Lab-10 Using-Wireshark---analyzing-web-browser-artifacts-email-header-analysis

AIM:

To use Wireshark to analyze web browser activities and inspect email headers from captured network traffic.

DESIGN STEPS:

Step 1:

Launch Wireshark and start capturing traffic on the appropriate network interface.

Step 2:

Use filters like http, dns, or tcp.port == 80 to monitor web browser artifacts such as visited URLs, cookies, and user-agent strings.

Step 3:

Apply filters like smtp, pop, or imap to locate and analyze email header details (e.g., sender, receiver, subject) from email communications.

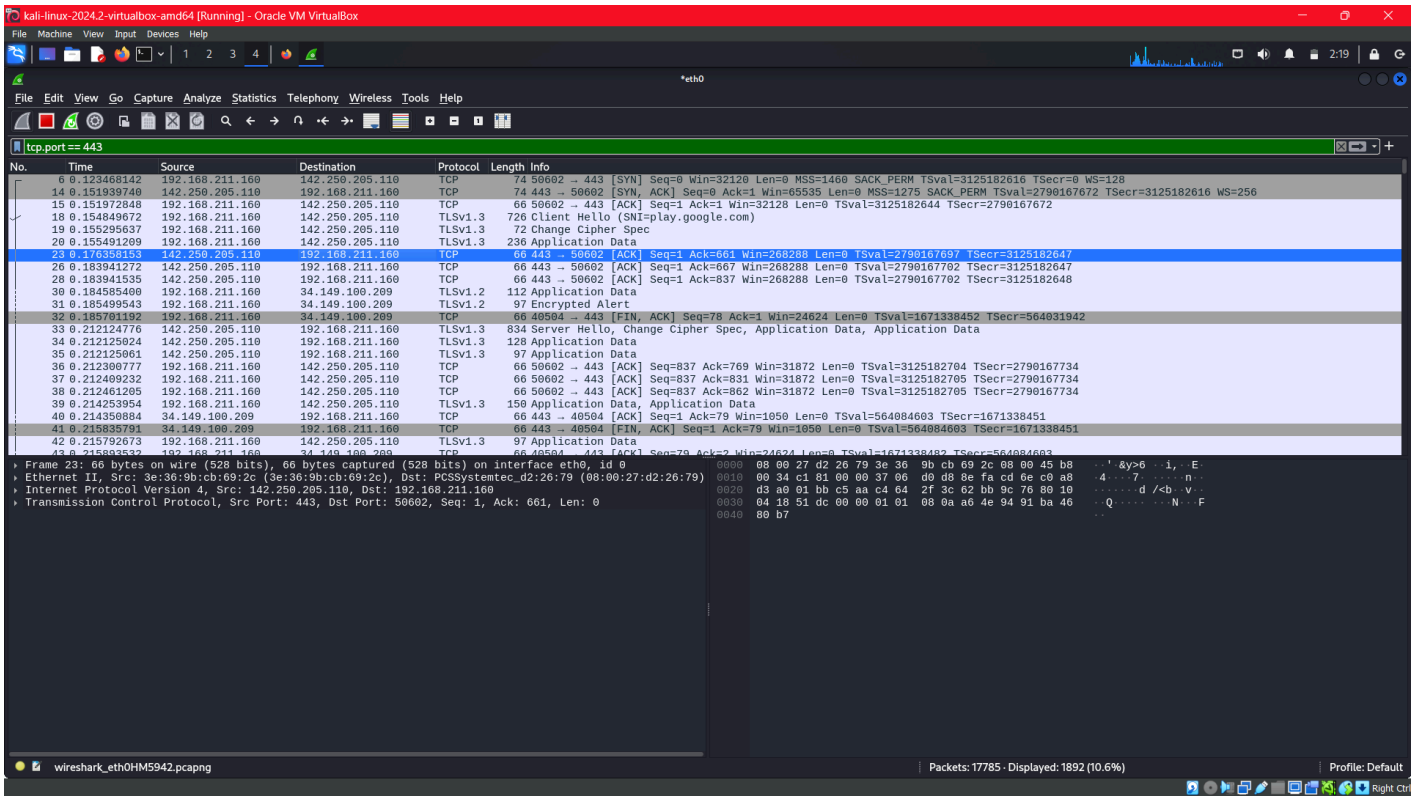
PROGRAM:

Wireshark Web and Email Traffic Filtering Steps

OUTPUT:

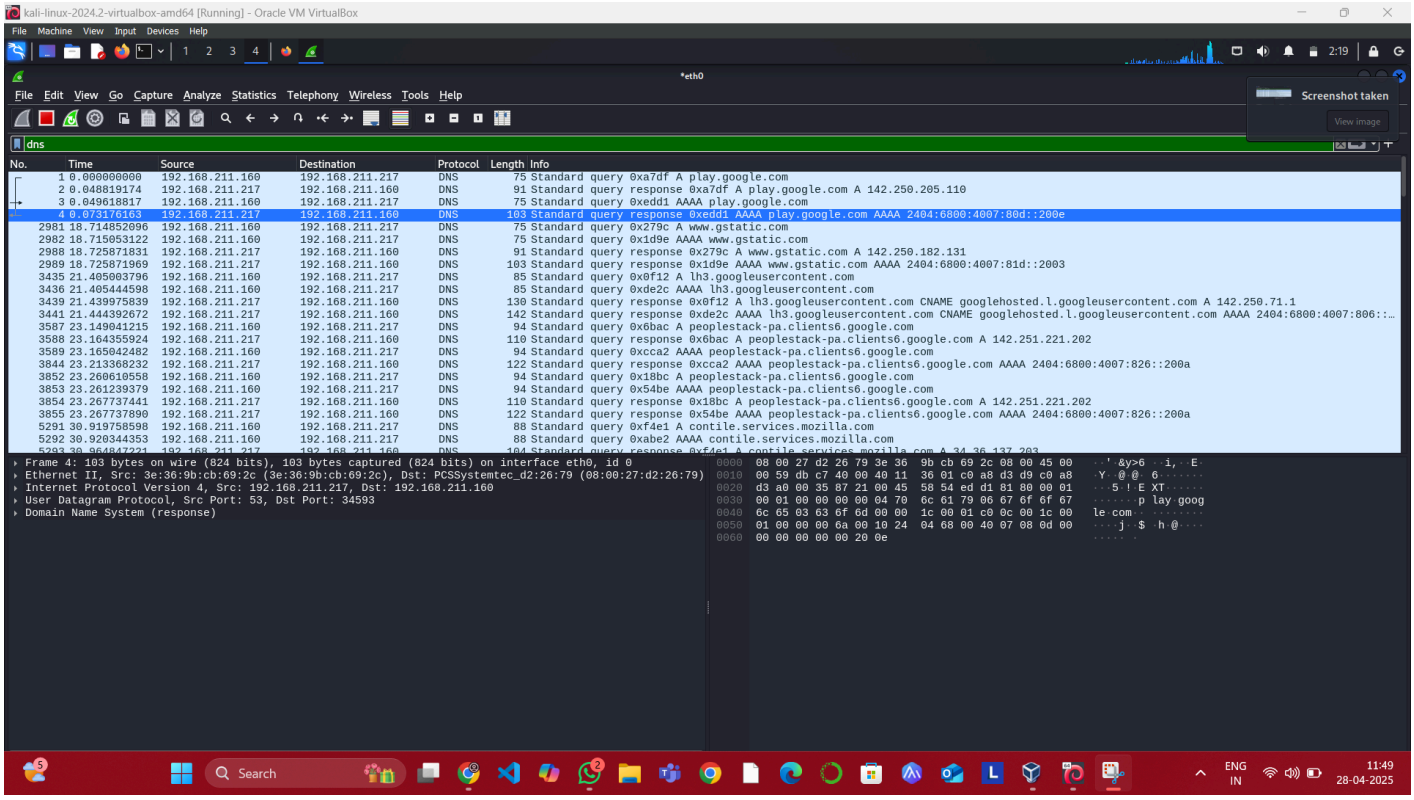
A. Capturing Traffic in Wireshark

1. Open Wireshark and start capturing on the active interface (Wi- Fi/Ethernet).
2. Perform activities like opening a website or sending an email through a client (e.g., Gmail via browser or Thunderbird).
3. Stop the capture once done.



Analyze DNS Queries: o Filter: dns

o Reveal domains the browser tried to resolve.



Email Header Analysis

1. Apply relevant filters:
2.

o For POP3: tcp.port == 110

o For SMTP: tcp.port == 25 or 587

o For IMAP: tcp.port == 143 or 993

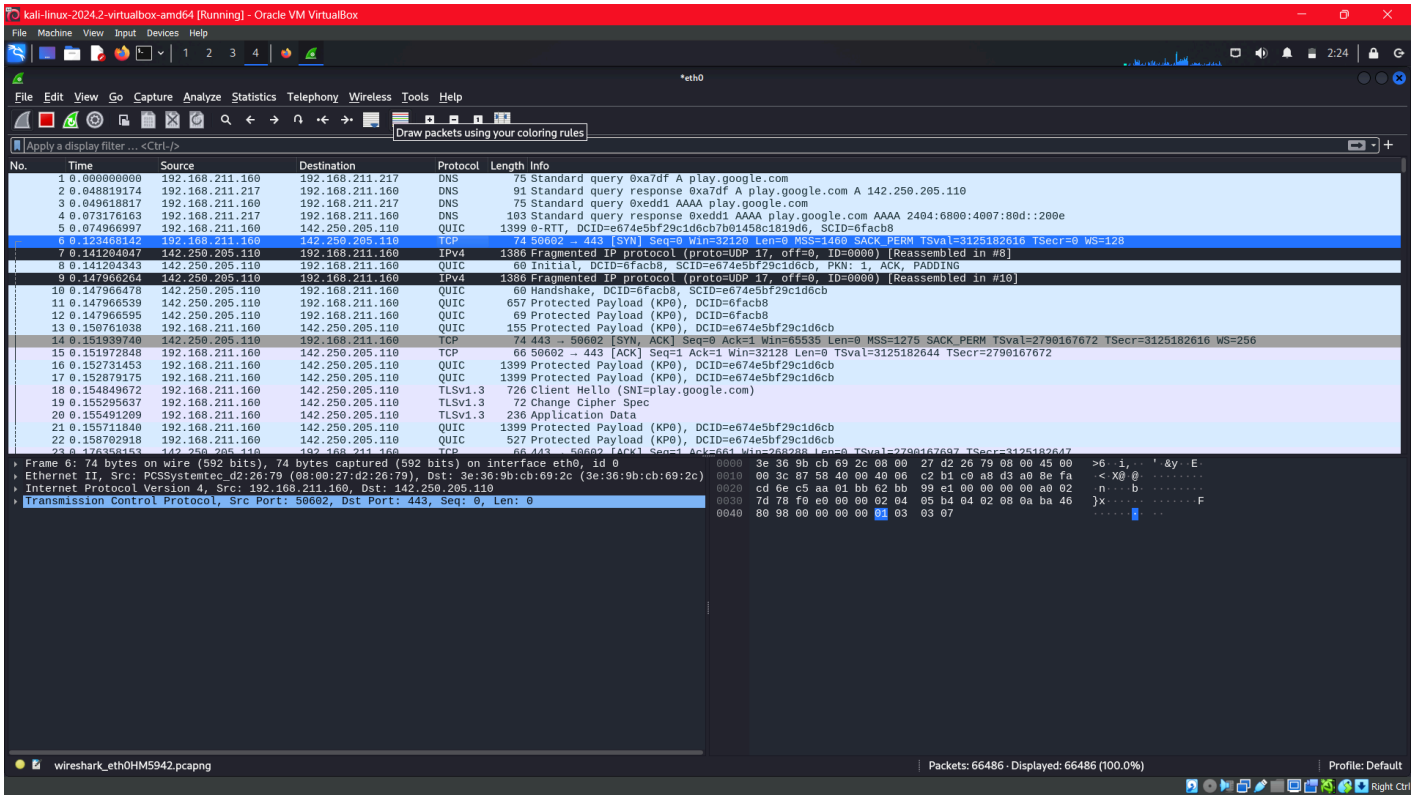
4. Locate email data:
5.

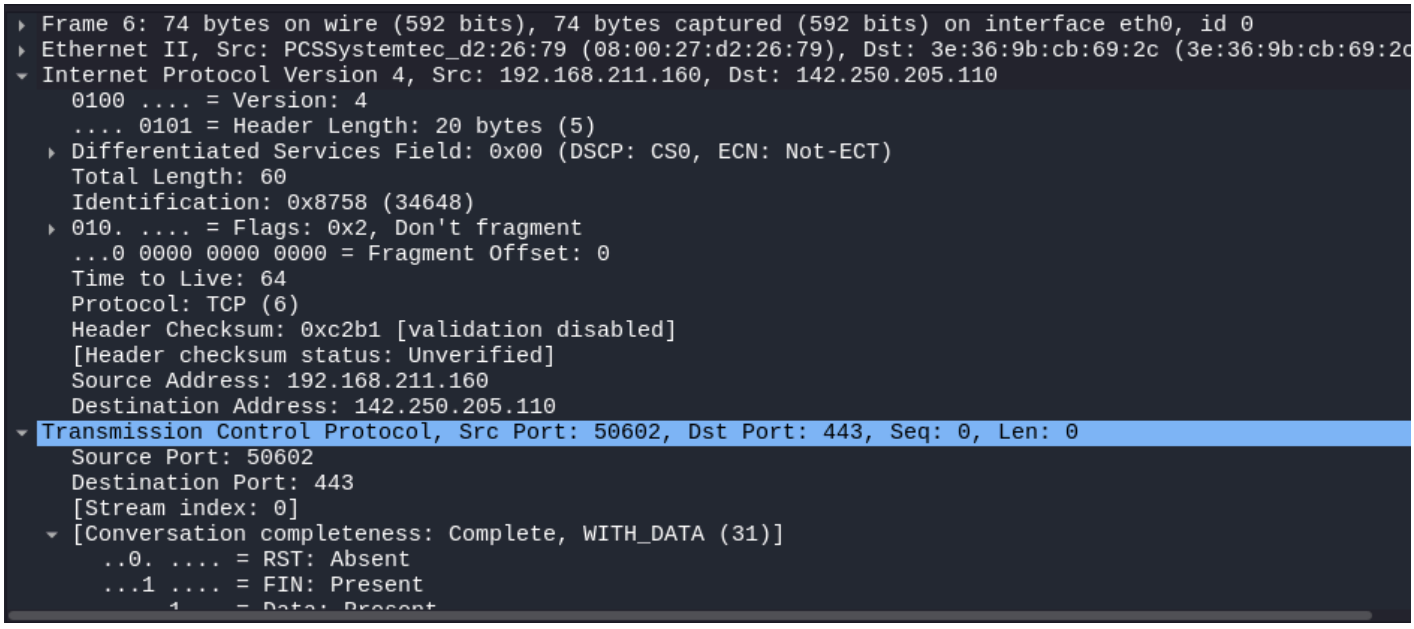
o Look for SMTP packets to see sender/receiver email addresses.

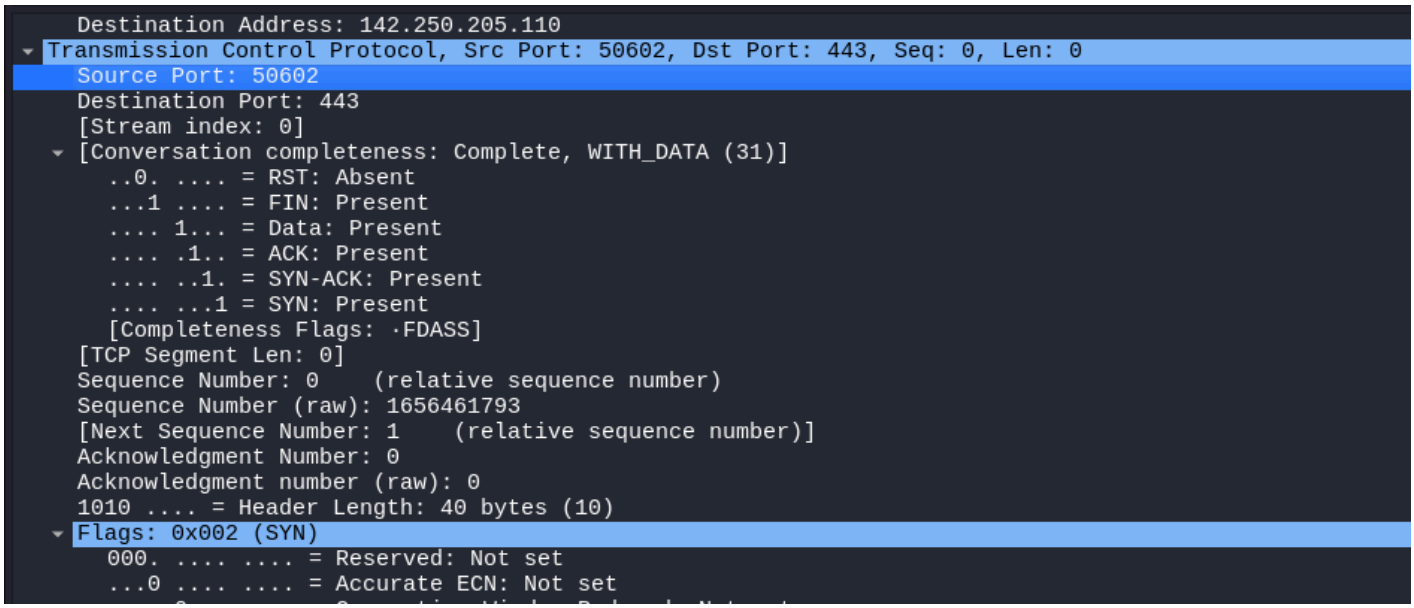
o Use "Follow TCP Stream" to view the full email headers and body if unencrypted.

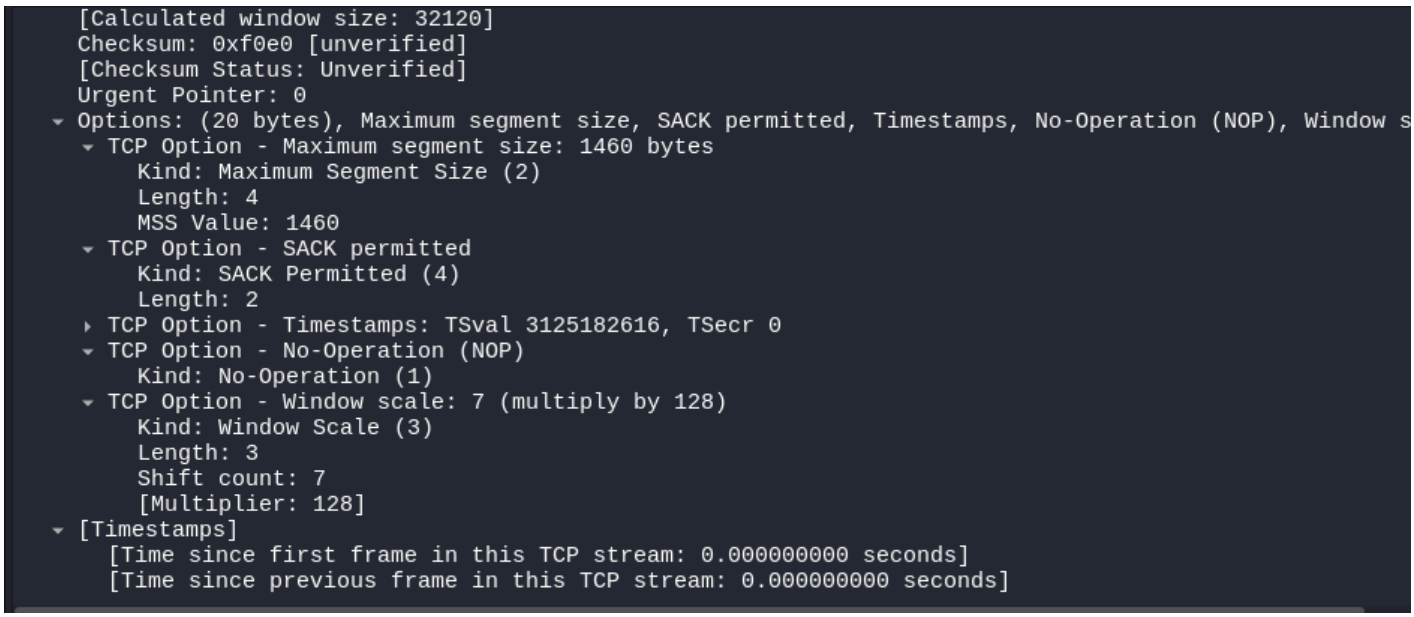
Extract Email Header Fields:

o Analyze From, To, Subject, Date, Message-ID, and relay servers used in sending the email.









RESULT:

Web browser artifacts and email headers were successfully analyzed using Wireshark