

1. Run *nslookup* to obtain the IP address of a Web server in Asia. What is its IP address? *ANSWER: I performed nslookup for www.rediff.com. Its IP address is 208.184.138.70* 

C:\Docum	ents and Settings>nslookup	www.rediff.com
Server:	dns-prime.poly.edu	
Address:	128.238.29.22	
Name:	www.rediff.com	
Address:	208.184.138.70	

Screenshot taken for question 1

2. Run *nslookup* to determine the authoritative DNS servers for a university in Europe. What is its IP address. *ANSWER*: I performed nslookup for a European University in Ioannina Greece. Its IP address is 128.238.29.22

C:\Documents and Setting	s\andromahe>cd
C:\Documents and Setting Server: dns-prime.poly. Address: 128.238.29.22	∣s>nslookup -type=NS uoi.gr edu
Non-authoritative answer uoi.gr nameserver = kou uoi.gr nameserver = mar uoi.gr nameserver = min	: Izina.noc.uoi.gr Tina.noc.uoi.gr
kouzina.noc.uoi.gr marina.noc.uoi.gr nic.grnet.gr internet	internet address = 195.130.120.110 internet address = 195.130.120.120 address = 194.177.210.210
C:\Documents and Setting	6>

Screenshot taken for question 2

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? *ANSWER:* the IP address of the mail server(s) is 18.72.0.3.

C:\Documents and Settings>nslookup mail.yahoo.com bitsy.mit.edu Server: BITSY.MIT.EDU Address: 18.72.0.3 Non-authoritative answer:

Name: login.yahoo.akadns.net Address: 216.109.127.60 Aliases: mail.yahoo.com, login.yahoo.com

C:\Documents and Settings>

Screenshot taken for question 3

PART 3a



Screenshot for DNS query

Screenshot for DNS response

4. Locate the DNS query and response messages. Are then sent over UDP or TCP? *ANSWER: 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? *ANSWER:* The destination port for the DNS query is 53 and the source port of the DNS response is 53.

C:\WINDOWS\s	system32\cmd.exe	
C:\Documents	and Settings∖Paula Wing≻ipconfig —all	-
Windows IP Co	onfiguration	
Host Prima Node IP Ro WINS DNS S	Name : wingamajig ry Dns Suffix : Type : Unknown uting Enabled : No Suffix Search List : nyhome.westell.com	
Ethernet adap	pter UMware Network Adapter UMnet8:	
Conne Desci IlMnet 8	ection-specific DNS Suffix .: •iption : UMware Virtual Ethernet Adapter :	for
Physi	ical Address 00-50-56-C0-00-08	
IP Ad Subne Defau	Enabled	
Ethernet adap	pter UMware Network Adapter UMnet1:	
Conne Desci UMpet1	ction-specific DNS Suffix .: •iption : UMware Virtual Ethernet Adapter :	for
Physi Dhop IP Ad Subne Defau	ical Address : 00-50-56-C0-00-01 Enabled No Molecs	
Ethernet adap	oter Local Area Connection 4:	
Conne Desci Physi Dhop Autor IP Ac Subne Defat DHCP DNS 5 Lease	sction-specific DNS Suffix       : myhome.vestell.com         ription       : NETGEAR GA3021 Gigabit Adapter         cal Address       : 00-09-28-61-8E-6D         Enabled       : Yes         onfiguration Enabled       : Yes         ldress       : 122.168.1.46         Gateway       : 252.255.255.0         ld Gateway       : 192.168.1.1         Server       : 192.166.1.1         levers       : 192.168.1.1         ervers       : 192.168.1.1         ervers <td: 192.168.1.1<="" td="">         ervers       <td: 192.168.1.1<="" td="">         ervers       <td: 192.168.1.1<="" td="">         ervers       : 192.168.1.1         ervers       <td: server<="" td="">         scrupt       : Furday, June 07. 2007 8:49:54 AM</td:></td:></td:></td:>	AM
C:\Documents	and Settings\Paula Wing>	-

*Screenshot for ipconfig –all* 

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? *ANSWER:* It's sent to 192.168.1.1, which is the IP address of one of my local DNS servers.

7. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"? *ANSWER:* It's a type A Standard Query and it doesn't contain any answers.

8. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain? *ANSWER:* There were 2 answers containing information about the name of the host, the type of address, class, the TTL, the data length and the IP address.

```
Answers
www.ietf.org: type A, class IN, addr 209.173.57.180
   Name:
  www.ietf.org
   Type: A (Host
   address) Class:
   IN (0x0001)
   Time to live: 30 minutes
   Data length: 4
  Addr: 209.173.57.180
www.ietf.org: type A, class IN, addr 209.173.53.180
  Name:
   www.ietf.org
   Type: A (Host
   address) Class:
   IN (0x0001)
   Time to live: 30 minutes
   Data length: 4
   Addr: 209.173.53.180
```

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? *ANSWER:* The first SYN packet was sent to 209.173.57.180 which corresponds to the first IP address provided in the DNS response message.

10. This web page contains images. Before retrieving each image, does your host issue new DNS queries? *ANSWER:* No

PART 3b

💽 (Unitiled) - Wireshark	😰 (Untitled) - Wireshark
Ble Edit View Go Capture Analyze Statistics Help	Ble Edit Yew Go Capture Analyze Statistics Beb
	■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■
Elter: [p. addr == 192.168.2.145 Topression Gen groly	Efter: [ip.addr == 192.168.2.145 * Expression Gear Apply
No Time Source Destination Protocol Info	No Time Source Destination Protocol Info
1 0.000000 192.168.2.145 192.168.1.1 DMS Standard query PTR 1.1.168.192.1n-addr.ar	10.000000 192.168.2.145 192.168.1.1 DNS Standard guery PTR 1.1.158.192.1n-addr.an
3 0.013838 192.166.2.145 192.166.1.1 DNS Standard query A www.mit.edu.wyhome.weste	3 0.01338 192.168.2.145 192.168.1.1 DNS Standard guery response Pite dus house
4 0.074934 192.108.1.1 192.108.2.145 DNS Standard guery response 5 0.084593 192.168.2.145 192.168.1.1 DNS Standard guery A www.mit.edu	4 0.074954 192.168.1.1 192.168.2.145 DNS Standard query response 5.084591 192.168.2.145 192.168.1.1 DNS Standard query A www.mit.edu
6 0.140633 192.168.1.1 192.168.2.145 DNS Standard query response A 18.7.22.83	6 0.140633 192.168.1.1 192.168.2.145 DNS Standard query response A 18.7.22.83
<pre>me destination: Lifesysid_A190:a8 (00:00:41:45:90:a8) # Storre: Mergan_GilseR6 (00:00:95:55:61:86:16) * Flags: 00:80 (Stundard query response, No error) # Wexer Res: 0 Additional Res: 0 # Flags: 00:80 (Stundard query response, No error) # Wexer Res: 0 Additional Res: 0 # Additional Res: 0 # Additional Res: 0 # Harder Res: 0 # Wexer Res: 0 Additional Res: 0 # Harder Res: 0 # Hard</pre>	
20000 00 0C 41 45 90 38 00 09 50 61 8e 6d 08 00 45 00	Image: 1         Image: 1
Pie: "C:[DOCUME-r1]PALAW-r1[LOCALS-r1]TempletherX000a01796" 713 8ytes 00:001 P: 6 D: 6 M: 0 Drops: 0	Pier "C:(DOCUME~1)PALLAW~1(LOCALS~1)Templether/2003/01796" 713 8ytes 00:0. P: 6 D: 6 M: 0 Drops: 0

Screenshot for DNS query

Screenshot for DNS response

11. What is the destination port for the DNS query message? What is the source port of DNS response message? *ANSWER:* The destination port of the DNS query is 53 and the source port of the DNS 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? *ANSWER:* It's sent to 192.168.1.1 which as we can see from the ipconfig –all screenshot, is the default local DNS server.

13. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"? *ANSWER*: *The query is of type A and it doesn't contain any answers*.

14. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain? *ANSWER:* The response DNS message contains one answer containing the name of the host, the type of address, the class, and the IP address.

```
Answers

www.mit.edu: type A, class IN, addr 18.7.22.83

Name: www.mit.edu

Type: A (Host

address) Class:

IN (0x0001)

Time to live: 1 minute

Data length: 4

Addr: 18.7.22.83
```

15. Provide a screenshot.

## PART 3c

📶 dns-ethereal-trace-3 - Wireshark	
Eile Edit View Go Capture Analyze Statistics E	<u>t</u> elp
u u u u u u u u u	% △ Q ♀ ♀ ∞ ⊼ 쏘 🗐 📑 Q ♀ Q 🖸
Eilter: jip.addr == 128.238.38.160	▼ Expression ⊆lear Apply
No Time Source	Destination Protocol Info
488 30.916492 128.238.38.160	128.238.29.22 DNS Standard query PTR 22.29.238.128.in-addr.
489 30.916859 128.238.29.22	128.238.38.160 DNS Standard query response PIR dns-prime.pol
491 30.918044 128.238.29.22	128.238.38.160 DNS Standard query response, No such name
492 30.918275 128.238.38.160	128.238.29.22 DNS Standard query NS mit.edu
493 30.918636 128.238.29.22	128.238.38.160 DNS Standard query response NS bitsy.mit.edu
4	P
Authority RRs: 0	
Additional RRs: 3	
🖂 Queries	
🗆 mit.edu: type NS, class IN	
Name: mit.edu	
Type: NS (Authoritative name	server)
Class: IN (UXUUUI)	
□ mit edu: type NS class IN ps	hitsy mit edu
Name: mit.edu	sitsy.mit.edu
Type: NS (Authoritative name	serverl
Class: IN (0x0001)	
Time to live: 5 hours, 45 mir	nutes, 36 seconds
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)
Class: IN (0x0001)	
0000 00 09 6b 10 60 99 00 b0 8e 83	е4 54 08 00 45 00k.` тЕ.
0010 00 a2 00 57 00 00 7e 11 f6 61 3	80 ee 1d 16 80 eeW~a
0030 00 03 00 00 00 03 03 6d 69 74	03 65 64 75 00 00m it.edu
	00 51 00 00 08 05Q
File: "C:\Documents and Settings\Paula Wing\My Documents\\	Wireshark\traces - ethere P: 560 D: 6 M: 0

Screenshot for DNS response

16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? *ANSWER:* It was sent to 128.238.29.22 which is my default DNS server.

17. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"? *ANSWER:* It's a type NS DNS query that doesn't contain any answers.

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? *ANSWER:* The nameservers are bitsy, strawb and w20ns. We can find their IP addresses if we expand the Additional records field in Wireshark as seen below.

Answers mit.edu: type NS, class inet, ns bitsy.mit.edu mit.edu: type NS, class inet, ns strawb.mit.edu mit.edu: type NS, class inet, ns w20ns.mit.edu Additional records bitsy.mit.edu: type A, class inet, addr 18.72.0.3 strawb.mit.edu: type A, class inet, addr 18.71.0.151 w20ns.mit.edu: type A, class inet, addr 18.70.0.160

19. Provide a screenshot.

## PART 3d

🖊 (Untitled) - Wireshark					
Eile Edit View <u>G</u> o <u>C</u> apture Analyze <u>S</u> tatistics <u>H</u> elp					
Elter: jp.addr == 192.168.2.145					
No Time Source Destination Protocol Info					
3 0.000348 192.168.2.145 192.168.1.1 DNS Standard query A bitsy.mit.edu					
4 0.041424 192.168.1.1 192.168.2.145 DNS Standard query response A 18.72.0.3 5 0.053028 192.168.2.145 18 72.0.3 DNS Standard query PT 3.0.72.18 in-addr arna					
6 0.103413 18.72.0.3 192.168.2.145 DNS Standard query resonse PTR BITSY.MIT.EDU					
7 0.112180 192.168.2.145 18.72.0.3 DNS Standard query A www.aiit.or.kr.myhome.we					
8 0.1/1300 18.72.0.3 192.108.2.145 DNS Standard guery response 9 0.174800 192.168.2.145 18.72.0.3 DNS Standard guery a www.aiit on kr					
10 0.527466 18.72.0.3 197.168.2.145 DNS Standard query response A 222.106.36.102					
Ethernat II. Spc. Linksver 45:00:38 (00:0-:41:45:00:38) . Det. Natmaar 61:80:64 (00:00:5h:61:80:64)					
Therefore Protocol. Src. 18.72.0.3 (18.72.0.3). DSt: 192.168.2.145 (192.168.2.145)					
Hise Datagram Protocol. Src Port: domain (53). DSt Port: 16071 (1607)					
Domain Name System (response)					
[Request In: 9]					
[Time: 0.352576000 seconds]					
Transaction ID: 0x0003					
B Flags: 0x8180 (Standard query response, No error)					
Questions: 1					
Answer RRs: 1					
Authority RRs: 2					
Adattional RRS: 2					
Discover addition knot type A class IN					
□ www.aitt.or.kr: type A, class IN					
Type: A (Host address)					
Class: IN (0x0001)					
Answers					
⊞ www.aiit.or.kr: type A, class IN, addr 222.106.36.102					
Authoritative nameservers					
⊞ aiit.or.kr: type NS, class IN, ns w3.aiit.or.kr					
🗉 aiit.or.kr: type NS, class IN, ns ns.aiit.or.kr					
⊟ Additional records					
⊞ ws.anit.or.kr: type A, Class IN, addr 222.106.36.67					
⊞ HS.airt.ur.kr: type A, Class IN, auur 222.100.30.00					
0040 67 72 02 66 72 00 00 01 00 01 00 77 77 77 04 61 or.kr www.a					
0060 0 0 10 00 04 de 6a 24 66 c0 24 00 02 00 01 00 00					
0070 0 <u>e 10 00 05 02 77 33 C0</u> 24 c0 24 00 02 00 01 00 <u>w3</u> <b>\$.\$</b>					
P: 10 D: 8 M: 0 Drops: 0					

Screenshot for DNS response

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? *ANSWER: The query is sent to 18.72.0.3 which corresponds to bitsy.mit.edu.* 

21. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"? *ANSWER* It's a standard type A query that doesn't contain any answers.

22. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain? *ANSWER:* One answer is provided in the DNS response message. It contains the following:

Answers

```
www.aiit.or.kr: type A, class inet, addr 222.106.36.102
Name: www.aiit.or.kr
Type: Host address
Class: inet
Time to live: 1 hour
Data length: 4
Addr: 222.106.36.102
```

23. Provide a screenshot.