

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.

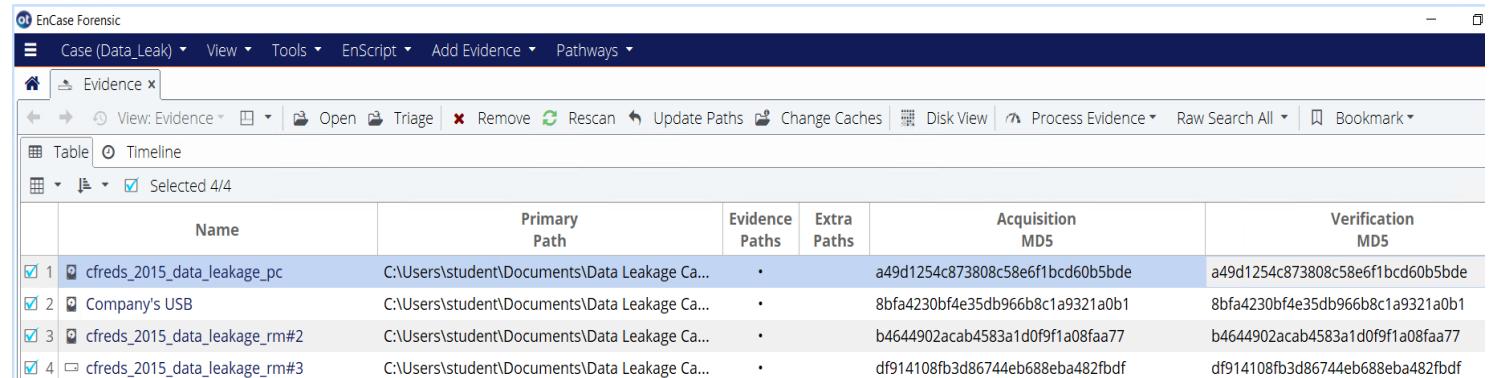
[Please note: If you have any issues clicking on the links to download the files, please "right click" and choose to "save as".]

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

| Evidence | Hash Algorithm | Hash value |
|----------------|----------------|--|
| PC | MD5 | a49d1254c873808c58e6f1bcd60b5bde |
| | SHA-1 | afe5c9ab487bd47a8a9856b1371c2384d44fd785 |
| RM#1 | MD5 | 8bfa4230bf4e35db966b8c1a9321a0b1 |
| | SHA-1 | f6bb840e98dd7c325af45539313fc3978fff812c |
| RM#2 | MD5 | b4644902acab4583a1d0f9f1a08faa77 |
| | SHA-1 | 048961a85ca3eced8cc73f1517442d31d4dca0a3 |
| RM#3 | MD5 | df914108fb3d86744eb688eba482fbdf |
| (Type3) | SHA-1 | 7f3c2eb1f1e2db97be6e963625402a0e362a532c |

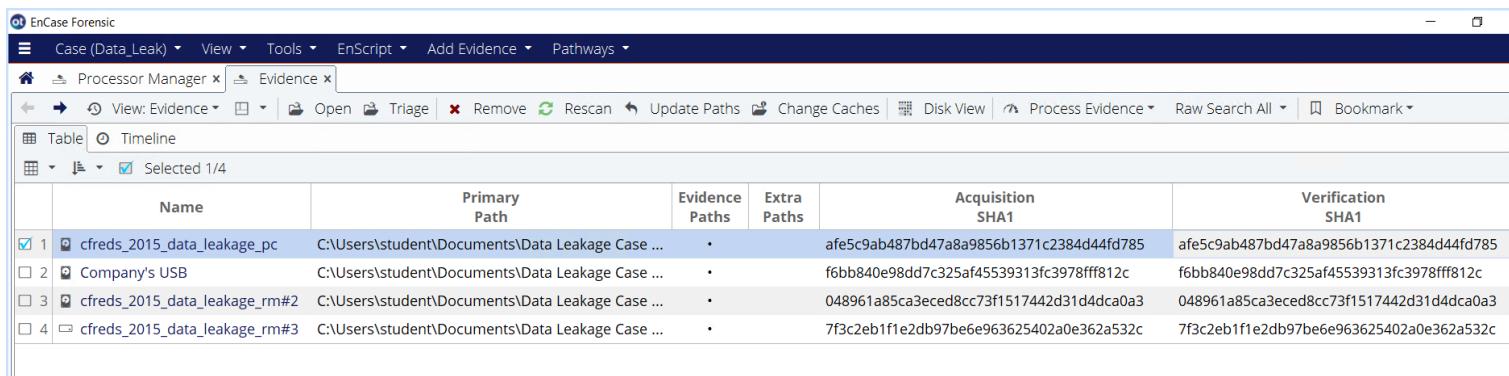
Answer:

- Evidence from EnCase:**



The screenshot shows the EnCase Forensic interface with the 'Evidence' tab selected. The table displays four pieces of evidence with their names, primary paths, and hash values. The columns are: Name, Primary Path, Evidence Paths, Extra Paths, Acquisition MD5, and Verification MD5.

| | Name | Primary Path | Evidence Paths | Extra Paths | Acquisition MD5 | Verification MD5 |
|-----|-------------------------------|---|----------------|-------------|----------------------------------|----------------------------------|
| ✓ 1 | cfreds_2015_data_leakage_pc | C:\Users\student\Documents\Data Leakage Ca... | • | | a49d1254c873808c58e6f1bcd60b5bde | a49d1254c873808c58e6f1bcd60b5bde |
| ✓ 2 | Company's USB | C:\Users\student\Documents\Data Leakage Ca... | • | | 8bfa4230bf4e35db966b8c1a9321a0b1 | 8bfa4230bf4e35db966b8c1a9321a0b1 |
| ✓ 3 | cfreds_2015_data_leakage_rm#2 | C:\Users\student\Documents\Data Leakage Ca... | • | | b4644902acab4583a1d0f9f1a08faa77 | b4644902acab4583a1d0f9f1a08faa77 |
| ✓ 4 | cfreds_2015_data_leakage_rm#3 | C:\Users\student\Documents\Data Leakage Ca... | • | | df914108fb3d86744eb688eba482fbdf | df914108fb3d86744eb688eba482fbdf |



The screenshot shows the EnCase Forensic interface with the 'Processor Manager' tab selected, which also displays the 'Evidence' view. The table structure is identical to the one above, showing four pieces of evidence with their names, primary paths, and hash values.

| | Name | Primary Path | Evidence Paths | Extra Paths | Acquisition SHA1 | Verification SHA1 |
|-----|-------------------------------|--|----------------|-------------|--|--|
| ✓ 1 | cfreds_2015_data_leakage_pc | C:\Users\student\Documents\Data Leakage Case ... | • | | afe5c9ab487bd47a8a9856b1371c2384d44fd785 | afe5c9ab487bd47a8a9856b1371c2384d44fd785 |
| □ 2 | Company's USB | C:\Users\student\Documents\Data Leakage Case ... | • | | f6bb840e98dd7c325af45539313fc3978fff812c | f6bb840e98dd7c325af45539313fc3978fff812c |
| □ 3 | cfreds_2015_data_leakage_rm#2 | C:\Users\student\Documents\Data Leakage Case ... | • | | 048961a85ca3eced8cc73f1517442d31d4dca0a3 | 048961a85ca3eced8cc73f1517442d31d4dca0a3 |
| □ 4 | cfreds_2015_data_leakage_rm#3 | C:\Users\student\Documents\Data Leakage Case ... | • | | 7f3c2eb1f1e2db97be6e963625402a0e362a532c | 7f3c2eb1f1e2db97be6e963625402a0e362a532c |

- Evidence verified from FTK Imager:**

| Drive/Image Verify Results | |
|----------------------------|--|
| Name | data_leakage_pc.E01 |
| Sector count | 41943040 |
| MD5 Hash | |
| Computed hash | a49d1254c873808c58e6f1bcd60b5bde |
| Stored verification hash | a49d1254c873808c58e6f1bcd60b5bde |
| Verify result | Match |
| SHA1 Hash | |
| Computed hash | afe5c9ab487bd47a8a9856b1371c2384d44fd785 |
| Stored verification hash | afe5c9ab487bd47a8a9856b1371c2384d44fd785 |
| Verify result | Match |
| Bad Blocks List | |
| Bad block(s) in image | No bad blocks found in image |

| Drive/Image Verify Results | |
|----------------------------|--|
| Name | data_leakage_rm#1.E01 |
| Sector count | 7821312 |
| MD5 Hash | |
| Computed hash | 8bfa4230bf4e35db966b8c1a9321a0b1 |
| Stored verification hash | 8bfa4230bf4e35db966b8c1a9321a0b1 |
| Verify result | Match |
| SHA1 Hash | |
| Computed hash | f6bb840e98dd7c325af45539313fc3978fff812c |
| Stored verification hash | f6bb840e98dd7c325af45539313fc3978fff812c |
| Verify result | Match |
| Bad Blocks List | |
| Bad block(s) in image | No bad blocks found in image |

| Drive/Image Verify Results | |
|----------------------------|--|
| Name | data_leakage_rm#2.E01 |
| Sector count | 7821312 |
| MD5 Hash | |
| Computed hash | b4644902acab4583a1d0f9f1a08faa77 |
| Stored verification hash | b4644902acab4583a1d0f9f1a08faa77 |
| Verify result | Match |
| SHA1 Hash | |
| Computed hash | 048961a85ca3eced8cc73f1517442d31d4dca0a3 |
| Stored verification hash | 048961a85ca3eced8cc73f1517442d31d4dca0a3 |
| Verify result | Match |
| Bad Blocks List | |
| Bad block(s) in image | No bad blocks found in image |

| Drive/Image Verify Results | |
|----------------------------|--|
| Name | data_leakage_rm#3_type3.E01 |
| Sector count | 52513 |
| MD5 Hash | |
| Computed hash | df914108fb3d86744eb688eba482fbdf |
| Stored verification hash | df914108fb3d86744eb688eba482fbdf |
| Verify result | Match |
| SHA1 Hash | |
| Computed hash | 7f3c2eb1f1e2db97be6e963625402a0e362a532c |
| Stored verification hash | 7f3c2eb1f1e2db97be6e963625402a0e362a532c |
| Verify result | Match |
| Bad Blocks List | |
| Bad block(s) in image | No bad blocks found in image |

2. Identify the partition information of PC image.

Answer:

| No. | Name | File system | Start Sector | Total Sectors | Size |
|-----|------|-------------|--------------|---------------|---------|
| 1 | C: | NTFS | 2,048 | 204,800 | 100 MB |
| 2 | D: | NTFS | 206,848 | 41,734,144 | 19.9 GB |

| Name | Description | Initialized Size | Physical Size | Starting Extent | File Extents | Permissions | Physical Location |
|--------------------|--|------------------|---------------|-----------------|--------------|-------------|-------------------|
| 1 C | Volume, Sector 2048-206847, 100 MB, Folder, Internal, Hidden, System | 4,096 | 4,096 | 0C-C44 | 1 | • | 1,228,800 |
| 2 D | Volume, Sector 206848-41940991, 19.9 GB, Folder, Internal, Overwritten, Hidden, System | 12,288 | 12,288 | 0D-C3 | 1 | • | 105,918,464 |
| 3 Unused Disk Area | File, Unallocated Clusters | 2,096,640 | 2,096,640 | 0S1 | 2 | | 512 |

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

Answer: This path points to a critical section within the SOFTWARE registry hive for user profile on a Windows system. The **CurrentVersion** key under **Microsoft\Windows NT** stores essential information about the current version of Windows and its components, including installed software, system settings, user preferences, and application data.

Analyzing this key can reveal crucial details about the user's software environment, system configuration, and potentially any modifications or anomalies related to installed programs or system settings, which could be valuable in a digital forensics investigation. The information about the OS is mentioned below.

Path:

Data_Leak\cfreds_2015_data_leakage_pc\Windows\System32\config\SOFTWARE\CMICreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\Microsoft\Windows NT\CurrentVersion

| Serial Number | OS Information | Answer |
|---------------|-------------------|--|
| 1 | Current Version | 6.1 |
| 2 | Current Build | Client |
| 3 | Software Type | System |
| 4 | Current Type | Multiprocessor free |
| 5 | Install Date | 22 nd March 2015; Sunday; 14:34:26 GMT+0000 (TS=1427034866) |
| 6 | Registered Owner | Informant |
| 7 | System Root | C:\Windows |
| 8 | Installation Type | Client |
| 9 | Edition ID | Ultimate |
| 10 | Product Name | Windows 7 Ultimate |
| 11 | Product ID | 00426-292-0000007-85262 |

The screenshot shows two windows side-by-side. The left window is 'Case Analyzer' showing a list of selected targets (5 items) with columns: Target, Product Name, Product ID, Version, Registered Owner, System Root, Path, and Install Date. The right window is a timestamp converter titled 'Convert epoch to human-readable date and vice versa'. It has a text input field containing '1427034866', a button 'Timestamp to Human date [batch convert]', and explanatory text about supporting Unix timestamps in seconds, milliseconds, microseconds, and nanoseconds. It also provides details about the timestamp: GMT: Sunday, March 22, 2015 2:34:26 PM; Your time zone: Sunday, March 22, 2015 10:34:26 AM GMT-04:00 DST; and Relative: 10 years ago.

| Target | Product Name | Product ID | Version | Registered Owner | System Root | Path | Install Date |
|-------------------------------|--------------------|-------------------------|---------|------------------|-------------|------------|--|
| 1 cfreds_2015_data_leakage_pc | Windows 7 Ultimate | 00426-292-0000007-85262 | 6.1 | 7601 informant | C:\Windows | C:\Windows | 03/22/15 10:34:26 AM (-4:00 Eastern Daylight Time) |
| 2 cfreds_2015_data_leakage_pc | Windows 7 Ultimate | 00426-292-0000007-85262 | 6.1 | 7601 informant | C:\Windows | C:\Windows | 03/22/15 10:34:26 AM (-4:00 Eastern Daylight Time) |
| 3 cfreds_2015_data_leakage_pc | Windows 7 Ultimate | 00426-292-0000007-85262 | 6.1 | 7601 informant | C:\Windows | C:\Windows | 03/22/15 10:34:26 AM (-4:00 Eastern Daylight Time) |
| 4 cfreds_2015_data_leakage_pc | Windows 7 Ultimate | 00426-292-0000007-85262 | 6.1 | 7601 informant | C:\Windows | C:\Windows | 03/22/15 10:34:26 AM (-4:00 Eastern Daylight Time) |
| 5 cfreds_2015_data_leakage_pc | Windows 7 Ultimate | 00426-292-0000007-85262 | 6.1 | 7601 informant | C:\Windows | C:\Windows | 03/22/15 10:34:26 AM (-4:00 Eastern Daylight Time) |

Convert epoch to human-readable date and vice versa

1427034866 [Timestamp to Human date \[batch convert\]](#)

Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.

Assuming that this timestamp is in **seconds**:

GMT : Sunday, March 22, 2015 2:34:26 PM

Your time zone : Sunday, March 22, 2015 10:34:26 AM **GMT-04:00 DST**

Relative : 10 years ago

4. What is the timezone setting?

Answer: This path points to a registry key within the SYSTEM hive of a potentially compromised Windows system, specifically identifying the TimeZoneKeyName value for a particular user profile or control set. This value stores the name of the current time zone used by the system. In a forensic context, this information can be crucial for accurately interpreting timestamps, correlating events across different time zones, and understanding the system's geographical location or user's travel history. The time zone setting of the device is "**Eastern Standard Time**"

Path:

Data_Leak\cfreds_2015_data_leakage_pc\Windows\System32\config\SYSTEM\CMS-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}\ControlSet001\Control\TimeZoneInformation\TimeZoneKeyName

Evidence:

| | Target | Registr. | Active Time Bias | Bias | Standard Bias | Standard Name | Standard Start | Daylight Bias | Daylight Name | Daylight Start |
|---|------------------|----------|------------------|------|---------------|-----------------------|-------------------------------------|---------------|-----------------------|------------------------------------|
| 1 | cfreds_2015_data | D | -4 | -5 | 0 | Eastern Standard Time | Month: 11 - Sunday: 1 - Time: 02:00 | +1 | Eastern Daylight Time | Month: 3 - Sunday: 2 - Time: 02:00 |
| 2 | cfreds_2015_data | D | -4 | -5 | 0 | Eastern Standard Time | Month: 11 - Sunday: 1 - Time: 02:00 | +1 | Eastern Daylight Time | Month: 3 - Sunday: 2 - Time: 02:00 |
| 3 | cfreds_2015_data | D | -4 | -5 | 0 | Eastern Standard Time | Month: 11 - Sunday: 1 - Time: 02:00 | +1 | Eastern Daylight Time | Month: 3 - Sunday: 2 - Time: 02:00 |
| 4 | cfreds_2015_data | D | -4 | -5 | 0 | Eastern Standard Time | Month: 11 - Sunday: 1 - Time: 02:00 | +1 | Eastern Daylight Time | Month: 3 - Sunday: 2 - Time: 02:00 |
| 5 | cfreds_2015_data | D | -4 | -5 | 0 | Eastern Standard Time | Month: 11 - Sunday: 1 - Time: 02:00 | +1 | Eastern Daylight Time | Month: 3 - Sunday: 2 - Time: 02:00 |

5. What is the computer name?

Answer: The name of computer is "**INFORMANT-PC**"

Path:

Data_Leak\cfreds_2015_data_leakage_pc\Windows\System32\config\SYSTEM\CMS-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}

| Name | Type | Value |
|-----------------------------|---------|-------|
| DaylightStart | Unknown | 16 |
| StandardBias | Unknown | 4 |
| StandardName | Unknown | 32 |
| StandardStart | Unknown | 16 |
| TimeZoneKeyName | String | 256 |
| DynamicDaylightTimeDisabled | Unknown | 4 |

7CB51D4737F5}\ControlSet001\Control\ComputerName\ComputerName\ComputerName

Evidence:

This file path points to a specific registry key within the SYSTEM hive of a Windows system revealing the **computer name**. The path also reveals that the data comes from the SYSTEM hive which contains the system-wide settings and ControlSet001 that usually have the active configuration. This helps understand the context of the computer name within the system's setup.

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

Answer: The users other than Administrator, Guest, systemprofile, LocalService are:

- informant
- admin11
- ITechTeam
- Temporary

| Account | SID | Login Count | Account Created Time | Last Login Time | Login Failure Time |
|-----------|------|-------------|----------------------|---------------------|---------------------|
| informant | 1000 | 10 | 2015-03-22 09:33:54 | 2015-03-25 09:45:59 | 2015-03-25 09:45:43 |
| admin11 | 1001 | 2 | 2015-03-22 10:51:54 | 2015-03-22 10:57:02 | 2015-03-22 10:53:02 |
| ITechTeam | 1002 | 0 | 2015-03-22 10:52:30 | - | - |
| Temporary | 1003 | 1 | 2015-03-22 10:53:01 | 2015-03-22 10:55:57 | 2015-03-22 10:56:37 |

| | Target | User | Friendly Name | Last Logon | Security ID |
|------|-----------------------------|---------------|---------------|--|--|
| □ 36 | cfreds_2015_data_leakage_pc | Administrator | Administrator | 11/20/10 10:47:20 PM (-5:00 Eastern Standard Time) | S-1-5-21-2425377081-3129163575-2985601102-500 |
| □ 37 | cfreds_2015_data_leakage_pc | temporary | temporary | 03/22/15 11:55:57 AM (-4:00 Eastern Daylight Time) | S-1-5-21-2425377081-3129163575-2985601102-1003 |
| □ 38 | cfreds_2015_data_leakage_pc | temporary | temporary | 03/22/15 11:55:57 AM (-4:00 Eastern Daylight Time) | S-1-5-21-2425377081-3129163575-2985601102-1003 |
| □ 39 | cfreds_2015_data_leakage_pc | temporary | temporary | 03/22/15 11:55:57 AM (-4:00 Eastern Daylight Time) | S-1-5-21-2425377081-3129163575-2985601102-1003 |
| □ 40 | cfreds_2015_data_leakage_pc | temporary | temporary | 03/22/15 11:55:57 AM (-4:00 Eastern Daylight Time) | S-1-5-21-2425377081-3129163575-2985601102-1003 |
| □ 41 | cfreds_2015_data_leakage_pc | temporary | temporary | 03/22/15 11:55:57 AM (-4:00 Eastern Daylight Time) | S-1-5-21-2425377081-3129163575-2985601102-1003 |
| □ 42 | cfreds_2015_data_leakage_pc | temporary | temporary | 03/22/15 11:55:57 AM (-4:00 Eastern Daylight Time) | S-1-5-21-2425377081-3129163575-2985601102-1003 |
| □ 43 | cfreds_2015_data_leakage_pc | admin11 | admin11 | 03/22/15 11:57:02 AM (-4:00 Eastern Daylight Time) | S-1-5-21-2425377081-3129163575-2985601102-1001 |
| □ 44 | cfreds_2015_data_leakage_pc | admin11 | admin11 | 03/22/15 11:57:02 AM (-4:00 Eastern Daylight Time) | S-1-5-21-2425377081-3129163575-2985601102-1001 |
| □ 45 | cfreds_2015_data_leakage_pc | admin11 | admin11 | 03/22/15 11:57:02 AM (-4:00 Eastern Daylight Time) | S-1-5-21-2425377081-3129163575-2985601102-1001 |
| □ 46 | cfreds_2015_data_leakage_pc | admin11 | admin11 | 03/22/15 11:57:02 AM (-4:00 Eastern Daylight Time) | S-1-5-21-2425377081-3129163575-2985601102-1001 |
| □ 47 | cfreds_2015_data_leakage_pc | admin11 | admin11 | 03/22/15 11:57:02 AM (-4:00 Eastern Daylight Time) | S-1-5-21-2425377081-3129163575-2985601102-1001 |
| □ 48 | cfreds_2015_data_leakage_pc | admin11 | admin11 | 03/22/15 11:57:02 AM (-4:00 Eastern Daylight Time) | S-1-5-21-2425377081-3129163575-2985601102-1001 |
| □ 49 | cfreds_2015_data_leakage_pc | informant | informant | 03/25/15 10:45:59 AM (-4:00 Eastern Daylight Time) | S-1-5-21-2425377081-3129163575-2985601102-1000 |
| □ 50 | cfreds_2015_data_leakage_pc | informant | informant | 03/25/15 10:45:59 AM (-4:00 Eastern Daylight Time) | S-1-5-21-2425377081-3129163575-2985601102-1000 |
| □ 51 | cfreds_2015_data_leakage_pc | informant | informant | 03/25/15 10:45:59 AM (-4:00 Eastern Daylight Time) | S-1-5-21-2425377081-3129163575-2985601102-1000 |
| □ 52 | cfreds_2015_data_leakage_pc | informant | informant | 03/25/15 10:45:59 AM (-4:00 Eastern Daylight Time) | S-1-5-21-2425377081-3129163575-2985601102-1000 |
| □ 53 | cfreds_2015_data_leakage_pc | informant | informant | 03/25/15 10:45:59 AM (-4:00 Eastern Daylight Time) | S-1-5-21-2425377081-3129163575-2985601102-1000 |

7. Who was the last user to log on to a PC?

Answer: The Last user to logon into the PC was "informant". He logged into the system at "03/25/15 10:45:59 AM (-4:00 Eastern Daylight Time)"

Path: Data_Leak\cfreds_2015_data_leakage_pc\Windows\System32\config\SAM\CMICreateHive{C4E7BA2B-68E8-499C-B1A1-371AC8D717C7}\SAM\Domains\Account\Users\

Evidence:

| | Target | User | Friendly Name | Last Logon |
|------|-----------------------------|-----------|---------------|--|
| □ 51 | cfreds_2015_data_leakage_pc | admin11 | admin11 | 03/22/15 11:57:02 AM (-4:00 Eastern Daylight Time) |
| □ 52 | cfreds_2015_data_leakage_pc | admin11 | admin11 | 03/22/15 11:57:02 AM (-4:00 Eastern Daylight Time) |
| □ 53 | cfreds_2015_data_leakage_pc | admin11 | admin11 | 03/22/15 11:57:02 AM (-4:00 Eastern Daylight Time) |
| □ 54 | cfreds_2015_data_leakage_pc | admin11 | admin11 | 03/22/15 11:57:02 AM (-4:00 Eastern Daylight Time) |
| □ 55 | cfreds_2015_data_leakage_pc | admin11 | admin11 | 03/22/15 11:57:02 AM (-4:00 Eastern Daylight Time) |
| □ 56 | cfreds_2015_data_leakage_pc | admin11 | admin11 | 03/22/15 11:57:02 AM (-4:00 Eastern Daylight Time) |
| □ 57 | cfreds_2015_data_leakage_pc | informant | informant | 03/25/15 10:45:59 AM (-4:00 Eastern Daylight Time) |
| □ 58 | cfreds_2015_data_leakage_pc | informant | informant | 03/25/15 10:45:59 AM (-4:00 Eastern Daylight Time) |
| □ 59 | cfreds_2015_data_leakage_pc | informant | informant | 03/25/15 10:45:59 AM (-4:00 Eastern Daylight Time) |
| □ 60 | cfreds_2015_data_leakage_pc | informant | informant | 03/25/15 10:45:59 AM (-4:00 Eastern Daylight Time) |
| □ 61 | cfreds_2015_data_leakage_pc | informant | informant | 03/25/15 10:45:59 AM (-4:00 Eastern Daylight Time) |
| □ 62 | cfreds_2015_data_leakage_pc | informant | informant | 03/25/15 10:45:59 AM (-4:00 Eastern Daylight Time) |
| □ 63 | cfreds_2015_data_leakage_pc | informant | informant | 03/25/15 10:45:59 AM (-4:00 Eastern Daylight Time) |

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

Answer: the last recorded shutdown date and time was **March 25, 2015, at 3:31:05 PM GMT.**

This was derived by converting the given time of 11:31:05 AM EST on March 25, 2015, to GMT, taking into account that Daylight Saving Time (DST) was in effect.

Path:

Data_Leak\cfreds_2015_data_leakage_pc\Windows\System32\config\SYSTEM\CMS-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}\ControlSet001\Control\Windows\ShutdownTime

Evidence:

| Name | Value |
|-------------------------------|----------------------|
| High ASCII | W\H\r g\ |
| Unicode | 时间 |
| Picture/Unix Date (Time/Date) | 05/18/66 03:53:59 PM |
| Windows Date/Time (Time/Date) | 03/25/15 11:31:05 AM |
| HFS Plus Date (Time/Date) | 09/14/86 05:34:45 AM |
| DOS Date (DOS Date) | 10/08/70 09:10:46 PM |

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

Answer:

| Serial Number | Network Interface Information | Answer |
|---------------|-------------------------------|---|
| 1 | DHCP Enabled | Yes |
| 2 | DHCP Server | 10.11.11.254 |
| 3 | IP Address | 10.11.11.129 |
| 4 | Subnet Mask | 10.11.11.254 |
| 5 | Server Name | 10.11.11.2 |
| 6 | Domain Name | localdomain |
| 7 | Default Gateway | 255.255.255.0 |
| 8 | Network Card | Intel(R) PRO/1000 MT Network Connection |

Path:

Data_Leak\cfreds_2015_data_leakage_pc\Windows\System32\config\SOFTWARE\CMI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\Microsoft\Windows NT\CurrentVersion\NetworkCards\8\Description

| Name | Last Written |
|-------------|--|
| Description | Data_Leak\cfreds_2015_data_leakage_pc\Windows\System32\config\SOFTWARE\CMI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\Microsoft\Windows NT\CurrentVersion\NetworkCards\8\Description |
| ServiceName | Data_Leak\cfreds_2015_data_leakage_pc\Windows\System32\config\SOFTWARE\CMI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\Microsoft\Windows NT\CurrentVersion\NetworkCards\8\Description |

Path:

Data_Leak\cfreds_2015_data_leakage_pc\Windows\System32\config\SYSTEM\CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}\ControlSet001\services\Tcpip\

| Name | Value |
|-----------------------|----------------------|
| High ASCII | informant-PC |
| Unicode | informant-PC |
| Unix Date (Time/Date) | 03/25/70 05:31:05 AM |

CYFI-720 Data Leakage Case

Mohit Dhabuwala

| | Name | Last Written | |
|------|------------------------------|--|---|
| □ 1 | Adapters | 03/25/15 06:17:15 AM (-4:00 Eastern Daylight Time) | Data_Leak\cfreds_2015_data_leakage_pc\D\Windows\System32\config |
| □ 2 | DataBasePath | | Data_Leak\cfreds_2015_data_leakage_pc\DWWindows\System32\config |
| □ 3 | DeadGWDetectDefault | | Data_Leak\cfreds_2015_data_leakage_pc\DWWindows\System32\config |
| □ 4 | DhcpDomain | | Data_Leak\cfreds_2015_data_leakage_pc\DWWindows\System32\config |
| □ 5 | DhcpNameServer | | Data_Leak\cfreds_2015_data_leakage_pc\DWWindows\System32\config |
| □ 6 | DNSRegisteredAdapters | 11/20/10 10:39:53 PM (-5:00 Eastern Standard Time) | Data_Leak\cfreds_2015_data_leakage_pc\DWWindows\System32\config |
| □ 7 | Domain | | Data_Leak\cfreds_2015_data_leakage_pc\DWWindows\System32\config |
| □ 8 | DontAddDefaultGatewayDefault | | Data_Leak\cfreds_2015_data_leakage_pc\DWWindows\System32\config |
| □ 9 | EnableICMPRedirect | | Data_Leak\cfreds_2015_data_leakage_pc\DWWindows\System32\config |
| □ 10 | EnableWsd | | Data_Leak\cfreds_2015_data_leakage_pc\DWWindows\System32\config |

| | Name | Last Written | |
|------|------------------------------|--|---|
| □ 1 | Adapters | 03/25/15 06:17:15 AM (-4:00 Eastern Daylight Time) | Data_Leak\cfreds_2015_data_leakage_pc\DWWindows\System32\config |
| □ 2 | DataBasePath | | Data_Leak\cfreds_2015_data_leakage_pc\DWWindows\System32\config |
| □ 3 | DeadGWDetectDefault | | Data_Leak\cfreds_2015_data_leakage_pc\DWWindows\System32\config |
| □ 4 | DhcpDomain | | Data_Leak\cfreds_2015_data_leakage_pc\DWWindows\System32\config |
| □ 5 | DhcpNameServer | | Data_Leak\cfreds_2015_data_leakage_pc\DWWindows\System32\config |
| □ 6 | DNSRegisteredAdapters | 11/20/10 10:39:53 PM (-5:00 Eastern Standard Time) | Data_Leak\cfreds_2015_data_leakage_pc\DWWindows\System32\config |
| □ 7 | Domain | | Data_Leak\cfreds_2015_data_leakage_pc\DWWindows\System32\config |
| □ 8 | DontAddDefaultGatewayDefault | | Data_Leak\cfreds_2015_data_leakage_pc\DWWindows\System32\config |
| □ 9 | EnableICMPRedirect | | Data_Leak\cfreds_2015_data_leakage_pc\DWWindows\System32\config |
| □ 10 | EnableWsd | | Data_Leak\cfreds_2015_data_leakage_pc\DWWindows\System32\config |

| | Name | Last Written | |
|------|----------------------------|--------------|--|
| □ 1 | AddressType | | Data_Leak\cfreds_2015_data_leakage_pc\D\Windows\System32\config\ |
| □ 2 | DhcpConnForceBroadcastFlag | | Data_Leak\cfreds_2015_data_leakage_pc\D\Windows\System32\config\ |
| □ 3 | DhcpDefaultGateway | | Data_Leak\cfreds_2015_data_leakage_pc\D\Windows\System32\config\ |
| □ 4 | DhcpDomain | | Data_Leak\cfreds_2015_data_leakage_pc\D\Windows\System32\config\ |
| □ 5 | DhcpGatewayHardware | | Data_Leak\cfreds_2015_data_leakage_pc\D\Windows\System32\config\ |
| □ 6 | DhcpGatewayHardwareCount | | Data_Leak\cfreds_2015_data_leakage_pc\D\Windows\System32\config\ |
| □ 7 | DhcpInterfaceOptions | | Data_Leak\cfreds_2015_data_leakage_pc\D\Windows\System32\config\ |
| □ 8 | DhcpIPAddress | | Data_Leak\cfreds_2015_data_leakage_pc\D\Windows\System32\config\ |
| □ 9 | DhcpNameServer | | Data_Leak\cfreds_2015_data_leakage_pc\D\Windows\System32\config\ |
| □ 10 | DhcpServer | | Data_Leak\cfreds_2015_data_leakage_pc\D\Windows\System32\config\ |

| | Name | Last Written |
|------|----------------------------|--|
| □ 1 | AddressType | Data_Leak\cfreds_2015_data_leakage_pc\DWIndows\System32\config |
| □ 2 | DhcpConnForceBroadcastFlag | Data_Leak\cfreds_2015_data_leakage_pc\DWIndows\System32\config |
| □ 3 | DhcpDefaultGateway | Data_Leak\cfreds_2015_data_leakage_pc\DWIndows\System32\config |
| □ 4 | DhcpDomain | Data_Leak\cfreds_2015_data_leakage_pc\DWIndows\System32\config |
| □ 5 | DhcpGatewayHardware | Data_Leak\cfreds_2015_data_leakage_pc\DWIndows\System32\config |
| □ 6 | DhcpGatewayHardwareCount | Data_Leak\cfreds_2015_data_leakage_pc\DWIndows\System32\config |
| □ 7 | DhcpInterfaceOptions | Data_Leak\cfreds_2015_data_leakage_pc\DWIndows\System32\config |
| □ 8 | DhcpIPAddress | Data_Leak\cfreds_2015_data_leakage_pc\DWIndows\System32\config |
| □ 9 | DhcpNameServer | Data_Leak\cfreds_2015_data_leakage_pc\DWIndows\System32\config |
| □ 10 | DhcpServer | Data_Leak\cfreds_2015_data_leakage_pc\DWIndows\System32\config |

Doc Transcript Condition Filter EnScript Decode Tag

Find Find Next Bookmark

| Name | Value |
|------------|------------|
| High ASCII | 10.11.11.2 |

1 00 31 00 2B 00 32 00 00 1·0···1·1··1·1··2·

| | Name | Last Written |
|------|----------------------------|--|
| □ 1 | AddressType | Data_Leak\cfreds_2015_data_leakage_pc\DWIndows\System32\config |
| □ 2 | DhcpConnForceBroadcastFlag | Data_Leak\cfreds_2015_data_leakage_pc\DWIndows\System32\config |
| □ 3 | DhcpDefaultGateway | Data_Leak\cfreds_2015_data_leakage_pc\DWIndows\System32\config |
| □ 4 | DhcpDomain | Data_Leak\cfreds_2015_data_leakage_pc\DWIndows\System32\config |
| □ 5 | DhcpGatewayHardware | Data_Leak\cfreds_2015_data_leakage_pc\DWIndows\System32\config |
| □ 6 | DhcpGatewayHardwareCount | Data_Leak\cfreds_2015_data_leakage_pc\DWIndows\System32\config |
| □ 7 | DhcpInterfaceOptions | Data_Leak\cfreds_2015_data_leakage_pc\DWIndows\System32\config |
| □ 8 | DhcpIPAddress | Data_Leak\cfreds_2015_data_leakage_pc\DWIndows\System32\config |
| □ 9 | DhcpNameServer | Data_Leak\cfreds_2015_data_leakage_pc\DWIndows\System32\config |
| □ 10 | DhcpServer | Data_Leak\cfreds_2015_data_leakage_pc\DWIndows\System32\config |

Doc Transcript Condition Filter EnScript Decode Tag

Find Find Next Bookmark

| Name | Value |
|------------|--------------|
| High ASCII | 10.11.11.129 |
| Unicode | 10.11.11.129 |

31 00 31 00 2B 00 31 00 32 1·0···1·1··1·1··1·2·

| | Name | Last Written |
|------|--------------------------|--|
| □ 4 | DhcpDomain | Data_Leak\cfreds_2015_data_leakage_pc\DWIndows\System32\config |
| □ 5 | DhcpGatewayHardware | Data_Leak\cfreds_2015_data_leakage_pc\DWIndows\System32\config |
| □ 6 | DhcpGatewayHardwareCount | Data_Leak\cfreds_2015_data_leakage_pc\DWIndows\System32\config |
| □ 7 | DhcpInterfaceOptions | Data_Leak\cfreds_2015_data_leakage_pc\DWIndows\System32\config |
| □ 8 | DhcpIPAddress | Data_Leak\cfreds_2015_data_leakage_pc\DWIndows\System32\config |
| □ 9 | DhcpNameServer | Data_Leak\cfreds_2015_data_leakage_pc\DWIndows\System32\config |
| □ 10 | DhcpServer | Data_Leak\cfreds_2015_data_leakage_pc\DWIndows\System32\config |
| □ 11 | DhcpSubnetMask | Data_Leak\cfreds_2015_data_leakage_pc\DWIndows\System32\config |
| □ 12 | DhcpSubnetMaskOpt | Data_Leak\cfreds_2015_data_leakage_pc\DWIndows\System32\config |
| □ 13 | Domain | Data_Leak\cfreds_2015_data_leakage_pc\DWIndows\System32\config |

Doc Transcript Condition Filter EnScript Decode Tag

Find Find Next Bookmark

| Name | Value |
|------------|---------------|
| High ASCII | 255.255.255.0 |
| Unicode | 255.255.255.0 |

5 00 2B 00 32 00 35 00 35 2·5·5··2·5·5··2·5·5·

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

Answer:

11. List application execution logs.

(Executable path, execution time, execution count...)

Answer: The execution logs can be found from many directories like: prefetch directory, UserAssist Key, Shimcache (AppCompatCache), Event Logs, Jump Lists, etc. This are the prime directories where this file execution logs are usually available.

Path: Data_Leak\cfreds_2015_data_leakage_pc\Program Files (x86)\Common Files\Apple\Internet Services\iCloudWeb.exe

| | Target | Link File | Base Path |
|------|-----------------------------|------------------------------------|--|
| □ 1 | cfreds_2015_data_leakage_pc | Google Chrome.lnk | C:\Program Files (x86)\Google\Chrome\Application\chrome.exe |
| □ 2 | cfreds_2015_data_leakage_pc | Google Drive.lnk | C:\Program Files (x86)\Google\Drive\googledrivesync.exe |
| □ 3 | cfreds_2015_data_leakage_pc | Google Sheets.lnk | C:\Program Files (x86)\Google\Drive\googledrivesync.exe |
| □ 4 | cfreds_2015_data_leakage_pc | Google Slides.lnk | C:\Program Files (x86)\Google\Drive\googledrivesync.exe |
| □ 5 | cfreds_2015_data_leakage_pc | Google Docs.lnk | C:\Program Files (x86)\Google\Drive\googledrivesync.exe |
| □ 6 | cfreds_2015_data_leakage_pc | iCloud.lnk | C:\Program Files (x86)\Common Files\Apple\Internet Services\iCloud.exe |
| □ 7 | cfreds_2015_data_leakage_pc | Mail.lnk | C:\Program Files (x86)\Common Files\Apple\Internet Services\iCloudWeb.exe |
| □ 8 | cfreds_2015_data_leakage_pc | Contacts.lnk | C:\Program Files (x86)\Common Files\Apple\Internet Services\iCloudWeb.exe |
| □ 9 | cfreds_2015_data_leakage_pc | Calendar.lnk | C:\Program Files (x86)\Common Files\Apple\Internet Services\iCloudWeb.exe |
| □ 10 | cfreds_2015_data_leakage_pc | Find My iPhone.lnk | C:\Program Files (x86)\Common Files\Apple\Internet Services\iCloudWeb.exe |
| □ 11 | cfreds_2015_data_leakage_pc | Notes.lnk | C:\Program Files (x86)\Common Files\Apple\Internet Services\iCloudWeb.exe |
| □ 12 | cfreds_2015_data_leakage_pc | Reminders.lnk | C:\Program Files (x86)\Common Files\Apple\Internet Services\iCloudWeb.exe |
| □ 13 | cfreds_2015_data_leakage_pc | iCloud Photos.lnk | C:\Program Files (x86)\Common Files\Apple\Internet Services\ShellStreamsShortcut.exe |
| □ 14 | cfreds_2015_data_leakage_pc | Eraser.lnk | C:\Program Files\Eraser\Eraser.exe |
| □ 15 | cfreds_2015_data_leakage_pc | Internet Explorer.lnk | C:\Program Files\Internet Explorer\iexplore.exe |
| □ 16 | cfreds_2015_data_leakage_pc | Google Chrome.lnk | C:\Program Files (x86)\Google\Chrome\Application\chrome.exe |
| □ 17 | cfreds_2015_data_leakage_pc | Internet Explorer (No Add-ons).lnk | C:\Program Files\Internet Explorer\iexplore.exe |
| □ 18 | cfreds_2015_data_leakage_pc | Internet Explorer.lnk | C:\Program Files\Internet Explorer\iexplore.exe |

There are multiple executable files executed, and all the files are in different directories.

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.)

Answer: This data is taken from the event log file named "security.evtx and system.evtx."

These values can be interpreted from the Event ID column of the activity log. Path for both successful logons and logoffs: **D:\Windows\System32\winevt\Logs\Security.evtx**

| Manage Saved Reports | | | | | |
|----------------------|--|--------------------------------|---|------------------|--|
| Selected 0/57 | | Selected 0/625 | | Constraint | |
| | | | | Clear Constraint | |
| | | Target | Name | Event ID | Generated |
| | | 1 cfreds_2015_data_leakage_pc | An account was successfully logged on. Subject:Security | 4624 | 03/22/15 10:51:14 AM (-4:00 Eastern Daylight Time) 03/22/15 10:51:14 A |
| | | 2 cfreds_2015_data_leakage_pc | An account was successfully logged on. Subject:Security | 4624 | 03/22/15 10:51:14 AM (-4:00 Eastern Daylight Time) 03/22/15 10:51:14 A |
| | | 3 cfreds_2015_data_leakage_pc | An account was successfully logged on. Subject:Security | 4624 | 03/22/15 10:51:14 AM (-4:00 Eastern Daylight Time) 03/22/15 10:51:14 A |
| | | 4 cfreds_2015_data_leakage_pc | An account was successfully logged on. Subject:Security | 4624 | 03/22/15 10:51:14 AM (-4:00 Eastern Daylight Time) 03/22/15 10:51:14 A |
| | | 5 cfreds_2015_data_leakage_pc | An account was successfully logged on. Subject:Security | 4624 | 03/22/15 10:51:14 AM (-4:00 Eastern Daylight Time) 03/22/15 10:51:14 A |
| | | 6 cfreds_2015_data_leakage_pc | An account was successfully logged on. Subject:Security | 4624 | 03/22/15 11:22:31 AM (-4:00 Eastern Daylight Time) 03/22/15 11:22:31 A |
| | | 7 cfreds_2015_data_leakage_pc | An account was successfully logged on. Subject:Security | 4624 | 03/22/15 11:22:31 AM (-4:00 Eastern Daylight Time) 03/22/15 11:22:31 A |
| | | 8 cfreds_2015_data_leakage_pc | An account was successfully logged on. Subject:Security | 4624 | 03/22/15 11:22:31 AM (-4:00 Eastern Daylight Time) 03/22/15 11:22:31 A |
| | | 9 cfreds_2015_data_leakage_pc | An account was successfully logged on. Subject:Security | 4624 | 03/22/15 11:22:31 AM (-4:00 Eastern Daylight Time) 03/22/15 11:22:31 A |
| | | 10 cfreds_2015_data_leakage_pc | An account was successfully logged on. Subject:Security | 4624 | 03/22/15 11:22:31 AM (-4:00 Eastern Daylight Time) 03/22/15 11:22:31 A |
| | | 11 cfreds_2015_data_leakage_pc | An account was successfully logged on. Subject:Security | 4624 | 03/22/15 11:43:36 AM (-4:00 Eastern Daylight Time) 03/22/15 11:43:36 A |
| | | 12 cfreds_2015_data_leakage_pc | An account was successfully logged on. Subject:Security | 4624 | 03/22/15 11:43:36 AM (-4:00 Eastern Daylight Time) 03/22/15 11:43:36 A |
| | | 13 cfreds_2015_data_leakage_pc | An account was successfully logged on. Subject:Security | 4624 | 03/22/15 11:43:36 AM (-4:00 Eastern Daylight Time) 03/22/15 11:43:36 A |
| | | 14 cfreds_2015_data_leakage_pc | An account was successfully logged on. Subject:Security | 4624 | 03/22/15 11:43:36 AM (-4:00 Eastern Daylight Time) 03/22/15 11:43:36 A |
| | | 15 cfreds_2015_data_leakage_pc | An account was successfully logged on. Subject:Security | 4624 | 03/22/15 11:43:36 AM (-4:00 Eastern Daylight Time) 03/22/15 11:43:36 A |
| | | 16 cfreds_2015_data_leakage_pc | An account was successfully logged on. Subject:Security | 4624 | 03/23/15 01:24:23 PM (-4:00 Eastern Daylight Time) 03/23/15 01:24:23 P |
| | | 17 cfreds_2015_data_leakage_pc | An account was successfully logged on. Subject:Security | 4624 | 03/23/15 01:24:23 PM (-4:00 Eastern Daylight Time) 03/23/15 01:24:23 P |
| | | 18 cfreds_2015_data_leakage_pc | An account was successfully logged on. Subject:Security | 4624 | 03/23/15 01:24:23 PM (-4:00 Eastern Daylight Time) 03/23/15 01:24:23 P |

There are total of 625 successful logons made into the computer. This figure is not accurate as it contains many duplicated values as well

There are total of 55 successful logoffs made into the computer. This figure is not accurate as it contains many duplicated values as well

- Event ID 1100: Audit Log Cleared

| Security Number of events: 1,193 | | | | | |
|----------------------------------|------------------------------|----------|-------------|-------------------------|--|
| Level | Date and Time | Source | Event ID | Task Category | |
| Event ID: 1100 (8) | | | | | |
| Information | 3/22/2015 11:19:42 AM | Eventlog | 1100 | Service shutdown | |
| Information | 3/22/2015 12:00:09 PM | Eventlog | 1100 | Service shutdown | |
| Information | 3/22/2015 11:28:28 AM | Eventlog | 1100 | Service shutdown | |
| Information | 3/23/2015 5:02:59 PM | Eventlog | 1100 | Service shutdown | |
| Information | 3/24/2015 5:07:26 PM | Eventlog | 1100 | Service shutdown | |
| Information | 3/25/2015 6:18:29 AM | Eventlog | 1100 | Service shutdown | |
| Information | 3/25/2015 11:31:00 AM | Eventlog | 1100 | Service shutdown | |
| Information | 3/22/2015 10:38:16 AM | Eventlog | 1100 | Service shutdown | |

- Event ID 4624: Successful Logon

| | | | | | |
|-----------------------------|-----------------------|---------------------------------|------|-------|--|
| Event ID: 4624 (141) | | | | | |
| Information | 3/23/2015 1:24:24 PM | Microsoft Windows security a... | 4624 | Logon | |
| Information | 3/25/2015 6:19:46 AM | Microsoft Windows security a... | 4624 | Logon | |
| Information | 3/23/2015 1:24:24 PM | Microsoft Windows security a... | 4624 | Logon | |
| Information | 3/23/2015 1:24:24 PM | Microsoft Windows security a... | 4624 | Logon | |
| Information | 3/23/2015 1:24:25 PM | Microsoft Windows security a... | 4624 | Logon | |
| Information | 3/23/2015 1:24:26 PM | Microsoft Windows security a... | 4624 | Logon | |
| Information | 3/25/2015 6:33:14 AM | Microsoft Windows security a... | 4624 | Logon | |
| Information | 3/25/2015 6:33:16 AM | Microsoft Windows security a... | 4624 | Logon | |
| Information | 3/23/2015 1:24:24 PM | Microsoft Windows security a... | 4624 | Logon | |
| Information | 3/25/2015 10:57:18 AM | Microsoft Windows security a... | 4624 | Logon | |
| Information | 3/23/2015 1:24:23 PM | Microsoft Windows security a... | 4624 | Logon | |
| Information | 3/25/2015 6:19:46 AM | Microsoft Windows security a... | 4624 | Logon | |
| Information | 3/22/2015 11:57:54 AM | Microsoft Windows security a... | 4624 | Logon | |
| Information | 3/22/2015 11:57:54 AM | Microsoft Windows security a... | 4624 | Logon | |
| Information | 3/22/2015 11:55:57 AM | Microsoft Windows security a... | 4624 | Logon | |
| Information | 3/25/2015 6:19:30 AM | Microsoft Windows security a... | 4624 | Logon | |
| Information | 3/25/2015 6:19:46 AM | Microsoft Windows security a... | 4624 | Logon | |
| Information | 3/22/2015 11:57:02 AM | Microsoft Windows security a... | 4624 | Logon | |
| Information | 3/22/2015 11:57:02 AM | Microsoft Windows security a... | 4624 | Logon | |
| Information | 3/23/2015 4:01:01 PM | Microsoft Windows security a... | 4624 | Logon | |
| Information | 3/22/2015 10:34:28 AM | Microsoft Windows security a... | 4624 | Logon | |
| Information | 3/22/2015 10:34:28 AM | Microsoft Windows security a... | 4624 | Logon | |

- Event ID 4648: Logon Attempt Using Explicit Credentials

| | | | | | |
|----------------------------|-----------------------|---------------------------------|------|-------|--|
| Event ID: 4648 (15) | | | | | |
| Information | 3/25/2015 10:45:59 AM | Microsoft Windows security a... | 4648 | Logon | |
| Information | 3/22/2015 11:45:16 AM | Microsoft Windows security a... | 4648 | Logon | |
| Information | 3/25/2015 9:06:08 AM | Microsoft Windows security a... | 4648 | Logon | |
| Information | 3/24/2015 9:21:44 AM | Microsoft Windows security a... | 4648 | Logon | |
| Information | 3/22/2015 11:53:44 AM | Microsoft Windows security a... | 4648 | Logon | |
| Information | 3/24/2015 2:28:38 PM | Microsoft Windows security a... | 4648 | Logon | |
| Information | 3/22/2015 11:57:54 AM | Microsoft Windows security a... | 4648 | Logon | |
| Information | 3/22/2015 11:57:02 AM | Microsoft Windows security a... | 4648 | Logon | |
| Information | 3/22/2015 11:55:57 AM | Microsoft Windows security a... | 4648 | Logon | |
| Information | 3/24/2015 9:47:06 AM | Microsoft Windows security a... | 4648 | Logon | |
| Information | 3/22/2015 11:24:03 AM | Microsoft Windows security a... | 4648 | Logon | |
| Information | 3/23/2015 4:23:27 PM | Microsoft Windows security a... | 4648 | Logon | |
| Information | 3/22/2015 10:53:39 AM | Microsoft Windows security a... | 4648 | Logon | |
| Information | 3/22/2015 10:34:28 AM | Microsoft Windows security a... | 4648 | Logon | |
| Information | 3/23/2015 1:24:41 PM | Microsoft Windows security a... | 4648 | Logon | |

- Event ID 4634: Logoff

| Event ID: 4634 (11) | | | |
|---------------------|-----------------------|---------------------------------|-------------|
| (i) Information | 3/22/2015 11:56:45 AM | Microsoft Windows security a... | 4634 Logoff |
| (i) Information | 3/22/2015 11:56:45 AM | Microsoft Windows security a... | 4634 Logoff |
| (i) Information | 3/24/2015 2:28:38 PM | Microsoft Windows security a... | 4634 Logoff |
| (i) Information | 3/22/2015 11:57:56 AM | Microsoft Windows security a... | 4634 Logoff |
| (i) Information | 3/22/2015 11:57:55 AM | Microsoft Windows security a... | 4634 Logoff |
| (i) Information | 3/22/2015 11:58:26 AM | Microsoft Windows security a... | 4634 Logoff |
| (i) Information | 3/25/2015 10:45:59 AM | Microsoft Windows security a... | 4634 Logoff |
| (i) Information | 3/22/2015 11:58:26 AM | Microsoft Windows security a... | 4634 Logoff |
| (i) Information | 3/22/2015 11:57:55 AM | Microsoft Windows security a... | 4634 Logoff |
| (i) Information | 3/24/2015 2:28:38 PM | Microsoft Windows security a... | 4634 Logoff |
| (i) Information | 3/25/2015 10:45:59 AM | Microsoft Windows security a... | 4634 Logoff |

- Event ID 4647: User Initiated Logoff

| Event ID: 4634 (11) | | | |
|---------------------|-----------------------|---------------------------------|-------------|
| (i) Information | 3/22/2015 11:56:45 AM | Microsoft Windows security a... | 4634 Logoff |
| (i) Information | 3/22/2015 11:56:45 AM | Microsoft Windows security a... | 4634 Logoff |
| (i) Information | 3/24/2015 2:28:38 PM | Microsoft Windows security a... | 4634 Logoff |
| (i) Information | 3/22/2015 11:57:56 AM | Microsoft Windows security a... | 4634 Logoff |
| (i) Information | 3/22/2015 11:57:55 AM | Microsoft Windows security a... | 4634 Logoff |
| (i) Information | 3/22/2015 11:58:26 AM | Microsoft Windows security a... | 4634 Logoff |
| (i) Information | 3/25/2015 10:45:59 AM | Microsoft Windows security a... | 4634 Logoff |
| (i) Information | 3/22/2015 11:58:26 AM | Microsoft Windows security a... | 4634 Logoff |
| (i) Information | 3/22/2015 11:57:55 AM | Microsoft Windows security a... | 4634 Logoff |
| (i) Information | 3/24/2015 2:28:38 PM | Microsoft Windows security a... | 4634 Logoff |
| (i) Information | 3/25/2015 10:45:59 AM | Microsoft Windows security a... | 4634 Logoff |

| Event ID: 4647 (10) | | | |
|---------------------|-----------------------|---------------------------------|-------------|
| (i) Information | 3/25/2015 11:30:57 AM | Microsoft Windows security a... | 4647 Logoff |
| (i) Information | 3/23/2015 5:02:53 PM | Microsoft Windows security a... | 4647 Logoff |
| (i) Information | 3/22/2015 10:38:15 AM | Microsoft Windows security a... | 4647 Logoff |
| (i) Information | 3/24/2015 5:07:25 PM | Microsoft Windows security a... | 4647 Logoff |
| (i) Information | 3/22/2015 11:57:41 AM | Microsoft Windows security a... | 4647 Logoff |
| (i) Information | 3/22/2015 12:00:08 PM | Microsoft Windows security a... | 4647 Logoff |
| (i) Information | 3/22/2015 11:28:28 AM | Microsoft Windows security a... | 4647 Logoff |
| (i) Information | 3/22/2015 11:55:52 AM | Microsoft Windows security a... | 4647 Logoff |
| (i) Information | 3/22/2015 11:56:58 AM | Microsoft Windows security a... | 4647 Logoff |
| (i) Information | 3/22/2015 11:18:52 AM | Microsoft Windows security a... | 4647 Logoff |

- Event ID 4608: Windows Is Starting Up

| Event ID: 4608 (8) | | | |
|--------------------|-----------------------|---------------------------------|----------------------------|
| (i) Information | 3/24/2015 9:21:29 AM | Microsoft Windows security a... | 4608 Security State Change |
| (i) Information | 3/23/2015 1:24:23 PM | Microsoft Windows security a... | 4608 Security State Change |
| (i) Information | 3/25/2015 9:05:41 AM | Microsoft Windows security a... | 4608 Security State Change |
| (i) Information | 3/22/2015 10:51:14 AM | Microsoft Windows security a... | 4608 Security State Change |
| (i) Information | 3/25/2015 6:19:26 AM | Microsoft Windows security a... | 4608 Security State Change |
| (i) Information | 3/25/2015 6:15:35 AM | Microsoft Windows security a... | 4608 Security State Change |
| (i) Information | 3/22/2015 11:43:36 AM | Microsoft Windows security a... | 4608 Security State Change |
| (i) Information | 3/22/2015 11:22:31 AM | Microsoft Windows security a... | 4608 Security State Change |

13. What web browsers were used?

Answer: The web browsers used were “Google Chrome” and “Internet Explorer”

Path for Chrome: Data_Leak\cfreds_2015_data_leakage_pc\Program Files (x86)\Google\Chrome\Application\chrome.exe

Evidence:

| | Name |
|---|----------------------------|
| 1 | 41.0.2272.101 |
| 2 | VisualElementsManifest.xml |
| 3 | chrome.exe |

Path for Internet Explore: Data_Leak\cfreds_2015_data_leakage_pc\Program Files (x86)\Internet Explorer\iexplore.exe

Evidence:

| | Name |
|----|------------------------------|
| 25 | F12Tools.dll:\$TFX_DATA |
| 26 | ieinstal.exe:\$TFX_DATA |
| 27 | ieinstal.exe |
| 28 | IESHims.dll:\$TFX_DATA |
| 29 | IESHims.dll |
| 30 | ie9props.propdesc:\$TFX_DATA |
| 31 | ie9props.propdesc |
| 32 | sqmapi.dll |
| 33 | sqmapi.dll:\$TFX_DATA |
| 34 | iexplore.exe |
| 35 | iexplore.exe:\$TFX_DATA |

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

Answer:

➤ **Google Chrome:**

| Serial Number | Artifact Name | Path |
|---------------|------------------------|--|
| 1 | History | Data_Leak\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Google\Chrome\User Data\Default\History |
| 2 | Cookies | Data_Leak\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Cookies |
| 3 | Cookies | Data_Leak\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Google\Chrome\User Data\Default\ Cookies |
| 4 | Last Tabs | Data_Leak\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Last Tabs |
| 5 | Current Tabs | Data_Leak\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Current Tabs |
| 6 | Visited Links | Data_Leak\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Visited Links |
| 7 | Cache | Data_Leak\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Cache |
| 8 | GPU Cache | Data_Leak\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Google\Chrome\User Data\Default\GPUCache |
| 9 | History Provider Cache | Data_Leak\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache |

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

Answer: This data has been taken from the history.db file from the google chrome folder located in:

Data_Leak\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Google\Chrome\User Data\Default\History.db for google chrome and from the History.IE5 file of internet explorer:

Data_Leak\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012015031620150323

| URL | Browser |
|--|---|
| http://windows.microsoft.com/en-us/internet-explorer/ie-11-worldwide-languages | Download Internet Explorer 11 (Offline installer) - Internet Explorer |
| https://www.google.com/chrome/browser/thankyou.html?brand=CHNG&platform=win&clickonceinstalled=1 | Chrome Browser |
| https://www.google.com/search?hl=en&source=hp&q=internet+explorer+11&gbv=2&oq=internet+explorer+11&gs_l=heirloom-hp..0l10.5163.7893.0.9562.20.13.0.7.0.156.1110.11j2.13.0.msedr...0...1ac.1.34.heirloom-hp..0.20.1250.5j7Xm44tv5w | internet explorer 11 - Google Search |
| http://www.msn.com/?ocid=iehp | msn |
| http://windows.microsoft.com/en-us/internet-explorer/download-ie | Download Web Browser - Internet Explorer |
| http://windows.microsoft.com/en-US/internet-explorer/products/ie-8/welcome | |
| http://go.microsoft.com/fwlink/?LinkID=121792 | |
| http://windows.microsoft.com/en-us/internet-explorer/ie-8>Welcome | Your browser has been upgraded - Microsoft Windows |

| | |
|---|--|
| https://www.google.com/?gws_rd=ssl | Google |
| 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 | |
| https://www.google.com/webhp?hl=en | Google |
| https://www.google.com/chrome/index.html?hl=en&brand=CHNG&utm_source=en-hpp&utm_medium=hpp&utm_campaign=en | Chrome |
| http://go.microsoft.com/fwlink/?LinkId=69157 | |
| http://tools.google.com/chrome/intl/en/welcome.html | Getting Started |
| https://www.google.com/intl/en/chrome/browser/welcome.html | Getting Started |
| https://www.google.com/ | Google |
| http://www.bing.com/ | Bing |
| https://www.google.com/#q=outlook+2013+settings | Google |
| https://support.office.com/en-nz/article/Set-up-email-in-Outlook-2010-or-Outlook-2013-for-Office-365-or-Exchange-based-accounts-6e27792a-9267-4aa4-8bb6-c84ef146101b | Set up email in Outlook 2010 or Outlook 2013 for Office 365 or Exchange-based accounts |
| https://www.google.com/webhp?hl=en#q=Emmy+Noether&oi=ddle&ct=emmy-noethers-133rd-birthday-5681045017985024-hp&hl=en | Emmy Noether - Google Search |
| https://www.google.com/webhp?hl=en#hl=en&q=data+leakage+methods | data leakage methods - Google Search |
| http://www.sans.org/reading-room/whitepapers/awareness/data-leakage-threats-mitigation_1931 | |
| http://www.sans.org/reading-room/whitepapers/awareness/data-leakage-threats-mitigation-1931 | |

| | |
|---|--|
| https://www.google.com/webhp?hl=en#hl=en&q=leaking+confidential+information | leaking confidential information - Google Search |
| https://www.google.com/webhp?hl=en#q=leaking+confidential+information&hl=en&start=10 | |
| https://www.google.com/webhp?hl=en#q=leaking+confidential+information&hl=en&start=20 | |
| https://www.google.com/webhp?hl=en#hl=en&q=information+leakage+cases | information leakage cases - Google Search |
| http://www.emirates247.com/business/technology/top-5-sources-leaking-personal-data-2015-03-13-1.584027 | Top 5 sources leaking personal data - Emirates 24 7 |
| https://www.google.com/webhp?hl=en#q=information+leakage+cases&hl=en | |
| https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&site=webhp&source=lnms&tbo=isch&sa=X&ei=21UQVb20Eu-HsQTJ5IDAAQ&ved=0CAgQ_AUoAw | information leakage cases - Google Search |
| https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&site=webhp&tbo=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1 | information leakage cases - Google Search |
| https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&site=webhp&tbo=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#q=information+leakage+cases&hl=en | intellectual property theft - Google Search |
| http://www.mediapost.com/publications/article/205047/google-to-settle-data-leakage-case-for-85-mill.html?edition= | Google To Settle 'Data Leakage' Case For \$8.5 Million 07/23/2013 |
| https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&site=webhp&tbo=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1 | how to leak a secret - Google Search |

| | |
|---|--|
| UQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=intellectual+property+theft | |
| http://www.fbi.gov/about-us/investigate/white_collar/ipr/ipr | FBI â€“ Intellectual Property Theft |
| http://en.wikipedia.org/wiki/Intellectual_property | Intellectual property - Wikipedia, the free encyclopedia |
| https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&site=webhp&tbo=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=how+to+leak+a+secret | cloud storage - Google Search |
| http://research.microsoft.com/en-us/um/people/yael/publications/2001-leak_secret.pdf | |
| https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&site=webhp&tbo=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=cloud+storage | |
| http://en.wikipedia.org/wiki/Cloud_storage | Cloud storage - Wikipedia, the free encyclopedia |
| http://www.pcadvisor.co.uk/test-centre/internet/3506734/best-cloud-storage-dropbox-google-drive-onedrive-icloud/ | 7 best cloud storage services 2015: Dropbox vs Google Drive - PC Advisor |
| https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&site=webhp&tbo=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=digital+forensics | digital forensics - Google Search |
| http://en.wikipedia.org/wiki/Digital_forensics | Digital forensics - Wikipedia, the |

| | |
|---|---|
| | free encyclopedia |
| http://nij.gov/topics/forensics/evidence/digital/pages/welcome.aspx | Digital Evidence and Forensics National Institute of Justice |
| http://nij.gov/Pages/PageNotFoundError.aspx?requestUrl=http://nij.gov/topics/forensics/evidence/digital/standards/pages/welcome.aspx | NIJ Home Page Page not found (404 Error) |
| http://nij.gov/topics/forensics/evidence/digital/analysis/pages/welcome.aspx | Digital Evidence Analysis Tools National Institute of Justice |
| https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&site=webhp&tbs=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=how+to+delete+data | how to delete data - Google Search |
| https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&site=webhp&tbs=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=anti-forensics | anti-forensics - Google Search |
| http://forensicswiki.org/wiki/Anti-forensic_techniques | Anti-forensic techniques - ForensicsWiki |
| https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&site=webhp&tbs=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=how+to+recover+data | how to recover data - Google Search |
| https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&site=webhp&tbs=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=data+recovery+tools | information leakage cases - Google Search |
| http://en.wikipedia.org/wiki/List_of_data_recovery_software | List of data recovery |

| | |
|---|--|
| | software - Wikipedia, the free encyclopedia |
| http://www.forensicswiki.org/wiki/Tools:Data_Recovery | Tools:Data Recovery - ForensicsWiki |
| https://www.google.com/webhp?hl=en#hl=en&q=google | |
| https://www.google.com/webhp?hl=en#hl=en&q=apple+icloud | apple icloud - Google Search |
| https://www.apple.com/icloud/ | Apple - iCloud - Everything you love, everywhere you go. |
| https://www.apple.com/icloud/setup/pc.html | Apple - iCloud - Learn how to set up iCloud on all your devices. |
| http://support.apple.com/kb/DL1455?locale=en_US | iCloud for Windows |
| https://support.apple.com/kb/DL1455?locale=en_US | iCloud for Windows |
| https://www.google.com/webhp?hl=en#hl=en&q=google+drive | google drive - Google Search |
| https://www.google.com/drive/ | Google Drive - Cloud Storage & File Backup for Photos, Docs & More |
| https://www.google.com/drive/download/ | Download Google Drive - Free Cloud Storage |

| | |
|---|--|
| https://tools.google.com/dlpage/drive/index.html?hl=en#eula | Download Google Drive Now â€“ For Free |
| https://tools.google.com/dlpage/drive/thankyou.html?hl=en | Google Drive |
| https://news.google.com/nwshp?hl=en&tab=wn&ei=xnARVdWfPPLjsASdgIKoAw&ved=0CAUQqS4oBQ | Google News |
| https://news.google.com/news/section?pz=1&cf=all&ned=us&topic=w&siidp=0b2226a6a5dab3b27ee85fc5e8d21f28f01e | World |
| https://news.google.com/news/section?pz=1&cf=all&ned=us&topic=t&siidp=e6116f8175cb189b8dd7fd58ef6bc922ec04 | Technology |
| https://news.google.com/news?pz=1&cf=all&ned=us&siidp=0c33ef04190b3734a22c5bae18801ff1041e | Google News |
| http://www.cbsnews.com/news/germanwings-flight-9525-pulverized-plane-parts-rough-mountain-terrain/ | Germanwings Flight 9525: "Everything is pulverized" - CBS News |
| https://news.google.com/news/section?pz=1&cf=all&ned=us&topic=w&siidp=538c61c825aba06be7485be747a619778015 | World |
| https://news.google.com/news?pz=1&cf=all&ned=us&siidp=f206159a77e2be8861b5231ddc055443b303 | Google News |
| https://news.google.com/news/section?pz=1&cf=all&ned=us&topic=s&siidp=545d9217fe5452fcfbce251400793f398ac | Sports |
| https://news.google.com/news?pz=1&hl=en&tab=nn | Google News |
| https://www.google.com/#q=security+checkpoint+cd-r | security checkpoint cd-r - Google Search |

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

Answer:

17. List all user keywords at the search bar in Windows Explorer. (Timestamp, Keyword)

Answer: In this screenshot, we can see the **WordWheelQuery** registry key located under Software\Microsoft\Windows\CurrentVersion\Explorer in the NTUSER.DAT file. This registry key records the search terms that a user has entered in the Windows Explorer search bar, which is a valuable source of information for digital forensics investigators to trace user search activity on a system.

Key Observations:

- Registry Path:** The path in the registry, Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery, is where Windows stores recent search entries.
- Search Keyword:** Under WordWheelQuery\0, the keyword secret appears, which indicates that the user searched for "secret" in Windows Explorer.
- Timestamp:** There is a timestamp field that shows 03/18/70 09:40:51 AM. However, this date seems invalid or corrupted, likely due to issues in recording or interpreting the timestamp data. Some forensic tools may not accurately parse timestamps from certain registry entries, or it could indicate that no timestamp was associated with this search term.
- Hex View:** The hex representation at the bottom shows the ASCII characters for "secret," which confirms the stored search keyword.

| Name | Value |
|-------------------------------|----------------------|
| High ASCII | secret |
| Unicode | secret |
| Unix Date (Time/Date) | 03/18/70 09:40:51 AM |
| Windows Date/Time (Time/Date) | Invalid |

18. What application was used for e-mail communication?

Answer: The application used for e-mail communication is “Microsoft Outlook.” The **default** registry key within the **SOFTWARE** registry hive specifies the default email client for the user. The Default value here, within this key contains the name of the email program “Microsoft Outlook”.

Path:

Data_Leak\cfreds_2015_data_leakage_pc\Windows\System32\config\SOFTWARE\CMSI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\Clients\Mail\Microsoft Outlook\Default

Evidence:

| Name | True Path |
|-------------------|---|
| 1 Protocols | Data_Leak\cfreds_2015_data_leakage_pc\Windows\System32\config\SOFTWARE\CMSI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A6...} |
| 2 InstallInfo | Data_Leak\cfreds_2015_data_leakage_pc\Windows\System32\config\SOFTWARE\CMSI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A6...} |
| 3 Envelope | Data_Leak\cfreds_2015_data_leakage_pc\Windows\System32\config\SOFTWARE\CMSI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A6...} |
| 4 shell | Data_Leak\cfreds_2015_data_leakage_pc\Windows\System32\config\SOFTWARE\CMSI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A6...} |
| 5 MSIInstallOnWTS | Data_Leak\cfreds_2015_data_leakage_pc\Windows\System32\config\SOFTWARE\CMSI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A6...} |
| 6 DLLPath | Data_Leak\cfreds_2015_data_leakage_pc\Windows\System32\config\SOFTWARE\CMSI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A6...} |
| 7 MSIOfficeLCID | Data_Leak\cfreds_2015_data_leakage_pc\Windows\System32\config\SOFTWARE\CMSI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A6...} |
| 8 MSIComponentID | Data_Leak\cfreds_2015_data_leakage_pc\Windows\System32\config\SOFTWARE\CMSI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A6...} |
| 9 DLLPathEx | Data_Leak\cfreds_2015_data_leakage_pc\Windows\System32\config\SOFTWARE\CMSI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A6...} |
| 10 SupportUTF8 | Data_Leak\cfreds_2015_data_leakage_pc\Windows\System32\config\SOFTWARE\CMSI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A6...} |
| 11 (Default) | Data_Leak\cfreds_2015_data_leakage_pc\Windows\System32\config\SOFTWARE\CMSI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A6...} |

Outlook is also the default email application in the user profile of the suspect (informant). The file path is of the registry key that stores the name of the default Outlook profile for the user on a Windows system.

Path: Data_Leak\cfreds_2015_data_leakage_pc\Users\informant\NTUSER.DAT\CMSI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft\Office\15.0\Outlook\DefaultProfile

Evidence:

| Name | Value |
|-------------------------------|----------------------|
| High ASCII | Outlook |
| Unicode | Outlook |
| Unix Date (Time/Date) | 03/21/70 10:29:17 AM |
| Windows Date/Time (Time/Date) | Invalid |

19. Where is the e-mail file located?

Answer: The file is located at

C:\Users\informant\AppData\Local\Microsoft\Office\iaman.informant@nist.gov.ost

This path points to an OST file, which stands for Offline Storage Table. OST files are utilized by Microsoft Outlook to store a synchronized copy of mailbox data from an Exchange server or other IMAP account. This allows users to access their emails and other Outlook data even when they are offline.

The identified path was extracted from the **LastCorruptStore** registry key within the user's NTUSER.DAT hive. This registry key serves the purpose of storing the location of the last Outlook data file that encountered corruption errors. In this specific instance, the value associated with the LastCorruptStore key indicates that the corrupted file is an OST file named "**iaman.informant@nist.gov.ost**". This file resides within the user's Outlook profile directory.

Path: Data_Leak\cfreds_2015_data_leakage_pc\D\Users\informant\NTUSER.DAT\CMSI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft\Office\15.0\Outlook\PST\LastCorruptStore

Evidence:

The screenshot shows the EnCase Forensic software interface with the following details:

- Left pane (File Tree):** Shows the structure of the NTUSER.DAT hive, including categories like Options, Perf, Profiles, PST, Resiliency, Search, Catalog, and Security.
- Middle pane (Table View):** A table titled "Table" with columns "Name" and "True Path". It shows one entry: "LastCorruptStore" with the value "Data_Leak\cfreds_2015_data_leakage_pc\D\Users\informant\NTUSER.DAT\CMSI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft\Office\15.0\Outlook\PST\LastCorruptStore".
- Bottom pane (Hex and ASCII View):** Displays the raw hex and ASCII data for the registry key "LastCorruptStore". The ASCII view shows the string "iaman.informant@nist.gov.ost".
- Bottom right pane (Properties View):** A table showing properties of the registry key:

| Name | Value |
|-------------------------------|--|
| High ASCII | C:\Users\informant\AppData\Local\Microsoft\Outlook\iaman.informa |
| Unicode | C:\Users\informant\AppData\Local\Microsoft\Outlook\iaman.informa |
| Unix Date (Time/Date) | 02/13/70 06:52:35 PM |
| Windows Date/Time (Time/Da... | Invalid |
| HFS Plus Date (Time/Date) | 09/20/75 09:13:36 AM |
| DOS Date (DOS Date) | 01/26/80 12:02:06 AM |
| 32-bit Integer (UInt32) | 3801155 |
| 32-bit Integer (Int32) | 3801155 |

20. What was the e-mail account used by the suspect?

Answer: The email account used by the suspect is iaman.informant@nist.gov.

An **Offline Storage Table (OST) file** is an offline copy of a user's mailbox from Microsoft Outlook, allowing access to emails, calendar events, and other data without an internet connection. The naming conventions for OST files depend on the version of Microsoft Outlook and the settings configured by the user or administrator. Here's how they are typically named:

Default Naming Convention: By default, the OST file is named as the **user's email address** or **mailbox alias**. For example, if the email address is user@example.com, the OST file might be named user@example.com.ost.

The file is located at

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

| Name | Last Written |
|---|---|
| fc39fbc8c85bcb43816b40b7d4c72f22 - Autodiscover.xml | 03/25/15 10:41:36 AM (-4:00 Eastern Daylight Time) |
| iaman.informant@nist.gov.ost | 03/25/15 11:11:47 AM (-4:00 Eastern Daylight Time) |
| mapisvc.inf | 03/25/15 10:41:03 AM (-4:00 Eastern Daylight Time) |
| Offline Address Books | 03/22/15 11:50:21 AM (-4:00 Eastern Daylight Time) |
| RoamCache | 03/23/15 03:29:29 PM (-4:00 Eastern Daylight Time) |
| -iaman.informant@nist.gov.ost.tmp | 03/25/15 10:41:04 AM (-4:00 Eastern Daylight Time) |

21. List all e-mails of the suspect. If possible, identify deleted e-mails.

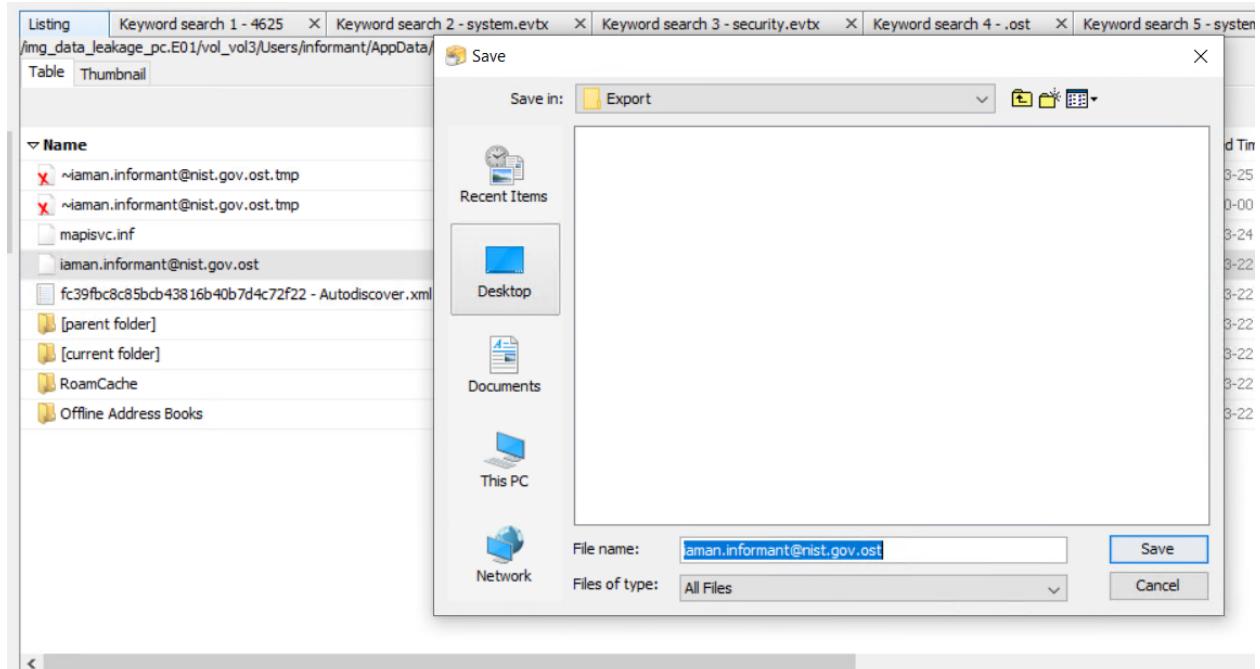
(You can identify the following items: *Timestamp, From, To, Subject, Body, and Attachment*)

[Hint: just examine the OST file only.]

Answer: To analyse the E-mail data like sent emails, deleted emails and inbox, firstly I extracted the OST file and then converted the OST file into a PST file using a tool called **“Kernel for OST to PST - Evaluation Version.”** OST files are designed to work with Exchange Server or IMAP accounts, allowing offline access to mailboxes. They function as synchronized copies of the server data. However, OST files are intrinsically linked to the original profile and Exchange server they were created on. This means you can't simply open an OST file on a different computer or in a different Outlook profile.

Converting OST to PST creates a portable, independent copy of the mailbox data. PST files (Personal Storage Table) are not tied to a specific profile or server, making them accessible on any computer with Outlook. This conversion becomes essential when:

- **Migrating data:** Moving mailboxes to a new computer, profile, or email system.
- **Backing up data:** Creating a standalone backup of the mailbox.
- **Recovering from corruption:** If the OST file is corrupted, converting it to PST can sometimes salvage the data.
- **Accessing data without Exchange:** Viewing OST content when the Exchange server is unavailable, or the user is no longer connected to it.
- The file is located at
Data_Leak\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Microsoft\Outlook\iaman.informant@nist.gov.ost



➤ Inbox emails(6):

The screenshot shows a mail client interface with a folder list on the left and an inbox on the right.

Folder List:

- Root - Mailbox
 - ~MAPISP(Internal)
 - Common Views
 - Drizzle
 - Finder
- IPM_SUBTREE
 - Calendar
 - Contacts
 - Conversation Action Settings
 - Deleted Items**
 - Drafts
 - Inbox
 - Journal
 - Junk Email
 - Notes
 - Outbox
 - Quick Step Settings
 - RSS Feeds
 - Sent Items
 - SmsAndChatsSync
 - Sync Issues
 - Conflicts
 - Local Failures
 - Server Failures
- Root - Public
- NON_IPM_SUBTREE
- EFORMS REGISTRY
 - Organization Forms

| From | Subject | Date/Time | Lost/Deleted |
|--------------------------------|----------------------|-------------------------|--------------|
| <FILTER> | <FILTER> | <FILTER> | <FILTER> |
| spy <spy.conspirator@nist.gov> | Hello, iaman | Mon 03/23/2015 12:29 PM | Existing |
| spy <spy.conspirator@nist.gov> | Good job, buddy. | Mon 03/23/2015 14:15 PM | Existing |
| spy <spy.conspirator@nist.gov> | RE: Good job, buddy. | Mon 03/23/2015 14:20 PM | Existing |
| spy <spy.conspirator@nist.gov> | Important request | Mon 03/23/2015 14:26 PM | Existing |
| spy <spy.conspirator@nist.gov> | Last request | Tue 03/24/2015 08:25 AM | Existing |
| spy <spy.conspirator@nist.gov> | Watch out! | Tue 03/24/2015 14:32 PM | Lost/Deleted |

Simple View Advanced Properties View

Hello, iaman
spy <spy.conspirator@nist.gov>
To: iaman <iaman.informant@nist.gov>

How are you doing?

➤ Deleted Emails(7):

The screenshot shows a mail client interface with a folder list on the left and a deleted items list on the right.

Folder List:

- Root - Mailbox
 - ~MAPISP(Internal)
 - Common Views
 - Drizzle
 - Finder
- IPM_SUBTREE
 - Calendar
 - Contacts
 - Conversation Action Settings
 - Deleted Items**
 - Drafts
 - Inbox
 - Journal
 - Junk Email
 - Notes
 - Outbox
 - Quick Step Settings
 - RSS Feeds
 - Sent Items
 - SmsAndChatsSync
 - Sync Issues
 - Conflicts
 - Local Failures
 - Server Failures
 - Tasks
 - Working Set
 - Shared Data
 - Shortcuts
 - Views
- Root - Public
- NON_IPM_SUBTREE
- EFORMS REGISTRY
 - Organization Forms

| From | Subject | Date/Time | Lost/Deleted |
|--------------------------------|---------------------|-------------------------|--------------|
| <FILTER> | <FILTER> | <FILTER> | <FILTER> |
| spy <spy.conspirator@nist.gov> | RE: It's me | Mon 03/23/2015 15:41 PM | Existing |
| iaman | RE: Last request | Tue 03/24/2015 08:35 AM | Existing |
| iaman | RE: Watch out! | Tue 03/24/2015 14:34 PM | Existing |
| iaman | Done | Tue 03/24/2015 16:05 PM | Existing |
| spy <spy.conspirator@nist.gov> | RE: Last request | Tue 03/24/2015 08:30 AM | Lost/Deleted |
| spy <spy.conspirator@nist.gov> | Watch out! | Tue 03/24/2015 14:32 PM | Lost/Deleted |
| iilan | RE: Good job, buddy | Mon 03/23/2015 14:19 PM | Lost/Deleted |

Simple View Advanced Properties View

RE: It's me
spy <spy.conspirator@nist.gov>
To: iaman <iaman.informant@nist.gov>

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/0Bz0ye6gXtiZaVl8yVU5mWHGbWc/view?usp=sharing>

<https://drive.google.com/file/d/0Bz0ye6gXtaakx6d3R3c0JmM1U/view?usp=sharing>

➤ Sent emails(3):

Sent Items (3)

| From | Subject | Date/Time | Lost/Deleted |
|----------|-----------------------|-------------------------|--------------|
| <FILTER> | <FILTER> | <FILTER> | <FILTER> |
| iaman | RE: Hello, iaman | Mon 03/23/2015 13:44 PM | Existing |
| iaman | RE: Important request | Mon 03/23/2015 14:27 PM | Existing |
| iaman | It's me | Mon 03/23/2015 15:38 PM | Lost/Deleted |

RE: Hello, iaman
iaman
To: spy<spy.conspirator@nist.gov>

Successfully secured.

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

How are you doing?

| Timestamp | Source | From | To | Subject | Body |
|---------------------|------------|--------------------------|--------------------------|-------------------------|---|
| 23-03-2015 13:29 | Inbox | spy.conspirator@nist.gov | iaman.informant@nist.gov | Hello, laman | How are you doing? |
| 23-03-2015 14:44 | Sent Items | iaman.informant@nist.gov | spy.conspirator@nist.gov | RE: Hello, laman | RE: Hello, laman |
| 23-03-2015 15:14 | Inbox | spy.conspirator@nist.gov | iaman.informant@nist.gov | Good job, buddy. | Good, job. I need a more detailed data about this business. |
| 23-03-2015 15:20 | Inbox | spy.conspirator@nist.gov | iaman.informant@nist.gov | RE: Good job, buddy. | 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. |
| 23-03-2015 15:26 | Inbox | spy.conspirator@nist.gov | iaman.informant@nist.gov | Important request | I confirmed it. But I need a more data. Do your best. |

| | | | | | |
|---------------------|---------------|--------------------------|--------------------------|-----------------------|--|
| | | | | | 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. |
| 23-03-2015 15:27 | Sent Items | iaman.informant@nist.gov | spy.conspirator@nist.gov | RE: Important request | Use links below, https://drive.google.com/file/d/0Bz0ye6gXtiZaVl8yVU5mWHIGbWc/view?usp=sharing https://drive.google.com/file/d/0Bz0ye6gXtiZaakx6d3R3c0JmM1U/view?usp=sharing |
| 23-03-2015 16:38 | Deleted Items | iaman.informant@nist.gov | spy.conspirator@nist.gov | It's me | 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/0Bz0ye6gXtiZaVl8yVU5mWHIGbWc/view?usp=sharing |
| | | | | | https://drive.google.com/file/d/0Bz0ye6gXtiZaakx6d3R3c0JmM1U/view?usp=sharing |
| 24-03-2015 09:25 | Inbox | spy.conspirator@nist.gov | iaman.informant@nist.gov | Last request | <p>This is the last request.</p> <p>I want to get the remaining data.</p> |
| | | | | | <p>This is the last time..</p> <p>-----</p> <p>From: spy</p> <p>Sent: Tuesday, March 24, 2015 9:34 AM</p> <p>To: iaman</p> <p>Subject: RE: Last request</p> <p>No problem.</p> <p>U can directly deliver storage devices that stored it.</p> <p>-----</p> <p>From: iaman</p> <p>Sent: Tuesday, March 24, 2015 9:30 AM</p> <p>To: spy</p> <p>Subject: RE: Last request</p> <p>Stop it!</p> |

| | | | | | |
|---------------------|---------------|--------------------------|--------------------------|----------------|---|
| | | | | | <p>It is very hard to transfer all data over the internet!</p> <p>-----</p> <p>From: spy</p> <p>Sent: Tuesday, March 24, 2015 9:26 AM</p> <p>To: iaman</p> <p>Subject: Last request</p> <p>This is the last request.</p> <p>I want to get the remaining data.</p> |
| 24-03-2015 15:34 | Deleted Items | iaman.informant@nist.gov | spy.conspirator@nist.gov | RE: Watch out! | <p>I am trying.</p> <p>-----</p> <p>From: spy</p> <p>Sent: Tuesday, March 24, 2015 3:33 PM</p> <p>To: iaman</p> <p>Subject: Watch out!</p> <p>USB device may be easily detected.</p> <p>So, try another method.</p> |
| 24-03-2015 17:05 | Deleted Items | iaman.informant@nist.gov | spy.conspirator@nist.gov | Done | It's done. See you tomorrow. |

22. List external storage devices attached to PC.

Answer: There are 2 connected external devices to the PC having name “**SanDisk Cruzer Fit USB Device**” and serial number: “**4C530012450531101593&0**” and “**4C530012550531106501&0**”

| | Target | Serial # | Device | Friendly Name | Vendor | Product |
|------|-----------------------------|------------------------|-------------------------------|-------------------------------|---------|------------|
| □ 1 | cfreds_2015_data_leakage_pc | 4C530012450531101593&0 | SanDisk Cruzer Fit USB Device | SanDisk Cruzer Fit USB Device | SanDisk | Cruzer_Fit |
| □ 2 | cfreds_2015_data_leakage_pc | 4C530012450531101593&0 | SanDisk Cruzer Fit USB Device | SanDisk Cruzer Fit USB Device | SanDisk | Cruzer_Fit |
| □ 3 | cfreds_2015_data_leakage_pc | 4C530012450531101593&0 | SanDisk Cruzer Fit USB Device | SanDisk Cruzer Fit USB Device | SanDisk | Cruzer_Fit |
| □ 4 | cfreds_2015_data_leakage_pc | 4C530012450531101593&0 | SanDisk Cruzer Fit USB Device | SanDisk Cruzer Fit USB Device | SanDisk | Cruzer_Fit |
| □ 5 | cfreds_2015_data_leakage_pc | 4C530012450531101593&0 | SanDisk Cruzer Fit USB Device | SanDisk Cruzer Fit USB Device | SanDisk | Cruzer_Fit |
| □ 6 | cfreds_2015_data_leakage_pc | 4C530012450531101593&0 | SanDisk Cruzer Fit USB Device | SanDisk Cruzer Fit USB Device | SanDisk | Cruzer_Fit |
| □ 7 | cfreds_2015_data_leakage_pc | 4C530012550531106501&0 | SanDisk Cruzer Fit USB Device | SanDisk Cruzer Fit USB Device | SanDisk | Cruzer_Fit |
| □ 8 | cfreds_2015_data_leakage_pc | 4C530012550531106501&0 | SanDisk Cruzer Fit USB Device | SanDisk Cruzer Fit USB Device | SanDisk | Cruzer_Fit |
| □ 9 | cfreds_2015_data_leakage_pc | 4C530012550531106501&0 | SanDisk Cruzer Fit USB Device | SanDisk Cruzer Fit USB Device | SanDisk | Cruzer_Fit |
| □ 10 | cfreds_2015_data_leakage_pc | 4C530012550531106501&0 | SanDisk Cruzer Fit USB Device | SanDisk Cruzer Fit USB Device | SanDisk | Cruzer_Fit |
| □ 11 | cfreds_2015_data_leakage_pc | 4C530012550531106501&0 | SanDisk Cruzer Fit USB Device | SanDisk Cruzer Fit USB Device | SanDisk | Cruzer_Fit |
| □ 12 | cfreds_2015_data_leakage_pc | 4C530012550531106501&0 | SanDisk Cruzer Fit USB Device | SanDisk Cruzer Fit USB Device | SanDisk | Cruzer_Fit |

Path:

Data_Leak\cfreds_2015_data_leakage_pc\D\Windows\System32\config\SYSTEM\CMSI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}\ControlSet001\Enum\USBSTOR\Disk&Ven_SanDisk&Prod_Cruzer_Fit&Rev_2.01\4C530012450531101593&0

The screenshot shows the EnCase Evidence Analyzer interface. The top navigation bar includes tabs for Processor Manager, Artifacts, Evidence, and Case Analyzer. Below the tabs, there are buttons for View: SYSTEM, Bookmark, Go to file, Tags, and Find Related.

The left pane displays a tree view of registry keys under the SYSTEM hive:

- PCI
- PCIIDE
- Root
- SCSI
- STORAGE
- SW
- UMB
- USB
- USBSTOR
- Disk&Ven_SanDisk&Prod_Cruzer_Fit&Rev_2.01 (selected)
- 4C530012450531101593&0
- 4C530012550531106501&0

The right pane contains a table titled "Table" with the following data:

| Name |
|--------------------------|
| 1 4C530012550531106501&0 |
| 2 4C530012450531101593&0 |

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: Initially extracted **\$UsnJrnl** and then converted it into a csv file for analysis. For conversion, MFTECMd.exe tool was used. The **\$UsnJrnl** file in NTFS is a detailed log of file system changes, crucial for forensic investigations. It records actions like file creation, deletion, renaming, and modifications, aiding in data recovery, timeline reconstruction, and malware analysis. Each record includes timestamps, filenames, reasons for change, and other attributes. To identify renamed files, even with missing parent directories, investigators can filter the journal by date, identify "rename" events, and extract relevant information like filenames and timestamps.

Path: Data_Leak\cfreds_2015_data_leakage_pc\D\\$Extend\\$UsnJrnl\\$J

```
Command line: -f C:\Users\student\Desktop\$UsnJrnl\$J --csv C:\Users\student\Desktop\  

File type: UsnJournal  

Processed C:\Users\student\Desktop\$UsnJrnl\$J in 1.6720 seconds  

Usn entries found in C:\Users\student\Desktop\$UsnJrnl\$J: 317,137  

CSV output will be saved to C:\Users\student\Desktop\20241112034034_MFTECmd_\$J_Output.csv  

C:\Users\student\Documents>
```

The table mentioned below covers all the file rename activity conducted by the suspect between 2015-03-23 and 2015-03-24. It mentions about the change in name of the .docx, .pptx, .xlsx, .jpg, .png file along with the old name as well as new name.

| Name | Extension | Sequence Number | UpdateSequenceNumber | UpdateTimestamp | UpdateReasons |
|---|-----------|-----------------|----------------------|-----------------|---------------|
| Sample Table (Annual Report Timeless design).docx | .docx | 2 | 56190648 | 3/23/2015 | RenameOldName |

| | | | | | |
|---|-------|---|----------|-----------|---------------|
| TM02835272[[fn=Sample Table (Annual Report Timeless design)]] .docx | .docx | 2 | 56190808 | 3/23/2015 | RenameNewName |
| Cover Page (Annual Report Red and Black design).docx | .docx | 2 | 56191272 | 3/23/2015 | RenameOldName |
| TM02835264[[fn=Cover Page (Annual Report Red and Black design)]] .docx | .docx | 2 | 56191440 | 3/23/2015 | RenameNewName |
| Cover Page (Annual Report Timeless design).docx | .docx | 1 | 56193256 | 3/23/2015 | RenameOldName |
| TM02835265[[fn=Cover Page (Annual Report Timeless design)]] .docx | .docx | 1 | 56193416 | 3/23/2015 | RenameNewName |
| Text Sidebar (Annual Report Red and Black design).docx | .docx | 1 | 56193688 | 3/23/2015 | RenameOldName |
| TM02835233[[fn=Text Sidebar (Annual Report Red and Black design)]] .docx | .docx | 1 | 56193856 | 3/23/2015 | RenameNewName |
| Sample Table (Annual Report Red and Black design).docx | .docx | 1 | 56194832 | 3/23/2015 | RenameOldName |
| TM02835271[[fn=Sample Table (Annual Report Red and Black design)]] .docx | .docx | 1 | 56195000 | 3/23/2015 | RenameNewName |
| Cover Letter (Timeless design Resume).docx | .docx | 8 | 56195928 | 3/23/2015 | RenameOldName |
| TM02836362[[fn=Cover letter (Resume Timeless Design)]] .docx | .docx | 8 | 56196072 | 3/23/2015 | RenameNewName |
| Text Cover (Student Report Blue design).docx | .docx | 2 | 56199504 | 3/23/2015 | RenameOldName |
| TM02835232[[fn=Text Cover (Student Report Blue design)]] .docx | .docx | 2 | 56199656 | 3/23/2015 | RenameNewName |
| Cover Letter (Chronological resume Simple design).docx | .docx | 3 | 56202816 | 3/23/2015 | RenameOldName |
| TM02835266[[fn=Cover Letter (Chronological Resume Simple design)]] .docx | .docx | 3 | 56202984 | 3/23/2015 | RenameNewName |

| | | | | | |
|--|-------|---|----------|-----------|---------------|
| Cover with Logo (Annual Report Red and Black design).docx | .docx | 2 | 56204008 | 3/23/2015 | RenameOldName |
| TM02835267[[fn=Cover with Logo (Annual Report Red and Black design)]] .docx | .docx | 2 | 56204184 | 3/23/2015 | RenameNewName |
| Text Cover with TOC (Student Report Blue design).docx | .docx | 4 | 56206328 | 3/23/2015 | RenameOldName |
| TM02835231[[fn=Text Cover with TOC (Student Report Blue design)]] .docx | .docx | 4 | 56206496 | 3/23/2015 | RenameNewName |
| Photo Sidebar (Annual Report Red and Black design).docx | .docx | 2 | 56210448 | 3/23/2015 | RenameOldName |
| TM02835270[[fn=Photo Sidebar (Annual Report Red and Black design)]] .docx | .docx | 2 | 56210624 | 3/23/2015 | RenameNewName |
| Photo Cover with TOC (Student Report Blue design).docx | .docx | 3 | 56212696 | 3/23/2015 | RenameOldName |
| TM02835269[[fn=Photo Cover with TOC (Student Report blue design)]] .docx | .docx | 3 | 56212864 | 3/23/2015 | RenameNewName |
| Photo Cover (Student Report Blue design).docx | .docx | 2 | 56214952 | 3/23/2015 | RenameOldName |
| TM02835268[[fn=Photo Cover (Student Report Blue design)]] .docx | .docx | 2 | 56215104 | 3/23/2015 | RenameNewName |
| [secret_project]_detailed_proposal.docx | .docx | 4 | 56306184 | 3/23/2015 | RenameOldName |
| landscape.png | .png | 4 | 56306328 | 3/23/2015 | RenameNewName |
| [secret_project]_design_c_oncept.ppt | .ppt | 7 | 56307712 | 3/23/2015 | RenameOldName |
| space_and_earth.mp4 | .mp4 | 7 | 56307848 | 3/23/2015 | RenameNewName |
| googledrivesync.exe | .exe | 1 | 56434408 | 3/23/2015 | RenameNewName |
| icloudsetup.exe | .exe | 2 | 56437312 | 3/23/2015 | RenameNewName |

| | | | | | |
|---|-------|----|----------|-----------|---------------|
| (secret_project)_pricing_decision.xlsx | .xlsx | 7 | 58506640 | 3/23/2015 | RenameOldName |
| happy_holiday.jpg | .jpg | 7 | 58506776 | 3/23/2015 | RenameNewName |
| [secret_project]_final_meeting.pptx | .pptx | 5 | 58510288 | 3/23/2015 | RenameOldName |
| do_u_wanna_build_a_snow_man.mp3 | .mp3 | 5 | 58510424 | 3/23/2015 | RenameNewName |
| ~WRD0001.docx | .docx | 6 | 59583528 | 3/23/2015 | RenameNewName |
| ~WRD0003.docx | .docx | 7 | 59584688 | 3/23/2015 | RenameNewName |
| [secret_project]_detailed_design.pptx | .pptx | 18 | 59801680 | 3/24/2015 | RenameOldName |
| winter_whether_advisory.zip | .zip | 18 | 59801816 | 3/24/2015 | RenameNewName |
| [secret_project]_revised_points.ppt | .ppt | 6 | 59802408 | 3/24/2015 | RenameOldName |
| [secret_project]_design_concept.ppt | .ppt | 13 | 59803456 | 3/24/2015 | RenameOldName |
| space_and_earth.mp4 | .mp4 | 13 | 59803592 | 3/24/2015 | RenameNewName |
| [secret_project]_proposal.docx | .docx | 6 | 59804952 | 3/24/2015 | RenameOldName |
| [secret_project]_proposal.docx | .docx | 6 | 59805072 | 3/24/2015 | RenameNewName |
| space_and_earth.mp4 | .mp4 | 13 | 59805312 | 3/24/2015 | RenameOldName |
| space_and_earth.mp4 | .mp4 | 13 | 59805416 | 3/24/2015 | RenameNewName |
| winter_whether_advisory.zip | .zip | 18 | 59805984 | 3/24/2015 | RenameOldName |
| winter_whether_advisory.zip | .zip | 18 | 59806104 | 3/24/2015 | RenameNewName |
| [secret_project]_detailed_proposal.docx | .docx | 38 | 59806560 | 3/24/2015 | RenameOldName |
| [secret_project]_detailed_proposal.docx | .docx | 38 | 59806704 | 3/24/2015 | RenameNewName |
| [secret_project]_final_meeting.pptx | .pptx | 4 | 59814352 | 3/24/2015 | RenameOldName |
| do_u_wanna_build_a_snow_man.mp3 | .mp3 | 4 | 59814488 | 3/24/2015 | RenameNewName |
| (secret_project)_market_analysis.xlsx | .xlsx | 7 | 59814904 | 3/24/2015 | RenameOldName |
| new_years_day.jpg | .jpg | 7 | 59815040 | 3/24/2015 | RenameNewName |

| | | | | | |
|---|-------|----|----------|-----------|---------------|
| (secret_project)_market_shares.xls | .xls | 9 | 59815232 | 3/24/2015 | RenameOldName |
| (secret_project)_price_analysis_#1.xlsx | .xlsx | 8 | 59815536 | 3/24/2015 | RenameOldName |
| my_favorite_movies.7z | .7z | 8 | 59815680 | 3/24/2015 | RenameNewName |
| (secret_project)_price_analysis_#2.xls | .xls | 10 | 59815968 | 3/24/2015 | RenameOldName |
| (secret_project)_pricing_decision.xlsx | .xlsx | 14 | 59816312 | 3/24/2015 | RenameOldName |
| happy_holiday.jpg | .jpg | 14 | 59816448 | 3/24/2015 | RenameNewName |
| [secret_project]_progress_#1.docx | .docx | 4 | 59816880 | 3/24/2015 | RenameOldName |
| my_smartphone.png | .png | 4 | 59817008 | 3/24/2015 | RenameNewName |
| [secret_project]_progress_#2.docx | .docx | 6 | 59817984 | 3/24/2015 | RenameOldName |
| [secret_project]_progress_#3.doc | .doc | 3 | 59818320 | 3/24/2015 | RenameOldName |
| [secret_project]_detailed_proposal.docx | .docx | 38 | 59818624 | 3/24/2015 | RenameOldName |
| a_gift_from_you.gif | .gif | 38 | 59818768 | 3/24/2015 | RenameNewName |
| [secret_project]_proposal.docx | .docx | 6 | 59818976 | 3/24/2015 | RenameOldName |
| landscape.png | .png | 6 | 59819096 | 3/24/2015 | RenameNewName |
| [secret_project]_technical_review_#1.docx | .docx | 7 | 59819272 | 3/24/2015 | RenameOldName |
| [secret_project]_technical_review_#1.pptx | .pptx | 6 | 59819592 | 3/24/2015 | RenameOldName |
| [secret_project]_technical_review_#2.docx | .docx | 3 | 59819912 | 3/24/2015 | RenameOldName |
| [secret_project]_technical_review_#2.ppt | .ppt | 4 | 59823280 | 3/24/2015 | RenameOldName |
| [secret_project]_technical_review_#3.doc | .doc | 3 | 59823600 | 3/24/2015 | RenameOldName |
| [secret_project]_technical_review_#3.ppt | .ppt | 6 | 59823920 | 3/24/2015 | RenameOldName |
| Resignation_Letter_(laman_Informant).docx | .docx | 4 | 64188592 | 3/24/2015 | RenameOldName |
| Resignation_Letter_(laman_Informant).docx | .docx | 7 | 64203528 | 3/24/2015 | RenameOldName |
| Resignation_Letter_(laman_Informant).docx | .docx | 9 | 64212992 | 3/24/2015 | RenameOldName |

| | | | | | |
|--|-------|-----|----------|-----------|---------------|
| Resignation_Letter_(laman_Informant).docx | .docx | 8 | 64223992 | 3/24/2015 | RenameOldName |
| Chrysanthemum.jpg | .jpg | 285 | 64404640 | 3/24/2015 | RenameOldName |
| \$RKXD1U3.jpg | .jpg | 285 | 64404736 | 3/24/2015 | RenameNewName |
| Desert.jpg | .jpg | 10 | 64405352 | 3/24/2015 | RenameOldName |
| \$RI3FM2A.jpg | .jpg | 10 | 64405504 | 3/24/2015 | RenameNewName |
| Hydrangeas.jpg | .jpg | 10 | 64406824 | 3/24/2015 | RenameOldName |
| \$R508CBB.jpg | .jpg | 10 | 64406912 | 3/24/2015 | RenameNewName |
| IE11-Windows6.1-x64-en-us.exe | .exe | 7 | 64407528 | 3/24/2015 | RenameOldName |
| \$RJEMT64.exe | .exe | 7 | 64407648 | 3/24/2015 | RenameNewName |
| Jellyfish.jpg | .jpg | 8 | 64408264 | 3/24/2015 | RenameOldName |
| \$R8YP3XK.jpg | .jpg | 8 | 64408352 | 3/24/2015 | RenameNewName |
| Koala.jpg | .jpg | 10 | 64408968 | 3/24/2015 | RenameOldName |
| \$RU3FKWI.jpg | .jpg | 10 | 64409048 | 3/24/2015 | RenameNewName |
| Lighthouse.jpg | .jpg | 16 | 64409688 | 3/24/2015 | RenameOldName |
| \$RX538VH.jpg | .jpg | 16 | 64409776 | 3/24/2015 | RenameNewName |
| Penguins.jpg | .jpg | 12 | 64410392 | 3/24/2015 | RenameOldName |
| \$RFVCH5V.jpg | .jpg | 12 | 64410480 | 3/24/2015 | RenameNewName |
| Tulips.jpg | .jpg | 10 | 64411096 | 3/24/2015 | RenameOldName |
| \$RDOI3HE.jpg | .jpg | 10 | 64411176 | 3/24/2015 | RenameNewName |

Some of the entries in this table may be duplicated entries or from the recycled values.

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

Answer: The name of the shared user drive is "**10.11.11.128\secured_drive**"

Path: Data_Leak\cfreds_2015_data_leakage_pc\D\Users\informant\NTUSER.DAT\CMSI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU\b

- This file path points to a registry key that stores information about recently used Run commands for the user on a Windows system.

Evidence:

The screenshot shows the EnCase Forensic software interface. The left pane displays a tree view of registry keys under 'View: NTUSER.DAT'. One key, 'RunMRU\b', is expanded, showing three entries: 'a', 'b', and 'MRUL...'. The right pane contains two tables. The top table, titled 'True Path', lists the three entries with their full paths. The bottom table, titled 'Value', shows the details for entry 'b':

| Name | Value |
|-------------------------------|-------------------------------|
| High ASCII | \10.11.11.128\secured_drive\1 |
| Unicode | \10.11.11.128\secured_drive\1 |
| Unix Date (Time/Date) | 03/11/70 01:50:04 PM |
| Windows Date/Time (Time/Date) | Invalid |

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

Answer:

| Timestamp | Directory Path |
|---------------------|--|
| 2015-03-24 10:00:19 | E:\Secret Project Data\ |
| 2015-03-24 10:01:11 | E:\Secret Project Data\technical review\ |
| 2015-03-24 10:01:14 | E:\Secret Project Data\proposal\ |
| 2015-03-24 10:01:15 | E:\Secret Project Data\progress\ |
| 2015-03-24 10:01:17 | E:\Secret Project Data\pricing decision\ |
| 2015-03-24 10:01:29 | E:\Secret Project Data\design\ |
| 2015-03-24 16:54:07 | E:\Secret Project Data\ |
| 2015-03-24 16:54:07 | E:\Secret Project Data\progress\ |

- **Path:** Data_Leak\cfreds_2015_data_leakage_pc\%D\Users\informant\NTUSER.DAT\CMS-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft\Windows\Shell\BagMRU\0

| Name | Last Written |
|------|---|
| 3 5 | Data_Leak\cfreds_2015_data_leakage_pc\ |
| 4 5 | 03/23/15 04:24:35 PM (-4:00 Eastern Daylight Time) Data_Leak\cfreds_2015_data_leakage_pc\ |
| 5 4 | 03/23/15 04:24:33 PM (-4:00 Eastern Daylight Time) Data_Leak\cfreds_2015_data_leakage_pc\ |
| 6 4 | Data_Leak\cfreds_2015_data_leakage_pc\ |
| 7 3 | 03/23/15 04:24:29 PM (-4:00 Eastern Daylight Time) Data_Leak\cfreds_2015_data_leakage_pc\ |
| 8 3 | Data_Leak\cfreds_2015_data_leakage_pc\ |
| 9 2 | 03/23/15 04:24:22 PM (-4:00 Eastern Daylight Time) Data_Leak\cfreds_2015_data_leakage_pc\ |
| 10 2 | Data_Leak\cfreds_2015_data_leakage_pc\ |
| 11 1 | 03/23/15 04:24:19 PM (-4:00 Eastern Daylight Time) Data_Leak\cfreds_2015_data_leakage_pc\ |
| 12 1 | Data_Leak\cfreds_2015_data_leakage_pc\ |

This file path points to a registry key that stores **ShellBags** information for a specific user on a Windows system. These are registry entries that record information about user interactions with folders and files in Windows Explorer. They store details like folder paths, view settings, and timestamps while **0** represents a specific ShellBag entry within the BagMRU key.

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

Answer:

27. List all directories that were traversed in the company's network drive.

Answer: There were 3 parent directories that were traversed in the company's network drive. They were:

- I. **Secret Project Data** (03/23/15 04:28:17 PM (-4:00 Eastern Daylight Time))
- II. **Common Data** (03/23/15 04:24:07 PM (-4:00 Eastern Daylight Time))
- III. **Past Projects** (03/23/15 04:24:09 PM (-4:00 Eastern Daylight Time))

Path: Data_Leak\cfreds_2015_data_leakage_pc\D\Users\informant\NTUSER.DAT\CMS-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft\Windows\Shell\BagMRU\0\0\0

- This file path points to a registry key that stores **ShellBags** information for user on a Windows system. **ShellBags**: These are registry entries that record information about user interactions with folders and files in Windows Explorer. They store details like folder paths, view settings, and timestamps.
- **0\0\0** represents a specific ShellBag entry within the BagMRU key. Each number likely corresponds to a level in the folder hierarchy. BagMRU is a registry key that stores **ShellBags**, which are records of user interactions with folders in Windows Explorer

| Timestamp | Directory Path |
|---------------------|---|
| 2015-03-23 16:24:01 | \\\10.11.11.128\secured_drive\Common Data\ |
| 2015-03-23 16:24:08 | \\\10.11.11.128\secured_drive\Past Projects\ |
| 2015-03-23 16:24:12 | \\\10.11.11.128\secured_drive\Secret Project Data\design\ |
| 2015-03-23 16:24:15 | \\\10.11.11.128\secured_drive\Secret Project Data\pricing decision\ |
| 2015-03-23 16:24:16 | \\\10.11.11.128\secured_drive\Secret Project Data\final\ |
| 2015-03-23 16:24:18 | \\\10.11.11.128\secured_drive\Secret Project Data\technical review\ |
| 2015-03-23 16:24:20 | \\\10.11.11.128\secured_drive\Secret Project Data\proposal\ |
| 2015-03-23 16:24:27 | \\\10.11.11.128\secured_drive\Secret Project Data\progress\ |
| 2015-03-23 16:26:53 | \\\10.11.11.128\secured_drive\Secret Project Data\pricing decision\ |
| 2015-03-23 16:26:54 | \\\10.11.11.128\secured_drive\Secret Project Data\pricing decision\ |
| 2015-03-23 16:27:24 | V:\Secret Project Data\ |
| 2015-03-23 16:27:29 | V:\Secret Project Data\final\ |
| 2015-03-23 16:27:33 | V:\Secret Project Data\final\ |
| 2015-03-23 16:27:33 | V:\Secret Project Data\final\ |
| 2015-03-23 16:28:17 | \\\10.11.11.128\secured_drive\Secret Project Data\ |
| 2015-03-23 16:28:17 | \\\10.11.11.128\secured_drive\Secret Project Data\pricing decision\ |
| 2015-03-24 09:47:54 | \\\10.11.11.128\secured_drive\ |
| 2015-03-24 09:47:54 | \\\10.11.11.128\secured_drive\Past Projects\ |

The screenshot shows the Case Analyzer interface with the 'Case' tab selected. The left sidebar displays a tree view of reports categories: Reports, Accounts and Users, Drives Removable + Local, Drives Shared + Network, UNC Folders Visited, File Activity, Logfile, Documents, Explorer Typed Folders, File Browser History, Link Files, Multimedia, Recent Files, Hardware, and Internet Activity. The 'File Activity' section is expanded, showing a list of 21 items. The main pane lists these items in a table with columns: Target, Folder, User Name, Reg Key Last Modified, Network Share, and Re. Most entries are for 'informant' user and point to '\\10.11.11.128\secured_drive\Secret Project Data\pricing decision\[secret_project]_pricing_decision.xlsx'. Item 21 is for 'rfrds_2015_data_leakage_pc' and points to 'V:\Secret Project Data\final\[secret_project]_final_meeting.pptx'.

| | Target | Folder | User Name | Reg Key Last Modified | Network Share | Re |
|----|-----------------------------|---|-----------|--|---------------|----|
| 4 | 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 |
| 5 | 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 |
| 6 | 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 |
| 7 | 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 |
| 8 | 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 |
| 9 | 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 |
| 10 | 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 |
| 11 | 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 |
| 12 | 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 |
| 13 | 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 |
| 14 | 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 |
| 15 | 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 |
| 16 | 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 |
| 17 | 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 |
| 18 | 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 |
| 19 | 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 |
| 20 | 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 |
| 21 | rfrds_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 |

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

Answer: The files accessed were (secret_project)_pricing_decision.xlsx and [secret_project]_final_meeting.pptx. Here, V: is mapped on \\10.11.11.128. It means that the drive letter V: acts as a shortcut to the shared folder on the computer with the IP address **10.11.11.128**.

Path: Data_Leak\cfreds_2015_data_leakage_pc\D\Users\informant\NTUSER.DAT\CMS-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft\Office\15.0\Excel\File MRU\Item 1

| Timestamp | Directory Path |
|---------------------|--|
| 2015-03-23 16:26:53 | \\10.11.11.128\SECURED_DRIVE\Secret Project Data\pricing decision\[secret_project]_pricing_decision.xlsx |
| 2015-03-23 16:26:53 | \\10.11.11.128\SECURED_DRIVE\Secret Project Data\pricing decision\[secret_project]_pricing_decision.xlsx |
| 2015-03-23 16:26:53 | \\10.11.11.128\SECURED_DRIVE\Secret Project Data\pricing decision\[secret_project]_pricing_decision.xlsx |
| 2015-03-23 16:26:56 | \\10.11.11.128\secured_drive\Secret Project Data\pricing decision\[secret_project]_pricing_decision.xlsx |
| 2015-03-23 16:27:33 | V:\Secret Project Data\final\[secret_project]_final_meeting.pptx |
| 2015-03-23 16:27:33 | V:\Secret Project Data\final\[secret_project]_final_meeting.pptx |

| | |
|---------------------|---|
| 2015-03-23 16:27:37 | V:\Secret Project Data\final\[secret_project]_final_meeting.pptx |
| 2015-03-23 16:27:37 | V:\Secret Project Data\final\[secret_project]_final_meeting.pptx |

Evidence:

- Excel file

- **PowerPoint file:**

Data_Leak\cfreds_2015_data_leakage_pc\D\Users\informant\NTUSER.DAT\CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft\Office\15.0\PowerPoint\File MRU\Item 1

The screenshot shows the Encase Forensic software interface. On the left, a tree view displays the contents of the NTUSER.DAT file, including sections like MAPI, Microsoft Office 2013, Outlook, PowerPoint, File MRU, Change, First Run, Options, Place MRU, Security, and Registration. On the right, a table titled "Table" shows search results for "Selected 0/7817". The columns are "Name" and "Last Written". The first row, highlighted in blue, is for "Change" with the value "03/23/15 04:27:37 PM (-4:00 Eastern Daylight Time)". Below the table, the status bar shows "Data_Leak\cfred...". At the bottom, there is a hex dump view of the file content, showing binary data and ASCII characters.

29. Find traces related to cloud services on PC.

(Service name, log files...)

Answer: There are instances were traces of 2 different cloud services were found. The name of cloud services are **Google Drive and Apple iCloud**.

Path related to google drive: Data_Leak\cfreds_2015_data_leakage_pc\D\Program Files (x86)\Google\Drive\

Evidence:

| Name | Last Written |
|-----------------------|--|
| nativeproxy.exe | 02/19/15 01:19:00 PM (-5:00 Eastern Standard Time) |
| Microsoft.VC90.MFC | 03/23/15 04:02:44 PM (-4:00 Eastern Daylight Time) |
| Microsoft.VC90.CRT | 03/23/15 04:02:44 PM (-4:00 Eastern Daylight Time) |
| Microsoft.VC90.ATL | 03/23/15 04:02:44 PM (-4:00 Eastern Daylight Time) |
| Languages | 03/23/15 04:02:43 PM (-4:00 Eastern Daylight Time) |
| googledrivesync64.dll | 02/19/15 01:24:26 PM (-5:00 Eastern Standard Time) |
| googledrivesync.exe | 02/19/15 01:24:24 PM (-5:00 Eastern Standard Time) |
| contextmenu64.dll | 02/19/15 01:24:28 PM (-5:00 Eastern Standard Time) |

Path related to Apple iCloud:

Data_Leak\cfreds_2015_data_leakage_pc\D\Users\informant\Downloads\icloudsetup.exe

Evidence:

| Name | Last Written |
|-------------------------------------|--|
| icloudsetup.exe.Zone.Identifier | 03/23/15 03:56:53 PM (-4:00 Eastern Daylight Time) |
| icloudsetup.exe | 03/23/15 03:56:53 PM (-4:00 Eastern Daylight Time) |
| googledrivesync.exe.Zone.Identifier | 03/23/15 03:56:33 PM (-4:00 Eastern Daylight Time) |
| googledrivesync.exe | 03/23/15 03:56:33 PM (-4:00 Eastern Daylight Time) |
| desktop.ini | 03/22/15 10:34:59 AM (-4:00 Eastern Daylight Time) |

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: There are 2 deleted files are “**do_u_wanna_build_a_snow_man.mp3**” and “**happy_holiday.jpg**.”

Path:

Data_Leak\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Google\Drive\user_default\sync_log.log

- **2015-03-23 16:42:17,026 -0400 INFO pid=2576 4004:LocalWatcher**
 common.change_buffer:1017 Adding event to change buffer: RawEvent(**DELETE**,
 path=u'\\\\?\C:\\Users\\informant\\Google
 Drive**do_u_wanna_build_a_snow_man.mp3**', time=1427143336.964,
 ino=1125899906846942L, parent_ino=844424930207017L, affects_gdoc=False,
 is_cancelled=<RawEventIsCancelledFlag.FALSE: 0>,
 backup=<Backup.NO_BACKUP_CONTENT: (False, False)>)

- **2015-03-23 16:42:17,026 -0400 INFO pid=2576 4004:LocalWatcher**
 common.aggregator:114 -----> Received event RawEvent(**DELETE**,
 path=u'\\\\?\C:\\Users\\informant\\Google Drive**happy_holiday.jpg**',
 time=1427143336.964, ino=4503599627374809L, parent_ino=844424930207017L,
 affects_gdoc=False, is_cancelled=<RawEventIsCancelledFlag.FALSE: 0>,
 backup=<Backup.NO_BACKUP_CONTENT: (False, False)>) None

| | | | |
|------|----------------|--|---|
| 1624 | 03-23 16:42:19 | 369 -0400 WARNING pid=2576 3568:Worker-0 | logging:1602 Path \\\\C:\\Users\\informant\\Google Drive\\do_u_wanna_build_a_snow_man.mp3 that was supposed to be operated on r |
| 1625 | 03-23 16:42:19 | 369 -0400 INFO pid=2576 3568:Worker-0 | common.proxy_manager:352 Removing stale proxy entry from cache |
| 1626 | 03-23 16:42:19 | 385 -0400 INFO pid=2576 2820:Worker-1 | common.workers:188 Worker starting on [ImmutableChange(Direction.UPLOAD |
| 1627 | 03-23 16:42:19 | 385 -0400 WARNING pid=2576 2820:Worker-1 | logging:1602 Path \\\\C:\\Users\\informant\\Google Drive\\happy_holiday.jpg that was supposed to be operated on no longer exist |

31. Identify account information for synchronizing Google Drive.

Answer: The account used here is iaman.informant.personal@gmail.com. And it logged on at **2015-03-23 16:05:32**.

Path:

Data_Leak\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Google\Drive\user_default\sync_log.log

Log: 2015-03-23 16:05:32,279 -0400 INFO pid=2576 2828:LaunchThreads
 common.service.user:64 Initializing User instance with new credentials.

iaman.informant.personal@gmail.com 2015-03-23 16:05:32,279 -0400 INFO pid=2576
 2828:LaunchThreads common.sync_app:1153 Feature Switches: FeatureSwitchSettings(
 accept_blob_download_gzip_encoding=True, auto_backup=False,
 backup_polling_interval_secs=7200, cloud_graph_disk_generation=2,
 crash_log_size_limit=10000000, crash_throttle_percentage=99.7,
 disabled_cloud_graph_disk_app_versions=['1.8.4288.4175', '1.8.4340.2022',
 '1.10.4711.1662', '1.10.4657.9104', '1.10.4658.6881'], docs_list_page_size=1000,
 download_in_place=False, download_progress_bar=False,
 download_strategy='url_template',
 download_url='https://googledrive.com/p/host/{doc_id}', enable_batch_upload=True,
 enable_context_menu=True, enable_dapper_trace=False, enable_disk_dict=False,

| | | |
|------|---------------------|---|
| 1819 | 2015-03-25 11:21:36 | 782 -0400 INFO pid=3164 3140:LaunchThreads common.service.user:64 Initializing User instance with new credentials. iaman.informant.personal@gmail.com |
| 1820 | 2015-03-25 11:21:36 | 782 -0400 INFO pid=3164 3140:LaunchThreads common.features:109 Loads feature switches. |
| 1821 | 2015-03-25 11:21:36 | 782 -0400 INFO pid=3164 3140:LaunchThreads common.features:138 Loading feature switches with server. |
| 1822 | 2015-03-25 11:21:36 | 782 -0400 INFO pid=3164 3140:LaunchThreads common.feature_switch_manager:551 Calling server to get feature switches. |

32. What a method (or software) was used for burning CD-R?

Answer: The method used for burning the CD-R was likely **Windows' default CD/DVD burning feature (Burning Type 2: Mastered)**.

Path: cfreds_2015_data_leakage_pc\D\Windows\System32\winevt\Logs\System.evtx

Justification:

1. **Event ID 133:** The screenshot shows multiple instances of Event ID 133 in the System event log, indicating a **Type-2 burn**. This event, associated with the "IMAPI CD-Burning COM Service," is logged when Windows' built-in burning service is used. If a third-party application had been used, it likely would have generated its own events or modified the behavior of the IMAPI service, resulting in different event IDs or details.
2. **Burning Type 2 (Mastered):** Microsoft distinguishes between two types of CD/DVD burning:
 - **Type 1 (Like a USB flash drive):** This allows you to add and remove files from the disc like a USB drive. This method typically doesn't involve the IMAPI service and wouldn't generate Event ID 133.
 - **Type 2 (Mastered):** This creates a finalized, read-only disc compatible with standard CD/DVD players. This method utilizes the IMAPI service and generates Event ID 133, as seen in the screenshot.
3. **cdrom Source:** The "cdrom" source in the event log entries further indicates that these events are related to the CD/DVD drive and the built-in burning functionality.

4. **Timestamp Correlation:** The timestamps of the Event ID 133 entries might correlate with the "last modified" timestamps of the files on the CD-R, further supporting the conclusion that these events are associated with the burning process.

Based on the presence of **Event ID 133** in the System event log, the absence of any third-party software events, and the correlation with the "Mastered" burning type described in the Microsoft documentation, it is highly likely that the CD-R was burned using Windows' default CD/DVD burning feature.

| Event ID: 133 (4) | | | | | |
|-------------------|----------------------|-------|-----|------|--|
| (i) Information | 3/24/2015 3:47:47 PM | cdrom | 133 | None | |
| (i) Information | 3/24/2015 3:56:11 PM | cdrom | 133 | None | |
| (i) Information | 3/24/2015 4:41:21 PM | cdrom | 133 | None | |
| (i) Information | 3/24/2015 4:24:46 PM | cdrom | 133 | None | |

- The screenshot is from the **system.evtx** file, which is the Windows System event log. This log file records events related to system components, services, and drivers. The **system.evtx** file was first extracted from the forensic image and then opened using the Windows Event Viewer for analysis. The **system.evtx** file is crucial in digital forensics as it provides valuable information about system activities, errors, and events that can help investigators understand the timeline and context of events on a computer. In this case, it helps determine the method used for burning the CD-R.

33. When did the suspect burn CD-R?

[Hint: It may be one or more times.]

Answer: As per the data from the “system.evtx” log file, there were 4 instances where the suspect burns the CD-R.

Path: cfred_s_2015_data_leakage_pc\D\Windows\System32\winevt\Logs\System.evtx

| Timestamp | Source | Event ID | Description |
|----------------------|-----------------|----------|-----------------------|
| 3/24/2015 3:47:47 PM | System.evtx log | 133 | Burning Type 2: cdrom |
| 3/24/2015 3:56:11 PM | System.evtx log | 133 | Burning Type 2: cdrom |
| 3/24/2015 4:41:21 PM | System.evtx log | 133 | Burning Type 2: cdrom |
| 3/24/2015 4:24:46 PM | System.evtx log | 133 | Burning Type 2: cdrom |

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: Root Entry:

Data_Leak\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\1b4dd67f29cb1962.automaticDestinations-ms\Root Entry

35. What files were opened from CD-R?

Answer: The files accessed from the CD-R are listed below.

| Timestamp | File Path |
|------------------------|---|
| 2015-03-24 16:44:13 | D:\de\winter_whether_advisory.zip\ |
| 2015-03-24 16:44:14 | D:\de\winter_whether_advisory.zip\ppt\ |
| 2015-03-24 16:44:16 | D:\de\winter_whether_advisory.zip\ppt\slides\ |
| 2015-03-24 16:44:18 | D:\de\winter_whether_advisory.zip\ppt\slideMasters\ |
| 2015-03-24 16:44:18 | D:\de\winter_whether_advisory.zip |
| 2015-03-24 17:01:10 | D:\Penguins.jpg |
| 2015-03-24 17:01:12 | D:\Koala.jpg |
| 2015-03-24 17:01:14 | D:\Tulips.jpg |

Path: Root Entry:

Data_Leak\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\1b4dd67f29cb1962.automaticDestinations-ms\Root Entry.

This file path points to a root storage location within the Jump List file for the recently accessed files and application used by the user "informant" on a Windows system. A **Jump List** file is a feature in Windows 7 that keeps track of recently opened items and tasks associated with a specific application. It's like a personalized history for each app, allowing you to quickly access files or resume tasks you were working on. Jump Lists provide quick access to recently or frequently used items within an application, saving you time from searching for them manually.

The screenshot shows two windows from the Volatility Framework. The top window is a table titled 'Root Entry' with columns 'Name' and 'Last Written'. It lists several entries: 'Big Block FAT', 'MFT', 'Root', 'Root Entry' (selected), 'Small Block FAT', and 'Unallocated Clusters'. The 'Root Entry' row has a timestamp of 'Data_Leak\cfreds_2015_data_leakage_pc\0'. The bottom window shows memory dump details with tabs for 'Fields', 'Report', 'Text', etc. It includes a hex dump of a file named 'winter_whether_advisory.zip' and a table of memory values.

| Name | Last Written |
|----------------------|---|
| Big Block FAT | Data_Leak\cfreds_2015_data_leakage_pc\0 |
| MFT | Data_Leak\cfreds_2015_data_leakage_pc\0 |
| Root | Data_Leak\cfreds_2015_data_leakage_pc\0 |
| Root Entry | Data_Leak\cfreds_2015_data_leakage_pc\0 |
| Small Block FAT | Data_Leak\cfreds_2015_data_leakage_pc\0 |
| Unallocated Clusters | Data_Leak\cfreds_2015_data_leakage_pc\0 |

| Name | Value |
|-------------------------------|---|
| High ASCII | D:\de\winter_whether_advisory.zip\ppt\GEO*Z |
| Unicode | D:\de\winter_whether_advisory.zip\ppt\高风险 L A |
| Unix Date (Time/Date) | 02/13/70 06:52:36 PM |
| Windows Date/Time (Time/Date) | Invalid |
| HFS Plus Date (Time/Date) | 04/01/76 01:33:52 PM |
| DOS Date (DOS Date) | 01/26/80 12:02:08 AM |
| 32-bit Integer (UInt32) | 3801156 |

Some file access evidence can be found from the root entry logs while some of the recently accessed files are available in the RECENT folder, this is the directory where Windows stores **Jump List** files for different applications and stores is in .lnk format.

Path: Root Entry:

Data_Leak\cfreds_2015_data_leakage_pc\0\Users\informant\AppData\Roaming\Microsoft\Windows\Recent

The screenshot shows the 'Recent' folder structure and its contents. The left pane shows a tree view of recent files, including 'Protect', 'Sticky Notes', 'SystemCertificates', 'Templates', 'UProof', 'Windows' (which contains 'Cookies', 'DNTEception', 'IECompatCache', 'IECompatUACache', 'IEDownloadHistory', 'IETldCache', 'Libraries', 'Network Shortcuts', 'Printer Shortcuts', 'PrivacIE', and 'Recent'), and 'Word'. The right pane shows a table of recent files with columns 'Name' and 'Last Written'. The files listed are: 'CD Drive.lnk' (03/24/15 04:47:30 PM), 'CustomDestinations.lnk' (03/25/15 11:15:54 AM), 'desktop.ini' (03/22/15 10:34:59 AM), 'final.lnk' (03/23/15 04:27:33 PM), 'Koala.jpg.lnk' (03/24/15 05:01:12 PM), 'Penguins.jpg.lnk' (03/24/15 05:01:10 PM), 'pricing decision.lnk' (03/23/15 04:26:54 PM), 'Resignation_Letter_(laman_informant).docx.lnk' (03/25/15 11:29:08 AM), 'Resignation_Letter_(laman_informant).xps.lnk' (03/25/15 11:28:33 AM), 'secret.lnk' (03/23/15 02:38:21 PM), 'Tulips.jpg.lnk' (03/24/15 05:01:14 PM), and 'winter_whether_advisory.zip.lnk' (03/24/15 04:44:18 PM).

| Name | Last Written |
|---|--|
| CD Drive.lnk | 03/24/15 04:47:30 PM (-4:00 Eastern Daylight Time) |
| CustomDestinations.lnk | 03/25/15 11:15:54 AM (-4:00 Eastern Daylight Time) |
| desktop.ini | 03/22/15 10:34:59 AM (-4:00 Eastern Daylight Time) |
| final.lnk | 03/23/15 04:27:33 PM (-4:00 Eastern Daylight Time) |
| Koala.jpg.lnk | 03/24/15 05:01:12 PM (-4:00 Eastern Daylight Time) |
| Penguins.jpg.lnk | 03/24/15 05:01:10 PM (-4:00 Eastern Daylight Time) |
| pricing decision.lnk | 03/23/15 04:26:54 PM (-4:00 Eastern Daylight Time) |
| Resignation_Letter_(laman_informant).docx.lnk | 03/25/15 11:29:08 AM (-4:00 Eastern Daylight Time) |
| Resignation_Letter_(laman_informant).xps.lnk | 03/25/15 11:28:33 AM (-4:00 Eastern Daylight Time) |
| secret.lnk | 03/23/15 02:38:21 PM (-4:00 Eastern Daylight Time) |
| Tulips.jpg.lnk | 03/24/15 05:01:14 PM (-4:00 Eastern Daylight Time) |
| winter_whether_advisory.zip.lnk | 03/24/15 04:44:18 PM (-4:00 Eastern Daylight Time) |

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: This data can be obtained from the \$MFT table of the NTFS file system.

Filename: Resignation_Letter_(Iaman_Informant).docx

Parent Path: .\Users\informant\Desktop

| Timestamp | Standard Information | Source |
|--------------------------|----------------------|-------------|
| 3/24/2015 2:48:41 PM EST | File Created | \$MFT Table |
| 3/24/2015 2:59:31 PM EST | File Modified | \$MFT Table |
| 3/24/2015 2:59:31 PM EST | Last Record Change | \$MFT Table |
| 3/24/2015 2:59:31 PM EST | Entry Modified | \$MFT Table |

The \$MFT (Master File Table) is a critical component of the NTFS file system used in Windows. It's essentially a database that stores information about every file and directory on an NTFS volume. Think of it as a central catalog or index for all the files on your hard drive. It stores the following data:

- **File Records:** Each file and directory on the NTFS volume has a corresponding entry in the \$MFT called a "file record."
- **File Attributes:** These file records contain various attributes that describe the file, including:
 - **\$FILE_NAME:** The file's name and extension.
 - **\$STANDARD_INFORMATION:** File size, creation time, modification time, access time, and file attributes (e.g., read-only, hidden). Denoted by 0x10
 - **\$DATA:** The actual data content of the file (for small files) or pointers to where the data is stored on the disk (for larger files).
 - **\$SECURITY_DESCRIPTOR:** Security permissions for the file (who can access it and what they can do).
 - Other attributes related to data encryption, compression, object IDs, etc.

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

Answer: Upon analysis of the \$MFT table entries, there are 5 instances of the user accessing the Resignation_Letter_(Iaman_Informant) file. Each instance having different file extensions like .docx, .xps and .ink.

How the Suspect Printed the Resignation File: The suspect printed the resignation file by utilizing the "Microsoft XPS Document Writer," a virtual printer that outputs documents in

XPS format. This method creates an electronic file that retains the document's formatting and layout, like a PDF.

When the Suspect Printed the Resignation File: The suspect printed the resignation file on **March 25, 2015, at 11:28:34 AM** (timezone applied). This timestamp likely reflects the creation time of the XPS file, which serves as an indicator of when the "printing" action occurred.

The printed resignation file, in XPS format, is located at the following path:

Data_Leak\cfreds_2015_data_leakage_pc\D\Users\informant\Desktop\Resignation_Letter_(laman_Informant).docx

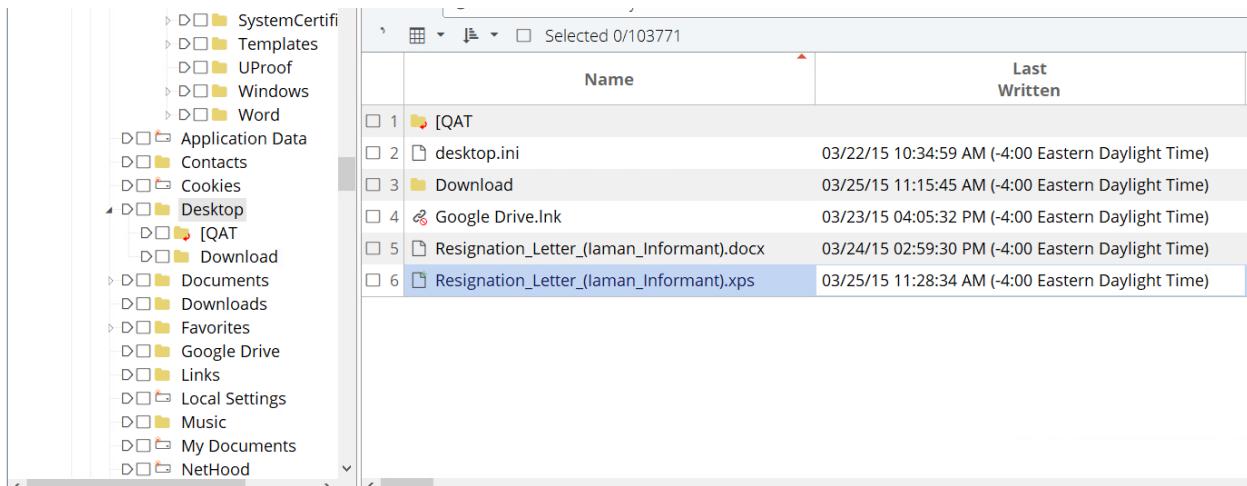
This indicates that the file was "printed" or saved to the user's desktop.

Considerations and Supporting Evidence:

- **No Physical Printers:** The absence of real printer devices on the system suggests that the suspect did not print the resignation letter to a physical printer.
- **XPS File on Desktop:** The presence of an XPS file with a relevant filename on the user's desktop further supports the conclusion that the "Microsoft XPS Document Writer" was used.
- **Registry Keys:** The registry keys under **Data_Leak\cfreds_2015_data_leakage_pc\Windows\System32\config\SOFTWARE\CMI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\Microsoft\Windows NT\CurrentVersion\Print\Printers** list the available printers on the system, including "Fax" and "Microsoft XPS Document Writer." This confirms there was no physical printer connected.

Based on the available evidence, it can be concluded that the suspect "printed" the resignation file to an XPS document on their desktop using the "Microsoft XPS Document Writer" on March 25, 2015, at 11:28:34 AM. This method allows for electronic storage and sharing of the document while preserving its formatting and layout.

| Type | Description |
|-------|---|
| How | Converted to XPS format |
| When | 03/25/15 11:28:34 AM (-4:00 Eastern Daylight Time) |
| Where | \D\Users\informant\Desktop\Resignation_Letter_(laman_Informant).xps |



The screenshot shows a file explorer window with a tree view on the left and a list view on the right. The tree view shows various folders like SystemCertificates, Templates, UProof, Windows, Word, Application Data, Contacts, Cookies, Desktop, Documents, Downloads, Favorites, Google Drive, Links, Local Settings, Music, My Documents, and NetHood. The list view is titled 'Selected 0/103771' and contains the following data:

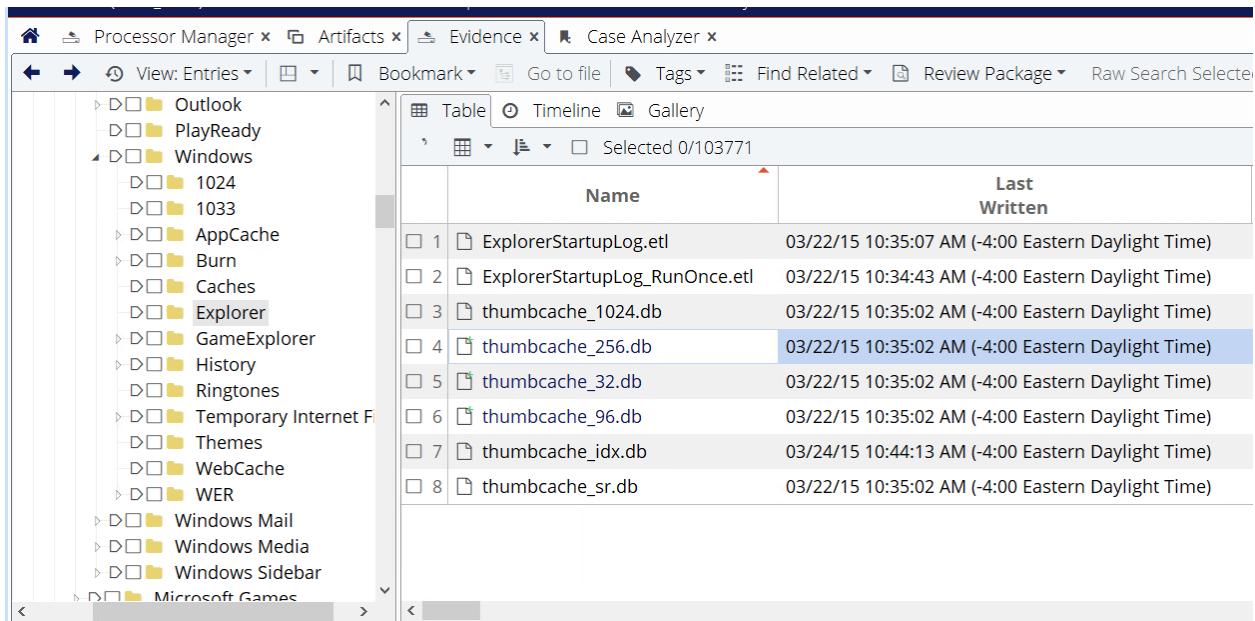
| | Name | Last Written |
|---|---|--|
| 1 | [QAT] | |
| 2 | desktop.ini | 03/22/15 10:34:59 AM (-4:00 Eastern Daylight Time) |
| 3 | Download | 03/25/15 11:15:45 AM (-4:00 Eastern Daylight Time) |
| 4 | Google Drive.Ink | 03/23/15 04:05:32 PM (-4:00 Eastern Daylight Time) |
| 5 | Resignation_Letter_(laman_Informant).docx | 03/24/15 02:59:30 PM (-4:00 Eastern Daylight Time) |
| 6 | Resignation_Letter_(laman_Informant).xps | 03/25/15 11:28:34 AM (-4:00 Eastern Daylight Time) |

38. Where are ‘Thumbcache’ files located?

Answer: The thumbcache files are located at
 “Data_Leak\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Microsoft\Windows\Explorer”

Windows thumbnail cache files are used by windows to store thumbnail images of pictures, videos, and documents so that they can be displayed quickly in File Explorer's thumbnail view. Here's a breakdown of the files:

- **thumbcache_xxx.db**: These are the main thumbnail cache databases. The xxx represents the size of the thumbnails stored in that specific file (32, 96, 256, 1024 pixels).
- **thumbcache_idx.db**: This file acts as an index for the thumbnail cache, helping Windows quickly locate specific thumbnails.
- **thumbcache_sr.db**: This file stores information about the image resolution and other properties.



The screenshot shows a forensic tool interface with a navigation bar at the top and a tree view on the left. The tree view shows various folders under Windows, including 1024, 1033, AppCache, Burn, Caches, Explorer, GameExplorer, History, Ringtones, Temporary Internet File, Themes, WebCache, WER, Windows Mail, Windows Media, Windows Sidebar, and Microsoft Games. The list view is titled 'Selected 0/103771' and contains the following data:

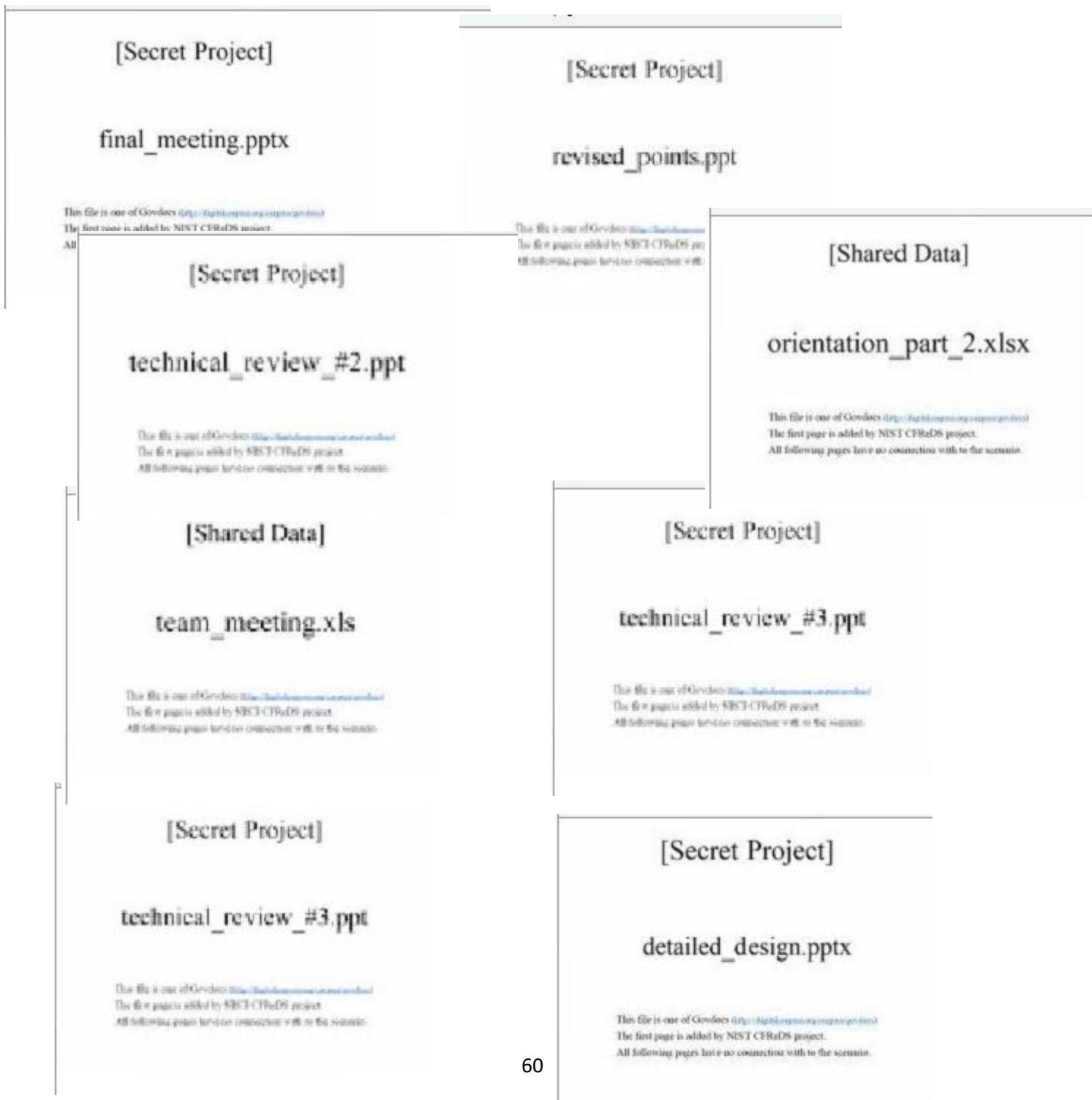
| | Name | Last Written |
|---|--------------------------------|--|
| 1 | ExplorerStartupLog.etl | 03/22/15 10:35:07 AM (-4:00 Eastern Daylight Time) |
| 2 | ExplorerStartupLog_RunOnce.etl | 03/22/15 10:34:43 AM (-4:00 Eastern Daylight Time) |
| 3 | thumbcache_1024.db | 03/22/15 10:35:02 AM (-4:00 Eastern Daylight Time) |
| 4 | thumbcache_256.db | 03/22/15 10:35:02 AM (-4:00 Eastern Daylight Time) |
| 5 | thumbcache_32.db | 03/22/15 10:35:02 AM (-4:00 Eastern Daylight Time) |
| 6 | thumbcache_96.db | 03/22/15 10:35:02 AM (-4:00 Eastern Daylight Time) |
| 7 | thumbcache_idx.db | 03/24/15 10:44:13 AM (-4:00 Eastern Daylight Time) |
| 8 | thumbcache_sr.db | 03/22/15 10:35:02 AM (-4:00 Eastern Daylight Time) |

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

Answer: There are traces of several confidential files like .pptx and xlsx found under the thumbcache directory. These items are found under the thumbcache_256.db directory and these are the cache images of the first page of PowerPoint files.

Path:

Data_Leak\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db



40. Where are Sticky Note files located?

Answer: The stick notes file is located at

“Data_Leak\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Roaming\Microsoft\Sticky Notes\StickyNotes.snt”

- A **StickyNotes.snt** file is the data file used by the **Sticky Notes** application in Windows. It stores the contents of all sticky notes, including the text, formatting (font, color, size), and position on the desktop.

The screenshot shows the Case Analyzer interface. On the left, there is a tree view of artifacts categorized under Microsoft, including Addins, Bibliography, Credentials, Crypto, Document Building, Excel, Internet Explorer, Network, Office, Outlook, PowerPoint, Proof, Protect, Sticky Notes, SystemCertificates, Templates, and iProof. Under the Sticky Notes category, the file 'StickyNotes.snt' is listed. In the center, there is a table view showing the file's details: Name (StickyNotes.snt), Last Written (03/24/15 02:31:59 PM (-4:00 Eastern Daylight Time)), and its path (Data_Leak\cfreds_2015_data_leakage_pc\D\Users\informant). Below the table, there are tabs for Fields, Report, Text, Hex, Doc, Transcript, and a large hex dump of the file's content. To the right, there is a detailed view of the file's contents, showing various fields like Name, Value, and their corresponding binary and ASCII representations.

41. Identify notes stored in the Sticky Note file.

Answer: There is a note stored in the sticky notes that reads “T o m o r r o w . . . E v e r y t h i n g w i l l b e O K . . . ”

Path:

Data_Leak\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Roaming\Microsoft\Sticky Notes\StickyNotes.snt\Root Entry\ccbb72fb-d253-11e4-b\3

Evidence:

```

Root Entry cccb72fb-d253-11e4-b
ÿþ cccb72fb-d253-11e4-b {\rtf1\ansi\ansicpg1252\deff0\deflang1033{\fonttbl{\f0\fnil\fcha0
rset0 Segoe Print;}{\f1\fnil Segoe Print;}}
{*generator Msftedit
5.41.21.2510;}\viewkind4\uc1\pard\tx360\tx720\tx1080\tx1440\tx1800\tx2160\tx2520\tx2880\tx3240\tx3600\tx3960\tx
x4320\tx4680\tx5040\tx5400\tx5760\tx6120\tx6480\tx6840\tx7200\tx7560\tx7920\tx8280\tx8640\tx9000\tx9360\tx9720
\tx10080\tx10440\tx10800\tx11160\tx11520\highlight0\f0\fs22 Tomorrow...\par
Everything will be OK...\par
\lang9\f1\par
Tomorrow...
Everything will be OK...

```

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: Yes, the windows search and indexing function is enabled on this system. It can be verified from the **software** registry hive by looking at the “*SetupCompletedSuccessfully*” key.

- The “*SetupCompletedSuccessfully*:“ Indicates if the initial setup of Windows Search was completed. If set to 1, it suggests the service is configured to run.
- Path:**
Data_Leak\cfreds_2015_data_leakage_pc\Windows\System32\config\SOFTWARE\Microsoft\CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\Microsoft\Windows Search\SetupCompletedSuccessfully
- Evidence:** The hex value 01 00 00 00 when converted to dec, represents 1 that indicates that search and index is turned ON

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

Answer: This evidence can be inferred from the value of the key “FILENAME” under the database directory. The SOFTWARE hive that likely stores information related to the Windows Search database and **FileName** key contain the name and path of the Windows.edb file, which is the actual database file where Windows Search stores its index of files and content. The general file path for the search index database is:

“C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb”

Path:

Data_Leak\cfreds_2015_data_leakage_pc\Windows\System32\config\SOFTWARE\CMS-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\Microsoft\Windows Search\Databases\Windows\FileName

The screenshot shows the EnCase Forensic software interface. On the left, the tree view displays the registry keys under the SOFTWARE hive, including CatalogNames, CrawlScopeManager, Databases (with Windows selected), Gather, Gathering Manager, Indexer, and InstallDirectory. In the center, a table view shows two entries under the 'Selected 0/441498' section:

| Name | Last Written |
|------------|---|
| 1 FileName | Data_Leak\cfreds_2015_data_leakage_pc\Windows\System32\config\SOFTWARE\CMS-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\Microsoft\Windows Search\Databases\Windows\FileName |
| 2 LogPath | Data_Leak\cfreds_2015_data_leakage_pc\Windows\System32\config\SOFTWARE\CMS-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}\Microsoft\Windows Search\Databases\Windows\FileName |

Below the table, there is a hex dump of the file data, showing binary values and corresponding ASCII characters. On the right, a details pane shows various file metadata fields:

| Name | Value |
|----------------------|--|
| High ASCII | C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Window |
| Unicode | C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Window |
| Unix Date (Time/... | 02/13/70 06:52:35 PM |
| Windows Date/TI... | Invalid |
| HFS Plus Date (Ti... | 09/20/75 09:13:36 AM |
| DOS Date (DOS ... | 01/26/80 12:02:06 AM |

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: The table given below, extracted from the Windows Search database (Windows.edb), reveals traces of Internet Explorer usage by the suspect between March 22nd and 23rd, 2015. The table shows the System_DateModified and Microsoft_IE_TargetUrl columns, indicating the time of modification and the specific URLs accessed using Internet Explorer.

| Timestamp | Internet Explorer Data |
|------------------|--|
| 22-03-2015 11:09 | http://windows.microsoft.com/en-us/internet-explorer/ie-8-welcome |
| 22-03-2015 11:09 | http://www.msn.com/?ocid=iehp |
| 22-03-2015 11:09 | https://www.google.com/?gws_rd=ssl |
| 22-03-2015 11:09 | https://www.google.com/search?hl=en&source=hp&q=internet+explorer+11&gbv=2&oq=internet+explorer+11&gs_l=hp..0l10.5163.7893.0.9562.20.13.0.7.7.0.156.1110.11j2.13.0.msedr...0...1ac.1.34.heirloom-hp..0.20.1250.5j7Xm44tv |

| | |
|------------------|---|
| 22-03-2015 11:09 | 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-jTxbaV |
| 22-03-2015 11:09 | http://windows.microsoft.com/en-us/internet-explorer/download-ie |
| 22-03-2015 11:09 | 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=AFQjCNE7UKIWE |
| 22-03-2015 11:10 | http://windows.microsoft.com/en-us/internet-explorer/ie-11-worldwide-languages |
| 22-03-2015 11:10 | https://www.google.com/webhp?hl=en |
| 22-03-2015 11:10 | https://www.google.com/chrome/index.html?hl=en&brand=CHNG&utm_source=en-hpp&utm_medium=hpp&utm_campaign=CHNG_HPP |
| 22-03-2015 11:11 | http://download.microsoft.com/download/7/1/7/7179A150-F2D2-4502-9D70-4B59EA148EAA/IE11-Windows6.1-x64-All%5B%5D.exe |
| 22-03-2015 11:11 | https://www.google.com/chrome/browser/thankyou.html?brand=CHNG&platform=win&clickonceinstalled=1 |
| 23-03-2015 13:26 | https://odc.officeapps.live.com/odc/emailhrd?lcid=1033&syslcid=1033&uilcid=1033&app=5&ver=15&build=15.0.44208.1000 |
| 23-03-2015 13:27 | http://www.microsoft.com/en-us/ie-firstrun/win-7/ie-11/vie |
| 23-03-2015 13:27 | http://www.bing.com/search |
| 23-03-2015 13:27 | http://go.microsoft.com/fwlink/?LinkId=69157 |
| 23-03-2015 13:28 | http://www.bing.com/ |
| 23-03-2015 14:07 | http://www.bing.com/news/search?q=Top+Stories&FORM=NSBABR |
| 23-03-2015 14:07 | http://www.bing.com/search?q=Top+Stories&FORM=HDRSC1 |
| 23-03-2015 14:07 | http://www.bing.com/news/search?q=file+sharing+and+tethering&FORM=HDRSC6 |
| 23-03-2015 14:08 | http://www.bing.com/search?q=file+sharing+and+tethering&qs=n&form=QBLH&pq=file+sharing+and+tethering&sc=0-1&sk=&cvid=171b77e4ffd54b2a92c4e97abf995fe1 |
| 23-03-2015 14:08 | http://sysinfotools.com/blog/tethering-internet-files-sharing/ |
| 23-03-2015 14:11 | http://resources.infosecinstitute.com/windows-systems-and-artifacts-in-digital-forensics-part-i-registry/ |
| 23-03-2015 14:12 | https://technet.microsoft.com/en-us/library/cc162846.aspx |
| 23-03-2015 14:12 | https://support.microsoft.com/en-us/kb/308427 |
| 23-03-2015 14:12 | http://en.wikipedia.org/wiki/Event_Viewer |
| 23-03-2015 14:13 | https://msdn.microsoft.com/en-us/library/windows/desktop/dd562212(v=vs.85).aspx |
| 23-03-2015 14:14 | http://www.forensicswiki.org/wiki/USB_History_Viewing |
| 23-03-2015 16:43 | http://www.bing.com/search?q=external%20device%20and%20forensics&qs=n&form=QBRE&pq=external%20device%9&sp=-1&sk=&cvid=c30c4b1f36114b1c9bc683838c69823a |
| 23-03-2015 16:43 | http://www.bing.com/?FORM=Z9FD1 |
| 23-03-2015 16:43 | http://www.bing.com/news?FORM=Z9LH3 |
| 23-03-2015 16:44 | http://www.bing.com/news?q=science+technology+news&FORM=NWBTCB |
| 23-03-2015 16:45 | http://www.wired.com/?p=1756538 |

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 | Source | From | To | Subject | Body |
|---------------------|------------|--------------------------|--------------------------|-------------------------|--|
| 23-03-2015 13:29 | Inbox | spy.conspirator@nist.gov | iaman.informant@nist.gov | Hello, laman | How are you doing? |
| 23-03-2015 14:44 | Sent Items | iaman.informant@nist.gov | spy.conspirator@nist.gov | RE: Hello, laman | RE: Hello, laman |
| 23-03-2015 15:14 | Inbox | spy.conspirator@nist.gov | iaman.informant@nist.gov | Good job, buddy. | Good, job. I need a more detailed data about this business. |
| 23-03-2015 15:19 | Sent Items | iaman.informant@nist.gov | spy.conspirator@nist.gov | 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. |
| 23-03-2015 15:20 | Inbox | spy.conspirator@nist.gov | iaman.informant@nist.gov | RE: Good job, buddy. | 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 |

| | | | | | |
|---------------------|---------------|--------------------------|--------------------------|-----------------------|--|
| | | | | | <p>Sent: Monday, March 23, 2015 3:15 PM</p> <p>To: iaman</p> <p>Subject: Good job, buddy.</p> <p>Good, job.</p> <p>I need a more detailed data about this business.</p> |
| 23-03-2015 15:26 | Inbox | spy.conspirator@nist.gov | iaman.informant@nist.gov | Important request | <p>I confirmed it.</p> <p>But I need a more data.</p> <p>Do your best.</p> |
| 23-03-2015 15:27 | Sent Items | iaman.informant@nist.gov | spy.conspirator@nist.gov | RE: Important request | <p>Umm..... I need time to think.</p> <p>-----</p> <p>From: spy</p> <p>Sent: Monday, March 23, 2015 3:26 PM</p> <p>To: iaman</p> <p>Subject: Important request</p> <p>I confirmed it.</p> <p>But, I need a more data.</p> <p>Do your best.</p> |
| 23-03-2015 16:38 | Deleted Items | iaman.informant@nist.gov | spy.conspirator@nist.gov | It's me | <p>Use links below,</p> <p>https://drive.google.com/file/d/0Bz0ye6gXtiZaVl8yVU5mWHIGbWc/view?usp=sharing</p> |

| | | | | | |
|---------------------|---------------|--------------------------|--------------------------|------------------|---|
| | | | | | https://drive.google.com/file/d/0Bz0ye6gXtiZaakx6d3R3c0JmM1U/view?usp=sharing |
| 23-03-2015 16:41 | Deleted Items | spy.conspirator@nist.gov | iaman.informant@nist.gov | RE: It's me | <p>I got it.</p> <p>-----</p> <p>From: iaman Sent: Monday, March 23, 2015 4:39 PM To: spy Subject: It's me</p> <p>Use links below,</p> <p>https://drive.google.com/file/d/0Bz0ye6gXtiZaVl8yVU5mWHIGbWc/view?usp=sharing</p> <p>https://drive.google.com/file/d/0Bz0ye6gXtiZaakx6d3R3c0JmM1U/view?usp=sharing</p> |
| 24-03-2015 09:25 | Inbox | spy.conspirator@nist.gov | iaman.informant@nist.gov | Last request | <p>This is the last request.</p> <p>I want to get the remaining data.</p> |
| 24-03-2015 09:30 | Sent Items | iaman.informant@nist.gov | spy.conspirator@nist.gov | RE: Last request | <p>Stop it! It is very hard to transfer all data over the internet!</p> <p>-----</p> <p>From: spy Sent: Tuesday, March 24, 2015 9:26 AM To: iaman Subject: Last request</p> <p>This is the last request.</p> |

| | | | | | |
|---------------------|---------------|--------------------------|--------------------------|------------------|--|
| | | | | | I want to get the remaining data. |
| 24-03-2015 09:32 | Inbox | spy.conspirator@nist.gov | iaman.informant@nist.gov | Watch out! | USB device may be easily detected. So, try another method. |
| 24-03-2015 09:33 | Inbox | spy.conspirator@nist.gov | iaman.informant@nist.gov | 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. |
| 24-03-2015 15:34 | Deleted Items | iaman.informant@nist.gov | spy.conspirator@nist.gov | RE: Watch out! | I am trying. ----- From: spy Sent: Tuesday, March 24, 2015 3:33 PM |
| 24-03-2015 09:35 | Deleted Items | iaman.informant@nist.gov | spy.conspirator@nist.gov | RE: Last request | |

| | | | | | |
|---------------------|------------------|--------------------------|--------------------------|----------------|---|
| | | | | | |
| 24-03-2015 15:34 | Deleted Items | iaman.informant@nist.gov | spy.conspirator@nist.gov | RE: Watch out! | <p>To: iaman</p> <p>Subject: Watch out!</p> <p>USB device may be easily detected.</p> <p>So, try another method.</p> <hr/> <p>From: iaman</p> <p>Sent: Tuesday, March 24, 2015 9:30 AM</p> <p>To: spy</p> <p>Subject: RE: Last request</p> <p>Stop it!</p> <p>It is very hard to transfer all data over the internet!</p> <hr/> <p>From: spy</p> <p>Sent: Tuesday, March 24, 2015 9:26 AM</p> <p>To: iaman</p> <p>Subject: Last request</p> <p>This is the last request.</p> <p>I want to get the remaining data.</p> <p>I am trying.</p> |

| | | | | | |
|---------------------|---------------|--------------------------|--------------------------|------|---|
| | | | | | <p>-----</p> <p>From: spy</p> <p>Sent: Tuesday, March 24, 2015 3:33 PM</p> <p>To: iaman</p> <p>Subject: Watch out!</p> <p>USB device may be easily detected.</p> <p>So, try another method.</p> |
| 24-03-2015 17:05 | Deleted Items | iaman.informant@nist.gov | spy.conspirator@nist.gov | Done | It's done. See you tomorrow. |

The evidence presented in the table is derived from the Windows Search database, specifically the **Windows.edb file**. This file, which utilizes the Microsoft ESE (Extensible Storage Engine) database format, functions as an index of files and content to enable faster searching within Windows. This windows.edb file is in **Data_Leak\cfreds_2015_data_leakage_pc\D\ProgramData\Microsoft\Search\Data\Appllications\Windows\Windows.edb**

This email conversation is tabulated using the data from various columns extracted from this database, including:

- **System_ItemPathDisplay:** This column likely contains the file paths of indexed items, providing information about the location of files within the file system.
- **System_Message_FromName, System_Message_ToAddress, System_Message_ToName, System_Message_DateSent, System_Message_DateReceived, and System_Message_AttachmentNames:** These columns appear to be related to email data, suggesting that the Windows Search index included email content. These columns likely store information about the sender's name, recipient's email address and name, the dates when the email was sent and received, and the names of any attachments associated with the email.

46. List files and directories related to Windows Desktop stored in Windows Search database.

(Windows Desktop directory: \Users\informant\Desktop\)

Answer:

| Desktop Files | Creation Timestamps |
|--|----------------------------|
| C:\Users\informant\Desktop\temp\Tulips.jpg | 3/24/2015 19:52 |
| C:\Users\informant\Desktop\temp\Penguins.jpg | 3/24/2015 19:52 |
| C:\Users\informant\Desktop\temp\Lighthouse.jpg | 3/24/2015 19:52 |
| C:\Users\informant\Desktop\temp\Koala.jpg | 3/24/2015 19:52 |
| C:\Users\informant\Desktop\temp\Jellyfish.jpg | 3/24/2015 19:52 |
| C:\Users\informant\Desktop\temp\IE11-Windows6.1-x64-en-us.exe | 3/24/2015 19:52 |
| C:\Users\informant\Desktop\temp\Hydrangeas.jpg | 3/24/2015 19:52 |
| C:\Users\informant\Desktop\temp\Desert.jpg | 3/24/2015 19:52 |
| C:\Users\informant\Desktop\temp\Chrysanthemum.jpg | 3/24/2015 19:52 |
| C:\Users\informant\Desktop\temp | 3/24/2015 19:52 |
| C:\Users\informant\Desktop\S data\Secret Project Data\Secret Project Data\proposal\[secret_project]_proposal.docx | 3/24/2015 13:40 |
| C:\Users\informant\Desktop\S data\Secret Project Data\Secret Project Data\proposal\[secret_project]_detailed_proposal.docx | 3/24/2015 13:40 |
| C:\Users\informant\Desktop\S data\Secret Project Data\Secret Project Data\proposal | 3/24/2015 13:47 |
| C:\Users\informant\Desktop\S data\Secret Project Data\Secret Project Data\pricing decision\[secret_project]_price_analysis_#1.xlsx | 3/24/2015 13:47 |
| C:\Users\informant\Desktop\S data\Secret Project Data\Secret Project Data\pricing decision\[secret_project]_market_shares.xls | 3/24/2015 13:47 |
| C:\Users\informant\Desktop\S data\Secret Project Data\Secret Project Data\pricing decision\[secret_project]_market_analysis.xlsx | 3/24/2015 13:47 |
| C:\Users\informant\Desktop\S data\Secret Project Data\Secret Project Data\final\[secret_project]_final_meeting.pptx | 3/24/2015 13:47 |
| C:\Users\informant\Desktop\S data\Secret Project Data\Secret Project Data\design\winter WHETHER_advisory.zip | 3/24/2015 13:40 |
| C:\Users\informant\Desktop\S data\Secret Project Data\Secret Project Data\design\winter_storm.amr | 3/24/2015 13:40 |
| C:\Users\informant\Desktop\S data\Secret Project Data\Secret Project Data\design\space_and_earth.mp4 | 3/24/2015 13:40 |
| C:\Users\informant\Desktop\S data\Secret Project Data\Secret Project Data\design\[secret_project]_detailed_design.pptx | 3/24/2015 13:47 |
| C:\Users\informant\Desktop\Resignation_Letter_(laman_Informant).docx | 3/24/2015 18:48 |
| C:\Users\informant\Desktop\Google Drive.lnk | 3/23/2015 20:05 |
| C:\Users\informant\Desktop\Download\IE11-Windows6.1-x64-en-us.exe | 3/22/2015 15:11 |
| C:\Users\informant\Desktop\Download | 3/22/2015 15:08 |
| C:\Users\informant\Desktop\desktop.ini | 3/22/2015 14:34 |

The evidence presented in the table is derived from the Windows Search database, specifically the **Windows.edb** file. This file, which utilizes the Microsoft ESE (Extensible Storage Engine) database format, functions as an index of files and content to enable faster searching within the Windows operating system. The table displays various columns extracted from this database, including System_DateCreated, and System_ItemPathDisplay. These columns likely provide information about file creation and modification timestamps, and file paths respectively.

47. Where are Volume Shadow Copies stored? When were they created?

Answer: **Volume Shadow Copies** are essentially snapshots of your data at a specific point in time. Imagine you're working on a document and accidentally deleting a crucial paragraph. Volume Shadow Copy Service (VSS) shadow copies are typically stored in the hidden System Volume Information folder in the root directory of a drive. However, the shadow copy storage location can be configured to use a different NTFS volume. Generally, folder is located at the root of each volume (e.g., C:\System Volume Information).

- **Path:** Data_Leak\cfreds_2015_data_leakage_pc\D\System Volume Information
- **Creation Time:**
- **Evidence:**

The screenshot shows the EnCase Forensic interface. On the left, a tree view of the file system shows the path: \$Recycle.Bin, Config.Msi, Documents and Settings, Program Files, ProgramData, Recovery, System Volume Information (containing SPP, OnlineMetadataCache, SppCbsHiveStore, SppGroupCache), Users, Windows, and Lost Files. The main pane displays a table of files with columns for Name and Last Written. The table shows several files, including MountPointManagerRemoteDatabase, SPP, Syscache.hve, Syscache.hve.LOG1, Syscache.hve.LOG2, tracking.log, and several files starting with {3808876b-c176-4e48-b7ae-04046e6cc752} and {9b365807-d2ef-11e4-b734-000c29ff2429}. The last row, {9b365826-d2ef-11e4-b734-000c29ff2429}, has a red 'X' icon next to it, indicating it has been deleted from the current file system. Below the table, there is a hex dump of the file's content, showing ASCII and binary data. A bottom pane shows file metadata for the deleted file, including Name (informant-PC), Value (informant-PC), and various date/time fields.

| Name | Last Written |
|--|--|
| MountPointManagerRemoteDatabase | 03/25/15 06:15:18 AM (-4:00 Eastern Daylight Time) |
| SPP | 03/25/15 10:57:24 AM (-4:00 Eastern Daylight Time) |
| Syscache.hve | 03/25/15 11:31:05 AM (-4:00 Eastern Daylight Time) |
| Syscache.hve.LOG1 | 03/25/15 11:20:57 AM (-4:00 Eastern Daylight Time) |
| Syscache.hve.LOG2 | 03/25/15 06:15:55 AM (-4:00 Eastern Daylight Time) |
| tracking.log | 03/25/15 06:16:09 AM (-4:00 Eastern Daylight Time) |
| {3808876b-c176-4e48-b7ae-04046e6cc752} | 03/25/15 10:50:37 AM (-4:00 Eastern Daylight Time) |
| {9b365807-d2ef-11e4-b734-000c29ff2429}{3808876b-c176-4e48-b7ae-04046e6cc752} | 03/25/15 10:57:27 AM (-4:00 Eastern Daylight Time) |
| {9b365826-d2ef-11e4-b734-000c29ff2429}{3808876b-c176-4e48-b7ae-04046e6cc752} | 03/25/15 10:57:24 AM (-4:00 Eastern Daylight Time) |

| Name | Value |
|-------------------------------|---------------------------|
| High ASCII | informant-PC informant-PC |
| Unicode | informant-PC informant-PC |
| Unix Date (Time/Date) | 03/25/70 05:31:05 AM |
| Windows Date/Time (Time/Date) | Invalid |
| HFS Plus Date (Time/Date) | 12/03/95 08:45:36 AM |
| DOS Date (DOS Date) | 03/14/80 12:03:18 AM |

The red "X" icon in the EnCase view indicates that the file has been deleted from the *current* file system, meaning it no longer exists in its original location. However, the file is still present within the Volume Shadow Copy. This means the file was present when the

shadow copy was created but was deleted sometime afterward. The file “{9b365826-d2ef-11e4-b734-000c29ff2429}\3808876b-c176-4e48-b7ae-04046e6cc752}” appears to be a Volume Shadow Copy file. Its name consists of two GUIDs (Globally Unique Identifiers). These GUIDs represent:

- **{9b365826-d2ef-11e4-b734-000c29ff2429}**: A specific Volume Shadow Copy point.
- **{3808876b-c176-4e48-b7ae-04046e6cc752}**: The System Protection storage area

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?

| Name | Last Written |
|--|--|
| MountPointManagerRemoteDatabase | 03/25/15 06:15:18 AM (-4:00 Eastern Daylight Time) |
| SPP | 03/25/15 10:57:24 AM (-4:00 Eastern Daylight Time) |
| Syscache.hve | 03/25/15 11:31:05 AM (-4:00 Eastern Daylight Time) |
| Syscache.hve.LOG1 | 03/25/15 11:20:57 AM (-4:00 Eastern Daylight Time) |
| Syscache.hve.LOG2 | 03/25/15 06:15:55 AM (-4:00 Eastern Daylight Time) |
| tracking.log | 03/25/15 06:16:09 AM (-4:00 Eastern Daylight Time) |
| {3808876b-c176-4e48-b7ae-04046e6cc752} | 03/25/15 10:50:37 AM (-4:00 Eastern Daylight Time) |
| {9b365807-d2ef-11e4-b734-000c29ff2429}(3808876b-c176-4e48-b7ae-04046e6cc752) | 03/25/15 10:57:27 AM (-4:00 Eastern Daylight Time) |
| {9b365826-d2ef-11e4-b734-000c29ff2429}(3808876b-c176-4e48-b7ae-04046e6cc752) | 03/25/15 10:57:24 AM (-4:00 Eastern Daylight Time) |

Answer:

The traces related to google drive services.

- **2015-03-23 16:47:55,993 -0400 INFO pid=2576 1836:CloudWatcher common.utils:640 Execute cleanup callback**
'persistence_sqlite:340f44a941574c189c7389b6db2237b2C:\Users\INFORM~1\AppData\Local\Google\Drive\user_default\sync_config.db'
- common.persistence.sqlite:379 Close connection.
path=C:\Users\INFORM~1\AppData\Local\Google\Drive\user_default\sync_config.db
- **2015-03-23 16:47:55,993 -0400 INFO pid=2576 1836:CloudWatcher common.utils:640 Execute cleanup callback**
'persistence_sqlite:340f44a941574c189c7389b6db2237b2C:\Users\INFORM~1\AppData\Local\Google\Drive\user_default\snapshot.db'

- ➔ **2015-03-23 16:47:56,003 -0400 INFO pid=2576 2820:Worker-1**
 common.utils:640 Execute cleanup callback
 'persistence_sqlite:0963338d6ddc43139c54ac552165a5d0C:\Users\INFORM~1\Ap
 pData\Local\Google\Drive\user_default\snapshot.db'
- ➔ **2015-03-23 16:47:56,003 -0400 INFO pid=2576 2820:Worker-1**
 common.utils:640 Execute cleanup callback
 'persistence_sqlite:79c68ef94b804b05a961e7c12eaabcb2C:\Users\INFORM~1\Ap
 pData\Local\Google\Drive\user_default\sync_config.db'

The discrepancies observed between the current system image and the Volume Shadow Copy (VSC) indicate that the VSC represents an earlier state of the system, captured before a logoff activity occurred on March 25, 2015. This is evidenced by the presence of the sync_log.log file and two SQLite files (**snapshot.db** and **sync_config.db**) within the VSC, which are absent in the current system image. The last entry in the sync_log.log file within the VSC is timestamped March 23, 2015, while the VSC itself was created on *March 25, 2015, at 10:57:27 AM*, after the logoff activity that presumably deleted the log file and SQLite databases. This discrepancy confirms that the VSC provides a snapshot of the system's state before the logoff activity and the associated deletion of files.

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: Forensic analysis of the Volume Shadow Copy (VSC) located at **Data_Leak\cfred\2015_data_leakage_pc\1\System Volume Information\{9b365826-d2ef-11e4-b734-000c29ff2429}\3808876b-c176-4e48-b7ae-04046e6cc752}** revealed evidence of file deletion. Specifically, two deleted records were identified within the *snapshot.db* file contained in the VSC. The first deleted record was found at file offset 0x702, while the second was located at file offset 0x77A. These deleted records suggest that the user intentionally or unintentionally removed these files from the system. However, due to the nature of Volume Shadow Copies, these deleted files remain preserved within the VSC, providing valuable forensic evidence for potential recovery or analysis of the user's actions.

Screenshot of a file system analysis tool showing a list of files in the System Volume Information folder. The list includes tracking.log, Syscache.hve.LOG2, Syscache.hve.LOG1, Syscache.hve, SPP, and MountPointManagerRemoteDatabase. The tool also shows a preview of a file named "wanna_build_a_snow_man.mp3" which contains the text "wanna_build_a_snow_man.mp3" and "happy_holiday.jpg". A search results pane on the right shows a single result for "High ASCII happy".

| Name | Last Written |
|--|--|
| {9b365826-d2ef-11e4-b734-000c29ff2429}\{380... | 03/25/15 10:57:24 AM (-4:00 Eastern Daylight Time) |
| {9b365807-d2ef-11e4-b734-000c29ff2429}\{380... | 03/25/15 10:57:27 AM (-4:00 Eastern Daylight Time) |
| {3808876b-c176-4e48-b7ae-04046e6cc752} | 03/25/15 10:50:37 AM (-4:00 Eastern Daylight Time) |
| tracking.log | 03/25/15 06:16:09 AM (-4:00 Eastern Daylight Time) |
| Syscache.hve.LOG2 | 03/25/15 06:15:55 AM (-4:00 Eastern Daylight Time) |
| Syscache.hve.LOG1 | 03/25/15 11:20:57 AM (-4:00 Eastern Daylight Time) |
| Syscache.hve | 03/25/15 11:31:05 AM (-4:00 Eastern Daylight Time) |
| SPP | 03/25/15 10:57:24 AM (-4:00 Eastern Daylight Time) |
| MountPointManagerRemoteDatabase | 03/25/15 06:15:18 AM (-4:00 Eastern Daylight Time) |

Screenshot of a file system analysis tool showing a list of files in the System Volume Information folder. The list includes tracking.log, Syscache.hve.LOG2, Syscache.hve.LOG1, Syscache.hve, SPP, and MountPointManagerRemoteDatabase. The tool also shows a preview of a file named "wanna_build_a_snow_man.mp3" which contains the text "wanna_build_a_snow_man.mp3" and "happy_holiday.jpg". A search results pane on the right shows a single result for "High ASCII happy".

| Name | Last Written |
|--|--|
| {9b365826-d2ef-11e4-b734-000c29ff2429}\{380... | 03/25/15 10:57:24 AM (-4:00 Eastern Daylight Time) |
| {9b365807-d2ef-11e4-b734-000c29ff2429}\{380... | 03/25/15 10:57:27 AM (-4:00 Eastern Daylight Time) |
| {3808876b-c176-4e48-b7ae-04046e6cc752} | 03/25/15 10:50:37 AM (-4:00 Eastern Daylight Time) |
| tracking.log | 03/25/15 06:16:09 AM (-4:00 Eastern Daylight Time) |
| Syscache.hve.LOG2 | 03/25/15 06:15:55 AM (-4:00 Eastern Daylight Time) |
| Syscache.hve.LOG1 | 03/25/15 11:20:57 AM (-4:00 Eastern Daylight Time) |
| Syscache.hve | 03/25/15 11:31:05 AM (-4:00 Eastern Daylight Time) |
| SPP | 03/25/15 10:57:24 AM (-4:00 Eastern Daylight Time) |
| MountPointManagerRemoteDatabase | 03/25/15 06:15:18 AM (-4:00 Eastern Daylight Time) |

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

Answer: To include OST files in VSS, a specific registry key needs to be modified. If this modification hasn't been done, the OST file won't be included in the shadow copy. To include OST files in the backup, you need to access the registry editor and navigate to the following location:

Data_Leak\cfreds_2015_data_leakage_pc\Windows\System32\config\SYSTEM\CMSI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}\ControlSet001\Control\BackupRestore\FilesNotToSnapshot\OutlookOST.

Within this SYSTEM hive, you will find a subfolder named "FilesNotToSnapshot" and within this subfolder there is a subkey called "**OutlookOST**". By deleting this key, we can allow VSC to include the Outlook's email data in Volume Shadow Copy.

The screenshot shows the EnCase Evidence browser interface. The left pane displays a tree view of registry keys under the SYSTEM hive. One of the keys is expanded to show subkeys like Control, BackupRestore, and FilesNotToSnapshot. The BackupRestore key contains subkeys for FilesNotToBackup, FilesNotToSnapshot, and KeysNotToRestore. The FilesNotToSnapshot key is selected. The right pane shows a table view of the contents of this key, with a single row highlighted. The table has a header row with a 'Name' column. The data rows are numbered 1 through 6, with row 4 (OutlookOST) being the one currently selected.

| Name |
|--------------|
| 1 FVE |
| 2 OfficeODC |
| 3 OutlookOAB |
| 4 OutlookOST |
| 5 RAC |
| 6 WUA |

51. Examine 'Recycle Bin' data in PC.

Answer: The PC under investigation, in this case, is a windows 7 computer. Thus, When you delete a file in Windows 7, two files are created in the Recycle Bin:

- **\$I[random].extension:** This is the **information file**. It stores metadata about the original file, such as its original location, deletion date, and file size. The \$I file keeps track of important information about the deleted file, allowing Windows to restore it to its original location if needed.

- **\$R[random].extension:** This is the **contents file**. It stores the actual data of the deleted file. If you restore a deleted file, Windows uses the information in the **\$I** file to put the data from the **\$R** file back where it belongs.

Even if the Recycle Bin has been emptied, these \$I and \$R files can persist in unallocated space or within a forensic image. The data in the \$RecycleBin can be accessed from **Data_Leak\cfreds_2015_data_leakage_pc\D\\$Recycle.Bin\S-1-5-21-2425377081-3129163575-2985601102-1000**

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

| Name | Last Written |
|--------------------------|--|
| \$IX538VH.jpg | 03/24/15 04:11:42 PM (-4:00 Eastern Daylight Time) |
| \$IXWGVWC | 03/24/15 03:51:47 PM (-4:00 Eastern Daylight Time) |
| Chrysanthemum.jpg | |
| Desert.jpg | |
| desktop.ini | 03/22/15 10:34:46 AM (-4:00 Eastern Daylight Time) |
| desktop.ini | 03/24/15 03:57:20 PM (-4:00 Eastern Daylight Time) |
| Hydrangeas.jpg | |
| IE11-Windows6.1-x64-e... | |
| IE11-Windows6.1-x64-e... | |
| Jellyfish.jpg | |
| Koala.jpg | |
| Lighthouse.jpg | |
| Penguins.jpg | |

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

Answer:

- Path:**

Data_Leak\cfreds_2015_data_leakage_pc\D\Users\informant\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\ccc0fa1b9f86f7b3.customDestinations-ms\Jump list for (ccc0fa1b9f86f7b3)\Link @ 36.lnk

| Timestamp (EST) | Description |
|--------------------------------|---|
| 2015-03-25 10:46:44 | anti-forensic tools |
| 2015-03-25 10:46:54 | eraser |
| 2015-03-25 10:47:34 | http://iweb.dl.sourceforge.net/project/eraser/Eraser%206/6.2/Eraser%206.2.0.2962.exe |
| 2015-03-25 10:47:51 | ccleaner |
| 2015-03-25 10:48:12 | http://www.piriform.com/ccleaner/download |
| 2015-03-25 10:50:14 | \USERS\INFORMANT\Desktop\DOWNLOAD\ERASER 6.2.0.2962.EXE |
| 2015-03-25 10:57:56 | \USERS\INFORMANT\Desktop\DOWNLOAD\CCSETUP504.EXE |
| 2015-03-25 11:13:30 | \PROGRAM FILES\Eraser\Eraser.exe |
| 2015-03-25 11:13:39 ~ 11:14:44 | \User\Informant\Desktop\Temp\Chrysanthemum.jpg \User\Informant\Desktop\Temp\Desert.jpg \User\Informant\Desktop\Temp\Hydrangeas.jpg \User\Informant\Desktop\Temp\IE11-Windows6.1-x64-en-us.exe \User\Informant\Desktop\Temp\Jellyfish.jpg \User\Informant\Desktop\Temp\Koala.jpg \User\Informant\Desktop\Temp\Lighthouse.jpg \User\Informant\Desktop\Temp\Penguins.jpg \User\Informant\Desktop\Temp\Tulips.jpg \User\Informant\Desktop\Temp\Tulips.jpg \User\Informant\Desktop\Temp\ |
| 2015-03-25 11:15:45 | \Users\informant\Desktop\Download\ccsetup504.exe \Users\informant\Desktop\Download\Eraser 6.2.0.2962.exe |
| 2015-03-25 11:15:50 | \PROGRAM FILES\CCLEANER\CCLEANER64.EXE |
| 2015-03-25 11:18:29 | \PROGRAM FILES\CCLEANER\UNINST.EXE |

The screenshot shows two windows from a forensic analysis tool. The top window is a table view titled 'Table' with columns 'Name' and 'Last Written'. It lists six entries, each with a checkbox, a file name, and a path: 'Link @ 6761.lnk' (Data_Leak\cfreds_2015_data_leakage_pc\D\U\), 'Link @ 5128.lnk' (Data_Leak\cfreds_2015_data_leakage_pc\D\U\), 'Link @ 36.lnk' (Data_Leak\cfreds_2015_data_leakage_pc\D\U\), 'Link @ 3481.lnk' (Data_Leak\cfreds_2015_data_leakage_pc\D\U\), 'Link @ 1840.lnk' (Data_Leak\cfreds_2015_data_leakage_pc\D\U\), and 'Link @ 1687.lnk' (Data_Leak\cfreds_2015_data_leakage_pc\D\U\). The entry 'Link @ 36.lnk' is selected. The bottom window is a hex editor showing the raw data of a file named 'ProgramFiles%CCleaner64.exe'. The file's header is visible, including the string 'ProgramFiles%CCleaner64.exe'. The right side of the hex editor has a sidebar with options like 'Decode', 'High ASCII', 'Text', etc.

This information suggests that the forensic investigator is examining the \$UsnJrnl (Update Sequence Number Journal) file to identify traces of the Eraser tool being used to wipe files.

- **\$UsnJrnl:** This is a system file in NTFS that logs file system activities, including file creation, deletion, renaming, and attribute changes. It's a valuable resource for forensic investigations.
- **Eraser:** This is a secure data removal tool that overwrites files with random data to make them unrecoverable.
- **How Eraser Works:** Eraser uses a specific process to wipe files:
 1. **Renames the target file:** It changes the file's name to a random string of bytes.
 2. **Fills with random data:** It overwrites the file's contents with random data multiple times, making it extremely difficult to recover the original data.
- **Wiping Traces in \$UsnJrnl:** Even though Eraser aims to securely delete files, it leaves traces of its activity in the \$UsnJrnl. These traces can be identified by analyzing the journal entries.

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

Answer: During the forensic analysis of the RM#2 drive, the traces of directories like DESIGN\, pricing decision, PROGRESS, PROPOSAL, technical review\ were recovered from the unallocated cluster of the USB drive through HEX analysis.

The screenshot shows a digital forensics environment with multiple panes. The top-left pane displays a tree view of 'Entries' under 'cfreds_2015_data_leakage_rm#2'. The main pane is a table titled 'Table' showing file details like Name, Last Written, and Path. The table includes rows for 'Volume Boot', 'Unallocated Clusters', 'Secondary FAT', 'Primary FAT', and 'IAMAN \$._@'. The bottom-left pane shows a hex dump of a file, and the bottom-right pane shows a 'High ASCII' dump with some text visible.

| Name | Last Written | Path |
|----------------------|-----------------------------------|--|
| Volume Boot | | Data_Leak\cfreds_2015_data_leakage_rm#2\Volume Boot |
| Unallocated Clusters | | Data_Leak\cfreds_2015_data_leakage_rm#2\Unallocated Clusters |
| Secondary FAT | | Data_Leak\cfreds_2015_data_leakage_rm#2\Secondary FAT |
| Primary FAT | | Data_Leak\cfreds_2015_data_leakage_rm#2\Primary FAT |
| IAMAN \$._@ | 03/24/15 05:02:36 PM (Local Time) | Data_Leak\cfreds_2015_data_leakage_rm#2\IAMAN \$._@ |

54. What actions were performed for anti-forensics on USB drive 'RM#2'?

[Hint: this can be inferred from the results of Question 53.]

55. What files were copied from PC to USB drive 'RM#2'?

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

How to determine proper filenames of the original files prior to renaming tas

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

58. Create a detailed timeline of data leakage processes.

Answer: Let's break down this case to create a concise and structured timeline of the data leakage processes:

Phase 1: Reconnaissance and Preparation (March 22nd - 23rd)

- Normal Business Works (March 22nd):** The suspect appears to be engaged in typical work activities, installing software (Microsoft Office, Internet Explorer, Google Chrome) and setting up accounts (email, user accounts). This could be a cover for establishing the infrastructure needed for later data exfiltration.
- Researching Data Leakage Methods (March 23rd, 14:01 - 14:21):** The suspect performs extensive web searches related to data leakage, cloud storage, anti-forensics, and data recovery. This indicates an active effort to learn about techniques for exfiltrating and concealing data.

Phase 2: Initial Data Exfiltration (March 23rd)

- Accessing and Copying Confidential Data (March 23rd, 14:31 - 14:41):** The suspect connects a USB drive ("RM#1"), searches for confidential files using

keywords, and copies those files to their local machine. They then rename the files and their extensions to obfuscate their content.

- **Emailing Data and Links (March 23rd, 14:44 - 16:43):** The suspect sends emails to an external address (spy.conspirator@nist.gov) with messages indicating successful data acquisition. They also upload files to Google Drive and share links to those files via email. Later, they delete the files from Google Drive, possibly to remove evidence.

Phase 3: Expanding Exfiltration and Anti-Forensics (March 24th)

- **Copying More Data (March 24th, 09:38 - 10:07):** After further communication with the external address, the suspect copies more confidential files from a USB drive ("RM#1") and a network share to their local machine. They rename the files and copy them to another USB drive ("RM#2"). They then delete the files from their local machine using "Shift + Delete" to bypass the Recycle Bin.
- **CD-R Burning and Anti-Forensics (March 24th, 15:38 - 17:06):** The suspect practices burning files to a CD-R, copies confidential files to a CD-R with renamed directories, and then formats the CD-R. They burn another copy of the files to a second CD-R ("RM#3") and delete the files from the CD-R. They also format the USB drive ("RM#2") and perform web searches related to CD-R security checkpoints, likely researching ways to avoid detection.

Phase 4: Cleanup and Final Actions (March 25th)

- **Anti-Forensic Activities (March 25th, 10:46 - 11:28):** The suspect downloads and installs anti-forensic tools (Eraser, CCleaner), deletes emails from Outlook, wipes the temporary directory used for CD-R burning, empties the Recycle Bin, uninstalls the anti-forensic tools, logs out of Google Drive, and cleans up their desktop.
- **Resignation and Departure (March 25th, 11:28 - 11:30):** The suspect creates and prints a resignation letter, then shuts down the system and attempts to leave with the USB drive ("RM#2") and the CD-R ("RM#3").

Key Observations:

- **Escalation:** The suspect's actions escalate from seemingly normal work to deliberate data exfiltration and sophisticated anti-forensic activities.
- **Multiple Methods:** The suspect uses a variety of methods to transfer data (email, cloud storage, USB drives, CD-Rs).
- **Obfuscation and Evasion:** The suspect employs renaming, formatting, and secure deletion to hide their actions and evade detection.

- **Anti-Forensics:** The suspect actively uses anti-forensic tools and techniques to remove traces of their activities.

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

Answer: This data presents a breakdown of the suspect's activities related to potential attempts to transfer confidential data. Multiple approaches were used to transfer the data. Here's a systematic analysis:

1. Network Transmission

- **Email:**
 - **2015-03-23 15:19:** The suspect sent an email with the file space_and_earth.mp4 attached. This suggests potential transfer of a video file via email.
 - **2015-03-23 16:38:** The suspect sent another email containing links to files shared on a cloud storage service. This indicates the suspect might be sharing files indirectly through cloud storage rather than attaching them directly to the email.
- **Cloud Storage Services:**
 - **2015-03-23 16:32:** The suspect uploaded files named happy_holiday.jpg and do_u_wanna_build_a_snow_man.mp3 to a cloud storage service. This implies the use of cloud storage for storing and potentially sharing files.

2. Storage Devices

- **USB Flash Drive:**
 - **2015-03-24 09:58 ~ 10:00:** The suspect copied files, including winter WHETHER_advisory.zip, to a USB flash drive. This suggests the use of a physical storage device for data transfer or storage.
 - **Formatted Partition:** The suspect formatted the partition on the USB drive, likely in an attempt to erase the data. However, the files still exist in the unused area of the drive, indicating incomplete data erasure. This could be crucial evidence.
- **CD-R:**
 - **2015-03-24 16:54 ~ 16:58:** The suspect burned 17 files, including winter WHETHER_advisory.zip, onto a CD-R. This indicates the use of optical media for data storage or transfer.

- **Deleted Files:** The suspect attempted to delete confidential files from the CD-R. However, these files persist in the unused area of the disc, suggesting incomplete erasure and potential evidence recovery.

Forensic Implications:

- **Data Exfiltration:** These activities point to potential data exfiltration, where the suspect is attempting to transfer sensitive data outside of the organization's control.
- **Anti-Forensics:** The attempts to format the USB drive and delete files from the CD-R suggest anti-forensic activities aimed at hindering the investigation.
- **Data Recovery:** The presence of files in the unused areas of the USB drive and CD-R indicates the possibility of data recovery using forensic techniques.

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

Answer: Here is the visually structured timeline infographic of the data leakage event across the specified phases. Let me know if you'd like any adjustments.

