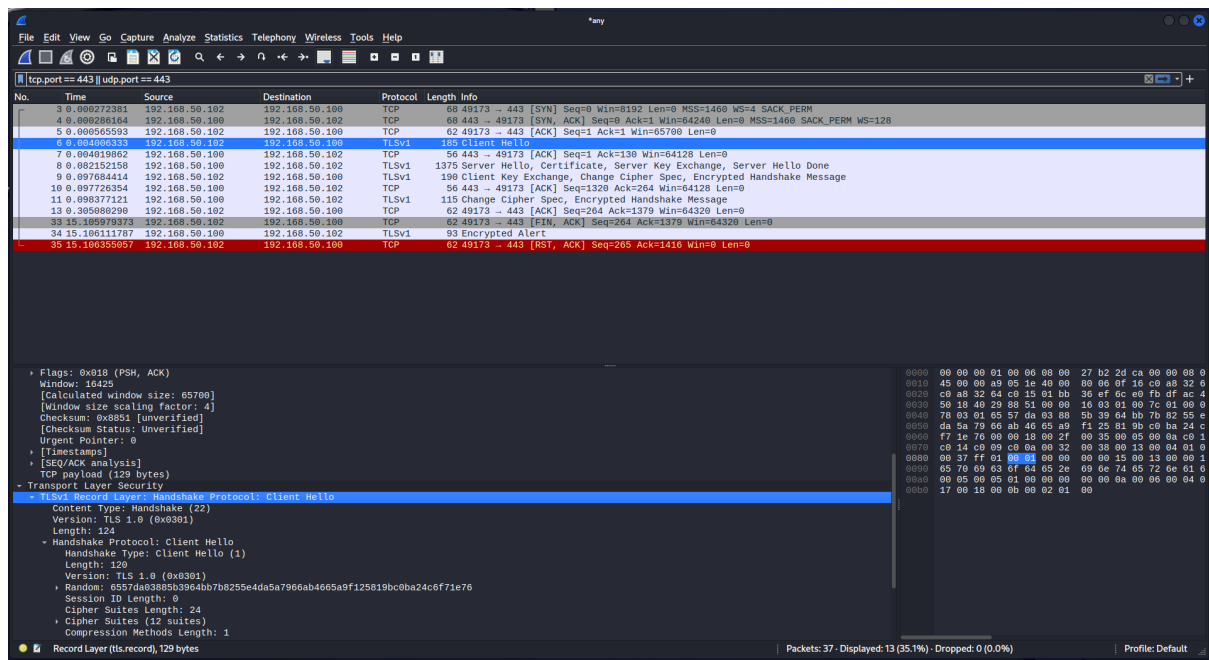


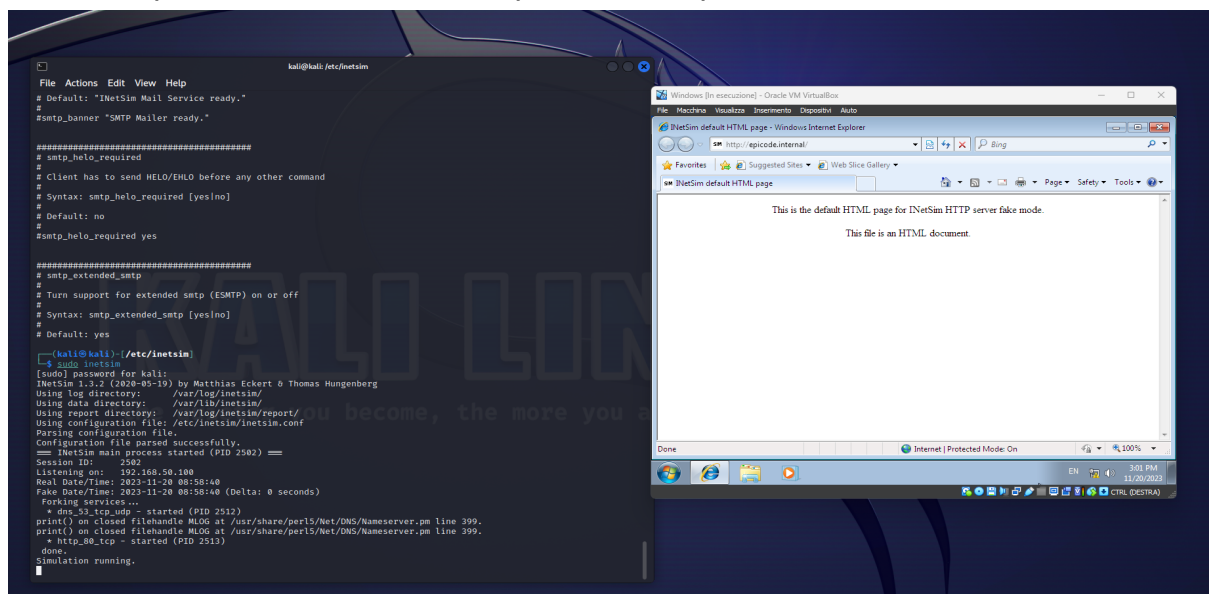
Differenze pacchetti http - https:

► Dopo aver configurato *Inetsim* per la funzione DNS: facendo in modo che il sito *epicode.internal* venga associato all'indirizzo IP assegnato nella macchina VM Kali.

I pacchetti catturati che viaggiavano tramite il protocollo https il contenuto del pacchetto come user agent, lingua e il testo html non erano visibili per via della crittografia TLS (successore di SSL) di https che li rende leggibili solo al destinatario che può decifrare.



Nel protocollo utilizzato http la trasmissione dei pacchetti non viene cifrata e quindi il contenuto può essere letto da terze parti o chiunque abbia accesso alla rete.



In questo caso possiamo vedere le chiamate client server e viceversa, come la lingua impostata (en-us), L'user agent necessario per capire il browser utilizzato, la risoluzione, il sistema operativo e se si è un utente desktop o mobile. Da questo protocollo a differenza di https notiamo anche il tipo di connessione stabilita in questo caso keep-alive e infine anche il contenuto html inviato dal server con tutto quello che contiene.

The image shows a Wireshark packet capture of an HTTP transaction. The top pane displays a list of packets, with packet 10 selected. The middle pane shows the details of the selected packet, including the Hypertext Transfer Protocol section. The bottom pane shows the raw packet data in hexadecimal and ASCII. The HTTP request is a GET request for a file named '1.txt' on the server 'epicode.internal'. The response is a 200 OK status with a Content-Type of 'text/html'.

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000137798	192.168.50.102	192.168.50.100	TCP	68	49162 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
4	0.000152597	192.168.50.100	192.168.50.102	TCP	68	80 → 49162 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
5	0.000332336	192.168.50.102	192.168.50.100	TCP	62	49162 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
6	0.001759880	192.168.50.102	192.168.50.100	HTTP	467	GET / HTTP/1.1
7	0.001773342	192.168.50.100	192.168.50.102	TCP	56	80 → 49162 [ACK] Seq=1 Ack=412 Win=64128 Len=0
8	0.020615671	192.168.50.100	192.168.50.102	TCP	206	80 → 49162 [PSH, ACK] Seq=1 Ack=412 Win=64128 Len=150 [TCP segment of a reassembled PDU]
9	0.023244999	192.168.50.100	192.168.50.102	HTTP	314	HTTP/1.1 200 OK (text/html)
10	0.023452144	192.168.50.102	192.168.50.100	TCP	62	49162 → 80 [ACK] Seq=412 Ack=410 Win=65292 Len=0
11	0.023553829	192.168.50.102	192.168.50.100	TCP	62	49162 → 80 [FIN, ACK] Seq=412 Ack=410 Win=65292 Len=0
12	0.023561797	192.168.50.100	192.168.50.102	TCP	56	80 → 49162 [ACK] Seq=410 Ack=413 Win=64128 Len=0

Details of packet 10 (HTTP request 1/1):

- Accept: image/jpeg, application/x-ms-application, image/gif, application/xaml+xml, image/pjpeg, application/x-ms-xbap, */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR...
Accept-Encoding: gzip, deflate
Host: epicode.internal
Connection: Keep-Alive

Raw packet data (hex):

```
0000 50 18 40 29 21 ee 08 00 47 45 54 20 2f 41 63 63 65 70  
0040 50 18 40 29 21 ee 08 00 47 45 54 20 2f 41 63 63 65 70  
0080 69 63 61 74 69 6f 6e 2f 78 2d 6d 73 2d 65 67 2c 20 61  
00c0 6c 69 63 61 74 69 6f 6e 2c 20 69 6d 61 69 63 61 74  
00e0 6f 69 6c 2c 20 61 78 70 6c 69 63 61 74  
0100 2f 78 61 6d 6c 2b 78 6d 6c 2c 20 69 6d 6d  
0120 2f 70 6a 70 65 6f 2c 20 61 70 70 6c 69  
0140 69 6f 6e 2f 78 2d 6d 73 2d 78 62 61 70  
0160 2f 2a 00 0a 41 63 65 70 74 2d 4c 61  
0180 61 67 65 3a 20 65 6e 2d 55 53 0d 0a 55  
01a0 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c  
01c0 34 2e 30 20 28 63 6f 6d 70 61 74 69 6d  
01e0 20 4d 53 49 45 20 30 2e 30 3b 20 57 69  
0200 77 73 20 4e 54 20 36 2e 31 3b 20 54 72  
0220 6e 74 2f 34 2e 30 3b 20 53 4c 43 43 32  
0240 4e 45 54 20 43 4c 52 20 32 2e 30 2e 35  
0260 37 3b 20 2e 4e 45 54 20 43 4c 52 20 33  
0280 33 30 37 32 39 3b 20 2e 4e 45 54 20 43
```

The image shows a Wireshark packet capture of an HTTP transaction. The top pane displays a list of packets, with packet 10 selected. The middle pane shows the details of the selected packet, including the Hypertext Transfer Protocol section. The bottom pane shows the raw packet data in hexadecimal and ASCII. The HTTP response is a 200 OK status with a Content-Type of 'text/html'. The body of the response is an HTML document.

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000137798	192.168.50.102	192.168.50.100	TCP	68	49162 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
4	0.000152597	192.168.50.100	192.168.50.102	TCP	68	80 → 49162 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
5	0.000332336	192.168.50.102	192.168.50.100	TCP	62	49162 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
6	0.001759880	192.168.50.102	192.168.50.100	HTTP	467	GET / HTTP/1.1
7	0.001773342	192.168.50.100	192.168.50.102	TCP	56	80 → 49162 [ACK] Seq=1 Ack=412 Win=64128 Len=0
8	0.020615671	192.168.50.100	192.168.50.102	TCP	206	80 → 49162 [PSH, ACK] Seq=1 Ack=412 Win=64128 Len=150 [TCP segment of a reassembled PDU]
9	0.023244999	192.168.50.100	192.168.50.102	HTTP	314	HTTP/1.1 200 OK (text/html)
10	0.023452144	192.168.50.102	192.168.50.100	TCP	62	49162 → 80 [ACK] Seq=412 Ack=410 Win=65292 Len=0
11	0.023553829	192.168.50.102	192.168.50.100	TCP	62	49162 → 80 [FIN, ACK] Seq=412 Ack=410 Win=65292 Len=0
12	0.023561797	192.168.50.100	192.168.50.102	TCP	56	80 → 49162 [ACK] Seq=410 Ack=413 Win=64128 Len=0

Details of packet 10 (HTTP response 1/1):

- Server: INetSim HTTP Server
[Time since request: 0.021485119 seconds]
[Request URI: http://epicode.internal/]
File Data: 258 bytes
Line-based text data: text/html (10 lines)

Raw packet data (hex):

```
0000 65 72 0d 0a 0d 0a 3c 68 74 6d 6c 3e 0a  
0040 68 65 61 64 3e 0a 20 20 20 3c 74 69  
0080 3e 49 4e 65 74 53 69 6d 20 64 65 66 61  
00c0 20 48 54 4d 4c 20 70 61 67 65 3c 2f 74  
00e0 65 3e 0a 20 20 3c 2f 68 65 61 64 3e 0a  
0100 62 6f 64 79 3e 0a 20 20 20 3c 70 3e  
0120 3e 0a 20 20 20 3c 70 20 61 6c 69 67  
0140 63 65 6e 74 65 72 3e 54 68 69 73 20  
0160 74 68 65 20 64 65 66 61 75 6c 74 20 48  
0180 20 70 61 67 65 20 66 6f 72 29 49 4e 65  
01a0 6d 20 48 54 50 20 73 65 72 70 65 72  
01c0 6b 65 20 6d 6f 64 65 2e 3c 2f 70 3e 0a  
01e0 20 3c 70 20 61 6c 69 67 6e 3d 22 63 65  
0200 72 22 3e 54 68 69 73 20 66 69 6c 65 20  
0220 61 6e 20 48 54 4d 4e 20 64 6f 63 75 6d  
0240 2e 3c 2f 70 3e 0a 20 3c 2f 62 6f 64  
0260 3c 2f 68 74 6d 6c 3e 0a
```

Oggi quasi tutti i siti web utilizzano il protocollo https per garantire una maggior sicurezza ed evitare il transito dei pacchetti in chiaro. Il protocollo cifrato è assolutamente necessario nei siti dove transitano informazioni sensibili: es. Siti di home banking, e-commerce, exchange di criptovalute ma anche siti di whistleblowing.