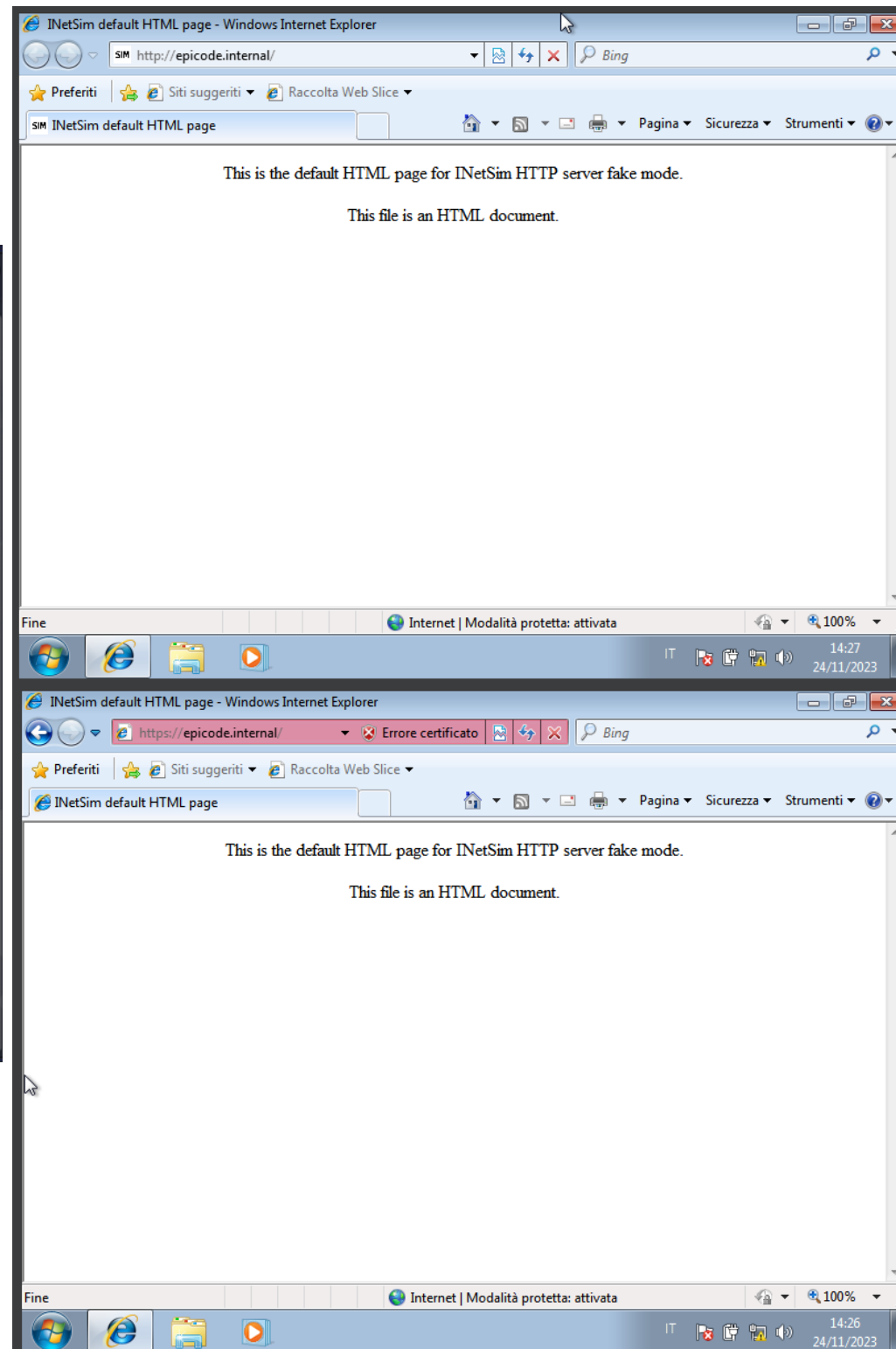


```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.32.100 netmask 255.255.255.0 broadcast 192.168.32.255  
    inet6 fe80::a00:27ff:feeb:7ef5 prefixlen 64 scopeid 0<link>  
    ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)  
    RX packets 498 bytes 53476 (52.2 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 1074 bytes 98908 (96.5 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 1061 bytes 108483 (105.9 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 1061 bytes 108483 (105.9 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@kali)-[~]  
$ sudo ping 192.168.32.101  
PING 192.168.32.101 (192.168.32.101) 56(84) bytes of data:  
64 bytes from 192.168.32.101: icmp_seq=1 ttl=128 time=27.9 ms  
64 bytes from 192.168.32.101: icmp_seq=2 ttl=128 time=0.745 ms  
64 bytes from 192.168.32.101: icmp_seq=3 ttl=128 time=0.551 ms  
64 bytes from 192.168.32.101: icmp_seq=4 ttl=128 time=0.595 ms  
64 bytes from 192.168.32.101: icmp_seq=5 ttl=128 time=0.666 ms  
^C  
— 192.168.32.101 ping statistics —  
5 packets transmitted, 5 received, 0% packet loss, time 4064ms  
rtt min/avg/max/mdev = 0.551/6.085/27.869/10.892 ms  
  
(kali@kali)-[~]  
$
```

```
Windows7 [In esecuzione] - Oracle VM VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto  
  
C:\Windows\system32\cmd.exe  
Microsoft Windows [Versione 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. Tutti i diritti riservati.  
C:\Users\Windows7>ipconfig  
Configurazione IP di Windows  
  
Scheda Ethernet Connessione alla rete locale (LAN):  
    Suffisso DNS specifico per connessione:  
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::bc1c:5c06:a1c5:d76d%11  
    Indirizzo IPv4. . . . . : 192.168.32.101  
    Subnet mask . . . . . : 255.255.255.0  
    Gateway predefinito . . . . . : 192.168.32.1  
  
Scheda Tunnel isatap.{6AE31740-4B40-43BD-986F-2EBE4C8BFB96}:  
    Stato supporto. . . . . : Supporto disconnesso  
    Suffisso DNS specifico per connessione:  
  
C:\Users\Windows7>ping 192.168.32.100  
Esecuzione di Ping 192.168.32.100 con 32 byte di dati:  
Risposta da 192.168.32.100: byte=32 durata<1ms TTL=64  
Risposta da 192.168.32.100: byte=32 durata<1ms TTL=64  
Risposta da 192.168.32.100: byte=32 durata<1ms TTL=64  
Risposta da 192.168.32.100: byte=32 durata<1ms TTL=64  
  
Statistiche Ping per 192.168.32.100:  
    Pacchetti: Trasmessi = 4, Ricevuti = 4,  
    Persi = 0 (0% persi),  
    Tempo approssimativo percorsi andata/ritorno in millisecondi:  
        Minimo = 0ms, Massimo = 1ms, Medio = 0ms  
  
C:\Users\Windows7>_
```

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo inetsim  
[sudo] password for kali:  
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg  
Using log directory: /var/log/inetsim/  
Using data directory: /var/lib/inetsim/  
Using report directory: /var/log/inetsim/report/  
Using configuration file: /etc/inetsim/inetsim.conf  
Parsing configuration file.  
Configuration file parsed successfully.  
== INetSim main process started (PID 72077) ==  
Session ID: 72077  
Listening on: 192.168.32.100  
Real Date/Time: 2023-11-24 08:25:43  
Fake Date/Time: 2023-11-24 08:25:43 (Delta: 0 seconds)  
Forking services ...  
* dns_53_tcp_udp - started (PID 72079)  
print() on closed filehandle MLOG at /usr/share/perl5/Net/DNS/Nameserver.pm line 399.  
print() on closed filehandle MLOG at /usr/share/perl5/Net/DNS/Nameserver.pm line 399.  
* https_443_tcp - started (PID 72081)  
* http_80_tcp - started (PID 72080)  
done.  
Simulation running.  
□
```



Wireshark interface showing network traffic capture on interface eth0. The packet list displays several packets, including ARP requests and responses, and a GET request over HTTP. The packet details pane shows the structure of the selected packet (Frame 6: 451 bytes on wire).

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PcsCompu_5f:81:8f	Broadcast	ARP	60	Who has 192.168.32.100? Tell 192.168.32.101
2	0.000054703	PcsCompu_cb:7e:f5	PcsCompu_5f:81:8f	ARP	42	192.168.32.100 is at 08:00:27:cb:7e:f5
3	0.001403897	192.168.32.101	192.168.32.100	TCP	66	49274 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
4	0.001442958	192.168.32.100	192.168.32.101	TCP	66	80 → 49274 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
5	0.002618057	192.168.32.101	192.168.32.100	TCP	60	49274 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
6	0.005937050	192.168.32.101	192.168.32.100	HTTP	451	GET / HTTP/1.1
7	0.005966824	192.168.32.100	192.168.32.101	TCP	54	80 → 49274 [ACK] Seq=1 Ack=398 Win=64128 Len=0
8	0.017536559	192.168.32.100	192.168.32.101	TCP	204	80 → 49274 [PSH, ACK] Seq=1 Ack=398 Win=64128 Len=150 [TCP segment of a reassembled PDU]
9	0.019973267	192.168.32.100	192.168.32.101	HTTP	312	HTTP/1.1 200 OK (text/html)
10	0.021131790	192.168.32.101	192.168.32.100	TCP	60	49274 → 80 [ACK] Seq=398 Ack=410 Win=65292 Len=0
11	0.021132307	192.168.32.101	192.168.32.100	TCP	60	49274 → 80 [FIN, ACK] Seq=398 Ack=410 Win=65292 Len=0
12	0.021202392	192.168.32.100	192.168.32.101	TCP	54	80 → 49274 [ACK] Seq=410 Ack=399 Win=64128 Len=0
13	5.164135668	PcsCompu_cb:7e:f5	PcsCompu_5f:81:8f	ARP	42	Who has 192.168.32.101? Tell 192.168.32.100
14	5.166299859	PcsCompu_5f:81:8f	PcsCompu_cb:7e:f5	ARP	60	192.168.32.101 is at 08:00:27:5f:81:8f

Frame 6: 451 bytes on wire (3608 bits), 451 bytes captured (3608 bits) on interface eth0, id 0

Ethernet II, Src: PcsCompu_5f:81:8f (08:00:27:5f:81:8f), Dst: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)

- Destination: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)
- Source: PcsCompu_5f:81:8f (08:00:27:5f:81:8f)
- Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 437
- Identification: 0x036c (876)
- 010. = Flags: 0x2, Don't fragment
- ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 128
- Protocol: TCP (6)
- Header Checksum: 0x33bd [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 192.168.32.101
- Destination Address: 192.168.32.100

Transmission Control Protocol, Src Port: 49274, Dst Port: 80, Seq: 1, Ack: 1, Len: 397

Hypertext Transfer Protocol

- GET / HTTP/1.1\r\n
- Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg, application/x-ms-xbap, */*\r\n
- Accept-Language: it-IT\r\n
- User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729)\r\n
- Accept-Encoding: gzip, deflate\r\n
- Host: epicode.internal\r\n
- Connection: Keep-Alive\r\n
- \r\n
- [Full request URI: http://epicode.internal/]
- [HTTP request 1/1]
- [Response in frame: 9]

Wireshark interface showing network traffic capture on interface eth0. The packet list displays several packets, including ARP requests and responses, and a GET request over HTTP. The packet details pane shows the structure of the selected packet (Frame 6: 451 bytes on wire).

RILEVATO IL PROTOCOLLO HTTP, dove possiamo vedere tutto il contenuto .

Durante l’intercettazione dei dati grazie a Wireshark, si può notare che sia l’indirizzo IP che il contenuto sono visibili e non cifrati. I dati che viaggiano sulla rete sono esposti a potenziali attacchi per esempio quello di “man-in-the-middle”, dove un utente malevolo intercetta i dati per rubarli ed utilizzare gli stessi in modo illecito.

Wireshark interface showing network traffic analysis. The top bar indicates the interface is *eth0. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains icons for various functions like capture, analysis, and display filtering.

The main display area shows a list of captured packets. The selected packet (No. 29) is highlighted in blue. The packet details pane on the right shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (TCP).

No.	Time	Source	Destination	Protocol	Length	Info
18	17.974231895	192.168.32.101	192.168.32.100	TCP	66	[TCP Retransmission] 49264 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
19	17.974260292	192.168.32.100	192.168.32.101	TCP	54	80 → 49264 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
20	18.490493393	192.168.32.101	192.168.32.100	TCP	62	[TCP Retransmission] 49264 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM
21	18.490548199	192.168.32.100	192.168.32.101	TCP	54	80 → 49264 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	26.374840066	192.168.32.101	192.168.32.100	TCP	66	49266 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
23	26.374875015	192.168.32.100	192.168.32.101	TCP	66	443 → 49266 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
24	26.376526873	192.168.32.101	192.168.32.100	TCP	60	49266 → 443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
25	26.381639485	192.168.32.101	192.168.32.100	TLSv1	183	Client Hello
26	26.381665395	192.168.32.100	192.168.32.101	TCP	54	443 → 49266 [ACK] Seq=1 Ack=130 Win=64128 Len=0
27	26.412295850	192.168.32.100	192.168.32.101	TLSv1	1373	Server Hello, Certificate, Server Key Exchange, Server Hello Done
28	26.416970756	192.168.32.101	192.168.32.100	TLSv1	188	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
29	26.417853349	192.168.32.100	192.168.32.101	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
30	26.446350531	PcsCompu_5f:81:8f	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101
31	26.623863839	192.168.32.100	192.168.32.101	TCP	113	[TCP Retransmission] 443 → 49266 [PSH, ACK] Seq=1320 Ack=264 Win=64128 Len=59
32	26.624358260	192.168.32.101	192.168.32.100	TCP	60	49266 → 443 [ACK] Seq=264 Ack=1379 Win=64320 Len=0 SLE=1320 SRE=1379
33	26.957382957	PcsCompu_5f:81:8f	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101
34	27.957684807	PcsCompu_5f:81:8f	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101
35	29.589245529	fe80::bc1c:5c06:a1c...	ff02::1:3	LLMNR	84	Standard query 0x5fb2 A wpad
36	29.589245819	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0x5fb2 A wpad
37	29.693002442	fe80::bc1c:5c06:a1c...	ff02::1:3	LLMNR	84	Standard query 0x5fb2 A wpad
38	29.693002734	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0x5fb2 A wpad
39	29.895249968	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD<00>
40	30.645433228	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD<00>
41	31.395755607	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD<00>
42	32.156051112	PcsCompu_5f:81:8f	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101
43	32.957588099	PcsCompu_5f:81:8f	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101
44	33.957339324	PcsCompu_5f:81:8f	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101

Frame 29: 113 bytes on wire (904 bits), 113 bytes captured (904 bits) on interface eth0, id 0

Ethernet II, Src: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5), Dst: PcsCompu_5f:81:8f (08:00:27:5f:81:8f)

- Destination: PcsCompu_5f:81:8f (08:00:27:5f:81:8f)
- Source: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)
- Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.101

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 99
- Identification: 0xc60a (50794)
- 010. = Flags: 0x2, Don't fragment
- ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 64
- Protocol: TCP (6)
- Header Checksum: 0xb210 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 192.168.32.100
- Destination Address: 192.168.32.101

Transmission Control Protocol, Src Port: 443, Dst Port: 49266, Seq: 1320, Ack: 264, Len: 59

Ethernet (eth), 14 bytes

Packets: 70 · Displayed: 70 (100.0%) · Dropped: 0 (0.0%) Profile: Default

RILEVATO IL PROTOCOLLO HTTPS, dove possiamo notare che i dati sono criptati.

Il traffico HTTPS mostra che il contenuto è cifrato, grazie al protocollo TLS, che fornisce un livello di sicurezza aggiuntivo nel caso degli attacchi provenienti da hacker malintenzionati. Ciò risulta fondamentale per quanto riguarda la trasmissione dei dati sensibili e personali, nonché password e dati finanziari.

The image shows a Wireshark network traffic capture on interface eth0. The packet list shows a series of network events, including ARP requests, LLMNR queries, NBNS queries, and a TCP connection establishment sequence. The selected packet is a TCP RST packet with Seq=265, Ack=1416, Win=0, Len=0.

No.	Time	Source	Destination	Protocol	Length	Info
31	26.623863839	192.168.32.100	192.168.32.101	TCP	113	[TCP Retransmission] 443 → 49266 [PSH, ACK] Seq=1320 Ack=264 Win=64128 Len=59
32	26.624558266	192.168.32.101	192.168.32.100	TCP	66	49266 → 443 [ACK] Seq=264 Ack=1379 Win=64320 Len=0 SLE=1320 SRE=1379
33	26.957382957	PcsCompu_5f:81:8f	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101
34	27.957684807	PcsCompu_5f:81:8f	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101
35	29.589245529	fe80::bc1c:5c06:a1c...	ff02::1:3	LLMNR	84	Standard query 0x5fb2 A wpad
36	29.589245819	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0x5fb2 A wpad
37	29.693002442	fe80::bc1c:5c06:a1c...	ff02::1:3	LLMNR	84	Standard query 0x5fb2 A wpad
38	29.693002734	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0x5fb2 A wpad
39	29.895249968	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD<00>
40	30.645433228	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD<00>
41	31.395755607	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD<00>
42	32.156051112	PcsCompu_5f:81:8f	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101
43	32.957588099	PcsCompu_5f:81:8f	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101
44	33.957339324	PcsCompu_5f:81:8f	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101
45	35.292209001	fe80::bc1c:5c06:a1c...	ff02::1:3	LLMNR	84	Standard query 0xccc1 A wpad
46	35.292209239	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0xccc1 A wpad
47	35.403147840	fe80::bc1c:5c06:a1c...	ff02::1:3	LLMNR	84	Standard query 0xccc1 A wpad
48	35.403148307	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0xccc1 A wpad
49	35.599029449	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD<00>
50	36.349306585	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD<00>
51	37.098717146	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD<00>
52	37.849456046	192.168.32.101	192.168.32.100	DNS	90	Standard query 0x894b A www.download.windowsupdate.com
53	37.867256104	192.168.32.100	192.168.32.101	DNS	106	Standard query response 0x894b A www.download.windowsupdate.com A 127.0.0.1
54	38.889487269	192.168.32.101	192.168.32.100	TCP	60	49266 → 443 [FIN, ACK] Seq=264 Ack=1379 Win=64320 Len=0
55	38.890240293	192.168.32.100	192.168.32.101	TLSv1	91	Encrypted Alert
56	38.890986237	192.168.32.101	192.168.32.100	TCP	60	49266 → 443 [RST, ACK] Seq=265 Ack=1416 Win=0 Len=0
57	51.844262275	192.168.32.101	192.168.32.100	TCP	66	49268 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
58	51.844292334	192.168.32.100	192.168.32.101	TCP	54	80 → 49268 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
59	52.349082630	192.168.32.101	192.168.32.100	TCP	66	[TCP Retransmission] 49268 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM

Frame 55: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface eth0, id 0

Ethernet II, Src: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5), Dst: PcsCompu_5f:81:8f (08:00:27:5f:81:8f)

- Destination: PcsCompu_5f:81:8f (08:00:27:5f:81:8f)
- Source: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)
- Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.101

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 77
- Identification: 0xc66c (50796)
- 010. = Flags: 0x2, Don't fragment
- ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 64
- Protocol: TCP (6)
- Header Checksum: 0xb224 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 192.168.32.100

Ethernet (eth), 14 bytes

Packets: 70 · Displayed: 70 (100.0%) · Dropped: 0 (0.0%) Profile: Default

Utilizzando il Wireshark e confrontando i due protocolli possiamo quindi affermare che , l’HTTP è esposto alla compromissione dei dati durante la loro trasmissione, invece l’HTTPS protegge il contenuto da potenziali minacce di intercettazione grazie alla crittografia della comunicazione. I MAC address sia di sorgente che della destinazione vengono evidenziati, ed è fondamentale per controllare e tracciare gli accessi ed i dispositivi all’interno di una rete.