Legal and Technical Implications of Collecting Wireless Data as an Evidence Source

Benjamin Turnbull, Grant Osborne, and Matthew Simon

Defence and Systems Institute, University of South Australia
Mawson Lakes Campus, Mawson Lakes, South Australia 5095
Benjamin.Turnbull@unisa.edu.au, Grant.Osborne@unisa.edu.au,
Matthew.Simon@unisa.edu.au

Abstract. The collection of digital devices for forensic analysis is an area that requires constant revision. New technologies and connectivity options change what devices are able to hold electronic evidence and also the methods needed to secure it. This work focuses on the development of an 802.11-based wireless networking (Wi-Fi) forensic analysis tool that can aid in the identification and collection of evidence by identifying the presence of wireless networks and the devices to which they are attached. Specifically, this paper seeks to discuss the potential legal and technical challenges faced in the development of a wireless forensic tool.

1 Introduction

It has been hypothesized that the collection and analysis of wireless signals is of potential benefit to investigators. Specifically, investigators may wish to know of wireless networks within an area and the topography of each when identifying and collecting physical evidence. This may be for both proactive and reactive investigations.

There are several forms of misuse and crime that current investigative processes are unlikely to detect and identify, with the result that such devices may not be seized as sources of evidence, despite potentially having potential value (Turnbull & Slay 2005). Several cases exist in the public domain to substantiate this claim. There are also a number of potential, but unsubstantiated methods that wireless devices can be misused that may remain undetected by investigating bodies.

The electronic analysis of computers and devices would be incomplete if devices are undetected when collection occurs as they will not be present for later analysis. This is especially possible for wireless devices and systems that may be active but not physically accessible. Additionally, within a computer forensic examination, there is no published process for extracting the number and details of wireless networks that a device has connected to.

There have been several academic sources calling for the need for further investigation into the forensic collection and analysis of wireless devices noting several potential issues that may result from its use. Mike Schiffman, formerly of *@Stake*, was the first to discuss the need for a forensically sound 802.11 tool or series of tools at the 2002 Blackhat computer security conference (Schiffman 2002).

M. Sorell (Ed.): e-Forensics 2009, LNICST 8, pp. 36 – 41, 2009.

However, the potential contents and uses of this toolkit were never discussed and the project remained incomplete. From an academic perspective, Casey and Ferraro stated in the text *Investigating Child Exploitation and Pornography*; *the internet, law and forensic science* that:

"Wireless access to the Internet will undoubtably create new challenges for law enforcement. Wireless computing devices are by nature highly mobile, and wireless Internet access is more difficult to track than hard-wired systems. Security weaknesses also can wreak havoc because attributing criminal activity to an individual can become difficult"(Casey & Ferraro 2005). D'Ovidioa (2007) has also acknowledged the growing potential for wireless devices to be misused which he states as a factor in the growth of computer-based crime.

Schiffman (2002), Casey and Ferraro (2005) and D'Ovidioa (2007) have identified a research need. Wei (2004) has taken this further and discussed possible means of countering the issues raised and introduces the idea of wireless forensics as a possible extension to network forensics. Wei introduced several possible locations of evidence in a wireless network and made a distinction between the possible sources: evidence from the network and evidence via the network. However, this work gives no further details or discussion on wireless forensics either as a form of network forensics or with wireless devices potentially being a form of evidence.

This work seeks to explore the Australian context for the development of wireless networking analysis as a forensic tool, specifically on the effectiveness, forensic soundness and legality. Specifically, it is the authors assertion that a wireless network forensic tool, as with any other computer forensic program, should comply with fundamental forensic principles. Specifically the system should have the following features:

- Minimal interaction - minimal interaction with potential sources of evidence, and where such interaction is required, the interaction and effects understood and justifiable.
- Accuracy and repeatability – the use of the system in the same environment will provide the same result. Also, that the system operates accurately, and the technical limitations (if any) are known.
- Operation in accordance with all legal requirements.

These three features represent forensic minimums for software that potentially has a legal outcome. The first feature can be related to work from McKemmish (1999) or Pollitt (2007) and is linked with forensic process. The second feature required in a forensic application is an extension on scientific principle ensuring repeatability in experimentation. The final feature stated is of importance in all areas of computing, but requires in-depth consideration in the development of forensic and analysis tools where the product may have legal outcomes.

2 Existing Wireless Network Scanning Software

There are several products, designed for both consumers and for network administrators, which perform wireless site surveys and monitor network traffic. Beyond the

systems provided by Operating Systems, the most applicable examples of wireless network monitors are the applications *NetStumbler* (Milner 2004) and *Kismet* (Kershaw 2007).Prior to developing an application to search for wireless networks for forensic investigators, it is wise to analyse similar existing applications that perform similar functions.. Whilst there are several other applications, both open-source and commercial, these are two that encompass a large cross-section of the community. Both have a standard feature-set and implement known methods.

The major difference between NetStumbler and Kismet is their mode of operation. NetStumbler is active while Kismet is passive in nature (Vladimirov, Gavrilenko, et al 2004). Active wireless network scanners actively probe networks by sending out *probe request* packets, to which wireless Access Points respond with *probe responses*. Passive network scanners do not actively probe networks in the area. The card enters a mode of operation called *monitor mode*, which allows it to receive all network traffic on a given channel without having to join a specific network.

From a forensic perspective, there are several issues with active network scanners:

- Information gathered relates only to wireless Access Points and Peer-to-peer networks, rather than other clients and devices which a wireless card cannot immediate connect to.
- There is a reliance on wireless Access Points to be self-identifying.
- Active wireless scanners are interacting with the wireless networks for which they are gathering information. Any such interaction will alter the environment and is detectable.

The designed use of active network discovery is for users to locate wireless networks. It is understandable that the most immediate limitation in its use is that it will only detect wireless Access Points or Peer-to-Peer wireless networks. It will not provide an outline of all devices on a network.

Whilst the use of the probe request and probe response frames are part of the IEEE 802.11b/a/g wireless specifications (Institute of Electrical and Electronic Engineers 1999), there are several vendors that deviate from the specification by allowing wireless Access Points to ignore probe requests. This practice is called ‘cloaking’ and will effectively hide wireless Access Points from active network scanning used by Operating Systems and active network scanners such as NetStumbler. Whilst this presents a limitation, it does not invalidate any findings from such systems but may mean that the findings are incomplete. Networks found would not be incorrect, but more networks may exist than discovered.

It is for three reasons that active network scanners are less than ideal for forensic purposes: they rely on Access Points being self identifying, limited information is obtainable (only wireless Access Points, rather than all networked devices) and interaction is required..

By contrast to active network scanners, applications such as Kismet are passive. They operate by placing the wireless card into monitor mode, which allows the receipt of all wireless data on a specific channel without any interaction. Analysis of this data may allow all wireless network Access Points and clients to be discovered, regardless of their cloaked status. In principle, the use of passive network scanning is more suitable for forensic purposes. No interaction is required to collect information, as no packets are sent. Additionally, all network devices can be identified rather than

just Access Points. The issue that makes existing implementations of passive wireless network scanners less than suitable for forensic purposes relates to the potential legal issues with current implementations. This is introduced as follows.

3 Legality of Wireless Network Interception

The Australian Telecommunications Act (1997) and Telecommunications (Interception and Access) Act (1979) has equivalent legislation in many western countries. These define the law for private individuals, companies and law enforcement, to intercept different forms of telecommunications.

The definition of a telecommunications network is equally applicable to wired and wireless computer networking. However, the definition of a telecommunications network within the Telecommunications Act (1997) and the Telecommunications (Interception and Access) Act differ. The Telecommunications Act is much broader in its definition, stating that a *"a "telecommunications network" means a system, or series of systems, that carries, or is capable of carrying, communications by means of guided and/or unguided electromagnetic energy"* whereas the Telecommunications (Interception and Access) Act (1979) appends *"…or both, but does not include a system, or series of systems, for carrying communications solely by means of radiocommunication"*.

From respective definitions, it can be interpreted that whilst the Telecommunications Act does consider purely wireless networks as telecommunications networks (as does the Radiocommunications Act), the Telecommunications (Interception and Access) Act does not. The additional wording in the definition for a telecommunications network explicitly excludes networks that are solely radiocommunication-based.

Although the Radiocommunications Act (1992) may be applicable in some circumstances, a wireless network may or may not be entirely wireless – it may or may not have wired components. Any non-wireless component makes such a network a telecommunications network. It cannot be easily determined whether a wireless network operates purely by radio-frequency or is connected to a wired network.

To fully examine all legal issues, both forms of wireless network must be examined – the legalities for purely radio-based communication and a wireless network that has a wired component. To ensure legal compliance, both acts of legislation must be followed, so that regardless of network topology is, the interception of data is legal.

In the event that a network topology has both a wired and wireless component, the most appropriate legislation regarding network data interception is the Telecommunications (Interception and Access) Act (1979). Of note is that this legislation specifically prohibits the capture and storage of network data without a warrant. There are several exceptions such as being an intended recipient, or as required for finding faults in service by authorised individuals. This is relevant to this work, given that the purpose of the intended application relates directly to the capture and analysis of wireless network traffic. However, the term "data" within this legislation is interesting, as it does not include metadata, but relates directly to the payload of a packet or frame.

In all IP-based networks, headers of data-packets in transit may be examined by either intermediate nodes or by nodes in a shared broadcast medium (Zalewski 2005).

This information is analogous to the address on an envelope and the frame's payload being the private contents. Network-level protocols are defined such that intermediate nodes need only examine headers rather than the payload. Relating this information to legislation documenting telecommunications interception, there are obvious issues should that header-information interception be included in such legislation. Principally, interception of packet header-data is intrinsic to the operation of such networks. It is therefore not surprising that the Telecommunications (Interception and Access) Act (1979) does not legislate conditions for intercepting header information, or metadata regarding communication. There is therefore no legal impediment outlined in the Telecommunications (Interception and Access) Act that prevents the collection of such data. The frame and packet payloads themselves may be considered communication; however headers may be defined as a form of metadata. Relating this legislation to existing wireless applications in existence, it can be inferred that passive network discovery applications may be illegal by virtue of the fact that they record raw frames – both headers and payloads - from wireless networks. This is against legislation within the Telecommunications (Interception and Access) Act (1979) and cannot legally be performed without a warrant. However, Kismet, in its fundamental operation, operates similarly to all 802.11 network devices. In a shared collision domain, all network data must be collected by every client. Through header analysis, clients can discard packets if they are not the intended recipient. Therefore, if the proposed system was to only analyse and store frame headers, there would not be a requirement under the Telecommunications (Interception and Access) Act (1979) to obtain a warrant.

At this stage, the options for developing a wireless forensic tool are to either adapt an existing open-source passive wireless network scanner, or to develop an equivalent from the ground-up. There are advantages and disadvantages to each of these two methods. Whilst it is beneficial to leverage on existing, operational systems, it has been discussed that the end-user operational requirements and legal strictures for systems such as Kismet are very different to that required for forensic investigators. Kismet is designed to locate wireless networks, perform network-based testing and alerts. It does not discuss any legal issues associated with its use. A tool designed for investigators will require some overlap in functionality with a network administration utility, but will require differences in collection, logging and in the interface.

Adapting existing source code is a potential disadvantage in the development of a forensic wireless network scanning application. Large-scale modifications would be required to ensure that legal requirements are met. Specifically, before existing passive network capture software is used, payloads would need to be stripped from the captured data. This would require substantial sections of the code to be rewritten. For this reason, the decision was made to develop the proposed system without any reliance on existing passive scanning software products. This allowed the software development team to ensure that legal constraints were maintained in all sections of the code.

4 Conclusion and Outcomes

Whilst development of this tool is ongoing, its creation can now be validated as conforming to network and computer forensic science principles. Without such in-depth

analysis, it is possible that application outcomes would have been legally unusable or technically less than adequate. This work highlights the potential pitfalls that may occur in the use of non-forensic software for forensic purposes; there are constraints required for forensic outcomes and software used. There are several areas of future work that this research has highlighted, and the most obvious is the development of the tool discussed. Similarly, this work has highlighted that the use of non-forensic tools for forensic purposes is not always appropriate, legal or technically sound.

References

Australian Legislation - Radiocommunications Act (1992)

Australian Legislation - Telecommunications Act (1997)

Australian Legislation - Telecommunications (Interception and Access) Act (1979)

Casey, E., Ferraro, M.: Investigating Child Exploitation and Pornography; the internet, law and forensic science. Elsevier Academic Press, Massachusetts (2005)

D'Ovidioa, R.: The evolution of computers and crime: complicating security practice. Security Journal (2007)

Institute of Electrical and Electronic Engineers. 802.11b Standard (1999), http://www.standards.ieee.org/ (retrieved May 24, 2003)

Kershaw, M.: Kismet Readme - Kismet 2007-01-R1 (2007), http://www.kismetwireless.net/documentation.shtml (retrieved January 12, 2007)

McKemmish, R.: What is forensic computing? Australian Institute of Criminology (1999), http://www.aic.gov.au/ (retrieved March 12, 2003)

Milner, M.: NetStumbler v0.4.0 Release Notes (2004), http://www.netstumbler.com/downloads/netstumbler_v0.4.0_release_notes.pdf (retrieved November 13, 2006)

Pollitt: An Ad Hoc Review of Digital Forensic Models. In: Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE 2007) (2007)

Schiffman, M.: The need for an 802.11 Wireless Toolkit. Paper presented at the Proc. BlackHat Security Conference, Las Vegas, United States of America, July 31 (2002)

Turnbull, B., Slay, J.: The 802.11 Technology Gap Case Studies in Crime. In: Tencon 2005 - IEEE Region 10 Conference, Melbourne, November 21 (2005)

Vladimirov, A.A., Gavrilenko, K.V., et al.: Wi-Foo: The Secrets of Wireless Hacking. Pearson / Addison Wesley, Boston, Massachusetts (2004)

Wei, R.: On A Conceptual Model of Network Forensics System for Information Security. In: The Proceeding of The Third International Conference of Information Systems Technology and its Applications STA 2004, Salt Lake City, Utah, United States of America (2004)

Zalewski, M.: Silence on the Wire: A field guide to passive reconnaissance and indirect attacks. No Starch Press Inc., San Francisco (2005)