Module 05: Defeating Anti-forensics Techniques

Lab Scenario

In order to investigate cybercrimes, as a forensic investigator, you must be able to collect and analyze evidence from victims' or attackers' systems. The attackers attempt to avert detection through the forensics processes by applying some anti-forensics techniques that damage evidence, hide the pathways used, and delete the data exfiltrated from the victims' systems. You must be aware of such techniques and their impact on the evidence and systems.

Lab Objectives

The objective of this lab is to provide expert knowledge about the following:

- Solid-state drive (SSD) file carving on Windows and Linux file systems
- Recovering lost/deleted partitions and their contents
- Cracking passwords of various applications
- Detecting steganography

Overview of Defeating Anti-forensics Techniques

There are different types of anti-forensics techniques such as data/file deletion, wiping/overwriting of data and metadata, corruption/degaussing, cryptographic file systems, password protection, etc.

Forensic investigators need to overcome/defeat anti-forensics techniques so that an investigator yields concrete and accurate evidence that helps identify and prosecute the perpetrators.

Lab Tasks

The following are the recommended labs that will assist you in defeating anti-forensics techniques:

- SSD file carving on a Linux file system
- Recovering data from lost/deleted disk partition
- Cracking application passwords
- Detecting steganography

Lab 1: SSD File Carving on a Linux File System

Lab Scenario

Sam, a forensic investigator, is supposed to perform file carving on a forensic image file of an SSD acquired from a Linux file system. Law enforcement agents acquired the image from the machine of a suspect who is accused in a child pornography case. Now, the forensic investigator should use file carving techniques to recover more data related to the case. To do so, the investigator should possess knowledge of the file system structure to identify and recover files and fragments of files from the unallocated space of the SSD in the absence of file metadata.

As a forensics investigator, you should know how to perform SSD file carving on a Linux file system.

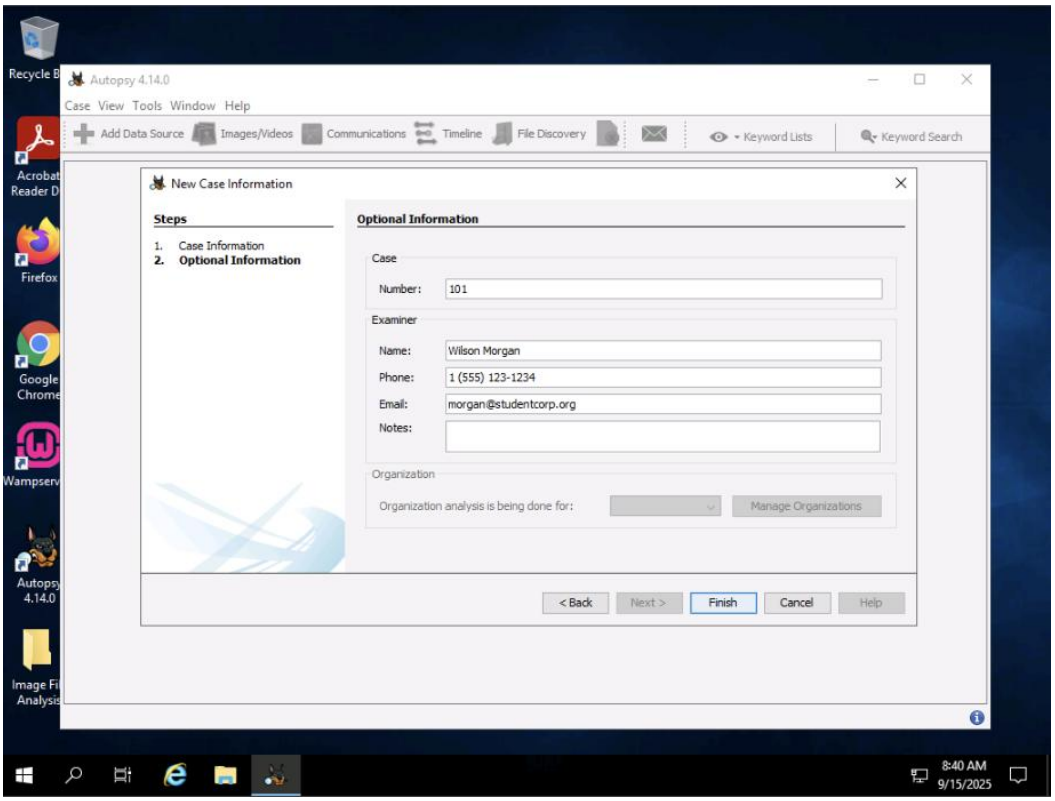
Lab Objectives

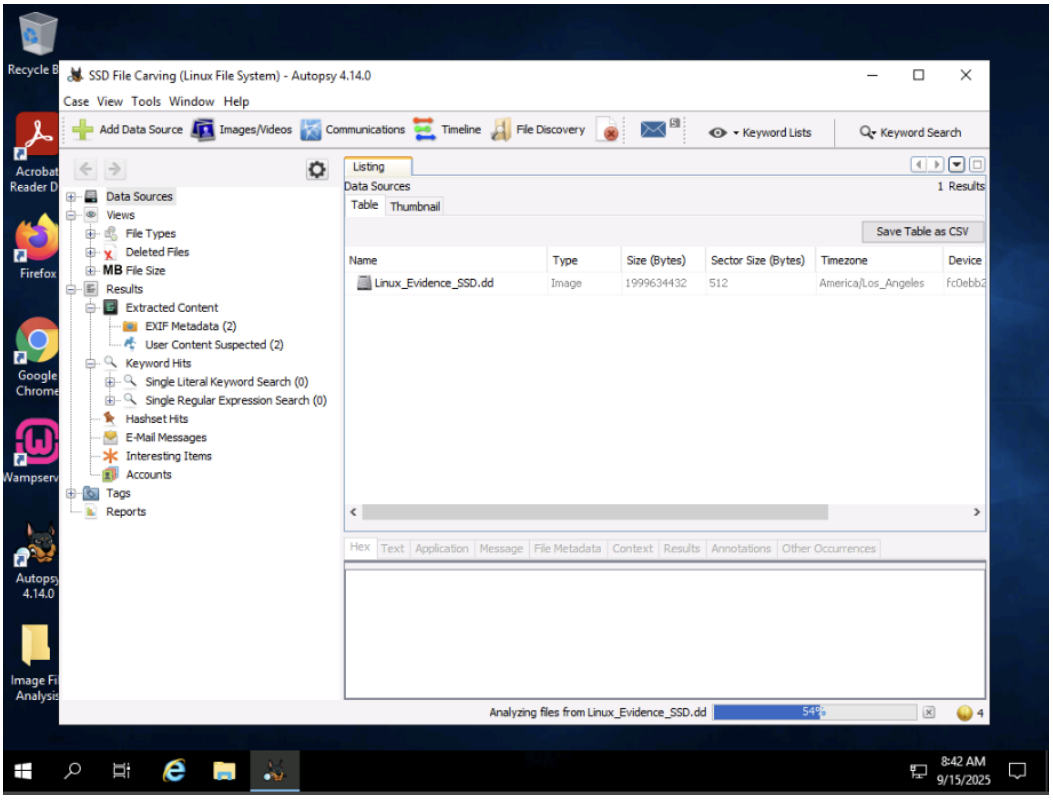
File carving is a technique to recover files and fragments of files from unallocated hard disk space in the absence of file metadata. SSD file carving on a Linux file system is performed using the forensics tool Autopsy.

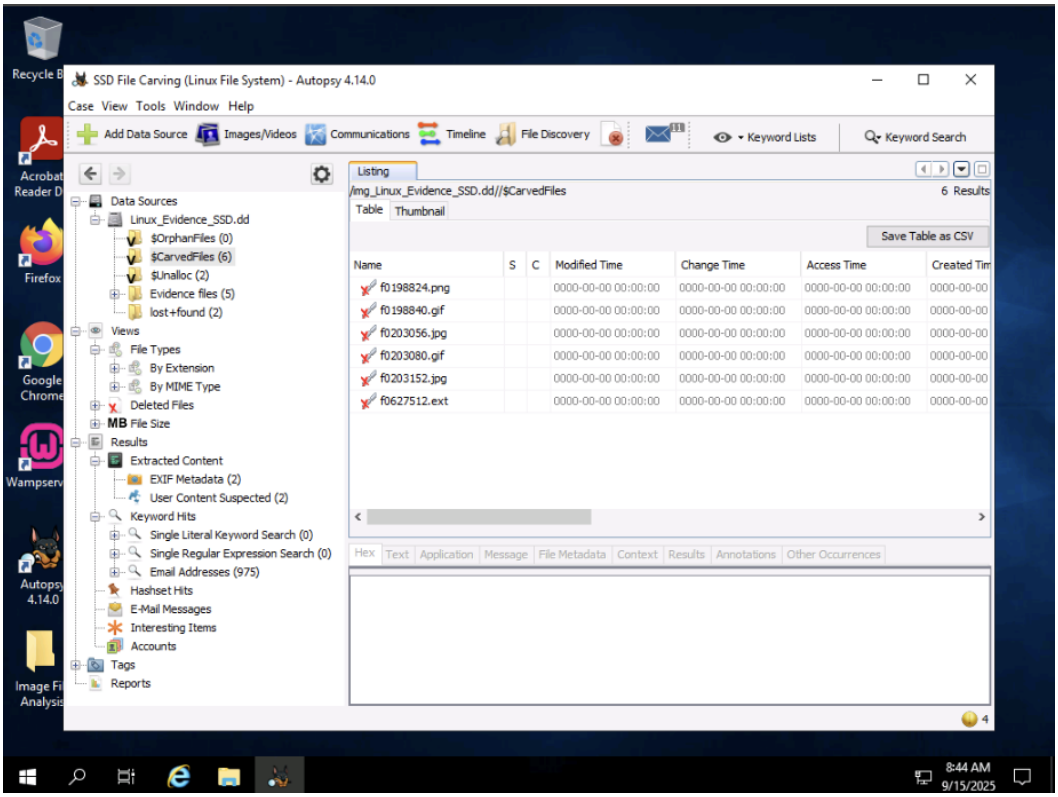
The objective of this lab is to help you understand how to perform SSD file carving on a Linux file system.

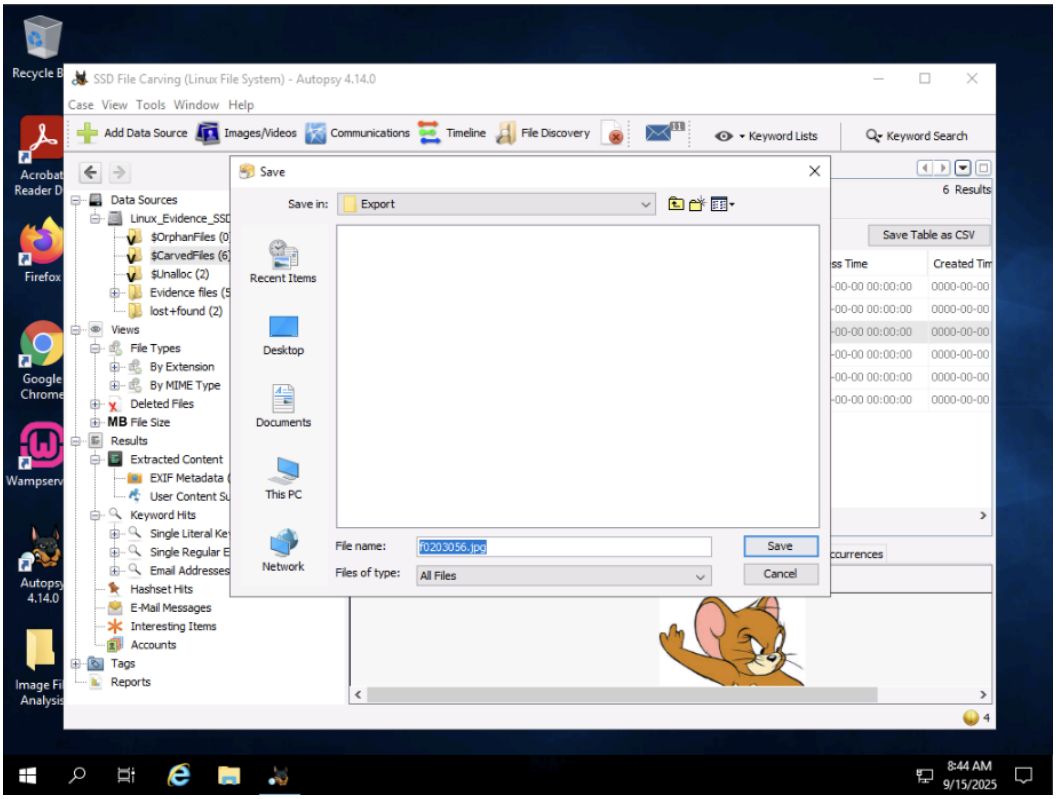
Overview of the Lab

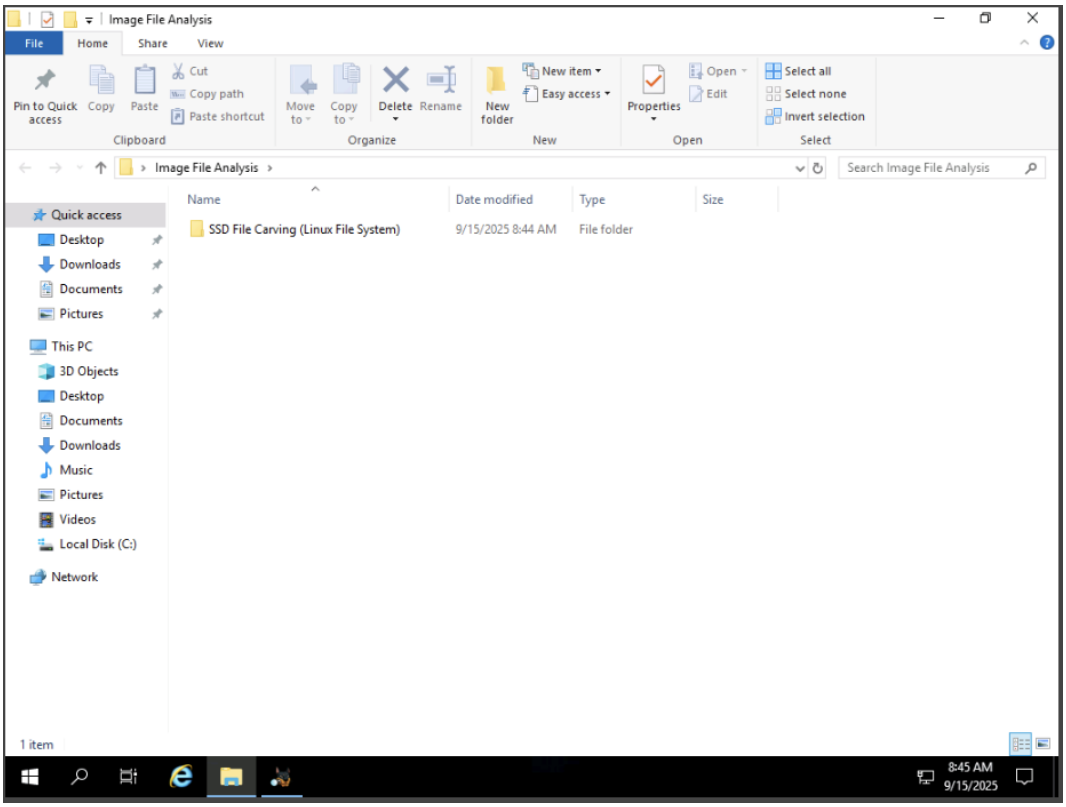
This lab familiarizes you with the Autopsy tool and helps you understand how to recover data from a Linux file system on an SSD when the TRIM functionality is disabled.


Autopsy 4.14.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Timeline
File Discovery
Keyword Lists
Keyword Search
New Case Information
Steps
1. Case Information
2. Optional Information
Optional Information
Case
Number: 101
Examiner
Name: Wilson Morgan
Phone: 1 (555) 123-1234
Email: morgan@studentcorp.org
Notes:
Organization
Organization analysis is being done for:
Manage Organizations
< Back
Next >
Finish
Cancel
Help
8:40 AM
9/15/2025


SSD File Carving (Linux File System) - Autopsy 4.14.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Timeline
File Discovery
Keyword Lists
Keyword Search
Data Sources
Views
File Types
Deleted Files
File Size
Results
Extracted Content
EXIF Metadata (2)
User Content Suspected (2)
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Hashset Hits
E-Mail Messages
Interesting Items
Accounts
Tags
Reports
Listing
Data Sources
1 Results
Table
Thumbnail
Save Table as CSV
Name
Type
Size (Bytes)
Sector Size (Bytes)
Timezone
Device
Linux_Evidence_SSD.dd
Image
1999634432
512
America/Los_Angeles
Hex
Text
Application
Message
File Metadata
Context
Results
Annotations
Other Occurrences
Analyzing files from Linux_Evidence_SSD.dd
54%
8:42 AM
9/15/2025


SSD File Carving (Linux File System) - Autopsy 4.14.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Timeline
File Discovery
Keyword Lists
Keyword Search
Data Sources
Linux_Evidence_SSD.dd
$OrphanFiles (0)
$CarvedFiles (6)
$Unalloc (2)
Evidence files (5)
lost+found (2)
Views
File Types
By Extension
By MIME Type
Deleted Files
File Size
Results
Extracted Content
EXIF Metadata (2)
User Content Suspected (2)
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Email Addresses (975)
Hashset Hits
E-Mail Messages
Interesting Items
Accounts
Tags
Reports
Listing
/img_Linux_Evidence_SSD.dd//$CarvedFiles
6 Results
Table
Thumbnail
Save Table as CSV
Name
S
C
Modified Time
Change Time
Access Time
Created Tim
f0198824.png
f0198840.gif
f0203056.jpg
f0203080.gif
f0203152.jpg
f0627512.ext
0000-00-00 00:00:00
Hex
Text
Application
Message
File Metadata
Context
Results
Annotations
Other Occurrences
8:44 AM
9/15/2025


SSD File Carving (Linux File System) - Autopsy 4.14.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Timeline
File Discovery
Keyword Lists
Keyword Search
Save
Save in:
Export
Recent Items
Desktop
Documents
This PC
Network
File name:
f0203056.jpg
Files of type:
All Files
Save
Cancel
Save Table as CSV
6 Results
8:44 AM
9/15/2025



Lab 2: Recovering Data from Lost/Deleted Disk Partition

Lab Scenario

An attacker saved malicious files in one of the disk partitions of the victim's workstation system and executed them to steal sensitive business data. After committing the crime, the attacker deleted the entire disk partition in which they had saved the malicious files to prevent their crime and identity from being detected. The victim discovered that one of the disk partitions on their system was missing. They also found that the system was behaving suspiciously and reported the matter to their organization's cyber-security department. As a part of forensic investigation in this case, investigators must now recover the deleted disk partition so that the files that were stored in it (both normal and malicious files) can be retrieved and the malicious files can be sent for further investigation.

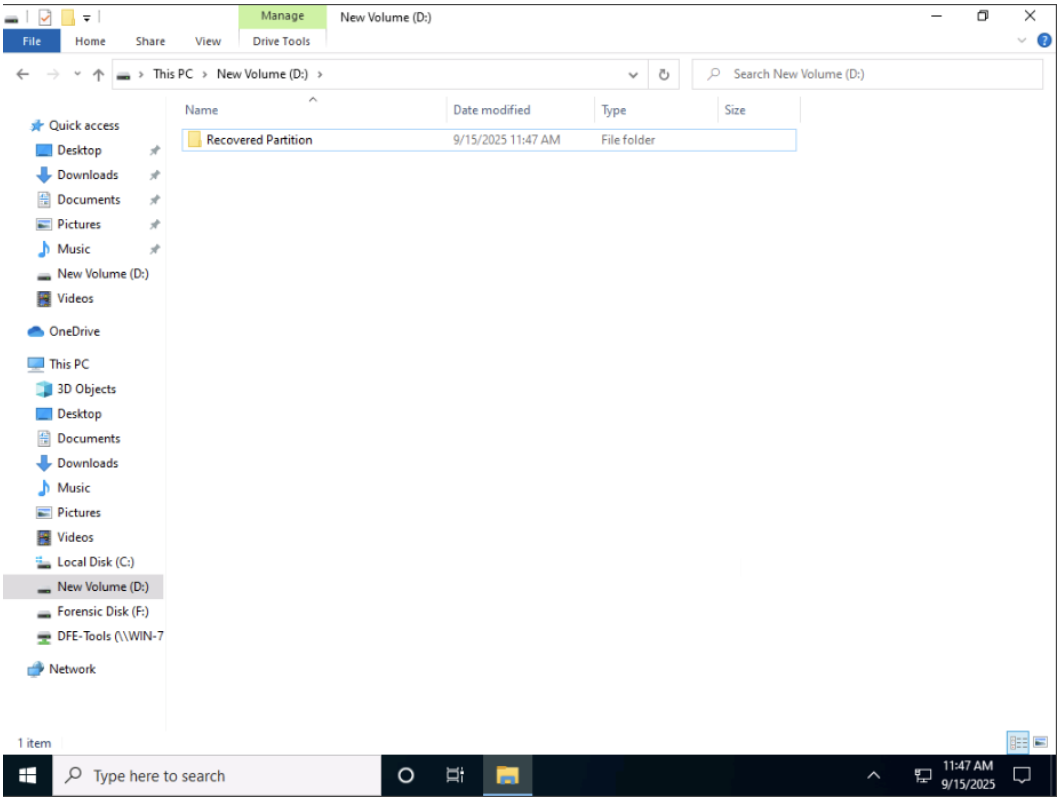
Lab Objectives

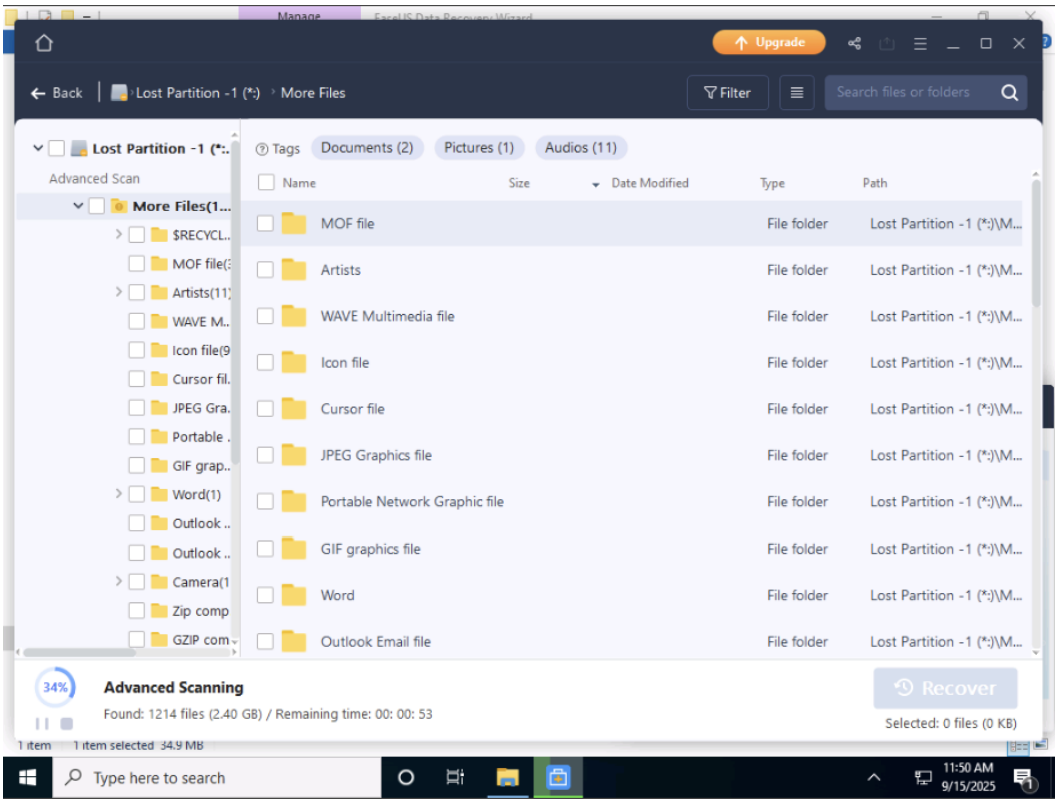
When a partition is deleted from a disk, the files within the disk are lost, and the entries related to the deleted partition are removed by the computer from the MBR partition table. However, as long as the corresponding section of the disk is not overwritten, there is a chance to recover the deleted partition and the files within it.

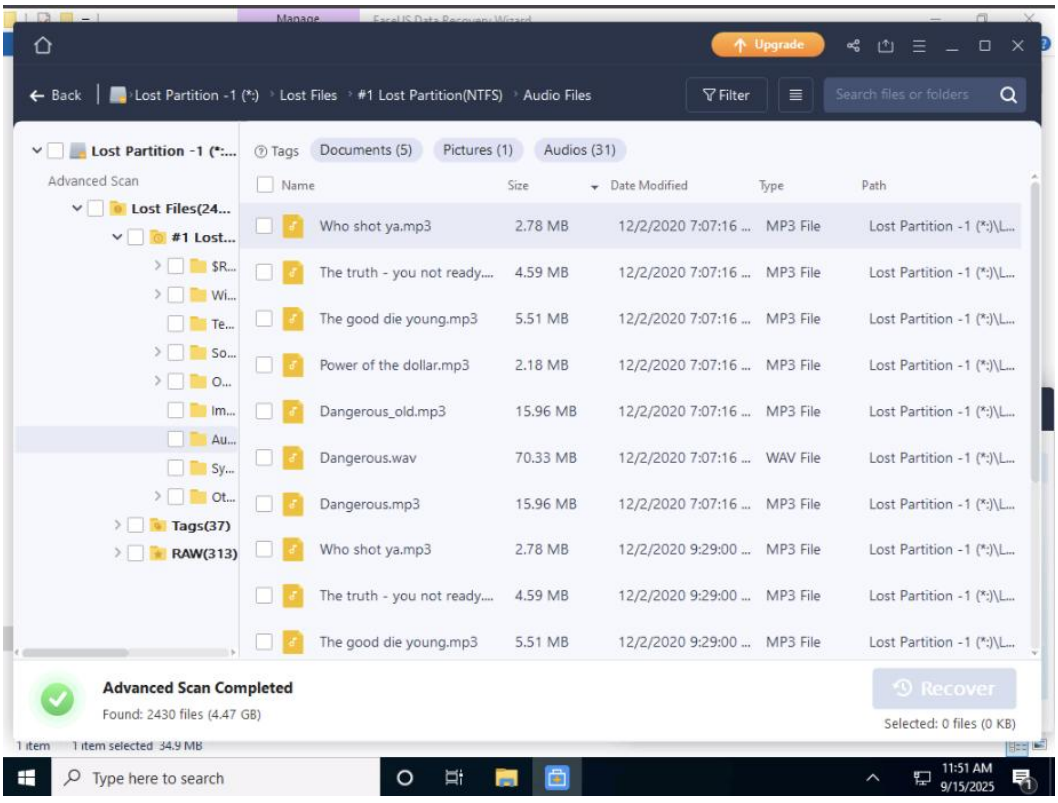
The objective of the lab is to help you understand how to recover data from lost/deleted partitions.

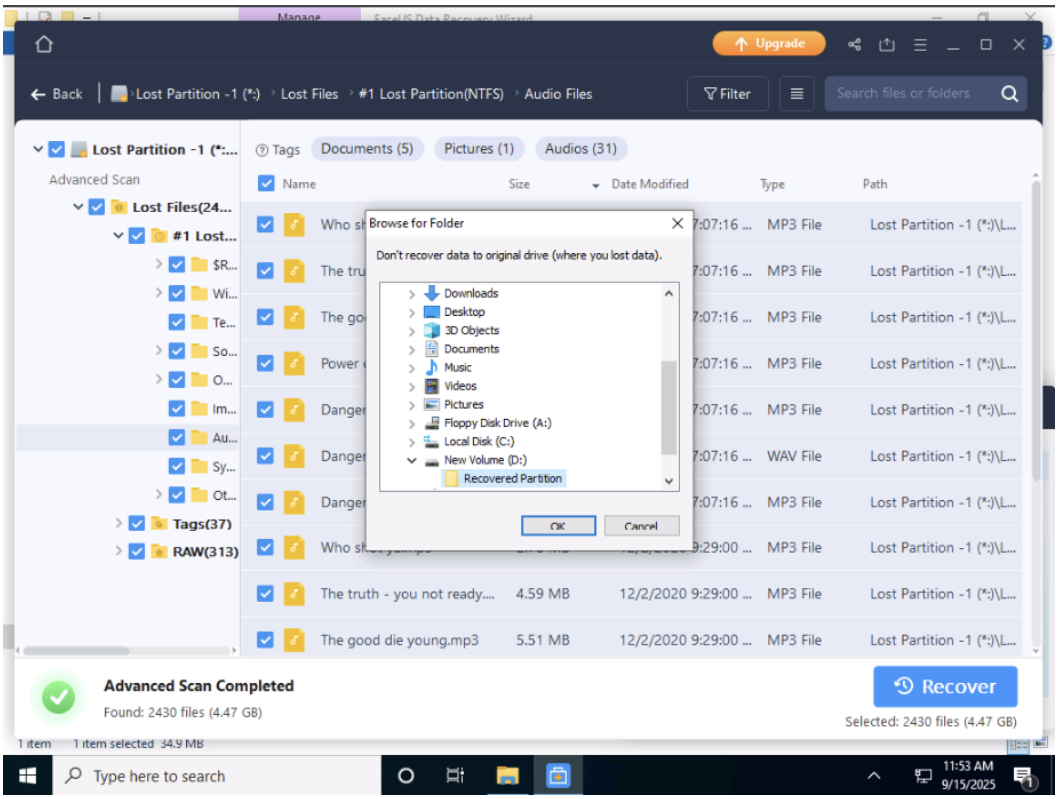
Overview of the Lab

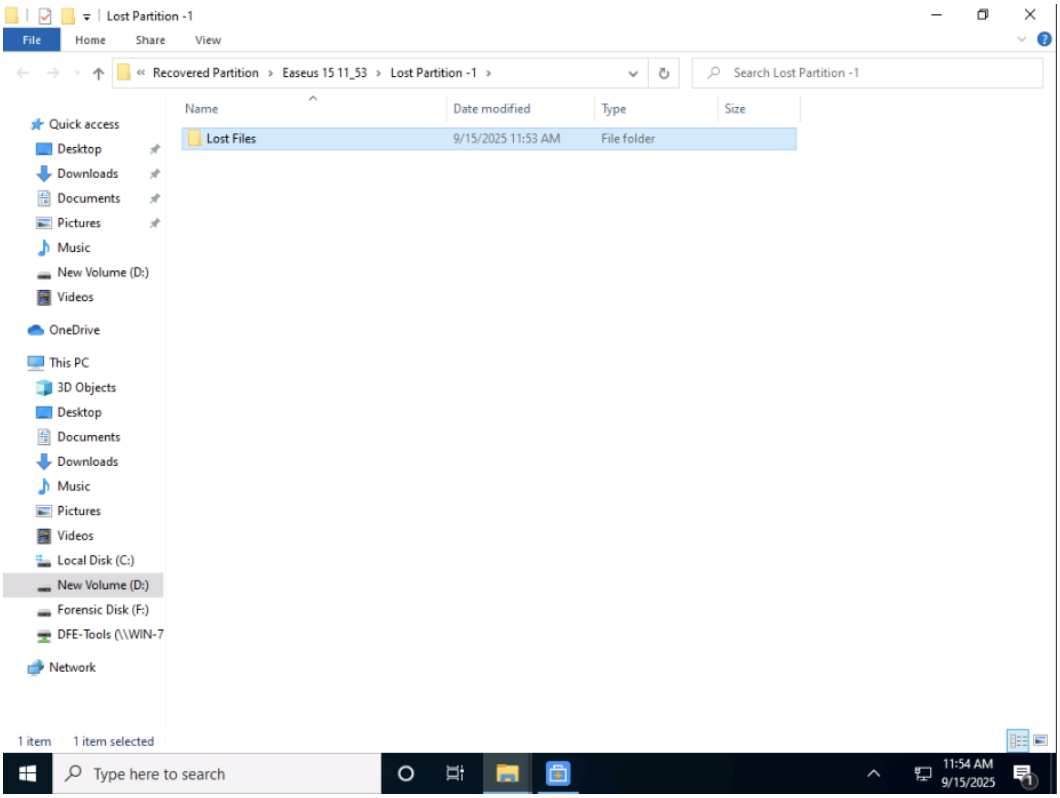
This lab familiarizes you with EaseUS Data Recovery Wizard and helps you understand how to recover a disk partition that may have been deleted by an attacker. A deleted disk partition may contain vital artifacts pertaining to an attacker's crime.

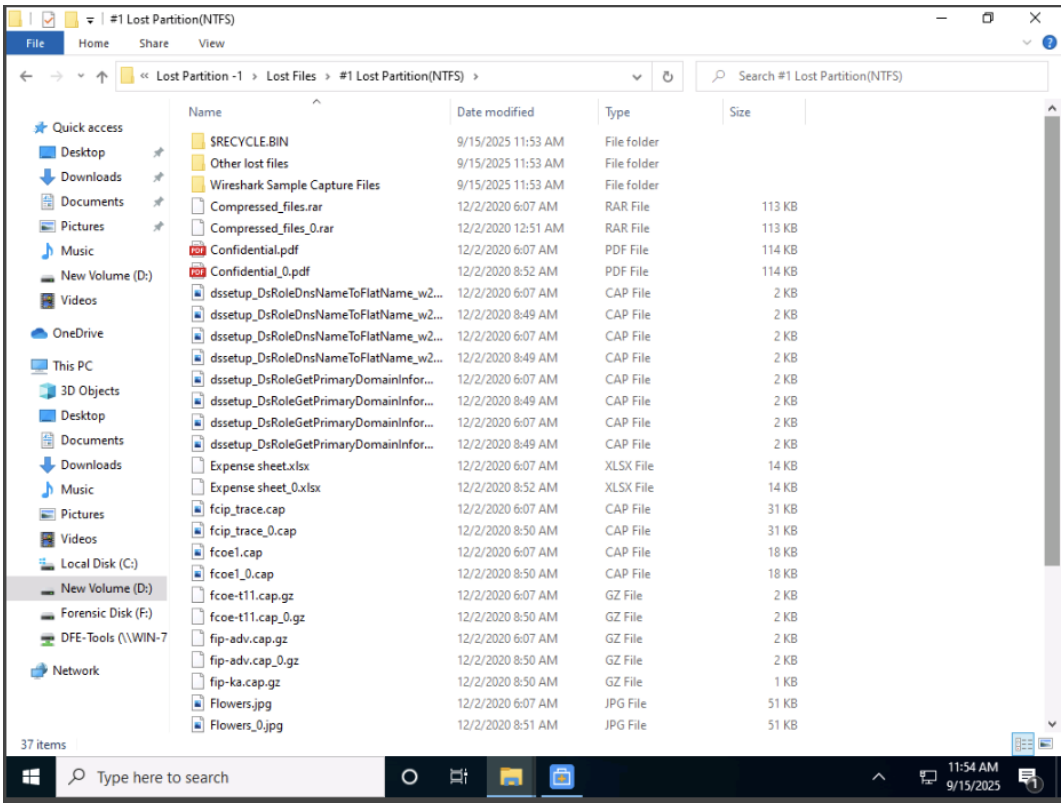



Upgrade
Back
Lost Partition -1 (*:)
More Files
Filter
Search files or folders
Lost Partition -1 (*:
Advanced Scan
More Files(1...
$RECYCL..
MOF file(
Artists(11
WAVE M..
Icon file(9
Cursor fil.
JPEG Gra.
Portable .
GIF grap..
Word(1)
Outlook ..
Outlook ..
Camera(1
Zip comp
GZIP com
Tags
Documents (2)
Pictures (1)
Audios (11)
Name
Size
Date Modified
Type
Path
MOF file
File folder
Lost Partition -1 (*:)\M...
Artists
WAVE Multimedia file
Icon file
Cursor file
JPEG Graphics file
Portable Network Graphic file
GIF graphics file
Word
Outlook Email file
34%
Advanced Scanning
Found: 1214 files (2.40 GB) / Remaining time: 00: 00: 53
Recover
Selected: 0 files (0 KB)
1 item
1 item selected 34.9 MB
Type here to search
11:50 AM
9/15/2025


Upgrade
Back
Lost Partition -1 (*:)
Lost Files
#1 Lost Partition(NTFS)
Audio Files
Filter
Search files or folders
Lost Partition -1 (*:...
Advanced Scan
Lost Files(24...
#1 Lost...
$R...
Wi...
Te...
So...
O...
Im...
Au...
Sy...
Ot...
Tags(37)
RAW(313)
Tags
Documents (5)
Pictures (1)
Audios (31)
Name
Size
Date Modified
Type
Path
Who shot ya.mp3
2.78 MB
12/2/2020 7:07:16 ...
MP3 File
Lost Partition -1 (*:)\L...
The truth - you not ready....
4.59 MB
The good die young.mp3
5.51 MB
Power of the dollar.mp3
2.18 MB
Dangerous_old.mp3
15.96 MB
Dangerous.wav
70.33 MB
WAV File
Dangerous.mp3
15.96 MB
Who shot ya.mp3
2.78 MB
12/2/2020 9:29:00 ...
The truth - you not ready....
4.59 MB
The good die young.mp3
5.51 MB
Advanced Scan Completed
Found: 2430 files (4.47 GB)
Recover
Selected: 0 files (0 KB)
1 item
1 item selected 34.9 MB
Type here to search
11:51 AM
9/15/2025


Upgrade
Back
Lost Partition -1 (*:)
Lost Files
#1 Lost Partition(NTFS)
Audio Files
Filter
Search files or folders
Tags
Documents (5)
Pictures (1)
Audios (31)
Name
Size
Date Modified
Type
Path
Browse for Folder
Don't recover data to original drive (where you lost data).
Downloads
Desktop
3D Objects
Documents
Music
Videos
Pictures
Floppy Disk Drive (A:)
Local Disk (C:)
New Volume (D:)
Recovered Partition
OK
Cancel
The truth - you not ready....
4.59 MB
12/2/2020 9:29:00 ...
MP3 File
Lost Partition -1 (*:)\L...
The good die young.mp3
5.51 MB
WAV File
Advanced Scan Completed
Found: 2430 files (4.47 GB)
Recover
Selected: 2430 files (4.47 GB)
Type here to search
11:53 AM
9/15/2025


Lost Partition -1
File
Home
Share
View
Recovered Partition
Easeus 15 11_53
Lost Partition -1
Search Lost Partition -1
Quick access
Desktop
Downloads
Documents
Pictures
Music
New Volume (D:)
Videos
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
New Volume (D:)
Forensic Disk (F:)
DFE-Tools (\\WIN-7
Network
Name
Date modified
Type
Size
Lost Files
9/15/2025 11:53 AM
File folder
1 item
1 item selected
Type here to search
11:54 AM
9/15/2025



Lab 3: Cracking Application Passwords

Lab Scenario

An investigation into a case of theft of intellectual property and trade secrets belonging to an investment-banking organization has led forensic investigators to a personal computer belonging to the perpetrator. The perpetrator has stored all the stolen information in the form of various documents on their computer and has set passwords for those documents to prevent them from being accessed by others. With the help of law enforcement authorities, forensic investigators seized the perpetrator's machine to search through it for stolen information. During the course of investigation, the investigators found some password-protected files, the passwords for which must be cracked in order to gain access to the sensitive information that belongs to the investment-banking organization. How should the investigators proceed to crack the passwords of the protected documents?

As an expert forensic investigator, you must know how to crack the passwords of password-protected files and applications.

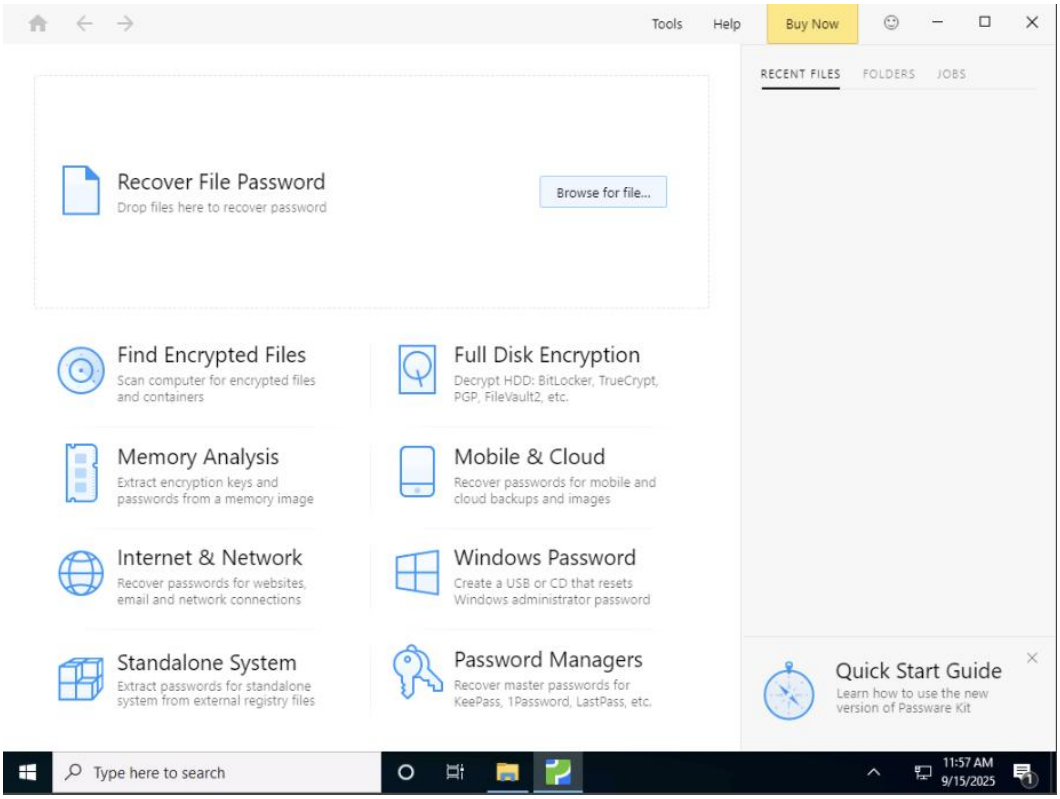
Lab Objectives

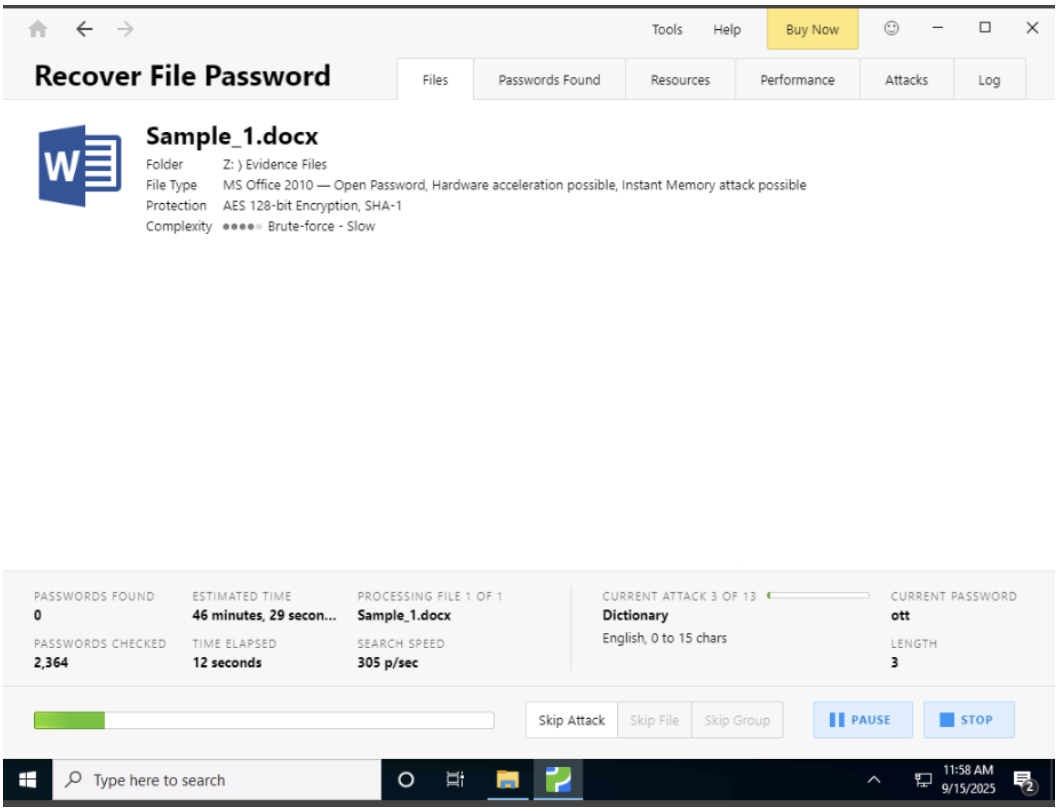
Passwords are typically a string of characters used to verify the identity of a user during an authentication process.

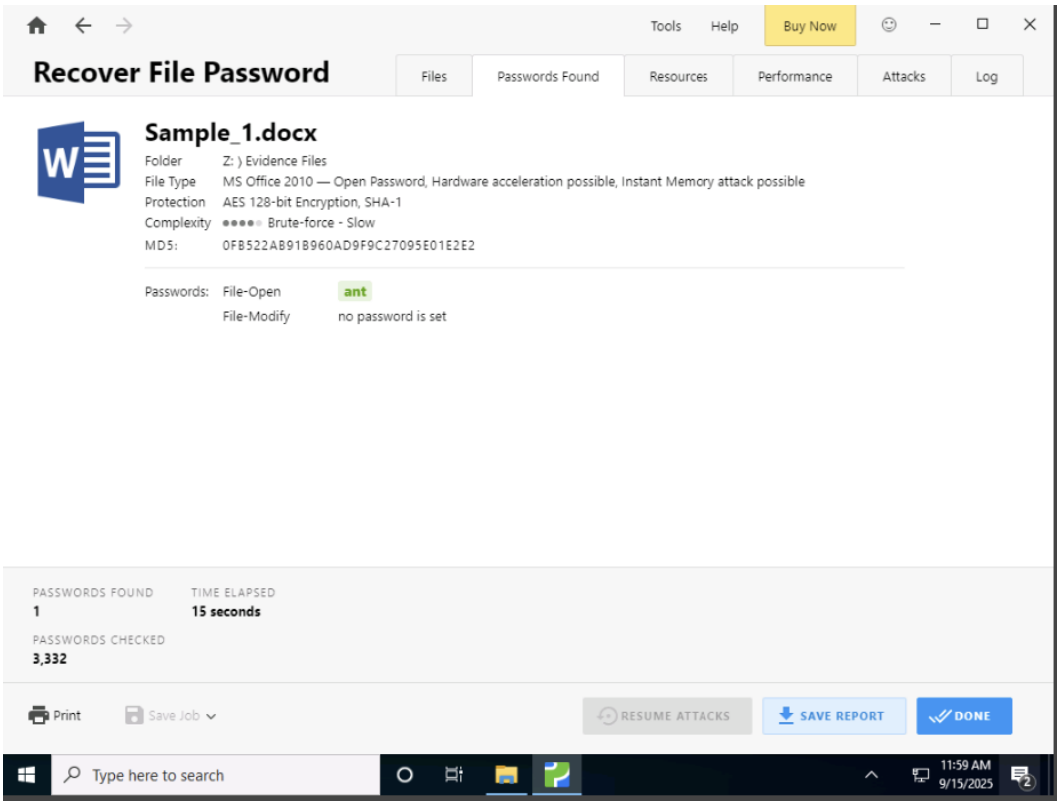
The objective of this lab is to help you understand how to crack the passwords of password-protected files and applications.

Overview of the Lab

This lab familiarizes you with the Passware Kit Forensic tool and helps you understand how to crack passwords of password-protected applications/files on a computer for purposes of forensic investigation.







Lab 4: Detecting Steganography

Lab Scenario

Attackers occasionally attempt to deceive users and system security by hiding a malicious program with an apparently useful image or file. By doing this, they can avert security checks and lure victims into downloading and running malware as well as prevent forensic identification.

As an expert forensic investigator, you must be able to detect and analyze steganography files.

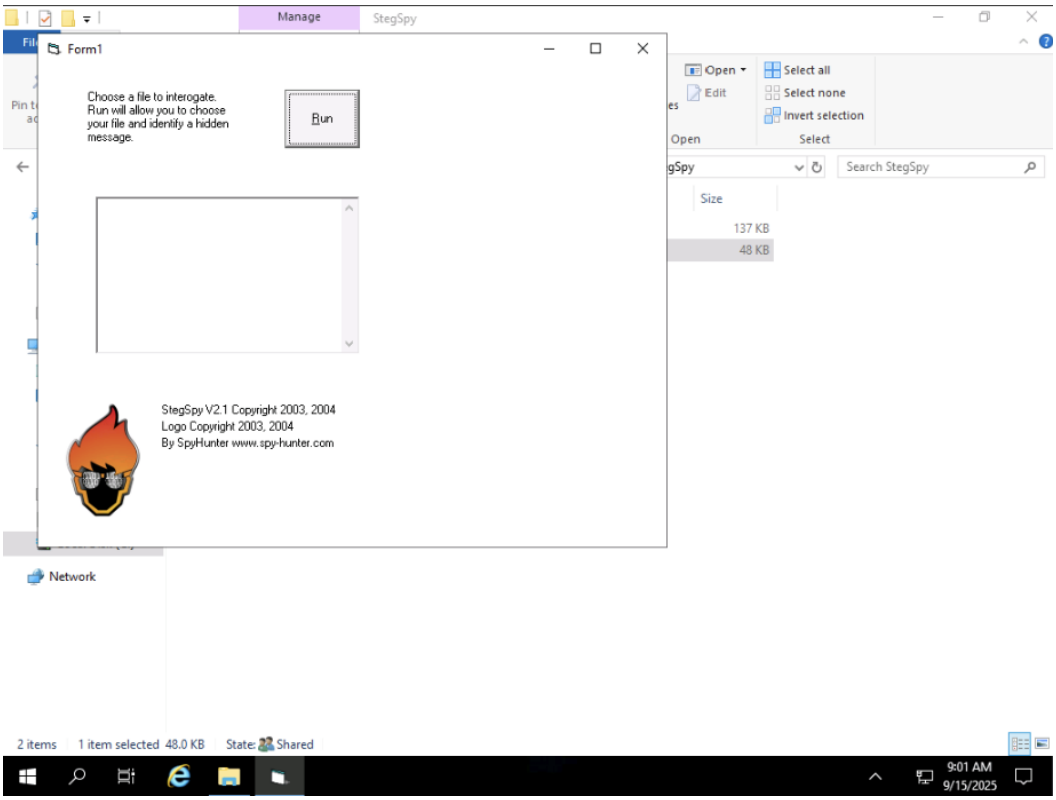
Lab Objectives

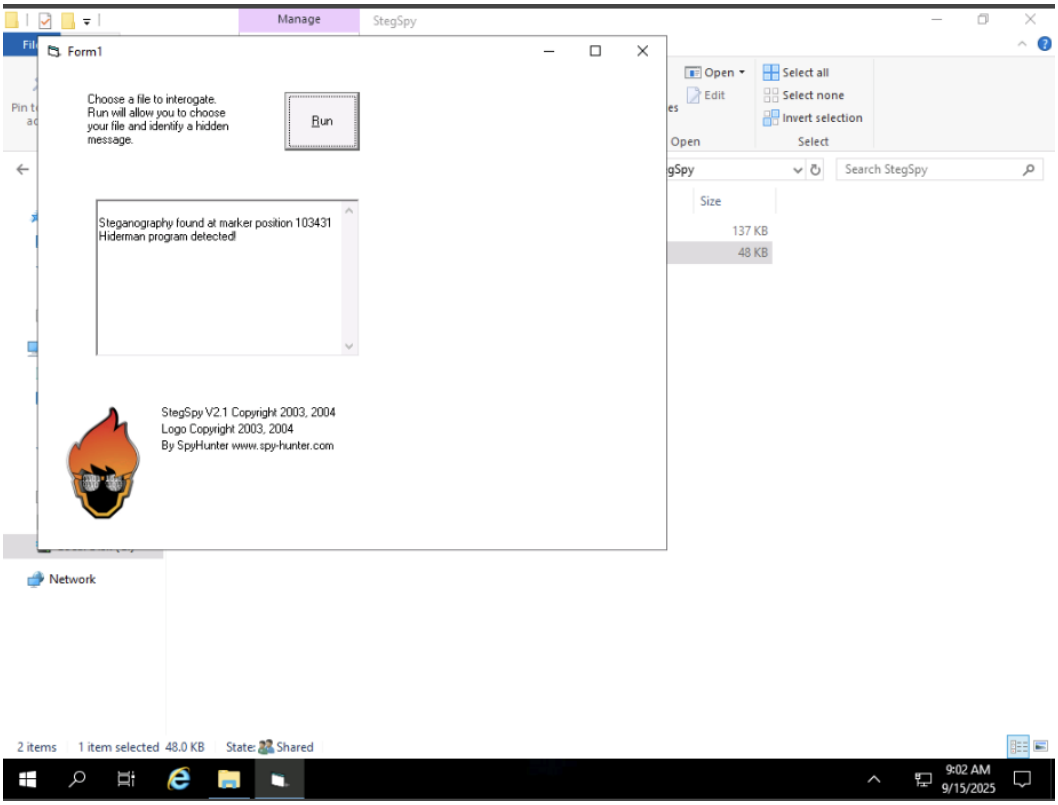
Steganography is the process of hiding information or a file within another file. In other words, it is the process of disguising a harmful file as a safe file.

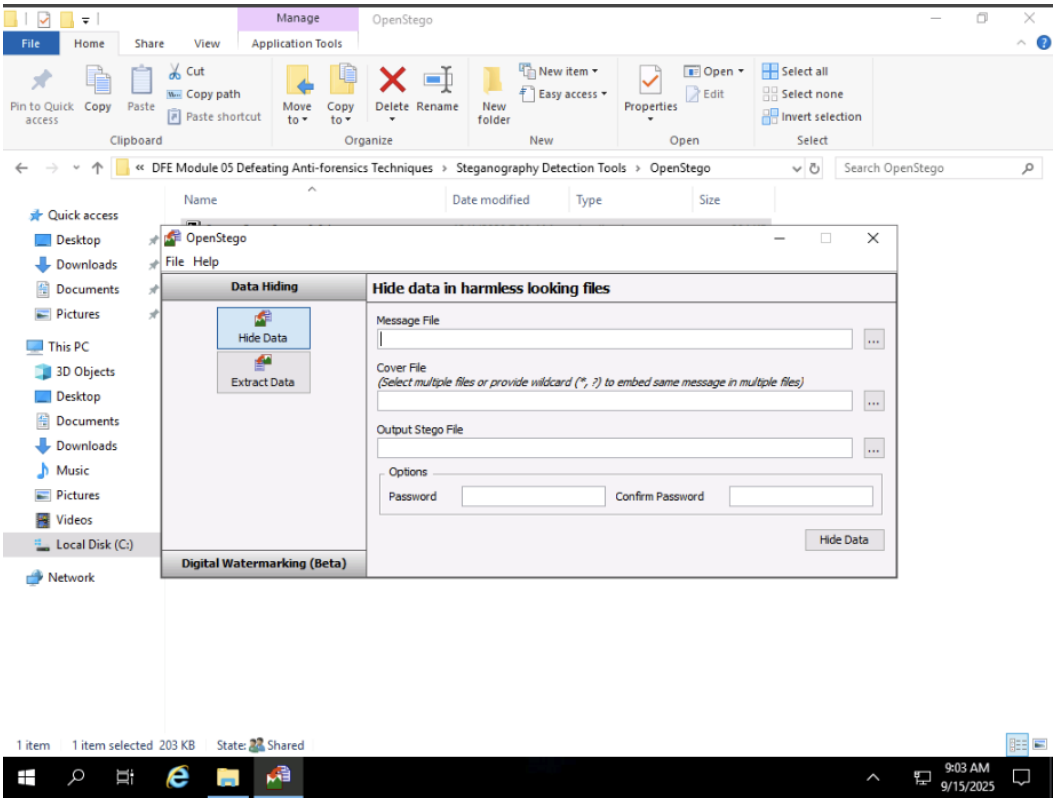
The objective of this lab is to help you analyze files hidden using steganography and find their impact on a system or network.

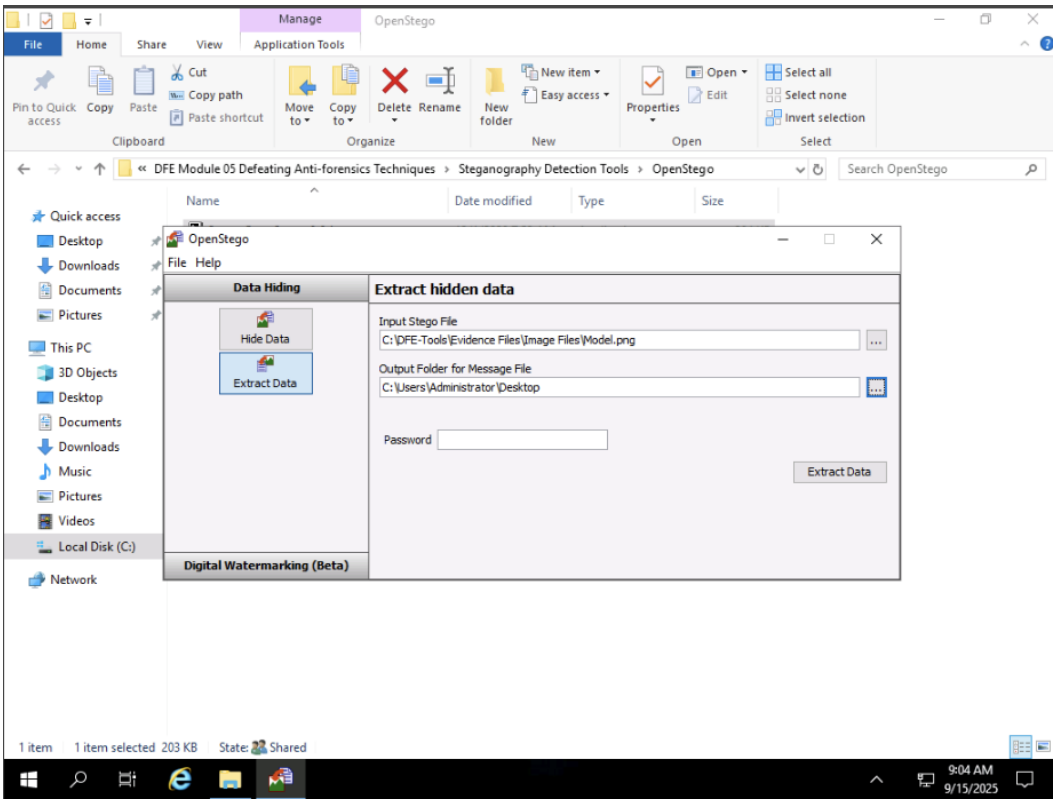
Overview of the Lab

This lab familiarizes you with tools such as StegSpy and OpenStego and helps you understand how to identify messages or files with hidden content using these tools.

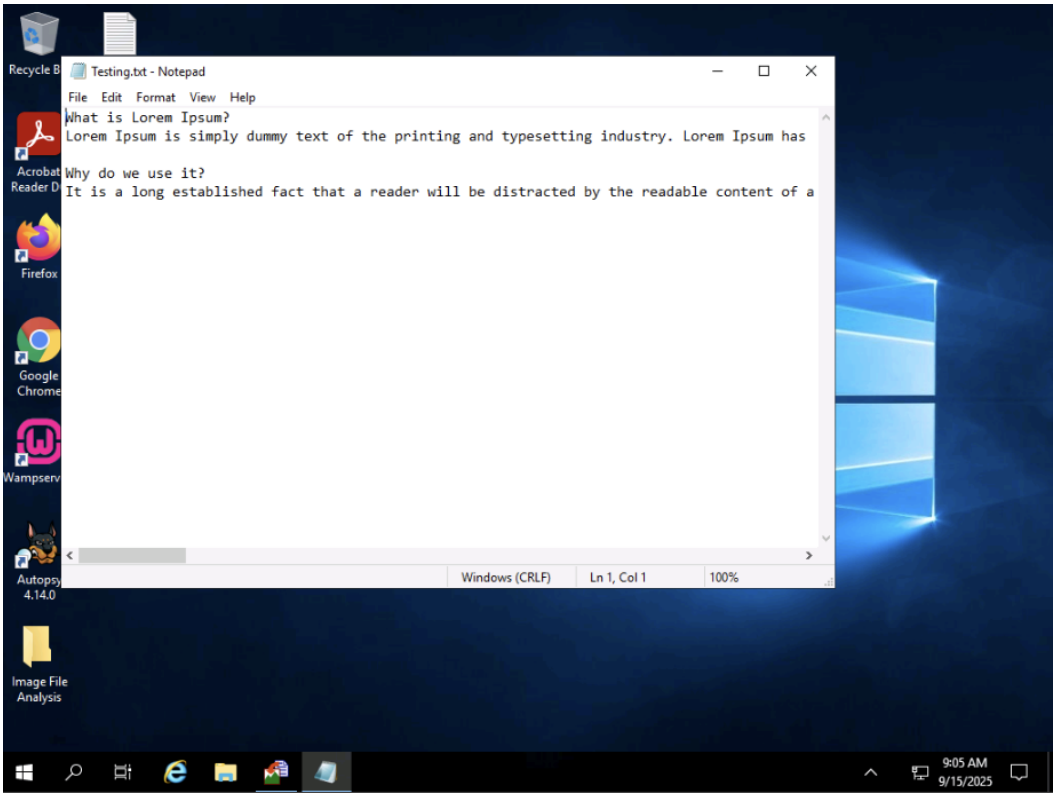



Manage
StegSpy
Form1
Choose a file to interogate.
Run will allow you to choose
your file and identify a hidden
message.
Run
Steganography found at marker position 103431
Hiderman program detected!
StegSpy V2.1 Copyright 2003, 2004
Logo Copyright 2003, 2004
By SpyHunter www.spy-hunter.com
Open
Edit
Select all
Select none
Invert selection
Open
Select
Search StegSpy
Size
137 KB
48 KB
Network
2 items
1 item selected 48.0 KB
State: Shared
9:02 AM
9/15/2025


Manage
OpenStego
File
Home
Share
View
Application Tools
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
Select all
Select none
Invert selection
Select
DFE Module 05 Defeating Anti-forensics Techniques
Steganography Detection Tools
OpenStego
Search OpenStego
Name
Date modified
Type
Size
Quick access
Desktop
Downloads
Documents
Pictures
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Network
OpenStego
File Help
Data Hiding
Hide Data
Extract Data
Digital Watermarking (Beta)
Hide data in harmless looking files
Message File
Cover File
(Select multiple files or provide wildcard (*, ?) to embed same message in multiple files)
Output Stego File
Options
Password
Confirm Password
Hide Data
1 item
1 item selected 203 KB
State: Shared
9:03 AM
9/15/2025


Manage
OpenStego
File
Home
Share
View
Application Tools
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
Open
Select all
Select none
Invert selection
Select
« DFE Module 05 Defeating Anti-forensics Techniques › Steganography Detection Tools › OpenStego
Search OpenStego
Name
Date modified
Type
Size
Quick access
Desktop
Downloads
Documents
Pictures
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Network
OpenStego
File Help
Data Hiding
Hide Data
Extract Data
Digital Watermarking (Beta)
Extract hidden data
Input Stego File
C:\DFE-Tools\Evidence Files\Image Files\Model.png
Output Folder for Message File
C:\Users\Administrator\Desktop
Password
Extract Data
1 item
1 item selected 203 KB
State: Shared
9:04 AM
9/15/2025


Recycle Bin
Testing.txt
Acrobat Reader DC
Firefox
Google Chrome
Wampserve...
Autopsy 4.14.0
Image File Analysis
9:05 AM
9/15/2025



Module 05: Defeating Anti-forensics Techniques

Lab 1: SSD File Carving on a Linux File System

- Students performed file carving on a Linux SSD image using Autopsy to recover files and fragments from unallocated space when metadata was unavailable.
- This demonstrates how to retrieve evidence even when TRIM or other SSD features might limit recoverability.

Lab 2: Recovering Data from Lost/Deleted Disk Partition

- Students used EaseUS Data Recovery Wizard to recover a deleted partition.
- The lab highlighted methods to restore lost files, including malicious artifacts, from sections of the disk that had not been overwritten.

Lab 3: Cracking Application Passwords

- Students practiced using Passware Kit Forensic to recover passwords from protected files and applications.

- This lab reinforced how to gain access to encrypted evidence for investigation purposes.

Lab 4: Detecting Steganography

- Students explored StegSpy and OpenStego to detect hidden information in files.
- The lab demonstrated methods to identify concealed data within otherwise benign-looking files or images.

Overall Summary:
Module 5 provided hands-on experience in counteracting anti-forensics techniques, including file carving, partition recovery, password cracking, and steganography detection. These labs reinforce skills for recovering, analyzing, and interpreting digital evidence in scenarios where attackers attempt to obscure their tracks.