1. Open the capture file and note the total number of packets.

2. From Statistics → Protocol Hierarchy, identify the top 3 protocols by packet count.

3. Apply filter ip.src == 10.207.231.112 How many packets match?

4. Apply filter http. Identify one GET request. Write the Host + URI.

5. Apply filter dns. List any two domain names queried.

6. Apply filter tcp.port == 443. How many HTTPS packets were captured?

7. Apply filter arp. Write one Request and its Reply (with MACs).

8. Find a TCP Reset (RST) packet. Write source + destination IPs.

9. Add a new column Delta time displayed. Write delay between 1st and 2nd HTTP packet.

10. Save only HTTP packets into a new file set1_http.pcapng.

1. From Statistics → Protocol Hierarchy, write the percentage of TCP, UDP, ICMP.

2. Apply filter arp. Find one ARP Request + Reply.

3. Apply filter icmp. Identify one Echo Request and its Reply (with sequence no.).

4. Select a TCP conversation → Follow TCP Stream. Write a short note on the contents.

5. From Statistics → Conversations, find the top 2 IP pairs.

6. Apply filter tcp.flags.syn == 1. Write first SYN packet number.

7. Apply filter dns. Note one query + its resolved IP.

8. Use Edit → Coloring Rules to highlight UDP traffic. Note first highlighted packet.

9. Add a column for tcp.stream index. Write values for the first 3 TCP connections.

10. Export the first 50 packets into a plain text file. Note file size.

1. Apply filter tcp && ip.src == 64.233.170.188. Count packets.

2. Apply filter ip.src[0:1]==172. Count packets.

3. Apply filter dns. Find one query + response IP.

4. Find one ICMP Request and Reply. Write RTT (Round Trip Time).

5. Use File → Export Objects → HTTP. Export one file. Note filename + size.

6. Apply filter tls. Write the TLS version observed.

7. Apply filter tcp.analysis.retransmission. Count retransmissions.

8. Find the largest packet in the capture. Write size + protocol.

9. Apply filter http.request. Write first User-Agent string.

10. From Statistics → Conversations, note the conversation with highest bytes exchanged.

1. Count the total number of packets captured.

2. From Protocol Hierarchy, identify top 3 protocols by percentage.

3. Apply filter http.request.method == "POST". Write Host and Content-Type.

4. Apply filter arp. Write one Request and Reply (with MACs).

5. Find one TCP Reset (RST) packet. Write IP + ports.

6  Apply filter tls. Write the TLS version observed.

7. Export packet dissections of the first 25 packets into plain text. Note file size.

8. Find the first HTTP response code (200/404/etc.). Write a packet number.

9. From Statistics → Endpoints, identify top 2 IPs by traffic.

10. Add a Coloring Rule for TCP SYN packets. Note first highlighted packet.

1. Change Time Format → Seconds Since Beginning. Write arrival time for the first 3 packets.

2. Apply filter udp. Identify 2 source ports + 2 destination ports.

3. Apply filter icmp. Find a Destination Unreachable message. Write packet no.

4. Apply filter (ip.src == 10.0.0.2 && tcp) || dns. Count packets.

5. Apply filter http. Write one GET request URI.

6. From Conversations, identify the longest TCP conversation.

7. Apply filter tcp.flags.syn == 1. Write first SYN packet number.

8. Export one HTTP object. Write filename + size.

9. Apply filter dns. Write one query + resolved IP.

10. Add Delta Time Displayed column. Write delay between two ICMP packets.

1. Count the total number of packets captured.

2. Apply filter http. Follow one HTTP stream. Write a short note on the exchange.

3. Apply filter http.request.method == "POST". Write Host and Content-Type.

4. Apply filter arp. Write one Request and Reply with MAC Addresses.

5. Identify SYN, SYN-ACK, ACK packet numbers + sequence numbers.

6. Use Find Packet → Regex. Search for “User-Agent”. Note packet number.

7. Apply filter dns. Write one query + resolved IP.

8.Apply filter ip.addr in {192.168.1.10 192.168.1.15}. Count packets.

9. From Conversations, identify the top 2 IP pairs.

10. Export one HTTP object. Write filename + size.