Network Traffic Analysis

Marcelle Lee
@marcellelee
October 21, 2017

About me...

- Threat Researcher, LookingGlass Cyber Solutions, Inc.
- Co-founder and CEO, Fractal Security Group, LLC
- Adjunct faculty
- Compulsive volunteer - WSC, ISACA, ISSA, NIST, to name a few…
- Certs: CSX-P, GCIA, GPEN, CCNA, blah blah blah
- CTF enthusiast

Workshop Materials...

http://ow.ly/6D1Q30fURKV

Why We Look at Packets

- Troubleshooting
- Detection of badness
- Post-mortem forensics

How We Look at Packets (for free)

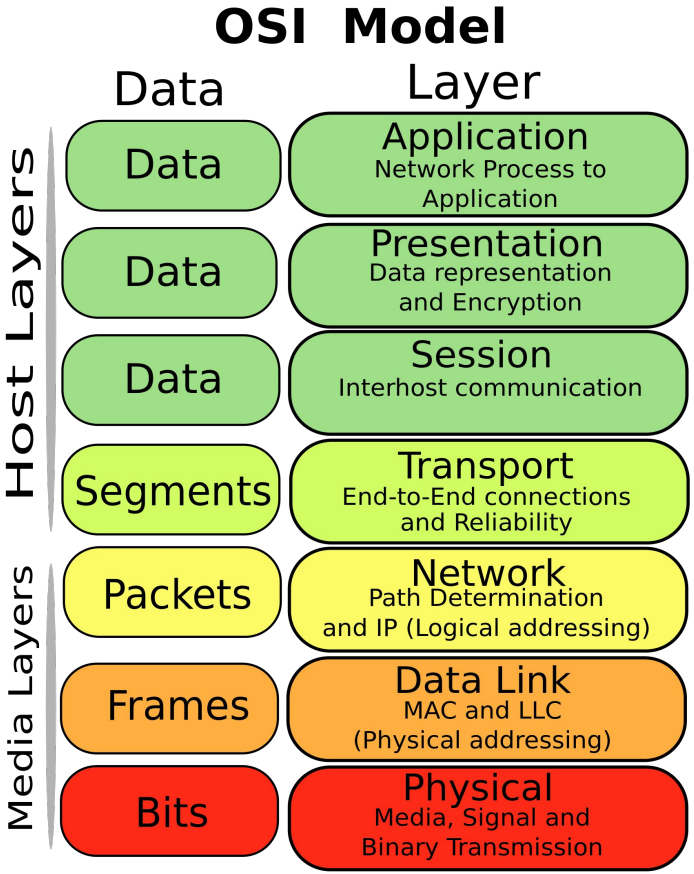
Network Traffic Models

OSI MODEL

VS

TCP/IP Stack

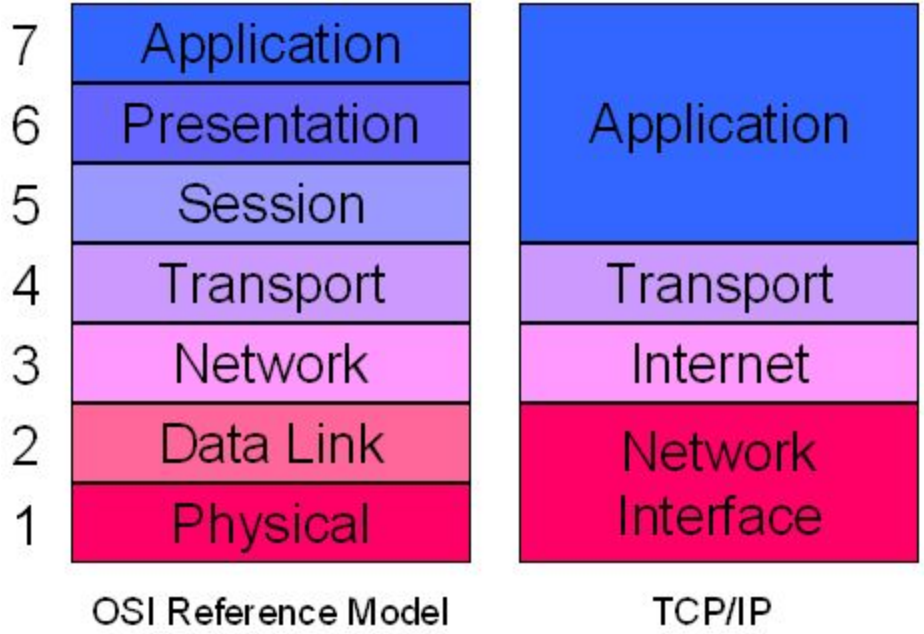
OSI Model


OSI Model
Data
Layer
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data representation and Encryption
Data
Session
Interhost communication
Segments
Transport
End-to-End connections and Reliability
Packets
Network
Path Determination and IP (Logical addressing)
Frames
Data Link
MAC and LLC (Physical addressing)
Bits
Physical
Media, Signal and Binary Transmission

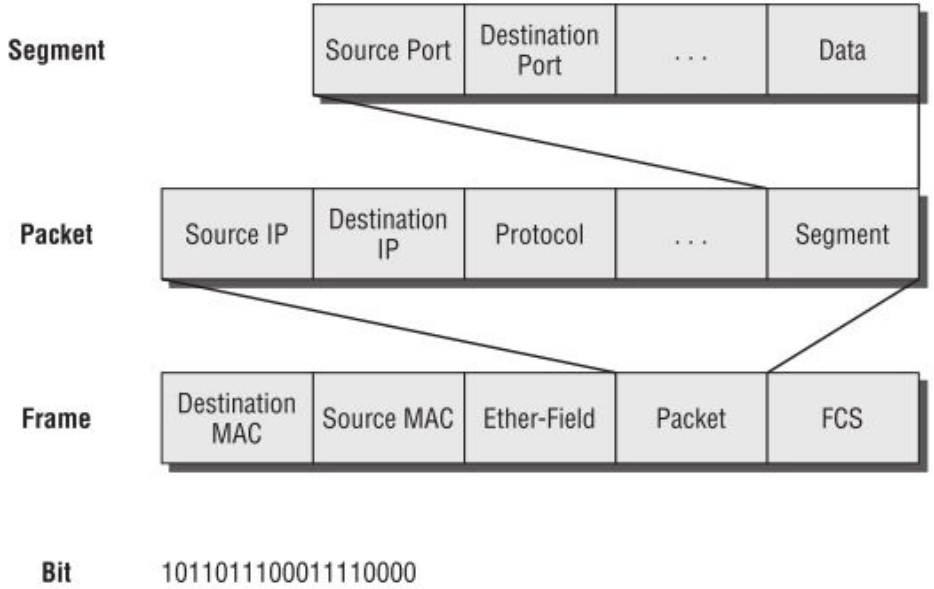
TCP/IP Stack

Application Layer
Transport Layer
Internet Layer
Network Access Layer

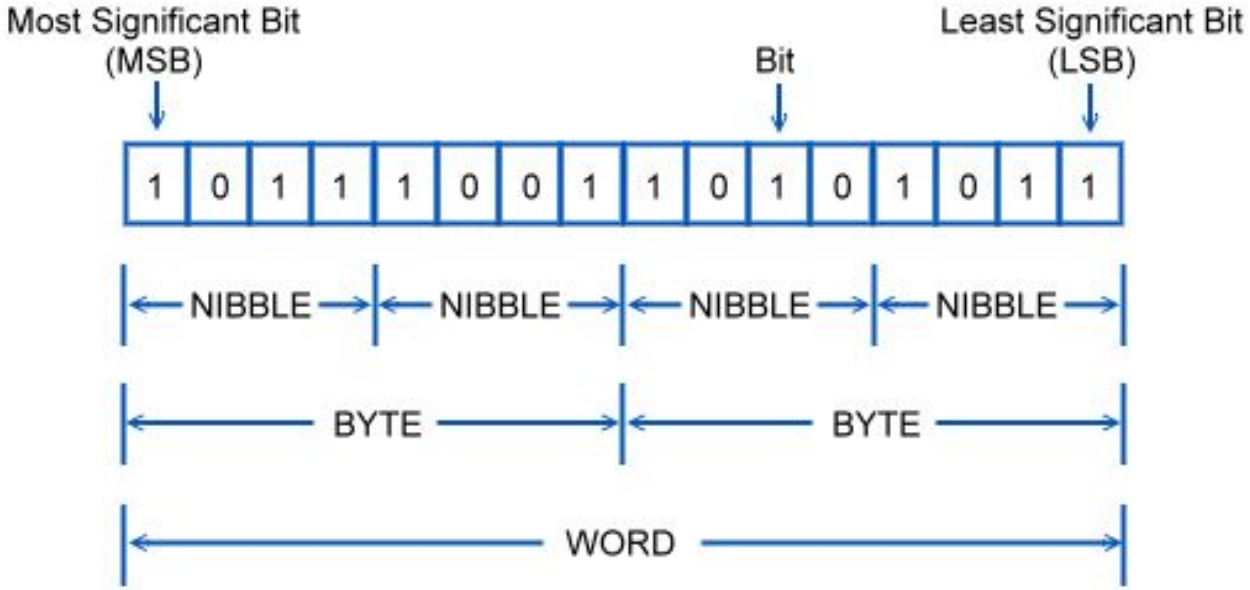
OSI Model vs TCP/IP Stack



Structure (we call everything packets)



Bits & Bytes


Most Significant Bit
(MSB)
Bit
Least Significant Bit
(LSB)
1 0 1 1 1 0 0 1 1 0 1 0 1 0 1 1
NIBBLE
NIBBLE
NIBBLE
NIBBLE
BYTE
BYTE
WORD

ASCII-Decimal-Binary-Hex

ASCII	Decimal (base10)	Binary (base2)	Hexadecimal (base 16)
a	97	0110 0001	61
b	98	0110 0010	62
c	99	0110 0011	63
d	100	0110 0100	64

Application Layer

chrome

REQUEST

Feedback

What is packet? - Definition from WhatIs.com - SearchNetworking
searchnetworking.techtarget.com › Network Administration › Network software
A **packet** is the unit of data that is routed between an origin and a destination on the Internet or any other **packet**-switched network.

Network packet - Wikipedia
https://en.wikipedia.org/wiki/Network_packet
A network **packet** is a formatted unit of data carried by a **packet**-switched network. When data is formatted into **packets**, and **packet** switching is employed, the bandwidth of the communication medium can be better shared among users than with circuit switching.
Terminology · Packet framing · Example: IP packets · Example: Radio and TV ...

What is a network packet? | HowStuffWorks
computer.howstuffworks.com › Tech › Computer › Computer Hardware › Networking
It turns out that everything you do on the Internet involves **packets**. For example, every Web page that you receive comes as a series of **packets**, and every e-mail ...

What Is a Data Packet? - Lifewire
https://www.lifewire.com › How To › Internet & Network › Tips & Tricks
Sep 1, 2017 - A data **packet** is a basic block that carries our data over a digital network. Data is broken down into the **packet** before transmission and ...

RESPONSE

Application Layer: Secure vs Insecure Protocols

Secure	Insecure
HTTPS	HTTP
SSH	FTP
SFTP	Telnet

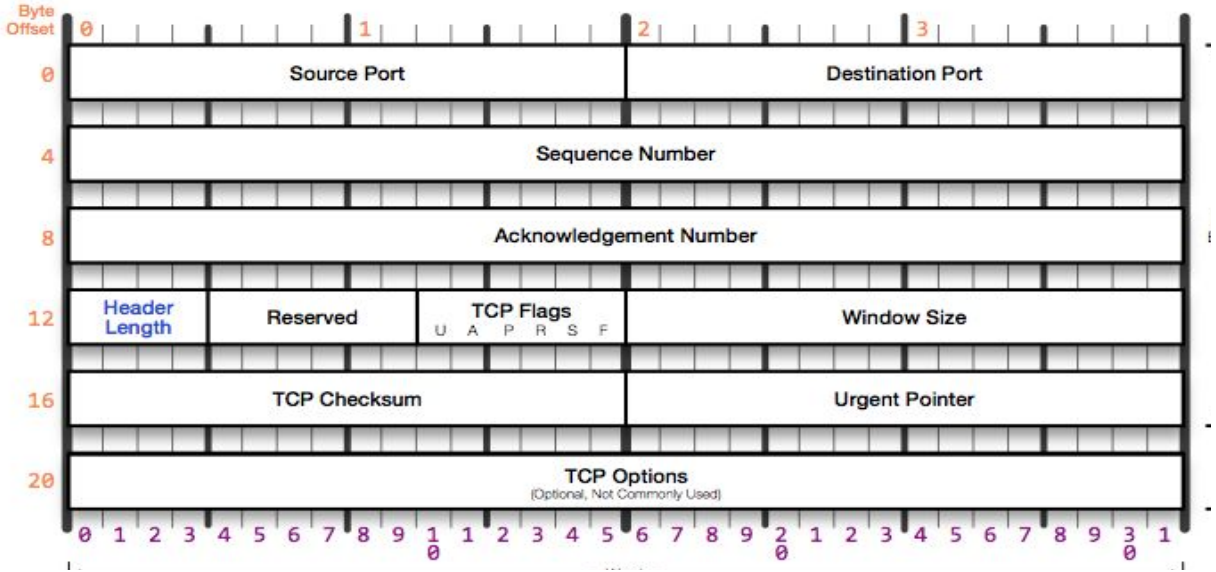
telnet-cooked.pcap

Transport Layer

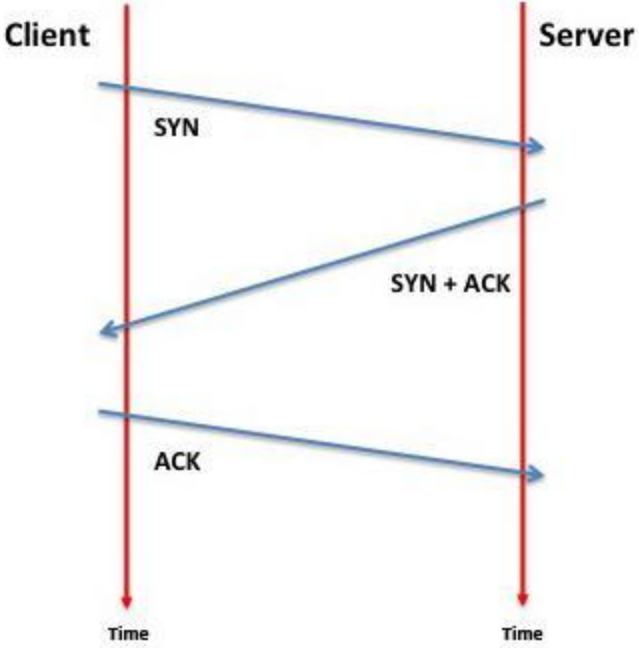
UDP – “send it and forget it”

TCP – “text me when you get home safely”

Transport Layer: TCP Header

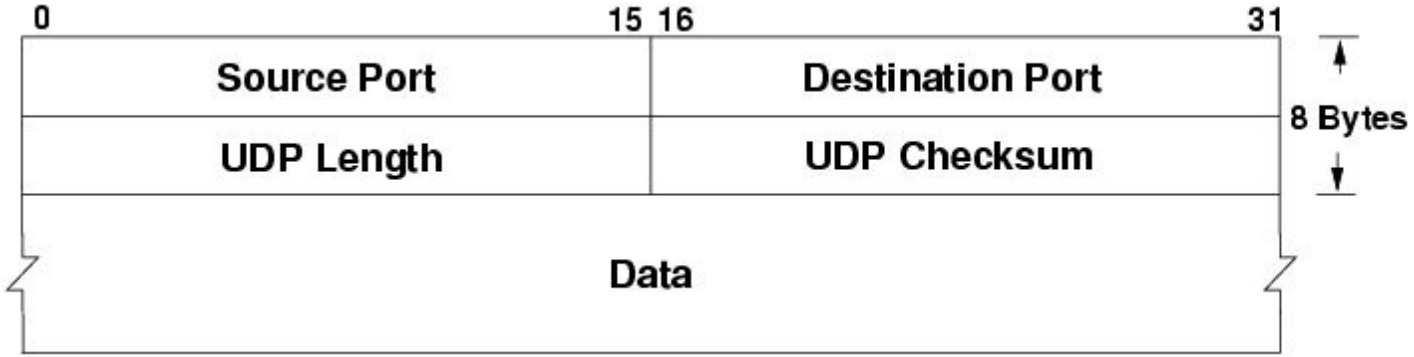


Transport Layer: TCP 3-Way Handshake



find the 3-way handshake

Transport Layer: UDP Header



Transport Layer: Ports & Service

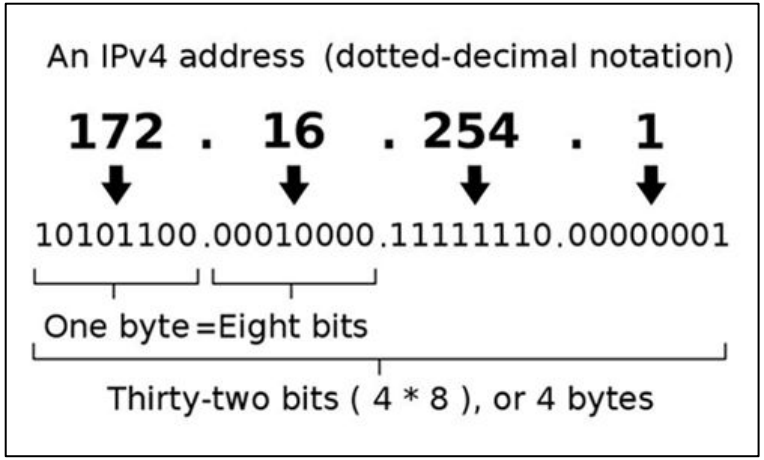
Common Ports

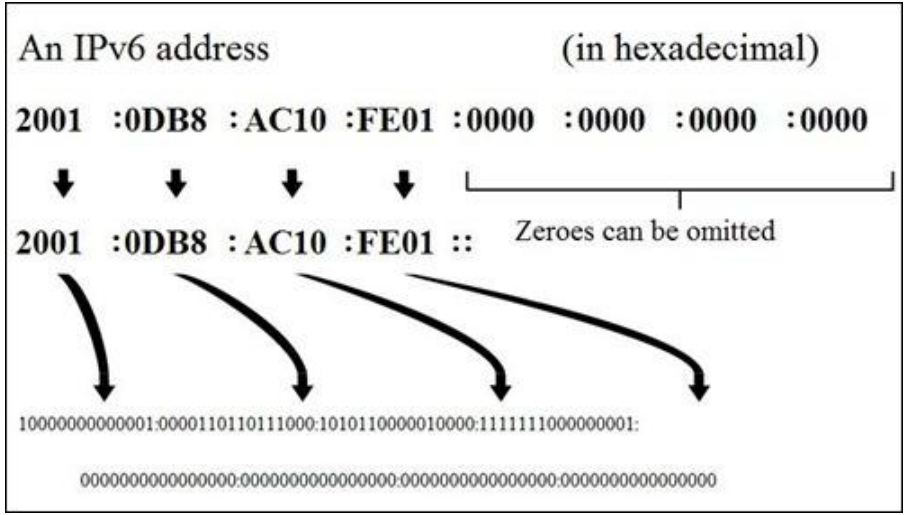
packetlife.net

TCP/UDP Port Numbers

7	Echo	554	RTSP	2745	Bagle.H	6891-6901	Windows Live
19	Chargen	546-547	DHCPv6	2967	Symantec AV	6970	Quicktime
20-21	FTP	560	rmonitor	3050	Interbase DB	7212	GhostSurf
22	SSH/SCP	563	NNTP over SSL	3074	XBOX Live	7648-7649	CU-SeeMe
23	Telnet	587	SMTP	3124	HTTP Proxy	8000	Internet Radio
25	SMTP	591	FileMaker	3127	MyDoom	8080	HTTP Proxy
42	WINS Replication	593	Microsoft DCOM	3128	HTTP Proxy	8086-8087	Kaspersky AV
43	WHOIS	631	Internet Printing	3222	GLBP	8118	Privoxy
49	TACACS	636	LDAP over SSL	3260	iSCSI Target	8200	VMware Server
53	DNS	639	MSDP (PIM)	3306	MySQL	8500	Adobe ColdFusion
67-68	DHCP/BOOTP	646	LDP (MPLS)	3389	Terminal Server	8767	TeamSpeak
69	TFTP	691	MS Exchange	3689	iTunes	8866	Bagle.B
70	Gopher	860	iSCSI	3690	Subversion	9100	HP JetDirect
79	Finger	873	rsync	3724	World of Warcraft	9101-9103	Bacula

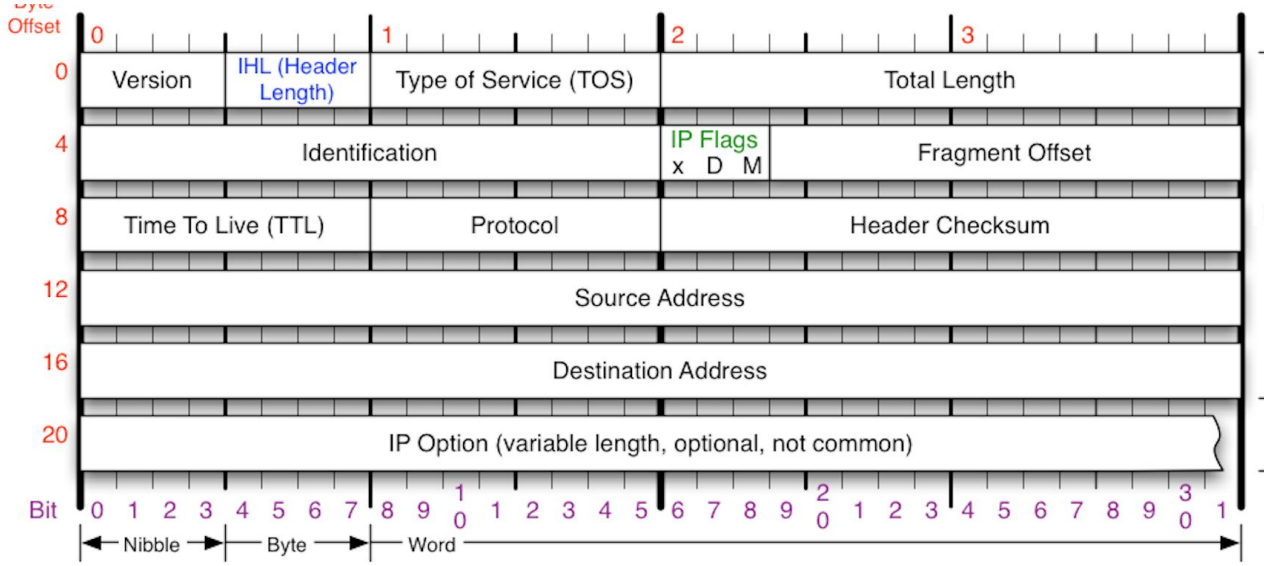
Internet Layer: IPv4 vs IPv6



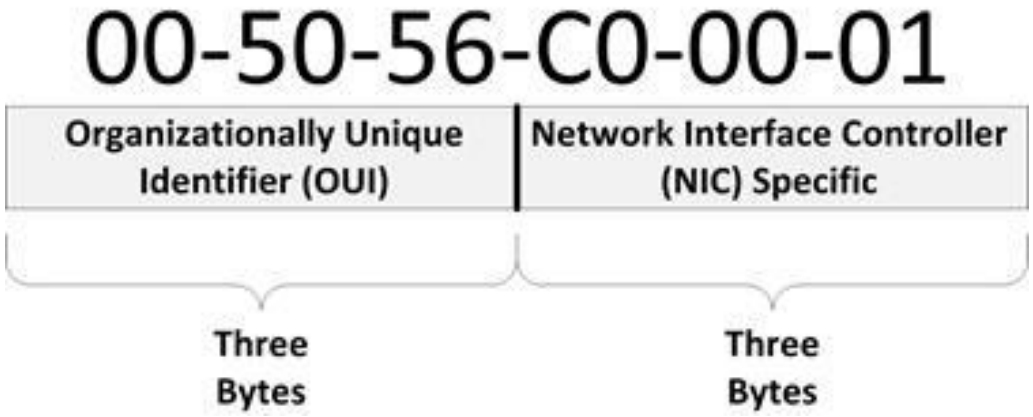


Internet Layer: IP Header

RFC 3514
The Security Flag in the IPv4 Header
1 April 2003



Network Access Layer: MAC Address



Network Access Layer: Network Interfaces

What interfaces do you have available?

Windows: ipconfig /all

Linux/Mac: ifconfig -a

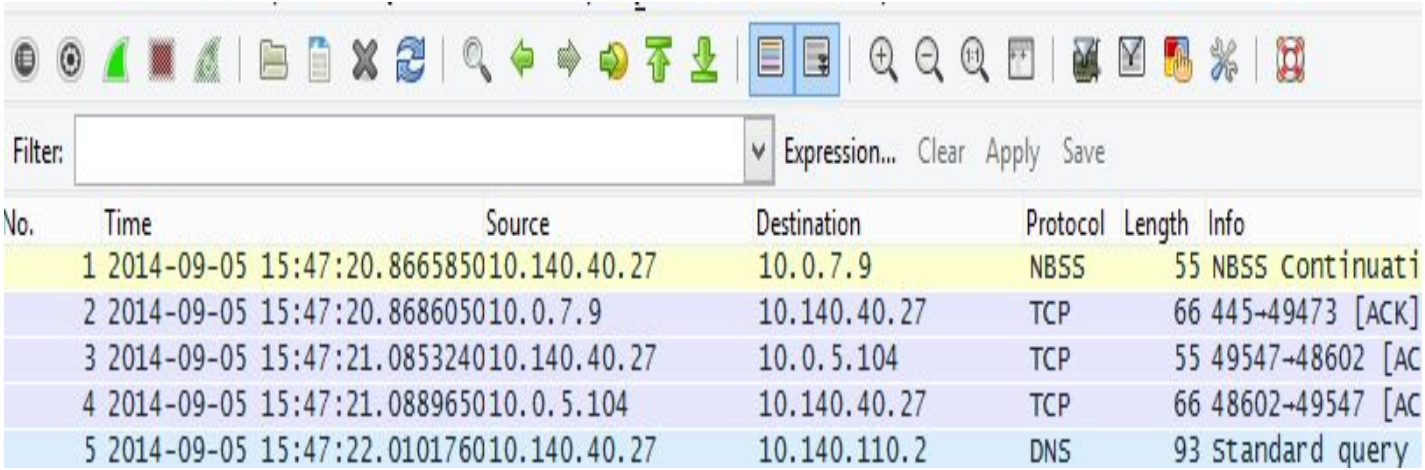
```
        nd6 options=1<PERFORMNUD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether 6c:40:08:ba:f4:04
        inet6 fe80::6e40:8ff:feba:f404%en0 prefixlen 64 scopeid 0x4
        inet 192.168.1.16 netmask 0xffffff00 broadcast 192.168.1.255
        nd6 options=1<PERFORMNUD>
        media: autoselect
        status: active
en1: flags=963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX> mtu 1500
        options=60<TSO4,TSO6>
        ether 72:00:07:26:f4:60
        media: autoselect <full-duplex>
        status: inactive
en2: flags=963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX> mtu 1500
        options=60<TSO4,TSO6>
        ether 72:00:07:26:f4:61
        media: autoselect <full-duplex>
```

identify your IP address and interface

Create Your Own Capture

- Select interface and start your capture
- Perform some activities to generate traffic
  - Browse the Internet
  - Ping an IP address or domain
  - Do a DNS lookup for an IP address or domain (command is nslookup)
- Stop the capture

Capture Review: Packet List Pane



Capture Review: Packet Details Pane

```
⊞ Frame 3092: 182 bytes on wire (1456 bits), 182 bytes captured (1456 bits) on interface 0
⊞ Ethernet II, Src: 20:b3:99:54:35:5c (20:b3:99:54:35:5c), Dst: 5c:f9:dd:75:21:34 (5c:f9:dd:75:21:34)
⊞ Internet Protocol Version 4, Src: 10.140.110.2 (10.140.110.2), Dst: 10.140.40.27 (10.140.40.27)
⊞ Transmission Control Protocol, Src Port: 445 (445), Dst Port: 55136 (55136), Seq: 25143, Ack: 16402, Len: 1
⊞ NetBIOS Session Service
⊞ SMB2 (Server Message Block Protocol version 2)
```

Capture Review: Packet Bytes Pane

```
0000  5c f9 dd 75 21 34 20 b3  99 54 35 5c 08 00 45 00   \..u!4 . .T5\..E.
0010  00 a8 0e e9 40 00 7f 06  41 32 0a 8c 6e 02 0a 8c   ....@... A2..n...
0020  28 1b 01 bd d7 60 ab f7  2a f1 08 e8 b5 28 50 18   (....`.. *....(P.
0030  01 fc b5 5c 00 00 00 00  00 7c fe 53 4d 42 40 00   ...\.... .|.SMB@.
0040  01 00 00 00 00 00 06 00  01 00 01 00 00 00 00 00   ........ ........
0050  00 00 49 00 00 00 00 00  00 00 ff fe 00 00 01 00   ..I..... ........
0060  00 00 2d 00 00 64 1f 04  00 00 00 00 00 00 00 00   ..-..d.. ........
0070  00 00 00 00 00 00 00 00  00 00 3c 00 01 00 00 00   ........ ..<.....
0080  00 00 d7 09 56 3c 7e 72  ce 01 11 75 93 76 26 8e   ....V<~r ...u.v&.
0090  ce 01 11 75 93 76 26 8e  ce 01 11 75 93 76 26 8e   ...u.v&. ...u.v&.
00a0  ce 01 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 30 00 00 00                                  ..0...
```

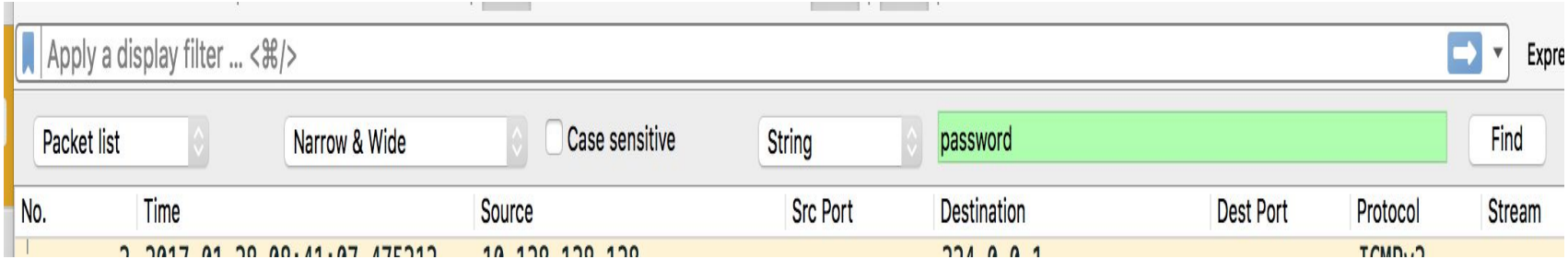
Capture Analysis: Statistics

- Statistics > Summary – overall summary of the packet capture
- Statistics > Protocol Hierarchy – breakdown of the various protocols
- Statistics > Conversations – list of each individual “conversation” between endpoints
- Statistics > Endpoints – list of source and destination addresses

Capture Analysis: Follow Streams

- Select a packet of interest and go to Analyze > Follow TCP Stream (or Follow UDP stream) – what can you see in the output?
- How would this output be useful in investigating an incident?
- What other types of information could be obtained?

Capture Analysis: Find



Capture Analysis: Filters

Filtering is a powerful tool in Wireshark. There are multiple ways to create filters, including:

- Type in the filter window using the correct terminology and operators to find the desired data. For example, typing ip.proto == 17 and ip.addr == 192.168.1.13 in the filter window will show you all UDP traffic associated with address 192.168.1.13.
- Right-click on any packet and select “Apply as Filter.”

Capture Analysis: Your Capture

Find the following in your capture:

- TCP handshake
- At least four different protocols
- What websites were visited?
- What address was pinged? Was it successful?

acunetix.pcap

- What is the email address of the registrant? (Hint: use this site to decipher text http://www.urldecoder.org/.)

hotel.pcap

- What is the name of the hotel?
- What type of computer is the guest using?

travel.pcap

- What type of travel is this?
- What is the name of the travel service?
- Were there any stops?
- What was the email address of the traveler?
- Who were some of the other travelers?

offshore.pcap

- What location was the subject of this capture?
- Who was doing the research on the location?
- What place did they claim to love?

iot.pcap

- What type of device is it?
- Who is the manufacturer? What is the model?
- What services are running?
- What are the device credentials?

video.pcap

- Find the downloaded video.
- Extract and play on your host.

injection.pcap

- What was the attacker IP?
- What was the target IP?
- What type of injection was used?
- What was the attacker able to accomplish?
- Hint - use http://www.urldecoder.org/

webshell.pcap

- What was the attacker IP?
- What was the target IP?
- How did the attacker access the target?
- What did the attacker do while on the system?

rogue_user.pcap

- A user was created - what was the user name?
- What level of privilege ~~did they have?~~ did the attacker have?

evil.pcap

- What was the attacker IP?
- What was the target IP and OS?
- What did the attacker learn about open ports on the target?
- Was there exfil? If so, what was it?
- Was there anything sent to the target?

Contact Info

@marcellelee

mlee@lookingglasscyber.com