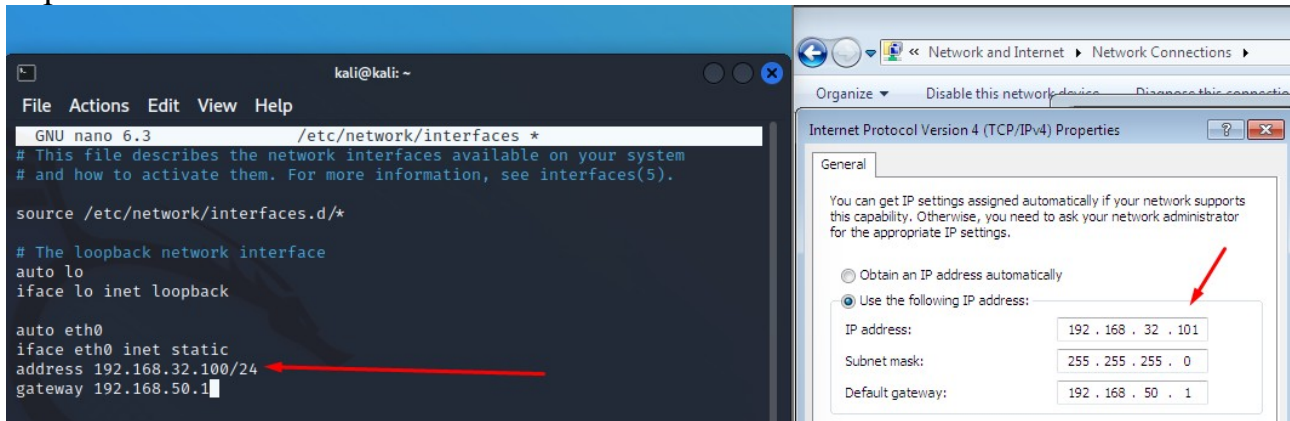
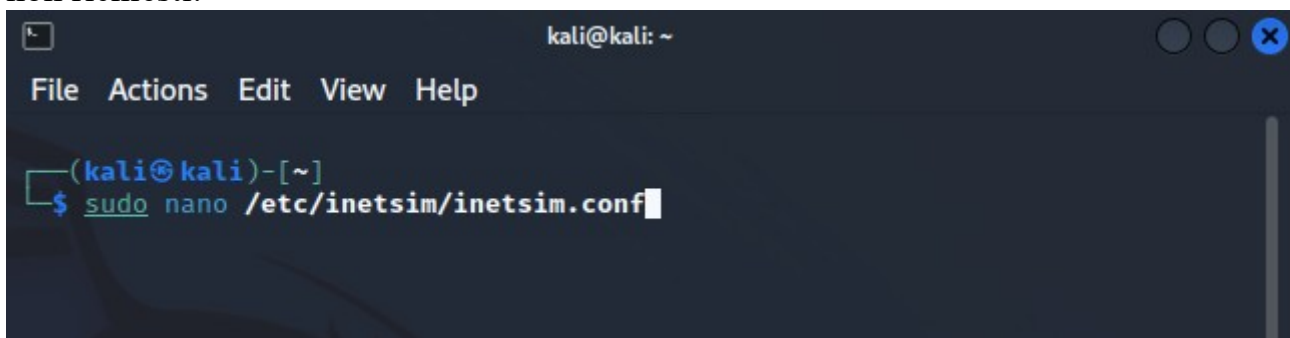


Esercizio Weekend

Come prima cosa andiamo ad impostare i nuovi indirizzi IP alle macchine virtuali, rispettivamente:



Ora andiamo a configurare il servizio INETSIM andando anche a disabilitare i servizi non richiesti:



```
kali@kali: ~  
File Actions Edit View Help  
GNU nano 6.3 /etc/inetsim/inetsim.conf *  
# 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
```

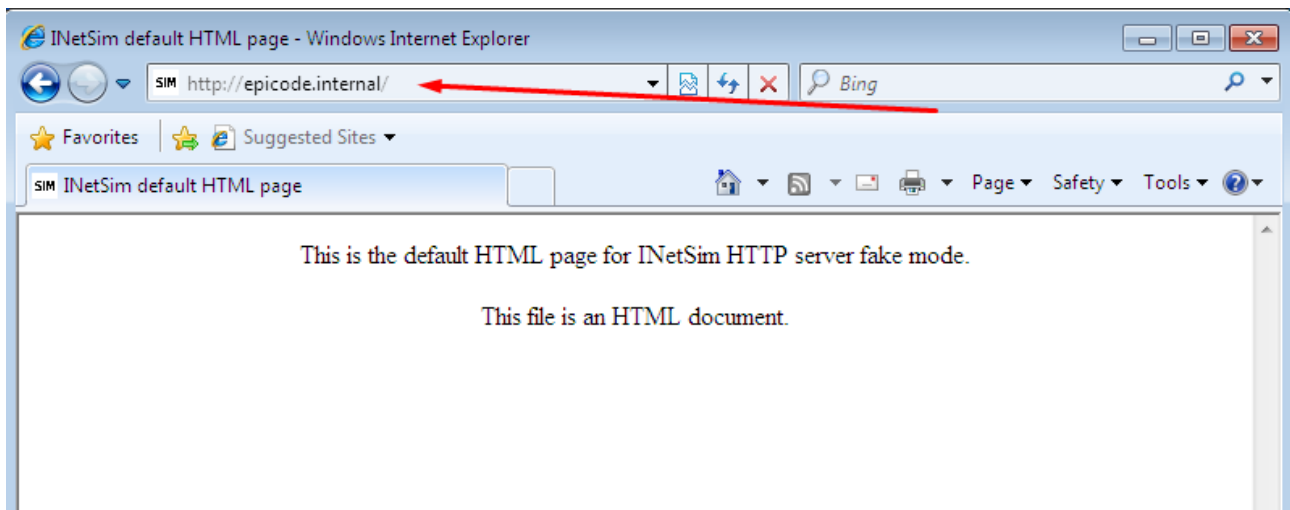
```
#####  
# service_bind_address  
#  
# IP address to bind services to  
#  
# Syntax: service_bind_address <IP address>  
#  
# Default: 127.0.0.1  
#  
#service_bind_address 10.10.10.1  
service_bind_address 192.168.32.100
```

Imposto come IP del DNS, quello della macchina Kali Linux

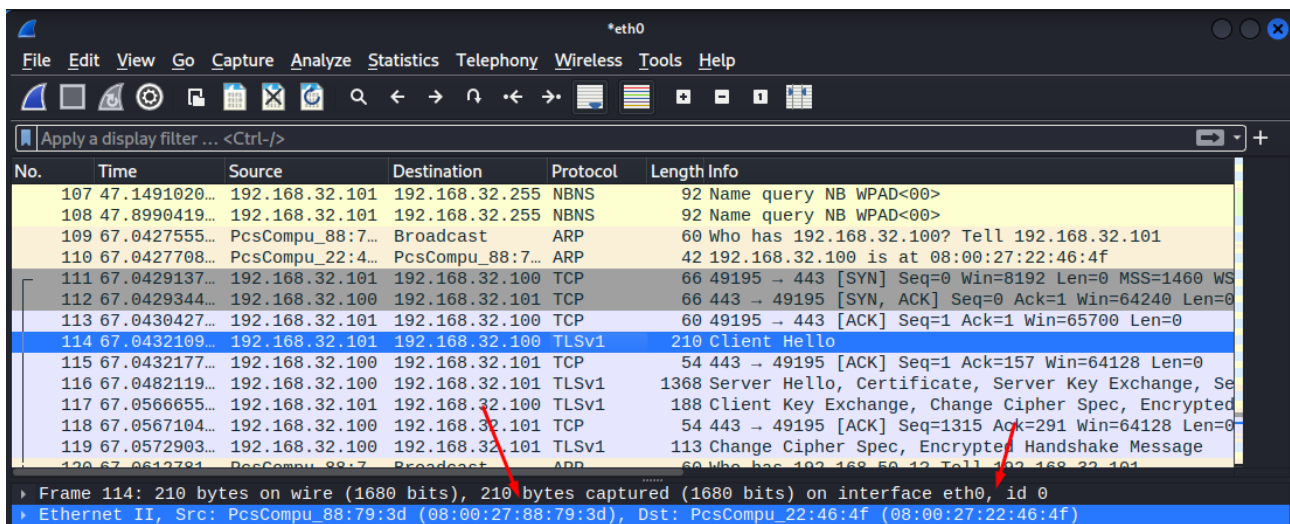
Adesso impostiamo come dns statico epicode.internal

```
#####  
# 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
```

Fatto ciò ora non rimane altro che verificare se viene effettuata la connessione al DNS server da Windows 7:

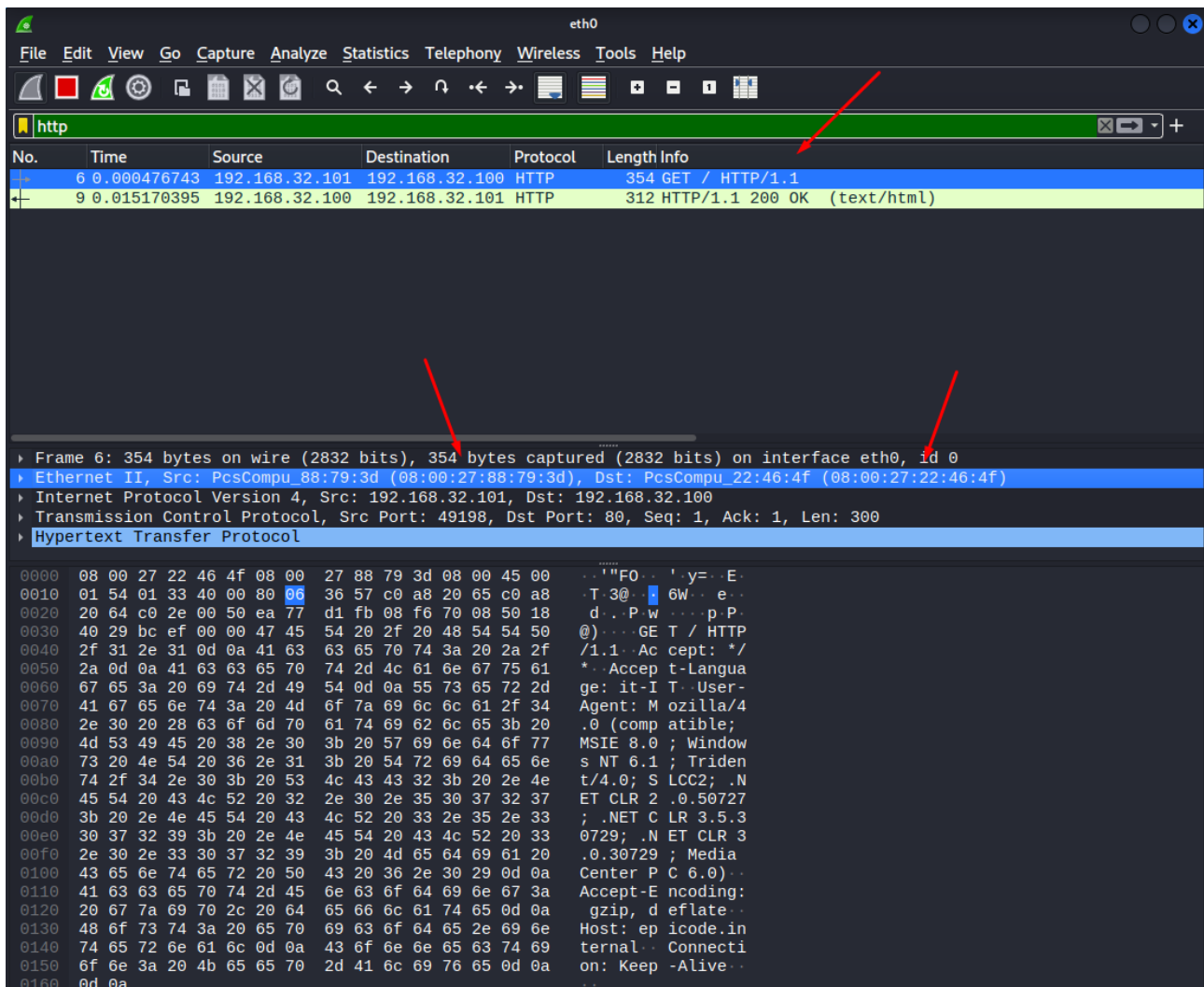


Ora aprendo Wireshark, andiamo a controllare i pacchetti inviati nel server HTTPS:



08:00:27:88:79:3d (Win7)

08:00:27:22:46:4f (Kali)



Le principali differenze che possiamo notare sono:

- Il protocollo usato nei pacchetti dei siti web, ossia HTTP e TLSv1;
- Il pacchetto TLSv1 non può essere analizzato poiché prima dell'invio dei pacchetti, viene creato un tunnel sicuro in cui si scambiano le chiavi, criptandone il messaggio, cosa che non succede nell'invio di pacchetti con protocollo HTTP.