FAKULTETI I TEKNOLOGJISE SE INFORMACIONIT

Laboratori: Rrjeta Telematike

Punë laboratori Nr 2

Tema: Analiza ne Wireshark i protokolleve te modelit OSI.

Objektivat:

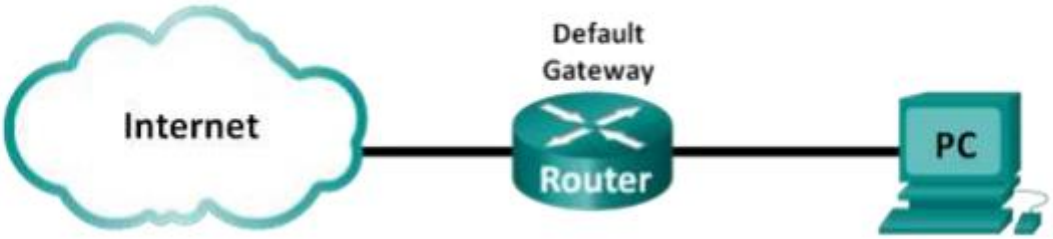
Pjesa 1: Gjeni informacionin e konfigurimit IP të kompjuterit tuaj.

Pjesa 2: Përdorni Wireshark për te kapur paketat HTTP, ICMP.

Pjesa 3: Analizoni paketat e kapura.

Punoi:Piro Gjikdhima

Topology



Burimet e kërkuara:

1. **1 PC (Windows 7 ose 8, akses në internet dhe instalimi i Wireshark)**

Pjesa 1: Gjeni informacionin e konfigurimit IP të kompjuterit tuaj

Perdorni komanden ipconfig/all ne CMD për te plotesuar hapsirat e tabeles se meposhtme:

IP address	**192.168.1.3**
MAC address	**F8-9E-94-E6-A7-C1**
Default gateway IP address	**192.168.1.1**
DNS server IP address	**192.168.1.1**

Pjesa 2: Përdorni Wireshark për te kapur DNS Queries, HTTP, ICMP

Në Pjesën 2 ju do të perdorni Wireshark për të kapur paketat DNS për të demonstruar përdorimin e protokollit te transportit UDP gjatë komunikimit me një server DNS.

a. Klikoni butonin Start të Windows dhe hapni programin Wireshark.

b. Zgjidh një ndërfaqe për Wireshark për të kapur paketa. Përdorni **Interface List** për të zgjedhur ndërfaqen që është i lidhur me adresat IP dhe MAC të regjistruara të kompjuterit tuaj, në Pjesën 1.

c. Pas zgjedhjes së ndërfaqes së dëshiruar, klikoni Start për të kapur paketat.

d. Hapni një shfletues web dhe shkruani **www.google.com**. Shtypni Enter për të vazhduar.

e. Kliko Stop për të ndaluar kapjen e Wireshark kur shihni faqen kryesore të Google

Krijimi i trafikut ICMP

a. Klikoni butonin Start të Windows dhe hapni programin Wireshark.

b. Zgjidh një ndërfaqe për Wireshark për të kapur paketa. Përdorni **Interface List** për të zgjedhur ndërfaqen që është i lidhur me adresat IP dhe MAC të regjistruara të kompjuterit tuaj, në Pjesën 1.

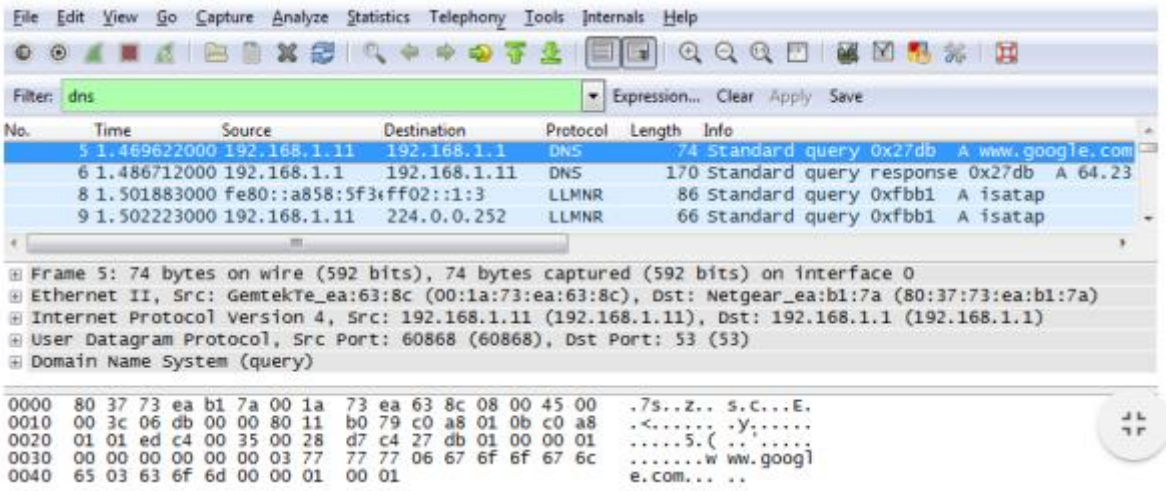
c. Ndersa wireshark është duke identifikuar paketat qe transmetohen ne rrjet, hapni cmd dhe bej ping adresen IP te google 8.8.8.8 dhe kaloni ne wireshark për te pare paketat icmp te krijuara.

Pjesa 3: Shfaq informacionin e pajisjes

Në Pjesën 3, ju do të shqyrtoni paketat UDP që janë krijuar kur komunikojnë me një server DNS për të bere perkthimin e adreses IP qe do te përdoret për www.google.com.

Hapi 1: Filtro paketat DNS.

Shënim: Nëse nuk shihni ndonjë rezultat pas aplikimit të filtrit DNS, mbyllni shfletuesin. Në komandën e dritares së shpejtë, shkruani **ipconfig / flushdns** për të hequr të gjitha rezultatet e mëparshme DNS. Ristartoni Wireshark dhe përsërisni udhëzimet në Pjesën 2b -2e. Nëse kjo nuk e zgjidh çështjen, shtypni **nslookup www.google.com** në cmd si një alternativë për shfletuesin e uebit.



Zgjidhni framen 5 si ne figure për te analizuar. Sa byte data ka frama qe perbehet nga DNS query për ti bere kerkese serverit për adresen IP te www.google.com?

Frama ka : 74 bytes on wire (592 bits)

Ne pjesen e Ethernet II gjeni dhe shkruani MAC adresen burim dhe destinacion qe është përdorur. Nga identifikimi i MAC adresen burim, me ke ju ngjason kjo adrese?

MAC Address →Burim = (f8:9e:94:e6:a7:c1) .
Adresa Destinacion (c8:3a:35:3f:a3:f0).
Adresa burim ngjason me Physical address te Wireless LAN adapter Wi-Fi.

Ne pjesen Internet Protocol Version 4, gjeni dhe shkruani adresen IP burim dhe destinacion si dhe informacionet perkatese ne tabelën e meposhtme:

Frame size	**74 bytes (592 bits)**
Source MAC address	**F8:9E:94:E6:A7:C1**
Destination MAC address	**C8:3A:35:3F:A3:F0**
Source IP address	**192.168.1.3**
Destination IP address	**192.168.1.1**
Source port	**57275**
Destination port	**53**

Shpjegoni cila është arsyeja qe janë përdorur këto numra te portave?

Një porte DNS përdoret për komunikim midis një klienti DNS dhe një serveri DNS.
Porta standarde Për DNS është 53.Klienti përdor ketë porte për ti dërguar kërkesë serverit i cili kthen përgjigje
duke përdorur te njëjtën porte. Kjo porte siguron koherence midis databazës DNS dhe serverit.

Analizoni përgjigjen DNS qe kthen serveri. Gjeni paketën e kapur ne wireshark qe përmban informacion mbi përgjigjen DNS qe kthen serveri. Plotësoni përsëri tabelën:

Frame size	**90 bytes (720 bits)**
Source MAC address	**C8:3A:35:3F:A3:F0**
Destination MAC address	**F8:9E:94:E6:A7:C1**
Source IP address	**192.168.1.1**
Destination IP address	**192.168.1.3**
Source port	**53**
Destination port	**57275**

Hapi 2. Filtro paketat ICMP dhe HTTP dhe përsërisni hapat e mësipërme.

ICMP		**HTTP**	
Reply	**Request**	**Reply**	**Request**
174 bytes	**110 bytes**	**238 bytes**	**326 bytes**
C8:3A:35:3F:A3:F0	**F8:9E:94:E6:A7:C1**	**C8:3A:35:3F:A3:F0**	**F8:9E:94:E6:A7:C1**
F8:9E:94:E6:A7:C1	**C8:3A:35:3F:A3:F0**	**F8:9E:94:E6:A7:C1**	**C8:3A:35:3F:A3:F0**
106.205.171.47	**192.168.1.3**	**79.106.40.16**	**192.168.1.3**
192.168.1.3	**106.205.171.47**	**192.168.1.3**	**79.106.40.16**
3	**3**	**80**	**54910**
3	**3**	**54910**	**80**

Ne rastin e paketës ICMP nuk ka numra portash Source dhe Destination.Kjo sepse komunikimi i informacionit te network layer kryhet midis hosts dhe routers,jo midis proceseve te application layer. Në vend të portave ne tabele janë vendosur “Type” dhe “Code” përkatësisht.

Konkluzionet nga grupi i studenteve si me poshte:

Nxorëm konkluzione mbi shtresat e ndryshme dhe komunikimin midis tyre.
Duke përdorur CMD vumë re përdorimin e ipconfig/all per te pare Windows IP configuration
dhe ndërfaqet e ndryshme qe me vone do te përdornim ne Wireshark për te pare paketat te
ndryshme.
Duke bere kërkesa, në rastin tone me linkun www.google.com nxorëm konkluzione mbi
përmasën e frameve, adresat burim destinacion dhe me vone studiuam përgjigjen e kërkesës ne
po te njëjtën mënyre.