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

Open the file wireshark_aug18.pcapng in Wireshark.

1. Show only DNS queries not responses.(Hint: dns.flags.response == 0)
2. Show TCP packets where the destination port is 443. (Hint:tcp.dstport == 443)
3. Display packets larger than 500 bytes. (Hint: frame.len > 500)
4. Show all ICMP Echo Request packets. (Hint: icmp.type == 8)
5. Show traffic where the source IP is 145.254.160.237 and the destination port is 80.
6. Show traffic from either 145.254.160.237 or 172.16.18.160
7. Exclude ARP packets from display
8. Find the number of HTTP GET requests.
9. Filter packets involved in a TCP handshake. (Hint: tcp.flags.syn == 1 || tcp.flags.ack == 1)
10. Check if there was any retransmission. (Hint: tcp.analysis.retransmission)
11. Show only packets captured between 10 and 20 seconds. (Hint: frame.time_relative >= 10 && frame.time_relative <= 20)
12. Extract only the first 2 bytes of every source IP address. (Hint: ip.src[0:2])
13. Show HTTP requests where Host contains example.com. (Hint: http.host matches "example\.com")
14. Show DNS queries ending with .edu. (Hint: dns.qry.name matches "\.edu$")

15. Extract first 3 bytes of destination MAC. (Hint: eth.dst[0:3])
16. Mark all packets with TCP RST. (Hint: tcp.flags.reset == 1)
17. Show all traffic except TCP & UDP.(Hint: !(tcp || udp))
18. Display packets with TCP destination port in {80, 443, 8080}.(Hint: tcp.dstport in {80 443 8080})
19. Show packets where the source IP is either 145.254.160.237, 172.16.18.160, or 65.208.228.223.(Hint: ip.src in {145.254.160.237, 172.16.18.160, 65.208.228.223.})
20. Display packets where the first byte of the source IP is 192. (Hint: ip.src[0:1] == 172)
21. Extract the first 4 bytes of packet payload. (Hint: frame[0:4])
22. Extract the last 4 bytes of the frame.
23. Show HTTP requests where the URI contains /login. (Hint: http.request.uri matches "/login")
24. Filter DNS responses containing the IP 8.8.8.8. (Hint: dns.a == 8.8.8.8)
25. Show only ICMP packets where the code is not 0. (Hint: icmp.code != 0)