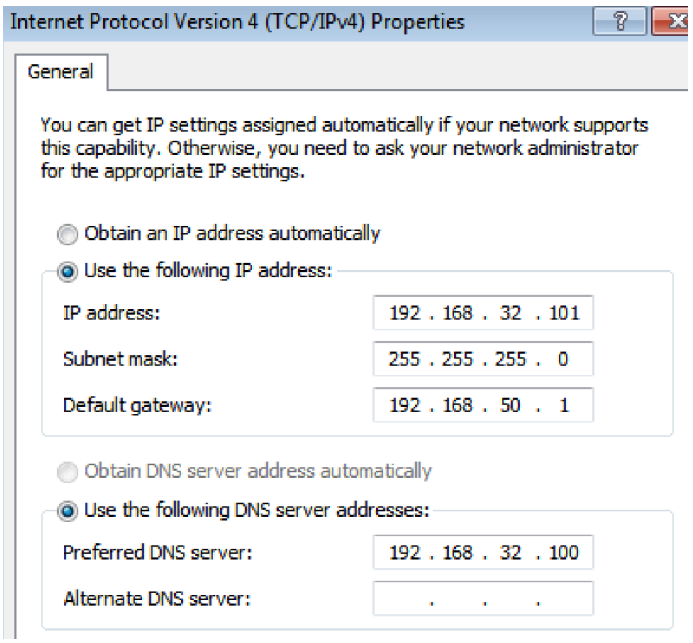
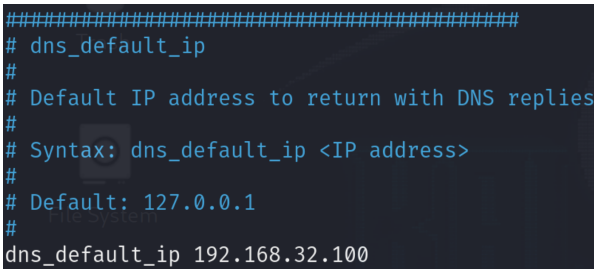
5. Simulazione di rete complessa
Per risolvere tale esercizio iniziamo dal setup degli indirizzi IP che ci vengono forniti.
In Windows 7 è necessario modificare le impostazioni del protocollo IPv4 accedendo dal pannello di controllo alle impostazioni della scheda di rete come si vede in figura.

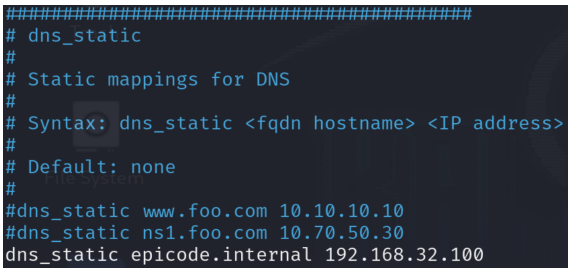


Così facendo Windows 7 avrà IP 192.168.32.101. Si noti inoltre che ho già impostato il server DNS con l'IP di Kali (passaggio che sarà approfondito più avanti). Aggiungiamo le eventuali regole al firewall di Windows così da permettere la comunicazione.
Ora andiamo a modificare l'indirizzo IP di Kali, modificando come segue il file nel percorso: *<u>/etc/network/interfaces.</u>*

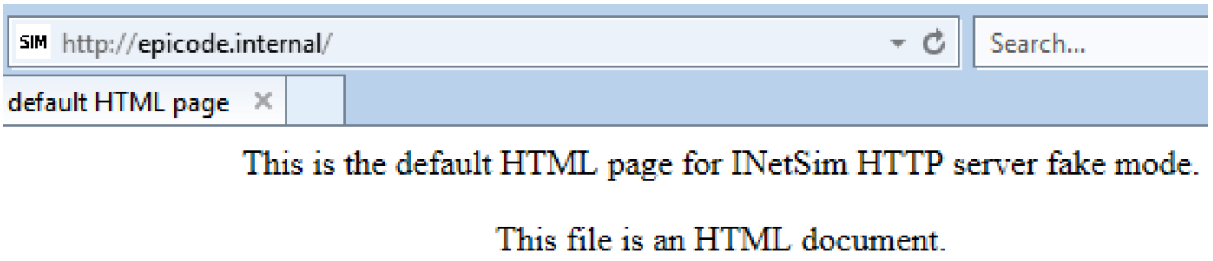
```
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.32.100/24
gateway 192.168.50.1
```

Fatto ciò si può eseguire un test di ping da una qualsiasi delle 2 macchine virtuali per verificare il corretto funzionamento del collegamento.
Il prossimo passo prevede il setup dell'applicazione Inetsim per emulare i servizi di rete.
Procediamo nel modificare il file al seguente percorso:
<u>/etc/inetsim/inetsim.conf</u>

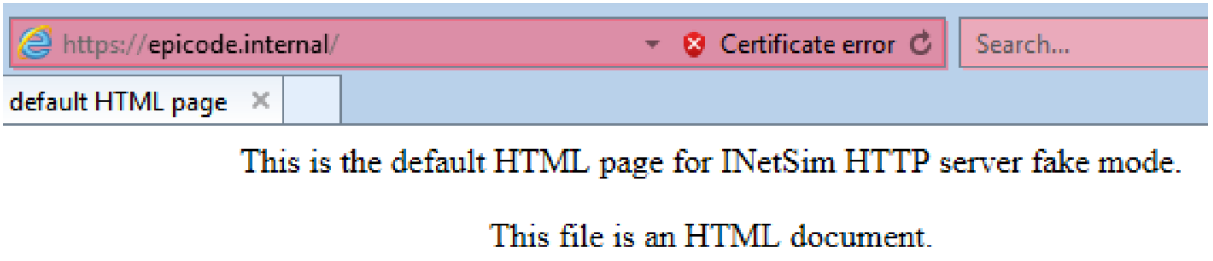




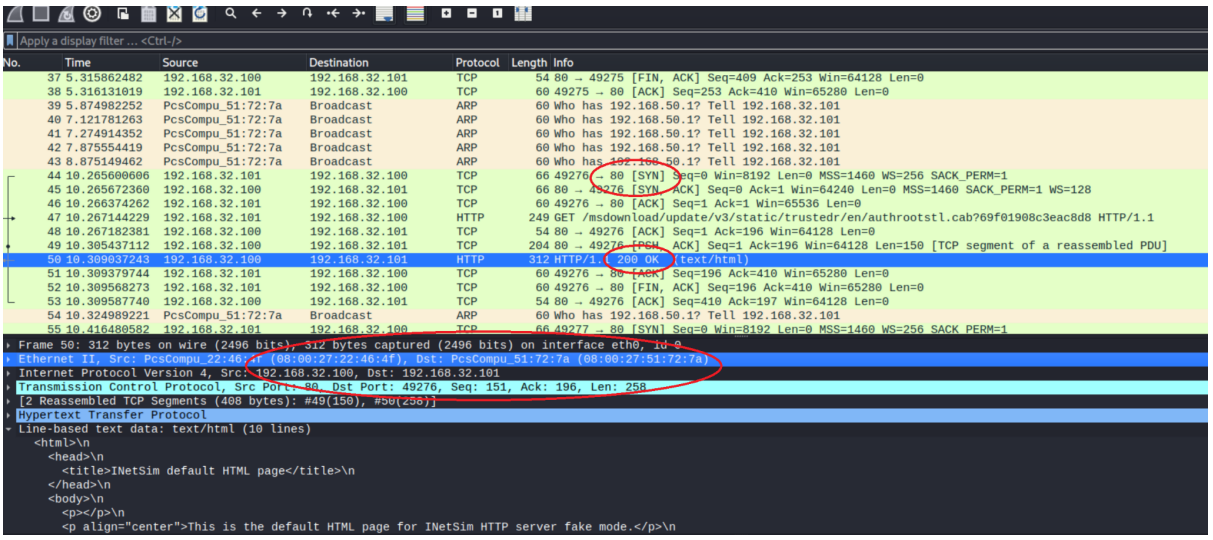
Nella prima immagine è stato assegnato l'IP al server DNS mentre nella seconda è stata aggiunta la regola tale per cui ad ogni richiesta del tipo "epicode.internal" il client verrà reindirizzato all'IP desiderato, in questo caso quello della nostra macchina.
Per verificare la corretta impostazione di Inetsim lanciamo tale applicazione dal terminale di Kali.
Passiamo ora al browser di Windows 7 (internet explorer purtroppo) dove andremo a digitare l'host_name ovvero "epicode.internal" così ottenendo:



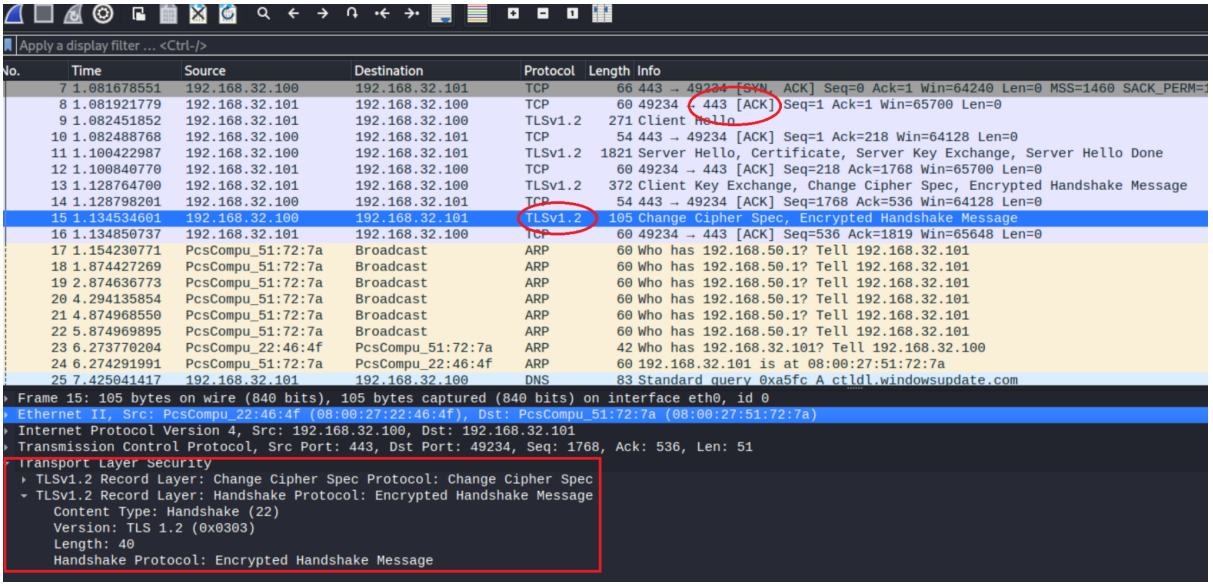
ripetiamo l'operazione inotrando una richiesta del tipo HTTPS ottendo:



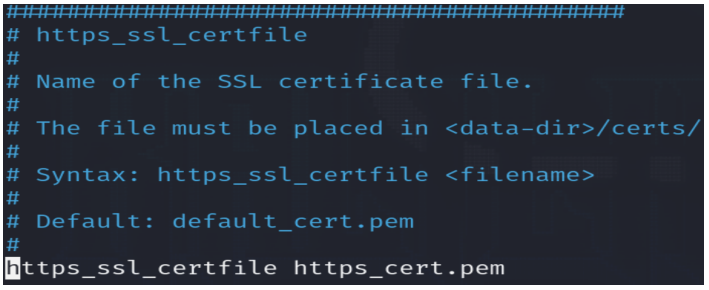
Notiamo subito che il browser cerca di proteggerci da un eventuale minaccia dato che il server fittizio di Inetsim è sprovvisto dei necessari certificati SSL necessari per la crittografia TLS.
Infine torniamo su Kali aprendo Wireshark, necessario per sniffare i pacchetti della conversazione sul canale *eth0.*
E ripetiamo sia la richiesta HTTP che quella HTTPS dal browser di windows 7 così da catturare i pacchetti.



In questa conversazione di tipo HTTP possiamo notare evidenziati gli indirizzi IP e MAC dei destinatari e riceventi, oltre alla porta 80 caratteristica di questo tipo di comunicazione, 200 ovvero il codice di avvenuta comunicazione e in fondo il codice HTML della pagina.



Per ultimo andiamo ad analizzare la conversazione HTTPS che come da immagine inizia comunicando dalla porta 443 utilizzando il metodo TLS v1.2 e notando la presenza del transport layer security. Tuttavia essendo il server sprovvisto di certificato SSL la connessione non sarà sicura nè criptata.
è possibile aggiungere il certificato a Inetsim modificando il file di configurazione in tal modo:



così da ottenere una conversazione criptata.