Table of Contents

1 Section 1 – Practical Digital Forensics Investigation

1.1 Introduction

This section documents the digital forensic process for investigating the allegations against the staff member, Susan Canning. The investigation was conducted using the Advanced Data Acquisition model (ADAM) and aligned with the ACPO guide, Good Practice Guide for Digital Evidence (2012). The tools used for this investigation include Autopsy, OpenStego, and John the Ripper (with RockYou wordlist), which were used to identify and extract hidden information from image files, uncover encrypted documents and provide the relevant evidence to support this investigation.

The investigation started with the imaging and analysis of a forensically prepared suspect USB Drive, ultimately leading to the recovery and analysis of hidden documents and spreadsheets related to the unauthorised sale of academic work.

This investigation consists of two parts. Section 1 includes a forensic investigation of the alleged misuse of the university's IT systems by the accused person, Susan Canning. While section 2 consists of the legal and ethical issues linked to section 1.

1.2 Forensic Methodologies:

Three industry methodologies guided this forensic investigation, including the ADAM Model, the NIST SP 800-86 process and the ACPO Good Practice Guide for Digital Evidence. This ensured that all the evidence was handled in a forensically sound manner, was legally viable, and was fully documented.

1.2.1 ADAM Model (Advanced Data Acquisition Model):

The investigation followed the three stages in the ADAM Model (Adams, Hobbs and Mann, 2013):

1. Preparation and Planning:

   Before any data was used, the two USB drives were wiped using Diskpart to ensure they were forensically clean. Drive A was used to load the suspect data (from Blackboard), while Drive B was used to store any recovered evidence and outputs. The investigation used forensic tools such as Autopsy, OpenStego and John the Ripper, and a specific process to ensure they would not alter the original data.

2. Acquisition:

   The suspect drive was added to Autopsy using the "Local Disk" option. Although a forensic image was not created, Autopsy read the drive using read-only mode, preserving the original data without modifying it.

3. Analysis and Reporting:

   The data was then analysed for any signs of tampering, hidden files and anti-forensic techniques. Bitmap files within the data were noticed as having unusually large sizes and odd naming conventions, which were tested using OpenStego, based upon passwords acquired by the green notepad (*Figure 1 – Photograph 11 from*

Investigation Scenario). The Excel files were encrypted and required decryption, which was done using John the Ripper and the *rockyou* wordlist in Kali Linux.

All evidence was documented with:

- Timestamps
- Screenshots
- Passwords used
- Tool outputs
- Description of file contents.

This ensured the investigation included the complete chain of custody and documented recordings.

1.2.2 NIST SP 800-86 Framework:

The investigation followed the NIST SP 800-86 guidelines (Dr Muhammad Usman, 2024):

- Collection – Data was collected from Blackboard and transferred to the suspect USB using Autopsy in a forensically sound manner.
- Examination – Tools like Autopsy and OpenStego were used to uncover hidden files and metadata (e.g., hidden flags, large file sizes).
- Analysis – The extracted files (invoices, spreadsheets, passwords) were analysed and further decrypted using John the Ripper.
- Reporting – The investigation followed a clear timeline and evidence chain, which has been presented in the report evidence table.

This ensured that the integrity of the data was kept, as well as that every action was repeatable and justified, in line with forensic best practices.

1.2.3 ACPO Good Practice Guide for Digital Evidence (2012) Guidelines:

The investigation followed the four ACPO principles to preserve data integrity and follow the legal guidelines so the evidence is credible (ACPO, 2012).

The key principle observed throughout the process was:

Principle 1: ‘*No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.’* – Complies by using read-only analysis (Autopsy) and separate evidence storage.

Principle 2: ‘*In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.’* – This was followed by only accessing the data through forensic tools (e.g., Autopsy, OpenStego, John the Ripper) and documenting all of the steps in a transparent manner and at no point was the original data modified or directly written to.

Principle 3: ‘*An audit trail or other record of all processes applied to digital evidence should be created and preserved.’* – Every action was recorded with supporting screenshots, timestamps and process notes.

Principle 4: ‘*The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.’* – The investigation was conducted professionally and legally from start to finish.

1.3 Outline Plan:

To begin the investigation, two USB Drives were used:

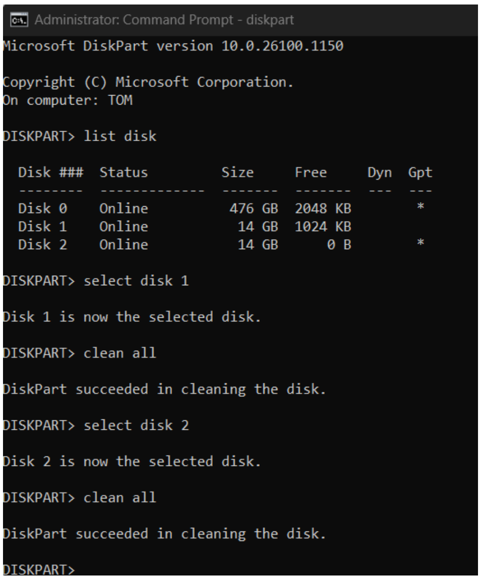
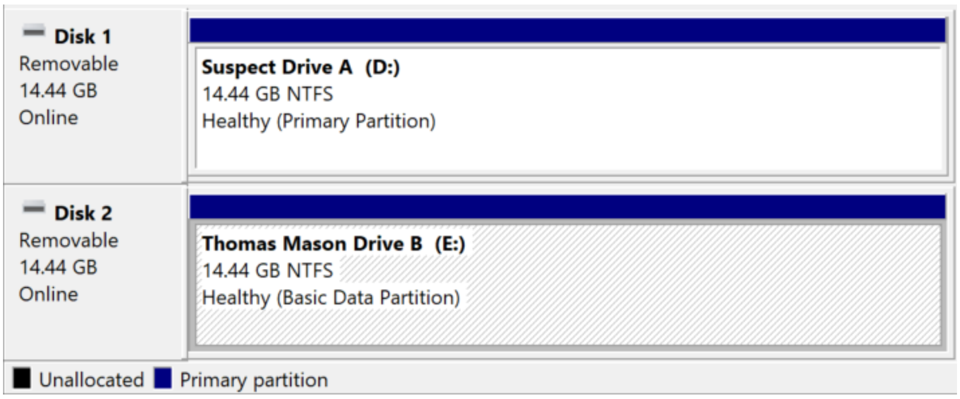
- Drive 1 – Suspect Drive (contains the suspicious data)
- Drive 2 – Thomas Mason Drive (used to store the evidence)

Both drives were forensically wiped using DiskPart on Windows before their use; this ensured that there was no pre-existing data that would interfere with the investigation. The data that Blackboard provided was copied to drive 1 (Suspect Drive) to represent the suspect’s device. The investigation consisted of using the software Autopsy, which is a digital forensic software that is used for file analysis, recovery of deleted files and timeline analysis (Cybervie, 2021). The investigation followed the principles of the ADAM forensic framework, which has three stages:

1. Initial Planning
2. Data Acquisition
3. Data Management

This methodology helped ensure that the proper handling, integrity and analysis of the digital evidence was strict and thorough throughout the process.

-- Table 1: The formatting process

Process Number	Description	Screenshot
1)	*Formatting both disks using DiskPart on the command line.*	
2)	*Disk 1 and 2 Partitions Created.*	

Administrator: Command Prompt - diskpart

```
Microsoft DiskPart version 10.0.26100.1150

Copyright (C) Microsoft Corporation.
On computer: TOM

DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online          476 GB  2048 KB        *
  Disk 1    Online           14 GB  1024 KB
  Disk 2    Online           14 GB      0 B        *

DISKPART> select disk 1

Disk 1 is now the selected disk.

DISKPART> clean all

DiskPart succeeded in cleaning the disk.

DISKPART> select disk 2

Disk 2 is now the selected disk.

DISKPART> clean all

DiskPart succeeded in cleaning the disk.

DISKPART>
```

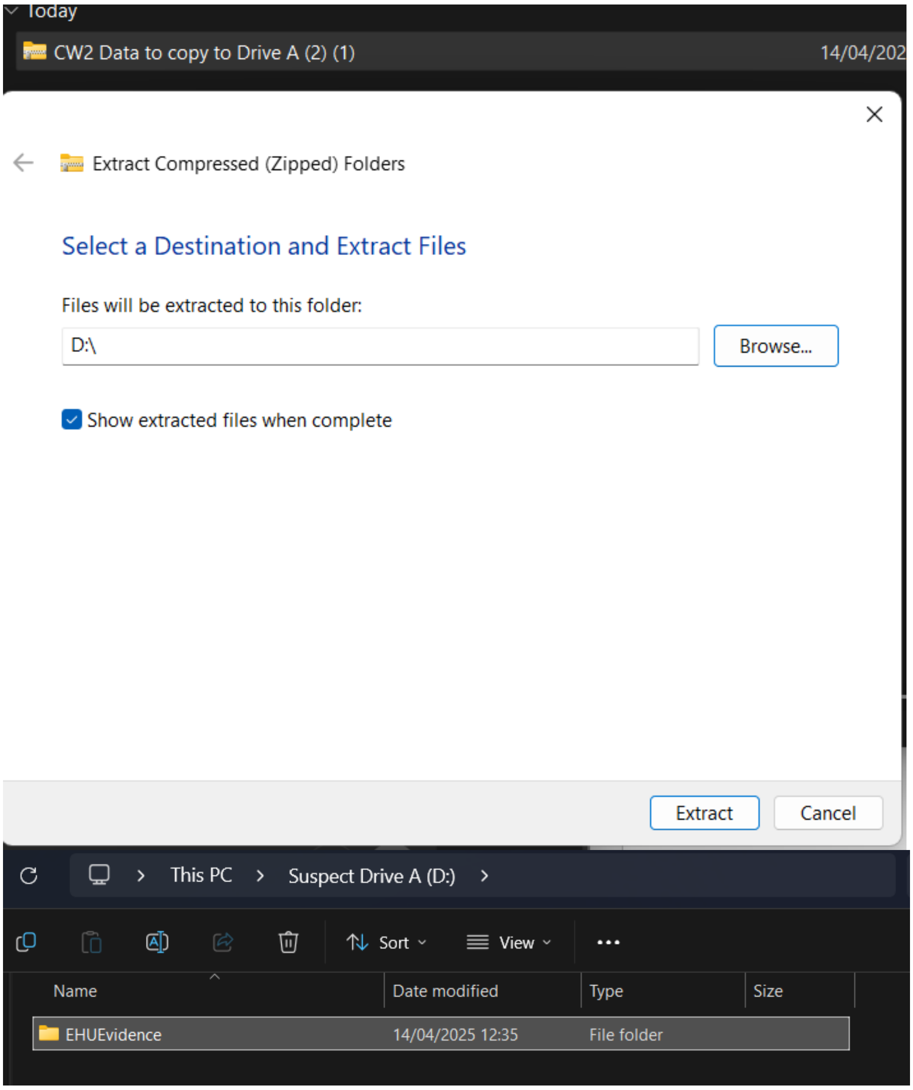
Disk 1
Removable
14.44 GB
Online

Suspect Drive A (D:)
14.44 GB NTFS
Healthy (Primary Partition)

Disk 2
Removable
14.44 GB
Online

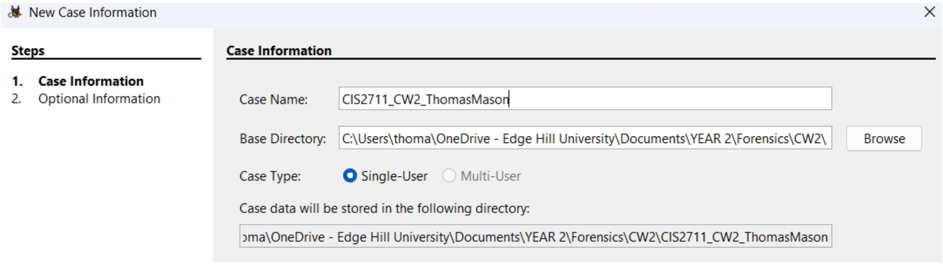
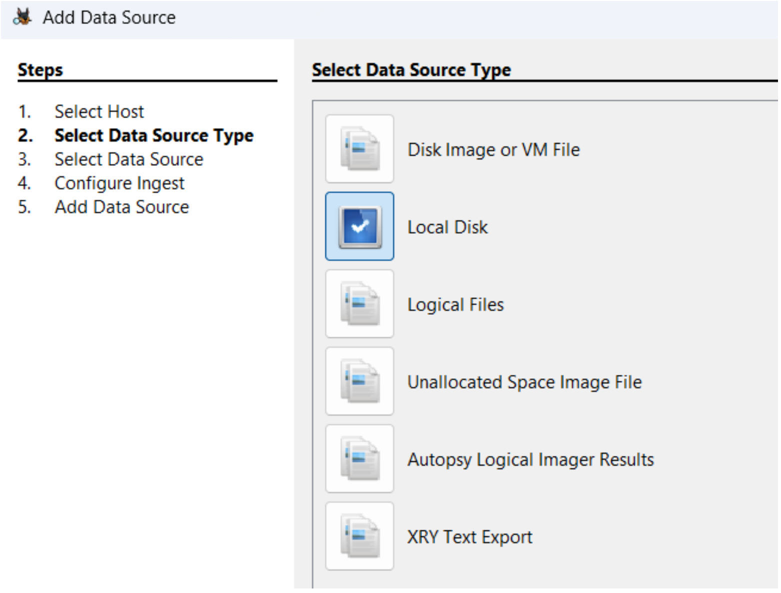
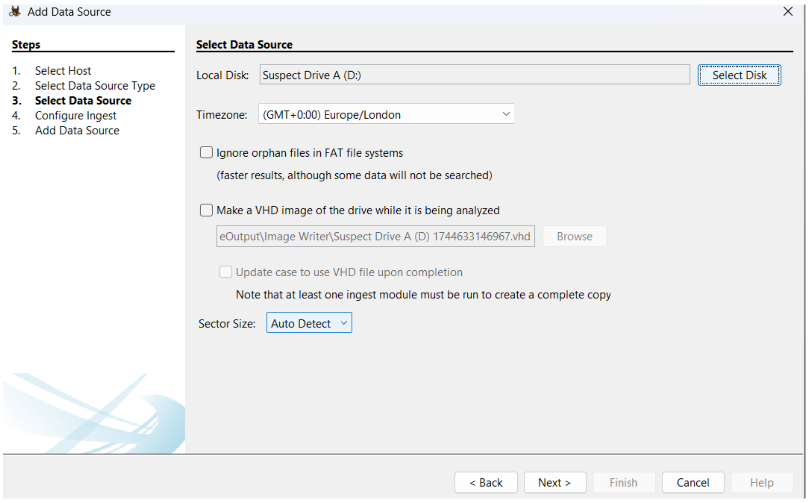
Thomas Mason Drive B (E:)
14.44 GB NTFS
Healthy (Basic Data Partition)

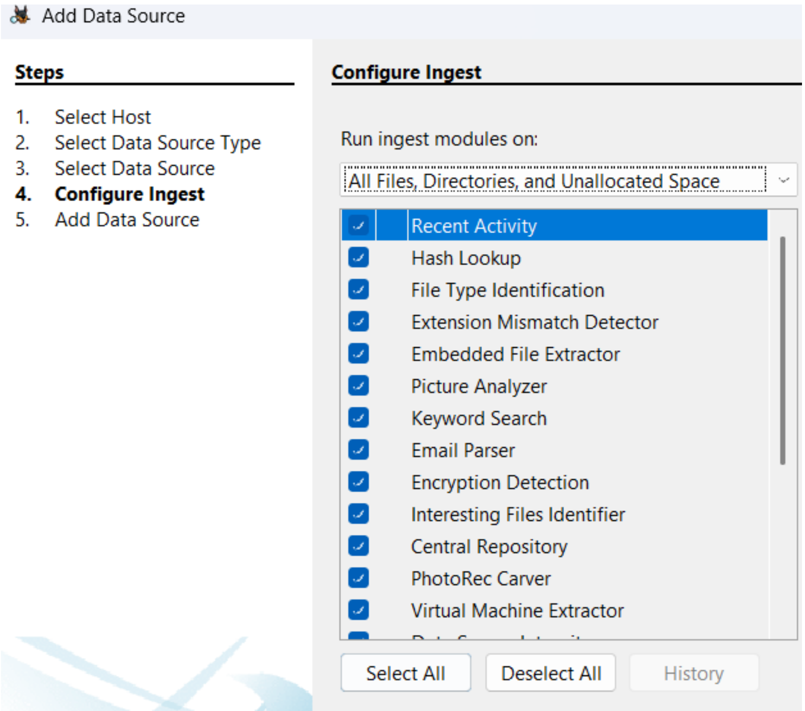
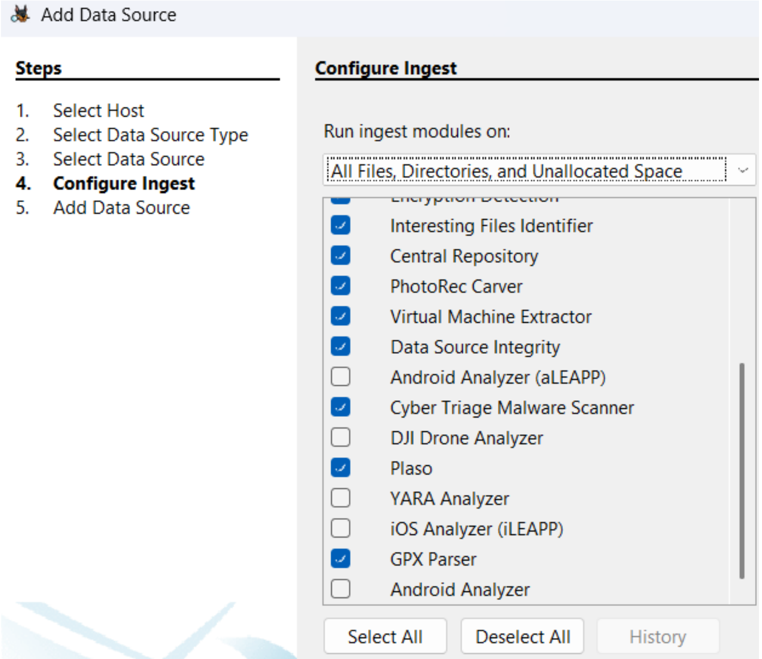
■ Unallocated ■ Primary partition

3)	*Extracting data from the zip folder 'Data to Copy to Drive A' to Disk 1:*	 Today CW2 Data to copy to Drive A (2) (1) 14/04/202 Extract Compressed (Zipped) Folders Select a Destination and Extract Files Files will be extracted to this folder: D:\ Browse... ☑ Show extracted files when complete Extract Cancel This PC > Suspect Drive A (D:) > Sort View Name Date modified Type Size EHUEvidence 14/04/2025 12:35 File folder

1.4 Creating the Case:

-- Table 2: The setup process using Autopsy

Process Number	Description	Screenshot
1)	A new case was created named CIS2711_CW2_ThomasMason, and the base directory for the case was set up in the dedicated folder.	 New Case Information Steps 1. **Case Information** 2. Optional Information **Case Information** Case Name: CIS2711_CW2_ThomasMason Base Directory: C:\Users\thoma\OneDrive - Edge Hill University\Documents\YEAR 2\Forensics\CW2\ Case Type: ● Single-User ○ Multi-User Case data will be stored in the following directory: ɔma\OneDrive - Edge Hill University\Documents\YEAR 2\Forensics\CW2\CIS2711_CW2_ThomasMason
2)	Disk 1 was added as the data source.	 Add Data Source Steps 1. Select Host 2. **Select Data Source Type** 3. Select Data Source 4. Configure Ingest 5. Add Data Source **Select Data Source Type** Disk Image or VM File Local Disk ✓ Logical Files Unallocated Space Image File Autopsy Logical Imager Results XRY Text Export  Add Data Source Steps 1. Select Host 2. Select Data Source Type 3. **Select Data Source** 4. Configure Ingest 5. Add Data Source **Select Data Source** Local Disk: Suspect Drive A (D:) Timezone: (GMT+0:00) Europe/London □ Ignore orphan files in FAT file systems (faster results, although some data will not be searched) □ Make a VHD image of the drive while it is being analyzed eOutput\Image Writer\Suspect Drive A (D) 1744633146967.vhd □ Update case to use VHD file upon completion Note that at least one ingest module must be run to create a complete copy Sector Size: Auto Detect

3)	Autopsy ingest was configured as follows, and once ingested, the investigation began.	 Add Data Source **Steps** 1. Select Host 2. Select Data Source Type 3. Select Data Source **4. Configure Ingest** 5. Add Data Source **Configure Ingest** Run ingest modules on: All Files, Directories, and Unallocated Space ☑ Recent Activity ☑ Hash Lookup ☑ File Type Identification ☑ Extension Mismatch Detector ☑ Embedded File Extractor ☑ Picture Analyzer ☑ Keyword Search ☑ Email Parser ☑ Encryption Detection ☑ Interesting Files Identifier ☑ Central Repository ☑ PhotoRec Carver ☑ Virtual Machine Extractor  Add Data Source **Steps** 1. Select Host 2. Select Data Source Type 3. Select Data Source **4. Configure Ingest** 5. Add Data Source **Configure Ingest** Run ingest modules on: All Files, Directories, and Unallocated Space ☑ Interesting Files Identifier ☑ Central Repository ☑ PhotoRec Carver ☑ Virtual Machine Extractor ☑ Data Source Integrity ☐ Android Analyzer (aLEAPP) ☑ Cyber Triage Malware Scanner ☐ DJI Drone Analyzer ☑ Plaso ☐ YARA Analyzer ☐ iOS Analyzer (iLEAPP) ☑ GPX Parser ☐ Android Analyzer

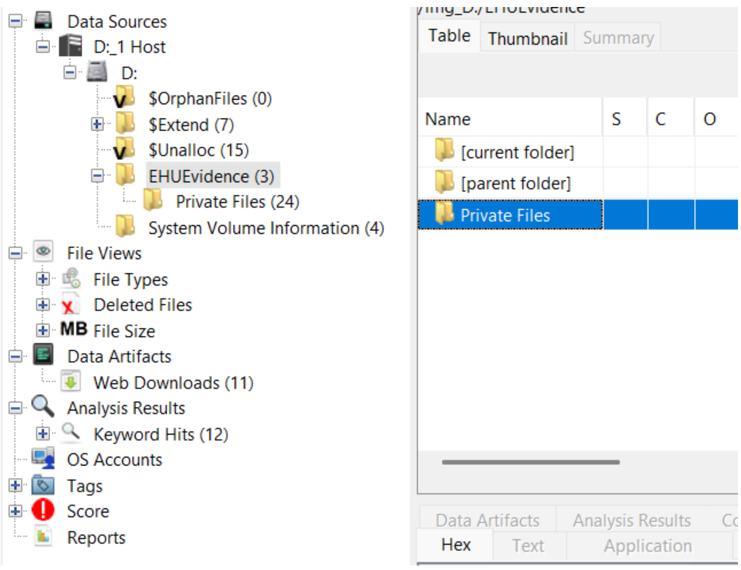
1.5 Summary of Autopsy:

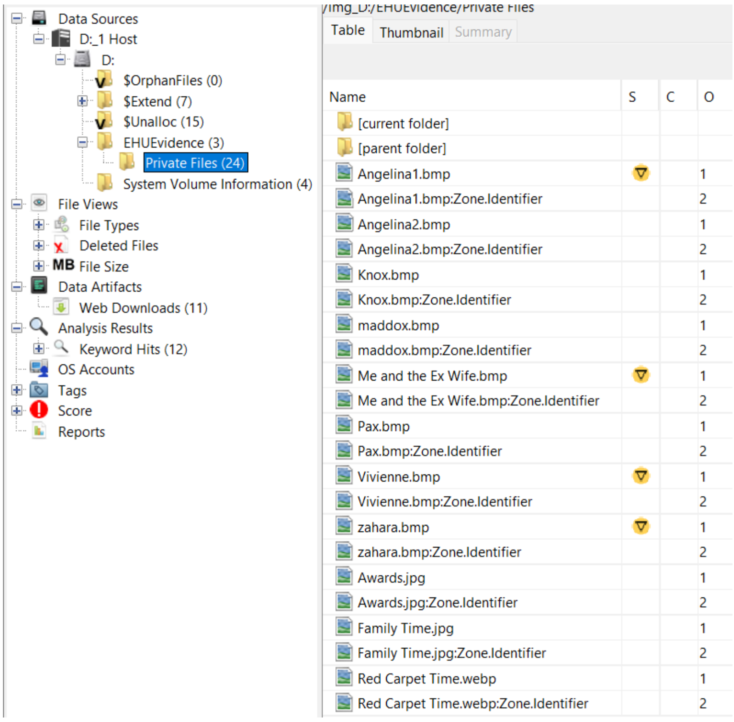
Autopsy was chosen over other forensic tools, such as FTK Imager or Encase, because it is open source, recognised academically and provides a comprehensive range of functions such as timeline analysis, metadata extraction and file recovery (Autopsy, 2023).

During the forensic analysis in Autopsy, several .bmp images were flagged as suspicious due to their inconsistently large file sizes and unexpected file formats (BMP rather than typical JPEGs). Despite appearing visually normal, the size and metadata of these files suggest that they may be used to embed hidden information.

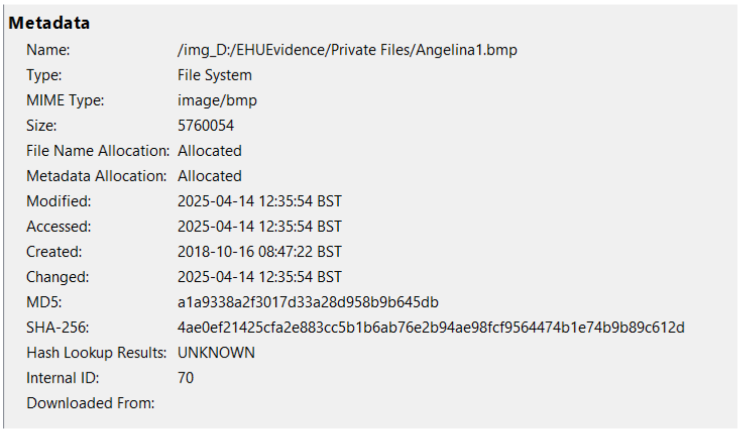
1.6 Evidence Table: Autopsy

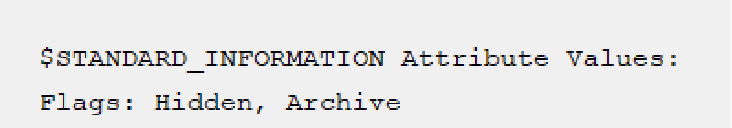
-- Table 3: The evidence collected from Autopsy and the process

Timeline	Screenshot	Notes / Process
16/04/2025, 8:30 AM	 Data Sources D:_1 Host D: $OrphanFiles (0) $Extend (7) $Unalloc (15) EHUEvidence (3) Private Files (24) System Volume Information (4) File Views File Types Deleted Files MB File Size Data Artifacts Web Downloads (11) Analysis Results Keyword Hits (12) OS Accounts Tags Score Reports /img_D:/EHUEvidence Table Thumbnail Summary Name S C O [current folder] [parent folder] Private Files Data Artifacts Analysis Results Hex Text Application	Analysed the local disk and found the ‘EHUEvidence’ folder, which contained a ‘Private Files’ folder.

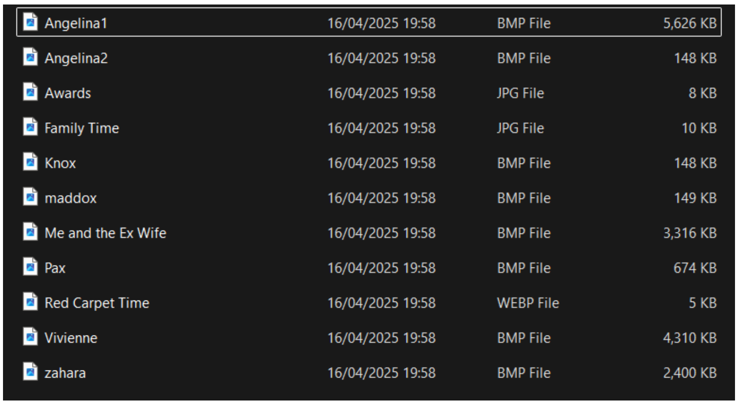
<table>
<tr>
<td>16/04/2025, 8:45 AM</td>
<td>


Data Sources
D:_1 Host
D:
$OrphanFiles (0)
$Extend (7)
$Unalloc (15)
EHUEvidence (3)
Private Files (24)
System Volume Information (4)
File Views
File Types
Deleted Files
MB File Size
Data Artifacts
Web Downloads (11)
Analysis Results
Keyword Hits (12)
OS Accounts
Tags
Score
Reports

/img_D:/EHUEvidence/Private Files
Table Thumbnail Summary
<table>
<tr><th>Name</th><th>S</th><th>C</th><th>O</th></tr>
<tr><td>[current folder]</td><td></td><td></td><td></td></tr>
<tr><td>[parent folder]</td><td></td><td></td><td></td></tr>
<tr><td>Angelina1.bmp</td><td>▼</td><td></td><td>1</td></tr>
<tr><td>Angelina1.bmp:Zone.Identifier</td><td></td><td></td><td>2</td></tr>
<tr><td>Angelina2.bmp</td><td></td><td></td><td>1</td></tr>
<tr><td>Angelina2.bmp:Zone.Identifier</td><td></td><td></td><td>2</td></tr>
<tr><td>Knox.bmp</td><td></td><td></td><td>1</td></tr>
<tr><td>Knox.bmp:Zone.Identifier</td><td></td><td></td><td>2</td></tr>
<tr><td>maddox.bmp</td><td></td><td></td><td>1</td></tr>
<tr><td>maddox.bmp:Zone.Identifier</td><td></td><td></td><td>2</td></tr>
<tr><td>Me and the Ex Wife.bmp</td><td>▼</td><td></td><td>1</td></tr>
<tr><td>Me and the Ex Wife.bmp:Zone.Identifier</td><td></td><td></td><td>2</td></tr>
<tr><td>Pax.bmp</td><td></td><td></td><td>1</td></tr>
<tr><td>Pax.bmp:Zone.Identifier</td><td></td><td></td><td>2</td></tr>
<tr><td>Vivienne.bmp</td><td>▼</td><td></td><td>1</td></tr>
<tr><td>Vivienne.bmp:Zone.Identifier</td><td></td><td></td><td>2</td></tr>
<tr><td>zahara.bmp</td><td>▼</td><td></td><td>1</td></tr>
<tr><td>zahara.bmp:Zone.Identifier</td><td></td><td></td><td>2</td></tr>
<tr><td>Awards.jpg</td><td></td><td></td><td>1</td></tr>
<tr><td>Awards.jpg:Zone.Identifier</td><td></td><td></td><td>2</td></tr>
<tr><td>Family Time.jpg</td><td></td><td></td><td>1</td></tr>
<tr><td>Family Time.jpg:Zone.Identifier</td><td></td><td></td><td>2</td></tr>
<tr><td>Red Carpet Time.webp</td><td></td><td></td><td>1</td></tr>
<tr><td>Red Carpet Time.webp:Zone.Identifier</td><td></td><td></td><td>2</td></tr>
</table>
</td>
<td>After initially reviewing the files, it was found that specific files contained a notable analytical score.</td>
</tr>
<tr>
<td>16/04/2025,
9:00 AM</td>
<td>


<b>Metadata</b>
Name: /img_D:/EHUEvidence/Private Files/Angelina1.bmp
Type: File System
MIME Type: image/bmp
Size: 5760054
File Name Allocation: Allocated
Metadata Allocation: Allocated
Modified: 2025-04-14 12:35:54 BST
Accessed: 2025-04-14 12:35:54 BST
Created: 2018-10-16 08:47:22 BST
Changed: 2025-04-14 12:35:54 BST
MD5: a1a9338a2f3017d33a28d958b9b645db
SHA-256: 4ae0ef21425cfa2e883cc5b1b6ab76e2b94ae98fcf9564474b1e74b9b89c612d
Hash Lookup Results: UNKNOWN
Internal ID: 70
Downloaded From:
</td>
<td>The metadata contains MD5 and SHA-256 hash values, which can be used in the future to verify the integrity of the evidence.</td>
</tr>
<tr>
<td>16/04/2025,
9:15 AM</td>
<td>


<code>$STANDARD_INFORMATION Attribute Values:</code>
<code>Flags: Hidden, Archive</code>
</td>
<td>Upon further investigation, all the files contained hidden flags within the file metadata, suggesting the files have been manually hidden within the file explorer, and suggesting anti-forensic techniques.</td>
</tr>
</table>

16/04/2025, 9:40 AM	 Angelina1 16/04/2025 19:58 BMP File 5,626 KB Angelina2 16/04/2025 19:58 BMP File 148 KB Awards 16/04/2025 19:58 JPG File 8 KB Family Time 16/04/2025 19:58 JPG File 10 KB Knox 16/04/2025 19:58 BMP File 148 KB maddox 16/04/2025 19:58 BMP File 149 KB Me and the Ex Wife 16/04/2025 19:58 BMP File 3,316 KB Pax 16/04/2025 19:58 BMP File 674 KB Red Carpet Time 16/04/2025 19:58 WEBP File 5 KB Vivienne 16/04/2025 19:58 BMP File 4,310 KB zahara 16/04/2025 19:58 BMP File 2,400 KB	All the files within the folder 'Private Files' were exported to the USB Drive 2 for further investigation. This is due to the files being suspiciously hidden, having inconsistently large file sizes, and unexpected file formats.

1.7 Anti-Forensic Techniques:

The next part of the investigation consisted of researching anti-forensic methods for images. One particular anti-forensic technique was specific to hiding data in images: Steganography works by using a graphical image as a front to cover up and hide data in files to prevent the detection of data (Tai, 2022). This can be used for images such as JPEG and BMP, which are included in the evidence drive (The ITM Team and Weston, 2024).

1.8 OpenStego Data Extraction:

OpenStego was selected for the steganographic analysis because of its simplicity and reliability, with the ability to embed files to hide them and extract hidden files with a password. Compared to alternatives such as StegHide, OpenStego uses an easy-to-use GUI and is well-suited for forensic investigations where multiple images require systematic analysis. Furthermore, its compatibility with BMP files made it highly well-suited for the purposes of this investigation (Vaidya, 2021).

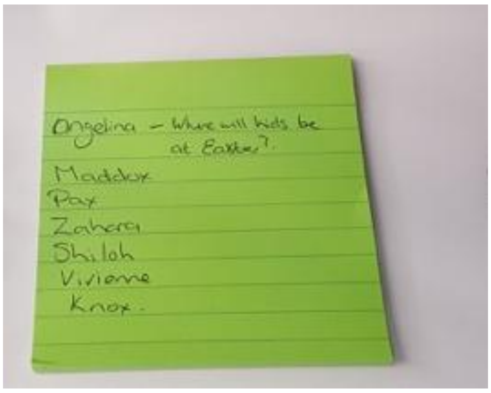
OpenStego is a steganography software that can hide and extract files using images. In order to successfully extract data from the images, a password is needed; photograph 11 was used from the investigation scenario, as it was noted to potentially contain passwords.

1.9 John the Ripper Password Extraction:

John the Ripper was chosen as the password cracking tool due to its long-standing reputation and effectiveness for cracking encrypted files using a dictionary (such as rockyou.txt) and brute force attacks. While there are other tools, such as hashcat, which also offer powerful cracking abilities, John the Ripper was best suited for this investigation because of its smooth integration with Kali Linux, support for Microsoft Office hash formats, and doesn't require high-performance GPU hardware (Wikipedia, 2021).

1.10 How the Passwords were Cracked:

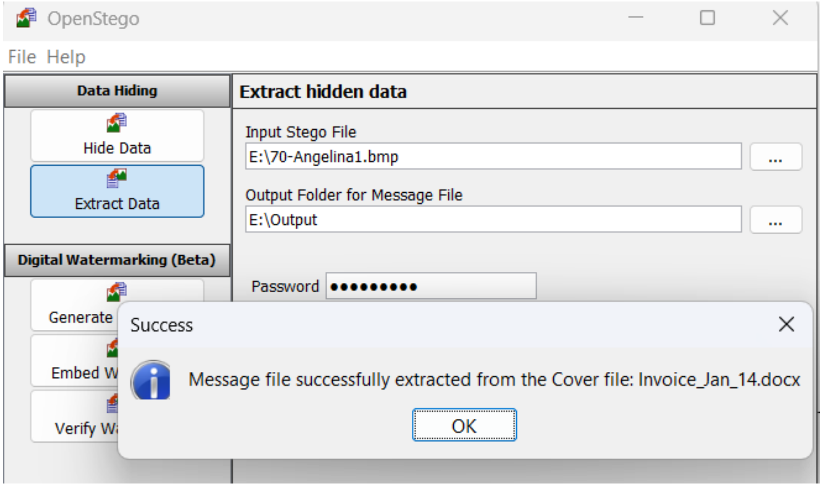
Figure 1: Green notepad with passwords – Photograph 11 from Investigation Scenario.

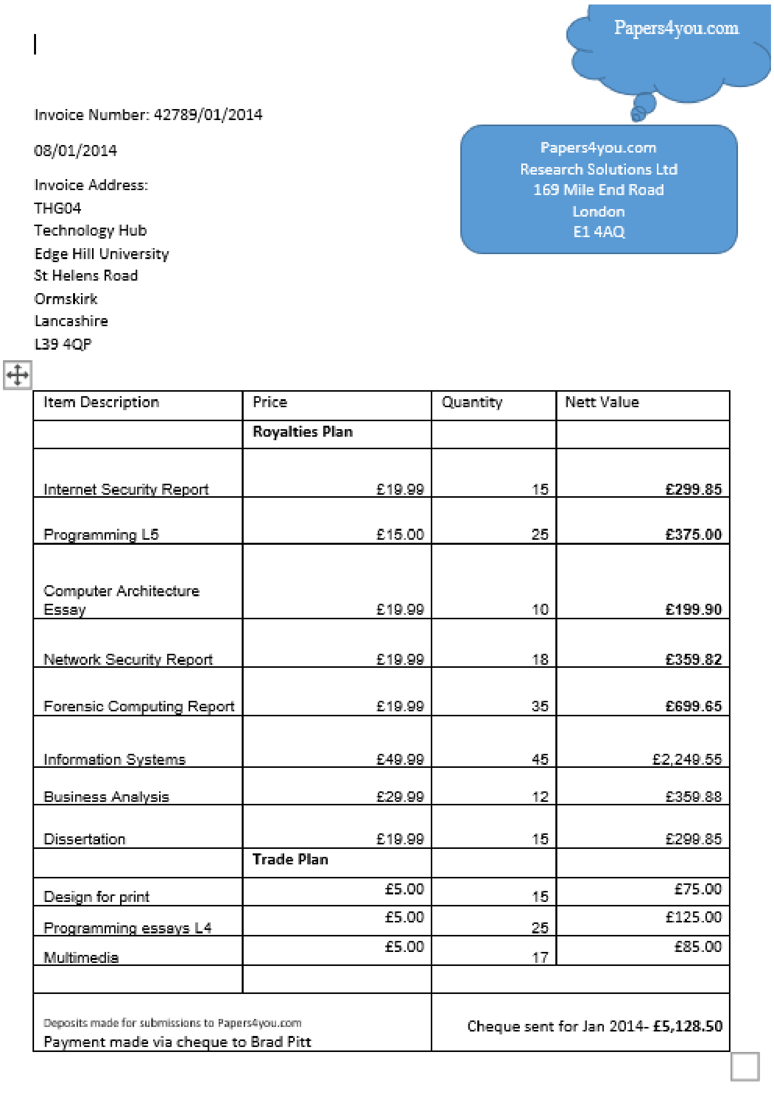


During the investigation, one of the biggest dilemmas was successfully cracking the passwords for the BMP images. Within the investigation scenario, photograph 11 included a list of potential passwords. For the majority of the passwords, it was the file name or one of the names in the notepad, all in lowercase. However, for the image "Me and the Ex Wife", the password was not the file name and was 'shiloh' from the notepad, which was solved using a process of logical elimination for the remaining names.

1.11 Evidence Table: Openstego and Extracted Files

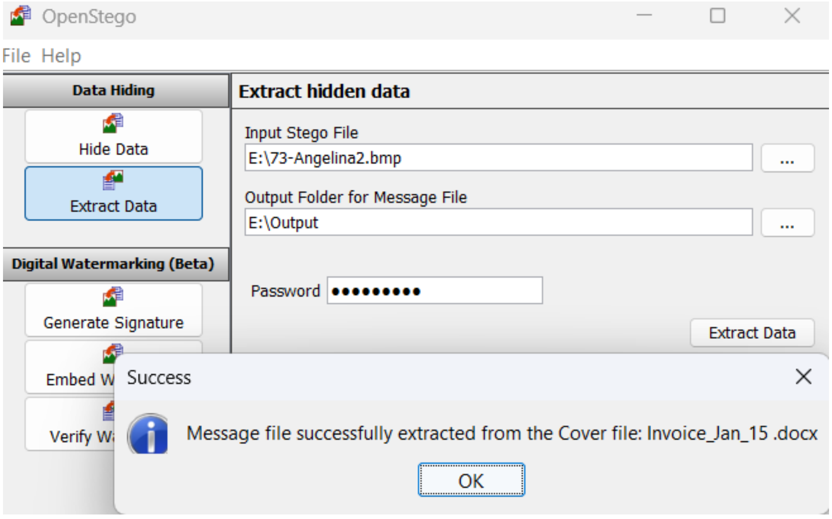
-- Table 4: The evidence collected from OpenStego and John the Ripper

Timeline	Screenshot	Notes / Process
16/04/2025, 11:02AM	 OpenStego File Help Data Hiding Hide Data Extract Data Digital Watermarking (Beta) Generate Embed W Verify W Extract hidden data Input Stego File E:\70-Angelina1.bmp Output Folder for Message File E:\Output Password ••••••••• Success Message file successfully extracted from the Cover file: Invoice_Jan_14.docx OK	Evidence Number 1 *Angelina1.bmp*, which was identified via Autopsy as suspicious. The file stood out due to its unusually large file size (5,626 KB) and BMP format, which is less common for everyday use but commonly used for steganography techniques due to its lossless compression. 1) Originally, '*angelina'* was entered, corresponding to the green note (figure 1); however, within the

<table>
<tr><td></td><td></td><td>private files, there were 2 ‘<i>Angelina</i>’ images.
2) The number ‘1’ was then applied at the end.
3) The password ‘<i>angelina1</i>’ was entered into OpenStego to extract the hidden document successfully.</td></tr>
<tr><td>16/04/2025,
11:27 AM</td><td>
Papers4you.com
Invoice Number: 42789/01/2014
08/01/2014
Invoice Address:
THG04
Technology Hub
Edge Hill University
St Helens Road
Ormskirk
Lancashire
L39 4QP
Papers4you.com
Research Solutions Ltd
169 Mile End Road
London
E1 4AQ
<table>
<tr><th>Item Description</th><th>Price</th><th>Quantity</th><th>Nett Value</th></tr>
<tr><td></td><td><b>Royalties Plan</b></td><td></td><td></td></tr>
<tr><td>Internet Security Report</td><td>£19.99</td><td>15</td><td>£299.85</td></tr>
<tr><td>Programming L5</td><td>£15.00</td><td>25</td><td>£375.00</td></tr>
<tr><td>Computer Architecture Essay</td><td>£19.99</td><td>10</td><td>£199.90</td></tr>
<tr><td>Network Security Report</td><td>£19.99</td><td>18</td><td>£359.82</td></tr>
<tr><td>Forensic Computing Report</td><td>£19.99</td><td>35</td><td>£699.65</td></tr>
<tr><td>Information Systems</td><td>£49.99</td><td>45</td><td>£2,249.55</td></tr>
<tr><td>Business Analysis</td><td>£29.99</td><td>12</td><td>£359.88</td></tr>
<tr><td>Dissertation</td><td>£19.99</td><td>15</td><td>£299.85</td></tr>
<tr><td></td><td><b>Trade Plan</b></td><td></td><td></td></tr>
<tr><td>Design for print</td><td>£5.00</td><td>15</td><td>£75.00</td></tr>
<tr><td>Programming essays L4</td><td>£5.00</td><td>25</td><td>£125.00</td></tr>
<tr><td>Multimedia</td><td>£5.00</td><td>17</td><td>£85.00</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">Deposits made for submissions to Papers4you.com
Payment made via cheque to Brad Pitt</td><td colspan="2">Cheque sent for Jan 2014- <b>£5,128.50</b></td></tr>
</table></td><td>This Word document, extracted from ‘<i>Angelina1.bmp</i>’, shows the financial transactions related to the sale of academic materials.
A payment of £5,128.50 is documented.
It shows the cheque was made out to Brad Pitt, not the suspected staff member, Susan Canning.
This provided the first direct link between Brad Pitt and the sale of academic work supporting the theory that brad was using Susan's computer.</td></tr>
</table>

16/04/2025,

12:05 PM



Input Stego File: E:\73-Angelina2.bmp

Output Folder for Message File: E:\Output

Password: ●●●●●●●●●

Success

Message file successfully extracted from the Cover file: Invoice_Jan_15 .docx

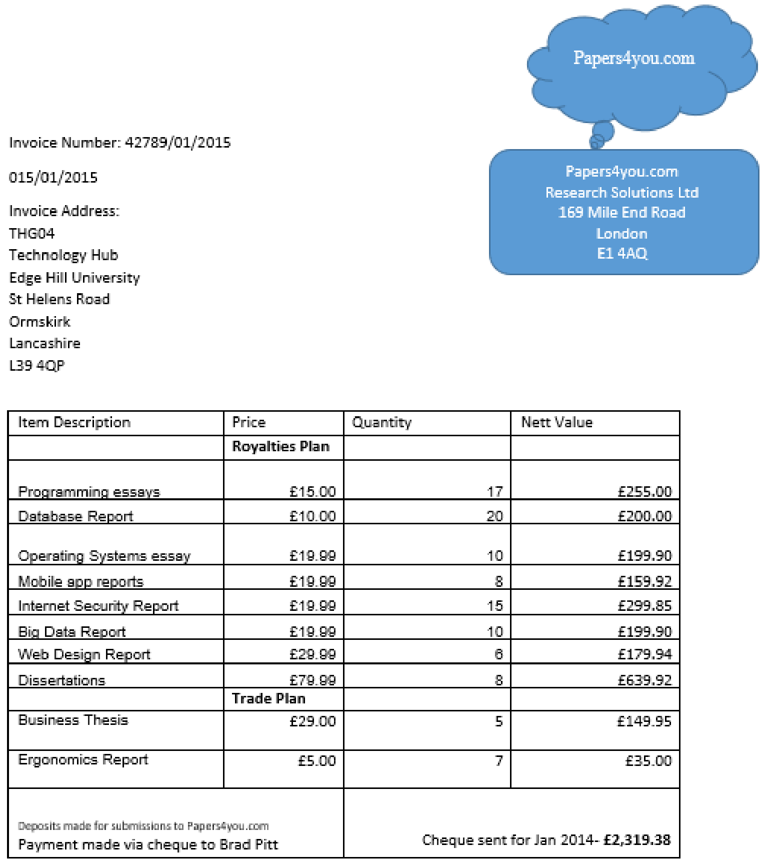
Evidence Number 2, *Angelina2.bmp,* which was identified via Autopsy, was not unusually large (148 KB).

While the file size was not unusual compared to the other .bmp files, there could be a smaller image or hidden file size, and therefore, testing needed to be conducted on the image.

Applying the same logic as the Angelina1 image, the password '*angelina2*' was entered into OpenStego to extract the hidden document successfully.

16/04/2025,

12:31 PM



Papers4you.com

Papers4you.com
Research Solutions Ltd
169 Mile End Road
London
E1 4AQ

Invoice Number: 42789/01/2015

015/01/2015

Invoice Address:
THG04
Technology Hub
Edge Hill University
St Helens Road
Ormskirk
Lancashire
L39 4QP

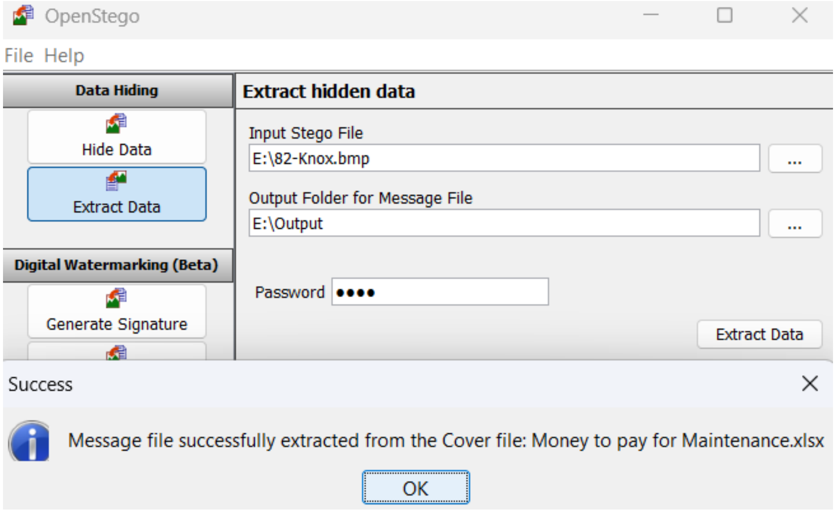
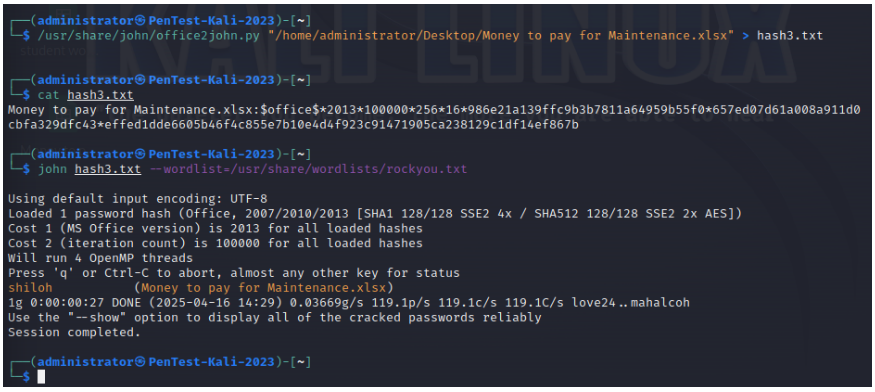
Item Description	Price	Quantity	Nett Value
	Royalties Plan		
Programming essays	£15.00	17	£255.00
Database Report	£10.00	20	£200.00
Operating Systems essay	£19.99	10	£199.90
Mobile app reports	£19.99	8	£159.92
Internet Security Report	£19.99	15	£299.85
Big Data Report	£19.99	10	£199.90
Web Design Report	£29.99	6	£179.94
Dissertations	£79.99	8	£639.92
	Trade Plan		
Business Thesis	£29.00	5	£149.95
Ergonomics Report	£5.00	7	£35.00
Deposits made for submissions to Papers4you.com Payment made via cheque to Brad Pitt		Cheque sent for Jan 2014- **£2,319.38**	

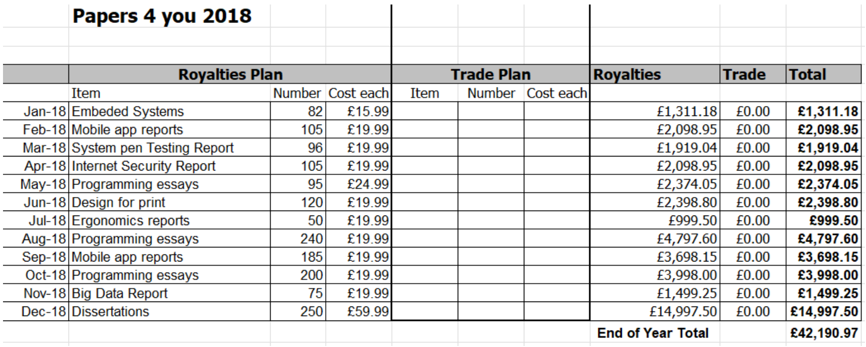
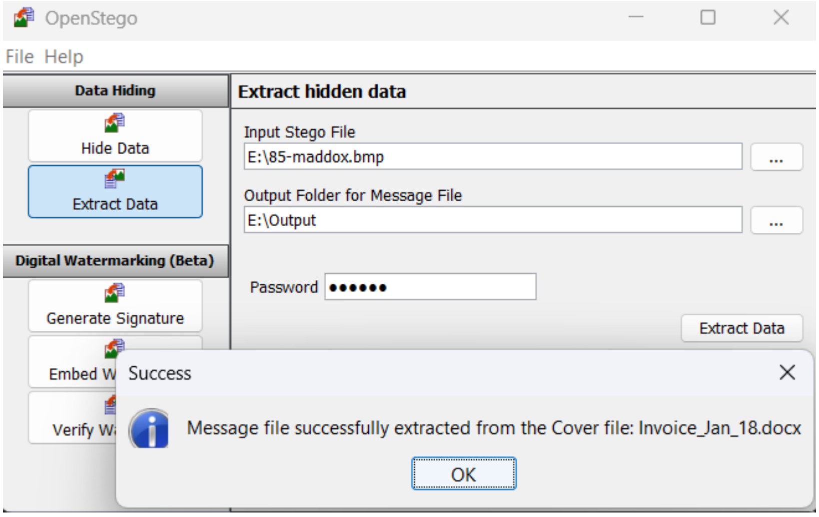
This document, extracted from *Angelina2.bmp*, provides further proof of evidence for academic assignments being sold.

The invoice includes essays, reports and dissertations and provides a check amount of £2,319.38, which was issued to Brad Pitt and not Susan Canning.

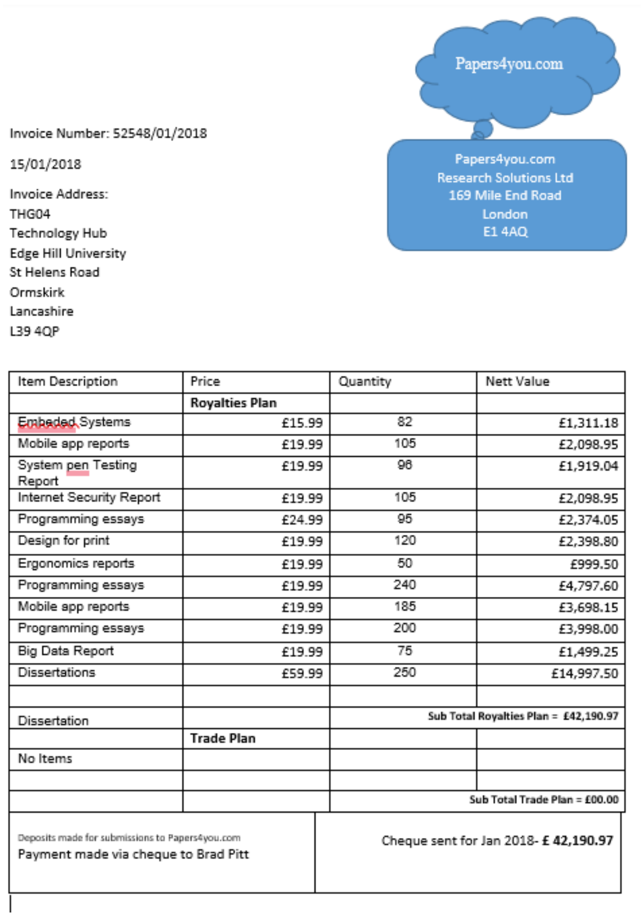
The intentional use of steganography to hide the invoice suggests that it was a deliberate effort to conceal the transactions.

This further adds to the chain of financial evidence that links Brad

		Pitt to the seller of academic work.
16/04/2025, 1:15 PM	 OpenStego File Help Data Hiding Hide Data Extract Data Digital Watermarking (Beta) Generate Signature Extract hidden data Extract Data OK Input Stego File E:\82-Knox.bmp Output Folder for Message File E:\Output Password •••• Success Message file successfully extracted from the Cover file: Money to pay for Maintenance.xlsx	Evidence Number 3, *Knox.bmp* (148 KB) was flagged for testing due to the matching name '*Knox*', which was written on the Green notepad (figure 1) found within the investigation scenario. While the file was relatively small and not obviously suspicious, it was another BMP file, and due to the pattern of hidden content using passwords from the notebook, it was tested and found to successfully reveal a hidden file using the password '*knox*'.
16/04/2025, 2:02 PM	 ┌──(administrator㉿PenTest-Kali-2023)-[~] └─$ /usr/share/john/office2john.py "/home/administrator/Desktop/Money to pay for Maintenance.xlsx" > hash3.txt ┌──(administrator㉿PenTest-Kali-2023)-[~] └─$ cat hash3.txt Money to pay for Maintenance.xlsx:$office$*2013*100000*256*16*986e21a139ffc9b3b7811a64959b55f0*657ed07d61a008a911d0cbfa329dfc43*effed1dde6605b46f4c855e7b10e4d4f923c91471905ca238129c1df14ef867b ┌──(administrator㉿PenTest-Kali-2023)-[~] └─$ john hash3.txt --wordlist=/usr/share/wordlists/rockyou.txt Using default input encoding: UTF-8 Loaded 1 password hash (Office, 2007/2010/2013 [SHA1 128/128 SSE2 4x / SHA512 128/128 SSE2 2x AES]) Cost 1 (MS Office version) is 2013 for all loaded hashes Cost 2 (iteration count) is 100000 for all loaded hashes Will run 4 OpenMP threads Press 'q' or Ctrl-C to abort, almost any other key for status shiloh (Money to pay for Maintenance.xlsx) 1g 0:00:00:27 DONE (2025-04-16 14:29) 0.03669g/s 119.1p/s 119.1c/s 119.1C/s love24..mahalcoh Use the "--show" option to display all of the cracked passwords reliably Session completed. ┌──(administrator㉿PenTest-Kali-2023)-[~] └─$	Upon opening the Maintenance.xlsx file extracted from *Knox.bmp*, it was found that the Excel file was encrypted with a password. 1) The file was processed through *office2john.py,* a Kali Linux tool for extracting password hashes. 2) The password hash was saved and cracked using *John the Ripper* with the *rockyou* wordlist. 3) The password was successfully cracked and identified as '*shiloh'*, and upon reviewing the green

<table>
<tr><td></td><td></td><td>password note (Figure 1), it also appears there.</td></tr>
<tr><td>16/04/2025,
2:13 PM</td><td>
<table>
<tr><td></td><td colspan="3"><b>Papers 4 you 2018</b></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="3"><b>Royalties Plan</b></td><td colspan="3"><b>Trade Plan</b></td><td><b>Royalties</b></td><td><b>Trade</b></td><td><b>Total</b></td></tr>
<tr><td></td><td>Item</td><td>Number</td><td>Cost each</td><td>Item</td><td>Number</td><td>Cost each</td><td></td><td></td><td></td></tr>
<tr><td>Jan-18</td><td>Embeded Systems</td><td>82</td><td>£15.99</td><td></td><td></td><td></td><td>£1,311.18</td><td>£0.00</td><td><b>£1,311.18</b></td></tr>
<tr><td>Feb-18</td><td>Mobile app reports</td><td>105</td><td>£19.99</td><td></td><td></td><td></td><td>£2,098.95</td><td>£0.00</td><td><b>£2,098.95</b></td></tr>
<tr><td>Mar-18</td><td>System pen Testing Report</td><td>96</td><td>£19.99</td><td></td><td></td><td></td><td>£1,919.04</td><td>£0.00</td><td><b>£1,919.04</b></td></tr>
<tr><td>Apr-18</td><td>Internet Security Report</td><td>105</td><td>£19.99</td><td></td><td></td><td></td><td>£2,098.95</td><td>£0.00</td><td><b>£2,098.95</b></td></tr>
<tr><td>May-18</td><td>Programming essays</td><td>95</td><td>£24.99</td><td></td><td></td><td></td><td>£2,374.05</td><td>£0.00</td><td><b>£2,374.05</b></td></tr>
<tr><td>Jun-18</td><td>Design for print</td><td>120</td><td>£19.99</td><td></td><td></td><td></td><td>£2,398.80</td><td>£0.00</td><td><b>£2,398.80</b></td></tr>
<tr><td>Jul-18</td><td>Ergonomics reports</td><td>50</td><td>£19.99</td><td></td><td></td><td></td><td>£999.50</td><td>£0.00</td><td><b>£999.50</b></td></tr>
<tr><td>Aug-18</td><td>Programming essays</td><td>240</td><td>£19.99</td><td></td><td></td><td></td><td>£4,797.60</td><td>£0.00</td><td><b>£4,797.60</b></td></tr>
<tr><td>Sep-18</td><td>Mobile app reports</td><td>185</td><td>£19.99</td><td></td><td></td><td></td><td>£3,698.15</td><td>£0.00</td><td><b>£3,698.15</b></td></tr>
<tr><td>Oct-18</td><td>Programming essays</td><td>200</td><td>£19.99</td><td></td><td></td><td></td><td>£3,998.00</td><td>£0.00</td><td><b>£3,998.00</b></td></tr>
<tr><td>Nov-18</td><td>Big Data Report</td><td>75</td><td>£19.99</td><td></td><td></td><td></td><td>£1,499.25</td><td>£0.00</td><td><b>£1,499.25</b></td></tr>
<tr><td>Dec-18</td><td>Dissertations</td><td>250</td><td>£59.99</td><td></td><td></td><td></td><td>£14,997.50</td><td>£0.00</td><td><b>£14,997.50</b></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td><b>End of Year Total</b></td><td></td><td><b>£42,190.97</b></td></tr>
</table></td><td>The Excel document extracted from <i>Knox.bmp</i> includes detailed financial records, which are linked to essays, reports, and dissertation services.
The use of both steganography and password encryption demonstrates the initial attempt to hide this misconduct.
The cracked password ‘<i>shiloh’</i> further conveys that the green note (Figure 1) was, in fact, the master password list, and this extraction continues to support the theory that Brad Pitt was operating from Susan Canning’s workstation.</td></tr>
<tr><td>16/04/2025,
2:37 PM</td><td>
OpenStego
File Help
Data Hiding
Hide Data
Extract Data
Digital Watermarking (Beta)
Generate Signature
Embed W
Verify W
...
Extract Data
OK

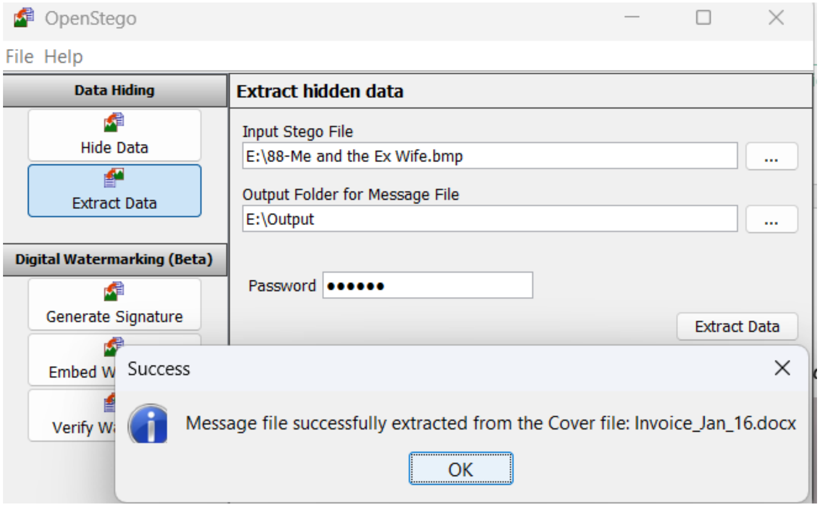
Extract hidden data
Input Stego File: E:\85-maddox.bmp
Output Folder for Message File: E:\Output
Password: ••••••
Success
Message file successfully extracted from the Cover file: Invoice_Jan_18.docx</td><td>Evidence number 4, maddox.bmp (149 KB), matched one of the names on the green notepad (Figure 1). While the file size is not especially large, it followed the same naming source and password pattern as previous successful extractions.
Entering ‘<i>maddox’</i> into OpenStego resulted in the successful extraction of the hidden word document.</td></tr>
</table>

<table>
<tr>
<td>16/04/2025,
2:45 PM</td>
<td>

Papers4you.com

Papers4you.com
Research Solutions Ltd
169 Mile End Road
London
E1 4AQ

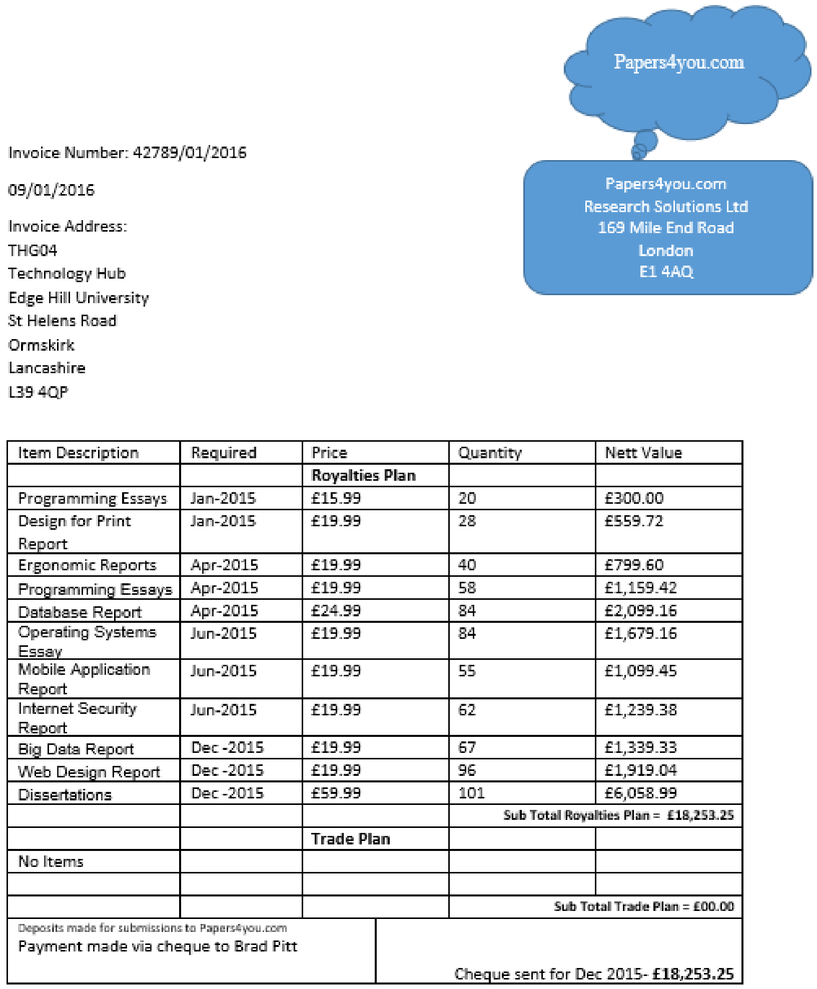
Invoice Number: 52548/01/2018
15/01/2018
Invoice Address:
THG04
Technology Hub
Edge Hill University
St Helens Road
Ormskirk
Lancashire
L39 4QP
<table>
<tr><th>Item Description</th><th>Price</th><th>Quantity</th><th>Nett Value</th></tr>
<tr><td></td><td><b>Royalties Plan</b></td><td></td><td></td></tr>
<tr><td>Embeded Systems</td><td>£15.99</td><td>82</td><td>£1,311.18</td></tr>
<tr><td>Mobile app reports</td><td>£19.99</td><td>105</td><td>£2,098.95</td></tr>
<tr><td>System pen Testing Report</td><td>£19.99</td><td>96</td><td>£1,919.04</td></tr>
<tr><td>Internet Security Report</td><td>£19.99</td><td>105</td><td>£2,098.95</td></tr>
<tr><td>Programming essays</td><td>£24.99</td><td>95</td><td>£2,374.05</td></tr>
<tr><td>Design for print</td><td>£19.99</td><td>120</td><td>£2,398.80</td></tr>
<tr><td>Ergonomics reports</td><td>£19.99</td><td>50</td><td>£999.50</td></tr>
<tr><td>Programming essays</td><td>£19.99</td><td>240</td><td>£4,797.60</td></tr>
<tr><td>Mobile app reports</td><td>£19.99</td><td>185</td><td>£3,698.15</td></tr>
<tr><td>Programming essays</td><td>£19.99</td><td>200</td><td>£3,998.00</td></tr>
<tr><td>Big Data Report</td><td>£19.99</td><td>75</td><td>£1,499.25</td></tr>
<tr><td>Dissertations</td><td>£59.99</td><td>250</td><td>£14,997.50</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td>Dissertation</td><td></td><td colspan="2"><b>Sub Total Royalties Plan = £42,190.97</b></td></tr>
<tr><td></td><td><b>Trade Plan</b></td><td></td><td></td></tr>
<tr><td>No Items</td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td colspan="2"><b>Sub Total Trade Plan = £00.00</b></td></tr>
<tr><td colspan="2">Deposits made for submissions to Papers4you.com
Payment made via cheque to Brad Pitt</td><td colspan="2">Cheque sent for Jan 2018- <b>£ 42,190.97</b></td></tr>
</table>
</td>
<td>This document, extracted from <i>maddox.bmp</i>, provides the financial summary for 2018 from <i>Papers4you.com</i> addressed to Edgehill University.

The invoice includes large quantities of academic work being sold, with 250 dissertations and hundreds of programming essays, mobile app reports, security reports and more; this brings a sub-total of £42,190.97.

This file is the single largest financial invoice that has been recovered, shows the scale of the operation, and once again confirms Brad Pitt as the receiver of the cheque.</td>
</tr>
<tr>
<td>16/04/2025,
3:24 PM</td>
<td>


Extract hidden data
Input Stego File: E:\88-Me and the Ex Wife.bmp
Output Folder for Message File: E:\Output
Password: ••••••
Success
Message file successfully extracted from the Cover file: Invoice_Jan_16.docx
</td>
<td>Evidence number 5 stood out due to its unique filename: <i>Me and the Ex Wife.bmp,</i> and the only <i>.bmp</i> file which did not match any passwords directly based on the file name. The image had a large file size (3,316 KB), which suggested it may contain hidden data.

1) The password was found using a process of elimination from (Figure 1) the green notepad (e.g, angelina, maddox, knox), which had already been successfully used,</td>
</tr>
</table>

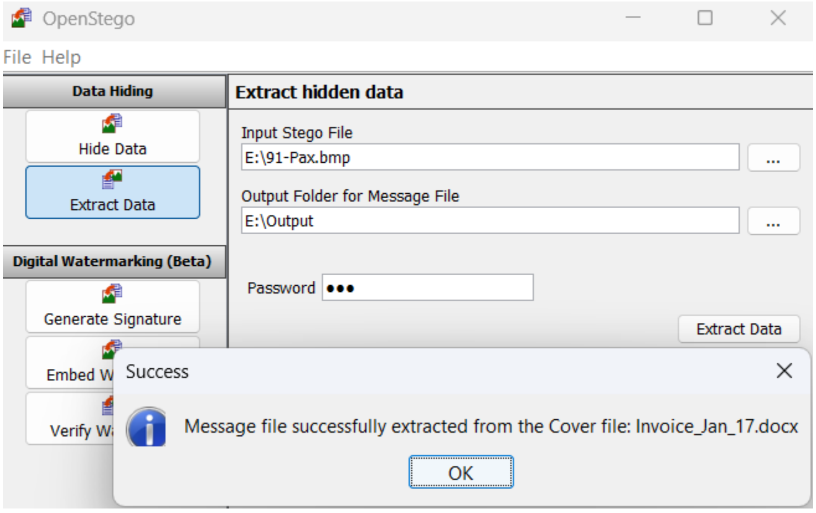
<table>
<tr>
<td></td>
<td></td>
<td>leaving four potential names.
2) Using the same process as before, the password usually matched the file name on the green notepad (Figure 1) in lowercase.
3) After comparing the other files to Notepad, one unused name was left, which was Shiloh.
4) Once entered in all lowercase (<i>shiloh</i>), OpenStego successfully extracted the hidden word document.</td>
</tr>
<tr>
<td>16/04/2025,
3:32 PM</td>
<td>
Papers4you.com
Papers4you.com
Research Solutions Ltd
169 Mile End Road
London
E1 4AQ

Invoice Number: 42789/01/2016

09/01/2016

Invoice Address:
THG04
Technology Hub
Edge Hill University
St Helens Road
Ormskirk
Lancashire
L39 4QP
<table>
<tr><td>Item Description</td><td>Required</td><td>Price</td><td>Quantity</td><td>Nett Value</td></tr>
<tr><td></td><td></td><td><b>Royalties Plan</b></td><td></td><td></td></tr>
<tr><td>Programming Essays</td><td>Jan-2015</td><td>£15.99</td><td>20</td><td>£300.00</td></tr>
<tr><td>Design for Print Report</td><td>Jan-2015</td><td>£19.99</td><td>28</td><td>£559.72</td></tr>
<tr><td>Ergonomic Reports</td><td>Apr-2015</td><td>£19.99</td><td>40</td><td>£799.60</td></tr>
<tr><td>Programming Essays</td><td>Apr-2015</td><td>£19.99</td><td>58</td><td>£1,159.42</td></tr>
<tr><td>Database Report</td><td>Apr-2015</td><td>£24.99</td><td>84</td><td>£2,099.16</td></tr>
<tr><td>Operating Systems Essay</td><td>Jun-2015</td><td>£19.99</td><td>84</td><td>£1,679.16</td></tr>
<tr><td>Mobile Application Report</td><td>Jun-2015</td><td>£19.99</td><td>55</td><td>£1,099.45</td></tr>
<tr><td>Internet Security Report</td><td>Jun-2015</td><td>£19.99</td><td>62</td><td>£1,239.38</td></tr>
<tr><td>Big Data Report</td><td>Dec -2015</td><td>£19.99</td><td>67</td><td>£1,339.33</td></tr>
<tr><td>Web Design Report</td><td>Dec -2015</td><td>£19.99</td><td>96</td><td>£1,919.04</td></tr>
<tr><td>Dissertations</td><td>Dec -2015</td><td>£59.99</td><td>101</td><td>£6,058.99</td></tr>
<tr><td></td><td></td><td></td><td colspan="2"><b>Sub Total Royalties Plan = £18,253.25</b></td></tr>
<tr><td></td><td></td><td><b>Trade Plan</b></td><td></td><td></td></tr>
<tr><td>No Items</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td colspan="2"><b>Sub Total Trade Plan = £00.00</b></td></tr>
<tr><td colspan="2">Deposits made for submissions to Papers4you.com
Payment made via cheque to Brad Pitt</td><td colspan="3">Cheque sent for Dec 2015- <b>£18,253.25</b></td></tr>
</table>
</td>
<td>This document was extracted from <i>Me and the Ex Wife.bmp</i> and includes an invoice from Papers4You.com addressed to Edeg Hill University.
The invoice includes a breakdown of assignments sold throughout 2015, with a total payment of £18,253.25 sent to Brad Pitt via cheque.
There is no mention of Susan Canning being made, and the document adds to the recurring pattern of Brad Pitt being the primary suspect based on the evidence for all academic work sales.</td>
</tr>
</table>

16/04/2025,
3:56 PM



Extract hidden data

Input Stego File: E:\91-Pax.bmp

Output Folder for Message File: E:\Output

Password: •••

Extract Data

Success

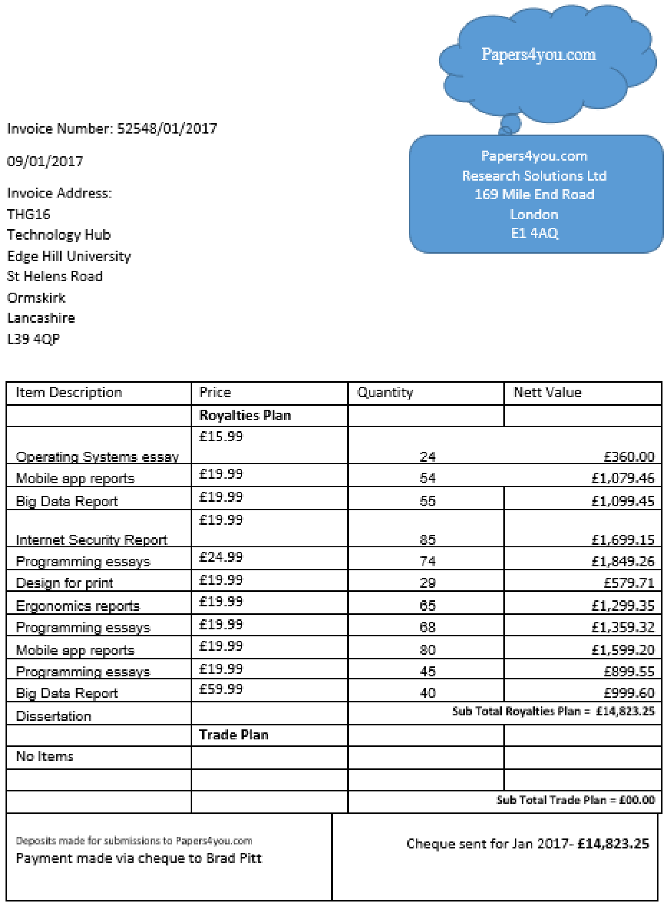
Message file successfully extracted from the Cover file: Invoice_Jan_17.docx

OK

Evidence number 6, named *Pax.bmp* (674 KB), was a slightly larger than expected BMP file.

The name 'Pax' matched an entry on the green notepad (Figure 1), and the same extraction method as previously was used. The password 'pax' (all lowercase) was entered, and the Word document was successfully extracted.

16/04/2025,
4:12 PM



Papers4you.com

Papers4you.com
Research Solutions Ltd
169 Mile End Road
London
E1 4AQ

Invoice Number: 52548/01/2017

09/01/2017

Invoice Address:
THG16
Technology Hub
Edge Hill University
St Helens Road
Ormskirk
Lancashire
L39 4QP

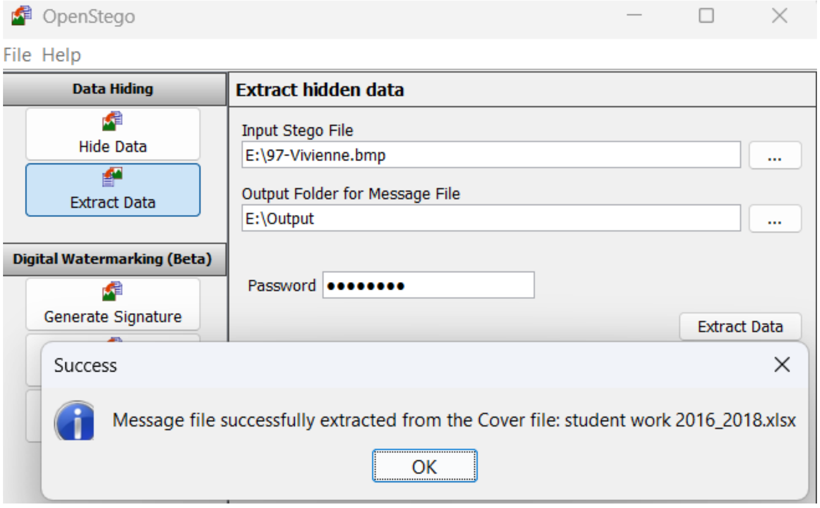
Item Description	Price	Quantity	Nett Value
	Royalties Plan		
Operating Systems essay	£15.99	24	£360.00
Mobile app reports	£19.99	54	£1,079.46
Big Data Report	£19.99	55	£1,099.45
Internet Security Report	£19.99	85	£1,699.15
Programming essays	£24.99	74	£1,849.26
Design for print	£19.99	29	£579.71
Ergonomics reports	£19.99	65	£1,299.35
Programming essays	£19.99	68	£1,359.32
Mobile app reports	£19.99	80	£1,599.20
Programming essays	£19.99	45	£899.55
Big Data Report	£59.99	40	£999.60
Dissertation		Sub Total Royalties Plan = £14,823.25	
	Trade Plan		
No Items			
		Sub Total Trade Plan = £00.00	

Deposits made for submissions to Papers4you.com Payment made via cheque to Brad Pitt	Cheque sent for Jan 2017- **£14,823.25**

This document was extracted from *Pax.bmp* and includes an invoice from Papers4You.com addressed to Edeg Hill University.

The invoice includes a breakdown of assignments sold throughout 2017, with a total payment of £14,823.25 sent to Brad Pitt via cheque.

There is no mention of Susan Canning. Instead, this document further supports that Brad Pitt was consistently paid across multiple years, and these hidden documents were used to conceal any evidence.

<table>
<tr>
<td>16/04/2025,
4:34 PM</td>
<td>


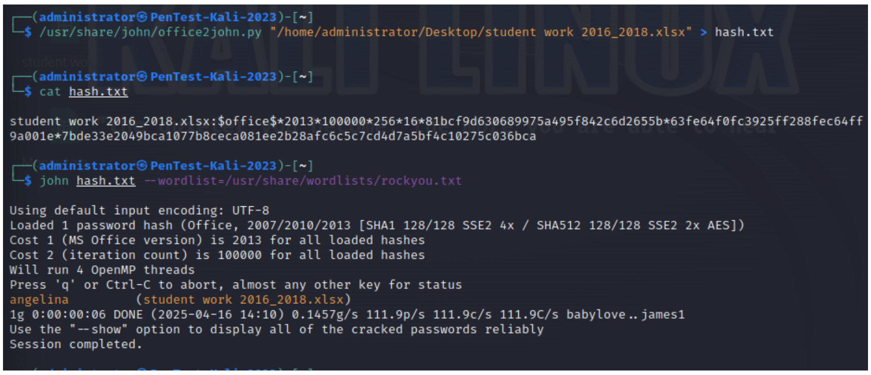
Extract hidden data

Input Stego File: E:\97-Vivienne.bmp

Output Folder for Message File: E:\Output

Password: ••••••••

Success

Message file successfully extracted from the Cover file: student work 2016_2018.xlsx
</td>
<td>
<p>Evidence number 7, named <em>Vivienne.bmp</em> (4,310 KB), was one of the largest files found during autopsy analysis, raising suspicion of embedded content.</p>
<p>The filename matched the name “Vivienne”, which was listed on the green notepad (Figure 1), and previously confirmed to be a working password list.</p>
<p>The password ‘<em>vivienne’</em> (lowercase) was entered, and an Excel document was successfully extracted.</p>
</td>
</tr>
<tr>
<td>16/04/2025,
4:54 PM</td>
<td>

<pre>
┌──(administrator㉿PenTest-Kali-2023)-[~]
└─$ /usr/share/john/office2john.py "/home/administrator/Desktop/student work 2016_2018.xlsx" > hash.txt

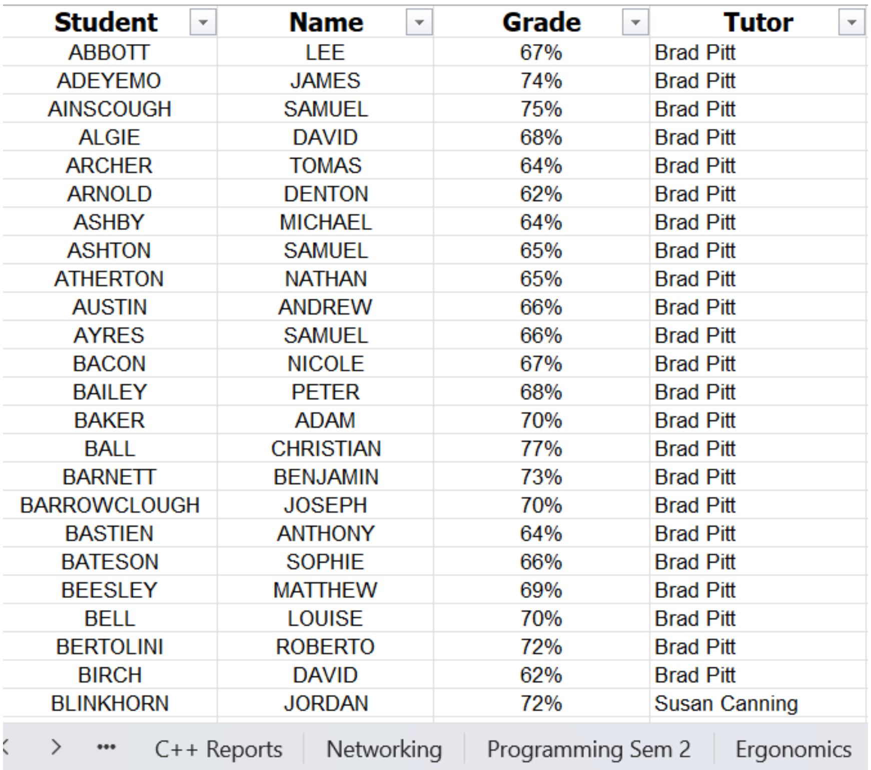
┌──(administrator㉿PenTest-Kali-2023)-[~]
└─$ cat hash.txt

student work 2016_2018.xlsx:$office$*2013*100000*256*16*81bcf9d630689975a495f842c6d2655b*63fe64f0fc3925ff288fec64ff
9a001e*7bde33e2049bca1077b8ceca081ee2b28afc6c5c7cd4d7a5bf4c10275c036bca

┌──(administrator㉿PenTest-Kali-2023)-[~]
└─$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt

Using default input encoding: UTF-8
Loaded 1 password hash (Office, 2007/2010/2013 [SHA1 128/128 SSE2 4x / SHA512 128/128 SSE2 2x AES])
Cost 1 (MS Office version) is 2013 for all loaded hashes
Cost 2 (iteration count) is 100000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
angelina   (student work 2016_2018.xlsx)
1g 0:00:00:06 DONE (2025-04-16 14:10) 0.1457g/s 111.9p/s 111.9c/s 111.9C/s babylove..james1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
</pre>
</td>
<td>
<p>The Excel file student work 2016_2018.xlsx, extracted from Vivienne.bmp, was password protected.</p>
<p>1) To recover access to the file, a hash value of the password is generated using ‘<em>office2john.py’</em> and stored as a text file.</p>
<p>2) The hash was cracked using <em>John the Ripper</em> with the wordlist <em>rockyou.txt.</em></p>
<p>3) The password was successfully recovered as Angelina, which was also a name found on the green notepad (Figure 1) used in previous evidence.</p>
</td>
</tr>
</table>

16/04/2025, 5:04 PM



Student	Name	Grade	Tutor
ABBOTT	LEE	67%	Brad Pitt
ADEYEMO	JAMES	74%	Brad Pitt
AINSCOUGH	SAMUEL	75%	Brad Pitt
ALGIE	DAVID	68%	Brad Pitt
ARCHER	TOMAS	64%	Brad Pitt
ARNOLD	DENTON	62%	Brad Pitt
ASHBY	MICHAEL	64%	Brad Pitt
ASHTON	SAMUEL	65%	Brad Pitt
ATHERTON	NATHAN	65%	Brad Pitt
AUSTIN	ANDREW	66%	Brad Pitt
AYRES	SAMUEL	66%	Brad Pitt
BACON	NICOLE	67%	Brad Pitt
BAILEY	PETER	68%	Brad Pitt
BAKER	ADAM	70%	Brad Pitt
BALL	CHRISTIAN	77%	Brad Pitt
BARNETT	BENJAMIN	73%	Brad Pitt
BARROWCLOUGH	JOSEPH	70%	Brad Pitt
BASTIEN	ANTHONY	64%	Brad Pitt
BATESON	SOPHIE	66%	Brad Pitt
BEESLEY	MATTHEW	69%	Brad Pitt
BELL	LOUISE	70%	Brad Pitt
BERTOLINI	ROBERTO	72%	Brad Pitt
BIRCH	DAVID	62%	Brad Pitt
BLINKHORN	JORDAN	72%	Susan Canning

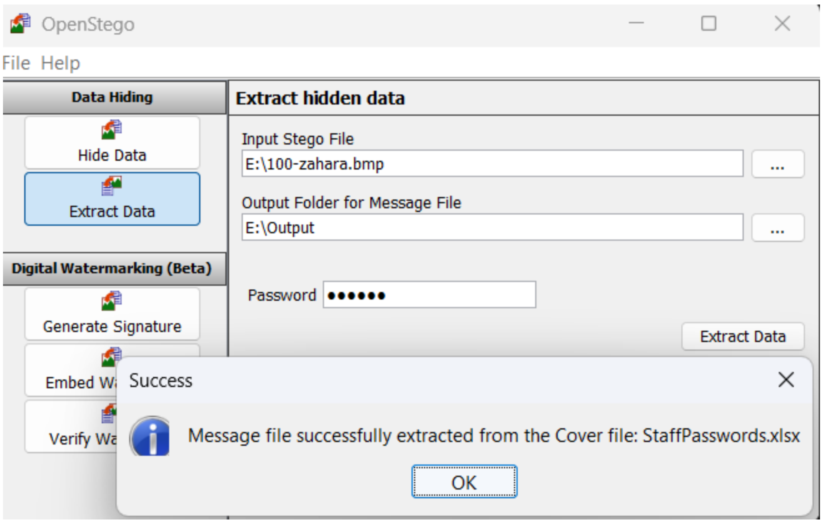
This decrypted hidden spreadsheet contains detailed academic records across 3 years (2016-2018) that were sold via Papers4You.com.

An analysis of the spreadsheet revealed that Brad Pitt's name repeatedly appears as the tutor listed for many assignments. This could indicate that he was fulfilling multiple roles or that he had unauthorised access to staff systems.

The subjects directly align with the assignments being sold across all the previous invoices.

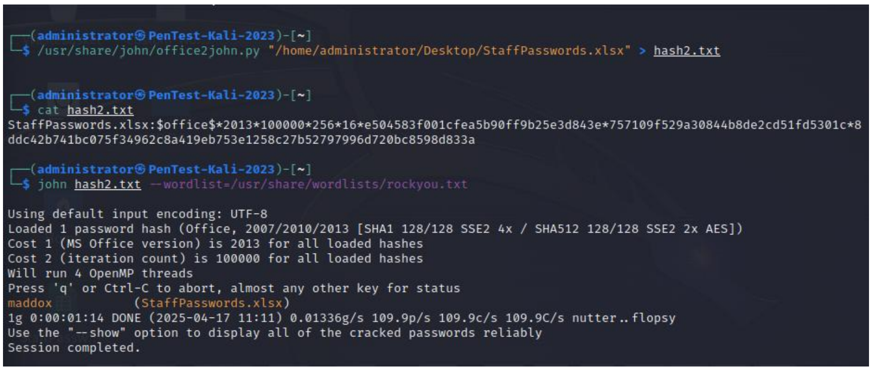
The structure, formatting, and consistency confirm it was not just academic tracking, but used as a log, monitoring and management system used for assignments that were being sold.

This further links back to Brad Pitt, who is consistently listed on the invoices as the payee.

<table>
<tr>
<td>16/04/2025,
5:54 PM</td>
<td>


Input Stego File: E:\100-zahara.bmp
Output Folder for Message File: E:\Output
Password ●●●●●●
Message file successfully extracted from the Cover file: StaffPasswords.xlsx
</td>
<td>Evidence number 8 was a file named <em>zahara.bmp</em> with a relatively large size (2,400 KB).

The name “Zahara” was the final unused entry from the green notepad (Figure 1).

Using OpenStego, the password zahara (all lowercase) was entered, and the embedded file StaffPasswords.xlsx was successfully revealed.</td>
</tr>
<tr>
<td>16/04/2025,
6:12 PM</td>
<td>

<pre>
┌──(administrator㉿PenTest-Kali-2023)-[~]
└─$ /usr/share/john/office2john.py "/home/administrator/Desktop/StaffPasswords.xlsx" > hash2.txt

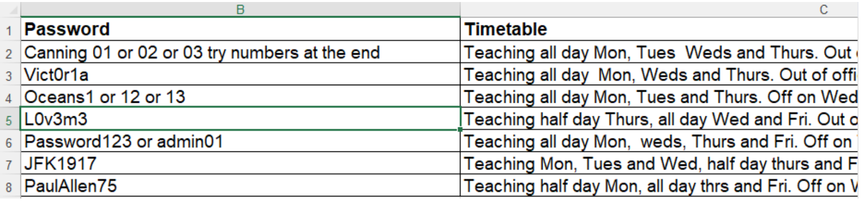
┌──(administrator㉿PenTest-Kali-2023)-[~]
└─$ cat hash2.txt
StaffPasswords.xlsx:$office$*2013*100000*256*16*e504583f001cfea5b90ff9b25e3d843e*757109f529a30844b8de2cd51fd5301c*8
ddc42b741bc075f34962c8a419eb753e1258c27b52797996d720bc8598d833a

┌──(administrator㉿PenTest-Kali-2023)-[~]
└─$ john hash2.txt --wordlist=/usr/share/wordlists/rockyou.txt

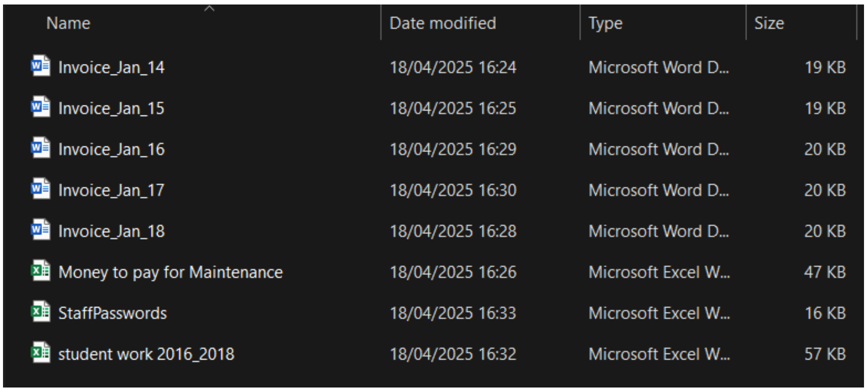
Using default input encoding: UTF-8
Loaded 1 password hash (Office, 2007/2010/2013 [SHA1 128/128 SSE2 4x / SHA512 128/128 SSE2 2x AES])
Cost 1 (MS Office version) is 2013 for all loaded hashes
Cost 2 (iteration count) is 100000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
maddox   (StaffPasswords.xlsx)
1g 0:00:01:14 DONE (2025-04-17 11:11) 0.01336g/s 109.9p/s 109.9c/s 109.9C/s nutter..flopsy
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
</pre>
</td>
<td>The Excel file StaffPasswords.xlsx, extracted from zahara.bmp was found to be encrypted.

1) Using Kali Linux, the password hash was generated using <em>office2john.py</em> and saved as a text file.

2) The file was then cracked using <em>John the Ripper</em> with the <em>rockyou</em> wordlist.

3) The password to the Excel file was ‘maddox’, which was also found on the green notepad (Figure 1).</td>
</tr>
<tr>
<td>16/04/2025,
6:37 PM</td>
<td>

<table>
<tr><th></th><th>B</th><th>C</th></tr>
<tr><td>1</td><td><b>Password</b></td><td><b>Timetable</b></td></tr>
<tr><td>2</td><td>Canning 01 or 02 or 03 try numbers at the end</td><td>Teaching all day Mon, Tues Weds and Thurs. Out</td></tr>
<tr><td>3</td><td>Vict0r1a</td><td>Teaching all day Mon, Weds and Thurs. Out of offi</td></tr>
<tr><td>4</td><td>Oceans1 or 12 or 13</td><td>Teaching all day Mon, Tues and Thurs. Off on Wed</td></tr>
<tr><td>5</td><td>L0v3m3</td><td>Teaching half day Thurs, all day Wed and Fri. Out c</td></tr>
<tr><td>6</td><td>Password123 or admin01</td><td>Teaching all day Mon, weds, Thurs and Fri. Off on</td></tr>
<tr><td>7</td><td>JFK1917</td><td>Teaching Mon, Tues and Wed, half day thurs and F</td></tr>
<tr><td>8</td><td>PaulAllen75</td><td>Teaching half day Mon, all day thrs and Fri. Off on V</td></tr>
</table>
</td>
<td>This StaffPasswords.xlsx Excel file contains a list of login credentials for multiple Edge Hill University staff members.

Notably, Brad Pitt’s name or login credentials does not appear anywhere in</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td></td>
<td>this file. This highly suggests that he was the creator and had no need to record his credentials, reinforcing the idea of him being in control of the data.
The structure of the file indicates that it may have been used to gain unauthorised access to internal university systems for specific staff members. This could explain why Brad Pitt’s name appeared frequently as the “Tutor” across multiple assignments and may have used these credentials to impersonate staff or gain access to coursework submissions.</td>
</tr>
<tr>
<td>18/04/2025, 5:52 PM</td>
<td>
<table>
<tr><th>Name</th><th>Date modified</th><th>Type</th><th>Size</th></tr>
<tr><td>Invoice_Jan_14</td><td>18/04/2025 16:24</td><td>Microsoft Word D...</td><td>19 KB</td></tr>
<tr><td>Invoice_Jan_15</td><td>18/04/2025 16:25</td><td>Microsoft Word D...</td><td>19 KB</td></tr>
<tr><td>Invoice_Jan_16</td><td>18/04/2025 16:29</td><td>Microsoft Word D...</td><td>20 KB</td></tr>
<tr><td>Invoice_Jan_17</td><td>18/04/2025 16:30</td><td>Microsoft Word D...</td><td>20 KB</td></tr>
<tr><td>Invoice_Jan_18</td><td>18/04/2025 16:28</td><td>Microsoft Word D...</td><td>20 KB</td></tr>
<tr><td>Money to pay for Maintenance</td><td>18/04/2025 16:26</td><td>Microsoft Excel W...</td><td>47 KB</td></tr>
<tr><td>StaffPasswords</td><td>18/04/2025 16:33</td><td>Microsoft Excel W...</td><td>16 KB</td></tr>
<tr><td>student work 2016_2018</td><td>18/04/2025 16:32</td><td>Microsoft Excel W...</td><td>57 KB</td></tr>
</table>
</td>
<td>This screenshot presents all the files recovered from bitmap images from the forensic investigation using OpenStego.
The files include:
<b>5 Word documents</b> (Invoices) – Confirming a yearly cheque payment to Brad Pitt.
<b>3 Excel spreadsheets</b>: Containing student sale records, maintenance payments and staff passwords.</td>
</tr>
</table>

1.12 Key Evidence Summary:

- Tools Used:
    - Autopsy (for forensic imaging and analysis)
    - OpenStego (for hidden file extraction)
    - Kali Linux + John the Ripper (for password cracking)
- Data Recovered:
    - 5 Word Invoice Documents
    - 3 Excel Spreadsheets (decrypted)
- Findings:
    - Documents confirm the sale of academic essays via Papers4You.
    - Spreadsheets include student data, password lists, and financial records.
    - All five invoices show payments via cheque to Brad Pitt:
        - 2014: £5,128.50
        - 2015: £2,319.38
        - 2016: £18,253.25
        - 2017: £14,823.25
        - 2018: £42,190.97
    - Total confirmed: £82,715.35 was paid to Brad Pitt. This evidence indicates that Brad Pitt was involved in this misconduct.

1.13 Limitations and Suggested Improvements

The investigation was conducted in a forensic sound manner, but there were a few limitations. Firstly, no forensic image of the USB drive was created, and instead, only a read-only mode was used. While this did preserve the data, it did not provide a full evidential copy. Only a limited number of tools for the investigation were used (Autopsy, OpenStego and John the Ripper), and the password cracking was relied upon using the '*rockyou.txt'* wordlist. In future investigations, using a forensic image and a wider range of tools would improve the evidence and reliability of the investigation.

1.14 Conclusion:

This investigation followed the process of using the ADAM model, the NIST forensic process, and the ACPO principles to successfully examine the suspect's USB drive in a forensically sound, structured, and legal manner. Using forensic tools such as Autopsy, OpenStego, and John the Ripper, critical evidence was revealed to support the misconduct of academic work being sold.

Out of all the files examined from the 'Private Files', a group of eight bitmap (.bmp) images were found hidden files using steganography. The files that were hidden included five Word invoices and three encrypted Excel spreadsheets. Using password clues found from the green notepad (Figure 1) image from the Investigation Scenario, ‘Photograph 11’, each bitmap image was successfully extracted and decrypted. The extracted files revealed significant insights into the sales of the academic work, with Word documents providing yearly invoices and cheques being cashed out to Brad Pitt, while the Excel files provided logs of student work, maintenance payments and staff credentials. All of this suggested that Brad was the leader of the operation.

In contrast, there were several JPEGS and a WEBP file that was also tested using the same password list and methodology, which was analysed due to their inclusion within the hidden ‘Private Files’ folder and tested using OpenStego. However, none of these files revealed any hidden content or matched any of the known passwords, and the file sizes that were between 5 and 10KB didn’t suggest any suspicion of steganographic embedding. Therefore, while they were examined to ensure integrity, they were excluded from the final evidence list because of their lack of value.

All the evidence that was collected showed clear documentation with screenshots, timestamps, cracked passwords and extracted contents. There were no references or links that was found to Susan Canning in any of the recovered documents. Instead, the consistent appearance of Brad Pitt’s name as the recipient of the invoices and potential impersonator of tutors indicates that he is the primary suspect in this investigation.

The digital trail that was revealed by this investigation shows a strong case of Brad Pitt using steganography, encryption, and stolen credentials to sell academic work for his financial gain over a period of several years.

2. Section 2 – Ethical and Legal Issues within Digital Forensic Investigations

Based on the evidence that was gathered from the forensic analysis, which included invoices, student records and staff credentials, it is clear that Brad Pitt was guilty of the unauthorised sale of academic work and potentially misused the university's systems. These findings not only demonstrate the misuse of the computer systems but also raise serious concerns about the legal and ethical implications.

The following section evaluates the legal and ethical responsibilities related to the investigation, ensuring that the process and outcome both align with UK law and forensic standards.

2.1 Introduction:

This section explores the ethical and legal responsibilities of a digital forensic analyst, particularly in the context of the investigation in Section 1. The investigation involved the potentially criminal activity of the unauthorised sale of academic work, the hidden data using steganography, and the potential misuse of staff credentials. In order to ensure that the findings of this investigation were legally and ethically correct, it was essential to follow relevant UK laws, digital forensics standards and ethical morals.

2.2 Legal Frameworks Relevant to Digital Forensics:

In the UK, following the proper legal frameworks for digital forensic investigations ensures the protection of integrity, privacy and admissibility of digital evidence in court.

2.2.1 Computer Misuse Act 1990

The Computer Misuse Act provides laws for unauthorised access to computer systems, data modification, and actions that could damage the operation of computers. In this investigation, the *StaffPasswords.xlsx* file revealed the login credentials for multiple staff members. If Brad Pitt used these passwords to access confidential systems or impersonate tutors, this would violate the Act under sections related to unauthorised access (Sections 1 and 2), which could result in 12 months imprisonment or a fine or both or up to two years in prision on indictment (The Crown Prosecution Service, 2020).

2.2.2 Data Protection Act 2018 / UK GDPR

The Excel spreadsheet *student work 2016_2018.xlsx* contained personal details such as names, grades and tutors, which would violate the personal data laws under the UK GDPR. Processing, storing, or disclosing this personal data without the consent of the students breaches the Data Protection Act. It could lead to disciplinary sanctions and ICO involvement with the university having a maximum fine of £17.5 million or 4% annual turnover (UK Government, 2018). During the forensic investigation, care was taken only to access the relevant data, and it was secured appropriately.

2.2.3 Copyright, Design and Patents Act 1988

Within the investigation, invoices show Brad Pitt receiving payment for reusing and selling academic work. Since submitted assignments are classed as intellectual property, reusing them without consent could amount to being liable for the act of copyright infringement, which has a maximum fine of £5,000 or six months imprisonment (Government of UK, 1988).

2.3 Ethical Responsibilities of the Forensic Analyst

2.3.1 Integrity and Impartiality

A forensic analyst must approach every case with an unbiased approach, avoiding any external pressures or opinions (Edinbox Team, 2024). The investigation ensured that all possibilities were explored before reaching any conclusions, and although the original suspicion was placed upon Susan Canning, the evidence clearly pointed towards Brad Pitt.

2.3.2 Confidentiality

All the data recovered, especially the personal information from spreadsheets, was treated as confidential due to its sensitivity. The findings should only be shared with the authorised individuals, such as the investigator, the university or a legal representative (Conference of International Investigators, 2021).

2.3.3 Competence and Professionalism

The forensic analyst must have the ability to demonstrate sufficient technical competencies and knowledge using only validated forensic tools (Horsman and Dodd, 2024). This investigation used well-known and established tools like Autopsy, OpenStego, and John the Ripper. Furthermore, the documentation of all the forensic investigation steps, notes, and screenshots also shows adherence to professional standards and allows for repeatability.

2.3.4 Avoiding Unnecessary Intrusion

Only the data that is strictly relevant to the investigation will be extracted and examined to respect the privacy of the individuals who are involved (College of Policing, 2020). While other files were reviewed for the investigation (JPEG and WEBP images), they were later dismissed from the investigation due to not being forensically valuable, which was in line with the ethical standards.

2.4 Organisational and Criminal Investigations

The investigation was a blend of characteristics from both the organisation and criminal contexts:

From the criminal perspective, Brad Pitt’s actions violate several UK laws, including the Computer Misuse Act, Data Protection Act and Copyright, Designs and Patent Act. These violations may result in criminal prosecution, especially if unauthorised access or personal data misuse violations are confirmed.

From the organisation's perspective, this incident raises significant concerns within Edge Hill University. This includes:

Academic misconduct – the sale of academic work violates the university's integrity, plagiarism and assessment fairness.

Staff misuse of resources – If Brad Pitt impersonated another staff member with their login details, it would breach the university's code of conduct.

Data protection violations – storing student work, personal details, and staff credentials without authorisation violates the internal data protection polices.

Reputational Damage – any leak or disclosure of academic work fraud may harm the university’s reputation and public image, affecting the students and staff.

In this case, the digital forensics evidence may be used to give an internal disciplinary action and a formal legal investigation. The forensic analyst must ensure that the evidence is presented appropriately for internal and external sources.

2.5 Conclusion:

Ethical and legal considerations are incredibly fundamental to any digital forensic investigation to ensure that the evidence is admissible, the individual's rights are respected, and the investigation is credible. In this case, the investigation was conducted in a professional, lawful and unbiased manner, allowing the evidence to be admissible in both the organisational and legal contexts.

This case has highlighted the importance of following legal compliance. Frameworks such as the ACPO Good Practice Guide, the Computer Misuse Act and GDPR are used to uphold the integrity and privacy of all the individuals involved. Additionally, the investigation upheld the ethical responsibility by avoiding biased conclusions and maintaining professional standards throughout every stage of the investigation. The approach taken not only preserved the integrity of the digital evidence but also ensured that both the investigation conclusions were defensible across the university's disciplinary and legal domains.

The role of the digital forensic analyst is not only to deliver technically accurate findings but also to follow ethical and legal considerations to ensure the credibility of the report and that the evidence is accurate, ensuring that the final report is reliable and ethically sound.

References:

ACPO (2012) *ACPO Good Practice Guide for Digital Evidence*. [online] Available at: *https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf* [Accessed 28 Apr. 2025].

Adams, R., Hobbs, V. and Mann, G. (2013) 'The Advanced Data Acquisition Model (Adam): A Process Model for Digital Forensic Practice', *Journal of Digital Forensics, Security and Law*, 8(4). doi: *https://doi.org/10.15394/jdfsl.2013.1154*.

Autopsy (2023) *Autopsy | Digital Forensics*. [online] Available at: *https://www.autopsy.com/* [Accessed 28 Apr. 2025].

College of Policing (2020) *Authorised Professional Practice: The extraction of digital data from personal devices*. [online] Available at: *https://assets.college.police.uk/s3fs-public/2020-12/APP-extraction-data-from-personal-devices.pdf* [Accessed 21 Apr. 2025].

Conference of International Investigators (2021) *Conference of International Investigators (CII 2021) General Principles for Digital Evidence PREAMBLE*. [online] Available at: *https://www.ciinvestigators.org/wp-content/uploads/2021/11/CII-General-Principles-for-Digital-Evidence-21stCII.pdf* [Accessed 21 Apr. 2025].

Cybervie (2021) *Introduction To Autopsy | An Open-Source Digital Forensics Tool*. [online] Available at: *https://cybervie.com/blog/introduction-to-autopsy-an-open-source-digital-forensics-tool/* [Accessed 15 Apr. 2025].

Dr Muhammad Usman (2024) *Week 2 Lecture - What is Computer Misuse*. [online] Blackboard. Available at: *https://learningedge.edgehill.ac.uk/ultra/courses/_318897_1/outline/file/_5864901_1* [Accessed 19 Apr. 2025].

Edinbox Team (2024) *Ethics In Forensics*. [online] Available at: *https://edinbox.com/council/forensic-sciences-gfsec/2494-ethics-in-forensics* [Accessed 21 Apr. 2025].

Government of UK (1988) *Copyright, Designs and Patents Act 1988*. [online] Available at: *https://www.legislation.gov.uk/ukpga/1988/48* [Accessed 21 Apr. 2025].

Horsman, G. and Dodd, A. (2024) 'Competence in digital forensics', *Forensic Science International: Digital Investigation*, 51, p.301840. doi: *https://doi.org/10.1016/j.fsidi.2024.301840*.

Tai, J. (2022) 'Defeating Anti-forensics Techniques', [online] Available at: *https://johntai.net/posts/chfi-notes/module-05/* [Accessed 17 Apr. 2025].

The Crown Prosecution Service (2020) *Computer Misuse Act*. [online] Available at: *https://www.cps.gov.uk/legal-guidance/computer-misuse-act* [Accessed 21 Apr. 2025].

The Edge Hill University Digital Forensic Team (EHUDFT) (2025) *CW2 Investigation Scenario*. [online] Blackboard. Available at: *https://learningedge.edgehill.ac.uk/ultra/courses/_318897_1/outline* [Accessed 15 Apr. 2025].

The ITM Team and Weston, J. (2024) *Steganography | Anti-Forensics*. [online] Insider Threat MatrixTM. Available at: *https://www.insiderthreatmatrix.org/articles/AR5/sections/AF008* [Accessed 17 Apr. 2025].

UK Government (2018) *Data Protection Act*. [online] Available at: *https://www.gov.uk/data-protection* [Accessed 21 Apr. 2025].

Vaidya, S. (2021) *OpenStego*. [online] Available at: *https://www.openstego.com/* [Accessed 28 Apr. 2025].

Wikipedia (2021) *John the Ripper*. [online] Available at: *https://en.wikipedia.org/wiki/John_the_Ripper* [Accessed 28 Apr. 2025].