# RETO 7 SEGURIDAD EN SISTEMAS Y REDES

**CIM31-G11**

## Capturas Realizadas

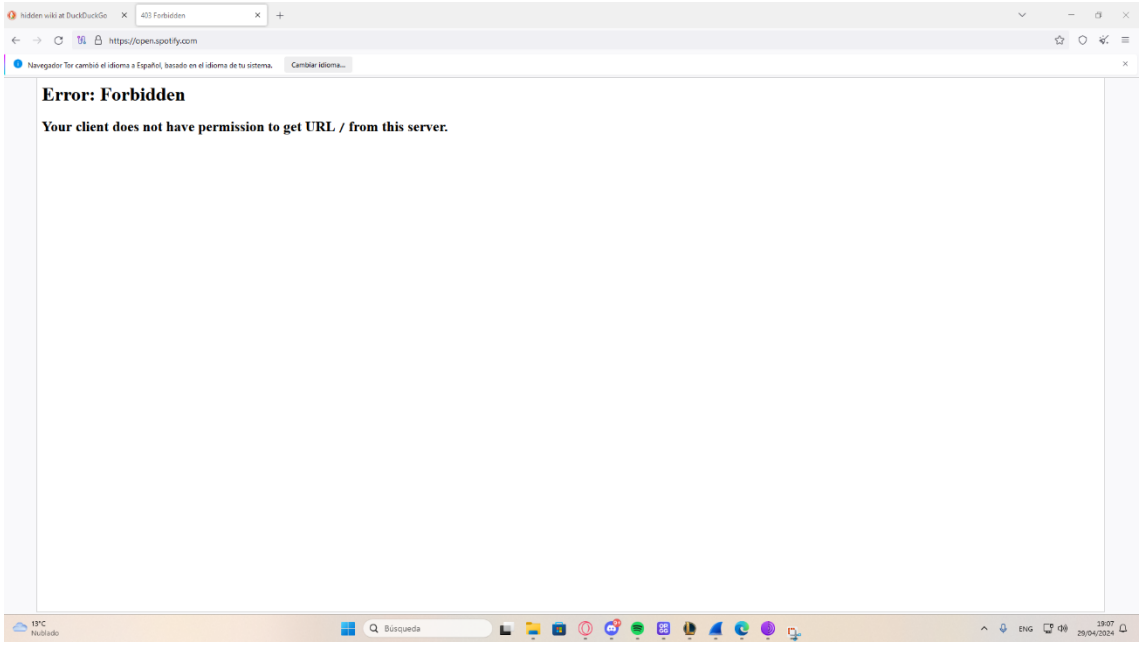
### 1. Entrada a una página web tradicional (capturas 1 y 2).

| | | | | | |
|---|---|---|---|---|---|
| 7616 | 41.457322 | 35.212.99.138 | 192.168.1.151 | TCP | 66 443 → 60961 [SYN, ACK] Seq=0 Ack=1 Win=32660 Len=0 MSS=1420 SACK_PERM WS=128 |
| 7617 | 41.457416 | 192.168.1.151 | 35.212.99.138 | TCP | 54 60961 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0 |
| 7618 | 41.457879 | 192.168.1.151 | 35.212.99.138 | TLSv1.3 | 1872 Client Hello (SNI=maqlions.com) |

| | | | | | |
|---|---|---|---|---|---|
| 1764 | 5.413942 | 192.168.1.151 | 146.75.42.91 | TCP | 66 61690 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 1778 | 5.574579 | 192.168.1.151 | 146.75.42.91 | TCP | 54 61690 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0 |
| 1779 | 5.574931 | 192.168.1.151 | 146.75.42.91 | TLSv1.3 | 1796 Client Hello (SNI=kbfi-v4.pops.fastly-insights.com) |
| 1800 | 5.737046 | 192.168.1.151 | 146.75.42.91 | TCP | 54 61690 → 443 [ACK] Seq=1743 Ack=2873 Win=132352 Len=0 |
| 1804 | 5.737505 | 192.168.1.151 | 146.75.42.91 | TCP | 54 61690 → 443 [ACK] Seq=1743 Ack=5817 Win=132352 Len=0 |
| 1805 | 5.738720 | 192.168.1.151 | 146.75.42.91 | TLSv1.3 | 118 Change Cipher Spec, Application Data |
| 1806 | 5.738910 | 192.168.1.151 | 146.75.42.91 | TLSv1.3 | 737 Application Data |
| 1832 | 5.899613 | 192.168.1.151 | 146.75.42.91 | TCP | 54 61690 → 443 [ACK] Seq=2490 Ack=7203 Win=131072 Len=0 |
| 1834 | 5.899982 | 192.168.1.151 | 146.75.42.91 | TCP | 54 61690 → 443 [ACK] Seq=2490 Ack=7204 Win=131072 Len=0 |
| 1835 | 5.900213 | 192.168.1.151 | 146.75.42.91 | TCP | 54 61690 → 443 [FIN, ACK] Seq=2490 Ack=7204 Win=131072 Len=0 |

Las dos capturas anteriores representan el acceso a una página web tradicional, donde se ven las conexiones seguras realizadas. El tráfico observado se corresponde con el típico de las conexiones HTTPS directas, no dando indicios de relaciones con la red TOR.

### 2. Entrada a una página web tradicional con TOR (capturas 3 y 4).



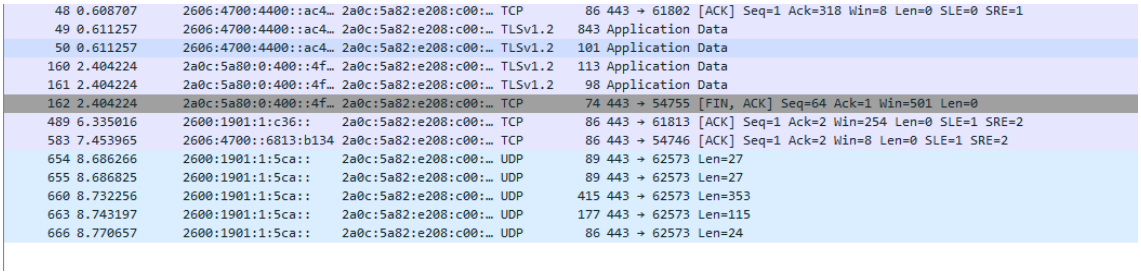

| | | | | | |
|---|---|---|---|---|---|
| 1764 | 5.413942 | 192.168.1.151 | 146.75.42.91 | TCP | 66 61690 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 1778 | 5.574579 | 192.168.1.151 | 146.75.42.91 | TCP | 54 61690 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0 |
| 1779 | 5.574931 | 192.168.1.151 | 146.75.42.91 | TLSv1.3 | 1796 Client Hello (SNI=kbfi-v4.pops.fastly-insights.com) |
| 1800 | 5.737046 | 192.168.1.151 | 146.75.42.91 | TCP | 54 61690 → 443 [ACK] Seq=1743 Ack=2873 Win=132352 Len=0 |
| 1804 | 5.737505 | 192.168.1.151 | 146.75.42.91 | TCP | 54 61690 → 443 [ACK] Seq=1743 Ack=5817 Win=132352 Len=0 |
| 1805 | 5.738720 | 192.168.1.151 | 146.75.42.91 | TLSv1.3 | 118 Change Cipher Spec, Application Data |
| 1806 | 5.738910 | 192.168.1.151 | 146.75.42.91 | TLSv1.3 | 737 Application Data |
| 1832 | 5.899613 | 192.168.1.151 | 146.75.42.91 | TCP | 54 61690 → 443 [ACK] Seq=2490 Ack=7203 Win=131072 Len=0 |
| 1834 | 5.899982 | 192.168.1.151 | 146.75.42.91 | TCP | 54 61690 → 443 [ACK] Seq=2490 Ack=7204 Win=131072 Len=0 |
| 1835 | 5.900213 | 192.168.1.151 | 146.75.42.91 | TCP | 54 61690 → 443 [FIN, ACK] Seq=2490 Ack=7204 Win=131072 Len=0 |

En estas capturas se puede observar cómo no se puede entrar a Spotify en la red TOR. Esto se debe a que normalmente este tipo de páginas tienen bloqueo de VPNs, impidiendo su acceso.

**Diego Espinosa, Manuel Neto, Lucía González y Paul Rodríguez**

## Capturas Realizadas

### 3. Entrada a una página web con dominio .onion con TOR (captura 5).



| | | | | | | |
|---|---|---|---|---|---|---|
| 48 | 0.608707 | 2606:4700:4400::ac4… | 2a0c:5a82:e208:c00:… | TCP | 86 | 443 → 61802 [ACK] Seq=1 Ack=318 Win=8 Len=0 SLE=0 SRE=1 |
| 49 | 0.611257 | 2606:4700:4400::ac4… | 2a0c:5a82:e208:c00:… | TLSv1.2 | 843 | Application Data |
| 50 | 0.611257 | 2606:4700:4400::ac4… | 2a0c:5a82:e208:c00:… | TLSv1.2 | 101 | Application Data |
| 160 | 2.404224 | 2a0c:5a80:0:400::4f… | 2a0c:5a82:e208:c00:… | TLSv1.2 | 113 | Application Data |
| 161 | 2.404224 | 2a0c:5a80:0:400::4f… | 2a0c:5a82:e208:c00:… | TLSv1.2 | 98 | Application Data |
| 162 | 2.404224 | 2a0c:5a80:0:400::4f… | 2a0c:5a82:e208:c00:… | TCP | 74 | 443 → 54755 [FIN, ACK] Seq=64 Ack=1 Win=501 Len=0 |
| 489 | 6.335016 | 2600:1901:1:c36:: | 2a0c:5a82:e208:c00:… | TCP | 86 | 443 → 61813 [ACK] Seq=1 Ack=2 Win=254 Len=0 SLE=1 SRE=2 |
| 583 | 7.453965 | 2606:4700::6813:b134 | 2a0c:5a82:e208:c00:… | TCP | 86 | 443 → 54746 [ACK] Seq=1 Ack=2 Win=8 Len=0 SLE=1 SRE=2 |
| 654 | 8.686266 | 2600:1901:1:5ca:: | 2a0c:5a82:e208:c00:… | UDP | 89 | 443 → 62573 Len=27 |
| 655 | 8.686825 | 2600:1901:1:5ca:: | 2a0c:5a82:e208:c00:… | UDP | 89 | 443 → 62573 Len=27 |
| 660 | 8.732256 | 2600:1901:1:5ca:: | 2a0c:5a82:e208:c00:… | UDP | 415 | 443 → 62573 Len=353 |
| 663 | 8.743197 | 2600:1901:1:5ca:: | 2a0c:5a82:e208:c00:… | UDP | 177 | 443 → 62573 Len=115 |
| 666 | 8.770657 | 2600:1901:1:5ca:: | 2a0c:5a82:e208:c00:… | UDP | 86 | 443 → 62573 Len=24 |

Sin embargo, y como se puede apreciar en la captura anterior, sí se puede acceder dentro de la red TOR a dominios .onion, donde estos carecen de Windows hello y son diseñados para poder acceder desde esta red.