An introduction to Network Analyzers

Dr. Farid Farahmand

9/15/2016

Network Analysis and Sniffing

- Process of capturing, decoding, and analyzing network traffic
  - Why is the network slow
  - What is the network traffic pattern
  - How is the traffic being shared between nodes
- Also known as
  - traffic analysis, protocol analysis, sniffing, packet analysis, eavesdropping*, etc.

*Listen secretly to what is said in private!

Network Analyzer

- A combination of hardware and software tools what can detect, decode, and manipulate traffic on the network
  - Passive monitoring (detection) - Difficult to detect
  - Active (attack)
- Available both free and commercially
- Mainly software-based (utilizing OS and NIC)
  - Also known as *sniffer*
  - A program that monitors the data traveling through the network *passively*

- Common network analyzers
  - Wireshark / Ethereal
  - Windump
  - Etherpeak
  - Dsniff
  - And much more….

Read: Basic Packet-Sniffer Construction from the Ground Up!
by Chad Renfro
Checkout his program: sniff.c

Network Analyzer
Components

Capturing the data is easy!
The question is what to do with it!

- Hardware
  - Special hardware devices
    - Monitoring voltage fluctuation
    - Jitter (random timing variation)
    - Jabber (failure to handle electrical signals)
    - CRC and Parity Errors
  - NIC Card

- Capture driver
  - capturing the data
- Buffer
  - memory or disk-based
- Real-time analysis
  - analyzing the traffic in real time; detecting any intrusions
- Decoder
  - making data readable

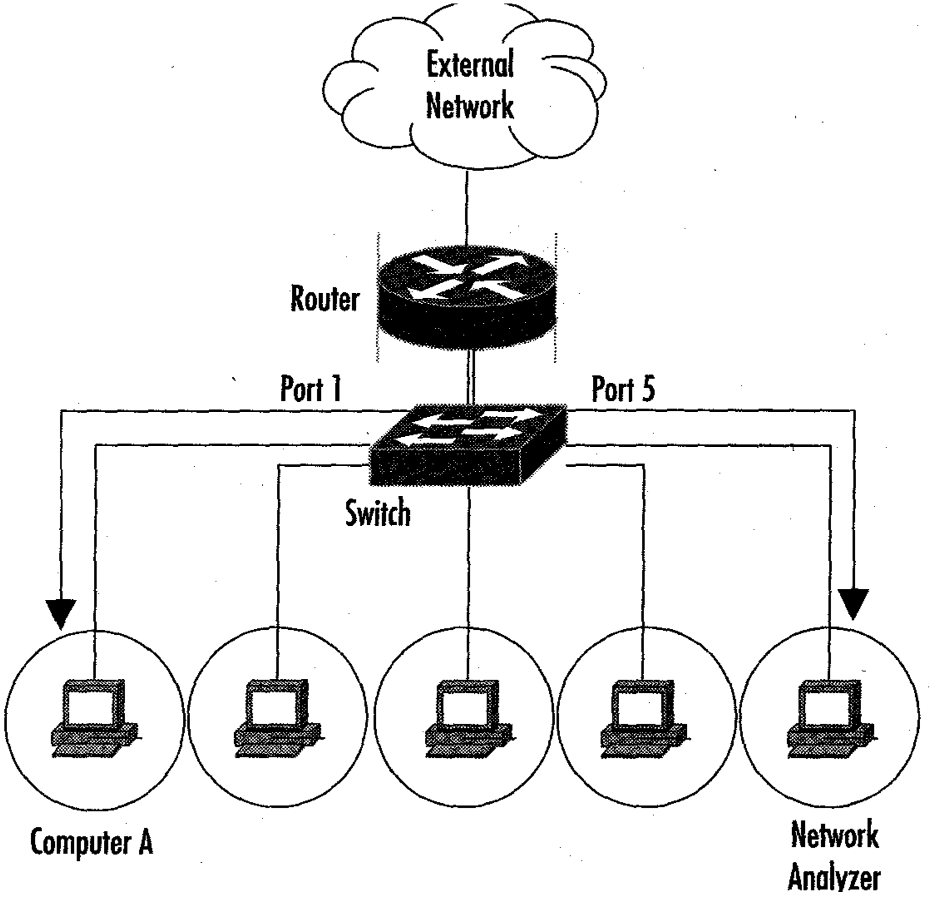
Who Uses Network Analyzers

- System administrators
  - Understand system problems and performance
- Malicious individuals (intruders)
  - Capture cleartext data
  - Passively collect data on vulnerable protocols
    - FTP, POP3, IMAP, SMATP, rlogin, HTTP, etc.
    - Capture VoIP data
  - Mapping the target network
  - Traffic pattern discovery
  - Actively break into the network (backdoor techniques)

Basic Operation

- Ethernet traffic is broadcasted to all nodes on the same segment
- Sniffer can capture all the incoming data when the NIC is in ***promiscuous*** mode:
  - `ifconfig eth0 promisc`
  - `ifconfig eth0 -promisc`
  - Default setup is ***non-promiscuous*** (only receives the data destined for the NIC)
  - Remember: a hub receives all the data!
- If switches are used the sniffer must perform **port spanning**
  - Also known as port mirroring
  - The traffic to each port is mirrored to the sniffer

Port Monitoring



Protecting Against Sniffers

Remember: 00:01:02:03:04:05
MAC address (HWaddr)=
Vender Address + Unique NIC #

- Spoofing the MAC is often referred to changing the MAC address (in Linux:)
  - `ifconfig eth0 down`
  - `ifconfig eth0 hw ether 00:01:02:03:04:05`
  - `ifconfig eth0 up`
  - Register the new MAC address by broadcasting it
    - `ping -c 1 -b 192.168.1.1`
- To detect a sniffer (Linux)
  - Download **Promisc.c**)
  - `ifconfig -a (search for` **`promisc`**`)`
  - `ip link (search for` **`promisc`**`)`
- To detect a sniffer (Windows)
  - Download PromiscDetect

Protecting Against Sniffers

Remember: Never use unauthorized Sniffers at wok!

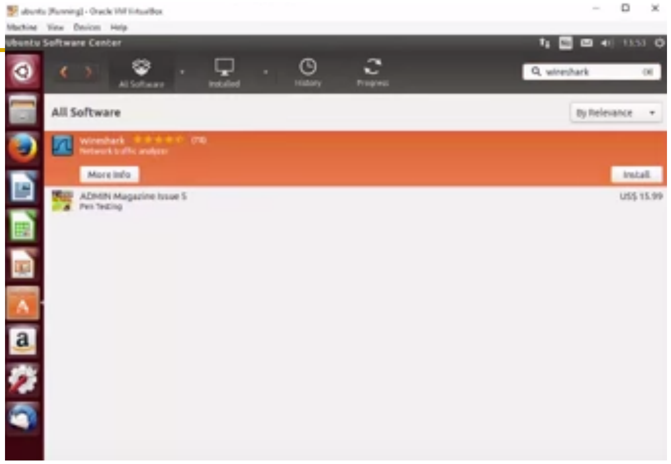
- Using switches can help
- Use encryption
  - Making the intercepted data unreadable
  - Note: in many protocols the packet headers are cleartext!
- VPNn use encryption and authorization for secure communications
  - VPN Methods
    - Secure Shell (SSH): headers are not encrypted
    - Secure Sockets Layer (SSL): high network level packet security; headers are not encrypted
    - IPsec: Encrypted headers but does not used TCP or UDP

What is Wireshark?

Remember: You must have a good understanding of the network before you use Sniffers effectively!

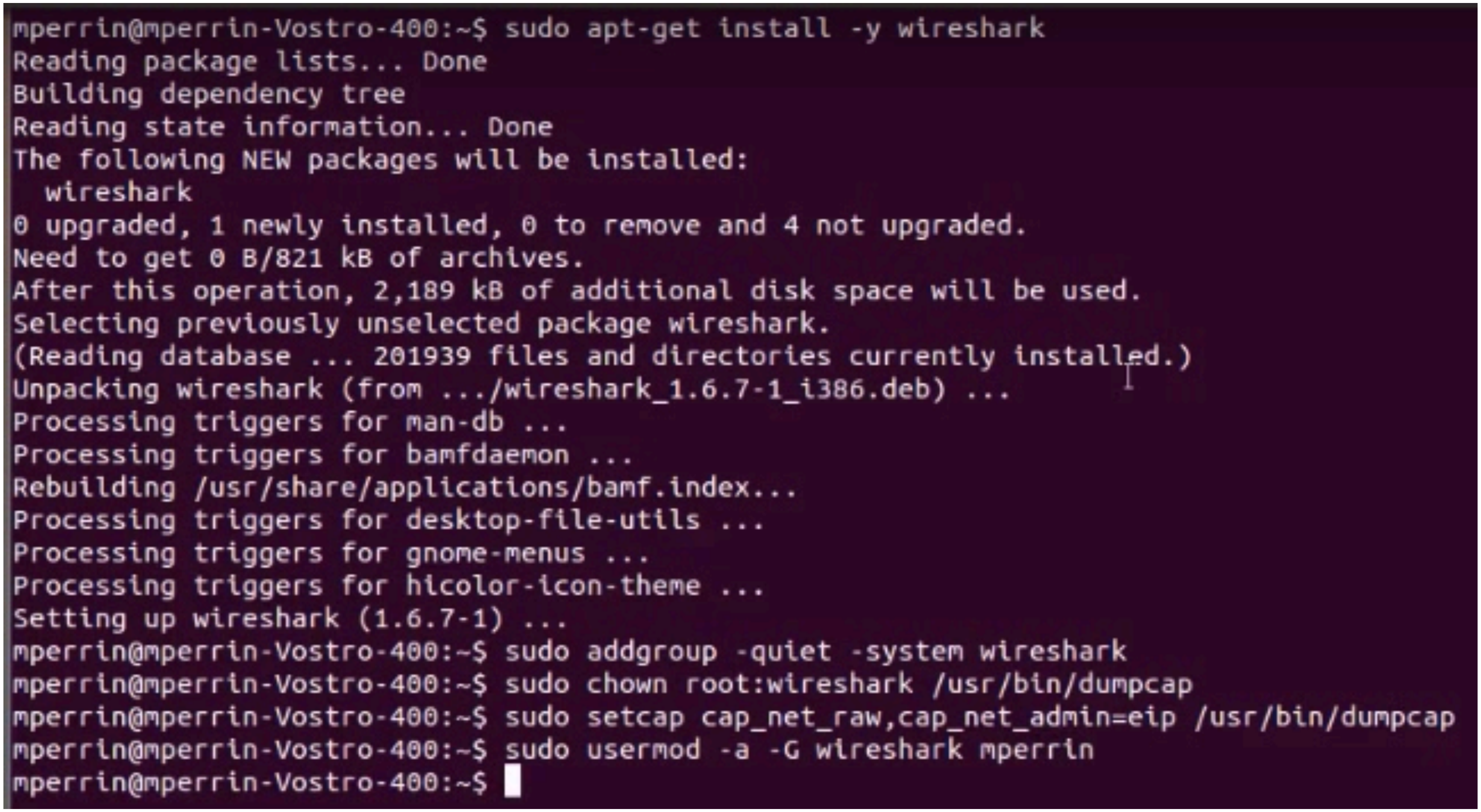
- Formerly called ***Ethereal***
- An open source program
  - free with many features
- Decodes over 750 protocols
- Compatible with many other sniffers
- Plenty of online resources are available
- Supports command-line and GUI interfaces
  - TSHARK (offers command line interface) has three components
    - Editcap (similar to Save as..to translate the format of captured packets)
    - Mergecap (combine multiple saved captured files)
    - Text2pcap (ASCII Hexdump captures and write the data into a libpcap output file)

Installing Wireshark



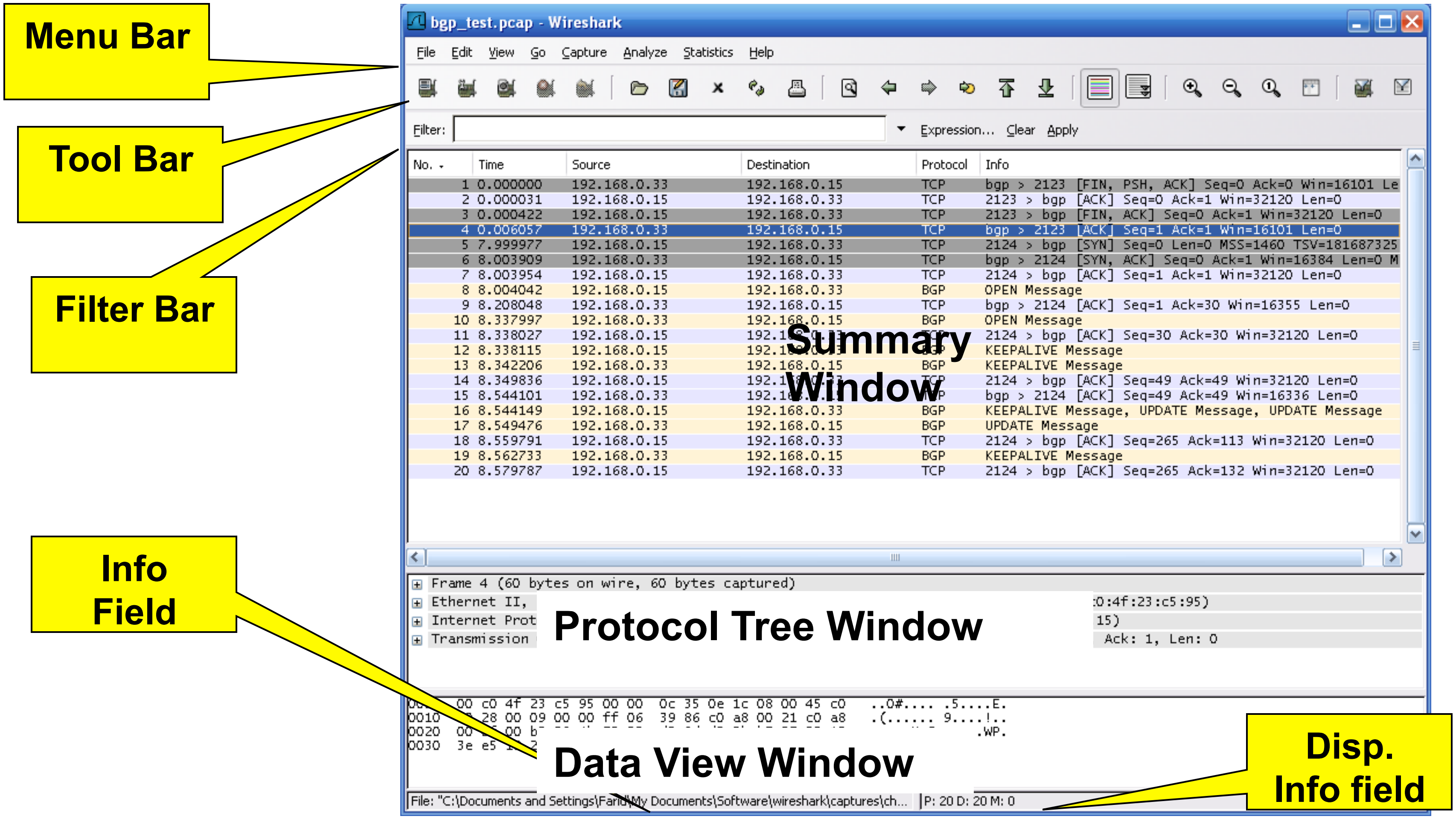
- Download the program from
  - www.wireshark.org/download.html
- Capture drivers include (monitor ports and capture all traveling packets)
  - Linux: libpcap
  - Windows: winpcap (www.winpcap.org)
- In Ubuntu
  - Use software Center https://www.youtube.com/watch?v=T3-3H9Bs5Nc
  - Or just open a terminal (Ctrl + Alt + T) and type *sudo* ***apt****-get* install <package name> .

Installing Wireshark – Command Line



```
mperrin@mperrin-Vostro-400:~$ sudo apt-get install -y wireshark
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  wireshark
0 upgraded, 1 newly installed, 0 to remove and 4 not upgraded.
Need to get 0 B/821 kB of archives.
After this operation, 2,189 kB of additional disk space will be used.
Selecting previously unselected package wireshark.
(Reading database ... 201939 files and directories currently installed.)
Unpacking wireshark (from .../wireshark_1.6.7-1_i386.deb) ...
Processing triggers for man-db ...
Processing triggers for bamfdaemon ...
Rebuilding /usr/share/applications/bamf.index...
Processing triggers for desktop-file-utils ...
Processing triggers for gnome-menus ...
Processing triggers for hicolor-icon-theme ...
Setting up wireshark (1.6.7-1) ...
mperrin@mperrin-Vostro-400:~$ sudo addgroup -quiet -system wireshark
mperrin@mperrin-Vostro-400:~$ sudo chown root:wireshark /usr/bin/dumpcap
mperrin@mperrin-Vostro-400:~$ sudo setcap cap_net_raw,cap_net_admin=eip /usr/bin/dumpcap
mperrin@mperrin-Vostro-400:~$ sudo usermod -a -G wireshark mperrin
mperrin@mperrin-Vostro-400:~$ █
```

Wireshark Window



Menu Bar

Tool Bar

Filter Bar

Info Field

Summary Window

Protocol Tree Window

Data View Window

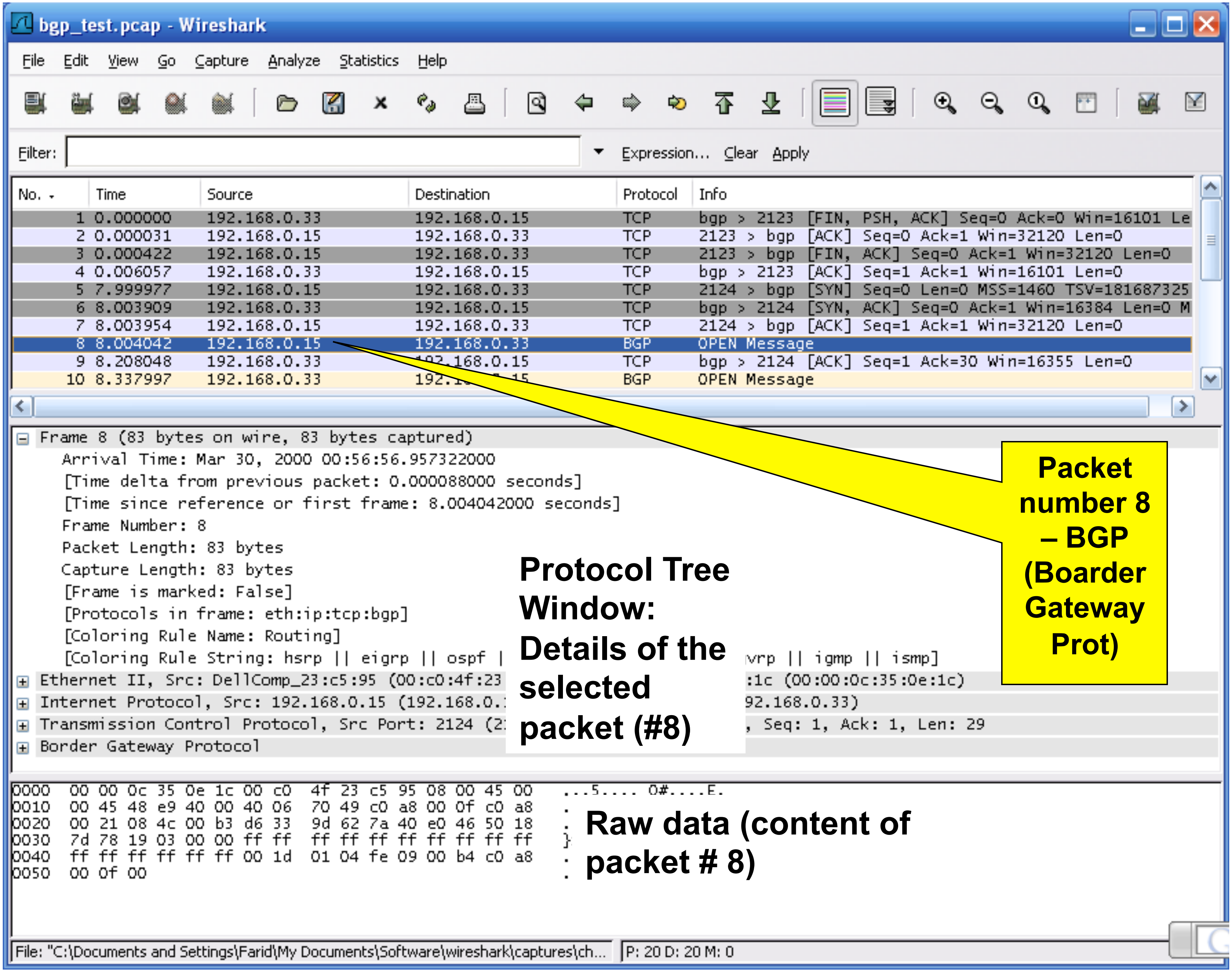
Disp. Info field

```
No. .  Time       Source         Destination    Protocol  Info
     1 0.000000   192.168.0.33   192.168.0.15   TCP       bgp > 2123 [FIN, PSH, ACK] Seq=0 Ack=0 Win=16101 Le
     2 0.000031   192.168.0.15   192.168.0.33   TCP       2123 > bgp [ACK] Seq=0 Ack=1 Win=32120 Len=0
     3 0.000422   192.168.0.15   192.168.0.33   TCP       2123 > bgp [FIN, ACK] Seq=0 Ack=1 Win=32120 Len=0
     4 0.006057   192.168.0.33   192.168.0.15   TCP       bgp > 2123 [ACK] Seq=1 Ack=1 Win=16101 Len=0
     5 7.999977   192.168.0.15   192.168.0.33   TCP       2124 > bgp [SYN] Seq=0 Len=0 MSS=1460 TSV=181687325
     6 8.003909   192.168.0.33   192.168.0.15   TCP       bgp > 2124 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 M
     7 8.003954   192.168.0.15   192.168.0.33   TCP       2124 > bgp [ACK] Seq=1 Ack=1 Win=32120 Len=0
     8 8.004042   192.168.0.15   192.168.0.33   BGP       OPEN Message
     9 8.208048   192.168.0.33   192.168.0.15   TCP       bgp > 2124 [ACK] Seq=1 Ack=30 Win=16355 Len=0
    10 8.337997   192.168.0.33   192.168.0.15   BGP       OPEN Message
    11 8.338027   192.168.0.15   192.1                    2124 > bgp [ACK] Seq=30 Ack=30 Win=32120 Len=0
    12 8.338115   192.168.0.15   192.1                    KEEPALIVE Message
    13 8.342206   192.168.0.33   192.168.0.15   BGP       KEEPALIVE Message
    14 8.349836   192.168.0.15   192.1                    2124 > bgp [ACK] Seq=49 Ack=49 Win=32120 Len=0
    15 8.544101   192.168.0.33   192.1                    bgp > 2124 [ACK] Seq=49 Ack=49 Win=16336 Len=0
    16 8.544149   192.168.0.15   192.168.0.33   BGP       KEEPALIVE Message, UPDATE Message, UPDATE Message
    17 8.549476   192.168.0.33   192.168.0.15   BGP       UPDATE Message
    18 8.559791   192.168.0.15   192.168.0.33   TCP       2124 > bgp [ACK] Seq=265 Ack=113 Win=32120 Len=0
    19 8.562733   192.168.0.33   192.168.0.15   BGP       KEEPALIVE Message
    20 8.579787   192.168.0.15   192.168.0.33   TCP       2124 > bgp [ACK] Seq=265 Ack=132 Win=32120 Len=0
```

```
⊞ Frame 4 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II,                                                      :0:4f:23:c5:95)
⊞ Internet Prot                                                     15)
⊞ Transmission                                                       Ack: 1, Len: 0
```

```
        00 c0 4f 23 c5 95 00 00  0c 35 0e 1c 08 00 45 c0   ..0#.... .5....E.
0010       28 00 09 00 00 ff 06  39 86 c0 a8 00 21 c0 a8   .(...... 9....!..
0020    00    00 b                                                     .WP.
0030    3e e5    2
```

File: "C:\Documents and Settings\Farid\My Documents\Software\wireshark\captures\ch... | P: 20 D: 20 M: 0


bgp_test.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
No. .  Time       Source         Destination    Protocol  Info
    1 0.000000   192.168.0.33   192.168.0.15   TCP       bgp > 2123 [FIN, PSH, ACK] Seq=0 Ack=0 Win=16101 Le
    2 0.000031   192.168.0.15   192.168.0.33   TCP       2123 > bgp [ACK] Seq=0 Ack=1 Win=32120 Len=0
    3 0.000422   192.168.0.15   192.168.0.33   TCP       2123 > bgp [FIN, ACK] Seq=0 Ack=1 Win=32120 Len=0
    4 0.006057   192.168.0.33   192.168.0.15   TCP       bgp > 2123 [ACK] Seq=1 Ack=1 Win=16101 Len=0
    5 7.999977   192.168.0.15   192.168.0.33   TCP       2124 > bgp [SYN] Seq=0 Len=0 MSS=1460 TSV=181687325
    6 8.003909   192.168.0.33   192.168.0.15   TCP       bgp > 2124 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 M
    7 8.003954   192.168.0.15   192.168.0.33   TCP       2124 > bgp [ACK] Seq=1 Ack=1 Win=32120 Len=0
    8 8.004042   192.168.0.15   192.168.0.33   BGP       OPEN Message
    9 8.208048   192.168.0.33   192.168.0.15   TCP       bgp > 2124 [ACK] Seq=1 Ack=30 Win=16355 Len=0
   10 8.337997   192.168.0.33   192.168.0.15   BGP       OPEN Message
```

```
⊟ Frame 8 (83 bytes on wire, 83 bytes captured)
    Arrival Time: Mar 30, 2000 00:56:56.957322000
    [Time delta from previous packet: 0.000088000 seconds]
    [Time since reference or first frame: 8.004042000 seconds]
    Frame Number: 8
    Packet Length: 83 bytes
    Capture Length: 83 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:ip:tcp:bgp]
    [Coloring Rule Name: Routing]
    [Coloring Rule String: hsrp || eigrp || ospf |              vrp || igmp || ismp]
⊞ Ethernet II, Src: DellComp_23:c5:95 (00:c0:4f:23              :1c (00:00:0c:35:0e:1c)
⊞ Internet Protocol, Src: 192.168.0.15 (192.168.0.             92.168.0.33)
⊞ Transmission Control Protocol, Src Port: 2124 (2             , Seq: 1, Ack: 1, Len: 29
⊞ Border Gateway Protocol
```

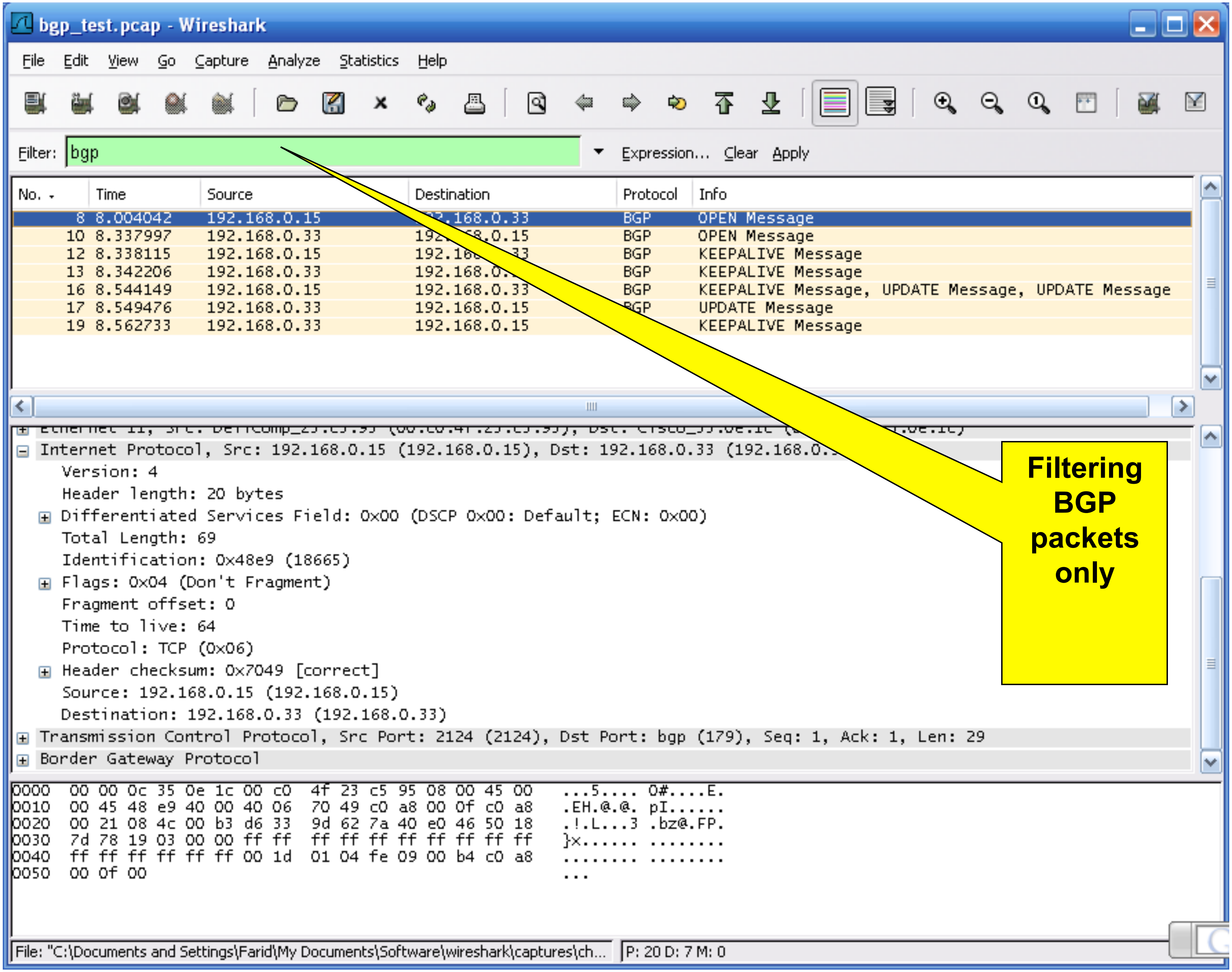
```
0000  00 00 0c 35 0e 1c 00 c0  4f 23 c5 95 08 00 45 00   ...5.... O#....E.
0010  00 45 48 e9 40 00 40 06  70 49 c0 a8 00 0f c0 a8   .
0020  00 21 08 4c 00 b3 d6 33  9d 62 7a 40 e0 46 50 18   .
0030  7d 78 19 03 00 00 ff ff  ff ff ff ff ff ff ff ff   }
0040  ff ff ff ff ff ff 00 1d  01 04 fe 09 00 b4 c0 a8   .
0050  00 0f 00                                           .
```

File: "C:\Documents and Settings\Farid\My Documents\Software\wireshark\captures\ch... P: 20 D: 20 M: 0

Packet number 8 – BGP (Boarder Gateway Prot)

Protocol Tree Window: Details of the selected packet (#8)

Raw data (content of packet # 8)



bgp_test.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: bgp
Expression... Clear Apply

```
No. .  Time      Source         Destination    Protocol  Info
    8 8.004042  192.168.0.15   2.168.0.33     BGP       OPEN Message
   10 8.337997  192.168.0.33   192.  8.0.15   BGP       OPEN Message
   12 8.338115  192.168.0.15   192.16    33   BGP       KEEPALIVE Message
   13 8.342206  192.168.0.33   192.168.0.     BGP       KEEPALIVE Message
   16 8.544149  192.168.0.15   192.168.0.33   BGP       KEEPALIVE Message, UPDATE Message, UPDATE Message
   17 8.549476  192.168.0.33   192.168.0.15   BGP       UPDATE Message
   19 8.562733  192.168.0.33   192.168.0.15             KEEPALIVE Message
```

```
⊞ Ethernet II, Src: DellComp_23:c5:95 (00:c0:4f:23:c5:95), Dst: Cisco_35:0e:1c (0   :0e:1c)
⊟ Internet Protocol, Src: 192.168.0.15 (192.168.0.15), Dst: 192.168.0.33 (192.168.0.
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 69
    Identification: 0x48e9 (18665)
  ⊞ Flags: 0x04 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
  ⊞ Header checksum: 0x7049 [correct]
    Source: 192.168.0.15 (192.168.0.15)
    Destination: 192.168.0.33 (192.168.0.33)
⊞ Transmission Control Protocol, Src Port: 2124 (2124), Dst Port: bgp (179), Seq: 1, Ack: 1, Len: 29
⊞ Border Gateway Protocol
```

```
0000  00 00 0c 35 0e 1c c0  4f 23 c5 95 08 00 45 00   ...5.... O#....E.
0010  00 45 48 e9 40 00 40 06  70 49 c0 a8 00 0f c0 a8   .EH.@.@. pI......
0020  00 21 08 4c 00 b3 d6 33  9d 62 7a 40 e0 46 50 18   .!.L...3 .bz@.FP.
0030  7d 78 19 03 00 00 ff ff  ff ff ff ff ff ff ff ff   }x...... ........
0040  ff ff ff ff ff ff 00 1d  01 04 fe 09 00 b4 c0 a8   ........ ........
0050  00 0f 00                                            ...
```

File: "C:\Documents and Settings\Farid\My Documents\Software\wireshark\captures\ch... P: 20 D: 7 M: 0

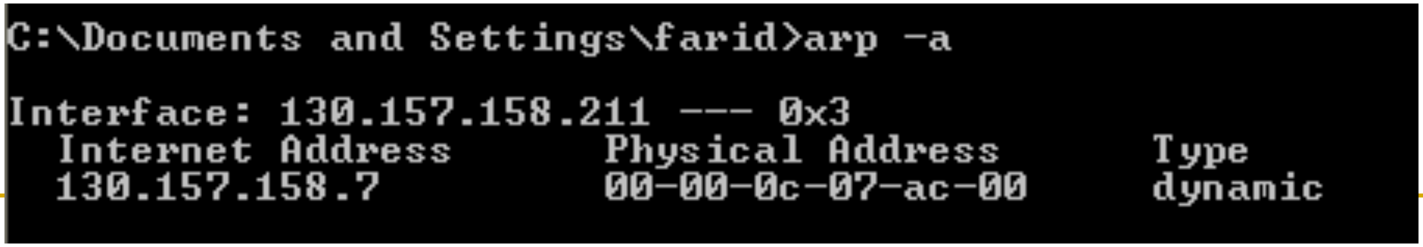
Filtering BGP packets only

We continue in the lab….

- Download the following files and copy them in your HW:
  - `bgp_test`
  - `tcp_stream_analysis`
  - `follow_tcp_stream`

Remember….

- Protocols are standard for communications
- Ethernet is the most popular protocol standard to enable computer communication
  - Based on shared medium and broadcasting
- Ethernet address is called MAC address
  - 48 bit HW address coded in the RON of the NIC card
  - The first 12 bits represent the vender
  - The second 12 bits represent the serial number
  - Use: `arp -a`
- Remember: IP address is logical addressing
  - Network layer is in charge of routing
  - Use: `ipconfig`



```
C:\Documents and Settings\farid>arp -a

Interface: 130.157.158.211 --- 0x3
  Internet Address      Physical Address      Type
  130.157.158.7         00-00-0c-07-ac-00     dynamic
```