SeanCronin-FSF-Asgn1-24

Sean Cronin

November 2024

1 Introduction

A forensic analysis was conducted in response to an investigation on Buster Bloggs. The objective was to obtain files that could benefit the investigation from an image of a floppy disk. This image was modified by cutting one sector from the original file so that all forensic tools would be usable throughout the investigation.

The primary objectives of this investigation were:

1. Duplicating the floppy disk image while also checking the hash values to ensure data integrity from the disk image given.
2. Examining the file system structure of the disk, including data clusters and directory entries.
3. Retrieving deleted files and verifying key files.

2 Tools Selected

The following tools were selected for this investigation:

- **dd**: Used to duplicate the disk image while also checking if the data was modified.
- **Autopsy**: A GUI-based forensic tool used to analyze the disk image, recover files, and inspect file system metadata.
- **Photorec**: A command-line tool specializing in file carving and recovery, used to cross-verify file recovery alongside Autopsy.
- **fls** and **istat** (Sleuth Kit tools): Used to examine directory entries, map cluster chains, and extract file metadata.

3 Duplicates

A duplicate copy of the disk image was made using the command `dd`, maintaining data integrity whilst not tampering the evidence.

To create the duplicate,following `dd` command was used:

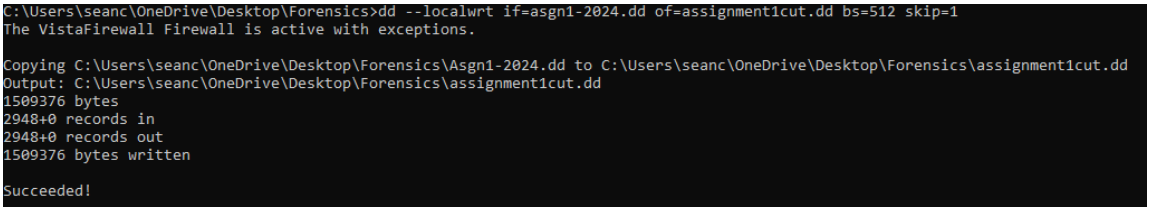


Figure 1: Command used to create duplicate of image with `dd`

The hash values of the original and duplicate were then verified:

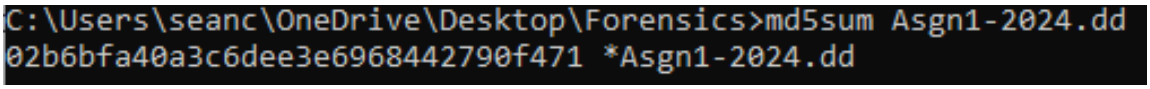


Figure 2: Hash values of original file in command prompt

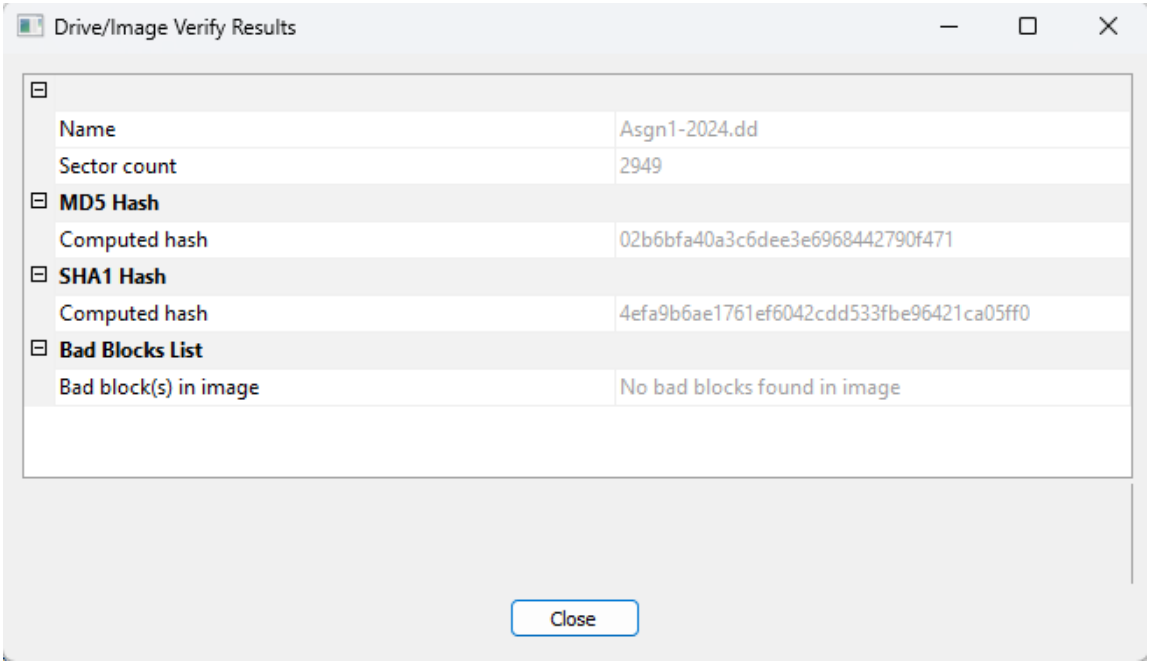


Figure 3: FTK imager to verify hash values

s

4 Data Structures

To understand the layout of the disk, the data structures were examined using ‘fsstat‘, ‘fls‘, and ‘istat‘ commands. This then identified key areas such as the Reserved Area, FAT tables, Root Directory, and Data Area.

Area	Sector Range	Description
Reserved Area & Boot Sector	0	Contains boot information
FAT 0	1 - 9	First file allocation table
FAT 1	10 - 18	Second file allocation table for redundancy
Root Directory	19 - 50	Holds file and directory metadata
Data Area	51 - 2947	Main storage area for file data

Table 1: Map of Disk Image Structure with Sector Ranges

The disk image structure, as revealed by the ‘fsstat‘ command, shows the allocation of sectors across the reserved areas, FAT tables, root directory, and cluster area.

```
C:\Users\seanc\OneDrive\Desktop\Forensics>fsstat assignment1cut.dd
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: FAT12

OEM Name: BSD  4.4
Volume ID: 0xe1d41918
Volume Label (Boot Sector): ASGN1-2024
Volume Label (Root Directory):
File System Type Label: FAT12

Sectors before file system: 1

File System Layout (in sectors)
Total Range: 0 - 2947
* Reserved: 0 - 0
** Boot Sector: 0
* FAT 0: 1 - 9
* FAT 1: 10 - 18
* Data Area: 19 - 2947
** Root Directory: 19 - 50
** Cluster Area: 51 - 2947

METADATA INFORMATION
--------------------------------------------
Range: 2 - 46870
Root Directory: 2

CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 512
Total Cluster Range: 2 - 2898

FAT CONTENTS (in sectors)
--------------------------------------------
51-51 (1) -> EOF
52-52 (1) -> EOF
61-61 (1) -> EOF
62-69 (8) -> EOF
70-70 (1) -> EOF
71-78 (8) -> EOF
79-1406 (1328) -> EOF
1407-1407 (1) -> EOF
1408-1415 (8) -> EOF
1416-1494 (79) -> EOF
1495-1495 (1) -> EOF
1496-1496 (1) -> EOF
1497-1504 (8) -> EOF
1505-1505 (1) -> EOF
1506-1506 (1) -> EOF

C:\Users\seanc\OneDrive\Desktop\Forensics>fls assignment1cut.dd
r/r 3:  ASGN1-2024  (Volume Label Entry)
d/d 5:  .fseventsd
r/r * 7:        For Buster
r/r * 9:        ._For Buster
d/d 11: .Trashes
d/d * 12:       _NTITL~7
d/d 14: Folder1
d/d * 15:       _hip
v/v 46867:      $MBR
v/v 46868:      $FAT1
v/v 46869:      $FAT2
V/V 46870:      $OrphanFiles
```

Figure 4: File System Layout from `fsstat` command output

4.1 Directory Structure Analysis

The ‘fls‘ command provided a directory listing, identifying key nodes within the image, as shown below:

```
C:\Users\seanc\OneDrive\Desktop\Forensics>fls assignment1cut.dd
r/r 3:  ASGN1-2024  (Volume Label Entry)
d/d 5:  .fseventsd
r/r * 7:        For Buster
r/r * 9:        ._For Buster
d/d 11: .Trashes
d/d * 12:       _NTITL~7
d/d 14: Folder1
d/d * 15:       _hip
v/v 46867:      $MBR
v/v 46868:      $FAT1
v/v 46869:      $FAT2
V/V 46870:      $OrphanFiles
```

Figure 5: Directory Listing from `fls` command output

4.2 Directory Entry Analysis

The‘istat‘ command was then used to examine individual nodes in detail, providing info into allocation status, timestamps, and clusters used for each entry. Below are the findings for nodes up to 15:

- Node 3: Volume Label Entry

```
C:\Users\seanc\OneDrive\Desktop\Forensics>istat assignment1cut.dd 3
Directory Entry: 3
Allocated
File Attributes: Volume Label, Archive
Size: 0
Name: ASGN1-2024

Directory Entry Times:
Written:        2024-10-23 18:29:20 (GMT Summer Time)
Accessed:       0000-00-00 00:00:00 (UTC)
Created:        0000-00-00 00:00:00 (UTC)

Sectors:
```

Figure 6: `istat` output for Node 3

- Node 5: Directory `.fseventsd`

```
C:\Users\seanc\OneDrive\Desktop\Forensics>istat assignment1cut.dd 5
Directory Entry: 5
Allocated
File Attributes: Directory, Hidden
Size: 512
Name: FSEVEN~1

Directory Entry Times:
Written:        2024-10-23 18:25:40 (GMT Summer Time)
Accessed:       2024-10-23 00:00:00 (GMT Summer Time)
Created:        2024-10-23 18:25:40 (GMT Summer Time)

Sectors:
51
```

Figure 7: `istat` output for Node 5

- Node 7: File `For Buster`

```
C:\Users\seanc\OneDrive\Desktop\Forensics>istat assignment1cut.dd 7
Directory Entry: 7
Not Allocated
File Attributes: File, Archive
Size: 218
Name: _ORBUS~3

Directory Entry Times:
Written:        2024-10-23 18:18:14 (GMT Summer Time)
Accessed:       2024-10-23 00:00:00 (GMT Summer Time)
Created:        2024-10-23 17:59:02 (GMT Summer Time)

Sectors:
61
```

Figure 8: `istat` output for Node 7

- Node 9: File `._For Buster`

```
C:\Users\seanc\OneDrive\Desktop\Forensics>istat assignment1cut.dd 9
Directory Entry: 9
Not Allocated
File Attributes: File, Hidden, Archive
Size: 4096
Name: _FORBU~5

Directory Entry Times:
Written:        2024-10-23 18:25:48 (GMT Summer Time)
Accessed:       2024-10-23 00:00:00 (GMT Summer Time)
Created:        2024-10-23 18:25:48 (GMT Summer Time)

Sectors:
62
```

Figure 9: `istat` output for Node 9

- Node 11: Directory `.Trashes`

```
C:\Users\seanc\OneDrive\Desktop\Forensics>istat assignment1cut.dd 11
Directory Entry: 11
Allocated
File Attributes: Directory, Hidden
Size: 512
Name: TRASHE~7

Directory Entry Times:
Written:        2024-10-23 18:29:16 (GMT Summer Time)
Accessed:       2024-10-23 00:00:00 (GMT Summer Time)
Created:        2024-10-23 18:29:16 (GMT Summer Time)

Sectors:
1495
```

Figure 10: `istat` output for Node 11

- Node 12: Directory `_NTITL~7`

```
C:\Users\seanc\OneDrive\Desktop\Forensics>istat assignment1cut.dd 12
Directory Entry: 12
Not Allocated
File Attributes: Directory
Size: 0
Name: _NTITL~7

Directory Entry Times:
Written:        2024-10-23 18:27:30 (GMT Summer Time)
Accessed:       2024-10-23 00:00:00 (GMT Summer Time)
Created:        2024-10-23 18:27:30 (GMT Summer Time)

Sectors:
1407
```

Figure 11: `istat` output for Node 12

- Node 14: Directory `Folder1`

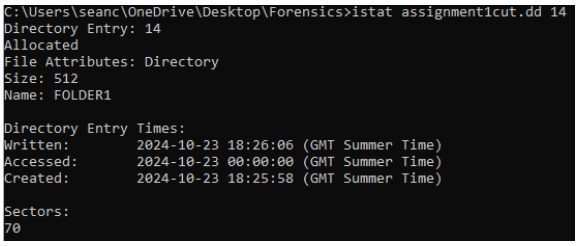


Figure 12: `istat` output for Node 14

- Node 15: Directory `_hip`

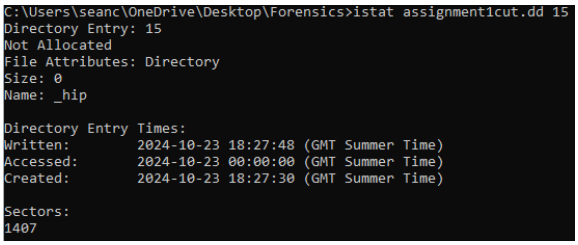


Figure 13: `istat` output for Node 15

5 Directory Entry

To analyze the `For Buster` directory, the hex data in 32-byte segments was examined, each representing a directory entry. This decoded gave vital details such as filenames, file attributes, starting clusters, and file sizes. The goal was to identify allocated and unallocated files and directories within the disk image.

5.1 Manual Decoding of `For Buster` Directory Entry

The `For Buster` directory entry was located at sector 61 (address `0x7A00`). Below is the decoded information for this entry, where primarily the focus was on fields such as field name, file attributes, starting cluster number, and file content.

Each 32-byte entry represents specific metadata related to files or directories. Below is the manually decoded information for the `For Buster` directory entry.

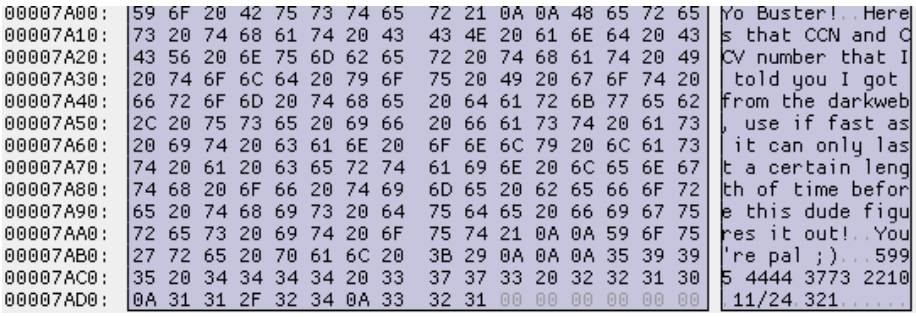


Figure 14: Hex Editor View of `For Buster` Directory Entry

Field	Bytes	Hex Value	Decoded Value
Filename	0–7	59 6F 20 42 75 73 74	Yo Buster!
Extension	8–10	20 21 0A	(empty)
		48 65 72 65 73 20 74 68 61 74	
Content Preview	11–31	20 43 43 4E 20 61 6E 64 20 43 43 56 (continues)	Text message and additional content

Table 2: Decoded Directory Entry for `For Buster` Directory

5.2 Directory Structure Analysis with TSK Commands

To supplement the manual decoding, the ‘fls‘ and ‘istat‘ commands were used from The Sleuth Kit (TSK) to validate and analyze the `For Buster` directory entry.

```
fls assignment1cut.dd
istat assignment1cut.dd 7
```

The ‘istat‘ command output provided metadata, such as timestamps, cluster usage, and file size, confirming the structure and storage details of the `For Buster` directory.

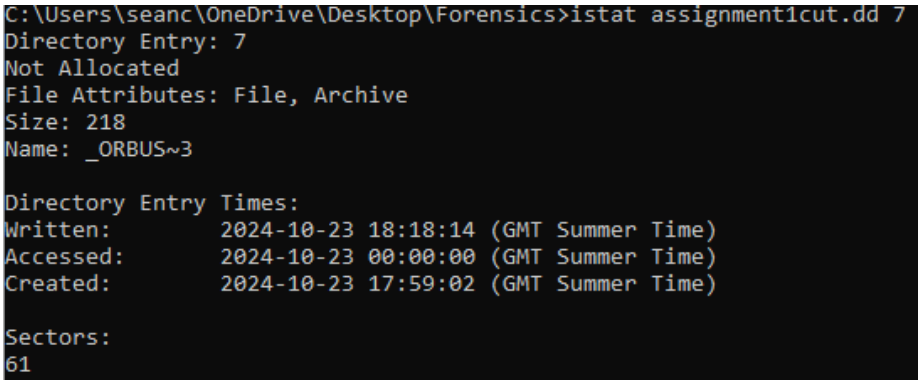


Figure 15: `istat` output for Node Example: `For Buster` Directory

This combination of manual decoding and TSK tools provided a thorough understanding of the data structure, enabling accurate verification of content within the `For Buster` directory.

6 Storage and Deletion

This section demonstrates how files are stored and what changes occur in the FAT12 file system when files are deleted, using examples from the disk image.

6.1 File Storage

To understand file storage, the file `For Buster` was analyzed, examining its clusters and data structure in the FAT12 file system:

- **Cluster Allocation**: The `istat` command shows the clusters allocated to this file. Each allocated cluster is linked in the FAT, pointing to the next cluster in the chain, marking the file's active storage on the disk.

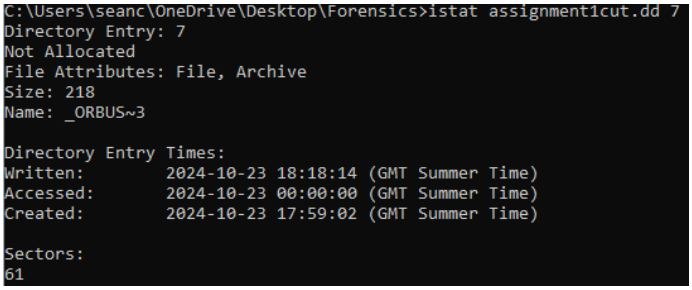


Figure 16: `istat` output showing clusters allocated to `For Buster`

- **Hex Data**: The hex editor view shows how data is stored within clusters for this file. In the stored state, all data clusters are filled with file content, and the FAT entries point to each cluster until reaching an End of File (EOF) marker.

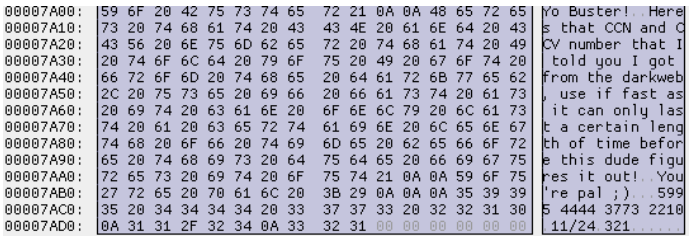


Figure 17: Hex editor view of data clusters allocated to `For Buster`

Stored State Characteristics: - In the stored state, the file is fully integrated into the FAT and directory structure. - The filename is listed in the directory entry, the FAT clusters point from one to the next, and the last cluster has an EOF marker. - File data is fully readable, intact within its assigned clusters, allowing normal access and usage.

6.2 File Deletion

When a file is deleted in FAT12, specific changes occur in the file system structure, marking it as "deleted" but not immediately erasing the file data. Using the `fls` command, the files were identified as deleted by the system.

Deletion Process in FAT12: - **Filename Marker**: The first byte of the filename is replaced with 'E5', signaling the system that this file is no longer active but available for potential overwriting. - **FAT Update**: The FAT entries that previously pointed to the file's clusters are marked as available, releasing these clusters back into the pool of unallocated space. - **Data Remnants**: The data within the clusters remains until new data overwrites these areas, making it possible to recover the deleted file content in forensic analysis.

- **Filename Indicator**: As shown in the hex editor, the first byte of the filename is replaced with 'E5', which marks the entry as deleted. This byte change is the primary indicator of a deleted file.

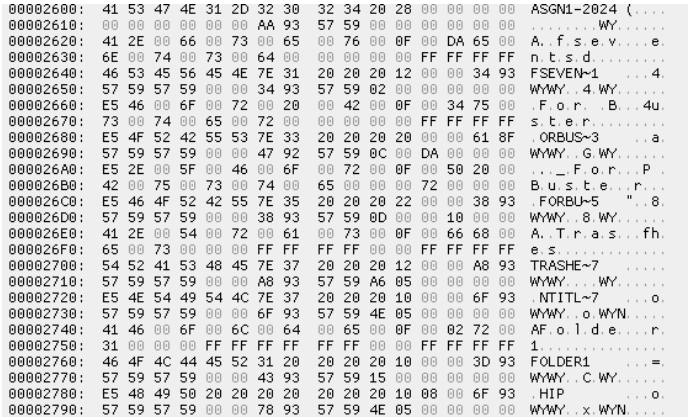


Figure 18: Hex editor view showing 'E5' marker for a deleted file

- **FAT Changes**: With clusters now marked as available, the FAT no longer links these clusters in a chain. The `istat` output below shows how the clusters are now free to be allocated to new files.

Deleted State Characteristics: - In the deleted state, the file's entry is marked by 'E5' in the first byte, and its clusters are freed in the FAT. - Although the FAT no longer links the clusters, the actual data remains in place within the cluster area until it is overwritten. - This leftover data allows forensic tools to recover the file contents as long as they haven't been overwritten by new data.

6.3 Comparison of Stored and Deleted States

The differences between the stored and deleted states provide insights into the recoverability of deleted files:

- **Cluster Allocation**: In the stored state, clusters are allocated and linked; in the deleted state, the FAT releases the clusters, marking them as unallocated.
- **Filename Indicator**: The stored state shows a regular filename, while the deleted state begins with ‘E5‘, indicating that the file is deleted but may still exist in the data area.
- **Data Availability**: In the stored state, the file’s data is readily accessible. In the deleted state, while the FAT releases the clusters, the data itself remains intact until overwritten.

7 File Recovery

File recovery was conducted using Autopsy, where essential files were recovered and analyzed. These files were verified for data integrity through hashing, ensuring they matched the original hash values where available. The primary files recovered included a text file, a PO Box receipt (image file), and an invoice (PDF file).

7.1 Recovered Files

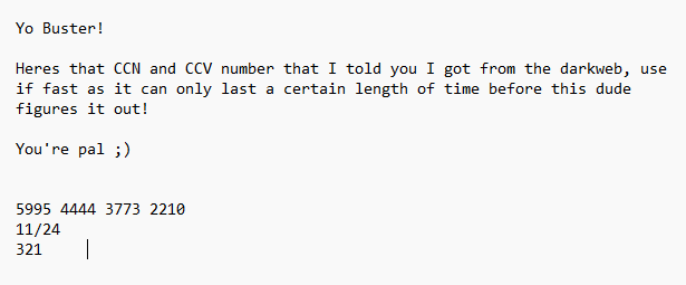
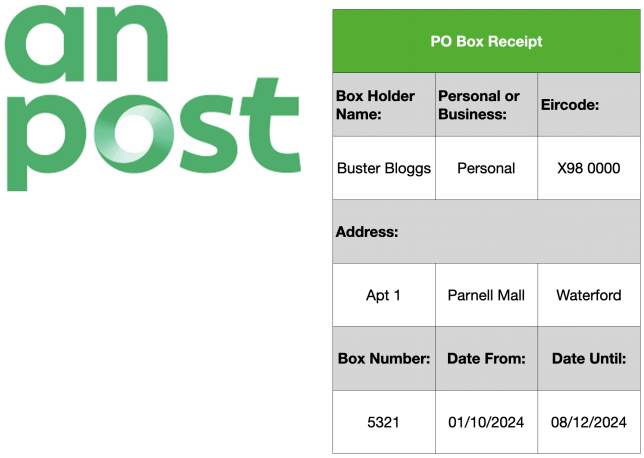
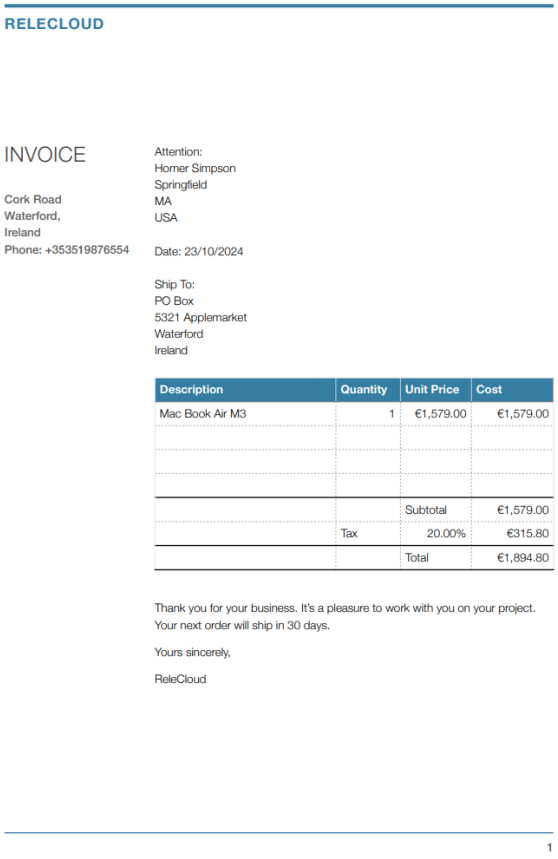


Figure 19: Recovered Text File - Details of Communication



PO Box Receipt		
Box Holder Name:	**Personal or Business:**	**Eircode:**
Buster Bloggs	Personal	X98 0000
Address:		
Apt 1	Parnell Mall	Waterford
Box Number:	**Date From:**	**Date Until:**
5321	01/10/2024	08/12/2024

Figure 20: Recovered PO Box Receipt - Image of the Receipt



RELECLOUD

INVOICE

Cork Road
Waterford,
Ireland
Phone: +353519876554

Attention:
Homer Simpson
Springfield
MA
USA

Date: 23/10/2024

Ship To:
PO Box
5321 Applemarket
Waterford
Ireland

Description	Quantity	Unit Price	Cost
Mac Book Air M3	1	€1,579.00	€1,579.00
		Subtotal	€1,579.00
	Tax	20.00%	€315.80
		Total	€1,894.80

Thank you for your business. It's a pleasure to work with you on your project.
Your next order will ship in 30 days.

Yours sincerely,

ReleCloud

1

Figure 21: Recovered Invoice - PDF Document

7.2 Dual Tool Verification

To ensure that data was not compromised each file recovered was verified with their hash values from the extracted files of autopsy and also by using the dd extraction command matched up these hash values.

```
C:\Users\seanc\OneDrive\Desktop\Forensics>md5sum textfilecut.bin
22298f2bbdb4a6e6ad9361a019aac40d *textfilecut.bin

C:\Users\seanc\OneDrive\Desktop\Forensics>md5sum text_file_autopsy
22298f2bbdb4a6e6ad9361a019aac40d *text_file_autopsy
```

Figure 22: Hash Verification for Recovered Text File

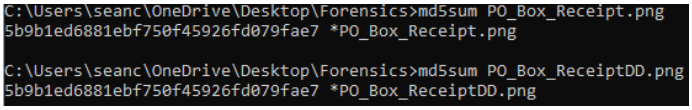


Figure 23: Hash Verification for PO Box Receipt Image

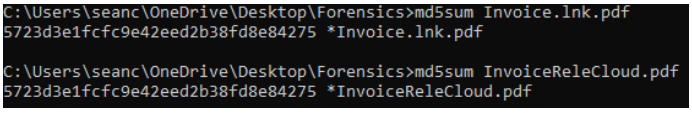


Figure 24: Hash Verification for Invoice PDF

7.3 File Carving

In addition to standard recovery, file carving techniques were used by using Photorec to extract any additional fragments. The file carving process is shown below, demonstrating the steps taken to ensure all recoverable data was extracted.

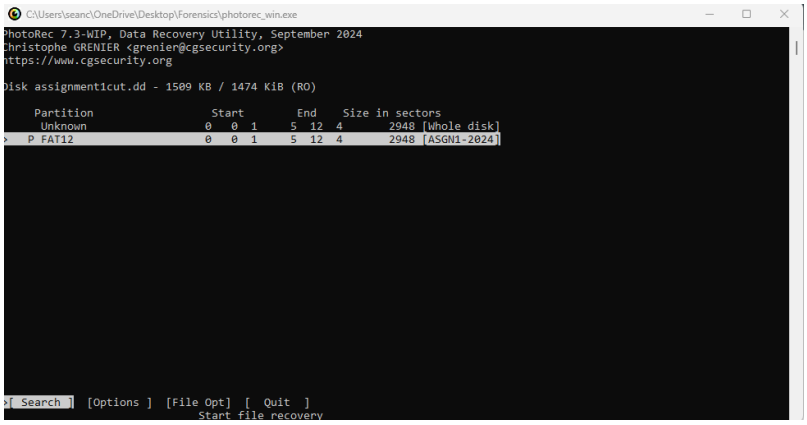


Figure 25: Photorec in Progress for File Carving

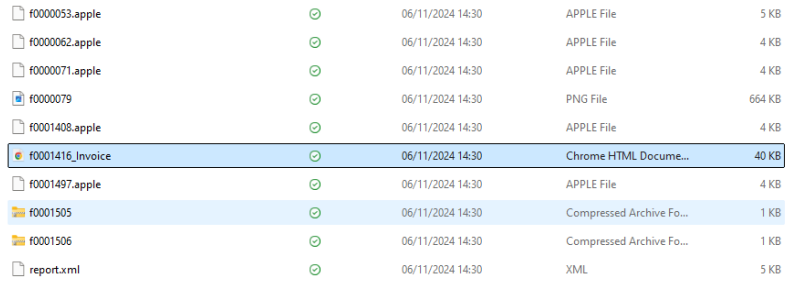


Figure 26: Additional Files Recovered through Photorec File Carving

7.4 Search for Hidden Passwords

A search for hidden passwords was conducted on the extracted text files using command-line tools.

```
C:\Users\seanc\OneDrive\Desktop\Forensics>strings recovered_file.txt | findstr /i "password pass login"
No matching files were found.
```

Figure 27: Command-Line Search for Hidden Passwords

No hidden passwords were identified in this instance.

8 Conclusion

The forensic investigation successfully identified and extracted essential evidence from the disk image, confirming key details related to the case.

- **Victim Identification:** The victim in this investigation is Homer Simpson, as identified from the recovered files.
- **Credit Card Information:** During analysis, the following credit card details were recovered:
  - Card Number: 5995 4444 3773 2210
  - Expiration Date: 11/24
  - CVV: 321
- **Ordered Item:** Evidence confirms that the item ordered was a MacBook Air M3, linked directly to the victim's credit card.
- **Delivery Location:** The MacBook Air M3 was shipped to PO Box 5321 at Applemarket, Waterford, Ireland, as confirmed from the recovered invoice details.
- **Connection Between Suspect and Delivery Location:** The suspect, Buster Bloggs, is directly connected to the delivery location. A PO Box receipt found in the disk image identifies Buster Bloggs as the registered holder of the PO Box where the item was delivered, linking him to the fraudulent order.

This investigation has therefore established a clear connection between the suspect and the order placed with the victim's credit card information, solidifying the evidence against Buster Bloggs.

References

[1] Carrier, B. (2005). *The Sleuth Kit (TSK) & Autopsy: Open Source Digital Forensics Tools*. Retrieved from `https://www.sleuthkit.org/`

[2] Carrier, B. (2018). *Autopsy: Digital Forensics*. Retrieved from `https://www.autopsy.com/`

[3] Grenier, C. (2008). *PhotoRec: File Recovery Software*. CGSecurity. Retrieved from `https://www.cgsecurity.org/wiki/PhotoRec`

[4] Fairfax County, VA. (n.d.). *FAU Forensics Tools: Windows Incident Response & Digital Forensics*. Retrieved from `https://fau.forensicstools.org/`