Digital Forensics and Cyber Investigation Report

Your name

University of Maryland Global Campus

DFCS 605: Digital Forensics and Cyber Investigation Foundations

Instructor’s name

Due date

# Project: Digital Forensic Investigation

## 1. Summary

In response to the request from M. Smyth, a junior analyst at the Security Operations Center (SOC), a forensic examination was conducted on the USB flash drive discovered near the hotel desks used by the Sales and Marketing Teams. The analysis aimed to identify executable files, compare them against known threat indicators from a recent Threat Intel Report, determine the timestamps of file transfers, ascertain the likely owner of the USB device through metadata examination, and highlight any noteworthy findings with corresponding recommendations.  
After a meticulous forensic examination of the provided digital image, no executable files were identified that align with the criteria specified in the recent Threat Intelligence Report. This comprehensive analysis indicates an absence of the particular malware artifacts detailed in the report.2. List of Evidence

## 2. List of Evidence

*This section should include a list of the evidence that was analyzed along with their hashes. Each item should be on its own row.*

The evidence analysed in this case included the items listed in Table 1.

## Table 1: Evidence

|  |  |
| --- | --- |
| Item / File | Hashes |
| Image\_Project.E01 | MD5: 8ef137042f948e977e000a456cc121a0  SHA1: c2bc77285fadfed457c973bb255fc724d5d2327e |

## 3. List of Forensic Tools

*This section should contain a list of the forensic tools that were used along with their version numbers. Do not list tools that are not forensic tools, e.g., Microsoft Word.*

The tools listed in Table 2 were used to analyze evidence.

## Table 2: Forensic Tools

|  |  |
| --- | --- |
| Tool | Version Number |
| Forensic ToolKit (FTK) | 4.7.2.11 |
|  |  |
|  |  |

## 4. Explanation of Work

*This section should be several paragraphs long and should include a description of the analysis that was performed. For example, this section might include paragraphs that state evidence was hashed, a file signature analysis was performed, keyword searches were performed, and that the evidence was hashed at the end of the investigation to show the evidence had not changed. It is not necessary to explain how to log into the virtual machine or how to launch an application.*

## 5. Results

*This section should contain the results of the analysis from the investigation. Findings should be supported by screenshots where appropriate. An example of a screenshot is shown below. All figures should be labelled and there should be a brief explanation of what is in the figure.*

*Figure 1 shows the file signature for the file named alpha.jpg as seen in FTK Imager.*

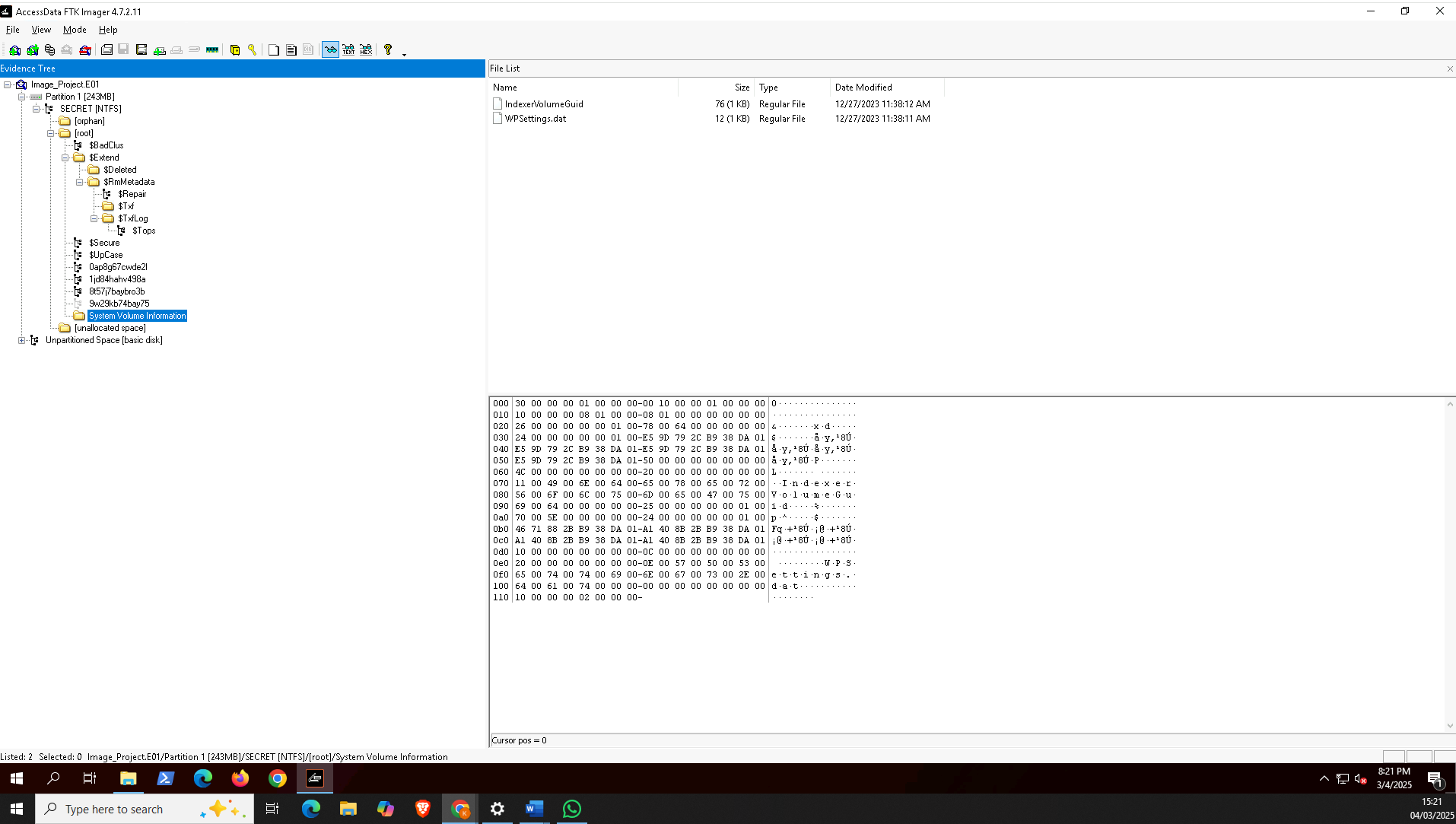
*Figure 1: File signature for alpha.jpg*

A computer screen shot of a file

Description automatically generated

*Figure 1 shows the directories that the content files were not found*

*Figure 1: File file.jpg.*



## 6. Recommendations

*This section should contain recommendations which resulted from the examination.*

*The first paragraph should list any recommendations for additional evidence that should be seized. For example, if it is suspected that there may be value in examining additional computers, logs, etc., those items should be listed. The request should be as specific as possible.*

*The second paragraph should include any recommendations for securing related computer systems. For example, if configurations should be changed, then they should be listed. If network traffic should be analysed for files, then those items such as network file signatures, should be listed.*

## 7. Chain of Custody Form

*A chain of custody form should be included with the report. The chain of custody form should document each person who handled the evidence from the time the evidence collected to the time it was analysed to the time the evidence was returned to the evidence custodian. You my use your instructor’s name as the name of the evidence custodian.*

# Chain of Custody Form

|  |  |
| --- | --- |
| Description of Evidence |  |
| Manufacturer |  |
| Model |  |
| Serial Number |  |
| Markings |  |
| Notes |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Date / Time | Released by | Received by | Reason for Transfer |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## 8. References

*If references were used, then this list should be updated.*

Author’s last name, Initial(s). (Year of publication). *Title of the book*. Publisher. <https://doi.org/DOI>

Author’s last name, Initial(s). (Year of publication). Title of the article. *Title of Journal*, *Volume* (Issue), Pages. <https://doi.org/DOI>

Author’s last name, Initial(s). (Year, Month Day of publication). *Title of the work*. Website. <https://URL>

Author’s last name, Initial(s). (Year of publication). Title of the article. *Newspaper*. <https://URL>

Last name, Initial(s). [Channel]. (Year, Month Day of publication). *Title of the video* [Video]. Website. <https://URL>

Organization. (Year of publication). Word. In *Dictionary*. Publisher. https://URL

**References**

<add your references below using the format examples shown as needed>

Author’s last name, Initial(s). (Year of publication). *Title of the book*. Publisher. https://doi.org/DOI

Author’s last name, Initial(s). (Year of publication). Title of the article. *Title of Journal*, *Volume*(Issue), Pages. https://doi.org/DOI

Author’s last name, Initial(s). (Year, Month Day of publication). *Title of the work*. Website. https://URL

Author’s last name, Initial(s). (Year of publication). Title of the article. *Newspaper*. https://URL

Last name, Initial(s). [Channel]. (Year, Month Day of publication). *Title of the video* [Video]. Website. https://URL

Organization. (Year of publication). Word. In *Dictionary*. Publisher. https://URL