Cell Phone Forensics For Legal Professionals

GUARDIAN DIGITAL FORENSICS

Lars E. Daniel, EnCE, ACE, AME, CTNS, SCE, SCCM, SCA
Digital Forensics Examiner

Cell Phone Acquisition and Examination

GUARDIAN DIGITAL FORENSICS

Collection and Acquiring Cell Phones

Unique Preservation Issues

- **Phone must be isolated from the network.**
- **Data can be destroyed very easily by police, first responders, others.**
- **Turning the phone on can destroy data permanently**

Preservation

Phones should be left in the original condition and placed in a Faraday bag.

GUARDIAN DIGITAL FORENSICS

Collection and Acquiring Cell Phones

- Cop "thumbs through" the phone at the scene.
  - **Phone is collected and either turned off and placed in evidence**
  - **Phone is collected and left on and placed in evidence**
- Cop pulls phone from evidence and does a "thumb forensics" exam with no records or documentation.

GUARDIAN DIGITAL FORENSICS

Dangers Of "Thumb Forensics"

- Usually cannot tell if something has been deleted
- Usually cannot tell if anything has been created

GUARDIAN DIGITAL FORENSICS

Logical Acquisition Of A Cell Phone

How it Works

- Using forensic software and hardware, a connection is made to the phone and the forensic tools "ask" for the data from the phone.
- Based on modem technology

Data That Can Be Recovered

- Can recover only data that is still present on the phone (information that has not been deleted)
- Data that can be recovered includes: contacts, call history, images, videos, email, text messages, address book, etc.

GUARDIAN DIGITAL FORENSICS

Logical Acquisition Of A Cell Phone

Why do a logical acquisition of a cell phone when you could get the same information using "Thumb Forensics"?

- Verification
- Advanced Reporting
- Will Stand Up In Court
- Forensic Best Practices

GUARDIAN DIGITAL FORENSICS

Physical Acquisition Of A Cell Phone

How it Works

- Using forensic software and hardware, the physical memory of the phone or a device in the phone is recovered. This allows for the recovery of deleted data.
- Deleted data can be recovered from SIM Cards, Media Cards, and on some phones the physical memory itself.

Data That Can Be Recovered

- If the physical memory of the phone can be accessed, or a SIM Card or Media card is present in the phone it is possible to recover any type of deleted data.

GUARDIAN DIGITAL FORENSICS

Physical Acquisition Of A Cell Phone

How it Works

- Like a computer acquisition
- Forces the cell phone to give up its data

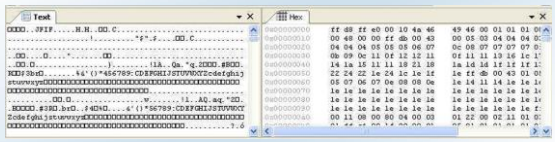
Deleted information can be recovered if a physical acquisition can be Performed.

GUARDIAN DIGITAL FORENSICS

Physical Acquisition Of A Cell Phone

How it Works

- This data was manually carved out to recover a deleted picture.



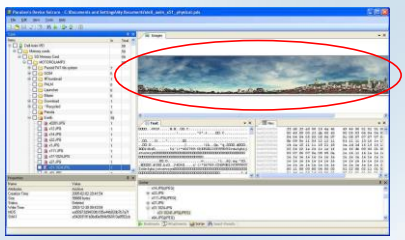
- A qualified examiner can "read" what you see above. If an examiner cannot, then they will not be able to get back the deleted picture since it must be manually recovered.
- The next slide shows the picture that was recovered.

GUARDIAN DIGITAL FORENSICS

Physical Acquisition Of A Cell Phone

How it Works

- Deleted picture that has been recovered



GUARDIAN DIGITAL FORENSICS

Manual Examination of A Cell Phone

Manual Examination: The last resort in cell phone examinations

- If no option is available to examine a cell phone logically or physically, a manual examination is performed.
- A manual examination of a cell phone should follow best forensics practices.

GUARDIAN DIGITAL FORENSICS

Manual Examination of A Cell Phone

1. A camera is used to take pictures of the screen as an examiner manipulates the phone using the keypad.
2. A video camera should record the entire examination so that a record is kept showing that no information was modified or deleted.
3. Without full documentation of the process, there is no way to know if someone deleted information in the process of a manual examination.

GUARDIAN DIGITAL FORENSICS

What Deleted Data Can Be Recovered?

Almost everything that has been deleted on a cell phone can be recovered.

- Text Messages
- Email
- Videos
- Pictures
- Voicemails (iPhone)
- Application Data
- Audio Recordings

GUARDIAN DIGITAL FORENSICS

What Deleted Data Can Be Recovered?

Deleted Text Messages

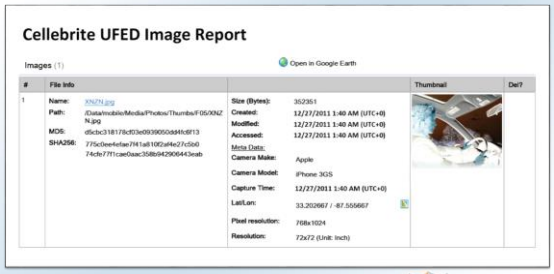
CelleBrite SMS Report

SMS Messages (21)

#	Folder	Party	Time	Status	Message	Del?
1	Sent	To: +19104770985 Brandon*	9/29/2011 7:00:17 PM(UTC+0)	Sent	U never smoke before class??	Yes
2	Inbox	From: +19104770985 Brandon*	9/29/2011 7:01:04 PM(UTC+0)	Read	Wills there... Only if im confident about the material	Yes
3	Sent	To: +19104770985 Brandon*	9/29/2011 8:10:46 PM(UTC+0)	Sent	Are you confident?? i may txt will then	Yes
4	Inbox	From: +19104770985 Brandon*	10/22/2011 4:37:28 PM(UTC+0)	Read	Its all good brotha, glad you made it home ok	Yes
5	Sent	To: +19104770985 Brandon*	10/22/2011 4:39:52 PM(UTC+0)	Sent	That was easy ;-)	Yes
6	Sent	To: +19104770985 Brandon*	12/27/2011 1:15:06 AM (UTC+0)	Sent	Yo be still, this is Aliyah. What are you up to today? I've got something if you want to help me finish it =D	Yes
7	Inbox	From: +19104770985 Brandon*	12/27/2011 1:20:30 AM (UTC+0)	Read	Haha what time	Yes
8	Sent	To: +19104770985 Brandon*	12/27/2011 1:24:23 AM (UTC+0)	Sent	Well I'll be done just around 2	Yes

What Deleted Data Can Be Recovered?

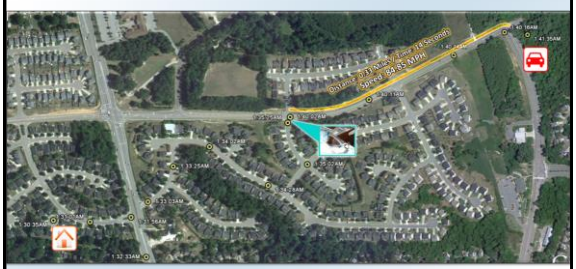
Deleted Pictures



GUARDIAN DIGITAL FORENSICS

Picture Geo-Location

Geo-Location can help put the pieces together



GUARDIAN DIGITAL FORENSICS

No Cell Phone? There is still hope!

Phone backup files on a computer can be as good, or better than the actual phone itself.

- Can recover deleted information from a backup
- Snapshot in time

(Case Example) iPhone Backup – Bank Employee (also known as “Smart Phones…Dumb People)

GUARDIAN DIGITAL FORENSICS

Challenging the Evidence

Challenging Cell Phone Manual Examinations

If a phone is evidence in a case, any manipulation of that phone constitutes a manual examination.

It is a simple process, but rarely performed correctly.

- Isolate the cell phone from the cellular network
- Video verification during the examination
- Complete chain of custody documentation

Challenging Cell Phone Manual Examinations

AFFIDAVIT EXAMPLE

Taking screenshots of a cell phone constitutes a forensic manual examination of a cell phone as the actual evidence item (the phone) must be manipulated by a forensic examiner in order to preserve the contents of the phone.

The forensic acquisition of a cell phone through the process of a manual examination requires specific skills, training, and experience in order to properly document, acquire, and preserve the evidence on a phone.

Challenging Cell Phone Manual Examinations

Isolation from Cellular Network

The forensic acquisition of a cell phone using any kind of forensic examination requires that a cell phone be isolated from the cellular network. If the phone is not isolated from the cellular network, new data is coming onto the phone and potentially destroying evidentiary data in the process of overwriting old data with that newer data.

GUARDIAN DIGITAL FORENSICS

Challenging Cell Phone Manual Examinations

The following quote is from the National Institute for Standards in Technology (NIST) article 'Guidelines on Cell Phone Forensics" by Wayne Jansen and Rick Ayers.

> Isolating the phone from the radio network is important to keep new traffic, such as SMS messages, from overwriting existing data, if the phone is turned on when found. Besides the risk of overwriting potential evidence, the question may arise whether data received on the phone after seizure is within the scope of the original authority granted. Add-on programs, such as LockMe[12] and OmniProtect[13], are also available that enable the phone lock to be set remotely upon receipt of a properly formatted message. Moreover, vulnerabilities may exist that can be exploited. For example, a malformed message sent to a Nokia 6210 phone has been shown to disable it completely, much like the a malformed ICMP packet known as the "ping of death" did to older Windows computers [Ley01].

GUARDIAN DIGITAL FORENSICS

Challenging Cell Phone Manual Examinations

The following quote is from the book "Digital Evidence and Computer Crime, Third Edition" by Eoghan Casey and Benjamin Turnbull.

> Network isolation ensures that the contents of a phone reflect the time at which it was seized, disallowing changes that may occur to it after it has been seized. Actions over the network that can alter content include receiving phone calls, messages, network polling activity, and the use of remote erasure systems; the latter being an enterprise feature designed for corporate smart phones. Such network activities can alter the contents of a mobile device, potentially adding new data, overwriting existing data or unallocated space, or erasing the phone contents remotely.
>
> Some devices can be reconfigured to prevent communication with the network. Devices that do not have such a feature can be isolated from radio waves by placing them in Faraday isolation, such as radio-frequency shielded evidence containers, which block network communications. Signal jamming systems provide another means for preventing mobile devices from communicating with a network but this type of equipment is illegal in some jurisdictions. Network isolation practices must be maintained during forensic analysis, and this is achieved with shielded mobile phone examination rooms or extraction cases. To protect the device against damage or accidental activation, package it in an envelope or bag.

Challenging Cell Phone Manual Examinations

The following quote is from the book "Digital Evidence and Computer Crime, Third Edition" by Eoghan Casey and Benjamin Turnbull.

> Network isolation ensures that the contents of a phone reflect the time at which it was seized, disallowing changes that may occur to it after it has been seized. Actions over the network that can alter content include receiving phone calls, messages, network polling activity, and the use of remote erasure systems; the latter being an enterprise feature designed for corporate smart phones. Such network activities can alter the contents of a mobile device, potentially adding new data, overwriting existing data or unallocated space, or erasing the phone contents remotely.
>
> Some devices can be reconfigured to prevent communication with the network. Devices that do not have such a feature can be isolated from radio waves by placing them in Faraday isolation, such as radio-frequency shielded evidence containers, which block network communications. Signal jamming systems provide another means for preventing mobile devices from communicating with a network but this type of equipment is illegal in some jurisdictions. Network isolation practices must be maintained during forensic analysis, and this is achieved with shielded mobile phone examination rooms or extraction cases. To protect the device against damage or accidental activation, package it in an envelope or bag.

Challenging Cell Phone Manual Examinations

The following quote is from the book "Digital Forensics for Legal Professionals", by Larry Daniel and Lars Daniel.

> **37.1.1 Protecting cell phone evidence**
>
> Like all digital evidence, the data on cell phones must be protected from being changed or destroyed during the examination process that can occur if the cell phone is allowed to connect to a cellular network. To do this, a cell phone must be isolated from all networks to prevent the phone from sending or receiving. This is usually handled by using a Faraday bag to block radio signals to or from the phone. Figure 37.2 shows a phone inside a Faraday bag for isolation during an exam.
>
> A Faraday bag blocks any signals that a cell phone might pick up by blocking electrical fields and radio frequencies. A microwave uses this same technology, utilizing a Faraday cage to contain the radio frequency generated by the magnetron within the cooking chamber. A cell phone can also be isolated from any networks by wrapping the phone in radio frequency shielding cloth and placing the phone into Airplane mode. These are the most common methods of isolating a cell phone from any networks it might connect to. There are others, but whatever methods are used to block the cell phone's signal, they need to comply with best forensic practices and be recognized as a viable solution by the digital forensics community.

Challenging Cell Phone Manual Examinations

The following quote is from the book "Digital Forensics for Legal Professionals", by Larry Daniel and Lars Daniel.

> **37.1.1 Protecting cell phone evidence**
>
> Like all digital evidence, the data on cell phones must be protected from being changed or destroyed during the examination process that can occur if the cell phone is allowed to connect to a cellular network. To do this, a cell phone must be isolated from all networks to prevent the phone from sending or receiving. This is usually handled by using a Faraday bag to block radio signals to or from the phone. Figure 37.2 shows a phone inside a Faraday bag for isolation during an exam.
>
> A Faraday bag blocks any signals that a cell phone might pick up by blocking electrical fields and radio frequencies. A microwave uses this same technology, utilizing a Faraday cage to contain the radio frequency generated by the magnetron within the cooking chamber. A cell phone can also be isolated from any networks by wrapping the phone in radio frequency shielding cloth and placing the phone into Airplane mode. These are the most common methods of isolating a cell phone from any networks it might connect to. There are others, but whatever methods are used to block the cell phone's signal, they need to comply with best forensic practices and be recognized as a viable solution by the digital forensics community.

Challenging Cell Phone Manual Examinations

Video Verification
When performing a manual examination of a cell phone, video verification must be made to comply with cell phone forensics Best Practices for the forensic acquisition of a cell phone. Otherwise, there can be no way to determine if evidence was deleted, created, or modified intentionally to tamper with the evidence, or unintentionally through ineptitude.

Best Practices require that the entirety of a manual examination of a cell phone, from the moment it is turned on until the examination is completed and the phone is powered off, that every moment of the manual forensic examination is recorded for verification purposes.

GUARDIAN DIGITAL FORENSICS

Challenging Cell Phone Manual Examinations

The following quote is from the NIST article 'Guidelines on Cell Phone Forensics" by Wayne Jansen and Rick Ayers

> Invariably, not all relevant data viewable on a phone using the available menus can be captured through a logical acquisition. For example, draft and archived messages are sometimes not recovered by forensic tools. Manually scrutinizing the contents via the phone interface menus while video recording the process not only allows such items to be captured and reported, but also confirms that the contents reported by the tool are consistent with observable data. Manual acquisition must always be done with care, preserving the integrity of the device in case further, more elaborate acquisitions need to be conducted.

GUARDIAN DIGITAL FORENSICS

Challenging Cell Phone Manual Examinations

The following quote is from the book "Digital Evidence and Computer Crime, Third Edition" by Eoghan Casey and Benjamin Turnbull.

Table 20.2 Methods of Extracting Information from Mobile Devices

Method	Description
Manual operation via user interface	Examiner manually accesses the phone through the user interface. To ensure that all details are documented and the chain of custody is preserved, this process is normally photographed or videotaped. Only data accessible through the operating system is retrievable. The most basic process.

GUARDIAN DIGITAL FORENSICS

Challenging Cell Phone Manual Examinations

The following quote is from the book "Digital Forensics for Legal Professionals", by Larry Daniel and Lars Daniel.

> Pictures only tell part of the story; what could have happened during the time between the individual pictures being taken? Pictures alone do not provide any real verification that the phone evidence has not been modified or tampered with. The only way to make a truly verifiable manual examination of a cell phone is to also record the process using a digital video camera running continuously throughout the process with no breaks, pauses, or edits. The video should begin before the phone is taken out of the secure evidence container and should be powered on in view of the camera. At the end of the examination, the phone should be powered down in view of the camera and placed back into a secure evidence container.

GUARDIAN DIGITAL FORENSICS

Challenging Cell Phone Manual Examinations

1. In the screenshots of iMessage communication allegedly from DEFENDANT to the alleged victim, it can be seen in the top left hand corner of all of the screenshots that the cell phone has both cellular and wireless service enabled. This is not forensically sound.
2. No video verification has been provided as documentation of the manual examination. Without said documentation, there is no way to verify the authenticity or falsity of the text message conversations.
3. No information concerning the digital forensic qualifications, certifications, or experience of the person who performed the forensic manual examination of the cell phone have been provided.
4. No documentation concerning the protocols, procedures, and software or hardware tools used in the forensic manual examination of the cell phone have been provided to verify the preservation, authentication, or chain of custody of the cell phone evidence item.

GUARDIAN DIGITAL FORENSICS

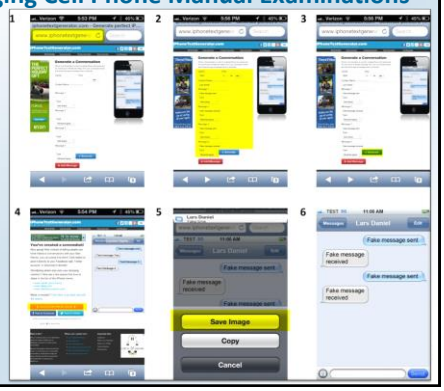
Challenging Cell Phone Manual Examinations

Pictures or Screenshots of Text Messages are not Enough: They can be faked easily, quickly, and require a low level of technical sophistication.

GUARDIAN DIGITAL FORENSICS

Challenging Cell Phone Manual Examinations

Fake Text Message Generator Website



Challenging Cell Phone Manual Examinations

GUARDIAN DIGITAL FORENSICS

Challenging Cell Phone Manual Examinations

GUARDIAN DIGITAL FORENSICS

Challenging Cell Phone Manual Examinations

GUARDIAN DIGITAL FORENSICS

Challenging the Evidence:

How Cell Phones Work: Possession, Preservation, and Distribution.

'It's either there or it ain't!"

GUARDIAN DIGITAL FORENSICS

Challenging the Evidence:

How Cell Phones Work: Possession, Preservation, and Distribution.

When receiving a MMS or SMS message on an iPhone, the recipient of the message cannot determine the contents of the message until it has already been received and viewed. Further, with a SMS or MMS message, the user does not have the ability to prevent the reception of the message.

If a person sends a SMS or MMS message to someone else, that message is automatically delivered to the other person regardless of their consent or intent to receive that message.

The delivery and receiving of MMS and SMS messages is an automated process carried out by cellular service providers and cell phone hardware that does not allow for a user to determine what SMS or MMS messages they receive. The only way to determine what the contents of SMS and MMS message are is to view the message. This description of the sending and receiving of MMS and SMS text messages is not isolated only to iPhones, but is the normal operation of almost all cellular phones.

GUARDIAN DIGITAL FORENSICS

Challenging the Evidence:

How Cell Phones Work: Possession, Preservation, and Distribution.

When receiving a MMS or SMS message on an iPhone, the recipient of the message cannot determine the contents of the message until it has already been received and viewed. Further, with a SMS or MMS message, the user does not have the ability to prevent the reception of the message.

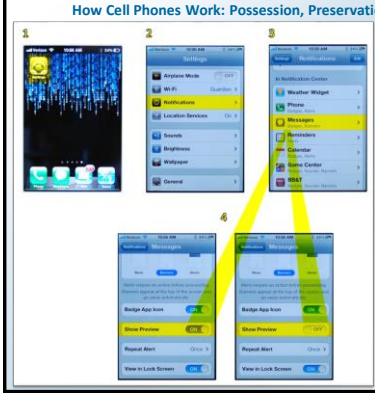
If a person sends a SMS or MMS message to someone else, that message is automatically delivered to the other person regardless of their consent or intent to receive that message.

The delivery and receiving of MMS and SMS messages is an automated process carried out by cellular service providers and cell phone hardware that does not allow for a user to determine what SMS or MMS messages they receive. The only way to determine what the contents of SMS and MMS message are is to view the message. This description of the sending and receiving of MMS and SMS text messages is not isolated only to iPhones, but is the normal operation of almost all cellular phones.

GUARDIAN DIGITAL FORENSICS

Challenging the Evidence:

How Cell Phones Work: Possession, Preservation, and Distribution.



Preview Options:
Can be enabled or disabled on an iPhone. But it doesn't change the fact that you have to see a picture to know what it is.

GUARDIAN DIGITAL FORENSICS

Challenging the Evidence:

How Cell Phones Work: Possession, Preservation, and Distribution.

Preview Options:
Can be enabled or disabled on an iPhone. But it doesn't change the fact that you have to see a picture to know what it is.

GUARDIAN DIGITAL FORENSICS

Challenging the Evidence:

How Cell Phones Work: Possession, Preservation, and Distribution.

Saving an MMS Message to an iPhone

When an MMS message containing a picture is received on an iPhone, it will only exist within the SMS folder of the file system on iPhone. The picture is automatically saved there upon receipt of the message without any input or preservation steps taken by the user. An image existing within the SMS folder of an iPhone file system will have file path that is consistent with the following example:

Library/SMS/Parts/35/05/55555-5.jpg

GUARDIAN DIGITAL FORENSICS

Challenging the Evidence:

How Cell Phones Work: Possession, Preservation, and Distribution.

1

2

3

4

For a user to intentionally preserve that image, it has to be saved to the *Photos* application on the iPhone by selecting the image, then viewing it in full screen mode, selecting the *Save Image* icon, and then selecting the *Save Image* option in the pop-up dialogue box.

GUARDIAN DIGITAL FORENSICS

Challenging the Evidence:

How Cell Phones Work: Possession, Preservation, and Distribution.

1

2

3

4

For a user to intentionally preserve that image, it has to be saved to the *Photos* application on the iPhone by selecting the image, then viewing it in full screen mode, selecting the *Save Image* icon, and then selecting the *Save Image* option in the pop-up dialogue box.

GUARDIAN DIGITAL FORENSICS

Challenging the Evidence:

How Cell Phones Work: Possession, Preservation, and Distribution.

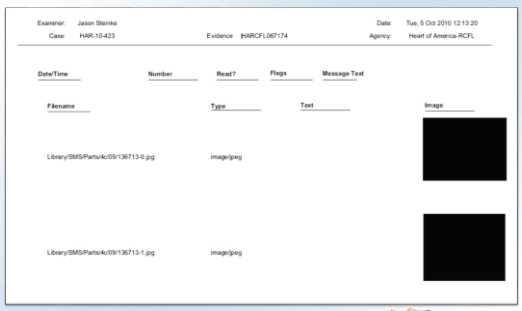
Images Received By DEFENDANT

The files of interest received by the DEFENDANT exist only within the SMS file of the iPhone file system. The following file paths and images are from a report prepared by EXAMINER at the HARCFL (Heart of America Regional Forensics Lab). The images have been redacted.

GUARDIAN DIGITAL FORENSICS

Challenging the Evidence:

How Cell Phones Work: Possession, Preservation, and Distribution.



Examiner: Jason Steinke
Case: HAR-10-423
Evidence: HARCFL067174
Date: Tue, 5 Oct 2010 12:13:20
Agency: Heart of America-RCFL

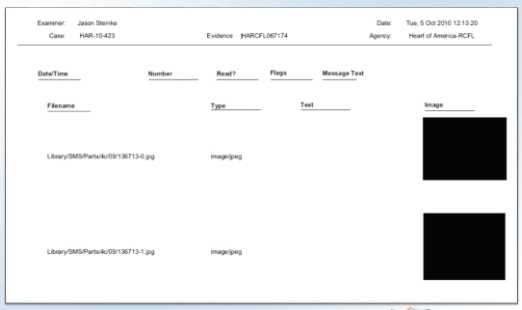
Date/Time	Number	Read?	Flags	Message Text

Filename	Type	Text	Image
Library/SMS/Parts/4c/09/136713-0.jpg	image/jpeg		[redacted]
Library/SMS/Parts/4c/09/136713-1.jpg	image/jpeg		[redacted]

GUARDIAN DIGITAL FORENSICS

Challenging the Evidence:

How Cell Phones Work: Possession, Preservation, and Distribution.



Examiner: Jason Steinke
Case: HAR-10-423
Evidence: HARCFL067174
Date: Tue, 5 Oct 2010 12:13:20
Agency: Heart of America-RCFL

Date/Time	Number	Read?	Flags	Message Text

Filename	Type	Text	Image
Library/SMS/Parts/4c/09/136713-0.jpg	image/jpeg		[redacted]
Library/SMS/Parts/4c/09/136713-1.jpg	image/jpeg		[redacted]

GUARDIAN DIGITAL FORENSICS

Challenging the Evidence:

How Cell Phones Work: Possession, Preservation, and Distribution.

Under the heading "Filename" in the report the entire file path where that file exists is listed. All of the images of interest exist within the file path **Library/SMS/Parts**.

This means that all of the images exist within the SMS folder of the iPhone file system. The images listed in the report are not images that have been intentionally preserved using the previously described method of saving images to the *Photos* application on an iPhone.

Challenging the Evidence:

How Cell Phones Work: Possession, Preservation, and Distribution.

Under the heading "Filename" in the report the entire file path where that file exists is listed. All of the images of interest exist within the file path **Library/SMS/Parts**.

This means that all of the images exist within the SMS folder of the iPhone file system. The images listed in the report are not images that have been intentionally preserved using the previously described method of saving images to the *Photos* application on an iPhone.

Beyond Cell Phones

Pads, Players, and Pods

Devices such as iPads, Android Tablets, and Microsoft Tablets are really just oversized cell phone that don't make calls technologically speaking.

- Run on the same operating systems
- Can recover deleted data from them
- Can be used to communication (text, email, and even phone calls)

Get Their Documentation
(because it is ammunition)

GUARDIAN DIGITAL FORENSICS

Forensic Procedure: Acquisition of Cellular Phones

Lars Daniel, EnCE, ACE
Guardian Digital Forensics

Chain of Custody

1. Complete a chain of custody form for receipt of the cell phone and any accessories.
   a. Each item is to be listed separately on the chain of custody form.

GUARDIAN DIGITAL FORENSICS

Get Their Documentation
(because it is ammunition)

2. All items of interest will be photographed before any work is performed for chain of custody purposes.
   a. If the cell phone is in a bag, or other container, take a photo of the container prior to removing the cell phone for inspection from the front, back, and top of the container.
   b. If the cell phone is not in a container, take a photo of the laptop in its current state of the top, bottom, front, back, left side and right side.
   c. Take close up photos of any identifying information including any asset tags, the serial number, MEID HEX, product number, ESN, and any other identifying information.
   d. If the cell phone is a flip phone, open the device to show the screen and keypad. Take photos of the screen and the keyboard area.

GUARDIAN DIGITAL FORENSICS

Get Their Documentation
(because it is ammunition)

3. Have the producing custodian sign the chain of custody form indicating that they have reviewed the inventory on the Chain of Custody form and are transferring the items to Guardian.

Forensic Acquisition Process

1. Forensic Acquisition
   a. Determine if the cell phone is currently powered on or off. If the phone is powered on, document that information and photograph the screen.
   b. Place the phone in a Faraday bag to block potential cellular reception going to the phone. Power the phone on once it is securely in the Faraday bag. Depending on the model of the phone:

GUARDIAN DIGITAL FORENSICS

Get Their Documentation
(because it is ammunition)

Forensic Acquisition Process

1. Forensic Acquisition
    a. Determine if the cell phone is currently powered on or off. If the phone is powered on, document that information and photograph the screen.
    b. Place the phone in a Faraday bag to block potential cellular reception going to the phone. Power the phone on once it is securely in the Faraday bag. Depending on the model of the phone:

GUARDIAN DIGITAL FORENSICS

Get Their Documentation
(because it is ammunition)

    a. Leave the phone in the Faraday bag for the duration of the examination from when it is powered on until it is powered off.
    b. Place the phone in "Airplane Mode" after powering the phone on while inside the Faraday bag. The phone can then be removed from the Faraday bag for examination.
2. Attach a prepared external hard drive or other data storage device to the computer. This is the "Target" storage location where the forensic images of the cell phone will be stored.
3. Using the appropriate cable, attach the cell phone to the forensic hardware extraction device (Cellebrite UFED) or directly to the computer as specified by the forensics software/hardware being used in the examination of the phone.

GUARDIAN DIGITAL FORENSICS

Get Their Documentation
(because it is ammunition)

4. Forensically image the cell phone using the selected forensic hardware or software.
5. Upon completion of the forensic imaging process:
    a. If the phone is in a Faraday bag for the duration of the examination, power the phone off while still in the Faraday bag before removal.
    b. If the phone has been placed in "Airplane Mode" and removed from the Faraday bag, place the phone back into the Faraday bag and proceed to power the phone off.

GUARDIAN DIGITAL FORENSICS

Get Their Documentation
(because it is ammunition)

Post Forensic Acquisition

1. Detach the phone from the cable and associated forensic hardware/software.
2. Open the forensic image of the cell phone in the associated forensics software program to ensure the image was completed successfully, fully, and verifiably.
3. Have the producing custodian sign the chain of custody form indicating that they have reviewed the inventory on the Chain of Custody form and are receiving the items back into their custody from Guardian Digital Forensics.
4. Create a copy of the evidence onto appropriate media storage for preservation as well as for creating copies for opposing counsel.

GUARDIAN DIGITAL FORENSICS

Questions?

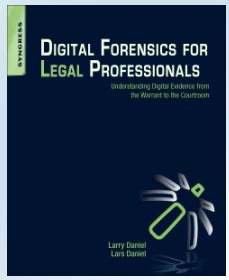
Contact Information:

Email: Lars@guardiandf.com

Phone: 919-868-6281

Web: www.guardiandf.com
Blog: www.exforensis.com

Book: **Digital Forensics for Legal Professionals**
Syngress Publishing
Larry E. Daniel and Lars E. Daniel



GUARDIAN DIGITAL FORENSICS

Motion to Compel Production of Cellular Phone

Comes now DEFENDANT, by and through his attorney ATTORNEY NAME, and moves this Court to compel production of the alleged victim's cellular phone for forensic examination.

DEFEDANT is charged with _____, of the most serious offenses under Illinois law. Considering the seriousness of this charge, it is absolutely imperative that DEFENDANT have all relevant resources available for his defense.

FACTS of the case:

On _____, 20XX, VICTIM claimed that DEFENDANT sexually assaulted her in her hotel room. Her claim is that she left her hotel room door open in anticipation of a friend's later arrival and then fell asleep. She further claims that the defendant entered her room and sexually molested her.

It is the defendant's belief that evidence contained in the electronic storage of her cellular phone (smart phone), specifically related to Twitter messages she sent to the Internet and subsequently deleted from her Twitter timeline can be recovered from the cellular phone device and that such "tweets" are critical to his defense.

In the same way that evidence collected from a cellular phone can be used to link a perpetrator to a victim, in this case, such evidence can be used to show that the victim posted information related to the alleged assault to the Internet via the service, Twitter, via "tweets", that is in conflict with her account of the crime.

Therefore the defendant respectfully requests that the court compel the alleged victim to produce the cellular "smart" phone for forensic examination for evidence of said "tweets" and other electronic communications, including email and other correspondence that would prove exculpatory to the defendant.

Forensic examinations of cellular phones are conducted every day on a routine basis by law enforcement agencies in the US and such examinations yield a great deal of evidence that is brought to bear in cases by the government. _____ is simply asking the court to allow an expert in cellular phone examinations to provide the same services for the purpose of producing exculpatory evidence that the victim may have produced communications that are in conflict with her claims via the use of her cellular phone.

Such forensic examinations are well known at this point in time with current forensic examination methods to have the ability to recover information and data that has been deleted from cellular phones, even for a significant period of time after such a deletion has occurred.

Due to the personal nature of a cellular phone, in that such devices are carried on or about a person nearly at all times, this makes the cellular phone a critical repository of evidence and as such, should be produced for examination by the defense's expert, in the same way that a

defendant's cellular phone would have been examined by the government's expert in a criminal case with an accusation of such a serious crime as this one.