Lab 1: Packet analysis at application layer using Wireshark

SCSR1213 Network Communications

Universiti Teknologi Malaysia

Objective:

1. Understanding of network protocols by observing the sequence of messages exchanged between two protocol entities, delving down into the details of protocol operation, and causing protocols to perform certain actions and then observing these actions and their consequences.

2. To introduce student with Wireshark software tool for packet analyzer.

3. To analyze protocol used in application layer such as http and dns.

Reference material: Computer Networking: A Top-Down Approach, 7th ed., J.F. Kurose and K.W. Ross.

Name : Chua Jia Lin

Metric No : A23CS0069

Section : 12

Name : Cheryl Cheong Kah Voon

Metric No : A23CS0060

Section : 12

Mark

PART A: Wireshark Getting Started

1.0 Introduction

The basic tool for observing the messages exchanged between executing protocol entities is called a **packet sniffer**. As the name suggests, a packet sniffer captures ("sniffs") messages being sent/received from/by your computer; it will also typically store and/or display the contents of the various protocol fields in these captured messages. A packet sniffer itself is passive. It observes messages being sent and received by applications and protocols running on your computer, but never sends packets itself. Similarly, received packets are never explicitly addressed to the packet sniffer. Instead, a packet sniffer receives a *copy* of packets that are sent/received from/by application and protocols executing on your machine.

Figure A.1 shows the structure of a packet sniffer. At the right of Figure 1 are the protocols (in this case, Internet protocols) and applications (such as a web browser or ftp client) that normally run on your computer. The packet sniffer, shown within the dashed rectangle in Figure A.1 is an addition to the usual software in your computer, and consists of two parts. The **packet capture library** receives a copy of every link-layer frame that is sent from or received by your computer. In Figure A.1, the assumed physical media is an Ethernet, and so all upper-layer protocols are eventually encapsulated within an Ethernet frame. Capturing all link-layer frames thus gives you all messages sent/received from/by all protocols and applications executing in your computer.

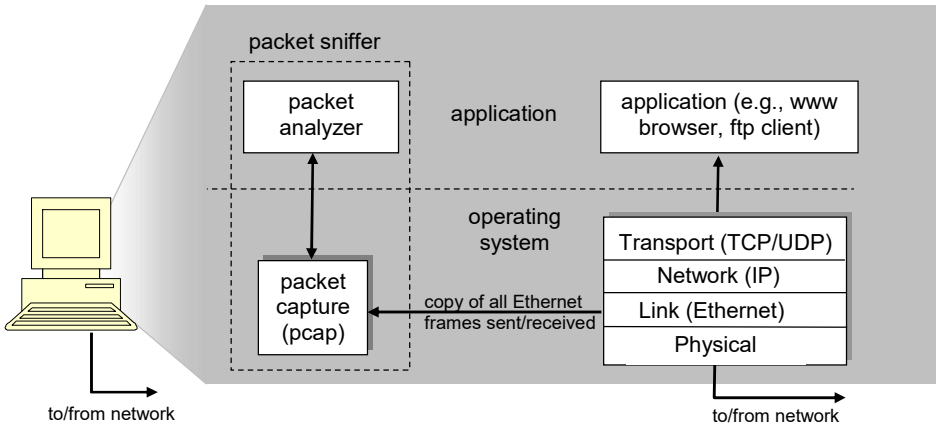


Figure A.1: Packet sniffer structure

The second component of a packet sniffer is the **packet analyzer**, which displays the contents of all fields within a protocol message. In order to do so, the packet analyzer must "understand" the structure of all messages exchanged by protocols. The packet analyzer understands the format of Ethernet frames, and so can identify the IP datagram within an Ethernet frame. It also understands the IP datagram format, so that it can extract the TCP segment within the IP datagram. Finally, it understands the TCP segment structure, so it can extract the HTTP message contained in the TCP segment. Finally, it understands the HTTP protocol and so, for example, knows that the first bytes of an HTTP message will contain the string "GET," "POST," or "HEAD".

2.0 Getting Wireshark Ready

- Download and install the Wireshark software
- Run Wireshark. Wireshark startup screen shown in Figure A.2.

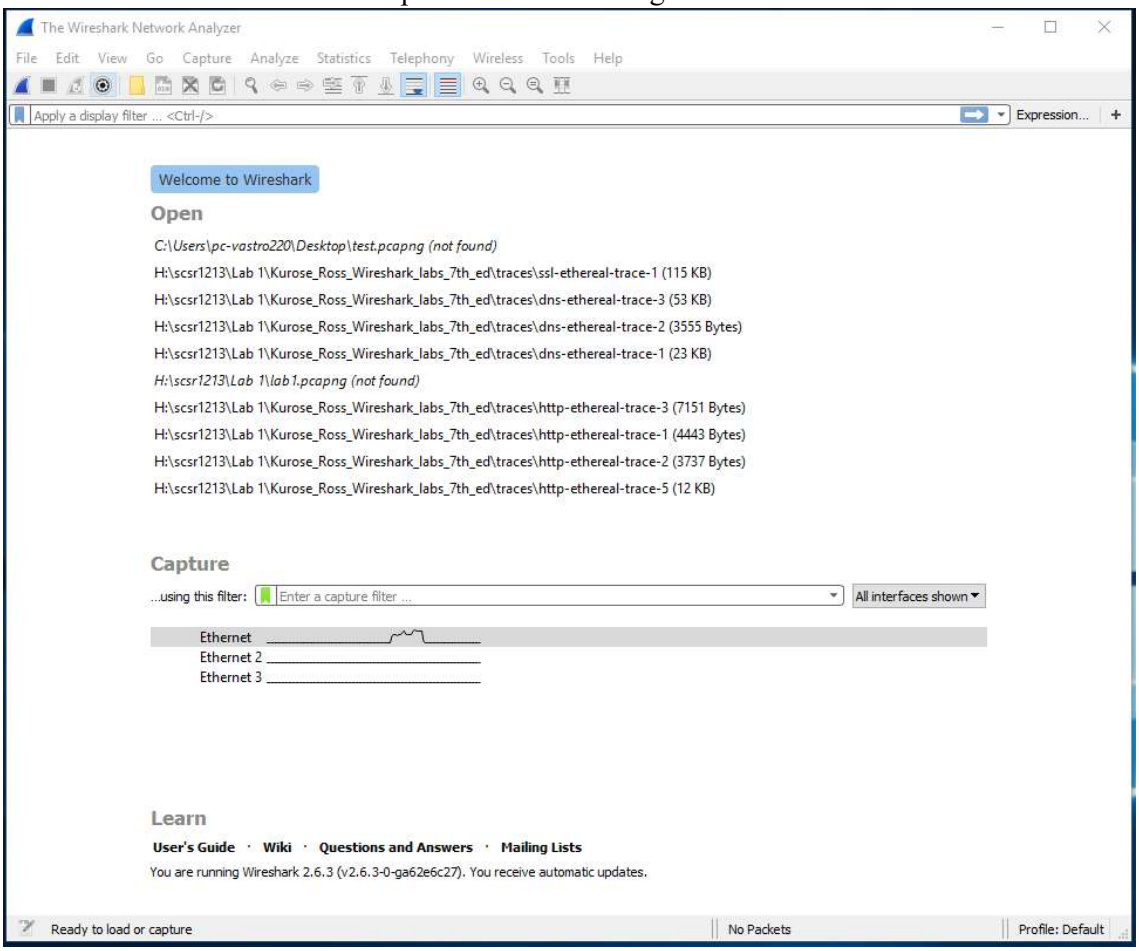


Figure A.2: Initial Wireshark startup screen

- The Wireshark interface has five major components as shown in Figure A.3.

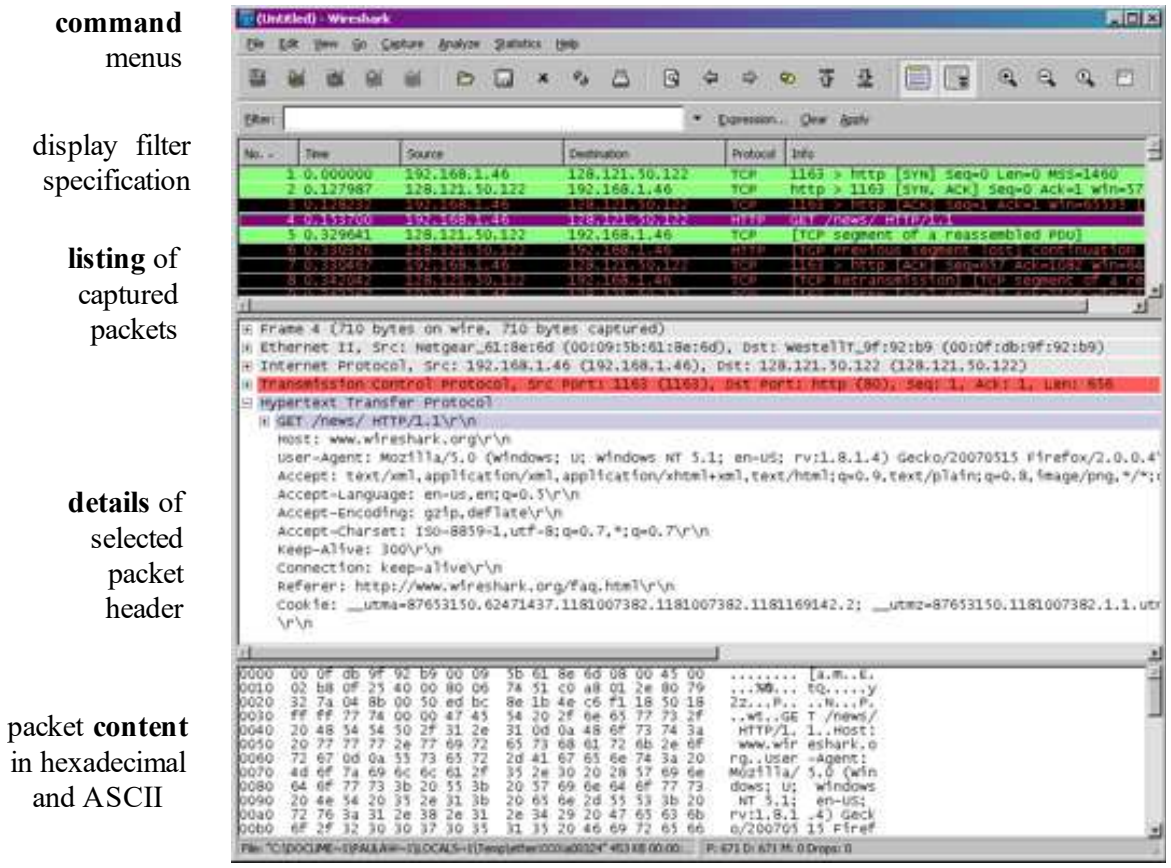


Figure A.3: Wireshark Graphical User Interface, during packet capture and

- The **command menus** are standard pulldown menus located at the top of the window.
- The **packet display filter field,** into which a protocol name or other information can be entered in order to filter the information displayed in the packet-listing window.
- The **packet-listing window** displays a one-line summary for each packet captured, including the packet number, the time at which the packet was captured, the packet's source and destination addresses, the protocol type, and protocol-specific information contained in the packet.
- The **packet-header details window** provides details about the packet selected (highlighted) in the packet-listing window. These details include information about the Ethernet frame and IP datagram that contains this packet. The amount of Ethernet and IP-layer detail displayed can be expanded or minimized by clicking on the plus minus boxes to the left of the Ethernet frame or IP datagram line in the packet details window. If the packet has been carried over TCP or UDP, TCP or UDP details will also be displayed, which can similarly be expanded or minimized. Finally, details about the highest-level protocol that sent or received this packet are also provided.
- The **packet-contents window** displays the entire contents of the captured frame, in both ASCII and hexadecimal format.

3.0 Test Run Wireshark

- Start up the Wireshark software.
- To begin packet capture, select the Capture pull down menu and pick Options menu. Select appropriate interfaces on your compute and click Start button to begin packet capture. Refer to Figure A.4

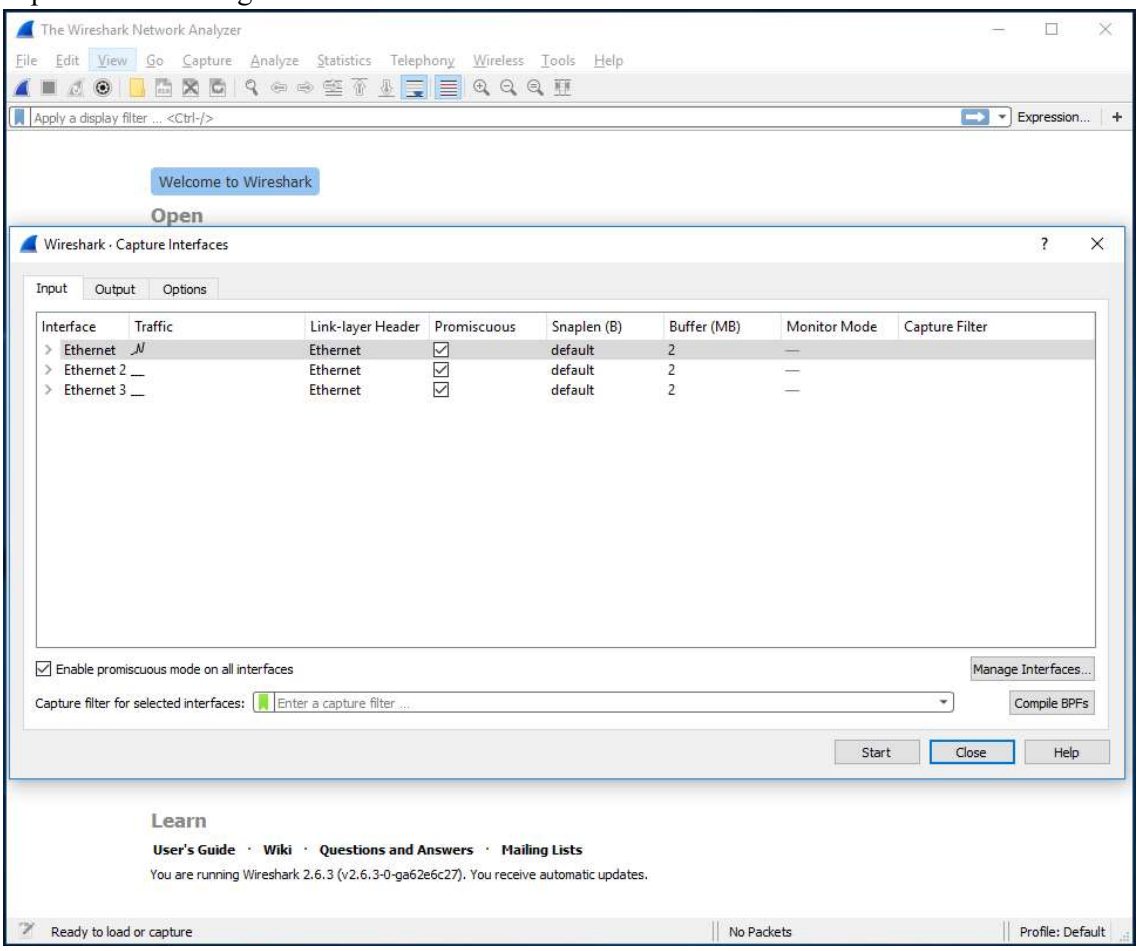


Figure A.4: Capture and Options Menu

- Once you begin packet capture, result will be shown as in Figure A.5.

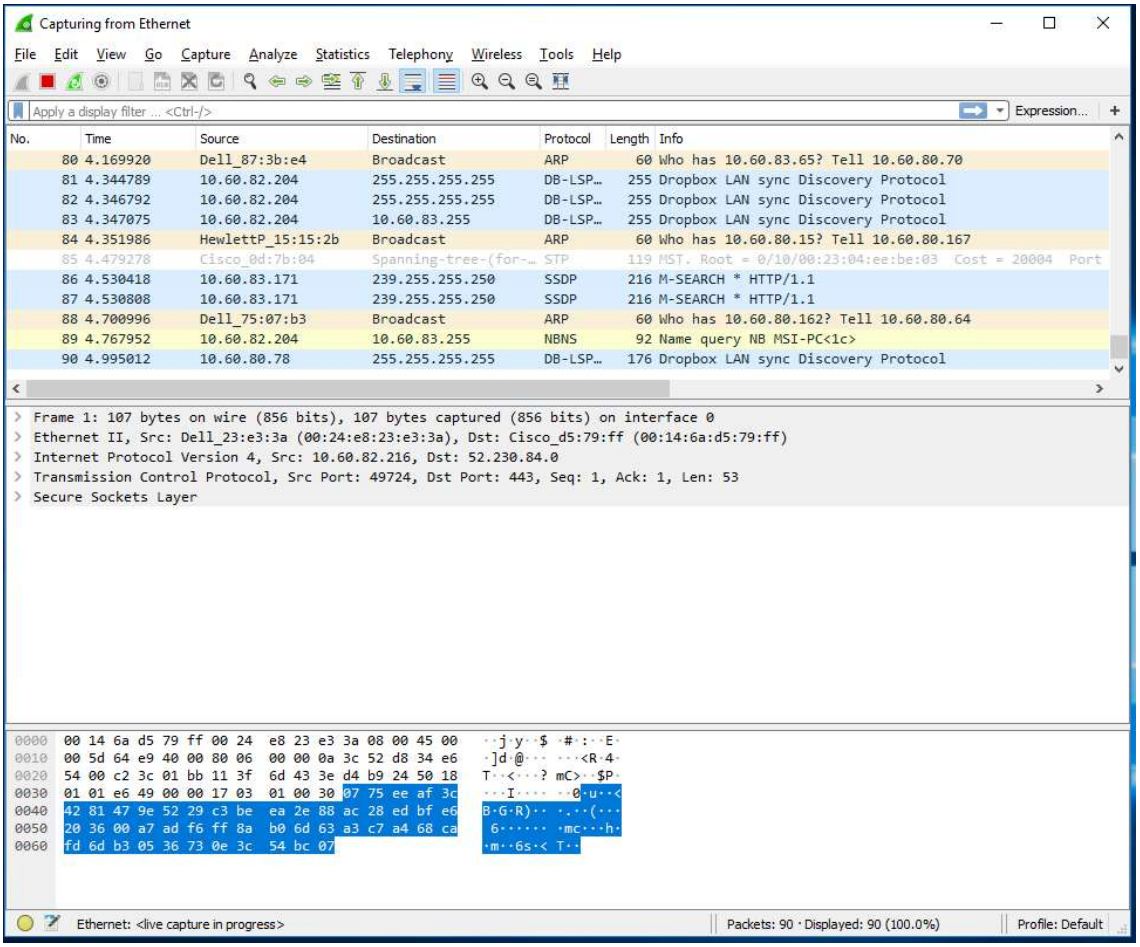


Figure A.5: Wireshark packet capture result

- By selecting Capture pulldown menu and selecting Stop, you can stop packet capture.

- Type “arp” in packet display filter field and press Enter key. This will cause only ARP message to be displayed in the packet-listing window as shown in Figure A.6.

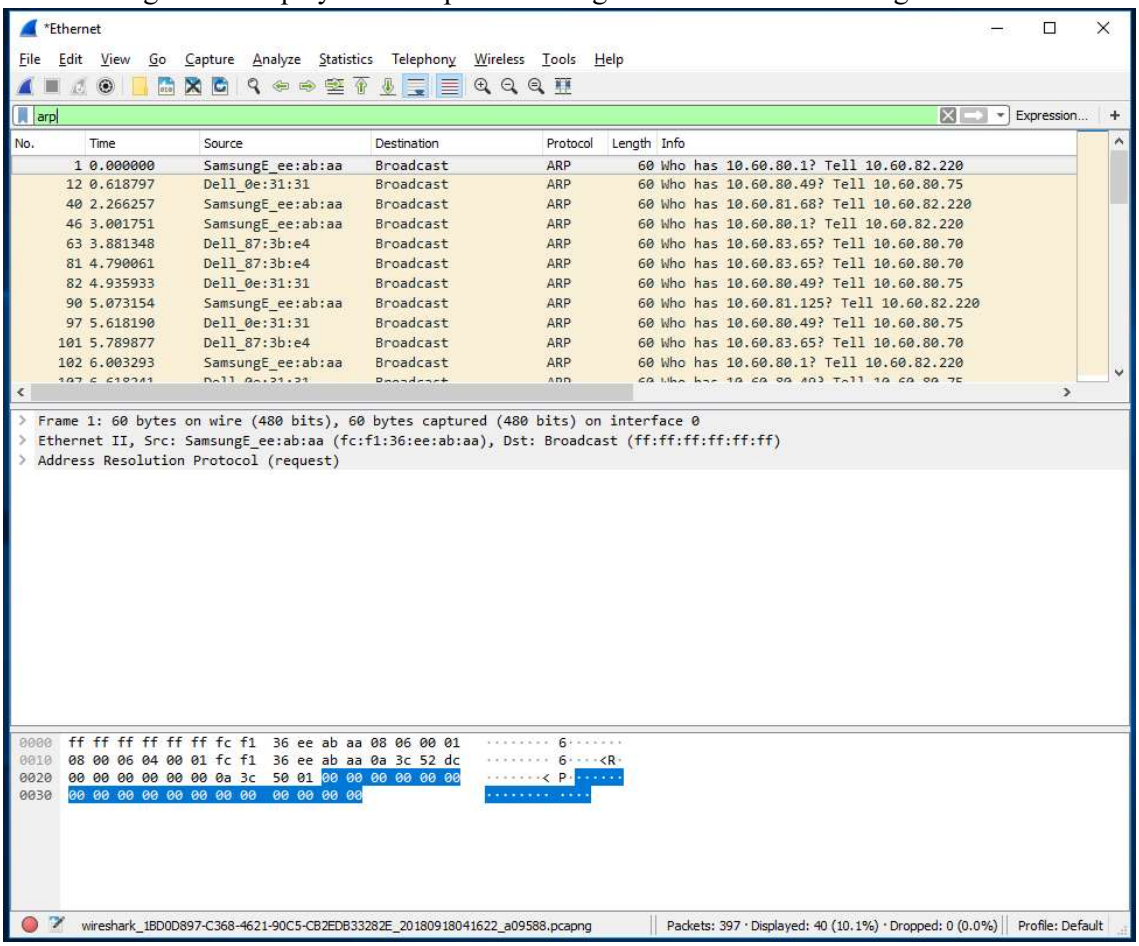


Figure A.6: ARP packet capture

- To save the trace result, use File pulldown menu and select Save function as shown in Figure A.7.

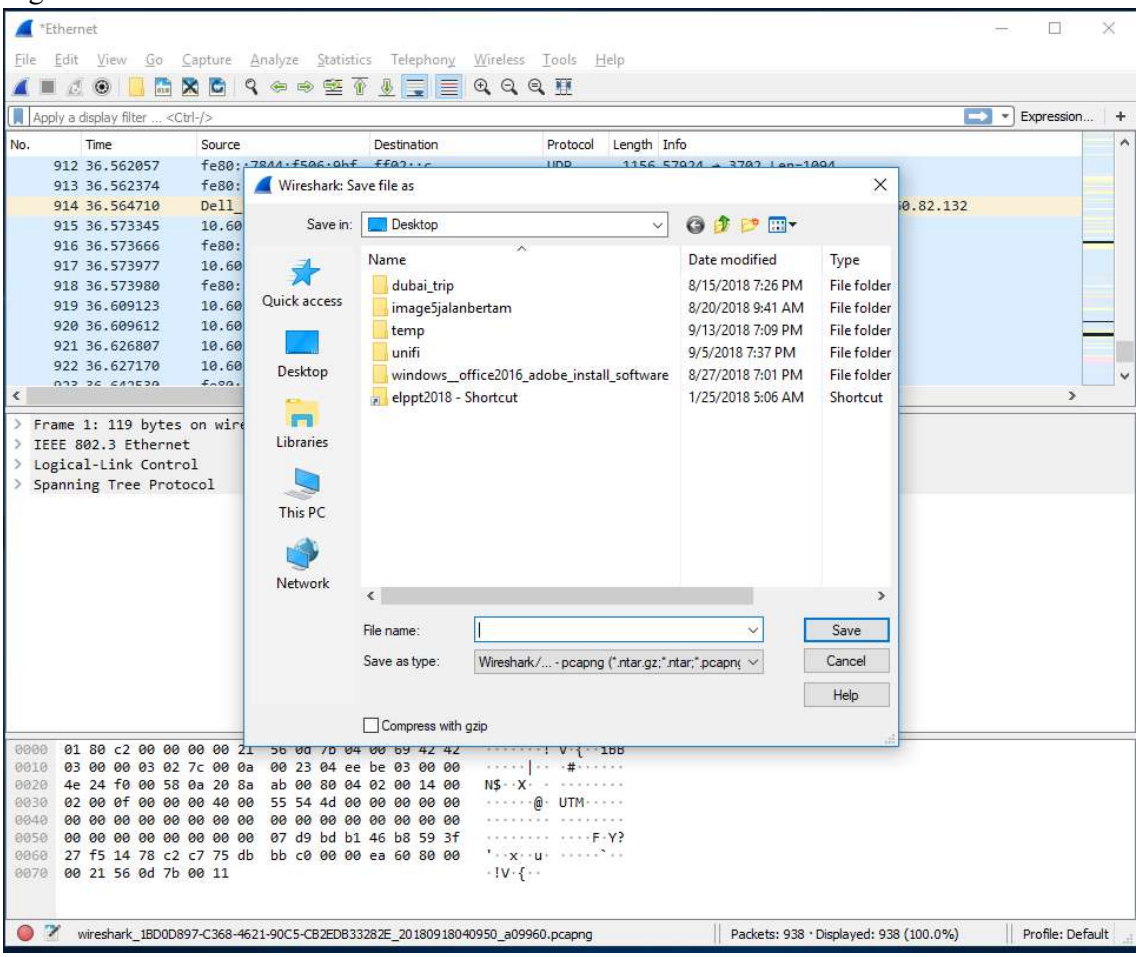


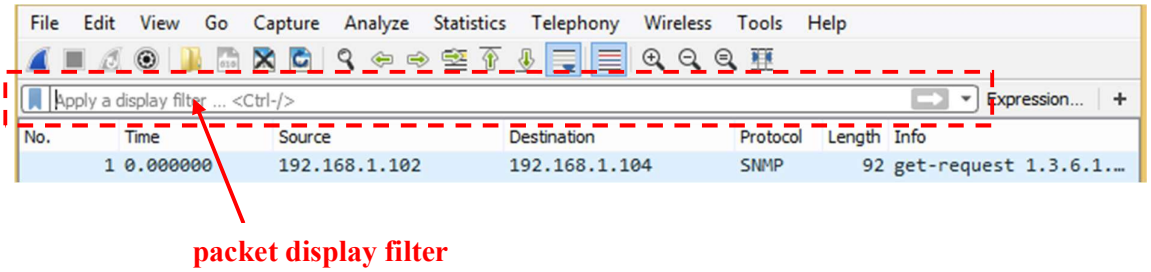
Figure A.7: Save Wireshark trace result

PART B: HTTP Trace

In this part, we'll explore several aspects of the HTTP protocol: the basic GET/response interaction, HTTP message formats and retrieving HTML files with embedded objects. Before beginning these labs, you might want to review Section 2.2 of the textbook.

B.1 The Basic HTTP GET/response interaction

- Open packet trace file **lab1-http-B01.pcapng**.
- Enter "**http**" (just the letters, not the quotation marks) in the **packet display filter field**, so that only captured HTTP messages will be displayed later in the packet-listing window. Refer to figure below:



- By looking at the information in the HTTP GET and response messages, answer the following questions:

1. What version of HTTP is the server running?

   HTTP/1.1

2. What is the IP address of the client computer?

   192.168.1.102

3. What is the IP address of the gaia.cs.umass.edu server?

   128.119.245.12

4. How many bytes of content are being returned to client browser?

   73 bytes, and 1071 bytes

5. What is the status code returned from the server to client browser?

   200 OK, and 404 Not Found

B.2 The HTTP CONDITIONAL GET/response interaction

- Open packet trace file **lab1-http-B02.pcapng**.
- By looking at the information in the HTTP GET and response messages, answer the following questions:

1. 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?

   There is no "IF-MODIFIED-SINCE" line in the HTTP GET.

2. Inspect the contents of the server response after the first GET request from client. Did the server explicitly return the contents of the file? How can you tell?

   The server returns the contents of the file. In packet 10, the server response HTTP/1.1 200 OK status, indicating success. Besides, the content of the file returned to client is same as the content in server, which confirms the file content were sent.

3. 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?

   The second HTTP GET request in packet 14 includes the "IF-MODIFIED-SINCE:" header. The information follows the "IF-MODIFIED-SINCE:" header is "Tue, 23 SEP 2003 05:35:00"

4. 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.

   304 Not Modified. The server did not explicitly return the contents of the file due to the "Not Modified" message. The server did not send the updated content of the file, but retrieve the previous version from the browser's cache memory.

B.3 HTML Documents with Embedded Objects

- Open packet trace file **lab1-http-B03.pcapng**.
- By looking at the information in the HTTP GET and response messages, answer the following questions:

1. How many HTTP GET request messages did client browser send?

   3 HTTP GET request messages were sent.

2. To which Internet addresses were these GET requests sent?

   128.119.245.12, 165.193.123.218, and 134.241.6.82

3. How many bytes of content are being returned to client browser for the **pearson-logo-footer.gif** image file?

   3357 bytes

4. How many bytes of content are being returned to client browser for the **cover.jpg** image file?

   15642 bytes

PART C: DNS Trace

1.0 nslookup

nslookup tool allows the host running the tool to query any specified DNS server for a DNS record. The queried DNS server can be a root DNS server, a top-level-domain DNS server, an authoritative DNS server, or an intermediate DNS server. To accomplish this task, nslookup sends a DNS query to the specified DNS server, receives a DNS reply from that same DNS server, and displays the result.

- To run it in Windows, open the Command Prompt (cmd) and run nslookup on the command line as shown in Figure C.1 and Figure C.2

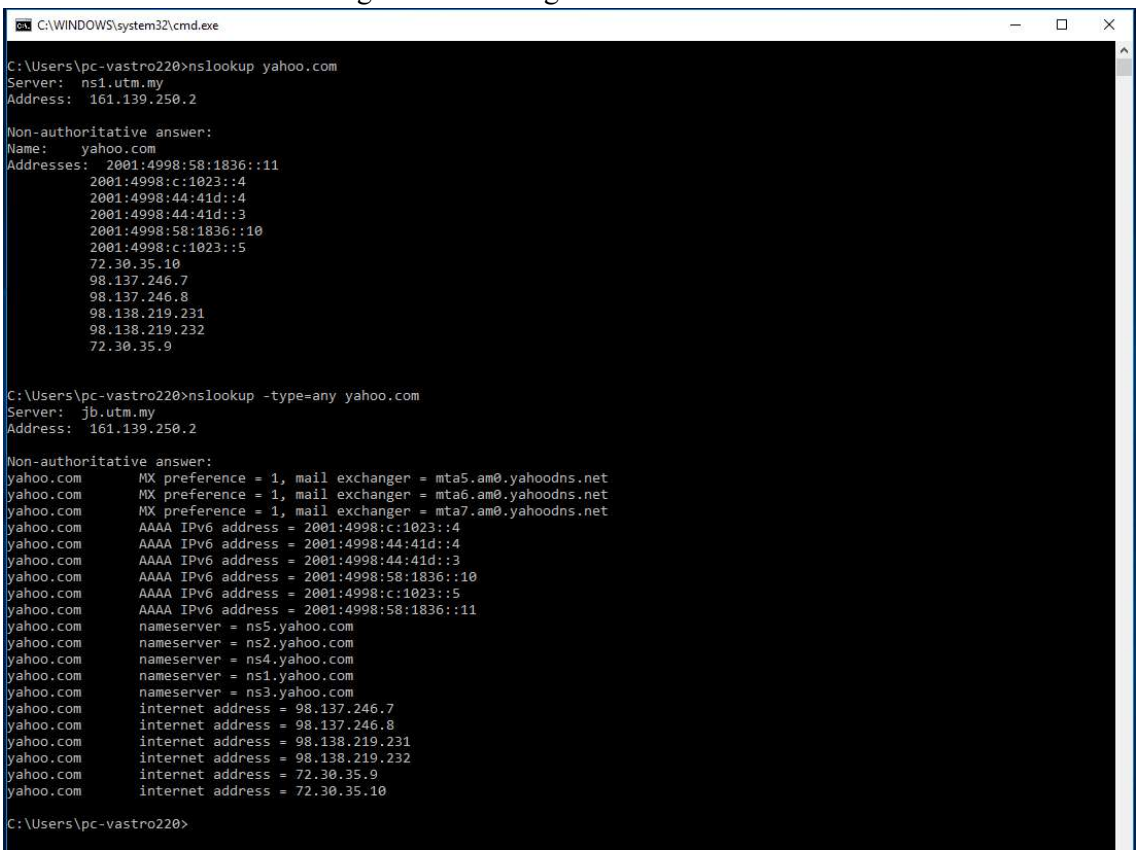


Figure C.1: nslookup result

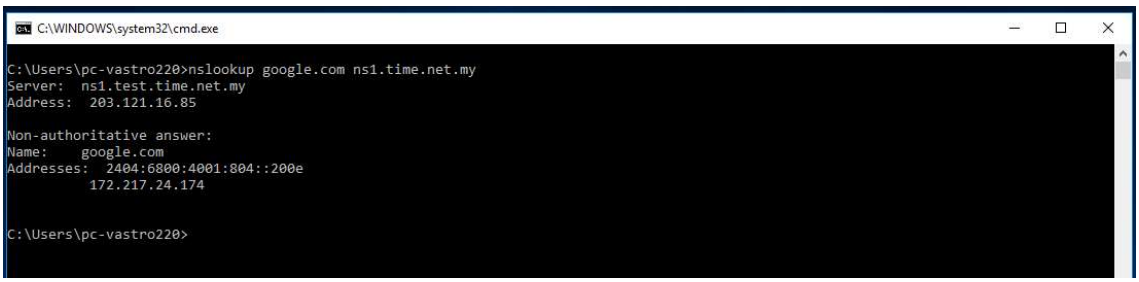
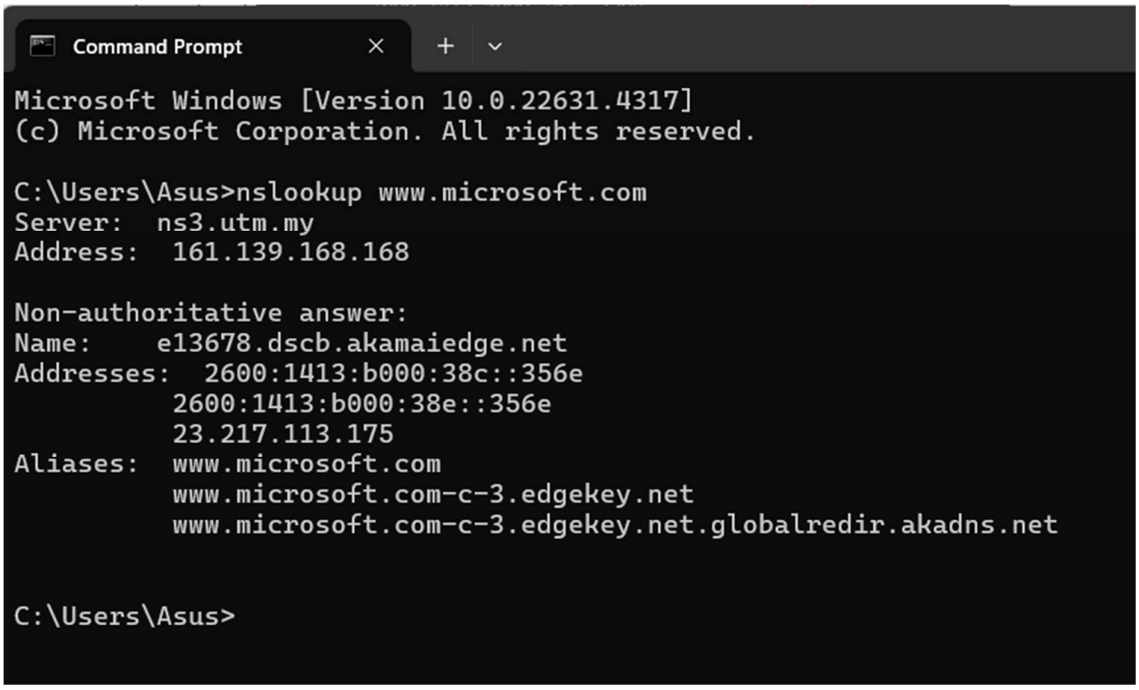


Figure C.2: nslookup result

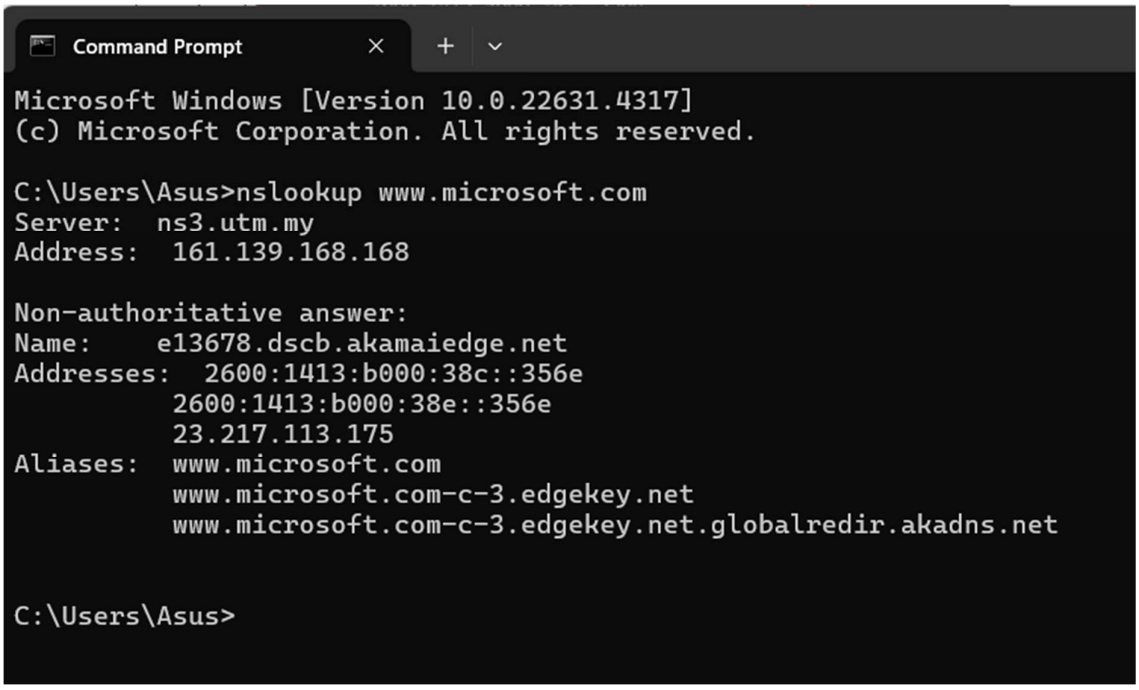
1. Run nslookup to obtain the IP address of a www.microsoft.com server. What is the IP address of that server? Add screenshot to your answer.

   IP address of the server: 161.139.168.168



2. Run nslookup to determine the non-authoritative DNS servers for domain microsoft.com. Add screenshot to your answer.

   2600:1413:b000:38c::356e
   2600:1413:b000:38e::356e
   23.217.113.175



2.0 ipconfig

ipconfig can be used to show your current TCP/IP information, including your address, DNS server addresses, adapter type and so on.

- Information about host, use the following command: ipconfig /all

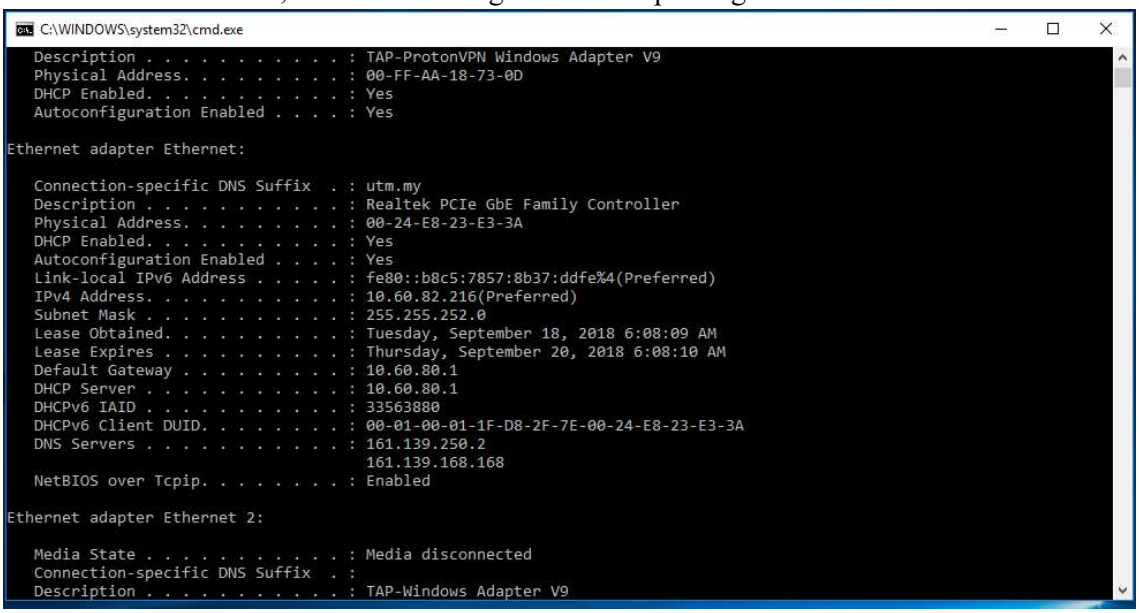


Figure C.3: ipconfig /all result

- ipconfig is also very useful for managing the DNS information stored in your host. Each entry shows the remaining Time to Live (TTL) in seconds.
  Command: ipconfig /displaydns

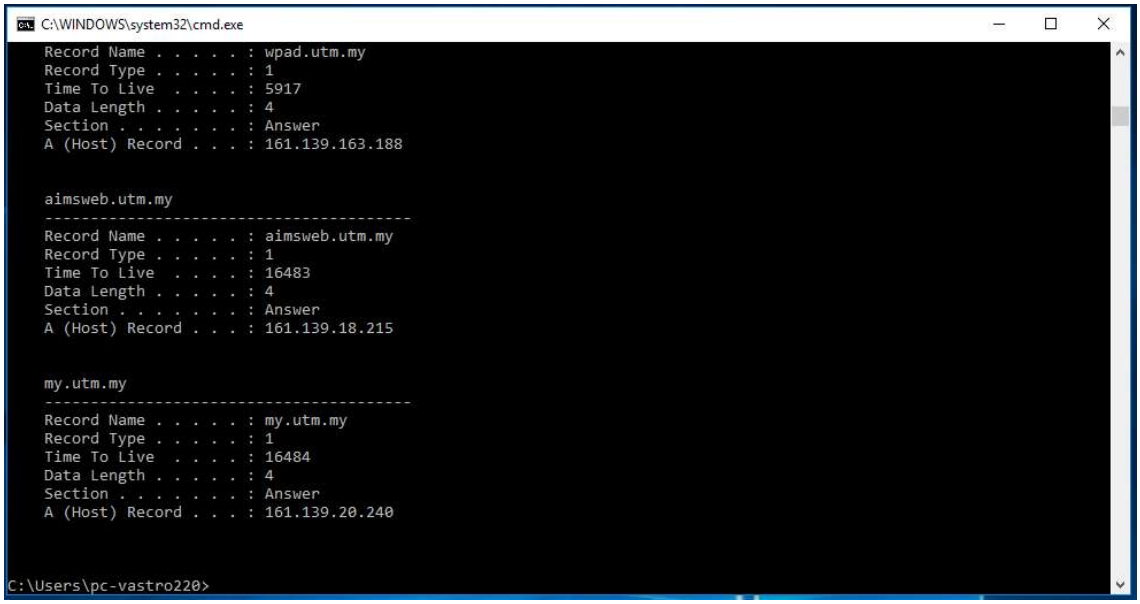


Figure C.4: ipconfig /displaydns result

- Flushing the DNS cache clears all entries and reloads the entries from the hosts file.

  Command: ipconfig /flushdns

Figure C.5: ipconfig /flushdns result

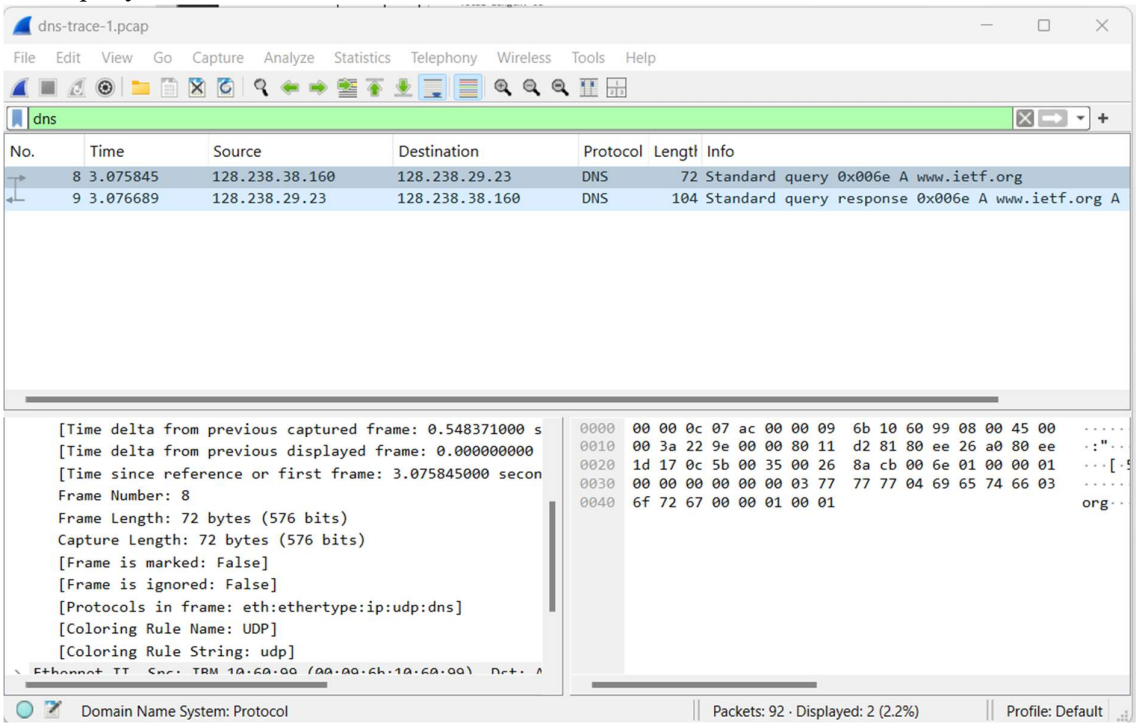
3.0 Tracing DNS with Wireshark

- Open packet trace file dns-trace-1. Answer the following questions.

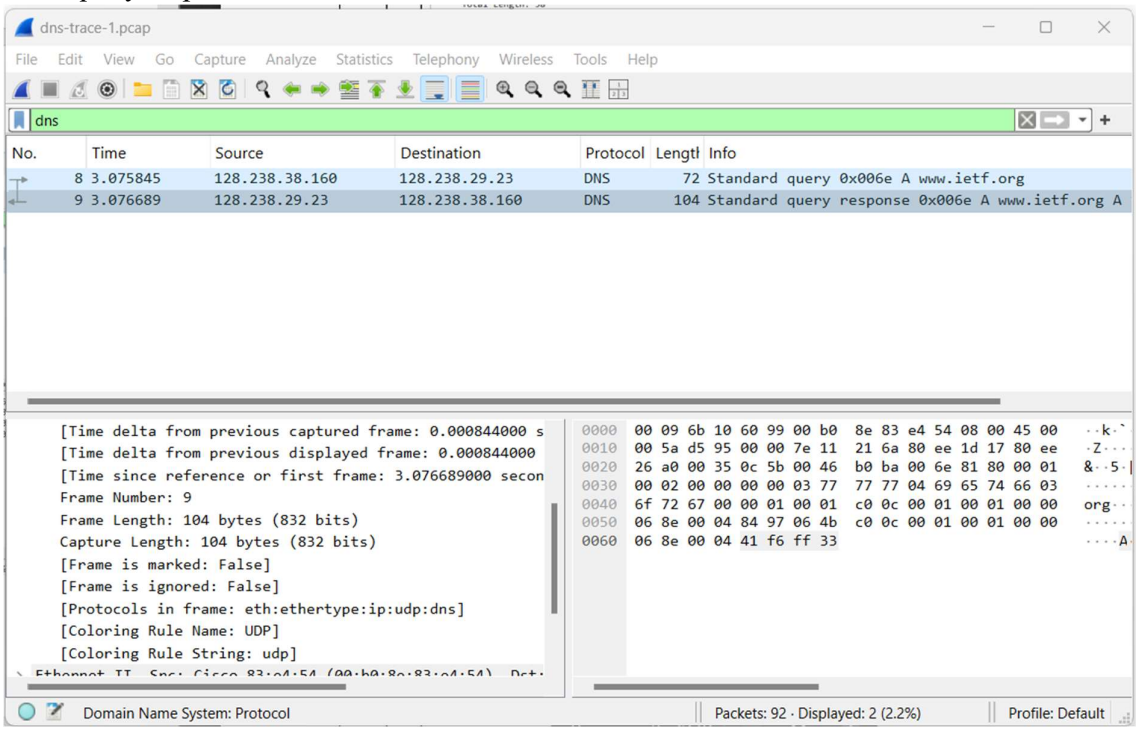
1. Locate the DNS query and response messages. Are then sent over UDP or TCP? Add screenshots in your answer.

   DNS query: UDP
   DNS query response: UDP

DNS query:



DNS query response:

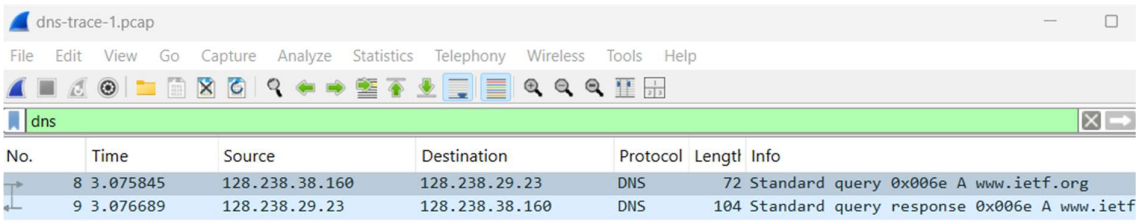


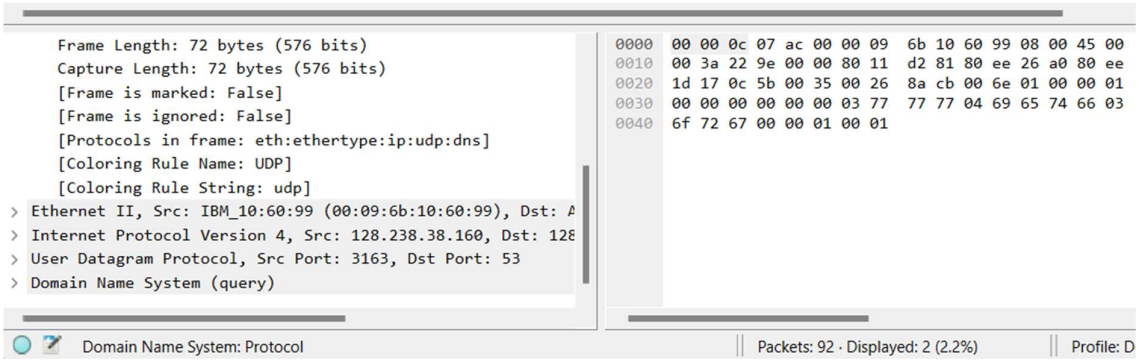
2. What is the destination port for the DNS query message? What is the source port of DNS response message? Add screenshots in your answer.

Destination port for DNS query message: Port 53

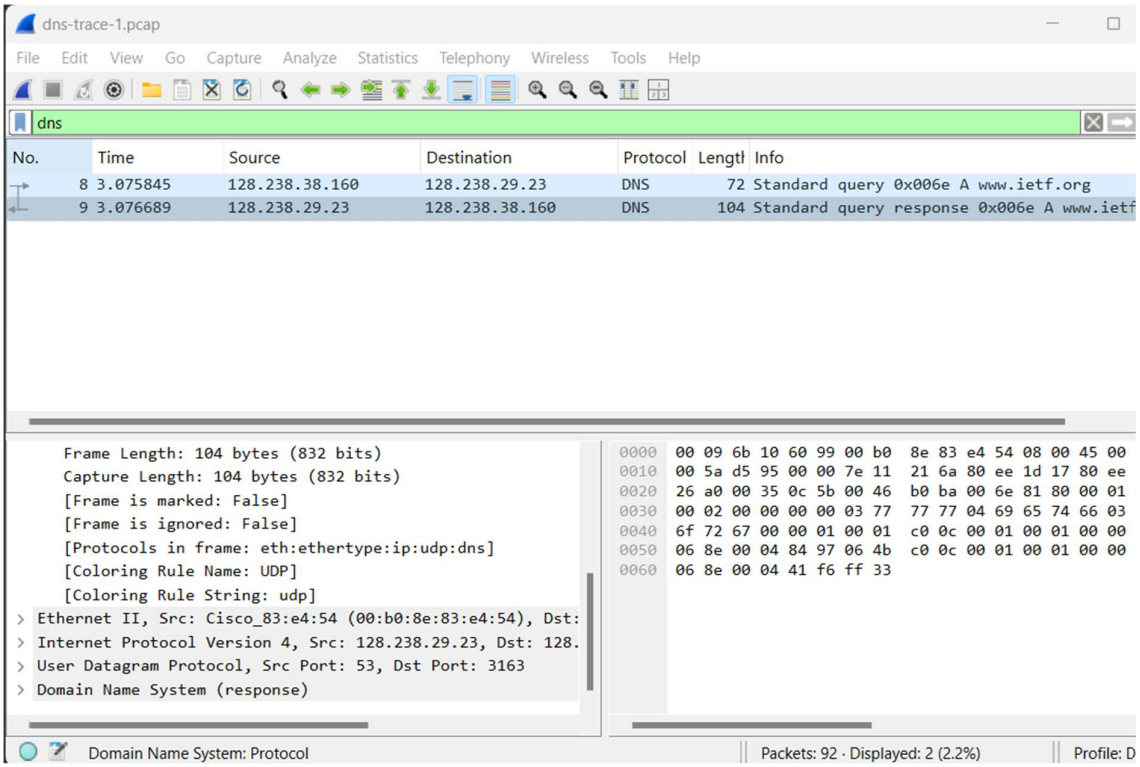
Source port of DNS response message: Port 53

Destination port for DNS query message:



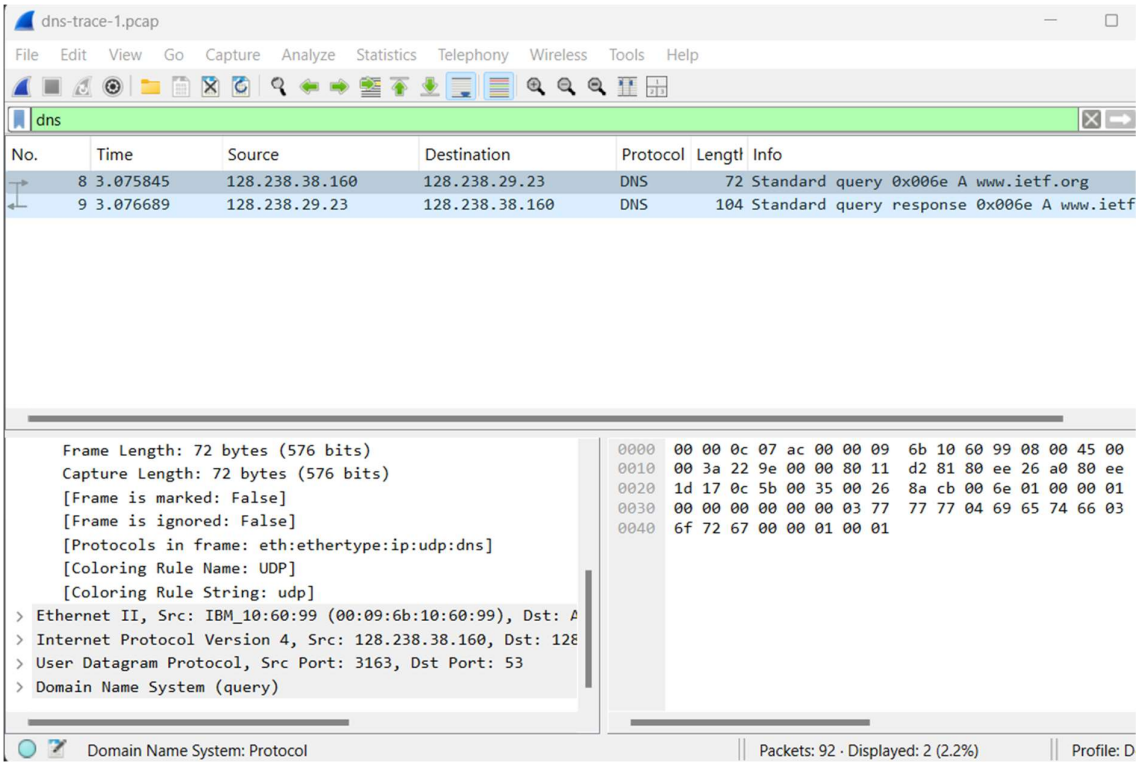


Source port of DNS response message:


dns-trace-1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Lengtl Info
8 3.075845 128.238.38.160 128.238.29.23 DNS 72 Standard query 0x006e A www.ietf.org
9 3.076689 128.238.29.23 128.238.38.160 DNS 104 Standard query response 0x006e A www.ietf
Frame Length: 104 bytes (832 bits)
Capture Length: 104 bytes (832 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: Cisco_83:e4:54 (00:b0:8e:83:e4:54), Dst:
Internet Protocol Version 4, Src: 128.238.29.23, Dst: 128.
User Datagram Protocol, Src Port: 53, Dst Port: 3163
Domain Name System (response)
0000 00 09 6b 10 60 99 00 b0 8e 83 e4 54 08 00 45 00
0010 00 5a d5 95 00 00 7e 11 21 6a 80 ee 1d 17 80 ee
0020 26 a0 00 35 0c 5b 00 46 b0 ba 00 6e 81 80 00 01
0030 00 02 00 00 00 00 03 77 77 77 04 69 65 74 66 03
0040 6f 72 67 00 00 01 00 01 c0 0c 00 01 00 01 00 00
0050 06 8e 00 04 84 97 06 4b c0 0c 00 01 00 01 00 00
0060 06 8e 00 04 41 f6 ff 33
Domain Name System: Protocol
Packets: 92 · Displayed: 2 (2.2%)
Profile: D

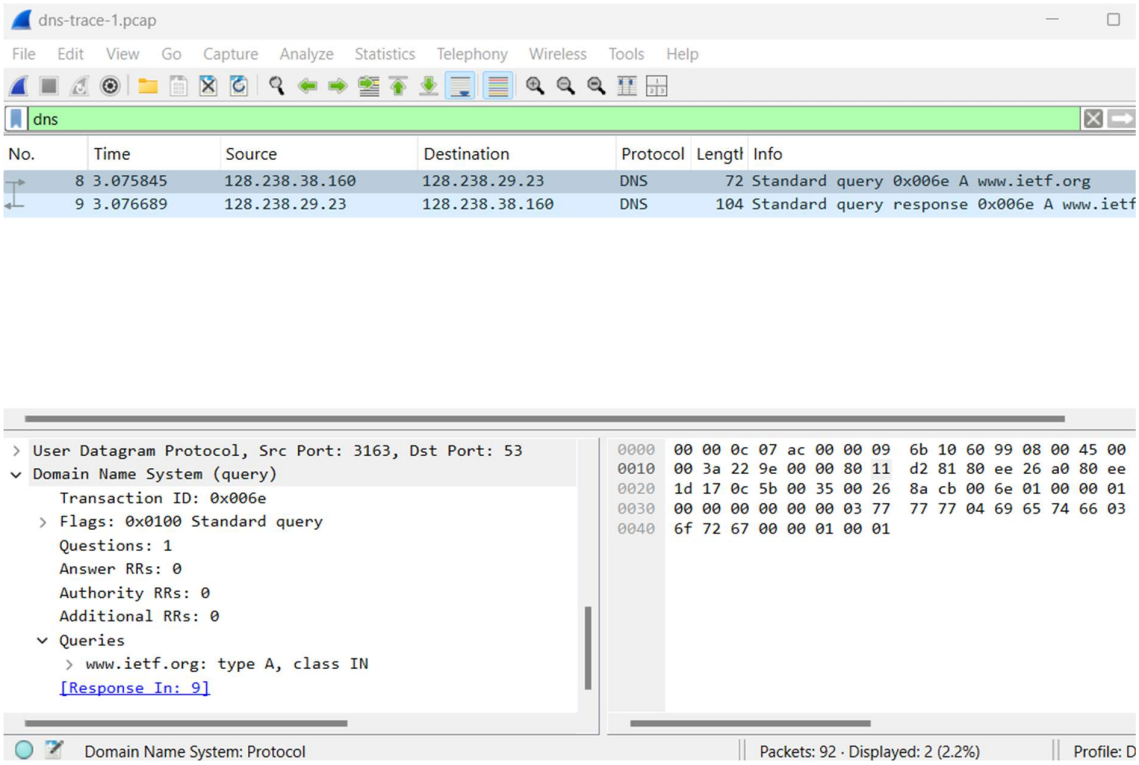
3. To what IP address is the DNS query message sent? Add screenshots in your answer.

   128.238.38.160



4. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"? Add screenshots in your answer.

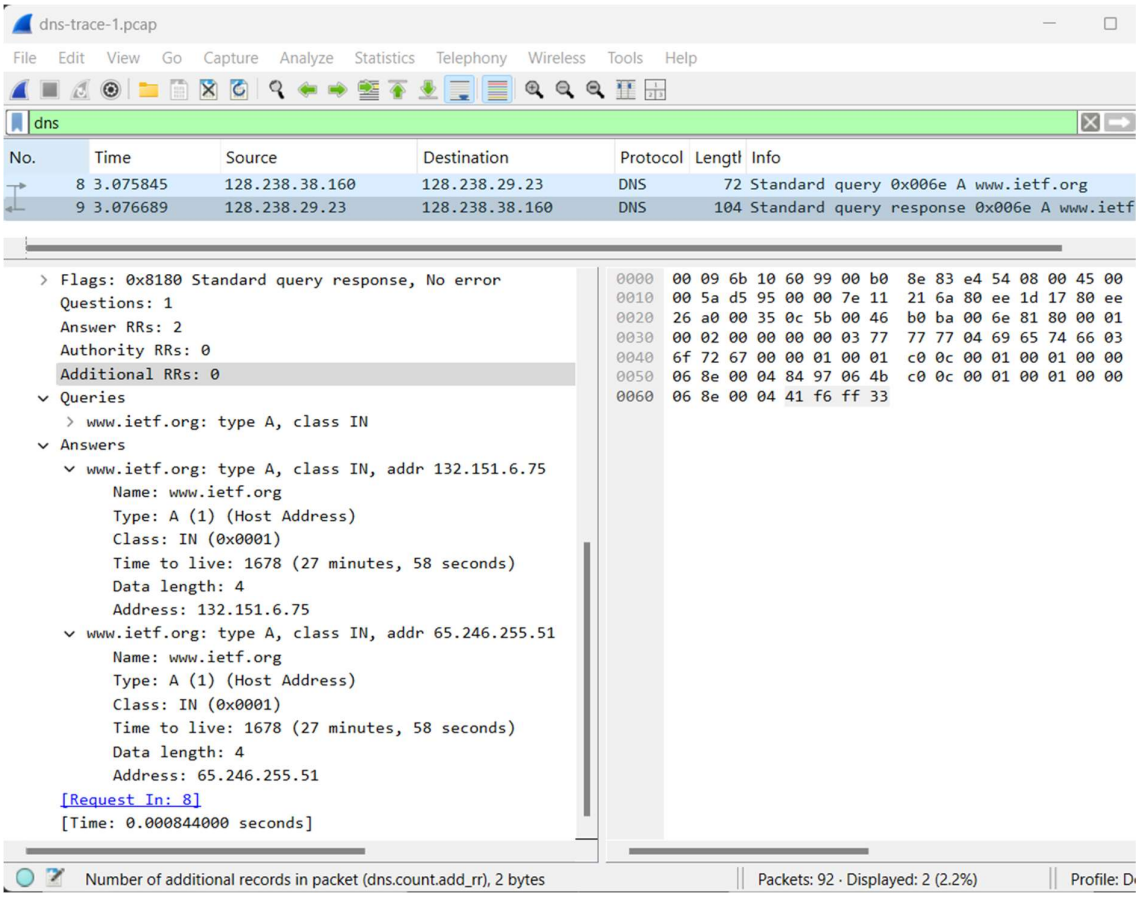
   Type A. The query message contains 0 "answers".



5. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain? Add screenshots in your answer.

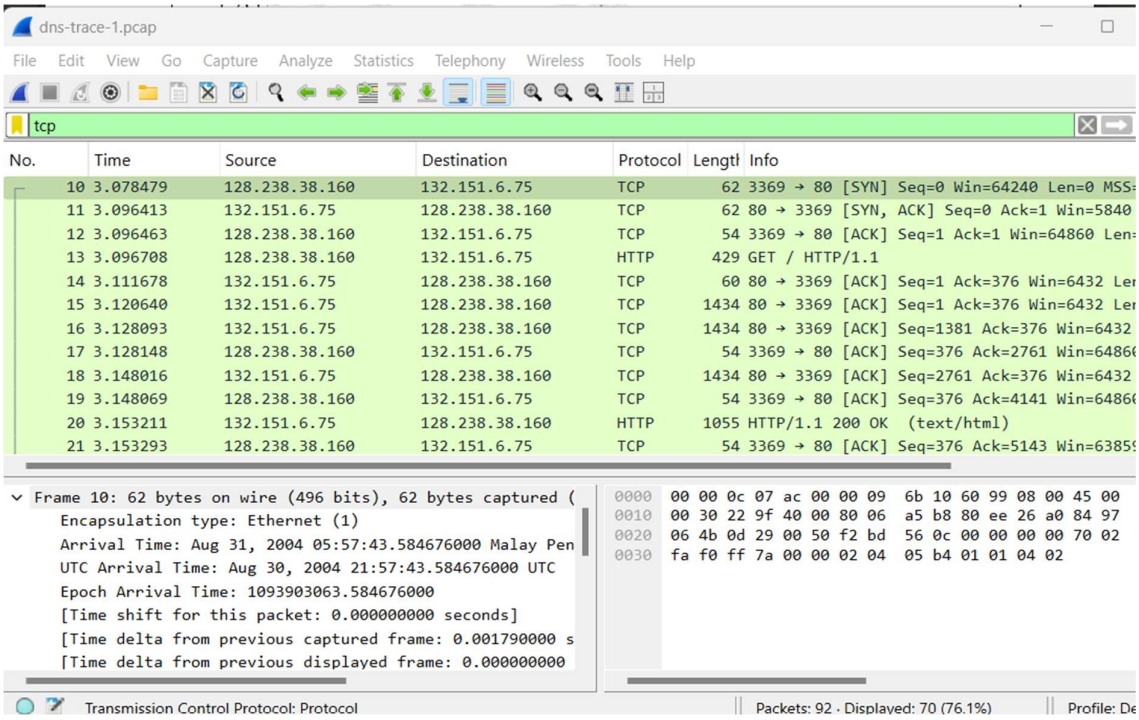
   2 “answers” are provided.

   Content of answers:


dns-trace-1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Lengtl Info
8 3.075845 128.238.38.160 128.238.29.23 DNS 72 Standard query 0x006e A www.ietf.org
9 3.076689 128.238.29.23 128.238.38.160 DNS 104 Standard query response 0x006e A www.ietf
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 0
Queries
www.ietf.org: type A, class IN
Answers
www.ietf.org: type A, class IN, addr 132.151.6.75
Name: www.ietf.org
Type: A (1) (Host Address)
Class: IN (0x0001)
Time to live: 1678 (27 minutes, 58 seconds)
Data length: 4
Address: 132.151.6.75
www.ietf.org: type A, class IN, addr 65.246.255.51
Name: www.ietf.org
Type: A (1) (Host Address)
Class: IN (0x0001)
Time to live: 1678 (27 minutes, 58 seconds)
Data length: 4
Address: 65.246.255.51
[Request In: 8]
[Time: 0.000844000 seconds]
0000 00 09 6b 10 60 99 00 b0 8e 83 e4 54 08 00 45 00
0010 00 5a d5 95 00 00 7e 11 21 6a 80 ee 1d 17 80 ee
0020 26 a0 00 35 0c 5b 00 46 b0 ba 00 6e 81 80 00 01
0030 00 02 00 00 00 00 03 77 77 77 04 69 65 74 66 03
0040 6f 72 67 00 00 01 00 01 c0 0c 00 01 00 01 00 00
0050 06 8e 00 04 84 97 06 4b c0 0c 00 01 00 01 00 00
0060 06 8e 00 04 41 f6 ff 33
Number of additional records in packet (dns.count.add_rr), 2 bytes
Packets: 92 · Displayed: 2 (2.2%)
Profile:

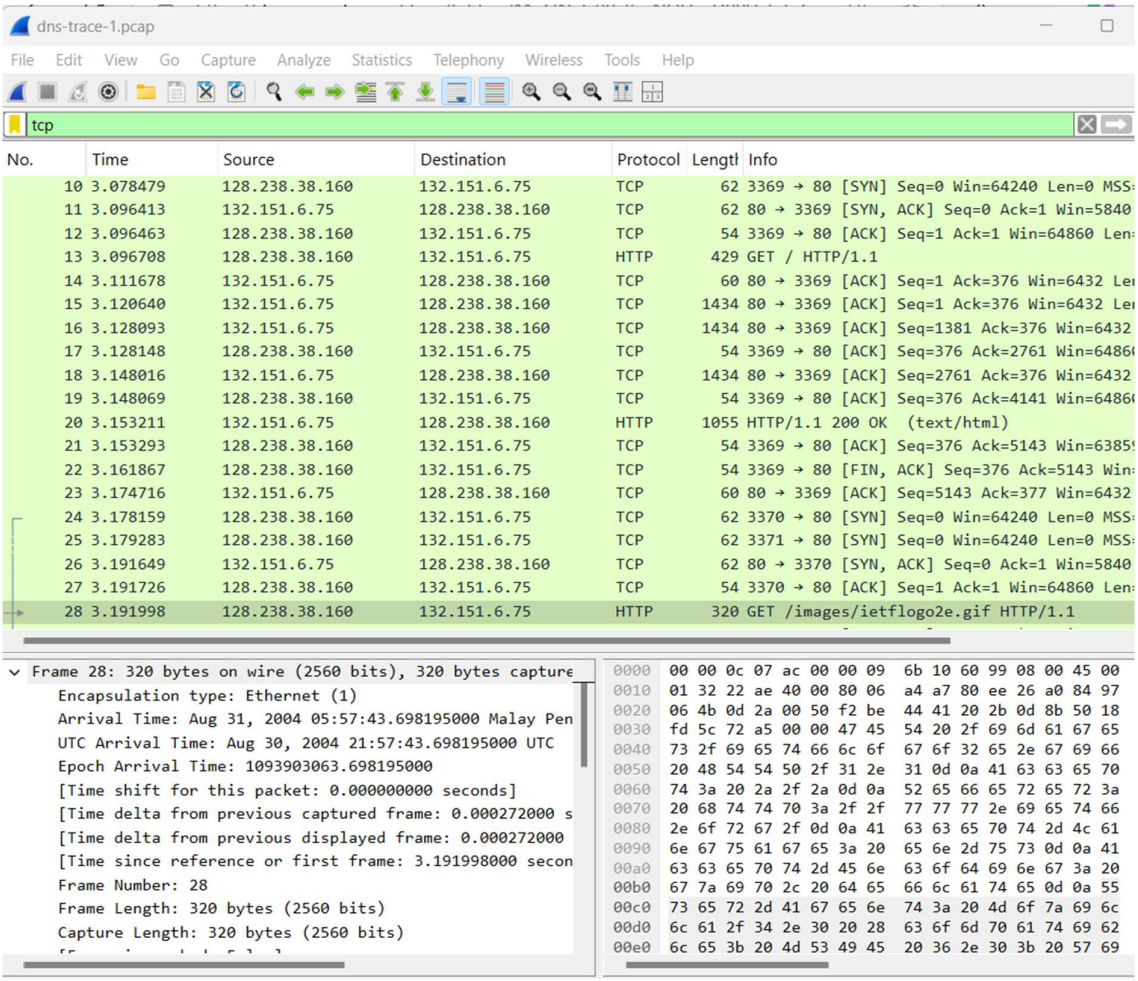
6. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message? Add screenshots in your answer.

   Yes, the destination IP address of the SYN packet correspond to the IP addresses provided in the DNS response message.



7. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

   No, because DNS query will only appear once in entire tracing. No new DNS queries issue by the host between line 10 to line 27 before retrieving image in line 28.



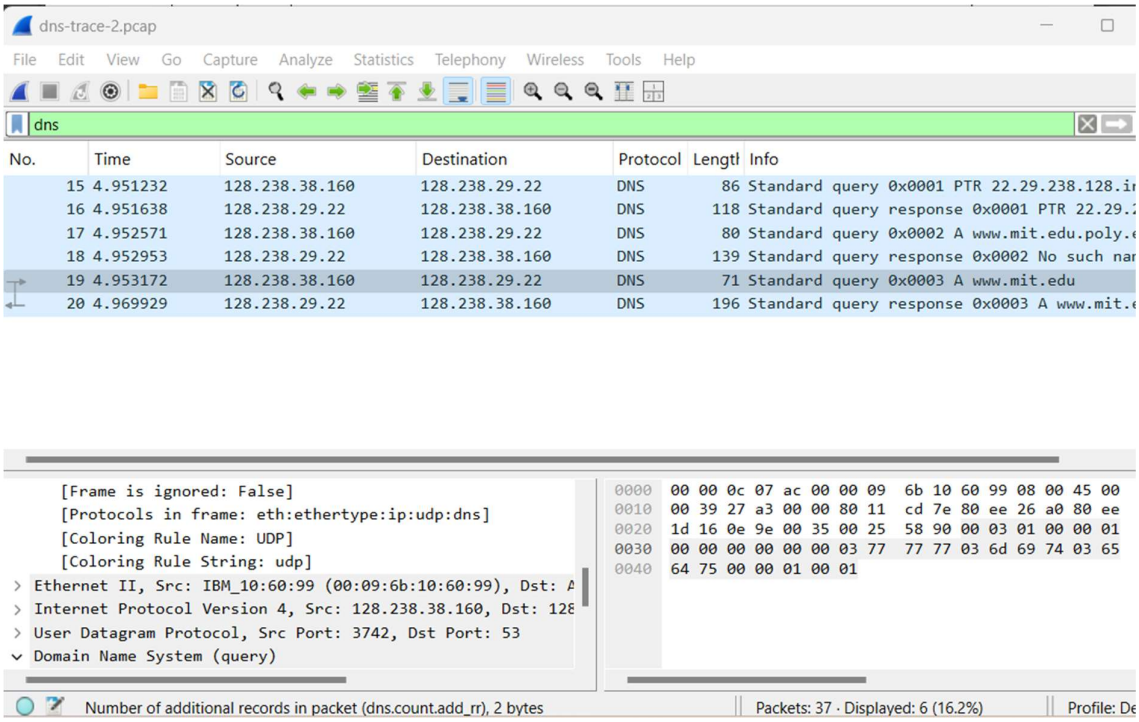
- Open packet trace file dns-trace-2 for nslookup.
- We see from Wireshark that nslookup actually sent three DNS queries and received three DNS responses. For the purpose of this lab, ignore the first two sets of queries/responses, as they are specific to nslookup and are not normally generated by standard Internet applications. You should instead focus on the last query and response messages.
- Answer the following questions.

8. What is the destination port for the DNS query message? What is the source port of DNS response message? Add screenshots in your answer.

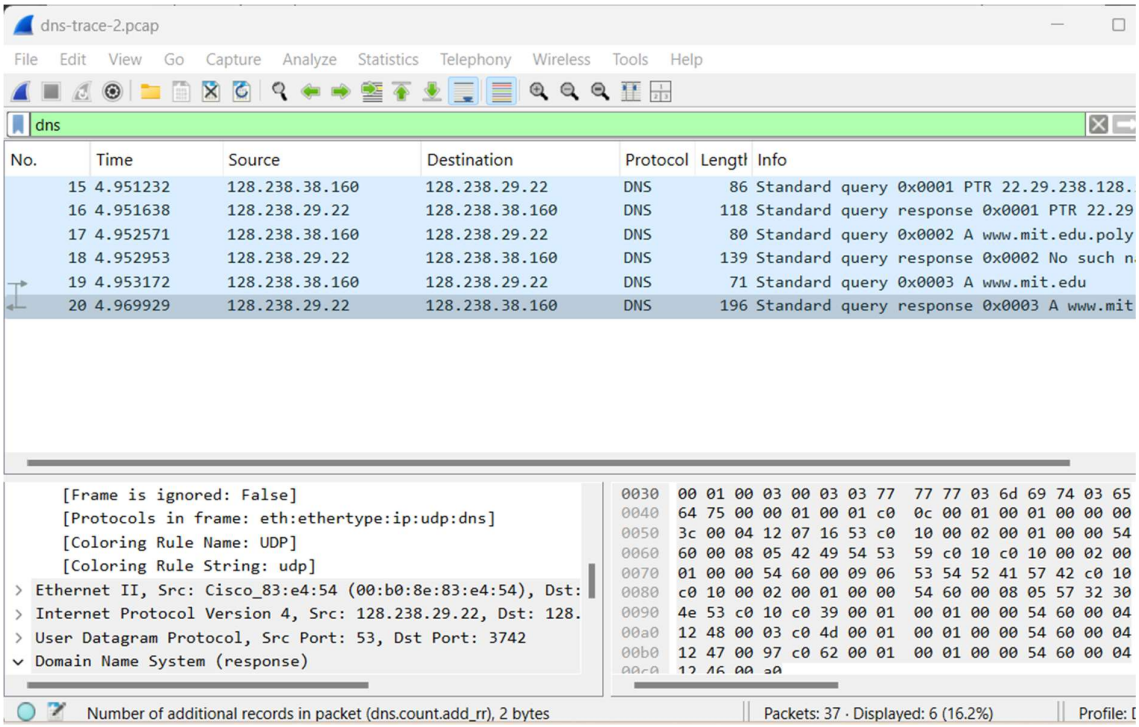
   Destination port for the DNS query message: Port 53

   Source port of DNS response message: Port 53

Destination port for the DNS query message:



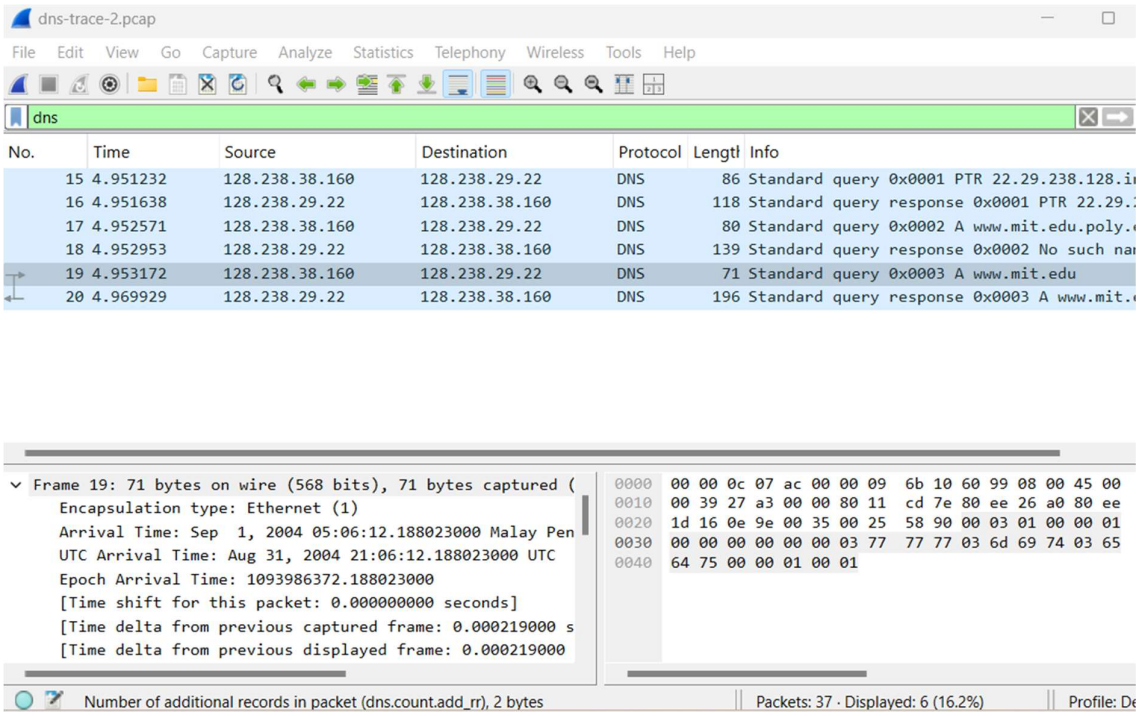
Source port of DNS response message:

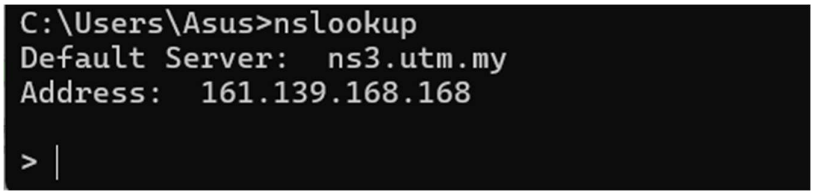


9. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? Add screenshots in your answer.

   Destination IP address of the DNS query message sent: 128.238.29.22

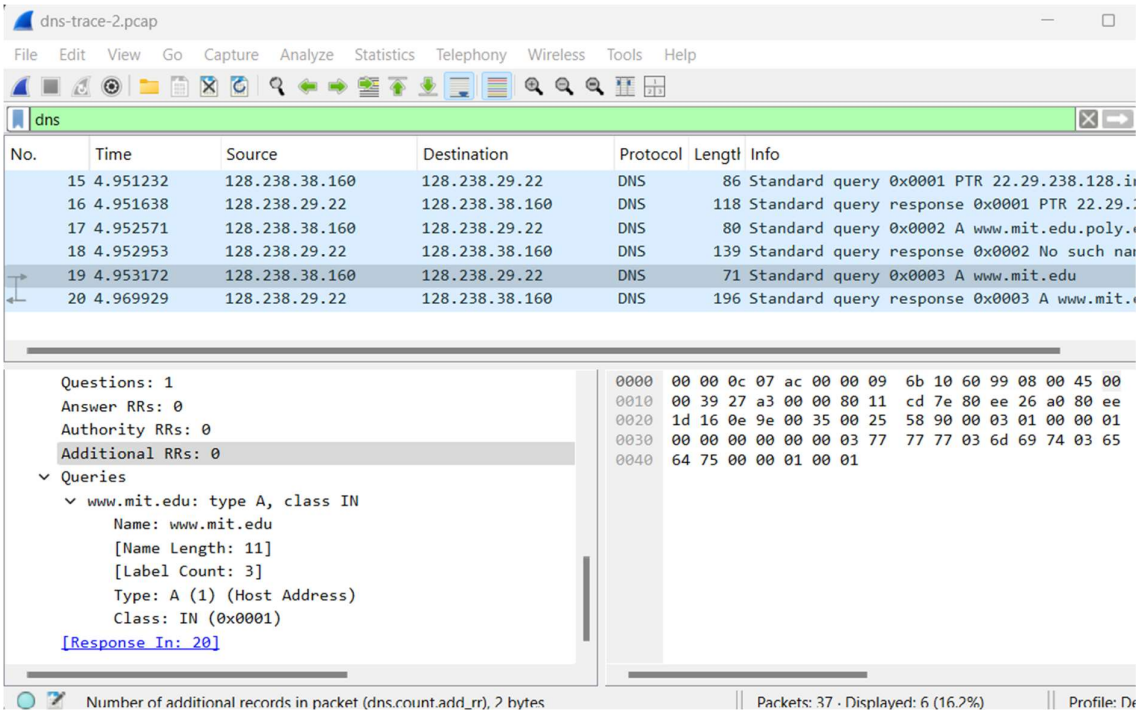
   The destination IP address is different with my default local DNS server.





10. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"? Add screenshots in your answer.

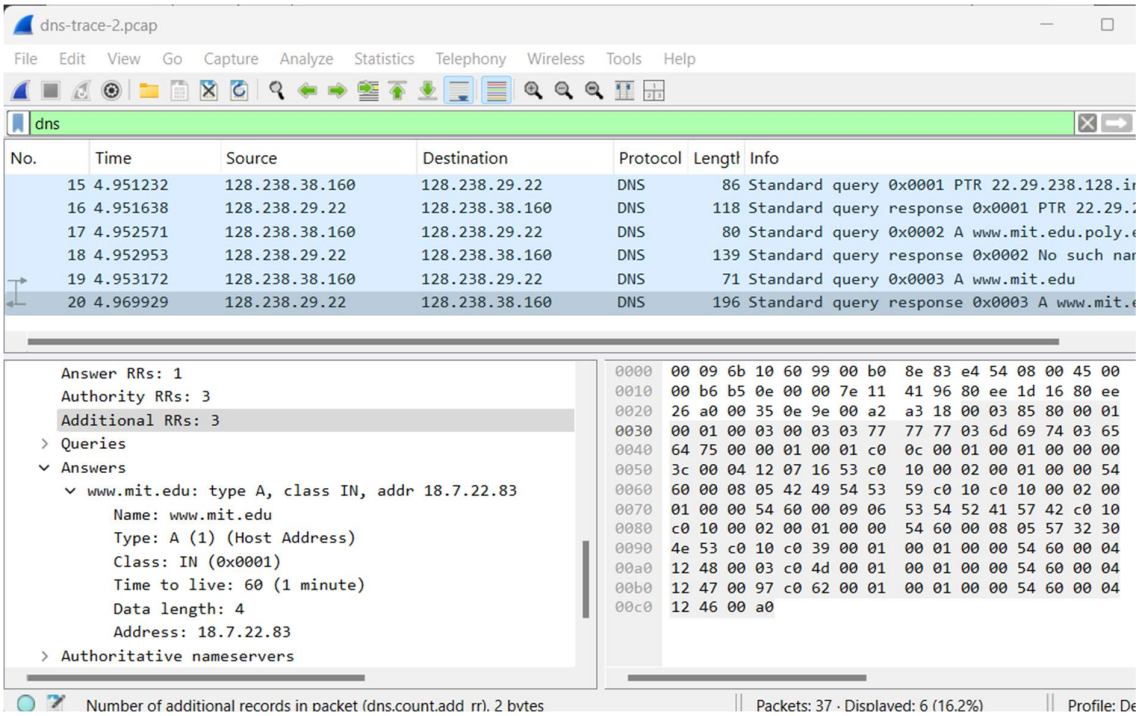
    Type A. The query contains 0 "answers".



11. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain? Add screenshots in your answer.

    1 “answer” is provided.

    Content of answer:


dns-trace-2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Lengtl Info
15 4.951232 128.238.38.160 128.238.29.22 DNS 86 Standard query 0x0001 PTR 22.29.238.128.i
16 4.951638 128.238.29.22 128.238.38.160 DNS 118 Standard query response 0x0001 PTR 22.29.
17 4.952571 128.238.38.160 128.238.29.22 DNS 80 Standard query 0x0002 A www.mit.edu.poly.
18 4.952953 128.238.29.22 128.238.38.160 DNS 139 Standard query response 0x0002 No such na
19 4.953172 128.238.38.160 128.238.29.22 DNS 71 Standard query 0x0003 A www.mit.edu
20 4.969929 128.238.29.22 128.238.38.160 DNS 196 Standard query response 0x0003 A www.mit.
Answer RRs: 1
Authority RRs: 3
Additional RRs: 3
Queries
Answers
www.mit.edu: type A, class IN, addr 18.7.22.83
Name: www.mit.edu
Type: A (1) (Host Address)
Class: IN (0x0001)
Time to live: 60 (1 minute)
Data length: 4
Address: 18.7.22.83
Authoritative nameservers
0000 00 09 6b 10 60 99 00 b0 8e 83 e4 54 08 00 45 00
0010 00 b6 b5 0e 00 00 7e 11 41 96 80 ee 1d 16 80 ee
0020 26 a0 00 35 0e 9e 00 a2 a3 18 00 03 85 80 00 01
0030 00 01 00 03 00 03 03 77 77 77 03 6d 69 74 03 65
0040 64 75 00 00 01 00 01 c0 0c 00 01 00 01 00 00 00
0050 3c 00 04 12 07 16 53 c0 10 00 02 00 01 00 00 54
0060 60 00 08 05 42 49 54 53 59 c0 10 c0 10 00 02 00
0070 01 00 00 54 60 00 09 06 53 54 52 41 57 42 c0 10
0080 c0 10 00 02 00 01 00 00 54 60 00 08 05 57 32 30
0090 4e 53 c0 10 c0 39 00 01 00 01 00 00 54 60 00 04
00a0 12 48 00 03 c0 4d 00 01 00 01 00 00 54 60 00 04
00b0 12 47 00 97 c0 62 00 01 00 01 00 00 54 60 00 04
00c0 12 46 00 a0
Number of additional records in packet (dns.count.add_rr), 2 bytes
Packets: 37 · Displayed: 6 (16.2%)
Profile: De