# Assignment 2

## Part A – Exploring DNS using nslookup, ipconfig and Wireshark

### nslookup

1. I ran the command **`nslookup www.baidu.com`** which is the most popular search engine in China. The IP address returned was **`103.235.46.39`** which I confirmed was in Asia using [www.infosniper.net](www.infosniper.net)

```
C:\Users\charl>nslookup www.baidu.com
Server:  node-1w7jr9n24twqzs2cg5ed4tjkj.ipv6.telus.net
Address:  2001:568:ff09:10c::53

Non-authoritative answer:
Name:    www.a.shifen.com
Address:  103.235.46.39
Aliases:  www.baidu.com
```

2. I ran **`nslookup -type=NS www.ox.ac.uk`** for to look for the authoritative DNS server for Oxford University. The primary name server returned is **`nighthawk.dns.ox.ac.uk`**

```
C:\Users\charl>nslookup -type=NS www.ox.ac.uk
Server:  node-1w7jr9n24twqzs2cg5ed4tjkj.ipv6.telus.net
Address:  2001:568:ff09:10c::53

ox.ac.uk
        primary name server = nighthawk.dns.ox.ac.uk
        responsible mail addr = hostmaster.ox.ac.uk
        serial  = 2016030372
        refresh = 3600 (1 hour)
        retry   = 1800 (30 mins)
        expire  = 1209600 (14 days)
        default TTL = 900 (15 mins)
```

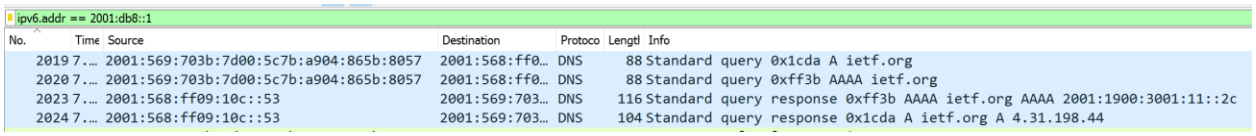
3. I ran the command **`nslookup mail.yahoo.com ox.ac.uk`**. The DNS request timed out, but returned the address **`129.67.242.154`** first. I then ran **`nslookup 129.67.242.154`** to learn the name of the server which returned **`aurochs-web-154.nsms.ox.ac.uk`**.

```
C:\Users\charl>nslookup mail.yahoo.com ox.ac.uk
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  129.67.242.154

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
```

```
C:\Users\charl>nslookup 129.67.242.154
Server:  node-1w7jr9n24twqzs2cg5ed4tjkj.ipv6.telus.net
Address:  2001:568:ff09:10c::53

Name:    aurochs-web-154.nsms.ox.ac.uk
Address:  129.67.242.154
```

## Tracing DNS with Wireshark

4. The DNS query and responses were sent over UDP.




5. The destination port of the DNS *query* and the source port of the *response* are both port **53**.

*Query:*

```
> Frame 2019: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface 0
> Ethernet II, Src: Microsof_df:7d:df (b4:ae:2b:df:7d:df), Dst: Actionte_e0:ec:98 (a8:39:44:e0:ec:98)
> Internet Protocol Version 6, Src: 2001:569:703b:7d00:5c7b:a904:865b:8057, Dst: 2001:568:ff09:10c::53
v User Datagram Protocol, Src Port: 62187 (62187), Dst Port: 53 (53)
    Source Port: 62187
    Destination Port: 53
    Length: 34
  > Checksum: 0x03ae [validation disabled]
    [Stream index: 21]
v Domain Name System (query)
    [Response In: 2024]
    Transaction ID: 0x1cda
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
```

*Response:*

```
> Frame 2023: 116 bytes on wire (928 bits), 116 bytes captured (928 bits) on interface 0
> Ethernet II, Src: Actionte_e0:ec:98 (a8:39:44:e0:ec:98), Dst: Microsof_df:7d:df (b4:ae:2b:df:7d:df)
> Internet Protocol Version 6, Src: 2001:568:ff09:10c::53, Dst: 2001:569:703b:7d00:5c7b:a904:865b:8057
v User Datagram Protocol, Src Port: 53 (53), Dst Port: 57133 (57133)
    Source Port: 53
    Destination Port: 57133
    Length: 62
  > Checksum: 0x83b4 [validation disabled]
    [Stream index: 22]
v Domain Name System (response)
    [Request In: 2020]
    [Time: 0.040957000 seconds]
    Transaction ID: 0xff3b
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  > Answers
```

6. The DNS query message is sent to IP address **2001:568:ff09:10c::53**. I ran the command **ipconfig /all** and identified the DNS Servers, the first listed among them is indeed the same as the above IP address.

```
   DNS Servers . . . . . . . . . . . : 2001:568:ff09:10c::53
                                       2001:568:ff09:10d::53
                                       192.168.1.254
                                       75.153.176.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

7. Both a Type A query and a Type AAAA query were sent. Neither query contains an answer.

| No. | Time | Sour | Dest | Protoco | Lengtl | Info |
|---|---|---|---|---|---|---|
| 2019 | 7.… | 20… | 20… | DNS | 88 | Standard query 0x1cda A ietf.org |
| 2020 | 7.… | 20… | 20… | DNS | 88 | Standard query 0xff3b AAAA ietf.org |
| 2023 | 7.… | 20… | 20… | DNS | 116 | Standard query response 0xff3b AAAA ietf.org AAAA 2001:1900:3001:11::2c |
| 2024 | 7.… | 20… | 20… | DNS | 104 | Standard query response 0x1cda A ietf.org A 4.31.198.44 |

```
> Frame 2020: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface 0
> Ethernet II, Src: Microsof_df:7d:df (b4:ae:2b:df:7d:df), Dst: Actionte_e0:ec:98 (a8:39:44:e0:ec:98)
> Internet Protocol Version 6, Src: 2001:569:703b:7d00:5c7b:a904:865b:8057, Dst: 2001:568:ff09:10c::53
> User Datagram Protocol, Src Port: 57133 (57133), Dst Port: 53 (53)
v Domain Name System (query)
    [Response In: 2023]
    Transaction ID: 0xff3b
  v 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
```

8. Both the Type A response and the Type AAAA response contained one answer. Both contained the Name, Type, Class, TTL, Length, and Address. However, the Type A response contained the IPv4 address and the Type AAAA response contained the IPv6 address.

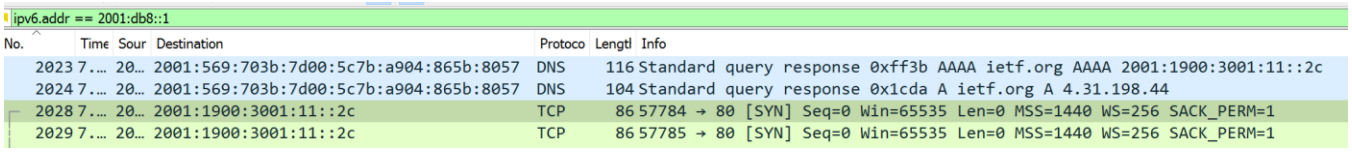
*Type A*

```
v Domain Name System (response)
    [Request In: 2019]
    [Time: 0.041717000 seconds]
    Transaction ID: 0x1cda
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > ietf.org: type A, class IN
  v Answers
    v ietf.org: type A, class IN, addr 4.31.198.44
        Name: ietf.org
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 1800
        Data length: 4
        Address: 4.31.198.44
```

*Type AAAA*

```
v Domain Name System (response)
    [Request In: 2020]
    [Time: 0.040957000 seconds]
    Transaction ID: 0xff3b
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > ietf.org: type AAAA, class IN
  v Answers
    v ietf.org: type AAAA, class IN, addr 2001:1900:3001:11::2c
        Name: ietf.org
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
        Time to live: 1800
        Data length: 16
        AAAA Address: 2001:1900:3001:11::2c
```

9. The TCP SYN packet sent by my host was to the IDv6 address provided in the Type AAAA response answer.




10. Additional DNS queries are not issued for each HTTP request because we have cached the address.

11. The destination port for the DNS query message is port number 53, and the source of the response message as also port 53.

12. The query is sent to IP address **2001:568:ff09:10c::53**, this is the address of my local DNS server.

13. Similarly as above, both a Type A and a Type AAAA query is sent. Neither query contains an answer.

14. The response to the Type A query contains 3 answers, the response to the Type AAAA query contains 4 answers. The first answer to the Type A query has the *Name* **www.mit.edu** and *CNAME* **www.mit.edu.edgekey.net**, the second answer has the *Name* **www.mit.edu.edgekey.net** and the *CNAME* **e9566.dscb.akamaiedge.net**, the third answer has the *Name* **e9566.dscb.akamaiedge.net** and the *Address* **23.14.160.128**. The Type AAAA query follows a similar process but returns the IPv6 address.

15. *Type A*

```
Domain Name System (response)
  [Request In: 38]
  [Time: 0.033781000 seconds]
  Transaction ID: 0x0004
  Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 3
  Authority RRs: 0
  Additional RRs: 0
  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: 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: 1
      Data length: 24
      CNAME: e9566.dscb.akamaiedge.net
    e9566.dscb.akamaiedge.net: type A, class IN, addr 23.14.160.128
      Name: e9566.dscb.akamaiedge.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 20
      Data length: 4
      Address: 23.14.160.128
```

*Type AAAA*

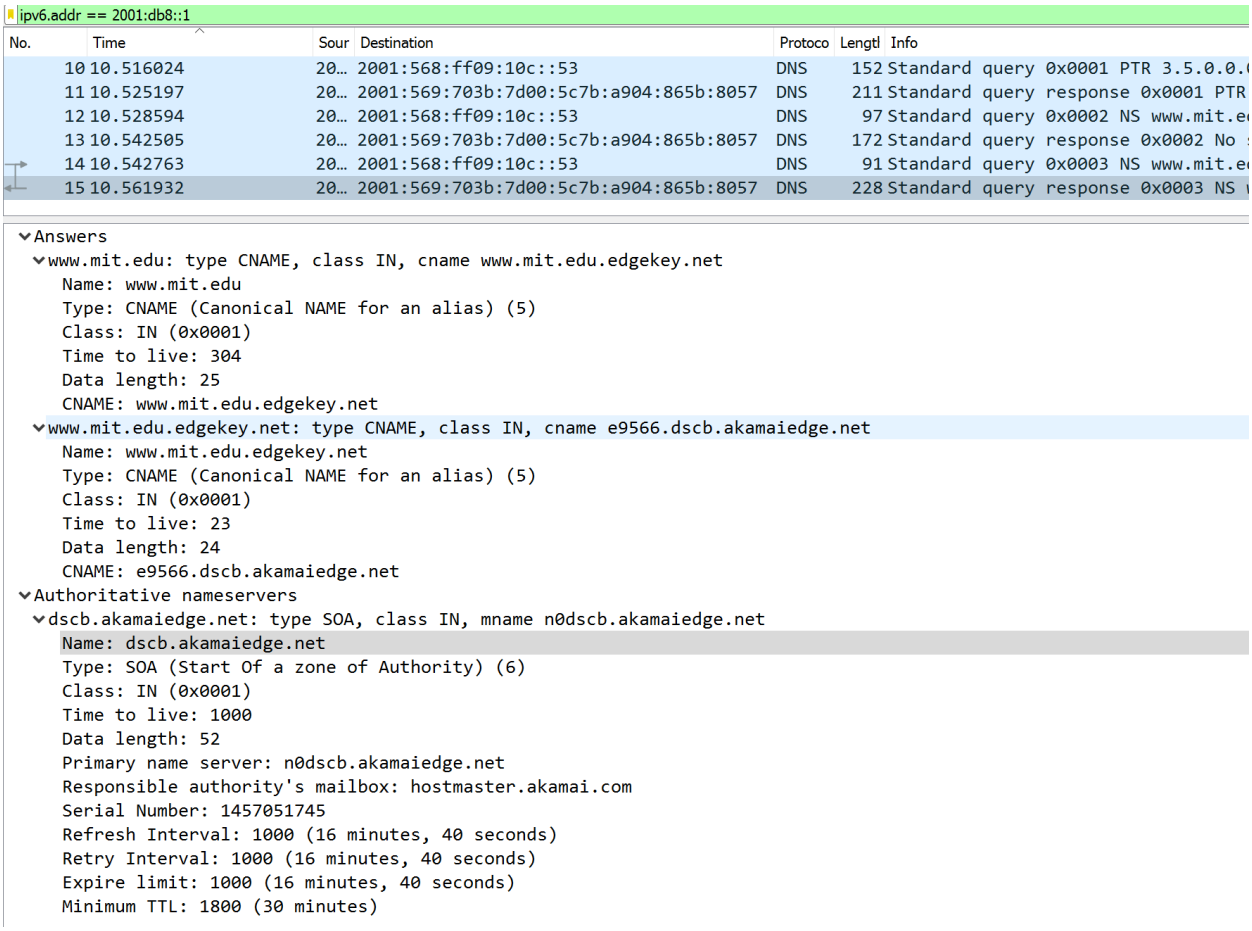
```
Domain Name System (response)
  [Request In: 40]
  [Time: 0.049721000 seconds]
  Transaction ID: 0x0005
 Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 4
  Authority RRs: 0
  Additional RRs: 0
 Queries
 Answers
  www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
    Name: www.mit.edu
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 925
    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: 12
    Data length: 24
    CNAME: e9566.dscb.akamaiedge.net
  e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2600:1409:a:18c::255e
    Name: e9566.dscb.akamaiedge.net
    Type: AAAA (IPv6 Address) (28)
    Class: IN (0x0001)
    Time to live: 20
    Data length: 16
    AAAA Address: 2600:1409:a:18c::255e
  e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2600:1409:a:193::255e
    Name: e9566.dscb.akamaiedge.net
    Type: AAAA (IPv6 Address) (28)
    Class: IN (0x0001)
    Time to live: 20
    Data length: 16
    AAAA Address: 2600:1409:a:193::255e
```

16. The destination IP address of the query message is **`2001:568:ff09:10c::53`**, which is the address of my default local DNS server.

17. It is a type **NS** query and does not contain any answers.

18. The authoritative nameserver provided by the response is **n0dscb.akamaiedge.net**, it does not provide the IP address.

19.



ipv6.addr == 2001:db8::1

| No. | Time | Sour | Destination | Protoco | Lengtl | Info |
|---|---|---|---|---|---|---|
| 10 | 10.516024 | 20… | 2001:568:ff09:10c::53 | DNS | 152 | Standard query 0x0001 PTR 3.5.0.0.( |
| 11 | 10.525197 | 20… | 2001:569:703b:7d00:5c7b:a904:865b:8057 | DNS | 211 | Standard query response 0x0001 PTR |
| 12 | 10.528594 | 20… | 2001:568:ff09:10c::53 | DNS | 97 | Standard query 0x0002 NS www.mit.e |
| 13 | 10.542505 | 20… | 2001:569:703b:7d00:5c7b:a904:865b:8057 | DNS | 172 | Standard query response 0x0002 No |
| 14 | 10.542763 | 20… | 2001:568:ff09:10c::53 | DNS | 91 | Standard query 0x0003 NS www.mit.e |
| 15 | 10.561932 | 20… | 2001:569:703b:7d00:5c7b:a904:865b:8057 | DNS | 228 | Standard query response 0x0003 NS |

```
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: 304
    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: 23
    Data length: 24
    CNAME: e9566.dscb.akamaiedge.net
Authoritative nameservers
  dscb.akamaiedge.net: type SOA, class IN, mname n0dscb.akamaiedge.net
    Name: dscb.akamaiedge.net
    Type: SOA (Start Of a zone of Authority) (6)
    Class: IN (0x0001)
    Time to live: 1000
    Data length: 52
    Primary name server: n0dscb.akamaiedge.net
    Responsible authority's mailbox: hostmaster.akamai.com
    Serial Number: 1457051745
    Refresh Interval: 1000 (16 minutes, 40 seconds)
    Retry Interval: 1000 (16 minutes, 40 seconds)
    Expire limit: 1000 (16 minutes, 40 seconds)
    Minimum TTL: 1800 (30 minutes)
```

20. The DNS queries relating to *bitsy.mit.edu* are sent to the IP address **2001:568:ff09:10d::53**, like before this is one of my DNS servers. The DNS queries relating to *www.aiit.or.kt* are sent to **18.72.0.3**.

| | | | | | | |
|---|---|---|---|---|---|---|
| 59 | 37… | 20… | 2001:568:ff09:10c::53 | DNS | 93 | Standard query 0x4031 A bitsy.mit.edu |
| 60 | 37… | 20… | 2001:568:ff09:10c::53 | DNS | 93 | Standard query 0x4163 AAAA bitsy.mit.edu |
| 61 | 37… | 20… | 2001:568:ff09:10d::53 | DNS | 93 | Standard query 0x4031 A bitsy.mit.edu |
| 62 | 37… | 20… | 2001:568:ff09:10d::53 | DNS | 93 | Standard query 0x4163 AAAA bitsy.mit.edu |
| 63 | 37… | 20… | 2001:569:703b:7d00:5c7b:a904:865b:8057 | DNS | 158 | Standard query response 0x4163 AAAA bitsy.mit.edu SOA use2.akam.net |
| 64 | 37… | 20… | 2001:569:703b:7d00:5c7b:a904:865b:8057 | DNS | 109 | Standard query response 0x4031 A bitsy.mit.edu A 18.72.0.3 |
| 65 | 37… | 20… | 2001:569:703b:7d00:5c7b:a904:865b:8057 | DNS | 109 | Standard query response 0x4031 A bitsy.mit.edu A 18.72.0.3 |
| 66 | 37… | 19… | 18.72.0.3 | DNS | 82 | Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa |
| 67 | 37… | 20… | 2001:569:703b:7d00:5c7b:a904:865b:8057 | DNS | 158 | Standard query response 0x4163 AAAA bitsy.mit.edu SOA use2.akam.net |
| 69 | 39… | 19… | 18.72.0.3 | DNS | 80 | Standard query 0x0002 NS www.aiit.or.kr.telus |
| 75 | 41… | 19… | 18.72.0.3 | DNS | 74 | Standard query 0x0003 NS www.aiit.or.kr |

21. Observing the last query listed, it is an NS type message containing no answers.

22. Unfortunately, I never received a response message from *www.aiit.or.kr* because the nslookup would always time out before a response, even when I increased the timeout.

```
C:\Users\charl>nslookup -timeout=30 www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 30 seconds.
Server:  UnKnown
Address:  18.72.0.3

DNS request timed out.
    timeout was 30 seconds.
DNS request timed out.
    timeout was 30 seconds.
DNS request timed out.
    timeout was 30 seconds.
DNS request timed out.
    timeout was 30 seconds.
*** Request to UnKnown timed-out

C:\Users\charl>
```

23. As you can see, I don't receive a response from *www.aiit.or.kr*

| | | | | | | |
|---|---|---|---|---|---|---|
| 59 | 37… | 20… | 2001:568:ff09:10c::53 | DNS | 93 | Standard query 0x4031 A bitsy.mit.edu |
| 60 | 37… | 20… | 2001:568:ff09:10c::53 | DNS | 93 | Standard query 0x4163 AAAA bitsy.mit.edu |
| 61 | 37… | 20… | 2001:568:ff09:10d::53 | DNS | 93 | Standard query 0x4031 A bitsy.mit.edu |
| 62 | 37… | 20… | 2001:568:ff09:10d::53 | DNS | 93 | Standard query 0x4163 AAAA bitsy.mit.edu |
| 63 | 37… | 20… | 2001:569:703b:7d00:5c7b:a904:865b:8057 | DNS | 158 | Standard query response 0x4163 AAAA bitsy.mit.edu SOA use2.akam.net |
| 64 | 37… | 20… | 2001:569:703b:7d00:5c7b:a904:865b:8057 | DNS | 109 | Standard query response 0x4031 A bitsy.mit.edu A 18.72.0.3 |
| 65 | 37… | 20… | 2001:569:703b:7d00:5c7b:a904:865b:8057 | DNS | 109 | Standard query response 0x4031 A bitsy.mit.edu A 18.72.0.3 |
| 66 | 37… | 19… | 18.72.0.3 | DNS | 82 | Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa |
| 67 | 37… | 20… | 2001:569:703b:7d00:5c7b:a904:865b:8057 | DNS | 158 | Standard query response 0x4163 AAAA bitsy.mit.edu SOA use2.akam.net |
| 69 | 39… | 19… | 18.72.0.3 | DNS | 80 | Standard query 0x0002 NS www.aiit.or.kr.telus |
| 75 | 41… | 19… | 18.72.0.3 | DNS | 74 | Standard query 0x0003 NS www.aiit.or.kr |

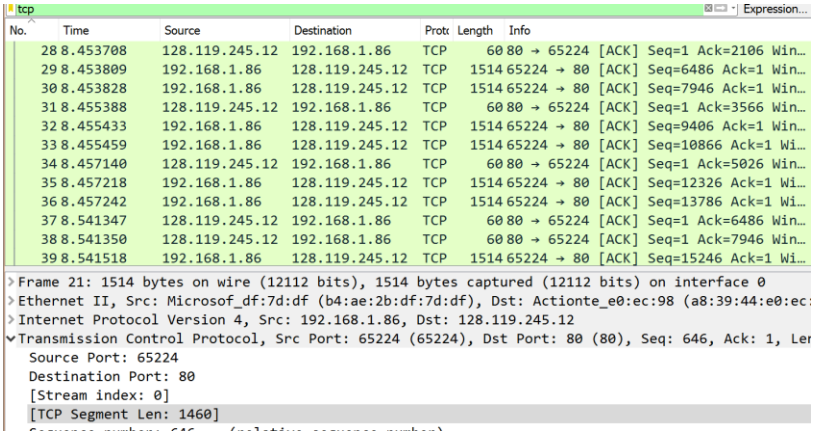
# Part B – Exploring TCP using Wireshark

## 2. A first look at the captured trace

1. The source of the transferred file in the provided trace was IP address **192.168.1.102**, port **1161**.

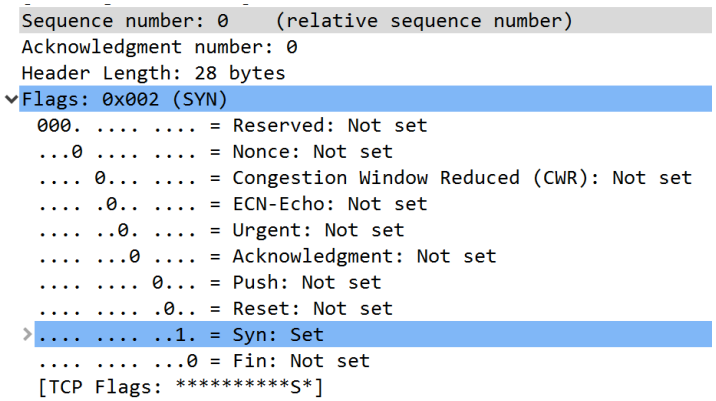
2. The destination of the transferred file was IP address **128.119.245.12**, port **80**.

3. In my trace, the source was **192.168.1.86**, port **65224**.




## 3. TCP Basics

4. The sequence number is **0**, but this has been noted **"relative sequence number"**. I could not find any "absolute sequence number". This segment is identified as a SYN segment because the flags have been set to 0x002, indicating that the "Syn" flag is set.



**5.** The sequence number of the SYNACK segment is **0** and the acknowledgement number is **1**.

The acknowledgement number has been set to **1** because the server successfully received segment **0** (the SYN segment) and is now expecting a segment with the sequence number **1**.

This segment is identified as a SYNACK segment because both the Syn and Acknowledgement flags are set, ie. the flags have a value of 0x012.

**6.** TCP segment with the data containing the **POST /ethereal-labs/lab3-1-reply.htm HTTP/1.1** command has the sequence number **1**.

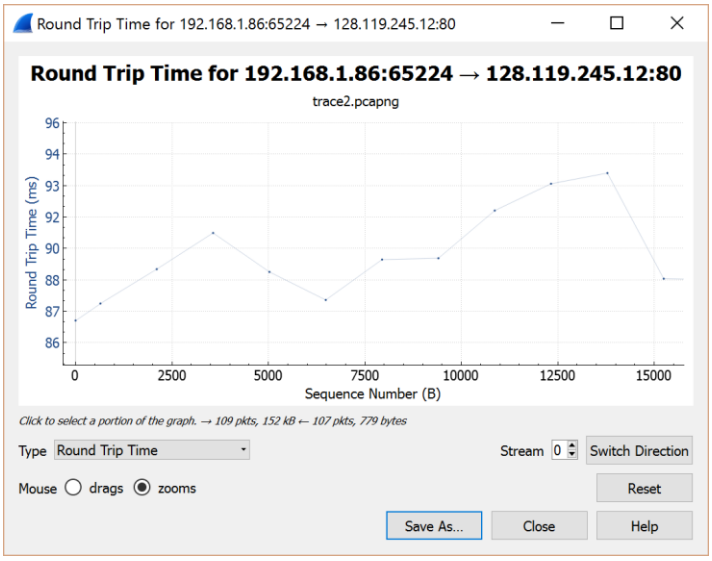
**7.** After the first three segments (SYN, SYNACK, ACK), starting with the sequence number **1**, the conversation with data-carrying segments goes as follows:

EstimatedRTT calculated using the formula:

```
alpha = 1/8 = 0.125
EstimatedRTT = (1-alpha)*EstimatedRTT + alpha*SampleRTT
```

And taking the initial EstimatedRTT to be equal to the initial SampleRTT

| Sequence Number | Corresponding ACK Number | Time Data Segment Sent | Time ACK Received | SampleRTT | EstimatedRTT |
|---|---|---|---|---|---|
| 1 | 646 | 8.365824 | 8.45383 | 0.088006 | **0.088006** |
| 646 | 2106 | 8.366337 | 8.453708 | 0.087371 | **0.08792663** |
| 2106 | 3566 | 8.366377 | 8.455388 | 0.089011 | **0.08806217** |
| 3566 | 5026 | 8.366401 | 8.45714 | 0.090739 | **0.08839678** |
| 5026 | 6486 | 8.452468 | 8.541347 | 0.088879 | **0.08845705** |
| 6486 | 7946 | 8.453809 | 8.54135 | 0.087541 | **0.08834255** |

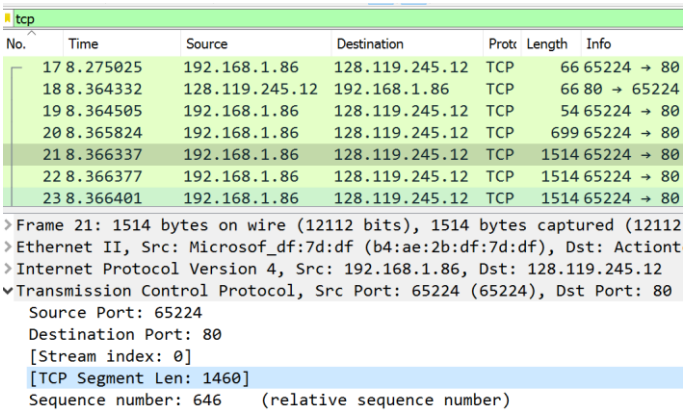



Outputting the RTT using Wireshark's TCP Stream Graph tool agrees with my calculated SampleRTT.

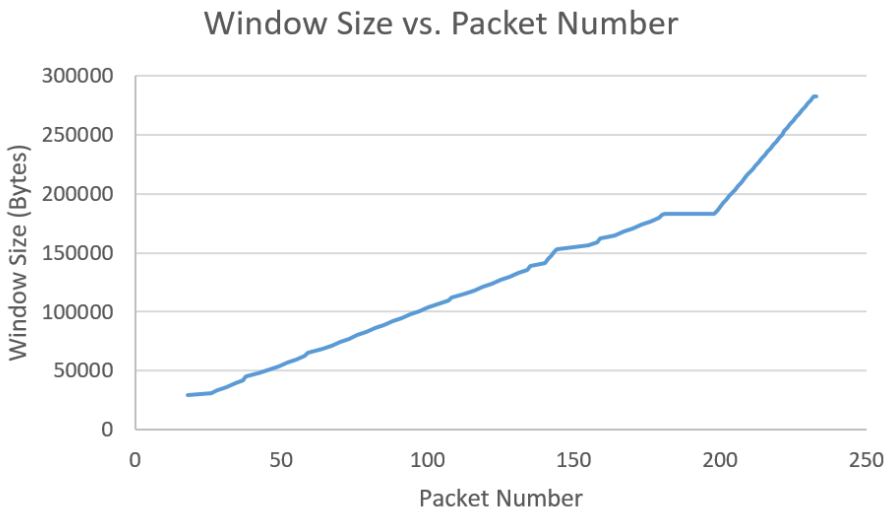
**8.**

| Sequence Number | TCP Segment Length |
|---|---|
| 1 | 645 |
| 646 | 1460 |
| 2106 | 1460 |
| 3566 | 1460 |
| 5026 | 1460 |
| 6486 | 1460 |

**Note:** This value was taken from the TCP Segment Length field in the TCP segment, not the length column in the traced packets stack. See the figure below.




**9.** In the SYNACK response from receiver, the TCP segment advertises a window size of **29200** bytes which is the smallest window size advertised in the entire conversation. The window size decreases once throughout the conversation from **182400** to **183296**, indicating that the sender is once throttled via flow control due to lack of buffer space.



**10.** I exported the trace to Excel and all recorded packets sent from the client have unique sequence numbers, indicating that **no TCP segments are retransmitted**.

**11.** The amount of data acknowledged by an ACK segment is the difference between that segment's acknowledgement number and the acknowledgment number of the previous ACK segment.

Using Excel I analyzed the difference between acknowledgement numbers. The vast majority of ACK segments acknowledge **1460** bytes, however, there was once instance of the ACK segment acknowledging 1296 bytes, once instance of it acknowledging 645 bytes, and one instance of it acknowledging **2920** bytes. Because 2920 is double 1460, that leads me to believe when 2920 bytes are acknowledged the receiver is indeed acknowledging every other segment.

**12.** You can calculate the throughput by dividing all the data transmitted in the conversation by the time elapsed in the conversation. In my exchange with the server I transmitted 166003 bytes in 0.622343 seconds, giving my an average throughput of **266.7 Kb/sec**

Using Wireshark's TCP Stream Graph tool, I outputted the throughput throughout the conversation which seems to agree.