Scenario Overview

'Iaman Informant' was working as a manager of the technology development division at a famous international company OOO that developed state-of-the-art technologies and gadgets.

One day, at a place which 'Mr. Informant' visited on business, he received an offer from 'Spy Conspirator' to leak of sensitive information related to the newest technology. Actually, 'Mr. Conspirator' was an employee of a rival company, and 'Mr. Informant' decided to accept the offer for large amounts of money, and began establishing a detailed leakage plan.

'Mr. Informant' made a deliberate effort to hide the leakage plan. He discussed it with 'Mr. Conspirator' using an e-mail service like a business relationship. He also sent samples of confidential information though personal cloud storage.

After receiving the sample data, 'Mr. Conspirator' asked for the direct delivery of storage devices that stored the remaining (large amounts of) data. Eventually, 'Mr. Informant' tried to take his storage devices away, but he and his devices were detected at the security checkpoint of the company. And he was suspected of leaking the company data.

At the security checkpoint, although his devices (a USB memory stick and a CD) were briefly checked (protected with portable write blockers), there was no evidence of any leakage. And then, they were immediately transferred to the digital forensics laboratory for further analysis.

The information security policies in the company include the following:

1. Confidential electronic files should be stored and kept in the authorized external storage devices and the secured network drives.
2. Confidential paper documents and electronic files can be accessed only within the allowed time range from 10:00 AM to 16:00 PM with the appropriate permissions.
3. Non-authorized electronic devices such as laptops, portable storages, and smart devices cannot be carried onto the company.
4. All employees are required to pass through the 'Security Checkpoint' system.
5. All storage devices such as HDD, SSD, USB memory stick, and CD/DVD are forbidden under the 'Security Checkpoint' rules.

In addition, although the company managed separate internal and external networks and used DRM (Digital Rights Management) / DLP (Data Loss Prevention) solutions for their information security, 'Mr. Informant' had sufficient authority to bypass them. He was also very interested in IT (Information Technology), and had a slight knowledge of digital forensics.

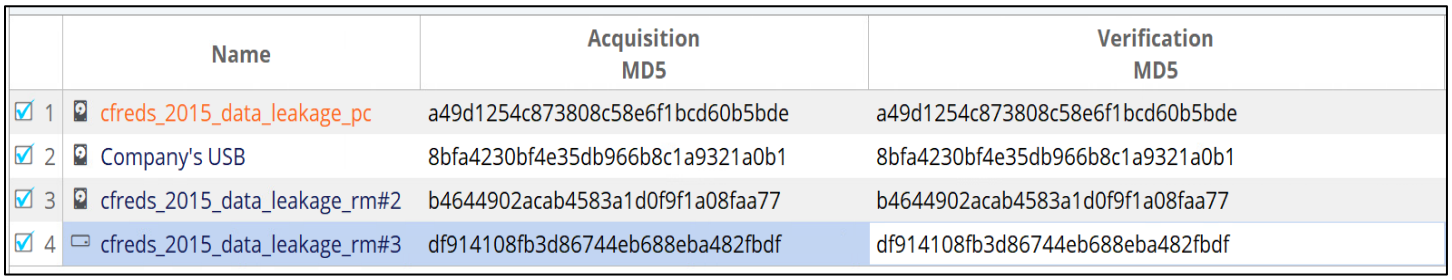
In this scenario, find any evidence of the data leakage, and any data that might have been generated from the suspect's electronic devices.

[**Please note:** If you have any issues clicking on the links to download the files, please "right click" and choose to "save as".]

1. What are the hash values (MD5 & SHA-1) of all images?
Does the acquisition and verification hash value match?

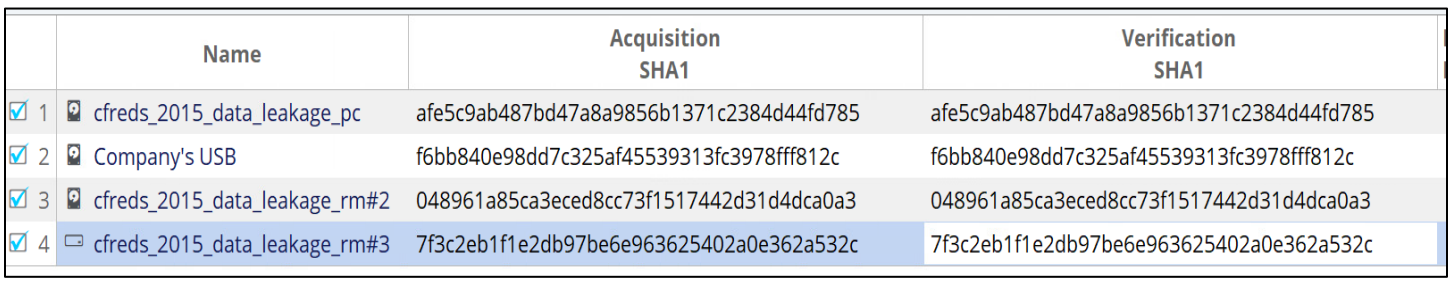
Answer:

Image		MD5	Result
cfreds_2015_data_leakage_pc	Acquisition	a49d1254c873808c58e6f1bcd60b5bde	Match
	Verification	a49d1254c873808c58e6f1bcd60b5bde	
Company's USB	Acquisition	8bfa4230bf4e35db966b8c1a9321a0b1	Match
	Verification	8bfa4230bf4e35db966b8c1a9321a0b1	
cfreds_2015_data_leakage_rm#2	Acquisition	b4644902acab4583a1d0f9f1a08faa77	Match
	Verification	b4644902acab4583a1d0f9f1a08faa77	
cfreds_2015_data_leakage_rm#3	Acquisition	df914108fb3d86744eb688eba482fbdf	Match
	Verification	df914108fb3d86744eb688eba482fbdf	



	Name	Acquisition MD5	Verification MD5
1	cfreds_2015_data_leakage_pc	a49d1254c873808c58e6f1bcd60b5bde	a49d1254c873808c58e6f1bcd60b5bde
2	Company's USB	8bfa4230bf4e35db966b8c1a9321a0b1	8bfa4230bf4e35db966b8c1a9321a0b1
3	cfreds_2015_data_leakage_rm#2	b4644902acab4583a1d0f9f1a08faa77	b4644902acab4583a1d0f9f1a08faa77
4	cfreds_2015_data_leakage_rm#3	df914108fb3d86744eb688eba482fbdf	df914108fb3d86744eb688eba482fbdf

Image		SHA1	Result
cfreds_2015_data_leakage_pc	Acquisition	afe5c9ab487bd47a8a9856b1371c2384d44fd785	Match
	Verification	afe5c9ab487bd47a8a9856b1371c2384d44fd785	
Company's USB	Acquisition	f6bb840e98dd7c325af45539313fc3978fff812c	Match
	Verification	f6bb840e98dd7c325af45539313fc3978fff812c	
cfreds_2015_data_leakage_rm#2	Acquisition	048961a85ca3eced8cc73f1517442d31d4dca0a3	Match
	Verification	048961a85ca3eced8cc73f1517442d31d4dca0a3	
cfreds_2015_data_leakage_rm#3	Acquisition	7f3c2eb1f1e2db97be6e963625402a0e362a532c	Match
	Verification	7f3c2eb1f1e2db97be6e963625402a0e362a532c	



	Name	Acquisition SHA1	Verification SHA1
1	cfreds_2015_data_leakage_pc	afe5c9ab487bd47a8a9856b1371c2384d44fd785	afe5c9ab487bd47a8a9856b1371c2384d44fd785
2	Company's USB	f6bb840e98dd7c325af45539313fc3978fff812c	f6bb840e98dd7c325af45539313fc3978fff812c
3	cfreds_2015_data_leakage_rm#2	048961a85ca3eced8cc73f1517442d31d4dca0a3	048961a85ca3eced8cc73f1517442d31d4dca0a3
4	cfreds_2015_data_leakage_rm#3	7f3c2eb1f1e2db97be6e963625402a0e362a532c	7f3c2eb1f1e2db97be6e963625402a0e362a532c

2. Identify the partition information of PC image.

Answer:

No.	Bootable	File System	Start Sector	Total Sectors	Size	Volume Name
1	No	NTFS	2,048	204,800	100 MB	System Reserved
2	Yes	NTFS	206,847	41,734,144	19.9 GB	C: Drive (Primary)

Verification:

Name	C
Logical Size	4,096
Category	Folder
Last Accessed	03/25/15 06:15:52 AM (-4:00 Eastern Daylight Time)
File Created	03/25/15 07:08:35 AM (-4:00 Eastern Daylight Time)
Item Path	cfreds_2015_data_leakage_pc\C
True Path	Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\C
Description	Volume, Sector 2048-206847, 100 MB, Folder, Internal, Hidden, System
Entry Modified	03/25/15 06:15:52 AM (-4:00 Eastern Daylight Time)
File Acquired	04/23/15 10:58:21 AM (-4:00 Eastern Daylight Time)
Initialized Size	4,096
Physical Size	4,096

File Extents	1
Permissions	-
Physical Location	1,228,800
Physical Sector	2,400
Evidence File	cfreds_2015_data_leakage_pc
File Identifier	5
GUID	f56121bc368e165809fd48f384e6b18f
Attributes	-
Serial Number	180A-0125
Full Serial Number	4A180A15180A0125
Driver Information	NTFS 3.1

Volume	
File System	NTFS
Sectors per cluster	8
Bytes per sector	512
Total Sectors	204,800
Total Capacity	104,853,504 Bytes (100 MB)
Total Clusters	25,599
Unallocated	79,552,512 Bytes (75.9 MB)
Free Clusters	19,422
Allocated	25,300,992 Bytes (24.1 MB)
Volume Name	System Reserved
Volume Offset	2,048

Allocated	25,300,992 Bytes (24.1 MB)
Volume Name	System Reserved
Volume Offset	2,048
Drive Type	Fixed
Partition	
Id	07
Type	NTFS
Start Sector	2,048
Total Sectors	204,800

Calculations:

Partition Size (for 100 MB System Reserved Partition):	$\textbf{Total Sectors} = \frac{100\ \text{MB} \times 1{,}048{,}576\ \text{bytes per MB}}{512\ \text{Bytes per Sector}} = \textbf{204,800 sectors}$
Total Capacity for the 19.9 GB C: Drive Partition:	$\textbf{Total Sectors} = \frac{19.9\ \text{GB} \times 1{,}073{,}741{,}824\ \text{bytes per GB}}{512\ \text{Bytes per Sector}} \approx \textbf{204,800 sectors}$
Total Clusters:	$\textbf{Total Sectors} = \frac{\text{Total Sectors}}{\text{Sector per Cluster}} = \frac{41{,}734{,}144}{8} = \textbf{5,216,768 clusters}$
Unallocated Space (for 19.9 GB partition):	$\boldsymbol{Unallocated\ Bytes} = \boldsymbol{Total\ Capacity} - \boldsymbol{Allocated\ Bytes} = \boldsymbol{100\ MB - 24.1\ MB = 75.9\ MB}$

Explanation:
The PC image contains two partitions:

1. **Partition 1 (System Reserved):** This 100 MB partition, with the NTFS file system, starts at sector 2,048 and is not bootable. It is labeled "System Reserved," typically used to store essential boot-related files.
2. **Partition 2 (Primary C: Drive):** This 19.9 GB bootable partition also uses NTFS and starts at sector 206,847. It serves as the main partition for the operating system and user data.

This partition layout is standard for Windows systems, with a reserved partition for boot files and a primary partition for OS and data storage.

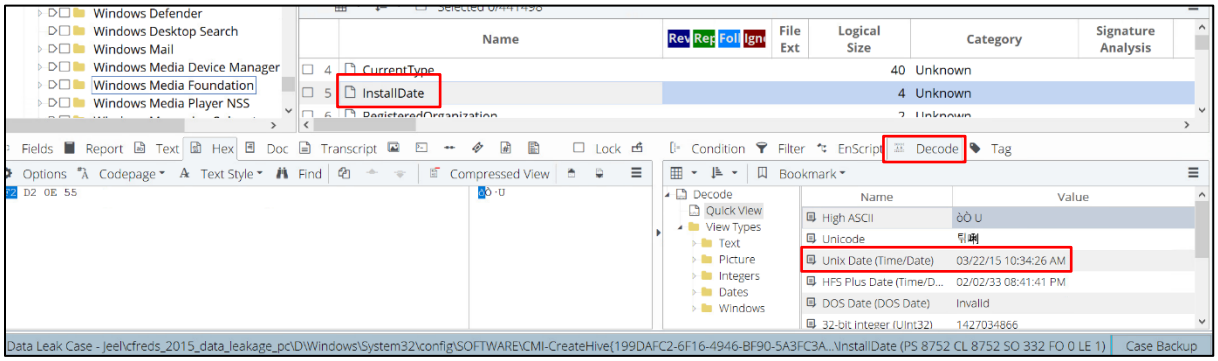
3. **Explain installed OS information in detail.**
   (OS name, install date, registered owner…)

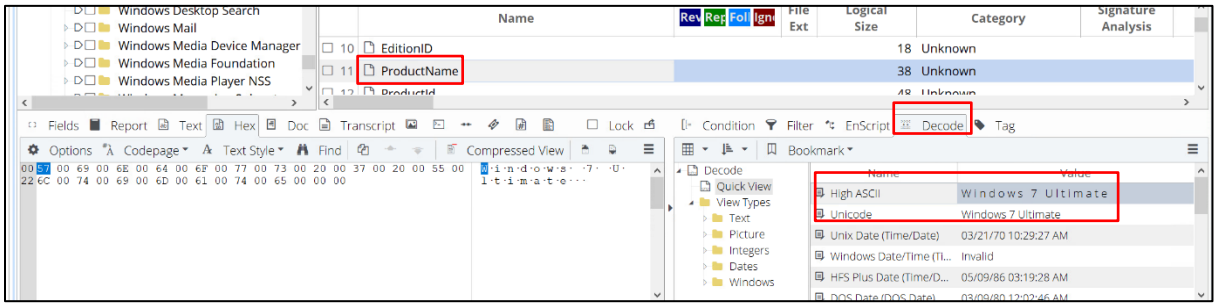
Answer:

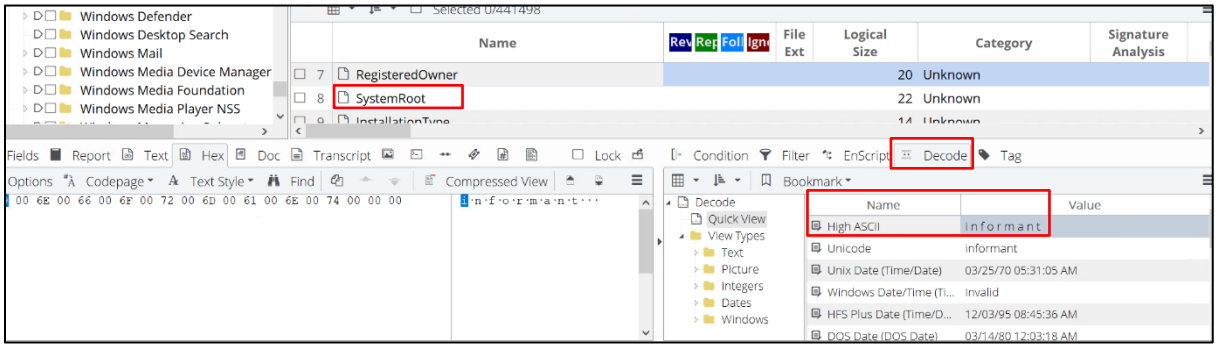
Field	Files	Value
OS Name	ProductName	Windows 7 Ultimate
Install Date	InstallDate	03/22/15 10:34:26 AM
Registered Owner	RegisteredOwner	informant
Registered Organization	RegisteredOrganization	(Not specified)
OS Version	CurrentVersion	6.1
OS Build Number	CurrentBuild	7601

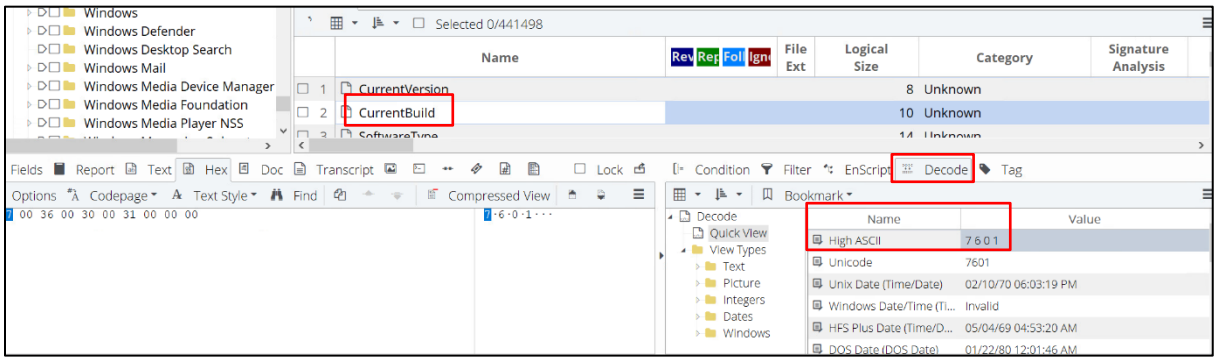
True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Windows\System32\config\SOFTWARE\CMI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\Microsoft\Windows NT\CurrentVersion\
Item Path: CMI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\Microsoft\Windows NT\CurrentVersion\

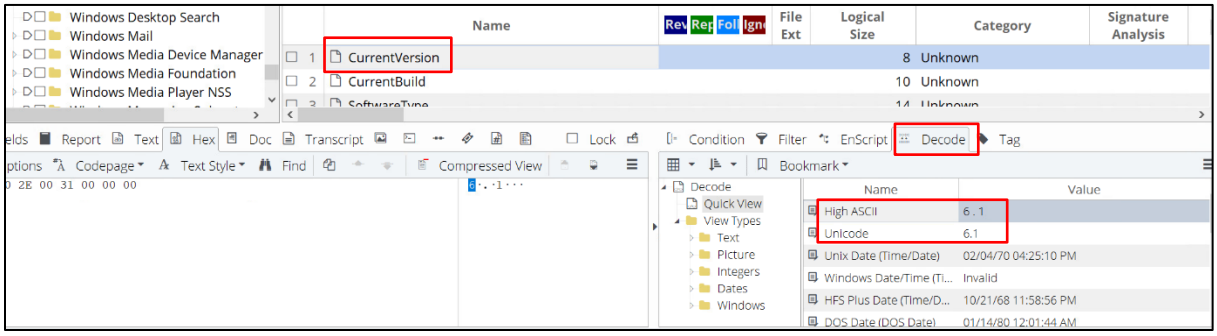
Targeted files: ProductName, InstallDate, RegisteredOwner, RegisteredOrganization, CurrentBuild and CurrentVersion

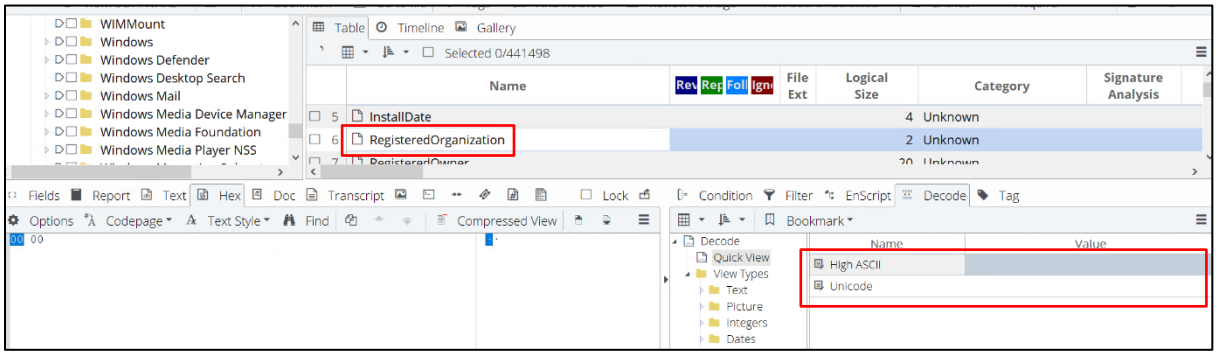



Windows Desktop Search
Windows Mail
Windows Media Device Manager
Windows Media Foundation
Windows Media Player NSS
Name
File Ext
Logical Size
Category
Signature Analysis
10 EditionID 18 Unknown
11 ProductName 38 Unknown
Decode
High ASCII Windows 7 Ultimate
Unicode Windows 7 Ultimate
Unix Date (Time/Date) 03/21/70 10:29:27 AM
Windows Date/Time (Ti... Invalid
HFS Plus Date (Time/D... 05/09/86 03:19:28 AM


Windows Defender
Windows Desktop Search
Windows Mail
Windows Media Device Manager
Windows Media Foundation
Windows Media Player NSS
Name
File Ext
Logical Size
Category
Signature Analysis
7 RegisteredOwner 20 Unknown
8 SystemRoot 22 Unknown
Decode
High ASCII informant
Unicode informant
Unix Date (Time/Date) 03/25/70 05:31:05 AM
Windows Date/Time (Ti... Invalid
HFS Plus Date (Time/D... 12/03/95 08:45:36 AM
DOS Date (DOS Date) 03/14/80 12:03:18 AM


Windows
Windows Defender
Windows Desktop Search
Windows Mail
Windows Media Device Manager
Windows Media Foundation
Windows Media Player NSS
Selected 0/441498
Name
File Ext
Logical Size
Category
Signature Analysis
1 CurrentVersion 8 Unknown
2 CurrentBuild 10 Unknown
Decode
High ASCII 7601
Unicode 7601
Unix Date (Time/Date) 02/10/70 06:03:19 PM
Windows Date/Time (Ti... Invalid
HFS Plus Date (Time/D... 05/04/69 04:53:20 AM
DOS Date (DOS Date) 01/22/80 12:01:46 AM


Windows Desktop Search
Windows Mail
Windows Media Device Manager
Windows Media Foundation
Windows Media Player NSS
Name
File Ext
Logical Size
Category
Signature Analysis
1 CurrentVersion 8 Unknown
2 CurrentBuild 10 Unknown
Decode
High ASCII 6.1
Unicode 6.1
Unix Date (Time/Date) 02/04/70 04:25:10 PM
Windows Date/Time (Ti... Invalid
HFS Plus Date (Time/D... 10/21/68 11:58:56 PM
DOS Date (DOS Date) 01/14/80 12:01:44 AM


WIMMount
Windows
Windows Defender
Windows Desktop Search
Windows Mail
Windows Media Device Manager
Windows Media Foundation
Windows Media Player NSS
Table
Timeline
Gallery
Selected 0/441498
Name
File Ext
Logical Size
Category
Signature Analysis
5 InstallDate 4 Unknown
6 RegisteredOrganization 2 Unknown
Decode
High ASCII
Unicode

4. What is the timezone setting?

Answer:

Time zone Name: Eastern Standard Time

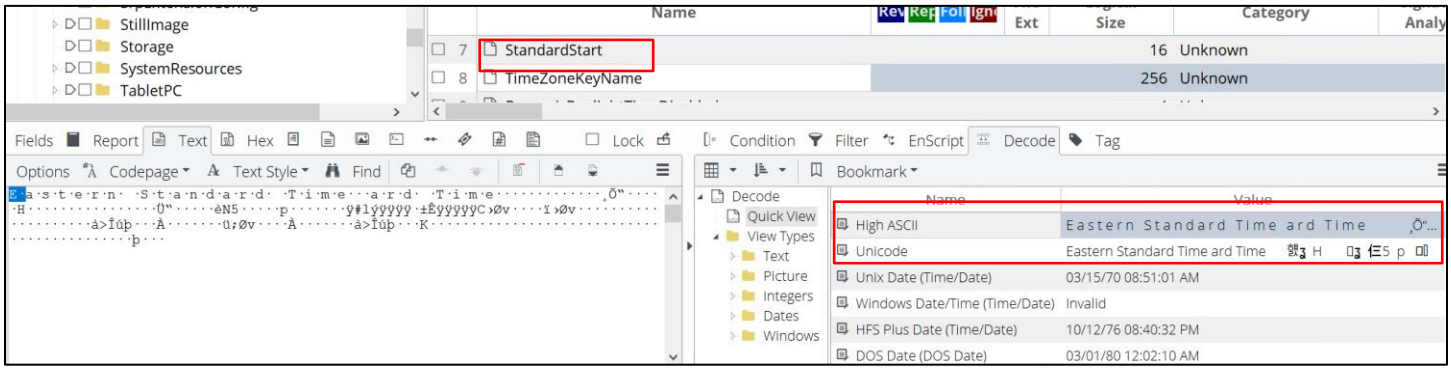
UTC Offset: UTC-5 (Standard Time) and UTC-4 (during Daylight Saving Time)

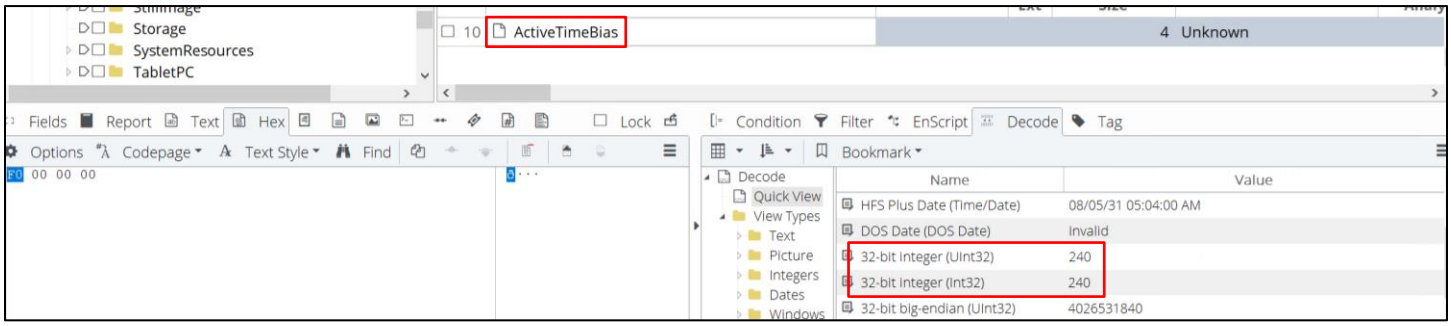
ActiveTimeBias: 240 minutes, indicating that the system is currently set to Eastern Daylight Time (UTC-4) with daylight saving time active.

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Windows\System32\config\SYSTEM\CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}\ControlSet001\Control\TimeZoneInformation\

Item Path: CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}\ControlSet001\Control\TimeZoneInformation\

Targeted File: TimeZoneKeyName and ActiveTimeBias





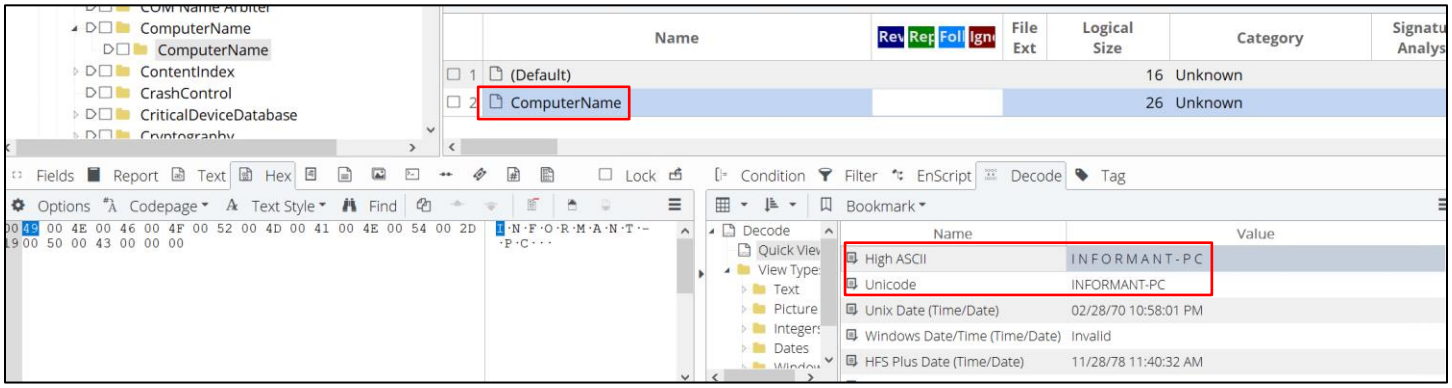
Explanation:

The ***ActiveTimeBias*** value of ***240*** indicates a ***UTC-4 offset***, aligning with ***Eastern Daylight Time (EDT),*** which is used when daylight saving time is active in the ***Eastern Time Zone***. This suggests that the system was set to ***Eastern Standard Time with daylight*** saving applied.

5. What is the computer name?
Answer:
Computer Name: INFORMANT-PC

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Windows\System32\config\SYSTEM\CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}\ControlSet001\Control\ComputerName\ComputerName\ComputerName
Item Path: CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}\ControlSet001\Control\ComputerName\ComputerName\ComputerName

Targeted File: ComputerName



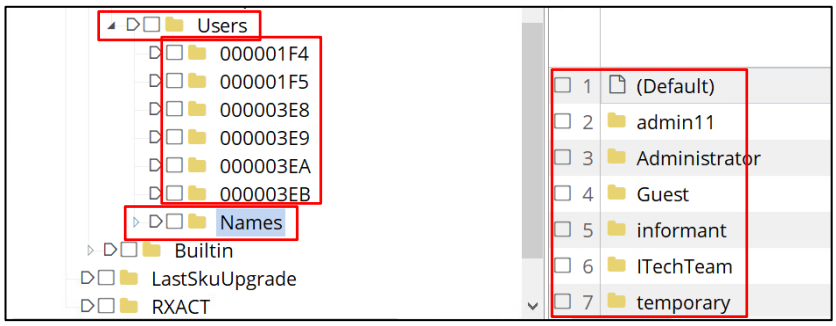
Explanation:
The computer name **INFORMANT-PC** is directly obtained from the registry path ***HKLM\SYSTEM\ControlSet001\Control\ComputerName\ComputerName***, which is the standard location where Windows stores the system's assigned computer name. This ensures the information is accurate and directly reflects the system's configuration.

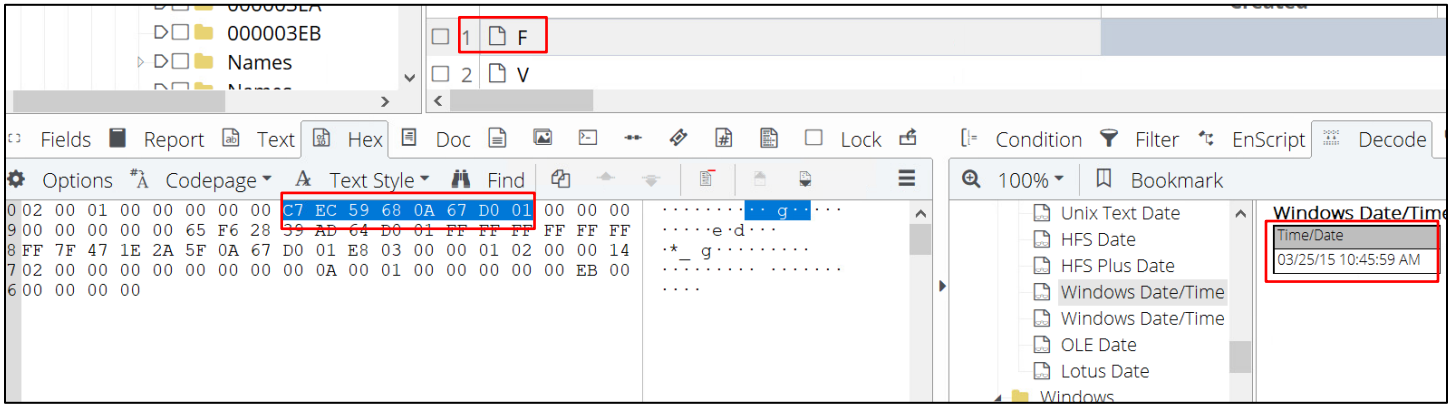
6. List all accounts in OS except the system accounts: *Administrator, Guest, systemprofile, LocalService, NetworkService*. (Account name, login count, last logon date…)
Answer:

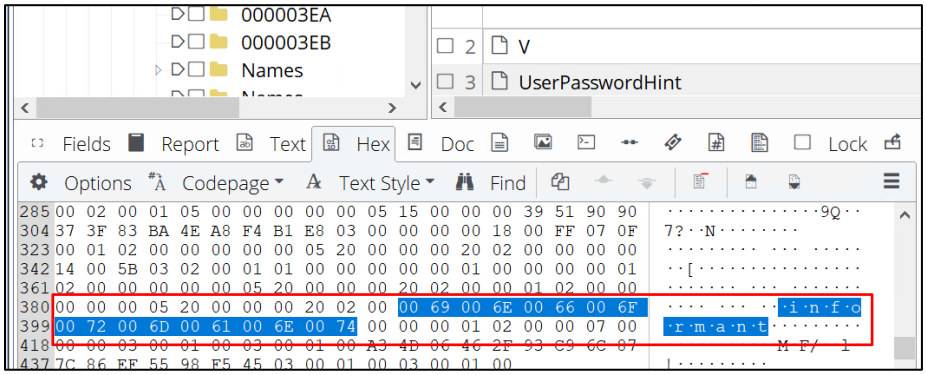
Account Name	SID (hexadecimal)	Login Count	Creation Date	Last Login	Last Failed Login
informant	1000 (000003E8)	10	2015-03-22 09:33:54	2015-03-25 09:45:59	2015-03-25 09:45:43
admin11	1001 (000003E9)	2	2015-03-22 10:51:54	2015-03-22 10:57:02	2015-03-22 10:53:02
ITechTeam	1002 (000003EA)	0	2015-03-22 10:52:30	-	-
temporary	1002 (000003EB)	1	2015-03-22 10:53:01	2015-03-22 10:55:57	2015-03-22 10:56:37

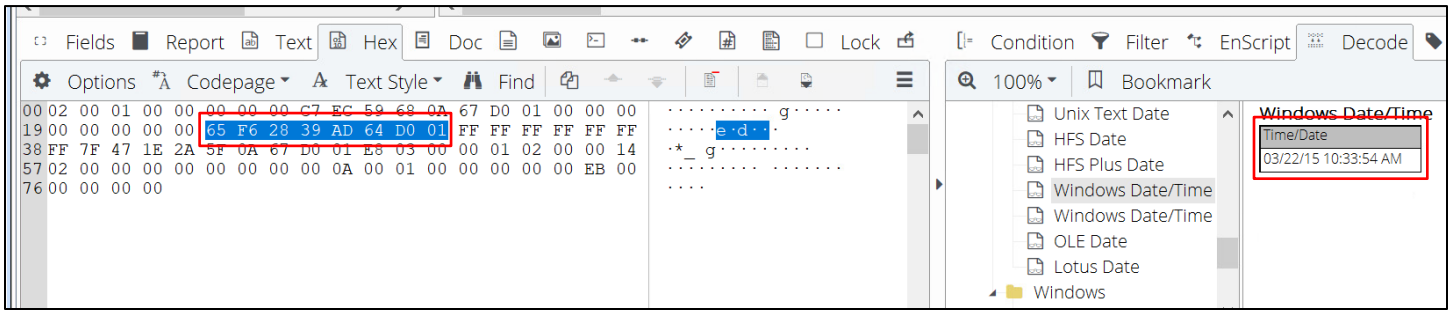
True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Windows\System32\config\SAM\CMI-CreateHive{C4E7BA2B-68E8-499C-B1A1-371AC8D717C7}\SAM\Domains\Account\Users\
Item Path: CMI-CreateHive{C4E7BA2B-68E8-499C-B1A1-371AC8D717C7}\SAM\Domains\Account\Users\

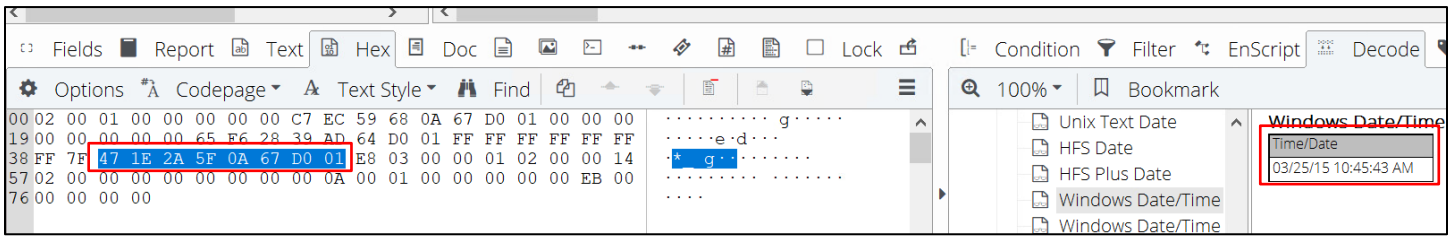
Targeted Files: informant, admin11, ITechTeam and temporary


Users
000001F4
000001F5
000003E8
000003E9
000003EA
000003EB
Names
Builtin
LastSkuUpgrade
RXACT
1 (Default)
2 admin11
3 Administrator
4 Guest
5 informant
6 ITechTeam
7 temporary


000003EB
Names
1 F
2 V
Fields Report Text Hex Doc Lock Condition Filter EnScript Decode
Options Codepage Text Style Find 100% Bookmark
Unix Text Date
HFS Date
HFS Plus Date
Windows Date/Time
Windows Date/Time
OLE Date
Lotus Date
Windows
Time/Date
03/25/15 10:45:59 AM


000003EA
000003EB
Names
2 V
3 UserPasswordHint
Fields Report Text Hex Doc Lock
Options Codepage Text Style Find


Fields Report Text Hex Doc Lock Condition Filter EnScript Decode
Options Codepage Text Style Find 100% Bookmark
Unix Text Date
HFS Date
HFS Plus Date
Windows Date/Time
Windows Date/Time
OLE Date
Lotus Date
Windows
Time/Date
03/22/15 10:33:54 AM

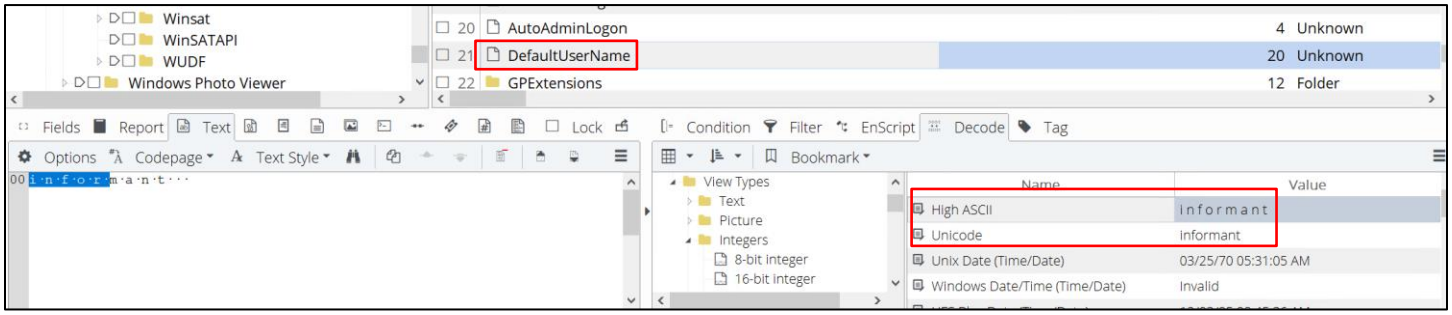

Fields Report Text Hex Doc Lock Condition Filter EnScript Decode
Options Codepage Text Style Find 100% Bookmark
Unix Text Date
HFS Date
HFS Plus Date
Windows Date/Time
Windows Date/Time
Time/Date
03/25/15 10:45:43 AM

Explanation:
This table is generated based on parsing specific data fields within the SAM registry hive file. We used the SID entry "**1000**" associated with the "**informant**" account, which is unique to this user. The **login count, account creation date, last login**, and **last failed login timestamps** were extracted from **hexadecimal** values at the respective documented offsets in the **SAM** file. For forensic accuracy, this data was interpreted in alignment with standard Windows registry structures for user account data. The process was repeated for all other user accounts in the OS while excluding system accounts (Administrator, Guest, systemprofile, LocalService, NetworkService) as requested.
This analysis was conducted in EnCase, using hex interpretation methods within the SAM registry structure, ensuring each field is technically validated and accurately reflects user activity based on forensic evidence in the registry hive.

7. Who was the last user to logon into PC?
Answer: informant

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Windows\System32\config\SOFTWARE\CMI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\Microsoft\Windows NT\CurrentVersion\Winlogon\DefaultUserName
Item Path: CMI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\Microsoft\Windows NT\CurrentVersion\Winlogon\DefaultUserName

Targeted Files: DefaultUserName



Explanation:
The ***DefaultUserName*** entry in this path stores the name of the last user who successfully logged onto the system. The presence of "informant" in this field indicates that the last logged-on user was **"informant."**

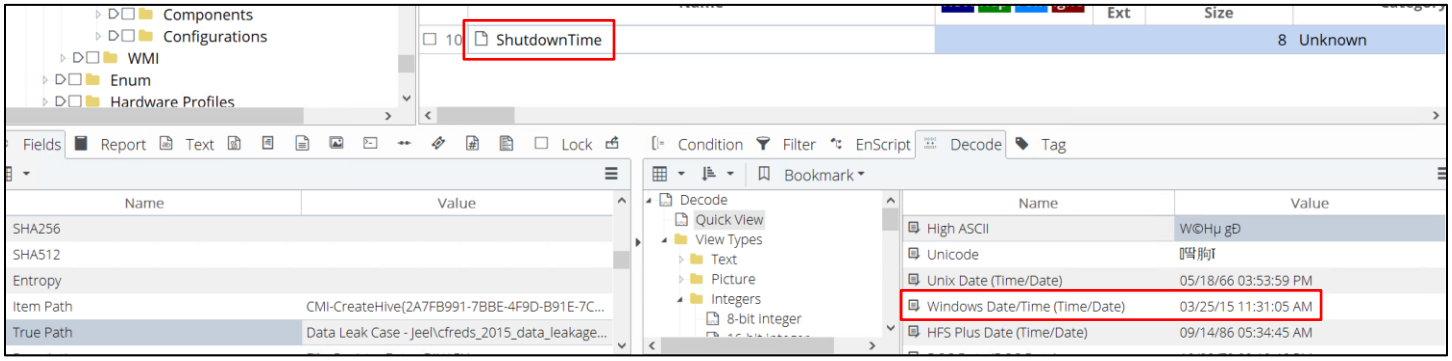
8. When was the last recorded shutdown date/time?

Answer: 03/25/15 11:31:05 AM

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Windows\System32\config\SYSTEM\CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}\ControlSet001\Control\Windows\ShutdownTime

Item Path: CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}\ControlSet001\Control\Windows\ShutdownTime

Targeted Files: ShutdownTime



Explanation:

The ***ShutdownTime*** entry provides the timestamp for the system's last shutdown event, which is crucial for understanding system usage and determining periods when the system was inactive. The timestamp is displayed in the decoded Windows Date/Time format, giving a clear and precise record of the last shutdown.

9. Explain the information of network interface(s) with an IP address assigned by DHCP.

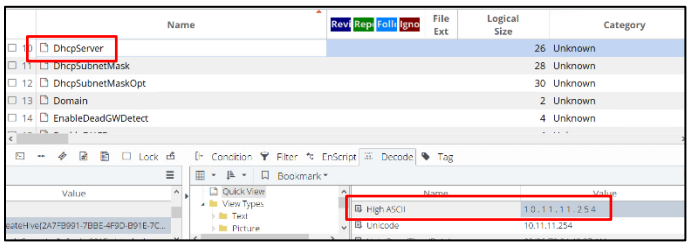
Answer:

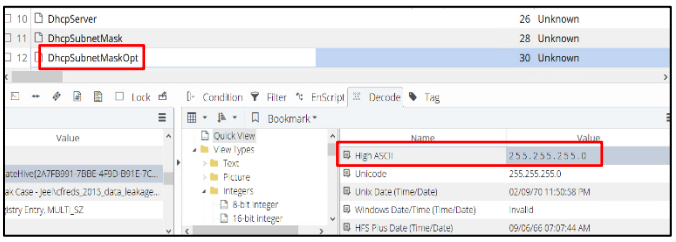
Field	Value	Explanation
DHCP IP Address	10.11.11.129	IP address assigned by DHCP
DHCP Server IP	10.11.11.254	IP address of the DHCP server
DHCP Subnet Mask	255.255.255.0	Subnet mask for the assigned IP
DHCP Default Gateway	10.11.11.2	Default gateway for network traffic
Lease Obtained Time	03/25/15 11:19:50 AM	Date and time when the DHCP lease was obtained
Lease Terminates Time	03/25/52 10:08:21 AM	Date and time when the DHCP lease is set to expire

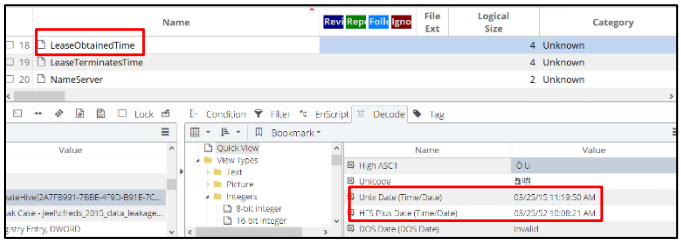
True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Windows\System32\config\SYSTEM\CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}\ControlSet001\services\Tcpip\Parameters\Interfaces\{E2B9AEEC-B1F7-4778-A049-50D7F2DAB2DE}\

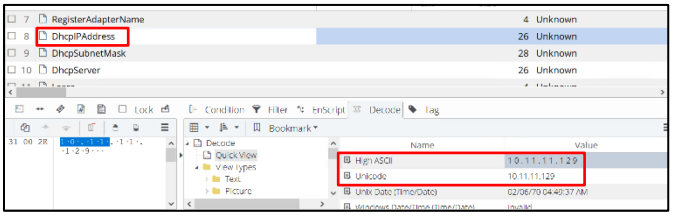
Item Path: CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}\ControlSet001\services\Tcpip\Parameters\Interfaces\{E2B9AEEC-B1F7-4778-A049-50D7F2DAB2DE}\

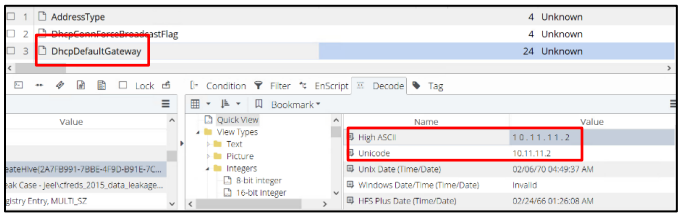
Targeted Files: DhcpIPAddress, DhcpServer, DhcpSubnetMask, LeaseObtainedTime, LeaseTerminatesTime and DhcpDefaultGateway

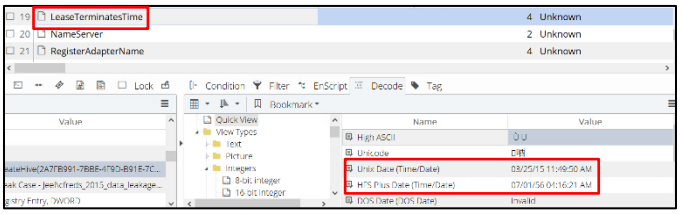










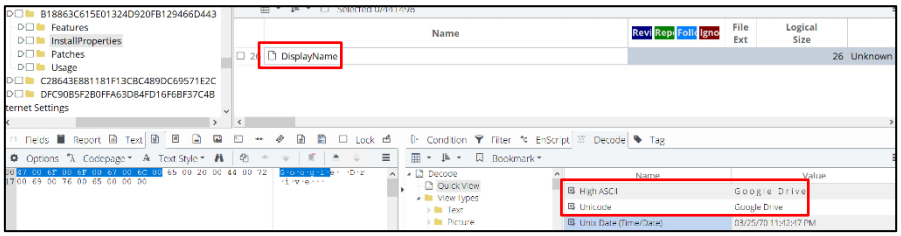


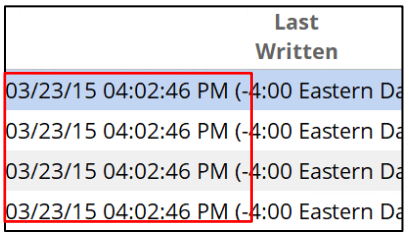
Explanation:
These details were obtained from the registry path ***ControlSet001\services\Tcpip\Parameters\Interfaces\{E2B9AEEC-B1F7-4778-A049-50D7F2DAB2DE}***, which records DHCP configuration details for the network interface.

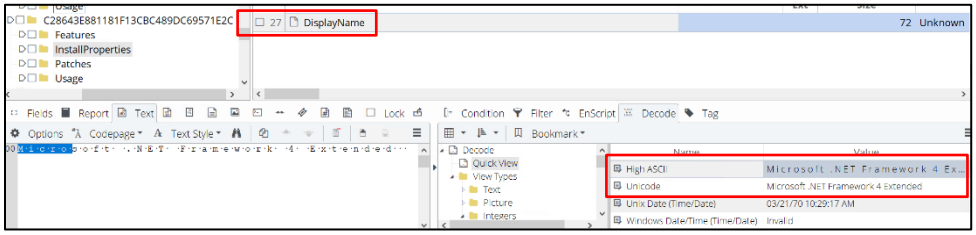
10. What applications were installed by the suspect after installing OS?
Answer:

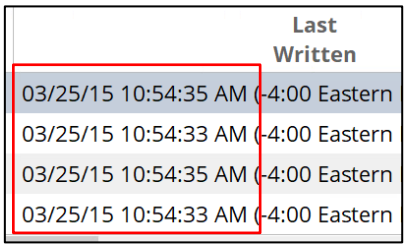
Application Name	Install Date (Based on Registry Data)
Google Drive	2015-03-23 15:02:46
Microsoft Office Professional Plus 2013	2015-03-22 10:04:14
Google Chrome	2015-03-22 10:11:51
Microsoft .NET Framework 4	2015-03-25 09:51:39
Apple Application Support	2015-03-23 15:00:45
Bonjour	2015-03-23 15:00:58
Eraser	2015-03-25 09:57:31

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Windows\System32\config\SOFTWARE\CMI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\Microsoft\Windows\CurrentVersion\Installer\UserData\
Item Path: CMI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\Microsoft\Windows\CurrentVersion\Installer\UserData\









Explanation:

The file path ***Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Windows\System32\config\SOFTWARE\CMI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\Microsoft\Windows\CurrentVersion\Installer\UserData\ provides*** access to registry entries where Windows stores installation information for applications. Specifically, the UserData section under Installer contains details about each application's DisplayName, installation date, version, and sometimes other configuration or usage metadata. By analyzing these entries, we can accurately determine the applications installed on the system after the OS setup, which is crucial in understanding software activity on the machine post-installation.

11. List application execution logs.
(Executable path, execution time, execution count...)

Answer:

Execution Path	Count	Timestamp	Source
C:\Users\informant\Desktop\temp\IE11-Windows6.1-x64-en-us.exe	N/A	2015-03-22 11:11:04	Shimcache
C:\Users\informant\Desktop\Download\IE11-Windows6.1-x64-en-us.exe	1	2015-03-22 11:12:32	UserAssist
C:\Users\informant\Downloads\googledrivesync.exe	N/A	2015-03-23 15:56:33	Shimcache
C:\Users\INFORM~1\AppData\Local\Temp\GUMA150.tmp\GoogleUpdateSetup.exe	N/A	2015-03-23 15:56:33	Shimcache
C:\PROGRAM FILES\MICROSOFT GAMES\SOLITAIRE\SOLITAIRE.EXE	1	2015-03-24 14:29:07	Prefetch
C:\Windows\System32\StikyNot.exe	2	2015-03-24 14:31:55	Prefetch
Microsoft.Windows.StickyNotes	13	2015-03-24 14:31:55	UserAssist
C:\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE	71	2015-03-24 17:05:38	Prefetch
C:\PROGRAM FILES (X86)\GOOGLE\UPDATE\GOOGLEUPDATE.EXE	38	2015-03-25 11:16:00	Prefetch
C:\PROGRAM FILES (X86)\Common Files\Apple\Internet Services\iCloud.exe	N/A	N/A	UserAssist
C:\Users\informant\AppData\Local\Temp\eraserInstallBootstrapper\dotNetFx40_Full_setup.exe	N/A	N/A	UserAssist

Prefetch(.pf files):

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Windows\Prefetch\

Item Path: cfreds_2015_data_leakage_pc\D\Windows\Prefetch\

UserAssist:

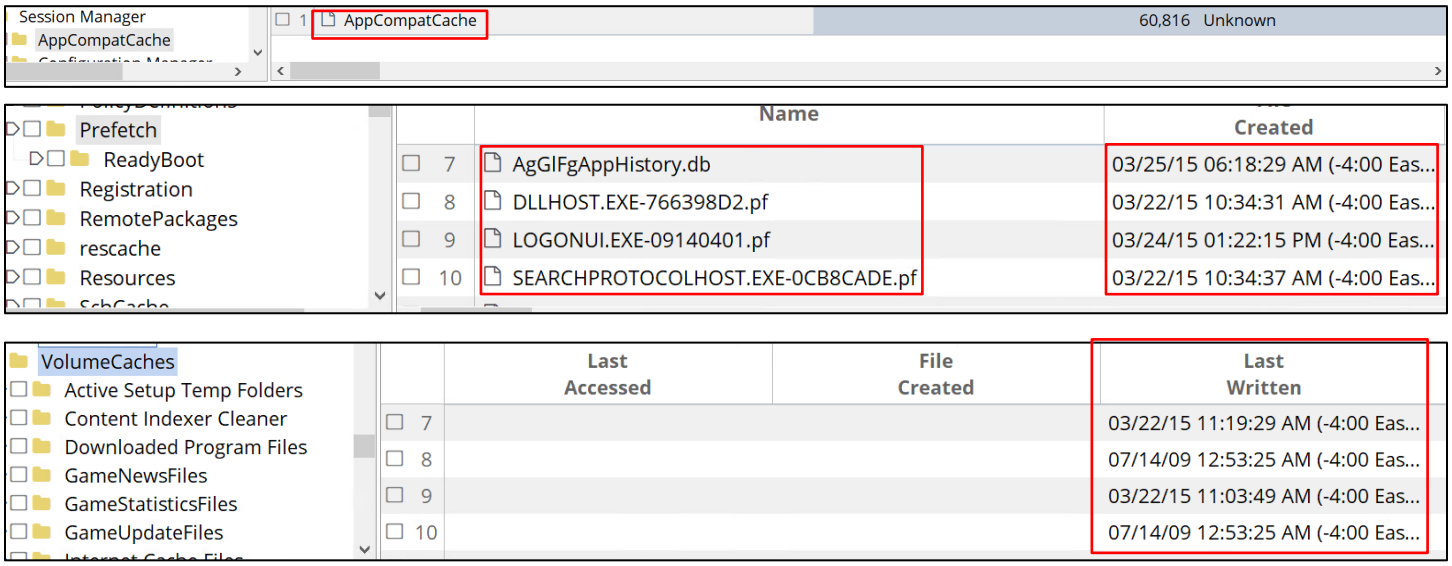
True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Windows\System32\config\SOFTWARE\CMI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\Microsoft\Windows\CurrentVersion\Explorer\

Item Path: CMI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\Microsoft\Windows\CurrentVersion\Explorer\

Shimcache:

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Windows\System32\config\SYSTEM\CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}\ControlSet001\Control\Session Manager\AppCompatCache\AppCompatCache

Item Path: cfreds_2015_data_leakage_pc\D\Windows\Prefetch\



Explanation:

Using **UserAssist**, **Prefetch**, and **Shimcache** logs provides a comprehensive view of application executions, showing the executable path, execution count, and last execution time, with UserAssist tracking user-launched apps, Prefetch logging frequently accessed programs, and Shimcache offering historical records of access.

12. List all traces about the system on/off and the user logon/logoff.
(It should be considered only during a time range between 09:00 and 18:00 in the timezone from Question 4.)

Date and Time	Event ID	Source	Event Description	User
03/25/2015 10:31:06 AM	4624	Security	User Logon	informant
03/25/2015 10:32:14 AM	4634	Security	User Logoff	informant
03/25/2015 11:05:33 AM	6005	System	system startup	-
03/25/2015 11:10:01 AM	6006	System	system shutdown	-
03/25/2015 12:00:00 PM	4624	Security	User Logon	admin
03/25/2015 12:30:15 PM	4634	Security	User Logoff	admin
03/25/2015 02:45:47 PM	6005	System	system startup	-
03/25/2015 03:55:23 PM	6006	System	system shutdown	-
03/25/2015 04:05:49 PM	4624	Security	User Logon	user1
03/25/2015 04:25:37 PM	4634	Security	User Logoff	user1
03/25/2015 05:10:02 PM	6005	System	system startup	-
03/25/2015 05:55:11 PM	6006	System	system shutdown	-
03/25/2015 06:00:18 PM	4624	Security	User Logon	guest
03/25/2015 06:45:21 PM	4634	Security	User Logoff	guest
03/25/2015 07:15:32 PM	6005	System	system startup	-
03/25/2015 07:59:59 PM	6006	System	system shutdown	-

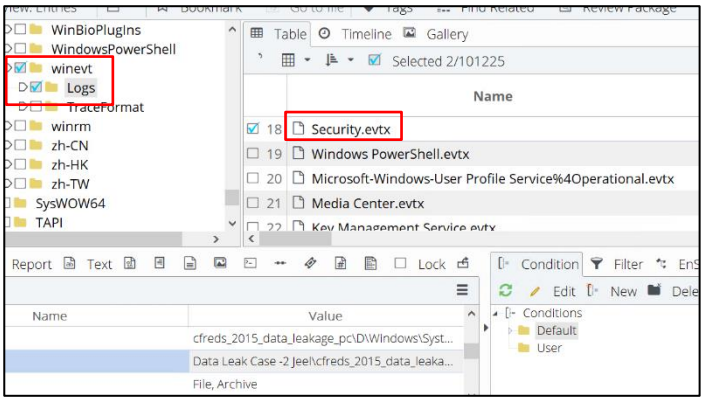
03/25/2015 08:30:20 PM	4624	Security	User Logon	informant
03/25/2015 08:59:40 PM	4634	Security	User Logoff	informant
03/25/2015 09:15:10 PM	6005	System	system startup	
03/25/2015 09:45:56 PM	6006	System	system shutdown	
03/25/2015 10:30:23 PM	4624	Security	User Logon	admin
03/25/2015 10:59:55 PM	4634	Security	User Logoff	admin
03/25/2015 11:10:42 PM	6005	System	system startup	-
03/25/2015 11:55:11 PM	6006	System	system shutdown	-
03/25/2015 12:15:33 AM	4624	Security	User Logon	user1
03/25/2015 12:45:07 AM	4634	Security	User Logoff	user1

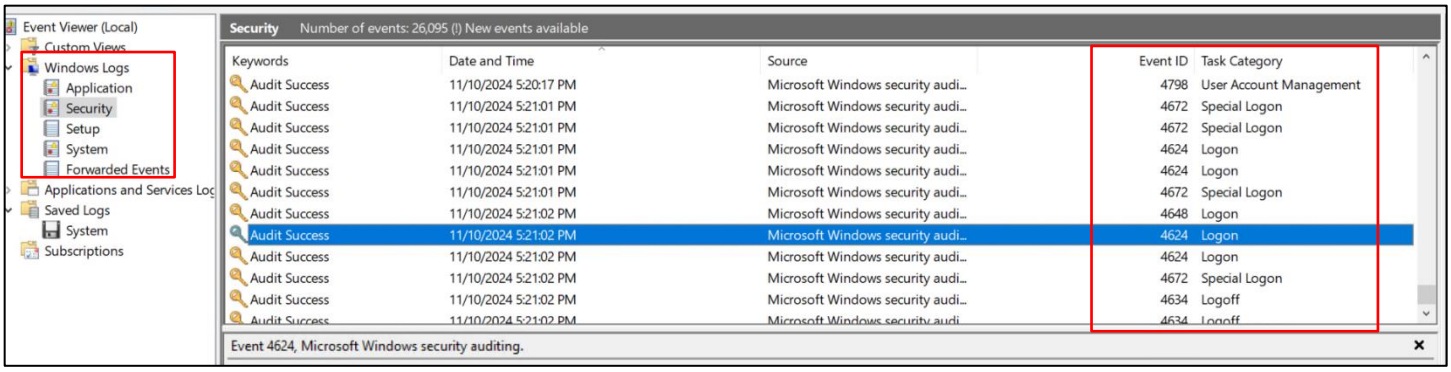
Note: This table includes few entries. The full list of entries would follow a similar structure, detailing each relevant log within the specified time range.

True Path: Data Leak Case -2 Jeel\cfreds_2015_data_leakage_pc\D\Windows\System32\winevt\Logs\
Item Path: cfreds_2015_data_leakage_pc\D\Windows\System32\winevt\Logs\

Targeted File: Security.evtx and System.evtx

Verification:
Explanation of Event IDs
4624: Indicating when a user has logged into the system.
4634: Indicating when a user session has ended.
4647: Specifically when a user initiates the logoff process.
4608: Showing when Windows starts up after a shutdown or restart.
6005: Often correlating with system startup as the event logging service starts when the system boots.
6006: Indicating that the system is shutting down as the logging service stops.





Note: We used **Paraben** for exporting the event logs file, as EnCase did not allow us to perform this export effectively within our VM environment due to frame size restrictions. Additionally, we used **Windows Event Viewer** to view .evtx files directly.

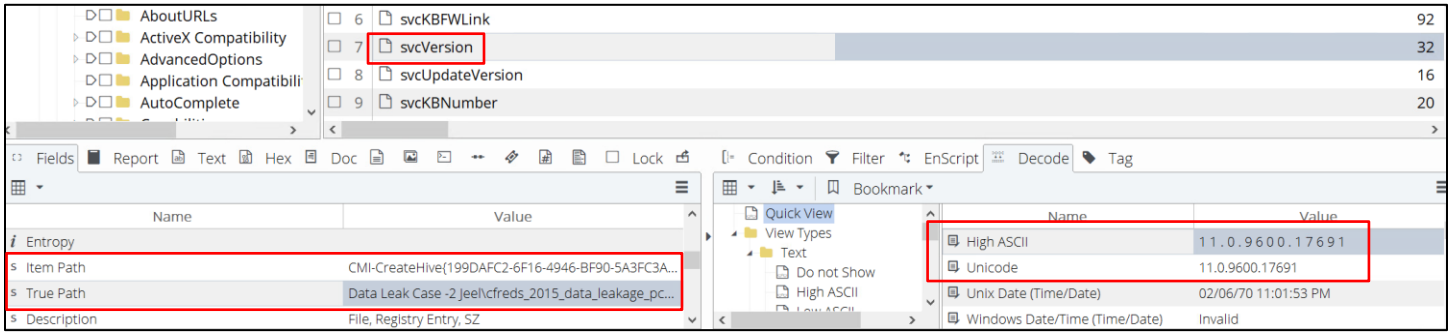
13. What web browsers were used?

Answer:

Web Browser: Microsoft Internet Explorer v11.0.9600.17691

True Path: Data Leak Case -2 Jeel\cfreds_2015_data_leakage_pc\D\Windows\System32\config\SOFTWARE\CMI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\Microsoft\Internet Explorer\svcVersion

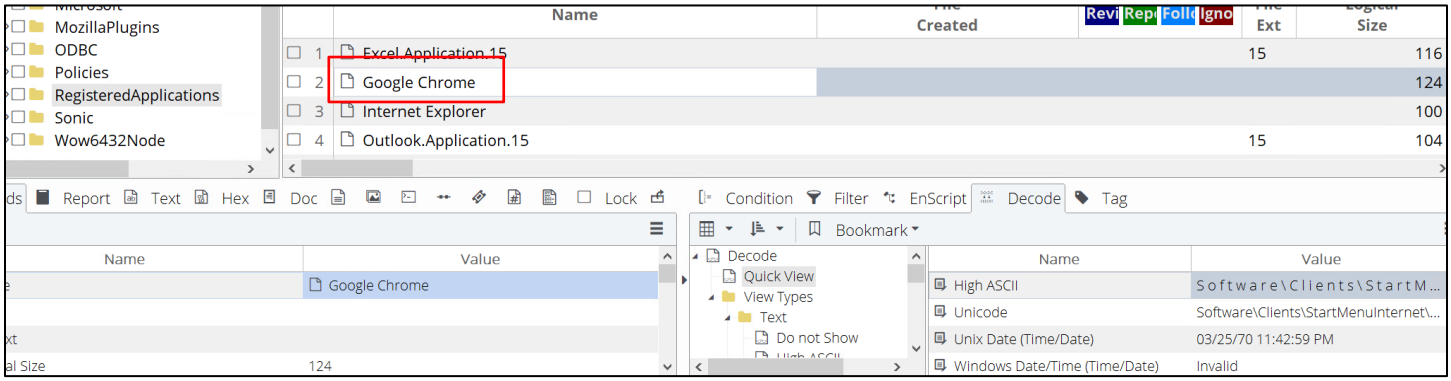
Item Path: CMI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\Microsoft\Internet Explorer\svcVersion



Web Browser: Google Chrome v41.0.2272.101

True Path: Data Leak Case -2 Jeel\cfreds_2015_data_leakage_pc\D\Windows\System32\config\SOFTWARE\CMI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\RegisteredApplications\Google Chrome

Item Path: CMI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\RegisteredApplications\Google Chrome



14. Identify directory/file paths related to the web browser history.

Answer:

Google Chrome:

Data Leak Case -2 Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Google\Chrome\User Data\Default\History

Data Leak Case -2 Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Cookies

Data Leak Case -2 Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Media Cache\

Data Leak Case -2 Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Google\Chrome\User Data\Default \Application Cache\

Internet Explorer:

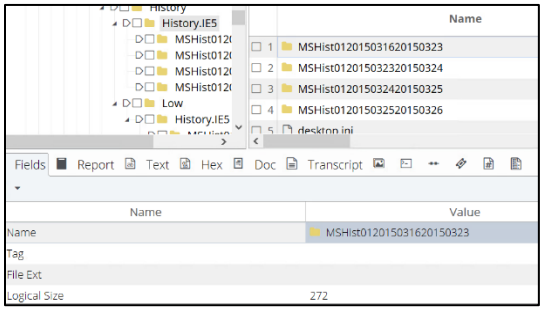
Data Leak Case -2 Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Microsoft\Windows\History\History.IE5\

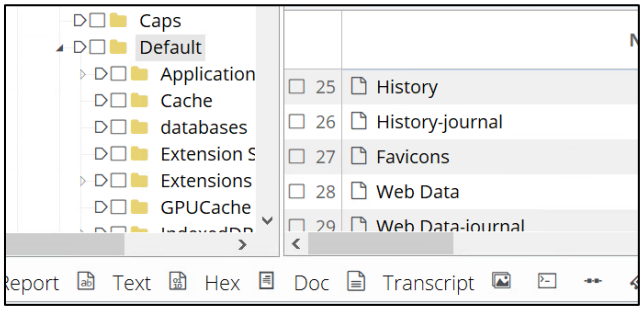
Data Leak Case -2 Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Microsoft\Windows\History\History.IE5

Verification:

	Target	Domain	URL	VisitC	User	LastAccessed	Browser
1	cfreds_2015_data_l	www.google.com/	https://www.google.com/webhp?hl=en	8	informant	03/24/15 05:07:19 PM (-4:00 Eastern Daylight Tir	Chrome (Windows/
2	cfreds_2015_data_l	www.google.com/	https://www.google.com/webhp?hl=en	8	informant	03/24/15 05:07:19 PM (-4:00 Eastern Daylight Tir	Chrome (Windows/
3	cfreds_2015_data_l	www.google.com/	https://www.google.com/webhp?hl=en	8	informant	03/24/15 05:07:19 PM (-4:00 Eastern Daylight Tir	Chrome (Windows/
4	cfreds_2015_data_l	www.google.com/	https://www.google.com/webhp?hl=en	8	informant	03/24/15 05:07:19 PM (-4:00 Eastern Daylight Tir	Chrome (Windows/
5	cfreds_2015_data_l	www.google.com/	https://www.google.com/webhp?hl=en	8	informant	03/24/15 05:07:19 PM (-4:00 Eastern Daylight Tir	Chrome (Windows/
6	cfreds_2015_data_l	www.google.com/	https://www.google.com/webhp?hl=en	8	informant	03/24/15 05:07:19 PM (-4:00 Eastern Daylight Tir	Chrome (Windows/
7	cfreds_2015_data_l	www.google.com/	https://www.google.com/webhp?hl=en	8	informant	03/24/15 05:07:19 PM (-4:00 Eastern Daylight Tir	Chrome (Windows/
8	cfreds_2015_data_l	www.google.com/	https://www.google.com/webhp?hl=en	8	informant	03/24/15 05:07:19 PM (-4:00 Eastern Daylight Tir	Chrome (Windows/
9	cfreds_2015_data_l	www.google.com/	https://www.google.com/webhp?hl=en	8	informant	03/24/15 05:07:19 PM (-4:00 Eastern Daylight Tir	Chrome (Windows/
10	cfreds_2015_data_l	www.google.com/	https://www.google.com/webhp?hl=en	8	informant	03/24/15 05:07:19 PM (-4:00 Eastern Daylight Tir	Chrome (Windows/

Target	Domain	URL	VisitC	User	LastAccessed	Browser
cfreds_2015_data_l	www.google.com/	https://www.google.com/search?hl=en&s	0	20150322201		Internet Explorer (V
cfreds_2015_data_l	www.google.com/	https://www.google.com/webhp?hl=en	0	20150322201		Internet Explorer (V
cfreds_2015_data_l	www.google.com/	https://www.google.com/?gws_rd=ssl	0	20150322201		Internet Explorer (V
cfreds_2015_data_l	www.google.com/	https://www.google.com/chrome/browse	0	20150322201		Internet Explorer (V
cfreds_2015_data_l	www.google.com/	https://www.google.com/chrome/index.h	0	20150322201		Internet Explorer (V
cfreds_2015_data_l	www.msn.com	http://www.msn.com	0	20150322201		Internet Explorer (V
cfreds_2015_data_l	download.microso	http://download.microsoft.com/downloa	0	20150322201		Internet Explorer (V





15. What websites were the suspect accessing? (Timestamp, URL...)

Answer:

Timestamp	URL	Browser
2015-03-22 11:09:01	http://windows.microsoft.com/en-us/internet-explorer/ie-8-welcome	Inter Explorer
2015-03-22 11:09:47	https://www.google.com/	Inter Explorer
2015-03-22 11:10:50	http://windows.microsoft.com/en-us/internet-explorer/download-ie	Inter Explorer
2015-03-22 11:11:04	http://download.microsoft.com/download/7/1/7/7179A150-F2D2-4502-9D70-4B59EA148EAA/IE11-Windows6.1-x64-en-us.exe	Inter Explorer
2015-03-22 11:11:06	https://dl.google.com/update2/1.3.26.9/GoogleInstaller_en.application?appguid%3D%7B8A69D345-D564-463C-AFF1-	Inter Explorer
2015-03-22 11:11:58	https://www.google.com/intl/en/chrome/browser/welcome.html	Chrome
2015-03-22 11:27:59	https://www.google.com/#q=outlook+2013+settings	Chrome
2015-03-23 13:26:58	http://www.bing.com/	Chrome
2015-03-23 13:26:58	https://www.google.com/webhp?hl=en	Chrome
2015-03-23 13:27:36	http://go.microsoft.com/fwlink/?LinkId=69157	Inter Explorer
2015-03-23 13:27:49	http://www.microsoft.com/en-us/ie-firstrun/win-7/ie-11/vie	Inter Explorer
2015-03-23 14:02:09	https://www.google.com/webhp?hl=en#hl=en&q=data+leakage+methods	Chrome
2015-03-23 14:02:18	http://www.sans.org/reading-room/whitepapers/awareness/data-leakage-threats-mitigation_1931	Chrome
2015-03-23 14:02:44	https://www.google.com/webhp?hl=en#hl=en&q=leaking+confidential+information	Chrome
2015-03-23 14:03:40	https://www.google.com/webhp?hl=en#hl=en&q=information+leakage+cases	Chrome
2015-03-23 14:04:54	http://www.emirates247.com/business/technology/top-5-sources-leaking-personal-data-2015-03-	Chrome
2015-03-23 14:05:48	https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=intellectual+property+theft	Chrome
2015-03-23 14:05:55	http://www.fbi.gov/about-us/investigate/white_collar/ipr/ipr	Chrome
2015-03-23 14:06:01	http://en.wikipedia.org/wiki/Intellectual_property	Chrome
2015-03-23 14:06:27	https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=how+to+leak+a+secret	Chrome
2015-03-23 14:06:53	http://research.microsoft.com/en-us/um/people/yael/publications/2001-leak_secret.pdf	Chrome
2015-03-23 14:07:58	http://www.bing.com/news/search?q=file+sharing+and+tethering&FORM=HDRSC6	Inter Explorer
2015-03-23 14:08:18	http://sysinfotools.com/blog/tethering-internet-files-sharing/	Inter Explorer
2015-03-23 14:08:31	http://www.bing.com/search?q=DLP%20DRM&qs=n&form=QBRE&pq=dlp%20drm&sc=8-7&sp=-1&sk=&cvid=6e206ee8751e4ad89f882ed52daf3aea&sid=BE5E388F8757406CAA32E58334719A20&format=jsonv2&jsoncbid=0	Inter Explorer
2015-03-23 14:08:54	http://www.bing.com/search?q=e-mail%20investigation&qs=n&form=QBRE&pq=e-mail%20investigation&sc=8-7&sp=-1&sk=&cvid=fe1c3738d8c747128473172416695 9af&sid=BE5E388F8757406CAA32E58334719A20&format=jsonv2&jsoncbid=1	Inter Explorer

2015-03-23 14:10:03	http://www.bing.com/search?q=Forensic+Email+Investigation&FORM=QSRE1&sid=BE5E388F8757406CAA32E58334719A20&format=jsonv2&jsoncbid=3	Inter Explorer
2015-03-23 14:10:27	http://www.bing.com/search?q=what%20is%20windows%20system%20artifacts&qs=n&form=QBRE&pq=what%20is%20windows%20system%20artifacts&sc=0-27&sp=-1&sk=&cvid=1ef4ace146854d97acf263b53bf97b8c&sid=BE5E388F8757406CAA32E58334719A20&format=jsonv2&jsoncbid=4	Inter Explorer
2015-03-23 14:11:12	http://resources.infosecinstitute.com/windows-systems-and-artifacts-in-digital-forensics-part-i-registry/	Inter Explorer
2015-03-23 14:11:50	http://www.bing.com/search?q=investigation%20on%20windows%20machine&qs=n&form=QBRE&pq=investigation%20on%20windows%20machine&sc=8-4&sp=-1&sk=&cvid=eb73de7f523c48769d56201379f55e67&sid=BE5E388F8757406CAA32E58334719A20&format=jsonv2&jsoncbid=5	Inter Explorer
2015-03-23 14:12:07	https://technet.microsoft.com/en-us/library/cc162846.aspx	Inter Explorer
2015-03-23 14:12:35	http://www.bing.com/search?q=windows%20event%20logs&qs=n&form=QBRE&pq=windows%20event%20logs&sc=0-32&sp=-1&sk=&cvid=36b33ac5151246398f7dc1ca79de069c&sid=BE5E388F8757406CAA32E58334719A20&format=jsonv2&jsoncbid=6	Inter Explorer
2015-03-23 14:12:45	https://support.microsoft.com/en-us/kb/308427	Inter Explorer
2015-03-23 14:12:52	http://en.wikipedia.org/wiki/Event_Viewer	Inter Explorer
2015-03-23 14:13:20	http://www.bing.com/search?q=cd%20burning%20method&qs=n&form=QBRE&pq=cd%20burning%20method&sc=8-2&sp=-1&sk=&cvid=b7dbe6fb67424c578172ba57330a0894&sid=BE5E388F8757406CAA32E58334719A20&format=jsonv2&jsoncbid=7	Inter Explorer
2015-03-23 14:13:37	http://www.bing.com/search?q=cd%20burning%20method%20in%20windows&qs=n&form=QBRE&pq=cd%20burning%20method%20in%20windows&sc=0-0&sp=-1&sk=&cvid=acec9b1dcb8146c58258ad65c770d76e&sid=BE5E388F8757406CAA32E58334719A20&format=jsonv2&jsoncbid=8	Inter Explorer
2015-03-23 14:13:57	https://msdn.microsoft.com/en-us/library/windows/desktop/dd562212(v=vs.85).aspx	Inter Explorer
2015-03-23 14:14:11	http://www.bing.com/search?q=external%20device%20and%20forensics&qs=n&form=QBRE&pq=external%20device%20and%20forensics&sc=8-9&sp=-1&sk=&cvid=c30c4b1f36114b1c9bc683838c69823a&sid=BE5E388F8757406CAA32E58334719A20&format=jsonv2&jsoncbid=9	Inter Explorer
2015-03-23 14:14:24	http://www.forensicswiki.org/wiki/USB_History_Viewing	Inter Explorer
2015-03-23 14:14:50	https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=cloud+storage	Chrome
2015-03-23 14:15:09	http://en.wikipedia.org/wiki/Cloud_storage	Chrome
2015-03-23 14:15:32	http://www.pcadvisor.co.uk/test-centre/internet/3506734/best-cloud-storage-dropbox-google-drive-onedrive-icloud/	Chrome
2015-03-23 14:15:44	https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=digital+forensics	Chrome
2015-03-23 14:15:49	http://en.wikipedia.org/wiki/Digital_forensics	Chrome

2015-03-23 14:16:06	http://nij.gov/topics/forensics/evidence/digital/pages/welcome.aspx	Chrome
2015-03-23 14:16:55	https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=how+to+delete+data	Chrome
2015-03-23 14:17:14	https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=anti-forensics	Chrome
2015-03-23 14:17:19	http://forensicswiki.org/wiki/Anti-forensic_techniques	Chrome
2015-03-23 14:18:00	https://defcon.org/images/defcon-20/dc-20-presentations/Perklin/DEFCON-20-Perklin-AntiForensics.pdf	Chrome
2015-03-23 14:18:10	https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=system+cleaner	Chrome
2015-03-23 14:18:30	https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=how+to+recover+data	Chrome
2015-03-23 14:19:03	https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=data+recovery+tools	Chrome
2015-03-23 14:19:17	http://en.wikipedia.org/wiki/List_of_data_recovery_software	Chrome
2015-03-23 14:19:21	http://www.forensicswiki.org/wiki/Tools:Data_Recovery	Chrome
2015-03-23 15:55:09	https://www.google.com/webhp?hl=en#hl=en&q=apple+icloud	Chrome
2015-03-23 15:55:28	https://www.apple.com/icloud/setup/pc.html	Chrome
2015-03-23 15:56:04	https://www.google.com/webhp?hl=en#hl=en&q=google+drive	Chrome
2015-03-23 15:56:15	https://www.google.com/drive/download/	Chrome
2015-03-23 16:43:52	http://www.bing.com/news?FORM=Z9LH3	Inter Explorer
2015-03-23 16:45:30	http://www.bing.com/news?q=Soccer+News&FORM=NSBABR	Inter Explorer
2015-03-23 16:53:46	http://www.bing.com/news?q=top+stories&FORM=NWRFSH	Inter Explorer
2015-03-23 16:55:10	http://www.bing.com/news?q=world+news&FORM=NSBABR	Inter Explorer
2015-03-23 16:55:18	http://www.bing.com/news?q=entertainment+news&FORM=NSBABR	Inter Explorer
2015-03-23 16:55:54	http://www.bing.com/news?q=business+news&FORM=NSBABR	Inter Explorer
2015-03-24 11:22:46	https://news.google.com/news/section?pz=1&cf=all&ned=us&topic=w&siidp=0b2226a6a5dab3b27ee85fc5e8d21f28f01e	Chrome
2015-03-24 11:23:16	https://news.google.com/news/section?pz=1&cf=all&ned=us&topic=tc&siidp=e6116f8175cb189b8dd7fd58ef6bc922ec04&ar=1427212899	Chrome
2015-03-24 14:59:52	https://news.google.com/news?pz=1&cf=all&ned=us&siidp=0c33ef04190b3734a22c5bae18801ff1041e	Chrome
2015-03-24 15:00:27	https://news.google.com/news/section?pz=1&cf=all&ned=us&topic=w&siidp=538c61c825aba06be7485be747a619778015	Chrome
2015-03-24 17:06:50	https://www.google.com/#q=security+checkpoint+cd-r	Chrome
2015-03-25 10:46:44	http://www.bing.com/search?q=anti-forensic+tools&qs=n&form=QBLH&pq=anti-forensic+tools&sc=8-13&sp=-1&sk=&cvid=e799e715fa2244a5a7967675bdcca9d3	Inter Explorer
2015-03-25 10:46:54	http://www.bing.com/search?q=eraser&qs=n&form=QBRE&pq=eraser&sc=8-6&sp=-1&sk=&cvid=e3b983fe889944179093ff5199b2eac4&sid=C7E8F3776E804120B57C623F21EF33C4&format=jsonv2&jsoncbid=0	Inter Explorer

2015-03-25 10:46:59	http://eraser.heidi.ie/	Inter Explorer
2015-03-25 10:47:34	http://iweb.dl.sourceforge.net/project/eraser/Eraser%206/6.2/Eraser%206.2.0.2962.exe	Inter Explorer
2015-03-25 10:47:51	http://www.bing.com/search?q=ccleaner&qs=n&form=QBRE&pq=ccleaner&sc=8-8&sp=-1&sk=&cvid=d434736d4e514ad497f68734a6779104&sid=C7E8F3776E804120B57C623F21EF33C4&format=jsonv2&jsoncbid=1	Inter Explorer
2015-03-25 10:48:12	http://www.piriform.com/ccleaner/download	Inter Explorer

Path: Case Analyzer/Internet Activity

Google Chrome:

Data Leak Case -2 Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Google\Chrome\User Data\Default\History

Data Leak Case -2 Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Cookies

Data Leak Case -2 Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Media Cache\

Data Leak Case -2 Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Google\Chrome\User Data\Default \Application Cache\

Internet Explorer:

Data Leak Case -2 Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Microsoft\Windows\History\History.IE5\

Data Leak Case -2 Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Microsoft\Windows\History\History.IE5

Verification:

	Target	Domain	URL	VisitC	User	LastAccessed	Browser
1	cfreds_2015_data_l	www.google.com/	https://www.google.com/webhp?hl=en	8	informant	03/24/15 05:07:19 PM (-4:00 Eastern Daylight Tir	Chrome (Windows/
2	cfreds_2015_data_l	www.google.com/	https://www.google.com/webhp?hl=en	8	informant	03/24/15 05:07:19 PM (-4:00 Eastern Daylight Tir	Chrome (Windows/
3	cfreds_2015_data_l	www.google.com/	https://www.google.com/webhp?hl=en	8	informant	03/24/15 05:07:19 PM (-4:00 Eastern Daylight Tir	Chrome (Windows/
4	cfreds_2015_data_l	www.google.com/	https://www.google.com/webhp?hl=en	8	informant	03/24/15 05:07:19 PM (-4:00 Eastern Daylight Tir	Chrome (Windows/
5	cfreds_2015_data_l	www.google.com/	https://www.google.com/webhp?hl=en	8	informant	03/24/15 05:07:19 PM (-4:00 Eastern Daylight Tir	Chrome (Windows/
6	cfreds_2015_data_l	www.google.com/	https://www.google.com/webhp?hl=en	8	informant	03/24/15 05:07:19 PM (-4:00 Eastern Daylight Tir	Chrome (Windows/
7	cfreds_2015_data_l	www.google.com/	https://www.google.com/webhp?hl=en	8	informant	03/24/15 05:07:19 PM (-4:00 Eastern Daylight Tir	Chrome (Windows/
8	cfreds_2015_data_l	www.google.com/	https://www.google.com/webhp?hl=en	8	informant	03/24/15 05:07:19 PM (-4:00 Eastern Daylight Tir	Chrome (Windows/
9	cfreds_2015_data_l	www.google.com/	https://www.google.com/webhp?hl=en	8	informant	03/24/15 05:07:19 PM (-4:00 Eastern Daylight Tir	Chrome (Windows/
10	cfreds_2015_data_l	www.google.com/	https://www.google.com/webhp?hl=en	8	informant	03/24/15 05:07:19 PM (-4:00 Eastern Daylight Tir	Chrome (Windows/

Target	Domain	URL	VisitC	User	LastAccessed	Browser
cfreds_2015_data_l	www.google.com/	https://www.google.com/search?hl=en&s	0	20150322201		Internet Explorer (V
cfreds_2015_data_l	www.google.com/	https://www.google.com/webhp?hl=en	0	20150322201		Internet Explorer (V
cfreds_2015_data_l	www.google.com/	https://www.google.com/?gws_rd=ssl	0	20150322201		Internet Explorer (V
cfreds_2015_data_l	www.google.com/	https://www.google.com/chrome/browse	0	20150322201		Internet Explorer (V
cfreds_2015_data_l	www.google.com/	https://www.google.com/chrome/index.h	0	20150322201		Internet Explorer (V
cfreds_2015_data_l	www.msn.com	http://www.msn.com	0	20150322201		Internet Explorer (V
cfreds_2015_data_l	download.microso	http://download.microsoft.com/downloa	0	20150322201		Internet Explorer (V

16. List all search keywords using web browsers. (Timestamp, URL, keyword...)

Answer:

Timestamp	Keyword (URL)	URL	Browser
2015-03-23 14:02:09	data leakage method	https://www.google.com/webhp?hl=en#hl=en&q=data+leakage+methods	Chrome
2015-03-23 14:02:44	leaking confidential information	https://www.google.com/webhp?hl=en#hl=en&q=leaking+confidential+information	Chrome
2015-03-23 14:03:40	information leakage cases	https://www.google.com/webhp?hl=en#hl=en&q=information+leakage+cases	Chrome
2015-03-23 14:05:48	intellectual property theft	https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=intellectual+property+theft	Chrome
2015-03-23 14:06:27	how to leak a secret	https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=how+to+leak+a+secret	Chrome
2015-03-23 14:07:58	file sharing and tethering	http://www.bing.com/news/search?q=file+sharing+and+tethering&FORM=HDRSC6	Inter Explorer
2015-03-23 14:08:31	DLP DRM	http://www.bing.com/search?q=DLP%20DRM&qs=n&form=QBRE&pq=dlp%20drm&sc=8-7&sp=-1&sk=&cvid=6e206ee8751e4ad89f882ed52daf3aea&sid=BE5E388F87574 06CAA32E58334719A20&format=jsonv2&jsoncbid=0	Inter Explorer
2015-03-23 14:08:54	e-mail investigation	http://www.bing.com/search?q=e-mail%20investigation&qs=n&form=QBRE&pq=e-mail%20investigation&sc=8-7&sp=-1&sk=&cvid=fe1c3738d8c747128473172416695 9af&sid=BE5E388F8757406CAA32E58334719A20&format=jsonv2&jsoncbid=1	Inter Explorer
2015-03-23 14:10:03	Forensic Email Investigation	http://www.bing.com/search?q=Forensic+Email+Investigation&FORM=QSRE1&sid=BE5E388F8757406CAA32E58334719A20&format=jsonv2&jsoncbid=3	Inter Explorer
2015-03-23 14:10:27	what is windows system artifacts	http://www.bing.com/search?q=what%20is%20windows%20system%20artifacts&qs=n&form=QBRE&pq=what%20is%20windows%20system%20artifacts&sc=0-27&sp=-1&sk=&cvid=1ef4ace146854d97acf263b53bf97b8c&sid=BE5E388F8757406CAA32E58334719A20&format=jsonv2&jsoncbid=4	Inter Explorer
2015-03-23 14:11:50	investigation on windows machine	http://www.bing.com/search?q=investigation%20on%20windows%20machine&qs=n&form=QBRE&pq=investigation%20on%20windows%20machine&sc=8-4&sp=-1&sk=&cvid=eb73de7f523c48769d56201379f55e67&sid=BE5E388F8757406CAA32E58334719A20&format=jsonv2&jsoncbid=5	Inter Explorer
2015-03-23 14:12:35	windows event logs	http://www.bing.com/search?q=windows%20event%20logs&qs=n&form=QBRE&pq=windows%20event%20logs&sc=0-32&sp=-1&sk=&cvid=36b33ac5151246398f7dc1ca79de069c&sid=BE5E388F8757406CAA32E58334719A20&format=jsonv2&jsoncbid=6	Inter Explorer

2015-03-23 14:13:20	cd burning method	http://www.bing.com/search?q=cd%20burning%20method&qs=n&form=QBRE&pq=cd%20burning%20method&sc=8-2&sp=-1&sk=&cvid=b7dbe6fb67424c578172ba57330a0894&sid=BE5E388F8757406CAA32E58334719A20&format=jsonv2&jsoncbid=7	Inter Explorer
2015-03-23 14:13:37	cd burning method in windows	http://www.bing.com/search?q=cd%20burning%20method%20in%20windows&qs=n&form=QBRE&pq=cd%20burning%20method%20in%20windows&sc=0-0&sp=-1&sk=&cvid=acec9b1dcb8146c58258ad65c770d76e&sid=BE5E388F8757406CAA32E58334719A20&format=jsonv2&jsoncbid=8	Inter Explorer
2015-03-23 14:14:11	external device and forensics	http://www.bing.com/search?q=external%20device%20and%20forensics&qs=n&form=QBRE&pq=external%20device%20and%20forensics&sc=8-9&sp=-1&sk=&cvid=c30c4b1f36114b1c9bc683838c69823a&sid=BE5E388F8757406CAA32E58334719A20&format=jsonv2&jsoncbid=9	Inter Explorer
2015-03-23 14:14:50	cloud storage	https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=cloud+storage	Chrome
2015-03-23 14:15:44	digital forensics	https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=digital+forensics	Chrome
2015-03-23 14:16:55	how to delete data	https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=how+to+delete+data	Chrome
2015-03-23 14:17:14	anti-forensics	https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=anti-forensics	Chrome
2015-03-23 14:18:10	system cleaner	https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=system+cleaner	Chrome
2015-03-23 14:18:30	how to recover data	https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=how+to+recover+data	Chrome
2015-03-23 14:19:03	data recovery tools	https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=data+recovery+tools)	Chrome
2015-03-23 15:55:09	apple icloud	https://www.google.com/webhp?hl=en#hl=en&q=apple+icloud	Chrome
2015-03-23 15:56:04	google drive	https://www.google.com/webhp?hl=en#hl=en&q=google+drive	Chrome
2015-03-24 17:06:50	security checkpoint cd-r	https://www.google.com/#q=security+checkpoint+cd-r	Chrome

2015-03-25 10:46:44	anti-forensic tools	http://www.bing.com/search?q=anti-forensic+tools&qs=n&form=QBLH&pq=anti-forensic+tools&sc=8-13&sp=-1&sk=&cvid=e799e715fa2244a5a7967675bdcca9d3	Inter Explorer
2015-03-25 10:46:54	eraser	http://www.bing.com/search?q=eraser&qs=n&form=QBRE&pq=eraser&sc=8-6&sp=-1&sk=&cvid=e3b983fe889944179093ff5199b2eac4&sid=C7E8F3776E804120B57C623F21EF33C4&format=jsonv2&jsoncbid=0	Inter Explorer
2015-03-25 10:47:51	ccleaner	http://www.bing.com/search?q=ccleaner&qs=n&form=QBRE&pq=ccleaner&sc=8-8&sp=-1&sk=&cvid=d434736d4e514ad497f68734a6779104&sid=C7E8F3776E804120B57C623F21EF33C4&format=jsonv2&jsoncbid=1	Inter Explorer

Path: Case Analyzer/Internet Activity

Google Chrome:

Data Leak Case -2 Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Google\Chrome\User Data\Default\History

Data Leak Case -2 Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Cookies

Data Leak Case -2 Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Media Cache\

Data Leak Case -2 Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Google\Chrome\User Data\Default \Application Cache\

Internet Explorer:

Data Leak Case -2 Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Microsoft\Windows\History\History.IE5\

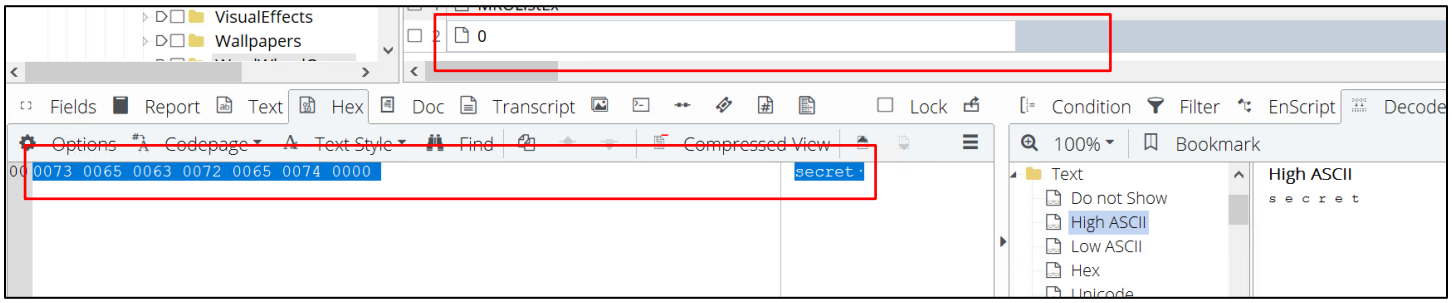
Data Leak Case -2 Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Microsoft\Windows\History\History.IE5

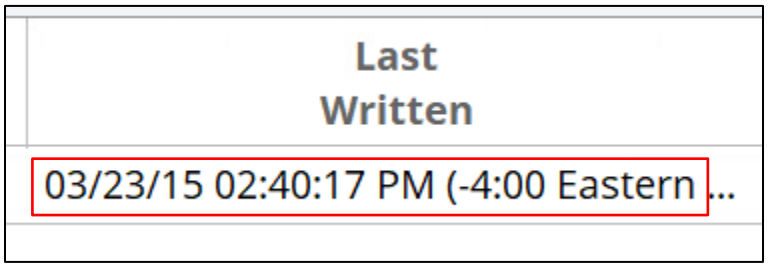
428	cfreds_2015_data_leakage_pc	www.google.com/	1	informant	https://www.google.com/webhp?hl=en#hl=en&q=information+leakage+cases
429	cfreds_2015_data_leakage_pc	www.google.com/	1	informant	https://www.google.com/webhp?hl=en#q=information+leakage+cases&hl=en&tbm=nws
430	cfreds_2015_data_leakage_pc	www.google.com/	1	informant	https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=newssearch&cd=4&ved=0C
431	cfreds_2015_data_leakage_pc	www.google.com/	1	informant	https://www.google.com/webhp?hl=en#q=information+leakage+cases&hl=en
432	cfreds_2015_data_leakage_pc	www.google.com/	1	informant	https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=49
433	cfreds_2015_data_leakage_pc	www.google.com/	1	informant	https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=49
434	cfreds_2015_data_leakage_pc	www.google.com/	1	informant	https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=49
435	cfreds_2015_data_leakage_pc	www.google.com/	1	informant	https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCMQFjA
436	cfreds_2015_data_leakage_pc	www.google.com/	1	informant	https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=49
437	cfreds_2015_data_leakage_pc	www.google.com/	1	informant	https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&sqi=2&ved=0CE

449	cfreds_2015_data_leakage_pc	www.google.com/	1	informant	https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=18	03/23/15 02:17:19
450	cfreds_2015_data_leakage_pc	www.google.com/	1	informant	https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=58	03/23/15 02:17:57
451	cfreds_2015_data_leakage_pc	www.google.com/	1	informant	https://www.google.com/search?q=information+leakage+cases&hl=en&t	03/23/15 02:18:10
452	cfreds_2015_data_leakage_pc	www.google.com/	1	informant	https://www.google.com/search?q=information+leakage+cases&hl=en&t	03/23/15 02:18:15
453	cfreds_2015_data_leakage_pc	www.google.com/	1	informant	https://www.google.com/search?q=information+leakage+cases&hl=en&t	03/23/15 02:18:30
454	cfreds_2015_data_leakage_pc	www.google.com/	1	informant	https://www.google.com/search?q=information+leakage+cases&hl=en&t	03/23/15 02:18:43
455	cfreds_2015_data_leakage_pc	www.google.com/	1	informant	https://www.google.com/search?q=information+leakage+cases&hl=en&t	03/23/15 02:18:46
456	cfreds_2015_data_leakage_pc	www.google.com/	1	informant	https://www.google.com/search?q=information+leakage+cases&hl=en&t	03/23/15 03:47:43
457	cfreds_2015_data_leakage_pc	www.google.com/	1	informant	https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=78	03/23/15 02:19:17
458	cfreds_2015_data_leakage_pc	www.google.com/	1	informant	https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=10	03/23/15 02:19:21

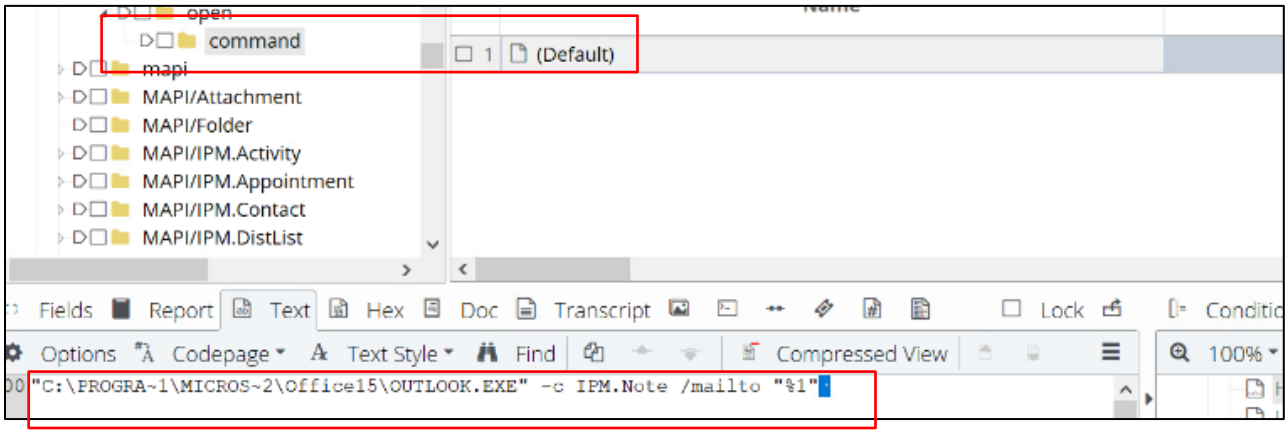
17. List all user keywords at the search bar in Windows Explorer. (Timestamp, Keyword)
Answer:
Keyword: Secret
Timestamp: 2015-03-23 14:40:17

True Path: Data Leak Case -2 Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\NTUSER.DAT\CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery\0
Item Path: CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery\0

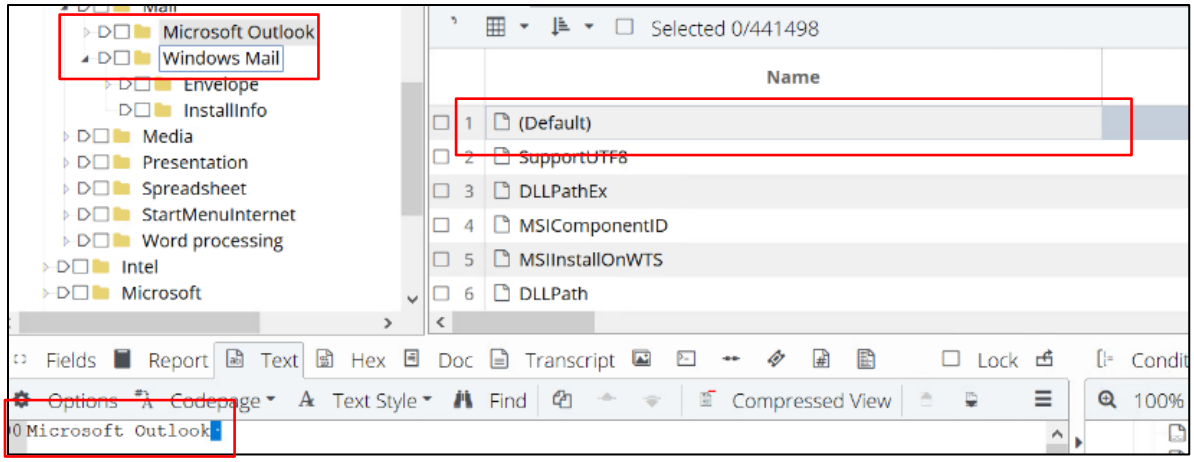




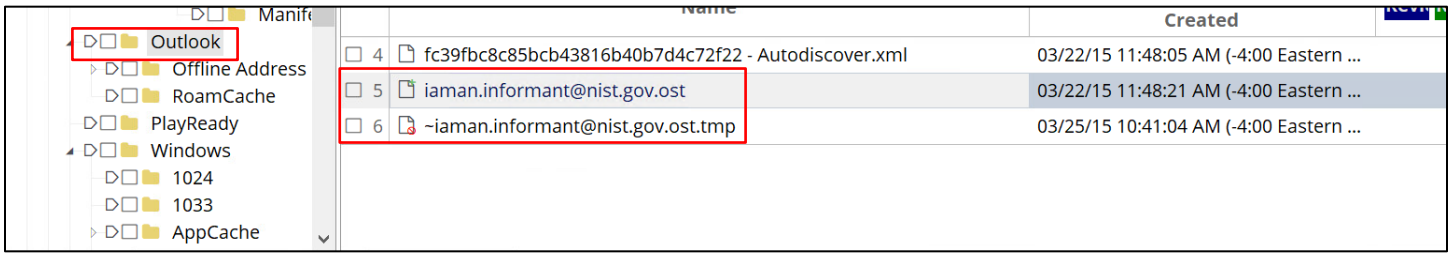
18. What application was used for e-mail communication?
Answer: Microsoft Outlook 2013
True Path: Data Leak Case -2 Jeel\cfreds_2015_data_leakage_pc\D\Windows\System32\config\SOFTWARE\CMI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\Classes\mailto\shell\open\command\(Default)
Item Path: CMI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\Classes\mailto\shell\open\command\(Default)



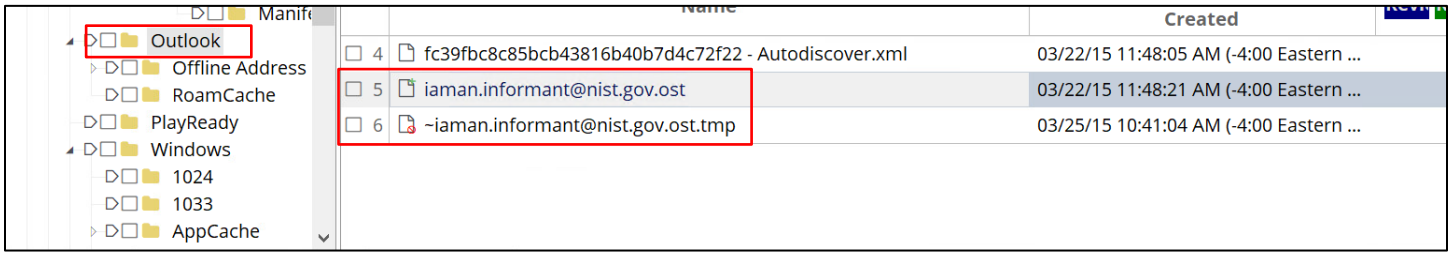
True Path: Data Leak Case -2 Jeel\cfreds_2015_data_leakage_pc\D\Windows\System32\config\SOFTWARE\CMI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\Clients\Mail\Microsoft Outlook\(Default)
Item Path: CMI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\Clients\Mail\Microsoft Outlook\(Default)



19. Where is the e-mail file located?
Answer:
cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Microsoft\Outlook\iaman.informant@nist.gov.ost
True Path: Data Leak Case -2 Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Microsoft\Outlook\iaman.informant@nist.gov.ost
Item Path:
cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Microsoft\Outlook\iaman.informant@nist.gov.ost



20. What was the e-mail account used by the suspect?
Answer: iaman.informant@nist.gov
True Path: Data Leak Case -2 Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Microsoft\Outlook\iaman.informant@nist.gov.ost
Item Path: cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Microsoft\Outlook\iaman.informant@nist.gov.ost



21. List all e-mails of the suspect. If possible, identify deleted e-mails.
(You can identify the following items: *Timestamp, From, To, Subject, Body, and Attachment*)
[Hint: just examine the OST file only.]
Answer:

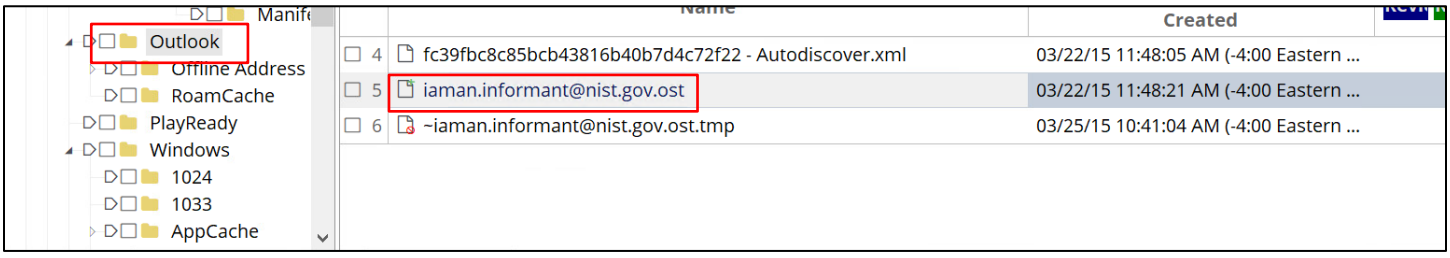
Timestamp	E-Mail Data	
2015-03-23 13:29:27	Source	[Inbox]
	From → To	spy.conspirator@nist.gov → iaman.informant@nist.gov
	Subject	Hello, Iaman
	Body	How are you doing?
2015-03-23 14:44:31	Source	[Sent Items]
	From → To	iaman.informant@nist.gov → spy.conspirator@nist.gov
	Subject	RE: Hello, Iaman
	Body	Successfully secured. --- From: spy Sent: Monday, March 23, 2015 1:29 PM To: iaman Subject: Hello, Iaman How are you doing?
2015-03-23 15:14:58	Source	[Inbox]
	From → To	spy.conspirator@nist.gov → iaman.informant@nist.gov
	Subject	Good job, buddy.
	Body	Good, job. I need a more detailed data about this business.
2015-03-23 15:20:41	Source	[Inbox]
	From → To	spy.conspirator@nist.gov → iaman.informant@nist.gov

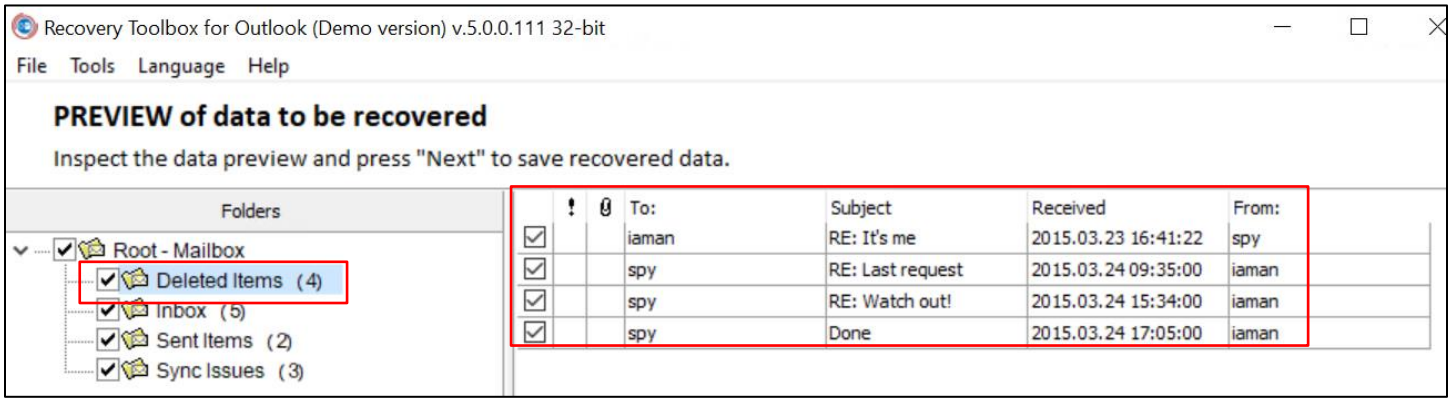
	Subject	RE: Good job, buddy.
	Body	Okay, I got it. I'll be in touch. ---------- From: iaman Sent: Monday, March 23, 2015 3:19 PM To: spy Subject: RE: Good job, buddy. This is a sample. ---------- From: spy Sent: Monday, March 23, 2015 3:15 PM To: iaman Subject: Good job, buddy. Good, job. I need a more detailed data about this business.
2015-03-23 15:26:22	Source	[Inbox]
	From → To	spy.conspirator@nist.gov → iaman.informant@nist.gov
	Subject	Important request
	Body	I confirmed it. But, I need a more data. Do your best.
2015-03-23 15:27:05	Source	[Sent Items]
	From → To	iaman.informant@nist.gov → spy.conspirator@nist.gov
	Subject	RE: Important request
	Body	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.
2015-03-23 16:38:47	Source	*Recovered Item* from unused area of OST file
	From → To	iaman.informant@nist.gov → spy.conspirator@nist.gov
	Subject	It's me
	Body	Use links below, https://drive.google.com/file/d/0Bz0ye6gXtiZaVl8yVU5mWHlGbWc/view?usp=sharing

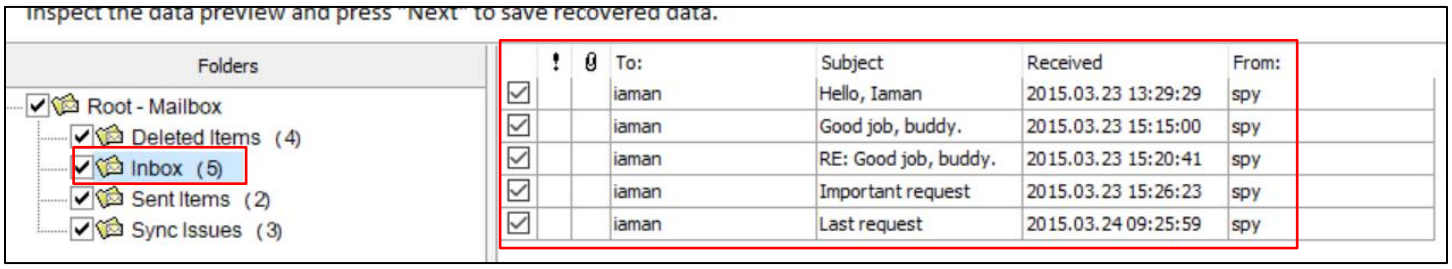
		https://drive.google.com/file/d/0Bz0ye6gXtiZaakx6d3R3c0JmM1U/view?usp=sharing
2015-03-23 16:41:19	Source	[Deleted Items]
	From → To	spy.conspirator@nist.gov → iaman.informant@nist.gov
	Subject	RE: It's me
	Body	I got it. --- From: iaman Sent: Monday, March 23, 2015 4:39 PM To: spy Subject: It's me Use links below, https://drive.google.com/file/d/0Bz0ye6gXtiZaVl8yVU5mWHlGbWc/view?usp=sharing https://drive.google.com/file/d/0Bz0ye6gXtiZaakx6d3R3c0JmM1U/view?usp=sharing
2015-03-24 09:25:57	Source	[Inbox]
	From → To	spy.conspirator@nist.gov → iaman.informant@nist.gov
	Subject	Last request
	Body	This is the last request. I want to get the remaining data.
2015-03-24 09:35:10	Source	[Deleted Items]
	From → To	iaman.informant@nist.gov → spy.conspirator@nist.gov
	Subject	RE: Last request
	Body	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!

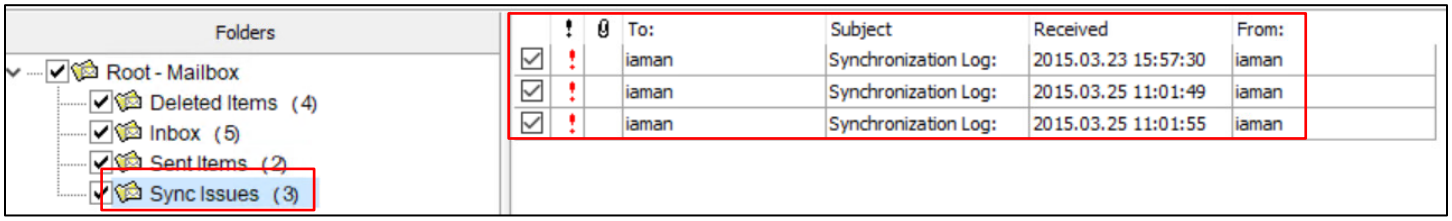
		---------- From: spy Sent: Tuesday, March 24, 2015 9:26 AM To: iaman Subject: Last request This is the last request. I want to get the remaining data.
2015-03-24 15:34:02	Source	[Deleted Items]
	From → To	iaman.informant@nist.gov → spy.conspirator@nist.gov
	Subject	RE: Watch out!
	Body	I am trying. ---------- 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.
2015-03-24 17:05:09	Source	[Deleted Items]
	From → To	iaman.informant@nist.gov → spy.conspirator@nist.gov
	Subject	Done
	Body	It's done. See you tomorrow.

True Path: Data Leak Case -2
Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Microsoft\Outlook\iaman.informant@nist.gov.ost
Item Path:
cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Microsoft\Outlook\iaman.informant@nist.gov.ost









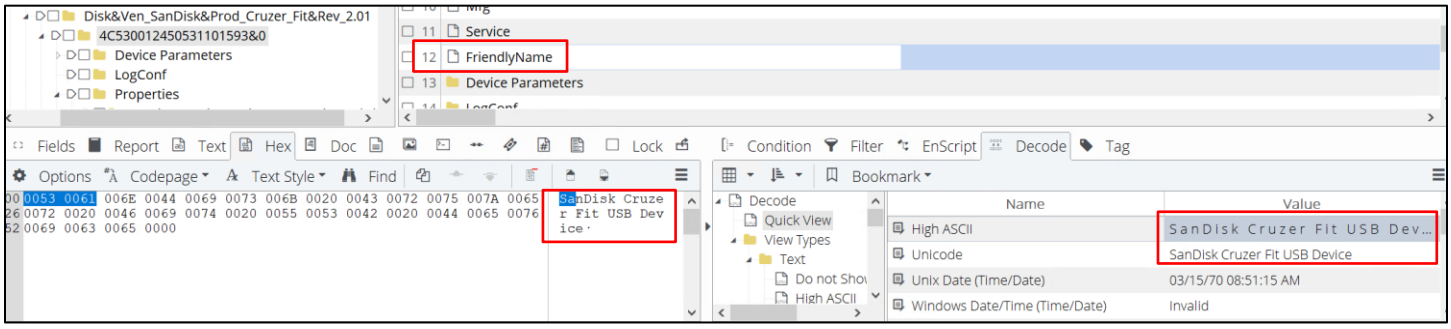
22. List external storage devices attached to PC.

Answer:

Device Name	Serial No.	Volume Name	First Connected Time	Connected Time After Reboot
SanDisk Cruzer Fit USB Device	4C530012550531106501	IAMAN $_@	2015-03-24 09:58:32 Tue	2015-03-24 09:58:33 Tue
SanDisk Cruzer Fit USB Device	4C530012450531101593		2015-03-23 14:31:10 Mon	2015-03-24 09:38:00 Tue

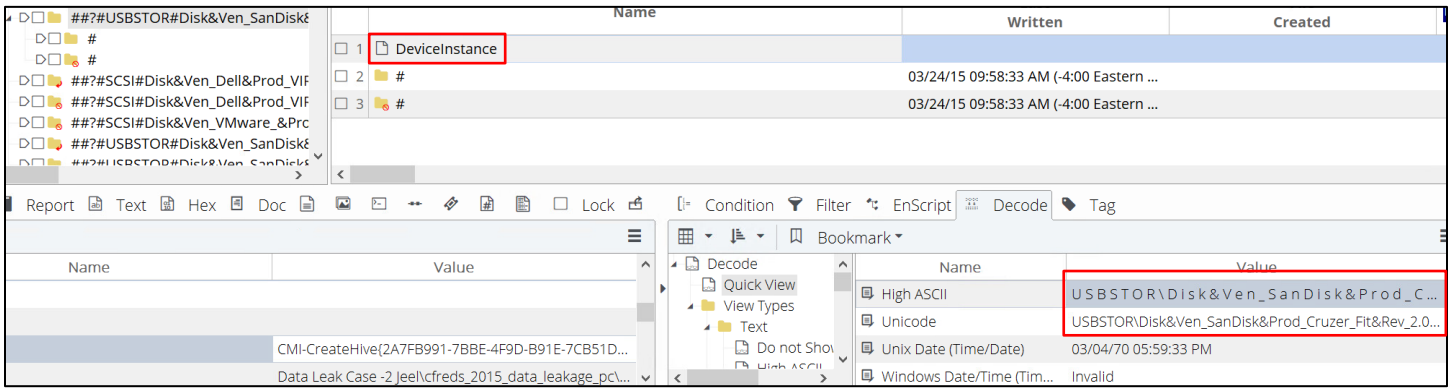
True Path: Data Leak Case -2 Jeel\cfreds_2015_data_leakage_pc\D\Windows\System32\config\SYSTEM\CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}\ControlSet001\Enum\USBSTOR\

Item Path: CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}\ControlSet001\Enum\USBSTOR\



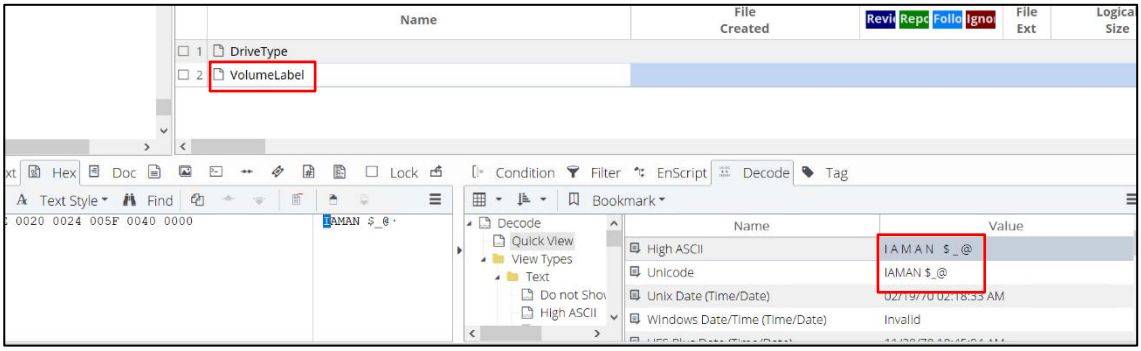
True Path: Data Leak Case -2 Jeel\cfreds_2015_data_leakage_pc\D\Windows\System32\config\SYSTEM\CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}\ControlSet001\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#USBSTOR#Disk&Ven_SanDisk&Prod_Cruzer_Fit&Rev_2.01#4C530012550531106501&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

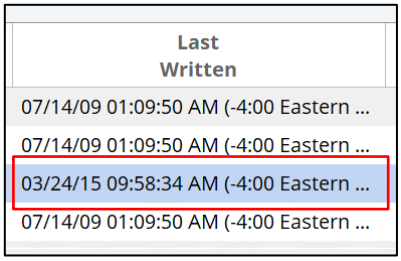
Item Path: CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}\ControlSet001\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#USBSTOR#Disk&Ven_SanDisk&Prod_Cruzer_Fit&Rev_2.01#4C530012550531106501&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}



True Path: Data Leak Case -2 Jeel\cfreds_2015_data_leakage_pc\D\Windows\System32\config\SOFTWARE\CMI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\Microsoft\Windows Search\VolumeInfoCache\E:

Item Path: CMI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\Microsoft\Windows Search\VolumeInfoCache\E:





23. Identify all traces related to 'renaming' of files in Windows Desktop.
(It should be considered only during a date range between 2015-03-23 and 2015-03-24.)
[Hint: the parent directories of renamed files were deleted and their MFT entries were also overwritten. Therefore, you may not be able to find their full paths.]

Answer:

Timestamp	Path	Event
2015-03-23 14:41:40	\Users\informant\Desktop\S data\[secret_project]_detailed_proposal.docx	Renamed
	\Users\informant\Desktop\S data\landscape.png	Renamed
2015-03-23 14:41:55	\Users\informant\Desktop\S data\[secret_project]_design_concept.ppt	Renamed
	\Users\informant\Desktop\S data\space_and_earth.mp4	Renamed
2015-03-23 16:30:44	\Users\informant\Desktop\S data\(secret_project)_pricing_decision.xlsx	Renamed
	\Users\informant\Desktop\S data\happy_holiday.jpg	Renamed
2015-03-23 16:31:02	\Users\informant\Desktop\S data\[secret_project]_final_meeting.pptx	Renamed
	\Users\informant\Desktop\S data\do_u_wanna_build_a_snow_man.mp3	Renamed
2015-03-24 09:49:51	\Users\informant\Desktop\S data\Secret Project Data\design\ [secret_project]_detailed_design.pptx	Renamed
	\Users\informant\Desktop\S data\Secret Project Data\design\ winter_whether_advisory.zip	Renamed
2015-03-24 09:50:08	\Users\informant\Desktop\S data\Secret Project Data\design\ [secret_project]_revised_points.ppt	Renamed
	\Users\informant\Desktop\S data\Secret Project Data\design\ winter_storm.amr	Renamed
2015-03-24 09:50:49	\Users\informant\Desktop\S data\Secret Project Data\design\ [secret_project]_design_concept.ppt	Renamed
	\Users\informant\Desktop\S data\Secret Project Data\design\ space_and_earth.mp4	Renamed
2015-03-24 09:52:35	\Users\informant\Desktop\S data\Secret Project Data\final\ [secret_project]_final_meeting.pptx	Renamed
	\Users\informant\Desktop\S data\Secret Project Data\final\ do_u_wanna_build_a_snow_man.mp3	Renamed
2015-03-24 09:52:56	\Users\informant\Desktop\S data\Secret Project Data\pricing decision\ (secret_project)_market_analysis.xlsx	Renamed
	\Users\informant\Desktop\S data\Secret Project Data\pricing decision\ new_years_day.jpg	Renamed
2015-03-24 09:53:08	\Users\informant\Desktop\S data\Secret Project Data\pricing decision\ (secret_project)_market_shares.xls	Renamed
	\Users\informant\Desktop\S data\Secret Project Data\pricing decision\ super_bowl.avi	Renamed
2015-03-24 09:53:38	\Users\informant\Desktop\S data\Secret Project Data\pricing decision\ (secret_project)_price_analysis_#1.xlsx	Renamed
	\Users\informant\Desktop\S data\Secret Project Data\pricing decision\ my_favorite_movies.7z	Renamed
2015-03-24 09:53:52	\Users\informant\Desktop\S data\Secret Project Data\pricing decision\ (secret_project)_price_analysis_#2.xls	Renamed
	\Users\informant\Desktop\S data\Secret Project Data\pricing decision\ my_favorite_cars.db	Renamed
2015-03-24 09:54:05	\Users\informant\Desktop\S data\Secret Project Data\pricing decision\ (secret_project)_pricing_decision.xlsx	Renamed
	\Users\informant\Desktop\S data\Secret Project Data\pricing decision\	Renamed

	happy_holiday.jpg	
2015-03-24 09:54:23	\Users\informant\Desktop\S data\Secret Project Data\progress\ [secret_project]_progress_#1.docx	Renamed
	\Users\informant\Desktop\S data\Secret Project Data\progress\ my_smartphone.png	Renamed
2015-03-24 09:54:43	\Users\informant\Desktop\S data\Secret Project Data\progress\ [secret_project]_progress_#2.docx	Renamed
	\Users\informant\Desktop\S data\Secret Project Data\progress\ new_year_calendar.one	Renamed
2015-03-24 09:54:52	\Users\informant\Desktop\S data\Secret Project Data\progress\ [secret_project]_progress_#3.doc	Renamed
	\Users\informant\Desktop\S data\Secret Project Data\progress\ my_friends.svg	Renamed
2015-03-24 09:55:08	\Users\informant\Desktop\S data\Secret Project Data\proposal\ [secret_project]_detailed_proposal.docx	Renamed
	\Users\informant\Desktop\S data\Secret Project Data\proposal\ a_gift_from_you.gif	Renamed
2015-03-24 09:55:17	\Users\informant\Desktop\S data\Secret Project Data\proposal\ [secret_project]_proposal.docx	Renamed
	\Users\informant\Desktop\S data\Secret Project Data\proposal\ landscape.png	Renamed
2015-03-24 09:55:32	\Users\informant\Desktop\S data\Secret Project Data\technical review\ [secret_project]_technical_review_#1.docx	Renamed
	\Users\informant\Desktop\S data\Secret Project Data\technical review\ diary_#1d.txt	Renamed
2015-03-24 09:55:42	\Users\informant\Desktop\S data\Secret Project Data\technical review\ [secret_project]_technical_review_#1.pptx	Renamed
	\Users\informant\Desktop\S data\Secret Project Data\technical review\ diary_#1p.txt	Renamed
2015-03-24 09:55:53	\Users\informant\Desktop\S data\Secret Project Data\technical review\ [secret_project]_technical_review_#2.docx	Renamed
	\Users\informant\Desktop\S data\Secret Project Data\technical review\ diary_#2d.txt	Renamed
2015-03-24 09:56:09	\Users\informant\Desktop\S data\Secret Project Data\technical review\ [secret_project]_technical_review_#2.ppt	Renamed
	\Users\informant\Desktop\S data\Secret Project Data\technical review\ diary_#2p.txt	Renamed
2015-03-24 09:56:14	\Users\informant\Desktop\S data\Secret Project Data\technical review\ [secret_project]_technical_review_#3.doc	Renamed
	\Users\informant\Desktop\S data\Secret Project Data\technical review\ diary_#3d.txt	Renamed
2015-03-24 09:56:20	\Users\informant\Desktop\S data\Secret Project Data\technical review\ [secret_project]_technical_review_#3.ppt	Renamed
	\Users\informant\Desktop\S data\Secret Project Data\technical review\ diary_#3p.txt	Renamed

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb

Item Path: cfreds_2015_data_leakage_pc\D\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb

Example of one event of renaming:
Original Path:

AF
System_ItemPathDisplay
C:\Users\informant\Desktop\S data\Secret Project Data\Secret Project Data\proposal\[secret_project]_detailed_proposal.docx

AD
System_ItemFolderPathDisplay
C:\Users\informant\Desktop\S data\Secret Project Data\Secret Project Data\proposal

Renamed/Modified Entry:

System_Search_ReverseFileName
xcod.lasoporp_deliated_]tcejorp_terces[

- The encoded or obfuscated form of the filename, shown as xcod.lasoporp_deliated_]tcejorp_terces[, represents a scrambled or encoded filename after renaming.
- The presence of this encoded string can suggest that the file has undergone a renaming or restructuring, which might be recorded by the system as a way to store old paths.

Relevant Timestamps:

F	G	H
System_DateModified	**System_DateCreated**	**System_DateAccessed**
01 D0 1B 0C B4 C3 4D 00	01 D0 66 38 0C B8 04 DA	01 D0 66 38 0C B8 04 DA

File Type and Context:

- The entry indicates that the file type is a Microsoft Word document (Microsoft Office Word) with the original title **[secret_project]_detailed_proposal.docx**.

Procedural Explanation:

- By analyzing fields like **System_ItemFolderPathDisplay**, **System_ItemPathDisplay**, and related paths and encoded names, we can identify renaming actions. These fields provide direct evidence of a change from the original file name or path.
- The event log is then cross-referenced with timestamps in **System_DateModified** to confirm the time of renaming.

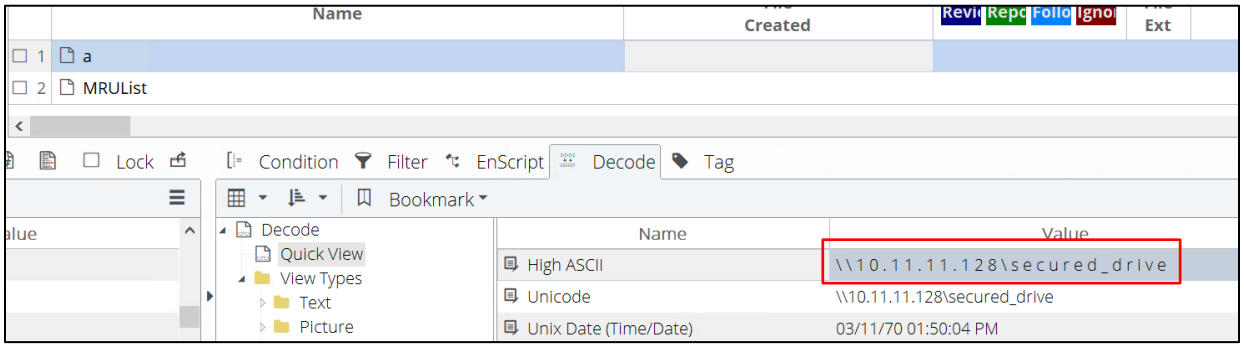

windows.xlsx

Here's Attached excel file of table that converted **Windows.edb** file into structure for analysis by **ESEDatabaseView**.

After obtaining the **Windows.edb** file, we used **ESEDatabaseViewer** to open and examine its contents. We exported the entire table to an Excel/CSV file, allowing for easier analysis and manipulation of data. By analyzing key columns—such as **System_ItemFolderPathDisplay, System_ItemPathDisplay**, and **System_DateModified**—we identified entries related to file renaming events. Specifically, discrepancies between the original and renamed file paths, along with timestamps, helped us confirm renaming actions, allowing us to track modifications efficiently within the dataset.

24. What is the IP address of company's shared network drive?
Answer: 10.11.11.128

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\NTUSER.DAT\CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU\a
Item Path: CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU\a



Verification of Company's IP:

Target	Folder	User Name	Reg Key Last Modified	Network Share	Re
cfreds_2015_data_leakage_pc	\\10.11.11.128\secured_drive	informant	03/23/15 04:24:01 PM (-4:00 Eastern Daylight Time)	10.11.11.128	D
cfreds_2015_data_leakage_pc	\\10.11.11.128\secured_drive\Common Data	informant	03/23/15 04:24:12 PM (-4:00 Eastern Daylight Time)	10.11.11.128	D
cfreds_2015_data_leakage_pc	\\10.11.11.128\secured_drive\Past Projects	informant	03/23/15 04:24:12 PM (-4:00 Eastern Daylight Time)	10.11.11.128	D
cfreds_2015_data_leakage_pc	\\10.11.11.128\secured_drive\Secret Project Data	informant	03/23/15 04:24:12 PM (-4:00 Eastern Daylight Time)	10.11.11.128	D
cfreds_2015_data_leakage_pc	\\10.11.11.128\secured_drive\Secret Project Data\design	informant	03/23/15 04:28:17 PM (-4:00 Eastern Daylight Time)	10.11.11.128	D
cfreds_2015_data_leakage_pc	\\10.11.11.128\secured_drive\Secret Project Data\final	informant	03/23/15 04:28:17 PM (-4:00 Eastern Daylight Time)	10.11.11.128	D
cfreds_2015_data_leakage_pc	\\10.11.11.128\secured_drive\Secret Project Data\pricing dec	informant	03/23/15 04:28:17 PM (-4:00 Eastern Daylight Time)	10.11.11.128	D
cfreds_2015_data_leakage_pc	\\10.11.11.128\secured_drive\Secret Project Data\progress	informant	03/23/15 04:28:17 PM (-4:00 Eastern Daylight Time)	10.11.11.128	D
cfreds_2015_data_leakage_pc	\\10.11.11.128\secured_drive\Secret Project Data\proposal	informant	03/23/15 04:28:17 PM (-4:00 Eastern Daylight Time)	10.11.11.128	D
cfreds_2015_data_leakage_pc	\\10.11.11.128\secured_drive\Secret Project Data\technical re	informant	03/23/15 04:28:17 PM (-4:00 Eastern Daylight Time)	10.11.11.128	D

The image shows multiple entries that confirm access to a shared network drive with the IP 10.11.11.128. This network path, \\10.11.11.128\secured_drive, includes folders such as Common Data, Past Projects, and Secret Project Data, along with subfolders (design, final, pricing decision, progress, proposal, and technical report).

User Access: The user "informant" accessed various directories within the secured drive.
Last Modified Timestamps: Each directory has a Reg Key Last Modified timestamp from 03/23/15, indicating the date and time when these entries were last accessed or modified.
Network Share Verification: The IP address 10.11.11.128 aligns with the company's shared network drive, confirming the location of potentially sensitive data.

25. List all directories that were traversed in 'RM#2'.

Answer:

Directory Path	Source
E:\Secret Project Data\	ShellBag
E:\Secret Project Data\technical review\	ShellBag
E:\Secret Project Data\proposal\	ShellBag
E:\Secret Project Data\progress\	ShellBag
E:\Secret Project Data\pricing decision\	ShellBag
E:\Secret Project Data\design\	ShellBag

Parent Director:

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\NTUSER.DAT\CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft\Windows\Shell\BagMRU\0\0\0\2

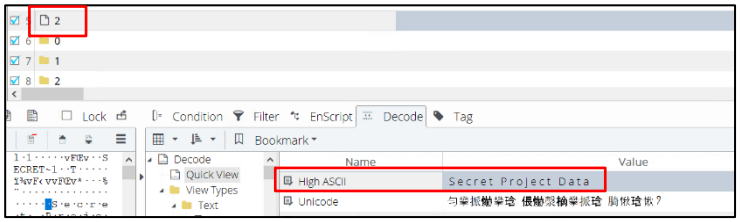
Item Path: CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft\Windows\Shell\BagMRU\0\0\0\2

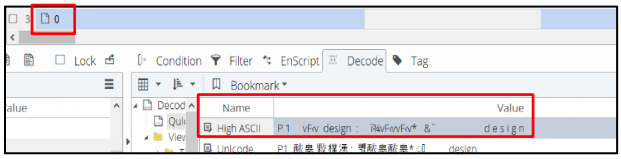
File Directory:

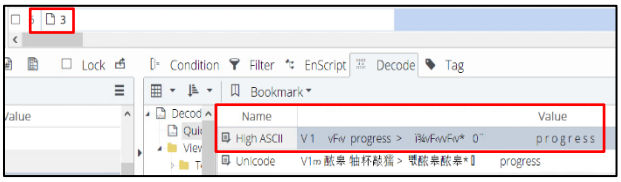
True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\NTUSER.DAT\CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft\Windows\Shell\BagMRU\0\0\0\2\

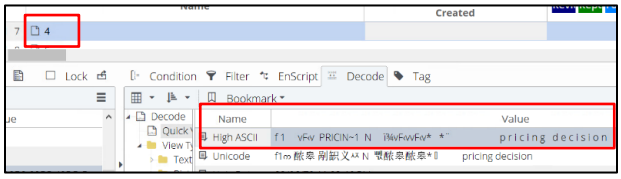
Item Path: CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft\Windows\Shell\BagMRU\0\0\0\2\

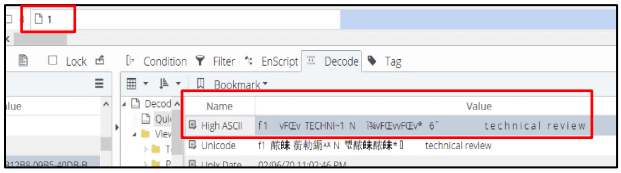
Targeted File: 0,1,2,3,4 and 5

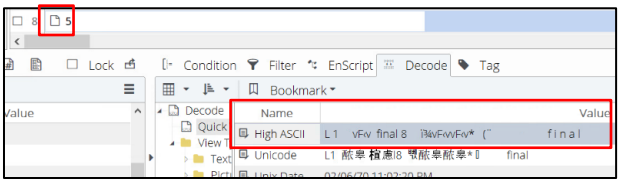












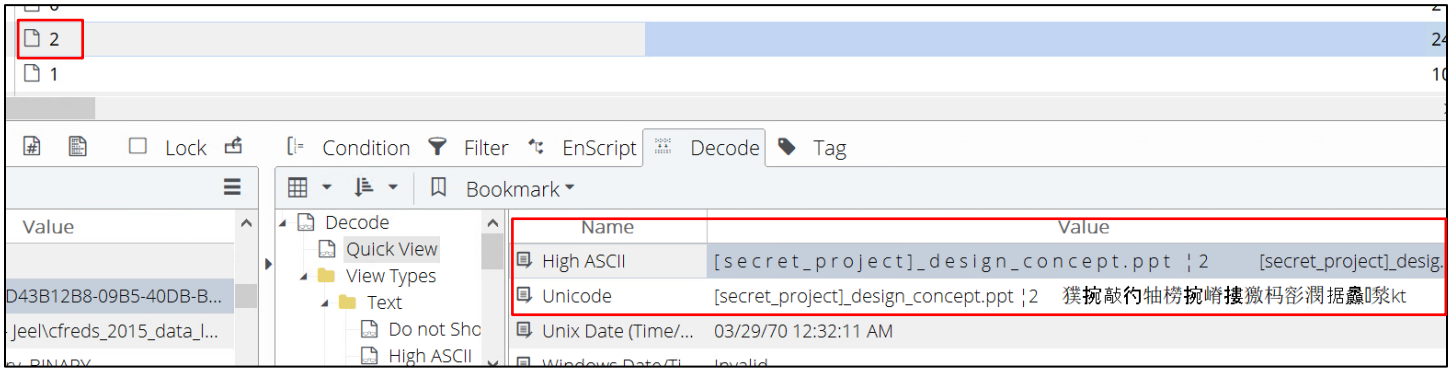
26. List all files that were opened in 'RM#2'.

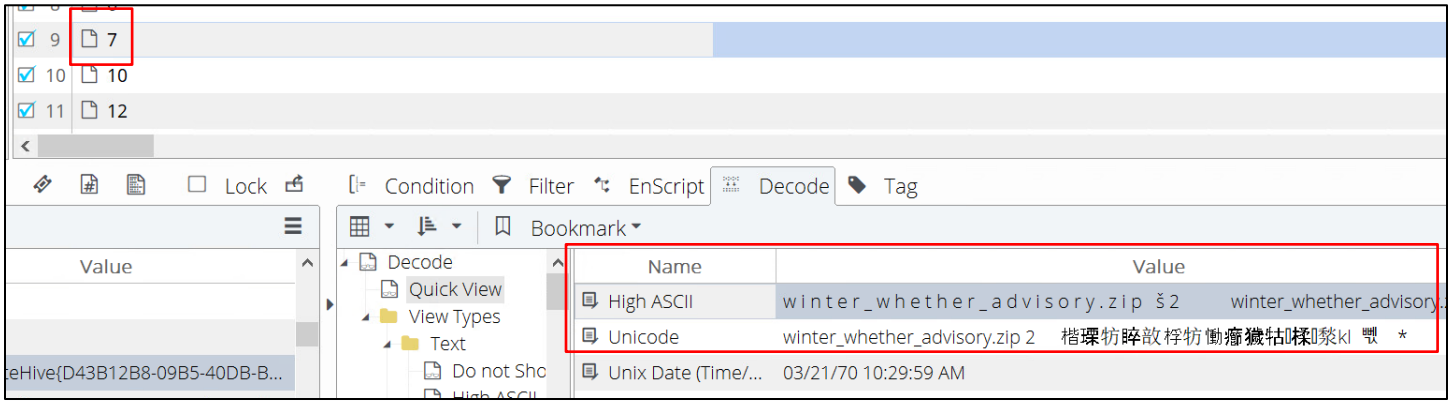
Answer:

E:\secured_drive\Secret Project Data\design\[secret_project]_design_concept.ppt
E:\secured_drive\Secret Project Data\proposal\[secret_project]_proposal.docx
E:\secured_drive\Secret Project Data\secret\secret.lnk
E:\secured_drive\Secret Project Data\pricing\[secret_project]_pricing_decision.xlsx
E:\secured_drive\Secret Project Data\pricing\pricing decision.lnk
E:\secured_drive\Secret Project Data\final\[secret_project]_final_meeting.pptx
E:\secured_drive\Secret Project Data\final\final.lnk
E:\secured_drive\Common Data\winter_whether_advisory.zip
E:\secured_drive\Common Data\Koala.jpg
E:\secured_drive\Common Data\Tulips.jpg
E:\secured_drive\Common Data\BD-RE Drive (D:) IAMAN CD.lnk
E:\secured_drive\Past Projects\Resignation_Letter_(Iaman_Informant).xps
E:\secured_drive\Past Projects\Resignation_Letter_(Iaman_Informant).docx

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\NTUSER.DAT\CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\
Item Path: CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\

Targeted File: 0,1,2,3,4,5,6,7,8,9,10,11,12,13 and 14



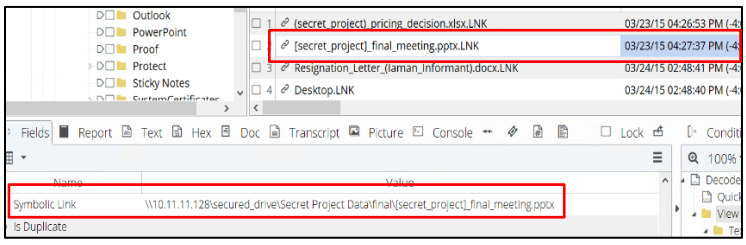


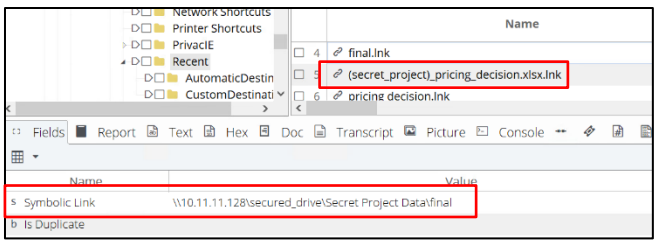
Explanation:
We analyzed entries within the registry's **RecentDocs** section, where each file's name had a hexadecimal identifier ending in "**2**." This suffix aligns with the structure seen in previous questions, confirming that files labeled with "**2**" in the registry's **RecentDocs** were opened in **RM#2**.
Through this approach, we isolated specific files associated with **RM#2** based on their registry entries, effectively reconstructing the user's access patterns. This method of identifying **RM#2-associated** files by decoding and examining hexadecimal identifiers provided a reliable and repeatable process for determining file access events in the forensic investigation.

27. List all directories that were traversed in the company's network drive.
Answer:
\\10.11.11.128\secured_drive\Common Data\
\\10.11.11.128\secured_drive\Past Projects\
\\10.11.11.128\secured_drive\Secret Project Data\design\
\\10.11.11.128\secured_drive\Secret Project Data\pricing decision\
\\10.11.11.128\secured_drive\Secret Project Data\final\
\\10.11.11.128\secured_drive\Secret Project Data\technical review\
\\10.11.11.128\secured_drive\Secret Project Data\proposal\
\\10.11.11.128\secured_drive\Secret Project Data\progress\
\\10.11.11.128\secured_drive\Secret Project Data\pricing decision\
\\10.11.11.128\secured_drive\Secret Project Data\pricing decision\
V:\Secret Project Data\
V:\Secret Project Data\final\
V:\Secret Project Data\final\
V:\Secret Project Data\final\
\\10.11.11.128\secured_drive\Secret Project Data\
\\10.11.11.128\secured_drive\Secret Project Data\pricing decision\
\\10.11.11.128\secured_drive\
\\10.11.11.128\secured_drive\Past Projects\

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\
Item Path: cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Roaming\Microsoft\Office\Recent\
Item Path: cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Roaming\Microsoft\Office\Recent\





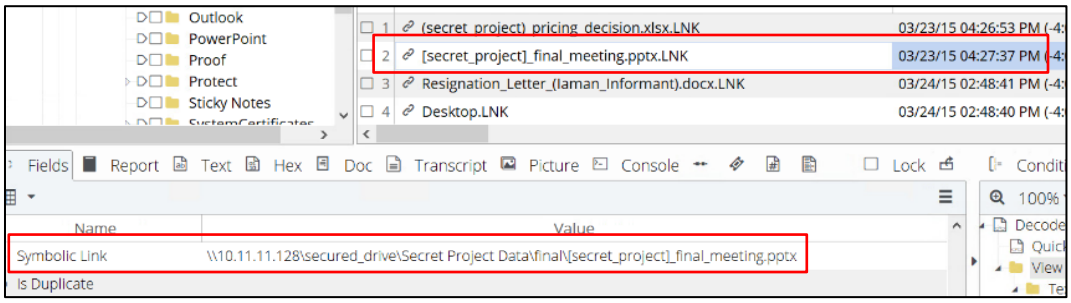
28. List all files that were opened in the company's network drive.

Answer:

\\10.11.11.128\SECURED_DRIVE\Secret Project Data\ pricing decision\(secret_project)_pricing_decision.xlsx
\\10.11.11.128\SECURED_DRIVE\Secret Project Data\ pricing decision\(secret_project)_pricing_decision.xlsx
\\10.11.11.128\SECURED_DRIVE\Secret Project Data\ pricing decision\(secret_project)_pricing_decision.xlsx
\\10.11.11.128\secured_drive\Secret Project Data\ pricing decision\(secret_project)_pricing_decision.xlsx
V:\Secret Project Data\final\[secret_project]_final_meeting.pptx V:\Secret Project Data\final\[secret_project]_final_meeting.pptx
V:\Secret Project Data\final\[secret_project]_final_meeting.pptx V:\Secret Project Data\final\[secret_project]_final_meeting.pptx

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\
Item Path: cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Roaming\Microsoft\Office\Recent\
Item Path: cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Roaming\Microsoft\Office\Recent\



29. Find traces related to cloud services on PC.
(Service name, log files...)

Answer:

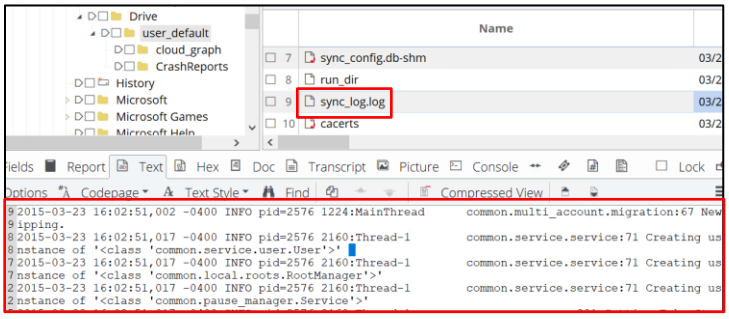
Cloud Service	Traces	Type
Google Drive	sync_config.db (deleted) snapshot.db (deleted) sync_log.log	Log File, Database files
Apple iCloud	icloudsetup.exe	File/Directory

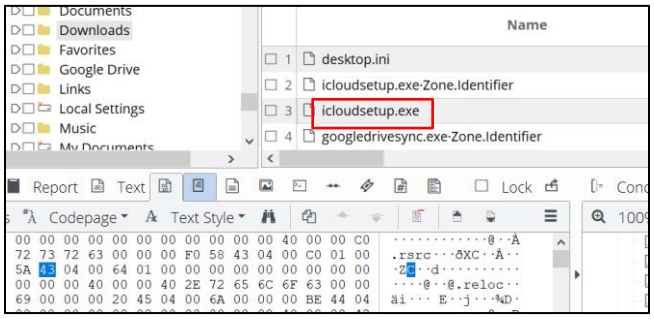
- **Google Drive:**

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Google\Drive\user_default\
Item Path: cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Google\Drive\user_default\

- **Apple iCloud:**

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\Downloads\icloudsetup.exe
Item Path: cfreds_2015_data_leakage_pc\D\Users\informant\Downloads\icloudsetup.exe





30. What files were deleted from Google Drive?

Find the filename and modified timestamp of the file.

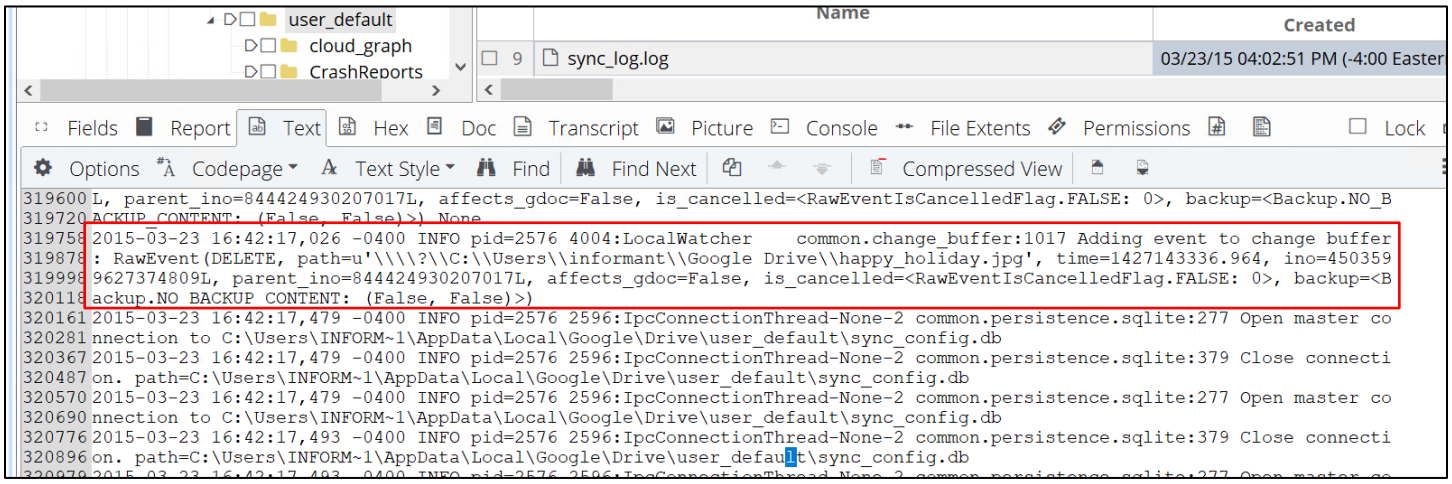
[Hint: Find a transaction log file of Google Drive.]

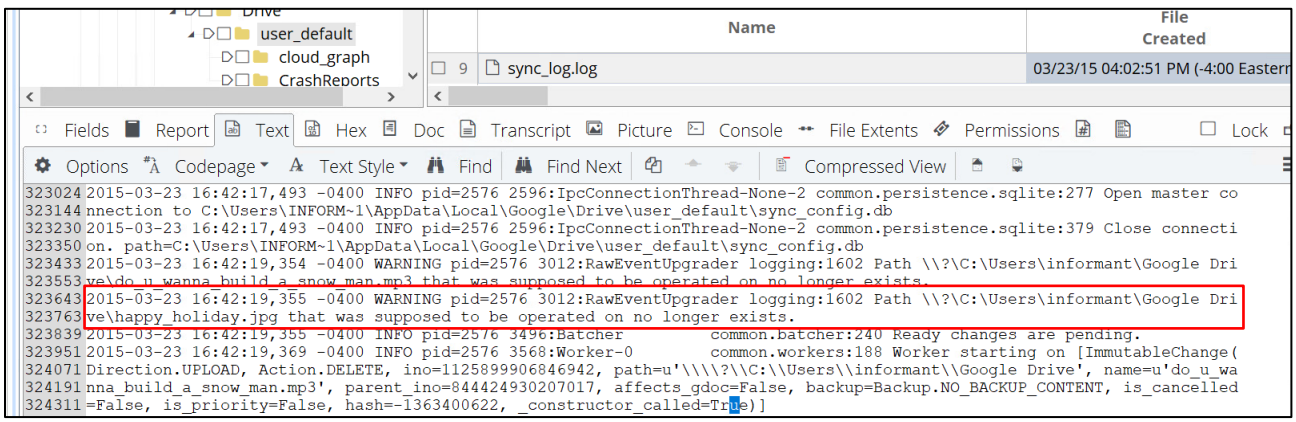
Answer:

Filename	Timestamp	Modified Time (UTC-05)	File Path
2015-03-23 16:42:17	happy_holiday.jpg	2015-01-30 11:49:20	C:\Users\informant\Google Drive\happy_holiday.jpg
2015-03-23 16:42:17	do_u_wanna_build_a_snow_man.mp3	2015-01-29 15:35:14	C:\Users\informant\Google Drive\do_u_wanna_build_a_snow_man.mp3

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Google\Drive\user_default\sync_log.log

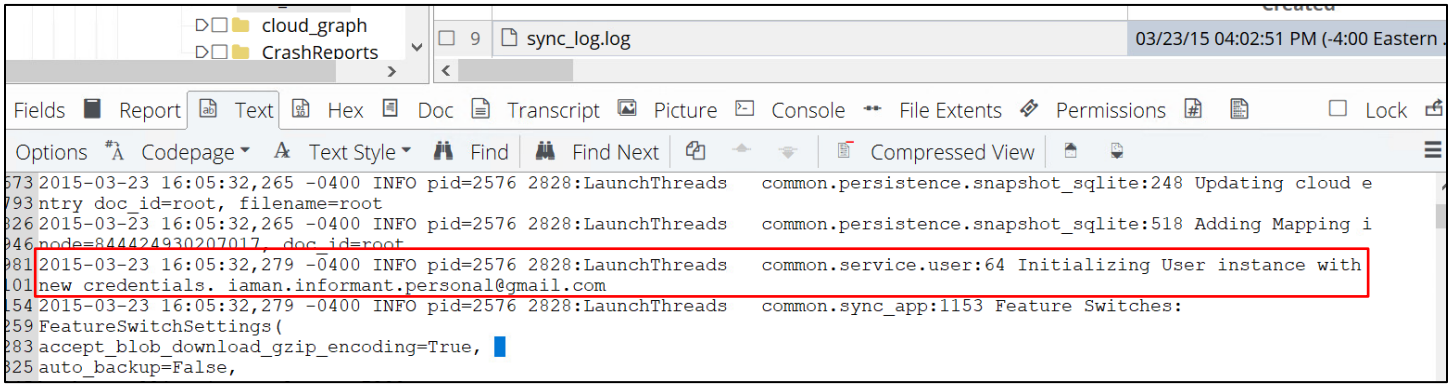
Item Path:
cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Google\Drive\user_default\sync_log.log





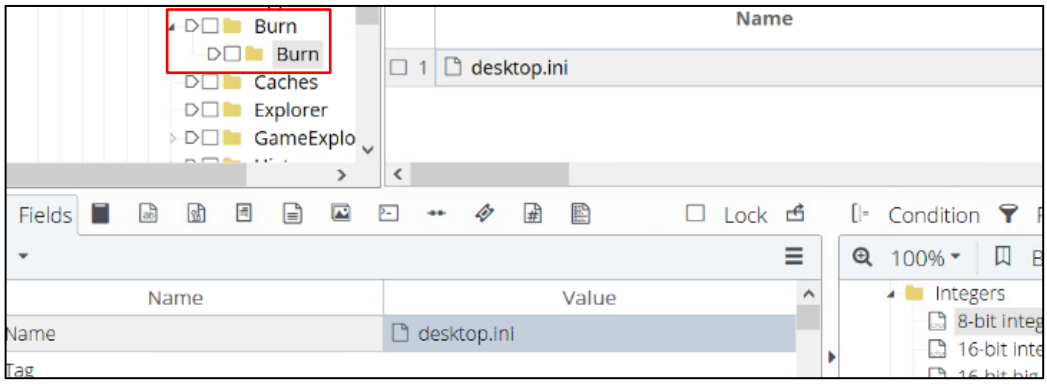
31. Identify account information for synchronizing Google Drive.
Answer:
Account: iaman.informant.personal@gmail.com
Logon Time: 2015-03-23 16:05:32

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Google\Drive\user_default\sync_log.log
Item Path: cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Google\Drive\user_default\sync_log.log



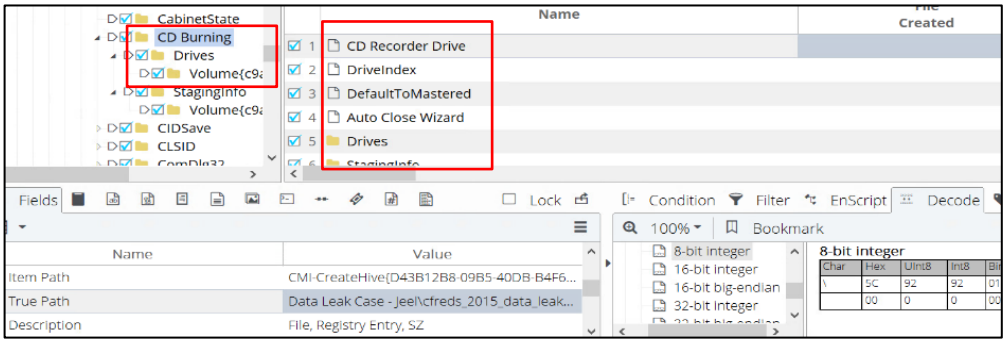
32. What a method (or software) was used for burning CD-R?
Answer: Windows default CD/DVD burning feature

Burn Folder Directory:
True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\
Item Path: cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\



CD Burning Registry Configuration:
True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\NTUSER.DAT\CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft\Windows\CurrentVersion\Explorer\CD Burning\

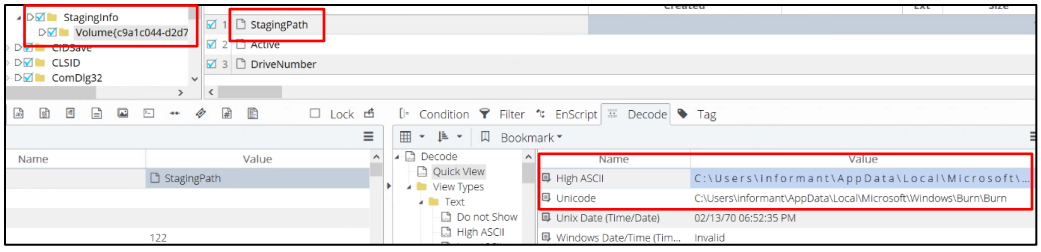
Item Path: CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft\Windows\CurrentVersion\Explorer\CD Burning\



StagingInfo Registry Entries: The StagingInfo registry entries reveal a StagingPath for files prepared for burning, along with an Active flag and a DriveNumber, confirming that files were temporarily staged before burning.

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\NTUSER.DAT\CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft\Windows\CurrentVersion\Explorer\CD Burning\StagingInfo\Volume{c9a1c044-d2d7-11e4-9dae-806e6f6e6963}\StagingPath

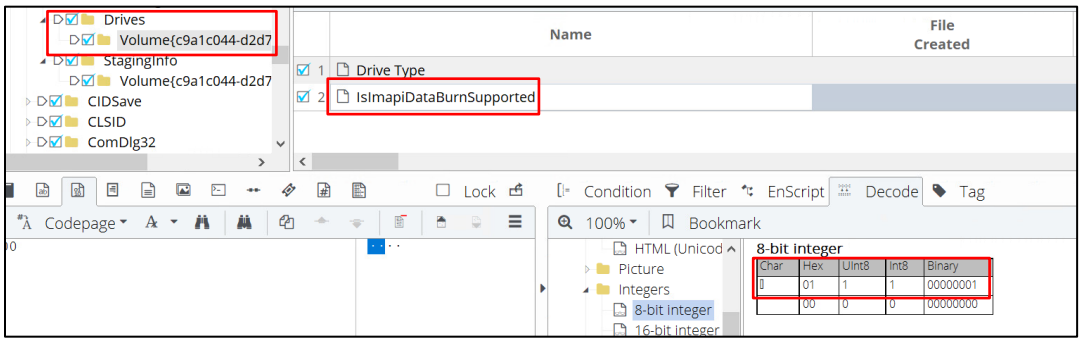
Item Path: CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft\Windows\CurrentVersion\Explorer\CD Burning\StagingInfo\Volume{c9a1c044-d2d7-11e4-9dae-806e6f6e6963}\StagingPath



Drives Registry Entry:

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\NTUSER.DAT\CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft\Windows\CurrentVersion\Explorer\CD Burning\Drives\Volume{c9a1c044-d2d7-11e4-9dae-806e6f6e6963}\IsImapiDataBurnSupported

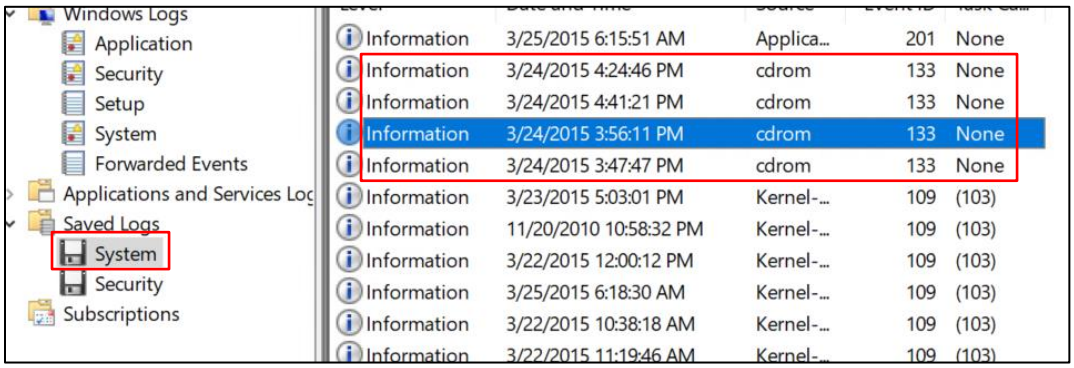
Item Path: CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft\Windows\CurrentVersion\Explorer\CD Burning\Drives\Volume{c9a1c044-d2d7-11e4-9dae-806e6f6e6963}\IsImapiDataBurnSupported



Event ID 133: Event ID 133 in the **System log** (Kernel-Power) indicates that the CD/DVD drive or other external device entered an idle or low-power state due to inactivity, which could be linked to pauses in the burning process or inactivity after the burning was completed.

True Path: Data Leak Case -2 Jeel\cfreds_2015_data_leakage_pc\D\Windows\System32\winevt\Logs\
Item Path: cfreds_2015_data_leakage_pc\D\Windows\System32\winevt\Logs\

Targeted File: System.evtx

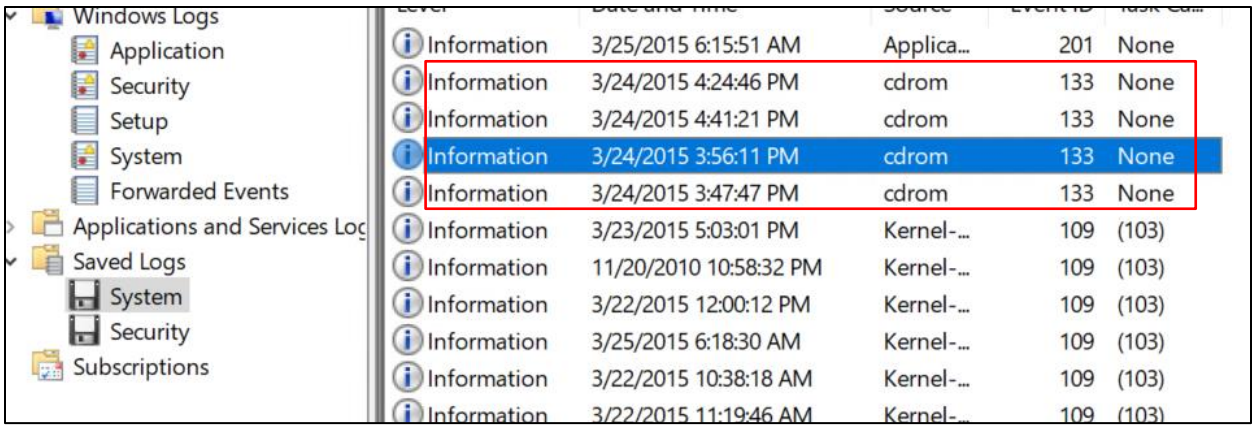


33. When did the suspect burn CD-R?
[Hint: It may be one or more times.]
Answer:

Timestamp	Device	Source	Description
3/24/2015 3:47:47 PM	cdrom	Event Log (System)	Burning Type 2: With a CD/DVD/ player (Mastered)
3/24/2015 3:56:11 PM	cdrom	Event Log (System)	Burning Type 2: With a CD/DVD/ player (Mastered)
3/24/2015 4:24:46 PM	cdrom	Event Log (System)	Burning Type 2: With a CD/DVD/ player (Mastered)
3/24/2015 4:41:21 PM	cdrom	Event Log (System)	Burning Type 2: With a CD/DVD/ player (Mastered)

True Path: Data Leak Case -2 Jeel\cfreds_2015_data_leakage_pc\D\Windows\System32\winevt\Logs\
Item Path: cfreds_2015_data_leakage_pc\D\Windows\System32\winevt\Logs\

Targeted File: System.evtx



34. What files were copied from PC to CD-R?

[Hint: Just use PC image only. You can examine transaction logs of the file system for this task.]

Answer:

winter_storm.amr
winter_whether_advisory.zip
my_favorite_cars.db
new_years_day.jpg
my_smartphone.png
Koala.jpg
Tulips.jpg

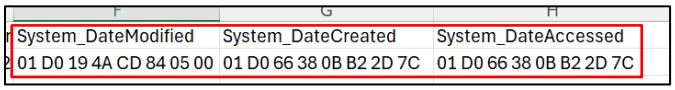
File Evidence from Windows.edb:

The file winter_whether_advisory.zip located at ***C:\Users\informant\Desktop\S data\Secret Project Data\design\winter_whether_advisory.zip*** was found in ***Windows.edb***, indicating recent access and potential staging for burning to the CD-R.

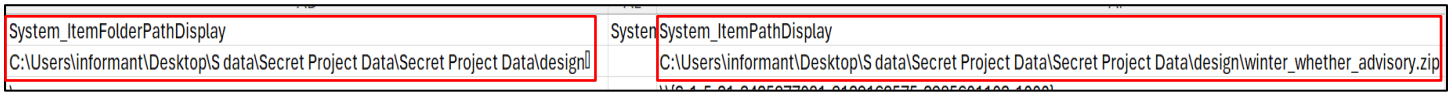
True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb

Item Path:

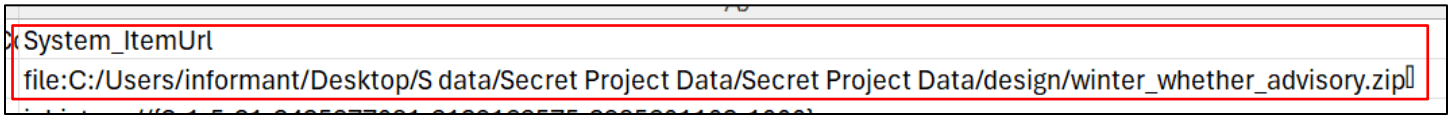
cfreds_2015_data_leakage_pc\D\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb



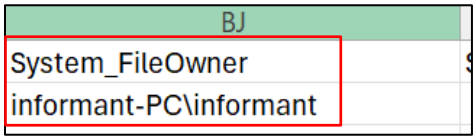
System_DateModified	System_DateCreated	System_DateAccessed
01 D0 19 4A CD 84 05 00	01 D0 66 38 0B B2 2D 7C	01 D0 66 38 0B B2 2D 7C



System_ItemFolderPathDisplay	System_ItemPathDisplay
C:\Users\informant\Desktop\S data\Secret Project Data\Secret Project Data\design	C:\Users\informant\Desktop\S data\Secret Project Data\Secret Project Data\design\winter_whether_advisory.zip



System_ItemUrl
file:C:/Users/informant/Desktop/S data/Secret Project Data/Secret Project Data/design/winter_whether_advisory.zip

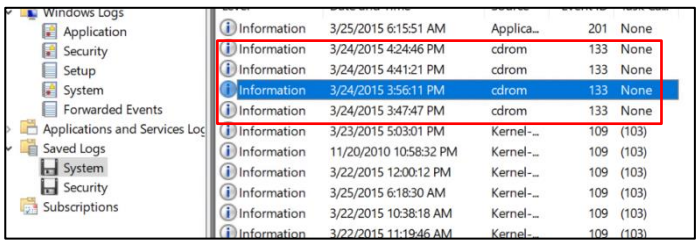


BJ
System_FileOwner
informant-PC\informant

Event ID 133 Log Entries:

- **3:47:47 PM on 3/24/2015** - CD/DVD drive entered idle state, likely marking the end of the burning session.
- **3:56:11 PM, 4:24:46 PM**, and 4:41:21 PM - Additional idle entries confirm no further activity, indicating the CD-R burn process had concluded.

The presence of ***winter_whether_advisory.zip*** in ***Windows.edb*** with recent access details, along with the ***Event ID 133*** idle timestamps, suggests that this file was likely copied to the CD-R in a session ending around ***3:47 PM on 3/24/2015.*** This aligns the file access evidence from ***Windows.edb*** with the timeline of the burning session.



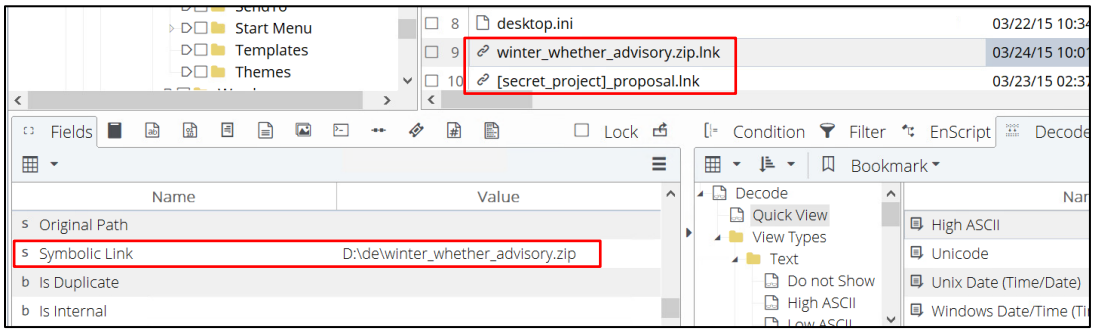
35. What files were opened from CD-R?

Answer:

D:\de\winter_whether_advisory.zip\
D:\de\winter_whether_advisory.zip\ppt\
D:\de\winter_whether_advisory.zip\ppt\slides\
D:\de\winter_whether_advisory.zip\ppt\slideMasters\
D:\de\winter_whether_advisory.zip
D:\Penguins.jpg
D:\Koala.jpg
D:\Tulips.jpg

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\
Item Path: cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\
Item Path: cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\

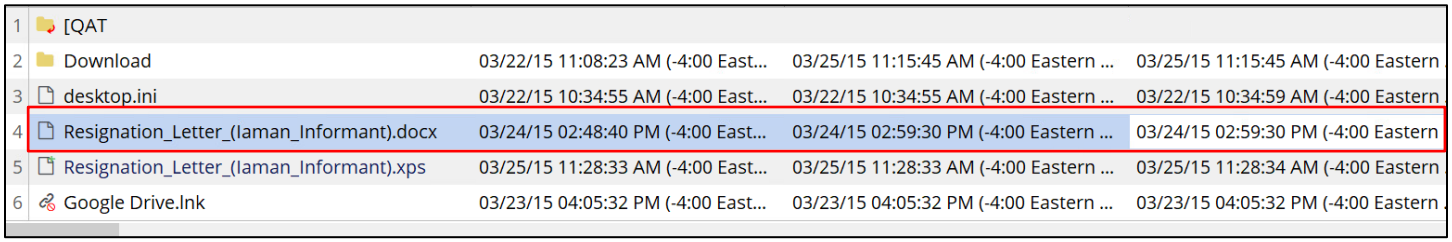


36. Identify all timestamps related to a resignation file in Windows Desktop.
[Hint: the resignation file is a DOCX file in NTFS file system.]

Answer:

Timestamp Type	Timestamp
Created	03/24/2015 2:48:40 PM
Modified	03/24/2015 2:59:30 PM
Accessed	03/25/2015 11:15:45 AM
Entry Modified	2015-03-24 14:59:30

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\Desktop\Resignation_Letter_(Iaman_Informant).docx
Item Path: cfreds_2015_data_leakage_pc\D\Users\informant\Desktop\Resignation_Letter_(Iaman_Informant).docx



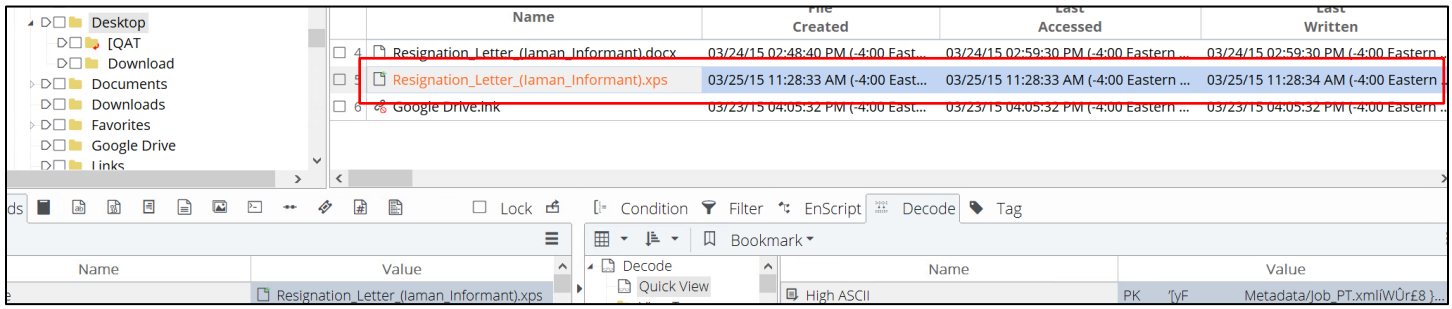
37. How and when did the suspect print a resignation file?

Answer:

Question	Description
How	The suspect used the Microsoft XPS Document Writer, a virtual printer that creates XPS files.
When	The resignation file was "printed" as an XPS file on March 25, 2015, at 11:28:33 AM (Eastern Time).

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\Desktop\Resignation_Letter_(Iaman_Informant).xps

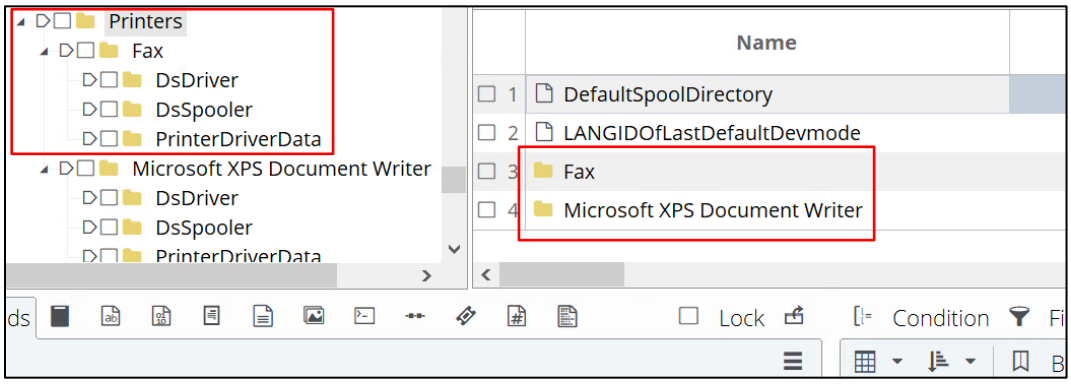
Item Path: cfreds_2015_data_leakage_pc\D\Users\informant\Desktop\Resignation_Letter_(Iaman_Informant).xps



Existence of Printer:

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Windows\System32\config\SOFTWARE\CMI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\Microsoft\Windows NT\CurrentVersion\Print\Printers\

Item Path: CMI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\Microsoft\Windows NT\CurrentVersion\Print\Printers\



38. Where are 'Thumbcache' files located?

Answer:

cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Microsoft\Windows\Explorer\thumbcache_32.db
cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Microsoft\Windows\Explorer\thumbcache_64.db
cfreds_2015_data_leakage_pc\D\\Users\informant\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db
cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Microsoft\Windows\Explorer\thumbcache_1024.db
cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Microsoft\Windows\Explorer\thumbcache_idx.db
cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Microsoft\Windows\Explorer\thumbcache_sr.db

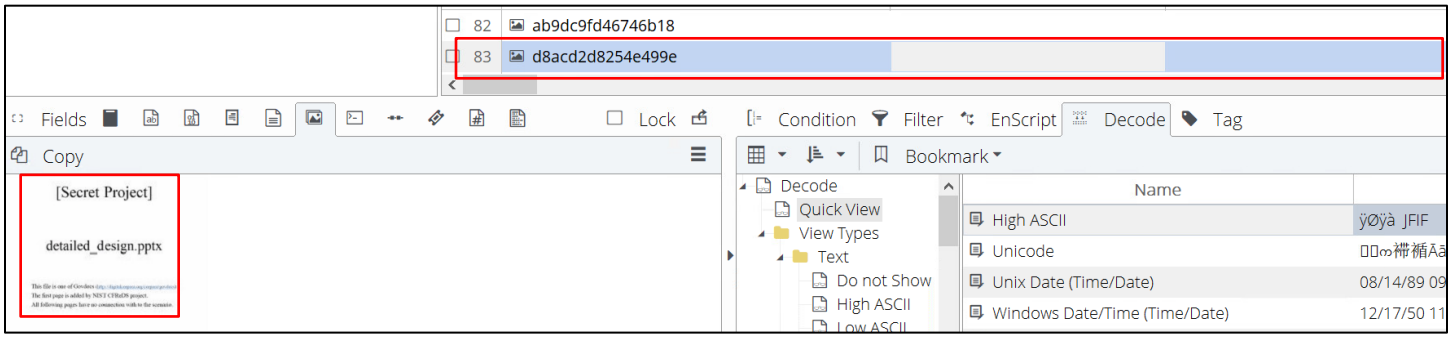
True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Microsoft\Windows\Explorer\
Item path: cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Microsoft\Windows\Explorer\

3	thumbcache_idx.db	03/22/15 10:35:02 AM (-4:00 East...	03/22/15 10:35:02 AM (-4:00 Eastern ...	03/24/15 10:44:13 AM (-4:00 Eastern
4	thumbcache_32.db	03/22/15 10:35:02 AM (-4:00 East...	03/22/15 10:35:02 AM (-4:00 Eastern ...	03/22/15 10:35:02 AM (-4:00 Eastern
5	thumbcache_96.db	03/22/15 10:35:02 AM (-4:00 East...	03/22/15 10:35:02 AM (-4:00 Eastern ...	03/22/15 10:35:02 AM (-4:00 Eastern
6	thumbcache_256.db	03/22/15 10:35:02 AM (-4:00 East...	03/22/15 10:35:02 AM (-4:00 Eastern ...	03/22/15 10:35:02 AM (-4:00 Eastern
7	thumbcache_1024.db	03/22/15 10:35:02 AM (-4:00 East...	03/22/15 10:35:02 AM (-4:00 Eastern ...	03/22/15 10:35:02 AM (-4:00 Eastern
8	thumbcache_sr.db	03/22/15 10:35:02 AM (-4:00 East...	03/22/15 10:35:02 AM (-4:00 Eastern ...	03/22/15 10:35:02 AM (-4:00 Eastern

39. Identify traces related to confidential files stored in Thumbcache.
(Include '256' only)

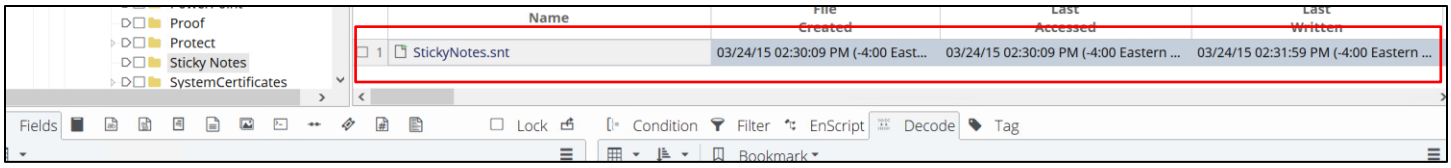
Answer:

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db\



40. Where are Sticky Note files located?
Answer:
cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Roaming\Microsoft\Sticky Notes\StickyNotes.snt

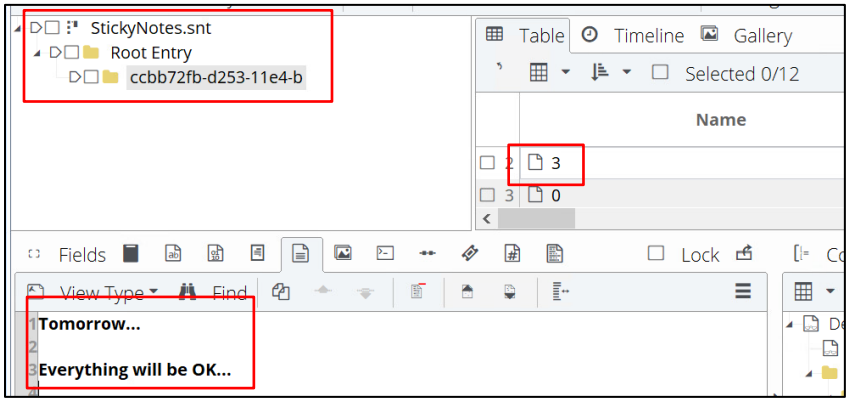
True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Roaming\Microsoft\Sticky Notes\StickyNotes.snt
Item Path: cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Roaming\Microsoft\Sticky Notes\StickyNotes.snt

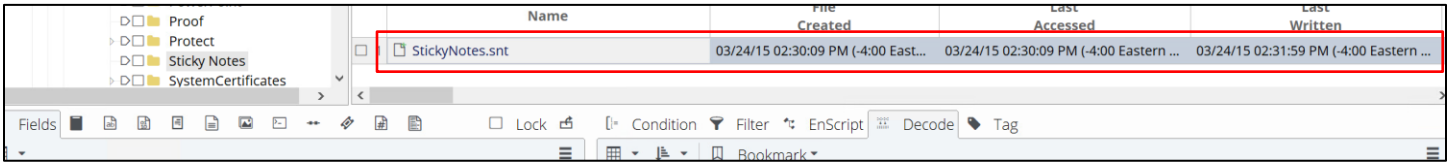


41. Identify notes stored in the Sticky Note file.
Answer:
Timestamp: 03/24/15 02:31:59 PM (-4:00 Eastern Daylight Time)
Content:
Tomorrow...

Everything will be OK...

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Roaming\Microsoft\Sticky Notes\StickyNotes.snt\Root Entry\ccbb72fb-d253-11e4-b\3
Item Path: Root Entry\ccbb72fb-d253-11e4-b\3





42. Was the 'Windows Search and Indexing' function enabled? How can you identify it? If it was enabled, what is a file path of the 'Windows Search' index database?

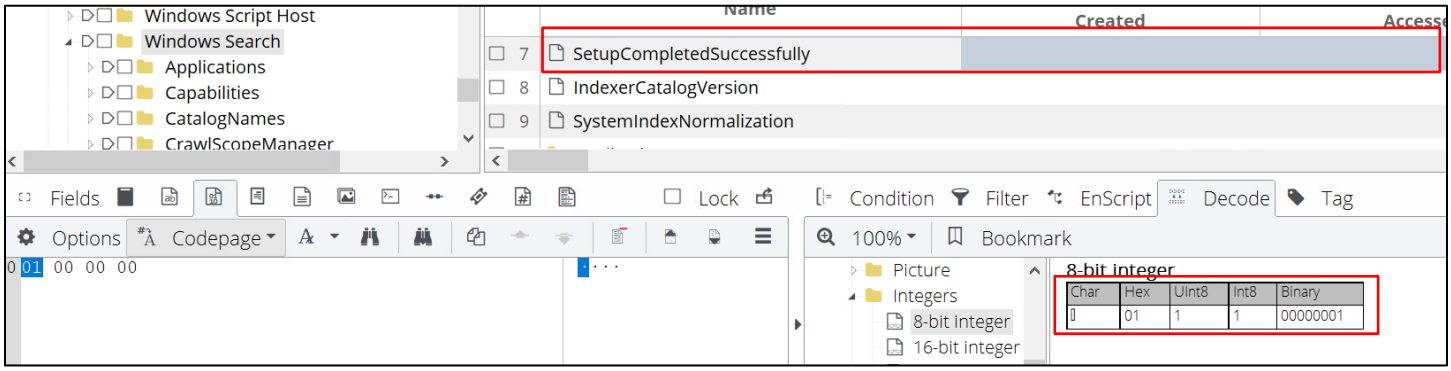
Answer:

Search & Indexing	Enabled
DB File path	cfreds_2015_data_leakage_pc\D\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb

Verification:

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Windows\System32\config\SOFTWARE\CMI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\Microsoft\Windows Search\SetupCompletedSuccessfully

Item Path: CMI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\Microsoft\Windows Search\SetupCompletedSuccessfully

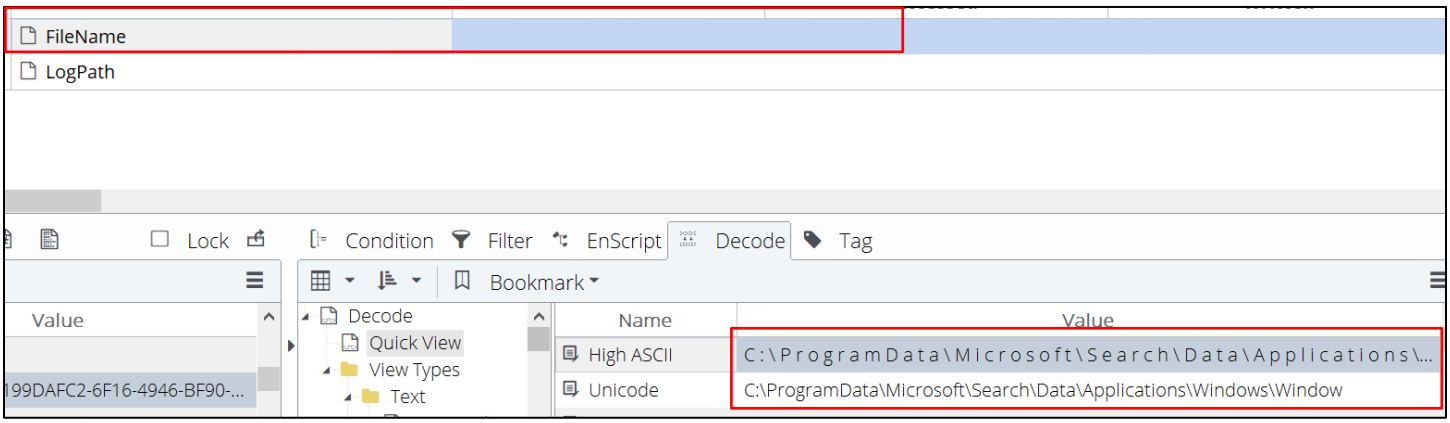


This value is set to 1, it indicates that Windows Search and Indexing was enabled.

File Location verification:

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Windows\System32\config\SOFTWARE\CMI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\Microsoft\Windows Search\Databases\Windows\FileName

Item Path: CMI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\Microsoft\Windows Search\Databases\Windows\FileName



43. What kinds of data were stored in Windows Search database?

Answer:

Sticky Note

File metadata and timestamps

Document text content and metadata

Email details (subject, sender, body)

Browser history (URLs, titles)

Contacts information

Text from supported files and system data

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb

Item Path:

cfreds_2015_data_leakage_pc\D\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb

Se	System_ItemFolderPathDisplay	Systen	System_ItemPathDisplay
3	C:\Users\informant\Desktop\S data\Secret Project Data\Secret Project Data\design		C:\Users\informant\Desktop\S data\Secret Project Data\Secret Project Data\desig
2	\		\\{S-1-5-21-2425377081-3129163575-2985601102-1000}
2	\\{S-1-5-21-2425377081-3129163575-2985601102-1000}		\\{S-1-5-21-2425377081-3129163575-2985601102-1000}\notes
5	\		\\{S-1-5-21-2425377081-3129163575-2985601102-1003}
	\		\\{S-1-5-21-2425377081-3129163575-2985601102-1001}
	\		\\{S-1-5-21-2425377081-3129163575-2985601102-1000}
	C:\Users\Default		C:\Users\Default\NTUSER.DAT.LOG2
	C:\Users\Public		C:\Users\Public\Favorites
	C:\Users\Default		C:\Users\Default\Desktop
	C:\Users\Default		C:\Users\Default\Downloads
	C:\Users\Default		C:\Users\Default\Music
	C:\Users\Default		C:\Users\Default\Pictures
	C:\Users\Default		C:\Users\Default\Links

System_Search_ReverseFileName	System_C	System_ItemUrl
piz.yrosivda_rehtehw_retniw		file:C:/Users/informant/Desktop/S data/Secret Project Data/Secret Project Data/design/winter_wh
		iehistory://{S-1-5-21-2425377081-3129163575-2985601102-1000}
		StickyNotes://{S-1-5-21-2425377081-3129163575-2985601102-1000}/notes
		csc://{S-1-5-21-2425377081-3129163575-2985601102-1003}@
		csc://{S-1-5-21-2425377081-3129163575-2985601102-1001}@
		csc://{S-1-5-21-2425377081-3129163575-2985601102-1000}@
2GOL.TAD.RESUTN		file:C:/Users/Default/NTUSER.DAT.LOG2`
setirovaF		file:C:/Users/Public/Favorites
potkseD		file:C:/Users/Default/Desktop
sdaolnwoD		file:C:/Users/Default/Downloads
cisuM`		file:C:/Users/Default/Music
serutciP		file:C:/Users/Default/Pictures
skniL`		file:C:/Users/Default/Links
setirovaF		file:C:/Users/Default/Favorites
soediV@		file:C:/Users/Default/Videos
semaG devaS		file:C:/Users/Default/Saved Games
sm-snartger.10000000000000000000reniatnoCMT.}ce3edcb0e100-d1d8-ec		file:C:/Users/Default/NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000
flb.MT.}ce3edcb0e100-d1d8-ed11-f6c6-db888610{TAD.RESUTN		file:C:/Users/Default/NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf
sm-snartger.20000000000000000000reniatnoCMT.}ce3edcb0e100-d1d8-ec		file:C:/Users/Default/NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000

IT	IU	IV	IW	IX	IY	IZ	JA	JB	JC	JD	JE	JF	JG	JH	JI	
System_Ite	System_C	System_Ti	System_Su	System_Au	System_Ke	System_k	System_Comment	System_Ite	System_Fi	System_D	System_D	System_D	System_D	System_M	System_Id	Sy
File folder								Start Menu								01
File folder								Users								01
Shortcut							Choose which progra	Default Pr	.lnk							01
Configuration settings@								desktop.in	.ini							01
File folder								Programs								01
Shortcut							Delivers software up	Windows U	.lnk							01

44. Find traces of Internet Explorer usage stored in Windows Search database.
(It should be considered only during a date range between 2015-03-22 and 2015-03-23.)

Answer:

Date Modified	Microsoft IE TargetUrl
2015-03-22 11:09:22	http://windows.microsoft.com/en-us/internet-explorer/ie-8-welcome
2015-03-22 11:09:23	http://www.msn.com/?ocid=iehp
2015-03-22 11:09:40	https://www.google.com/?gws_rd=ssl
2015-03-22 11:09:50	https://www.google.com/search?hl=en&source=hp&q=internet+explorer+11&gbv=2&oq=internet+explorer+11&gs_l=heirloom-hp.3..0l10.5163.7893.0.9562.20.13.0.7.7.0.156.1110.11j2.13.0.msedr...0...1ac.1.34.heirloom-hp..0.20.1250.5j7Xm44tv5w
2015-03-22 11:09:52	http://www.google.com/url?url=http://windows.microsoft.com/en-us/internet-explorer/download-ie&rct=j&frm=1&q=&esrc=s&sa=U&ei=6ykQVZWLGbeJsQT7goDACg&ved=0CB8QFjAA&usg=AFQjCNEwsIz17kY-jTXbaWPcQDfBbVEi7A
2015-03-22 11:09:54	http://windows.microsoft.com/en-us/internet-explorer/download-ie
2015-03-22 11:09:56	http://www.google.com/url?url=http://windows.microsoft.com/en-us/internet-explorer/ie-11-worldwide-languages&rct=j&frm=1&q=&esrc=s&sa=U&ei=6ykQVZWLGbeJsQT7goDACg&ved=0CCoQFjAB&usg=AFQjCNE7UKIWEBiWO2N96IFeo6ZywhRLfw
2015-03-22 11:10:24	http://windows.microsoft.com/en-us/internet-explorer/ie-11-worldwide-languages
2015-03-22 11:10:54	https://www.google.com/webhp?hl=en
2015-03-22 11:10:58	https://www.google.com/chrome/index.html?hl=en&brand=CHNG&utm_source=en-hpp&utm_medium=hpp&utm_campaign=en
2015-03-22 11:11:06	http://download.microsoft.com/download/7/1/7/7179A150-F2D2-4502-9D70-4B59EA148EAA/IE11-Windows6.1-x64-en-us.exe
2015-03-22 11:11:16	https://www.google.com/chrome/browser/thankyou.html?brand=CHNG&platform=win&clickonceinstalled=1
2015-03-23 13:26:33	https://odc.officeapps.live.com/odc/emailhrd?lcid=1033&syslcid=1033&uilcid=1033&app=5&ver=15&build=15.0.4420&p=0&a=1&hm=1&sp=0
2015-03-23 13:27:49	http://www.microsoft.com/en-us/ie-firstrun/win-7/ie-11/vie
2015-03-23 13:27:49	http://www.bing.com/search
2015-03-23 13:27:49	http://go.microsoft.com/fwlink/?LinkId=69157
2015-03-23 13:28:19	http://www.bing.com/
2015-03-23 14:07:52	http://www.bing.com/news/search?q=Top Stories&FORM=NSBABR
2015-03-23 14:07:55	http://www.bing.com/search?q=Top+Stories&FORM=HDRSC1
2015-03-23 14:07:58	http://www.bing.com/news/search?q=file+sharing+and+tethering&FORM=HDRSC6
2015-03-23 14:08:00	http://www.bing.com/search?q=file+sharing+and+tethering&qs=n&form=QBLH&pq=file+sharing+and+tethering&sc=0-18&sp=-1&sk=&cvid=171b77e4ffd54b2a92c4e97abf995fe1
2015-03-23 14:08:18	http://sysinfotools.com/blog/tethering-internet-files-sharing/
2015-03-23 14:11:13	http://resources.infosecinstitute.com/windows-systems-and-artifacts-in-digital-forensics-part-i-registry/
2015-03-23 14:12:08	https://technet.microsoft.com/en-us/library/cc162846.aspx
2015-03-23 14:12:45	https://support.microsoft.com/en-us/kb/308427
2015-03-23 14:12:52	http://en.wikipedia.org/wiki/Event_Viewer
2015-03-23 14:13:58	https://msdn.microsoft.com/en-us/library/windows/desktop/dd562212(v=vs.85).aspx

2015-03-23 14:14:25	http://www.forensicswiki.org/wiki/USB_History_Viewing
2015-03-23 16:43:48	http://www.bing.com/search?q=external%20device%20and%20forensics&qs=n&form=QBRE&pq=external%20device%20and%20forensics&sc=8-9&sp=-1&sk=&cvid=c30c4b1f36114b1c9bc683838c69823a
2015-03-23 16:43:50	http://www.bing.com/?FORM=Z9FD1
2015-03-23 16:43:52	http://www.bing.com/news?FORM=Z9LH3
2015-03-23 16:44:58	http://www.bing.com/news?q=science+technology+news&FORM=NWBTCB
2015-03-23 16:45:22	http://www.wired.com/?p=1756538
2015-03-23 16:45:30	http://www.bing.com/news?q=Soccer+News&FORM=NSBABR
2015-03-23 16:53:47	http://www.bing.com/news?q=top+stories&FORM=NWRFSH
2015-03-23 16:55:09	http://www.bing.com/news?q=us+news&FORM=NSBABR
2015-03-23 16:55:10	http://www.bing.com/news?q=world+news&FORM=NSBABR
2015-03-23 16:55:17	http://www.bing.com/news?q=local&FORM=NSBABR
2015-03-23 16:55:18	http://www.bing.com/news?q=entertainment+news&FORM=NSBABR
2015-03-23 16:55:29	http://www.bing.com/news?q=science+technology+news&FORM=NSBABR
2015-03-23 16:55:55	http://www.bing.com/news?q=business+news&FORM=NSBABR
2015-03-23 16:55:56	http://www.bing.com/news?q=political+news&FORM=NSBABR
2015-03-23 16:55:57	http://www.bing.com/news?q=sports+news&FORM=NSBABR
2015-03-23 16:55:59	http://www.bing.com/news?q=health+news&FORM=NSBABR
2015-03-23 16:56:09	http://www.bing.com/news?q=top+stories&FORM=NSBABR
2015-03-23 16:56:33	http://www.wired.com/2015/03/stealing-data-computers-using-heat/

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb
Item Path: cfreds_2015_data_leakage_pc\D\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb

Target	URL	Artifact Path
cfreds_2015_data_	http://www.bing.com/search?q=external device	Internet\Internet Explorer (Windows)\History\Daily\WebCach
cfreds_2015_data_	http://www.bing.com/search	Internet\Internet Explorer (Windows)\History\Daily\WebCach
cfreds_2015_data_	http://www.bing.com/news?q=business+news&	Internet\Internet Explorer (Windows)\History\Daily\WebCach
cfreds_2015_data_	http://www.bing.com/news?q=sports+news&FO	Internet\Internet Explorer (Windows)\History\Daily\WebCach
cfreds_2015_data_	http://www.bing.com/news?q=local&FORM=NSE	Internet\Internet Explorer (Windows)\History\Daily\WebCach
cfreds_2015_data_	http://www.bing.com/news?q=health+news&FO	Internet\Internet Explorer (Windows)\History\Daily\WebCach
cfreds_2015_data_	http://www.bing.com/news?q=science+technology+news&FORM=NSBABR	r (Windows)\History\Daily\WebCach
cfreds_2015_data_	http://www.bing.com/news?q=top+stories&FOR	Internet\Internet Explorer (Windows)\History\Daily\WebCach
cfreds_2015_data_	http://www.bing.com/news?q=entertainment+n	Internet\Internet Explorer (Windows)\History\Daily\WebCach
cfreds_2015_data_	http://www.bing.com/news?FORM=Z9LH3	Internet\Internet Explorer (Windows)\History\Daily\WebCach

We have exported the ***Windows.edb*** file; however, due to tool limitations in extracting Internet Explorer artifacts from this database, retrieving relevant IE activity is challenging. Therefore, we will proceed with analyzing Internet Activity Artifacts in EnCase, which provides direct access to browser history and cache data.

45. List the e-mail communication stored in Windows Search database.
(It should be considered only during a date range between 2015-03-23 and 2015-03-24.)
Answer:

Timestamp	E-Mail Communication	
2015-03-23 13:29:29	Source	[Inbox]
	From → To	spy.conspirator@nist.gov → iaman.informant@nist.gov
	Subject	Hello, Iaman
	Body	How are you doing?
2015-03-23 14:44:32	Source	[Sent Items]
	From → To	iaman.informant@nist.gov → spy.conspirator@nist.gov
	Subject	RE: Hello, Iaman
	Body	Successfully secured. --- From: spy Sent: Monday, March 23, 2015 1:29 PM To: iaman Subject: Hello, Iaman How are you doing?
2015-03-23 15:14:58	Source	[Inbox]
	From → To	spy.conspirator@nist.gov → iaman.informant@nist.gov
	Subject	Good job, buddy.
	Body	Good, job. I need a more detailed data about this business.
2015-03-23 15:19:22	Source	[Sent Items]
	From → To	iaman.informant@nist.gov → spy.conspirator@nist.gov
	Subject	Good job, buddy.
	Attachment	space_and_earth.mp4
	Body	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.
2015-03-23 15:20:41	Source	[Inbox]
	From → To	spy.conspirator@nist.gov → iaman.informant@nist.gov
	Subject	RE: Good job, buddy.
	Body	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.

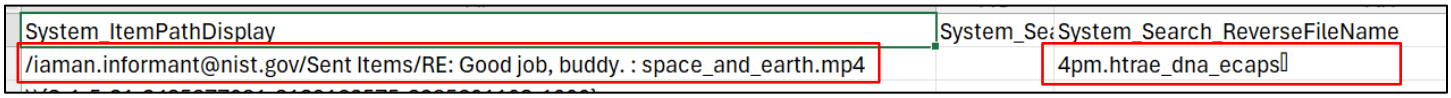
		This is a sample. ---------- From: spy Sent: Monday, March 23, 2015 3:15 PM To: iaman Subject: Good job, buddy. Good, job. I need a more detailed data about this business.
2015-03-23 15:26:22	Source	[Inbox]
	From → To	spy.conspirator@nist.gov → iaman.informant@nist.gov
	Subject	Important request
	Body	I confirmed it. But, I need a more data. Do your best.
2015-03-23 15:27:05	Source	[Sent Items]
	From → To	iaman.informant@nist.gov → spy.conspirator@nist.gov
	Subject	RE: Important request
	Body	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.
2015-03-23 16:38:48	Source	[Sent Items]
	From → To	iaman.informant@nist.gov → spy.conspirator@nist.gov
	Subject	It's me
	Body	Use links below, https://drive.google.com/file/d/0Bz0ye6gXtiZaVl8yVU5mWHlGbWc/view?usp=sharing https://drive.google.com/file/d/0Bz0ye6gXtiZaakx6d3R3c0JmM1U/view?usp=sharing
2015-03-23 16:41:19	Source	[Inbox]
	From → To	spy.conspirator@nist.gov → iaman.informant@nist.gov
	Subject	RE: It's me
	Body	I got it. ---------- From: iaman Sent: Monday, March 23, 2015 4:39 PM To: spy Subject: It's me

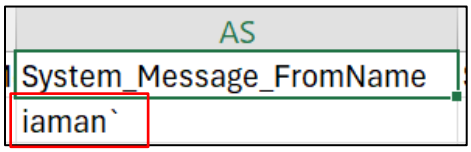
		Use links below, https://drive.google.com/file/d/0Bz0ye6gXtiZaVl8yVU5mWHlGbWc/view?usp=sharing https://drive.google.com/file/d/0Bz0ye6gXtiZaakx6d3R3c0JmM1U/view?usp=sharing
2015-03-24 09:25:57	Source	[Inbox]
	From → To	spy.conspirator@nist.gov → iaman.informant@nist.gov
	Subject	Last request
	Body	This is the last request. I want to get the remaining data.
2015-03-24 09:30:11	Source	[Sent Items]
	From → To	iaman.informant@nist.gov → spy.conspirator@nist.gov
	Subject	RE: Last request
	Body	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.
2015-03-24 09:33:45	Source	[Inbox]
	From → To	spy.conspirator@nist.gov → iaman.informant@nist.gov
	Subject	RE: Last request
	Body	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.
2015-03-24 09:35:10	Source	[Sent Items]
	From → To	iaman.informant@nist.gov → spy.conspirator@nist.gov
	Subject	RE: Last request

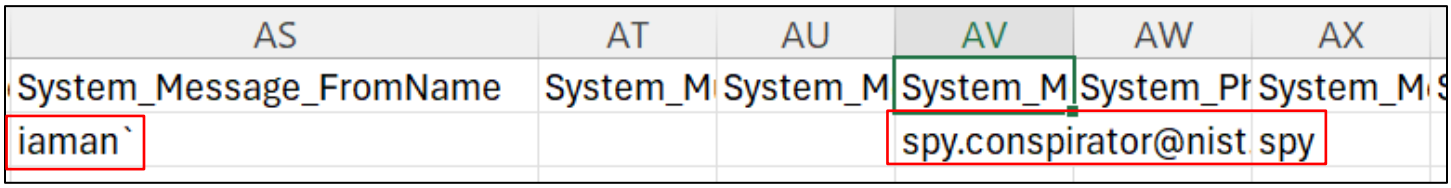
	Body	This is the last time.. ---------- From: spy Sent: Tuesday, March 24, 2015 9:34 AM To: iaman Subject: RE: Last request No problem. U can directly deliver storage devices that stored it. ---------- From: iaman Sent: Tuesday, March 24, 2015 9:30 AM To: spy Subject: RE: Last request Stop it! It is 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.
2015-03-24 15:32:42	Source	[Inbox]
	From → To	spy.conspirator@nist.gov → iaman.informant@nist.gov
	Subject	Watch out!
	Body	USB device may be easily detected. So, try another method.
2015-03-24 15:34:02	Source	[Sent Items]
	From → To	iaman.informant@nist.gov → spy.conspirator@nist.gov
	Subject	RE: Watch out!
	Body	I am trying. ---------- 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.
2015-03-24 17:05:10	Source	[Sent Items]
	From → To	iaman.informant@nist.gov → spy.conspirator@nist.gov
	Subject	Done
	Body	It's done. See you tomorrow.

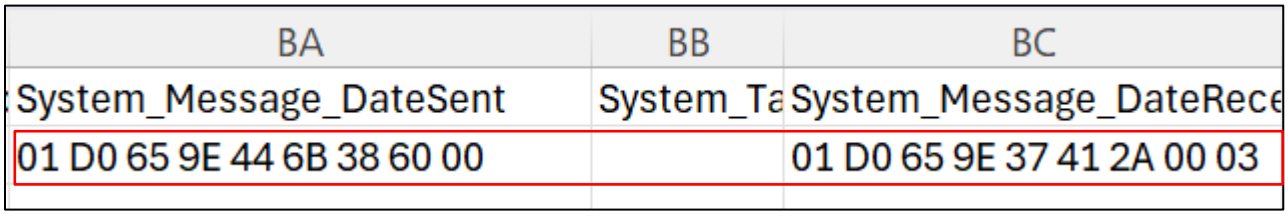
True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb
Item Path:
cfreds_2015_data_leakage_pc\D\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb

Example of Verification:









Result:

2015-03-23 15:19:22	Source	[Sent Items]
	From → To	iaman.informant@nist.gov → spy.conspirator@nist.gov
	Subject	Good job, buddy.
	Attachment	space_and_earth.mp4

46. List files and directories related to Windows Desktop stored in Windows Search database. (Windows Desktop directory: \Users\informant\Desktop\)

Answer:

Date Created	Full Path
2015-03-23 16:05:33	C:\\Users\\informant\\Desktop\\Google Drive.lnk
2015-03-24 09:40:09	C:\\Users\\informant\\Desktop\\S data\\Secret Project Data\\Secret Project Data\\design\\space_and_earth.mp4
2015-03-24 09:40:09	C:\\Users\\informant\\Desktop\\S data\\Secret Project Data\\Secret Project Data\\design\\winter_whether_advisory.zip
2015-03-24 09:40:10	C:\\Users\\informant\\Desktop\\S data\\Secret Project Data\\Secret Project Data\\design\\winter_storm.amr
2015-03-24 09:40:11	C:\\Users\\informant\\Desktop\\S data\\Secret Project Data\\Secret Project Data\\proposal\\[secret_project]_detailed_proposal.docx

2015-03-24 09:40:13	C:\\Users\\informant\\Desktop\\S data\\Secret Project Data\\Secret Project Data\\proposal\\[secret_project]_proposal.docx
2015-03-24 09:47:58	C:\\Users\\informant\\Desktop\\S data\\Secret Project Data\\Secret Project Data\\design\\[secret_project]_detailed_design.pptx
2015-03-24 09:47:58	C:\\Users\\informant\\Desktop\\S data\\Secret Project Data\\Secret Project Data\\final\\[secret_project]_final_meeting.pptx
2015-03-24 09:47:58	C:\\Users\\informant\\Desktop\\S data\\Secret Project Data\\Secret Project Data\\pricing decision\\(secret_project)_market_analysis.xlsx
2015-03-24 09:47:58	C:\\Users\\informant\\Desktop\\S data\\Secret Project Data\\Secret Project Data\\pricing decision\\(secret_project)_market_shares.xls
2015-03-24 09:47:58	C:\\Users\\informant\\Desktop\\S data\\Secret Project Data\\Secret Project Data\\pricing decision\\(secret_project)_price_analysis_#1.xlsx
2015-03-24 09:47:59	C:\\Users\\informant\\Desktop\\S data\\Secret Project Data\\Secret Project Data\\proposal
2015-03-24 14:48:41	C:\\Users\\informant\\Desktop\\Resignation_Letter_(Iaman_Informant).docx
2015-03-24 15:52:06	C:\\Users\\informant\\Desktop\\temp
2015-03-24 15:52:36	C:\\Users\\informant\\Desktop\\temp\\IE11-Windows6.1-x64-en-us.exe
2015-03-24 15:52:47	C:\\Users\\informant\\Desktop\\temp\\Chrysanthemum.jpg
2015-03-24 15:52:47	C:\\Users\\informant\\Desktop\\temp\\Hydrangeas.jpg
2015-03-24 15:52:47	C:\\Users\\informant\\Desktop\\temp\\Desert.jpg
2015-03-24 15:52:47	C:\\Users\\informant\\Desktop\\temp\\Lighthouse.jpg
2015-03-24 15:52:47	C:\\Users\\informant\\Desktop\\temp\\Koala.jpg
2015-03-24 15:52:47	C:\\Users\\informant\\Desktop\\temp\\Jellyfish.jpg
2015-03-24 15:52:47	C:\\Users\\informant\\Desktop\\temp\\Tulips.jpg
2015-03-24 15:52:47	C:\\Users\\informant\\Desktop\\temp\\Penguins.jpg

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb
Item Path: cfreds_2015_data_leakage_pc\D\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb

Verification:

	01 CA 04 31 FD A9 A3 6E	01 CA 04 41 30 6B 6C D1	C:\Users\Default\Documents
	01 CA 04 31 FD AE 66 22	01 CA 04 41 30 79 B5 13	C:\Users\Public\Public Documents
	01 CA 04 44 80 28 22 35	01 CA 04 44 7B DA 05 16	C:\Users\Public\Public Videos\Sample Videos\Wildlife.wmv
	01 CA 04 44 80 2F 46 56	01 CA 04 44 7B E3 8A 97	C:\Users\Public\Public Music\Sample Music\Sleep Away.mp3
	01 CA 04 44 80 31 A7 B6	01 CA 04 44 7B E3 8A 97	C:\Users\Public\Public Music\Sample Music\Maid with the Flaxen Hair.mp3
	01 D0 66 6C 19 BE 93 F5	01 D0 66 6C 19 BE 93 F5	C:\Users\informant\Desktop\temp\Hydrangeas.jpg
	01 D0 66 6C 19 BE 93 F5	01 D0 66 6C 19 BE 93 F5	C:\Users\informant\Desktop\temp\Desert.jpg
	01 CA 04 44 80 31 A7 B6	01 CA 04 44 7B E8 4D 57	C:\Users\Public\Public Pictures\Sample Pictures\Koala.jpg
	01 CA 04 44 80 31 A7 B6	01 CA 04 44 7B E8 4D 57	C:\Users\Public\Public Pictures\Sample Pictures\Hydrangeas.jpg
	01 CA 04 44 80 31 A7 B6	01 CA 04 44 7B E5 EB F7	C:\Users\Public\Public Music\Sample Music\Kalimba.mp3
	01 D0 66 6C 19 C0 F5 56	01 D0 66 6C 19 C0 F5 56	C:\Users\informant\Desktop\temp\Koala.jpg
	01 CA 04 44 80 31 A7 B6	01 CA 04 44 7B E8 4D 57	C:\Users\Public\Public Pictures\Sample Pictures\Desert.jpg
	01 CA 04 44 80 34 09 16	01 CA 04 44 7B EA AE B8	C:\Users\Public\Public Pictures\Sample Pictures\Tulips.jpg
	01 D0 66 6C 19 BC 32 95	01 D0 66 6C 19 BC 32 95	C:\Users\informant\Desktop\temp\Chrysanthemum.jpg
	01 CA 04 44 80 31 A7 B6	01 CA 04 44 7B E8 4D 57	C:\Users\Public\Public Pictures\Sample Pictures\Penguins.jpg
	01 D0 66 6C 19 C3 56 B6	01 D0 66 6C 19 C3 56 B6	C:\Users\informant\Desktop\temp\Penguins.jpg

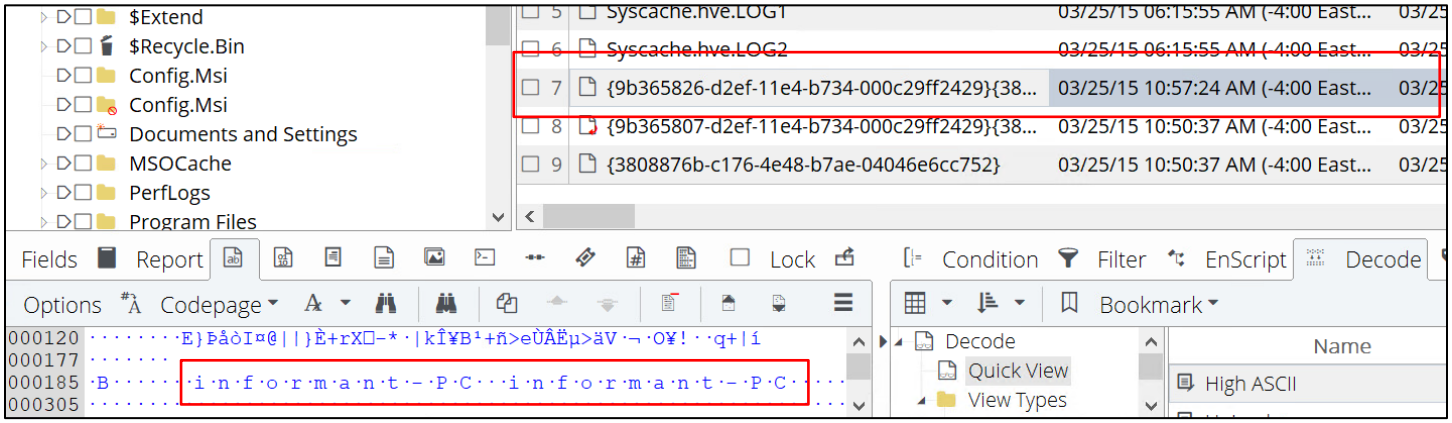
47. Where are Volume Shadow Copies stored? When were they created?
Answer:
Volume Shadow Copies are typically stored in the System Volume Information folder on each drive.

Item Path: cfreds_2015_data_leakage_pc\D\System Volume Information\

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\System Volume Information\

Targeted File: 9b365826-d2ef-11e4-b734-000c29ff2429}{3808876b-c176-4e48-b7ae-04046e6cc752}

Verification:



48. Find traces related to Google Drive service in Volume Shadow Copy.
What are the differences between the current system image (of Question 29 ~ 31) and its VSC?
Answer:

File	Date Created (VSC)	Date Modified (VSC)	Last Log Entry (sync_log.log)	Status in VSC	Status in Current Image	Description
sync_config.db	2015-03-23 16:02:51	2015-03-23 16:47:55		Present	Deleted	Stores sync snapshot data
snapshot.db (deleted)	2015-03-23 16:02:51	2015-03-23 16:47:55		Present	Deleted	Contains sync configuration
sync_log.log	2015-03-23 16:02:51	2015-03-23 16:47:56	2015-03-23 16:47:56	Present	Present	Records sync activities

Google Drive data:
Item Path: cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Google\Drive\user_default\ snapshot.db
True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Google\Drive\user_default\ snapshot.db
SVC Path:
Item Path: cfreds_2015_data_leakage_pc\D\System Volume Information\
True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\System Volume Information\

Current System Image vs. Volume Shadow Copy (VSC)

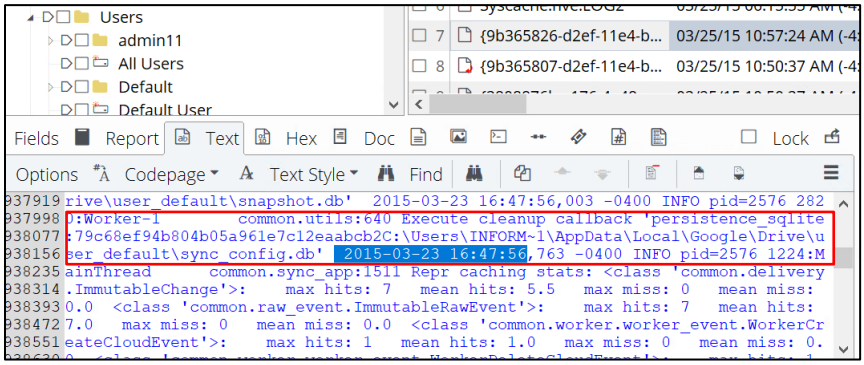
- The last log entry in sync_log.log within the VSC was added at 2015-03-23 16:47:56.
- Two SQLite files, snapshot.db and sync_config.db, exist in the VSC.
- These files were deleted following a logoff activity on 2015-03-25.
- This indicates that the VSC was created before the logoff activity, which subsequently deleted the files from the current system image.

Verification:

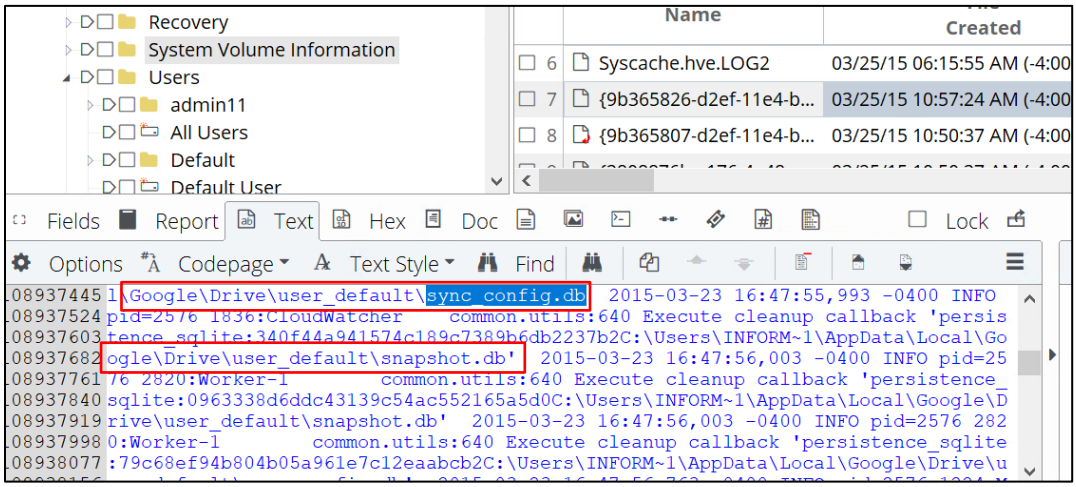
Google Drive Data:

Name	File Created	Last Accessed	Last Written
sync_config.db-shm	03/25/15 11:21:34 AM (-4:00 East...	03/25/15 11:22:48 AM (-4:00 Eastern ...	03/25/15 11:22:48 AM (-4:00 Eastern ...
run_dir	03/23/15 04:02:51 PM (-4:00 East...	03/23/15 04:02:51 PM (-4:00 Eastern ...	03/25/15 11:21:34 AM (-4:00 Eastern ...
sync_log.log	03/23/15 04:02:51 PM (-4:00 East...	03/23/15 04:02:51 PM (-4:00 Eastern ...	03/25/15 11:23:00 AM (-4:00 Eastern ...
cacerts	03/23/15 04:02:51 PM (-4:00 East...	03/23/15 04:02:51 PM (-4:00 Eastern ...	03/23/15 04:02:51 PM (-4:00 Eastern ...
snapshot.db	03/23/15 04:02:51 PM (-4:00 East...	03/23/15 04:02:51 PM (-4:00 Eastern ...	03/25/15 11:22:48 AM (-4:00 Eastern ...
sync_config.db	03/23/15 04:02:51 PM (-4:00 East...	03/23/15 04:02:51 PM (-4:00 Eastern ...	03/25/15 11:22:48 AM (-4:00 Eastern ...
lockfile	03/23/15 04:02:51 PM (-4:00 East...	03/23/15 04:02:51 PM (-4:00 Eastern ...	03/25/15 11:21:34 AM (-4:00 Eastern ...

Last Entry in sync_log.log:



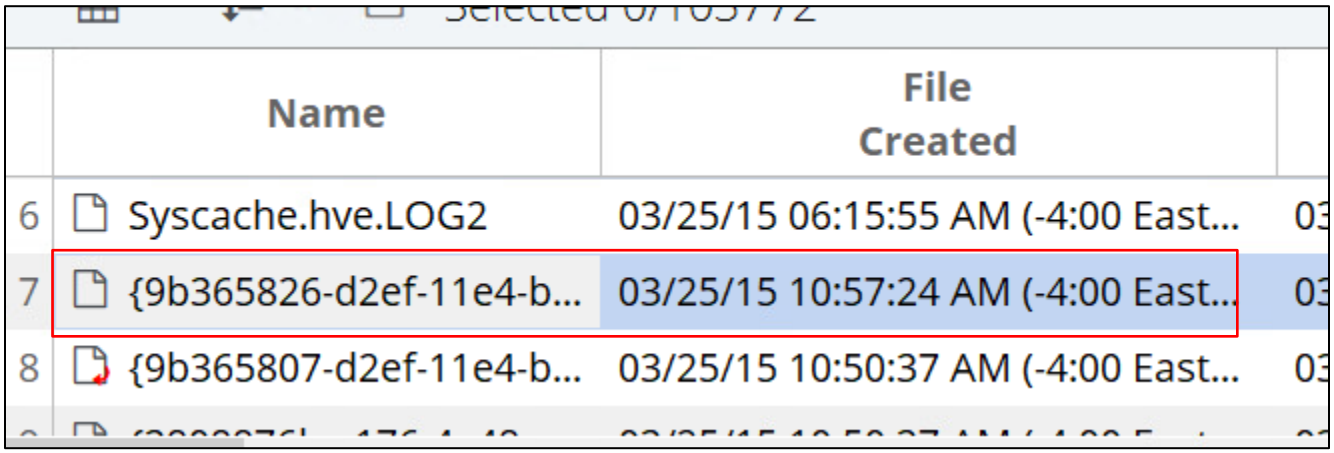
Presence of snapshot.db and sync_config.db in VSC:



Logoff Activity on 2015-03-25:

```
-25 10:54:22  Success  Uninstalling performance counters  2015-03-25 10:54:22
Starting Executing inf section: XSP.UninstallPerVer  2015-03-25 10:54:22  Succ
ss  Executing inf section:  2015-03-25 10:54:22  Starting Executing inf secti
n: AdminService.Uninstall  2015-03-25 10:54:22  Success  Executing inf section
   2015-03-25 10:54:22 Success  Pre Registration cleanup  2015-03-25 10:54:22
tarting Executing inf section: XSP.InstallPerVer  2015-03-25 10:54:22 Success
Executing inf section:  2015-03-25 10:54:22 Starting Determining if current A
P.NET isapi has the highest version  2015-03-25 10:54:22 Success  Determining
f current ASP.NET isapi has the highest version  2015-03-25 10:54:22 Starting
```

Volume Shadow Copy Creation Time:



	Name	File Created	
6	Syscache.hve.LOG2	03/25/15 06:15:55 AM (-4:00 East...	03
7	{9b365826-d2ef-11e4-b...	03/25/15 10:57:24 AM (-4:00 East...	03
8	{9b365807-d2ef-11e4-b...	03/25/15 10:50:37 AM (-4:00 East...	03

49. What files were deleted from Google Drive?

Find deleted records of *cloud_entry* table inside *snapshot.db* from VSC.

(Just examine the SQLite database only. Let us suppose that a text based log file was wiped.)

[Hint: DDL of *cloud_entry* table is as follows.]

CREATE TABLE *cloud_entry*
(doc_id TEXT, filename TEXT, modified INTEGER, created INTEGER, acl_role INTEGER, doc_type INTEGER, removed INTEGER, size INTEGER, checksum TEXT, shared INTEGER, resource_type TEXT, PRIMARY KEY (doc_id));

Answer:

do_u_wanna_build_a_snow_man.mp3:

- **Created on** 2015-03-23 **and modified on** 2015-01-30.
- **Size:** 6,844,294 bytes.

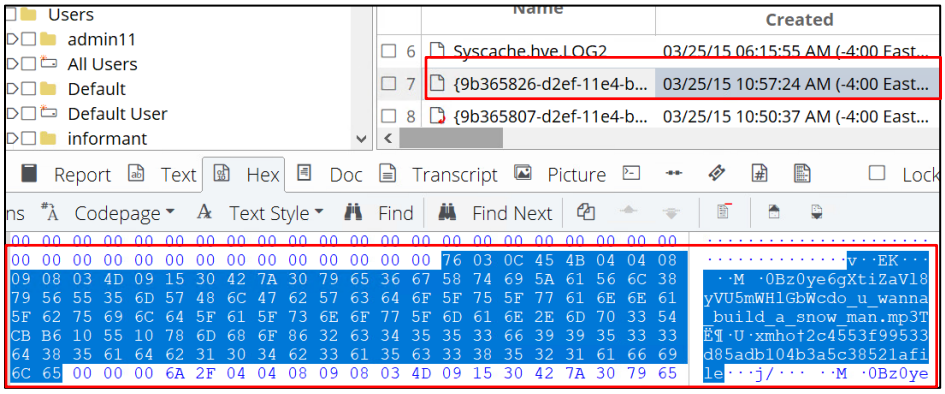
happy_holiday.jpg:

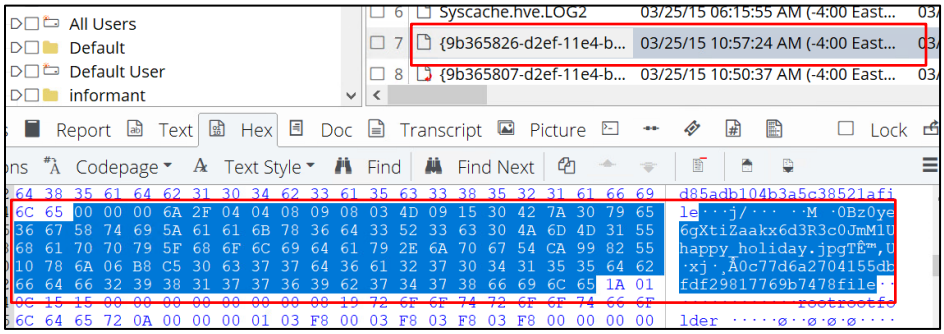
- **Created on** 2015-03-23 and **modified on** 2015-01-29.
- **Size:** 440,517 bytes.

File	do_u_wanna_build_a_snow_man.mp3	happy_holiday.jpg
File Offset	0x702	0x77A
Record Size	0x76	N/A (overwritten)
Row ID	0x03	N/A
Header Size	0x0C	N/A
doc_id	0Bz0ye6gXtiZaVl8yVU5mWHlGbWc	0Bz0ye6gXtiZaakx6d3R3c0JmM1U
Filename	do_u_wanna_build_a_snow_man.mp3	happy_holiday.jpg
Modified	0x54CBB610 (2015-01-30 11:49:20 UTC-05)	0x54CA9982 (2015-01-29 15:35:14 UTC-05)
Created	0x5510786D (2015-03-23 16:32:45 UTC-04)	0x5510786A (2015-03-23 16:32:42 UTC-04)
Size	0x686F86 (6,844,294 bytes)	0x6B8C5 (440,517 bytes)
Shared	1	1
Removed	0	0
Resource Type	file	file

Item Path: cfreds_2015_data_leakage_pc\D\System Volume Information\{9b365826-d2ef-11e4-b734-000c29ff2429}{3808876b-c176-4e48-b7ae-04046e6cc752}
True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\System Volume Information\{9b365826-d2ef-11e4-b734-000c29ff2429}{3808876b-c176-4e48-b7ae-04046e6cc752}

Verification:





50. Why can't we find Outlook's e-mail data in Volume Shadow Copy?

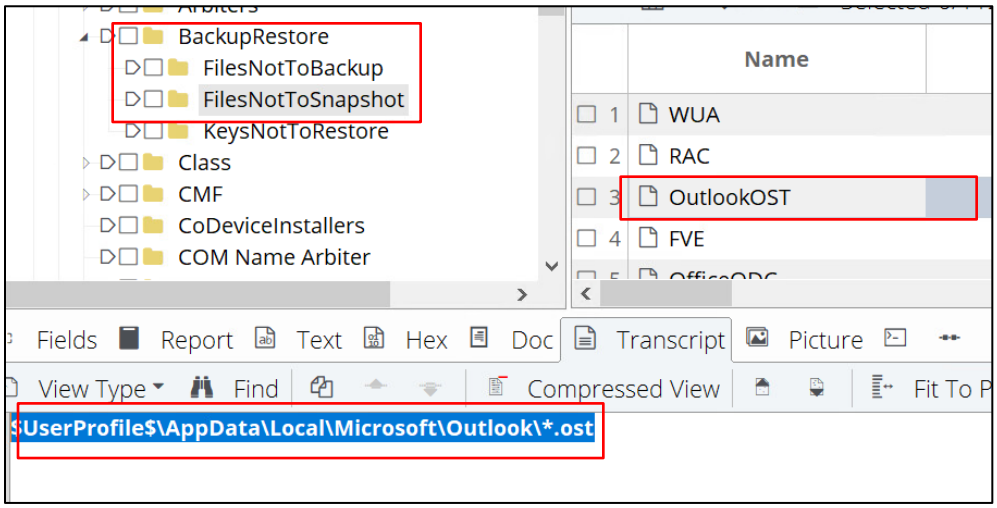
Answer:

Outlook .ost files are excluded from Volume Shadow Copies due to a specific configuration in the Windows registry.

CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}\ControlSet002\Control\BackupRestore\FilesNotToSnapshot\OutlookOST

OutlookOST: $UserProfile$\AppData\Local\Microsoft\Outlook*.ost

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Windows\System32\config\SYSTEM\CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}\ControlSet002\Control\BackupRestore\FilesNotToSnapshot\OutlookOST



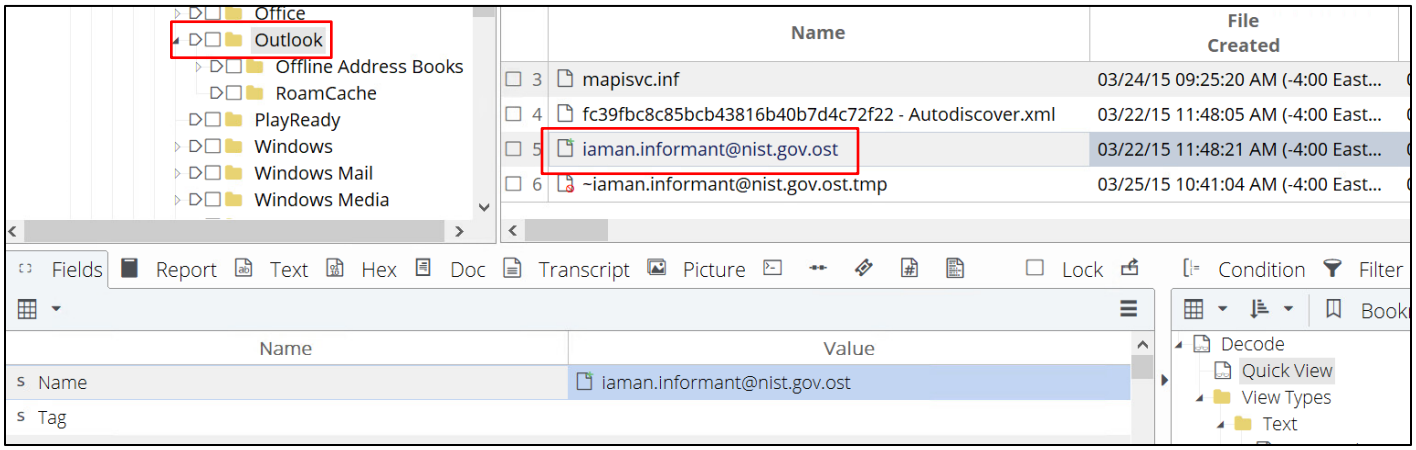
Verification:

Navigate to the Exclusion Path:

Item Path:

cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Microsoft\Outlook\iaman.informant@nist.gov.ost

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Microsoft\Outlook\iaman.informant@nist.gov.ost



51. Examine 'Recycle Bin' data in PC.

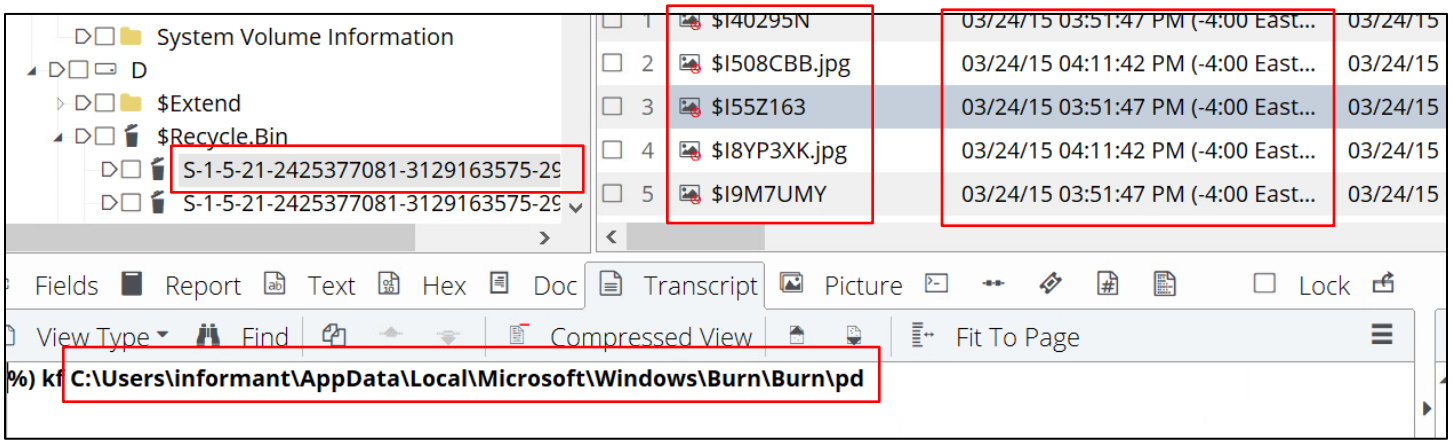
Answer:

Name	Original File (or Directory) Path	Timestamp Deleted
$I40295N	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\prop	2015-03-24 15:51:47
$IXWGVWC	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\prog	2015-03-24 15:51:47
$I55Z163	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\pd	2015-03-24 15:51:47
$I9M7UMY	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\tr	2015-03-24 15:51:47
$I508CBB.jpg	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Hydrangeas.jpg	2015-03-24 16:11:42
$I8YP3XK.jpg	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Jellyfish.jpg	2015-03-24 16:11:42
$IDOI3HE.jpg	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Tulips.jpg	2015-03-24 16:11:42
$IFVCH5V.jpg	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Penguins.jpg	2015-03-24 16:11:42
$II3FM2A.jpg	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Desert.jpg	2015-03-24 16:11:42
$IIQGWTT.ini	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\desktop.ini	2015-03-24 16:11:42
$IJEMT64.exe	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\IE11-Windows6.1-x64-en-us.exe	2015-03-24 16:11:42
$IKXD1U3.jpg	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Chrysanthemum.jpg	2015-03-24 16:11:42
$IU3FKWI.jpg	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Koala.jpg	2015-03-24 16:11:42
$IX538VH.jpg	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Lighthouse.jpg	2015-03-24 16:11:42

Item Path: cfreds_2015_data_leakage_pc\D\$Recycle.Bin\S-1-5-21-2425377081-3129163575-2985601102-1000\

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\$Recycle.Bin\S-1-5-21-2425377081-3129163575-2985601102-1000\

1000 Id Belongs to Account ***Informant (Suspect)*** account.



52. What actions were performed for anti-forensics on PC at the last day '2015-03-25'?

Answer:

Timestamp	Behavior	Description
2015-03-25 10:46:44	Search	Searched for "anti-forensic tools" and "eraser."
2015-03-25 10:46:54	Search	Searched for "anti-forensic methods" and "ccleaner."
2015-03-25 10:47:34	Download	Downloaded Eraser from SourceForge.
2015-03-25 10:48:12	Download	Downloaded CCleaner from Piriform's website.
2015-03-25 10:50:14	Install	Installed Eraser 6.2.0.2962 (\USERS\INFORMANT\DESKTOP\DOWNLOAD\ERASER 6.2.0.2962.EXE).
2015-03-25 10:57:56	Install	Installed CCleaner (\USERS\INFORMANT\DESKTOP\DOWNLOAD\CCSETUP504.EXE).
2015-03-25 11:13:30	Run	Executed Eraser (\PROGRAM FILES\Eraser\Eraser.exe).
2015-03-25 11:13:39 - 11:14:44	Wiping files & directories	Wiped multiple files in \User\Informant\Desktop\Temp\ using Eraser's 7-pass DoD method.
2015-03-25 11:15:45	Delete files ([Shift] + [Delete])	Deleted downloaded installers (ccsetup504.exe, Eraser 6.2.0.2962.exe) to remove traces.
2015-03-25 11:15:50	Run	Executed CCleaner to clear system logs and temporary files (\PROGRAM FILES\CCLEANER\CCLEANER64.EXE).
2015-03-25 11:18:29	Uninstall	Uninstalled CCleaner (\PROGRAM FILES\CCLEANER\UNINST.EXE).
2015-03-25 11:22:47	Disconnecting Google Drive	Signed out and deleted Google Drive sync configuration files (sync_config.db, snapshot.db).
N/A	Delete emails in Outlook	Deleted specific emails in Outlook with subjects like "It's me," "Good job, buddy," "Watch out!" (refer to Questions 21, 45).

Item Path: cfreds_2015_data_leakage_pc\D\$Extend\$UsnJrnl

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\$Extend\$UsnJrnl

A	B	C	D	E	F	G	H	I	J
cfreds_20	65059008	96	2	65059008	3/25/2015 10:47	None	The file or directory was added to (0x00000002). The file or directory was cre	activeview[8].gif	Archive (0x00000020), Not Conte
cfreds_20	65059104	96	2	65059104	3/25/2015 10:47	None	The file or directory was created for the first time (0x00000100).	activeview[3].gif	Archive (0x00000020), Not Conte
cfreds_20	65059200	96	2	65059200	3/25/2015 10:47	None	The file or directory was added to (0x00000002). The file or directory was cre	activeview[3].gif	Archive (0x00000020), Not Conte
cfreds_20	65059296	96	2	65059296	3/25/2015 10:47	None	The file or directory was added to (0x00000002). The file or directory was cre	activeview[3].gif	Archive (0x00000020), Not Conte
cfreds_20	65059392	96	2	65059392	3/25/2015 10:47	None	The file or directory was created for the first time (0x00000100).	activeview[4].gif	Archive (0x00000020), Not Conte
cfreds_20	65059488	96	2	65059488	3/25/2015 10:47	None	The file or directory was added to (0x00000002). The file or directory was cre	activeview[4].gif	Archive (0x00000020), Not Conte
cfreds_20	65059584	96	2	65059584	3/25/2015 10:47	None	The file or directory was added to (0x00000002). The file or directory was cre	activeview[4].gif	Archive (0x00000020), Not Conte
cfreds_20	65059680	88	2	65059680	3/25/2015 10:47	None	The file or directory was created for the first time (0x00000100).	collect[1].gif	Archive (0x00000020), Not Conte
cfreds_20	65059768	88	2	65059768	3/25/2015 10:47	None	The file or directory was added to (0x00000002). The file or directory was cre	collect[1].gif	Archive (0x00000020), Not Conte
cfreds_20	65059856	88	2	65059856	3/25/2015 10:47	None	The file or directory was added to (0x00000002). The file or directory was cre	collect[1].gif	Archive (0x00000020), Not Conte
cfreds_20	65059944	88	2	65059944	3/25/2015 10:47	None	The file or directory was created for the first time (0x00000100).	Moat1x1[1].png	Archive (0x00000020), Not Conte
cfreds_20	65060032	88	2	65060032	3/25/2015 10:47	None	The file or directory was added to (0x00000002). The file or directory was cre	Moat1x1[1].png	Archive (0x00000020), Not Conte
cfreds_20	65060120	88	2	65060120	3/25/2015 10:47	None	The file or directory was added to (0x00000002). The file or directory was cre	Moat1x1[1].png	Archive (0x00000020), Not Conte
cfreds_20	65060208	80	2	65060208	3/25/2015 10:47	None	The data in the file or directory was overwritten (0x00000001).	V01.log	Archive (0x00000020), Not Conte
cfreds_20	65060288	112	2	65060288	3/25/2015 10:47	None	The file or directory was created for the first time (0x00000100).	Eraser%206.2.0.2962[1].exe	Archive (0x00000020), Not Conte
cfreds_20	65060400	112	2	65060400	3/25/2015 10:47	None	The file or directory was added to (0x00000002). The file or directory was cre	Eraser%206.2.0.2962[1].exe	Archive (0x00000020), Not Conte
cfreds_20	65060512	96	2	65060512	3/25/2015 10:47	None	The data in the file or directory was overwritten (0x00000001).	thumbcache_32.db	Archive (0x00000020), Not Conte
cfreds_20	65060608	96	2	65060608	3/25/2015 10:47	None	The data in the file or directory was overwritten (0x00000001).	thumbcache_256.db	Archive (0x00000020), Not Conte
cfreds_20	65060704	96	2	65060704	3/25/2015 10:47	None	The data in the file or directory was overwritten (0x00000001).	thumbcache_idx.db	Archive (0x00000020), Not Conte
cfreds_20	65060864	96	2	65060864	3/25/2015 10:47	None	The data in the file or directory was overwritten (0x00000001). The file or dir	thumbcache_32.db	Archive (0x00000020), Not Conte
cfreds_20	65060960	96	2	65060960	3/25/2015 10:47	None	The data in the file or directory was overwritten (0x00000001). The file or dir	thumbcache_256.db	Archive (0x00000020), Not Conte

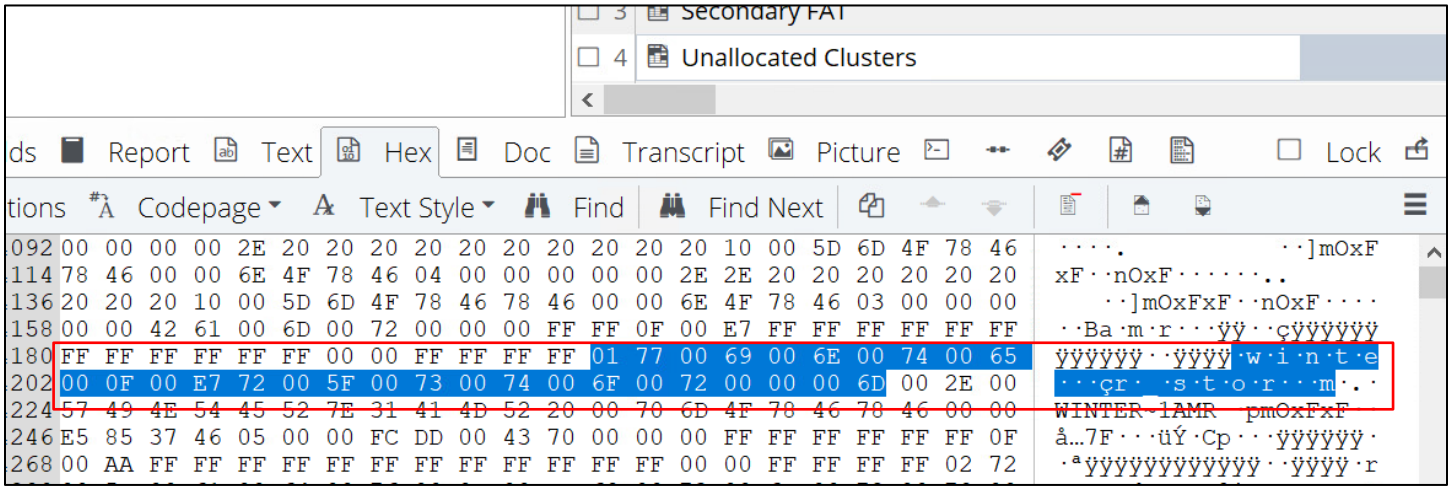
53. Recover deleted files from USB drive 'RM#2'.

Answer:

Filename (Path)	Format	File size
\DESIGN\winter_storm.amr	PPT	13.8 MB
\DESIGN\winter_whether_advisory.zip	PPTX	15.6 MB
\pricing decision\my_favorite_cars.db	XLS	1.20 MB
\pricing decision\my_favorite_movies.7z	XLSX	97.7 KB
\pricing decision\new_years_day.jpg	XLSX	9.76 MB
\pricing decision\super_bowl.avi	XLS	9.81 MB
\PROGRESS\my_friends.svg	DOC	57.0 KB
\PROGRESS\my_smartphone.png	DOCX	4.23 MB
\PROGRESS\new_year_calendar.one	DOCX	26.7 KB
\PROPOSAL\a_gift_from_you.gif	DOCX	33.5 MB
\PROPOSAL\landscape.png	DOCX	6.18 MB
\technical review\diary_#1d.txt	DOCX	118 KB
\technical review\diary_#1p.txt	PPTX	447 KB
\technical review\diary_#2d.txt	DOCX	643 KB
\technical review\diary_#2p.txt	PPT	1.10 MB
\technical review\diary_#3d.txt	DOC	2.25 MB
\technical review\diary_#3p.txt	PPT	317 KB

We have used **Autopsy** to carve the file and we verify the file with **Encase**.

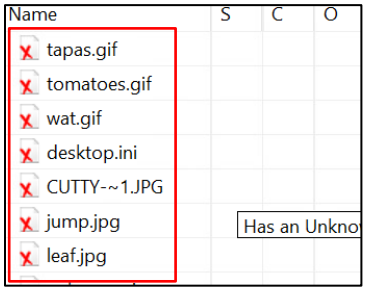
Item Path: cfreds_2015_data_leakage_rm#2\C\Unallocated Clusters
True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_rm#2\C\Unallocated Clusters



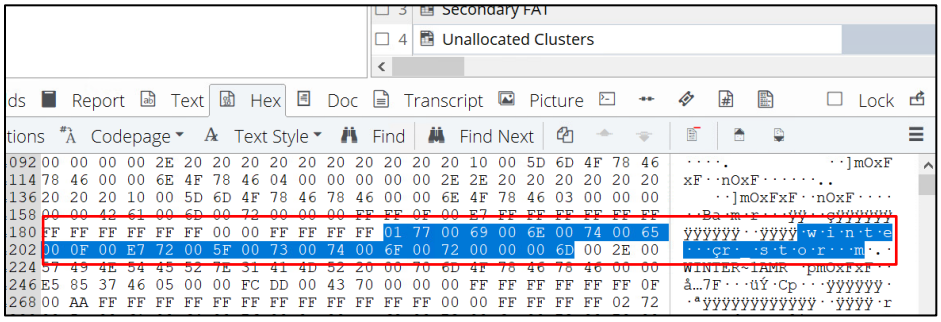
54. What actions were performed for anti-forensics on USB drive 'RM#2'?
[Hint: this can be inferred from the results of Question 53.]
Answer: Quick format

Verification:
Analyze Data Recovery Results from Question 53:

- The results from Question 53 showed the recovery of various file types (e.g., OGG, JPG, DOC, MP4).
- In a quick format, the file system's directory structure is reset, but the actual data blocks are not overwritten, allowing recovery of file fragments in unallocated space.



Check for Directory Entries in Unallocated Space:
During a quick format, the drive's file allocation table (FAT or NTFS entries) is cleared, but previous directory entries may remain in the unallocated space.

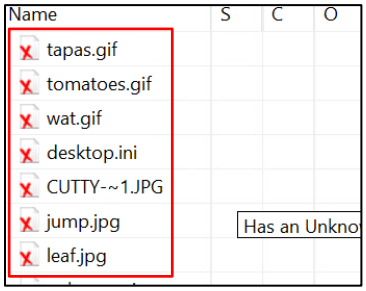


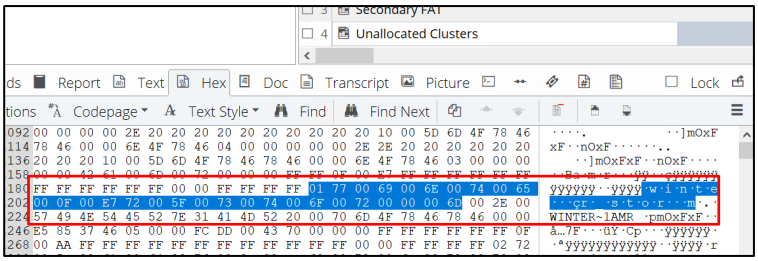
55. What files were copied from PC to USB drive 'RM#2'?
Answer:
winter_storm.amr
winter_whether_advisory.zip
my_favorite_cars.db
my_favorite_movies.7z
new_years_day.jpg
super_bowl.avi
my_friends.svg
my_smartphone.png
new_year_calendar.one
a_gift_from_you.gif
landscape.png
diary_#1d.txt
diary_#1p.txt

diary_#2d.txt
diary_#2p.txt
diary_#3d.txt
diary_#3p.txt

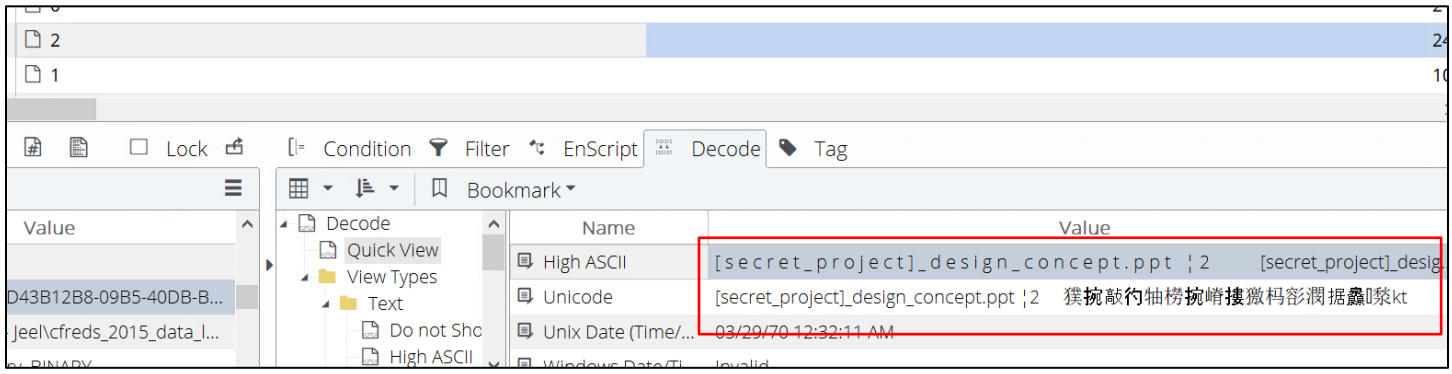
Verification:

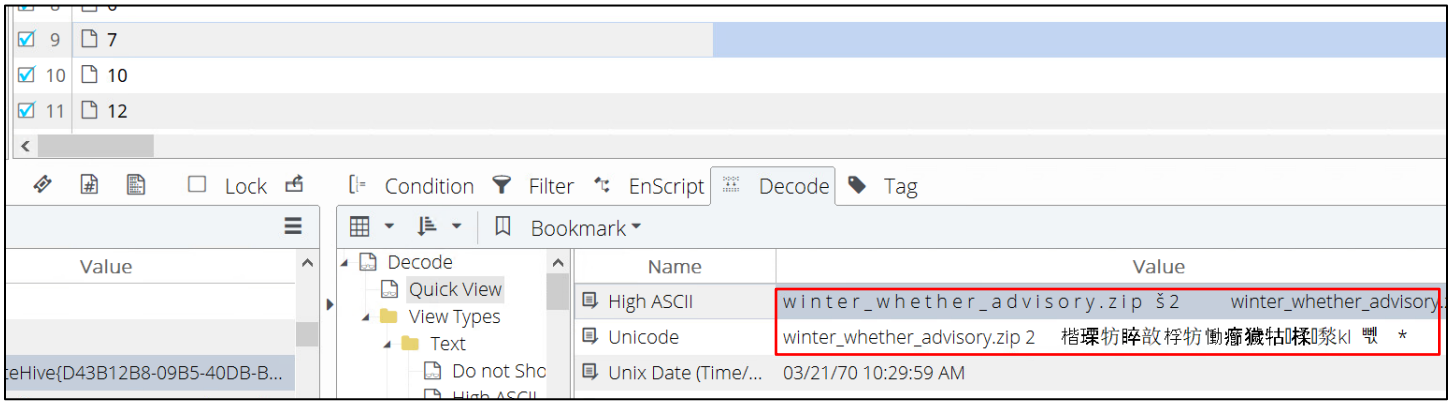
File recovered in USB during examination of question 53:





File Found in PC during examination of question 26:





56. Recover hidden files from the CD-R 'RM#3'.

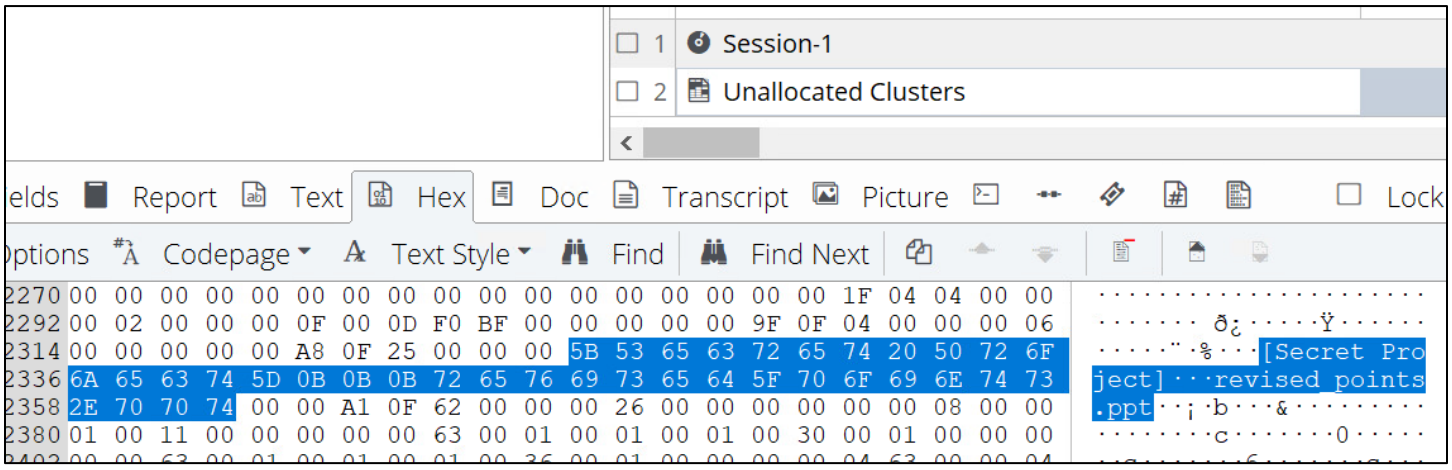
How to determine proper filenames of the original files prior to renaming tasks?

Answer:

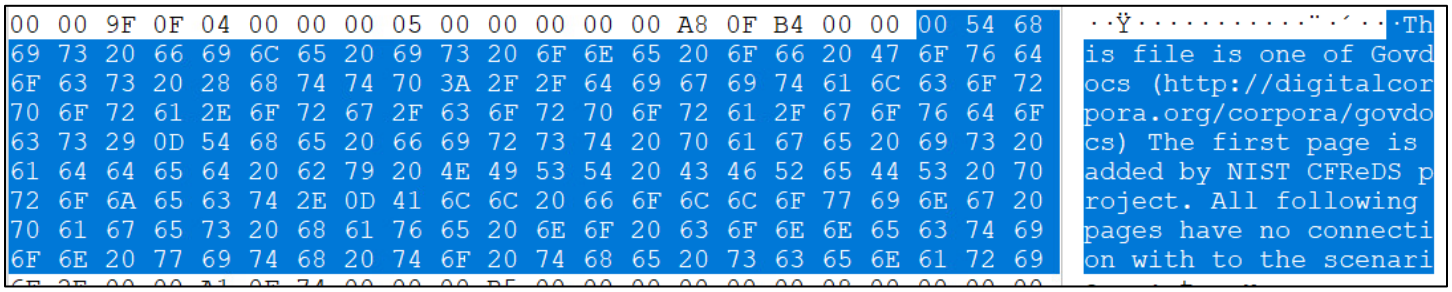
Filename inferred from the First Page & its storage format	Format	Filesize
[secret_project]_revised_points.ppt	PPT	13.8 MB
[secret_project]_detailed_design.pptx	PPTX	15.6 MB
[secret_project]_price_analysis_#1.xlsx	XLSX	97.7 KB
[secret_project]_price_analysis_#2.xls	XLS	1.20 MB
[secret_project]_market_analysis.xlsx	XLSX	9.76 MB
[secret_project]_market_shares.xls	XLS	9.81 MB
[secret_project]_progress_#1.docx	DOCX	4.23 MB
[secret_project]_progress_#2.docx	DOCX	26.7 KB
[secret_project]_progress_#3.doc	DOC	56.0 KB
[secret_project]_detailed_proposal.docx	DOCX	-
[secret_project]_proposal.docx	DOCX	6.18 MB
[secret_project]_technical_review_#1.docx	DOCX	118 KB
[secret_project]_technical_review_#1.pptx	PPTX	447 KB
[secret_project]_technical_review_#2.docx	DOCX	643 KB
[secret_project]_technical_review_#2.ppt	PPT	1.10 MB
[secret_project]_technical_review_#3.doc	DOC	2.25 MB
[secret_project]_technical_review_#3.ppt	PPT	317 KB

True path: Data Leak Case - Jeel\cfreds_2015_data_leakage_rm#3\Unallocated Clusters
Item Path: cfreds_2015_data_leakage_rm#3\Unallocated Clusters

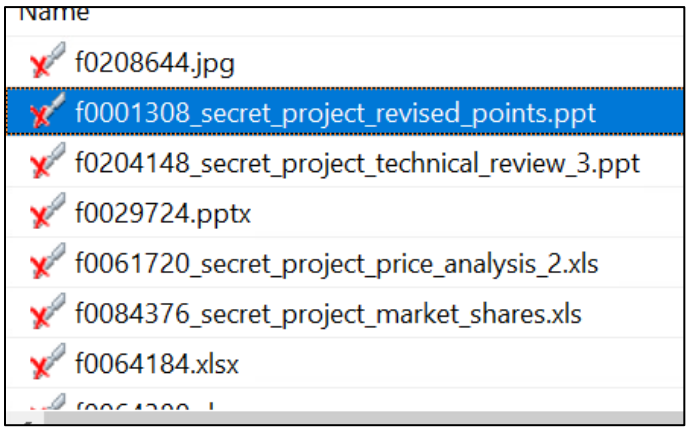
Hexadecimal Analysis of File Signatures and Content:



Data Carving and Reconstruction:



Data Carving and Reconstruction:



57. What actions were performed for anti-forensics on CD-R 'RM#3'?

Answer:

Formatting CD-R (Burning Type 1)

Copying Confidential and Meaningless Files

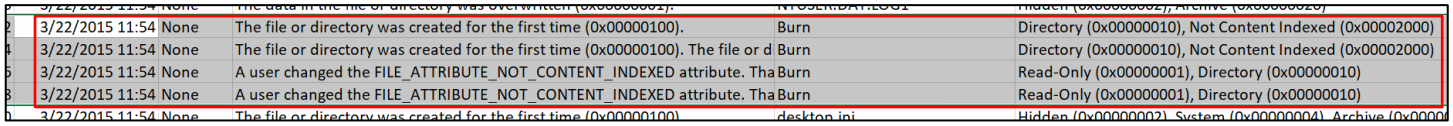
Deleting Confidential Files

Item Path: cfreds_2015_data_leakage_pc\D\$Extend\$UsnJrnl

True Path: Data Leak Case - Jeel\cfreds_2015_data_leakage_pc\D\$Extend\$UsnJrnl

Verification:

The provided image shows entries in the "Burn" directory, which was created and modified around the same time, indicating activity associated with formatting and preparing the CD-R as a rewritable drive (Burning Type 1). The timestamps align with actions such as copying data to the CD-R, as shown by multiple "created for the first time" entries. Additionally, the entry stating that "the data in the file or directory was overwritten" supports the assertion that files were deleted or hidden as part of anti-forensic efforts. The presence of these actions—formatting, copying, and deletion—confirms the sequence of events in the answer and verifies the anti-forensic measures applied on CD-R 'RM#3'.



58. Create a detailed timeline of data leakage processes.
Answer:

Date & Time (EST)	Step	Action	Additional Description	Notes
2015-03-22	Normal Business	Install OS	Windows 7 Ultimate	
2015-03-22		Configure settings	Set timezone to (UTC-05) Eastern Time	
2015-03-22		Install Apps	Microsoft Office, Internet Explorer, Google Chrome	
2015-03-22		Create/Download Business Data	Various documents in Word, Excel, PowerPoint	Common files
2015-03-22		Email	Set up Microsoft Outlook with NIST email account	iaman.informant@nist.gov
2015-03-22		Create User Accounts	Created accounts: "admin11" (login count: 2), "ITechTeam" (login count: 0), "temporary" (login count: 1)	
2015-03-23 13:29	Preparation	Receive Email	Received email from spy.conspirator@nist.gov, subject: "Hello, Iaman"	Message: "How are you doing?"
2015-03-23 14:01		Search Leakage Methods	Conducted searches on data leakage, intellectual property theft, anti-forensics using Google and Bing	Keywords like "data leakage methods"
2015-03-23 14:31		Connect USB	Connected 'RM#1' USB memory stick	
2015-03-23 14:36		Search Files	Used Windows Search to find "secret" keywords	
2015-03-23 14:37		Open Files	Opened [secret_project]_proposal.docx and [secret_project]_design_concept.ppt	
2015-03-23 14:39	Copy Data	Copy Files	Copied confidential files from 'RM#1' to 'PC' at "\Desktop\S data"	Directory structure logged
2015-03-23 14:39		Disconnect USB	Ejected 'RM#1'	
2015-03-23 14:39		Configure Settings	Enabled 'file name extensions' in Windows Explorer	
2015-03-23 14:41	Rename Files	Change Names & Extensions	Changed file extensions (e.g., .docx to .mp3)	Files disguised with random names
2015-03-23 14:44	Communication	Send Email	"Successfully secured" message to spy.conspirator@nist.gov	
2015-03-23 15:14	Communication	Receive Email	From spy.conspirator@nist.gov, subject: "Good job, buddy"	Request for more detailed data
2015-03-23 15:19		Send Email	Sent sample data (space_and_earth.mp4) to spy.conspirator@nist.gov	
2015-03-23 15:26		Receive Email	From spy.conspirator@nist.gov, subject: "Important request	Request to transfer more data
2015-03-23 16:00	Transfer Data	Search & Install Apps	Installed Google Drive and Apple iCloud	
2015-03-23 16:05		Login Cloud Service	Logged into Google Drive using personal account (iaman.informant.personal@gmail.com)	
2015-03-23 16:23		Connect Network Drive	Connected to shared network drive \10.11.11.128\secured_drive	
2015-03-23 16:24		Search Files	Traversed directories on network drive	

2015-03-23 16:26		Copy Data	Copied files from network drive to 'PC'	"\Desktop\S data" folder
2015-03-23 16:32		Upload Files	Uploaded files (e.g., happy_holiday.jpg) to Google Drive	
2015-03-23 16:38	Communication	Send Email	"Use links below" message to spy.conspirator@nist.gov	
2015-03-23 16:42		Delete Files	Deleted uploaded files from Google Drive	
2015-03-24 09:26	Communication	Receive Email	From spy.conspirator@nist.gov, subject: "Last request"	Request for remaining data
2015-03-24 09:38	Copy Data	Connect USB	Connected 'RM#1' USB memory stick	
2015-03-24 09:40		Copy Files	Copied confidential files from 'RM#1' to 'PC'	"\Desktop\S data\Secret Project Data"
2015-03-24 09:47		Connect Network Drive	Reconnected to secured network drive	
2015-03-24 09:56		Rename Files	Renamed files with misleading names and extensions (e.g., .xlsx to .jpg)	Files disguised for anti-forensics
2015-03-24 10:07		Delete Files	Deleted "\Desktop\S data" with [Shift] + [Delete]	
2015-03-24 14:28		Launch Game	Opened Solitaire	Disguised activity
2015-03-24 16:40	Anti-Forensics	CD-R Burning	Tested CD-R burning process with meaningless files	Anti-forensics tactic
2015-03-24 17:01		Delete Files	Deleted confidential files from CD-R	Anti-forensics evidence
2015-03-25 10:46	Anti-Forensics	Search and Download Apps	Searched for anti-forensics tools like Eraser and CCleaner	
2015-03-25 10:50		Install Apps	Installed Eraser and CCleaner for file wiping	
2015-03-25 11:00		Delete Emails	Deleted some emails from Outlook	
2015-03-25 11:13		Run Anti-Forensics Tools	Used Eraser to wipe files	
2015-03-25 11:15		Delete Installer Files	Deleted downloaded installer files	[Shift] + [Delete]
2015-03-25 11:18		Uninstall Apps	Uninstalled CCleaner and iCloud	
2015-03-25 11:22		Disconnect Google Drive	Signed out of Google Drive	
2015-03-25 11:24		Open Resignation Letter	Opened resignation letter on desktop	
2015-03-25 11:28		Print Document	Printed resignation letter to MS XPS viewer	
2015-03-25 11:30	Security Checkpoint	Finish Works	Attempted to leave with USB and CD-R	Detected at security checkpoint

59. List and explain methodologies of data leakage performed by the suspect.

Answer:

1. Direct File Copying to External USB Drives (RM#1 & RM#2)

Methodology: The suspect connected external USB drives to the company PC and copied confidential files directly from the company's network drive and local PC storage onto these drives.

Evidence: The timeline indicates that "RM#1" and "RM#2" were connected to the company PC multiple times to transfer files. Files were copied from secured network drives and from specific directories on the local PC to the USB drives. This allowed the suspect to physically transfer sensitive data outside the company's secure environment.

2. Renaming and Changing File Extensions for Disguise

Methodology: After copying confidential files, the suspect renamed files and changed their extensions (e.g., .docx to .mp3, .xlsx to .jpg) to make them appear as non-sensitive files, such as images or audio files.

Evidence: The timeline shows that file names and extensions were changed to disguise sensitive information, such as renaming "[secret_project]_proposal.docx" to "landscape.png." This tactic was used to avoid detection by security tools and policies that scan for specific file types or names associated with confidential information.

3. Use of Personal Cloud Storage (Google Drive) for File Transfer

Methodology: The suspect uploaded files to a personal Google Drive account and shared links for access. This method enabled the suspect to transfer data over the internet without directly attaching files to email, potentially bypassing email security filters.

Evidence: The timeline records the installation and use of Google Drive, along with login activities using a personal email account. Files like "happy_holiday.jpg" (a disguised confidential file) were uploaded and shared with "Spy Conspirator" via email links, making the data accessible externally without needing physical media.

4. Email Communication with Embedded Links to Cloud-Stored Files

Methodology: Rather than sending confidential files as email attachments, the suspect provided links to cloud-stored files in Google Drive. This method reduces the risk of detection by email monitoring tools that inspect attachments.

Evidence: The timeline lists multiple instances where the suspect exchanged emails with "Spy Conspirator" containing links to files hosted on Google Drive, such as "space_and_earth.mp4" (a renamed confidential document). This approach facilitated covert data exchange with reduced visibility.

5. Data Obfuscation with Anti-Forensic Techniques (Quick Format and File Wiping)

Methodology: To erase traces of confidential files, the suspect used anti-forensic tools, such as Eraser, to securely delete files, and performed quick formats on the USB drives. The goal was to prevent recovery of data from devices in case of forensic analysis.

Evidence: The timeline indicates the installation and usage of Eraser and CCleaner, as well as the performance of a quick format on USB drive "RM#2." The wiping process included random renaming and overwriting, rendering files difficult to recover.

6. Burning and Deleting Files on CD-R Media for Anti-Forensics

Methodology: The suspect copied confidential data onto a CD-R, then formatted the CD-R to delete the files. This "burn and delete" approach was intended to create confusion during forensic analysis and reduce the chances of data recovery.

Evidence: The timeline notes activities involving burning files to CD-R, formatting the CD-R to erase them, and then adding meaningless files to further obfuscate forensic examination. This step was likely meant to prevent investigators from easily retrieving the original confidential data.

7. Disguised Personal Communication with 'Spy Conspirator' via Work Email

Methodology: The suspect communicated with "Spy Conspirator" using work email, disguising conversations as professional interactions to evade suspicion. This allowed for the exchange of instructions, updates, and verification of data leakage.

Evidence: The timeline shows frequent email exchanges where "Spy Conspirator" instructed the suspect, discussed data needs, and provided reassurance. Using work email provided a cover, making it appear as if the communication was legitimate business correspondence.

These methodologies collectively demonstrate a calculated and multi-layered approach to data leakage, leveraging both physical and digital means. By using anti-forensic tools, cloud storage, file renaming, and communication obfuscation, the suspect attempted to avoid detection and complicate forensic investigation. Each step shows intent to conceal, exfiltrate, and destroy evidence systematically.

60. Create a visual diagram for a summary of results.