

Progetto

Requisiti e servizi:

- Kali Linux IP: 192.168.32.100
- Windows 7 IP: 192.168.32.101
- HTTPS server: attivo
- Server DNS per risoluzione nomi di dominio: attivo

Traccia:

Simulare, in ambiente di laboratorio virtuale, un'architettura client server in cui un client con indirizzo 192.168.32.101 (Windows 7) richiede tramite web browser una risorsa all'hostname epicode.internal che risponde all'indirizzo 192.168.32.100 (Kali).

Si intercetti poi la comunicazione con Wireshark, evidenziando i MAC address di sorgente e destinazione ed il contenuto della richiesta HTTPS.

Ripetere l'esercizio, sostituendo il server HTTPS, con un server HTTP. Si intercetti nuovamente il traffico, evidenziando le eventuali differenze tra il traffico appena catturato in HTTP ed il traffico precedentemente in HTTPS. Spiegare, motivandole, le principali differenze se presenti.

Svolgimento:

Windows 7:

```
C:\Users\Valerio>ipconfig /all

Configurazione IP di Windows

Nome host . . . . . : Valerio-PC
Suffisso DNS primario . . . . . :
Tipo nodo . . . . . : Ibrido
Routing IP abilitato . . . . . : No
Proxy WINS abilitato . . . . . : No

Scheda Ethernet Connessione alla rete locale (LAN):

Suffisso DNS specifico per connessione:
Descrizione . . . . . : Scheda desktop Intel(R) PRO/1000 MT
Indirizzo fisico . . . . . : 08-00-27-3A-A8-FE
DHCP abilitato . . . . . : No
Configurazione automatica abilitata . . . . . : Sì
Indirizzo IPv4 . . . . . : 192.168.32.101(Preferenziale)
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.32.1
Server DNS . . . . . : 192.168.32.100
NetBIOS su TCP/IP . . . . . : Attivato
```

Kali:

```
(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  
    inet6 fe80::a00:27ff:fe66:d4e0 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:66:d4:e0 txqueuelen 1000 (Ethernet)  
    RX packets 30 bytes 5525 (5.3 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 45 bytes 5984 (5.8 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 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 4 bytes 240 (240.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4 bytes 240 (240.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali㉿kali)-[~]  
$
```

Ping da Kali a Windows 7:

```
(kali㉿kali)-[/]  
$ 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=0.307 ms  
64 bytes from 192.168.32.101: icmp_seq=2 ttl=128 time=0.197 ms  
64 bytes from 192.168.32.101: icmp_seq=3 ttl=128 time=0.180 ms  
64 bytes from 192.168.32.101: icmp_seq=4 ttl=128 time=0.202 ms  
64 bytes from 192.168.32.101: icmp_seq=5 ttl=128 time=0.191 ms  
64 bytes from 192.168.32.101: icmp_seq=6 ttl=128 time=0.187 ms  
64 bytes from 192.168.32.101: icmp_seq=7 ttl=128 time=0.192 ms  
^C  
— 192.168.32.101 ping statistics —  
7 packets transmitted, 7 received, 0% packet loss, time 6140ms  
rtt min/avg/max/mdev = 0.180/0.208/0.307/0.040 ms
```

Ping da Windows 7 a Kali:

```

C:\Users\Valerio>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 = 0ms, Medio = 0ms

C:\Users\Valerio>

```

Nel file di configurazione di InetSim aggiungere l'hostname:

```

#####
# dns_static
#
# Static mappings for DNS
#
# Syntax: dns_static <fqdn hostname> <IP address>
#
# Default: none
#
#dns_static www.foo.com 10.10.10.10
#dns_static ns1.foo.com 10.70.50.30
#dns_static ftp.bar.net 10.10.20.30
dns_static epicode.internal 192.168.32.100

#####

```

Nel file di configurazione di InetSim lasciare attivi i servizi DNS e HTTPS disattivando i servizi HTTP:

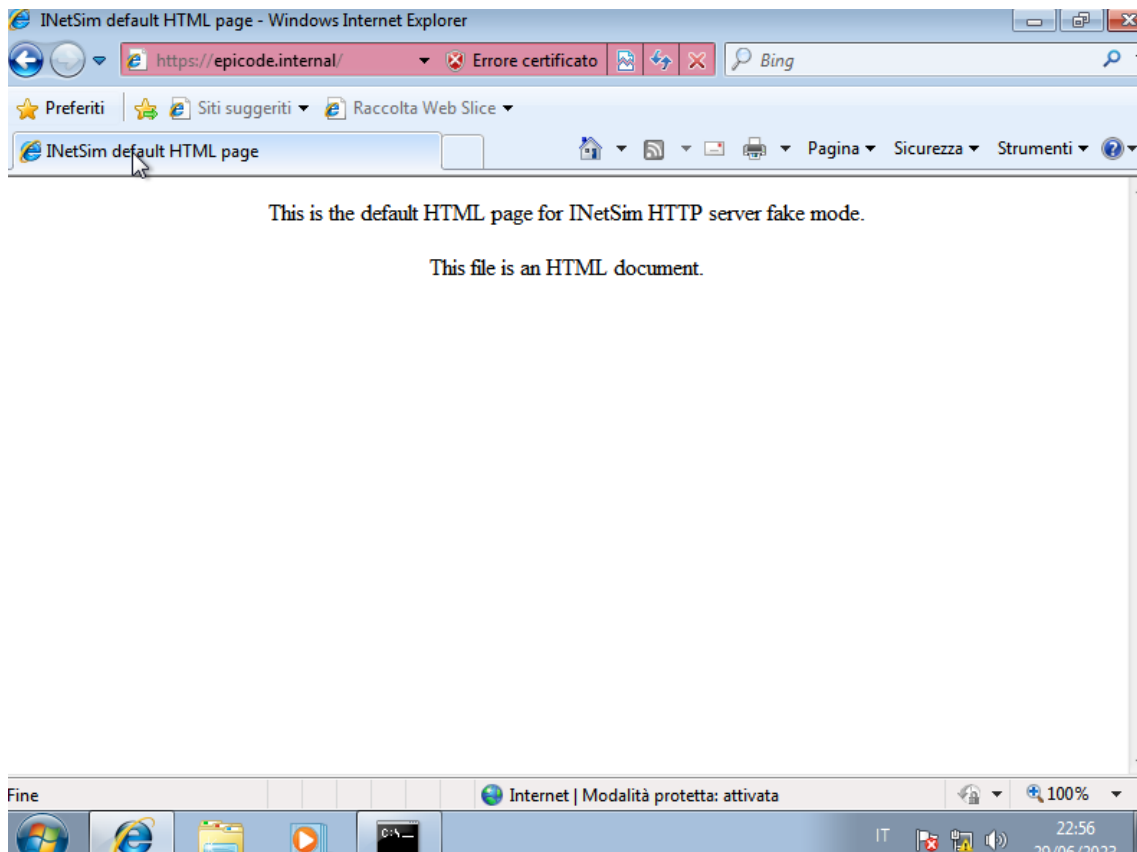
```
# time_udp, daytime_tcp, daytime_udp, echo_tcp,
# echo_udp, discard_tcp, discard_udp, quotd_tcp,
# quotd_udp, chargen_tcp, chargen_udp, finger,
# ident, syslog, dummy_tcp, dummy_udp, smtps, pop3s,
# ftps, irc, https
#
start_service dns
#start_service http
start_service https
start_service smtp
start_service smtps
start_service pop3
start_service pop3s
start_service ftp
start_service ftps
start_service tftp
start_service irc
start_service ntp
start_service finger
start_service ident
start_service syslog
start_service time_tcp
start_service time_udp
start_service daytime_tcp
start_service daytime_udp
start_service echo_tcp
start_service echo_udp
start_service discard_tcp
start_service discard_udp
start_service quotd_tcp
start_service quotd_udp
start_service chargen_tcp
start_service chargen_udp
start_service dummy_tcp
start_service dummy_udp
```

```
#####
```

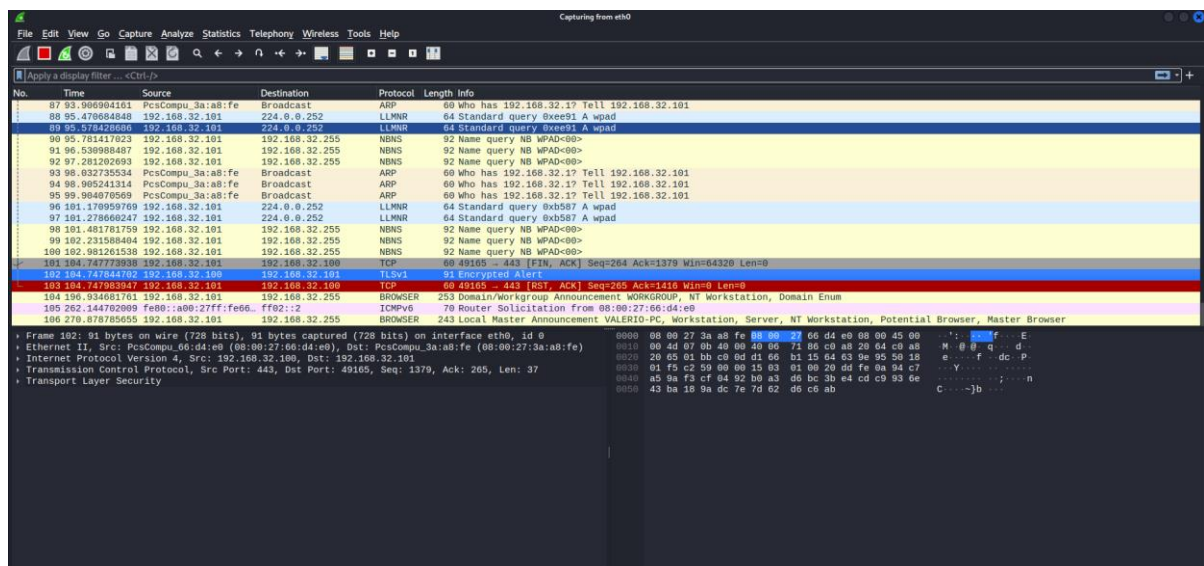
Lanciare InetSim:

```
(kali㉿kali)-[~]
└─$ sudo inetsim
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 1730) ==
Session ID: 1730
Listening on: 192.168.32.100
Real Date/Time: 2023-06-29 16:51:47
Fake Date/Time: 2023-06-29 16:51:47 (Delta: 0 seconds)
Forking services...
* dns_53_tcp_udp - started (PID 1740)
* ntp_123_udp - started (PID 1750)
* ftps_990_tcp - started (PID 1747)
* irc_6667_tcp - started (PID 1749)
* time_37_udp - started (PID 1755)
* finger_79_tcp - started (PID 1751)
* quotd_17_tcp - started (PID 1762)
* ident_113_tcp - started (PID 1752)
* chargen_19_tcp - started (PID 1764)
* syslog_514_udp - started (PID 1753)
* chargen_19_udp - started (PID 1765)
* time_37_tcp - started (PID 1754)
* dummy_1_tcp - started (PID 1766)
* dummy_1_udp - started (PID 1767)
* pop3s_995_tcp - started (PID 1745)
* quotd_17_udp - started (PID 1763)
* daytime_13_tcp - started (PID 1756)
* discard_9_tcp - started (PID 1760)
* discard_9_udp - started (PID 1761)
* daytime_13_udp - started (PID 1757)
* https_443_tcp - started (PID 1741)
* echo_7_tcp - started (PID 1758)
* smtp_25_tcp - started (PID 1742)
* pop3_110_tcp - started (PID 1744)
* echo_7_udp - started (PID 1759)
* smtps_465_tcp - started (PID 1743)
* tftp_69_udp - started (PID 1748)
* ftp_21_tcp - started (PID 1746)
done.
Simulation running.
```

Richiesta web browser "epicode.internal":



Cattura tramite wireshark dei pacchetti criptati:



No.	Time	Source	Destination	Protocol	Length	Info
88	95.478684848	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0xee91 A vpad
89	95.578428686	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0xee91 A vpad
90	95.784147023	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD-00
91	96.539988487	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD-00
92	97.182126093	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD-00
93	98.032739534	PcsCompu_3a:a8:fe	Broadcast	ARP	60	Who has 192.168.32.17 Tell 192.168.32.101
94	98.965241314	PcsCompu_3a:a8:fe	Broadcast	ARP	60	Who has 192.168.32.17 Tell 192.168.32.101
95	99.904870569	PcsCompu_3a:a8:fe	Broadcast	ARP	60	Who has 192.168.32.17 Tell 192.168.32.101
96	101.170959769	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0xb587 A vpad
97	101.278686247	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0xb587 A vpad
98	101.481781759	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD-00
99	102.231588404	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD-00
100	102.981261538	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD-00
101	104.747779908	192.168.32.101	192.168.32.100	TCP	60	49150 -> 443 [RST, ACK] Seq=264 Ack=1379 Win=64320 Len=0
102	104.747844702	192.168.32.100	192.168.32.101	TLSv1	91	Encrypted Alert
103	104.747893947	192.168.32.101	192.168.32.100	TCP	60	49105 -> 443 [RST, ACK] Seq=265 Ack=1416 Win=0 Len=0
104	105.246461011	192.168.32.252	192.168.32.252	WORKGROUP	253	Local/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enu
105	105.2144792099	fe08:1a80:27ff:fe6b::f192:12	fe08:1a80:27ff:fe6b::f192:12	ICMPv6	78	Router Solicitation from 98:08:27:66:d4:e
106	106.2787878555	192.168.32.101	192.168.32.255	BROWSER	243	Local Master Announcement VALERIO-PC, Workstation, Server, NT Workstation, Potential Browser, Master Browser
107	106.4794832563	192.168.32.101	192.168.32.255	BROWSER	253	Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enu
<p>Frame 104: 253 bytes on wire (2024 bits), 253 bytes captured (2024 bits) on interface eth0, id 0</p> <p>Ethernet II, Src: PcsCompu_3a:a8:fe (08:00:27:3c:8d:96), Dst: Broadcast (ff:ff:ff:ff:ff:ff)</p> <p>Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.255</p> <p>User Datagram Protocol, Src Port: 138, Dst Port: 138</p> <p>NetBIOS Datagram Service</p> <p>SMB (Server Message Block Protocol)</p> <p>SMB Mailslot Protocol</p> <p>Microsoft Windows Browser Protocol</p>						
0000	ff	ff	ff	ff	ff	ff 08 00 27 3c 8d 96 00 11 76 aa c0 80 05 c0 85
0001	20	ff	00	8a	00	8a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0002	20	05	00	8a	00	c5 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0003	40	80	45	46	44	45 46 44 45 46 44 45 46 44 45 46 44 45 46 44 45
0004	40	80	45	46	44	45 46 44 45 46 44 45 46 44 45 46 44 45 46 44 45
0005	41	43	41	43	41	43 41 41 43 41 41 43 41 41 43 41 41 43 41 41 43
0006	40	50	45	46	44	45 46 44 45 46 44 45 46 44 45 46 44 45 46 44 45
0007	40	45	46	44	45	46 44 45 46 44 45 46 44 45 46 44 45 46 44 45 46 44 45
0008	25	00	00	00	00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0009	00	00	00	00	00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0010	00	00	00	00	00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0011	00	00	00	00	00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0012	00	00	2b	00	50	00 03 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01
0013	00	00	2b	00	50	00 03 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01
0014	00	8c	4d	41	49	4c 53 4c 54 5c 42 52 47 52 47 53
0015	40	50	45	46	e0	93 04 60 57 52 4b 40 57 52 4b 40 57 52 4b 40 57 52
0016	50	00	00	00	00	00 00 00 00 00

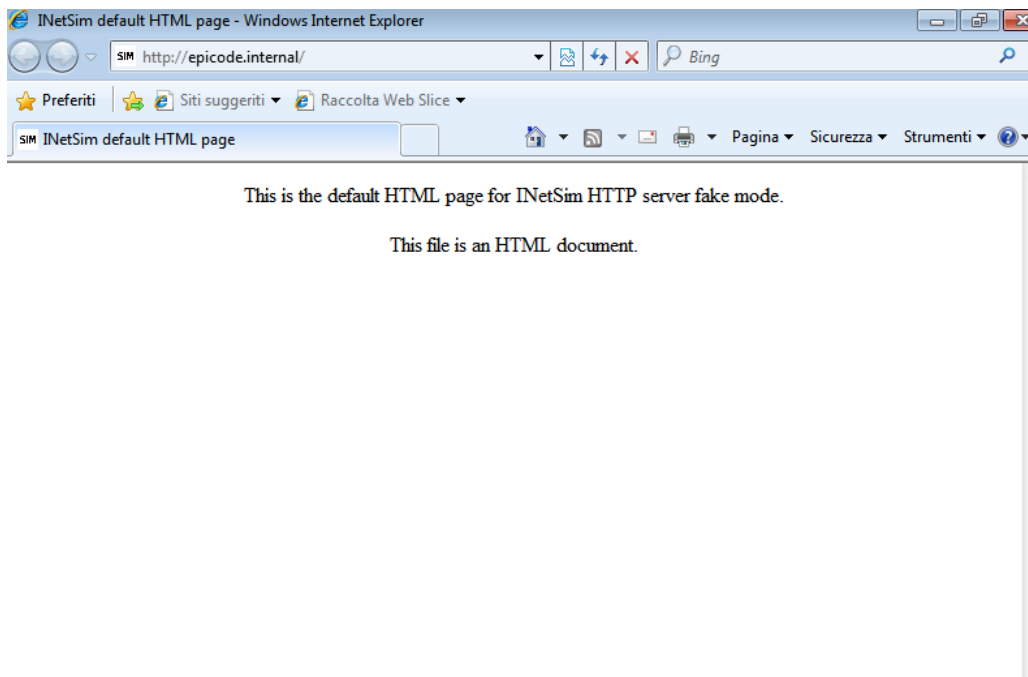
Nel file di configurazione di InetSim lasciare attivi i servizi DNS e HTTP disattivando i servizi HTTPS:

```
# ident, syslog, dummy_tcp, dummy_udp, smtps, pop3s,  
# ftps, irc, https  
#  
start_service dns  
start_service http  
#start_service https  
start_service smtp  
start_service smtps  
start_service pop3  
start_service pop3s  
start_service ftp  
start_service ftps  
start_service tftp  
start_service irc  
start_service ntp  
start_service finger  
start_service ident  
start_service syslog  
start_service time_tcp  
start_service time_udp  
start_service daytime_tcp  
start_service daytime_udp  
start_service echo_tcp  
start_service echo_udp  
start_service discard_tcp  
start_service discard_udp  
start_service quotd_tcp  
start_service quotd_udp  
start_service chargen_tcp  
start_service chargen_udp  
start_service dummy_tcp  
start_service dummy_udp  
  
#####  
#service bind-443tcp
```


Lanciare InetSim:

```
(kali㉿kali)-[~]
$ sudo inetSim
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 9588) ==
Session ID: 9588
Listening on: 192.168.32.100
Real Date/Time: 2023-06-29 17:07:45
Fake Date/Time: 2023-06-29 17:07:45 (Delta: 0 seconds)
Forking services...
* dns_53_tcp_udp - started (PID 9590)
* irc_6667_tcp - started (PID 9599)
* chargen_19_tcp - started (PID 9614)
* finger_79_tcp - started (PID 9601)
* quotd_17_udp - started (PID 9613)
* dummy_1_udp - started (PID 9617)
* echo_7_udp - started (PID 9609)
* pop3s_995_tcp - started (PID 9595)
* syslog_514_udp - started (PID 9603)
* discard_9_udp - started (PID 9611)
* quotd_17_tcp - started (PID 9612)
* discard_9_tcp - started (PID 9610)
* ntp_123_udp - started (PID 9600)
* chargen_19_udp - started (PID 9615)
* time_37_tcp - started (PID 9604)
* http_80_tcp - started (PID 9591)
* daytime_13_tcp - started (PID 9606)
* ident_113_tcp - started (PID 9602)
* smtp_25_tcp - started (PID 9592)
* time_37_udp - started (PID 9605)
* daytime_13_udp - started (PID 9607)
* echo_7_tcp - started (PID 9608)
* tftp_69_udp - started (PID 9598)
* dummy_1_tcp - started (PID 9616)
* smtps_465_tcp - started (PID 9593)
* ftp_21_tcp - started (PID 9596)
* ftps_990_tcp - started (PID 9597)
* pop3_110_tcp - started (PID 9594)
done.
Simulation running.
```

Richiesta web browser “epicode.internal”:



[illegible]

3	0.00012637	192.168.32.101	192.168.32.100	TCP	60 49168 - 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM	
4	0.000137559	192.168.32.100	192.168.32.101	TCP	66 88 - 49168 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128	
5	0.000234712	192.168.32.101	192.168.32.100	TCP	60 49168 - 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0	
6	0.000606077	192.168.32.101	192.168.32.100	HTTP	472 GET / HTTP/1.1	
7	0.000628065	192.168.32.101	192.168.32.101	TCP	54 80 - 49168 [ACK] Seq=1 Ack=419 Win=64128 Len=0	
8	0.011506414	192.168.32.100	192.168.32.101	TCP	204 80 - 49168 [PSH, ACK] Seq=1 Ack=419 Win=64128 Len=158 [TCP segment of a reassembled PDU]	
9	0.011948557	192.168.32.100	192.168.32.101	HTTP	312 HTTP/1.1 200 OK (text/html)	
10	0.012861039	192.168.32.101	192.168.32.100	TCP	60 49168 - 80 [ACK] Seq=419 Ack=419 Win=65292 Len=0	
11	0.012580364	192.168.32.101	192.168.32.100	TCP	60 49168 - 80 [FIN, ACK] Seq=419 Ack=419 Win=65292 Len=0	
12	0.0125159157	192.168.32.100	192.168.32.101	TCP	54 80 - 49168 [ACK] Seq=419 Ack=420 Win=64128 Len=0	
13	0.005825604	192.168.32.101	192.168.32.100	TCP	60 49168 - 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM	
14	0.005838496	192.168.32.100	192.168.32.101	TCP	66 88 - 49169 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128	
15	0.005849434	192.168.32.100	192.168.32.100	TCP	54 49168 - 80 [ACK] Seq=0 Ack=1 Win=65700 Len=0	
16	0.005841593	192.168.32.101	192.168.32.100	HTTP	348 GET /favicon.ico HTTP/1.1	
17	0.005852058	192.168.32.100	192.168.32.101	TCP	54 80 - 49169 [ACK] Seq=1 Ack=295 Win=64128 Len=0	
18	0.001189332	192.168.32.100	192.168.32.101	TCP	207 80 - 49169 [PSH, ACK] Seq=1 Ack=295 Win=64128 Len=153 [TCP segment of a reassembled PDU]	
19	0.002747007	192.168.32.101	192.168.32.101	TCP	252 HTTP/1.1 200 OK (image/x-ico)	
20	0.002762037	192.168.32.101	192.168.32.100	TCP	60 49169 - 80 [ACK] Seq=295 Ack=353 Win=65340 Len=0	

```

Frame 5: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
    Ethernet II, Src: PcsCompu3:a8:f6 (00:02:73:a8:f6), Dst: PcsCompu.66:d4:e0 (00:02:73:d4:e0):
    Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
    Transmission Control Protocol, Src Port: 49168, Dst Port: 80, Seq: 1, Len: 0

```

La prima differenza che notiamo è che la connessione HTTPS comunica sulla porta 80 mentre la connessione HTTP comunica sulla porta 443 questo perché le informazioni che viaggiano su questa porta sono crittografate attraverso la tecnologia SSL/TLS. Come possiamo notare infatti la connessione HTTPS è protetta e le informazioni sono mantenute al sicuro durante il loro transito. Uno dei pacchetti intercettati infatti ha come info "Encrypted Alert". Per quanto riguarda invece la connessione HTTP è messa completamente in chiaro e compaiono all'interno dei pacchetti intercettati tutte le info come l'IP sorgente, l'IP di destinazione, il MAC Address sorgente ed il MAC Address di destinazione. Nella connessione HTTPS vediamo anche dai pacchetti intercettati che viene utilizzata la procedura denominata "three way handshake" la quale permette di instaurare in modo affidabile una connessione TCP.