available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/diin

Digital Investigation

The growing need for on-scene triage of mobile devices

Richard P. Mislan [a,*], *Eoghan Casey* [b], *Gary C. Kessler* [c]

[a] *Purdue University, College of Technology, Department of Computer and Information Technology, Center for Education Research Information Assurance and Security, 401 N Grant Avenue, West Lafayette, IN 47907-2021, USA*

[b] *Johns Hopkins University Information Security Institute, USA*

[c] *Gary Kessler Associates, School of Computer and Information Science, Edith Cowan University, Australia*

ARTICLE INFO

Article history:
Received 9 February 2010
Received in revised form
3 March 2010
Accepted 8 March 2010

Keywords:
Mobile device forensics
Cell phone forensics
On-scene triage inspection
Mobile device technician

ABSTRACT

The increasing number of mobile devices being submitted to Digital Forensic Laboratories (DFLs) is creating a backlog that can hinder investigations and negatively impact public safety and the criminal justice system. In a military context, delays in extracting intelligence from mobile devices can negatively impact troop and civilian safety as well as the overall mission. To address this problem, there is a need for more effective on-scene triage methods and tools to provide investigators with information in a timely manner, and to reduce the number of devices that are submitted to DFLs for analysis. Existing tools that are promoted for on-scene triage actually attempt to fulfill the needs of both on-scene triage and in-lab forensic examination in a single solution. On-scene triage has unique requirements because it is a precursor to and distinct from the forensic examination process, and may be performed by mobile device technicians rather than forensic analysts. This paper formalizes the on-scene triage process, placing it firmly in the overall forensic handling process and providing guidelines for standardization of on-scene triage. In addition, this paper outlines basic requirements for automated triage tools.

1. Introduction

As the prevalence and functionality of mobile devices increase, they are becoming more common as sources of intelligence and evidence in a wide range of investigations. Mobile devices such as cell phones and smart phones have been instrumental in solving homicides, are used by terrorists for reconnaissance and coordination, can be used to smuggle contraband across borders, and are frequently found in prisons despite being prohibited. It is no wonder that mobile devices are now nearly ubiquitous at crime scenes, given that there are 10 times more mobile devices being produced in the world today than babies being born (Rose, 2009). In the U.S. alone, 245 million out of the total 307 million citizens have a data-capable mobile device, and 40 million of those are smart phones or wireless-enabled personal digital assistants (PDAs) (CTIA, 2009). Given the personal nature of information on mobile devices like contacts, call history, and text messages, immediately acquired evidence can lead an investigator to the next suspect or victim. At the same time, an investigator may see private communications that at any prior point in our history would have been considered beyond the reach of any warrant or investigation.

Mobile devices present several challenges from a forensic perspective. Mobile devices are fundamentally networked devices, creating a dynamic operating environment that can be difficult for digital investigators to isolate and preserve. Furthermore, in order to extract information, it is necessary to interact with the device, often altering the system's state (Punja & Mislan, 2008). Fortunately, with the proper approach and documentation, it is possible to obtain usable digital evidence from mobile devices in a forensically sound manner

* *Corresponding author.*
E-mail address: rmislan@purdue.edu (R.P. Mislan).
1742-2876/$ – see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.diin.2010.03.001

(Casey, 2007). It is generally acceptable for properly trained personnel to access original data on a mobile device provided the implications of all actions can be explained (ACPO, 2008).

Given the dynamic and rapidly evolving nature of mobile device forensics, it is sometimes necessary to acquire data the moment it is observed and available. For instance, certain information may be lost or overwritten when a mobile device loses power or is moved to a different location. Some systems support remote wiping, enabling someone to send a command over the network that will obliterate data stored on the mobile device. Whether mobile devices are a source of intelligence or evidence in investigations or military operations, there is a need for better methods of extracting usable information in a timely manner. In some situations, such as military operations or bomb threats, there is neither the time nor resources to isolate the device from the network prior to extracting information. Furthermore, any delays could allow timed security locks to activate or provide a window for remote wiping. Effective on-scene triage processes and tools may preserve evidence that would otherwise be lost, and can make the difference between life and death in certain situations.

Unfortunately, there are limited methods and tools for performing effective on-scene triage inspections, and it is common practice to bring most mobile devices back to digital forensic laboratories (DFLs) for processing. Although some cases require in-lab processing, certain investigations are better served by immediate information. Despite their best efforts to keep up with this glut of personal cellular technologies, many DFLs have substantial backlogs (Casey et al., 2009; Parsonage, 2009). In addition to possibly missing the opportunity to preserve time-sensitive data associated with mobile devices, such delays in processing evidence will inevitably slow down the criminal justice system, giving offenders time to commit additional crimes and causing immeasurable damage to falsely accused individuals.

There have been some stopgap measures to address this growing problem. Some DFLs are providing less technical investigators with dedicated mobile forensic kiosks containing data synchronization software and digital camera rigs to streamline the processing of mobile devices. Another approach is to repackage commercial off-the-shelf mobile forensic equipment in a hardened briefcase for field use by less technical digital investigators. These mobile forensic field kits are being used by some groups, including military units and vice squads, to perform their own on-scene examination. However, these approaches do not provide sufficient standardization or automation to make it effective for use on-scene by less technical digital investigators. Furthermore, these stopgap solutions shift the responsibility of forensic analysis onto digital investigators who are not qualified in mobile device forensics. Effective extraction and interpretation of digital evidence from mobile devices using currently available methods and tools requires training which can be costly and is generally unsuitable for the vast majority of investigators.

There is clearly a need for more standardized and automated solutions in on-scene triage inspections that can be performed by less technical digital investigators, referred to as mobile device technicians in this paper. To paint a clearer picture of what the ideal on-scene triage inspection process would entail, consider a kidnapping case in which the victim's mobile device is found at the crime scene. A mobile device technician with basic training in mobile device triage would arrive at the scene, and would follow a simple protocol to preserve evidence on the device detect the type of mobile device. This protocol would include the use of an automated tool to extract readily accessible data from the mobile device and display it in a way that the technician could easily understand. This information could contain recent calls or text messages that the mobile device technician conveys to the primary investigators, and possibly help them identify and locate the victim and offender. If the primary investigators on the case believe that a mobile device contains additional evidence that was not obtained by the triage inspection, they can send the device to the DFL for further analysis. As such, on-scene triage inspections are distinct from, and potentially a precursor to, forensic analysis in DFLs. When technical questions arise in relation to mobile devices or expert testimony is required, this is beyond the training of a mobile device technician and generally calls for an experienced and properly educated forensic analyst.

When many mobile devices are found at a crime scene, the triage inspection process involves targeted on-scene review of all available media to obtain immediate intelligence and to determine which items contain the most useful evidence and require additional processing at a DFL. The triage inspection process presented in this paper extends existing process models for conducting digital investigations, and is part of a three-tiered strategy for performing forensic examinations that enables DFLs to produce useful results in a timely manner primary at different phases of an investigation (Casey et al., 2009). The aim of this paper is to clearly define the on-scene triage inspection process, and to differentiate it from forensic analysis techniques more suitable to a laboratory environment. This triage-driven, tiered approach has the added benefit of reducing unnecessary expenditure of resources on less serious matters. Another aim of this paper is to formalize and standardize the on-scene inspection process, moving practitioners away from ad hoc on-scene inspections of mobile devices. Such formalization and standardization will increase the consistency of results and reduce the risk of missed information.

This paper begins by discussing the current approaches that DFLs are employing in an effort to deal with the large number of mobile devices being seized in digital investigations. The role of on-scene triage is discussed along with the requirements for supporting tools. The importance of training is emphasized throughout this paper, whether mobile devices are being handled by mobile device technicians on-scene or forensic analysts in a laboratory. A methodical approach to performing on-scene triage is presented, followed by a discussion of what types of forensic processing are unsuitable to the triage process. Finally, the economic, legal and ethical implications of on-scene triage inspections are covered.

2. Background

The information found on mobile devices can provide contextual clues about who the owners knew, who they

communicated with, and what they found worth saving or sharing. The address book and the call history (calls dialed, missed and received) provide investigators with information about the phone owner's cohorts. The text messages found on a mobile device can reveal personal communications that the phone's owner never expected others to see. Finally, the images and videos saved on a mobile device show what was important to the phone's owner. In their entirety, these evidential points of mobile device data help construct a digital sketch of a suspect or victim that can lead the investigator to their next interview or incident. In short, triage inspection of a mobile device produces intelligence that can lead to a complete and correct analysis.

Mobile device forensics is developing rapidly, not only to keep pace with new technologies but also to extract more data from flash memory (van der Knijff, 2009). Following the well-established and tested procedures of computer forensics, DFLs can preserve, acquire, and analyze data on certain mobile devices in a manner similar to computers. This model directly relates to computer forensics in that it attempts to image the entire mobile device through a variety of tools. However, full memory dumps are only supported for certain device models, and most current acquisition tools for mobile devices only acquire active data because they rely on AT, Binary Runtime Environment for Wireless (BREW), or Object Exchange (OBEX) commands that simply request information from various memory stores located in the mobile device (Delaitre and Jansen, 2008; Jansen and Ayers, 2006).

Currently, many DFLs follow the same rigorous procedures for every mobile device, regardless of the circumstances of the case. Some DFLs employ triage but standards of practice are lacking in this area, and available tools do not adequately support this process. In addition, given the variety of mobile devices, it is often necessary to utilize multiple mobile device applications to access different parts of the mobile device, which can be very time-consuming. Although this time-consuming approach may be warranted in certain cases, it is ineffective when specific information is needed from the device quickly and is unsuitable for on-scene triage inspections.

Digital investigators are often required to respond quickly to a crisis, and decide how much attention to devote to a particular case or item of evidence. When making such decisions, it is necessary to consider non-forensic aspects of an investigation, including the seriousness of offense, case circumstances and types of evidence sought, and relevance of other digital evidence (Casey et al., 2009). On-scene triage inspections may provide to the data necessary for investigators subsequently:

(1) assess the severity of a crime and prioritizing it accordingly;
(2) assess the offender's possible danger to society (Rogers et al., 2006);
(3) obtain actionable intelligence in exigent circumstances (e.g., missing person, military operations, risk of evidence destruction);
(4) identify the richest sources of digital evidence pertaining to an investigation;
(5) identify victims that are or may be at acute risk;
(6) identify potential charges related to the current situation; and
(7) determine whether a certain item requires deeper inspection, such as recovery of deleted information or decoding of encrypted data.

Although information obtained from on-scene triage inspections may resolve certain questions in a case, it is more often just the starting point in an investigation.

There have been several stopgap solutions to expedite the forensic acquisition of sensitive evidence from mobile devices.

2.1. *Thumb/scroll through*

In the past, the Thumb/Scroll Through approach has been performed on-scene by a detective or arresting officer. This approach is used in the DFL to validate tool results or when no automated forensic tool works. This initial approach dates back to the use of pagers and is still in use today. This model is exactly what it sounds like in that it has non-technical personnel thumbing through the mobile devices looking for any numbers, messages, or files (images, videos, etc.) of importance. Usually the investigator is looking for information such as a known contact or a recently made or received call or text message, or even an image or video of something relevant to the current case. When investigators use this approach on-scene, it is generally because they do not have access to an automated tool to extract the data. The primary shortcomings of this approach from a forensic perspective are the lack of consistency and the potential for inadvertently altering or obliterating useful evidence. Unless the individual performing the operation follows documented and consistent procedures that specify the actions to be performed and documentation to be created, it will not be clear how the resulting data were obtained and what impact the operation may have had on the evidential device. Therefore, this approach is not well-suited to the on-scene triage process, and it is generally recommended that Scroll Through examinations be performed by trained individuals, following standard operating procedures and using proper recording equipment.

2.2. *Federal kiosk*

Recently, due to the backlog in processing evidence from mobile devices, some DFLs have created dedicated kiosks in an attempt to help less technical digital investigators perform their own forensic acquisition and analysis of data on mobile devices. These kiosks are simply a combination of several data synchronization tools with a digital camera. Although this is a commendable attempt to help from local and state law enforcement officers obtain information mobile devices in a timely manner, the law enforcement officer still has to drive to the location of the kiosk. If the evidence is not isolated and preserved evidence may be lost when the mobile device receives calls, messages, or destructive wipe commands during transportation. Furthermore, specialized training is needed to make effective use of the tools on these kiosks. In essence, these kiosks shift the responsibility of forensic analysis onto less technical personnel who are generally not

qualified to use these tools properly, and to evaluate the accuracy and completeness of their results. Finally, there is no guarantee that the tools at these kiosks will be able to extract the desired information from a given mobile device, resulting in a wasted trip for busy law enforcement officer.

2.3. *Lab in a kit*

The latest push from forensic tool vendors has seen numerous versions of a laptop computer placed inside a hardened case adorned with anywhere from 20 to 100 cables, power chargers, and other accoutrements. The laptops have the latest version of the forensic tool software loaded on them ready for the next forensic acquisition of data from a mobile device. The loaded software is the exact same as their lab version of software and, in some cases, these hardened case kits are sold as being perfect for use in DFLs. There are several problems with pushing these hardened case kits. First of all, they are heavy and expensive. Second, the software is not designed specifically with on-scene triage in mind, and the data acquisition process is generally slow. Thirdly, and probably most importantly, the software is not designed for mobile device technician, and is more like a tool for the forensic analyst back in the laboratory. Furthermore, there is no increase in acquisition speed, which for many investigations is essential.

All of the above methods generally assume that the evidential mobile device has been isolated from the network to prevent alteration and remote wiping. If data can be acquired immediately on-scene, it may be unnecessary to spend resources and time on equipment or procedures for blocking network connectivity. There is the added risk that delays will activate a security lock on an evidential device that could prevent investigators from obtaining any data on the device and so it may be better if data can be acquired immediately on-scene while a device is unlocked.

A more methodical and immediate approach that mobile device technicians can use for on-scene acquisition of information from mobile devices is needed to address the limitations of the above stopgap measures. The approach proposed in this paper involves the rapid, targeted review of readily accessible items to provide digital investigators with the most useful information in the least amount of time. The items of greatest importance from a triage standpoint generally include contacts, call history, multimedia, and communications such as SMS, MMS and e-mail.

Whether information is being extracted from mobile devices on-scene or in a DFL, the importance of training cannot be overstated since all forensic work is predicated upon the trustworthiness and competence of individuals performing the work. As such, any mobile device technician performing on-scene triage inspections should be properly trained and should be able to explain their actions.

3. Triage of mobile devices

An on-scene triage inspection is the first of three levels of forensic examination: (1) survey/triage forensic inspections, (2) preliminary forensic examination, and (3) in-depth forensic examination (Casey et al., 2009). The triage inspection process involves the rapid review of potential sources of digital evidence for specific information, with the goal of quickly obtaining the most relevant evidence. By reviewing the specifics of contacts, call history, text messages, images and videos, a mobile device technician at the scene can provide the primary investigators with information to help them make informed decisions as to where to take their investigation. The on-scene triage process is also useful for processing a large number of devices in a timely manner to find those with the most relevant information. As such, triage inspections have a role in large-scale digital investigations, including security breaches within an organization and electronic discovery in civil cases.

An added benefit of the triage process is that it can mitigate the risk of privacy violations resulting from a digital investigation. When dealing with mobile devices as a source of evidence, there may be a concern that text messages, images, and videos are private, and that there needs to be a limit on what can and cannot be viewed. Triage inspections can be designed to acquire a limited set of data from mobile devices such as images, and can arrange to limit access to other forms of data. This is particularly important in light of recent decisions such as U.S. vs. CDT setting some controls for forensic examinations of digital evidence.

When performing on-scene triage inspections, there is a risk that important information will not be accessible. For instance, on-scene triage techniques and tools are generally limited to logical data, and cannot recover deleted items. In addition, looking for artifacts of criminal activities commonly found in past cases may overlook evidence relating to more serious crimes such as murder or the production of child pornography, or the use of new technologies to facilitate criminal activity. Therefore, to be effective and mitigate the risk of relevant evidence being overlooked, there is a need for guidelines and continuously updated tools to enable mobile device technicians to perform effective on-scene triage inspections. In addition, mobile device technicians must be trained to assess the results of an on-scene triage inspection, and decide whether the device needs to be brought to a DFL for in-depth forensic analysis.

3.1. *Pre-processing decisions*

Mobile device technicians at the scene can make certain immediate decisions about a mobile device as a potential source of evidence, even before employing any forensic methods or tools. These decisions include whether the device most likely contains the information being sought, whether an on-scene triage inspection will be fruitful, and whether the mobile device should be brought to a DFL for processing.

From the outset of an investigation, witness statements or case background may suggest that pertinent information is stored on particular devices. For instance, a witness might report that relevant evidence is stored on the device, or the nature of the crime might suggest that a mobile device was involved (Parsonage, 2009).

When assessing the potential importance of a particular mobile device as a source of evidence and considering the most effective approach for handling a particular mobile

device, it is useful to consider devices in three general categories based on their capabilities and properties.

Type 1: Basic phone – less data, more volatility (e.g., call logs, Short Message Service (SMS) messages).

Type 2: Camera phone – moderate data, moderate volatility (e.g., images/videos).

Type 3: Smart phone – more data, less volatility (e.g., e-mail, documents, Web browsing history).

The list above is not meant to suggest that Type 3 devices, for example, do not contain the same volatile information as a Type 1 device, but that the preponderance of what will be found on a Type 3 device is less volatile than a Type 1 device. With this in mind, since Type 1 devices are the most volatile, it is often desirable to extract information from them immediately, making these obvious candidates for on-scene triage inspection. Type 2 and 3 devices may preserve more stored data indefinitely but, in some cases, it may still be desirable to extract some information immediately on-scene.

Because Type 1 devices cannot generate images and other multimedia, they might be excluded as a likely source of evidence in certain circumstances like production of child pornography or a border check looking for contraband. Therefore, investigators can be trained to identify devices that are more likely to contain the evidence they seek and how to extract this information quickly. It must be borne in mind that although a Type 1 device cannot take pictures, it might be able to receive MMS messages that contain photographs.

On-scene triage inspections may reveal that the desired or expected data are not present on the device. At this point, mobile device technicians, in conjunction with the primary digital investigators, must decide whether more advanced forensic techniques available at a DFL should be applied to the device. For instance, when deleted data are being sought, specialized tools and methods may be required and it may be necessary to bring the mobile device to a DFL where forensic analysts may be able to acquire and analyze a full memory dump from the device.

4. Triage inspection tools

Triage inspection of mobile devices generally involves a number of manual operations, including putting the device in standalone mode and disabling security features. However, the data acquisition and review processes are more conducive to automation. To maintain consistency and ensure that reliable results are obtained in a timely manner, it is preferable to have automated tools for performing triage inspections. This section outlines some basic requirements for triage inspection tools.

Existing tools that are currently promoted as mobile device forensics tools are well-suited to supporting triage inspection. For instance, Microsystemation's XRY, Athena from Radio Tactics, and Cellebrite UFED can be adapted to meet the above requirements for triage inspection. Athena and Cellebrite have a user-friendly interface, maintain audit logs to varying degrees, and have some ability to acquire only selected data from mobile devices. Athena has a touch screen and compact design, which is both user-friendly and highly desirable for on-scene triage. Unfortunately, all of these tools attempt to fulfill the needs of both on-scene triage and in-lab forensic examination in a single solution. On-scene triage has unique requirements because it is a precursor to and distinct from the forensic examination process, and may be performed by mobile device technicians rather than forensic analysts. The requirements for tools that support on-scene triage are listed here and discussed further below to help distinguish between triage inspection and forensic examination.

At a minimum, a mobile device forensics tool should meet the following requirements:

- have a user-friendly design that less technical digital investigators can utilize with some basic training;
- indication of what information can or cannot be acquired from a given mobile device;
- display a warning before taking any action that could lock or wipe the evidential device;
- change as little as possible on the evidential device and document any necessary changes;
- acquire data accurately – in particular, dates and content should accurately represent original;
- provide access controls to restrict viewing of results and prevent unauthorized access;
- present acquired data objects in a useable format;
- provide meaningful errors when a particular mobile device cannot be accessed, or certain data cannot be acquired from the device;
- maintain an audit trail or other record of applied processes; and
- store data in a form that can be accessed and reviewed at a later time.

In addition, although it is difficult to support all mobile devices fully, on-scene triage inspection tools should at least provide minimal information from the majority of devices specific to different regions. This specificity also pertains to exclusive cable packs for different regions (e.g., United States, Europe, Asia).

4.1. *Simplicity of use*

As a filter of information for on-scene mobile device technicians, the most important success factor for a triage inspection tool is simplicity. The tool should not interfere with the process, but instead should facilitate the gathering of intelligence. A compact design and touch screen make triage inspection tools more portable and manageable when performing actions on-scene. In addition, clear messages are critical during the data extraction process, particularly when errors occur, to help a mobile device technician deal with problems.

Another ongoing issue that increases the simplicity of use is the availability of drivers for various mobile devices, which enable the forensic tool to communicate with an evidential device. As a new mobile device is delivered to market, many times a new set of drivers is required for its connection. All mobile forensic products (hardware and software) fall victim to the necessity of adding drivers for each new device, regardless of the operating system upon which they operate. Known as the software update, this must be an instrumental

piece of any triage inspection tool. Ideally, this update occurs weekly and with limited user intervention to keep up with the release of new devices.

The data acquired by a triage tool should be presented correctly in native formats and provide information in a form that is usable on-scene by mobile device technicians. Text must be portrayed exactly as it is displayed on the mobile device. Date-time stamps must also be accurately converted given the proprietary nature of mobile device standards. Incorrect translation of date/time stamps, alphanumeric characters, or languages is a failure in accurate representation of forensic evidence. The triage inspection tool should not attempt to translate languages, only present it as provided.

4.2. *Audit trail*

From a forensic perspective, it is imperative that any triage inspection tool maintains an audit trail of all actions performed on the evidential device. This audit trail can be used to assess the forensic soundness of the process by documenting that the triage inspection tool obtained an accurate copy of acquire data while making little or no changes to the original data on the evidential mobile device.

The audit trail must include how the data were acquired, how it was converted, and what steps were taken to ensure it is complete and accurate. The audit documentation should also define any unusual steps that are taken to retrieve the data or convert it to a usable format. In addition, any triage inspection tool should calculate cryptographic hashes (e.g., MD5, SHA1) of the acquired data and record these values for future comparison, enabling forensic analysts to verify that evidence has not been altered since it was acquired.

4.3. *Access control*

To increase their utility and limit privacy concerns, on-scene triage inspection tools should support restricted viewing of results.

With mobile devices, the expectation of privacy can be complicated from a legal viewpoint (Bischoff, 2009; Gershowitz, 2008; Orso, 2009). Contacts and images are stored on a mobile device and usually not shared with anyone unless the contact is called, or the image is sent via e-mail or MMS. Once a call is made it becomes part of the phone's call history as it is shared with the network provider. SMS messages and the number to which they are being sent also fall under this sharing with the network provider. Some mobile subscribers even pay extra to backup their contacts through the network provider. Finally, their voicemail may also be stored on the network provider servers.

With the correct technology employed, the triage inspection tool could simply determine provide a "positive" or "negative" indication that certain types of data are contained in the device. For example, if the mobile device contains known child pornography, the triage inspection tool could simply report that such contraband is possibly present without displaying the images or videos.

5. Guidelines for triage inspections

Standard operating procedures for handling sources of digital evidence help provide solid evidence that can be relied on by decision makers, whether they are in a court room or board room. Any method for performing triage inspections must maintain the reliability, completeness, accuracy, and verifiability of mobile device evidence (Golden, 2006; Kenneally and Brown, 2005). To this end, the following steps are proposed as a standard minimum requirement for triage inspections of mobile devices:

(1) initiate chain of custody;
(2) isolate device from network (if feasible and applicable);
(3) disable security features (if feasible and applicable);
(4) extract limited data;
(5) review extracted data; and
(6) preview removable storage media;

Documentation is a critical component of every part of the triage inspection process, enabling others to validate the process and results. Therefore, it is important to record what was done to the device and what information was obtained. Each stage in the triage inspection process is discussed below.

5.1. *Chain of custody*

Documenting the chain of custody is an essential element in asserting the integrity of any evidence seized in an investigation, particularly one that ends up in court. The chain of custody documentation starts with an inventory describing:

- the devices that were seized;
- the date and time of seizure;
- the location where the devices were found; and
- the person responsible for initially seizing the devices.

The evidence custodian has the responsibility to maintain a log of every person who comes in contact with the individual evidentiary items. If a person checks out a device, the log should note:

- the person who is taking the device(s);
- the date and time when the device was checked out;
- the purpose for which the device was taken; and
- the date and time when the device was returned.

In addition, the log should contain the name and signature of the person relinquishing custody as well as the person accepting custody of the device(s). In this way, two people are involved in every transaction. If any obvious tampering is done to any of the devices, such tracking will help narrow down when such changes might have taken place.

This chain of custody mechanism is not foolproof because it is based upon trust – trust that the evidence custodian is honest and trust that the storage facility is secure.

Consider, as an example, a mobile device with a SIM card and microSD memory expansion card. Currently, few digital investigators have the knowledge and/or take the time to do a complete inventory of the device in the field; it is not until the forensic analysis that such an inventory performed. An unscrupulous individual might remove a memory card from a mobile device, and this act could go unnoticed if it occurred prior to an exam. For this reason, performing a thorough inventory of digital devices that, in fact, contain multiple forms of media is encouraged in the field.

Another custodial issue, as discussed in the next section of this paper, is that contents of digital devices might be altered even after the device has been secured and stored. In particular, the owner of a mobile device that has been seized legally could advise the service provider that the device was stolen; in some cases, the service provider will send a signal to wipe the mobile device of all personal content the next time that the device connects to the network. For this reason, whenever feasible and applicable, all precautions should be taken to ensure that the device remain isolated from the service provider's network.

Chain-of-custody documentation is crucial to maintaining evidentiary integrity. Without this documentation, there is no way to refute a claim that an unauthorized person accessed, and possibly tampered with, the evidence. While the existence of chain of custody records cannot prove absolutely that no one tampered with evidence, lack of such records can allow evidence to be challenged.

After on-scene triage inspection, all seized devices should be placed into a tamper-resistant (or tamper-proof) container so that any disturbance to the physical devices can be easily noted. If possible, photographs of the devices should be taken at the time and place of seizure.

5.2. *Block network connectivity*

While a mobile device is connected to a network, it can send and receive data that could alter valuable evidence on the device. In addition, certain smart phones can be wiped remotely, obliterating all user data on the device. Therefore, if feasible and applicable, it is generally recommended that evidential mobile devices be isolated from the networks to prevent communication with telecommunications, WiFi, and Bluetooth networks by putting the devices in standalone/airplane mode, in Faraday container, or using some other isolation mechanism (e.g., jammer). Fig. 1 shows a MyTouch (Android) device being put into standalone mode. Although holding down the power key will bring up a menu to put this device in airplane mode, depressing the same button will activate the security lock. Therefore, it is prudent to navigate to the settings options and explicitly enable airplane mode under wireless controls as shown in Fig. 1.

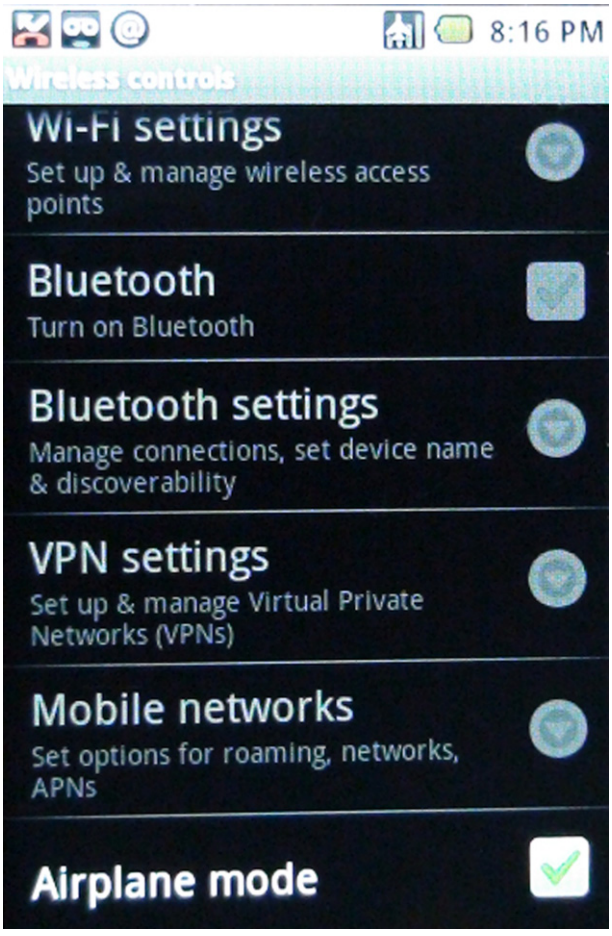

Fig. 1 – Android device being put in airplane mode to prevent it from communicating with networks.

Although it has become common practice to isolate the device from the network prior to performing any data extraction, this may be unnecessary or even counterproductive in certain circumstances. Some devices will be configured to lock automatically after some period of inactivity (e.g., 15 min), potentially preventing digital investigators from gaining access to data on the device. In exigent circumstances like military operations or missing persons cases, delays simply may not be tolerable because there may not be enough time to transport the mobile device to a DFL for processing.

5.3. *Disable security mechanisms*

To ensure that the device will be accessible to forensic analysts after it is turned off or loses power, it is advisable to disable all locking and encryption mechanisms on the device. If feasible and applicable, disable locking/security features: Remove password locking and encryption to prevent device from becoming inaccessible in the event of power loss or timed lockout. Fig. 2 shows the security features of a MyTouch (Android) device are enabled, as indicated by the check mark on the right. Touching each option on the device screen will uncheck (disable) the feature.

5.4. *Data extraction*

Generally the aim of an on-scene triage inspection is to obtain certain information quickly, and to convey the information to the primary investigators and help them determine whether it is of relevance to the investigation. This information usually includes device identifiers like IMEI and user-generated data like address book entries, call logs, SMS/MMS, photographs, and videos. Ideally, the process of extracting and displaying this information should be automated and easy to perform on-scene by mobile device technicians with basic training. Portable, user-friendly tools have been developed to facilitate on-scene triage inspections of mobile devices. Fig. 3 shows Athena from Radio Tactics being used to acquire data from a Blackberry device.

Although existing tools have vastly varying results in which devices are supported and what information is extracted, certain expectations for data extraction can be applied to any tool as demonstrated by the tools testing initiative at the U.S. National Institute of Standards and Testing (www.cftt.nist.gov).

As triage inspection tools mature, there is a need for more standardization in the mobile devices that are supported and the information that is extracted.

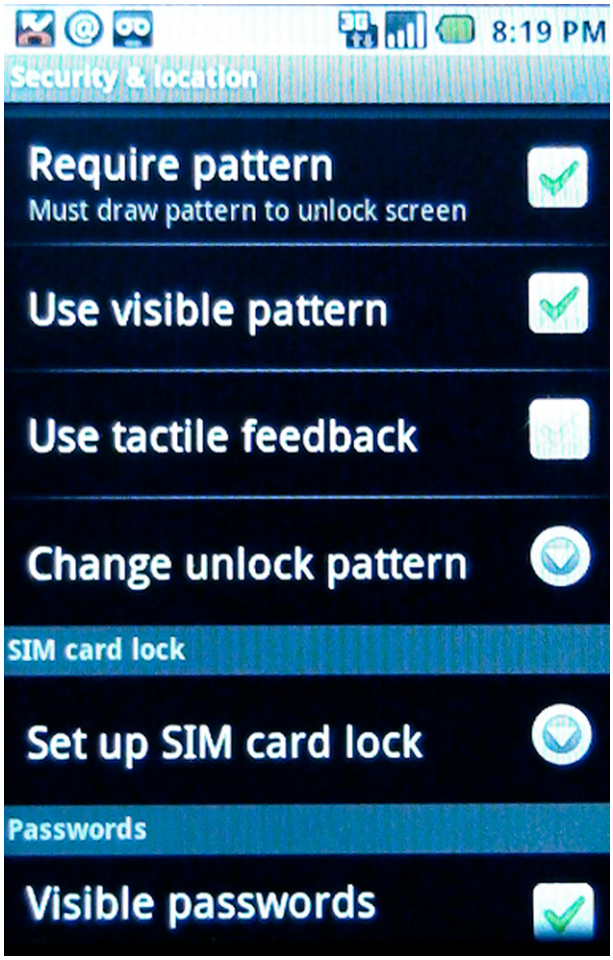

Fig. 2 – Screen lock configuration enabled on Android device.

Fig. 3 – Data being acquired from a Blackberry device using Athena from Radio Tactics.

5.5. *Data review*

When performing a triage inspection, after data has been extracted from a mobile device, the triage inspection tool should present data in a format that mobile device technician can review easily on-scene. Mobile devices can contain substantial amounts of data, particularly Type 3 devices, not all of which is of interest in an on-scene triage inspection context. Therefore, some data reduction or filtering may be desirable to focus on items or time periods of interest. For instance, Fig. 4 shows select information from SIM card being displayed in a summary fashion.

In addition, mobile devices store data in a variety of formats, some of which must be decoded into a human-readable format. Triage inspection tools must decode such data automatically present it in a form that is usable by mobile

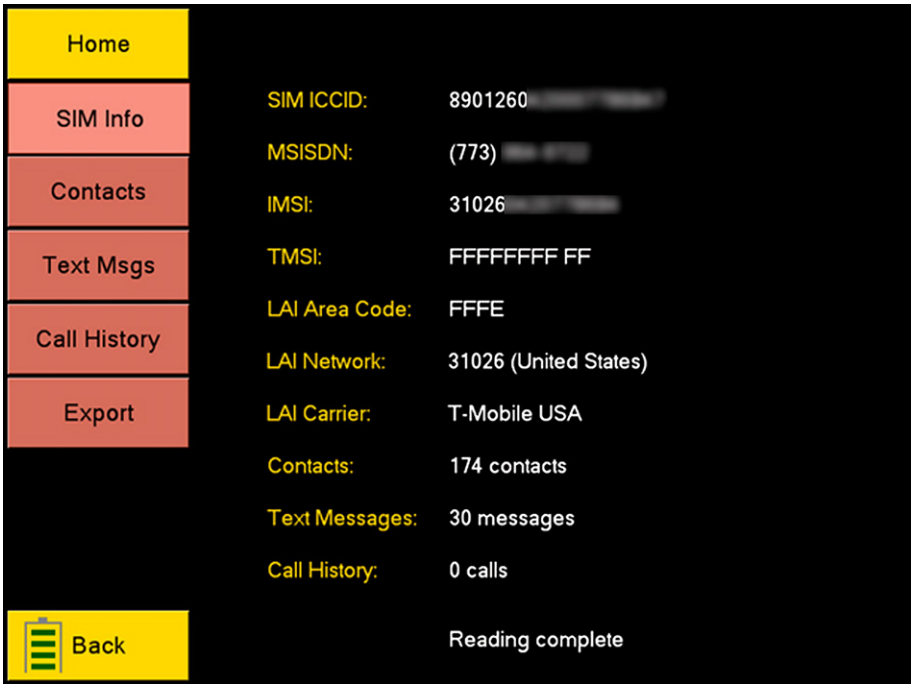

Fig. 4 – Summary of data on a SIM card.

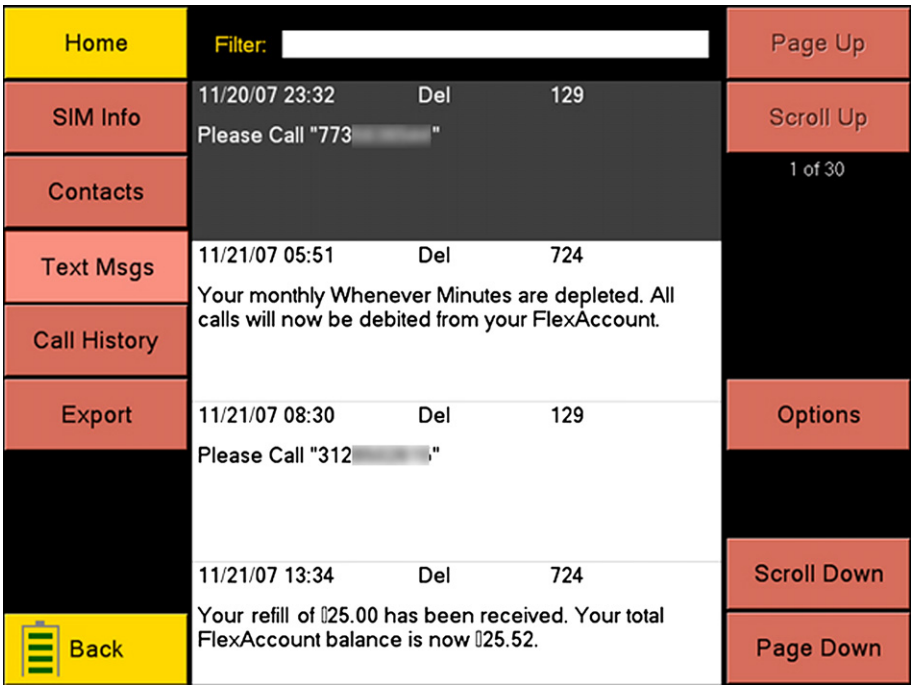

Fig. 5 – Example of simplified view of text messages as converted, formatted and displayed automatically by the tool for ease of review by mobile device technicians.

device technicians. For example, text messages and date-time stamps on SIM cards and many mobile devices are encoded. Fig. 5 shows deleted text messages extracted from a SIM card with dates and content that the tool automatically converted into a format that is easily readable by a mobile device technician.

The number of components in mobile devices combined with their varied identifiers and data formats make mobile device forensics a complicated process. Therefore, it is critical that mobile device technicians performing on-scene triage inspections are trained to understand data on mobile devices.

5.6. *Preview removable storage media*

Some mobile devices have removable storage media that may contain information of relevance to an investigation. The two most common approaches to extracting information from removable storage media in mobile devices are: (1) to remove the media card and create a forensic duplicate using a read only method, and (2) access the media card via the mobile device operating system. Circumstances will dictate which approach is more appropriate in a specific case.

From a forensic perspective, the primary advantages of the first approach are that the original is unaltered and all data is acquired, including deleted data. In addition, because most media cards are FAT formatted, they can be examined using file system forensics tools (e.g., TSK, EnCase, FTK, XWays). A limitation of this approach is that mobile device technicians may mistakenly remove a SIM card rather than removable media card, which may alter or destroy data on the device. The main advantage of the second approach is that it is generally faster and can be performed at the same time other information is being extracted from the mobile device. However, this approach only captures active data and may alter the original data, such as updating last accessed dates of files on the media card.

Mobile device technicians may decide that getting immediate results outweighs the risk of altering last accessed dates of files on removable storage media. It should be borne in mind that modern mobile devices can be configured to encrypt data on removable storage media. When a media card is encrypted, the most efficient way to extract data in unencrypted form is to access the media via the mobile device.

In the context of on-scene triage inspections, it may be necessary to view only file system metadata like names and date-time stamps. When this is the case, it can save time for mobile device technicians to preview just file system details rather than copying the entire contents of removable storage media. Fig. 6 shows a preview of a file system with metadata like names and date-time stamps.

6. Legal considerations

In the United States, there are several legal allowances for examining mobile devices when probable cause is present: consent, a search incident to arrest, exigent circumstances, and a search warrant.

6.1. *Consent*

A search conducted with consent is when an individual allows the on-scene investigator to review the mobile device upon request. The consent can be either written or spoken, and can be reversed by the individual at any time. Consent must be

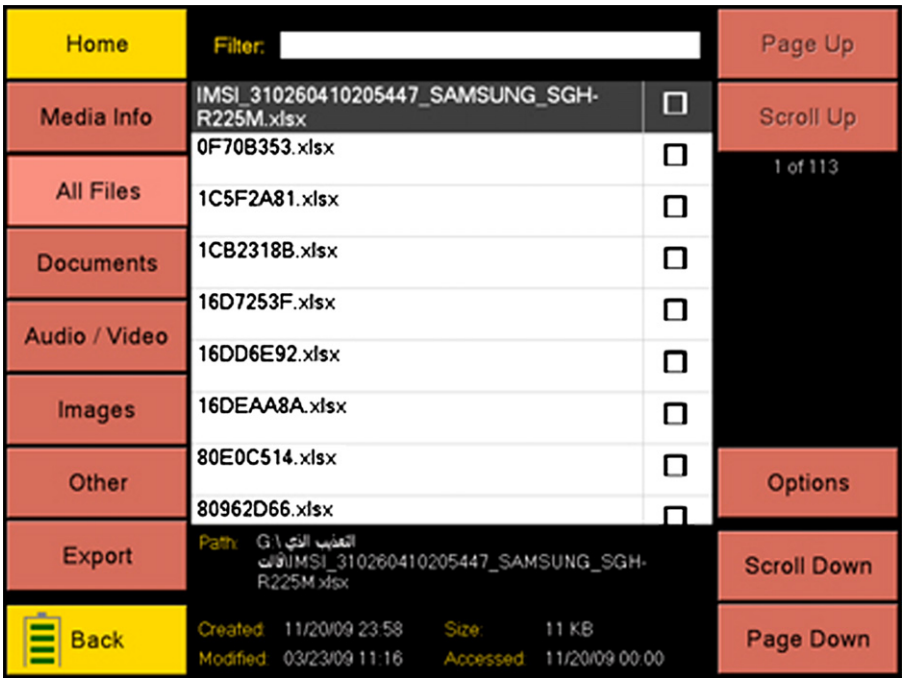

Fig. 6 – Example of a file system preview with metadata.

granted by an individual of appropriate authority such as the person who owns the phone; in the case of a minor, the parents may be the owners and might be able to provide consent.

6.2. *Search incident to arrest*

A search incident to arrest is one of the most questionable allowances for on-scene examination. Through many cases – including *U.S. v. Robinson*, *New York v. Belton*, *Thornton v. U.S.*, *U.S. v. Chan*, *U.S. v. Finley*, *U.S. v. Valdez*, *U.S. v. Curry*, *U.S. v. Lottie*, *U.S. v. Mercado-Nova*, *U.S. v. Zamora*, *U.S. v. Murphy*, *U.S. v. Diaz*, *U.S. v. Cote*, *U.S. v, Brookes*, and *U.S. v. Parada* – at present what is searchable on a mobile device is not as clear cut from a legal viewpoint (Gershowitz, 2008; Orso, 2009). With modern day mobile devices merging multiple technologies from the computer world – i.e., today's mobile devices are a combination of yesterday's PDA, telephone, and computer – we are starting to see the questions mounting as to what is considered private data and what is considered searchable data incident to an arrest. During an arrest, the rule of thumb is that a mobile device and its contents may be seized as long as the search is contemporaneous with the arrest (Gershowitz, 2008). Most recently, the issue has been further amended to include that the search must be related to the offense of arrest (Arizona v. Gant, 2009). Furthermore, the search may be limited to any device that is within the immediate access and control of the person arrested; e.g., a mobile device on the belt of the suspect would certainly fall into that individual's locus of control and be subject to a search incident to arrest although the phone in the next room would not be.

At least one recent court decision may provide a chilling effect to searching phones incident to arrest. Ohio v. Smith (2009) concluded that the search of a mobile device incident to arrest was unlawful because there was neither a risk to the safety of the officer or others, nor exigent circumstances. While a paper address book found on a person is subject to search incident to arrest, the *Smith* decision suggests that the phonebook on a mobile device is not subject to such a search.

6.3. *Exigent circumstances*

Exigent circumstances are loosely defined as those circumstances where a reasonable person could believe that there was an imminent danger of physical harm to a person (including a police officer), the destruction of evidence, the escape of a suspect, or some other circumstance that might prevent a law enforcement officer from lawfully executing their job (United States v. McConney, 1984). The key factors in determining an exigent circumstance for a mobile device is as important as what must be searched, and the application of exigency to the seizure and search of mobile devices is not without some controversy.

The prevention of the destruction of evidence can provide for lawful seizure of a mobile device and its contents. In illegal drug trafficking cases, multiple mobile devices can be an instrumentality of the offense and may be seized under the plain view exception to the requirement for a search warrant. The exigent circumstance holds that data stored on a mobile device can be destroyed by accident or by a deliberate act. In as much as the mobile device has a shelf life, if mishandled, its call history could be lost, SMS messages could be overwritten or wiped, and images could be deleted. Indeed, smart phones such as the iPhone, Blackberry, and Windows Mobile-based devices, as well as other devices could be the victims of a remote wipe when the owner reports them "stolen" to the network administrator or service

provider (thus the importance of isolating the phone from the network as soon as possible after a seizure).

It has been stated that the network service provider maintains information and records relating to mobile devices and their use. Call history and text messages are the two sources of information found at the carrier (Orso, 2009), however, the carrier does not normally maintain contacts, images, or videos and usually only stores SMS or MMS for a short period of time, if at all.

6.4. *Search warrant*

A mobile device may be lawfully searched under the auspices of a valid search warrant. Search warrant issues that affect mobile devices, as well as other evidence, include staleness, scope, and correctness.

Staleness refers to the time limitations given for the search; e.g., it is common for a search warrant to state that the search must occur with ten days of the date of the warrant, although it is not always the case that a complete search can be performed in this time frame. Many jurisdictions allow that the commencement of the search within ten days follows the intent of the warrant.

Scope refers to what objects on the mobile device may be examined. Most mobile device warrants specify that all information, including but not limited to call history, SMS messages, contact lists, images, videos, etc., may be examined while other warrants might specify that, for example, only images can be searched. This situation might become more problematic as mobile devices really become recognized as mobile personal computers, raising the question of whether searching the phone's Word files is under the scope of a warrant.

Correctness refers to the description of the device in the warrant. If the search warrant has an error in the description of the device, the entire warrant may be invalidated. As an example, consider a search warrant that describes a phone by color, serial number, phone number, manufacturer, and model. If any one of these descriptors is in error, the digital investigator is well advised to consider obtaining a new warrant because a good faith exception is not allowed in many jurisdictions.

7. Economic benefits

It is well known that law enforcement agencies operate with "limited budget and finite resources" (Moore, 2006). The DFLs that these agencies rely on are no different as they continually struggle to keep pace with the technological changes in digital forensics and, more specifically, mobile device forensics. Through a cursory search of product pricing in this space, it can be said that current mobile device forensics tools costs much more than computer forensics tools simply related to the diversity of manufacturers, proprietary operating systems, and storage formats related to each and every mobile device.

Ranging in price from free to over twenty-five thousand United States dollars, each product has its own variety of mobile device coverage, and more specifically amongst each device, its own definition of what can be extracted. For instance, one mobile device forensic tool may be highly successful at retrieving basic phone identification information, personal contacts, and images used as wallpaper, while another tool may be more comprehensive with its data retrieval, extracting the call histories, text messages, and audio and video files. The economic problem lies with the DFL having to purchase both of these tools, if not several more, relying on the "Swiss Army knife approach" to perform a more comprehensive data acquisition from each model of phone that may be encountered. In addition, the cost of training and updates to the hardware and software for each system can be substantial. These constantly changing technological growth issues hinder the development of a specific forensic methodology that states that every digital investigation will be able to provide the following information from a mobile device: phone identification information, contacts, call history, text message, multimedia messages, e-mails, images, videos, and ringtones. Instead, many DFLs rely on the tools they can afford which may give them only a limited set of evidence.

As these many different mobile device forensic tools provide multiple types of evidence, it is often the case that an investigator only needs certain pieces of data from the device. Many times it is just the contacts, call history and text messages. Other times it is just the images and videos. Either way these are faster examinations than an entire acquisition of the mobile device. Nonetheless, most DFLs are still treating these devices as computer hard drives, using every tool at their disposal to try to get everything. While not only time consuming, many times the data acquired is overwhelming to the investigator. This plays out in several ways. Firstly, the time spent churning through a 16Gb Type 3 mobile device could be hours. If the contacts, call history and text messages were the necessary information for the investigation, the DFL has created its own backlog, processing a device for more than it was worth. Secondly, when investigators are handed a report back from a DFL with 16Gb of information from a Type 3 mobile phone, they contribute further to the delay in having to sift through unnecessary information.

This costly need to own every tool for getting every piece of data off of every mobile phone could be reduced through the effective use of triage inspections. If on-scene triage inspection tools were available, mobile device technicians could use these tools as front-line filters of information gatherers, reducing the backlog created in the DFL by hundreds if not thousands of mobile devices by greatly reducing the number of devices submitted to DFLs.

8. Conclusions

Mobile devices carry more and more intimate information than ever. Because these are single-user systems, usually stored in a person's pocket, in a purse, or on a belt, it is becoming easier to put a person's fingers on the keyboard of a mobile smart phone than it is a computer. As mobile devices such as BlackBerry and iPhone emerge with advanced computing power and functionality, they can contain significant amounts of probative information. The increasing number of mobile devices being seized that potentially contain useful evidence is creating backlogs in DFLs that

adversely impact public safety and the criminal justice system. In a military context, delays in extracting intelligence from mobile devices can negatively impact troop and civilian safely as well as the overall mission.

To address this problem, there is a need for effective methods and supporting tools that mobile device technicians can use to perform on-scene triage inspections. On-scene triage inspections of mobile devices enable the primary investigators to make informed decisions in a case using information that is collected contemporaneous to the crime rather waiting for the same data to be extracted at a DFL. A methodical, largely automated on-scene triage inspection process will help agencies find those devices with probative information so that the limited personnel resources are optimally assigned.

On-scene triage inspection tools need to be simple to use, yield quick results, and must not sacrifice forensic soundness for automation and a user-friendly interface. Whether in a military, law enforcement, or corporate setting, the triage inspection process should focus strictly on the authorized needs of digital investigators, allowing for the acquisition of information that can be quickly made use of by mobile device technicians in the field and examined in detail by a trained forensic examiner later.

Although the primary purpose of on-scene triage inspections is to use the digital evidence to support any kind of investigation, a side benefit of this process is economic. Front-line mobile device technicians, armed with the proper training, guidelines, and on-scene triage inspection tools, quickly get the information needed to further the overall investigation. By doing a triage inspection in-field, mobile device technicians may eliminate the need for the device to be brought to a DFL, and thus not add to backlog of mobile devices in DFLs. An effective on-scene triage inspection also allows DFLs to focus on higher level examinations of these mobile devices.

REFERENCES

ACPO. Good practice guide for computer-based electronic evidence. Available online: http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf; 2008.

Arizona v. Gant. Supreme Court of the United States. Available from: http://www.supremecourtus.gov/opinions/08pdf/07-542.pdf; 2009 [accessed 10.10.09].

Bischoff L. Cellphone searches. Available from: http://www.oxfordpress.com/news/oxford-news/cell-phone-search-requires-a-warrant-says-ohio-supreme-court-448880.html; 2009 [accessed 26.12.09].

Casey E. What does "forensically sound" really mean? J Digit Invest 2007;4(2):49–50.

Casey E, Ferraro M, Nguyen L. Investigation delayed is justice denied: proposals for expediting forensic examinations of digital evidence. J Forens Sci 2009;54(6):1353–64.

CTIA. The wireless association announces semi-annual wireless industry survey results. Available from: http://www.businesswire.com/portal/site/google/?ndmViewId=news_viewandnewsId=20091007006200andnewsLang=en; 2009 [accessed 10.10.09].

Delaitre A, Jansen W. Forensic filtering of cell phone protocols. NISTIR 7516. Gaithersburg, MD: National Institute of Standards and Technology; 2008.

Gershowitz A. The iphone meets the fourth amendment. Available from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1084503; 2008 [accessed 10.10.09].

Jansen W, Ayers R. Guidelines on cell phone forensics. Special Publication 800-101. Gaithersburg, MD: National Institute of Standards and Technology; 2006.

Kenneally EE, Brown C. Risk sensitive digital evidence collection. Digit Invest 2005, June;2(2):101–19.

Moore T. The economics of digital forensics. In Proceedings of the fifth workshop on the economics of information security, Cambridge, UK; 2006.

Ohio v. Smith. Court of appeals of Ohio, Slip opinion No. 2009-Ohio-6426. Available from: http://www.supremecourt.ohio.gov/rod/docs/pdf/0/2009/2009-Ohio-6426.pdf; 2009, December 15 [accessed 07.01.10].

Orso M. Cellular phones, warrantless searches, and the new frontier of fourth amendment jurisprudence. Santa Clara Law Review:2010. Available from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1329863, 2009, January 18;50 [accessed 10.10.09].

Parsonage H. Computer forensics case assessment and triage. Available from: http://computerforensics.parsonage.co.uk/triage/ComputerForensicsCaseAssessmentAndTriageDiscussionPaper.pdf; 2009, November [accessed 10.10.09].

Punja SG, Mislan RJ. Mobile device analysis. Small Scale Digital Device Forensics Journal 2008;2(1) (http://www.ssddfj.org/papers/SSDDFJ_V2_1_Punja_Mislan.pdf).

Rogers M, et al. Computer forensics field triage process model. J Digit Forens Secur Law(2). Available from: http://www.thesedonaconference.org/dltForm?did=TSC_PRINCP_2nd_ed_607.pdf, 2006;1 [accessed 12.12.09].

Rose C. A look at the future of mobile technology with Daniel Hesse. Charlie Rose Web site. Available from: http://www.charlierose.com/view/interview/10589; 2009 [accessed 10.10.09].

United States v. McConney. 728 F.2d 1195, 1199 (9th Cir.), cert. denied, 469 U.S. 824; 1984.

van der Knijff R. Embedded systems. In: Handbook of digital forensics and investigation. London: Academic Press; 2009.

FURTHER READING

Garfinkel S. Forensic feature extraction and cross-drive analysis. Digit Invest 2006;3S:S71–81. Available from, http://www.dfrws.org/2006/proceedings/10-Garfinkel.pdf [accessed 01.03.10].

Kenneally EE, Brown C. Revisiting risk sensitive digital evidence collection. Available from: http://euro.ecom.cmu.edu/program/law/08-732/Evidence/KenneallyandBrown.pdf [accessed 10.10.09].

Kerr O. The Fourth amendment and new technologies: constitutional myths and the case for caution. Michigan Law Review. Available from: http://ssrn.com/abstract¼421560; 2009 [accessed 10.10.09].

Lendino J. Kill your phone remotely. PCMag.com Web site. Available from: www.pcmag.com/article2/0,2817,2352755,00.asp; 2009, September 11 [accessed 26.12.09].

Population Reference Bureau. 2009 World population data sheet. Available from: http://www.prb.org/Publications/Datasheets/2009/2009wpds.aspx; 2009 [accessed 10.10.09].

The Sedona Conference. In: Redgrave JM, editor. The Sedona principles. 2nd ed. Available from: www.thesedonaconference.org/dltForm?did¼TSC_PRINCP_2nd_ed_607.pdf; 2007, June [accessed 10.10.09].

Stuntz W. Race, class, and drugs. Columbia Law Rev 1998;97:1795.