

# Wireshark Analysis: Port 80 vs Port 443

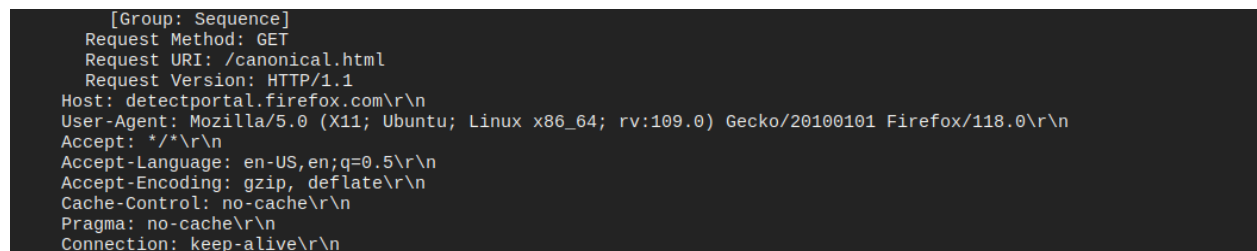
Utilizing Wireshark, I conducted an in-depth analysis of the traffic on my home network. Curiosity led me to dive into two pivotal ports: 80 and 443. Port 80 is synonymous with HTTP communication, while port 443 is its encrypted counterpart, utilized for HTTPS traffic. Throughout my analysis, I wanted to discern the stark differences between these two protocols. While HTTP operates through plain text, HTTPS elevates security using TLS or SSL encryption.



Here I am running a filter, to solely look at traffic on port 80.

Protocol	Length	Info
TCP	74	47270 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSV...
TCP	60	80 → 47270 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
TCP	54	47270 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
HTTP	355	GET /canonical.html HTTP/1.1
TCP	60	80 → 47270 [ACK] Seq=1 Ack=302 Win=64240 Len=0
HTTP	352	HTTP/1.1 200 OK (text/html)
TCP	54	47270 → 80 [ACK] Seq=302 Ack=299 Win=63942 Len=0
HTTP	355	GET /canonical.html HTTP/1.1
TCP	60	80 → 47270 [ACK] Seq=299 Ack=603 Win=64240 Len=0
HTTP	352	HTTP/1.1 200 OK (text/html)
TCP	54	47270 → 80 [ACK] Seq=603 Ack=597 Win=63942 Len=0
TCP	54	[TCP Keep-Alive] 47270 → 80 [ACK] Seq=602 Ack=597 Win=63942 L...
TCP	54	[TCP Keep-Alive] 47270 → 80 [ACK] Seq=602 Ack=597 Win=63942 L...
TCP	60	[TCP Keep-Alive ACK] 80 → 47270 [ACK] Seq=597 Ack=603 Win=642...
TCP	54	[TCP Keep-Alive] 47270 → 80 [ACK] Seq=602 Ack=597 Win=63942 L...
TCP	60	[TCP Keep-Alive ACK] 80 → 47270 [ACK] Seq=597 Ack=603 Win=642...

As we can see here, port 80, used for HTTP communication, runs without the shield of encryption such as SSL or TLS. This absence of encryption allows extreme vulnerability for data transmitted through this port. Without HTTPS, data exchanged over port 80 is very susceptible to interception by malicious actors. It is evident that HTTPS is a luxury and a necessity for protecting data online.



While looking at a *GET* request using HTTP Protocol, you are able to see different information about my PC. I am running Wireshark on an Ubuntu virtual machine, which is very visible among other information.

```
tcp.port == 443
```

Here I run the filter, to look at traffic on port 443.

TCP	74	58402 → 443	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TS...
TCP	60	443 → 58402	[SYN, ACK]	Seq=0	Ack=1	Win=64240	Len=0	MSS=1460	
TCP	54	58402 → 443	[ACK]	Seq=1	Ack=1	Win=64240	Len=0		
TLSv1.3	721	Client Hello (SNI=sposcs.getpocket.com)							
TCP	60	443 → 58402	[ACK]	Seq=1	Ack=668	Win=64240	Len=0		
TLSv1.3	1466	Server Hello, Change Cipher Spec							
TCP	54	58402 → 443	[ACK]	Seq=668	Ack=1413	Win=63540	Len=0		
TLSv1.3	3092	Application Data							
TCP	54	58402 → 443	[ACK]	Seq=668	Ack=4451	Win=61320	Len=0		
TCP	74	42024 → 443	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TS...
TCP	60	443 → 42024	[SYN, ACK]	Seq=0	Ack=1	Win=64240	Len=0	MSS=1460	
TCP	54	42024 → 443	[ACK]	Seq=1	Ack=1	Win=64240	Len=0		
TLSv1.2	270	Client Hello (SNI=content-signature-2.cdn.mozilla.net)							
TCP	60	443 → 42024	[ACK]	Seq=1	Ack=217	Win=64240	Len=0		
TLSv1.2	3073	Server Hello, Certificate, Server Key Exchange, Server Hello ...							
TCP	54	42024 → 443	[ACK]	Seq=217	Ack=3020	Win=62780	Len=0		

When comparing port 80 traffic to port 443 traffic, the disparity is like night and day. Port 443 is fortified by the TLS 1.2 and TLS 1.3 encryption protocols, allowing for secure network traffic. This encryption safeguards sensitive information such as login credentials, personal details, and financial transactions from malicious actors.

```
Handshake Protocol: Server Hello
Handshake Type: Server Hello (2)
Length: 118
Version: TLS 1.2 (0x0303)
Random: df3cd5b8df90e0a7677328cd4e5bbe45246b65022e04e15d88773601d92c6c9b
Session ID Length: 32
Session ID: bcf55ec37cd1bbf779a2d9bc644101e9d8f6173e5dfe2d6bb03e1d8c9ee0b185
Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
Compression Method: null (0)
Extensions Length: 46
  Extension: key_share (len=36) x25519
  Extension: supported_versions (len=2) TLS 1.3
[JAS Fullstring: 771,4865,51-43]
```

Dissecting the network traffic on port 443 reveals the server's choice of cipher suite. AES-128, a symmetric algorithm, is coupled with the SHA-256 hashing algorithm. Combining these two epitomizes the pinnacle of cryptographic security standards. With this encryption, each packet traversing the network remains secure. The session ID ensures seamless and secure data transmission.

The difference in security between ports 80 and 443 is astounding. It serves as a reminder of the importance of HTTPS in safeguarding our online interactions. In the era of cyber threats and data breaches, we must remember to prioritize keeping our information secure. By adhering to that principle and prioritizing HTTPS-enabled websites, we can prevent our personal information from falling into the wrong hands. If you are ever greeted by the "Not Secure" label while visiting a website, treat that with the utmost importance.