Wireshark: The Basics

### 🧠 **Wireshark: The Basics – Notes**

### ✅ **Task 1: Introduction**

* **Wireshark** is a free and open-source packet analyzer used for:
  + Network troubleshooting
  + Analysis
  + Communications protocol development
  + Cybersecurity (e.g., packet inspection, malware analysis)

### ✅ **Task 2: Tool Overview**

* **Main Areas of the Interface:**
  + **Capture Panel:** Shows live network interfaces
  + **Packet List Panel:** Displays captured packets (summary view)
  + **Packet Details Panel:** Shows detailed info of the selected packet (protocols)
  + **Packet Bytes Panel:** Shows raw hex + ASCII view of the packet
* **Capture Filters** (before capture):
  + E.g., tcp, host 192.168.1.1, port 80
* **Display Filters** (after capture):
  + E.g., http, ip.src == 192.168.1.100

### ✅ **Task 3: Packet Dissection**

* Each packet has **layers**:
  + **Frame:** Overall packet
  + **Ethernet:** MAC addresses
  + **IP:** Source and Destination IP
  + **TCP/UDP:** Ports, Flags
  + **Application Layer:** Protocol-specific data (HTTP, DNS, etc.)
* Expand sections to see full protocol breakdown.

### ✅ **Task 4: Packet Navigation**

* Use:
  + **Arrow keys** to move up/down in the packet list
  + **Ctrl + F** to search for string, hex, or display filter
  + **Right-click** > Follow TCP Stream to view complete conversation
  + **Time column** shows when each packet was captured

### ✅ **Task 5: Packet Filtering**

* **Useful Display Filters:**
  + http → Show HTTP traffic
  + tcp.port == 80 → Filter TCP traffic on port 80
  + ip.addr == 192.168.1.1 → Packets from/to this IP
  + tcp.flags.syn == 1 → SYN packets (start of TCP handshake)
  + dns → DNS queries/responses
  + Combine filters with &&, || or ! for negation

### ✅ **Task 6: Conclusion**

* Wireshark is a powerful tool used in both:
  + **Blue Team:** Detect threats
  + **Red Team:** Analyze exploits or C2 communication
* Mastering packet navigation and filtering is key to effective analysis.

