

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



Εκφόνηση 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

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ	4
1 Question 1	6
1.1 Answer.....	6
2 Question 2	7
2.1 Answer.....	7
3 Question 3	8
3.1 Answer.....	8
4 Question 4	10
4.1 Answer.....	10
5 Question 5	11
5.1 Answer.....	11
6 Question 6	12
6.1 Answer.....	12
7 Question 7	13
7.1 Answer.....	13
8 Question 7	16
8.1 Answer.....	16
9 Question 9	23
9.1 Answer.....	23
10 Question 10	27
10.1 Answer.....	27
11 Question 11	28
11.1 Answer.....	28
12 Question 12	31
12.1 Answer.....	31
13 Question 13	37
13.1 Answer.....	37



14 Question 14	44
14.1 Answer.....	44
15 Question 15	47
15.1 Answer.....	47
16 Question 16	48
16.1 Answer.....	48
17 Question 17	53
17.1 Answer.....	53
18 Question 18	55
18.1 Answer.....	55
19 Question 19	59
19.1 Answer.....	59
20 Question 20	60
20.1 Answer.....	60
21 Βιβλιογραφικές Πηγές.....	68



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.

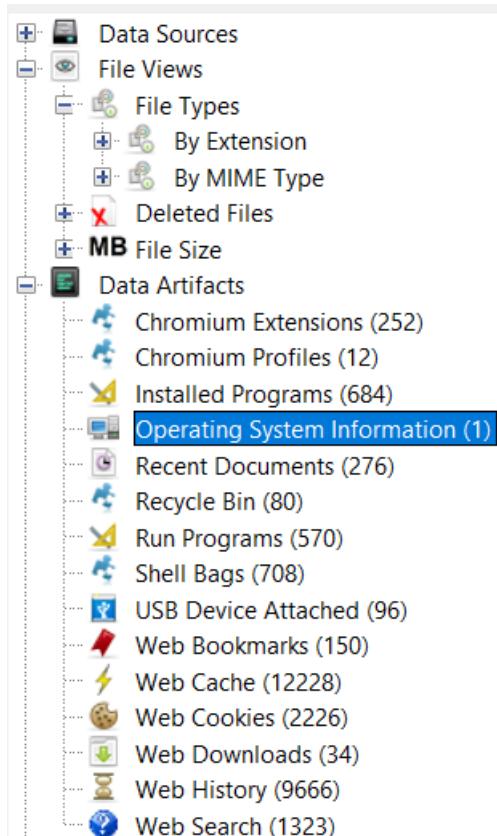


4 Question 4

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



Listing

Operating System Information

1 Results

Table | Thumbnail | Summary | Save Table as CSV

Source Name	S	C	O	Name	Program Name	Processor Architecture	Temporary Files Directory	Path	Product ID
exam.E01				INFORMANT-PC	Windows 7 Ultimate Service Pack 1	AMD64	%SystemRoot%\TEMP	C:\Windows	00426-29

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Type: E01
Size: 21474836480
MD5: a49d1254c873808c58e6f1bcd60b5bde
SHA1: afe5c9ab487bd47a8a9856b1371c2384d44fd785
SHA-256: Not calculated
Sector Size: 512
Time Zone: Europe/Athens
Acquisition Details: Description: cfreds_2015_data_leakage_pc

So the answer 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.

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 1 of 1 Result ← → | Operating System Information

Type	Value	Source(s)
Name	INFORMANT-PC	Recent Activity
Program Name	Windows 7 Ultimate Service Pack 1	Recent Activity
Processor Archit	AMD64	Recent Activity
Temporary Files	%SystemRoot%\TEMP	Recent Activity

So the answer is **INFORMANT-PC**



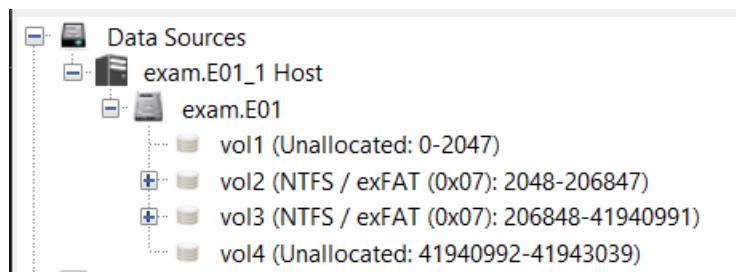
6 Question 6

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
[CURRENT FOLDER]				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	200
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)

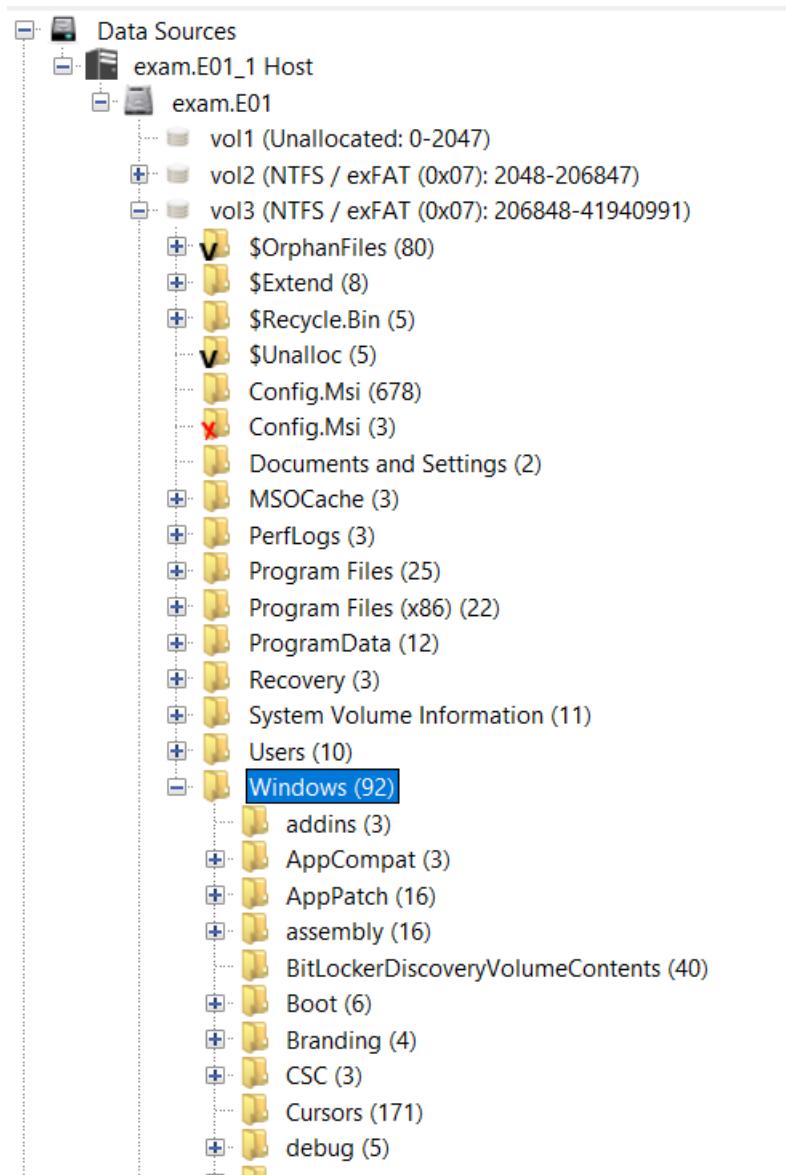
7.1 Answer

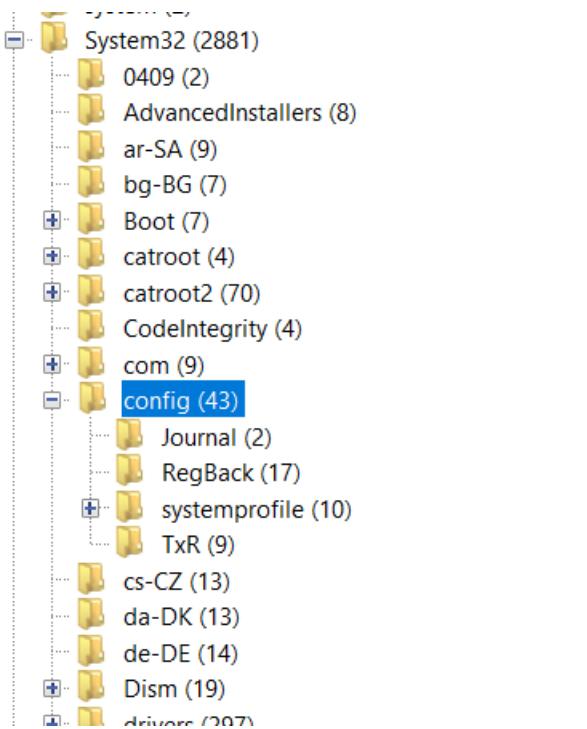
The answer is behind the Windows Registry. (Firstly we checked under the Operating System Information section but we only found the OS version and not the installation date)

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.





Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
SECURITY.LOG				2010-11-21 09:20:59 EET	2015-03-25 13:13:48 EET	2010-11-21 09:20:59 EET	2009-07-14 10:07
SECURITY.LOG1				2015-03-25 17:31:05 EET	2015-03-25 17:31:05 EET	2009-07-14 05:34:08 EEST	2009-07-14 05:34
SECURITY.LOG2				2009-07-14 05:34:08 EEST	2015-03-25 17:31:05 EET	2009-07-14 05:34:08 EEST	2009-07-14 05:34
SOFTWARE				2015-03-25 17:31:05 EET	2015-03-25 17:31:05 EET	2015-03-25 17:31:05 EET	2009-07-14 05:34
SOFTWARE.LOG				2010-11-21 09:21:00 EET	2015-03-25 13:13:50 EET	2010-11-21 09:21:00 EET	2009-07-14 10:07
SOFTWARE.LOG1				2015-03-25 17:31:05 EET	2015-03-25 17:31:05 EET	2009-07-14 05:34:08 EEST	2009-07-14 05:34
SOFTWARE.LOG2				2009-07-14 05:34:08 EEST	2015-03-25 17:31:05 EET	2009-07-14 05:34:08 EEST	2009-07-14 05:34
SYSTEM				2015-03-25 17:31:05 EET	2015-03-25 17:31:05 EET	2015-03-25 17:31:05 EET	2009-07-14 05:34

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



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

Metadata

Name: **CurrentVersion**
Number of subkeys: 73
Number of values: 21
Modification Time: 2015-03-22 15:21:53 GMT+00:00

Name	Type	Value
CurrentVersion	REG_SZ	6.1
CurrentBuild	REG_SZ	7601
SoftwareType	REG_SZ	System
CurrentType	REG_SZ	Multiprocessor Free
InstallDate	REG_DWORD	0x550ed2f2 (1427034866)
RegisteredOrganization	REG_SZ	(value not set)
RegisteredOwner	REG_SZ	informant
SystemRoot	REG_SZ	C:\Windows
InstallationType	REG_SZ	Client
EditionID	REG_SZ	Ultimate
ProductName	REG_SZ	Windows 7 Ultimate
ProductId	REG_SZ	00426-292-0000007-85262
DigitalProductId	REG_BIN	A4 00 00 00 03 00 00 30 30 34 32 36 2D 32 39...
DigitalProductId4	REG_BIN	F8 04 00 00 04 00 00 30 00 30 00 34 00 32 00...
CurrentBuildNumber	REG_SZ	7601
BuildLab	REG_SZ	7601.win7sp1_gdr.130828-1532
BuildLabEx	REG_SZ	7601.18247.amd64fre.win7sp1_gdr.130828-1532
BuildGUID	REG_SZ	cefa1a79-8b62-4cee-a9ff-1c96c94a8e4d
CSDBuildNumber	REG_SZ	1130
PathName	REG_SZ	C:\Windows
CSDVersion	REG_SZ	Service Pack 1

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
 - + **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)**
 - * 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-1-5-80-2620923248-4247863784-3378508180-2E			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:

Name	S	C	O	Login Name	Host	Scope	Realm Name
S-1-5-18				SYSTEM	exam.E01_1 Host	Local	NT AUTHORITY
S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464			0		exam.E01_1 Host	Local	NT SERVICE
S-1-5-21-2425377081-3129163575-2985601102-1001			0	admin11	exam.E01_1 Host	Domain	
S-1-5-21-2425377081-3129163575-2985601102-1000			0	informant	exam.E01_1 Host	Domain	
S-1-5-21-2425377081-3129163575-2985601102-1003			0	temporary	exam.E01_1 Host	Domain	
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-1-5-80-2620923248-4247863784-3378508180-2659151310-2535246811			0		exam.E01_1 Host	Local	NT SERVICE
S-1-5-21-2425377081-3129163575-2985601102-1002			0	ITechTeam	exam.E01_1 Host	Domain	
S-1-5-21-2425377081-3129163575-2985601102-500			0	Administrator	exam.E01_1 Host	Domain	
S-1-5-21-2425377081-3129163575-2985601102-501			0	Guest	exam.E01_1 Host	Domain	

exam.E01_1 Host Details

Last Login: 2015-03-22 17:57:02 EET
Login Count: 2
Administrator: True
Password Fail Date: 2015-03-22 17:53:02 EET
Password Settings: Password does not expire
Flag: Normal user account
Last Login: 2015-03-22 17:57:02 EET



Here are the relevant entries with their logon times:

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

Name	S	C	O	Login Name	Host	Scope	Realm Name
S-1-5-18				SYSTEM	exam.E01_1 Host	Local	NT AUTHORITY
S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464		0			exam.E01_1 Host	Local	NT SERVICE
S-1-5-21-2425377081-3129163575-2985601102-1001		0		admin11	exam.E01_1 Host	Domain	
S-1-5-21-2425377081-3129163575-2985601102-1000			0	informant	exam.E01_1 Host	Domain	
S-1-5-21-2425377081-3129163575-2985601102-1003		0		temporary	exam.E01_1 Host	Domain	
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-1-5-80-2620923248-4247863784-3378508180-2659151310-2535246811		0			exam.E01_1 Host	Local	NT SERVICE
S-1-5-21-2425377081-3129163575-2985601102-1002		0		ITechTeam	exam.E01_1 Host	Domain	
S-1-5-21-2425377081-3129163575-2985601102-500		0		Administrator	exam.E01_1 Host	Domain	
S-1-5-21-2425377081-3129163575-2985601102-501		0		Guest	exam.E01_1 Host	Domain	

exam.E01_1 Host Details

Last Login:	2015-03-25 15:06:08 EET
Login Count:	9
Administrator:	True
Password Hint:	IAMAN
Password Fail Date:	2015-03-22 17:57:48 EET
Password Settings:	Password does not expire, Password not required
Flag:	Normal user account

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



Name	S	C	O	Login Name	Host	Scope	Realm Name
S-1-5-18				SYSTEM	exam.E01_1 Host	Local	NT AUTHORITY
S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464		0			exam.E01_1 Host	Local	NT SERVICE
S-1-5-21-2425377081-3129163575-2985601102-1001		0		admin11	exam.E01_1 Host	Domain	
S-1-5-21-2425377081-3129163575-2985601102-1000		0		informant	exam.E01_1 Host	Domain	
S-1-5-21-2425377081-3129163575-2985601102-1003		0		temporary	exam.E01_1 Host	Domain	
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-1-5-80-2620923248-4247863784-3378508180-2659151310-2535246811		0			exam.E01_1 Host	Local	NT SERVICE
S-1-5-21-2425377081-3129163575-2985601102-1002		0		ITechTeam	exam.E01_1 Host	Domain	
S-1-5-21-2425377081-3129163575-2985601102-500		0		Administrator	exam.E01_1 Host	Domain	
S-1-5-21-2425377081-3129163575-2985601102-501		0		Guest	exam.E01_1 Host	Domain	

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

exam.E01_1 Host Details

Last Login: 2015-03-22 17:55:57 EET
Login Count: 1
Password Fail Date: 2015-03-22 17:56:37 EET
Password Settings: Password does not expire
Flag: Normal user account
Last Login: 2015-03-22 17:55:57 EET
Login Count: 1

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



Listing

11 Results

Table Thumbnail Summary Save Table as CSV

Name	S	C	O	Login Name	Host	Scope	Realm Name
S-1-5-18				SYSTEM	exam.E01_1 Host	Local	NT AUTHORITY
S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464		0			exam.E01_1 Host	Local	NT SERVICE
S-1-5-21-2425377081-3129163575-2985601102-1001		0		admin11	exam.E01_1 Host	Domain	
S-1-5-21-2425377081-3129163575-2985601102-1000		0		informant	exam.E01_1 Host	Domain	
S-1-5-21-2425377081-3129163575-2985601102-1003		0		temporary	exam.E01_1 Host	Domain	
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-1-5-80-2620923248-4247863784-3378508180-2659151310-2535246811		0			exam.E01_1 Host	Local	NT SERVICE
S-1-5-21-2425377081-3129163575-2985601102-1002		0		ITechTeam	exam.E01_1 Host	Domain	
S-1-5-21-2425377081-3129163575-2985601102-500		0		Administrator	exam.E01_1 Host	Domain	
S-1-5-21-2425377081-3129163575-2985601102-501		0		Guest	exam.E01_1 Host	Domain	

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

exam.E01_1 Host Details

Login Count: 0
Administrator: True
Password Fail Date: 2015-03-22 17:53:02 EET
Password Settings: Password does not expire
Flag: Normal user account
Login Count: 0
Administrator: True

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



digital-forensics-CD\$02 - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing /img_exam.E01/vol_voi3/Windows/System32/config
Table Thumbnail Summary

Save Table as CSV

Name S C O Modified Time Change Time Access Time Created Time

SECURITY 2015-03-25 17:31:05 EET 2015-03-25 17:31:05 EET 2015-03-25 17:31:05 EET 2009-07-14 05:34

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

Metadata
Name: LogonUI
Number of subkeys: 2
Number of values: 4
Modification Time: 2015-03-25 13:05:47 GMT+00:00

Values
Name Type Value
ShowTabletKeyboard REG_DWORD 0x00000000 (0)
LastLoggedOnProvider REG_SZ {6F45DC1E-5384-457A-BC13-2CD81B0D28ED}
LastLoggedOnSAMUser REG_SZ informant-PC\informant
LastLoggedOnUser REG_SZ \informant

CurrentVersion
App Management
App Paths
Applets
Audio
Authentication
Credential Provider Filters
Credential Providers
LogonUI
Background
BootAnimation
ShowTabletKeyboard
LastLoggedOnProvider
LastLoggedOnSAMUser
LastLoggedOnUser
PLAP Providers
BitLocker
BITS
Component Based Servicing
Control Panel
Controls Folder
DateTime
Device Installer
Device Metadata

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.



Screenshot of the EnCase Forensic application interface showing a file listing. The left pane displays a tree view of files and folders, including system logs like SAM.LOG, SECURITY.LOG, and SOFTWARE.LOG. The right pane shows a detailed table of log entries. A specific entry for the SYSTEM log is highlighted, showing details such as Name: SYSTEM, Type: REG_EXPAND_S..., Value: 57 A9 48 B5 10 67 D0 01.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
SAM.LOG				2010-11-21 09:20:59 EET	2015-03-25 13:13:48 EET	2010-11-21 09:20:59 EET	2009-07-14 10:07
SAM.LOG1				2015-03-25 16:46:37 EET	2015-03-25 16:46:37 EET	2009-07-14 05:40:08 EEST	2009-07-14 05:34
SAM.LOG2				2009-07-14 05:34:08 EEST	2015-03-25 17:31:05 EET	2009-07-14 05:34:08 EEST	2009-07-14 05:34
SECURITY				2015-03-25 17:31:05 EET	2015-03-25 17:31:05 EET	2009-07-14 05:34:08 EEST	2009-07-14 05:34
SECURITY.LOG				2010-11-21 09:20:59 EET	2015-03-25 18:13:49 EET	2010-11-21 09:20:59 EET	2009-07-14 10:07
SECURITY.LOG1				2015-03-25 17:31:05 EET	2015-03-25 17:31:05 EET	2009-07-14 05:34:08 EEST	2009-07-14 05:34
SECURITY.LOG2				2009-07-14 05:34:08 EEST	2015-03-25 17:31:05 EET	2009-07-14 05:34:08 EEST	2009-07-14 05:34
SOFTWARE				2015-03-25 17:31:05 EET	2015-03-25 17:31:05 EET	2015-03-25 17:31:05 EET	2009-07-14 05:34
SOFTWARELOG				2010-11-21 09:21:00 EET	2015-03-25 18:13:50 EET	2010-11-21 09:21:00 EET	2009-07-14 10:07
SOFTWARELOG1				2015-03-25 17:31:05 EET	2015-03-25 17:31:05 EET	2009-07-14 05:34:08 EEST	2009-07-14 05:34
SOFTWARE.LOG2				2009-07-14 05:34:08 EEST	2015-03-25 17:31:05 EET	2009-07-14 05:34:08 EEST	2009-07-14 05:34
SYSTEM				2015-03-25 17:31:05 EET	2015-03-25 17:31:05 EET	2015-03-25 17:31:05 EET	2009-07-14 05:34
SYSTEM.LOG				2010-11-21 09:20:59 EET	2015-03-25 18:13:50 EET	2010-11-21 09:20:59 EET	2009-07-14 10:07
SYSTEM.LOG1				2015-03-25 17:31:05 EET	2015-03-25 17:31:05 EET	2009-07-14 05:34:08 EEST	2009-07-14 05:34
SYSTEM.LOG2				2009-07-14 05:34:08 EEST	2015-03-25 17:31:05 EET	2009-07-14 05:34:08 EEST	2009-07-14 05:34
COMPONENTS.LOG1				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
COMPONENTS.LOG2				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
COMPONENTS(016888b8-6c6f-11de-8d1d-001e0b)				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
SECURITY.LOG1				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00

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

Screenshot of the EnCase Forensic application interface showing the Windows registry key for Controlset001/Control/Windows. The left pane shows a tree view of registry keys under Windows. The right pane displays the metadata and values for the ShutdownTime key. The value is listed as 57 A9 48 B5 10 67 D0 01.

Name	Type	Value
ShutdownTime	REG_BIN	57 A9 48 B5 10 67 D0 01

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

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

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



Download CyberChef [Download](#)

Last build: 6 days ago - Version 10 is here! Read about the new features [here](#)

Options [⚙️](#) About / Support [?](#)

Operations

- Swap
- Swap case**
- Swap endianness
- AES Key Wrap
- GOST Key Wrap
- Show on map
- AES Key Unwrap
- GOST Key Unwrap
- Favourites**
- Data format
- Encryption / Encoding
- Public Key
- Arithmetic / Logic
- Networking
- Language

Recipe

Swap endianness

Data format: Hex Word length (bytes): 8
 Pad incomplete words

Input

57 A9 48 B5 10 67 D0 01

Output

01 D0 67 10 B5 48 A9 57

rec 24 F= 1 Tr Raw Bytes ← LF

STEP [object Object]

01 D0 67 10 B5 48 A9 57

rec 24 F= 1 Tr Raw Bytes ← LF

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

Download CyberChef [Download](#)

Last build: 6 days ago - Version 10 is here! Read about the new features [here](#)

Options [⚙️](#) About / Support [?](#)

Operations

- remove
- Remove EXIF**
- Remove Diacritics
- Remove null bytes
- Remove whitespace
- Remove line numbers
- Fang URL
- Strip HTML tags
- Strip HTTP headers
- Unique
- Favourites**
- Data format
- Encryption / Encoding
- Public Key
- Arithmetic / Logic

Recipe

Swap endianness

Data format: Hex Word length (bytes): 8
 Pad incomplete words

Remove whitespace

Spaces Carriage returns (\r) Line feeds (\n)
 Tabs Form feeds (\f) Full stops

Input

57 A9 48 B5 10 67 D0 01

Output

01d06710b548a957

rec 24 F= 1 Tr Raw Bytes ← LF

STEP Auto Bake

01d06710b548a957

rec 16 F= 1 Tr Raw Bytes ← LF

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



Download CyberChef [Download](#)

Last build: 6 days ago - Version 10 is here! Read about the new features [here](#)

Options [⚙️](#) About / Support [?](#)

Operations

- windows
- UNIX Timestamp to Windows Filetime
- Windows Filetime to UNIX Timestamp
- Decode text
- Encode text
- Extract file paths
- LZNT1 Decompress
- NT Hash
- Text Encoding Brute Force

Favourites ★

- Data format
- Encryption / Encoding
- Public Key
- Arithmetic / Logic
- Networking

Recipe

Swap endianness

Data format: Hex
Word length (bytes): 8

Pad incomplete words

Remove whitespace

Spaces
 Carriage returns (\r)
 Line feeds (\n)

Tabs
 Form feeds (\f)
 Full stops

Windows Filetime to UNIX Timestamp

Output units: Seconds (s)
Input format: Hex (big endian)

STEP  Auto Bake

Input

```
57 A9 48 B5 10 67 D0 01
```

Output

```
1427297465.2320087
```

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

Download CyberChef [Download](#)

Last build: 6 days ago - Version 10 is here! Read about the new features [here](#)

Options [⚙️](#) About / Support [?](#)

Operations

- times
- To UNIX Timestamp
- From UNIX Timestamp
- Parse ObjectID timestamp
- UNIX Timestamp to Windows Filetime
- Windows Filetime to UNIX Timestamp
- LZString Compress
- LZString Decompress
- Bombe
- Count occurrences
- Extract RGBA
- From BCD
- Get Time
- NT Hash
- Randomize Colour Palette

Recipe

Swap endianness

Data format: Hex
Word length (bytes): 8

Pad incomplete words

Remove whitespace

Spaces
 Carriage returns (\r)
 Line feeds (\n)

Tabs
 Form feeds (\f)
 Full stops

Windows Filetime to UNIX Timestamp

Output units: Seconds (s)
Input format: Hex (big endian)

From UNIX Timestamp

Units: Seconds (s)

STEP  Auto Bake

Input

```
57 A9 48 B5 10 67 D0 01
```

Output

```
Wed 25 March 2015 15:31:05 UTC
```

So the answer 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

Name	Type	Value
UseZeroBroadcast	REG_DWORD	0x00000000 (0)
EnableDeadGWDetect	REG_DWORD	0x00000001 (1)
EnableDHCP	REG_DWORD	0x00000001 (1)
NameServer	REG_SZ	(value not set)
Domain	REG_SZ	(value not set)
RegistrationEnabled	REG_DWORD	0x00000001 (1)
RegisterAdapterName	REG_DWORD	0x00000000 (0)
DhcpIPAddress	REG_SZ	10.11.11.129
DhcpSubnetMask	REG_SZ	255.255.255.0
DhcpServer	REG_SZ	10.11.11.254
Lease	REG_DWORD	0x00000708 (1800)
LeaseObtainedTime	REG_DWORD	0x5512d216 (1427297690)
T1	REG_DWORD	0x5512d59a (1427297690)
T2	REG_DWORD	0x5512d83d (1427298365)
LeaseTerminatesTime	REG_DWORD	0x5512d91e (1427298590)
AddressType	REG_DWORD	0x00000000 (0)
IsServerNapAware	REG_DWORD	0x00000000 (0)
DhcpConnForceBroadcastFlag	REG_DWORD	0x00000000 (0)
DhcpInterfaceOptions	REG_BIN	2C 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00...
DhcpGatewayHardware	REG_BIN	0A 08 0B 02 06 00 00 00 50 56 EB B2 2C
DhcpGatewayHardwareCount	REG_DWORD	0x00000001 (1)
DhcpNameServer	REG_SZ	10.11.11.2
DhcpDefaultGateway	REG_MULTI_SZ	10.11.11.2,
DhcpDomain	REG_SZ	localdomain
DhcpSubnetMaskOpt	REG_MULTI_SZ	255.255.255.0

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.



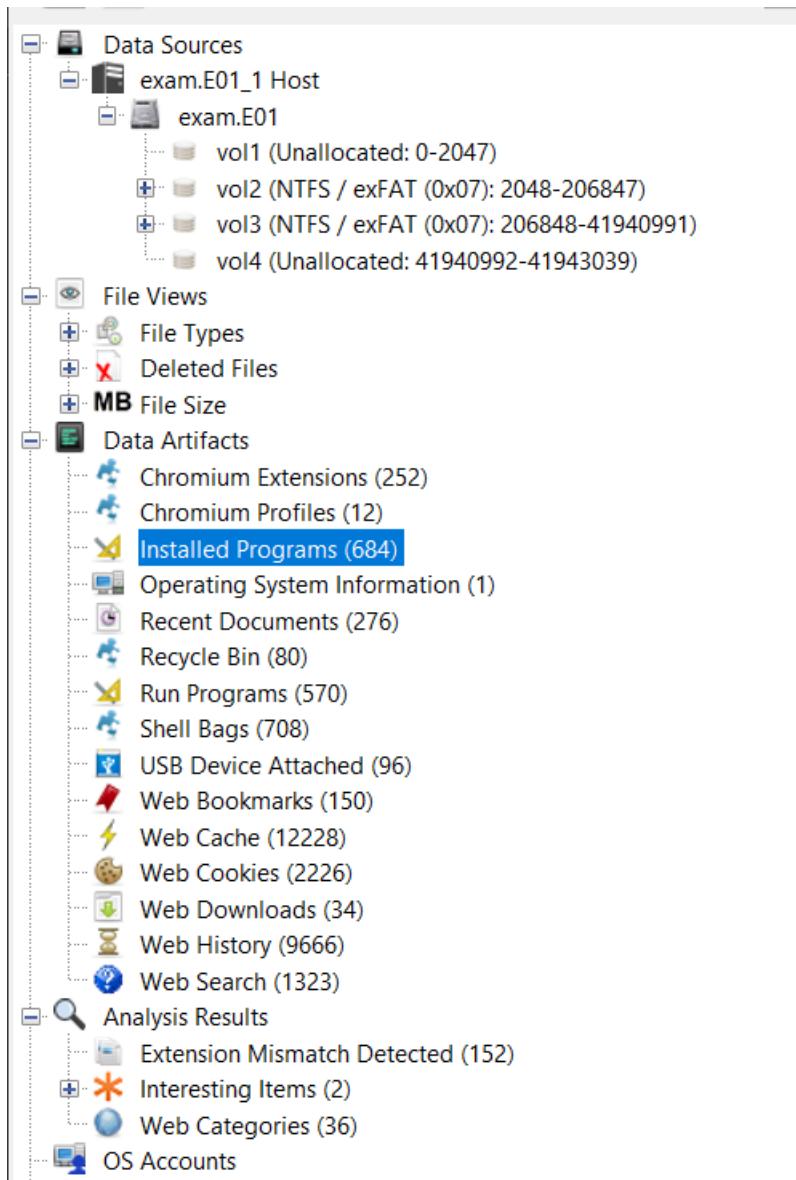
-
- On DhcpSubnetMask the subnet mask assigned by DHCP is 255.255.255.0.
 - On DhcpServer the DHCP server that assigned the IP address is 10.11.11.254.
 - On DhcpNameServer the DNS server provided by DHCP is 10.11.11.2.
 - On DhcpDefaultGateway the default gateway provided by DHCP is 10.11.11.2.
 - On 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.





Listing
Installed Programs
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.15.0.4420.1017	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.15.0.4420.10	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.15.0.4420.101	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 - FSpanish v.15.0.4420.101	2015-03-22 15:01:14 FFT	exam.F01

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
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 14:54:33 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 FFT	exam.F01

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.

The screenshot shows the EnCase Forensic interface. On the left, the file system tree displays various volumes and their contents, including several language packs (sv-SE, uk-UA, zh-CN, zh-HK, zh-TW) and system DLLs (TAPI, Tasks, Temp, tracing, twain_32, Vss, Web, win32k). The main pane shows a table titled "Listing" with the path "/img_exam.E01/vol_voi3/Windows/System32/winevt/Logs". The table lists event log files with columns for Name, S, C, O, Modified Time, Change Time, Access Time, and Created Time. The "Security.evtx" file is highlighted in blue. Below the table is a hex dump of the file's content, showing binary data and some ASCII strings like "ElfFile.....", ".....", and ".R.". At the bottom of the interface, there are tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
Microsoft-Windows-Windows Firewall With Advan...				2015-03-25 17:31:01 EET	2015-03-25 17:31:01 EET	2015-03-25 12:15:55 EET	2015-03-25 12:15:55 EET
Microsoft-Windows-WindowsBackup%4ActionCent...				2015-03-25 17:31:01 EET	2015-03-25 17:31:01 EET	2015-03-22 16:36:43 EET	2015-03-22 16:36:43 EET
Microsoft-Windows-WindowsSystemAssessmentTo...				2015-03-24 23:07:27 EET	2015-03-25 12:33:14 EET	2015-03-25 12:33:14 EET	2015-03-25 12:33:14 EET
Microsoft-Windows-WindowsUpdateClient%4Oper...				2015-03-25 17:31:01 EET	2015-03-25 17:31:01 EET	2015-03-25 12:18:28 EET	2015-03-25 12:18:28 EET
Microsoft-Windows-Winlogon%4operational.evtx				2015-03-22 16:38:16 EET	2015-03-22 16:38:16 EET	2015-03-22 16:38:43 EET	2015-03-22 16:38:43 EET
Alerts.evtx				2015-03-25 17:31:01 EET	2015-03-25 17:31:01 EET	2015-03-22 17:03:49 EET	2015-03-22 17:03:49 EET
Security.evtx				2015-03-25 17:31:01 EET	2015-03-25 17:31:01 EET	2015-03-25 12:15:47 EET	2015-03-25 12:15:47 EET
Setup.evtx				2015-03-25 17:31:01 EET	2015-03-25 17:31:01 EET	2015-03-25 12:18:25 EET	2015-03-25 12:18:25 EET
System.evtx				2015-03-25 17:31:01 EET	2015-03-25 17:31:01 EET	2015-03-25 12:15:47 EET	2015-03-25 12:15:47 EET
Windows PowerShell.evtx				2015-03-25 12:18:29 EET	2015-03-25 12:18:29 EET	2015-03-25 12:15:47 EET	2015-03-25 12:15:47 EET

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



Microsoft-Windows-Winlogon%4Operational.evtx

OAlerts.evtx

Security.evtx

Setup.evtx

System.evtx

Windows Power

Hex Text Application

Page: 1 of 69

Offset	Value	Comment
0x0000000000:	45 6C	
0x000000010:	0C 00	
0x000000020:	80 00	
0x000000030:	00 00	
0x000000040:	00 00	
0x000000050:	00 00	
0x000000060:	00 00	
0x000000070:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	91 52 7D 99
0x000000080:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x000000090:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

View File in Timeline...

View Item in New Window

Open in External Viewer Ctrl+E

Extract File(s)

Export Selected Rows to CSV

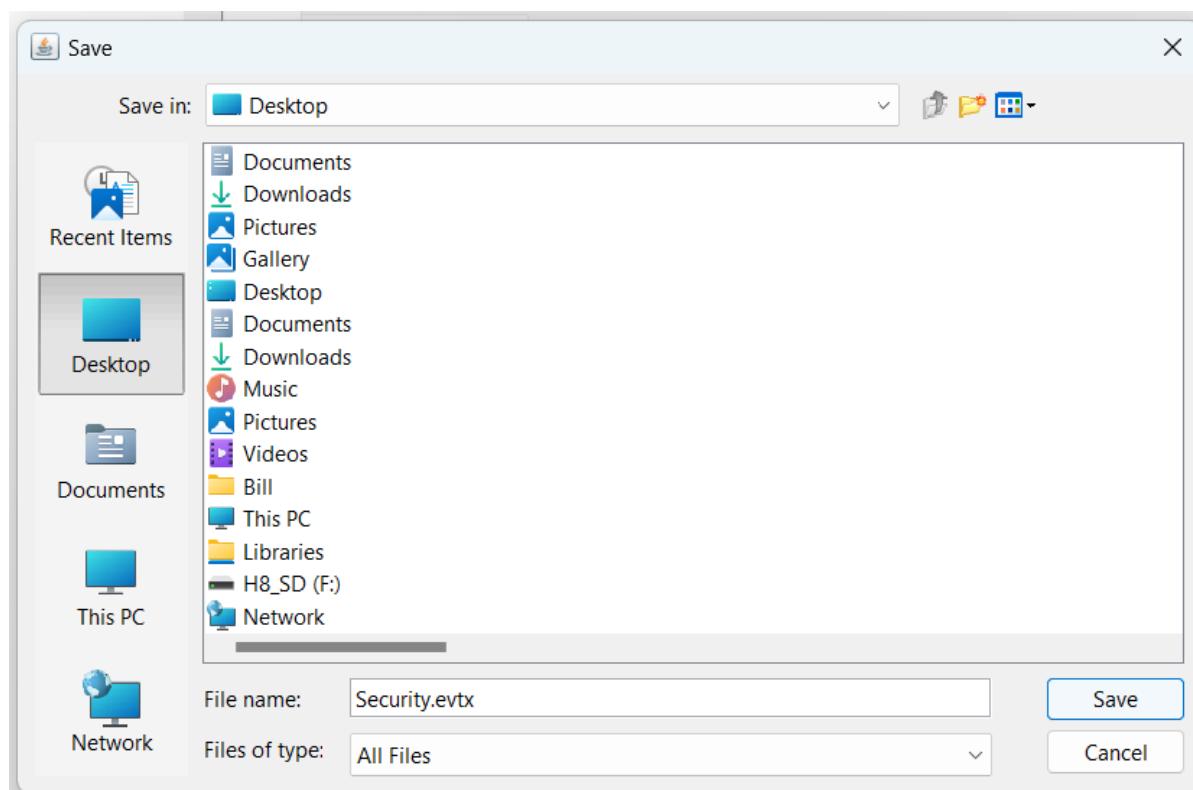
Add File Tag

Remove File Tag

Add/Edit Central Repository Comment (No MD5 Hash)

Add File to Hash Set (No MD5 Hash)

Properties





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 shutting down.

4672: Special privileges assigned to new logon.

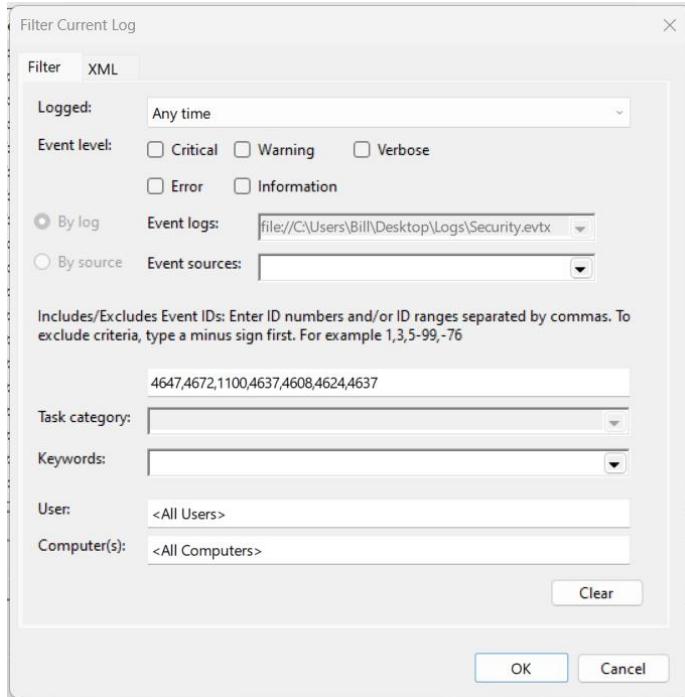
4647: User initiated logoff.

We will use the above ids.

The screenshot shows the Windows Event Viewer interface. On the left, the navigation pane lists 'Event Viewer (Local)', 'Custom Views', 'Windows Logs', 'Applications and Services Logs', 'Saved Logs' (with 'Security' selected), and 'Subscriptions'. The main pane displays a table of security events under the 'Security' category. The table has columns for Level, Date and Time, Source, Event ID, and Task Category. A large number of entries are listed, mostly 'Information' level events from 'Micros...' sources with Event IDs ranging from 4616 to 4647. The right pane, titled 'Actions', shows a context menu for the selected event (Event 4624). The menu includes options like 'Open Saved Log...', 'Create Custom View...', 'Import Custom View...', 'Filter Current Log...', 'Properties', 'Find...', 'Save All Events As...', 'View', 'Delete', 'Rename', 'Refresh', 'Help', 'Event Properties', 'Copy', 'Save Selected Events...', 'Refresh', and 'Help'. Below the main pane, a details window is open for 'Event 4624, Microsoft Windows security auditing.' It shows the 'General' tab with the message 'An account was successfully logged on.' and the 'Details' tab with fields: Log Name: Security; Source: Microsoft Windows security; Event ID: 4624; Task Category: Logon; Level: Information; User: N/A; OpCode: Info; Logged: 25-03-15 4:56:55 PM; Keywords: Audit Success; Computer: informant-PC. At the bottom left of the main pane, there is a note: 'Creates a filter.'



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



We classify base on date.

Level	Date and Time	Source	Event ID	Task Category
Information	25-03-15 5:18:54 PM	Microsoft Windows security auditing.	4624	Logon
Information	25-03-15 4:57:18 PM	Microsoft Windows security auditing.	4624	Logon
Information	25-03-15 4:57:18 PM	Microsoft Windows security auditing.	4624	Logon
Information	25-03-15 4:56:55 PM	Microsoft Windows security auditing.	4624	Logon
Information	25-03-15 4:50:50 PM	Microsoft Windows security auditing.	4624	Logon
Information	25-03-15 4:50:30 PM	Microsoft Windows security auditing.	4624	Logon
Information	25-03-15 4:50:30 PM	Microsoft Windows security auditing.	4624	Logon
Information	25-03-15 4:50:28 PM	Microsoft Windows security auditing.	4624	Logon
Information	25-03-15 4:45:59 PM	Microsoft Windows security auditing.	4624	Logon
Information	25-03-15 4:45:59 PM	Microsoft Windows security auditing.	4624	Logon
Information	25-03-15 4:45:59 PM	Microsoft Windows security auditing.	4634	Logoff
Information	25-03-15 4:45:59 PM	Microsoft Windows security auditing.	4634	Logoff
Information	25-03-15 4:31:53 PM	Microsoft Windows security auditing.	4624	Logon
Information	25-03-15 3:23:59 PM	Microsoft Windows security auditing.	4624	Logon
Information	25-03-15 3:07:49 PM	Microsoft Windows security auditing.	4624	Logon

Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject: Security ID: SYSTEM

Log Name: Security
Source: Microsoft Windows security
Event ID: 4624
Level: Information
User: N/A
OpCode: Info

More Information: [Event Log Online Help](#)



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

Security Number of events: 1,193
 Filtered: Log: file:///C:/Users/Bill/AppData/Local/Temp/Autopsy/digital-forensics-cds202_20240418_224129/Temp/Security.evtx; Source: ; Event ID: 4624,4634. Number of events: 152

Level	Date and Time	Source	Event ID	Task Category
(i) Information	25-03-15 4:45:59 PM	Microsoft Windows security auditing.	4624	Logon
(i) Information	25-03-15 4:45:59 PM	Microsoft Windows security auditing.	4624	Logon
(i) Information	25-03-15 4:45:59 PM	Microsoft Windows security auditing.	4634	Logoff
(i) Information	25-03-15 4:45:59 PM	Microsoft Windows security auditing.	4634	Logoff
(i) Information	25-03-15 4:31:53 PM	Microsoft Windows security auditing.	4624	Logon
(i) Information	25-03-15 3:23:59 PM	Microsoft Windows security auditing.	4624	Logon
(i) Information	25-03-15 3:07:49 PM	Microsoft Windows security auditing.	4624	Logon
(i) Information	25-03-15 3:06:16 PM	Microsoft Windows security auditing.	4624	Logon

Event 4634, Microsoft Windows security auditing.

General Details

An account was logged off.

Subject:

- Security ID: S-1-5-21-2425377081-3129163575-2985601102-1000
- Account Name: informant
- Account Domain: informant-PC
- Logon ID: 0x157773

Logon Type: 7

This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.

Log Name: Security
 Source: Microsoft Windows security
 Event ID: 4634
 Level: Information
 User: N/A
 OpCode: Info
 More Information: [Event Log Online Help](#)

The second recent was informant again



Security Number of events: 1,193

Filtered: Log: file:///C:/Users/Bill/AppData/Local/Temp/Autopsy/digital-forensics-cds202_20240418_224129(Temp)/Security.evtx; Source: ; Event ID: 4624,4634. Number of events: 152

Level	Date and Time	Source	Event...	Task Category
(i) Information	25-03-15 12:15:35 PM	Microsoft Windows security auditing.	4624	Logon
(i) Information	24-03-15 10:58:52 PM	Microsoft Windows security auditing.	4624	Logon
(i) Information	24-03-15 8:28:38 PM	Microsoft Windows security auditing.	4634	Logoff
(i) Information	24-03-15 8:28:38 PM	Microsoft Windows security auditing.	4624	Logon
(i) Information	24-03-15 8:28:38 PM	Microsoft Windows security auditing.	4624	Logon
(i) Information	24-03-15 8:28:38 PM	Microsoft Windows security auditing.	4634	Logoff
(i) Information	24-03-15 8:46:14 PM	Microsoft Windows security auditing.	4624	Logon
(i) Information	24-03-15 8:52:30 PM	Microsoft Windows security auditing.	4624	Logon

Event 4634, Microsoft Windows security auditing.

General Details

An account was logged off.

Subject:

Security ID:	S-1-5-21-2425377081-3129163575-2985601102-1000
Account Name:	informant
Account Domain:	informant-PC
Logon ID:	0x6CABDD

Logon Type: 7

This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.

Log Name: Security

Source: Microsoft Windows security

Event ID: 4634

Level: Information

User: N/A

OpCode: Info

More Information: [Event Log Online Help](#)

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.



Security Number of events: 1,193

Filtered: Log file:///C:/Users/Bill/AppData/Local/Temp/Autopsy/digital-forensics-cds202_20240418_224129/Temp/Security.evtx; Source: ; Event ID: 4624,4634. Number of events: 152

Level	Date and Time	Source	Event ID	Task Category
(i) Information	23-03-15 7:24:24 PM	Microsoft Windows security auditing.	4624	Logon
(i) Information	23-03-15 7:24:24 PM	Microsoft Windows security auditing.	4624	Logon
(i) Information	23-03-15 7:24:24 PM	Microsoft Windows security auditing.	4624	Logon
(i) Information	23-03-15 7:24:23 PM	Microsoft Windows security auditing.	4624	Logon
(i) Information	22-03-15 5:58:26 PM	Microsoft Windows security auditing.	4634	Logoff
(i) Information	22-03-15 5:58:26 PM	Microsoft Windows security auditing.	4634	Logoff
(i) Information	22-03-15 5:57:56 PM	Microsoft Windows security auditing.	4634	Logoff
(i) Information	22-03-15 5:57:55 PM	Microsoft Windows security auditing.	4634	Logoff

Event 4634, Microsoft Windows security auditing.

General Details

An account was logged off.

Subject:

- Security ID: S-1-5-21-2425377081-3129163575-2985601102-1001
- Account Name: admin11
- Account Domain: informant-PC
- Logon ID: 0x1354C8

Logon Type: 2

This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.

Log Name: Security
 Source: Microsoft Windows security
 Event ID: 4634
 Level: Information
 User: N/A
 OpCode: Info
 More Information: [Event Log](#) [Online Help](#)

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.



File Explorer interface showing the following tree structure:

- 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)** (highlighted in blue)
 - Web Search (1764)
- Analysis Results
 - Extension Mismatch Detected (152)
 - Interesting Items (2)
 - Web Categories (42)
- OS Accounts
- Tags
- Score
- Reports

Listing Web History

Table | Thumbnail | Summary | Go to Page: 1 of 2 | Pages: < > | 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
index.dat				System_Deployment_Log_goog...app_86fd5b6b43e6693	2015-03-22 15:11:21 EET			Internet Explorer Ar
index.dat				System_Deployment_Log_goog...app_86fd5b6b43e6693	2015-03-22 15:11:21 EET			Internet Explorer Ar
index.dat				System_Deployment_Log_goog...app_86fd5b6b43e6693	2015-03-22 15:11:21 EET			Internet Explorer Ar
index.dat				System_Deployment_Log_goog...app_86fd5b6b43e6693	2015-03-22 15:11:21 EET			Internet Explorer Ar
index.dat				System_Deployment_Log_goog...app_86fd5b6b43e6693	2015-03-22 15:11:21 EET			Internet Explorer Ar
index.dat				System_Deployment_Log_goog...app_86fd5b6b43e6693	2015-03-22 15:11:21 EET			Internet Explorer Ar
index.dat				about:blank				Internet Explorer Ar
WebCacheV01.dat				about:blank				Microsoft Edge Ana
WebCacheV01.dat				about:blank				Microsoft Edge Ana
WebCacheV01.dat				about:blank				Microsoft Edge Ana

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



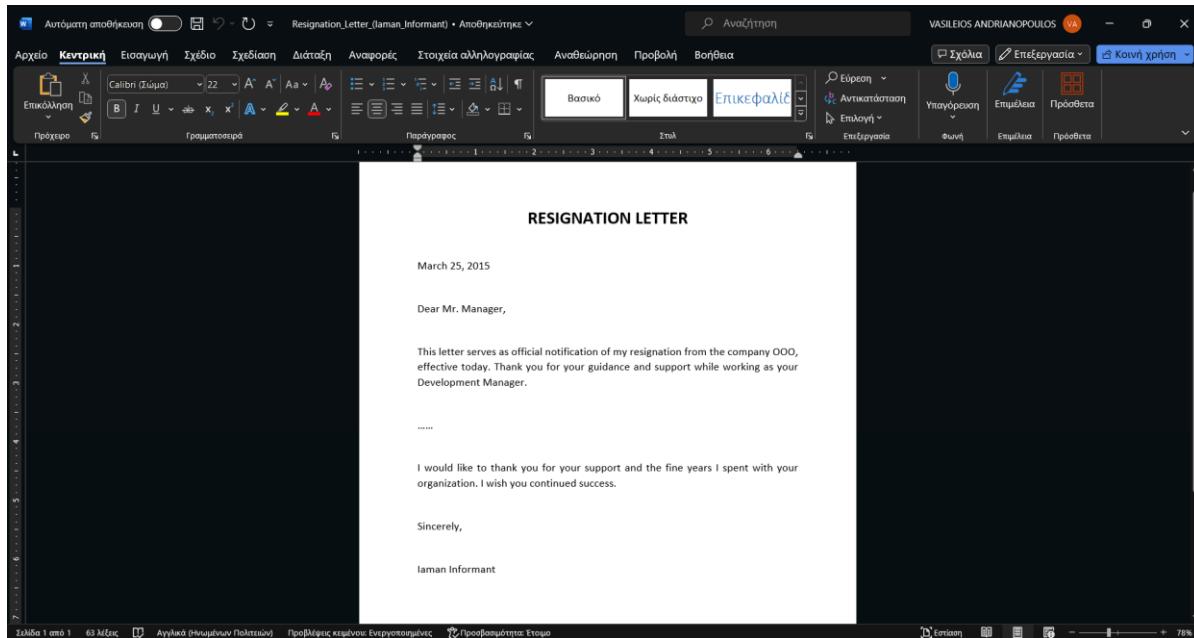
Then we can find the entries like “file://”

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

Source Name	S	C	O	URL	Date Accessed	Referrer
WebCacheV01.dat				file:///C:/Users/informant/AppData/Local/Temp/nsVueF.tmp/g/gto/toolbar.html		
WebCacheV01.dat				file:///C:/Users/informant/Desktop/Resignation_Letter_(laman_Informant).docx		
WebCacheV01.dat				file:///C:/Users/informant/Desktop/Resignation_Letter_(laman_Informant).docx		
WebCacheV01.dat				file:///C:/Users/informant/Desktop/Resignation_Letter_(laman_Informant).docx		
WebCacheV01.dat				file:///C:/Users/informant/Desktop/Resignation_Letter_(laman_Informant).docx		
WebCacheV01.dat				file:///C:/Users/informant/Desktop/Resignation_Letter_(laman_Informant).docx		
WebCacheV01.dat				file:///C:/Users/informant/Desktop/Resignation_Letter_(laman_Informant).docx		
WebCacheV01.dat				file:///C:/Users/informant/Desktop/Resignation_Letter_(laman_Informant).xps		
WebCacheV01.dat				file:///C:/Users/informant/Desktop/Resignation_Letter_(laman_Informant).xps		
WebCacheV01.dat				file:///C:/Users/informant/Desktop/Resignation_Letter_(laman_Informant).xps		
WebCacheV01.dat				file:///C:/Users/informant/Desktop/Resignation_Letter_(laman_Informant).xps		

Hex	Text	Application	Source File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Type:	File System								
MIME Type:	application/octet-stream								
Size:	33619968								
File Name Allocation:	Allocated								
Metadata Allocation:	Allocated								
Modified:	2015-03-25 17:30:56 EET								
Accessed:	2015-03-22 17:24:20 EET								
Created:	2015-03-22 17:24:20 EET								
Changed:	2015-03-25 17:30:56 EET								
MD5:	Not calculated								
SHA-256:	Not calculated								



Then we have the file **Resignation_Letter_(Iaman_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

Source Name	S	C	O	URL	Date Accessed	Referrer U
WebCacheV01.dat				file:///C:/Users/informant/Desktop/Resignation_Letter_(Iaman_Informant).docx		
WebCacheV01.dat				file:///C:/Users/informant/Desktop/Resignation_Letter_(Iaman_Informant).docx		
WebCacheV01.dat				file:///C:/Users/informant/Desktop/Resignation_Letter_(Iaman_Informant).docx		
WebCacheV01.dat				file:///C:/Users/informant/Desktop/Resignation_Letter_(Iaman_Informant).xps		
WebCacheV01.dat				file:///C:/Users/informant/Desktop/Resignation_Letter_(Iaman_Informant).xps		
WebCacheV01.dat				file:///C:/Users/informant/Desktop/Resignation_Letter_(Iaman_Informant).xps		
WebCacheV01.dat				file:///C:/Users/informant/Desktop/Resignation_Letter_(Iaman_Informant).xps		
WebCacheV01.dat				file:///C:/Users/informant/Desktop/Resignation_Letter_(Iaman_Informant).xps		
WebCacheV01.dat				file:///C:/Users/informant/Desktop/Resignation_Letter_(Iaman_Informant).xps		
WebCacheV01.dat				file:///C:/Users/informant/Desktop/Resignation_Letter_(Iaman_Informant).xps		
WebCacheV01.dat				file:///C:/Windows/inf/setupapi.dev.log		

Save Table as CSV

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

Metadata

Name: /img_exam.E01/vol_voi3/Users/informant/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat
Type: File System
MIME Type: application/octet-stream
Size: 33619968
File Name Allocation: Allocated
Metadata Allocation: Allocated
Modified: 2015-03-25 17:30:56 EET
Accessed: 2015-03-22 17:24:20 EET
Created: 2015-03-22 17:24:20 EET
Changed: 2015-03-25 17:30:56 EET



We can navigate to informant's Desktop folder



Then admin11 opened a file called setupapi.dev.log which 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.

Source Name	S	C	O	URL	Date Accessed	Referrer URL	Title	Program Name
WebCacheV01.dat				file:///C:/Windows/int/setupapi.dev.log				Microsoft Edge An
WebCacheV01.dat				file:///C:/Windows/int/setupapi.dev.log				Microsoft Edge An
WebCacheV01.dat				file:///C:/Windows/int/setupapi.dev.log				Microsoft Edge An
WebCacheV01.dat				file:///C:/Windows/int/setupapi.dev.log				Microsoft Edge An
WebCacheV01.dat				file:///C:/Windows/int/setupapi.dev.log				Microsoft Edge An
WebCacheV01.dat				file:///C:/Windows/int/setupapi.dev.log				Microsoft Edge An
WebCacheV01.dat				file:///C:/Windows/int/setupapi.dev.log				Microsoft Edge An
WebCacheV01.dat				file:///D:/Koala.jpg				Microsoft Edge An

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

Metadata

Name: /img_exam.E01/vol_vol3/Users/admin11/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat
 Type: File System
 MIME Type: application/octet-stream
 Size: 33619968
 File Name Allocation: Allocated
 Metadata Allocation: Allocated
 Modified: 2015-03-22 17:57:41 EET
 Accessed: 2015-03-22 17:53:59 EET
 Created: 2015-03-22 17:53:59 EET
 Changed: 2015-03-22 17:57:41 EET
 MD5: Not calculated
 SHA-256: Not calculated



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

The screenshot shows a dark-themed text editor window. The menu bar includes 'File', 'Edit', and 'View'. The title bar says 'setup X'. The main area contains a log file with the following content:

```
[Device Install Log]
OS Version = 6.1.7601
Service Pack = 1.0
Suite = 0x0100
ProductType = 1
Architecture = amd64

[BeginLog]

[Boot Session: 2015/03/25 02:14:55.468]

>>> [Setup Plug and Play Device Install]
>>> Section start 2015/03/25 03:15:54.764
set: ACPI\PNP0A05\2E -> setting CONFIGFLAG_FINISH_INSTALL on started device.
set: ROOT\LEGACY_SPLDR\0000 -> setting CONFIGFLAG_FINISH_INSTALL on started device.
set: ACPI\PNP0A05\49 -> setting CONFIGFLAG_FINISH_INSTALL on started device.
set: ROOT\LEGACY_AMDIDE\0000 -> setting CONFIGFLAG_FINISH_INSTALL on started device.
set: ROOT\LEGACY_NFRD960\0000 -> setting CONFIGFLAG_FINISH_INSTALL on started device.
set: ACPI\PNP0501\1 -> setting CONFIGFLAG_FINISH_INSTALL on started device.
set: ROOT\LEGACY_IASTORV\0000 -> setting CONFIGFLAG_FINISH_INSTALL on started device.
set: ACPI_HAL\PNP0C08\0 -> setting CONFIGFLAG_FINISH_INSTALL on started device.
set: ACPI\PNP0A05\2F -> setting CONFIGFLAG_FINISH_INSTALL on started device.
set: ACPI\PNP0A05\4A -> setting CONFIGFLAG_FINISH_INSTALL on started device.
set: ROOT\MS_NDISWANIP\0000 -> setting CONFIGFLAG_FINISH_INSTALL on started device.
set: PCIIDE\IDECHANNEL\5&35C44269&0&29 -> setting CONFIGFLAG_FINISH_INSTALL on started device.

Ln 1, Col 1           100%           Windows (CRLF)           UTF-8
```

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.

The screenshot shows a digital forensics interface. At the top, there are tabs for 'Listing', 'Web History', 'Table', 'Thumbnail', and 'Summary'. The 'Table' tab is selected. The table has columns: Source Name, S, C, O, URL, Date Accessed, Referrer URL, Title, and Program Name. The data shows multiple entries for 'WebCacheV01.dat' files, all pointing to 'file:///D/Koala.jpg' and accessed by 'Microsoft Edge Analyzer'. Below the table, there are navigation buttons for 'Page: 1 of 2', 'Pages:', 'Go to Page:', and 'Save Table as CSV'. At the bottom, there are tabs for 'Hex', 'Text', 'Application', 'Source File Metadata', 'OS Account', 'Data Artifacts', 'Analysis Results', 'Context', 'Annotations', and 'Other Occurrences'. The 'Analysis Results' tab is selected. It displays 'Visit Details' for the informant viewing 'file:///D/Koala.jpg' with 'Program Name: Microsoft Edge Analyzer'. The 'Source' section shows the host as 'exam.E01_1 Host', data source as 'exam.E01', and file path as '/img_exam.E01/vol_vol3/Users/informant/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat'.



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

Metadata

Name:	/img_exam.E01/vol_vol3/Users/informant/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat
Type:	File System
MIME Type:	application/octet-stream
Size:	33619968
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2015-03-25 17:30:56 EET
Accessed:	2015-03-22 17:24:20 EET
Created:	2015-03-22 17:24:20 EET
Changed:	2015-03-25 17:30:56 EET
MD5:	Not calculated
SHA-256:	Not calculated

We continue the same and finally we have the following table

File Name	File Path	Owner	Accessed
Resignation_Letter_(I aman_Informant).doc x	C:/Users/informant/D esktop/Resignation_L etter_(Iaman_Inform ant).docx	informant	2015-03-22 17:24:20 EET
setupapi.dev.log	C:/Windows/inf/setu papi.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_advi sory.zip	D:/de/winter_whethe r_advisory.zip	Informant	2015-03-22 17:24:20 EET
[secret_project]_desi gn_concept.ppt	E:/RM#1/Secret%20P roject%20Data/desi gn/[secret_project]_de sign_concept.ppt	informant	2015-03-22 17:24:20 EET
[secret_project]_prop osal.docx	E:/RM#1/Secret%20P roject%20Data/propo sal/[secret_project]_p roposal.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/nsvEOF.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.

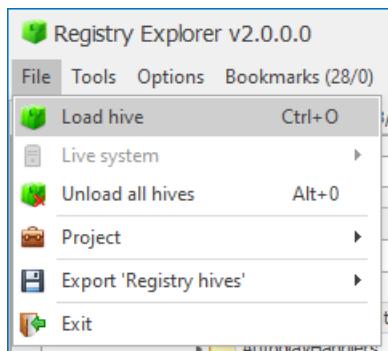
We navigate to Users/informant and we export ntuser.dat file to our pc.



Screenshot of the Autopsy digital forensics tool interface. The left sidebar shows a tree view of data sources, including 'exam.E01_1 Host' which contains various partitions and files like 'NTUSER.DAT', 'ntuser.dat.LOG1', etc. The main pane displays a table of file metadata with columns: Name, S, C, O, Modified Time, Change Time, Access Time, and Created Time. A context menu is open over the 'NTUSER.DAT' row, with options like 'View File in Timeline...', 'Extract File(s)', and 'Properties'. The bottom right corner of the table header says 'Annotations Other Occurrences'.

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.





The screenshot shows the Registry Explorer interface. The left pane displays the registry tree under the key `C:\Users\will\Desktop\NTUSER.DAT`. The right pane shows a table titled "Values" with columns: Value Name, Value Type, Data, Value Slack, Is Deleted, and Data Record Reallocated. A search bar at the top of the values viewer allows grouping by column headers. The "Type viewer" section below the table is currently empty.

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
=	=	=	=	=	=
11	2015-03-25 15:30:57	2015-03-25 12:06:09			
2	2015-03-22 14:34:41				
36	0	2015-03-22 14:34:41			
14	2015-03-22 15:45:59				
2	0	2015-03-22 14:34:41			
4	2015-03-22 14:34:41				
1	2015-03-22 14:34:48				
3	2015-03-22 14:34:42				
0	2015-03-22 14:34:41				
3	2015-03-22 14:34:41				
10	2015-03-25 15:18:36				
1	2015-03-22 14:34:41				
10	0				

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

And we see that the word that was searched was secret

The screenshot shows the Registry Explorer interface. The left pane displays the registry tree under the key `Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery`. The right pane shows a table titled "Values" with columns: Search Term, Mru Position, Key Name, and Last Write Timestamp. A search bar at the top of the values viewer allows grouping by column headers. The "Type viewer" section below the table is currently empty.

Search Term	Mru Position	Key Name	Last Write Timestamp
=	=	=	=
secret	0	WordWheelQuery	2015-03-23 18:40:17



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/Microsoft/Windows/Currentversion/Explorer/Map Network Drive MRU

The screenshot shows the Registry Explorer interface with the title bar "Registry Explorer v2.0.0.0". The menu bar includes File, Tools, Options, Bookmarks (28/0), View, and Help. The toolbar has buttons for File, Tools, Options, Bookmarks, and Help. The main window displays the registry keys under the "Selected hive: NTUSER.DAT" section. The "Key name" column lists various registry keys such as Explorer, Advanced, ApplicationDestinations, AutoplayHandlers, BitBucket, CobainState, CD Burning, CIDSave, CLSID, ComDig32, ControlPanel, Dicardable, FileExts, LowRegistry, Map Network Drive ..., MenuOrder, Modules, MountPoints2, NewShortcutHandlers, RecentDocs, RunRU, SearchPlatform, Shell Folders, StartPage, StartPage2, Streams, StudRects2, Taskband, TypePaths, User Shelf Folders, User Assist, VisualEffects, Wallpapers, and WordWheelQuery. The "Values" tab is selected, showing a table with columns: Value Name, Value Type, Data, Value Slack, Is Deleted, and Data Record Reallocated. One value is listed: NROList, RegSz, \\\|10.11.11.128\secured_drive, 00-00, Is Deleted (checkbox checked), and Data Record Reallocated (checkbox checked). Below the table, there are tabs for Type viewer, Slack viewer, and Binary viewer. The Type viewer shows Value name: \\\|10.11.11.128\secured_drive, Value type: RegSz, and Value raw value: 5C-00-5C-00-31-00-30-00-2E-00-31-00-31-00-2E-00-31-00-32-00-38-00-5C-00-73-00-65-00-63-00-75-00-72-00-65-00-64-00-5F-00-64-00-72-00-69-00-76-00-65-00-00-00. The Slack viewer shows Slack: 00-00. At the bottom, status bars show Key: Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU, Selected hive: NTUSER.DAT, Last write: 2015-03-23 20:26:04, 2 of 2 values shown (100.0%), Load complete, Value: a, Collapse all hives, Hidden keys: 0, and a checkbox for 1.

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_vo13/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
AutomaticDestinations				2015-03-25 17:28:47 EET	2015-03-25 17:28:47 EET	2015-03-25 17:28:47 EET	2015-03-22 16:35:02
CustomDestinations				2015-03-25 17:15:54 EET	2015-03-25 17:15:54 EET	2015-03-25 17:15:54 EET	2015-03-22 16:35:01
(secret_project)_pricing_decision.xlsx.lnk				2015-03-23 22:26:53 EET	2015-03-23 22:26:53 EET	2015-03-23 22:26:53 EET	2015-03-23 22:26:53
[secret_project]_design_concept.lnk				2015-03-23 20:38:21 EET	2015-03-23 20:38:21 EET	2015-03-23 20:38:21 EET	2015-03-23 20:38:21
[secret_project]_final_meeting.pptx.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
[secret_project]_proposal.lnk				2015-03-23 20:37:20 EET	2015-03-23 20:37:20 EET	2015-03-23 20:37:20 EET	2015-03-23 20:37:20
CD Drive (2).lnk				2015-03-24 23:01:14 EET	2015-03-24 23:01:14 EET	2015-03-24 23:01:14 EET	2015-03-24 23:01:11

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

Result: 1 of 8 Recent Documents

Type	Value	Source(s)
Path	\\\10.11.11.128\SECURED_DRIVE\Secret Project Data\pricing decision\secret_project_pricing_decision.xlsx	RecentActivity
Path ID	-1	RecentActivity
Date Accessed	2015-03-23 22:26:53 EET	RecentActivity
Source File Path	/img_exam.E01/vol_vo13/Users/informant/AppData/Roaming/Microsoft/Windows/Recent/(secret_project)_pricing_decision.xlsx.lnk	
Artifact ID	-9223372036854775783	

Listing /img_exam.E01/vol_vo13/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
[secret_project]_design_concept.lnk				2015-03-23 20:38:21 EET	2015-03-23 20:38:21 EET	2015-03-23 20:38:21 EET	2015-03-23 20:38:21
[secret_project]_final_meeting.pptx.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
[secret_project]_proposal.lnk				2015-03-23 20:37:20 EET	2015-03-23 20:37:20 EET	2015-03-23 20:37:20 EET	2015-03-23 20:37:20
CD Drive (2).lnk				2015-03-24 23:01:14 EET	2015-03-24 23:01:14 EET	2015-03-24 23:01:14 EET	2015-03-24 23:01:11
CD Drive.lnk				2015-03-24 22:47:30 EET	2015-03-24 22:47:30 EET	2015-03-24 22:47:30 EET	2015-03-24 22:47:22
desktop.ini				2015-03-22 16:34:59 EET	2015-03-22 16:34:59 EET	2015-03-22 16:34:59 EET	2015-03-22 16:34:55
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

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

Result: 1 of 8 Recent Documents

Type	Value	Source(s)
Path	\\\10.11.11.128\secured_drive\Secret Project Data\final\secret_project_final_meeting.pptx	RecentActivity
Path ID	-1	RecentActivity
Date Accessed	2015-03-23 22:27:33 EET	RecentActivity
Source File Path	/img_exam.E01/vol_vo13/Users/informant/AppData/Roaming/Microsoft/Windows/Recent/[secret_project]_final_meeting.pptx.lnk	
Artifact ID	-9223372036854775766	



Listing
/img_exam.E01/vol_vo3/Users/informant/AppData/Roaming/Microsoft/Windows/Recent
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
desktop.ini				2015-03-22 16:34:59 EET	2015-03-22 16:34:59 EET	2015-03-22 16:34:55 EET	2015-03-22 16:34:55
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_(laman_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_(laman_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
carrot.lnk				2015-03-22 20:38:21 EET	2015-03-22 20:38:21 EET	2015-03-22 20:38:21 EET	2015-03-22 20:37:20

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

Result: 1 of 8 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_vo3/Users/informant/AppData/Roaming/Microsoft/Windows/Recent/final.lnk	
Artifact ID	-9223372036854775778	

Listing
/img_exam.E01/vol_vo3/Users/informant/AppData/Roaming/Microsoft/Windows/Recent
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
desktop.ini				2015-03-22 16:34:59 EET	2015-03-22 16:34:59 EET	2015-03-22 16:34:55 EET	2015-03-22 16:34:55
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_(laman_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_(laman_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
carrot.lnk				2015-03-22 20:38:21 EET	2015-03-22 20:38:21 EET	2015-03-22 20:38:21 EET	2015-03-22 20:37:20

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

Result: 1 of 8 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_vo3/Users/informant/AppData/Roaming/Microsoft/Windows/Recent/pricing decision.lnk	
Artifact ID	-9223372036854775775	



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

Listing /img_exam.E01/vol_vo3/Users/informant/AppData/Roaming/Microsoft/Office/Recent 10 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
[current folder]				2015-03-25 17:28:09 EET	2015-03-25 17:28:09 EET	2015-03-25 17:28:09 EET	2015-03-23 20:37:54 EET
[parent folder]				2015-03-23 20:37:54 EET	2015-03-23 20:37:54 EET	2015-03-23 20:37:54 EET	2015-03-23 19:29:31 EET
(secret_project)_pricing_decision.xlsx.LNK				2015-03-23 22:26:56 EET	2015-03-23 22:26:56 EET	2015-03-23 22:26:56 EET	2015-03-23 22:26:56 EET
[secret_project].design_concept.LNK				2015-03-23 20:38:23 EET	2015-03-23 20:38:23 EET	2015-03-23 20:38:23 EET	2015-03-23 20:38:23 EET
[secret_project].final_meeting.pptx.LNK				2015-03-23 22:27:37 EET	2015-03-23 22:27:37 EET	2015-03-23 22:27:37 EET	2015-03-23 22:27:37 EET
[secret_project].proposal.LNK				2015-03-23 20:37:54 EET	2015-03-23 20:37:54 EET	2015-03-23 20:37:54 EET	2015-03-23 20:37:54 EET
Desktop.LNK				2015-03-24 20:48:40 EET	2015-03-24 20:48:40 EET	2015-03-24 20:48:40 EET	2015-03-24 20:48:40 EET

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\secret_project)_pricing_decision.xlsx	RecentActivity
Path ID	-1	RecentActivity
Date Accessed	2015-03-23 22:26:53 EET	RecentActivity
Source File Path	/img_exam.E01/vol_vo3/Users/informant/AppData/Roaming/Microsoft/Office/Recent/(secret_project)_pricing_decision.xlsx.LNK	
Artifact ID	-9223372036854775793	

Listing /img_exam.E01/vol_vo3/Users/informant/AppData/Roaming/Microsoft/Office/Recent 10 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
[secret_project].design_concept.LNK				2015-03-23 20:38:23 EET	2015-03-23 20:38:23 EET	2015-03-23 20:38:23 EET	2015-03-23 20:38:23 EET
(secret_project).final_meeting.pptx.LNK				2015-03-23 22:27:37 EET	2015-03-23 22:27:37 EET	2015-03-23 22:27:37 EET	2015-03-23 22:27:37 EET
[secret_project].proposal.LNK				2015-03-23 20:37:54 EET	2015-03-23 20:37:54 EET	2015-03-23 20:37:54 EET	2015-03-23 20:37:54 EET
Desktop.LNK				2015-03-24 20:48:40 EET	2015-03-24 20:48:40 EET	2015-03-24 20:48:40 EET	2015-03-24 20:48:40 EET
index.dat				2015-03-25 17:28:09 EET	2015-03-25 17:28:09 EET	2015-03-23 20:37:54 EET	2015-03-23 20:37:54 EET
Resignation_Letter_(laman_informant).docx.LNK				2015-03-25 17:28:09 EET	2015-03-25 17:28:09 EET	2015-03-25 17:28:09 EET	2015-03-24 20:48:40 EET
Templates.LNK				2015-03-23 20:38:12 EET	2015-03-23 20:38:12 EET	2015-03-23 20:38:12 EET	2015-03-23 20:38:12 EET

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\secret_project)_final_meeting.pptx	RecentActivity
Path ID	-1	RecentActivity
Date Accessed	2015-03-23 22:27:37 EET	RecentActivity
Source File Path	/img_exam.E01/vol_vo3/Users/informant/AppData/Roaming/Microsoft/Office/Recent/[secret_project].final_meeting.pptx.LNK	
Artifact ID	-9223372036854775785	



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

The screenshot shows the Registry Explorer V2.0.0 interface. The left pane displays the registry tree under 'File' (Windows Registry Editor) with several keys expanded, such as 'F12', 'Fax', 'Faxed', 'FTP', 'GDIPlus', 'IAMI', 'IME', 'INIEP', 'INIEP2', 'Internal Connection Wizard', 'Internet Explorer', 'Internet Mail and News', 'Keyboard', 'MediaLayer', 'MS Design Tools', 'Microsoft', 'MDF', 'Multimedia', 'Office', '15.0', 'Common', 'Encryption', 'Fax', 'FaxRun', 'Groove', 'MAPI', 'Microsoft Office 2013', 'Outlook', 'PowerPoint', 'Printers', 'PrintRun', 'Options', 'Place MRU', 'Security', and 'Registration'. The right pane shows a search result for 'final_meeting.pptx' with two items listed:

Value Name	Last Opened	Last Closed	File Name
Item 1	2015-03-23 20:27:37	--	E:\VM#1\Secret Project\Secret Project\Design\{secret_project\}_design_concept.ppt
Item 2	2015-03-23 18:38:23	--	

Below the search results, there is a 'Total rows: 2' message and an 'Export' button. The bottom status bar indicates the selected hive is NTUSER.DAT, the last writer was 'Software\Microsoft\Office\15.0\PowerPoint\Final MRU', and the search term was 'final_meeting.pptx'. The status bar also shows '2 of 2 values shown (100.00%)' and 'Load complete'.



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.

The screenshot shows the Autopsy software interface. At the top, there are several icons: a green plus sign for 'Add Data Source', a camera for 'Images/Videos', a speech bubble for 'Communications', a location pin for 'Geolocation', and a gear for settings. Below the toolbar, there are navigation buttons for back and forward, and a search bar. The main pane displays a hierarchical tree view of data sources:

- Data Sources
- File Views
- File Types
 - Deleted Files
 - File System (7539)
 - All (7539) (Selected)
- MB File Size
- Data Artifacts
 - Chromium Extensions (336)
 - Chromium Profiles (16)

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.



Listing All 7539 Results

Table Thumbnail Summary Save Table as CSV

Name	S	C	O	Modified Time	Change Time
X COMPONENTS(016888b8-6c6f-11de-8d1d-001e0bcde3ec).TxR2.regtrans-ms				2015-03-25 16:50:30 EET	2015-03-25 1
X tmp.edb				2015-03-25 16:50:27 EET	2015-03-25 1
X (22546D89-D2FE-11E4-B734-000C29FF2429).dat				2015-03-25 16:49:32 EET	2015-03-25 1
X (22546D8A-D2FE-11E4-B734-000C29FF2429).dat				2015-03-25 16:49:32 EET	2015-03-25 1
X ccsetup504.exe				2015-03-25 16:48:28 EET	2015-03-25 1
X ccsetup504.exe:Zone.Identifier				2015-03-25 16:48:28 EET	2015-03-25 1
X Eraser 6.2.0.2962.exe				2015-03-25 16:47:40 EET	2015-03-25 1
X Eraser 6.2.0.2962.exe:Zone.Identifier				2015-03-25 16:47:40 EET	2015-03-25 1
X ~DFC63A36FEE260F768.TMP				2015-03-25 16:46:06 EET	2015-03-25 1
X jsonstrings[1].js				2015-03-25 16:41:13 EET	2015-03-25 1
X ~\$rmailEmail.dotm				2015-03-25 16:41:10 EET	2015-03-25 1
X ~iaman.informant@nist.gov.ost.tmp				2015-03-25 16:41:04 EET	2015-03-25 1
X WebCacheV01.htm				2015-03-25 16:41:04 EET	2015-03-25 1

ccsetup504.exe and Eraser 6.2.0.2963.exe

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

Listing /img_exam.E01/vol_vol3/Users/informant/Desktop/Download 8 Results

Table Thumbnail Summary Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags
[parent folder]				2015-03-25 17:29:08 EET	2015-03-25 17:29:08 EET	2015-03-25 17:29:08 EET	2015-03-22 16:34:41 EET	56	Allocated
[current folder]				2015-03-25 17:15:45 EET	2015-03-25 17:15:45 EET	2015-03-25 17:15:45 EET	2015-03-22 17:08:23 EET	56	Allocated
X ccsetup504.exe				2015-03-25 16:48:28 EET	2015-03-25 16:48:28 EET	2015-03-25 16:48:28 EET	2015-03-25 16:48:28 EET	5344528	Unallocated
X ccsetup504.exe:Zone.Identifier				2015-03-25 16:48:28 EET	2015-03-25 16:48:28 EET	2015-03-25 16:48:28 EET	2015-03-25 16:48:28 EET	26	Unallocated
X Eraser 6.2.0.2962.exe				2015-03-25 16:47:40 EET	2015-03-25 16:47:40 EET	2015-03-25 16:47:40 EET	2015-03-25 16:47:40 EET	8317032	Unallocated
X Eraser 6.2.0.2962.exe:Zone.Identifier				2015-03-25 16:47:40 EET	2015-03-25 16:47:40 EET	2015-03-25 16:47:40 EET	2015-03-25 16:47:40 EET	26	Unallocated
IE11-Windows6.1-x64-en-us.exe				2015-03-22 17:11:04 EET	2015-03-22 17:11:04 EET	2015-03-22 17:11:04 EET	2015-03-22 17:11:04 EET	55915216	Allocated
IE11-Windows6.1-x64-en-us.exe:Zone.Identifier				2015-03-22 17:11:04 EET	2015-03-22 17:11:04 EET	2015-03-22 17:11:04 EET	2015-03-22 17:11:04 EET	26	Allocated

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:

- 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_vo3/Windows/Prefetch 145 Results

Table Thumbnail Summary Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	F
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	A
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	A
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	A
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	A
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	A
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	A
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	A
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	A
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	A
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	A
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	A
AgGIFaultHistory.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	A

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

Result: 1 of 8 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_vo3/Windows/Prefetch/UNINST.EXE-0867DC84.pf	
Artifact ID	-922337203685476916	

Then twice

Listing /img_exam.E01/vol_vo3/Windows/Prefetch 145 Results

Table Thumbnail Summary Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	F
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	A
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	A
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	A
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	A
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	A
AgGIFaultHistory.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	A
AgIGfAppHistory.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	A
AgIGlobalHistory.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	A
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	A
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-7C6EEDEA2.pf				2015-03-25 16:57:20 EET	2015-03-25 16:57:20 EET	2015-03-22 17:00:10 EET	2015-03-22 17:00:10 EET	10500	A

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

Result: 1 of 8 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_vo3/Windows/Prefetch/CCLEANER64.EXE-779BD542.pf	
Artifact ID	-9223372036854769258	



Eraser

twice

Listing
/img_exam.E01/vol_voi3/Windows/Prefetch
Table | Thumbnail | Summary | Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	F
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	A
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	A
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	A
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	A
AgGIFaultHistory.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	A
AgGIFgAppHistory.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	A
AgGIGlobalHistory.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	A
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	A
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-7CFDEA3.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
MSOURCEXE-20AE5C10.pf				2015-03-25 16:57:20 EET	2015-03-25 16:57:20 EET	2015-03-22 17:00:10 EET	2015-03-22 17:00:10 EET	50722	A

Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences | Run Programs

Type	Value	Source(s)
Program Name	ERASER.EXE	Windows Prefetch A
Path	/PROGRAM FILES/ERASER	Windows Prefetch A
Date/Time	2015-03-25 17:13:30 EET	Windows Prefetch A
Count	2	Windows Prefetch A
Comment	Prefetch File	Windows Prefetch A
Source File Path	/img_exam.E01/vol_voi3/Windows/Prefetch/ERASER.EXE-CE61944A.pf	
Artifact ID	-9223372036854769222	

Ccleaner setup only once



Listing /img_exam.E01/vol_vol3/Windows/Prefetch 145 Result

Table Thumbnail Summary Save Table as CSV

Name	AgGIHistory.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-72CD500D.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
MSCORSW.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_REGII.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 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 Result

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	22212	A
WUSA.EXE-A8D05906C.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 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.

The screenshot shows the Registry Explorer interface. The left pane displays the registry tree under 'Registry hives (1)'. The 'Run' key under 'Microsoft\Windows\CurrentVersion\Run' is selected. The right pane shows the 'Values' tab with a table of registry values. One entry, 'Eraser', is highlighted. The details pane at the bottom shows the following information for the 'Eraser' value:

Type viewer	Slack viewer	Binary viewer
Value name	Eraser	
Value type	RegSz	
Value	"C:\Program Files\Eraser\Eraser.exe" /atRestart	
Raw value	22-00-43-00-3A-00-5C-00-50-00-72-00-6F-00-67-00-72-00-61-00-60-00-20-00-46-00-69-00-6C-00-65-00-73-00-5C-00-45-00-72-00-61-00-73-00-65-00-72-00-60-00-2E-00-65-00-78-00-65-00-22-00-20-00-2F-00-61-00-74-00-52-00-65-00-73-00-74-00-61-00-72-00-74-00-00-00	
Slack	00-53-00-79	

At the bottom, status bars show: Key: Microsoft\Windows\CurrentVersion\Run, Selected hive: SOFTWARE, Last write: 2015-03-25 14:57:31, 1 of 1 values shown (100.00%), Load complete, Value: Eraser, Hidden keys: 0 | 1.



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

The screenshot shows the Digital Forensics New - Autopsy 4.21.0 interface. The left sidebar displays a tree view of registry keys under 'Case' > 'Windows Registry'. A specific key path is selected: 'HKLM\Software\Classes\mailto\shell\open\command'. The main pane shows a table of registry entries with columns: Name, S, C, O, Modified Time, Change Time, Access Time, and Created Time. There are four entries listed:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
SECURITY.LOG2				2009-07-14 05:34:08 EEST	2015-03-25 17:31:05 EET	2009-07-14 05:34:08 EEST	2009-07-14 05:34
SOFTWARE				2015-03-25 17:31:05 EET	2015-03-25 17:31:05 EET	2015-03-25 17:31:05 EET	2009-07-14 05:34
SOFTWARE.LOG				2010-11-21 09:21:00 EET	2015-03-25 13:13:50 EET	2010-11-21 09:21:00 EET	2009-07-14 10:07
SOFTWARELOG1				2015-03-25 17:31:05 EET	2015-03-25 17:31:05 EET	2009-07-14 05:34:08 EEST	2009-07-14 05:34
SOFTWARE.LOG2				2009-07-14 05:34:08 EEST	2015-03-25 17:31:05 EET	2009-07-14 05:34:08 EEST	2009-07-14 05:34

The right pane shows a detailed view of the 'command' key under 'mailto\shell\open'. It includes sections for 'Metadata' (Name: command, Number of subkeys: 0, Number of values: 1, Modification Time: 2015-03-22 15:03:42 GMT+00:00) and 'Values' (Name: (Default), Type: REG_S_, Value: "C:\PROGRA~1\MICROS~2\Office15\OUTLOOK.EXE" ...).

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



Registry Explorer v2.0.0.0

File Tools Options Bookmarks (28/0) View Help

Registry hives (2) Available bookmarks (60/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write time
FirstRun	1	0	2015-03-23
Groove	0	1	2015-03-22
MAPI	0	0	2015-03-25
Microsoft Office 2013	0	0	2015-03-23
Outlook	6	18	2015-03-25
AddInLoadTimes	5	0	2015-03-25
AddIns	1	6	2015-03-24
AutoDiscover	0	1	2015-03-22
Display Types	0	1	2015-03-22
Message	1	0	2015-03-24
Office Explorer	1	0	2015-03-25
Options	1	2	2015-03-22
Perf	0	1	2015-03-22
Preferences	4	0	2015-03-23
Profiles	0	1	2015-03-25
PST	1	0	2015-03-25
Resiliency	0	1	2015-03-25
Search	1	1	2015-03-24
Security	1	0	2015-03-23
Setup	6	0	2015-03-22
SQM	6	0	2015-03-25
Today	0	1	2015-03-24
Userinfo	3	0	2015-03-22

Values

Value Name	Type	Data
C:\Users\informant\AppData\Local\Microsoft\Outlook\jaman.informant@nist.gov.ost	RegDword	36...

Type viewer Binary viewer

Value name C:\Users\informant\AppData\Local\Microsoft\Outlook\jaman.informant@nist.gov.ost

Value type RegDword

Value 3631093

Key Software\Microsoft\Office\15.0\Outlook\Search
Selected hive: NTUSER.DAT Last write: 2015-03-24 13:29:24 1 of 1 values shown (100.00%) Load complete Hidden keys: 0 1

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

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

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

Digital Forensics New - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing /img_exam.E01/vol3/Users/informant/AppData/Local/Microsoft/Outlook 9 Results

Name S C O Modified Time Change Time Access Time Create

RoamCache				2015-03-23 21:29:29 EET	2015-03-23 21:29:29 EET	2015-03-23 21:29:29 EET	2015-03-23 21:29:29 EET
[current folder]				2015-03-25 17:11:47 EET	2015-03-25 17:11:47 EET	2015-03-25 17:11:47 EET	2015-03-25 17:11:47 EET
[parent folder]				2015-03-23 19:29:57 EET	2015-03-23 19:29:57 EET	2015-03-23 19:29:57 EET	2015-03-23 19:29:57 EET
fc39bdc85bcd43816b40b7d4c72f22 - Autodiscover.xml				2015-03-25 16:41:36 EET	2015-03-25 16:41:36 EET	2015-03-22 17:48:05 EET	2015-03-22 17:48:05 EET
iaman.informant@nist.gov.ost				2015-03-25 17:11:47 EET	2015-03-25 17:11:47 EET	2015-03-22 17:48:21 EET	2015-03-22 17:48:21 EET

Save Table as CSV

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

Result: 2 of 15 Result ← →

From: iaman </o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=25fb3fee5874a5497f8807234114f65-iaman> 2015-03-24 15:30:20 To: spy CC: Subject: RE: Last request

Headers Text HTML RTF Attachments (0) Accounts Download Images

To: iaman Subject: Last request

This is the last request.
I want to get the remaining data.



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.

The screenshot shows a digital forensics tool interface with a "Listing" tab selected. The main pane displays an email message. The header information is as follows:

From: spy <spy.conspirator@nist.gov>
To:
CC:
Subject: Hello, iaman

The timestamp on the right indicates the message was sent on 2015-03-23 19:29:29 EET. Below the header, there are tabs for Headers, Text, HTML, RTF, Attachments (0), and Accounts. A "Download Images" button is also present. The body of the email contains the text: "How are you doing?"

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

iaman responds, confirming successful completion of a task.

The screenshot shows a digital forensics tool interface with a "Listing" tab selected. The main pane displays an email message. The header information is as follows:

From: iaman </o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=25fb3fee58f74a5497f8807234114f65-iaman>
To: spy
CC:
Subject: RE: Hello, iaman

The timestamp on the right indicates the message was sent on 2015-03-23 20:44:00 EET. Below the header, there are tabs for Headers, Text, HTML, RTF, Attachments (0), and Accounts. A "Download Images" button is also present. The body of the email contains the text: "Successfully secured." followed by the original message from Spy.

From: spy
Sent: Monday, March 23, 2015 1:29 PM
To: iaman
Subject: Hello, iaman

How are you doing?



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

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

Listing

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

Result: 8 of 15 Result E-Mail Messages

From: spy <spy.conspirator@nist.gov> 2015-03-23 21:20:41 EET
To:
CC:
Subject: RE: Good job, buddy.

Headers Text HTML RTF Attachments (0) Accounts
Download Images

Okay, I got it.
I'll be in touch.

From: iaman
Sent: Monday, March 23, 2015 3:19 PM
To: spy
Subject: RE: Good job, buddy.

This is a sample.

From: spy
Sent: Monday, March 23, 2015 3:15 PM
To: iaman
Subject: Good job, buddy.

Good, job.
I need a more detailed data about this 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: 9 of 15 Result E-Mail Messages

From: spy <spy.conspirator@nist.gov> 2015-03-23 21:26:23 EET
To:
CC:
Subject: Important request

Headers Text HTML RTF Attachments (0) Accounts
Download Images

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: 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/0BzOye6gXtiZaVl8yVU5mWHIGbWc/view?usp=sharing>

<https://drive.google.com/file/d/0BzOye6gXtiZaakx6d3R3c0jmM1U/view?usp=sharing>



5. Last Request (March 24, 2015):

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

Listing /imo_exam.F01/vol.vol3/Users/informant/AnnData/Local/Microsoft/Outlook

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

Result: 10 of 15 Result E-Mail Messages

From: spy <spy.conspirator@nist.gov> To: CC: Subject: Last request

2015-03-24 15:25:59 EET

Headers Text HTML RTF Attachments (0) Accounts Download Images

This is the last request.
I want to get the 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.

Listing /imo_exam.F01/vol.vol3/Users/informant/AnnData/Local/Microsoft/Outlook

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

Result: 2 of 15 Result E-Mail Messages

From: iaman </o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=25fb3fee58f74a5497f8807234114f65-iaman> To: spy CC: Subject: RE: Last request

2015-03-24 15:35:00 EET

Headers Text HTML RTF Attachments (0) Accounts Download Images

This is the last time..

From: spy
Sent: Tuesday, March 24, 2015 9:34 AM
To: iaman
Subject: RE: Last request

No problem.
U can directly deliver storage devices that stored it.

From: iaman
Sent: Tuesday, March 24, 2015 9:30 AM
To: spy
Subject: RE: Last request

Stop it!
It is very hard to transfer all data over the internet!

From: spy
Sent: Tuesday, March 24, 2015 9:26 AM
To: iaman
Subject: Last request

This is the last request.
I want to get the remaining data.



7. Warning (March 24, 2015):

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

The screenshot shows a digital forensic interface with a search bar at the top containing the path: /imo_exam.E01/vol.vol3/Users/informant/AppData/Local/Microsoft/Outlook. Below the search bar is a navigation bar with tabs: Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences. The 'Text' tab is selected. A results summary indicates 1 of 15 results found. The main pane displays an email message titled 'RE: Watch out!' sent from iaman to spy on March 24, 2015, at 21:34:00 EET. The message body contains the following text:

```
I am trying.  
-----Original Message-----  
From: spy  
Sent: Tuesday, March 24, 2015 3:33 PM  
To: iaman  
Subject: Watch out!  
  
USB device may be easily detected.  
  
So, try another method.
```

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

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

The screenshot shows a digital forensic interface with a search bar at the top containing the path: /imo_exam.E01/vol.vol3/Users/informant/AppData/Local/Microsoft/Outlook. Below the search bar is a navigation bar with tabs: Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences. The 'Text' tab is selected. A results summary indicates 5 of 15 results found. The main pane displays an email message titled 'Done' sent from iaman to spy on March 24, 2015, at 23:05:00 EET. The message body contains the following text:

```
It's done. See you tomorrow.
```



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.