Lab 5: DNS & HTTP

ECSE 308 Introduction to Communication Systems and Networks

Chenyi Xu 260948311

Yongru Pan 261001758

Abstract: The lab is divided into three parts. The objective of the first part is to use Wireshark to investigate the Domina Name System(DNS) protocol from the DNS client's standpoint. In the second part of the lab, the focus was to use Wireshark to investigate the UDP structure and protocol properties. Last but not least, the third part concentrate on using Wireshark to collect traces and investigates the different aspects of the HTTP protocol operation.

Introduction

This lab explores the core concepts of Domain Name System (DNS), Datagram Protocol (UDP), and Hypertext Transfer Protocol (HTTP), utilizing tools like nslookup and Wireshark to capture and analyze packet data. By performing a series of queries and analyzing responses, the lab investigates how DNS resolves domain names into IP addresses, the mechanics of UDP as a transport layer protocol for DNS, and the intricacies of HTTP for web communication. Through these exercises, key networking principles such as packet structure, protocol efficiency, and system reliability are examined, providing comprehensive understanding of how these foundational internet protocols interact to deliver seamless user experiences.

Analysis

Part I: Domain Name System (DNS)

Q1: Use nslookup to determine the IP address of www.cbc.ca. What is the IP address of this web server?

The IP address is 184.25.129.124

Q2: Use nslookup to determine the authoritative DNS servers for McGill University.

The authoritative DNS is pirns1.mcgill.ca, with the IP address 132.206.44.21.

Q3: Run nslookup to obtain the IP address of www.wikipedia.org by sending a query to 8.8.4.4 which is the IP address of the google public DNS server.

```
C:\Users\pyrpo>nslookup www.wikipedia.org 8.8.4.4
Server: dns.google
Address: 8.8.4.4

Non-authoritative answer:
Name: dyna.wikimedia.org
Addresses: 2620:0:861:ed1a::1
208.80.154.224

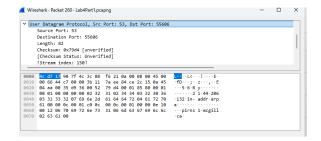
Aliases: www.wikipedia.org

C:\Users\pyrpo>
```

The IPv6 address is 2620:0:861:ed1a::1

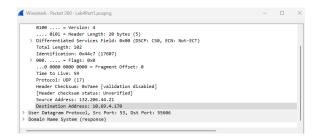
The IPv4 address is 208.80.154.224

Q4: What are the destination port number for the DNS query message and the source port number of the DNS response message?



The destination port number is 55606.

Q5: What is the destination IP address of the DNS query? Is this the IP address of your default local DNS server?



The destination IP address is 10.69.4.170

Q6: Examine the DNS query. What is the "Type" of the DNS query? What does this "Type" mean? What are the other values for this field?

	259 9.715164	10.69.4.170	132.286.44.21	DNS	86 Standard query 0x0001 PTR 21.44.206.132.in-addr.arg
	260 9.716256	132.206.44.21	10.69.4.170	DNS	116 Standard query response 0x0001 PTR 21.44.206.132.ir
	261 9.716808	10.69.4.170	132.286.44.21	DNS	89 Standard query 0x0002 A www.ieee.org.campus.mcgill.
+-	262 9.719133	132.206.44.21	18.69.4.178	DNS	158 Standard query response 0x0002 No such name A www.1
	263 9.719595	10.69.4.170	132.286.44.21	DNS	89 Standard query 0x0003 AAAA www.ieee.org.campus.mcgi
	264 9.720956	132.286.44.21	10.69.4.170	DNS	158 Standard query response 0x8003 No such name AAAA we
	265 9.721178	18.69.4.178	132.206.44.21	DNS	82 Standard query 0x0084 A www.ieee.org.mcgill.ca
	266 9.722966	132.206.44.21	10.69.4.170	DNS	149 Standard query response 0x0004 No such name A www.1
	267 9.723222	10.69.4.170	132.286.44.21	DNS	82 Standard query 0x0005 AAAA www.ieee.org.mcgill.ca
	268 9.724752	132.206.44.21	10.69.4.170	DNS	149 Standard query response 0x0005 No such name AAAA we
	269 9.724982	10.69.4.170	132.206.44.21	DNS	86 Standard query 0x0006 A www.ieee.org.ece.mcgill.ca
	278 9.726628	132.206.44.21	10.69.4.170	DNS	153 Standard query response 0x0006 No such name A www.i
	271 9.726875	10.69.4.170	132.206.44.21	DNS	86 Standard query 0x0007 AAAA www.ieee.org.ece.mcgill.
	272 9.728349	132.206.44.21	10.69.4.170	DNS	153 Standard query response 0x0007 No such name AAAA we
	273 9.728606	10.69.4.170	132.286.44.21	DNS	72 Standard query 0x0008 A www.ieee.org
	274 9.738446	132.206.44.21	10.69.4.170	DNS	178 Standard query response 0x0008 A www.ieee.org CNAME
	275 9,732072	10,69,4,170	132.206.44.21	DNS	72 Standard query 0x0009 AAAA www.ieee.org
	255 0 2555			2005	

The "Type" of the DNS query is A, AAAA, SOA, and CNAME. A signifies the queries for IPv4 address of the host. AAAA signifies the queries for IPv6 address of the host. SOA signifies the query asking for the Start of Authority record. CNAME signifies the query asking for the alias of a domain. Other values include MX, NS, PTR, and TXT.

Q7: Which bit in the "Flags" field indicates that the message is a query or a response?



The QR bit indicates this. If QR = 0, the message is a query. If QR = 1: indicates the message is a response.

Q8: Which field of the response message contains the IP address of www.ieee.org?

In the "Answer" field, you can find the IP address of www.ieee.org.

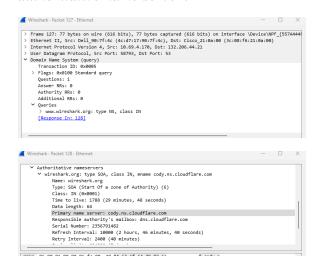
Q9: Provide a screenshot.

. Tou	Some	Jemen	Princip	leaft to
256 K-955620	18,185.6,159	219, 244, 344, 248	186	100 A007 + 150 (and 50
257 5, 436783	18.68.4.170	290,111,4,112	705	56 USGOT = 667 FeOCT SecreSSOD destrates storage turner
250 5.449428	38.89.4.120	55,111,226.9	104	be used? - est (ADE) tears acted wired blood
259 9, 723334	28.49.4.170	202,284,46,25	080	SE Charlest survey States, PTS 21, 50, 200, 112, 51 with saver
269 5, 750255	350:306-44-75	10-00-A-178	285	116 Standard early response 8x860, FTA 21-44-206-153, (n-add-arps FTB pirrol_ergill_co
281 9,75080	38.43.4,326	137, 190, 44, 25	Des	68 Otendard warry 4x8002 A max.inse.org.campat.mcg[1].ca
DAZ 4. YDVCOX	332,396,44,25	36.69.4.176	055	IN Standard query response moment to cust name a man, larguages, org. Largest, org. Li, co with public, company, org. Li, co
DES N. VINNES	18.09, 6:170	113,184,44,21	045	80 Nigraland Warry Science Addition to Language Company organization
254.9.728956-	337,306,44,21	20.49.4,178	046	159 Standard query response 8x800 No such have able less any negotia negitia os SAA prioti, cempo, engitia ce
285-9,721370	28.49.4.229	132,285,44,21	985	62 Standard query dombée à sex.lere.com.explil.com
200. 5, 122500	522,299,44,25	26.49.4.179	589	DOT Disident manny requires Buffort by such neer a way, lear any negatilize not gireat engillize
397. 9. YENZEL	38.69.4, 170	157-786-44-71	585	82 Standard spary Scient Additions, been one explicate
268.9.724752	132,204,44,25	38.69.4.178	045	188 Standard many response 8x895 to such have seen any magilling this simul sugilling
299 9, 124962	28,68,4,270	152,286,44,21	Dtri	TO DESCRIPT SHAPE SHAPE A MANAGEMENT AND ACCURATE AND ACC
270 9.720628	112-204-44-21	28.46.4.276	035	155 Nambrid query response 8:0000 to care name is manifere angles engillina 500 pirent mgillina
275 3-720675	18.49.4,376	252-260-44-25	045	85 Standard garry 0x0007 AAAA inn. Seet org. etc. org. Etc.
272 9,720340	532,200,44,25	10.49.4.178	045	153 Standard guary response 8x8007 to such name AAAA saw, less.org.acc.acgill.cs 500 pirnsh.acgill.cs
279 N. 128686	18.10.1.170	255, 284, 44, 22	DES	72 Standard query models A user, ince., org
276 9.798640	132.204.44.21	26.69.4.176	045	178 Standard query response 6x8000 4 non-term ong COST x2555ghanden claudfront each A 15.225.195.29 2 15.225.195.12 A 15.225.195.60
275 5.752672	38.09.4,370	232-280-44-21	045	12 Spring pary makey Add one jass are
276 8,729725	38.96, 8, 217	239,255,255,250	100	MI 1188 - 1760 Len-108
STY 9. TELEDIS	352,296,48,25	58.49.4.178	590	THE STANDARY MANY CHARGOS BARRIES AND HAS BEEN AND HAS BEEN ARREST AND RESIDENCE AND ADDRESS OF A DAMPE STANDARD AND ADDRESS O
276 5, 754792	28.68.35.56	216, 235, 255, 256	Signiff.	141 N-15900 1 8778/3-3
270 9, 040552	38.67, 15, 500	236,155,255,256	530F	143 H-50405 * HTR/L 1
286 9, 929786	38.05.6.00	25.40.4.205	109	E2 6618 = 1947 (at-48)

Q10: What is the destination IP address of the DNS query? What does this address correspond to?

The destination IP address is "132.206.44.21". This is the DNS server of mcgill.

Q 11: Determine the "Type" of DNS query. What is the authoritative name server of www.wireshark.org. What is the role of an authoritative name server?



The type of the DNS query is NS.

The authoritative nameservers is cody.ns.cloudflare.com

Role of an Authoritative Name Server is to hold the authoritative DNS records for this domain and provides definitive answers to DNS queries related to it.

Q12: Provide a screenshot.

760.	100	Source	LIMETRATION	F1930CBI	segn ans
	119 3,798884	10.65.4.170	132,386,44,21	DNS	86 Standard query 8x8001 P78 21.44.286.133.in-addr.args
	129 3.761862	152,280,44,21	28.09.4.279	DNS	116 Standard query response 0x0001 PTR 21.44.200.132.in-addr.arga PTR pirms1.acgill.ca
	121 3.763020	10.60.4.170	132.206.44.21	DIES	94 Stanfard query 8x8002 NS new wireshark.org.campus.mcgill.ca
	122 3.761753	132.286.44.21	18.49.4.178	DRES	183 Standard query response 8x8002 No such nome NO www.wireshark.org.compus.mcgill.co 50% pdc04.compus.mcgill.co
	123 3.764827	10.69.4.176	132.266.44.21	DRIS	87 Standard query 8x8003 NS www.wireshark.org.ecgili.ca
	124 3.765642	192.286.44.21	28.49.4.179	0865	154 Stanfard query response mammed No such same NS www.wireshark.org.mcgill.ca 506 pirast.mcgill.ca
	125 5,765879	10.49.4.170	132,206,44,21	DNS	Wi Stanfard query 0x0004 NS user, wireshark.org.ecm.ecgill.ca
	126 3.767787	132.286.44.21	18.65.4.178	DNS	158 Standard query response dudded No such same NS seas.wireshark.org.ece.ecgill.ca 50% pirosi.ecgill.ca
	127 3.767967	10.09.4.170	132.286.44.21	DHS	77 Standard query 8x8005 NS www.wireshark.org
	128 3.768459	133,386,66,21	10.69.4.170	1865	153 Standard query response 8x8665 NS wee, wirestork, org 501 cody so.cloudflare.com
	202 0.140689	10.09.4.170	132,286,44,21	DRIS	74 Stardard query Smrf35 A see google.com
	203 6,149219	10.49.4.170	132.266.64.21	DNS	76 Standard query Bolica HTTPS was google.com
	284 6.159272	152,280,44,21	20.09.4.270	DRES	90 Standard query response disc535 A sees google.com A 142,250.09.100
	205 6.150272	132,286,44,21	10.49.4.179	DRIS	89 Standard query response 0x21rs HTTPS www.google.com HTTPS

Q13: What are the destination IP addresses for the two DNS queries? What do these IP addresses correspond to?

It can be seen from the screenshot that the two queries each have the following destination address: 192.168.18.1, which is the local router or DNS server address. The other one is 8.8.8.8, which is Google's public DNS server address.

Q 14: What IP addresses are returned by these two queries? Do they return the same IP addresses for www.google.com? Explain your answer.

```
### CBM Vine Co. Colore Analysis Studies Mandrey Wines No. 191

### CBM Vine Co. Colore Analysis Studies Mandrey Wines No. 191

### CBM Vine Co. Colore Analysis Studies Mandrey Wines No. 191

### CBM Vine Co. Colore Analysis Studies Mandrey Wines No. 191

### CBM Vine Co. Colore Analysis Studies Mandrey Wines No. 191

### CBM Vine Co. Colore Analysis Studies Mandrey Wines No. 191

### CBM Vine Co. Colore Analysis Studies Mandrey Wines No. 191

### CBM Vine Co. Colore Analysis Studies Mandrey Wines No. 191

### CBM Vine Co. Colore Analysis Studies Mandrey Wines No. 191

### CBM Vine Co. Colore Analysis Studies Mandrey Wines No. 191

### CBM Vine Co. Colore Analysis Studies Mandrey Wines No. 191

### CBM Vine Co. Colore Analysis Studies Mandrey Wines No. 191

### CBM Vine Co. Colore Analysis Studies Mandrey Wines No. 191

### CBM Vine Co. Colore Analysis Studies Mandrey Wines No. 191

### CBM Vine Co. Colore Analysis Studies Mandrey Wines No. 191

### CBM Vine Co. Colore Analysis Studies Mandrey Wines No. 191

### CBM Vine Co. Colore Analysis Studies Mandrey Wines No. 191

### CBM Vine Co. Colore Analysis Studies Mandrey Wines No. 191

### CBM Vine Co. Colore Analysis Studies Mandrey Wines No. 191

### CBM Vine Co. Colore Analysis Studies Mandrey Wines No. 191

### CBM Vine Co. Colore Analysis Studies Mandrey Wines No. 191

### CBM Vine Co. Colore Analysis Studies Mandrey Wines No. 191

### CBM Vine Co. Colore Analysis Studies Mandrey Wines No. 191

### CBM Vine Co. Colore Analysis Studies Mandrey Wines No. 191

### CBM Vine Co. Colore Analysis Studies Mandrey Wines No. 191

### CBM Vine Co. Colore Analysis Studies Mandrey Wines No. 191

### CBM Vine Colore Analysis Studies Mandrey Wines No. 191

### CBM Vine Colore Analysis Studies Mandrey Wines No. 191

### CBM Vine Colore Analysis Studies Mandrey Wines No. 191

### CBM Vine Colore Analysis Studies Mandrey Wines No. 191

### CBM Vine Colore Analysis Studies Mandrey Wines No. 191

### CBM Vine Colore Analysis Studies Mandrey Wines No. 191

### CBM Vine Colore An
```

I have chosen packet 97 and packet 210 because packet 97's source is 192.168.18.1 and packet 210's source is 8.8.8.8, and they end up having the same IP address for www.google.com. The reason behind this can be that they both access the same cached record, or that they have received the same response from Google's authoritative DNS.

Q15: Provide a screen shot.

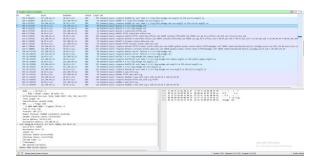
Part II: User Datagram Protocol (UDP)

Ip address = 10.69.4.112

Q16: What transport layer protocol is used to transfer the DNS query and the response message?

UDP

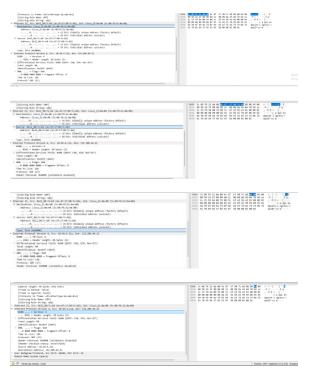
Q17: To set up the connection, how many UDP datagrams are exchanged between your computer and the server? Explain your answer.



61 UDP datagrams are exchanged between the computer and the server. A filter is used to filter out all the DNS. According to Wireshark, 61 UDP datagrams are exchanged.

Q18: Select the first DNS packet in your trace. From this packet, determine the header fields of UDP.

Destination, Source, Types, Version and header length, Differentiated Service Fields, Total length, Identification, Flags, Fragment offset, Time to live, Protocol, Header Checksum, Source address, Destination address, Source port, destination port, length, checksum, UDP payload



Communication in March 100	(1980年 日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本
2 000; = Tage: 000; = Tage: 000; Time to time: 330 Time to time: 330 Teach to time: 330 Teach to time: 330	
[Reder checkson status: Newrified] Source Affirms 18.00 4.13 Source Affirms 18.00 4.13 Source Affirms 18.00 4.13 Source Affirms Petroni, Sor Parts 6444, Sat Parts 53 Sounce Source (Source (George) Sounce Source (Source (George))	
Section (Long Co. 10 April 10	
Control	
moint of sections seems [mallerine strandors] [moster decisions stations (new-right) [most products stations (new-right) [most products and most products (new right) [most products (new right) [most integrous Products, (new right station, (new right) [most integrous Products, (new right station, (new right) [most integrous Products, (new right station, (new right) [most integrous Products, (new right) [most integrous products (new right) [most integro	Activate Windows Go to Setting to activate Windows
Control Angelon, 20 April (192 Mill) Limited to appear of Mary Limited to Appear of Mary Limited to Appear of Mary Limited to Appear of Mary Limited to Appear of Mary Limited to Appear of Mary Limited to Appear of Mary Limited to Appear of Mary Limited to Appear of Mary Limited to Appear of Mary Limited to Appear of Mary Limited to Appear of Mary Limited to Appear of Mary Limited to Appear of Mary Limited to Appear of Mary Limited to Appear of Mary Limited to Appear of Mary Limited to Appear of Mary Limited to Appear of Mary	1
(Calaring Mod Strings vols) Stimmer 37, Enr 604,399/2168 (Sec.4512708-72185), Sec. (Sec. 25:64:88 (Sec.46176-25:46:68) Stimmer 37, Enr 604,399/2168 (Sec.4617-25:66:7485), Sec. (Sec. 25:64:68) (Sec.46176-25:46:68) Stimmer Frenched Striptin 4, Sec. (6:64-64.32), Sec. 143.284, 44.32 Sec. 26:65 - 8-8-864 (seq.47); 3 - 85-86.33	
> Infferentiated Services Filds: 6000 (SSCP: CSA, EDIC Not-CCT) COLL Laught. SOURT (SERVICE) (SERVICES SOURCE (SERVICE) (SERVICES SOURCE (SERVICES) (SERVICES SOURCE SOURCE (SERVICES) (SERVICES SOURCE SOURC	<u></u>
Then it is inc. 1887 The first inc. 1887 The firs	
Destination Address: 13, 50-06.0. It Destinates the Company of the	Activate 1 Co to Settin
Capture Length: 765 liptes (752 lids)	1000 左線性及動物化の 野際左端機器体験 でした・ ・4-
Special complete, the basics (Con Mills) From the property format From t	0000 24 ml 52 ml 50
Powered TL, Set DELING FIRST (AND ADDRESS)	
Final Legits 88 DIST (0447) Intertitional Build' (0447) Service Stage Frequent Offset: 8 Time to line: 128 - Frequent Offset: 8	
Protection and (AT) Meader Checkman status NormalTeal [Namader che	
) been Drigges Protocol, for Purit (6005, But Purit S) Demain Seer System (pury)	
Copher Longitz 54 Syrias (732 bits) (Frame its marked folio)	
Section Laught in Agen 100 (200) The control of th	(日本) (日本) (日本) (日本) (日本) (日本) (日本) (日本)
#### = Terrijon: 4 ### Terrijon: 4	
one	_
Nourse Address: 28.68.6.139 Best Latina Address: 100.084.6.28 Bour Managem Frederic, Dirt Avert 10005, Syst Parts: 13 Bour Managem Control, Dirt Avert 10005, Syst Parts: 13 Bourde Managem (System (Marry)) 10006 Managem (System (Marry))	Activate Windows de to Settings to activate
Control country in the Control	2000 20 80 61 20 80 60 41 27 12 90 21 60 80 80 50 60 41 11 11 11 11 11 11 11 11 11 11 11 11
	-
100 100	
Protectic 100 (37) Instale Columbia shifted (waldardine diambie) Instale Columbia shifted (waldardine diambie) Instale didward 18-18-1-13 (1997) Instale didward 18-18-18-19-19 Instale didward 18-18-18-19-19 Instale didward 18-18-18-19-19 Instale didward 18-18-19-19 Instale didward 18-19-19-19 Instale didward 18-19-19-19-19 Instale didward 18-19-19-19-19 Instale didward 18-19-19-19-19-19-19 Instale didward 18-19-19-19-19-19-19-19-19-19-19-19-19-19-	
Data Statigna McCocke, SV. Perts seets, por north sa basels near spirit (eproy) 2 Ten Doc (a) Mr. 1 (b)	Co. to Cellings to a Pedero CRA- displayed is SLPA- forward is 8 PAQ
Capture Length: 94 Sytes (752 Stts)	1000 1c 00 ft 21 dc 00 4c 27 17 90 7c 10 00 00 00 00 00 c 1 c c c c c c
[Frame in Spinred: Filials] [Protection in Frame: other interestype: Spinred; [Coloring Male Hame: (CO)] [Coloring Male Hame: (CO)]	1000 1 cm
(and or simple) in given (700 MHz) (from the quarter (100) (100 MHz) (from the quarter (100 MHz) (from the quar	
Note Lought on House Court (George State Court) And Afficiation House Court (George State Court)	
Production DDF (ET) D	
) ber Detagram Protecti, Src Perz: 6486, Ost Perz: 53 Deseix Seen System (serry)	
Capture Length: 94 Systes (752 Inits)	THE RESIDENCE TO SHARE A STATE OF THE STATE
Control (1987) in Page (1987) in Pag	10 10 10 10 10 10 10 10
** Internet Products* (version 4, Not. 1848-6-132, 2011-181-180-6-25 1008 ** POSICION 4 2011 - Madder Langton 120 Spats (5) Tribal Langton (colorion Flation and (5007-150), 100n met-CCT) Tribal Langton (colorion Flation and (5007-150), 100n met-CCT)	
Identification 0x350 (4647) 200 Figgs the Suggest Office 1 Time to Lines 130 in reggest Office 0 Find to Lines 130 in reggest Office 1 Find to Lines 130 in reggest Office 1	
Index Constitute Selecting (Validation) Index Constitute Selecting (Validation) Index Advances Index (Validation) Index Advances Index (Validation) Index Advances Index (Validation) Index Index (Validation) Index Index (Validation) Index (Va	
	Editoria 2006 - German de GO 2943 - German de B. ANG
Signor Langlin M Syste (712 bits) (Franc La revisel Folia) (Franc La separat Folia)	
Control of the Section 1997 (Control of the Section 1997) (Section	100
Section Couples in James (No. 1996) The couples of	
General State State State (part) State Sta	
Capture Lingth: 94 ligites (750 bits)	■ 1
Context ranges in larges (150 km); (rest in Springer Stage) (rest in	1000 1, 100 6 1 1 1 1 1 1 1 1 1

TOTAL SAMPLE OF THE PROPERTY (SAMP) 3 000	
resources one (LT) mades Chestes demme (wilsotion disable) [Nucleo chestes attents sourceffed] mades describe the (LT) mades above the (LT) The chestes attents (March LT)	Activat



Q19: By consulting the displayed information in Wireshark's packet content field for the first DNS message, determine the length(in bytes) of each of the UDP header fields.

Destination 6 bytes

Source 6 bytes

Types: 2 bytes

IP Version and header length: 1 byte

Differentiated Service Fields: 1 byte

Total length: 2 bytes

Identification: 2 bytes

Fragment offset: 2 byte

Flags: 1 byte

Time to live: 1 byte

Protocol: 1 byte

Header Checksum: 2 bytes

Source address: 4 bytes

Destination adresse: 4 bytes

Source port: 2 bytes

Destination port: 2 bytes

Length: 2 bytes

Checksum: 2 bytes

UDP payload: 52 bytes

Q20: The value in the Length field indicates the length of what? Verify your claim with

your captured UDP packet.

It specifies the size of the entire UDP datagram. The length field here shows a value of 60 bytes. 8 bytes are used for the UDP header(source, destination, length, checksum) and 52 bytes are used for the UDP payload.

Q21: What is the maximum number of bytes that can be included in a UDP payload? (Hint: The answer to this question can be determined by your previous answer).

Since length occupies 2 bytes. The largest possible number is ff ff which is 65535. 8 bytes are used for the header field. So the maximum number of bytes that can be included in a UDP pauload is ff ff -

Q22: What is the largest possible source port number?

Source port occupies 2 bytes. The largest possible source port number would be ff ff

which is 65535

Q23: Determine whether a checksum is provided for the first DNS message or not. What is the usage of this field?

Yes, it is provided. It ensures that the data in the UDP header and payload arrives without corruption.

Q24: Determine the destination port number for the DNS query message and the source port number of the DNS response. What is the relationship between the two? Which port number is a well-known port number?

Destination port number: 53

Source port number: 64845

Port 53 is a well-known port number, as it is reserved for the DNS protocol. It is used by DNS servers to listen for incoming queries from clients.

The client initiates the query, using the dynamic source port (64845 in this case) and sends the request to port 53 on the DNS server. The server replies using port 53 as its source port (matching the client's query destination port) and sends the response to the dynamic port (64845) that was originally used as the client's source port.

Q25: List two other well-known port numbers used by UDP

Port 67, Port 123

Q26: Determine the IP address of your local DNS sever (use ipcongif). Is it the same as destination IP address of the DNS query?

Destination address of the DNS query: 132.206.44.21. It is the same as the

destination IP address of the local DNS server.

Q27: Examine the DNS response message. How many answers are provided in this message? What do each of these answers contain?

5 answers are provided in the message. Each of those answers contain Name, Type, Class, Time to live, Data Length, CNAME



Q28: By checking the trace, determine whether UDP is a reliable protocol or not. Explain your answer.

131 1.925388	19.69.4.112	132,286,44,21	DNS	80 Standard query 0x4cfa A t-s2-ring.msedge.net
133 1.954876	10.69.4.112	132,216,44,21	DNS	80 Standard query 0x4cfa A t-s2-ring.msedge.net
156 2.954491	10.69.4.112	132,286,44,21	DNS	80 Standard query 0x4cfa A t-s2-ring.msedge.net
185 3.859757	10.69.4.112	132,286,44,21	DNS	82 Standard query 0x3021 A t-ring-fdv2.msedge.net
186 3.861155	10.69.4.112	132,216,44,21	DNS	
286 4.960263		132.216.44.21		82 Standard query 0x3021 A t-ring-fdv2.msedge.net
	10.69.4.112		DNS	80 Standard query 0x4cfa A t-s2-ring.msedge.net
207 4,960305	10.69.4.112	132.216.44.21	DNS	80 Standard query 0x4cfa A t-s2-ring.msedge.net

The trace demonstrates that UDP is unreliable because it does not guarantee packet delivery or handle retransmissions, as evidenced by the repeated DNS queries. It is the best trying mechanism. The DNS queries was sent repeatedly indicating the transmission failed. Hence not reliable.

Q29: Why does DNS use UDP services?

It uses UDP due to its speed, efficiency, and suitability. It is a connectionless protocol. No need to establish connection which reduces latency, allowing DNS to resolve queries more quickly. UDP has low overhead. It is ideal for DNS, where most queries and responses are small and don't need the reliability mechanism of TCP.

Part III: Hyper-Text Transfer Protocol (HTTP)

Q30. What HTTP request method is used to retrieve the HTML file?

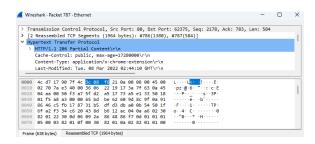
The HTTP request method used to retrieve the HTML file is **GET**.

Q31. What is the URI of the requested file?



The URI is as shown in the screenshot

Q32. What HTTP version is your browser running? What are the other versions of HTTP?



The HTTP version is HTTP/1.1

The other versions of HTTP include HTTP/0.9, HTTP/1.0, HTTP/1.1, HTTP/2, and HTTP/3.

Q33. What languages does your browser accept for response?



These are the accepted languages.

Q 34. What is the IP address of your computer?

The IP of my computer is 10.69.4.170

Q35. What is the server's IP address?

The IP address of the server is 34.223.124.45

36. What is the relationship between source and destination IP addresses of the first GET and the source and destination IP addresses of the first Response?

The first GET's source and destination IP addresses is the first response's destination and source IP addresses.

37. What is the status code of the first response message? What does this code indicate? What code is returned if the requested file cannot be found on the server?

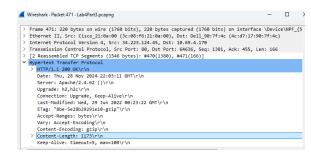
The status code is 200. It indicates that the request is successful, and that the content has delivered. If the requested file cannot be found the code will be 404.

38. When was the last time that the received HTML file was modified at the server?



Last-Modified: Wed, 29 Jun 2022 00:26:43 GMT\r\n

39. What is the size of the content that is returned to your browser?

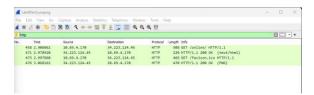


The size is 1173 Bytes.

Q40: How many HTTP GET request messages are sent by your web browser?

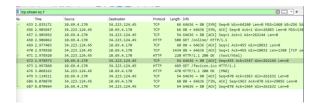
Two GET are sent by my browser.

41. By inspecting the entire trace, determine the number of packets that contain HTTP header. Explain your answer.



Four packets contain the HTTP header because it is being filtered out by http.

Q42. How many TCP segments are transmitted to your computer? Why multiple segments are required to retrieve this single HTML file?



9 TCP segments are transmitted to my computer.

The reason behind needing multiple segments is that the TCP handshake and connection management (e.g., SYN, ACK, FIN packets) and segmentation of HTTP headers and body based on the Maximum Segment Size (MSS).

43. Determine the length of these TCP segments. Do they have the same size? Explain your answer.

The lengths are as follows:

66 bytes for packets 433 and 456

60 bytes for packets 468 and 486

1434 bytes for packets 470

54 bytes for packets 472, 479 and 687

They do not have the same size. The size of the packets depends on the purpose of the packet. If they are control packets, they tend to be small like those with a length of 54, 60, and 66. If they are data packets, they tend to be bigger like the one with the 1434 bytes.

Q44. Which message and what field in that message indicate that the server was able to process the request successfully?

The 200 ok in the status code field tells us that indicates the server was able to process the request successfully.

Q45. What is the status code of the first response message?

200

Q46. What is the value of the content size of the first response message?

File Data: 2238 bytes

Q47. What is the etag of the first response message?

ETag: "7c-5e28b351ffe27"\r\n

Q48. What is the application of etag in conditional HTTP request? Which line in the second response contains the etag value of the first response?

ETags optimize HTTP interactions by enabling conditional requests that validate cached resources, prevent unnecessary updates, and avoid redundant data transfers. This helps improve web performance and ensures data consistency during interactions between the client and server. It is found under Hypertext transfer protocol section.

Q49. Which HTTP Get contains the IF-MODIFIED_SINCE line? What is the usage of this field?



It is used in HTTP GET requests to optimize the retrieval of resources by checking if they have been modified since a specific date and time.

Q50. What is the status code of the second response message? What does this code mean?

200, it is a three digit number that is included in the server's response to a client's request. It indicates the result of the request and provides information about how client should handle the request. 200 represent that the request was successful, and the server is returning the requested resource.

Q51. What is the content length of the second response? Explain.

File Data: 124 bytes

This information does not contain any header. It's the smallest and content only.

Q52. How many HTTP GET Requests are sent by your web browser?

2 request

Q53. What is the content type of each response message?

Text/html, and PNG

Q54. Did your browser download the two images serially or in parallel? Explain. What are the pros and cons of each approach.

There is only 1 image in this web. The browser can download image both serially and in parallel.

Serial:

Pros: Lower resource usage, images downloaded in a predictable order, reduce the risk of overwhelming the network

Cons: Slower total completion time, inefficient use of resources

Parallel:

Pros: faster overall download time, better resource utilization, resilient to slow connections

Cons: higher resource usage, potential server overload, complex error handling, image may not download in the desired order.

Q55. Has the HTTP used persistent or non-persistent connection? Explain your answer.

HTTP use persistent connection. TCP connection reused for multiple requests. It is reflected through source and destination ports on Wireshark.

Q56. What is the requested URL in the frame #101? What HTTP field contains the username and password information? What are the submitted values for the username and password?

Request URI Query contains the information

Request Method: GET

[Full request URI: http://192.168.0.2:8000/lab1Ex5a.html?username=wireshark&password=lab1]

Request URI Query: username=wireshark&password=lab1 Request URI Query Parameter: username=wireshark Request URI Query Parameter: password=lab1 Q57. What HTTP request method is used in the frame #172? What HTTP field contains the username and password information? Explain the difference between this request method and the GET method.

Request Method: POST

| HTML Form URL Encoded: application/x-www-form-urlencoded
| Form item: "username" = "wireshark"
| Form item: "password" = "lab1"

GET fetch data from the server. Data located in URL query string. It is safe. Responses can be cached. Data is visible in URL. Data size is limited by URL length.

POST send data to the server. Data locates in HTTP request body. It is not safe. Responses typically not cached. Data is hidden in request body. There is no practical data size limit.

Q58. What is the status code of the frame #174? What is the description of this code?

501 Not Implemented indicates that the server lacks the ability to perform the requested operation because the required functionality is not implemented.

Conclusion

This lab effectively demonstrated the functionality and interaction of DNS, UDP, and HTTP protocols within network communication. Through hands-on analysis, we observed how DNS resolves domain names to IP addresses, facilitated by UDP for its efficiency and speed. Wireshark packet traces highlighted the headers, fields, and payloads involved in these exchanges, reinforcing the concepts of protocol design and reliability. In the HTTP section, we

explored GET and POST methods, status codes, and resource transfer efficiency. This lab underscored the significance of these protocols in enabling reliable and efficient internet communication while exposing their respective strengths, limitations, and tradeoffs in real-world applications.