TShark: CLI Wireshark Features

## **Task 1 – Introduction**

* **TShark** is the **command-line version of Wireshark**.
* It allows you to **capture** and **analyze packets** without a GUI.
* Works well for:
  + Headless servers
  + Automation
  + Scripting
* **Syntax:**

bash

CopyEdit

tshark [options]

* Common use cases:
  + Live packet capture
  + Reading .pcap files
  + Filtering traffic
  + Extracting statistics and objects

## **Task 2 – Command-Line Features I | Statistics I**

* **Count packet statistics:**

bash

CopyEdit

tshark -z io,stat,interval

Example:

bash

CopyEdit

tshark -r file.pcap -z io,stat,1

→ Shows packets/bytes per second.

* **Protocol hierarchy statistics:**

bash

CopyEdit

tshark -r file.pcap -z io,phs

→ Lists protocols present and their percentage.

* **Conversations:**

bash

CopyEdit

tshark -r file.pcap -z conv,tcp

→ Shows TCP connections with packet counts, bytes, and duration.

## **Task 3 – Command-Line Features II | Statistics II**

* **Endpoints (hosts) stats:**

bash

CopyEdit

tshark -r file.pcap -z endpoints,ip

→ Lists IP addresses with packet and byte counts.

* **Service response time:**

bash

CopyEdit

tshark -r file.pcap -z "rtp,streams"

(RTP) or:

bash

CopyEdit

tshark -r file.pcap -z "dns,stat"

(DNS query/response times).

* **Capture filtering** (BPF syntax):

bash

CopyEdit

tshark -i eth0 port 80

→ Capture only HTTP packets.

## **Task 4 – Command-Line Features III | Streams, Objects, and Credentials**

* **Follow TCP/HTTP stream:**

bash

CopyEdit

tshark -r file.pcap -q -z follow,tcp,0

(0 is stream index).

* **Export HTTP objects:**

bash

CopyEdit

tshark -r file.pcap --export-objects http,output\_folder

* **Extract credentials:**  
  Filter for protocols carrying logins (FTP, HTTP Basic, Telnet):

bash

CopyEdit

tshark -r file.pcap -Y "ftp.request.command == USER || ftp.request.command == PASS"

## **Task 5 – Advanced Filtering Options | Contains, Matches, and Fields**

* **Contains** – checks if field contains a value (case-sensitive):

bash

CopyEdit

-Y "http contains 'login'"

* **Matches** – regex match:

bash

CopyEdit

-Y "frame matches 'regex\_here'"

* **Display specific fields:**

bash

CopyEdit

tshark -r file.pcap -T fields -e ip.src -e ip.dst -e tcp.port

* **AND / OR filtering**:

bash

CopyEdit

-Y "ip.src == 192.168.1.5 && tcp.port == 443"

## **Task 6 – Use Cases | Extract Information**

* **Find unique IPs:**

bash

CopyEdit

tshark -r file.pcap -T fields -e ip.src -e ip.dst | sort -u

* **Count occurrences:**

bash

CopyEdit

tshark -r file.pcap -T fields -e ip.src | sort | uniq -c | sort -nr

* **Extract all HTTP hostnames:**

bash

CopyEdit

tshark -r file.pcap -Y http.host -T fields -e http.host

## **Task 7 – Conclusion**

* TShark is **Wireshark’s CLI counterpart** for efficient, automated packet analysis.
* Strong points:
  + Works in servers without GUI.
  + Integrates into scripts for automated monitoring.
  + Useful for CTFs and network forensics.
* Key skill: **Knowing the right -z statistics command** and **-T fields extractions** for your goal.

