Lab – Explore 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 on a Windows system and use Wireshark to filter for DNS packets and view the details of both DNS query and response packets.

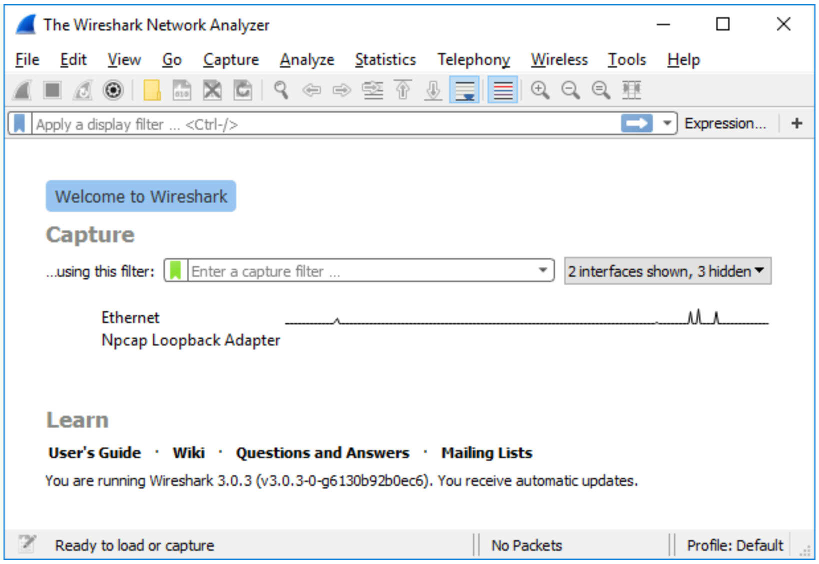
Required Resources

- 1 Windows PC with internet access and Wireshark installed

Instructions

Step 1: Capture DNS traffic.

a. Open **Wireshark** and start a Wireshark capture by double clicking a network interface with traffic.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
2 interfaces shown, 3 hidden
Ethernet
Npcap Loopback Adapter
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.0.3 (v3.0.3-0-g6130b92b0ec6). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default

b. At the Command Prompt, enter **ipconfig /flushdns** clear the DNS cache.

```
C:\Users\Student> ipconfig /flushdns
```

```
Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

c. Enter **nslookup** at the prompt to enter the nslookup interactive mode.

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

```
C:\Users\Student> nslookup
Default Server:  UnKnown
Address:  68.105.28.16

> www.cisco.com
Server:  UnKnown
Address:  68.105.28.16

Non-authoritative answer:
Name:    e2867.dsca.akamaiedge.net
Addresses:  2001:578:28:68d::b33
          2001:578:28:685::b33
          96.7.79.147
Aliases:  www.cisco.com
          www.cisco.com.akadns.net
          wwwds.cisco.com.edgekey.net
          wwwds.cisco.com.edgekey.net.globalredir.akadns.net
```

e. Enter **exit** when finished to exit the nslookup interactive mode. Close the command prompt.

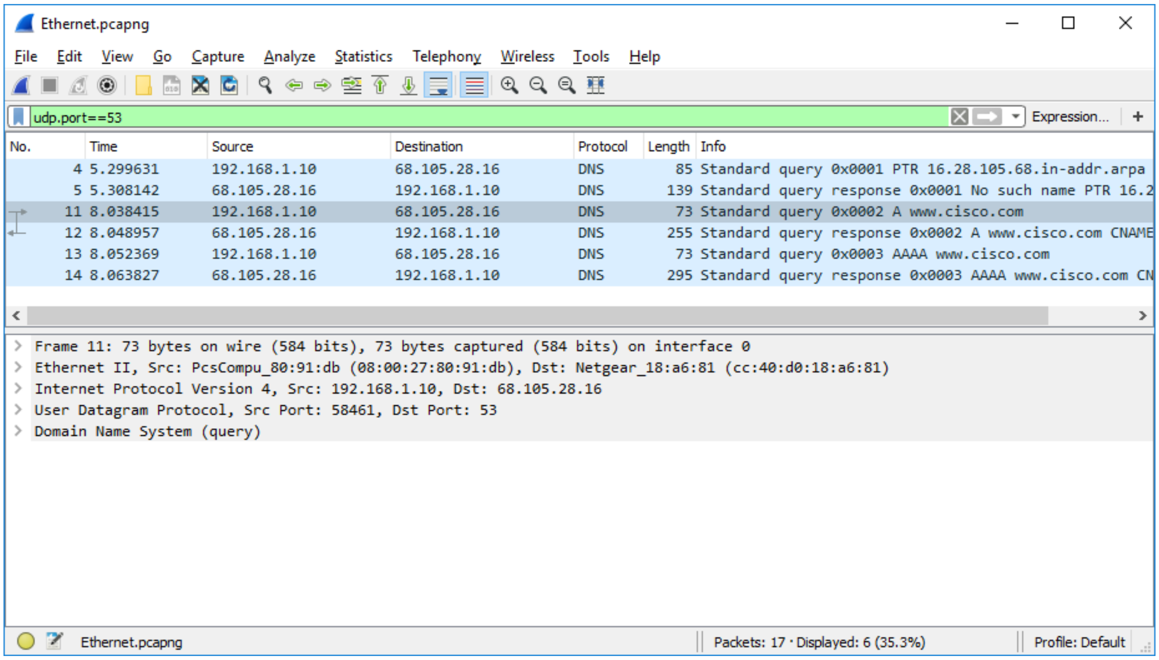
f. Click **Stop capturing packets** to stop the Wireshark capture.

Step 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.

b. Select the DNS packet labeled **Standard query 0x0002 A www.cisco.com**.

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


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

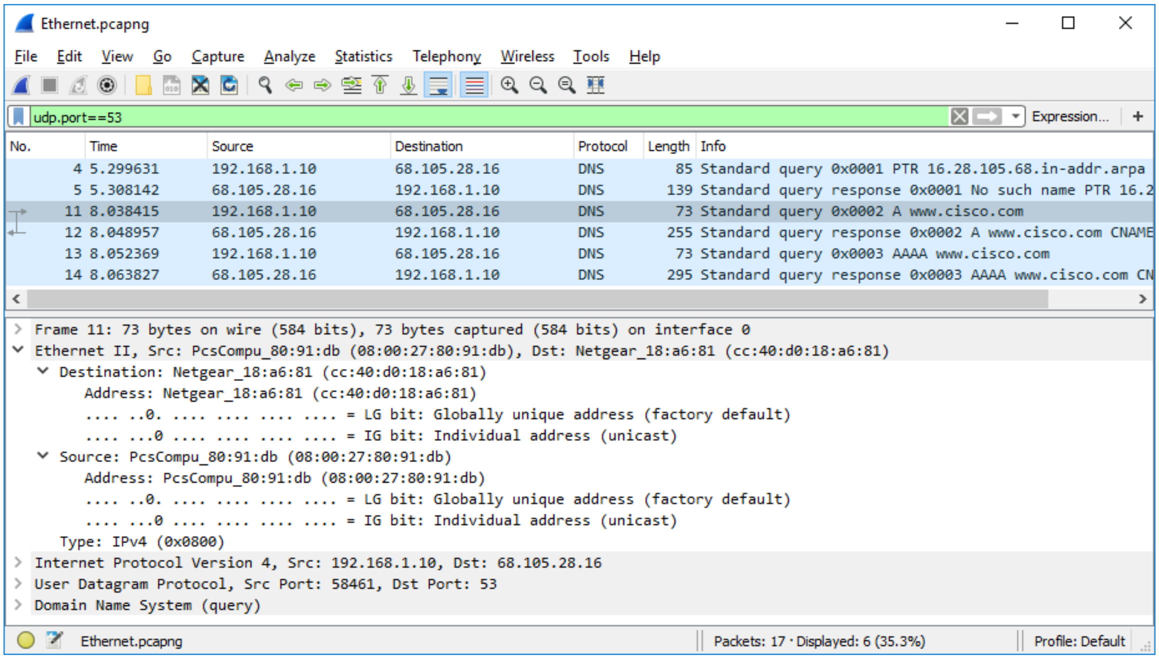
udp.port==53

```
No.   Time       Source         Destination    Protocol  Length  Info
    4 5.299631   192.168.1.10   68.105.28.16   DNS           85  Standard query 0x0001 PTR 16.28.105.68.in-addr.arpa
    5 5.308142   68.105.28.16   192.168.1.10   DNS          139  Standard query response 0x0001 No such name PTR 16.2
   11 8.038415   192.168.1.10   68.105.28.16   DNS           73  Standard query 0x0002 A www.cisco.com
   12 8.048957   68.105.28.16   192.168.1.10   DNS          255  Standard query response 0x0002 A www.cisco.com CNAME
   13 8.052369   192.168.1.10   68.105.28.16   DNS           73  Standard query 0x0003 AAAA www.cisco.com
   14 8.063827   68.105.28.16   192.168.1.10   DNS          295  Standard query response 0x0003 AAAA www.cisco.com CN
```

```
> Frame 11: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
> Ethernet II, Src: PcsCompu_80:91:db (08:00:27:80:91:db), Dst: Netgear_18:a6:81 (cc:40:d0:18:a6:81)
> Internet Protocol Version 4, Src: 192.168.1.10, Dst: 68.105.28.16
> User Datagram Protocol, Src Port: 58461, Dst Port: 53
> Domain Name System (query)
```

Ethernet.pcapng | Packets: 17 · Displayed: 6 (35.3%) | Profile: Default

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


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

udp.port==53

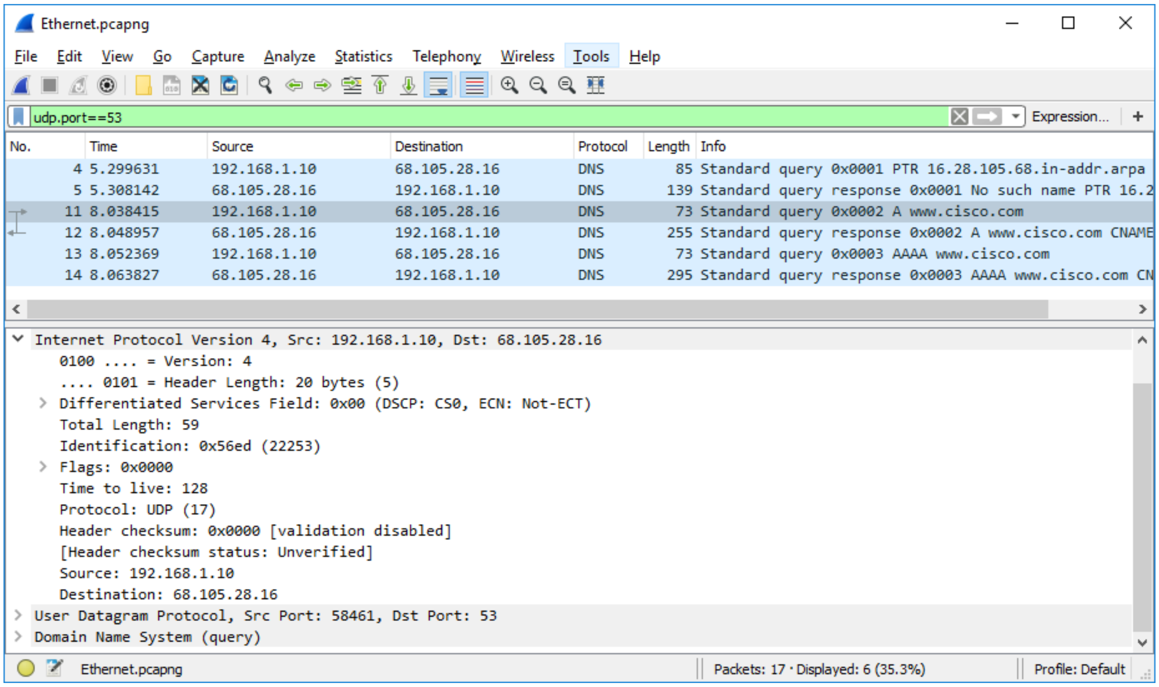
```
No.   Time       Source         Destination    Protocol  Length  Info
    4 5.299631   192.168.1.10   68.105.28.16   DNS           85  Standard query 0x0001 PTR 16.28.105.68.in-addr.arpa
    5 5.308142   68.105.28.16   192.168.1.10   DNS          139  Standard query response 0x0001 No such name PTR 16.2
   11 8.038415   192.168.1.10   68.105.28.16   DNS           73  Standard query 0x0002 A www.cisco.com
   12 8.048957   68.105.28.16   192.168.1.10   DNS          255  Standard query response 0x0002 A www.cisco.com CNAME
   13 8.052369   192.168.1.10   68.105.28.16   DNS           73  Standard query 0x0003 AAAA www.cisco.com
   14 8.063827   68.105.28.16   192.168.1.10   DNS          295  Standard query response 0x0003 AAAA www.cisco.com CN
```

```
> Frame 11: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
v Ethernet II, Src: PcsCompu_80:91:db (08:00:27:80:91:db), Dst: Netgear_18:a6:81 (cc:40:d0:18:a6:81)
  v Destination: Netgear_18:a6:81 (cc:40:d0:18:a6:81)
      Address: Netgear_18:a6:81 (cc:40:d0:18:a6:81)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: PcsCompu_80:91:db (08:00:27:80:91:db)
      Address: PcsCompu_80:91:db (08:00:27:80:91:db)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.10, Dst: 68.105.28.16
> User Datagram Protocol, Src Port: 58461, Dst Port: 53
> Domain Name System (query)
```

Ethernet.pcapng | Packets: 17 · Displayed: 6 (35.3%) | Profile: Default

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

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


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

udp.port==53

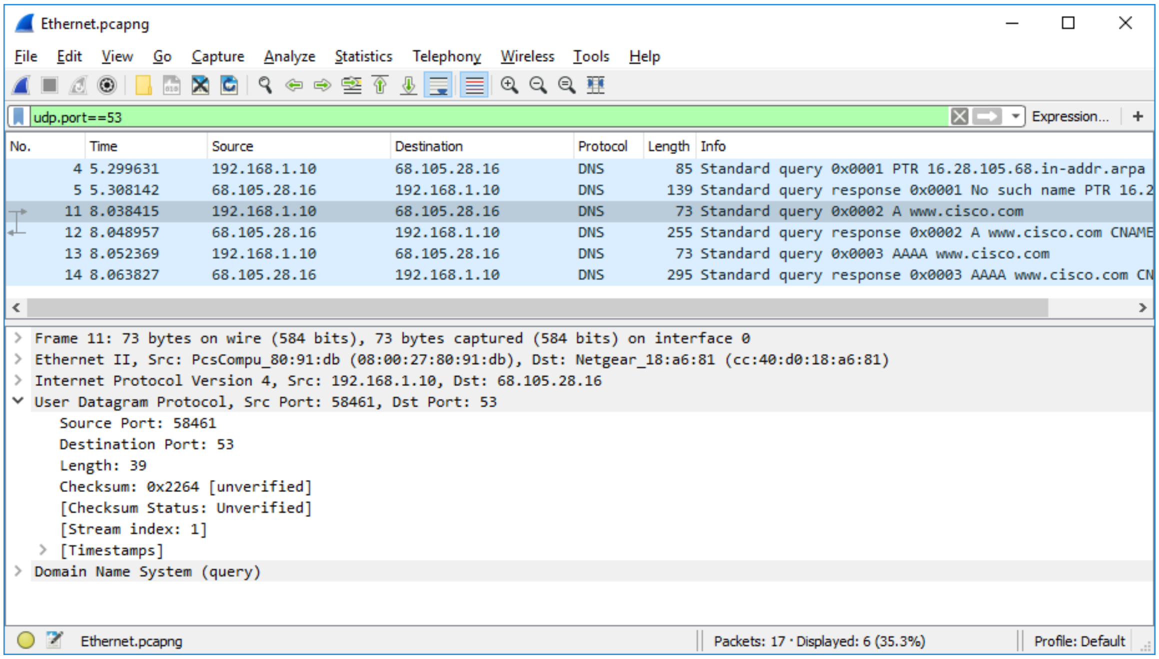
```
No.  Time        Source         Destination    Protocol  Length  Info
   4 5.299631    192.168.1.10   68.105.28.16   DNS           85  Standard query 0x0001 PTR 16.28.105.68.in-addr.arpa
   5 5.308142    68.105.28.16   192.168.1.10   DNS          139  Standard query response 0x0001 No such name PTR 16.2
  11 8.038415    192.168.1.10   68.105.28.16   DNS           73  Standard query 0x0002 A www.cisco.com
  12 8.048957    68.105.28.16   192.168.1.10   DNS          255  Standard query response 0x0002 A www.cisco.com CNAME
  13 8.052369    192.168.1.10   68.105.28.16   DNS           73  Standard query 0x0003 AAAA www.cisco.com
  14 8.063827    68.105.28.16   192.168.1.10   DNS          295  Standard query response 0x0003 AAAA www.cisco.com CN
```

```
v Internet Protocol Version 4, Src: 192.168.1.10, Dst: 68.105.28.16
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 59
     Identification: 0x56ed (22253)
   > Flags: 0x0000
     Time to live: 128
     Protocol: UDP (17)
     Header checksum: 0x0000 [validation disabled]
     [Header checksum status: Unverified]
     Source: 192.168.1.10
     Destination: 68.105.28.16
> User Datagram Protocol, Src Port: 58461, Dst Port: 53
> Domain Name System (query)
```

Ethernet.pcapng | Packets: 17 · Displayed: 6 (35.3%) | Profile: Default

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

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


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

udp.port==53

No.	Time	Source	Destination	Protocol	Length	Info
4	5.299631	192.168.1.10	68.105.28.16	DNS	85	Standard query 0x0001 PTR 16.28.105.68.in-addr.arpa
5	5.308142	68.105.28.16	192.168.1.10	DNS	139	Standard query response 0x0001 No such name PTR 16.2
11	8.038415	192.168.1.10	68.105.28.16	DNS	73	Standard query 0x0002 A www.cisco.com
12	8.048957	68.105.28.16	192.168.1.10	DNS	255	Standard query response 0x0002 A www.cisco.com CNAME
13	8.052369	192.168.1.10	68.105.28.16	DNS	73	Standard query 0x0003 AAAA www.cisco.com
14	8.063827	68.105.28.16	192.168.1.10	DNS	295	Standard query response 0x0003 AAAA www.cisco.com CN

```
> Frame 11: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
> Ethernet II, Src: PcsCompu_80:91:db (08:00:27:80:91:db), Dst: Netgear_18:a6:81 (cc:40:d0:18:a6:81)
> Internet Protocol Version 4, Src: 192.168.1.10, Dst: 68.105.28.16
v User Datagram Protocol, Src Port: 58461, Dst Port: 53
    Source Port: 58461
    Destination Port: 53
    Length: 39
    Checksum: 0x2264 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  > [Timestamps]
> Domain Name System (query)
```

Ethernet.pcapng | Packets: 17 · Displayed: 6 (35.3%) | Profile: Default

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

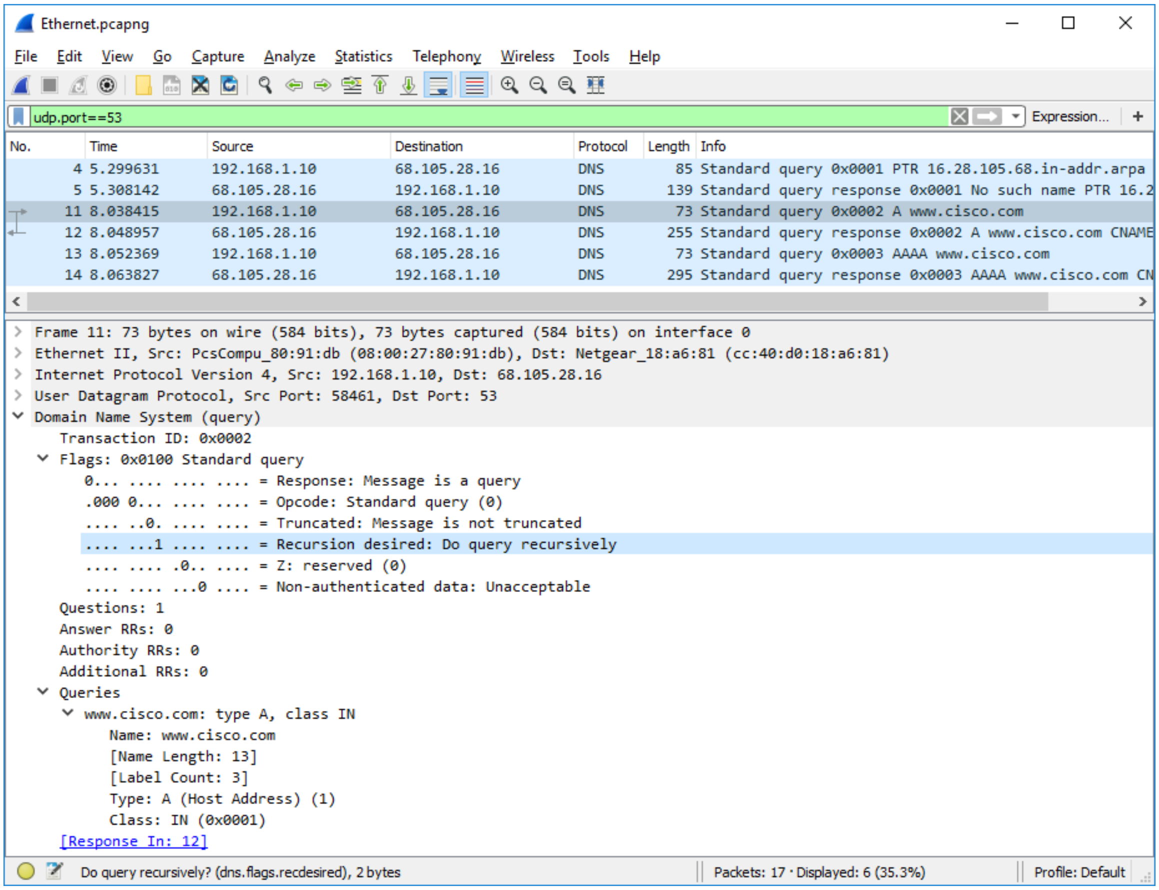
c. Open a Command Prompt and enter **arp –a** and **ipconfig /all** to record the MAC and IP addresses of the PC.

```
C:\Users\Student> arp -a

Interface: 192.168.1.10 --- 0x4
  Internet Address      Physical Address      Type
  192.168.1.1           cc-40-d0-18-a6-81     dynamic
  192.168.1.122         b0-a7-37-46-70-bb     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\Studuent> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
   Physical Address. . . . . . . . . : 08-00-27-80-91-DB
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d829:6d18:e229:a705%4(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.10(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Tuesday, August 20, 2019 5:39:51 PM
   Lease Expires . . . . . . . . . . : Wednesday, August 21, 2019 5:39:50 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 50855975
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-21-BA-64-08-00-27-80-91-DB
   DNS Servers . . . . . . . . . . . : 68.105.28.16
                                       68.105.29.16
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Compare the MAC and IP addresses in the Wireshark results to the results from the **ipconfig /all** results. What is your observation?

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

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


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

udp.port==53

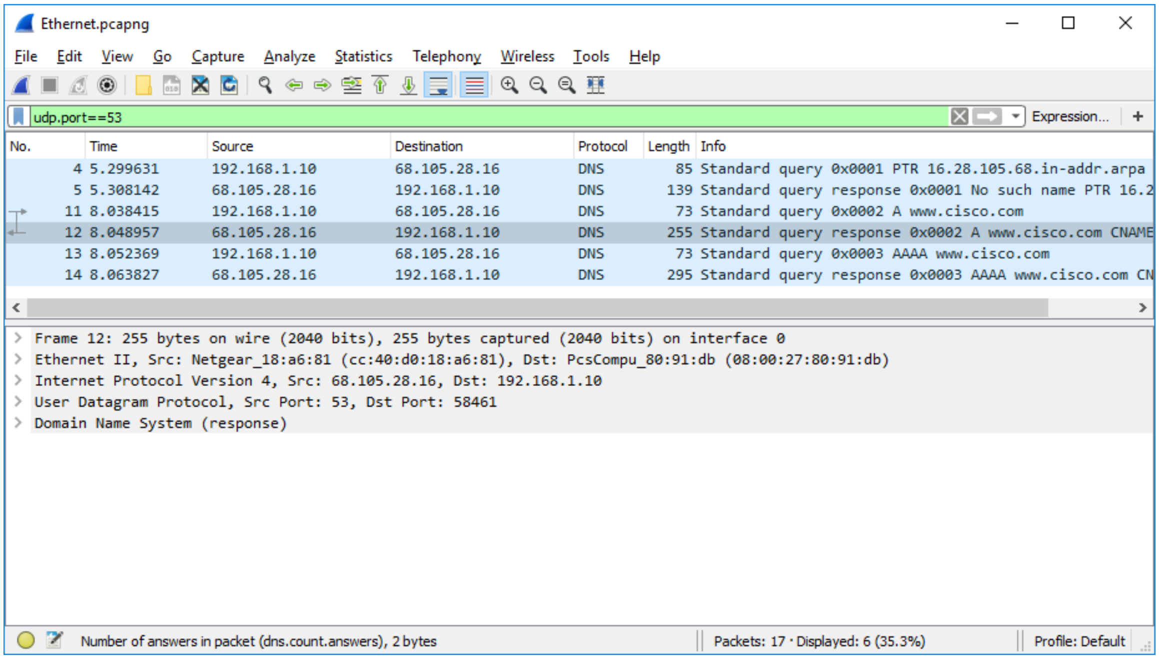
```
No.  Time      Source        Destination   Protocol Length Info
   4 5.299631  192.168.1.10  68.105.28.16  DNS        85 Standard query 0x0001 PTR 16.28.105.68.in-addr.arpa
   5 5.308142  68.105.28.16  192.168.1.10  DNS       139 Standard query response 0x0001 No such name PTR 16.2
  11 8.038415  192.168.1.10  68.105.28.16  DNS        73 Standard query 0x0002 A www.cisco.com
  12 8.048957  68.105.28.16  192.168.1.10  DNS       255 Standard query response 0x0002 A www.cisco.com CNAME
  13 8.052369  192.168.1.10  68.105.28.16  DNS        73 Standard query 0x0003 AAAA www.cisco.com
  14 8.063827  68.105.28.16  192.168.1.10  DNS       295 Standard query response 0x0003 AAAA www.cisco.com CN
```

```
> Frame 11: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
> Ethernet II, Src: PcsCompu_80:91:db (08:00:27:80:91:db), Dst: Netgear_18:a6:81 (cc:40:d0:18:a6:81)
> Internet Protocol Version 4, Src: 192.168.1.10, Dst: 68.105.28.16
> User Datagram Protocol, Src Port: 58461, Dst Port: 53
v Domain Name System (query)
    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)
    [Response In: 12]
```

Do query recursively? (dns.flags.recdesired), 2 bytes | Packets: 17 · Displayed: 6 (35.3%) | Profile: Default

Step 3: Explore DNS Response Traffic

a. Select the corresponding response DNS packet labeled **Standard query response 0x0002 A www.cisco.com**.


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

udp.port==53

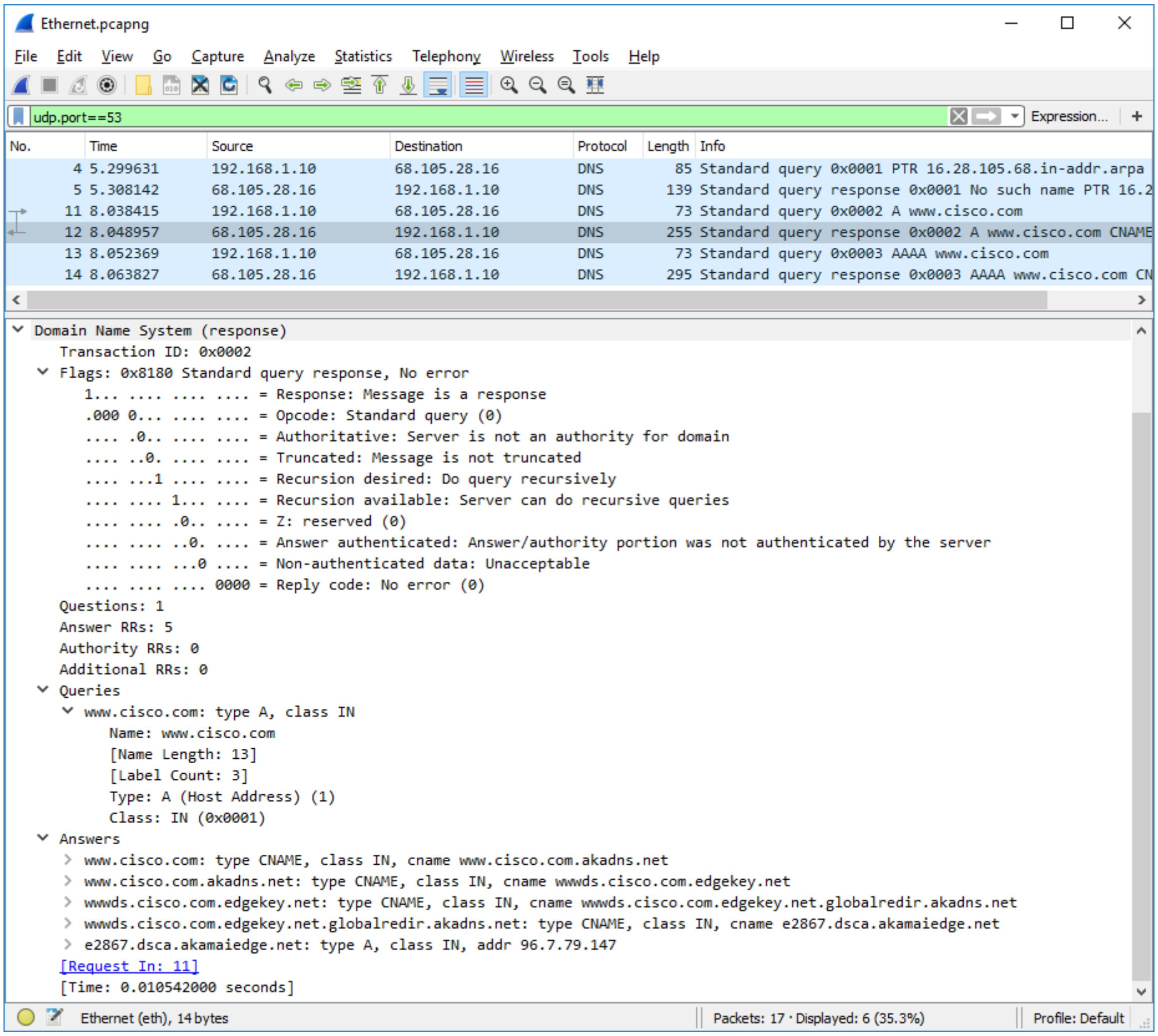
```
No.   Time       Source          Destination     Protocol  Length Info
    4 5.299631   192.168.1.10    68.105.28.16    DNS           85 Standard query 0x0001 PTR 16.28.105.68.in-addr.arpa
    5 5.308142   68.105.28.16    192.168.1.10    DNS          139 Standard query response 0x0001 No such name PTR 16.2
   11 8.038415   192.168.1.10    68.105.28.16    DNS           73 Standard query 0x0002 A www.cisco.com
   12 8.048957   68.105.28.16    192.168.1.10    DNS          255 Standard query response 0x0002 A www.cisco.com CNAME
   13 8.052369   192.168.1.10    68.105.28.16    DNS           73 Standard query 0x0003 AAAA www.cisco.com
   14 8.063827   68.105.28.16    192.168.1.10    DNS          295 Standard query response 0x0003 AAAA www.cisco.com CN
```

```
> Frame 12: 255 bytes on wire (2040 bits), 255 bytes captured (2040 bits) on interface 0
> Ethernet II, Src: Netgear_18:a6:81 (cc:40:d0:18:a6:81), Dst: PcsCompu_80:91:db (08:00:27:80:91:db)
> Internet Protocol Version 4, Src: 68.105.28.16, Dst: 192.168.1.10
> User Datagram Protocol, Src Port: 53, Dst Port: 58461
> Domain Name System (response)
```

Number of answers in packet (dns.count.answers), 2 bytes | Packets: 17 · Displayed: 6 (35.3%) | Profile: Default

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?

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



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

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

```
No.   Time        Source          Destination     Protocol  Length Info
    4 5.299631    192.168.1.10    68.105.28.16    DNS           85 Standard query 0x0001 PTR 16.28.105.68.in-addr.arpa
    5 5.308142    68.105.28.16    192.168.1.10    DNS          139 Standard query response 0x0001 No such name PTR 16.2
   11 8.038415    192.168.1.10    68.105.28.16    DNS           73 Standard query 0x0002 A www.cisco.com
   12 8.048957    68.105.28.16    192.168.1.10    DNS          255 Standard query response 0x0002 A www.cisco.com CNAME
   13 8.052369    192.168.1.10    68.105.28.16    DNS           73 Standard query 0x0003 AAAA www.cisco.com
   14 8.063827    68.105.28.16    192.168.1.10    DNS          295 Standard query response 0x0003 AAAA www.cisco.com CN
```

```
Domain Name System (response)
    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 server
      .... .... ...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.akadns.net
    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 96.7.79.147
    [Request In: 11]
    [Time: 0.010542000 seconds]
```

```
Ethernet (eth), 14 bytes    Packets: 17 · Displayed: 6 (35.3%)    Profile: Default
```

Can the DNS server do recursive queries?

c. Observe the CNAME and A records in the answers details.

How do the results compare to nslookup results?

Reflection Question

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

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