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	**PRN: 250860940037**
Chandan Vikas Shimpi	**PRN: 250860940008**
Prachi Chandrakant Sabade	**PRN: 250860940022**
Shravani Kawale	**PRN: 250860940035**
Utkarsh Krishnarao Pote	**PRN: 250860940046**

Under The Guidance Of

Mr. Jayaram P.	**Dr. Priya P. Sajan**
Centre Co-ordinator	**Project Guide**

Table of Contents **Page No.**

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
Total Evidence		**~20GB**	

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

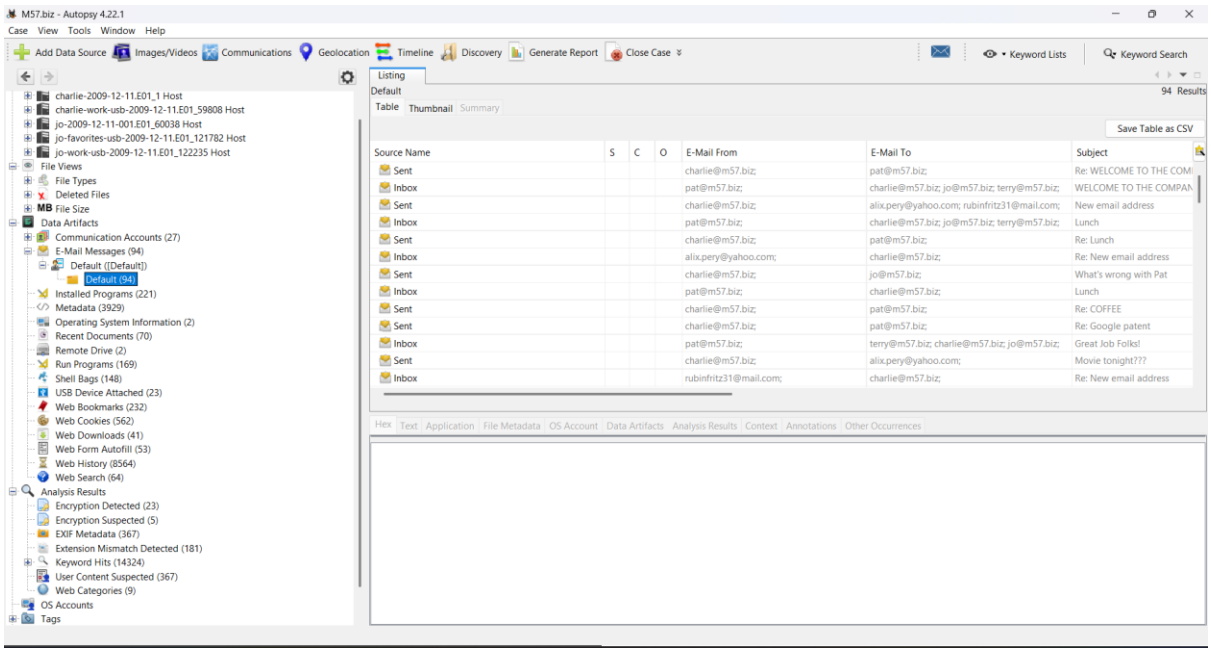


Fig. 3.2

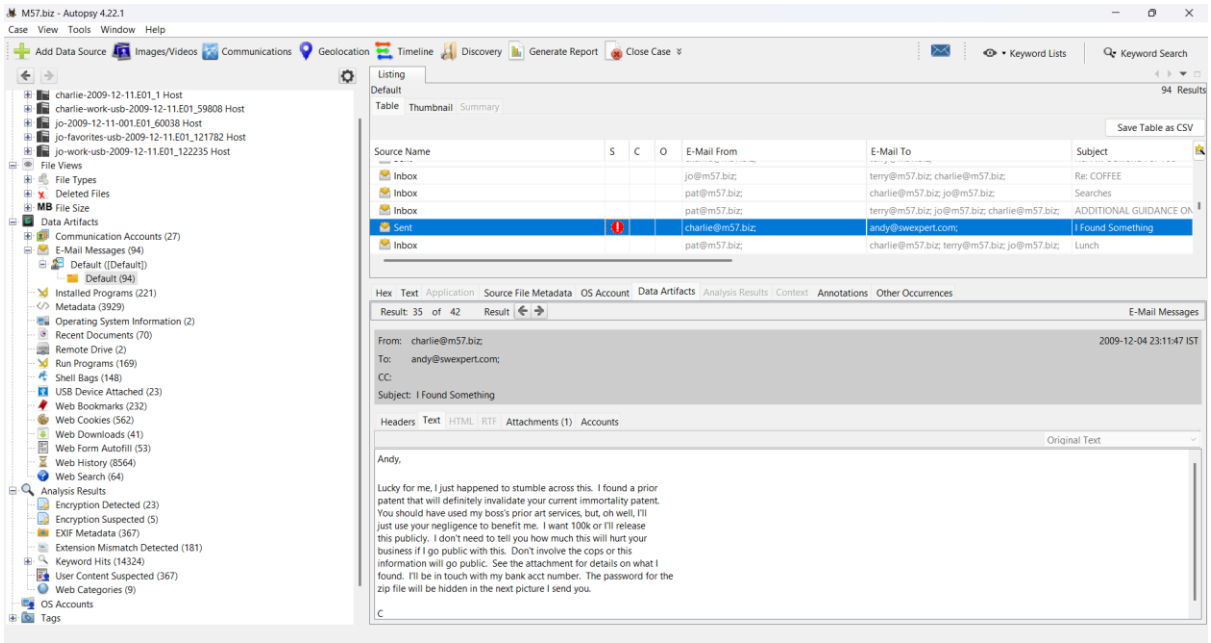


Fig. 3.3 Found Attachment

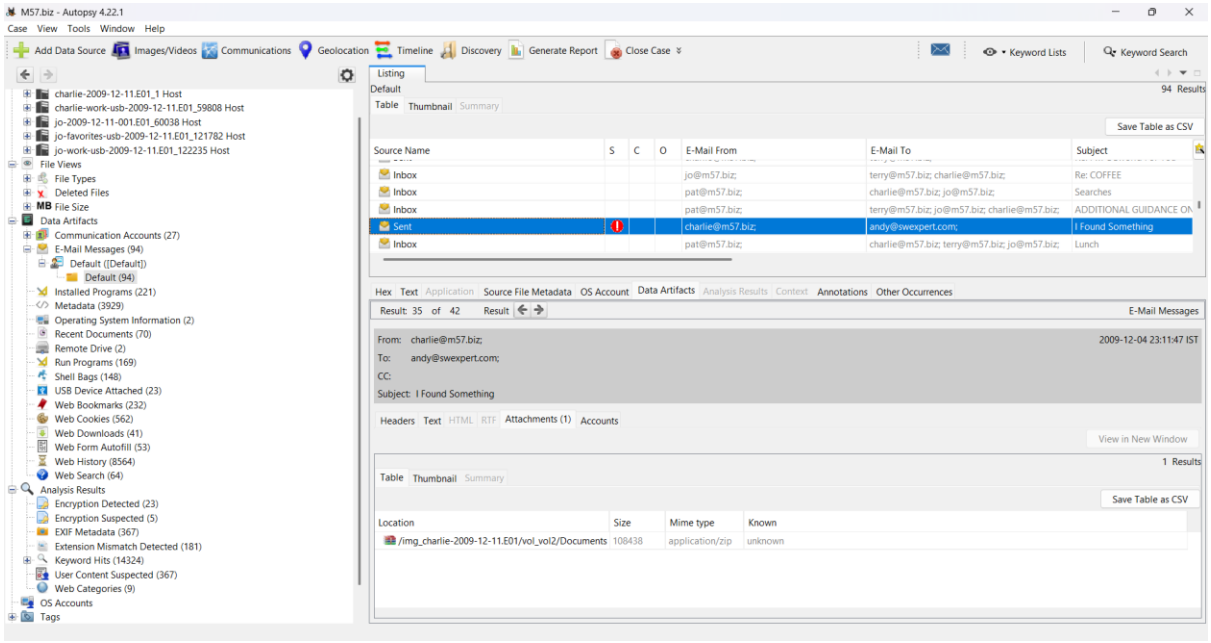


Fig. 3.4

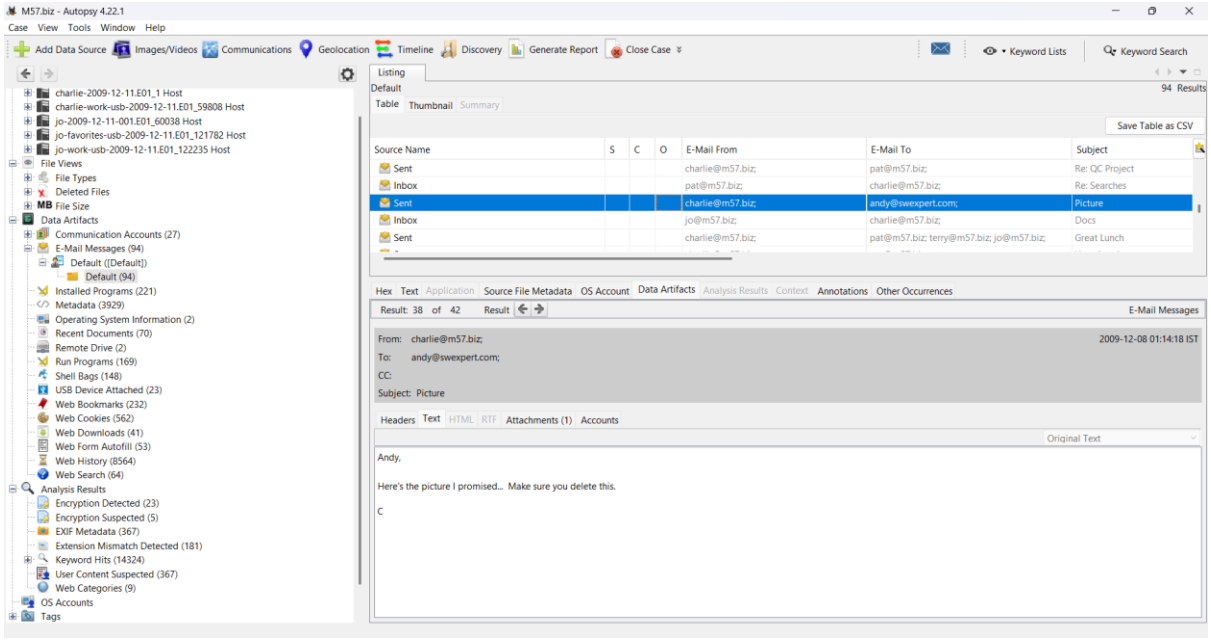


Fig. 3.5

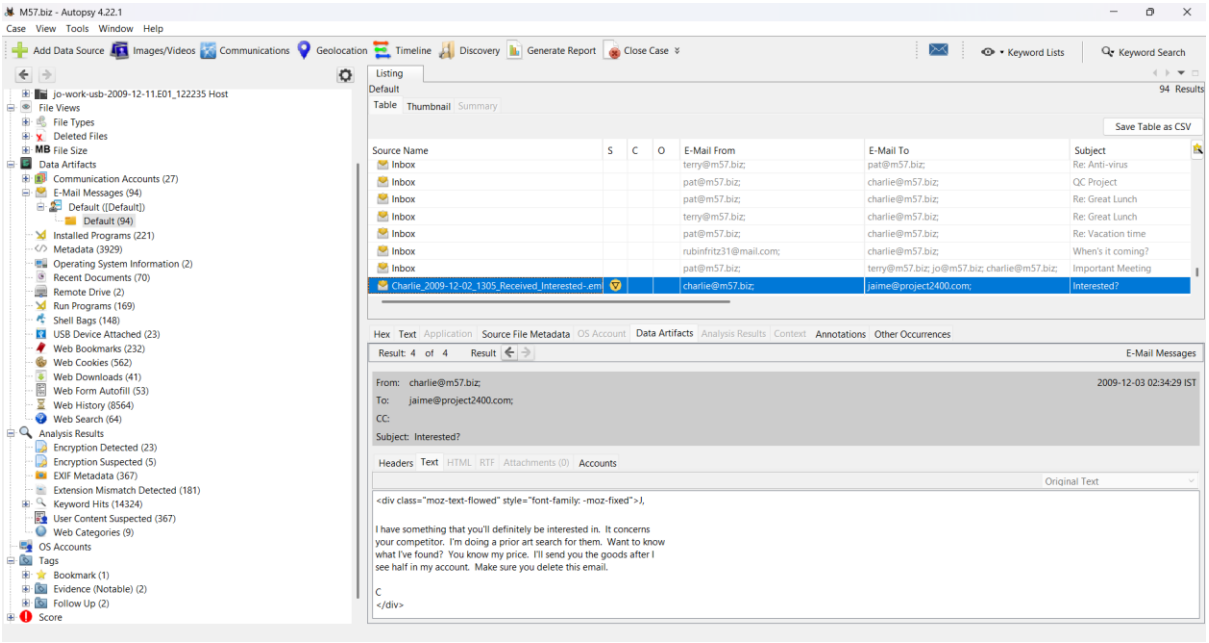

M57.biz - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
jo-work-usb-2009-12-11.E01_122235 Host
File Views
File Types
Deleted Files
File Size
Data Artifacts
Communication Accounts (27)
E-Mail Messages (94)
Default ([Default])
Default (94)
Installed Programs (221)
Metadata (3929)
Operating System Information (2)
Recent Documents (70)
Remote Drive (2)
Run Programs (169)
Shell Bags (148)
USB Device Attached (23)
Web Bookmarks (232)
Web Cookies (562)
Web Downloads (41)
Web Form Autofill (53)
Web History (8564)
Web Search (64)
Analysis Results
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
Tags
Bookmark (1)
Evidence (Notable) (2)
Follow Up (2)
Score
Listing
Default
94 Results
Table Thumbnail Summary
Save Table as CSV
Source Name S C O E-Mail From E-Mail To Subject
Inbox terry@m57.biz; pat@m57.biz; Re: Anti-virus
Inbox pat@m57.biz; charlie@m57.biz; QC Project
Inbox pat@m57.biz; charlie@m57.biz; Re: Great Lunch
Inbox terry@m57.biz; charlie@m57.biz; Re: Great Lunch
Inbox pat@m57.biz; charlie@m57.biz; Re: Vacation time
Inbox rubinfritz31@mail.com; charlie@m57.biz; When's it coming?
Inbox pat@m57.biz; terry@m57.biz; jo@m57.biz; charlie@m57.biz; Important Meeting
Charlie_2009-12-02_1305_Received_Interested-.em charlie@m57.biz; jaime@project2400.com; Interested?
Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Result: 4 of 4 Result
E-Mail Messages
From: charlie@m57.biz; 2009-12-03 02:34:29 IST
To: jaime@project2400.com;
CC:
Subject: Interested?
Headers Text HTML RTF Attachments (0) Accounts
Original Text
J,
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.
C

Fig. 3.6

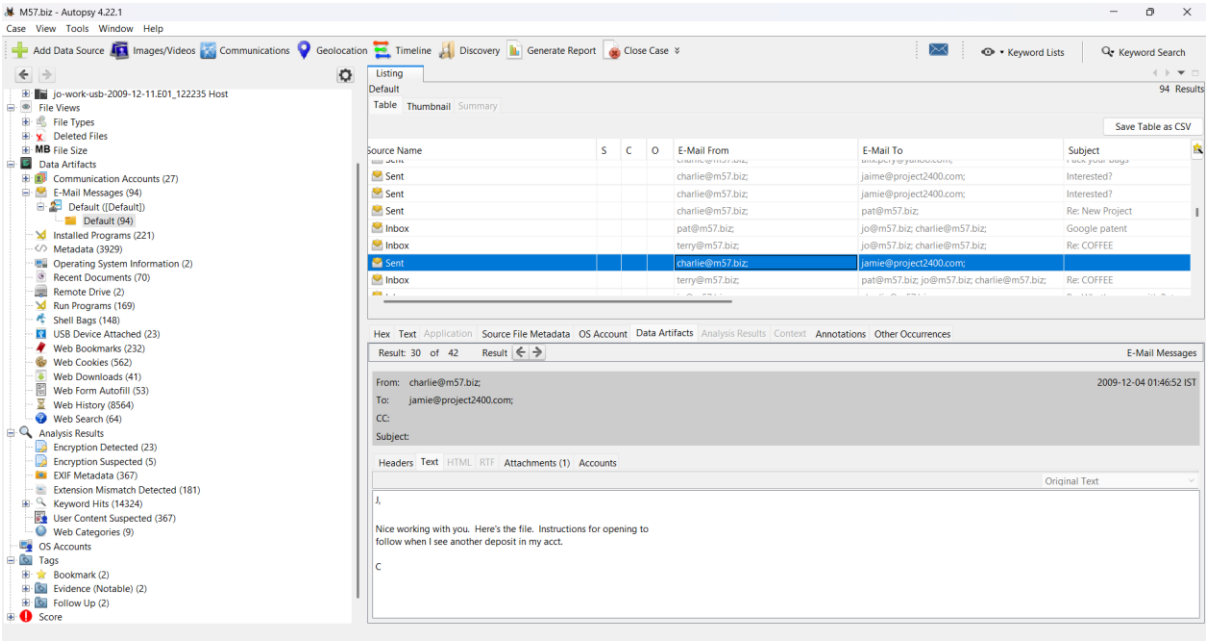

M57.biz - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
jo-work-usb-2009-12-11.E01_122235 Host
File Views
File Types
Deleted Files
File Size
Data Artifacts
Communication Accounts (27)
E-Mail Messages (94)
Default ([Default])
Default (94)
Installed Programs (221)
Metadata (3929)
Operating System Information (2)
Recent Documents (70)
Remote Drive (2)
Run Programs (169)
Shell Bags (148)
USB Device Attached (23)
Web Bookmarks (232)
Web Cookies (562)
Web Downloads (41)
Web Form Autofill (53)
Web History (8564)
Web Search (64)
Analysis Results
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
Tags
Bookmark (2)
Evidence (Notable) (2)
Follow Up (2)
Score
Listing
Default
94 Results
Table Thumbnail Summary
Save Table as CSV
Source Name S C O E-Mail From E-Mail To Subject
Sent charlie@m57.biz; jaime@project2400.com; Interested?
Sent charlie@m57.biz; jamie@project2400.com; Interested?
Sent charlie@m57.biz; pat@m57.biz; Re: New Project
Inbox pat@m57.biz; jo@m57.biz; charlie@m57.biz; Google patent
Inbox terry@m57.biz; jo@m57.biz; charlie@m57.biz; Re: COFFEE
Sent charlie@m57.biz; jamie@project2400.com;
Inbox terry@m57.biz; pat@m57.biz; jo@m57.biz; charlie@m57.biz; Re: COFFEE
Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Result: 30 of 42 Result
E-Mail Messages
From: charlie@m57.biz; 2009-12-04 01:46:52 IST
To: jamie@project2400.com;
CC:
Subject:
Headers Text HTML RTF Attachments (1) Accounts
Original Text
J,
Nice working with you. Here's the file. Instructions for opening to follow when I see another deposit in my acct.
C

Fig. 3.7

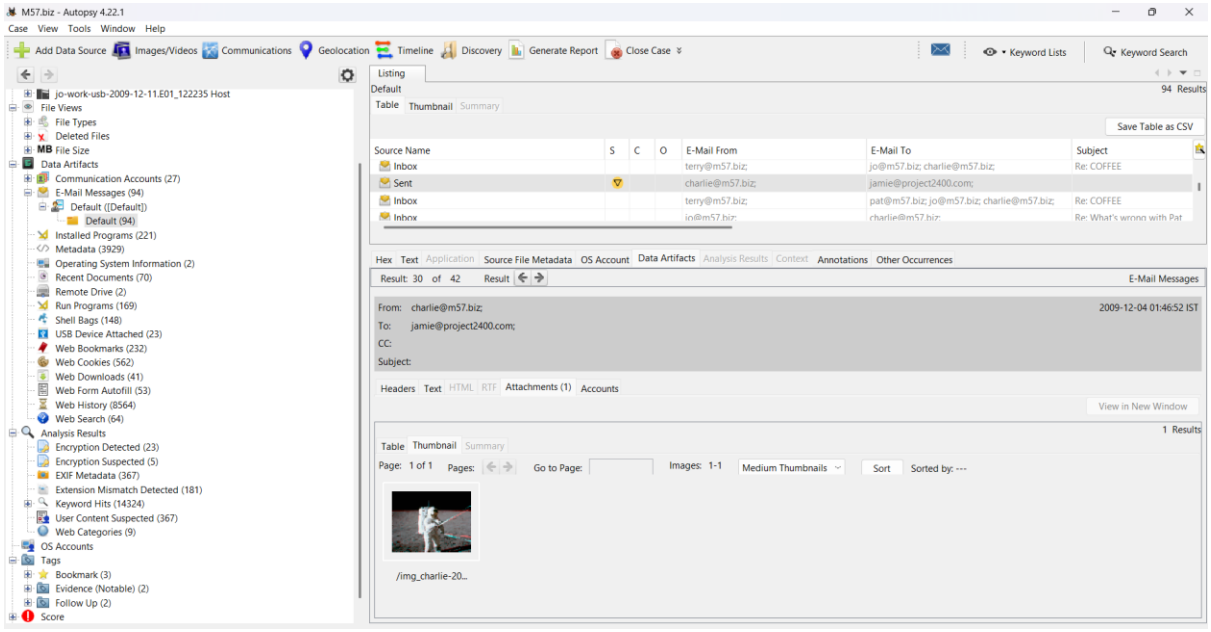

M57.biz - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
jo-work-usb-2009-12-11.E01_122235 Host
File Views
File Types
Deleted Files
File Size
Data Artifacts
Communication Accounts (27)
E-Mail Messages (94)
Default ([Default])
Default (94)
Installed Programs (221)
Metadata (3929)
Operating System Information (2)
Recent Documents (70)
Remote Drive (2)
Run Programs (169)
Shell Bags (148)
USB Device Attached (23)
Web Bookmarks (232)
Web Cookies (562)
Web Downloads (41)
Web Form Autofill (53)
Web History (8564)
Web Search (64)
Analysis Results
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
Tags
Bookmark (3)
Evidence (Notable) (2)
Follow Up (2)
Score
Listing
Default
94 Results
Table Thumbnail Summary
Save Table as CSV
Source Name S C O E-Mail From E-Mail To Subject
Inbox terry@m57.biz; jo@m57.biz; charlie@m57.biz; Re: COFFEE
Sent charlie@m57.biz; jamie@project2400.com;
Inbox terry@m57.biz; pat@m57.biz; jo@m57.biz; charlie@m57.biz; Re: COFFEE
Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Result: 30 of 42 Result
E-Mail Messages
From: charlie@m57.biz; 2009-12-04 01:46:52 IST
To: jamie@project2400.com;
CC:
Subject:
Headers Text HTML RTF Attachments (1) Accounts
View in New Window
1 Results
Table Thumbnail Summary
Page: 1 of 1 Pages: Go to Page: Images: 1-1 Medium Thumbnails Sort Sorted by: ---
/img_charlie-20...

Fig. 3.8

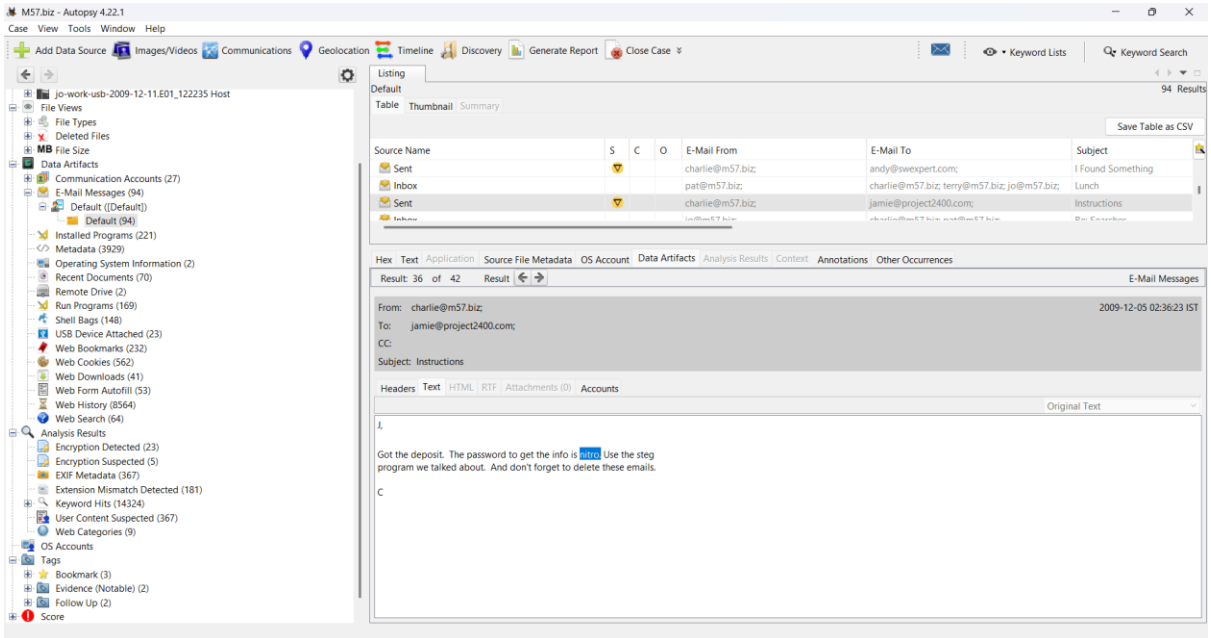

M57.biz - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
jo-work-usb-2009-12-11.E01_122235 Host
File Views
File Types
Deleted Files
File Size
Data Artifacts
Communication Accounts (27)
E-Mail Messages (94)
Default ([Default])
Default (94)
Installed Programs (221)
Metadata (3929)
Operating System Information (2)
Recent Documents (70)
Remote Drive (2)
Run Programs (169)
Shell Bags (148)
USB Device Attached (23)
Web Bookmarks (232)
Web Cookies (562)
Web Downloads (41)
Web Form Autofill (53)
Web History (8564)
Web Search (64)
Analysis Results
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
Tags
Bookmark (3)
Evidence (Notable) (2)
Follow Up (2)
Score
Listing
Default
94 Results
Table Thumbnail Summary
Save Table as CSV
Source Name S C O E-Mail From E-Mail To Subject
Sent charlie@m57.biz; andy@swexpert.com; I Found Something
Inbox pat@m57.biz; charlie@m57.biz; terry@m57.biz; jo@m57.biz; Lunch
Sent charlie@m57.biz; jamie@project2400.com; Instructions
Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Result: 36 of 42 Result
E-Mail Messages
From: charlie@m57.biz; 2009-12-05 02:36:23 IST
To: jamie@project2400.com;
CC:
Subject: Instructions
Headers Text HTML RTF Attachments (0) Accounts
Original Text
),
Got the deposit. The password to get the info is nitro. Use the steg
program we talked about. And don't forget to delete these emails.
C

Fig. 3.9

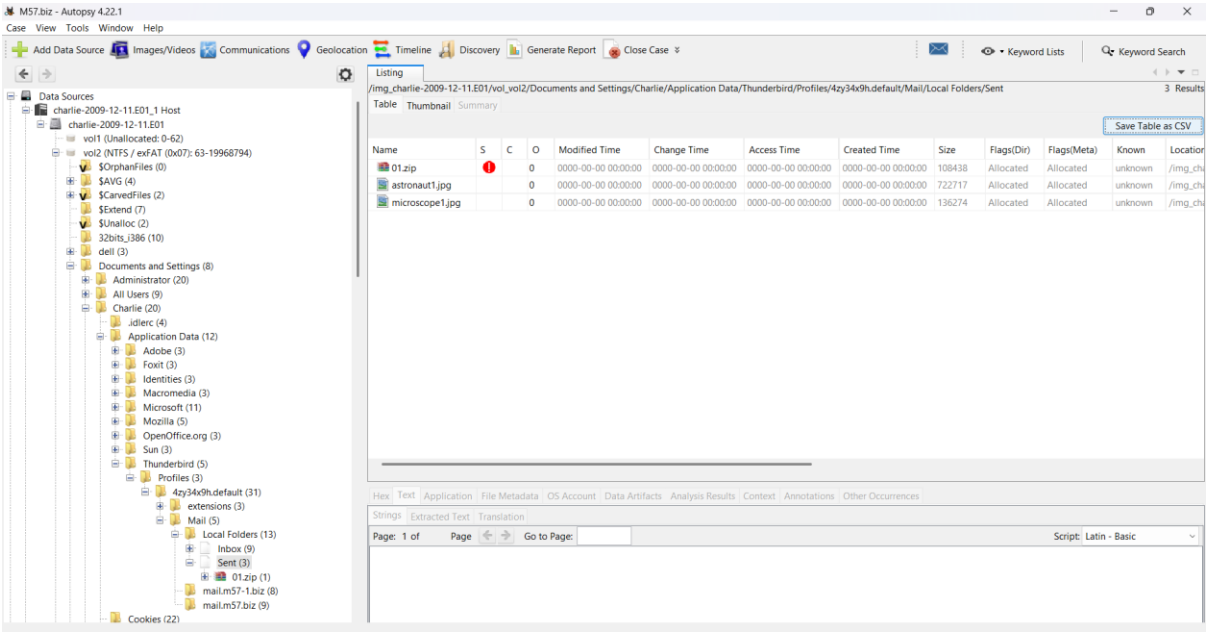


Fig. 3.10

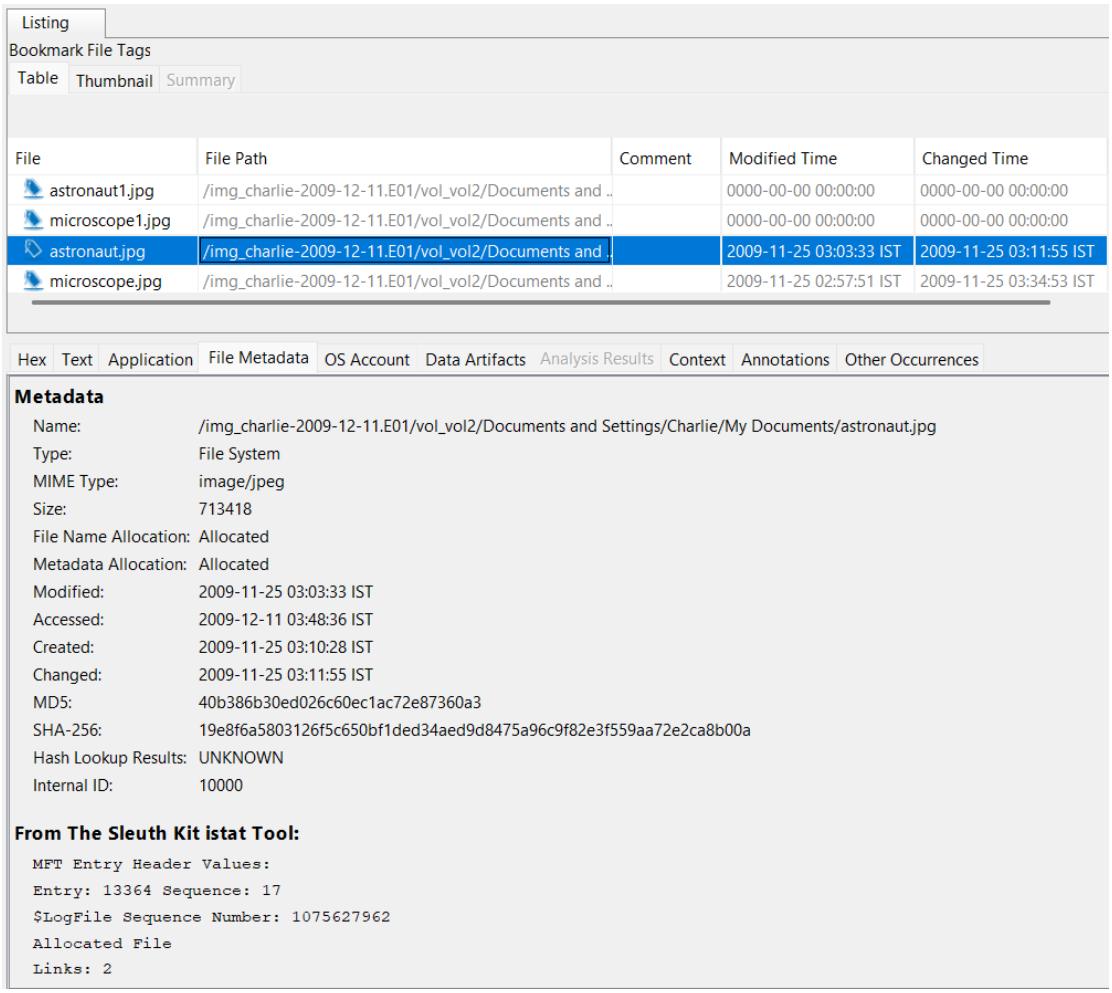


Fig. 3.11

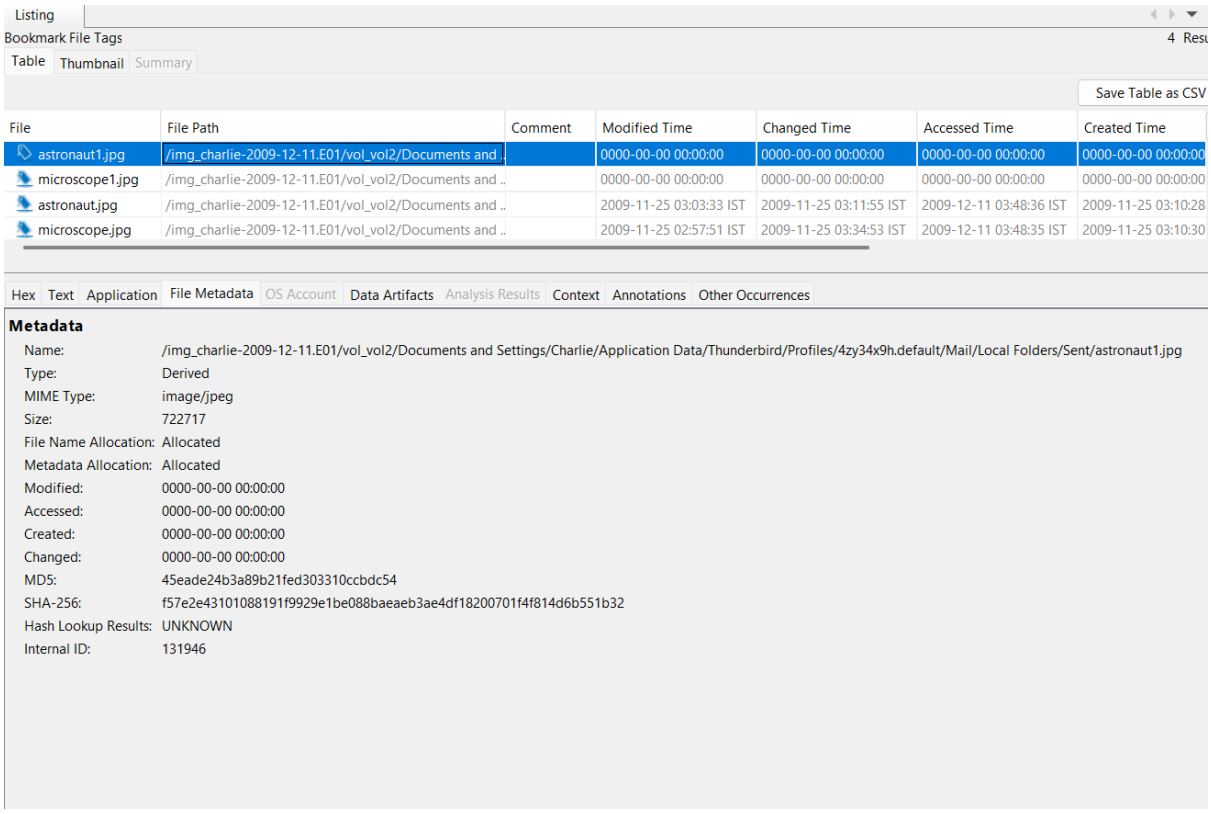


Fig. 3.12

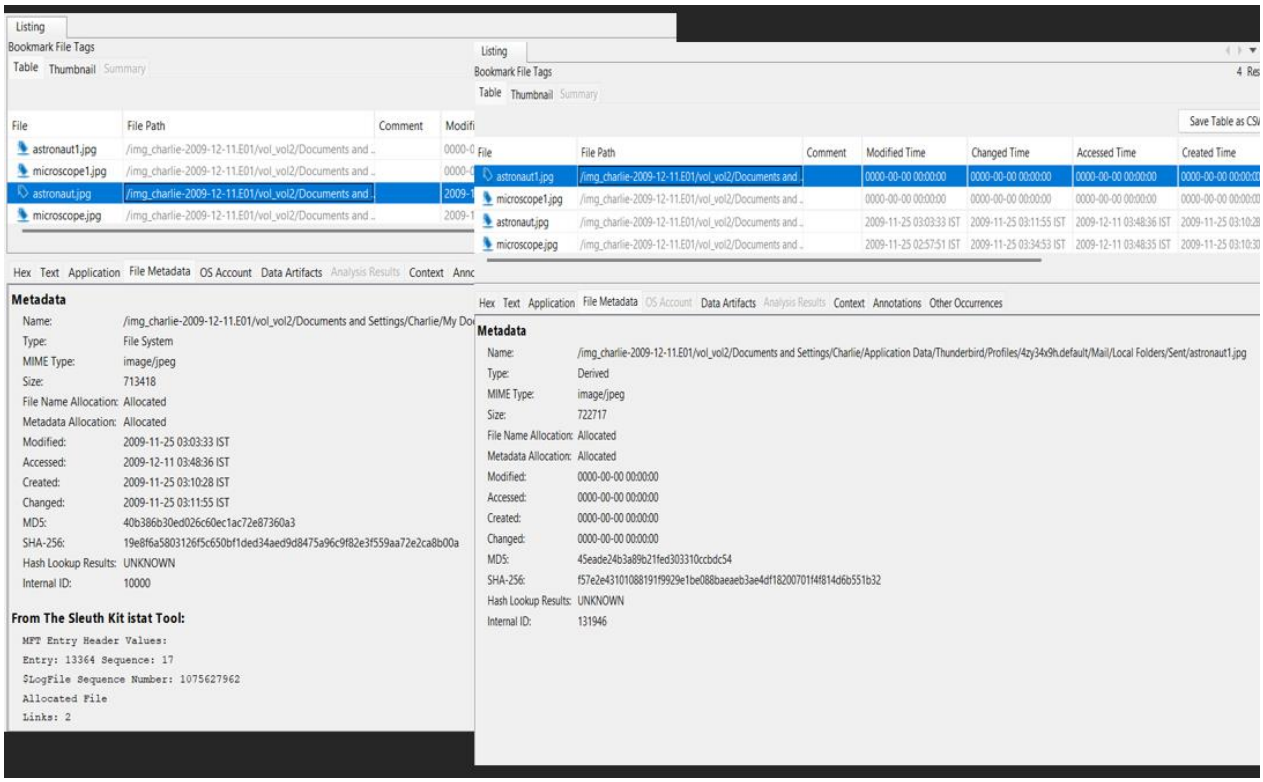


Fig. 3.13

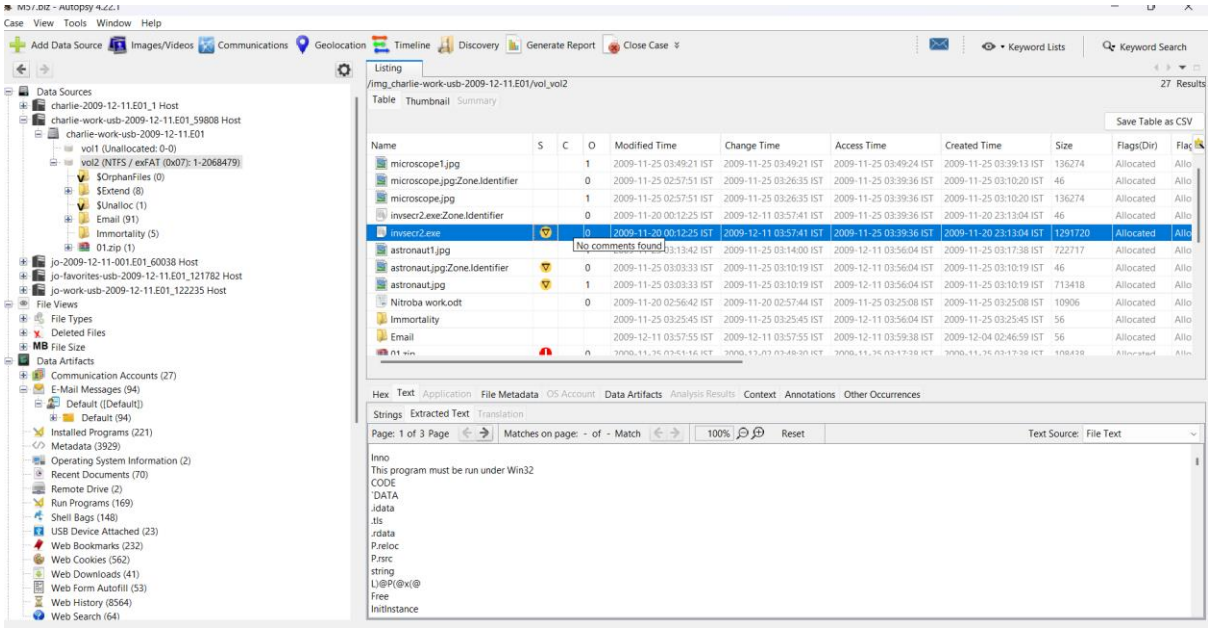


Fig. 3.14

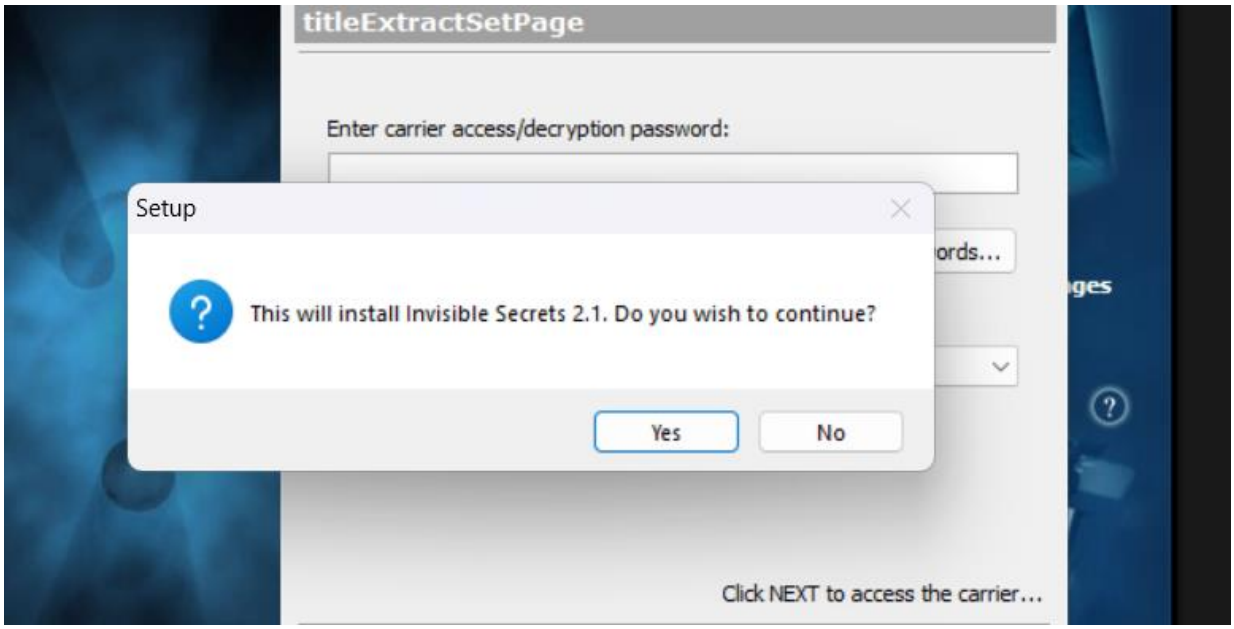


Fig. 3.15

Fig. 3.16

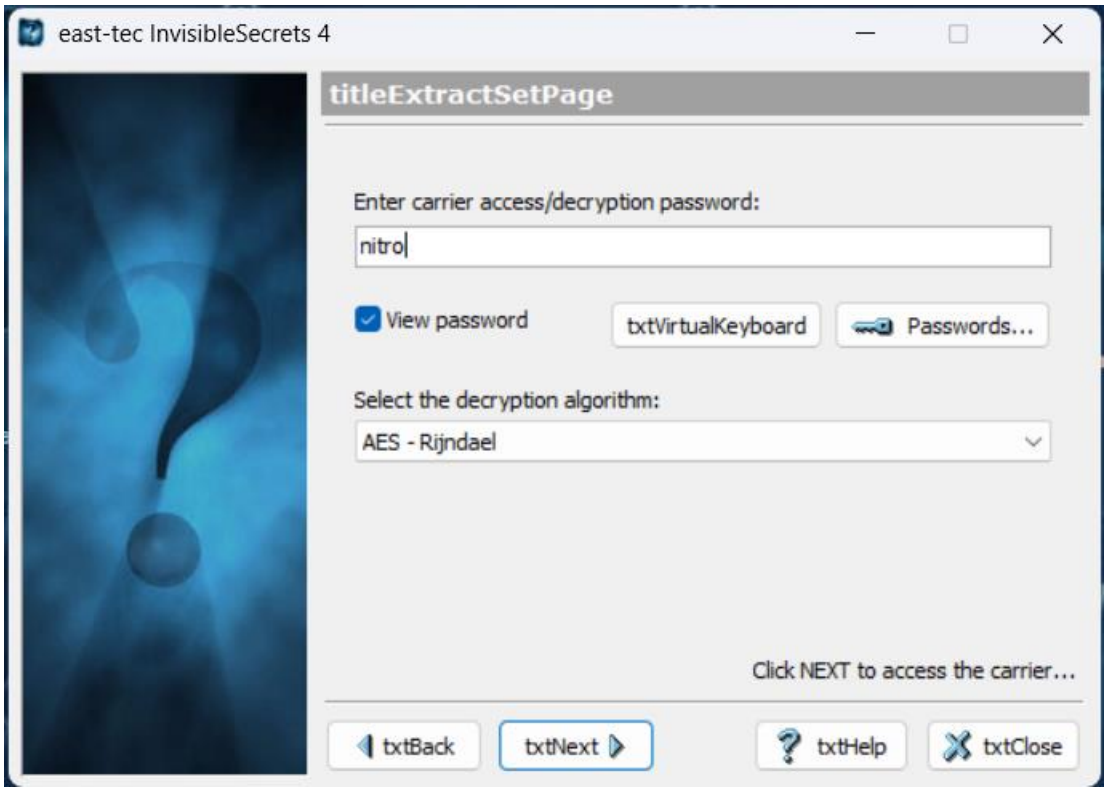


Fig. 3.17

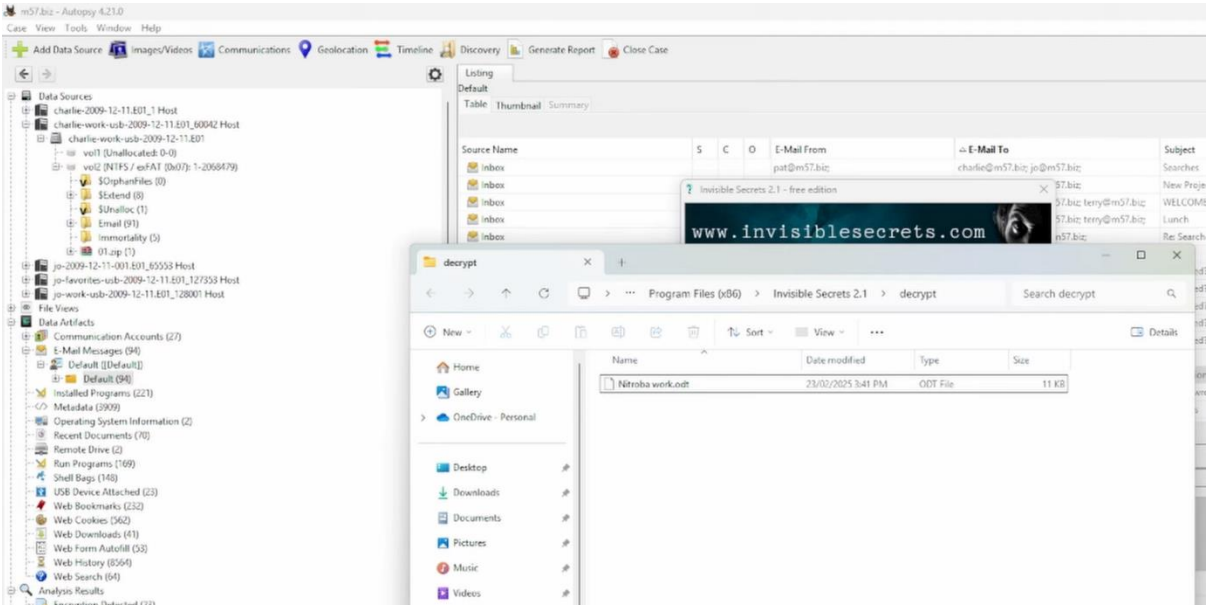


Fig. 3.18

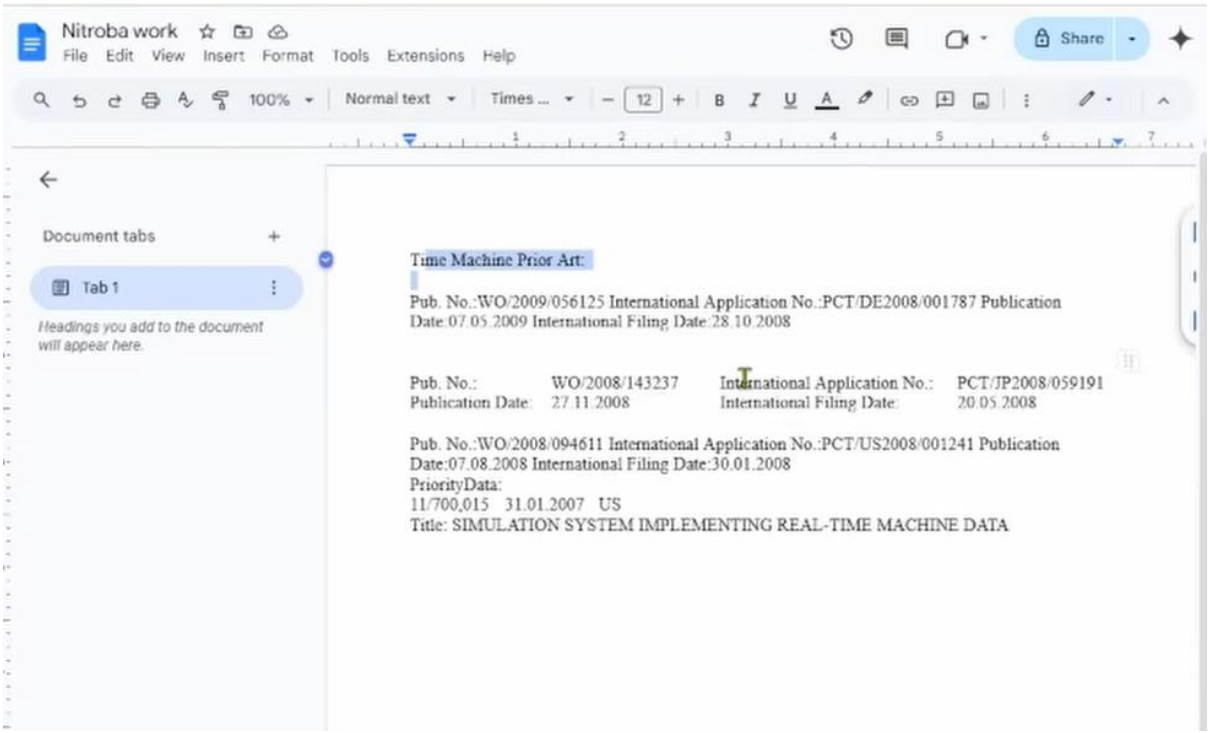


Fig. 3.19

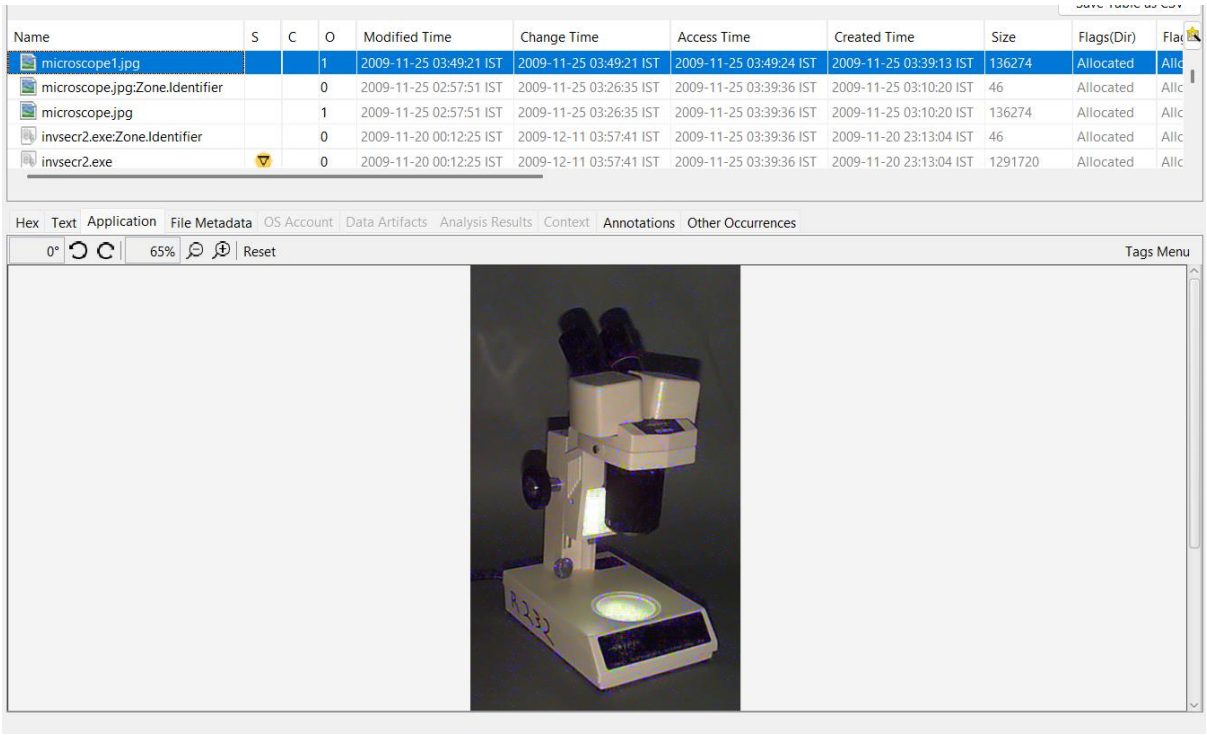


Fig. 3.20

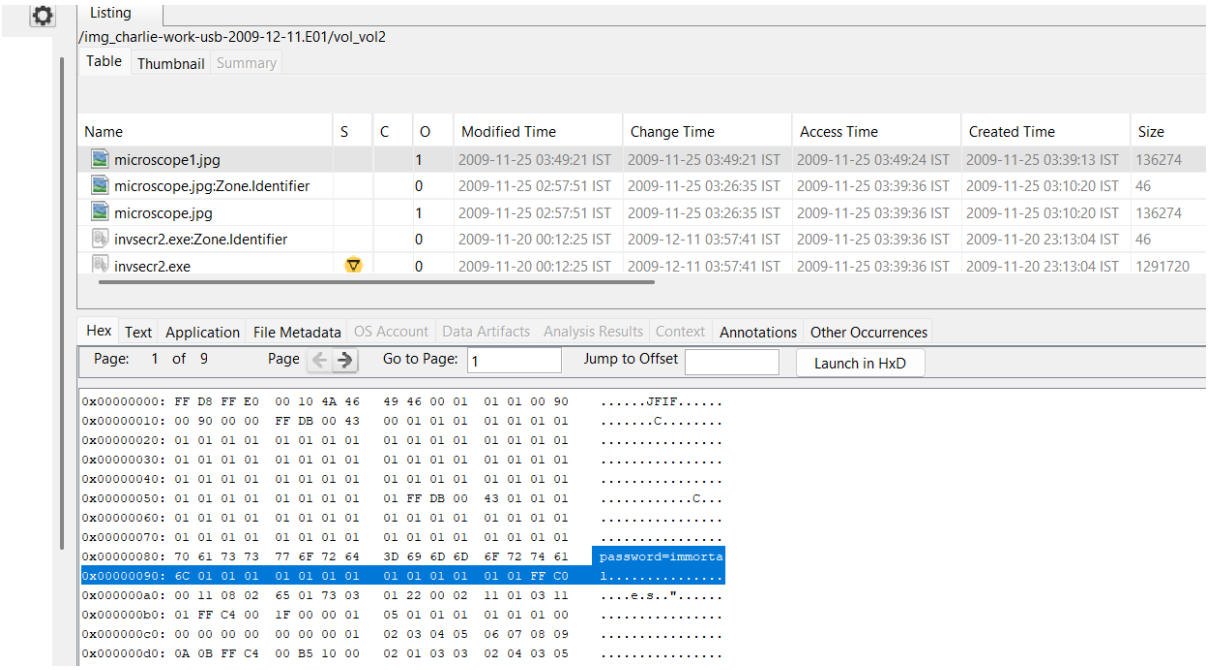


Fig. 3.21

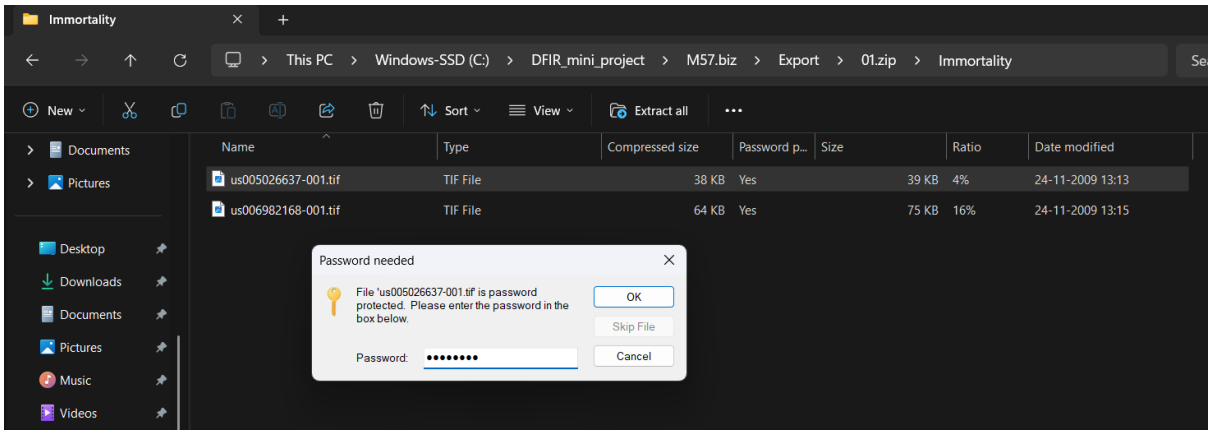
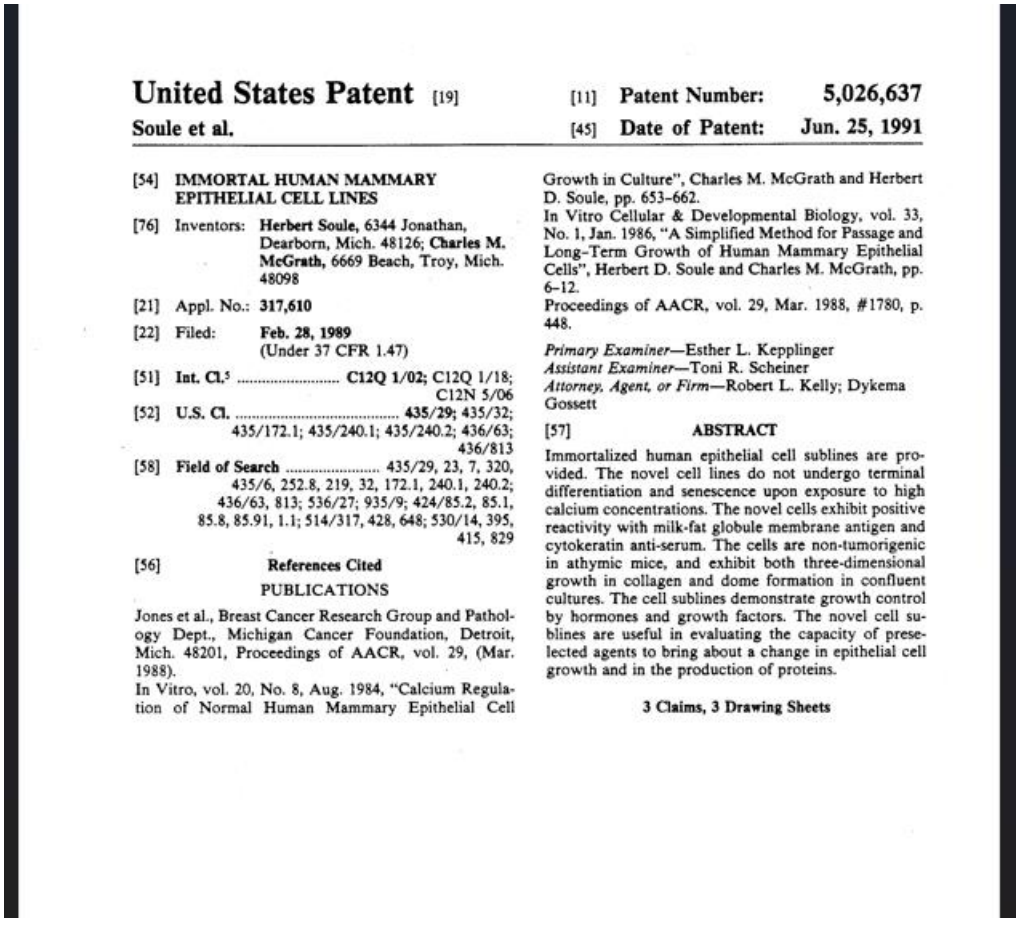


Fig. 3.22



United States Patent [19]

Soule et al.

[11] **Patent Number: 5,026,637**

[45] **Date of Patent: Jun. 25, 1991**

[54] **IMMORTAL HUMAN MAMMARY EPITHELIAL CELL LINES**

[76] Inventors: **Herbert Soule**, 6344 Jonathan, Dearborn, Mich. 48126; **Charles M. McGrath**, 6669 Beach, Troy, Mich. 48098

[21] Appl. No.: **317,610**

[22] Filed: **Feb. 28, 1989** (Under 37 CFR 1.47)

[51] **Int. Cl.**[5] **C12Q 1/02**; C12Q 1/18; C12N 5/06

[52] **U.S. Cl.** **435/29**; 435/32; 435/172.1; 435/240.1; 435/240.2; 436/63; 436/813

[58] **Field of Search** 435/29, 23, 7, 320, 435/6, 252.8, 219, 32, 172.1, 240.1, 240.2; 436/63, 813; 536/27; 935/9; 424/85.2, 85.1, 85.8, 85.91, 1.1; 514/317, 428, 648; 530/14, 395, 415, 829

[56] **References Cited**

PUBLICATIONS

Jones et al., Breast Cancer Research Group and Pathology Dept., Michigan Cancer Foundation, Detroit, Mich. 48201, Proceedings of AACR, vol. 29, (Mar. 1988).
In Vitro, vol. 20, No. 8, Aug. 1984, "Calcium Regulation of Normal Human Mammary Epithelial Cell Growth in Culture", Charles M. McGrath and Herbert D. Soule, pp. 653–662.
In Vitro Cellular & Developmental Biology, vol. 33, No. 1, Jan. 1986, "A Simplified Method for Passage and Long-Term Growth of Human Mammary Epithelial Cells", Herbert D. Soule and Charles M. McGrath, pp. 6–12.
Proceedings of AACR, vol. 29, Mar. 1988, #1780, p. 448.

Primary Examiner—Esther L. Kepplinger
Assistant Examiner—Toni R. Scheiner
Attorney, Agent, or Firm—Robert L. Kelly; Dykema Gossett

[57] **ABSTRACT**

Immortalized human epithelial cell sublines are provided. The novel cell lines do not undergo terminal differentiation and senescence upon exposure to high calcium concentrations. The novel cells exhibit positive reactivity with milk-fat globule membrane antigen and cytokeratin anti-serum. The cells are non-tumorigenic in athymic mice, and exhibit both three-dimensional growth in collagen and dome formation in confluent cultures. The cell sublines demonstrate growth control by hormones and growth factors. The novel cell sublines are useful in evaluating the capacity of preselected agents to bring about a change in epithelial cell growth and in the production of proteins.

3 Claims, 3 Drawing Sheets

4. Tools explations

- **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