

EE4013 Lab 3

Q1: Address: 58.229.6.225

```
rory@rory-Inspiron-5558:~$ nslookup aiiit.or.kr
Server:          127.0.1.1
Address:         127.0.1.1#53

Non-authoritative answer:
Name:   aiiit.or.kr
Address: 58.229.6.225
```

Q2: Address: 195.130.120.109

```
rory@rory-Inspiron-5558:~$ nslookup uoi.gr
Server:          127.0.1.1
Address:         127.0.1.1#53

Non-authoritative answer:
Name:   uoi.gr
Address: 195.130.120.109
```

Servers:

```
Authoritative answers can be found from:
marina.noc.uoi.gr      internet address = 195.130.120.120
kouzina.noc.uoi.gr    internet address = 195.130.120.110
sns1.grnet.gr         internet address = 83.212.5.22
```

Q3: Address: 195.130.120.120#53

```
rory@rory-Inspiron-5558:~$ nslookup mail.yahoo.com marina.noc.uoi.gr
Server:          marina.noc.uoi.gr
Address:         195.130.120.120#53

Non-authoritative answer:
mail.yahoo.com canonical name = login.yahoo.com.
```

Q4: Sent using UDP

458	11:46:48.345401449	10.52.242.144	10.220.1.11	ICMP	184 Destination unreachable (Port unreachable)
459	11:46:48.353807694	104.20.1.85	10.52.242.144	TCP	74 80 → 33674 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=...
460	11:46:48.353840012	10.52.242.144	104.20.1.85	TCP	66 33674 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=25...
461	11:46:48.371611128	104.20.1.85	10.52.242.144	TCP	74 80 → 33672 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=...
462	11:46:48.371641662	10.52.242.144	104.20.1.85	TCP	66 33672 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=25...
467	11:46:48.479808992	10.52.242.144	10.220.1.10	DNS	77 Standard query 0xf988 A www.cafepress.com
468	11:46:48.479882989	10.52.242.144	10.220.1.10	DNS	72 Standard query 0x87f1 A www.iana.org
469	11:46:48.480015618	10.52.242.144	10.220.1.10	DNS	83 Standard query 0x5ca6 A www.internetsociety.org
470	11:46:48.498452909	10.220.1.10	10.52.242.144	DNS	156 Standard query response 0xf988 A www.cafepress.com CN...
471	11:46:48.499530267	4.31.198.44	10.52.242.144	TCP	74 443 → 50330 [SYN, ACK] Seq=0 Ack=1 Win=43440 Len=0 MS...
472	11:46:48.499561266	10.52.242.144	4.31.198.44	TCP	66 50330 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=2...
[Coloring Rule Name: UDP]					
[Coloring Rule String: udp]					
▼ Ethernet II, Src: IntelCor_db:89:3b (e4:f8:9c:db:89:3b), Dst: Fortinet_09:00:17 (00:09:0f:09:00:17)					
▶ Destination: Fortinet_09:00:17 (00:09:0f:09:00:17)					
▶ Source: IntelCor_db:89:3b (e4:f8:9c:db:89:3b)					
Type: IPv4 (0x0800)					
▶ Internet Protocol Version 4, Src: 10.52.242.144, Dst: 10.220.1.10					
▶ User Datagram Protocol, Src Port: 10159, Dst Port: 53					
▼ Domain Name System (query)					
[Response In: 470]					
Transaction ID: 0xf988					
▶ Flags: 0x0100 Standard query					

Q5: Src Port: 53

Destination Port: 10159

```
▼ Ethernet II, Src: Fortinet_09:00:17 (00:09:0f:09:00:17), Dst: IntelCor_db
  ► Destination: IntelCor_db:89:3b (e4:f8:9c:db:89:3b)
  ► Source: Fortinet_09:00:17 (00:09:0f:09:00:17)
  Type: IPv4 (0x0800)
  ► Internet Protocol Version 4, Src: 10.220.1.10, Dst: 10.52.242.144
  ► User Datagram Protocol, Src Port: 53, Dst Port: 10159
▼ Domain Name System (response)
  [Request In: 467]
  [Time: 0.018643917 seconds]
  Transaction ID: 0xf988
```

Q6: It's sent to 10.52.255.255

```
wlp6s0  Link encap:Ethernet HWaddr e4:f8:9c:db:89:3b
        inet addr:10.52.242.144 Bcast:10.52.255.255 Mask:255.255.240.0
        inet6 addr: fe80::f6e7:14:86e2:1553/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:379761 errors:0 dropped:0 overruns:0 frame:0
        TX packets:47513 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:122872750 (122.8 MB) TX bytes:6487116 (6.4 MB)

rory@rory-Inspiron-5558:~$
```

Q7: It's a type A standard query and it doesn't contain any answers.

```
▼ Queries
  ▼ www.internetsociety.org: type A, class IN
    Name: www.internetsociety.org
    [Name Length: 23]
    [Label Count: 3]
    Type: A (Host Address) (1)
    Class: IN (0x0001)
```

Q8: There were 2 answers containing information about the name of the host, the type of address, class, the time to live, the data length and the IP address.

```
▼ www.iana.org: type CNAME, class IN, cname ianawww.vip.icann.org
  Name: www.iana.org
  Type: CNAME (Canonical NAME for an alias) (5)
  Class: IN (0x0001)
  Time to live: 2528
  Data length: 20
  CNAME: ianawww.vip.icann.org
▼ ianawww.vip.icann.org: type A, class IN, addr 192.0.32.8
  Name: ianawww.vip.icann.org
  Type: A (Host Address) (1)
  Class: IN (0x0001)
  Time to live: 30
  Data length: 4
  Address: 192.0.32.8
```

Q9: The first SYN packet was sent to 192.0.32.8 (see image above).

Q10: No

476	11:46:48.50277931	10.52.242.144	4.31.198.44	TLSv1.2	583 Client Hello
477	11:46:48.502820996	4.31.198.44	10.52.242.144	TCP	74 443 → 50334 [SYN, ACK] Seq=0 Ack=1 Win=43440 Len=0 MS...
478	11:46:48.502829396	10.52.242.144	4.31.198.44	TCP	66 50334 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=2...
479	11:46:48.502909257	10.52.242.144	4.31.198.44	TLSv1.2	583 Client Hello
484	11:46:48.573037115	10.220.1.10	10.52.242.144	DNS	99 Standard query response 0x5ca6 A www.internet-society...
485	11:46:48.584044028	10.220.1.10	10.52.242.144	DNS	120 Standard query response 0x87f1 A www.iana.org CNAME i...
487	11:46:48.671804788	4.31.198.44	10.52.242.144	TCP	66 443 → 50330 [ACK] Seq=1 Ack=518 Win=45056 Len=0 TSval...
488	11:46:48.673921244	4.31.198.44	10.52.242.144	TLSv1.2	1514 Server Hello
489	11:46:48.673936237	10.52.242.144	4.31.198.44	TCP	66 50330 → 443 [ACK] Seq=518 Ack=1449 Win=32128 Len=0 TS...
490	11:46:48.674921013	4.31.198.44	10.52.242.144	TCP	1514 [TCP segment of a reassembled PDU]
491	11:46:48.674930159	10.52.242.144	4.31.198.44	TCP	66 50330 → 443 [ACK] Seq=518 Ack=2897 Win=35072 Len=0 TS...
492	11:46:48.675965619	4.31.198.44	10.52.242.144	TCP	1266 [TCP segment of a reassembled PDU]
493	11:46:48.675979874	10.52.242.144	4.31.198.44	TCP	66 50330 → 443 [ACK] Seq=518 Ack=4097 Win=37888 Len=0 TS...

Q11: Source port: 37391
Destination: 53

```

Frame 2: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
▶ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▶ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.1.1
▶ User Datagram Protocol, Src Port: 37391, Dst Port: 53
▶ Domain Name System (query)

```

Q12: Address: 127.0.1.1

Yes

```

[Header checksum status: Unverified]
Source: 127.0.0.1
Destination: 127.0.1.1
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 37391, Dst Port: 53

```

Q13: Standard type A, no answers

```

▼ Queries
  ▼ www.mit.edu: type A, class IN
    Name: www.mit.edu
    [Name Length: 11]
    [Label Count: 3]
    Type: A (Host Address) (1)
    Class: IN (0x0001)

```

Q14: 3 answers containing name, type, class, TTL, data length and CNAME

```

      Class: IN (0x0001)
    ▼ Answers
      ▼ www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
        Name: www.mit.edu
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 1800
        Data length: 25
        CNAME: www.mit.edu.edgekey.net
      ▼ www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
        Name: www.mit.edu.edgekey.net
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 60
        Data length: 24
        CNAME: e9566.dscb.akamaiedge.net
      ▼ e9566.dscb.akamaiedge.net: type A, class IN, addr 2.22.134.2
        Name: e9566.dscb.akamaiedge.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 20
        Data length: 4

```

Q15: See image above for screenshot

Q16: Address: 127.0.1.1

Yes

```

▶ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▶ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.1.1
▶ User Datagram Protocol, Src Port: 44430, Dst Port: 53
▶ Domain Name System (query)

```

Q17: Type A standard query, no answers

```

      ▼ Queries
    ▼ Answers
      ▼ www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
        Name: www.mit.edu
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 1138
        Data length: 25
        CNAME: www.mit.edu.edgekey.net
      ▼ www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
        Name: www.mit.edu.edgekey.net
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 60
        Data length: 24
        CNAME: e9566.dscb.akamaiedge.net
      ▼ e9566.dscb.akamaiedge.net: type A, class IN, addr 2.22.134.2
        Name: e9566.dscb.akamaiedge.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 20
        Data length: 4
        Address: 2.22.134.2

```

Q18: www.mit.edu, www.mit.edu.edgekey.net, e9566.dscb.akamaiedge.net

Q19:

```
▼ Answers
  ▼ www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
    Name: www.mit.edu
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 1138
    Data length: 25
    CNAME: www.mit.edu.edgekey.net
  ▼ www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
    Name: www.mit.edu.edgekey.net
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 60
    Data length: 24
    CNAME: e9566.dscb.akamaiedge.net
  ▼ e9566.dscb.akamaiedge.net: type A, class IN, addr 2.22.134.2
    Name: e9566.dscb.akamaiedge.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 20
    Data length: 4
    Address: 2.22.134.2
```

Q20: Address: 127.0.1.1

Yes

```
▶ Frame 2: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
▶ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▶ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.1.1
▶ User Datagram Protocol, Src Port: 44430, Dst Port: 53
▶ Domain Name System (query)
```

Q21: Standard type A, no answers

```
▼ Queries
  ▼ www.mit.edu: type A, class IN
    Name: www.mit.edu
    [Name Length: 11]
    [Label Count: 3]
    Type: A (Host Address) (1)
    Class: IN (0x0001)
```

Q22: 3 answers containing name, type, class, TTL, data length and CNAME

Q23:

▼ Answers

```
▼ www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
  Name: www.mit.edu
  Type: CNAME (Canonical NAME for an alias) (5)
  Class: IN (0x0001)
  Time to live: 1138
  Data length: 25
  CNAME: www.mit.edu.edgekey.net
▼ www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
  Name: www.mit.edu.edgekey.net
  Type: CNAME (Canonical NAME for an alias) (5)
  Class: IN (0x0001)
  Time to live: 60
  Data length: 24
  CNAME: e9566.dscb.akamaiedge.net
▼ e9566.dscb.akamaiedge.net: type A, class IN, addr 2.22.134.2
  Name: e9566.dscb.akamaiedge.net
  Type: A (Host Address) (1)
  Class: IN (0x0001)
  Time to live: 20
  Data length: 4
  Address: 2.22.134.2
```
