Nazir_Purposal.docx

by Muhammad Nazir

Submission date: 19-Jul-2024 04:49PM (UTC+1000)
Submission ID: 2419075935
File name: Nazir_Purposal.docx (19.25K)
Word count: 1622
Character count: 9907

Forensic Investigation Proposal

Introduction

Summary of the Offence:

The investigation concerns the suspected smuggling of 1 kilogram of Methamphetamine into New Zealand, facilitated by individuals identified as Jane Esteban and John Fredricksen. Intelligence provided by the Australian government suggested their involvement in illegal activities related to drug trafficking. John Fredricksen allegedly communicated with a local drug distributor, Steve Kowhai, to arrange the smuggling operation, utilizing digital communication channels and potentially employing steganography to conceal sensitive information.

Details of Parties Involved:

1. **Jane Esteban:** An undercover officer from the Australian Federal Police (AFP), posing as a drug user to gather intelligence on John Fredricksen and his associate Steve Kowhai.

2. **John Fredricksen:** Alleged smuggler who communicated with Steve Kowhai to coordinate the transportation and delivery of the illicit substance into Wellington, New Zealand.

3. **Steve Kowhai:** Local drug distributor based in the lower North Island of New Zealand, who provided information and logistics support to John Fredricksen for the smuggling operation.

Details of Computers or Devices Pertaining to the Investigation:

- **John Fredricksen's Windows Laptop:** Used for communication with Steve Kowhai via Discord and potentially for receiving documents related to the smuggling operation.

- **Jane Esteban's Windows Laptop:** Utilized as part of her undercover role to communicate with John Fredricksen and gather evidence regarding the drug trafficking activities.

- **Unknown Suspect's Desktop Computer:** Located at 666 Rewera Avenue, Petone, containing drugs, guns, and a desktop computer in the living room. This device is of interest due to its potential connection to the drug trafficking network.

What Are We Looking At, and Why?

We are examining digital devices to:

- **Identify Communication:** Analyze communications between John Fredricksen and Steve Kowhai to establish the extent of their involvement in planning the smuggling operation.

- **Evidence of Intent:** Look for documents or files that indicate intent or preparation for the illegal transport of Methamphetamine into New Zealand.

- **Steganographic Techniques:** Investigate the use of steganography to hide sensitive information within images or other digital media, as suggested by intelligence reports.

Background

Summary of the Digital Forensics Process:

The process typically includes:

1. **Identification and Preservation:** Identifying relevant devices and ensuring the integrity of digital evidence through proper preservation techniques.

2. **Acquisition:** Making a forensic copy (image) of the storage media to prevent alteration of original data.

3. **Analysis:** Examining the acquired data using specialized tools and techniques to extract relevant information and artifacts.

4. **Documentation:** Documenting findings in a detailed report that can be used in legal proceedings, maintaining a chain of custody to ensure admissibility of evidence.

Factual Details Pertaining to the Investigation:

Location of Offence: The offence involves the smuggling of Methamphetamine from Brisbane, Australia to Wellington, New Zealand.

Individuals Involved:

Jane Esteban: An undercover AFP officer tasked with investigating the drug ring involving John Fredricksen and Steve Kowhai.
John Fredricksen: Alleged smuggler who communicated with Steve Kowhai to arrange the smuggling operation.
Steve Kowhai: Local drug distributor in New Zealand, providing logistics support for the smuggling operation.

Others Potentially Involved:

The unknown suspect whose desktop computer was found with drugs and guns at 666 Rewera Avenue, Petone, suggesting a broader network or associates linked to the drug trafficking activities.

Statements Made by Offenders or Third Parties:

John Fredricksen: Allegedly communicated with Steve Kowhai via Discord and received instructions and documents related to the smuggling operation.

Jane Esteban: Posing as a drug user, she has interacted with John Fredricksen to gather intelligence on the drug trafficking activities.

Known Problems Relating to Suspects/Victims or Evidence:

Legal and Procedural Challenges: Admissibility of digital evidence, chain of custody issues, and ensuring forensic integrity throughout the investigation process.

Complexity of Digital Evidence: Different Windows 10 builds on the devices may lead to varied artifact locations, requiring meticulous analysis and interpretation.

Concealment Techniques: The use of steganography to hide documents within images poses challenges in identifying and extracting hidden data.

Objectives

SMART Objectives for the Investigation:

1. Extract and analyze Discord chat logs and email communications from John Fredricksen's laptop to identify communication with Steve Kowhai regarding the smuggling operation.

- **Measurable:** Review and document all relevant chat logs and emails found on John Fredricksen's laptop within 2 weeks of acquisition.
- **Achievable:** Utilize forensic tools like FTK Imager and X-Ways Forensics to ensure comprehensive extraction and analysis of communication artifacts.
- **Relevant:** This objective directly supports the investigation by uncovering direct evidence linking John Fredricksen to the planning and coordination of the drug smuggling.
- **Timely:** Complete the initial analysis of Discord and email communications by the end of Week 2 of the investigation.

2. Investigate the use of steganography on Jane Esteban's laptop to identify any hidden documents or files related to the smuggling operation.

- **Measurable:** Conduct thorough steganalysis using tools such as Stegdetect and stegextract to identify and extract hidden data within images or other media files on Jane Esteban's laptop.

- **Achievable:** Employ steganography detection techniques and tools to identify potential hidden content within a variety of digital media files.
- **Relevant:** This objective aims to uncover potentially concealed evidence that could provide further insights into the smuggling operation.
- **Timely:** Complete steganalysis and document findings by the end of Week 3 of the investigation.

3. Analyze the desktop computer found at 666 Rewera Avenue, Petone, to identify any digital evidence linking it to the drug trafficking activities.
- **Measurable:** Image and analyze the desktop computer using forensic tools to identify and document any relevant files, documents, or communications related to drug trafficking.
- **Achievable:** Ensure comprehensive analysis of the desktop computer to uncover any potential evidence of involvement in the smuggling operation.
- **Relevant:** This objective seeks to establish connections between the physical location and the broader drug trafficking network.
- **Timely:** Complete the forensic analysis of the desktop computer and compile findings by the end of Week 4 of the investigation.

Strategies

Analysis Approach:

1. **Discord and Email Communication Analysis (John Fredricksen's Laptop):**
- **Process:** Use FTK Imager to acquire a forensic image of John Fredricksen's laptop. Analyze the acquired image using forensic software to search for Discord chat logs and email databases.
- **Method:** Utilize keyword searches and timeline analysis to identify relevant communications between John Fredricksen and Steve Kowhai regarding the smuggling operation.
- **Tools:** FTK Imager for imaging, Autopsy or X-Ways Forensics for analysis.
- **Progress Indicators:** Number of chat logs and emails identified, relevance of the content to the smuggling operation.

2. **Steganography Detection (Jane Esteban's Laptop):**
- **Process:** Image Jane Esteban's laptop using FTK Imager. Conduct steganalysis using tools like Stegdetect and stegextract to detect hidden information within media files (images, videos).
- **Method:** Employ statistical analysis and examination of LSB (Least Significant Bit) alterations in images to detect steganographic payloads.
- **Tools:** Stegdetect, stegextract, and other steganalysis tools.
- **Progress Indicators:** Number of files analyzed, detection of steganographic content, extraction of hidden data.

3. **Analysis of Desktop Computer (666 Rewera Avenue, Petone):**
- **Process:** Perform forensic imaging of the desktop computer found at the specified address. Analyze the acquired image using forensic tools to examine files, documents, and internet history.

- **Method:** Use keyword searches, file carving techniques, and link analysis to identify any evidence linking the desktop computer to drug trafficking activities.
- **Tools:** FTK Imager for imaging, Encase or Forensic Toolkit for analysis.
- **Progress Indicators:** Identification of relevant files correlation with physical evidence found at the location.

Milestones

1. **Week 1: Initial Acquisition and Analysis (Jane Esteban's Laptop)**
   - Acquire forensic image of Jane Esteban's laptop.
   - Begin steganalysis process to detect hidden data.

2. **Week 2: Discord and Email Analysis (John Fredricksen's Laptop)**
   - Complete acquisition of John Fredricksen's laptop.
   - Analyze Discord chat logs and email communications.

3. **Week 3: Continued Analysis (Jane Esteban's Laptop)**
   - Complete steganography detection and document findings.
   - Begin analysis of any additional evidence found on Jane Esteban's laptop.

4. **Week 4: Desktop Computer Analysis (666 Rewera Avenue, Petone)**
   - Image and analyze the desktop computer found at 666 Rewera Avenue, Petone.
   - Compile findings from all devices and prepare preliminary report.

Conclusion

Summary of the Steps Taken:

Several critical steps were undertaken to gather digital evidence and analyze it thoroughly:

1. **Device Acquisition:** Forensic images of John Fredricksen's laptop, Jane Esteban's laptop, and the desktop computer found at 666 Rewera Avenue, Petone, were acquired using FTK Imager.

2. **Communication Analysis:** Discord chat logs and email communications from John Fredricksen's laptop were scrutinized using forensic software. This aimed to uncover any conversations smuggling of Methamphetamine into New Zealand.

3. **Steganography Detection:** Jane Esteban's laptop underwent steganalysis to detect any hidden files or messages concealed within images or other media files.

4. **Desktop Computer Analysis:** The desktop computer located at 666 Rewera Avenue, Petone, was meticulously analyzed to identify digital evidence linking it to drug trafficking activities.

5. **Documentation and Reporting:** Throughout the investigation, meticulous documentation was maintained, detailing findings, methodologies, and forensic processes. This documentation forms the basis for the preliminary report.

Next Steps to Be Taken:

1. **Finalize Analysis and Reporting:** Complete the analysis of all acquired data and compile a comprehensive forensic report detailing the findings from each device. The report should include:
   - Summaries of key findings
   - Analysis of communication
   - Results of steganalysis
   - Evidence linking the suspects

2. **Presentation to Stakeholders:** Prepare a presentation summarizing the forensic findings and implications for the ongoing investigation. This presentation will be crucial for updating stakeholders and planning further actions.

3. **Legal Consultation and Action:** Consult with legal advisors to ensure the admissibility of digital evidence and discuss potential legal actions against the suspects identified in the investigation.

4. **Follow-Up Investigation:** Based on the findings and identified leads, initiate further investigative actions such as interviews, surveillance agencies to dismantle the drug trafficking network effectively.

Nazir_Purposal.docx

ORIGINALITY REPORT

2%	0%	0%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Southern Cross University Student Paper	2%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		