2016

A forensic examination of several mobile device Faraday bags & materials to test their effectiveness

Ashleigh Lennox-Steele
Auckland University of Technology, a.lennoxsteele@gmail.com

Alastair Nisbet
Auckland University of Technology, alastair.nisbet@aut.ac.nz

DOI: 10.4225/75/58a550b153635
Lennox-Steele, A., & Nisbet, A. (2016). A forensic examination of several mobile device Faraday bags & materials to test their effectiveness. In Valli, C. (Ed.). (2016). *The Proceedings of 14th Australian Digital Forensics Conference, 5-6 December 2016, Edith Cowan University, Perth, Australia*. (pp 34-41).

A FORENSIC EXAMINATION OF SEVERAL MOBILE DEVICE FARADAY BAGS & MATERIALS TO TEST THEIR EFFECTIVENESS

Ashleigh Lennox-Steele, Alastair Nisbet
Security & Forensic Research Group, Auckland University of Technology
Auckland, New Zealand
a.lennoxsteele@gmail.com, alastair.nisbet@aut.ac.nz

Abstract

A Faraday bag is designed to shield a mobile phone or small digital device from radio waves entering the bag and reaching the device, or to stop radio waves escaping through the bag from the device. The effectiveness of these shields is vital for security professionals and forensic investigators who seize devices and wish to ensure that their contents are not read, modified or deleted prior to a forensic examination. This research tests the effectiveness of several readily available Faraday bags. The Faraday bags tested are all available through online means and promise complete blocking of all signals through the bag. Additionally, other materials that can be used if a Faraday bag is not available, such as tin foil and a tin can are tested and compared with the Faraday bags. A selection of common mobile phones from various manufacturers is tested in the shielding material. Additionally, 3G / 4G, WiFi and Bluetooth are tested with the bags and materials on those so equipped devices to ascertain whether the material blocks all signals from communicating technologies on the phones. Results show that performance of the bags is not as promised by most vendors and that in urgent situations other materials at hand may suffice to perform the same function as a Faraday bag.

Keywords
privacy, security, shielding, mobile, forensics, Faraday bags

INTRODUCTION

The utilisation of smart mobile devices plays a key role in the majority of day-to-day lives, where most carry at least one electronic device, whether they be for corporate use as a portable office, or personal use for tasks such as social networking and entertainment (Rajendran & Gopalan, 2016). This reliance on smartphones is credited to their proven advantages regarding efficiency in fulfilling both personal needs and business development, supported by the influx of availability and variety of mobile devices and their compatible applications (Khan, Abbas, & Al-Muhtadi, 2015). Current mobile devices, specifically the smartphone, combine telephony and computer services in a convenient handheld device. Standard telephone services are provided through a cellular network, while Internet services are utilised through a Wi-Fi connection or via 3G and 4G cellular data networks (Soukup, 2015). Google's Android, and Apple's iOS are the two main platforms which dominate today's mobile market (FireEye, 2015), with the everyday use of smart devices steadily increasing, while the utilisation and cost of basic feature phones and personal computers continually fall (Ophoff & Robinson, 2014). Where older models of mobile phones could only store a limited amount of data, which was easily obtainable by forensic investigators, the increased popularity and development of smart devices has complicated the techniques which must be employed by forensic investigators in order to retrieve the many variants of stored data in a forensically sound manner (Bennett, 2012).

LITERATURE REVIEW

A mobile device must have at least one wireless network interface to allow for data communications, whether it be Wi-Fi, cellular networking or additional technologies which can be used for connecting a device to networks or the Internet, as well as providing built-in data storage. In order to be considered a mobile device, the device must host an operating system which is not considered a complete operating system such as found on a desktop or laptop and have compatible applications which are available through multiple means. The smartphone has been described by Androulidakis (2016) as one of the most characteristic digital devices of current times, with its pervasion into everyday life and worldwide distribution.

Over time, an abundance of data is collected and stored on a smartphone based on its use, which is strongly correlated to the device's owner or primary user. This stored data has become increasingly sought after and may be involved in court trials to support the solving of crimes with evidence which can be retrieved from the device. Some types of evidence which can be extracted from a mobile phone as identified by Androulidakis (2016), include; device location, which can be based on the serving base location or GPS data; association of

contacts, based on call logs which detail incoming and outgoing calls to and from the device; and communication content such as messages and emails which may have been sent, received or stored on the handset. Digital Evidence has been defined by the National Institute of Justice (2016) as information which is stored or transmitted in binary form which can be relied on in court. Digital evidence has grown from being primarily associated with electronic crime to now being utilised to support the prosecution of all crimes due to the nature of information which individuals store on their personal devices it may be possible to derive critical evidence regarding criminal intent, whereabouts in relation to a crime, or relationships to other suspects or involved parties.

As identified by Rajendran and Gopalan (2016) in their mobile forensics investigation lifecycle process, once a digital device has been acquired, and information regarding the devices specifications and its surroundings upon acquisition have been gathered, the immediate action which needs to be taken is disabling the device from not only the mobile network and the Internet, but also disabling Bluetooth, tethering, and any other kind of external connections. Androulidakis (2016) states that the main principle of digital forensics is the preservation of data. This supports the idea of data preservation and network isolation as a compulsory measure to ensure that data cannot be altered in order to stand up in court. In the case that digital evidence has been altered, which can occur due to data which can change or destroy the contents of a mobile device being received or transferred, a court case can be lost. Incoming traffic from the network such as phone calls, messages or communication with installed apps can result in the contamination of potential evidence. In addition to this incoming traffic, it is possible that destruction mechanisms could be configured on the device which can result in the deletion of data or the locking of the device (Androulidakis, 2016). The following step in the aforementioned lifecycle is to ensure the preservation of the smartphone's data. It is suggested by Rajendran and Gopalan (2016), in order to support data preservation, that electronic devices be stored in a Faraday bag.

Faraday bags are described by Doherty (2016) as similar in appearance to antistatic bags, with the difference being that an antistatic bag will prevent damage to electronic devices from static electrical charges which have built up, whereas a Faraday bag poses the purpose of protecting electronic devices from external connectivity. Faraday bags are based on the concept of the Faraday cage, which is an enclosure which prevents external signals from reaching electronic devices. Doherty (2016) details the effectiveness of a Faraday bag being reliant on the materials of which it is made, the purpose of which is to stop wireless signals from penetrating the bag and reaching the device, which in turn supports the protection of the devices integrity from external influences. While awaiting examination, it is crucial that effective measures are taken which prevent any data which is stored on a device from being altered or remotely destroyed. Gershowitz (2013) identifies three operations which could be utilised in order to protect device integrity without utilising changes to the running applications so as switching off WiFi or entering Airplane Mode, these are: an extraction device that can copy phone contents to a secure offsite location; a Faraday bag; or alternatively a piece of aluminium foil. The benefits of the data extraction device at the time of seizure are evident. However, it is likely that high costs will be associated with such a device and it is unlikely that a forensic investigator or Police Officer will have such a device with them at all times. The benefit of using a Faraday bag is that once inside, a phone is no longer able to communicate with any external sources, and in turn, external sources are unable to reach a phone which is stored in a Faraday bag.

Generally, the primary material which Faraday bags are made from is aluminium foil, which suggests that the utilisation of a simple solution such as wrapping a mobile device in aluminium foil may provide many of the same benefits as a Faraday bag. Although it is possible that aluminium foil may not completely prevent all attempts at communication with the wrapped device, it may act as a suitable intermediary process between the seizure of the device and the secure transportation and storage of a device until further actions can be taken with the potential evidence. In support of the Faraday option Androulidakis (2016) suggests that the best solution for isolating a device from the network and preserving its data is the use of a "Faraday Cage" which isolates electromagnetic radiation. It is stated that Faraday bags are smaller, more convenient option for device isolation. Ayers et al. (2014) define evidence preservation as the process for securely maintaining custody of a digital device without its contents being altered, and is the first step in digital evidence recovery. Incorrect procedures, or improper handling of a device can cause the loss or alteration of digital data. An inability to correctly preserve evidence can forfeit a whole investigation, and potentially lead to the loss of a legal case due to the acquired evidence being disrupted and therefore not standing up in court (Ayers et al., 2014). NIJ (2008) detail recommended items which first responders should have to comprise a "digital evidence collection toolkit" to assist them in performing their investigation in a forensically sound manner. Within this toolkit, alongside notepads, gloves, and a camera for documenting evidence, it is suggested that radio frequency shielding materials be on hand in the case that smartphones or other mobile communication devices are involved in an investigation and need to be securely seized. The specific radio frequency shielding materials which are suggested by NIJ (2008) are Faraday isolation bags, or aluminium foil.

NIJ (2008) emphasise the importance of leaving a mobile device in the power state in which it was found. If the phone is on when the first responders arrive, the phone should be left on, if it is powered off, then it should remain off; the device should then be packaged in a material which will shield it from incoming signals, in preparation for secure transportation. In contrast to this, SWDGE (2011) state that in the event a mobile device cannot be processed immediately, it should be powered off, its battery removed, and not turned back on. Benefits of turning mobile devices off include: the preservation of call logs and last cell tower location information (LOCI); avoiding overwriting of deleted data; stopping remote data destruction signals from reaching the device; and preventing accidental device usage such as messaging, dialling, and accessing and altering files and data. The risks of switching off the mobile device can result in the activation of security and authentication mechanisms such as PIN codes and passwords which further restrict access to the devices content (SWDGE, 2011). However, in support of NIJ's (2008) claims, SWDGE (2011) state that in the event a mobile device must remain powered on, it should then be isolated from the network. Rather than suggesting the use of radio frequency shielding material to avoid the mobile device communicating with cell towers and in turn, altering the phones data, SWDGE (2011) propose that mobile devices can be switched to "Airplane" mode to limit their access to the towers, and where practical, first responders should disable the device's WiFi, Bluetooth, RFID, and infrared communications. Whilst the guidelines provide for a range of procedures which at times are conflicting, it was decided for the purpose of these experiments that a forensic investigator would likely place the phone in a Faraday bag or other shielding material without altering any settings or switching off any technologies.

There is currently a paucity of empirical research on the effectiveness of common Faraday bags for mobile signal shielding. There was even less available in regards to literature which provided findings, results or suggestions in relation to alternative materials which may be utilised in the place of Faraday bags for the purpose of blocking mobile signals from reaching a smartphone. That which could be derived from the literature surrounding alternative materials is the effectiveness of tinfoil regarding the blocking of signals can be attributed to its conductivity. This suggests that any conductive material such as copper, iron, and steel have the potential to create a barrier between a mobile device and radio signals or at least cause interference between the sending and receiving of frequency signals (Barrett, n.d.; Science Buddies, 2011).

RESEARCH DESIGN

The first step in the design of the experiments was to review several previous studies into shielding properties of various materials. None of these studies provided all necessary steps that were suitable for this research so ideas for testing were based on the previous research but with necessary modifications. As mobile devices may have up to three different wireless technologies active, 3G / 4G, WiFi and Bluetooth, it was decided to test all three. It was recognized that different phone manufacturers and models may provide differing results so six common phones from three different manufacturers were chosen for the tests. Five easily available Faraday bags were chosen for testing representing four different manufacturers. To compliment these dedicated Faraday bags and to act as a comparison, tin foil and a tin can were added to test as these were materials that could likely be located by an investigator at a scene when a Faraday bag is not available. The experimental design is described in the following section.

Experimental Design

This research investigates the shielding and preservation capabilities of a range of different Faraday bags, with the main research question to be addressed being: *What is the capability of Faraday bags and alternative materials for blocking mobile network, Wi-Fi, and Bluetooth signals to mobile devices for the purpose of data preservation?* This research provides an opportunity to explore the effectiveness of materials in supporting mobile evidence preservation in order to improve the mobile forensic investigation process. By providing a comparison of a range of available Faraday bags, in addition to two alternative household materials which could be used in the absence of Faraday bags, forensic investigators have the capability to identify materials which may be beneficial to their investigations, and provide support to the preservation of potential evidence.

Table 1: Experimental phones & materials

Mobile Devices		Shielding Materials
Samsung Galaxy S3		*Faraday Defence 3mm*
Samsung Galaxy S5	*Tested with*	*Faraday Defence 7mm*
Samsung Galaxy S7		*EDEC Black Hole Faraday Bag*
Sony Xperia Z5		*Blackout Faraday Shield*
Apple iPhone 5		*ESD Faraday Cage Bag*
Samsung GT-B2710		*Aluminium foil & Tin can*

Research Method

To ensure consistent results, the same method was implemented for each mobile device and Faraday bag combination. The prerequisites for testing included:

- A fully charged battery, due to the high drain nature of the testing
- Device volume set to maximum to support identification of failed shielding where bags restrict vision and interaction
- Installed and configured Viber application for placing and receiving calls through Wi-Fi connection
- Bluetooth turned on, device visibility set as discoverable, and discovery timeout set to "Never"
- Screen timeout set to the longest period available per device
- Mobile Data turned off as to not interfere with the Wi-Fi tests

Prior to shielding the receiving device, two calls will be placed, one over the network, and one over Wi-Fi, using the Viber application, to ensure that all required features were functioning appropriately. In addition, a Bluetooth search will be conducted from the transmitting device to ensure visibility of the phone being tested.

The mobile device is placed in a Faraday bag and a timer pre-set for 30 second intervals over the duration of two minutes. Within every 30 second interval, a network call, and a Viber call is made from the transmission device, to the shielded, reception device. If the communications are received by the shielded device, the test will be considered a failure, and in the event no signals are received then a success is recorded. In the event the majority of results for a specific shielding bag have failed, the shielded device is placed within another bag, so that the device is nested within two bags of the same make and the testing process is then repeated. If after two bags the results are still mostly failures, the testing process is performed again with three nested bags. If after three nested bags the tests still fail, the Faraday bag in question will be considered completely ineffective.

Independent tests are conducted for Bluetooth connectivity to determine the effectiveness of the shielding materials at varying distances, 1 metre, 3 metres, 5 metres and 10 metres. In the event of a failed test, the nesting approach will not be implemented for the Bluetooth testing but instead the distance between the transmitting and shielded receiving device will be increased. If after 10 metres Bluetooth communication can still be established, the material being tested will be considered ineffective.

RESULTS

The 7 shielding materials, 5 Faraday bags, tin foil and a tin box were all tested using similar parameters. Of primary interest is the 3G / 4G shielding capabilities as this is the communication technology that provides the capability to alter the data on the phone from a considerable distance. The results of the experiments are shown in figure 1 where the vertical bar represents a failure to shield the reception.

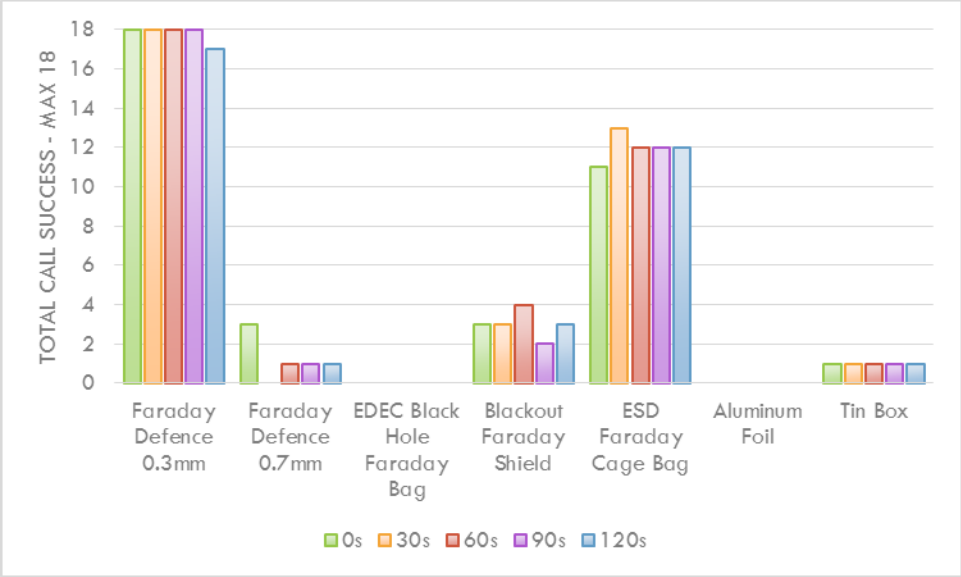

Figure 1. 3G / 4G Call Failures

Of the 7 tested scenarios, only the EDEC Black Hole Faraday Bag and the aluminium foil shielded all 18 calls from penetrating to the device. The time of the phone call had minimal impact on the measured ability of the material so that a very short call is a good indication of whether the material is effective or not. Whilst the Faraday Defense 3mm performed the worst of the 7, 4 other materials let through at least one of the calls. Surprisingly, tin foil performed equally to the best Faraday Bag with no calls getting through to the device. The next communication technology tested is WiFi as this technology has potential communication distances of several hundreds of metres. The results for the WiFi tests are shown in figure 2.

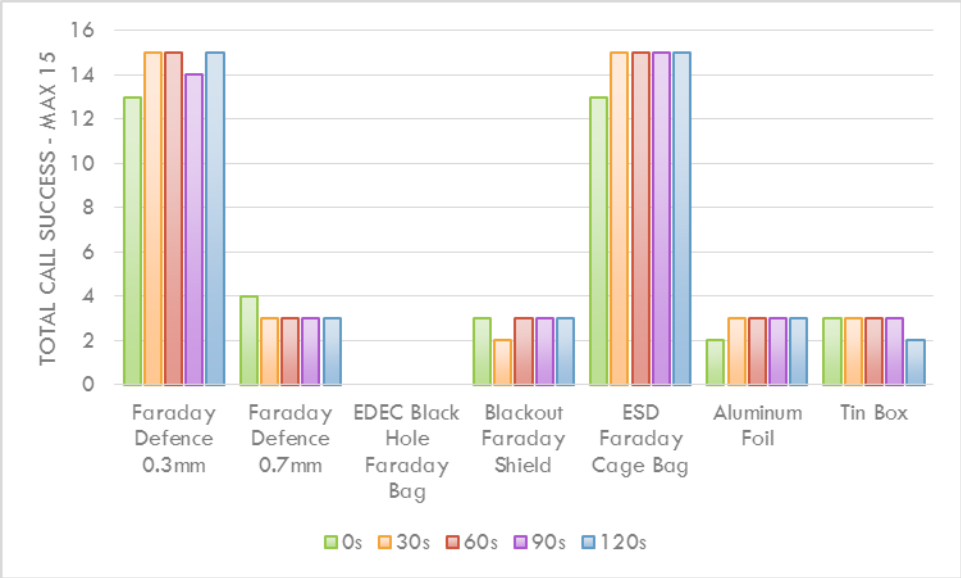

Figure 2. WiFi Call Failures

The 2.4GHz WiFi tests show that the most effective material is the EDEC Black Hole Faraday Bag with none of the communication attempts able to penetrate the bag. The other materials let through at least 2 of the attempts at communication with aluminium foil allowing as many attempts as several of the other scenarios. The final communication technology tested is Bluetooth and the results for this experiment are shown in figure 3.

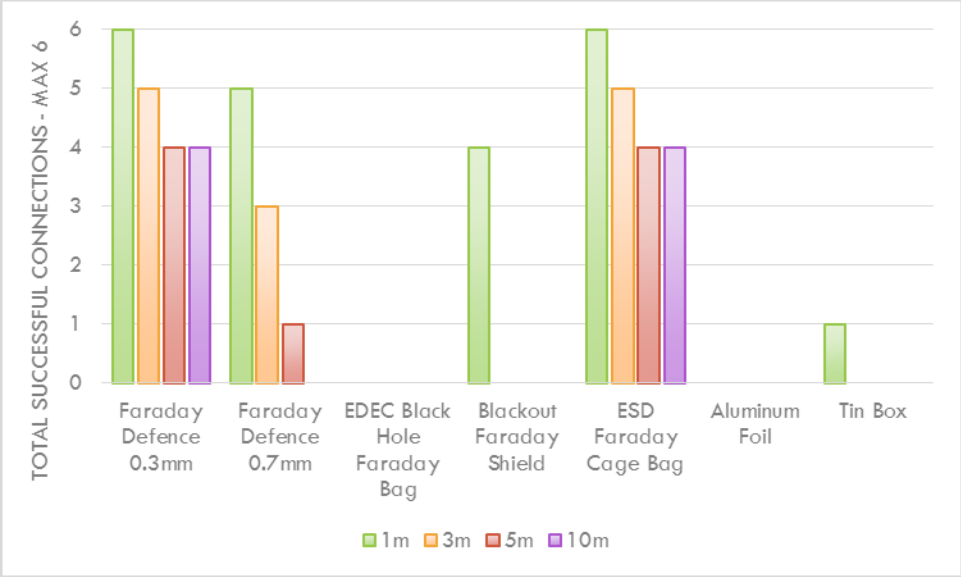

Figure 3. Bluetooth Call Failures

For the Bluetooth tests, the distance between the devices has a noticeable impact on the effectiveness of the materials and this can be expected with the very limited range of Bluetooth. The following tables 2 – 6 show the results for the various phone models with the 5 Faraday bags. Ticks indicate that the signal has penetrated the bag where a cross indicates a successful shielding of the signal.

Table 2: 3G / 4G and WiFi results for Faraday Defence 0.3mm

	3G/4G						Wi-Fi				
	0s	30s	60s	90s	120s		0s	30s	60s	90s	120s
Samsung Galaxy S3	✔	✔	✔	✔	✔		x	✔	✔	✔	✔
Samsung Galaxy S5	✔	✔	✔	✔	✔		✔	✔	✔	✔	✔
Samsung Galaxy S7	✔	✔	✔	✔	✔		✔	✔	✔	✔	✔
Sony Xperia Z5	✔	✔	✔	✔	✔		x	✔	✔	✔	✔
Apple iPhone 5	✔	✔	✔	✔	✔		✔	✔	✔	✔	✔
Basic Phone	✔	✔	✔	✔	✔		**n/a**	**n/a**	**n/a**	**n/a**	**n/a**

Table 3: 3G / 4G and WiFi results for Faraday Defence 0.7mm

	3G/4G						Wi-Fi				
	0s	30s	60s	90s	120s		0s	30s	60s	90s	120s
Samsung Galaxy S3	x	x	x	x	x		✔	✔	✔	✔	✔
Samsung Galaxy S5	✔	x	x	x	x		✔	✔	✔	✔	✔
Samsung Galaxy S7	x	x	x	x	x		✔	✔	✔	✔	✔
Sony Xperia Z5	x	x	x	x	x		x	x	x	x	x
Apple iPhone 5	✔	x	x	✔	✔		✔	x	x	x	x
Basic Phone	x	x	✔	x	x		**n/a**	**n/a**	**n/a**	**n/a**	**n/a**

Table 4: 3G / 4G and WiFi results for EDEC Faraday Bag

	3G/4G						Wi-Fi				
	0s	30s	60s	90s	120s		0s	30s	60s	90s	120s
Samsung Galaxy S3	x	x	x	x	x		x	x	x	x	x
Samsung Galaxy S5	x	x	x	x	x		x	x	x	x	x
Samsung Galaxy S7	x	x	x	x	x		x	x	x	x	x
Sony Xperia Z5	x	x	x	x	x		x	x	x	x	x
Apple iPhone 5	x	x	x	x	x		x	x	x	x	x
Basic Phone	x	x	x	x	x		**n/a**	**n/a**	**n/a**	**n/a**	**n/a**

Table 5: 3G / 4G and WiFi results for Faraday Cage ESD Bag

	3G/4G						Wi-Fi				
	0s	30s	60s	90s	120s		0s	30s	60s	90s	120s
Samsung Galaxy S3	✔	✔	✔	✔	✔		✔	✔	✔	✔	✔
Samsung Galaxy S5	✔	✔	✔	✔	✔		✔	✔	✔	✔	✔
Samsung Galaxy S7	x	x	x	x	x		✔	✔	✔	✔	✔
Sony Xperia Z5	x	x	x	x	x		x	✔	✔	✔	✔
Apple iPhone 5	✔	✔	✔	✔	✔		✔	✔	✔	✔	✔
Basic Phone	✔	✔	✔	✔	✔		n/a	n/a	n/a	n/a	n/a

Table 6: 3G / 4G and WiFi results for Blackout Faraday Shield

	3G/4G						Wi-Fi				
	0s	30s	60s	90s	120s		0s	30s	60s	90s	120s
Samsung Galaxy S3	✔	✔	✔	✔	✔		✔	✔	✔	✔	✔
Samsung Galaxy S5	x	x	x	x	x		x	x	x	x	x
Samsung Galaxy S7	x	x	x	x	x		✔	✔	✔	✔	✔
Sony Xperia Z5	x	x	x	x	x		✔	x	✔	✔	✔
Apple iPhone 5	✔	✔	x	x	✔		x	x	x	x	x
Basic Phone	✔	✔	✔	✔	✔		n/a	n/a	n/a	n/a	n/a

Of particular interest in these results is that whilst only the EDEC Faraday bag is successful in all experiments, other bags have varied success depending on the mobile phone make and model, which different models from the same manufacturer providing different results. Tables 7 and 8 show the results for the aluminium foil and tin can as a shielding material.

Table 7: 3G / 4G and WiFi results for Aluminium Foil

	3G/4G						Wi-Fi				
	0s	30s	60s	90s	120s		0s	30s	60s	90s	120s
Samsung Galaxy S3	x	x	x	x	x		x	x	x	x	x
Samsung Galaxy S5	x	x	x	x	x		x	✔	✔	✔	✔
Samsung Galaxy S7	x	x	x	x	x		x	x	x	x	x
Sony Xperia Z5	x	x	x	x	x		✔	✔	✔	✔	✔
Apple iPhone 5	x	x	x	x	x		✔	✔	✔	✔	✔
Basic Phone	x	x	x	x	x		n/a	n/a	n/a	n/a	n/a

Table 8: 3G / 4G and WiFi results for Tin Box

	3G/4G						Wi-Fi				
	0s	30s	60s	90s	120s		0s	30s	60s	90s	120s
Samsung Galaxy S3	x	x	x	x	x		x	x	x	x	x
Samsung Galaxy S5	x	x	x	x	x		✔	✔	✔	✔	✔
Samsung Galaxy S7	x	x	x	x	x		✔	✔	✔	✔	✔
Sony Xperia Z5	x	x	x	x	x		x	x	x	x	x
Apple iPhone 5	x	x	x	x	x		x	x	x	x	x
Basic Phone	✔	✔	✔	✔	✔		n/a	n/a	n/a	n/a	n/a

Table 7 indicates that aluminium foil can be utilised for 3G / 4G signal shielding and is successful at shielding the Sony Xperia Z5 and Iphone 5 from WiFi signals. In contrast, the tin box will prevent signal penetration of 3G / 4G for the basic phone which is not equipped with WiFi and will shield against WiFi for the Samsung Galaxy S5 and S7 only. These results clearly show that no one rule for shielding material can be applied in all circumstances with all phones or all technologies.

CONCLUSION

The use of Faraday bags, and in exceptional circumstances other materials to prevent unwanted radio communications with seized wireless devices is an accepted and vital addition to the forensic investigators toolkit. Forensic evidence is only of evidentiary value if it is maintained in the state that it was seized in without modification or alteration. The ready availability of Faraday bags at little cost would seem to allow investigators

to cheaply equip themselves with Faraday bags in readiness for a mobile phone seizure. However, the results of this research show that only one of the 5 tested bags consistently provided reliable protection from radio waves penetrating the bag. This same bag provided radio wave blocking for all 3 tested communication technologies and surprisingly aluminium foil was as reliable in all but blocking of WiFi signals. The other bags, even when nested inside each other to provide greater protection failed to completely block the radio signals with selections of phones but that only testing of the phones and materials provided a guide as to their effectiveness. It is not sufficient to estimate the effectiveness based on how they perform with some phones and extrapoloate the results to incorporate untested phones. The forensic investigator should be aware that not all bags are of equal reliability and the choice of which bag to utilise from which manufacturer should be made after reviewing rigorous testing procedures such as these to ascertain their effectiveness. Additionally, should a reliable bag not be available, aluminium foil will serve as an emergency measure provided the WiFi on the device is disabled by the investigator.

REFERENCES

Androulidakis, I. I. (2016). *Mobile phone security and forensics : A practical approach* (2 ed.). Retrieved from http://AUT.eblib.com.au/patron/FullRecord.aspx?p=4455173

Barrett, J. T. (n.d.). *Why does aluminium foil block cell phone signals?* Retrieved from http://techin.oureverydaylife.com/aluminium-foil-block-cell-phone-signals-2475.html

Bennett, D. (2012). The challenges facing computer forensics investigators in obtaining information from mobile devices for use in criminal investigations. *Information Security Journal: A Global Perspective, 21*(3), 159-168. doi:10.1080/19393555.2011.654317

Doherty, E. P. (2016). *Digital forensics for handheld devices* (1 ed.). Retrieved from http://AUT.eblib.com.au/patron/FullRecord.aspx?p=981555

FireEye. (2015). *Out of pocket: A comprehensive mobile threat assessment of 7 million iOS and Android apps*. Retrieved from https://www2.fireeye.com/MobileThreatAssessment.html

Gershowitz, A. M. (2013). Seizing a cell phone incident to arrest: Data extraction devices, Faraday bags, or aluminium foil as a solution to the warrantless cell phone search problem [article]. *The William and Mary Bill of Rights Journal, 22*(2), 601-612.

Khan, J., Abbas, H., & Al-Muhtadi, J. (2015). Survey on Mobile User's Data Privacy Threats and Defense Mechanisms [Article]. *Procedia Computer Science, 56*, 376-383. doi:10.1016/j.procs.2015.07.223

Ophoff, J., & Robinson, M. (2014). *Exploring end-user smartphone security awareness within a South African context.* presented at the meeting of the 2014 Information Security for South Africa, doi:10.1109/ISSA.2014.6950500

Rajendran, S., & Gopalan, N. P. (2016). Mobile Forensic Investigation (MFI) life cycle process for digital data discovery (DDD). *Proceedings of the International Conference on Soft Computing Systems (ICSCS) 2015, 2*, 393-403. doi:10.1007/978-81-322-2674-1_37

Science Buddies. (2011). *Block radio waves*. Retrieved from http://www.scientificamerican.com/article/bring-science-home-block-radio-waves/

Soukup, P. A. (2015). Smartphones. *Communication Research Trends, 34*(4), 3-39.