LAV10 - WireShark

Program WireShark je odlično orodje za analizo omrežnega prometa. Analizirajte naslednje datoteke in odgovorite na vprašanja. Napišite tudi kratek opis kako ste to našli.

Pomagajte si z internetom!

Datoteka LAV10_A.pcapng

1. Ugotovi MAC in IP naslov računalnika ter proizvajalca mrežne kartice
    - MAC:
    - IP:
    - proizvajalec:
2. Kakšen je IP naslov DNS strežnika, ki ga uporablja ta računalnik
    - IP:
3. Napiši vsaj 3 spletne strani (domene), ki jih je obiskal uporabnik računalnika
    - domena 1:
    - domena 2:
    - domena 3:
4. Napiši zaporedne številke vsaj enega TCP začetka seje
    - zap. številka paketka SYN:
    - zap. številka paketka SYN, ACK:
    - zap. številka paketka ACK:
5. Koliko bajtov je velikost največjega okvirja, ki ga je prejel ali poslal računalnik? Kdo ga je poslal komu?
    - velikost v bajtih:
    - IP pošiljatelja:
    - IP prejemnika:

Lastni zajem

Začnite zajem prometa na svojem računalniku. Medtem v cmd poženite ukaz `ipconfig /renew` ko ta konča ustavite zajem prometa. Odgovorite na naslednja vprašanja.

1. Ali ima vaš računalnik vklopljen IPv6 protokol?
    - odgovor + razlaga:
2. Napišite naslov DHCP strežnika, ki je vašemu računalniku dodelil IP naslov
    - IP naslov strežnika:
    - kateri DHCP naslov je bil dodeljen:
    - za koliko časa je bil dodeljen:

3. Koliko ARP poizvedb se je zgodilo v času zajemanja prometa. Kdo je proizvajalec mrežne kartice te naprave?
    - število poizvedb:
    - proizvajalec:
4. Kliknite na Statistics > Conversations. Kateri napravi (IPv4) je vaš računalnik postal največ podatkov? Koliko časa je trajala ta povezava?
    - IP naslov naprave:
    - količina podatkov:
    - trajanje povezave:

Datoteka LAV10_B.pcapng

1. Ali lahko ugotoviš kaj je vsebina spletne strani, ki jo je računalnik obiskal na IP naslovu `192.168.107.57`. (Namig: desni klik na paket > Follow > HTTP Stream)
    - nekaj besed, ki se pojavi na spletni strani:
2. Koliko je skupno število zajetih paketov v tej datoteki? Koliko časa je računalnik zajemal omrežni promet?
    - število paketov:
    - čas zajemanja:
3. Koliko ARP poizvedb se je zgodilo v času zajemanja prometa
    - število poizvedb:
4. Napiši ime vsaj ene slike, ki se je prenesla ob obisku spletne strani (uporabi isti trik kot pri 1. nalogi):
    - ime slike:

Datoteka LAV10_C.pcapng

1. Katera TCP vrata (port) uporablja protokol Telnet (na strežniku)
    - vrata:
2. Katera vrata je operacijski sistem dodelil Telnet odjemalcu (client)?
    - vrata:
3. Ali lahko najdeš uporabniško ime in geslo, ki ju je uporabnik vpisal, da se je na strežnik povezal preko protokola Telnet. (Namig: desni klik na paket > Follow > TCP stream; Rdeče je kar smo poslali, modro kar smo prejeli).
    - IP naslov strežnika:
    - uporabniško ime:
    - geslo:
    - ukaz, ki da je uporabnik izvedel na strežniku: