1.Identify the true statements (Choix multiple) [Lecture 5 - Slide #13]

Answer 1: This packet belongs to a UDP flow

Answer 2: This is the first packet of a TCP connection

Answer 3: It's not possible to read the payload of this packet because it is encrypted

Answer 4: From this tcpdump output, we can identify the source/destination IP, source/destination port, TCP flags, and packet sequence number.

2.True or False: Port mirroring is more suitable for packet capture at high-speed links? (Choix unique)

Answer 1: True

Answer 2: False

True or False: Network Tap is low-cost and easy to setup whereas port mirroring depends on expensive hardware (Choix unique)

Answer 1: True

Answer 2: False

3. Identify the correct statements (Choix multiple)

Answer 1: Interface counts requires less storage needs compared to packet capture

Answer 2: Interface count is useful to measure link utilization for billing purposes

Answer 3: Interface count allows to identify the source of a Denial of Service attack

4. Identify the correct statements (Choix multiple)

Answer 1: Flow capture provides less details than interface counts but more information than packet capture

Answer 2: Flow capture overheads can be reduced via Sampling

Answer 3: Flow capture can provide per-packet information

Answer 4: Flow eviction strategies are defined to remove records of malicious flows from the flow cache