

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.

- 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.
- 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.

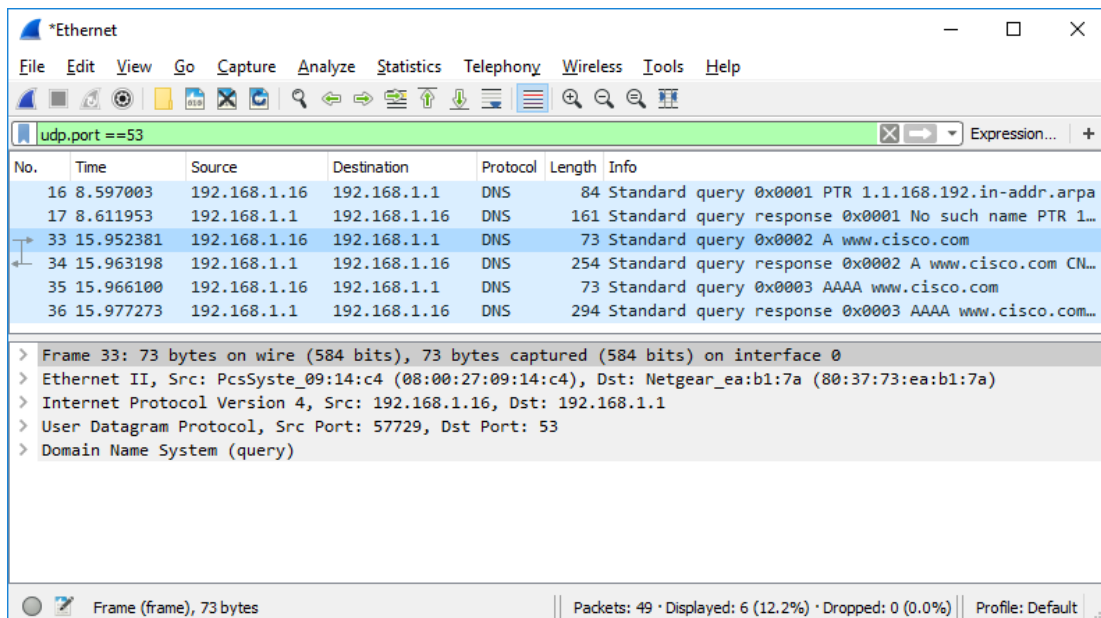
- Start Wireshark. Select an active interface with traffic for packet capture.
- Clear the DNS cache.
 - In Windows, enter **ipconfig /flushdns** in Command Prompt.
 - For the majority of Linux distributions, one of the following utilities is used for DNS caching: Systemd - Resolved, DNSMasq, and NSCD. 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.
 - 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**

Lab - Exploring DNS Traffic

- (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 may be slightly different.



- 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).

Lab - Exploring DNS Traffic

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

The screenshot shows the Wireshark interface with a packet capture filter of `udp.port == 53`. The packet list pane displays the following data:

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...

The packet details pane for packet 33 is expanded to show the following layers:

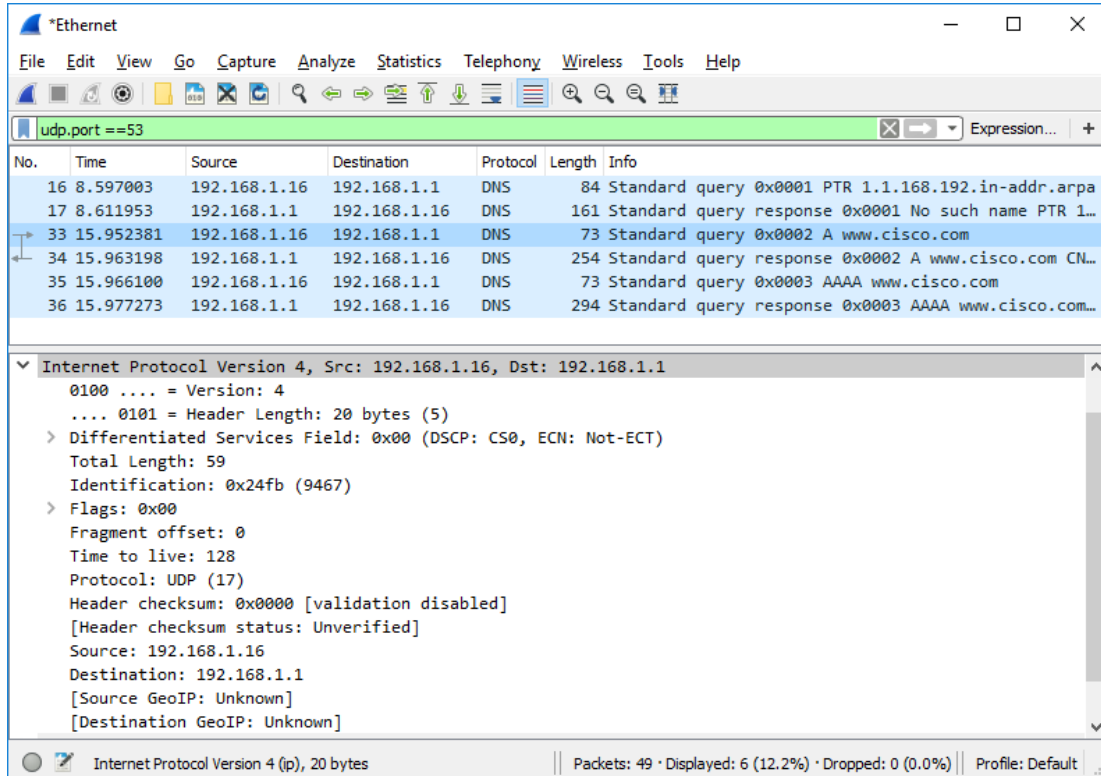
- Frame 33: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
- Ethernet II, Src: PcsSyste_09:14:c4 (08:00:27:09:14:c4), Dst: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)
 - Destination: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)
 - Address: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)
 -0. = LG bit: Globally unique address (factory default)
 -0. = IG bit: Individual address (unicast)
 - 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)

The status bar at the bottom indicates: 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?

Lab - Exploring DNS Traffic

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



The image shows a Wireshark packet capture window titled "*Ethernet". The filter bar contains the expression "udp.port == 53". The packet list pane shows six packets, with packet 33 selected. The packet details pane is expanded to show the "Internet Protocol Version 4" section. The status bar at the bottom indicates "Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%)".

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...

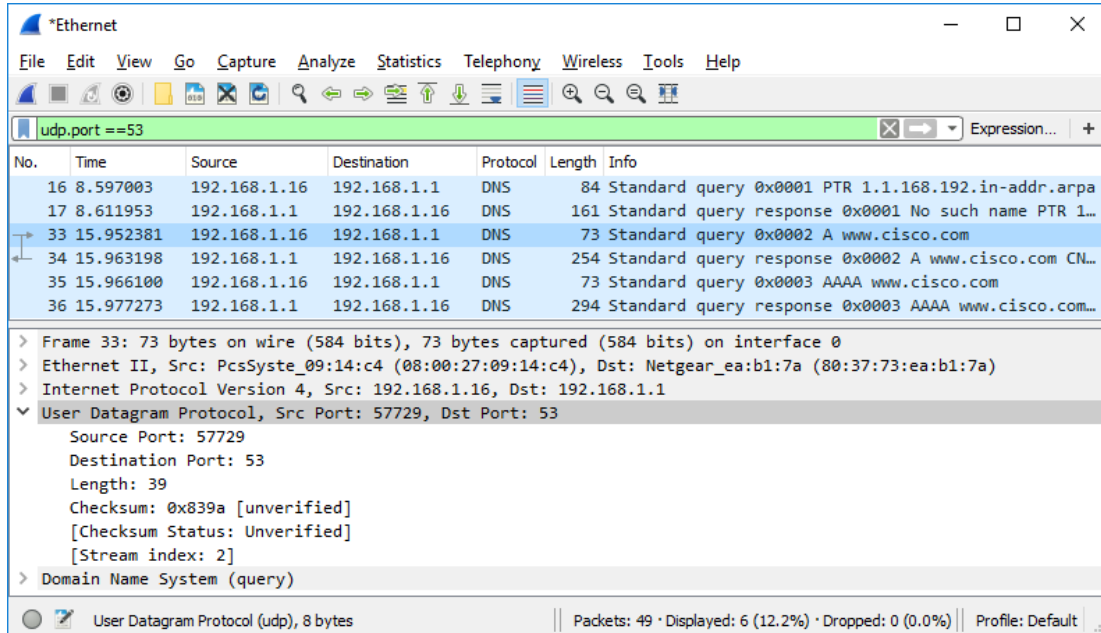
Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1

- 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]

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

Lab - Exploring DNS Traffic

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



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
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

What are the source and destination ports? What 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.

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

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

Lab - Exploring DNS Traffic

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

The image shows a Wireshark packet capture window titled "*Ethernet". The filter bar at the top is set to "udp.port == 53". The packet list pane shows several DNS packets. Packet 33 is selected, showing a query for "www.cisco.com". The packet details pane is expanded to show the "Domain Name System (query)" section. The transaction ID is 0x0002. The flags are 0x0100, indicating a standard query with recursion desired. The question section shows a query for "www.cisco.com" of type A and class IN.

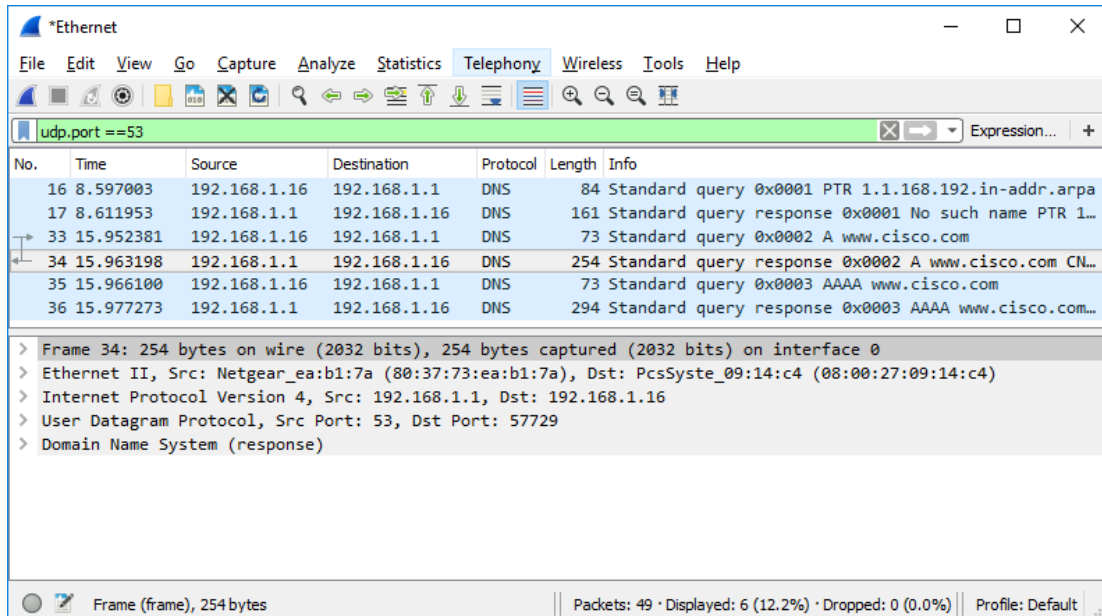
No.	Time	Source	Destination	Protocol	Length	Info
16	8.597003	192.168.1.16	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
17	8.611953	192.168.1.1	192.168.1.16	DNS	161	Standard query response 0x0001 No such name PTR 1...
33	15.952381	192.168.1.16	192.168.1.1	DNS	73	Standard query 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
Domain Name System (query)
[Response In: 34]
Transaction ID: 0x0002
Flags: 0x0100 Standard query
0... .. = Response: Message is a query
.000 0... .. = Opcode: Standard query (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
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)

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.



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**.
- c. Observe the results.
Can the DNS server do recursive queries?

Lab - Exploring DNS Traffic

The image shows a Wireshark capture of DNS traffic. The packet list pane shows several DNS packets. Packet 34 is selected, showing a 'Standard query response' for 'A www.cisco.com'. The packet details pane shows the 'Domain Name System (response)' structure, including flags, questions, and answers. The answers section lists several CNAME and A records for www.cisco.com.

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 wwds.cisco.com.edgekey.net
    wwds.cisco.com.edgekey.net: type CNAME, class IN, cname wwds.cisco.com.edgekey.net.globalredir.akadn
    wwds.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
```

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

How do the results compare to nslookup results?

Reflection

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?