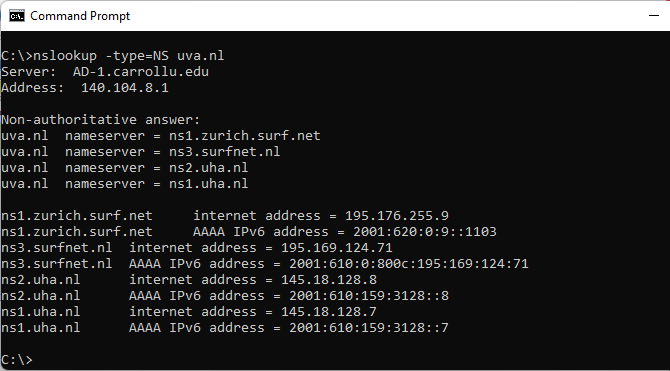
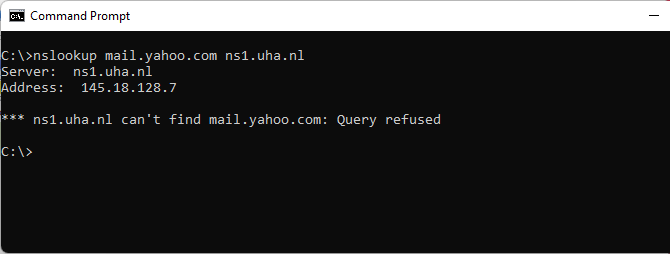
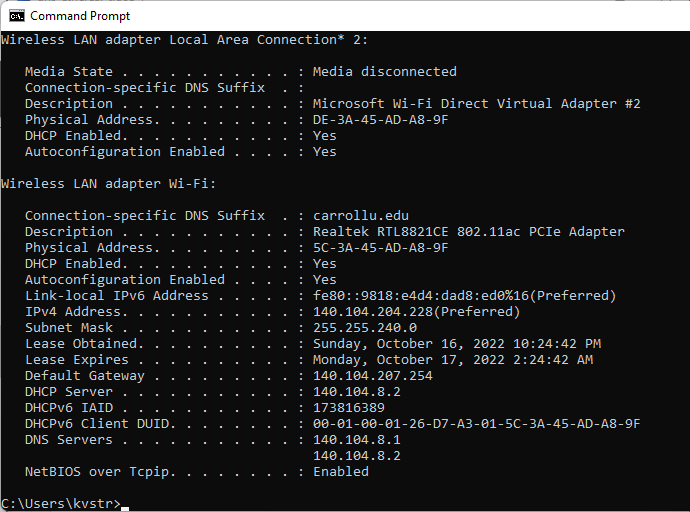
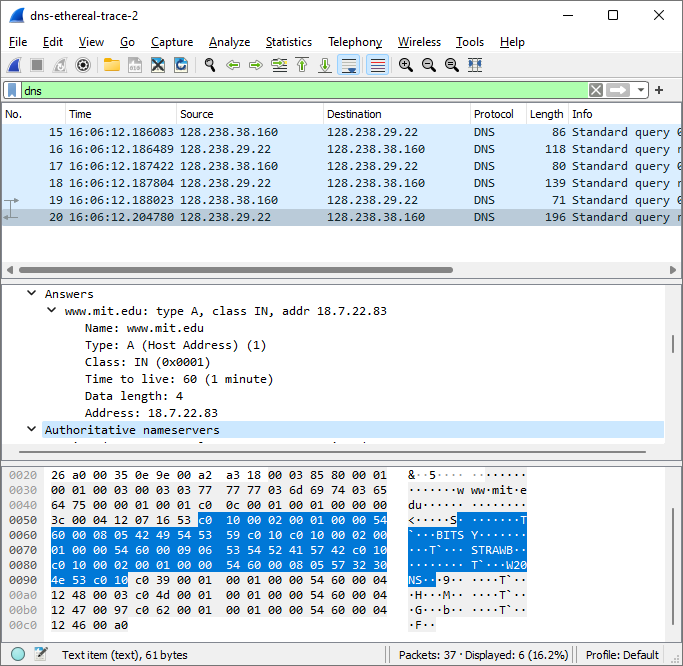
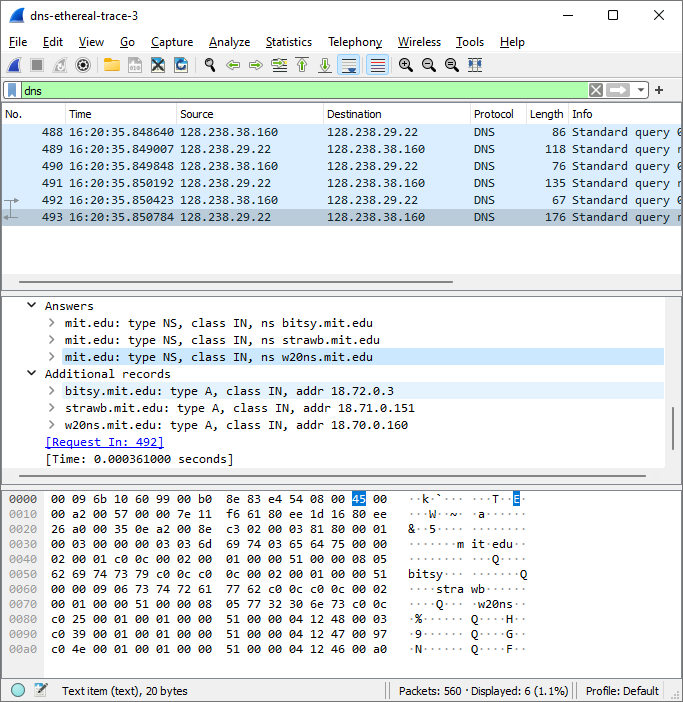
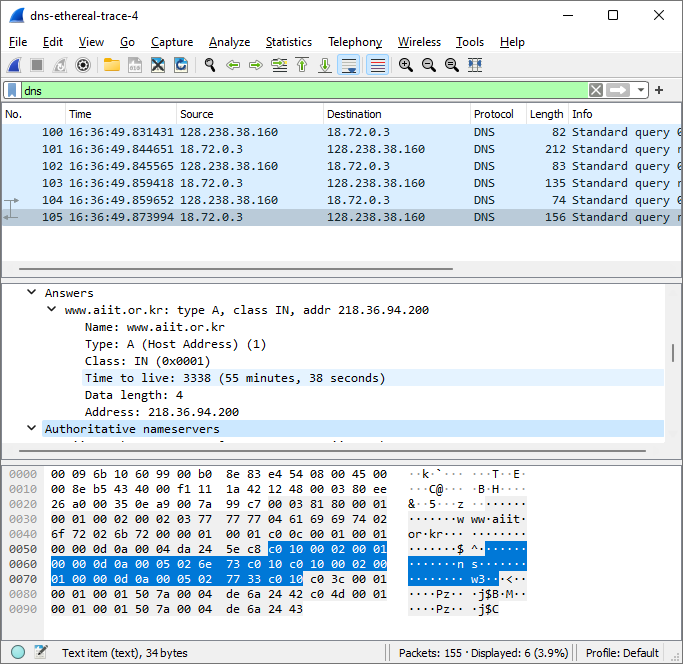
1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?
   1. I performed a looked of a site called [www.devolopment.asia](http://www.devolopment.asia) and the IP address is 54.251.50.43 Graphical user interface, text, application

      Description automatically generated
2. Run nslookup to determine the authoritative DNS servers for a university in Europe
   1. I ran an nslookup for the university of amsterdam 
3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?
   1. I got a query refused error on all DNS servers I looked at for the university of Amsterdam 
4. Locate the DNS query and response messages. Are then sent over UDP or TCP?
   1. They are sent over UDP
5. What is the destination port for the DNS query message? What is the source port of DNS response message?
   1. The destination port of the query is 53, The source port of the response message is also 53
6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?
   1. The message is sent to 128.238.29.23(via the trace). My local DNS server is 140.104.8.1
7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
   1. It is a standard query and it does not contain any answers.
8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?
   1. The response message provides two answers, and they both contain information about the host.
9. 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?
   1. Yes the destination IP address is the first IP provided in the DNS response message
10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?
    1. No it does not
11. What is the destination port for the DNS query message? What is the source port of DNS response message?
    1. The destination port for the query is 53 and the source port for the response is 53.
12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
    1. It is sent to 128.238.29.22, which is not the same as MY DNS server since I am using an ethereal trace.
13. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
    1. It is query type A and it does not provide any answers.
14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?
    1. There is one answer and it contains information about the host name, type, and IP address
15. Provide a screenshot.
    1. 
16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
    1. It is sent to 128.238.29.22, which is not the same as MY DNS server since I am using an ethereal trace.
17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
    1. This query is a NS query and does not contain any messages
18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT nameservers?
    1. The nameservers provided are bitsy, strawb, and w20ns. The response message does provide the IP addresses of the nameservers under additional information
19. Provide a screenshot
    1. 
20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?
    1. The query is sent to 18.72.0.3, which corresponds to the IP address for bitsy.mit.edu
21. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
    1. It is a type A standard and it does not contain any answers
22. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?
    1. It contains one answer it the answer contains the host name, type. Class and IP.
23. Provide a screenshot
    1. 

**Trace 1**

C :\Users\kv str\Downloads\dns-ethereal-trace-1 92 total packets, 2 shown No. Time Source Destination Protocol Length Info 8 16:57:43.582042 128.238.38.160 128.238.29.23 DNS 72 Standard query 0x006e A www.ietf.org Frame 8: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) Ethernet II, Src: IBM\_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers\_00 (00:00:0c:07:ac:00) Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.23 User Datagram Protocol, Src Port: 3163, Dst Port: 53 Source Port: 3163 Destination Port: 53 Length: 38 Checksum: 0x8acb [unverified] [Checksum Status: Unverified] [Stream index: 1] [Timestamps] UDP payload (30 bytes) Domain Name System (query) Transaction ID: 0x006e Flags: 0x0100 Standard query Questions: 1 Answer RRs: 0 Authority RRs: 0 Additional RRs: 0 Queries [Response In: 9] No. Time Source Destination Protocol Length Info 9 16:57:43.582886 128.238.29.23 128.238.38.160 DNS 104 Standard query response 0x006e A www.ietf.org A 132.151.6.75 A 65.246.255.51 Frame 9: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) Ethernet II, Src: Cisco\_83:e4:54 (00:b0:8e:83:e4:54), Dst: IBM\_10:60:99 (00:09:6b:10:60:99) Internet Protocol Version 4, Src: 128.238.29.23, Dst: 128.238.38.160 User Datagram Protocol, Src Port: 53, Dst Port: 3163 Source Port: 53 Destination Port: 3163 Length: 70 Checksum: 0xb0ba [unverified] [Checksum Status: Unverified] [Stream index: 1] [Timestamps] UDP payload (62 bytes) Domain Name System (response) Transaction ID: 0x006e Flags: 0x8180 Standard query response, No error Questions: 1 Answer RRs: 2 Authority RRs: 0 Additional RRs: 0 Queries Answers www.ietf.org: type A, class IN, addr 132.151.6.75 Name: www.ietf.org Type: A (Host Address) (1) 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 (Host Address) (1) 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]

**Trace 2**

C :\Users\kv str\Downloads\dns-ethereal-trace-2 37 total packets, 6 shown No. Time Source Destination Protocol Length Info 19 16:06:12.188023 128.238.38.160 128.238.29.22 DNS 71 Standard query 0x0003 A www.mit.edu Frame 19: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) Ethernet II, Src: IBM\_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers\_00 (00:00:0c:07:ac:00) Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.22 User Datagram Protocol, Src Port: 3742, Dst Port: 53 Source Port: 3742 Destination Port: 53 Length: 37 Checksum: 0x5890 [unverified] [Checksum Status: Unverified] [Stream index: 3] [Timestamps] UDP payload (29 bytes) Domain Name System (query) Transaction ID: 0x0003 Flags: 0x0100 Standard query Questions: 1 Answer RRs: 0 Authority RRs: 0 Additional RRs: 0 Queries [Response In: 20] No. Time Source Destination Protocol Length Info 20 16:06:12.204780 128.238.29.22 128.238.38.160 DNS 196 Standard query response 0x0003 A www.mit.edu A 18.7.22.83 NS BITSY.mit.edu NS STRAWB.mit.edu NS W20NS.mit.edu A 18.72.0.3 A 18.71.0.151 A 18.70.0.160 Frame 20: 196 bytes on wire (1568 bits), 196 bytes captured (1568 bits) Ethernet II, Src: Cisco\_83:e4:54 (00:b0:8e:83:e4:54), Dst: IBM\_10:60:99 (00:09:6b:10:60:99) Internet Protocol Version 4, Src: 128.238.29.22, Dst: 128.238.38.160 User Datagram Protocol, Src Port: 53, Dst Port: 3742 Source Port: 53 Destination Port: 3742 Length: 162 Checksum: 0xa318 [unverified] [Checksum Status: Unverified] [Stream index: 3] [Timestamps] UDP payload (154 bytes) Domain Name System (response) Transaction ID: 0x0003 Flags: 0x8580 Standard query response, No error Questions: 1 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 (Host Address) (1) Class: IN (0x0001) Time to live: 60 (1 minute) Data length: 4 Address: 18.7.22.83 Authoritative nameservers mit.edu: type NS, class IN, ns BITSY.mit.edu Name: mit.edu Type: NS (authoritative Name Server) (2) Class: IN (0x0001) Time to live: 21600 (6 hours) Data length: 8 Name Server: BITSY.mit.edu mit.edu: type NS, class IN, ns STRAWB.mit.edu Name: mit.edu Type: NS (authoritative Name Server) (2) Class: IN (0x0001) Time to live: 21600 (6 hours) Data length: 9 Name Server: STRAWB.mit.edu mit.edu: type NS, class IN, ns W20NS.mit.edu Name: mit.edu Type: NS (authoritative Name Server) (2) Class: IN (0x0001) Time to live: 21600 (6 hours) Data length: 8 Name Server: W20NS.mit.edu Additional records BITSY.mit.edu: type A, class IN, addr 18.72.0.3 Name: BITSY.mit.edu Type: A (Host Address) (1) C :\Users\kv str\Downloads\dns-ethereal-trace-2 37 total packets, 6 shown Class: IN (0x0001) Time to live: 21600 (6 hours) Data length: 4 Address: 18.72.0.3 STRAWB.mit.edu: type A, class IN, addr 18.71.0.151 Name: STRAWB.mit.edu Type: A (Host Address) (1) Class: IN (0x0001) Time to live: 21600 (6 hours) Data length: 4 Address: 18.71.0.151 W20NS.mit.edu: type A, class IN, addr 18.70.0.160 Name: W20NS.mit.edu Type: A (Host Address) (1) Class: IN (0x0001) Time to live: 21600 (6 hours) Data length: 4 Address: 18.70.0.160 [Request In: 19] [Time: 0.016757000 seconds]

**Trace 3**

C :\Users\kv str\Downloads\dns-ethereal-trace-3 560 total packets, 6 shown No. Time Source Destination Protocol Length Info 492 16:20:35.850423 128.238.38.160 128.238.29.22 DNS 67 Standard query 0x0003 NS mit.edu Frame 492: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) Ethernet II, Src: IBM\_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers\_00 (00:00:0c:07:ac:00) Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.22 User Datagram Protocol, Src Port: 3746, Dst Port: 53 Source Port: 3746 Destination Port: 53 Length: 33 Checksum: 0xd282 [unverified] [Checksum Status: Unverified] [Stream index: 15] [Timestamps] UDP payload (25 bytes) Domain Name System (query) Transaction ID: 0x0003 Flags: 0x0100 Standard query Questions: 1 Answer RRs: 0 Authority RRs: 0 Additional RRs: 0 Queries mit.edu: type NS, class IN [Response In: 493] No. Time Source Destination Protocol Length Info 493 16:20:35.850784 128.238.29.22 128.238.38.160 DNS 176 Standard query response 0x0003 NS mit.edu NS bitsy.mit.edu NS strawb.mit.edu NS w20ns.mit.edu A 18.72.0.3 A 18.71.0.151 A 18.70.0.160 Frame 493: 176 bytes on wire (1408 bits), 176 bytes captured (1408 bits) Ethernet II, Src: Cisco\_83:e4:54 (00:b0:8e:83:e4:54), Dst: IBM\_10:60:99 (00:09:6b:10:60:99) Internet Protocol Version 4, Src: 128.238.29.22, Dst: 128.238.38.160 User Datagram Protocol, Src Port: 53, Dst Port: 3746 Source Port: 53 Destination Port: 3746 Length: 142 Checksum: 0xc302 [unverified] [Checksum Status: Unverified] [Stream index: 15] [Timestamps] UDP payload (134 bytes) Domain Name System (response) Transaction ID: 0x0003 Flags: 0x8180 Standard query response, No error Questions: 1 Answer RRs: 3 Authority RRs: 0 Additional RRs: 3 Queries mit.edu: type NS, class IN Answers mit.edu: type NS, class IN, ns bitsy.mit.edu mit.edu: type NS, class IN, ns strawb.mit.edu mit.edu: type NS, class IN, ns w20ns.mit.edu Additional records bitsy.mit.edu: type A, class IN, addr 18.72.0.3 strawb.mit.edu: type A, class IN, addr 18.71.0.151 w20ns.mit.edu: type A, class IN, addr 18.70.0.160 [Request In: 492] [Time: 0.000361000 seconds]

**Trace 4**

C :\Users\kv str\Downloads\dns-ethereal-trace-4 155 total packets, 6 shown No. Time Source Destination Protocol Length Info 104 16:36:49.859652 128.238.38.160 18.72.0.3 DNS 74 Standard query 0x0003 A www.aiit.or.kr Frame 104: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) Ethernet II, Src: IBM\_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers\_00 (00:00:0c:07:ac:00) Internet Protocol Version 4, Src: 128.238.38.160, Dst: 18.72.0.3 User Datagram Protocol, Src Port: 3753, Dst Port: 53 Source Port: 3753 Destination Port: 53 Length: 40 Checksum: 0xf547 [unverified] [Checksum Status: Unverified] [Stream index: 6] [Timestamps] UDP payload (32 bytes) Domain Name System (query) Transaction ID: 0x0003 Flags: 0x0100 Standard query Questions: 1 Answer RRs: 0 Authority RRs: 0 Additional RRs: 0 Queries www.aiit.or.kr: type A, class IN [Response In: 105] No. Time Source Destination Protocol Length Info 105 16:36:49.873994 18.72.0.3 128.238.38.160 DNS 156 Standard query response 0x0003 A www.aiit.or.kr A 218.36.94.200 NS ns.aiit.or.kr NS w3.aiit.or.kr A 222.106.36.66 A 222.106.36.67 Frame 105: 156 bytes on wire (1248 bits), 156 bytes captured (1248 bits) Ethernet II, Src: Cisco\_83:e4:54 (00:b0:8e:83:e4:54), Dst: IBM\_10:60:99 (00:09:6b:10:60:99) Internet Protocol Version 4, Src: 18.72.0.3, Dst: 128.238.38.160 User Datagram Protocol, Src Port: 53, Dst Port: 3753 Source Port: 53 Destination Port: 3753 Length: 122 Checksum: 0x99c7 [unverified] [Checksum Status: Unverified] [Stream index: 6] [Timestamps] UDP payload (114 bytes) Domain Name System (response) Transaction ID: 0x0003 Flags: 0x8180 Standard query response, No error Questions: 1 Answer RRs: 1 Authority RRs: 2 Additional RRs: 2 Queries www.aiit.or.kr: type A, class IN Answers www.aiit.or.kr: type A, class IN, addr 218.36.94.200 Name: www.aiit.or.kr Type: A (Host Address) (1) Class: IN (0x0001) Time to live: 3338 (55 minutes, 38 seconds) Data length: 4 Address: 218.36.94.200 Authoritative nameservers aiit.or.kr: type NS, class IN, ns ns.aiit.or.kr Name: aiit.or.kr Type: NS (authoritative Name Server) (2) Class: IN (0x0001) Time to live: 3338 (55 minutes, 38 seconds) Data length: 5 Name Server: ns.aiit.or.kr aiit.or.kr: type NS, class IN, ns w3.aiit.or.kr Name: aiit.or.kr Type: NS (authoritative Name Server) (2) Class: IN (0x0001) Time to live: 3338 (55 minutes, 38 seconds) Data length: 5 Name Server: w3.aiit.or.kr Additional records ns.aiit.or.kr: type A, class IN, addr 222.106.36.66 Name: ns.aiit.or.kr Type: A (Host Address) (1) Class: IN (0x0001) Time to live: 86138 (23 hours, 55 minutes, 38 seconds) Data length: 4 Address: 222.106.36.66 w3.aiit.or.kr: type A, class IN, addr 222.106.36.67 C :\Users\kv str\Downloads\dns-ethereal-trace-4 155 total packets, 6 shown Name: w3.aiit.or.kr Type: A (Host Address) (1) Class: IN (0x0001) Time to live: 86138 (23 hours, 55 minutes, 38 seconds) Data length: 4 Address: 222.106.36.67 [Request In: 104] [Time: 0.014342000 seconds]