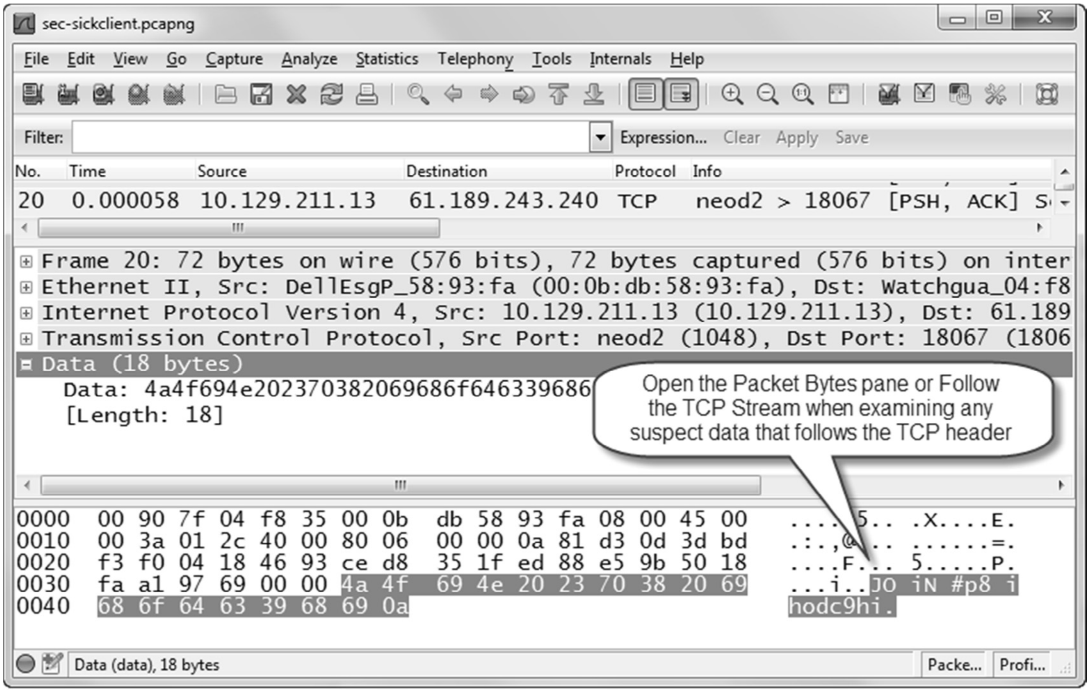
Port Resolution Vulnerabilities

Port resolution relies on the integrity of the *services* file and the application requesting to use a particular port number.

If a malicious user or program has altered the content of the *services* file, the port resolution process may be affected. Applications can also define which ports they will use. A malicious FTP program might use port 80 knowing that many companies do not block outbound traffic to this port.

Figure 377 shows an IRC communication that is not decoded as an IRC conversation because it uses a non-standard port number (18067).

Bot-infected hosts often use Internet Relay Chat (IRC) to communicate with Command and Control (C&C) servers. In this case, the bot-infected host connects to the IRC server on port 18067 and Wireshark defines the IRC communications as simply “Data”. In the bytes pane we can see the packet contains the JOIN command used to connect to an IRC channel.


sec-sickclient.pcapng
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No. Time      Source         Destination     Protocol Info
20  0.000058  10.129.211.13  61.189.243.240  TCP      neod2 > 18067 [PSH, ACK] S

⊞ Frame 20: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on inter
⊞ Ethernet II, Src: DellEsgP_58:93:fa (00:0b:db:58:93:fa), Dst: Watchgua_04:f8
⊞ Internet Protocol Version 4, Src: 10.129.211.13 (10.129.211.13), Dst: 61.189
⊞ Transmission Control Protocol, Src Port: neod2 (1048), Dst Port: 18067 (1806
⊟ Data (18 bytes)
    Data: 4a4f694e202370382069686f646339686
    [Length: 18]

0000  00 90 7f 04 f8 35 00 0b  db 58 93 fa 08 00 45 00   .....5.. .X....E.
0010  00 3a 01 2c 40 00 80 06  00 00 0a 81 d3 0d 3d bd   .:.,@... ......=.
0020  f3 f0 04 18 46 93 ce d8  35 1f ed 88 e5 9b 50 18   ....F... 5.....P.
0030  fa a1 97 69 00 00 4a 4f  69 4e 20 23 70 38 20 69   ...i..JO iN #p8 i
0040  68 6f 64 63 39 68 69 0a                            hodc9hi.
```

Open the Packet Bytes pane or Follow the TCP Stream when examining any suspect data that follows the TCP header

Figure 377. Traffic using non-standard ports may use the wrong dissector or not be decoded at all [sec-sickclient.pcapng]

Using the **right click | Decode As** function, we can force Wireshark to temporarily dissect traffic to and from port 18067 as IRC traffic as shown in Figure 378.

When you restart Wireshark or change to another profile, the dissector will not be in place.

In Wireshark 1.8 you can save your Decode As settings in a profile. Select **Analyze | User Specified Decodes** after you have applied a temporary decode. Click **Save** and Wireshark retains your new decode setting in a *decode_as_entries* file in your profile directory.