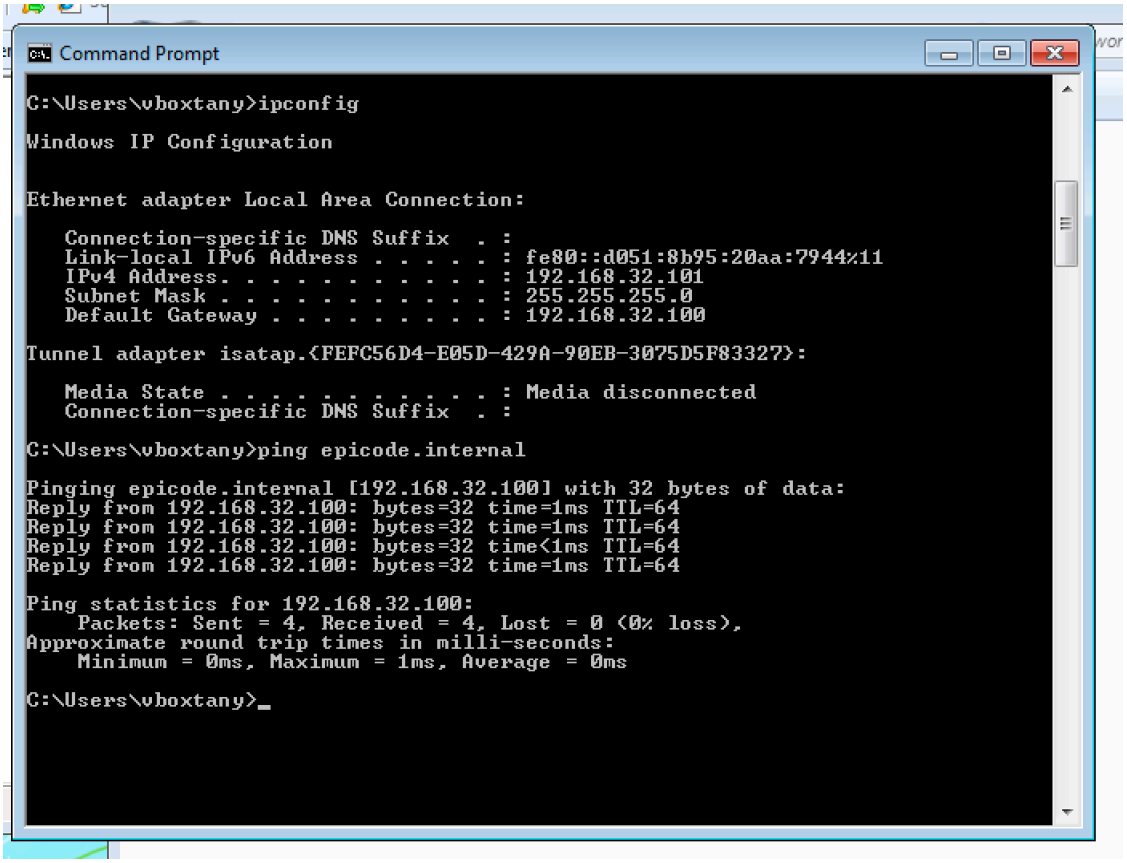
PROGETTO 1° Modulo

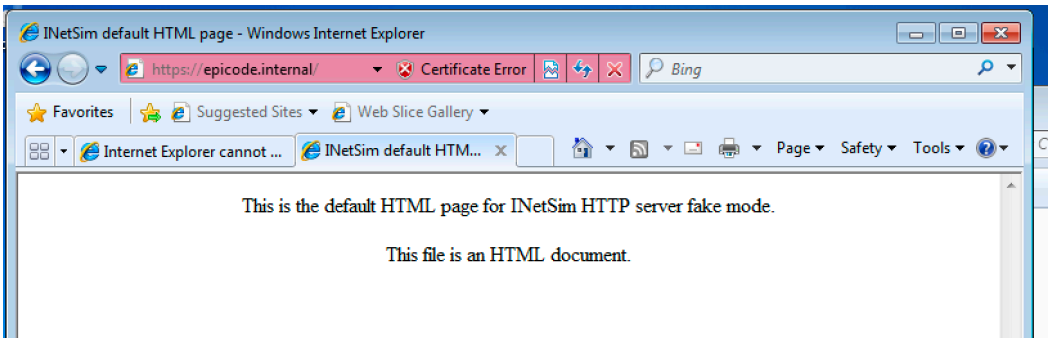
1) Kali Linux con IP `192.168.32.10`

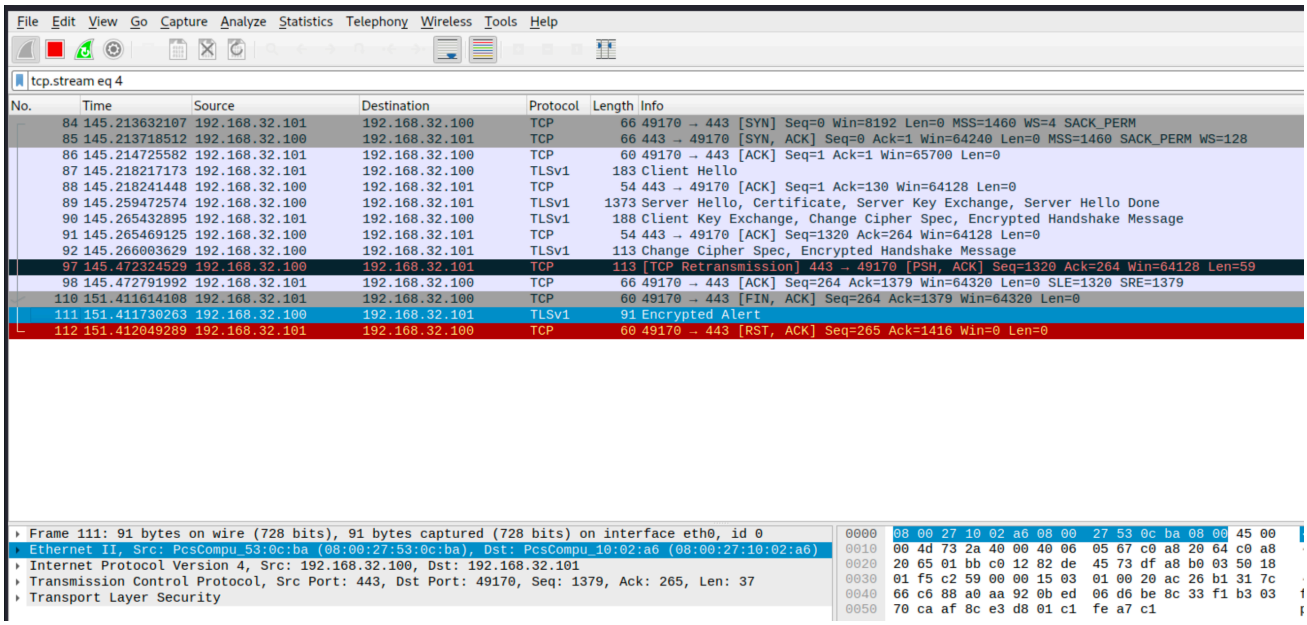
```
┌──(kali㉿kali)-[~]
└─$ sudo setxkbmap it
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:53:0c:ba brd ff:ff:ff:ff:ff:ff
    inet 192.168.32.100/24 brd 192.168.32.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe53:cba/64 scope link
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$
```

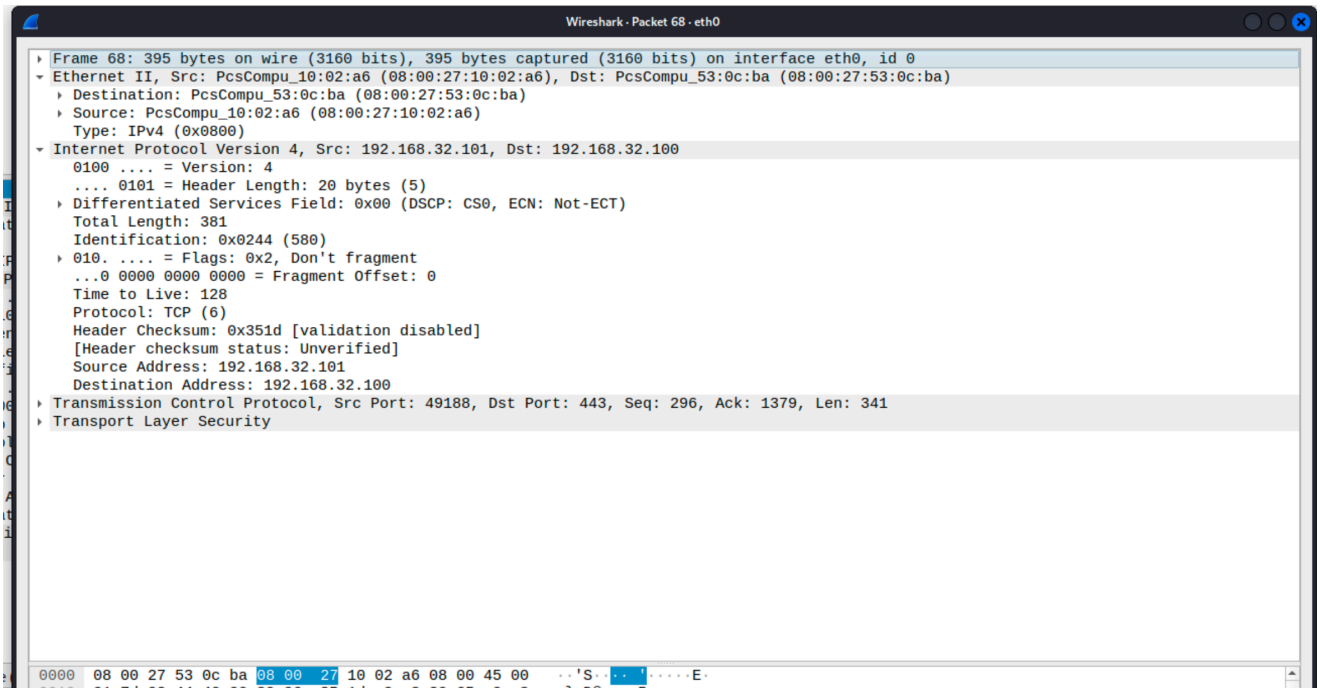
2) Windows7 con IP `192.168.32.101`



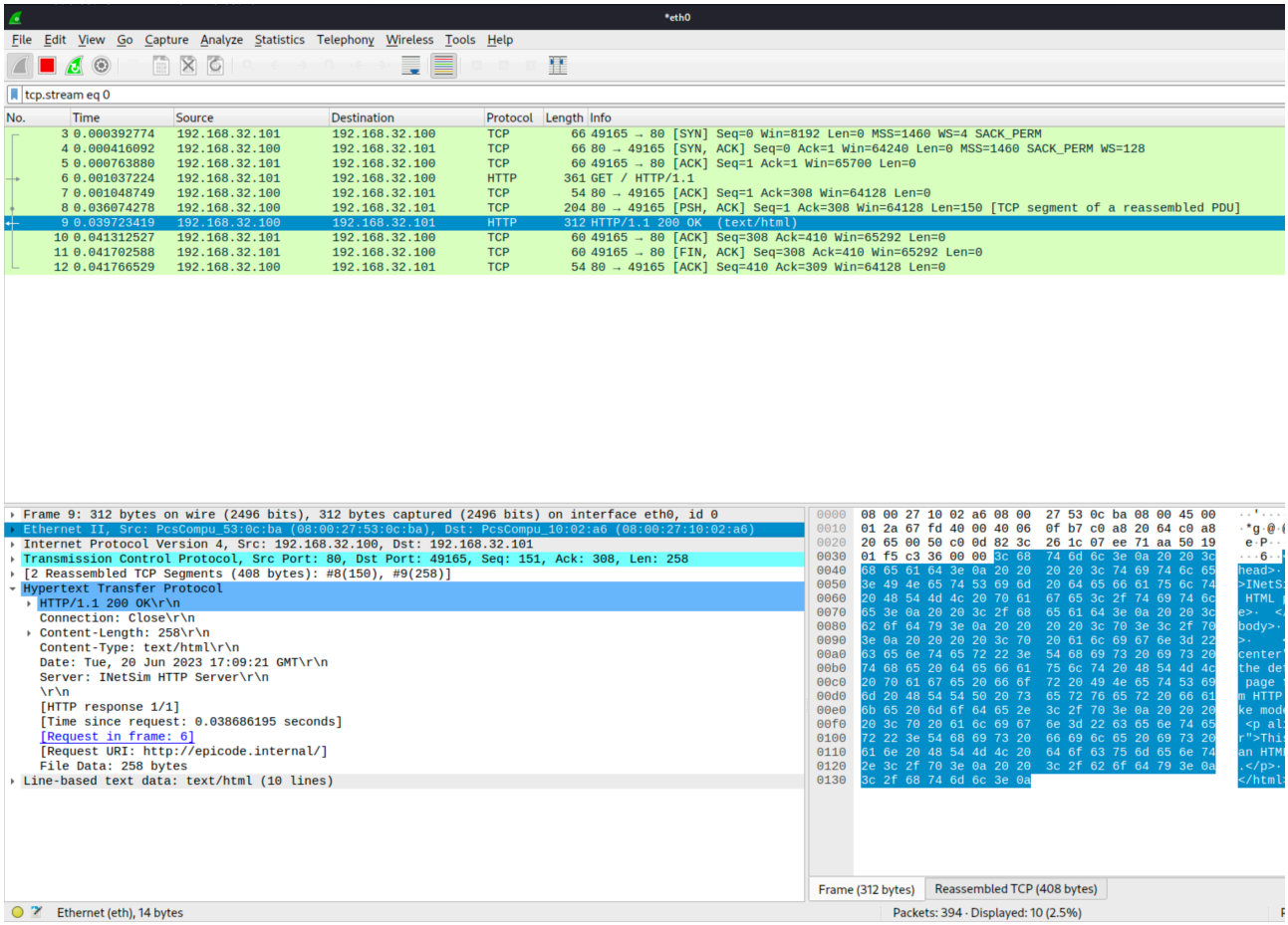
3) Richiesta tramite web browser “epicode.internal”, intercettazione con Wireshark e MAC Address di sorgente e destinazione evidenziati.
Contenuto della richiesta HTTPS.







4) Richiesta con server HTTP.



Le differenze con il protocollo HTTP e quello HTTPS sono che quest'ultimo è la versione sicura e rendere cifrato il traffico web.

Quindi vediamo che con la richiesta HTTP tutto il traffico è in chiaro, possiamo vedere tutti i pacchetti generati e il contenuto, mentre con la richiesta HTTPS il traffico catturato non è visibile, ci sono solo pacchetti generici di cui non sappiamo il contenuto, quindi mostrano solo dati criptati.