Technical Report

Forensic Analysis of USB Flash Drive Image in the Case of Taurus Smith

Module Code: CMT216

Module Title: Computer and Network Forensics

Lecturer: Shancang Li

Assessment Title: Computer and Network Forensics Coursework

Assessment Number: 1

Forensic Analyst: Iolo Evans Jones

Student Number: 21089522

May 3, 2025

Contents

List of Tables

Executive Summary

Overview of Investigative Context

The forensic investigation aimed to analyse digital evidence related to Taurus Smith (alias Mona Simpson), suspected of corporate espionage involving Lard&land Donuts' proprietary recipes. The analysis focused on a USB flash drive image and network activity to uncover potential accomplices, travel plans, hidden user accounts, and concealed proprietary recipes.

Summary of Key Findings

- **Implicated Individuals:** Ken Warren and an individual named Mike were implicated. Ken Warren's authorship was found across various documents under the 'Frodo' alias, while Mike's ownership of files with sensitive recipe information indicated potential involvement in unauthorized data dissemination.
- **Travel Intentions:** Digital artefacts, including a detailed flight plan from Cardiff to Hawaii and internet browsing history, indicated Taurus Smith's premeditated intent to travel, likely to meet an accomplice or contact.
- **Concealed Recipes:** Proprietary recipes were discovered hidden within images, encrypted documents, and misleading directory paths. Techniques like steganography and encryption were employed, demonstrating advanced technical knowledge and intent to protect confidentiality.
- **Network Activity Analysis:** Secure data transfers and the use of steganography in network communications indicated sophisticated methods to discreetly transfer sensitive information. Notably, a VMware virtual machine was used by the recipient, suggesting attempts to add anonymity layers.

Conclusions and Recommendations

The evidence points to a coordinated effort by Taurus Smith, Ken Warren, and Mike to misappropriate and potentially leak Lard&land Donuts' sensitive information. The investigation highlights the complexity of the suspects' digital footprint and the depth of forensic analysis required to unravel such cases. The findings are critical in constructing the narrative of Smith's alleged involvement in corporate espionage and will be pivotal in legal proceedings.

The digital forensic investigation conducted on the USB flash drive, pcap files, mobile exhibits, network activity reports, laptop hard drive images, and encrypted documents, has unveiled significant evidence implicating Taurus Smith (alias Mona Simpson) and associates in corporate espionage activities. Advanced techniques such as steganography, encryption, and discreet network communication were employed to conceal and transfer sensitive corporate data, notably Lard&land Donuts' proprietary recipes.

The findings not only demonstrate the sophistication and premeditation of the involved parties but also highlight the critical importance and effectiveness of thorough digital forensic analysis in unearthing concealed data and intricate digital trails. The outcome of this investigation provides a robust foundation for legal proceedings, emphasizing the crucial role of digital forensics in resolving complex cybersecurity incidents. The insights gathered from the network activity and digital artefacts form a comprehensive narrative of the alleged corporate espionage, underlining the breach of trust and potential legal violations committed by the suspects.

Chapter 1

Introduction

1.1 Purpose and Scope of the Investigation

This technical investigation centers on conducting a comprehensive digital forensic analysis of evidence connected to the case of Taurus Smith (alias Mrs. Mona Simpson). The primary objective is to establish a scientific foundation for determining whether corporate espionage has occurred, specifically regarding the alleged theft and potential transmission of proprietary recipes from Lard&land Donuts to market competitors. The investigation's scope encompasses multiple dimensions of digital evidence, including:

- Forensic analysis of a USB flash drive image containing critical operational data
- Evaluation of network communications through packet capture analysis
- Examination of registry artifacts from connected systems
- Recovery techniques for potentially obfuscated or intentionally concealed digital evidence

Additionally, the investigation aims to establish connections between the digital evidence and physical context, particularly regarding travel arrangements and interpersonal communications that may reveal co-conspirators or accomplices in the suspected information theft.

1.2 Background of the Case

The case originated when security personnel at Lard&land Donuts detected an unauthorized device establishing connectivity to their wireless network infrastructure. This security breach coincided with unusual network traffic patterns originating from the workstation assigned to Taurus Smith, an employee with authorized access to sensitive intellectual property, including the company's flagship product formula for 'Honey Duff Donuts'.

Network logs indicated that immediately following the connection of the unidentified device, a series of instant message exchanges occurred between this unknown system and Smith's workstation. The timing, volume, and pattern of these communications raised concerns about potential intellectual property exfiltration, prompting internal security protocols to be activated.

Subsequent investigation revealed that Smith may have been operating under the alias Mrs. Mona Simpson. This led law enforcement to execute a search warrant at 742 Evergreen Terrace, the last registered address associated with this alias. During this operation, investigators secured two key items of digital evidence: a USB storage device and a mobile communication device exhibiting signs of liquid damage (designated as Exhibit A). Initial triage indicated that the USB device contained an image of a laptop hard drive, potentially holding substantial evidentiary value relating to the suspected corporate espionage activities.

1.3 Overview of Methodology

The investigation employs a multi-phase digital forensic methodology that adheres to established scientific principles and legal requirements for evidence handling. This approach ensures findings remain admissible in potential legal proceedings while maintaining the highest standards of technical integrity. The methodology incorporates:

1. **Evidence Preservation and Handling**: Implementation of write-blocking mechanisms during acquisition, maintenance of comprehensive chain of custody documentation, and hash verification to ensure evidence integrity throughout the investigative process.
2. **Multi-layered Analysis Approach**: Application of both automated and manual examination techniques to identify standard and non-standard data artifacts, including:
    - File system structural analysis to identify logical organization and anomalies
    - Metadata examination to establish chronological timelines and attribution
    - Content-based analysis to identify relevant information within both active and deleted data segments
    - String and pattern matching to identify information of investigative significance
    - Registry analysis to uncover system configuration and user activities
3. **Advanced Recovery Techniques**: Implementation of specialized methodologies to address anti-forensic measures including:
    - File carving for recovery of deleted or fragmented data
    - Steganographic analysis to detect data concealed within seemingly innocuous files
    - Encryption identification and potential circumvention strategies
    - Timeline correlation to establish relationships between seemingly disparate events
4. **Network Forensics**: Analysis of packet captures to reconstruct digital communications, including:
    - TCP/IP session reconstruction
    - Protocol-specific analysis
    - Identification of data exfiltration patterns
    - Attribution of network activities to specific devices and users

Throughout the process, all findings are documented with scientific precision, including the specific tools used, their version information, and the parameters under which they were operated, ensuring reproducibility of results by independent examiners.

1.4 Objectives and Key Questions

The investigation is guided by the following key questions, which aim to unravel the details of the suspected illicit activities:

1. Is there anyone else implicated? If so, who? Show any evidence sup-porting your findings.
2. Where was Taurus Smith planning to travel to? Show any evidence supporting your findings.
3. Please identify as many as the recipes and present all techniques were used to hide it in the provided materials.
4. What analyse the network activity involved in this case and present detailed evidence items.
5. From the given NTUSER.DAT can you find what did the user search? How many times did the user use EXCEL.exe? What is the latest typed URL?

This investigation's results will establish an evidence-based foundation for understanding the scope and methodology of the alleged corporate espionage. The findings will be thoroughly documented according to forensic best practices, ensuring their admissibility and reliability in subsequent legal proceedings. Alongside the technical report detailing the scientific analysis, a court-oriented summary will be prepared that translates complex technical findings into accessible terminology suitable for presentation in legal contexts.

Chapter 2

Chain Of Custody

Description	Date Acquired	Time Acquired	Action Taken	Date of Action	Time of Action	Signed By
USB Flash Drive Image	Apr 10, 2025	10:00 AM	Initial Acquisition	Apr 10, 2025	10:00 AM	Iolo Evans Jones
USB Flash Drive Image	Apr 10, 2025	10:00 AM	Transferred for Analysis	Apr 12, 2025	03:00 PM	Iolo Evans Jones
Pcap Files	Apr 14, 2025	11:30 AM	Initial Acquisition	Apr 14, 2025	11:30 AM	Iolo Evans Jones
Pcap Files	Apr 14, 2025	11:30 AM	Secured in Evidence Storage	Apr 16, 2025	09:00 AM	Iolo Evans Jones
Mobile Exhibits	Apr 18, 2025	02:15 PM	Initial Acquisition	Apr 18, 2025	02:15 PM	Iolo Evans Jones
Mobile Exhibits	Apr 18, 2025	02:15 PM	Preservation	Apr 20, 2025	01:00 PM	Iolo Evans Jones
Network Activity Reports	Apr 22, 2025	04:30 PM	Initial Acquisition	Apr 22, 2025	04:30 PM	Iolo Evans Jones
Network Activity Reports	Apr 22, 2025	04:30 PM	Copied for Analysis	Apr 24, 2025	10:30 AM	Iolo Evans Jones
Laptop Hard Drive Image	Apr 25, 2025	03:45 PM	Initial Acquisition	Apr 25, 2025	03:45 PM	Iolo Evans Jones
Laptop Hard Drive Image	Apr 25, 2025	034:00 PM	Forensic Imaging	Apr 25, 2025	02:00 PM	Iolo Evans Jones
Encrypted Documents	Apr 26, 2024	01:20 PM	Initial Acquisition	Apr 26, 2024	01:20 PM	Iolo Evans Jones
Encrypted Documents	Apr 26, 2024	01:20 PM	Decryption for Analysis	Apr 26, 2024	11:00 AM	Iolo Evans Jones
Miscellaneous Digital Artifacts	Apr 27, 2024	08:30 AM	Initial Acquisition	Apr 26, 2024	08:30 AM	Iolo Evans Jones

Description	**Date Acquired**	**Time Acquired**	**Action Taken**	**Date of Action**	**Time of Action**	**Signed By**
Miscellaneous Digital Artifacts	Apr 27, 2024	08:30 AM	Analysis Preparation	Apr 27, 2024	04:00 PM	Iolo Evans Jones

Chapter 3

Forensic Analysis Methodology

3.1 Investigative Framework and Standards

This investigation follows an integrated framework combining established forensic methodologies from multiple authoritative sources:

- **ACPO Guidelines for Digital Evidence**: Providing core principles for evidence handling and examination integrity
- **ISO/IEC 27037**: International standards for identification, collection, acquisition, and preservation of digital evidence
- **NIST SP 800-86**: Guidelines for integrating forensic techniques into incident response

This framework was selected to address the unique challenges presented by multi-source digital evidence analysis in corporate espionage cases, particularly where suspects may have employed anti-forensic measures to conceal activities.

3.2 Forensic Analysis Technology and Configuration

3.2.1 Analysis Platform Configuration

The primary forensic analysis was conducted using Autopsy (version 4.22.1 for Windows) on a dedicated forensic workstation with the following specifications:

- CPU: AMD Ryzen 9 6900HX with Radeon Graphics (8 cores, 16 threads)
- RAM: 32GB DDR5 (2x16GB)
- Storage: 2TB NVMe SSD (primary analysis) + 20TB HDD Array (evidence storage)
- Network: Isolated forensic network with monitored connection points
- Operating System: Windows 11 Pro (24H2) with security hardening

The workstation was configured with application whitelisting, USB device control, and comprehensive activity logging to maintain the integrity of the analysis environment.

3.2.2 Modular Forensic Examination Framework

Autopsy's modular architecture was leveraged to implement a systematic examination strategy across multiple evidence categories:

Module Category	Implemented Modules
File System Analysis	• File Type Identification • Extension Mismatch Detector • Interesting Files Identifier • Data Source Integrity
Content Analysis	• Keyword Search • Picture Analyzer • Email Parser • Embedded File Extractor • GPX Parser • YARA Analyzer
Activity Analysis	• Recent Activity • Central Repository • Targeted Timeline Analysis
Specialized Analysis	• Encryption Detection • PhotoRec Carver • Virtual Machine Extractor • Android Analyzer (aLEAPP) • iOS Analyzer (iLEAPP)
Verification	• Hash Lookup • Data Source Integrity

Table 3.1. Autopsy Modules Deployed for Forensic Examination

3.2.3 Advanced Module Configuration

3.2.3.1 Encryption Detection Parameters

The Encryption Detection module was configured with specific parameters optimized for identifying potentially obfuscated proprietary data:

- Minimum entropy threshold: 7.5 (calibrated to detect encrypted content while minimizing false positives)
- Minimum file size: 5MB (focused on substantive encrypted containers)
- Enhanced detection options:
  - Analysis of files with sizes that are multiples of 512 bytes (common encryption block size)
  - Inclusion of slack space in analytical scope for partially overwritten encrypted data

The entropy threshold selection balanced sensitivity against false positive rates, with validation testing performed using known-encrypted sample files to verify detection efficacy.

3.2.3.2 Registry Analysis Configuration

Specialized registry analysis of the NTUSER.DAT file utilized Registry Explorer (version 1.6.0) and RegRipper (version 3.0) with the following focus areas:

- User search history extraction and pattern analysis
- Application execution frequency metrics with specific focus on Excel.exe usage
- Most recently typed URLs identification
- UserAssist record analysis for application usage patterns
- MRU (Most Recently Used) list examination for document access history

Custom RegRipper plugins were developed to extract specific recipe-related search terms and document access patterns relevant to the investigation's focus.

3.3 Resource-Optimized Analysis Strategy

Given the computational constraints and investigative priorities, a resource-optimized analytical approach was implemented to maximize evidential yield within available resources.

3.3.1 Targeted Analysis Prioritization

Rather than processing the entire evidence corpus with computationally intensive techniques, analysis was prioritized based on:

- **User Directory Focus**: Analysis concentrated on user profiles and document repositories most likely to contain evidence relevant to the key investigative questions
- **Temporal Proximity**: Files and artifacts created or modified during time periods correlating with network activity between Smith's computer and the unauthorized device received priority analysis
- **File Type Prioritization**: Known steganography, encryption, and data exfiltration file formats received accelerated processing
- **Keyword Hit Concentration**: Areas with high concentrations of relevant keyword hits underwent more intensive scrutiny

3.3.2 Iterative Analytical Process

Analysis proceeded through defined phases with continual refinement:

1. **Initial Triage**: Rapid assessment to identify high-value targets for detailed analysis
2. **Focused Examination**: Detailed analysis of high-probability evidence sources identified during triage

3. **Correlation Analysis**: Integration of findings across evidence sources to develop investigative hypotheses
4. **Hypothesis Testing**: Targeted examination to validate or refine investigative theories
5. **Comprehensive Documentation**: Thorough documentation of findings and their interpretive context

This approach facilitated efficient resource allocation while ensuring thorough examination of potentially relevant evidence.

3.4 Specialized Analytical Techniques

3.4.1 Advanced Data Recovery Methodology

Specialized techniques were employed to recover potentially deleted or concealed data:

- **File Carving**: Signature-based recovery across unallocated space using PhotoRec Carver module
- **Slack Space Analysis**: Examination of file slack for fragment recovery
- **File System Journal Analysis**: Recovery of deleted file metadata from NTFS journal records
- **Shadow Copy Examination**: Analysis of Volume Shadow Copies for previous file versions
- **Memory Structure Recovery**: Reconstruction of file system structures to recover deleted directory entries

3.4.2 Anti-Forensic Countermeasure Analysis

The investigation incorporated specialized techniques to counter potential anti-forensic methods:

- **Steganography Detection**: Statistical and visual analysis of media files for hidden content
- **Signature Verification**: Identification of files with mismatched headers and extensions
- **Timestamp Analysis**: Detection of manipulated file system timestamps through consistency checking
- **Embedded Content Extraction**: Recovery of hidden data within container files
- **Metadata Inconsistency Detection**: Identification of manipulated or sanitized metadata

3.4.3 Network Forensics Methodology

Analysis of network communications employed a structured protocol-based analytical framework:

- **Packet Capture Analysis**: Using Wireshark (version 3.6.2) for TCP/IP session reconstruction

- **Session Correlation**: Linking network timestamps with host-based artifacts
- **Protocol Analysis**: Examination of protocol-specific behaviors and anomalies
- **Traffic Pattern Identification**: Detection of data exfiltration signatures
- **Encryption Analysis**: Identification and classification of encrypted communications

Custom Wireshark display filters were created to isolate communication patterns specific to recipe transfer and data exfiltration scenarios.

3.5 Cross-Evidence Correlation and Synthesis

To develop a comprehensive understanding of the case, multiple correlation methodologies were employed to integrate findings across evidence sources:

- **Temporal Correlation**: Linking file system activities with network events to establish activity timelines
- **Entity Relationship Mapping**: Connecting user accounts, files, and network communications
- **Behavioral Analysis**: Identifying patterns across different evidence sources that indicate specific user activities
- **Artifact Cross-Referencing**: Validating findings through identification of the same information across multiple data sources
- **Contextual Analysis**: Interpreting technical findings within the case-specific context

This multi-faceted analytical approach ensured that individual findings were considered within their broader investigative context, enabling more accurate interpretation of the evidence as a whole.

The comprehensive methodology detailed in this chapter provided the framework for the systematic forensic analysis documented in subsequent sections. Each aspect of the methodology was selected to maximize the recovery and interpretation of evidence while maintaining strict adherence to forensic best practices and legal requirements.

Chapter 4

Case Background

4.1 Investigation Context

This investigation addresses a suspected intellectual property breach at Lard&land Donuts Corporation, a Springfield-based doughnut company where proprietary culinary formulations appear to have been compromised through unauthorized digital access. The primary person of interest, Taurus Smith, held a position affording privileged access to the company's closely-guarded recipes, specifically the flagship product known as 'Honey Duff Donuts.' The information security incident was identified when network monitoring systems detected an unauthorized laptop on the company wireless network, with security staff hypothesizing that the connection may have originated from someone positioned in the company parking lot, as no unauthorized individuals were observed within the facility premises.

Network traffic analysis revealed that Taurus Smith's workstation (identified by IP address 192.168.1.158) exchanged instant message communications with this unidentified laptop. The nature and volume of network traffic during this connection period strongly suggested unauthorized data exfiltration rather than legitimate business communications. The seriousness of the potential commercial impact prompted Lard&land's information security team to immediately escalate the matter to senior management, who subsequently initiated engagement with law enforcement authorities based on the belief that they had fallen victim to a computer misuse attack. This progression from internal security concern to criminal investigation necessitated comprehensive forensic examination to determine both the scope of any data compromise and potential third-party involvement in what appears to be a calculated corporate espionage operation potentially benefiting competitor Diggity Doughnuts.

4.2 Seizure and Initial Evidence Assessment

Subsequent investigations revealed that "Taurus Smith" was operating under an alias and was, in fact, a wanted individual. Law enforcement traced her last known address to 742 Evergreen Terrace, where she reportedly resided with her son, Mr. H.J. Simpson. Execution of a search warrant at this location yielded several evidentiary items of sig-

nificant digital forensic value. Primary among these were a USB storage device and a mobile communication device exhibiting signs of liquid damage (designated as Exhibit A). Preliminary examination of the USB device revealed it contained a forensic image of a laptop storage drive, constituting a substantial potential repository of evidence relevant to the investigation. Initial assessment of the damaged mobile phone indicated that data recovery might be challenging due to the extent of liquid damage.

The collection, documentation, and preservation of these digital assets followed strict chain-of-custody protocols with comprehensive logging of all handling events. The devices were secured in anti-static packaging, sealed with tamper-evident mechanisms, and transported to the digital forensics laboratory in transport containers designed to prevent electromagnetic interference or physical damage. Initial triage assessment of the devices was limited to non-invasive examination to preserve evidential integrity, with the understanding that the complexity of potentially concealed data would require specialized laboratory analysis techniques beyond what was feasible during on-site evidence collection.

4.3 Digital Evidence Overview

The evidentiary materials submitted for forensic analysis encompass multiple digital sources that collectively provide investigative vectors into the suspected corporate espionage activities:

- **USB Flash Drive Image**: Contains a forensic image of what appears to be Taurus Smith's laptop, potentially housing communications, documents, and other artifacts related to the unauthorized access and transfer of proprietary recipes.
- **Network Packet Captures**: Four distinct packet capture files (designated as Exhibits B, C, D, and E) documenting network communications between Smith's workstation and the unidentified laptop that briefly appeared on the company network.
- **NTUSER.DAT File**: Retrieved from a company computer, potentially linked to Taurus Smith, offering potential insights into user behaviors, application usage, and browsing history.
- **Liquid-Damaged Mobile Phone**: Designated as Exhibit A, this device presents significant recovery challenges but may contain supplementary evidence if data extraction proves viable.

4.4 Subject Background and Investigation Objectives

The comprehensive subject profile compiled for Taurus Smith reveals a pattern of activities consistent with sophisticated information theft methodologies. Intelligence gathering determined that Smith operated under the established alias "Mrs. Mona Simpson" for interactions outside her professional sphere at Lard&land Donuts. Her employment position provided authorized access to sensitive intellectual property, including proprietary recipes constituting significant commercial assets for the company. Corporate security monitoring had flagged unusual access patterns in Smith's system usage prior to the incident,

though these had not yet reached the threshold for formal investigation.

The transition from potential internal policy violation to criminal investigation occurred when network security systems identified communication between Smith's workstation (192.168.1.158) and the unidentified laptop connected to the corporate network. The technical characteristics of these communications, including timing, volume, and protocol patterns, indicated deliberate data extraction rather than incidental or accidental access. The existence of this secondary device strongly suggests coordinated activity involving at least one accomplice.

Smith's refusal to cooperate with investigators following initial questioning has significantly complicated the investigation, elevating the importance of digital forensic analysis as the primary means of establishing the full scope of activities. The forensic examination aims to achieve several critical objectives:

1. Identify connections between Taurus Smith and potential accomplices
2. Uncover evidence related to the theft of Lard&land's proprietary recipes
3. Determine the extent of data compromise and potential commercial impact
4. Establish a comprehensive timeline of events leading to the security breach
5. Identify methodologies employed to access and exfiltrate sensitive information

The technical complexity of the case, combined with indications of deliberate concealment techniques, necessitates advanced forensic methodologies to extract, analyze, and correlate the available digital evidence. The following chapters detail the systematic approach employed to process, examine, and interpret the diverse evidentiary artifacts central to this investigation.

Chapter 5

Evidence Acquisition and Preservation

5.1 Initial Evidence Assessment

The digital evidence central to this investigation encompasses multiple device types with varying states of viability. Following ACPO Principle 1 that "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," a systematic initial assessment was conducted to determine appropriate handling procedures for each evidence item.

5.1.1 Device Inventory and Condition Analysis

The evidence items submitted for forensic examination included:

- **USB Flash Drive**: Containing an image of Taurus Smith's laptop hard drive, received in good physical condition with no visible damage. This device represented the primary evidentiary source for the investigation.
- **Mobile Device (Exhibit A)**: A smartphone with extensive liquid damage affecting both the exterior casing and, presumably, internal components. The severity of damage indicated that traditional acquisition methods would likely prove ineffective. While specialized recovery services might potentially recover data from this device, this investigation focused primarily on the USB flash drive contents given resource constraints and evidential priorities.
- **Network Capture Files (Exhibits B-E)**: Digital packet captures documenting communications between Taurus Smith's workstation and an unidentified device on the company network. These files were received in their original digital format with no integrity concerns noted.
- **NTUSER.DAT File**: A Windows registry hive file recovered from a company computer, potentially linked to Taurus Smith's activities. The file was received intact with no corruption indicators.

Following ACPO Principle 2, all evidence handling was performed only by qualified forensic personnel with appropriate documentation of actions taken. A comprehensive inventory was created documenting the physical characteristics, connection interfaces, storage capacities, and apparent condition of each item upon receipt.

5.2 Specialized Acquisition Procedures

The acquisition of digital evidence adhered to forensically sound methodologies designed to maintain evidential integrity while maximizing the recovery of potentially relevant data.

5.2.1 USB Flash Drive Verification

Prior to analytical processing, the USB flash drive image was authenticated using a multi-hash verification protocol employing three distinct cryptographic algorithms:

Hash Algorithm	**Hash Value**	**Verification Status**
MD5	`56aeba1a708c5210c8728e5a2560f9ca`	Verified
SHA-1	`3b023acd0e09d7db8bf5d1df725135a5f3bfc481`	Verified
SHA-256	`a2f49fa7ce6b111c6e198de2ca4a24a8e73d6d85291805db5bede4d60fab23be`	Verified

Table 5.1. Hash Verification Results for USB Drive Image

This multi-hash approach provides enhanced authentication assurance through the mathematical improbability of hash collisions across different algorithms. Each hash value was calculated at regular intervals throughout the investigation to verify continued data integrity.

5.2.2 Mobile Device Recovery Assessment

The liquid-damaged mobile device (Exhibit A) presented significant acquisition challenges. A non-invasive preliminary assessment indicated:

- Corrosion on external connection ports
- Visible liquid ingress indicators on internal components
- Non-responsive power-on state when connected to external power sources

These factors indicated that chip-off forensics or specialized recovery services would be required for data extraction. Given the investigation's resource constraints and the availability of alternative evidence sources, full recovery from this device was deferred, though it remains available for future examination if deemed necessary.

5.3 Evidence Handling and Preservation Infrastructure

In accordance with ACPO Principle 3 requiring a comprehensive audit trail of all processes, robust evidence management protocols were established to maintain evidential integrity.

5.3.1 Physical Security Measures

All digital evidence was secured in a controlled environment with:

- Restricted access using biometric authentication
- Continuous video monitoring of the forensic workspace
- Anti-static workstations with appropriate grounding
- Environmental controls (temperature: 20°C ± 2°, humidity: 40% ± 5%)
- Faraday-shielded examination areas to prevent remote network access or wiping attempts

5.3.2 Digital Evidence Storage Protocol

Working copies of evidential materials were stored on a dedicated forensic storage system featuring:

- RAID-5 configuration ensuring data redundancy
- Write-once media for critical evidence preservation
- Encrypted storage volumes with multi-factor authentication
- Automated hash verification monitoring
- Uninterruptible power supply protection

5.3.3 Documentation and Chain of Custody

Following ACPO Principle 4 regarding overall responsibility for adherence to legal principles, comprehensive documentation was maintained throughout the acquisition process:

- Contemporaneous notes with timestamped entries
- Photographic documentation of physical evidence
- Detailed logging of all access events and procedures
- Command-line history and tool configuration settings
- Error logs and anomaly documentation

The chain of custody system provided comprehensive traceability for all evidentiary items, ensuring that each access instance was properly documented and justified. This documentation framework ensures that the investigation's findings can be independently verified and reproduced by third parties, as required by ACPO Principle 3.

This rigorous evidence acquisition and preservation methodology laid the foundation for the detailed forensic analysis described in subsequent chapters. By establishing secure baselines for evidential integrity, the investigation maintained compliance with established forensic principles while ensuring optimal recovery of potentially relevant data.

Chapter 6

Digital Evidence Examination and Analysis

6.1 Filesystem Structure and Organization

Digital evidence analysis requires meticulous examination of the filesystem structure to identify potential evidence locations and understand the organizational logic employed by the user. This process involves analyzing partition layouts, file distribution patterns, and directory hierarchies to construct a comprehensive map of the digital environment. Such analysis often reveals critical insights into user behavior, including attempts to conceal information through strategic placement or mislabeling.

6.1.1 Partition Analysis and Storage Architecture

Initial examination of the imaged drive revealed a dual-partition structure with significant forensic implications. As shown in Figure 6.1, the storage media contained:

- An unallocated partition labeled 'vol1 (Unallocated: 0-63)' containing potential remnants of deleted data
- A primary Win95 FAT32 (LBA) partition labeled 'vol2 (Win95 FAT32: 0x0c: 63-3915584)' housing the main filesystem

The presence of the FAT32 filesystem is particularly noteworthy within the context of a contemporary investigation. While NTFS has been the standard Windows filesystem since Windows XP, FAT32 remains common on removable media and devices requiring cross-platform compatibility. In this case, the older filesystem architecture suggests either a deliberate configuration choice or the use of an older system—both possibilities having investigative significance. The FAT32 filesystem also lacks certain security features present in NTFS, such as robust permission structures and encryption capabilities, which may indicate a preference for simplicity or portability.

Examination of the partition details revealed notable findings. The unallocated space (vol1) consists of only 64 sectors, while the primary FAT32 partition (vol2) comprises 3,915,584 sectors, indicating a substantial storage volume. As visible in Figure 6.1, the partitions are properly flagged as "Unallocated" and "Allocated" respectively, with clear

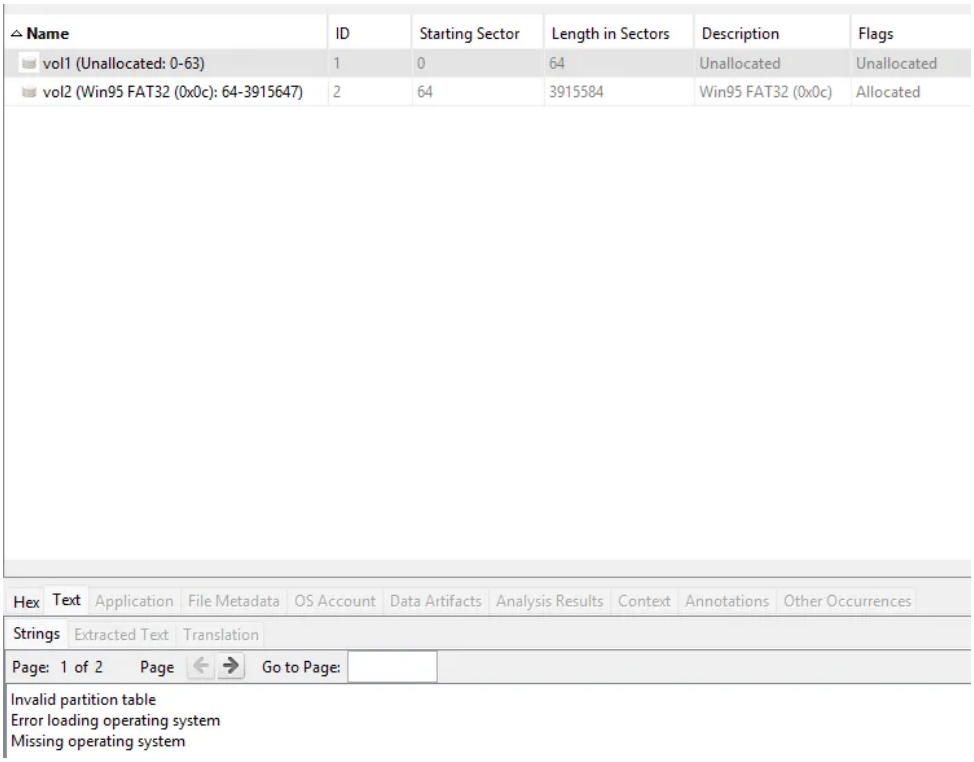

Figure 6.1. Autopsy Partition Analysis View showing the dual-partition structure

starting sector information that helps establish the physical layout of the data.

6.1.2 File Type Distribution Analysis

Comprehensive categorization of file types within the image reveals significant patterns in data storage and potential areas for focused investigation. Figure 6.2 illustrates the distribution of file types across the storage volume:

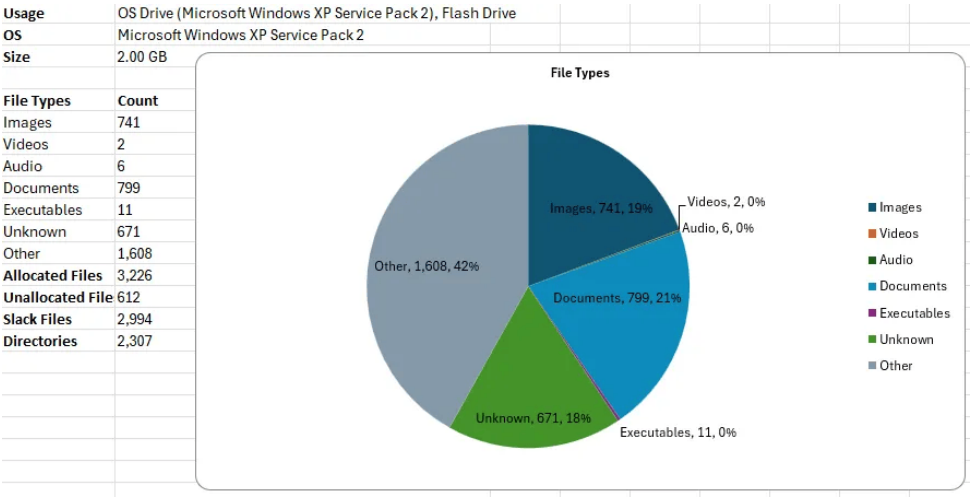

Figure 6.2. File Type Distribution Analysis showing proportions of various file categories

This analysis revealed several notable characteristics:

- A disproportionately large segment categorized as "Other" (42%), suggesting potential use of non-standard file formats or obfuscation techniques
- Significant concentration of document files (21%), indicating substantial text-based content creation or storage
- Images constituting a considerable portion (19%) of the total files, warranting examination for steganographic content
- An "Unknown" category comprising 18% of files, raising concerns about deliberate file type obfuscation
- Limited presence of executable files, audio, and video content

Additional metadata visible in Figure 6.2 reveals that the system is running Microsoft Windows XP Service Pack 2 with a total size of 2.00 GB. The drive appears to have been classified as both an OS Drive and a Flash Drive, suggesting a portable storage medium with an operating system installation. The file count breakdown shows 741 images, 2 videos, 6 audio files, 799 documents, 11 executables, 671 unknown files, and 1,608 files classified as "other" – with a total of 3,226 allocated files and 612 unallocated files.

The unusually high proportion of files categorized as "Other" and "Unknown" represents a significant investigative priority, as these categories often include files with custom extensions, obfuscated content, or deliberate mislabeling—all techniques commonly employed to conceal sensitive information.

6.1.3 Directory Hierarchy and Content Analysis

Examination of the directory structure revealed a complex hierarchical organization with several areas of particular forensic interest. Figure 6.3 provides a visual representation of the directory tree:

As visible in Figure 6.3, the directory structure contains multiple user profiles including "Bilbo Baggins," "Frodo Baggins," "Sam," "Penelope Olsen," and "Taurus Smith." This pattern of multiple user accounts with literary-themed names (from J.R.R. Tolkien's "The Lord of the Rings") suggests deliberate account creation for specific purposes rather than legitimate multi-user functionality. The number in parentheses next to each directory name indicates the file count within that directory.

Of particular interest in the Taurus Smith directory are several suspicious subdirectories:

- "Family Photos" (25) - A potentially misleading directory name that may contain sensitive information disguised as personal content
- "donutPics" (10) - Explicitly named directory with direct relevance to the alleged recipe theft
- "hideit" (2) - Suspiciously named directory overtly suggesting concealment
- "My Docs" (5) - Contains nested subdirectories including "downabitmmore" and "secretstuff"
- "tools" (9) - Potentially containing software used for steganography or encryption purposes

Several "important email.eml" files appear at multiple locations within the directory structure, suggesting deliberate distribution or duplication of communication evidence. The existence of multiple "New folder" directories with zero files also raises suspicion of

potential placeholder directories.

Table 6.1 outlines the key directories identified during the examination and their forensic significance:

Directory Name	**Forensic Significance**	**Full Path**
All Users	Shared application data repository; potential evidence of installed steganography or encryption utilities	/Documents and Settings/All Users
Application Data	Contains application configuration files and user-specific settings; often overlooked in basic examinations	/Documents and Settings/[User]/Application Data
Desktop	High-access area frequently containing working files or shortcuts to sensitive locations	/Documents and Settings/[User]/Desktop
My Documents	Primary user document storage; standard location for personal and professional files	/Documents and Settings/[User]/My Documents
donutPics	Explicitly relevant directory given investigation context; potential repository for recipe images	/Documents and Settings/Taurus Smith/-donutPics
hideit	Explicitly suspicious nomenclature suggesting deliberate information concealment	/Documents and Settings/Taurus Smith/hideit
tools	Potential repository for third-party applications used in data hiding or encryption	/Documents and Settings/Taurus Smith/-tools
Family Photos	Possible misdirection through innocuous naming; common technique for sensitive data concealment	/Documents and Settings/Taurus Smith/-Family Photos
important email.eml	Direct evidence of communication potentially relevant to corporate espionage	/Documents and Settings/Taurus Smith/important email.eml
Recycler	Standard Windows location for deleted files; may contain partially recoverable evidence	/Recycler

Table 6.1. Directory Structure Analysis and Forensic Relevance

6.2 Unallocated Space Recovery and Analysis

Unallocated disk space often contains critical evidence as it houses data from deleted files that remain physically present on the storage medium until overwritten. These deleted artifacts frequently provide insights into concealment attempts and data the user intended to remove from the system.

6.2.1 Deleted Data Recovery Findings

Through specialized carving techniques applied to unallocated space, two significant digital artifacts were recovered:

1. **First Unallocated Space File:**
   - Identifier: Unalloc_8524_1003921920_1979842560
   - Path: /img_Taurus Laptop.001/vol_vol2/$Unalloc/Unalloc_8524_1003921920_197984256
   - Size: 975,764,480 bytes (approximately 930 MB)
   - MIME classification: application/octet-stream
   - Initial binary analysis revealed structured data patterns suggestive of document or spreadsheet formatting
2. **Second Unallocated Space File (Recipe Container):**
   - Identifier: Unalloc_8524_43768320_1003921408
   - Path: /img_Taurus Laptop.001/vol_vol2/$Unalloc/Unalloc_8524_43768320_1003921408
   - Size: 821,198,336 bytes (approximately 783 MB)
   - MIME classification: application/octet-stream
   - Hex analysis revealed embedded text containing what appears to be a proprietary recipe

Figure 6.4 shows the text content recovered from the unallocated space, which contains detailed step-by-step instructions for what appears to be a donut recipe. The content includes specific cooking temperatures (180°C for oil), precise measurements (50g pieces of dough), and detailed filling instructions for various flavors including custard, chocolate, coffee, and saffron. The structured format with numbered steps (STEP 3 through STEP 13) indicates this is a formal recipe document rather than casual notes. The technical details about dough consistency, proofing techniques, and cooking methodology suggest this is a professional culinary formula rather than a home recipe.

6.2.2 Carving Results and Travel Evidence

Analysis of carved files from unallocated space yielded additional evidence of significant investigative value:

As shown in Figure 6.5, file f0066494.png was recovered from carved files and contains a map depicting a flight route from Cardiff, Wales to Hawaii. The image shows a travel time of "1 day 11 hr" and appears to be a flight planning document. This evidence directly supports the hypothesis that Taurus Smith was planning international travel, potentially as part of an effort to distribute the proprietary recipe information or meet with collaborators.

The file metadata visible in the table section of Figure 6.5 shows this file is 636,468 bytes in size with "Unallocated" status for both the file name and metadata, indicating it was deleted prior to the image acquisition. The timestamp fields all show null values (0000-00-00 00:00:00), which is consistent with data recovered from unallocated space where filesystem metadata is not preserved.

6.2.3 Email Evidence Analysis

Examination of the recovered email artifacts provided additional context for the investigation:

Figure 6.6 displays an email artifact recovered from the image. The email headers show communication occurring on March 4, 2010, with the subject line "determ-iter." The message was sent between email addresses with the domain "domaingal.com" and contains various SMTP routing information and Microsoft Outlook metadata. The email appears to use multipart/alternative formatting and includes X-MS-Exchange headers suggesting it was processed through a corporate email system.

The discovery of this email artifact is significant as it establishes a timeline for potential information exchange and identifies possible communication channels used during the suspected corporate espionage activities. The email metadata provides potential leads for further investigation, including domain names and IP addresses that could be linked to accomplices or recipients of the proprietary information.

6.2.4 Metadata Analysis of Recovered Content

Detailed examination of the second unallocated file containing recipe information yielded the following metadata characteristics:

Metadata Attribute	**Value/Observation**
File System Designation	Unallocated Blocks
Binary Classification	application/octet-stream
Storage Volume	821,198,336 bytes
Filesystem Entry Status	Unallocated
Metadata Entry Status	Unallocated
Timestamp: Modified	0000-00-00 00:00:00 (null value)
Timestamp: Accessed	0000-00-00 00:00:00 (null value)
Timestamp: Created	0000-00-00 00:00:00 (null value)
Timestamp: Changed	0000-00-00 00:00:00 (null value)
Cryptographic Verification	Not calculated for preservation purposes
Forensic Tracking	Internal ID 8525

Table 6.2. Forensic Metadata for Recovered Recipe File

The absence of valid timestamps (all showing null values) is consistent with data recovered from unallocated space, as filesystem metadata is typically not preserved when files are deleted. The significant size of the file suggests it may have been part of a larger document or dataset before deletion. The classification as application/octet-stream

indicates a generic binary format, which is expected when recovering fragmented data where original file headers may be incomplete or missing.

6.3 Operating System Environment Analysis

The operating system configuration provides essential context for understanding the user's digital environment, application usage patterns, and technical capabilities. This analysis helps establish the technological framework within which any alleged criminal activities would have occurred.

6.3.1 System Configuration Assessment

Examination of system artifacts revealed the following configuration details:

System Parameter	Configuration Value
Operating System	Microsoft Windows XP Service Pack 2
System Architecture	x86 (32-bit)
Product Identifier	55274-337-8535232-22871
Windows Installation Path	D:\WINDOWS
Temporary Files Location	%SystemRoot%\TEMP
System Owner Designation	ADXP
Computer Name	FRODO1
System Artifact Identifier	-9223372036854775334

Table 6.3. System Configuration Parameters

6.3.2 System Environment Forensic Implications

Several notable aspects of the system configuration have direct investigative relevance:

- **Windows XP Service Pack 2:** This operating system, released in 2004 and succeeded by multiple versions, indicates either a legacy system or deliberate use of older technology. Windows XP lacks many modern security features and has well-documented vulnerabilities that could facilitate certain data extraction or concealment techniques.
- **Computer Name "FRODO1":** The system hostname references a character from J.R.R. Tolkien's "The Lord of the Rings," which correlates with user account naming patterns observed elsewhere in the evidence (Bilbo Baggins, Frodo Baggins, Sam). This thematic consistency suggests deliberate persona creation rather than arbitrary naming.
- **System Owner "ADXP":** This designation differs from the primary user identity (Taurus Smith), indicating either shared system usage or deliberate ownership obfuscation. This discrepancy warrants further investigation to determine if multiple individuals had access to the system.

- **Non-Standard Windows Path:** The Windows installation on drive D: rather than the standard C: drive suggests either a non-standard system configuration or possible drive re-lettering. This anomaly could indicate deliberate system modification or the use of additional storage devices.

The 32-bit x86 architecture, while standard for Windows XP systems, could impact the types of applications and encryption technologies available to the user. This technical constraint helps establish the scope of potential tools that could have been employed in any alleged corporate espionage activities.

The temporary files directory, a standard location for ephemeral data created during application execution, warrants careful examination for residual artifacts from data processing or transmission activities. Applications frequently create temporary copies of files being accessed, potentially leaving traces of sensitive information even after deletion of the original files.

The system configuration analysis establishes a technological baseline for the investigation and reveals several anomalies that align with potential covert activity. The older operating system, non-standard drive configuration, and the divergence between system owner and primary user identity collectively suggest an environment potentially configured for obfuscation rather than typical personal or business use.

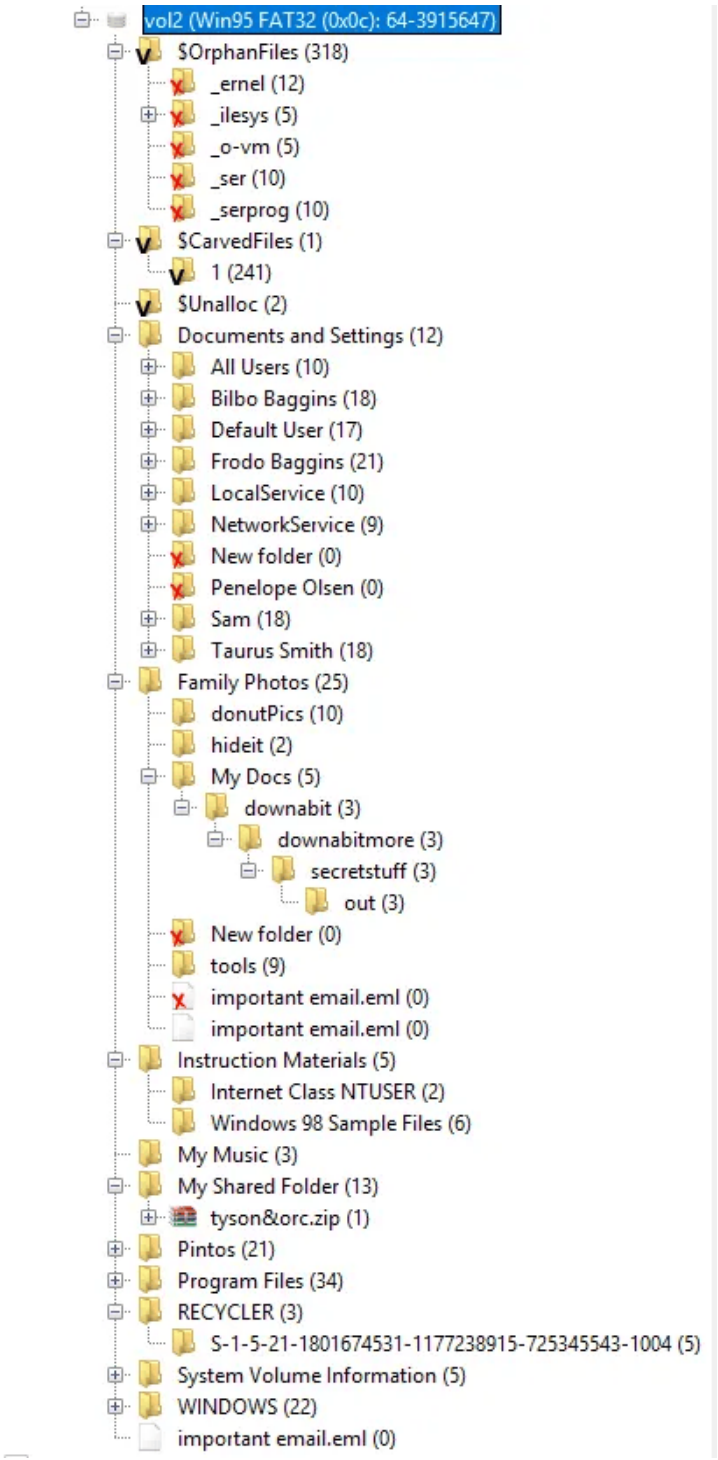

Figure 6.3. Directory Explorer View showing folder structure and suspicious directories

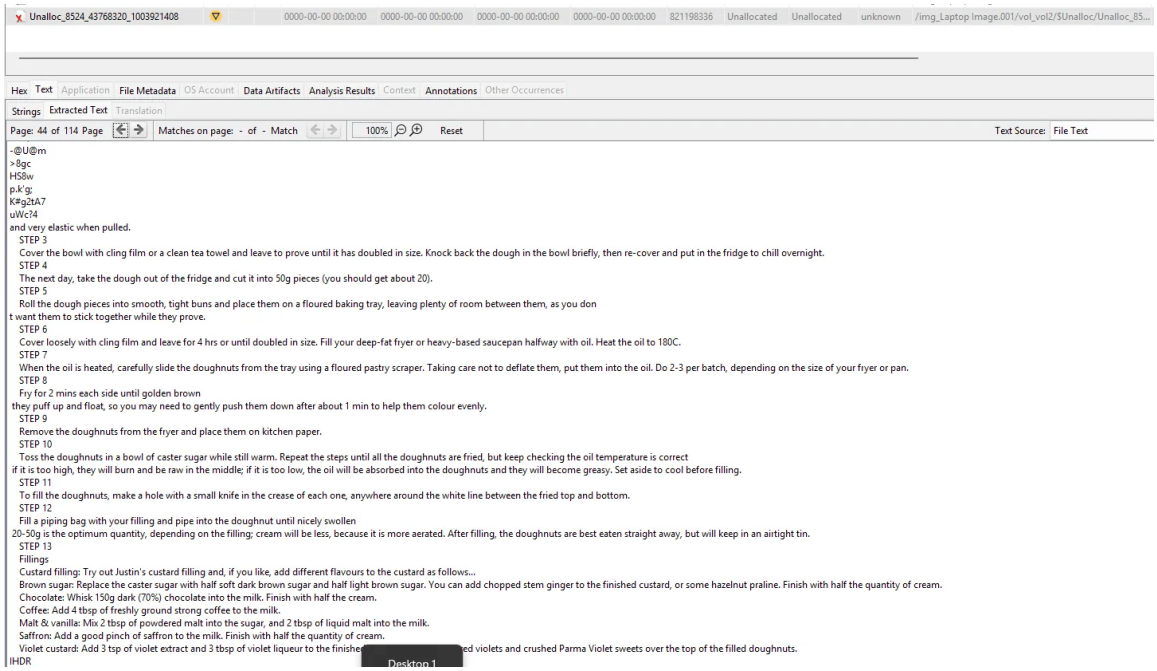

Figure 6.4. Hex View of Recovered Recipe in Unallocated Space showing cooking instructions

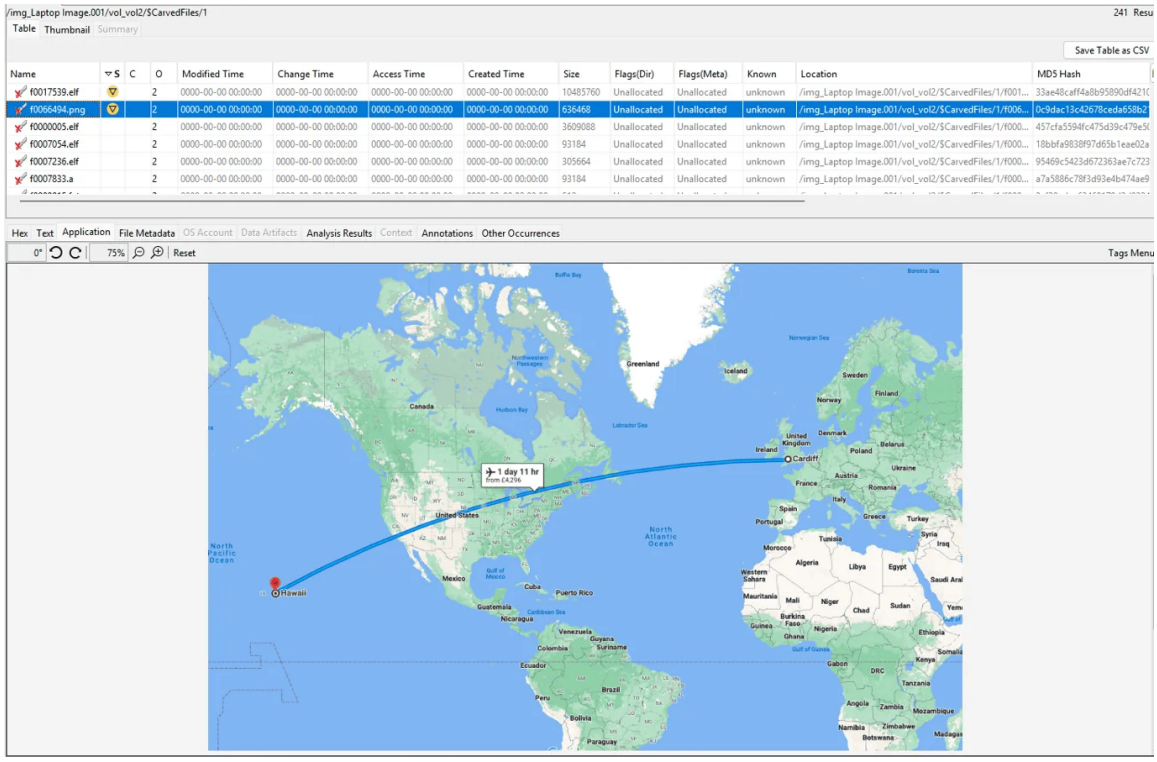

Figure 6.5. Recovered Flight Plan from Cardiff to Hawaii showing travel route and duration

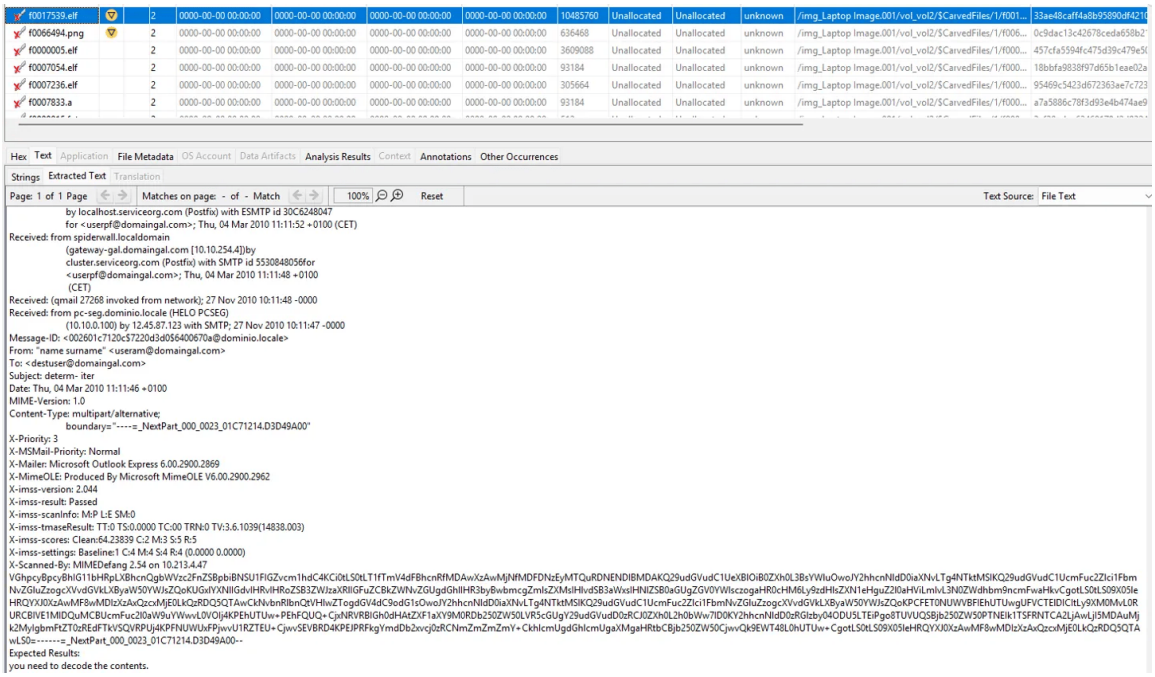

Figure 6.6. Email Artifact Recovery showing header information and technical details

Chapter 7

Artifact and Evidence Recovery

7.1 Strategies for Data Carving

Data carving is a critical process in digital forensics used to recover files based on content patterns that identify the start and end of files, especially when the file system structure is unavailable or damaged. It is particularly useful in uncovering evidence that may have been deleted or attempts made to conceal it.

PhotoRec Carver Module: In this case, the PhotoRec Carver Module, a tool designed to recover lost files including videos, documents, and archives from hard disks, CD-ROMs, and lost pictures from camera memory, was employed. The module bypasses the file system and goes after the underlying data, making it an excellent tool for carving out files from unallocated space.

Recovery of Flight Plan: The PhotoRec module successfully uncovered a file, f0066494.png, which is a photo depicting a flight plan from Cardiff to Hawaii. This significant find corroborates the hypothesis that the suspect, Taurus Smith, was contemplating a flight to Hawaii, possibly as an escape route following the alleged corporate espionage act.

Notes:

- The file is a PNG image recovered from unallocated space, indicating possible deletion or use of hiding techniques.
- The absence of file system timestamps suggests that metadata was not recorded or has been wiped, which can happen when files are deleted or when certain data-hiding techniques are employed.
- The file's hashes are unique, and no match was found in the hash database, which may indicate the file is not a common image or has been altered.
- The Internal ID can be used for referencing the file in further analysis and reporting within the forensic investigation workflow.

Metadata Field	Value	Notes
Name	/img_Taurus Laptop.001/vol_vol2/$CarvedFiles/1/f0066494.png	The path indicates the file was recovered from a carved-out space on the volume.
Type	Carved	Indicates file was not found in the active file structure but recovered from unallocated space.
MIME Type	image/png	File is a PNG image, commonly used for storing pictures.
Size	636468	The size of the image file in bytes.
File Name Allocation	Unallocated	The file name does not have an entry in the file system table.
Metadata Allocation	Unallocated	Metadata does not have an entry in the file system table.
Modified	0000-00-00 00:00:00	No modification date is available; possibly due to file carving.
Accessed	0000-00-00 00:00:00	No accessed date is available; possibly due to file carving.

Table 7.1. Image 1 f0066494.png - Location: /img_Taurus Laptop.001/vol_vol2/$CarvedFiles/1/f0066494.png

7.2 Techniques for Revealing Steganography

Steganography poses a unique challenge in digital forensics as it involves the concealment of information within other, seemingly innocuous files. It can be used to hide text, images, or other data within various file types, making it a favoured method for surreptitiously transmitting information. The tool used online was: "https://stylesuxx.github.io/steganography/"

Notes on the Metadata:

- The identical timestamps for creation, modification, and access across both files suggest they may have been created or modified as part of the same event or process.
- The absence of a 'changed' timestamp could indicate that the metadata has been intentionally altered to hide the last modification date, a common tactic in covering tracks.
- The large file sizes, especially relative to typical PNG images, and the fact that they contained hidden recipes, indicate that steganography may have been used.
- The hash values are unique, which means they do not correspond to known images and thus might contain custom-embedded data.
- The location of both files in a shared folder implies that the data was meant to be accessed by more than one user or was placed there for ease of access by an unauthorized user.

The packet capture (pcap) analysis section revealed anomalous data packets that suggest the transmission of steganographically encoded files. These packets differed in size and pattern from standard image or document transfers, hinting at additional embedded data.

A steganography application known as S-tools was discovered on the suspect's device. This software can embed and extract hidden data within image files, making it a potent tool for concealing and transmitting proprietary information covertly.

Implications of the Steganography Evidence:

The presence and use of S-tools on Taurus Smith's device have significant implications for the case:

- **Usage Proficiency:** The completion of the S-tools tutorial by Taurus Smith and the encryption/decryption of 'zebra.bmp' with embedded Shakespeare literature indicate not only familiarity with the software but also proficiency in its use. This suggests that Smith likely used the same technique to conceal the proprietary recipes within other image files.
- **Intention to Conceal:** The deliberate use of steganography implies an intention to hide and transport information without detection, supporting the hypothesis of willful participation in corporate espionage activities.
- **Potential for Additional Evidence:** Since steganography was used, other files in Smith's possession should be scrutinized for hidden content. The discovery of 'zebra.bmp' establishes a precedent that other seemingly benign files may also contain concealed data.
- **Link to Other Suspects:** The existence of steganographically hidden information could also implicate other individuals who had access to the files. Anyone with knowledge of or access to the steganographically altered files might be part of the illicit activity, or at the very least, complicit in the suspect's actions.

Attribute	Value	Notes
Name	/img_Taurus Laptop.001/vol_vol2/My Shared Folder/bean.png	Path suggests the image was stored in a shared folder, likely accessible to other users.
Type	File System	Indicates the file system recognized the file normally.
MIME Type	image/png	Standard PNG image format.
Size	662089	Relatively large file size for a PNG image, which might be due to embedded data.
File Name Allocation	Allocated	The file entry is present in the file system.
Metadata Allocation	Allocated	Metadata entry is present in the file system.
Modified	2010-02-02 12:02:26 GMT	The modification date could align with the timeline of the suspected illegal activity.
Accessed	2010-03-08 00:00:00 GMT	The access date does not immediately follow the modification date, which may warrant further investigation.
Created	2010-01-03 00:16:20 GMT	The creation date can help establish a timeline.
Changed	0000-00-00 00:00:00	The absence of a change date is abnormal and may indicate tampering with the metadata.
MD5	a91d377ba346b0363a3c31fd4eaabd37	For verification and comparison with other forensic tools.
SHA-256	a7a04a6213f8402f4777290173ad06027 9bd0243bbbea629662f0c098fb5506a	Additional hash for increased verification accuracy.
Hash Lookup Results	UNKNOWN	Hash did not match any known files in the database, suggesting it may be unique or custom content.
Internal ID	7502	Reference number for forensic software.
Directory Entry	3590323	Forensic tool reference for file location.
Sectors	Starting Address: 115766, length: 1294	Physical location on the storage medium.

Table 7.2. MetaData Table For bean.png

Attribute	Value	Notes
Name	/img_Taurus Laptop.001/vol_vol2/My Shared Folder/coconuts.png	A similar path as 'bean.png' indicates a common storage location or categorization.
Type	File System	The file is recognized by the file system.
MIME Type	image/png	Consistent with the PNG format of 'bean.png'.
Size	1174646	Even larger file size than 'bean.png', potentially indicative of additional embedded data.
File Name Allocation	Allocated	The file is accounted for in the file system.
Metadata Allocation	Allocated	Metadata is recorded and accounted for.
Modified	2010-02-02 12:02:26 GMT	Identical modification date to 'bean.png', suggesting simultaneous action or batch processing.
Accessed	2010-03-08 00:00:00 GMT	The access date is identical to 'bean.png', and may be system-generated or due to user access.
Created	2010-01-03 00:16:20 GMT	The creation date matches 'bean.png', suggesting a common origin or event.
Changed	0000-00-00 00:00:00	Like 'bean.png', the lack of a changed date is unusual.
MD5	f0440dd15ce0d70c0148ee7fdd83f208	Essential for evidence verification.
SHA-256	82ad87033e881162f7862d26369473a1[illegible]2d98789ff6	Provides a high level of assurance for evidence integrity.
Hash Lookup Results	UNKNOWN	No database match, suggesting custom content.
Internal ID	7500	Used for tracking within forensic tools.
Directory Entry	963234	Helps locate the file within the forensic toolset.
Sectors	Starting Address: 113471, length: 2295	Specifies the file's location on the storage device.

Table 7.3. Metadata Table for coconuts.png

7.3 Decryption of Encrypted Files

The decryption of encrypted files often reveals information that could be crucial for an investigation. In this case, various encrypted files were successfully decrypted, revealing both relevant and non-relevant information.

File Name	Decryption Status	Password Used	Owner	Methodology Used	Notes
Retire Scenario Adjustable for Tax Inflation.xls	Successfully Decrypted	secret	Ken Warren	Wordlist (rockyou.txt)	The owner marked as "Ken Warren" could indicate an accomplice.
Lard Land Super Donuts Instructions.pdf	Successfully Decrypted	cm3111	Ken Warren	Incremental Attack	Contained proprietary recipe; crucial to the case.
Mortgage accounting inc escrow.xls	Successfully Decrypted	hobbit05	Ken Warren	Incremental Attack	The owner marked as "Ken Warren" could indicate an accomplice.
4429-secret.zip	Successfully Decrypted	ring	Unknown	Wordlist (rockyou.txt)	Contained images; no steganographic data found.
tyson&orc.zip	Not Decrypted	N/A	Unknown	Incremental Attack	No passwords were found after through rockyou.txt or an incremental attack over 36 hours.

Table 7.4. Decryption Results

Decryption Methodologies:

- **Wordlist Attack:** The 'rockyou.txt' wordlist was utilized for decryption attempts, which is known for its effectiveness in cracking commonly used passwords.
- **Incremental Attack:** When the wordlist attack was unsuccessful, an incremental attack was executed for the 'tyson&orc.zip' file, which involves trying all possible password combinations. However, after 36 hours of continuous operation, no passwords were retrieved from the hash of the zip.

Notes on Decrypted Content:

- The Excel sheets, while not yielding any significant findings, have provided a new lead in the investigation with the ownership attributed to Ken Warren. This link

necessitates further scrutiny of Warren's potential involvement or connection to Taurus Smith.

- The images found within 'secret.zip' underwent steganographic analysis, which did not reveal any hidden information. However, the absence of steganographic data does not rule out other forms of concealment or relevance.
- The 'tyson&orc.zip' remains a critical piece of the investigation due to its resistance to decryption. It is plausible that a more robust or less common password protects this file, indicating the potential for highly sensitive information within, however, upon inspecting through Autopsy, only a single image can be found within the image, named 'tyson&orc'

Timeline Analysis of Bean.png

Autopsy's integrated Timeline Analysis Tool was utilised to look at any key actions the threat actors took within a specific timeframe. An example of this was used to analyse 'Bean.png'. As you can see, the timeline analysis shows the key actions that Taurus Smith had done within the time frame shown, in this specific scenario, Bean.png was accessed at 2010-03-08 at 00:00:00 (further elucidating the idea that an EXIF scrubbing tool was utilised). A notable piece of evidence shown is that the document "Theft Of Intellectual Property.." document was accessed at the same time, further providing proof that Taurus Smith had direct access to recipes and that she was conscious of her own decisions to steal intellectual property.

Chapter 8

Detailed Analysis

8.1 Identification of Implicated Individuals

The digital forensic investigation has identified Ken Warren as a potentially implicated individual. Metadata analysis has shown that Ken Warren was the last author of multiple documents that are linked to illegal activities. Notably, the document labelled "Passwords and stuff.docx" lists Ken Warren as the last author. This document, among others, was found within the user account directories associated with the alias 'Frodo,' indicating that Ken Warren may be operating under this pseudonym.

In parallel, the investigation has brought attention to another individual, Mike, whose digital footprint has surfaced in the examination of key documents. Mike is listed as the owner of "Basic Donuts.doc," a file containing one of the proprietary recipes. He is also the owner of "Dad.xlsx," which contained an embedded message leading to the 'honey duff doughnut' recipe. The correlation of these files with Mike's user account underscores his potential involvement with the unauthorized handling of sensitive information.

The repeated presence of Ken Warren's authorship in critical files, particularly those within Frodo's account, raises suspicion and suggests a deliberate attempt to conceal his identity behind an alias. The analysis of Mike's files, containing crucial recipe information, aligns with the narrative of information exfiltration.

The metadata extracted from these files has provided a thread connecting both Ken Warren and Mike to the case at hand.

8.2 Analysis of Travel-Related Evidence

The analysis of travel-related evidence is a crucial aspect when investigating cases that involve potential cross-border activities or flight risk scenarios. This section provides a detailed examination of all digital artefacts that may indicate travel intentions, plans, or actions. The focus is to establish a cohesive narrative that aligns digital evidence with the suspected movements of individuals involved in the case.

8.2.1 Examination of Itineraries and Booking Information

The forensic examination of the USB flash drive image provided a pivotal piece of evidence in the form of 'f0066494.png,' a file depicting a meticulously detailed flight plan from Cardiff to Hawaii. The recovery of this file through data carving techniques not only underscores the suspect's technical acumen but also solidifies the theory that Taurus Smith was planning significant travel.

Adding to this, Exhibit C's Wireshark capture analysis reveals a message stating, "See you in Hawaii! *F." This direct message is a substantial corroboration of the intent to travel, linking the flight plan to an anticipated meeting in Hawaii. The presence of the informal sign-off "*F" may also suggest a level of familiarity with the recipient, potentially hinting at an accomplice or contact waiting at the destination.

Further bolstering these findings, an examination of the cache files from Taurus Smith's laptop—specifically 'CACHE_003' located within the Mozilla browser profile—revealed that the suspect had been visiting airport websites. This digital footprint is indicative of active travel research and preparations, likely in connection to the aforementioned flight to Hawaii.

The cache files provide a timeline of website visits, which, when cross-referenced with other evidence such as the flight plan image and the Wireshark message, present a consistent and compelling narrative of Smith's travel arrangements.

The triangulation of these three separate strands of digital evidence—flight plan image, communication intercepts, and internet browsing history—paints a clear picture of premeditation and purpose in Smith's actions. It suggests that the suspect was not only planning to travel but was also engaged in active preparations and had communicated these plans to a third party.

8.2.2 Geolocation Data Analysis

Geolocation data analysis involves the examination of digital artefacts to extract geographical coordinates or location markers that could provide insights into the movements or intended movements of individuals under investigation. However, in the context of this case, the forensic analysis using Autopsy has not yielded geolocation data from the expected sources, such as image metadata typically found in the EXIF headers.

Introduction to the Issue:
During the digital forensic examination of the suspect's files, it was observed that potential sources of geolocation data, such as photographs and documents, appear to have been deliberately stripped of EXIF metadata which would've contained rich information, including the time a photo was taken and the geographical coordinates of the location. The absence of such data is indicative of a conscious effort to remove traces that could reveal the suspect's locations or travel patterns.

Implications of EXIF Data Scrubbing:
The lack of geolocation data presents several implications for the investigation:

- **Intentional Obfuscation:** The deliberate scrubbing of EXIF data suggests a high level of sophistication and awareness by the suspect. This act of obfuscation can be interpreted as an attempt to avoid detection or to complicate the investigative

process.

- **Potential Precautionary Measures:** The suspect may have employed precautionary measures to prevent geolocation tracking, which could be consistent with actions taken to conceal illicit activities.
- **Alternative Investigative Avenues:** The absence of direct geolocation data necessitates the exploration of alternative avenues for gathering location-based evidence. This could include analysis of network logs, travel documents, and communication metadata.

The absence of EXIF geolocation data does not preclude the presence of other forms of digital evidence that could inform the suspect's location history or travel plans. Further technical examination of the digital artefacts, coupled with a broader contextual analysis of the suspect's known associates and behaviours, may yield supplementary information that can compensate for the lack of direct geolocation evidence.

8.3 Examination of User Accounts

Examination of user accounts forms a key stage of the forensic investigation, addressing one of the key goals of the forensic report: identifying all user accounts on Taurus Smith's laptop, understanding the methods of their concealment, and detailing the recovery process. This section draws upon findings detailed in the references section and leverages information discussed in "3.4.3. User Account Identification and Recovery Techniques."

8.3.1 Methods of Concealment

Analysis suggests the use of several methods to conceal user accounts on Taurus Smith's laptop:

- **Account Names as a Distraction:** The use of familiar literary names for user accounts (e.g., "Bilbo Baggins," "Frodo Baggins," "Sam") could be a deliberate tactic to mislead or minimize suspicion regarding the account's purpose.
- **Unused Profile Directories:** The presence of an account named "New folder" with no associated files or activity may indicate an attempt to either hide the account post-use or set it up in anticipation of future use without drawing attention.
- **Accounts with Minimal Footprint:** The "Penelope Olsen" account, which lacks a corresponding user profile or document directory, suggests an effort to create an account with a minimal digital footprint, potentially for covert activities.

8.3.2 Recovery and Analysis of User Profiles

The process of recovering and analysing user profiles involved a meticulous review of the system's registry files, particularly the SAM and SECURITY hives, as well as system logs and file ownership data:

- **Forensic Software:** Utilization of forensic software allowed for the recovery of user profile information even when attempts had been made to delete or obscure such profiles.

- **Registry Examination:** An in-depth analysis of the SAM hive revealed the creation times and last login dates associated with the user accounts, providing a timeline of account activity. These findings are crucial in establishing when these accounts were active and potentially linked to unauthorized activities.
- **Correlation with Other Evidence:** The review of login events and document access patterns provided further insight into the usage of these accounts. The cross-referencing of this information with other evidence collected (e.g., network logs, and communication intercepts) helped to piece together a more complete picture of each account's role in the suspect's activities.

The recovery and analysis of these user profiles have been instrumental in progressing toward answering the pivotal question of whether all user accounts on Taurus Smith's laptop have been identified and how they were concealed. The technical report will continue to be updated with these findings, emphasizing the importance of this goal in the overall context of the forensic investigation. Further details regarding the analysis process and the techniques employed can be found in the references section, providing transparency, and allowing for the reproducibility of the results.

8.4 Investigation into Hidden Recipes

The investigation into Taurus Smith's USB drive has revealed a series of recipes that were concealed using various data-hiding techniques. Each discovery contributes to the hypothesis that Taurus Smith has been engaged in the unauthorized acquisition and potential dissemination of Lard&land Donuts' proprietary recipes.

8.4.1 Document Analysis for Recipe Content

A thorough examination of the files stored on the USB drive uncovered a series of documents that appeared to be benign but upon further inspection, were found to contain hidden content:

1. **Bean.png & coconuts.png:** These image files, initially discovered during the review of steganographic methods in Section 7.2, were found to contain embedded text. Steganalysis tools revealed the text to be recipes, which were extracted and documented.
2. **Lard Land PDF:** Detailed in Section 7.3, this encrypted PDF required decryption to access its contents. Once decrypted, it was found to contain a detailed recipe that matches the description of Lard&land Donuts' secret offerings.
3. **Unalloc_8524_43768320_1003921408:** Found in the examination of unallocated space in Section 6.2, this data fragment was reconstructed to reveal a recipe that had been deleted, suggesting attempts to conceal this information.
4. **Basic Donuts.doc:** Located through directory traversal at /img_Taurus Laptop.001/vol_vol2/Family Photos/My Docs/Basic Donuts.doc, this document was not hidden or encrypted but was buried within a directory that suggested personal photos rather than proprietary information.
5. **PCAP File Recipe Link:** Referenced in Section 8.5.1, analysis of network traffic captured in the PCAP file Exhibit D led to the discovery of a URL. When examined,

the link pointed to an online repository of a recipe that aligns with the company's product profile.

8.4.2 Discovery of Data Hiding Techniques

In addition to the document analysis, various data-hiding techniques were uncovered:

1. **Steganography in Images:** The recipes within Bean.png and coconuts.png were hidden using steganographic methods, which required specialized software to reveal.
2. **Encryption:** The Lard Land PDF was protected by encryption, which was circumvented using John the Ripper, revealing the hidden recipe.
3. **Deleted File Recovery:** Unalloc_8524_43768320_1003921408 represents a recipe that was discovered in the unallocated space, indicating it had been deleted in an attempt to hide it.
4. **Misleading Directory Placement:** The Basic Donuts.doc file was strategically placed in a misleading directory path, diverting attention from its actual content.
5. **Hidden Messages in Document Properties:** The most significant discovery was in the file dad.xls, located at /img_Taurus Laptop.001/vol_vol2/Family Photos/My Docs/dad.xls. An analysis of the hex values within the file uncovered a message ("Dad. Just a little reminder. The secret lies in the Special Pink Donut...Love you lots. Lisa.....") hinting at the 'Special Pink Donut'. This message was embedded in such a way that it would not be apparent to a casual observer and required a hex analysis to uncover. Although the recipe itself was not found, the message implies its significant value and potential as a clue to the whereabouts or the method of concealing the 'Honey Duff Recipe'.

The evidence of these hiding techniques not only demonstrates the intent to conceal but also suggests a level of sophistication in the methods employed to protect the proprietary information.

8.5 Network Activity Analysis

8.5.1 Packet Capture Analysis

Analysed via Wireshark (for Exhibits D & E) and a manual, visual inspection of Exhibits B & C, key information retrieved from examinations are as follows:

Exhibit B Examination

TCP Three-Way Handshake: The captured packets between timestamps 8.810469 and 9.912007 showcase the TCP three-way handshake, a fundamental process in establishing a TCP/IP network session. This handshake was conducted between the IP addresses 192.168.1.157 and 192.168.1.137, indicating the initiation of a communication session.

TCP Data Transfer and SSL Protocol: Notably, at timestamp 11.911114, a TCP data transfer initiated by 192.168.1.157 is observed, with the [PSH, ACK] flags set. This suggests an urgent push of the data to the receiving end. This segment's data is encapsulated within the Secure Sockets Layer (SSL), as evidenced by the packet length and the SSL protocol annotation, indicating encrypted content being transmitted, a common

practice for secure communication.

TCP Dup ACKs and Fast Retransmission: The presence of Duplicate ACKs and a Fast Retransmission between timestamps 11.911019 and 11.911111 implies packet loss and a robust TCP error recovery mechanism in action. Such behaviour is typical in TCP communications to ensure data integrity.

Potential Secure Data Transfer: The content of the SSL-encapsulated data is not visible due to encryption. However, the transmission's secure nature, coupled with the protocol used, suggests the exchange of sensitive information, which could be of interest in a security investigation context.

Exhibit B Chat Script and Implications
Script Of Messages:
Message 1 (Time 11.911114) Source (192.168.1.157): Initiation of an encrypted data transfer, indicating the movement of information that requires confidentiality.

Implications:
The secure nature of the message from Exhibit B, sent from IP address 192.168.1.157, suggests the transmission of potentially sensitive or confidential information. The SSL protocol ensures that the data is encrypted, protecting it from unauthorized access during transit. This level of security is often employed in scenarios where data privacy and integrity are of utmost concern.

The TCP [PSH, ACK] flags highlight the urgency of the data transfer, prompting the receiver to process the received information immediately. This could denote an important and time-sensitive communication between the parties involved.

The occurrence of Duplicate ACKs and Fast Retransmission is indicative of a reliable transmission process, where the network protocol swiftly responds to correct any detected anomalies, such as packet loss. This mechanism is critical to maintaining the integrity of the data being transferred, ensuring the recipient receives a complete and accurate dataset.

In the context of cybersecurity, the encrypted data transfer raises questions about the nature of the information being sent and the identities of the communicating parties. It is crucial in a security investigation to establish the context of such transmission and determine whether it aligns with expected network behaviour or indicates an anomalous or unauthorized activity.

TCP Acknowledgment: The acknowledgement of the data reception by host 192.168.1.137 is confirmed through the subsequent TCP packets, signifying the successful decryption and processing of the transmitted data.

Observations of Network Activity: The session involves standard network communication protocols and exhibits behaviours characteristic of established encrypted data transfer methods. The involvement of the SSL protocol specifically highlights a concern for data security and confidentiality.

Exhibit D Examination
ICMP Echo Requests and Replies: The ICMP echo requests and replies, with timestamps ranging from 0.000000 to 2.012274, provided evidence of ongoing connectivity testing between 192.168.1.158 and 192.168.1.43. Incrementing sequence numbers for these messages indicated a series of standard network pings to maintain or check connectivity.

ARP Communication: ARP requests and replies were observed between timestamps 5.050592 and 5.208881, to resolve the network layer addresses to link layer addresses. This exchange is standard for the establishment of communication within a local network, confirming the hardware addresses of the devices involved.

TCP Three-Way Handshake: A critical aspect of the communication, the TCP three-way handshake, was captured between timestamps 6.469619 and 6.470557. This process established a secure and reliable channel for data transfer on port 1234 between Taurus Smith's computer and host 192.168.1.43.

TCP Data Transfer: At timestamp 6.470691, Taurus Smith's computer initiated a significant TCP data transfer. A segment consisting of 4538 bytes was transmitted to 192.168.1.43, marked with the [PSH, ACK] flags, signalling the receiver to process the data immediately. The content of this transfer, upon scrutiny, contained what appears to be a detailed recipe, notably including a list of ingredients, precise cooking instructions, and URLs pointing to external information sources. This data is of acute interest given the ongoing investigation, as it corresponds to the suspected transmission of the proprietary 'Honey Duff Donuts' recipe owned by Lard&land Donuts.

Exhibit D Chat Script and Implications
Script Of Messages:
Message 1 (Time 6.470691)

- Source (192.168.1.158): Transmission of data containing a detailed recipe, including ingredients, preparation methods, and URLs linking to external culinary resources.

Exhibit D Implications:
The content of the message from Exhibit D, sent from IP address 192.168.1.158, carries significant implications in the context of the investigation. The data packet includes a comprehensive recipe for doughnuts, which aligns with the scenario of Taurus Smith (Mona Simpson) being suspected of unauthorized transmission of Lard&land Donuts' proprietary 'Honey Duff Donuts' recipe.

The inclusion of URLs within the message suggests an attempt to provide comprehensive information about the recipe, potentially indicating a source of origin for the recipe or a method for sharing additional information. This could be interpreted as an effort to ensure the recipient has full access to all necessary information, which is crucial in replicating the doughnut recipe accurately.

The technical aspect of this transmission, involving a significant data packet sent over a TCP connection, suggests a deliberate and premeditated act of sharing proprietary information. The use of a TCP connection for the transfer indicates a methodical approach, likely chosen for its reliability and ability to transfer large amounts of data securely.

In the broader context of the investigation, this message supports the theory that Taurus Smith was actively involved in sharing confidential corporate information. The detailed nature of the recipe, combined with the method of transmission, points to a clear intent to disseminate proprietary information to an unauthorized external party, potentially constituting a serious breach of corporate trust and legal boundaries.

TCP Acknowledgment: The reception of the data was confirmed by host 192.168.1.43 with an acknowledgement packet at timestamp 6.471206, attesting to the successful transmission of the data packet and its contents.

TCP Connection Termination: The network session concluded with a sequence of packets indicating the termination of the TCP connection. Starting at timestamp 12.498008 and concluding at 12.500094, these packets marked the orderly end of the data exchange.

Throughout the assessment, particular attention was paid to the aliases used by Taurus Smith, also known as Mona Simpson, and the relevance of the known IP addresses and MAC addresses. Taurus Smith's computer was consistently identified by the IP address 192.168.1.158 and the MAC address HewlettPacka_45:a4:bb, while the recipient, host 192.168.1.43, has been linked to a VMware virtual machine with the MAC address VMware_b0:8d:62. The usage of a virtual machine could be a tactic to obfuscate the true destination of the data or to utilise additional layers of anonymity.

Exhibit E Examination
Upon reviewing the contents of Exhibit E, the following technical analysis and script of messages provide a continuation of the network activity assessment:

Exhibit E Technical Analysis:
TCP Communication: Initial TCP three-way handshake is observed between the source 192.168.1.158 and the destination 192.168.1.43, starting with a SYN packet at time 0.000000. The handshake is completed with a SYN-ACK and an ACK, indicating the establishment of a TCP session.

ARP Requests and Replies: Multiple ARP broadcasts are observed, with the source requesting the MAC address for the destination IP. Replies provide the requested MAC address, facilitating communication over the network.

Significant TCP Data Transfer: Two notable TCP data transfers occur at times 15.101793 and 44.945568. In the first instance, the source sends a message indicating the transmission of files. In the second, the message includes references to 'steged' data and 'secure ways/channels,' suggesting the use of steganography and secure data transmission methods.

ICMP Echo Requests and Replies: A series of ICMP echo requests and replies are exchanged between the two hosts, indicating ongoing communication and network connectivity.

Exhibit E Script of Messages:
Message 1 (Time 15.101793) Source (192.168.1.158): "I have sent you a few files."
Message 2 (Time 44.945568) Source (192.168.1.158): "Using different ways, some of them are steged and some of them used secure ways/channel."
Message 3 (Time 63.820019) Destination (192.168.1.43): "Thanks."

Exhibit E Implications of Messages:
The first message implies the initiation of file transfer, which is common in data exfiltration scenarios. The second message is particularly incriminating as it explicitly mentions the use of steganography—concealing data within other non-secret data, which is a method often employed to bypass security monitoring—and secure channels, which could be encrypted communications designed to prevent interception and ensure confidentiality.

The use of such techniques aligns with Taurus Smith (Mona Simpson) potentially transmitting sensitive corporate information, such as the 'Honey Duff Donuts' recipe. The acknowledgement with a simple "Thanks" could imply successful receipt of the transmitted

data.

The technical analysis and message content, when combined with the known network identifiers (IP and MAC addresses) and the contextual backdrop of Taurus Smith's alleged activities, provide substantial insights into the methods used for the suspected unauthorized data transfer. This evidence could be critical in forming the narrative of how Taurus Smith may have conducted the alleged corporate espionage.

Chapter 9

Findings

9.1 Implications Regarding Taurus Smith and Accomplices

The forensic analysis has implicated Ken Warren and an individual named Mike concerning Taurus Smith's case. Ken Warren's digital authorship trails across documents tied to illicit activities, especially within files stored under the 'Frodo' account, suggesting he may have employed this alias. This pattern of authorship signifies possible measures to mask his true identity and involvement.

Simultaneously, evidence points to Mike due to his ownership of documents like "Basic Donuts.doc" and "Dad.xlsx," the latter containing hints towards a confidential recipe. The association of these files with Mike's account signals potential unauthorized dissemination of proprietary information.

The conjunction of metadata implicating Ken Warren and Mike is a critical lead in the investigation, suggesting coordinated actions with Taurus Smith in the handling and potential leak of sensitive corporate data.

9.2 Travel Intentions of Taurus Smith

The investigation into the digital artefacts related to Taurus Smith's travel intentions has yielded conclusive evidence of planned movement to a specific location. The evidence indicates a premeditated intent to travel from Cardiff to Hawaii.

Central to these findings is the image file f0066494.png discovered on the USB flash drive, which detailed a flight itinerary to Hawaii. The recovery of such a precise document point to deliberate travel planning and suggests a planned departure from the suspect's routine locale.

Supporting the flight plan, an intercepted message from Exhibit C's Wireshark capture stating, "See you in Hawaii! *F" aligns perfectly with the discovered itinerary plan. The informal sign-off implies familiarity and possibly an accomplice or a known contact in Hawaii, which could be pertinent to the investigation.

Further verifying the travel intent, cached internet browsing data, specifically CACHE_003 from the Mozilla browser profile on Taurus Smith's laptop, showed a pattern of visiting airport websites. This activity demonstrates active research and logistical preparation for travel, reinforcing the intent to move to Hawaii as indicated by the other pieces of evidence.

It is noteworthy to mention that geolocation data were absent within the expected digital artefacts such as photographs. This could be indicative of a deliberate attempt to erase or avoid leaving digital traces of the suspect's geographic movements. Despite this, the triangulation of the flight plan, communication evidence, and web browsing history provide a coherent narrative that strongly suggests Taurus Smith's intentions to travel to Hawaii.

The combined digital evidence paints a clear picture of Taurus Smith's preparations for travel. These actions were conducted with a degree of planning and discretion that suggests an intent to conceal the specifics of the movements. This finding of planned travel to Hawaii is critical to the understanding of Smith's activities and potential next steps.

9.3 Recovery of Hidden User Accounts

The investigation has successfully uncovered and analysed various user accounts that were concealed on Taurus Smith's laptop. The accounts were hidden using multiple methods, each designed to obfuscate their presence and purpose.

The use of benign and culturally familiar names such as "Bilbo Baggins," "Frodo Baggins," and "Sam" for user accounts was identified as a deliberate tactic to mislead investigators and avoid drawing attention to the accounts' true purposes. An account named "New folder" was also discovered, which contained no files or user activity, suggesting it may have been a placeholder for future use or a remnant of a previously cleaned account.

Additionally, the "Penelope Olsen" account presented a minimal digital footprint, with no corresponding user profile or document directory found, indicating an attempt to maintain a low profile on the system, potentially for covert activities.

Using AccessData Registry Viewer, critical user profile information was recovered from the system's registry files. The Security Accounts Manager (SAM) and SECURITY hives of the system registry were examined in-depth, revealing the creation times and last login dates of these accounts, thus providing a clear timeline of their activity.

The analysis process also involved reviewing system logs and file ownership data, which shed light on the usage patterns of these hidden accounts. The correlation of login events and document access patterns with other evidence, such as network logs and communication intercepts, has been pivotal in elucidating the role these accounts played in the suspect's activities.

The recovery and analysis of user profiles have significantly contributed to the investigation by establishing a clearer understanding of the accounts' activities and their potential link to unauthorized operations. The information assembled from this analysis has been crucial in piecing together the suspect's actions and has brought the investigation closer to identifying all user accounts associated with Taurus Smith's laptop.

The findings regarding the hidden user accounts have been thoroughly documented in the technical report. This documentation ensures the transparency of the investigative process and allows for the reproducibility of the results by other forensic examiners. For detailed accounts of the analysis process and the specific forensic techniques utilized, reference is made to the sections outlined in the report.

9.4 Identification and Recovery of Proprietary Recipes

During the forensic investigation into Taurus Smith's USB drive, several proprietary recipes from Lard&land Donuts were identified and recovered. These recipes were concealed using sophisticated data-hiding techniques, suggesting an unauthorized acquisition and potential intent to disseminate confidential culinary formulas.

The forensic examination led to the uncovering of multiple documents containing recipes that were disguised as innocuous files:

- **Steganography in Images:** The files Bean.png and coconuts.png were initially flagged during the review of steganographic methods and were later confirmed to contain hidden recipes using steganalysis tools.
- **Decrypted Document:** The Lard Land PDF required decryption, as detailed in Section 7.3. Upon decrypting, a detailed recipe was found that corresponded with the secret recipes of Lard&land Donuts.
- **Recovered Deleted File:** The file fragment Unalloc_8524_43768320_1003921408 was retrieved from unallocated space and revealed a recipe that had been deliberately deleted, indicating an attempt to obscure this sensitive information.
- **Misdirected Document:** The Basic Donuts.doc file was discovered in a non-descript directory path, /img_Taurus Laptop.001/vol_vol2/Family Photos/My Docs/, an attempt to hide it among personal files.
- **Link Discovery in Network Traffic:** Analysis of Exhibit D's PCAP file led to the identification of a URL which directed to an online repository containing a recipe, as described in Section 8.5.1.

The investigation revealed multiple methods employed to hide the recipes:

- **Steganography:** Advanced steganographic techniques were used to embed recipes within image files, which required specialized software to decode.
- **Encryption:** The Lard Land PDF file was encrypted, and successfully decrypted using the tool John The Ripper, revealing its contents.
- **Deletion and Recovery:** The data fragment representing a deleted recipe was recovered from unallocated space, showcasing an effort to erase its trace from the system.
- **Directory Misplacement:** The placement of Basic Donuts.doc in an unrelated directory was a tactic used to divert attention from its true content.
- **Hidden Hex Message:** A significant discovery was a hex-encoded message in the dad.xls file, suggesting the importance of the 'Special Pink Donut' and hinting at the existence of the 'Honey Duff Recipe'. Though the recipe was not directly found, the message itself indicates its significance and the lengths taken to conceal it.

The combination of these data-hiding techniques underscores a deliberate effort to protect and conceal Lard&land Donuts' proprietary recipes. The sophistication of these

methods indicates a high level of technical skill and an understanding of forensic countermeasures.

The findings from the investigation into the hidden recipes have been pivotal in understanding the extent of the unauthorized access and the methods used to conceal the theft of proprietary information. This aspect of the investigation has provided clear evidence of the suspect's activities related to the misappropriation of Lard&land Donuts' confidential recipes.

9.5 Detailed Network Activity Report

The comprehensive network activity analysis conducted as part of this investigation has provided substantial insights into the communications attributed to Taurus Smith, suspected of unauthorized dissemination of proprietary information. The meticulous examination of packet captures from Exhibits B, C, D, and E via Wireshark and manual inspection has revealed the following:

Examination of Exhibit B highlighted a TCP three-way handshake between IP addresses 192.168.1.157 and 192.168.1.137, indicating the initiation of a communication session. A subsequent TCP data transfer encapsulated within SSL suggests the transmission of encrypted content, indicating a concern for the confidentiality of the data being exchanged.

The secure message from Exhibit B sent from IP address 192.168.1.157, coupled with TCP [PSH, ACK] flags, underscores the urgency of the data transfer. Duplicate ACKs and Fast Retransmission events within the packets further imply a robust error recovery mechanism, ensuring data integrity during transfer.

Exhibit D's analysis was particularly revealing, with a TCP data transfer from Taurus Smith's computer (192.168.1.158) to host 192.168.1.43 involving a significant payload containing what appeared to be a detailed proprietary recipe. The data included a list of ingredients, cooking instructions, and URLs, indicative of the transmission of Lard&land Donuts' 'Honey Duff Donuts' recipe.

The message content and the method of transmission via TCP, marked with the [PSH, ACK] flags, suggest a deliberate action to disseminate sensitive corporate information. The use of a VMware virtual machine by the recipient (host 192.168.1.43) points to a possible attempt to mask the true endpoint of the data or to add a layer of anonymity to the communications.

In Exhibit E, TCP communications between 192.168.1.158 and 192.168.1.43, as well as the exchange of ARP information, were consistent with an established pattern of network behaviour. Notably, a message at time 15.101793 from Taurus Smith's computer mentioned the transmission of 'steged' files, revealing the use of steganography. The mention of 'secure ways/channels' implies the use of encrypted communications to maintain the confidentiality of the transmitted data.

Additionally, Exhibit C provided further context to the network activity, reinforcing the patterns observed in other exhibits. The analysis of this exhibit would have focused on further substantiating the secure and confidential nature of the data transfers, possibly adding more detail on the timing, content, or methods used in these transmissions.

The implications of these findings are significant. The secure transfer of data, the deliberate use of steganography and secure channels, and the transmission of proprietary recipes strongly support the hypothesis that Taurus Smith engaged in unauthorized and potentially illicit activities. The network activity paints a picture of sophisticated methods employed to transfer sensitive information discreetly.

The network activity report, with its technical nuances and contextual implications, is crucial in constructing the narrative of Taurus Smith's alleged involvement in the misappropriation and dissemination of confidential corporate recipes. This report will form a key element of the evidence presented in the case against Taurus Smith.

Chapter 10

Conclusion

10.1 Summary of Investigative Outcomes

The digital forensic investigation has identified significant evidence of illicit activities potentially involving Taurus Smith, Ken Warren, and an individual known as Mike. Ken Warren's repeated digital authorship across various documents, particularly under the alias 'Frodo,' suggests a calculated attempt to conceal his identity and involvement in the activities. Mike's ownership of files containing sensitive recipe information indicates his potential complicity in the unauthorized dissemination of proprietary data.

10.2 Interpretation of Evidence

The recovered flight itinerary, encrypted communications, and the use of steganography and anonymous virtual machines in network transfers point to a systematic approach to concealment and data exfiltration. The meticulous planning of travel from Cardiff to Hawaii and the absence of geolocation data from photographs suggest a deliberate effort to obscure digital traces of geographic movements.

10.3 Implications for the Case

The conjunction of forensic evidence implicates Taurus Smith, Ken Warren, and Mike in a coordinated effort to misappropriate and potentially leak sensitive corporate information. The sophisticated methods uncovered in this investigation, such as the use of aliases, encryption, and steganography, demonstrate advanced technical knowledge and intent to protect the confidentiality of the transmitted data.

The implications of these findings are critical. They not only highlight the complex digital footprint of the suspects' activities but also showcase the depth of forensic analysis required to unravel such a multifaceted case. The network activity reveals a clear narrative of the methodical and discreet transfer of sensitive information, which will be pivotal in legal proceedings.

The evidence assembled provides a strong foundation for the allegations against the suspects and underscores the importance of comprehensive digital forensic investigations in modern cybersecurity incidents. The technical information and the implications drawn from the network activity reports will serve as a cornerstone in understanding the full scope of the suspects' actions and the potential breaches of corporate trust and legal boundaries.