Module 03: Understanding Hard Disks and File Systems

Lab Scenario

Sam, a security professional at a company, discovered that one of the company's employees was gathering crucial, confidential information about the company and saving it on his/her computer so that he/she could use it later for an illicit purpose. Sam immediately started checking each of his employee's computers in order to identify the dishonest employee. In order to escape from being caught, the culprit employee permanently deleted the gathered information.

Sam called a forensics investigator to launch an investigation. Sam explained the situation to the investigator. After listening to the story, the investigator decided to analyze the file systems and recover the deleted files to catch the dishonest employee.

Lab Objectives

The objective of this lab is to help the students understand how to:

- Analyze file system of Linux image file
- Recover files deleted from a hard disk

Overview of Understanding Hard Disks and File Systems

While investigating a computer-based crime, it is most important to understand hard disks and file systems, as these are the major sources of data storage. People usually delete their tracks after committing a crime using a computer in order to avoid being traced. Therefore, recovering the deleted files of hard disks and analyzing file systems is important when investigating a computer-based crime.

Lab Tasks

Recommended labs to assist you in understanding hard disks and file systems:

- Analyzing file system of a Linux image
- Recovering deleted files from hard disks

Lab 1: Analyzing File System of a Linux Image

Lab Scenario

An inspector, who is probing a murder incident, has found a dead system in a crime scene and suspects that the system is related to the incident and could provide clues about it. When the inspector brings the system to the cyber forensics department, he/she creates

an image of the hard disk and begins to analyze the image using Autopsy. On further analysis of the file systems, the investigator finds some crucial evidence that might help in solving the case.

In order to investigate a hard disk, as a forensic investigator you must know the types of file systems and how to analyze them using various tools.

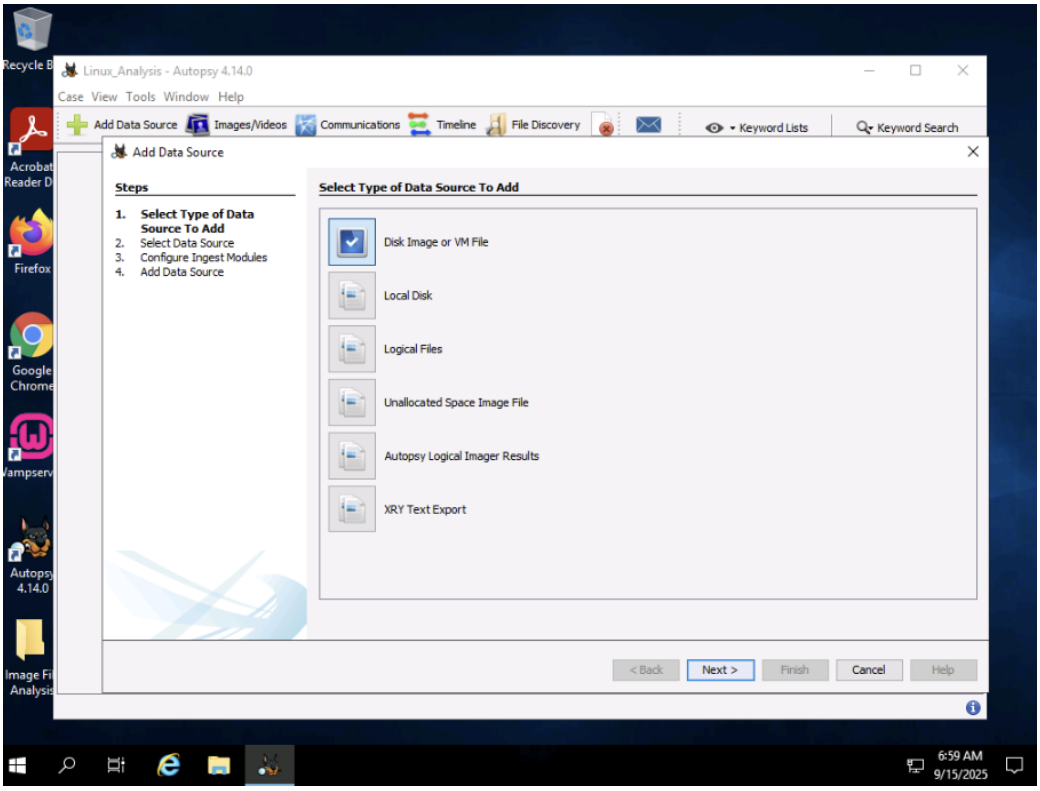
Lab Objectives

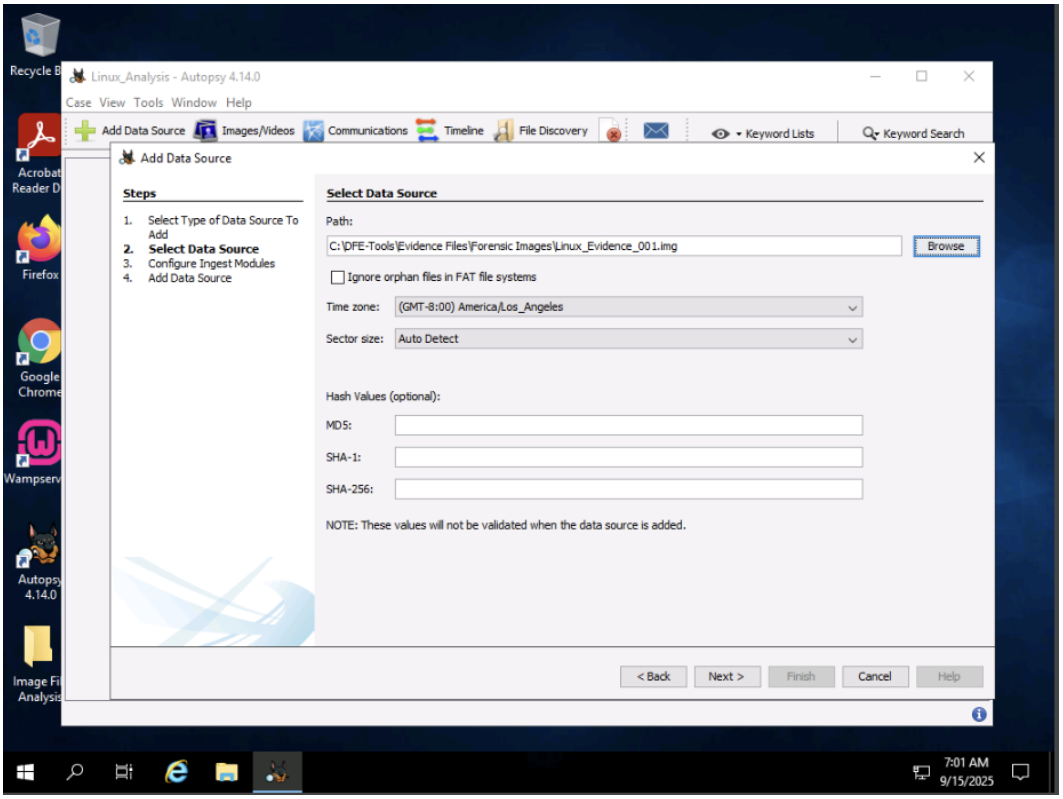
The objective of this lab is to help investigators learn and perform file system analysis using Autopsy. Performing file system analysis allows an investigator to determine the following information:

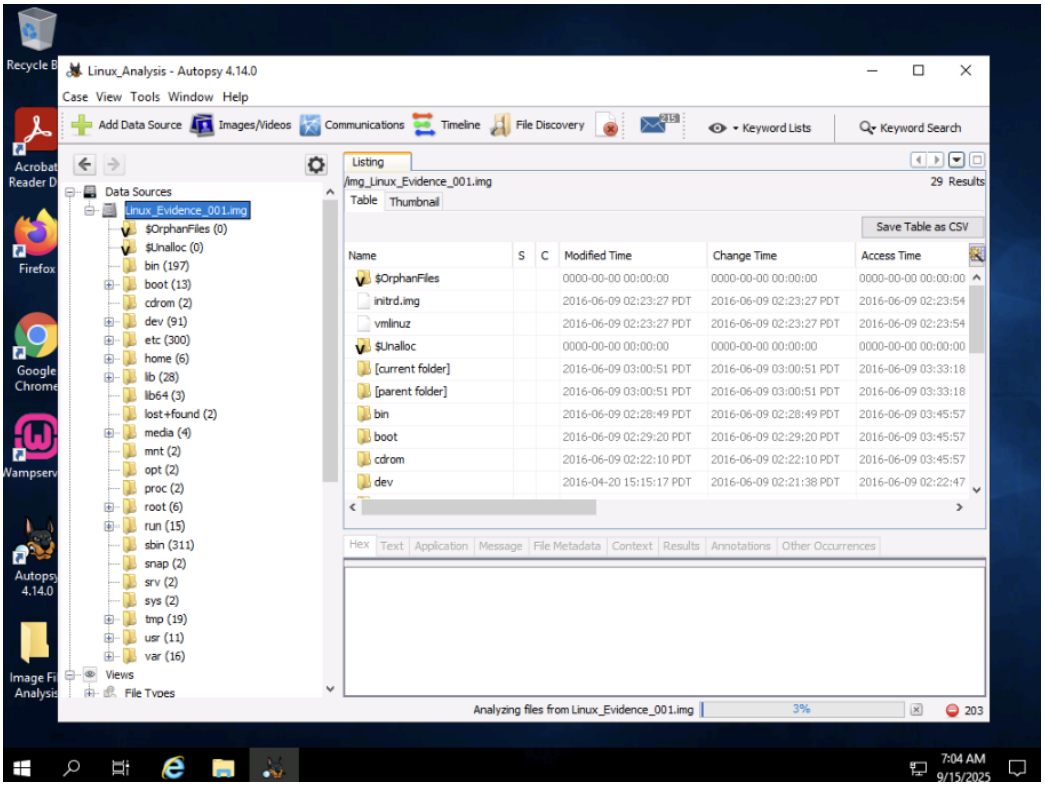
- File system type
- Metadata information
- Content information

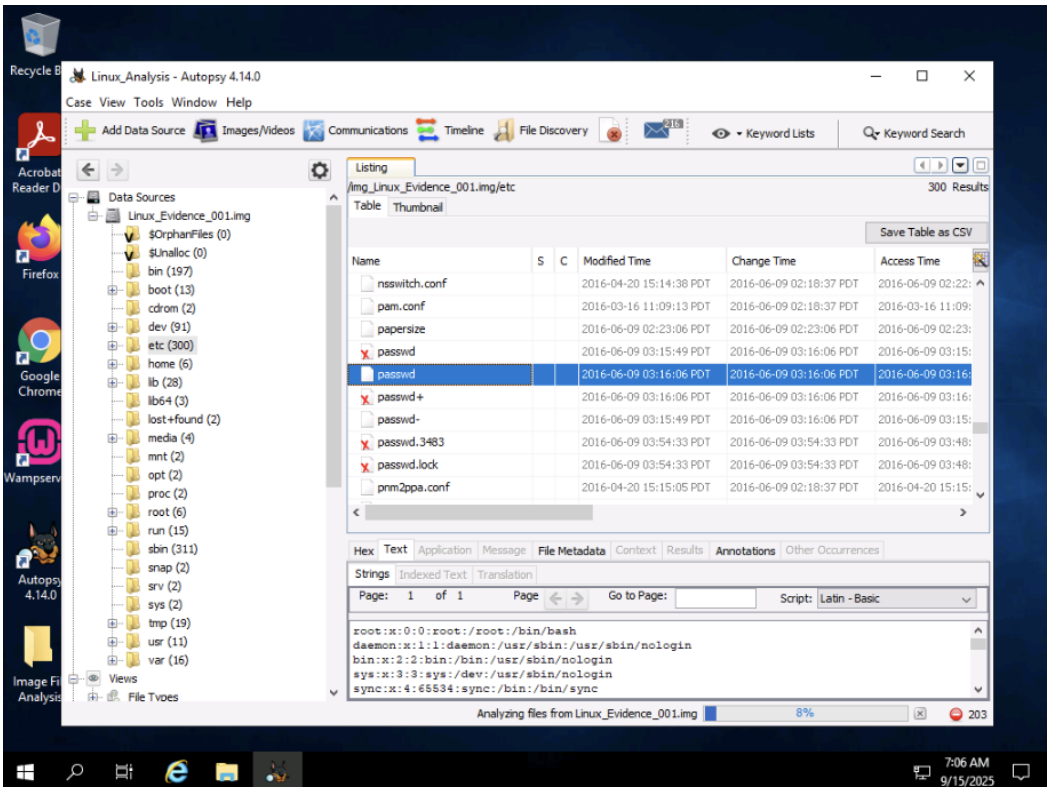
Overview of the Lab

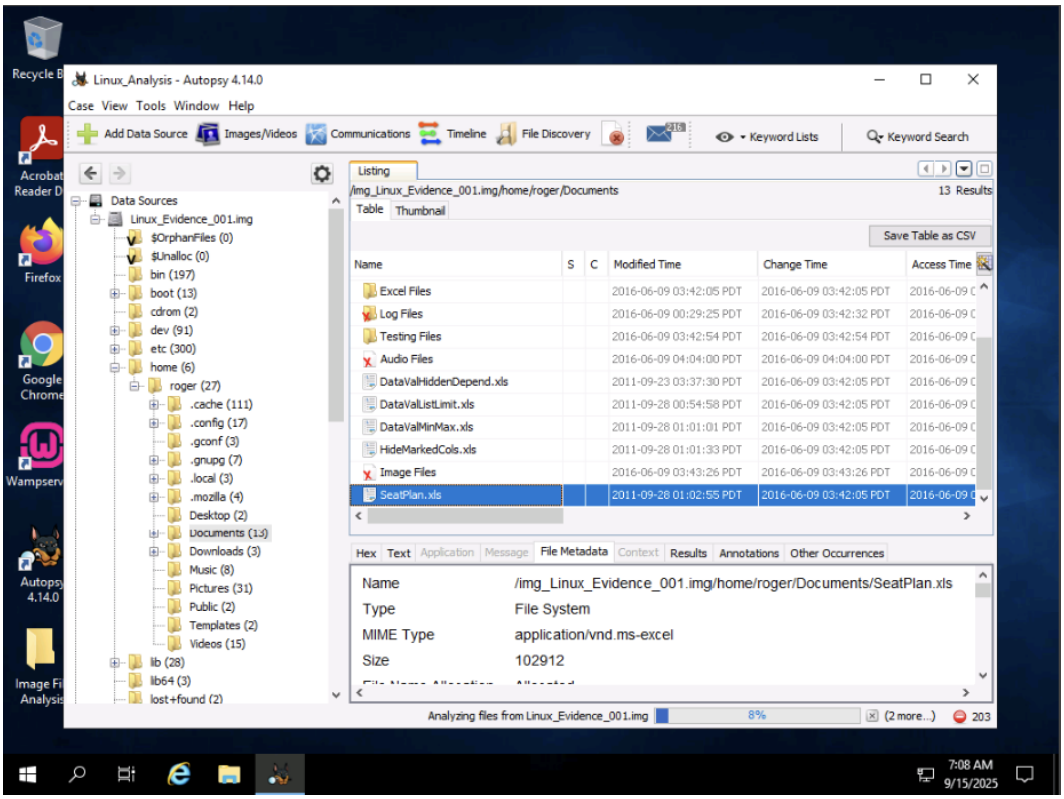
This lab familiarizes you with file system analysis using Autopsy. It helps you understand how to create a case in Autopsy and then examine the file system using the application.

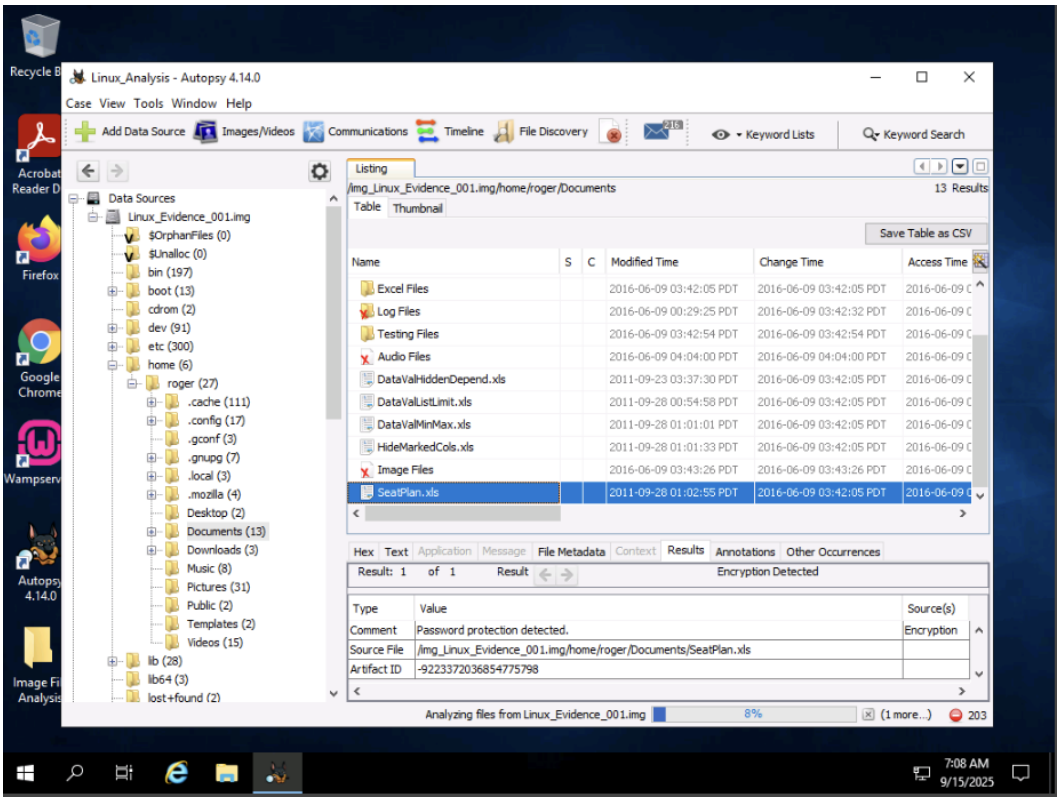


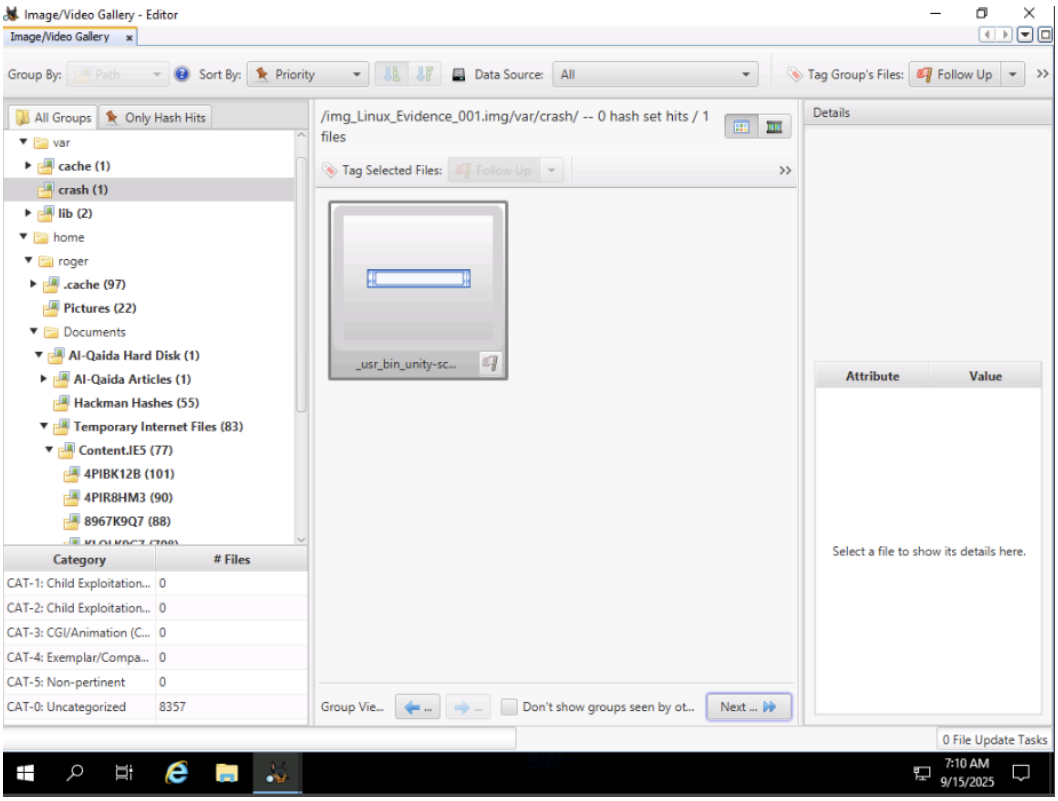

Linux_Analysis - Autopsy 4.14.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Timeline
File Discovery
Keyword Lists
Keyword Search
Add Data Source
Steps
1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source
Select Data Source
Path:
C:\DFE-Tools\Evidence Files\Forensic Images\Linux_Evidence_001.img
Browse
Ignore orphan files in FAT file systems
Time zone:
(GMT-8:00) America/Los_Angeles
Sector size:
Auto Detect
Hash Values (optional):
MD5:
SHA-1:
SHA-256:
NOTE: These values will not be validated when the data source is added.
< Back
Next >
Finish
Cancel
Help
7:01 AM
9/15/2025


Linux_Analysis - 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_001.img
$OrphanFiles (0)
$Unalloc (0)
bin (197)
boot (13)
cdrom (2)
dev (91)
etc (300)
home (6)
lib (28)
lib64 (3)
lost+found (2)
media (4)
mnt (2)
opt (2)
proc (2)
root (6)
run (15)
sbin (311)
snap (2)
srv (2)
sys (2)
tmp (19)
usr (11)
var (16)
Views
File Types
Listing
/img_Linux_Evidence_001.img
29 Results
Table
Thumbnail
Save Table as CSV
Name
S
C
Modified Time
Change Time
Access Time
$OrphanFiles
initrd.img
vmlinuz
$Unalloc
[current folder]
[parent folder]
bin
boot
cdrom
dev
Hex
Text
Application
Message
File Metadata
Context
Results
Annotations
Other Occurrences
Analyzing files from Linux_Evidence_001.img
3%
203
7:04 AM
9/15/2025


Linux_Analysis - Autopsy 4.14.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Timeline
File Discovery
Keyword Lists
Keyword Search
Listing
/img_Linux_Evidence_001.img/etc
300 Results
Table
Thumbnail
Save Table as CSV
Name
S
C
Modified Time
Change Time
Access Time
nsswitch.conf
2016-04-20 15:14:38 PDT
2016-06-09 02:18:37 PDT
pam.conf
2016-03-16 11:09:13 PDT
2016-06-09 02:18:37 PDT
papersize
2016-06-09 02:23:06 PDT
2016-06-09 02:23:06 PDT
passwd
2016-06-09 03:15:49 PDT
2016-06-09 03:16:06 PDT
passwd
2016-06-09 03:16:06 PDT
2016-06-09 03:16:06 PDT
passwd+
2016-06-09 03:16:06 PDT
2016-06-09 03:16:06 PDT
passwd-
2016-06-09 03:15:49 PDT
2016-06-09 03:16:06 PDT
passwd.3483
2016-06-09 03:54:33 PDT
2016-06-09 03:54:33 PDT
passwd.lock
2016-06-09 03:54:33 PDT
2016-06-09 03:54:33 PDT
pnm2ppa.conf
2016-04-20 15:15:05 PDT
2016-06-09 02:18:37 PDT
Hex
Text
Application
Message
File Metadata
Context
Results
Annotations
Other Occurrences
Strings
Indexed Text
Translation
Page: 1 of 1
Page
Go to Page:
Script: Latin - Basic
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
Analyzing files from Linux_Evidence_001.img
8%
203
Data Sources
Linux_Evidence_001.img
$OrphanFiles (0)
$Unalloc (0)
bin (197)
boot (13)
cdrom (2)
dev (91)
etc (300)
home (6)
lib (28)
lib64 (3)
lost+found (2)
media (4)
mnt (2)
opt (2)
proc (2)
root (6)
run (15)
sbin (311)
snap (2)
srv (2)
sys (2)
tmp (19)
usr (11)
var (16)
Views
File Types
7:06 AM
9/15/2025


Linux_Analysis - Autopsy 4.14.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Timeline
File Discovery
Keyword Lists
Keyword Search
Listing
/img_Linux_Evidence_001.img/home/roger/Documents
13 Results
Table
Thumbnail
Save Table as CSV
Name
S
C
Modified Time
Change Time
Access Time
Excel Files
2016-06-09 03:42:05 PDT
2016-06-09 03:42:05 PDT
Log Files
2016-06-09 00:29:25 PDT
2016-06-09 03:42:32 PDT
Testing Files
2016-06-09 03:42:54 PDT
2016-06-09 03:42:54 PDT
Audio Files
2016-06-09 04:04:00 PDT
2016-06-09 04:04:00 PDT
DataValHiddenDepend.xls
2011-09-23 03:37:30 PDT
2016-06-09 03:42:05 PDT
DataValListLimit.xls
2011-09-28 00:54:58 PDT
2016-06-09 03:42:05 PDT
DataValMinMax.xls
2011-09-28 01:01:01 PDT
2016-06-09 03:42:05 PDT
HideMarkedCols.xls
2011-09-28 01:01:33 PDT
2016-06-09 03:42:05 PDT
Image Files
2016-06-09 03:43:26 PDT
2016-06-09 03:43:26 PDT
SeatPlan.xls
2011-09-28 01:02:55 PDT
2016-06-09 03:42:05 PDT
Hex
Text
Application
Message
File Metadata
Context
Results
Annotations
Other Occurrences
Name
/img_Linux_Evidence_001.img/home/roger/Documents/SeatPlan.xls
Type
File System
MIME Type
application/vnd.ms-excel
Size
102912
Analyzing files from Linux_Evidence_001.img
8%
(2 more...)
203
Data Sources
Linux_Evidence_001.img
$OrphanFiles (0)
$Unalloc (0)
bin (197)
boot (13)
cdrom (2)
dev (91)
etc (300)
home (6)
roger (27)
.cache (111)
.config (17)
.gconf (3)
.gnupg (7)
.local (3)
.mozilla (4)
Desktop (2)
Documents (13)
Downloads (3)
Music (8)
Pictures (31)
Public (2)
Templates (2)
Videos (15)
lib (28)
lib64 (3)
lost+found (2)
7:08 AM
9/15/2025


Linux_Analysis - 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_001.img
$OrphanFiles (0)
$Unalloc (0)
bin (197)
boot (13)
cdrom (2)
dev (91)
etc (300)
home (6)
roger (27)
.cache (111)
.config (17)
.gconf (3)
.gnupg (7)
.local (3)
.mozilla (4)
Desktop (2)
Documents (13)
Downloads (3)
Music (8)
Pictures (31)
Public (2)
Templates (2)
Videos (15)
lib (28)
lib64 (3)
lost+found (2)
Listing
/img_Linux_Evidence_001.img/home/roger/Documents
13 Results
Table
Thumbnail
Save Table as CSV
Name
S
C
Modified Time
Change Time
Access Time
Excel Files
Log Files
Testing Files
Audio Files
DataValHiddenDepend.xls
DataValListLimit.xls
DataValMinMax.xls
HideMarkedCols.xls
Image Files
SeatPlan.xls
2011-09-28 01:02:55 PDT
Hex
Text
Application
Message
File Metadata
Context
Results
Annotations
Other Occurrences
Result: 1 of 1
Result
Encryption Detected
Type
Value
Source(s)
Comment
Password protection detected.
Encryption
Source File
/img_Linux_Evidence_001.img/home/roger/Documents/SeatPlan.xls
Artifact ID
-9223372036854775798
Analyzing files from Linux_Evidence_001.img
8%
(1 more...)
203
7:08 AM
9/15/2025


Image/Video Gallery - Editor
Image/Video Gallery
Group By:
Sort By:
Priority
Data Source:
All
Tag Group's Files:
Follow Up
All Groups
Only Hash Hits
var
cache (1)
crash (1)
lib (2)
home
roger
.cache (97)
Pictures (22)
Documents
Al-Qaida Hard Disk (1)
Al-Qaida Articles (1)
Hackman Hashes (55)
Temporary Internet Files (83)
Content.IE5 (77)
4PIBK12B (101)
4PIR8HM3 (90)
8967K9Q7 (88)
/img_Linux_Evidence_001.img/var/crash/ -- 0 hash set hits / 1 files
Tag Selected Files:
_usr_bin_unity-sc...
Details
Attribute
Value
Select a file to show its details here.
Category
Files
CAT-1: Child Exploitation...
CAT-2: Child Exploitation...
CAT-3: CGI/Animation (C...
CAT-4: Exemplar/Compa...
CAT-5: Non-pertinent
CAT-0: Uncategorized
8357
Group Vie...
Don't show groups seen by ot...
Next ...
0 File Update Tasks
7:10 AM
9/15/2025

Lab 2: Recovering Deleted Files from Hard Disks

Lab Scenario

The forensic investigators started scanning the computers for deleted data to catch the perpetrator, who has been collecting the company's private data for harmful purposes. To avoid identification, the perpetrator had deleted the data from the system. However, the investigators were able to trace the system used by the perpetrator by analyzing the file systems and recovering deleted data using the WinHex tool.

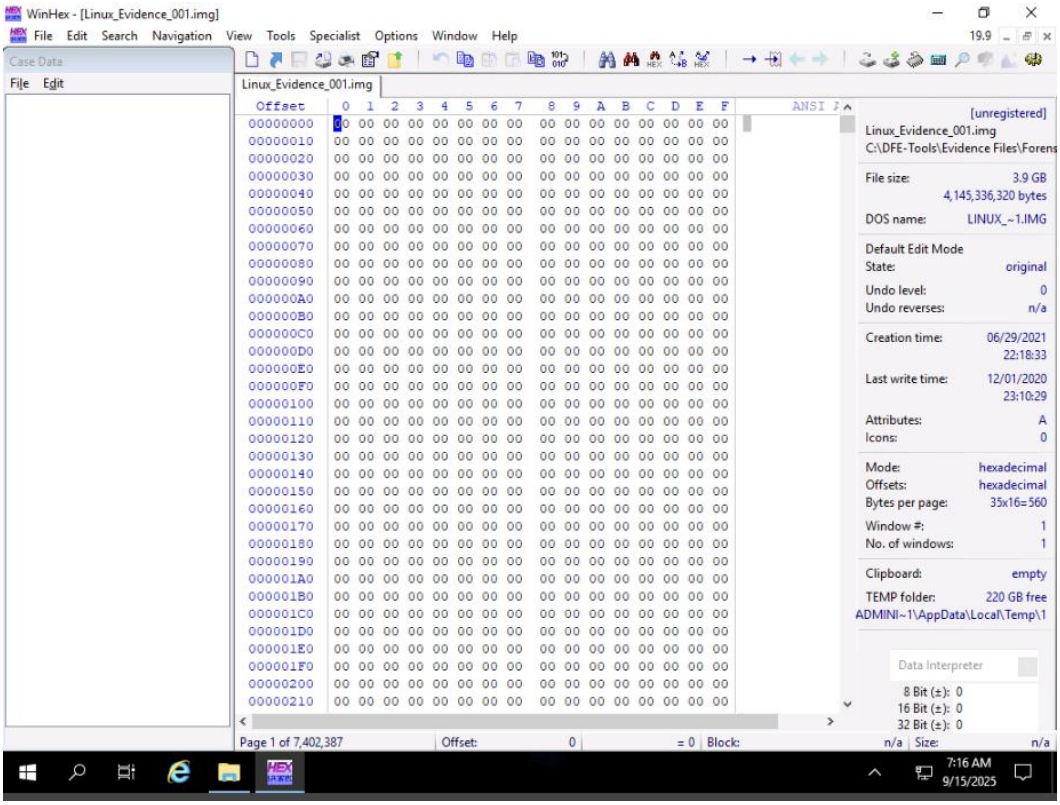
As a computer forensic investigator, you should know how to recover files that have been permanently deleted and the tools that can be used for recovering them.

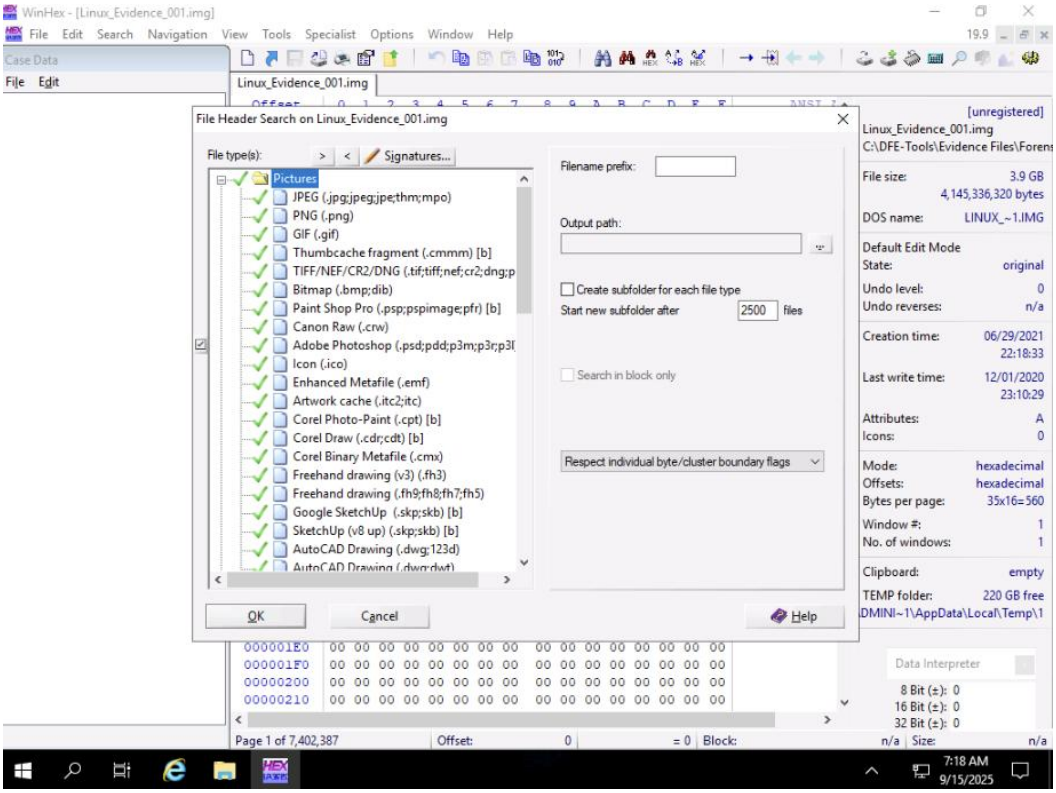
Lab Objectives

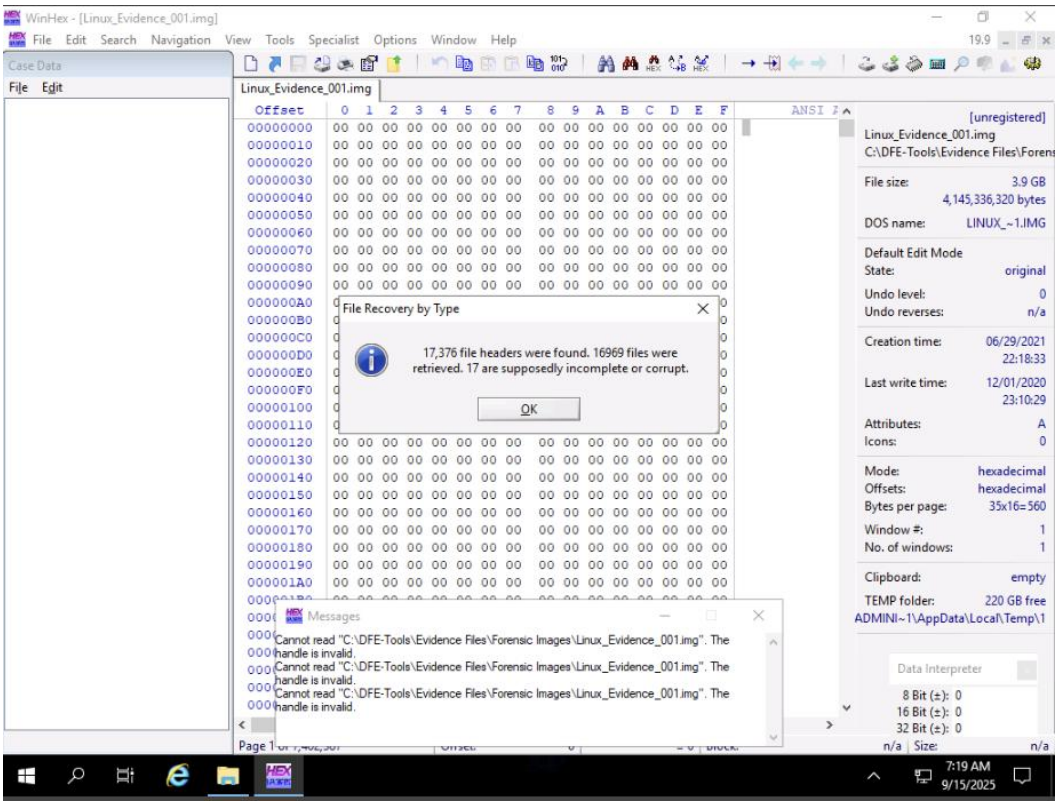
The objective of this lab is to help you understand how to recover files that have been permanently deleted using the WinHex tool.

Overview of the Lab

This lab familiarizes you with the WinHex tool. It helps you understand how to import an image into this application and recover files of specified file types from the image file.




WinHex - [Linux_Evidence_001.img]
File Edit Search Navigation View Tools Specialist Options Window Help
Case Data
File Edit
Linux_Evidence_001.img
File Header Search on Linux_Evidence_001.img
File type(s):
Signatures...
Pictures
JPEG (.jpg;jpeg;jpe;thm;mpo)
PNG (.png)
GIF (.gif)
Thumbcache fragment (.cmmm) [b]
TIFF/NEF/CR2/DNG (.tif;tiff;nef;cr2;dng;p
Bitmap (.bmp;dib)
Paint Shop Pro (.psp;pspimage;pfr) [b]
Canon Raw (.crw)
Adobe Photoshop (.psd;pdd;p3m;p3r;p3l
Icon (.ico)
Enhanced Metafile (.emf)
Artwork cache (.itc2;itc)
Corel Photo-Paint (.cpt) [b]
Corel Draw (.cdr;cdt) [b]
Corel Binary Metafile (.cmx)
Freehand drawing (v3) (.fh3)
Freehand drawing (.fh9;fh8;fh7;fh5)
Google SketchUp (.skp;skb) [b]
SketchUp (v8 up) (.skp;skb) [b]
AutoCAD Drawing (.dwg;123d)
AutoCAD Drawing (.dwg;dwt)
Filename prefix:
Output path:
Create subfolder for each file type
Start new subfolder after
2500
files
Search in block only
Respect individual byte/cluster boundary flags
OK
Cancel
Help
[unregistered]
Linux_Evidence_001.img
C:\DFE-Tools\Evidence Files\Forens
File size: 3.9 GB
4,145,336,320 bytes
DOS name: LINUX_~1.IMG
Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a
Creation time: 06/29/2021 22:18:33
Last write time: 12/01/2020 23:10:29
Attributes: A
Icons: 0
Mode: hexadecimal
Offsets: hexadecimal
Bytes per page: 35x16=560
Window #: 1
No. of windows: 1
Clipboard: empty
TEMP folder: 220 GB free
DMINI~1\AppData\Local\Temp\1
Data Interpreter
8 Bit (±): 0
16 Bit (±): 0
32 Bit (±): 0
Page 1 of 7,402,387
Offset: 0
Block:
Size:
7:18 AM
9/15/2025


WinHex - [Linux_Evidence_001.img]
File Edit Search Navigation View Tools Specialist Options Window Help
Case Data
File Edit
Linux_Evidence_001.img
Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F
File Recovery by Type
17,376 file headers were found. 16969 files were retrieved. 17 are supposedly incomplete or corrupt.
OK
Messages
Cannot read "C:\DFE-Tools\Evidence Files\Forensic Images\Linux_Evidence_001.img". The handle is invalid.
Cannot read "C:\DFE-Tools\Evidence Files\Forensic Images\Linux_Evidence_001.img". The handle is invalid.
Cannot read "C:\DFE-Tools\Evidence Files\Forensic Images\Linux_Evidence_001.img". The handle is invalid.
[unregistered]
Linux_Evidence_001.img
C:\DFE-Tools\Evidence Files\Forens
File size: 3.9 GB
4,145,336,320 bytes
DOS name: LINUX_~1.IMG
Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a
Creation time: 06/29/2021 22:18:33
Last write time: 12/01/2020 23:10:29
Attributes: A
Icons: 0
Mode: hexadecimal
Offsets: hexadecimal
Bytes per page: 35x16=560
Window #: 1
No. of windows: 1
Clipboard: empty
TEMP folder: 220 GB free
ADMINI~1\AppData\Local\Temp\1
Data Interpreter
8 Bit (±): 0
16 Bit (±): 0
32 Bit (±): 0
Size:
7:19 AM
9/15/2025

Module 03: Understanding Hard Disks and File Systems

Lab 1: Analyzing File System of a Linux Image

- The lab focused on analyzing a Linux disk image (Linux_Evidence_001.img) using Autopsy.
- Students created a new case in Autopsy, added the disk image, and explored the filesystem.
- Key tasks included examining folders/files (e.g., /etc/passwd), viewing file metadata, Hex and Annotations, and validating evidence using MD5 hashes.
- Image and video files in the evidence were also reviewed in the Autopsy gallery.
- This lab reinforced understanding of file system structures, metadata analysis, and integrity verification.

Lab 2: Recovering Deleted Files from Hard Disks

- The lab focused on recovering deleted files from the Linux disk image using WinHex.
- Students opened the image in WinHex, selected file types to recover (e.g., images), and specified a target folder.
- The recovery process was executed, and recovered files were viewed in the destination folder.
- Some files were not retrievable due to lab constraints (step 14 did not occur).
- This lab reinforced skills in data recovery, file type identification, and handling forensic images.

Overall Summary:
Module 3 provided hands-on experience in analyzing file systems, exploring metadata, calculating hashes, and recovering deleted data. Both labs demonstrated practical forensic methods for extracting, validating, and preserving digital evidence in real-world scenarios.