

## EJERCICIOS WIRESHARK – UNIDAD 2 - SPRINT 2

### Hacer una trama de una página web

1. Ir a la página web de [www.thebridge.tech](http://www.thebridge.tech)
2. Capturar la trama con Wireshark
3. Aplicar los siguientes filtros en Wireshark:
  - Filtrar los requerimientos ejecutado desde su dirección IP
  - Filtrar los requerimientos que tengan HTTP.
  - Filtrar los requerimientos que sean del protocolo DNS.
  - Filtrar los requerimientos ejecutado desde su dirección IP y que tengan el protocolo distinto a DNS.

#### ■ Filtro 1

| ip.src == 10.0.2.4 |              |          |                |          |        |             |
|--------------------|--------------|----------|----------------|----------|--------|-------------|
| No.                | Time         | Source   | Destination    | Protocol | Length | Info        |
| 1                  | 0.000000000  | 10.0.2.4 | 142.250.185.3  | TCP      | 56     | 37848 → 80  |
| 3                  | 1.227704710  | 10.0.2.4 | 34.36.165.17   | TLSv1.2  | 95     | Application |
| 5                  | 1.236920698  | 10.0.2.4 | 34.36.165.17   | TCP      | 56     | 37522 → 443 |
| 6                  | 1.283577408  | 10.0.2.4 | 142.250.184.3  | TCP      | 56     | 59652 → 80  |
| 7                  | 1.283595495  | 10.0.2.4 | 142.250.185.3  | TCP      | 56     | 39198 → 80  |
| 10                 | 1.535655736  | 10.0.2.4 | 142.250.184.3  | TCP      | 56     | 59638 → 80  |
| 11                 | 1.535775978  | 10.0.2.4 | 2.21.39.19     | TCP      | 56     | 56510 → 80  |
| 14                 | 2.303056364  | 10.0.2.4 | 2.21.39.17     | TCP      | 56     | 57058 → 80  |
| 16                 | 2.559030926  | 10.0.2.4 | 192.229.221.95 | TCP      | 56     | 52496 → 80  |
| 17                 | 2.559050102  | 10.0.2.4 | 2.21.39.17     | TCP      | 56     | 57048 → 80  |
| 20                 | 2.628192564  | 10.0.2.4 | 142.250.185.3  | TCP      | 56     | [TCP Previo |
| 23                 | 2.637768835  | 10.0.2.4 | 142.250.185.3  | TCP      | 56     | 37848 → 80  |
| 24                 | 4.229228311  | 10.0.2.4 | 34.117.188.166 | TLSv1.2  | 95     | Application |
| 25                 | 4.229270138  | 10.0.2.4 | 34.117.188.166 | TLSv1.2  | 95     | Application |
| 29                 | 4.238870671  | 10.0.2.4 | 34.117.188.166 | TCP      | 56     | 38698 → 443 |
| 31                 | 4.240095851  | 10.0.2.4 | 34.117.188.166 | TCP      | 56     | 38706 → 443 |
| 32                 | 4.634706476  | 10.0.2.4 | 2.21.39.19     | TCP      | 56     | [TCP Previo |
| 35                 | 4.644372274  | 10.0.2.4 | 2.21.39.19     | TCP      | 56     | 56510 → 80  |
| 36                 | 5.888300837  | 10.0.2.4 | 18.154.48.19   | TCP      | 56     | 46554 → 80  |
| 38                 | 6.911793159  | 10.0.2.4 | 108.157.118.26 | TCP      | 56     | 35148 → 80  |
| 40                 | 7.167707680  | 10.0.2.4 | 18.154.40.210  | TCP      | 56     | 54768 → 80  |
| 42                 | 7.423495150  | 10.0.2.4 | 18.154.40.210  | TCP      | 56     | 54782 → 80  |
| 43                 | 7.423577648  | 10.0.2.4 | 104.18.38.233  | TCP      | 56     | 52088 → 80  |
| 46                 | 9.230772822  | 10.0.2.4 | 34.107.243.93  | TLSv1.2  | 95     | Application |
| 48                 | 9.240249621  | 10.0.2.4 | 34.107.243.93  | TCP      | 56     | 55008 → 443 |
| 49                 | 10.232252009 | 10.0.2.4 | 34.117.188.166 | TLSv1.2  | 95     | Application |
| 50                 | 10.232301096 | 10.0.2.4 | 34.117.188.166 | TLSv1.2  | 95     | Application |
| 52                 | 10.241286026 | 10.0.2.4 | 34.117.188.166 | TCP      | 56     | 38706 → 443 |
| 53                 | 10.241448220 | 10.0.2.4 | 34.117.188.166 | TLSv1.2  | 95     | Application |
| 55                 | 10.241576397 | 10.0.2.4 | 34.117.188.166 | TLSv1.2  | 80     | Application |
| 56                 | 10.241592796 | 10.0.2.4 | 34.117.188.166 | TCP      | 56     | 38706 → 443 |
| 58                 | 10.241670568 | 10.0.2.4 | 34.117.188.166 | TCP      | 56     | 38698 → 443 |
| 60                 | 10.241851495 | 10.0.2.4 | 34.117.188.166 | TLSv1.2  | 95     | Application |
| 62                 | 10.241919753 | 10.0.2.4 | 34.117.188.166 | TLSv1.2  | 80     | Application |
| 63                 | 10.241934886 | 10.0.2.4 | 34.117.188.166 | TCP      | 56     | 38698 → 443 |
| 66                 | 11.281588721 | 10.0.2.4 | 34.209.165.250 | TLSv1.2  | 94     | Application |
| 69                 | 11.456899159 | 10.0.2.4 | 34.209.165.250 | TCP      | 56     | 55150 → 443 |
| 70                 | 11.520525994 | 10.0.2.4 | 142.250.185.3  | TCP      | 56     | [TCP Dup AC |
| 71                 | 11.520605266 | 10.0.2.4 | 142.250.184.3  | TCP      | 56     | [TCP Dup AC |

Frame 1: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface any, id 0

Linux cooked capture v1

Packet type: Sent by us (4)

Link-layer address type: Ethernet (1)

Link-layer address length: 6

Source: PCSSystemtec\_1c:12:50 (08:00:27:1c:12:50)

Unused: 0000

Protocol: IPv4 (0x0800)

Internet Protocol Version 4, Src: 10.0.2.4, Dst: 142.250.185.3

Transmission Control Protocol, Src Port: 37848, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

Se ha usado el comando `ip.src == 10.0.2.4` apareciendo solo los paquetes que tienen mi dirección de origen.

## EJERCICIOS WIRESHARK – UNIDAD 2 - SPRINT 2

### ■ Filtro 2

| tls   |           |                |                |          |        |                   |
|---|-----------|----------------|----------------|----------|--------|-------------------|
| No.   | Time      | Source         | Destination    | Protocol | Length | Info              |
| 3   | 0.305568  | 10.0.2.4       | 52.24.78.187   | TLSv1.2  | 102    | Application Data  |
| 4   | 0.484791  | 52.24.78.187   | 10.0.2.4       | TLSv1.2  | 102    | Application Data  |
| 17  | 3.116263  | 79.116.255.16  | 10.0.2.4       | TLSv1.2  | 80     | Application Data  |
| 19  | 3.116376  | 10.0.2.4       | 79.116.255.16  | TLSv1.2  | 95     | Application Data  |
| 21  | 3.116620  | 10.0.2.4       | 79.116.255.16  | TLSv1.2  | 80     | Application Data  |
| 36  | 7.314789  | 10.0.2.4       | 104.16.117.116 | TLSv1.2  | 95     | Application Data  |
| 37  | 7.323917  | 104.16.117.116 | 10.0.2.4       | TLSv1.2  | 95     | Application Data  |
| 49  | 8.315149  | 10.0.2.4       | 142.250.200.99 | TLSv1.2  | 95     | Application Data  |
| 50  | 8.315189  | 10.0.2.4       | 93.184.221.165 | TLSv1.2  | 95     | Application Data  |
| 51  | 8.325401  | 142.250.200.99 | 10.0.2.4       | TLSv1.2  | 95     | Application Data  |
| 53  | 8.326116  | 93.184.221.165 | 10.0.2.4       | TLSv1.2  | 95     | Application Data  |
| 57  | 10.321598 | 10.0.2.4       | 142.251.37.51  | TLSv1.2  | 95     | Application Data  |
| 58  | 10.321650 | 10.0.2.4       | 18.154.22.112  | TLSv1.2  | 95     | Application Data  |
| 59  | 10.331865 | 18.154.22.112  | 10.0.2.4       | TLSv1.2  | 95     | Application Data  |
| 61  | 10.377140 | 142.251.37.51  | 10.0.2.4       | TLSv1.2  | 95     | Application Data  |
| 63  | 10.377192 | 10.0.2.4       | 34.209.165.250 | TLSv1.2  | 94     | Application Data  |
| 64  | 10.552036 | 34.209.165.250 | 10.0.2.4       | TLSv1.2  | 88     | Application Data  |
| 72  | 12.322252 | 10.0.2.4       | 34.36.165.17   | TLSv1.2  | 95     | Application Data  |
| 74  | 12.332195 | 34.36.165.17   | 10.0.2.4       | TLSv1.2  | 95     | Application Data  |
| 76  | 12.379218 | 10.0.2.4       | 34.254.7.187   | TLSv1.2  | 97     | Application Data  |
| 80  | 14.327200 | 10.0.2.4       | 13.107.42.14   | TLSv1.2  | 102    | Application Data  |
| 82  | 14.336565 | 13.107.42.14   | 10.0.2.4       | TLSv1.2  | 102    | Application Data  |
| 88  | 16.328813 | 10.0.2.4       | 52.50.93.182   | TLSv1.2  | 95     | Application Data  |
| 90  | 16.379681 | 52.50.93.182   | 10.0.2.4       | TLSv1.2  | 95     | Application Data  |
| 98  | 19.332027 | 10.0.2.4       | 35.190.43.134  | TLSv1.2  | 95     | Application Data  |
| 99  | 19.341479 | 35.190.43.134  | 10.0.2.4       | TLSv1.2  | 95     | Application Data  |
| 101   | 20.332305 | 10.0.2.4       | 104.16.141.209 | TLSv1.2  | 95     | Application Data  |
| 102   | 20.341575 | 104.16.141.209 | 10.0.2.4       | TLSv1.2  | 95     | Application Data  |
| 107   | 22.556450 | 3.5.72.136     | 10.0.2.4       | SSLv2    | 11736  | Encrypted Data    |
| 109   | 22.556487 | 3.5.72.136     | 10.0.2.4       | SSLv2    | 19036  | Encrypted Data    |
| 111   | 22.556509 | 3.5.72.136     | 10.0.2.4       | SSLv2    | 16116  | Encrypted Data    |
| 113   | 22.556623 | 3.5.72.136     | 10.0.2.4       | TCP      | 11736  | [TCP segment of a |
| 115   | 22.556643 | 3.5.72.136     | 10.0.2.4       | SSLv2    | 5896   | Encrypted Data    |
| 117   | 22.556893 | 3.5.72.136     | 10.0.2.4       | TCP      | 1516   | [TCP segment of a |
| 118   | 22.556894 | 3.5.72.136     | 10.0.2.4       | SSLv2    | 30716  | Encrypted Data    |
| 120   | 22.556967 | 3.5.72.136     | 10.0.2.4       | TCP      | 8816   | [TCP segment of a |
| 121   | 22.556968 | 3.5.72.136     | 10.0.2.4       | TCP      | 5896   | [TCP segment of a |
| 123   | 22.557050 | 3.5.72.136     | 10.0.2.4       | TCP      | 11736  | [TCP segment of a |
| 125   | 22.557142 | 3.5.72.136     | 10.0.2.4       | TCP      | 1351   | [TCP segment of a |
| ▶ Frame 3: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0<br>▶ Linux cooked capture v1<br>▶ Internet Protocol Version 4, Src: 10.0.2.4, Dst: 52.24.78.187<br>▶ Transmission Control Protocol, Src Port: 52198, Dst Port: 443, Seq: 1, Ack: 1, Len: 46<br>▶ Transport Layer Security<br>▼ TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol<br>Content Type: Application Data (23)<br>Version: TLS 1.2 (0x0303)<br>Length: 41<br>Encrypted Application Data: 000000000000000528545bb69e4e837292edf72a2c81a6b2875ab796edc700a9b0ea5...<br>[Application Data Protocol: Hypertext Transfer Protocol] |           |                |                |          |        |                   |
| Record Layer (tls.record), 46 byte(s)   |           |                |                |          |        |                   |

Se ha usado el comando “tls” en vez de “http”, ya que la pagina web capturada usa el protocolo cifrado “https”, por lo que no podremos verlo, pero si los protocolos SSL/TLS.

## EJERCICIOS WIRESHARK – UNIDAD 2 - SPRINT 2

### ■ Filtro 3

| dns.flags.response |              |                         |             |          |        |                |
|--------------------|--------------|-------------------------|-------------|----------|--------|----------------|
| No.                | Time         | dns.flags.response == 1 | Destination | Protocol | Length | Info           |
| 8                  | 8.19456      | dns.flags.response == 0 | 100.100.1.1 | DNS      | 92     | Standard query |
| 9                  | 8.208033055  | 100.100.1.1             | 10.0.2.4    | DNS      | 124    | Standard query |
| 37                 | 9.234793213  | 10.0.2.4                | 100.100.1.1 | DNS      | 80     | Standard query |
| 38                 | 9.253626484  | 100.100.1.1             | 10.0.2.4    | DNS      | 191    | Standard query |
| 64                 | 9.623621079  | 10.0.2.4                | 100.100.1.1 | DNS      | 81     | Standard query |
| 65                 | 9.633424616  | 100.100.1.1             | 10.0.2.4    | DNS      | 196    | Standard query |
| 147                | 10.451608057 | 10.0.2.4                | 100.100.1.1 | DNS      | 77     | Standard query |
| 148                | 10.460853546 | 100.100.1.1             | 10.0.2.4    | DNS      | 158    | Standard query |
| 207                | 12.644650654 | 10.0.2.4                | 100.100.1.1 | DNS      | 79     | Standard query |
| 208                | 12.644668810 | 10.0.2.4                | 100.100.1.1 | DNS      | 79     | Standard query |
| 224                | 12.654121770 | 100.100.1.1             | 10.0.2.4    | DNS      | 111    | Standard query |
| 225                | 12.654225683 | 100.100.1.1             | 10.0.2.4    | DNS      | 135    | Standard query |
| 324                | 13.557396508 | 10.0.2.4                | 100.100.1.1 | DNS      | 90     | Standard query |
| 325                | 13.557946853 | 10.0.2.4                | 100.100.1.1 | DNS      | 75     | Standard query |
| 326                | 13.557958168 | 10.0.2.4                | 100.100.1.1 | DNS      | 75     | Standard query |
| 327                | 13.567055681 | 100.100.1.1             | 10.0.2.4    | DNS      | 122    | Standard query |
| 328                | 13.567056644 | 100.100.1.1             | 10.0.2.4    | DNS      | 91     | Standard query |
| 329                | 13.567057418 | 100.100.1.1             | 10.0.2.4    | DNS      | 103    | Standard query |

Frame 9: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface any, id 0  
Linux cooked capture v1  
Internet Protocol Version 4, Src: 100.100.1.1, Dst: 10.0.2.4  
User Datagram Protocol, Src Port: 53, Dst Port: 58340  
Domain Name System (response)

Se ha usado el comando “dns.flags.response” para filtrar visualmente tanto las solicitudes (==0) y las respuestas (==1) del protocolo DNS.

## EJERCICIOS WIRESHARK – UNIDAD 2 - SPRINT 2

### ■ Filtro 4:

| ip.src == 10.0.2.4 && !dns |              |          |              |          |        |                   |
|----------------------------|--------------|----------|--------------|----------|--------|-------------------|
| No.                        | Time         | Source   | Destination  | Protocol | Length | Info              |
| 42                         | 9.264339267  | 10.0.2.4 | 18.154.48.66 | TLSv1.3  | 585    | Client Hello (SNI |
| 44                         | 9.274533535  | 10.0.2.4 | 18.154.48.66 | TCP      | 56     | 44820 → 443 [ACK] |
| 45                         | 9.275018803  | 10.0.2.4 | 18.154.48.66 | TLSv1.3  | 120    | Change Cipher Spe |
| 46                         | 9.275958657  | 10.0.2.4 | 18.154.48.66 | TLSv1.3  | 226    | Application Data  |
| 47                         | 9.276007263  | 10.0.2.4 | 18.154.48.66 | TLSv1.3  | 1813   | Application Data  |
| 50                         | 9.276683282  | 10.0.2.4 | 18.154.48.66 | TLSv1.3  | 212    | Application Data  |
| 51                         | 9.277151966  | 10.0.2.4 | 18.154.48.66 | TLSv1.3  | 215    | Application Data  |
| 53                         | 9.277302714  | 10.0.2.4 | 18.154.48.66 | TLSv1.3  | 213    | Application Data  |
| 54                         | 9.277436294  | 10.0.2.4 | 18.154.48.66 | TLSv1.3  | 212    | Application Data  |
| 57                         | 9.327415136  | 10.0.2.4 | 18.154.48.66 | TCP      | 56     | 44820 → 443 [ACK] |
| 59                         | 9.327600415  | 10.0.2.4 | 18.154.48.66 | TCP      | 56     | 44820 → 443 [ACK] |
| 60                         | 9.327710783  | 10.0.2.4 | 18.154.48.66 | TLSv1.3  | 87     | Application Data  |
| 63                         | 9.621186895  | 10.0.2.4 | 34.254.7.187 | TLSv1.2  | 936    | Application Data  |
| 66                         | 9.633891461  | 10.0.2.4 | 13.107.42.14 | TCP      | 76     | 37666 → 443 [SYN] |
| 68                         | 9.645546648  | 10.0.2.4 | 13.107.42.14 | TCP      | 56     | 37666 → 443 [ACK] |
| 69                         | 9.646759874  | 10.0.2.4 | 13.107.42.14 | TLSv1.2  | 714    | Client Hello (SNI |
| 71                         | 9.658014834  | 10.0.2.4 | 13.107.42.14 | TCP      | 56     | 37666 → 443 [ACK] |
| 72                         | 9.658710426  | 10.0.2.4 | 13.107.42.14 | TLSv1.2  | 107    | Change Cipher Spe |
| 73                         | 9.658945992  | 10.0.2.4 | 13.107.42.14 | TLSv1.2  | 233    | Application Data  |
| 74                         | 9.658966212  | 10.0.2.4 | 13.107.42.14 | TLSv1.2  | 359    | Application Data  |
| 75                         | 9.658986433  | 10.0.2.4 | 13.107.42.14 | TLSv1.2  | 1631   | Application Data  |
| 79                         | 9.667531373  | 10.0.2.4 | 13.107.42.14 | TLSv1.2  | 94     | Application Data  |
| 81                         | 9.711652794  | 10.0.2.4 | 13.107.42.14 | TCP      | 56     | 37666 → 443 [ACK] |
| 83                         | 9.815153121  | 10.0.2.4 | 13.107.42.14 | TCP      | 56     | 37666 → 443 [ACK] |
| 86                         | 9.991388067  | 10.0.2.4 | 18.154.48.66 | TCP      | 56     | 44820 → 443 [ACK] |
| 89                         | 9.991673076  | 10.0.2.4 | 18.154.48.66 | TCP      | 56     | 44820 → 443 [ACK] |
| 91                         | 10.000230744 | 10.0.2.4 | 18.154.48.66 | TCP      | 56     | 44820 → 443 [ACK] |
| 96                         | 10.015678082 | 10.0.2.4 | 18.154.48.66 | TCP      | 56     | 44820 → 443 [ACK] |
| 97                         | 10.015692331 | 10.0.2.4 | 18.154.48.66 | TCP      | 56     | 44820 → 443 [ACK] |
| 98                         | 10.015698859 | 10.0.2.4 | 18.154.48.66 | TCP      | 56     | 44820 → 443 [ACK] |
| 101                        | 10.015892548 | 10.0.2.4 | 18.154.48.66 | TCP      | 56     | 44820 → 443 [ACK] |
| 106                        | 10.056923991 | 10.0.2.4 | 18.154.48.66 | TCP      | 56     | 44820 → 443 [ACK] |
| 107                        | 10.056937563 | 10.0.2.4 | 18.154.48.66 | TCP      | 56     | 44820 → 443 [ACK] |
| 108                        | 10.056943284 | 10.0.2.4 | 18.154.48.66 | TCP      | 56     | 44820 → 443 [ACK] |
| 111                        | 10.057432203 | 10.0.2.4 | 18.154.48.66 | TCP      | 56     | 44820 → 443 [ACK] |
| 116                        | 10.070441070 | 10.0.2.4 | 18.154.48.66 | TCP      | 56     | 44820 → 443 [ACK] |
| 117                        | 10.070459192 | 10.0.2.4 | 18.154.48.66 | TCP      | 56     | 44820 → 443 [ACK] |
| 120                        | 10.070517895 | 10.0.2.4 | 18.154.48.66 | TCP      | 56     | 44820 → 443 [ACK] |
| 123                        | 10.070780835 | 10.0.2.4 | 18.154.48.66 | TCP      | 56     | 44820 → 443 [ACK] |

▶ Frame 66: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)  
 ▶ Linux cooked capture v1  
 ▶ Internet Protocol Version 4, Src: 10.0.2.4, Dst: 13.107.42.14  
 ▶ Transmission Control Protocol, Src Port: 37666, Dst Port: 443, Seq: 0, Len: 0

Source Port: 37666  
 Destination Port: 443  
 [Stream index: 4]  
 ▶ [Conversation completeness: Complete, WITH\_DATA (47)]  
 [TCP Segment Len: 0]  
 Sequence Number: 0 (relative sequence number)  
 Sequence Number (raw): 1036986120  
 [Next Sequence Number: 1 (relative sequence number)]

Aquí se ha usado dos filtros unidos, en primer lugar, el filtrado la ip de origen de la maquina (ip.src ==10.0.2.4) y después, para que aparezcan todos los protocolos menos el DNS (! dns), uniéndolos por “&&”:

“ip.src == 10.0.2.4 && !dns”