

Task 1

- a) amazon.co.uk
- b) UTeM
- c) Shell

a(i)

```
C:\Users\PeiKang>nslookup www.amazon.co.uk
Server: ns8.maxis.net.my
Address: 2001:d08:10:201::10

Non-authoritative answer:
Name: e15314.dsca.akamaiedge.net
Addresses: 2001:d08:11:b98::3bd2
           2001:d08:11:b99::3bd2
           65.8.109.144
Aliases: www.amazon.co.uk
         tp.bfbdc3ca1-frontier.amazon.co.uk
         www.amazon.co.uk.edgekey.net
```

a(ii)

```
C:\Users\PeiKang>nslookup -type=NS amazon.co.uk
Server: ns8.maxis.net.my
Address: 2001:d08:10:201::10

Non-authoritative answer:
amazon.co.uk      nameserver = ns2.amzndns.com
amazon.co.uk      nameserver = ns2.amzndns.net
amazon.co.uk      nameserver = ns1.amzndns.co.uk
amazon.co.uk      nameserver = ns1.amzndns.org
amazon.co.uk      nameserver = ns2.amzndns.co.uk
amazon.co.uk      nameserver = ns2.amzndns.org
amazon.co.uk      nameserver = ns1.amzndns.net
amazon.co.uk      nameserver = ns1.amzndns.com

C:\Users\PeiKang>
```

b(i)

```
C:\Users\PeiKang>nslookup www.utm.edu.my
Server: ns8.maxis.net.my
Address: 2001:d08:10:201::10

Non-authoritative answer:
Name: www.utm.edu.my
Addresses: 64:ff9b::67c6:341f
           103.198.52.31
```

b(ii)

```
C:\Users\PeiKang>nslookup -type=NS www.utm.edu.my
Server: ns8.maxis.net.my
Address: 2001:d08:10:201::10

utm.edu.my
    primary name server = utm01.utm.edu.my
    responsible mail addr = zainudinsalleh.utm.edu.my
    serial = 2023032901
    refresh = 10800 (3 hours)
    retry = 900 (15 mins)
    expire = 604800 (7 days)
    default TTL = 10800 (3 hours)
```

c(i)

```
C:\Users\PeiKang>nslookup www.shell.com
Server: ns8.maxis.net.my
Address: 2001:d08:10:201::10

Non-authoritative answer:
Name: e11738.dscb.akamaiedge.net
Addresses: 2001:d08:11:ba1::2dda
           2001:d08:11:b8c::2dda
           118.214.32.116
Aliases: www.shell.com
          www.shell.com.edgekey.net
```

c(ii)

```
C:\Users\PeiKang>nslookup -type=NS www.shell.com
Server: ns8.maxis.net.my
Address: 2001:d08:10:201::10

Non-authoritative answer:
www.shell.com canonical name = www.shell.com.edgekey.net
www.shell.com.edgekey.net canonical name = e11738.dscb.akamaiedge.net

dscb.akamaiedge.net
    primary name server = n0dscb.akamaiedge.net
    responsible mail addr = hostmaster.akamai.com
    serial = 1684501459
    refresh = 1000 (16 mins 40 secs)
    retry = 1000 (16 mins 40 secs)
    expire = 1000 (16 mins 40 secs)
    default TTL = 1800 (30 mins)
```

Task2

1)

User Datagram Protocol, Src Port: 65024, Dst Port: 53

2)

175 2.201400 192.168.1.109 8.8.8.8 DNS 78 Standard query 0x7a66 AAAA analytics.ietf.org

```
DNS Servers . . . . . : 2001:d08:10:201::10
                        2001:d08:11:201::10
                        8.8.8.8
```


-Two IP addresses are the SAME


3)

```
Queries
  analytics.ietf.org: type AAAA, class IN
    Name: analytics.ietf.org
    [Name Length: 18]
    [Label Count: 3]
    Type: AAAA (IPv6 Address) (28)
    Class: IN (0x0001)
```


-Type : AAAA(IPv6Address)

4)

- (i)  analytics.ietf.org: type CNAME, class IN, cname analytics.ietf.org.cdn.cloudflare.net
Name: analytics.ietf.org
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 1800 (30 minutes)
Data length: 39
CNAME: analytics.ietf.org.cdn.cloudflare.net

- (ii)  analytics.ietf.org.cdn.cloudflare.net: type AAAA, class IN, addr 2606:4700::6810:2d63
Name: analytics.ietf.org.cdn.cloudflare.net
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Time to live: 300 (5 minutes)
Data length: 16
AAAA Address: 2606:4700::6810:2d63



Task 3

- 1)  User Datagram Protocol, Src Port: 58085, Dst Port: 53

- 2) 171 5.014779 2001:d08:e1:2e55:e8... 2001:d08:10:201::10 DNS 91 Standard query 0x0002 A www.mit.edu

```
DNS Servers . . . . . : 2001:d08:10:201::10
                        2001:d08:11:201::10
                        8.8.8.8
```

-It is my default local DNS server

- 3)  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)

-Type: A(Host Address)

4) - 3 Answers

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 (30 minutes)
 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 (1 minute)
 Data length: 24
 CNAME: e9566.dscb.akamaiedge.net

e9566.dscb.akamaiedge.net: type A, class IN, addr 104.111.167.128
 Name: e9566.dscb.akamaiedge.net
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Time to live: 20 (20 seconds)
 Data length: 4
 Address: 104.111.167.128

5)

The image shows a Wireshark packet capture window titled '*Wi-Fi'. The packet list on the left shows several packets, with packet 171 selected. The packet details pane on the right shows the structure of the selected packet, which is a DNS Standard query response. The packet bytes pane at the bottom shows the raw data of the packet.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
171	5.014779	2001:d08:e1:2e55:e8...	2001:d08:10:201::10	DNS	91	Standard query 0x0002 A www.mit.edu
172	5.222420	2001:d08:10:201::10	2001:d08:e1:2e55:e8...	DNS	180	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 104.111.167.128
173	5.222420	52.1.39.206	192.168.1.109	TCP	54	443 → 53609 [ACK] Seq=5471 Ack=2161 Win=47360 Len=0
174	5.222420	52.1.39.206	192.168.1.109	TLSv1.2	264	Application Data
175	5.230127	2001:d08:e1:2e55:e8...	2001:d08:10:201::10	DNS	91	Standard query 0x0003 AAAA www.mit.edu
176	5.263115	192.168.1.109	52.1.39.206	TCP	54	53609 → 443 [ACK] Seq=2161 Ack=5681 Win=131072 Len=0
177	5.362212	2001:d08:10:201::10	2001:d08:e1:2e55:e8...	DNS	220	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAAA 2001:d08:11...
178	5.440433	2001:d08:e1:2e55:e8...	2001:d08:10:201::10	DNS	99	Standard query 0x6e23 A wac-ring.msedge.net
179	5.440850	2001:d08:e1:2e55:e8...	2001:d08:10:201::10	DNS	99	Standard query 0xce90 AAAA wac-ring.msedge.net
180	5.448970	2001:d08:10:201::10	2001:d08:e1:2e55:e8...	DNS	212	Standard query response 0xce90 AAAA wac-ring.msedge.net CNAME wac-ring.wac-9999.wac-msedge.net CNAME wac-9999.wac-msedge.net A...
181	5.449464	2001:d08:10:201::10	2001:d08:e1:2e55:e8...	DNS	188	Standard query response 0x6e23 A wac-ring.msedge.net CNAME wac-ring.wac-9999.wac-msedge.net CNAME wac-9999.wac-msedge.net A 52...
182	5.450842	192.168.1.109	52.108.8.254	TCP	66	53610 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
183	5.471473	52.108.8.254	192.168.1.109	TCP	66	443 → 53610 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
184	5.471622	192.168.1.109	52.108.8.254	TCP	54	53610 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
185	5.472096	192.168.1.109	52.108.8.254	TLSv1.2	566	Client Hello
186	5.490518	52.108.8.254	192.168.1.109	TCP	54	443 → 53610 [ACK] Seq=1 Ack=513 Win=4194304 Len=0
187	5.492366	52.108.8.254	192.168.1.109	TCP	1506	443 → 53610 [ACK] Seq=1 Ack=513 Win=4194304 Len=1452 [TCP segment of a reassembled PDU]

Packet Details:

- Frame 171: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{95182499...}
- Ethernet II, Src: IntelCor_d1:b1:2c (8c:c6:81:d1:b1:2c), Dst: Tp-LinkT_8c:f6:34 (d8:0d:17:8c:f6:34)
- Internet Protocol Version 6, Src: 2001:d08:e1:2e55:e80f:a85e:eff6:c4b4, Dst: 2001:d08:10:201::10
- User Datagram Protocol, Src Port: 58085, Dst Port: 53
- Domain Name System (query)
 - Transaction ID: 0x0002
 - Flags: 0x0100 Standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
 - 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)

Packet Bytes:

```

0000  d8 0d 17 8c f6 34 8c c6 81 d1 b1 2c 86 dd 60 0d .....4...
0010  7c 6a 00 25 11 40 20 01 0d 08 00 e1 2e 55 e8 0f |j%@...U..
0020  a8 5e ef f6 c4 b4 20 01 0d 08 00 10 02 01 00 00 .....5%...
0030  00 00 00 00 00 10 e2 e5 00 35 00 25 d0 b9 00 02 .....www-
0040  01 00 00 01 00 00 00 00 00 00 03 77 77 03 6d .....it-edu...
0050  69 74 03 65 64 75 00 00 01 00 01
  
```