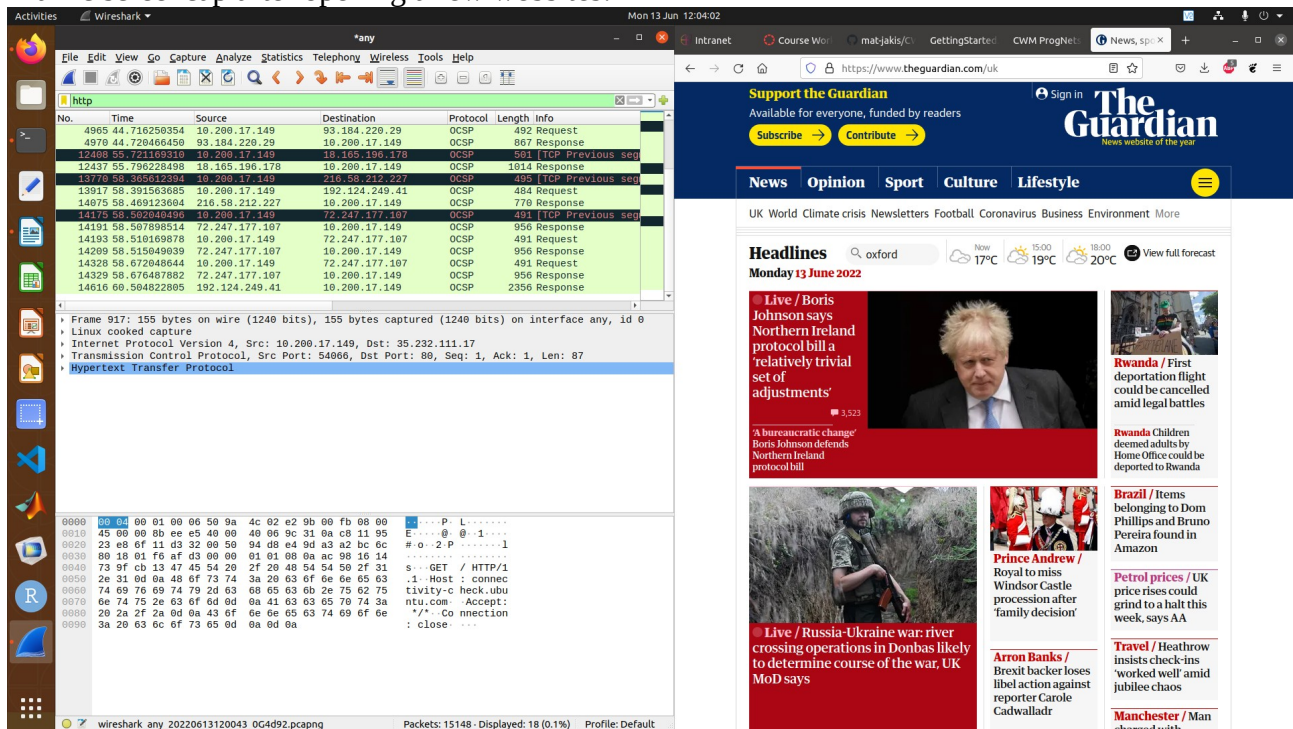


Assignment 1
Mateusz Zorga
CWM ProgNet TT22

1. After using Wireshark on the Ethernet cable, the only traffic is “Standard query” packets sent every 20 seconds and responses to them.
2. HTTP traffic is seen when a new website is opened. However, if the website has already been opened recently, it will use a cached version instead and the protocol is not sent.

Traffic screencap after opening a few websites:



- ### 3. RasPi captured traffic screencap:

```

root@kali:~# $ tcpdump -c captured.pcap
reading from file captured.pcap, link-type EN10MB (Ethernet), snapshot length 262144
13:53:45.997369 IP6 fe80::6c1b:c07b:e79c:f73e.mdns > ff02::fb.mdns: 0* [0q] 2/0/0 (Cache flush) PTR engs-labb13-30498.local., (Cache flush) AAAA fe80::6c1b:c07b:e79c:f73e (149)
13:53:45.997511 IP 192.168.10.1.mdns > 224.0.0.251.mdns: 0* [0q] 4/0/0 (Cache flush) PTR engs-labb13-30498.local., (Cache flush) A 192.168.10.1, (Cache flush) PTR engs-labb13-30498.local., (Cache flush)
AAAA fe80::6c1b:c07b:e79c:f73e (200)
13:53:45.964712 IP6 fe80::6c1b:c07b:e79c:f73e.mdns > ff02::fb.mdns: 0 [2q] [2n] ANY (QM)? e.3.7.f.c.9.7.e.b.7.0.c.b.1.c.6.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. ANY (QM)? engs-labb13-30499.local. (161)
13:53:45.964969 IP 192.168.10.1.mdns > 224.0.0.251.mdns: 0 [3q] [4n] ANY (QM)? e.3.7.f.c.9.7.e.b.7.0.c.b.1.c.6.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. ANY (QM)? engs-labb13-30499.local. ANY (QM)? 1.10.168.192.1.in-addr.arpa. (218)
13:53:46.214576 IP6 fe80::6c1b:c07b:e79c:f73e.mdns > ff02::fb.mdns: 0 [2q] [2n] ANY (QM)? e.3.7.f.c.9.7.e.b.7.0.c.b.1.c.6.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. ANY (QM)? engs-labb13-30499.local. (161)
13:53:46.214713 IP 192.168.10.1.mdns > 224.0.0.251.mdns: 0 [3q] [4n] ANY (QM)? e.3.7.f.c.9.7.e.b.7.0.c.b.1.c.6.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. ANY (QM)? engs-labb13-30499.local. ANY (QM)? 1.10.168.192.1.in-addr.arpa. (218)
13:53:46.466697 IP6 fe80::6c1b:c07b:e79c:f73e.mdns > ff02::fb.mdns: 0 [2q] [2n] ANY (QM)? e.3.7.f.c.9.7.e.b.7.0.c.b.1.c.6.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. ANY (QM)? engs-labb13-30499.local. (161)
13:53:46.466951 IP 192.168.10.1.mdns > 224.0.0.251.mdns: 0 [3q] [4n] ANY (QM)? e.3.7.f.c.9.7.e.b.7.0.c.b.1.c.6.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. ANY (QM)? engs-labb13-30499.local. ANY (QM)? 1.10.168.192.1.in-addr.arpa. (218)
13:53:46.665933 IP 192.168.10.1.mdns > 224.0.0.251.mdns: 0* [0q] 4/0/0 (Cache flush) PTR engs-labb13-30499.local., (Cache flush) A 192.168.10.1, (Cache flush) PTR engs-labb13-30499.local., (Cache flush)
AAAA fe80::6c1b:c07b:e79c:f73e (200)
13:53:46.666007 IP6 fe80::6c1b:c07b:e79c:f73e.mdns > ff02::fb.mdns: 0* [0q] 2/0/0 (Cache flush) PTR engs-labb13-30499.local., (Cache flush) AAAA fe80::6c1b:c07b:e79c:f73e (149)

```

- 4. - Can filter by using both the packet length (64) and computer's IP address. This will only show the python packets sent by the PC
- Packet size is 64 bytes (512 bits)
- Protocol used is UDP

Link to new python file:

<https://github.com/mat-jakis/CWM-ProgNets/blob/main/assignment1/send.py>