Name: Muhammad Arham Khan
Section: CS421-1
ID: 21701848

Q1:

a) Ten protocols are: MDNS, LLMNR, HTTP, ARP, TCP, UDP, SSDP, DNS, DHCP, TLSv1.2.

b) 0.2183s

c) User Address : GAIA Address = 139.179.206.24 : 128.119.245.12

d)

```
GET /images/qupmember.gif HTTP/1.1\r\n
Host: www.scalable-networks.com\r\n
Connection: keep-alive\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.80 Safari/537.36\r\n
DNT: 1\r\n
Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8\r\n
Referer: http://gaia.cs.umass.edu/\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9,ur-PK;q=0.8,ur;q=0.7,tr;q=0.6\r\n
\r\n
[Full request URI: http://www.scalable-networks.com/images/qupmember.gif]
[HTTP request 1/1]
[Response in frame: 19580]
```

```
GET /favicon.ico HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.80 Safari/537.36\r\n
DNT: 1\r\n
Accept: */*\r\n
Referer: http://gaia.cs.umass.edu/\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9,ur-PK;q=0.8,ur;q=0.7,tr;q=0.6\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/favicon.ico]
[HTTP request 3/3]
[Prev request in frame: 19558]
[Response in frame: 19616]
```

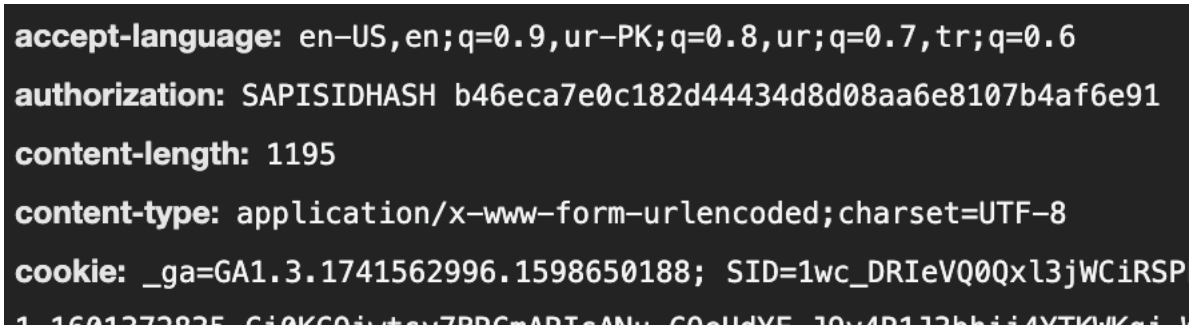
PART 1: HTTP Requests

Q1) Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

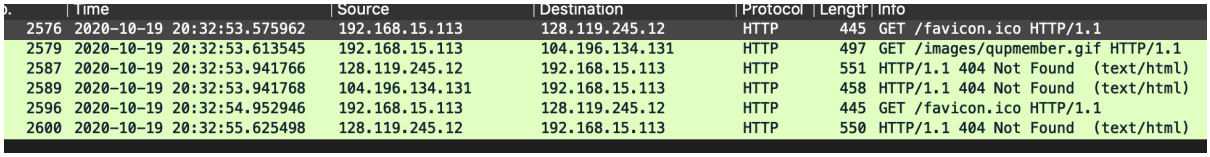
- Yes, my browser and server both are running HTTP 1.1

Q2) What languages (if any) does your browser indicate that it can accept to the server?

- Language = en

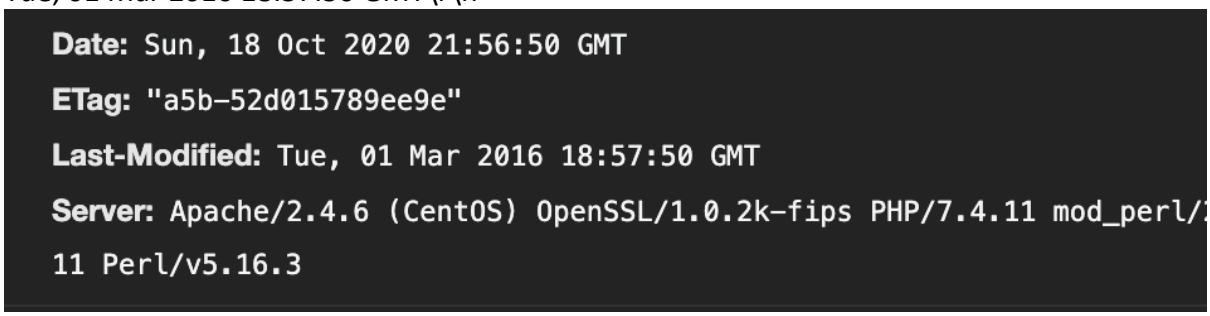
- 

Q3) What is the IP address of your computer? Of the gaia.cs.umass.edu server?

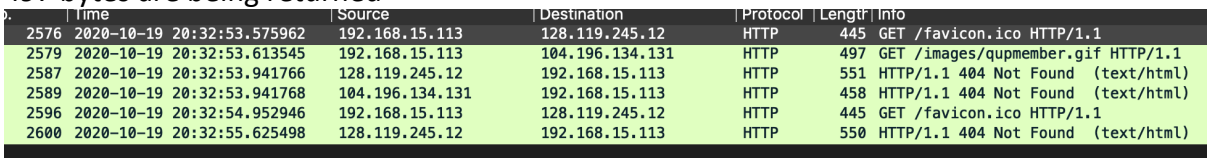
- User Address : 139.179.206.181
- GAIA Address: 128.119.245.12
- 

	Time	Source	Destination	Protocol	Length	Info
2576	2020-10-19 20:32:53.575962	192.168.15.113	128.119.245.12	HTTP	445	GET /favicon.ico HTTP/1.1
2579	2020-10-19 20:32:53.613545	192.168.15.113	104.196.134.131	HTTP	497	GET /images/qupmember.gif HTTP/1.1
2587	2020-10-19 20:32:53.941766	128.119.245.12	192.168.15.113	HTTP	551	HTTP/1.1 404 Not Found (text/html)
2589	2020-10-19 20:32:53.941768	104.196.134.131	192.168.15.113	HTTP	458	HTTP/1.1 404 Not Found (text/html)
2596	2020-10-19 20:32:54.952946	192.168.15.113	128.119.245.12	HTTP	445	GET /favicon.ico HTTP/1.1
2600	2020-10-19 20:32:55.625498	128.119.245.12	192.168.15.113	HTTP	550	HTTP/1.1 404 Not Found (text/html)

Q4) When was the HTML file that you are retrieving last modified at the server?

- Tue, 01 Mar 2016 18:57:50 GMT\r\n
- 

Q5) How many bytes of content are being returned to your browser?

- 497 bytes are being returned
- 

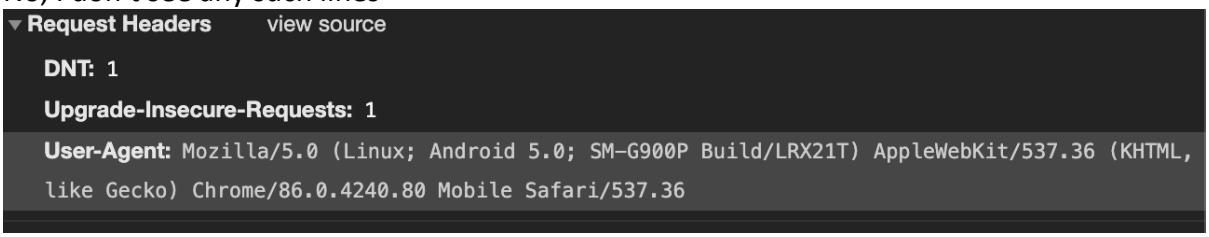
	Time	Source	Destination	Protocol	Length	Info
2576	2020-10-19 20:32:53.575962	192.168.15.113	128.119.245.12	HTTP	445	GET /favicon.ico HTTP/1.1
2579	2020-10-19 20:32:53.613545	192.168.15.113	104.196.134.131	HTTP	497	GET /images/qupmember.gif HTTP/1.1
2587	2020-10-19 20:32:53.941766	128.119.245.12	192.168.15.113	HTTP	551	HTTP/1.1 404 Not Found (text/html)
2589	2020-10-19 20:32:53.941768	104.196.134.131	192.168.15.113	HTTP	458	HTTP/1.1 404 Not Found (text/html)
2596	2020-10-19 20:32:54.952946	192.168.15.113	128.119.245.12	HTTP	445	GET /favicon.ico HTTP/1.1
2600	2020-10-19 20:32:55.625498	128.119.245.12	192.168.15.113	HTTP	550	HTTP/1.1 404 Not Found (text/html)

Q6) By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

- No, I don’t see any such headers
-

Q8) Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

- No, I don't see any such lines



Q9) Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

- It returned a full file in HTTP contents, and the status code was 200, that means the request was accepted

```
<html>
<head>
<title>Computer Network Research Group - UMass Amherst
</title>
</head>
<body bgcolor="#ffffff">
<center>
<p><img
src="cnrg_imap.jpg"
border="0" usemap="#cnrg_imapMAP">
<map name="cnrg_imapMAP">
<area coords="290,177,407,205" shape="rect" href="/networks/resources/index.html">
<area coords="163,178,275,205" shape="rect" href="/networks/education/index.html">
<area coords="62,165,145,191" shape="rect" href="/search.html">
<area coords="6,63,157,90" shape="rect" href="/networks/collaborations.html">
<area coords="64,7,146,34" shape="rect" href="/networks/people.html">
<area coords="163,7,270,33" shape="rect" href="/networks/research.html">
<area coords="288,6,417,33" shape="rect"
href="/networks/publications.html">
</map>
<P>
<BR>
<BR>
```

Q10) Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET? If so, what information follows the "IF-MODIFIED-SINCE:" header?

- If-Modified-Since: Wed, 04 Mar 2020 06:59:02 GMT

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
If-None-Match: "80-5a001f499b1eb"\r\n
If-Modified-Since: Wed, 04 Mar 2020 06:59:02 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
```

Q11) What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

- No, there were no contents returned, and the status code was 304, meaning the file has not been changes

```
Keep-Alive: timeout=5, max=100\r\n
ETag: "80-5a001f499b1eb"\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.190377000 seconds]
[Request in frame: 130]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
```

Q12) How many HTTP GET request messages were sent by your browser?

- Just one request was sent by my browser
-

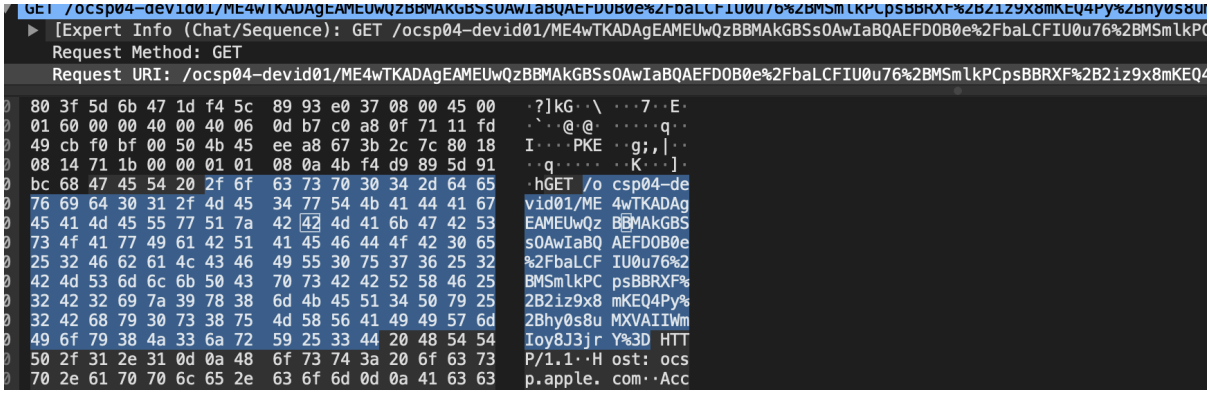
Q13) How many data-containing TCP segments were needed to carry the single HTTP response?

- TCP segments were 4
- [4 Reassembled TCP Segments (4861 bytes): #48(1460), #49(1460), #50(1460), #51(481)]

Q14) What is the status code and phrase associated with the response to the HTTP GET request?

- 200, OK
- 8080 2020-10-19 21:14:21.649568 192.168.15.113 192.168.15.114 HTTP 352 HTTP/1.1 200 OK (PNG)

Q15) Are there any HTTP status lines in the transmitted data associated with a TCP induced "Continuation"?



Q16) How many HTTP GET request messages were sent by your browser? To which Internet addresses were these GET requests sent?

- 3 requests with different addresses but same IPs
- 84 23:47:49.529191 139.179.206.181 128.119.245.12 HTTP 519 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
  86 23:47:49.736871 128.119.245.12 139.179.206.181 HTTP 1127 HTTP/1.1 200 OK (text/html)
  88 23:47:49.846296 139.179.206.181 128.119.245.12 HTTP 451 GET /pearson.png HTTP/1.1
  94 23:47:50.038263 128.119.245.12 139.179.206.181 HTTP 745 HTTP/1.1 200 OK (PNG)
  98 23:47:50.039347 139.179.206.181 128.119.245.12 HTTP 465 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
  176 23:47:50.660409 128.119.245.12 139.179.206.181 HTTP 632 HTTP/1.1 200 OK (JPEG JFIF image)

Q17) Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

- They were downloaded serially because each GET request was made after the response was given for the prior request, seen by the timestamp

Q18) What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

- 401 unauthorized

Q19) When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

- Authorization was added in the second message, it contained the username and password

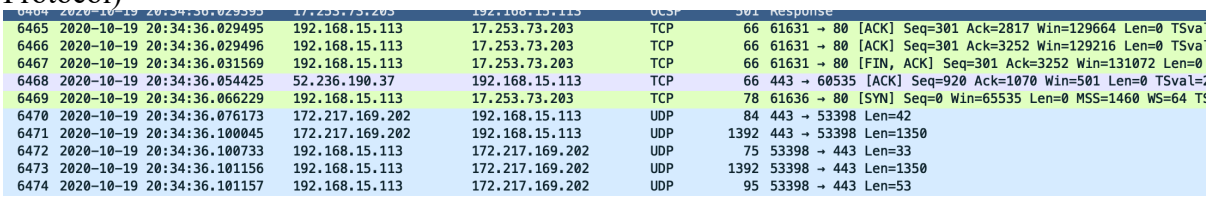
PART 2: NSLOOKUP

1. A web server in asia is: aliexpress.com
2. A web server of university in London is https://www.kingston.ac.uk/
3. firat.bcc.bilkent.edu.tr

`/sbin/ifconfig`

```
mak@arhams-macbook ~ % /sbin/ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
en0: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether f4:5c:89:93:e0:37
        inet6 fe80::b0:9ee:3d4a:a660%en0 prefixlen 64 secured scopeid 0x4
        inet 192.168.15.113 netmask 0xffffff00 broadcast 192.168.15.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
en1: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=460<TSO4,TSO6,CHANNEL_IO>
        ether 82:17:06:80:2e:80
        media: autoselect <full-duplex>
        status: inactive
p2p0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 2304
        options=400<CHANNEL_IO>
        ether 06:5c:89:93:e0:37
        media: autoselect
        status: inactive
en2: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=460<TSO4,TSO6,CHANNEL_IO>
        ether 82:17:06:80:2e:81
        media: autoselect <full-duplex>
        status: inactive
awdl0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1484
        options=400<CHANNEL_IO>
        ether 96:f5:21:71:f7:6c
        inet6 fe80::94f5:21ff:fe71:f76c%awdl0 prefixlen 64 scopeid 0x8
```

Q4) Locate the DNS query and response messages. Are they sent over UDP or TCP?

- It shows DNS on the listing, but in packet information, it shows UDP (User Datagram Protocol)
- 

6465	2020-10-19 20:34:36.029495	192.168.15.113	17.253.73.203	TCP	66	61631 → 80 [ACK] Seq=301 Ack=2817 Win=129664 Len=0 TSva
6466	2020-10-19 20:34:36.029496	192.168.15.113	17.253.73.203	TCP	66	61631 → 80 [ACK] Seq=301 Ack=3252 Win=129216 Len=0 TSva
6467	2020-10-19 20:34:36.031569	192.168.15.113	17.253.73.203	TCP	66	61631 → 80 [FIN, ACK] Seq=301 Ack=3252 Win=131072 Len=0
6468	2020-10-19 20:34:36.054425	52.236.190.37	192.168.15.113	TCP	66	443 → 60535 [ACK] Seq=920 Ack=1070 Win=501 Len=0 TSval=
6469	2020-10-19 20:34:36.066229	192.168.15.113	17.253.73.203	TCP	78	61636 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TS
6470	2020-10-19 20:34:36.076173	172.217.169.202	192.168.15.113	UDP	84	443 → 53398 Len=42
6471	2020-10-19 20:34:36.100045	172.217.169.202	192.168.15.113	UDP	1392	443 → 53398 Len=1350
6472	2020-10-19 20:34:36.100733	192.168.15.113	172.217.169.202	UDP	75	53398 → 443 Len=33
6473	2020-10-19 20:34:36.101156	192.168.15.113	172.217.169.202	UDP	1392	53398 → 443 Len=1350
6474	2020-10-19 20:34:36.101157	192.168.15.113	172.217.169.202	UDP	95	53398 → 443 Len=53

Q5) What is the destination port for the DNS query message? What is the source port of DNS response message?

- Source Port: 62675, Destination Port: 53

Q6) To what IP address is the DNS query message sent? Use *ipconfig* to determine the IP address of your local DNS server. Are these two IP addresses the same?

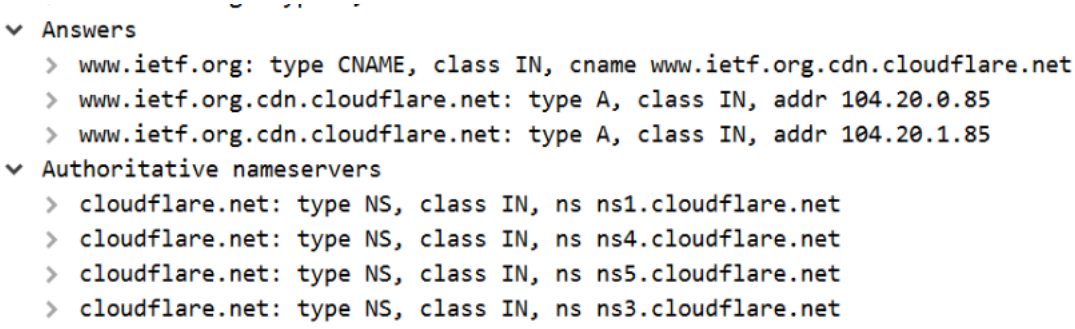
- The IP, DNS query was sent to, and the DNS servers listed in the ipconfig are both the same.

Q7) Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

- The query is Type 'A', The message does not contain any answers.

Q8) Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?

- There are 3 answers in the response message and they contain the address for the Domain Searched for.



Q9) Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

- Yes, the Ip address for the SYN packet is the same as the address in answer by DNS response.