**Forensics Investigation Report**

(<Case Type>)

Prepared for

<Client>

<Client Address>

<Client City>, <Client State> <Client Zip>

<Client Phone>

Prepared By

**<Agency Name>**

<Agency Address>

<Agency City>, <Agency State> <Agency Country> <Agency Zip>

<Agency Phone>

<Agency Website>

<Agency Tagline>

**Table of Contents**

[INTRODUCTION 4](#__RefHeading___Toc855_215068410)

[1. Nature of incident 4](#__RefHeading___Toc857_215068410)

[1. Location 4](#__RefHeading___Toc859_215068410)

[VICTIMS 4](#__RefHeading___Toc861_215068410)

[1. Victim details 4](#__RefHeading___Toc863_215068410)

[2. Victim Testimony 4](#__RefHeading___Toc865_215068410)

[LOCATION OF EVIDENCE 4](#__RefHeading___Toc867_215068410)

[1. Evidence description 4](#__RefHeading___Toc869_215068410)

[1. System, Network, Server Descriptions 4](#__RefHeading___Toc871_215068410)

[2. Seizure details 4](#__RefHeading___Toc873_215068410)

[3. Handling Details (Chain of Custody) 4](#__RefHeading___Toc875_215068410)

[5. Location of Evidence 5](#__RefHeading___Toc877_215068410)

[DEFINITIONS 5](#__RefHeading___Toc879_215068410)

[1. Definitions 5](#__RefHeading___Toc881_215068410)

[2. Tools 5](#__RefHeading___Toc883_215068410)

[1. License Information 5](#__RefHeading___Toc885_215068410)

[PRESERVATION OF EVIDENCE 5](#__RefHeading___Toc887_215068410)

[1. Validation of Original Evidence 5](#__RefHeading___Toc889_215068410)

[1. Procedures 5](#__RefHeading___Toc891_215068410)

[2. Result 6](#__RefHeading___Toc893_215068410)

[3. Validation 6](#__RefHeading___Toc895_215068410)

[2. Imaging 6](#__RefHeading___Toc897_215068410)

[1. Procedures 6](#__RefHeading___Toc899_215068410)

[2. Result 6](#__RefHeading___Toc901_215068410)

[3. Validation 6](#__RefHeading___Toc903_215068410)

[INITIAL EVALUATION OF THE EVIDENCE 6](#__RefHeading___Toc905_215068410)

[1. Existing Data Details 6](#__RefHeading___Toc907_215068410)

[1. <First data detail>. 6](#__RefHeading___Toc909_215068410)

[2. <Second data detail> 6](#__RefHeading___Toc911_215068410)

[ANALYSIS STEPS 6](#__RefHeading___Toc913_215068410)

[1. Procedures 6](#__RefHeading___Toc915_215068410)

[1. <First procedure followed> 6](#__RefHeading___Toc917_215068410)

[2. <Second procedure followed> 6](#__RefHeading___Toc919_215068410)

[RESULTS 7](#__RefHeading___Toc921_215068410)

[1. Pertinent Document Summaries 7](#__RefHeading___Toc923_215068410)

[1. Document 1 Summary – <document name> 7](#__RefHeading___Toc925_215068410)

[2. Document 2 Summary -<document name> 7](#__RefHeading___Toc927_215068410)

[2. Pertinent Images Summary 7](#__RefHeading___Toc929_215068410)

[1. Image 1 Summary – <name or category of images> 7](#__RefHeading___Toc931_215068410)

[2. Image 2 Summary – <name or category of images> 7](#__RefHeading___Toc933_215068410)

[CONCLUSIONS 7](#__RefHeading___Toc935_215068410)

[1. Summary 7](#__RefHeading___Toc937_215068410)

[2. Activity Summary and Timeline 7](#__RefHeading___Toc939_215068410)

[Appendix A – Software Licenses 8](#__RefHeading___Toc961_215068410)

[Appendix B – Seizure Details 8](#__RefHeading___Toc959_215068410)

[Appendix C – Chain of Custody Forms 8](#__RefHeading___Toc957_215068410)

[Appendix D – System Details 8](#__RefHeading___Toc955_215068410)

[Appendix E – Initial Data Details 8](#__RefHeading___Toc953_215068410)

[Appendix F – Analysis Logs 8](#__RefHeading___Toc951_215068410)

[Appendix G – Supporting Evidence Index 8](#__RefHeading___Toc949_215068410)

[Appendix H – Supporting Evidence Descriptions 8](#__RefHeading___Toc947_215068410)

[Appendix I – Investigator Back Ground (CV) 8](#__RefHeading___Toc945_215068410)

[Appendix J – Citations 8](#__RefHeading___Toc943_215068410)

[Appendix K – Detailed Definitions 8](#__RefHeading___Toc941_215068410)

* INTRODUCTION
  1. Nature of incident

<General description of incident>

* + 1. Location

<Location where incident occurred)

* VICTIMS
  1. Victim details

<Describe victim details here>

* 1. Victim Testimony

<Evidence testimony here>

* LOCATION OF EVIDENCE
  1. Evidence description
     1. System, Network, Server Descriptions
        1. System 1

<Server type, etc.>

* 1. Seizure details

< Seizure details here>.

* 1. Handling Details (Chain of Custody)

<Details here>

* 1. Location of Evidence

<Location details here>

* DEFINITIONS
  1. Definitions

**Acquisition of Digital Evidence:** Begins when information and/or physical items are collected or stored for examination purposes. The term "evidence" implies that the collection of evidence is recognized by the courts. The process of collecting is also assumed to be a legal process and appropriate for rules of evidence in that locality. A data object or physical item only becomes evidence when so deemed by a law enforcement official or designee.

**Data Objects:** Objects or information of potential probative value that are associated with physical items. Data objects may occur in different formats without altering the original information.

**Digital Evidence:** Information of probative value stored or transmitted in digital form. Physical Items: Items on which data objects or information may be stored and/or through which data objects are transferred.

**Original Digital Evidence**: Physical items and the data objects associated with such items at the time of acquisition or seizure.

**Duplicate Digital Evidence:** An accurate digital reproduction of all data objects contained on an original physical item.

**Copy:** An accurate reproduction of information contained on an original physical item, independent of the original physical item.

* 1. Tools

<Tool list here>

* + 1. License Information

<Software license information here>

* PRESERVATION OF EVIDENCE
  1. Validation of Original Evidence
     1. Procedures

<Procedure list here such as hashing of hard drive>

* + 1. Result

<Results here>

* + 1. Validation

<Validation - Acquisition Hash>

* 1. Imaging
     1. Procedures

<Procedure description>

* + 1. Result

<Results here>

* + 1. Validation

<Validation - Acquisition Hash & file integrity>

* INITIAL EVALUATION OF THE EVIDENCE
  1. Existing Data Details
     1. <First data detail>.

<Description of first data detail>

* + 1. <Second data detail>

<Description of second data detail>

* ANALYSIS STEPS
  1. Procedures
     1. <First procedure followed>

<Detail description of first procedure>

* + 1. <Second procedure followed>

<Detail description of second procedure>

* RESULTS
  1. Pertinent Document Summaries
     1. Document 1 Summary – <document name>

<Description of document and events or evidence, e.g., /var/log/secure>

<Attachments here>

* + 1. Document 2 Summary -<document name>

<Description of document and events or evidence>

<Attachments here>

* 1. Pertinent Images Summary
     1. Image 1 Summary – <name or category of images>

<Description of image(s)>

<Attachments here>

* + 1. Image 2 Summary – <name or category of images>

<Description of image(s)>

<Attachments here>

* CONCLUSIONS
  1. Summary

<General summary of the incident>

* 1. Activity Summary and Timeline

<Activity summary of the incident with timelines>

Appendix A – Software Licenses

Appendix B – Seizure Details

Appendix C – Chain of Custody Forms

Appendix D – System Details

Appendix E – Initial Data Details

Appendix F – Analysis Logs

Appendix G – Supporting Evidence Index

Appendix H – Supporting Evidence Descriptions

Appendix I – Investigator Back Ground (CV)

Appendix J – Citations

Appendix K – Detailed Definitions