Chapter **8a**

Hands-On: Wireshark Packet Capture

LEARNING OBJECTIVES

By the end of this chapter, you should be able to:

- Use the Wireshark packet capture program at a novice level.
- Capture packets in real time.
- Analyze the packets at a novice level.

INTRODUCTION

A good way to practice what you have learned in this chapter is to look at individual packets. Packet capture programs record packets going into and out of your computer. If you capture a brief webserver interaction, you can look at header fields, TCP three-step connection starts, and other information. There are several good packet capture programs. We look at Wireshark, which is simple to use, popular, and free to download. (At least at the time of this writing.)

GETTING WIRESHARK

To get Wireshark, go to wireshark.org. Do *not* go to wireshark.com. Follow the instructions and download the program on your computer.

USING WIRESHARK

Getting Started

After installation, open the Wireshark program. You will see the opening screen. It will look like the screen in Figure 8a-1. There will be controls at the top with a blank area below them. You will soon fill this area with your packet capture.

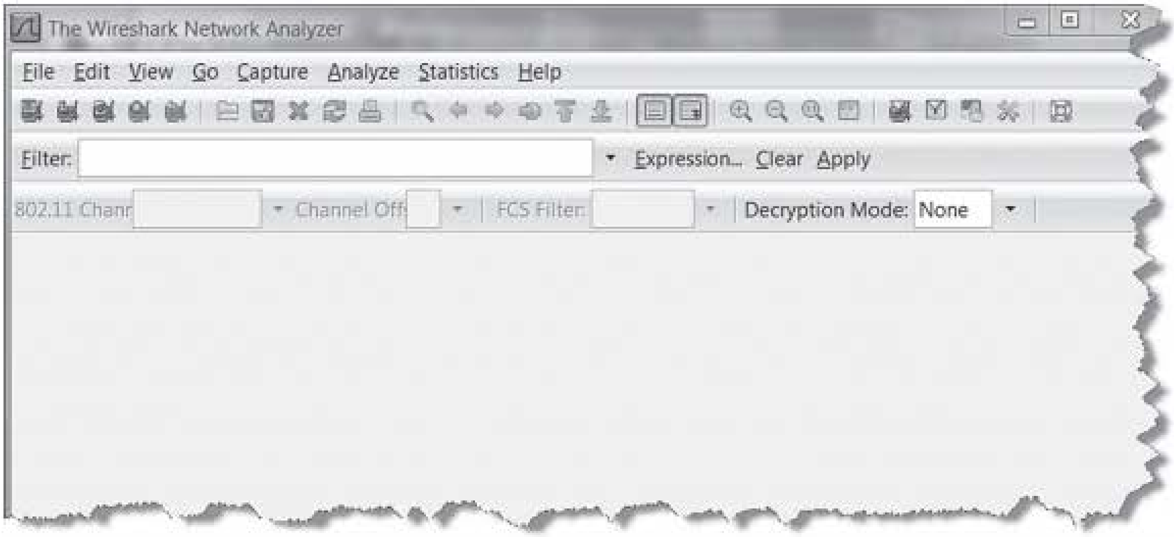

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
802.11 Chann
Channel Off
FCS Filter:
Decryption Mode: None

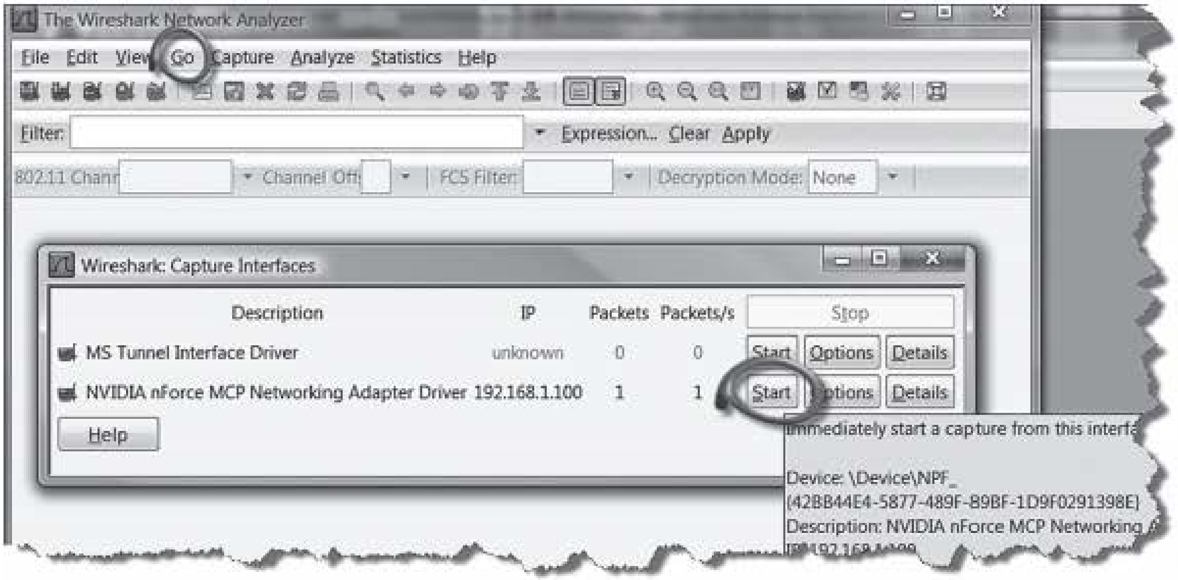
FIGURE 8a-1 Initial Wireshark Screen

Starting a Packet Capture

To start a packet capture, click on the Go menu item. Then, when the Wireshark: Capture Interfaces dialog box appears, as Figure 8a-2 illustrates, select a network interface and click on Start.

Getting Data

Your browser should already be open. Switch to your browser and enter a URL. (In this example, the author went to Wikipedia.org.) This creates a flurry of packets between

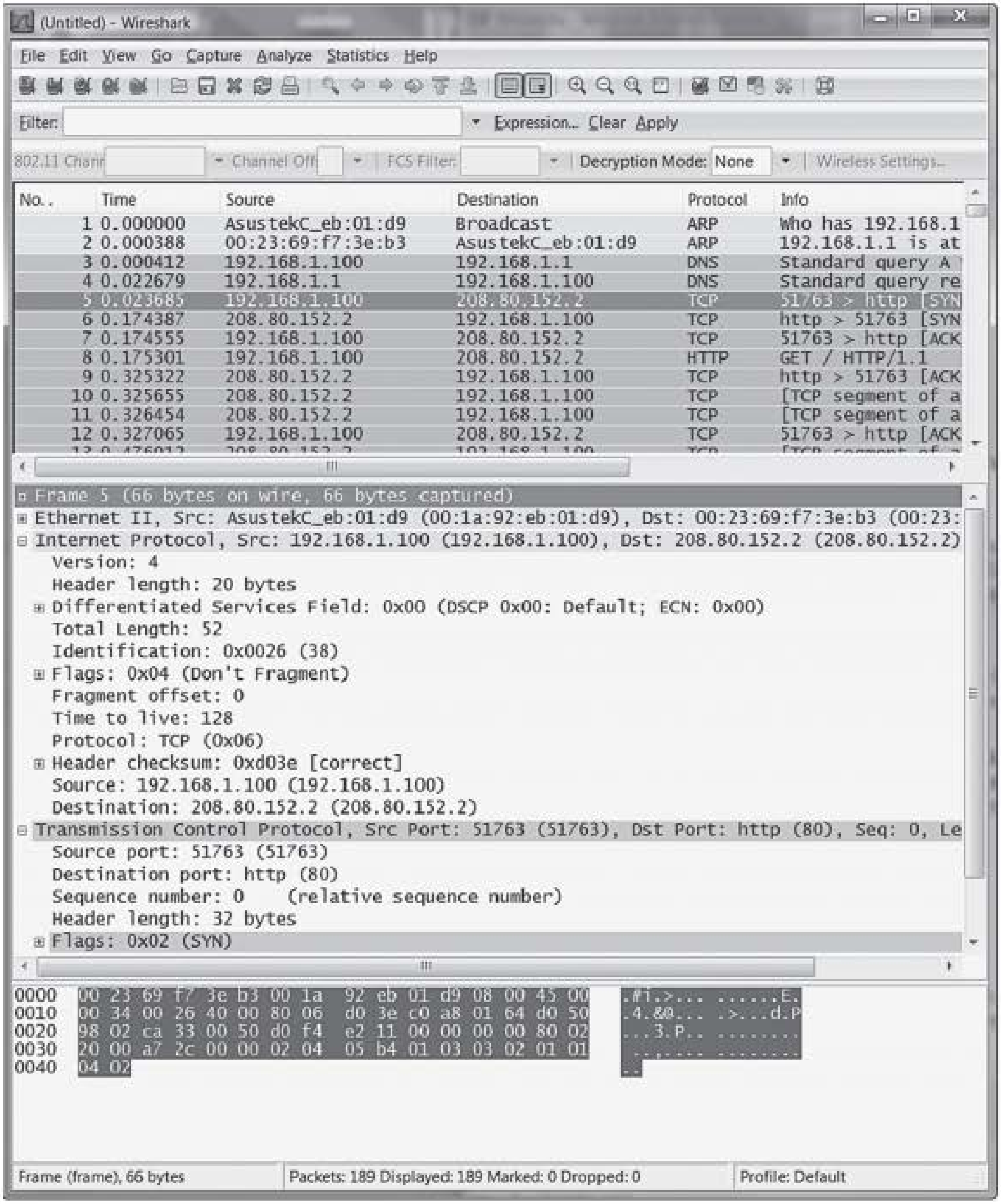

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
802.11 Chann
Channel Off
FCS Filter:
Decryption Mode: None
Wireshark: Capture Interfaces
Stop
Help

Description	IP	Packets	Packets/s			
MS Tunnel Interface Driver	unknown	0	0	Start	Options	Details
NVIDIA nForce MCP Networking Adapter Driver	192.168.1.100	1	1	Start	ptions	Details

mmediately start a capture from this interfa

Device: \Device\NPF_
{42BB44E4-5877-489F-89BF-1D9F0291398E}
Description: NVIDIA nForce MCP Networking A
IP: 192.168.1.100

FIGURE 8a-2 Starting a Packet Capture in Wireshark



No. .	Time	Source	Destination	Protocol	Info
1	0.000000	AsustekC_eb:01:d9	Broadcast	ARP	Who has 192.168.1
2	0.000388	00:23:69:f7:3e:b3	AsustekC_eb:01:d9	ARP	192.168.1.1 is at
3	0.000412	192.168.1.100	192.168.1.1	DNS	Standard query A
4	0.022679	192.168.1.1	192.168.1.100	DNS	Standard query re
5	0.023685	192.168.1.100	208.80.152.2	TCP	51763 > http [SYN
6	0.174387	208.80.152.2	192.168.1.100	TCP	http > 51763 [SYN
7	0.174555	192.168.1.100	208.80.152.2	TCP	51763 > http [ACK
8	0.175301	192.168.1.100	208.80.152.2	HTTP	GET / HTTP/1.1
9	0.325322	208.80.152.2	192.168.1.100	TCP	http > 51763 [ACK
10	0.325655	208.80.152.2	192.168.1.100	TCP	[TCP segment of a
11	0.326454	208.80.152.2	192.168.1.100	TCP	[TCP segment of a
12	0.327065	192.168.1.100	208.80.152.2	TCP	51763 > http [ACK

```
⊞ Frame 5 (66 bytes on wire, 66 bytes captured)
⊞ Ethernet II, Src: AsustekC_eb:01:d9 (00:1a:92:eb:01:d9), Dst: 00:23:69:f7:3e:b3 (00:23:
⊟ Internet Protocol, Src: 192.168.1.100 (192.168.1.100), Dst: 208.80.152.2 (208.80.152.2)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 52
    Identification: 0x0026 (38)
  ⊞ Flags: 0x04 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (0x06)
  ⊞ Header checksum: 0xd03e [correct]
    Source: 192.168.1.100 (192.168.1.100)
    Destination: 208.80.152.2 (208.80.152.2)
⊟ Transmission Control Protocol, Src Port: 51763 (51763), Dst Port: http (80), Seq: 0, Le
    Source port: 51763 (51763)
    Destination port: http (80)
    Sequence number: 0    (relative sequence number)
    Header length: 32 bytes
  ⊞ Flags: 0x02 (SYN)
```

```
0000  00 23 69 f7 3e b3 00 1a  92 eb 01 d9 08 00 45 00   .#i.>... ......E.
0010  00 34 00 26 40 00 80 06  d0 3e c0 a8 01 64 d0 50   .4.&@... .>...d.P
0020  98 02 ca 33 00 50 d0 f4  e2 11 00 00 00 00 80 02   ...3.P.. ........
0030  20 00 a7 2c 00 00 02 04  05 b4 01 03 03 02 01 01    ..,..... ........
0040  04 02                                              ..
```

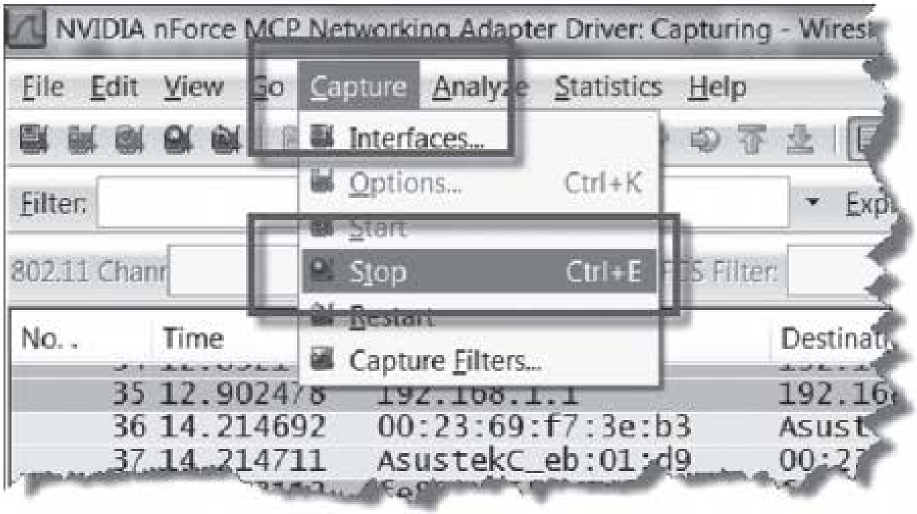
Frame (frame), 66 bytes | Packets: 189 Displayed: 189 Marked: 0 Dropped: 0 | Profile: Default

FIGURE 8a-3 Collecting Data

you and the host specified in the URL. These appear on the window below the controls, as shown in Figure 8a-3.

Stopping Data Collection

To stop the data collection, click on the Capture menu item, as Figure 8a-4 shows. When the dropdown menu appears, select *Stop*. You now have a packet stream to analyze.



```
35 12.902478  192.168.1.1         192.16
36 14.214692  00:23:69:f7:3e:b3   Asust
37 14.214711  AsustekC_eb:01:d9   00:2
```

FIGURE 8a-4 Stopping the Data Collection

Looking at Individual Packets

Now you can begin looking at individual packets. To see how to do this, look again at Figure 8a-3.

Packet Summary Window In the upper window in the display area, you can see the packets one at a time. The capture begins with two ARP packets, which identify the data link layer address of the host with IP address 192.168.1.1.

Then comes two DNS packets. In the example, the author typed the host name Wikipedia.org in the URL. The author's computer (192.168.1.100) sent a DNS request message to its DNS server to get the IP address for Wikipedia.org. The DNS sent back the requested IP address.

Now, the author's computer opened a connection to 208.80.152.2, which is Wireshark.org's IP address.[1] It first sent a TCP SYN segment to 208.80.152.2. This is Frame 5. In Figure 8a-3, the frame has been selected.

Information about the contents of this particular frame is shown in a window below the window showing each frame on a single line. First, the window shows information on the Ethernet header and trailer. Next comes information about the IP packet, followed by information about the TCP SYN segment contained in the packet.

Window with Detailed Information on the Selected Packet The Ethernet information has been minimized. Only the source and destination MAC addresses are shown. However, information about the IP packet has been maximized. You can see the values of the individual fields in the selected packet. For example, note that the Time to Live Field in this packet has the value 128. In addition, the protocol field value indicates that the data field contains a TCP segment.

[1] If you try this, you may get a different IP address. Many firms have multiple physical webservers that they associate with a host name. A DNS response message returns the IP address of one of these physical servers.

The TCP segment information also is expanded, although only the first few fields are shown in the window. Note that the destination port is 80, indicating that the author was contacting the Wireshark.org webserver. Note also that the Flag Fields information says that the SYN bit is set, as one would expect.

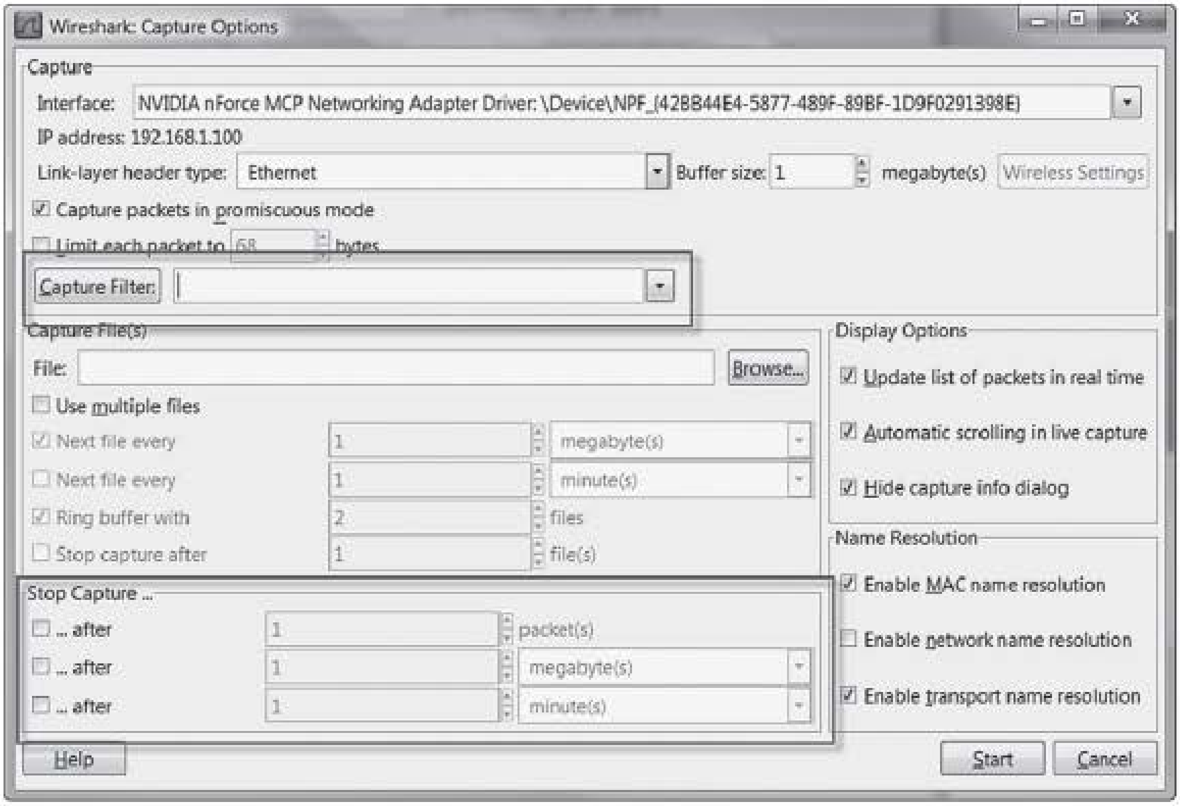
To make life easier for you, Wireshark does as much translation as possible. For example, it interprets the information in the protocol field as indicating that there is a TCP segment in the packet's data field. It also indicates that Port 80 is HTTP.

The information on sequence number is highly simplified compared to the discussion in Chapter 2. This is the first TCP segment being sent. It is given the value 0 rather than its complex real value.

Hex Window The lowest window shows the contents of the packet in hexadecimal (Base 16) format. Hex is difficult for new analysts to interpret, but it is very compact compared to the information in the middle window. Experienced packet analysts quickly learn the positions of important fields and learn to read the hex symbols for that field.

Options

Figure 8a-5 shows that Wireshark capture options allow you to control what packets are captured. If you are connected to multiple external servers simultaneously, this can allow you to capture only packets for a particular connection.



Wireshark: Capture Options

Capture

Interface: NVIDIA nForce MCP Networking Adapter Driver: \Device\NPF_{42BB44E4-5877-489F-89BF-1D9F0291398E}

IP address: 192.168.1.100

Link-layer header type: Ethernet Buffer size: 1 megabyte(s) Wireless Settings

☑ Capture packets in promiscuous mode

□ Limit each packet to 68 bytes

Capture Filter:

Capture File(s)

File: Browse...

□ Use multiple files

☑ Next file every 1 megabyte(s)

□ Next file every 1 minute(s)

☑ Ring buffer with 2 files

□ Stop capture after 1 file(s)

Stop Capture ...

□ ... after 1 packet(s)

□ ... after 1 megabyte(s)

□ ... after 1 minute(s)

Display Options

☑ Update list of packets in real time

☑ Automatic scrolling in live capture

☑ Hide capture info dialog

Name Resolution

☑ Enable MAC name resolution

□ Enable network name resolution

☑ Enable transport name resolution

FIGURE 8a-5 Wireshark Options

HANDS-ON EXERCISES

1. Do the following:
   - Download Wireshark.
   - Start Wireshark.
   - Turn on Wireshark capture.
   - Type a URL in your browser window (not Wikipedia.org).
   - After a few seconds, stop the capture.
   - Answer the following questions:

     1a. What URL did you use? What was the IP address of the webserver?

     1b. Find the frame in which your PC sent the SYN packet. List the source and destination IP address, the source and destination port numbers, and the header checksum.

     1c. Select the SYN/ACK packet. List the source and destination IP address, the source and destination port numbers, and the header checksum.

     1d. Select the packet that acknowledges the SYN/ACK segment. List the source and destination IP address, the source and destination port numbers, and the header checksum.

2. Change the options so that only packets you send are recorded. Do a capture. Click on the window containing Wireshark and hit Alt-Enter. This captures the window to your clipboard. Paste it into your homework.