

# TD Seance 5: Exercice 1 Wireshark

SANNA Thomas

November 14, 2024

### Question 3

Après avoir ouvert Firefox, et ensuite avoir lancé une écoute Wireshark, lorsque l'on ouvre le lien dans <https://random.dog/woof.json>, on peut voir que l'on envoie et reçoit des paquets de type TCP.

|   |           |                        |                |         |                      |
|---|-----------|------------------------|----------------|---------|----------------------|
| 1 | 0.000000  | 172.21.2.233           | 162.243.205.13 | TLSv1.2 | 649 Application Data |
| 2 | 0.104501  | 162.243.205.13         | 172.21.2.233   | TLSv1.2 | 546 Application Data |
| 3 | 0.146595  | 172.21.2.233           | 162.243.205.13 | TCP     | 54 49995 → 443 [ACK] |
| 4 | 0.240025  | fe80::67bc:51bb:9f1... | ff02::1        | ICMPv6  | 86 Neighbor Adverti  |
| 5 | 10.108579 | 172.21.2.233           | 162.243.205.13 | TCP     | 55 [TCP Keep-Alive]  |
| 6 | 10.247503 | 162.243.205.13         | 172.21.2.233   | TCP     | 66 [TCP Keep-Alive]  |

Figure 1: Capture de paquets

### Question 4

Plusieurs protocoles sont utilisés pour la communication:

- TCP
- TLSv1.2
- ICMPV6
- HTTP ne semble pas être utilisé

### Question 5

Les protocoles dont le paquet contient l'adresse IP du serveur est le protocole ICMPV6 (IPV6) et le protocole TCP (IPV4).

### Question 6

Les protocoles utilisés pour l'envoi de données sont le protocole TCP et le protocole TLSv1.2.

| No. | Time     | Source         | Destination    | Protocol | Length | Info  |
|-----|----------|----------------|----------------|----------|--------|---|
| 1   | 0.000000 | 172.21.2.233   | 162.243.205.13 | TLSv1.2  | 649    | Application Data                                |
| 2   | 0.104501 | 162.243.205.13 | 172.21.2.233   | TLSv1.2  | 546    | Application Data                                |
| 3   | 0.146595 | 172.21.2.233   | 162.243.205.13 | TCP      | 54     | 49995 → 443 [ACK] Seq=596 Ack=493 Win=508 Len=0 |

  

|  |      |                         |                         |                       |
|--|------|-------------------------|-------------------------|-----------------------|
| Time to Live: 128  | 0000 | b4 0c 25 e0 40 10 14 f6 | d8 26 48 55 08 00 45 00 | x 0 0 0 0 0 0 0 0     |
| Protocol: TCP (6)  | 0010 | 02 70 36 6c 40 00 00 0c | 00 00 ac 15 02 e9 e2 f3 | (610 0 0 0 0 0 0 0 0) |
| Header checksum: 0x0000 [validation disabled]  | 0020 | cd 0d c3 4b 01 bb 5e 15 | ce 52 d0 55 09 ec 50 18 | K 0 0 0 0 0 0 0 0     |
| [Header checksum status: Unverified]   | 0030 | 01 fe 21 6d 00 00 17 03 | 03 02 4e 80 00 00 00 00 | Im 0 0 0 0 0 0 0 0    |
| Source Address: 172.21.2.233   | 0040 | 00 00 02 61 b5 bd 61 7c | 31 a9 86 ee 61 f5 3f f5 | 0 0 0 0 0 0 0 0       |
| Destination Address: 162.243.205.13  | 0050 | 69 36 70 f2 96 d4 39 f7 | 7b 27 23 cf 1a a6 15 fd | 0 0 0 0 0 0 0 0       |
| [Stream index: 0]  | 0060 | 1e 40 8c 16 c3 de bb e4 | bd 05 7a c3 98 27 09 06 | 0 0 0 0 0 0 0 0       |
| Transmission Control Protocol, Src Port: 49995, Dst Port: 443, Seq: 1, Ack: 1, Len: 59 | 0070 | a1 a8 ac 91 d1 c4 ce b9 | b3 b9 76 ef d2 a8 d2 02 | A 0 0 0 0 0 0 0 0     |
| Source Port: 49995   | 0080 | 8a 4f fb 93 83 72 cd f4 | d5 0b f1 65 1a eb 90 98 | 0 0 0 0 0 0 0 0       |
| Destination Port: 443  | 0090 | 0b 27 62 46 29 f0 dd 3d | c9 f5 21 d0 c6 c2 d6 c7 | 0 0 0 0 0 0 0 0       |
| [Stream index: 0]  | 00a0 | 2a a3 a3 87 88 77 ab e2 | 61 61 bc 16 32 b9 59 67 | 0 0 0 0 0 0 0 0       |
| [Stream Packet Number: 1]  | 00b0 | 10 0c 00 5a cc be 80 f5 | 35 c5 b7 b3 63 86 b1 26 | 0 0 0 0 0 0 0 0       |
| [Conversation completeness: Incomplete (12)]   | 00c0 | 81 0f 0f 04 17 ae b0 65 | 24 98 c4 dc bf 58 dd c1 | 0 0 0 0 0 0 0 0       |
| [TCP Segment Len: 595]   | 00d0 | 0a 42 02 8e e3 76 df a2 | 73 66 44 3b ad 0b 0e 0e | 0 0 0 0 0 0 0 0       |
| Sequence Number: 1 (relative sequence number)  | 00e0 | f6 e2 02 5a 8a 54 d8 c6 | a4 e8 19 1b 6b 16 27 ad | 0 0 0 0 0 0 0 0       |
| Sequence Number (raw): 1578487378  | 00f0 | 20 ed 74 44 63 ae 85 71 | 1b 1d d3 06 03 d8 e5 03 | 0 0 0 0 0 0 0 0       |
| [Next Sequence Number: 596 (relative sequence number)]                                 | 0100 | 51 26 ed 1a 94 e2 9a 0e | 7e 3d a4 f4 34 dd ef    | 0 0 0 0 0 0 0 0       |
| Acknowledgment number (raw): 3495266796  | 0110 | 52 be d3 98 3b 8d 96 4f | 35 f8 e6 0d bf b8 94 72 | 0 0 0 0 0 0 0 0       |
| 0101 .... = Header Length: 20 bytes (5)  | 0120 | 99 de 67 ab 59 0e 05 99 | 14 c9 2e 10 c4 2d 12 ea | 0 0 0 0 0 0 0 0       |
| Flags: 0x018 (PSH, ACK)  | 0130 | 5a 37 90 de ae 71 6d a0 | d2 ec ae 1a 64 73 43 e7 | 0 0 0 0 0 0 0 0       |
| Window: 510  | 0140 | 0f 1c 24 53 82 84 78 0d | bf 23 ac da 77 e3 c3 1b | 0 0 0 0 0 0 0 0       |
| [calculated window size: 510]  | 0150 | a0 75 a1 57 4b b9 ec a6 | 34 24 17 07 47 dd 4c 02 | 0 0 0 0 0 0 0 0       |
| [Window size scaling factor: -1 (unknown)]   | 0160 | 4c 06 1a 27 93 eb e0 20 | 6d e6 9c 9f a6 c6 96 f4 | 0 0 0 0 0 0 0 0       |
| Checksum: 0x216d [unverified]  | 0170 | 04 54 cb 75 af a8 e1 cb | ee fa 32 1f 5a 09 f0 3f | 0 0 0 0 0 0 0 0       |
| [Checksum Status: Unverified]  | 0180 | d0 4a 07 50 e2 49 9c e8 | 65 f5 2c 17 b2 09 05 6b | 0 0 0 0 0 0 0 0       |
| Urgent Pointer: 0  | 0190 | 58 86 d0 71 3b fe f5 c4 | 1f 31 79 c3 9d ec 7b 72 | 0 0 0 0 0 0 0 0       |
| [Timestamp]  | 01a0 | f4 0c 03 7c d8 d3 a3 76 | 78 4a b1 78 8a ab e7 57 | 0 0 0 0 0 0 0 0       |
| [SEQ/ACK analysis]   | 01b0 | 9f c1 81 9d ae 49 84 e1 | a7 0c 72 82 09 bc 57 40 | 0 0 0 0 0 0 0 0       |
| TCP payload (595 bytes)  | 01c0 | 34 4f ff 3c 00 e5 6f 8d | 2b 88 e7 a0 a8 ad de d6 | 0 0 0 0 0 0 0 0       |
| Transport Layer Security   | 01d0 | 2a e7 e6 2d c9 8a fc 9d | 98 df e4 17 8d 39 e1 82 | 0 0 0 0 0 0 0 0       |
| TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol           | 01e0 | c9 e4 b0 27 3d 12 58 19 | 80 57 09 0f 61 09 08 fa | 0 0 0 0 0 0 0 0       |
| Content Type: Application Data (23)  | 01f0 | 07 76 0e 74 6e 27 75 b1 | 4d b4 be 21 46 b8 34 2a | 0 0 0 0 0 0 0 0       |
| Version: TLS 1.2 (0x0303)  | 0200 | 64 58 1f 25 fb df 74 ec | 13 d8 54 e4 e4 56 2c 77 | 0 0 0 0 0 0 0 0       |
| Length: 590  | 0210 | e4 d6 95 ac af a9 41 c4 | 92 27 35 a4 b1 ed 82 20 | 0 0 0 0 0 0 0 0       |
| Encrypted Application Data [...]   | 0220 | 71 ed 38 7a 7e 89 43 a3 | b3 65 72 40 11 6f 10 40 | 0 0 0 0 0 0 0 0       |
| [Application Data Protocol: Hypertext Transfer Protocol]                               | 0230 | c7 38 1a 80 42 1a b7 b5 | d0 51 3f 49 5a 39 bf a5 | 0 0 0 0 0 0 0 0       |
|  | 0240 | 8f 54 e7 f8 45 e0 f5 ab | 04 92 15 93 6e 60 ae 8c | 0 0 0 0 0 0 0 0       |
|  | 0250 | f5 6e b0 07 93 2c 73 77 | ab ef 23 8d 28 80 f5 c6 | 0 0 0 0 0 0 0 0       |
|  | 0260 | 7e c2 36 ae 8d 62 9d 7e | f2 12 a2 18 81 5c e9 8e | 0 0 0 0 0 0 0 0       |
|  | 0270 | 96 85 ca 61 0e b0 a7 65 | ec 45 34 b5 be c0 35 81 | 0 0 0 0 0 0 0 0       |

Figure 2: Capture de paquets