Tarea 3

Nombre: Univ. Mamani Chavez Carla Vanesa	CI: 9124602 LP
Docente : Ms.c Gallardo Portanda Franz Ramiro	**Fecha :** 15/03/2020

1. Con los comandos nmap y nestat captura cualquier búsqueda que realices con Google donde se determinen los puertos de los servicios que se abren en la dirección remota y en la dirección de la red local.

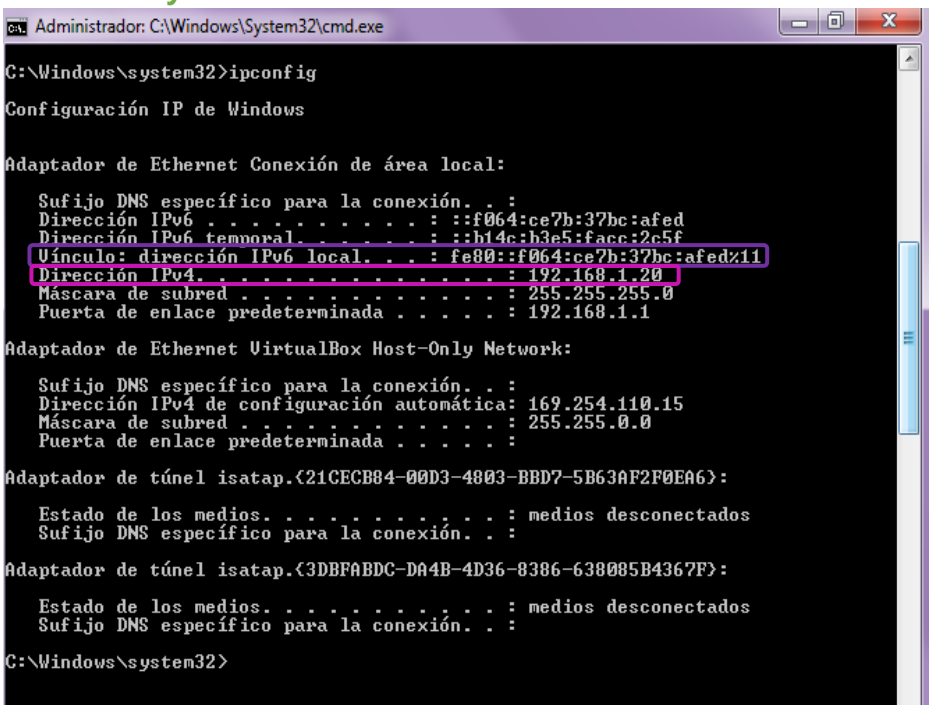

Figura 1.

Con el analizador de protocolos WIRESHARK se utilizó en S.O. Windows se capturo y analizo los paquetes de Facebook así mismo de la red Local.

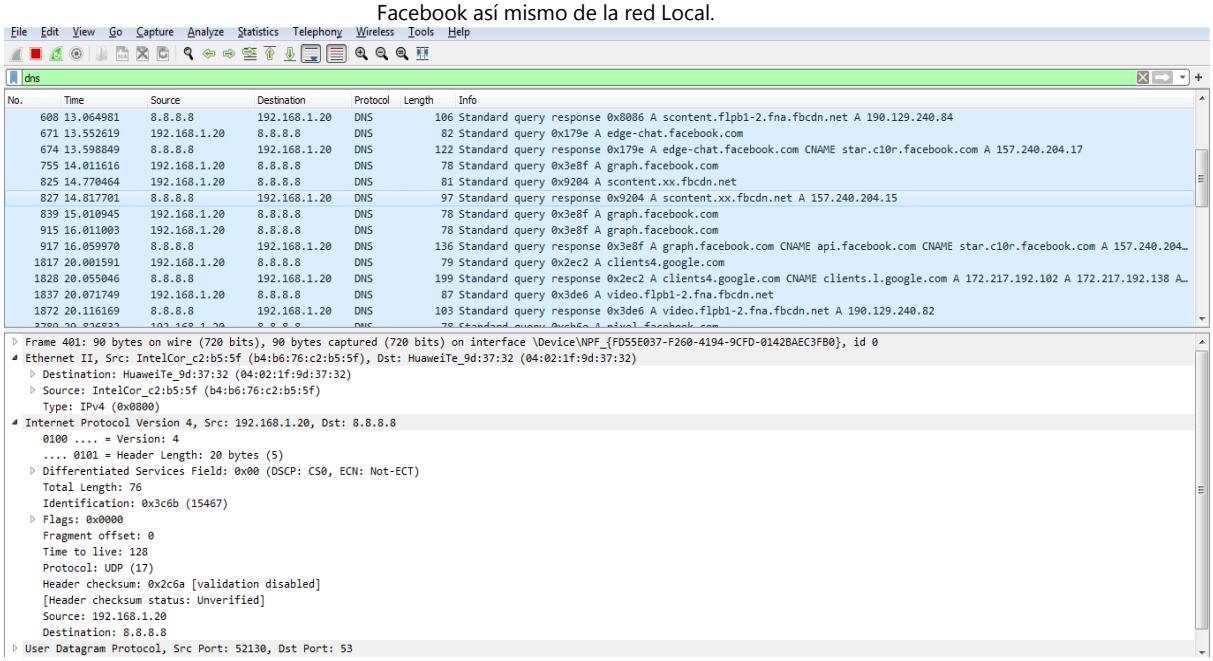

Figura 2

2. Mediante opciones del comando nmap, mostrar un reporte en la que viene asociada la información del fabricante del producto.

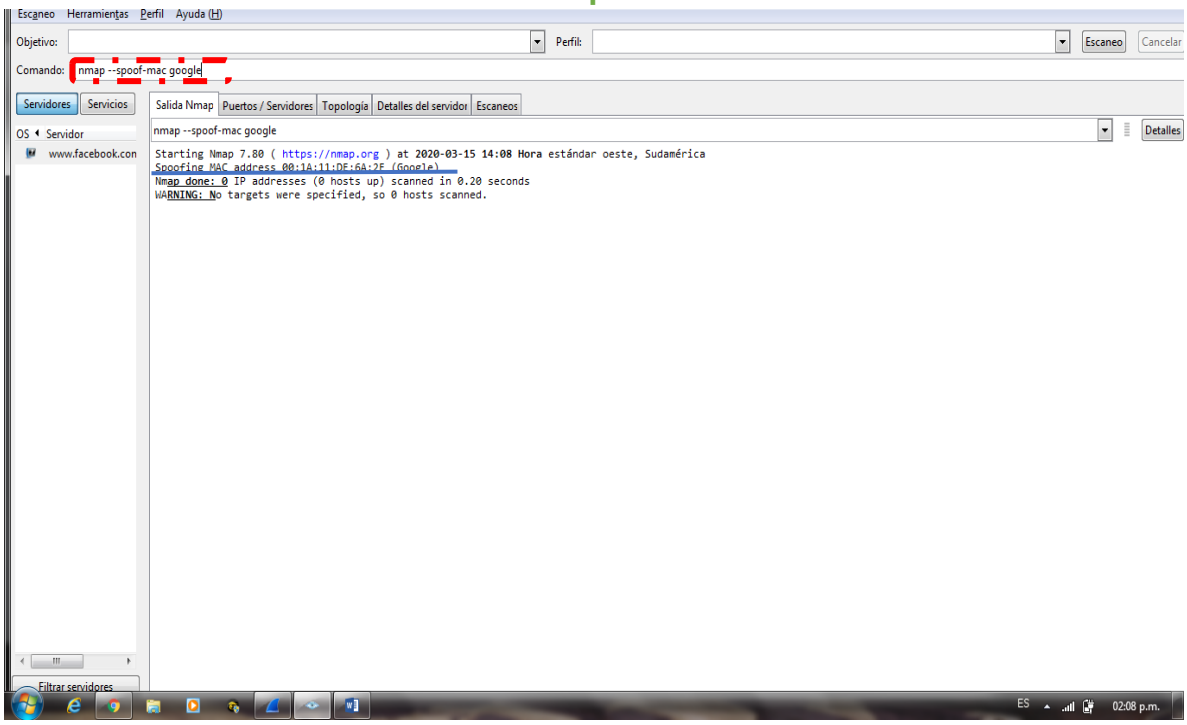

Figura 3

3. Si su host se encuentra conectado a internet, mostrar con reportes lo siguiente:

a) A través de cuál interface?

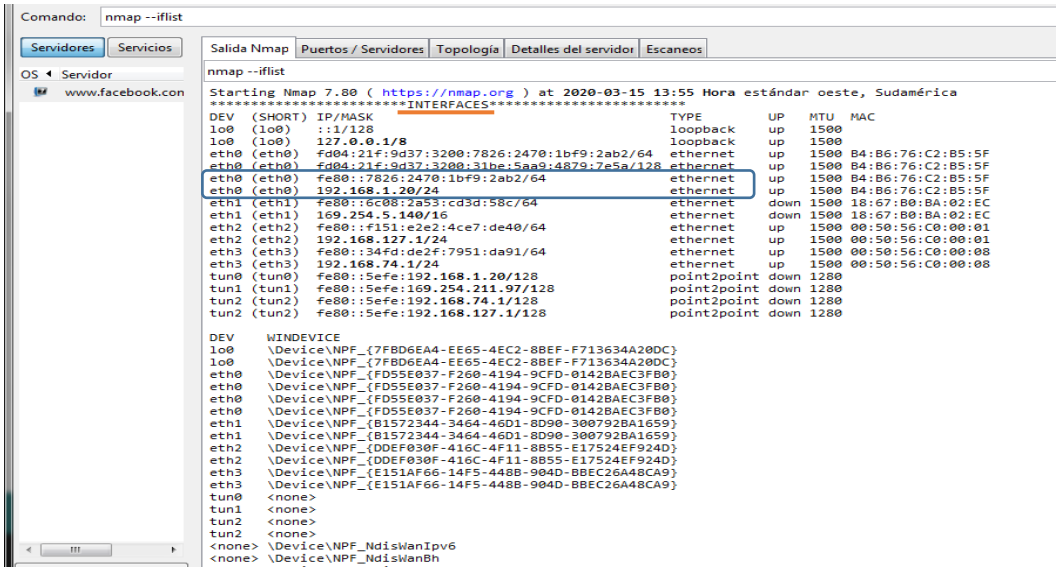

Figura 4

b) Cuál es el trayecto o ruta que recorre para llegar al servidor de Facebook.

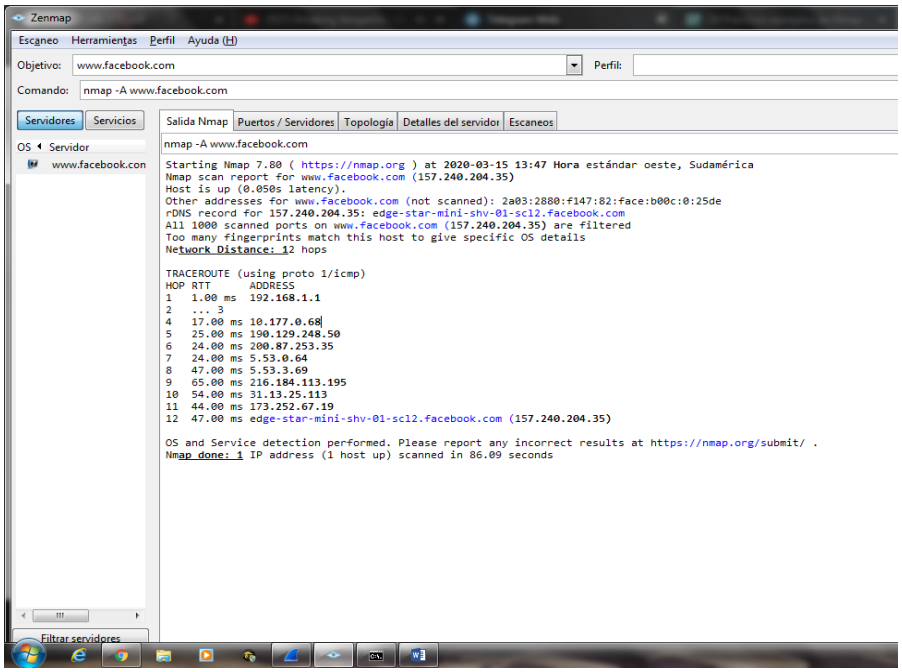

Figura 5

4. Interprete el siguiente reporte

En el reporte se analiza toda una subred, la cual puede escanearse toda una subred o rango de direcciones IP usando Nmap proporcionado con el comodín * el cual se muestra con el cuadro verde.

El resultado del reporte se puede ver que nmap escanea toda una subred y da toda la información sobre el hosts que están en la red.

En el cuadro se muestra los puertos como por ejemplo:

El puerto 80/ tcp en estado abierto y del tipo servicio http, el cual pertenece a la capa de aplicación del servicio web.

```
[root@server1 ~]# nmap 192.168.0.*

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-11 16:11 EST
Interesting ports on server1.mimaquina.com (192.168.0.100):
Not shown: 1677 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
111/tcp  open  rpcbind
851/tcp  open  unknown

Interesting ports on server2.mimaquina.com (192.168.0.101):
Not shown: 1674 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
957/tcp  open  unknown
3306/tcp open  mysql
8888/tcp open  sun-answerbook
MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

Nmap finished: 256 IP addresses (2 hosts up) scanned in 5.550 seconds
You have new mail in /var/spool/mail/root
```

Figura 6

5. Para cada uno de los incisos las expresiones que deberían utilizarse para capturar:

a) Tráfico que tenga como origen y/o destino la red 192.168.80.0/24

Se utilizó el filtro → **(IP.ADDR == 192.168.80.0)**

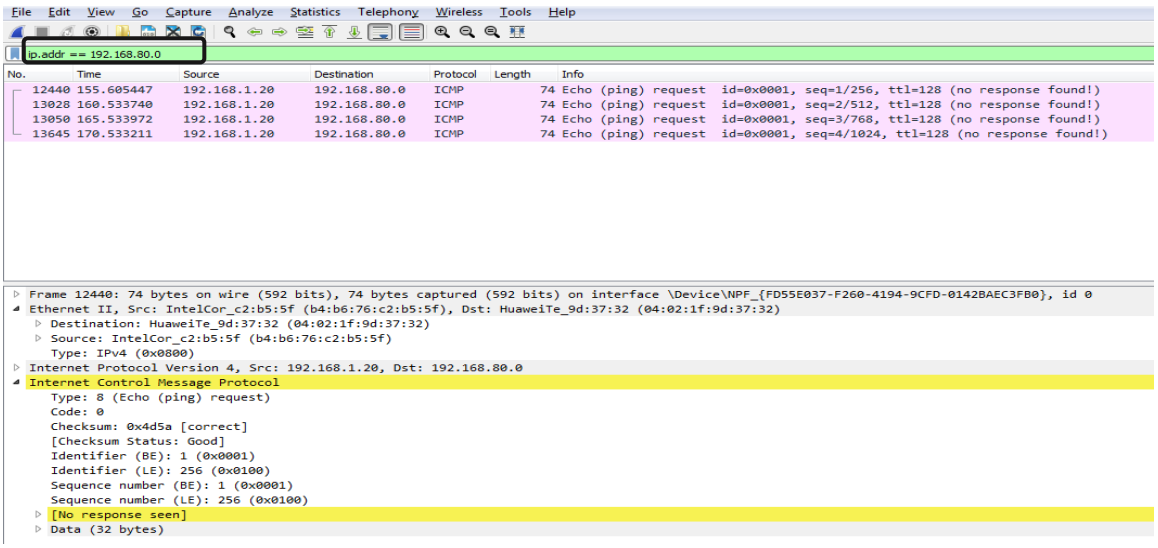

Figura 7

b) Que no sea ni HTTP ni DNS

Se utilizó el filtro → **(NOT DNS AND NOT HTTP)**

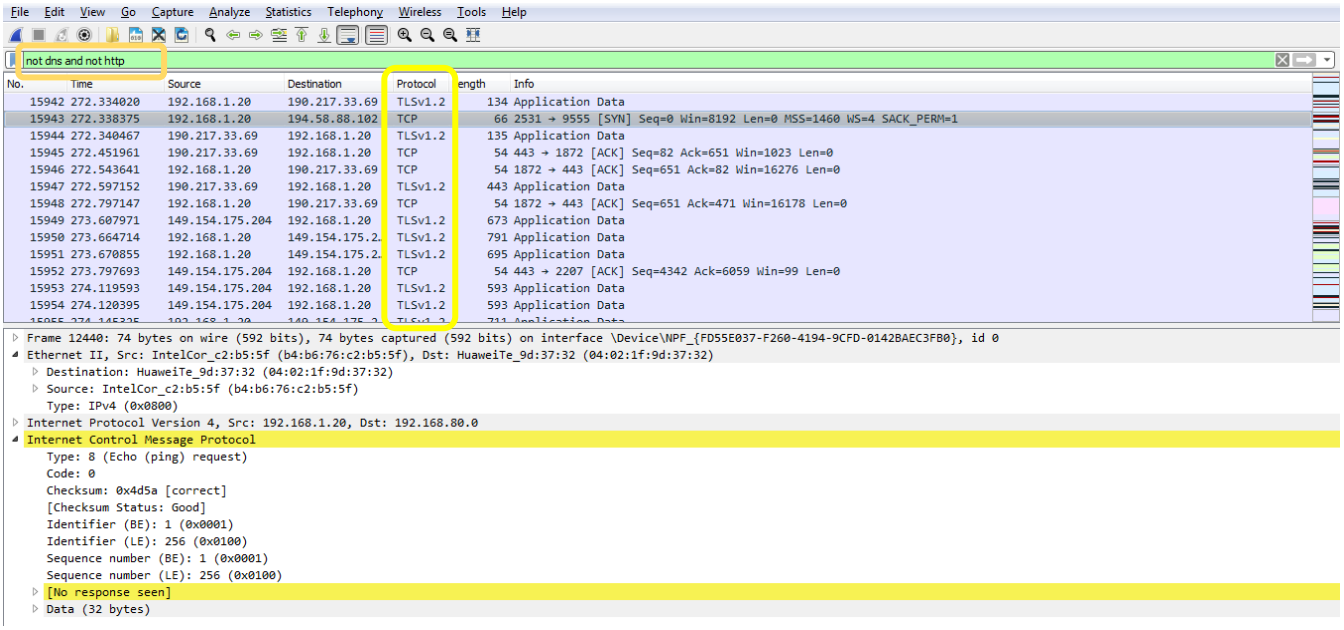

Figura 8

c) Que involucre a un rango de puertos como ser: 1000 a 1150

Se utilizó el filtro → **(NOT DNS AND NOT HTTP)**

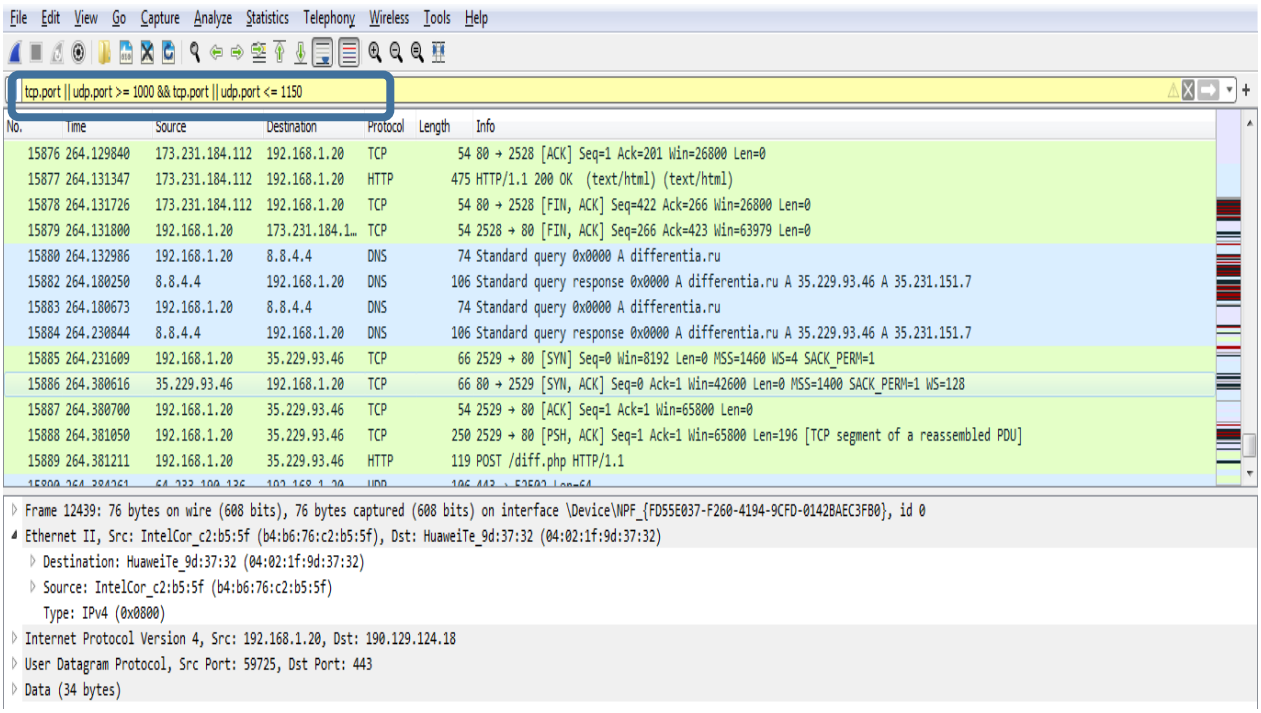

Figura 9

d) Solo tráfico únicas

Se utilizó el filtro → **(GNUTELLA OR BITTORRENT OR EDONKEY)**

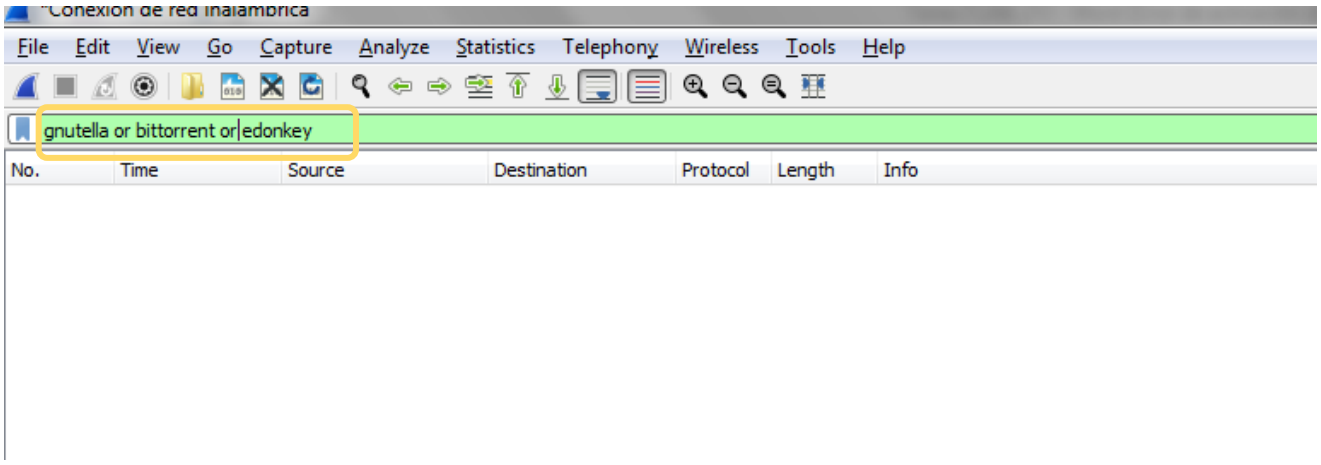

Figura 10