DIGITAL FORENSIC REPORT

BRUCE INDUSTRIES

Course: MGS 610 Digital Forensics

Instructor: Dominic Sellito

May 09, 2025

Table of Contents

PREFACE – SCENARIO DESIGN

We started off with the idea of simulating a cyberattack and then performing forensic analysis to understand what kind of data might have been exfiltrated. The initial approach was purely technical, there was no storyline behind it. It was just about carrying out an attack and analyzing the system afterward.

At first, we explored the idea of DNS tunneling, but that plan was dropped since it would have required a registered domain to make it work properly. From there, the scenario began to evolve. Then we decided to bring in a social engineering angle - something like phishing - and that's when the story started taking shape.

Instead of treating the insider as simply malicious, we thought it would be more interesting to present the user as someone who had been manipulated or coerced. That added a more layered perspective to the situation.

As the storyline developed, we added in technical elements like phishing emails,vRemote File Inclusion (RFI), and privilege escalation through sudoers misconfiguration. The final scenario blended both behavioral and technical aspects, giving us a well-rounded case to investigate from a forensic standpoint.

1 Team Members and Company Background

This section introduces the forensic investigation team responsible for analyzing the incident at Bruce Industries and provides an overview of the company itself. Understanding the organizational environment in which the incident occurred helps set the stage for understanding the scope, impact, and relevance of the findings detailed in this report.

1.1 Team Members

This investigation was conducted by a five-member digital forensics team. The team members are listed below:

1. Collin Heeb
2. Faraz Ahmed
3. Kathiresan Kandasamy
4. Pramath Yaji
5. Raghavi Ayyathurai

1.2 Company Background

Bruce Industries is a globally recognized leader in **Very-Large-Scale Integration (VLSI) design** and **semiconductor manufacturing**. With decades of innovation, the company is known for developing **advanced microarchitecture solutions** that power next-generation computing technologies. It serves clients across a broad range of high-tech sectors.

To safeguard its digital assets - particularly against **espionage** and **insider** leaks - Bruce Industries has heavily invested in internal security infrastructure. A key measure is the deployment of a **Transport Layer Security (TLS)** interception system, or **SSL proxy**, which **decrypts**, **inspects**, and **re-encrypts** employee **HTTPS traffic** to detect anomalies such as **phishing attempts**, **malware infections**, and **unauthorized data transfers**.

Acknowledging the increasing complexity of modern cyberattacks, the company proactively initiated a **Red Team simulation** to evaluate the effectiveness of its Incident Response procedures and the readiness of its Digital Forensics team. The simulation centered on a potential **insider threat** under external coercion, testing the organization's ability to detect, analyze, and respond to blended, real-world threats.

2 Executive Summary

An employee supporting Bruce Industries' **HR department** unknowingly became the focal point of a **simulated cyber incident** designed to test the organization's forensic and incident response capabilities. After receiving a **deceptive communication** from a **spoofed source**, the employee made a series of changes that introduced vulnerabilities into the system - ultimately **enabling unauthorized access** to **confidential HR data**. This internal **Red Team simulation** was intended to evaluate how well Bruce Industries could detect, investigate, and respond to such blended threats involving both technical compromise and human manipulation.

The simulation began on **April 15, 2025** and was conducted in a controlled environment, following standard forensic procedures. The investigation included analysis of **system activity**, **user behavior**, and **network traffic** using forensic tools and secure inspection methods. Key findings revealed that under simulated pressure the employee, **modified system configurations** in ways that weakened security. While the employee did not directly extract data, their actions created a pathway for sensitive information to be exposed. This raised important questions about insider risk awareness and monitoring capabilities.

As a result of the simulation, the security team at Bruce Industries recommends **enhancing phishing awareness programs**, **tightening access controls**, and implementing **proactive monitoring** for **anomalous user activity**. These findings provide actionable insights to strengthen the organization's overall cyber resilience.

3 Introduction

This report documents the results of a Red Team simulation conducted at **Bruce Industries** on **April 15, 2025**. The purpose of the exercise was to evaluate the organization's ability to respond to a complex cyber incident involving insider threat. This report outlines the **methodology** used during the investigation, the **key findings**, and the **recommended steps** for enhancing the organization's security posture.

3.1 Case Background

During routine encrypted traffic inspection, Bruce Industries' TLS interception system detected the exposure of a **private cryptocurrency key** belonging to an internal employee temporarily supporting the HR department. Rather than responding immediately, the **Chief Information Security Officer (CISO)** used this discovery to initiate a controlled Red Team simulation. The objective was to evaluate how a subtle, coercion-based threat could influence an internal user and test the organization's ability to investigate insider risk.

A **phishing email** was sent to the employee from a **spoofed domain** mimicking a well-known cryptocurrency platform. The message suggested that unauthorized transactions had occurred and warned the employee to comply with future instructions. Over time, the employee **introduced vulnerabilities** into the HR web portal, including **insecure file upload** mechanisms and **misconfigured permissions**, enabling simulated external access to sensitive employee data.

The scenario required the forensic team to analyze not only the technical indicators of compromise but also the underlying behavioral factors contributing to the incident.

3.2 Objectives

The purpose of this investigation was to examine how Bruce Industries' security team would detect and handle a subtle, high-stakes security scenario involving an internal user influenced by external pressure. By simulating a blended threat that combined social engineering with technical exploitation, the exercise tested the organization's ability to respond to ambiguous and evolving risks.

The investigation aimed to:

- Reconstruct key events leading to the **unauthorized exposure** of **sensitive data**.
- Identify how vulnerabilities were introduced and exploited.
- Assess the **readiness** and **decision-making** process of the forensic team.
- Inform future improvements to **insider threat detection**, **user monitoring**, and **training protocols**.

4 Methodology

The following section outlines the investigative approach used during the incident analysis, emphasizing transparency, repeatability, and forensic soundness. All steps were conducted in a controlled environment to ensure the reliability and integrity of evidence examined throughout the case.

4.1 Tools Used

The investigation primarily relied on the following forensic tools:

- **Autopsy:** Used for disk image analysis, timeline reconstruction, keyword searches, and file system exploration.
- **Wireshark:** Used to examine PCAP files capturing HTTP traffic from within the internal network. These packets included decrypted HTTPS sessions made available through TLS interception, allowing the forensic team to identify suspicious POST requests and file uploads to vulnerable endpoints.
- **Screenshot capture tools:** Used to preserve transient evidence such as phishing emails and browser content.

All tools used in this investigation are widely accepted within the digital forensics community and maintain a strong reputation for forensic reliability. **Autopsy**, in particular, is built on **The Sleuth Kit** and adheres to recognized standards for forensic integrity and evidence handling [1].

[1] https://www.sleuthkit.org/autopsy/

4.2 Procedures

The forensic process began with the review of **network traffic captures** using **Wireshark**. These captures included **decrypted HTTPS sessions** obtained through Bruce Industries' TLS interception infrastructure. Analysts observed unusual POST requests and file uploads to the HR web server, suggesting potential exploitation of upload functionality.

Following this, a disk image of the affected HR system was examined using **Autopsy**. The analysis focused on **file access patterns**, **user activity**, and **indicators of privilege escalation**.

Key forensic procedures included:

- Analysis of **authentication logs** to track account elevation and privilege misuse.
- Examination of **file transfers**, including the movement of sensitive encrypted files and the extraction of decryption keys.
- Detection of **steganographic behavior**, where confidential data was embedded in media files.
- Timeline reconstruction by correlating **user commands**, **timestamps**, and **system responses**.
- Validation of actions through screenshots and command history for evidentiary support.

The disk image was mounted in a read-only state to ensure evidence integrity. All actions taken were documented and aligned with forensic best practices to ensure repeatability and reliability of findings.

4.3 Chain of Custody and/or Integrity

Evidence was collected in accordance with standard forensic procedures to ensure integrity and repeatability. The disk image of the affected system was acquired using **Guymager**, a widely accepted forensic imaging tool that supports **hash verification** during and after acquisition. **SHA-256** hashing was applied and verified to confirm the authenticity of the acquired image [Refer to **Appendix A1** and **A2**].

5 Findings & Analysis

This section outlines the findings of the controlled simulation conducted to test Bruce Industries' response to a blended threat scenario. Forensic artifacts were analyzed from both **system logs** and **network traffic** to understand how the simulated threat progressed and how the organization responded.

5.1 Sequence of Key Events

- **Phishing Email Discovered:** A simulated phishing email was planted in the **user faraz's** inbox, sent from a **typosquatted domain (alerts@coinbbase.com)**. It mimicked a Coinbase alert and claimed the user's **private crypto wallet** had been compromised.
- **Unreported Phishing and Behavior Shift:** The phishing email was not reported and after receiving it, the user's behavior shifted — including transferring sensitive HR data into a personal account.
- **Steganography Detected:** Data was intentionally embedded within image files to conceal. These files were later found in faraz's directory during forensic review.
- **Follow-up Instructions Executed:** A second phishing message in the simulation instructed the user to introduce vulnerabilities. Logs confirmed the scripted insertion of:

  SQL Injection vectors.

  Remote File Inclusion (RFI) upload capability.

  Sudoers misconfiguration allowing daemon to escalate privileges via vim.

- **Shift to Attacker Activity:** As the simulation progressed, the user ceased direct interaction. The attacker, took advantage of the planted vulnerabilities to gain root access and explore the HR directory.
- **Simulated Data Exfiltration:** The final phase involved exfiltration of HR data via a Python-based server.

5.2 Evidence Analysis

The investigation uncovered a phishing email received from **alerts@coinbbase.com**, a typosquatted domain impersonating **Coinbase**. The email warned the user, faraz, of a wallet compromise and threatened further loss if he failed to comply with instructions. This email was never reported to the security team, a failure that became a critical red flag and shifted faraz's role from potential victim to someone whose actions enabled further compromise [Refer to **Appendix A3** and **A4**].

Shortly after receiving the initial phishing email, the user faraz accessed **sensitive HR data** and transferred it into his personal directory. Subsequent analysis revealed that this data had been concealed using **steganography** - a technique that embeds confidential information within seemingly benign image files to evade detection. [Refer to **Appendix A5** and **A6**].

However, upon recognizing that Bruce Industries employs Transport Layer Security (TLS) interception to inspect encrypted traffic, faraz appeared to halt any direct exfiltration attempts. The awareness that outbound data transfers from his account could be monitored likely contributed to this behavioral shift, as no further external communication was observed from his user profile at that stage.

This changed after a second phishing message was delivered via the spoofed web portal. The message issued explicit instructions not to alert the security team and directed faraz to weaken internal security controls. From that point onward, system activity closely mirrored the steps outlined in the attacker's communication. The first notable action involved the exploitation of a **SQL Injection** vulnerability introduced into the HR portal. This allowed unauthorized access to backend data, potentially exposing sensitive employee information [Refer to **Appendix A7**].

Subsequently, the attacker leveraged a **Remote File Inclusion (RFI) vulnerability** - also intentionally introduced into the application - to upload **malicious PHP scripts** to the server. These scripts enabled persistent remote access to the system by allowing arbitrary command execution through a web shell interface [Refer to **Appendix A8**]. In parallel, faraz modified the **system's sudoers file** to grant the daemon user **passwordless administrative access** through the **vim** binary. This deliberate misconfiguration exploited vim's ability to spawn a root shell, effectively allowing the attacker to escalate privileges and gain full root access to the system without authentication [Refer to **Appendix A9** and **A10**].

Once **root** access was achieved, the attacker conducted extensive **reconnaissance** within the HR directory, reviewing sensitive files and identifying high-value data [Refer to **Appendix A11**]. The final phase of the incident involved **data exfiltration** via a custom **Python server**, marking the completion of the simulated breach scenario [Refer to **Appendix 12**].

These findings underscore the broader lesson that even well-secured environments can become vulnerable when small oversights align with opportunity. Whether introduced by design or discovered through investigation, every weakness revealed in this case reinforces the need for constant vigilance, layered defenses, and a security culture that anticipates the unexpected.

6 Conclusion & Recommendations

The purpose of this section is to summarize the most critical discoveries from the investigation and outline actionable mitigation strategies to reduce the risk of future security incidents.

6.1 Summary of Findings

The investigation uncovered a staged insider threat scenario in which a combination of **phishing-based coercion**, **application-layer vulnerabilities**, and **system misconfigurations** were exploited. The attacker gained initial access by delivering instructions to an internal user, resulting in:

- **Unauthorized access** and **transfer** of HR-related data into a personal directory.
- Use of **steganography** to conceal sensitive data within image files.
- Introduction and exploitation of **SQL Injection** and **Remote File Inclusion (RFI)** vulnerabilities.
- Modification of the **sudoers** file to enable **privilege escalation** via vim.
- **Root-level** access and subsequent **reconnaissance** of sensitive directories.
- Final **exfiltration** of files using a covert communication channel.

6.2 Mitigation Steps

To address the gaps identified during the simulation, the following general mitigation strategies are recommended:

- Deliver ongoing, role-specific **training** to improve employee recognition of phishing, social engineering, and abnormal system behavior.
- Regularly **audit user permissions** and **privilege escalation pathways** to ensure alignment with operational needs.
- Identify and remediate **web application flaws** through secure development practices and vulnerability scans.
- Utilize **system** and **network monitoring** to flag unusual activities, such as unsanctioned sudo changes, shell activity, and data movements.
- Perform regular **integrity checks** on files like sudoers, and enforce hardened defaults for services exposed internally or externally.
- Continue **regular assessments** to evaluate detection, response, and containment capabilities in evolving threat scenarios.

7 Appendix

7.1 Evidence Acquisition and Integrity Validation

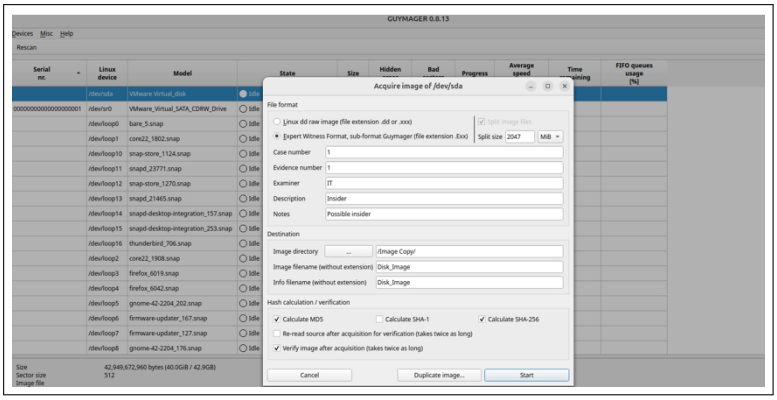

Figure A1: Disk Imaging Using Guymager

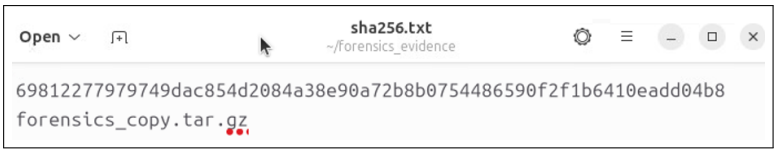

Figure A2: SHA-256 Hash Verification

7.2 Phishing Communication and Coercive Messaging

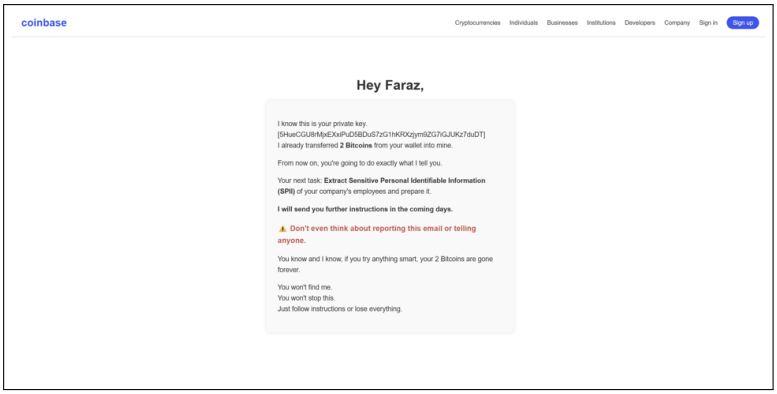

Figure A3: Phishing Email from Spoofed Domain

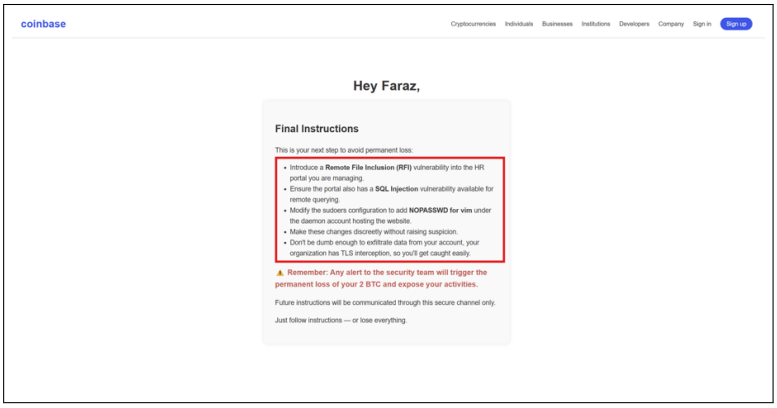

Figure A4: Follow-Up Phishing Email with Exploit Instructions

7.3 Steganographic Evidence and Data Extraction

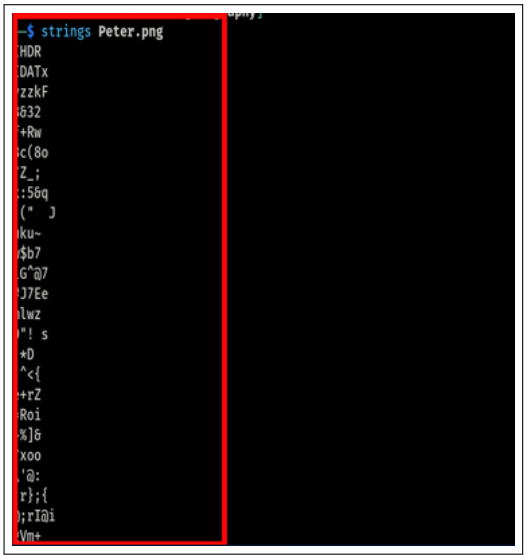

Figure A5: Initial Inspection of Image File Using strings Utility

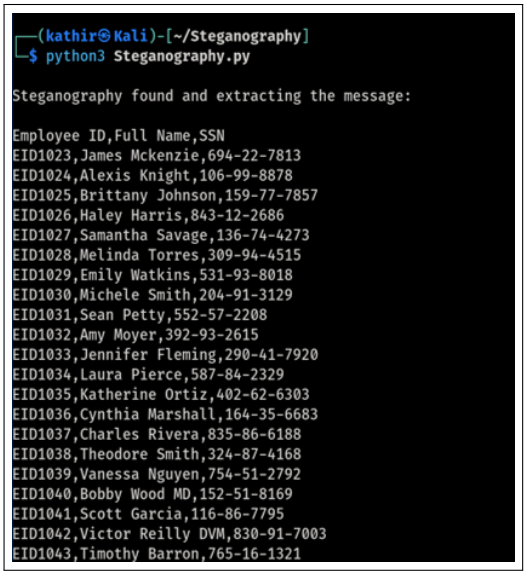

Figure A6: Extracted Employee Data from Steganographic Image

7.4 Vulnerability Exploitation Evidence

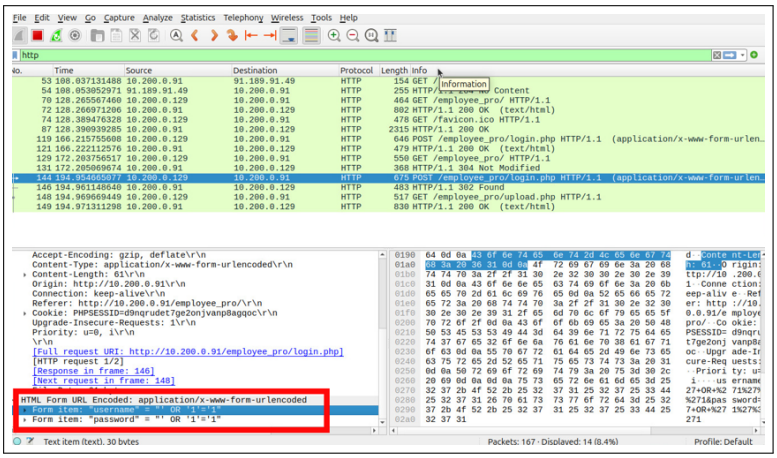

Figure A7: SQL Injection Attempt

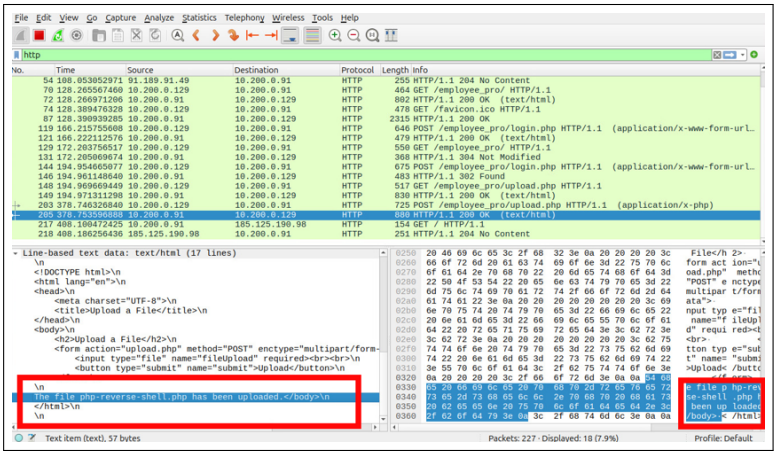

Figure A8: Successful Upload of a PHP Reverse Shell

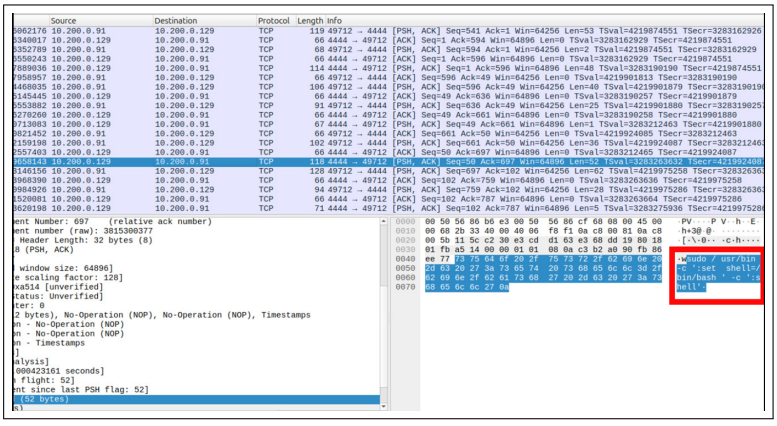

Figure A9: Wireshark Capture Showing Privilege Escalation via vim

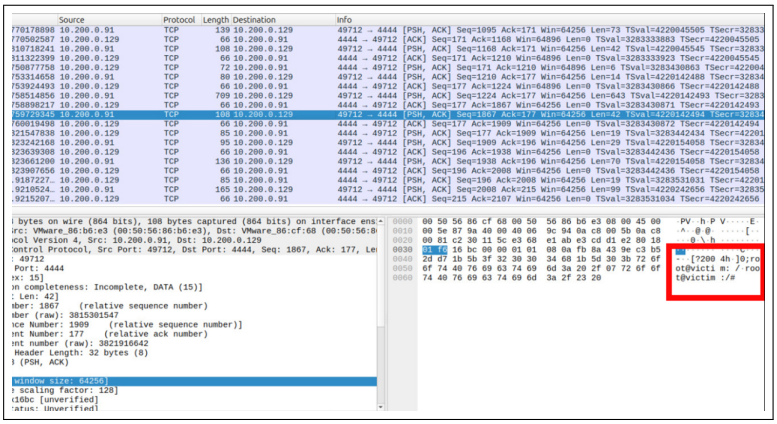

Figure A10: Evidence of Remote Root Shell Session

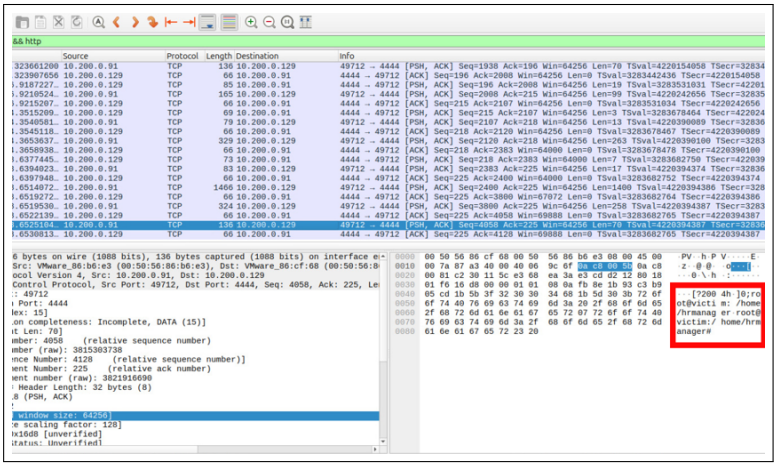

Figure A11: Reconnaissance in the HR Manager's Directory

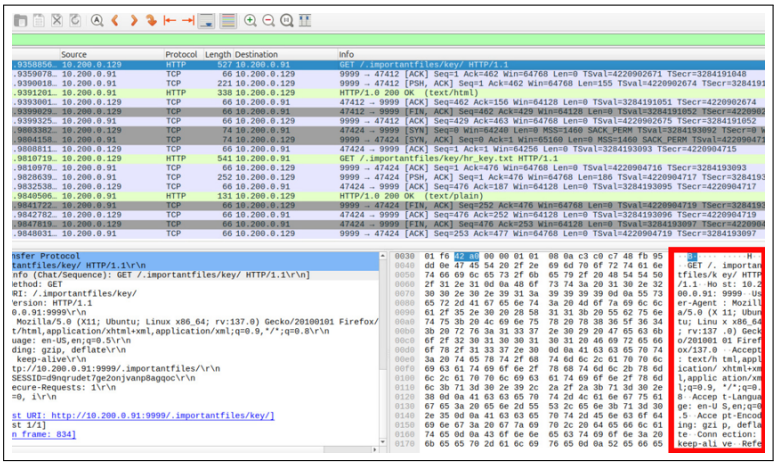

Figure A12: Exfiltrating Data Through Python Server