SharkFest '18 ASIA

05 - Sneaking in The Backdoor

Hacking the Non-Standard Layers

Phill "Sherlock" Shade

Merlion's Keep Consulting

Phillip “Sherlock” Shade (Phill)

phill.shade@gmail.com

- Certified instructor and internationally recognized network security and forensics expert with more than 30 years of experience
- Retired US Navy and the founder of Merlion’s Keep Consulting, a professional services company specializing in network and forensics analysis
- A member of the Global Cyber Response Team (GCRT), FBI InfraGard, Computer Security Institute, and the IEEE and volunteer at Cyber Warfare Forum Initiative
- Holds numerous certifications, including Certified Network Expert (CNX)-Ethernet, CCNA, Certified Wireless Network Administrator (CWNA), and WildPackets Certified Network Forensics Analysis Expert (WNAX)
- Certified Wireshark University, Sniffer University and Planet 3 Wireless instructor

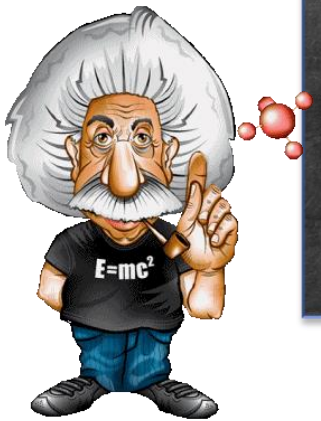
Today's Agenda

1. Welcome to my World..... I'm not a good guy.....

2. Key Forensics Questions to Ask? and those Things You Have to Know - Overview and Terminology

3. What should I look For?

3. Exploiting the lower Layers – Cases Studies to Surprise and Impress (hopefully) you!



Case Studies

1. MK - Forensics Case Study #4 – Man-in-the-Middle
2. MK - WiFi - Attack - Denial of Silence (Extended)
3. Attack - MAC Flood - Capture 2 (macof) Switch
4. MK - Advanced Analysis Lab 8c / e / 9d
5. MK - Sample - IPv4 - IPv6 - Tunneled Ping
6. MK - Advanced Analysis Lab 8f - IPX Exploit
7. MK - IP Service Scan
8. Covert Channels-ping-example5.

Welcome to my World....

Key Network Forensics Questions to Ask

1. What damage has been done?
2. Who was the intruder and how did they penetrate the existing security precautions?
3. What did they do? - (Did the intruder leave anything such as a new user account, a Trojan horse or perhaps some new type of Worm or Bot software behind?)
4. Is there sufficient data to analyze and reproduce the attack and verify the fix will work?

For This to Work - Normal or Abnormal?

Source	Destination	Protocol	Length	Src Port	Dst Port	Info
Micro-St_70:13:b7	IPv6mcast_00:00:00:	SSDP	208	51760	1900	M-SEARCH * HTTP/1.1
Micro-St_70:13:b7	IPv6mcast_00:00:00:	SSDP	208	51760	1900	M-SEARCH * HTTP/1.1
Micro-St_70:13:b7	Netgear_52:9e:a0	DNS	71	58501	53	Standard query A www.cnn.com
Netgear_52:9e:a0	Micro-St_70:13:b7	DNS	288	53	58501	Standard query response A 157.166.255.19
Micro-St_70:13:b7	Netgear_52:9e:a0	TCP	66	65045	80	65045 > 80 [SYN] Seq=419029810 Win=8192 L
Netgear_52:9e:a0	Micro-St_70:13:b7	TCP	66	80	65045	80 > 65045 [SYN, ACK] Seq=1914813027 Ack=
Micro-St_70:13:b7	Netgear_52:9e:a0	TCP	54	65045	80	65045 > 80 [ACK] Seq=419029811 Ack=191481
Micro-St_70:13:b7	Netgear_52:9e:a0	TCP	1448	65045	80	[TCP segment of a reassembled PDU]
Micro-St_70:13:b7	Netgear_52:9e:a0	TCP	1448	65045	80	[TCP segment of a reassembled PDU]
Netgear_52:9e:a0	Micro-St_70:13:b7	TCP	60	80	65045	80 > 65045 [ACK] Seq=1914813028 Ack=41903
Micro-St_70:13:b7	Netgear_52:9e:a0	HTTP	1194	65045	80	GET / HTTP/1.1
Netgear_52:9e:a0	Micro-St_70:13:b7	TCP	60	80	65045	80 > 65045 [ACK] Seq=1914813028 Ack=41903
Netgear_52:9e:a0	Micro-St_70:13:b7	TCP	60	80	65045	80 > 65045 [ACK] Seq=1914813028 Ack=41903
Netgear_52:9e:a0	Micro-St_70:13:b7	TCP	1448	80	65045	[TCP segment of a reassembled PDU]
Netgear_52:9e:a0	Micro-St_70:1					eassembled PDU]
Micro-St_70:13:b7	Netgear_52:9e					q=419033739 Ack=191481
Netgear_52:9e:a0	Micro-St_70:1					eassembled PDU]
Netgear_52:9e:a0	Micro-St_70:1					eassembled PDU]
Micro-St_70:13:b7	Netgear_52:9e					q=419033739 Ack=191481
Netgear_52:9e:a0	Micro-St_70:1					eassembled PDU]
Netgear_52:9e:a0	Micro-St_70:1					eassembled PDU]

Forensics Analysis Tip: Be familiar with the expected or Baseline behavior of protocols before trying to identify suspect behavior!

The Key – Reference / Baseline Files

- How can you recognize suspicious behavior unless you understand the expected behavior of a protocol?
- This is where the use of known-good reference or baseline files becomes important!
  - Reference files of standard network activities
  - Samples of network device behavior
  - Many devices, Scanning tools, Exploits, Hackers have specific signatures or patterns that can be used to identify a specific behavior

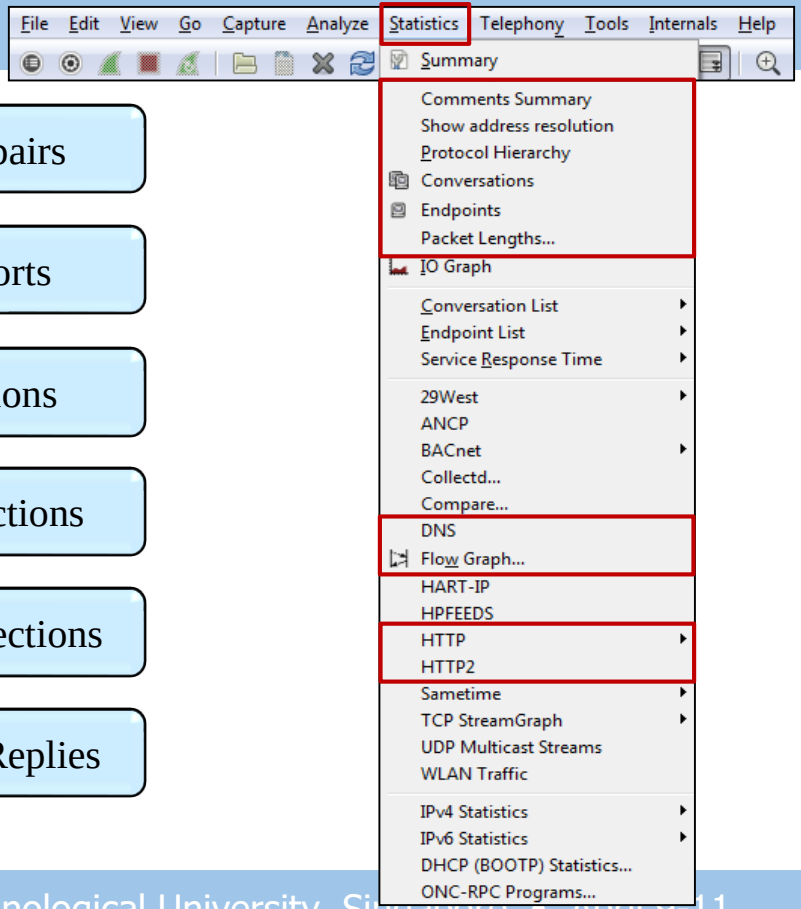
So…
Where do I Get Samples to Start With?

- http://packetlife.net/captures/
- http://www.pcapr.net
- http://www.netresec.com/?page=PcapFiles
- https://wiki.wireshark.org/SampleCaptures
- http://ambitwire.com/useful-links/public-pcap-repositories/link/public-pcap-repositories-ambitwires-ultimate-collection
- http://contagiodump.blogspot.nl/2013/04/collection-of-pcap-files-from-malware.html
- https://www.evilfingers.com/repository/pcaps.php
- https://www.bro.org/community/traces.html
- http://www.secrepo.com/

Forensics Analysis Tip: For specific requests, email me! Phill.shade@gmail.com

What Should I Look For?

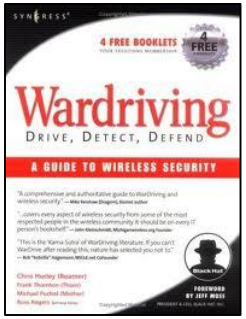
- Unusual communication pairs
- Unusual protocols and ports
- Excessive failed connections
- Suspicious inbound connections
- Suspicious Outbound Connections
- Suspicious DNS Queries / Replies

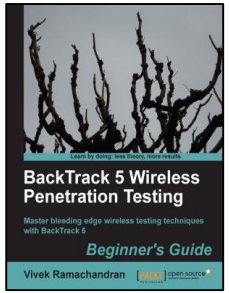


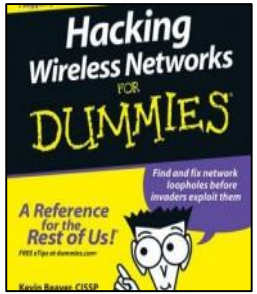
Let's Have Some Fun...

#1 - First We Need Some Tools…

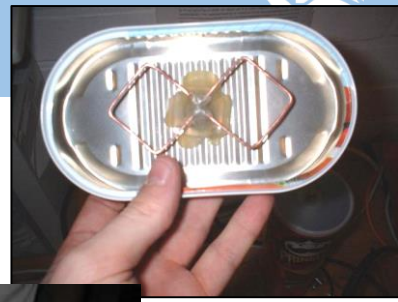
- Portable computer
  - Capture device such as AirPcap
  - Wireless card
- Software
  - Wireless Network analysis Tool
    - Wireshark
    - Airsnort
    - NetStumbler
    - Kismet
    - Air-Jack (and variants)
  - Vendor-provided "discovery and configuration" tools
    - Cisco Aironet Utilities

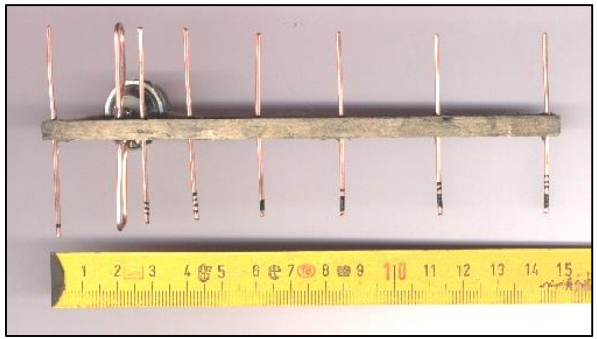




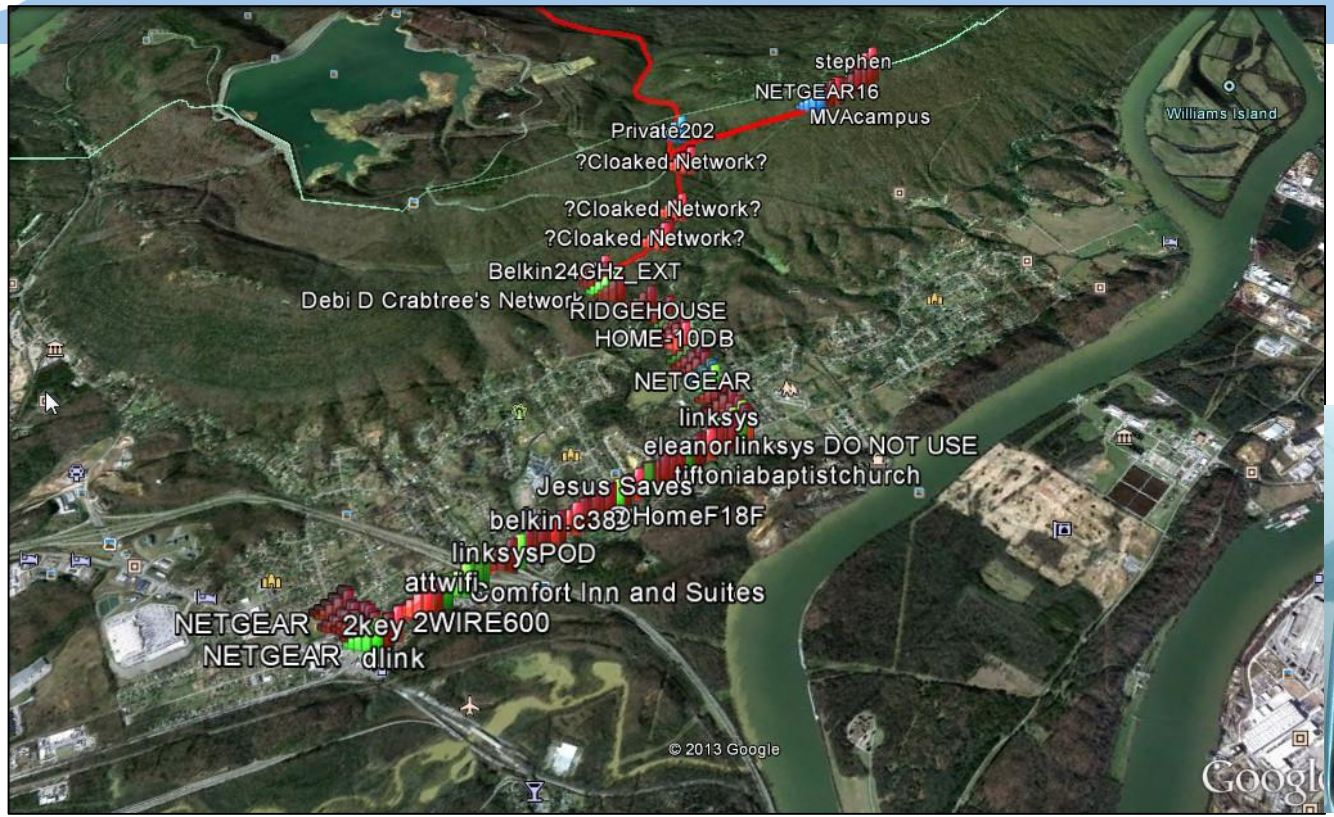


#2 - Now We Need an Antenna…





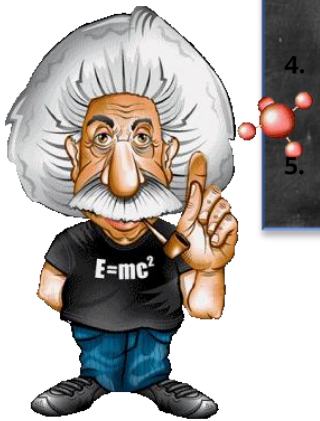
#3 - Now We Need a Target...



Follow Along in the Pcap:

MK - Forensics Case Study #4

Layer 2 - Case Study: Man-in-the-Middle Attack



Setting the Stage...

1. A major network analysis vendor had been working on a key project for two years
2. One week prior to product launch, a competitor trademarked the primary and secondary names for the product
3. Company was forced to research, develop, and produce an entirely new marketing campaign, literature, and product documentation
4. A forensics investigation aided by the company's data recorders revealed that the software company had been "Man-in-the-Middle" victimized
5. Cost to company was in excess of $4,000,000 USD

Scene of the Crime...

Forensic Reconstruction of the Crime...

Before Intrusion

No Encryption

No Encryption

After Intrusion

Dual-Radio Access Point

ARP Poison in Progress

No.	Source	Destination	Time	Length	Protocol	Info
990	IntelCor_ac:b1:5e	IntelCor_ac:b1:3e	137.161139	60	ARP	Who has 192.168.60.3? Tell 192.168.60.1
991	IntelCor_ac:b1:5e	IntelCor_ac:b1:3e	137.161139	60	ARP	Who has 192.168.60.3? Tell 192.168.60.1
992	IntelCor_ac:b1:5e	IntelCor_ac:b1:3e	137.161139	60	ARP	Who has 192.168.60.3? Tell 192.168.60.1
993	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
994	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
995	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
996	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
997	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
998	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
999	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
1000	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
1001	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
1002	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
1003	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
1004	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
1005	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
1006	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
1007	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
1008	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl

The device IntelCor_ac:b1:5e is attempting to trick the Projector (CiscoInc_cd-fe-do) into thinking it is the client while making the client (IntelCor_ac:b1:3e) think it is the Projector.

Results of the Investigation…

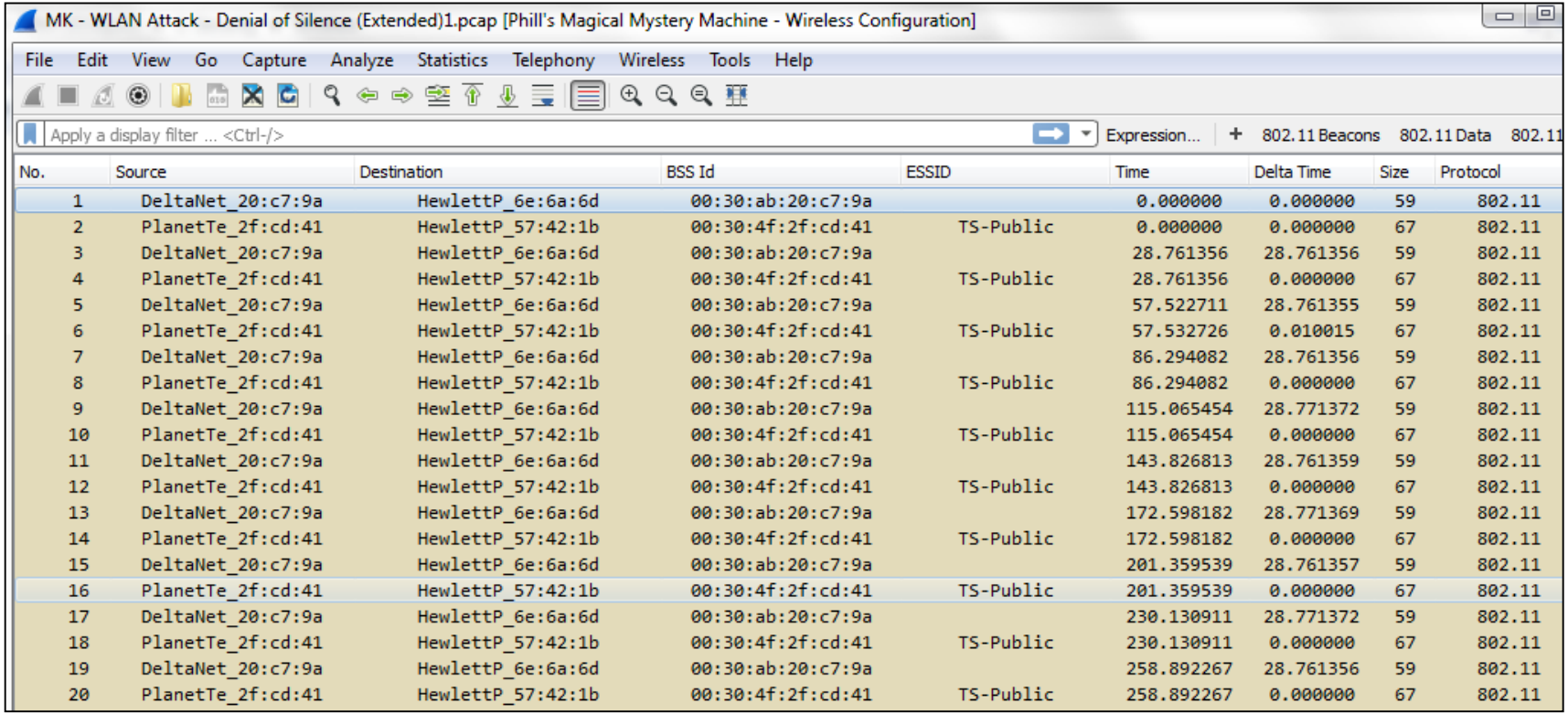
The results of the internal Forensic Investigation revealed several findings:

1. The original Wired Projector in the executive conference room had been replaced with an unauthorized WiFi model (that did not support any type of NAC or encryption)
2. Encryption was switched off on the presenters laptop to enable connecting to the WiFi projector
3. Rogue Access point was located outside conference room in a tree!

Follow Along in the Pcap:

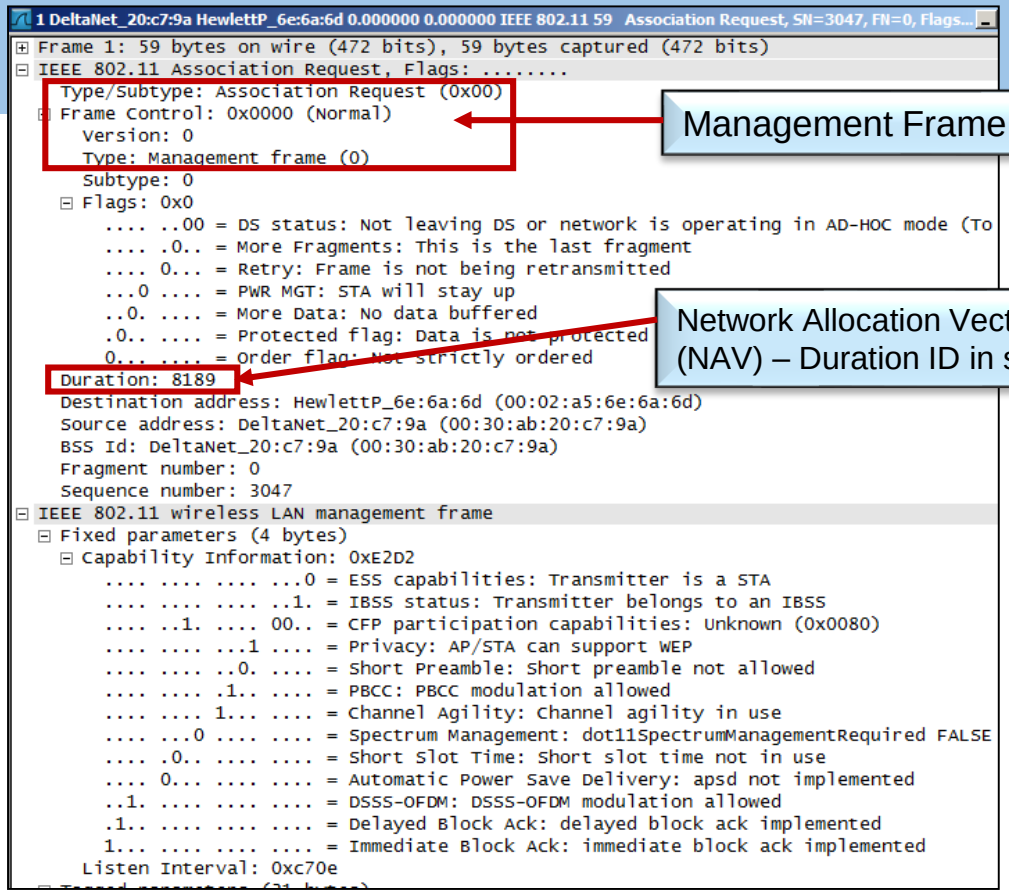
MK - WiFi - Attack - Denial of Silence (Extended)

WiFi Layer 1 - Denial of Silence Attack



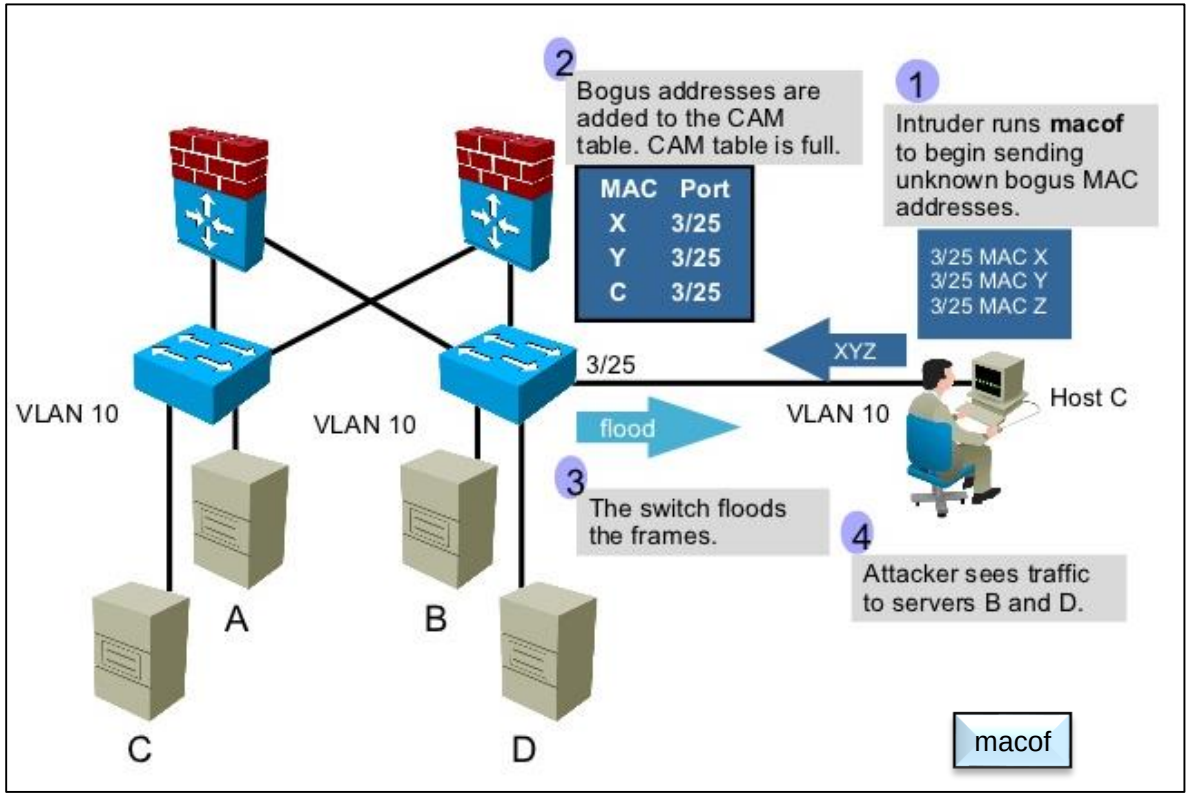
No.	Source	Destination	BSS Id	ESSID	Time	Delta Time	Size	Protocol
1	DeltaNet_20:c7:9a	HewlettP_6e:6a:6d	00:30:ab:20:c7:9a		0.000000	0.000000	59	802.11
2	PlanetTe_2f:cd:41	HewlettP_57:42:1b	00:30:4f:2f:cd:41	TS-Public	0.000000	0.000000	67	802.11
3	DeltaNet_20:c7:9a	HewlettP_6e:6a:6d	00:30:ab:20:c7:9a		28.761356	28.761356	59	802.11
4	PlanetTe_2f:cd:41	HewlettP_57:42:1b	00:30:4f:2f:cd:41	TS-Public	28.761356	0.000000	67	802.11
5	DeltaNet_20:c7:9a	HewlettP_6e:6a:6d	00:30:ab:20:c7:9a		57.522711	28.761355	59	802.11
6	PlanetTe_2f:cd:41	HewlettP_57:42:1b	00:30:4f:2f:cd:41	TS-Public	57.532726	0.010015	67	802.11
7	DeltaNet_20:c7:9a	HewlettP_6e:6a:6d	00:30:ab:20:c7:9a		86.294082	28.761356	59	802.11
8	PlanetTe_2f:cd:41	HewlettP_57:42:1b	00:30:4f:2f:cd:41	TS-Public	86.294082	0.000000	67	802.11
9	DeltaNet_20:c7:9a	HewlettP_6e:6a:6d	00:30:ab:20:c7:9a		115.065454	28.771372	59	802.11
10	PlanetTe_2f:cd:41	HewlettP_57:42:1b	00:30:4f:2f:cd:41	TS-Public	115.065454	0.000000	67	802.11
11	DeltaNet_20:c7:9a	HewlettP_6e:6a:6d	00:30:ab:20:c7:9a		143.826813	28.761359	59	802.11
12	PlanetTe_2f:cd:41	HewlettP_57:42:1b	00:30:4f:2f:cd:41	TS-Public	143.826813	0.000000	67	802.11
13	DeltaNet_20:c7:9a	HewlettP_6e:6a:6d	00:30:ab:20:c7:9a		172.598182	28.771369	59	802.11
14	PlanetTe_2f:cd:41	HewlettP_57:42:1b	00:30:4f:2f:cd:41	TS-Public	172.598182	0.000000	67	802.11
15	DeltaNet_20:c7:9a	HewlettP_6e:6a:6d	00:30:ab:20:c7:9a		201.359539	28.761357	59	802.11
16	PlanetTe_2f:cd:41	HewlettP_57:42:1b	00:30:4f:2f:cd:41	TS-Public	201.359539	0.000000	67	802.11
17	DeltaNet_20:c7:9a	HewlettP_6e:6a:6d	00:30:ab:20:c7:9a		230.130911	28.771372	59	802.11
18	PlanetTe_2f:cd:41	HewlettP_57:42:1b	00:30:4f:2f:cd:41	TS-Public	230.130911	0.000000	67	802.11
19	DeltaNet_20:c7:9a	HewlettP_6e:6a:6d	00:30:ab:20:c7:9a		258.892267	28.761356	59	802.11
20	PlanetTe_2f:cd:41	HewlettP_57:42:1b	00:30:4f:2f:cd:41	TS-Public	258.892267	0.000000	67	802.11

WiFi Attack – Denial of Silence Details

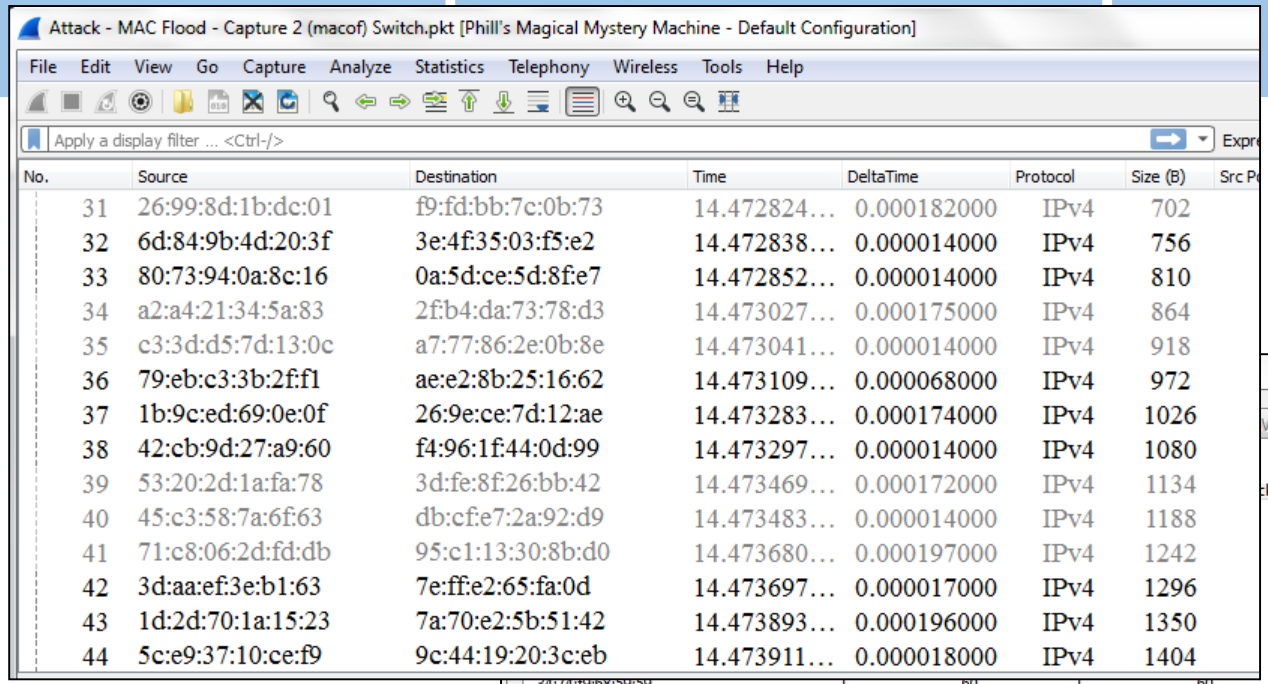


Follow Along in the Pcap:
Attack - MAC Flood - Capture 2 (macof) Switch

Layer 2 - MAC / CAM Table Overflow Attacks



Sample macof Pcap



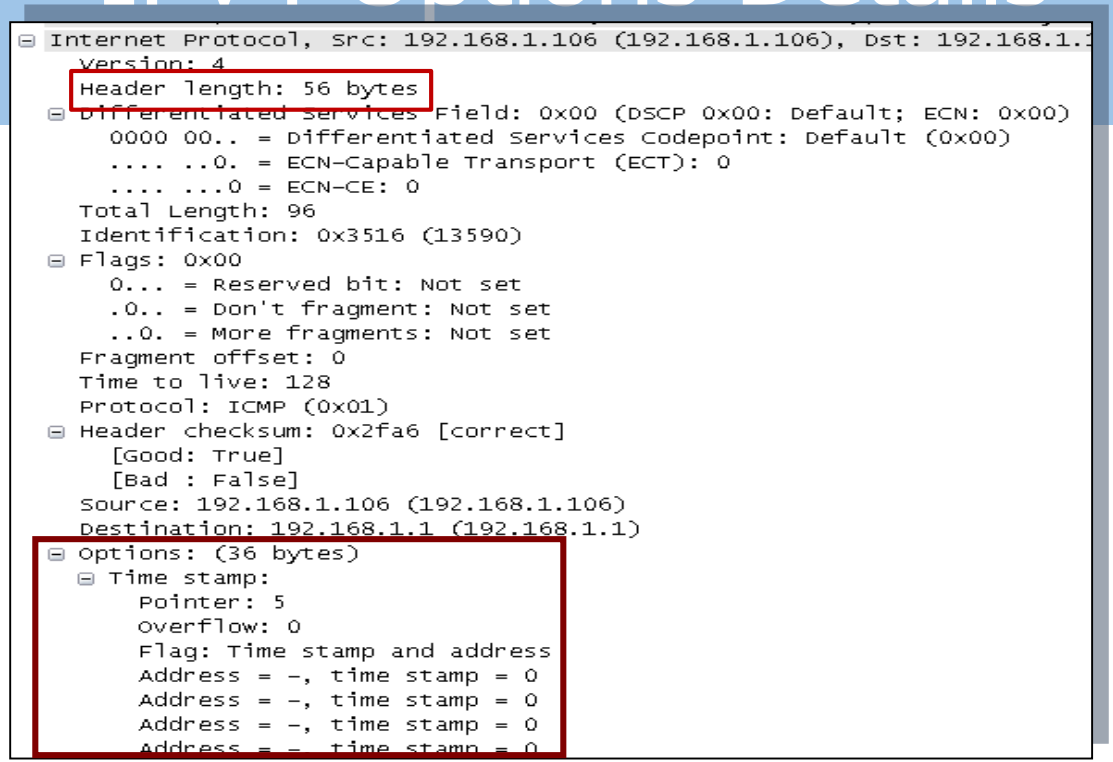
Follow Along in the Pcap:
MK - Advanced Analysis Lab 8c / e / 9d

Layer 3 - IPv4 Options

- Default length of the IP header is 20 bytes (Greater than 20 bytes indicates the presence of IP options)
  - Many options have been present since the early days of IP and continue to be added.
    - Most are rare and few protocols take advantage of them– one of the few protocols that does is IGMP
    - Many of these options can be generated via the DOS ping command – Type 'ping -?' for a list of options
  - Some of the options lend themselves to exploit potential

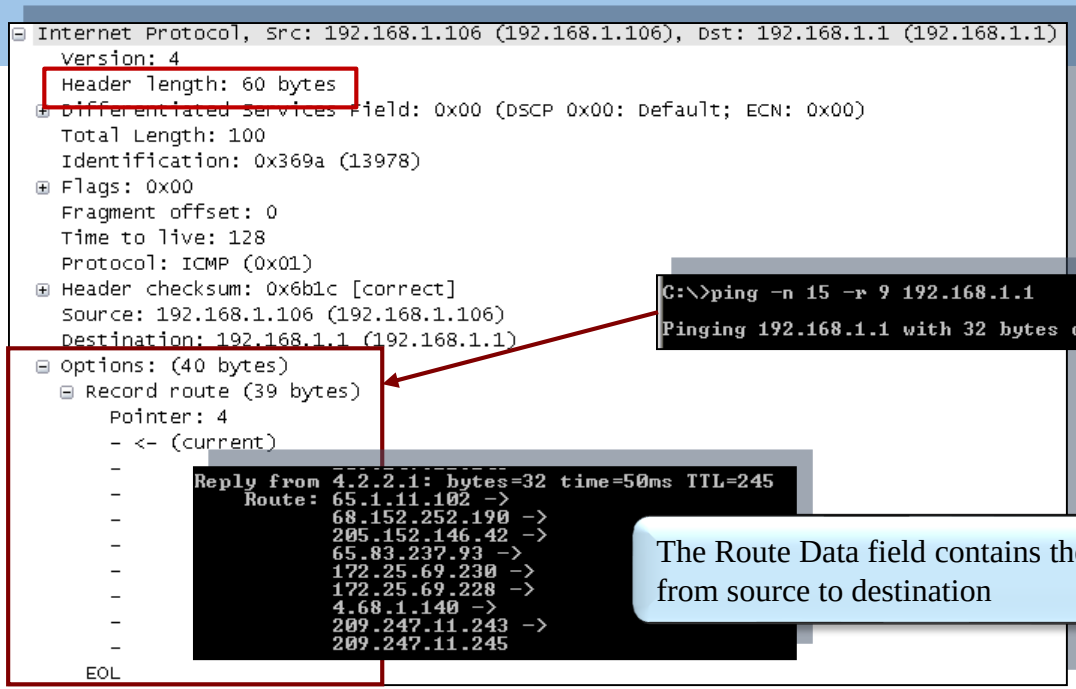
```
C:\>ping -?

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] target_name

Options:
    -t              Ping the specified host until stopped.
                    To see statistics and continue - type Control-Break;
                    To stop - type Control-C.
    -a              Resolve addresses to hostnames.
    -n count        Number of echo requests to send.
    -l size         Send buffer size.
    -f              Set Don't Fragment flag in packet.
    -i TTL          Time To Live.
    -v TOS          Type Of Service.
    -r count        Record route for count hops.
    -s count        Timestamp for count hops.
    -j host-list    Loose source route along host-list.
    -k host-list    Strict source route along host-list.
    -w timeout      Timeout in milliseconds to wait for each reply.
```

IPv4 Options Details



Forensics Analysis Tip: IP options are very often used in exploits – although some exceptions include IGMP and other routing protocols

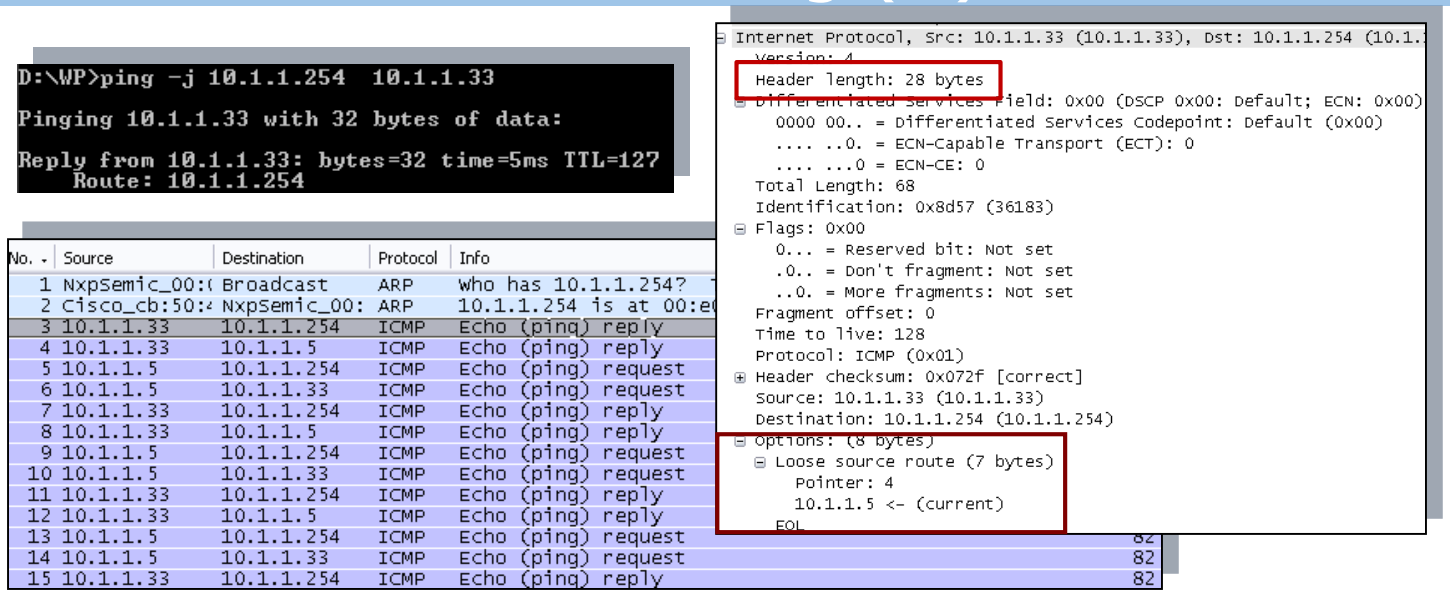
Layer 3 Exploit - Record Route - Ping (–r)



The Route Data field contains the list of routers from source to destination

Forensics Analysis Tip: Presence of IP Option: Record Route is a probable indication of a network under reconnaissance by an intruder with the goal of identifying routers to attack

Layer 3 Router Exploit – Loose / Strict Source Routing (-J)



Forensics Analysis Tip: This option allows a packet sender to override a router's normal forwarding process and potentially sneak packets past firewalls

Follow Along in the Pcap:

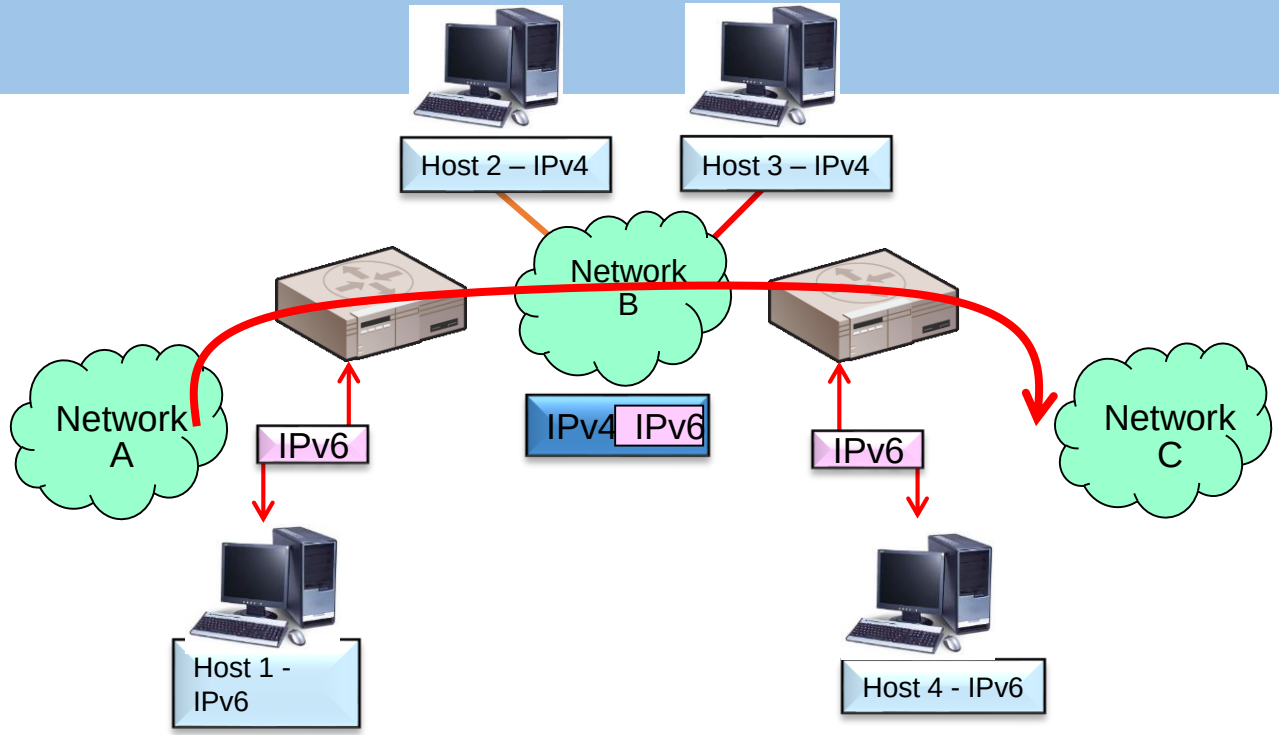
MK - Sample - IPv4 - IPv6 - Tunneled Ping

Layer 3 - Emerging IPv6 Trends

- Exhaustion of available IPv4 addresses in February 2011 forced many IP Address changes:
  - Significant increase in the use of Network Address Translation (NAT) and related use of "Private" IPv4 addressing
  - Most applications and devices have migrated to IPv6
  - Most Operating Systems now enable IPv6 compatibility as a default (dual stack)
    - Windows XP pro + / Linux Redhat 2.4+ / etc…

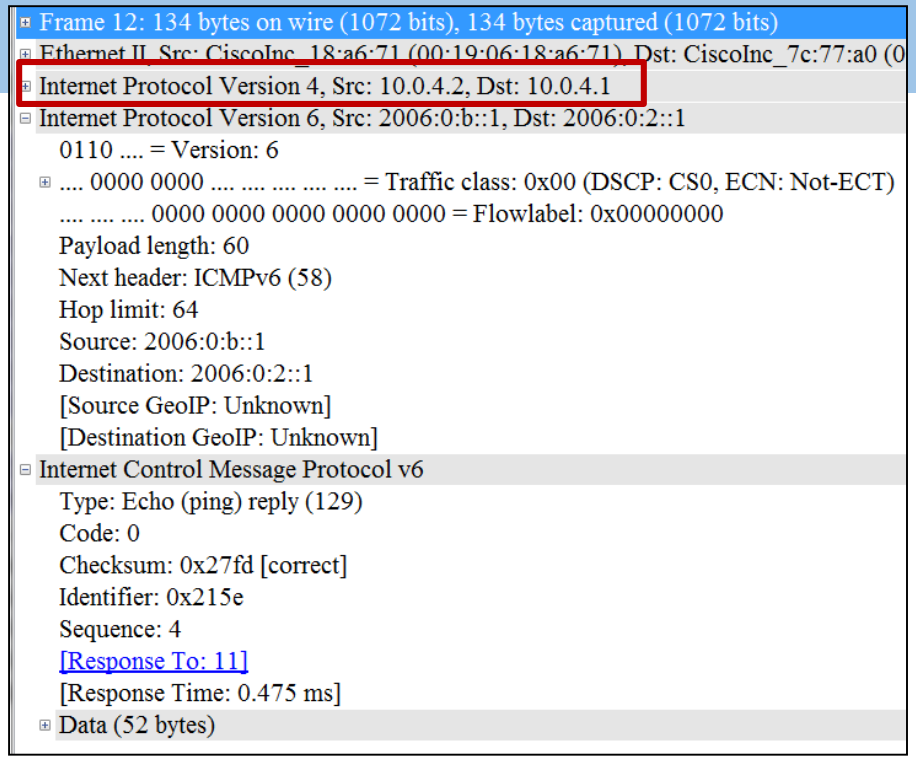
- Criminals / Hackers elements of the Internet have embraced IPv6 in a large part due to the perceived unfamiliarity of Law Enforcement community as well as the shortcomings of many of the current generation of LE tools
  - New Attacks and Exploits are emerging to take advantage of this

Layer 3 - Interfacing IPv4 with IPv6: Tunneling



Note: IPv6 packets must be encapsulated before traversing the IPv4 network

Layer 3 Exploit – IPv6 Tunnel Attack



Forensics Analysis Tip: Since IPv6 tunnels over IPv4 are transparent, the best way to identify their use within a network is by setting a series of capture filters on a network analyzer located within the firewall or DMZ

Follow Along in the Pcap:

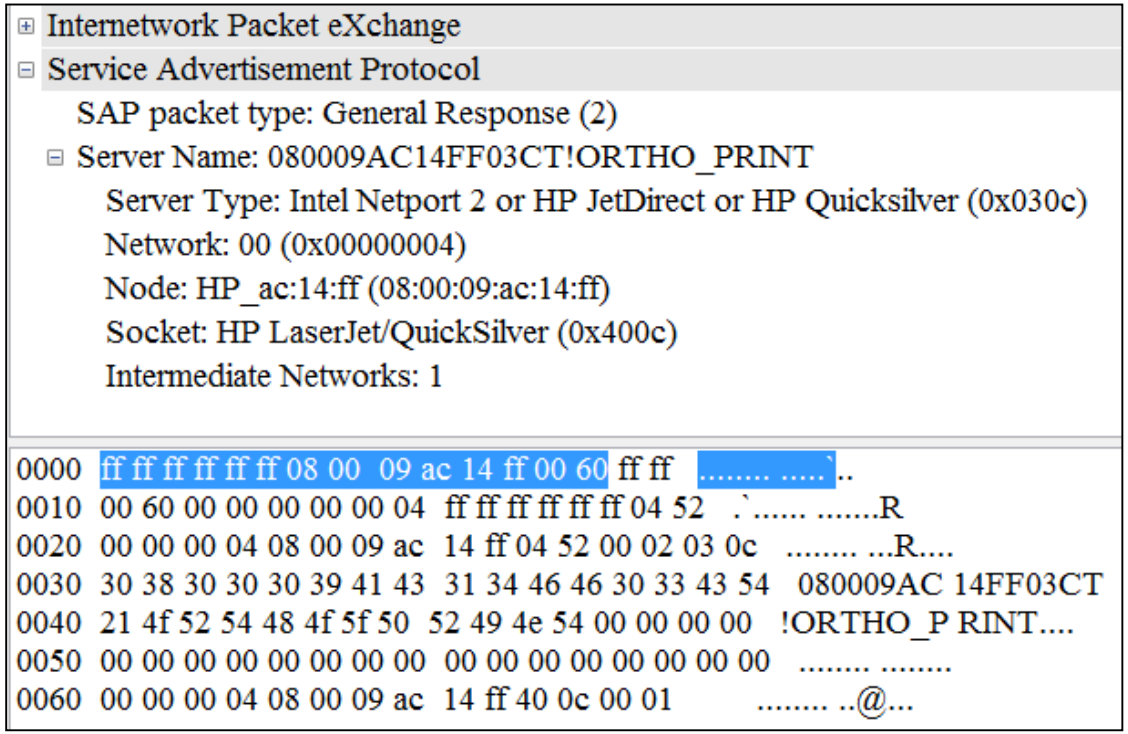
MK - Advanced Analysis Lab 8f

Layer 3 - Overview of IPX SAP

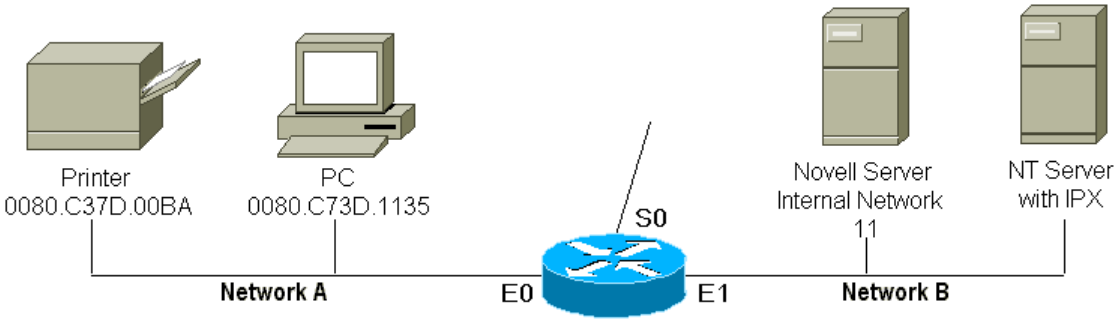
- Service Advertising Protocol (SAP) is included in the IPX protocol

- Used to make the process of adding and removing services dynamic in IPX enabled network
  - As devices join or leave the network, they may advertise their services as joining or leaving the network using SAP

Layer 3 - IPX SAP Header - Details



Layer 3 - IPX SAP in Operation




```
IPX Routing  0000.0C34.E923

interface ethernet 0
   ipx network A

interface ethernet 1
   ipx network B
```

Device	Network	Node
Printer	A	0080.C73D.00BA
PC	A	0080.C73D.1135
RTR-E0	A	0000.0C34.C923
RTR-E1	B	0000.0C29.DCFA
Novell Server (Int)	11	0000.0000.0001
Novell Server (Ext)	B	0000.1B3D.5678

Layer 3 - IPX SAP Exploits

- Compromise IPX SAP enabled devices (such as Printers and Servers) to inject malware from inside the network
- Spoof IPX / SAP enabled printers to steal network or printer traffic
  - Man-in-the-Middle
- Use IPX SAP enabled devices as basis for a Escalation of Privileges attack

Follow Along in the Challenge Pcap:

MK - IP Service Scan

Follow Along in the Challenge Pcap:
Covert Channels-ping-example

Questions and Answers / Discussion

Instructor Contact Information

Phill Shade: phill.shade@gmail.com

LinkedIn: Phill “Sherlock” Shade

Merlion’s Keep Consulting: merlions.keep@gmail.com

International: info@cybersecurityinstitute.eu

Merlion’s Keep Consulting & Training

Packets Never Lie


LOUNGE BAR
Thank You!