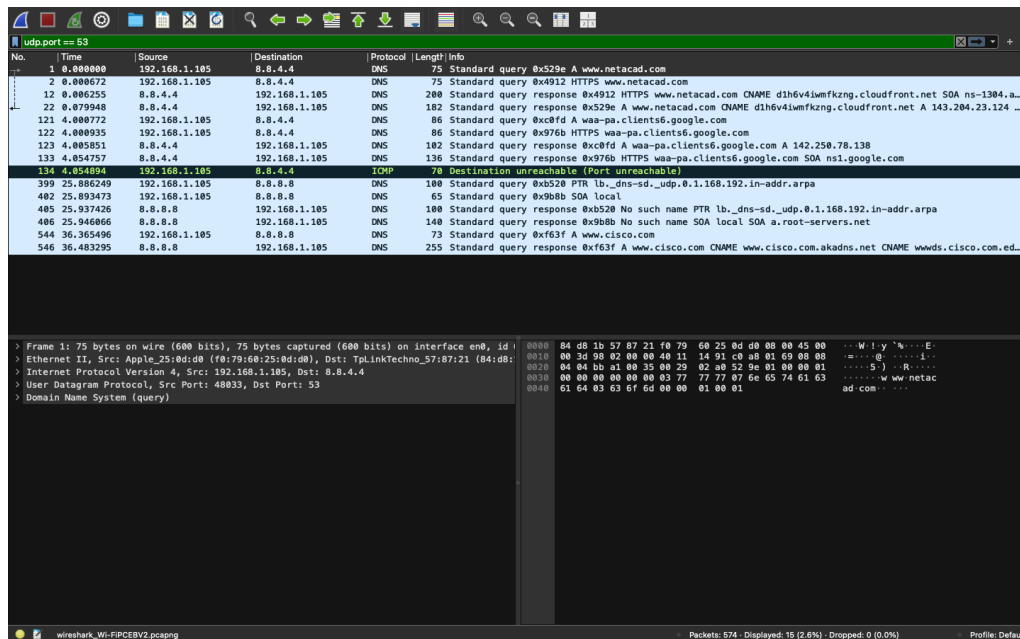


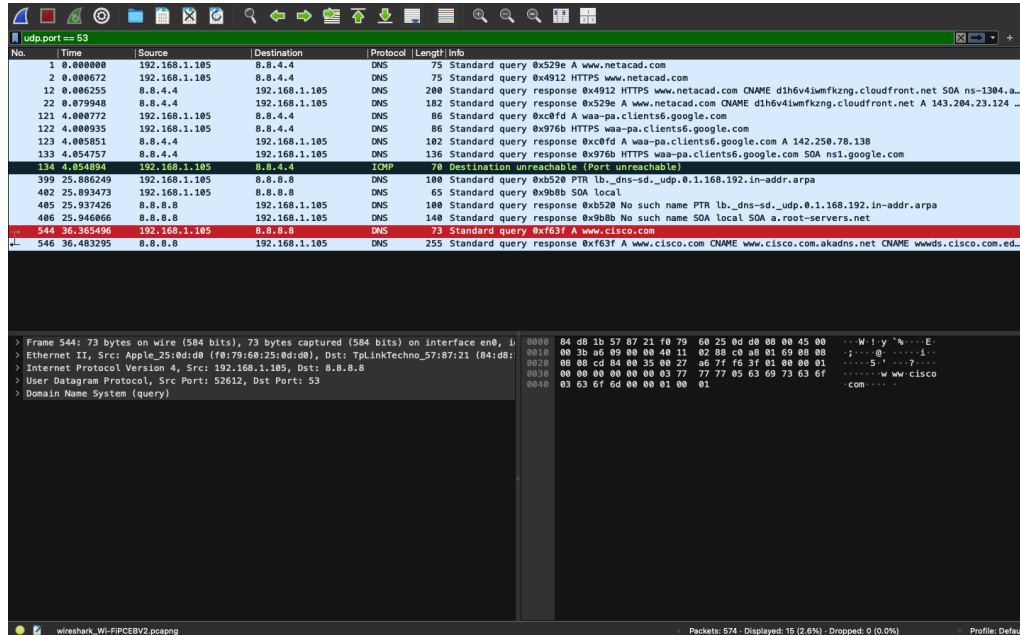
## Brandon Stick Buitrago Ruiz

### Parte 1: Capture el tráfico DNS



### Parte 2: Explorar tráfico de consultas DNS

B) Seleccione el paquete DNS que contiene la Standard query ( Consulta estándar) y a www.cisco.com en la columna Información.



D) Expanda Ethernet II para ver los detalles. Observe los campos de origen y de destino.

Wireshark packet capture showing Ethernet II details. The packet list shows a DNS query from 192.168.1.105 to 8.8.4.4. The packet details pane is expanded to show Ethernet II fields: Destination (08:00:27:00:00:00) and Source (08:00:27:00:00:00). The packet bytes pane shows the raw data in hexadecimal and ASCII.

¿Qué sucedió con las direcciones MAC de origen y de destino? ¿Con qué interfaces de red están asociadas estas direcciones MAC?

Respuestas :En este ejemplo, la dirección MAC de origen pertenece a la tarjeta de red de la computadora, mientras que la dirección MAC de destino corresponde al gateway predeterminado. Si hay un servidor DNS local, la dirección MAC de destino sería la del servidor DNS..

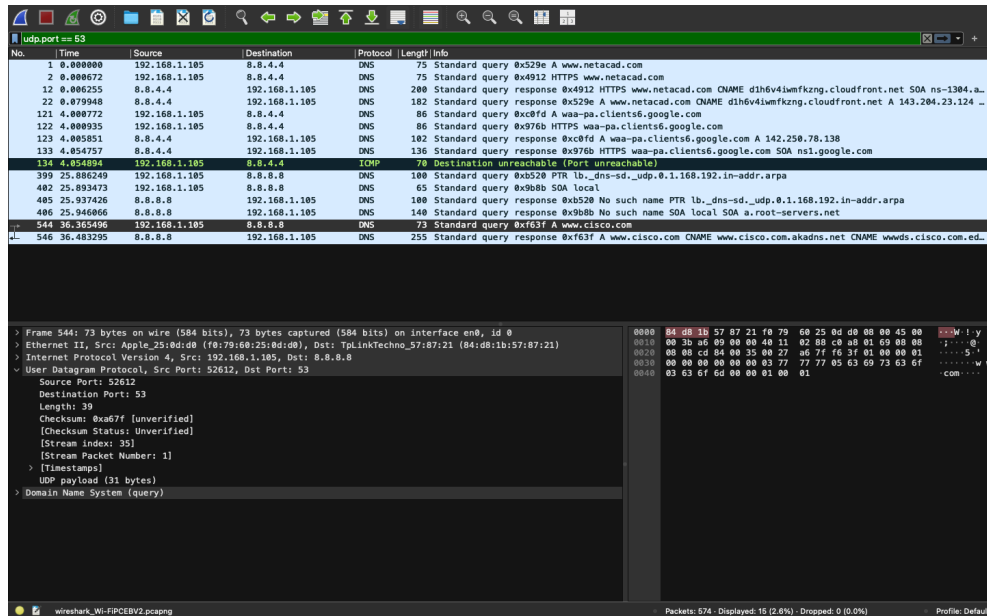
E) Expanda Internet Protocol Version 4. Observe las direcciones IPv4 de origen y de destino.

Wireshark packet capture showing Internet Protocol Version 4 details. The packet list shows a DNS query from 192.168.1.105 to 8.8.4.4. The packet details pane is expanded to show Internet Protocol Version 4 fields: Source (192.168.1.105) and Destination (8.8.4.4). The packet bytes pane shows the raw data in hexadecimal and ASCII.

¿Cuáles son las direcciones IP de origen y destino? ¿Con qué interfaces de red están asociadas estas direcciones IP?

Respuesta: En este caso, la dirección IP de origen está vinculada a la tarjeta de red de la computadora, mientras que la dirección IP de destino se refiere al gateway predeterminado.

F) Expanda el User Datagram Protocol. Observe los puertos de origen y de destino.



The screenshot shows a Wireshark packet capture of network traffic. The packet list at the top shows a series of DNS queries and responses. The selected packet is a DNS query from 192.168.1.105 to 8.8.4.4. The packet details pane on the right shows the User Datagram Protocol section expanded, displaying the source port as 577729 and the destination port as 53. The packet bytes pane at the bottom shows the raw data of the packet.

¿Cuáles son los puertos de origen y de destino? ¿Cuál es el número de puerto de DNS predeterminado?

Respuesta : El número de puerto de origen es 577729 y el puerto de destino es 53, el cual es el número de puerto DNS ya configurado

G) Determine las direcciones IP y MAC de la computadora personal.

```
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
    options=1203<RXCSUM, TXCSUM, TXSTATUS, SW_TIMESTAMP>
    inet 127.0.0.1 netmask 0xff000000
    inet6 ::1 prefixlen 128
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
    nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether f0:79:60:25:0d:d0
    inet6 fe80::879:f9f1:d9cc:bc57%en0 prefixlen 64 secured scopeid 0x4
    inet 192.168.1.105 netmask 0xfffff00 broadcast 192.168.1.255
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect
    status: active
en1: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
    options=400<TSO4,TSO6,CHANNEL_IO>
    ether 82:18:2f:c4:83:00
    media: autoselect <full-duplex>
    status: inactive
bridge0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=63<RXCSUM, TXCSUM, TSO4, TSO6>
    ether 82:18:2f:c4:83:00
    Configuration:
        id 0:0:0:0:0:0 priority 0 hellotime 0 fwddelay 0
        maxage 0 holdcnt 0 proto stp maxaddr 100 timeout 1200
        root id 0:0:0:0:0:0 priority 0 ifcost 0 port 0
        ipfilter disabled flags 0x0
        member: en1 flags=3<LEARNING,DISCOVER>
            ifmaxaddr 0 port 5 priority 0 path cost 0
        nd6 options=201<PERFORMNUD,DAD>
        media: <unknown type>
        status: inactive
p2p0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 2304
    options=400<CHANNEL_IO>
    ether 02:79:60:25:0d:d0
    media: autoselect
    status: inactive
awd10: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1484
    options=400<CHANNEL_IO>
    ether 5a:5f:bb:3c:a6:c4
    inet6 fe80::585f:bbff:fe3c:a6c4%awd10 prefixlen 64 scopeid 0x8
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect
    status: active
llw0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether 5a:5f:bb:3c:a6:c4
    inet6 fe80::585f:bbff:fe3c:a6c4%llw0 prefixlen 64 scopeid 0x9
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect
    status: active
utun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
    inet6 fe80::f78:9faa:707c:4f52%utun0 prefixlen 64 scopeid 0xa
    nd6 options=201<PERFORMNUD,DAD>
utun1: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 2000
    inet6 fe80::ed65:4b13:f24f:327e%utun1 prefixlen 64 scopeid 0xb
    nd6 options=201<PERFORMNUD,DAD>
utun2: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1000
    inet6 fe80::ce81:b1c:bd2c:69e%utun2 prefixlen 64 scopeid 0xc
    nd6 options=201<PERFORMNUD,DAD>
manuellozano@MacBook-Air-de-Manuel ~ %
```

Compare las direcciones MAC y las direcciones IP presentes en los resultados de Wireshark con los resultados obtenidos del símbolo del sistema o terminal. ¿Cuál es su opinión?

Respuesta: Las direcciones IP y MAC capturadas en los resultados de Wireshark son las mismas que figuran en el comando ifconfig.

```
Source: Apple_25:0d:d0 (f0:79:60:25:0d:d0)
```

```
Source Address: 192.168.1.105
```

```
ether f0:79:60:25:0d:d0
inet6 fe80::879:f9f1:d9cc:bc57%en0 prefixlen 64 secured scopeid 0x4
inet 192.168.1.105 netmask 0xfffff00 broadcast 192.168.1.255
```

H) Expanda Domain Name System (query) en el panel de Detalles del paquete. Luego, expanda Flags y Queries.

Wireshark packet capture showing a DNS query. The packet list shows a query from 192.168.1.105 to 8.8.8.8. The packet details show the query for www.cisco.com. The packet bytes show the raw data.

### Parte 3: Explorar tráfico de respuestas DNS

A) Seleccione el paquete que contiene la Standard query response (respuesta de consulta estándar) y A www.cisco.com en la columna "Info" (Información)

Wireshark packet capture showing a DNS response. The packet list shows a response from 8.8.8.8 to 192.168.1.105. The packet details show the response for www.cisco.com. The packet bytes show the raw data.

¿Cuáles son las direcciones MAC e IP y los números de puerto de origen y de destino? ¿Qué similitudes y diferencias tienen con las direcciones presentes en los paquetes de consultas DNS?

MAC origen: TpLinkTechno\_57:87:21

MAC destino: Apple\_25:d0:0d

IP origen: 8.8.8.8 (servidor DNS)

IP destino: 192.168.1.105 (cliente)

Puerto origen: 53 (DNS)

Puerto destino: 52612 (cliente)

Similitudes:

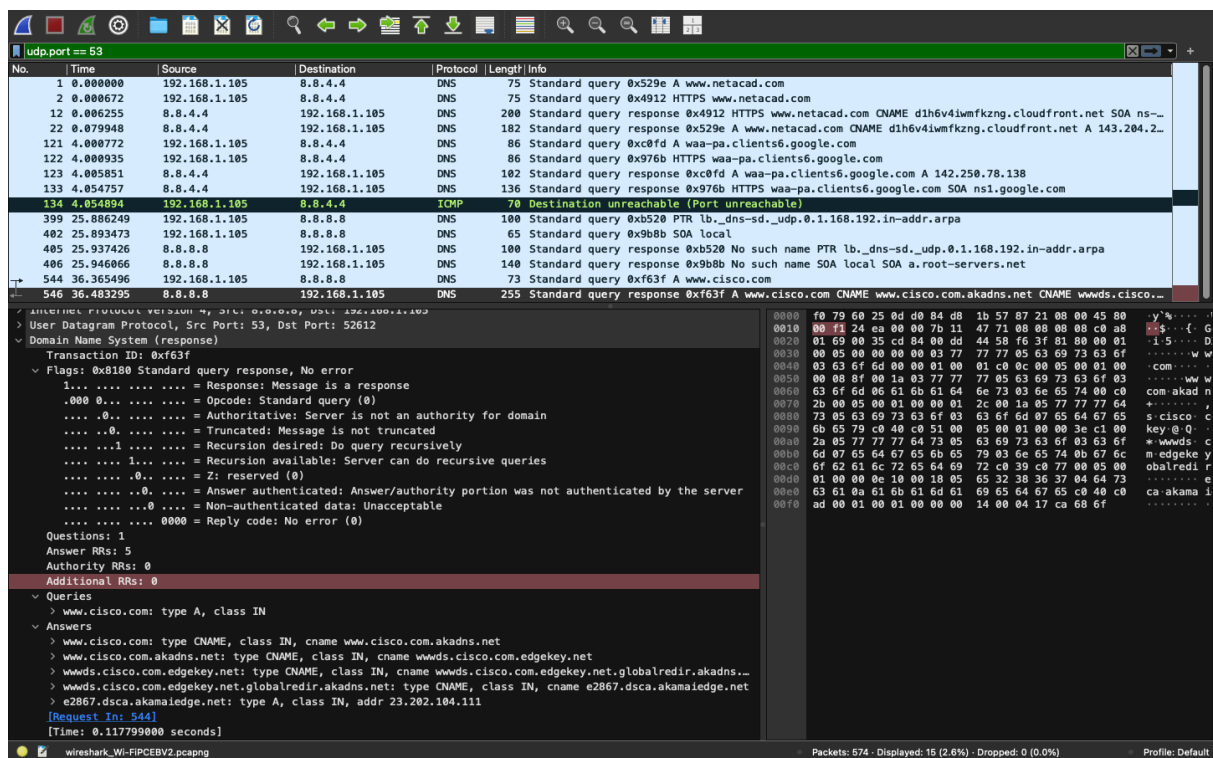
Misma IP y MAC para cliente y servidor.

El puerto de origen sigue siendo 53 (DNS).

Diferencias:

Las IP y puertos de origen/destino se invierten entre la consulta y la respuesta.

B) Expanda Domain Name System (response). Después expanda Flags, Queries y Answers .



```
1 0.000000 192.168.1.105 8.8.8.4.4 DNS 75 Standard query 0x529e A www.netacad.com
2 0.000672 192.168.1.105 8.8.4.4 DNS 75 Standard query 0x4912 HTTPS www.netacad.com
12 0.006255 8.8.4.4 192.168.1.105 DNS 200 Standard query response 0x4912 HTTPS www.netacad.com CNAME dh6v4lwmfkzng.cloudfront.net SOA ns-...
22 0.079948 8.8.4.4 192.168.1.105 DNS 182 Standard query response 0x529e A www.netacad.com CNAME dh6v4lwmfkzng.cloudfront.net A 143.204.2...
121 4.000772 192.168.1.105 8.8.4.4 DNS 86 Standard query 0xc0fd A waa-pa.clients6.google.com
122 4.000935 192.168.1.105 8.8.4.4 DNS 86 Standard query 0x976b HTTPS waa-pa.clients6.google.com
123 4.005851 8.8.4.4 192.168.1.105 DNS 182 Standard query response 0xc0fd A waa-pa.clients6.google.com A 142.250.78.138
133 4.054757 8.8.4.4 192.168.1.105 DNS 136 Standard query response 0x976b HTTPS waa-pa.clients6.google.com SOA ns1.google.com
134 4.054894 192.168.1.105 8.8.4.4 ICMP 70 Destination unreachable (Port unreachable)
399 25.886249 192.168.1.105 8.8.8.8 DNS 100 Standard query 0xb520 PTR lb_dns-sd_udp.0.1.168.192.in-addr.arpa
402 25.893473 192.168.1.105 8.8.8.8 DNS 65 Standard query 0x9b8b SOA local
405 25.937426 8.8.8.8 192.168.1.105 DNS 100 Standard query response 0xb520 No such name PTR lb_dns-sd_udp.0.1.168.192.in-addr.arpa
406 25.946066 8.8.8.8 192.168.1.105 DNS 140 Standard query response 0x9b8b No such name SOA local SOA a.root-servers.net
544 36.365496 192.168.1.105 8.8.8.8 DNS 73 Standard query 0xf63f A www.cisco.com
546 36.483295 8.8.8.8 192.168.1.105 DNS 255 Standard query response 0xf63f A www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwds.cisco...

User Datagram Protocol, Src Port: 53, Dst Port: 52612
Domain Name System (response)
Transaction ID: 0xf63f
Flags: 0x0100 Standard query response, No error
1... .. = Response: Message is a response
.000 0... .. = Opcode: Standard query (0)
... .. = Authoritative: Server is not an authority for domain
... .. = Truncated: Message is not truncated
... .. = Recursion desired: Do query recursively
... .. = Recursion available: Server can do recursive queries
... .. = Z: reserved (0)
... .. = Answer authenticated: Answer/authority portion was not authenticated by the server
... .. = Non-authenticated data: Unacceptable
... .. = Reply code: No error (0)
Questions: 1
Answer RRs: 5
Authority RRs: 0
Additional RRs: 0
Queries
> www.cisco.com: type A, class IN
Answers
> www.cisco.com: type CNAME, class IN, cname www.cisco.com.akadns.net
> www.cisco.com.akadns.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey.net
> wwwds.cisco.com.edgekey.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey.net.globalredir.akadns...
> wwwds.cisco.com.edgekey.net.globalredir.akadns.net: type CNAME, class IN, cname e2867.dsca.akamaiedge.net
> e2867.dsca.akamaiedge.net: type A, class IN, addr 23.202.104.111
[Request In: 544]
[Time: 0.117799000 seconds]
```

¿El servidor DNS puede realizar consultas recursivas?

Respuesta: Sí, el DNS puede gestionar consultas variadas

D) Observe los registros "CNAME" y "A" en los detalles de "Answers" (respuestas).

```
Answers
> www.cisco.com: type CNAME, class IN, cname www.cisco.com.akadns.net
> www.cisco.com.akadns.net: type CNAME, class IN, cname wwds.cisco.com.edgekey.net
> wwds.cisco.com.edgekey.net: type CNAME, class IN, cname wwds.cisco.com.edgekey.net.globalredir.akadns...
> wwds.cisco.com.edgekey.net.globalredir.akadns.net: type CNAME, class IN, cname e2867.dsca.akamaiedge.net
> e2867.dsca.akamaiedge.net: type A, class IN, addr 23.202.104.111
[Request In: 544]
```

¿Qué similitudes y diferencias tienen con los resultados de nslookup?

Respuesta : Los resultados en Wireshark son parecidos a los obtenidos con el comando nslookup, se puede ver en los CNAME (Canonical Name) que no tienen gran diferencia

## Reflexión

1. A partir de los resultados de Wireshark. ¿qué más pueden averiguar sobre la red cuando quitan el filtro?

Respuesta: Sin aplicar filtros, los resultados incluyen otros paquetes, como DHCP y ARP. A partir de estos paquetes y la información que contienen, puedes identificar otros dispositivos y sus roles dentro de la red local.

2. ¿De qué manera un atacante puede utilizar Wireshark para poner en riesgo la seguridad de sus redes?

Respuesta: Un atacante en la red local puede utilizar Wireshark para monitorear el tráfico y, si los datos no están encriptados, podría acceder a información sensible contenida en los detalles de los paquetes.