

REPORT - 1

07.05.2023

Eseguito da: Anatoliy Prisyazhnyuk

Configurazione delle macchine virtuali (VM) Kali Linux e Windows 7:

Kali Linux:

Generale	
Nome:	kali-linux-2023.1-virtualbox-amd64
Sistema operativo:	Debian (64-bit)
Sistema	
Memoria di base:	4931 MB
Processori:	2
Ordine di avvio:	Disco fisso, Ottico
Accelerazione:	Paginazione nidificata, PAE/NX, Paravirtualizzazione KVM
Schermo	
Memoria video:	128 MB
Scheda grafica:	VMSVGA
Server di desktop remoto:	Disabilitato
Registrazione:	Disabilitata
Archiviazione	
Controller: IDE	
Dispositivo IDE secondario 0:	[Lettore ottico] Vuoto
Controller: SATA	
Porta SATA 0:	kali-linux-2023.1-virtualbox-amd64.vdi (Normale, 80,09 GB)
Audio	
Driver host:	Windows DirectSound
Controller:	ICH AC97
Rete	
Scheda 1:	Intel PRO/1000 MT Desktop (Rete interna, 'intnet')
USB	
Controller USB:	OHCI
Filtri dispositivi:	0 (0 attivo)
Cartelle condivise	
Nessuna	

Windows 7:

Generale	
Nome:	Windows 7
Sistema operativo:	Windows 7 (64-bit)
Sistema	
Memoria di base:	2048 MB
Processori:	2
Ordine di avvio:	Floppy, Ottico, Disco fisso
Accelerazione:	Paginazione nidificata, PAE/NX, Paravirtualizzazione Hyper-V
Schermo	
Memoria video:	27 MB
Scheda grafica:	VBoxSVGA
Server di desktop remoto:	Disabilitato
Registrazione:	Disabilitata
Archiviazione	
Controller: SATA	
Porta SATA 0:	Windows 7_vdi (Normale, 55,11 GB)
Porta SATA 1:	[Lettore ottico] GSP1RMCPRXFRER_EN_DVD.ISO (3,09 GB)
Porta SATA 2:	[Lettore ottico] 7601.24214.180801-1700.win7sp1_ldr_escrow_CLIENT_ULTIMATE_x64FRE_en-us.iso (5,47 GB)
Audio	
Driver host:	Predefinita
Controller:	Intel HD Audio
Rete	
Scheda 1:	Intel PRO/1000 MT Desktop (Rete interna, 'intnet')
USB	
Controller USB:	OHCI, EHCI
Filtri dispositivi:	0 (0 attivo)
Cartelle condivise	
Nessuna	

Su Kali Linux:

Ho eseguito il comando ifconfig per verificare che IP era presente;

Ho cambiato l'IP ed il gateway con il comando "sudo nano /etc/network/interfaces"

```
GNU nano 7.2 /etc/network/interfaces *
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

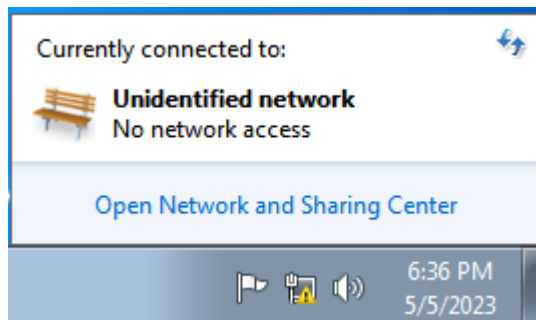
auto eth0
iface eth0 inet static
address 192.168.32.100/24
gateway 192.168.32.1
```

Ho verificato se effettivamente si era cambiato l'IP, controllando con "ifconfig":

```
(kali@kali)~[~]  
$ 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
```

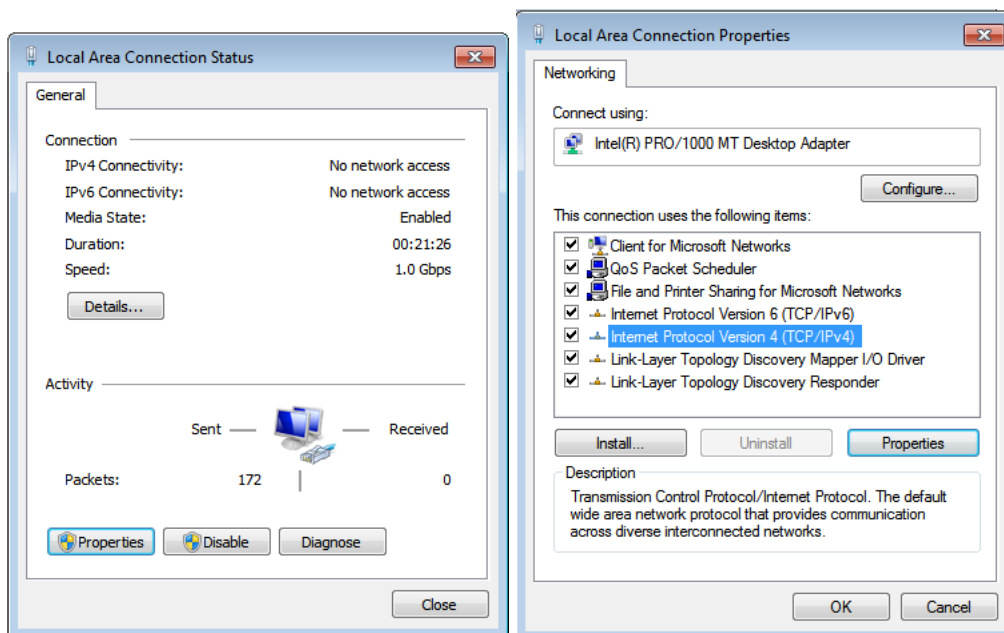
Su Windows 7:

Per effettuare il cambio IP, ho cliccato su "Open Network and Sharing Center", dopodichè su "Local Area Connection":

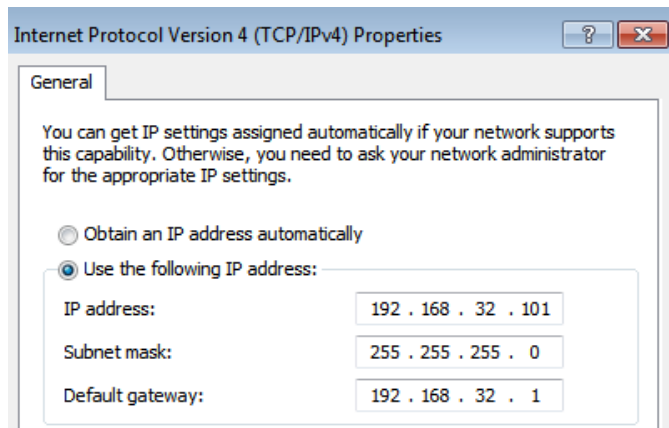


Access type: No network access
Connections: Local Area Connection

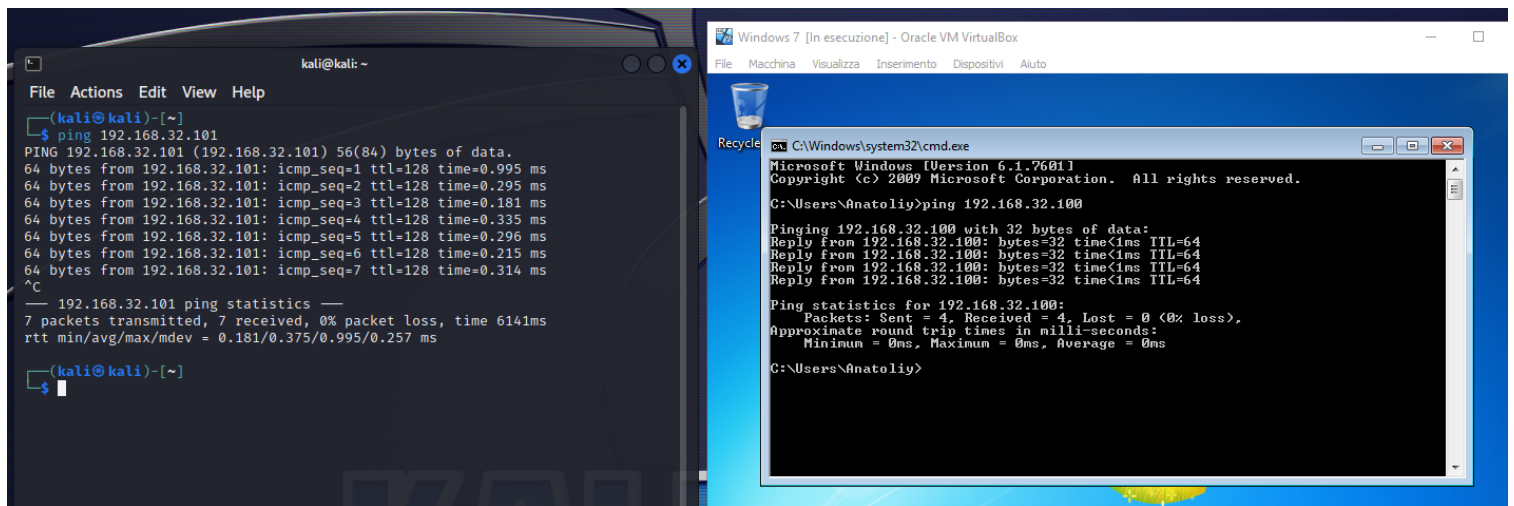
Aperta la schermata del "Local Area Connection", mi dirigo verso "Properties", cliccando poi su "Internet Protocol Version 4 (TCP/IPv4)" per poi cambiare le proprietà:



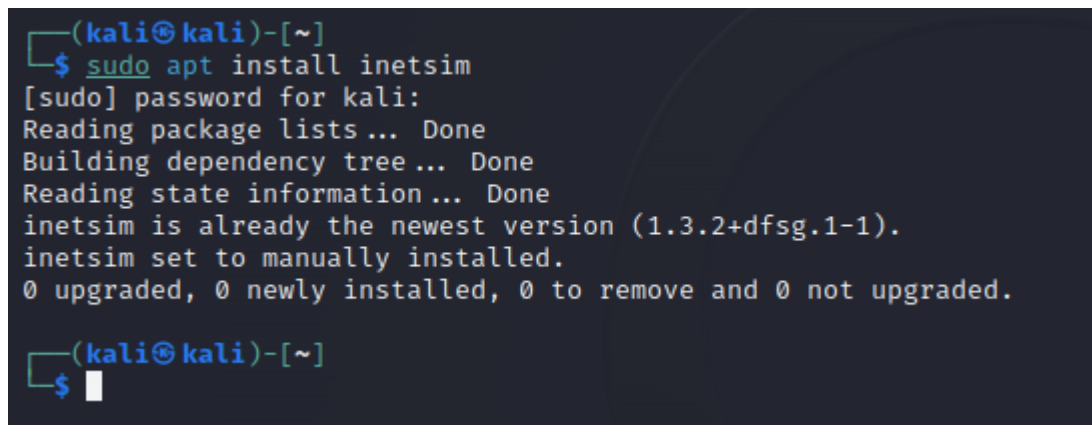
Nella seguente schermata ho cambiato l'IP ed il Default gateway:



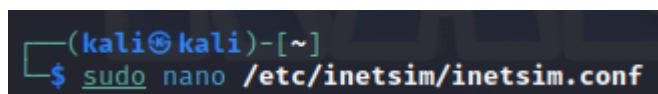
Ho eseguito un controllo se le due Virtual Machine (VM) fossero collegate, con ping e l'IP:



Ho installato InetSim



Dopodichè ho aperto la configurazione dell'InetSim con il comando sottostante:



Modificò il `service_bind_address`, `dns_default_ip` ed anche il DNS static, inserendo il link del sito `epicode.internal` insieme all'IP:

```
#####  
# service_bind_address  
#  
# IP address to bind services to  
#  
# Syntax: service_bind_address <IP address>  
#  
# Default: 127.0.0.1  
#  
service_bind_address 192.168.32.100
```

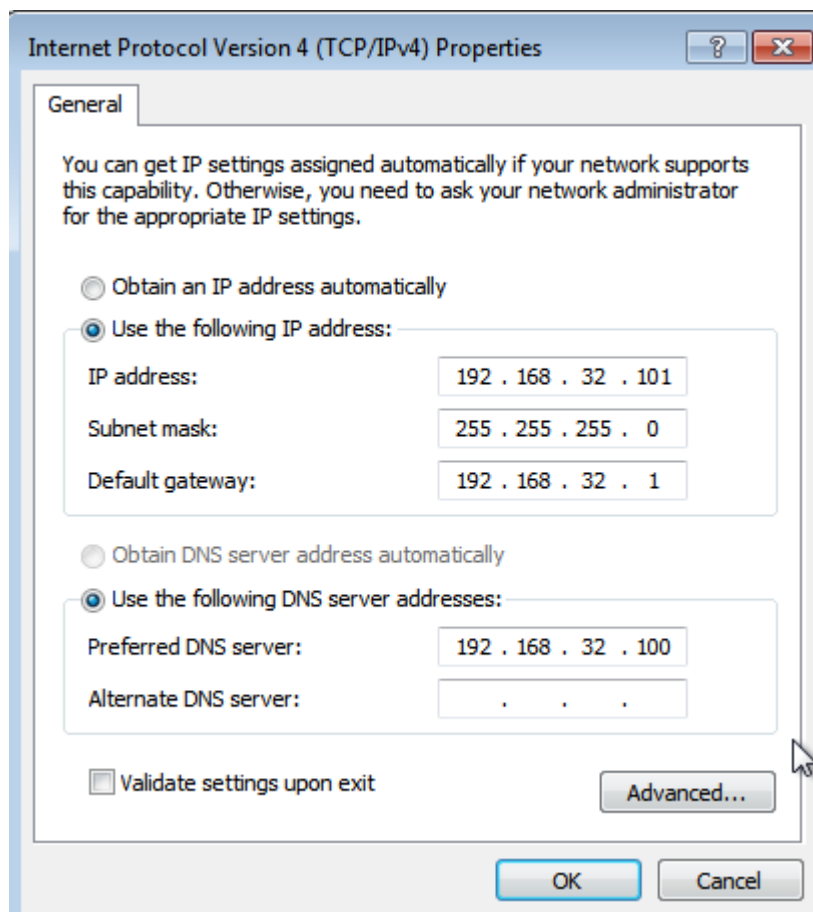
```
#####  
# dns_default_ip  
#  
# Default IP address to return with DNS replies  
#  
# Syntax: dns_default_ip <IP address>  
#  
# Default: 127.0.0.1  
#  
dns_default_ip 192.168.32.100
```

```
#####  
# dns_static  
#  
# Static mappings for DNS  
#  
# Syntax: dns_static <fqdn hostname> <IP address>  
#  
# Default: none  
#  
dns_static epicode.internal 192.168.32.100
```

Ho eseguito il comando “`sudo inetsim`” per effettuare l’avvio di InetSim:

```
(kali㉿kali)-[~]  
$ sudo inetsim  
Simulation running.
```

Su **Windows 7**, ho immesso l'IP del **DNS Server**:



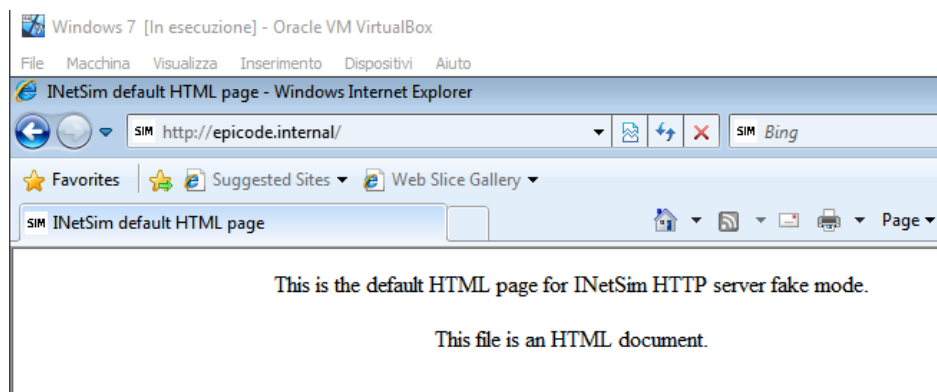
Ho eseguito un check per verificare se pingava *epicode.internal*:

```
C:\Users\Anatoliy>ping epicode.internal

Pinging epicode.internal [192.168.32.100] with 32 bytes of data:
Reply from 192.168.32.100: bytes=32 time<1ms TTL=64
Reply from 192.168.32.100: bytes=32 time<1ms TTL=64
Reply from 192.168.32.100: bytes=32 time<1ms TTL=64
Reply from 192.168.32.100: bytes=32 time<1ms TTL=64

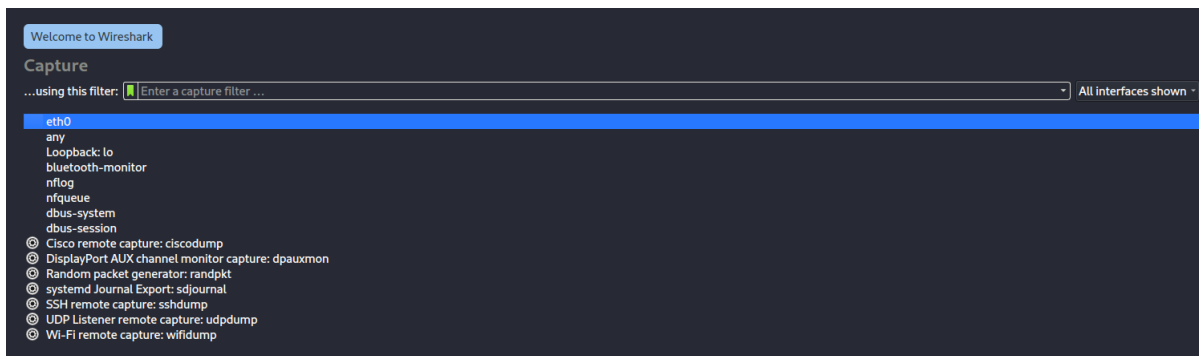
Ping statistics for 192.168.32.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Anatoliy>
```



Wireshark:

Aperto il programma Wireshark, ho fatto doppio click su eth0 per far eseguire il check dei pacchetti:



Dopodichè ho cliccato sul tasto “Restart current capture”



Tra un paio di secondi l’ho stoppato con il pulsante “Stop capturing packets”



Eseguito il check dei pacchetti, ricevo queste informazioni:

No.	Time	Source	Destination	Protocol	Length	Info
3	53.645419378	192.168.32.101	192.168.32.100	TCP	66	49166 → http(80) [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
4	53.645443502	192.168.32.100	192.168.32.101	TCP	66	http(80) → 49166 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
5	53.645542244	192.168.32.101	192.168.32.100	TCP	60	49166 → http(80) [ACK] Seq=1 Ack=1 Win=65700 Len=0
6	53.645663059	192.168.32.101	192.168.32.100	HTTP	361	GET / HTTP/1.1
7	53.645670992	192.168.32.100	192.168.32.101	TCP	54	http(80) → 49166 [ACK] Seq=1 Ack=308 Win=64128 Len=0
8	53.657033074	192.168.32.100	192.168.32.101	TCP	204	http(80) → 49166 [PSH, ACK] Seq=1 Ack=308 Win=64128 Len=150 [TCP segment of a reassembled PDU]
9	53.658460360	192.168.32.100	192.168.32.101	HTTP	312	HTTP/1.1 200 OK (text/html)
10	53.658579628	192.168.32.101	192.168.32.100	TCP	60	49166 → http(80) [ACK] Seq=308 Ack=410 Win=65292 Len=0
11	53.658663859	192.168.32.101	192.168.32.100	TCP	60	49166 → http(80) [FIN, ACK] Seq=308 Ack=410 Win=65292 Len=0
12	53.658676098	192.168.32.100	192.168.32.101	TCP	54	http(80) → 49166 [ACK] Seq=410 Ack=309 Win=64128 Len=0

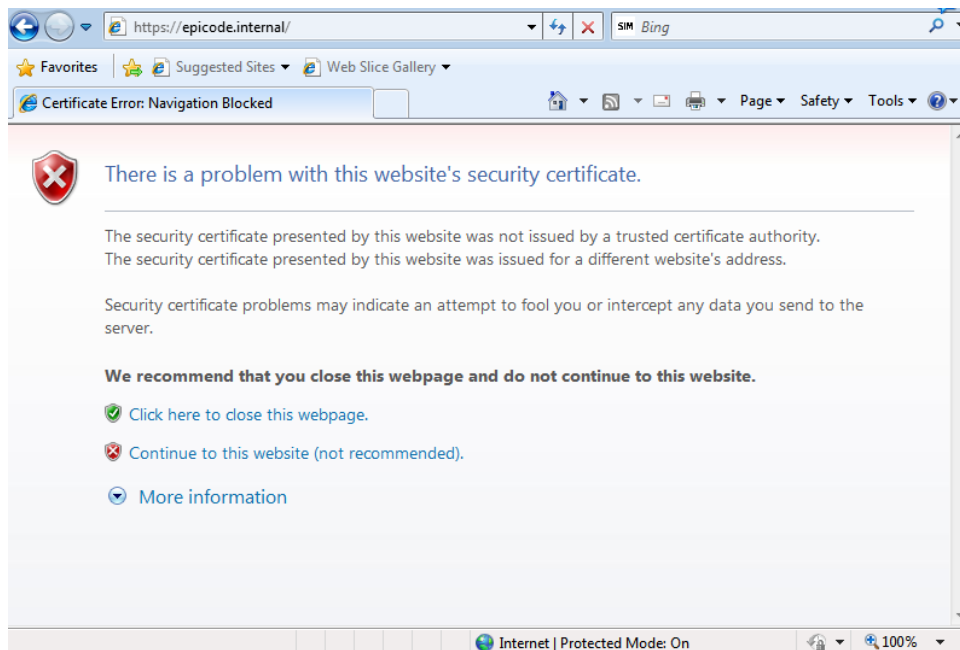
Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0


Ethernet II, Src: PcsCompu (08:00:27:00:00:00), Dst: PcsCompu (08:00:27:00:00:00)

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

Transmission Control Protocol, Src Port: 49166 (49166), Dst Port: http (80), Seq: 0, Len: 0

HTTPS è il protocollo di comunicazione preferibile in quanto offre maggiore sicurezza rispetto a HTTP. HTTPS utilizza certificati SSL per proteggere gli scambi di dati tra il client e il server, mentre HTTP scambia i dati in chiaro. L'analisi dei pacchetti tramite HTTPS risulta quindi più difficile rispetto ad HTTP, poiché i dati sono crittografati e non leggibili. Questo garantisce una maggiore sicurezza delle informazioni trasmesse tramite HTTPS.



Da come vediamo, cliccando su “Continue to this website (not recommended)” ci fa entrare lo stesso, ma pur sempre ci avvisa dell’assenza del certificato con questa icona: 

Ho eseguito un secondo check con Wireshark per HTTPS, ecco i risultati:

ip.addr == 192.168.32.101 tcp.port == 443						
No.	Time	Source	Destination	Protocol	Length	Info
5	0.000362068	192.168.32.101	192.168.32.100	TCP	60	49197 → https(443) [ACK] Seq=1 Ack=1 Win=65700 Len=0
6	0.000501045	192.168.32.101	192.168.32.100	TLSv1	215	Client Hello
7	0.000509004	192.168.32.100	192.168.32.101	TCP	54	https(443) → 49197 [ACK] Seq=1 Ack=162 Win=64128 Len=0
8	0.027695019	192.168.32.100	192.168.32.101	TLSv1	1373	Server Hello, Certificate, Server Key Exchange, Server Hello Done
9	0.031674866	192.168.32.101	192.168.32.100	TLSv1	188	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10	0.032005654	192.168.32.100	192.168.32.101	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
12	0.234963911	192.168.32.101	192.168.32.100	TCP	60	49197 → https(443) [ACK] Seq=296 Ack=1379 Win=64320 Len=0
16	3.176790975	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0xe62a A wpad
18	3.283048551	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0xe62a A wpad
19	3.487172308	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD<00>
20	4.236165558	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD<00>
21	4.986496537	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD<00>
28	8.881202426	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0xdeae A wpad
30	8.988974251	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0xdeae A wpad
31	9.191896590	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD<00>
32	9.942579184	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD<00>
33	10.692871860	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD<00>
34	11.443837461	192.168.32.101	192.168.32.100	TCP	66	49198 → http(80) [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
35	11.443862425	192.168.32.100	192.168.32.101	TCP	66	http(80) → 49198 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
36	11.444045267	192.168.32.101	192.168.32.100	TCP	60	49198 → http(80) [ACK] Seq=1 Ack=1 Win=65536 Len=0
37	11.444045357	192.168.32.101	192.168.32.100	HTTP	271	GET /msdownload/update/v3/static/trusted/en/authrootstl.cab HTTP/1.1
38	11.444071620	192.168.32.100	192.168.32.101	TCP	54	http(80) → 49198 [ACK] Seq=1 Ack=218 Win=64128 Len=0
39	11.455640811	192.168.32.100	192.168.32.101	TCP	204	http(80) → 49198 [PSH, ACK] Seq=1 Ack=218 Win=64128 Len=150 [TCP segment of a reassembled PDU]
40	11.457070677	192.168.32.100	192.168.32.101	HTTP	312	HTTP/1.1 200 OK (text/html)
41	11.457279800	192.168.32.101	192.168.32.100	TCP	60	49198 → http(80) [ACK] Seq=218 Ack=410 Win=65280 Len=0
42	11.457280114	192.168.32.101	192.168.32.100	TCP	60	49198 → http(80) [FIN, ACK] Seq=218 Ack=410 Win=65280 Len=0
43	11.457309004	192.168.32.100	192.168.32.101	TCP	54	http(80) → 49198 [ACK] Seq=410 Ack=219 Win=64128 Len=0

Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0	0000	08 00 27 c7 e1 36 08 00	27 09 99 6c 08 00 45 00	..6..l.E
Ethernet II, Src: PcsCompu.09:99:6c (08:00:27:09:99:6c), Dst: PcsCompu.c7:e1:36 (08:00:27:c7:e1:36)	0010	00 34 02 23 40 00 80 06	36 87 c0 a8 20 65 c0 a8	.4 #0...6...e
Internet Protocol Version 4, Src: 192.168.32.101 (192.168.32.101), Dst: 192.168.32.100 (192.168.32.100)	0020	29 64 c0 2d 01 bb 99 6d	7c 70 00 00 00 00 80 02	d...m p....
Transmission Control Protocol, Src Port: 49197 (49197), Dst Port: https (443), Seq: 0, Len: 0	0030	29 00 b5 35 00 00 02 04	05 b4 01 03 03 02 01 01	5.....
	0040	04 02		