Wireless: network forensics unplugged

Network Security and Forensics

Common wireless devices

- AM/FM radios
- Cordless phones
- Cell phones
- Bluetooth headsets
- Infrared devices, such as TV remotes
- Wireless doorbells
- Zigbee devices, such as HVAC, thermostat, lighting, and electrical controls
- Wi-Fi (802.11)—LAN networking over RF
- WiMAX (802.16)—“last-mile” broadband2

Cases involving wireless networks

- Recover a stolen laptop by tracking it on the wireless network.
- Identify rogue wireless access points that have been installed by insiders for convenience or to bypass enterprise security.
- Investigate malicious or inappropriate activity that occurred via a wireless network.
- Investigate attacks on the wireless network itself, including denial-of-service, encryption cracking, and authentication bypass attacks.

IEEE Layer 2 protocol series

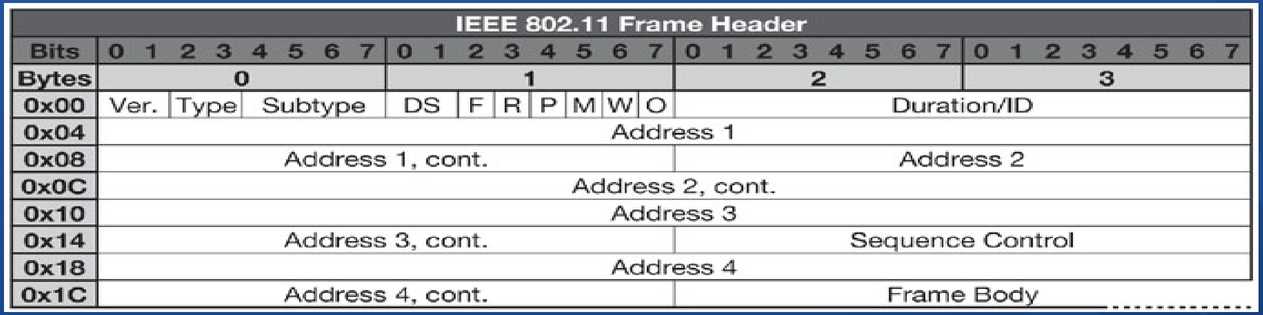
- 802 series
  - 802.3 (Ethernet)
  - 802.1q (trunking)
  - 802.1X (LAN based authentication)
  - 802.11 (Wi-Fi)
    - 2.4 GHz
    - 3.7 GHz
    - 5 GHz
- RF has different characteristic than copper, requires different protocol

802.11 frame types

- Three types
  - Management Frames—Govern communications between stations, except flow control;
  - Control Frames—Support flow control over a variably available medium (such as RF);
  - Data Frames—Encapsulate the Layer 3+ data that moves between stations actively engaged in communication on a wireless network

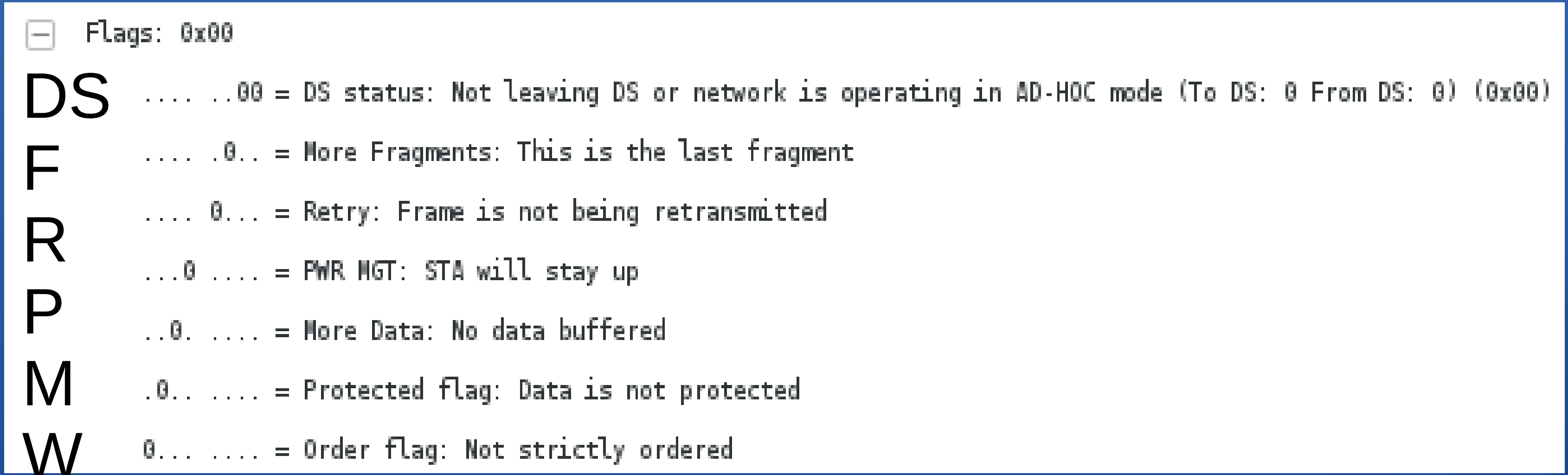
Management frames

- Type 0
- Coordinate communication
- Forensic benefit
  - Not encrypted
  - MAC addresses
  - Basic Service Set Identification (BSSID)
  - Service Set Identifiers (SSIDs)
  - Often point of attacks:
  - WEP cracking
  - Evil Twin



<table>
<tr><th colspan="33">IEEE 802.11 Frame Header</th></tr>
<tr><th>Bits</th><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th></tr>
<tr><th>Bytes</th><th colspan="8">0</th><th colspan="8">1</th><th colspan="8">2</th><th colspan="8">3</th></tr>
<tr><td>0x00</td><td colspan="2">Ver.</td><td colspan="2">Type</td><td colspan="4">Subtype</td><td colspan="2">DS</td><td>F</td><td>R</td><td>P</td><td>M</td><td>W</td><td>O</td><td colspan="16">Duration/ID</td></tr>
<tr><td>0x04</td><td colspan="32">Address 1</td></tr>
<tr><td>0x08</td><td colspan="16">Address 1, cont.</td><td colspan="16">Address 2</td></tr>
<tr><td>0x0C</td><td colspan="32">Address 2, cont.</td></tr>
<tr><td>0x10</td><td colspan="32">Address 3</td></tr>
<tr><td>0x14</td><td colspan="16">Address 3, cont.</td><td colspan="16">Sequence Control</td></tr>
<tr><td>0x18</td><td colspan="32">Address 4</td></tr>
<tr><td>0x1C</td><td colspan="16">Address 4, cont.</td><td colspan="16">Frame Body</td></tr>
</table>

Flags



```
⊟ Flags: 0x00
  .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x00)
  .... .0.. = More Fragments: This is the last fragment
  .... 0... = Retry: Frame is not being retransmitted
  ...0 .... = PWR MGT: STA will stay up
  ..0. .... = More Data: No data buffered
  .0.. .... = Protected flag: Data is not protected
  0... .... = Order flag: Not strictly ordered
```

DS
F
R
P
M
W
O

Management frame subtypes

- 0x0 — Association Request
- 0x1 — Association Response
  - Status Code: 0x0000 — Successful
- 0x4 — Probe Request
- 0x5 — Probe Response
- 0xA — Disassociation
- 0xB — Authentication
- 0xC — Deauthentication

Control frames

- Type 1
- Manage the flow of traffic
- Problem of the hidden node addressed here
  - 0x1B—Request-to-send (RTS)
  - 0x1C—Clear-to-send (CTS)
  - 0x1D—Acknowledgment

Data frame

- Type 2
- Actual data
  - Includes encapsulated higher-layer protocols
- Subtypes examples
  - 4 = null function
  - No data
  - 0 = data

802.11 frame analysis

- Endianness
  - Big-endian
  - Most significant byte represented, stored or transmitted first
  - Little-endian
  - Least significant byte represented, stored or transmitted first

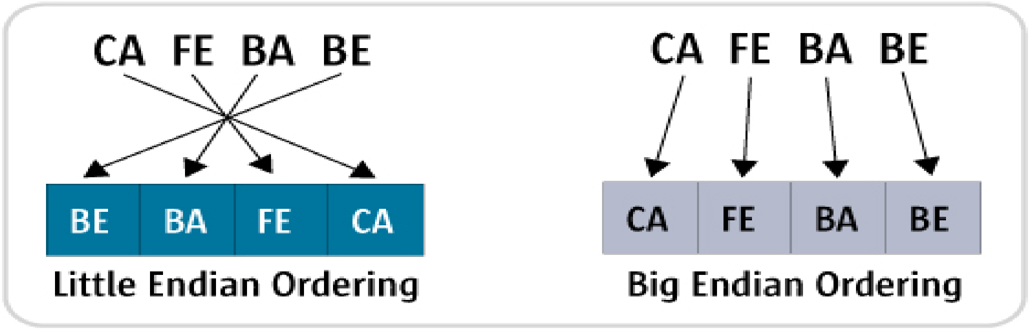
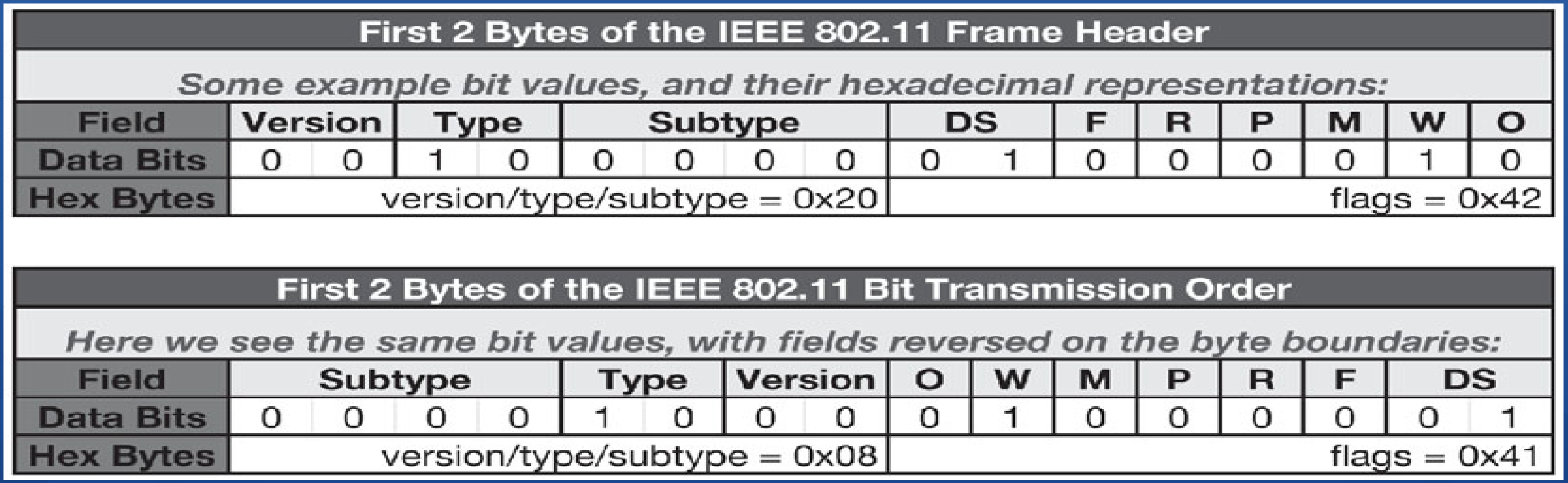


Figure 2 Byte ordering

802.11 Mixed-endian

- Bit order within each individual data-field – big endian
- Fields themselves – little endian

Top – written protocol Bottom – actual transmitted order



First 2 Bytes of the IEEE 802.11 Frame Header

Some example bit values, and their hexadecimal representations:

Field	Version		Type		Subtype				DS		F	R	P	M	W	O
Data Bits	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0
Hex Bytes	version/type/subtype = 0x20								flags = 0x42							

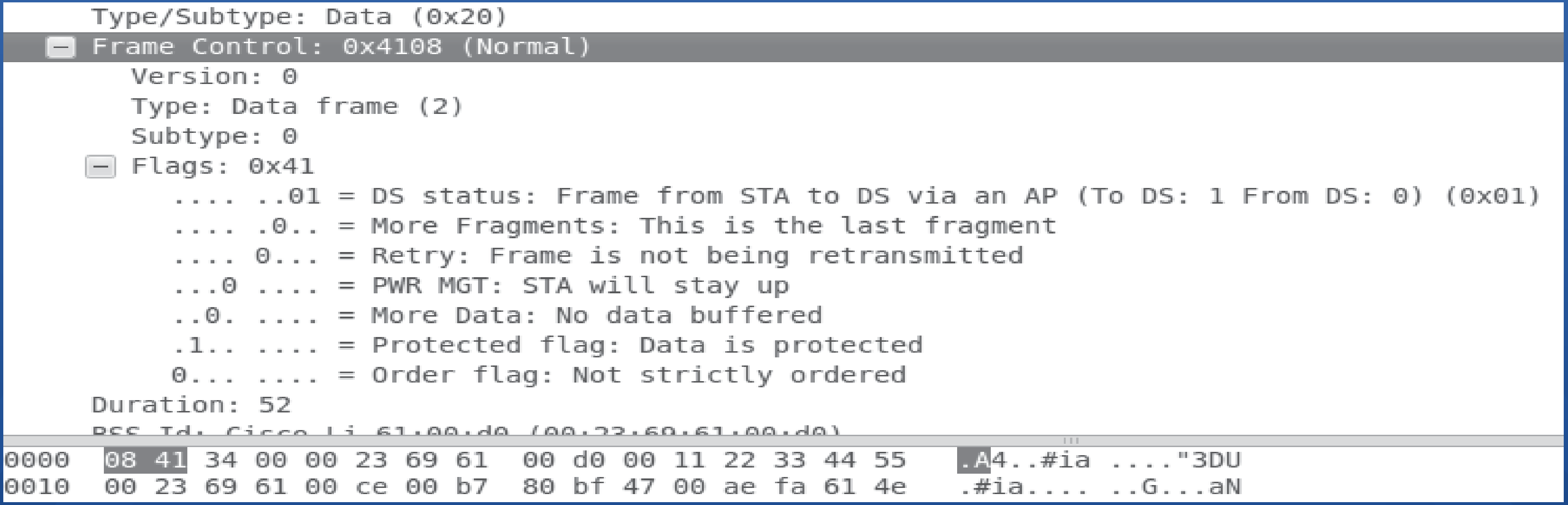
First 2 Bytes of the IEEE 802.11 Bit Transmission Order

Here we see the same bit values, with fields reversed on the byte boundaries:

Field	Subtype				Type		Version		O	W	M	P	R	F	DS	
Data Bits	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	1
Hex Bytes	version/type/subtype = 0x08								flags = 0x41							

Wireshark example

- Wireshark will correctly interpret the first byte– 0x20 (0b00100000)
- The raw data show the actual order – 0x08 (0b00001000)



```
     Type/Subtype: Data (0x20)
   ⊟ Frame Control: 0x4108 (Normal)
       Version: 0
       Type: Data frame (2)
       Subtype: 0
     ⊟ Flags: 0x41
           .... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x01)
           .... .0.. = More Fragments: This is the last fragment
           .... 0... = Retry: Frame is not being retransmitted
           ...0 .... = PWR MGT: STA will stay up
           ..0. .... = More Data: No data buffered
           .1.. .... = Protected flag: Data is protected
           0... .... = Order flag: Not strictly ordered
     Duration: 52
     BSS Id: Cisco_Li_61:00:d0 (00:23:69:61:00:d0)

0000  08 41 34 00 00 23 69 61  00 d0 00 11 22 33 44 55   .A4..#ia ...."3DU
0010  00 23 69 61 00 ce 00 b7  80 bf 47 00 ae fa 61 4e   .#ia.... ..G...aN
```

Wired equivalent privacy (WEP)

- WEP
  - Private
  - "Shared" secret ??
- WEP is broken
  - Aircrack-ng – brute force attack
- Why learn it?
  - Legacy Equipment
  - Modern equipment with legacy support
- Encrypted?
  - Private bit – Confidentiality of data frames needed
  - Protected bit to 1 – WEP, WPA, WPA2 used

TKIP, AES, WPA and WPA2

- Wi-Fi Protected Access (WPA)
  - Uses key rotation – Temporal Key Integrity Protocol (TKIP)
  - Broken – preshared Keys
- WPA2
  - Used Counter Mode with CBC-MAC Protocol (CCMP) mode of AES
  - Difficult to break
- Both WPA and WPA2
  - Robust security networks (RSN) – to improve security
  - Management frame includes:
    - Beacons
    - Association Requests
    - Reassociation Requests
    - Probe Requests

802.1X

- Module, extensible authentication framework regardless of physical medium
- Framework for low-layer authentication
- Extensible Authentication Protocol (EAP)
  - Improves PPP
  - PPP is still commonly used
    - PPPoE
    - EV-DO
    - CHAP
    - PAP
  - Based on central authentication store
  - EAP- Transport Layer Security (EAP-TLS)
  - Protected EAP (PEAP)
  - Lightweight EAP (LEAP)
- Much more likely to have an audit trail

WAPs

- Layer 2 device
- All stations have access to signals
  - Interception easy
- Logging capabilities
- MAC address filtering
- DHCP service
- Routers
- SNMP
- Special case in investigation
  - Nearly unlimited access like a hub
  - Can include Layer 3 routing and Layer 4 NATing

Why investigate?

- Locally stored logs of connection attempts, authentication successes and failures, and other local WAP activity.
- Logs to track the physical movements of a wireless client throughout a building or campus.
- Configuration may provide insight regarding how an attacker gained access to the network.
- Configuration could be modified by an unauthorized party as part of an attack. Equivalent to compromising WAP.
  - Example – login to a switch and then write libraries which can mimic user action

Type of Access Points

- Enterprise access points
  - Support for IEEE 802.11a/b/g/n
  - Centralized authentication
  - Audit of access logs (local and central)
  - Station location tracking
  - Performance monitoring capabilities
- Consumer End Access Points
  - Less facilities than enterprise

WAP evidence

Volatile

- History of connections by MAC address
- List of IPs associated with MACs
- Historical logs of wireless events (access requests, key rotation, etc.)
- History of client signal strength (can help identify geographic location)
- Routing tables
- Packet counts and statistics
- ARP table (MAC address to IP address mappings)
- DHCP lease assignments
- Access control lists
- I/O memory
- Running configuration
- Processor memory
- Flow data and related statistics

Persistent

- Operating system image
- Boot loader
- Startup configuration files

Off-System

- Aggregation
- storage

Spectrum analysis

- IEEE supports three frequencies:
  - 2.4 GHz (802.11b/g/n)
  - Country based issues
    - US only allows uses of channels 1 – 11
    - Japan allows uses through 14
  - 3.6 GHz (802.11y)
  - 5 GHz (802.11a/h/j/n)
- Greenfield (GF) mode
  - 802.11n devices operating in GF are not visible to 802.11a/b/g
- Software
  - Netsurveyor
  - Kismet

Passive evidence acquisition

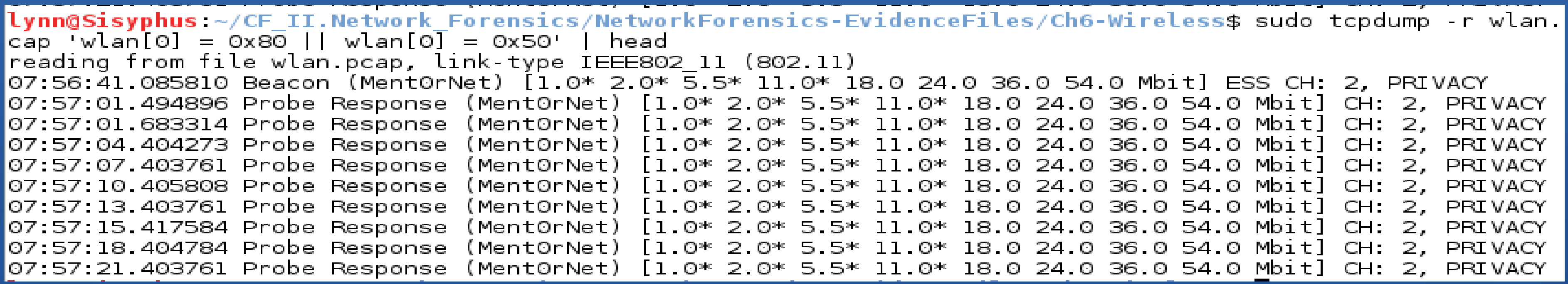
- Wireless card must have Monitor mode
  - A separate card used only for Monitor mode is best
  -
- Info that can be gathered
  - Broadcast SSIDs
  - WAP MAC addresses
  - Supported encryption / authentication algorithms
  - Associated client MAC addresses

Efficient analysis

- Are there any beacons in the wireless traffic?
- Are there any probe responses?
- Can you find all the BSSIDs/SSIDs from authenticated/associated traffic?
- Can you find malicious traffic? What does that look like?
- Is the captured traffic encrypted using WEP/WPA? Is anyone trying to break the encryption?

Tcpdump and tshark

- Use BPF filters and wireless protocol knowledge
- Find WAPs
  - ‘wlan[0] = 0x80’

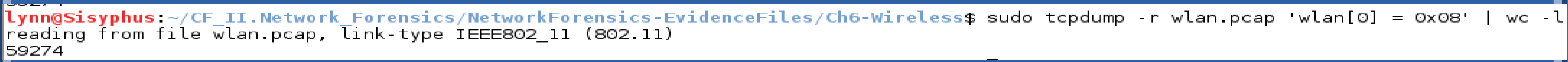


```
lynn@Sisyphus:~/CF_II.Network_Forensics/NetworkForensics-EvidenceFiles/Ch6-Wireless$ sudo tcpdump -r wlan.
cap 'wlan[0] = 0x80 || wlan[0] = 0x50' | head
reading from file wlan.pcap, link-type IEEE802_11 (802.11)
07:56:41.085810 Beacon (MentOrNet) [1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] ESS CH: 2, PRIVACY
07:57:01.494896 Probe Response (MentOrNet) [1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] CH: 2, PRIVACY
07:57:01.683314 Probe Response (MentOrNet) [1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] CH: 2, PRIVACY
07:57:04.404273 Probe Response (MentOrNet) [1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] CH: 2, PRIVACY
07:57:07.403761 Probe Response (MentOrNet) [1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] CH: 2, PRIVACY
07:57:10.405808 Probe Response (MentOrNet) [1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] CH: 2, PRIVACY
07:57:13.403761 Probe Response (MentOrNet) [1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] CH: 2, PRIVACY
07:57:15.417584 Probe Response (MentOrNet) [1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] CH: 2, PRIVACY
07:57:18.404784 Probe Response (MentOrNet) [1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] CH: 2, PRIVACY
07:57:21.403761 Probe Response (MentOrNet) [1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] CH: 2, PRIVACY
```

- Encrypted data frames
  - 'wlan [0] = 0x08 and wlan [1] & 0x40 = 0x40 '

Count Data Frames

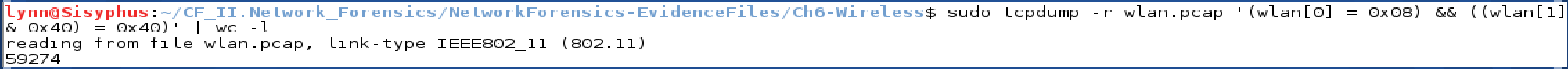
First Byte – Version 0, Type 2, Subtype 0 = 00 10 0000 (as parsed)
= 0000 10 00 (as sent) = 0x08



```
lynn@Sisyphus:~/CF_II.Network_Forensics/NetworkForensics-EvidenceFiles/Ch6-Wireless$ sudo tcpdump -r wlan.pcap 'wlan[0] = 0x08' | wc -l
reading from file wlan.pcap, link-type IEEE802_11 (802.11)
59274
```

Count Encrypted Frames

Second Byte – Protected bit set = xx x x x x 1 x (as parsed)
= x 1 x x x x xx (as sent) & 0 1 0 0 0 0 00 = 0x40



```
lynn@Sisyphus:~/CF_II.Network_Forensics/NetworkForensics-EvidenceFiles/Ch6-Wireless$ sudo tcpdump -r wlan.pcap '(wlan[0] = 0x08) && ((wlan[1]
& 0x40) = 0x40)' | wc -l
reading from file wlan.pcap, link-type IEEE802_11 (802.11)
59274
```

http://www.wireshark.org/docs/dfref/w/wlan_mgt.html

Common attacks

- Sniffing
  - An attacker eavesdrops on the network
- Rogue Wireless Access Points
  - Unauthorized wireless devices that extend the local network, often for an end-user’s convenience
  - Changing the channel
  - Illegal use of channel 14
  - Greenfield mode
  - Wireless Port knocking
    - Installing root kits and waiting for particular sequence of ports to be opened.

Common attacks continued

- The Evil Twin Attack
  - An attacker sets up a WAP with the same SSID as a legitimate WLAN
  - Man-in-the-middle attack
- WEP Cracking
  - An attacker attempts to recover the WEP encryption key to gain unauthorized access to a WEP-encrypted network.
  - Forced generation of large amounts of initialization vectors (IV) until right one is created

Locating wireless devices

- Strategies:
  1. Gather station descriptors, such as MAC addresses, which can help provide a physical description so that you know what to look for
     - MAC address has a manufacturer field – could be spoofed
  2. For clients, identify the WAP that the station is associated with (by SSID)
  3. Leverage commercial enterprise wireless mapping software
  4. Poll the device’s signal strength
     - Closest more powerful signal
  5. Triangulate on the signal

Signal Strength

- Received Signal Strength Indication (RSSI) and Transmit (Tx) Rate
  - Sent only if the capture tool supplies the data
  - Wireshark can be configured as such by editing user preferences
- NetStumbler
  - Windows tool (XP, Vistumbler is a Win 7 option)
  - Presence can be detected
  - Supports GPS integration
  - Useful for wardriving and warwalking
- KisMet
- KisMac
- SkyHook
  - Wireless Positioning Systems

Signal strength continued again

- KisMAC
- Commercial Enterprise Tools
  - Aruba and Cisco
- Skyhook
  - Wireless Positioning System (WPS)
  - Apples “Locate Me” feature
  - Eye-Fi SD cards

- https://github.com/chrissanders/packets
  Use the pcap files given by Chris Sanders for studying tshark wireshark tcpdump etc. in detail.

Works Cited

Davidoff, S., & Ham, J. (2012). *Network Forensics Tracking Hackers Through Cyberspace.* Boston: Prentice Hall.