SHRINIDHI
231901050

EXPERIMENT-2

Aim :

Live Forensics Case Investigation using Autopsy .

Here is the procedure and expected result for Experiment 2 (Live Forensics Case Investigation using Autopsy):

Procedure :

1. ***Download and Install Autopsy:***
   o Obtain Autopsy from the official website and install it on your PC.
2. ***Create a New Case:***
   o Launch Autopsy, select "New Case".
   o Enter a case name, base directory, and specify report location.
3. ***Enter Case Details:***
   o Fill in case number and examiner details, then click Finish.
4. ***Add Data Source:***
   o In the new window, choose "Add Data Source".
   o Browse to the file path of your evidence (disk image, device, etc.) and add it.
5. ***Configure Ingest Modules:***
   o Select all ingest modules to perform a comprehensive investigation (file analysis, extracting artifacts, operating system info, user accounts, web history, downloads, cookies, email addresses, and more).
6. ***Start Investigation:***
   o Click Finish in Add Data Source. Autopsy will process the data and add it to the local database.
7. ***Explore Investigation Results:***
   o After processing, review outputs by clicking on:
      □ ***Devices Attached***: See connected devices.
      □ ***EXIF Metadata***: Inspect image info.
      □ ***Installed Programs***: View programs on the system.
      □ ***Operating System Information***: Analyze OS details.
      □ ***Operating System User Account***: List user accounts.
      □ ***Recent Documents***: Find recently opened docs.
      □
      □ ***Web Bookmarks/History/Downloads/Search/Cookies***: Analyze user browsing artifacts.
      □ ***Email addresses***: Review found emails.

Data Source Integrity Module:	4.22.1
Email Parser Module:	4.22.1
Embedded File Extractor Module:	4.22.1
Encryption Detection Module:	4.22.1
Extension Mismatch Detector Module:	4.22.1
File Type Identification Module:	4.22.1
GPX Parser Module:	1.2
Hash Lookup Module:	4.22.1
Interesting Files Identifier Module:	4.22.1
Keyword Search Module:	4.22.1
PhotoRec Carver Module:	7.0
Picture Analyzer Module:	4.22.1
Recent Activity Module:	4.22.1
Virtual Machine Extractor Module:	4.22.1
YARA Analyzer Module:	4.22.1
iOS Analyzer (iLEAPP) Module:	4.22.1

Ingest History:

Job 1:

Data Source:	disk.vmdk
Status:	STARTED
Enabled Modules:	Recent Activity
	Hash Lookup
	File Type Identification
	Extension Mismatch Detector
	Embedded File Extractor
	Picture Analyzer
	Keyword Search
	Email Parser
	Encryption Detection
	Interesting Files Identifier
	Central Repository
	PhotoRec Carver
	Virtual Machine Extractor
	Data Source Integrity
	Android Analyzer (aLEAPP)
	DJI Drone Analyzer
	YARA Analyzer
	iOS Analyzer (iLEAPP)

Data Source Integrity
Android Analyzer (aLEAPP)
DJI Drone Analyzer
YARA Analyzer
iOS Analyzer (iLEAPP)

iOS Analyzer (iLEAPP)
GPX Parser
Android Analyzer

Powered by Autopsy Open Source Digital Forensics Platform - www.sleuthkit.org

Result

Thus, the forensic tools executed successfully, and the evidence was captured and analyzed accurately.