Task2

1.I Chose the site www.cloudways.com which is a company from Singapore that I found on the internet. Just note that the Non-authoritative answer is Ok as I read online because my address is not in their name server list, to read more in the answers here: https://serverfault.com/questions/413124/dns-nslookup-what-is-the-meaning-of-the-non-authoritative-answer

```
C:\Users\gabi>nslookup www.cloudways.com
Server:  home.home
Address:  10.0.0.138

Non-authoritative answer:
Name:    www.cloudways.com.cdn.cloudflare.net
Addresses:  172.67.8.150
          104.22.61.124
          104.22.60.124
Aliases:  www.cloudways.com
```

2.For the first time I tried to look up for Oxford university, I got some information but I didn't their IP as we can see:

```
C:\Users\gabi>nslookup -type=NS www.ox.ac.uk
Server:  home.home
Address:  10.0.0.138

ox.ac.uk
        primary name server = raptor.dns.ox.ac.uk
        responsible mail addr = hostmaster.ox.ac.uk
        serial  = 2022042340
        refresh = 3600 (1 hour)
        retry   = 1800 (30 mins)
        expire  = 1209600 (14 days)
        default TTL = 900 (15 mins)
```

So I tried another one Arden university in Berlin, Which I found the IP Address for their site

105.251.192.76

```
C:\Users\gabi>nslookup -type=NS arden.ac.uk
Server:  home.home
Address:  10.0.0.138

Non-authoritative answer:
arden.ac.uk     nameserver = ns-76.awsdns-09.com
arden.ac.uk     nameserver = ns-1728.awsdns-24.co.uk
arden.ac.uk     nameserver = ns-1388.awsdns-45.org
arden.ac.uk     nameserver = ns-1013.awsdns-62.net

ns-76.awsdns-09.com     internet address = 205.251.192.76
ns-1013.awsdns-62.net   internet address = 205.251.195.245
ns-1728.awsdns-24.co.uk internet address = 205.251.198.192
ns-1728.awsdns-24.co.uk AAAA IPv6 address = 2600:9000:5306:c000::1
```

Note that in Oxford I am no getting the Non authoritative but in Arden I do, this is happening probably because Oxford is converting from the URL.

3.

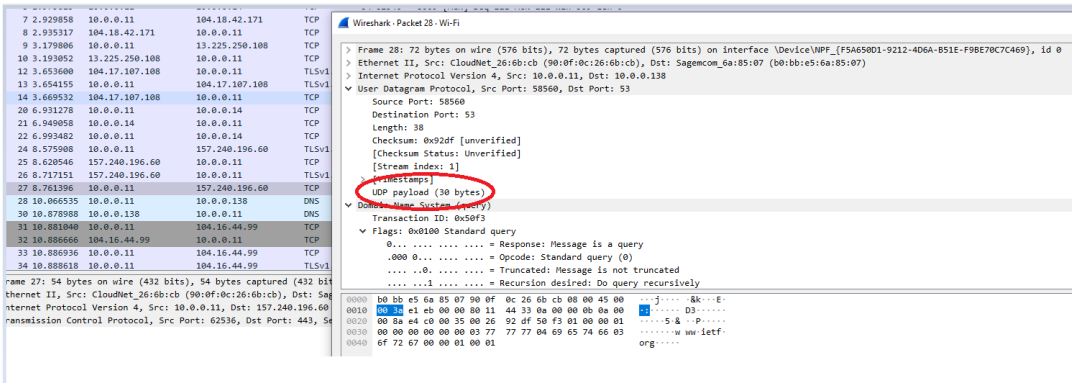
The question is asking to query one of the universities above, I tried to do anything I found to query one of them (or other universities) to get the yahoo. Mail information but anything I tried including (changing The IP addressed manually, including restarting the "nslookup" etc.) There for because the idea of this question is to query some other site and get the information using is DNS, I queried google DNS to get yahoo. Mail as the following picture shows.

```
C:\Users\gabi>nslookup mail.yahoo.com 8.8.8.8
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    edge.gycpi.b.yahoodns.net
Addresses:  2a00:1288:80:807::2
          2a00:1288:80:807::1
          87.248.119.251
          87.248.119.252
Aliases:  mail.yahoo.com
```

4 .They are both sent on UDP.

This is for the query:



This is for the response:

```
> Frame 30: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NF
> Ethernet II, Src: Sagemcom_6a:85:07 (b0:bb:e5:6a:85:07), Dst: CloudNet_26:6b:cb (90:0f:0c:26:6b
> Internet Protocol Version 4, Src: 10.0.0.138, Dst: 10.0.0.11
v User Datagram Protocol, Src Port: 53, Dst Port: 58560
    Source Port: 53
    Destination Port: 58560
    Length: 115
    Checksum: 0x3834 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  > [Timestamps]
    UDP payload (107 bytes)
v Domain Name System (response)
    Transaction ID: 0x50f3
  v Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated

0000  90 0f 0c 26 6b cb b0 bb  e5 6a 85 07 08 00 45 00   ···&k··· ·j····E·
0010  00 87 42 74 40 00 40 11  e3 5d 0a 00 00 8a 0a 00   ··Bt@·@· ·]******
0020  00 0b 00 35 e4 c0 00 73  38 34 50 f3 81 80 00 01   ···5···s 84P·····
0030  00 03 00 00 00 00 03 77  77 77 04 69 65 74 66 03   *******w ww·ietf·
0040  6f 72 67 00 00 01 00 01  c0 0c 00 05 00 01 00 00   org····· ********
0050  07 08 00 21 03 77 77 77  04 69 65 74 66 03 6f 72   ···!·www ·ietf·or
0060  67 03 63 64 6e 0a 63 6c  6f 75 64 66 6c 61 72 65   g·cdn·cl oudflare
0070  03 6e 65 74 00 c0 2a 00  01 00 01 00 00 01 2c 00   ·net··*· ******,·
0080  04 68 10 2c 63 c0 2a 00  01 00 01 00 00 01 2c 00   ·h·,c·*· ******,·
0090  04 68 10 2d 63                                     ·h·-c
```

5.The destination port for the query is 53 as we can see in the first image of question 4 (second line).

The source port of the response massage is also 53 (make sense because it was the destination of the query, and he is responding to that massage) as we can see in the second picture of the last question (first line).

6.It is sent to 10.0.0.138 which is the IP address of one of my local DNS as we can see in the picture the Default Getway.

```
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : A2-0F-0C-26-6B-CB
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : home
   Description . . . . . . . . . . . : Qualcomm QCA61x4A 802.11ac Wireless Adapter
   Physical Address. . . . . . . . . : 90-0F-0C-26-6B-CB
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::69a2:fe23:b326:5433%16(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.0.0.11(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Sunday, April 24, 2022 2:48:39 PM
   Lease Expires . . . . . . . . . . : Sunday, April 24, 2022 4:14:08 PM
   Default Gateway . . . . . . . . . : 10.0.0.138
   DHCP Server . . . . . . . . . . . : 10.0.0.138
   DHCPv6 IAID . . . . . . . . . . . : 150439360
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-28-DF-93-97-F4-EE-08-D7-03-75
   DNS Servers . . . . . . . . . . . : 10.0.0.138
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Physical Address. . . . . . . . . : 90-0F-0C-26-6B-CC
   DHCP Enabled. . . . . . . . . . . : Yes
```

7.It is a standard query of type A as we can see in the picture, and it doesn't have any answers (make sense it is a query).

```
    Transaction ID: 0x50f3
  ✓ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ✓ Queries
    > www.ietf.org: type A, class IN
    [Response in: 28]

0000  b0 bb e5 6a 85 07 90 0f  0c 26 6b cb 08 00 45 00   ···j···· ·&k···E·
0010  00 3a e1 eb 00 00 80 11  44 33 0a 00 00 0b 0a 00   ·:····· D3·····
0020  00 8a e4 c0 00 35 00 26  92 df 50 f3 01 00 00 01   ·····5·& ··P·····
0030  00 00 00 00 00 00 03 77  77 77 04 69 65 74 66 03   ·******w ww·ietf·
0040  6f 72 67 00 00 01 00 01                            org·····
```

8. 3 answers are provided 2 of them containing the name of the host, the type of the class, the time of living the data length and the address, the first one is a "CNAME" which is a type of DNS record that maps an alias name to a true or canonical domain name.

```
✓ Answers
  ✓ www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
      Name: www.ietf.org
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 1800 (30 minutes)
      Data length: 33
      CNAME: www.ietf.org.cdn.cloudflare.net
  ✓ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
      Name: www.ietf.org.cdn.cloudflare.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 4
      Address: 104.16.44.99
  ✓ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
      Name: www.ietf.org.cdn.cloudflare.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 4
      Address: 104.16.45.99
  [Request In: 28]
  [Time: 0.812453000 seconds]
```

9.Yes, as we can see in the following picture the SNY packet was sent to address 104.16.44.99, which corresponds to the addresses of the second answers from the last question.

30	10.878988	10.0.0.138	10.0.0.11	DNS	149 Standard query response 0x50f3 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.n
31	10.881040	10.0.0.11	104.16.44.99	TCP	66 56698 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
32	10.886666	104.16.44.99	10.0.0.11	TCP	66 443 → 56698 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1 WS=1024
33	10.886936	10.0.0.11	104.16.44.99	TCP	54 56698 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0

10.No, I don't have new queries.

11.The destination port for the DNS query is 53 as we can see int the following picture:

```
    Source Port: 59634
    Destination Port: 53
    Length: 57
    Checksum: 0xaf38 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
  > [Timestamps]
    UDP payload (29 bytes)
v Domain Name System (query)
    Transaction ID: 0x0004
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0

0000  b0 bb e5 6a 85 07 90 0f  0c 26 6b cb 08 00 45 00   ···j···· ·&k···E·
0010  00 39 e3 bd 00 00 80 11  42 62 0a 00 00 0b 0a 00   ·9····· Bb******
0020  00 8a e8 f2 00 35 00 25  af 38 00 04 01 00 00 01   ******5· ·8******
0030  00 00 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   *******w ww·mit·e
0040  64 75 00 00 01 00 01                               du·····
```

The source port for the response massage is also 53(make sense) as we can see in the following picture:

```
    Source Port: 53
    Destination Port: 59634
    Length: 129
    Checksum: 0xf39a [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
  > [Timestamps]
    UDP payload (121 bytes)
v Domain Name System (response)
    Transaction ID: 0x0004
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0

0000  90 0f 0c 26 6b cb b0 bb  e5 6a 85 07 08 00 45 00   ···&k··· ·j····E·
0010  00 95 52 f1 40 00 40 11  d2 d2 0a 00 00 8a 0a 00   ··R·@·@· ********
0020  00 0b 00 35 e8 f2 00 81  f3 9a 00 04 81 80 00 01   ···5···· ********
0030  00 03 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   *******w ww·mit·e
0040  64 75 00 00 01 00 01 c0  0c 00 05 00 01 00 00 07   du****** ********
0050  08 00 19 03 77 77 77 03  6d 69 74 03 65 64 75 07   ····www· mit·edu·
0060  65 64 67 65 6b 65 79 03  6e 65 74 00 c0 29 00 05   edgekey· net··)··
0070  00 01 00 00 00 3c 00 1b  05 65 39 35 36 36 04 64   *****<·· ·e9566·d
0080  73 63 62 0a 61 6b 61 6d  61 69 65 64 67 65 03 6e   scb·akam aiedge·n
0090  65 74 00 c0 4e 00 01 00  01 00 00 00 14 00 04 17   et··N··· ********
00a0  32 bc c4                                           2··
```

12.It is sent to 10.0.0.138 Which is my IP address of my default "DNS" as we can see from the picture of question 6 (ipconfig /all).

```
    Total Length: 57
    Identification: 0xe3bd (58301)
  v Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x4262 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.0.11
    Destination Address: 10.0.0.138
v User Datagram Protocol, Src Port: 59634, Dst Port: 53
    Source Port: 59634

0000  b0 bb e5 6a 85 07 90 0f  0c 26 6b cb 08 00 45 00   ···j···· ·&k···E·
0010  00 39 e3 bd 00 00 80 11  42 62 0a 00 00 0b 0a 00   ·9****** Bb******
0020  00 8a e8 f2 00 35 00 25  af 38 00 04 01 00 00 01   ******5· ·8******
0030  00 00 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   *******w ww·mit·e
0040  64 75 00 00 01 00 01                               du·····
```

13. It is a standard query of type A as we can see in the picture, and it doesn't have any answers (make sense it is a query).

```
  Transaction ID: 0x0004
> Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
v Queries
  v 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)
  [Response In: 18]
```

14.contains 3 answers 2 of them are "CNAME" which is a type of DNS record that maps an alias name to a true or canonical domain name and one which contains the name the type the class the time of living the length and the address.

```
v Answers
  v 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
  v 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: 27
      CNAME: e9566.dscb.akamaiedge.net
  v e9566.dscb.akamaiedge.net: type A, class IN, addr 23.50.188.196
      Name: e9566.dscb.akamaiedge.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 20 (20 seconds)
      Data length: 4
      Address: 23.50.188.196
  [Request In: 17]
  [Time: 0.208057000 seconds]
```

15.screenshot provided for any question including the last one.

16. It is sent to 10.0.0.138 Which is my IP address of my default "DNS" as we can see from the picture of question 6 (ipconfig /all).

```
Internet Protocol Version 4, Src: 10.
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 byte
  > Differentiated Services Field: 0x0
    Total Length: 53
    Identification: 0xe42a (58410)
  v Flags: 0x00
        0... .... = Reserved bit: Not s
        .0.. .... = Don't fragment: Not
        ..0. .... = More fragments: Not
    ...0 0000 0000 0000 = Fragment Off
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x41f9 [validatio
    [Header checksum status: Unverifie
    Source Address: 10.0.0.11
    Destination Address: 10.0.0.138
```

17.It is a standard query of type NS that doesn't have any answers:

```
v Domain Name System (query)
    Transaction ID: 0x0003
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v mit.edu: type NS, class IN
        Name: mit.edu
        [Name Length: 7]
        [Label Count: 2]
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
    [Response In: 21]
```

18.Nothing from MIT but I do get from "akam" which is a domain The name servers of "akam" are: asia1, ns1-37, use2, eur5, usw2, use5, asia2, ns1-173 as we can see in the following picture, we can get their IP addresses as we also can see in the picture under Additional records.

```
        Class: IN (0x0001)
  Answers
    mit.edu: type NS, class IN, ns asia1.akam.net
    mit.edu: type NS, class IN, ns ns1-37.akam.net
    mit.edu: type NS, class IN, ns use2.akam.net
    mit.edu: type NS, class IN, ns eur5.akam.net
    mit.edu: type NS, class IN, ns usw2.akam.net
    mit.edu: type NS, class IN, ns use5.akam.net
    mit.edu: type NS, class IN, ns asia2.akam.net
    mit.edu: type NS, class IN, ns ns1-173.akam.net
  Additional records
    eur5.akam.net: type A, class IN, addr 23.74.25.64
    use2.akam.net: type A, class IN, addr 96.7.49.64
    use5.akam.net: type A, class IN, addr 2.16.40.64
    usw2.akam.net: type A, class IN, addr 184.26.161.64
    asia1.akam.net: type A, class IN, addr 95.100.175.64
    asia2.akam.net: type A, class IN, addr 95.101.36.64
    ns1-37.akam.net: type A, class IN, addr 193.108.91.37
    ns1-173.akam.net: type A, class IN, addr 193.108.91.173
    use5.akam.net: type AAAA, class IN, addr 2600:1403:a::40
    ns1-173.akam.net: type AAAA, class IN, addr 2600:1401:2::ad
  [Request In: 20]
  [Time: 0.064257000 seconds]
```

19.A picture is provided in any question, here I will provide the main Wireshark picture.

16	3.348277	10.0.0.11	10.0.0.138	DNS	83	Standard query 0x0001 PTR 138.0.0.10.in-addr.arpa
17	3.351466	10.0.0.138	10.0.0.11	DNS	106	Standard query response 0x0001 PTR 138.0.0.10.in-addr.arpa PTR h
18	3.355146	10.0.0.11	10.0.0.138	DNS	72	Standard query 0x0002 NS mit.edu.home
19	3.358296	10.0.0.138	10.0.0.11	DNS	72	Standard query response 0x0002 No such name NS mit.edu.home
20	3.359895	10.0.0.11	10.0.0.138	DNS	67	Standard query 0x0003 NS mit.edu
21	3.424152	10.0.0.138	10.0.0.11	DNS	418	Standard query response 0x0003 NS mit.edu NS asia1.akam.net NS n

20.It was sent to 18.0.72.3 which is the IP address of bitsy.mit.edu.

```
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 60
  Identification: 0x9079 (36985)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: UDP (17)
  Header Checksum: 0x462a [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.0.0.11
  Destination Address: 18.0.72.3
User Datagram Protocol, Src Port: 58337, Dst Port: 53
Domain Name System (query)
```

21.It is a standard query of type A as we can see in the following picture.

```
  Transaction ID: 0x0004
> Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
v Queries
  v www.aiit.or.kr: type A, class IN
      Name: www.aiit.or.kr
      [Name Length: 14]
      [Label Count: 4]
      Type: A (Host Address) (1)
      Class: IN (0x0001)

0000  b0 bb e5 6a 85 07 90 0f  0c 26 6b cb 08 00 45 00
0010  00 3c 90 79 00 00 80 11  46 2a 0a 00 00 0b 12 00
0020  48 03 e3 e1 00 35 00 28  75 d9 00 04 01 00 00 01
```

22.Just one answer that provides the following data:

```
  Transaction ID: 0x0004
> Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
v Queries
  > www.aiit.or.kr: type A, class IN
v Answers
  v www.aiit.or.kr: type A, class IN, addr 58.229.6.225
      Name: www.aiit.or.kr
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 3374 (56 minutes, 14 seconds)
      Data length: 4
      Address: 58.229.6.225
  [Request In: 19]
  [Time: 0.002290000 seconds]
```

23. All pictures provided in the questions including the last one.