

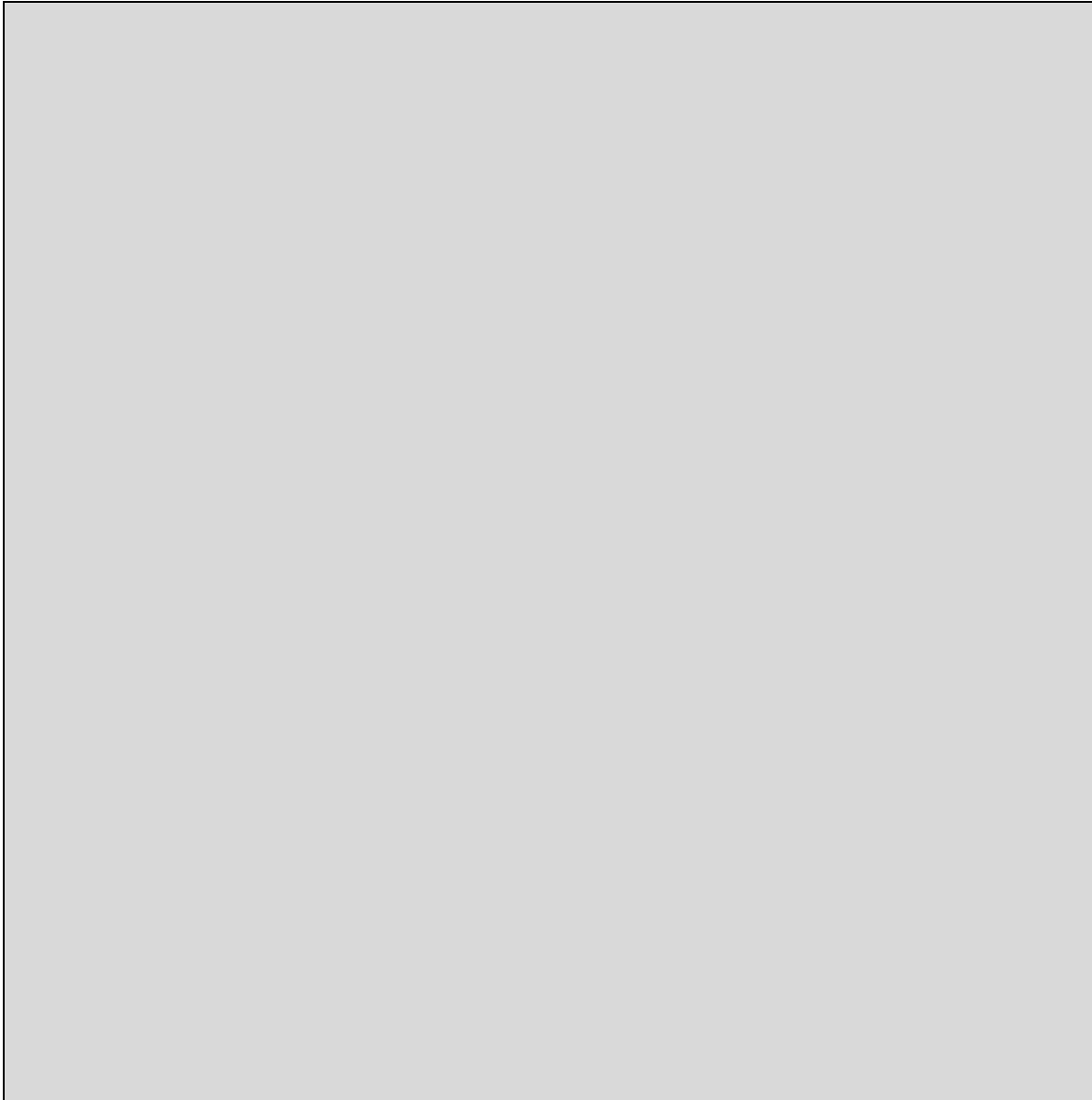
Forensics Investigative Analysis Report

[Date]

Incident Report Number:	
Report Name:	
Location Category:	
Reported Incident Date:	

Executive Summary

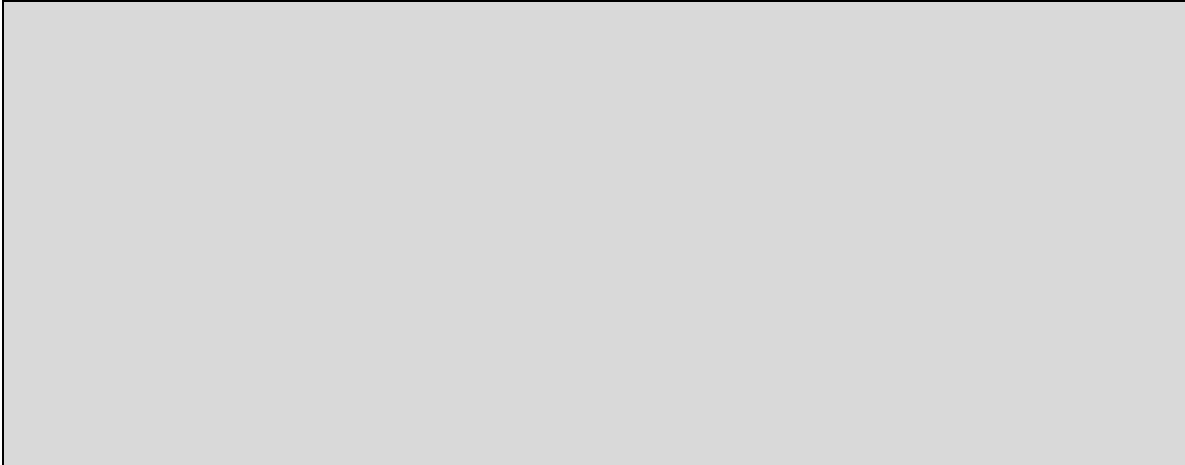
[Briefly describe the executive summary of this report.]



1. Initial Incident Discovery

1.1 Summary

*[*Include summary of the initial incident discovery]*

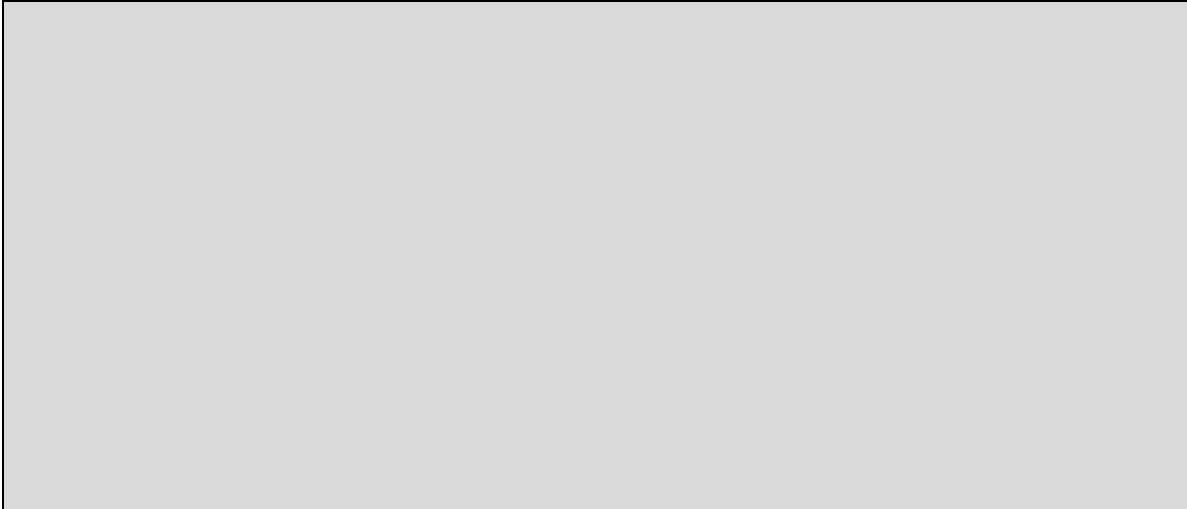


1.2 Action Items

*[*List out the actions taken by all the IT Professionals.*

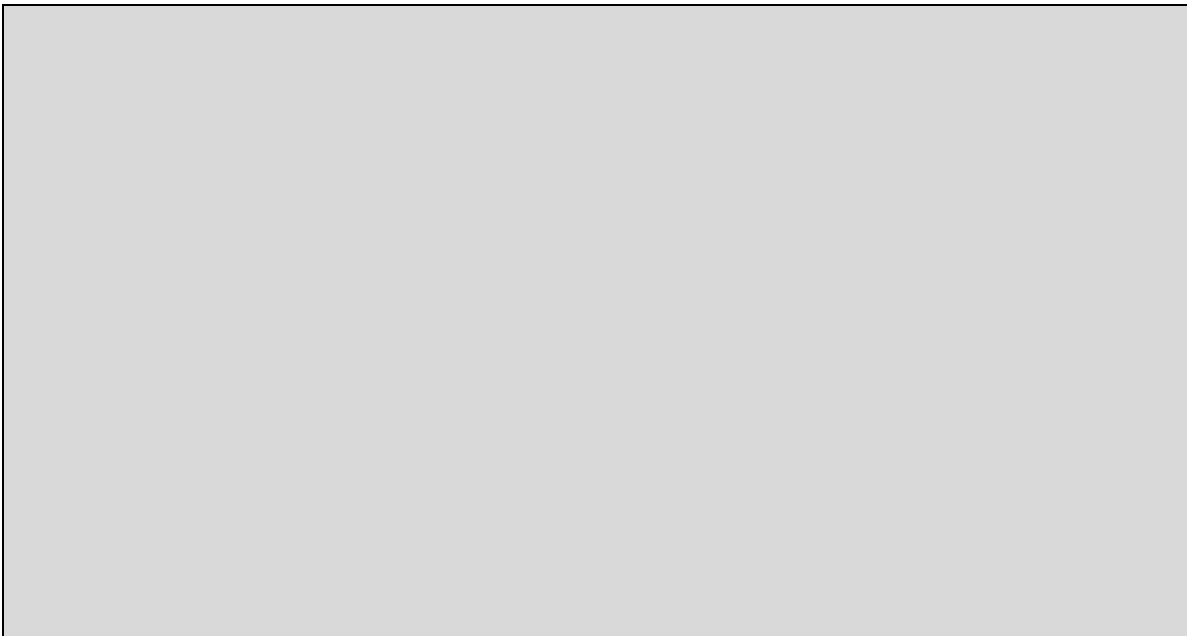
Example:

- *An exhaustive search of the website – Web Server Administrator*
- *Capture and analyze a segment of network data using Wireshark, Netwitness, etc. – Security Analyst*
- *Produce digital image of disk contained in the suspected system – Forensic Technician*
- *Detailed list of findings – Forensic Case Manager*
- *Final Forensic Analysis Report – Forensic Investigator.]*



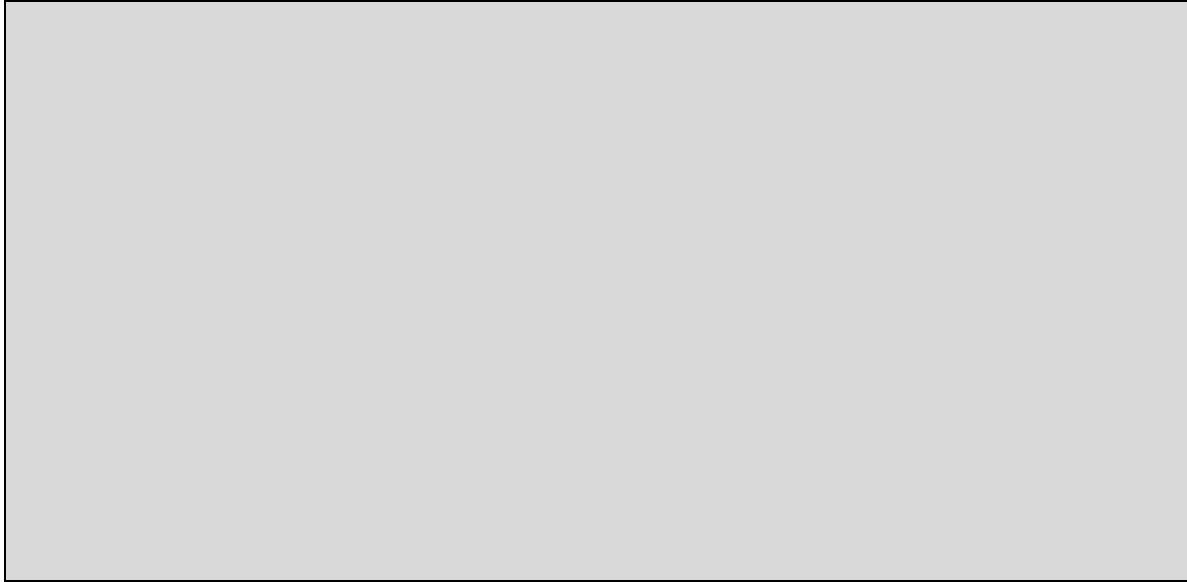
1.3 Description of System(s) in Question

*[*Give description of all affected systems such as web servers, database servers, network devices, hosts, etc.]*



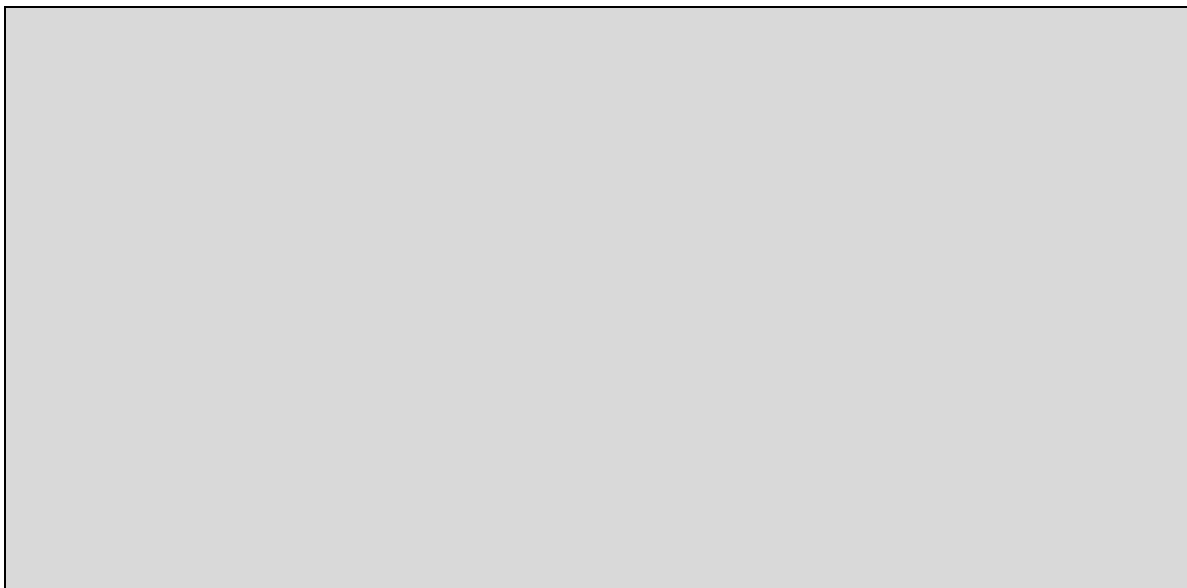
1.4 Security Mechanisms in Place

*[*Give description of the existing security mechanisms that helped in the investigation process, e.g., security measures that prevent unauthorized access such as DMZ, firewalls, IDS/IPS, SIEM, etc.]*

A large, empty rectangular box with a thin black border, intended for the user to provide a detailed description of the security mechanisms in place during the investigation.

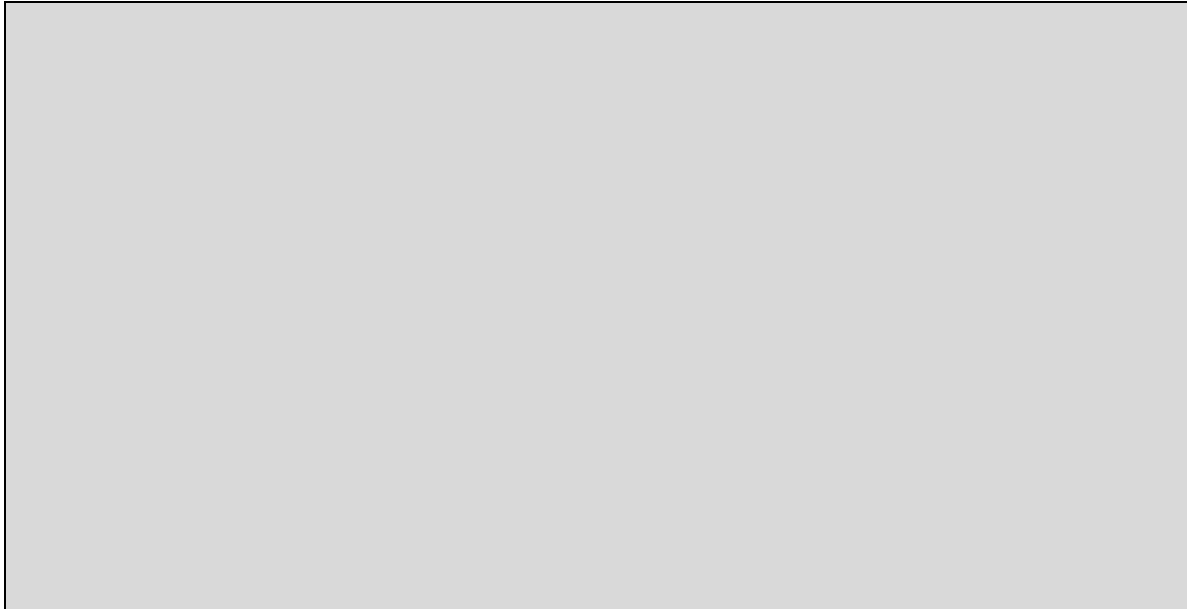
1.5 Initial Forensic Discovery

*[*Describe what is detected in the initial forensic discovery phase, e.g. detected no unusual files, detected susceptible activities between the workstation and web server, etc.]*

A large, empty rectangular box with a thin black border, intended for the user to provide a detailed description of the findings from the initial forensic discovery phase.

1.6 Initial Corrective Action

*[*Discuss the initial corrective measures taken to avoid risk temporarily and to perform further analysis, e.g., restrictive access to web server]*



1.7 Participants

*[*List out all the participants involved in the forensic investigation.]*

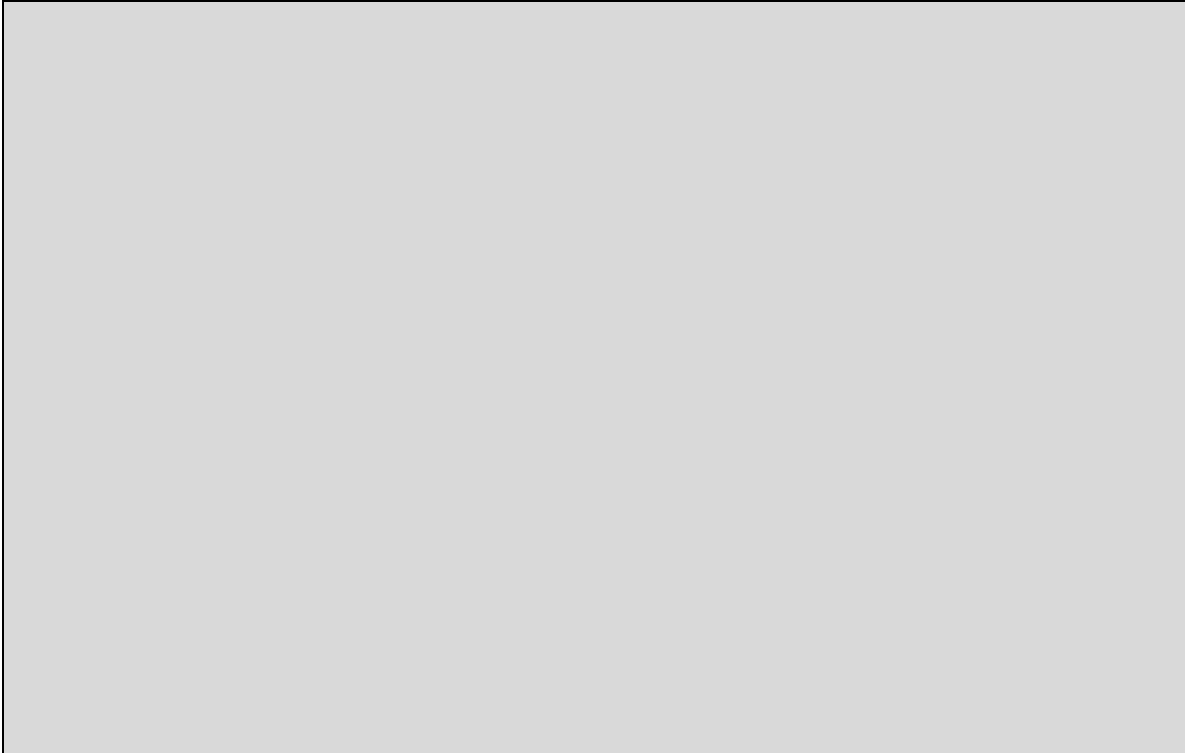
Professional Name	Extension Number	Job Title

2. Forensic Process

*[*This section discusses the steps performed in the investigation process. It describes various actions taken to complete the investigation process.]*

2.1 Tools

*[*Discuss the tools used for completing the forensic evidence analysis, e.g., Wireshark, EnCase Forensic, OSForensics, etc.]*



2.2 Investigation Structure

*[*Investigation process is divided into three parts for the structure and organization of the report.]*

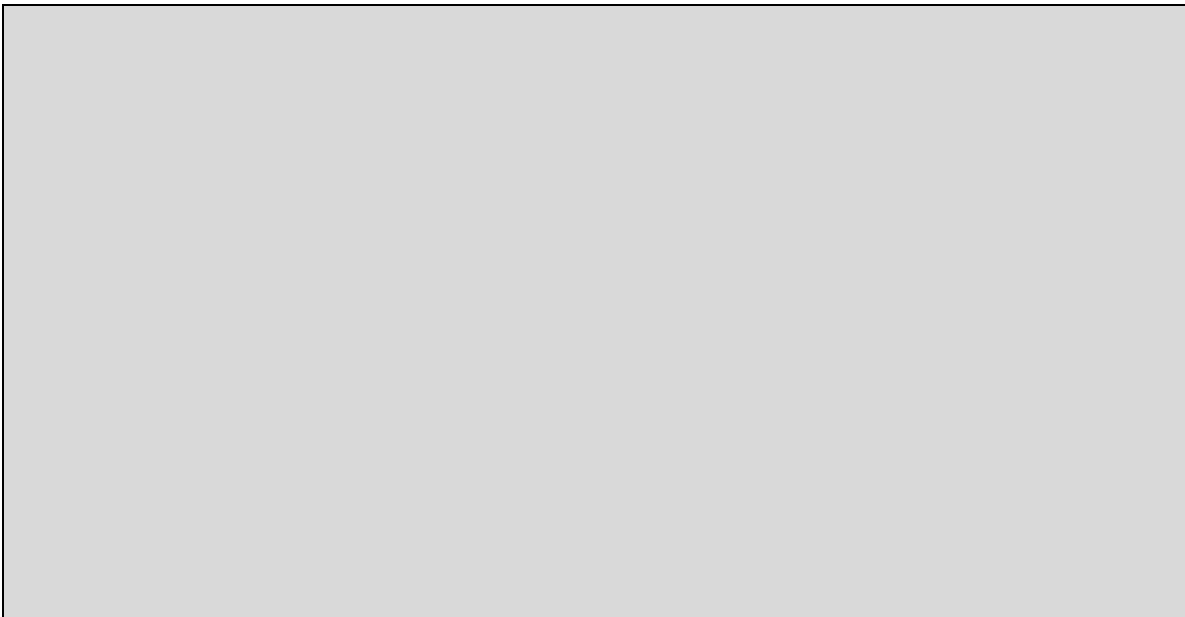
2.2.1 Initial Discovery

*[*Describe the process and tools used for the initial discovery.]*

A large, empty rectangular box with a thin black border, intended for the user to describe the initial discovery process and tools used.

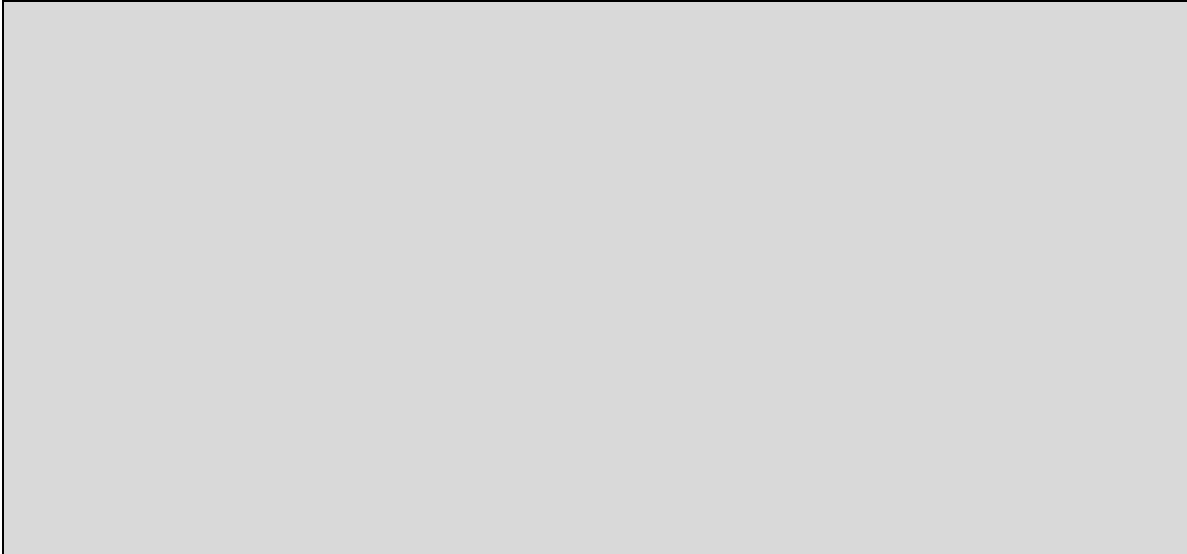
2.2.2 Image Analysis

*[*Based on the gathered evidence describe the process and tools used for evidence analysis]*

A large, empty rectangular box with a thin black border, intended for the user to describe the image analysis process and tools used based on gathered evidence.

2.2.3 Case Report

*[*Discuss the final conclusion after evidence analysis that led to generation of this report.]*



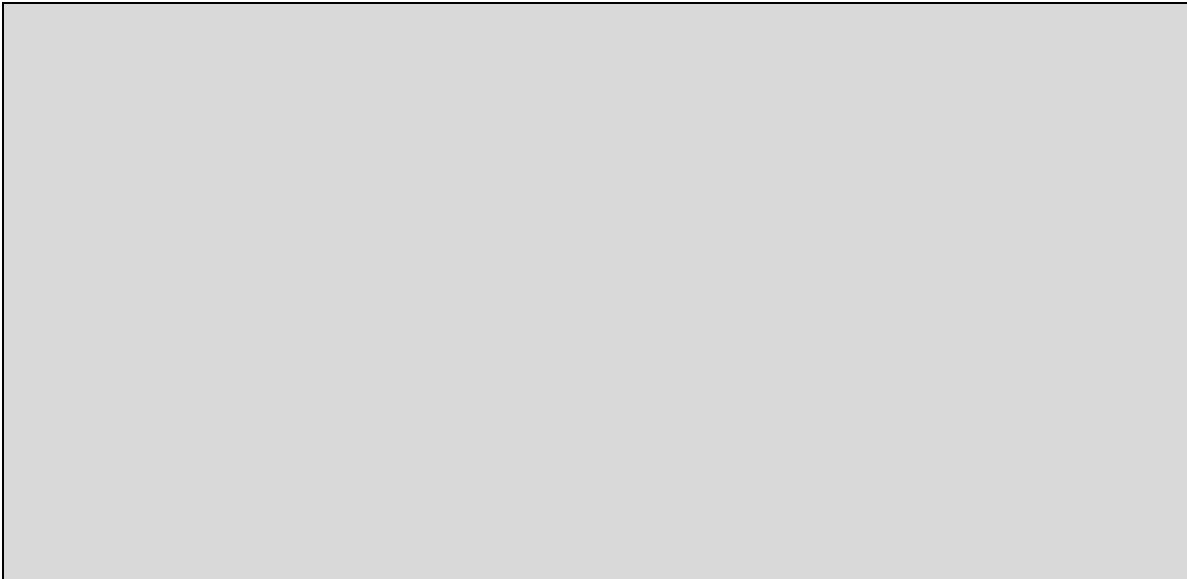
2.3 Procedure

*[*Discuss the procedures followed during the investigation and analysis phase.]*

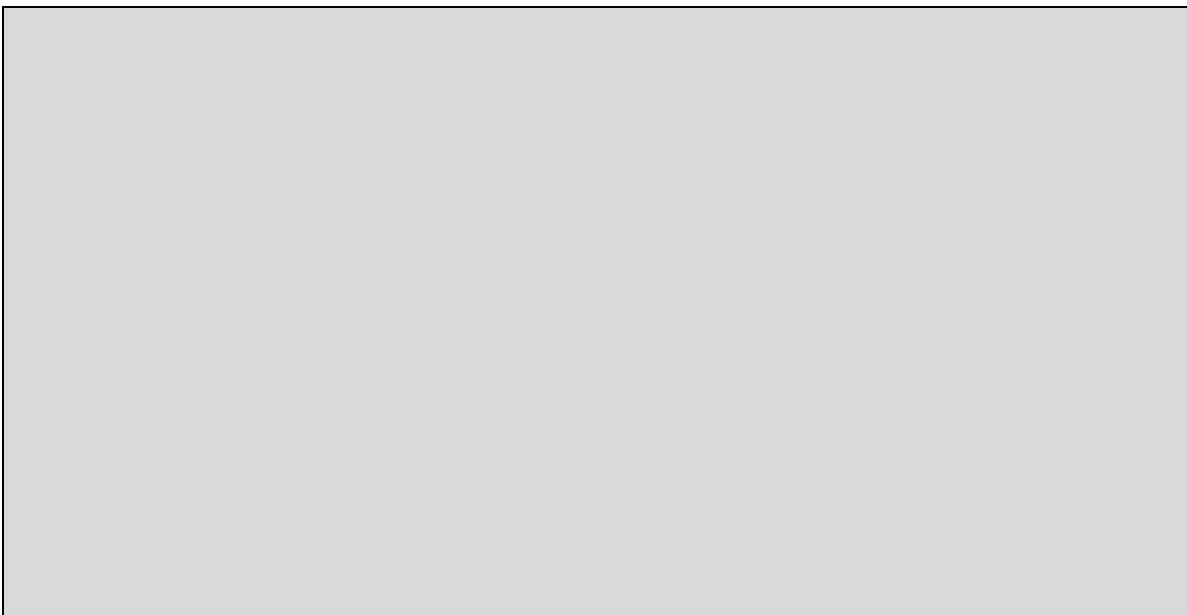
2.3.1 Procedure 1: _____



2.3.2 Procedure 2: _____

A large, empty gray rectangular box with a thin black border, intended for the user to write the details of Procedure 2.

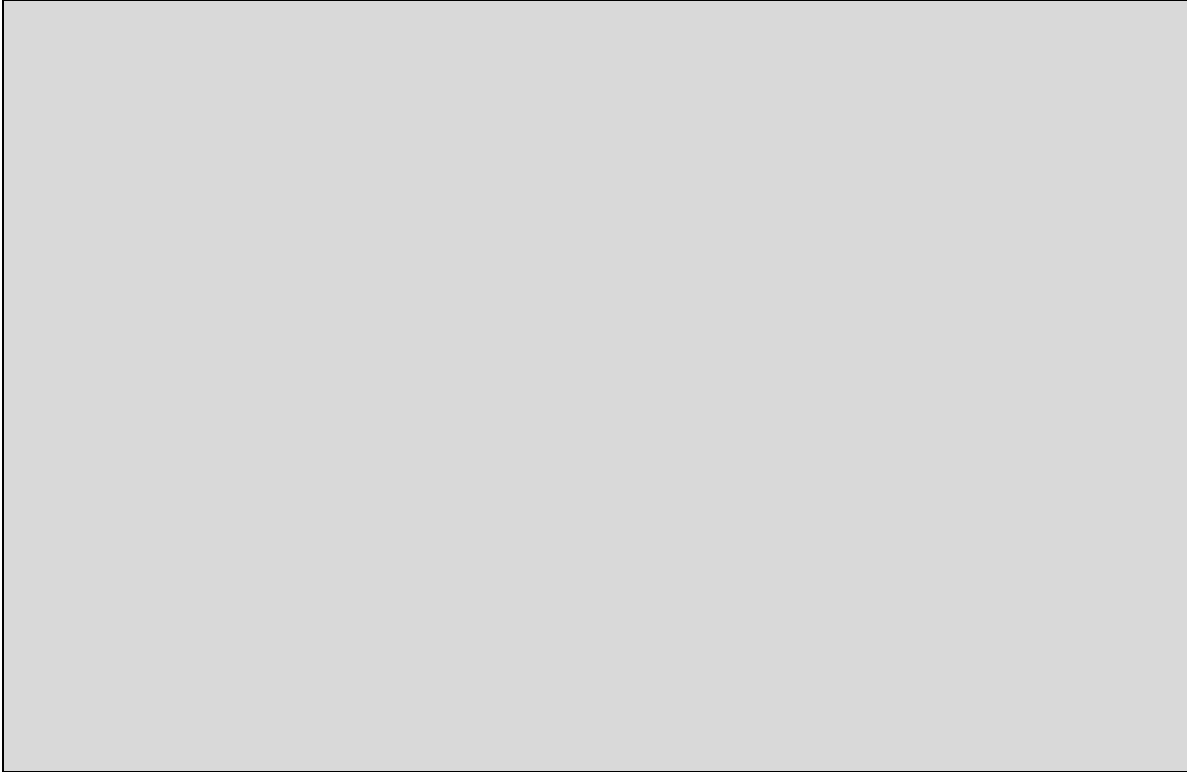
2.3.3 Procedure 3: _____

A large, empty gray rectangular box with a thin black border, intended for the user to write the details of Procedure 3.

3. Results and Findings

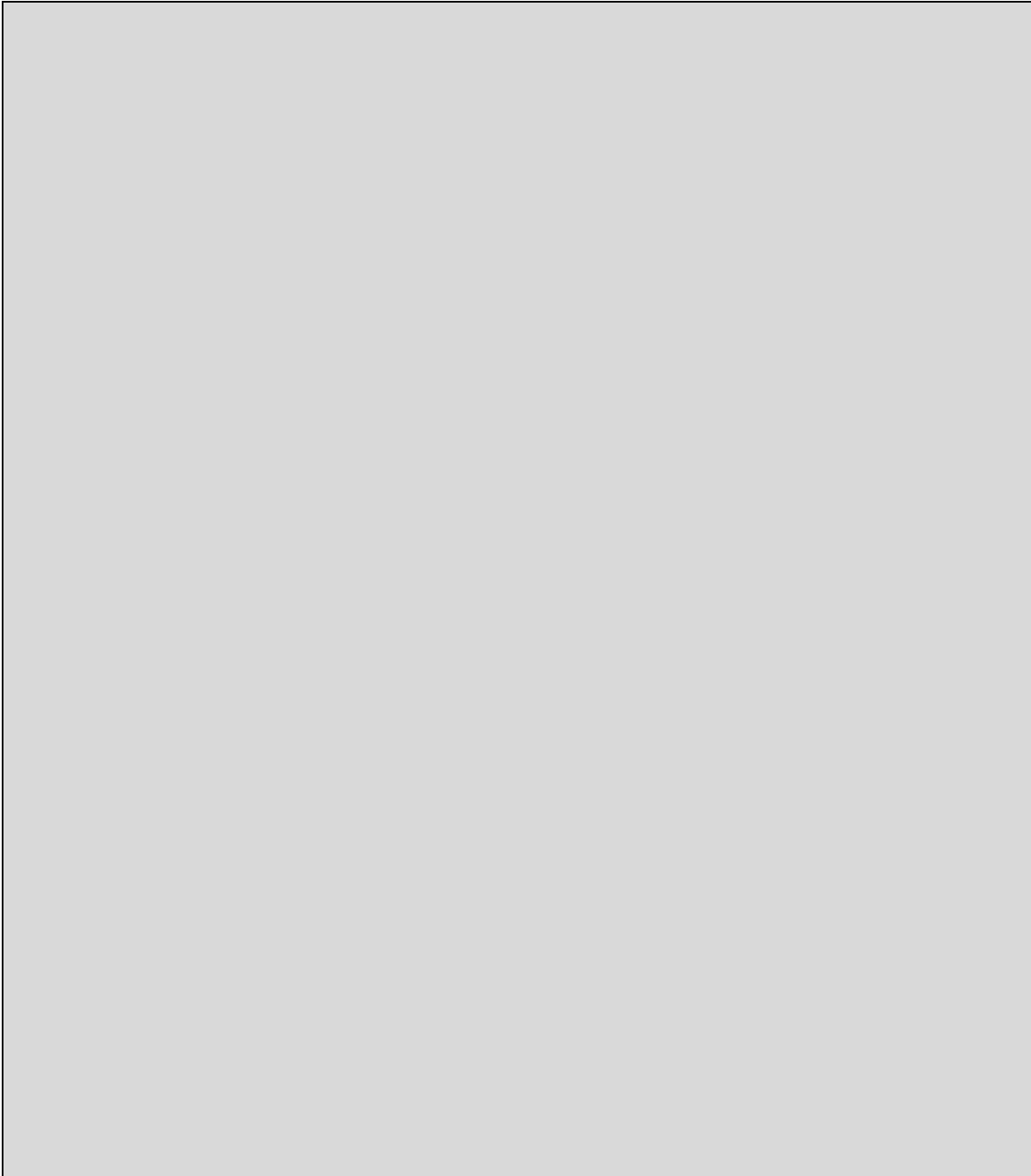
3.1 Summary

*[*Give the overall summary of the investigation process and include final conclusions on the digital crime.]*



3.2 Findings

*[*Discuss the overall findings in the evidence analysis process; you can include screenshots of the tools for proof submission.]*



3.3 Corrective Measures/Recommendations

*[*Based on the forensic analysis investigation report, list out all the corrective measures or actions to be taken to prevent such incidents in future, e.g. Create software restriction policy to restrict access to unauthorized users, Create an account lockout policy, etc.]*

