University of Antwerp
Faculty of Applied Engineering

Sten Hulsbergen - 20242689

Session 5

1.

- DNS

```
58 4.943188  143.129.40.79      143.169.252.201     DNS      108 Standard query 0x494e A course-3networkarchitecture.ei.fti.uantwerpen.be
59 4.943929  143.169.252.201    143.129.40.79       DNS      124 Standard query response 0x494e A course-3networkarchitecture.ei.fti.uantwerpen.be A 143.129.43.250
60 5.007019  143.129.40.79      143.169.252.201     DNS      108 Standard query 0x7d2c A course-3networkarchitecture.ei.fti.uantwerpen.be
```

- HTTP

```
 826 8.024724  143.129.40.79      143.129.43.250     HTTP      548 GET / HTTP/1.1
 830 8.030398  143.129.43.250     143.129.40.79      HTTP      518 HTTP/1.1 302 FOUND  (text/html)
 835 8.039844  143.129.40.79      143.129.43.250     HTTP      580 GET /student_number?redirection=index HTTP/1.1
 838 8.045136  143.129.43.250     143.129.40.79      HTTP     1050 HTTP/1.1 200 OK  (text/html)
 852 8.136041  143.129.40.79      143.129.43.250     HTTP      557 GET /favicon.ico HTTP/1.1
 859 8.141867  143.129.43.250     143.129.40.79      HTTP      439 HTTP/1.1 404 NOT FOUND  (text/html)
1090 18.256714 143.129.40.79      143.129.43.250     HTTP      882 POST /student_number HTTP/1.1  (application/x-www-form-urlencoded)
1093 18.260913 143.129.43.250     143.129.40.79      HTTP     1121 HTTP/1.1 200 OK  (text/html)
1194 26.261377 143.129.40.79      143.129.43.250     HTTP      864 POST /student_number HTTP/1.1  (application/x-www-form-urlencoded)
1195 26.266034 143.129.43.250     143.129.40.79      HTTP      494 HTTP/1.1 302 FOUND  (text/html)
1202 26.271169 143.129.40.79      143.129.43.250     HTTP      679 GET /?student_number=20242689 HTTP/1.1
1204 26.275614 143.129.43.250     143.129.40.79      HTTP      980 HTTP/1.1 200 OK  (text/html)
1271 29.145878 143.129.40.79      143.129.43.250     HTTP      672 GET /session5/?student_number=20242689 HTTP/1.1
1272 29.150171 143.129.43.250     143.129.40.79      HTTP      861 HTTP/1.1 200 OK  (text/html)
```

- TCP

```
  87 5.023758  143.129.40.79      143.129.43.250     TCP       66 50926 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 200 5.276115  143.129.40.79      143.129.43.250     TCP       66 50930 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 530 6.034754  143.129.40.79      143.129.43.250     TCP       66 [TCP Retransmission] 50926 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 728 6.286637  143.129.40.79      143.129.43.250     TCP       66 [TCP Retransmission] 50930 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 823 8.022000  143.129.40.79      143.129.43.250     TCP       66 50936 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 825 8.024435  143.129.40.79      143.129.43.250     TCP       54 50936 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
 836 8.043847  143.129.40.79      143.129.43.250     TCP       66 [TCP Retransmission] 50926 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 843 8.091895  143.129.40.79      143.129.43.250     TCP       54 50936 → 80 [ACK] Seq=1021 Ack=1461 Win=262656 Len=0
 898 8.186581  143.129.40.79      143.129.43.250     TCP       54 50936 → 80 [ACK] Seq=1524 Ack=1846 Win=262400 Len=0
 903 8.296589  143.129.40.79      143.129.43.250     TCP       66 [TCP Retransmission] 50930 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 964 12.058607 143.129.40.79      143.129.43.250     TCP       66 [TCP Retransmission] 50926 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 975 12.301301 143.129.40.79      143.129.43.250     TCP       66 [TCP Retransmission] 50930 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1099 18.303671 143.129.40.79      143.129.43.250     TCP       54 50936 → 80 [ACK] Seq=2352 Ack=2913 Win=261120 Len=0
1128 20.060212 143.129.40.79      143.129.43.250     TCP       66 [TCP Retransmission] 50926 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1137 20.311779 143.129.40.79      143.129.43.250     TCP       66 [TCP Retransmission] 50930 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1212 26.317774 143.129.40.79      143.129.43.250     TCP       54 50936 → 80 [ACK] Seq=3787 Ack=4279 Win=261632 Len=0
1279 29.202295 143.129.40.79      143.129.43.250     TCP       54 50936 → 80 [ACK] Seq=4405 Ack=5086 Win=262656 Len=0
```

Layer	Protocol
Application	HTTP, DNS
Transport	TCP
Network	
Link	
Physical	

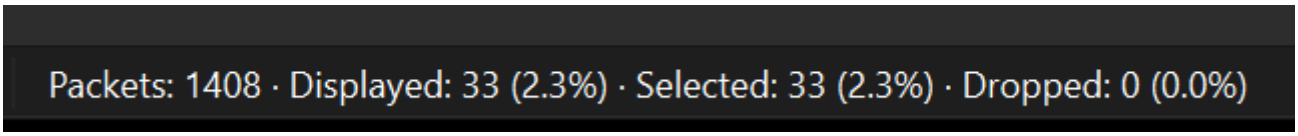
2.

- DNS (**Domain Name System**)
    - Linking an easier readable name, called a domain, to an IP-address of a system or service.
- HTTP (**Hypertext Transfer Protocol**)
    - Used in communication between webserver and webbrowser. Data can be accessed and send with it.
- TCP (**Transmission Control Protocol**)
    - Used in datatransfer on the internet in the form of a stream of data, like a large download. To be assured the datatransfer is complete, this will be used.

3.

First the DNS-resolver is being spoken to, followed up by the communication.

In my case, when filtering the destination and source address, out of the 1408 packets there were 33 packets exchanged in my session.



4.

The IP-address in Wireshark is `143.129.43.250`. After installing *dnsutils* with `sudo apt install dnsutils` it is possible to do `dnslookup course-3networkarchitecture.ei.fti.uantwerpen.be` which resulted in the same IP-address `143.129.43.250`.

```
s0242689@3networkarchitecture-s0242689:~$ nslookup course-3networkarchitecture.ei.fti.uantwerpen.be
Server:         143.169.252.201
Address:        143.169.252.201#53

Non-authoritative answer:
Name:   course-3networkarchitecture.ei.fti.uantwerpen.be
Address: 143.129.43.250
```