SCHEME :K

Name :_____
Roll No.:_____ Year : 20 ___ 20 __
Exam Seat No. :_____

LABORATORY MANUAL FOR

DIGITAL FORENSIC AND HACKING TECHNIQUES (316315)

COMPUTER ENGINEERING GROUP

MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION, MUMBAI
(Autonomous)(ISO21001:2018)(ISO/IEC27001:2013)

VISION

To ensure that the Diploma Level Technical Education constantly matches the latest requirements of Technology and industry and includes the all-round personal development of students including social concerns and to become globally competitive, technology led organization.

MISSION

To provide high quality technical and managerial manpower, information and consultancy services to the industry and community to enable the industry and community to face the challenging technological & environmental challenges.

Quality Policy

We, at MSBTE are committed to offer the best-in-class academic services to the students and institutes to enhance the delight of industry and society. This will be achieved through continual improvement in management practices adopted in the process of curriculum design, development, implementation, evaluation and monitoring system along with adequate faculty development programmes.

Core Values

MSBTE believes in the following:

- Skill development in line with industry requirements.
- Industry readiness and improved employability of Diploma holders.
- Synergistic relationship with industry.
- Collective and Cooperative development of all stake holders.
- Technological interventions in societal development.
- Access to uniform quality technical education.

A Laboratory Manual
for

DIGITAL FORENSIC AND HACKING TECHNIQUES (316315)

Semester– VI

"K-SCHEME"

(AI/ BD/ CM/ CO/ CW/ DS/ HA/ IF/ IH/ SE)

Maharashtra State

Board of Technical Education, Mumbai

(Autonomous) (ISO 21001:2018) (ISO/IEC 27001:2013)

MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION

(Autonomous) (ISO 21001:2018) (ISO/IEC27001:2013)

Address: 4th floor, Govt. Polytechnic Building, 49,

Kherwadi, Bandra (E), Mumbai- 400 051

(Printed on: _____)

Maharashtra State
Board of Technical Education

Certificate

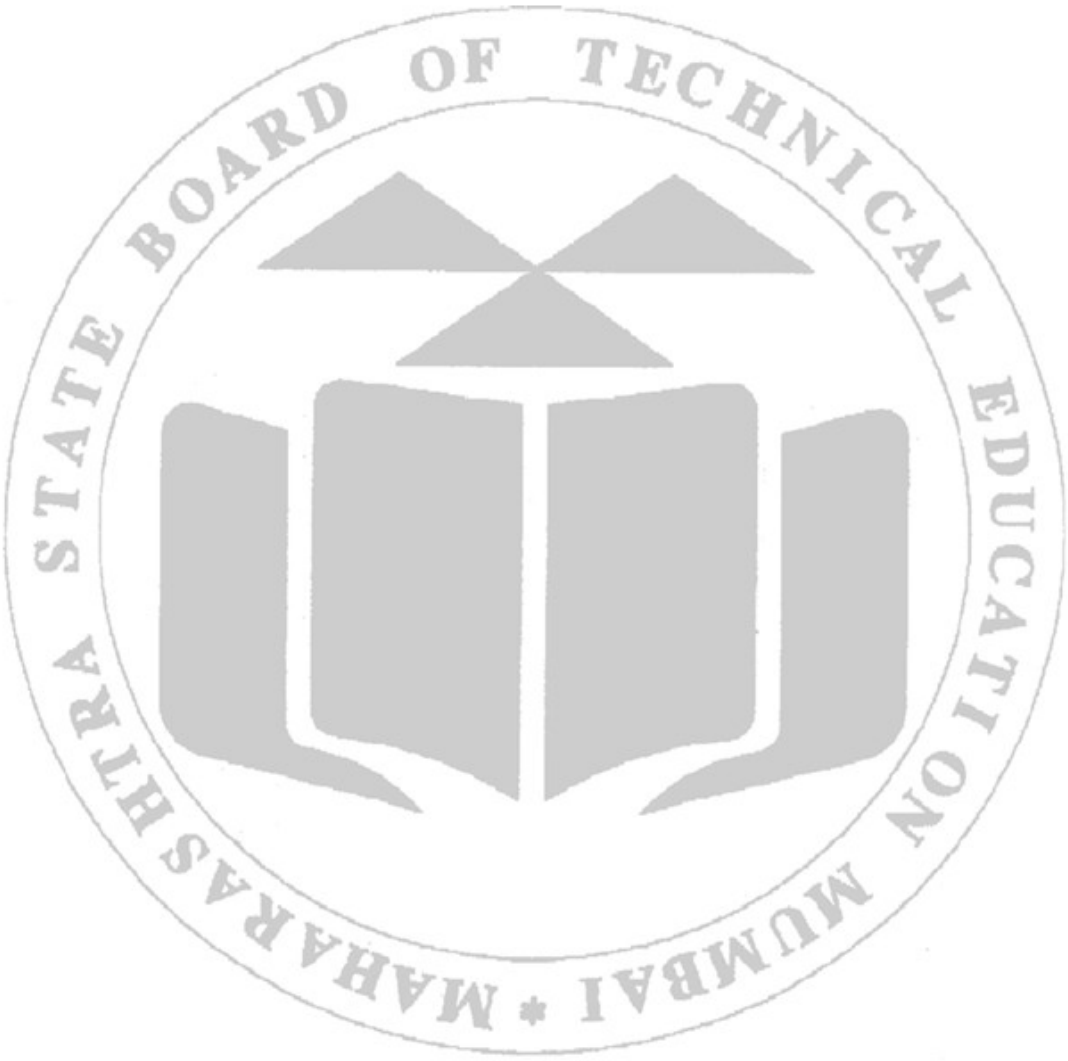
This is to certify that Mr. / Ms. ……………………………………………..……. Roll No……………………… of Sixth Semester of Diploma in ………………………………….….….….……. of the Institute ……………………………………………………………….…………….…… (Inst. Code………………...) has completed the term work satisfactorily in course **Digital Forensic and Hacking Techniques (316315)** for the academic year 20…….to 20…….as prescribed in the curriculum.

Place ………………. Enrollment No……………………

Date…...................... Exam Seat No. …………………......

Course Teacher **Head of the Department** **Principal**

Institute Seal


MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION MUMBAI

Preface

Laboratory practice forms an integral part of technical education, enabling students to convert theoretical knowledge into practical competence. In keeping with the objectives of the K Scheme of MSBTE and the National Education Policy 2020 (NEP 2020), this laboratory manual for Digital Forensic and Hacking Techniques (Course Code: 316315) is designed to promote outcome-based learning and develop essential professional skills among diploma students.

The subject focuses on two major aspects of modern cybersecurity — Digital Forensics and Ethical Hacking. Digital Forensics deals with the collection, preservation, and analysis of digital evidence to investigate cybercrimes, while Ethical Hacking emphasizes identifying and securing vulnerabilities before they can be exploited by malicious users. Together, these disciplines prepare students to safeguard information systems, ensure data integrity, and contribute to the creation of secure digital environments.

This manual has been structured to help students apply forensic methodologies and hacking techniques through well-defined practical exercises. Each practical is aligned with specific Course Outcomes (COs) and Laboratory Learning Outcomes (LLOs) to ensure systematic development of industry-relevant competencies. Students will gain hands-on experience with widely used tools such as FTK Imager, Wireshark, Nmap, HashCalc, and the Social-Engineer Toolkit (SET).

The experiments encourage learners to investigate digital evidence, perform network analysis, simulate penetration testing, and apply ethical principles in all activities. Students are expected to study the theoretical concepts in advance, follow procedures accurately, and maintain detailed observation records. This approach enhances both technical proficiency and professional ethics — vital traits for future cybersecurity professionals.

The development team expresses its gratitude to MSBTE for its continuous efforts toward outcome-based education through the K Scheme. We also acknowledge the valuable inputs from subject experts and reviewers who contributed to the preparation of this manual. While every effort has been made to ensure accuracy and clarity, constructive feedback and suggestions for improvement are most welcome for future editions.

Lab Manual Development Team

Program Outcomes (POs) to be achieved through Practical of this Course

Following POs are expected to be achieved through the practicals of the **Digital Forensic and Hacking Techniques** course.

PO 1. **Basic and Discipline specific knowledge**: Apply knowledge of basic mathematics, science and engineering fundamentals and engineering specialization to solve the engineering problems.

PO 2. **Problem analysis:** Identify and analyze well-defined engineering problems using codified standard methods.

PO 3. **Design/ development of solutions**: Design solutions for well-defined technical problems and assist with the design of systems components or processes to meet specified needs.

PO 4. **Engineering Tools, Experimentation and Testing**: Apply modern engineering tools and appropriate technique to conduct standard tests and measurements.

PO 5. **Engineering practices for society, sustainability and environment**: Apply appropriate technology in context of society, sustainability, environment and ethical practices.

PO 6. **Project Management**: Use engineering management principles individually, as a team member or a leader to manage projects and effectively communicate about well-defined engineering activities in diverse and multidisciplinary fields.

PO 7. **Life-long learning**: Ability to analyze individual needs and engage in updating in the context of technological changes.

List of Industry Relevant Skills:

The following industry relevant skills of the competency 'Digital Forensic And Hacking Techniques' are expected to be developed in you by undertaking the practical of this laboratory manual.

- Operating System Proficiency
- Networking Knowledge
- Digital forensic Tool Mastery
- Data Recovery and Artifact Analysis
- Cryptography

Practical- Course Outcome (CO) matrix

CO1 - Explain digital forensics investigation process.
CO2 - Apply various Digital Forensic Investigation Models.
CO3 - Apply digital Evidence collecting and handling techniques.
CO4 - Identify various types of cyber-attacks.
CO5 - Apply Tools and Techniques for Ethical Hacking.

Sr. No.	Title of the Practical	CO 1	CO 2	CO 3	CO 4	CO 5
1	* a. Monitor CPU Utilization and Memory Utilization for detecting unauthorized process activations. (Hint: More CPU utilization as compared to Memory is an indicator of anomaly) b. Create complete memory dump using windows c. Read Memory Dump Using Windows Driver toolkit	√	-	-	-	-
2	*Study the DFRWS Investigative Model and apply it in a simulated digital forensic investigation. Investigate according to phases of model. Prepare report detailing the steps taken during the investigation.		√	-	-	-
3	Analyze a real-world or hypothetical case where ethical issues arose in a digital forensics investigation Task to be performed by students: a. Select a real-world case of a digital forensics investigation where ethical issues played a significant role (e.g., the case of the FBI's investigation of the San Bernardino iPhone, The Ashley Madison Hack (2015)) b. Analyze the case based on following points: • Ethical issues involved in the investigation • Situation handling procedure followed by Investigator • Does the investigation based on professional ethical norms • Or what Ethical guidelines should be followed c. Prepare Report on ethical issues, their impact on the investigation and a conclusion on how the situation could have been managed ethically	-	√	-	-	-
4	*Investigate data in a cloud environment, focusing on issues like data privacy and security breaches a. Conduct a forensic analysis of cloud storage	-	√	-	-	-

	(e.g., Dropbox, Google Drive) for potential data breaches or misuse b. Retrieve access logs and analyze activities that suggest unauthorized access or tampering (Hint: Use Cloud storage APIs, AWS CloudTrail, Google Cloud Platform logs.)					
5	Collect live data on windows/Linux: a. Create a response toolkit on windows having utility cmd.exe, PsLoggedOn, netstat b. Establish TCP connection between forensic workstation and the target system using netcat c. Run trusted cmd.exe, identify logged users and remote access users, Record creation, access times and all the modifications made to the files.	-	-	√	-	-
6	Create Forensic Images with any Imager Tool like Exterro FTK Imager	-	-	√	-	-
7	*Perform Hashing to verify the authenticity of digital evidence a. Create a file and generate a hash (MD5, SHA-256) using hashing tools b. Alter the file slightly and generate the hash again to observe how the hash changes (Use HashCalc, MD5 & SHA Checksum Utility, Python's hashlib or any such tool)	-	-	√	-	-
8	Recover deleted or corrupted files from a storage device and perform file carving (e.g., photos, documents) using any data recovery tool	-	-	√	-	-
9	*Read and Interpret Operating Systems logs on Windows file system	-	-	-	√	-
10	Install Kali Linux	-	-	-	√	-
11	*Use nmap utility to perform following tasks: a. Install Nmap on Linux or Windows OS b. Detect which devices are live on your local network. Identify the services and their versions running on a particular host c. Detect the operating system of a target host d. Perform a port scan on a specific set of ports e. Perform an aggressive scan to gather as much information as possible about a target host f. Use Nmap's scripting engine to search for vulnerabilities in a target system	-	-	-	√	-

12	Establish DoS attack using TCP/ICMP flooding: a. Ping continuously a particular machine at a time from different machines and observe the machine behavior on Network Write shell script for continuously flooding a Machine with ping and observe the machine behavior on Network	-	-	-	√	-
13	* Capture Network traffic using Wireshark tool a. Install Wireshark tool on Windows/Kali Linux b. Use Wireshark tool to capture network traffic and to understand three-way handshaking concept/Analyze the packet c. Examine HTTP, FTP, or other protocols for evidence of cybercrime	-	-	-	-	√
14	Collect information of IP addresses, domain names and emails using any information gathering tool like Recon-ng	-	-	-	-	√
15	*Use Social-Engineer Toolkit (SET) tool for Simulating phishing attacks to test human vulnerabilities	-	-	-	-	√

Guidelines to Teachers

1. For incidental writing on the day of each practical session every student should maintain a dated logbook for the whole semester, apart from this laboratory manual, which s/he has to submit for assessment to the teacher in the next practical session.
2. Teachers should give opportunity to students for hands-on after the demonstration.
3. Assess the skill achievement of the students and COs of each unit.
4. Explain prior concepts to the students before starting of each experiment.
5. List of few sample questions for reference are given. Teachers must design more such questions so as to ensure the achievement of identified CO.
6. Teacher should ensure that the practical skill and competencies are developed in the students after the completion of the practical exercise.
7. Teacher may provide additional knowledge and skills to the students even though it's not covered in the manual but are expected from the students by the industries.
8. Teacher may suggest the students to refer additional related literature of the Technical papers/ Reference books/ Seminar proceedings, etc.
9. Teacher shall assess the performance of students continuously as per norms prescribed by MSBTE.
10. During assessment teacher is expected to ask questions to the students to tap their Achievements grading related knowledge and skills. So that, student can prepare while submitting record of the practical focus should be given on development of enlisted skills rather than theoretical knowledge.

Instructions for Students

1. Understand the purpose of practical and its implementation.
2. Student shall develop practical skills as expected by the industries.
3. Listen carefully to the instructions given by the teacher about importance of relevant program Outcomes, relevant course outcomes, practical significance, competency and practical skills, practical outcome and the theoretical background during the practical session.
4. Write the answers of the questions allotted by the teacher during practical session.
5. Student should develop the habit of group discussion related to the practical, so that exchange of knowledge/skills could take place.
6. Student shall attempt to develop related hands-on-skills to gain confidence.
7. Student shall refer technical magazines, websites related to the scope of the course.
8. Student should develop habit to submit the practical, exercise continuously and progressively on the scheduled dates and should get the assessment done.
9. Student should be well prepared while submitting the write up of the exercise.
10. Student should not hesitate to ask any difficulty faced during conduct of practical.

Content Page

List of Practical and Formative Assessment Sheet

Sr. No.	Laboratory Practical Titles	Page No.	Date of performance	Date of submission	FA PR marks (25)	Dated sign. of teacher	Remarks (if any)
1	a. * Monitor CPU Utilization and Memory Utilization for detecting unauthorized process activations. b. Create complete memory dump using windows c. Read Memory Dump Using Windows Driver toolkit	1					
2	*Study the DFRWS Investigative Model and apply it in a simulated digital forensic investigation. a. Investigate according to phases of model. b. Prepare report detailing the steps taken during the investigation.	8					
3	Analyze a real-world or hypothetical case where ethical issues arose in a digital forensics' investigation Task to be performed by students: a. Select a real-world case of a digital forensics investigation where ethical issues played a significant role (e.g., the case of the FBI's investigation of the San Bernardino iPhone, The Ashley Madison Hack (2015)) b. Analyze the case based on following points: • Ethical issues involved in the investigation • Situation handling procedure followed by Investigator • Does the investigation base on professional ethical norms • Or what Ethical guidelines should be followed	15					

Sr. No.	Laboratory Practical Titles	Page No.	Date of performance	Date of submission	FA PR marks (25)	Dated sign. of teacher	Remarks (if any)
	Prepare Report on ethical issues, their impact on the investigation and a conclusion on how the situation could have been managed ethically						
4	*Investigate data in a cloud environment, focusing on issues like data privacy and security breaches A. Conduct a forensic analysis of cloud storage (e.g., Dropbox, Google Drive) for potential data breaches or misuse. B. Retrieve access logs and analyze activities that suggest unauthorized access or tampering (Hint: Use Cloud storage APIs, AWS CloudTrail, Google Cloud Platform logs.)	21					
5	Collect live data on Windows/Linux: a. Create a response toolkit on windows having utility cmd.exe, PsLoggedOn, netstat b. Establish TCP connection between forensic workstation and the target system using netcat c. Run trusted cmd.exe, identify logged users and remote access users, Record creation, access times and all the modifications made to the files.	31					
6	Create Forensic Images with any Imager Tool like Exterro FTK Imager	37					
7	*Perform Hashing to verify the authenticity of digital evidence a. Create a file and generate a hash (MD5, SHA-256) using hashing tools b. Alter the file slightly and generate the hash again to observe how the hash changes (Use HashCalc, MD5 & SHA Checksum Utility, Python's hashlib or any such tool)	44					

Sr. No.	Laboratory Practical Titles	Page No.	Date of performance	Date of submission	FA PR marks (25)	Dated sign. of teacher	Remarks (if any)
8	Recover deleted or corrupted files from a storage device and perform file carving (e.g., photos, documents) using any data recovery tool	49					
9	*Read and Interpret Operating Systems logs on Windows file system	55					
10	Install Kali Linux	62					
11	*Use nmap utility to perform following tasks: a. Install Nmap on Linux or Windows OS b. Detect which devices are live on your local network. Identify the services and their versions running on a particular host c. Detect the operating system of a target host d. Perform a port scan on a specific set of ports e. Perform an aggressive scan to gather as much information as possible about a target host Use Nmap's scripting engine to search for vulnerabilities in a target system	70					
12	Establish DoS attack using TCP/ICMP flooding: a. Ping continuously a particular machine at a time from different machines and observe the machine behavior on Network Write shell script for continuously flooding a Machine with ping and observe the machine behavior on Network	79					
13	* Capture Network traffic using Wireshark tool a. Install Wireshark tool on Windows/Kali Linux b. Use Wireshark tool to capture network traffic and to understand three-way handshaking	85					

Sr. No.	Laboratory Practical Titles	Page No.	Date of performance	Date of submission	FA PR marks (25)	Dated sign. of teacher	Remarks (if any)
	concept/Analyze the packet c. Examine HTTP, FTP, or other protocols for evidence of cybercrime						
14	Collect information of IP addresses, domain names and emails using any information gathering tool like Recon-ng	96					
15	*Use Social-Engineer Toolkit (SET) tool for Simulating phishing attacks to test human vulnerabilities	100					
Total							

Note: To be transferred to Proforma of CIAAN-2023.

Note: Out of above suggestive LLOs -

- '*' Marked Practical's (LLOs) Are mandatory.
- Minimum 80% of above list of lab experiment are to be performed.
- Judicial mix of LLOs is to be performed to achieve desired outcomes.

Practical No. 1: a. Monitor CPU Utilization and Memory Utilization for detecting unauthorized process activations.
(Hint: More CPU utilization as compared to Memory is an indicator of anomaly)
b. Create complete memory dump using windows
c. Read Memory Dump Using Windows Driver toolkit

I. Practical Significance

Monitoring network traffic using browser developer tools is essential for analyzing how a website loads and communicates with servers. It helps identify slow-loading resources, failed requests, and inefficient API calls, allowing developers to improve performance and fix bugs quickly. This tools also aids in verifying data exchanges, testing backend connections, and ensuring secure transmission of information. Additionally, it supports optimization efforts by revealing caching behavior and bandwidth usage.

II. Industry / Employer Expected outcome(s)

Monitoring CPU and memory utilization is expected to yield proactive threat detection, reduced incident response time, and improved system reliability

III. Course Level Learning outcome(s)

CO1: Explain digital forensics investigation process.

IV. Laboratory Learning outcome(s)

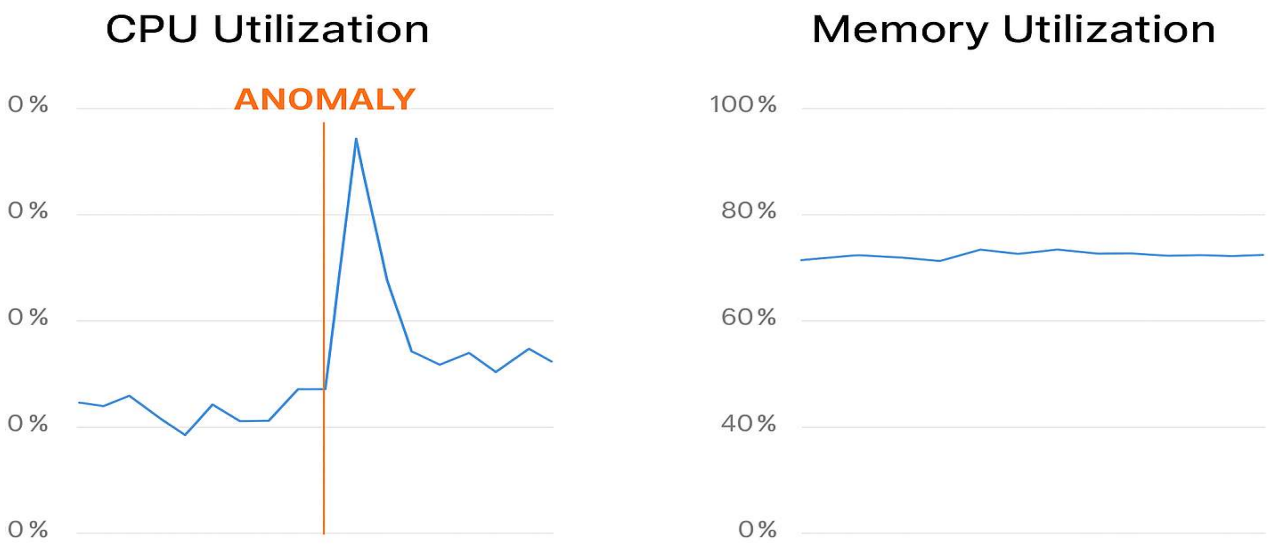
LLO1.1: Monitor CPU and Memory Utilization.

V. Relevant Affective Domain related Outcome(s)

Values accuracy and thoroughness in monitoring system resources to identify abnormalities.

VI. Relevant Theoretical Background

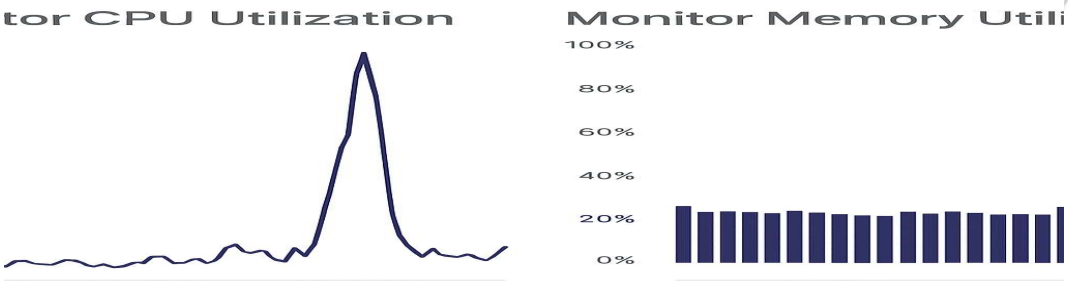
This approach assumes that normal system behavior follows predictable patterns in resource usage, and deviations from these patterns—especially disproportionate CPU spikes with low memory consumption, can signal anomalies such as malware, crypto miners, or unauthorized scripts. Techniques from statistical analysis (e.g., threshold-based alerts, time-series modeling) and machine learning (e.g., Kalman filters, DBSCAN clustering) are commonly applied to identify these anomalies in real-time. These methods are grounded in the principles of behavioral modeling, pattern recognition, and system reliability engineering, enabling proactive threat detection and forensic investigation



Stepwise Procedure

Step 1: Establish a Baseline

- Monitor normal CPU and memory usage over time.
- Identify typical resource consumption patterns for authorized processes.
- Tools: top, htop, Windows Task Manager, Performance Monitor.



Step 2: Define Thresholds and Alerts

- Set thresholds for CPU (%) and memory (MB/GB) usage.
- Example: Alert if CPU > 80% or memory > 70% for more than 5 minutes.
- Use OS tools or third-party monitoring software to configure alerts.

Step 3: Whitelist Approved Processes

- Create a list of known, authorized processes.
- Include process name, expected resource usage, and launch schedule.
- Store in a secure config file or database.

Step 4: Real-Time Monitoring

- Continuously monitor active processes and their resource usage.
- Compare against the whitelist and thresholds.
- Tools:
    - **Linux**: ps, top, vmstat, pidstat, glances
    - **Windows**: PowerShell (Get-Process), Task Manager, WMI scripts

b. Create complete memory dump using windows

Step 1: Set Page File Size

- Ensure the system drive (usually C:) has a page file large enough to store the memory dump.
- Recommended: Page file size = RAM size + 1 MB.

Step 2: Enable Complete Memory Dump

1. Press Windows + R, type sysdm.cpl, and press Enter.
2. Go to the **Advanced** tab → Click **Settings** under *Startup and Recovery*.
3. Under *Write debugging information*, select **Complete memory dump**.
4. Confirm the dump file location (default: %SystemRoot%\MEMORY.DMP).
5. Click OK and restart if prompted.

Step 3: Manually Trigger a Dump (Optional)

- You can manually generate a dump using keyboard shortcuts:
    - Enable the registry setting:
        - Run regedit → Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kbdhid\Parameters
        - Add a new DWORD: CrashOnCtrlScroll = 1
    - Reboot the system.
    - Press Ctrl + Scroll Lock twice to trigger a crash and generate the dump.

Step 4: Verify Dump Creation

- After a crash or manual trigger, check %SystemRoot%\MEMORY.DMP.
- Use tools like **WinDbg** or **WhoCrashed** to analyze the dump.

c. Read Memory Dump Using Windows Driver toolkit

Step 1: Install Windows Driver Kit (WDK)

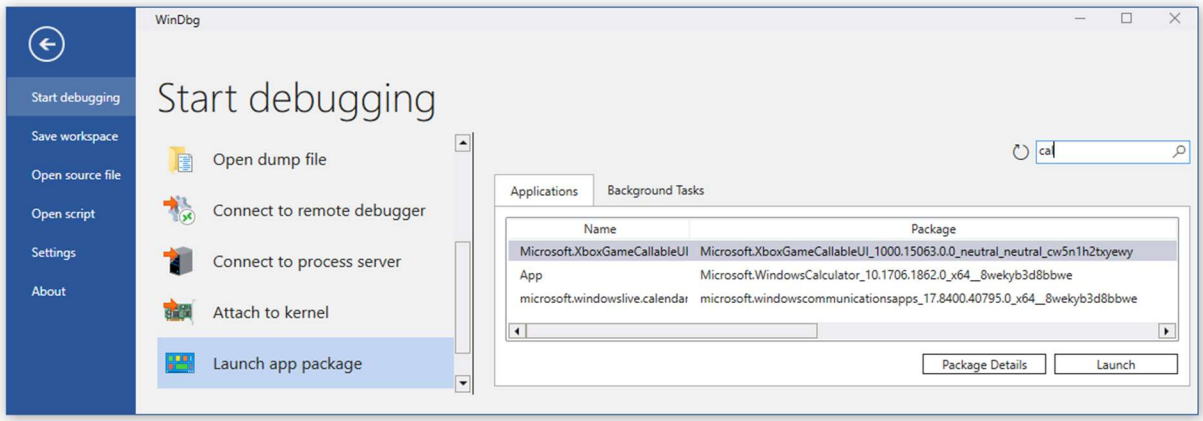
- Download and install WDK from the Microsoft official site.(https://learn.microsoft.com/en-us/windows-hardware/drivers/download-the-wdk)
- Ensure **WinDbg** (Windows Debugger) is included in the installation.

Step 2: Locate the Memory Dump File

- Common paths:
    - Full dump: C:\Windows\MEMORY.DMP
    - Mini dump: C:\Windows\Minidump*.dmp

Step 3: Launch WinDbg

- Open **WinDbg (x64)** or **WinDbg Preview**.



- Run as Administrator for full access.

Step 4: Load the Dump File

- In WinDbg:
  - Go to **File → Open Crash Dump**
  - Select the .dmp file
  -
- Wait for symbols to load (can take time if not cached).

Step 5: Set Symbol Path

- Use Microsoft's symbol server:
  Code
  .sympath srv*C:\Symbols*https://msdl.microsoft.com/download/symbols
- Reload symbols:
  Code
  .reload

Step 6: Analyze the Dump

- Run initial analysis:
  Code
  !analyze -v
- Review output for:
  - Faulting module or driver
  - Bug check code (e.g., 0x0000007E)
  - Stack trace and process info

Step 7: Use Additional Commands

- View loaded drivers: lm
- Inspect process list: !process 0 0
- Examine threads: ~*
- Check memory usage: !vm

Step 8: Export or Save Analysis

- Copy output to a text file for documentation or further review.

VII. Resources required

Sr. No.	Name of Resource	Specification	Quantity	Remarks (If any)
1.	Computer System	Computer (i3-i5 preferable RAM>2 GB	As Per Batch Size	
2.	Storage Type	Disk Space >20 GB		
3.	Internet Connectivity	Minimum 10 Mbps stable connection for download		

VIII. Conclusion

……

……

……

IX. Practical Related Questions

Note: Below are a few sample questions for reference. Teachers must design more such questions to ensure the achievement of the identified CO.

1. Which tool is commonly used in Windows to analyze a complete memory dump?
2. What is the default location for a complete memory dump file in Windows?
3. What is a valid reason to monitor CPU and memory utilization?
4. Which registry key enables manual crash dump generation using Ctrl + Scroll Lock?
5. Which command in WinDbg initiates a detailed analysis of a memory dump?

(Space for answers)

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

X. References/Suggestions for further Reading Assessment Scheme

1. https://www.winfrgui.com
2. https://www.winfr.org/docs.html

XI. Assessment Scheme

The given performance indicators should serve as a guideline for assessment regarding process and product related marks. Faculty must fill only the table at bottom.

Performance Indicators		Weightage
Process related (15 Marks)		**60%**
1	Logic formation	30%
2	Debugging ability	20%
3	Follow ethical practices	10%
Product related (10 Marks)		**40%**
4	Expected output	10%
5	Timely Submission	15%
6	Answer to sample questions	15%
	Total: 25 Marks	**100%**

Marks obtained			**Dated Sign of Teacher**
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No. 2: Study the DFRWS Investigative Model and apply it in a simulated digital forensic investigation (Consider digital forensic scenario like a case involving a potential data breach or unauthorized access to a computer system).

a. Investigate according to phases of the model.

b. Prepare a report detailing the steps taken during the investigation.

I. Practical Significance

The DFRWS Investigative Model plays a vital role in guiding digital forensic investigations with a structured and legally sound approach. In a simulated case involving a suspected data breach of a company's HR database, the model's phases help ensure thorough and defensible handling of digital evidence. The process begins with identification, where unusual access logs reveal a potential breach. Preservation follows, securing the affected server and creating forensic images to prevent data tampering.

II. Industry / Employer Expected outcome(s)

The industry expects digital forensic investigations to deliver legally sound, technically accurate insights that enable swift remediation, compliance, and future risk mitigation.

III. Course Level Learning outcome(s)

CO 2: Apply various Digital Forensic Investigation Models.

IV. Laboratory Learning outcome(s)

LLO2.1: Investigate the given Digital Forensic scenario and prepare report.

V. Relevant Affective Domain related Outcome(s)

Develops a strong commitment to following systematic, established forensic investigation models (like DFRWS).

VI. Relevant Theoretical Background

The DFRWS (Digital Forensic Research Workshop) Investigative Model was developed to provide a structured and systematic approach to digital forensic investigations. Rooted in principles similar to physical crime scene analysis, the model treats each digital device as a potential crime scene and emphasizes the importance of preserving evidence integrity. It consists of six core phases: identification, preservation, collection, examination, analysis, and presentation. These phases guide investigators from recognizing an incident to presenting findings in a legally admissible format. The

model supports both proactive and reactive investigations and is designed to adapt to evolving technologies and cyber threats.

Stepwise Procedure

Identification

- **Goal**: Recognize and define the incident.
- **Actions**:
  - Monitor IDS alerts and firewall logs.
  - Confirm unusual login attempts and data exfiltration patterns.
  - Interview IT staff to gather initial observations.

Preservation

- **Goal: Protect and preserve digital evidence.**
- **Actions:**
- Disconnect affected systems from the network.
  - Create forensic disk images using tools like FTK Imager or dd.
  - Secure logs from servers, routers, and firewalls.
  - Document chain of custody for all evidence.

Collection

- **Goal: Gather relevant data for examination.**
- **Actions:**
  - Collect system logs, access logs, and network traffic captures.
  - Retrieve user account details and file access records.
  - Acquire email logs and USB device connection history.

Examination

- **Goal: Filter and extract relevant information.**
- **Actions:**

  - Use forensic tools (Autopsy, EnCase) to scan for anomalies.
  - Identify unauthorized access times and IP addresses.
  - Detect malware or suspicious scripts.

Analysis

- **Goal: Interpret evidence to reconstruct events.**
- **Actions:**
  - Correlate login attempts with external IPs.
  - Analyze file access patterns and confirm data exfiltration.
  - Identify the attacker's methods (e.g., phishing, privilege escalation).

Presentation

- **Goal: Report findings clearly and accurately.**
- **Actions:**
  - Prepare a detailed forensic report (see below).
  - Include timelines, evidence summaries, and conclusions.
  - Present findings to stakeholders and legal teams.

Decision

- **Goal: Support legal or administrative action.**
- **Actions:**
  - Recommend security improvements.
  - Assist in prosecution or internal disciplinary measures.
  - Help implement incident response and recovery plans.

b. Sample Forensic Investigation Report

Title: Digital Forensic Investigation Report – Suspected Data Breach

Date: 14 October 2025

Investigator: ABC

Institution: XYZ

Executive Summary

A suspected data breach was reported involving unauthorized access to the internal server. This investigation followed the DFRWS model to identify, preserve, examine, and analyze digital evidence.

2. Incident Description

- Date of detection: 10 October 2025
- Affected system: Internal customer database server
- Symptoms: Unusual outbound traffic, failed login attempts, and modified access logs

3. Investigation Steps

Phase	Actions Taken
Identification	IDS alerts reviewed; initial scope defined
Preservation	Systems isolated, forensic images created
Collection	Logs, user data, and network captures gathered
Examination	Malware detected; unauthorized access traced
Analysis	Data exfiltration confirmed, attacker IP identified
Presentation	Report compiled; evidence documented
Decision	Security patches recommended, legal notified

4. Key Findings

- Unauthorized access occurred via compromised credentials.
- Data exfiltration involved customer records.
- Attacker used a remote access trojan (RAT) to maintain persistence.

5. Recommendations

- Reset all user credentials.
- Implement multi-factor authentication.
- Conduct staff training on phishing awareness.
- Update firewall and IDS rules.

VII. Resources required

Sr. No.	Name of Resource	Specification	Quantity	Remarks (If any)
1.	Computer System	Computer (i3-i5 preferable RAM>2 GB	As Per Batch Size	
2.	Storage Type	Disk Space >20 GB		
3.	Internet Connectivity	Minimum 10 Mbps stable connection for download		

VIII. Conclusion

……

……

……

IX. Practical Related Questions

Note: Below are a few sample questions for reference. Teachers must design more such questions to ensure the achievement of the identified CO.

1. What steps are involved in the Identification phase of a digital forensic investigation?
2. How do you preserve digital evidence to maintain its integrity during an investigation?
3. What types of data are typically collected during the Collection phase?
4. Which tools and techniques are used during the Examination phase to detect anomalies?
5. What key elements should be included in a forensic report during the Presentation phase?

(Space for answers)

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

X. References/Suggestions for further Reading Assessment Scheme

1. https:// hawkeyeforensic.com/digital-forensics-investigation-process/
2. https:// www.investigatesc.com/digital-forensic-investigation/

XI. Assessment Scheme

The given performance indicators should serve as a guideline for assessment regarding process and product related marks. Faculty must fill only the table at bottom.

Performance Indicators		Weightage
Process related (15 Marks)		**60%**
1	Logic formation	30%
2	Debugging ability	20%
3	Follow ethical practices	10%
Product related (10 Marks)		**40%**
4	Expected output	10%
5	Timely Submission	15%
6	Answer to sample questions	15%
	Total: 25 Marks	**100%**

Marks obtained			Dated Sign of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No. 3: Analyze a real-world or hypothetical case where ethical issues arose in a digital forensics investigation Task to be performed by students:

a. **Select a real-world case of a digital forensics investigation where ethical issues played a significant role (e.g., the case of the FBI's investigation of the San Bernardino iPhone, The Ashley Madison Hack (2015))**
b. **Analyze the case based on following points: Ethical issues involved in the investigation Situation handling procedure followed by Investigator Does the investigation based on professional ethical norms Or what Ethical guidelines should be followed**
c. **Prepare Report on ethical issues, their impact on the investigation and a conclusion on how the situation could have been managed ethically investigation.**

I. Practical Significance

Analyzing the ethical issues in the FBI–Apple San Bernardino iPhone case offers students practical insight into the real-world complexities of digital forensics, where legal authority, privacy rights, and technological integrity often collide. This case highlights the tension between national security and individual privacy, challenging students to evaluate how forensic investigators should ethically handle encrypted data without compromising broader public trust or setting dangerous precedents. By exploring professional codes of conduct and legal frameworks, students gain a deeper understanding of responsible decision-making in digital investigations, preparing them to navigate similar dilemmas in future roles across cybersecurity, law enforcement, and tech policy.

II. Industry / Employer Expected outcome(s)

The industry-expected outcome of this practical is to equip students with the ability to ethically navigate complex digital forensic investigations, especially those involving privacy, legal compliance, and public accountability.

III. Course Level Learning outcome(s)

CO 2: Apply various Digital Forensic Investigation Models.

IV. Laboratory Learning outcome(s)

LLO 3.1: Analyze the given real-world case and prepare the report based on the ethical issues arose.

V. Relevant Affective Domain related Outcome(s)

Accepts responsibility for maintaining high ethical standards and professional integrity when analyzing complex case studies.

VI. Relevant Theoretical Background

This practical draws from key theories in ethics, law, and digital forensics. Deontological ethics (duty-based) emphasizes the investigator's obligation to follow professional codes regardless of outcomes, while consequentialism (outcome-based) weighs the benefits of accessing data against potential harm to privacy. Information ethics explores how data should be handled responsibly in digital environments, and privacy theory highlights the individual's right to control personal information

Stepwise Procedure

Case Study Report: Ethical Issues in the FBI–Apple San Bernardino iPhone Investigation

Case Overview

In December 2015, a terrorist attack in San Bernardino, California, left 14 people dead. The FBI recovered an iPhone 5C belonging to one of the shooters and sought access to its encrypted data, believing it could contain critical information about the attack and potential accomplices. Apple refused to create a backdoor to bypass the phone's security features, citing privacy and security concerns.

Ethical Issues Involved

- Privacy vs. National Security The core ethical dilemma was balancing individual privacy rights against the collective need for national security. Unlocking the phone could set a precedent for future government access to private data.
- Creation of a Backdoor the FBI requested Apple to develop software that would bypass the iPhone's security. Apple argued this would compromise the integrity of all iPhones, potentially exposing millions of users to cyber threats.
- Corporate Responsibility vs. Legal Obligation Apple faced pressure to comply with a court order under the All-Writs Act. The ethical question was whether a company should be compelled to weaken its own security systems for law enforcement purposes.
- Transparency and Public Trust The case raised concerns about government overreach and the lack of transparency in surveillance practices. Public trust in both government and tech companies was at stake.

Situation Handling Procedure

- The FBI initially sought Apple's assistance informally, then through legal channels.
- Apple provided data it had access to and offered technical guidance but refused to create a tool to bypass the phone's encryption.
- The Justice Department obtained a court order, which Apple challenged publicly and legally.
- Eventually, the FBI accessed the phone's data through a third-party vendor, ending the legal standoff

Ethical Guidelines and Professional Norms

- **ACM Code of Ethics**: Emphasizes protecting privacy, avoiding harm, and respecting the public good.
- **ISFCE Code of Ethics:** Digital forensic professionals must maintain integrity, objectivity, and confidentiality.
- Suggested Guidelines:
  - Use the least intrusive methods to obtain evidence.
  - Avoid creating tools that could be misused or repurposed.
  - Ensure transparency in legal and technical processes.
  - Engage in public discourse to balance ethical concerns.

Impact of Ethical Issues on the Investigation

- **Delay in Accessing Data**: The ethical standoff delayed the FBI's ability to retrieve potential evidence.
- **Public Debate:** Sparked global discussions on encryption, privacy, and government surveillance.
- **Policy Implications**: Influenced future legislation and corporate policies on data access and encryption.

Conclusion: Ethical Management of the Situation

The situation could have been managed more ethically by:

- Establishing clearer legal frameworks for digital evidence access.
- Creating independent oversight bodies to evaluate such requests.
- Encouraging collaboration between tech companies and law enforcement with strict safeguards.
- Promoting public awareness and dialogue on digital rights and responsibilities.

VII. Resources required

Sr. No.	Name of Resource	Specification	Quantity	Remarks (If any)
1.	Computer System	Computer (i3-i5 preferable RAM>2 GB	As Per Batch Size	
2.	Storage Type	Disk Space >20 GB		
3.	Internet Connectivity	Minimum 10 Mbps stable connection for download		

VIII. Conclusion

……

……

……

IX. Practical Related Questions

Note: Below are a few sample questions for reference. Teachers must design more such questions to ensure the achievement of the identified CO.

1. What are the ethical boundaries of such cooperation?
2. How can digital forensic investigators balance the need for evidence with the protection of individual privacy rights?
3. Does creating a backdoor for one case justify the potential risk to millions of users' data security?
4. What role should transparency and public accountability play in digital forensic investigations involving private data?
5. If Apple had complied with the FBI's request, how might that have changed the ethical landscape of digital privacy and surveillance?

(Space for answers)

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

X. References/Suggestions for further Reading Assessment Scheme

1. https://www.pingplotter.com/manual/
2. https://www.wireshark.org/docs/wsug_html_chunked/

XI. Assessment Scheme

The given performance indicators should serve as a guideline for assessment regarding process and product related marks. Faculty must fill only the table at bottom.

Performance Indicators		Weightage
Process related (15 Marks)		**60%**
1	Logic formation	30%
2	Debugging ability	20%
3	Follow ethical practices	10%
Product related (10 Marks)		**40%**
4	Expected output	10%
5	Timely Submission	15%
6	Answer to sample questions	15%
	Total: 25 Marks	**100%**

Marks obtained			Dated Sign of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No. 4: Investigate data in a cloud environment, focusing on issues like data privacy and security breaches

a. **Conduct a forensic analysis of cloud storage (e.g., Dropbox, Google Drive) for potential data breaches or misuse**
b. **Retrieve access logs and analyze activities that suggest unauthorized access or tampering**
(Hint: Use Cloud storage APIs, AWS CloudTrail, Google Cloud Platform logs.)

I. Practical Significance

These practical holds significant real-world value as it equips learners with essential skills in cloud forensics, enabling them to detect, investigate, and respond to data privacy violations and security breaches in platforms like Dropbox, Google Drive, AWS, and GCP. By analyzing access logs, file histories, and API activity, students gain hands-on experience with industry-standard tools and develop a deeper understanding of how to trace unauthorized access, ensure regulatory compliance, and strengthen organizational cybersecurity.

II. Industry / Employer Expected outcome(s)

The industry expects this practical to produce professionals capable of conducting real-time forensic investigations in cloud environments, identifying unauthorized access, data misuse, and breaches using tools like AWS CloudTrail, Google Cloud Audit Logs, and cloud storage APIs. Graduates should be able to interpret access logs, detect anomalies, ensure compliance with data protection regulations, and contribute to incident response and risk mitigation strategies.

III. Course Level Learning outcome(s)

CO 2: Apply various Digital Forensic Investigation Models.

IV. Laboratory Learning outcome(s)

LLO 4.1: Investigate data in a cloud environment focusing on issues like data privacy and security breaches.

V. Relevant Affective Domain related Outcome(s)

Demonstrates concern for data privacy and security breaches when working within cloud environments.

VI. Relevant Theoretical Background

Cloud forensics is a specialized branch of digital forensics focused on investigating incidents within cloud computing environments. It builds on foundational principles of digital evidence handling,

including data integrity, chain of custody, and authentication, but adapts them to the distributed, virtualized nature of cloud platforms.

Stepwise Procedure

A. Forensic Analysis of Cloud Storage

1. Dropbox

- **Artifacts to collect:**
  - File metadata (creation, modification, deletion timestamps)
  - Shared link history
  - Login and session records

- **Tools & Techniques:**
  - Use Dropbox API to extract audit logs and file history
  - Analyze `.dropbox.cache` folder on synced devices
  - Examine local SQLite databases for sync activity

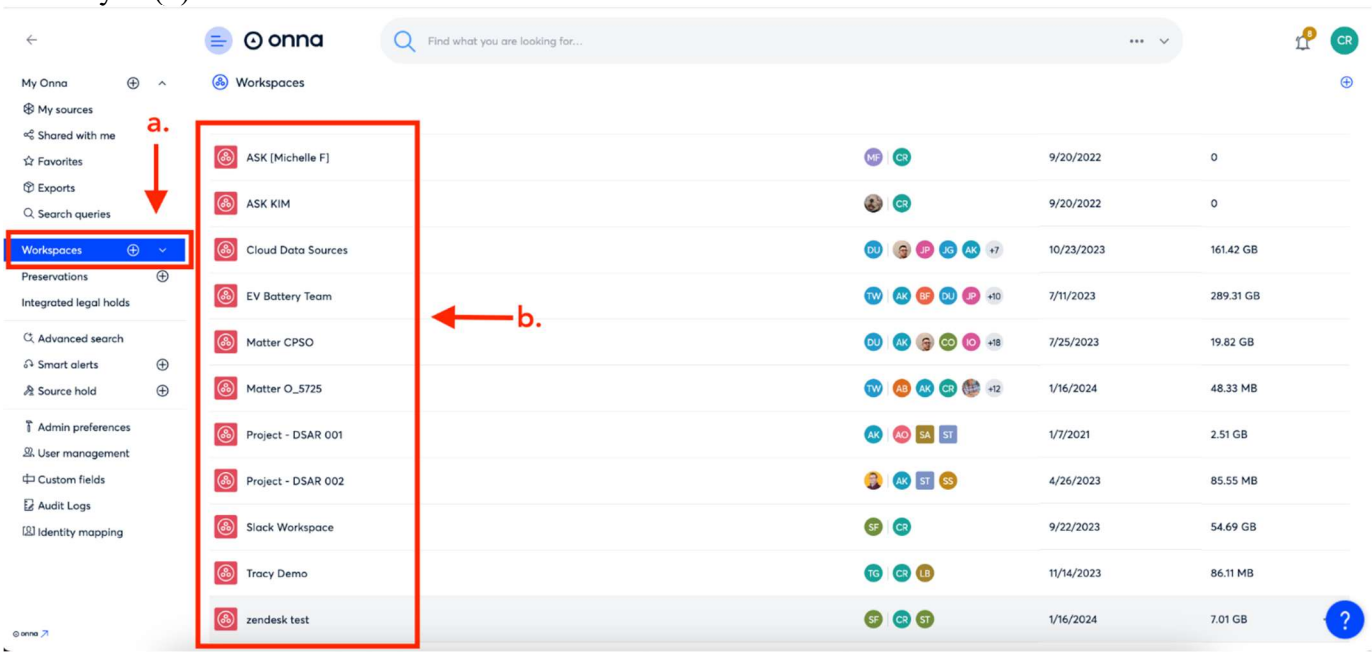
How to Connect and Collect Using Dropbox Business

Note: Before beginning a sync, we recommend signing into your Dropbox Business account in your browser. If you are using a service account, we recommend signing out of your regular account and signing back in with the service account credentials before running the collection.

To create a new Dropbox Business collection, follow the steps below:

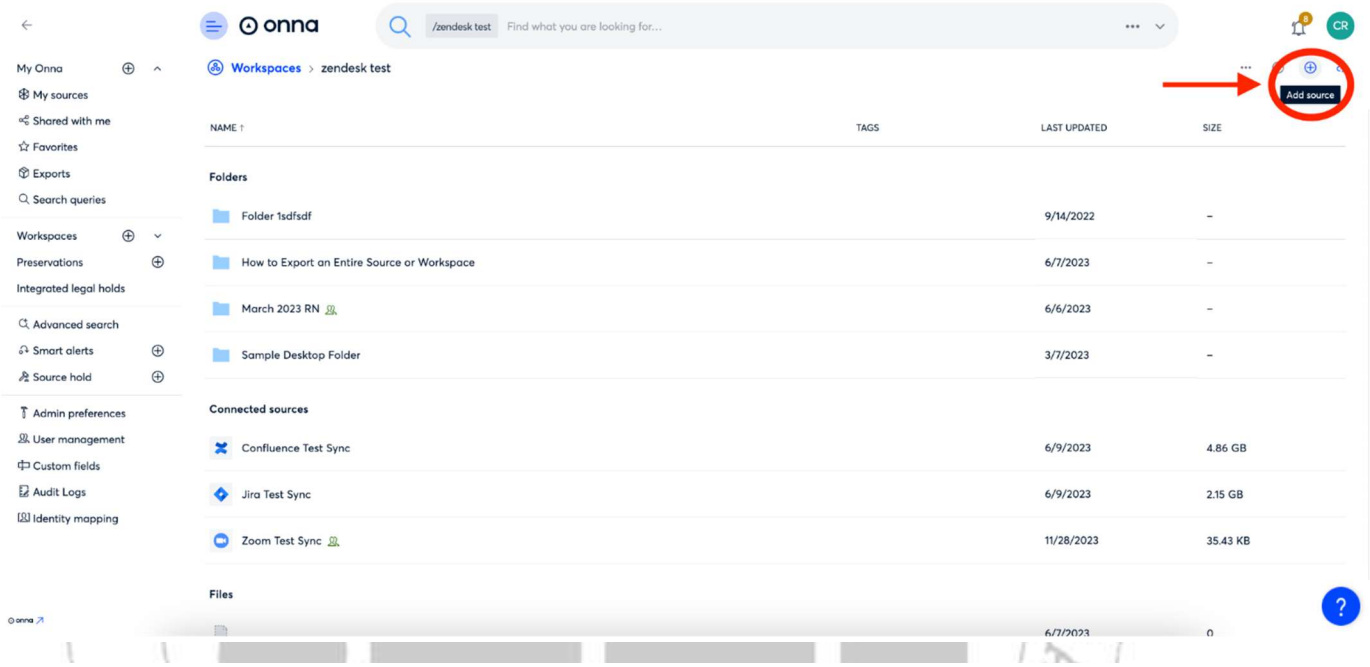
Step 1

Click on 'Workspaces' in the main menu (a), then click on the workspace where you'd like to add a new sync (b).



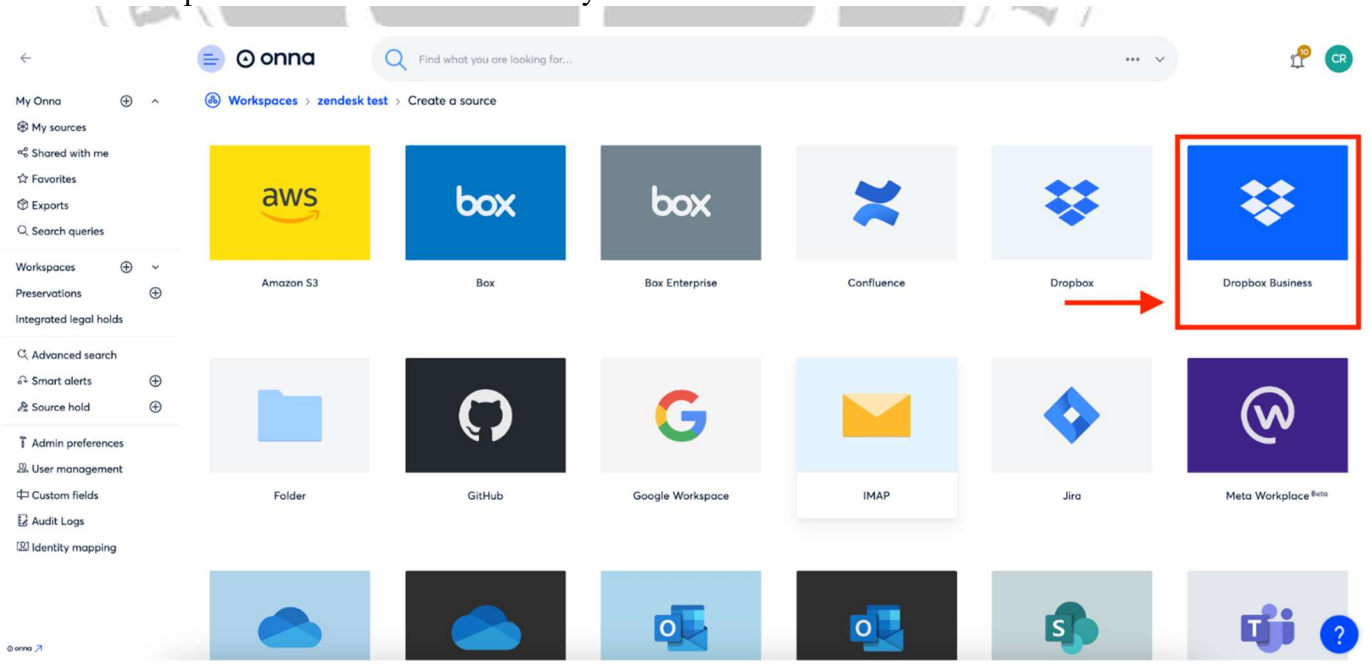
Step 2

Click on the '+' icon in the upper right corner to add a new source



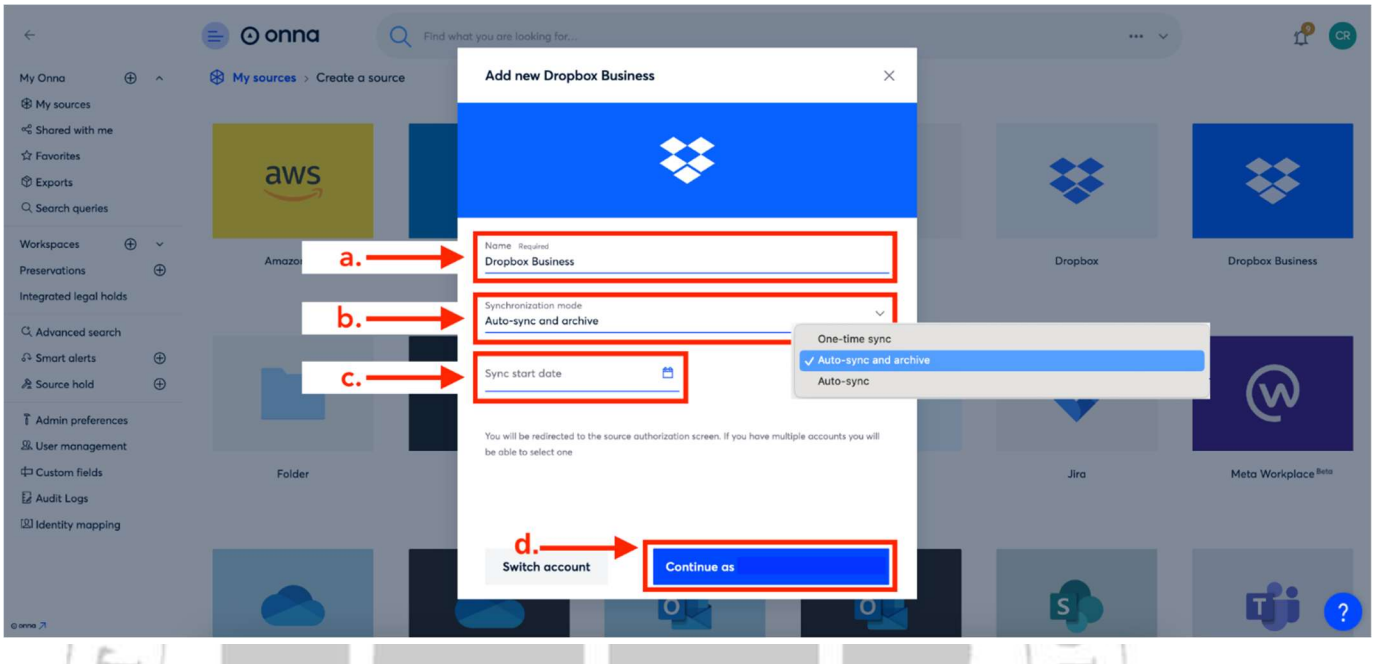
Step 3

Select the Dropbox Business connector from your list of available connectors.



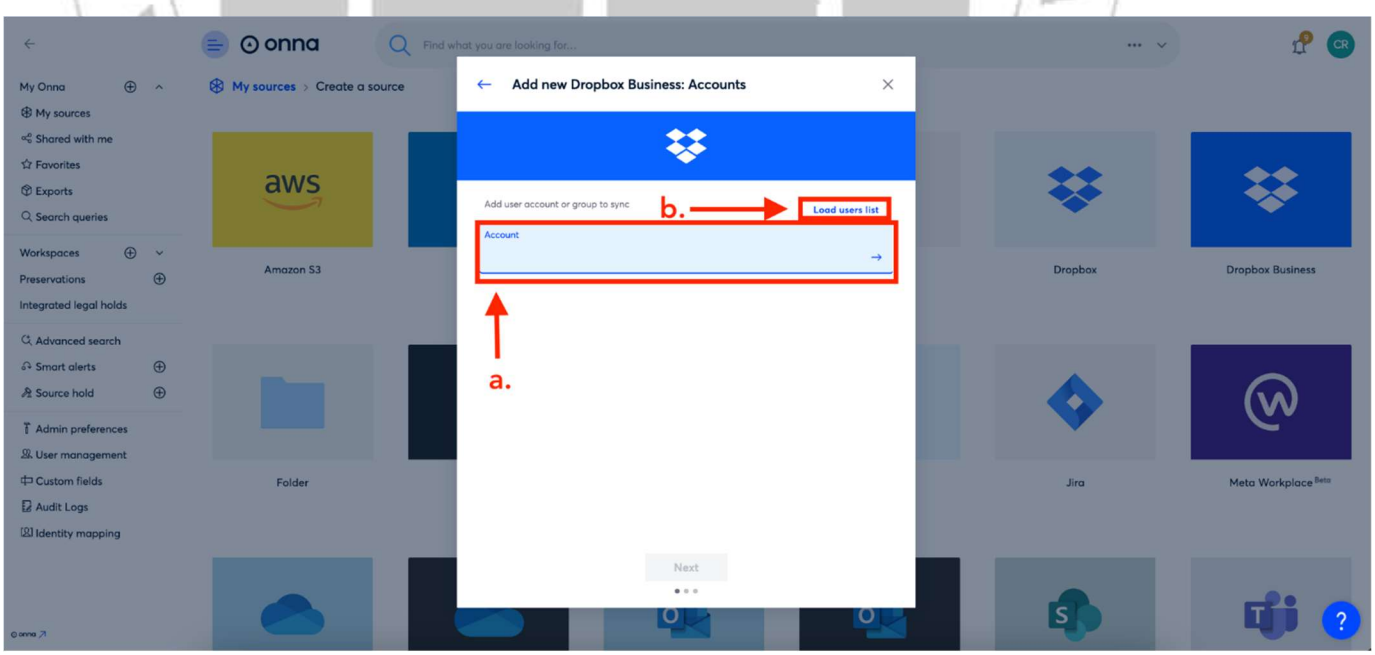
Step 4

To configure your Dropbox sync you'll first name your sync in the 'Name' field (a). Then, select your synchronization mode (b) and set your sync start and/or end date (c). Then, click the blue 'Continue as' button (d).



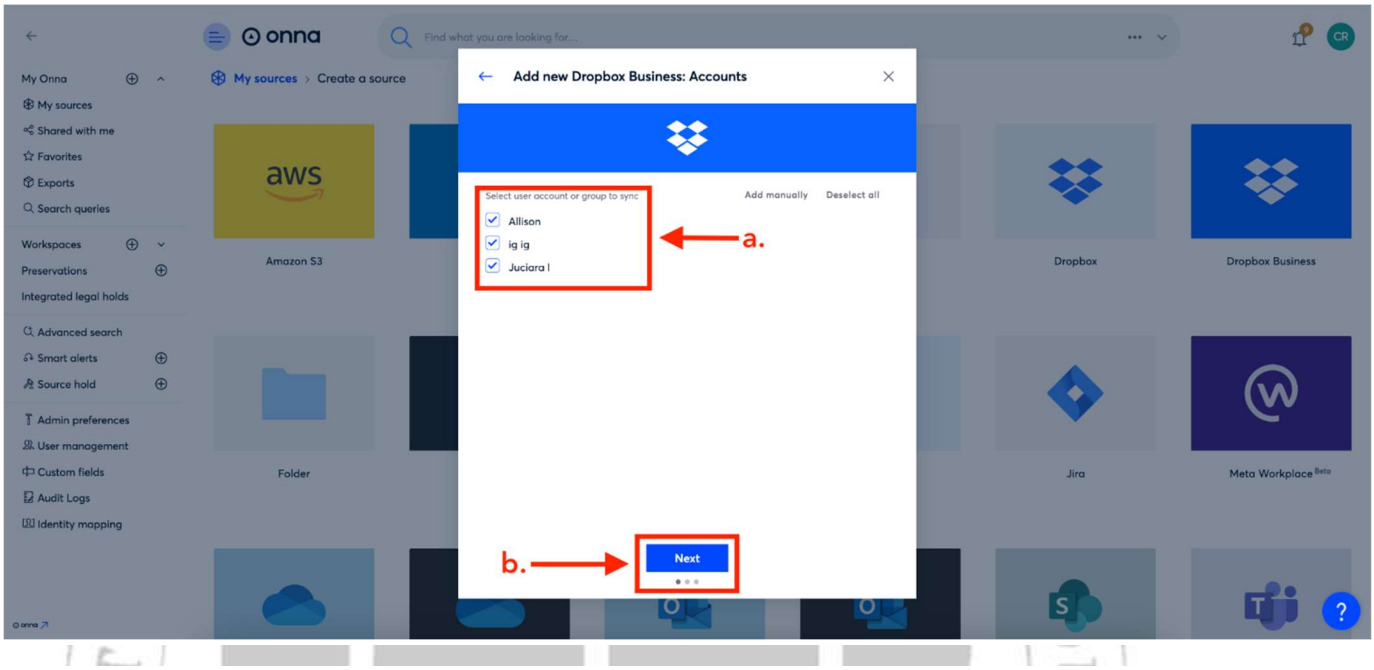
Step 5

You can now add users to your sync. You can do this by manually adding user account email addresses in the 'Add user accounts to sync field' (a), or selecting the 'Load users' option (b).



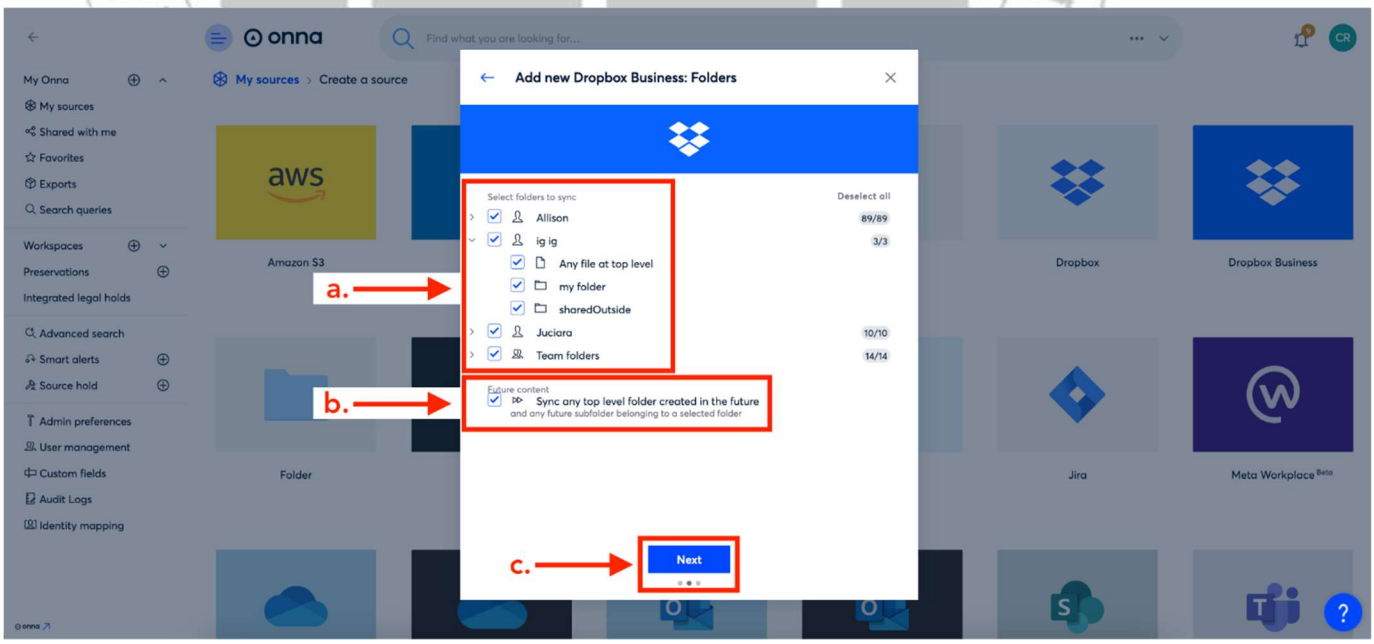
Step 6

If you 'Load users' list of all users in your Dropbox account will appear and you can select users by putting a check in the box next to their name (a). Then, click the blue 'Next' button (b).



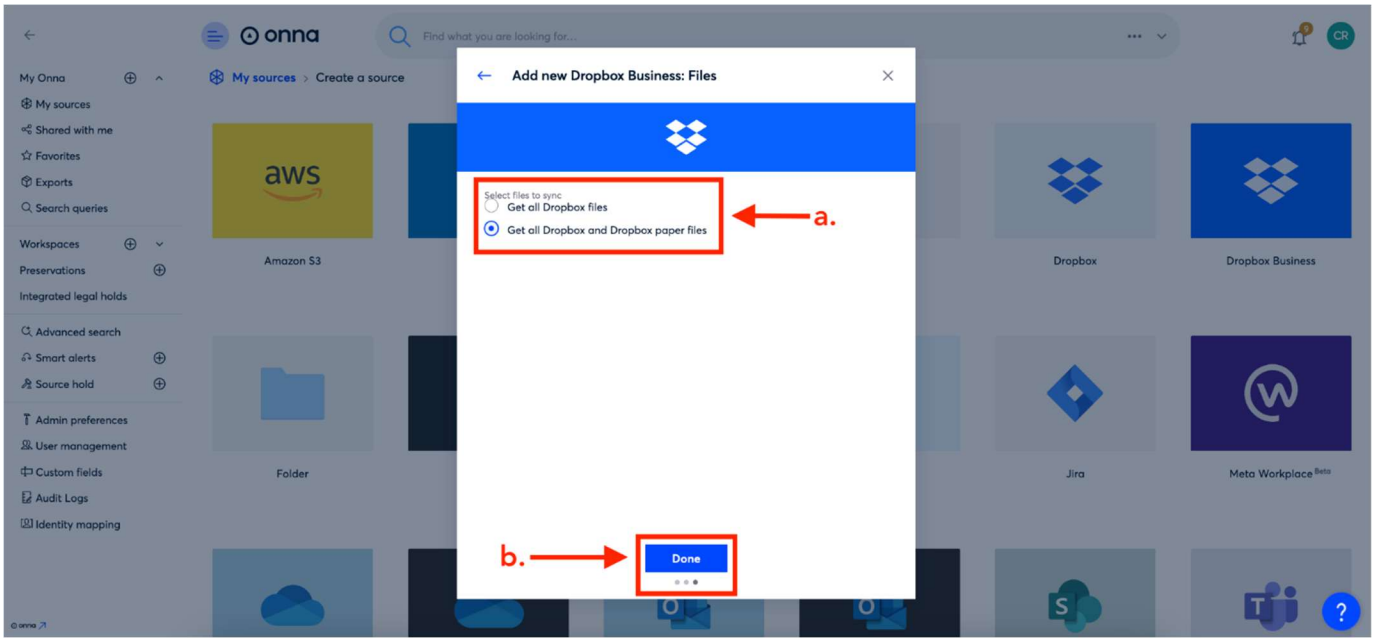
Step 7

On the next screen, you'll select the folders you want to include in your sync (a) and then, if you'd like to sync future content, put a check in the box next to 'Sync any top level folder created in the future' (b). Then, click the blue 'Next' button (c).



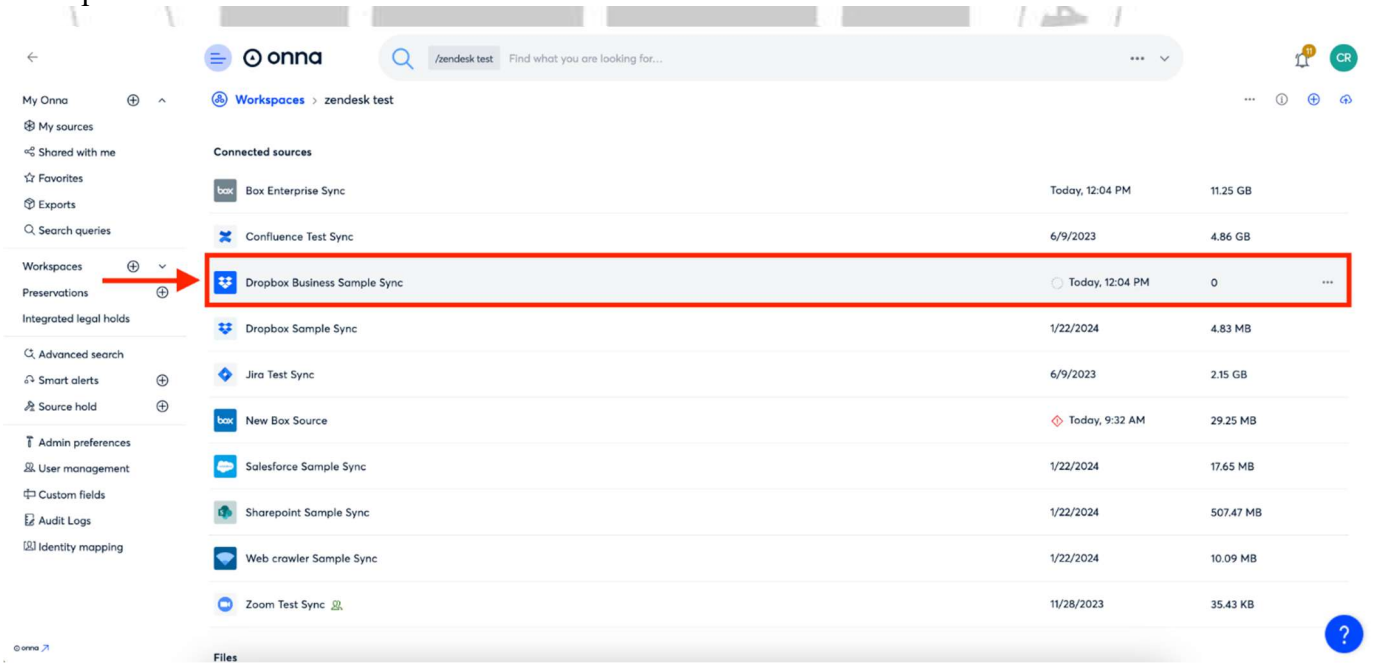
Step 8

Your final step is to select files to sync (a). You can either select 'Get all Dropbox files' or 'Get all Dropbox and Dropbox paper files'. Once you've selected your file preference you will click the blue 'Done' button (b).



Step 9

You'll now see your new source appear alphabetically in the list of 'Connected sources' in your workspace.



2. Google Drive

- **Artifacts to collect:**
  - Document version history
  - Access permissions and sharing settings
  - User activity logs
- **Tools & Techniques:**
  - Use Google Drive API to extract metadata and revision history

- Retrieve audit logs via Google Workspace Admin Console
- Analyze metadata for signs of tampering or unauthorized edits

B. Retrieve Access Logs & Analyze for Breaches

1. AWS CloudTrail

- **Steps:**
  - Enable CloudTrail logging for all regions
  - Filter logs for ConsoleLogin, GetObject, PutObject, DeleteObject
  - Look for anomalies like logins from unusual IPs or access outside business hours

Google Cloud Platform (GCP)

- **Steps:**
  - Use Cloud Audit Logs to monitor access to storage buckets
  - Analyze dataAccess logs for unauthorized reads/writes
  - Correlate IAM policy changes with suspicious activity

3. Dropbox & Google Drive APIs

- **What to look for:**
  - Sudden changes in file sharing settings
  - Access from unknown devices or IP addresses
  - Bulk downloads or deletions

Challenges & Considerations

- **Data Privacy:** Ensure compliance with GDPR, HIPAA, or other relevant regulations when accessing user data
- **Log Retention:** Cloud providers may limit how long logs are stored—set up automated exports
- **Encryption:** Understand how data is encrypted at rest and in transit to assess exposure risk

VII. Resources required

Sr. No.	Name of Resource	Specification	Quantity	Remarks (If any)
1.	Computer System	Computer (i3-i5 preferable RAM>2 GB	As Per Batch Size	
2.	Storage Type	Disk Space >20 GB		
3.	Internet Connectivity	Minimum 10 Mbps stable connection for download		

VIII. Conclusion

……...……

……...……

……...……

IX. Practical Related Questions

Note: Below are a few sample questions for reference. Teachers must design more such questions to ensure the achievement of the identified CO.

1. What types of logs can be retrieved from AWS CloudTrail and how can they help identify unauthorized access to cloud resources?
2. How does the use of APIs (e.g., Dropbox API, Google Drive API) facilitate forensic investigation in cloud storage environments?
3. What are the key indicators in access logs that suggest a potential data breach or misuse of cloud storage?
4. How do legal and jurisdictional challenges affect the collection and analysis of forensic evidence in cloud environments?
5. Compare the forensic capabilities of Google Cloud Platform and AWS in terms of log granularity, retention

(Space for answers)

.....

.....

.....

.....

.....

.....

.....

.....

.....

X. References/Suggestions for further Reading Assessment Scheme

1. https://developer.mozilla.org/en-US/docs/Web/Media/Streaming
2. https://wiki.wireshark.org/RTP

XI. Assessment Scheme

The given performance indicators should serve as a guideline for assessment regarding process and product related marks. Faculty must fill only the table at bottom.

Performance Indicators		Weightage
Process related (15 Marks)		**60%**
1	Logic formation	30%
2	Debugging ability	20%
3	Follow ethical practices	10%
Product related (10 Marks)		**40%**
4	Expected output	10%
5	Timely Submission	15%
6	Answer to sample questions	15%
	Total: 25 Marks	**100%**

Marks obtained			Dated Sign of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No. 5: Collect live data on Windows\Linux:

a. **Create a response toolkit on windows having utility cmd.exe, PsLoggedOn, netstat**
b. **Establish TCP connection between forensic investigation and workstation and the target system using netcat**
c. **Run trusted cmd.exe, identify logged users and remote access users, Record creation, access times and all the modifications made to the files**

I. Practical Significance

The practical significance of this live data collection exercise lies in its direct application to real-world digital forensic investigations and incident response. It trains practitioners to capture volatile evidence—such as logged-in users, active network connections, and file activity—before it disappears, which is critical in cases involving cyber intrusions, insider threats, or unauthorized access. By using trusted tools and remote access techniques like netcat, investigators learn to minimize contamination and maintain the integrity of the evidence.

II. Industry / Employer Expected outcome(s)

The industry-expected outcome for this live data collection practical in digital forensics is a structured, reliable, and legally sound acquisition of volatile evidence from a running system. Professionals are expected to demonstrate proficiency in using trusted tools (e.g., cmd.exe, PsLoggedOn, netstat) to identify active users, remote sessions, and network activity, while maintaining the integrity of the system. They should be able to establish secure remote connections (e.g., via netcat), extract file metadata (creation, access, modification times), and document all actions to preserve the chain of custody.

III. Course Level Learning outcome(s)

CO3: Apply digital Evidence collecting and handling techniques.

IV. Laboratory Learning outcome(s)

LLO 5.1: Run given commands on Windows/Linux OS to collect live data.

V. Relevant Affective Domain related Outcome(s)

Shows diligence and readiness in executing prescribed commands to collect volatile live data promptly and correctly.

VI. Relevant Theoretical Background

Live data collection in digital forensics involves acquiring volatile information from a running system to preserve evidence that would be lost upon shutdown. This includes identifying logged-in users, active network connections, and file metadata such as creation, access, and modification times. Tools like cmd.exe, PsLoggedOn, and netstat are used on Windows systems to gather this data, while netcat facilitates remote access by establishing a TCP connection between the forensic workstation and the target machine

Stepwise Procedure

a. Response Toolkit on Windows

Create a toolkit with the following utilities:

1. cmd.exe
    a. Native Windows command-line interpreter.
    b. Use for executing built-in commands like dir, tasklist, whoami, net user, etc.
2. PsLoggedOn (Sysinternals)
    a. Identifies users currently logged on locally and remotely.
    b. Command:PsLoggedOn.exe
3. netstat
   Displays active network connections and listening ports.
   Command: netstat –ano

b. Establish TCP Connection Using Netcat

- Netcat (nc) is a versatile tool for creating TCP connections between systems.
- On Target System (Listener):nc -lvp 4444
- On Forensic Workstation (Client): nc [target_ip] 4444
- This sets up a raw TCP channel. You can redirect shell output or transfer files through this connection.

c. Run Trusted cmd.exe and Collect Data

Once connected, execute trusted commands to gather forensic data.

1. Identify Logged-In Users
   Cmd query user
   PsLoggedOn.exe
2. Check Remote Access Users
   Cmd netstat -ano | findstr ESTABLISHED
   Match PIDs with tasklist to identify remote sessions.

3. File Metadata Collection
   Use dir and fsutil to inspect timestamps:
   Cmd dir /T:C /T:A /T:W
   /T:C → Creation time
   /T:A → Last access time
   /T:W → Last write time
   For NTFS timestamps:
   Cmd fsutil file queryfileid [filename]
4. Audit File Modifications
   Enable auditing via Group Policy or use PowerShell:
   Powershell Get-FileHash [filename]
   Compare hashes over time to detect changes.

VII. Resources required

Sr. No.	Name of Resource	Specification	Quantity	Remarks (If any)
1.	Computer System	Computer (i3-i5 preferable RAM>2 GB	As Per Batch Size	
2.	Storage Type	Disk Space >20 GB		
3.	Internet Connectivity	Minimum 10 Mbps stable connection for download		

VIII. Conclusion

……...……

……...……

……...……

IX. Practical Related Questions

Note: Below are a few sample questions for reference. Teachers must design more such questions to ensure the achievement of the identified CO.

1. What are the risks of using netcat for remote forensic data collection, and how can they be mitigated?
2. How can you verify the integrity of the response toolkit before deploying it on a target system?
3. What types of user activity can be inferred from PsLoggedOn and netstat, and how reliable are these indicators?
4. How do NTFS file timestamps help in forensic investigations, and what are their limitations?

5. What are the legal and ethical considerations when collecting live data from a suspect system?

(Space for answers)

.....

.....

.....

.....

.....

.....

.....

.....

X. References/Suggestions for further Reading Assessment Scheme

1. https://developer.mozilla.org/en-US/docs/Web/Media/Streaming
2. https://wiki.wireshark.org/RTP

XI. Assessment Scheme

The given performance indicators should serve as a guideline for assessment regarding process and product related marks. Faculty must fill only the table at bottom.

	Performance Indicators	Weightage
	Process related (15 Marks)	**60%**
1	Logic formation	30%
2	Debugging ability	20%
3	Follow ethical practices	10%
	Product related (10 Marks)	**40%**
4	Expected output	10%
5	Timely Submission	15%
6	Answer to sample questions	15%
	Total: 25 Marks	**100%**

Marks obtained			Dated Sign of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No. 6: Create Forensic Images with any Imager Tool like Exterro FTK Imager

I. Practical Significance

The practical significance of forensic imaging using FTK Imager lies in its critical role in preserving digital evidence for legal and investigative purposes. By creating a bit-for-bit copy of a storage device, investigators can analyze data including deleted files, hidden partitions, and system metadata without altering the original source. This ensures the integrity and admissibility of evidence in court, supports incident response in cybersecurity cases, and enables repeatable analysis by multiple experts.

II. Industry / Employer Expected outcome(s)

The industry-expected outcome for a forensic imaging practical using FTK Imager is the ability to perform a complete, accurate, and legally admissible acquisition of digital evidence. This includes selecting the correct source and image format, applying write-blocking techniques to prevent data alteration, generating and verifying cryptographic hash values to ensure integrity, and documenting the process thoroughly for chain-of-custody compliance.

III. Course Level Learning outcome(s)

CO3: Apply digital Evidence collecting and handling techniques.

IV. Laboratory Learning outcome(s)

LLO 6.1: Create Forensic Images with any Imager Tool.

V. Relevant Affective Domain related Outcome(s)

Appreciates the necessity of creating forensic images to ensure the authenticity and legal defensibility of evidence.

VI. Relevant Theoretical Background

Forensic imaging is a foundational process in digital forensics that involves creating an exact, bit-for-bit copy of a digital storage device to preserve evidence without altering the original data. Tools like Exterro FTK Imager facilitate this by capturing all data—including deleted files, slack space, and system metadata—into formats such as E01 or RAW, which support compression and integrity verification through hashing algorithms like MD5 or SHA1. This process ensures the integrity and admissibility of digital evidence in legal proceedings by maintaining a clear chain of custody and enabling investigators to analyze the image without compromising the original source.

Stepwise Procedure

How to Create Forensic Images Using FTK Imager

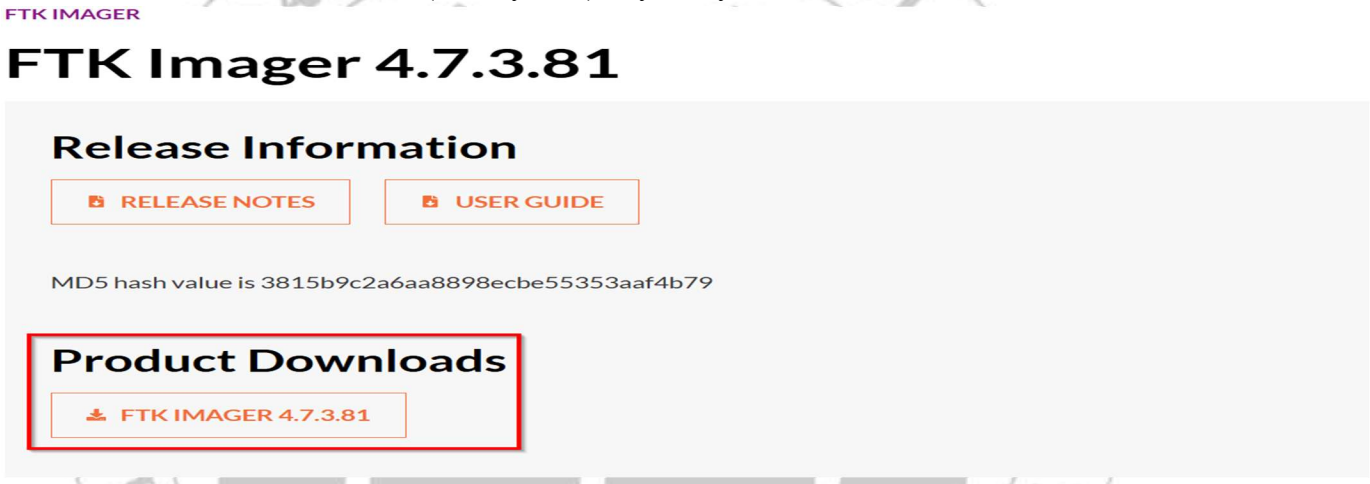
What You'll Need

- A computer with FTK Imager installed

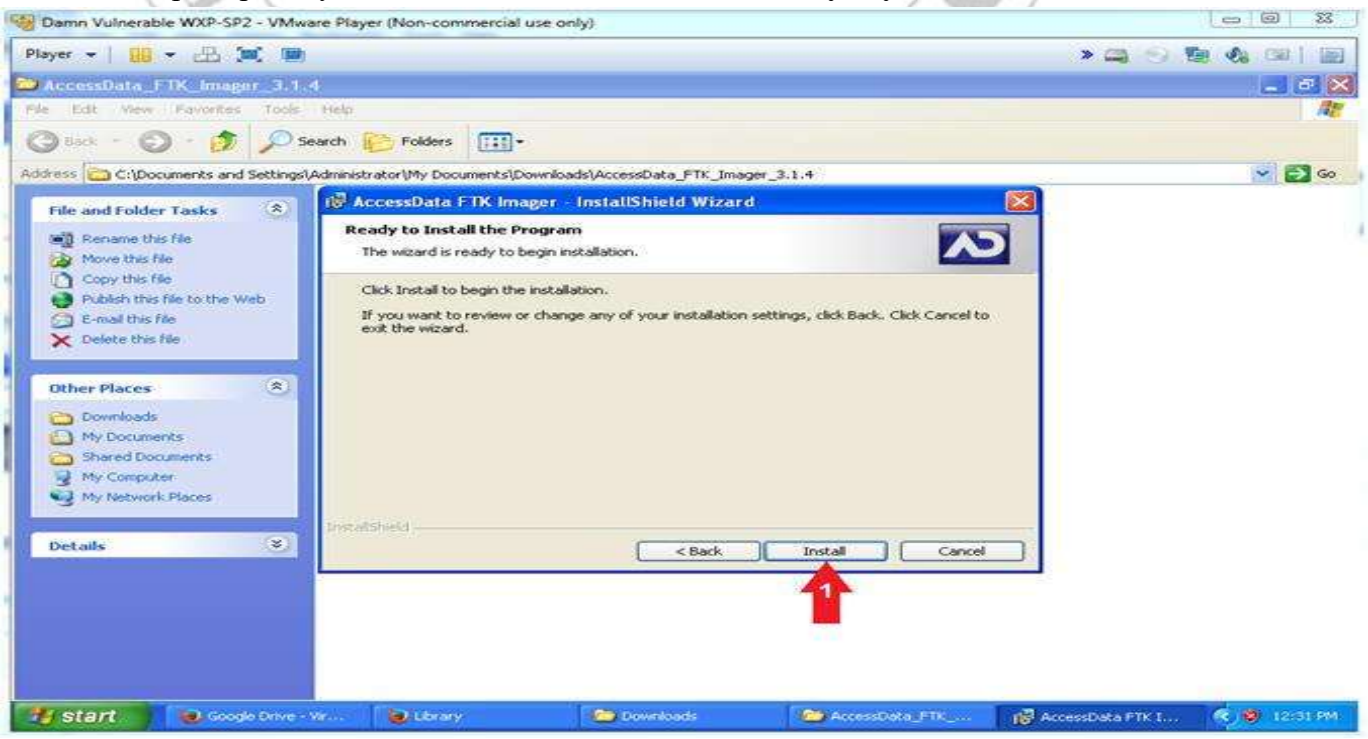
- External storage (e.g., USB drive or external HDD) for saving the image
- Administrator privileges

Stepwise Installation Guide for FTK Imager

1. **Download FTK Imager**
   - Visit the official AccessData/Exterro website or trusted sources like LetsDefend.
   - Fill out the download form (you can use alias details if preferred).
   - Save the installer file (usually .exe) to your system.



- **Run the Installer**
   - Locate the downloaded file (e.g., FTK Imager.exe).
   - Double-click to start installation.
   - If prompted by Windows SmartScreen, click **Run Anyway**.



3. **Accept License Agreement**
   - Read and accept the **End User License Agreement (EULA)**.
   - Click **Next** to proceed.

4. Choose Installation Location
   - By default, FTK Imager installs in C:\Program Files\AccessData\FTK Imager.
   - You may change the directory if needed.
   - Click **Next**.

5. Select Components
   - Choose whether to install shortcuts (Desktop/Start Menu).
   - Leave default options checked for a standard installation.
   - Click **Install**.

6. Installation Progress
   - The installer will copy files and configure FTK Imager.
   - Wait until the progress bar completes.

7. Finish Installation
   - Once complete, click **Finish**.
   - You can launch FTK Imager immediately or later from the Start Menu.

8. Verify Installation
   - Open FTK Imager.
   - Check the version under **Help → About** to confirm successful installation.

Steps to Create a Forensic Image

1. **Launch FTK Imager**
   - Open the application with administrative rights.
2. **Select the Source**
   - Go to File → Create Disk Image.
   - Choose the source type:
     - Physical Drive
     - Logical Drive
     - Image File
     - Folder
3. **Choose the Drive or Folder**
   - Select the specific drive or folder you want to image.
   - Click Finish to proceed.
4. **Configure Image Destination**
   - Choose the image type:
     - Raw (dd)
     - SMART
     - E01 (Expert Witness Format)
     - AFF

- Set the destination path and filename.
- Add a case number, examiner name, and description (optional but recommended).

5. **Set Image Fragment Size**
   - Useful if you need to split the image into smaller parts (e.g., for FAT32 drives).
6. **Enable Verification**
   - Check the box to verify the image after creation (MD5/SHA1 hash comparison).
7. **Start Imaging**
   - Click Start to begin the imaging process.
   - Monitor progress and ensure no errors occur.
8. **Review Logs**
   - FTK Imager will generate a log file with details of the imaging process.
   - Save this for your case documentation.

VII. Resources required

Sr. No.	Name of Resource	Specification	Quantity	Remarks (If any)
1.	Computer System	Computer (i3-i5 preferable RAM>2 GB	As Per Batch Size	
2.	Storage Type	Disk Space >20 GB		
3.	Internet Connectivity	Minimum 10 Mbps stable connection for download		

VIII. Conclusion

……...……

……...……

……...……

IX. Practical Related Questions

Note: Below are a few sample questions for reference. Teachers must design more such questions to ensure the achievement of the identified CO.

1. What image format should I choose (E01, RAW, AFF), and how does each affect compression and metadata?
2. How do I verify the integrity of the forensic image after creation?
3. Can I image a live system without shutting it down, and what are the risks?
4. How do I handle encrypted drives or partitions during imaging?
5. What's the best way to document the imaging process for chain-of-custody compliance?

(Space for answers)

.....

.....

.....

.....

.....

.....

.....

X. References/Suggestions for further Reading Assessment Scheme

1. https://www.geeksforgeeks.org/ethical-hacking/how-to-create-a-forensic-image-with-ftk-imager/
2. https://archive.org/download/Digital-Forensics-FTK-AZM/Digital%20Forensics%20%28FTK%29%20%28AZM%29%20.pdf

XI. Assessment Scheme

The given performance indicators should serve as a guideline for assessment regarding process and product related marks. Faculty must fill only the table at bottom.

Performance Indicators		Weightage
Process related (15 Marks)		**60%**
1	Logic formation	30%
2	Debugging ability	20%
3	Follow ethical practices	10%
Product related (10 Marks)		**40%**
4	Expected output	10%
5	Timely Submission	15%
6	Answer to sample questions	15%
	Total: 25 Marks	**100%**

Marks obtained			Dated Sign of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No. 7: Create Forensic Images with any Imager Tool like Exterro FTK Imager

I. Practical Significance

The practical significance of hashing in digital forensics lies in its ability to ensure the integrity and authenticity of digital evidence throughout an investigation. By generating a unique hash value for a file at the time of collection, investigators can later verify that the evidence has not been altered by comparing it with the original hash. This is crucial for maintaining a trustworthy chain of custody, especially when evidence is transferred between devices, analysts, or legal entities.

II. Industry / Employer Expected outcome(s)

In the digital forensics and cybersecurity industry, the expected outcome of applying hashing techniques is the reliable verification of data integrity and authenticity. When digital evidence is collected, its hash value is generated and securely stored. Throughout the investigation and legal process, this hash is used to confirm that the evidence remains unchanged. Any alteration, even a single byte, results in a completely different hash, immediately signaling tampering. This process ensures trust in the chain of custody, supports admissibility in court, and aligns with industry standards for handling digital artifacts securely and transparently.

III. Course Level Learning outcome(s)

CO3: Apply digital Evidence collecting and handling techniques

IV. Laboratory Learning outcome(s)

LLO 7.1: Perform Hashing to verify the authenticity of digital evidence.

V. Relevant Affective Domain related Outcome(s)

Defends the importance of hashing to ensure data integrity and verify the evidence's authenticity in a digital investigation.

VI. Relevant Theoretical Background

Hashing is a cryptographic technique used to convert digital data into a fixed-length string, known as a hash value, which uniquely represents the original content. Common hash algorithms like MD5 and SHA-256 are widely used in digital forensics to verify the integrity and authenticity of evidence. These hash functions are deterministic, meaning the same input always produces the same output, and they exhibit the avalanche effect—where even a minor change in the input drastically alters the hash. Because hashes are irreversible and collision-resistant, they serve as reliable digital fingerprints.

Stepwise Procedure

a. Create a File and Generate Hashes

Create a text file:

- Save the following content in a file named evidence.txt:
- Code: This is the original digital evidence.

Generate MD5 and SHA-256 hashes:

Use the following Python code:

```
import hashlib
def generate_hashes(file_path):
    with open(file_path, 'rb') as f:
        data = f.read()
        md5_hash = hashlib.md5(data).hexdigest()
        sha256_hash = hashlib.sha256(data).hexdigest()
        print(f"MD5: {md5_hash}")
        print(f"SHA-256: {sha256_hash}")
generate_hashes('evidence.txt')
```

b. Alter the File and Generate Hashes Again

Modify the file slightly:

Change the content to:

- Code - This is the original digital evidence!

Run the same Python code again:

You'll see that both the MD5 and SHA-256 hashes have changed completely.

VII. Resources required

Sr. No.	Name of Resource	Specification	Quantity	Remarks (If any)
1.	Computer System	Computer (i3-i5 preferable RAM>2 GB	As Per Batch Size	
2.	Storage Type	Disk Space >20 GB		
3.	Internet Connectivity	Minimum 10 Mbps stable connection for download		

VIII. Conclusion

……...……

……...……

……...……

IX. Practical Related Questions

Note: Below are a few sample questions for reference. Teachers must design more such questions to ensure the achievement of the identified CO.

1. How can law enforcement use hashing to prove that digital evidence hasn't been tampered with?
2. What happens if two files have the same hash value? Can this compromise evidence authenticity?
3. How do forensic analysts verify the integrity of a suspect's hard drive image using hashing?
4. Why is it important to use cryptographic hash functions instead of simple checksums for evidence verification?
5. Can hashing be used to detect unauthorized changes in log files or system configurations?

(Space for answers)

.....

.....

.....

.....

.....

.....

.....

.....

X. References/Suggestions for further Reading Assessment Scheme

1. https://labex.io/tutorials/comptia-digital-forensics-evidence-acquisition-and-integrity-594581%20"
2. https://www.sans.org/white-papers/hashing-digital-evidencehunting

XI. Assessment Scheme

The given performance indicators should serve as a guideline for assessment regarding process and product related marks. Faculty must fill only the table at bottom.

Performance Indicators		Weightage
Process related (15 Marks)		**60%**
1	Logic formation	30%
2	Debugging ability	20%
3	Follow ethical practices	10%
Product related (10 Marks)		**40%**
4	Expected output	10%
5	Timely Submission	15%
6	Answer to sample questions	15%
	Total: 25 Marks	**100%**

Marks obtained			Dated Sign of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No. 8: Recover deleted or corrupted files from a storage device and perform file carving (e.g., photos, documents) using any data recovery tool

I. Practical Significance

File recovery is the process of restoring lost, deleted, or corrupted data from storage devices such as hard drives, SSDs, USB drives, or memory cards. When a file is deleted, its data remains on the storage medium until it is overwritten by new information. Recovery tools use various techniques to locate and reconstruct such files.

II. Industry / Employer Expected outcome(s)

The aim of this course is to help the students to attain the following industry identified outcomes through various teaching learning experiences: Apply Digital Forensic methodology to carry out investigations and penetration tests.

III. Course Level Learning outcome(s)

CO3: Apply digital Evidence collecting and handling techniques.

IV. Laboratory Learning outcome(s)

LLO 8.1 Recover deleted or corrupted files from a storage device.

V. Relevant Affective Domain related Outcome(s)

Displays perseverance in using recovery tools to successfully locate and restore corrupted or deleted files.

VI. Relevant Theoretical Background

In file recovery, File carving is a data recovery technique used to retrieve files from storage devices without using file system information. Instead of relying on file names or directories, it scans the raw binary data of the disk and looks for file signatures unique patterns that mark the beginning and end of a file.

Some commonly used free recovery tools on Windows include:

1. WinfrGUI
2. Windows File Recovery
3. Wonder share recoverit
4. Disk Drill
5. PhotoRec
6. Recuva

In this practical, two tools are used to perform file recovery and file carving

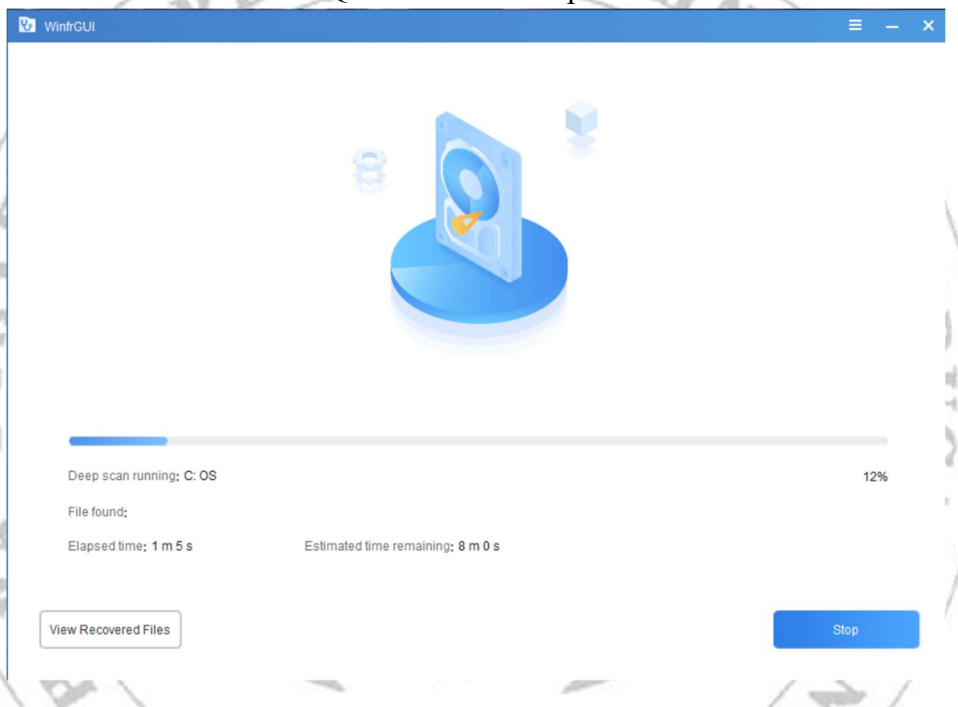
1. **WinfrGUI (Graphical Interface for Windows File Recovery)**
2. **Windows File Recovery (Command-line Tool)**

1. **Using WinfrGUI**

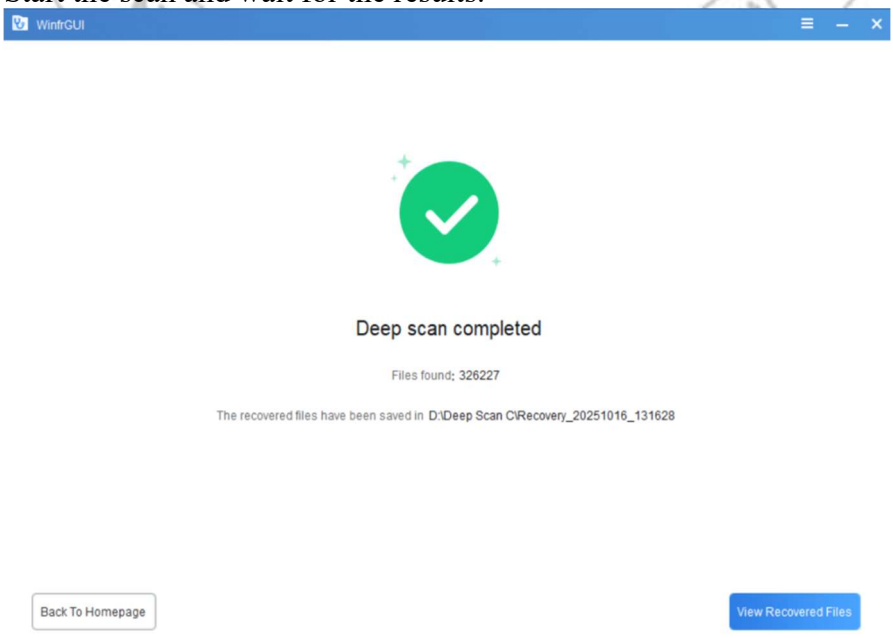
   WinfrGUI is a graphical version of the Windows File Recovery tool. It provides an easy-to-use interface for recovering deleted files without using complex command-line syntax.

   Steps:

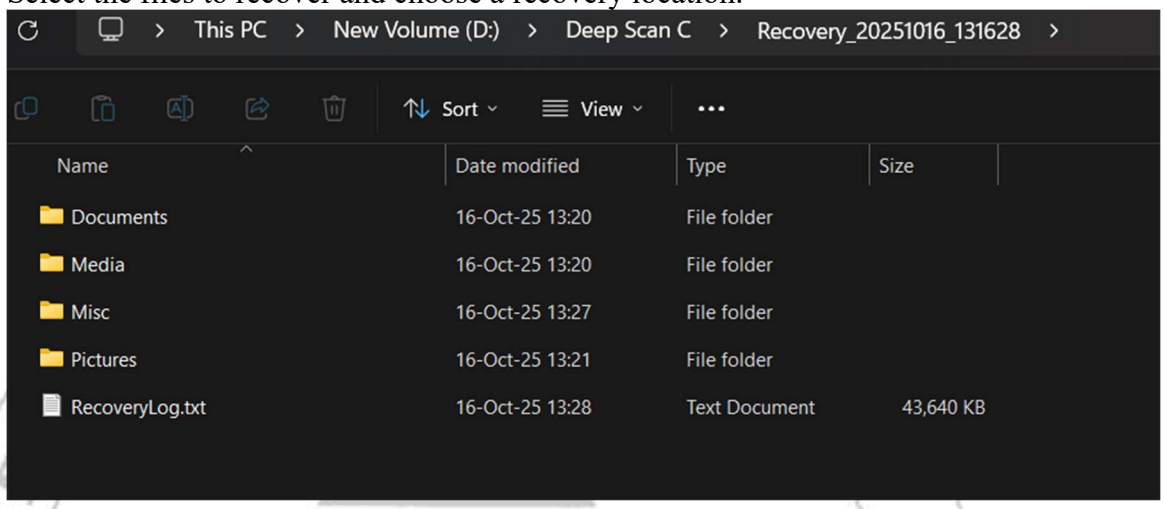
   1. Download (https://www.winfr.org)and install WinfrGUI.
   2. Launch the application and select the drive from which files are to be recovered.
   3. Choose the scan mode – Quick Scan or Deep Scan.



   4. Start the scan and wait for the results.



5. Select the files to recover and choose a recovery location.



2. Using Windows File Recovery (Command-line Tool)

Windows File Recovery is a command-line utility developed by Microsoft for restoring deleted files. It can recover files from local hard drives, USB drives, and memory cards.

Steps:

i. Install Windows File Recovery from Microsoft Store (for some its inbuilt).

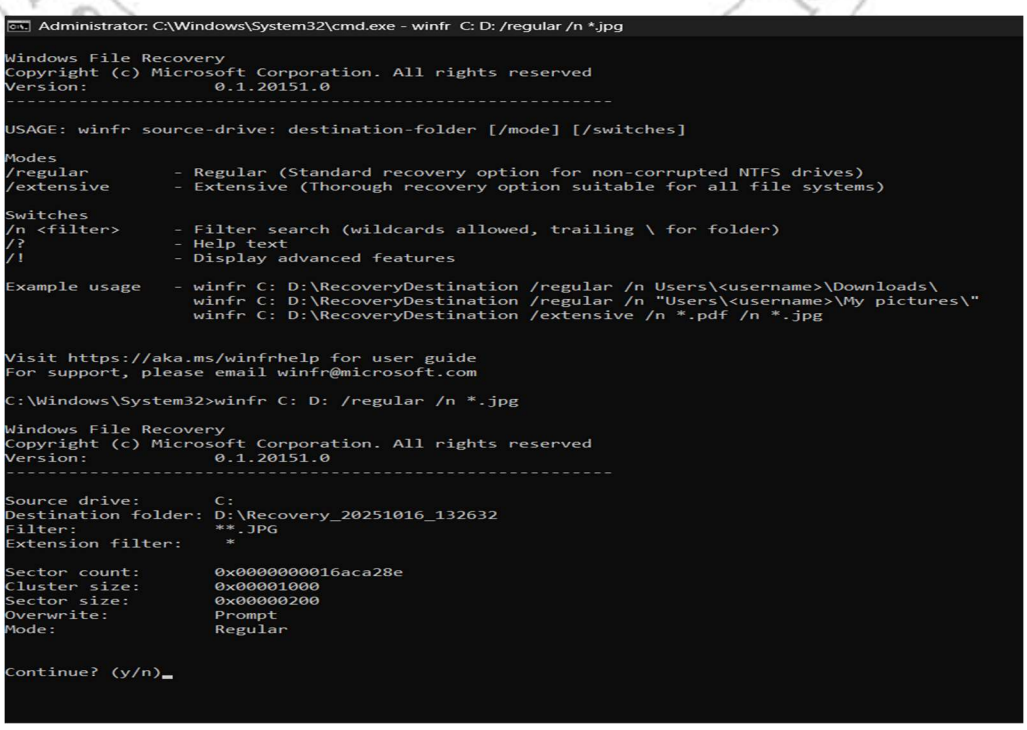
ii. Open Command Prompt with Administrator privileges (run as administrator).

iii. Run the recovery command specifying the source and destination drives.

Example Command:

winfr C: D: /regular /n *.jpg

This command recovers all .jpg files from drive C: to drive D: using regular mode



4. Wait for the process to complete and check the destination folder for recovered files. File carving enhances recovery accuracy, especially when file system information is missing or corrupted.

VII. Resources required

Sr. No.	Name of Resource	Specification	Quantity	Remarks (If any)
1.	Computer System	Computer (i3-i5 preferable RAM>2 GB	As Per Batch Size	
2.	Storage Type	Disk Space >20 GB		
3.	Internet Connectivity	Minimum 10 Mbps stable connection for download		

VIII. Conclusion

……

……

……

IX. Practical Related Questions

Note: Below are a few sample questions for reference. Teachers must design more such questions to ensure the achievement of the identified CO.

1. What are Quick Scan and Deep Scan?
2. What file systems are supported?
3. You accidentally deleted photos from your USB drive (E:). Describe the steps to recover them using WinfrGUI.

(Space for answers)

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

X. References/Suggestions for further Reading Assessment Scheme

1. https://www.winfrgui.com
2. https://www.winfr.org/docs.html

XI. Assessment Scheme

The given performance indicators should serve as a guideline for assessment regarding process and product related marks. Faculty must fill only the table at bottom.

Performance Indicators		Weightage
Process related (15 Marks)		**60%**
1	Logic formation	30%
2	Debugging ability	20%
3	Follow ethical practices	10%
Product related (10 Marks)		**40%**
4	Expected output	10%
5	Timely Submission	15%
6	Answer to sample questions	15%
	Total: 25 Marks	**100%**

Marks obtained			Dated Sign of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No 9. *Read and Interpret Operating Systems logs on Windows file system Hint: Check whether the log gives information about file systems. Any such entry indicates some malicious activity.

I. Practical Significance

Logs are records kept by the Operating System. They tell what is happening inside the computer like a diary of system events. Examples: system start-up, shutdown, software installation, login attempts, file creation/deletion, etc.

II. Industry / Employer Expected outcome(s)

The aim of this course is to help the students to attain the following industry identified outcomes through various teaching learning experiences: Apply Digital Forensic methodology to carry out investigations and penetration tests.

III. Course Level Learning outcome(s)

CO4 - Identify various types of cyber-attacks.

IV. Laboratory Learning outcome(s)

LLO 9.1 Read and Interpret Operating Systems logs on Windows file system.

V. Relevant Affective Domain related Outcome(s)

Seeks actively to interpret system logs, recognizing their importance as a source of evidence for potential malicious activity.

VI. Relevant Theoretical Background

Logs are like a diary or record book that Windows keeps to store information about everything happening inside the system such as: Who logged in, which files were opened, created, deleted, which programs are running and any errors or warnings. These records are saved automatically by Windows.

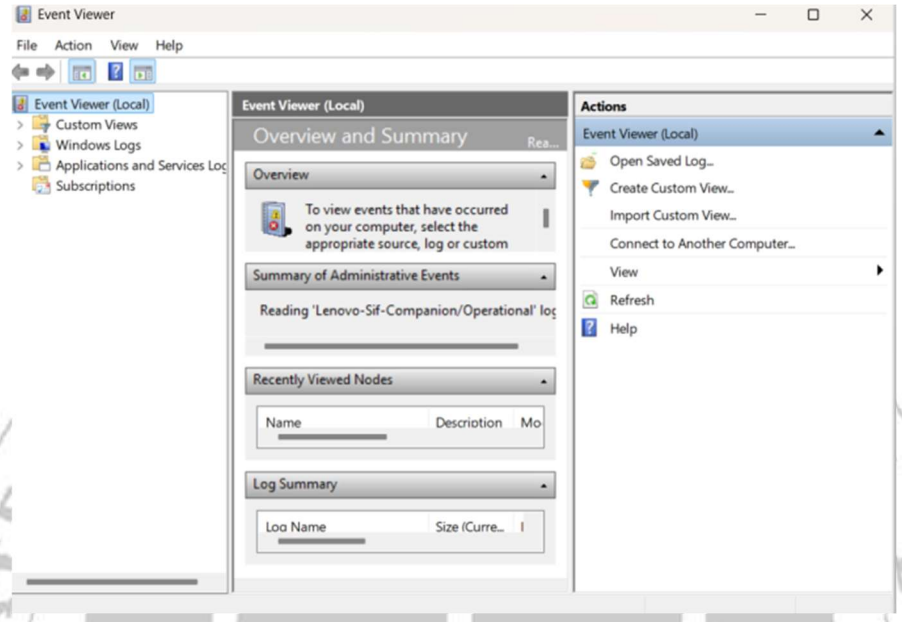
Logs are saved inside a special place called the Event Viewer.

To open it:

1. Press Windows + R
2. Type eventvwr.msc
3. Press Enter

you can see different types of logs like:

- Application Logs → Events from apps/programs
- System Logs → Events from Windows itself
- Security Logs → Login attempts, file access, etc.



File System Logs:

These logs record what happens to files and folders on the computer .when file created, opened, read, modified, deleted and change file permissions. These are called File System events and usually have event IDs like 4656, 4663, 4660.

logs important due to reasons:

1. Security: Helps detect hacking or malware (e.g., files changed without permission).
2. Troubleshooting: Find out why a program or file didn't work.
3. Monitoring: Know who accessed which file and when.

Steps to Read and Interpret OS Logs:

Example: If someone deleted a file from your PC, open the Security Logs.

Step 1: Open Event Viewer

1. Press Windows + R
2. Type eventvwr.msc
3. Press Enter

This opens the Event Viewer, where Windows stores all logs.

Step 2: Choose a Log Type

In the left panel, you'll see:

- Application Logs → Logs from installed apps
- System Logs → Logs from Windows services and drivers
- Security Logs → Logs for login, file access, etc. (this is most useful for file system monitoring)

Click Windows Logs → Security

Step 3: Read a Log Entry

Each log entry has:

- Date & Time – when the event happened

- Event ID – a number that tells what type of event it is
- User Name – who did the action
- Description – details of what happened

Example (in Security log):
Event ID: 4663
Description: An attempt was made to access an object
File name: C:\TestAudit\demo.txt
Access: Delete
User: Varad-PC\Admin
This means someone tried to delete or access that file.
Step 4: Interpret the Log
Reading is not enough, we must understand what it means

Event ID	Meaning	Interpretation
4656	File handle requested	A file was opened
4663	File accessed	Someone read, wrote, or deleted a file
4660	File deleted	The file was removed
4670	Permissions changed	Someone modified access control
4624	Logon	Someone logged in
4625	Failed logon	Someone tried and failed to log in

Step 5: Find File System Logs Using a Filter
To focus only on file activity:

1. Right-click Security log → click Filter Current Log.
2. In the Event IDs box, type: 4656,4663,4660,4670
3. Click OK.

Now you'll only see file system related events.
Step 6: Detect Suspicious Activity
You can interpret logs like this:

- Normal: User accessed their own documents.
- Suspicious: Unknown program accessed system files.
- Very suspicious: Files deleted or encrypted by unknown user or process.

Some files on OS logs
1. Event Logs (System, Application, Security, etc.)
Location: C:\Windows\System32\winevt\Logs\

File Type: .evtx files

Eg. System.evtx, Application.evtx, Security.evtx

2. Windows Update Logs

Windows 10 update logs can be viewed in the Event Viewer by navigating to Applications and Services Logs > Microsoft > Windows > WindowsUpdateClient > Operational.

Alternatively, you can see a history of installed updates in Settings under Update & Security > Windows Update > View update history.

For a more detailed and readable log file:

In Modern Windows (Windows 10/11**) ,** open PowerShell as an administrator and run the Get-WindowsUpdateLog command, which will generate the .log file on your desktop

3. System Boot and Driver Logs

Boot Logs Enable via: msconfig > Boot tab > Boot log

Log file location: C:\Windows\ntbtlog.txt

4. CBS (Component-Based Servicing) Logs

Useful for diagnosing Windows updates and system file corruption.

Location: C:\Windows\Logs\CBS\CBS.log

5. DISM Logs

From using the DISM tool (e.g., system repair commands).

Location: C:\Windows\Logs\DISM\dism.log

6. Setup Logs (Windows Install/Upgrade)

Location: C:\Windows\Panther\

Files: setupact.log, setuperr.log

7. Group Policy Logs

Location: C:\Windows\System32\GroupPolicy\

8. Task Scheduler Logs

In the event viewer>Applications and Service Logs>Microsoft > Windows > TaskScheduler

9. Application Logs

Many apps log to: C:\ProgramData\ or %LOCALAPPDATA%\

VII. Resources required

Sr. No.	Name of Resource	Specification	Quantity	Remarks (If any)
1.	Computer System	Computer (i3-i5 preferable RAM>2 GB	As Per Batch Size	
2.	Storage Type	Disk Space >20 GB		
3.	Internet Connectivity	Minimum 10 Mbps stable connection for download		

VIII. Conclusion

……...……

……...……

……...……

IX. Practical Related Questions

Note: Below are a few sample questions for reference. Teachers must design more such questions to ensure the achievement of the identified CO.

1. Why are system logs important?
2. What is the difference between an error log, access log, and event log?
3. How do you ensure log security?

(Space for answers)

.....

.....

.....

.....

.....

.....

.....

X. References/Suggestions for further Reading Assessment Scheme

1. https://www.loggly.com/ultimate-guide/windows-logging-basics/
2. https://docs.appian.com/suite/help/25.3/Logging.html

XI. Assessment Scheme

The given performance indicators should serve as a guideline for assessment regarding process and product related marks. Faculty must fill only the table at bottom.

	Performance Indicators	Weightage
	Process related (15 Marks)	**60%**
1	Logic formation	30%
2	Debugging ability	20%
3	Follow ethical practices	10%
	Product related (10 Marks)	**40%**
4	Expected output	10%
5	Timely Submission	15%
6	Answer to sample questions	15%
	Total: 25 Marks	**100%**

Marks obtained			Dated Sign of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No 10: Install Kali Linux

I. Practical Significance

Installing Kali Linux provides a powerful, specialized platform for cybersecurity learning, ethical hacking, system auditing, and hands-on security testing. Tools like Nmap, Wireshark, Metasploit, Aircrack-ng, and Burp Suite are already included in it. This saves time and ensures the tools are correctly configured in a security-focused environment. By exploring Kali's tools, users can discover weaknesses in their own networks or systems. This helps in proactively patching and securing systems.

II. Industry / Employer Expected outcome(s)

The aim of this course is to help the students to attain the following industry identified outcomes through various teaching learning experiences: Apply Digital Forensic methodology to carry out investigations and penetration tests.

III. Course Level Learning outcome(s)

CO4 - Identify various types of cyber-attacks.

IV. Laboratory Learning outcome(s)

LLO 10.1 Configure Kali Linux.

V. Relevant Affective Domain related Outcome(s)

Shows interest and initiative by successfully installing and configuring a specialized security OS (Kali Linux).

VI. Relevant Theoretical Background

Kali Linux is a powerful, open-source Linux distribution specifically designed for **penetration testing**, **ethical** hacki**ng**, **digital forensics** and **cybersecurity research**. It is maintained and developed by **Offensive Security**, a leading provider of security training and certifications.

It is developed and maintained by **Offensive Security** and comes with **hundreds of built-in tools** used by security experts to test the safety of computer systems and networks.

Examples of these tools include:

Nmap – for network scanning, **Metasploit** – for penetration testing, **Wireshark** – for network analysis, **Aircrack-ng** – for wireless security testing

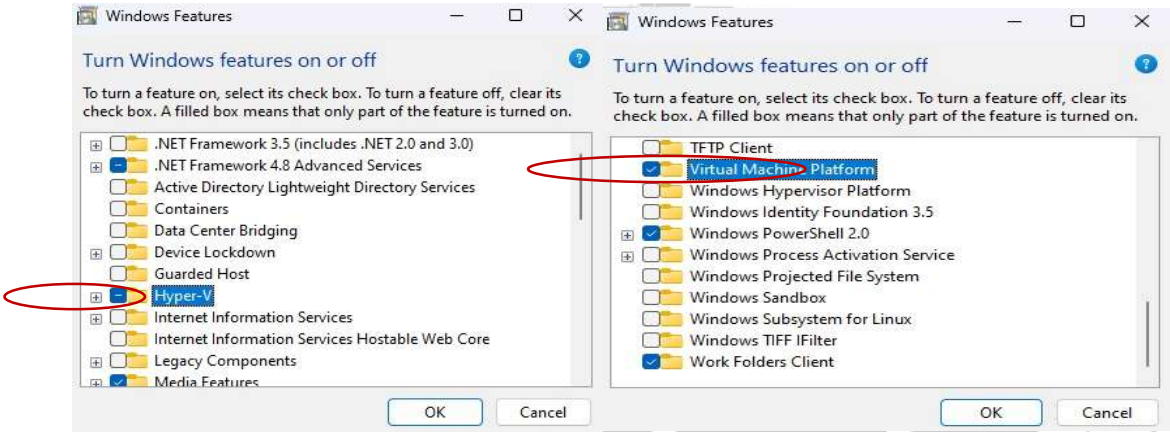
Pre-installation steps for Virtual Machine (Virtual Box)

Check System Requirements

Make sure your system can run Kali smoothly:

- CPU: 64-bit processor (x86_64) (not mandatory but better)
- RAM: Minimum 2 GB (4 GB or more recommended)
- Disk Space: 20 GB minimum (50+ GB recommended)
- USB/DVD (for bootable media)

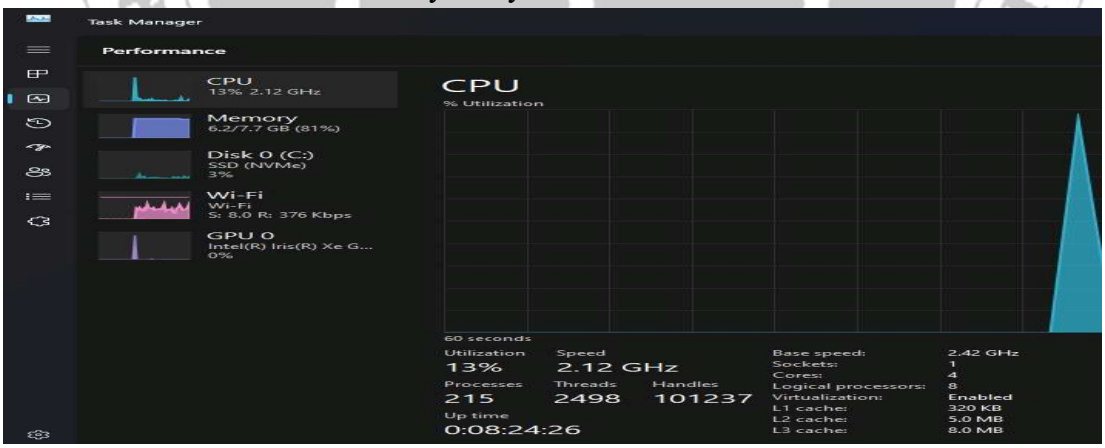
- UEFI/BIOS settings: Know how to boot from USB/DVD if installing
- Some steps to do before installation:
  - Open: Windows Features
  - Then enable these settings for virtualization:



These settings are crucial for installing Kali Linux in VirtualBox because:

Hyper-V and **Virtual Machine Platform** are Microsoft's built-in virtualization tools.

VirtualBox and Hyper-V/VMP are competing hypervisors that often **conflict** when running simultaneously or when both are enabled. For VirtualBox to run at **full speed and performance** using its native hardware acceleration (VT-x/AMD-V), you must **disable** Hyper-V and VMP in Windows Features and reboot your system.



Confirm by checking **Virtualization: Enabled in** task manager.

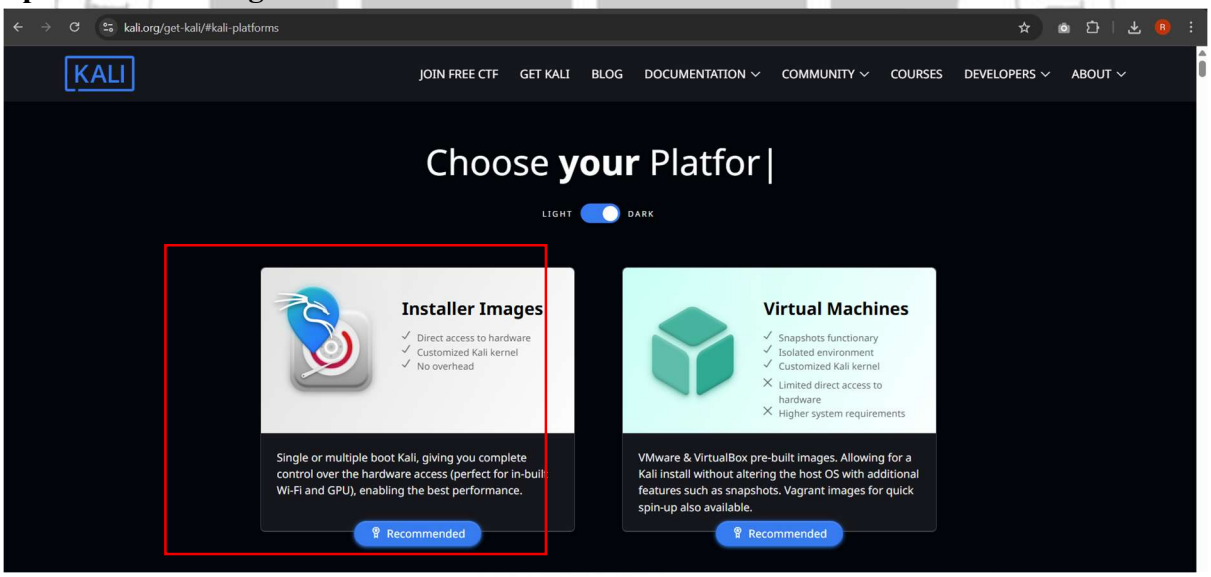
Install Kali Linux on Virtual Box

Step 1: Download & Install Virtual Box

- Go to the official Virtual Box site and download Virtual Box: https://www.virtualbox.org/
- Choose your systems OS.
- We are going to select **Windows hosts**

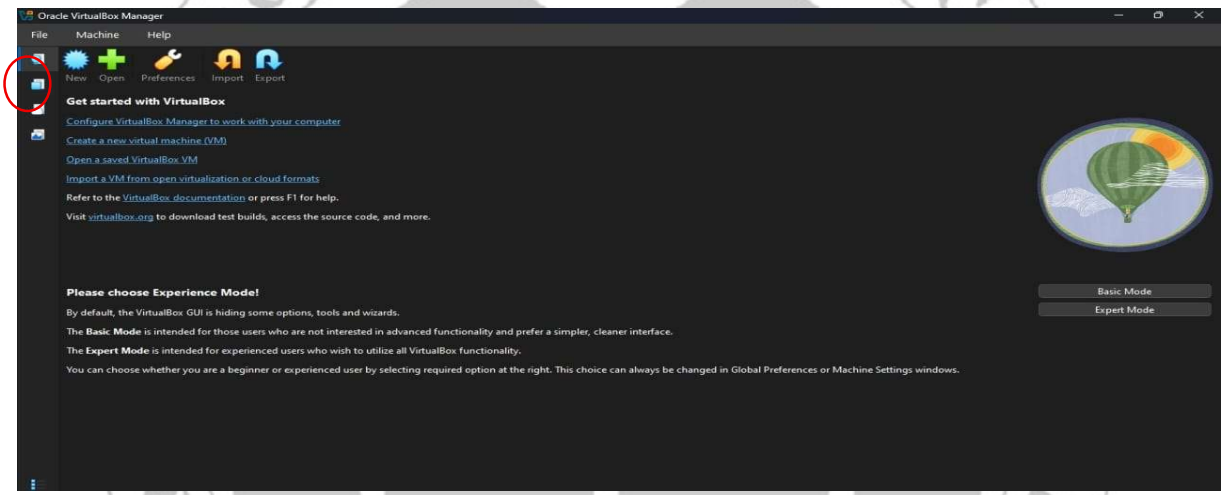
- After clicking, it will starts downloading
- **Installation:**
  Installation process is not complex. It is easy and straightforward. So, after double clicking on the downloaded file, then we have to proceed next easy steps and then it will get installed.

Step 2: Downloading Kali Linux

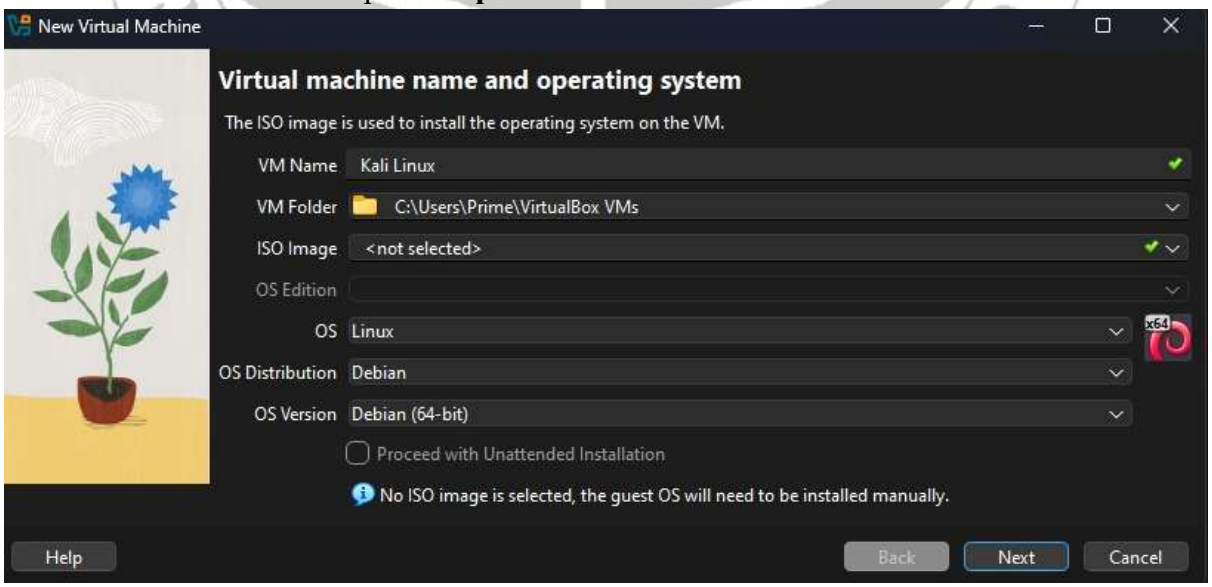


Download Kali Linux from official website: *https://www.kali.org/get-kali/#kali-platforms*
Select any of them:
1.Virtual Machines (Second Option): Easy to install, straight forward but not too customizable as we compared with **Installer Images.**
2.Installer Images (First Option): Little bit more complex than second option but it is Customizable than Virtual Machines
We are choosing Installer Images

- Click on this: After clicking it will starts downloading

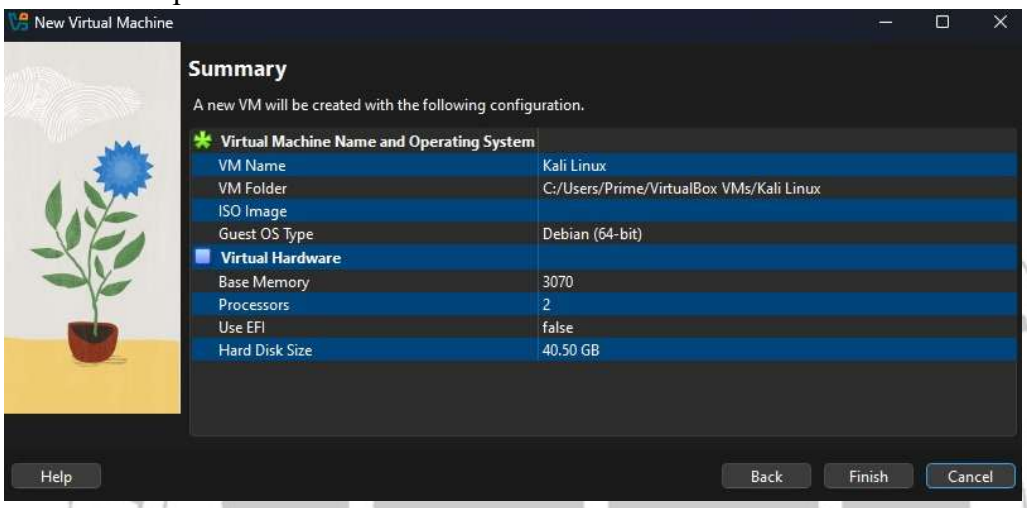


- After download completed **Open Virtual Box** and click on **New**

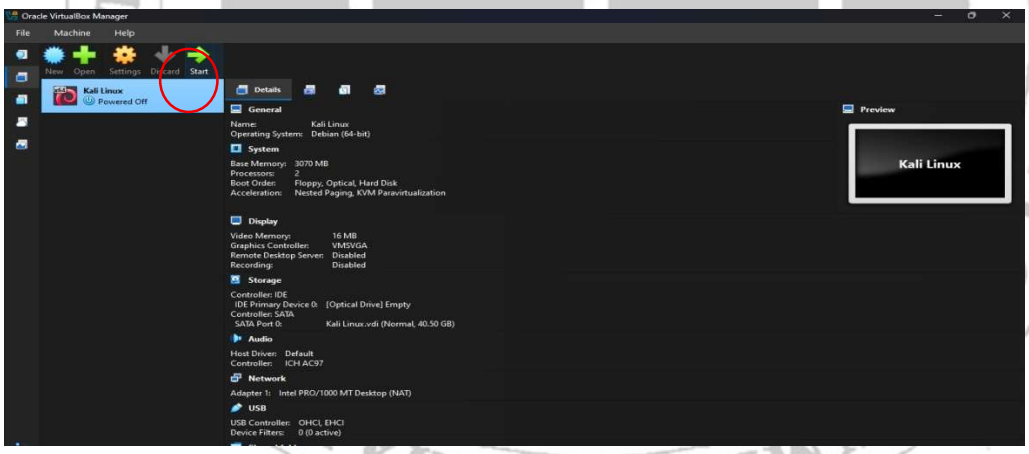


- Give Your Custom VM Name, choose VM Folder or keep as it is, select OS: Linux, OS Distribution: Debian OS Version: Debian(64-bit) and at last press Next.
  Note: *Don't choose ISO Image right now*
- Give proper Memory and CPUs as per your configuration (like if you have 8GB RAM you can give 2GB, 4GB, etc. and if you have 6 Cores you can give 1,2,3, etc.)

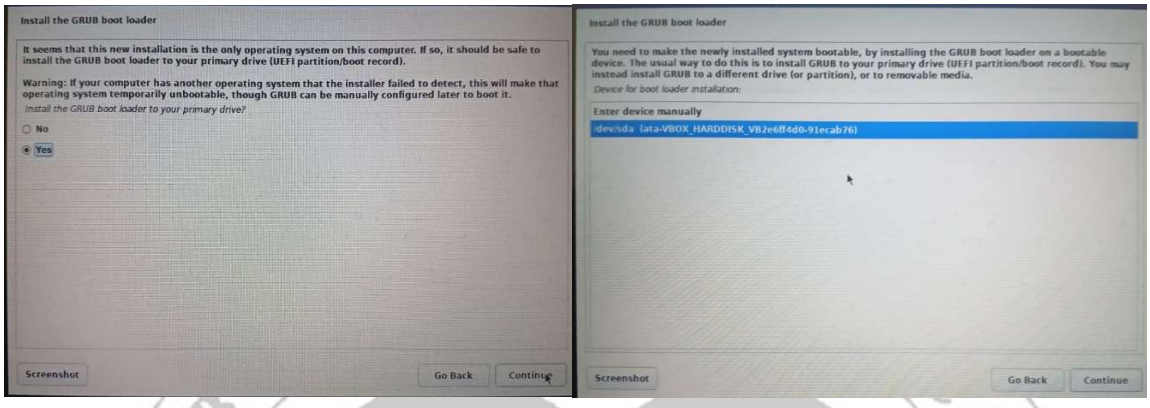
- Give proper size of Disk. (Give minimum 20GB at least)
  Note: *Don't give full configuration.*
- Then press **Next**



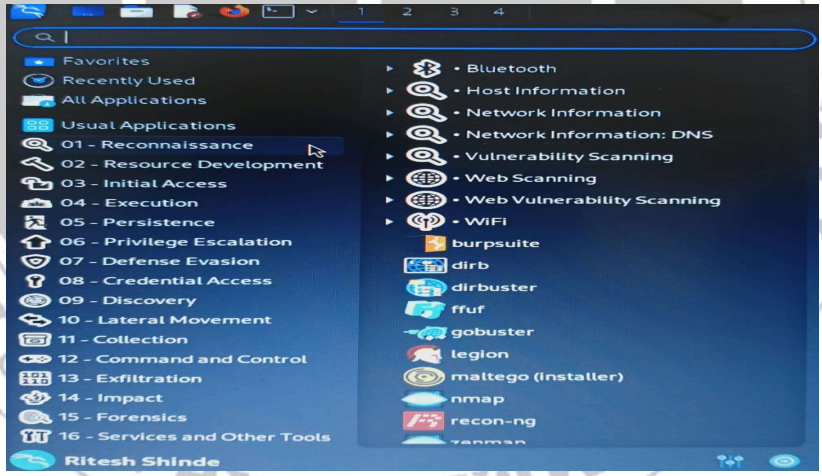
- Confirm and click on **Finish**



- Press **Start**
- Click on **DVD dropdown** and then click on **Others**
- Locate and **open** the downloaded **iso file**
- Then click on **Mount and Retry Boot**
- click on **Graphical Install** within **30** seconds If not clicked within 30 seconds, then speech synthesis will start. If you don't want this then power off your VM and then Restart VM.
- Follow the steps and set up user, username, password and then press continue, it will wait for configuration of clock



- Write the changes to the disk press Yes and then continue
- After pressing continue it will take lot of time for installation…….
- Press Yes on first image and select second option in second image, then click continue
- Finally, the installation is done press Continue for reboot
- After entering the correct username and password, we will move on the HOME SCREEN of Kali Linux.



As we can see, there are no. of pre-installed software and tools are available. So, before starting Run these commands on Terminal Emulator

VII. Resources required

Sr. No.	Name of Resource	Specification	Quantity	Remarks (If any)
1.	Computer System	Computer (i3-i5 preferable RAM>2 GB	As Per Batch Size	
2.	Storage Type	Disk Space >20 GB		
3.	Internet Connectivity	Minimum 10 Mbps stable connection for download		

VIII. Conclusion

……...……

……...……

……...……

IX. Practical Related Questions

Note: Below are a few sample questions for reference. Teachers must design more such questions to ensure the achievement of the identified CO.

1. Why Kali Linux is Used
2. What are features of Kali Linux?
3. What are advantages of kali Linux?

(Space for answers)

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

X. References/Suggestions for further Reading Assessment Scheme

1. https://www.virtualbox.org/
2. https://www.kali.org/get-kali/#kali-platforms

XI. Assessment Scheme

The given performance indicators should serve as a guideline for assessment regarding process and product related marks. Faculty must fill only the table at bottom.

	Performance Indicators	Weightage
	Process related (15 Marks)	**60%**
1	Logic formation	30%
2	Debugging ability	20%
3	Follow ethical practices	10%
	Product related (10 Marks)	**40%**
4	Expected output	10%
5	Timely Submission	15%
6	Answer to sample questions	15%
	Total: 25 Marks	**100%**

Marks obtained			**Dated Sign of Teacher**
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No 11. * Use Nmap utility to perform following tasks:

a. **Install Nmap on Linux or Windows OS.**
b. **Detect which devices are live on your local network. Identify the services and their versions running on a particular host.**
c. **Detect the operating system of a target host.**
d. **Perform a port scan on a specific set of ports.**
e. **Perform an aggressive scan to gather as much information as possible about a target host.**
f. **Use Nmap's scripting engine to search for vulnerabilities in a target system.**

I. Practical Significance

The practical use of Nmap is to give network administrator, security professional and ethical hackers a deep, actionable understanding of a network's infrastructure. This insight is vital for both proactive defense and reactive troubleshooting which transforming a network's complexity into a manageable "map".

II. Industry / Employer Expected outcome(s)

Apply Digital Forensic methodology to carry out investigations and penetration tests.

III. Course Level Learning outcome(s)

CO4 - Identify various types of cyber-attacks.

IV. Laboratory Learning outcome(s)

LLO 11.1 Use nmap utility for scanning.

V. Relevant Affective Domain related Outcome(s)

Respects the limitations and ethical boundaries of powerful scanning tools (like Nmap) while using them for legitimate testing purposes.

VI. Relevant Theoretical Background

Nmap is a network tool used to discover devices, open ports, and services on a network for management and security purposes. Nmap (Network Mapper) is a free and open-source tool used to discover devices on a network used to analyse their security. It is commonly used by network administrator and security professional to see which hosts, services and vulnerabilities are active, run, might exist respectively.

Key Uses of Nmap:

Network Discovery – Find devices (computers, servers, routers) on a network.

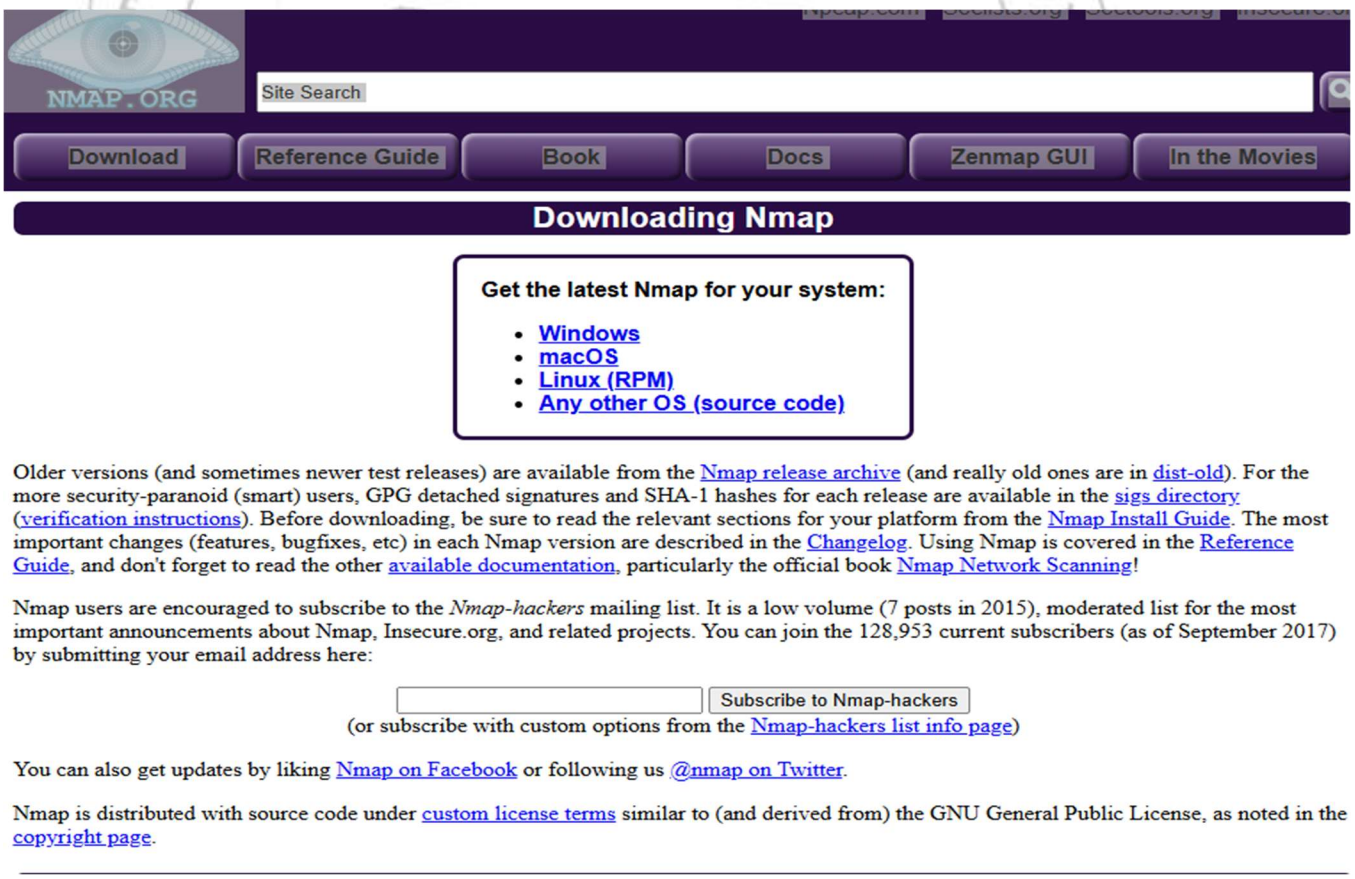
Port Scanning – Check which ports are open on a device.
Service & Version Detection – Identify what software and version is running on open ports.
Operating System Detection – Guess the OS of the target device.
Security Auditing – Detect potential vulnerabilities using scripts.

a. Install Nmap on Windows OS

(Note: In kali Linux, there is no need to install Nmap. Because Nmap and many more tools come pre-installed in kali Linux.)

For Windows: Official installer

Download the Windows installer from the official site: nmap.org (file looks like nmap-<version>-setup.exe).



1. Run the installer and follow the GUI prompts.
   You can install: Nmap (command line) and Zenmap (graphical UI) (optional)
2. Open PowerShell or Command Prompt and verify: *nmap –version*

b. Detect which devices are live on your local network. Identify the services and their versions running on a particular host

To find live devices on your local network with Nmap on Windows, open Command Prompt or PowerShell as an administrator and run (replace with your network's IP range).

nmap -sn 192.168.1.0/24

This command performs a "ping scan" that uses ARP to discover active hosts on the local subnet and lists their IP addresses without performing a full port scan.

Step 1: Find your network's IP range

1. Open Command Prompt or PowerShell.
2. Type `ipconfig` and press Enter.
3. Find the "IPv4 Address" and "Subnet Mask" for your active network connection.
4. Your network range is typically the first three sets of numbers from the IPv4 address followed by 0/24.

Eg. if your IP is 192.168.1.100 and your subnet mask is 255.255.255.0, your network range is 192.168.1.0/24.

Step 2: Run the Nmap command

Open Command Prompt or PowerShell as an administrator>>Type the following command (replacing the IP range with your own)

nmap -sn 192.168.1.0/24

-sn tells Nmap to perform a ping scan (host discovery) without performing a port scan.

For local networks, this command uses ARP requests, which is faster and more reliable than ICMP echo requests.

Step 3: Analyze the output

Nmap will list all the devices that responded to the scan with their IP addresses, often along with their MAC addresses. The output will show you which IPs are "up" or active on your network.

c. Service & version detection on a selected host:

To perform service and version detection on a selected host using Nmap in Windows, follow these steps:

Step1: Open Command Prompt or PowerShell

Step2: Navigate to Nmap Directory (if necessary): If Nmap is not in your system's PATH, navigate to the directory where Nmap is installed (e.g., cd "C:\Program Files (x86)\Nmap").

Step3: Execute the Nmap command

Use the -sV flag to enable service version detection.

Syntax:

nmap -sV <target_host>

eg.nmap -sV 192.168.1.100

Step 4: For more comprehensive scanning, OS detection, version detection, script scanning, and

traceroute use the -A flag

nmap -A <target_host>

eg. nmap -A 192.168.1.100

Understanding the Output: After running the scan, Nmap will provide output detailing the open ports, the services running on those ports, and their detected versions. The output will typically show:

Port Number/Protocol: The port number and the protocol (TCP/UDP) being used.

State: Whether the port is open, closed, or filtered.

Service: The name of the service identified (e.g., http, ftp, ssh).

Version: The specific version of the service detected, if available.

Note: The accuracy of version detection can vary depending on the service and its configuration. Some services may not reveal their versions, or Nmap might provide a "soft match" with a question mark indicating uncertainty.

d. Perform a port scan on a specific set of ports

You can perform a port scan on a specific set of ports in Windows using either the built-in netstat command to check for listening ports on the local machine or by using tool Nmap to scan both local and remote machines.
To check local ports, open Command Prompt as an administrator and use

netstat -an | find "<port number>".

For example: To check port 8080: netstat -an | find "8080"

(for local and remote machines)

1. **Scan a specific port:** To scan a single port, use the `-p` flag:

   nmap -p 80 <target IP>

2. **Scan a range of ports:** To scan a range of ports, separate the start and end ports with a hyphen:

   nmap -p 1-50 <target IP>

3. **Scan a list of ports:** To scan a list of specific ports, separate them with commas

   nmap -p 80,443,22 <target IP>

4. **Scan all ports:** To scan all 65,535 ports, use -p-

nmap -p- <target IP>

Nmap gives detailed info (state, service, version, OS detection, etc.) if you add flags like:

nmap -sV -p 22,80 192.168.1.10

Important Notes

Always make sure you have **permission** to scan the target host. Unauthorized scanning can be illegal.

If scanning localhost, use 127.0.0.1 or your machine's IP.

e. Perform an aggressive scan to gather as much information as possible about a target host

An **aggressive scan** provides far better information than a regular scan. It is performed by using the

-A option which enables:

1. OS detection (-O)
2. Version detection (-sV)
3. Script scanning (-sC)
4. Traceroute (--traceroute)

Aggressive scans send out more probes than a regular scan, and are more likely to be detected during a security audit.

Syntax

nmap -A <target IP Address >

nmap -A 192.168.1.101

Example

The following example runs an aggressive scan on the site scanme.nmap.org

nmap –A scanme.nmap.org

Additional Useful Options

To make the scan faster and more comprehensive use:

1. **Timing Template (**-T4 or -T5**):** To Adjusts the scan speed.

   -T4 is considered an aggressive timing template.

   -T5 is even faster but can be less reliable and more easily detected.

   nmap -A -T4 <Target IP Address>

2. **Scan All Ports (** - p-): By default, Nmap scans the 1000 most common ports. The -p- option scans all 65535 TCP ports.

   nmap -A -T4 -p- <Target IP Address>

3. **Include UDP Scan (** - sU**):** To scan for open UDP ports

   You can add -sU (or scan all TCP and UDP ports with - sS -sU -p-).

4. **Verbose Output** (-v): Provides more detailed, real-time information during the scan process.
   nmap -A -T4 -v <Target IP Address>

f. Use Nmap's scripting engine to search for vulnerabilities in a target system

In Windows:

Nmap comes with a variety of pre-installed scripts. The most common category for vulnerability checks is `vuln` category.

OR

Powerful third-party scripts like vulners.nse or vulscan.nse.

1. Update the Script Database

It's a good practice to update the script database if you have added new scripts:

nmap --script-updatedb

2. Run Built-in Vulnerability Scripts

The following command tells Nmap to perform a service version detection (-sV) and run all scripts in the vuln category against the target IP address:

nmap -sV --script vuln <target_IP_address>

eg. nmap -sV --script vuln 192.168.1.100

-sV: Enables version detection, which is necessary for many scripts to identify specific software versions and match them against known vulnerabilities.

--script vuln: Specifies that Nmap should run all scripts belonging to the "vuln" category.

NSE has categories and many scripts. Only run vulnerability scripts (vuln) with permission and in controlled environments.

VII. Resources required

Sr. No.	Name of Resource	Specification	Quantity	Remarks (If any)
1.	Computer System	Computer (i3-i5 preferable RAM>2 GB	As Per Batch Size	
2.	Storage Type	Disk Space >20 GB		
3.	Internet Connectivity	Minimum 10 Mbps stable connection for download		

VIII. Conclusion

……...……

……...……

……...……

IX. Practical Related Questions

Note: Below are a few sample questions for reference. Teachers must design more such questions to ensure the achievement of the identified CO.

1. What is Nmap and why it is used?
2. What are the ethical considerations when using Nmap?
3. How can you use Nmap to detect services and their versions?
4. A server is not reachable. How can Nmap help troubleshoot this issue?

(Space for answers)

.....

.....

.....

.....

.....

.....

.....

.....

X. References/Suggestions for further Reading Assessment Scheme

1. https://www.virtualbox.org/
2. https://www.kali.org/get-kali/#kali-platforms

XI. Assessment Scheme

The given performance indicators should serve as a guideline for assessment regarding process and product related marks. Faculty must fill only the table at bottom.

	Performance Indicators	Weightage
	Process related (15 Marks)	**60%**
1	Logic formation	30%
2	Debugging ability	20%
3	Follow ethical practices	10%
	Product related (10 Marks)	**40%**
4	Expected output	10%
5	Timely Submission	15%
6	Answer to sample questions	15%
	Total: 25 Marks	**100%**

Marks obtained			Dated Sign of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No. 12: Establish DoS attack using TCP/ICMP flooding:

a. **Ping continuously a particular machine at a time from different machines and observe the machine behavior on Network.**
b. **Write shell script for continuously flooding a Machine with ping and observe the machine behavior on Network.**

I. Practical Significance

TCP and ICMP floods remain important because they're simple, low-cost ways for attackers to deny service, cause outages, impose costs, and test or probe defenses while defenders need pragmatic detection and layered mitigation to reduce impact.

II. Industry / Employer Expected outcome(s)

Apply Digital Forensic methodology to carry out investigations and penetration tests.

III. Course Level Learning outcome(s)

CO4 - Identify various types of cyber-attacks.

IV. Laboratory Learning outcome(s)

LLO 12.1 Establish DoS attack using TCP/ICMP flooding

V. Relevant Affective Domain related Outcome(s)

Appreciates the need for robust network defenses by experiencing the disruptive impact of DoS attack simulation.

VI. Relevant Theoretical Background

A **Denial-of-Service (DoS) attack** is a type of cyber-attack in which one or more attackers attempt to make a target machine or network resource unavailable to its intended users.

ICMP Flood (Ping Flood)

An ICMP Flood or Ping Flood is a network attack in which the attacker sends a large number of ICMP Echo Request (ping) packets to a target system. The target must respond with ICMP Echo Reply packets for each request, consuming both network bandwidth and system processing power. This can lead to slow responses, high latency, or even complete network unavailability

TCP Flood

A **TCP Flood attack** targets the **Transmission Control Protocol (TCP)** by sending a large volume of TCP packets often connection requests (SYN packets) to the target system. This causes the system to allocate resources for each incoming connection, eventually exhausting available connection

tables**,** CPU power**, and** memory, As a result legitimate users may experience failed or delayed TCP connections

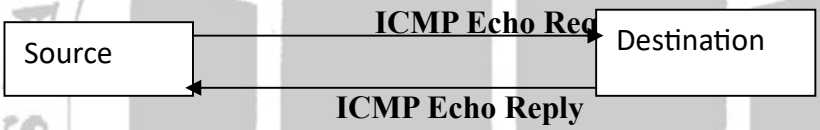
Types of TCP Floods:

- **SYN Flood:** Sends many TCP SYN packets to exhaust connection queues.
- **ACK/PSH Flood:** Sends large volumes of packets that mimic active connections.
- **Connection-Exhaustion Flood:** Creates multiple incomplete connections to overload the server.

a. **Ping continuously a particular machine at a time from different machines and observe the machine behavior on Network**

Ping is a basic network utility used to test the reachability of a host on an IP network and measure the **round-trip time (RTT)** of messages sent from the source to the destination

Detect which devices are live on your local network. Identify the services and their versions running on a particular host



The tool then measures response time and packet loss to evaluate network health.

When to Use Ping:

- To verify if a host is reachable.
- To measure latency and detect packet loss.
- For initial troubleshooting before deeper tools like **traceroute** or **tcpdump.**

Example

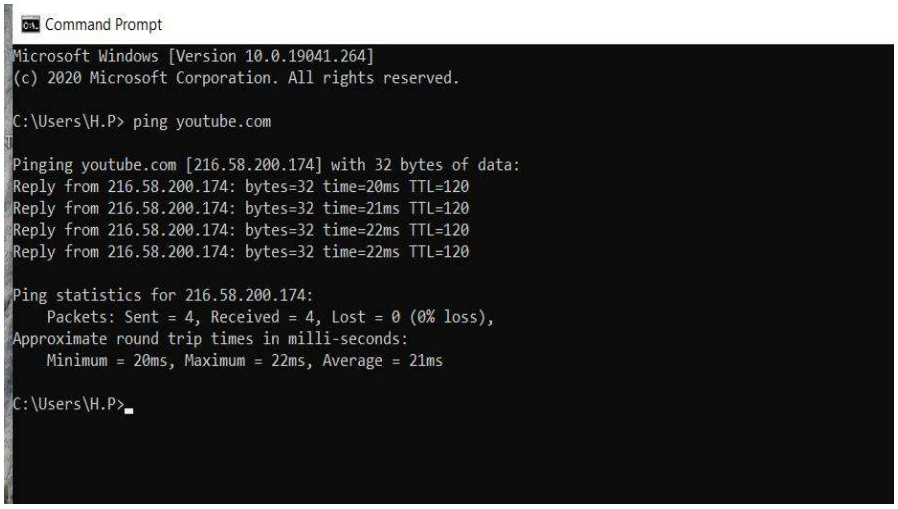
If you would like to test the network connection between two computers on an on-going basis, the "**continuous ping**" option is available.

Step 1: Open the Windows command prompt or windows + R and enter the command CMD.

Step 2: Enter the command line *ping* with the *-t* option and any address and confirm by clicking.

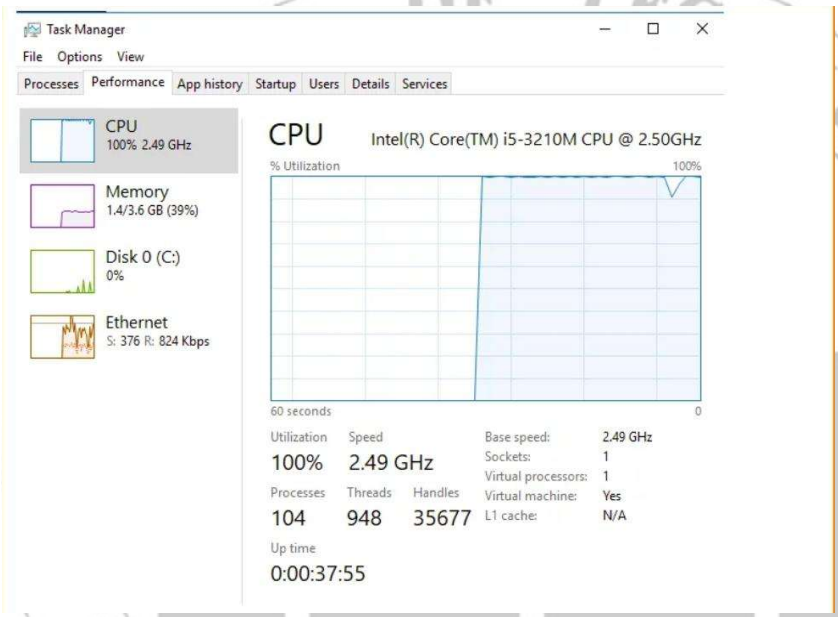
ping -t youtube.com

Windows runs the command line program as a continuous ping in an endless loop



Step 3: Observe Target Machine Behavior On the target machine:

1. Open Task Manager → Performance tab → Network
2. Watch for increased network usage or latency
3. Try normal browsing or file transfer .It may become slower
4. we can also check network statistics with: ping 8.8.8.8



If you stop the ping, the program displays a statistical summary (ping statistics) at its conclusion.

b. Write shell script for continuously flooding a Machine with ping and observe the machine behaviour on Network

```
#!/usr/bin/env bash
# safe-ping-monitor.sh
TARGET="8.8.8.8"      # change to your authorized target
INTERVAL=10           # seconds between pings
LOSS_THRESHOLD=50     # percent
RTT_THRESHOLD=200     # ms
while true;
do
 # single ping with 1 second timeout
 out=$(ping -c 5 -W 1 $TARGET)
 # parse packet loss and average rtt
 loss=$(echo "$out" | awk -F', ' '/packet loss/ {print $3}' | sed 's/% packet loss//')
 rtt=$(echo "$out" | awk -F'/' '/rtt/ {print $5}')
 loss=${loss:-100}
 rtt=${rtt:-9999}
 timestamp=$(date -Iseconds)
 echo "$timestamp target=$TARGET loss=${loss}% rtt=${rtt}ms"
```

```
  if (( ${loss%.*} >= LOSS_THRESHOLD )); then
    echo "ALERT: packet loss ${loss}% for $TARGET" | tee /tmp/ping_alert.log
    # optionally send email / webhook
  fi
  if (( ${rtt%.*} >= RTT_THRESHOLD )); then
    echo "ALERT: high RTT ${rtt}ms for $TARGET" | tee -a /tmp/ping_alert.log
  fi
  sleep $INTERVAL
done
```

VII. Resources required

Sr. No.	Name of Resource	Specification	Quantity	Remarks (If any)
1.	Computer System	Computer (i3-i5 preferable RAM>2 GB	As Per Batch Size	
2.	Storage Type	Disk Space >20 GB		
3.	Internet Connectivity	Minimum 10 Mbps stable connection for download		

VIII. Conclusion

……

……

……

IX. Practical Related Questions

Note: Below are a few sample questions for reference. Teachers must design more such questions to ensure the achievement of the identified CO.

1. What is a DoS / DDoS attack?
2. How does a TCP Flood exploit this?
3. Why is it illegal to perform TCP floods?

(Space for answers)

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

X. References/Suggestions for further Reading Assessment Scheme

1. https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/
2. https://en.wikipedia.org/wiki/Denial-of-service_attack

XI. Assessment Scheme

Performance Indicators		Weightage
Process related (15 Marks)		**60%**
1	Logic formation	30%
2	Debugging ability	20%
3	Follow ethical practices	10%
Product related (10 Marks)		**40%**
4	Expected output	10%
5	Timely Submission	15%
6	Answer to sample questions	15%
	Total: 25 Marks	**100%**

Marks obtained			Dated Sign of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No.13: * Capture Network traffic using Wireshark tool

a. **Install Wireshark tool on Windows/Kali Linux.**
b. **Use Wireshark tool to capture network traffic and to understand three-way handshaking concept/Analyze the packet.**
c. **Examine HTTP, FTP, or other protocols for evidence of cybercrime.**

I. Practical Significance

Wireshark software widely used to analyze data packets in a network. It is completely free and open source. This packet analyzer is used for a variety of purposes like troubleshooting networks, understanding communication between two systems, developing new protocols, etc.

This software is written in C and C++. Wireshark is a cross-platform software, it can be run on Linux, windows, mac, and any other operating system.

II. Industry / Employer Expected outcome(s)

The aim of this course is to help the students to attain the following industry identified outcomes through various teaching learning experiences: Apply Digital Forensic methodology to carry out investigations and penetration tests.

III. Course Level Learning outcome(s)

CO5 - Apply Tools and Techniques for Ethical Hacking.

IV. Laboratory Learning outcome(s)

LLO 13.1 Use Wireshark tool to analyze network traffic.

V. Relevant Affective Domain related Outcome(s)

Subscribes to the belief that detailed packet analysis (via Wireshark) is crucial for understanding and diagnosing network security events.

VI. Relevant Theoretical Background

Wireshark is a **network protocol analyzer** used to capture, inspect, and analyze data packets traversing a network in real time. It provides a graphical interface for examining network traffic, enabling users to view detailed information about the protocols, headers, and payloads of packets. It is widely used in fields such as network administration, cybersecurity, and academic research for troubleshooting, monitoring, and learning about network communications.

Install Wireshark tool on Windows/Kali Linux

Follow the below steps to install Wireshark on Windows:

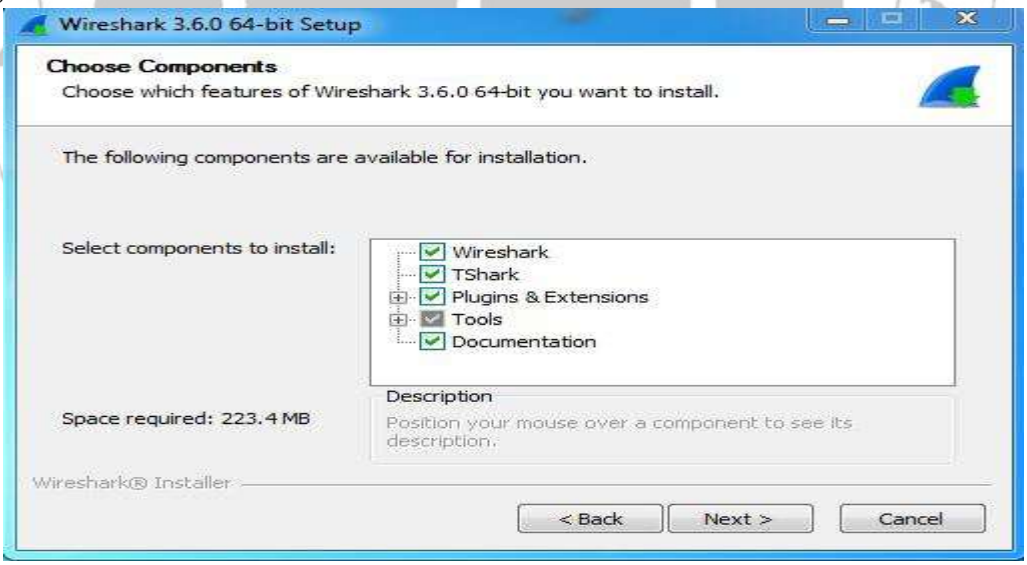
Step 1: Visit the official Wireshark website using any web browser.

Step 2: Click on Download, a new webpage will open with different installers of Wireshark.

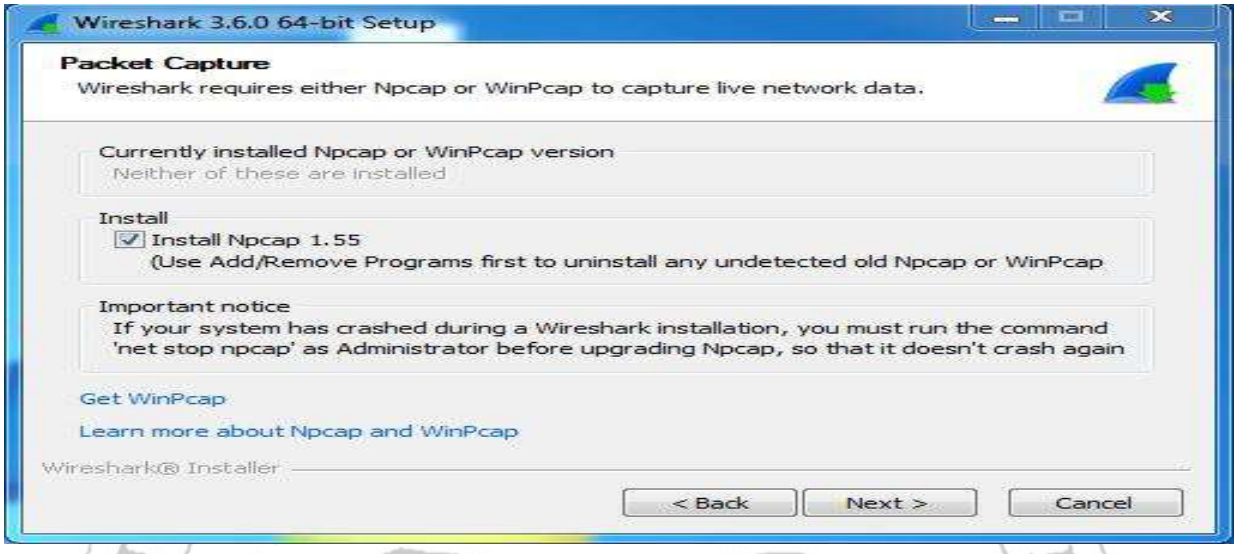
Step 3: Downloading of the executable file will start shortly. It is a small 73.69 MB file that will take some time.

Step 4: Now check for the executable file in downloads in your system and run it.
Step 5: It will prompt confirmation to make changes to your system. Click on Yes.
Step 6: Setup screen will appear, click on Next.

Step 7: The next screen will be of License Agreement, click on Noted.
Step 8: This screen is for choosing components, all components are already marked so don't change anything just click on the Next button.



Step 9: This screen is of choosing shortcuts like start menu or desktop icon along with file extensions which can be intercepted by Wireshark, tick all boxes and click on Next button.
Step 10: The next screen will be of installing location so choose the drive which will have sufficient memory space for installation. It needed only a memory space of 223.4 MB.
Step 11: Next screen has an option to install Npcap which is used with Wireshark to capture packets *pcap* means packet capture so the install option is already checked don't change anything and click the next button.



Step 12: Next screen is about USB network capturing so it is one's choice to use it or not, click on Install.

Step 13: After this installation process will start.

Step 14: This installation will prompt for Npcap installation as already checked so the license agreement of Npcap will appear to click on the *I Agree* button.

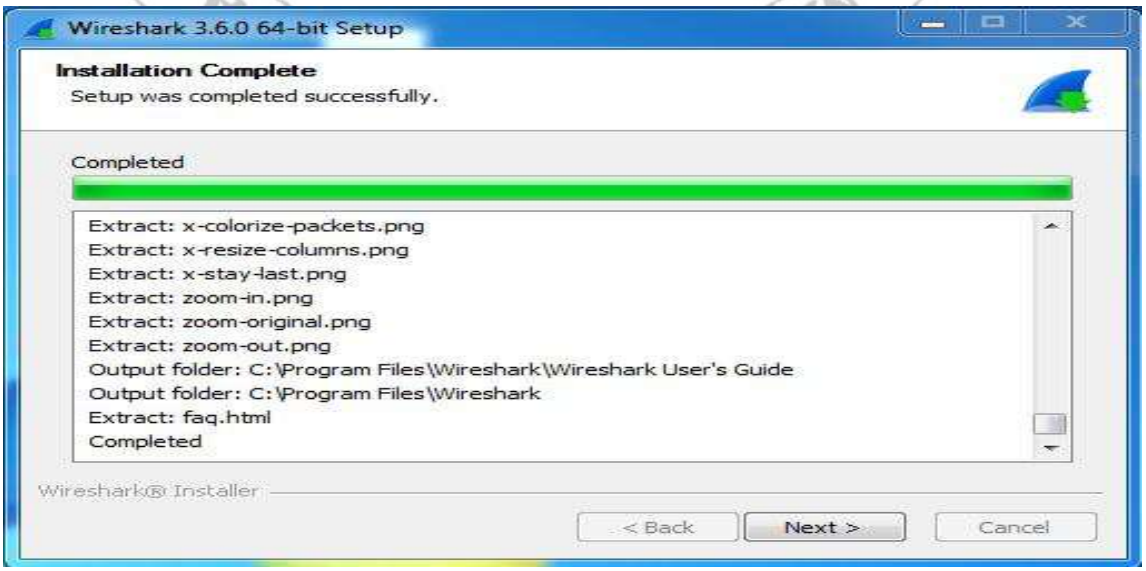
Step 15: Next screen is about different installing options of *npcap*, don't do anything click on Install.

Step 16: After this installation process will start which will take only a minute.

Step 17: After this installation process will complete click on the Next button.

Step 18: Click on Finish after the installation process is complete.

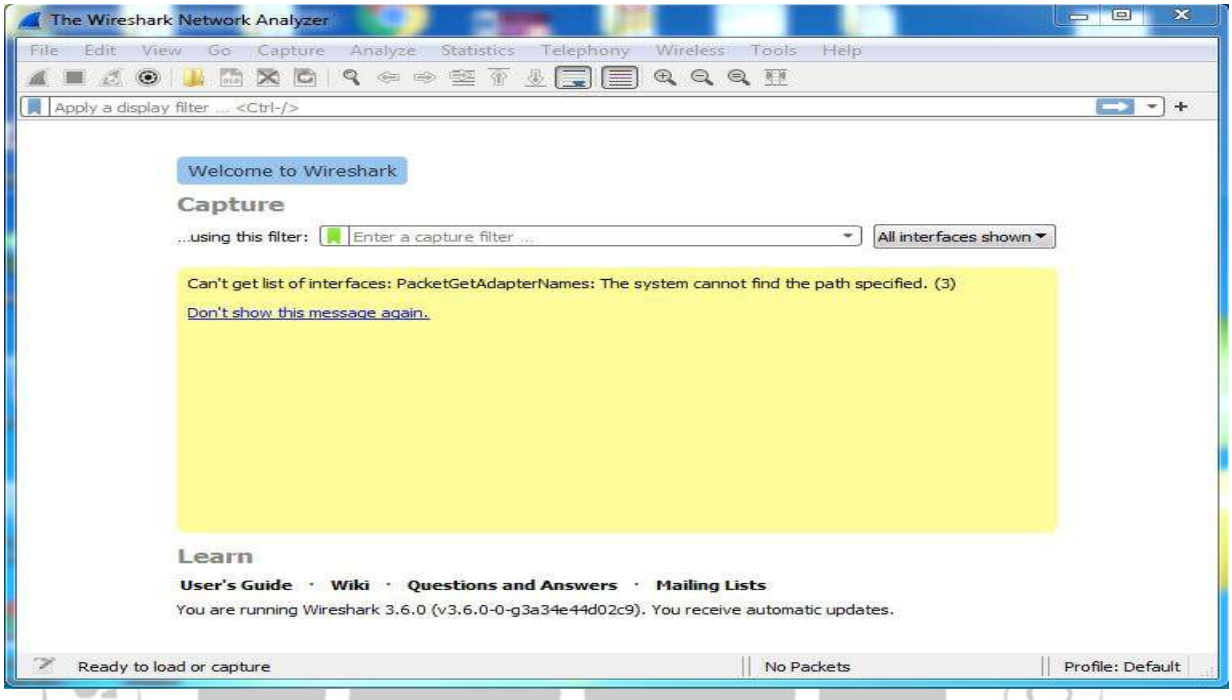
Step 19: After this installation process of Wireshark will complete click on the Next button.



Step 20: Click on Finish after the installation process of Wireshark is complete.

Wireshark is successfully installed on the system and an icon is created on the desktop.

Now run the software and see the interface.



At this point, you have successfully installed Wireshark on your windows system.

b. Use Wireshark tool to capture network traffic and to understand three-way handshaking concept/Analyze the packet

Information Technology (IT) and Networking are essential elements in cybersecurity. IT is effective in software development, data management, and system security. Network Communication enables data transfer by providing the connection between devices. TCP/IP protocol basis of the Internet on this infrastructure, communication protocols such as HTTP Wireshark Tool helps to observe network traffic and detect possible security breaches.

Importance and Working Principle of TCP 3-Way Handshake:

The TCP 3-way handshake protocol is a series of processes used to initiate reliable communication between computers before establishing a connection.

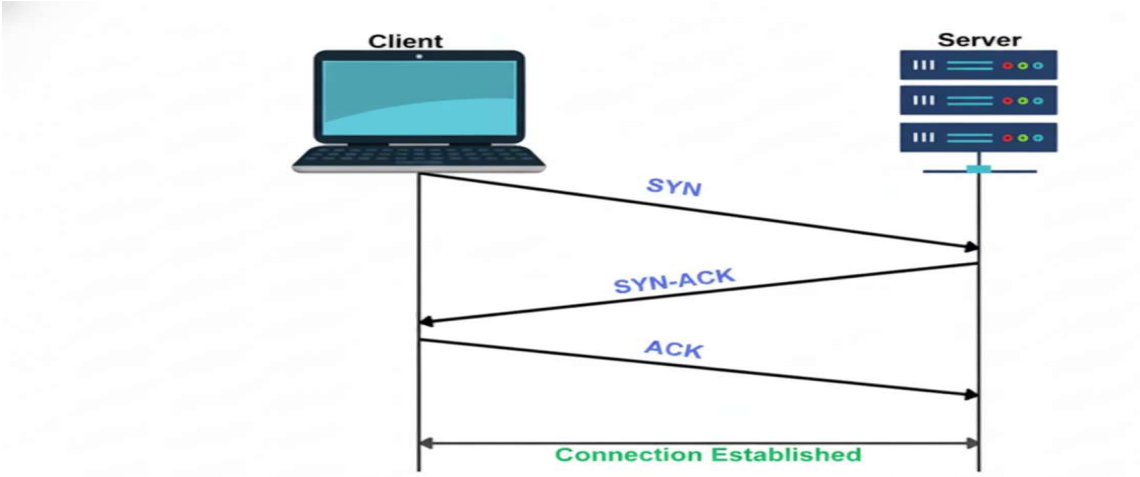
This process consists of Three steps:

Step 1 (SYN): client computer sends a SYN (synchronize) packet to the target server.

This packet represents a request to communicate, and a connection request is transmitted to the server to which the client wants to connect.

Step 2 (SYN-ACK): The server responds with a SYN-ACK (synchronize-acknowledge) packet to confirm that it received the client's request. This packet indicates that it has received the request and is ready for communication.

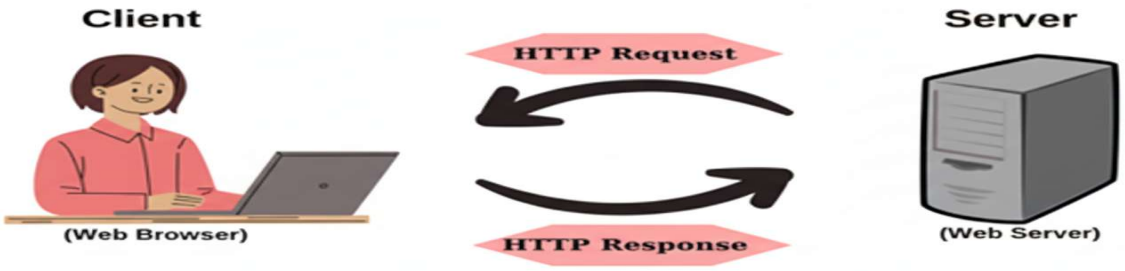
Step 3 (ACK): client computer sends an ACK (acknowledge) packet to verify the server's response and initiate communication. This packet confirms that the server has received its response and communication officially begins.



Once the 3-way handshake is completed, a secure and mutual communication channel is opened. This process verifies that both parties are ready for communication and provides a reliable connection for exchanging data.

When communication ends, the connection is closed with a similar step. This process supports the TCP protocol's ability to provide reliable and regular data communication.

HTTP Protocol and Working Principle:



HTTP (Hypertext Transfer Protocol) is a communication protocol used to transfer documents between web browsers and servers.

This text-based protocol basically follows the client-server model

Client: Usually a web browser. Sends an HTTP request to the server to access a specific resource (web page, image, etc.).

Server: Receives the client's request and returns an appropriate response to the request.

The HTTP request is usually specified with a URL and comes with the request method (GET, POST, PUT, DELETE, etc.).

Once the server receives the request, it takes appropriate actions and responds with an HTTP response. This response contains the requested resource or processing result to the client.

It is based on the TCP/IP protocol family that enables data communication on the Internet and communicates over this infrastructure. As in every field of technology, there are improved and updated versions of HTTP.

Frequently Used HTTP Headers:

HTTP Request Header:

1.Host: Specifies the server name.

2.User-Agent: Contains information on the client program (browser information).

3.Accept: Specifies the media types the client can accept.

4.Content-Type: Specifies the type of data being sent (for example, JSON, XML).

5.Authorization: Contains the authentication information requested from the client by the server (for example, username and password).

HTTP Response Header:

1.Status: Indicates the status of the request (for example, 404 Not Found).

2. Content-Type: Specifies the type of data sent by the server.

3. Cache-Control: Controls caching settings.

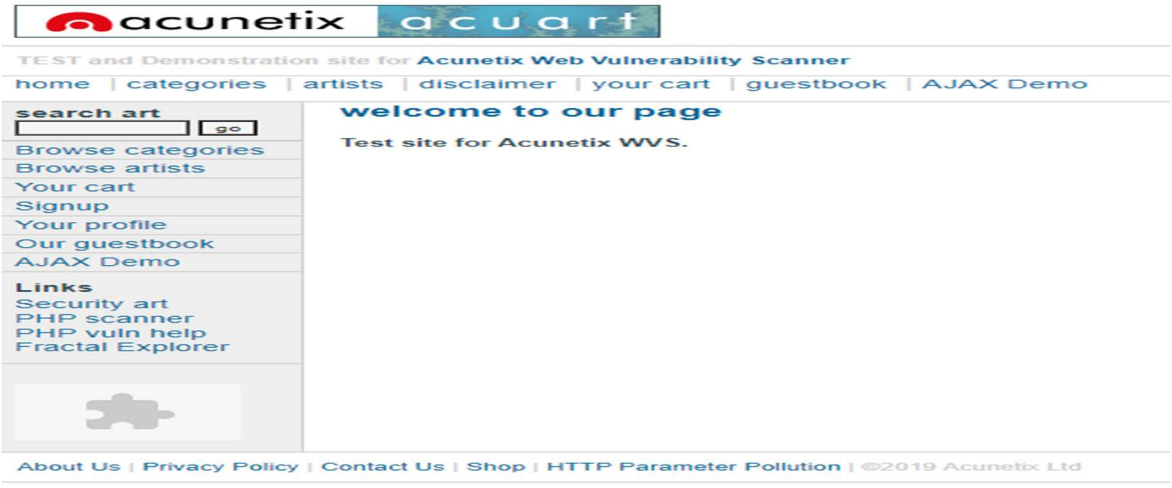
4. Location: Specifies the new location in redirect situations.

5. Server: Contains software or server information running on the server side.

Capturing HTTP Traffic and Viewing Its Content with Wireshark:

Wireshark is a popular network protocol analysis tool used to capture, inspect, and analyze network traffic. This software listens and records data packets coming from different network interfaces and displays the contents of these packets in detail. Supporting various network protocols, Wireshark can capture packets of a wide range of protocols such as TCP/IP, HTTP, DNS, and DHCP. Each of these packets represents the data carried between the devices involved in the communication and the operations of the communication. Wireshark can be used for a variety of purposes, such as diagnosing network problems, detecting security threats, analyzing network performance, or finding errors in communications. Wireshark is the tool preferred by network administrators, security experts, network engineers, and many technology professionals because it provides an in-depth understanding of network communications and data traffic and contributes greatly to troubleshooting processes. Now let's make a simple application example where we capture HTTP packets with Wireshark:

1. First, turn on your Wireshark, and start packet capture.
2. Chose the site "http://testphp.vulnweb.com/".



.

3. Ping this site to find out its IP address.

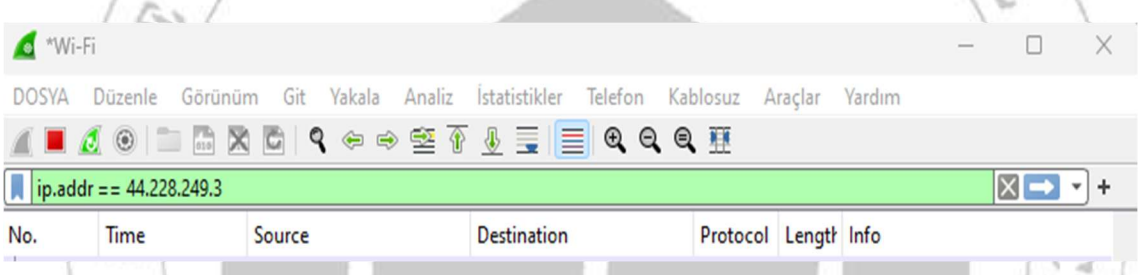
```
C:\Program Files (x86)\VMware\VMware Workstation\bin>ping testphp.vulnweb.com

Pinging testphp.vulnweb.com [44.228.249.3] with 32 bytes of data:
Reply from 44.228.249.3: bytes=32 time=216ms TTL=50
Reply from 44.228.249.3: bytes=32 time=227ms TTL=50
Reply from 44.228.249.3: bytes=32 time=224ms TTL=50
Reply from 44.228.249.3: bytes=32 time=219ms TTL=50

Ping statistics for 44.228.249.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 216ms, Maximum = 227ms, Average = 221ms
```

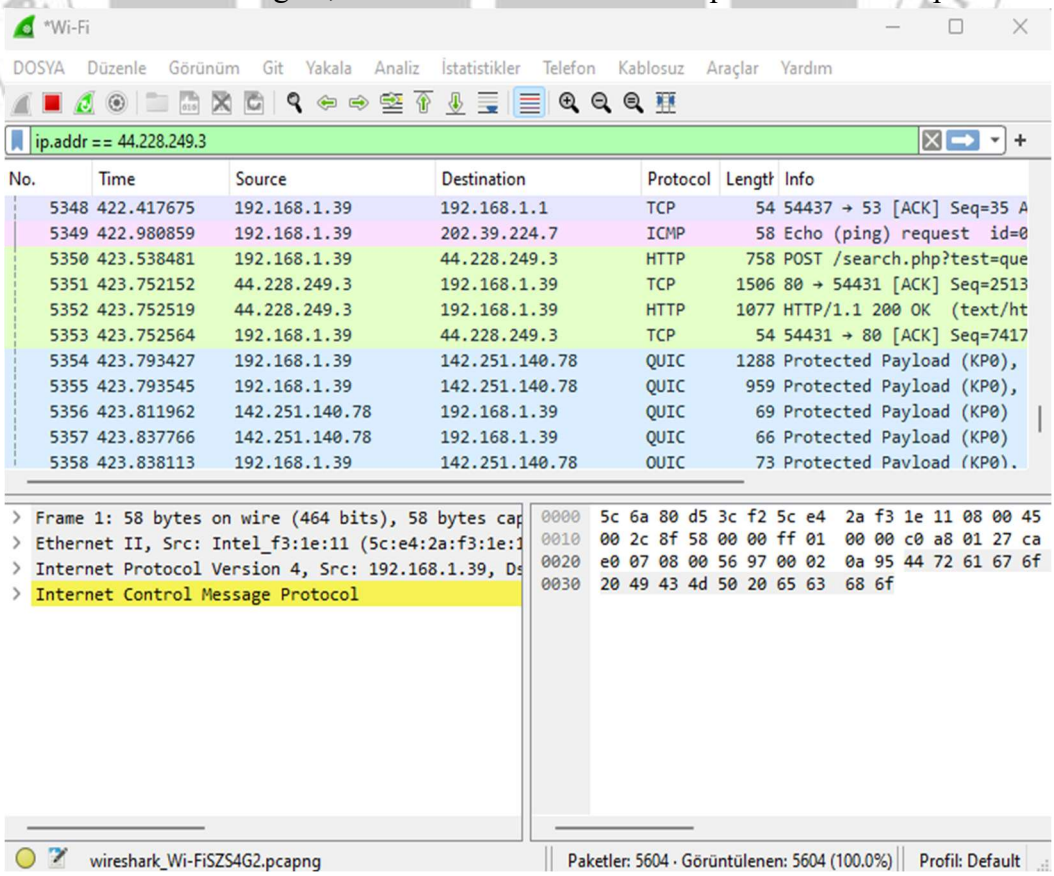
IP address = 44.228.2499.3

4. entered the IP address into the filtering section. Then examine the packets on this IP address.



5. type anything in the “Search” box to observe the HTTP protocol.

6. When Wireshark turns on again, we can observe that it has captured the HTTP packet.



c. Examine HTTP, FTP, or other protocols for evidence of cybercrime

STEP 1: Open Wireshark

1. Click Start → Type Wireshark → Open it.
2. You'll see a list of network interfaces (Wi-Fi, Ethernet, etc.)

STEP 2: Start capturing

Click the interface name (e.g., Wi-Fi) to begin capturing.

STEP 3: Generate simple HTTP

1. Open Command Prompt (Windows)
2. Run: curl http://example.com

STEP 4: Stop capturing

Click the red square Stop button in Wireshark (top left).

You now have captured packets to inspect.

STEP 5: Investigate for suspicious activity

Look for signs of cybercrime: exposed credentials, file transfers, brute-force attempts, or connections to unknown hosts.

A. Inspect HTTP traffic

1. In the filter bar type: http and press Enter now only HTTP packets are shown.
2. Click a packet. In the middle pane expand: Hypertext Transfer Protocol
3. Look for fields like:

GET / or POST /login
Host: (server)
User-Agent: (client info)
Authorization: (possible credentials)

Suspicious signs: Authorization: Basic ... → may include base64-encoded username:password (decode to check).

Repeated POST /login requests → possible brute-force.

Content-Disposition: form-data; name="file" or large POST bodies → file upload (possible data exfiltration).

Right-click a packet → Follow → HTTP Stream to view the full client-server conversation in readable text

VII. Resources required

Sr. No.	Name of Resource	Specification	Quantity	Remarks (If any)
1.	Computer System	Computer (i3-i5 preferable RAM>2 GB	As Per Batch Size	
2.	Storage Type	Disk Space >20 GB		
3.	Internet Connectivity	Minimum 10 Mbps stable connection for download		

VIII. Conclusion

……

……

……

IX. Practical Related Questions

Note: Below are a few sample questions for reference. Teachers must design more such questions to ensure the achievement of the identified CO.

1. Describe the steps to begin a capture on an interface.
2. Describe the process and file format (e.g., .pcap or .pcapng).
3. What is “Follow TCP Stream” used for?

(Space for answers)

.....

.....

.....

.....

.....

.....

.....

.....

.....

X. References/Suggestions for further Reading Assessment Scheme

1. https://www.wireshark.org/
2. https://www.varonis.com/blog/how-to-use-wireshark

XI. Assessment Scheme

The given performance indicators should serve as a guideline for assessment regarding process and product related marks. Faculty must fill only the table at bottom.

	Performance Indicators	Weightage
	Process related (15 Marks)	**60%**
1	Logic formation	30%
2	Debugging ability	20%
3	Follow ethical practices	10%
	Product related (10 Marks)	**40%**
4	Expected output	10%
5	Timely Submission	15%
6	Answer to sample questions	15%
	Total: 25 Marks	**100%**

Marks obtained			**Dated Sign of Teacher**
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No 14: Collect information of IP addresses, domain names and emails using any information gathering tool like Recon-ng.

I. Practical Significance

Information gathering is important and fundamental step of ethical hacking or cybersecurity analysis. Before performing any penetration test or security assessment, it is essential to collect information about the target system. This phase is called reconnaissance, and it helps ethical hackers to understand the target's environment and plan the testing process effectively. Recon-ng is a powerful open-source reconnaissance tool written in Python that automates the process of gathering information. It provides a command-line interface similar to Metasploit and includes several built-in modules for collecting data from different sources.

II. Industry / Employer Expected outcome(s)

Apply Digital Forensic methodology to carry out investigations and penetration tests.

III. Course Level Learning outcome(s)

CO5 - Apply Tools and Techniques for Ethical Hacking.

IV. Laboratory Learning outcome(s)

LLO 14.1 Use any information gathering tool to collect information of IP addresses, domain names and emails.

V. Relevant Affective Domain related Outcome(s)

Demonstrates a conscious awareness of personal and organizational information exposure during the reconnaissance phase.

VI. Relevant Theoretical Background

Some basic terms those are important for understanding reconnaissance.

IP Address: unique number assigned to every device connected to a network (e.g.,192.168.1.1).

Domain Name: A human-readable name that maps to an IP address, like http://www.google.com

Email Address: An identifier for sending and receiving digital messages (e.g., info@example.com).

Recon-ng is a modular framework designed for web-based information gathering.

It allows the user to gather information about domains, hosts, and people from multiple sources like search engines, public databases, and APIs. The tool organizes its features into modules, each performing a specific function like domain enumeration, contact harvesting, or IP address resolution.

Features of Recon-ng:

- **Modular Design**: perform different tasks such as DNS lookup, data extraction, and analysis.
- **Database Integration**: stores gathered information in an internal database for later use.
- **User-Friendly Interface**: easy-to-use command-line interface for launching and managing modules.

- **API Integration**: Recon-ng connects with APIs such as Shodan, Bing, and Google to gather online data efficiently.

Collect information of IP addresses, domain names and emails using **Recon-**

Step1: Start Recon-ng

./recon-ng
workspaces create lab
add domains target.com

Step2: Find Domains/Subdomains

use recon/domains-hosts/bing_domain_web
set SOURCE target.com
run

Step3: Get IP Addresses

use recon/hosts-hosts/dns
set SOURCE target.com
run

Step4: Collect Emails

use recon/domains-contacts/whois
set SOURCE target.com
run

Step5: View & Export

show hosts
show contacts
export csv /tmp/results.csv contacts.

VII. Resources required

Sr. No.	Name of Resource	Specification	Quantity	Remarks (If any)
1.	Computer System	Computer (i3-i5 preferable RAM>2 GB	As Per Batch Size	
2.	Storage Type	Disk Space >20 GB		
3.	Internet Connectivity	Minimum 10 Mbps stable connection for download		

VIII. Conclusion

……...……

……...……

……...……

IX. Practical Related Questions

Note: Below are a few sample questions for reference. Teachers must design more such questions to ensure the achievement of the identified CO.

1. What is Recon-ng?
2. How can Recon-ng find subdomains?
3. How can Recon-ng find email addresses?

(Space for answers)

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

X. References/Suggestions for further Reading Assessment Scheme

1. https://www.101labs.net/comptia-security/lab-3-recon-ng/
2. https://hackertarget.com/recon-ng-tutorial/

XI. Assessment Scheme

The given performance indicators should serve as a guideline for assessment regarding process and product related marks. Faculty must fill only the table at bottom.

Performance Indicators		Weightage
Process related (15 Marks)		**60%**
1	Logic formation	30%
2	Debugging ability	20%
3	Follow ethical practices	10%
Product related (10 Marks)		**40%**
4	Expected output	10%
5	Timely Submission	15%
6	Answer to sample questions	15%
	Total: 25 Marks	**100%**

Marks obtained			Dated Sign of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	

Practical No 15: *Use Social-Engineer Toolkit (SET) tool for simulating phishing attacks to test human vulnerabilities.

I. Practical Significance

SET gives organizations to run realistic, controlled phishing simulations so they can quickly discover how people respond to attacks to fix the weakest links.

It is Useful to find real risk, prioritize fixes, Validate defenses & processes, Measures impact and Cost-effectiveness.

II. Industry / Employer Expected outcome(s)

Apply Digital Forensic methodology to carry out investigations and penetration tests.

III. Course Level Learning outcome(s)

CO5 - Apply Tools and Techniques for Ethical Hacking.

IV. Laboratory Learning outcome(s)

LLO 15.1 Simulate phishing attacks using Social-Engineer Toolkit.

V. Relevant Affective Domain related Outcome(s)

Developing ethical awareness, responsible use and valuing network security while using the tool.

VI. Relevant Theoretical Background

SET (Social-Engineer Toolkit) is an open-source framework designed to perform **social-engineering** attacks in a safe, repeatable way for security testing, awareness training, and red-teaming rather than technical hacking. Unlike tools that break passwords or scan networks, SET targets the human factor, which is often the weakest link in security.

Some common attack techniques supported by SET are:

- Phishing Attacks – Fake websites or emails that trick users into entering their credentials.
- Credential Harvesting – Collecting usernames and passwords when a victim enters them on a cloned website.
- Spear Phishing – Sending a targeted email with a malicious link or attachment.
- USB/Media Attacks – Creating infected files that look harmless, like PDFs or images.
- Payload Delivery – Injecting malicious software through phishing campaigns.

SET is used by security professionals, educators, and penetration testers to raise awareness and test how easily people can be deceived.

Importance of Using SET

- Helps organizations train employees about real-world cyber threats.
- Demonstrates how attackers can use simple tricks to bypass even strong technical security.

- Useful in penetration testing and red teaming to identify weak points in human behavior.
- Provides a safe environment to practice and learn ethical hacking.

1. Installing and Setting up SET

SET comes pre-installed in Kali Linux, which is the most commonly used operating system for penetration testing. If not available, it can be easily installed using terminal commands.

Steps to Install SET in Kali Linux:

1. Update the system

sudo apt update && sudo apt upgrade -y

2. Install SET (if not already installed)

sudo apt install set -y

3. Start SET

sudo setoolkit

4. Accept the terms and you will see a menu-based interface with different attack options.

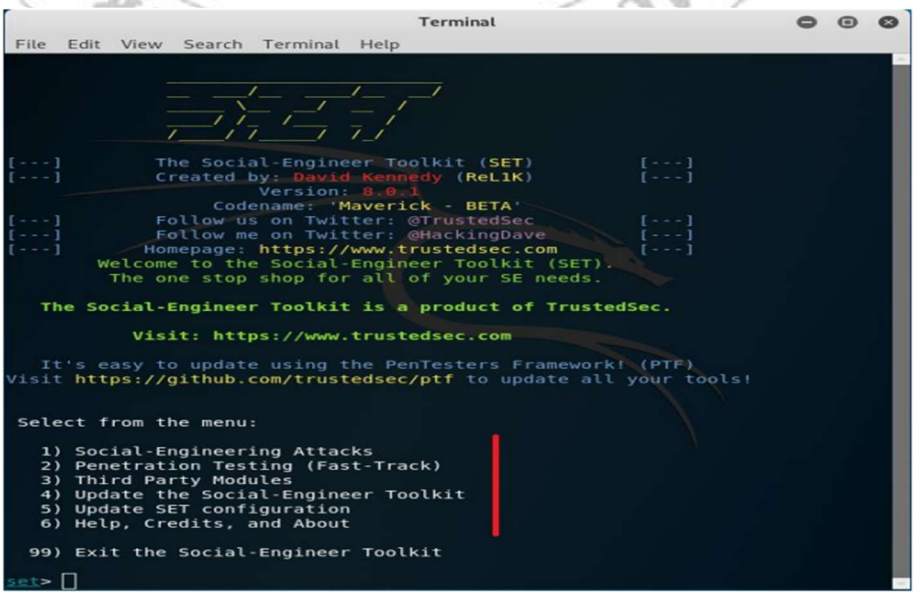
Note: Before running any attack, make sure you are working in a lab environment using two machines (an attacker machine and a victim machine) in the same network.

2 Steps to Perform a Phishing Attack using SET

Here we will see how to simulate a phishing attack in a safe and controlled environment. This example uses the Credential Harvester Attack Method.

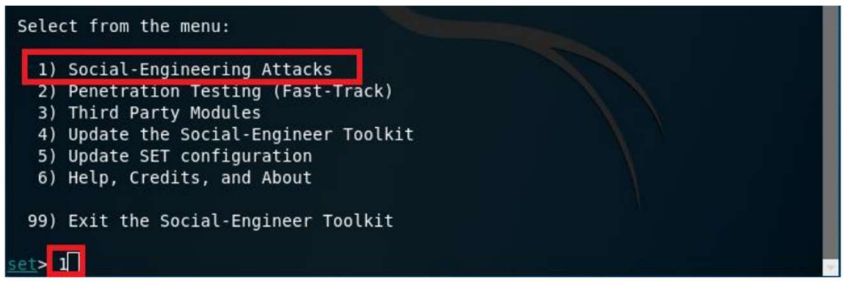
Step 1: Start SET

sudo setoolkit



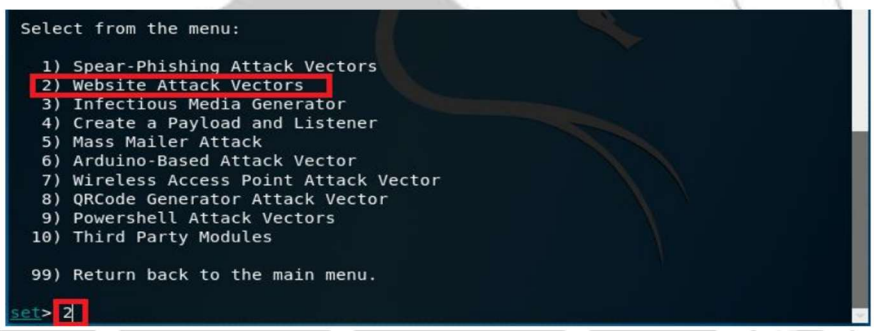
Step 2: Select Attack Type

Choose: 1) Social-Engineering Attacks



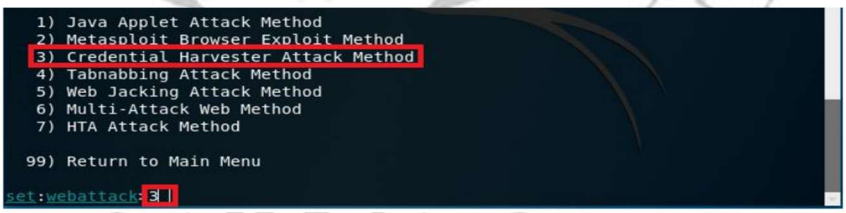
Step 3: Select Attack Vector

Choose: 2) Website Attack Vectors



Step 4: Choose Attack Method

Choose: 3) Credential Harvester Attack Method



Step 5: Choose Site Cloner

Select: 2) Site Cloner

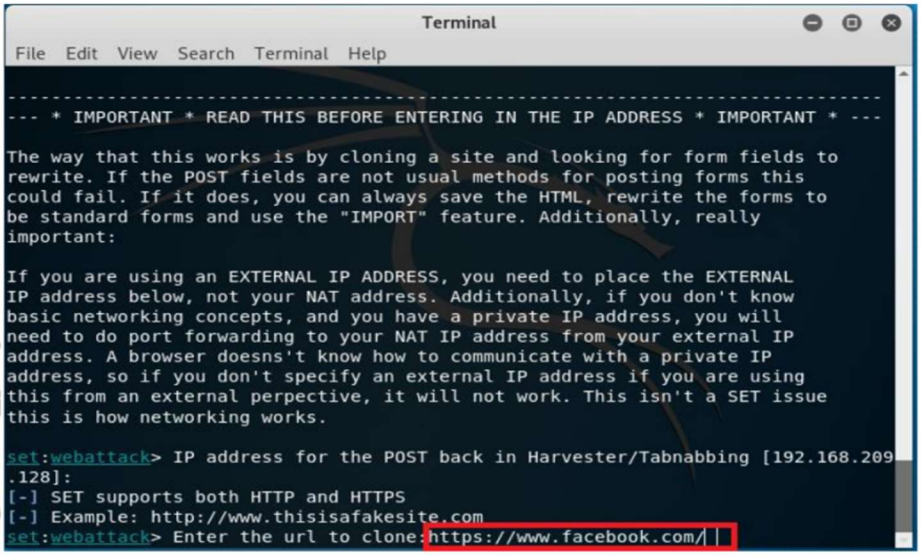
Step 6: Enter Attacker IP

Example: 192.168.1.10 (your Kali Linux machine's local IP address)

Step 7: Enter Website to Clone

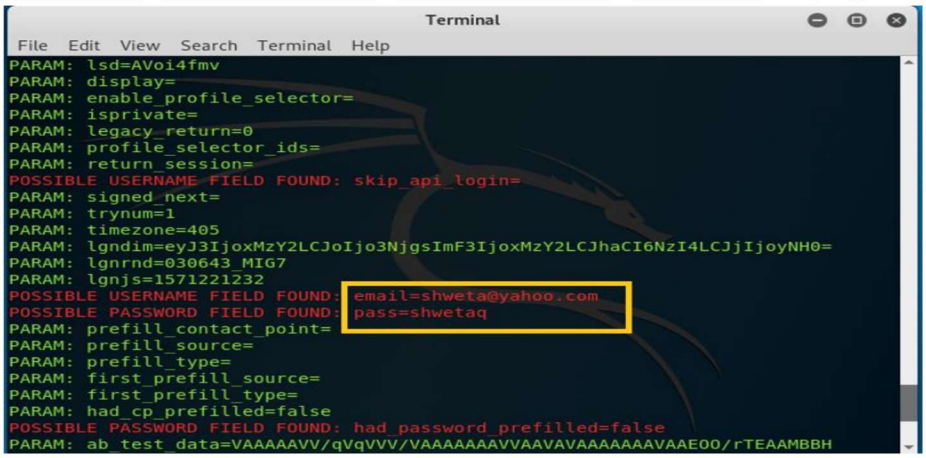
Example: http://www.facebook.com (use only in lab or for demo purposes).

SET will clone the website and host it on your attacker machine.



Step 8: Victim Access

When the victim visits the attacker's IP (e.g., http://192.168.1.10), they will see a fake login page. If they enter credentials, they are captured by SET and displayed on the attacker's terminal.



VII. Resources required

Sr. No.	Name of Resource	Specification	Quantity	Remarks (If any)
1.	Computer System	Computer (i3-i5 preferable RAM>2 GB	As Per Batch Size	
2.	Storage Type	Disk Space >20 GB		
3.	Internet Connectivity	Minimum 10 Mbps stable connection for download		

VIII. Conclusion

……...……

……...……

……...……

IX. Practical Related Questions

Note: Below are a few sample questions for reference. Teachers must design more such questions to ensure the achievement of the identified CO.

1. What is a social-engineering tool?
2. What ethical and privacy considerations exist?
3. What are the features SET tool?

(Space for answers)

.....

.....

.....

.....

.....

.....

.....

.....

.....

X. References/Suggestions for further Reading Assessment Scheme

1. https://cybertalents.com/blog/what-is-social-engineering-toolkit-complete-guide
2. https://trustedsec.com/resources/tools/the-social-engineer-toolkit-set/

XI. Assessment Scheme

The given performance indicators should serve as a guideline for assessment regarding process and product related marks. Faculty must fill only the table at bottom.

	Performance Indicators	Weightage
	Process related (15 Marks)	**60%**
1	Logic formation	30%
2	Debugging ability	20%
3	Follow ethical practices	10%
	Product related (10 Marks)	**40%**
4	Expected output	10%
5	Timely Submission	15%
6	Answer to sample questions	15%
	Total: 25 Marks	**100%**

Marks obtained			Dated Sign of Teacher
Process Related (15)	**Product Related (10)**	**Total (25)**	