Advanced Networks — Laboratory 10

Juliusz Chroboczek

28 April 2025

Exercice 1.

1. On your personal machine, run the command

   ```
   sudo tcpdump -n
   ```

   What is being displayed? Try again with the `-X` option.
2. Run `wireshark`. Select your default network interface (you may use the command `ip route show` to find out what it is), and click « Capture ».
3. Why do we insist on encrypting all network traffic?

Exercice 2. Download the file

```
https://www.irif.fr/~jch/enseignement/sieci/trace.pcap
```

and examine it, first using the command `tcpdump -r -n`, then using `tcpdump -r`, finally using `wireshark`. What application-layer protocol is being used? Was the capture done on the client or the server? Have there been lost packets?

Exercice 3. What happens in each of the following traces? All traces were captured on the machine *A* (is it obvious?).

1.

```
22:45:26.121149 A.32769 > B.www: S 2919412148:2919412148(0) win 5840
                                   <mss 1460,nop,wscale 1>
22:45:26.123055 B.www > A.32769: S 4144006771:4144006771(0)
                                   ack 2919412149 win 65535
                                   <mss 1460,nop,wscale 1>
22:45:26.123120 A.32769 > B.www: . ack 1 win 2920
22:45:26.124144 A.32769 > B.www: P 1:146(145) ack 1 win 2920
22:45:26.130323 B.www > A.32769: . 1:1461(1460) ack 146 win 32850
22:45:26.130402 A.32769 > B.www: . ack 1461 win 4380
22:45:26.130750 B.www > A.32769: . 1461:2921(1460) ack 146 win 32850
```

2.

```
22:45:26.195481 B.www > A.32769: . 74461:75921(1460) ack 146 win 32850
22:45:26.196216 B.www > A.32769: P 75921:77381(1460) ack 146 win 32850
22:45:26.196228 A.32769 > B.www: . ack 77381 win 64240
22:45:26.211281 B.www > A.32769: . 77381:78841(1460) ack 146 win 32850
22:45:26.211772 B.www > A.32769: P 78841:80301(1460) ack 146 win 32850
22:45:26.211783 A.32769 > B.www: . ack 80301 win 64240
```

3.

```
22:45:26.240764 B.www > A.32769: P 127021:128387(1366) ack 146 win 32850
22:45:26.240776 A.32769 > B.www: . ack 128387 win 64240
22:45:26.249437 A.32769 > B.www: F 146:146(0) ack 128387 win 64240
22:45:26.251418 B.www > A.32769: . ack 147 win 32850
22:45:26.251840 B.www > A.32769: F 128387:128387(0) ack 147 win 32850
22:45:26.251871 A.32769 > B.www: . ack 128388 win 64240
```

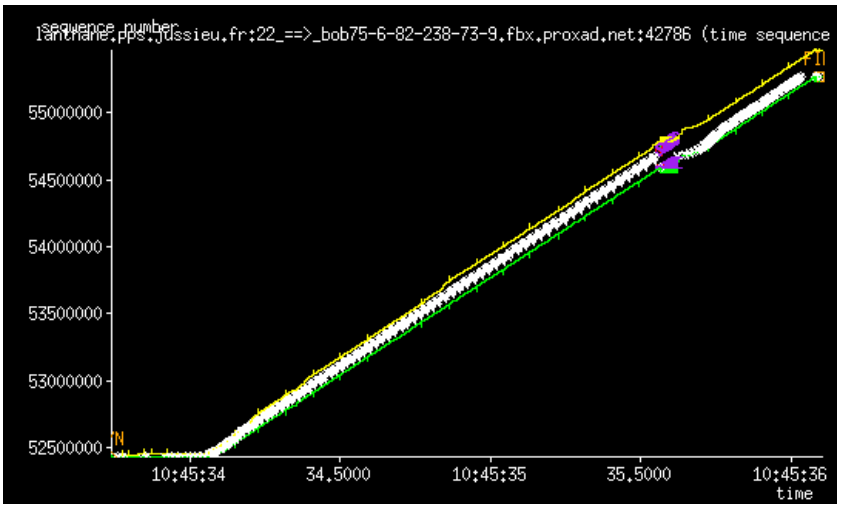
4.

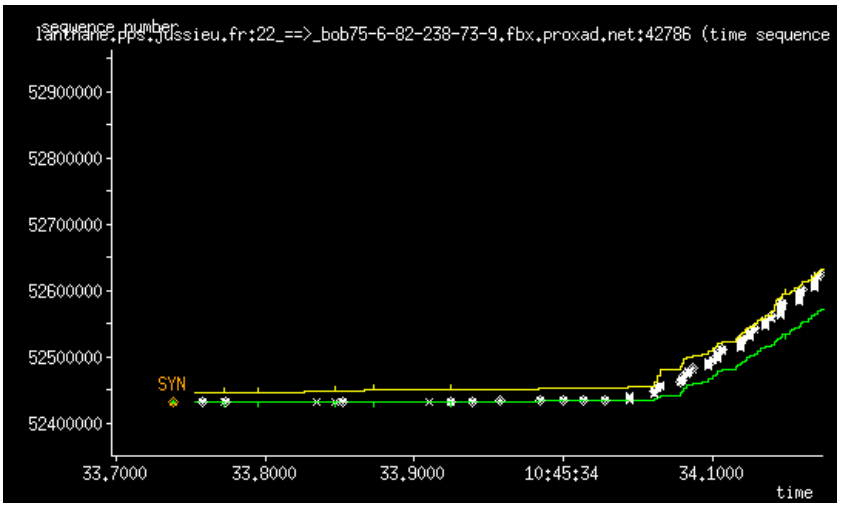
```
22:49:22.739301 A.32775 > C.ssh: . 110064:111524(1460) ack 2336 win 5104
22:49:22.739312 A.32775 > C.ssh: . 111524:112984(1460) ack 2336 win 5104
22:49:22.772816 C.ssh > A.32775: . ack 96924 win 62780
22:49:22.772828 A.32775 > C.ssh: . 112984:114444(1460) ack 2336 win 5104
22:49:22.772838 A.32775 > C.ssh: . 114444:115904(1460) ack 2336 win 5104
22:49:22.773905 C.ssh > A.32775: . ack 99844 win 62780
```

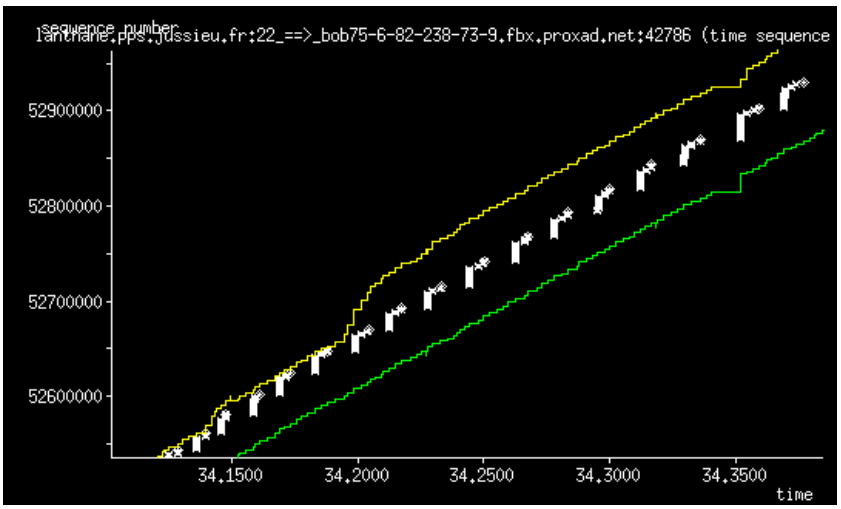
5.

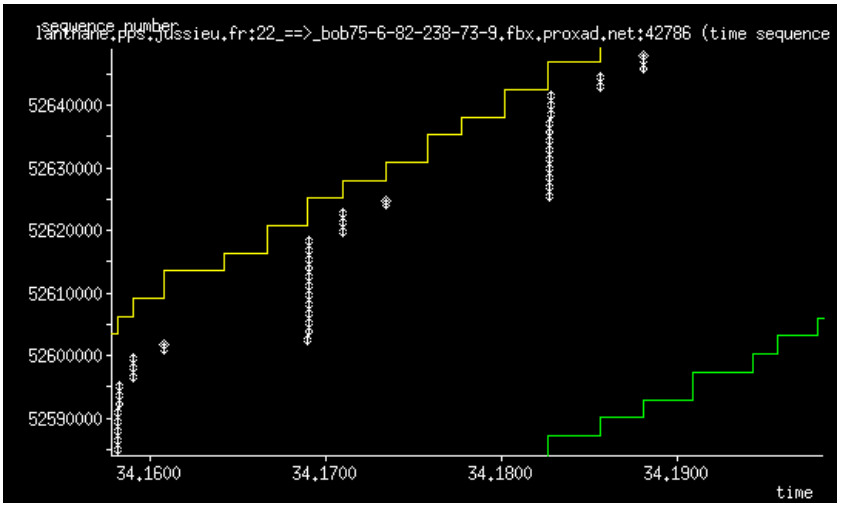
```
22:53:47.759896 D.17775 > A.32782: . 75921:77381(1460) ack 1 win 17520
22:53:47.760031 D.17775 > A.32782: . 77381:78841(1460) ack 1 win 17520
22:53:47.760055 A.32782 > D.17775: . ack 78841 win 64240
22:53:47.885001 D.17775 > A.32782: . 80301:81761(1460) ack 1 win 17520
22:53:47.885072 A.32782 > D.17775: . ack 78841 win 64240
22:53:47.885816 D.17775 > A.32782: . 83221:84681(1460) ack 1 win 17520
22:53:47.885834 A.32782 > D.17775: . ack 78841 win 64240
22:53:47.885951 D.17775 > A.32782: . 84681:86141(1460) ack 1 win 17520
22:53:47.885962 A.32782 > D.17775: . ack 78841 win 64240
22:53:47.917054 D.17775 > A.32782: . 86141:87601(1460) ack 1 win 17520
22:53:47.917065 A.32782 > D.17775: . ack 78841 win 64240
22:53:48.042369 D.17775 > A.32782: . 78841:80301(1460) ack 1 win 17520
22:53:48.042419 A.32782 > D.17775: . ack 81761 win 64240
22:53:48.199537 D.17775 > A.32782: . 81761:83221(1460) ack 1 win 17520
22:53:48.199602 A.32782 > D.17775: . ack 87601 win 64240
22:53:48.199718 D.17775 > A.32782: . 89061:90521(1460) ack 1 win 17520
22:53:48.199732 A.32782 > D.17775: . ack 87601 win 64240
22:53:48.356490 D.17775 > A.32782: . 87601:89061(1460) ack 1 win 17520
22:53:48.356551 A.32782 > D.17775: . ack 90521 win 64240
22:53:48.356620 D.17775 > A.32782: . 90521:91981(1460) ack 1 win 17520
```

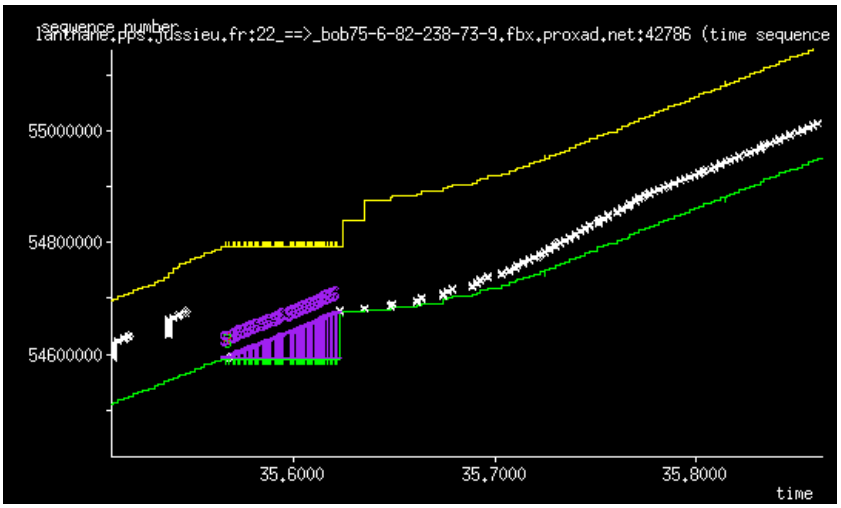
Exercice 4. What happens on each of the following time-sequence diagrams?

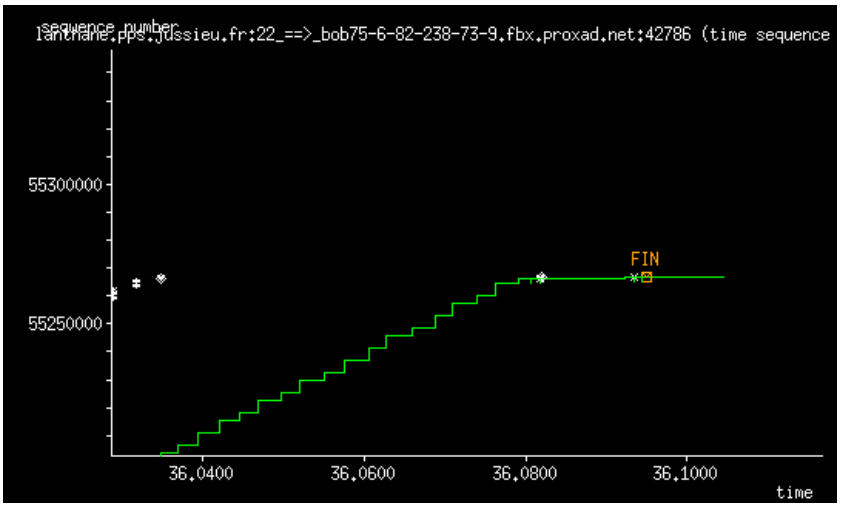







sequence number
lanthane.pps.jussieu.fr:22_==>_bob75-6-82-238-73-9.fbx.proxad.net:42786 (time sequence
52640000
52630000
52620000
52610000
52600000
52590000
34.1600
34.1700
34.1800
34.1900
time


sequence number
lanthane.pps.jussieu.fr:22_==>_bob75-6-82-238-73-9.fbx.proxad.net:42786 (time sequence
55000000
54800000
54600000
35.6000
35.7000
35.8000
time


sequence number
lanthane.pps.jussieu.fr:22_==>_bob75-6-82-238-73-9.fbx.proxad.net:42786 (time sequence
55300000
55250000
FIN
36.0400
36.0600
36.0800
36.1000
time