

Benchmark M1

esercitazione finale modulo 1

Ignazio Saba

INTRODUZIONE

in questa esercitazione simuliamo una comunicazione client server e ne catturiamo i risultati tramite wireshark

il server sarà simulato tramite kali e inetsim a cui attiveremo i servizi dns, http e https
il server sarà così configurato-

IP: 192.168.32.100

netmask: 255.255.255.0

gateway: 192.168.32.1

DNS: 192.168.32.100

il client sarà simulato tramite Windows 7 e sarà così configurato-

IP: 192.168.32.101

netmask: 255.255.255.0

gateway: 192.168.32.1

DNS: 192.168.32.100

configurazioni

network

```
GNU nano 7.2
# This file describes the network interfaces
# and how to activate them. For more information,
# see /usr/share/doc/networking-guide/html/networking.html

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
    dns 192.168.32.100
```

inetsim services

```
#####
# quotd_udp, chargen_tcp, chargen_udp, finger,
# ident, syslog, dummy_tcp, dummy_udp, smtps, pop3s, you can
# 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
```

```
#####
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
service_bind_address 0.0.0.0
```

```
#####
# 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_default_domainname
#
# Default domain name to return with DNS replies
#
# Syntax: dns_default_domainname <domain name>
#
# Default: inetsim.org
#
dns_default_domainname episode.internal
```

configurazioni

network windows 7

```
Ethernet adapter Local Area Connection:

  Connection-specific DNS Suffix . . . . . : 
  Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
  Physical Address . . . . . : 08-00-27-7B-41-73
  DHCP Enabled. . . . . : No
  Autoconfiguration Enabled . . . . . : Yes
  Link-local IPv6 Address . . . . . : fe80::e440:7dd2:595b:c2fx11<Preferred>
  IPv4 Address. . . . . : 192.168.32.101<Preferred>
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.32.1
  DHCPv6 IAID . . . . . : 235405351
  DHCPv6 Client DUID. . . . . : 00-01-00-01-2C-CC-EF-E8-08-00-27-7B-41-73

  DNS Servers . . . . . : 192.168.32.100
                           8.8.4.4
  NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter isatap.{5A70ACFE-DB22-46D7-80FD-72B04FDD4AD1}:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . : 
  Description . . . . . : Microsoft ISATAP Adapter
  Physical Address. . . . . : 00-00-00-00-00-00-E0
  DHCP Enabled. . . . . : No
  Autoconfiguration Enabled . . . . . : Yes

C:\>
```

configurazioni

network windows 7

```
Ethernet adapter Local Area Connection:

  Connection-specific DNS Suffix . . . . . : 
  Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
  Physical Address . . . . . : 08-00-27-7B-41-73
  DHCP Enabled. . . . . : No
  Autoconfiguration Enabled . . . . . : Yes
  Link-local IPv6 Address . . . . . : fe80::e440:7dd2:595b:c2fx11<Preferred>
  IPv4 Address. . . . . : 192.168.32.101<Preferred>
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.32.1
  DHCPv6 IAID . . . . . : 235405351
  DHCPv6 Client DUID. . . . . : 00-01-00-01-2C-CC-EF-E8-08-00-27-7B-41-73

  DNS Servers . . . . . : 192.168.32.100
                           8.8.4.4
  NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter isatap.{5A70ACFE-DB22-46D7-80FD-72B04FDD4AD1}:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . : 
  Description . . . . . : Microsoft ISATAP Adapter
  Physical Address. . . . . : 00-00-00-00-00-00-E0
  DHCP Enabled. . . . . : No
  Autoconfiguration Enabled . . . . . : Yes

C:\>
```

avvio servizi inetsim

```
(kali㉿kali)-[~/inetSim]
$ 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/      If you entered the right address, you can:
Using report directory:   /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf • Try again later
Parsing configuration file.
Configuration file parsed successfully.          • Check your network connection
===== INetSim main process started (PID 46002) ===== • Check that Firefox has permission to access the v
Session ID:      46002
Listening on:    0.0.0.0
Real Date/Time: 2023-11-18 07:48:58
Fake Date/Time: 2023-11-18 07:48:58 (Delta: 0 seconds)
Forking services ...
  * dns_53_tcp_udp - started (PID 46012)
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 46014)
  * http_80_tcp - started (PID 46013)
done.
Simulation running.
```

Hmm, we're having trouble connecting to the server at episode.interactive-hacking.com

We can't connect to the server at episode.interactive-hacking.com

If you entered the right address, you can:

• Try again later

• Check your network connection

• Check that Firefox has permission to access the website

TEST HTTPS

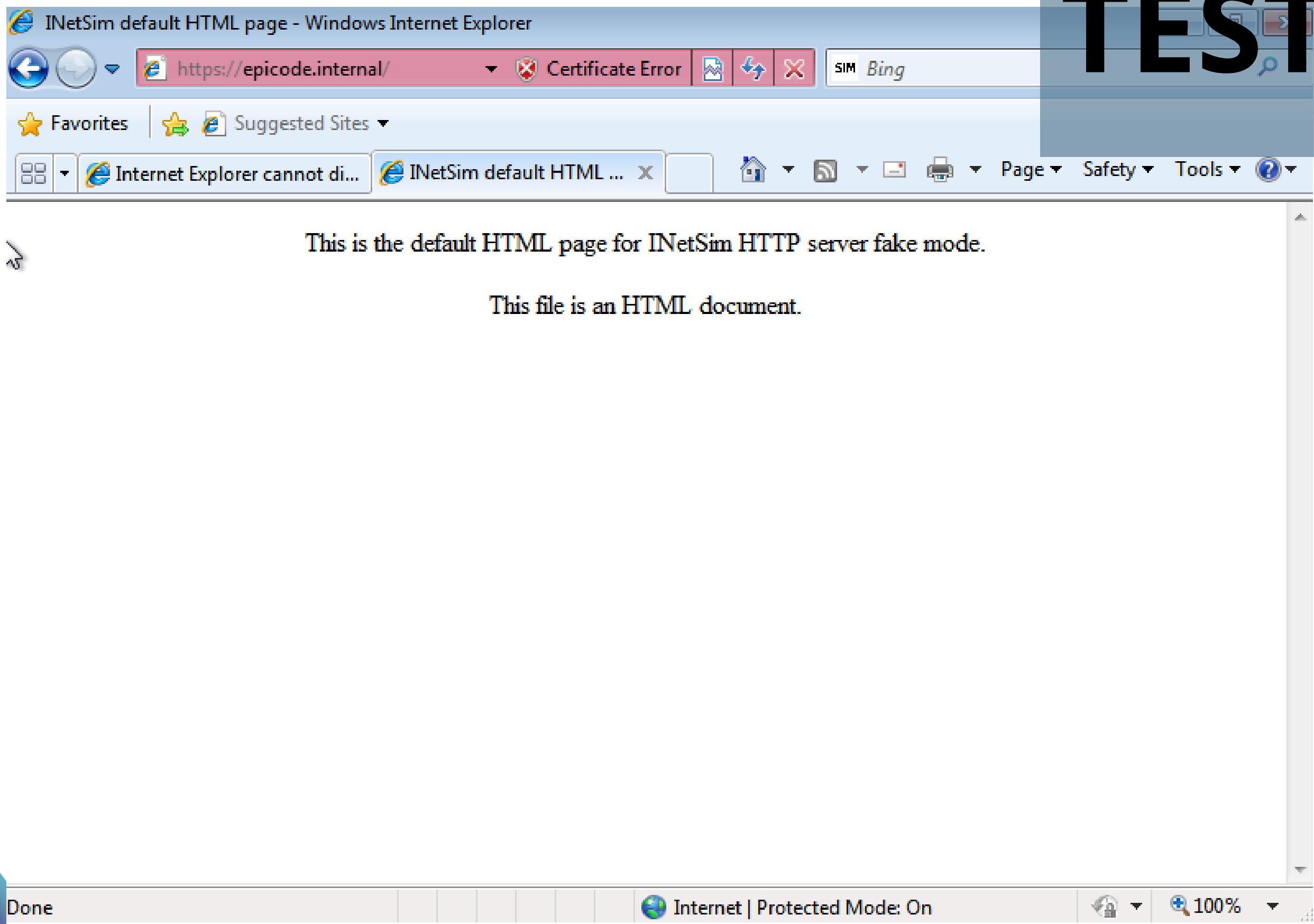
No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000000	192.168.32.101	192.168.32.255	BROWSER	247	Domain/Workgroup Announcement WORKGROUP, NT Workstation
2	2.926416591	192.168.32.101	192.168.32.100	TCP	66	49168 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SA
3	2.926438140	192.168.32.100	192.168.32.101	TCP	66	443 → 49168 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=60 S
4	2.926575657	192.168.32.101	192.168.32.100	TCP	60	49168 → 443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
5	2.926740104	192.168.32.101	192.168.32.100	TLSv1	215	Client Hello
6	2.926745829	192.168.32.100	192.168.32.101	TCP	54	443 → 49168 [ACK] Seq=1 Ack=162 Win=64128 Len=0
7	3.004102208	192.168.32.100	192.168.32.101	TLSv1	1373	Server Hello, Certificate, Server Key Exchange, Server Hello Done
8	3.009878458	192.168.32.101	192.168.32.100	TLSv1	188	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
9	3.009895854	192.168.32.100	192.168.32.101	TCP	54	443 → 49168 [ACK] Seq=1320 Ack=296 Win=64128 Len=0
10	3.010511201	192.168.32.100	192.168.32.101	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
11	3.017944079	PcsCompu_7b:41:73	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101
12	3.215545224	192.168.32.100	192.168.32.101	TCP	113	[TCP Retransmission] 443 → 49168 [PSH, ACK] Seq=1320 Ack=296 Win=64128 Len=59
13	3.215705513	192.168.32.101	192.168.32.100	TCP	66	49168 → 443 [ACK] Seq=296 Ack=1379 Win=64320 Len=0 SLE=1320 SRE=1379
14	3.908076286	PcsCompu_7b:41:73	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101
15	4.908987365	PcsCompu_7b:41:73	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101
16	6.149785457	fe80::e440:7dd2:595...	ff02::1:3	LLMNR	84	Standard query 0x51c0 A wpad
17	6.149883202	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0x51c0 A wpad
18	6.252730871	fe80::e440:7dd2:595...	ff02::1:3	LLMNR	84	Standard query 0x51c0 A wpad
19	6.252731059	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0x51c0 A wpad
20	6.456874808	192.168.32.101	192.168.32.255	MBMS	92	Name QUERY_NB_WPAD<00>

Frame 5: 215 bytes on wire (1720 bits), 215 bytes captured (1720 bits) on interface eth0, tx 0
 Ethernet II, Src: PcsCompu_7b:41:73 (08:00:27:7b:41:73), Dst: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)
 - Destination: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)
 Address: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
 ▾ Source: PcsCompu_7b:41:73 (08:00:27:7b:41:73)
 Address: PcsCompu_7b:41:73 (08:00:27:7b:41:73)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
 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: 201
 Identification: 0x0070 (112)
 010. = Flags: 0x2, Don't fragment
 ...0 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 128
 Protocol: TCP (6)
 Header Checksum: 0x37a5 [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 192.168.32.101

0000	08	00	27	cb	7e	f5	08	00	27	7b	41	73	08	00	45	00	..	'~	'{As	E		
0010	00	c9	00	70	40	00	80	06	37	a5	c0	a8	20	65	c0	a8	..	p@	7	e..		
0020	20	64	c0	10	01	bb	53	8d	64	61	ba	8c	71	b9	50	18	d	..	S	da	qP	
0030	40	29	ab	cd	00	00	16	03	01	00	9c	01	00	00	98	03	@)	
0040	01	65	58	9e	07	04	3b	9f	d7	f5	ea	bf	a0	4f	15	74	eX	;	..	0	t	
0050	83	e6	79	b1	8e	4c	ec	85	ab	93	2c	03	74	36	b1	c3	..y	L	..,	t6..		
0060	57	20	d0	28	5e	d4	a5	36	6c	0a	43	6f	6b	e7	4f	28	W	..(^	6	l	Cok	0(
0070	de	86	61	74	16	07	8c	47	8b	a5	97	40	17	a3	8e	28	..at	..G	..@	(
0080	74	69	00	18	00	2f	00	35	00	05	00	0a	c0	13	c0	14	ti	..	/	5		
0090	c0	09	c0	0a	00	32	00	38	00	13	00	04	01	00	00	37	..2	8	..	7		
00a0	ff	01	00	01	00	00	00	00	15	00	13	00	00	10	65	70ep		
00b0	69	63	6f	64	65	2e	69	6e	74	65	72	6e	61	6c	00	05	icode.in	ternal..		
00c0	00	05	01	00	00	00	00	00	0a	00	06	00	04	00	17	00		
00d0	18	00	0b	00	02	01	00	00	00	00	00	00	00	00	00	00	00	

dalla riga 2 alla 4 possiamo vedere lo scambio di chiavi col tiple hand shake mentre le chiamate TLSV1 sono gli scambi dei pacchetti criptati
 nel riquadro rosso vediamo i due mac address del client e server
source: 08:00:27:7b:41:73 destination: 08:00:27:cb:7e:f5

TEST HTTPS



TEST HTTP

Applica un filtro di visualizzazione ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
10	30.606589931	PcsCompu_7b:41:73	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101
11	30.637517524	fe80::e440:7dd2:595...	ff02::1:2	DHCPv6	146	Solicit XID: 0x3714b1 CID: 000100012cccefe80800277b4173
12	30.732242690	192.168.32.101	192.168.32.100	TCP	66	49168 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
13	30.732263681	192.168.32.100	192.168.32.101	TCP	66	80 → 49168 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
14	30.732381165	192.168.32.101	192.168.32.100	TCP	60	49168 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
15	30.732541805	192.168.32.101	192.168.32.100	HTTP	471	GET /fwlink/?LinkId=69157 HTTP/1.1
16	30.732547380	192.168.32.100	192.168.32.101	TCP	54	80 → 49168 [ACK] Seq=1 Ack=418 Win=64128 Len=0
17	30.749318505	192.168.32.100	192.168.32.101	TCP	204	80 → 49168 [PSH, ACK] Seq=1 Ack=418 Win=64128 Len=150 [TCP segment of a reassembled PDU]
18	30.751433824	192.168.32.100	192.168.32.101	HTTP	312	HTTP/1.1 200 OK (text/html)
19	30.751571806	192.168.32.101	192.168.32.100	TCP	60	49168 → 80 [ACK] Seq=418 Ack=410 Win=65292 Len=0
20	30.751677574	192.168.32.101	192.168.32.100	TCP	60	49168 → 80 [FIN, ACK] Seq=418 Ack=410 Win=65292 Len=0
21	30.751685722	192.168.32.100	192.168.32.101	TCP	54	80 → 49168 [ACK] Seq=410 Ack=419 Win=64128 Len=0
22	30.771621981	192.168.32.101	192.168.32.100	TCP	66	49169 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
23	30.771640672	192.168.32.100	192.168.32.101	TCP	66	80 → 49169 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
24	30.771766290	192.168.32.101	192.168.32.100	TCP	60	49169 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
25	30.771848330	192.168.32.101	192.168.32.100	HTTP	327	GET /favicon.ico HTTP/1.1
26	30.771853830	192.168.32.100	192.168.32.101	TCP	54	80 → 49169 [ACK] Seq=1 Ack=274 Win=64128 Len=0
27	30.787120922	192.168.32.100	192.168.32.101	TCP	207	80 → 49169 [PSH, ACK] Seq=1 Ack=274 Win=64128 Len=153 [TCP segment of a reassembled PDU]
28	30.789260989	192.168.32.100	192.168.32.101	HTTP	252	HTTP/1.1 200 OK (image/x-icon)
29	30.789413793	192.168.32.101	192.168.32.100	TCP	60	49169 → 80 [ACK] Seq=274 Ack=353 Win=65348 Len=0
30	30.789534282	192.168.32.101	192.168.32.100	TCP	60	49169 → 80 [FIN, ACK] Seq=274 Ack=353 Win=65348 Len=0
31	30.789542016	192.168.32.100	192.168.32.101	TCP	54	80 → 49169 [ACK] Seq=275 Win=64128 Len=0

Frame 18: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) on interface eth0, id 0

Ethernet II, Src: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5), Dst: PcsCompu_7b:41:73 (08:00:27:7b:41:73)

- Destination: PcsCompu_7b:41:73 (08:00:27:7b:41:73)
- 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

Transmission Control Protocol, Src Port: 80, Dst Port: 49168, Seq: 151, Ack: 418, Len: 258

Source Port: 80
Destination Port: 49168
[Stream index: 0]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 258]
Sequence Number: 151 (relative sequence number)
Sequence Number (raw): 2427676771
[Next Sequence Number: 410 (relative sequence number)]
Acknowledgment Number: 418 (relative ack number)
Acknowledgment number (raw): 1965049375
0101 = Header Length: 20 bytes (5)

Flags: 0x019 (FIN, PSH, ACK)
Window: 501
[Calculated window size: 64128]
[Window size scaling factor: 128]
Checksum: 0xc336 [unverified]

Frame (312 bytes) | Reassembled TCP (408 bytes)

```

0000 08 00 27 7b 41 73 08 00 27 cb 7e f5 08 00 45 00
0010 01 2a e7 22 40 00 40 06 90 91 c0 a8 20 64 c0 a8
0020 20 65 00 50 c0 10 90 b3 68 63 75 20 46 1f 50 19
0030 01 f5 c3 36 00 00 3c 68 74 6d 6c 3e 0a 20 20 3c
0040 68 65 61 64 3e 0a 20 20 20 20 3c 74 69 74 6c 65
0050 3e 49 4e 65 74 53 69 6d 20 64 65 66 61 75 6c 74
0060 20 48 54 4d 4c 20 70 61 67 65 3c 2f 74 69 74 6c
0070 65 3e 0a 20 20 3c 2f 68 65 61 64 3e 0a 20 20 3c
0080 62 6f 64 79 3e 0a 20 20 20 20 3c 70 3e 3c 2f 70
0090 3e 0a 20 20 20 20 3c 70 20 61 6c 69 67 6e 3d 22
00a0 63 65 6e 74 65 72 22 3e 54 68 69 73 20 69 73 20
00b0 74 68 65 20 64 65 66 61 75 6c 74 20 48 54 4d 4c
00c0 20 70 61 67 65 20 66 6f 72 20 49 4e 65 74 53 69
00d0 6d 20 48 54 54 50 20 73 65 72 76 65 72 20 66 61
00e0 6b 65 20 6d 6f 64 65 2e 3c 2f 70 3e 0a 20 20 20
00f0 20 3c 70 20 61 6c 69 67 6e 3d 22 63 65 6e 74 65
0100 72 22 3e 54 68 69 73 20 66 69 6c 65 20 69 73 20
0110 61 6e 20 48 54 4d 4c 20 64 6f 63 75 6d 65 6e 74
0120 2e 3c 2f 70 3e 0a 20 20 3c 2f 62 6f 64 79 3e 0a
0130 3c 2f 68 74 6d 6c 3e 0a

```

'{As...'.~..E.
.*"@... d..
e.P... hcu F.P.
...6.<h tml>. <
head> <title
>INetSim default
HTML pa ge</titl
e> </h ead> <
body> <p></p
> <p align="center"> This is
the defa ult HTML
page fo r INetSi
m HTTP s erver fa
ke mode. </p>
<p align="cente
r">This file is
an HTML document
. </p> </body>
</html>.

A differenza delle chiamate https qui dopo lo scambio delle chiavi la trasmissione delle informazioni è in chiaro, come si può vedere nella riga selezionata, nel riquadro rosso vediamo il contenuto della pagina http

TEST HTTP

