UNIVERSITY OF ZAGREB

FACULTY OF ELECTRICAL ENGINEERING AND COMPUTING

Subject: Computer Forensics

SEMINAR

Wireless Forensics

Hristina Marošević

Mentor: *doc. dr. sc. Predrag Pale*

Zagreb, January, 2017

Contents

1. Introduction 3
1.1. Main components, function and architecture of the wireless networks 3
1.2. IEEE standards 4
1.3. Operational modes 5
1.4. Frames 5
1.5. Security 6
1.5.1. 802.11 security protocols 6
2. Technical challenges for WiFi traffic acquisition 6
2.1. Dealing with the wireless physical medium 7
2.2. Mobile clients and roaming 7
2.3. Wireless traffic features and extend 8
2.4. Performance issues capturing wireless traffic 9
2.5. Wireless network forensics tools 10
2.5.1. Tool design requirements and best practices for wireless forensics 10
2.5.2. Open source and commercial tools 11
3. Wireless network forensics 12
3.1. Wireless attacks 12
3.2. Wireless network forensics investigation 14
4. Conclusion 17
5. References 18

1. Introduction

1.1. Main components, functions and architecture of the wireless network

A wireless network interface card (adapter) is a device, called a *station*, providing the network physical layer over a radio link to another station.
An *access point* (AP) is a station that provides frame distribution service to stations associated with it. The AP itself is typically connected by wire to a LAN.

One station can communicate with the chosen AP, once it has authenticated and associated with it [1].

An 802.11 LAN is based on a cellular architecture where the system is subdivided into cells, where each cell (called Basic Service Set or BSS according to the 802.11 nomenclature, that is the access point itself and all the stations connected to it) is controlled by the Base Station (BS), also known as access point (AP).
The station and AP each contain a network interface that has a Media Access Control (MAC) address, just as wired network cards do. This address is a world-wide-unique 48-bit number, assigned to it at the time of manufacture.

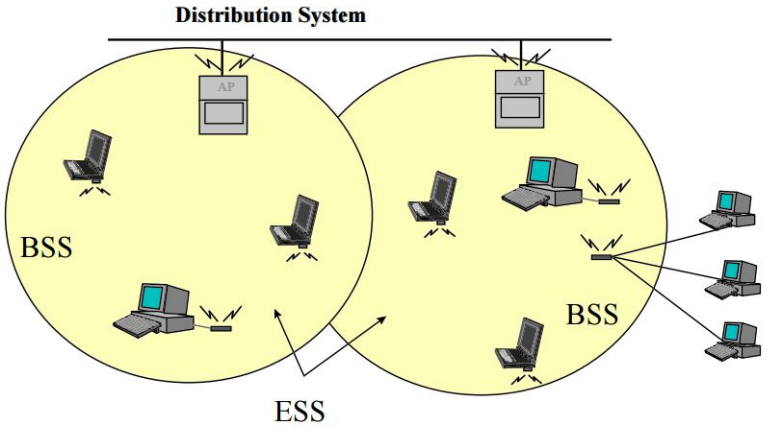
- The MAC address of the AP is known as BSSID (Basic Service Set ID)

Even though that a Wireless LAN may be formed by a single cell, with a single AP, most installation are formed by several cells where the APs are connected through some kind of backbone (called Distribution System, DS) typically Ethernet (and in some cases wireless itself).
The whole interconnected Wireless LAN including the different cells, their respective APs and the DS is seen to the upper layers of the OSI model as a single 802 network and is called (in the standard) Extended Service Set (ESS).

- each network/ESS has its own 0 to 32 byte long SSID (Service Set Identifier)/ESSID (Extended Service Set Identifier) that is commonly called a network name.
- The SSID is used to segment the airwaves for usage. If two wireless networks are physically close, the SSIDs label the respective networks, and allow the components of one network to ignore those of the other. SSIDs can also be mapped to virtual LANs; thus, some APs support multiple SSIDs.
- Unlike fully qualified host names (e.g., gamma.cs.wright.edu), SSIDs are not registered, and it is possible that two unrelated networks use the same SSID [2].

While moving one station can connect from one AP (BSS) to another AP (BSS) in the ESS.
The process of maintaining uninterrupted connection in this scenario is called roaming [2].

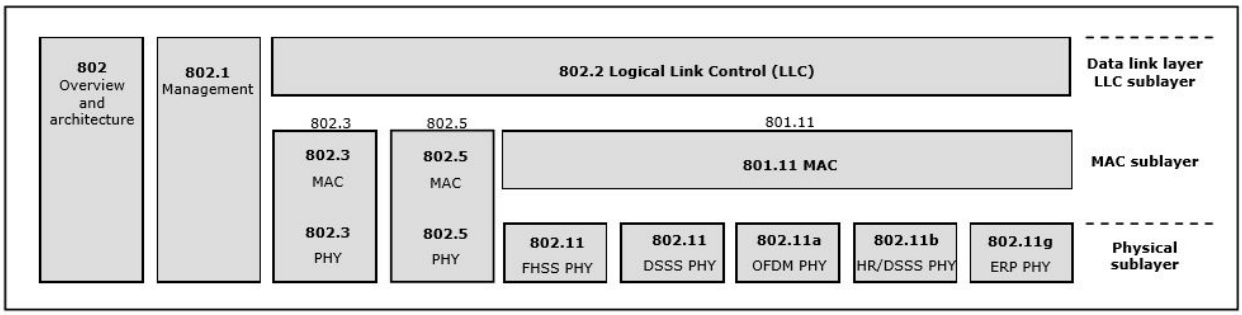
Picture 1 shows a typical 802.11 LAN with its components described previously.



Picture 1. Typical Wireless LAN architecture
Source:http://www.sss-mag.com/pdf/802_11tut.pdf

1.2. IEEE Standards [3]

IEEE 802.11 – otherwise known as the Wi-Fi standard – denotes a set of standards for wireless LANs. The original IEEE 802.11 standard, released in 1997, defines a common media access control (MAC) layer that supports the operation of all 802.11-based WLANs by performing core functions such as managing communications between radio network cards and access points. Subsequent amendments to 802.11 define specific physical (PHY) layers, such as 802.11b, 802.11g, or 802.11a. The physical layer defines the data transmission for the WLAN, using various modulation schemes.
The standards used on the data link and physical layer in wireless network are given on the picture below, Picture 2.



Picture 2. 802.11 data link and physical layers
Source:802.11 Wireless Networks, O'Reilly

Much of the impetus for standardization has come from the Wi-Fi Alliance, an organization of technology and service companies dedicated to the adoption of a single worldwide-accepted standard for high-speed wireless local area networking. In common usage, the term Wi-Fi has come to embrace the 802.11b, 802.11g, and 802.11a physical layer standards, and the products based on those standards.

The IEEE 802.11b standard is the most popular and widely implemented of the 802.11 family standards, for reasons including its early availability and the price of supported products.

- 2.4 GHz industrial, scientific, and medical (ISM) unlicensed frequency band
- 11 (US), 13 (Europe), 14 (Japan) channels separated by 5 MHz
- 3 non-overlapping channels
- Data rate: 11Mbps (real:4-5 Mbps)
- Modulation: DSSS
- Interference: microwave ovens, cordless phones, Bluetooth devices, wireless headsets, garage door openers, and other appliances – all of which use the same limited 2.4 GHz range

The IEEE 802.11g standard is a direct extension of 802.11b that extends the maximum data rate (signaling speed) to 54 Mbps, making it possible to serve up to five times as many users

- 2.4 GHz industrial, scientific, and medical (ISM) unlicensed frequency band
- 11 (US), 13 (Europe), 14 (Japan) channels separated by 5 MHz
- 3 non-overlapping channels
- Data rate: 54Mbps
- Modulation: DSSS/OFDM
- Interference: microwave ovens, cordless phones, Bluetooth devices, wireless headsets, garage door openers, and other appliances – all of which use the same limited 2.4 GHz range

The IEEE 802.11a standard provides the same 54 Mbps maximum data rate as 802.11g. But unlike 802.11b and 802.11g, the 802.11a standard operates in the 5 GHz ISM band.

- 5 GHz industrial, scientific, and medical (ISM) unlicensed frequency band
- 11 (US), 13 (Europe), 14 (Japan) channels separated by 5 MHz
- 19 non-overlapping channels
- Data rate: 54Mbps
- Modulation: OFDM
- 802.11a devices are not subject to interference that affects 802.11g and 802.11b devices, but they are still subject to interference from other products designed to use this 5 GHz ISM band

The draft 802.11n standard defines a new physical layer for increasing the throughput of wireless local area networks 802.11n is based on MIMO (multiple input/multiple output) OFDM technology, which allows the transmission of up to 100 Mbps over a much wider range than earlier versions. MIMO uses multiple transmitters and receivers to allow for increased throughput through spatial multiplexing and increased range

1.3. Operation modes

A wireless network operates in one of two modes [2].
In the *ad hoc* mode, each station is a peer to the other stations and communicates directly with other stations within the network which means that no AP is involved. All stations can send Beacon and Probe frames.

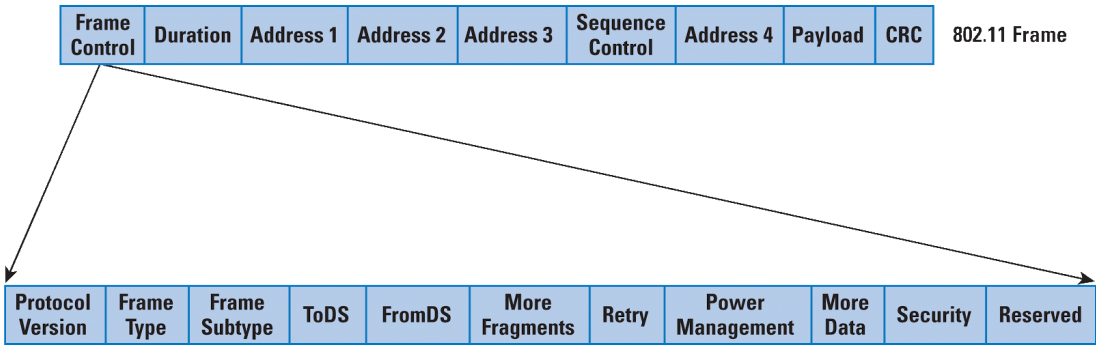
- the ad hoc mode stations form an Independent Basic Service Set (IBSS).

A station in the *infrastructure* mode communicates only with an AP. Basic Service Set (BSS) is a set of stations that are logically associated with each other and controlled by a single AP. Together they operate as a fully connected wireless network.

- The BSSID uniquely identifies each BSS.

1.4. Frames

Both the station and AP radiate and gather 802.11 frames as needed.
Most of the frames contain IP packets. The other frames are for the management and control of the wireless connection.
The structure of the 802.11 frame is shown on picture 3 [8].



Picture 3. 802.11 Frame
Source:http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-42/114-wifi.html

There are three classes of frames.

- The *management* frames establish and maintain communications. The are transmitted the same way as data frames to exchange management information, but are not forwarded to upper layers.
  These are of Association request, Association response, Reassociation request, Reassociation response, Probe request, Probe response, Beacon, Announcement traffic indication message, Disassociation, Authentication, Deauthentication types. The SSID is part of several of the management frames. Management messages are always sent in the clear, even when link encryption (WEP or WPA) is used, so the SSID is visible to anyone who can intercept these frames.
- The *control* frames help in the delivery of data and are used to control the access to the medium (e.g. RTS, CTS, ACK)
- The *data* frames encapsulate the OSI Network Layer packets. These contain the source and destination MAC address, the BSSID, and the TCP/IP datagram. The payload part of the datagram is WEP-encrypted [2].

1.5. Security

Once the station has found an AP and decided to join its BSS, it will go through the authentication process, which is the interchange of information between the AP and the station, where each site proves the knowledge of a given password.
When the station is authenticated, then it will start the association process, which is the exchange of information about the stations and BSS capabilities, and which allows the DSS to know about the current position of the station. Only after the association process is completed, a station is capable of transmitting and receiving data frames.

But using authentication does not automatically mean that the data traffic is encrypted too! [4]
- When data confidentiality is required the “Security” bit in the management frame is set to 1
- When WEP, WPA or WPA2 is used the “Protected” bit within the first byte offset of the 802.11 MAC framing is set to 1

1.5.1. 802.11 Security Protocols [6]

Initially, WEP (Wired Equivalent Privacy) was the only link-level security option defined in the 802.11 standard. Its main purpose was the protection of the confidentiality and integrity of the wireless network traffic. WEP was designed to provide comparable confidentiality to a traditional wired network, hence the name.
- Using RC4
- WEP key (62-128 bits; pseudo-random) = RC4 {IV (Initialization Vector, 24bits; dynamic; random) + Shared Secret(40-104bits)}

WPA (WiFi Protected Access) was introduced as an interim security enhancement over WEP while the 802.11i wireless security standard was being developed.
- Using TKIP (Temporal Key Integrity Protocol). 802.1x and MIC (Message Integrity Code)
- PSK (Pre-Shared Key) or Personal WPA
- Enterprise (using username/password combination and using authentication server to generate keys or certificates)

WPA2 is much better and more secure than WPA and has the same two modes as WPA. It is Based on the 802.11i wireless security standard, which was finalized in 2004.
- Using AES (Advanced Encryption Standard)
- PSK (Pre-Shared Key) or Personal
- Enterprise (using username/password combination)

2. Technical challenges for WiFi traffic acquisition

The main technical challenges associated to wireless forensics are due to the intrinsic nature of radio frequency (RF) communications and the complexity of the physical medium and the 802.11 specifications. The following sections focus on the major handicaps the forensic examiner, and his capture tools, must overcome.

2.1. Dealing with the wireless physical medium

The first wireless forensic tool consideration is that it **must support the 802.11 modulation** of the network to monitor; therefore, it is recommended that one **use 802.11 a/b/g multi-band wireless cards that support the three most common standards.**

Standard wireless equipment only contains a single radio component therefore, it is only capable of listening to a specific channel in a given moment.
Wireless tools have used a technique called channel hopping to scan the whole frequency spectrum and sample all the different channels, however, using this method the radio is only listening for a few milliseconds in each channel.

- when dealing with a single wireless access point, capturing traffic is not a challenge, because the access point transmits in a unique channel, so the analyst simply needs to configure its card to listen to that channel
- however, enterprise and large environments with multiple access points present a challenge for accurate traffic captures. Wireless forensics tools must be capable of capturing all the traffic from all the wireless networks in a given area when a suspect is located. Therefore, the tools need to **listen to all channels simultaneously.** The only way of accomplishing this goal is by having **as many radio devices as there are channels to monitor.**

Although laws and regulations specify the 802.11 channels allowed in every country or region, attackers don't follow the law.

- therefore, when talking about 802.11b/g networks, it is imperative for the forensic analyst to **collect traffic from all 14 channels available worldwide.**

Regulations also define the maximum transmission power (in mW or W) for 802.11 equipment, but again, attackers will break these limits.

- the analyst must **be prepared for this illegal usage, as well as for the newest wireless technologies, such as MIMO (802.11n)and WiMAX (802.16)**

2.2. Mobile clients and roaming

One of the major advantages wireless networks provide is client mobility, that is, the capability of moving around the wireless network range without losing the network connection. For large networks, this is mainly accomplished through roaming, a technique to fast switch from the current access point to the nearest one while sending and receiving data. This functionality presents complex challenges for wireless forensics.
Wireless clients roam from one access point to another once their network card determines that the former access point signal is too weak to continue transmitting and receiving data. These roaming events typically involve moving from one channel to another.

- if the wireless forensic tool used to capture data during roaming activities does not **monitor all channels, specifically the initial and final channels**, portions of the session will be lost, negatively affecting the evidence collected.

Additionally, the location of mobile wireless clients and the facility's physical layout directly influence from where the traffic can be captured. Occasionally, the location from where the forensic examiner is collecting traffic is no longer valid once the client moves, for example, to an opposite location inside a building. Sometimes, only one end of the communication can be collected.

The only place where the data can be accurately collected for a wireless infrastructure network (seeing both ends of the communication) is near the access point, but this is not a realistic scenario, especially when the network is conformed by multiple access points (the analyst cannot be in all them at the same time) or when wireless ad-hoc (client to client) networks are used.

- from a wireless forensic perspective this challenge can only be solved by **placing multiple traffic capture sensors around the facilities that must be monitored.** Having three or more sensors can also help to apply **triangulation methods to approximately locate the source of a transmission.**

2.3. Wireless traffic features and extent

When capturing wireless traffic it is important to consider its main characteristics, such as frames types, sizes, approximate number of frames and bandwidth requirements.

The **802.11 MTU (Maximum Transmission Unit) for data frames is 2304 bytes** (frame payload size before encryption).
Based on the encryption method use, the final payload size varies:

- WEP adds a header of 8 bytes for a total of 2312 bytes,
- WPA (TKIP) adds a header of 20 bytes for a total of 2324 bytes, and
- WPA2 (AES) adds a header of 16 bytes, for a total of 2320 bytes.

As an example, when using WEP, the maximum total frame size (payload + 802.11 header + trailer) is 2346 bytes (2312 + 30 + 4 bytes). This is the number reflected in the 802.11 specification, much bigger than the default MTU for Ethernet, 1500 bytes.

Additionally, the 802.11 specifications define three different types of frames required to manage the unreliable RF medium: control, management and data frames. The first two only exist on wireless networks, as opposed to wired networks, and **will influence the amount of data captured during the forensic activities.**

For example, due to synchronization requirements, wireless networks (specifically the access point) generate a special type of management frame called beacons. Commonly, each AP generates 10 beacons per second by default. This means that, for a single wireless network based on only one access point, the forensic examiner is going to collect 36000 frames per hour. The implications of these environment peculiarities from the performance and storage perspective must be considered in advance.

To exemplify all these peculiarities using a real-world scenario, Table 1 reflects the details and numbers obtained while collecting 802.11b/g data, from all 14 channels, using a 6dBi omnidirectional antenna. It corresponds to a case following a suspect by car, at low speeds (20-40 Km/h – 12-25 Mph), in a less crowded small town, mainly made of two or three-storey buildings and detached houses.

Wireless technology	802.11b/g (all 14 channels)
Capture time	25 minutes
Amount of data collected	74 Mbytes (~265,000 frames)
Wireless networks detected	60
Wireless networks taxonomy	12 Open (20%), 42 WEP (70%), 6 WPA (10%)
Wireless networks with data traffic	13
Wireless traffic taxonomy	25% Data, 39% Management, 36% Control

Table 1. Traffic capture statistics for a moving attacker scenario
Source:https://www.symantec.com/connect/articles/wireless-forensics-tapping-air-part-one

In the same scenario, another example associated to the static collection of traffic around the suspect facilities from the parking lot, provided the details of Table 2.

Wireless technology	802.11b/g (all 14 channels)
Capture time	5 minutes
Amount of data collected	24 Mbytes (~107,000 frames)
Wireless networks detected	24
Wireless networks taxonomy	4 Open (17%), 17 WEP (71%), 3 WPA (12%)
Wireless networks with data traffic	6
Wireless traffic taxonomy	6% Data, 53% Management, 41% Control

Table 2. Traffic capture statistics for a static scenario
Source:https://www.symantec.com/connect/articles/wireless-forensics-tapping-air-part-one

These two examples provide a rough estimation of the minimum amount of traffic you can find in a wireless forensics exercise, or around 200-300Mbytes/hour. Obviously, the requirements would increase tremendously in more densely populated locations, such as in major cities and downtown areas with dozens of multi-tenant buildings shared by multiple companies and individuals.

2.4. Performance issues capturing wireless traffic

From a hardware design perspective, **the wireless capture device must be able to accommodate the theoretical maximum throughput associated to all the communication channels**.

- by default, 802.11g networks can transmit at 54 Mbps rates, that is, an aggregated throughput of 756 Mbps (14 channels x 54 Mbps).

The device internal architecture bus, interconnecting all the wireless cards, can affect the tool performance and discard traffic, invalidating the evidence collected. To avoid that, **the computing architecture must support this maximum aggregated capacity**.

- as a reference, these are the maximum data rates for the most commonly used PC-based bus technologies available nowadays: PCI 2.2 (264 Mbps), USB 2.0 (480Mbps), CardBus (1056 Mbps), PCI-X (1064 Mbps), Express Card (2.5 Gbps) and PCI-X 2.0 (4.3 Gbps).

Not only the main bus, but other components, such as the memory bus or the disk interface and hard drives must support the previously mentioned data rate.

- as a reference, DDR2-667 SDRAM memory modules provide high data transfer up to 42 Gbps and current SATA disks support 1.5 Gbps data rates.

Based on a specific legal case, the analyst could be required to collect data from multiple domains, such as static locations, like office buildings or company facilities, the suspect's home, public areas such as hotels or airports, and moving locations, such as in a car prosecution.

- therefore, wireless forensics solutions require **large storage devices** to save all the data collected

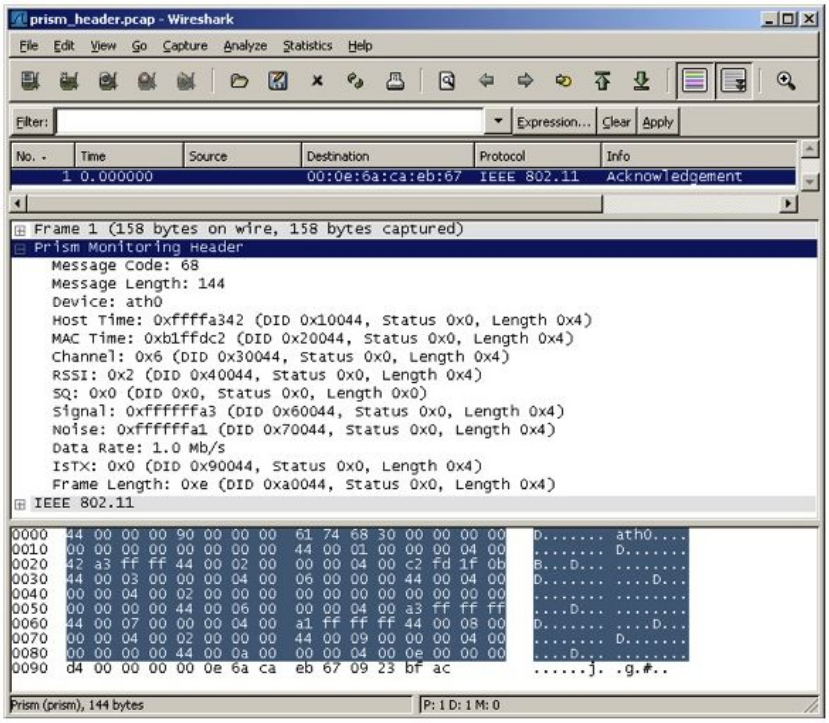
2.5. Wireless network forensics tools

2.5.1. Tool design requirements and best practices for wireless forensics

The following list summarizes some best practices, tips and tricks, and additional technical forensic considerations that should be evaluated when building or acquiring a wireless forensic tool or device for capturing 802.11 network traffic as legal evidence.

- The device should have 15 radio components (or cards) to be able to monitor all fourteen 802.11b/g channels and, at the same time, channel hop through the spectrum to identify new wireless networks (this being the purpose of the 15th radio).
- The use of a GPS (Geographical Positioning System) device can provide accurate timestamps and outdoor location capabilities, required to corroborate when and where the evidence (wireless traffic) was collected. Open-source implementations, such as gpsd, are commonly used for this purpose by wireless tools like Kismet for wardriving purposes. This GPS logging information is crucial during the analysis phase to match the data collected with the physical location of the capturing devices.
- From a forensic perspective, and in order to be able to consider the GPS data as evidence too, it is very relevant to measure and log the internals of when the GPS device is synchronized with the GPS satellites, that is, be able to show that the device is providing accurate information.
- The tool must capture all traffic without applying any capture filter, to not miss any real evidence. Only if regulations enforce it, filters would be applied during the capture phase to only collect traffic from specific access points or clients based on their MAC addresses (BSSID or station address). Filters can always be applied later, during the analysis phase, to focus on specific traffic flows.
- It is recommended that the wireless forensic tool be a completely passive device, not generating any traffic into the medium. This constraint can be enforced by design using a hardware attenuator that reduces or cancels the transmission power, or/and a one-way reception amplifier. This can also be enforced at the software level by placing the wireless cards in monitor mode, although it is important to denote that the latest Linux wireless cards drivers allow one to inject traffic in this “passive” mode.
- The device should provide an external antenna connector to expand the default wireless cards’ reception capabilities by using high-gain directional or omnidirectional antennas. The antennas increase the distance from where the RF signal, and therefore network traffic, can be collected. For high range reception, it is recommended to use, as a generic reference, omidirectional antennas of around 15dBi and directional parabolic grid antennas of around 24dBi.
- In some risky scenarios, it can be dangerous for the forensic examiner (and his physical integrity) to stay near or around the suspect area, so it would be desirable to have some kind of remote access capabilities to the capture device. For example, including an additional 802.11a interface to a pure 802.11b/g capture device allows accessing the system wirelessly and remotely without interferences. This remote management interface must be strongly secured so that the forensic device is not compromised, both from the wireless access perspective, and from the upper-layer protocols point of view, using SSH, SSL or IPSec to provide strong authentication and encryption.
- In order to collect additional information about the traffic, and what the estimated suspect location is, it is recommended to add specific signal strength information, in the form of the Prism monitoring header, when capturing wireless traffic.This additional header (see Picuture 4 below) adds 144 bytes, is generated by the wireless driver, and contains received signal strength (RSSI), capture device, channel, and other signal/noise quality information.

Although the signal information reported by the wireless cards cannot be accurately translated to the physical layout location due to multiple RF behaviors, such as reflection, refraction, diffraction or scattering, this information can be very useful to compare the different values collected during a capture session and map network traffic with signal properties.



Picture 4. Prism monitoring header through Wireshark
Source: https://www.symantec.com/connect/articles/wireless-forensics-tapping-air-part-one

- The tool should collect the traffic in the standard Pcap format (Packet CAPture, associated to the libpcap library), recognized by most commercial and open-source traffic capture and analysis tools.
- The wireless hardware (cards or radio components) used must have very good receive sensitivity (Rx), to increase the chance of collecting traffic even in the worst conditions. The best wireless cards in the market nowadays are capable of providing a Rx of -105 dBms at very low rates, such as the Atheros XR technology (-85 dBm is the reference value reflected in the IEEE 802.11 specification).
- The wireless output power is not relevant unless the tool implements some active transmission capabilities, such as when traffic is generated to increase the chance of obtaining the WEP key (covered in part two). Prior to running active actions, their legal implications must be evaluated.
- The physical characteristics of the multiple wireless hardware components limit the reception quality of the device. The internal device design should consider the usage of a high performance low noise reception amplifier to compensate the loss associated to all the cabling, the power splitter and the connectors linking all the different built-in cards.
- It is recommended to have advanced logging capabilities in the capture device itself, so that all the actions and steps executed in the device can be accurately tracked and used as evidence corroboration in the court of law. The integrity of these logging records should be assured through hashing algorithms (MD5 and SHA-1).
- Finally, all the data collected, specifically, the Pcap files and GPS information, must be cryptographically hashed once the capture session has been finalized, and apart from having a

repository of hash values, they should be included in the audit log too. This hashing information will help to preserve and verify the integrity of the evidence.

2.5.2. Open-source and commercial tools

The type of tool required for professional wireless forensics activities can be built using standard equipment, such as a common PC-architecture and commercial wireless network cards. However, a high-quality device that meets all the different requirements mentioned along this article would require a considerable design and implementation investment.

Nowadays there are also a couple of commercial tools that could be used for wireless forensics:

- The Janus Project is a commercial tool, presented at the Defcon 2006 conference, that contains 8 wireless cards for wireless scanning, data capture and encryption cracking.
  - this tool was conceived as a wireless traffic capture and cracking tool.
- The WLAN-14 Linux-based commercial device, from Aircapture, was designed as a pure wireless forensics tool for law enforcement and security officers to securely collect 802.11b/g wireless data. It offers 15 wireless cards, a GPS, one external antenna connector and support for hot-swappable disks.
  - this tool was conceived as a pure wireless forensic tool.

3. Wireless network forensics

The huge adoption of wireless technologies over recent years has placed wireless data (or Wi-Fi) networks, based on the 802.11 specifications, as one of the major attack vectors for organizations nowadays. Incident handlers and law enforcement have been forced to deal with the complexity associated with these technologies when managing and responding to security incidents.

Wireless Forensics is a discipline included within the computer forensic science, and specifically, within the network forensic field, and it's a term coined by Marcus Ranum in 1997. Its main goal is to provide the methodology and tools required to collect and analyze (wireless) network traffic that can be presented as valid digital evidence in a court of law. The evidence collected can correspond to plain data or, with the broad usage of Voice-over-IP (VoIP) technologies, especially over wireless, can include voice conversations.

The wireless forensic process involves capturing all data moving over the network and analyzing network events in order to uncover network anomalies, discover the source of security attacks, and investigate breaches on computers and wireless networks to determine whether they are or have been used for illegal or unauthorized activities.

When performing wireless forensics, the security analyst must follow the same general principles that apply to computer forensics: identify, preserve and analyze the evidence, in order to impartially report the findings and conclusions.

This chapter focuses on investigating wireless attacks.
It discusses the various types of wireless technologies available and the different types of attacks launched against them. It also covers how to investigate a wireless attack.

3.1. Wireless Attacks [7]

There are various kinds of wireless attacks. The following are some methods hackers use to facilitate wireless attacks:

- **Wardriving**: Wardriving is a technique hackers use to locate insecure wireless networks while driving around.
- **Warflying**: Similar to wardriving, warflying involves flying around in an aircraft, looking for open wireless networks.
- **Warchalking**: Warchalking involves using chalk to place a special symbol on a sidewalk or another surface to indicate a nearby wireless network that offers Internet access.

1. Passive attacks

A passive attack is a type of attack where an unauthorized user monitors communications to gather information.

For example, eavesdropping on network traffic is a passive attack.

- an eavesdropper can easily seize the network traffic using tools such as Network Monitor, Tcpdump, or AirSnort
- passive attacks are **difficult to detect and identify**
- passive attacks are often **symmetric**, meaning that the attacker can monitor the communication in both directions.
- Some other examples of passive attacks are traffic analysis and traffic monitoring.

2. Electronic emanations

Electronic emanations are the electromagnetic waves of radiation that electronic devices emit during their operation. Wireless technology is subject to these emanations. An attacker can intercept the emanations and use them to figure out how to gain the proper credentials to join a wireless network.

- the major problem is that **the administrator of the network cannot identify that the attacker has intercepted the signals.**

3. Active attacks

Active attacks on wireless networks are similar to those on wired networks, in which an attacker tries to alter or corrupt the data or services on a network.

These types of attacks include flooding, spoofing, and unauthorized access. The information that an attacker collects during a successful passive attack can make it easier for him or her to actively attack a network.

3.1. Denial of Service attack

Wireless systems are vulnerable to the same protocol-based DoS attacks that strike wired networks. They are also vulnerable to other types of DoS attacks, because the signals used to transmit data over the air can be easily disrupted. The main objective of DoS attacks is to deny access to network services and resources.

- it is **difficult to track such attacks on wireless networks**

Modes of attack. DoS attacks have varied modes of attacks that include consumption, alteration, and physical destruction of network components or resources. The following are some common modes of attack:

- *Consumption of resources*: This involves consuming the resources a system needs, including the following:
  - *Bandwidth*: An intruder can redirect packets to the network in order to consume all of the available bandwidth on the network.
  - *Memory*: This is normally accomplished by saving unnecessary e-mails, causing intentional errors, or sharing unimportant files and folders.
- *Alteration of resources or information*: Altering the configuration of a machine can prevent a user from being able to use it.

- *Physical destruction of the computer/network elements:* This type of attack concerns the destruction of the physical elements, such as computers and routers

Results of DoS attack. The most significant loss due to these attacks is the time and money that an organization loses while the services are unavailable.

3.2. Flooding

The goal of flooding is to degrade the performance of the network by directing unnecessary packets of data toward it. This may result in a loss of connection requests or a complete denial of service. Flooding is a multicasting technique wherein packets from one source are directed toward multiple destinations on the network.

4. Man-In-The-Middle attacks

A man-in-the middle (MITM) attack is when an intruder accesses information being transmitted between the sender and the receiver. The transmission proves to be insecure because the information is not encrypted. In such cases, there is a possibility of the intruder altering the data.

The following are the two types of MITM attacks:

1. *Eavesdropping*: Eavesdropping is a **passive attack technique**. The attacker intercepts data being transmitted between one system and another. Security mechanisms such as IPSec, SSH, and SSL help prevent eavesdropping.

2. *Manipulation*: Manipulation is an extended step of eavesdropping. In this type of man-in-the-middle attack, the attacker manipulates the data that he or she intercepts. This manipulation can be done using a technique such as ARP poisoning.

5. Hijacking and Modifying a Wireless Network

In a wireless network, TCP/IP packets go through switches, routers, and wireless access points. Each device looks at the destination IP address and checks for that address in its table of local IP addresses. This table is dynamically built up from traffic that passes through the device and from Address Resolution Protocol (ARP) notifications from devices joining the network. If the destination IP address is not in the device's table, it passes the address off to its default gateway. However, there is no authentication or verification of the validity of a packet that a device receives. A malicious user can send messages to routing devices and access points stating that his or her MAC address is associated with a known IP address. All traffic that goes through those devices that is intended for the hijacked IP address will instead go to the malicious user's machine.

6. Association of a Wireless Access Point and a Device

A wireless access point (WAP) is a node configured to allow wireless devices to access the local area network (LAN). WAPs are just plugged into a switch or into an Ethernet hub. An access point has its own range. When two or more access points are in an environment, the range overlaps to provide roaming.

The following two methods provide some level of security between a device and the WAP with which it is associated:

1. *MAC filtering*: The media access control (MAC) address is the 12-character (48 bits written in hexadecimal notation) unique hardware address of a particular system. The MAC address is used in the data-link layer of the network. **MAC filtering is used to restrict unauthorized users**. Only those devices with MAC addresses on the WAP's white list are allowed access to the network.

2. *Preshared key (PSK)* or *use of encryption*: The wireless device and the access point use a shared secret key. A **checksum is added to every packet transmitted over the network**. If the packet is cracked, then the value of the checksum changes, and it is easy to identify the intrusion. The transmitting device creates a packet-concentrated vector that is combined with the key to encrypt the packet. At the receiving end, the same key is used to decrypt the packet.

3.2. Wireless network forensics process [7]

The following are the steps involved in performing forensic investigations in a wireless environment:

1. Obtain a search warrant.
    - The investigator should ensure that the search warrant application addresses the on-site examination of all computers and wireless-related equipment. The investigator can perform forensic analysis only on those pieces of equipment specified in the warrant

2. Identify wireless devices.
    - The investigator needs to identify all the different wireless devices connected to the network. He or she needs to check the physical locations of the following wireless hardware:
      • Wireless routers
      • Wireless access points (and rogue access points, using tools like network stumbler or mini stumbler)
      The investigator can use the following techniques to find WAPs:
        - *Manual detection*: For manual detection, the investigator has to configure some sort of mobile device such as a handheld PC or laptop. To detect WAPs, the investigator has to physically visit the area where a WAP is likely to be. He or she can then use techniques such as wardriving or warflying to detect the WAPs. •
        - *Active wireless scanning technique:* The active scanning technique involves broadcasting a probe message and waiting for a response from devices in the range. This technique identifies many WAPs but obviously cannot find those WAPs that do not respond to the probe message.
        - *Passive wireless scanning technique*: The passive scanning technique identifies the presence of any wireless communication. Through this technique, an investigator can identify all active WAP connections, but he or she may not find a WAP that is not currently serving any devices

      A rogue access point is an **unauthorized access point in a wireless network**. Attackers typically deploy these access points **to sniff important data on the network**. Attackers can also use rogue access points **to hijack user sessions on the wireless network**.
        - An investigator can detect a rogue access point by following two steps:
          1. *Access point detection*: The investigator first needs to use one of the techniques for detecting a wireless access point to discover the access point on the network.
          2. *Verifying whether or not the access point is a rogue access point*: After identifying the access point in the network, the next step is to verify whether or not the identified access point is a rogue access point.
          To tell whether an access point is authorized, the investigator has to check the following:
            • MAC
            • SSID
            • Vendor
            • Media type
            • Channel
      • Wireless modems
      • Wireless network adapters
      • Repeaters
      • Hard drives
      • Antennas

3. Document the scene and maintain the chain of custody.

- The investigator should do the following at the scene:
  • Document all devices connected to the wireless network
  • Take photographs of all evidence
  • Document the state of each device during seizure
  • Maintain the chain of custody of documents, photographs, and evidence

4. Detect wireless connections.

- The investigator can detect wireless connection using scanning tools such as the following:
  • ClassicStumbler
  • MacStumbler
  • iStumbler
  • Airport Signal
  • Airfart
  • Kismet

5. Determine the wireless field's strength.

- The investigator can use a tool called Field Strength Meter (FSM) to determine the wireless field's strength. FSM is a software application that extends a conventional SSB receiver to allow an investigator to measure and calculate the field strength of radio signals or interference.
- The following are some of the features of FSM:
  • Measures true root-mean-square (RMS), quasipeak, and peak audio power
  • Calculates received RF power (RMS, quasipeak, and peak) in dBm
  • Calculates field strength (RMS, quasipeak, and peak) in dBuV/m
  • Extrapolates calculated field strengths to a normalized bandwidth for comparisons
  • Saves results to text files, e-mails, and Web transactions

6. Map wireless zones and hot spots.

- Once an investigator has detected all wireless connections and collected other information about the wireless networks involved in the crime, he or she can analyze all the information to prepare a static map of the wireless zones and hot spots. Investigators typically use tools such as Microsoft Visio to create these maps.

7. Connect to the wireless network.

- The following are methods for accessing a WAP:
  • Directly connecting to the wireless access point
  • Sniffing traffic between the access point and associated devices

8. Acquire and analyze wireless data.

- The investigator can capture wireless traffic using wireless network monitoring and sniffing tools such as Wireshark and Tcpdump.

Acquiring Other Data and Performing Analysis.

- The investigator should acquire the DHCP logs, firewall logs, and network logs. He or she can use tools like fwanalog and Firewall Analyzer to view the firewall log files.

- The investigator should check the following:
    - DHCP log files for issued IP addresses
    - Firewall log files for intrusions
    - Network log files for intrusion activities

The investigator can use tools like Hydra and Cain & Abel to crack the passwords on password-protected log files.

- The investigator should also analyze the registry on any Windows computers for information about any wireless devices the computer has used.

9. Generate a report.

The investigator's report should include the following:

- Name of the investigator
- List of wireless evidence
- Documents of the evidence and other supporting items
- List of tools used for investigation
- Devices and setup used in the examination
- Brief description of the examination steps
- Details about the findings:
    - Information about the files
    - Internet-related evidence
    - Data and image analysis
- Investigator's conclusion

4. Conclusion

Wireless technologies, and especially Wi-Fi, are here to stay and are expanding to new devices used with both harmless and malicious intent. The first part of this seminar has described wireless forensics as a discipline required to investigate security attacks and incidents through (and over) 802.11 wireless data networks.

The article has pointed out the challenges and the complexity associated with wireless traffic acquisition, and has provided design requirements, tool references and best practices for wireless forensics.

At the end of this seminar given are the main steps in doing the wireless network forensics. Once we have the right tools and required equipment, knowing the possible attacks we can do the network forensics investigation in the wireless environment following the steps in the wireless forensics process.

5. References

[1] Mateti, P. (2005) *Http://cecs.Wright.Edu/*. Available at: http://cecs.wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks.htm#_Toc77524644 (Accessed: 12 January 2017)
[2] Brenner, P. (1997) *Http://www.Sss-mag.Com/*. Available at: http://www.sss-mag.com/pdf/802_11tut.pdf (Accessed: 12 January 2017)
[3] HP Innovations. (2006) *Planning a Wireless Network*.
[4] Pale, P. (2017) *Wireless Forensics*.
[5] Siles, R. (2007) *Symantec*. Available at: https://www.symantec.com/connect/articles/wireless-forensics-tapping-air-part-one (Accessed: 12 January 2017).
[6] Carlos Wong, L. (2014) *SANS*. Available at: https://www.sans.org/reading-room/whitepapers/wireless/overview-80211-wireless-network-security-standards-mechanisms-1530 (Accessed: 12 January 2017).
[7] Press, E.-C., EC-Council and Helba, S. (2009) *Investigating wireless networks and devices: Ec-council L press*. New York, NY, United States: Delmar Cengage Learning.
[8] Sridhar, T. (2008) *Wi-Fi, Bluetooth and WiMAX - the Internet protocol journal, volume 11, no. 4*. Available at: http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-42/114-wifi.html (Accessed: 12 January 2017).