Capture and Analyse DNS Packets using Wireshark.

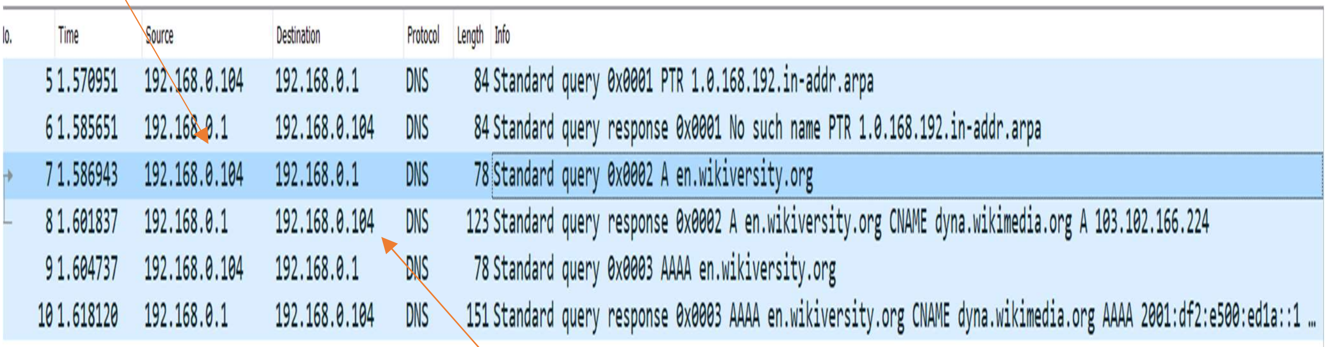
a. Analyse DNS Query and Response Packets.

b. By using the captured packets identify the source and destination ports query and response messages.

c. Check whether a DNS request receives multiple responses, if so, determine the the reason for this

local machine requesting for en.wikiversity.org

A)



lo.	Time	Source	Destination	Protocol	Length	Info
5	1.570951	192.168.0.104	192.168.0.1	DNS	84	Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa
6	1.585651	192.168.0.1	192.168.0.104	DNS	84	Standard query response 0x0001 No such name PTR 1.0.168.192.in-addr.arpa
7	1.586943	192.168.0.104	192.168.0.1	DNS	78	Standard query 0x0002 A en.wikiversity.org
8	1.601837	192.168.0.1	192.168.0.104	DNS	123	Standard query response 0x0002 A en.wikiversity.org CNAME dyna.wikimedia.org A 103.102.166.224
9	1.604737	192.168.0.104	192.168.0.1	DNS	78	Standard query 0x0003 AAAA en.wikiversity.org
10	1.618120	192.168.0.1	192.168.0.104	DNS	151	Standard query response 0x0003 AAAA en.wikiversity.org CNAME dyna.wikimedia.org AAAA 2001:df2:e500:ed1a::1 …

My DNS server responding with the Ip address of that URL

Here my local machine is my computer and DNS server is my rourter.

Here My ip is:192.168.0.104

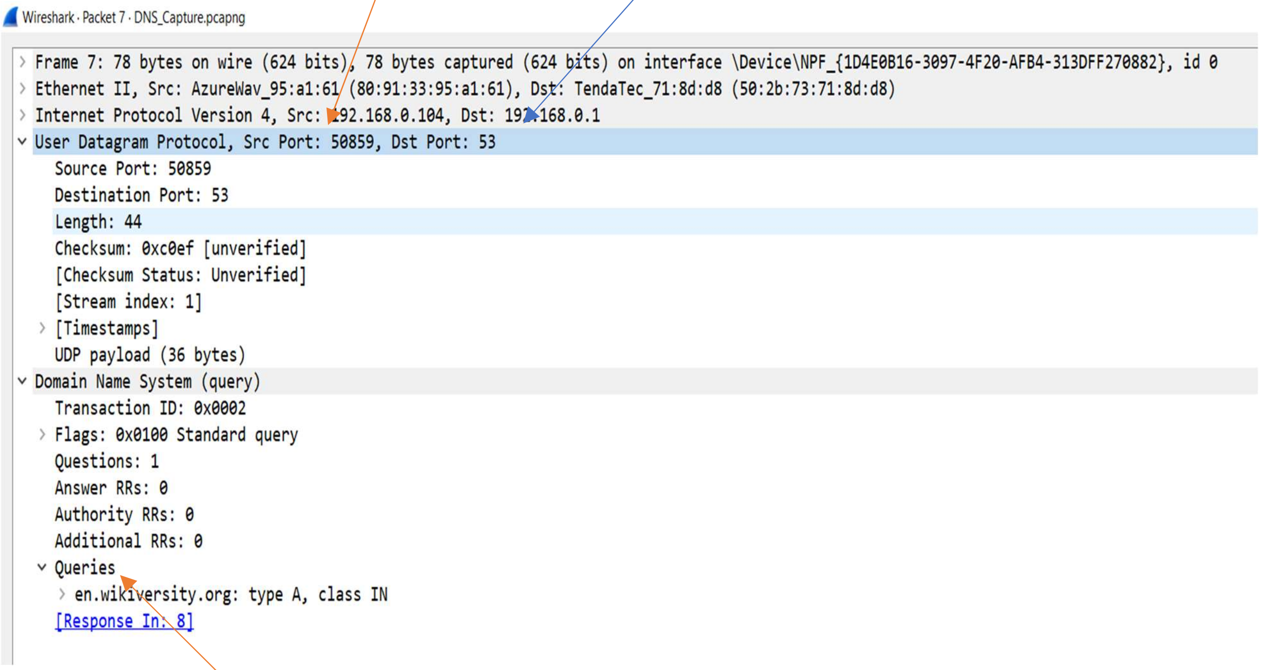
My DNS serverip :192.168.0.1

B)

- ***requesting for URL***

Source ip address

Destination IP



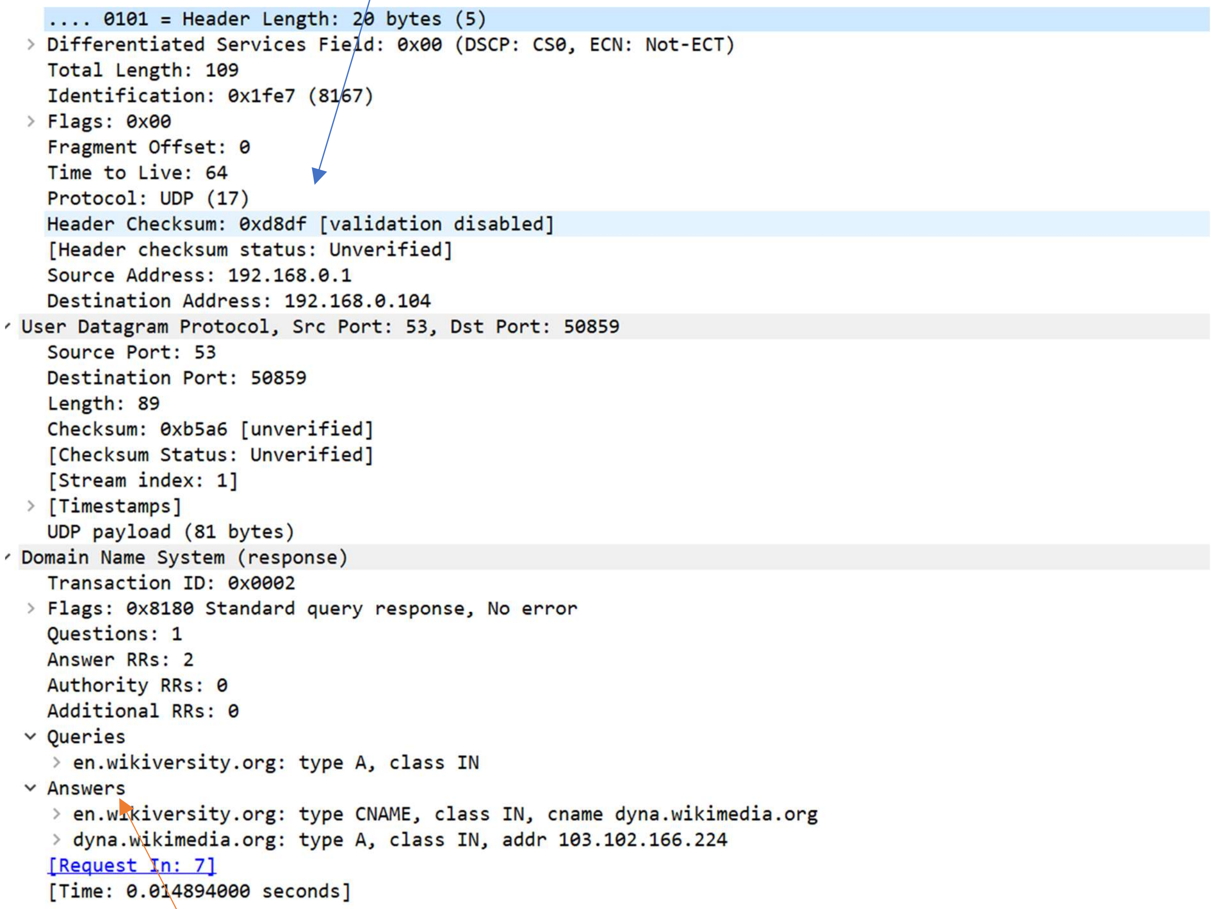
Wireshark · Packet 7 · DNS_Capture.pcapng

```
> Frame 7: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{1D4E0B16-3097-4F20-AFB4-313DFF270882}, id 0
> Ethernet II, Src: AzureWav_95:a1:61 (80:91:33:95:a1:61), Dst: TendaTec_71:8d:d8 (50:2b:73:71:8d:d8)
> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.0.1
v User Datagram Protocol, Src Port: 50859, Dst Port: 53
    Source Port: 50859
    Destination Port: 53
    Length: 44
    Checksum: 0xc0ef [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  > [Timestamps]
    UDP payload (36 bytes)
v Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > en.wikiversity.org: type A, class IN
    [Response In: 8]
```

DNS Quary

DNS response

User and Destination IP along with port number

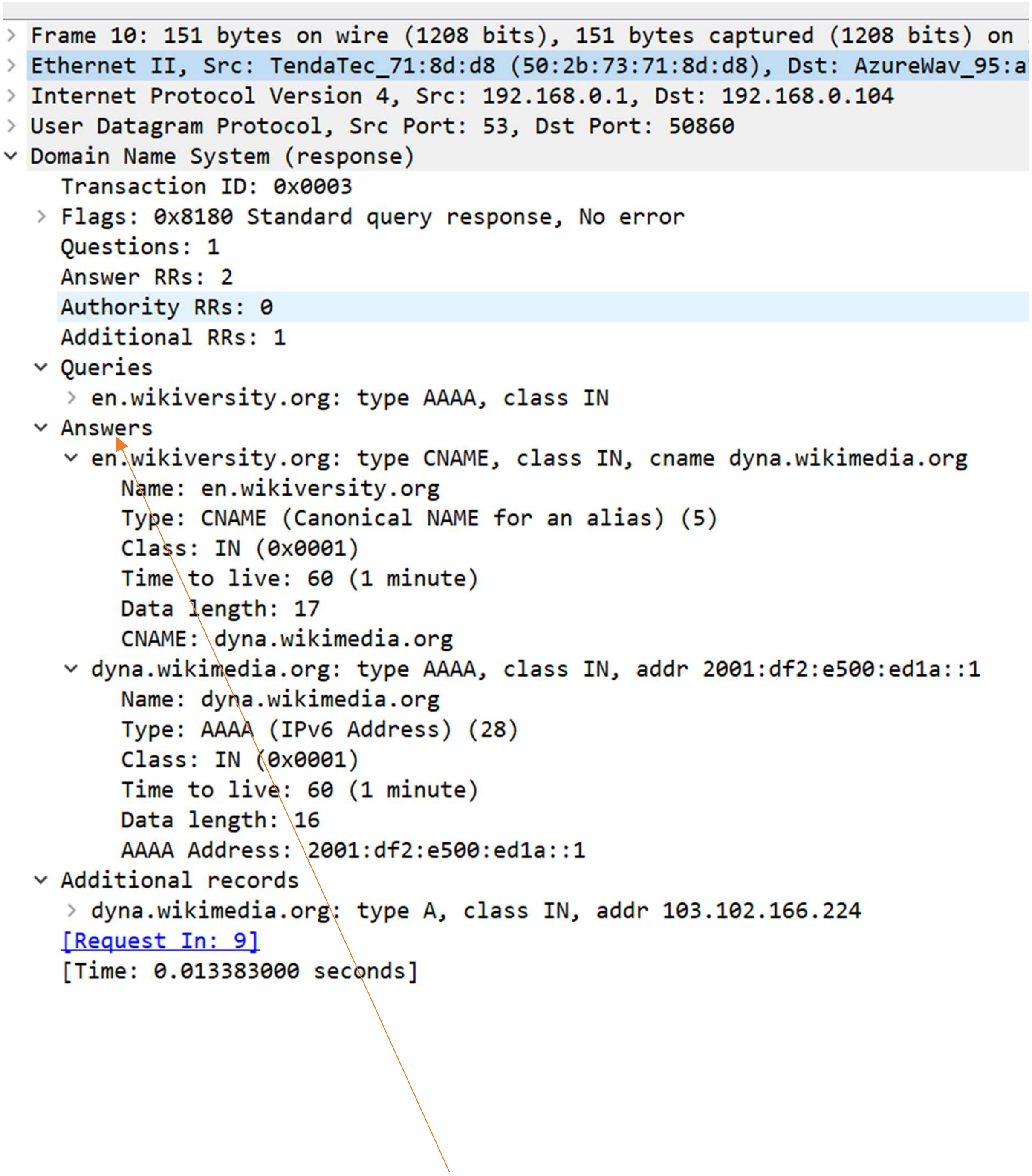


```
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 109
  Identification: 0x1fe7 (8167)
> Flags: 0x00
  Fragment Offset: 0
  Time to Live: 64
  Protocol: UDP (17)
  Header Checksum: 0xd8df [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.0.1
  Destination Address: 192.168.0.104
User Datagram Protocol, Src Port: 53, Dst Port: 50859
  Source Port: 53
  Destination Port: 50859
  Length: 89
  Checksum: 0xb5a6 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 1]
> [Timestamps]
  UDP payload (81 bytes)
Domain Name System (response)
  Transaction ID: 0x0002
> Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 2
  Authority RRs: 0
  Additional RRs: 0
v Queries
  > en.wikiversity.org: type A, class IN
v Answers
  > en.wikiversity.org: type CNAME, class IN, cname dyna.wikimedia.org
  > dyna.wikimedia.org: type A, class IN, addr 103.102.166.224
  [Request In: 7]
  [Time: 0.014894000 seconds]
```

response

3)

Yes in the below picture there are multiple response one is type AAAA and other is type CNAME



```
> Frame 10: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits) on
> Ethernet II, Src: TendaTec_71:8d:d8 (50:2b:73:71:8d:d8), Dst: AzureWav_95:a
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.104
> User Datagram Protocol, Src Port: 53, Dst Port: 50860
v Domain Name System (response)
    Transaction ID: 0x0003
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 1
  v Queries
    > en.wikiversity.org: type AAAA, class IN
  v Answers
    v en.wikiversity.org: type CNAME, class IN, cname dyna.wikimedia.org
        Name: en.wikiversity.org
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 60 (1 minute)
        Data length: 17
        CNAME: dyna.wikimedia.org
    v dyna.wikimedia.org: type AAAA, class IN, addr 2001:df2:e500:ed1a::1
        Name: dyna.wikimedia.org
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
        Time to live: 60 (1 minute)
        Data length: 16
        AAAA Address: 2001:df2:e500:ed1a::1
  v Additional records
    > dyna.wikimedia.org: type A, class IN, addr 103.102.166.224
    [Request In: 9]
    [Time: 0.013383000 seconds]
```

Responces by DNS