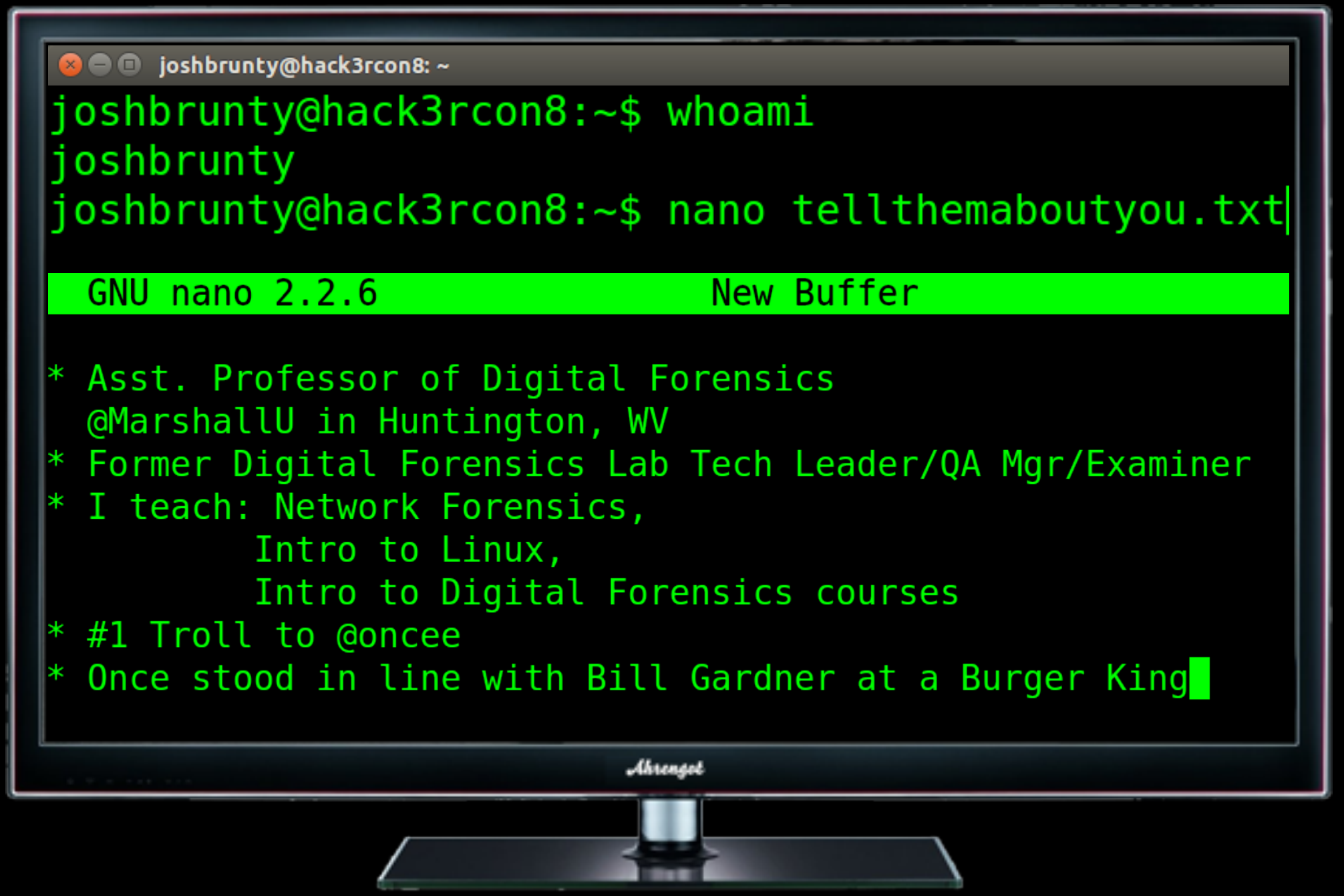
Mobile Device Forensics (An Introduction)

Josh Brunty,
CCME, CCO, CCPA, CHFI, MPSC, ACE

Assistant Professor
Marshall University

DIGITAL FORENSICS
INFORMATION ASSURANCE


joshbrunty@hack3rcon8: ~
joshbrunty@hack3rcon8:~$ whoami
joshbrunty
joshbrunty@hack3rcon8:~$ nano tellthemaboutyou.txt
GNU nano 2.2.6 New Buffer
* Asst. Professor of Digital Forensics
@MarshallU in Huntington, WV
* Former Digital Forensics Lab Tech Leader/QA Mgr/Examiner
* I teach: Network Forensics,
Intro to Linux,
Intro to Digital Forensics courses
* #1 Troll to @oncee
* Once stood in line with Bill Gardner at a Burger King

Schedule

Part I

- Cell Phones and Crime

Part II

- Terms and Technology

Part III

- Sources of Cell Phone Evidence

Part IV

- Seizing/Analyzing Cell Phones

Part I

CELL PHONES AND CRIME

Why we need to learn about mobile devices

Because they are used in crimes like…

- Drug Trafficking
- Homicide
- Gang Activity
- Terrorism
- Harassment/Threats
- Child Pornography
- Kidnapping
- Security breaches (i.e. credit card skimming)
- iOT Threats
- Actually, just about any crime!

TERRORISM

CNN.com

PRINT THIS
Powered by Clickability

Click to Print

SAVE THIS | EMAIL THIS | Close

Mobiles used in high-tech terror

By CNN's Jim Boulden

LONDON, England (CNN) -- Mobile phones are in the hands of millions of people around the world. And increasingly, it appears, in the hands of terrorists.

The bombers who targeted commuter trains in Madrid on March 11 used the built-in alarm clock in mobile phones to set off explosives.

In Jerusalem, it is believed a call to a cell phone in a rucksack set off a bomb at Hebrew University in 2002, killing seven.

One of the Bali bombs outside the Sari nightclub in October 2002 had a cell phone attached, as did a car bomb which killed 12 people at the Jakarta Marriott hotel last August.

David Claridge, of the Risk Advisory Group, said: "Mobile phones are relatively cheap, you can acquire them in relatively large numbers and you can build a whole stack of them at one time and place them and set them off at your leisure.

"It means that you can step away some considerable distance, the other side of the world, in order to initiate the explosive device."

Searches following attacks in Riyadh, Saudi Arabia, last May led to an FBI warning about the use of cell phones, saying the modifications needed to turn a phone into a trigger were "relatively minor."

Child Pornography

Sep 26, 2007 11:44 am US/Central Digg | Facebook | E-mail | Print

Mansfield Police Find Child Porn On Cell Phone

by Stephanie Lucero

MANSFIELD (CBS 11 News) — A North Texas high school student is accused of using his cell phone to make child porn and police are asking the public for help in identifying the victims.

A day after Mansfield Police confiscated two cell phones when they stopped an 18-year-old on a bicycle they say they found nudity, child pornography and a possible sexual assault in progress.

During police dash camera video moments after Deaun Akles was stopped by police, the officers say when they flipped open one of them, there was an image of a topless girl on the main screen.

"How old is she?" one of the detectives is heard asking on the video. Akles responds, 15.

"Okay, you gave him permission to use your phone and he found a picture of a 15-year-old girl naked on your phone? You're being arrested for possession of child pornography," the officer responds.

Mansfield police say the two cell phones contained numerous pictures of child pornography.

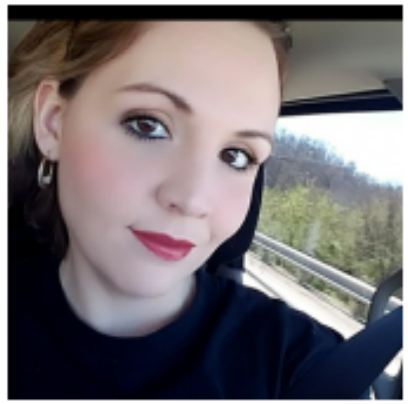
On Tuesday, the day after Akles' arrest, authorities say video in the cell phone was most disturbing.

"The victim is engaged in sexual intercourse," explains Det. Barry Moore with the Mansfield Police Department.

MetroNews
THE VOICE OF WEST VIRGINIA

Teacher arrested for sending nude pictures to students

By **Chris Lawrence** in **News** | September 01, 2017 at 4:11PM



Logan Co. Sheriff's Dept.
Tracy Miller

LOGAN, W.Va. — A Logan High School teacher is charged after investigators say she confessed to sending inappropriate pictures of herself to students.

Tracy Miller, 27, who started teaching at Logan High School in January, now faces three counts of distribution of obscene material to minors.

"We spoke to one of the students who allegedly got the pictures and observed the pictures," said Logan County Chief Deputy Mike Mayes. "There's possibly up to five students who could have pictures of the teacher."

Miller confessed to sending nude pictures to the high school boys when interviewed by investigators.

The Herald-Dispatch
herald-dispatch.com
HUNTINGTON, WV

Credit card vulnerability awareness rises

By JOSHUA QUALLS Nov 2, 2017 (0)

"We're never going to completely get rid of vulnerabilities," said Joshua Brunty, assistant professor of digital forensics and information assurance at Marshall University.

"When people do that, I think we'll see less skimming incidents occur."

Consumers are especially vulnerable at gas pumps, where they soon will be filling up for road trips to visit family over the holiday season.

Skimming devices often are hidden inside gas pumps or secretly affixed to keypads and credit card readers, and they can capture names, credit card numbers and Social Security numbers embedded into magnetic strips.

Cell Phone Laws

MSNBC.com

Texas targets cell phone use by gangs

Proposal would require state-issued ID to purchase prepaids

By Jeff Carlton

The Associated Press

updated 7:09 p.m. ET, Thurs., Jan. 31, 2008

DALLAS - A Texas lawmaker said Thursday he plans to target international gangs by going after technology that has kept them a step ahead of law enforcement: prepaid cellular telephones.

State Sen. John Carona introduced a proposal that would require a state-issued ID to buy prepaid cell phones, and retailers to track who is buying them. If it becomes law, Carona's proposal would limit consumers to buying no more than three prepaid cell phones at a time.

Carona, the chairman of the Senate Committee on Transportation and Homeland Security, said it's time to update a law enforcement approach to gang activity that "hasn't changed much since the days of Elliott Ness and Tommy guns."

"Prepaids are popular with criminals because they are cheap, accessible, untraceable and discardable," said Carona, R-Dallas, during a news conference at Dallas police headquarters.

Under his plan, cell phone makers and service providers would preserve phone records and make them available to police during criminal investigations. Carona said he will introduce the proposal in next year's legislative session.

"These devices are used regularly in the commission of crimes," Carona said. "Criminals have the enormous ability to be able to communicate in an untouchable fashion — and that's unacceptable."

Dallas Police Chief David Kunkle said prepaid cell phones are popular with international gangs because they are difficult to trace back to the original buyer.

"The primary tool they used to communicate among each other is prepaid cell phones," Kunkle said. "And it's made investigation of drug trafficking and street gang criminal activity very difficult and, in many cases, impossible for us."

Spyware/Malware

ZDNet.co.uk
WHERE TECHNOLOGY MEANS BUSINESS

Phone phishing attack hits US

Criminals are trying a new approach to try to dupe people into downloading a Trojan horse program

Criminals have launched a blended attack which attempts to lure users to a malicious Web site via text message.

IT managers have been warned to alert their staff to the attack, which uses social engineering techniques to try to trick users to the phishing site, according to security vendor Websense.

Users are sent an SMS text message to their mobile phone, thanking them for subscribing to a fictitious dating service. The message states that they will be automatically charged a subscription fee of $2.00 per day, which will be added to their phone bill, until their subscription is cancelled at the online site.

The same message has also been spammed to the comments section of numerous bulletin boards.

Once victims visit the site to unsubscribe, they are prompted to download a Trojan horse program which is a variant of a program Websense calls "Dumador". Once installed, the program turns the computer into a zombie, allowing it to be remotely controlled by the hackers.

Once machines have been compromised, they become part of a bot network, which can then be used to launch distributed denial of service attacks, install keylogging software and store account information.

Part II

TERMS AND TECHNOLOGY

Terms and Technology

Some of the terms and technology we are explaining here, become important later when we discuss search and seizure. For example,

- What are SIM card and MicroSD cards, and what do they look like?
- What passwords might you encounter on the phone?
- What type of information will the network provider have?

Cell Phone Technology

GSM
Global System for Mobile Communication

(e.g. Sprint, AT&T)

CDMA
Code Division Multiple Access

(e.g. Verizon)

These two technologies do the same thing.

Remember?

VHS vs. BETA

BlueRay vs. HD-DVD

Cell Phone Technologies

Cell phone devices have unique identifying electronic serial numbers.

IMEI International Mobile Equipment Identifier	A unique number which identifies a phone handset on a GSM network.
ESN Electronic Serial Number	A unique number which identifies a phone handset on a CDMA network.
MEID Mobile Equipment Identification	A unique number which identifies a phone handset on a CDMA network. Replaced ESN number on new phones.

About SIM Cards

GSM phones have a small smartcard inside the phone which contains the subscriber information, called a SIM.

SIM stands for “Subscriber Identity Module.”

Look for these during searches, and include as an item to be seized in your search warrants for cell phones.

More about SIM Cards

When you move a SIM card from one phone to a second phone, you move the telephone number to the second phone, too!

SIM cards are popular with International travelers as you can buy pre-paid SIM card in the country where you travel and make local calls.

A user can have more than one SIM card per phone.

A user can use his/her SIM card in other phones.

Cell Phone Technology

SIM Cards have two unique serial numbers.

ICC-ID Integrated Circuit Card Identifier	The unique serial number of the SIM card. Contains encoded information about the country and the provider who issued it.
IMSI International Mobile Subscriber Identifier	A unique number related to the subscriber's account. It also contains encoded information about the country and the provider who issued it.

Passwords - SIM

A SIM card may be locked with a password. This is called a PIN or Personal Identification Code.

- The use of a PIN can be enabled or disabled.
- The user can change the pin.
- The PIN is not known by the Network Provider.
- 3 PIN attempts allowed, then card can only be accessed with PUK.

- A PUK (PIN Unblocking Key) will allow the PIN to be reset.
- PUK is not changeable by the user and is known by the network provider.
- 10 PUK attempts allowed, then card permanently disabled.
- NEVER guess the PUK. It will destroy all data on the card!

Passwords- Device Lock

A device may be locked with a password. This is called a keyboard lock or handset password.

- When you power off the phone, you may be required to enter the password when you restart the phone.
- It may be impossible to recover any data from the phone handset without the password.

Part III

SOURCES OF MOBILE DEVICE EVIDENCE

Information found on Mobile Devices

Called Phone Numbers

Incoming Call Numbers

Missed Calls Phone Numbers

Address Books

Contact Lists

Memos/Notes

Photographs/Pictures

Video

Voice Recordings

GPS Coordinates (both WIFI & tower)

Web Addresses (URL)

Internet Activity History

Text Messages

Chat

Email

Calendars

Seven Sources of Evidence

Phone handset memory

SIM Card
- or other identity module card

Removable media
- such as Micro SD card

Documentation
- Phone Bills, manuals, packaging, etc.

Cellular Network/3rd Party Providers

Subscriber or other persons
- having knowledge of the cell phone usage or account data.

Computers
- cell phone or removable media may have been attached to for data transfer and/or backup.

1. Phone Handset Memory

The phone handset contains memory chips that hold data, such as

- Operating System
- Applications
- User Data
  - Phone numbers
  - Text messages
  - Pictures
  - And more!

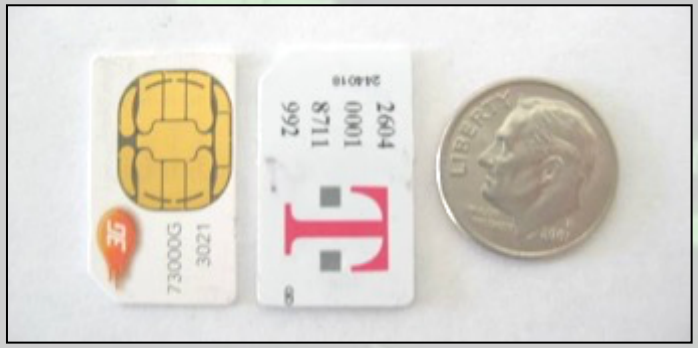
2. SIM Cards

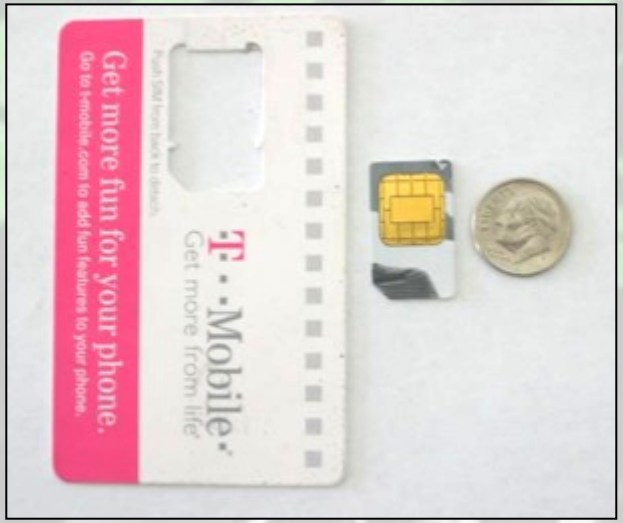
SIM Cards may contain:

- Last dialed numbers (LDN)
- Text messages (SMS)
- “Phonebook” (ADN)
- Serial Number (ICC-ID)
- Last cell tower (LOCI)

Data can be stored on phone’s memory or SIM card or both

WARNING: Do NOT place substitute SIM card into a GSM phone. It will alter or delete phone data.





2. SIM Cards –Example

Front view

Battery view (back cover removed)

Battery removed and SIM card inserted

Battery removed and SIM card removed

2. SIM Cards – iPhone/Android

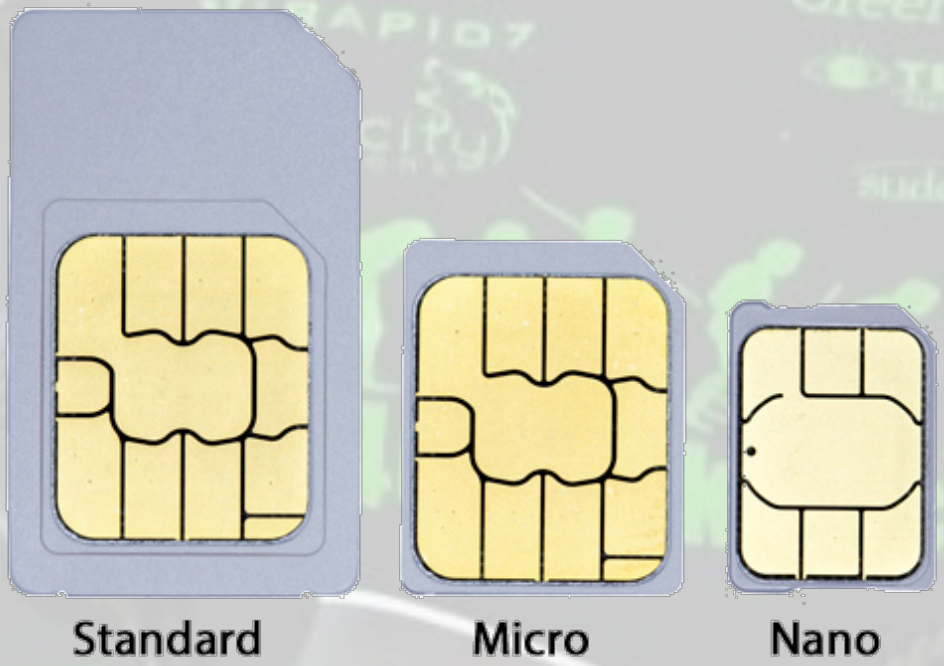
2. SIM Cards – Dual SIM phone

Multiple SIMs allows user to switch between multiple subscriber accounts.

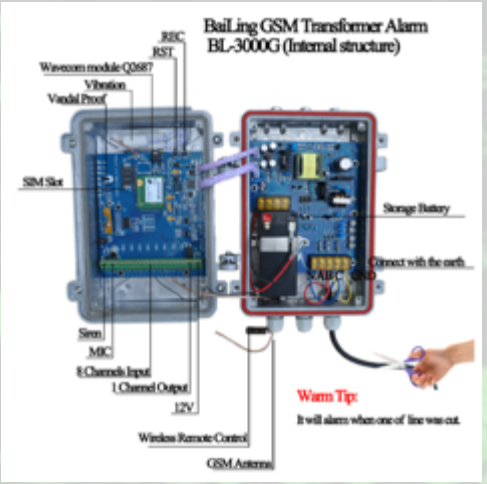
2. SIM Cards - MicroSIM

There are various sizes (form factors) for SIM cards. These three can be found in cell phones or other handheld devices:

- SIM (ID-000)
- Micro SIM (3FF)
- Nano SIM (4FF)



2. SIM Cards - Miscellaneous



SIM cards can be hidden easily. Search carefully.

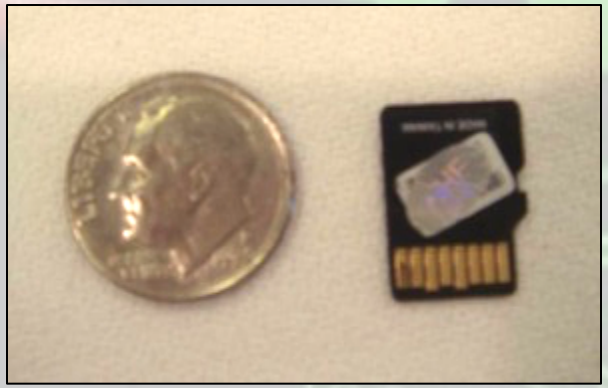
SIM cards can also be used in devices other than phones, such as this eavesdropping device or in devices like tablets (e.g. iPad).

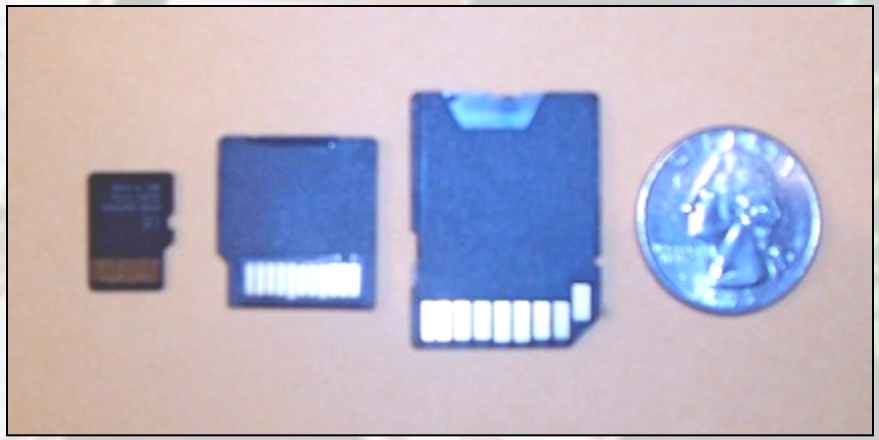
3. Removable Media

The MicroSD card (pictured right) is smaller than a dime!

The cards can hold 2-32GB (gigabytes) of information!

The cards can hold any files, whether useable by the phone or not.





The picture (left) depicts cards: MicroSD, MiniSD, and SD cards, shown left to right, with a quarter.

“SD” means “Secure Digital”

4. Documentation

- Phone Bills
- Manuals
- Software
- SIM Card Holder
- Original Packaging

5. Cellular Network/3rd Party Providers

The network carrier may have important information or evidence. Know what information the cellular network may provide.

Know what information you need.

- Subscriber/Billing information.
- Call Records
- Location information (cell tower, GPS)
- Data backups
- Photo Albums

5. Cellular Network/3rd Party Providers

3rd party providers

- iCloud
- WhatsApp
- Facebook Messenger
- Snapchat
- Dropbox
- Applications such as skype, gmail, facebook, GoogleDocs
- Other cloud computer/web-based services (i.e. Evernote)

5. Cellular Network/3rd Party Providers

Data retention periods (if any) may be very short. Consider submitting a “preservation order” to the provider while obtaining a search warrant or subpoena.

Preservation Orders (18 USC 2703f)

- Purpose is to alert provider not to purge data
- Without notice to subscriber
- No change to user’s account status
- Verify request received.

6. People Associated With the Phone

Ask people questions about the phone…

- What is the phone number?
- Who is the subscriber on the account?
- Who pays the bills?
- Who is the network provider?
- Is there a password/code needed to unlock the phone?

7. Computers Associated With the Phone

Ask: Has this phone been connected to a computer to synchronize data or to change phones?

- You may want to seize that computer, too.

Finding data cables and/or software may be an indication that the phone was connected to a computer (transfer/backup phone data).

Finding removable media and/or adapters may be an indication that the phone media was connected to a computer (transfer/backup files).

Part IV

SEIZING CELL PHONES

Seizing Phones

So, as you see there may be a lot of data and file types associated with a cellular phone.

It is likely that some of that information might be helpful in your investigation.

Please consult with your prosecutor, district attorney, and/or administrators regarding legal issues in your jurisdiction.

How do we properly seize a Cell Phone and preserve the data?

Basic Steps for Seizing Cell Phones

1. Secure the phone. Prevent the phone from being used. Capture information on display.
2. Prevent phone's access to the carrier or mobile network.
3. Ask for information.
4. Seize related hardware/software.
5. Seize related documentation.
6. Transportation and storage. Store securely and maintain chain of custody.
7. Obtain services of qualified examiner to analyze phone. (Keep phone charged, if appropriate.)

Step 1: Secure The Phone

If phone is off,

- Leave the phone off.
- Do not allow users to operate the phone.

If phone is on,

- Do not allow users to operate the phone.
- Record any important information that may be viewable on the phone's display screen, using notes, video, or photography. This information may not be recoverable later.

If Phone Stays Connected to Network

Location/cell tower information stored on the phone and/or SIM and with the network provider changes.

Modified incoming call logs (e.g. if the maximum number of calls recorded is reached, and new calls come in, old calls get deleted from the phone).

Deleted text messages will be overwritten by new incoming text messages.

A “kill signal” may be sent from the enterprise or provider, which will delete user data on the phone.

If data are changing, deleted information may be overwritten.

Step 2. Prevent Access to Network

Turn off phone (We will cover this on next slides)

- Pull the battery?
- Turn off normally?

Use radio frequency blocking container/fabric. (Faraday)

Leave phone on, but turn off receiver
(e.g. Airplane mode)
Not available on all phones.

Use a radio signal "jamming" device with small radius.

- Illegal at this time.
  Only Federal Law Enforcement may use.

Contact provider to have phone taken off network.

- Can you rely on it?

Issues With Turning Phone Off…

- Turning the phone off will engage password protection (such as a keyboard lock or SIM PIN) if enabled by the user. If the examiner needs to power on the phone for examination, they will need a way to bypass this security.
  - If phone is turned off by pulling the battery, information stored on the phone may be lost, and/or the phone's date/time could be reset.
    (Battery access is hindered on some phones.)
  - If phone is turned off by normal means, phone will "de-register" from provider's network, changing location information stored with provider.

Radio Frequency Blocking

Known as “Faraday” Devices

- RF blocking fabrics
- Commercial Faraday bags
- Commercial Faraday tents
- RF shielded boxes
- Other Methods:
  Arson Can
  RF blocking paints
  etc…

Radio Frequency Blocking

WARNING:

Phones that have been blocked from connecting to a network will boost power output trying to obtain a radio signal. These phones will drain battery power much faster than normal.

If you leave a seized phone on, and block its connection to the cellular network, it is important to put the phone on a battery charger.

Be careful that the battery charger does not function as an antenna, and carry signal from the provider to the phone.

Radio Frequency Blocking

Specifications

- What frequency ranges can be blocked?
- WiFi: 2.4GHz, 3.6GHz, 5GHz (IEEE 802.11)
- Bluetooth: 2.4GHz – 2.5GHz
- Cell: 800/900MHz, 1700/1800/1900MHz

Did you test and validate on a wide range of devices in different conditions?

- Remember to re-test often, as some devices wear over time or develop small flaws.

Step 3. Ask For Information

Is there a PIN, password, or other security codes to access/operate the phone?

What is the phone number of the phone?

Whose phone is it?

Who is the network provider (e.g. Sprint, Verizon, T-Mobile, AT&T)?

Was the phone connected to a computer?

Step 4. Seize Related Hardware/Software

Where is the charger?

Is there a data cable?

Was the phone ever connected to a computer?

Are there software disks?

Any other SIM cards?

Any old handsets?

Is there loose removable media for the phone?

Step 4. Seize Related Hardware/Software

Storage media adapters and SIM card readers

Some adapters will have internal storage capacity.

- **Do <u>not</u> use the card reader seized at a crime scene, to avoid compromising evidence stored in the reader's internal memory.**

Step 4. Seize Related Hardware/Software

The presence of phone modification hardware, such as “flash boxes” and loose mobile phone components may indicate an advanced user or hacker.

You may wish to seize these devices as well as the computer, as they may have been used to create flash dumps of data in a phone’s memory.

Step 5. Seize Related Documentation

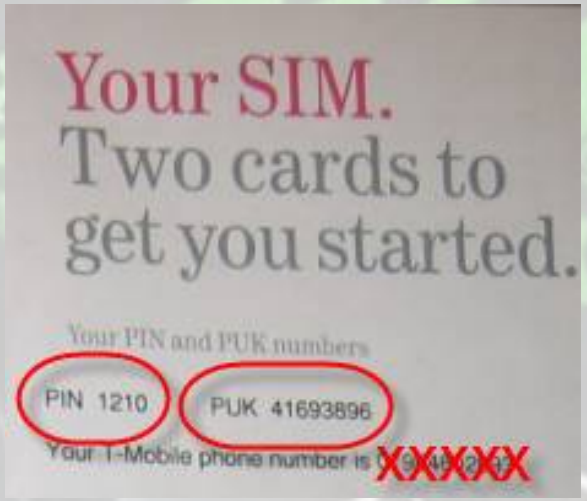
Is there a recent phone bill for the phone?

Where is the original packaging for the phone?

Is there SIM packaging?

Is there a user manual for the phone?

- What can this phone do? Take pictures? Record Video? Play music?



Step 6. Transportation and Storage

- Package and transport appropriately.
- Maintain chain of custody.
- Store securely. Continue to block phone from connecting to a cellular network while in storage.
- Plug in the phone while in storage, if stored with the power on or with the battery inside the phone.
  - Dead battery may reset date/time to mfg default. Example: Nokia will reset to 00-00-00-00:00:00
- Follow all procedures for proper evidence handling, as per your agency guidelines.

Step 6. Transportation and Storage

Some identifying numbers may not be available to you. Why?

- Obliterated by suspect.
- Written under battery and you do not want to power-off.
- First responder typically will not be disassembling the phone.

Step 7. Analyzing The mobile device

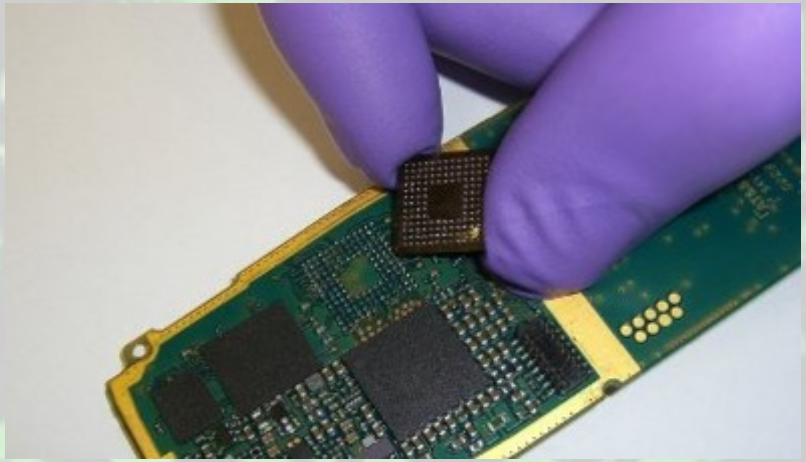
Find a trained examiner to perform a forensic analysis of the phone.

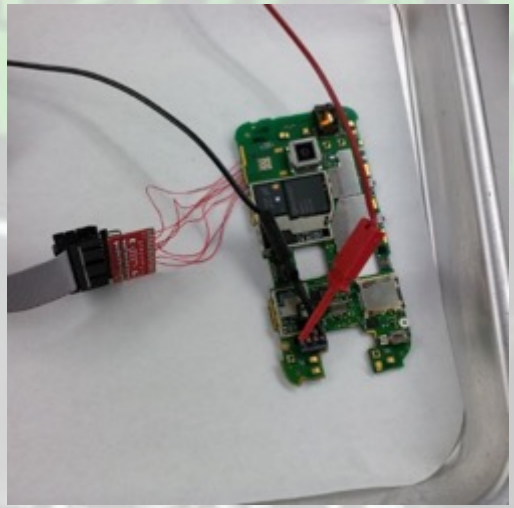
An expert examiner should have experience in all of the three methods of examining cellular phones.

- Scroll Analysis
- Logical Analysis
- Physical Analysis (Chip-off, JTAG)

Step 7. Analyzing The Mobile Device

- Scroll Analysis of Phone
  - Manually scanning through the phone. Will not show deleted data.
  - Navigate menus and capture data by photographing or taking video of each screen.
  - Using a recording method such as “Project-a-phone.”
- Logical Analysis of Phone (i.e. XRY or Cellebrite)
  - Typically does not capture deleted data.
  - May not support all data types on all phones (e.g. calendar)
  - Need multiple packages to capture all data.
- Physical Analysis/Flash of Phone Memory
  - Requires user to capture phone’s memory into “flash file.”
  - JTAG- Joint Test Action Group
  - Chip-off Forensics (produces binary dump that needs decode
  - Interpret and decode binary file, if possible, which may reveal deleted data.





First Responder
Mobile Phone Seizure Flowchart

The phone is evidence:
- Secure the phone
- Do not allow anyone to operate
- Do not navigate the menu or open any messages at this time
- Document all information visible on the current screen

Document all actions taken

Phone Power Status

ON

Block Phone From Network

Select a Method

- RF Blocking:
  - Faraday Bag
  - RF Nylon mesh fabric
- Turn off receiver:
  - "Airplane Mode"
  - Contact Network Provider
- Cell frequency "jammer" (*if legal*)

OFF

Leave Phone Off

Turn Phone Off

CAUTION May engage phone lock

Pull Battery

Normal Shutdown

Document all actions:
- Ask questions:
  - What is the PIN/PUK
  - Who is the service provider
  - What is the phone number
- Seize all related material:
  - *SIM and memory cards
  - Phone bills
  - Software and cable
- Computer may be potential evidence if mobile was ever connected.
- Package all items carefully and transport to a qualified mobile phone examiner

This flow chart is provided as a general guide for "best practices" in seizing mobile phones. It is not intended to replace agency guidelines or policy.

North America
P.O. Box 205
Warrington, PA 18976-0205
Tel: 888.781.7178
Fax: 215.491.3670
info@BKForensics.com

Visit www.BKForenscis for additional information on cell phone forensics

BKForensics Europe
Ninaberlaan 83
7447 AC Hellendoorn
The Netherlands
Tel: +31 548 659066
Fax +31 548 659 010
europe@BKForensics.eu

Mobile Device Forensics (An Introduction)

Josh Brunty,
CCME, CCO, CCPA, CHFI, MPSC, ACE
Assistant Professor
Marshall University