CYBER SECURITY TOOLS AND PRACTICES

Digital Forensic Investigation

Sergiusz Pieszak

Contents

1. Introduction

The digital investigation team was assigned the task of performing data forensics on a desktop machine, provided by one of [redacted] clients. With precision, the team extracted the hard drive, ensuring the security, validation, and preservation of data integrity. Employing an evidence bag to establish a clear chain of custody and utilizing hash values for chain of custody record-keeping, they maintained a thorough documentation process with accordance to the ACPO and College of Policing guidelines.

Following the imaging of the hard drive using FTK Data Imager software, the resulting disk image was thoughtfully imported into Autopsy software for an in-depth analysis. The team's primary objective was to check the drive comprehensively in search of any instances of personally identifiable information (PII). This investigative process was undertaken with a focus on ethical standards and precision to uncover relevant digital evidence for the client.

2. Extracting the hard drive

When extracting data from the computer the team had to approach the computer with the highest professionality and standards. The standards that were used by the team were taken from the ACPO and College of Policing guidelines. According to (*Forensics Control*, 2020), ACPO being the Association of Chief Police Officers. Provides a set of guidelines for computer-based evidence that must be followed by computer forensics experts. These guidelines come with a suite of four essential principles. The principles are as follows:

- “No action must be taken that will change data held on a digital device that could later be relied on as evidence in Court.
- If it’s necessary to access original data held on a digital device, you must be both competent to do so and able to explain your actions, as well as explain the impact of them on any digital evidence used in a Court.
- A trail or record of all the actions taken and applied to the digital evidence must be created and kept safely and securely. If an independent third party forensic expert examines the processes they should be able to come to the exact same conclusion.

- The person in charge of the investigation has the overall responsibility of making sure these principles are followed." (*Forensics Control*, 2020)

When approaching the computer, it is important to make sure that specific guidelines are followed. Firstly, in line with College of Policing (2020) principle 3 states that the investigators need to ask the owner of the device, in this case [redacted] to take possession of the digital device, once permission if given the investigators may move on. Secondly, according to Association of Chief Police Officers (2012) guidelines the team first had to validate whether the computer was switched on or off. The team verified that the computer was switched off. However, if the computer was switched on, additional guidance would need to be followed. Shipley, T. and Reeve, H. (2006) stated that computers require a certain amount of random access memory (RAM) to be used by the operating system and its applications when the computer is in operation. The RAM is then utilized to write the current processes it is using as a form of a virtual clipboard. The information is there for immediate reference and use by the process. This type of data is called "volatile data" because it simply goes away and is irretrievable when the computer is turned off. Volatile data stored in the RAM can contain information of interest to the investigator. This information could include, for example: Running processes; Executed console commands; Passwords in clear text; Unencrypted data; Instant messages (IMs); Internet Protocol (IP) addresses. Whilst working with volatile data is difficult and unpredictable, it provides investigators with the highest quality data as listed previously.

When extracting the hard drive one of the team members was responsible for writing a detailed timeline (*Figure 1*) of each step of the extraction so that it can be referenced in the future and to maintain a constant chain of custody.

```
Sergiusz - Forensic Extractor
James    - Coordinator
Rhys     - Photographer
Jay      - Documentation

02 November 2023

Client has given permission for New Folder to forensically remove the hard drive

12:52 James starts the procedure and says the ACPO guidelines will be followed in this procedure
12:52 Rhys takes photo of desktop unotuched
12:53 Sergiez gets the equipment ready(computer repair tool kit)
12:53 Antistatic measures were taken and device has been checked to be unplugged by James
12:54 Desktop case side comes off by Sergiez
12:54 Photograph taken by Rhys of the side of the case taken off
12:54 James says to Sergiez to take the cd disk out of the desktop to uncover the hard drive
12:54 Cd disk unplugged then screw taken out  by Sergiez
12:55 Cd disk physically removed by Sergiez
12:55 Photograph taken of removed cd disk by Rhys
12:56 Cd disk bracket taken out by Sergiez
12:56 Image of bracket taken out by Rhys
12:56 James says to Remove the hard drive (since the hard drive is now uncovered)
12:56 Hard drive removed by Sergiez
12:56 Image of hard drive removed by Rhys
12:56 Final image of wires shown to be unplugged (blue wire - hard drive //  orange wire - cd drive) taken by Rhys
13:06 James says the device scan procedure starts at 13:06
13:06 Rhys takes image of evidence bag with the device inside
13:06 Hard drive is taken out of the evidence bag and image is taken by James
13:07 Device is plugged into the pc by James
13:07 Image of device plugged into the pc is taken by Rhys
13:08 Files transfer begins
13:10 File transfer finishes
13:11 Searching the files Evidence Test E.01 has all data for the hard drive
13:11 Evidence Test E.01 Hash uncovered MD5 and SHA1 hash( MD5 checksum:    8e3aa05a3c33e7f43c1929b76a2051cc
                                    SHA1 checksum:   99eef54eee0bca6c5cbb037570a495387b7eb428)
13:12 Evidence Test E.01 gets transfered to the group (New Folder) in Microsoft Teams
```

Real time notes taken by member of the team, according to ACPO guidelines - Figure 1

Proceeding further, ACPO instructs the operator to photograph the process of extracting the hard drive. Below is an annotated album of photographs the team obtained, each photograph has an associated time that it was taken.

Figure 2. This photograph shows the PC in the state it was found by the investigators as stated by the guidelines “Photograph or video the scene and all the components including the leads in situ.” Association of Chief Police Officers (2012). There are no power cables connected to the device. This indicates that the computer is powered off and the investigators can move forward, to extracting the hard drive as the guidelines clearly state that. (12:52)

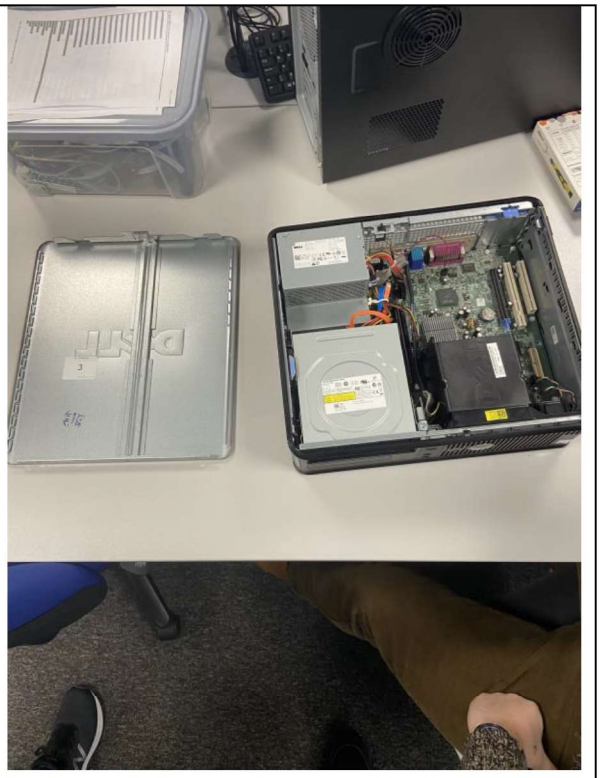
Figure 3. After the PC was confirmed to be turned off, the investigator responsible for the physical data extraction starts the extraction by taking the case off the PC (12:54).

Figure 4. To get access to the hard drive, the team needed to remove the CD/ROM device. To do this they had to unplug the internal power cable, and the data SATA cable (12:55).

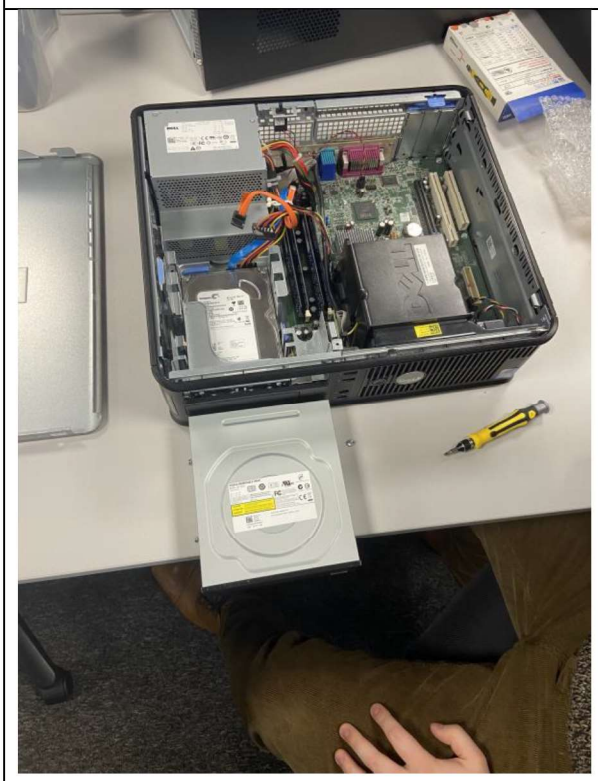
Figure 5. Removed the SATA cable from the original hard drive. (12:56)

Figure 6. and *Figure 7.* The coordinator then instructed the extractor to remove the hard drive placing it into evidence bag, as Association of Chief Police Officers (2012) states to “Ensure that all items have signed and completed exhibit labels attached to them.”, the bag was then sealed and signed to maintain a chain of custody. (12:56)

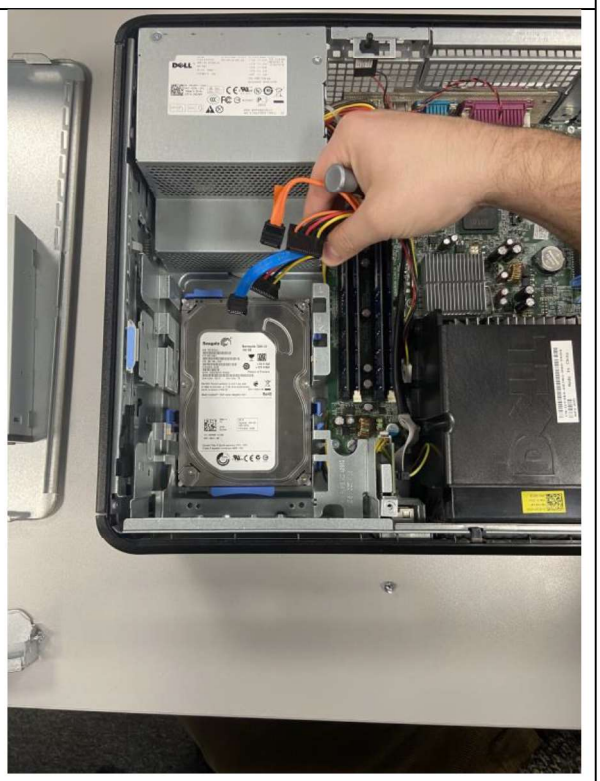
Photo of how the computer was found - Figure 2



Case removed from PC - Figure 3

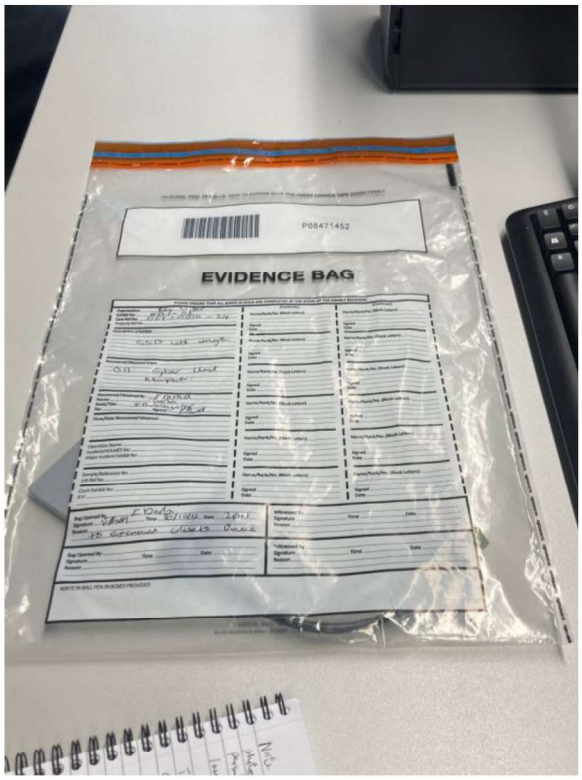


CD/ROM device removed from PC - Figure 4



SATA and power cable unplugged - Figure 5

Removed Drive from the computer - Figure 6



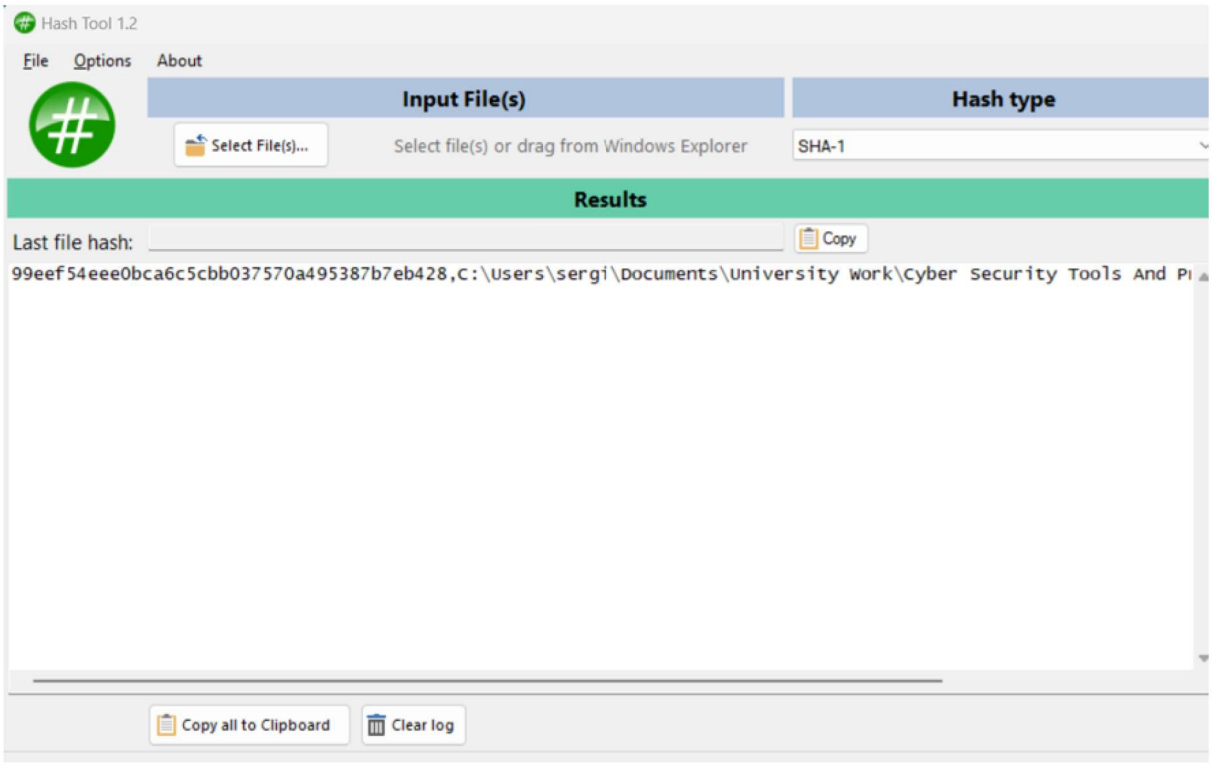
Hard Drive placed inside of a sealed evidence bag- Figure 7

3. Verification of data

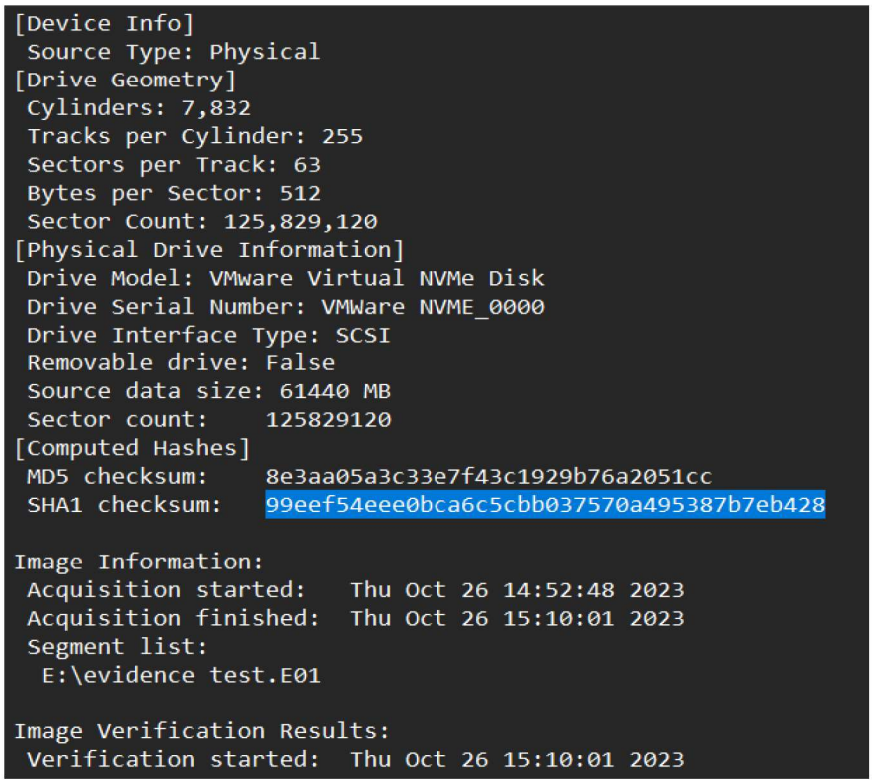
The key to any investigation, whether physical or digital is integrity of information. It is important to be able to prove that data has not been tampered with, especially if it is being used as an evidence artefact. The way data integrity is maintained throughout the investigation is through a process of hashing. As Forensics Digest (2020) mentioned, the most important rule in digital forensics is to never perform direct examination and analysis on the original digital evidence. In doing so, the date and time or file properties such as modified, accessed and created (MAC) will be changed. This makes the evidence unusable. To prevent this the investigator will use a tool such as FTK Data Imager, to image the digital evidence, creating a mirrored image of the drive. The team will then work on the copied drive to maintain the data integrity of the

original evidence. To prove that the data has not been tampered with, the industry uses hashing.

The imaged .EO1 folder has been shared across with all the other team members however we can check the SHA-1 hash value to prove that the image is the same as the original, uncorrupted evidence drive. The original hash in *figure 9* can be compared to the hash derived from the copy of the image in *figure 8*, the hash is the same showing that the evidence is uncorrupted.



SHA-1 hash value of the downloaded from the original image - Figure 8



Original file information, provided by FTK Data Images in a .txt file - Figure 9

4. Reflection on working in the team.

The team worked well together. Clear roles were set to each member of the team, and each individual member knew what their task was and what they were supposed to do. The following roles were assigned:

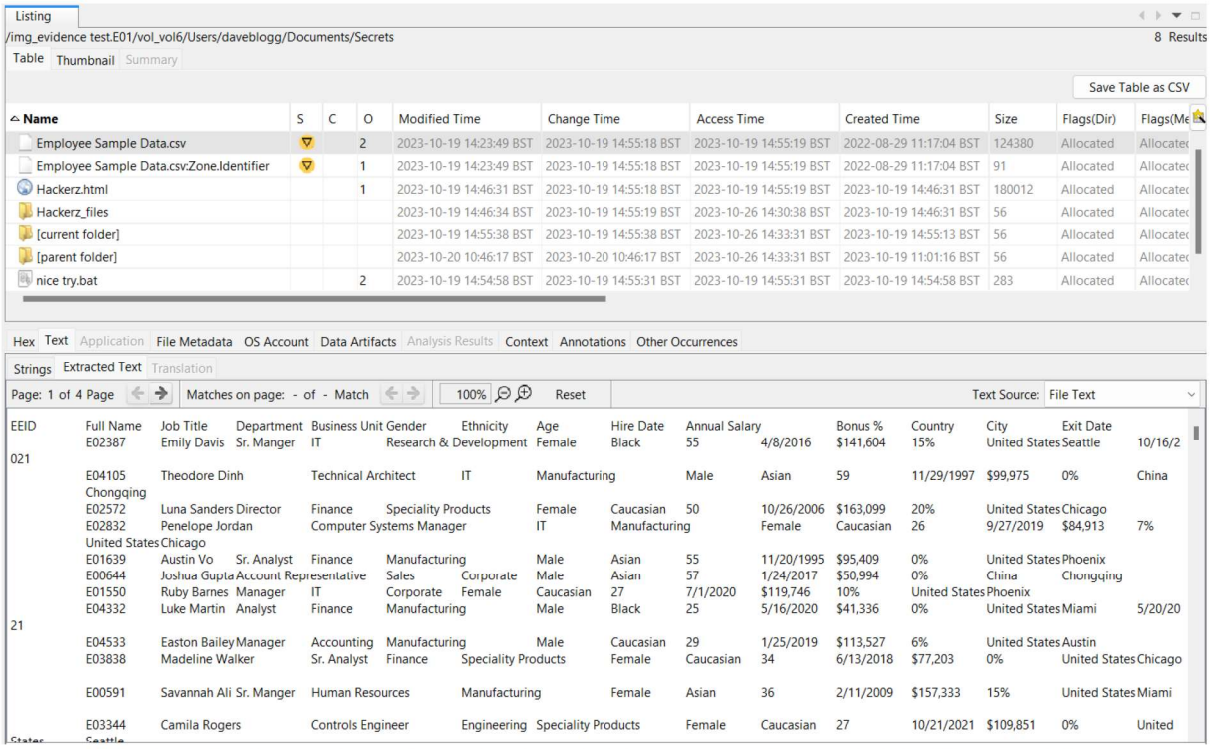
Sergiusz was the forensic extractor, taking apart the computer and removing the required digital evidence.

[redacted] was the photographer, gathering photographic evidence of the extraction process, in line with ACPO guidelines.

[redacted] was responsible for keeping all documentation of the extraction process, making sure that a log was being kept with appropriate timelines.

[redacted] was the coordinator, making sure that the process ran smoothly and efficiently. He also made sure that the extraction was in line with ACPO guidelines and that all the maintained integrity.

5. Summary of findings


Listing

/img_evidence test.E01/vol_vol6/Users/daveblogg/Documents/Secrets — 8 Results

Table | Thumbnail | Summary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Me
Employee Sample Data.csv			2	2023-10-19 14:23:49 BST	2023-10-19 14:55:18 BST	2023-10-19 14:55:19 BST	2022-08-29 11:17:04 BST	124380	Allocated	Allocate
Employee Sample Data.csv:Zone.Identifier			1	2023-10-19 14:23:49 BST	2023-10-19 14:55:18 BST	2023-10-19 14:55:19 BST	2022-08-29 11:17:04 BST	91	Allocated	Allocate
Hackerz.html			1	2023-10-19 14:46:31 BST	2023-10-19 14:55:18 BST	2023-10-19 14:55:19 BST	2023-10-19 14:46:31 BST	180012	Allocated	Allocate
Hackerz_files				2023-10-19 14:46:34 BST	2023-10-19 14:55:19 BST	2023-10-26 14:30:38 BST	2023-10-19 14:46:31 BST	56	Allocated	Allocate
[current folder]				2023-10-19 14:55:38 BST	2023-10-19 14:55:38 BST	2023-10-26 14:33:31 BST	2023-10-19 14:55:13 BST	56	Allocated	Allocate
[parent folder]				2023-10-20 10:46:17 BST	2023-10-20 10:46:17 BST	2023-10-26 14:33:31 BST	2023-10-19 11:01:16 BST	56	Allocated	Allocate
nice try.bat			2	2023-10-19 14:54:58 BST	2023-10-19 14:55:31 BST	2023-10-19 14:55:31 BST	2023-10-19 14:54:58 BST	283	Allocated	Allocate

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

Strings | Extracted Text | Translation

Page: 1 of 4 Page | Matches on page: - of - Match | 100% | Reset | Text Source: File Text

EEID	Full Name	Job Title	Department	Business Unit	Gender	Ethnicity	Age	Hire Date	Annual Salary	Bonus %	Country	City	Exit Date	
E02387	Emily Davis	Sr. Manger	IT	Research & Development	Female	Black	55	4/8/2016	$141,604	15%	United States	Seattle	10/16/2	021
E04105	Theodore Dinh	Technical Architect	IT	Manufacturing	Male	Asian	59	11/29/1997	$99,975	0%	China	Chongqing		
E02572	Luna Sanders	Director	Finance	Speciality Products	Female	Caucasian	50	10/26/2006	$163,099	20%	United States	Chicago		
E02832	Penelope Jordan	Computer Systems Manager	IT	Manufacturing	Female	Caucasian	26	9/27/2019	$84,913	7%	United States	Chicago		
E01639	Austin Vo	Sr. Analyst	Finance	Manufacturing	Male	Asian	55	11/20/1995	$95,409	0%	United States	Phoenix		
E00644	Joshua Gupta	Account Representative	Sales	Corporate	Male	Asian	57	1/24/2017	$50,994	0%	China	Chongqing		
E01550	Ruby Barnes	Manager	IT	Corporate	Female	Caucasian	27	7/1/2020	$119,746	10%	United States	Phoenix		
E04332	Luke Martin	Analyst	Finance	Manufacturing	Male	Black	25	5/16/2020	$41,336	0%	United States	Miami	5/20/20	21
E04533	Easton Bailey	Manager	Accounting	Manufacturing	Male	Caucasian	29	1/25/2019	$113,527	6%	United States	Austin		
E03838	Madeline Walker	Sr. Analyst	Finance	Speciality Products	Female	Caucasian	34	6/13/2018	$77,203	0%	United States	Chicago		
E00591	Savannah Ali	Sr. Manger	Human Resources	Manufacturing	Female	Asian	36	2/11/2009	$157,333	15%	United States	Miami		
E03344	Camila Rogers	Controls Engineer	Engineering	Speciality Products	Female	Caucasian	27	10/21/2021	$109,851	0%	United			

A data dump found on the hard drive, consisting of PII - Figure 10

Using an open-sources forensics software called Autopsy, the following information was found. *Figure 10* shows a .cvs file of personal identifiable information that was discovered. Additional information was found however the investigation must be kept in the scope that was permitted by the client, as stated by the College of Policing (2020) “Principle 1 – Strictly necessary and avoiding unnecessary intrusion. Data will only be extracted from a personal digital device if it is strictly necessary for an investigation. Intrusion into the personal or family life of device owners will be avoided wherever possible. Only the minimum data that is strictly necessary will be extracted.” therefore additional information should be disregarded by the investigator.

6. Conclusion

In conclusion, the digital investigation team successfully carried out a careful and secure data forensics procedure on the desktop computer belonging to the customer. Following established procedures and guidelines, they made sure the data was accurate by using evidence bags, implementing hash values for chain of custody, and

carefully extracting the data. Their dedication to thorough inquiry was evident in the imaging and analysis of the hard drive that followed, which focused on precisely and ethically locating personally identifiable information (PII). The client's goals were achieved by the team's methodical approach, which produced trustworthy digital evidence during a thorough investigation.

7. References

Association of Chief Police Officers (2012) *ACPO Good Practice Guide for Computer-Based Electronic Evidence* Available at: https://www.datainvestigations.co.uk/files/ACPO%20Guidelines%20Computer%20Evidence%20v4.pdf (Accessed on: 29 October 2023)

College of Policing (2020) *Authorised Professional Practice: The extraction of digital data from personal devices.* Available at: https://assets.college.police.uk/s3fs-public/2020-12/APP-extraction-data-from-personal-devices.pdf.(Accessed on: 29 November 2023)

Forensic Control (2020) ACPO Guidelines & Principles Explained. Available at: https://forensiccontrol.com/guides/acpo-guidelines-and-principles-explained/ (Accessed on: 15 November 2023)

Forensics Digest (2020). Hashing and Data Imaging. Available at: https://forensicsdigest.com/hashing-and-data-imaging/. (Accessed on: 29 November 2023)

Shipley, T. and Reeve, H. (2006) Collecting Evidence from a Running Computer: *A Technical and Legal Primer for the Justice Community SEARCH*. Available at: https://www.search.org/files/pdf/CollectEvidenceRunComputer.pdf. (Accessed on: 27 November 2023)