need a more data.
Do your best.


Listing
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Result: 4 of 15 Result
E-Mail Messages
From: spy <spy.conspirator@nist.gov> 2015-03-23 22:41:22 EET
To:
CC:
Subject: RE: It's me
Headers Text HTML RTF Attachments (0) Accounts
Download Images
I got it.
From: iaman
Sent: Monday, March 23, 2015 4:39 PM
To: spy
Subject: It's me
Use links below,
https://drive.google.com/file/d/0Bz0ye6gXtiZaVl8yVU5mWHlGbWc/view?usp=sharing
https://drive.google.com/file/d/0Bz0ye6gXtiZaakx6d3R3c0JmM1U/view?usp=sharing

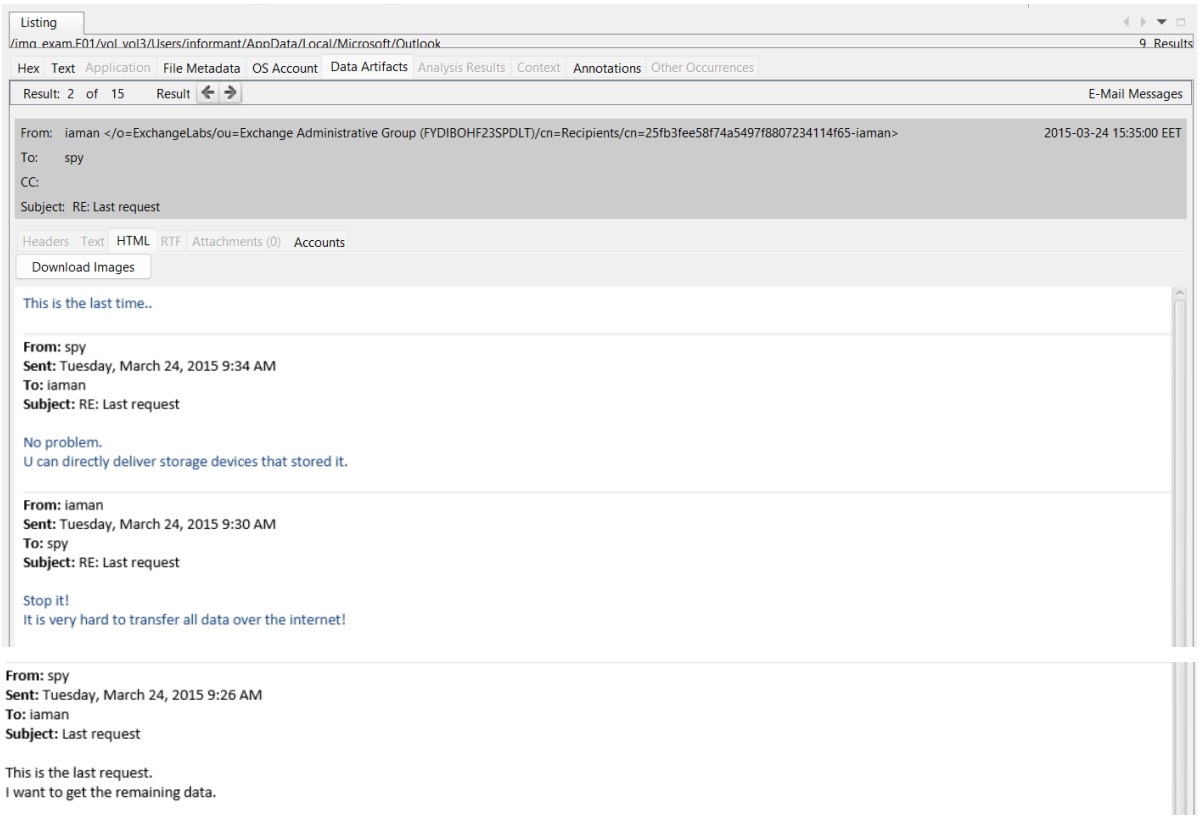
5. Last Request (March 24, 2015):

Spy sends a message indicating that this is the last request for remaining data.



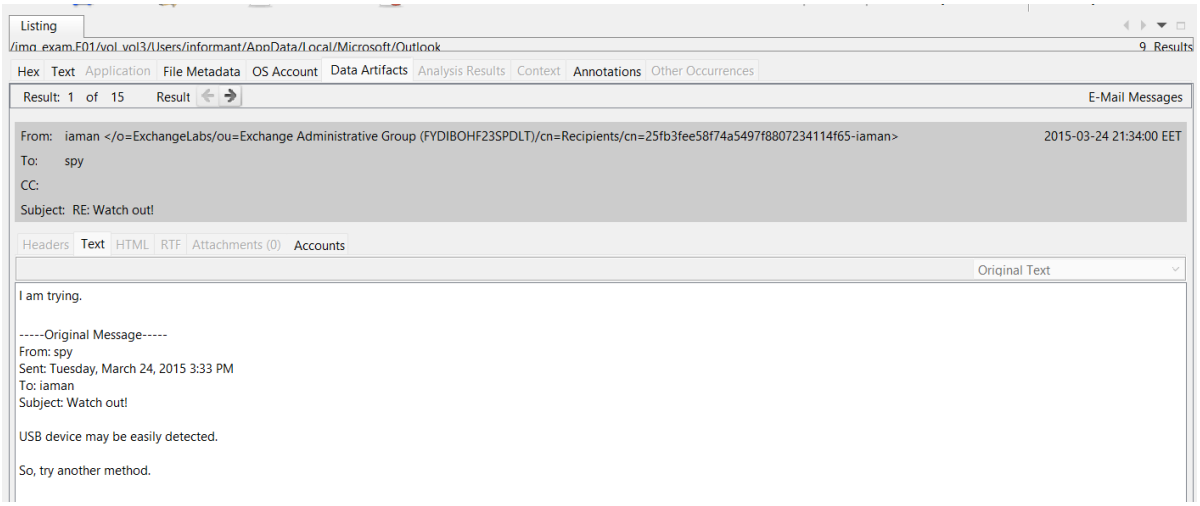
6. Discussion on Data Transfer (March 24, 2015):

Spy suggests transferring data via storage devices.Iaman expresses difficulty with transferring all data over the internet.



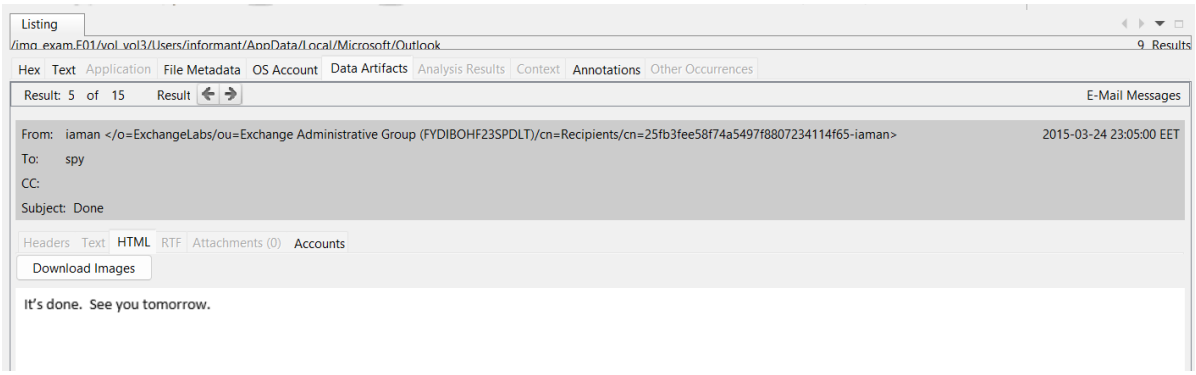
7. Warning (March 24, 2015):

Spy warns iaman about potential detection of USB devices and suggests using another method.



8. Confirmation of Completion (March 24, 2015):

Iaman confirms that the task is completed and mentions seeing spy the next day.



Initially, "spy" emails "iaman," inquiring about their well-being. It seems quite informal, like if they are already close friends or something. "iaman" then answers, stating that they have completed a task satisfactorily. It appears that "iaman" may be offering "spy" assistance in the form of information or updates.

Subsequently, "spy" requests further information regarding the project they are working on. It appears like the information being given is significant for whatever project they are working on. "Spy" repeatedly asks for more details, giving the impression that they're pressed for time or require more details.

"iaman" answers, stating that they're having some issues uploading all the info online, possibly due to the fact that it's too dangerous. Instead, "Spy" recommends transferring the data via storage devices, although "iaman" isn't too fond of the notion.

But eventually, "iaman" says they've completed the assignment and says they'll see "spy" tomorrow. Thus, it appears that they are moving forward, despite certain obstacles in their path.

All things considered, Your Honor, the correspondence presents an image of two people engaged in some rather covert actions, such as espionage or handling confidential information. They are demonstrating that they are aware of the hazards associated with what they are doing by being circumspect in their speech and attempting to avoid being discovered.

21 Βιβλιογραφικές Πηγές

1. **Carvey, Harlan**. "Memory Forensics: An Analysis of Windows Hibernation Files." In Advances in Digital Forensics XII, pp. 229-242. Springer, Cham, 2016.
2. **Dolan-Gavitt, Brendan**, "Forensic Analysis of Windows Hibernation Files." Digital Investigation 10, no. 4 (2013): 318-332.
3. **Sachdeva, Monika**, "Memory Analysis in Digital Forensics: Tools, Techniques, and Trends." International Journal of Information Technology and Computer Science 8, no. 5 (2016): 54-60.
4. **Casey, Eoghan**. "Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet." Academic Press, 2011.
5. **Krishnamurthy, Diwakar**. "A Review of Digital Evidence Preservation Techniques." In 2012 Fifth International Conference on Emerging Trends in Engineering and Technology, pp. 892-898. IEEE, 2012.
6. **European Network of Forensic Science Institutes (ENFSI).** "Guidelines on Evidence Collection and Archiving." ENFSI Digital and Multimedia Evidence Working Group, 2015.
7. **National Institute of Justice (NIJ).** "Best Practices for Seizing Electronic Evidence." NIJ Guide, 2008.
8. Forensic Focus (https://www.forensicfocus.com/), Digital Forensics Community (https://www.digitalforensicscommunity.com/), etc.
9. **Altheide, Cory, and Harlan Carvey**. "Digital Forensics with Open Source Tools." Syngress, 2011.
10. **VMware Documentation**. Available online on the VMware website.
11. **SANS Institute**. Available on the SANS website.