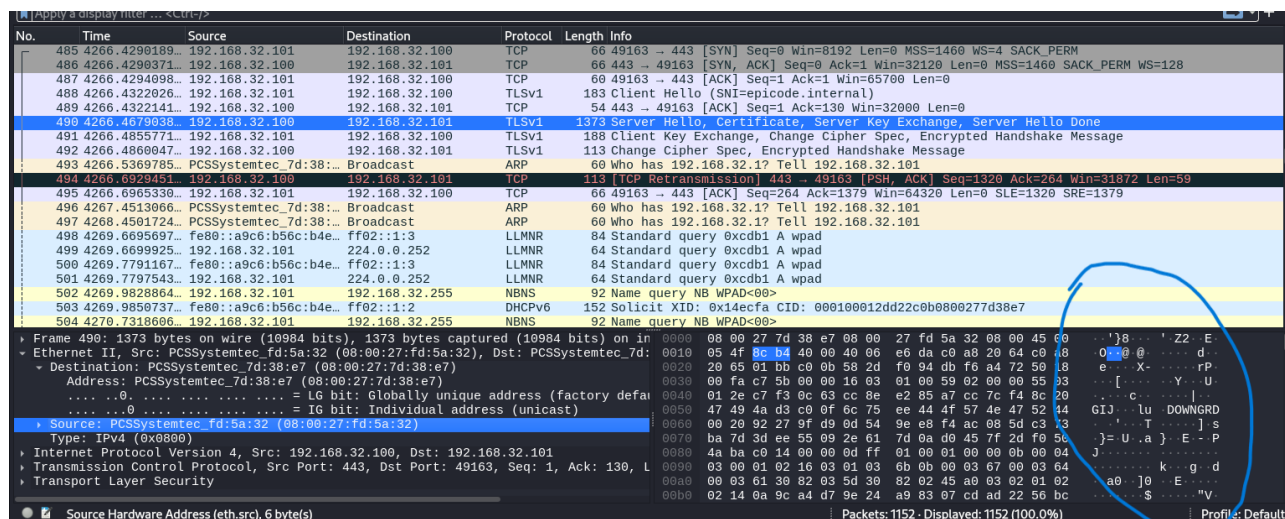


Il protocollo https è una versione sicura e criptata del protocollo http utilizzato per la comunicazione tra un client e un server web. La differenza principale tra i due protocolli è che https garantisce una trasmissione affidabile dei dati attraverso l'utilizzo di un certificato digitale.

MAC Address destination (08:00:27:7d:38:e7)

MAC Address source (08:00:27:fd:5a:32)

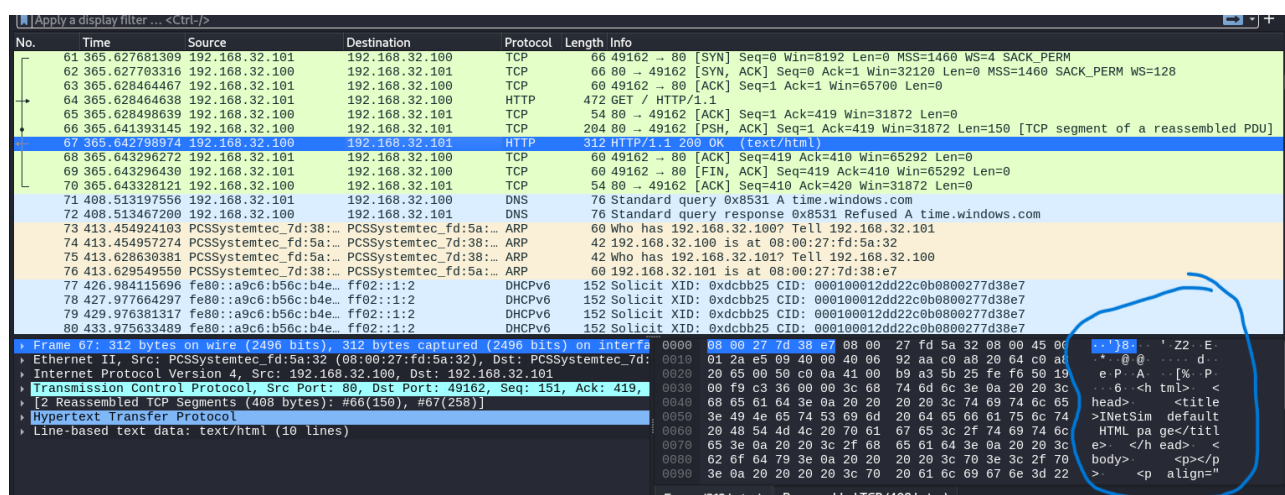


No.	Time	Source	Destination	Protocol	Length	Info
485	4266.4290189	192.168.32.101	192.168.32.100	TCP	66	49163 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
486	4266.4290371	192.168.32.100	192.168.32.101	TCP	66	443 → 49163 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1460 SACK_PERM WS=128
487	4266.4294098	192.168.32.101	192.168.32.100	TCP	60	49163 → 443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
488	4266.4322026	192.168.32.101	192.168.32.100	TLSv1	183	Client Hello (SNI=epicode.internal)
489	4266.4322141	192.168.32.100	192.168.32.101	TCP	54	443 → 49163 [ACK] Seq=1 Ack=130 Win=32000 Len=0
490	4266.4322141	192.168.32.100	192.168.32.101	TLSv1	1373	Server Hello, Certificate, Server Key Exchange, Server Hello Done
491	4266.485571	192.168.32.101	192.168.32.100	TLSv1	188	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
492	4266.4860947	192.168.32.100	192.168.32.101	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
493	4266.5369785	PCSSystemtec_7d:38:...	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101
494	4266.6929451	192.168.32.100	192.168.32.101	TCP	113	[TCP Retransmission] 443 → 49163 [PSH, ACK] Seq=1320 Ack=264 Win=31872 Len=59
495	4266.6965330	192.168.32.101	192.168.32.100	TCP	66	49163 → 443 [ACK] Seq=264 Ack=1379 Win=64320 Len=0 SLE=1320 SRE=1379
496	4267.4513066	PCSSystemtec_7d:38:...	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101
497	4268.4581724	PCSSystemtec_7d:38:...	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101
498	4269.6695097	fe80::a9c6:b56c:b4e...	ff02::1:3	LLMNR	84	Standard query 0xcdb1 A wpad
499	4269.6695925	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0xcdb1 A wpad
500	4269.7791167	fe80::a9c6:b56c:b4e...	ff02::1:3	LLMNR	84	Standard query 0xcdb1 A wpad
501	4269.7797543	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0xcdb1 A wpad
502	4269.9828864	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD<00>
503	4269.9850737	fe80::a9c6:b56c:b4e...	ff02::1:2	DHCPv6	152	Solicit XID: 0x14ecfa CID: 000100012dd22c0b0800277d38e7
504	4270.7318606	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD<00>

Le informazioni trasmesse tramite HTTP non sono crittografate, rendendo i dati vulnerabili agli attacchi di tipo “sniffing” o intercettazione da parte di terze parti malintenzionate.

MAC Address destination (08:00:27:7d:38:e7)

MAC Address source (08:00:27:fd:5a:32)



No.	Time	Source	Destination	Protocol	Length	Info
61	365.627681309	192.168.32.101	192.168.32.100	TCP	66	49162 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
62	365.627703316	192.168.32.100	192.168.32.101	TCP	66	80 → 49162 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1460 SACK_PERM WS=128
63	365.628464467	192.168.32.101	192.168.32.100	TCP	60	49162 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
64	365.628464638	192.168.32.101	192.168.32.100	HTTP	472	GET / HTTP/1.1
65	365.628468039	192.168.32.100	192.168.32.101	TCP	54	80 → 49162 [ACK] Seq=1 Ack=419 Win=31872 Len=0
66	365.641393145	192.168.32.100	192.168.32.101	TCP	204	80 → 49162 [PSH, ACK] Seq=1 Ack=419 Win=31872 Len=150 [TCP segment of a reassembled PDU]
67	365.642798974	192.168.32.100	192.168.32.101	HTTP	312	HTTP/1.1 200 OK (text/html)
68	365.643296272	192.168.32.101	192.168.32.100	TCP	60	49162 → 80 [ACK] Seq=419 Ack=410 Win=65292 Len=0
69	365.643296430	192.168.32.101	192.168.32.100	TCP	60	49162 → 80 [FIN, ACK] Seq=419 Ack=410 Win=65292 Len=0
70	365.643282121	192.168.32.100	192.168.32.101	TCP	54	80 → 49162 [ACK] Seq=410 Ack=420 Win=31872 Len=0
71	408.513197556	192.168.32.100	192.168.32.101	DNS	76	Standard query 0x8531 A time.windows.com
72	408.513467200	192.168.32.101	192.168.32.100	DNS	76	Standard query response 0x8531 Refused A time.windows.com
73	413.454924103	PCSSystemtec_7d:38:...	PCSSystemtec_fd:5a:...	ARP	60	Who has 192.168.32.100? Tell 192.168.32.101
74	413.454957274	PCSSystemtec_fd:5a:...	PCSSystemtec_7d:38:...	ARP	42	192.168.32.100 is at 08:00:27:fd:5a:32
75	413.628636381	PCSSystemtec_fd:5a:...	PCSSystemtec_7d:38:...	ARP	42	Who has 192.168.32.101? Tell 192.168.32.100
76	413.629549550	PCSSystemtec_7d:38:...	PCSSystemtec_fd:5a:...	ARP	60	192.168.32.101 is at 08:00:27:7d:38:e7
77	426.984115696	fe80::a9c6:b56c:b4e...	ff02::1:2	DHCPv6	152	Solicit XID: 0xdccbb25 CID: 000100012dd22c0b0800277d38e7
78	427.977664297	fe80::a9c6:b56c:b4e...	ff02::1:2	DHCPv6	152	Solicit XID: 0xdccbb25 CID: 000100012dd22c0b0800277d38e7
79	429.976381317	fe80::a9c6:b56c:b4e...	ff02::1:2	DHCPv6	152	Solicit XID: 0xdccbb25 CID: 000100012dd22c0b0800277d38e7
80	433.975633489	fe80::a9c6:b56c:b4e...	ff02::1:2	DHCPv6	152	Solicit XID: 0xdccbb25 CID: 000100012dd22c0b0800277d38e7

La principale differenza tra HTTP e HTTPS consiste nella presenza di un livello di sicurezza aggiuntivo fornito da un protocollo chiamato SSL/TLS.