

Lënda: Rrjetat Kompjuterike

**Fletore e Ushtrimeve Laboratorike Laboratori
Katër**

v 7.0

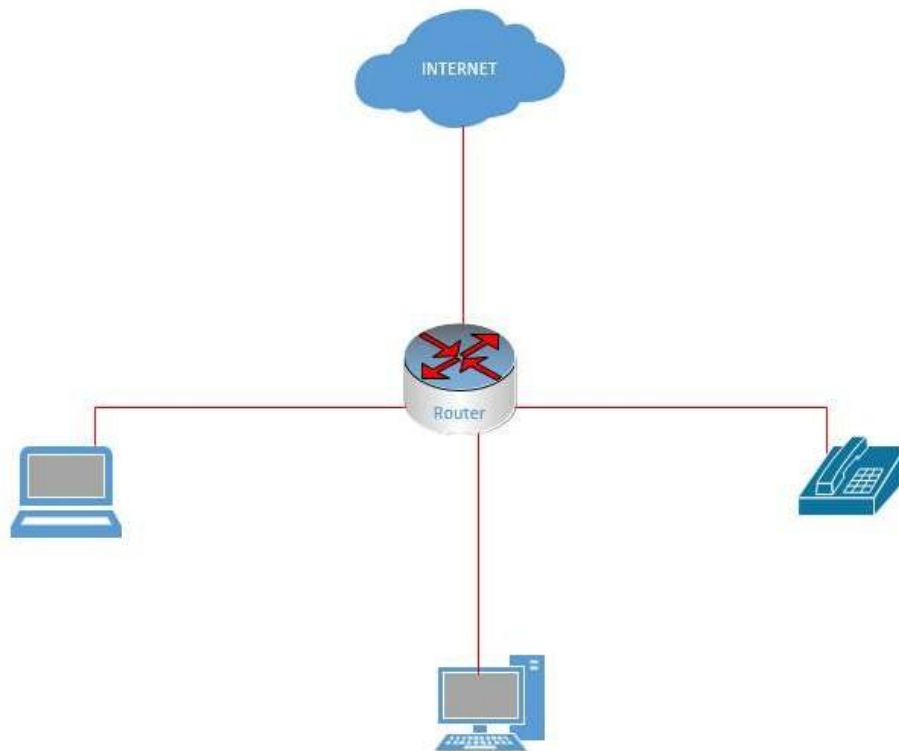
Lamir Shkurti

Behar Haxhismajli

Viti Akademik 2023/2024

Laboratori 4 – Analiza e trafikut në rrjetë duke përdorur Wireshark

Topologjia



Objektivat

Detyra 1: Me Wireshark të kapen dhe analizohen të dhënat lokale të ICMP-së

- Filloni dhe ndalni kapjen e të dhënave të trafikut të ping tek hostët lokal.
- Gjeni IP dhe MAC adresën në PDU-të e kapura.

Detyra 2: Me Wireshark të kapen dhe analizohen të dhënat e largëta të ICMP-së

- Filloni dhe ndalni kapjen e të dhënave të trafikut të pingut tek hostët e largët.
- Gjeni IP dhe MAC adresën në PDU(Protocol Data Unit)-të e kapura.
- Sqaroni pse MAC adresat për hostët e largët dallojnë nga ato të hostëve lokal.

Skenari

Wireshark është një softuer që shërben për analizimin e protokolleve, por gjithashtu është një aplikacion ndryshe i quajtur si “vjedhës i paketave”, i cili përdoret për të analizuar rrjetën, softuerët si dhe protokollet. Përderisa të dhënat qarkullojnë nëpër rrjetë, “vjedhësi i paketave” kap secilin PDU (Protocol Data Unit) dhe mund të dekodoj dhe analizoj përmbajtjen e PDU-së bazuar në RFC(Request for Comments) adekuate apo specifikacionet tjera.

Wireshark është një vegël shumë e dobishme për këdo që punon me rrjetet kompjuterike dhe mund të përdoret për shumicën e ushtrimeve në kurset CCNA për analizimin e të dhënave dhe për përcaktimin e problemeve në rrjetë. Në këtë ushtrim janë të përfshira instruksionet për shkarkimin dhe instalimin e Wireshark, edhe pse ju mund ta keni atë të instaluar tashmë në kompjuter. Në këtë ushtrim, ju do të përdorni Wireshark për të kapur IP adresat e paketave të të dhënave të ICMP(Internet Control Message Protocol)-së dhe MAC adresat e kornizave të Ethernet.

Resurset e Nevojshme

- Një Kompjuter (Windows 10, Linux Unix që ka qasje në internet)
- Kompjuter shtesë në një LAN(Local Area Network) do të përdoren për tu përgjigjur kërkesave të pingut. “Vjedhësi i paketave i kap të gjitha njësitë e të dhënave të protokollit (PDU) dhe mund të dekodoj dhe analizoj përmbajtjen e tij bazuar në RFC-të e përshtatshëm apo specifikacionet tjera.

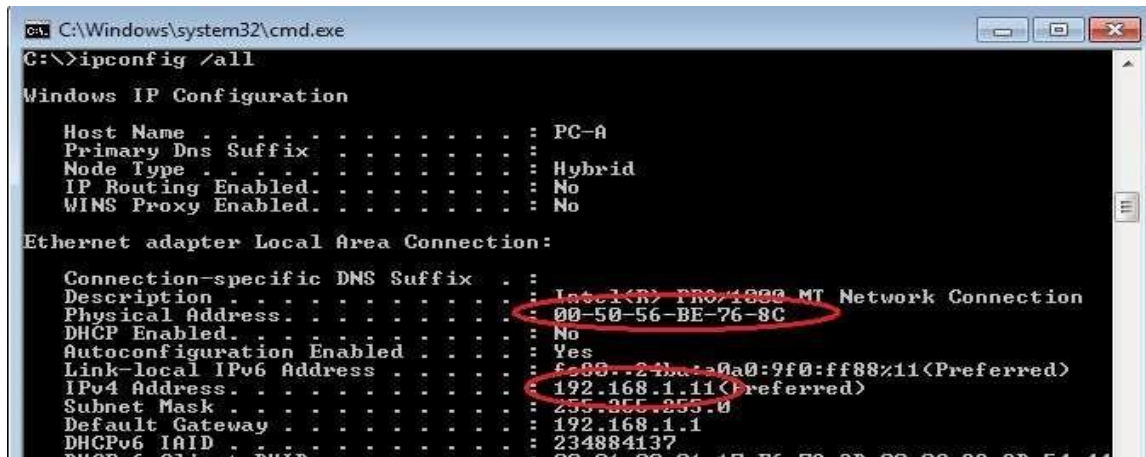
Detyra 1: Me Wireshark të Kapen dhe Analizohen të Dhënat Lokale të ICMPsë

Në pjesën e dytë të ushtrimit, ju do të pingoni një tjetër kompjuter në LAN dhe do të kapni kërkesat dhe përgjigjet e ICMP-së me anë të Wireshark. Ju gjithashtu duhet të analizoni paketat e kapura, dhe me anë të kësaj analize ju do të keni një pasqyrë më të qartë se si hederët e paketave përdoren për të transmetuar të dhënat tek destinacioni i tyre.

Hapi 1: Rishiko ndërfaqet e adresave të kompjuterit tuaj

Për këtë ushtrim, ju duhet të rishikoni IP adresën e kompjuterit tuaj dhe adresën fizike të NIC(Network Interface Card), të quajtur MAC adresë.

- Hapni dritaren e komandave dhe shkruani **ipconfig/all**, dhe shtypni Enter.
- Shkruani në fletore IP dhe MAC adresën e kompjuterit tuaj.



```
C:\Windows\system32\cmd.exe
C:\>ipconfig /all

Windows IP Configuration

Host Name . . . . . : PC-A
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

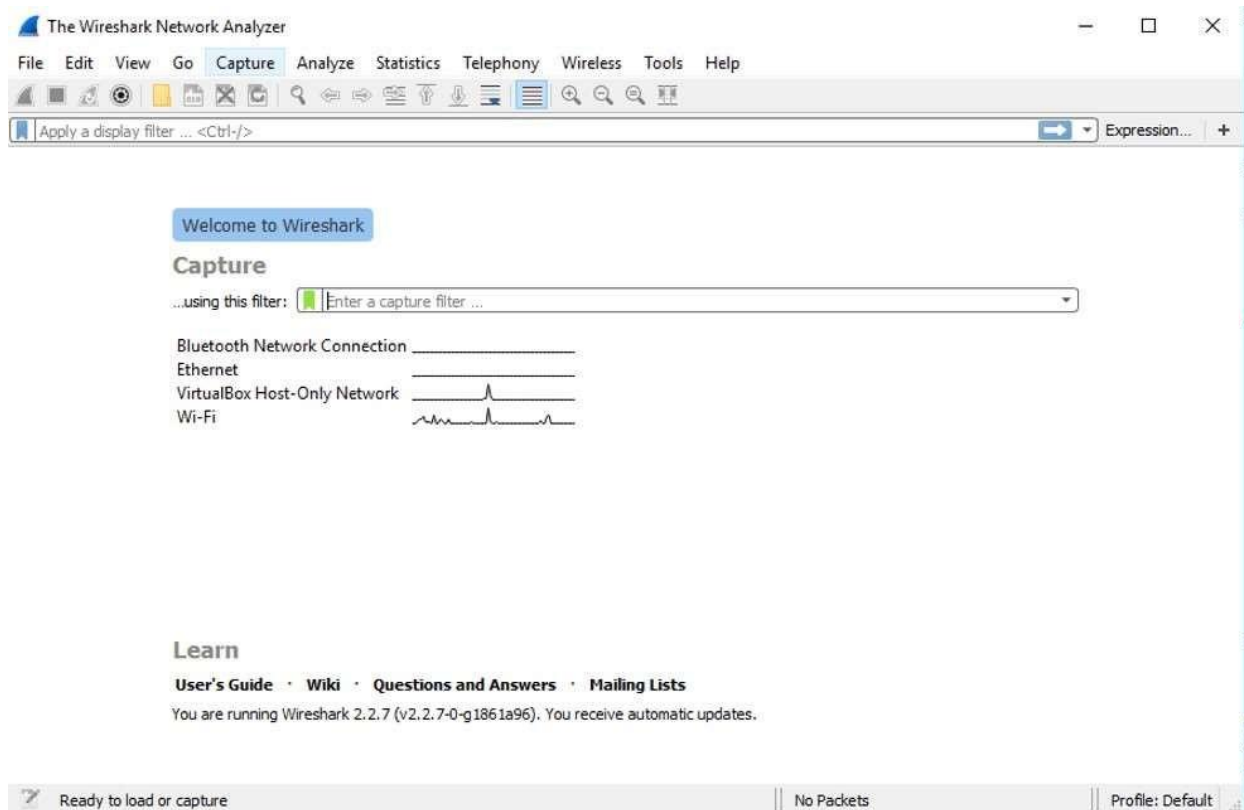
Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . . : .
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address. . . . . : 00-50-56-BE-76-8C
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::21b:56:be:76%11(Preferred)
IPv4 Address. . . . . : 192.168.1.11(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 234884137
DHCPv6 Client DUID . . . . . : 00-01-00-01-15-B6-73-2D-88-8C-30-0D-F4-44
```

- Pyetni një koleg tuajin për IP adresën e kompjuterit tuaj dhe tregojani atij IP adresën e kompjuterit tuaj. Në këtë fazë mos ia tregoni MAC adresën e kompjuterit tuaj kolegut tuaj.

Hapi 2: Startoni Wireshark dhe filloni kapjen e të dhënave.

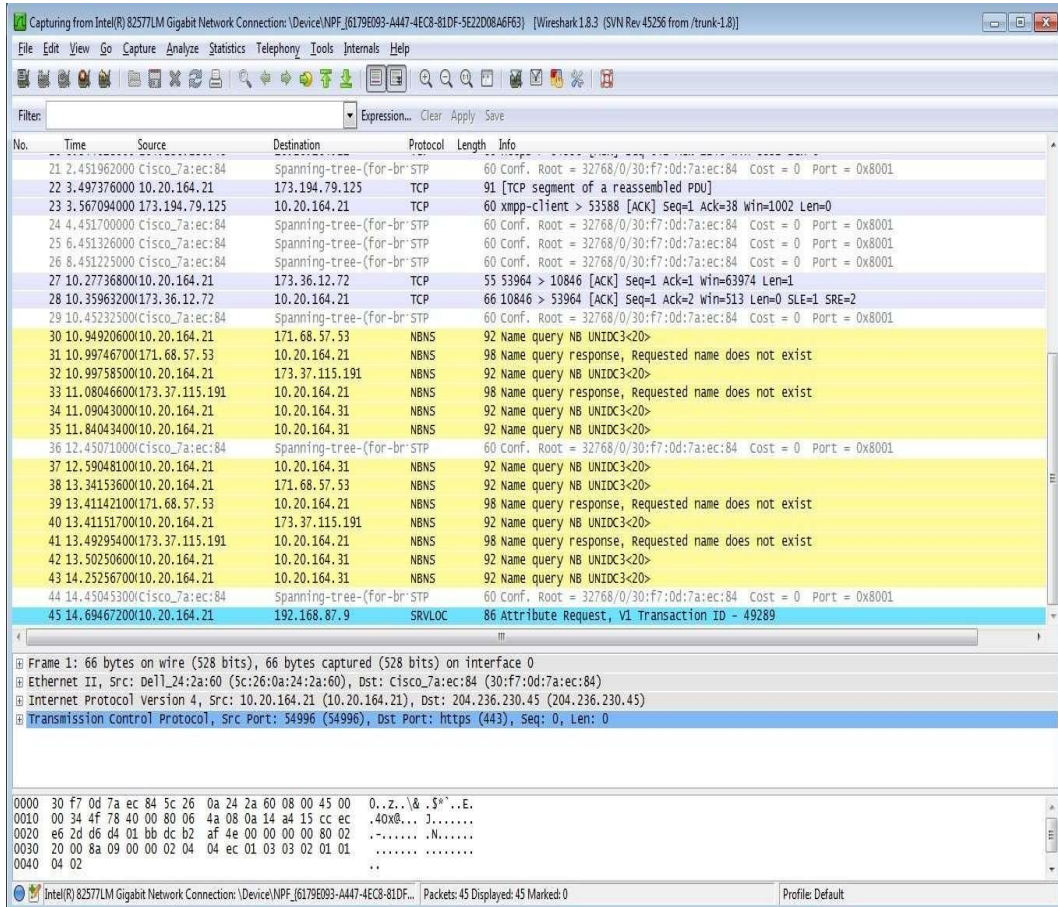
- a. Në kompjuterin tuaj, klikoni butonin me logon e Windows **Start** për të parë Wireshark të listuar tek programet në menyë kryesore. Klikoni dy herë në **Wireshark**.



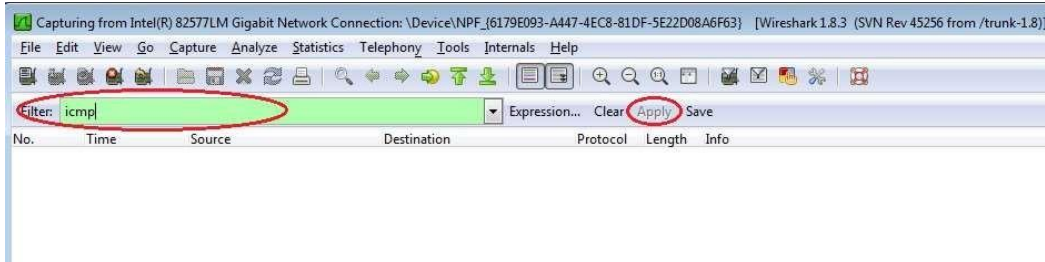
Vërejtje: Lista e ndërfaqeve paraqitet edhe nëse klikohet **Capture/Interfaces**.

- b. Pasi të startohet Wireshark dhe pasi të paraqitet dritarja *Capture Interfaces*, klikoni butonin kontrollues përkrah ndërfaqes që ju jeni të lidhur me Wi-fi.

Informacioni do të fillojë të paraqitet në dritaren e Wireshark. Linjat e të dhënave do të paraqiten në ngjyra të ndryshme bazuar në protokollet përkatëse.

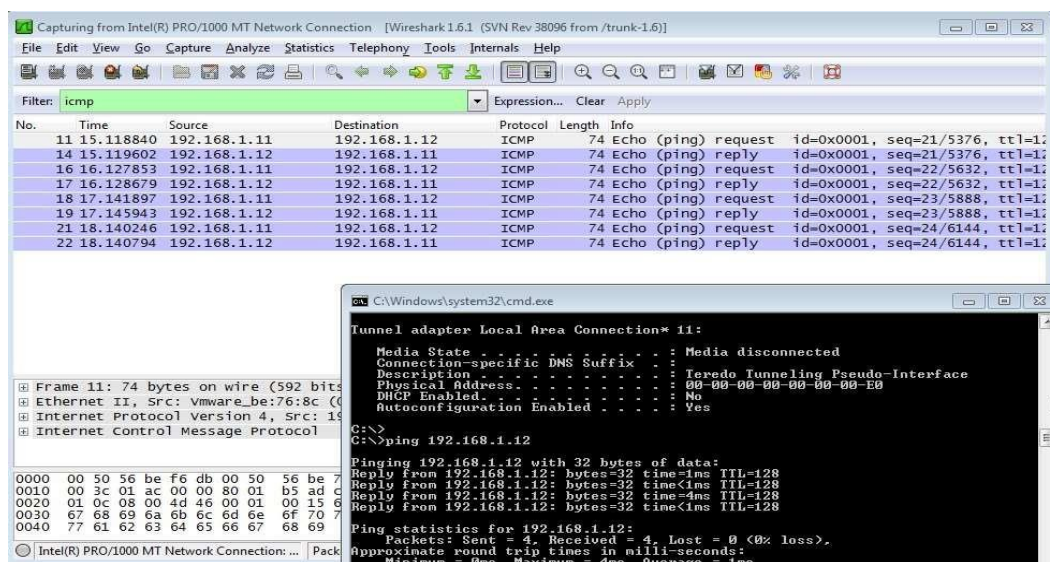


- c. Informacioni mund të shtohet me shpejtësi të madhe, varësisht nga lloji i komunikimit që është duke u zhvilluar ndërmjet kompjuterit tuaj dhe LAN-it. Ne mund të aplikojmë një filtër për ta bërë më të lehtë shikimin dhe punën me të dhënat që janë kapur nga Wireshark.



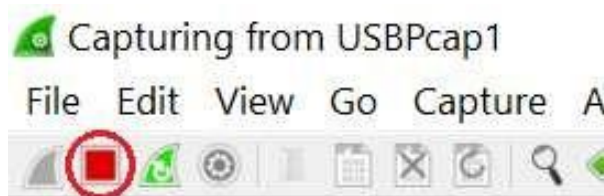
Në këtë ushtrim ne dëshirojmë të shohim vetëm PDU-të e ICMP-së (ping).

Aplikimi i filtrit bën që të gjitha të dhënat në dritaren kryesore të largohen megjithëse kapja e trafikut që kalon nëpër ndërfaqe vazhdon. Hapeni përsëri dritaren e komandave që e keni hapur më herët dhe pingoni IP adresën që e keni marrë nga kolegu juaj. Vëreni që tashmë fillojnë të paraqiten të dhëna përsëri në dritaren kryesore të Wireshark.



Vërejtje: Nëse kompjuteri i kolegut tuaj nuk jep përgjigje ndaj pingut tuaj, kjo mund të ndodh për shkak se Firewall i kompjuterit të tij është duke i bllokuar kërkesat e pingut. Shikoni shtojcën A “Të lejohet trafiku ICMP përgjatë një Firewall” për të marrë informacione shtesë për mënyrën se si të lejohet kalimi i trafikut të ICMP-së përgjatë Firewall duke përdorur Windows 7.

- d. Ndalni kapjen e të dhënave duke klikuar ikonën e **Stop Capture**.



Hapi 3: Kontrolloni të dhënat e kapura

Në hapin 3, kontrolloni të dhënat që janë gjeneruar nga kërkesa ping që keni bërë ndaj kompjuterit të kolegut tuaj. Të dhënat e Wireshark janë paraqitur në tre seksione: 1) Seksioni kryesor paraqet një listë të kornizave PDU të kapura, me një përmbledhje të informacionit për paketat IP të listuara, 2) Seksioni i mesëm paraqet një listë të informacionit të PDU-së për kornizat e zgjedhura në pjesën kryesore të dritares dhe i ndan kornizat e PDU-së në bazë të shtresave të protokollit, dhe 3) seksioni në fund paraqet të dhënat e papërpunuara nga secili nivel. Të dhënat e papërpunuara janë paraqitur edhe në formën decimale edhe në atë heksadecimale.

Wireshark interface showing packet capture data for ICMP. The top section displays a list of packets. The middle section shows the details of a selected packet (Frame 11). The bottom section shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
11	15.118840	192.168.1.11	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=21/5376, ttl=128
14	15.119602	192.168.1.12	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=21/5376, ttl=128
16	16.127853	192.168.1.11	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=22/5632, ttl=128
17	16.128679	192.168.1.12	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=22/5632, ttl=128
18	17.141897	192.168.1.11	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=23/5888, ttl=128
19	17.145943	192.168.1.12	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=23/5888, ttl=128
21	18.140246	192.168.1.11	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=24/6144, ttl=128
22	18.140794	192.168.1.12	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=24/6144, ttl=128

Top Section

Frame 11: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

Ethernet II, Src: IntelCor_34:92:1c (58:94:6b:34:92:1c), Dst: Intel_Of:91:48 (00:11:11:0f:91:48)

Internet Protocol Version 4, Src: 192.168.1.11 (192.168.1.11), Dst: 192.168.1.12 (192.168.1.12)

Internet Control Message Protocol

Middle Section

0000 00 50 56 be f6 db 00 50 56 be 76 8c 08 00 45 00 .PV....P V.v...E.
0010 00 3c 01 ac 00 00 80 01 b5 ad c0 a8 01 0b c0 a8 .<.....
0020 01 0c 08 00 4d 46 00 01 00 15 61 62 63 64 65 66MF... ..abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69 wabcdegh

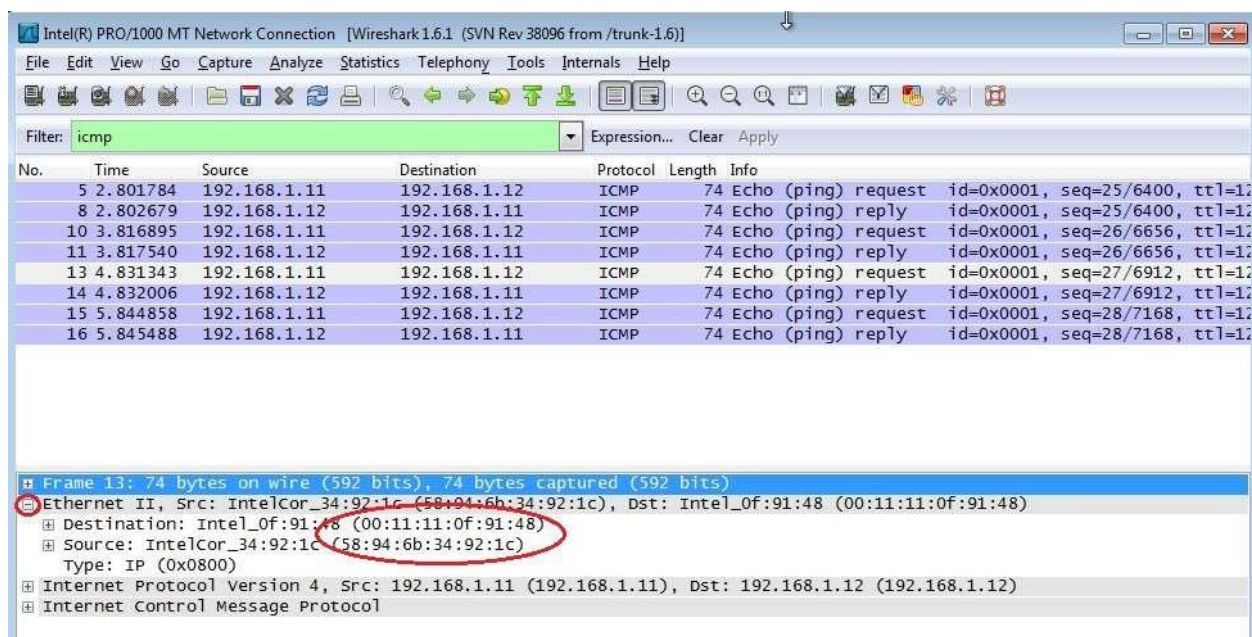
Bottom Section

g. Fillimisht klikoni kërkesën e parë ICMP të kornizave PDU në seksionin kryesor të Wireshark. Shikoni që kolona e burimit e ka IP adresën e kompjuterit tuaj, dhe destinacioni përmban IP adresën e kompjuterit të kolegut tuaj që e keni pinguar.

Wireshark interface showing packet capture data for ICMP. The top section displays a list of packets. The middle section shows the details of a selected packet (Frame 13). The bottom section shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
5	2.801784	192.168.1.11	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=25/6400, ttl=128
8	2.802679	192.168.1.12	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=25/6400, ttl=128
10	3.816895	192.168.1.11	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=26/6656, ttl=128
11	3.817540	192.168.1.12	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=26/6656, ttl=128
13	4.831343	192.168.1.11	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=27/6912, ttl=128
14	4.832006	192.168.1.12	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=27/6912, ttl=128
15	5.844858	192.168.1.11	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=28/7168, ttl=128
16	5.845488	192.168.1.12	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=28/7168, ttl=128

Me këtë kornizë PDU ende të selektuar në seksionin kryesor, navigoni në seksionin e mesëm dhe klikoni shenjën e plusit në të majtë të rreshtit të Ethernet për të shikuar MAC adresat e burimit dhe destinacionit.



A përputhet MAC adresa e burimit me ndërfaqen e kompjuterit tuaj?

A përputhet MAC adresa e destinacionit në Wireshark me MAC adresën e kompjuterit të kolegut tuaj?

Cila është MAC adresa e kompjuterit të pinguar e cila fitohet nga kompjuteri juaj?

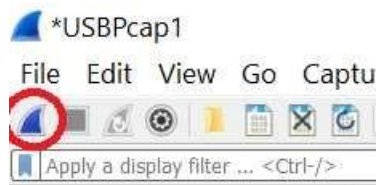
Vërejtje: Në shembullin vijues të kërkesës ICMP të kapur, të dhënat e ICMP-së janë enkapsuluar brenda PDU paketës së IPv4 e cila pastaj është enkapsuluar në një ethernet II kornizë PDU për transmetim në LAN.

Detyra 2: Me Wireshark të kapen dhe analizohen të dhënat e largëta të ICMPsë

Në pjesën e tretë, ju do të pingoni një host në distancë (host që nuk është në LAN) dhe do të ekzaminoni të dhënat që gjenerohen nga këto pingime. Pas ekzaminimit të të dhënave, ju do të tregoni dallimin ndërmjet të dhënave të tanishme nga ato të analizuara në pjesën 2.

Hapi 1: Filloni kapjen e të dhënave në ndërfaqe

- a. Klikoni ne butonin start ku gjendet në të majtë lartë të menysë kryesore.



- b. Një dritare paraqitet për të ruajtur të dhënat që janë kapur më herët përpara se të fillon kapja e të dhënave tjera. Nëse nuk është e domosdoshme që të ruhen këto të dhëna atëherë klikoni **Continue Without Saving**.



Me kapjen aktive, pingoni URL-të e tre ueb sajteve në vijim:

- i. www.yahoo.com
- ii. www.cisco.com
- iii. www.microsoft.com

```
C:\Windows\system32\cmd.exe

C:\>ping www.yahoo.com

Pinging www.yahoo.com [72.30.38.140] with 32 bytes of data:
Reply from 72.30.38.140: bytes=32 time=1ms TTL=255
Reply from 72.30.38.140: bytes=32 time<1ms TTL=255
Reply from 72.30.38.140: bytes=32 time<1ms TTL=255
Reply from 72.30.38.140: bytes=32 time<1ms TTL=255

Ping statistics for 72.30.38.140:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping www.cisco.com

Pinging www.cisco.com [198.133.219.25] with 32 bytes of data:
Reply from 198.133.219.25: bytes=32 time<1ms TTL=255
Reply from 198.133.219.25: bytes=32 time<1ms TTL=255
Reply from 198.133.219.25: bytes=32 time<1ms TTL=255
Reply from 198.133.219.25: bytes=32 time<1ms TTL=255

Ping statistics for 198.133.219.25:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping www.google.com

Pinging www.google.com [74.125.129.99] with 32 bytes of data:
Reply from 74.125.129.99: bytes=32 time=1ms TTL=255
Reply from 74.125.129.99: bytes=32 time<1ms TTL=255
Reply from 74.125.129.99: bytes=32 time<1ms TTL=255
Reply from 74.125.129.99: bytes=32 time<1ms TTL=255

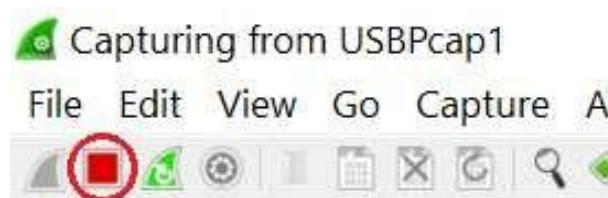
Ping statistics for 74.125.129.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>_
```

Vërejtje:

Kur të pingoni URL-të e listuara këtu, shikoni se DNS(Domain Name Server) e përkthen URL-në në një IP adresë. Shikoni IP adresën e pranuar për secilin URL.

- c. Ju mund të ndalni kapjen e të dhënave duke klikuar ikonën e **Stop Capture**.



Hapi 2: Ekzaminimi dhe analizimi i të dhënave nga hostët e largët.

- a. Rishikoni të dhënat që janë kapur në Wireshark, ekzaminoni IP dhe MAC adresat e tre lokacioneve që ju keni pinguar. Listoni IP dhe MAC adresat e destinacioneve për të tre lokacionet përkatëse në hapësirën më poshtë.

Lokacioni 1: IP: MAC: _____:_____:_____:_____:_____:_____

Lokacioni 2: IP: MAC: _____:_____:_____:_____:_____:_____

Lokacioni 3: IP: MAC: _____:_____:_____:_____:_____:_____

- b. Çka është e rëndësishme për këtë informacion?

- c. Çfarë dallon ky informacion nga informacioni i pingut lokal që e pranuat në pjesën e dytë?

Pyetje:

Pse Wireshark e paraqet MAC adresën aktuale të hostëve lokal, por jo MAC adresën aktuale të hostëve të largët?

Detyra 3: Gjurimi i DNS me Wireshark

Në pjesën e tretë të ushtrimit, ju do të përdorni veglën nslookup në një domain të caktuar dhe do të kapni kërkesat dhe përgjigjet e DNS me anë të Wireshark. Ju gjithashtu duhet të analizoni paketat e kapura, dhe me anë të kësaj analize ju do të keni një pasqyrë më të qartë se si hederët e paketave përdoren për të transmetuar të dhënat tek destinacioni i tyre.

NSLOOKUP:

Në këtë laborator, ne do të përdorim mjetin nslookup, i cili është në dispozicion në shumicën e platformave Microsoft/Linux/Unix sot. Për të ekzekutuar nslookup në Windows / Linux / Unix, thjesht shkruani komandën nslookup në command line.

Në operacionin më themelor, mjeti nslookup lejon hostin që drejton mjetin të kërkojë ndonjë server të specifikuar DNS për një rekord DNS si psh (IP Adresën). Një DNS server mund të jetë; root DNS server, top-level-domain DNS server, authoritative DNS server, ose një server ndërmjetësues DNS (intermediate DNS server). Për të përmbushur këtë detyrë, nslookup dërgon një DNS query në DNS server-in e caktuar, merr një përgjigje nga i njëjti server DNS dhe tregon rezultatin.

Shembull:

```
C:\Users\dell>nslookup www.ubt-uni.net
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:     www.ubt-uni.net
Addresses: 2606:4700:30::681c:e28
           2606:4700:30::681c:f28
           104.28.15.40
           104.28.14.40
```


Hapi 1: Përdorni ipconfig për të pastruar DNS cache në hostin tuaj

Për të pastruar domain-ët dhe IP adresat që ruhen në DNS chache të hostit tuaj duhet përdorur komanda: **ipconfig /flushdns**

Shfaqja e DNS cache paraprak me anë të komandes **ipconfig /displaydns**

```
C:\Users\dell>ipconfig /displaydns

Windows IP Configuration

    fcmconnection.googleapis.com
    -----
    Record Name . . . . . : fcmconnection.googleapis.com
    Record Type . . . . . : 1
    Time To Live . . . . . : 293
    Data Length . . . . . : 4
    Section . . . . . : Answer
    A (Host) Record . . . : 172.217.23.106

    imap.gmail.com
    -----
    Record Name . . . . . : imap.gmail.com
    Record Type . . . . . : 1
    Time To Live . . . . . : 288
    Data Length . . . . . : 4
    Section . . . . . : Answer
    A (Host) Record . . . : 74.125.206.109

    Record Name . . . . . : imap.gmail.com
    Record Type . . . . . : 1
    Time To Live . . . . . : 288
    Data Length . . . . . : 4
    Section . . . . . : Answer
    A (Host) Record . . . : 74.125.206.108
```

Shfaqja e DNS cache pasi që e përdorim komanden: **ipconfig /flushdns**

```
C:\Users\dell>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\dell>ipconfig /displaydns

Windows IP Configuration

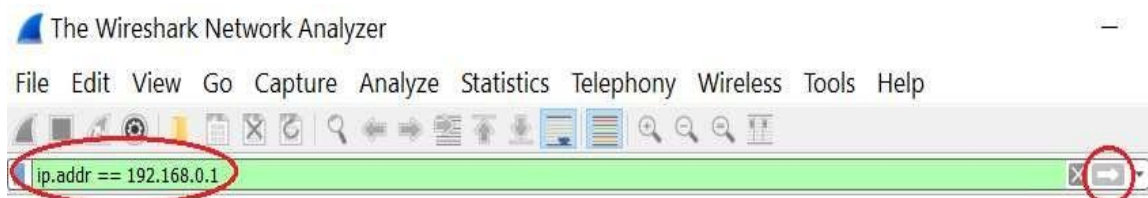
Could not display the DNS Resolver Cache.
```

Hapi 2: Të bëhet hapja e Wireshark në PC e juaj dhe filloni kapjen e paketave

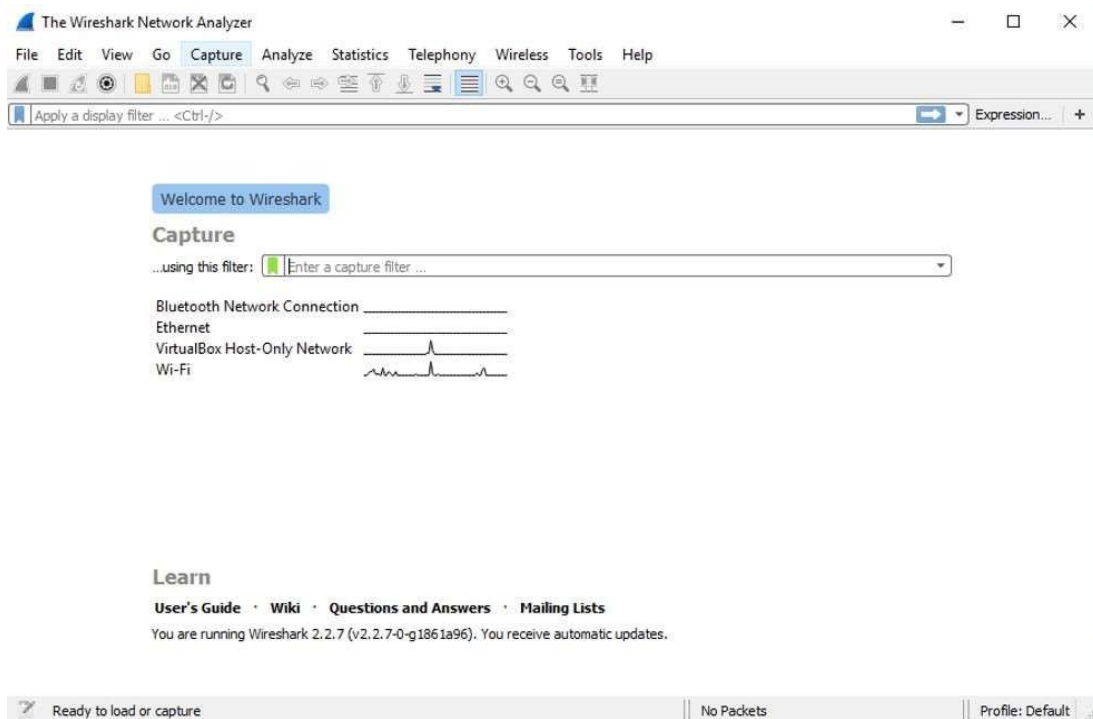
a) Të klikohet ikona e Wireshark

b) Shkruani në fushën e aplikimit të filtrit “ip.addr == your_IP_address” ku kjo bën që të gjitha të dhënat në dritaren kryesore të largohen megjithëse kapja e trafikut që kalon nëpër ndërfaqe vazhdon dhe vetëm shfaqë paketat të cilat burim ose destinacion kanë IP adresën e juaj.

Hint: Përdorni komandën ipconfig në cmd për të gjetur IP Adresën e kompjuterit tuaj.



c) Pasi të paraqitet dritarja *Capture Interfaces*, klikoni butonin kontrollues përkrah ndërfaqes që ju jeni të lidhur me Wi-fi.

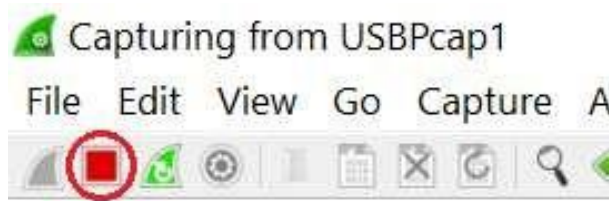


d) Pasi të zgjedhet ndërfaqja Wi-fi në *Capture Interfaces*, ekzekutoni komandën nslookup me domain www.ubt-uni.net.

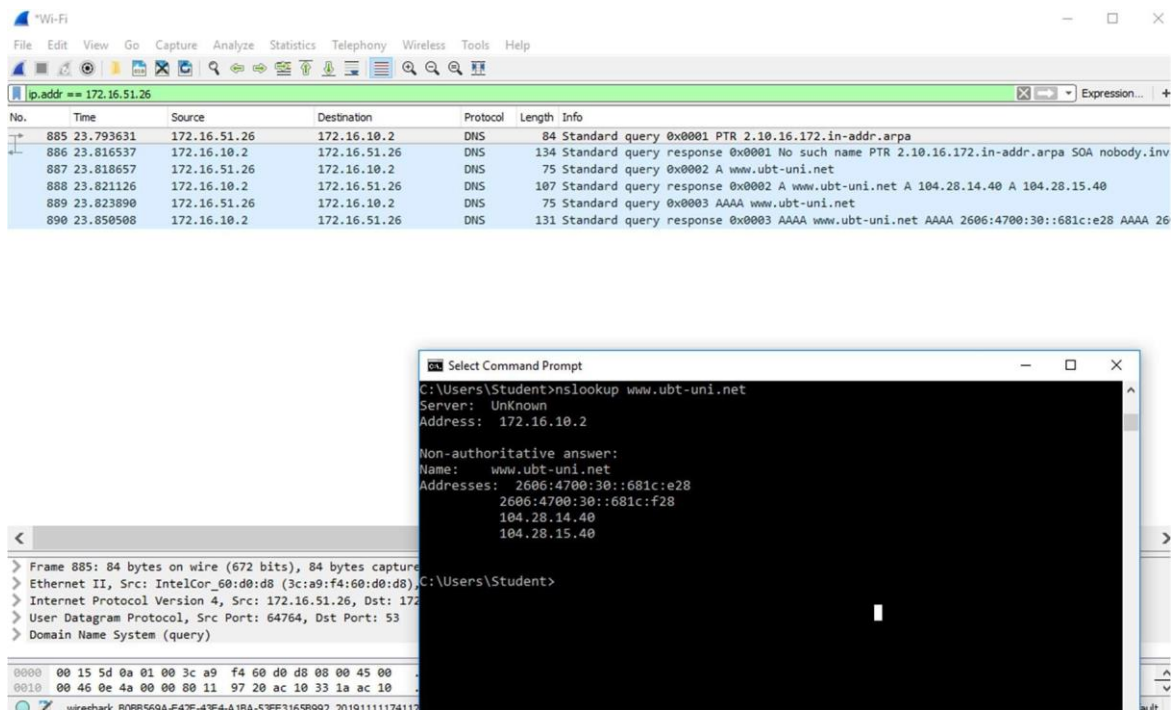
```
C:\Users\dell>nslookup www.ubt-uni.net
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:     www.ubt-uni.net
Addresses: 2606:4700:30::681c:e28
           2606:4700:30::681c:f28
           104.28.14.40
           104.28.15.40
```

f) Ndalni kapjen e të dhënave duke klikuar ikonën e **Stop Capture**.



g) Rezultati I fituar duhet të jetë si më poshtë:



Shënim shtesë:

Ne shohim nga pamja e mësipërme që nslookup dërgoi në të vërtetë tre pyetje DNS dhe mori tre përgjigje DNS.

Pyetje:

- a) Cili është porti i destinacionit për mesazhin e pyetjes (query message) DNS? Cila është porti i burimit të mesazhit të përgjigjes (response message) DNS?

- b) Në cilën adresë IP dërgohet mesazhi i pyetjes (query message) DNS? A është kjo IP adresa e DNS serverit tuaj lokal ?

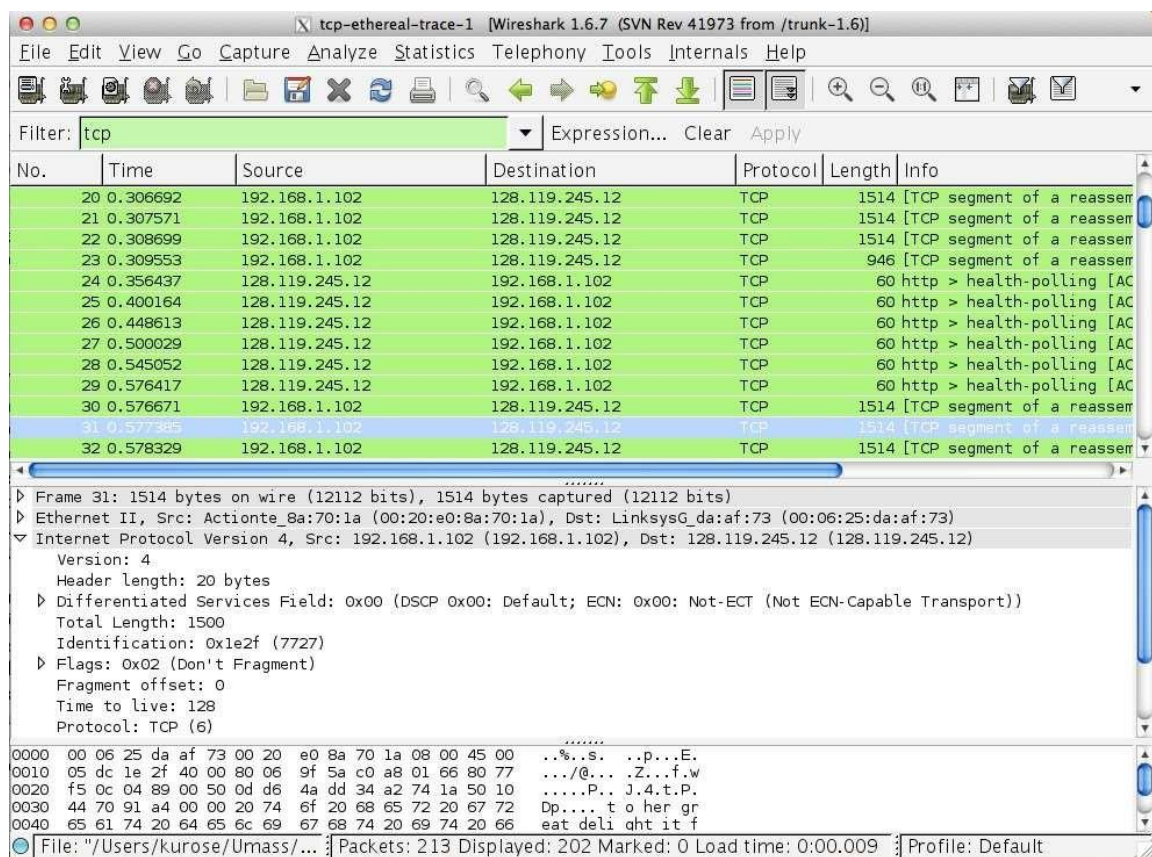
Hint: Përdorni ipconfig për të përcaktuar IP adresën e serverit tuaj lokal DNS. A janë të njëjta këto dy adresa IP ?

TCP

Shiqoni me kujdes parametrat e paketit te TCP protokolit dhe pastaj do te analizojm trafikun e TCP protocol ne Wireshark.

- Ne fillim duhet bere nje inicim I nje kerkese ne internet ku do te pastrohet Historija ne web browser dhe pastaj te vizitohet web faqja www.ubt-uni.net .
- I gjith procesi duhet te behet ashtu qe te startohet Wireshark e pastaj te inicohet hapja e Web faqes se kerkuar me lart.
-

Pasi qe te iniconi lidhjen me web faqen ju shkarkoni nje fajll ne web faqe nga ushtrimet e juaja qe gjinden ne Moodle dhe pastaj te analizohet TCP protokoli.



Pyetje:

- Cila eshte IP adresa e burimit dhe numri TCP portit te kompjuterit tuaj si dhe, numri I portit te perdorur per webfaqen ku eshte inicuar lidhja ?