



4/27/2025

INTERNATIONAL CYBERSECURITY AND DIGITAL FORENS ACADEMY

INT313 - Computer and Digital Forensics



AYILARA BUSARI DARE
IDEAS/24/28133

FACILITATOR: MAHMUD IBRAHIM KANI

INT313 - Computer and Digital Forensics – Lab 1 Lab Title: Digital Forensics Investigation of a USB Drive

A digital forensics investigation of a USB drive involves analyzing the device to extract and interpret data. This includes identifying the last time the USB drive was attached, using tools like Registry Editor, PowerShell, and USB Deview. The process encompasses several stages: preservation, collection, validation, identification, analysis, interpretation, and documentation of the findings. USB forensics focuses on external storage devices, examining the data stored on them for potential evidence. The goal is to understand the driver's usage and recover information related to its use.

The objective of this lab is to introduce the fundamentals of digital forensics through a practical investigation of a USB drive image. This practice will expose to the use of Autopsy to recover files and analyze data, applying the steps of digital investigation to understand the significance of the recovered information.

Part 1: Understanding Digital Forensics

1. What are Digital Forensics?

- Research and summarize the definition of digital forensics. Explain its importance in the context of investigations.

Definition of Digital Forensics

Digital forensics is the process of collecting, preserving, analyzing, and presenting electronic data in a manner that is legally acceptable. It involves the use of specialized techniques and tools to investigate incidents involving digital devices, such as computers, smartphones, and external storage media.

Importance in Investigations

Digital forensics plays a crucial role in investigations for several reasons:

1. **Evidence Collection:** It allows for the systematic gathering of digital evidence that can be critical in criminal cases, civil disputes, or corporate investigations.
2. **Data Recovery:** Forensic techniques can recover deleted or corrupted files, providing valuable information that may otherwise be lost.
3. **Timeline Creation:** Investigators can determine the sequence of events leading up to an incident by analyzing timestamps and data interactions.

4. **Legal Compliance:** Properly conducted digital forensics ensure that evidence is collected and handled in accordance with legal standards, making it admissible in court.
5. **Incident Response:** In the case of data breaches or cyber-attacks, digital forensics helps in understanding how the breach occurred, assessing its impact, and preventing future incidents.
6. **Accountability and Deterrence:** The application of digital forensics in investigations can deter criminal activity by increasing the likelihood of detection and prosecution.

2. Steps of Digital Investigation:

- Outline the essential steps involved in a digital investigation:
 - Identification
 - Preservation
 - Analysis
 - Presentation

1. Identification

- **Determine Scope:** Define the objectives of the investigation and identify relevant devices, data sources, and potential evidence.
- **Identify Key Evidence:** Decide which data types are pertinent (e.g., documents, emails, databases) and collect necessary information about the environment where the evidence might reside (e.g., network architecture, device configurations).

2. Preservation

- **Secure Evidence:** Ensure that all digital evidence is secured to prevent alteration or loss. This may involve physically securing devices or preventing data tampering.
- **Create Forensic Copies:** Use write-blockers to make bit-by-bit copies (forensic images) of data storage devices, ensuring the original data remains unchanged.
- **Document Everything:** Maintain a detailed chain of custody, documenting how and when evidence was collected to ensure its integrity for legal purposes.

3. Analysis

- **Examine Data:** Use forensic tools and methodologies to analyze the preserved data. This includes searching for specific files, recovering deleted items, and identifying relevant artifacts (e.g., logs, metadata).

- **Interpret Findings:** Correlate and interpret the data to build a timeline of events, determine the context of the evidence, and understand the significance of the findings.
- **Use of Tools:** Employ specialized software for data recovery, analysis, and reporting, such as EnCase, Autopsy, or FTK.

4. Presentation

- **Prepare Reports:** Document the findings clearly and concisely in a report. The report should include methodologies, findings, and conclusions drawn from the analysis.
- **Courtroom Readiness:** Ensure that the evidence and reports meet legal standards for admissibility and can be clearly explained to non-technical audiences, such as juries and judges.
- **Testify if Necessary:** Be prepared to present findings in court, explaining the investigation process, the evidence discovered, and its implications.

Part 2: Investigating the USB Drive with Autopsy

1. Setup Autopsy:

- Step 1: Download the USB drive image file from this link.
- Step 2: Install Autopsy if it is not already installed. Follow the instructions specifically to your operating system.
- Step 3: Load the USB drive image into Autopsy.

Answer

An autopsy was downloaded and installed, The USB drive image file called Ch01InChap01.dd was downloaded, open a new case on the autopsy named case001 and the name of the investigator. The path to the USB image was provided and it ready for file analysis.

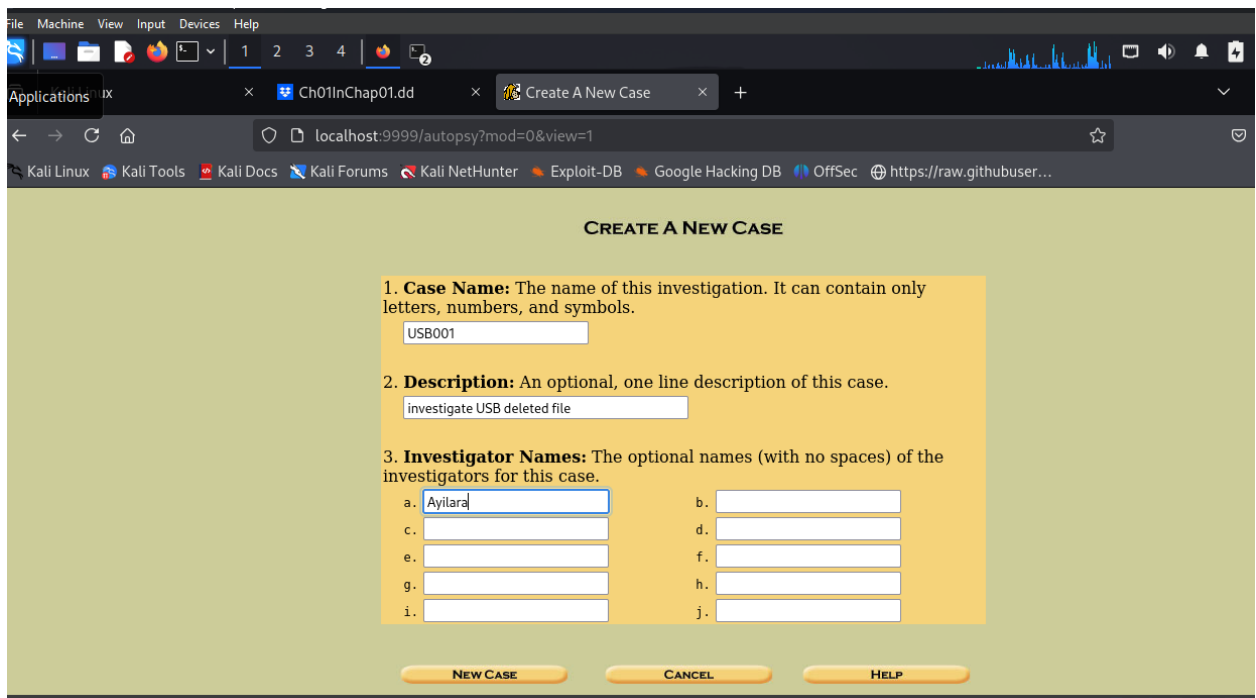


Figure 1: Load the USB drive image into Autopsy

2. File Recovery:

- Task: Use Autopsy to recover deleted Word files and images from the USB drive.

Answer

The USB image was downloaded and imported to autopsy for analysis by follow step by step instructions. The investigation discovered that four (4) files were deleted from the USB drive.

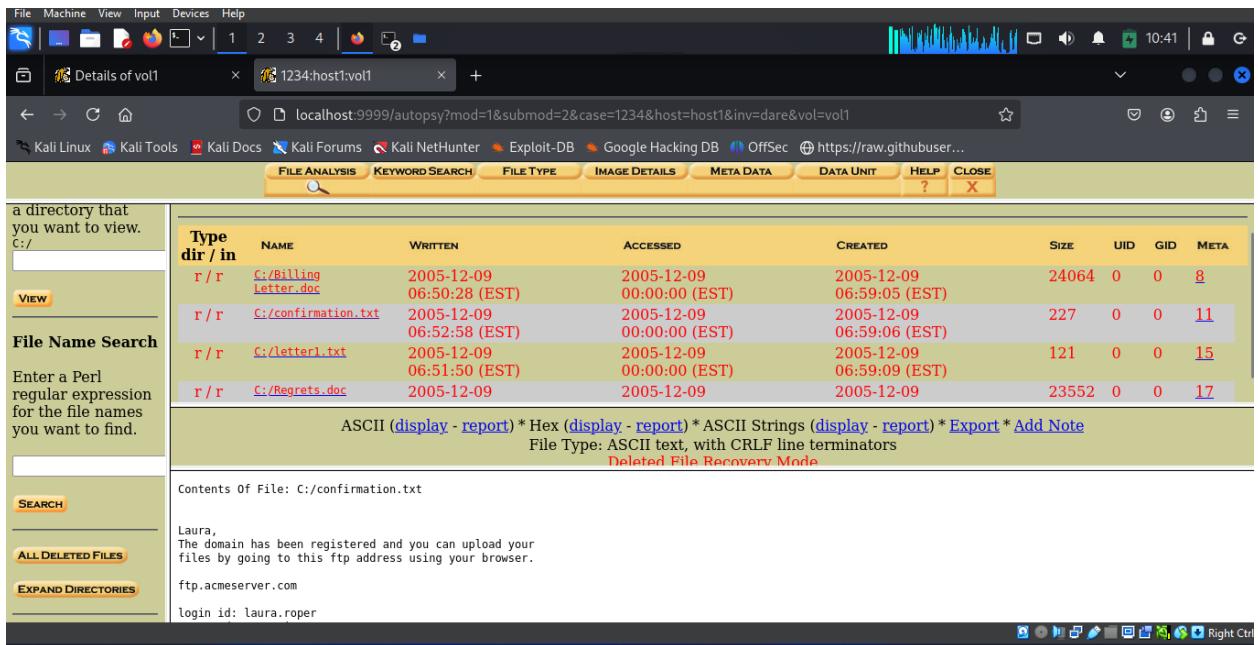


Figure 2: Recovery files

- Deliverable: Document the names and types of the recovered files in your lab report.

Answer

The documents and files recovered are Billing letter.doc, confirmation.txt, letter1.txt and Regret.doc, these files are deleted file and other files such clients info.mdb and income.xls

Part 3: Conducting Keyword Searches

1. Keyword Search:

- Task: Conduct a keyword search related to George Montgomery Document the keywords used.

• Answer

With keyword George Montgomery appear three (3) times and it shows that it is name of someone.

<div> <div> <div>←</div> <div>→</div> <div>↺</div> <div>🏠</div> </div> <div>localhost:9999/autopsy?mod=1&submod=2&case=1234&host=host1&inv=dare&vol=vol1</div> <div> <div>☆</div> <div>🔍</div> <div>👤</div> <div>🔖</div> <div>☰</div> </div> </div> <div> <div>Kali Linux</div> <div>Kali Tools</div> <div>Kali Docs</div> <div>Kali Forums</div> <div>Kali NetHunter</div> <div>Exploit-DB</div> <div>Google Hacking DB</div> <div>OffSec</div> <div>https://raw.githubusercontent.com/...</div> </div>									
<div> <div>FILE ANALYSIS</div> <div>KEYWORD SEARCH</div> <div>FILE TYPE</div> <div>IMAGE DETAILS</div> <div>META DATA</div> <div>DATA UNIT</div> <div>HELP</div> <div>CLOSE</div> </div>									
<div>Directory Seek</div> <div>Enter the name of a directory that you want to view.</div> <div>c:/</div> <div>VIEW</div> <div>File Name Search</div> <div>Enter a Perl regular expression for the file names you want to find.</div> <div>SEARCH</div>	v / v	\$FAT2	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	4608	0	0	45781
	v / v	\$MBR	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	512	0	0	45779
	✓ r / r	Billing_Letter.doc	2005-12-09 06:50:28 (EST)	2005-12-09 00:00:00 (EST)	2005-12-09 06:59:05 (EST)	24064	0	0	8
	r / r	Client_Info.mdb	2005-12-09 06:53:58 (EST)	2005-12-09 00:00:00 (EST)	2005-12-09 06:59:01 (EST)	104448	0	0	5
	✓ r / r	confirmation.txt	2005-12-09 06:52:58 (EST)	2005-12-09 00:00:00 (EST)	2005-12-09 06:59:06 (EST)	227	0	0	11
	r / r	Income.xls	2005-12-09	2005-12-09	2005-12-09	13824	0	0	13
	<div> <div>Per our conversation, you want to register a domain with the name of www.lauras_stuff.com. You have already chosen IT Connection Servers to host your website.</div> <div>I have been in contact with them to get the necessary information. My fee for the registration process is \$500. Please send a check or money order to the address listed below.</div> <div>George Montgomery</div> <div>3467 Main Street</div> <div>Bellevue, WA 98080</div> <div>If you fail to do so within 30 days of receipt of this letter, the domain ownership will revert to me and I will sell it to the highest bidder.</div> <div>Please call me at (206) 555-1212 or email me at george.montgomery@nowhere.com.</div> <div>Regards,</div> </div>								

- Deliverable: Summarize your findings in your lab report, highlighting any significant documents or images recovered.

Answer

The file system metadata, for forensic analysis. It includes file and directory entries, timestamps (creation, modification, access), and metadata about the file system itself (e.g., FAT1, FAT2, MBR). The timestamps are in both UTC and EST. A timestamp discrepancy was also identified which caused an issue with 'fls' and 'ils'.

Part 4: Analysis and Documentation

1. Analyze Recovered Data:

- Analyze the recovered files and summarize their relevance to the investigation.
- Deliverable: Provide a brief analysis (200-300 words) of the significance of the recovered data in your lab report.

Answer

The data recovered from the correspondence between George Montgomery and Laura Roper offers significant insights into the domain registration process and the dynamics of digital business transactions. Firstly, it highlights Laura Roper's intent to secure the domain name **www.lauras_stuff.com**, indicating a strategic move to establish an online presence.

George's role as the facilitator of this transaction is evident in clear communication regarding the chosen hosting provider, **IT Connection Servers**, and the associated costs. His specified fee

of **\$500** for the registration service, along with the request for payment via check or money order, raises important considerations about security and reliability in financial transactions.

The inclusion of a **30-day deadline** for payment underscores the competitive nature of domain registration, emphasizing the urgency for Laura to act swiftly or risk losing the domain to other buyers. This element of correspondence is crucial for understanding the pressures clients face in the digital marketplace. Additionally, the consequences of inaction clearly delineate legal implications, serving as a warning that insufficient promptness could lead to the domain's reallocation.

Furthermore, the letters demonstrate an ongoing professional relationship, with included contact information facilitating future communications about the domain registration. This consistency and formality in communication practices are indicative of a structured approach to client engagement.

2. Document Your Findings:

- Compile screenshots of the Autopsy interface showing recovered files, the keyword search process, and any relevant findings.
- Deliverable: Include all documentation in a cohesive lab report.

Answer

The screenshot displays the Autopsy interface. On the left, a sidebar shows search results for 'George Montgomery', indicating 3 occurrences were found. Below this, search options like ASCII, Case Insensitive, and Regular Expression are listed. The main pane shows the ASCII contents of Sector 240, dated 13 October 2005. The text is a letter from George Montgomery to Laura Roper, discussing domain registration for 'www.lauras_stuff.com' and requesting a \$500 fee.

New Search

3 occurrences of George Montgomery were found
Search Options:
ASCII
Case Insensitive
Regular Expression

Sector 240 ([Hex](#) - [Ascii](#))
1: 460

Sector 241 ([Hex](#) - [Ascii](#))
2: 292

Sector 316 ([Hex](#) - [Ascii](#))
3: 390

George Montgomery was not found
Search Options:
Unicode
Case Insensitive
Regular Expression

◀ PREVIOUS NEXT ▶
EXPORT CONTENTS ADD NOTE

ASCII (display - [report](#)) * Hex (display - [report](#)) * ASCII Strings (display - [report](#))
File Type: data

Sector: 240

ASCII Contents of Sector 240 in Ch01InChap01.dd-0-0

13 October 2005

Laura Roper
48 Mockingbird Lane
Seattle, WA 98119

Dear Laura,
Per our conversation, you want to register a domain with the name of . HYPERLINK http://www.lauras_stuff.com
..www.lauras_stuff.com.. You have already chosen IT Connection Servers to host your website.

I have been in contact with them to get the necessary information. My fee for the registration process is \$500. Please send a check or money order to the address listed below.

George Montgomery
3467 Main Street
Bellevue, WA 989

Figure 3: Conversation between George Montgomery and Laura Roper

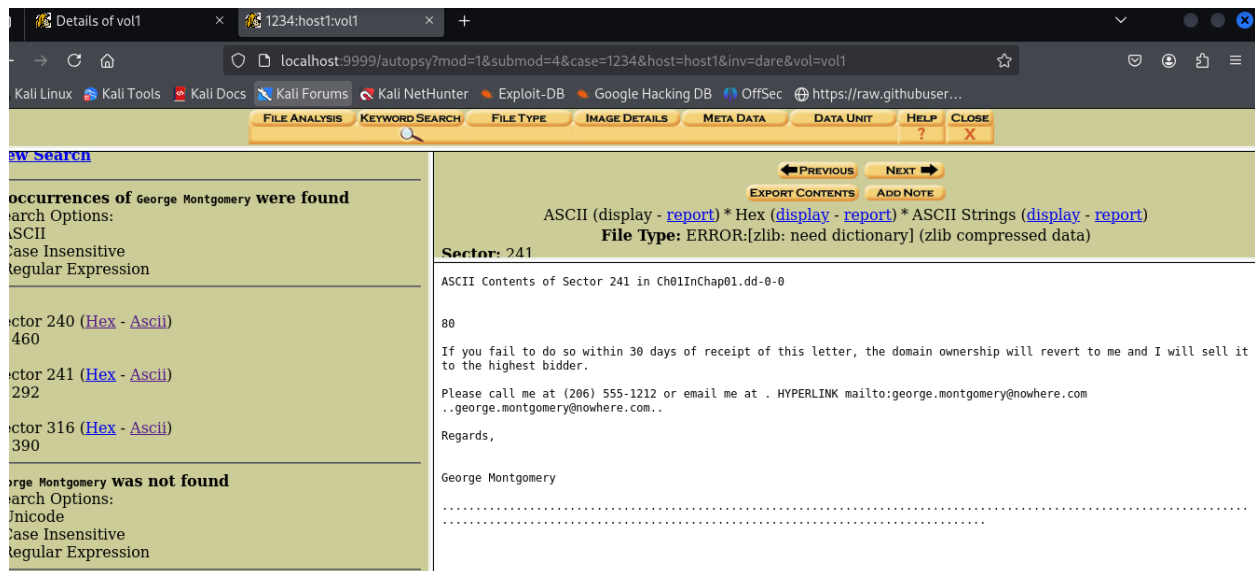


Figure 4: 30-day deadline for payment



Figure 5: Conversation between George Montgomery and Randall Watson

INT313 - Computer and Digital Forensics – Lab 2 Lab Title: Comparative Analysis of Autopsy and The Sleuth Kit (TSK)

The Sleuth Kit (TSK) is a C library and a suite of open-source, command-line tools used for digital forensics. It facilitates the analysis of disk images and the recovery of files from various file systems, including NTFS, FAT, EXT2FS, and FFS. TSK is available for both Unix-based and Windows operating systems, offering utilities for extracting data from storage devices. Its primary function is to enable in-depth examination of digital evidence.

Part 1: Overview of Autopsy and The Sleuth Kit

1. Autopsy vs. The Sleuth Kit:

- Provide a brief overview of the differences between Autopsy and TSK in terms of functionality and user interface.
- Deliverable: Write a comparison (150-200 words) to include in your lab report.

Answer

The Sleuth Kit (TSK)

- **Functionality:** TSK is primarily a set of command-line tools and a C library that provides low-level access to disk images, enabling detailed digital forensic analysis. It supports various file systems (like NTFS, FAT, EXT, and FFS) and is useful for tasks such as file recovery, data extraction, and forensic analysis.
- **User Interface:** TSK lacks a graphical user interface (GUI). Users interact with it through the command line, which requires familiarity with command syntax and typically demands more expertise in digital forensics. This can make TSK less user-friendly for those who prefer visual interfaces.

Autopsy

- **Functionality:** Autopsy is a forensic analysis tool built on top of TSK, providing a more accessible and comprehensive framework for digital investigations. It incorporates TSK's capabilities while adding features such as timeline analysis, keyword searching, and report generation. Autopsy also integrates with various additional modules for extended functionalities like web artifacts analysis and metadata examination.

- **User Interface:** Autopsy offers a user-friendly GUI that makes it easier for users to navigate through various tools and functionalities. The graphical interface allows users to view data, perform searches, and analyze results visually, making it a better option for those who may not be comfortable with command-line operations.

2. TSK Architecture:

- Research and summarize the layers of the TSK architecture.

Answer

1. File System Layer

- **Description:** This layer interacts directly with various file systems (e.g., NTFS, FAT, EXT, HFS+, etc.), enabling data extraction from disk images based on the unique structures and data formats of these file systems.
- **Functionality:** It interprets the specific file system structures to access files and metadata stored on devices, allowing TSK to read and analyze file and directory entries.

2. Image Layer

- **Description:** This layer handles raw disk images, including various formats like E01, Afflib, and raw images (dd).
- **Functionality:** It provides mechanisms to read and parse images, ensuring that the data can be properly examined regardless of the image format. This layer is crucial for manipulating the actual data stored on the physical media.

3. Data Access Layer

- **Description:** This layer acts as an intermediary between the file system layer and higher-level tools or applications, providing a standardized interface for accessing data.
- **Functionality:** It includes APIs and functions that allow higher-level components to request data while abstracting the details of how the data is stored or structured beneath. This promotes modularity and flexibility in the tool's design.

4. Application Layer

- **Description:** This layer includes the command-line tools and utilities that users interact with to perform forensic examinations using TSK.

- **Functionality:** It provides user-facing commands (like fls, blkls, icat, etc.) that invoke lower-level functionality to analyze file systems, recover files, and manage evidence. Users perform operations such as listing file contents, retrieving file metadata, and generating reports.

5. Extensions and Integrations Layer

- **Description:** This layer supports additional modules or third-party applications that can extend TSK's capabilities.
 - **Functionality:** It allows developers to create plugins and tools that can integrate with TSK, enhancing features like data visualization, reporting, and specialized analysis (such as registry analysis or web browser artifact extraction).
- **Deliverable:** Create a diagram or list showing the layers of TSK and the tools provided at each layer.

Answer

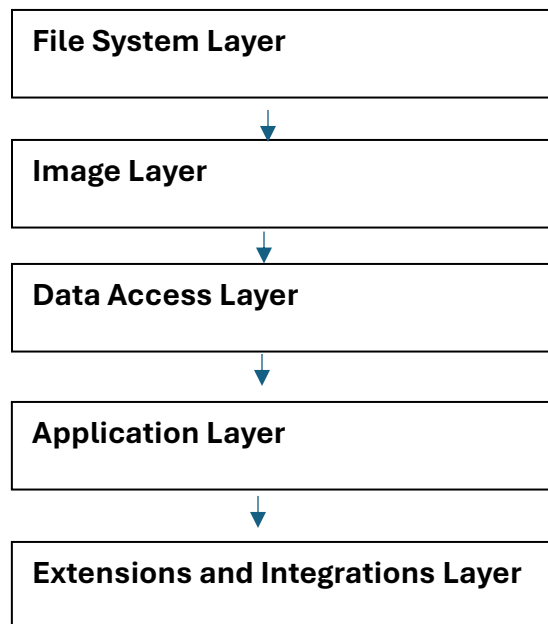


Figure 6: Diagram layers of TSK

Part 2: Examining a USB File Using TSK

1. Setup TSK:

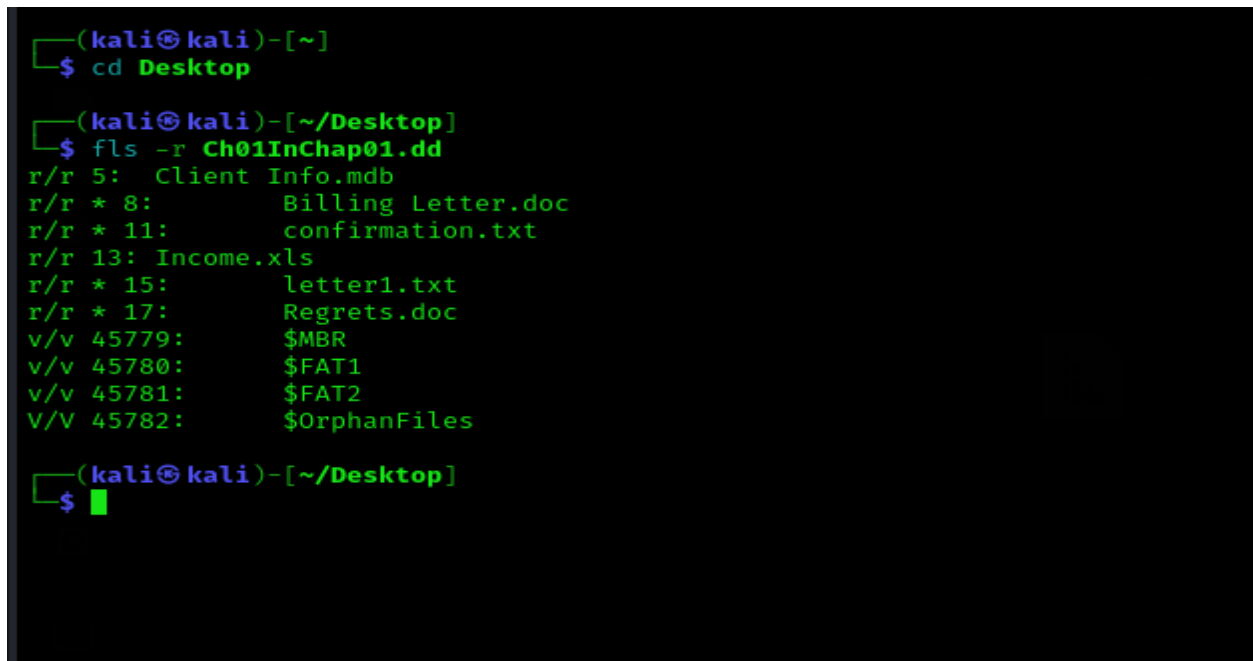
- Download the USB drive image from this link.

2. Using TSK Commands:

- Follow the PowerPoint presentations provided in class to practice all Linux commands related to The Sleuth Kit.

- **Task:** Determine how many deleted files are in the disk image.

Use the command: `fls -r Ch01InChap01.dd`



```
(kali㉿kali)-[~]  
$ cd Desktop  
  
(kali㉿kali)-[~/Desktop]  
$ fls -r Ch01InChap01.dd  
r/r 5: Client Info.mdb  
r/r * 8: Billing Letter.doc  
r/r * 11: confirmation.txt  
r/r 13: Income.xls  
r/r * 15: letter1.txt  
r/r * 17: Regrets.doc  
v/v 45779: $MBR  
v/v 45780: $FAT1  
v/v 45781: $FAT2  
V/V 45782: $OrphanFiles  
  
(kali㉿kali)-[~/Desktop]  
$ █
```

Figure 7: deleted file using fls command

3. Recovering Deleted Files:

- **Task:** Recover the deleted file *letter1.txt* using TSK commands.
- **Command Example:** `icat Ch01InChap01.dd <inode_number> > recovered_letter1.txt`
- **Deliverable:** Document the command used and any relevant outputs. Outputs.

Answer

```

    -k password: Decryption password for encrypted volumes

(kali㉿kali)-[~/Desktop]
$ icat Ch01InChap01.dd 15
Earl,
We need to meet on the 18th of August to confirm the work I am
doing for you. Please contact me ASAP.

George

(kali㉿kali)-[~/Desktop]
$ █
```

Figure 8: The content inside the file index number 15 (letter.txt)

Part 3: Demonstrating Recovery Tools

1. Recovering Deleted Files:

- Demonstrate the recovery of all deleted files using three different tools

introduced in class (e.g., fls, icat, and tsk_recover).

- Deliverable: For each tool, provide:
 - The command used.
 - The inputs required (e.g., URL or custom inputs).
 - The expected outputs.
 - An explanation of how each command works and how its parameters influence the output.

```

(kali㉿kali)-[~/Desktop]
$ tsk_recover Ch01InChap01.dd 15
Files Recovered: 4
```

Figure 9: Total recovery files

2. Selecting Questions:

- Based on your last four student ID or SSN digits, use the modulus operation to determine which questions to answer. For example, if your last four digits are 1234, calculate:
 - $1234 \bmod 28$ to get the index for your questions (2, 3, 4).
- Deliverable: Document the selected questions and your responses in the lab report.

INT313 - Computer and Digital Forensics – Lab 3 Lab Title: Disk Imaging Techniques: Acquisition Methods for USB Drives

Part 1: Understanding Disk Images

1. What is a Disk Image?

- Defining a disk image and its importance in digital forensics.

Answer

Definition of a Disk Image

A **disk image** is a sector-by-sector copy of the data contained on a storage device, such as a hard drive, solid-state drive (SSD), USB flash drive, or optical disc. It preserves not only the files and folders present on the storage medium but also the file system structure, metadata, and any unused data or allocated space. Disk images can be created in various formats, such as **RAW**, **E01** (EnCase), or **AFF** (Advanced Forensic Format), and are often stored in a single file that represents the entire contents of the original device.

Importance of Disk Images in Digital Forensics

1. **Preservation of Evidence:** Disk images provide a copy of the original evidence, allowing investigators to work on a duplicate while keeping the original data intact. This preserves the integrity of the evidence, ensuring it can be examined later if needed.
2. **Analysis of Deleted Data:** Since a disk image captures all sectors of a storage medium, it can contain remnants of deleted files and data that may not be visible in a live environment. This capability is crucial for recovering potentially valuable information in forensic investigations.
3. **Comprehensive Examination:** Disk images enable forensic analysts to perform thorough examinations of file systems, including metadata analysis, timeline creation, and recovery of hidden or encrypted files. This depth of analysis can uncover critical evidence in criminal cases, civil litigation, or cybersecurity incidents.
4. **Cross-Platform Compatibility:** Disk images can be analyzed on different operating systems and using various forensic tools, making it easier to collaborate among forensic teams with different expertise or resource preferences.

5. **Documentation and Reporting:** Disk images provide a documented snapshot of the forensic process, allowing investigators to generate accurate reports detailing their findings, methodologies, and the state of the evidence at the time of imaging. This documentation is vital for presenting findings in court.
 6. **Support for Multiple Investigations:** A single disk image can be examined multiple times by different forensic analysts without the risk of altering the original data. This flexibility allows for various lines of inquiry to be explored simultaneously.
- Deliverable: Write a brief explanation (100-150 words) discussing the purpose and benefits of creating disk images in forensic investigations.

Answer

Creating disk images in forensic investigations serves several critical purposes and offers significant benefits. Firstly, disk images provide a complete, sector-by-sector copy of a storage device, ensuring the preservation of original data and maintaining the integrity of the evidence. This is vital for legal proceedings, as any alterations to the original media could compromise the investigation.

Secondly, disk images allow forensic analysts to recover and examine deleted files, hidden data, and file system metadata, which may contain crucial evidence. Analyzing a disk image can uncover patterns of user behavior and timelines of activity.

Additionally, creating disk images supports the principle of working with duplicates, enabling multiple analysts to investigate the same evidence independently without risking changes to the original data. Overall, disk imaging is an indispensable practice in digital forensics, enhancing the reliability and thoroughness of investigations.

Part 2: Acquisition of USB Drives

Task 1: Acquisition Using FTK Imager (Windows)

1. Setup FTK Imager:

- Download and install FTK Imager from the official website.

2. Create a Disk Image:

- Step 1: Connect your USB flash drive to the Windows machine.
- Step 2: Open FTK Imager and select File > Create Disk Image.
- Step 3: Choose the connected USB drive from the list of available drives.
- Step 4: Select the output format (e.g., E01 or RAW) and specify a destination for the image file.
- Step 5: Click Finish to create the disk image.

3. Deliverable: Capture screenshots of each step in FTK Imager, including the final image file location.

Answer

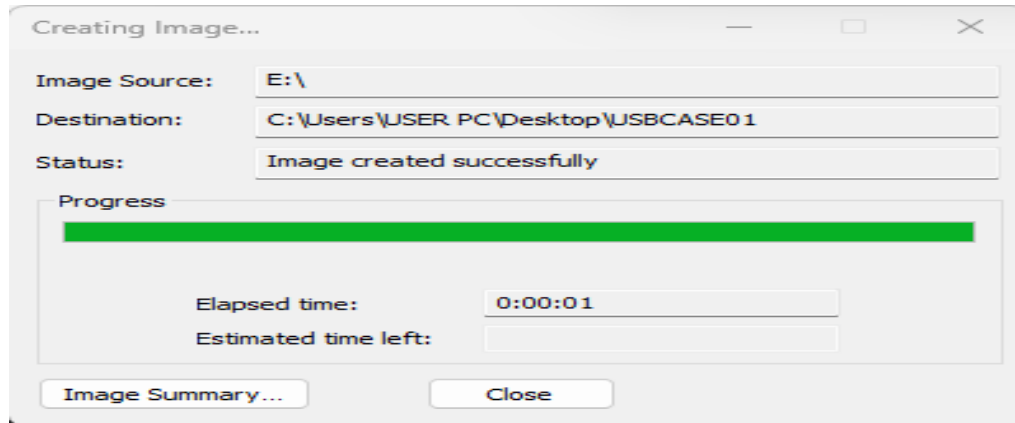


Figure 10: creation of disk image

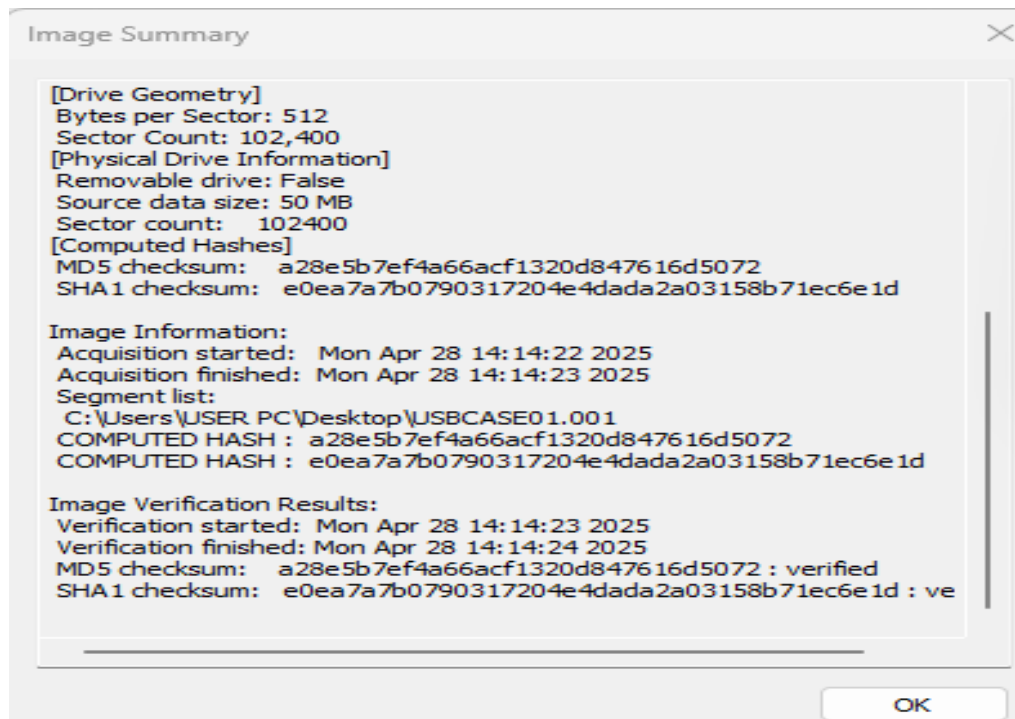


Figure 11: disk image summary

```
Windows PowerShell
-a----      3/3/2024  10:02 AM           2607 Mendeley Reference Manager.lnk
-a----     12/17/2023   7:38 AM          17455 motivation letter for KING abdu
-a----     12/17/2023   7:45 AM          76392 motivation letter for KING abdu
-a----      7/31/2024  11:49 PM       5423104 OpenVPN-2.6.12-I001-amd64.msi
-a----      4/20/2024   7:47 PM          1448 Opera Browser.lnk
-a----      3/28/2024   6:06 PM       1070615 optimal location of UPQC Chapte
-a----      3/28/2024   6:06 PM       1272371 optimal location of UPQC Chapte
-a----      3/27/2024   6:36 PM       1071584 optimal location of UPQC Chapte
-a----      9/5/2023   11:03 AM       393284 Optimal_Allocation_of_UPQC_for_
-a----     11/23/2024   8:02 AM       2497547 Optimal_Location_and_Sizing_of_
-a----      5/15/2024  10:13 AM          15090 Pre-Data Summary.docx
-a----      9/2/2023   10:06 AM       355586 prof.Ajenikoko Assignment.docx
-a----      9/11/2023   9:45 AM          15928 proposal1.docx
-a----     12/17/2023   7:28 AM          39780 Recommendation on Ayilara Busar
-a----     12/17/2023   7:42 AM          192240 Recommendation on Ayilara Busar
-a----     10/15/2023  11:15 PM       204988 resume_eng_advanced_w2017.pdf
-a----     10/15/2023  11:11 PM       159538 resume_eng_tech_entry_level_w20
-a----      4/1/2024   5:30 PM          1038 Telegram.lnk
-a----      6/9/2023   3:06 PM           420 This PC - Shortcut.lnk
-a----      4/28/2025   2:14 PM      52428800 USBCASE01.001
-a----      4/28/2025   2:14 PM          1295 USBCASE01.001.txt
-a----      1/12/2024  10:06 PM          1406 Visual Studio Code.lnk
-a----      1/14/2024   3:18 PM          2408 Work - Edge.lnk

PS C:\Users\USER PC\Desktop> certutil -hashfile USBCASE01.001 md5
MD5 hash of USBCASE01.001:
a28e5b7ef4a66acf1320d847616d5072
CertUtil: -hashfile command completed successfully.
PS C:\Users\USER PC\Desktop>
```

Figure 12: verify the integrity of the file or image

This check for the integrity of the USB image file

Task 2: Acquisition Using dd Command (Linux)

1. Setup Linux Environment:

- Use a Linux distribution (e.g., Ubuntu) and connect your USB flash drive.

2. Create a Disk Image:

- Step 1: Identify the USB drive using the lsblk command.
- Step 2: Use the dd command to create a disk image. Replace /dev/sdX with the correct identifier for your USB drive.

sudo dd if=/dev/sdX of=~/.usb_image.img bs=4M status=progress

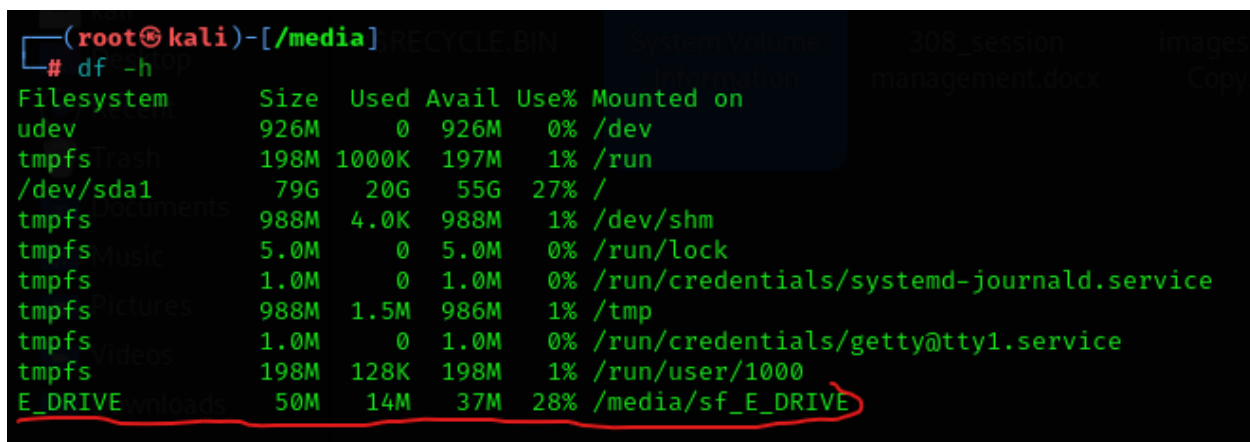
- Step 3: Wait for the process to complete. This may take some time depending on the size of the USB drive.

3. Deliverable: Document the command used and capture a screenshot of the terminal output showing image creation progress.

Answer

superuser permissions to access certain devices and create images were firstly ensuring. Lsblk or df -h was to use to list all the disks on the system, as shown in the figure 13, E_DRIVE with 50MB size was identified. This drive is mounted from host to virtual machine (VM), because of this, disk image cannot be created directly. The first thing to do is to create an archive of the files (mount drive) in that directory rather than a traditional disk image. If you want to create a **tar archive** instead, you can run:

sudo tar -cvf /home/user/E_DRIVE_backup.tar /media/sf_E_DRIVE and To verify that the backup was created successfully use ***tar -tvf /home/user/E_DRIVE_backup.tar*** as show in figure 14



```
(root@kali)-[/media]
# df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            926M   0    926M   0% /dev
tmpfs           198M 1000K  197M   1% /run
/dev/sda1       79G   20G   55G  27% /
tmpfs           988M  4.0K  988M   1% /dev/shm
tmpfs           5.0M   0    5.0M   0% /run/lock
tmpfs           1.0M   0    1.0M   0% /run/credentials/systemd-journald.service
tmpfs/Pictures  988M  1.5M  986M   1% /tmp
tmpfs           1.0M   0    1.0M   0% /run/credentials/getty@tty1.service
tmpfs           198M  128K  198M   1% /run/user/1000
E_DRIVE         50M   14M   37M  28% /media/sf_E_DRIVE
```

Figure 13: identify the drive

```
(root@kali)-[//]
# sudo tar -cvf /E_DRIVE_backup.tar /media/sf_E_DRIVE
tar: Removing leading '/' from member names
/media/sf_E_DRIVE/
/media/sf_E_DRIVE/$RECYCLE.BIN/
/media/sf_E_DRIVE/$RECYCLE.BIN/S-1-5-21-1792927627-2805342604-41705444-1000/
/media/sf_E_DRIVE/$RECYCLE.BIN/S-1-5-21-1792927627-2805342604-41705444-1000/$I8JQ3IW.pdf
/media/sf_E_DRIVE/$RECYCLE.BIN/S-1-5-21-1792927627-2805342604-41705444-1000/$IH4D5FN.docx
/media/sf_E_DRIVE/$RECYCLE.BIN/S-1-5-21-1792927627-2805342604-41705444-1000/$IP6LXIC.jpg
/media/sf_E_DRIVE/$RECYCLE.BIN/S-1-5-21-1792927627-2805342604-41705444-1000/$R8JQ3IW.pdf
/media/sf_E_DRIVE/$RECYCLE.BIN/S-1-5-21-1792927627-2805342604-41705444-1000/$RH4D5FN.docx
/media/sf_E_DRIVE/$RECYCLE.BIN/S-1-5-21-1792927627-2805342604-41705444-1000/$RP6LXIC.jpg
/media/sf_E_DRIVE/$RECYCLE.BIN/S-1-5-21-1792927627-2805342604-41705444-1000/desktop.ini
/media/sf_E_DRIVE/308_session management.docx
/media/sf_E_DRIVE/images kali l - Copy.png
/media/sf_E_DRIVE/images kali linux - Copy.jpeg
/media/sf_E_DRIVE/SECURE USER ACCESS MANAGEMENT IN LINUX.pdf
tar: /media/sf_E_DRIVE/System Volume Information: Cannot open: Operation not permitted
tar: Exiting with failure status due to previous errors

(root@kali)-[//]
# ls
bin  dev  etc  initrd.img  lib  lib64  media  opt  root  sbin  swapfile  team_project  usr  vmlinuz
boot  E_DRIVE_backup.tar  home  initrd.img.old  lib32  lost+found  mnt  proc  run  srv  sys  tmp  var  vmlinuz.old
```

Figure 14: create a *tar* archive

After successful archive back, the `dd` command was used to create the disk image. **`sudo dd if=/E_DRIVE_backup.tar of=~/.usb_image.img bs=4M status=progress`**. And this was verified in the path it save in figure 16

```
(root@kali)-[//]
# sudo dd if=/E_DRIVE_backup.tar of=~/.usb_image.img bs=4M status=progress

0+1 records in
0+1 records out
2160640 bytes (2.2 MB, 2.1 MiB) copied, 0.0366442 s, 59.0 MB/s

(root@kali)-[//]
```

Figure 15: creating disk image using `dd` command

```
(root@kali)-[~]
# ls
usb_image.img

(root@kali)-[~]
#
```

Figure 16: Image saves at `~(root)` directory

Task 3: Acquisition via Network

1. Network Imaging:

- Discuss the concept of acquiring disk images over a network.

Note: In this lab, students will not perform network acquisition but will learn about tools like FTK Imager and dd used in conjunction with network protocols (e.g., FTP, SCP) for remote imaging.

- **Deliverable:** Write a short paragraph (100 words) on the advantages and challenges of acquiring disk images via network methods.

Answer

Concept of Acquiring Disk Images Over a Network

1. Definition:

Acquiring disk images over a network refers to the practice of duplicating the contents of a storage device—such as a hard drive, SSD, or USB drive—over a network connection. This process typically involves copying the entire data, including the file system structure, metadata, and unused space, to a remote storage location.

2. Methods:

There are several methods to acquire disk images over a network:

- **Network File Transfer Protocols:** Common protocols for transferring disk images include:
 - **FTP/SFTP:** File Transfer Protocol and its secure version for transferring image files.
 - **SCP:** Secure Copy Protocol for encrypted transfer of files over SSH.
 - **HTTP/HTTPS:** For transferring files via web servers.
- **Network Imaging Tools:** Specialized tools designed for disk imaging can acquire images and transfer them over the network. Some examples include:
 - **FTK Imager:** Can create disk images and send them to a network location.
 - **dd over SSH:** Securely transfer disk images using the dd command piped through SSH.

dd if=/dev/sdX | ssh user@remote_host "cat > /path/to/remote/image.img"

- **Dedicated Solutions:** There are also dedicated forensic software solutions that automate the process of imaging and transferring disk images over the network, such as **EnCase**, **X1 Social Discovery**, and **Helix3**.

3. Network Environments:

Disk imaging over a network can be done in various environments, including:

- **Local Area Networks (LAN):** High-speed connections suitable for imaging operations.
- **Wide Area Networks (WAN):** Used for remote acquisitions, potentially slower due to bandwidth limitations.
- **Cloud-based Storage:** Acquiring images directly to cloud storage solutions can facilitate long-term storage and accessibility.

Benefits of Acquiring Disk Images Over a Network

1. **Remote Access:** Investigators can acquire disk images from systems that may be physically inaccessible, such as computers in another location or facilities where physical access is restricted.
2. **Minimal Disruption:** Imaging a disk over the network can often be done while the system remains operational, especially if the process is well-coordinated and the data is not being actively altered.
3. **Efficiency:** Centralized data collection can expedite investigations, especially in scenarios involving multiple devices or large amounts of data.
4. **Data Preservation:** Live acquisitions can help in preserving volatile data that may be lost if the system is powered down or rebooted.
5. **Scalability:** Organizations can scale their imaging efforts by leveraging existing network infrastructure, making it easier to handle large volumes of data.

Considerations and Challenges

1. **Network Bandwidth:** The speed and reliability of the network can significantly impact the time it takes to acquire disk images. Limited bandwidth may slow down the process.
2. **Data Integrity:** Ensuring the integrity and authenticity of the disk image during transfer is crucial. Techniques such as checksums (e.g., MD5 or SHA-1) must be employed to validate the image after transfer.

3. **Security Concerns:** Transferring disk images over the network introduces risks such as interception or unauthorized access. Using secure protocols (like SCP or SFTP) is essential.
4. **Legal and Ethical Considerations:** Acquiring disk images, especially over a network, must comply with legal standards and organizational policies regarding data privacy and handling.
5. **Technical Complexity:** The process can be technically complex, requiring specialized knowledge of network operations, disk imaging tools, and forensic procedures.