Detecting Evil with Network Traffic Analysis

Marcelle, Mari, and Joy
4 May 2018

Workshop Materials...

https://goo.gl/GQxvic

Wireshark

About Marcelle...

- Threat Researcher, LookingGlass Cyber Solutions, Inc.
- Co-founder and CEO, Fractal Security Group, LLC
- Adjunct faculty
- Champion of diversity in tech
- CTF enthusiast
- Compulsive volunteer

About Mari...

- Cyber Engineer, Large Casino in Las Vegas
- COO & Founding Board Member for Women’s Society of Cyberjutsu
- Aspiring author and speaker
- Avid traveler
- Arts and crafts fanatic

About Joy...

- Veteran
- Gamer, Sony/Nintendo/Arcade
- Founder, Defender Academy
- Foster Kid
- N00b Impostor

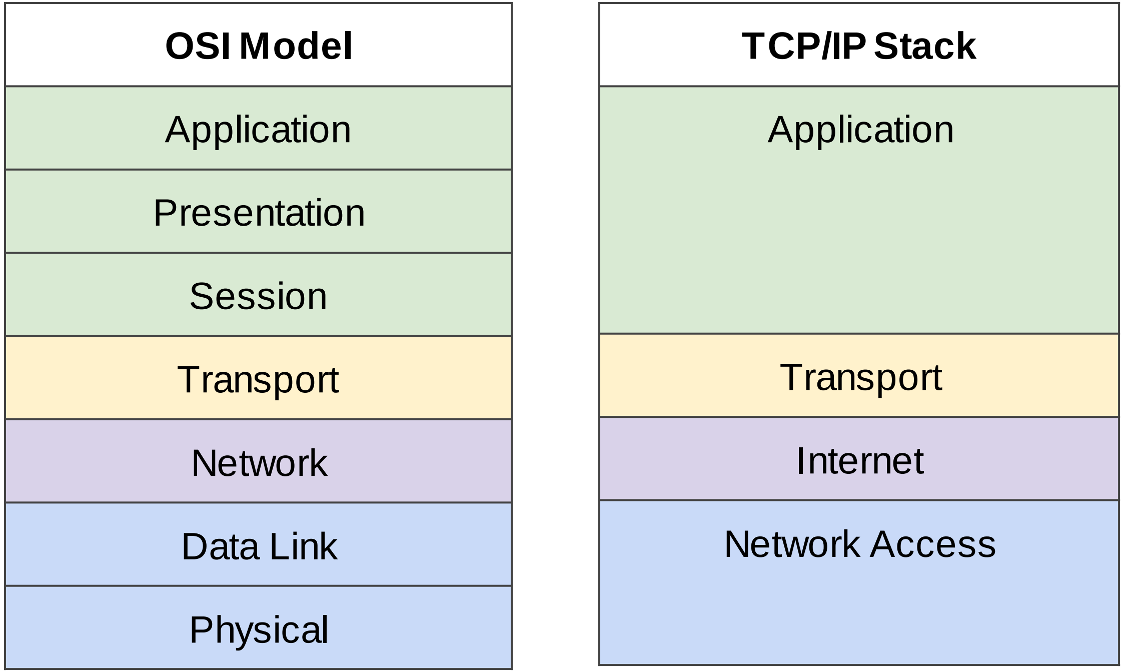
Why We Look at Packets

- Troubleshooting
- Detection of badness
- Post-mortem forensics

How We Look at Packets (for free)

Networking Fundamentals

Network Models



OSI Model

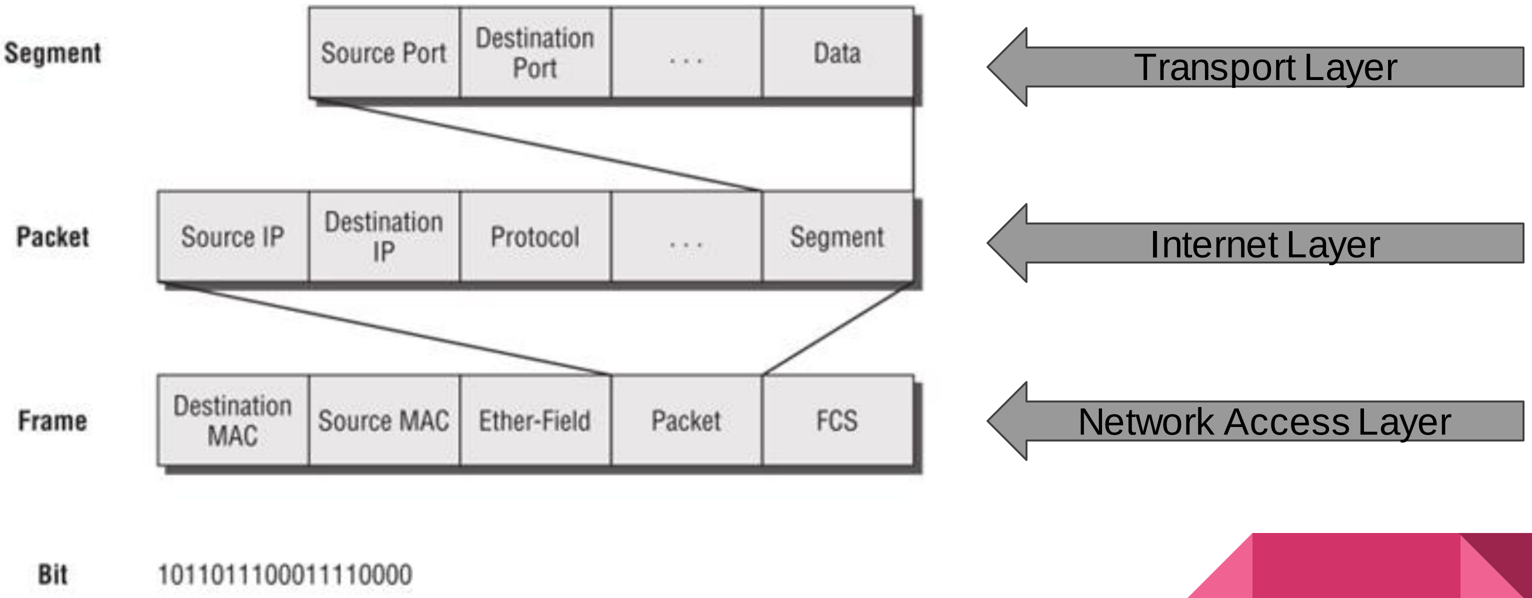
- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

TCP/IP Stack

- Application
- Transport
- Internet
- Network Access

See detailed model explanation in your resource material.

Encapsulation by Layers and PDU



Segment		Source Port	Destination Port	. . .	Data	Transport Layer
Packet	Source IP	Destination IP	Protocol	. . .	Segment	Internet Layer
Frame	Destination MAC	Source MAC	Ether-Field	Packet	FCS	Network Access Layer
Bit	1011011100011110000					

Protocols

Protocols define how network communications work. These are standards that are developed by the Internet Engineering Task Force (IETF) and are conveyed to the public via Requests for Comment (RFC).

Common protocols:

- Internet Control Message Protocol (ICMP)
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)

Ports & Services

Services are what we call the various types of network communications. Port numbers identify those services.

Port number assignment is managed by the Internet Assigned Numbers Authority (IANA).

- 0-1023 are well-known ports
- 1024-49151 are registered ports
- 49152-65535 are public ports

See port number reference sheet in your resource material.

Network Addressing

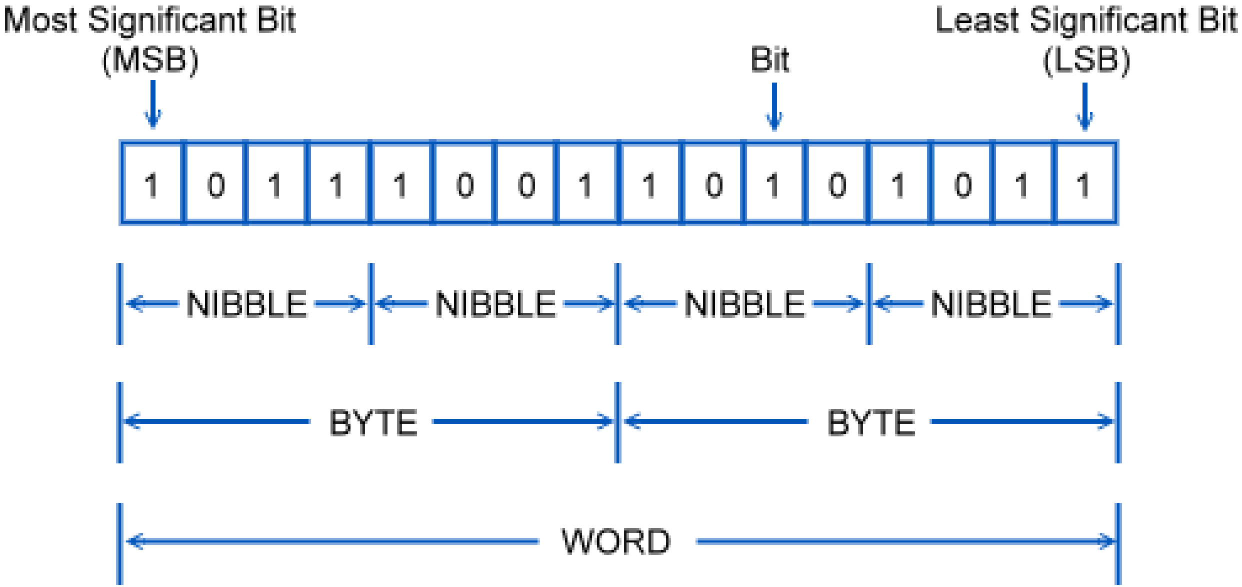
Internet Protocol (IP) addresses, used for inter-network communications:

- IPv4 - 32-bit address space represented in dotted decimal, e.g. 176.54.22.19
- IPv6 - 128-bit address space represented in hexadecimal, e.g. 2001:cdba:0000:0000:0000:0000:3257:9652

Media Access Control (MAC) addresses, used for intra-network communications:

- Network card address - 48-bit space represented in hexadecimal

Bits & Bytes

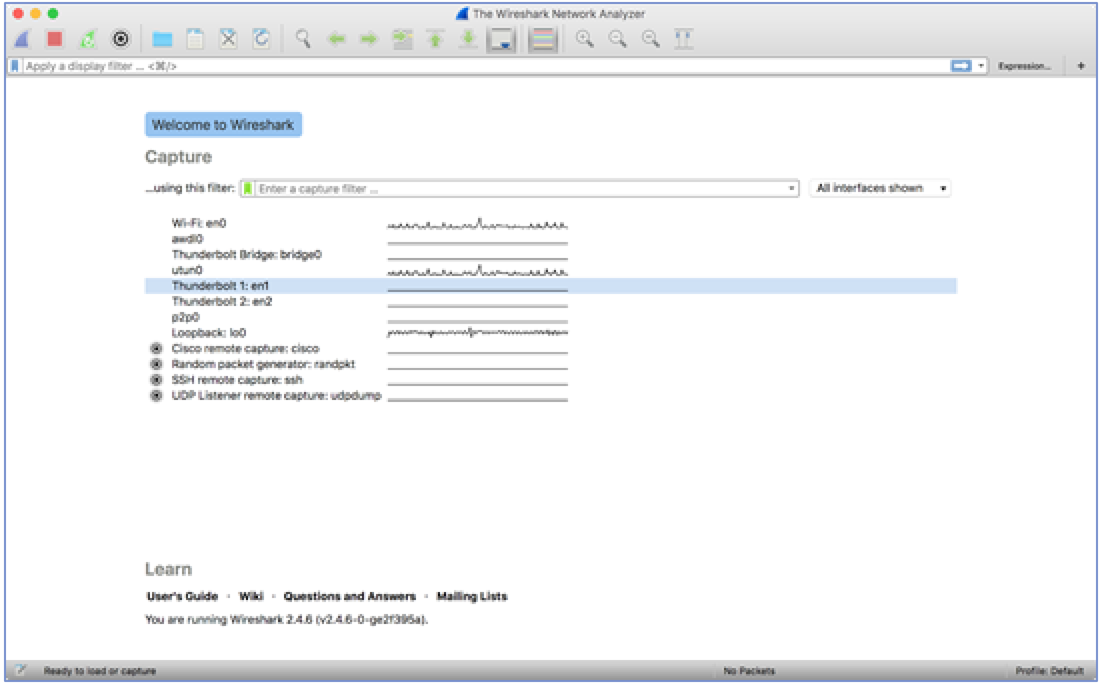

Most Significant Bit
(MSB)
Bit
Least Significant Bit
(LSB)
1 0 1 1 1 0 0 1 1 0 1 0 1 0 1 1
NIBBLE
NIBBLE
NIBBLE
NIBBLE
BYTE
BYTE
WORD

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

Getting Started with Wireshark

Activity: Getting to Know Wireshark

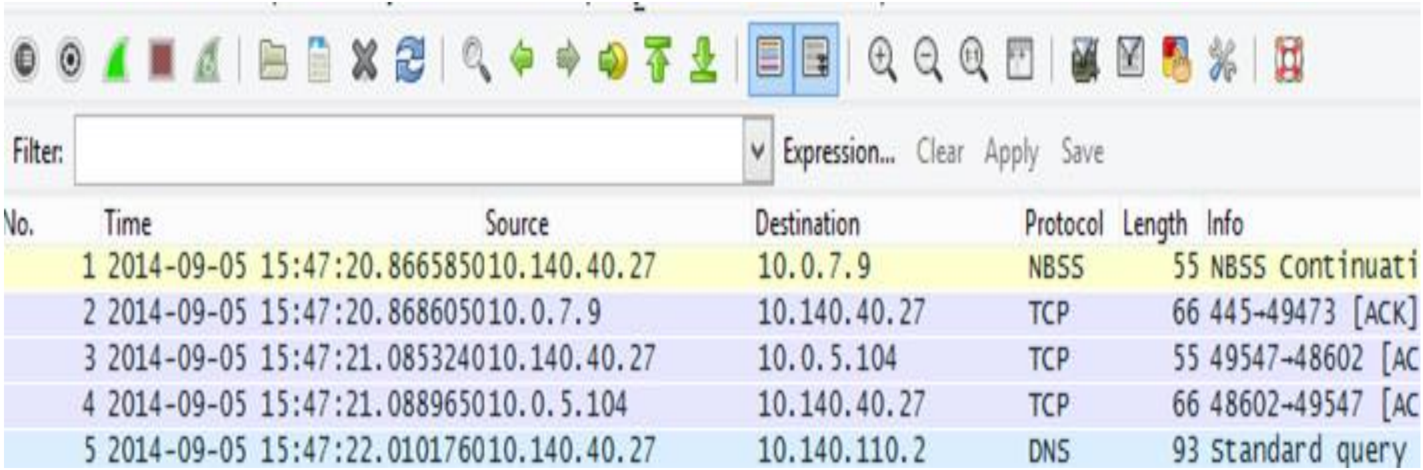

The Wireshark Network Analyzer
Apply a display filter ... <⌘/>
Expression...
+
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Wi-Fi: en0
awdl0
Thunderbolt Bridge: bridge0
utun0
Thunderbolt 1: en1
Thunderbolt 2: en2
p2p0
Loopback: lo0
Cisco remote capture: cisco
Random packet generator: randpkt
SSH remote capture: ssh
UDP Listener remote capture: udpdump
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
No Packets
Profile: Default

You are running Wireshark 2.4.6 (v2.4.6-0-ge2f395a).

Ready to load or capture

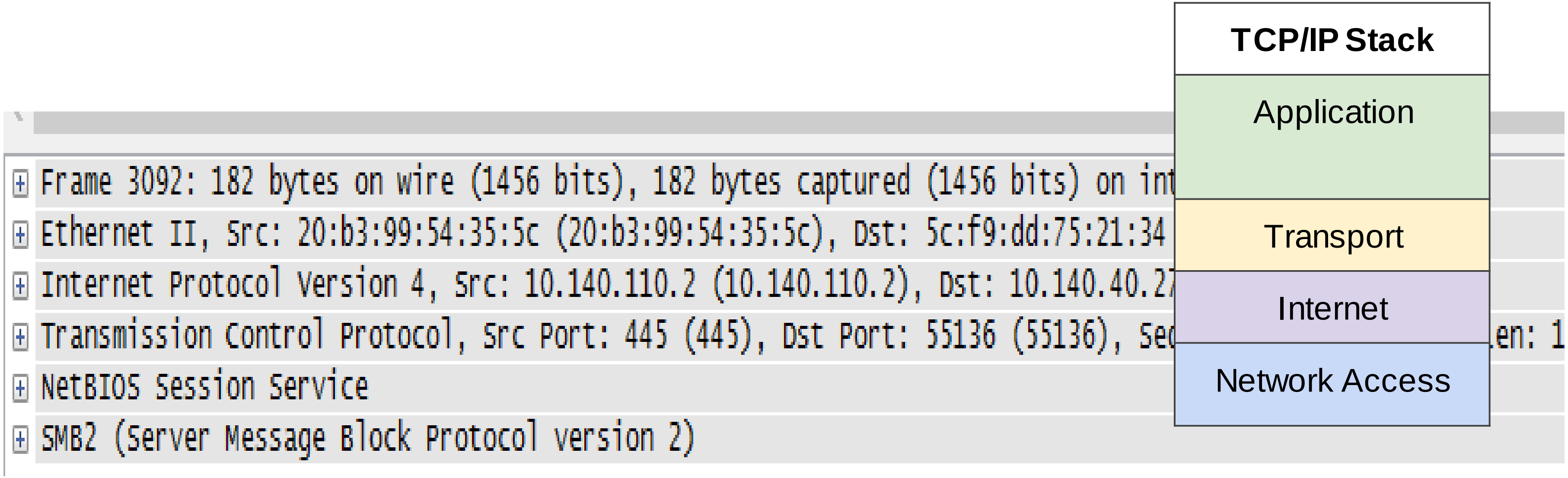
Launch Wireshark and open intro.pcap. Follow the prompts for activities in the next slides.

Packet List Pane



```
No.    Time                             Source         Destination    Protocol  Length  Info
     1 2014-09-05 15:47:20.866585010.140.40.27         10.0.7.9       NBSS          55 NBSS Continuati
     2 2014-09-05 15:47:20.868605010.0.7.9             10.140.40.27   TCP           66 445→49473 [ACK]
     3 2014-09-05 15:47:21.085324010.140.40.27         10.0.5.104     TCP           55 49547→48602 [AC
     4 2014-09-05 15:47:21.088965010.0.5.104           10.140.40.27   TCP           66 48602→49547 [AC
     5 2014-09-05 15:47:22.010176010.140.40.27         10.140.110.2   DNS           93 Standard query
```

Packet Details Pane



```
+ Frame 3092: 182 bytes on wire (1456 bits), 182 bytes captured (1456 bits) on int
+ Ethernet II, Src: 20:b3:99:54:35:5c (20:b3:99:54:35:5c), Dst: 5c:f9:dd:75:21:34
+ Internet Protocol Version 4, Src: 10.140.110.2 (10.140.110.2), Dst: 10.140.40.27
+ Transmission Control Protocol, Src Port: 445 (445), Dst Port: 55136 (55136), Sec                    .en: 1
+ NetBIOS Session Service
+ SMB2 (Server Message Block Protocol version 2)
```

TCP/IP Stack

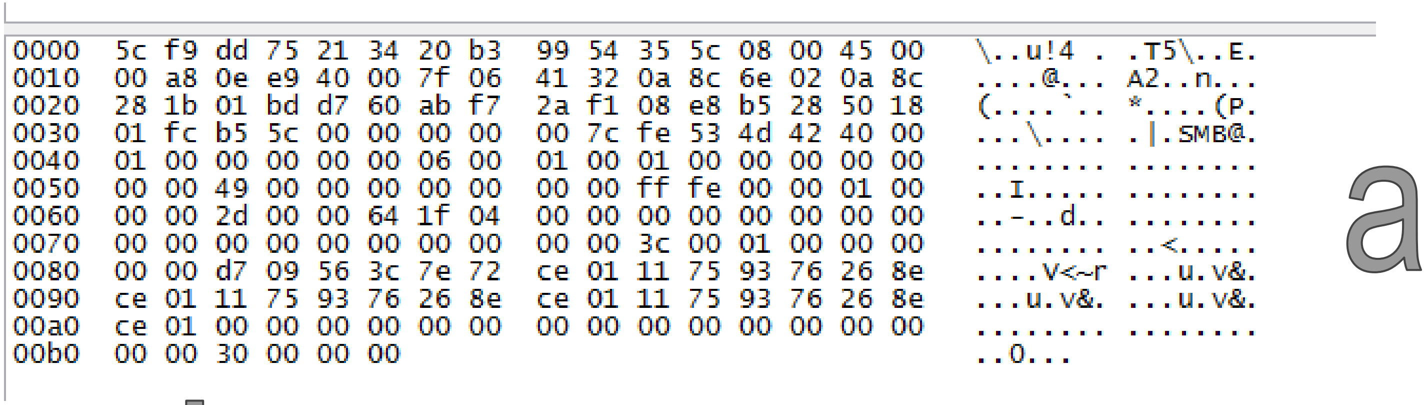
Application

Transport

Internet

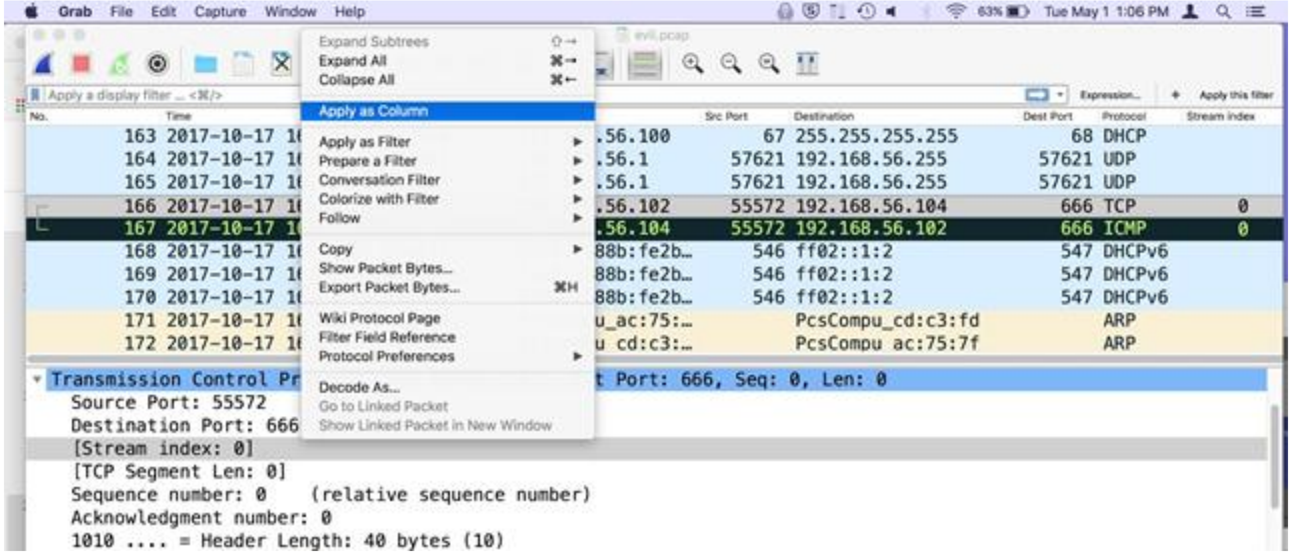
Network Access

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...
```

Customizing Columns



```
No.         Time                       Src Port  Destination        Dest Port  Protocol  Stream index
      163 2017-10-17 1(  .56.100           67 255.255.255.255        68 DHCP
      164 2017-10-17 1(  .56.1          57621 192.168.56.255      57621 UDP
      165 2017-10-17 1(  .56.1          57621 192.168.56.255      57621 UDP
      166 2017-10-17 1(  .56.102        55572 192.168.56.104        666 TCP              0
      167 2017-10-17 1(  .56.104        55572 192.168.56.102        666 ICMP             0
      168 2017-10-17 1(  88b:fe2b…        546 ff02::1:2             547 DHCPv6
      169 2017-10-17 1(  88b:fe2b…        546 ff02::1:2             547 DHCPv6
      170 2017-10-17 1(  88b:fe2b…        546 ff02::1:2             547 DHCPv6
      171 2017-10-17 1(  u_ac:75:…            PcsCompu_cd:c3:fd         ARP
      172 2017-10-17 1(  u cd:c3:…            PcsCompu ac:75:7f         ARP
```

```
▾ Transmission Control Pr                t Port: 666, Seq: 0, Len: 0
    Source Port: 55572
    Destination Port: 666
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 0
    1010 .... = Header Length: 40 bytes (10)
```

Right-click on desired field in selected frame and choose “Apply as Column”.

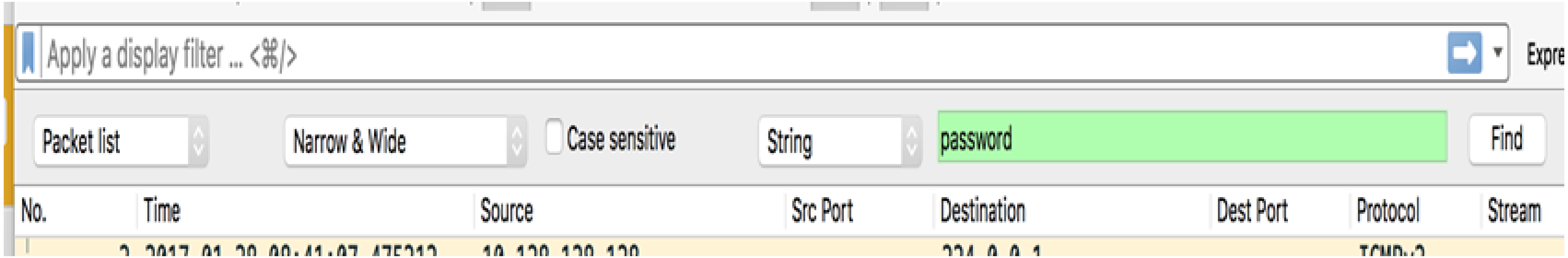
Capture Analysis: Statistics

- 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: Following 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



Apply a display filter ... <⌘/>

Packet list | Narrow & Wide | □ Case sensitive | String | password | Find

No. | Time | Source | Src Port | Destination | Dest Port | Protocol | Stream

Capture Analysis: Filters

See filter reference sheet in your resource material.

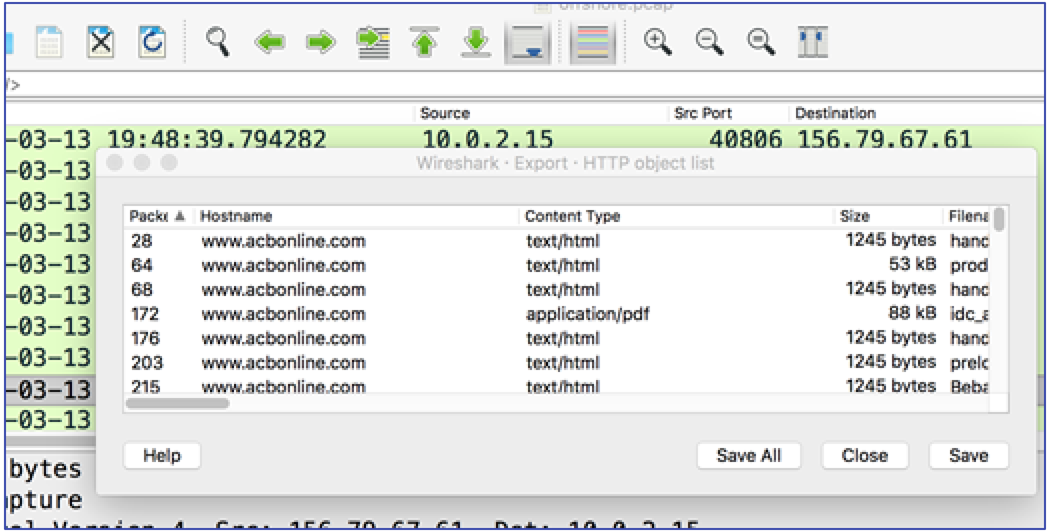
Filtering is a powerful tool in Wireshark. There are multiple ways to create filters, including:

- 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 detail and select “Apply as Filter.”

Capture Analysis: Export Objects

Exporting objects is file recovery without file carving.

File > Export Objects > HTTP (or other service as appropriate)



```
                                Source                Src Port  Destination
-03-13 19:48:39.794282          10.0.2.15                40806  156.79.67.61
-03-13
-03-13
-03-13
-03-13
-03-13
-03-13
-03-13
-03-13
-03-13
bytes
pture
```

Wireshark · Export · HTTP object list

Packe ▲	Hostname	Content Type	Size	Filena
28	www.acbonline.com	text/html	1245 bytes	hanc
64	www.acbonline.com	text/html	53 kB	prod
68	www.acbonline.com	text/html	1245 bytes	hanc
172	www.acbonline.com	application/pdf	88 kB	idc_a
176	www.acbonline.com	text/html	1245 bytes	hanc
203	www.acbonline.com	text/html	1245 bytes	prelc
215	www.acbonline.com	text/html	1245 bytes	Beba

Application Layer

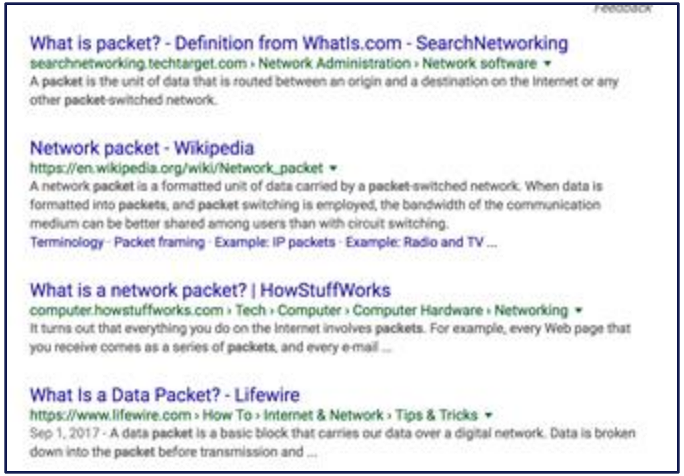
Application Layer

Googling packets

chrome

REQUEST

RESPONSE



Feedback

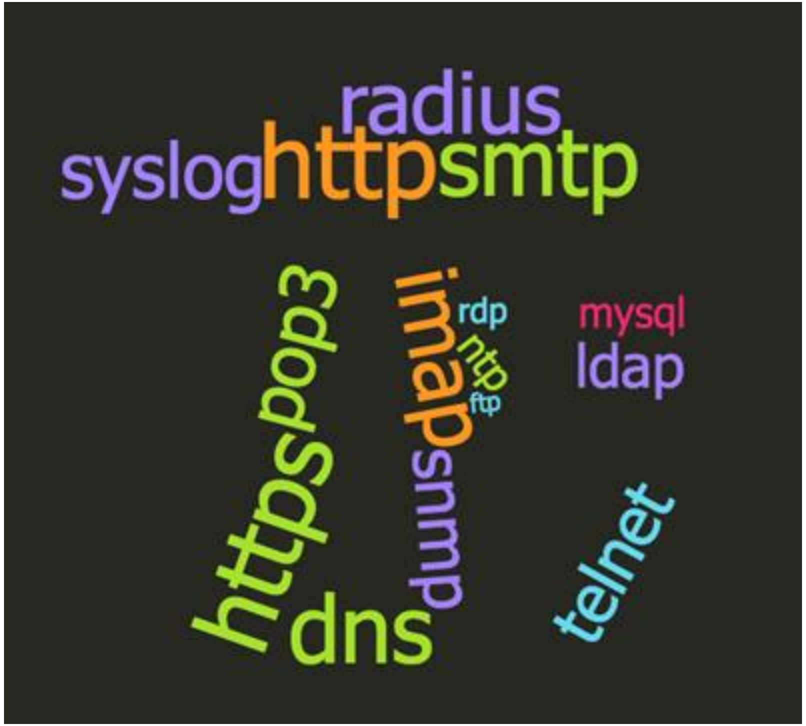
What is packet? - Definition from WhatIs.com - SearchNetworking
searchnetworking.techtarget.com › Network Administration › Network software ▾
A **packet** is the unit of data that is routed between an origin and a destination on the Internet or any other **packet**-switched network.

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 ...

Application Layer: Common Services



Application Layer: Secure vs Insecure Protocols

Secure

HTTPS

SSH

SFTP

Insecure

HTTP

FTP

Telnet

Activity: HTTP Reveals

Open offshore.pcap, and determine the following:

1. What geographic location was the subject of this capture?
2. Who was doing the research on the location?
3. What is their birthdate?
4. What is their business email address?
5. What is their personal email address?
6. What place did they claim to “love”?

Application Layer Attacks

Can be client-side or server-side

Leverage vulns in applications

Examples:

- Web shells
- Buffer overflows
- Injections
- MitM
- XSS/XSRF

Activity: I’ve Got the Poison...

Open injection.pcap and determine the following:

1. What type of injection attack was used?
2. Was it successful?
3. Who was the attacker able to login as?

Activity: Oh What a Tangled Web We Weave

Open web.pcap and determine the following:

1. What is the IP address of the target?
2. What type of attack was being leveraged?
3. What was the first command the attacker tried, and was it successful?
4. Who was the logged-on user on the system?
5. What was the message in secret.txt?

Activity: Here Phishy, Phishy

Open findingnemo.pcap and answer the following:

1. There is phishing activity - see if you can find it.
2. How many redirects were there?
3. What was the ultimate outcome?

Activity: It’s Getting Hot in Here

Open burnout.pcap and answer the following:

1. What kind of malicious activity is happening here?
2. What site is delivering it?
3. How could you prevent this activity?

Transport Layer

User Datagram Protocol

User Datagram Protocol (UDP)

RFC 768 (1980)
Protocol number 17
“Connectionless”
Common implementations:

- DNS
- TFTP
- DHCP

I'D TELL YOU
A JOKE ABOUT UDP
BUT I DON'T KNOW
IF YOU'D GET IT
imgflip.com

Activity: Misdirection

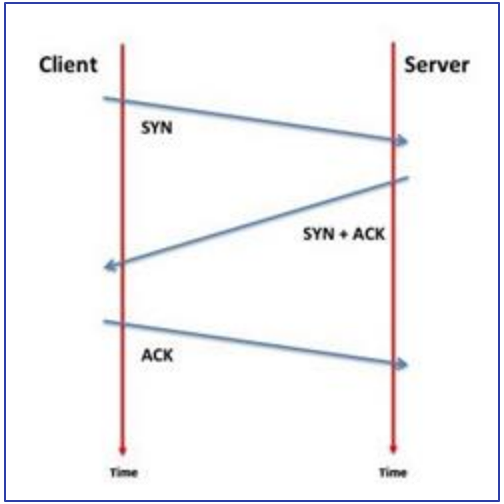
Open udp.pcap and answer the following:

1. Our victim tried to reach 3 different domains. What were they?
2. Where did they all ultimately land?
3. What type of attack was this?

Transport Control Protocol

Transport Control Protocol (TCP)

RFC 793 (1981)
Protocol number 6
“Connection-oriented”
Many implementations



URG | ACK | PSH | RST | SYN | FIN

TCP Port Scanning

SYN > open port, responds with SYN-ACK

SYN > closed port, responds with RST

SYN > filtered port, no response

For more info on different types of nmap scans, see: https://nmap.org/book/man-port-scanning-techniques.html

Activity: Scanz

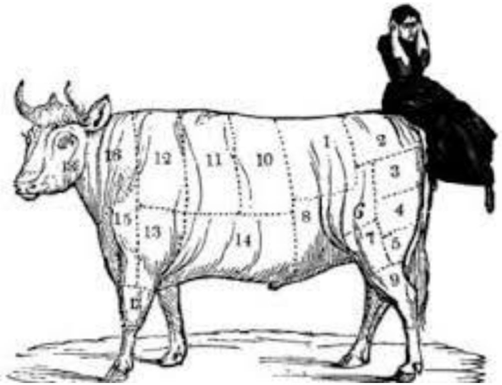
Open tcp.pcap and answer the following:

1. There was scanning activity. What ports were open on the scanned host?
2. There were encrypted communications. What was the version of the application used?

Activity: Where's the Beef?

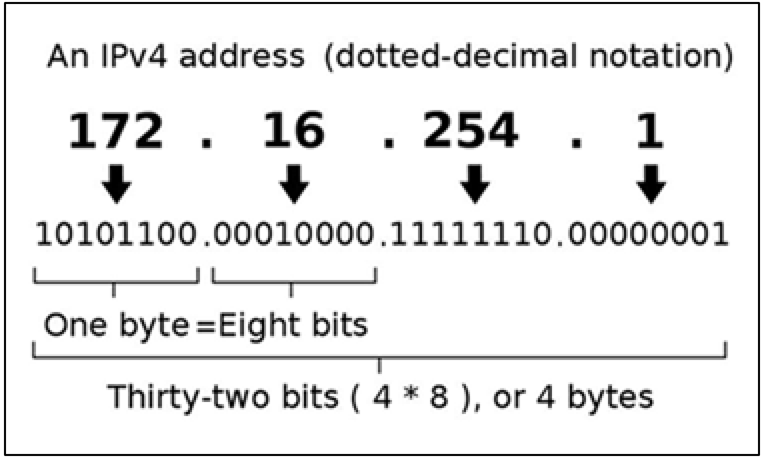
Open hook.pcap and answer the following:

1. What hacking tool is in use in this capture?
2. What is the server OS and version?
3. What site(s) are being hooked?



Internet Layer

Internet Layer: IPv4 vs IPv6



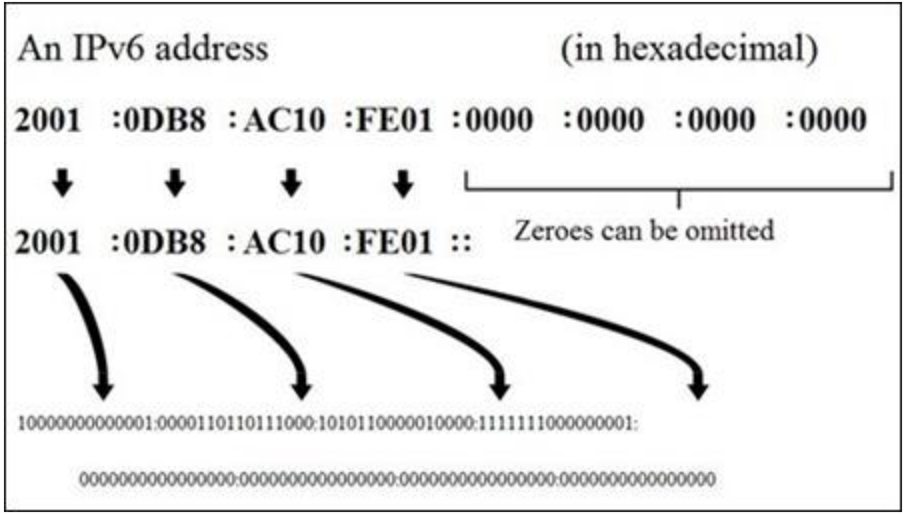
An IPv4 address (dotted-decimal notation)

172 . 16 . 254 . 1

10101100.00010000.11111110.00000001

One byte = Eight bits

Thirty-two bits (4 * 8), or 4 bytes



An IPv6 address (in hexadecimal)

2001 :0DB8 :AC10 :FE01 :0000 :0000 :0000 :0000

2001 :0DB8 :AC10 :FE01 ::

Zeroes can be omitted

10000000000001:0000110110111000:1010110000010000:1111111000000001:

0000000000000000:0000000000000000:0000000000000000:0000000000000000

IPv4

Internet Protocol v4 (IPv4)

RFC 3514, The Security Flag in the IPv4 Header, 1 April 2003 ("Evil Bit")

RFC 791 (1981)

Provides device IP addressing information

Required for inter-network communications

Used by routers to distribute traffic

Common implementations:

- ICMP
- OSPF

Internet Control Message Protocol

ICMP

RFC 792 (1981)
Transport or Internet Layer?
“ICMP, uses the basic support of IP as if it were a higher level protocol, however, ICMP is actually an integral part of IP, and must be implemented by every IP module.”

- Protocol number 1
- Typically associated with the “ping” command
- Primarily used for testing connectivity issues

Activity: Bring Out Your Dead

Open podping.pcap and answer the following:

1. How many bytes were exchanged in the largest conversation?
2. What was the largest frame length for ICMP traffic?
3. Was there any packet fragmentation?
4. What was the data that was transmitted with the ICMP traffic?
5. What type of attack was this?

Network Access Layer

Ethernet

RFC 894 (1984)
What we will typically observe in traffic
Features IEEE 802 standards
Involves MAC addresses (device addresses)
Used by switches to distribute traffic

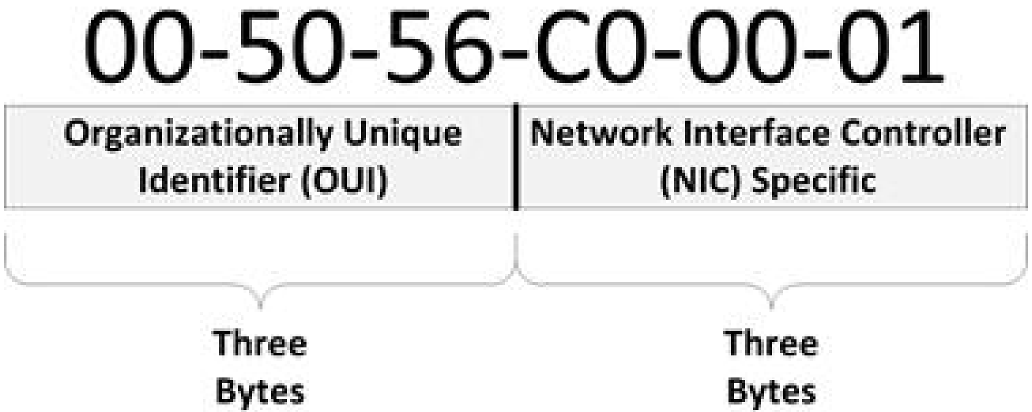
IEEE 802 Standards

Promulgated by Institute of Electrical and Electronics Engineers (IEEE)
Common implementations:

- 802.3 Ethernet
- 802.11 Wireless

See http://www.ieee802.org/

Network Access Layer: MAC Address



00-50-56-C0-00-01

Organizationally Unique Identifier (OUI)

Network Interface Controller (NIC) Specific

Three Bytes

Three Bytes

Network Layer Attacks

- MAC spoofing
- MAC flooding
- ARP spoofing

Contact Info

@marcelle_fsg

@marigalloway

@_Joyous_