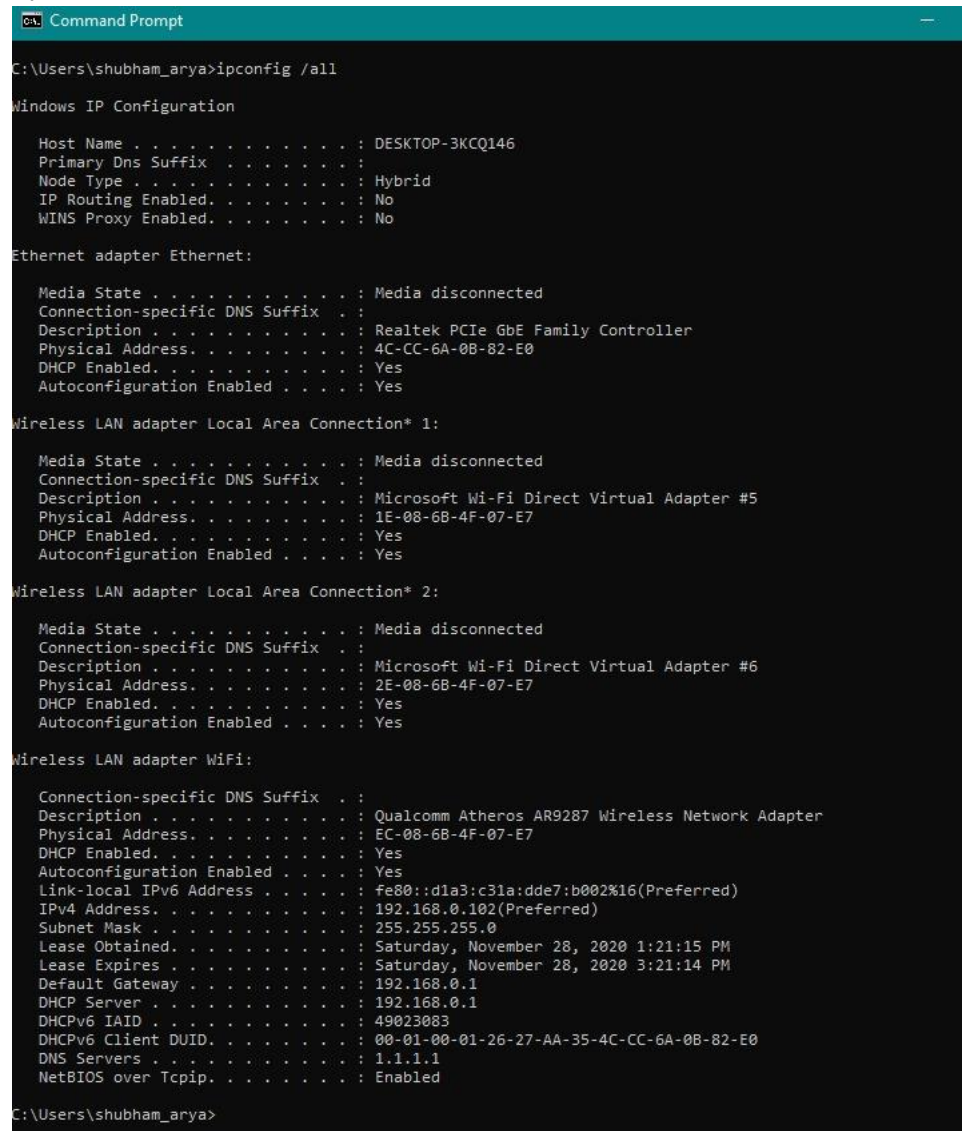


**CSE 4344 Lab 3****1.**

```
Command Prompt
C:\Users\shubham_arya>ipconfig /all

Windows IP Configuration

Host Name . . . . . : DESKTOP-3KCQ146
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Realtek PCIe GbE Family Controller
Physical Address. . . . . : 4C-CC-6A-0B-82-E0
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #5
Physical Address. . . . . : 1E-08-6B-4F-07-E7
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #6
Physical Address. . . . . : 2E-08-6B-4F-07-E7
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter WiFi:

Connection-specific DNS Suffix . :
Description . . . . . : Qualcomm Atheros AR9287 Wireless Network Adapter
Physical Address. . . . . : EC-08-6B-4F-07-E7
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::d1a3:c31a:dde7:b002%16(Preferred)
IPv4 Address. . . . . : 192.168.0.102(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Saturday, November 28, 2020 1:21:15 PM
Lease Expires . . . . . : Saturday, November 28, 2020 3:21:14 PM
Default Gateway . . . . . : 192.168.0.1
DHCP Server . . . . . : 192.168.0.1
DHCPv6 IAID . . . . . : 49023083
DHCPv6 Client DUID. . . . . : 00-01-00-01-26-27-AA-35-4C-CC-6A-0B-82-E0
DNS Servers . . . . . : 1.1.1.1
NetBIOS over Tcpip. . . . . : Enabled

C:\Users\shubham_arya>
```

**What is the IP address of this machine?**

IPv4 address: 192.168.0.102

▪ **How did the machine obtain this IP address?**

IP address are assigned by the DHCP Dynamic Host Configuration Protocol, which is a service running on the network. DHCP typically runs on network hardware such as routers or dedicated DHCP server.

▪ **What is the subnet part of the IP address?**

Subnet mask of the IP address: 255.255.255.0

▪ **What is the MAC address of this machine?**

EC-08-6B-4F-07-E7

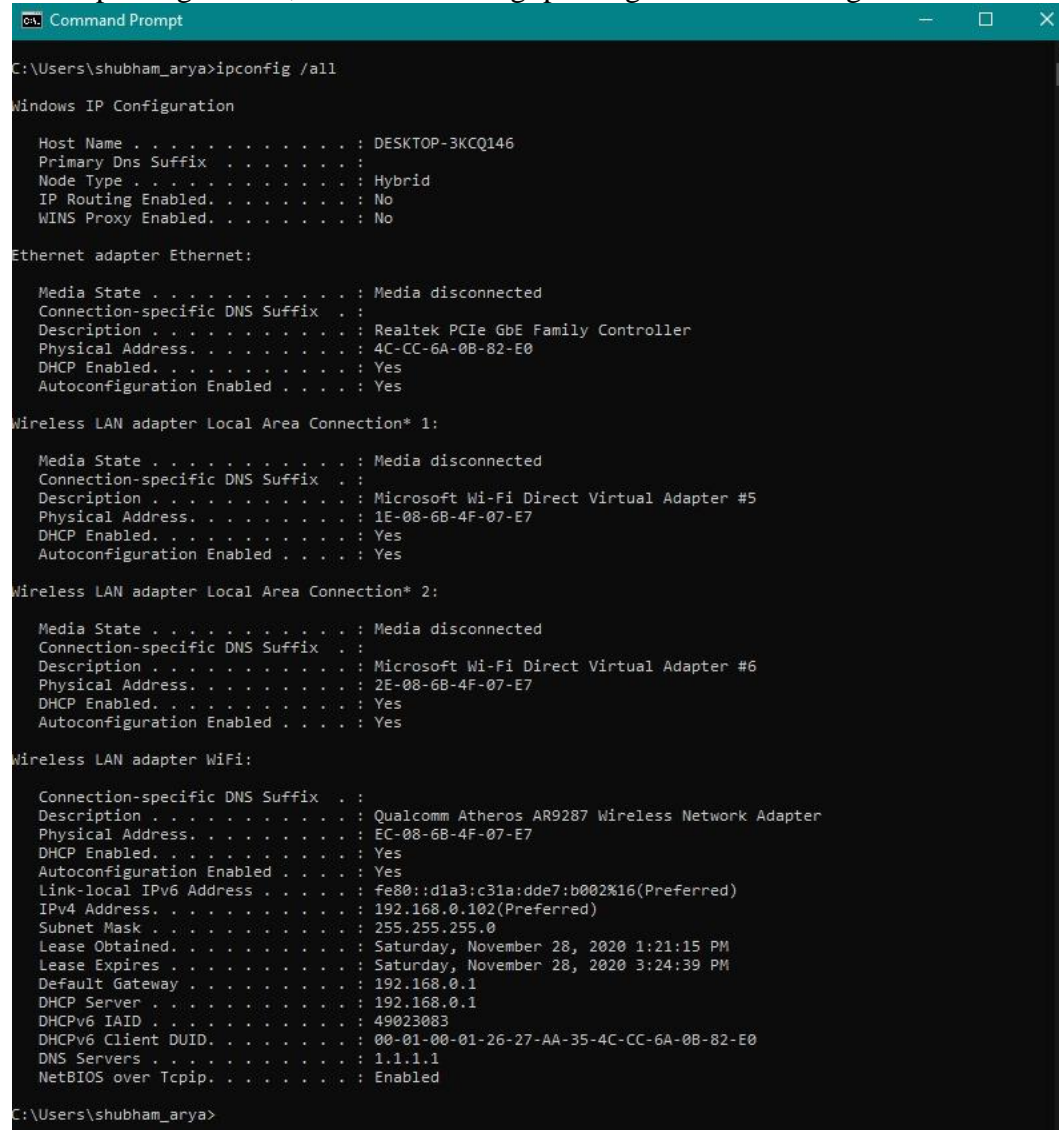
- **How did the NIC card obtain this MAC address?**

NIC card obtains the MAC address during the time of manufacturing. It is hard wired or hard coded on the computer's NIC and is a unique number.

- **What are the DNS servers' addresses?**

1.1.1.1

After ipconfig /renew, and then entering ipconfig /all command again.



```
C:\Users\shubham_arya>ipconfig /all

Windows IP Configuration

Host Name . . . . . : DESKTOP-3KCQ146
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Realtek PCIe GbE Family Controller
Physical Address. . . . . : 4C-CC-6A-0B-82-E0
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #5
Physical Address. . . . . : 1E-08-6B-4F-07-E7
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #6
Physical Address. . . . . : 2E-08-6B-4F-07-E7
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

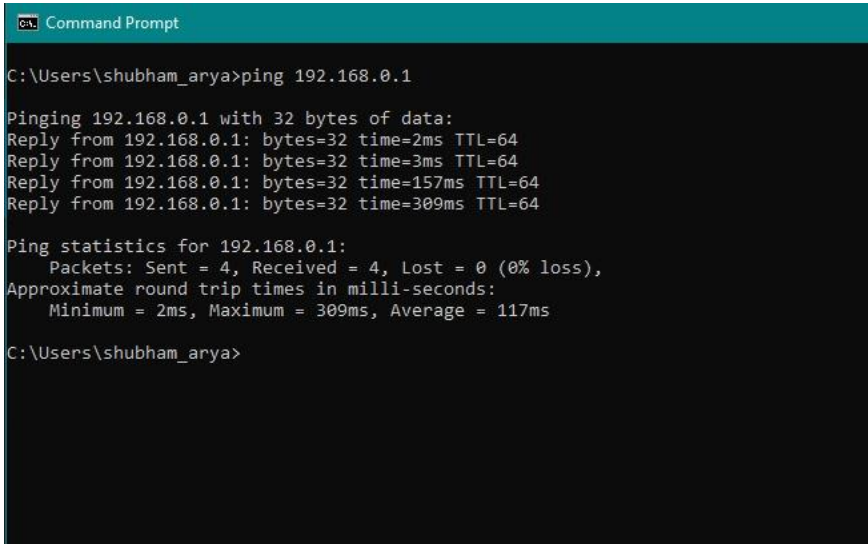
Wireless LAN adapter Wifi:

Connection-specific DNS Suffix . :
Description . . . . . : Qualcomm Atheros AR9287 Wireless Network Adapter
Physical Address. . . . . : EC-08-6B-4F-07-E7
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . : fe80::d1a3:c31a:dde7:b002%16(Preferred)
IPv4 Address. . . . . : 192.168.0.102(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Saturday, November 28, 2020 1:21:15 PM
Lease Expires . . . . . : Saturday, November 28, 2020 3:24:39 PM
Default Gateway . . . . . : 192.168.0.1
DHCP Server . . . . . : 192.168.0.1
DHCPv6 IAID . . . . . : 49023083
DHCPv6 Client DUID. . . . . : 00-01-00-01-26-27-AA-35-4C-CC-6A-0B-82-E0
DNS Servers . . . . . : 1.1.1.1
NetBIOS over Tcpip. . . . . : Enabled

C:\Users\shubham_arya>
```

The only difference is that the lease obtained, and lease expired date has changed. The lease expired has changed from Saturday, November 28, 2020 3:21:14 PM to Saturday, November 28, 2020 3:24:39 PM. The rest of the results are the same.

2.



```
CA Command Prompt
C:\Users\shubham_arya>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=2ms TTL=64
Reply from 192.168.0.1: bytes=32 time=3ms TTL=64
Reply from 192.168.0.1: bytes=32 time=157ms TTL=64
Reply from 192.168.0.1: bytes=32 time=309ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 309ms, Average = 117ms

C:\Users\shubham_arya>
```

The ping command is used to troubleshoot connectivity, reachability, and name resolution. Ping essentially sends an echo packet request to a destination (192.168.0.1 in our case) and then waits for a reply. Ping is only successful if the request is able to get to the destination. Ping uses Internet Control Message Protocol to send the echo message to the specified host. Once ping receives the reply message when packet is reached at the destination, some statistics are provided. Statistics like the number of packets sent, received and lost during transmission are given when the packet reaches back. It also tells the minimum, maximum and average round trip time it takes for the packet to reach the destination and then back to the source. Therefore, ping can check connectivity between hosts and/or servers. Ping uses ICMP to send the message to the destination and reply message is received when the echo message is received back. Ping gives the hosts details about transmission time and success rate for a message to go and come back to the host.

3.

```
Command Prompt

C:\Users\shubham_arya>ping www.utexas.edu

Pinging pantheon-systems.map.fastly.net [151.101.2.133] with 32 bytes of data:
Reply from 151.101.2.133: bytes=32 time=6ms TTL=58
Reply from 151.101.2.133: bytes=32 time=10ms TTL=58
Reply from 151.101.2.133: bytes=32 time=11ms TTL=58
Reply from 151.101.2.133: bytes=32 time=307ms TTL=58

Ping statistics for 151.101.2.133:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 307ms, Average = 83ms

C:\Users\shubham_arya>
```

Since the ping is going to a different destination, the round-trip time and the packets sent, received and lost will be different.

4.

```
Command Prompt

C:\Users\shubham_arya>tracert www.utexas.edu

Tracing route to pantheon-systems.map.fastly.net [151.101.2.133]
over a maximum of 30 hops:

  0  1 ms    1 ms    1 ms   192.168.0.1
  1  4 ms    1 ms    2 ms   192.168.1.1
  2  7 ms    2 ms   11 ms  abts-tn-dynamic-1.64.65.182-airtelbroadband.in [182.65.64.1]
  3  9 ms    4 ms    3 ms   125.17.103.181
  4 13 ms    3 ms    9 ms   182.79.153.43
  5 47 ms   54 ms   53 ms   167.82.128.128
  6  5 ms    5 ms    7 ms   151.101.2.133

Trace complete.

C:\Users\shubham_arya>
```

- a) The first hop in traceroute is usually the default gateway within the network. So, it is a router.
- b) While ping works by checking if a destination is reachable or not, traceroute traces a packet from the source to the destination, showing each hop along the way and the total number of hops taken. Ping also tells us the minimum, maximum and average round trip time whereas traceroute will show the round-trip time for each hop.

5.

```
Command Prompt
C:\Users\shubham_arya>tracert www.hostuk.org

Tracing route to www.hostuk.org [3.10.252.9]
over a maximum of 30 hops:

  1  1 ms    1 ms    1 ms  192.168.0.1
  2  8 ms    1 ms    5 ms  192.168.1.1
  3  4 ms    2 ms    3 ms  abts-tn-dynamic-1.64.65.182-airtelbroadband.in [182.65.64.1]
  4  4 ms    7 ms    4 ms  125.17.103.181
  5 159 ms   159 ms  194 ms 116.119.35.48
  6 163 ms   137 ms 137 ms 99.83.67.148
  7 142 ms   136 ms *     150.222.96.11
  8 265 ms   251 ms 204 ms 52.93.21.115
  9 *       *     *     Request timed out.
10 270 ms   215 ms 196 ms 150.222.241.27
11 204 ms   237 ms 238 ms 52.93.134.144
12 *       *     *     Request timed out.
13 263 ms   180 ms 180 ms 54.239.101.116
14 529 ms   466 ms 181 ms 52.94.35.47
15 236 ms   265 ms 278 ms 52.94.35.46
16 161 ms   158 ms 176 ms 52.94.33.125
17 152 ms   159 ms 162 ms 52.94.33.4
18 *       *     *     Request timed out.
19 *       *     *     Request timed out.
20 *       *     *     Request timed out.
21 *       *     *     Request timed out.
22 *       *     *     Request timed out.
23 *       *     *     Request timed out.
24 166 ms   156 ms 159 ms ec2-3-10-252-9.eu-west-2.compute.amazonaws.com [3.10.252.9]

Trace complete.

C:\Users\shubham_arya>
```

- a) The sudden time increase at one hop is due to the distance between the 2 routers. This suggests that there is increase in time due to undersea fiber or terrestrial link or space link.
- b) The average approximate RTT can be found by using ping. Below is a screenshot of the ping command for [www.hostuk.org](http://www.hostuk.org) as the destination.

```
C:\ Command Prompt
C:\Users\shubham_arya>ping www.hostuk.org

Pinging www.hostuk.org [3.10.252.9] with 32 bytes of data:
Request timed out.
Reply from 3.10.252.9: bytes=32 time=389ms TTL=45
Reply from 3.10.252.9: bytes=32 time=399ms TTL=45
Reply from 3.10.252.9: bytes=32 time=354ms TTL=45

Ping statistics for 3.10.252.9:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 354ms, Maximum = 399ms, Average = 380ms

C:\Users\shubham_arya>
```

From this, the approximate average round trip time is 380ms.

**6.**

The IP address is owned by the organization of University of Texas at Arlington.

This organization has a net range of 129.107.0.0 - 129.107.255.255

Here the first 16 bits are same for this range of IP address so UTA has a subnet mask of 16.

Therefore, we will have  $2^{(32-16)} = 2^{16} = 65536$  addresses. Hence UTA own 65536 addresses.

7.

Request message:

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The top toolbar contains various icons for file operations, capture control, and analysis. The main packet list pane on the left shows a list of captured packets, with packet 1270 (HTTP GET) selected. The packet details pane on the right provides a hierarchical view of the selected packet's structure, showing the status bar (200 OK), the request line (GET / HTTP/1.1), and the request body (empty). The packet bytes pane at the bottom shows the raw data of the packet in hexadecimal and ASCII.



## Response message:

*Wifi						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
http						
No.	Time	Source	Destination	Protocol	Length	Info
1262	20.803252	192.168.0.102	142.250.76.78	HTTP	807	GET / HTTP/1.1
1270	20.855870	142.250.76.78	192.168.0.102	HTTP	582	HTTP/1.1 301 Moved Permanently (text/html)
6265	48.906096	192.168.0.102	8.255.131.254	HTTP	303	GET /d/msdownload/update/others/2020/11/33072483_062ff96989c804766ccd1974dc45a38cc5d3246.cab HTTP/1.1
6274	48.966972	8.255.131.254	192.168.0.102	HTTP	603	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
6276	48.967474	192.168.0.102	8.255.131.254	HTTP	303	GET /d/msdownload/update/others/2020/11/33072482_082e30f101450339f0fd14f3a0c239724433df92.cab HTTP/1.1
6284	49.052850	8.255.131.254	192.168.0.102	HTTP	599	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
6286	49.053417	192.168.0.102	8.255.131.254	HTTP	303	GET /c/msdownload/update/others/2020/11/33072146_af5b2e01e99e42448b0f868090acb99265d7c2294.cab HTTP/1.1
6294	49.135458	8.255.131.254	192.168.0.102	HTTP	699	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
Frame 1270: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits) on interface \DeviceNPF_{AEB3935D-642F-445C-9B4B-9A7EC32CE35E}, id 0						
Ethernet II, Src: Tp-LinkT_29:3e:a1 (7c:8b:ca:29:3e:a1), Dst: Tp-LinkT_4f:07:e7 (ec:08:b0:4f:07:e7)						
Internet Protocol Version 4, Src: 142.250.76.78, Dst: 192.168.0.102						
Transmission Control Protocol, Src Port: 80, Dst Port: 56056, Seq: 1, Ack: 754, Len: 528						
Hypertext Transfer Protocol						
HTTP/1.1 301 Moved Permanently\r\n						
[Expert Info (Chat/Sequence): HTTP/1.1 301 Moved Permanently\r\n]						
[HTTP/1.1 301 Moved Permanently\r\n]						
[Severity level: Chat]						
[Group: Sequence]						
Response Version: HTTP/1.1						
Status Code: 301						
[Status Code Description: Moved Permanently]						
Response Phrase: Moved Permanently						
Location: http://www.google.com/\r\n						
Content-Type: text/html; charset=UTF-8\r\n						
Date: Mon, 30 Nov 2020 05:02:57 GMT\r\n						
Expires: Wed, 30 Dec 2020 05:02:57 GMT\r\n						
Cache-Control: public, max-age=2592000\r\n						
Server: gws\r\n						
Content-Length: 219\r\n						
[Content length: 219]						
X-XSS-Protection: 0\r\n						
X-Frame-Options: SAMEORIGIN\r\n						
\r\n						
[HTTP response 1/1]						
[Time since request: 0.052610000 seconds]						
[Request in frame: 1262]						
[Request URI: http://google.com/]						
File Data: 219 bytes						
Line-based text data: text/html (6 lines)						