

1. I searched for bazar.pk

```
C:\Users\Bilal>nslookup bazar.pk
Server: UnKnown
Address: fe80::1

Non-authoritative answer:
Name: bazar.pk
Address: 174.138.184.18

C:\Users\Bilal>
```

Their ip address is 174.138.184.18

2. The authoritative DNS for a university in Europe is

```
PS C:\WINDOWS\system32> nslookup -type=NS www.ed.ac.uk
Server: UnKnown
Address: fe80::1

ed.ac.uk
    primary name server = dns0.ed.ac.uk
    responsible mail addr = hostmaster.ed.ac.uk
    serial = 2020146463
    refresh = 1800 (30 mins)
    retry = 900 (15 mins)
    expire = 1209600 (14 days)
    default TTL = 900 (15 mins)
PS C:\WINDOWS\system32> nslookup www.ed.ac.uk dns0.ed.ac.uk
Server: is jcmb
Address: 129.215.200.7

DNS request timed out.
    timeout was 2 seconds.
Name: www.ed.ac.uk
Address: 23.185.0.1

PS C:\WINDOWS\system32> nslookup www.ed.ac.uk dns0.ed.ac.uk
DNS request timed out.
    timeout was 2 seconds.
Server: UnKnown
Address: 129.215.200.7

Name: www.ed.ac.uk
Addresses: 2620:12a:8001::1
           2620:12a:8000::1
           23.185.0.1

PS C:\WINDOWS\system32> D
```

3.

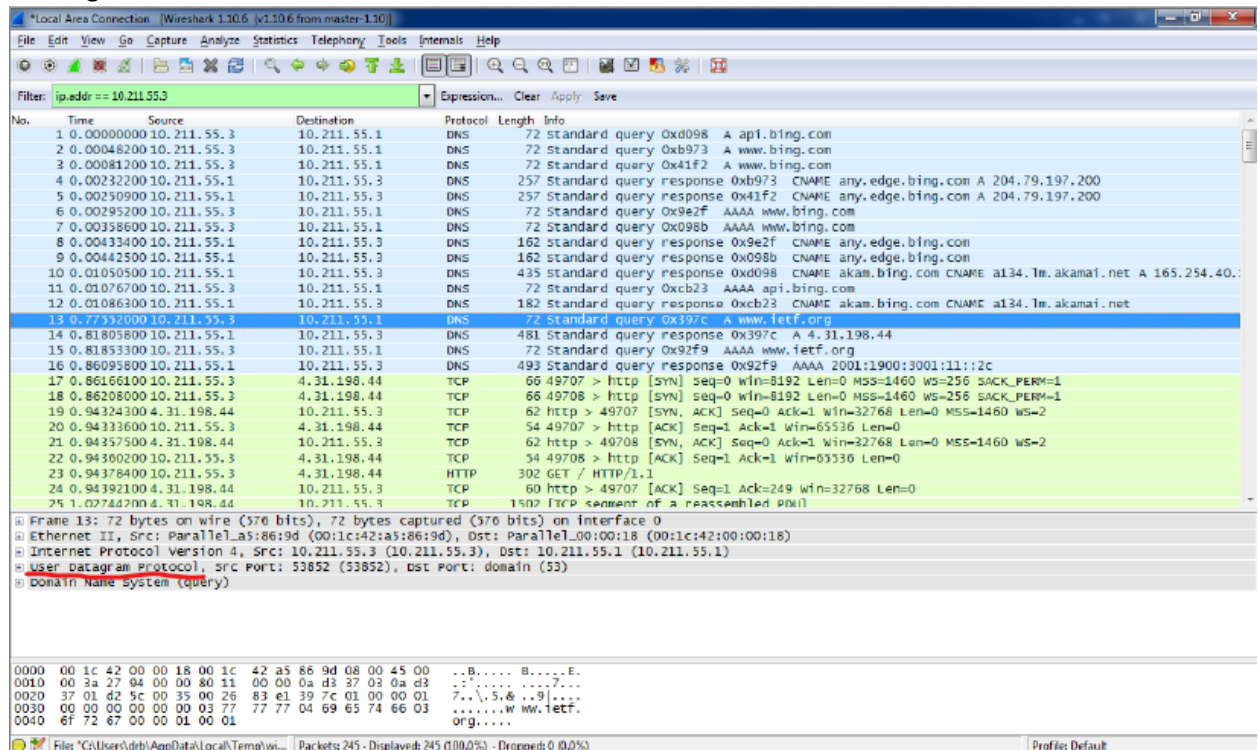
```

PS C:\WINDOWS\system32> nslookup www.ed.ac.uk mail.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
Server: UnKnown
Address: 87.248.119.251

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out
PS C:\WINDOWS\system32>

```

4. Messages are sent via UDP Protocol



5. See screenshot. Source port: 53853. Dest port: 53.

6. The screenshot shows that the DNS message was sent to 10.211.55.1. This matches the DNS server listed by the command `ipconfig /all`.

The screenshot displays a Wireshark packet capture with a filter set to `ip.addr == 10.211.55.3`. The packet list shows a series of DNS queries and responses. Packet 1 is a standard query for `api.bing.com` sent to 10.211.55.1. The packet details pane shows the User Datagram Protocol (UDP) and Domain Name System (DNS) sections. The DNS section indicates a standard query for `api.bing.com` with a query ID of 0x0000. The packet bytes pane shows the raw data of the DNS query, including the query ID, flags, and the domain name in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	10.211.55.3	10.211.55.1	DNS	72	Standard query 0x0098 A api.bing.com
2	0.00048200	10.211.55.3	10.211.55.1	DNS	72	Standard query 0xb973 A www.bing.com
3	0.00081200	10.211.55.3	10.211.55.1	DNS	72	Standard query 0x41f2 A www.bing.com
4	0.00232200	10.211.55.1	10.211.55.3	DNS	257	Standard query response 0xb973 CNAME any.edge.bing.com A 204.79.197.200
5	0.00250900	10.211.55.1	10.211.55.3	DNS	257	Standard query response 0x41f2 CNAME any.edge.bing.com A 204.79.197.200
6	0.00295200	10.211.55.3	10.211.55.1	DNS	72	Standard query 0x9e2f AAAA www.bing.com
7	0.00358600	10.211.55.3	10.211.55.1	DNS	72	Standard query 0x098b AAAA www.bing.com
8	0.00433400	10.211.55.1	10.211.55.3	DNS	162	Standard query response 0x9e2f CNAME any.edge.bing.com
9	0.00442500	10.211.55.1	10.211.55.3	DNS	162	Standard query response 0x098b CNAME any.edge.bing.com
10	0.01050500	10.211.55.1	10.211.55.3	DNS	435	Standard query response 0x0098 CNAME akan.bing.com CNAME a134.1m.akamai.net A 165.254.40.1
11	0.01076700	10.211.55.3	10.211.55.1	DNS	72	Standard query 0xcb23 AAAA api.bing.com
12	0.01086300	10.211.55.1	10.211.55.3	DNS	182	Standard query response 0xcb23 CNAME akan.bing.com CNAME a134.1m.akamai.net
13	0.77332000	10.211.55.3	10.211.55.1	DNS	72	Standard query 0x397c A www.ietf.org
14	0.81805800	10.211.55.1	10.211.55.3	DNS	481	Standard query response 0x397c A 4.31.198.44
15	0.81853300	10.211.55.3	10.211.55.1	DNS	72	Standard query 0x92f9 AAAA www.ietf.org
16	0.86095800	10.211.55.1	10.211.55.3	DNS	493	Standard query response 0x92f9 AAAA 2001:1900:3001:11::2c
17	0.86166100	10.211.55.3	4.31.198.44	TCP	66	49707 > http [SYN] seq=0 win=8192 len=0 MSS=1460 WS=256 SACK_PERM=1
18	0.86208000	10.211.55.3	4.31.198.44	TCP	66	49708 > http [SYN] seq=0 win=8192 len=0 MSS=1460 WS=256 SACK_PERM=1
19	0.94324300	4.31.198.44	10.211.55.3	TCP	62	http > 49707 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460 WS=2
20	0.94336600	10.211.55.3	4.31.198.44	TCP	54	49707 > http [ACK] Seq=1 Ack=1 Win=65536 Len=0
21	0.94357500	4.31.198.44	10.211.55.3	TCP	62	http > 49708 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460 WS=2
22	0.94360200	10.211.55.3	4.31.198.44	TCP	54	49708 > http [ACK] Seq=1 Ack=1 Win=65536 Len=0
23	0.94378400	10.211.55.3	4.31.198.44	HTTP	302	GET / HTTP/1.1
24	0.94392100	4.31.198.44	10.211.55.3	TCP	60	http > 49707 [ACK] Seq=1 Ack=249 Win=32768 Len=0
25	1.02744200	4.31.198.44	10.211.55.3	TCP	1502	TCP segment of a reassembled RST

Time to live: 128
Protocol: UDP (17)
Header checksum: 0x0000 [validation disabled]
Source: 10.211.55.3 (10.211.55.3)
Destination: 10.211.55.1 (10.211.55.1)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 53852 (53852), Dst Port: domain (53)
Domain Name System (query)
0000 00 1c 42 00 00 18 00 1c 42 a5 8b 9d 08 00 45 00 ..B....B....
0010 00 3a 27 94 00 00 80 11 00 00 0a d3 87 03 0a d3
0020 37 01 62 5c 00 35 00 26 83 e1 39 7c 01 00 00 01 7...5.&..9)....
0030 00 00 00 00 00 00 93 77 77 77 04 69 65 74 66 03Www.ietf.
0040 8f 72 67 00 00 01 00 01org.....

7. It is a "type A" query, which is for a standard host address resource record. No answers as shown in screenshot

11.

No.	Time	Source	Destination	Protocol	Length	Info
3	0.00013200	10.211.55.3	10.211.55.1	DNS	84	Standard query 0x0001 PTR 1.55.211.10.in-addr.arpa
4	0.00031600	10.211.55.1	10.211.55.3	DNS	133	Standard query response 0x0001 No such name
5	0.00204100	10.211.55.3	10.211.55.1	DNS	83	Standard query 0x0002 A www.mit.edu.localdomain
6	0.00327600	10.211.55.1	10.211.55.3	DNS	83	Standard query response 0x0002 No such name
7	0.00341600	10.211.55.3	10.211.55.1	DNS	83	Standard query 0x0003 AAAA www.mit.edu.localdomain
8	0.00348400	10.211.55.1	10.211.55.3	DNS	83	Standard query response 0x0003 No such name
9	0.00460300	10.211.55.3	10.211.55.1	DNS	71	Standard query 0x0004 A www.mit.edu
10	0.03914300	10.211.55.1	10.211.55.3	DNS	429	Standard query response 0x0004 CNAME www.mit.edu.edgekey.net CNAME
11	0.03981300	10.211.55.3	10.211.55.1	DNS	71	Standard query 0x0005 AAAA www.mit.edu
12	0.04160000	10.211.55.1	10.211.55.3	DNS	202	Standard query response 0x0005 CNAME www.mit.edu.edgekey.net CNAME

Source: 10.211.55.3 (10.211.55.3)
Destination: 10.211.55.1 (10.211.55.1)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]

⊟ User Datagram Protocol, Src Port: 63140, Dst Port: domain (53)
Source port: 63140 (63140)
Destination port: domain (53)
Length: 37
Checksum: 0x83e0 [validation disabled]

⊟ Domain Name System (query)
[Response in: 101](#)
Transaction ID: 0x0004
Flags: 0x0100 standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0

0000 00 1c 42 00 00 18 00 1c 42 a5 86 9d 08 00 45 00 ...B.....B....E.
0010 00 39 28 0f 00 00 80 11 00 00 04 d3 37 03 0a d3 ...9C.....7...
0020 37 01 f6 a4 00 35 00 25 83 e0 00 04 01 00 00 01 7...5.%
0030 00 00 00 00 00 00 03 77 77 77 03 6d 69 74 03 65w ww.mit.e
0040 64 75 00 00 01 00 01 du.....

Frame (frame), 71 bytes Packets: 12 • Displayed: 10 (83.3%) • Dropped: 0 (0.0%) Profile: Default

Source port: 63140. Dest port: 53

12. DNS Query message was sent to 10.211.55.1

13. Standard type A (Host address) query (see screenshot). The message only contains a query (no answers).

No.	Time	Source	Destination	Protocol	Length	Info
3	0.00013200	10.211.55.3	10.211.55.1	DNS	84	Standard query 0x0001 PTR 1.55.211.10.in-addr.arpa
4	0.00031600	10.211.55.1	10.211.55.3	DNS	133	Standard query response 0x0001 No such name
5	0.00204100	10.211.55.3	10.211.55.1	DNS	83	Standard query 0x0002 A www.mit.edu.localdomain
6	0.00327600	10.211.55.1	10.211.55.3	DNS	83	Standard query response 0x0002 No such name
7	0.00341600	10.211.55.3	10.211.55.1	DNS	83	Standard query 0x0003 AAAA www.mit.edu.localdomain
8	0.00348400	10.211.55.1	10.211.55.3	DNS	83	Standard query response 0x0003 No such name
9	0.00460300	10.211.55.3	10.211.55.1	DNS	71	Standard query 0x0004 A www.mit.edu
10	0.03914300	10.211.55.1	10.211.55.3	DNS	429	Standard query response 0x0004 CNAME www.mit.edu.edgekey.net CNAME
11	0.03981300	10.211.55.3	10.211.55.1	DNS	71	Standard query 0x0005 AAAA www.mit.edu
12	0.04160000	10.211.55.1	10.211.55.3	DNS	202	Standard query response 0x0005 CNAME www.mit.edu.edgekey.net CNAME

Source port: 65140 (65140)
Destination port: domain (53)
Length: 37
Checksum: 0x83e0 [validation disabled]

Domain Name System (query)
[Response in: 10]
Transaction ID: 0x0004
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
Type: A (Host address)
Class: IN (0x0001)

```

0000 00 1c 42 00 00 18 00 1c 42 a5 86 9d 08 00 45 00  .B....B....E.
0010 00 39 28 0f 00 00 80 11 00 00 0a 03 37 03 0a d3  .9(.....7...
0020 17 01 f6 a4 00 35 00 25 81 e0 00 04 01 00 00 01  7....5.%.....
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....

```

Frame (frame), 71 bytes Packets: 12 · Displayed: 10 (83.3%) · Dropped: 0 (0.0%) Profile: Default

- Three answers (resource records), two corresponding to CNAMEs and one host address.

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: **ip.addr == 10.211.55.3** Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
3	0.00013200	10.211.55.3	10.211.55.1	DNS	84	Standard query 0x0001 PTR 1.55.211.10.in-addr.arpa
4	0.00031600	10.211.55.1	10.211.55.3	DNS	133	Standard query response 0x0001 No such name
5	0.00204100	10.211.55.3	10.211.55.1	DNS	83	Standard query 0x0002 A www.mit.edu.localdomain
6	0.00327600	10.211.55.1	10.211.55.3	DNS	83	Standard query response 0x0002 No such name
7	0.00341600	10.211.55.3	10.211.55.1	DNS	83	Standard query 0x0003 AAAA www.mit.edu.localdomain
8	0.00348400	10.211.55.1	10.211.55.3	DNS	83	Standard query response 0x0003 No such name
9	0.00460300	10.211.55.3	10.211.55.1	DNS	71	Standard query 0x0004 A www.mit.edu
10	0.03914300	10.211.55.1	10.211.55.3	DNS	429	Standard query response 0x0004 CNAME www.mit.edu.edgekey.net CNAME
11	0.03981300	10.211.55.3	10.211.55.1	DNS	71	Standard query 0x0005 AAAA www.mit.edu

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)
 - Class: IN (0x0001)
 - Time to live: 30 minutes
 - Data length: 25
 - Primaryname: www.mit.edu.edgekey.net
- www.mit.edu.edgekey.net: type CNAME, class IN, cname e7086.b.akamaiedge.net
 - Name: www.mit.edu.edgekey.net
 - type: CNAME (canonical name for an alias)
 - Class: IN (0x0001)
 - Time to live: 5 minutes
 - Data length: 21
 - Primaryname: e7086.b.akamaiedge.net
- e7086.b.akamaiedge.net: type A, class IN, addr 23.208.102.151
 - Name: e7086.b.akamaiedge.net
 - type: A (Host address)
 - Class: IN (0x0001)
 - Time to live: 20 seconds
 - Data length: 4
 - Addr: 23.208.102.151 (23.208.102.151)
- Authoritative nameservers
 - e7086.b.akamaiedge.net: type NS, class IN, ns e7086.b.akamaiedge.net

0000 00 1c 42 a5 86 9d 00 1c 42 00 00 18 08 00 45 00 ...B....B....E.
 0010 01 9f 35 be 00 00 80 11 7f e6 0a d3 37 01 0a d3 ...5....7...
 0020 17 03 00 35 f6 a4 01 8b 0e 38 00 04 81 80 00 01 7.5....8...
 0030 00 03 00 08 00 08 03 77 77 77 03 6d 69 74 03 65w ww.mit.e
 0040 64 75 00 00 01 00 01 c0 0c 00 05 00 01 00 00 07 du.....
 0050 68 00 10 05 77 77 77 03 6d 80 7a 03 65 64 75 67 www.mit.edu

Frame (frame), 429 bytes Packets: 12 • Displayed: 10 (83.3%) • Dropped: 0 (0.0%) Profile: Default

16. It was sent to 23.33.6.100

Filter: **ip.addr == 23.33.6.100**

No.	Time	Source	Destination	Protocol	Length	Info
278	60.299427	192.168.100.40	23.33.6.100	DNS	84	Standard query 0x0001 PTR 100.6.33.23.in-addr.arpa
302	62.313547	192.168.100.40	23.33.6.100	DNS	68	Standard query 0x0002 A ♦type=NS
305	64.316212	192.168.100.40	23.33.6.100	DNS	68	Standard query 0x0003 AAAA ♦type=NS

> 000. = Flags: 0x0
 ...0 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 128
 Protocol: UDP (17)
 Header Checksum: 0xa153 [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 192.168.100.40
 Destination Address: 23.33.6.100

▼ User Datagram Protocol, Src Port: 55174, Dst Port: 53

Source Port: 55174
 Destination Port: 53
 Length: 50
 Checksum: 0x352b [unverified]
 [Checksum Status: Unverified]
 [Stream Index: 14]
 > [Timestamps]
 UDP payload (42 bytes)

▼ Domain Name System (query)

Identification of transaction (dns.id), 2 bytes

0000 24 44 27 26 ab e1 f4 8c 50 22 98 c7 08 00 45 4
 0010 00 46 56 fe 00 00 80 11 a1 53 c0 a8 64 2b 17 7
 0020 06 64 d7 86 00 35 00 32 35 2b 00 01 01 00 00 4
 0030 00 00 00 00 00 00 03 31 30 30 01 36 02 33 33 4
 0040 32 33 07 69 6e 2d 61 64 64 72 04 61 72 70 61 4
 0050 00 0c 00 01

Packets: 746 • Displayed: 3 (0.4%) Profile: Default

17. It is a "type A" query, which is for a standard host address resource record. No answers as shown in screenshot


```

    UDP payload (42 bytes)
  ▾ Domain Name System (query)
    Transaction ID: 0x0001
    > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    > Queries

```

18. No the query request timed out thus no answers

```

PS C:\WINDOWS\system32> nslookup -type=NS mit.edu
DNS request timed out.
    timeout was 2 seconds.
Server: UnKnown
Address: 23.33.6.100

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out
PS C:\WINDOWS\system32>

```

19. It's a DNS Query

ip.addr == 18.0.72.3

No.	Time	Source	Destination	Protocol	Length	Info
6172	483.357953	192.168.100.40	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
6192	485.365993	192.168.100.40	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
6259	487.379993	192.168.100.40	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
6299	489.902704	192.168.100.40	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
6370	491.919383	192.168.100.40	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr

[Coloring Rule String: udp]

▼ Ethernet II, Src: IntelCor_22:98:c7 (f4:8c:50:22:98:c7), Dst: HuaweiTe_26:ab:e1 (24:44:27:26:ab:e1)

- ▼ Destination: HuaweiTe_26:ab:e1 (24:44:27:26:ab:e1)
 - Address: HuaweiTe_26:ab:e1 (24:44:27:26:ab:e1)
 - = LG bit: Globally unique address (factory default)
 - = IG bit: Individual address (unicast)
- ▼ Source: IntelCor_22:98:c7 (f4:8c:50:22:98:c7)
 - Address: IntelCor_22:98:c7 (f4:8c:50:22:98:c7)
 - = LG bit: Globally unique address (factory default)
 - = IG bit: Individual address (unicast)
- Type: IPv4 (0x0800)
- > Internet Protocol Version 4, Src: 192.168.100.40, Dst: 18.0.72.3
- > User Datagram Protocol, Src Port: 60341, Dst Port: 53
- ▼ Domain Name System (query)
 - Transaction ID: 0x0001
 - > Flags: 0x0100 Standard query
 - Questions: 1
 - Answer RRs: 0

0000 24 44 27 26 ab e1 f4 8c 50 22 98 c7 08 00 45 00
 0010 00 44 7d 8b 00 00 80 11 3e 4a c0 a8 64 28 12 00
 0020 48 03 eb b5 00 35 00 30 e9 db 00 01 01 00 00 00
 0030 00 00 00 00 00 01 33 02 37 32 01 30 02 31 00
 0040 07 69 6e 2d 61 64 64 72 04 61 72 70 61 00 00 00
 0050 00 01

20. I was unable to get this to work with bitsy.mit.edu so I used the Google public DNS 8.8.8.8. The query is sent to 8.8.8.8 (not the default local DNS server).

21. It is a "type A" query, which is for a standard host address resource record. No answers as shown in screenshot


```
> User Datagram Protocol, Src Port: 60
▼ Domain Name System (query)
  Transaction ID: 0x0001
    > Flags: 0x0100 Standard query
      Questions: 1
      Answer RRs: 0
      Authority RRs: 0
      Additional RRs: 0
    > Queries
```

22. The request timed out thus no answers provided.

```
> User Datagram Protocol, Src Port: 60
▼ Domain Name System (query)
  Transaction ID: 0x0001
    > Flags: 0x0100 Standard query
      Questions: 1
      Answer RRs: 0
      Authority RRs: 0
      Additional RRs: 0
    > Queries
```