

**CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING (C-DAC), THIRUVANANTHAPURAM,  
KERALA**

**A PROJECT REPORT ON  
“M57.biz Incident Response & Forensics using Autopsy”**

**SUBMITTED TOWARDS THE**



**PG-DCSF August 2025**

**BY**

**Group Number - 06**

**Shreyas Prakash Math  
Chandan Vikas Shimpi  
Prachi Chandrakant Sabade  
Shravani Kawale  
Utkarsh Krishnarao Pote**

**PRN: 250860940037  
PRN: 250860940008  
PRN: 250860940022  
PRN: 250860940035  
PRN: 250860940046**

**Under The Guidance Of**

**Mr. Jayaram P.  
Centre Co-ordinator**

**Dr. Priya P. Sajan  
Project Guide**

<b>Table of Contents</b>	<b>Page No.</b>
<b>1 Abstract</b>	<b>3</b>
<b>2 Introduction</b>	<b>4</b>
<b>3 Workflow</b>	<b>5</b>
<b>3.1 Viewing the results</b>	<b>8</b>
<b>4 Tools Explanation</b>	<b>19</b>
<b>5 Features Explanation</b>	<b>21</b>
<b>6 Conclusion</b>	<b>23</b>
<b>7 References</b>	<b>24</b>

## **1. Abstract**

Digital forensics and incident response play a critical role in identifying, analysing, and mitigating cyber security incidents within an organization. This project focuses on conducting a structured forensic investigation of a simulated corporate security breach using industry relevant tools and methodologies. The objective of the study is to examine compromised digital evidence, reconstruct the sequence of malicious activities, and identify the root cause of the incident.

The investigation process begins with evidence acquisition from affected systems while maintaining forensic integrity. Disk images and system artifacts are analysed to detect indicators of compromise such as unauthorized access, suspicious file activity, data exfiltration attempts, and traces of malicious execution. Log correlation and timeline reconstruction are performed to understand attacker behaviour and map the progression of the breach. Advanced forensic techniques are applied to recover deleted files, examine user actions, and analyse system and network artifacts. The study emphasizes maintaining chain of custody, proper documentation, and adherence to legal and procedural standards throughout the investigation.

Findings from the analysis provide insights into how the breach occurred, what vulnerabilities were exploited, and what data assets were impacted. The project also highlights preventive and corrective security measures that organizations can implement to strengthen their defence posture. Overall, this work demonstrates the practical application of digital forensics and incident response in real world enterprise environments and reinforces the importance of proactive monitoring, evidence preservation, and rapid investigative capabilities in modern cyber security operations.

## **2. Introduction**

In today's digital environment, organizations face increasing risks of cyber incidents such as unauthorized access and data breaches. Digital forensics and incident response help investigators identify the cause of such incidents, analyse digital evidence, and reconstruct the sequence of events while maintaining evidence integrity.

This project focuses on a forensic investigation conducted in a simulated corporate setup to understand how hidden and visible digital artifacts can be identified and analysed. The study emphasizes evidence collection, concealed data discovery, and integrity validation.

Tools used during the investigation include Autopsy for forensic acquisition and disk analysis, Invisible Secrets for extracting hidden data from image files, and HxD for examining hexadecimal level information. Evidence authenticity was verified using SHA 256 Hashing to ensure data integrity throughout the forensic process.

## **Project Objectives**

The main things we want to achieve with this project are:

- To perform forensic acquisition and analysis of digital evidence using Autopsy.
- To identify and extract hidden data from image files using Invisible Secrets.
- To analyze files at hexadecimal level using HxD.
- To verify evidence integrity using SHA 256 Hashing.
- To detect signs of data concealment and manipulation.
- To reconstruct activities related to the security incident.
- To document forensic findings in a structured manner.
- To understand practical application of digital forensic techniques.

### **3. Workflow**

The Workflow of the Incident Response & Forensics using Autopsy: A Step-by-Step Breakdown

#### **Step 1 - Preparation**

The investigation started with setting up proper forensic procedures to make sure that every piece of evidence would remain legally valid and trustworthy. Chain of custody was established from the beginning so that the handling of evidence could be tracked at every stage. Original storage devices were secured and isolated to avoid any accidental modification. The scope of the investigation was defined, and a controlled forensic workspace was prepared where analysis could be carried out safely without affecting the source data.

#### **Step 2 - Imaging**

After preparation, forensic images of all evidence sources were created. This was done using bit stream imaging, which captures an exact copy of the storage media at the sector level. This approach ensures that deleted files, hidden fragments, and residual data are preserved. Once imaging was completed, the original devices were no longer used for analysis and were kept secure. All further examination was conducted only on verified image copies to maintain evidence integrity.

#### **Step 3 - Ingestion**

The forensic images were then processed inside Autopsy using its ingest processing features. During this stage, the software performed deep automated analysis of the data. It indexed keywords, examined file system structures, extracted metadata, and recovered artifacts from deleted and unallocated space. This process took several hours to complete, but it produced a structured dataset that made detailed investigation possible.

## **Step 4 - Triage**

Once processing was finished, an initial review of the evidence was conducted. The investigation involved five separate data sources totaling close to 20GB. At this stage, the focus shifted toward identifying high risk areas such as user communications, personal folders, and email repositories. By narrowing down the data, investigators were able to prioritize suspicious activity and reduce unnecessary analysis time.

Evidence Identifier	Source Description	Size	Type
M57-CB-WRK	Charlie Brown Workstation Image	~10GB	Hard Drive
M57-CB-USB	Charlie Brown Work USB Drive	~2GB	Portable Media
M57-JF-FAV	Joe Favorites/User Data	~4GB	Hard Drive
M57-EXT-IMG	Secondary Internal Workstation Image	~1GB	Hard Drive
M57-EML-CRP	94-Message Email Corpus	~3GB	Mail Repository
<b>Total Evidence</b>		<b>~20GB</b>	

## **Step 5: Attribution**

Communication analysis played a major role in identifying the primary suspect. Email records revealed that Charlie Brown was involved in suspicious exchanges with two external individuals, Jamie and Andy. The conversations indicated financial demands, sharing of confidential research, and repeated instructions to delete messages. These behavioral indicators helped establish intent and confirmed that the activity was deliberate rather than accidental.

## **Step 6: Decryption**

Further investigation uncovered encrypted archives linked to the suspect's communications. Investigators discovered that passwords had been hidden inside image files referenced in emails. By examining the raw file data at a hexadecimal level, hidden plaintext strings were identified within the image structure. These strings revealed archive passwords that were not visible through normal viewing methods. Using the recovered credentials, investigators unlocked protected files that contained stolen patent documents.

## **Step 7: Steganalysis**

As the investigation progressed, more advanced concealment methods were discovered. Evidence showed that sensitive files had been hidden inside images using steganography software. To confirm this, cryptographic hash values were compared using SHA 256, which proved that certain images had been modified. With the help of steganographic extraction tools and recovered passwords, hidden reports were successfully retrieved, confirming the covert transfer of proprietary information.

## 3.1 Results

Fig. 3.1 checking for evidences

Source Name	S	C	O	E-Mail From	E-Mail To	Subject
Inbox				charlie@m57.biz;	pat@m57.biz;	Re: WELCOME TO THE COMPANY
Inbox				pat@m57.biz;	charlie@m57.biz; jo@m57.biz; terry@m57.biz;	WELCOME TO THE COMPANY
Inbox				charlie@m57.biz;	alixpery@yahoo.com; rubinfritz31@mail.com;	New email address
Inbox				charlie@m57.biz;	charlie@m57.biz; jo@m57.biz; terry@m57.biz;	Lunch
Inbox				charlie@m57.biz;	charlie@m57.biz;	Re: Lunch
Inbox				charlie@m57.biz;	alixpery@yahoo.com;	Re: New email address
Inbox				charlie@m57.biz;	pat@m57.biz;	What's wrong with Pat
Inbox				charlie@m57.biz;	charlie@m57.biz;	Lunch
Inbox				charlie@m57.biz;	pat@m57.biz;	Re: COFFEE
Inbox				charlie@m57.biz;	pat@m57.biz;	Re: Google
Inbox				charlie@m57.biz;	terry@m57.biz; charlie@m57.biz; jo@m57.biz;	Great Job Folks!
Inbox				charlie@m57.biz;	alixpery@yahoo.com;	Movie tonight???
Inbox				rubinfritz31@mail.com;	charlie@m57.biz;	Re: New email address

Fig. 3.2 Found suspicious email

From: charlie@m57.biz  
To: andy@swexpert.com;  
CC:  
Subject: I Found Something

Headers: Text [HTML] [RTF] Attachments (1) Accounts

Original Text

Andy,

Lucky for me, I just happened to stumble across this. I found a prior patent that will definitely invalidate your current immortality patent. You should have used my boss's prior art services, but, oh well, I'll just use your negligence to benefit me. I want 100k or I'll release the publicly. I don't need to tell you how much this will hurt your business if I go public with this. Don't involve the cops or this email will go public. See the attachment for details on what I found. I'll be in touch with my bank act number. The password for the zip file will be hidden in the next picture I send you.

Fig. 3.3 Found suspicious email Attachment

The screenshot shows the Autopsy 4.2.2 interface with the following details:

- Case View:** M57.biz - Autopsy 4.2.2.1
- File Types:** Includes File Types, Deleted Files, and MB File Size.
- Data Artifacts:** Includes Communication Accounts (27), E-Mail Messages (94), Default ([Default]), and Default (94).
- Analysis Results:** Includes Encryption Detected (23), Encryption Suspected (5), EXIF Metadata (367), Extension Mismatch Detected (181), Keyword Hits (14324), User Content Suspected (367), Web Categories (9), OS Accounts, and Tags.
- Table View:** Shows a table of results with columns: Source Name, S, C, O, E-Mail From, E-Mail To, Subject, and a status icon (red exclamation mark). One row is highlighted with a red border.
- Message Preview:** Displays the following email details:
  - From: charlie@m57.biz
  - To: andy@swexpert.com;
  - CC:
  - Subject: I Found Something
  - Date: 2009-12-04 23:11:47 IST
- Message Content:** Headers, Text, HTML, RTF, Attachments (1), and Accounts.
- File Details:** Shows a table of file artifacts with columns: Location, Size, Mime type, and Known. One file is listed: /img\_charlie-2009-12-11.E01/vol\_v02/Documents: 108438 application/zip unknown.

Fig. 3.4 Suspicious founding no 2

The screenshot shows the Autopsy 4.2.2 interface with the following details:

- Case View:** M57.biz - Autopsy 4.2.2.1
- File Types:** Includes File Types, Deleted Files, and MB File Size.
- Data Artifacts:** Includes Communication Accounts (27), E-Mail Messages (94), Default ([Default]), and Default (94).
- Analysis Results:** Includes Encryption Detected (23), Encryption Suspected (5), EXIF Metadata (367), Extension Mismatch Detected (181), Keyword Hits (14324), User Content Suspected (367), Web Categories (9), OS Accounts, and Tags.
- Table View:** Shows a table of results with columns: Source Name, S, C, O, E-Mail From, E-Mail To, Subject, and a status icon (blue checkmark). One row is highlighted with a blue border.
- Message Preview:** Displays the following email details:
  - From: charlie@m57.biz
  - To: andy@swexpert.com;
  - CC:
  - Subject: Picture
  - Date: 2009-12-08 01:14:18 IST
- Message Content:** Headers, Text, HTML, RTF, Attachments (1), and Accounts.
- Text Preview:** Shows the message body: "Andy, Here's the picture I promised... Make sure you delete this." and "C".

Fig. 3.5 Found another Suspicious email

The screenshot shows the Autopsy 4.22.1 interface with the following details:

- Case Path:** jo-work-usb-2009-12-11.E01\_122235 Host
- Analysis Results:**
  - Encryption Detected (23)
  - Encryption Suspected (5)
  - EXIF Metadata (367)
  - Extension Mismatch Detected (181)
  - Keyword Hits (4324)
  - User Content Suspected (367)
  - Web Categories (9)
  - OS Accounts
  - Tags
  - Bookmarks (1)
  - Evidence (Notable) (2)
  - Follow Up (2)
  - Score
- Table View:** Shows a list of emails with columns for Source Name, S, C, O, E-Mail From, E-Mail To, and Subject.
- Selected Email:** Charlie 2009-12-02\_1305.Received\_Interested-email (highlighted in blue)
- Email Headers:**
  - From: charlie@m57.biz
  - To: jaime@project2400.com;
  - CC:
  - Subject: Interested?
- Email Body:**

```
<div class="moz-text-flowed" style="font-family: -moz-fixed">I have something that you'll definitely be interested in. It concerns your competitor. I'm doing a prior art search for them. Want to know what I've found? You know my price. I'll send you the goods after I see half in my account. Make sure you delete this email.
```

Fig. 3.6

The screenshot shows the Autopsy 4.22.1 interface with the following details:

- Case Path:** jo-work-usb-2009-12-11.E01\_122235 Host
- Analysis Results:** Same as Fig. 3.5
- Table View:** Shows a list of emails with columns for Source Name, S, C, O, E-Mail From, E-Mail To, and Subject.
- Selected Email:** Charlie 2009-12-04\_014652\_email (highlighted in blue)
- Email Headers:**
  - From: charlie@m57.biz
  - To: jaime@project2400.com;
  - CC:
  - Subject:
- Email Body:**

```
J.  
Nice working with you. Here's the file. Instructions for opening to follow when I see another deposit in my acct.
```

Fig. 3.7 Checking for Steganography

Source Name	S	C	O	E-Mail From	E-Mail To	Subject
Inbox				terry@m57.biz; charlie@m57.biz;	jo@m57.biz; charlie@m57.biz;	Re: COFFEE
Sent				charlie@m57.biz;	jamie@project2400.com; pat@m57.biz; jo@m57.biz; charlie@m57.biz;	Re: COFFEE
Inbox				in@m57.biz;	charlie@m57.biz;	Re: What's wrong with Pat

Fig. 3.8

Source Name	S	C	O	E-Mail From	E-Mail To	Subject
Sent				charlie@m57.biz; pat@m57.biz;	andy@swexpert.com; charlie@m57.biz; terry@m57.biz; jo@m57.biz;	I Found Something
Sent				charlie@m57.biz;	jamie@project2400.com;	Lunch
Inbox				terry@m57.biz;	charlie@m57.biz; terry@m57.biz; jo@m57.biz;	Instructions

Fig. 3.9 Steganographic images findings

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
01.zip		1	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	108438	Allocated	Allocated	unknown	/img_ch
astronaut1.jpg		0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	722717	Allocated	Allocated	unknown	/img_ch
microscope1.jpg		0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	136274	Allocated	Allocated	unknown	/img_ch

Fig. 3.10 Checking Metadata

File	File Path	Comment	Modified Time	Changed Time
astronaut1.jpg	/img_charlie-2009-12-11.E01/vol_vol2/Documents and ..		0000-00-00 00:00:00	0000-00-00 00:00:00
microscope1.jpg	/img_charlie-2009-12-11.E01/vol_vol2/Documents and ..		0000-00-00 00:00:00	0000-00-00 00:00:00
astronaut.jpg	/img_charlie-2009-12-11.E01/vol_vol2/Documents and ..		2009-11-25 03:03:33 IST	2009-11-25 03:11:55 IST
microscope.jpg	/img_charlie-2009-12-11.E01/vol_vol2/Documents and ..		2009-11-25 02:57:51 IST	2009-11-25 03:34:53 IST

### Metadata

Name:	/img_charlie-2009-12-11.E01/vol_vol2/Documents and Settings/Charlie/My Documents/astronaut.jpg
Type:	File System
MIME Type:	image/jpeg
Size:	713418
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2009-11-25 03:03:33 IST
Accessed:	2009-12-11 03:48:36 IST
Created:	2009-11-25 03:10:28 IST
Changed:	2009-11-25 03:11:55 IST
MD5:	40b386b30ed026c60ec1ac72e87360a3
SHA-256:	19e8f6a5803126f5c650bf1ded34aed9d8475a96c9f82e3f559aa72e2ca8b00a
Hash Lookup Results:	UNKNOWN
Internal ID:	10000

### From The Sleuth Kit istat Tool:

```

MFT Entry Header Values:
Entry: 13364 Sequence: 17
LogFile Sequence Number: 1075627962
Allocated File
Links: 2

```

Fig. 3.11 Checking Metadata

The screenshot shows the 'Listing' tab selected in the top navigation bar. Below it, the 'Bookmark File Tags' section has 'Table' selected. The main area displays a table of file metadata:

File	File Path	Comment	Modified Time	Changed Time	Accessed Time	Created Time
astronaut1.jpg	/img_charlie-2009-12-11.E01/vol_vo1/Documents and ..		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
microscope1.jpg	/img_charlie-2009-12-11.E01/vol_vo1/Documents and ..		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
astronaut.jpg	/img_charlie-2009-12-11.E01/vol_vo1/Documents and ..		2009-11-25 03:03:33 IST	2009-11-25 03:11:55 IST	2009-12-11 03:48:36 IST	2009-11-25 03:10:28
microscope.jpg	/img_charlie-2009-12-11.E01/vol_vo1/Documents and ..		2009-11-25 02:57:51 IST	2009-11-25 03:34:53 IST	2009-12-11 03:48:35 IST	2009-11-25 03:10:30

Below the table, there are tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences. The 'Metadata' tab is selected.

**Metadata**

```

Name: /img_charlie-2009-12-11.E01/vol_vo1/Documents and Settings/Charlie/Application Data/Thunderbird/Profiles/4zy34x9h.default/Mail/Local Folders/Sent/astronaut1.jpg
Type: Derived
MIME Type: image/jpeg
Size: 722717
File Name Allocation: Allocated
Metadata Allocation: Allocated
Modified: 0000-00-00 00:00:00
Accessed: 0000-00-00 00:00:00
Created: 0000-00-00 00:00:00
Changed: 0000-00-00 00:00:00
MD5: 45eade24b3a89b21fed303310ccbd54
SHA-256: f57e2e43101088191f9929e1be088baeaeb3ae4df18200701f4f814d6b551b32
Hash Lookup Results: UNKNOWN
Internal ID: 131946
  
```

Fig. 3.12 Comparing Hash values

This screenshot shows two side-by-side sessions of the 'Listing' tab in iStatool. Both sessions have 'Bookmark File Tags' set to 'Table'. The left session shows the same four files as Fig. 3.11. The right session shows identical files with slightly different modification times. Both sessions have the 'Metadata' tab selected.

**Session 1 (Left):**

File	File Path	Comment	Modified
astronaut1.jpg	/img_charlie-2009-12-11.E01/vol_vo1/Documents and ..		0000-00-00 00:00:00
microscope1.jpg	/img_charlie-2009-12-11.E01/vol_vo1/Documents and ..		0000-00-00 00:00:00
astronaut.jpg	/img_charlie-2009-12-11.E01/vol_vo1/Documents and ..		2009-11-25 03:03:33 IST
microscope.jpg	/img_charlie-2009-12-11.E01/vol_vo1/Documents and ..		2009-11-25 02:57:51 IST

**Session 2 (Right):**

File	File Path	Comment	Modified
astronaut1.jpg	/img_charlie-2009-12-11.E01/vol_vo1/Documents and ..		0000-00-00 00:00:00
microscope1.jpg	/img_charlie-2009-12-11.E01/vol_vo1/Documents and ..		0000-00-00 00:00:00
astronaut.jpg	/img_charlie-2009-12-11.E01/vol_vo1/Documents and ..		2009-11-25 03:11:55 IST
microscope.jpg	/img_charlie-2009-12-11.E01/vol_vo1/Documents and ..		2009-11-25 03:34:53 IST

Both sessions show the same metadata for each file, including name, type, MIME type, size, file name allocation, metadata allocation, and hash values.

Fig. 3.13 Suspicious finding

The screenshot shows the Autopsy 4.2.1 interface with a 'Listing' view. The left sidebar shows various data sources, file types, and system information. The main area displays a table of artifacts. One artifact, 'insec2.exe', is highlighted in yellow and has a tooltip 'No comments found'. The table includes the following columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), and Flag. The 'insec2.exe' entry has the following details:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flag
insec2.exe	0	0	0	2009-11-20 00:12:25 IST	2009-12-11 03:57:41 IST	2009-11-25 03:39:36 IST	2009-11-20 23:13:04 IST	1291720	Allocated	All

Fig. 3.14 InvisibleSecrets4 Tool installation

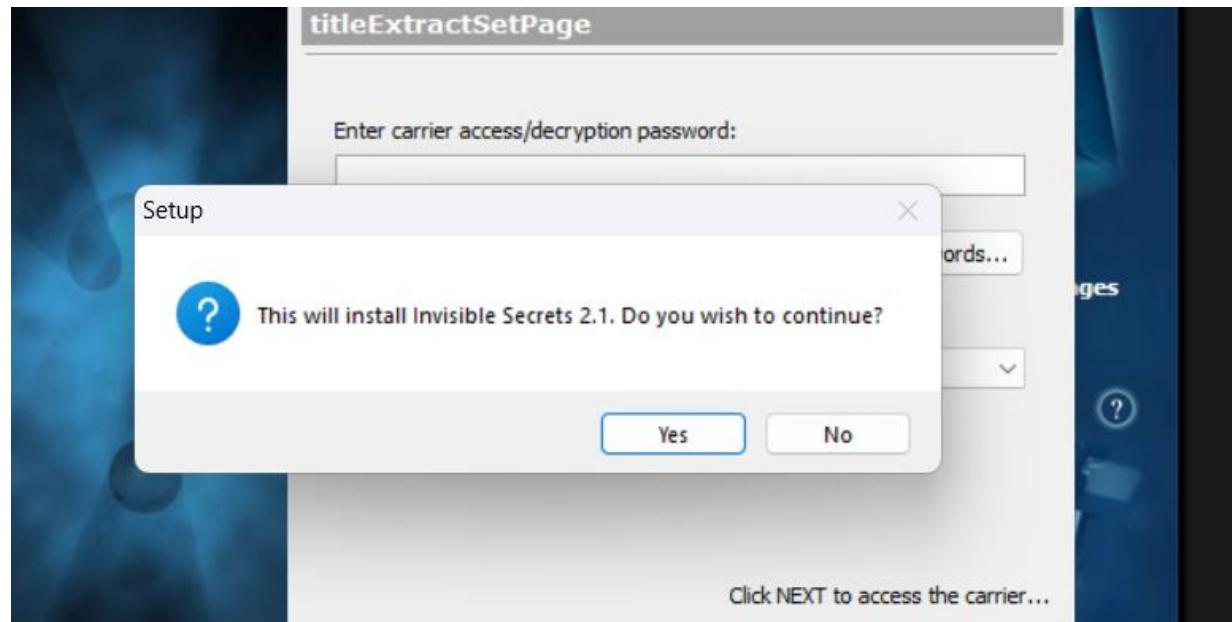


Fig. 3.15 Uploading Steganographic images



Fig. 3.16 Giving password found in suspicious email

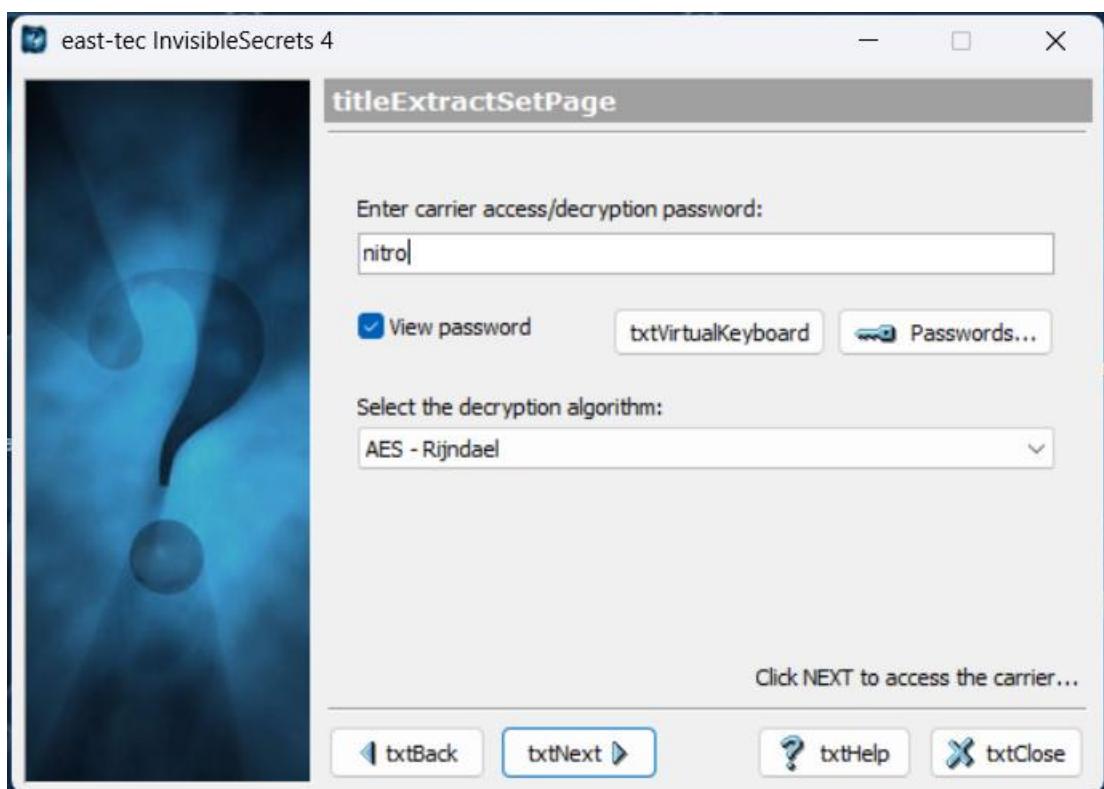


Fig. 3.17 Found Hidden Attachment

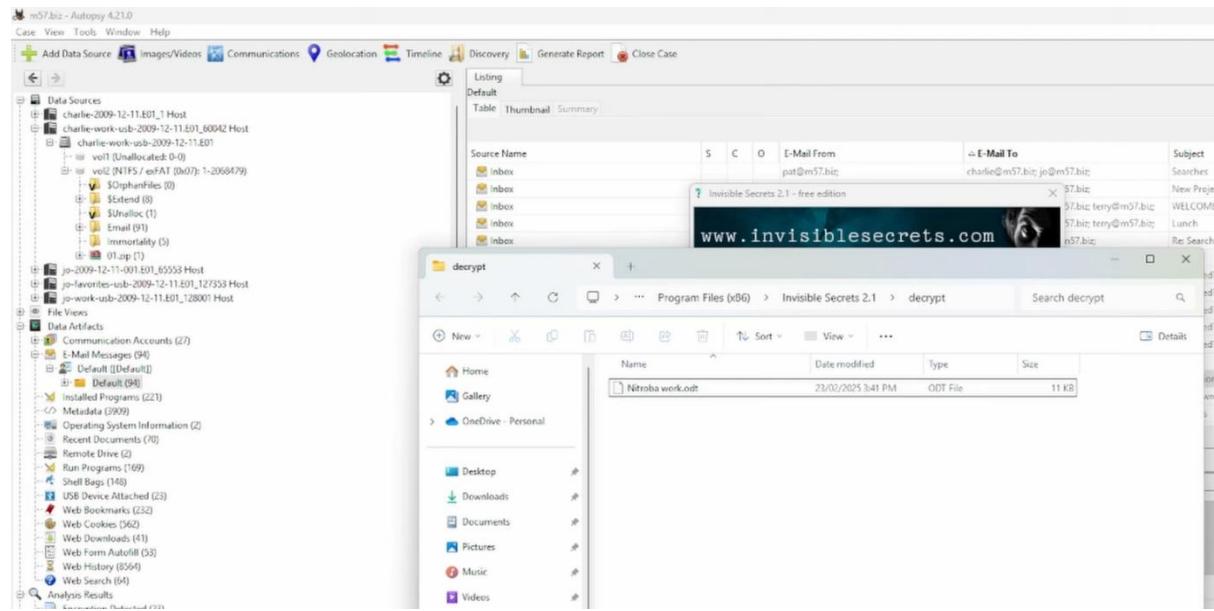


Fig. 3.18 Hidden Data

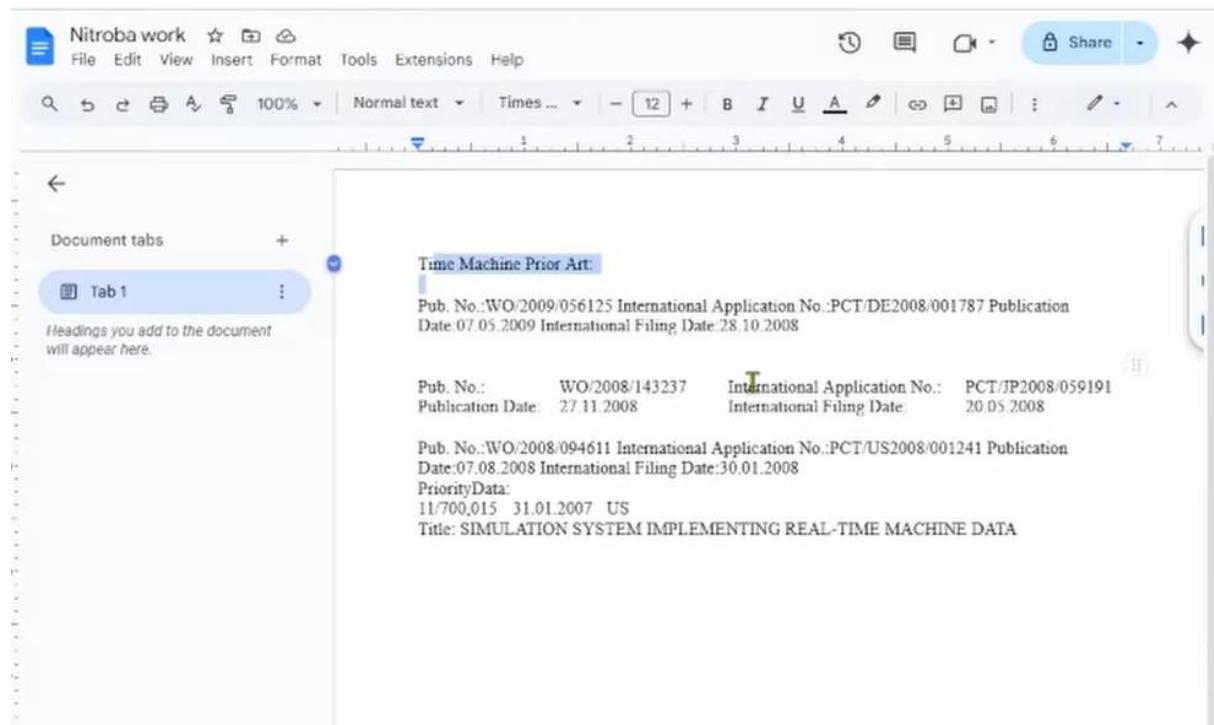


Fig. 3.19 Steganographic image 2

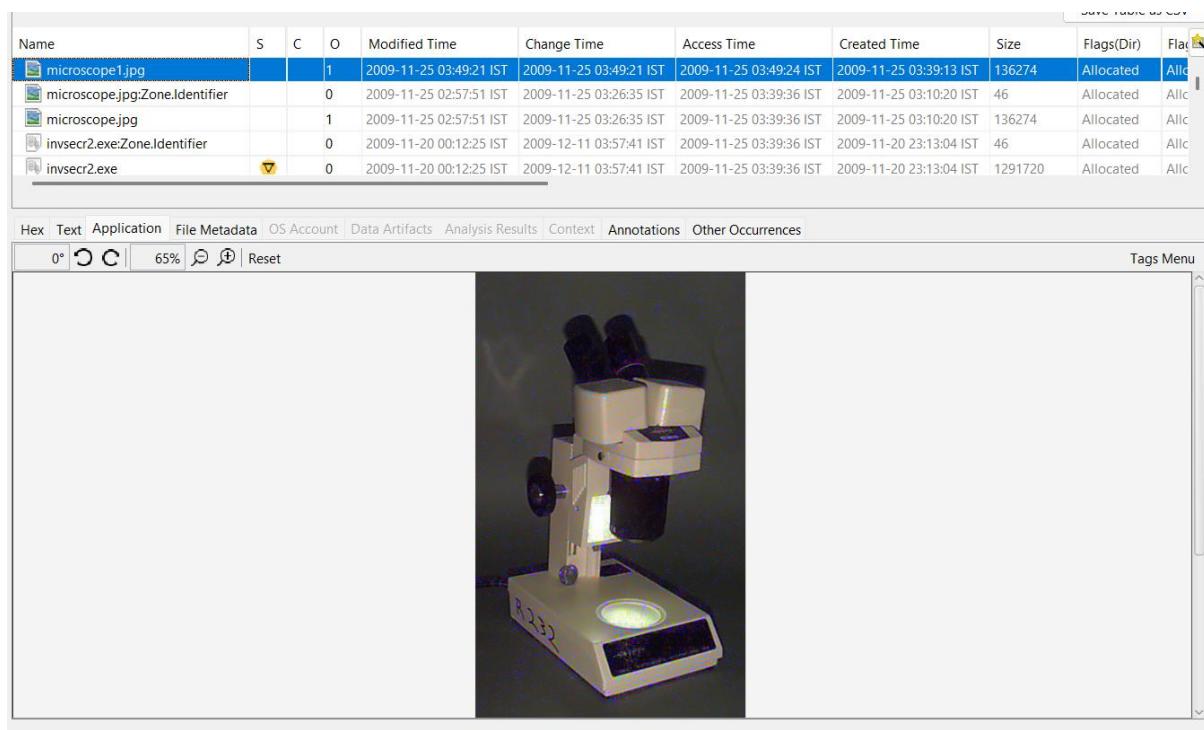


Fig. 3.20 Found Password in Hex of Image

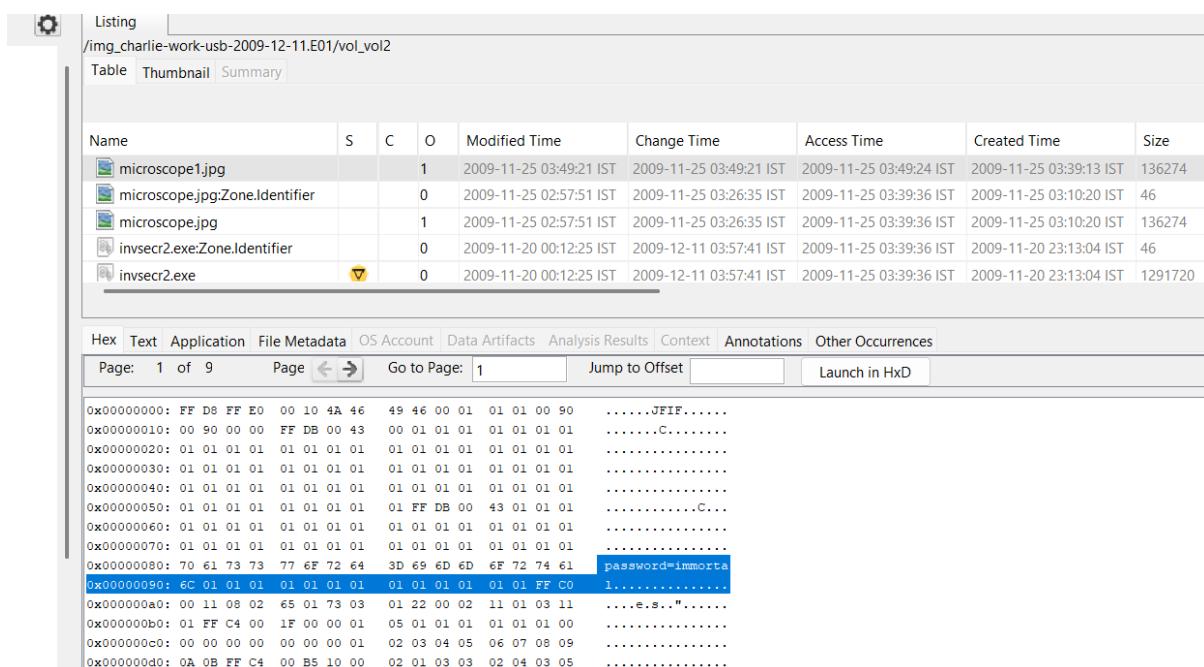


Fig. 3.21 Accessing hidden data

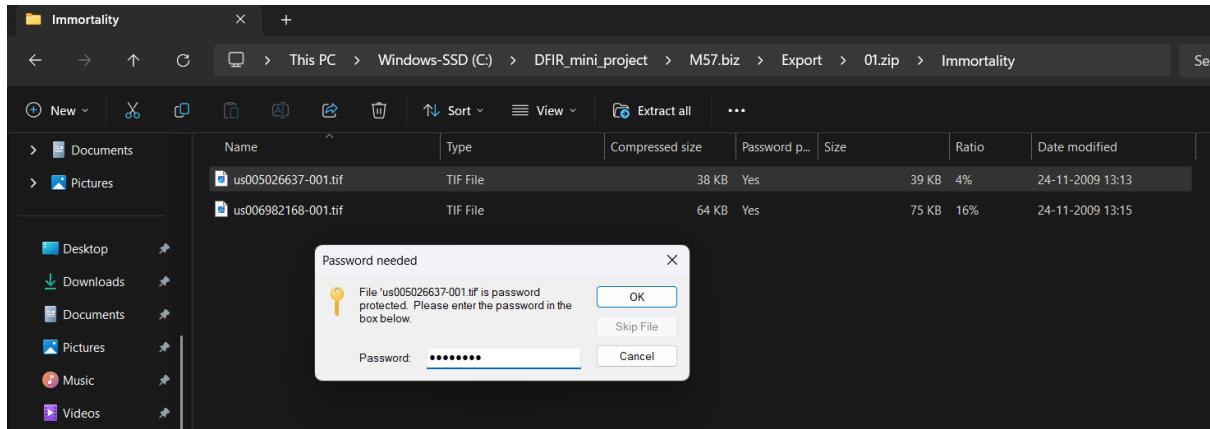
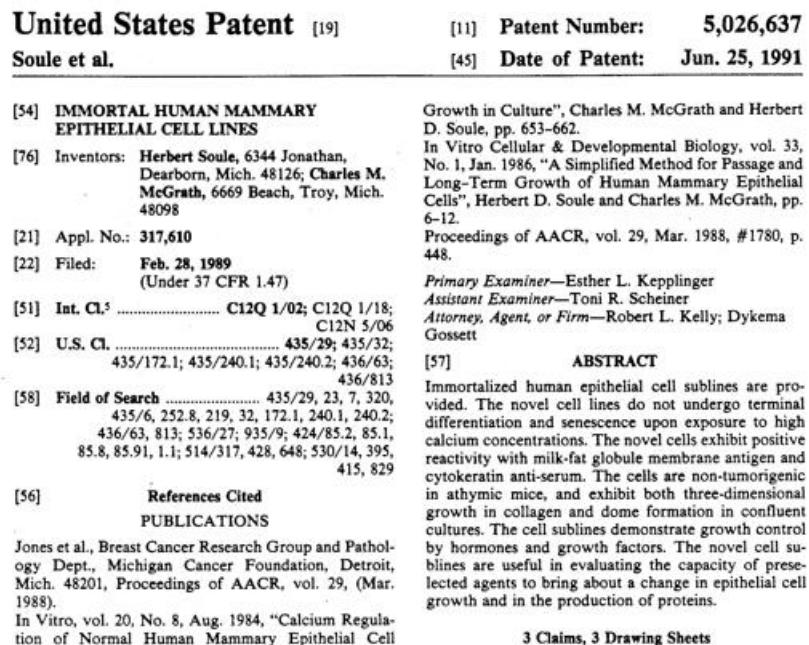


Fig. 3.22 Found Hidden Data



## **4. Tools explanations**

- **Autopsy**

Autopsy was the main forensic software used throughout the investigation. It is a digital forensics platform that helps investigators collect, organize, and examine digital evidence in a structured way. The tool provides a user-friendly interface where disk images can be loaded and analysed without affecting the original data.

In this project, Autopsy was used to create the forensic case and process all evidence sources. The evidence images were added to the case, and automated processing was carried out using ingest modules. This allowed the software to scan files, recover deleted data, extract emails, and identify important system artifacts. Investigators also used it to perform keyword searches and track communication records.

Its importance in the project was very high because it acted as the central workspace for the entire investigation. All major evidence analysis and artifact recovery activities were performed inside this platform.

- **Invisible secrets**

Invisible Secrets is a steganography software that is used to hide and extract information inside image files. Instead of simply protecting files with passwords, steganography conceals the existence of the data itself, making it much harder to detect.

During the investigation, certain image files found in email communications appeared suspicious. These images were examined using Invisible Secrets to check whether they contained hidden content. Through extraction processes, investigators were able to recover embedded files that had been secretly placed inside the images. Some of these hidden files were also protected with passwords that were later decoded.

The tool played a major role in proving that covert data transfer techniques were used. It helped uncover concealed documents that were critical to understanding the data exfiltration activity.

- **HxD**

HxD is a hexadecimal editor that allows investigators to view and analyze files in their raw binary format. Every digital file is made up of hexadecimal values, and examining this level of data can reveal information that is not visible in normal viewing software.

In this project, HxD was used to analyze suspicious image files more deeply. Although the images looked normal when opened, their raw data told a different story. Investigators discovered plaintext strings hidden within the file structure. These strings contained passwords that were required to open encrypted archives linked to the case.

HxD proved to be extremely useful because it exposed hidden data that could not be detected through conventional file viewing methods. This made it an important tool for uncovering concealed evidence.

- **SHA 256 Hashing**

SHA 256 hashing is a cryptographic technique used to verify the integrity of digital evidence. It generates a unique hash value for every file, which acts like a digital fingerprint. If a file is altered in any way, its hash value changes completely.

In this investigation, SHA 256 hashing was used to compare original image files with suspected modified versions. The differences in hash values confirmed that some files had been tampered with to include hidden data. Hashing was also used to ensure that forensic images remained unchanged during analysis.

This technique was essential because it provided mathematical proof of file manipulation and ensured that all evidence maintained its authenticity throughout the investigation.

## **5. Features Explanation**

- Evidence Analysis**

The project enables detailed examination of digital evidence collected from multiple sources. Using forensic tools, investigators can explore files, user activity, and system artifacts in an organized manner. This helps in identifying suspicious behavior and locating relevant data linked to the incident.

- Data Recovery**

One of the key features is the ability to recover deleted and hidden files that are not visible through normal system access. Through forensic processing, residual data from disk images can be extracted, allowing investigators to uncover information that suspects may have attempted to remove.

- Steganography Detection**

The project includes the capability to detect and extract hidden data concealed inside image files. By analyzing carrier images with specialized software, investigators can reveal secret payloads that were used for covert communication or data transfer.

- Hex Analysis**

Files can be examined at the hexadecimal level to identify hidden strings, appended data, or embedded credentials. This deep file inspection helps uncover information that cannot be detected through standard viewing methods.

- Integrity Verification**

The investigation ensures that all evidence remains authentic by applying cryptographic hashing techniques. Hash comparisons help confirm whether files were altered and maintain the reliability of forensic findings.

- **Email Tracing**

This feature focuses on analysing email communications found within the evidence. Investigators review message content, attachments, timestamps, and sender receiver relationships to identify suspicious interactions. Through this process, it becomes possible to trace conversations related to data sharing, financial motives, or collusion with external entities. Email tracing helps establish intent and provides contextual support to technical findings uncovered during forensic analysis.

- **Case Management**

The project maintains all evidence, analysis results, and investigation notes within a structured forensic case environment. This organized approach allows investigators to handle multiple data sources without confusion. It also ensures that every action taken during the investigation is documented properly. Effective case management supports evidence tracking, simplifies reporting, and helps maintain procedural accuracy throughout the forensic process.

## **6. Conclusion**

This project demonstrated the practical application of digital forensics and incident response techniques in investigating a simulated corporate security breach. Through a structured forensic approach, digital evidence was successfully acquired, preserved, and analysed without compromising its integrity. The investigation highlighted how seemingly ordinary files and communications can contain concealed information linked to malicious activity.

Using forensic analysis, hidden data embedded within image files was discovered and extracted. Hexadecimal examination revealed concealed passwords, while steganographic techniques exposed covert data transfer methods. Integrity verification further confirmed instances of file manipulation, strengthening the reliability of the findings.

The correlation of technical artifacts with email communications made it possible to reconstruct the sequence of events and identify the intent behind the data exfiltration. This reinforced the importance of combining technical forensic analysis with behavioural investigation.

Overall, the project provided valuable hands-on experience in evidence handling, artifact analysis, hidden data detection, and investigative reporting. It also emphasized the growing need for robust forensic capabilities to combat modern cyber threats and protect organizational intellectual property.

## **7. References**

- [1] Autopsy Digital Forensics Platform, “Autopsy® Forensic Browser,” Basis Technology. [Online]. Available: <https://www.autopsy.com>
- [2] Sleuth Kit Developers, “Autopsy and The Sleuth Kit,” Sleuth Kit. [Online]. Available: <https://sleuthkit.org/autopsy/>
- [3] Invisible Secrets Software, “Invisible Secrets Steganography Software,” Everstrike Software. [Online]. Available: <https://www.east-tec.com/invisiblesecrets/>
- [4] M. Hedenfalk, “HxD Hex Editor,” MH Nexus. [Online]. Available: <https://mh-nexus.de/en/hxd/>
- [5] National Institute of Standards and Technology, “Secure Hash Standard,” FIPS PUB 180 4. [Online]. Available: <https://csrc.nist.gov/publications/detail/fips/180/4/final>
- [6] National Institute of Standards and Technology, “Computer Forensics Tool Testing Program,” NIST. [Online]. Available: <https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program>