Labor 3

4.1)

A)

- Mekkora 1327 darab szkennelt keret mérete összesen? 823001 byte

- Mekkora a 6 másodperc alatti hálózati forgalom átlagos sávszélessége? 1539 mbit/s

- Mennyi keret haladt át a hálózati kártyán 6 másodperc alatt? 32

- Mekkora a 6 másodperc alatt forgalmazott átlagos keretméret? 1920 byte

B)

- Mekkora a tömörítési arány a pcap és a txt típusok esetén? Pcap – 37kb, txt – 312kb

- Mekkora a tömörítési arány a pcap és a pcapng típusok esetén? 42kb

4.2)

A)

- Jelenítse meg az ARP/RARP, ICMP, ICMPv6, IPv4, IPv6, TCP, UDP és egyéb forgalmak időgrafikonját

- Mi a Cisco cég OUI kódja? 001B67

- Mi az asztali gép NIC moduljának MAC címe? 9E-2F-9D-5E-B2-6D

B) - Hol található az Interneten a NIC gyártó cégek MAC OUI azonosítói? <https://www.meridianoutpost.com/resources/etools/network/ieee-oui-lookup.php>

- Mi a következő NIC gyártó cégek MAC OUI kódjai: Cisco, HP, Apple, Xiaomi, Huawei?

Huawei 0094EC

Cisco 001B67

HP 0068EB

Apple 000393

Xiaomi 009EC8

4.3)

1. Mi a saját gép forgalmát kizárólagosan szűrő szkennelési szabály Wireshark esetén? Enable promiscous mode kikapcsolása / Ether Host 9E-2F-9D-5E-B2-6D
2. Mi az üzenetszórási címre küldött kereteket kizárólagosan szűrő szkennelési szabály Wireshark esetén? ether host ff:ff:ff:ff:ff:ff

4.4)

1. Mi a saját gép forgalmát kizárólagosan szűrő megjelenítési szabály Wireshark esetén? eth.addr == 9E-2F-9D-5E-B2-6D
2. Mi az üzenetszórási címre küldött kereteket kizárólagosan szűrő megjelenítési szabály Wireshark esetén? ip.addr == 172.22.228.255

4.5)

1. Hol található a szkennelt keret lezáró mezője Wireshark esetén? Edit, preferences, protocols, frame

B) Mit jelölnek a „.” karakterek a legalsó mezőben? Értelmetlen karakter