Faculty of Computer Applications and Information Technology
M. Sc. (IT) – Sem 3
Network Analysis Tools
CEC Assignment - 1

Open the file sample2.pcap in Wireshark.

1. How many total packets are present?
2. List the top 3 protocols by frequency.
3. Identify and list all unique IP addresses observed.
4. Which IP address appears most frequently as a source?
5. Apply the filter ip.addr == <most frequent IP> and count the number of packets.
6. Apply the filter tcp – how many TCP packets are there?
7. Identify the source and destination MAC addresses of the first packet.
8. Apply a filter based on the source MAC address.
9. Find a complete TCP conversation (use Follow TCP Stream).
10. What protocol is used in the application layer (HTTP, FTP, etc.)?
11. Create a filter to show only TCP SYN packets: tcp.flags.syn == 1 and tcp.flags.ack == 0
12. How many packets match this filter?
13. List all unique destination TCP ports.
14. Which service (protocol) is most commonly used?
15. Add a column for “Time delta from previous captured packet”.
16. Identify the largest gap in packet arrival.
17. What is the average length of packets?
18. What is the length of the smallest and largest packet?
19. Create a color rule to highlight all TCP SYN packets in green.

20. Create a filter button for HTTP packets and assign a custom label.