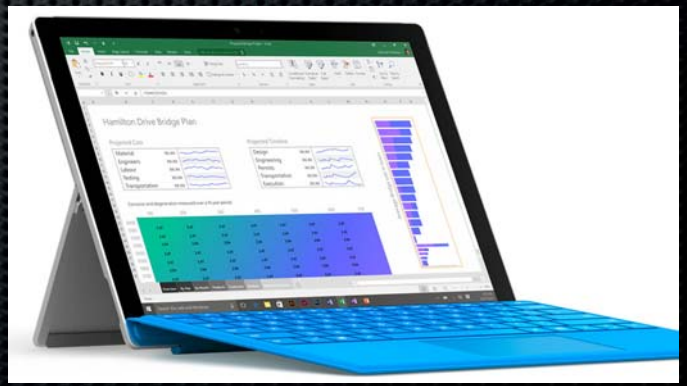
Cybercrime & Investigative Technologies Section

F/Sgt. Brian Bunner
bbunner@isp.in.gov



Cyber Crime Investigation

- Crimes where computers or any digital media was used as an element of the crime
  - Traditional crimes that have “digital evidence”
  - High Tech crimes also have “digital evidence”

Traditional Crime

- BTK Killer-Dennis Rader
  - Gave the news media a floppy disk which contained data that led investigators to his church and eventually the suspect
- Scott Peterson-
  - A few weeks before his pregnant wife, Laci, disappeared, he surfed the Web for information on tides and water currents in the same bay where her body turned up five months later

Traditional Crime

- Indiana Case
  - Infant was killed by boyfriend punching stomach. Google searches of “what happens when infant stomach beaten”

High Tech Crime

- Hacking for Personal Information
  - 2015 Anthem security breach 80 Million accounts
- Military or Terrorist Activities
  - China, North Korea, Russia military hacking

Legal Considerations

- Reasonable Expectation of Privacy
- Consent Searches
- “Control” of computer files
- Plain View
- Employer agreements

Securing Digital Evidence

- There are so many different devices now that can contain digital evidence
  - Computers
  - Digital Cameras
  - Thumb Drives
  - Cell Phones
  - Gaming Systems
  - MP3 Players
  - Refrigerator/Appliances

Memory Cards

Micro SD Memory

Thumb Drives

Mini Thumb Drive

Micro Thumb Drive

Thumb Drives

Thin Thumb Drive

Thumb Drives

Thumb Drives

Bullet 50 Cal
Thumb Drive

Credit Card
Thumb Drive

Thumb Drives

Bracelet
Thumb Drive

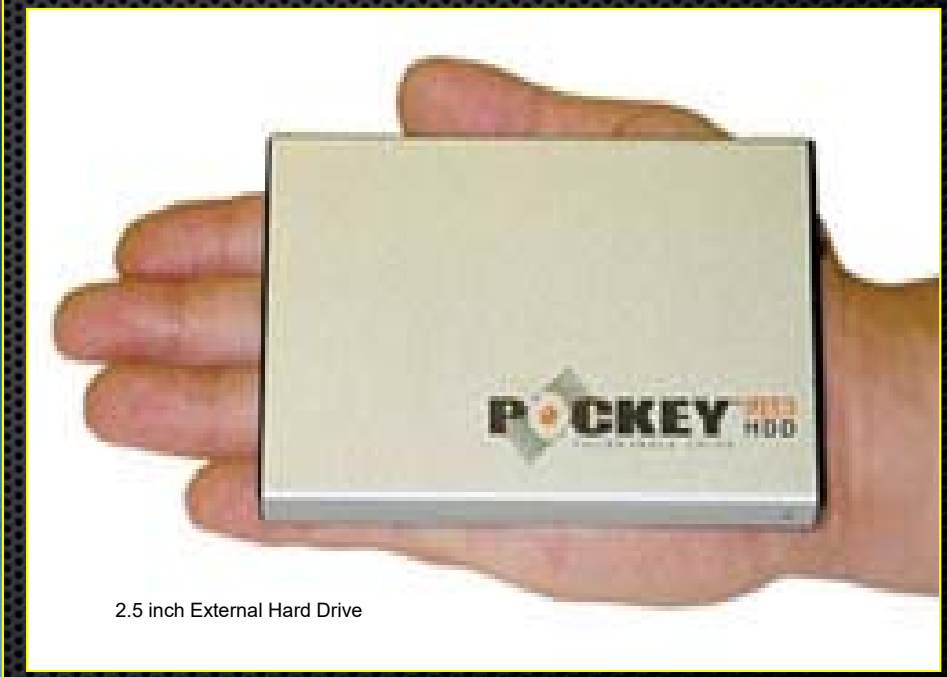
Leggo
Thumb Drive

Thumb Drives

Nike Shoe
Thumb Drive

Poker Chip
Thumb Drive

Swiss Army Pocket Knife
With USB Drive



2.5 inch External Hard Drive


2.2GB
Disk
SMModular
2.2GB
CF+ Type II

Pen with
USB
Thumb Drive

TiVo/Cable Box DVR


VS


NINTENDO DS

Securing A Computer

- Remove any potential suspects from the area
- On/Off Principle
  - If it is off, leave it off
  - If it is on
    - Document and photograph the screen
    - Pull the plug from the back of the computer (not the wall outlet)

Securing A Computer

- Photograph the back of the computer including everything plugged into it
- Note the make, model, and serial number of the computer
- Label according to standard procedures
- Take care during transport to avoid excess bouncing or jarring

Securing A Computer

- Networked computers (such as a business computer) – bring in a specialist, CALL CYBER CRIME UNIT
  - There could be other network computers with important data
  - You could adversely affect the business operation and be held liable

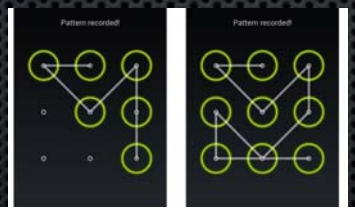
Securing Other Digital Devices

- Generally just “bag and tag” like any other evidence
- Only seize a Laptop power cord, Not a Desktop computer

Cell Phone Forensics Rule #1

GET THE PASSWORD

(or Pattern)



Smartphone Capabilities

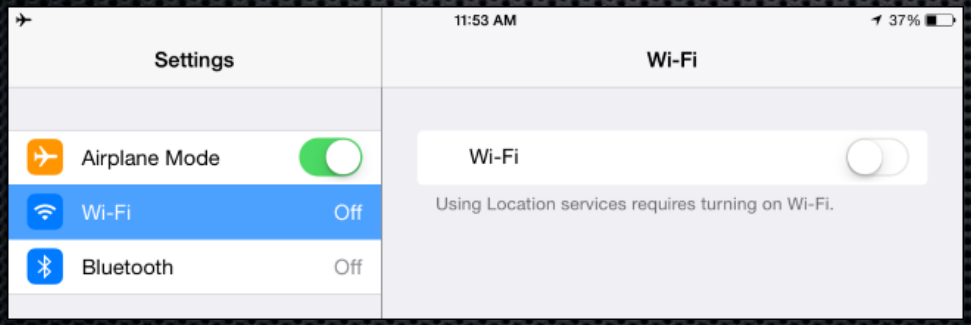
- Phone calls and texting
- Digital camera with video, HD and 4k
- Full internet browsing
- Emailing, Social Networking (Facebook)
- File sharing (Flickr, Picasa, Mobileme)
- Advanced GPS (tracking kids)
- VOIP (via Internet) Skype, Google Voice

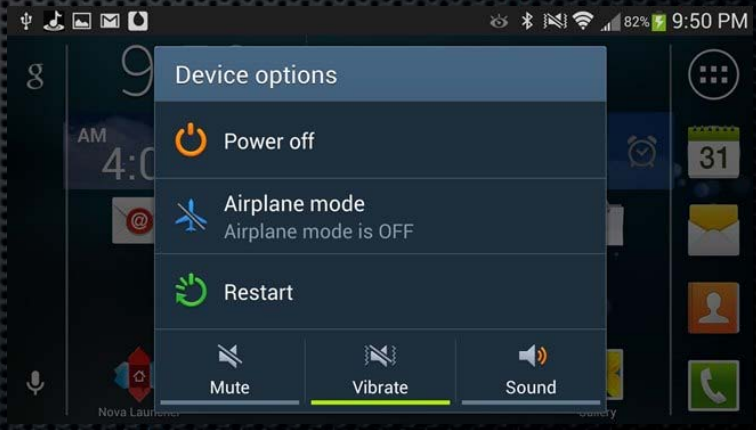
Remote Wiping/Deleting

This is a
BAD DAY

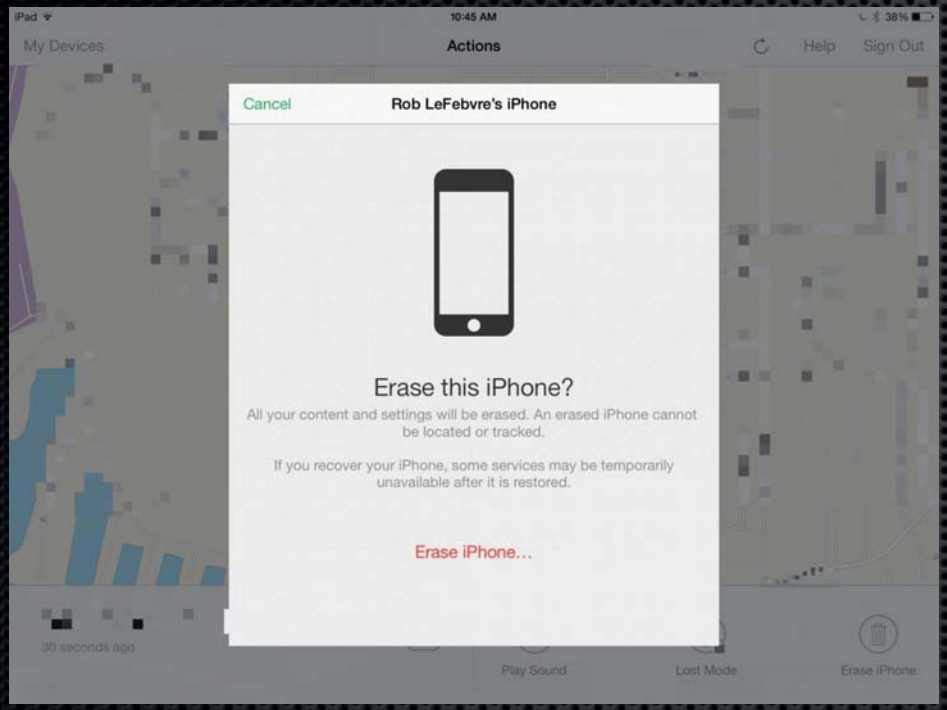
Remote Wiping/Deleting

- Suspect or person helping suspect can send a Remote Wipe signal to the smartphone to delete the contents.
- We highly recommend that when phone is seized by police officer that they put the phone in "Airplane Mode" AND turn the WiFi OFF.
- Apple WIPES ALL data, Androids are getting better at Factory Resetting





Remote Wiping/Deleting



- Suspect uses computer or another smartphone to login to his account and wipe his phone.
- If smartphone is not in “Airplane Mode” or taken off the cellular or WiFi network, wipe command will start.

Remote Wiping/Deleting

Remove device from all networks, then examine

Remote Wiping/Deleting

- No Aluminum foil or paint cans needed
- As long as Airplane Mode turned ON and Phone is turned OFF, remove battery if possible
- Place in regular evidence bag