



OCTOBER 13, 2015

## LAB 2

### EE 450 SESSION 3

TUSHAR TIWARI

Q1. It is 163.53.78.58

```
C:\Users\therelaxist>nslookup www.flipkart.com
Server: dns-cac-lb-01.rr.com
Address: 209.18.47.61

Non-authoritative answer:
Name: flipkart.com
Addresses: 2001:df0:23e:9002::15
[163.53.78.58]
Aliases: www.flipkart.com
```

Q2. I chose oxford university. The authoritative DNS servers are encircled.

```
C:\Users\therelaxist>nslookup -type=NS ox.ac.uk
Server: dns-cac-lb-01.rr.com
Address: 209.18.47.61

Non-authoritative answer:
ox.ac.uk      nameserver = dns2.ox.ac.uk
ox.ac.uk      nameserver = dns1.ox.ac.uk
ox.ac.uk      nameserver = dns0.ox.ac.uk
ox.ac.uk      nameserver = ns2.ja.net
```

Q3. 98.136.189.41. The DNS server I chose is ns2.ja.net but that refused my query. So I chose Google's DNS Server (8.8.8.8)

```
C:\Users\therelaxist>nslookup mail.yahoo.com ns2.ja.net
0.0.0.0.0.3.6.0.1.0.0.2.ip6.arpa      nameserver = ns0.ja.net
0.0.0.0.0.3.6.0.1.0.0.2.ip6.arpa      nameserver = ns4.ja.net
ns0.ja.net      internet address = 128.86.1.20
ns0.ja.net      internet address = 193.63.94.20
ns0.ja.net      AAAA IPv6 address = 2001:630:0:8::14
ns0.ja.net      AAAA IPv6 address = 2001:630:0:9::14
ns4.ja.net      internet address = 193.62.157.66
ns4.ja.net      AAAA IPv6 address = 2001:630:0:47::42
Server: UnKnown
Address: 2001:630:0:45::11

*** [UnKnown can't find mail.yahoo.com: Query refused]

C:\Users\therelaxist>nslookup mail.yahoo.com 8.8.8.8
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
Name: fo-ds-ats.member.g02.yahoodns.net
Addresses: 2001:4998:c:e33::50
[98.136.189.41]
Aliases: mail.yahoo.com
          login.yahoo.com
```

Q4. They are sent over UDP.

Q5. Destination Port is 53. Source Port is also 53.

Q6. The IP address is 209.18.47.62

Q7. It is of type A. Contains no answers.

Q8. 1 answer is provided. It contains the hostname, type, class, TTL, data length and the ipv4 address itself.

Q9. Yes, it is the ip address provided in the answer.

Q10. No.

## The DNS Query

No.	Time	Source	Destination	Protocol	Length	Info
7	1.11486500	104.27.175.166	192.168.0.5	TCP	56	80-58540 [ACK] Seq=1 Ack=2 Win=30 Len=0
8	1.20528500	104.131.12.233	192.168.0.5	TCP	56	80-58501 [ACK] Seq=1 Ack=2 Win=136 Len=0
10	4.55040500	192.168.0.5	209.18.47.61	DNS	68	Standard query 0xae46 A ietf.org
11	4.55053900	192.168.0.5	209.18.47.61	DNS	68	Standard query 0x6b9f AAAA ietf.org
12	4.56910400	192.168.0.5	209.18.47.62	DNS	68	Standard query 0x6b9f AAAA ietf.org
13	4.56910400	192.168.0.5	209.18.47.62	DNS	68	Standard query 0xae46 A ietf.org
14	4.59238400	209.18.47.62	192.168.0.5	DNS	96	Standard query response 0x6b9f AAAA 2001:1900:3001:11::2c

Frame 10: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0  
Ethernet II, Src: Apple\_bc:31:4b (a4:5e:60:bc:31:4b), Dst: ArrisGro\_e4:c4:27 (08:3e:0c:e4:c4:27)  
Internet Protocol Version 4, Src: 192.168.0.5 (192.168.0.5), Dst: 209.18.47.61 (209.18.47.61)  
User Datagram Protocol, Src Port: 64626 (64626), Dst Port: 53 (53)  
Domain Name System (query)  
[\[Response In: 26\]](#)  
Transaction ID: 0xae46  
Flags: 0x0100 Standard query  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries  
ietf.org: type A, class IN  
Name: ietf.org  
[Name Length: 8]  
[Label Count: 2]  
Type: A (Host Address) (1)  
Class: IN (0x0001)

## The DNS Response

No.	Time	Source	Destination	Protocol	Length	Info
13	4.56910400	192.168.0.5	209.18.47.62	DNS	68	Standard query 0xae46 A ietf.org
14	4.59238400	209.18.47.62	192.168.0.5	DNS	96	Standard query response 0x6b9f AAAA 2001:1900:3001:11::2c
15	4.59475800	209.18.47.62	192.168.0.5	DNS	84	Standard query response 0xae46 A 4.31.198.44
26	4.64077600	209.18.47.61	192.168.0.5	DNS	84	Standard query response 0xae46 A 4.31.198.44
27	4.64077600	209.18.47.61	192.168.0.5	DNS	86	Standard query response 0xae46 AAAA 2001:1900:3001:11::2c

Frame 15: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0  
Ethernet II, Src: ArrisGro\_e4:c4:27 (08:3e:0c:e4:c4:27), Dst: Apple\_bc:31:4b (a4:5e:60:bc:31:4b)  
Internet Protocol Version 4, Src: 209.18.47.62 (209.18.47.62), Dst: 192.168.0.5 (192.168.0.5)  
User Datagram Protocol, Src Port: 53 (53), Dst Port: 64626 (64626)  
Domain Name System (response)  
[\[Request In: 13\]](#)  
[Time: 0.025654000 seconds]  
Transaction ID: 0xae46  
Flags: 0x8180 Standard query response, No error  
Questions: 1  
Answer RRs: 1  
Authority RRs: 0  
Additional RRs: 0  
Queries  
Answers  
ietf.org: type A, class IN, addr 4.31.198.44  
Name: ietf.org  
Type: A (Host Address) (1)  
Class: IN (0x0001)  
Time to live: 1800  
Data length: 4  
Address: 4.31.198.44 (4.31.198.44)

ipconfig /all - This shows the default DNS server provided by DHCP.

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

#### Windows IP Configuration

```
Host Name . . . . . : DESKTOP-E28R8JI
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
```

#### Wireless LAN adapter Local Area Connection\* 3:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . : A6-5E-60-BC-31-4B
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
```

#### Wireless LAN adapter Wi-Fi:

```
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Broadcom 802.11ac Network Adapter
Physical Address. . . . . : A4-5E-60-BC-31-4B
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IPv6 Address. . . . . : 2605:e000:4e01:fa00:f9af:3b31:1bd2:6415(Preferred)
Temporary IPv6 Address. . . . . : 2605:e000:4e01:fa00:88c4:88d:cc45:282a(Preferred)
Link-local IPv6 Address . . . . . : fe80::f9af:3b31:1bd2:6415%7(Preferred)
IPv4 Address. . . . . : 192.168.0.5(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, October 12, 2015 12:47:17 AM
Lease Expires . . . . . : Monday, October 12, 2015 10:47:17 AM
Default Gateway . . . . . : fe80::a3e:cff:fee4:c427%7
                                         192.168.0.1
DHCP Server . . . . . : 192.168.0.1
DHCPv6 IAID . . . . . : 94658144
DHCPv6 Client DUID. . . . . : 00-01-00-01-1D-76-C0-B6-A4-5E-60-BC-31-4B
DNS Servers . . . . . : 209.18.47.61
                                         209.18.47.62
```

Q9. Yes, it contains the ip-address returned in the answers section.

Q10. No

- Q11. Destination Port: 53. Source port: 53.  
 Q12. 209.18.47.61. Yes. (See previous ipconfig /all for default DNS)  
 Q13. Type A. Contains no answers.  
 Q14. Only 1 answer is provided. It contains the hostname, type, class, ttl, data length and address of mit.edu.

## DNS Query

Filter: ip.addr == 192.168.0.5						Expression...	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length	Info			
12	7.716485000	192.168.0.5	209.18.47.61	DNS	85	Standard query	0x0001	PTR	61.47.18.209.in-addr.arpa
13	7.733461000	209.18.47.61	192.168.0.5	DNS	119	Standard query response	0x0001	PTR	dns-cac-lb-01.rr.com
14	7.734633000	192.168.0.5	209.18.47.61	DNS	67	Standard query	0x0002	A	mit.edu
15	7.759088000	209.18.47.61	192.168.0.5	DNS	83	Standard query response	0x0002	A	23.213.96.205

```

Frame 14: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
Ethernet II, Src: Apple_bc:31:4b (a4:5e:60:bc:31:4b), Dst: ArrisGro_e4:c4:27 (08:3e:0c:e4:c4:27)
Internet Protocol Version 4, Src: 192.168.0.5 (192.168.0.5), Dst: 209.18.47.61 (209.18.47.61)
User Datagram Protocol, Src Port: 50678 (50678), Dst Port: 53 (53)
Domain Name System (query)
[Response In: 15]
Transaction ID: 0x0002
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
mit.edu: type A, class IN
  Name: mit.edu
  [Name Length: 7]
  [Label Count: 2]
  Type: A (Host Address) (1)
  Class: IN (0x0001)

```

## DNS Response

Filter: ip.addr == 192.168.0.5						Expression...	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length	Info			
12	7.716485000	192.168.0.5	209.18.47.61	DNS	85	Standard query	0x0001	PTR	61.47.18.209.in-addr.arpa
13	7.733461000	209.18.47.61	192.168.0.5	DNS	119	Standard query response	0x0001	PTR	dns-cac-lb-01.rr.com
14	7.734633000	192.168.0.5	209.18.47.61	DNS	67	Standard query	0x0002	A	mit.edu
15	7.759088000	209.18.47.61	192.168.0.5	DNS	83	Standard query response	0x0002	A	23.213.96.205

```

Frame 15: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0
Ethernet II, Src: ArrisGro_e4:c4:27 (08:3e:0c:e4:c4:27), Dst: Apple_bc:31:4b (a4:5e:60:bc:31:4b)
Internet Protocol Version 4, Src: 209.18.47.61 (209.18.47.61), Dst: 192.168.0.5 (192.168.0.5)
User Datagram Protocol, Src Port: 53 (53), Dst Port: 50678 (50678)
Domain Name System (response)
[Request In: 14]
[Time: 0.024455000 seconds]
Transaction ID: 0x0002
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
Answers
mit.edu: type A, class IN, addr 23.213.96.205
  Name: mit.edu
  Type: A (Host Address) (1)
  Class: IN (0x0001)
  Time to live: 20
  Data length: 4
  Address: 23.213.96.205 (23.213.96.205)

```

Q16. 209.18.47.61. Yes. (See previous ipconfig /all for default DNS)

Q17. Type NS. Contains no answers.

Q19. 8 answers are provided. The name servers are asia1.akam.net, asia2.akam.net, usw2.akam.net, ns1-37.akam.net, use2.akam.net, use5.akam.net, ns1-173.akam.net, eur5.akam.net. No it does not contain the IP addresses.

## DNS Query

Filter: ip.addr == 192.168.0.5

No.	Time	Source	Destination	Protocol	Length	Info
5	2.460107000	192.168.0.5	209.18.47.61	DNS	85	Standard query 0x0001 PTR 61.47.18.209.in-addr.arpa
6	2.496428000	209.18.47.61	192.168.0.5	DNS	119	Standard query response 0x0001 PTR dns-cac-lb-01.rr.com
7	2.497593000	192.168.0.5	209.18.47.61	DNS	67	Standard query 0x0002 NS mit.edu
8	2.521068000	209.18.47.61	192.168.0.5	DNS	234	Standard query response 0x0002 NS asia1.akam.net NS use2.akam.net

Frame 7: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0

Ethernet II, Src: Apple\_bc:31:4b (a4:5e:60:bc:31:4b), Dst: ArrisGro\_e4:c4:27 (08:3e:0c:e4:c4:27)  
Internet Protocol Version 4, Src: 192.168.0.5 (192.168.0.5), Dst: 209.18.47.61 (209.18.47.61)  
User Datagram Protocol, Src Port: 55180 (55180), Dst Port: 53 (53)  
Domain Name System (query)  
[Response In: 8]  
Transaction ID: 0x0002  
Flags: 0x0100 Standard query  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries  
mit.edu: type NS, class IN  
Name: mit.edu  
[Name Length: 7]  
[Label Count: 2]  
Type: NS (authoritative Name Server) (2)  
Class: IN (0x0001)

## DNS Response

Filter: ip.addr == 192.168.0.5

No.	Time	Source	Destination	Protocol	Length	Info
6	2.496428000	209.18.47.61	192.168.0.5	DNS	119	Standard query response 0x0001 PTR dns-cac-lb-01.rr.com
7	2.497593000	192.168.0.5	209.18.47.61	DNS	67	Standard query 0x0002 NS mit.edu
8	2.521068000	209.18.47.61	192.168.0.5	DNS	234	Standard query response 0x0002 NS asia1.akam.net NS use2.akam.net

[Request At: / ]  
[Time: 0.023475000 seconds]  
Transaction ID: 0x0002  
Flags: 0x8180 Standard query response, No error  
Questions: 1  
Answer RRs: 8  
Authority RRs: 0  
Additional RRs: 0  
Queries  
Answers  
mit.edu: type NS, class IN, ns asia1.akam.net  
Name: mit.edu  
Type: NS (authoritative Name Server) (2)  
Class: IN (0x0001)  
Time to live: 322  
Data length: 16  
Name Server: asia1.akam.net  
mit.edu: type NS, class IN, ns use2.akam.net  
mit.edu: type NS, class IN, ns ns1-173.akam.net  
mit.edu: type NS, class IN, ns ns1-37.akam.net  
mit.edu: type NS, class IN, ns asia2.akam.net  
mit.edu: type NS, class IN, ns use5.akam.net  
mit.edu: type NS, class IN, ns eur5.akam.net  
mit.edu: type NS, class IN, ns usw2.akam.net

Command is **nslookup flipkart.com google-public-dns-a.google.com**. Because neither of the hostnames given in the question work.

Q16. 8.8.8. No. (See previous ipconfig /all for default DNS). It corresponds to google-public-dns-a.google.com.

Q17. Type A. Contains no answers.

Q19. Only 1 answer is provided. It contains the hostname, type, class, ttl, data length and ip address of flipkart.com.

## DNS Query

Filter: ip.addr == 192.168.0.5							Expression...	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length	Info				
2	1.360809000	192.168.0.5	8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.in-addr.arpa				
3	1.415798000	8.8.8	192.168.0.5	DNS	124	Standard query response 0x0001 PTR google-public-dns-a.google.c				
4	1.420490000	192.168.0.5	8.8.8	DNS	72	Standard query 0x0002 A flipkart.com				
5	1.475562000	8.8.8	192.168.0.5	DNS	88	Standard query response 0x0002 A 163.53.78.58				

```

Frame 4: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
Ethernet II, Src: Apple_bc:31:4b (a4:5e:60:bc:31:4b), Dst: ArrisGro_e4:c4:27 (08:3e:0c:e4:c4:27)
Internet Protocol Version 4, Src: 192.168.0.5 (192.168.0.5), Dst: 8.8.8.8 (8.8.8.8)
User Datagram Protocol, Src Port: 50993 (50993), Dst Port: 53 (53)
Domain Name System (query)
[Response In: 5]
Transaction ID: 0x0002
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
flipkart.com: type A, class IN
  Name: flipkart.com
  [Name Length: 12]
  [Label count: 2]
  Type: A (Host Address) (1)
  Class: IN (0x0001)
```

## DNS Response

Filter: ip.addr == 192.168.0.5							Expression...	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length	Info				
2	1.360809000	192.168.0.5	8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.in-addr.arpa				
3	1.415798000	8.8.8	192.168.0.5	DNS	124	Standard query response 0x0001 PTR google-public-dns-a.google.c				
4	1.420490000	192.168.0.5	8.8.8	DNS	72	Standard query 0x0002 A flipkart.com				
5	1.475562000	8.8.8	192.168.0.5	DNS	88	Standard query response 0x0002 A 163.53.78.58				

```

Ethernet II, Src: ArrisGro_e4:c4:27 (08:3e:0c:e4:c4:27), Dst: Apple_bc:31:4b (a4:5e:60:bc:31:4b)
Internet Protocol Version 4, Src: 8.8.8.8 (8.8.8.8), Dst: 192.168.0.5 (192.168.0.5)
User Datagram Protocol, Src Port: 53 (53), Dst Port: 50993 (50993)
Domain Name System (response)
[Request In: 4]
[Time: 0.055072000 seconds]
Transaction ID: 0x0002
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
flipkart.com: type A, class IN
Answers
flipkart.com: type A, class IN, addr 163.53.78.58
  Name: flipkart.com
  Type: A (Host Address) (1)
  Class: IN (0x0001)
  Time to live: 34
  Data length: 4
  Address: 163.53.78.58 (163.53.78.58)
```