Labor: Wiresharki kasutamine võrgu liikluse püüdmiseks (üks arvuti)

Eesmärgid:

• Osa 1: Kohaliku ICMP andmete püük Wiresharkis (loopback)
• Osa 2: Kaug-ICMP andmete püük Wiresharkis (ping veebisaitidele)

Nõutavad ressursid:

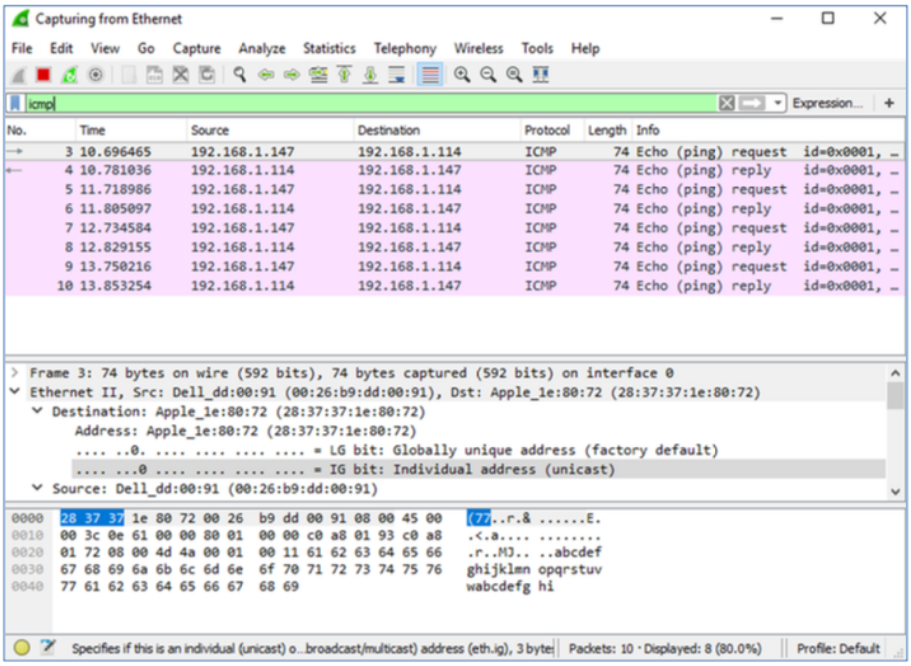
• 1 arvuti (Windows ja internetiühendus)
• Wireshark tarkvara

Wiresharki installimise juhised:

1. Ava Wiresharki ametlik veebileht: https://www.wireshark.org/download.html
2. Laadi alla Wiresharki installifail ja järgi ekraanil kuvatavaid juhiseid. Paigalda ka Npcap.
3. Pärast installatsiooni käivitamist vali võrgukaart, mille liiklust soovid jälgida.
   - Kohalike päringute jaoks vali 'loopback' (127.0.0.1).
   - Interneti liikluse jälgimiseks vali oma aktiivne võrgukaart (Ethernet või Wi-Fi).

Osa 1: Kohaliku ICMP andmete püük (loopback)

1. Käivita Wireshark ja vali 'loopback' liides (127.0.0.1).
2. Alusta andmete püüdmist.
3. Ava käsuviip ja sisesta: 'ping 127.0.0.1', et saata ICMP päringuid.
4. Wiresharkis näed ICMP päringuid ja vastuseid. Kasuta ICMP filtrit.
5. Peata andmete püük ja analüüsi tulemusi.



Osa 2: Kaug-ICMP andmete püük (ping veebisaitidele)

1. Käivita Wireshark ja vali oma aktiivne võrgukaart (sealt tuleb palju infot).
2. Alusta andmete püüdmist.
3. Ava käsuviip ja ping'i järgmisi veebisaite: www.google.com, www.cisco.com.
4. Peata andmete püük ja analüüsi tulemusi.

Osa 3: Andmete analüüs (ICMP päringud)

Wiresharki andmed kuvatakse kolmes jaotises:
1. Ülemine jaotis: Kuvab kõik püütud PDU kaadrid koos kokkuvõttega IP-paketi teabest.
2. Keskmine jaotis: Näitab valitud kaadri teavet erinevatel protokollikihtidel (Ethernet, IP, ICMP).
3. Alumine jaotis: Kuvab toorandmeid heksaadetsimaalses ja kümnendsüsteemis.

a. Vali esimene ICMP päringu kaader ja vaata allika ja sihtkoha IP-aadresse.
b. Klõpsa keskmises jaotises 'Ethernet II', et vaadata MAC-aadresse.
c. Klõpsa 'IPv4', et näha sihtkoha ja allika IP-aadresse.

Märkus: ICMP andmed on kapseldatud IPv4 paketti, mis omakorda on kapseldatud Ethernet II raami.

Küsimused:

1. Milline IP-aadress püüti pingimise ajal veebisaidile www.google.com?
   - Vastus: [Õpilane täidab]

2. Millist tööriista kasutasid võrgu liikluse püüdmiseks?
   - Vastus: [Õpilane täidab]

3. Lisa ekraanipilt Wiresharki ICMP liikluse püügist.
   - Vastus: [Õpilane lisab]