

The screenshot displays the Wireshark interface with a network capture from the interface `*eth0`. The packet list on the left shows various network events, including ARP requests, TCP connections, and TLS handshakes. Packet 6 is selected, showing a TLS Client Hello message. The packet details pane on the right provides a hierarchical view of the selected packet's structure, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane at the bottom shows the raw hexadecimal and ASCII data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PcsCompu_81:ec:65	Broadcast	ARP	60	Who has 192.168.32.100? Tell 192.168.32.101
2	0.000019913	PcsCompu_cb:7e:f5	PcsCompu_81:ec:65	ARP	42	192.168.32.100 is at 08:00:27:cb:7e:f5
3	0.000131553	192.168.32.101	192.168.32.100	TCP	66	49178 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
4	0.000153667	192.168.32.100	192.168.32.101	TCP	66	443 → 49178 [SYN,ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
5	0.000307309	192.168.32.101	192.168.32.100	TCP	60	49178 → 443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
6	0.001405977	192.168.32.101	192.168.32.100	TLSv1	215	Client Hello
7	0.001420940	192.168.32.100	192.168.32.101	TCP	54	443 → 49178 [ACK] Seq=1 Ack=162 Win=64128 Len=0
8	0.029303740	192.168.32.100	192.168.32.101	TLSv1	1373	Server Hello, Certificate, Server Key Exchange, Server Hello Done
9	0.032838919	192.168.32.101	192.168.32.100	TLSv1	188	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10	0.033154511	192.168.32.100	192.168.32.101	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
11	0.043435310	PcsCompu_81:ec:65	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101
12	0.236368273	192.168.32.101	192.168.32.100	TCP	60	49178 → 443 [ACK] Seq=296 Ack=1379 Win=64320 Len=0
13	0.892419018	PcsCompu_81:ec:65	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101
14	1.893794337	PcsCompu_81:ec:65	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101
15	3.178420249	fe80::93e:a7c9:7d2e...	ff02::1:3	LLMNR	84	Standard query 0x9cd4 A wpad
16	3.178420518	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0x9cd4 A wpad
17	3.322468035	fe80::93e:a7c9:7d2e...	ff02::1:3	LLMNR	84	Standard query 0x9cd4 A wpad
18	3.322468960	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0x9cd4 A wpad
19	3.519290190	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD<00>
20	4.269598205	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD<00>
21	5.019713721	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD<00>
22	5.248633714	PcsCompu_cb:7e:f5	PcsCompu_81:ec:65	ARP	42	Who has 192.168.32.101? Tell 192.168.32.100
23	5.248885366	PcsCompu_81:ec:65	PcsCompu_cb:7e:f5	ARP	60	192.168.32.101 is at 08:00:27:81:ec:65
24	5.774637866	PcsCompu_81:ec:65	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101
25	6.427117687	PcsCompu_81:ec:65	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101
26	7.427326972	PcsCompu_81:ec:65	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101
27	8.916524024	fe80::93e:a7c9:7d2e...	ff02::1:3	LLMNR	84	Standard query 0x7a5b A wpad
28	8.916524537	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0x7a5b A wpad
29	9.022291017	fe80::93e:a7c9:7d2e...	ff02::1:3	LLMNR	84	Standard query 0x7a5b A wpad
30	9.022291346	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0x7a5b A wpad
31	9.232370880	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD<00>

Frame 6: 215 bytes on wire (1720 bits), 215 bytes captured (1720 bits) on interface *eth0
 Ethernet II, Src: PcsCompu_81:ec:65 (08:00:27:81:ec:65), Dst: 192.168.32.100 (08:00:27:cb:7e:f5)
 Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
 Transmission Control Protocol, Src Port: 49178, Dst Port: 443
 Transport Layer Security

Transport Layer Security (tls), 161 bytes

Packets: 69 - Displayed: 69 (100.0%) - Dropped: 0 (0.0%) | Profile: Default

Una volta configurato il sistema Operativo Kali Linux cambiandogli l'IP address (192.168.32.100) e impostando i parametri del server DNS tramite il portale INETSIM, inserendogli l'indirizzo IP a un sito browser epicode.internal e a sua volta al sistema Operativo Windows impostando l'IP 192.168.32.101 e configurando il server DNS si può notare che andando sul sito epicode.internal dal browser di Windows con l'indirizzo HTTPS avviene la comunicazione e lo scambio dei pacchetti in modalità sicura e cifrata dove non è possibile leggere il contenuto dello scambio dei pacchetti,

The screenshot shows a Wireshark capture on the *eth0 interface. The packet list displays 22 packets. The selected packet (No. 9) is an HTTP GET request from 192.168.32.100 to 192.168.32.101. The packet details pane shows the structure of the packet: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PcsCompu_81:ec:65	Broadcast	ARP	60	Who has 192.168.32.100? Tell 192.168.32.101
2	0.000020712	PcsCompu_cb:7e:f5	PcsCompu_81:ec:65	ARP	42	192.168.32.100 is at 08:00:27:cb:7e:f5
3	0.000350144	192.168.32.101	192.168.32.100	TCP	66	49194 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
4	0.000400210	192.168.32.100	192.168.32.101	TCP	66	80 → 49194 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
5	0.001095952	192.168.32.101	192.168.32.100	TCP	60	49194 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
6	0.001559945	192.168.32.101	192.168.32.100	HTTP	361	GET / HTTP/1.1
7	0.001582613	192.168.32.100	192.168.32.101	TCP	54	80 → 49194 [ACK] Seq=1 Ack=308 Win=64128 Len=0
8	0.011672543	192.168.32.100	192.168.32.101	TCP	204	80 → 49194 [PSH, ACK] Seq=1 Ack=308 Win=64128 Len=150 [TCP segment of a reassembled PDU]
9	0.012862793	192.168.32.100	192.168.32.101	HTTP	312	HTTP/1.1 200 OK (text/html)
10	0.013184809	192.168.32.101	192.168.32.100	TCP	60	49194 → 80 [ACK] Seq=308 Ack=410 Win=65292 Len=0
11	0.013236866	192.168.32.101	192.168.32.100	TCP	60	49194 → 80 [FIN, ACK] Seq=308 Ack=410 Win=65292 Len=0
12	0.013247238	192.168.32.100	192.168.32.101	TCP	54	80 → 49194 [ACK] Seq=410 Ack=309 Win=64128 Len=0
13	0.760954930	192.168.32.101	192.168.32.100	TCP	66	49197 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
14	0.760990729	192.168.32.100	192.168.32.101	TCP	66	80 → 49197 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
15	0.761419808	192.168.32.101	192.168.32.100	TCP	60	49197 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
16	0.761591580	192.168.32.101	192.168.32.100	HTTP	361	GET / HTTP/1.1
17	0.761604690	192.168.32.100	192.168.32.101	TCP	54	80 → 49197 [ACK] Seq=1 Ack=308 Win=64128 Len=0
18	0.771520228	192.168.32.100	192.168.32.101	TCP	204	80 → 49197 [PSH, ACK] Seq=1 Ack=308 Win=64128 Len=150 [TCP segment of a reassembled PDU]
19	0.772733222	192.168.32.100	192.168.32.101	HTTP	312	HTTP/1.1 200 OK (text/html)
20	0.773154787	192.168.32.101	192.168.32.100	TCP	60	49197 → 80 [ACK] Seq=308 Ack=410 Win=65292 Len=0
21	0.773155120	192.168.32.101	192.168.32.100	TCP	60	49197 → 80 [FIN, ACK] Seq=308 Ack=410 Win=65292 Len=0
22	0.773188704	192.168.32.100	192.168.32.101	TCP	54	80 → 49197 [ACK] Seq=410 Ack=309 Win=64128 Len=0

Frame 9: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) on interface *eth0
 Ethernet II, Src: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5), Dst: PcsCompu_81:ec:65 (08:00:27:cb:7e:f5)
 Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.101
 Transmission Control Protocol, Src Port: 80, Dst Port: 49197
 [2 Reassembled TCP Segments (408 bytes): #8(150), #9(258)]
 Hypertext Transfer Protocol
 Line-based text data: text/html (10 lines)

Frame (312 bytes) Reassembled TCP (408 bytes)

Packets: 22 · Displayed: 22 (100.0%) · Dropped: 0 (0.0%) Profile: Default

Invece in questa schermata. Lanciando il sito con l'indirizzo HTTP sempre sul sistema Operativo Windows si può vedere come avviene lo scambio dei pacchetti tra i due sistemi operativi ma questa volta non cifrati e non in modalità sicura e si può leggere cosa ci sia all'interno dei pacchetti