

Wireless Forensics: Tapping the Air - Part Two

Raul Siles, GSE 2007-01-08

Introduction

In [part one of this series](#), we discussed the technical challenges for wireless traffic acquisition and provided design requirements and best practices for wireless forensics tools. In this second article, we take it a step further and focus on the technical challenges for wireless traffic analysis. Additionally, advanced anti-forensic techniques that could thwart a forensic investigation are analyzed. Finally, apart from the technical details, as a forensic write-up, the article covers some legal aspects about wireless forensics for both the U.S. and Europe.

Wireless forensics: Technical considerations for traffic analysis

Once the traffic has been collected by the forensic examiner, it must be analyzed to draw some conclusion about the case. The main technical considerations, tools and challenges associated to the analysis of 802.11 traffic from a wireless forensics perspective are presented below.

The scope of the article is to focus on wireless forensics from the traffic point of view, although in a real scenario, there are other sources of information to complement the data related with the case. These sources of information would include access points and wired network devices logs, ARP and CAM tables, and the data collected by wireless IDS.

Network Forensic Analysis Tools (NFAT): Commercial and open-source traffic analysis tools

The analysis of wireless traffic demands the same capabilities required in pure wired network forensics, that is, an in-depth understanding of the protocols involved in the data communications collected. For wireless, this commonly means TCP/IP-based protocols over 802.11.

The set of network tools used to analyze traffic from a forensic perspective is commonly called NFAT (Network Forensic Analysis Tool), a term coined in 2002. The major commercial players in the wired field are Sandstorm NetIntercept [[ref 1](#)], Niksun NetVCR [[ref 2](#)] and eTrust Network Forensics [[ref 3](#)]. Wireless forensics would require these tools to provide wireless traffic analysis capabilities, that is, advanced analysis functions for the specific 802.11 headers and protocol flows and behaviors. At the time of this writing, both NetIntercept and eTrust NF state 802.11 capabilities.

From an open-source perspective, there are no well-known, dedicated NFAT alternatives. However, there are multiple tools [[ref 4](#)] that provide network traffic analysis capabilities that are very useful for the forensic examiner to find specific pieces of information in the evidence collected.

Simplifying things, the graphical Wireshark [[ref 5](#)] protocol dissector is used to inspect in-depth every field of the frames captured, ngrep (network grep) [[ref 6](#)] is used to search for specific strings in the contents of the frames, and the text-based tcpdump [[ref 7](#)] or tshark [[ref 5](#)] sniffers are used to automate and script the analysis of certain tasks, such as filtering traffic

based on specific conditions. Most commercial and open-source tools support the standardized Pcap file format (referenced in the [first part](#) of this article) for interoperability and data exchange purposes.

Analyzing wireless traffic

The traffic analysis process involves multiple tasks, such as data normalization and mining (to be able to easily manipulate and search through the data obtained), traffic pattern recognition (required to identify anomalies and suspicious patterns), protocol dissection (very relevant for understanding all the different protocol header fields and their contents) and the reconstruction of application sessions (to obtain application-level visualization).

The coverage of all these areas (very similar to standard traffic analysis for wired networks) could require its own book, therefore, this section contains specific technical issues that should be considered during the analysis phase for wireless traffic. These issues include merging traffic from multiple channels, managing traffic from overlapping channels, filtering capabilities and fast analysis. One of the main particular challenges associated with wireless forensics is related to the built-in 802.11 layer-2 encryption features of this technology. This aspect is covered in the next section.

One of the first wireless analysis issues to consider is the merge of the capture files corresponding to all the individual channels. When using a multi-card device, as the one suggested on the first part of this article, each card listens to a specific channel and collects data for this channel in a single Pcap file.

In some scenarios, such as with roaming clients, it is required to merge the data from various channels to reconstruct the roaming session. For this purpose, it is possible to use the `mergcap` tool included with Wireshark. The tool allows one to merge multiple capture files in a single output Pcap file (-w option), as shown below:

```
# mergcap -w all_channels.pcap channel_1.pcap channel_2.pcap ... channel_14.pcap
```

Wireshark also provides a menu option, "File – Merge..." to merge two Pcap files. This is required to merge the packets chronologically to reflect the traffic over the time.

An example has been made available to the reader to follow along [[ref 8](#)]. It is a slightly modified version of a file capture provided by Aircapture, and includes two Pcap files containing a VoIP session from a roaming client switching between two access points, from channel 11 to channel 1. The example is provided so that the reader can test the merging functionality using Wireshark and reconstruct the audio conversation (that, by the way, contains a commercial message) for this VoIP session. The details about how to use Wireshark (previously called Ethereal) to reconstruct the VoIP RTP protocol sessions have been detailed in a previous SecurityFocus article [[ref 9](#)]. The briefly summarized steps for the new Wireshark version are:

- Decode RTP packets: Select the first RTP packet in the Pcap file and select "Statistics – RTP – Stream Analysis...".
- RTP Stream Analysis: Select "Save payload..." to store the media stream.
- Save the audio: Select the ".au" format, the "forward" channel and the filename to save

the audio stream that contains the voice captured.

Due to the lack of SIP packets, and the usage of 8000 as the source and destination ports, the RTP packets in the capture file for channel 1 are decoded by default in Wireshark as OICQ packets. It is required to decode them as RTP; this can be accomplished by selecting any OICQ packet, go to "Analyze – Decode As...", find and select the RTP protocol and click OK.

To get the most from this exercise, it is recommended that the reader first reconstruct and listen to the media stream for the two individual files, and then merge both into a single file, and reconstruct its media stream. The later contains the concatenation of the media stream fragments captured from each wireless channel. At about 30 seconds into the playback, the roaming takes place.

Additionally, another wireless analysis issue to consider is the fact that the capture file for a given channel might contain data from overlapping channels, that is, traffic from networks in adjacent channels. Based on the access point transmission and the analyst's reception device capabilities, such as the output transmission (Tx) power, the reception (Rx) sensitivity, and the antennas used, it is possible to capture data from multiple channels simultaneously.

The capture file shown below in Figure 1, which is also available to the reader [ref 10], corresponds to the beacon frames of a capture session on channel 9. The sniffer collected traffic from channels 9 (Null SSID and SSID "WLAN_7B"), 11 (SSID "WopR") and 12 (SSID "ANA"). The channel information is included in the beacon frame, specifically, in the "DS Parameter set: Current Channel" field of the "Tagged parameters" section inside the "IEEE 802.11 wireless LAN management frame" header.

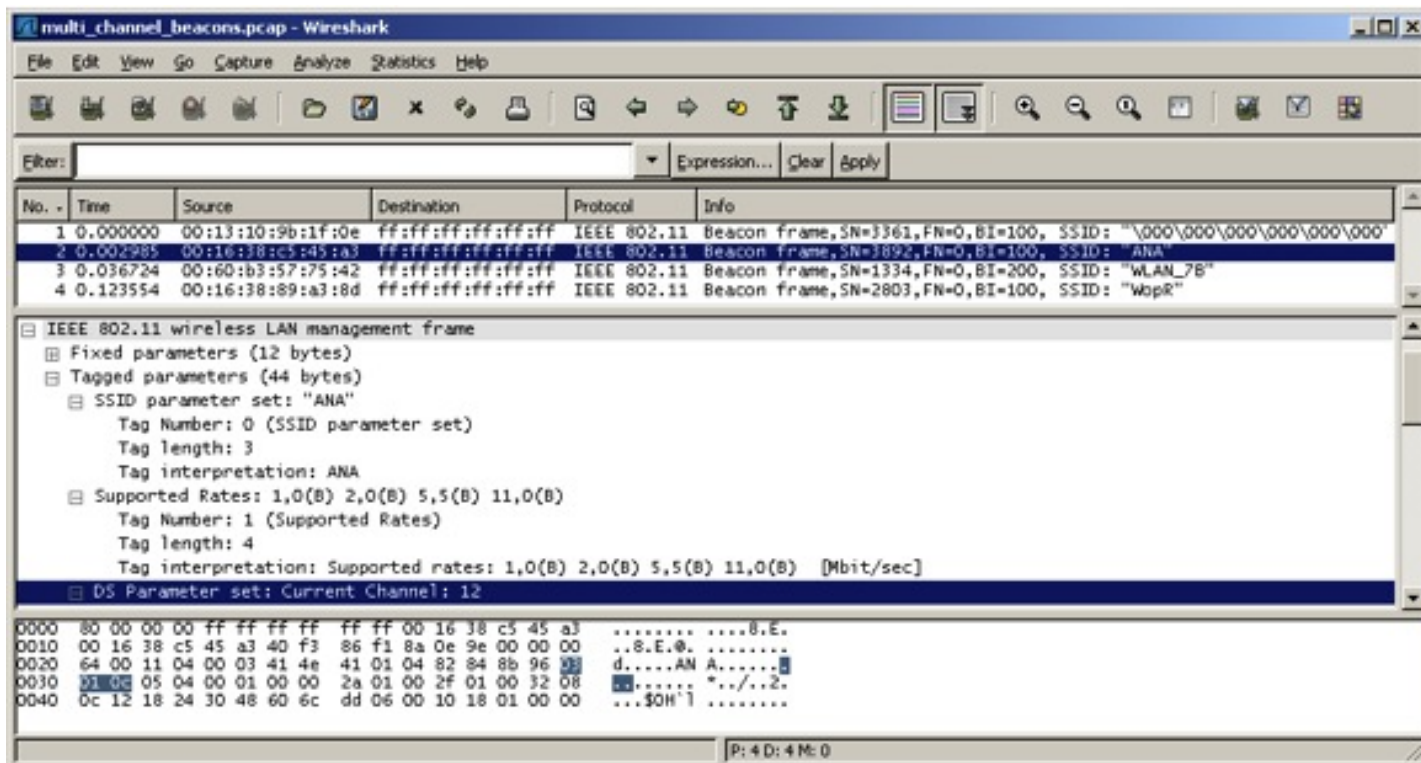


Figure 1. Beacons frames from multiple channels captured from channel 9.

Therefore, during the analysis phase it is necessary to identify and discard duplicated frames and manage these kind of multi-channel interferences and collisions.

Probably, the most commonly used feature when dealing with huge amounts of information is the traffic analyzer filtering capabilities. Once the traffic has been merged in a single Pcap file, for example, filters allow one to display the traffic associated to a single client across all channels, based on its MAC address, or display just the traffic from a single access point, based on its BSSID address, or only display data frames (versus management and control frames). The filtering options in tools like Wireshark are uncountable [ref 11] and something the forensic examiner must get familiarized with.

Finally, there is a relatively new open-source tool to parse single or multiple Pcap files and produce an initial analysis report identifying significant traffic events, statistics and flows, called Honeysnap [ref 12]. It provides security analysts a pre-processed list of high value network activity, aimed at focusing manual forensic analysis and saving relevant incident investigation time.

Although it was designed as a honeynet-related tool to quickly analyze the data collected by a honeynet, it could be very helpful for the network forensic investigator to draw initial facts about the traffic collected. Once the analyst has identified data that interests him, he can then use other tools for more in depth analysis. Currently, the tool can decode TCP and UDP-based protocols, such as HTTP, IRC or DNS, but does not have wireless capabilities, therefore, it is only useful on the wireless unencrypted traffic. However, due to its extensible modular infrastructure, it can be easily modified to include the wireless knowledge required for forensics analysis.

Continued on page 2... (link below)

[ref 1] Sandstorm NetIntercept. <http://www.sandstorm.net/products/netintercept/>

[ref 2] Niksun NetVCR. http://www.niksun.com/Products_NetVCR.htm

[ref 3] eTrust Network Forensics. <http://www3.ca.com/solutions/Product.aspx?ID=4856>

[ref 4] "Summary of tools commonly used to support network forensic investigations". <http://searchsecurity.techtarget.com/searchSecurity/downloads/NetworkForensicToolsSidebar.pdf>

[ref 5] Wireshark & tshark. <http://www.wireshark.org>

[ref 6] ngrep (network grep). <http://ngrep.sourceforge.net>

[ref 7] tcpdump. <http://www.tcpdump.org>

[ref 8] "Pcap files containing a roaming VoIP session". http://www.raulsiles.com/downloads/VoIP_roaming_session.zip

[ref 9] "Two attacks against VoIP". Peter Thermos. April 2006. <http://www.securityfocus.com/print/infocus/1862>

[ref 10] "Pcap file containing traffic from multiple channels and captured from a single channel, 9". http://www.raulsiles.com/downloads/multi_channel_beacons.pcap

[ref 11] "Wireshark & Ethereal Network Protocol Analyzer Toolkit". Angela Orebaugh, Gilbert Ramirez, Jay Beale (Series Editor). Syngress. ISBN: 1597490733. Chapter 5 – "Filters": http://www.syngress.com/book_catalog/377_Eth_2e/sample.pdf

[ref 12] Honeysnap. The Honeynet Project. 2006. <http://www.honeynet.org/tools/honeysnap/>

Overcoming wireless encryption

The main drawback for the forensic examiner is not being able to obtain the key used by the suspect to encrypt/decrypt the wireless traffic; this key is required to analyze the traffic contents, so it is a crucial aspect of the forensic process.

The wireless 802.11 standards define multiple types of data encryption. From the insecure unencrypted mode, where all traffic travels in the clear, to the secure 802.11i specification, that uses advanced encryption algorithms, such as AES. The current state-of-the-art to bypass wireless encryption is summarized in Table 1 and described below.

Encryption	Key	Security level	Auditing tool	Key acquisition
<i>Open</i>	No	N/A	Sniffer	Not required
WEP	PSK	Low [1]	Aircrack-ng	Feasible
WPA or WPA2 – Personal	PSK	Medium [2]	CoWPAtty	Feasible
WPA or WPA2 – Enterprise	EAP	High [3]	N/A	Other methods

Table 1. State-of-the-art to bypass wireless encryption.

By collecting enough wireless traffic, it is always possible to obtain the WEP key [1]. WEP, and its derivatives (WEP+, DWEAP...), are insecure encryption mechanisms that can be defeated in multiple ways, with tools like the Aircrack-ng suite [ref 13].

The level of security in Table 1 for WPA/PSK is mainly based on the strength of the pre-shared key [2]. If the key is not long enough and/or is based on dictionary words (or can be derived from them) a dictionary attack could guess the encryption key. The forensic examiner can also consider the usage of pre-calculated keys (aka Rainbow tables) to speed up the process of discovering the network key. Tools like Aircrack-ng or CoWPAtty [ref 14] can be used to audit the security of WPA/PSK networks. A new version of CoWPAtty [ref 15] was released during the last DefCon conference to audit the security of WPA2/PSK networks. Once the key has been obtained, the traffic can be decrypted using Wireshark [ref 5] for WEP or airdecap-ng [ref 13] for WEP or TKIP (WPA).

The WPA(2)/Enterprise mode encryption keys [3] are randomly generated by the RADIUS server, therefore, it is not possible to launch a dictionary attack against them. The main weakness associated to this mode of operation is in the authentication mechanism used by the corresponding EAP type. To simplify, we'll consider it secure enough not to be feasible to gather the key in a reasonable amount of time without using brute force techniques.

To sum up, only WPA or WPA2 personal mode with robust pre-shared keys (PSK), more than 20 characters in length (as recommended by the IEEE 802.11i specification [ref 16], Annex H4.1) and not based on dictionary words, or enterprise mode through robust EAP protocols, such as PEAP or EAP/TLS, could be considered unbreakable. In these scenarios, the forensic examiner would require other methods to access to the traffic contents, such as getting the encryption keys or material from the access points, wireless clients, RADIUS server or backend user authentication database.

Finally, it is very common nowadays to find wireless deployments where encryption is used at higher levels (layer 3 or upper protocols), such as VPN solutions based on IPSec, SSL or SSH.

These scenarios, although not only related to wireless but also wired networks, present new and complex challenges for the forensic examiner. The next section describes advanced traffic analysis techniques and tools that can be applied in these situations. However, if the suspect is illegally using a third party wireless network (a very frequent scenario), this means he had to overcome the same encryption constraints pointed out above for the forensic examiner, and therefore most probably he is using an open network, WEP-based or WPA-PSK with a discoverable pre-shared key.

Advanced traffic analysis and fingerprinting techniques

If layer 2 (or upper layer) encryption cannot be bypassed, it is not possible to draw direct conclusions from the data contents; then, a commonly used option is to perform protocol statistical analysis. Besides that, with wireless traffic it is possible to derive information from the traffic's clear text portions, such as the headers of the data frames, or from the management and control frames (that always travel in the clear). This clear text data can provide enough information such as, if the suspect was trying to establish a connection against a specific network: whether or not the connection succeeded, the authentication methods used, the wireless network features and capabilities, including the encryption methods supported...

Unfortunately, in this scenario, the IP header information (layer 3) is not available to provide details about the connection end-points, that is, who the suspect is communicating with and vice-versa. This is not the case with wired networks where typically there are no layer 2 encryption mechanisms in place.

Tools like f10p [ref 17] can be very useful for this type of encrypted traffic analysis. F10p is a flow-analyzing passive layer 7 fingerprinting tool that works by examining the sequence of client-server exchanges, their relative payload sizes and transmission intervals. This information is matched against a database of traffic pattern signatures to infer interesting facts about the encrypted sessions, such as login failures, discriminate between human and automated actions - even deducing specific security settings and the existence of user prompts - based on timing conditions, or identify evasion techniques, anomalies and protocols used.

Additionally, in a wireless network, it is trivial for an unauthorized user to impersonate a valid user when basic MAC address authentication mechanisms are used. The suspect can access and exchange data in the network by spoofing the MAC address of a valid client. In this scenario, the main forensic examiner challenge is to differentiate between the traffic generated by the suspect and by the valid user.

Through passive traffic analysis and fingerprinting methods, it could be feasible to differentiate between several stations at the OS and at the wireless stack level. In order to succeed, the unauthorized and the authorized users should not be using the same access device, that is, operating system version, wireless network card and drivers.

Passive OS fingerprinting can be performed using passive tools like p0f [ref 18]. For reasons already stated in this paper, it is recommended from a forensic perspective not to use active OS fingerprinting tools like nmap or sinFP (although the later also has passive capabilities). All these tools base their results in the analysis of layer 3 and 4 (TCP/IP) specific OS idiosyncrasies; therefore, if the wireless traffic is encrypted at layer 2, they won't be able to bring any conclusion.

Wireless stack fingerprinting (at the chipset and device driver levels), can help to overcome the encryption constraint. This technique is applied through advance passive and active analysis techniques on 802.11 traffic, some of which have been implemented in the lib802finger tool [ref 19].

Wireless anti-forensic techniques

In the same way as there are multiple techniques and tools in computer forensics whose main goal is to thwart a forensic investigation, once wireless forensics techniques will be widely adopted, new wireless anti-forensic methods will appear. The information provided in this section can help to assist forensic investigators in understanding what they may be up against.

Anti-forensics is the science of evading forensic analysis. In the wireless field, this is commonly accomplished through basic methods, such as the usage of illegal channels, like channel 14 in US and Europe, or using strong layer-2 encryption (as previously covered).

However, there are advanced stealth wireless techniques that, although they were not designed for anti-forensic purposes, could bring advantage to the suspect if the forensic examiner is not aware of them, such as covert channels and the modification of the 802.11 specification.

Raw Covert [ref 20] is a proof of concept tool that uses the raw injection capabilities of current Linux drivers in monitor mode to embed information in 802.11 control frames. Specifically, the data is encoded in the receiver address (RA) field of ACK frames, so this method provides a very stealthy communication channel because wireless monitoring tools do not tend to inspect ACK frames. The same concept could be implemented using other fields and controls frames, such as CTS, RTS or PS-Poll frames, or even in the 802.11 management, data or invalid frames.

WiFi Advanced Stealth Patches [ref 21] are some proof of concept patches for the Linux madwifi-ng driver, associated to the Atheros chipset, that implement a stealth new "proprietary" protocol tweaking the 802.11 MAC layer. The technique is based on implementing a modified 802.11 network stack that can communicate only with another modified stack. In particular, this tool provides two patches, one modifies the 802.11 protocol field and another modifies the type of frame field. Although it uses the standard 802.11 PHY (physical) layer, that is the 802.11 frequency bands, the wireless sniffers and IDS are not capable of identifying this proprietary traffic.

From a forensic perspective, it is necessary to be aware of these tools, and similar future techniques, to be able to analyze in-depth the wireless communications associated to a given case.

Legal considerations

It's not required that one be a lawyer to identify that some of the tasks the wireless forensic analyst must perform could be considered illegal, or at least, within a grey line from a legal perspective. These tasks include capturing the network traffic, breaking the network encryption key or, obviously, active tasks such as traffic injection to speed-up the WEP key acquisition process.

In general, it is illegal in both the U.S. and most European countries to intercept wireless traffic

without the consent of at least one (and sometimes both/all) of the parties to a communication, subject to certain exceptions provided by the applicable law, such as interception by law enforcement with a warrant under a court order, or interception by the network operator or service provider in order to manage its business.

Monitoring or scanning wireless traffic simply to identify networks in the area, due to the fact it is an activity that does not involve capture of the message content or traffic data for specific communications (an area where the legal restrictions become really strict), could well be legal in most countries.

The traffic acquisition activities must be accomplished after receiving proper authorization, typically in the form of a search warrant (or other legal process), and are mainly regulated in the U.S. by the Communications Assistance for Law Enforcement Act (CALEA) of 1995 [ref 22] and in Europe by the European Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications (Official Journal C 329) [ref 23].

Three U.S. federal statutes govern the interception, accessing, use, disclosure and privacy protections of electronic and wire communications. The U.S. Electronic Communications Privacy Act (ECPA, 18 U.S.C. §§ 2701-2712) of 1986 [ref 24] covers stored communications. Real-time interception, as in wireless networks, is covered by the Pen/Trap Statute, 18 U.S.C. §§ 3121-3127 [ref 24], centered in addressing information (like 802.11 protocol headers), and by the Wiretap Statute ("Title III"), 18 U.S.C. §§ 2510-2522 [ref 24], centered in the contents of communication.

Similar laws apply worldwide, for example, at the European level, the resolutions of the "Convention on Cybercrime" [ref 25] establish the interception without right by any mean as a criminal offense in Chapter II - Section 1 - Article 3 - Illegal interception. Besides, Article 13 determines that each EU country should adopt the legislative sanctions and measures against these punishable acts, that can include deprivation of liberty as well as other dissuasive sanctions.

At the country level, particular EU Member States laws apply, and for example, the Spanish law, similar in this respect to the U.S. Code (Title 18 2511(1)), prohibits the eavesdropping, use and disclosure of other's communications (including electronic ones) in "Article 197.1 - Second paragraph" [ref 26]. Other EU countries apply similar statues, such as Section 1 of the Regulation of Investigatory Powers Act 2000 (RIPA) in UK [ref 27] or Section 206 of the Criminal Code [ref 28] or Section 89 of the Telecommunications Act in Germany [ref 29], to cite some examples.

All these laws prohibits unlawful monitoring and disclosure of the content of communications, and mandates law enforcement to follow proper procedures to review electronic communications, such as the search and seizure electronic evidence procedures detailed in the "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" [ref 24] document by the US DoJ, specifically sections III and IV, focused on electronic communications and surveillance.

The wireless forensic examiner should perform lawful interception (LI) to monitor the communications. Apart from following the laws and regulations enacted in the country the case is taking place, some technology groups, such as the IETF or ETSI, have created technical specifications to define appropriate LI procedures and solutions, like the RFC 3924 [ref 30] and

Eve(™) [ref 31] respectively.

Finally, when dealing with legal issues related to wireless technologies, it is important to consider not only the legal details for data acquisition, but also other legal aspects, such as the fact that the liability of the wireless owner can be called into question for having inadequate security. This was suggested by a case decided by the Hamburg State Court in Germany in July 2006 [ref 33], in which an unsecured open wireless connection was used for trading of copyrighted music with P2P software. Although the owner of the connection denied responsibility, the court found liability because the connection had not been protected. In a similar digital rights related case in Sweden, the suspect was considered innocent because he declared to have an unsecured wireless network; as the expert witness declared, it's trivial to break into this type of wireless network, so anyone could potentially have downloaded the copyrighted content [ref 32]. Therefore, everyone sharing their Internet connection through an open wireless network is in a legal grey area.

Concluding part two

Wireless forensics is a relatively new field, but as computer intrusions become more common through this communication medium, new techniques, tools and laws are required to manage the acquisition and analysis of wireless data.

In the [first article of the series](#), the main technical challenges and best practices for wireless traffic acquisition and tools were described. In this second article, we continued by focusing on the technical challenges for wireless traffic analysis, described advance scenarios where anti-forensic techniques could be used, and covered wireless forensics related laws for both, US and Europe. Wireless technologies in legal cases are still today a brand new field to explore, and, remember, attackers don't follow the laws.

Most of the challenges, technical considerations, and best practices covered along this article can also be applied to other wireless security-related fields, such as wireless IDS or wireless honeypots, and can be extended to other wireless data technologies, such as Bluetooth and WiMAX.

References

- [ref 1] Sandstorm NetIntercept. <http://www.sandstorm.net/products/netintercept/>
- [ref 2] Niksun NetVCR. http://www.niksun.com/Products_NetVCR.htm
- [ref 3] eTrust Network Forensics. <http://www3.ca.com/solutions/Product.aspx?ID=4856>
- [ref 4] "Summary of tools commonly used to support network forensic investigations". <http://searchsecurity.techtarget.com/searchSecurity/downloads/NetworkForensicToolsSidebar.pdf>
- [ref 5] Wireshark & tshark. <http://www.wireshark.org>
- [ref 6] ngrep (network grep). <http://ngrep.sourceforge.net>
- [ref 7] tcpdump. <http://www.tcpdump.org>
- [ref 8] "Pcap files containing a roaming VoIP session". http://www.raulsiles.com/downloads/VoIP_roaming_session.zip
- [ref 9] "Two attacks against VoIP". Peter Thermos. April 2006. <http://www.securityfocus.com/print/infocus/1862>
- [ref 10] "Pcap file containing traffic from multiple channels and captured from a single channel,

9". http://www.raulsiles.com/downloads/multi_channel_beacons.pcap

[ref 11] "Wireshark & Ethereal Network Protocol Analyzer Toolkit". Angela Orebaugh, Gilbert Ramirez, Jay Beale (Series Editor). Syngress. ISBN: 1597490733. Chapter 5 – "Filters": http://www.syngress.com/book_catalog/377_Eth_2e/sample.pdf

[ref 12] Honeysnap. The Honeynet Project. 2006. <http://www.honeynet.org/tools/honeysnap/>

[ref 13] Aircrack-ng. Christophe Devine (aircrack) et al (ng). <http://www.aircrack-ng.org>

[ref 14] CoWPAtty version 3.0. Joshua Wright. <http://cowpatty.sourceforge.net>

[ref 15] CoWPAtty version 4.0 (includes WPA2/PSK support). Church of WiFi. August 2006. <http://www.churchofwifi.org/FileLib/9-cowpatty-4.0.zip>

[ref 16] "802.11i. Amendment 6: Medium Access Control (MAC) Security Enhancements". IEEE. July 2004. <http://standards.ieee.org/getieee802/download/802.11i-2004.pdf>

[ref 17] "FIOP: a passive L7 flow fingerprinter". Michal Zalewski. December 2006. <http://lcamtuf.coredump.cx/soft/fiop-devel.tgz>

[ref 18] "POf v2: a versatile passive OS fingerprinting tool". Michal Zalewski. September 2006. <http://lcamtuf.coredump.cx/pOf.shtml>

[ref 19] "lib802finger: 802.11 implementation fingerprinting". Johnny Cache. September 2006. <http://www.802.11mercenary.net/lib802finger/> and http://www.802.11mercenary.net/~johnycsh/publications/06Sep_Elch.pdf and <http://www.uninformed.org/?v=5&a=1&t=sumry>

[ref 20] Raw Covert. Laurent Butti. 2006. http://rfakeap.tuxfamily.org/#Raw_Covert and <http://www.shmoocon.org/2006/presentations/Shmoo2006-Butti-Veysset-WiFi-1.pdf>

[ref 21] WiFi Advanced Stealth Patches. Laurent Butti and Franck Veysset. 2006. http://rfakeap.tuxfamily.org/#WiFi_Advanced_Stealth_Patches and <http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Veyssett.pdf>

[ref 22] "Communications Assistance for Law Enforcement Act (CALEA). Pub. L. No. 103-414, 108 Stat. 4279". USA. 1994. <http://www.askcalea.com>

[ref 23] "European Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications (Official Journal C 329)". Europe. 1995. <http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31996G1104:EN:HTML>

[ref 24] "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations". Computer Crime and Intellectual Property Section. Criminal Division. United States Department of Justice (US DoJ). July 2002. <http://www.cybercrime.gov/s&smanual2002.htm>

[ref 25] "Convention on Cybercrime". Budapest, 23.XI.2001. Council of Europe (COE). <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm> and <http://www.coe.int/T/E/Com/Files/Themes/Cybercrime/default.asp>

[ref 26] "Artículos del Código Penal Español referentes a Delitos Informáticos". Ley-Orgánica 10/1995, de 23 de Noviembre. BOE número 281, de 24 de Noviembre de 1.995. Artículo 197. <http://delitosinformaticos.com/legislacion/espana.shtml>

[ref 27] "Regulation of Investigatory Powers Act 2000 (RIPA)". Chapter 23. Crown. 2000. UK. <http://www.opsi.gov.uk/Acts/acts2000/20000023.htm>

[ref 28] "Section 206 of the German Criminal Code". Federal Ministry of Justice. 13 November 1998. Germany. <http://www.iuscomp.org/gla/statutes/StGB.htm#206>

[ref 29] "Section 89 of the German Telecommunications Act". Federal Regulatory Authority for Telecommunications and Posts. 25 July 1996. Germany. <http://www.iuscomp.org/gla/statutes/TKG.htm#89>

[ref 30] "Cisco Architecture for Lawful Intercept in IP Networks". RFC3924. IETF. October 2004.

[ref 31] "The EVE™ Lawful Interception Solution". TIIT & ETSI. <http://www.lawfulinterception.com/products.php>

[ref 32] "Expert witness frees suspect sharing files under trial". Stockholm. Sweden. October 2006. http://www.bitcopy.se/gfx/DOM_Mal_B8799-05.pdf (in Swedish)

[ref 33] "Unencrypted WLAN can become expensive!". German court case 308 O 407 / 06. Landgericht Hamburg. <http://www.lampmannbehn.de/wlan.html> (in German)

About the author

Raul Siles is a senior independent security consultant based in Spain and a SANS certified instructor. His current security research interests, related with this article, include wireless security, incident handling and computer forensics, and VoIP security. He is one of the few individuals who have earned the GIAC Security Expert (GSE) designation. More information can be found on his website, www.raulsiles.com.

Reprints or translations

Reprint or translation requests require [prior approval](#) from SecurityFocus.

© 2007 SecurityFocus

Comments?

Public comments for Infocus technical articles, as shown below, require technical merit to be published. General comments, article suggestions and feedback are encouraged but should be sent to the [editorial team](#) instead.

[Privacy Statement](#)

Copyright 2006, SecurityFocus