Experiment No.9
Case Study: Kali Linux Tools
Date of Performance:
Date of Submission:

Aim: Case Study- Kali Linux Tools

Objective:

1. To develop analysis ability in the student to perform the forensics investigation using Kali Linux tools
2. To gain the knowledge of various Kali Linux tools

Theory:

Tool 1: Wireshark

Category: Network Traffic Analysis
Purpose: Captures and analyzes packets at various layers of the network stack.
Usage:

•Launched via terminal: wireshark

•Captured live traffic on interface eth0

•Applied filters like http, ip.src == x.x.x.x to isolate traffic

•Exported .pcap file for offline analysis
Relevance in Investigation:
Helpful in identifying data exfiltration, malware communication with C2 servers, and suspicious port activity.

Tool 2: Volatility

Category: Memory Forensics
Purpose: Analyzes volatile memory (RAM dumps) for evidence of running processes, injected code, passwords, etc.
Usage:

•Ran: vol.py -f memory.img --profile=Win7SP1x64 pslist

•Detected running processes and used malfind to detect injected code
Relevance in Investigation:
Volatility helps in analyzing RAM snapshots to detect malware that doesn't touch disk, and to identify in-memory persistence techniques.

Tool 3: Scalpel

Category: Data Carving
Purpose: Recovers deleted files from disk images by searching for known file headers and footers.
Usage:

•Edited /etc/scalpel/scalpel.conf to uncomment desired file types (e.g., .jpg, .pdf)

•Ran: scalpel disk.img -o output/
Relevance in Investigation:
Extracted image and PDF files from deleted space — useful for recovering deleted evidence like documents or images.

Tool 4: Bulk_Extractor

Category: Metadata Extraction
Purpose: Extracts email addresses, phone numbers, URLs, and other features from raw disk images.
Usage:

•Ran: bulk_extractor -o results/ -e email disk.img

•Parsed email.txt to find communications
Relevance in Investigation:
Recovered email evidence from deleted areas; useful in cyberstalking, fraud, and phishing investigations.

Tool 5: Network Miner

Category: Passive Network Forensics
Purpose: Parses .pcap files to extract files, sessions, credentials, and host activity.
Usage:

•Loaded .pcap file and reviewed extracted files and sessions
Relevance in Investigation:
Quickly retrieved credentials and file transfers from intercepted traffic, supporting man-in-the-middle and data leak investigations.

Tool 6: Autopsy

Category: Full Forensic Suite
Purpose: Provides a GUI to analyze disk images for user activity (files, browser history, emails, etc.)
Usage:

•Created new case, added .img file, selected ingest modules

•Viewed deleted files, browser history, and timelines
Relevance in Investigation:
A complete tool for disk-level investigation, especially for beginners or when GUI is preferred.

Tool 7: Foremost

Category: File Recovery / Data Carving
Purpose: Recovers files based on headers/footers from raw disk images.
Usage:

- Run: foremost -i disk.img -o recovered_files/
- Extracted files like .jpg, .doc, and .zip from deleted areas
  Relevance in Investigation:
  Used to retrieve deleted evidence such as photos, documents, and compressed archives that are no longer accessible through file system.

Tool 8: Binwalk

Category: Firmware Analysis / Embedded File Extraction
Purpose: Analyzes binary files and extracts embedded files or firmware components.
Usage:

- Run: binwalk firmware.bin
- Used -e flag to extract contents: binwalk -e firmware.bin
  Relevance in Investigation:
  Helpful in examining IoT devices or malware-packed firmware to detect hidden payloads or trojans.

Tool 9: Xplico

Category: Network Forensics & Traffic Reconstruction
Purpose: Reconstructs application-level data (emails, HTTP, VoIP, etc.) from .pcap files.
Usage:

- Accessed via browser after running: xplico
- Uploaded .pcap file and viewed decoded sessions, emails, chat messages
  Relevance in Investigation:
  Valuable in reconstructing user activity from intercepted traffic — especially webmail and social media communications.

Tool 10: ExifTool

Category: Metadata Extraction
Purpose: Reads, writes, and edits metadata in image, document, and media files.
Usage:

- Run: exiftool image.jpg
- Extracted timestamp, GPS, camera model, and editing software data
  Relevance in Investigation:

Essential in cases involving photos or videos — can identify when, where, and with which device the media was created or manipulated.

Conclusion:

The exploration of multiple Kali Linux tools in this case study demonstrates the depth and versatility of the platform in conducting digital forensic investigations. Each tool serves a distinct function—ranging from network analysis, memory forensics, file recovery, and metadata extraction to firmware analysis and traffic reconstruction. Tools like Wireshark, Volatility, Scalpel, Bulk_Extractor, Network Miner, Autopsy, Foremost, Binwalk, Xplico, and ExifTool equip investigators with the capabilities to uncover hidden, deleted, or obscured digital evidence.

By leveraging these tools, investigators can reconstruct timelines, trace unauthorized activities, extract communication artifacts, and recover critical files that support the legal resolution of cybercrime cases. Kali Linux, as a unified platform, enhances the effectiveness, efficiency, and reliability of forensic workflows, making it indispensable for modern digital forensic practices.