Results of Field Testing Mobile Phone Shielding Devices

Eric Katz, Richard Mislan, Marcus Rogers, and Anthony Smith

Center for Education and Research Information Assurance and Security (CERIAS)
and Purdue Cyber Forensics
Purdue University, West Lafayette IN 47907-2086, USA
ekatz@purdue.edu

Abstract. This paper is based on thesis research from the authors. Mobile phones are increasingly a source of evidence in criminal investigations. The evidence on a phone is volatile and can easily be overwritten or deleted. There are many devices that claim to radio isolate a phone in order to preserve evidence. There has been little published research on how well these devices work in the field despite the escalating importance of mobile phone forensics. The purpose of this study was to identify situations where the devices used to protect evidence on mobile phones can fail. These devices were tested using mobile phones from three of the largest services providers in the U.S. Calls were made to contact the isolated phones using voice, SMS, and MMS at varying distances from the provider's towers. In the majority of the test cases the phones were not isolated from their networks.

Keywords: Mobile phones, forensics, shielding, radio isolation, thesis.

1 Introduction

Mobile phones have penetrated our society like few other technologies have. These phones are storing ever-increasing amounts of information about their owners. It is no surprise that mobile phones are now commonly seized as a source of evidence during an investigation. Unfortunately the evidence on a phone is volatile and can easily be overwritten or deleted. Vendors claim that their products can radio isolate a phone in order to preserve the evidence stored on it. Regrettably this may not always be true.

There can be an incredible amount of information stored on a mobile phone. When a crime is committed evidence may often be found on a phone if an investigator can find it. This evidence can take many forms such as call histories, contact lists, text messages, and multimedia. There are also several ways of deleting this data even if the phone has already been seized. Incoming calls and data packets can overwrite stored information and there are even some packets that can cause a phone to delete some or all information stored on it.

To protect evidence on a mobile phone it must be isolated from its network. As long as the signal is attenuated enough, communication will be prevented and the evidence preserved. One of the he most common methods of attenuating radio signal is to use a device that will shield the phone from radio waves [1]. These devices

P. Gladyshev and M.K. Rogers (Eds.): ICDF2C 2011, LNICST 88, pp. 47–61, 2012.

function like a Faraday cage but do not truly block all radio signals. Some signal can still penetrate the shield providing a chance for the shielding device to fail.

The purpose of this research was to test multiple shielding devices in order to points of failure where the phone is not isolated. This testing is necessary because if the devices can fail to protect evidence it needs to be known before being relied upon during an investigation. Phones from three of the largest providers in the United States were tested at varying distances from cellular towers. The results will show where different shields can potentially fail. Proof that the shielding device can fail is the first step to fixing the problem.

1.1 Problem Statement

Wireless preservation devices do not always successfully prevent network communication to a mobile phone as the vendors promised. The purpose of these devices is to protect evidence on a mobile phone from being deleted or changed. When the shields fail, it can mean that valuable evidence can be lost. According to Emil De Toffol, president of LessEMF, there are three reasons why shielding may fail. They are [2]:

- The material doesn't provide enough attenuation
- Leaks or seams in the shield allow signal through
- The conductive shield is too close to the phone and acts like an antenna

This research tested several of the shielding devices that are currently available to investigators for use with mobile phones. These experiments were used to determine if the distance from a tower, the type of information being transmitted, and the network being used effect the isolation capabilities of the shielding devices. If the shielding device can fail then it must be known under what circumstances this can happen.

1.2 Significance of the Problem

Within the past 10 years mobile phone use has skyrocketed. From 2005 to 2009, the number of wireless subscribers has jumped from 194.4 million to 276.6 million [3]. In 2006, nearly a billion mobile phones were sold worldwide and the number continues to rise [4]. Mobile phones are so common that in the United States roughly 89% of the population has at least one of them [3]. Mobile phones store more data about their users than ever before and addressing mobile phones as a source of evidence is becoming increasingly important.

Depending on the type of mobile phone, there is a potential wealth of information stored on a mobile phone that can be evidence once a crime has been committed. Information that is most commonly gathered from mobile phones include; the contact list, call history, and text messages. These three items are stored on almost every mobile phone and provide valuable information about the phone's user. Given the personal nature of this information, its no wonder that acquisition of the evidence can lead and investigator to the next suspect or victim [5]. Other items of interest include the Location Information (LOCI), Global Positioning System (GPS) data, pictures,

videos, Internet browser history, and a myriad of application and personal data [6]. All of this potential evidence needs to be protected when a phone is seized so that it can be properly analyzed later.

The National Institute for Standards and Technology (NIST) published guidelines for how a mobile phone investigation should be conducted. NIST recommends that phones be isolated from the radio network to keep new traffic from overwriting existing data [7]. Interpol and the Association of Chief Police Officers (ACPO) also recommend radio frequency isolation to protect evidence on a mobile phone as part of their first principle of seizing digital evidence [8].

With all the potential evidence available on mobile phones it is no surprise how much importance is placed on isolating mobile phones in order to preserve the evidence found on them. However, all the proper intentions and efforts are for naught if the devices being relied upon have unknown failures that might allow the evidence to be changed. It is for this reason that the tools must be tested and validated.

2 Methodology

"Validation and testing is the responsibility of the customer [9]". It is a simple statement that needs to be followed and is what this experiment was about. Before going into the field and potentially risking evidence, a tool should be properly and thoroughly tested. If there is a chance that a tool will fail, an investigator must know when, where, and how it happens in order to stand up to the rigors of court. This section describes the mobile phones that were used and the preservation tools tested. It also lays out the method by which the research was conducted and how the results were recorded.

2.1 Limitations

There are several limitations that must be dealt with when conducting this experiment. There are many devices available that can be used as shielding devices. Some of these devices are more common than others and some are cost prohibitive. Only a few of the shielding devices manufactured today will be examined in this research. These will be chosen based on availability and cost.

There are also many phones with different antennas and capabilities. It is possible that the form factors of the phone itself and of the shielding tool will effect how well the shield can isolate the mobile phone. Form factor such as: candy bar, clamshell, antenna design, and touch screen interface can all alter how well a particular shielding tool will work. The more phones examined the more a particular design difference can be found. The number and type of mobile phones to be examined will be limited by cost and availability. This is due to availability and cost of phones. When possible the same phone models will be used for different carriers. This will show if various signaling or provider differences impact the shielding tool's effectiveness.

There are also too many different forms of information that can be stored on a mobile phone to try them all in one study. For this experiment the information that

was examined are incoming phone calls, text messages, and multimedia messages. These are especially important because if the phone receives more calls while it's supposed to be protected inside a shielding tool the call history may be deleted or worse, a remote wipe could be activated.

2.2 Devices Used

There are many models of phones, too numerous to test them all. There are also too many shielding devices available to do an exhaustive and comprehensive study on them. Any device that is not commercially available specifically as a wireless preservation tool will be excluded in this study. Availability, cost, and scale were the main factors that prevented any specific device from being used.

Every phone has a different antenna configuration and strength. The more phones that are tested for each NSP the more comprehensive the test results. The phones used during this experiment were limited to what is available in the Purdue Cyber Forensics lab. This impacts the studies ability to generalize the shielding devices' performance across all phones. Using more models and form factors will create a more comprehensive study. Similar model phones were used from multiple providers to see if difference in GSM and CDMA networks affected the shielding device's performance. Due to the cost of acquiring phones T-Mobile was excluded from this experiment. The phones used in this study were:

Table 1. Phones Used During the Experiments

Network	Mobile Phone
AT&T	Apple iPhone 3Gs
	BlackBerry Curve 9300
	Palm Pixi Plus
Sprint	BlackBerry Curve 8330
	HTC Hero 2
	Motorola Clutch i465
	Palm Pixi
	Samsung Galaxy S
Verizon	Casio G'Zone Ravine
	HTC Droid Eris
	HTC Imagio
	HTC Droid 2

These shielding devices were chosen because they are commercially available tools marketed specifically for isolating mobile phones. Most of them were designed for use by law enforcement as a forensic device to protect evidence on mobile phones. These devices are also some of the most commonly used ones by law enforcement agencies and made testing them all the more important. The shielding devices used are:

- eDEC Black Hole Bag
- LessEMF High Performance Silver Mesh Fabric
- MWT Materials' Wireless Isolation Bag

- Paraben Stronghold Bag
- Ramsey STE3600 - Chest
- Ramsey STP1100 - Bag

2.3 Method

Three towers were located, one for AT&T, Sprint, and Verizon. The towers were outside of major city limits in order to keep away from any alternative sources of signal the phones can use such as a signal repeater. Where possible, towers near highways were chosen because it was believed they would have the highest power output.

A voice, MMS, and SMS call was placed to each phone before being placed in a shield to insure that all the needed features worked. This was done at every distance repeated at every distance in order to establish a baseline and confirm that the phone still received the calls at that location. The ringer volume for the mobile phones was turned to maximum. This alerted the researcher as to which call penetrated the shield because many of the shields do not allow any other interaction with the phone.

At the base of each tower a phone from the appropriate company was then placed in each shielding device. The shielded phone was then called with another mobile phone. It was then noted if the shielded phone received the call. Next SMS and MMS messages were also sent to the shielded phone. The results of each test were recorded.

This experiment was repeated with each phone from a distance of 100, 150, 200, and 500 feet from the towers. These distances follow the same distances used in Dankner and Gupta's research in 2007 and provided an opportunity to see how much distance altered performance of the shields. A Bushnell Yardage Pro Sport 450 laser range finder was used to determine the proper distances. It is often impossible to tell how far one is from a tower or signal regenerator. Testing from multiple distances better simulates possible conditions that an officer in the field might encounter while transporting a mobile phone back to a forensics lab.

The goal was to find out at what distances, if any, the shielding instruments failed to successfully isolate the mobile phone. Results are P for passed representing blocked calls and F for failure representing calls where the shield was penetrated. If for some reason a test couldn't be performed or measured the result was N/A. In this research the N/A results were caused when a phone did not have a data plan that permitted MMS calls.

When a mobile phone detects that it has lost signal to the network it increases power to its antennae in an attempt to reestablish the connection. To make sure that each of the tested shields could handle the increased power output each phone was called at 15-second intervals after being placed into a shielding device. The intervals were chosen because they provided an even distribution over one minute and would provide clues as to how time effected isolation. After each test call the phone was allowed to reestablish its connection and then shielded once more. If the phone is not isolated after 1 minute the shielding device was considered faulty at the current distance.

2.4 Hypothesis

The main hypothesis of this research is that the shielding devices do not fully protect a mobile phone once it is placed inside the shield. The most likely place for these devices to fail, if they will, is when they are close to the NSP towers. Due to the nature of radio waves, the signals to and from the mobile phones are stronger at this point and better attenuation is needed to isolate the phone. This means that not only do the devices have to attenuate the radio signal but that the level of attenuation must actually be capable of isolating the phone. If the attenuation capabilities of the tools are appropriate then there should be no failures.

The second hypothesis is that communications that don't require a high SNR value are more likely to penetrate the shielding devices. SMS requires the least signal quality and will therefore be more likely to penetrate the shield. MMS will be the next most likely to bypass the shields as voice call require a constant and steady connection.

The third hypothesis is that the shielding devices will perform better the farther they are from the tower. This is a corralary of the first hypothesis. Signal strength decreases with distance and makes the attenuation provided by the shield more likely to successfully isolate the mobile phone from its network.

3 Results

This was a pilot experiment to determine if mobile phone shielding devices could fail to protect evidence on a mobile phone. Each shielding device was tested at multiple distances with multiple phones. For each distance there were 360 tests for SMS and Voice calls and 300 tests for MMS. MMS had fewer possible tests because the iPhone 3Gs and the HTC Imagio that were tested did not have data plans that allowed for MMS messages. The overall rate of failure for all of the shields was 53.08%. Figure 1 shows the overall results of all the tests across all of the shields. That means over half of all the test cases resulted in the shields not isolating the phone.

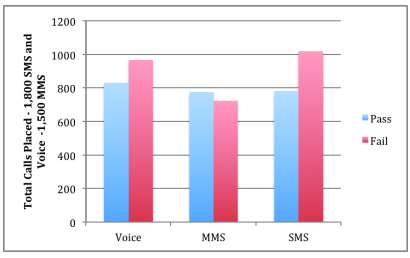

Fig. 1. Total Pass Fail Rates

The hypothesis that SMS messages were the most likely to penetrate the shields held true. SMS messages were only blocked 778 out of the 1,800 tests that were run. This is a 56.78% failure rate for blocking SMS messages. Figure 1 shows the overall results of all the tests across all of the shields.

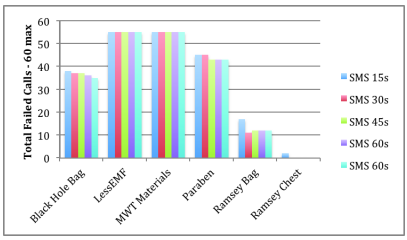

Fig. 2. Failed SMS Tests

Voice calls were the next most likely call type to penetrate the all of the shields. In total the shields failed to block 968 calls out of 1,800 or 53.78%. Any one of these calls will change the call history resulting in the potential loss of evidence.

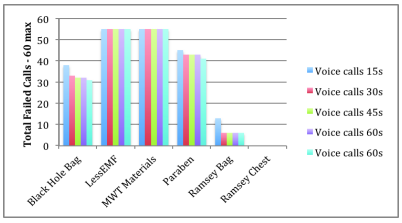

Fig. 3. Failed Voice Tests

MMS messages were the most commonly blocked call type, only penetrating the shields in 721 out of 1,500 tests or 48.07%. Figure 4.3 shows how the shields worked with MMS messages. A nearly 50% failure in even the best-blocked call type proves that the shielding devices cannot handle the increased power output of towers and mobile phones.

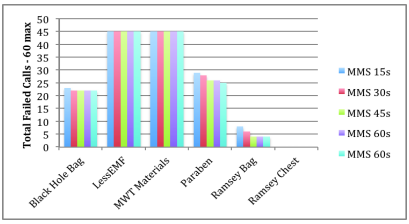

Fig. 4. Failed MMS Tests

3.1 Statistics

A MANOVA analysis was used to explore the results of the tests for statistical significance. The MANOVA used a 2x15 matrix. The independent variables were the 6 different shields and the 5 distances. The dependent variables were the calls measured in pass/fail. A post-hoc Scheffe test was also run in order to determine the

significant differences in the shields performance. A standard .05 alpha was used to set the level of significance.

In this study the results showed that the interaction between shields and distance was not significant. This means that the combined effect of the different shields and being farther distances away from the towers didn't explain the variations in the results. Looking at the main effects of distance overall, it was not significant with a Wilks-Lambda F-value of 1.026 and a p-value of .425. Breaking each distance down by the time of the calls, only two times was distance significant. This was with SMS mesages at 0s and 15s. At 0s the p-value was .022 and at 15s the p-value was .025. MMS messages at 0s were marginally significant with a p-value of .052. This supports the first hypothesis, that the shields blocked calls closer to the tower less often. It is likely that the distances did not increase far enough from the towers for there to be a statistical difference. Future studies could confirm if farther distances from the towers affect the performance of the shielding device.

Each of the different shields was statistically significant having a range of Wilks-Lambda F-values from 5.886 – 7.462 and their p-values all being .000. This means the different shields explained most of the variance in the results of this study. To find out which shields behaved differently than others a post-hoc Scheffe test was run. Table 2 is an example of how most of the homogeneous subsets were grouped. For most of the calls, the subsets were divided into 3 groups. The Ramsey shields were usually in the 1st subset together as the most effective. The eDec Black Hole Bag and Paraben StrongHold bag comprised the next subset. Finally the 3rd subset contained the LessEMF Mesh and MWT Materials' bag as well as the StrongHold bag again. This shows that the Stronghold bag's performance was marginal in its effectiveness. It performed better than the LessEMF and MWT shields but not as well as the Black Hole Bag. During the MMS tests the StrongHold Bag performed well enough that it was solidly grouped in the 2nd subset and not the 3rd.

Table 2. Standard Homogeneous Subset Table

Shield	N	1	2	3
STE3600	50	X		
STP1100	50	X		
BHB	50		X	
StrongHold	50		X	X
LessEMF	50			X
MWT	50			X

This is not the only grouping that was determined to exist. There are several instances where there were 4 homogeneous subsets, represented in table 3. In these instances the Ramsey STE3600 was always in the first subset, as it was the most effective at isolating the mobile phones from their networks. The Ramsey STP3600 was the next subset. The 3rd subset was comprised of the Black Hold Bag and the StrongHold bag. The 4th subset contained the StrongHold bag again as well as the LessEMF Mesh and MWT Materials bag.

Table 3. Homogeneous Subsets for Voice Calls at 0 seconds

Shield	N	1	2	3	4
STE3600	50	0			
STP1100	50		0.26		
BHB	50			0.6	
StrongHold	50			0.7	0.7
LessEMF	50				0.9
MWT	50				0.9

This shows not only did the shields performed differently, but which phones behaved most alike. The closer the value came to 0 the more effective the shield is at isolating a phone. The only shield that ever had 0.00 as its value was the Ramsey STE3600 chest. Unfortunately, there were a few tests that it did fail so it was not 100% effective in isolating the tested mobile phones from their networks. It is the most forensically sound of all the shields tested for this study. These tables provide a quick reference guide that can be used when deciding which shield will suit the needs and expectations of the user.

4 Conclusions

Many of the tested shielding devices are marketed as forensics tools, which implies that they should be forensically sound and accomplish their intended task. The vendors of these products state that they are 99.99% effective at blocking up to 90dB or that they can effectively block that many dB for signals between 3 and 30MHz. All of this is to increase marketability by implying that once a mobile phone is enclosed in their shielding device it will be isolated.

This study did not confirm or even test vendor claims on the dB that their products blocked. It did test the real world effectiveness of the RF shields. The purpose of this research was to find out if RF shielding devices would fail and what distance from a tower they fail at. Attempts were made to isolate as many variables as possible in order to eliminate extraneous factors that could influence the experiments results. This research isolated distance from a tower and time as factors on the effectiveness of RF shields.

It is evident that the shields do not always isolate the mobile phones. None of the RF shields tested were able to successfully isolate the phones 100% of the time. At the very least the call history on the phones will have been changed by the incoming calls. Worst case, any one of these failures could also potentially represent the complete loss of all evidence contained on the mobile phone due to a remote wipe command. Evidence on mobile phones can be too important to investigations to allow it to be contaminated or erased by not being properly protected. This is why there are recommendations from scientific and law enforcement communities, such as Interpol, NIST, and SWGDE, dictating that mobile phones should be isolated when they are

seized. The following subsections discuss the research results and their implications as well as what should be done in future testing of these and similar devices.

4.1 Legal Implications

Law enforcement officers know that mobile phones can contain valuable evidence. This is causing phones to be seized more often. As law enforcement departments establish policies detailing how mobile phones should be treated, it is likely they will follow the guidelines established by organizations such as INTERPOL and SWGDE. Standard operating procedure will be to isolate mobile phones after taking them as evidence. RF isolation shields such as the ones tested will become the equipment used to accomplish this. Unfortunately, the shields that were tested in this study couldn't isolate the mobile phones with absolute certainty. Law enforcement relying upon them to protect evidence may experience problems in the future because of this.

No matter where a phone is seized, it will have to come back to the police station to be examined and stored. If the phone is not near a tower when it is seized there is a decent chance it will pass near one on the way back to the station. For example, the Sprint tower used in this experiment is located next to I-65. The 500' test range that was used in this experiment easily crosses both lanes of the highway. Figure 5 shows the tower as a green marker and the red marker is positioned 500 feet away. Any Sprint phone being transported along this road would attempt to connect to this tower even if only for a few seconds. Those seconds of activity are all that are needed for a remote wipe command to be sent to the phone and have all the evidence on it zero out.

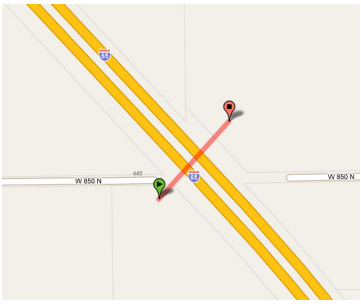

Fig. 5. Sprint Tower Outside of West Lafayette, IN

In a city, such as West Lafayette, towers are located to provide optimum coverage for the network service provider's customers. The urban environment can make it difficult for an officer to know where they are in relation to a tower. In Figure 6 an AT&T tower is located near Purdue University's main campus and is represented by a green marker. Within a 500' range are several important roads, shopping centers, a parking garage, library, and a church.

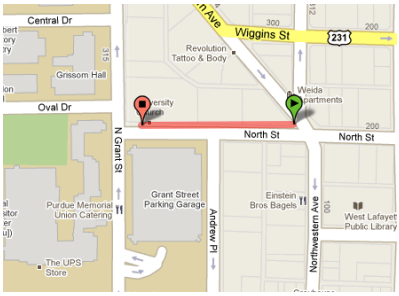

Fig. 6. AT&T Tower Located Near Purdue University in West Lafayette, IN

These are high traffic areas where the seizure of a cell phone incident to an arrest would not be uncommon. Just as with towers used for this research, mobile phones will attempt to maintain their connection to this tower. Without testing the shields with this tower it can't be said for certain if they are capable of isolating phones connected to this tower. Based on the results of this research though, the closer the phone is to the tower the less likely it will work. This goes to show how close people can be to a network tower and not even realize it. The denser the city population, the more towers will be present to allow the NSP to reuse bandwidth allowing them to have more subscribers. Future testing should cover more distance from the tower and measure the signal strength so more generalities can be made about the performance of the shields.

The results of this study show that there can be reason to suspect the integrity of any evidence taken from a shielded mobile phone. If this change occurs after the phone has been seized, there is a chance that any evidence later found on the phone can be called into question. The term "fruit of the poisoned tree" means that no matter how condemning evidence might be; once it is contaminated it is no longer reliable. This applies to evidence mobile phones as well as any other form of evidence. That is part of the reason protecting evidence on phones is so important. There are enough difficulties acquiring evidence from a mobile phone without having to worry if the evidence will change while the phone is in storage.

Defense attorneys could use this information to their advantage. As attorneys become more acquainted with evidence on mobile phones they will look for more ways to have it dismissed. It is not unreasonable to believe that an attorney could have evidence from an improperly protected phone dismissed from court entirely. Even if that evidence is not dismissed, there is now the problem of explaining to a jury why evidence has potentially changed. The results of this pilot study prove that more testing needs to be done and that shielding devices need to be improved in order truly protect evidence on mobile phones so it can be presented in court.

4.2 Scientific Implications

This was a pilot study into the field effectiveness of mobile phone shielding devices. It proved that the tested mobile phone shielding devices could potentially fail to isolate phones when used in a field environment. Knowing the rate of failure of these

devices is one of the criteria that are required to pass a Daubert examination. The American Academy of Science recently berated the entire forensic science community for not following scientific procedure and a lack of failure rates is one of the problems they addressed. More research needs to be done to determine the exact point and frequency of these failures, but this study is a good start. One of the major contributions of this study besides the results is the methodology that was used to conduct it. Determining what, where, and how to test the devices was a major part of this research. This methodology will be very useful for developing future studies and methods for investigating the effectiveness of mobile phone shielding devices.

The first thing that had to be determined was exactly what was to be tested. For this research MMS, SMS, and voice calls were determined to be the most important items to test. This is because they can quickly alter some of the most commonly used and important items of forensic evidence found on a mobile phone. Due to the threat these calls represent, the ability of the shields to isolate phones from these calls is of the utmost importance. The binary pass-fail tests conducted during this research were appropriate for the functionality the shields are meant to provide. When preserving evidence in a forensically sound manner, there is no room for partial protection. Evidence is either preserved or it isn't and that can make or break a trial. For scientists analyzing shielding devices, pass-fail tests conducting over a set time intervals and distances provides detailed knowledge of what is occurring without over complicating the information being collected. This is also a means to determine the expected rate of failure of these devices.

There are other means to transmit data to and from a mobile phone besides these calls. 3G and 4G capabilities were intentionally left out of this research, as it was a pilot study. Future research should include these features when possible. A simple test would be to start streaming a video to the phone and then seeing how long it takes a shield to interrupt this stream. Another test that would be appropriate to include in future studies is sending the remote wipe commands to phones that can utilize them. This test would examine how well these signals can penetrate shields and if they behave more like SMS or MMS messages. Other signals that could also be tested in future studies include GPS and Bluetooth. As mobile phones integrate with more technology it becomes important to make sure that they are isolated not only from their towers but also from anything else that they could potentially connect to.

The next problem addressed when developing this methodology was where should these tests be conducted. One goal of this test was to find out if the shields could in fact fail to isolate a phone and how far from a tower do they need to be to work. For this reason the towers chosen were outside of city limits. These towers have less population per square mile and broadcast at a higher wattage in order to provide coverage to larger areas (Stallings, 2005). One advantage of conducting these tests outside of city limits is that there was a clear line of sight to the tower. That meant factors such as alternative networks and multipath propagation were reduced and less likely to interfere with the results of the study allowing the strongest signal possible to reach the phones.

Tests were originally to be done at the base of the tower, 50', 100', 150', 200', and 500' from the towers. The reason for the 50' increments was to examine how much distance was necessary to provide different results. The 500' distance was set to determine if the longer distance would have a more significant effect. As this was a

pilot study there were no prior test results to use to determine what the best distances would be. One of the difficulties presented when testing began was that the towers had safety enclosures that pushed testing back 30' to 50' away. This is the reason the 50' testing point was removed from the methodology.

There was often little difference in the results when increasing the distance at 50-foot intervals. Future research would benefit by conducting the same experiments but setting the distance intervals to 100-foot distances and testing back to 1,000 feet or more from the tower. This will provide a better sense of how distance affects the shields performance. It will also more accurately demonstrate how shields can be expected to behave as phones are transported from one location.

More precise tests could be run using equipment that can read the output wattage of the towers. This would allow for exact signal strength to be recorded instead of distance. Eliminating distance in favor of wattage would not only be more accurate but also would allow for testing inside city conditions and not require the experiment to be done in isolated environments. Measuring signal strength's biggest advantage is that once a shield is tested against a known signal strength a generalized formula can be determined to predict the shields failure rate at any given distance and time. This would be tremendously useful to digital forensic science. It would provide known rates of failure for equipment used in evidence gathering. It would also allow law enforcement departments to defend the integrity of evidence collected in their jurisdictions when cases come to trial. The current results of this test provide a rate of failure for the shields but the power output of the towers is unknown. This makes determining a correct formula unfeasible at this point but does demonstrate that it can be done.

Using signal strength would also allow for a direct strength comparison to determine if there is a difference in CDMA or GSM networks. From the data collected during this research it would appear that Sprint has the weakest signal strength of all the NSPs. This could be true, but it could also be that the power output of the tower is lower than that of the AT&T and Verizon towers that were also tested. Sprint and Verizon are both CDMA networks but had drastically different responses. If the power of the signal from the tower was accounted for it is probable that this difference could be explained. At the time of this research equipment of this nature was unavailable.

Mobile phones automatically increase their power output when they lose connection to their network. To guarantee that the shields can continue to isolate the phone despite this ramped up power, time was a tested factor for this research. The results of this study show that over the course of a minute a phone was more likely to be isolated. Unknown factors in this test are how long does it take for a mobile phone to start increasing its power output and how long before it reaches maximum power. It is possible that one minute was not a long enough time interval to fully test this. Future research should include a longer time interval or find other means to determine the amount of time needed to test a fully powered phone antenna.

Another unknown factor in this study is the receiver sensitivity and transmitter output of each of the phones that was tested. This data is not located in the user manuals for phones nor is it published on the vendor websites. The reason this is important is that it is possible that the phones used in the study have higher output and receive capabilities than the average phone currently available. This would cause the

shields to appear to have a higher failure rate than an average phone would generate. Finding or determining these values would also help in creating an exact formula for determining the rate of failure for RF shielding devices.

The methodology designed for this research accomplished its goals and successfully tested the hypotheses. Future research will benefit greatly from following this model of testing. Repeating this study will allow for more generalizations to be made about the effectiveness of shielding devices to protect evidence on mobile phones. Improvements can be made to this methodology and are suggested. With the right equipment and time it should be possible to determine a formula to predict each shields performance based on distance from the tower and strength of the signal.

4.3 Improving Shields Devices

A side benefit to this study is that highlights the fact that shielding devices need to be improved. In the past few years touch screen phones have become more popular. The nature of materials used to make the shielding device causes them to be conductive. Most of the shields that were tested in this research are made from some form of copper, nickel, and silver mesh. When put into direct contact with touch screen phones the shields would often activate buttons at random. This resulted in all sorts of activity on the phones and in a couple of cases caused the phones to dial out. This is just as problematic as the shield not isolating the phone. Now the device being used to protect evidence is altering it, and altering it in an uncontrolled unspecified manner. This too will allow attorneys to question the integrity of any evidence found on a phone.

The Black Hole Bag was the only shield tested that was designed with a clear window to allow the user to interact with the phone while it is enclosed, but it too would activate buttons without user interaction. Placing a non-conductive material between the walls of the shields may prevent accidental button activation in future shielding devices. For the Black Hole Bag or any shield intending to allow user interaction, placing a bumper between the phone and the shield will allow users to manipulate the phone while preventing accidental activations. Future tests should include using foam rubber, bubble wrap, or similar non-conductive material insert to hold the phone away from the shield walls. This will prevent the shield from accidently activating buttons on touch screen phones. It may also increase performance of the shields as there is a chance the walls of the shield can become an antennae they make direct contact with the phone's antennae.

The STP1100 was the best performing of the bag style shields used in this study. This is because it used two separate layers to make each of its walls. This allowed it to act more like a true Faraday cage. The inner layer wrapped the signal being sent out by the phones around the inside of the shield. The outer layer spread the signal from the tower across the outside of the shield. Any signal that penetrated past the first layer still had waveguide beyond cutoff point of the second layer to pass through as well. As long as the holes in the two layers are not perfectly aligned this will make it more difficult for a radio wave to penetrate the shield. Some of the phones were still able to penetrate the STP1100 despite the advantages of its design. This may be because the two layers of the shield are in direct connection with each other. If possible, a double walled shield should be designed and tested with a nonconductive

padding placed between the walls to see if it improves the performance of the shield. It is also likely the shield's walls are too thin to completely isolate the phones. This would mean that performance could be improved by increasing the depth of the wall.

4.4 Closing Remarks

As the number of mobile phones taken into custody increases, more standard operating procedures will be developed dictating that phones be isolated to protect and preserve the evidence found on them. RF isolation shields, such as the ones tested, will likely be what are used to protect evidence on a mobile phone. There are limitations to this technology and improvements are needed. It is important for anyone using these shielding devices to know what can happen and not blindly rely upon them. As things currently stand, the shields that were tested cannot be guaranteed to block all signals coming to or from the mobile phones. These experiments were intentionally conducted near high power towers where nothing could interfere with the signal. The likelihood of having a high power tower near where a phone is being seized is unknown, but it is quite possible. Future tests following an improved version of this methodology should be able to develop a formula that can accurately predict any tested shield's rate of failure. This will allow for users to determine what they can expect from their products and hopefully prevent complications from arising in court. Vendors can use this study to find where improvements to their product can be made. Though this was a pilot study, it proves that RF shielding devices need to be verified before relying on them to preserve evidence. The results of this article are condensed from the thesis work of the authors. For more detailed information contact the authors or download the thesis from https://www.cerias.purdue.edu/apps/reports_and_papers/view/4562.

References

1. Scientific Working Group on Digital Evidence.: Best Practices for Mobile Phone Examinations (2009), http://www.swgde.org/documents/swgde2009/Best%20Practices%20for%20Mobile%20Phone%20Examinations%20v1.0.pdf
2. De Toffol, E.: Re: Wireless preservation (2009)
3. CTIA.: Wireless Quick Facts. CTIA The Wireless Association (2009), http://www.ctia.org/media/industry_info/index.cfm/AID/10323
4. Jansen, W., Delaitre, A., Moenner, L.: Overcomming Impediments to Cell Phone Forensics (2008)
5. Mislan, R., Casey, E., Kessler, G.: The growing need for on-scene triage of mobile devices. Digital Investigation 6(3-4), 112–124 (2010)
6. Lesemann, D., Mahalik, H.: Dialing Up and Drilling Down: Forensic Preservation of Handheld Devices. Information Security Systems Association Journal (2008)
7. Jansen, W., Ayers, R.: Guidelines on Cell Phone Forensics (2007)
8. Interpol European Working Party on IT Crime.: Good Practice Guide for Mobile Phone Seizure and Examination (2006)
9. BKForensics. Solutions (2010), http://www.bkforensics.com/Mesh.html