The Knowledge Hub Universities | partnered with Coventry University

School of Computing

[KH5036CMD]

Digital Forensic Expert Opinion

Investigation Report

Case Against: Informant: IAMAN

Case No: 1

Report compiled by Hala Ahmed | 2300277| 14762750 | Coventry EHACS Student

Dr. Haitham Ghalwash | Dr. Kareem ElDebassy

Coventry University Forensics Lab

Date of investigation 26/ 11/2025

Date report compiled 3/12/2025

Endorsement

The contents of this report are the result of an investigation undertaken by myself, and I hereby confirm that:

1. The investigation was conducted in accordance with the **UK ACPO principles**.
2. The software and hardware used to support this investigation were prepared and used in a manner designed to assure the forensic integrity of both the process and its outcomes.
3. The **opinions** presented at the end of this report are mine and mine alone and are based solely on the evidence found.

Signed by Hala Ahmed **[Hala Ahmed]**

Date **[3/12/2025]**

Executive Summary

Digital forensics is the process of digitally investigating a specific case to reach an outcome: either for incident response processes or court processes (Badman & Forrest, 2025). Therefore, any suspicious activity leads to a case; where the investigator follows some standard procedures to transform found artifacts, traces, into well trusted evidence. This report documents the process of investigation on a suspicious case, highlighted through the user's unusual behaviour on the suspect's workstation.

The employee named Iaman is suspected of data leakage; therefore, a 20GB windows disk image was statically acquired, on 16/11/2025 02:29 AM by Dr. Haitham and Dr. Kareem, for a strict digital forensics analysis, started at 24/11/2025 by Hala Ahmed, where forensics tools and python scripts were used for analysis. The investigation focused on determining whether the user had access to unauthorized data or not and whether the user transferred or leaked any confidential information.

After the analyses, the traces on the suspect's pc indicated that the user is a malicious insider actor, leaking confidential data. Artificats such as encrypted files, files with mismatched extensions, file sharing directories, suspicious running process and finally web components and email all indicated an extremely abnormal behaviour highlighting the unworking hours.

Moving forward, the actual evidence found was mostly through his web interaction, email, and files. Concluding, the evidence, artifacts, analyses, and logic flow all proved the informant's malicious intent and disgruntles to the entity, resulting in leaking its confidential data.

Analysis Result:

- positive suspicion: Iaman leaked data

Contents

s

1. Credentials of the Investigator

This report is presented to you by the upcoming investigator Hala Ahmed Sayed. Hala Ahmed is a year 5 ethical hacking and cybersecurity student at Coventry university. Hala has a 2-year experience in the cyber security field with almost 5 months experience in digital forensics. Qualified in university courses, extracellular courses, and internships, hala is equipped with the necessary knowledge and hands on experience to perform a structured and deep digital forensic investigation.

LinkedIn Link: https://www.linkedin.com/in/hala-ahmed-87b24a210/

ID: 202300277 | 14762750

2. Objectives and Scope of Work

This report aims to portray the technical digital forensics analysis of a 20GB Disk Image, highlighting any artifacts found and the tools used. In addition to, it finalizes the case, reports the whole incident, summarizes the incident's analysis flow, and identifies the malicious user.

3. Deliverables

As mentioned previously, this report aims to document the deep analysis results performed on the given disk image. Therefore, the deliverables of this part consist of a digital forensic expert opinion investigation report for the given case.

4. Introduction

This report is a technical based project presented as a business report, where a suspicious 20GB disk image is taken from a user and goes under a strict digital forensics analysis to investigate the suspicious behaviour done on the user's PC. As studied, digital forensics is the process of digitally investigating a specific case to reach an outcome: either for incident response processes or court processes (Badman & Forrest, 2025); therefore, any suspicious activity leads

to a case, where the investigator follows standard procedures to transform found artifacts into well trusted evidence. Consequently, this project tackles and documents the process of a suspicious case, highlighted through the user's suspicious behaviour on the PC, which revolves around leaking a company's sensitive data, disregarding the data's CIA, the company's policies, and global standards. By following the digital forensics procedures, using Python scripts and the help of forensic tools, this report investigates the 20GB disk image thoroughly, analysing multiple areas such as registries, user behaviour, file system and application usage, partitions, browsers, emails, and more, while providing technical, detailed documentation along with the tools, flow, evidence, and methodology used in a business report format.

5. Case Background

As per the digital forensics process, the case almost went through identification, preservation, and acquisition already. Based on the initial information given, the case seems to be about an identified internal employee in an entity where the employee or user, in this case, is suspected of leaking the entity's sensitive information. Therefore, a full image was taken from the user's disk which is a static acquisition method, making the focus of this project analysis and reporting. The original image size is 20GB; however, the zipped image file is 5GB. Using the hashes method, the image was checked for its integrity then analysis took place. For more clarification, the investigation process and methodology will be mentioned in the upcoming report section.

6. Target Systems and Devices

The target system is 20GB disk image taken from the suspected employee's pc which belongs to the entity's system. It is a windows 7 machine with NTFS file system. Therefore, the investigation is done on involatile data; consequently, this investigations boundary consists of any volatile data: network, memory, ram, etc.

7. Investigation Methodology

- ### Identification

Physical Identification Assumption:

According to the behaviour of the user, the entity identified the user as a potential suspicious user by various assumed indicators: unfamiliar interactions with competitors, exclusive access to sensitive data, escalation privileges indicators, physical access and handling of the entity's storage devices, or any behaviour that may have a negative impact on the data or reputation of the entity. These observations result in a triggered decision of an official digital forensic investigation.

Digital Forensics Identification:

The user's powered off pc was identified as an evidence source. A raw data image in a .dd extension was taken from the user's pc.

- ### Preservation

As an evidence source was found, Dr. Haitham and Dr. Kareem documented the evidence source, the time, and the location of it. The evidence source was the informant's pc, the location was the entity's workstation, and the date and time were on 16/11/2025 after midnight: in the range of 12 till 2:28 AM. Exact details are documented in the chain of custody, found in the upcoming sections.

- ### Collection

The evidence source which is the pc was found powered off; therefore, the disk was fully and statically acquisitioned by Dr. Haitham and Dr. Kareem on 16/11/2025 02:29 AM. The acquisition process followed all the standards, such as the ACPO, and ethical considerations, while still being documented in the chain of custody.

- Examination and Analysis

For accuracy, the disk image taken went through deep analysis where it was verified that the image is not corrupted. Then analysis on core areas such as the operating system, files, web activity, email and browser were performed. After the analyses was done, it is decided if the user is at fault or not.

- Documentation

In this step, Hala which is this case's investigator wrote a technical report where the documentation of the analyses, the processes followed, the specific accessed information, etc were all reported. This report then was submitted to Dr. Haitham and Dr. Kareem for a quick analysis before submitting an official opinionated report, ensuring accuracy.

- Reporting

This report is the official digital forensics report, where it presents the flow of the incident, the analysis, and the final findings of the case. As the report aims for transparency and compliance, it offers the entity a finalized picture what happened, how, where, when and who.

8. Chain of custody

Coventry Police Department

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Field	Details
Case Number	1
Offense	Data Leakage
Submitting Officer	Hala Ahmed (ID: 202300277)
Victim	Entity
Suspect	Employee / Informant
Date/Time Seized	16/11/2025 at 02:29 AM
Location of Seizure	The Knowledge Hub

Description of Evidence		
Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)
1	1	20GB Raw Disk Image: static acquisition, excellent condition

Chain of Custody				
Action	Date/Time	Done by (Signature & ID#)	Received by (Signature & ID#)	Status
Disk Image Static Acquisition	16/11/2025 02:29 AM	Dr. Kareem EL Debassy Dr. Haitham Ghalwash	Hala Ahmed | 2300277	Normal
Downloaded the zipped file image	24/11/2025 9:09 pm	Hala Ahmed | 2300277	-	Normal
Extracted the zipped file image	24/11/2025 11:28pm	Hala Ahmed | 2300277	-	Normal
FTK Hash Verification	25/11/2025 2:23am	Hala Ahmed | 2300277	-	Normal
Manual Hash Comparison	25/11/2025 2:30am	Hala Ahmed | 2300277	-	Normal
Quick FTK Manual Analysis	25/11/2025 2:42 am	Hala Ahmed | 2300277	-	Normal
PowerShell Hash Comparison	25/11/2025 3:00 am	Hala Ahmed | 2300277	-	Normal
Autopsy Mounting	25/11/2025 3:10-3:50	Hala Ahmed | 2300277	-	Normal
Autopsy Case Creation	25/11/2025 4:50 am	Hala Ahmed | 2300277	-	Normal
Autopsy Quick General Analysis	25/11/2025 8:00am	Hala Ahmed | 2300277	-	Moderate

Technical Working Group on Biological Evidence Preservation. *The Biological Evidence Preservation Handbook: Best Practices for Evidence Handlers*. U.S. Department of Commerce, National Institute of Standards and Technology. 2013.

Disk Editor Partition Analysis	25/11/2025 10:00am	Hala Ahmed	2300277	-	Normal
Registry Viewer: Hives Analysis	25/11/2025 3:00pm	Hala Ahmed	2300277	-	Moderate
Autopsy User List Analysis	25/11/2025 3:30pm	Hala Ahmed	2300277	-	Normal
Python Script Task 1 Done	25/11/2025 5:00pm	Hala Ahmed	2300277	-	Normal
Autopsy Web Browser Analysis	25/11/2025 6:48pm	Hala Ahmed	2300277	-	Suspicious
Autopsy Email Client Analysis	25/11/2025 6:58pm	Hala Ahmed	2300277	-	Normal
Software Hive Analysis	25/11/2025 7:10pm	Hala Ahmed	2300277	-	Suspicious
Linked Email Account Analysis	25/11/2025 7:20pm	Hala Ahmed	2300277	-	Suspicious
MRU Analysis	25/11/2025 8:00pm	Hala Ahmed	2300277	-	Suspicious
NTUSER.DAT Analysis	25/11/2025 8:12pm	Hala Ahmed	2300277	-	Suspicious
Security.evtx Analysis	25/11/2025 11:35pm	Hala Ahmed	2300277	-	Suspicious
Command Line Activity Analysis on Security.evtx, NTUSER and Autopsy	26/11/2025 12:00 am	Hala Ahmed	2300277	-	Suspicious
USB Analysis Done Autopsy	26/11/2025 8:00am	Hala Ahmed	2300277	-	Suspicious
Mail Analysis Done Autopsy	26/11/2025 8:30am	Hala Ahmed	2300277	-	Malicious
Cloud Analysis Done Autopsy	26/11/2025 8:50am	Hala Ahmed	2300277	-	Malicious
Web Analysis Done	26/11/2025 9:15am	Hala Ahmed	2300277	-	Suspicious
Python Script Task 2	26/11/2025 10:00am	Hala Ahmed	2300277	-	Moderate
File Analysis Done Autopsy	26/11/2025 2:00pm	Hala Ahmed	2300277	-	Malicious
Browser History Analysis Done Autopsy	26/11/2025 3:13pm	Hala Ahmed	2300277	-	Malicious
Email Analysis Done Autopsy	26/11/2025 8:00pm	Hala Ahmed	2300277	-	Malicious
Shared Files Analysis Done Autopsy	26/11/2025 8:43pm	Hala Ahmed	2300277	-	Malicious
Shared Files Analysis Done Autopsy	26/11/2025 11:00pm	Hala Ahmed	2300277	-	Malicious
Technical Report	26/11/2025 11:59pm	Hala Ahmed	2300277	Dr. Kareem, Dr. Haitham	Normal
Business Report	4/12/2025 11:59pm	Hala Ahmed	2300277	Dr. Kareem, Dr. Haitham	Normal

Illustrations 1,2: documents the case's digital forensics process

9. Evidence

As mentioned previously, the only tangible evidence was the disk image. Therefore, the disk image went through integrity verifications (using the hash values) and then deep forensics analysis where every component was analysed, documented, and related to the case.

Notes:

- The digital forensics image was verified, containing a hash of "a49d1254c873808c58e6f1bcd60b5bde" for the MD5 hash algorithm and "afe5c9ab487bd47a8a9856b1371c2384d44fd785" for the SHA1 hash algorithm.
- The table below shows the evidence details where it contains the evidence ID, evidence item, description, and quantity.

Evidence ID	Evidence Item	Description
1	Disk Image	Physical image of Informant's pc: 1
2	Registry Hives	SAM, SYSTEM, SOFTWARE, NTUSER.DAT files
2A	Registry Hives Traces	1. Users on the system: 6 2. Installed web browsers: 2 3. Email clients: 2 4. Linked email accounts: 2 5. Most Recently Used: 46 documents and 95 running programs 6. anti-forensics apps and executable files: 3 7. Secret Folder: 1 8. Resignation letter model: 1
3	User Behavior Retracement Traces	1. Non-working hours log in 2. Privilege escalation access
4	Unauthorized Data Access	1. USBS detection: 16 & 2 physical 2. Mail: 2 clients and 2 accounts 3. Cloud: 2
5	Web Activity	1. Chrome, IE history: many 2. Bookmarks referencing leakages: many

		3. Suspicous Cache file behavior: many 4. Anti-forensics, theft, and malicious methods documents: many 5. Websites documents: many 6. Unethical URLS: many 7. Executable malicious files: 4
6	Email Client Data	1. Outlook Files 2. Outlook ongoing Emails: 14 3. Synchronization logs: 2
7	File Activity	1. Encrypted Files: 13 2. Extension mismatched files: 77 3. Anti-forensics documents and tools: many 4. Virtual machine set up: 1
8	Recycle Bin Files	1. Deleted items stored in the Recycle.Bin: 10 2. Executable files: 2
9	Cloud Artifacts	1. iCloud and Google Drive are both used, but cant access them because of outdated version. 2. Synchronization logs: 2

10. The Forensic Workstation and Examination Tools

The forensic workstation in this project is the secure and isolated investigator's, hala, computer environment where the given DD disk image is analysed on. The laptop is from Excalibur: a gaming laptop brand; it is considered a gaming laptop with an SSD disk, windows 10 operating system, NTFS file system, and 2 allocated partitions. It was configured to avoid any alteration of the original evidence and contained the original license and tools needed to perform the required forensic tasks like Autopsy to examine the disk's data, hashing tools to detect integrity violations, and registry tools to investigate the hives files. All the tools used are listed with their usage below.

No.	Tool	Usage
1	FTK Imager	Automatic hash checking and quick manual analysis
2	PowerShell	Hash checking
3	Visual Studio	Writing and running Python scripts
4	Autopsy	Full analysis of all evidence
5	Registry Viewer	Registry hive analysis

6	Event Viewer	Security.evtx file analysis
7	Disk Editor	Disk and partition analysis
8	GitHub	Code version control
9	Microsoft Office	Report preparation

Tables 1,2: showcases the evidence and tools used and analysed

11. Evidence Analysis

Introduction: pc's components

As the analyses of the disk is done, it was found that the user is guilty through various evidence. Starting with the operating system, it was found that the user's pc, named informant pc, is a windows 7 operating system with an eastern standard time, a NTFS file system, and a disk, divided into 4 MBR partitions: 2 unallocated and 2 allocated. The 2 allocated partitions were divided on the operating system files and the data itself.

Registry Files:

Moving forward, the registry files or systems files were analysed, extracting the number users which is 6, the installed web browsers and email clients which contained google chrome, internet explorer, outlook, and windows email. As email clients were found, the case went through linked email accounts which showed two emails: iaman.informant@nist.gov.ost and spy.conspirator@nist.gov; these emails indicated data leakage. After this suspicion, the running processes were checked to confirm if Iaman is sending or just receiving an intentional malware. On the case time interval which is from 22 of march till 25th 2015, there is 46 recent documents and 95 run programs. The suspicious behaviour revolved around the secret project folder and the resignation letter document. The secret project folder consists of pricing decisions, design concept, proposal, and final meeting ppt. All these documents seem to be work related documents that are saved in folder called "secret", indicting a suspicious behaviour from the user. Regarding the running programs on 25/3/2025, some programs were

unsuspicious such as chrome, Microsoft office components, system files. On the other hand, there were suspicious programs such as eraser, cleaner and “DEVICEDISPLAYOBJECTPROVIDER.E" which took place starting from 24/3/2015 at 23:02:47 till 25/3/2015 at 17:13:30.

Note:

Based on the previous analyses, it was highlighted that the user is not satisfied with his job which was highlighted through the resignation document; therefore, the possibility of him committing this leakage is higher. Consequently, the user behaviour is retracted and analysed.

User Behaviour Retracement

Under suspicion, the user’s pc went under analyses for user behaviour retracement which contained logging in and logging out, command line activity, application and file usages, and signs of unauthorized data access. This step was done to confirm the leakage’s time to help in the investigation process by narrowing it down. After filtering the user’s access logs, there are 3 main logs related to the task: logon, logoff, special logon. Special logon is logon log but with higher privileges. There are 4 days in the logs: 22nd, 23rd, 24th and 25th of march, 2015; each day contained all the 3 types of logouts mentioned. The user was found accessing the system and expanding his privileges in non- working hours. The table below highlights the exact access type, time and logout time.

Date	Logon (4648) Time Range	Logoff (4634/4647) Time Range	Special Logon (4672) Time Range
3/22/2015	4:34:28 PM – 5:57:54 PM	4:38:15 PM – 6:00:08 PM	4:34:24 PM – 5:45:45 PM
3/23/2015	7:24:41 PM – 11:23:27 PM	11:02:53 PM	7:24:24 PM – 10:01:02 PM
3/24/2015	3:21:44 PM – 8:28:38 PM	8:28:38 PM – 11:07:25 PM	3:21:36 PM – 10:58:52 PM
3/25/2015	3:06:08 PM – 4:45:59 PM	4:45:59 PM – 5:30:57 PM	12:15:37 PM – 5:18:54 PM

Table 3: documents the user pcs' accessing process

Unauthorized data access:

After these traces especially the privilege escalation, the pc went under data transfer analysis where the USBS, mails and cloud were analysed. Using the same time intervals from 22nd till 25th, 16 USB devices were detected. The USBS detected are divided into 2: virtual and physical. The 2 physical USBS found belong to SanDisk and they were last accessed on 24/3/2015 at 21:38:09 EET and 15:38:00. The virtual devices are virtual USB Hub and virtual mouse; these are considered hardware in a virtual machine. Moving forward, there were 14 emails sent in the time range settled for the case: from 23/3/2015 at 19:29:29 EET till 25/3/2015 at 17:01:55pm. All the emails are between the 2 linked accounts already mentioned, Iaman and the spy, and the body of the emails confirms data leakage as emails are asking for data and different data transfer methods including USBS, cloud: google drive and iCloud, and email. The email scripts are provided in the exhibits section below.

File Activity:

Regarding file analysis, there are 10 deleted files stored in the recycle bin. Their extensions vary from .jpg to .ini and .exe. All the files seem suspicious as images are placed in an abnormal path which is not done except if the images or files are transferred. Additionally, there is a IE11-Windows6.1-x64-en-us.exe which is an executable file for Internet Explorer 11 installer. It should not be in this path, and it might carry malware or data as a disguise. Moving forward, a forensics information pdf from 2012 was found highlighting that the user's mindset is open to malicious acts and is aware of digital forensics including its precautions. Additionally, another file with a description of "Data Leakage -Threats and Mitigation" was found in the same case time interval: 23/3/2015 at 18:02:17 EET. In addition to, there were multiple files

with 77 mismatched extensions, 13 encrypted, and many unallocated all in the same case time interval: 22/3/2015 till 25/3/2015.

Web Activity:

Using forensics tools, the web elements including history, search and downloads are all analysed and documented in this section. The browser history consisted of suspicious URL which included deleted .exe file and data leakage cases, methods, techniques search. In addition to on 23/3/2015 at 20:02:17EET, the user also searched anti forensics techniques which shows his previous understanding in forensics as highlighted previously. Concepts including leaking methods, previous leakage cases, intellectual property theft, cloud storage (to know where the data should be transferred), anti-forensics techniques, deleting data techniques, encrypted folders, js and dll files were all searched on 22/3/2015 and implemented on his pc on different dates, but still in the case's time interval.

Moving to the web downloads, there are 9 files downloaded. 5 of them are downloaded from clouds and were also accessed during non-working hours: on 23/3/2015 with a time interval from 21:55:47 EET till 21:56:30 EET. Applications such as eraser and executable files were also downloaded which highlights the user's implementation of his search.

Email Analysis:

There are 14 emails sent and replied to from the informant and the spy. The first email documented was received from spy.conspirator@nist.gov on 23/3/2015 at 19:29:29 EET. Through the time interval of 21:15:00 till 22:41:22EET, emails are being sent from both clients. All the emails tackled data leakage files, methods (such as USBS, clouds and personal email), detection warnings, cloud links, and more information request. Additionally, the informant used a trick where he synchronizes the logs while sending data; therefore, the

sent data won't be detected which shows his malicious intent and his knowledge on digital forensics as highlighted through his downloads and search. A through script for the emails is written on notepad and is documented in the upcoming exhibits section.

Shared Files Analysis:

After concluding that the user is transferring data over the cloud, the shared files which include google drive and iCloud were analysed to view the sent documents as the synchronization trick and outdated version does not allow viewing the documents. The found documents were either allocated with no suspicious rate and unallocated with high suspicious rate. Regardless, it is proven through the email conversations that one of the data's leakage methods was through the user's drive.

12.A Graphical Timeline of the incident

Due to technical issues, the graphical timeline is converted into a table, but it still includes all the data needed with the dates.

Incident Timeline

Timestamp	Details
22 Mar 2015 – Initial Recognition	• Searches on data leakage, anti-forensics • Government website access • Encrypted folder browsing
23 Mar 2015 – First Spy Contact	• "Hello, Iaman" email received • Informant replies "Successfully secured" • Google Drive exfiltration links sent • Anti-forensics research escalates
23 Mar 2015 – System Activity	• Secret Project folder accessed • Resignation letter accessed • MRU list updated • IP theft research via browser (hiding traces method)
24 Mar 2015 – USB & Cleaner Activity	• Two SanDisk USB devices connected • Deleted files in transfer path • Presence of CCleaner / Eraser • Spy requests additional data
24 Mar 2015 –File Interaction	• VM-related files found • Encrypted files appear • Suspicious Temp folder mismatches
25 Mar 2015 – Synchronization	• Mailbox synchronization • Multiple sync events/minute • Evidence of covert email exfiltration
25 Mar 2015 – Cleanup & Hiding	• Deleted installers (IE11, RJEMT.exe) • Hidden browser cache references • Anti-forensic wiping techniques
21 Apr 2015 – Disk Image Creation	• Disk image metadata acquisition

Illustration: showcases a graphical flow of the investigators process

13.Summary and Finding in Relation to the Case.

Based on the findings in the case, the investigator, hala, believes that Iaman which is the informant is working in an entity where he's not comfortable or happy could be due to personal reasons or financial reasons. Being disgruntled was highlighted through the resignation form he had saved on his pc. Therefore, the first point is that he's not happy and wants to leave. Moving forward to the leakage evidence found, it is also relational with his environment. It is not known if the user gets money from leaking the data or better work experience, but in any case, the user gets gifted for leaking the data. This satisfies the user's psychology and physical needs which makes him happy, but unethical and a traitor. Concluding, Iaman, the entity's informant, is intentionally leaking confidential data to a spy through various data transfer which includes USBS, emails, clouds and lastly directly from the server; to gain more money, the informant did not comply with the entity's policies, global standards and regulations and finally the ethical human mindset. Please be noted that the informant retrieved the resignation paper he did on 24/3/2015 at 8:00 pm which is after his conversation with the spy on their last request.

This indicts guilt and fear; therefore, this report is presented to you without any escalation processes; however, upon your approval, any legal action towards Iaman could be taken.

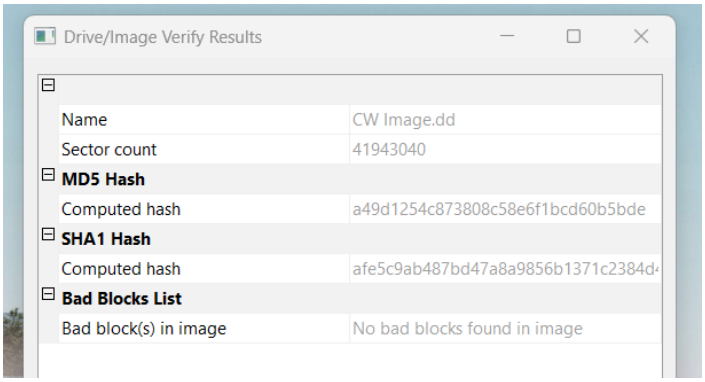
14. References

1. Badman, A., & Forrest, A. (2025, November 17). *What is digital forensics?* IBM. https://www.ibm.com/think/topics/digital-forensics
2. Editor, C. C. (n.d.-b). *Chain of custody - glossary: CSRC*. CSRC Content Editor. https://csrc.nist.gov/glossary/term/chain_of_custody
3. Special logon. What2Log. (n.d.). https://what2log.com/windows/logs/win10speciallogon/
4. nist.gov. (2015, June 5). Data leakage case. CFReDS. https://cfreds-archive.nist.gov/data_leakage_case/data-leakage-case.html

15. Exhibits

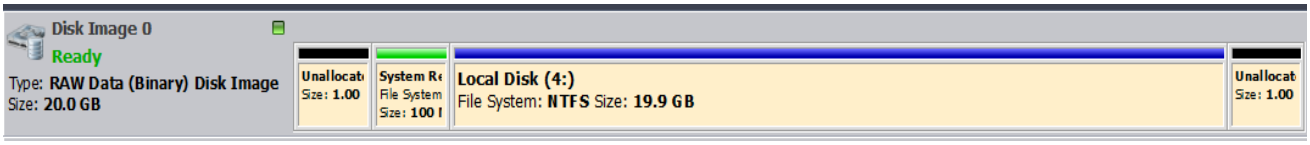
In this section, all the screenshots and visual evidence is presented for each section.

1. Image Hash Verification:



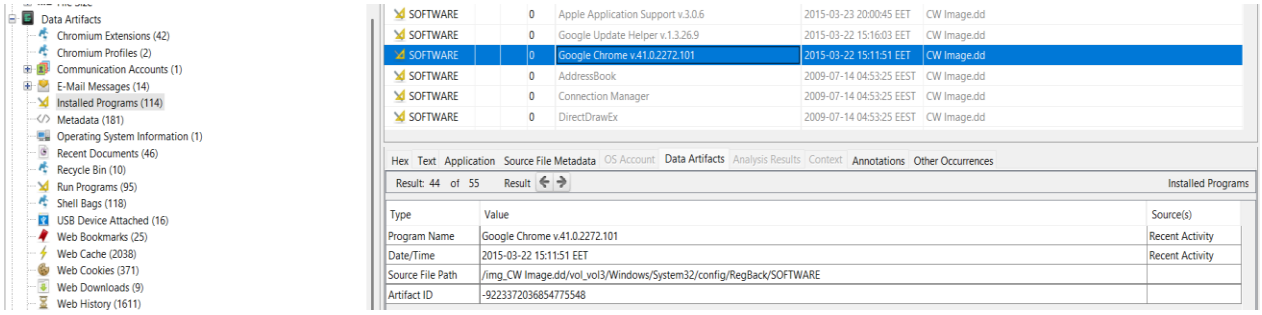

```
PS C:\Users\HALA AHMED> Get-FileHash "C:\Users\HALA AHMED\Desktop\year 2\sem 1\Digital Forensics\CW Disk Image\CW Image.dd" -Algorithm MD5

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             A49D1254C873808C58E6F1BCD60B5BDE                                       C:\Users\HALA AHMED\Desktop\year 2\sem 1\Digital Forensics\CW Dis...
```

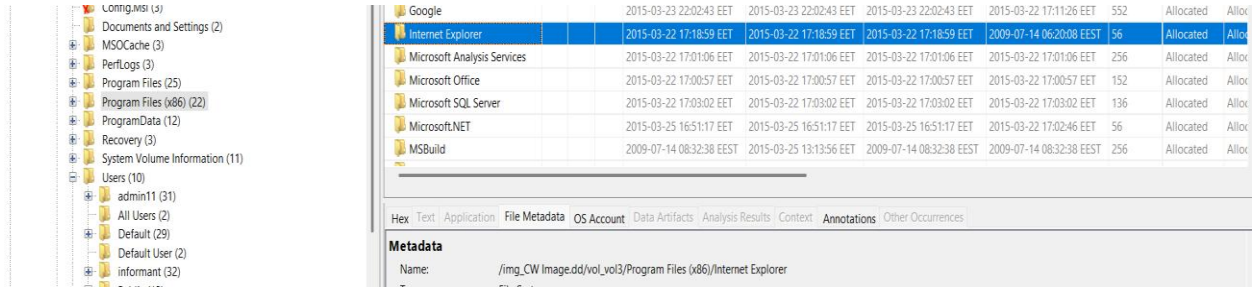
2. Disk Analysis



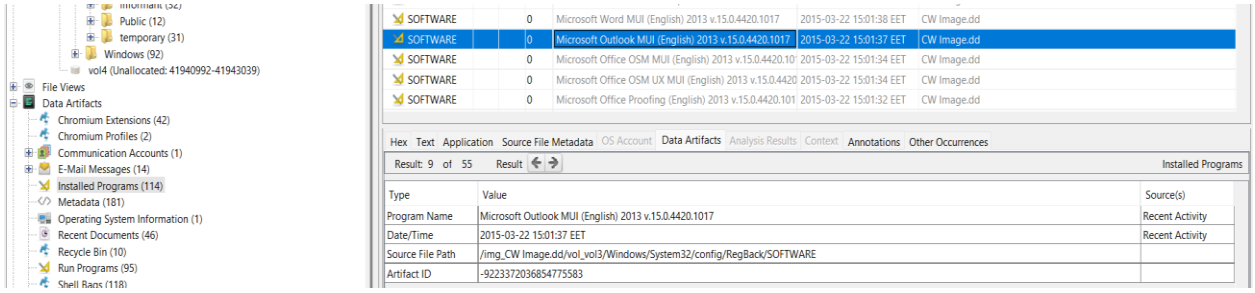
Partition	Bootable	Type (Hex)	Start Sector	Total Sectors	Start Offset (bytes)	Approx Size
1	True	0x07	2048	204800	1,048,576	0.10 GB
2	False	0x07	206848	41,734,144	105,906,176	19.90 GB
3	False	0x00	0	0	0	0.00 GB
4	False	0x00	0	0	0	0.00 GB

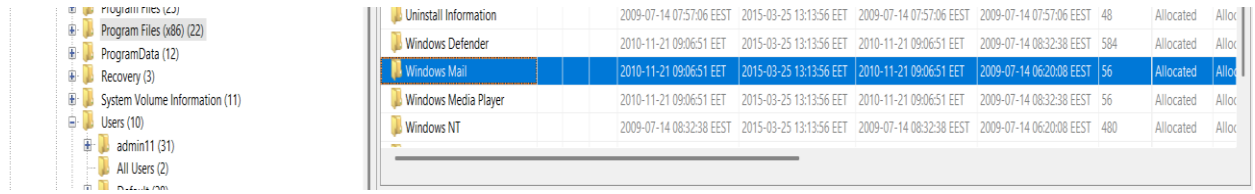
3. Web Browsers



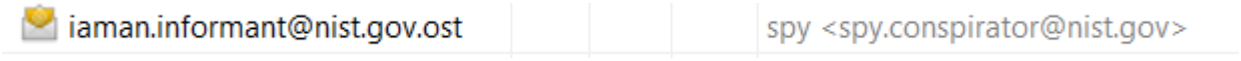


4. Email Clients

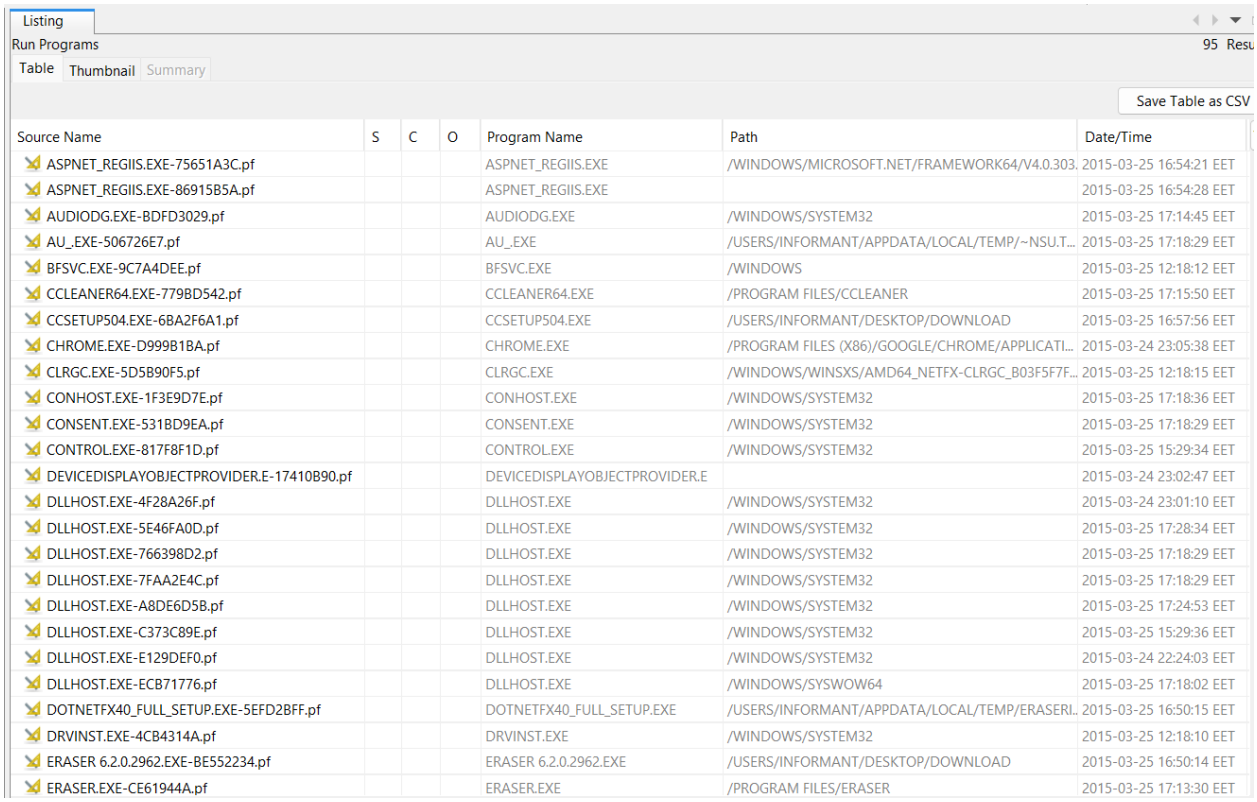




5. Linked Email Accounts:

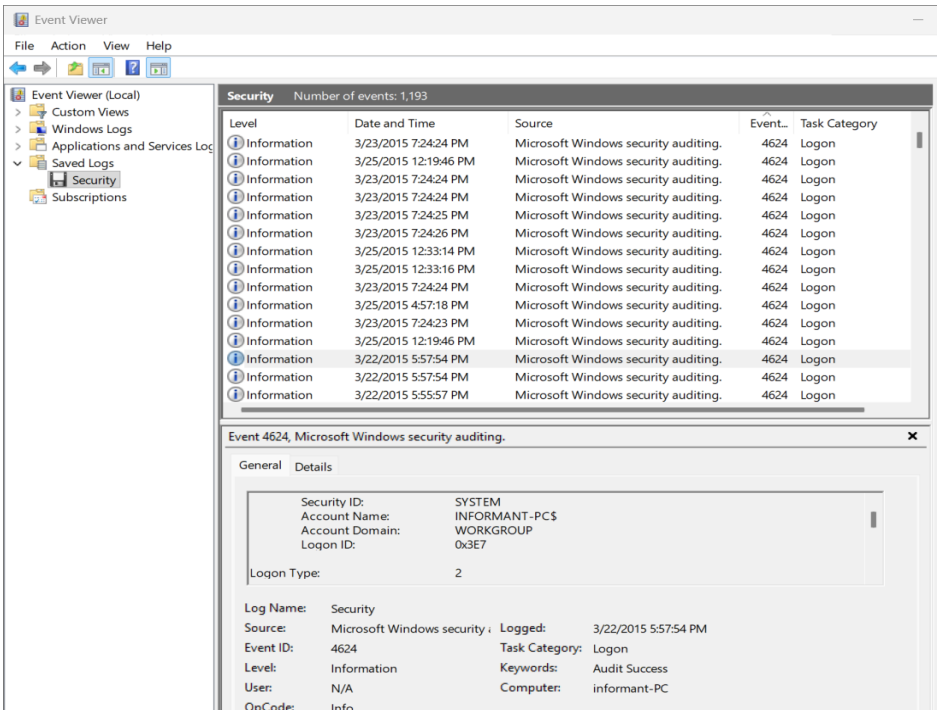


6. Running Process and MRU

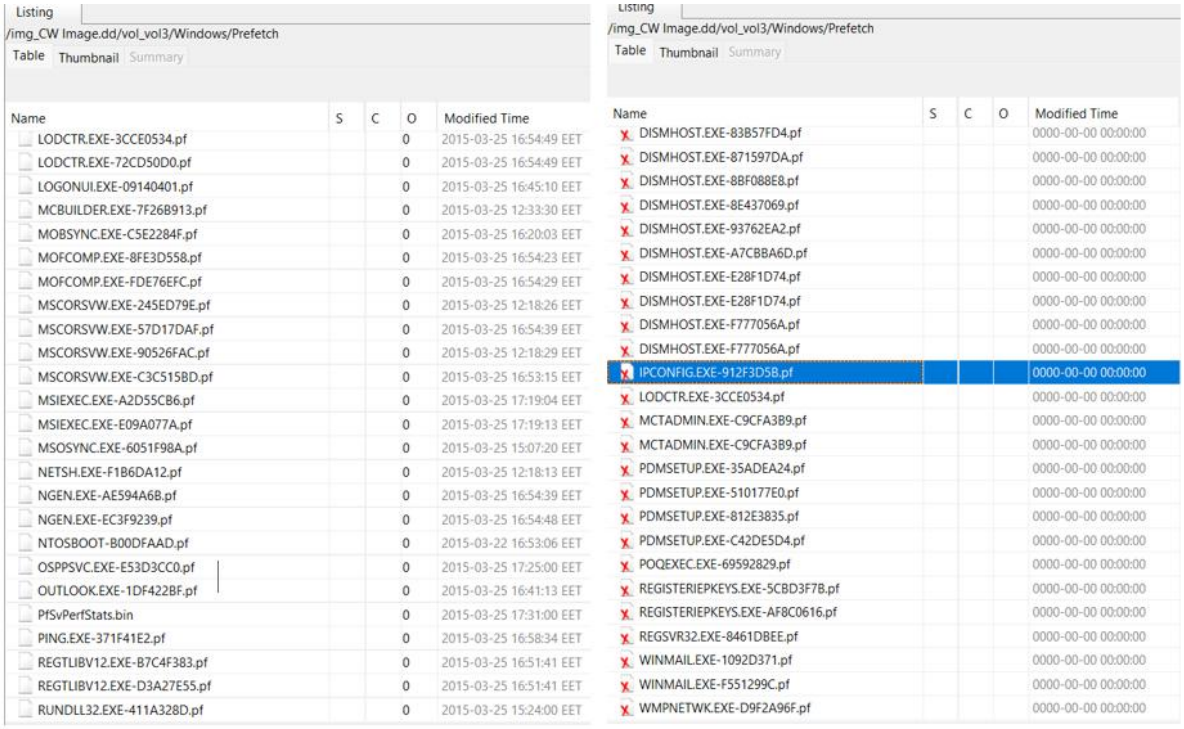


Source Name	S	C	O	Program Name	Path	Date/Time
ASPNET_REGIIS.EXE-75651A3C.pf				ASPNET_REGIIS.EXE	/WINDOWS/MICROSOFT.NET/FRAMEWORK64/V4.0.303.	2015-03-25 16:54:21 EET
ASPNET_REGIIS.EXE-86915B5A.pf				ASPNET_REGIIS.EXE		2015-03-25 16:54:28 EET
AUDIODG.EXE-BDFD3029.pf				AUDIODG.EXE	/WINDOWS/SYSTEM32	2015-03-25 17:14:45 EET
AU_.EXE-506726E7.pf				AU_.EXE	/USERS/INFORMANT/APPDATA/LOCAL/TEMP/~NSU.T...	2015-03-25 17:18:29 EET
BFSVC.EXE-9C7A4DEE.pf				BFSVC.EXE	/WINDOWS	2015-03-25 12:18:12 EET
CCLEANER64.EXE-779BD542.pf				CCLEANER64.EXE	/PROGRAM FILES/CCLEANER	2015-03-25 17:15:50 EET
CCSETUP504.EXE-6BA2F6A1.pf				CCSETUP504.EXE	/USERS/INFORMANT/DESKTOP/DOWNLOAD	2015-03-25 16:57:56 EET
CHROME.EXE-D999B1BA.pf				CHROME.EXE	/PROGRAM FILES (X86)/GOOGLE/CHROME/APPLICATI...	2015-03-24 23:05:38 EET
CLRGC.EXE-5D5B90F5.pf				CLRGC.EXE	/WINDOWS/WINSXS/AMD64_NETFX-CLRGC_B03F5F7F...	2015-03-25 12:18:15 EET
CONHOST.EXE-1F3E9D7E.pf				CONHOST.EXE	/WINDOWS/SYSTEM32	2015-03-25 17:18:36 EET
CONSENT.EXE-531BD9EA.pf				CONSENT.EXE	/WINDOWS/SYSTEM32	2015-03-25 17:18:29 EET
CONTROL.EXE-817F8F1D.pf				CONTROL.EXE	/WINDOWS/SYSTEM32	2015-03-25 15:29:34 EET
DEVICEDISPLAYOBJECTPROVIDER.E-17410B90.pf				DEVICEDISPLAYOBJECTPROVIDER.E		2015-03-24 23:02:47 EET
DLLHOST.EXE-4F28A26F.pf				DLLHOST.EXE	/WINDOWS/SYSTEM32	2015-03-24 23:01:10 EET
DLLHOST.EXE-5E46FA0D.pf				DLLHOST.EXE	/WINDOWS/SYSTEM32	2015-03-25 17:28:34 EET
DLLHOST.EXE-766398D2.pf				DLLHOST.EXE	/WINDOWS/SYSTEM32	2015-03-25 17:18:29 EET
DLLHOST.EXE-7FAA2E4C.pf				DLLHOST.EXE	/WINDOWS/SYSTEM32	2015-03-25 17:18:29 EET
DLLHOST.EXE-A8DE6D5B.pf				DLLHOST.EXE	/WINDOWS/SYSTEM32	2015-03-25 17:24:53 EET
DLLHOST.EXE-C373C89E.pf				DLLHOST.EXE	/WINDOWS/SYSTEM32	2015-03-25 15:29:36 EET
DLLHOST.EXE-E129DEF0.pf				DLLHOST.EXE	/WINDOWS/SYSTEM32	2015-03-24 22:24:03 EET
DLLHOST.EXE-ECB71776.pf				DLLHOST.EXE	/WINDOWS/SYSWOW64	2015-03-25 17:18:02 EET
DOTNETFX40_FULL_SETUP.EXE-5EFD2BFF.pf				DOTNETFX40_FULL_SETUP.EXE	/USERS/INFORMANT/APPDATA/LOCAL/TEMP/ERASERI..	2015-03-25 16:50:15 EET
DRVINST.EXE-4CB4314A.pf				DRVINST.EXE	/WINDOWS/SYSTEM32	2015-03-25 12:18:10 EET
ERASER 6.2.0.2962.EXE-BE552234.pf				ERASER 6.2.0.2962.EXE	/USERS/INFORMANT/DESKTOP/DOWNLOAD	2015-03-25 16:50:14 EET
ERASER.EXE-CE61944A.pf				ERASER.EXE	/PROGRAM FILES/ERASER	2015-03-25 17:13:30 EET

7. User Behaviour Retracement



8. Prefetch Files



Listing
/img_CW Image.dd/vol_vol3/Windows/Prefetch
Table Thumbnail Summary

Name	S	C	O	Modified Time
LODCTR.EXE-3CCE0534.pf			0	2015-03-25 16:54:49 EET
LODCTR.EXE-72CD50D0.pf			0	2015-03-25 16:54:49 EET
LOGONUI.EXE-09140401.pf			0	2015-03-25 16:45:10 EET
MCBUILDER.EXE-7F26B913.pf			0	2015-03-25 12:33:30 EET
MOBSYNC.EXE-C5E2284F.pf			0	2015-03-25 16:20:03 EET
MOFCOMP.EXE-8FE3D558.pf			0	2015-03-25 16:54:23 EET
MOFCOMP.EXE-FDE76EFC.pf			0	2015-03-25 16:54:29 EET
MSCORSVW.EXE-245ED79E.pf			0	2015-03-25 12:18:26 EET
MSCORSVW.EXE-57D17DAF.pf			0	2015-03-25 16:54:39 EET
MSCORSVW.EXE-90526FAC.pf			0	2015-03-25 12:18:29 EET
MSCORSVW.EXE-C3C515BD.pf			0	2015-03-25 16:53:15 EET
MSIEXEC.EXE-A2D55CB6.pf			0	2015-03-25 17:19:04 EET
MSIEXEC.EXE-E09A077A.pf			0	2015-03-25 17:19:13 EET
MSOSYNC.EXE-6051F98A.pf			0	2015-03-25 15:07:20 EET
NETSH.EXE-F1B6DA12.pf			0	2015-03-25 12:18:13 EET
NGEN.EXE-AE594A6B.pf			0	2015-03-25 16:54:39 EET
NGEN.EXE-EC3F9239.pf			0	2015-03-25 16:54:48 EET
NTOSBOOT-B00DFAAD.pf			0	2015-03-22 16:53:06 EET
OSPPSVC.EXE-E53D3CC0.pf			0	2015-03-25 17:25:00 EET
OUTLOOK.EXE-1DF422BF.pf			0	2015-03-25 16:41:13 EET
PfSvPerfStats.bin			0	2015-03-25 17:31:00 EET
PING.EXE-371F41E2.pf			0	2015-03-25 16:58:34 EET
REGTLIBV12.EXE-B7C4F383.pf			0	2015-03-25 16:51:41 EET
REGTLIBV12.EXE-D3A27E55.pf			0	2015-03-25 16:51:41 EET
RUNDLL32.EXE-411A328D.pf			0	2015-03-25 15:24:00 EET

Listing
/img_CW Image.dd/vol_vol3/Windows/Prefetch
Table Thumbnail Summary

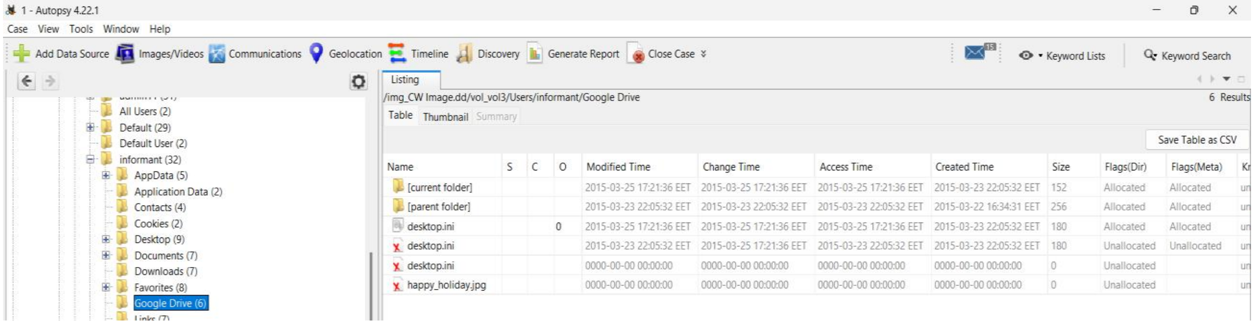
Name	S	C	O	Modified Time
DISMHOST.EXE-83B57FD4.pf				0000-00-00 00:00:00
DISMHOST.EXE-871597DA.pf				0000-00-00 00:00:00
DISMHOST.EXE-8BF088E8.pf				0000-00-00 00:00:00
DISMHOST.EXE-8E437069.pf				0000-00-00 00:00:00
DISMHOST.EXE-93762EA2.pf				0000-00-00 00:00:00
DISMHOST.EXE-A7CBBA6D.pf				0000-00-00 00:00:00
DISMHOST.EXE-E28F1D74.pf				0000-00-00 00:00:00
DISMHOST.EXE-E28F1D74.pf				0000-00-00 00:00:00
DISMHOST.EXE-F777056A.pf				0000-00-00 00:00:00
DISMHOST.EXE-F777056A.pf				0000-00-00 00:00:00
IPCONFIG.EXE-912F3D5B.pf				0000-00-00 00:00:00
LODCTR.EXE-3CCE0534.pf				0000-00-00 00:00:00
MCTADMIN.EXE-C9CFA3B9.pf				0000-00-00 00:00:00
MCTADMIN.EXE-C9CFA3B9.pf				0000-00-00 00:00:00
PDMSETUP.EXE-35ADEA24.pf				0000-00-00 00:00:00
PDMSETUP.EXE-510177E0.pf				0000-00-00 00:00:00
PDMSETUP.EXE-812E3835.pf				0000-00-00 00:00:00
PDMSETUP.EXE-C42DE5D4.pf				0000-00-00 00:00:00
POQEXEC.EXE-69592829.pf				0000-00-00 00:00:00
REGISTERIEPKEYS.EXE-5CBD3F7B.pf				0000-00-00 00:00:00
REGISTERIEPKEYS.EXE-AF8C0616.pf				0000-00-00 00:00:00
REGSVR32.EXE-8461DBEE.pf				0000-00-00 00:00:00
WINMAIL.EXE-1092D371.pf				0000-00-00 00:00:00
WINMAIL.EXE-F551299C.pf				0000-00-00 00:00:00
WMPNETWK.EXE-D9F2A96F.pf				0000-00-00 00:00:00

9. USB devices

USB Device Attached
Table Thumbnail Summary

Source Name	S	C	O	Date/Time	Device Make	Device Model	Device ID	Data Source
SYSTEM			1	2015-03-25 15:05:35 EET		ROOT_HUB	5&3bb57b&0	CW Image.dd
SYSTEM			1	2015-03-25 15:05:35 EET		ROOT_HUB20	5&299e1c9f&0	CW Image.dd
SYSTEM			1	2015-03-24 15:38:00 EET	SanDisk Corp.	Cruzer Fit	4C530012450531101593	CW Image.dd
SYSTEM			1	2015-03-24 21:38:09 EET	SanDisk Corp.	Cruzer Fit	4C530012550531106501	CW Image.dd
SYSTEM			1	2015-03-25 15:05:36 EET	VMware, Inc.	Virtual USB Hub	6&b77da92&0&2	CW Image.dd
SYSTEM			1	2015-03-25 15:05:36 EET	VMware, Inc.	Virtual Mouse	6&b77da92&0&1	CW Image.dd
SYSTEM			1	2015-03-25 15:05:36 EET	VMware, Inc.	Virtual Mouse	7&2a7d3009&0&0000	CW Image.dd
SYSTEM			1	2015-03-25 15:05:36 EET	VMware, Inc.	Virtual Mouse	7&2a7d3009&0&0001	CW Image.dd
SYSTEM			1	2015-03-25 15:05:35 EET		ROOT_HUB	5&3bb57b&0	CW Image.dd
SYSTEM			1	2015-03-25 15:05:35 EET		ROOT_HUB20	5&299e1c9f&0	CW Image.dd
SYSTEM			1	2015-03-24 15:38:00 EET	SanDisk Corp.	Cruzer Fit	4C530012450531101593	CW Image.dd
SYSTEM			1	2015-03-24 21:38:09 EET	SanDisk Corp.	Cruzer Fit	4C530012550531106501	CW Image.dd
SYSTEM			1	2015-03-25 15:05:36 EET	VMware, Inc.	Virtual USB Hub	6&b77da92&0&2	CW Image.dd
SYSTEM			1	2015-03-25 15:05:36 EET	VMware, Inc.	Virtual Mouse	6&b77da92&0&1	CW Image.dd
SYSTEM			1	2015-03-25 15:05:36 EET	VMware, Inc.	Virtual Mouse	7&2a7d3009&0&0000	CW Image.dd
SYSTEM			1	2015-03-25 15:05:36 EET	VMware, Inc.	Virtual Mouse	7&2a7d3009&0&0001	CW Image.dd

10. Shared Files

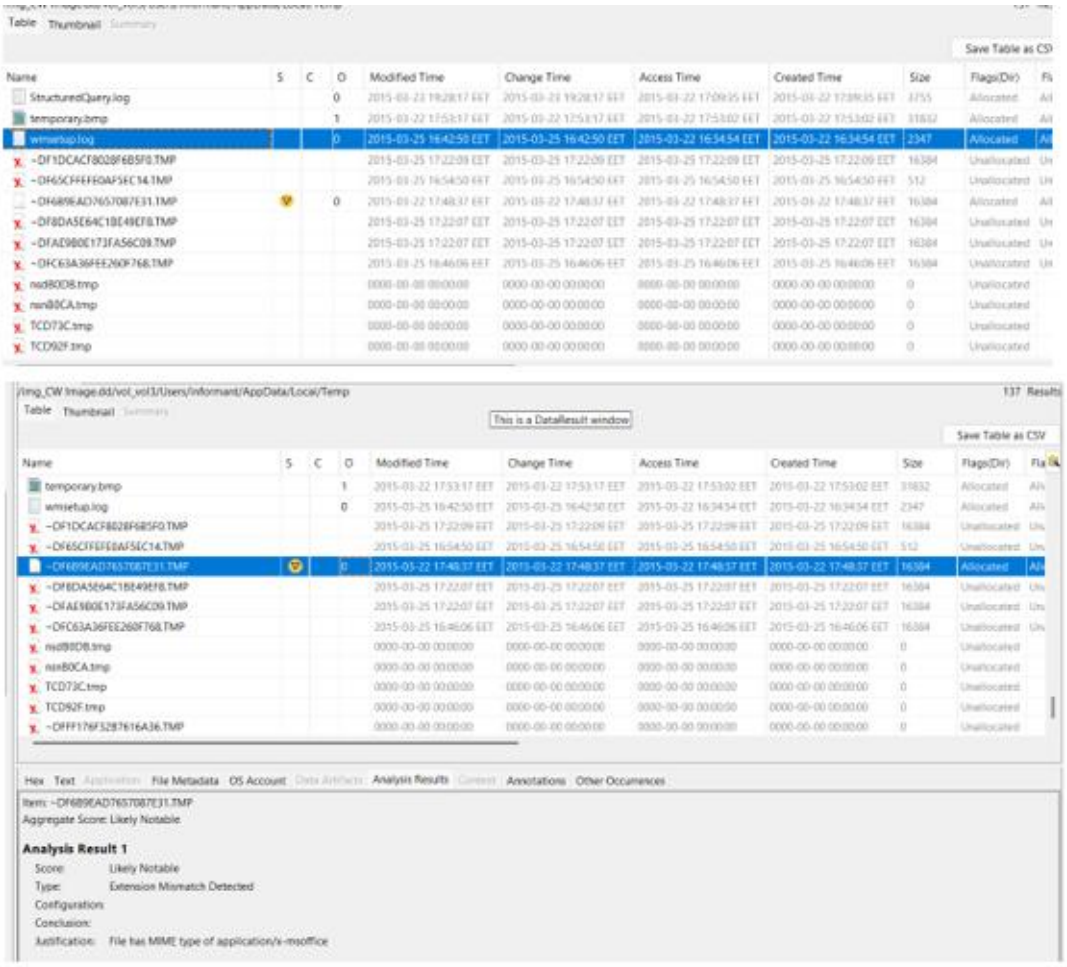


11. Web Activity

12. Deleted files

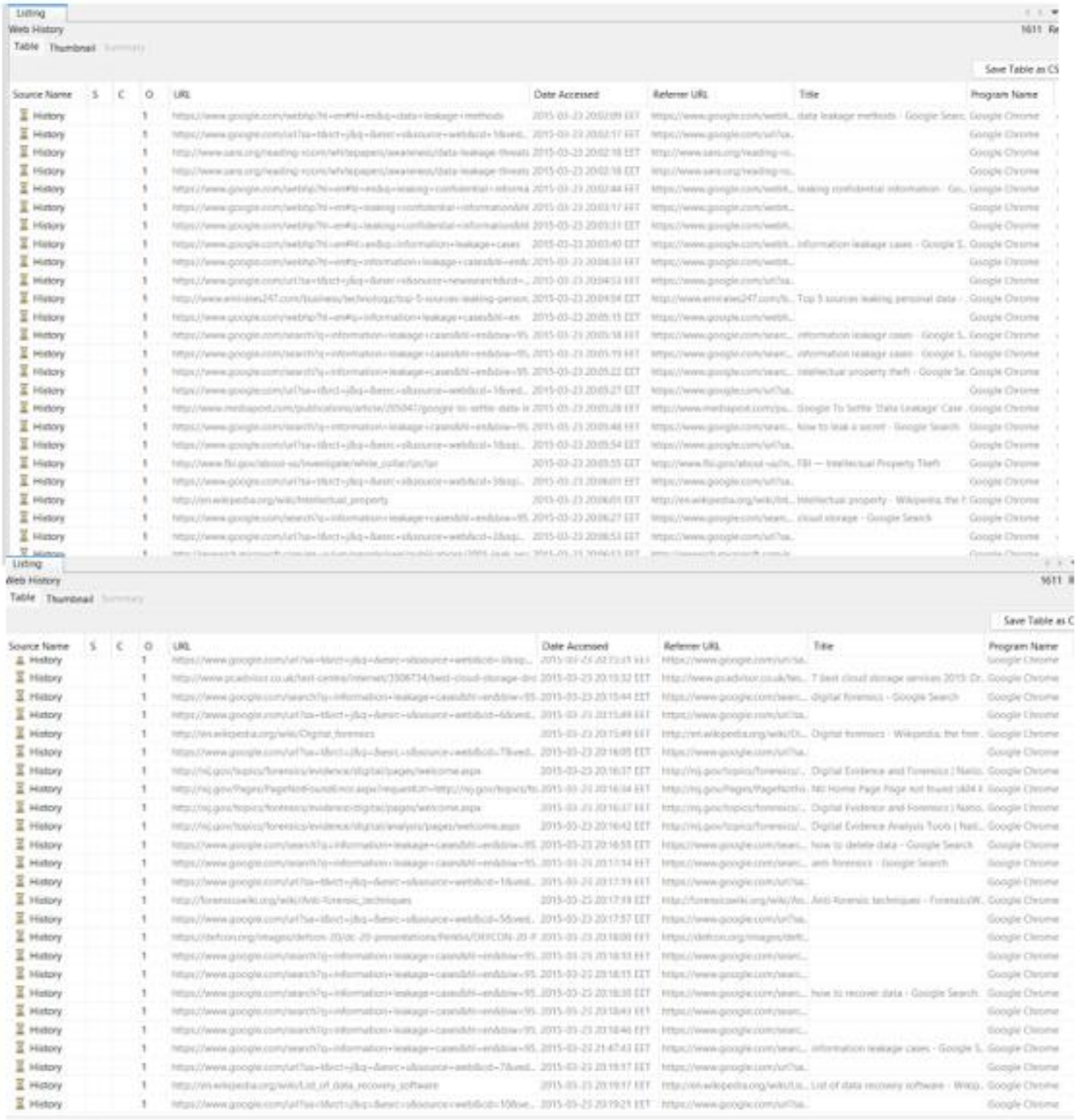
Source Name	S	C	O	Path	Time Deleted	Username	Data Source
$RKXD1U3.jpg				C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Chrysanthemum.jpg	2015-03-24 22:11:42 EET		CW Image.dd
$RI3FM2A.jpg				C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Desert.jpg	2015-03-24 22:11:42 EET		CW Image.dd
$RIQGWTT.ini				C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\desktop.ini	2015-03-24 22:11:42 EET		CW Image.dd
$RS08CBB.jpg				C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Hydrangeas.jpg	2015-03-24 22:11:42 EET		CW Image.dd
$RJEMT64.exe				C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\IE11-Windows6.1-x64-en-us.exe	2015-03-24 22:11:42 EET		CW Image.dd
$R8YP3XK.jpg				C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Jellyfish.jpg	2015-03-24 22:11:42 EET		CW Image.dd
$RU3FKWI.jpg				C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Koala.jpg	2015-03-24 22:11:42 EET		CW Image.dd
$RX538VH.jpg				C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Lighthouse.jpg	2015-03-24 22:11:42 EET		CW Image.dd
$RFVCH5V.jpg				C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Penguins.jpg	2015-03-24 22:11:42 EET		CW Image.dd
$RDOI3HE.jpg				C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Tulips.jpg	2015-03-24 22:11:42 EET		CW Image.dd

13. File System Analysis



Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Comment
659159[1].dat			0	File	Likely Notable			Suspected encryption due to high entropy (7.876996).	Suspected encryp
win7_scenic-demoshort_raw.wtv			1	File	Likely Notable			Suspected encryption due to high entropy (7.638412).	Suspected encryp
XboxMCX-V.XEX			1	File	Likely Notable			Suspected encryption due to high entropy (7.999667).	Suspected encryp
AgCx_S1_S-1-5-21-2425377081-3129163575-2985(			0	File	Likely Notable			Suspected encryption due to high entropy (7.849933).	Suspected encryp
AgCx_SC3_04B1D710D681061D.db			0	File	Likely Notable			Suspected encryption due to high entropy (7.739371).	Suspected encryp
AgCx_SC4.db			0	File	Likely Notable			Suspected encryption due to high entropy (7.848708).	Suspected encryp
AgGIFaultHistory.db			0	File	Likely Notable			Suspected encryption due to high entropy (7.923138).	Suspected encryp
AgGIFgAppHistory.db			0	File	Likely Notable			Suspected encryption due to high entropy (7.872529).	Suspected encryp
AgGIGlobalHistory.db			0	File	Likely Notable			Suspected encryption due to high entropy (7.921879).	Suspected encryp
AgGIUAD_S-1-5-21-2425377081-3129163575-2985			0	File	Likely Notable			Suspected encryption due to high entropy (7.909996).	Suspected encryp

14: Browser History



15: Downloaded Files

Source Name	S	C	O	Path	URL	Date Accessed	Domain	Username
History			1	C:\Users\informant\Downloads\icloudsetup.exe	https://support.apple.com/downloads/DL1455/en_US/iclo	2015-03-23 21:55:47 EET	apple.com	Default
History			1	C:\Users\informant\Downloads\icloudsetup.exe	http://download.info.apple.com/Mac_OS_X/031-13122.20	2015-03-23 21:55:47 EET	apple.com	Default
History			1	C:\Users\informant\Downloads\icloudsetup.exe	http://supportdownload.apple.com/download.info.apple.c	2015-03-23 21:55:47 EET	apple.com	Default
History			1	C:\Users\informant\Downloads\googledrivesync.exe	http://dl.google.com/tag/s/appguid%3D%7B3C122445-A	2015-03-23 21:56:30 EET	google.com	Default
History			1	C:\Users\informant\Downloads\googledrivesync.exe	https://dl.google.com/tag/s/appguid%3D%7B3C122445-.	2015-03-23 21:56:30 EET	google.com	Default
IE11-Windows6.1-x64-en-us.exe:Zone.Identifier				/Users/informant/Desktop/Download/IE11-Windows6.1				
Eraser 6.2.0.2962.exe:Zone.Identifier				/Users/informant/Desktop/Download/Eraser 6.2.0.2962.				
ccsetup504.exe:Zone.Identifier				/Users/informant/Desktop/Download/ccsetup504.exe				
$RJEMT64.exe:Zone.Identifier				/$Recycle.Bin/S-1-5-21-2425377081-3129163575-29856				

16: Email Analysis

23/3/2015

spy: Hello Iaman, How are you doing?

IAMAN: successfully secured

spy: Good, job. I need a more detailed data about this business.

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

spy: I confirmed it. But, I need a more data. Do your best.

IAMAN: Umm,,,, I need time to think.

NOTE IAMAN TO IAMAN synchronization log: downloaded data from server and sent it as offline folder

IAMAN: I got it. Its me. Use links below,

https://drive.google.com/file/d/0Bz0ye6gXtiZaVl8yVU5mWHlGbWc/view?usp=sharing

https://drive.google.com/file/d/0Bz0ye6gXtiZaakx6d3R3c0JmM1U/view?usp=sharing

Source Name	S	C	O	E-Mail From	E-Mail To	Subject	Date Received
iaman.informant@nist.gov.ost				spy <spy.conspirator@nist.gov>		Hello, Iaman	2015-03-23 19:29:29 EET
iaman.informant@nist.gov.ost				iaman </o=ExchangeLabs/ou=Exchange Administrative	spy	RE: Hello, Iaman	2015-03-23 20:44:00 EET
iaman.informant@nist.gov.ost				spy <spy.conspirator@nist.gov>		Good job, buddy	2015-03-23 21:15:00 EET
iaman.informant@nist.gov.ost				spy <spy.conspirator@nist.gov>		RE: Good job, buddy	2015-03-23 21:20:41 EET
iaman.informant@nist.gov.ost				spy <spy.conspirator@nist.gov>		Important request	2015-03-23 21:26:23 EET
iaman.informant@nist.gov.ost				iaman </o=ExchangeLabs/ou=Exchange Administrative	spy	RE: Important request	2015-03-23 21:27:00 EET
iaman.informant@nist.gov.ost				iaman	iaman	Synchronization Log	2015-03-23 21:57:30 EET
iaman.informant@nist.gov.ost				spy <spy.conspirator@nist.gov>		RE: It's me	2015-03-23 22:43:22 EET

24/3/2015

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

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

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

IAMAN: This is the last time..

Spy: Watch out! USB device may be easily detected.

So, try another method.

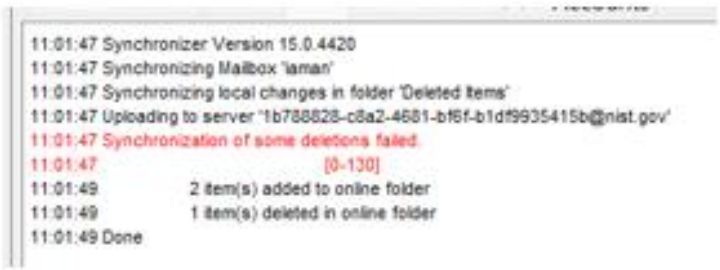
IAMAN: I'm trying

IAMAN: its done, see you tomorrow

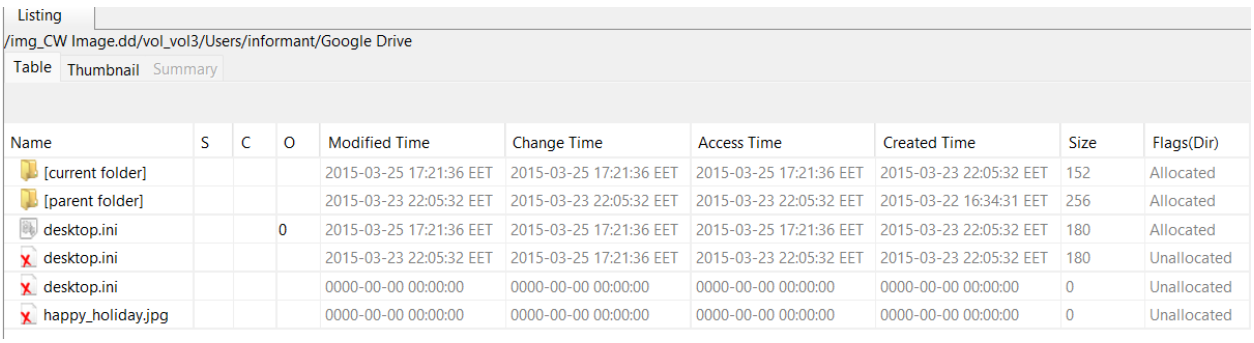
17: Email Analysis

25/3/2015: time synchronization logs, actions on server are taken

The entry in the synchronization log shows that there was a threat of data transfers that have been malicious done over the email client of the victim. The OST mailbox (iaman.informantnist.gov. occurs in multiple occurrences of synchronization in the same minute, indicating that there was communication between files or data between the local machine and an external mail server and the spy. Considering the case, time-regulated sync operations is a sign of stealing data with email. This action is one of the tricks of attackers who use email sync to transfer sensitive data silently without creating any file copy traces on the computer.

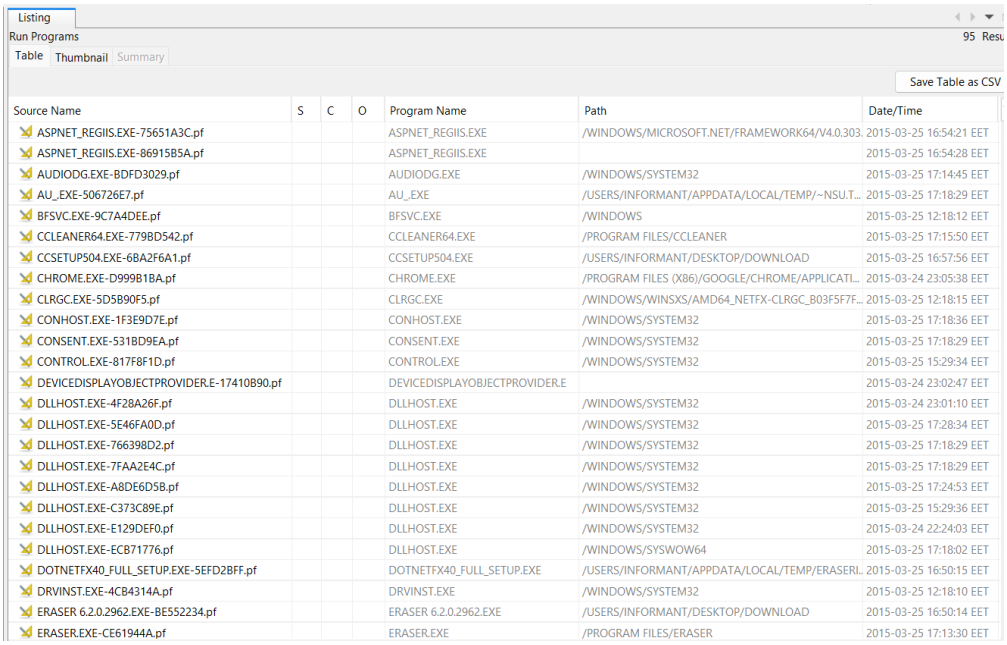


18: Unallocated files on shared folders:



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
[current folder]				2015-03-25 17:21:36 EET	2015-03-25 17:21:36 EET	2015-03-25 17:21:36 EET	2015-03-23 22:05:32 EET	152	Allocated
[parent folder]				2015-03-23 22:05:32 EET	2015-03-23 22:05:32 EET	2015-03-23 22:05:32 EET	2015-03-22 16:34:31 EET	256	Allocated
desktop.ini			0	2015-03-25 17:21:36 EET	2015-03-25 17:21:36 EET	2015-03-25 17:21:36 EET	2015-03-23 22:05:32 EET	180	Allocated
desktop.ini				2015-03-23 22:05:32 EET	2015-03-25 17:21:36 EET	2015-03-23 22:05:32 EET	2015-03-23 22:05:32 EET	180	Unallocated
desktop.ini				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated
happy_holiday.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated

19: Persistence Mechanisms



Listing

Run Programs 95 Resu

Table Thumbnail Summary

Save Table as CSV

Source Name	S	C	O	Program Name	Path	Date/Time
ASPNET_REGIIS.EXE-75651A3C.pf				ASPNET_REGIIS.EXE	/WINDOWS/MICROSOFT.NET/FRAMEWORK64/V4.0.303.	2015-03-25 16:54:21 EET
ASPNET_REGIIS.EXE-86915B5A.pf				ASPNET_REGIIS.EXE		2015-03-25 16:54:28 EET
AUDIODG.EXE-BDFD3029.pf				AUDIODG.EXE	/WINDOWS/SYSTEM32	2015-03-25 17:14:45 EET
AU_.EXE-506726E7.pf				AU_.EXE	/USERS/INFORMANT/APPDATA/LOCAL/TEMP/~NSU.T...	2015-03-25 17:18:29 EET
BFSVC.EXE-9C7A4DEE.pf				BFSVC.EXE	/WINDOWS	2015-03-25 12:18:12 EET
CCLEANER64.EXE-779BD542.pf				CCLEANER64.EXE	/PROGRAM FILES/CCLEANER	2015-03-25 17:15:50 EET
CCSETUP504.EXE-6BA2F6A1.pf				CCSETUP504.EXE	/USERS/INFORMANT/DESKTOP/DOWNLOAD	2015-03-25 16:57:56 EET
CHROME.EXE-D999B1BA.pf				CHROME.EXE	/PROGRAM FILES (X86)/GOOGLE/CHROME/APPLICATI...	2015-03-24 23:05:38 EET
CLRGC.EXE-5D5B90F5.pf				CLRGC.EXE	/WINDOWS/WINSXS/AMD64_NETFX-CLRGC_B03F5F7F...	2015-03-25 12:18:15 EET
CONHOST.EXE-1F3E9D7E.pf				CONHOST.EXE	/WINDOWS/SYSTEM32	2015-03-25 17:18:36 EET
CONSENT.EXE-531BD9EA.pf				CONSENT.EXE	/WINDOWS/SYSTEM32	2015-03-25 17:18:29 EET
CONTROL.EXE-817F8F1D.pf				CONTROL.EXE	/WINDOWS/SYSTEM32	2015-03-25 15:29:34 EET
DEVICEDISPLAYOBJECTPROVIDER.E-17410B90.pf				DEVICEDISPLAYOBJECTPROVIDER.E		2015-03-24 23:02:47 EET
DLLHOST.EXE-4F28A26F.pf				DLLHOST.EXE	/WINDOWS/SYSTEM32	2015-03-24 23:01:10 EET
DLLHOST.EXE-5E46FA0D.pf				DLLHOST.EXE	/WINDOWS/SYSTEM32	2015-03-25 17:28:34 EET
DLLHOST.EXE-766398D2.pf				DLLHOST.EXE	/WINDOWS/SYSTEM32	2015-03-25 17:18:29 EET
DLLHOST.EXE-7FAA2E4C.pf				DLLHOST.EXE	/WINDOWS/SYSTEM32	2015-03-25 17:18:29 EET
DLLHOST.EXE-A8DE6D5B.pf				DLLHOST.EXE	/WINDOWS/SYSTEM32	2015-03-25 17:24:53 EET
DLLHOST.EXE-C373C89E.pf				DLLHOST.EXE	/WINDOWS/SYSTEM32	2015-03-25 15:29:36 EET
DLLHOST.EXE-E129DEF0.pf				DLLHOST.EXE	/WINDOWS/SYSTEM32	2015-03-24 22:24:03 EET
DLLHOST.EXE-ECB71776.pf				DLLHOST.EXE	/WINDOWS/SYSWOW64	2015-03-25 17:18:02 EET
DOTNETFX40_FULL_SETUP.EXE-5EFD2BFF.pf				DOTNETFX40_FULL_SETUP.EXE	/USERS/INFORMANT/APPDATA/LOCAL/TEMP/ERASERI..	2015-03-25 16:50:15 EET
DRVINST.EXE-4CB4314A.pf				DRVINST.EXE	/WINDOWS/SYSTEM32	2015-03-25 12:18:10 EET
ERASER 6.2.0.2962.EXE-BE552234.pf				ERASER 6.2.0.2962.EXE	/USERS/INFORMANT/DESKTOP/DOWNLOAD	2015-03-25 16:50:14 EET
ERASER.EXE-CE61944A.pf				ERASER.EXE	/PROGRAM FILES/ERASER	2015-03-25 17:13:30 EET

16.Appendix

In the following the sections, all the digital forensics processes are provided. The google drive folder consists of the previous milestones, all the python scripts, all the extracted registry hives files, all the evidence screenshots, chain of custody full template, an additional evidence table with more details and finally an autopsy generated report.

Github link: https://github.com/hala-ahmedd/DIGITAL-FORENSICS-PYTHON-

Drive link: https://drive.google.com/drive/folders/136-SDflgc62GuVnBfzbmbmyVuUEw2rcW?usp=drive_link