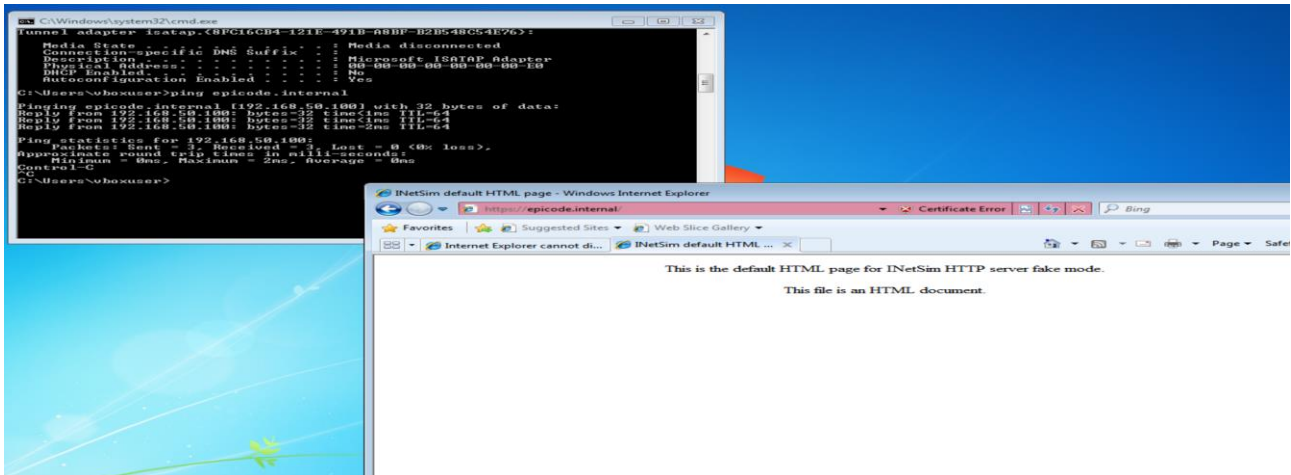
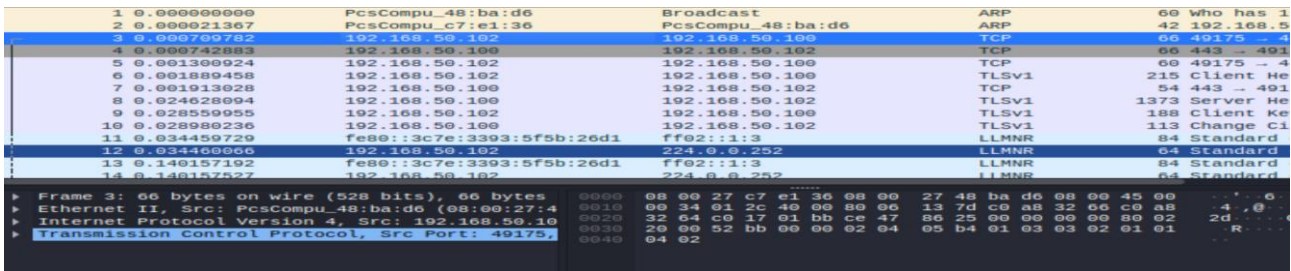


# Progetto Fine 1° Modulo

Chiamata <https://epicode.internal/>

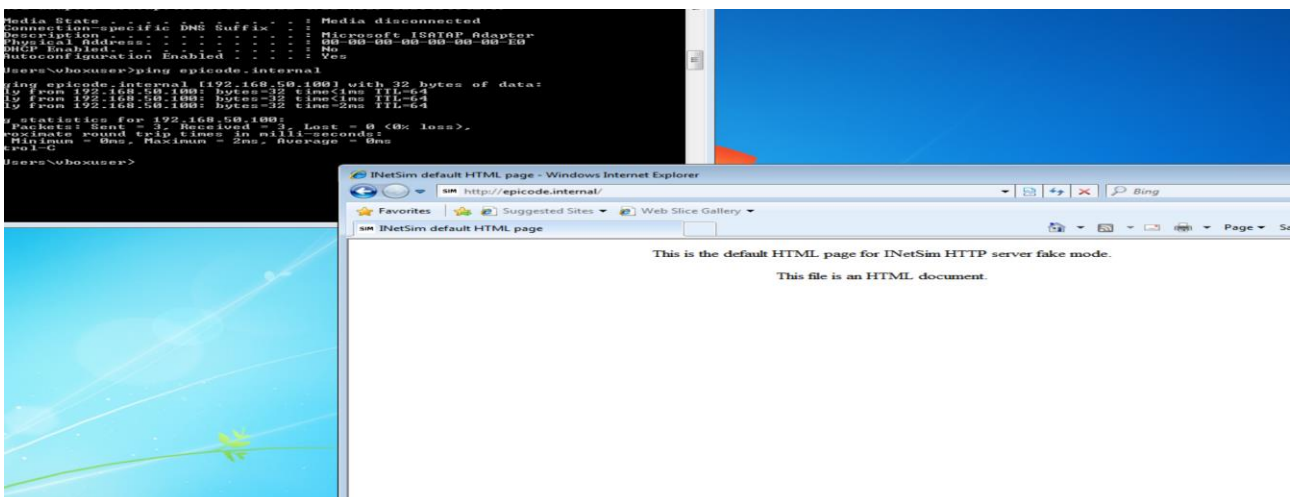


Catturo pacchetti con wireShark:



Indirizzo MAC: 08:00:27:48:ba:d6

Chiamata <http://epicode.internal/>



Catturo pacchetti con wireShark

1	0.000000000	PcsCompu_48:ba:d6	Broadcast	ARP	00 Who has 102.102.102.102
2	0.000000000	PcsCompu_c7:e1:30	PcsCompu_48:ba:d6	ARP	42 102.102.102.102
3	0.000000000	PcsCompu_c7:e1:30	PcsCompu_48:ba:d6	TCP	60 49175 -> 443 [FIN, ACK] Seq=1891
4	0.000000000	192.168.50.100	192.168.50.100	TCP	60 80 -> 49170 [SYN, ACK] Seq=1891
5	0.000000000	192.168.50.102	192.168.50.100	TCP	60 49170 -> 80 [ACK] Seq=1891
6	0.000000000	192.168.50.102	192.168.50.100	HTTP	472 GET / HTTP/1.1
7	0.000000000	192.168.50.100	192.168.50.102	TCP	64 80 -> 49170 [ACK] Seq=1891
8	0.000000000	192.168.50.100	192.168.50.102	TCP	284 80 -> 49170 [ACK] Seq=1891
9	0.000000000	192.168.50.100	192.168.50.102	HTTP	312 HTTP/1.1 200 OK
10	0.000000000	192.168.50.100	192.168.50.102	TCP	60 49170 -> 80 [ACK] Seq=1891
11	0.000000000	192.168.50.102	192.168.50.100	TCP	60 49170 -> 80 [ACK] Seq=1891
12	0.000000000	192.168.50.100	192.168.50.102	TCP	64 80 -> 49170 [ACK] Seq=1891
13	0.000000000	PcsCompu_c7:e1:30	PcsCompu_48:ba:d6	ARP	42 Who has 102.102.102.102
14	0.000000000	PcsCompu_48:ba:d6	PcsCompu_c7:e1:30	ARP	00 102.102.102.102
15	0.000000000	PcsCompu_c7:e1:30	PcsCompu_48:ba:d6	ARP	42 Who has 102.102.102.102

Indirizzo MAC: 08:00:27:48:ba:d6

## Differenze Trovate:

In caso di chiamata tramite protocollo https non viene catturato nessun pacchetto con protocollo di tipo http/https, in quanto essendo una comunicazione criptata non si evidenziano le risposte del server (nel nostro caso, nella chiamata http si evidenzia nella colonna info una "GET").

Nel caso della chiamata http viene utilizzata la porta 80, nel caso della chiamata https invece la porta 443

https:

TCP	60	49175	->	443	[FIN, ACK]	Seq=1891
TCP	54	443	->	49175	[ACK]	Seq=1891
TCP	66	49177	->	443	[SYN]	Seq=0 Win=0
TCP	66	443	->	49177	[SYN, ACK]	Seq=1891
TCP	60	49177	->	443	[ACK]	Seq=1 Ack=1
TLSv1	215	Client Hello				
TCP	54	443	->	49177	[ACK]	Seq=1 Ack=1

http:

192.168.50.100	TCP	60	49170
192.168.50.100	HTTP	472	GET /
192.168.50.102	TCP	54	80 -> 49170
192.168.50.102	TCP	284	80 -> 49170
192.168.50.102	HTTP	312	HTTP/1.1
192.168.50.100	TCP	60	49170
192.168.50.100	TCP	60	49170
192.168.50.102	TCP	54	80 -> 49170

Nel caso delle chiamate https, sono presenti i certificati TLSv1 per garantire la sicurezza della comunicazione, in quanto comunicazione criptata.

192.168.50.100	TCP	66	49177 -> 443 [SYN] Seq=0 Win=0 Len=0 MSS=1460 WS=4 SACK_PERM=1
192.168.50.100	TCP	66	443 -> 49177 [SYN, ACK] Seq=1891 Ack=1 Win=0 Len=0 MSS=1460 SACK_PERM=1
192.168.50.100	TCP	60	49177 -> 443 [ACK] Seq=1 Ack=1 Win=0 Len=0
192.168.50.100	TLSv1	215	Client Hello
192.168.50.102	TCP	54	443 -> 49177 [ACK] Seq=1 Ack=162 Win=64128 Len=0
192.168.50.102	TLSv1	1373	Server Hello, Certificate, Server Key Exchange, Server Hello Done
192.168.50.100	TLSv1	188	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
192.168.50.102	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
ff02::1:3	LLMNR	84	Standard query 0x03ee A wpad
224.0.0.252	LLMNR	64	Standard query 0x03ee A wpad
ff02::1:3	LLMNR	84	Standard query 0x03ee A wpad
224.0.0.252	LLMNR	64	Standard query 0x03ee A wpad
192.168.50.100	TCP	60	49177 -> 443 [ACK] Seq=296 Ack=1379 Win=64320 Len=0
192.168.50.255	NBNS	92	Name query NB WPAD<00>
192.168.50.255	NBNS	92	Name query NB WPAD<00>
192.168.50.255	NBNS	92	Name query NB WPAD<00>

Per concludere, i dati trasmessi tramite http saranno visibile e leggibili, i dati trasmessi tramite https invece saranno non leggibili.