



INT301 – Open-Source Technologies

PROJECT REPORT

(Project Semester January-May 2023)

Submitted by:

Chetna

Registration No: - 11901402

Section: KE040

Course Code: **INT301**

Under the Guidance of **Dr. Manjot Kaur: 28925 Assistant Professor.**

The domain of CSE/IT

**Lovely School of Computer Science and Engineering**

## CERTIFICATE

This is to certify that Ms. Chetna bearing Registration no 11901402 has completed the INT301: Open-Source Technologies project “To tamper ARP table of the victim machine and sniff network traffic between the victim and server.” under my guidance and supervision. To the best of my knowledge, the present work is the result of his/her initial development, effort, and study.

### Signature and Name of the Supervisor Designation of the Supervisor

**School of Computer Science and Engineering**

Lovely Professional University Phagwara, Punjab.

Date: 7/03/2023

## DECLARATION

I, **Chetna**, student of **Open-Source Technologies (INT301)** under CSE/IT Discipline at, Lovely Professional University, Punjab, at this moment declare that all the information furnished in this project report is based on my own intensive work and is genuine.

Date: 7/04/2023 Signature: Chetna (11901402)

Registration No.: 11901402

Name of the student: Ms. Chetna

**ACKNOWLEDGEMENT**

I would like to express my gratitude and appreciation to all those who gave me moral support and help to complete this report. Special thanks to my supervisor Mrs. Manjot Kaur whose help, stimulating suggestions, and encouragement always helped me during the Completion process and in writing this report. I also sincerely thank you for the time spent proofreading and correcting my many mistakes.

I would also like to acknowledge with much appreciation the crucial role of the students from my class, who gave me motivation and Guidance while completing my project. Many thanks go to all lecturers and supervisors who have given their full effort in guiding me in achieving the goal as well as their encouragement to maintain our progress track. My profound thanks go to all my classmates, especially to my friends for spending their time helping and giving support whenever I need it in my project.

**Introduction**

A MITM (Man-in-the-Middle) attack is a type of cyber attack where an attacker intercepts communication between two parties who believe they are directly communicating with each other. The attacker intercepts, alters, or manipulates the communication in real-time, making it difficult for the two parties to detect the attack.

In a typical MITM attack, the attacker positions themselves between the two parties, intercepting their communication and potentially stealing sensitive information like passwords, credit card numbers, or other personal data. This can be done in several ways, such as by intercepting unencrypted data over public Wi-Fi networks, by using malware to compromise one or both of the parties' devices, or by exploiting vulnerabilities in the communication protocol being used.

MITM attacks can have serious consequences, as they can result in financial loss, identity theft, or other forms of fraud. To protect against MITM attacks, it is recommended to use secure communication protocols such as SSL/TLS, to avoid public Wi-Fi networks, to use strong and unique passwords, and to keep software and security systems up to date.

MITM attacks can take many forms and can be conducted through various means, including physical, network, or software-based attacks. Some examples of MITM attacks include:

* Wi-Fi eavesdropping: An attacker can intercept unencrypted Wi-Fi traffic by setting up a rogue access point and masquerading as a legitimate Wi-Fi network. This allows them to intercept sensitive information transmitted over the network.
* ARP spoofing: In this attack, an attacker sends fake Address Resolution Protocol (ARP) messages to the network, tricking devices into sending their traffic to the attacker's device instead of the intended destination.
* DNS spoofing: An attacker can spoof the Domain Name System (DNS) and redirect users to fake websites that look like legitimate ones, stealing their login credentials or personal information.
* Email spoofing: Attackers can use phishing emails to trick users into clicking on links that lead to fake websites, allowing the attacker to capture sensitive information.
* SSL stripping: An attacker can force a website to use an unencrypted connection instead of a secure one, allowing them to intercept and read the data being transmitted.

**ARP attack**

An ARP (Address Resolution Protocol) attack is a type of network attack in which an attacker sends fake or spoofed ARP messages to a network in order to associate the attacker's MAC address with the IP address of another device on the network.

ARP is a protocol used to map a network address (such as an IP address) to a physical address (such as a MAC address) on a local network. In an ARP attack, the attacker can use ARP messages to associate their MAC address with the IP address of a legitimate device on the network, causing network traffic to be routed to the attacker instead of the intended recipient.

There are different types of ARP attacks, including ARP cache poisoning, ARP spoofing, and ARP flooding. These attacks can be used to intercept network traffic, steal sensitive information, and perform other malicious activities.

To prevent ARP attacks, network administrators can use techniques such as ARP spoofing detection, network segmentation, and implementing security measures like MAC address filtering and VLANs (Virtual Local Area Networks).

ARP Cache Poisoning: In this type of attack, the attacker sends fake ARP messages to the victim's device, telling it that the MAC address associated with a specific IP address has changed. The victim's device updates its ARP cache with the attacker's MAC address, and all traffic intended for the original IP address is sent to the attacker's machine.

ARP Spoofing: This is a more targeted version of ARP cache poisoning. The attacker spoofs the MAC address of a legitimate device on the network in order to intercept its traffic or gain access to sensitive information.

ARP Flooding: In this type of attack, the attacker sends a large number of fake ARP messages to flood the ARP cache of the victim's device, causing it to become overwhelmed and potentially crash.

ARP attacks are often used in conjunction with other types of attacks, such as man-in-the-middle attacks, where the attacker intercepts and modifies network traffic between two devices.

To protect against ARP attacks, network administrators can implement measures such as:

* Using ARP spoofing detection software to detect and block ARP spoofing attempts.
* Implementing network segmentation to limit the scope of an ARP attack.
* Using MAC address filtering to restrict network access to only authorized devices.
* Using VLANs to separate different parts of the network and limit the impact of an ARP attack.
* Regularly monitoring network activity and looking for signs of ARP attacks.

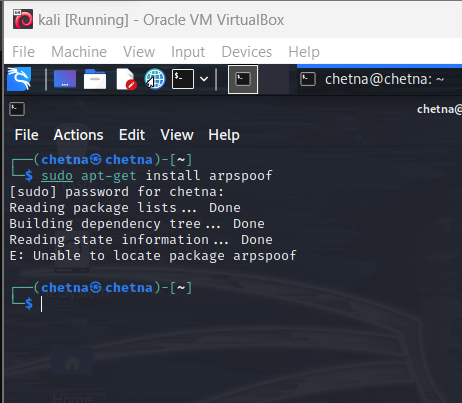
**Defences that can be used against ARP attacks:**

1. ARP spoofing prevention software: This type of software can detect and block ARP spoofing attempts by comparing the MAC address of incoming packets with the ARP cache on the device.
2. Static ARP tables: Network administrators can use static ARP tables to manually assign MAC addresses to specific IP addresses, which can prevent attackers from successfully modifying the ARP cache.
3. Network access controls: Limiting network access to only authorized devices can reduce the risk of an attacker gaining access to the network and launching an ARP attack.
4. Encryption: Using encryption to protect sensitive data in transit can make it more difficult for attackers to intercept and steal information.
5. Network monitoring: Regularly monitoring network activity and analysing traffic patterns can help detect signs of ARP attacks, such as an unusual amount of ARP traffic on the network.
6. Segmentation: Separating the network into smaller, more manageable segments can limit the scope of an ARP attack and prevent an attacker from compromising the entire network.
7. Virtual Private Networks (VPNs): Using a VPN to connect to the network can provide an additional layer of security by encrypting all network traffic and preventing attackers from intercepting sensitive information.
8. Port Security: Network switches can be configured to limit the number of MAC addresses allowed on each switch port, preventing attackers from using multiple MAC addresses to carry out an ARP attack.
9. DHCP Snooping: Dynamic Host Configuration Protocol (DHCP) snooping can be used to prevent attackers from using rogue DHCP servers to carry out an ARP attack. DHCP snooping can validate DHCP messages to ensure they are coming from authorized DHCP servers.
10. Network Behaviour Analysis (NBA): Network Behaviour Analysis can be used to identify suspicious network activity that may be indicative of an ARP attack. This approach involves analysing network traffic patterns to detect anomalies that may indicate an attack.
11. Intrusion Detection/Prevention Systems (IDS/IPS): IDS/IPS can be used to detect and prevent ARP attacks by analysing network traffic and comparing it against known attack patterns.
12. Network Access Control (NAC): NAC can be used to ensure that only authorized devices are allowed to connect to the network. NAC solutions can validate the identity of devices and enforce security policies to prevent unauthorized access.
13. Endpoint Protection: Endpoint protection software can be installed on devices to protect them from malware that may be used to carry out an ARP attack.
14. Network Access Control Lists (ACLs): ACLs can be used to control network traffic by defining rules that determine which devices are allowed to communicate with each other. This can help prevent unauthorized access and limit the scope of an ARP attack.
15. Regular Software Updates: Regularly updating network devices and software can help prevent vulnerabilities that can be exploited by attackers to carry out an ARP attack.
16. Employee Training: Educating employees about the risks of ARP attacks and how to detect and prevent them can help reduce the likelihood of an attack being successful.
17. Incident Response Plan: Having an incident response plan in place can help network administrators respond quickly and effectively to an ARP attack. The plan should include procedures for identifying and containing the attack, as well as steps for restoring network functionality.
18. Network Virtualization: Network virtualization can help improve network security by creating isolated virtual networks that can be accessed only by authorized users. This approach can help prevent ARP attacks by limiting the number of devices that can communicate with each other.
19. Security Information and Event Management (SIEM): SIEM solutions can be used to monitor network activity and detect potential security incidents, including ARP attacks. SIEM tools can collect and analyse data from multiple sources to identify patterns of suspicious behaviour.
20. Network Segmentation: Network segmentation can help prevent ARP attacks by dividing the network into smaller, more manageable segments. Each segment can be secured independently, making it more difficult for attackers to gain access to sensitive information.
21. User Authentication: Requiring users to authenticate themselves before accessing the network can help prevent unauthorized access and limit the risk of an ARP attack. This can involve using a username and password, as well as additional authentication measures such as biometric data or security tokens.
22. Secure Network Design: Network administrators can design the network in such a way as to minimize the risk of ARP attacks. This can involve using technologies such as virtual private networks (VPNs) to encrypt traffic, as well as implementing network security best practices such as using firewalls, intrusion detection systems, and anti-virus software.
23. Network Forensics: Network forensics can help detect and investigate ARP attacks by collecting and analysing network data. This approach can be used to identify the source of the attack and gather evidence that can be used in legal proceedings.
24. Least Privilege: Limiting user privileges to only the resources they need to perform their job duties can help prevent unauthorized access and limit the risk of an ARP attack. This approach involves giving users the minimum level of access required to perform their job functions.
25. Network Encryption: Encrypting network traffic can help prevent attackers from intercepting sensitive information, including ARP packets. This can involve using protocols such as Transport Layer Security (TLS) or Secure Sockets Layer (SSL) to encrypt network traffic.
26. Network Address Translation (NAT): NAT can help prevent ARP attacks by translating public IP addresses to private IP addresses, making it more difficult for attackers to identify and target specific devices on the network.
27. Network Segregation: Segregating the network into separate VLANs can help prevent ARP attacks by limiting the number of devices that can communicate with each other. This approach can be used to create separate network segments for different departments or functions within an organization.
28. Reducing Attack Surface: Minimizing the number of devices and services on the network can help reduce the attack surface and limit the risk of an ARP attack. This can involve removing unnecessary devices and disabling unused services.
29. Penetration Testing: Regularly conducting penetration testing can help identify vulnerabilities in the network and test the effectiveness of the defences against ARP attacks and other types of network attacks.

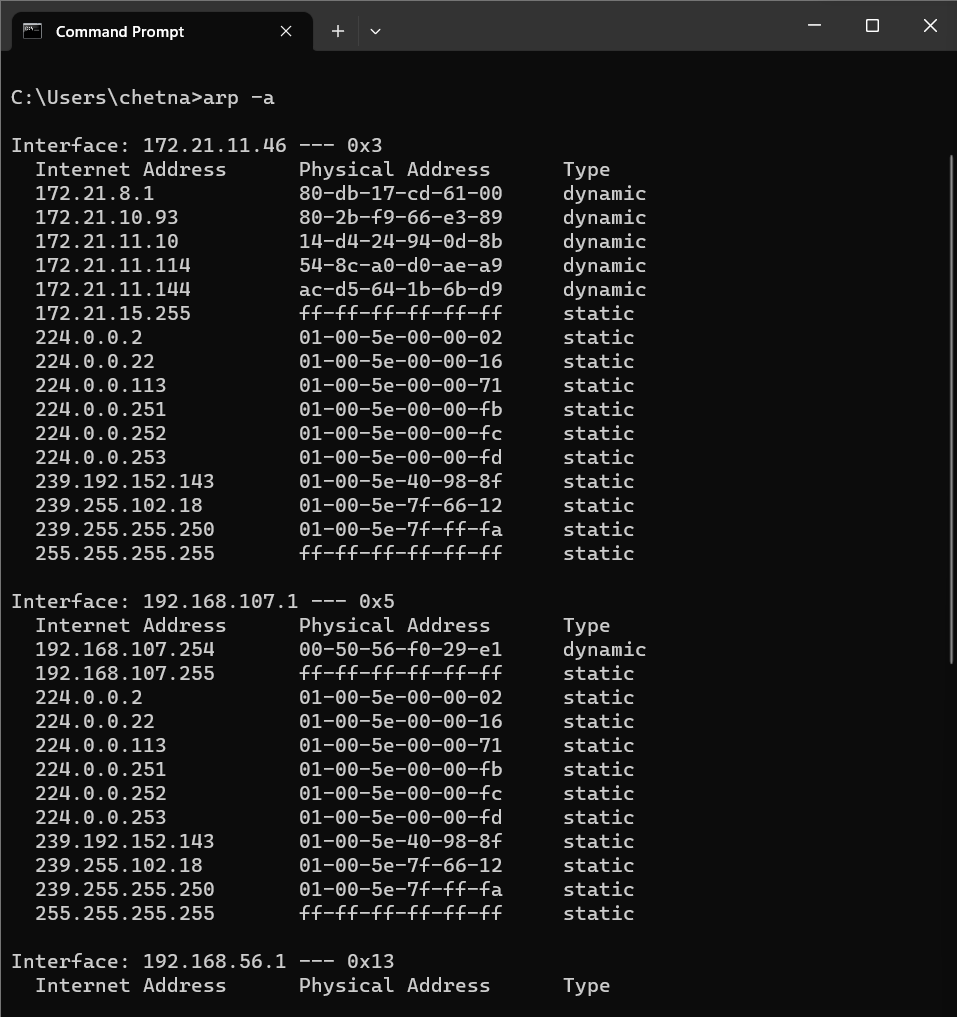
**Report analysis and system snapshots:**

1. **Instaling ARP spoof :**

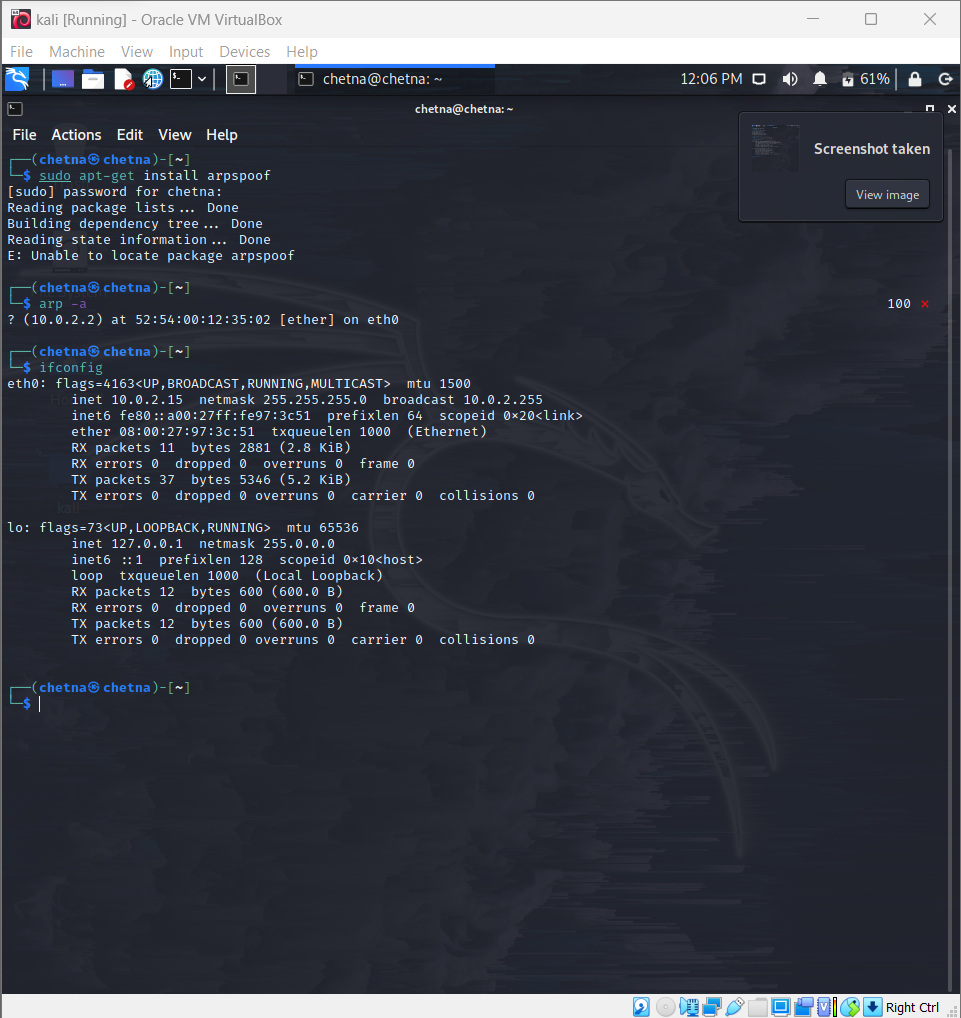
arpspoof is a command-line tool that is part of the dsniff package. To install dsniff and arpspoof.

****

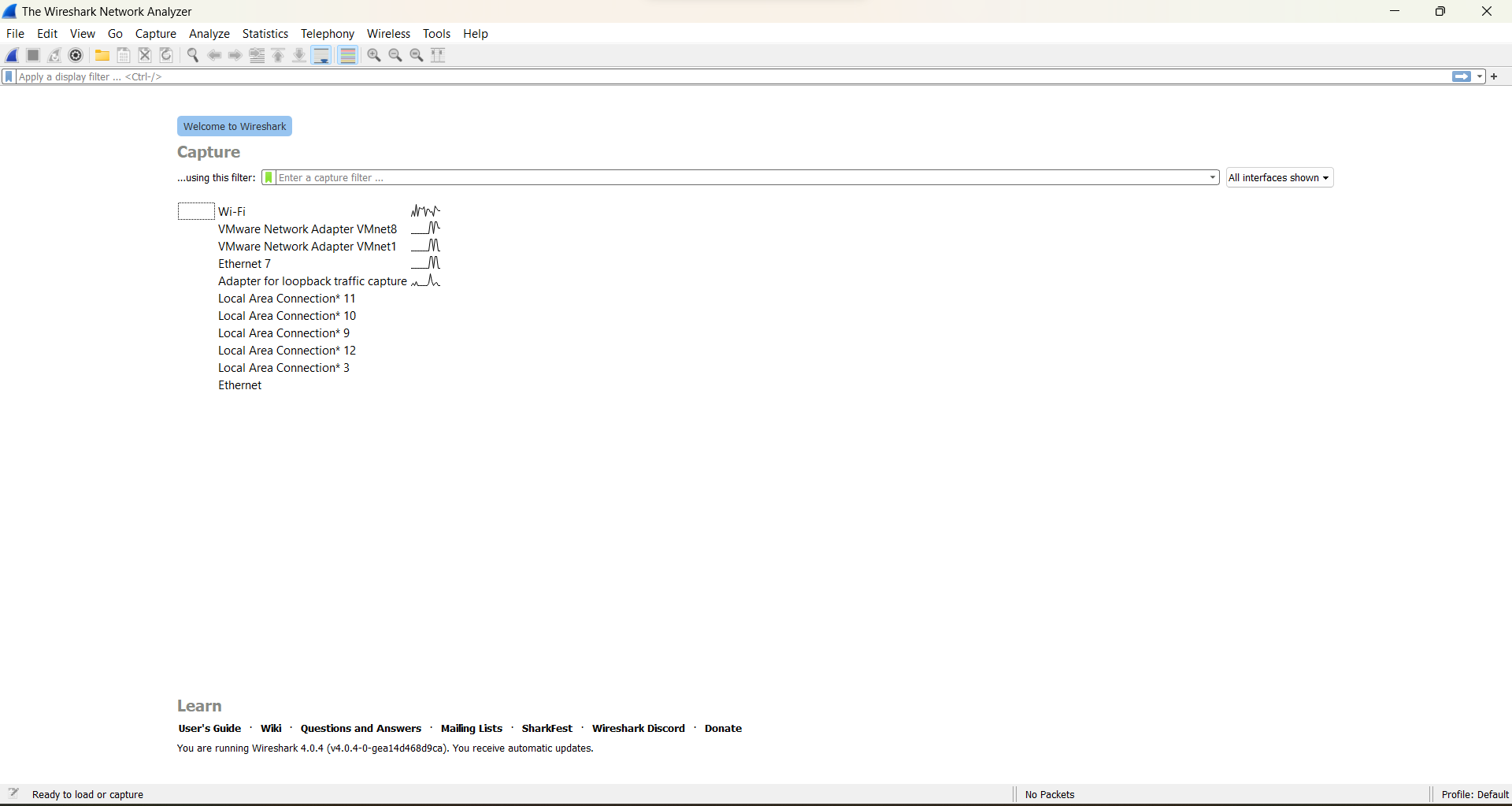
1. **Retrieving IP from command prompt :**

****

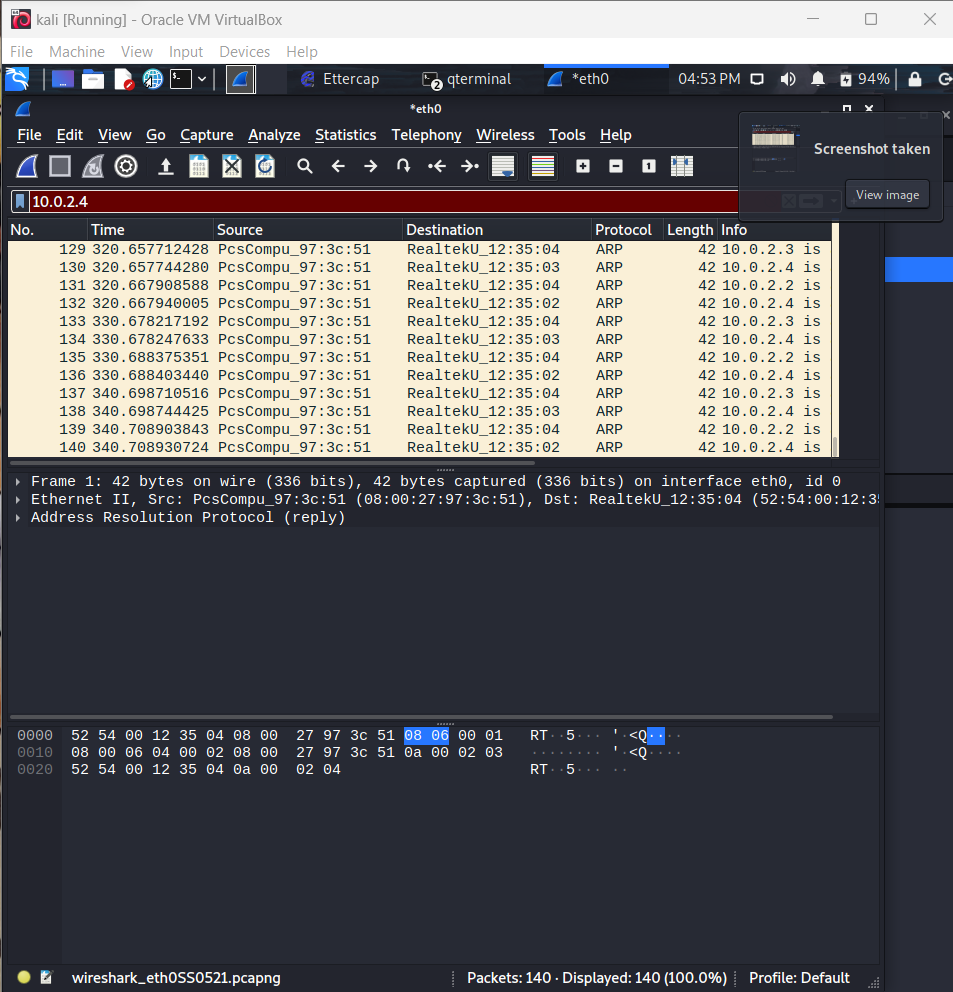
1. **Retriving IP from lunix mechine :**

****

1. **using wireshark to capture traffic from the servers**



1. **traffic captured using wire shark :**



Reference/Bibliography:

1. FileZilla Reference Documentation: <https://filezilla-project.org/documentation/>
2. WinSCP Documentation: <https://winscp.net/eng/docs/>
3. "FileZilla vs. WinSCP: Which Is the Best FTP Client for You?" by Jeffery Hicks, published in Redmond Magazine: <https://redmondmag.com/articles/2017/07/01/filezilla-vs-winscp.aspx>
4. "FileZilla vs WinSCP: Which One is Right for Your Needs?" by John Corpuz, published in Tom's Guide: [https://www.tomsguide.com/us/filezilla-vs-winscp,review-2127.html](https://www.tomsguide.com/us/filezilla-vs-winscp%2Creview-2127.html)
5. "5 Best FTP Client Software for Windows 10" by Hammad Baig, published on TechWiser: <https://techwiser.com/best-ftp-client-software-for-windows/>
6. "Best Free FTP Clients on Windows" by Sagar Basak, published on Beebom: https://beebom.com/best-free-ftp-clients-windows/
7. WinSCP Guide: https://winscp.net/eng/docs/start