TShark: The Basics

## **TShark: The Basics – Notes**

### **Task 1 – Introduction**

* **TShark** is the command-line version of Wireshark.
* Used for **packet capture**, **filtering**, and **analysis** without a GUI.
* Common use cases:
  + Headless environments (servers, SSH)
  + Automation via scripts
  + Large capture file analysis

### **Task 2 – Command-Line Packet Analysis Hints**

* **TShark basics**:
  + Syntax:

tshark [options]

* Useful CLI helpers:
  + grep – search patterns in output
  + less – page through long outputs
  + wc -l – count lines (packets)
  + cut / awk – extract specific fields
* Redirect output to files:

tshark ... > output.txt

### **Task 3 – Main Parameters I**

* -i <interface> → choose network interface  
  Example: tshark -i eth0
* -c <count> → stop after N packets  
  Example: tshark -i eth0 -c 10
* -a duration:<sec> → stop after time limit  
  Example: tshark -i eth0 -a duration:60
* -w <file> → write capture to file (.pcap)  
  Example: tshark -i eth0 -w capture.pcap

### **Task 4 – Main Parameters II**

* -r <file> → read from a capture file instead of live interface  
  Example: tshark -r file.pcap
* -V → detailed packet view (verbose)
* -T fields → output specific fields
* -e <field> → select fields to output  
  Example:

bash

CopyEdit

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

### **Task 5 – Capture Conditions**

* Use **automatic stop** conditions:
  + -a filesize:<KB> → stop after file reaches size
  + -b filesize:<KB> → ring buffer, multiple files
  + -b duration:<sec> → split captures over time
* Useful for long captures to avoid huge files

### **Task 6 – Capture vs. Display Filters**

* **Capture filters**: Applied **while capturing** (fewer packets stored)
* **Display filters**: Applied **after capture** (on stored data)
* Capture filters use **libpcap syntax** (like tcpdump)
* Display filters use **Wireshark syntax**
* Example:
  + Capture filter:

tshark -i eth0 -f "port 80"

* + Display filter:

tshark -r file.pcap -Y "http"

### **Task 7 – Capture Filters**

* Syntax: **BPF (Berkeley Packet Filter)**, same as tcpdump
* Examples:
  + Capture only HTTP: tcp port 80
  + Only ICMP: icmp
  + Specific host: host 192.168.1.10
  + Host + port: host 192.168.1.10 and port 443

### **Task 8 – Display Filters**

* Syntax: **Wireshark display filter language**
* Examples:
  + Only HTTP traffic: http
  + Source IP: ip.src == 192.168.1.5
  + Destination port: tcp.dstport == 443
  + Multiple conditions: ip.src == 192.168.1.5 && tcp
* More flexible than capture filters (can check packet contents, fields, etc.)

### **Task 9 – Conclusion**

* **TShark Advantages**:
  + Runs in headless/remote environments
  + Scriptable and automatable
  + Efficient for large pcap file processing
* **Key takeaway**:  
  Use **capture filters** to limit what is saved and **display filters** to analyze stored data.

