Exp.No.:1	Install Kali or Backtrack Linux / Metasploitable/ Windows XP.
DATE:	

AIM:

To Install Kali Linux on Windows using Oracle Virtual Box.

PROCEDURE:

Step 1: Install VirtualBox:

1. Download the latest version of VirtualBox from the official website: https://www.virtualbox.org/wiki/Downloads
2. Run the installer and complete the installation with default settings.

Expected Outcome: VirtualBox is successfully installed and ready to use.

Step 2: Download Kali Linux ISO Image:

1. Navigate to the official Kali Linux download page: https://www.kali.org/get-kali/#kali-installer-images
2. Download the **Kali Linux ISO** file.
   - Option 1: Direct ISO download.
   - Option 2: Torrent download.

Expected Outcome: Kali Linux ISO file is available on your system for installation.

Step 3: Create and Configure a Virtual Machine:

1. Launch **VirtualBox**.
2. Click **New** to create a new virtual machine.
3. Enter details:
   - **Name:** Kali Linux
   - **Type:** Linux
   - **Version:** Debian (64-bit) or any 64-bit Linux
   - **Folder:** Keep default location
   - **ISO Image:** Browse and select the downloaded Kali Linux ISO
4. Configure resources:
   - **Memory (RAM):** 2048 MB (minimum), 4096 MB recommended
   - **Processors:** 2–4 cores
5. Create a virtual hard disk:
   - **File Type:** VDI (VirtualBox Disk Image)
   - **Size:** 20–25 GB (minimum)
   - **Allocation:** Dynamically allocated (do not pre-allocate full size)
6. Click **Finish** to complete the VM creation.

Expected Outcome: A new virtual machine for Kali Linux is created and ready for installation.

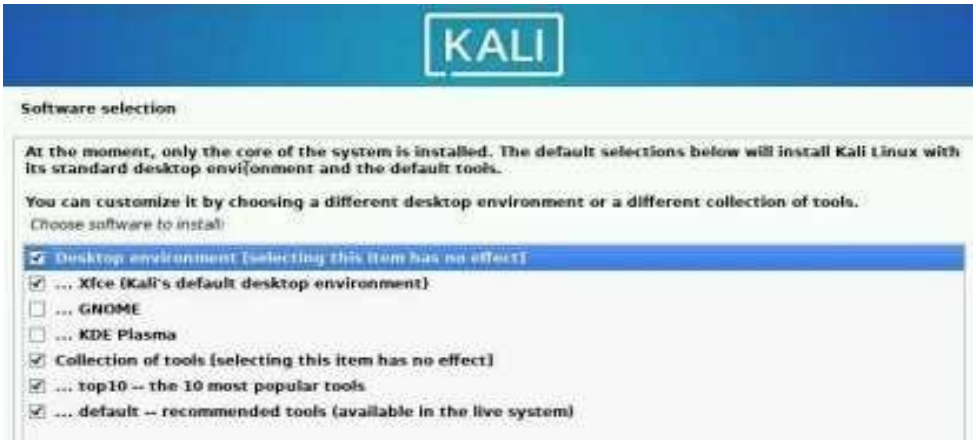
Step 4: Install Kali Linux

1. Start the virtual machine → click **Start**.
2. From the boot menu, select the **Install** option.

3. Follow the guided installer:
   - Select **Language**, **Region**, and **Keyboard**.
   - Configure a **Hostname** (optional).
   - Leave **Domain Name** blank.
   - Enter your **Full Name**, **Username**, and **Password**.

4. Partitioning:
   - Choose **Guided – Use Entire Disk** (recommended for VM).
   - Confirm changes.

5. Software selection:
    - Keep default selection: **Xfce Desktop Environment** and **Top Kali Tools**.



6. Wait for the installation process (approx. 10–15 minutes).
7. When prompted for GRUB installation:
    - Select **Yes**.
    - Install GRUB on **/dev/sda**.
8. After installation completes, select **Restart Now**.

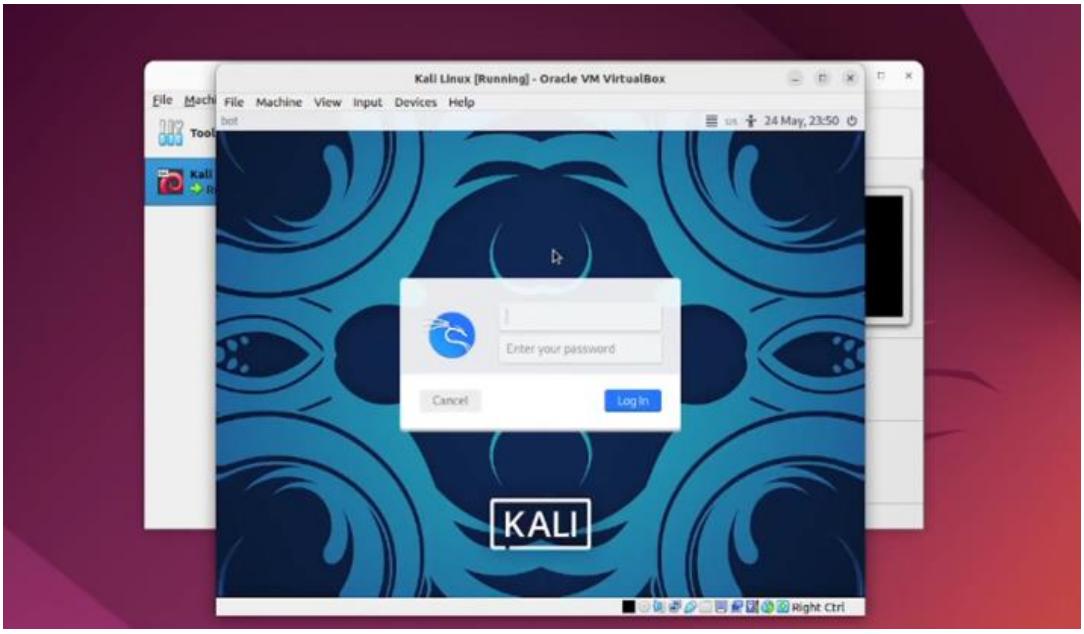
Expected Outcome: Kali Linux is successfully installed and the system reboots into the login screen.

Step 5: First Login

1. At the login screen, enter the **username and password** created during installation.
2. The **Kali Linux desktop environment** will load inside VirtualBox.

Expected Outcome: Kali Linux is fully installed and operational as a virtual machine in VirtualBox on Windows.

SAMPLE OUTPUT:



OUTPUT:

Pre-Lab Assessment

1. What is VirtualBox used for?

2. Why do we use a virtual machine for Kali Linux?

3. What file format is used to install Kali Linux on VirtualBox?

4. What is the minimum recommended RAM for Kali Linux in VirtualBox?

5. How much hard disk space should be allocated for Kali Linux?

6. Which type of hard disk file is commonly used in VirtualBox?

7. Which boot option should be selected to install Kali Linux?

8. What partitioning method is recommended in VirtualBox installation?

9. What is GRUB used for in Kali Linux installation?

10. Which desktop environment is usually selected by default in Kali Linux?

Pre-Lab Work

- Download and install **VirtualBox** on the system.
- Download the **Kali Linux ISO file** from the official website.
- Make sure the system has enough **RAM, storage, and virtualization enabled**.
- Get ready with a folder to save VM files.
- Revise the basic concepts of **virtual machines and operating system installation**.

Post-Lab Assessment

1. Which software was used to create the virtual machine?

2. Which operating system was installed in the virtual machine?

3. What is the role of the ISO file in the installation?

4. How much RAM was allocated to the Kali Linux VM in this lab?

5. How much hard disk space was assigned to the Kali Linux VM?

6. Which boot loader was installed during setup?

7. What credentials are required to log in after installation?

8. Which desktop environment was installed by default?

9. What is the final outcome of this lab?

10. Why is running Kali Linux in VirtualBox considered safe?

EVALUATION

CONTENT		MAXIMUM MARKS	MARKS OBTAINED
Pre-lab assessment	(A)	10	
Pre-lab work	(B)	20	
Conduct of Experiment	(C)	20	
Data observation	(D)	20	
Analysis and Interpretation	(E)	20	
Post-lab assessment/Viva Voce	(F)	10	
Total (A+B+C+D+E+F)		100	

RESULT:

The installation of **Kali Linux** on **Oracle VirtualBox** was successfully completed. A fully functional virtual machine was created, configured, and booted with the Kali Linux operating system, allowing secure and isolated usage of Kali Linux within the Windows environment.

Exp.No.:2	Practice the basics of reconnaissance.
DATE:	

AIM:

To practice the basics of reconnaissance in Ethical Hacking.

COMMANDS:

1. ***Ping Scan with Nmap:***

   A ping scan in Nmap is used to quickly check which devices (hosts) are **active and reachable** in a network, without scanning their ports.

Command Name: *nmap -sn <target_ip>*

Sample Output:

```
Starting Nmap 7.91 ( https://nmap.org ) at 2023-08-09 10:00 EDT
Nmap scan report for <target_ip>
Host is up (0.034s latency).
MAC Address: XX:XX:XX:XX:XX:XX (Manufacturer)
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

2. ***DNS Enumeration with Dig:***

   DNS enumeration with the dig command is used to **gather information about a domain**, such as its IP address, mail servers, and other DNS records.

Command Name: *dig <target_domain>*

Sample Output:

```
; <<>> DiG 9.16.1-Ubuntu <<>> <target_domain>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: XXXXX
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; QUESTION SECTION:
;<target_domain>.        IN  A

;; ANSWER SECTION:
<target_domain>.  300 IN  A   <target_ip>

<target_domain>.  300 IN  A   <another_ip>

;; Query time: 10 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Aug 09 10:05:53 EDT 2023
;; MSG SIZE  rcvd: 76
```

3. WHOIS Lookup:

A WHOIS lookup is used to **find information about the owner of a domain name or IP address**, such as registration details, contact info, and expiration date.

Command Name: *whois <domain_name>*

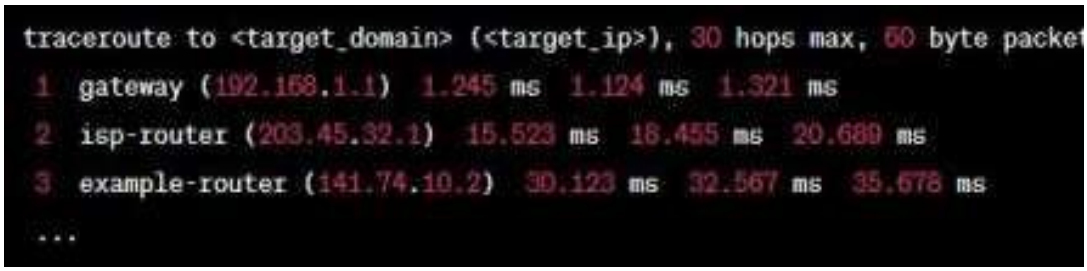
Sample Output:

4. Traceroute:

Traceroute is a network diagnostic tool used to **show the path and all the intermediate devices (routers) a packet takes to reach a target system**, along with the time taken at each step.

Command Name: *traceroute <target_ip_or_domain>*

Sample Output:



OUTPUT:

Pre-Lab Assessment

1. What is reconnaissance in ethical hacking?

2. Define active reconnaissance and passive reconnaissance.

3. Why is reconnaissance important before penetration testing?

4. Which tool is used for ping scanning in this experiment?

5. What does the `-sn` option in Nmap signify?

6. Which command is used for DNS enumeration?

7. What type of information does the WHOIS lookup provide?

8. What does the traceroute command reveal?

9. Differentiate between DNS A record and MX record.

10. Why is it important to identify live hosts in a target network?

Pre-Lab Work

- Install **Nmap, Dig, WHOIS, and Traceroute** utilities on the system.
- Review the basic syntax of each command.
- Select a safe and legal target domain/IP for testing (such as `example.com` or local private IPs).
- Ensure internet connectivity is available for DNS and WHOIS queries.
- Note down the expected purpose of each tool before execution.

Post-Lab Assessment

1. What did you observe from the Nmap ping scan results?

2. Which hosts were identified as live in your test?

3. What DNS records were retrieved using Dig?

4. From WHOIS output, what domain details were most useful?

5. How many hops were traced using traceroute to the target?

6. Which command gave the most detailed information about the target?

7. How can reconnaissance help an ethical hacker plan further testing?

8. Did you face any limitations while running these commands?

9. Which technique belongs to **active reconnaissance** and which to **passive reconnaissance**?

10. Summarize what you learned from this experiment in 2–3 sentences.

EVALUATION

CONTENT		MAXIMUM MARKS	MARKS OBTAINED
Pre-lab assessment	(A)	10	
Pre-lab work	(B)	20	
Conduct of Experiment	(C)	20	
Data observation	(D)	20	
Analysis and Interpretation	(E)	20	
Post-lab assessment/Viva Voce	(F)	10	
Total (A+B+C+D+E+F)		100	

RESULT:

The basic reconnaissance techniques in Ethical Hacking were learned and practiced successfully.

Exp.No.:3	**Using FOCA / SearchDiggity tools, extract metadata and expanding the target list.**
DATE:	

AIM:

To understand how to extract metadata from a website using FOCA (Fingerprinting Organizations with Collected Archives) software.

PROCEDURE:

1. Setting up SQL Server

- Open a web browser and navigate to the official Microsoft SQL Server Express download page.
- Click on the **Download** button to get the installer.
- Once downloaded, run the installer file.
- Accept the license terms and conditions.
- Select the installation type as **Basic** and proceed.
- Wait for the installation to complete.

2. Installing FOCA Software

- Download FOCA from its official website or a trusted source.
- Locate the downloaded **ZIP file** and extract it.
- Open the extracted folder and double-click **FOCA.exe** to launch the application.

3. Creating a New Project in FOCA

- On launching FOCA, click **New Project**.
- Provide a project name and enter the target website in the **Domain** field.
- Click **Create Project**.

4. Searching and Downloading Documents

- Select the search engines FOCA should use.
- Choose the types of documents to search (e.g., PDF, DOC, PPT, etc.).
- Click **Search All** to begin the search.
- A list of related files will appear.
- Right-click on the results and select **Download All** to save the files locally.

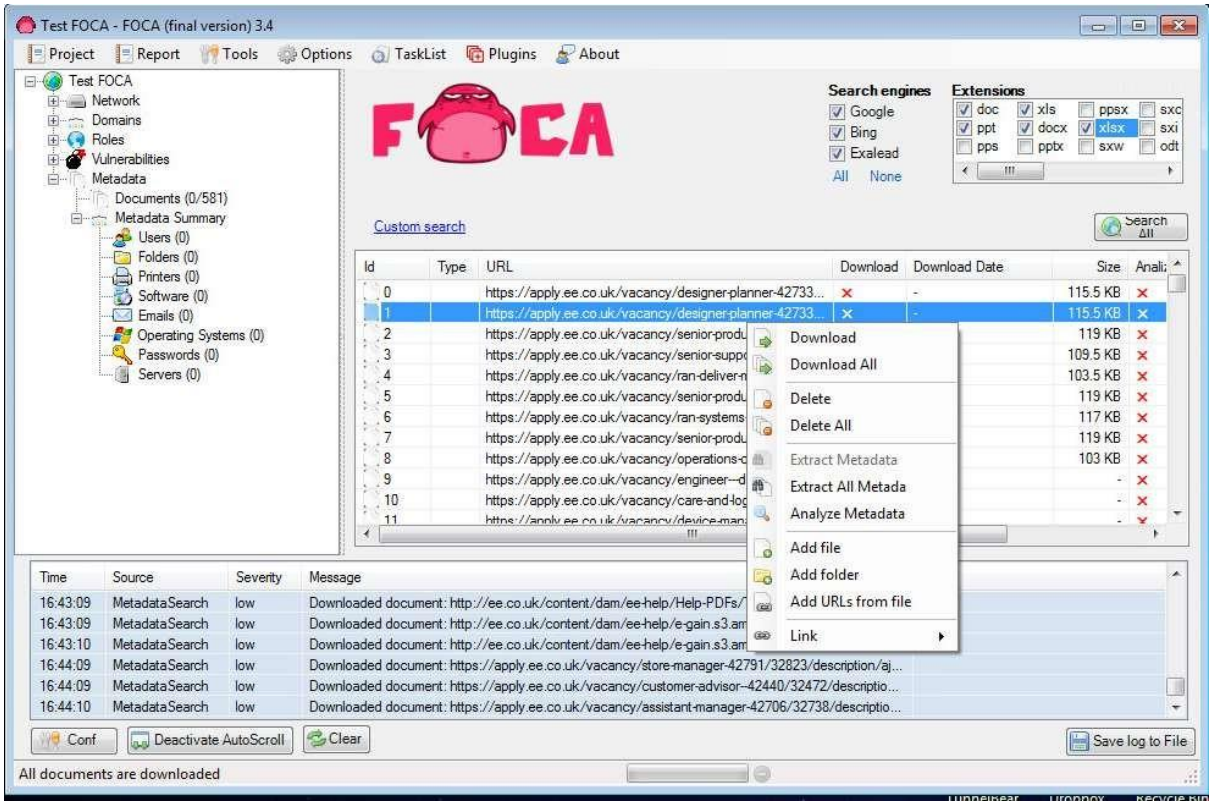
5. Extracting Metadata

- After downloading, right-click on any file in FOCA.
- Select **Extract All Metadata**.
- Wait until the extraction process is complete.

6. Viewing Extracted Metadata

- In the FOCA interface, click on the **Metadata** tab (left panel).
- View the list of extracted metadata details from the documents.

SAMPLE OUTPUT:



OUTPUT:

Pre-Lab Assessment

1. What is metadata?

2. Why is metadata extraction important in ethical hacking?

3. What does FOCA stand for?

4. Which types of documents can FOCA analyze?

5. What information can be revealed through metadata?

6. Why is SQL Server required for FOCA?

7. Differentiate between passive and active reconnaissance.

8. Give an example of sensitive information that can be found in metadata.

9. What are the risks for organizations exposing metadata?

10. Name any two alternatives to FOCA for metadata extraction

Pre-Lab Work

- Install **Microsoft SQL Server Express** for FOCA to function properly.
- Download and extract the FOCA software.
- Identify a safe and legal website for testing (e.g., `example.com`).
- Review the purpose of metadata and its role in reconnaissance.
- Ensure an active internet connection for FOCA searches.

Post-Lab Assessment

1. What metadata details were you able to extract from the documents?

2. Which search engines gave the best results in FOCA?

3. Did FOCA reveal any usernames or software versions?

4. How could an attacker misuse extracted metadata?

5. How can organizations protect themselves from metadata leakage?

6. Which step in FOCA was most critical for successful extraction?

7. What is the role of SQL Server in FOCA's functioning?

8. Was FOCA's extraction process active or passive reconnaissance? Why?

9. How does FOCA help in penetration testing?

10. Summarize what you learned from this experiment in two sentences.

EVALUATION

CONTENT		MAXIMUM MARKS	MARKS OBTAINED
Pre-lab assessment	(A)	10	
Pre-lab work	(B)	20	
Conduct of Experiment	(C)	20	
Data observation	(D)	20	
Analysis and Interpretation	(E)	20	
Post-lab assessment/Viva Voce	(F)	10	
Total (A+B+C+D+E+F)		100	

RESULT:

The experiment was successfully performed, and metadata extraction using FOCA was practiced. Useful details such as document authors, usernames, and file properties were obtained, fulfilling the objective of the experiment.

Exp.No.:4	**Aggregates information from public databases using online free tools like Paterva's Maltego.**
DATE:	

AIM:

To understand and practice the process of gathering and correlating open-source intelligence (OSINT) using Paterva's Maltego.

PROCEDURE:

1. **Installing Maltego**

- Visit the official Maltego website and download the software suitable for your operating system.
- Follow the installation wizard to complete the setup.
- Launch the Maltego application.
- Register for a new account or log in to an existing one.

2. **Creating a New Graph**

- Go to the **File** menu and select **New**.
- A new graph window will open, which serves as your workspace.

3. **Basic Entity Search**

- From the **Entity Palette**, drag and drop an entity type (e.g., *Domain*, *Email Address*) onto the graph.
- Double-click the entity and enter the specific value you want to investigate (such as a domain name or email address).

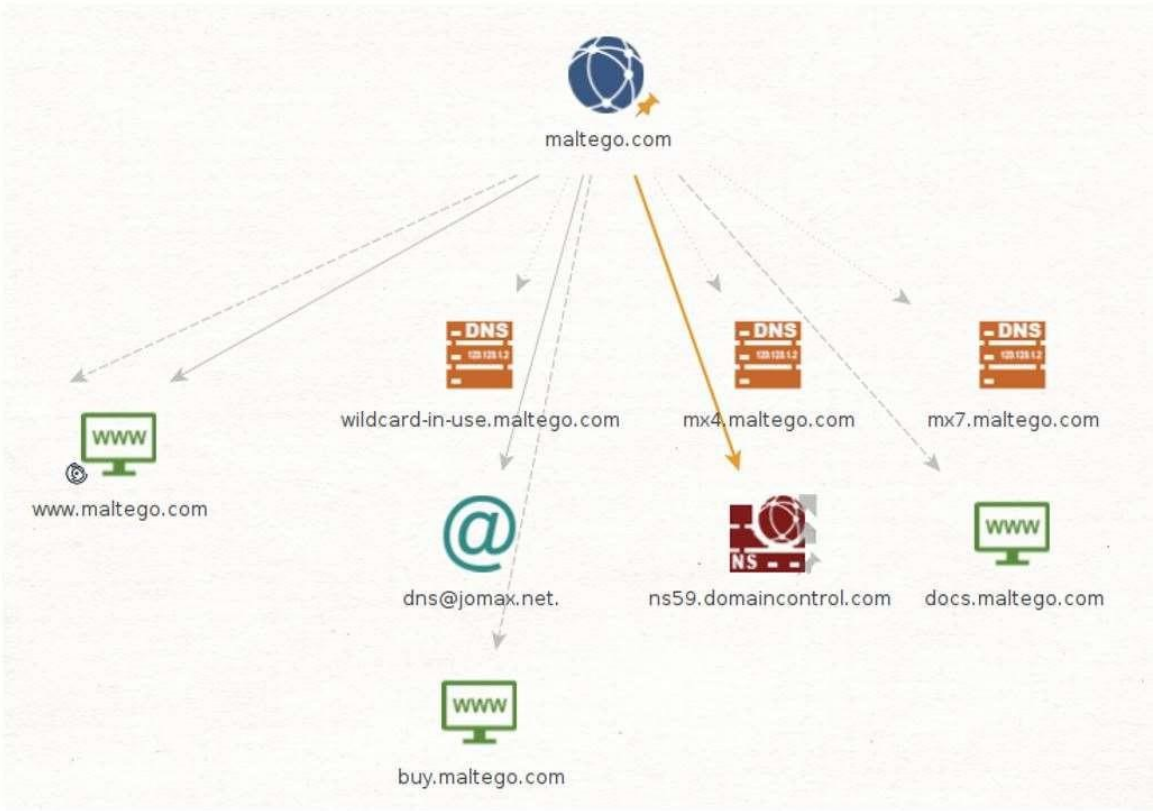
4. **Running a Transform**

- Right-click on the entity placed on the graph.
- From the **Run Transform** menu, choose an appropriate transform (e.g., *To Email [Using Search Engine]* for an email entity).
- Maltego will execute the transform and display newly discovered entities connected to your original input.

5. **Exploring and Aggregating Information**

- Continue running additional transforms on the discovered entities to gather more information.
- Adjust the graph by zooming, rearranging, or expanding entities for better visualization.
- The aggregated data may include related websites, IP addresses, social media accounts, and other linked information.

SAMPLE OUTPUT:



OUTPUT:

Pre-Lab Assessment

1. What is OSINT?

2. What is the primary purpose of Maltego?

3. Define “Entity” in the context of Maltego.

4. What is a “Transform” in Maltego?

5. Mention one difference between Maltego and traditional search engines.

6. Give an example of an entity that can be investigated in Maltego.

7. What kind of information can be aggregated using Maltego?

8. Why is visualization important in information security investigations?

9. Can Maltego work without an internet connection? Why/why not?

10. Name one field (besides cybersecurity) where Maltego can be applied.

Pre-Lab Work

- Install Maltego on your system (ensure correct version for OS).
- Create/Register a Maltego account.
- Review basic concepts of footprinting and reconnaissance in cybersecurity.
- Familiarize yourself with common entities such as domains, IP addresses, and emails.
- Ensure an active internet connection for transforms to run.
- Read about OSINT and its importance in cybersecurity.
- Prepare a test domain or email ID to be used for practice (avoid using sensitive data).

Post-Lab Assessment

1. What steps are involved in creating a new graph in Maltego?

2. How do you add an entity to the workspace?

3. Explain the process of running a transform on an entity.

4. What type of information did you obtain from your entity in this lab?

5. How does Maltego help in aggregating related information?

6. Mention one advantage of using Maltego for OSINT.

7. What visualization features in Maltego helped you understand relationships?

8. Which transform did you find most useful and why?

9. How can Maltego results support cybersecurity investigations?

10. Write one limitation of Maltego you observed during the lab.

EVALUATION

CONTENT		MAXIMUM MARKS	MARKS OBTAINED
Pre-lab assessment	(A)	10	
Pre-lab work	(B)	20	
Conduct of Experiment	(C)	20	
Data observation	(D)	20	
Analysis and Interpretation	(E)	20	
Post-lab assessment/Viva Voce	(F)	10	
Total (A+B+C+D+E+F)		100	

RESULT:

Thus, information aggregation using **Paterva's Maltego** was successfully performed and executed.

Exp.No.:5	Information gathering using tools like Robtex.
DATE:	

AIM:

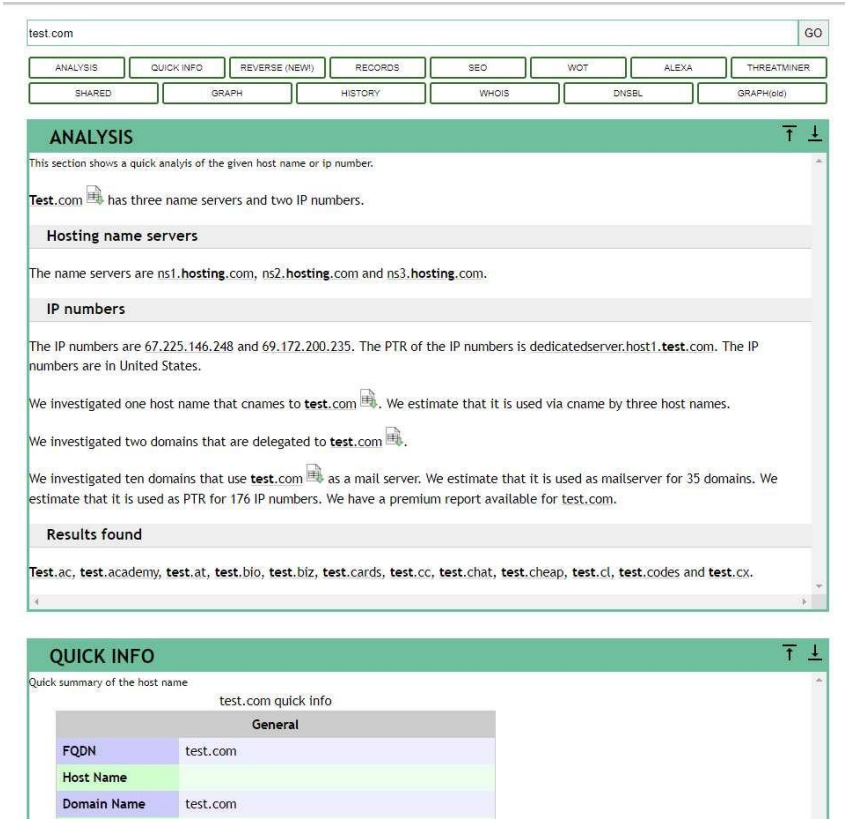
To study the role of Robtex in footprinting and information gathering during ethical hacking.

PROCEDURE:

1. **Accessing Robtex**
    - Open a web browser and navigate to https://www.robtex.com/.
    - On the homepage, you will find a search bar where you can enter a domain name, IP address, or network to investigate.
2. **Domain Lookup**
    - Enter the desired domain name (e.g., *example.com*) in the Robtex search bar.
    - Click the **Search** button or press **Enter**.
    - Robtex will display detailed information about the domain, such as DNS records, associated IP addresses, hosting details, and server location.
3. **IP Address Lookup**
    - Type the IP address you wish to investigate into the search bar.
    - Click **Search** or press **Enter**.
    - The tool will return data such as the organization owning the IP, its geolocation, ASN details, and domains hosted on the same IP.
4. **ASN Lookup**
    - If you want to explore an Autonomous System Number (ASN), enter it into the search bar.
    - Click **Search** to view results.
    - Robtex will provide information such as AS routes, allocated IP ranges, and associated domains.

5. **Understanding and Analyzing Results**
    - Review the different sections and tabs available for each type of lookup. These may include:
        - DNS records
        - Mail server records
        - Subdomains and domain siblings
        - Shared IP addresses
        - ASN details
    - Analyze the data to gain insights into the domain, IP address, or network under investigation.

SAMPLE OUTPUT:



OUTPUT:

Pre-Lab Assessment

1. What is the primary purpose of Robtex?

2. What kind of information can be retrieved using Robtex for a domain?

3. Define DNS records in simple terms.

4. What does IP address lookup reveal?

5. What is an ASN (Autonomous System Number)?

6. How does Robtex help in finding shared IP addresses?

7. Why is it important to analyze mail server records?

8. What is the difference between a domain lookup and an IP lookup?

9. How can subdomains provide useful insights?

10. Why is Robtex considered useful in cybersecurity investigations?

Pre-Lab Work

- Review the concepts of **DNS, IP addresses, and ASNs**.
- Identify at least **one domain name** and **one IP address** you will use during the experiment.
- Familiarize yourself with the Robtex website layout.
- Recall the role of tools like Robtex in **ethical hacking and footprinting**.

Post-Lab Assessment

1. What type of information did Robtex provide for the tested domain?

2. Were you able to find DNS and mail server records?

3. What insights were gained from the IP lookup?

4. Did the ASN lookup show routes and associated domains?

5. How do domain siblings or subdomains help in reconnaissance?

6. Was there any evidence of shared hosting on the IP address?

7. How can geolocation of IP help in security analysis?

8. Compare the usefulness of domain lookup vs IP lookup.

9. What challenges did you face while analyzing the results?

10. Summarize how Robtex can support cybersecurity and network research.

EVALUATION

CONTENT		MAXIMUM MARKS	MARKS OBTAINED
Pre-lab assessment	(A)	10	
Pre-lab work	(B)	20	
Conduct of Experiment	(C)	20	
Data observation	(D)	20	
Analysis and Interpretation	(E)	20	
Post-lab assessment/Viva Voce	(F)	10	
Total (A+B+C+D+E+F)		100	

RESULT:

Thus, information gathering using Robtex was performed successfully, and details about domains, IP addresses, and networks were analyzed.

Exp.No.:6	Scan the target using tools like Nessus.
DATE:	

AIM:

To understand how to use Nessus for vulnerability scanning on a target system or network.

PROCEDURE:

1. **Initial Setup and Login**

   - Launch Nessus from the program menu or desktop shortcut.
   - For first-time use, activate Nessus using the activation code obtained by registering on the Tenable website.
   - After activation, log in to the Nessus interface with your credentials.

2. **Updating Plugins**

   - Ensure Nessus plugins are updated to include the latest vulnerability checks.
   - Nessus usually updates plugins automatically, but manual updates can be performed from the *Plugins* section by selecting *Update*.

3. **Creating a New Scan**

   - From the dashboard, click on *New Scan*.
   - Select an appropriate scan template (e.g., *Basic Network Scan, Advanced Scan*).
   - Provide a scan name and description for reference.

4. **Configuring Scan Settings**

   - In the *Targets* field, enter the IP addresses or hostnames of the systems to be scanned (with proper authorization).
   - Configure additional options such as scheduling, notifications, and advanced scan preferences.
   - If required, set authentication credentials to enable deeper scanning of the target system.

5. **Starting the Scan**

   - Save the scan configuration by clicking *Save*.
   - Launch the scan by clicking the *Launch* button.

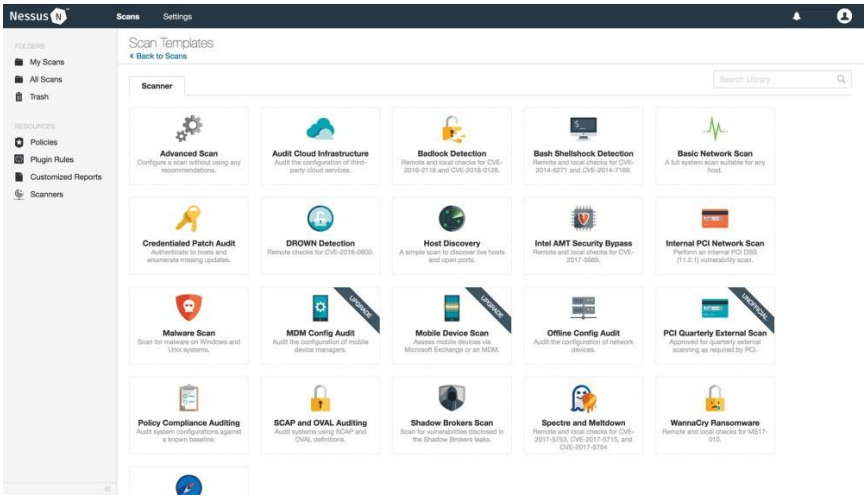
6. **Monitoring the Scan**

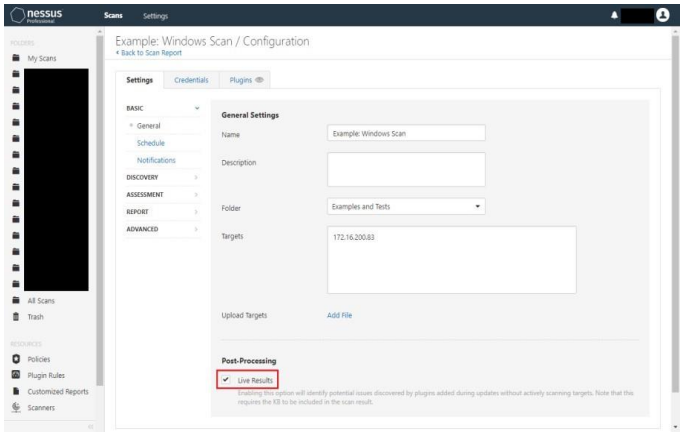
- Track the scan's progress from the dashboard.
- Nessus displays key statistics such as the number of vulnerabilities discovered and their severity levels.

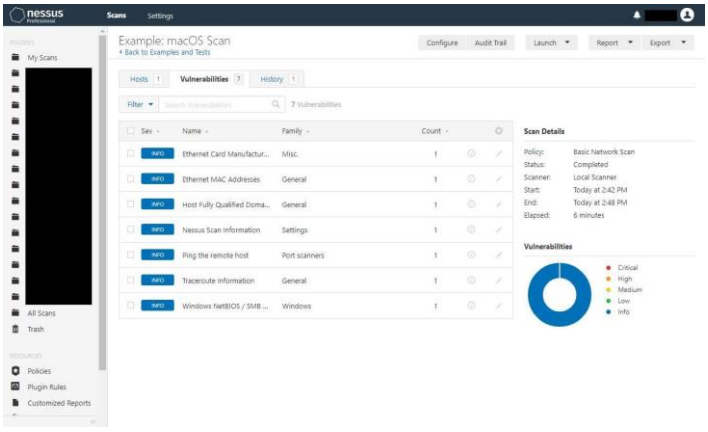
7. **Analyzing the Results**

- After completion, open the scan report to review findings.
- Vulnerabilities are categorized by severity: Critical, High, Medium, Low, or Informational.
- Each vulnerability entry provides details including description, potential impact, and recommended remediation steps.

SAMPLE OUTPUT:







OUTPUT:

Pre-Lab Assessment

1. What is Nessus used for?

2. Define vulnerability scanning in simple terms.

3. Why is it important to update Nessus plugins before a scan?

4. List two common Nessus scan templates.

5. What information is required to specify the target system?

6. What does “authenticated scan” mean in Nessus?

7. How are vulnerabilities categorized in Nessus reports?

8. Why should scanning only be done with authorization?

9. What is the difference between “Basic Network Scan” and “Advanced Scan”?

10. What should be checked after completing a vulnerability scan?

Pre-Lab Work

- Install and activate Nessus with a valid activation code.
- Ensure internet connectivity for plugin updates.
- Prepare a test system or network with proper authorization for scanning.
- Review basic scanning concepts and Nessus documentation.

Post-Lab Assessment

1. What is the purpose of using Nessus in cybersecurity?

2. How can plugin updates impact scan accuracy?

3. Why is authentication important for deeper scans?

4. What are the possible severity levels in Nessus reports?

5. What steps should be taken after vulnerabilities are identified?

EVALUATION

CONTENT		MAXIMUM MARKS	MARKS OBTAINED
Pre-lab assessment	(A)	10	
Pre-lab work	(B)	20	
Conduct of Experiment	(C)	20	
Data observation	(D)	20	
Analysis and Interpretation	(E)	20	
Post-lab assessment/Viva Voce	(F)	10	
Total (A+B+C+D+E+F)		100	

RESULT:

Thus, vulnerability scanning of a target system using Nessus was successfully performed and analyzed.

Exp.No.:7	View and capture network traffic using Wireshark.
DATE:	

AIM:

To view and capture network traffic using Wireshark.

PROCEDURE:

1. Download Wireshark

- Visit the official Wireshark website: https://www.wireshark.org/download.html.
- Download the appropriate version for your operating system (Windows, macOS, or Linux).

2. Install Wireshark

- Run the downloaded installer.
- Follow the on-screen instructions in the installation wizard to complete the setup.

3. Launch Wireshark

- After installation, open the Wireshark application.

4. Select a Network Interface

- Wireshark will display a list of available network interfaces.
- Select the interface through which you want to capture traffic (e.g., Ethernet or Wi-Fi).

5. Start Capturing Traffic

- Click the **Start** (Capture) button to begin capturing network traffic.

6. Analyze Captured Packets

- Monitor the live stream of captured packets.
- Apply filters and search options to focus on specific packet types or protocols.

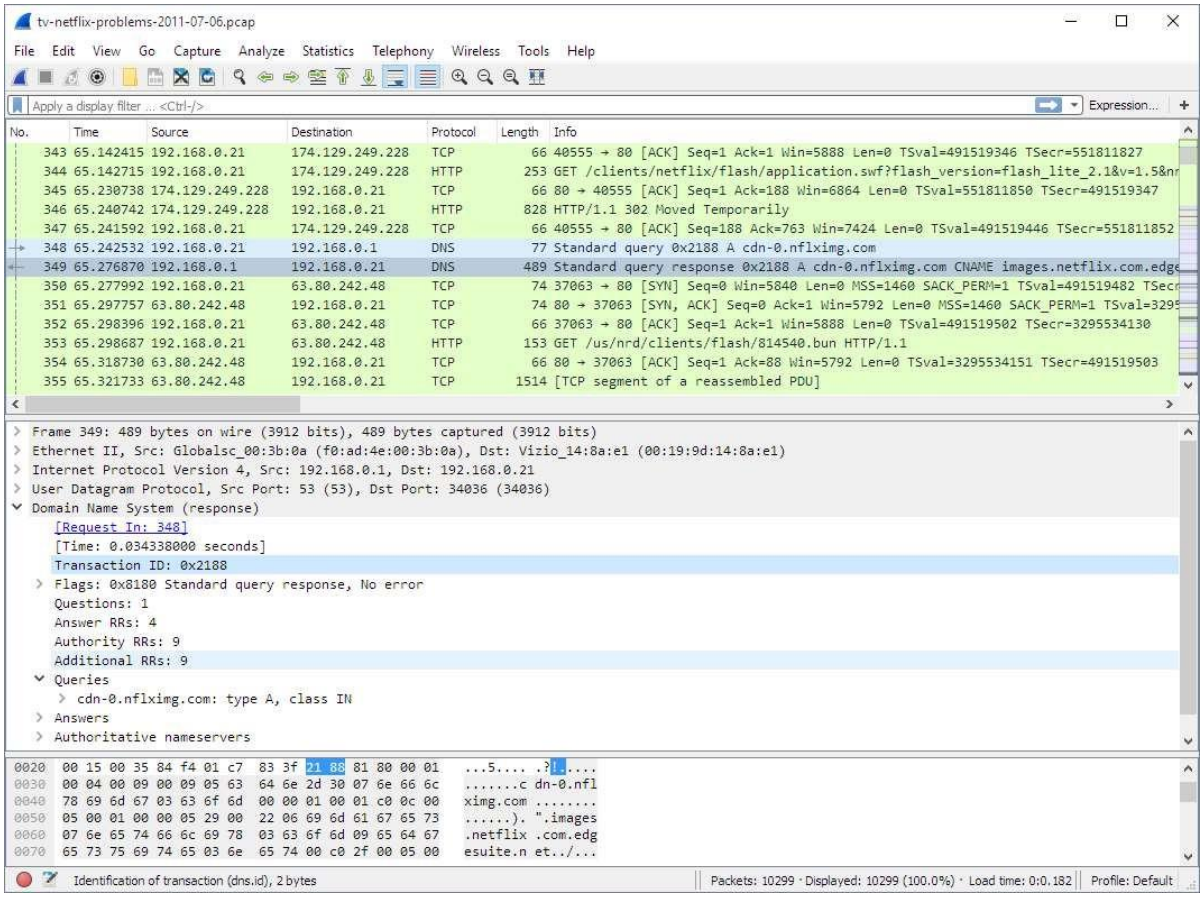
7. Stop Capturing

- Once sufficient data has been captured, click the **Stop** button to end the capture.

8. View Captured Packets

- Browse through the captured packets in the main window.
- Click on any packet to view detailed information such as source/destination IP addresses, protocols, and packet contents.

SAMPLE OUTPUT:



OUTPUT:

Pre-Lab Assessment

1. What is Wireshark used for?

2. Define packet sniffing.

3. Name two common network protocols visible in Wireshark.

4. What is the purpose of network interfaces?

5. Which layer of the OSI model deals with IP addresses?

6. Why do we apply filters in Wireshark?

7. Can Wireshark capture encrypted traffic?

8. Give one advantage of using Wireshark in troubleshooting.

9. Name a security concern when using packet sniffing tools.

10. What does the term “real-time traffic capture” mean?

Pre-Lab Work

- Download and install Wireshark from the official website.
- Familiarize yourself with the interface and available network adapters.
- Review basic network concepts (IP, TCP, UDP, HTTP).

Post-Lab Assessment

1. What type of information can be obtained from a captured packet?

2. How can filters improve analysis in Wireshark?

3. Give an example of a Wireshark display filter.

4. What does the three-pane view in Wireshark represent?

5. Why is it important to stop capturing at the right time?

6. How can Wireshark help detect malicious activity?

7. Differentiate between live capture and offline analysis.

8. Which tab in Wireshark shows packet details?

9. What does “protocol hierarchy” in Wireshark indicate?

10. Can Wireshark be used for wireless traffic analysis? Explain briefly.

EVALUATION

CONTENT		MAXIMUM MARKS	MARKS OBTAINED
Pre-lab assessment	(A)	10	
Pre-lab work	(B)	20	
Conduct of Experiment	(C)	20	
Data observation	(D)	20	
Analysis and Interpretation	(E)	20	
Post-lab assessment/Viva Voce	(F)	10	
Total (A+B+C+D+E+F)		100	

RESULT:

Thus, the process of viewing and capturing network traffic using Wireshark was successfully carried out and verified.

Exp.No.:8	Automate dig for vulnerabilities and match exploits using Armitage.
DATE:	

AIM:

To automate vulnerability discovery and match exploits using Armitage and FOCA.

PROCEDURE:

1. **Scanning and Reconnaissance:**

    - Launch Kali Linux and open **Armitage**.
    - Perform network scanning using tools like **Nmap** to identify open ports and active hosts.
    - Import the scan results into Armitage to generate a target list.

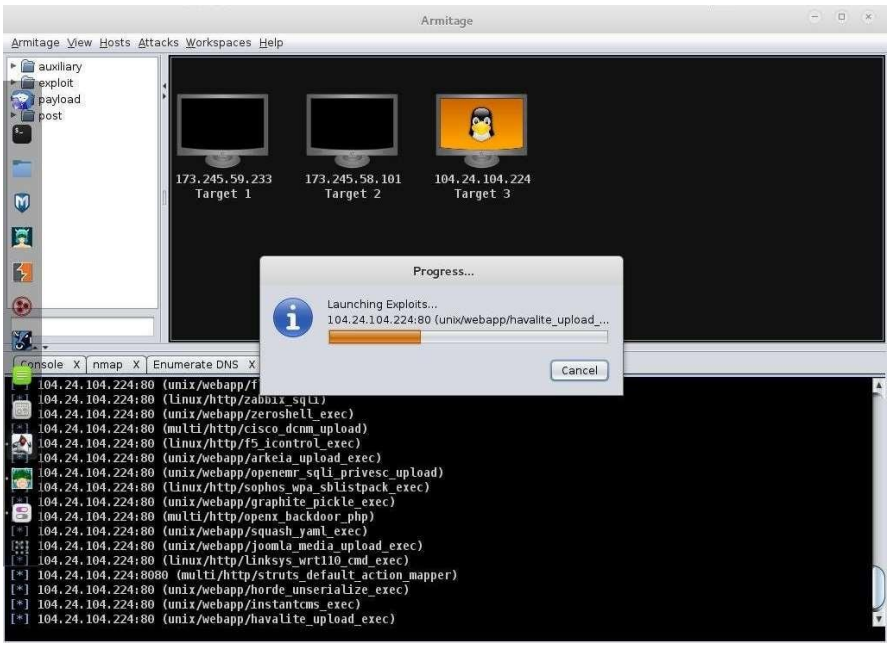
2. **Vulnerability Analysis:**

    - Use Armitage's built-in features to conduct vulnerability scanning on the target hosts.
    - Identify possible vulnerabilities such as outdated software, weak credentials, or system misconfigurations.
    - Employ **FOCA (Fingerprinting Organizations with Collected Archives)** to collect metadata and information from the target organization's public documents.

3. **Exploitation and Attack:**

    - In Armitage, browse the available exploits and payloads corresponding to the identified vulnerabilities.
    - Choose an appropriate exploit–payload combination for the target system.
    - Launch the attack and monitor the results through Armitage's interface.

SAMPLE OUTPUT:



OUTPUT:

Pre-lab Assessment

1. What is the purpose of Armitage in penetration testing?

2. Define vulnerability scanning.

3. What is the role of FOCA in reconnaissance?

4. What is an exploit in cybersecurity?

5. How does Nmap assist in scanning?

6. What is the difference between scanning and exploitation?

7. Why is metadata collection important in information gathering?

8. What is the use of payloads in Armitage?

9. Define the term “misconfiguration vulnerability.”

10. Why is automation useful in penetration testing?

Pre-lab Work

- Install and configure **Kali Linux**.
- Ensure **Armitage** and **Nmap** are installed and working.
- Download and install **FOCA** on a Windows system (since FOCA runs on Windows).
- Prepare a sample target network (test lab environment or VM).
- Familiarize with the Armitage interface and FOCA's metadata extraction process.

Post-lab Assessment

1. What information does FOCA extract from documents?

2. How does Armitage simplify exploitation compared to manual Metasploit use?

3. Which tool was used for network scanning in this experiment?

4. What is the purpose of importing Nmap results into Armitage?

5. Why is it necessary to match exploits with vulnerabilities?

EVALUATION

CONTENT		MAXIMUM MARKS	MARKS OBTAINED
Pre-lab assessment	(A)	10	
Pre-lab work	(B)	20	
Conduct of Experiment	(C)	20	
Data observation	(D)	20	
Analysis and Interpretation	(E)	20	
Post-lab assessment/Viva Voce	(F)	10	
Total (A+B+C+D+E+F)		100	

RESULT:

The automation of vulnerability discovery and exploitation using **Armitage** in combination with **FOCA** was successfully carried out.

CONTENT BEYOND THE SYLLABUS*

Exp.No.:1	Metadata Extraction using FOCA.
DATE:	

AIM:

To understand the process of metadata extraction and perform information gathering from publicly available documents and websites using FOCA (Fingerprinting Organizations with Collected Archives).

PROCEDURE:

1. Download and Install FOCA

- Visit a trusted source and download the FOCA installation package.
- Run the installer and complete the installation process.

2. Launch FOCA

- Open the FOCA application.
- Familiarize yourself with the interface, which includes options for projects, domains, and results.

3. Create a New Project

- Go to **File → New Project**.
- Enter a project name and provide the target domain (URL) or upload local documents.

4. Scanning for Documents

- FOCA automatically searches the target domain for publicly available files.
- It collects files such as `.docx`, `.pdf`, `.ppt`, `.xls`, etc.

5. Metadata Extraction

- Select the discovered files and start the metadata extraction process.
- FOCA analyzes the files and retrieves metadata including:
  - Author and company name
  - Creation and modification dates
  - Software and version used
  - Printer or network path information
  - Operating system or usernames

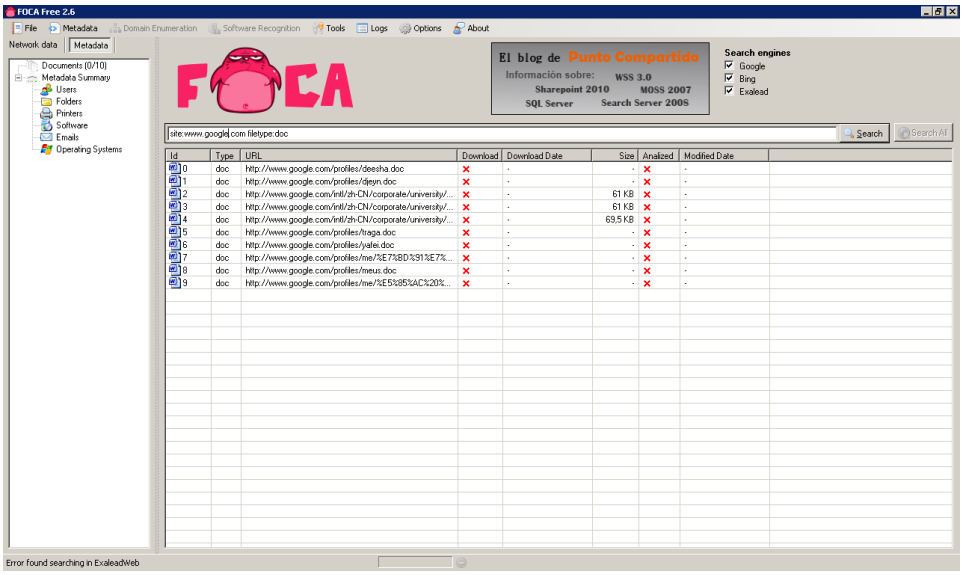
6. Analysis of Extracted Metadata

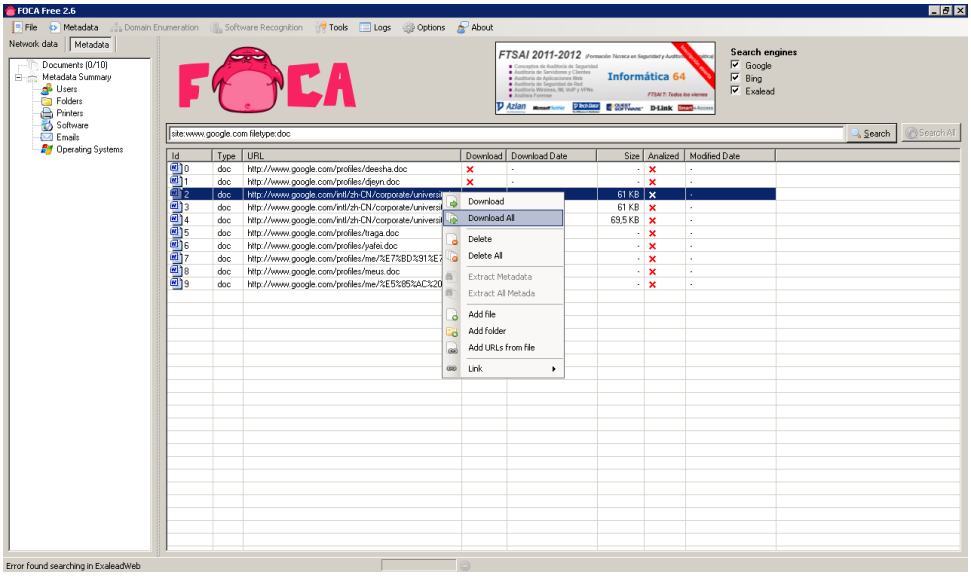
- Review the extracted metadata in FOCA's result window.
- Identify sensitive details that may expose internal organizational information.

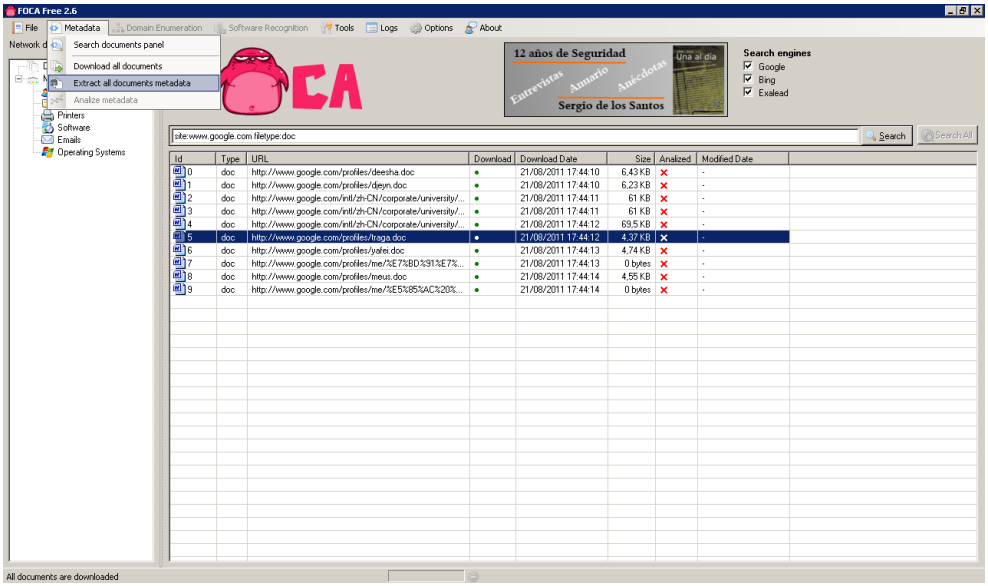
7. Save/Export Results

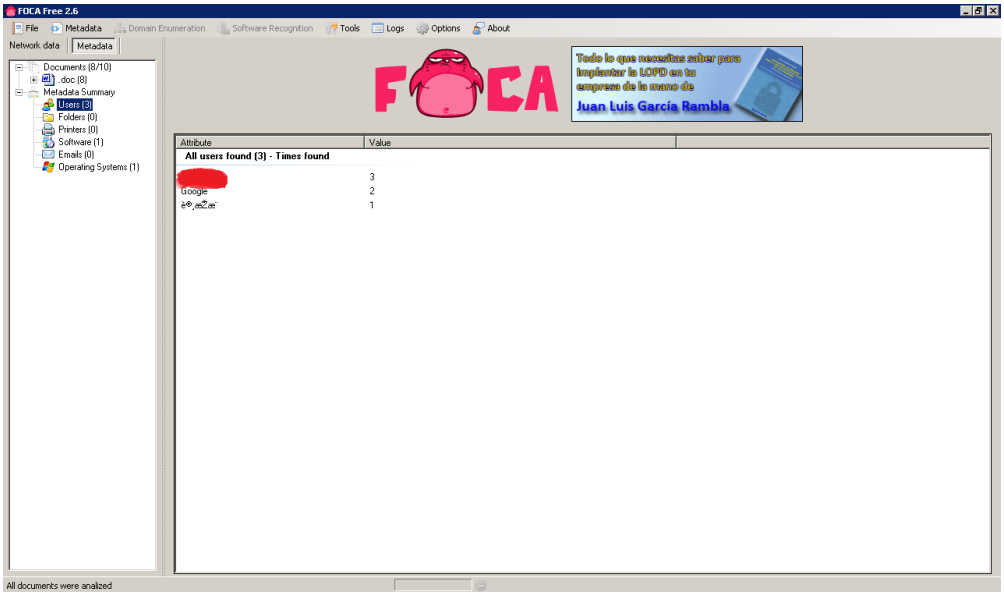
- Export the metadata analysis report for documentation or further investigation.

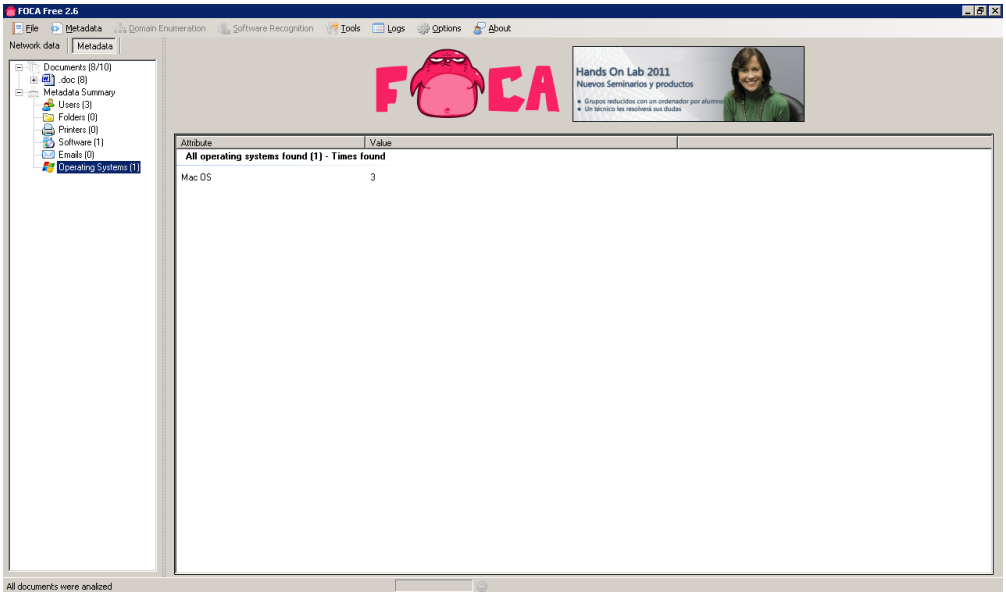
SAMPLE OUTPUT:

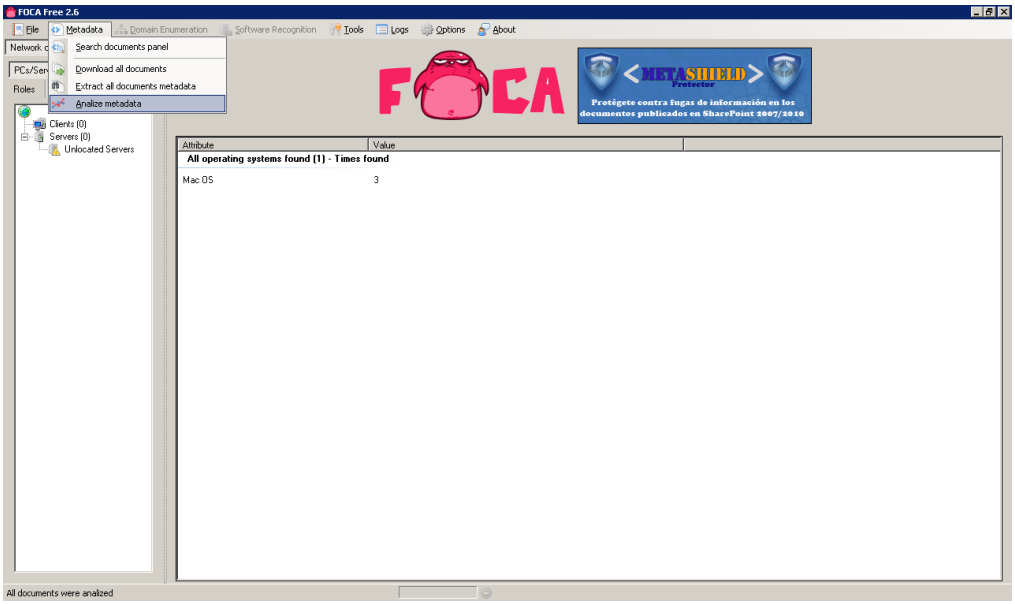


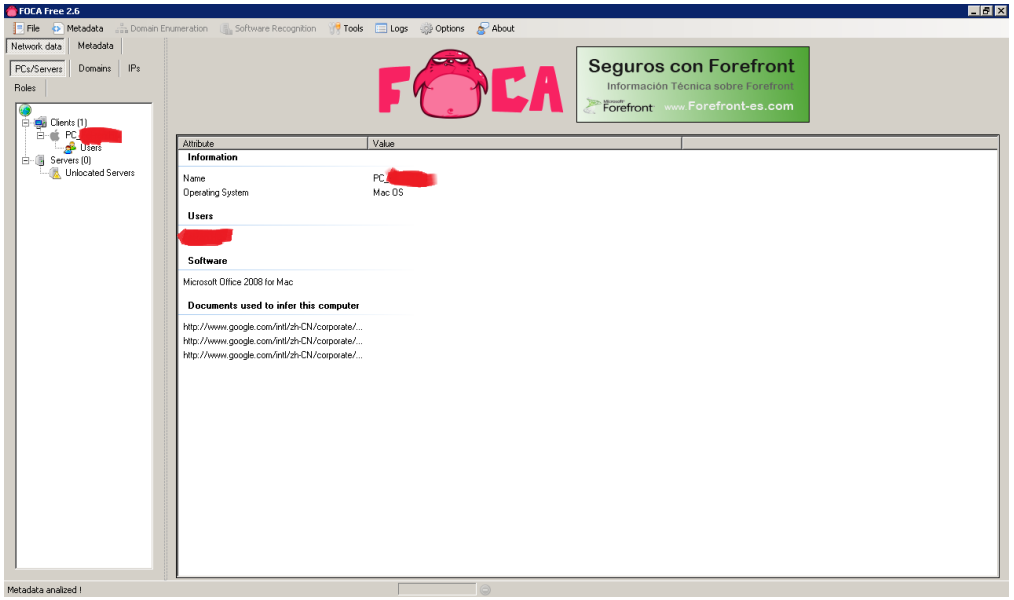


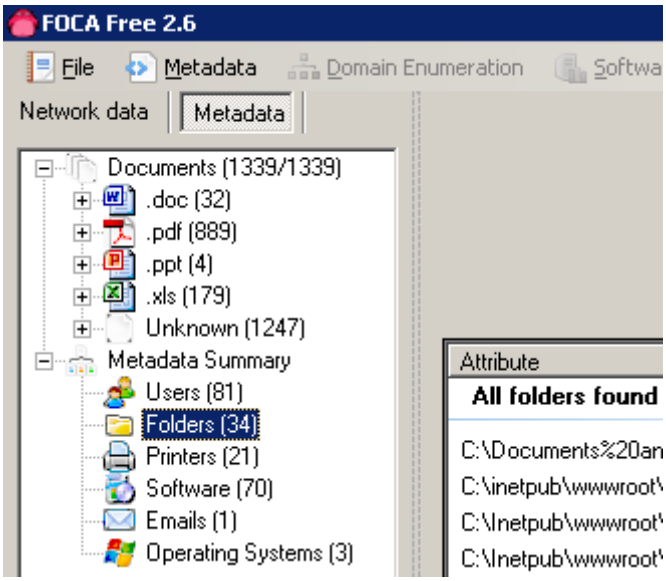

FOCA Free 2.6
File
Metadata
Domain Enumeration
Software Recognition
Tools
Logs
Options
About
Search documents panel
Download all documents
Extract all documents metadata
Analize metadata
Printers
Software
Emails
Operating Systems
12 años de Seguridad
Entrevistas
Anuario
Anécdotas
Una al día
Sergio de los Santos
Search engines
Google
Bing
Exalead
site:www.google.com filetype:doc
Search
Search All
Id
Type
URL
Download
Download Date
Size
Analized
Modified Date
0 doc http://www.google.com/profiles/deesha.doc 21/08/2011 17:44:10 6,43 KB
1 doc http://www.google.com/profiles/djeyn.doc 21/08/2011 17:44:10 6,23 KB
2 doc http://www.google.com/intl/zh-CN/corporate/university/... 21/08/2011 17:44:11 61 KB
3 doc http://www.google.com/intl/zh-CN/corporate/university/... 21/08/2011 17:44:11 61 KB
4 doc http://www.google.com/intl/zh-CN/corporate/university/... 21/08/2011 17:44:12 69,5 KB
5 doc http://www.google.com/profiles/traga.doc 21/08/2011 17:44:12 4,37 KB
6 doc http://www.google.com/profiles/yalei.doc 21/08/2011 17:44:13 4,74 KB
7 doc http://www.google.com/profiles/me/%E7%BD%91%E7%... 21/08/2011 17:44:13 0 bytes
8 doc http://www.google.com/profiles/meus.doc 21/08/2011 17:44:14 4,55 KB
9 doc http://www.google.com/profiles/me/%E5%85%AC%20%... 21/08/2011 17:44:14 0 bytes
All documents are downloaded

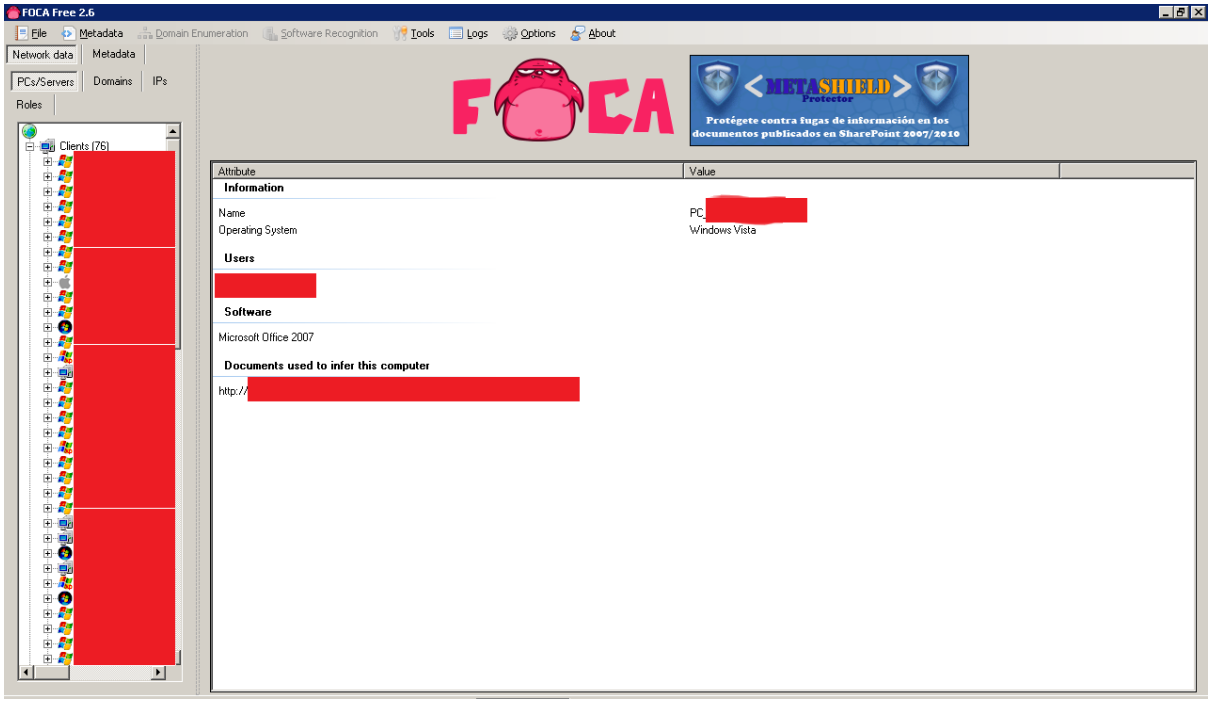

FOCA Free 2.6
File
Metadata
Domain Enumeration
Software Recognition
Tools
Logs
Options
About
Network data
Metadata
Documents (8/10)
.doc (8)
Metadata Summary
Users (3)
Folders (0)
Printers (0)
Software (1)
Emails (0)
Operating Systems (1)
Todo lo que necesitas saber para implantar la LOPD en tu empresa de la mano de
Juan Luis García Rambla
Attribute
Value
All users found (3) - Times found
[redacted] 3
Google 2
1
All documents were analized

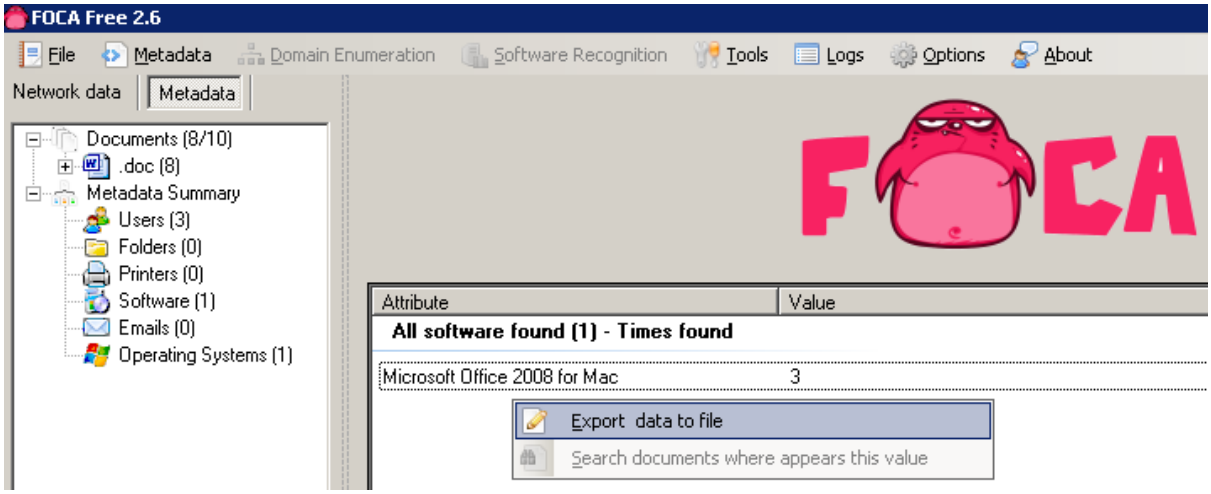

FOCA Free 2.6
File
Metadata
Domain Enumeration
Software Recognition
Tools
Logs
Options
About
Network data
Metadata
Documents (8/10)
.doc (8)
Metadata Summary
Users (3)
Folders (0)
Printers (0)
Software (1)
Emails (0)
Operating Systems (1)
Hands On Lab 2011
Nuevos Seminarios y productos
Attribute
Value
All operating systems found (1) - Times found
Mac OS 3
All documents were analized


FOCA Free 2.6
File
Metadata
Domain Enumeration
Software Recognition
Tools
Logs
Options
About
Search documents panel
Download all documents
Extract all documents metadata
Analize metadata
Clients (0)
Servers (0)
Unlocated Servers
Attribute
Value
All operating systems found (1) - Times found
Mac OS
3
All documents were analized


FOCA Free 2.6
Network data
Metadata
PCs/Servers
Domains
IPs
Roles
Clients (1)
Servers (0)
Unlocated Servers
Seguros con Forefront
Información Técnica sobre Forefront
www.Forefront-es.com
Attribute
Value
Information
Name
Operating System
Mac OS
Users
Software
Microsoft Office 2008 for Mac
Documents used to infer this computer
Metadata analized !


FOCA Free 2.6
File
Metadata
Domain Enumeration
Network data
Metadata
Documents (1339/1339)
.doc (32)
.pdf (889)
.ppt (4)
.xls (179)
Unknown (1247)
Metadata Summary
Users (81)
Folders (34)
Printers (21)
Software (70)
Emails (1)
Operating Systems (3)
Attribute
All folders found
C:\Documents%20an
C:\inetpub\wwwroot\
C:\Inetpub\wwwroot\
C:\Inetpub\wwwroot\


FOCA Free 2.6
File
Metadata
Domain Enumeration
Software Recognition
Tools
Logs
Options
About
Network data
Metadata
PCs/Servers
Domains
IPs
Roles
Clients (76)
FOCA
<METASHIELD>
Protector
Protégete contra fugas de información en los documentos publicados en SharePoint 2007/2010
Attribute
Value
Information
Name
PC
Operating System
Windows Vista
Users
Software
Microsoft Office 2007
Documents used to infer this computer
http://


FOCA Free 2.6
File
Metadata
Domain Enumeration
Software Recognition
Tools
Logs
Options
About
Network data
Metadata
Documents (8/10)
.doc (8)
Metadata Summary
Users (3)
Folders (0)
Printers (0)
Software (1)
Emails (0)
Operating Systems (1)
FOCA
Attribute
Value
All software found (1) - Times found
Microsoft Office 2008 for Mac
3
Export data to file
Search documents where appears this value

OUTPUT:

Pre-Lab Assessment

1. What is metadata?

2. Give two examples of metadata present in a document.

3. Why is metadata analysis important in cybersecurity?

4. What is the main purpose of FOCA?

5. List any two file formats supported by FOCA.

6. Define reconnaissance in ethical hacking.

7. How can attackers misuse metadata?

8. Differentiate between data and metadata.

9. Why should organizations sanitize files before publishing?

10. Mention an alternative tool used for metadata extraction.

Pre-Lab Work

- Install FOCA software from a trusted source.
- Collect a set of sample documents (Word, PDF, PPT) or identify a website with downloadable files.
- Revise concepts of reconnaissance and open-source intelligence (OSINT).
- Ensure proper internet connectivity for live domain analysis.

Post-Lab Assessment

1. What sensitive details can FOCA extract from a file?

2. How can metadata leakage be prevented?

3. Why is FOCA considered an information-gathering tool?

4. Give an example of how attackers may use extracted usernames.

5. What role does FOCA play in ethical hacking?

6. Can FOCA analyze metadata from images?

7. Why is it important to remove metadata before publishing documents online?

8. What is the difference between FOCA and Wireshark in terms of functionality?

9. How can FOCA help digital forensic investigators?

10. Mention a scenario where metadata can directly reveal a vulnerability.

EVALUATION

CONTENT		MAXIMUM MARKS	MARKS OBTAINED
Pre-lab assessment	(A)	10	
Pre-lab work	(B)	20	
Conduct of Experiment	(C)	20	
Data observation	(D)	20	
Analysis and Interpretation	(E)	20	
Post-lab assessment/Viva Voce	(F)	10	
Total (A+B+C+D+E+F)		100	

RESULT:

Thus, metadata extraction using FOCA was successfully performed, and sensitive details such as author names, dates, and software versions were identified, showing the importance of removing metadata before publishing files online.

Exp.No.:2	Network Packet Capture using Wireshark.
DATE:	

AIM:

To capture, view, and analyze network packets using Wireshark.

PROCEDURE:

1. Download and Install Wireshark

- Visit the official Wireshark website: https://www.wireshark.org/download.html.
- Download the appropriate version for your operating system (Windows, macOS, Linux).
- Run the installer and follow the setup wizard.
- During installation, ensure that the **WinPcap/Npcap driver** is installed (mandatory for capturing live network traffic).

2. Launch Wireshark

- After installation, open the Wireshark application.
- The home screen will display all available network interfaces on the system.

3. Select a Network Interface

- Wireshark lists interfaces such as Ethernet, Wi-Fi, and loopback adapters.
- Choose the interface currently being used to access the internet (e.g., Wi-Fi if connected wirelessly).
- The interface with active packet activity (small graph moving up and down) should be selected.

4. Start Capturing Packets

- Click the **blue shark fin icon** (or double-click the interface name) to begin capturing live network packets.
- Once started, packets begin to appear in real time in the packet list pane.

5. Generate Network Traffic (Optional Step for Testing)

- To produce more visible packets during capture, perform some network activity, such as:
  - Opening a web page in a browser.
  - Using the command prompt/terminal to run a `ping` command.
  - Downloading a small file.
- This ensures that different protocols (e.g., ICMP, HTTP, TCP) are visible in the capture.

6. Observe Captured Packets

- Packets will be listed with details such as:
  - **No.** (packet number)
  - **Time** (time of capture)
  - **Source and Destination** (IP addresses)
  - **Protocol** (e.g., TCP, UDP, ICMP, HTTP, ARP)
  - **Info** (summary of the packet contents)
- Each packet can be expanded into three sections:
  - **Packet Details Pane:** Shows protocol layers in a tree structure.
  - **Packet Bytes Pane:** Displays raw packet data in hexadecimal and ASCII.

7. Apply Capture/Display Filters

- Use filters to narrow down the captured traffic for analysis:
  - `icmp` → Shows only ping packets.
  - `http` → Displays only HTTP requests and responses.
  - `ip.addr == 192.168.1.1` → Captures traffic from/to a specific IP address.
- Filters make it easier to focus on relevant traffic types.

8. Stop Packet Capture

- Once sufficient packets are captured, click the **red square Stop button**.
- The captured packets remain in Wireshark for offline analysis.

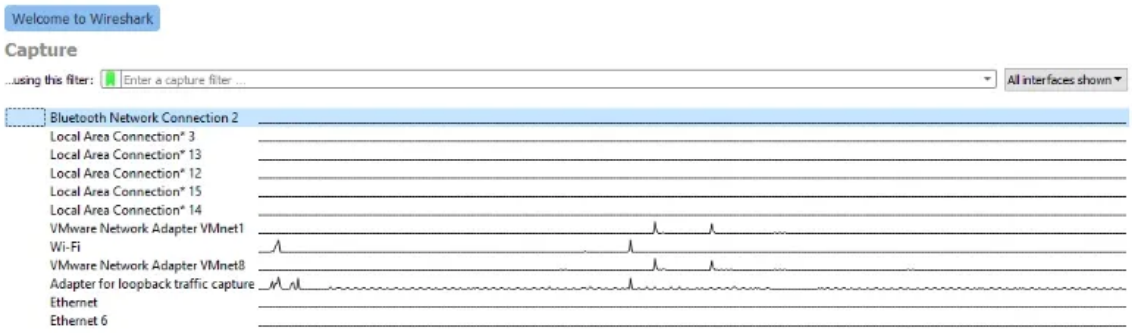
9. Analyze the Packets in Detail

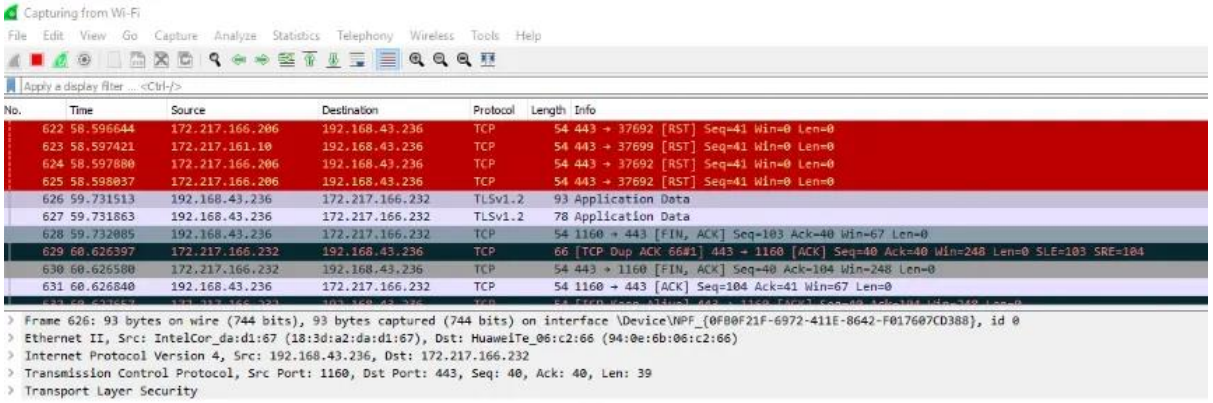
- Select any packet and expand its details to study:
  - Ethernet header (MAC addresses).
  - IP header (source and destination IPs, TTL, etc.).
  - TCP/UDP header (ports, sequence numbers).
  - Application-level data (HTTP requests, DNS queries).

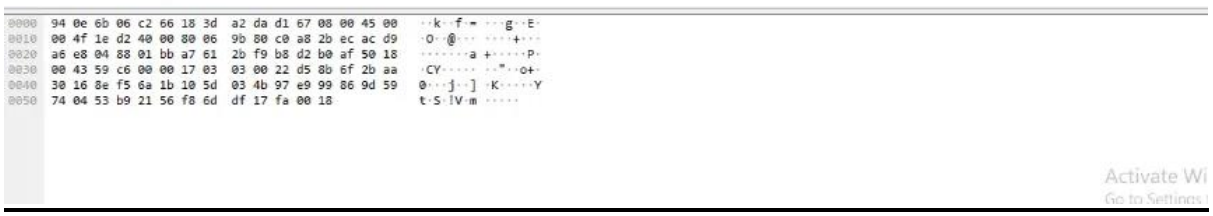
10. Save the Capture (Optional)

- Save the captured data for future reference:
  - Go to **File → Save As**.
  - Save the file in `.pcap` or `.pcapng` format.
- The saved file can later be reopened in Wireshark for additional analysis.

SAMPLE OUTPUT:







OUTPUT:

Pre-Lab Assessment

1. What is a packet in networking?

2. Define packet sniffing.

3. Name two common protocols that Wireshark can capture.

4. What is the purpose of using filters in Wireshark?

5. Which OSI layer deals with IP addressing?

6. Can Wireshark capture encrypted traffic? Explain briefly.

7. What is the difference between TCP and UDP?

8. Why is packet analysis important in cybersecurity?

9. What is the role of Npcap/WinPcap in Wireshark?

10. Give one practical use of Wireshark in troubleshooting.

Pre-Lab Work

- Install Wireshark and ensure Npcap/WinPcap drivers are available for live capture.
- Review the basics of computer networks (IP, TCP, UDP, ICMP, HTTP).
- Identify the active network interface (Wi-Fi or Ethernet) to be used during the experiment.
- Prepare a simple network activity (such as browsing a website or using the `ping` command) to generate traffic during the capture.

Post-Lab Assessment

1. What types of information can be extracted from captured packets?

2. Give an example of a display filter used in Wireshark.

3. How can Wireshark help in detecting malicious network activity?

4. What is the significance of the three-pane view in Wireshark?

5. Why should packet captures be stopped at the right time?

6. What does the “Info” column in Wireshark represent?

7. Differentiate between live capture and offline analysis.

8. Which pane shows the raw hexadecimal data of a packet?

9. How can captured data be saved for later analysis?

10. Why is Wireshark considered both powerful and risky if misused?

EVALUATION

CONTENT		MAXIMUM MARKS	MARKS OBTAINED
Pre-lab assessment	(A)	10	
Pre-lab work	(B)	20	
Conduct of Experiment	(C)	20	
Data observation	(D)	20	
Analysis and Interpretation	(E)	20	
Post-lab assessment/Viva Voce	(F)	10	
Total (A+B+C+D+E+F)		100	

RESULT:

Thus, network packet capture using Wireshark was successfully carried out, and live packets were analyzed to understand protocols, traffic flow, and network behavior.