

ECSE308 Lab 5

DNS & HTTP

ECSE308

Professor Tho Le-Ngoc

2023-11-15

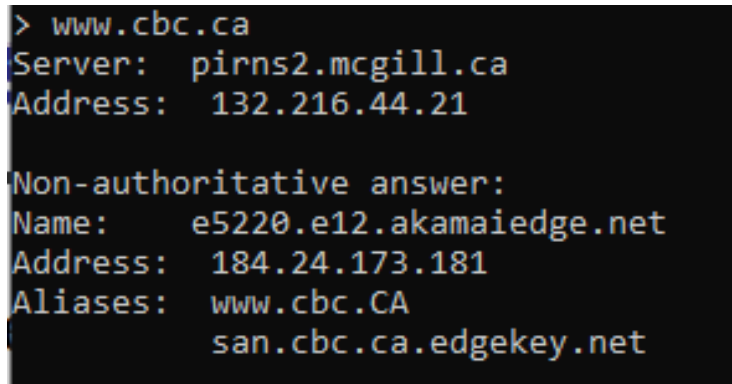
Lab 5: DNS & HTTP

Part 1: Domain Name System

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

Answer: IP address of the www.cbc.ca is 184.24.173.181.

IP address of the web server is 132.216.44.21.



```
> www.cbc.ca
Server:   pirns2.mcgill.ca
Address:  132.216.44.21

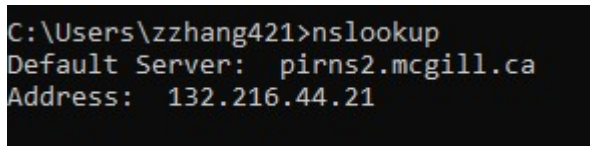
Non-authoritative answer:
Name:     e5220.e12.akamaiedge.net
Address:  184.24.173.181
Aliases:  www.cbc.ca
          san.cbc.ca.edgekey.net
```

Fig. 1. Run nslookup for www.cbc.ca

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

Answer:

We can see that the authoritative DNS server is pirns2.mcgill.ca with address 132.216.44.21.



```
C:\Users\zzhang421>nslookup
Default Server:  pirns2.mcgill.ca
Address:  132.216.44.21
```

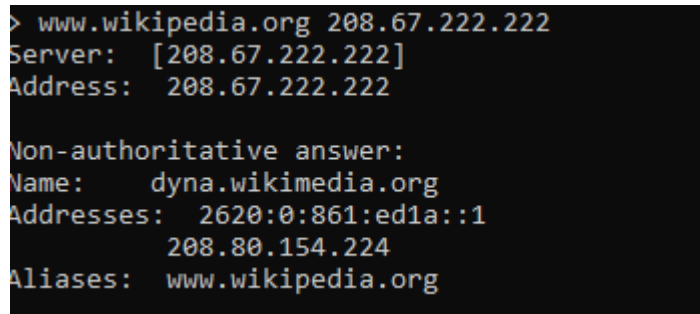
Fig. 2. Run nslookup.

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.

Answer:

We use another open DNS server 208.67.222.222 instead of 8.8.4.4.

We can see the IP address is 208.80.154.224



```
> www.wikipedia.org 208.67.222.222
Server: [208.67.222.222]
Address: 208.67.222.222

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

Fig. 2. Run nslookup to get the address of wikipedia.

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

Answer: Destination port number is 53 for the DNS query message. Source port number is 53 as well for the DNS response message.

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

Answer: Destination IP address of the DNS query is 132.216.44.21. Yes they are the same.

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?

Answer: Type is IPv4(0x0800). It indicates that you're requesting the IPv4 address associated with a domain name. Other values includes Mail eXchange(MX), TXT(Descriptive text) and so on.

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

Answer:

The first bit of “Flags” indicates whether the message is a query and response or not. If the first bit is 0 then it’s a query. If the first bit is 1, then the message is a response.

✓ Flags: 0x0100 Standard query

```

0... .. = Response: Message is a query
.000 0... .. = Opcode: Standard query (0)
.... ..0. .... = Truncated: Message is not truncated
.... ...1 .... = Recursion desired: Do query recursively
.... .... .0.. .... = Z: reserved (0)
.... .... ...0 .... = Non-authenticated data: Unacceptable

```

Fig. 4. Flags field for the query..

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

Answer: We can find the IP address of www.ieee.org in the Address field in the answer section as shown in figure 5. The address is 184.28.130.104.

```

Class: IN (0x0001)
Time to live: 4 (4 seconds)
Data length: 26
CNAME: www.ieee.org.edgekey.net
✓ www.ieee.org.edgekey.net: type CNAME, class IN, cname e1630.c.akamaiedge.net
  Name: www.ieee.org.edgekey.net
  Type: CNAME (Canonical NAME for an alias) (5)
  Class: IN (0x0001)
  Time to live: 18378 (5 hours, 6 minutes, 18 seconds)
  Data length: 24
  CNAME: e1630.c.akamaiedge.net
✓ e1630.c.akamaiedge.net: type A, class IN, addr 184.28.130.104
  Name: e1630.c.akamaiedge.net
  Type: A (Host Address) (1)
  Class: IN (0x0001)
  Time to live: 6 (6 seconds)
  Data length: 4
  Address: 184.28.130.104
[Request In: 746]
[Time: 0.001588000 seconds]
<
0030 00 03 00 00 00 00 03 77 77 77 04 69 65 65 65 03 .....w ww·ieee·
0040 6f 72 67 00 00 01 00 01 c0 0c 00 05 00 01 00 00 org·.....
0050 00 04 00 1a 03 77 77 77 04 69 65 65 65 03 6f 72 .....www ·ieee·or
0060 67 07 65 64 67 65 6b 65 79 03 6e 65 74 00 c0 2a g·edgeke y·net·*
0070 00 05 00 01 00 00 47 ca 00 18 05 65 31 36 33 30 .....G· ...e1630
0080 01 63 0a 61 6b 61 6d 61 69 65 64 67 65 03 6e 65 ·c·akama iedge·ne
0090 74 00 c0 50 00 01 00 01 00 00 00 06 00 04 b8 1c t·P·....
00a0 82 68 ·h

```

Fig. 5. IP address of the www.ieee.org.

Q9. Provide a screenshot.

Answer:

No.	Time	Source	Destination	Protocol	Length	Info
733	10.750865	132.216.44.21	10.69.4.58	DNS	158	Standard query response 0x0002 No such name A www.ietf.org. campus.mcgill.ca SOA pdc05...
734	10.751160	10.69.4.58	132.216.44.21	DNS	89	Standard query 0x0003 AAAA www.ietf.org. campus.mcgill.ca
735	10.752593	132.216.44.21	10.69.4.58	DNS	158	Standard query response 0x0003 No such name AAAA www.ietf.org. campus.mcgill.ca SOA pdc...
736	10.753017	10.69.4.58	132.216.44.21	DNS	82	Standard query 0x0004 A www.ietf.org. mcgill.ca
737	10.755651	132.216.44.21	10.69.4.58	DNS	149	Standard query response 0x0004 No such name A www.ietf.org. mcgill.ca SOA pirs1.mcgill...
738	10.756063	10.69.4.58	132.216.44.21	DNS	82	Standard query 0x0005 AAAA www.ietf.org. mcgill.ca
739	10.757651	132.216.44.21	10.69.4.58	DNS	149	Standard query response 0x0005 No such name AAAA www.ietf.org. mcgill.ca SOA pirs1.mcg...
740	10.757934	10.69.4.58	132.216.44.21	DNS	86	Standard query 0x0006 A www.ietf.org. ece.mcgill.ca
742	10.760927	132.216.44.21	10.69.4.58	DNS	153	Standard query response 0x0006 No such name A www.ietf.org. ece.mcgill.ca SOA pirs1.mc...
743	10.761324	10.69.4.58	132.216.44.21	DNS	86	Standard query 0x0007 AAAA www.ietf.org. ece.mcgill.ca
745	10.762712	132.216.44.21	10.69.4.58	DNS	153	Standard query response 0x0007 No such name AAAA www.ietf.org. ece.mcgill.ca SOA pirs1...
746	10.763110	10.69.4.58	132.216.44.21	DNS	72	Standard query 0x0008 A www.ietf.org
747	10.764698	132.216.44.21	10.69.4.58	DNS	162	Standard query response 0x0008 A www.ietf.org CNAME www.ietf.org.edgekey.net CNAME e16...
748	10.767421	10.69.4.58	132.216.44.21	DNS	72	Standard query 0x0009 AAAA www.ietf.org
749	10.772747	132.216.44.21	10.69.4.58	DNS	221	Standard query response 0x0009 AAAA www.ietf.org CNAME www.ietf.org.edgekey.net CNAME ...
954	14.722254	10.69.4.58	132.216.44.21	DNS	84	Standard query 0x3c03 A metadata.google.internal
955	14.723488	132.216.44.21	10.69.4.58	DNS	159	Standard query response 0x3c03 No such name A metadata.google.internal SOA a.root-serv...
956	14.723868	10.69.4.58	132.216.44.21	DNS	101	Standard query 0x728a A metadata.google.internal. campus.mcgill.ca
957	14.725530	132.216.44.21	10.69.4.58	DNS	170	Standard query response 0x728a No such name A metadata.google.internal. campus.mcgill.c...
958	14.725827	10.69.4.58	132.216.44.21	DNS	94	Standard query 0xe257 A metadata.google.internal. mcgill.ca
959	14.727300	132.216.44.21	10.69.4.58	DNS	157	Standard query response 0xe257 No such name A metadata.google.internal. mcgill.ca SOA p...
960	14.727577	10.69.4.58	132.216.44.21	DNS	98	Standard query 0xc715 A metadata.google.internal. ece.mcgill.ca
961	14.729743	132.216.44.21	10.69.4.58	DNS	165	Standard query response 0xc715 No such name A metadata.google.internal. ece.mcgill.ca S...

Time to Live: 128	0000	3c 08 f6 21 0a 00 a4 bb 6d b9 a8 b3 08 00 45 00	<...!... m...E...
Protocol: UDP (17)	0010	00 3a 2f 69 00 00 80 11 00 00 0a 45 04 3a 84 d8	...:/i... ..E+...
Header Checksum: 0x0000 [validation disabled]	0020	2c 15 ea da 00 35 00 26 bf a3 00 09 01 00 00 01	...5-&.....
[Header checksum status: Unverified]	0030	00 00 00 00 00 00 03 77 77 77 04 69 65 65 65 03w ww.ietf...
Source Address: 10.69.4.58	0040	6f 72 67 00 00 1c 00 01	org.....
Destination Address: 132.216.44.21			
User Datagram Protocol, Src Port: 60122, Dst Port: 53			
Domain Name System (query)			
Transaction ID: 0x0009			

Fig. 6. Screenshot.

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

Answer:

Destination IP address is 132.216.44.21, which corresponds to the DNS server that we are using.

Q11. 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?

Answer:

Type of DNS query is NS, which means name server.

Authoritative name server is cody.ns.cloudflare.com.

The authoritative name server provides the authoritative answers to DNS queries for that domain.

```

C:\Program Files\Microsoft Visual Studio\2022\Community>nslookup -type=NS www.wireshark.org
Server: pirns2.mcgill.ca
Address: 132.216.44.21

www.wireshark.org
primary name server = cody.ns.cloudflare.com
responsible mail addr = dns.cloudflare.com
serial = 2326359863
refresh = 10000 (2 hours 46 mins 40 secs)
retry = 2400 (40 mins)
expire = 604800 (7 days)
default TTL = 1800 (30 mins)

```

Fig. 7.

Q12. Provide a screenshot.

Answer:

No.	Time	Source	Destination	Protocol	Length	Info
270	4.130733	10.69.4.170	132.216.44.21	DNS	98	Standard query 0x0ffa PTR lb._dns-sd._udp.0.4.69.10.in-addr.arpa
271	4.131763	132.216.44.21	10.69.4.170	DNS	181	Standard query response 0x0ffa No such name PTR lb._dns-sd._udp.0.4.69.10.in-addr.arpa SOA
476	6.996738	10.69.4.170	132.216.44.21	DNS	86	Standard query 0x0001 PTR 21.44.216.132.in-addr.arpa
477	6.998429	132.216.44.21	10.69.4.170	DNS	116	Standard query response 0x0001 PTR 21.44.216.132.in-addr.arpa PTR pirns2.mcgill.ca
478	6.999049	10.69.4.170	132.216.44.21	DNS	94	Standard query 0x0002 NS www.wireshark.org.campus.mcgill.ca
479	6.999974	132.216.44.21	10.69.4.170	DNS	163	Standard query response 0x0002 No such name NS www.wireshark.org.campus.mcgill.ca SOA pdc01
480	7.000168	10.69.4.170	132.216.44.21	DNS	87	Standard query 0x0003 NS www.wireshark.org.mcgill.ca
481	7.001206	132.216.44.21	10.69.4.170	DNS	154	Standard query response 0x0003 No such name NS www.wireshark.org.mcgill.ca SOA pirns1.mcgill
482	7.001367	10.69.4.170	132.216.44.21	DNS	91	Standard query 0x0004 NS www.wireshark.org.ece.mcgill.ca
483	7.002570	132.216.44.21	10.69.4.170	DNS	158	Standard query response 0x0004 No such name NS www.wireshark.org.ece.mcgill.ca SOA pirns1.m
484	7.002753	10.69.4.170	132.216.44.21	DNS	77	Standard query 0x0005 NS www.wireshark.org
485	7.004142	132.216.44.21	10.69.4.170	DNS	153	Standard query response 0x0005 NS www.wireshark.org SOA cody.ns.cloudflare.com

Frame 484: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF{...}	0000	3c 08 f6 21 0a 00 a4 bb 6d b9 f3 fe 08 00 45 00	<...>
Ethernet II, Src: Dell_b9:f3:fe (a4:bb:6d:b9:f3:fe), Dst: Cisco_21:0a:00 (3c:08:f6:21:0a:00)	0010	00 3f cf 7f 00 00 80 11 00 00 0a 45 04 aa 84 d8	<...>
Destination: Cisco_21:0a:00 (3c:08:f6:21:0a:00)	0020	2c 15 c8 f4 00 35 00 2b c0 18 00 05 01 00 00 01	<...>
Source: Dell_b9:f3:fe (a4:bb:6d:b9:f3:fe)	0030	00 00 00 00 00 00 03 77 77 77 09 77 69 72 65 73	<...>
Type: IPv4 (0x0800)	0040	68 61 72 6b 03 6f 72 67 00 00 02 00 01	<...>

Internet Protocol Version 4, Src: 10.69.4.170, Dst: 132.216.44.21
User Datagram Protocol, Src Port: 51444, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x0005
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
[Response In: 485]

Fig. 8. Screen shot

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

Answer: Instead of using 8.8.8.8 as the DNS server, we use 208.67.222.222.

The destination IP address for the first DNS query is 132.216.44.21 which is the mcgill DNS server.

The destination IP address for the second DNS query is 208.67.222.222 which corresponds to the open DNS server that we use.

Q14. What IP addresses are returned by these two queries? Do they return the same IP addresses for www.google.com ? Explain your answer.

Answer: In the first query, the returned IP address is 172.217.13.164. In the second query, the returned IP address is 142.251.41.6. They are not the same. The first query uses the default DNS server while the second query uses the open DNS server. The IP address cache maybe different for them.

Q15. Provide a screen shot.

Answer:

No.	Time	Source	Destination	Protocol	Length	Info
3384	37.717089	10.69.4.58	208.67.222.222	DNS	91	Standard query 0x0003 AAAA www.google.com.campus.mcgill.ca
3410	37.751106	208.67.222.222	10.69.4.58	DNS	144	Standard query response 0x0003 No such name AAAA www.google.com.campus.mcgill.ca SOA p...
3411	37.751499	10.69.4.58	208.67.222.222	DNS	84	Standard query 0x0004 A www.google.com.mcgill.ca
3424	37.785595	208.67.222.222	10.69.4.58	DNS	137	Standard query response 0x0004 No such name A www.google.com.mcgill.ca SOA pens1.mcgil...
3425	37.785923	10.69.4.58	208.67.222.222	DNS	84	Standard query 0x0005 AAAA www.google.com.mcgill.ca
3431	37.820018	208.67.222.222	10.69.4.58	DNS	137	Standard query response 0x0005 No such name AAAA www.google.com.mcgill.ca SOA pens1.mc...
3432	37.820962	10.69.4.58	208.67.222.222	DNS	88	Standard query 0x0006 A www.google.com.ece.mcgill.ca
3436	37.854301	208.67.222.222	10.69.4.58	DNS	141	Standard query response 0x0006 No such name A www.google.com.ece.mcgill.ca SOA pens1.m...
3437	37.854716	10.69.4.58	208.67.222.222	DNS	88	Standard query 0x0007 AAAA www.google.com.ece.mcgill.ca
3443	37.899852	208.67.222.222	10.69.4.58	DNS	141	Standard query response 0x0007 No such name AAAA www.google.com.ece.mcgill.ca SOA pens...
3444	37.900807	10.69.4.58	208.67.222.222	DNS	74	Standard query 0x0008 A www.google.com
3445	37.912220	208.67.222.222	10.69.4.58	DNS	90	Standard query response 0x0008 A www.google.com A 142.251.41.36
3446	37.914309	10.69.4.58	208.67.222.222	DNS	74	Standard query 0x0009 AAAA www.google.com
3449	37.955046	208.67.222.222	10.69.4.58	DNS	102	Standard query response 0x0009 AAAA www.google.com AAAA 2607:f8b0:4020:805::2004
3553	39.799998	10.69.4.58	132.216.44.21	DNS	89	Standard query 0x3d49 SOA 156TR4090-06.campus.MCGILL.CA
3554	39.802231	132.216.44.21	10.69.4.58	DNS	151	Standard query response 0x3d49 SOA 156TR4090-06.campus.MCGILL.CA SOA pdc03.campus.MCGI...
3555	39.805079	10.69.4.58	132.216.44.21	DNS	82	Standard query 0xdd3b A pdc03.campus.MCGILL.CA
3556	39.807178	132.216.44.21	10.69.4.58	DNS	104	Standard query response 0xdd3b A pdc03.campus.MCGILL.CA A 132.206.85.21
3557	39.809669	10.69.4.58	132.206.85.21	DNS	157	Dynamic update 0xc91b SOA campus.MCGILL.CA CNAME AAAA A 10.69.4.58
3558	39.811926	132.206.85.21	10.69.4.58	DNS	157	Dynamic update response 0xc91b SOA campus.MCGILL.CA CNAME AAAA A 10.69.4.58

> Queries

Answers

www.google.com: type A, class IN, addr 142.251.41.36

Name: www.google.com

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 227 (3 minutes, 47 seconds)

Data length: 4

Address: 142.251.41.36

[Request In: 3444]

[Time: 0.011413000 seconds]

0000 a4 bb 6d b9 a8 b3 3c 08 f6 21 8a 00 08 00 45 00 ..m...<...|...E-

0010 00 4c 91 fc 40 00 35 11 f6 03 d0 43 de de 0a 45 .L-@5...C...E

0020 04 3a 00 35 ec 41 00 38 cd 1f 00 08 81 80 00 01 :5A8.....

0030 00 01 00 00 00 00 03 77 77 77 06 67 6f 67 6cw ww:googl

0040 65 03 63 6f 6d 00 00 01 00 01 c0 0c 00 01 01 e.com.....

0050 00 00 00 e3 00 04 8e fb 29 24)\$

Fig. 7. Screenshot.

Part 2: User Datagram Protocol (UDP)

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

Answer: UDP protocol is used to transfer the DNS query and the response message.

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

Answer:

There are 4 datagrams exchanged. 1. My computer sends a query to the DNS Resolver. 2. DNS resolver sends a query to an authoritative name server. 3. Authoritative name server responds to DNS resolver. 4. DNS resolver responds to my computer.

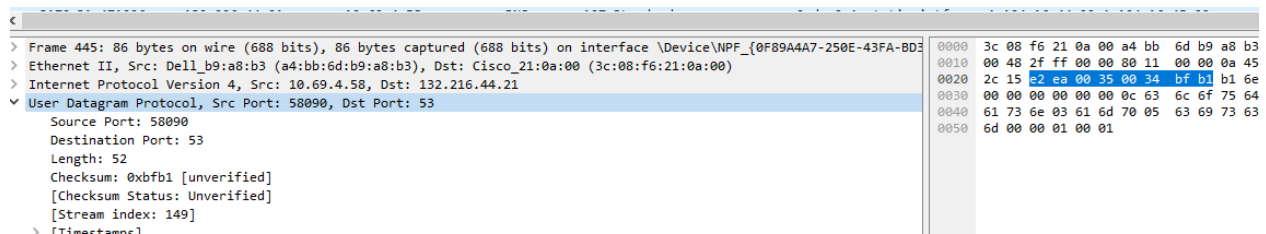
18. Select the first DNS packet in your trace. From this packet, determine the header fields of UDP.

Answer: UDP has source port, destination port,length,and checksum.

19. 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.

Answer:

There are 8 bytes in total for the DNS header. Each of 4 header fields have 2 bytes.



Offset	Hex	ASCII
0000	3c 08 f6 21 0a 00 a4 bb 6d b9 a8 b3	
0010	00 48 2f ff 00 00 80 11 00 00 0a 45	
0020	2c 15 e2 ea 00 35 00 34 bf b1 b1 6e	
0030	00 00 00 00 00 00 0c 63 6c 6f 75 64	
0040	61 73 6e 03 61 6d 70 05 63 6f 73 63	
0050	6d 00 00 01 00 01	

Fig. 8. Header for UDP

20. The value in the Length field indicates the length of what? Verify your claim with your captured UDP packet.

Answer:

The length field specifies the number of bytes in the UDP segment(header and data).

We can verify that the length = UDP payload + 8 in the above screen shot.

21. 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)

Answer: Maximum number of bytes in a UDP payload is $2^{16}-1-8 = 65527$ bytes.

22. What is the largest possible source port number?

Answer: The largest possible source port number is $2^{16}-1 = 65535$.

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

Answer: Yes, the checksum field is not empty. This checksum is calculated at the sender side and helps us in error detection at IP level.

24. 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?

Answer:

Destination port number for the DNS query: 53.

Source port number of the DNS response: 53.

They are the same port number.

Port 53 is a well-known port number.

25. List two other well-known port numbers used by UDP.

Answer: UDP ports 67 and 68.

Dynamic Host Configuration Protocol servers use UDP port 67 to listen for requests while DHCP clients communicate on UDP port 68.

26. Determine the IP address of your local DNS server (use ipconfig). Is it the same as destination IP address of the DNS query?

Answer: The IP address of my local DNS server is 132.206.44.21, which is the same as the destination IP address of the DNS query.

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

Answer:

There are two answers.

Answer contains the name of the host name, type of the address, class, TTL, data length and IP address.

```

  Answers
  www.ietf.org: type A, class IN, addr 104.16.45.99
    Name: www.ietf.org
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 300 (5 minutes)
    Data length: 4
    Address: 104.16.45.99
  www.ietf.org: type A, class IN, addr 104.16.44.99
    Name: www.ietf.org
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 300 (5 minutes)
    Data length: 4
    Address: 104.16.44.99
```

Fig. 9. Answers.

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

Answer:

UDP is a reliable protocol since we didn't see any missing or out-of-order packets in our trace.

29. Why does DNS use UDP services?

Answer: 1. UDP is efficient and lightweight, allowing DNS queries and responses to be transmitted faster.

2. UDP can handle high volume of queries.

Part 3: Hyper-Text Transfer Protocol (HTTP)

Questions:

HTTP GET request/response

Q1: What HTTP request method is used to retrieve the HTML file?

Answer: Request Method: GET

Q2: What is the URI of the requested file?

Answer:

Request URI: /online

[Full request URI: <http://uniquebrightgrandsecret.neverssl.com/online>]

Q3: What HTTP version is your browser running? What are the other versions of HTTP?

Answer:

Request Version: HTTP/1.1

Other versions of HTTP:

- HTTP/0.9
- HTTP/1.0
- HTTP/1.1
- HTTP/2
- HTTP/3

Q4: What languages does your browser accept for response?

Answer: Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6

Q5: What is the IP address of your computer?

Answer: 10.121.66.97

Q6: What is the server's IP address?

Answer: 34.223.124.45

Q7: 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?

Answer:

First Get:

- Source Address: 10.121.66.97
- Destination Address: 34.223.124.45

First Response:

- Source Address: 34.223.124.45
- Destination Address: 10.121.66.97

We noticed that the source IP address and destination IP address of the initial GET request are reversed in the first response

Q8: 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?

Answer:

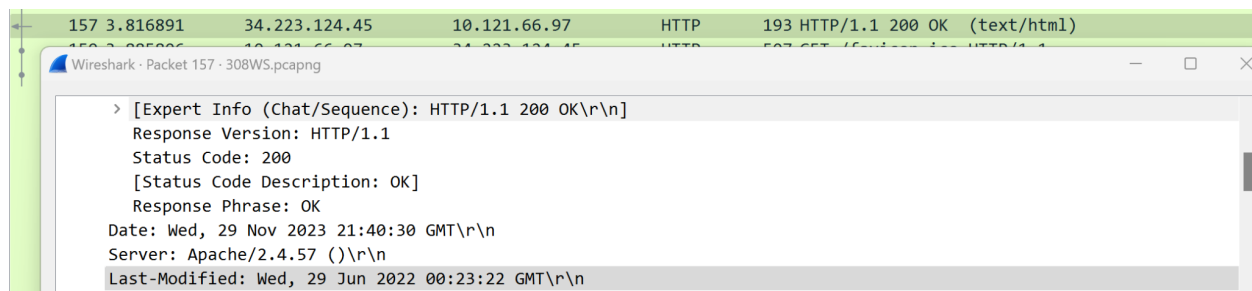
Status Code: 200 [Status Code Description: OK]

It indicates that the request was successfully received, understood, and accepted.

If the server cannot find the requested file, it would return a response with the status code 404.

Q9: When was the last time that the received HTML file was modified at the server?

Answer: Last-Modified: Wed, 29 Jun 2022 00:23:22 GMT



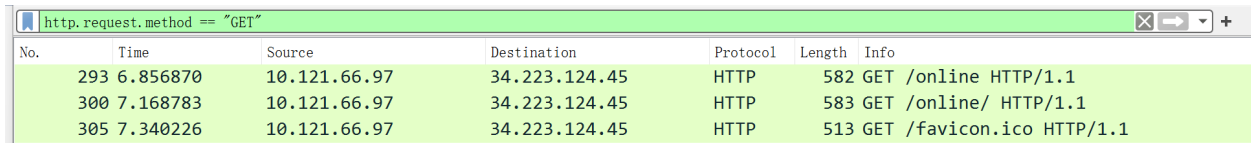
Q10: What is the size of the content that is returned to your browser?

Answer: 1173 byte

Long HTTP response

Q11: How many HTTP GET request messages are sent by your web browser

Answer: There are three request messages sent by my web browser



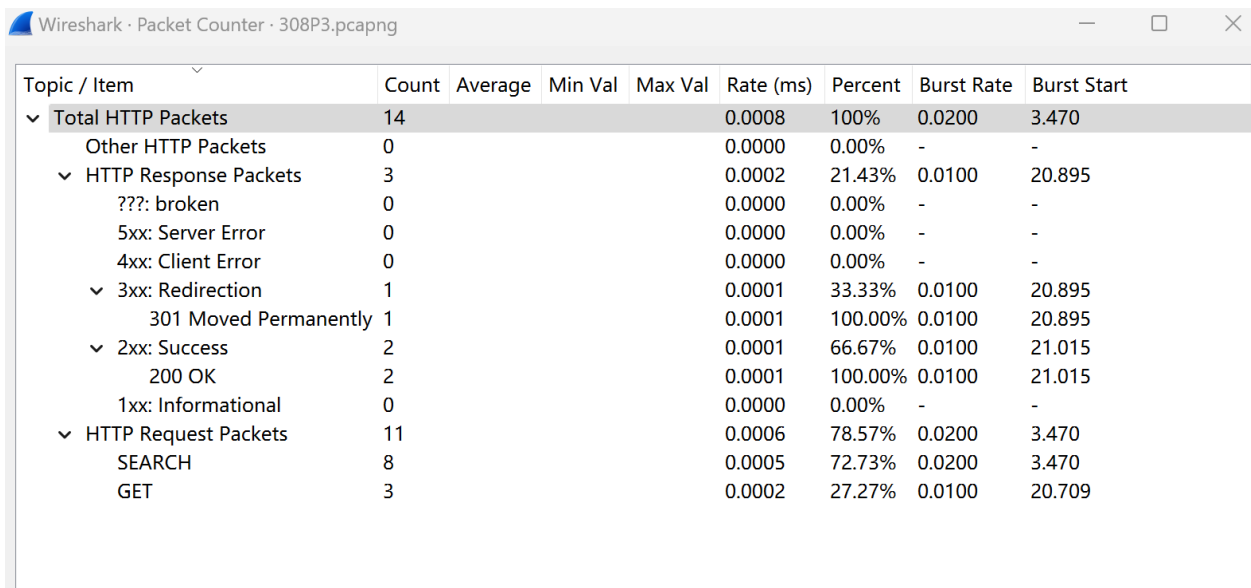
A screenshot of a Wireshark packet capture window. The filter bar at the top shows the filter 'http.request.method == "GET"'. The packet list below shows three packets, all of which are GET requests from 10.121.66.97 to 34.223.124.45. The first packet is 582 bytes, the second is 583 bytes, and the third is 513 bytes.

No.	Time	Source	Destination	Protocol	Length	Info
293	6.856870	10.121.66.97	34.223.124.45	HTTP	582	GET /online HTTP/1.1
300	7.168783	10.121.66.97	34.223.124.45	HTTP	583	GET /online/ HTTP/1.1
305	7.340226	10.121.66.97	34.223.124.45	HTTP	513	GET /favicon.ico HTTP/1.1

Q12: By inspecting the entire trace, determine the number of packets that contain HTTP header. Explain your answer.

Answer:

There are 14 packets that contain the HTTP header.



A screenshot of the Wireshark Packet Counter window for the file 308P3.pcapng. The table shows statistics for various HTTP-related topics. The 'Total HTTP Packets' row is expanded, showing a count of 14. Other rows show counts for different HTTP methods and status codes.

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
✓ Total HTTP Packets	14				0.0008	100%	0.0200	3.470
Other HTTP Packets	0				0.0000	0.00%	-	-
✓ HTTP Response Packets	3				0.0002	21.43%	0.0100	20.895
??? broken	0				0.0000	0.00%	-	-
5xx: Server Error	0				0.0000	0.00%	-	-
4xx: Client Error	0				0.0000	0.00%	-	-
✓ 3xx: Redirection	1				0.0001	33.33%	0.0100	20.895
301 Moved Permanently	1				0.0001	100.00%	0.0100	20.895
✓ 2xx: Success	2				0.0001	66.67%	0.0100	21.015
200 OK	2				0.0001	100.00%	0.0100	21.015
1xx: Informational	0				0.0000	0.00%	-	-
✓ HTTP Request Packets	11				0.0006	78.57%	0.0200	3.470
SEARCH	8				0.0005	72.73%	0.0200	3.470
GET	3				0.0002	27.27%	0.0100	20.709

Q13: How many TCP segments are transmitted to your computer? Why multiple segments are required to retrieve this single HTML file?

Answer:

There are 2 TCP segments transmitted to my computer.

The reason multiple TCP segments are required to retrieve a single HTML file is due to the Transmission Control Protocol (TCP) breaks down data into smaller units called segments for more efficient and reliable transmission.

TCP segment data (139 bytes)

✓ [2 Reassembled TCP Segments (1519 bytes): #827(1380), #828(139)]

[Frame: 827 payload: 0-1370 (1380 bytes)]

Q14: Determine the length of these TCP segments. Do they have the same size? Explain your answer.

Answer:

The length of TCP segments of HTTP responses are 1380 bytes and 139 bytes. Their sizes are different due to the different sizes of data.

Q15: Which message and what field in that message indicate that the server was able to process the request successfully?

Answer:

The 200 OK status code means that the request was successful when the request method is GET. It is in the “Hypertext Transfer Protocol” field.

```
> Internet Protocol Version 4, Src: 34.223.124.45, Dst: 10.121.66.97
> Transmission Control Protocol, Src Port: 80, Dst Port: 58965, Seq: 1842, Ack: 1058, Len: 219
> [2 Reassembled TCP Segments (1519 bytes): #302(1300), #303(219)]
✓ Hypertext Transfer Protocol
  ✓ HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
      Date: Thu, 30 Nov 2023 15:06:00 GMT\r\n
      Server: Apache/2.4.57 ( )\r\n
```

HTTP caching mechanism

Q16: What is the status code of the first response message?

Answer:

Status Code: 200 [Status Code Description: OK]

Q17: What is the value of the content size of the first response message?

Answer: [Content length: 1900]

Q18: What is the etag (identity tag) of the first response message

Answer: ETag: "8be-5e28b29291e10-gzip"

Q19: What is the application of etag in conditional HTTP request? Which line in the second response contains the etag value of the first response?

Answer:

The ETag HTTP response header serves as an identifier for a particular version of a resource, enabling the web server to avoid sending data if the content remains unchanged.

The line with the ETag in the "Not Modified" responses includes the ETag from the first response.

Q20: Which HTTP GET contains the “IF-MODIFIED-SINCE” line? What is the usage of this field

Answer:

The second HTTP GET contains the “IF-MODIFIED-SINCE” line.

If-Modified-Since: Tue, 28 Nov 2023 22:13:24 GMT

It indicates the time when a browser initially fetched a resource from the server, and this information is retained in the cache.

Q21: What is the status code of the second response message? What does this code mean?

Answer: Status code: 304 Not modified.

Q22: What is the content length of the second response? Explain

Answer: For a not modified HTTP response, there's no content length.

Retrieving a web page with embedded objects

Q23: How many HTTP GET requests are sent by your web browser?

Answer: Three

Q24: What is the content type of each response message?

Answer: text/html, PNG,

Q25: Did your browser download the two images serially or in parallel? Explain. What are the pros and cons of each approach?

Answer:

My browser downloaded the two images in parallel. It started the second download task without waiting for the first one to finish

The serial method involves fewer traces and pins, but the transfer rates are lower than parallel method. However, the parallel method needs more pins.

Q26: Has the HTTP used persistent or non-persistent connection? Explain your answer.

Answer:

The HTTP used a persistent connection. The "Connection" header is set to "keep-alive," it indicates a persistent connection

```
> Content-Length: 1173\r\n
  Keep-Alive: timeout=5, max=99\r\n
  Connection: Keep-Alive\r\n
```

HTTP Request Methods:

Q27: 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 the password?

Answer:

Request URI: /lab1Ex5a.html?username=wireshark&password=lab1

Request URI Query parameter fields contain username and password information.

Request URI Query Parameter: username=wireshark

Request URI Query Parameter: password=lab1

Q28: 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.

Answer:

Request Method: POST

HTML form URL encoded fields contains the username and password information

The POST method is more secure than the GET method, since the username and password are included in the URL string of the GET request, while in the POST request, this sensitive information is in the message.

Q29: What is the status code of the frame#174? What is the description of this code?

Answer:

Status Code: 501

[Status Code Description: Not Implemented]