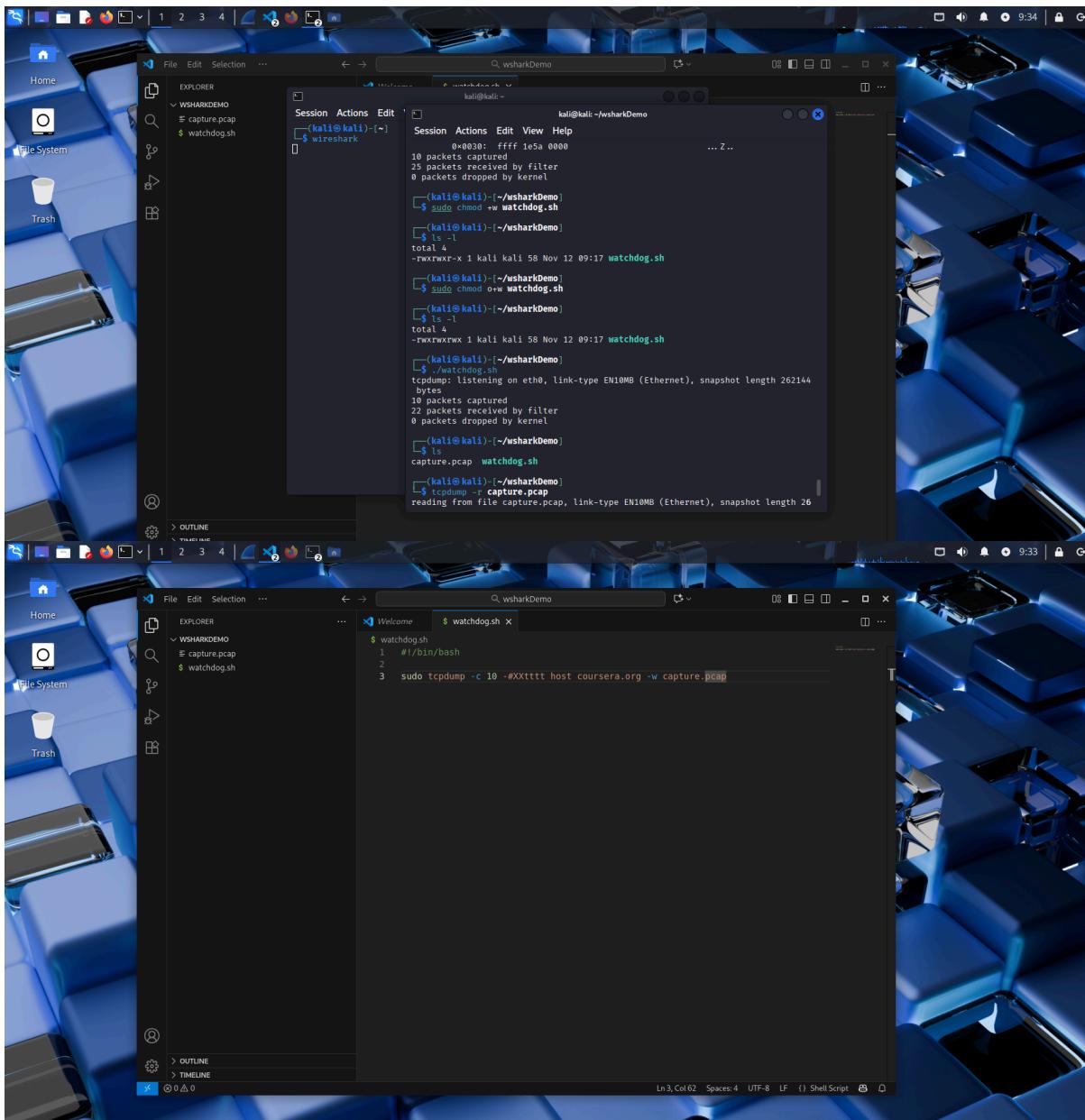


Wireshark Network Analysis: Full Workflow Documentation

This document provides a detailed walkthrough of network packet capture and analysis performed using Wireshark. It breaks down each major stage as part of a cybersecurity investigation workflow.

1. Launching Wireshark & Selecting an Interface

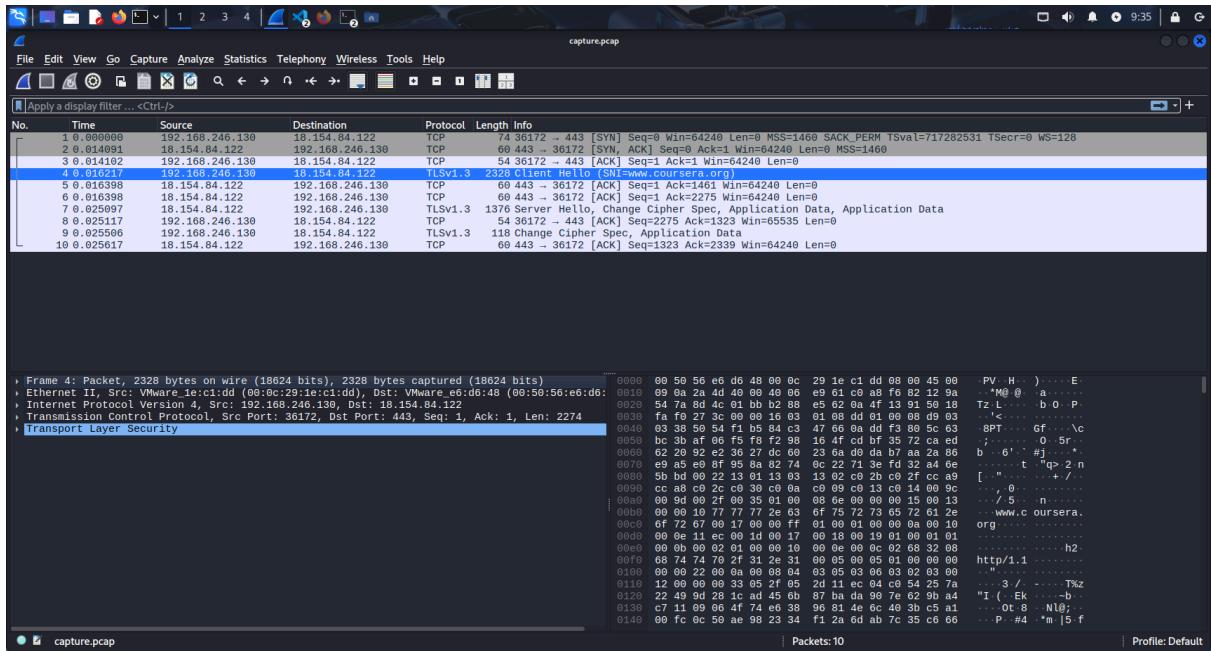
The process begins by opening Wireshark and selecting a network interface to monitor. This step is crucial as selecting the wrong interface would lead to incomplete or irrelevant traffic capture.



```
(kali㉿kali) [~/wsharkDemo] $ ./watchdog.sh
(kali㉿kali) [~/wsharkDemo] $ ls -l
total 4
-rwxrwxrwx 1 kali kali 58 Nov 12 09:17 watchdog.sh
(kali㉿kali) [~/wsharkDemo] $ ./watchdog.sh
(kali㉿kali) [~/wsharkDemo] $ ls -l
total 4
-rwxrwxrwx 1 kali kali 58 Nov 12 09:17 watchdog.sh
(kali㉿kali) [~/wsharkDemo] $ ./watchdog.sh
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
10 packets captured
22 packets received by filter
0 packets dropped by kernel
(kali㉿kali) [~/wsharkDemo] $ ls
capture.pcap  watchdog.sh
(kali㉿kali) [~/wsharkDemo] $ tcpdump -c 10 -#XXttt host coursera.org -w capture.pcap
$ ./watchdog.sh
1  #!/bin/bash
2
3  sudo tcpdump -c 10 -#XXttt host coursera.org -w capture.pcap
```

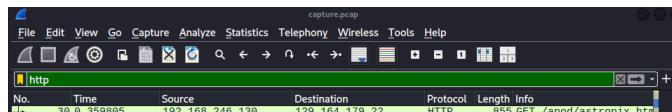
2. Starting the Packet Capture

Once the interface is selected, packet capture begins. Wireshark starts logging real-time network activity, displaying packets by protocol, source, destination, and size.



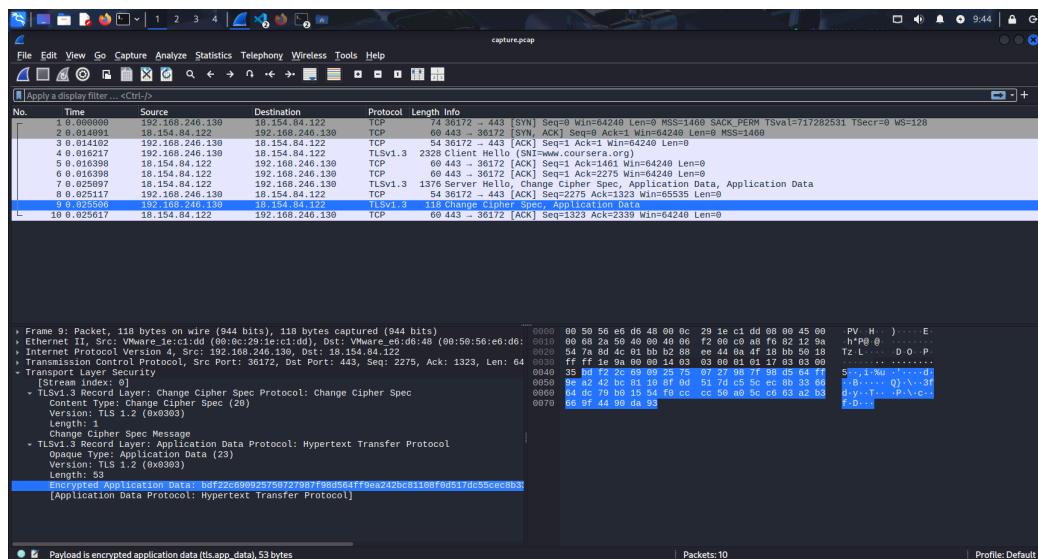
3. Filtering Traffic for Analysis

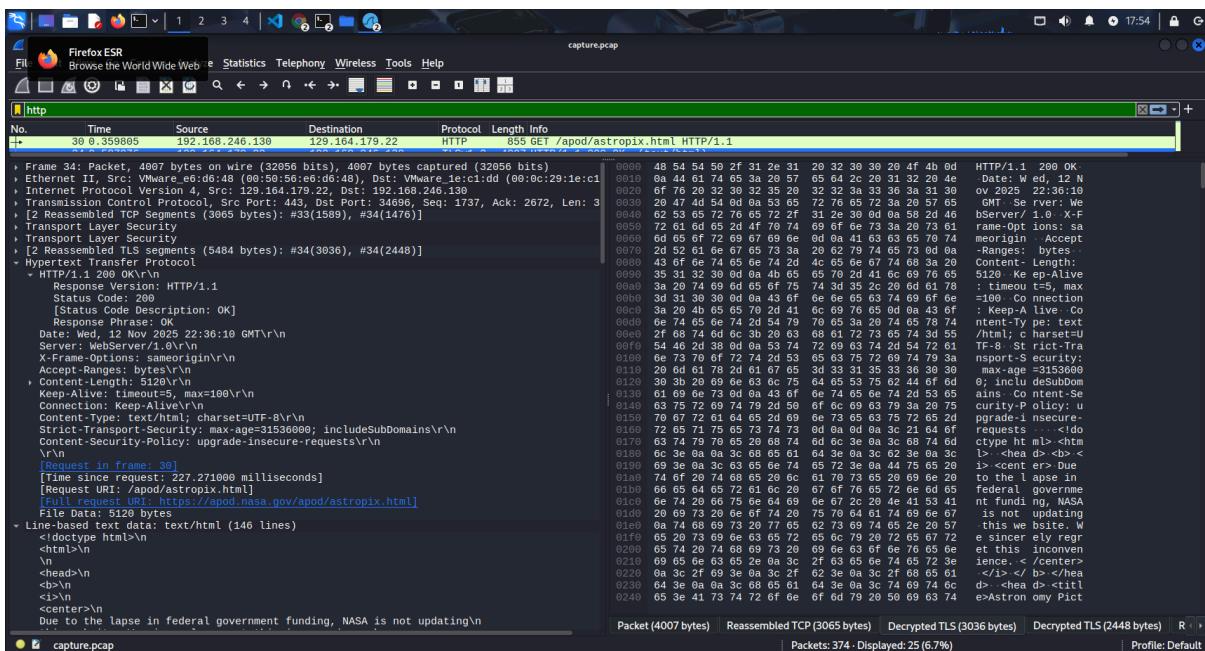
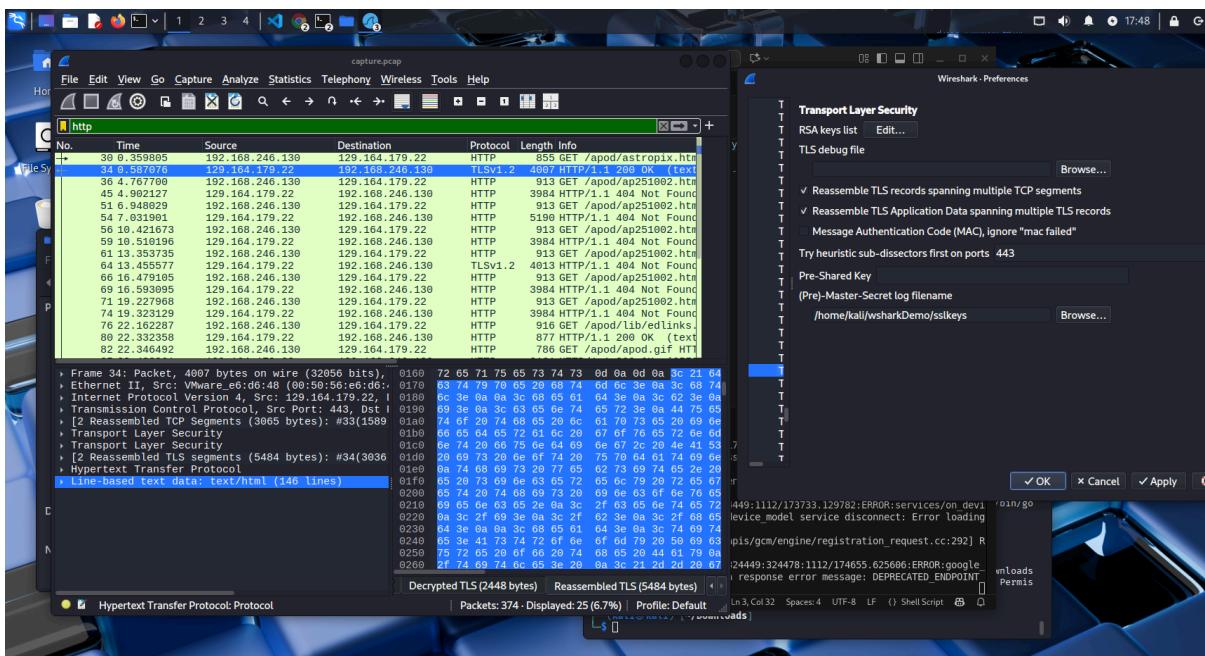
Filters are applied to isolate relevant packets. For example, filtering by protocol (e.g., HTTP, DNS, TCP) allows targeted investigation and reduces noise.



4. Inspecting Individual Packets

Packets are examined in detail to explore headers, payloads, etc then the application data is decrypted using captured SSL keys. This stage is essential for detecting anomalies.





5. Exporting Results & Final Report

The capture is exported or saved, and findings are summarised for reporting or incident response.