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

A PROJECT REPORT ON

“M57.biz Incident Response & Forensics using Autopsy”

SUBMITTED TOWARDS THE

Under The Guidance Of

Mr. Jayaram P.
Centre Co-ordinator

Dr. Priya P. Sajan
Project Guide

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

Abstract

- Focuses on digital forensics and incident response in a simulated corporate security breach.
- Aims to analyse compromised evidence and identify the root cause of the incident.
- Includes secure evidence acquisition while maintaining forensic integrity and chain of custody.
- Examines disk images, logs, and system artifacts to detect indicators of compromise (IOCs).
- Performs timeline reconstruction and log correlation to track attacker behaviour.
- Applies advanced techniques to recover deleted files and analyse user/system activities.
- Provides insights into exploited vulnerabilities and suggests preventive security measures for organizations.

Introduction

- Organizations face growing cyber threats such as unauthorized access and data breaches.
- Digital forensics and incident response help identify the cause, impact, and sequence of cyber incidents.
- Focuses on a simulated corporate forensic investigation.
- Emphasizes proper evidence collection and integrity preservation.
- Includes detection of hidden and visible digital artifacts.
- Tools used: Autopsy, Invisible Secrets, and HxD for forensic analysis.
- Evidence integrity verified using SHA-256 hashing to ensure authenticity.

Project Objectives

- 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.

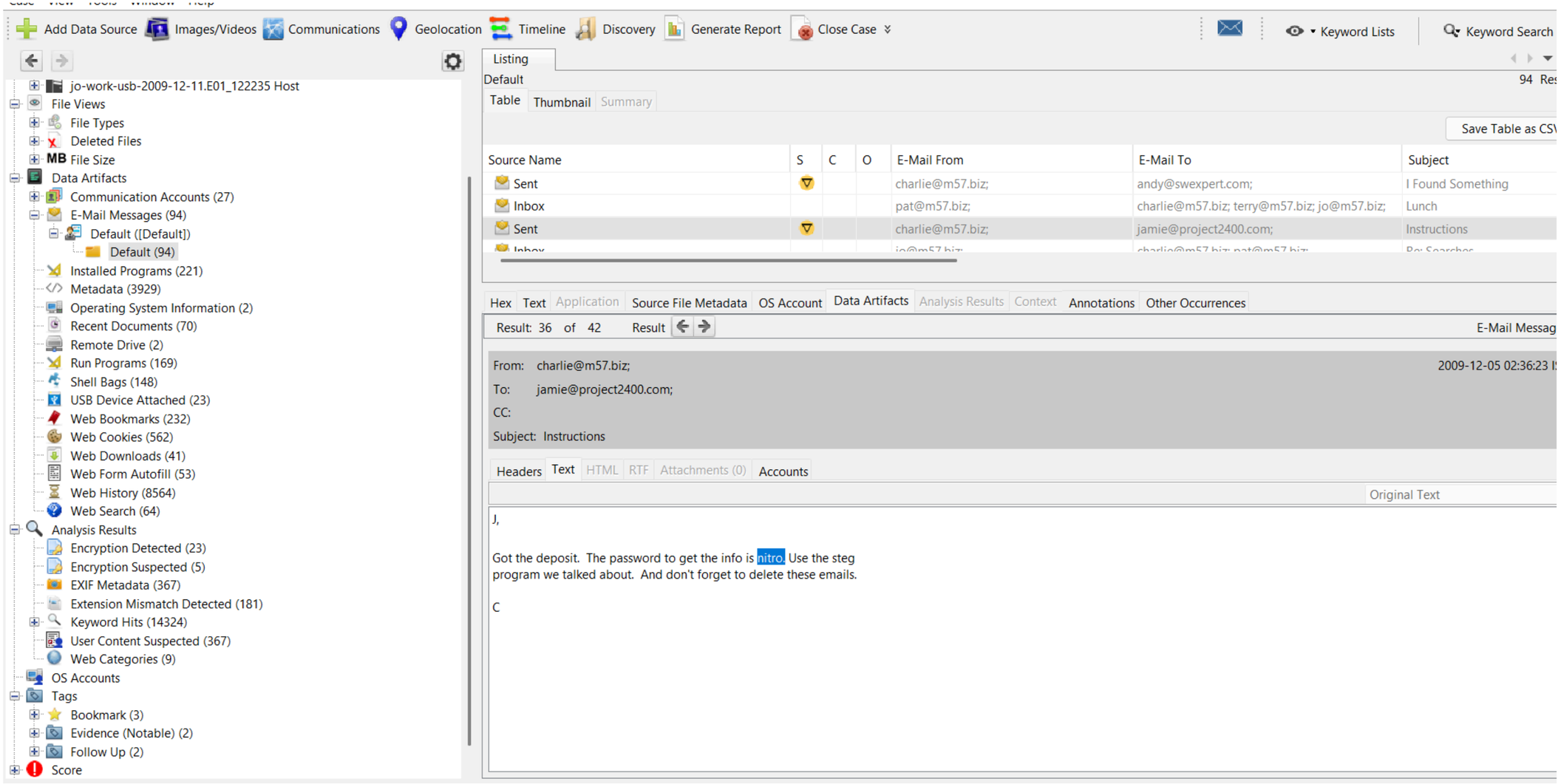
Investigation Workflow

1. Evidence Collection
2. Disk Imaging
3. Data Ingestion in Autopsy
4. Triage & Keyword Search
5. Email & File Analysis
6. Steganography & Decryption
7. Reporting & Documentation

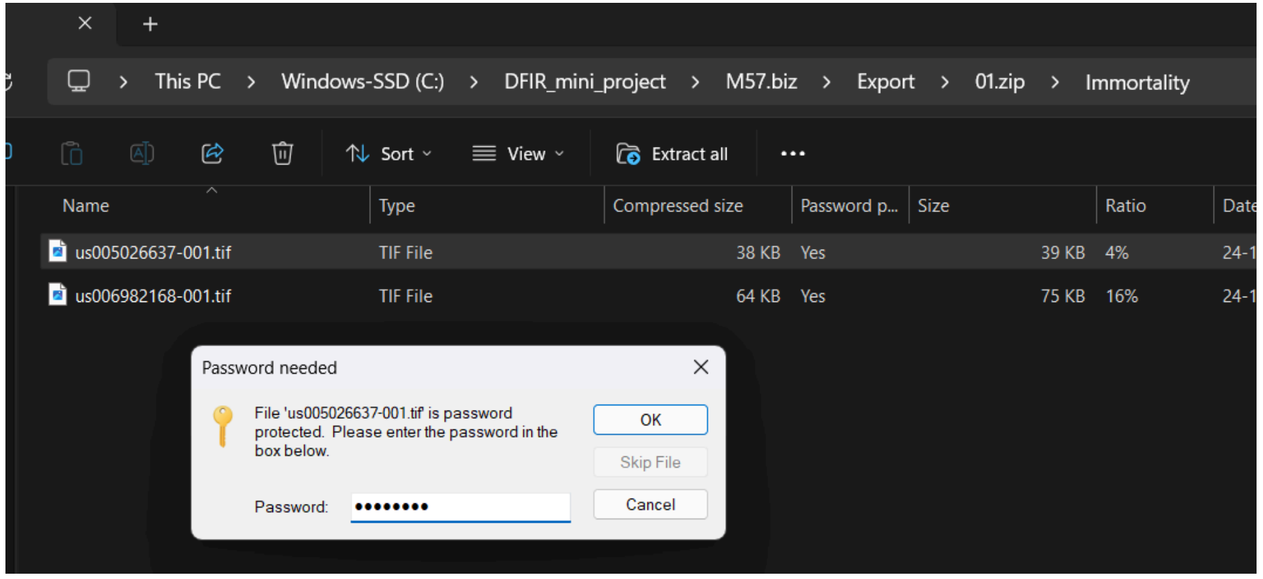
Evidence Sources

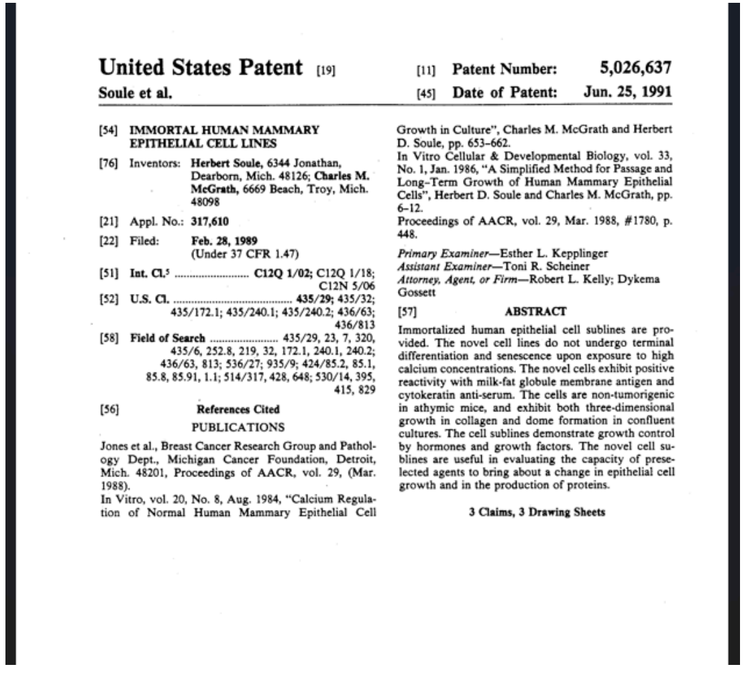
- Workstation Disk Image (~10GB)
- USB Drive Image (~2GB)
- User Data Files (~4GB)
- Secondary Workstation (~1GB)
- Email Corpus (~3GB)
- Total Evidence Analyzed: ~20GB

Email & User Activity Analysis



Steganography & Hex Analysis





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

Tools Used

- Autopsy – Disk & artifact analysis
- HxD – Hexadecimal file inspection
- Invisible Secrets – Hidden data extraction
- SHA-256 Hashing – Integrity verification

Findings & Conclusion

- Demonstrated practical application of digital forensics and incident response in a simulated breach.
- Digital evidence was securely acquired, preserved, and analysed with maintained integrity.
- Identified concealed information hidden within ordinary files and communications.
- Extracted hidden data from image files and uncovered concealed passwords through hex analysis.
- Detected file manipulation using integrity verification techniques.
- Reconstructed the sequence of events by correlating technical artifacts with email evidence.
- Highlighted the importance of strong forensic capabilities to prevent data exfiltration and intellectual property loss.

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