Assignment (Packet Capture)

---

1. Write a `tcpdump` command that captures all packets coming from the IP address `192.168.1.100`.
2. You want to capture traffic only on port 443 (HTTPS). Write the appropriate `tcpdump` capture filter to achieve this.
3. You need to capture all HTTP traffic (port 80) **and** all ICMP traffic. Write a single `tcpdump` filter to achieve this.
4. In Wireshark, how would you write a display filter to show only the HTTP GET requests from a capture file?
5. In Wireshark, write a capture filter using Berkeley Packet Filter (BPF) syntax to capture traffic from the IP address `192.168.1.1` to the IP address `192.168.1.2`.
6. You are tasked with analyzing only UDP traffic on port 53. Write a `tcpdump` command using the appropriate filter to capture this traffic.
7. Write a `tcpdump` filter to capture only the SYN packets during the TCP handshake.
8. How would you modify a BPF capture filter to exclude all traffic on port 22 (SSH) while still capturing HTTP traffic on port 80?
9. Write a Wireshark display filter to show DNS query packets for the domain name `example.com`.
10. You are analyzing network performance and want to capture only packets larger than 1000 bytes. Write the `tcpdump` filter to achieve this.
11. Write a `tcpdump` command that captures only the traffic between two specific IP addresses, `192.168.1.10` and `192.168.1.20`.
12. How would you use a BPF filter in Wireshark to capture only ARP traffic?
13. Write a `tcpdump` command that captures packets where the source IP is `192.168.2.5` and the destination port is `80`.
14. You need to capture all traffic related to a specific TCP stream (stream number 3). Write the appropriate `tcpdump` command to achieve this.
15. Write a `tcpdump` command that captures only traffic with the UDP protocol and a payload size greater than 512 bytes.
