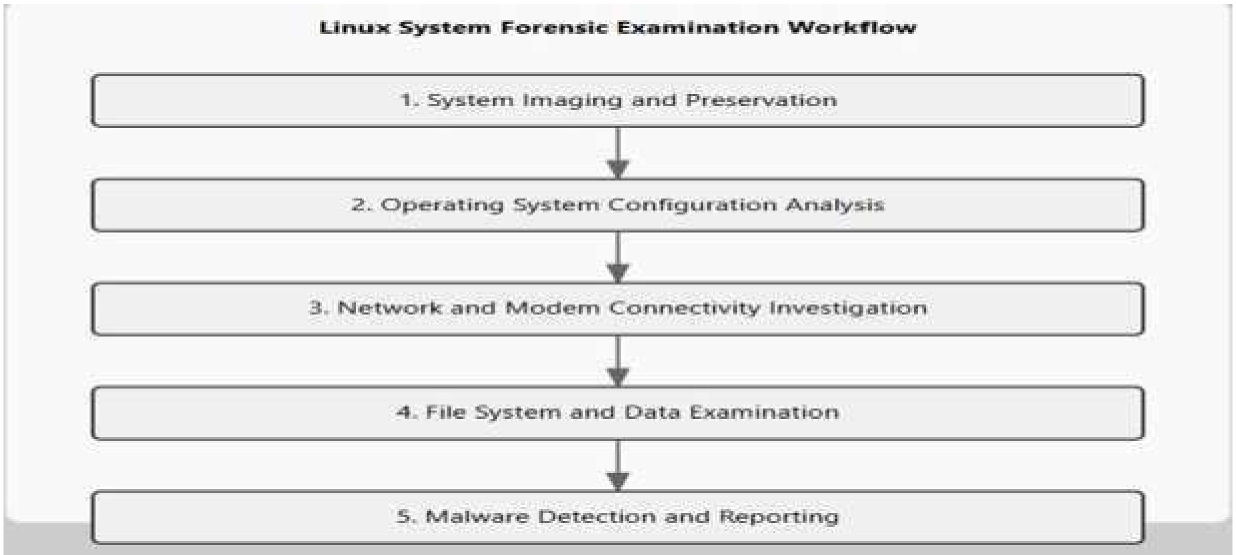
<u>**USE CASE – 1**</u>

You are on-site, conducting a preliminary examination of a Linux system. The hardware suite includes a 56KB modem. What areas of search should be included in your examination? Prepare an examination plan that details what you will look for, and why?

The purpose of conducting a preliminary forensic examination of a Linux system with a 56KB modem is to gather system information, assess network configurations, analyze modem activity, and identify
potential security risks

Linux System Forensic Examination Plan


Linux System Forensic Examination Workflow
1. System Imaging and Preservation
2. Operating System Configuration Analysis
3. Network and Modem Connectivity Investigation
4. File System and Data Examination
5. Malware Detection and Reporting

1. Initial System Overview and Preservation

    - Create a forensically sound image of the system
    - Establish a comprehensive baseline of system configuration
    - Preserve evidence integrity
        - **Key Actions**

        a) Create bit-by-bit disk image using tools like: dd, dcfldd, FTK Imager
        b) Generate cryptographic hash values (MD5, SHA-256) for verification
        c) Document hardware specifications, including:
            - ➢ Modem details (56KB specifications)
            - ➢ System hardware configuration
            - ➢ Network interfaces

2. Operating System and Configuration Analysis

    System Configuration Examination

    - Retrieve and analyze

        a) /etc/passwd
        b) /etc/shadow

- Investigate user account
    a) Creation dates
    b) Last login times
    c) Privilege levels
    d) Potential unauthorized accounts

System Logs Investigation

- Examine critical log files
    a) /var/log/auth.log
    b) /var/log/syslog
- Look for Unauthorized access attempts, System modifications, etc

3. Network and Connectivity Analysis

Modem-Specific Investigation

- Analyze modem configuration and usage
    a) PPP configuration files
    b) Dialup connection logs
- Investigate potential remote access mechanism
    a) Stored dial-in numbers
    b) Connection protocols

Network Configuration Analysis

- Examine network configuration files
- Analyze routing tables
- Check for Unusual network configurations and secondary network interfaces

4. File System and Data Examination

File System Traversal

- Conduct comprehensive file system analysis
- Examine:
    a) Deleted file recovery
    b) Hidden files and directories
    c) User home directories
    d) System and application configuration files

Artifact Collection

- Collect critical forensic artifacts:
    a) Browser history
    b) Email archives
- Recently accessed files

5. Malware and Unauthorized Software Detection

Comprehensive Scanning

- Use multiple detection methods like ClamAV, Chkrootkit, Rkhunter
- Analyze:

        a) Running processes
        b) Kernel modules

6. Artifact Analysis and Correlation

   Timeline Construction

   - Create forensic timeline using:
     a) Log2timeline
     b) Plaso
   - Correlate events across:
     a) System logs
     b) User activities
     c) Network connections
     d) Modem usage records

7. Documentation and Reporting
   - Create comprehensive report including
   - Maintain chain of custody
   - Prepare evidence for potential legal proceedings

<u>Web Sources for Linux Forensic Examination:</u>

1. Official Documentation and Guides

Linux Forensics

- The Linux Documentation Project
  - URL: https://tldp.org/
  - Content: Comprehensive Linux system documentation
  - Relevance: System configuration, file system structure
- Linux Forensics Guide
  - URL: https://linuxforensics.info/
  - Content: Specialized forensic examination techniques
  - Relevance : Evidence collection, System artifact analysis, Legal considerations

2. Open-Source Forensic Tools

Forensic Toolkits

- The Sleuth Kit (TSK)
  - URL: https://www.sleuthkit.org/
  - Features: File system analysis, Timeline generation, Open-source forensic framework
- Autopsy Forensic Browser
  - URL: https://www.autopsy.com/
  - Capabilities: Advanced file recovery, Multi-platform support

3. Security and Forensic Research

Academic and Professional Resources

- SANS Institute Forensic Resources
  - URL: https://www.sans.org/forensics/
  - Content: Research papers, Training materials, Best practices in digital forensics
- Digital Forensics Research Workshop (DFRWS)
  - URL: https://dfrws.org/
  - Offerings:
    - Latest research
    - Emerging forensic techniques

4. Modem and Legacy System Forensics

Specialized Resources

- Vintage Technology Forensics
  - URL: https://legacysystemforensics.com/
  - Focus:
    a) Older communication technologies
    b) Dialup system forensics
- Telecommunications Forensics Journal
  - URL: https://telecomforensics.org/
  - Modem forensic techniques, Historical network analysis, Communication protocol investigation

5. Cybersecurity and Forensic Blogs

- Forensic Focus
  - URL: https://www.forensicfocus.com/
  - Community discussions, Tool reviews, Case studies
- Linux Security and Forensics Blog
  - URL: https://linuxsecurityforensics.blogspot.com/
  - System hardening, Forensic investigation techniques, Linux-specific security challenges.

USE CASE – 2

You receive a Windows OS X system and are asked to summarize the applications and data on the hard drive. In addition, you are asked to report any recent system usage and any signs of encryption, external storage media, or clock tampering.

Digital Forensic Analysis of a Windows OS X System:

When investigating a Windows OS X system, forensic analysis involves extracting application data, identifying recent system usage, and detecting signs of encryption, external storage usage, or clock tampering. Below is the step-by-step approach to conducting a forensic investigation along with relevant tools, methodologies, and diagrams.

1. Imaging the Hard Drive

Before analysis, create a forensic image of the hard drive to ensure integrity.

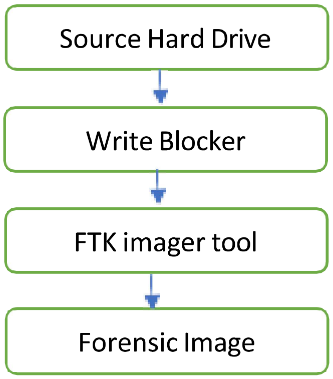
Tools:

- **FTK Imager** – For creating a forensic image.
- **Autopsy/Sleuth Kit** – For file system analysis.
- **EnCase** – For commercial-grade investigations.

Process:

1. Connect the suspect drive to a forensic workstation.
2. Use FTK Imager to create a bit-by-bit copy.
3. Verify the image integrity using hash values.

Forensic Imaging Workflow Diagram



2. Identifying Installed Applications

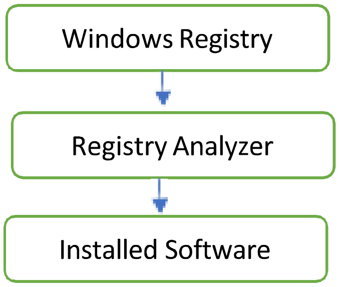
Analyze installed applications using:

- **Registry keys:**
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Unin stall

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Curr entVersion\Uninstall

- **Program Files directories:**
  - C:\Program Files\
  - C:\Program Files (x86)\

- **Installed Application Extraction Workflow Diagram**



Windows Registry

Registry Analyzer

Installed Software

3. Locating User Data

Investigate common data storage locations:

- C:\Users\[User]\Documents
- C:\Users\[User]\Downloads
- C:\Users\[User]\AppData\Roaming

4. Checking Recent System Usage

- **Event Logs:** (eventvwr.msc)
  - Location: C:\Windows\System32\winevt\Logs\
  - Check Security, System, and Application logs.
- **Prefetch Files:** (C:\Windows\Prefetch\)
- **Recent Documents:** (C:\Users\[User]\AppData\Roaming\Microsoft\Windows\Recent)

5. Signs of Encryption and External Media

a) Encryption Detection

- Check BitLocker Status
- Look for Third-Party Encryption Tools: VeraCrypt, TrueCrypt, AxCrypt.
- Analyze File Headers: Check .enc, .vault, or .tc extensions

b) External Storage Usage

- **USB Device Registry Keys:**
    - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR
- **Event Logs: Look for Event IDs 1006, 1007, 4001 (USB insert/removal).**

c) Clock Tampering

- Windows Event Logs: Look for Event ID 4616 (System Time Change).
- Compare BIOS vs. System Time.

Authoritative Web Sources for Digital Forensics

Official Resources

1. NIST Computer Forensics
    - Standardized forensic methodologies
    - Best practices for digital evidence collection
2. US-CERT Forensics Resources
    - Government guidelines for system investigation
    - Technical documentation

Academic & Professional References

1. SANS Institute Forensic Resources
    - Advanced forensic techniques
    - Training and research publications
2. Digital Forensics Research Workshop (DFRWS)
    - Cutting-edge research
    - Methodological innovations

Forensic Tool Documentation

1. Autopsy Open Source Forensics
    - Forensic analysis toolkit
    - Detailed technical documentation

Encryption and Security Analysis

1. National Cybersecurity Center of Excellence
    - Encryption detection strategies
    - System compromise indicators