Lab – USB Forensic Analysis
Instructor: Tesfaye W. Lemma

Lab - USB Forensic Analysis

This project documents a forensic analysis of a USB storage device conducted as part of an incident response exercise. The objective was to acquire and examine the contents of the USB device in a forensically sound manner, ensuring data integrity throughout the process. Using industry-standard forensic tools, the investigation focused on imaging the device, verifying cryptographic hashes, and analyzing the acquired image to identify file activity and potential indicators of compromise, following established incident response and digital forensics practices.

Tools Used

- FTK Imager
- Autopsy
- Windows Registry

Incident Response Report
USB Forensic Analysis

Nathalia Nathanson Bolinja

NWIT 247 – Introduction to Incident Response

Instructor: Tesfaye W. Lemma

December 16, 2025

Incident Response Report

Executive Summary

On December 16, 2025, at 8:37 PM EST, a forensic investigation was initiated on a USB device as part of NWIT 247 Project II. The objective of this investigation was to create a forensic image of the USB device using FTK Imager. The USB device was imaged in a safe environment to ensure the integrity of the original evidence. This image was created in a RAW format and using cryptographic hash values (MD5 and SHA1), was generated to confirm integrity. Later, the Autopsy tool analyzes the image created by FTK Imager to review user activity and document any potential indicators of compromise.

Examination Details

- Date: December 16, 2025
- Time: 8:37 PM EST
- Examined Media: USB Storage Device
- Examination Type: Forensic Imaging and Analysis

Methodology:

Before inserting the USB device, write protection was enabled on the system using the Windows Registry (StorageDevicePolicies) to avoid any alteration to the original data. This action guarantees the evidence will not change during the process.

FTK Imager was used to create a physical image of the USB device in RAW (dd) format. The image was created without compression to ensure an exact copy of the device. MD5 and SHA1 hash values were generated and verified after the acquisition to confirm the integrity of the image. Autopsy was used to analyze the image created by the FTK Imager. The investigation involved examining the files, deleted files, images, files system and timeline analysis.

Examination Timeline (EST)

December 16, 2025, at 8:37 PM EST:

Forensic examination initiated.

December 16, 2025, at 8:38 PM EST:

Write protection enabled via Windows Registry prior to evidence insertion.

December 16, 2025, at 8:43 PM EST:

Suspect USB device inserted under a write-protected state.

December 16, 2025, at 8:43 PM EST:

The operating system automatically mounted the USB device via Windows AutoPlay. No files were accessed or modified.

December 16, 2025, at 8:44 PM EST:

FTK Imager was launched with administrative privileges.

December 16, 2025, at 8:48 PM EST:

The USB physical drive was added as evidence in FTK Imager.

December 16, 2025, at 8:52 PM EST:

FTK Imager started the physical acquisition of the USB device.

December 16, 2025, at 10:46 PM EST:

FTK Imager completed the physical acquisition of the USB device; MD5 and SHA1 hash values were verified.

December 16, 2025, at 10:48 PM EST:

The USB device was safely removed after successful acquisition.

December 16, 2025, at 10:57 PM EST:

Autopsy data source configuration was initiated.

December 16, 2025, at 10:58 PM EST:

The disk image was selected as the data source in Autopsy.

December 16, 2025, at 10:59 PM EST:

The USB forensic image (USBForensics-247.001) was selected as the data source in Autopsy.

December 16, 2025, at 11:05 PM EST:

Autopsy ingest process started with the selected ingest modules.

December 16, 2025, at 11:08 PM EST:

Autopsy completed the ingestion and initial analysis of the USB forensic image.

December 16, 2025, at 11:26 PM EST:

Report preparation was completed.

Incident Response Lifecycle

1. Preparation

Before starting the analysis, the system was prepared to ensure an appropriate forensic process. Write protection was enabled in Windows Registry, using (StorageDevicePolicies), before inserting the USB device to avoid any changes to the original data.

2. Detection and Analysis

FTK Imager and Autopsy were used to acquire and analyze the USB device. Hash values were verified, and the image was reviewed without altering the original data.

Tools Use

FTK Imager and Autopsy were used for this examination. The FTK Imager was used to create a bit-for-bit copy of the USB device in a safe environment, and the Autopsy was used to review the image created by the FTK Imager, allowing the file system, files, and timeline activity to be examined.

Autopsy Analysis

Autopsy was used to examine the forensic image, focusing on the contents of the USB device, file activity, and available files through timeline analysis.

December 16, 2025, at 10:57 PM: Preparing the Image for Analysis

The forensic image was configured as a data source in Autopsy to ensure that the correct file was selected and ready for processing.

December 16, 2025, at 11:05 PM: Analysis Started

A limited set of ingest modules was used to identify file types and review basic file activity.

December 16, 2025, at 11:16 PM: Analysis Completed

Autopsy completed the analysis of the forensic image. The files and partitions were identified, and no confirmed indicators of compromise were found.

December 16, 2025, at 11:26 PM: Report Preparation

After completing the analysis, the results were documented in this report.

Findings

The forensic analysis identified the following file categories on the USB device:

- Images: 8,131 files
- Videos: 318 files
- Audio files: 2,114 files
- Databases: 30 files

Recommendations

User Awareness Training

Training users is one of most effective ways to reduce security risks. Users should understand why USB devices can be dangerous and be encouraged to avoid connecting unknown or unapproved media.

USB Usage Blockers

Limiting USB device use adds an extra layer of protection and helps prevent accidental infections and unauthorized data transfers.

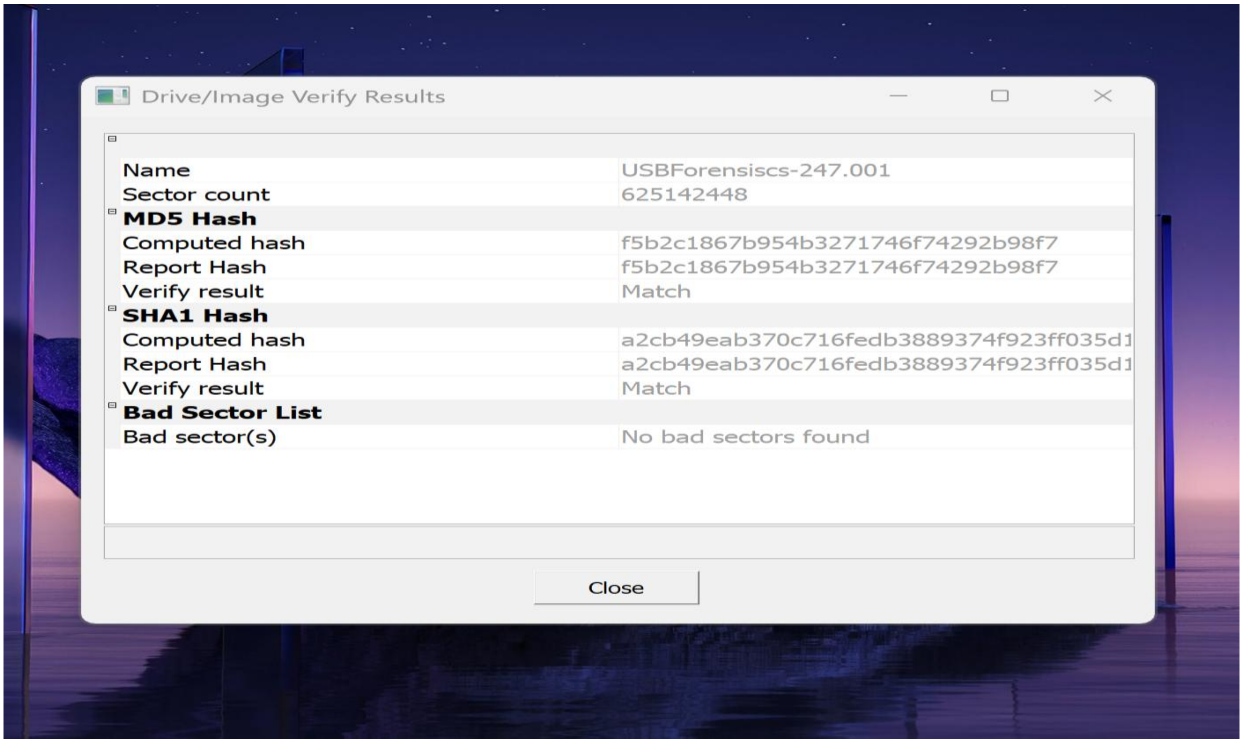
Monitoring Tools – Windows Event Views; SIEM

Basic monitoring and logging help identify unusual activity early and support faster response to security issues.

Appendices

- Autopsy — Forensic tool used to analyze the disk image and review artifacts.
- FTK Imager — Tool used to create a forensic image and verify data integrity.
- Write Protection — Prevents changes to original evidence during acquisition.
- Registry — Windows system database used to manage configuration settings.
- Hash Values (MD5, SHA1) — Used to confirm the integrity of forensic images.
- Metadata — Information about files, such as creation and modification times.
- USB — Removable storage device examined in this investigation.
- ZIP, PDF, HTML — Common file formats encountered during analysis.
- UTC — Standard time reference used for consistent timestamps.

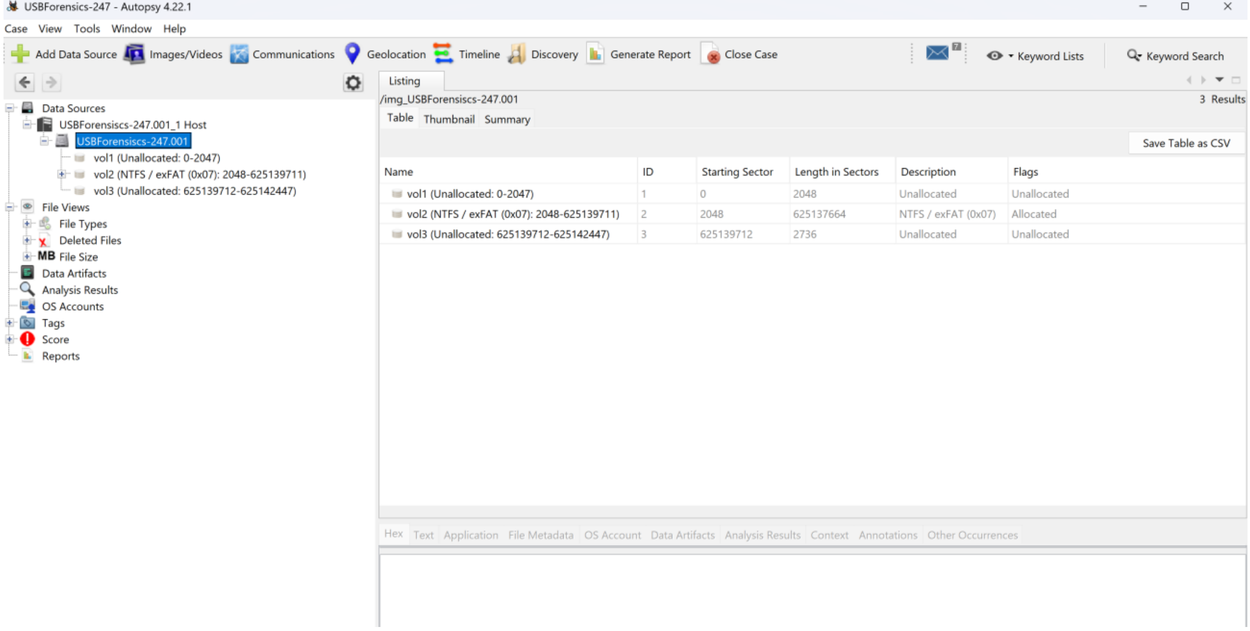
FTK Imager and MD5 Hash and SHA1 Hash:



Name	USBForensiscs-247.001
Sector count	625142448
MD5 Hash	
Computed hash	f5b2c1867b954b3271746f74292b98f7
Report Hash	f5b2c1867b954b3271746f74292b98f7
Verify result	Match
SHA1 Hash	
Computed hash	a2cb49eab370c716fedb3889374f923ff035d1
Report Hash	a2cb49eab370c716fedb3889374f923ff035d1
Verify result	Match
Bad Sector List	
Bad sector(s)	No bad sectors found

Autopsy

Autopsy_DataSource_Loaded.png

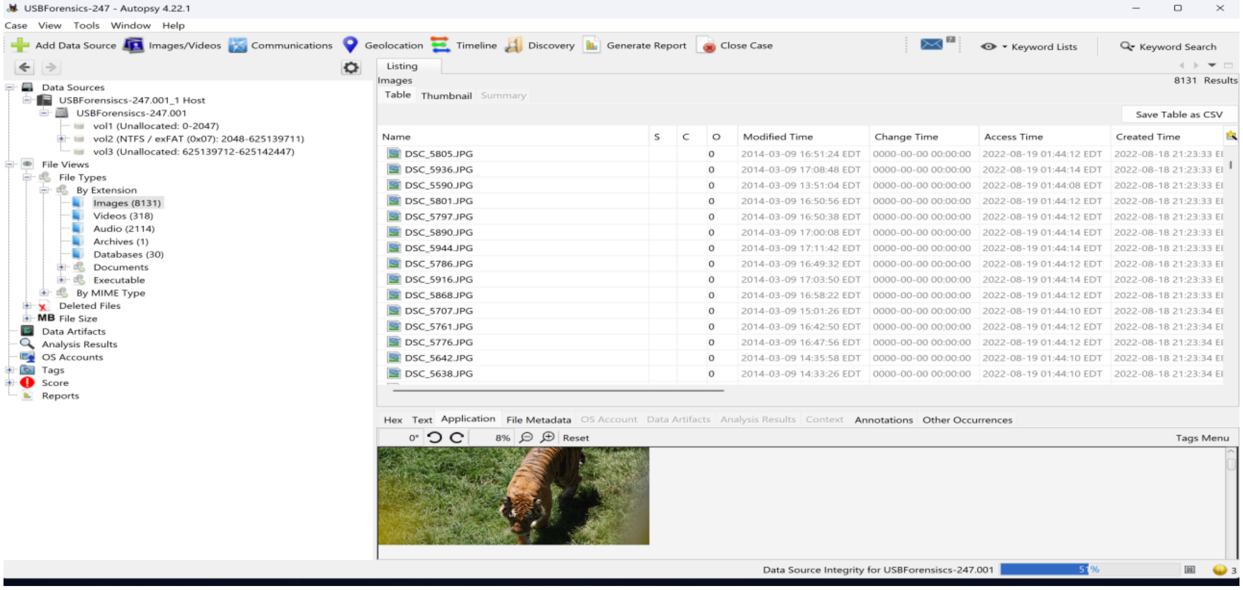


/img_USBForensiscs-247.001

3 Results

Name	ID	Starting Sector	Length in Sectors	Description	Flags
vol1 (Unallocated: 0-2047)	1	0	2048	Unallocated	Unallocated
vol2 (NTFS / exFAT (0x07): 2048-625139711)	2	2048	625137664	NTFS / exFAT (0x07)	Allocated
vol3 (Unallocated: 625139712-625142447)	3	625139712	2736	Unallocated	Unallocated

File Types



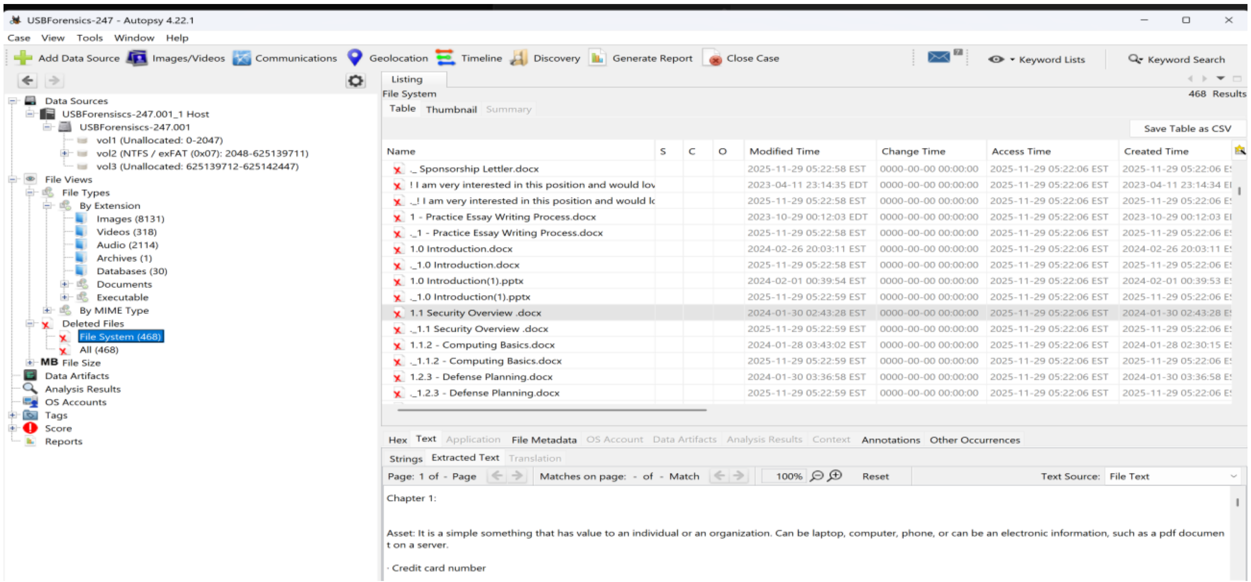
Images

8131 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
DSC_5805.JPG			0	2014-03-09 16:51:24 EDT	0000-00-00 00:00:00	2022-08-19 01:44:12 EDT	2022-08-18 21:23:33 EI
DSC_5936.JPG			0	2014-03-09 17:08:48 EDT	0000-00-00 00:00:00	2022-08-19 01:44:14 EDT	2022-08-18 21:23:33 EI
DSC_5590.JPG			0	2014-03-09 13:51:04 EDT	0000-00-00 00:00:00	2022-08-19 01:44:08 EDT	2022-08-18 21:23:33 EI
DSC_5801.JPG			0	2014-03-09 16:50:56 EDT	0000-00-00 00:00:00	2022-08-19 01:44:12 EDT	2022-08-18 21:23:33 EI
DSC_5797.JPG			0	2014-03-09 16:50:38 EDT	0000-00-00 00:00:00	2022-08-19 01:44:12 EDT	2022-08-18 21:23:33 EI
DSC_5890.JPG			0	2014-03-09 17:00:08 EDT	0000-00-00 00:00:00	2022-08-19 01:44:14 EDT	2022-08-18 21:23:33 EI
DSC_5944.JPG			0	2014-03-09 17:11:42 EDT	0000-00-00 00:00:00	2022-08-19 01:44:14 EDT	2022-08-18 21:23:33 EI
DSC_5786.JPG			0	2014-03-09 16:49:32 EDT	0000-00-00 00:00:00	2022-08-19 01:44:12 EDT	2022-08-18 21:23:33 EI
DSC_5916.JPG			0	2014-03-09 17:03:50 EDT	0000-00-00 00:00:00	2022-08-19 01:44:14 EDT	2022-08-18 21:23:33 EI
DSC_5868.JPG			0	2014-03-09 16:58:22 EDT	0000-00-00 00:00:00	2022-08-19 01:44:12 EDT	2022-08-18 21:23:33 EI
DSC_5707.JPG			0	2014-03-09 15:01:26 EDT	0000-00-00 00:00:00	2022-08-19 01:44:10 EDT	2022-08-18 21:23:34 EI
DSC_5761.JPG			0	2014-03-09 16:42:50 EDT	0000-00-00 00:00:00	2022-08-19 01:44:12 EDT	2022-08-18 21:23:34 EI
DSC_5776.JPG			0	2014-03-09 16:47:56 EDT	0000-00-00 00:00:00	2022-08-19 01:44:12 EDT	2022-08-18 21:23:34 EI
DSC_5642.JPG			0	2014-03-09 14:35:58 EDT	0000-00-00 00:00:00	2022-08-19 01:44:10 EDT	2022-08-18 21:23:34 EI
DSC_5638.JPG			0	2014-03-09 14:33:26 EDT	0000-00-00 00:00:00	2022-08-19 01:44:10 EDT	2022-08-18 21:23:34 EI

Data Source Integrity for USBForensiscs-247.001 51%

Deleted Files:



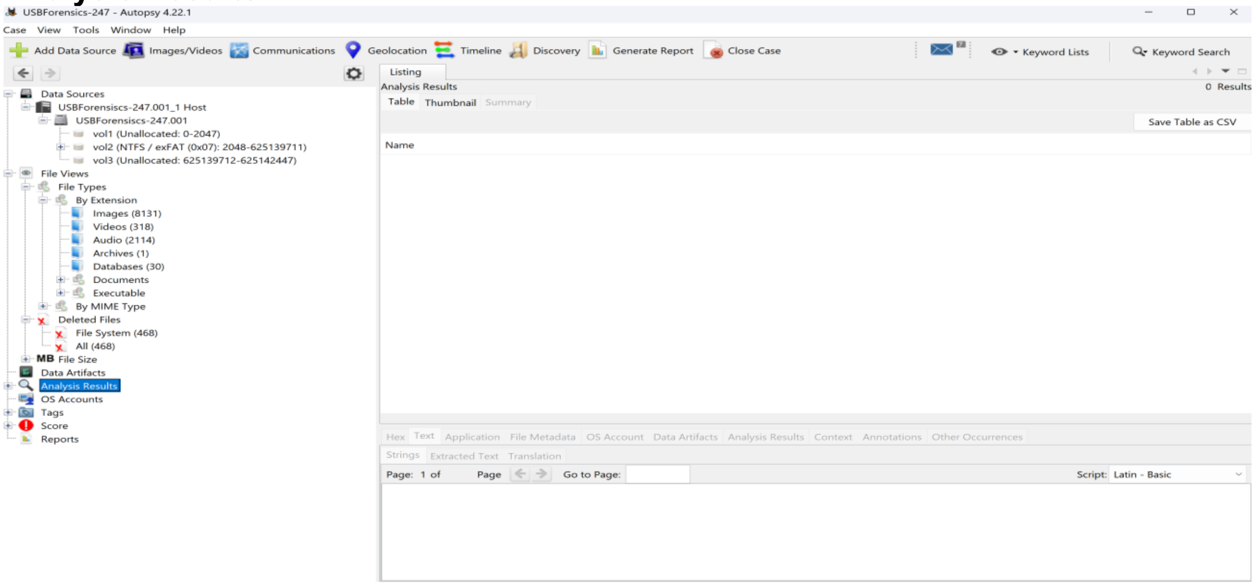
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
._ Sponsorship Lettler.docx				2025-11-29 05:22:58 EST	0000-00-00 00:00:00	2025-11-29 05:22:06 EST	2025-11-29 05:22:06 E
! I am very interested in this position and would lov				2023-04-11 23:14:35 EDT	0000-00-00 00:00:00	2025-11-29 05:22:06 EST	2023-04-11 23:14:34 E
._! I am very interested in this position and would lo				2025-11-29 05:22:58 EST	0000-00-00 00:00:00	2025-11-29 05:22:06 EST	2025-11-29 05:22:06 E
1 - Practice Essay Writing Process.docx				2023-10-29 00:12:03 EDT	0000-00-00 00:00:00	2025-11-29 05:22:06 EST	2023-10-29 00:12:03 E
._1 - Practice Essay Writing Process.docx				2025-11-29 05:22:58 EST	0000-00-00 00:00:00	2025-11-29 05:22:06 EST	2025-11-29 05:22:06 E
1.0 Introduction.docx				2024-02-26 20:03:11 EST	0000-00-00 00:00:00	2025-11-29 05:22:06 EST	2024-02-26 20:03:11 E
._1.0 Introduction.docx				2025-11-29 05:22:58 EST	0000-00-00 00:00:00	2025-11-29 05:22:06 EST	2025-11-29 05:22:06 E
1.0 Introduction(1).pptx				2024-02-01 00:39:54 EST	0000-00-00 00:00:00	2025-11-29 05:22:06 EST	2024-02-01 00:39:53 E
._1.0 Introduction(1).pptx				2025-11-29 05:22:59 EST	0000-00-00 00:00:00	2025-11-29 05:22:06 EST	2025-11-29 05:22:06 E
1.1 Security Overview .docx				2024-01-30 02:43:28 EST	0000-00-00 00:00:00	2025-11-29 05:22:06 EST	2024-01-30 02:43:28 E
._1.1 Security Overview .docx				2025-11-29 05:22:59 EST	0000-00-00 00:00:00	2025-11-29 05:22:06 EST	2025-11-29 05:22:06 E
1.1.2 - Computing Basics.docx				2024-01-28 03:43:02 EST	0000-00-00 00:00:00	2025-11-29 05:22:06 EST	2024-01-28 02:30:15 E
._1.1.2 - Computing Basics.docx				2025-11-29 05:22:59 EST	0000-00-00 00:00:00	2025-11-29 05:22:06 EST	2025-11-29 05:22:06 E
1.2.3 - Defense Planning.docx				2024-01-30 03:36:58 EST	0000-00-00 00:00:00	2025-11-29 05:22:06 EST	2024-01-30 03:36:58 E
._1.2.3 - Defense Planning.docx				2025-11-29 05:22:59 EST	0000-00-00 00:00:00	2025-11-29 05:22:06 EST	2025-11-29 05:22:06 E

Chapter 1:

Asset: It is a simple something that has value to an individual or an organization. Can be laptop, computer, phone, or can be an electronic information, such as a pdf document on a server.

· Credit card number

Analysis Results:



Conclusion

This forensic examination followed a procedure for obtaining and analyzing a USB storage device while maintaining the integrity of the evidence. FTK Imager was used to create a complete forensic image in asafe environment, and hash values (MD5 hash and SHA1 hash) were verified to ensure that the data was not altered during acquisition. The Autopsy was used to analyze the image, permitting a review of the file system, file types, and overall activity on the USB device. The analysis identified common user files such as images, audio, videos, and databases, and did not indicate any confirmed malicious activity. This investigation shows the importance of handling removable media and maintaining basic controls to reduce potential security risks in devices.

Name: Nathalia Nathanson Bolinja

To: Tesfaye W. Lemma

X

Nathalia Nathanson Bolinja