

W4D4

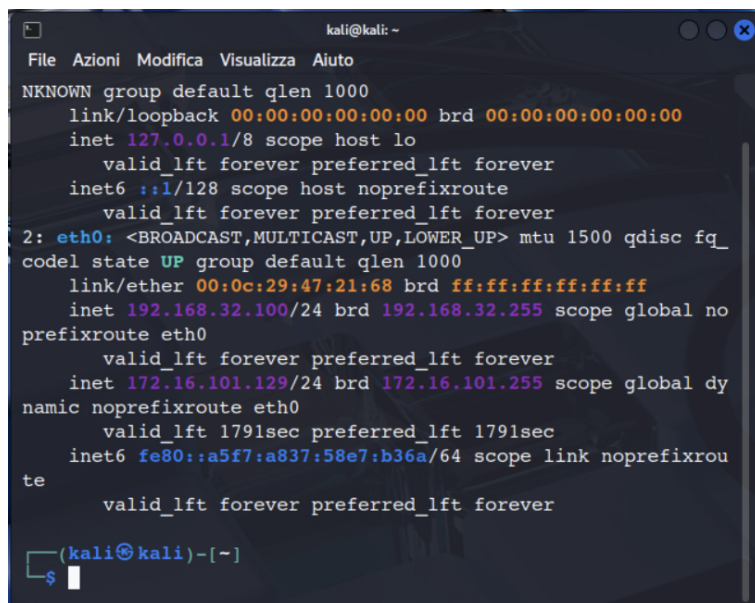
Progetto finale

Traccia: Simulare, in ambiente di laboratorio virtuale, un'architettura client server in cui un client con indirizzo 192.168.32.101 (Windows) richiede tramite web browser una risorsa all'hostname epicode.internal che risponde all'indirizzo 192.168.32.100 Kali.

Si intercetti poi la comunicazione con Wireshark, evidenziando i MAC address di sorgente e destinazione ed il contenuto della richiesta HTTPS.

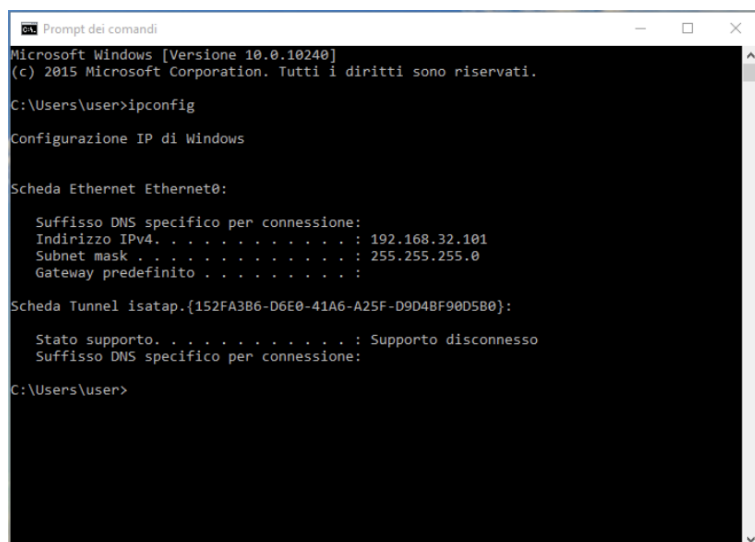
Ripetere l'esercizio, sostituendo il server HTTPS, con un server HTTP. Si intercetti nuovamente il traffico, evidenziando le eventuali differenze tra il traffico appena catturato in HTTP ed il traffico precedente in HTTPS. Spiegare, motivandole, le principali differenze se presenti.

Configurazione macchina virtuale Kali



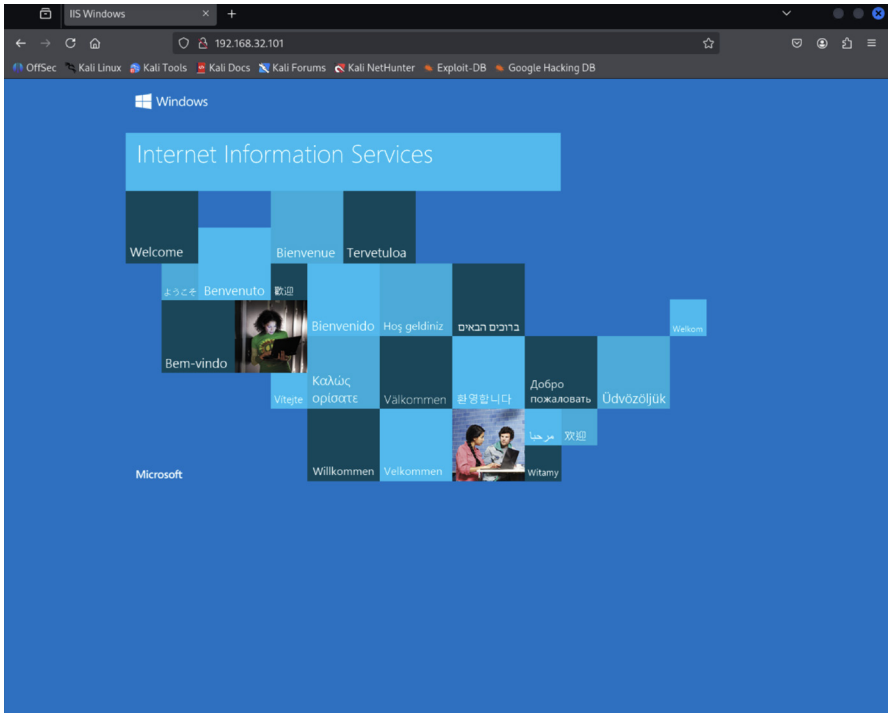
```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
UNKNOWN group default qlen 1000  
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
inet 127.0.0.1/8 scope host lo  
    valid_lft forever preferred_lft forever  
inet6 ::1/128 scope host noprefixroute  
    valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 00:0c:29:47:21:68 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.32.100/24 brd 192.168.32.255 scope global no  
prefixroute eth0  
    valid_lft forever preferred_lft forever  
    inet 172.16.101.129/24 brd 172.16.101.255 scope global dy  
namic noprefixroute eth0  
    valid_lft 1791sec preferred_lft 1791sec  
    inet6 fe80::a5f7:a837:58e7:b36a/64 scope link noprefixrou  
te  
    valid_lft forever preferred_lft forever  
  
(kali@kali)~  
$
```

Configurazione macchina virtuale Windows

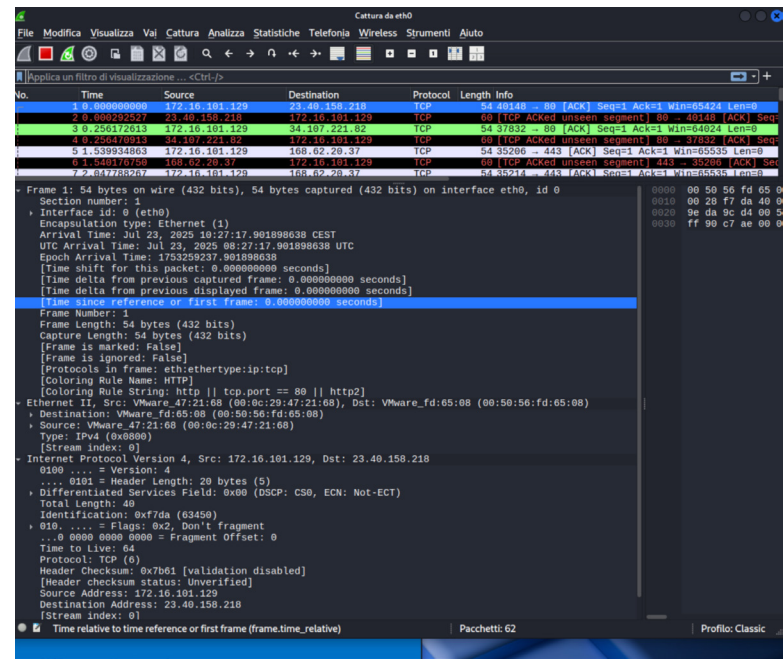


```
Prompt dei comandi  
Microsoft Windows [Versione 10.0.10240]  
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.  
  
C:\Users\User>ipconfig  
  
Configurazione IP di Windows  
  
Scheda Ethernet Ethernet0:  
  
    Suffisso DNS specifico per connessione:  
    Indirizzo IPv4. . . . . : 192.168.32.101  
    Subnet mask . . . . . : 255.255.255.0  
    Gateway predefinito . . . . . :  
  
Scheda Tunnel isatap.{152FA3B6-D6E0-41A6-A25F-D9D48F90D5B0}:  
  
    Stato supporto. . . . . : Supporto disconnesso  
    Suffisso DNS specifico per connessione:  
  
C:\Users\User>
```

Digitando l'indirizzo IP della macchina Windows `http://192.168.32.101` nel browser in Kali visualizzo la seguente schermata che conferma il collegamento



Tramite Wireshark posso intercettare i vari pacchetti della connessione HTTP essendo non criptati (query GET, url) su porta 80



digitando invece https://epicode.internal essendo una connessione criptata su porta 443 per cui l'analisi con wireshark è limitata a handshake IP e MAC

