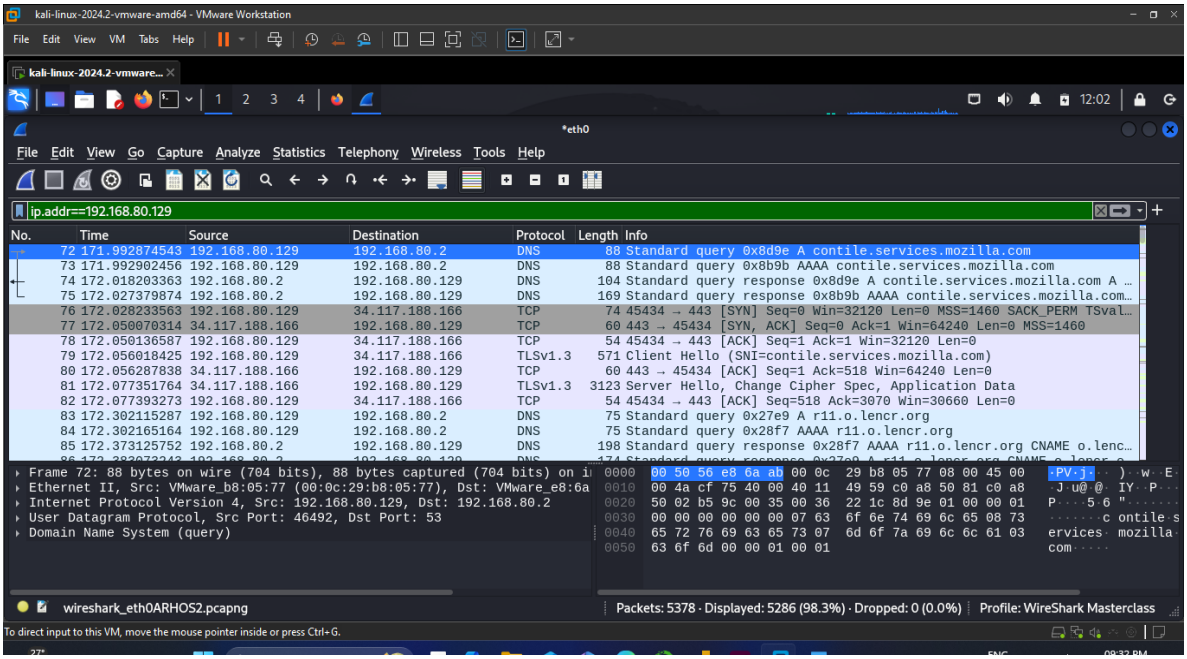
WIRESHARK

Functions to Perform:

1. Display Filters:

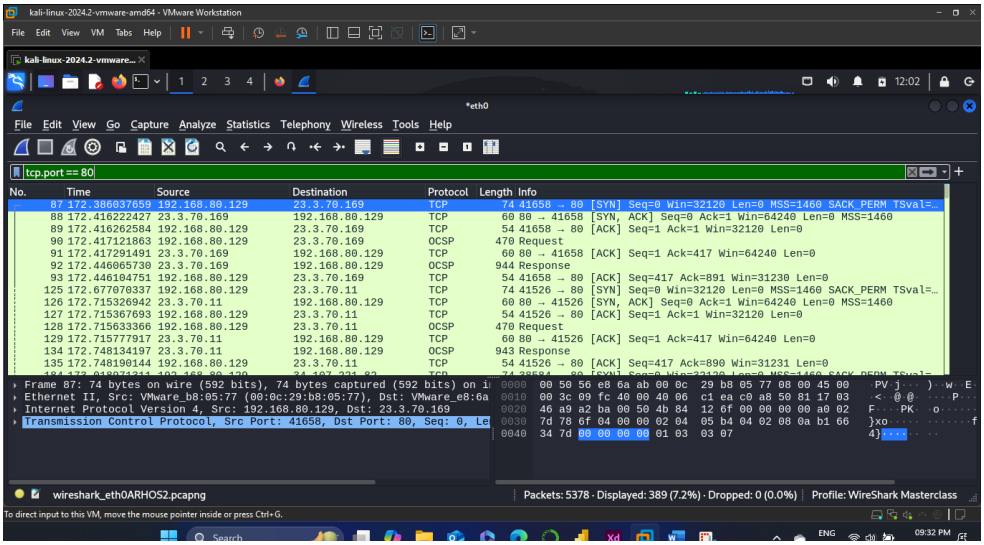
- **Basic IP Filter:**

  ip.addr == 192.168.80.129 — Show packets with the specified IP address as either the source or destination.



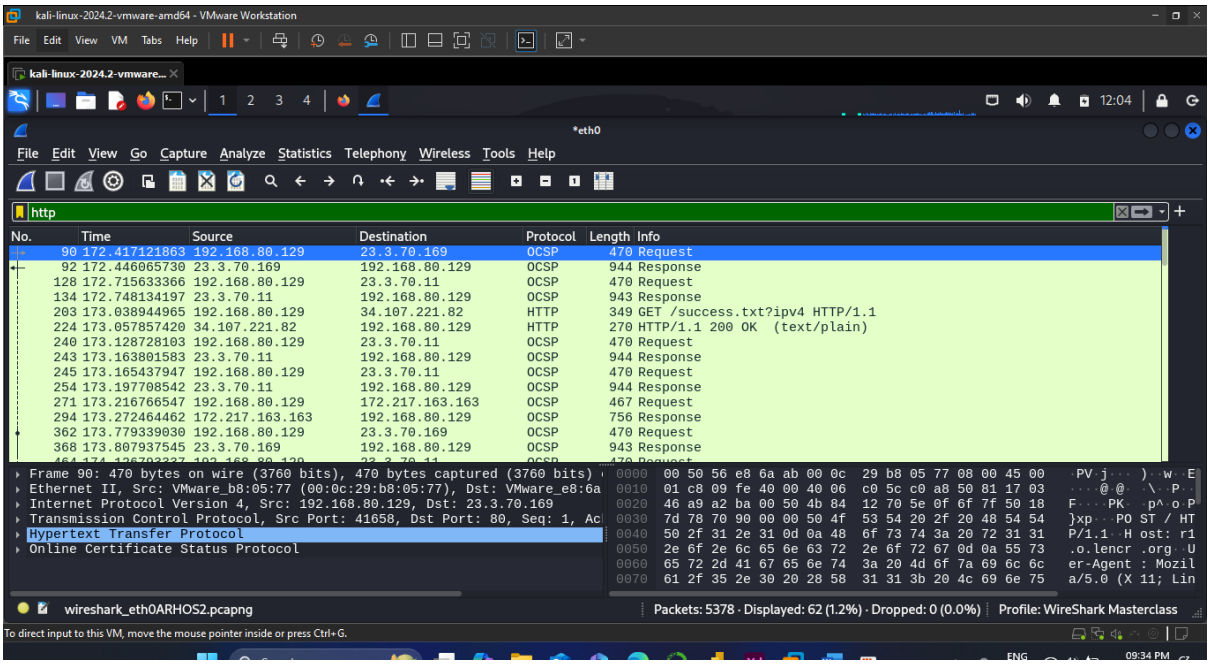
- **Port Filter:**

  tcp.port == 80 — Show only TCP traffic on port 80.



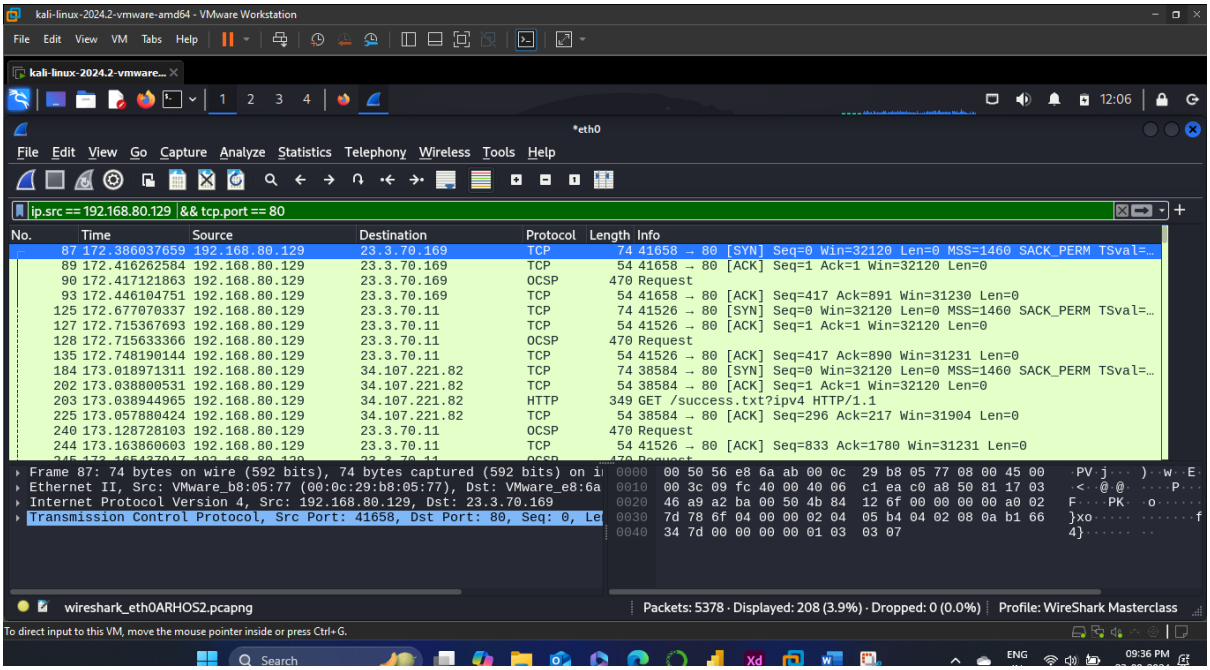
- **Protocol Filter:**

  http — Display only HTTP traffic.



- **Multiple Conditions:**

  ip.src == 192.168.80.129 && tcp.port == 80 — Show packets from IP 192.168.1.1 going to TCP port 80.



2. Capture Filters:

Capture filters in Wireshark are used to limit the amount of data that Wireshark captures. By applying capture filters, you can focus on specific types of network traffic, making it easier to analyze relevant data and reduce the amount of irrelevant information captured.

Basic IP Filter:

host 192.168.80.129 — Capture traffic to and from a specific IP address.

Port Filter:

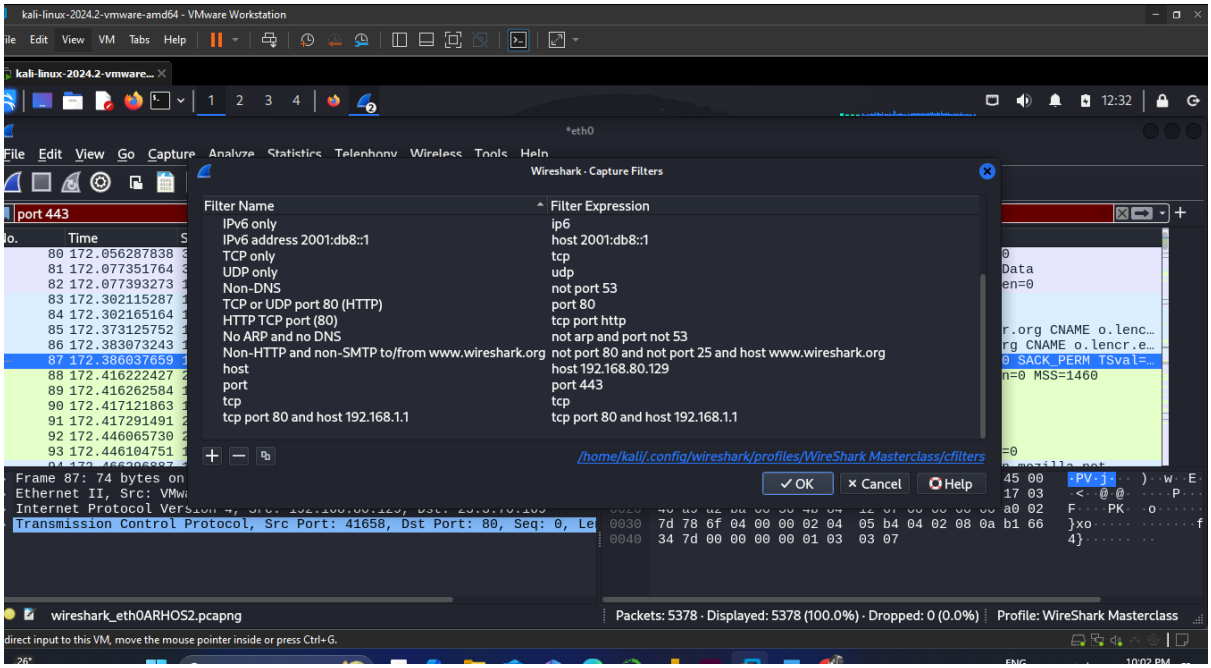
port 443 — Capture traffic on port 443 (usually HTTPS).

Protocol Filter:

tcp — Capture only TCP traffic.

Multiple Conditions:

tcp port 80 and host 192.168.1.1 — Capture TCP traffic on port 80 from or to a specific IP address.



3. Common Shortcuts in Wireshark GUI:

- **Start/Stop Capture:**

  Ctrl + E — Start or stop capturing packets (start recording and stop recording packet icon)

- **Open Capture File:**

  Ctrl + O — Open a previously saved capture file. (Open existing captures present in directory)

- **Save Capture File:**

  Ctrl + S — Save the current capture to a file. (Save the file)

- **Apply Display Filter:**

  Ctrl + / — Jump to the filter bar to enter or edit a display filter.

- **Clear Display Filter:**

  Ctrl + \ — Clear the current display filter.

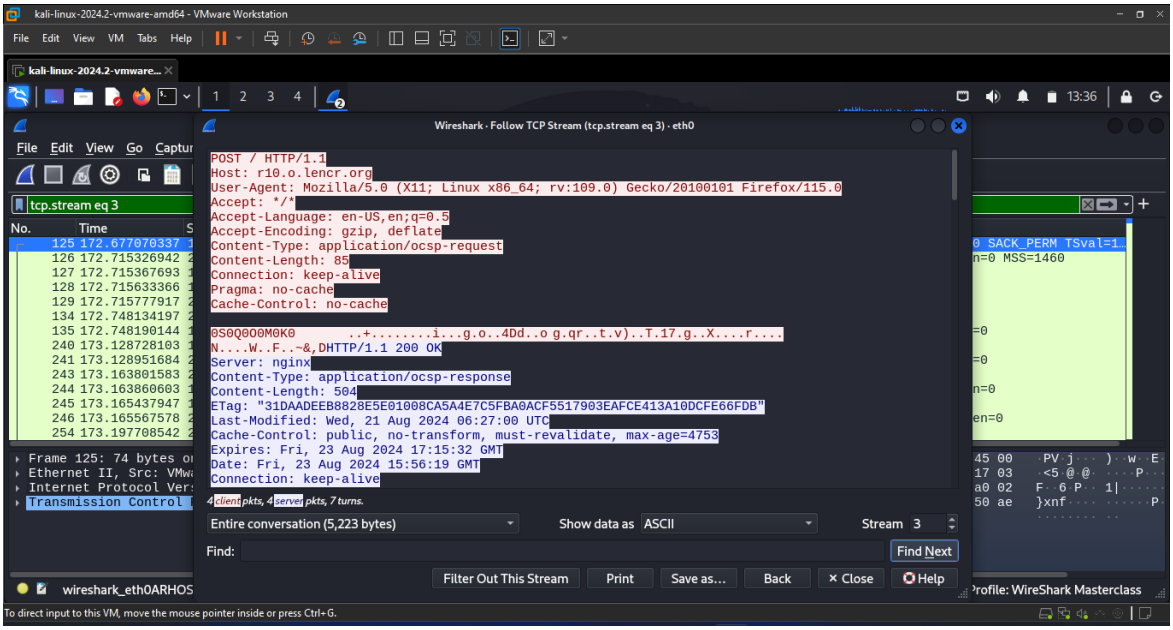
- **Find a Packet:**

  Ctrl + F — Open the "Find Packet" dialog to search for packets based on specific criteria.

4. Advanced Filters and Commands:

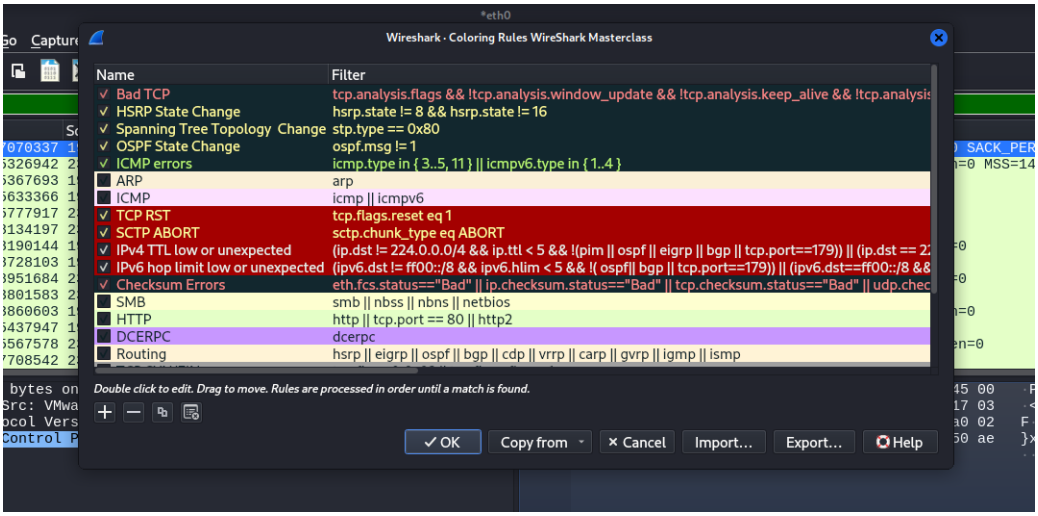
- **Follow TCP Stream:**

Right-click a TCP packet → Select "Follow" → Choose "TCP Stream" — This allows you to view the entire conversation for that stream.



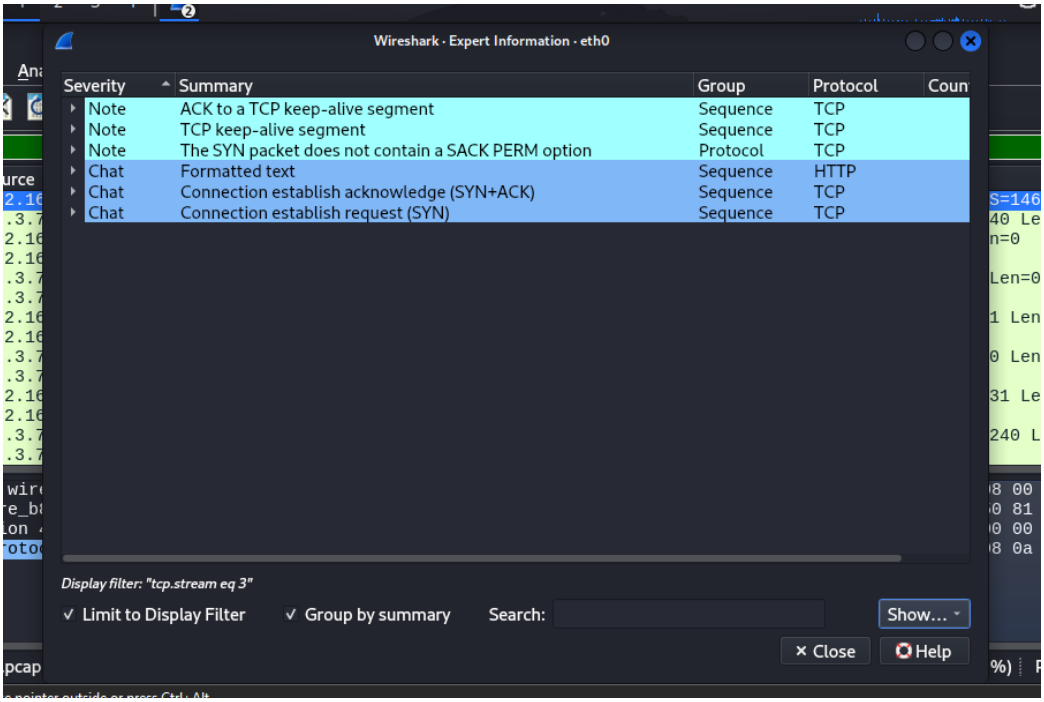
- **Colorize Traffic:**

Wireshark allows custom coloring rules to visually differentiate traffic types or anomalies. Go to View → Coloring Rules to customize.



- **Expert Information:**

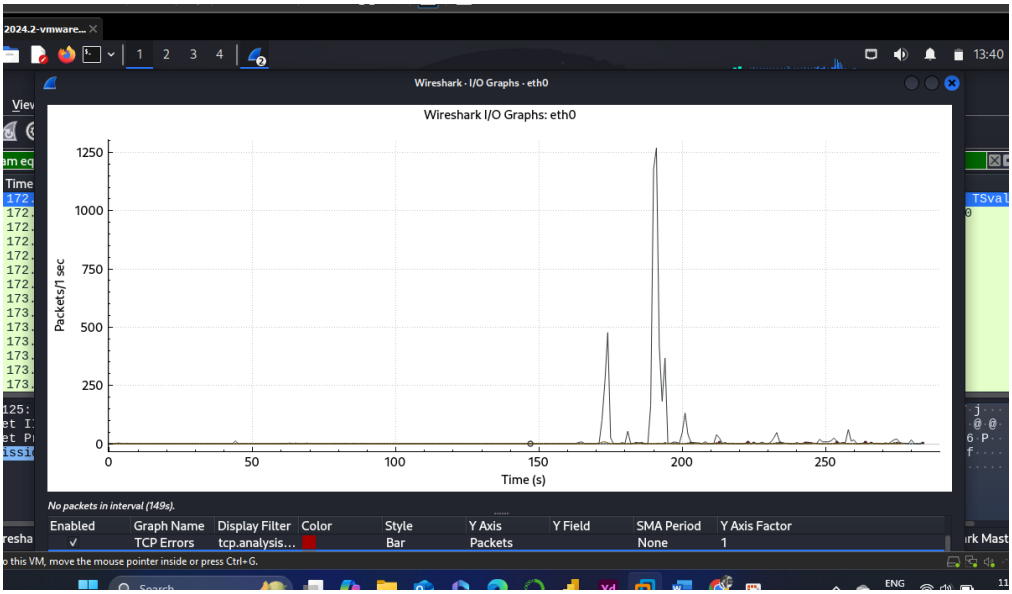
Analyze → Expert Information — This provides a summary of potential issues detected during the capture (e.g., retransmissions, checksum errors).



5. IO Graphs:

- **Open IO Graph:**

Statistics → IO Graphs — View traffic data over time, which can help identify trends or anomalies.



- **Customize Graphs:**

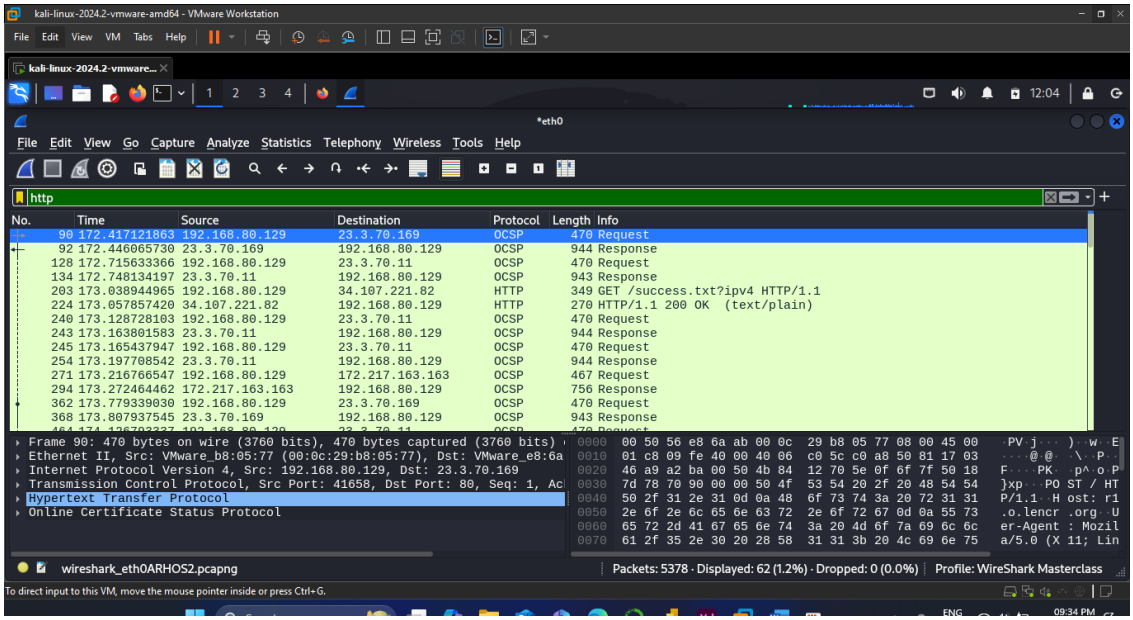
Customize the graph to display different data types (e.g., packet counts, byte counts, etc.) and apply filters to isolate specific traffic.

Related to Network:

1. Identifying Unencrypted Traffic

- **HTTP Traffic:**

http — Displays all HTTP traffic, which is unencrypted and can reveal sensitive data like usernames and passwords.



- **FTP Traffic:**

ftp — Displays FTP traffic, where credentials and data are transmitted in plaintext, making them vulnerable to interception.

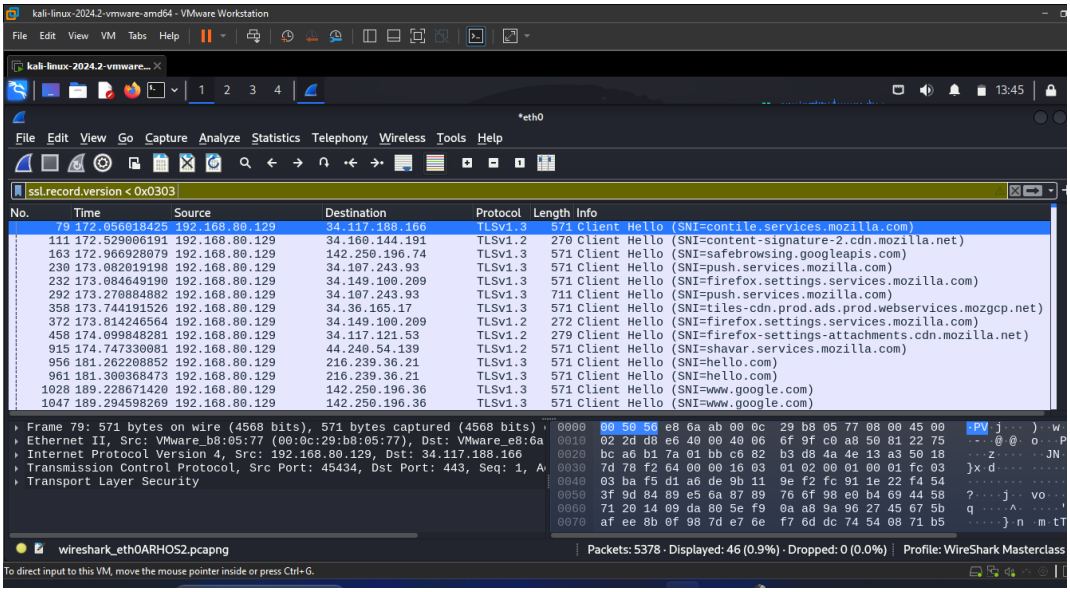
- **Telnet Traffic:**

telnet — Displays Telnet traffic, another protocol that transmits data, including passwords, in plaintext.

2. Detecting Use of Deprecated or Weak Protocols

- **SSL/TLS Versions:**

ssl.record.version < 0x0303 — Filters traffic for SSL/TLS versions older than TLS 1.2, which are considered vulnerable.



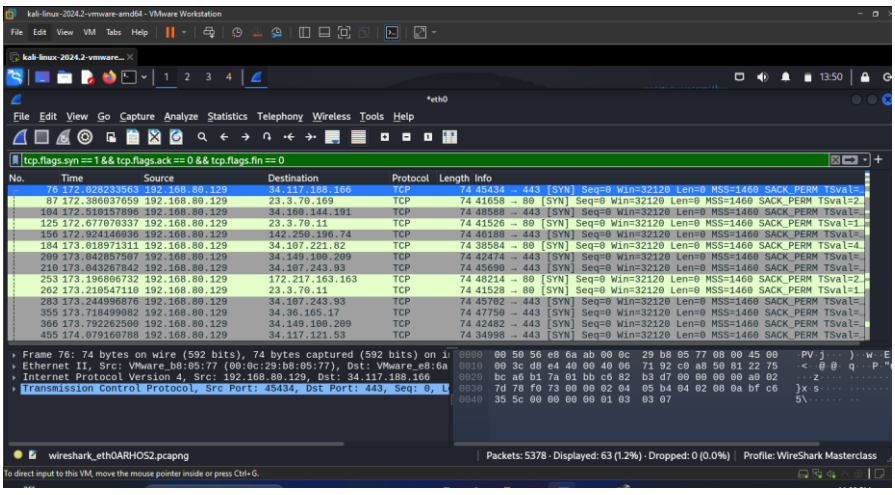
- **SMBv1 Traffic:**

smb && smb.version == 1 — Identifies traffic using SMBv1, a protocol known for its vulnerabilities, like those exploited by the WannaCry ransomware.

3. Analyzing Traffic for Signs of Malicious Activity

- **Port Scanning:**

tcp.flags.syn == 1 && tcp.flags.ack == 0 && tcp.flags.fin == 0 — Helps identify SYN scans, where a SYN packet is sent without completing the handshake (common in reconnaissance activities).



- **DNS Tunneling:**

dns.qry.name matches "(.*)\.(.*)\.(.*)\.(.*)\.(.*)" — Detects unusual or suspiciously long DNS queries that might be indicative of DNS tunneling, a technique used to bypass firewalls or exfiltrate data.

- **Suspicious File Transfers:**

ftp-data || tftp || smb2.cmd == 0x05 — Filters for file transfer protocols, helping to identify potential unauthorized file transfers that could indicate data exfiltration.

4. Identifying Anomalous Traffic Patterns

- **Unusual Port Activity:**

tcp.port == 4444 — Displays traffic on port 4444, often associated with the Metasploit framework or other remote exploits.

- **Excessive ICMP Requests:**

icmp.type == 8 — Shows ICMP Echo Requests (ping), which can indicate a potential ICMP flood attack if there are too many.

5. Filtering by Specific Security-Related Protocols

- **Kerberos Traffic:**

kerberos — Displays Kerberos traffic, allowing you to inspect potential issues with authentication mechanisms.

- **IKEv2 Traffic:**

isakmp — Shows ISAKMP (Internet Security Association and Key Management Protocol) traffic, used in IPsec VPNs, to inspect potential weaknesses in VPN setups.

6. Inspecting Traffic for Information Leakage

- **Email Traffic:**

smtp || pop || imap — Shows unencrypted email traffic, which could expose sensitive information if not properly secured.

- **Exposure of Internal IP Addresses:**

ip.src == 10.0.0.0/8 || ip.src == 172.16.0.0/12 || ip.src == 192.168.0.0/16 — Filters for internal IP ranges that should not be exposed externally.

7. Capturing and Analyzing Specific Vulnerability Indicators

- **Malformed Packets:**

eth.fcs.bad == 1 — Displays packets with bad Frame Check Sequences (FCS), which might indicate packet tampering or network issues.

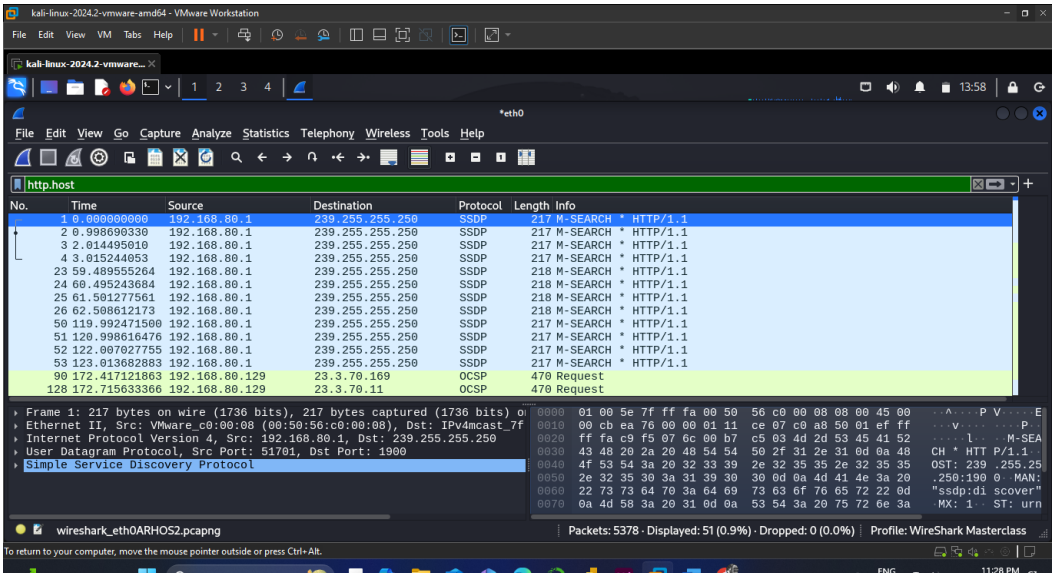
- **Excessive Retransmissions:**

tcp.analysis.retransmission — Identifies retransmitted packets, which could indicate network issues or an ongoing attack, such as a DoS (Denial of Service).

8. Monitoring for Outdated Software Versions

- **Identify Version Information in HTTP Headers:**

http.host contains "vulnerable_app" — Look for specific HTTP headers that might disclose outdated or vulnerable application versions.



9. Using Wireshark's Expert Information Tool

- **Expert Information:**

  How to Use:

  Go to Analyze → Expert Information to view warnings, errors, and other issues that Wireshark detects in the traffic.

  Look for issues like "Retransmissions," "Malformed Packets," or "Unencrypted Sensitive Data" that could point to potential vulnerabilities.

For More Reference and filters:

https://cdn.comparitech.com/wp-content/uploads/2019/06/Wireshark-Cheat-Sheet.pdf