**PLEASE NOTE: THE UNDERLYING FORMAT OF THIS DOCUMENT WAS GRACIOUSLY PROVIDED TO US BY THE DEFENSE CYBER CRIME CENTER (DC3)/DEFENSE COMPUTER FORENSICS LABORATORY (DCFL) TO ASSIST OUR IT EXPERTS IN PREPARING THEIR REPORTS. WE HAVE MODIFIED IT IN CERTAIN WAYS SO THAT IT IS MORE BROADLY APPLICABLE**

Company Name

Case Name

Case Number

Jane Student, Lead Forensic Examiner

John Doe, Forensic Examiner

Date of Report

1. Executive Summary

State what you were asked to do and list your conclusions. This is the most difficult part of the report for anyone who is new to being an expert, because, frequently, new experts do not want to commit themselves to an opinion. Unfortunately, that is what you are being “paid” to do. **A word of caution**: you are experts in IT Forensics. You are NOT experts in pathology or crime scene investigation and you are NOT allowed to give opinions in those areas. You can ONLY draw conclusions that relate to your particular discipline.

In this section, you want to speak to the big picture and at a high level. Keep in mind that you are telling a story based on facts. Include summarized key facts that will be supported in the next section. You can use bullets to list each of the summarized key facts.

This section is meant to be a table of contents for the sections that follow it. The last sentence of the first paragraph should either say “analysis of the evidence revealed the following:” or “analysis of the evidence revealed nothing relevant to the request.”

**Example:** *Senior Computer Forensic Examiner JOE SMITH, with the assistance of Computer Forensic Technician JACK BLACK, conducted an examination of the submitted evidence media from 21 Aug through 1 Oct 2007. The analysis of the evidence revealed the following:*

The middle of the Executive Summary should list each of the types of information found on the hard drive(s) or other device(s) that you examined. These entries should be separated by type, which can be either file type or category type, depending on the examination. A total number of files found should be included in each of these summary sentences. Each bullet should separated by a blank line.

These bullets should match the boxes listed in **Section 4 Findings and Analyses**.

**Example:** *One file of a known child victim, identified through comparison with the National Center of Missing and Exploited Children (NCMEC) hash set*

**Example:** *537 images of Ebay items.*

**Example:** *Internet related information was obtained and provided.*

1. **Table of Contents**

Executive Summary #

Table of Contents #

Introduction #

Methodology #

Trusted Forensic Workstation and Toolset #

Preparation of the Media #

Physical Handling of Evidence and Chain of Custody #

Acquisition and Verification of Media #

File Systems #

Operating Systems #

Installed Software #

User Accounts #

User Profiles #

My Documents #

My Pictures #

My Videos #

Desktop #

Shortcuts and References #

Internet Related Files – Caches and Cookies #

Recycle Bins and Deleted Files #

Files and Folders Outside of User Profiles #

Event Logs #

Encrypted and Password Protected Files #

Additional items #

Findings and Analyses #

Add subsections as appropriate #

Add subsections as appropriate #

Add subsections as appropriate #

Conclusions #

Supporting Documentation #

Technical Information #

Appendices #

Add additional appendices as appropriate #

Add additional appendices as appropriate #

Add additional appendices as appropriate #

List of Figures #

List of Tables #

1. Introduction

The introduction should provide a broad framework for the report. The introduction should provide the background to the case and state the objectives given to you by your client. The section should mirror the work that is defined in the engagement letter. You may use the Introduction from the Problem Set for this part of the report. If the State retained you, use paragraphs one and three. If the Defense retained you, use paragraphs one and two.

1. Methodology

The methodology section lays the foundation for the entire expert report and the conclusions formed by the IT experts. This section of the report is just as important as the results section. A well-written and thorough methodology is critical to the IT expert’s success. This section must explain to the reader, who is often a non-technical, layperson, the steps that were followed by the IT expert to acquire, preserve, recover, and analyze the data. The methodology section must show all of the steps that were followed to recover data and reach conclusions. This is essential for two reasons:

* + - 1. The trier of fact often has a non-technical background and he/she must be able to follow the logical steps that you followed. This means the IT expert must write about a technical subject using language which is understandable by a non-IT person.
      2. The procedure must be reproducible so another IT expert could follow the exact same steps and reach the exact same conclusion. If another IT expert cannot follow the procedures, the conclusions may not be reliable.

This is where you will identify:

* The forensic platform (including the make/model of the forensic computer that you used, its operating system, the virus scanning software, and the acquisition system)
* The procedures you followed to conduct your investigation. These procedures should be presented in a logical, orderly fashion. The purpose is to show a list of steps that are reproducible by another forensic expert.
* Additional software used in your investigation.
* Keep in mind that throughout this section, you must (1) define all technical terms in a way that can be understood by non-technical individuals and (2) describe exactly how each process works. For example, with respect to the term “MD-5 Hash Value,” you must define it and tell the reader its purpose. Frequently, this is accomplished by using an analogy. With respect to the software used by the forensic examiner in the analysis, such as Guidance Software’s *EnCase*, you must tell the reader exactly what the program does, and then explain, step-by-step, exactly how you used it.
* With respect to the latter, you must define/describe, at a minimum, the following terms:
* Bitstream Image
* Cache
* Cookie
* File Slack
* Hex Editor
* Index.dat File
* Link File
* MAC Times
* Malicious Files
* Metadata
* Swap File
* Temporary File
* Unallocated Space
* Write Blocking
* Forensic Image
* Verification Process
* User Profiles
* Keyword Searches
* Manual Review
* EnScripts
* The Registry
* Hash Values
* Hash Analysis
* File Signature
* File Signature Analysis
* Recycler/Info 2 Record Analysis
* User Account Analysis
* User Content Analysis
* Date/Time Analysis

The above is in no particular order; it is simply a list of topics that you must address. It is up to you to organize the material in the way that makes the most sense. In terms of formatting, it is best to drop footnotes that contain the definitions/analogies so that your reader is not required to flip back and forth between the text and a glossary.

Below is a high level outline of the sections that should be included in the expert report. IT experts may wish to add sections as necessary. The overarching theme of creating a logical, orderly, and repeatable methodology should provide the guiding framework.

4.1 Trusted Forensic Workstation and Toolset

4.2 Preparation of the Media

4.3 Physical Handling of Evidence and Chain of Custody

4.4 Acquisition and Verification of Media

4.4 File Systems

4.5 Operating Systems

4.6 Installed Software

4.7 User Accounts

4.8 User Profiles

4.8.1 My Documents

4.8.2 My Pictures

4.8.3 My Videos

4.8.4 Desktop

4.8.5 Shortcuts and References

4.8.6 Internet Related Files – Caches and Cookies

4.8.7 Recycle Bins and Deleted Files

4.9 Files and Folders Outside of User Profiles

4.10 Event Logs

4.12 Encrypted and Password Protected Files

4.13 Additional items

**Example starting paragraph:** *Forensic imaging, examination, and analysis were conducted in the following manner.*

1. Findings and Analyses

This section includes a step-by-step presentation of the key facts of the examination, including the hardware and software that you used. The key facts section will include grammatically-correct sentences organized into paragraphs. You will need to list all recovered material. Equally important is to list an analysis of the recovered materials. You may need to tie several artifacts together to make your analysis. For example, a recovered document may have important time/date stamps, a corresponding shortcut in the “My Recent Documents,” and important file ownership attributes.

**Recovered Files**For each exhibit or set of exhibits you must, at a minimum, answer the following questions:

1. What did you find?
2. Where did you find it? Make sure you explain any terms that may not be understood by the reader (e.g., web cache, shortcuts, profiles, user accounts).
3. What do the recovered files mean to the case? Make sure you explain any terms that may not be understood by the reader (e.g., time stamps, file ownership). This is an important step.
4. Where did you put the item(s) in the media that accompanies the report? Explain that it is found in the Exhibits folder in the zip file or DVD. (For an online course, use a zip file to bundle all exhibits together. It is not necessary to burn a DVD.)

Files that have major significance to the case should be described individually, as shown below. When a large number of files have been recovered; e.g., files from a web cache, place the names of the files in a table or in a Microsoft Excel spreadsheet that accompanies the report. Be certain to label the columns. As with most exhibits that consist of files, MAC times must be included. Explain MAC times in the first instance that you refer to them. The goal is to have all case information in a single report, but this is flexible depending on the type of information presented.

The “Exhibit Description” gives a general category to which the exhibit belongs. Examples of “Exhibit Descriptions” include Child Pornography, Malicious File, Virus, Text File, Word Document, and others.

**Exhibit Descriptions**

**Exhibit 3**

|  |  |
| --- | --- |
| Filename:  Location:  File created:  Entry modified:  Last accessed:  Hash value:  Exhibit Description:  Significance: | Special File.docx  C:\Documents and Settings\Username\My Documents\  02/12/06 04:43:54PM  02/12/06 04:43:54PM  02/12/06 04:43:54PM  0621dbed29da2976fb7c67fb36af3035  This Microsoft Word 2007 document contains correspondence between person X and person Y regarding the purchase of plutonium.  This file was created one day after an e-mail was sent between person X and person Y. |

**Exhibit 4 – Files Recovered from C:\Stuff\**

Remember, when a large number of files have been recovered; e.g., files from a web cache, place the names of the files in a table or in a Microsoft Excel Spreadsheet that accompanies the report. Be certain to use column headers so the reader will understand what is contained in each column. If you use a Microsoft Excel Spreadsheet, direct the user to the spreadsheet with a sentence similar to: *For a list of all files from the web cache, please see Recovered\_Files.xlsx, which is contained in the media.zip file.*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Filename | Original Location | Hash Value | Time Stamps | | | Location of file in accompanying media |
| File Created | Entry Modified | Last Accessed |
| File1.doc | C:\stuff\ | 0621dbed29da2976fb7c67fb36af3045 | 02/12/06 04:43:54PM | 02/12/06 04:43:54PM | 02/12/06 04:43:54PM | Zip folder\Exhibit 1\ |
| File2.xls | C:\stuff\ | 8951dbed29da2976fb7c67fb36af3068 | 02/12/06 04:58:54PM | 02/12/06 02:43:12PM | 02/12/06 02:43:12PM | Zip folder\Exhibit 1\ |
| Web.htm | C:\stuff\ | 7341dbed29da2976fb7c67fb36af3079 | 02/12/06 03:58:54PM | 02/12/06 12:43:24PM | 02/12/06 12:43:24PM | Zip folder\Exhibit 1\ |

**Exhibit 5 – Recovered Images**

In some cases, pictures may be recovered from a suspect’s hard drive or other electronic device. Where it makes sense, a copy of the picture should be shown.

|  |  |
| --- | --- |
| Filename:  Location:  File created:  Entry modified:  Last accessed:  Hash value:  Description:  Significance: | Picture1.jpg  C:\Documents and Settings\Username\My Documents\My Pictures\  02/12/06 04:43:54PM  02/12/06 04:43:54PM  02/12/06 04:43:54PM  0621dbed29da2976fb7c67fb36af3035  This file contains a picture of the subject’s house.  This file identifies the contents of the subject’s bookcase.  [LetterA](NULL) |

**Exhibit 6 – Recovered Images**

When creating a report with contraband, remove the contraband images and insert an “Image Removed” image instead of the actual image. This tells the reader that there was an image presented, but it was removed because its distribution is illegal. One “Image Removed” image should be used for each image replaced.

|  |  |
| --- | --- |
| Filename:  Location:  File created:  Entry modified:  Last accessed:  Hash value:  Description:  Significance: | PictureX.jpg  C:\Documents and Settings\Username\My Documents\My Pictures\  02/12/06 04:43:54PM  09/27/09 08:13:21PM  02/12/06 04:43:54PM  0621dbed29da2976fb7c67fb36af3035  This file contains suspected child pornography.  The timestamps of this file indicate that…  [Icon Image Removed](NULL) |

|  |  |
| --- | --- |
| Filename:  Location:  File created:  Entry modified:  Last accessed:  Hash value:  Description: | {6918FC25-8D20-4974-AD40-F25AC05B1E21}.jpg  C:\Documents and Settings\Philip Smell\Local Settings\Application Data\Microsoft\Media Player\Art Cache\LocalMLS\  02/12/06 04:43:54PM  09/27/09 08:13:21PM  02/12/06 04:43:54PM  0621dbed29da2976fb7c67fb36af3035  This image was a small screen shot from the movie file “\_little girls mix (lolitas-preteens-reelkiddymov-r@ygold-hussyfans-underage-girls-children-pedofilia-pthc-ptsc-xxx-sexy).mpeg” (Exhibit X). It was found within a Windows Media Player art cache folder indicating the movie file had been viewed on 02/12/06 at 04:43:54PM using Windows Media Player.  [Icon Image Removed](NULL) |

**FAQ**: “How do I choose which images to put in the report?” This is within the examiner’s discretion. You could choose one image from each victim if you have known victims, you could choose the first 20 according to MAC times, or you could randomly choose one file from each folder.

**FAQ**: “How will the reader know about an image if it’s removed in the Sanitized Report?” For all exhibits, you must include a description of the item. For example, “This image shows a prepubescent male and female engaged in a sexual act.”

**FAQ**: “What if there are no findings?” There is no such thing as “no findings.” With every case, you DO something, so produce some sort of product. “

1. Supporting Documentation

This section outlines all information in the report media; i.e., the zip file or DVD that accompanies the report, which came from outside sources. For example, it may be necessary to show BIOS information; this material may not have come from the digital media, but it is important to document it nonetheless. You may want to list references to the National Center for Missing and Exploited Children’s database, if you were analyzing suspected child pornography. If you reference material from the Internet or cite sources of information from a knowledgebase to substantiate your argument, you should list those references here.

You may not list supporting documents that you do not reference elsewhere

|  |  |
| --- | --- |
| Icon Folder  **NCMEC** | **You must answer WHY each of these folders is included in this section.**  **Example:** *This folder contains files that match the hash values from the National Center for Missing and Exploited Children (NCMEC) database. The files are in the subfolder that is named to correspond to the tag where the evidence was located. These images are CONTABAND.* |

|  |  |
| --- | --- |
| Icon Folder  **Known files** | **You must answer WHY each of these folders is included in this section.**  **Example:** *This folder contains a list of known good files contained within an operating system as recorded by the National Institute of Standards and Technology.* |

1. Technical Information

This section outlines information obtained by using forensic processes and tools. Things such as a Registry report, file listing, and malware information are included here. Remember, you must define all of these terms in non-technical ways.

At the end of the paragraphs in this section include the sentences: “The files located in these folders are provided so that a technical reader can review technical information pertaining to the case. The information within each file contains results from forensic processes.”

**Example Section 7 starting paragraphs:** *This section contains technical information directly outputted from forensic tools.*

*The files located in these folders are provided so that a technical reader can review technical information pertaining to the case. The information within each file contains results from forensic processes.*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Icon Folder  **Registry Information** | Folder containing files of registry listings. Note that not all the information from Registry Viewer is included.   |  |  | | --- | --- | |  | | | **Description (Tag Item)** | | | **Registered Owner** | Text | | **Registered Organization** | Text | | **Product Name** | Microsoft Windows XP (Version xxxxx) | | **Install Date** | 00 Aug 07, 00:00:00 | | **Shutdown Time** | 00 Aug 07, 00:00:00 | | **Standard Time Zone** | Eastern Standard Time | | **Daylight Time Zone** | Eastern Daylight Time |  |  |  | | --- | --- | |  | | | **Description 2 (Tag Item 2)** | | | **Registered Owner** | Text | | **Registered Organization** | Text | | **Product Name** | Microsoft Windows XP (Version xxxxx) | | **Install Date** | 00 Aug 07, 00:00:00 | | **Shutdown Time** | 00 Aug 07, 00:00:00 | | **Standard Time Zone** | Eastern Standard Time | | **Daylight Time Zone** | Eastern Daylight Time | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Icon Folder  **Malware**  **Information** | Folder containing information about malware or the malware itself. Note that only malware information that has a direct influence on the case should be written here in the report. All other malware should be kept in the report media.   |  |  | | --- | --- | |  | | | **Description (Tag Item2)** | | | SAV reported 3 threats in 77 files of 69,173 files scanned. | | | **Threat** | **Description** | | ThreatName1 | Description1 | | ThreatName2 | Description2 | | ThreatName3 | Description3 |  |  |  | | --- | --- | |  | | | **Description (Tag Item2)** | | | SAV reported 2 threats in 66 files of 58,062 files scanned. | | | **Threat** | **Description** | | ThreatName1 | Description1 | | ThreatName2 | Description2 | |

|  |  |
| --- | --- |
| Icon Folder  **File Listings** | Folder containing file listings. Explain that where the file listings came from.  **You must answer WHY each of these folders is included in this section.**  **Example:** *This folder contains an Access database of all files for each evidence item. The database contains the file properties of each file, including MAC times and file paths.* |

|  |  |
| --- | --- |
| Icon Folder  **Notes** | **You do not have to put the Notes folder and the Notes file links in the same report.**  **Example:** *This folder contains Examiner Notes, which is a detailed technical report in chronological order of the forensic analysis of the evidence media.* |

|  |  |
| --- | --- |
| Icon Text Document  **Evidence List** | This document is nothing more than a table of tag numbers and descriptions of evidence items. This is the section where you list the evidence items, their model number, and serial number. If there is any question about the Tag or Item number, then explain what the issue was. For example: “Tag 4 was not used because the number is bad luck (additional information in the description of tag number 5 below).”  **Example:** *The Evidence list document contains a table of tag numbers and descriptions of individual pieces of evidence pertaining to the case.* |

|  |  |
| --- | --- |
| Icon Text Document  **Examiner Notes** | Examiner notes.  **Example:** *The Examiner Notes document contains a detailed technical report in chronological order of the forensic analysis of the evidence media.* |

|  |  |
| --- | --- |
| Icon Text Document  **Technician Notes** | Technician Notes. Notice that the icon is different because we are linked directly to a file rather than a folder.  **Example:** *The Technician Notes document contains a detailed technical report in chronological order of the forensic preparation of evidence media.* |

|  |  |
| --- | --- |
| Icon Text Document  **Chain of Custody Forms** | Chain of Custody Forms. This section should list a copy of the forms used to document the chain of custody. |

**FAQ**: “Aren’t the evidence items described in the Examiner Notes?” Yes, in greater detail; however, the Evidence List linked in this section gives a brief snapshot of all evidence tags in an easy-to-read list.

**FAQ**: “Do we have to put the model and serial number in the Evidence List?” Yes, because we have to tie the media back to the original evidence.

**FAQ**: “What if multiple Examiners are working on a case?” There is only one Laboratory Report created per case no matter how many Examiners or Technicians worked on the case.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

YOUR NAME

Lead Computer Forensic Examiner

Attachment 1 – Report Layout Information

This report template can simply be cut-and-pasted or typed into directly, but should you need to ensure that your format is correct, use the following specifications.

Throughout the document the font size is 12 pt. The font style is Times New Roman. The margins are set at 1” at the top and bottom and 0.75” on the left and right. The display boxes all have a fixed table width of 7.5.” The header is 0.4” from the top edge and the footer is 0.25” from the bottom edge. The section titles (i.e. **1. Executive Summary**) are all 16 pt size and bold. Special handing notice information is located on the cover page of the document because the report is transmitted in hard copy.

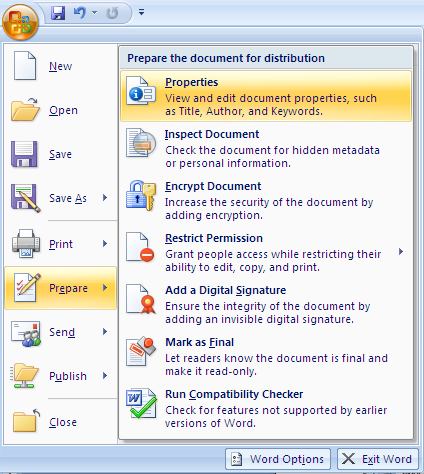
The header and footer repeat throughout the entire document. There should be no need to modify the footer.

Cover Page: The font style is Times New Roman style. The top block including the case number and requestor’s case number is bold and 16 pt size.

All primary tables have a width of 7.5 inches. Row height and column width can be modified at the writers’ discretion. In addition, height and width of embedded tables are not restricted.

Attachment 2 – File Properties

When creating reports, ensure that you modify the file properties.

1. Go to the Office Button 🡪 Prepare 🡪 Properties  
     
   
2. Change the Author, Subject, and Keywords.  
     
   