==========
ESERCITAZIONE: ANALISI PROTOCOLLO TCP E HANDSHAKE
(WIRESHARK/TCPDUMP)
Docente: [Tuo Nome/Cattedra]
==========

PARTE 1: ANALISI DEL FRAME 1 (SYN PACKET)
---
1. Qual è il numero di porta TCP di origine?
R: 42514

2. Come classificheresti la porta di origine? (Well-known, Registered, Dynamic?)
R: Porta Effimera

3. Qual è il numero di porta TCP di destinazione?
R: 80

4. Come classificheresti la porta di destinazione?
R: HTTP

5. Quale flag è impostato nel campo Flags?
R: SYN

6. A quale valore è impostato il numero di sequenza relativo?
R: 0

PARTE 2: ANALISI DEL FRAME 2 (SYN, ACK PACKET)
---
7. Quali sono i nuovi valori delle porte di origine e destinazione?
Porta Origine: 80
Porta Destinazione: 42514

8. Quali flag risultano impostati (Set) in questo pacchetto?
R: SYN, ACK

9. A quali valori sono impostati i numeri relativi di Seq e Ack?
Relative Sequence Number: 1
Relative Acknowledgment Number: 413

PARTE 3: ANALISI DEL FRAME 3 (ACK PACKET)
---
10. Quale flag è impostato nel terzo pacchetto dell'handshake?
R: SYN, ACK

11. I numeri relativi di Seq e Ack sono impostati a 1. Cosa indica questo?
R: Che il Three way handshake è stato completato

PARTE 4: STRUMENTI DA RIGA DI COMANDO E RIFLESSIONE
---
12. Cosa fa l'opzione "-r" nel comando tcpdump?
R: L'opzione `-r` **(read)** permette a `tcpdump` di leggere e analizzare un file di cattura precedentemente salvato

13. Elenca tre filtri di Wireshark utili per un amministratore di rete:
R1: `ip.addr == [indirizzo_IP]` – Filtra tutto il traffico (sorgente o destinazione) relativo a un host specifico, utile per isolare il comportamento di un singolo dispositivo sospetto.
R2: `tcp.flags.reset == 1` – Visualizza tutti i pacchetti con il flag RST impostato; utilissimo per individuare connessioni interrotte bruscamente o tentativi di port scanning
R3: `http.response.code >= 400` – Isola le risposte HTTP che indicano errori lato client o server, permettendo di individuare rapidamente malfunzionamenti di applicazioni web o tentativi di accesso a risorse inesistenti

14. In quali altri modi Wireshark può essere usato in una rete di produzione?
R: **Analisi delle prestazioni:** Identificare colli di bottiglia e latenze elevate (es. tramite il calcolo del *TCP Delta Time*).
Network Forensics: Ricostruire sequenze di attacco dopo un incidente di sicurezza per capire quali dati sono stati esfiltrati.
Verifica della conformità: Accertarsi che il traffico sensibile sia effettivamente crittografato (es. verificare che non passi traffico Telnet o HTTP in chiaro dove è richiesto SSH o HTTPS).
Troubleshooting VoIP: Analizzare la qualità delle chiamate e i flussi RTP per risolvere problemi di jitter o perdita di pacchetti.

==========
NOTE DI LABORATORIO (HACKING ETICO / DEFENSE):
_____
_____