Network Threat Hunting

Brian Olliff

Defensive Engineering Instructor

Key Concepts

+ **Network IOCs**

+ **Capturing network traffic**

+ **Analyzing captured packets**

MAJOR TOPICS

- Network IOCs
- Capturing traffic on Windows and Linux
- Analyzing traffic with various tools
- Recognizing abnormal traffic

LEARNING OUTCOMES

- Be familiar with different types of network IOCs
- Understand the methods to capture traffic on various systems
- Be able to effectively analyze traffic using Wireshark
- Be able to recognize different types of abnormal traffic (ARP, TCP, DNS, HTTP, etc)

PREREQUISITES

- Networking fundamentals
- Understand network protocols
- Cybersecurity fundamentals

Let’s Get Started!

Network Threat Hunting

+ Network IOCs
+ Capturing network traffic
+ Analyzing previously captured data

Introduction to Network Hunting

Network Threat Hunting

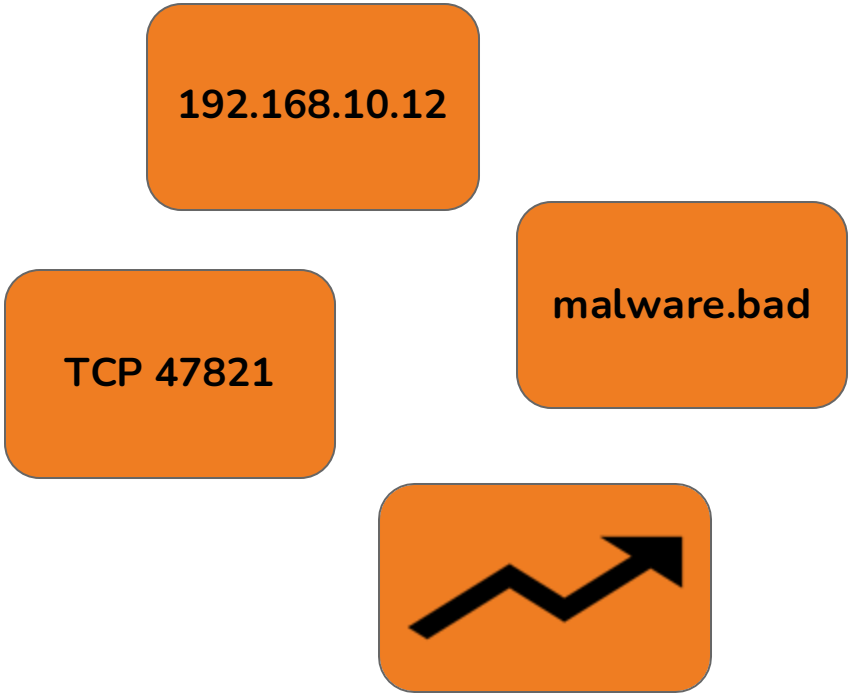
- Hunts with (primarily) network-based hypothesis and IOCs
  - Not based on TTPs
- Can begin with
  - Specific intelligence
  - Reports from SOC/network team
  - Alerts from monitoring systems
- Live network traffic capture
- Analysis of previously captured packet data

Hypothesis or Trigger

“An attacker has compromised the network and is communicating with <IPs>.”

“The network team reports suspicious traffic on port 53. An adversary may be exfiltrating data.”

Network IOCs



- Intelligence sources
  - Reports from ISACs/vendor
  - Paid/free feed
  - Network team/SOC
- Network security devices
  - IDS/IPS
  - Firewalls
- Network traffic captures
- Local endpoint logs
  - Applications
  - Sysmon

Network IOCs

IPs and Domains

- IP addresses
  - 123.45.67.89
  - 123.45.67.0/24
  - IPv6 addresses
    - 2001:0db8:85a3:0000:0000:8a2e:0370:7334
    - 2001:0db8:85a3::8a2e:370:7334
- Domain names
  - Subdomains
  - dm548gfsmn2k562l.malware.bad
  - rnicrosoft.com
  - goggle.com
- Important to check multiple intel sources

Protocol Misuse

- Protocol on non-typical ports
  - HTTP traffic on port 53
  - SSH traffic on port 8080
- Legitimate protocols being used on different ports
  - RDP on port 6645
  - HTTP on port 52981
- Protocols being used incorrectly or against standards
  - Traffic indicates it's DNS protocol
  - Packet contents are C2 communication

Abnormal Traffic

- Traffic patterns
  - Compared to baselines
  - Any type of unusual protocol usage
- Volume
  - Larger amount of data transferred than normal
  - Workstations uploading large volume of data to internet
- Frequency
  - Activity during evenings/weekends (or other “off” hours)
  - Regular connectivity (every 30 min, 1hr, etc)
- Source/destination
  - General workstations talking to unusual destinations
  - Ex: Sales endpoint with SSH connection to foreign country

Unexpected Transfers

- Requires baselines and knowledge of “normal”
- Large amount of data being transferred
  - Keep eye out for smaller transfers
  - Base hunt off source/destination, in addition to volume
- Directions
  - Internally (machine to machine) -> lateral movement, privesc
  - From inside to outside -> data exfiltration
  - From outside to inside -> possible payload download (usually smaller)

Capturing Network Traffic

Network Sensor Basics

- Can be individual devices or configurations on network devices
- Allows logging/capturing and analysis of traffic
- Placement in network determines logged traffic
  - On switch - can see any traffic on that switch
  - Between two routers - can see traffic between those devices
- Provide insight into exactly what is happening on network
  - Possible C2 activity
  - Workstations downloading payloads
  - Data exfiltration

Tap and Mirror

- Network Tap
  - Usually standalone device (can be built-in to other devices)
  - IPS systems can use this to monitor/block traffic
  - Three network ports
    - Traffic between two ports passes through
    - Traffic is copied and routed to monitor port for logging
- Port mirroring/SPAN
  - Configuration on network device
  - One port set up as “mirror” port
  - All traffic on device copied to that port for logging
  - Can affect performance and result in dropped packets

Application Capture

- Wireshark (or similar application)
- Provide ability to capture packets on individual workstation
  - Does not capture if workstation not source/destination
  - Except broadcasts
- Encrypted traffic is captured - but still encrypted
- Can result in very large capture file
  - Capture filters can reduce, but may miss important data

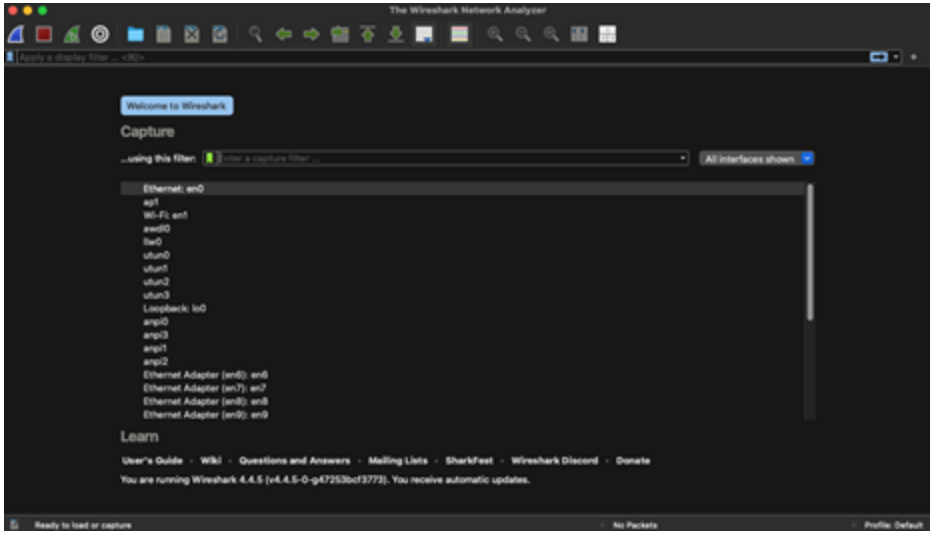
Network Analysis Tools

libpcap

- Unix library provides capabilities for packet sniffing/analysis
- Wireshark & tcpdump based on libpcap
- WinPcap - libpcap library designed for Windows
  - No longer developed or supported
  - Replaced with Npcap
    - Created by Nmap Project
- Uses Berkeley Packet Filter (BPF)
  - Expressions to filter captured packets
  - Used in multiple applications

Wireshark

- Network sniffer and protocol analyzer
  - Analysis of all network traffic on computer's network interface
- Cross platform
  - Windows/Linux/MacOS
- Capabilities
  - Live capture/analysis
    - Save pcap files
  - Analysis of previous captures
  - Capture/display filters
  - "Follow stream"
- TShark
  - Terminal-based Wireshark



tcpdump

- Unix-based packet sniffer
  - Linux, FreeBSD, MacOS
- Intercepts & displays transmitted/received on computer
- Similar capabilities to Wireshark/TShark

```
          :~$ sudo tcpdump -i eth0
[sudo] password for stduser:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
09:18:02.133182 IP 192.168.102.1.17500 > 192.168.102.255.17500: UDP, length 200
09:18:02.854919 IP 192.168.102.147.56976 > 192.168.102.2.domain: 53964+ PTR? 255.102.168.192.in-addr.arpa. (46)
09:18:02.864964 IP 192.168.102.2.domain > 192.168.102.147.56976: 53964 NXDomain 0/0/0 (46)
09:18:02.865051 IP 192.168.102.147.59910 > 192.168.102.2.domain: 12279+ PTR? 1.102.168.192.in-addr.arpa. (44)
09:18:02.875296 IP 192.168.102.2.domain > 192.168.102.147.59910: 12279 NXDomain 0/0/0 (44)
09:18:03.848147 IP 192.168.102.147.48873 > 192.168.102.2.domain: 27140+ PTR? 2.102.168.192.in-addr.arpa. (44)
09:18:03.858098 IP 192.168.102.2.domain > 192.168.102.147.48873: 27140 NXDomain 0/0/0 (44)
09:18:03.858183 IP 192.168.102.147.50818 > 192.168.102.2.domain: 50563+ PTR? 147.102.168.192.in-addr.arpa. (46)
09:18:03.867137 IP 192.168.102.2.domain > 192.168.102.147.50818: 50563 NXDomain 0/0/0 (46)
```

Others

- NetWitness Investigator
  - Different than full NetWitness SIEM platform
  - Summarizes contents of pcap files and shows important information
    - Service types, source/destination IP/port, email addresses, hostnames

- NetworkMiner
  - Capture and analysis
  - Can summarize information similar to NetWitness Investigator
  - Keyword searching and anomalies

Capturing Traffic with Wireshark

Wireshark Usage

- Can only monitor traffic that is destined for installed machine
  - Unless analyzing packet capture file (.pcap)
- Filters
  - Capture filters
    - Live filter, limits captured data
    - Reduces processing overhead and capture file size
  - Display filters
    - Can be used during capture, or afterwards
    - Doesn't reduce processing overhead
    - Assists with narrowing down what's shown
- "Follow stream"
  - Isolate specific entry
  - Follows the communication path and only shows that data

Linux
Network Capture

tcpdump

tcpdump [options] [filter expression]

```
sudo tcpdump -i eth0
```

- `--list-interfaces`
- `-c`
- `-w`
- Numerous capture filters

`https://www.tcpdump.org/manpages/tcpdump.1.html`

Packet Analysis with Wireshark

Wireshark Analysis

- Expert information
  - Overview of type of traffic in pcap
- Captured file properties
  - Information about file
- Resolved addresses
- Protocol hierarchy
  - Summary of protocols
- Conversations
- Display filters
- Follow stream

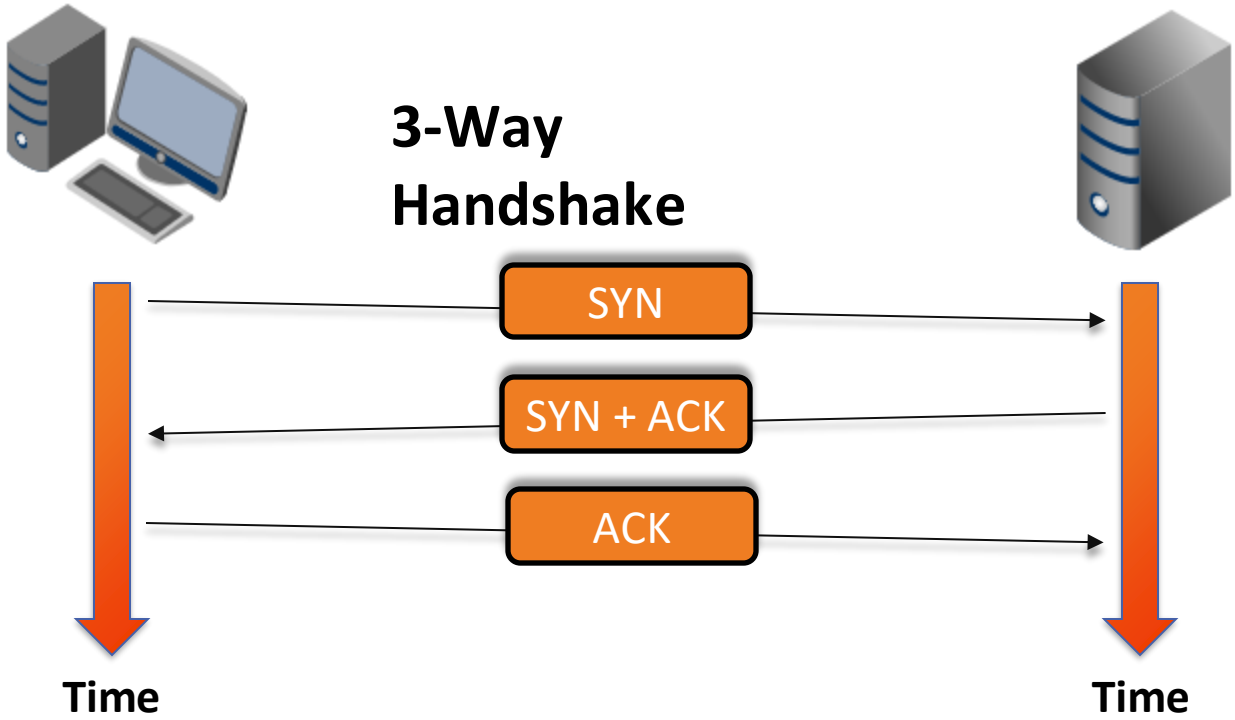
NetworkMiner

Recognizing Abnormal Traffic

Abnormal or Suspicious Traffic

- ARP
- TCP
- ICMP
- DHCP
- HTTP/S
- DNS

TCP

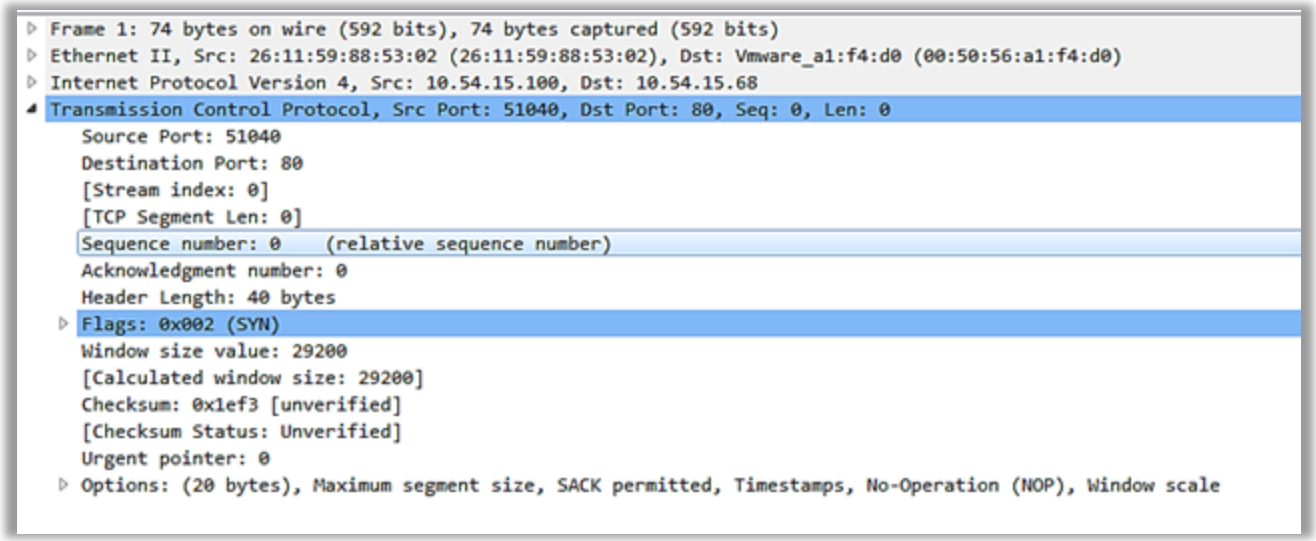


Normal vs Suspicious TCP

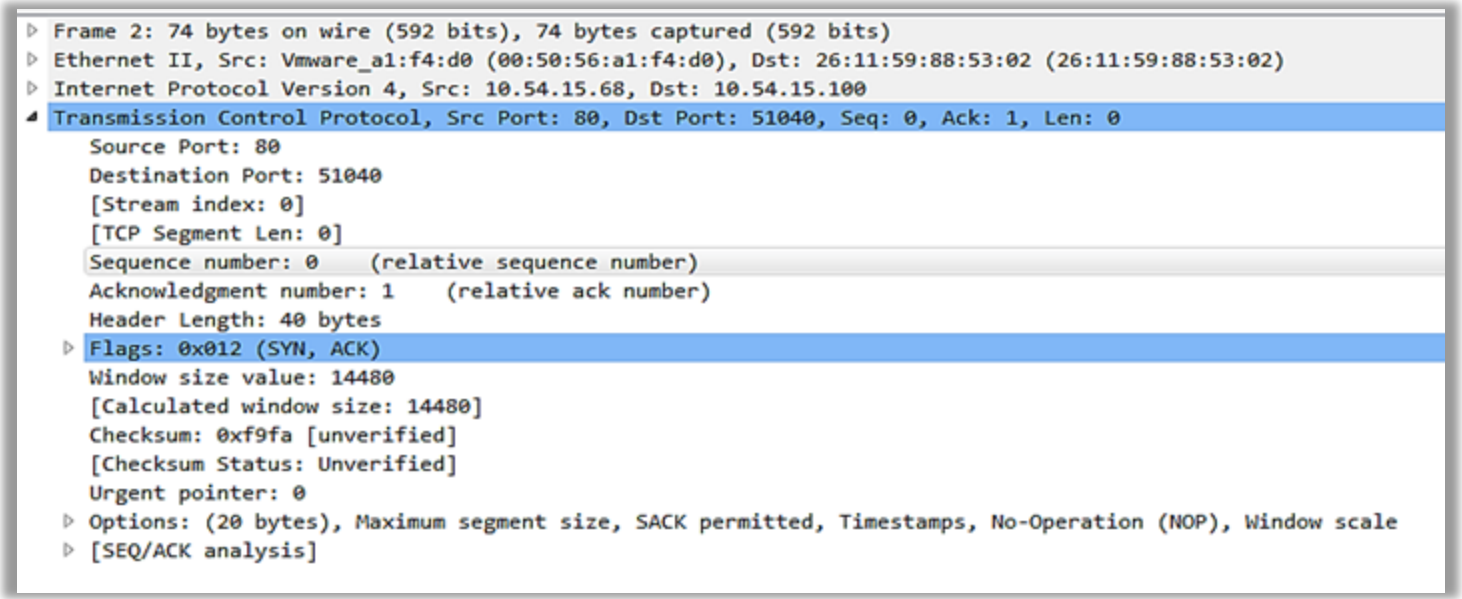
Normal TCP Traffic	Suspicious TCP Traffic
3-way handshake (SYN, SYN/ACK, ACK)	Excessive SYN packets (scanning)
	Smart TCP attacks (usage of different flags)
	Single host to multiple ports or single host to multiple nodes (scanning)

Normal TCP Traffic

	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.54.15.100	10.54.15.68	TCP	74	51040 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2677172 TSecr=0 WS=128
2	0.054908	10.54.15.68	10.54.15.100	TCP	74	80 → 51040 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1337 SACK_PERM=1 TSval=68008 TSecr=2677172 WS=4
3	0.054929	10.54.15.100	10.54.15.68	TCP	66	51040 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=2677186 TSecr=68008



Normal TCP Traffic



Suspicious TCP Traffic

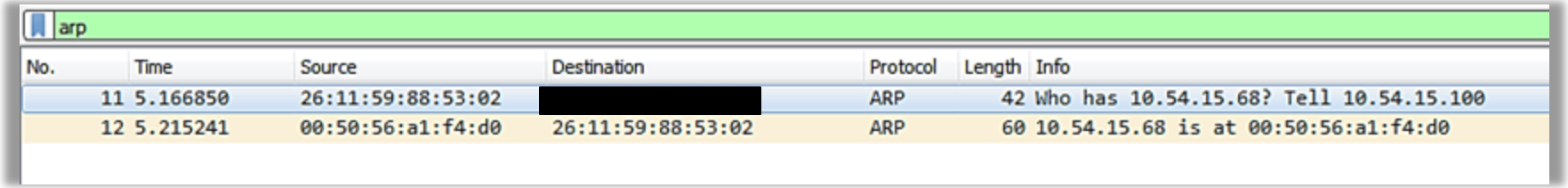
No.	Time	Source	Destination	Protocol	Length	Info
252	1.884272105	172.16.5.50	10.50.96.115	ICMP	42	Echo (ping) request id=0x26f4, seq=0/0, ttl=56 (no response found!)
528	3.239891218	172.16.5.50	10.50.96.115	ICMP	42	Echo (ping) request id=0xc7a1, seq=0/0, ttl=51 (no response found!)
1018	5.882700328	172.16.5.50	10.50.96.115	TCP	58	51286 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1054	6.163446779	172.16.5.50	10.50.96.115	TCP	58	51287 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1674	10.779530015	172.16.5.50	10.50.96.115	TCP	54	51286 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
1703	10.977220446	172.16.5.50	10.50.96.115	TCP	54	51287 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
2620	15.474233425	172.16.5.50	10.50.96.115	ICMP	54	Timestamp request id=0xa837, seq=0/0, ttl=41
3006	16.791005321	172.16.5.50	10.50.96.115	ICMP	54	Timestamp request id=0xe11a, seq=0/0, ttl=55
3406	18.151715145	172.16.5.50	10.50.96.115	ICMP	54	Timestamp request id=0x554a, seq=0/0, ttl=47
3843	19.454155429	172.16.5.50	10.50.96.115	ICMP	54	Timestamp request id=0xfb82, seq=0/0, ttl=46

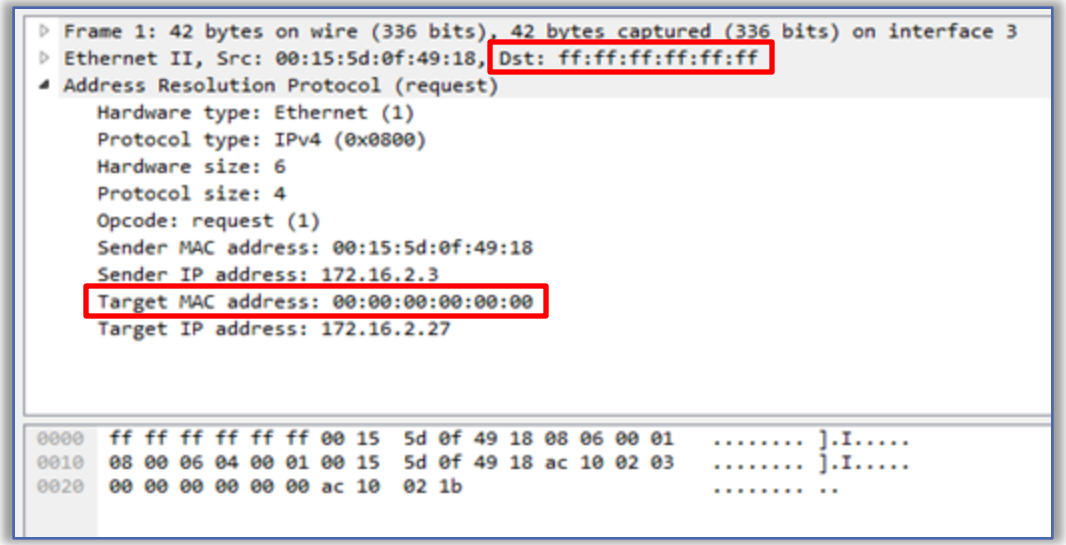
1	0.000000000	172.16.5.50	10.50.97.5	TCP	54	1140 → 1 [SYN] Seq=0 Win=512 Len=0
2	0.000068731	172.16.5.50	10.50.97.5	TCP	54	1140 → 2 [SYN] Seq=0 Win=512 Len=0
3	0.000072857	172.16.5.50	10.50.97.5	TCP	54	1140 → 4 [SYN] Seq=0 Win=512 Len=0
4	0.000074818	172.16.5.50	10.50.97.5	TCP	54	1140 → 6 [SYN] Seq=0 Win=512 Len=0
5	0.000076675	172.16.5.50	10.50.97.5	TCP	54	1140 → 7 [SYN] Seq=0 Win=512 Len=0
6	0.000078473	172.16.5.50	10.50.97.5	TCP	54	1140 → 9 [SYN] Seq=0 Win=512 Len=0
7	0.000080677	172.16.5.50	10.50.97.5	TCP	54	1140 → 11 [SYN] Seq=0 Win=512 Len=0
8	0.000082544	172.16.5.50	10.50.97.5	TCP	54	1140 → 13 [SYN] Seq=0 Win=512 Len=0
9	0.000084584	172.16.5.50	10.50.97.5	TCP	54	1140 → 15 [SYN] Seq=0 Win=512 Len=0
10	0.000086544	172.16.5.50	10.50.97.5	TCP	54	1140 → 17 [SYN] Seq=0 Win=512 Len=0
11	0.000088415	172.16.5.50	10.50.97.5	TCP	54	1140 → 18 [SYN] Seq=0 Win=512 Len=0
12	0.000090121	172.16.5.50	10.50.97.5	TCP	54	1140 → 19 [SYN] Seq=0 Win=512 Len=0
13	0.000091943	172.16.5.50	10.50.97.5	TCP	54	1140 → 20 [SYN] Seq=0 Win=512 Len=0
14	0.000093777	172.16.5.50	10.50.97.5	TCP	54	1140 → 21 [SYN] Seq=0 Win=512 Len=0
15	0.000095482	172.16.5.50	10.50.97.5	TCP	54	1140 → 22 [SYN] Seq=0 Win=512 Len=0

Normal vs Suspicious ARP

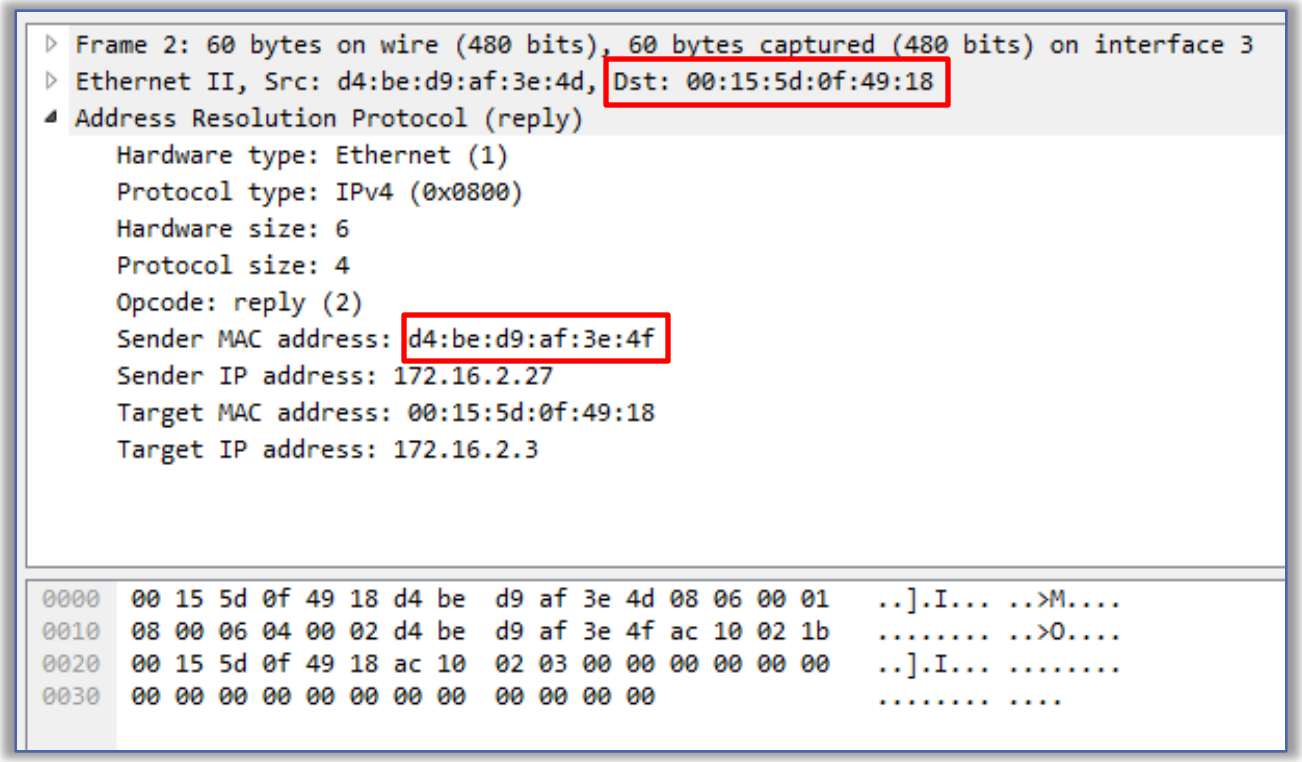
Normal ARP Traffic	Suspicious ARP Traffic
ARP broadcasts at a “reasonable” rate	Tens, hundreds, or even thousands of ARP broadcast messages in a small amount of time.
ARP response typically following a request	Gratuitous ARP replies
	Two identical MAC addresses with different IP addresses

Normal ARP Traffic





Normal ARP Traffic



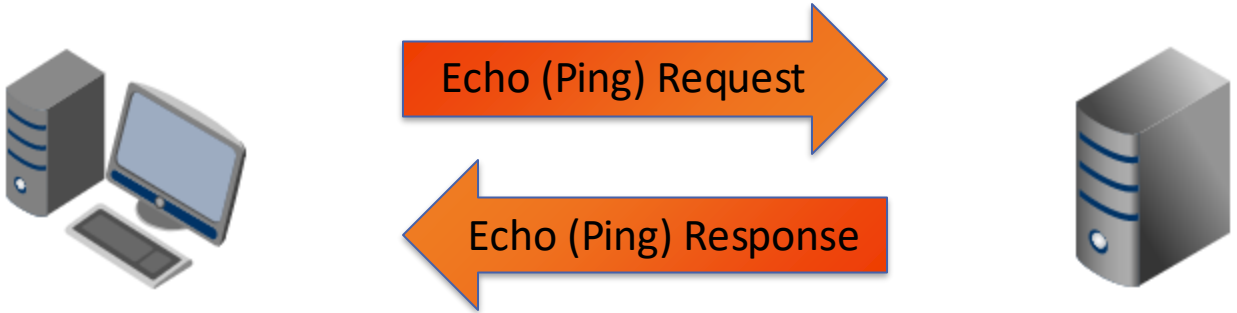
Suspicious ARP Traffic

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco251_af:f4:54	Broadcast	ARP	60	Who has 24.166.173.159? Tell 24.166.172.1
2	0.098594	Cisco251_af:f4:54	Broadcast	ARP	60	Who has 24.166.172.141? Tell 24.166.172.1
3	0.110617	Cisco251_af:f4:54	Broadcast	ARP	60	Who has 24.166.173.161? Tell 24.166.172.1
4	0.211791	Cisco251_af:f4:54	Broadcast	ARP	60	Who has 65.28.78.76? Tell 65.28.78.1
5	0.216744	Cisco251_af:f4:54	Broadcast	ARP	60	Who has 24.166.173.163? Tell 24.166.172.1
6	0.307909	Cisco251_af:f4:54	Broadcast	ARP	60	Who has 24.166.175.123? Tell 24.166.172.1
7	0.330433	Cisco251_af:f4:54	Broadcast	ARP	60	Who has 24.166.173.165? Tell 24.166.172.1

No.	Time	Source	Destination	Protocol	Length	Info
15	61.162590056	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.1? Tell 172.16.5.67
16	61.164533730	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.2? Tell 172.16.5.67
17	61.166589500	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.3? Tell 172.16.5.67
18	61.171696684	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.4? Tell 172.16.5.67
19	61.173595193	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.5? Tell 172.16.5.67
20	61.175482595	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.6? Tell 172.16.5.67
21	61.177434405	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.7? Tell 172.16.5.67
22	61.179428423	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.8? Tell 172.16.5.67
23	61.181401311	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.9? Tell 172.16.5.67
24	61.183387692	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.10? Tell 172.16.5.67
25	61.185470650	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.11? Tell 172.16.5.67
26	61.187379238	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.12? Tell 172.16.5.67
27	61.189625522	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.13? Tell 172.16.5.67
28	61.191455492	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.14? Tell 172.16.5.67
29	61.193387656	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.15? Tell 172.16.5.67
30	61.195423342	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.16? Tell 172.16.5.67
31	61.197387752	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.17? Tell 172.16.5.67
32	61.199389322	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.18? Tell 172.16.5.67
33	61.201395568	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.19? Tell 172.16.5.67
34	61.203388474	b2:fe:ed:db:02:32	Broadcast	ARP	42	Who has 172.16.5.20? Tell 172.16.5.67

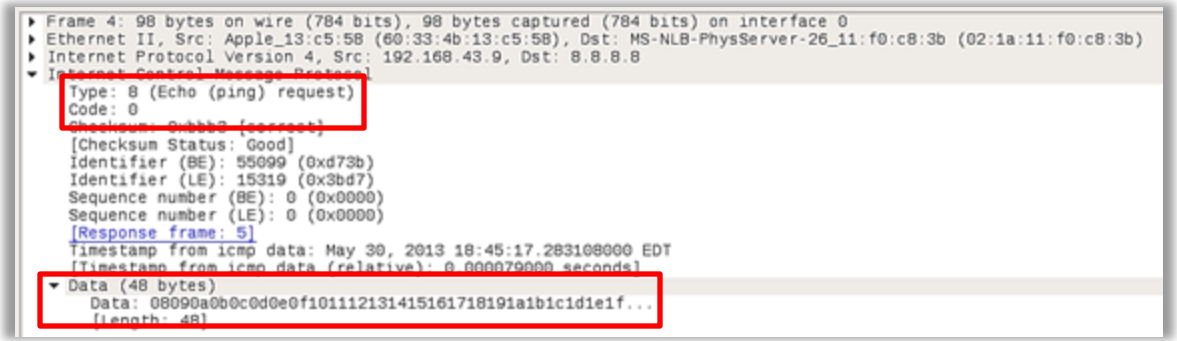
Recognizing Abnormal ICMP & DHCP Traffic

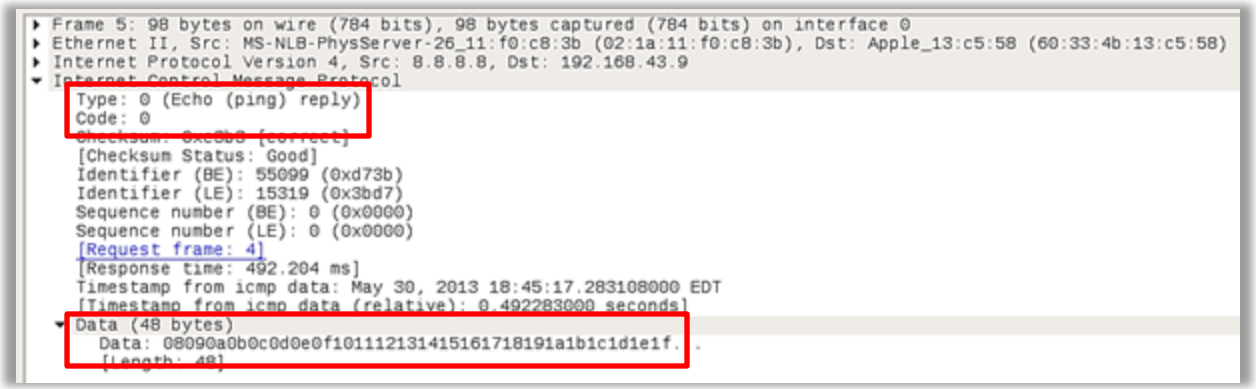
ICMP



4	5.013334	192.168.43.9	8.8.8.8	ICMP	98	Echo (ping) request id=0xd73b, seq=0/0, ttl=64 (reply in 5)
5	5.505538	8.8.8.8	192.168.43.9	ICMP	98	Echo (ping) reply id=0xd73b, seq=0/0, ttl=40 (request in 4)
6	6.019290	192.168.43.9	8.8.8.8	ICMP	98	Echo (ping) request id=0xd73b, seq=1/256, ttl=64 (reply in 7)
7	6.153653	8.8.8.8	192.168.43.9	ICMP	98	Echo (ping) reply id=0xd73b, seq=1/256, ttl=40 (request in 6)
8	7.015108	192.168.43.9	8.8.8.8	ICMP	98	Echo (ping) request id=0xd73b, seq=2/512, ttl=64 (reply in 9)
9	7.781987	8.8.8.8	192.168.43.9	ICMP	98	Echo (ping) reply id=0xd73b, seq=2/512, ttl=40 (request in 8)

ICMP Echo

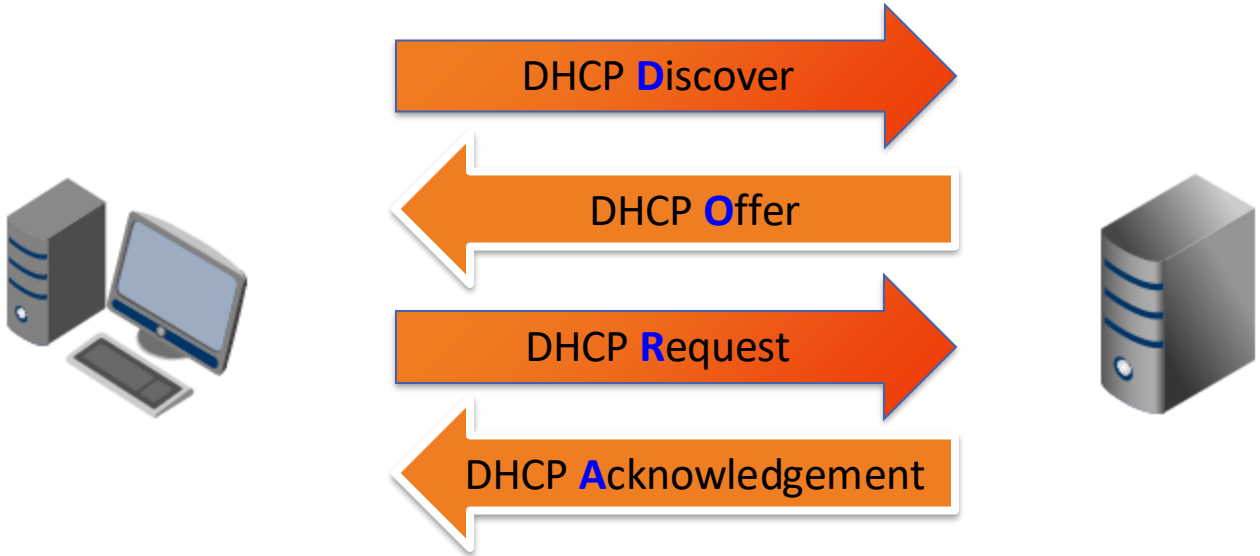




Normal vs Suspicious ICMP Echo

Normal ICMP Echo Traffic	Suspicious ICMP Echo Traffic
Limited number of echo requests on net	Tens, hundreds, or even thousands of echo requests in a small amount of time.
Echo reply should always follow request (request does not always receive reply)	Replies without requests
Small amount of info in “data” field	Large ICMP packets, esp in data field

DHCP



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	314	DHCP Discover - Transaction ID 0x3d1d
2	0.000295	192.168.0.1	192.168.0.10	DHCP	342	DHCP Offer - Transaction ID 0x3d1d
3	0.070031	0.0.0.0	255.255.255.255	DHCP	314	DHCP Request - Transaction ID 0x3d1e
4	0.070345	192.168.0.1	192.168.0.10	DHCP	342	DHCP ACK - Transaction ID 0x3d1e

Normal vs Suspicious DHCP

Normal ICMP Echo Traffic	Suspicious ICMP Echo Traffic
Follows DORA steps	Offers without request, other out of order traffic
Offers originate from legitimate DHCP server	Rogue DHCP server

Recognizing Abnormal DNS & HTTP Traffic

DNS

- Typically a query-response protocol
- Normally uses UDP 53
  - Many legitimate uses for TCP 53
- Traffic destination should always be DNS servers

Normal DNS Traffic	Suspicious DNS Traffic
UDP 53	TCP 53 (not always)
Should only go to DNS Servers	DNS traffic not going to DNS Servers
Query -> response	Multiple queries with no response Multiple responses, no queries

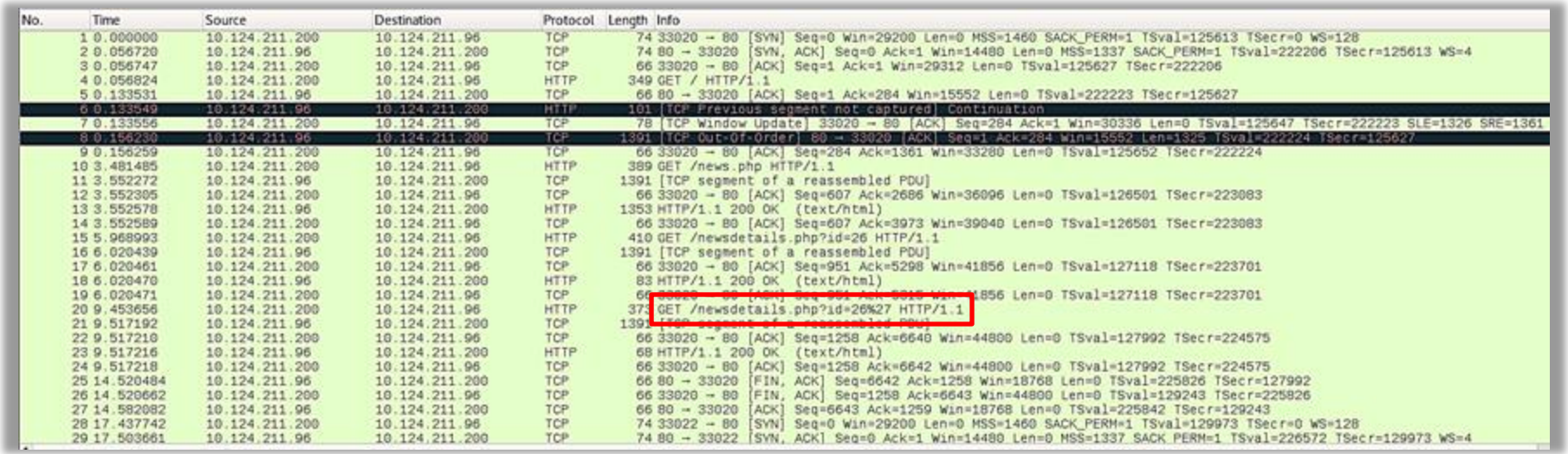
HTTP

- HTTP traffic typically requests and responses
  - Messages
  - Responses include 3-digit status code (200, 302, 404, etc)
- HTTP messages include message header and body
- Methods used to perform various operations
  - 9 current methods
  - GET, HEAD, PUT, POST, etc
- May be more difficult to spot malicious traffic

Normal vs Suspicious HTTP

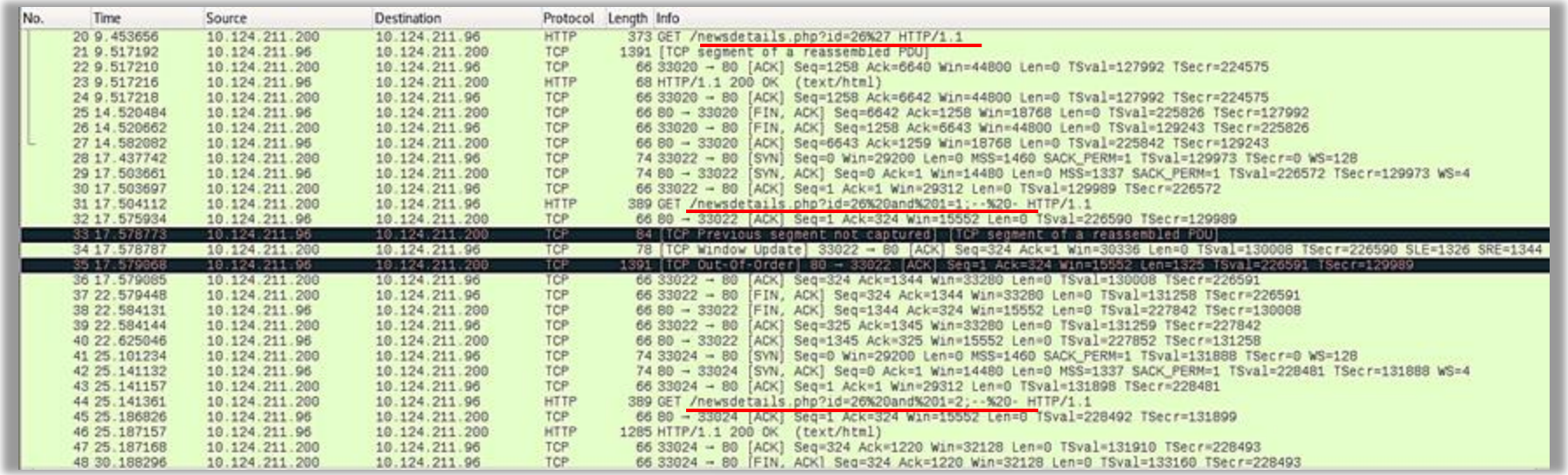
Normal HTTP Traffic	Suspicious HTTP Traffic
Port 80, TCP Port 8080, TCP Port 8088, TCP	Other, non-standard ports Standard ports may still be used by attackers Normally not blocked on networks
Plaintext traffic (NOT HTTPS)	Encrypted traffic on port 80 or using HTTP
FQDN connection to server	IP connection to server (especially external IPs)

Suspicious HTTP



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.124.211.200	10.124.211.96	TCP	74	33020 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=125613 TSecr=0 WS=128
2	0.056720	10.124.211.96	10.124.211.200	TCP	74	80 → 33020 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1337 SACK_PERM=1 TSval=222206 TSecr=125613 WS=4
3	0.056747	10.124.211.200	10.124.211.96	TCP	66	33020 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=125627 TSecr=222206
4	0.056824	10.124.211.200	10.124.211.96	HTTP	349	GET / HTTP/1.1
5	0.133531	10.124.211.96	10.124.211.200	TCP	66	80 → 33020 [ACK] Seq=1 Ack=284 Win=15552 Len=0 TSval=222223 TSecr=125627
6	0.133549	10.124.211.96	10.124.211.200	HTTP	101	[TCP Previous segment not captured] Continuation
7	0.133556	10.124.211.200	10.124.211.96	TCP	78	[TCP Window Update] 33020 → 80 [ACK] Seq=284 Ack=1 Win=30336 Len=0 TSval=125647 TSecr=222223 SLE=1326 SRE=1361
8	0.156230	10.124.211.96	10.124.211.200	TCP	1391	[TCP Out-Of-Order] 80 → 33020 [ACK] Seq=1 Ack=284 Win=15552 Len=1325 TSval=222224 TSecr=125627
9	0.156259	10.124.211.200	10.124.211.96	TCP	66	33020 → 80 [ACK] Seq=284 Ack=1361 Win=33280 Len=0 TSval=125652 TSecr=222224
10	3.481485	10.124.211.200	10.124.211.96	HTTP	389	GET /news.php HTTP/1.1
11	3.552272	10.124.211.96	10.124.211.200	TCP	1391	[TCP segment of a reassembled PDU]
12	3.552305	10.124.211.200	10.124.211.96	TCP	66	33020 → 80 [ACK] Seq=607 Ack=2686 Win=36096 Len=0 TSval=126501 TSecr=223083
13	3.552578	10.124.211.96	10.124.211.200	HTTP	1353	HTTP/1.1 200 OK (text/html)
14	3.552589	10.124.211.200	10.124.211.96	TCP	66	33020 → 80 [ACK] Seq=607 Ack=3973 Win=39040 Len=0 TSval=126501 TSecr=223083
15	5.968993	10.124.211.200	10.124.211.96	HTTP	410	GET /newsdetails.php?id=26 HTTP/1.1
16	6.020439	10.124.211.96	10.124.211.200	TCP	1391	[TCP segment of a reassembled PDU]
17	6.020461	10.124.211.200	10.124.211.96	TCP	66	33020 → 80 [ACK] Seq=951 Ack=5298 Win=41856 Len=0 TSval=127118 TSecr=223701
18	6.020470	10.124.211.96	10.124.211.200	HTTP	83	HTTP/1.1 200 OK (text/html)
19	6.020471	10.124.211.200	10.124.211.96	TCP	66	[illegible] 1856 Len=0 TSval=127118 TSecr=223701
20	9.453656	10.124.211.200	10.124.211.96	HTTP	37	GET /newsdetails.php?id=26%27 HTTP/1.1
21	9.517192	10.124.211.96	10.124.211.200	TCP	139	[TCP segment of a reassembled PDU]
22	9.517210	10.124.211.200	10.124.211.96	TCP	66	33020 → 80 [ACK] Seq=1258 Ack=6640 Win=44800 Len=0 TSval=127992 TSecr=224575
23	9.517216	10.124.211.96	10.124.211.200	HTTP	68	HTTP/1.1 200 OK (text/html)
24	9.517218	10.124.211.200	10.124.211.96	TCP	66	33020 → 80 [ACK] Seq=1258 Ack=6642 Win=44800 Len=0 TSval=127992 TSecr=224575
25	14.520484	10.124.211.96	10.124.211.200	TCP	66	80 → 33020 [FIN, ACK] Seq=6642 Ack=1258 Win=18768 Len=0 TSval=225826 TSecr=127992
26	14.520662	10.124.211.200	10.124.211.96	TCP	66	33020 → 80 [FIN, ACK] Seq=1258 Ack=6643 Win=44800 Len=0 TSval=129243 TSecr=225826
27	14.582082	10.124.211.96	10.124.211.200	TCP	66	80 → 33020 [ACK] Seq=6643 Ack=1259 Win=18768 Len=0 TSval=225842 TSecr=129243
28	17.437742	10.124.211.200	10.124.211.96	TCP	74	33022 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=129973 TSecr=0 WS=128
29	17.503661	10.124.211.96	10.124.211.200	TCP	74	80 → 33022 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1337 SACK_PERM=1 TSval=226572 TSecr=129973 WS=4

Suspicious HTTP



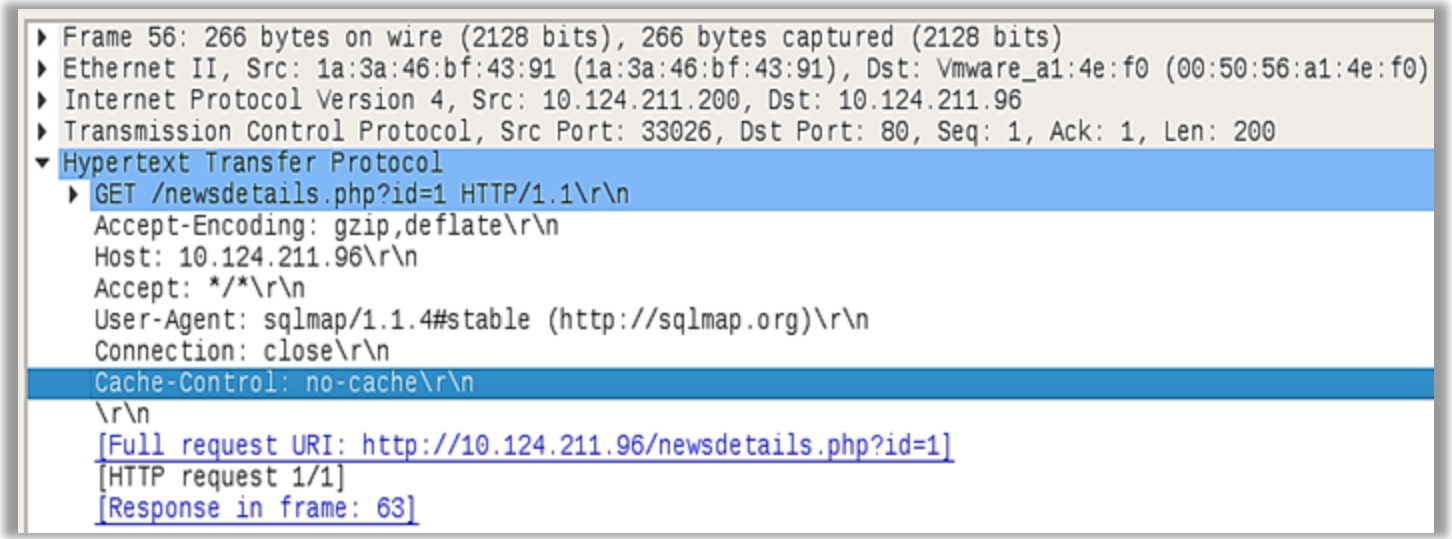
No.	Time	Source	Destination	Protocol	Length	Info
20	9.453656	10.124.211.200	10.124.211.96	HTTP	373	GET /newsdetails.php?id=26%27 HTTP/1.1
21	9.517192	10.124.211.96	10.124.211.200	TCP	1391	[TCP segment of a reassembled PDU]
22	9.517210	10.124.211.200	10.124.211.96	TCP	66	33020 → 80 [ACK] Seq=1258 Ack=6640 Win=44800 Len=0 TSval=127992 TSecr=224575
23	9.517216	10.124.211.96	10.124.211.200	HTTP	68	HTTP/1.1 200 OK (text/html)
24	9.517218	10.124.211.200	10.124.211.96	TCP	66	33020 → 80 [ACK] Seq=1258 Ack=6642 Win=44800 Len=0 TSval=127992 TSecr=224575
25	14.520484	10.124.211.96	10.124.211.200	TCP	66	80 → 33020 [FIN, ACK] Seq=6642 Ack=1258 Win=18768 Len=0 TSval=225826 TSecr=127992
26	14.520662	10.124.211.200	10.124.211.96	TCP	66	33020 → 80 [FIN, ACK] Seq=1258 Ack=6643 Win=44800 Len=0 TSval=129243 TSecr=225826
27	14.582082	10.124.211.96	10.124.211.200	TCP	66	80 → 33020 [ACK] Seq=6643 Ack=1259 Win=18768 Len=0 TSval=225842 TSecr=129243
28	17.437742	10.124.211.200	10.124.211.96	TCP	74	33022 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=129973 TSecr=0 WS=128
29	17.503661	10.124.211.96	10.124.211.200	TCP	74	80 → 33022 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1337 SACK_PERM=1 TSval=226572 TSecr=129973 WS=4
30	17.503697	10.124.211.200	10.124.211.96	TCP	66	33022 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=129989 TSecr=226572
31	17.504112	10.124.211.200	10.124.211.96	HTTP	389	GET /newsdetails.php?id=26%20and%201=1;--%20- HTTP/1.1
32	17.575934	10.124.211.96	10.124.211.200	TCP	66	80 → 33022 [ACK] Seq=1 Ack=324 Win=15552 Len=0 TSval=226590 TSecr=129989
33	17.578773	10.124.211.96	10.124.211.200	TCP	84	[TCP Previous segment not captured] [TCP segment of a reassembled PDU]
34	17.578787	10.124.211.200	10.124.211.96	TCP	78	[TCP Window Update] 33022 → 80 [ACK] Seq=324 Ack=1 Win=30336 Len=0 TSval=130008 TSecr=226590 SLE=1326 SRE=1344
35	17.579068	10.124.211.96	10.124.211.200	TCP	1391	[TCP Out-Of-Order] 80 → 33022 [ACK] Seq=1 Ack=324 Win=15552 Len=1325 TSval=226591 TSecr=129989
36	17.579085	10.124.211.200	10.124.211.96	TCP	66	33022 → 80 [ACK] Seq=324 Ack=1344 Win=33280 Len=0 TSval=130008 TSecr=226591
37	22.579448	10.124.211.200	10.124.211.96	TCP	66	33022 → 80 [FIN, ACK] Seq=324 Ack=1344 Win=33280 Len=0 TSval=131258 TSecr=226591
38	22.584131	10.124.211.96	10.124.211.200	TCP	66	80 → 33022 [FIN, ACK] Seq=1344 Ack=324 Win=15552 Len=0 TSval=227842 TSecr=130008
39	22.584144	10.124.211.200	10.124.211.96	TCP	66	33022 → 80 [ACK] Seq=325 Ack=1345 Win=33280 Len=0 TSval=131259 TSecr=227842
40	22.625046	10.124.211.96	10.124.211.200	TCP	66	80 → 33022 [ACK] Seq=1345 Ack=325 Win=15552 Len=0 TSval=227852 TSecr=131258
41	25.101234	10.124.211.200	10.124.211.96	TCP	74	33024 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=131888 TSecr=0 WS=128
42	25.141132	10.124.211.96	10.124.211.200	TCP	74	80 → 33024 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1337 SACK_PERM=1 TSval=228481 TSecr=131888 WS=4
43	25.141157	10.124.211.200	10.124.211.96	TCP	66	33024 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=131898 TSecr=228481
44	25.141361	10.124.211.200	10.124.211.96	HTTP	389	GET /newsdetails.php?id=26%20and%201=2;--%20- HTTP/1.1
45	25.186826	10.124.211.96	10.124.211.200	TCP	66	80 → 33024 [ACK] Seq=1 Ack=324 Win=15552 Len=0 TSval=228492 TSecr=131899
46	25.187157	10.124.211.96	10.124.211.200	HTTP	1285	HTTP/1.1 200 OK (text/html)
47	25.187168	10.124.211.200	10.124.211.96	TCP	66	33024 → 80 [ACK] Seq=324 Ack=1220 Win=32128 Len=0 TSval=131910 TSecr=228493
48	30.188296	10.124.211.200	10.124.211.96	TCP	66	33024 → 80 [FIN, ACK] Seq=324 Ack=1220 Win=32128 Len=0 TSval=133160 TSecr=228493

Suspicious HTTP

```
▸ Frame 44: 389 bytes on wire (3112 bits), 389 bytes captured (3112 bits)
▸ Ethernet II, Src: 1a:3a:46:bf:43:91 (1a:3a:46:bf:43:91), Dst: Vmware_a1:4e:f0 (00:50:56:a1:4e:f0)
▸ Internet Protocol Version 4, Src: 10.124.211.200, Dst: 10.124.211.96
▸ Transmission Control Protocol, Src Port: 33024, Dst Port: 80, Seq: 1, Ack: 1, Len: 323
▾ Hypertext Transfer Protocol
  ▸ GET /newsdetails.php?id=26%20and%201=2;--%20- HTTP/1.1\r\n
    Host: 10.124.211.96\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://10.124.211.96/newsdetails.php?id=26%20and%201=2;--%20-]
    [HTTP request 1/1]
    [Response in frame: 46]
```

```
▸ Frame 31: 389 bytes on wire (3112 bits), 389 bytes captured (3112 bits)
▸ Ethernet II, Src: 1a:3a:46:bf:43:91 (1a:3a:46:bf:43:91), Dst: Vmware_a1:4e:f0 (00:50:56:a1:4e:f0)
▸ Internet Protocol Version 4, Src: 10.124.211.200, Dst: 10.124.211.96
▸ Transmission Control Protocol, Src Port: 33022, Dst Port: 80, Seq: 1, Ack: 1, Len: 323
▾ Hypertext Transfer Protocol
  ▸ GET /newsdetails.php?id=26%20and%201=1;--%20- HTTP/1.1\r\n
    Host: 10.124.211.96\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://10.124.211.96/newsdetails.php?id=26%20and%201=1;--%20-]
    [HTTP request 1/1]
```

Suspicious HTTP



HTTPS

- Similar to HTTP, but encrypted
- Handshake between client & server prior to communication
  - Agree on protocol version
  - Cryptographic algorithms selected
  - Optional mutual authentication
- Attackers commonly use standard HTTPS ports (443, 8443, etc)
- Non-encrypted traffic on 443 should be suspicious
- Normally, data exchanged cannot be read
  - May be able to decrypt with Wireshark or other tools

Network Threat Hunting - Summary

Key Concepts

+ **Network IOCs**

+ **Capturing network traffic**

+ **Analyzing captured packets**

LEARNING OUTCOMES

- Be familiar with different types of network IOCs
- Understand the methods to capture traffic on various systems
- Be able to effectively analyze traffic using Wireshark
- Be able to recognize different types of abnormal traffic (ARP, TCP, DNS, HTTP, etc)

Next Steps

- Continue with Threat Hunting learning path
- Revisit courses or videos on network IOCs or network fundamentals
- Continue practice in hands-on labs
- Download various PCAP files from wiki.wireshark.org for additional practice

Thank you!

Network Threat Hunting

+ Network IOCs
+ Capturing and analyzing traffic
+ Recognizing abnormal or suspicious traffic
+ Thank you for your time!

EXPERTS AT MAKING YOU AN EXPERT