**CSE5344 Computer Networks**

**Project II– Network Trace Analysis**

**PART 1:**

1. **IP Address:** 129.107.235.88

**Link Local IPv6 Address:** fe80::448a:9a07:793a:45f%12

**Subnet Mask:** 255.255.248.0

**Default Gateway:** 129.107.232.1

1. **MAC Address:** 00-21-5C-77-4B-69
2. The command used to accomplish the above two tasks is: ipconfig /all
3. As IP is Class B, Network Address: 129.107

Taking subnet mask into consideration, Network address = 129.107.232

1. Class B is the class of IP address to which the IP address belongs.
2. IP address is in public domain.

**PART 2:**

**DNS Protocol:**

1. DNS
2. User Datagram Protocol (UDP)
3. **Query packet number:** 30

**Response packet number:** 31

1. **Size of DNS query packet at transport layer:** 41 bytes

**Header length:** 8 bytes

**PDU size:** 33 bytes

1. **Size of DNS response packet at transport layer:** 374 bytes

**Header length:** 8 bytes

**PDU size:** 366 bytes

1. **DNS server IP address:** 129.107.57.180
2. **Source port:** 62533

**Destination port:** 53

1. **Transaction ID:** 0x2a35

**hexadecimal code:** 2a 35

1. **Length:** 2 bytes
2. Transaction ID is 16 bit filed, used for identifying a specific DNS transaction. The DNS client can match responses to its requests using this transaction ID.
3. 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

**Hexadecimal code for flag field:** 0x0100

1. **Questions:** 1
2. **Domain:** maps.google.com

**String representation:** maps.google.com

**Hexadecimal representation:** 04 6d 61 70 73 06 67 6f 6f 67 6c 65 03 63 6f 6d 00

**Field length:** 17 bytes

1. **Query type:** A

**Meaning:** It returns a 32-bit [IPv4](http://en.wikipedia.org/wiki/IPv4) address, which is recorded. It is used to map [hostnames](http://en.wikipedia.org/wiki/Hostname) to an IP address of the host.

**String representation:** Type: A (Host address)

**Hexadecimal representation:** 00 01

**Field length:** 2 bytes

1. Below are the examples of DNS quer y types:

1) Type: A ; RR(decimal) value: 1; Description: Address record: Returns a 32-bit IPv4 address, most commonly used to map hostnames to an IP address of the host.

2) Type: AAAA ; RR(decimal) value: 28; Description: IPv6 Address record: Returns a 128-bit IPv6 address, most commonly used to map hostnames to an IP address of the host.

3) Type: CNAME ; RR(decimal) value: 5; Description: Canonical name record: Alias of one name to another: the DNS lookup will continue by retrying the lookup with the new name.

4) Type: CERT ; RR(decimal) value: 37; Description: Certificate record: Stores PKIX, SPKI, PGP, etc.

5) Type: DHCID ; RR(decimal) value: 49; Description: DHCP identifier: Used in conjunction with the FQDN option to DHCP.

6) Type: LOC ; RR(decimal) value: 29; Description: Location record: Specifies a geographical location associated with a domain name.

1. **Query Class:** IN

**Meaning:** IN refers to the Internet.

**String representation:** Class: IN (0x0001)

**Hexadecimal representation:** 00 01

**Field length:** 2 bytes

1. HS: Refers to the Hesiod class

CH: Refers to the Chaos class.

1. Yes
2. 1... .... .... .... = Response: Message is a response

.000 0... .... .... = Opcode: Standard query (0)

.... .0.. .... .... = Authoritative: Server is not an authority for domain

.... ..0. .... .... = Truncated: Message is not truncated

.... ...1 .... .... = Recursion desired: Do query recursively

.... .... 1... .... = Recursion available: Server can do recursive queries

.... .... .0.. .... = Z: reserved (0)

.... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server

.... .... ...0 .... = Non-authenticated data: Unacceptable

.... .... .... 0000 = Reply code: No error (0)

Hexadecimal code for flag field: 0x8180

1. 12
2. Yes. There are multiple answers to the query because there may be multiple Resource Records with the same labels.
3. Yes. The alias is maps.l.google.com
4. maps.l.google.com: type A, class IN, addr 173.194.46.3

**Name:** maps.l.google.com

**Type:** A (Host address)

**Class:** IN (0x0001)

**Time to live:** 17 seconds

**Data length:** 4

**Addr:** 173.194.46.3(173.194.46.3)

1. The type field in authoritative name servers is “NS” as NS refers to the name server record. Delegates a DNS zone to use the given authoritative name servers.
2. The IP addresses of all the authoritative name servers can be found in the additional records part. The name servers and corresponding IP addresses are as below:

ns1.google.com: 216.239.34.10

ns2.google.com: 216.239.32.10

ns3.google.com: 216.239.36.10

ns4.google.com: 216.239.38.10

**HTTP:**

1. 5.

Filter expression: http.request.method == “GET”

IP Addresses: 173.194.46.3, 74.125.225.231, 74.125.255.231 and 74.125.225.231.

1. 8

Filter expression: http.response

1. **Http Request:** 2133

**Http Response:** 2135

1. HTTP /1.1
2. Files: Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Languages: Accept-Language: en-US, en; q=0.5

Encoding: Accept-Encoding: gzip, deflate

**Character set:** charset=UTF-8

1. **Status code:** 302 Found
2. **Content type:** text/html

charset=UTF-8

Encoding: gzip

1. 663 bytes.
2. **Source port:** 51004

**Destination port:** 80

1. **Source port:** 80

**Destination port:** 51004

**PART 3:**

**HTTP STREAMING:**

1. Filter expression: http.host or http.server
2. 3

Filter expression: http.request.method == “GET”

1. 2 response messages were received.

1 type of response code messages were received.

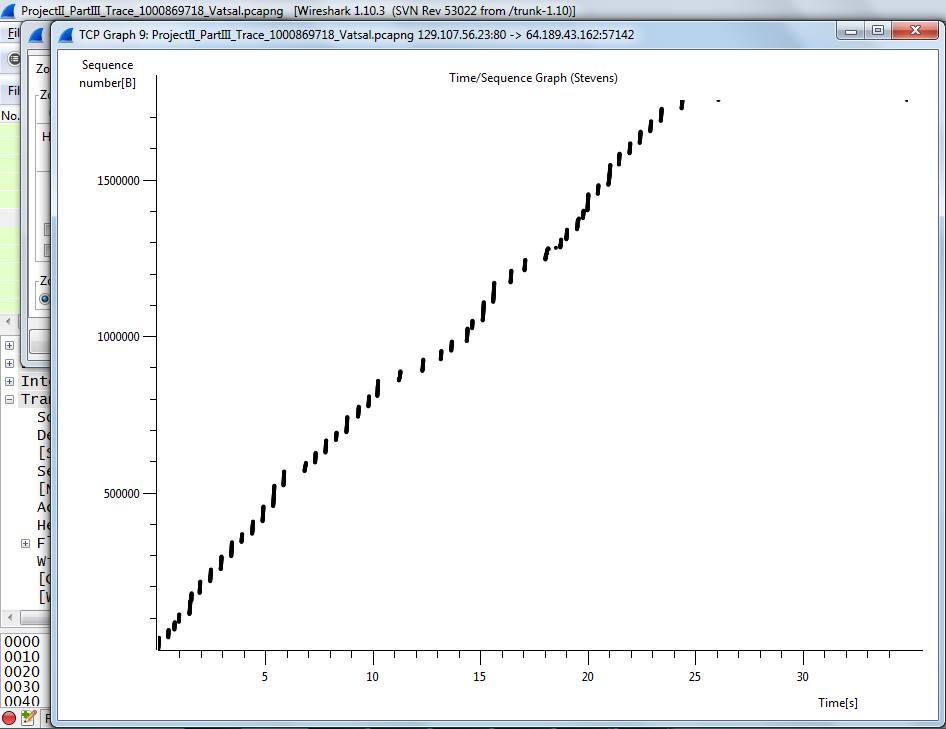
206 Partial Content:The server has fulfilled the partial GET request for the resource.

Filter expression: http.response

1. **Server IP Address:** 129.107.56.23
2. **Web server:** Apache. It can be inferred from the server field in the HTTP GET message.
3. **Content Type:** video/mp4

**TCP Window size:** 56 bytes  
**Window Size Scaling Factor:** 128  
**Window Size after Scaling Once:** 56\*128 bytes = 7168 bytes.  
Window scaling is used to increase the throughput.

1. **Fixed Step Value:** 1380  
   Fixed Step Vale indicates the size of each packet received.
2. Time sequence graph(Stevens)

I do not notice any kind of delay.

1. **Starting Sequence Number:** 0  
   **Ending Sequence Number:** 1752601  
   **Number of Packets Transmitted:** 2523
2. Estimated RTT(n) = (1-a)\*EstimatedRTT(n-1) + a\*SampleRTT(n)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Packet Number** | **Sent Time** | **Time of Receipt of ACK** | **Observed RTT** | **Estimated RTT** |
| 41 | 7.310048 | 7.31005 | 0.0000020 | 0.0000011 |
| 44 | 7.311027 | 7.316072 | 0.0050450 | 0.0006316 |
| 48 | 7.316791 | 7.322012 | 0.0052210 | 0.0012053 |
| 51 | 7.323018 | 7.323997 | 0.0009790 | 0.0011770 |
| 57 | 7.330043 | 7.330045 | 0.0000020 | 0.0010301 |
| 59 | 7.331022 | 7.332163 | 0.0011410 | 0.0010440 |
| 61 | 7.332168 | 7.332171 | 0.0000030 | 0.0009139 |
| 304 | 41.950688 | 41.951953 | 0.0012650 | 0.0009578 |
| 307 | 41.952989 | 41.957716 | 0.0047270 | 0.0014289 |
| 310 | 7.850844 | 7.851508 | 0.0006640 | 0.0025604 |

1. No delay or jitter was detected.
2. TCP is a reliable service and sends acknowledgements & re-transmits the packets if lost. Therefore the TCP service is quite slow.UDP is an unreliable service and is fast. Therefore Video streaming protocols use UDP rather than TCP to achieve higher transfer speeds.