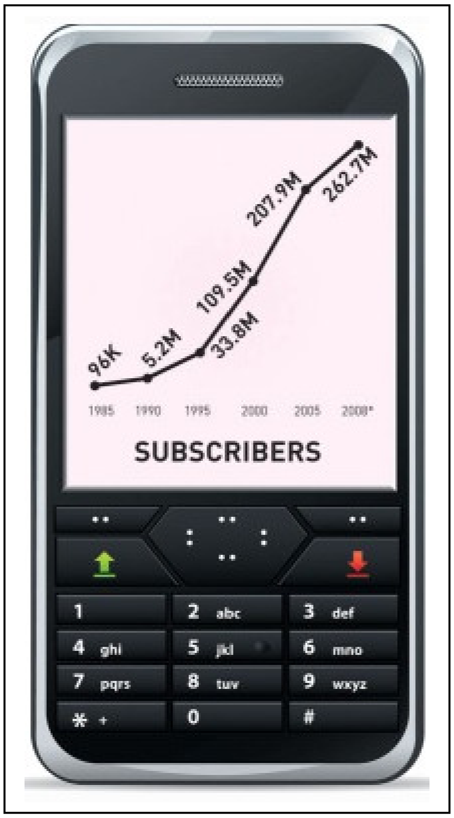
Small Scale Digital Device Forensics – Evidence from Mobile Phones and GPS Units May Surprise You!

John J. Carney, Esq.
Carney Forensics
Saint Paul

TABLE OF CONTENTS

A. Mobile Phone Market Penetration and Growth in U.S. 3
B. Text Message Usage in U.S. 3
C. Mobile Phone Prevalence and Use in Criminal and Drug-related Activities 4
D. Mobile Phone Forensics 6
1. Old Approach – Service Provider Business Records 7
2. New Approach – Direct Mobile Phone Extraction and Analysis 8
3. Information Available as Potential Evidence 8
4. Benefits of Direct Mobile Phone Extraction and Analysis 9
5. Mobile Phone Device Components 9
6. Mobile Phones are Different from Computers 10
7. Mobile Phone Extraction and Analysis Tools 12
E. Global Positioning Systems (GPS) Forensics 13
F. Can Legal Professionals Make Digital Forensics Examinations More Effective? ... 14
1. Attorneys 14
2. Investigators 15
G. Admissibility of Digital Forensic Evidence 16
H. Search & Seizure of Digital Forensic Evidence 18
I. References 19

A. Mobile Phone Market Penetration and Growth in U.S.



Skyrocketing Subscribers [1]

- Today, there are more than 262.7 million wireless subscribers— 83% of the total U.S. population. That equates to 2,869 times more subscribers today than in January 1985.

- The wireless industry saw almost 20 million new subscribers added in the last 12 months (July 2007 – June 2008).

- More than quadrupling, in the last decade (June 1998 – June 2008) the number of wireless subscribers has increased by more than 300% from 60.8 million (June 30, 1998) to 262.7 million (June 30, 2008).

- Engadget Mobile reports a study from mocoNews.net predicting 100% mobile phone penetration in the U.S. by year 2013. [2]

B. Text Message Usage in U.S.

1. Text is the New Talk: More than 384 billion text messages were reported by carriers this year [2008] between Jan. 1 – June 30, versus 295 billion voice calls. That is 22 billion more text messages than for all of 2007. Text messaging is <u>doubling</u> every year. [3]

2. Over 90 percent of handsets in the U.S. market are capable of sending and receiving SMS communications. [4]

C. Mobile Phone Prevalence and Use in Criminal and Drug-related Activities

Digital systems are found in a number of casual consumer tools, including cellular telephones. Their prevalence in society is matched by a growing presence as evidence in civil and criminal court cases. The current survey research in the U.S. suggests that cell phones and their potential evidence may be found in over half of all violent crime and even more substantially in drug crimes in some jurisdictions. [5]

A study from Europol and European Commission shows that over 70% of solved criminal cases in Europe involve phone forensics. In the U.K., Sweden, Germany, and France, it is over 90%. [6]

A search of "cell or cellular w/3 telephone or phone" within reported United States District Court opinions over a ten-year period shows dramatic growth in the number of cases in which these devices were considered to be relevant to legal proceedings. This is detailed in Figure 1. [5]

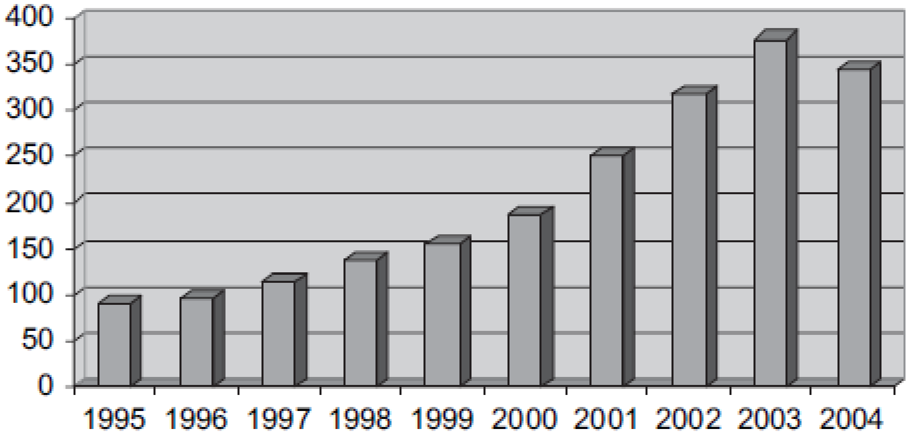


FIGURE 1 Analysis of U.S. District case opinions for involvement of cell phones 1995 through 2004.

These cases represent both criminal and civil matters with cellular telephone references for conversations, possession, use, and stored data. A sequential examination of the first one hundred such cases from May 1, 2004, to May 1, 2005, found that approximately one third were related to criminal actions. A similar search of federal appellate decisions found 219 cases over the same time period with similar references; of these, only one addressed a challenge to the admissibility of the cell phone evidence. [5]

During January of 2007, fifty-nine law enforcement executives (individuals at the rank of sergeant or above) from agencies throughout the United States who were attending a police executive leadership course were asked to respond to a written survey concerning the involvement of cell phones and crime in their jurisdictions. Specifically, they were asked whether or not a cell phone was present at the scene of the crime or in the possession or vicinity of a suspect or witness in (a) violent crimes and (b) drug crimes. [7] Figures 2 and 3 contain the responses to these questions.

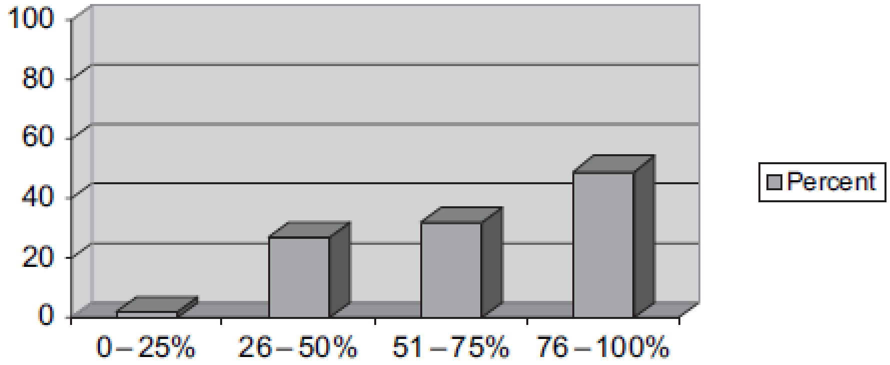


FIGURE 2 **Reported involvement of cell phones in violent crimes.**

As shown in Figure 2, these police executives reported frequent involvement of cell phones in violent crimes. A majority of the respondents (90 percent) reported knowing of some involvement. The minority reported “uncertainty” and could not respond to the question. However, as shown in Figure 2, of those who responded to the question, a clear majority (49 percent) reported they believed cell phones were involved in 76 to 100 percent of all violent crimes. A total of 81 percent of the sample responded they believed cell phones were involved in 50 percent or more of violent crimes. The observations of these police commanders show the clear and repeated involvement of cell phones on violent crimes. [5]

As with the responses to the question concerning violent crimes, approximately 4 percent of the commanders did not feel they could respond to the question. However, among those who responded, Figure 3 clearly shows their observations concerning the involvement of cell phones in drug crimes. Specifically, 81 percent reported they believed cell phones were involved in 76 to 100 percent of drug crimes. A total of 92 percent reported they believed cell phones were in involved in 51 percent or more of all drug crimes. As with the responses to questions of involvement of cell phones in violent crimes, these police commanders report an extremely high involvement of cell phones in drug crimes within their respective jurisdictions. The findings also show a higher rate of cell phone involvement in drug compared to violent crimes. [7]

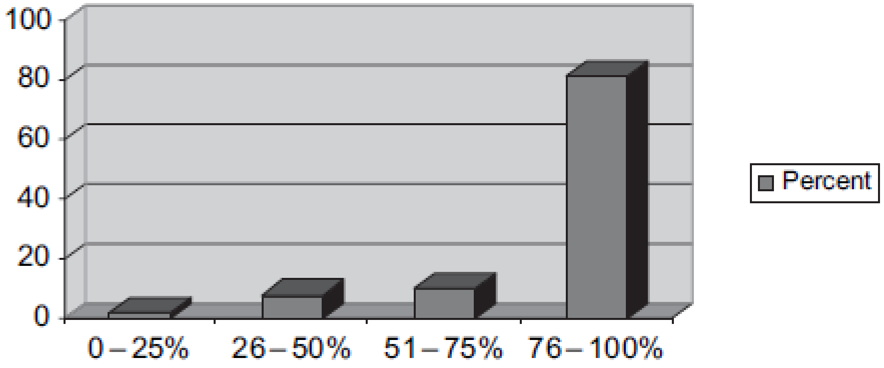


FIGURE 3 **Reported involvement of cell phones in drug crimes.**

The police commanders were additionally asked whether or not the cell phones they identified as involved in drug and violent crimes contained evidence related to the crime. The findings for this question are contained in Figure 4. In those cases where cell phones were involved with violent or drug crimes, they usually contained evidence relating to the offense. Figure 4 displays the frequency such evidence was found on these cellular telephones. [5]

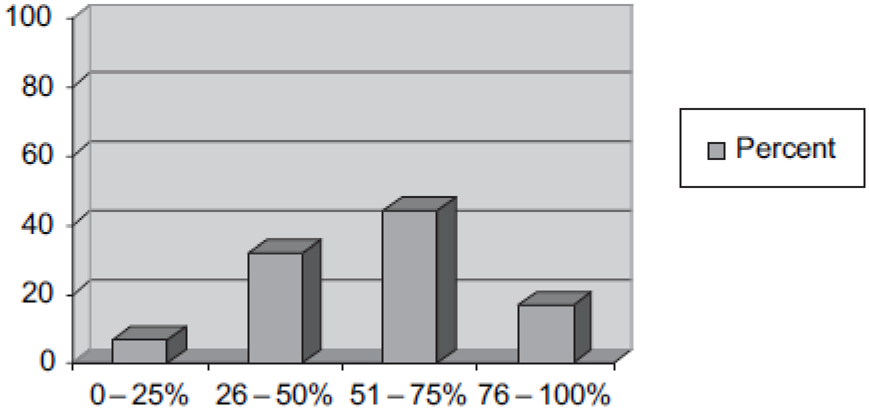


FIGURE 4 **Frequency of criminal evidence found in cell phones violent and drug crimes.**

D. Mobile Phone Forensics

Forensic evidence from mobile phones is frequently relevant in criminal cases and can help attorneys successfully prosecute or defend their cases.

1. Old Approach – Service Provider Business Records

    a. Until recently an attorney's only option to obtain mobile phone evidence was to request business records from cell phone service providers using the Electronic Communications Privacy Act.[8] A letter of preservation was required followed by a subpoena, court order, or search warrant.

    b. Information available using this technique is basic subscriber billing data and Call Detail Records (CDR). They are produced every time a user makes a call or sends a text message. The CDRs are produced in the switch where the call or message originates. CDRs are then gathered in a centralized database. Each CDR includes the following: [9]

        i. Date/time of call origination and termination
        ii. Called and calling party
        iii. Duration of call
        iv. Type of call (inbound, outbound)
        v. Originating and terminating tower (base station)

    c. Key mobile phone evidence is, however, omitted from Call Detail Records including:

        i. Phone address book
        ii. Photos (not e-mailed)
        iii. Videos
        iv. Audio clips
        v. Ring tones
        vi. Deleted phone objects

    d. Text messages are available as business records from a few service providers, if requested. But time periods to preserve them are extremely short and unworkable from a practical point of view:

i.	Sprint	12 days
ii.	Nextel	7 days
iii.	Verizon	3 to 5 days
iv.	AT&T	No preservation available

    e. Disadvantages to the business records approach include:

        i. Exposing trial strategy to opposing counsel.
        ii. Weeks, even months, of red tape involved to get records.
        iii. Business records are often confusing and difficult to interpret.
        iv. Service providers do not readily provide help for answers and assistance.

2. New Approach – Direct Mobile Phone Extraction and Analysis

   a. A new genre of cell phone forensic extraction tools bypasses service providers, their red tape and delays, and enables an entirely fresh and effective approach to evidence collection.

   b. Robert Morgester, a California deputy attorney general and expert on the topic, said that since cell phone extraction devices became available in the past couple of years, they have quickly become vital tools in solving crimes. "The reason why the cell phone is important is that you are carrying around a personal diary of who you talk to and often what you talked about," Morgester said in reference not to conversations but rather to texting, adding: "Youth today communicate through MySpace and texting." [10]

3. Information Available as Potential Evidence

   a. Mobile phone manufacturers typically offer a similar set of information handling features and capabilities, including Personal Information Management (PIM) applications, messaging and e-mail, and Web browsing. The set of features and capabilities can vary, of course, with the era in which the phone was manufactured, the version of firmware running, modifications made for a particular service provider, and any modifications or applications installed by the user. The potential evidence on these devices includes the following items: [11]

      i. Subscriber and equipment identifiers
      ii. Date and time stamps, language, and other settings
      iii. Phonebook information
      iv. Appointment and calendar information
      v. Text messages (SMS)
      vi. Dialed, incoming, and missed call logs
      vii. Electronic mail
      viii. Photos
      ix. Audio and video recordings
      x. Multi-media messages (MMS)
      xi. Instant messaging and web browsing activities
      xii. Electronic documents
      xiii. Location information

   b. Other data found on a mobile phone may also prove useful in an investigation. Even ring tones can sometimes be recovered, and they can be of probative value. If a victim was present when the suspect received a phone call at the crime scene and the witness can identify the ring tone's "melody" with particularity, the tone could add significantly to the quantum of evidence. A ring tone could implicate or exculpate a suspect.[12]

c. The items present on a device are dependent not only on the features and capabilities of the phone, but also on the voice and data services subscribed to by the user. For example, prepaid phone service typically does not include data services and rules out the possibility for multi-media messaging, electronic mail, and Web browsing. Similarly, a contract subscription may selectively exclude certain types of service, though the phone itself could support them. [13]

4. Benefits of Direct Mobile Phone Extraction and Analysis

a. Quick. Mobile phone data can be extracted and examined locally with forensics reports available in a day or two.

b. Not Public. No preservation letters, subpoenas, court orders, or search warrants are necessary.

c. Field-based. A new genre of portable forensic tools enables extraction at an attorney's or investigator's office, at the court house, or other remote location.

d. Clarity. Clear and understandable forensic reports are available now with new, advanced timelines and maps designed for attorneys and investigators coming soon.

e. Helpful. The forensic examiner can provide consulting assistance whenever and wherever needed and can serve as an expert witness to get evidence admitted.

f. Robust. Mobile phone evidence can be obtained from over 2,000 makes and models even though the service plan has been cancelled. Often text messages or images can be extracted from a phone that the owner thinks he or she has erased. So-called "deleted" data is often available, but only when new data hasn't been written over the old location in the mobile phone's memory. Phones that remain unused or lightly used since deletion are better candidates for extraction of "deleted" data.

5. Mobile Phone Device Components

a. Handsets. All mobile phones are equipped with a handset for operating the phone which includes a microphone, speaker, display, keypad or keyboard, most likely a camera and an almost endless array of other options. They also contain three essential components: Read Only

Memory (ROM) in which resides the operating system and other diagnostic software; Random Access Memory (RAM) used to store temporary data; and persistent user storage usually based on flash memory technology. Handsets can be password protected with a personal identification number to protect the privacy of the user's data residing on it.

b. SIM cards. Subscriber Identity Modules (SIM) work with a subset of mobile phone networks in use today. On them reside a user's phonebook, messages, user settings, and proof of his or her identity to the network. The SIM card allows the user to move from one mobile phone to another by simply transferring the SIM card to the new phone. SIM cards also have personal identification numbers to protect the user's data.

c. Media and smart cards. These are external memory cards that expand the storage capacity of the handset and give the user more space for messages, images, phonebook entries, etc. There are many varieties of media cards like SD (Secure Digital), MiniSD, MicroSD, and MMC mobile cards. They require special card readers in order to be read on a personal computer.

6. Mobile Phones are Different from Computers

   a. What are the Differences?

      i. Change. Mobile phone operating systems, hardware and software interfaces and standards, and storage technologies can change multiple times each year. Computer operating systems and standards are far more mature and stable and change much less frequently; usually every few years.

      ii. Platforms. A majority of desktop and notebook personal computers today run the same hardware platform and software operating system. Mobile phones are completely different and sport a staggering variety of platforms, many of them being proprietary. Even a single manufacturer, like Samsung or LG, will use many different platforms across their product line in order to remain innovative and competitive. Look at the variety of cables, over one hundred, which connect mobile phones to personal computers in the U.S. Look at all of the different types of power cords and connectors used to charge mobile phone batteries today.

      iii. Wireless. While many notebook computers have Wi-Fi connectivity, most personal computers today have a fast, direct connection to a local area network or a broadband connection to the Internet. Not so mobile phones. By definition they are untethered and use wireless communication exclusively. They incorporate one or more mobile phone radios used by cellular service providers. Most of them also support Wi-Fi, Bluetooth, or infrared wireless technologies.

b. How is Mobile Phone Forensics Different from Computer Forensics?

i. The mobile phone forensics field is only a few years old. That is relatively young compared to its more stable computer forensics ancestor that has been practiced traditionally for a couple of decades now.

ii. Many mobile phone manufacturers are pushing the envelope of emerging technology innovation using different, proprietary approaches to hardware, software, and the interfaces between them. There are very few, if any, industry standards in place. Working on a mobile phone often feels to forensics examiners like the proverbial Wild, Wild West where outlaws rule the day.

iii. Because the industry is so fragmented and moving at such a frenetic pace forensic examination of mobile phones is far less stable or predictable than computer forensics. "There are approximately 20 new cellular devices introduced to the market each month," says Richard Ayers, computer scientist at the National Institute of Standards and Technology (NIST). [14] The forensic tools are immature and lag behind new mobile phone technologies.

iv. Often a forensic examiner will need many different tools, both forensic and non-forensic, to complete an investigation successfully. No one tool can come close to doing it all.

v. Classical rules taken from traditional computer forensics may not always apply to mobile phone forensics. A fundamental tenet of computer forensics is to protect the evidence on the original device, usually a hard drive, by not allowing writes to the original data. But, sometimes a mobile phone forensic examiner will have to write to a mobile device, likely the operating system or other non-user data area, to install a software agent essential to the retrieval of information needed for investigation. A similar approach may be required to crack a phone's password or PIN to get access to the phone or its SIM card.

vi. Successful mobile phone forensic examination relies more on the skills, procedures, and problem solving abilities of the forensic examiner than it does on the technology used to extract evidence.

7. Mobile Phone Extraction and Analysis Tools

   a. History

      i. Device synchronization with personal computers. Non-forensic applications were used to synch PDAs and cell phones with PC applications like PIMs, contact managers, and even Microsoft Outlook in more recent years.

      ii. Retail mobile phone data migration. Cell phone forensic extraction is a relatively new technology that grew out of a problem faced by consumers who regularly switched cell phone carriers and wanted to load or port their old data into their new mobile phone. Early data migration tools were non-forensic, but were quickly adapted to forensic purposes by opportunistic vendors who could charge a premium for any product that could be described as "forensic".

      iii. PDA forensics. Small-scale digital forensics as a discipline began with these devices and then moved up to mobile phones and smart phones as PDAs merged with them. This convergence was driven by fashion-conscious consumers who did not want to carry multiple devices (PDA, phone, pager, etc.) on their belt or in their purse.

   b. Mobile Phone Toolkits Operate on Three Levels

      i. Manual Seizure Tools. Manual acquisition and reporting can be done by hand but has been found to be more expedient and reliable when using photographic tools. In this instance, the examiner operates the cell phone through the various screens of data as the camera records the findings and automatically puts the information into report form. Photography systems also play a key role when a new, unsupported cell phone device hits the market or the forensic examiner does not have compatible software to perform an extraction. These systems will work with all types of small-scale digital devices. [14]

      ii. Logical Acquisition Tools. These tools mine the logical "objects" in a mobile phone's memory structures. These objects include the phonebook, text messages, images, videos, etc. stored in the mobile phone. Once extracted they are usually presented in an easy-to-read report that attorneys can consult to learn more about that mobile phone's user and his or her contacts. But only active or "live" data can be acquired logically. Thus the primary disadvantage of logical acquisition is its inability to obtain and report on deleted information.

iii. Physical Acquisition Tools. "A physical acquisition recovers all the memory in a bitstream that must be parsed and interpreted to be understood," explains Wayne Jansen of the National Institute of Standards and Technology. This process yields more data — deleted files and data remnants — but is tedious and time-consuming to process manually into a readable format ready for examination, if not done automatically.[14] Yet, the difficult process is sometimes worth the effort when deleted (but "remembered") messages and images are recovered and are admissible in court.

E. Global Positioning Systems (GPS) Forensics

1. As the price of Global Positioning Systems (GPS) has dropped in recently years the market for them has exploded in the U.S. These devices hold information that can place an object at the scene of a crime, a path taken to a destination, or a favorite location recorded by its user. This information can help paint a clearer picture of the user and more importantly could solve an investigation or prove an alibi. GPS digital evidence can be used to show the nexus between time and place and to provide answers to the all-important "when" and "where" questions in a case.

2. Most cellular vendors are now offering phones and data plans that support the use of GPS and they work very similar to the smaller vehicle units. They can be used to obtain routing information and input desired addresses or points of interest. Being capable of conducting GPS routing using a cell phone is extremely convenient for many people as it alleviates the need to carry another device devoted to GPS navigation. [15]

3. The incorporation of GPS capabilities in cell phones has now created additional data values that can help tie the other activities on the cell phone to a specific location. [16]

4. The forensics analysis of a cell phone and GPS unit are very similar with the addition of so many related features. An investigation on a GPS unit in a vehicle can very likely reveal a wealth of information that includes phone calls made, contact lists, and paired devices. Likewise the cell phone may reveal GPS data and offer up a track created by the individual. Previously searched addresses or followed tracks can be apparent in the history of the device. The devices used today contain a lot more than a single specialized function that can be extremely revealing when thoroughly searched. [15]

5. In addition to the plotted tracks there may be saved routes that can be viewed in order to view trips that a user has taken or is planning on taking. Depending on the type of GPS device routes may consist of turn-by-turn directions along roads or trails, or they can contain data that is a direct route between points. Most devices also allow the creation of custom waypoints and points of interest (POI). Identifying these waypoints or POIs can help an examiner in understanding why the user moved through certain areas and what areas they were planning on visiting in the future. In most cases it is also possible to identify recent location searches, identify the coordinates of a home location, and possibly find information about the owner of the device such as name and phone number. [15]

F. Can Legal Professionals Make Digital Forensics Examinations More Effective?

1. Attorneys

   a. Mobile phones are everywhere today. And evidence residing in those phones is likely relevant, even pivotal, to winning cases. Have you thought about where that potential evidence might be? Could it be in county/city/town evidence lockers ready to be harvested? Could it be in the mobile phone possessed by your defendant, your client, your co-defendant, or a complaining witness? Or, could it be out there in use every day and in jeopardy of disappearing or being erased?

   b. It behooves each attorney with potential criminal evidence, either incriminating or exculpatory, residing in a mobile phone to find and analyze that evidence early – before that phone is:

      i. Lost at a gas station
      ii. Tossed in a lake or river
      iii. Stops working or its service discontinued ("pay as you go" plans, etc.)
      iv. Password protected and code is lost (PIN/PUK)
      v. Irreparably damaged
      vi. Wiped automatically over the network by its service provider or at the user's request
      vii. Accidentally or intentionally erased of its texts, images, videos
      viii. Used actively, day in and day out, which silently recycles deleted texts, images, and videos to accommodate "new" information

   c. With what benefits? When evidence is found, it can be analyzed and often admitted at court. It also leads to better communication with clients and with adversaries at law. It yields better case strategy and theories and better outcomes at court.

d. Timeliness is everything! It has a direct impact on authentication and admissibility of relevant evidence needed to win cases.

2. Investigators

a. Have you anticipated what the mobile phone forensic examiner will ask of you? He or she will ask for your mobile phone's:

i.	Make	(Samsung)
ii.	Model	(SGH-T919)
iii.	Street Name	(Behold)
iv.	Service Provider	(T-Mobile)

b. He or she will use National Consortium for Justice Information and Statistics (NCJIS) Device Worksheets, or an equivalent including:

i. Field Seized Handheld Device Worksheet
ii. Seized Handheld Device Analysis Worksheet
iii. Mobile Evidence Processing Request
iv. Handheld Device Analysis Control Sheet
v. SIM Card Analysis Worksheet

c. He or she will use "first responder" protocols. Do you have what you need to provide maximum assistance?

i. Maintain power to the device
ii. Isolate device from network
iii. Use protective case
iv. Gather media cards, SIM cards, and accessories (power cord, charger, cradle, cables, user manual, etc.)

d. Have you been alert to your mobile phone's:

i. Physical damage / water damage, etc.
ii. Passwords, PINs, PUKs
iii. Data encryption, if any

e. Have you observed international Standards for Handling Digital Evidence? [17]

i. Upon seizing digital evidence, actions taken should not change that evidence.
ii. When it is necessary for a person to access original digital evidence, that person must be forensically competent.
iii. All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.
iv. An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.

v. Any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles.

f. If you have become a custodian of potentially relevant evidence, have you observed strict Chain of Custody Procedures? [18]

i. Maintaining data integrity is crucial to admissibility of digital evidence.[19]

ii. Counsel must be certain the forensics examiner or investigator strictly keeps a complete chain of custody for all collected data including:[19]

1. Uniquely identify each item of property (media) to be placed under chain of custody control (examination test).
2. Document from whom the media was received or who authorized its removal.
3. Document the location where media was received.
4. Document the date and time investigator took control of media.
5. Document any mail or courier service transactions.
6. Keep a continuous record of custody of an item from time acquired until time transferred out of investigator's control.

G. Admissibility of Digital Forensic Evidence

1. Cell phone evidence may be used without the expert foundation of reliability required by U.S. Federal Rule of Evidence 702. "Every case involving equipment—whether it be computers, camera, or speed guns—does not automatically require a Daubert hearing regarding the physics behind the operation of the machine."[20] For example, a court may permit a witness to read telephone numbers from pager or cell phone memory for the jury.[21]

2. Both federal and state courts have well established precedents for how evidence should be handled and admissibility rules for the evidence and subsequent testimony of experts. The very rules which apply to admissibility of evidence also apply to the admissibility of evidence harvested from small scale digital devices. [22]

3. When admissibility in court is the ultimate goal for the electronic evidence, steps should be taken to ensure the evidentiary collection, examination, analysis and production methods can withstand a challenge under the Rules of Evidence. In particular, a civil matter in Federal court should be able to withstand the scrutiny of the Daubert Test. Some investigative instances will occur in which court admissibility is not the objective. The term "mobile phone exploitation," coined by Richard Mislan at the Purdue University Cyber

Forensics Lab, can be used to describe the intended deviation from methods which can withstand admissibility tests such as Frye or Daubert. [22]

4. There are many challenges facing the forensic examination of a small scale digital device. In 2007, the Scientific Working Group on Digital Evidence (SWGDE) published Special Considerations When Dealing With Cellular Telephones which included the following limitations: [23]

    a. Cables - access cables are often unique to a particular device.

    b. Passwords - passwords can restrict access to a device. Traditional password cracking methods can lead to permanent inaccessibility of data.

    c. SIM (Subscriber Identity Module) Cards – easily passed between cellular handsets, the amount and type of data that is located on a SIM card varies by manufacturer and carrier.

    d. Lack of Training - as a result of vendor specific technology, there is not a standardized method of extracting data from these devices.

    e. Dynamic Nature of the Data - most embedded devices do not have a non-intrusive method to access stored data. Specifically, the system data on cellular telephones is constantly changing regardless of conventional write blocking methods.

    f. Block Incoming and Outgoing Signals - attempts should be made to block incoming and outgoing signals of a wireless device. Common methods include portable Faraday bags and RF enclosures. However, these methods can be quite expensive and not always successful or practical.

    g. Legal Issues - unopened emails, unread text messages, and incoming phone calls of seized devices present nonconsensual eavesdropping issues, especially if the examination is not conducted in a timely manner.

    h. Condition of the Evidence - cell phones and similar devices are subject to be damaged or contaminated. Damaged / destroyed handsets present a unique challenge in that the current methodologies suggest interaction with an operable device.

    i. Loss of Power - many of these devices lose data or initiate additional security measures once discharged or shut down.

j. Unallocated Data - most of the forensic tools available do not address storages areas in cellular telephones that may contain deleted information.

H. Search & Seizure of Digital Forensic Evidence

5. State v. Novicky[24]

a. A recent Minnesota appellate court case challenged a warrantless search of a cell phone months after it was seized on the grounds it was a violation of his Fourth Amendment rights. The court determined defendant's Constitutional rights were not violated when the police searched his cell phone pursuant to the automobile exception. The police arrested the defendant while he was sitting on a car. They noticed a gun and two cell phones sitting on the seat of the vehicle. The defendant's cell phone was inventoried at the police station. On the first day of trial, one of the officers retrieved the cell phone from the drop safe, accessed the voicemail menu, and hit enter – showed the phone was calling defendant – indicated that the phone was his, thus tying him to the gun.

b. Specifically, the court's opinion held: [25]

i. Defendant had standing to challenge the search of the cell phone. Although it was in someone else's car, in plain site, and not password protected, he had a reasonable expectation of privacy.

ii. The warrantless search of defendant's cell phone was not incident to arrest due to remoteness in time from the arrest and lack of exigencies.

iii. But search of cell phone was valid under automobile exception.

1. Police had probable cause to believe the cell phone contained evidence of a crime and therefore could be reasonably searched as a container in an automobile.

2. This search does not need to occur contemporaneously with or close to the time of seizure of the automobile or container.

3. Defendant did not show that the delay adversely affected a privacy or possessory interest in the phone.

I. References

1. CTIA, Annual Total Wireless Subscribers (1985-2008). Available at http://www.ctia.org/content/index.cfm/AID/11499.

2. Darren Murph, engadget iMobile, Study suggests 100% mobile phone penetration in the US by 2013, Posted Aug 26th 2007 at 9:59AM. Available at http://www.engadgetmobile.com/2007/08/26/study-suggests-100-mobile-phone-penetration-in-the-us-by-2013/. Also available at http://moconews.net/article/419-us-mobile-penetration-to-hit-100-percent-by-2013-report/.

3. CTIA, The Wireless Association® Celebrates 25 Years of Mobile Communication, October 13, 2008. Available at http://www.ctia.org/media/press/body.cfm/prid/1781.

4. Enid Burns, Mobile Campaigns Transcend SMS, ClickZ, Dec 19, 2006. Available at http://www.clickz.com/3624235.

5. Michael Losavio, Dr. Deborah Wilson, Dr. Adel Elmaghraby, Prevalence, Use, and Evidentiary Issues of Digital Evidence of Cellular Telephone Consumer and Small-Scale Devices, Journal of Digital Forensic Practice, 1:291-296, 2006.

6. Martin Westman, Complete Mobile Phones Forensic Examination: Why We Need Both Logical & Physical Extractions, Micro Systemation Inc., presented to Mobile Forensics World 2009, Chicago, IL.

7. Losavio, Michael, Southern Police Institute Survey of Administrative Police Officers, February 27, 2007.

8. 18 U.S.C. §2510 et seq.

9. Svein Y. Willassen, M.Sc., Mobile Forensics: Evidence in Mobile Phone Systems. Available at http://web.archive.org/web/20041126135046/http://www.mobileforensics.com/

10. Tom Abate, Police Probe Cell Phones to Thwart Criminals, San Francisco Chronicle, September 9, 2008. Available at http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/09/07/BUPA12OC2V.DTL

11. Jansen, Wayne and Ayres, Rick. (May 2007). Guidelines on Cell Phone Forensics. Recommendations of the National Institute of Standards and Technology. U.S. Department of Commerce.

12. Michael J. Tonsing, New Techniques to Extract Evidence from Cellular Phones Create Dilemma for Courts, Prosecutors, and Criminal Defense Lawyers, Federal Lawyer, October, 2008.

13. Jansen, Wayne and Ayres, Rick. (May 2007). Guidelines on Cell Phone Forensics. Recommendations of the National Institute of Standards and Technology. U.S. Department of Commerce.

14. Jeannine Heinecke, An Evolution in Cell Forensics, Law Enforcement Technology, November, 2007. Available at http://www.officer.com/print/Law-Enforcement-Technology/An-evolution-in-cell-forensics/1$39629.

15. Chad Strawn, Expanding the Potential for GPS Evidence Acquisition, Small Scale Digital Forensics Journal, Vol. 3, No. 1, June 2009.

16. Smith, Nathan M. GPS GIS and Position Tracking Technology Privacy and Law Enforcement. Available at http://blog.nathanmsmith.com/index.php?entry=entry070508-233001.

17. International Principles for Computer Evidence (IOCE, October 1999).

18. State v. Hager, 325 N.W.2d 43, 44 (Minn. 1982).

19. Michele C.S. Lange, Kristin M. Nimsger, Electronic Evidence and Discovery: What Every Lawyer Should Know, American Bar Association, 2004.

20. United States v. Lauder, 409 F3d 1254, 1265 (10th Cir. 2005).

21. United States v. Wells, 347 F3d 280, 289 (8th Cir. Cert denied, 541 U.S. 1081, 124 S. Ct. 2435, 158 L.Ed. 2d 996 2004).

22. Rebecca Hendricks, Admissibility of Small Scale Digital Devices in U.S. Civil Litigation, Small Scale Digital Device Forensics Journal, Vol. 2, No. 1, June 2008.

23. Special Considerations When Dealing With Cellular Telephones. Scientific Working Group on Digital Evidence. (April 5, 2007). Available at http://68.156.151.124/documents/swgde2007.

24. State v. Novicky, 2008 WL 1747805 (Minn. Ct. App. 2008) (review denied June 18, 2008).

25. E-mail communication with Professor Edwin J. Butterfoss, Hamline University School of Law, April 3, 2009.