Cvičení 4

1. Připravte si vstupní data:
   (a) poskytnutý pcap záchyt dekompresujte do Vámi vybraného adresáře
   (b) převeďte si vstupní data do formátu, které umí zpracovávat Vámi vybrané knihovny

   - ***Tento krok můžete vynechat a použít už exportovaná data.***
   - *Pokud si to chcete zkusit, Wireshark (nás zajímá hlavně jeho součást 'tshark') by měl být dostupný i pro MacOS.*
   - *Ve windows potom výsledný příkaz vypadá takto:* `tshark.exe -T fields -e frame.number -e frame.time_relative -e frame.len -e eth.src -e eth.dst -e eth.type -e arp.opcode -e arp.src.hw_mac -e arp.src.proto_ipv4 -e arp.dst.hw_mac -e arp.dst.proto_ipv4 -e ip.src -e ip.dst -e ip.proto -e tcp.srcport -e tcp.dstport -e udp.srcport -e udp.dstport -E header=y -E separator=, -r file.pcap > file.csv.`
   - *Kde každý parametr* `-e something` *označuje sloupec který má výsledné CSV obsahovat. Jejich seznam naleznete v pdf přiloženém k originálnímu zadání.*
   - *Vybrat DNS servery obsahující daný substring pak můžete pomoci 'dns.qry.name contains "substring"'*

2. Data načtěte do paměti a zjistěte základní charakteristiky komunikační sítě:

   - Pokud jste vynechali krok 1 tak použijte **jenom** soubor viber.csv
   - celkový počet komunikujících zařízení,tj. IP a MAC adresy,
   - celkový počet přenesených paketů,
   - celkový počet zdrojových IP adres,
   - celkový počet cílových IP adres.

   - ***zajímá nás jenom traffic přes TCP a UDP protokoly***
   - *'ip.proto' sloupec obsahuje info o protokolu (tcp = 6, udp = 17)*

- *každý řádek csv je jeden paket*
- *'frame.len' sloupec obsahuje velikost paketu v bytech*
- *'eth.src' a 'eth.dst' jsou zdrojová a cílová MAC adresa*
- *'ip.src' a 'ip.dst' jsou zdrojová a cílová IP*
- *počet zařízení je rovný počtu unikátních MAC adres*

3. Vytvořte vizualizaci lokálních komunikační sítí mezi MAC a IP adresami. *Bude to bipartitní graf - MAC a IP*

4. Vytvořte vizualizaci komunikační sítě mezi IP adresami, tj. dvě IP adresy komunikují, pokud byl mezi přenesen alespoň jeden paket v rámci TCP či UDP protokolu.

5. Identifikujte Viber servery podle protokolu DNS.

   - *Pokud jste vynechali krok 1, použijte soubor v-dns.csv*
   - *IP adresy jsou ve sloupci 'Source'.*
   - *sloupec 'Info' obsahuje informace o DNS dotazu. Prohledejte je na klíčové slovo "viber.com" a nalezněte všechny domény služby viber*
   - *propojte IP adresy a domény služby viber a zobrazte je v tabulce.*

6. Hotovo.