**MARYMOUNT UNIVERSITY**

**Assignment:** IT520; Enterprise Infrastructure and Networks

**FINALS PART 1**

**Assigned:** May 1, 2018

**Instructor:** Dr. Ibrahim Waziri

**Student Name:** George Boakye

Source Host’s IP Address: **192.168.1.7**

**A screenshot of a cell phone

Description generated with very high confidence**

**QUESTIONS**

1. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

**ANSWER:** Browser sent 3 HTTP GET requests. Packet Number 204 contains the GET message for the Bill or Rights.

A screenshot of a social media post

Description generated with very high confidence

1. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

**ANSWER:** Packet Number 210 contains the status code and phrase HTTP/1.1 200 OK (text/html)

A screenshot of a social media post

Description generated with very high confidence

1. What is the status code and phrase in the response?

**ANSWER:** 200 OK

A screenshot of a social media post

Description generated with very high confidence

­­­

1. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

**ANSWER:** There were 4 data containing TCP segments. (i.e. 1460, 1460, 1460, and 481 bytes respectively. Total of 4861 bytes)

A screenshot of a social media post

Description generated with very high confidence

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

**ANSWER:** 401 Unauthorized

A screenshot of a computer

Description generated with very high confidence

1. When your browser sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

**ANSWER:** New field (status code and phrase) is now HTTP/1.1 200 OK (text/html)

A screenshot of a social media post

Description generated with very high confidence

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

**ANSWER:** The DNS queries and responses are sent over UDP protocol

A screenshot of a social media post

Description generated with very high confidence

1. What is the destination port for the DNS query message?

**ANSWER:** DNS query message is on Destination Port 53

A screenshot of a social media post

Description generated with very high confidence

1. What is the source port of DNS response message?

**ANSWER:** DNS response message is on Source Port 53

A screenshot of a computer

Description generated with very high confidence

1. To what IP address is the DNS query message sent?

**ANSWER:** Destination Host’s IP Address: 192.168.1.1

**A screenshot of a computer

Description generated with very high confidence**

1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

**ANSWER:** Type A. Query message doesn’t contain any answers (i.e. “Answers RRs: 0)

A screenshot of a computer

Description generated with very high confidence

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

**ANSWER:** 3 Answers are provided.

**1st Answer:** Name: ietf.org, Type: CNAME, Class: IN (0x0001), TTL: 360, Data Length: 33, CNAME: [www.ietf.org.cdn.cloudfare.net](http://www.ietf.org.cdn.cloudfare.net)

**2nd Answer:** Name: [www.ietf.org.cdn.cloudfare.net](http://www.ietf.org.cdn.cloudfare.net), Type: A (Host Address) (1), Class: IN, TTL: 300, Data Length:4, Address: 104.20.1.85

**3rd Answer:** Name: [www.ietf.org.cdn.cloudfare.net](http://www.ietf.org.cdn.cloudfare.net), Type: A (Host Address) (1), Class: IN, TTL: 300, Data Length:4, Address: 104.20.1.85

A screenshot of a computer

Description generated with very high confidence

1. 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?

**ANSWER:** Yes. IP 172.217.15.106 in the DNS response correspond to Destination of TCP SYN sent by 192.168.1.7 in packet number 56

A screenshot of a computer

Description generated with very high confidence

1. Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header

**ANSWER:** UDP packet number 54 was selected and has 4 fields: Source Port, Destination Port, Length, and Checksum

A screenshot of a social media post

Description generated with very high confidence

1. By consulting the displayed information in Wireshark’s packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.

**ANSWER:** All the fields have 2 bytes each

A screenshot of a social media post

Description generated with very high confidence

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

**ANSWER:** 38 bytes is the value in the length field. It is the 8bytes of the 4 fields, 30bytes encapsulated data

A screenshot of a social media post

Description generated with very high confidence

***Figure 1: Ping Command. Answering questions 17-25***

A screenshot of a computer

Description generated with high confidence

1. Explain what happened in Figure 1. (pay close attention to the command.)

**ANSWER:** Host sent 10 specific request messages to the targeted IP address [176.32.103.205] at periodic intervals and measured the time it took for the 10 response messages to arrive. There was no loss during the transmission.

1. Which protocol is used to carry out the instruction in Figure 1.

**ANSWER:** The ping command above used Internet Control Message Protocol (ICMP)

1. Who owns the IP?

**ANSWER:** IP 176.32.103.205 is owned by Amazon (<https://www.amazon.com/homepage.html/147-0833370-3725660?_encoding=UTF8&opf_redir=1> )

A screenshot of a cell phone

Description generated with very high confidence

1. In addition to a screenshot, in a tabular form, list all the hops between your computer’s IP and the IP address in Figure 1. The table should include the owner, and location of the IP address.

**ANSWER:**

***Fig. 2: Trace Route command***

A screenshot of a cell phone

Description generated with very high confidence

***Table 1: Hops, Owner, & Location***

|  |  |  |  |
| --- | --- | --- | --- |
| **HOP COUNT** | **IP ADDRESS** | **ORGANIZATION (IP OWNER)** | **LOCATION (US STATE/COUNTRY)** |
| **1** | 192.168.1.1 | Internet Assigned Number Authority (IANA) | Los Angeles (CA) |
| **2** | 96.241.173.1 | MCI Communications Services (Verizon Business) | Ashburn (VA) |
| **3** | 100.41.128.16 | MCI Communications Services (Verizon Business) | Ashburn (VA) |
| **4** | 140.222.2.201 | ANS CO+RE Systems, Inc | Purchase (NY) |
| **5** | 152.179.50.58 | ANS Communication, Inc | Ashburn (VA) |
| **6** | 54.239.108.72 | Amazon Technologies Inc. | Seattle (WA) |
| **7** | 54.239.108.93 | Amazon Technologies Inc. | Seattle (WA) |
| **8** | 205.251.245.172 | Amazon.com, Inc. | Seattle (WA) |
| **9** | 176.32.103.205 | Amazon-IAD-PROD | US |

***New IP capture: 10.8.39.3 (Questions 21-25)***

A screenshot of a cell phone

Description generated with very high confidence

1. What version of TLS does the IP above use? Hint: Visit the website of the owners IP address, and capture the “Client Hello” packet.

**ANSWER:** TLS Version 1.2

A screenshot of a cell phone

Description generated with very high confidence

1. List all the algorithms listed in the Cipher Suite of the “Client Hello” packet in 21.

**ANSWER:** AES, ECDHE, RSA, and SHA

A screenshot of a computer

Description generated with very high confidence

1. What TCP port number is used by the “Client Hello” packet, and why is it using that port number?

**ANSWER:** TCP port 443 because it is the default port number used by Hypertext Transfer Protocol Secure (HTTPS).

A screenshot of a computer

Description generated with very high confidence

1. What are the source and destination MAC addresses?

**ANSWER:** Source MAC: 34:02:86:8a:1e:c0. Destination MAC: 00:2c:c8:59:ec:bf

A screenshot of a cell phone

Description generated with very high confidence

1. Identify the company that manufactured the network cards with the MAC address identified in 24 above.

**ANSWER:** Source MAC: 34:02:86:8a:1e:c0 (**Intel Corporate**). Destination MAC: 00:2c:c8:59:ec:bf (**Cisco Systems, Inc**)

MAC Lookup source: <https://macvendors.com/>

A picture containing screenshot

Description generated with very high confidence

A picture containing screenshot

Description generated with very high confidence

**EXTRA CREDIT**

***GitHub account: Create the account at home and add the link***