

Wireshark Assignment

Dr. Fareed Zaffar

Network Centric Computing

Wireshark

Wireshark is an open-source packet analyzer which is used by professionals all over the world for network troubleshooting, analysis, software and communication protocol development. Wireshark can be used to analyze packets in a live network and can also be used to analyze packets from a packet dump. Wireshark can also be used to make these dump.

The following assignment is fairly simple. So please do the assignment individually.

Any and all plagiarism cases will be forwarded to the disciplinary committee.

Problem 1

Download and install Wireshark. After installation, make sure that there is no network activity on your machine. Turn on Wireshark and follow the instruction below.

- Set Wireshark filter such that it only lists HTTP packets
- Start Live Capture
- Open your browser and go to www.youtube.com
- Stop capturing packets

Answer the following questions

1. Based on the capture, what is your IP address?

10.103.96.36

10.xxx.xx.xx falls within LUMS domain.

2. What is the IP address of www.youtube.com?

216.58.208.78

Belongs to Google Inc.

3. Are there other IP address in the trace besides the aforementioned, if there are why do you think they are in the trace?

119.155.138.17

221.120.207.14

Yes, these IP addresses could belong to the DNS server hosted by local ISP where domain name requests are sent. Also, it could belong to the Ad-servers serving Ads on youtube (Adsense etc). Or perhaps it could belong to an update service of any background application running in my system such as anti-virus.

4. Will the trace show a different IP address for youtube.com if you changed your location?

Yes, probably. Youtube can make an educated guess of my location based on my IP address, cookies, and profile (if I am logged in). Then for various reasons such as serving content faster Google (Youtube) could redirect me to one of its datacenters closer to my location hence it will result in reduced RTT/latency due to reduced physical distance.

5. In the GET request, what are the source and destination physical addresses? Out of the two which one do you think belongs to you?

`http.request.method == "GET"`

Ethernet II,

Src: HewlettP_46:69:11 (a0:b3:cc:46:69:11) –source belongs to my machine. . My machine happens to be HP anyway!

Dst: Cisco_8b:93:69 (00:56:2b:8b:93:69) – destination belongs to the network interface at the server's machine.

6. What are the source and destination hardware addresses in the HTTP response?

Which one belongs to your machine?

Src: Cisco_8b:93:69 (00:56:2b:8b:93:69) – source belongs to the network interface at server since this is a response.

Dst: HewlettP_46:69:11 (a0:b3:cc:46:69:11) – destination belongs to my machine

7. What are the source and destination IP addresses in the http response? Which one belongs to your machine? To which machine/device does the other belong?

Internet Protocol Version 4, Src: 207.55.248.21, Dst: 10.90.0.71

Source: 207.55.248.21

Destination: 10.90.0.71

Destination belongs to me because again this is a response.

Problem 2

The following problem will test your understanding of how the Domain Name System (DNS) works.

Open a command prompt and type the following commands

ipconfig /displaydns

ipconfig /flushdns

For linux machines use the following commands

nsd -i hosts

sudo service dns-clean restart

Perform the following tasks after running the aforementioned commands

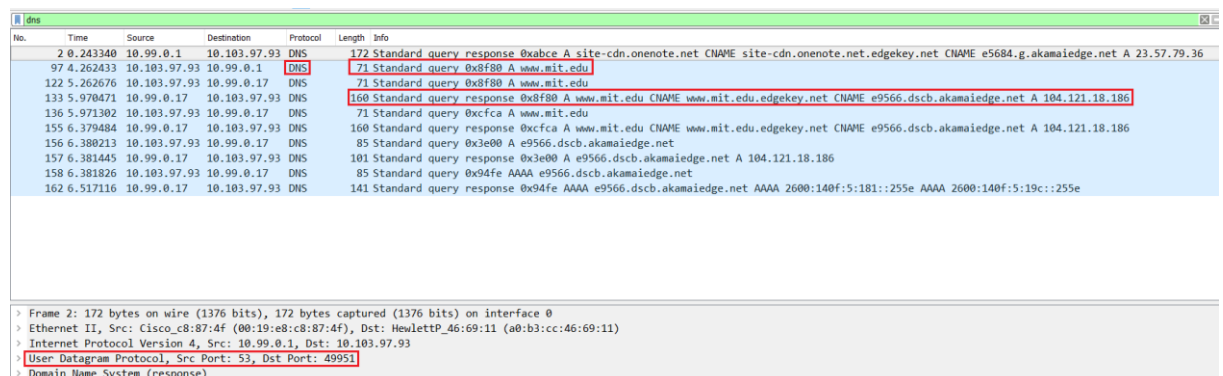
- Set wireshark filter to what seems relevant to you (You have to figure out the correct filters)
- Start live capture
- Visit
- As soon as the page opens, stop the capture

Answer the following questions

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

Explain your answer with an annotated screenshot.

Sent over **UDP** on port 53 which is typical of DNS requests. Sometimes when response data size exceeds 512 bytes – TCP maybe used instead of UDP for DNS queries.



No.	Time	Source	Destination	Protocol	Length	Info
2	0.243340	10.99.0.1	10.103.97.93	DNS	172	Standard query response 0xabce A site-cdn.onenote.net CNAME site-cdn.onenote.net.edgekey.net CNAME e5684.g.akamaiedge.net A 23.57.79.36
97	4.262433	10.103.97.93	10.99.0.1	DNS	71	Standard query 0x8f80 A www.mit.edu
122	5.262676	10.103.97.93	10.99.0.17	DNS	71	Standard query 0x8f80 A www.mit.edu
133	5.970471	10.99.0.17	10.103.97.93	DNS	160	Standard query response 0x8f80 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 104.121.18.186
136	5.971302	10.103.97.93	10.99.0.17	DNS	71	Standard query 0xcfa A www.mit.edu
155	6.379484	10.99.0.17	10.103.97.93	DNS	160	Standard query response 0xcfa A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 104.121.18.186
156	6.380213	10.103.97.93	10.99.0.17	DNS	85	Standard query 0x3e00 A e9566.dscb.akamaiedge.net
157	6.381445	10.99.0.17	10.103.97.93	DNS	101	Standard query response 0x3e00 A e9566.dscb.akamaiedge.net A 104.121.18.186
158	6.381826	10.103.97.93	10.99.0.17	DNS	85	Standard query 0x94fe AAAA e9566.dscb.akamaiedge.net
162	6.517116	10.99.0.17	10.103.97.93	DNS	141	Standard query response 0x94fe AAAA e9566.dscb.akamaiedge.net AAAA 2600:140f:5:181::255e AAAA 2600:140f:5:19c::255e

Frame 2: 172 bytes on wire (1376 bits), 172 bytes captured (1376 bits) on interface 0
Ethernet II, Src: Cisco_c8:87:4f (00:19:e8:c8:87:4f), Dst: HewlettP_46:69:11 (a0:b3:cc:46:69:11)
Internet Protocol Version 4, Src: 10.99.0.1, Dst: 10.103.97.93
User Datagram Protocol, Src Port: 53, Dst Port: 49951
Domain Name System (response)

Figure 1

88	2.013848	10.103.97.93	10.99.0.1	DNS	71	Standard query	0x2f63	A	www.mit.edu
101	3.184836	10.103.97.93	10.99.0.1	DNS	85	Standard query	0x3fb5	A	e9566.dscb.akamaiedge.net
835	6.139768	10.103.97.93	10.99.0.17	DNS	83	Standard query	0x8b10	A	stats.g.doubleclick.net
837	6.142429	10.103.97.93	10.99.0.17	DNS	83	Standard query	0x8fe8	A	stats.l.doubleclick.net
105	3.195802	10.103.97.93	10.99.0.1	DNS	81	Standard query	0x99c7	A	config.edge.skype.com
186	3.994140	10.103.97.93	10.99.0.1	DNS	79	Standard query	0xc1b0	A	clients1.google.com
145	3.702557	10.103.97.93	10.99.0.1	DNS	84	Standard query	0xfbc9	A	www.google-analytics.com
219	4.149976	10.103.97.93	10.99.0.1	DNS	79	Standard query	0xfca3	A	clients1.google.com
125	3.570678	10.99.0.1	10.103.97.93	DNS	183	Standard query response	0x0bb0	A	client-office365-
1	0.000000	10.99.0.1	10.103.97.93	DNS	125	Standard query response	0x0d75	A	ocsp.digicert.com
100	3.184128	10.99.0.1	10.103.97.93	DNS	160	Standard query response	0x0e6f	A	www.mit.edu CNAME
143	3.701685	10.99.0.1	10.103.97.93	DNS	144	Standard query response	0x1239	A	www.google-analyt
833	6.138900	10.99.0.17	10.103.97.93	DNS	169	Standard query response	0x1356	A	stats.g.doublecli
120	3.549459	10.99.0.1	10.103.97.93	DNS	141	Standard query response	0x26c5	AAAA	e9566.dscb.akai

> Frame 88: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
 > Ethernet II, Src: HewlettP_46:69:11 (a0:b3:cc:46:69:11), Dst: Cisco_c8:87:4f (00:19:e8:c8:87:4f)
 > Internet Protocol Version 4, Src: 10.103.97.93, Dst: 10.99.0.1
 > User Datagram Protocol, Src Port: 53566, Dst Port: 53
 > Domain Name System (query)

Figure 2

2. What is the destination port for DNS query message? What is the source port of DNS response message? How did you find them? Attach an annotated snapshot.

Standard Query Destination Port: 53 (Figure 2)

Standard Query Response Source Port: 53 (Figure 1)

Same in both case which should be obvious since response is made by the same port on DNS server to which the query was sent.

3. To what IP address is the DNS query message sent? What is your local DNS server IP? How did you find it? Are these two IP addresses the same? Why? or Why not?

DNS query is sent to IP address: **10.99.0.1**

Local DNS server IP: **10.99.0.1**

Yes, they are the same.

How? ipconfig /all in command prompt.

Why? It could be because this IP belongs to the default DNS server for domain lums.edu.pk. Also, <http://www.mit.edu/> may also exists in this DNS server's cache as it was recently visited by someone else from within LUMS network.

```
Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : lums.edu.pk
Description . . . . . : Realtek PCIe GBE Family Controller
Physical Address. . . . . : A0-B3-CC-46-69-11
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . : Yes
Link-local IPv6 Address . . . . : fe80::2c17:7cba:23d0:e1ca%9(Preferred)
IPv4 Address. . . . . : 10.103.97.93(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Wednesday, March 1, 2017 11:38:17 PM
Lease Expires . . . . . : Thursday, March 9, 2017 11:38:14 PM
Default Gateway . . . . . : 10.103.97.1
DHCP Server . . . . . : 10.99.0.157
DHCPv6 IAID . . . . . : 161526732
DHCPv6 Client DUID. . . . . : 00-01-00-01-1F-F7-B4-2E-A0-B3-CC-46-69-11
DNS Servers . . . . . : 10.99.0.17
                        10.99.0.1
NetBIOS over Tcpip. . . . . : Enabled
```

Problem 3

1. Why do you think DNS is used? Would it not be simpler to just use host names?

It may be simpler but it would not always work. The internet is based on all devices following the same protocol which happens to be TCP/IP protocol. TCP's addressing scheme requires each node to have a unique identifier which cannot be a name "string". It has to be an IP address.

Although let's say we replace all IP addresses with unique domain names.

IP addresses also carry the address of the device's local network. That is a device with IP 192.168.1.100 will be on the same network as a device with IP 192.168.1.200 and there is no need for routing to find that device while a device with IP 200.168.1.200 is on a different network. Hostnames will not have such a feature. They are easier to work with for humans but do not have enough addressing information.

Almost missed where did IP come from when DNS was the question? DNS is basically a system that translates domain names to numerical IP addresses.

Update 2nd March: Just studied IP subnetting in class today. This logical subdivision of an IP network would not be possible with hostnames.

2. Can you capture packets from a machine which is located on the same Local Area Network? Explain.

Yes. That's what Wireshark, tcpdump etc does. It captures most of the packets from all devices going to and from your local area network which could be connected via your router, switch etc. Although not if you are on a wired network in which case any traffic you see is meant for your specific MAC Address. That is one of the reasons why wireless networks are arguably less secure.

3. Can you capture packets from a machine which is not a part of the same Local Area Network? Explain.

Simply speaking, No! Packets can only be captured within the same wireless Local Area Network. However, it might be possible to have remote access to a machine over the internet that captures packets from its Local area network and uploads it into your machine for analysis. But that is virtually the same thing i.e. having remote access to a machine that is part of a different Local Area Network but for that machine it is the "same Local Area Network".