2015

The challenges of seizing and searching the contents of Wi-Fi devices for the modern investigator

Dan Blackman
Edith Cowan University, dblackm0@our.ecu.edu.au

Patryk Szewczyk
Security Research Institute, Edith Cowan University, p.szewczyk@ecu.edu.au

DOI: 10.4225/75/57b3f385fb887
13th Australian Digital Forensics Conference, held from the 30 November – 2 December, 2015 (pp. 37-48), Edith Cowan University Joondalup Campus, Perth, Western Australia.

THE CHALLENGES OF SEIZING AND SEARCHING THE CONTENTS OF WI-FI DEVICES FOR THE MODERN INVESTIGATOR

Dan Blackman[1], Patryk Szewczyk[1, 2]
Edith Cowan University[1], Security Research Institute[2] Perth, Australia
dblackm0@our.ecu.edu.au, p.szewczyk@ecu.edu.au

Abstract

To the modern law enforcement investigator, the potential for an offender to have a mobile device on his or her person, who connects to a Wi-Fi network, may afford evidence to place them at a scene, at a particular time. Whilst tools to interrogate mobile devices and Wi-Fi networks, have undergone significant development, little research has been conducted with regards to interrogating Wi-Fi routers and the evidence they may contain. This paper demonstrates that multiple inhibiting factors exist for forensic investigators when attempting to extract data from Wi-Fi routers at the scene. Data volatility means the Wi-Fi router cannot be powered down without losing a substantial quantity of data. Third party Wi-Fi enabled devices may connect to or interact with the access point after an event occurs. Multiple models exist, with varying internal architectures, operating systems, and external interfaces. This paper presents steps and considerations for at scene seizure of Wi-Fi devices for law enforcement, to ensure maximum digital forensic evidence is collected. It also lists a series of recommendations to the manufacturers of Wi-Fi devices to facilitate a standardised mechanism to collect forensic evidence, thus making future acquisitions easier and time efficient.

Keywords
Wi-Fi routers, router forensics, network forensics, digital forensics, law enforcement, first responder

INTRODUCTION

In Australia, the quantity of active Wi-Fi access points found throughout homes and businesses is continually increasing, as the technology becomes commonplace in many consumer grade networking and mobile devices (Potts, 2014). Internet Service Providers (ISPs) supply customers with Wi-Fi enabled devices as packages integrated with broadband contracts. Manufacturers typically enable Wi-Fi on smart phones, laptops and computers by default to streamline the configuration and networking process – improving perceived usability. The Wi-Fi enabled feature may also remain active purposefully, or unknowingly post-configuration. Alternatively, it is common practice for software and firmware upgrades to enable previously disabled Wi-Fi functionality on mobile computing devices such as the iPhone (Althuser, 2015). Enabling the Wi-Fi feature on smartphones after an update has occurred, streamlines the process of finalising the update process.

Australia's use of smart phones, is reaching saturation. Approximately 85% of Australia's mobile phone owners, use a smartphone as their primary mobile phone device (Rogers, 2015). Smartphones are versatile portable computing devices with benefits and feature set for all types of consumers. The tablet computer market is equally as prevalent. In 2014, approximately 55% of Australian tablet computer owners were accessing the Internet through Wi-Fi in contrast to approximately 15% of owners accessing the Internet through a dedicated 3G/4G network (ACMA, 2014). The widespread use of Wi-Fi technology amongst end-users may result in digital evidence of interest being present on Wi-Fi routers, for use in subsequent civil or criminal investigations.

Obtaining data of interest from Wi-Fi networking devices encompasses a series of challenges. For instance, Wi-Fi routers cannot be powered off without losing a significant quantity of data stored in volatile memory (Szewczyk, 2009). Subtle variations between Wi-Fi devices and their respective models, may prove problematic in attempting to use a standardised approach to extract data of interest (Liu, Chen, Yu & Fu, 2010). Furthermore, third party Wi-Fi enabled devices (e.g. a smartphone) may connect to, or interact with an access point, potentially erasing or overwriting previously stored evidentiary data. As a result it is important that first responders at the scene are adequately prepared and informed when operating in time critical situations.

This paper presents a series of empirical experiments and considerations for at scene seizure of Wi-Fi devices to ensure maximum digital forensic evidence is preserved and collected by first responders. The paper uses a law enforcement perspective in an attempt to identify and propose strategies that could be utilised by first responders at the scene. This paper also outlines a series of recommendations focusing towards the manufacturers of Wi-Fi

devices that would enable standardised methods to be used to collect evidence of interest, thus making collection easier and more time efficient.

The importance of wireless devices

Wi-Fi routers have received limited research focus from a digital forensics perspective (Akers, McGrew & Dampier, 2011; Minnaard, 2014; Turnbull & Slay, 2008). However those investigations, which have been conducted, have discovered that a wealth of information can be gained from networking devices in general (Fu, Zhang, Pingley, Yu, Wang & Zhao, 2012; Liu, et al., 2010; Szewczyk, 2011). A typical consumer grade Wi-Fi router has the ability to record and store at a minimum the:

- Media Access Control (MAC) address of connected devices;
- Logs of successful or failed authentication attempts;
- De-authenticated logs;
- Date and time, typically synced to a Network Time Protocol (NTP) Server; and
- User generated names of mobile computing devices.

A Wi-Fi router may also capture probe requests from Wi-Fi enabled mobile devices within the vicinity. Probe requests are special periodic requests used to identify what networks are currently active and available. Some consumer level Wi-Fi routers have been found to record these requests along with the device's MAC address (Turnbull & Slay, 2008). A MAC address of a device is a significant finding given that no two devices should theoretically have the same address (IEEE, 2015). This means that any MAC address that is recorded should be unique to that device and that device alone. Further to this, the first three bytes of a MAC address signifies the Organisation Unique Identifier (OUI) and allows inquiries to be conducted with the manufacturer to determine who purchased it and where the device was sold (Holman, 2012). This could assist in the identification of a Person Of Interest (POI). A study by the Australian Institute of Criminology found that of the 479 homicides in Australia between 2010-2012, 362 of these, or 75% of the offenders were well known to the victim (AIC, 2015). This may suggest the presence, at the time of a criminal act, successful authentication attempts, if the offender had been trusted and thus given access credentials to the victims' Wi-Fi network.

Mobile computing devices will attempt to automatically reconnect to a previously connected Wi-Fi router when within range. Following a successful connection, the router's logging mechanism may record this connection and include the name of the device, the MAC address, the local (IP) address issued and the time/date the device authenticated and de-authenticated from the wireless network. For the legal community, to place a device owned by an individual at a location at a guaranteed time, may provide a fundamental piece of evidence to a case. As many Wi-Fi routers are pre-configured to connect to NTP servers around the world to keep accurate times, this automatically reduces the possibility the device could be recording inaccurate dates or times. Whilst some challenges exist to prove that a POI had the mobile device on their person at the time, the circumstantial evidence, paired with other evidence may lead to a successful prosecution or finding of guilt.

The names of any device recorded may also offer investigators a line of inquiry, where the offender is unknown. In many cases it has been found that owners have named their devices based on their full name or part thereof (Könings, 2013). Whilst there have been advances with antennas, power output and attempts to reduce the noise surrounding the Wi-Fi network, the majority of consumer level routers provide only local connectivity typically for a household's device (Hamida & Chelius 2010; Fu et al., 2012). Therefore, any connectivity by a POI would need to be localised.

TECHNICAL PROCESSES

The aim of this study was to obtain a range of consumer level Wi-Fi routers and interrogate those devices to determine the quantity and usefulness of data that could be obtained from them by a first responder. Twenty consumer grade Wi-Fi routers were used for experimentation. The Wi-Fi routers were biasedly chosen based on devices previously seized by Police as part of investigations. This enables an authentic assessment to be undertaken based on previously encountered networking devices that would be maintained by end-users. To maintain the chain of custody, each device was individually labelled and photographed with its exhibit number. Documentation for each device and experiment was maintained. Photographs formed part of the inspection process as any damage was recorded along with accessible ports, internal hardware characteristics and model/revision numbers. To minimise anomalies being introduced into the tests due to environmental conditions, all experiments were undertaken under the same environmental conditions. Where possible, a faraday room was utilised to eliminate further environmental factors. Each device was restored to its factory default setting

replicating the typical Wi-Fi router's state experienced by end-users when installing a router. Table 1 depicts the brand, model and device version of the Wi-Fi routers used within this research.

Table 1 - Wi-Fi routers used for experimentation

Device #	Brand	Model	Version/Revision
1	Tompson	TL-WR1043ND	v1
2	Netgear	WGR614v9	v9
3	Belkin	P10808au	v1
4	TP-Link	TL-WR1043ND	v1
5	Linksys	WRT54GL	v1.1
6	2-Wire	2071	vA
7	Belkin	F5D8636-4	v1
8	Thompson	TG782T	v1
9	iiNet/Boblite	GL411	B
10	Netgear	DG834G	v4
11	Billion	740GE	v1
12	D-Link	604	vA3
13	Linksys	WRT54G	v7
14	iiNet/Belkin	F1P1234EGau	V1
15	Cisco	AP-1231G-A-K9	v1
16	Cisco	AP-1121G-A-K9	v1
17	Linksys	WAP54G	v3
18	Linksys	WRT54G	v1
19	Tp-Link	WDR4300	v1
20	Netgear	DGND4000	v1

Signal and Noise Level Tests

The purpose of the first test was to isolate the Wi-Fi router from interacting with third party devices. Each network device can produce different Wi-Fi signal strengths, thus a controlled test or baseline was firstly established. Creating a controlled test provides a mechanism to verify that the changes introduced were not as a result of an external factor. Following any change to the device, the results were verified against the control test to determine possible differences. A Rohde & Schwartz Spectrum Analyser model 'FSL' was utilised to measure the power output of each device in decibel megawatts (dBm). The output range for the Wi-Fi routers were measured from 0 to -100dBm. The closer the value to zero, the stronger the signal strength.

As the spectrum analyser samples the environment and cannot distinguish a single individual Wi-Fi router, environmental noise was also sampled. Environmental noise simulates a real life situation. Once the testing environment was established, each Wi-Fi router was moved further away from the spectrum analyser and the signal and noise levels were remeasured. The distances selected for measurements were at 1, 2, 3 and 5 meters.

The following tests were performed at the aforementioned distances:

- Remove external antennas (where antennas were present);
- Remove one and then both antennas (where the device had more than one antenna);
- Creating an ad-hoc faraday cage using aluminium foil;
- Creating an ad-hoc faraday cage using aluminium foil with exposed holes;
- Creating an ad-hoc faraday cage around the antennas using aluminium foil;
- De-soldering or cutting the antenna connections from the logic board; and
- De-soldering or cutting internal or external antennas and wrapping the remaining body in aluminium foil;

Log Files

A series of experiments were conducted to determine how long the log files on the Wi-Fi router were beneficial to a forensic investigator before they were deleted by the router's operating system. This experiment utilised Kali

Linux 2.0 and the Aircrack-ng packages (included in the Kali Linux distribution). Some devices provide granular log file configuration. Overall, the configuration categorises incidents into one of three events:

- Administrative events - Administer configuration changes along with power-up and start-up events are logged.
- Firewall events - Blocked incidents, port scans, access attempts from inside the network to sites on a block list, logged.
- Full/Detailed logging - All services including DHCP and wireless access including MAC addresses are logged.

A laptop was utilised to send large quantities of authentication data to the Wi-Fi router. The laptop was configured in monitor mode. Monitor mode allows the laptop to capture network traffic, without being associated with an access point and therefore announcing its presence. The following command placed the laptop into monitor mode:

```
# airmon-ng start wlan0
```

The mdk3 package was utilised to attack each Wi-Fi router, based on the Wi-Fi's MAC address of 44:94:fc:1b:1c:fb. This package utilises an authentication attack (*a switch*). The *–m switch* sets the authentication attack to use real world MAC addresses:

```
# mdk3 wlan0mon a -m  -a 44:94:fc:1b:1c:fb
```

With continuous monitoring of the log file of the Wi-Fi router, the log was timed to see how long before it filled and rotated. A final test utilised Kali Linux to send DHCPDISCOVER packets to the Wi-Fi router. These packets request a local Internet Protocol (IP) address from the Wi-Fi router. Continuous DHCPDISCOVER requests were made using the following command:

```
# dhcpx -i eth0
```

Memory

Volatile memory will typically contain portions of the log files, as these are written to memory before they are written to a file. A series of experiments were conducted to see how long a listing would remain in memory, despite the log file being deleted. A connection attempt was made from a laptop with a MAC address 00:e0:00:a7:24:66 and the log files were checked to ensure this MAC address could be found (Figure 2).

```
Jan  1 00:19:02 DD-WRT daemon.notice hostapd: ath0: STA 00:08:a1:81:21:5a IEEE 802.11: did not acknowledge authentication response
Jan  1 00:19:03 DD-WRT daemon.notice hostapd: ath0: STA 00:00:92:57:f5:63 IEEE 802.11: did not acknowledge authentication response
Jan  1 00:19:03 DD-WRT daemon.notice hostapd: ath0: STA 00:07:0e:78:6e:38 IEEE 802.11: did not acknowledge authentication response
Jan  1 00:19:03 DD-WRT daemon.notice hostapd: ath0: STA 00:40:96:f4:9e:3e IEEE 802.11: did not acknowledge authentication response
Jan  1 00:19:03 DD-WRT daemon.notice hostapd: ath0: STA 00:12:f0:7d:c7:e2 IEEE 802.11: did not acknowledge authentication response
Jan  1 00:19:04 DD-WRT daemon.notice hostapd: ath0: STA 00:e0:00:a7:24:66 IEEE 802.11: did not acknowledge authentication response
```

Figure 2 - MAC addresses authenticating

The laptop was connected to the Wi-Fi router using a shell and a capture was completed using the following command:

```
# dd if=/dev/mem of=memory-dump.bin
```

This wrote the contents of the Wi-Fi router's memory to a file called memory-dump.bin. A laptop was then utilised to check the file for the last known MAC address:

```
# cat memory-dump.bin | grep 00:e0:00:a7:24:66
```

On confirmation, the Wi-Fi router was then flooded with as many authentication requests as possible. At each 30-second interval, the same commands were rerun until the laptop's MAC address could no longer be found in memory.

RESULTS

Throughout this analysis a number of tests were undertaken, ultimately with the aim of gaining access to the Wi-Fi router to preserve the logs and volatile memory. Further tests were conducted to determine the lifespan of the log files, and therefore the criticality to have an investigator attend a scene to ensure they were preserved. Overall, it was found once the device lost power, the log files were deleted. The configuration files were not however affected by the loss of power, and could have potential evidentiary value.

Table 2 - Characteristics of Wi-Fi routers tested

Device number	Non Volatile RAM	Volatile RAM	Shell available	Shell accessible	On-board connectors	Logging enabled (Admin/Firewall/ Full)
1	8Mb	128Mb	Yes	No	Yes	Admin
2	2Mb	8Mb	Yes	No	Yes	Admin
3	2Mb	256Mb	No	No	Yes	Admin
5	8Mb	32Mb	Yes	Yes	Yes	Full
6	4Mb	128Mb	Yes	No	No	Admin
7	128Mb	256Mb	No	No	Yes	Admin
8	8Mb	32Mb	Yes	No	Yes	Admin
9	64Mb	256Mb	Yes	No	Yes	Admin
10	16Mb	512Mb	Yes	No	Yes	Firewall
11	4Mb	4Mb	No	No	Yes	Firewall
12	2Mb	8Mb	Yes	No	Yes	Admin
13	2Mb	16Mb	Yes	No	Yes	Firewall
14	4Mb	8Mb	Yes	Yes	Yes	Admin
15	8Mb	16Mb	Yes	No	No	Firewall
16	8Mb	32Mb	Yes	No	No	Admin
17	8Mb	128Mb	Yes	No	Yes	Admin
18	4Mb	8Mb	Yes	Yes	Yes	Full
19	4Mb	16Mb	Yes	Yes	Yes	Full
20	8Mb	128Mb	Yes	Yes	No	Full

Logging

Sixteen of the twenty devices inspected had little or no logging enabled by default, despite having the capability to log more extensive information. The devices which did log events, only stored administrative functions, such as logins, and power up events. It is unclear if the manufacturer reduced the logging functionality to minimise the required space on the device. Four of the twenty devices had logging enabled to a sufficient level that it would capture Domain Host Configuration Protocol (DHCP) assignments (Figure 3).

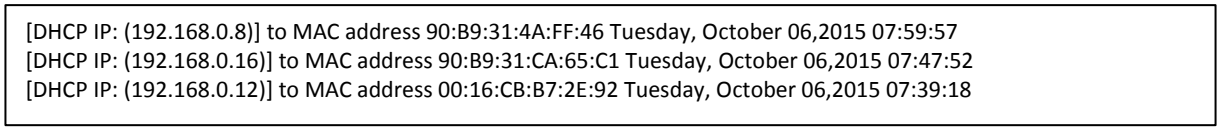

Figure 3- DHCP assignments for the Netgear DGND4000 "webgenie" interface

No devices had default logging capabilities to capture beacon/probe request packets and no devices had logging enabled to capture Wi-Fi authentication packets, despite this logging feature being available. During experimentation with a TP-Link TL-WDR4300, it was found that a brute force authentication attack using real world MAC addresses caused the log file to rotate within 14 minutes and 50 seconds. Conducting the same experiment, slowing the authentication attack to one attempt per second caused the log file to rotate after 26 minutes. Further experiments on a Linksys WRTG54G, which had approximately 8Mb of non-volatile RAM, found the device only allowed 204Kb of log files before rotating the log file. This 204Kb equated to approximately 1582 lines of data.

Further tests, using DHCPDISCOVER packets to request an IP address from a Netgear DGND4000, showed that the webpage log file contained a maximum of 261 lines of information. One packet request was sent per second

and despite some of these packets being ignored, the log file filled in 7 minutes and 31seconds. Once the log file had been rotated in both scenarios, the old log files were erased and no longer accessible on the device.

Antennas and Signal Strength

The devices investigated were found to have either an external or internal antenna (or a combination of both). For the first responding forensic investigator, this highlights the importance of properly inspecting the device internally and externally, without making assumptions that the external antenna is the only point for Wi-Fi transmission (Figure 4).

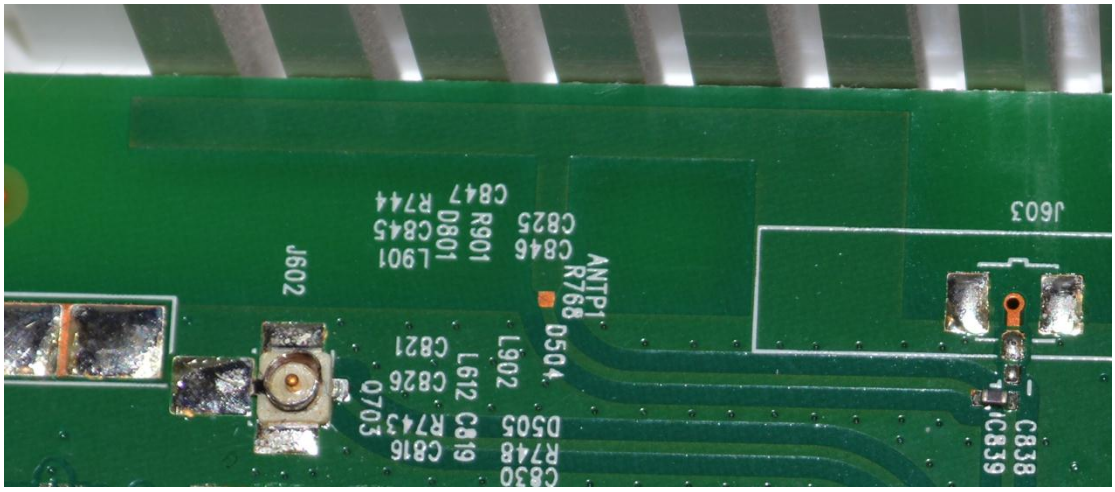

Figure 4 - F Antenna as found on a Thompson Bigpond TG782T device

Immediately after disconnecting the external antenna on the Thompson TG782T Wi-Fi router, it switched to the internal F antenna, thus preserving signal strength. Several Wi-Fi routers had similar antenna arrangements. Many Wi-Fi routers allow their external antennas to be removed. Removing any number of these antennas significantly reduces the ability for the router to provide an effective signal; however leaving any number of antennas still connected allowed the router to still transmit data effectively. Where a device had an internal aerial, which had been soldered directly to the circuit board, these antennas were either de-soldered from the circuit board or their shielded cable was cut (Figure 4). If the cable was cleanly cut and the wire was shielded, the device had no ability to transmit or receive data and was thus the Wi-Fi was deemed isolated.

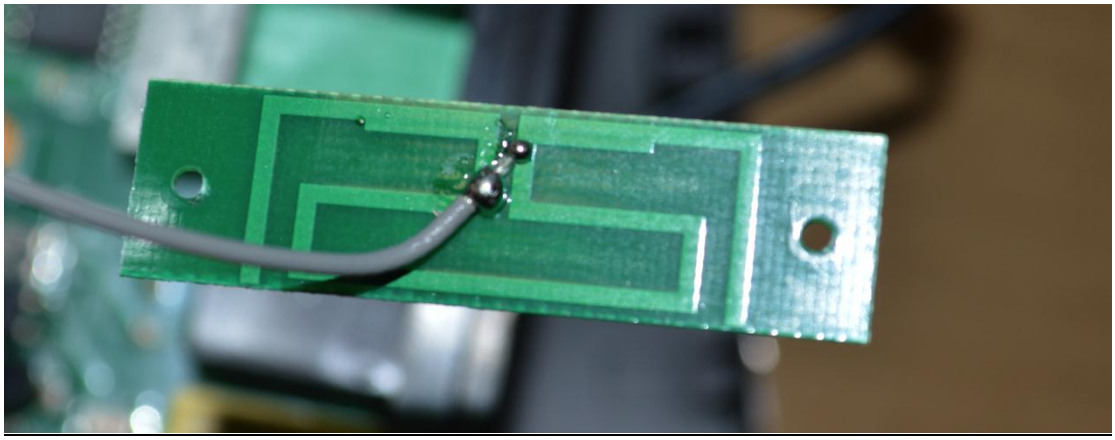

Figure 5 - Internal aerial as found on the iiNet Boblite GL411 device

A number of subject devices were tested using aluminium foil to block Wi-Fi data transmission. In all cases where aluminium foil was utilised to cover the entire device, the device was unable to communicate effectively. In cases where there was an opening in the aluminium foil, irrespective of where the opening was located, radio frequencies were able to leak beyond the confines of the aluminium foil (Figure 6). Similar risks could result

with the use of faraday bags, particularly in cases where the device needs to be kept powered. This is an important facet for a first responder to consider to minimise the contamination of evidence on the Wi-Fi router.

Figure 6 - TP-Link TL-WR1043ND covered in aluminium foil with large opening at the front

Memory

A brute force Wi-Fi authentication attack on a TP-Link WR1043ND, demonstrated that within 8 minutes the memory had been overwritten. During this time approximately 91,000 attempted connections were made. It was also found that the log files had been rotated. This meant that all history associated with a specific connection, prior to the attack, no longer resided in either the log files or the memory of the device. A subsequent authentication attack, limiting the authentication attacks to one attack per second, found that while the log files had been rotated, the memory still retained details after the 3 hour period of testing.

Additional tests within a busy office environment, in which the device had extensive network traffic, found the device typically only retained data for a maximum of 12 hours. After this period the chance of extracting a MAC address authentication request was minimal. These results suggest memory usage is extremely dependent on:

- The amount of traffic traversing the network;
- The number of authentication attempts; and
- The amount of free or available memory on the device.

Access Issues

For the majority of consumer grade Wi-Fi routers the ability to gain access via terminal or a shell has been removed as manufacturers have set an administration password, which is unknown and not included with product literature. In some Wi-Fi routers it was found the device allowed users shell access and then a firmware update later precluded this access (Turnbull & Slay, 2008). In the absence of a shell or terminal, ram captures are inhibited and detailed log analysis is reduced. The ability to connect to the Wi-Fi router's administration web interface is made difficult without the correct authentication credentials. However in some cases, the default administration details were found on the underside of the modem (Figure 7).

Figure 7 - Thomson branded ST585v6 Wi-Fi Modem sticker from underside

During inspection of the logic boards, some Wi-Fi routers had possible JTAG and serial port connections. These connections could potentially allow access via a console or a direct download. Typically these connections mitigate the need for access credentials. Ensuring the Wi-Fi router is powered on whilst removing the external casing to establish suitable connection points is challenging. Many of the pin configurations were unlabelled, and thus further analysis and research would be required, along with a suitable live-capture procedure.

In the absence of on board connections, the only remaining forensic process would be that of chip-off forensics. This technique involves the physical removal, using heat, to de-solder the microchip from the circuit board. Once removed, the microchip can then be connected to a NAND flash reader and its data subsequently interpreted. Typically this style of forensic exploration causes physical destruction to the device with the potential to negate the integrity of data and future operation of the Wi-Fi router.

DISCUSSION

Detailed Notes

During forensic investigations it is imperative that the investigator maintains detailed contemporaneous notes throughout the task. These notes should be similar to that of a police running sheet so the results can be utilised as evidence in court. The notes should also include the goals which were to be attempted, the actions towards reaching those goals, any critical decisions which were made at the time, the outcome – success or failure and the reasons why. Detailed notes are further critical in investigating Wi-Fi routers in that the process utilised may not necessarily work successfully on similar devices. This is an unfortunate factor associated with vendors revising and altering the hardware and software of each device, which is identified through associated revision numbers (i.e. A5).

Isolating and Seizing Devices

Wi-Fi routers can be sensitive and susceptible to forensic contamination, particularly if they are listening and logging beacon packets or possible authentication attempts. Once a crime scene has been declared, any Wi-Fi transmitting or receiving devices should be strictly quarantined from the area of concern. The Wi-Fi router should be kept powered up and isolated, with network connections disconnected. External antennas should be removed and the device should be preferably placed in a sealed faraday bag. However if one is not available to the first responder, it should at least be entirely covered in aluminium foil (with no holes present) to suppress any radio frequencies. In all cases where a live forensic acquisition is to be completed, the Wi-Fi router will need to be transported whilst powered on or evidence extracted at the scene.

Database of Devices

It is recommended that further research is undertaken to build a central database documenting Wi-Fi router specifications and characteristics. Once implemented, forensic investigators who have access to the database would benefit by accessing a quick point of reference, and increasing their knowledge of devices and evidence that may be afforded. The proposed database structure could use the following components:

1 Wi-Fi router table detailing the:
- Device model number;
- Hardware version ;
- Photograph(s) of the device; and
- Other specific device information.

The Wi-Fi table shows the physical device based on what can be read on it's labels and viewed in photographs.

2 A one-to-one relationship, star rating table.
- An indication of how forensically beneficial interrogating the device would be; and
- A explanation of the associated rating.

The star-rating table gives an overall rating of the ability for an examiner to collect data from the device. A single star rating may indicate a poor indicator whilst a high star rating could indicate shell access with the ability to download memory in a forensically sound manner. This information would benefit the first responder in adequately preparing for the at scene investigation.

3 A many-to-one relationship, hardware version table detailing:
- A hardware and firmware version of a device logic board;
- The number of serial ports on the device;
- The number of internal and external aerials; and
- Possible other hardware specific information;

The hardware version table records the differences between multiple software versions. Additionally it records the differences in the internal, component level designs of multiple devices.

4 A JTAG and serial access table
- Detail circuit board pin outs; and
- Configuration (including photographs to facilitate the process).

The JTAG/Serial Table addresses interfacing issues with the hardware of different devices.

5 A Firmware version table linked to the hardware version detailing:
- Versions of firmware;
- Default authentication credentials; and
- Known access credentials from manufactures.

A firmware version table would address the software differences along with the access credentials for those firmware versions.

6 An exploitability-rating table:
- A rating for the possible security/exploitation of the device; and
- An explanation of the metric for the rating.

The intention for this table is to demonstrate how exploitable the device firmware or hardware is for gaining access to the device. Should a device be more exploitable a higher rating maybe provider, a lower rating might demonstrate a device which is more secure.

7 A vulnerability assessment table with examples of successful vulnerabilities;

This table holds vulnerabilities and how they might relate to a device.

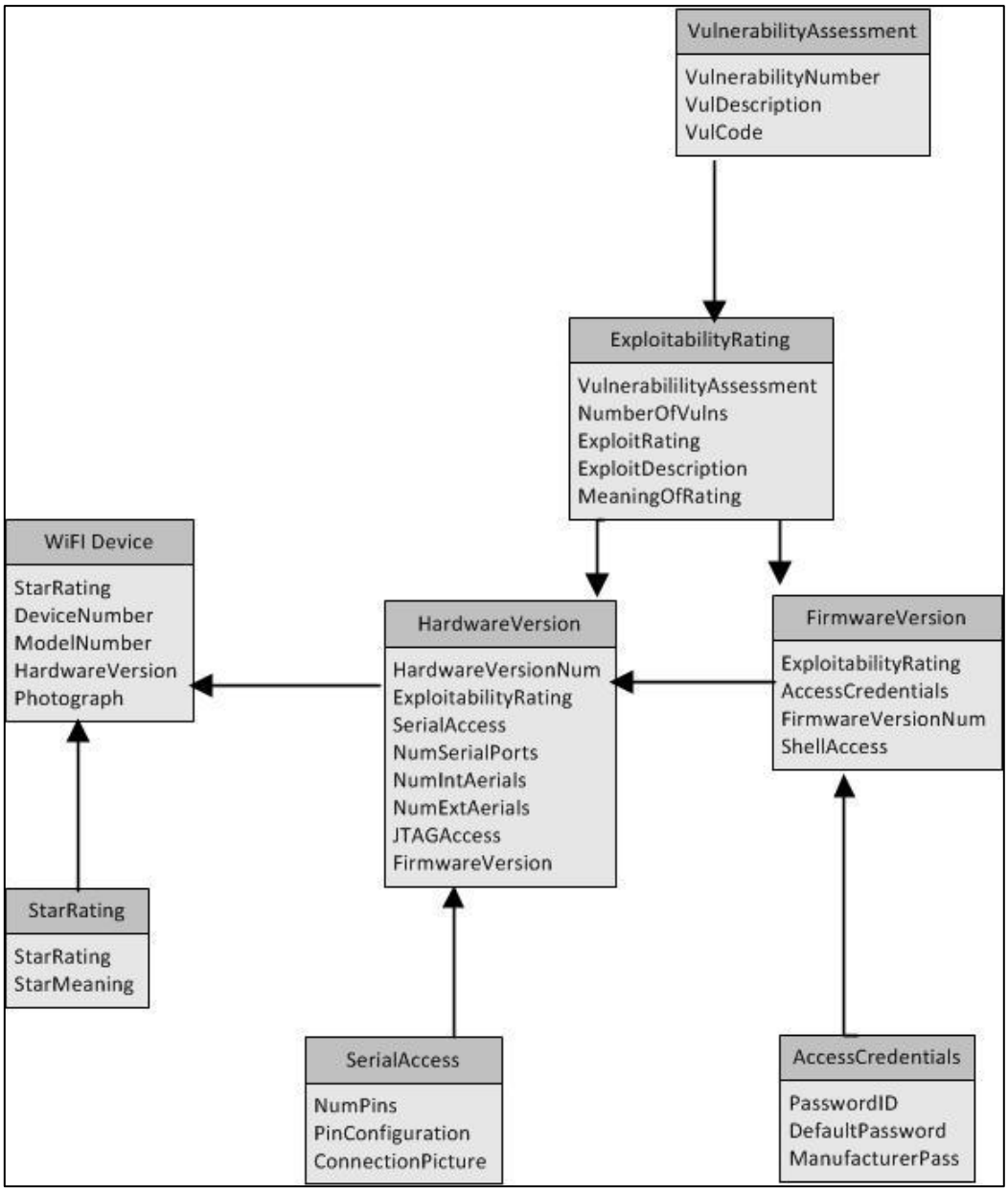

Figure 8: The proposed conceptual diagram of the database required

Standards

Despite the limited number of devices examined during this research, it was found that the multitude of Wi-Fi routers function differently from one another. Manufacturers regularly change the devices between firmware and hardware versions to suit their needs, and are typically motivated by financial reasons (Constantin, 2014). Manufacturing standards for Wi-Fi devices would be beneficial for subsequent law enforcement based investigations. Establishing these standards in Australia would provide several advantages:

- The device's data of interest could be extracted more accurately;
- The manner of obtaining data of interest would be simplified; and
- Training of forensic investigators would be simplified;

For these standards to be accepted by consumers, they need a simple way to recognise the Wi-Fi router they are about to purchase is both:

- A secure device for their day-to-day internet activities, produced by a legitimate Australian authorised identity; and
- A device that law enforcement agents can if required gain access to with minimal disruption.

A possible law enforcement tick of approval, or symbol, is a suitable example. This symbol can be placed on the packaging of manufactured products to educate consumers of the benefits of purchasing this device over another, which features no approval. For manufacturers to obtain this tick, they will need to conform to a series of requirements. Similar outlines have been presented to the manufacturers and customers purchasing CCTV systems (ANZPAA, 2014). For Wi-Fi devices, the most obvious need is a mechanism to connect and download the data of interest applicable to the device.

CONCLUSION

The Wi-Fi router could contain a critical piece of evidence for a forensic investigator. The ability to place an offender at a specific time and place, based on capturing their mobile device information, could lead to either a successful prosecution or plead of guilt.

However, as demonstrated through this research paper, multiple issues exist for extracting data of interest. The data capture is potentially costly, due to the differences in hardware, software and lack of standardisation amongst devices. In addition this capture typically needs to be completed at a scene, with the device remaining powered up. Due to these costs, further research is required before a comprehensive framework can be developed and put into the public domain to support first responders. A detailed database of Wi-Fi router specifications and characteristics could be used within the courts and legal practices of Australia.

Future research will focus on the development of an open accessed detailed database encompassing a range of Wi-Fi routers available in Australia. It is anticipated that the sharing of knowledge by various communities will facilitate the streamlined process of data extraction from Wi-Fi routers. Ultimately this further research of Wi-Fi routers and the potential evidence to law enforcement and Australian courts will assist making the community a safer place.

REFERENCES

ACMA. (2014). *Tablets take off: take-up and use of tablet computers in Australia*. Retrieved from http://www.acma.gov.au/theACMA/engage-blogs/engage-blogs/Research-snapshots/Tablets-take-off-take-up-and-use-of-tablet-computers-in-Australia

AIC. (2015). *Homicide in Australia: 2010–11 to 2011–12: National Homicide Monitoring Program report*. Retrived from http://aic.gov.au/media_library/publications/mr/mr23/mr23.pdf

Akers, P., McGrew, W., Dampier, D. A. (2011). *WiFi Stakeout: A network forensics tool for reconnaissance and first responders*. Paper presented at the 2011 International Conference on Engineering and Industries. Jeju Island, Korea

Althuser, J. (2015). *7 ways hackers can use Wi-Fi against you*. Retrieved from http://www.computerworld.com/article/3003202/data-security/7-ways-hackers-can-use-wi-fi-against-you.html#slide8

ANZPAA. (2014). *Police Recommendations for CCTV Systems*. Retrieved from https://www.anzpaa.org.au/upload/Corporate%20News%20and%20Publications/ANZPAA%20Publications/Police%20Recommendations%20for%20CCTV%20Systems.pdf

Könings, B. Bachmaier, C., Schaub, F. Weber, M. (2013). *Device Names in the Wild: Investigating Privacy Risks of Zero Configuration Networking*. Paper presented at the 14th IEEE International Conference on Mobile Data Management. Milan, Italy

Constantin, L. (2014). *Fifteen new vulnerabilities reported during router hacking content*. Retrieved from http://www.pcworld.com/article/2464300/fifteen-new-vulnerabilities-reported-during-router-hacking-contest.html

Fu. X., Zhang, N., Pingley, A., Yu, W., Wang, J., Zhao, W. (2012). The Digital Marauder's Map: A WiFi Forensic Positioning Tool. *IEEE Transactions on Mobile Computing*. 11(3), 377-389

Hamida, B. E., Chelius, G. (2010). *Investigating the impact of human activity on the performance of wireless networks — An experimental approach*. Paper presented at the 2010 IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks. Montreal, Canada

Holman, C. (2012). *Manufacturers of wireless devices at Swinburne*. Retrieved from http://caia.swin.edu.au/reports/121213A/CAIA-TR-121213A.pdf

IEEE. (2015). oui.txt. Retrieved from http://standards-oui.ieee.org/oui.txt

Liu, Z., Chen, Y., Yu, W., Fu, X. (2010). *Generic Network Forensic Data Acquisition from Household and Small Business Wireless Routers*. 2010 IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks. Montreal, Canada

Minnaard, W. (2014). Out of sight, but not out of mind: Traces of nearby devices' wireless transmission in volatile memory. *Digital Investigation*. *11*(1), 104-111.

Potts, J. (2014). Economics of public WiFi. *Australian Journal of Telecommunications and the Digital Economy*. *2*(1), 1-9

Rogers, E. (2015). *Survey: Australian Smartphone and Table Usage*. Retrived from http://www.hapticgeneration.com.au/survey-tells-us-how-australians-use-smartphones-and-tablets/

Szewczyk, P. (2009). *ADSL Router Forensics Part 2: Acquiring Evidence*. Paper presented at the 7th Australian Digital Forensics Conference. Kings Hotel, Perth, Western Australia

Szewczyk, P. (2011). Analysis of Data Remaining on Second Hand ADSL Routers. *Journal of Digital Forensics, Security and Law*. 6(3), 17-31

Turnbull, B., Slay, J. (2008). *Wi-Fi Network Signals as a Source of Digital Evidence: Wireless Network Forensics.* Third International Conference on Availability, Reliability and Security. Barcelona, Spain