
CSI
Crime Scene
Investigations
Did Jack do it?
CSI-CRIME SCENE INVESTIGA

Speaker Introductions

- **Amber Schroader**
  - ***Paraben Corporation***
  - ***Oodles of forensic experience***
- **Tyler Cohen**
  - ***Federal Government (Still Cool Person)***
  - ***IPod Obsession***

Case Summary:

CSI-Forensic Process

1. **Evidence Collection**
2. **Evidence Preservation**
3. **Analysis**
4. **Reporting**

What are the different forensics?

iPod

Cell Phone & PDA

Computer Forensics

1. Storage device requiring file system
2. Device is “static”
3. Larger storage capacity
4. Forensic:

   Bit Stream Imaging

Handheld Forensics

1. Embedded systems
2. Device is “active”
3. Smaller on board storage capacity
4. Forensic:

   Active Memory Imaging

CSI-Evidence Collection

- **Check all areas for potential evidence.**
- **Nothing is what it seems…**
- **Always wear gloves!**
  - **Biological evidence is still available.**

Our Evidence

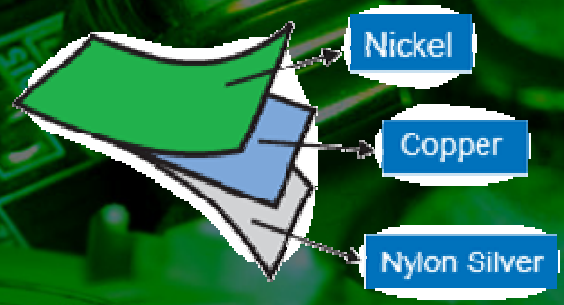
What are potential risks to evidence.

- **Suspect**
  - **Detain Suspect**
- **Friends of Suspect**
  - **Protect Evidence**

CSI-Evidence Collection/Preservation

- **Must maintain proper control of evidence**
- **Faraday Cage all wireless devices**
- **Maintain Power on all devices**

StrongHold Faraday



PURPOSE:	Shielding for wireless device signals
DESCRIPTION:	NI / CU / AG plated, rip stop or plain weave, nylon fabric
SURFACE RESISTIVITY:	0.03 Ohms/• Max ---average >0.02 Ohms/•
SHIELDING EFFECTIVENESS:	Average 80db from 30 Mhz to 1 Ghz
ABRASION RESISTANCE:	1,000,000 Cycles
TEMPURATURE RANGE:	-30°C to 90°C
TOTAL THICKNESS:	.076 mm / .003" nominal

CSI-CRIME SCENE INVESTIGA

StrongHold Faraday Time in a Tent…

Prioritize Your Exam

- **Power Volatile Data First**
  - **PDA**
- **Risk Volatile Data Second**
  - **Cell/Mobile Phone**
- **Static Data Last**
  - **iPod**

The BIG Questions

- **What was Jack Grove was up to?**
- **Who were his accomplices?**
- **Do we have the evidence to prosecute?**
- **What is the verdict?**

The BIG Questions

- **What was Jack Grove was up to?**
  - **Where to start?**
    - **What was last time devices had interaction?**
    - **Were the time stamps consistent with provider records?**
      - **How do you get provider records?**

Last Interaction with Suspect

- **Device Timestamp**
- **Virtual BlackBerry**

Last Interaction with Suspect

- **Device Timestamp**

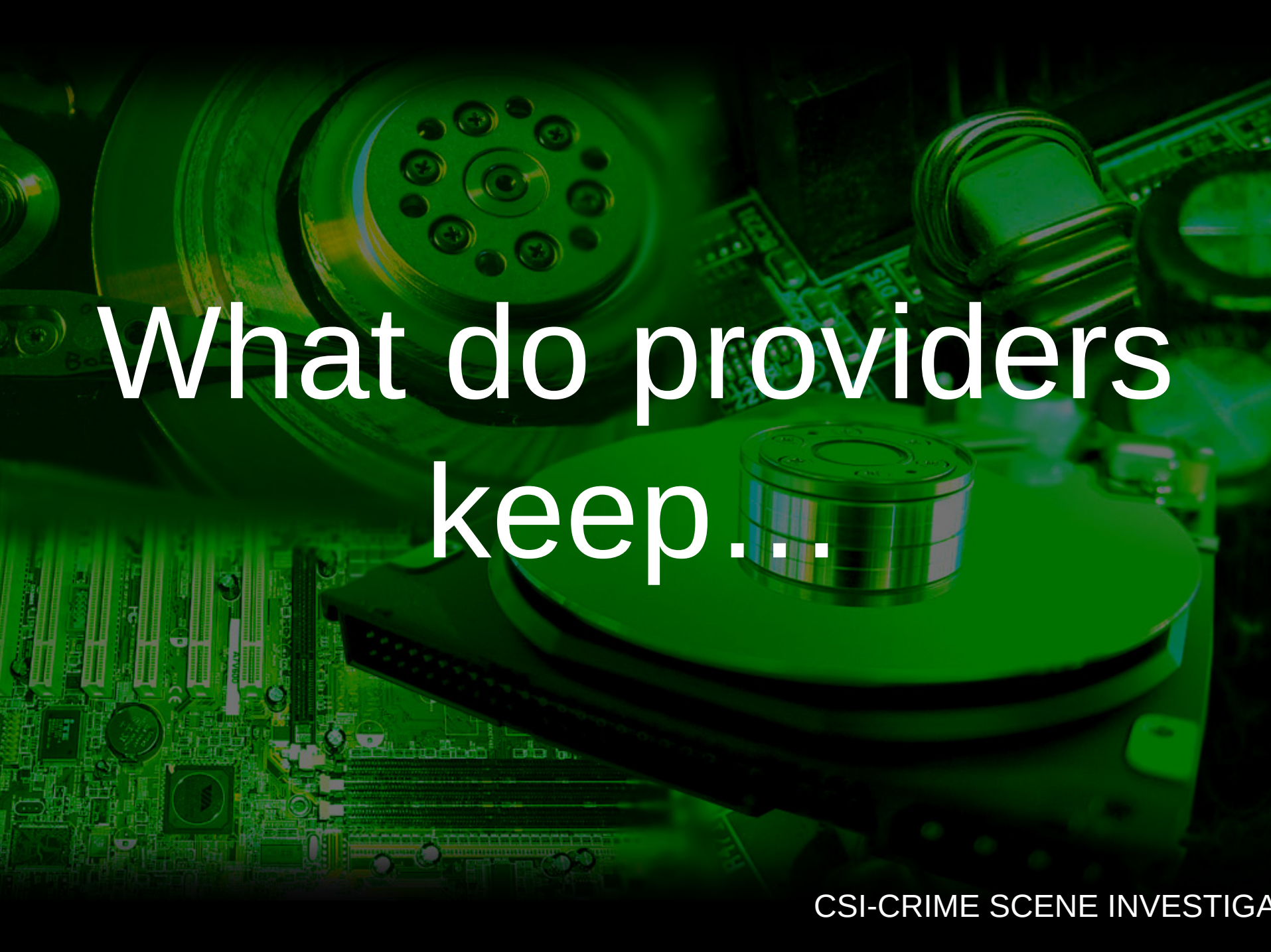
Properties

Name	Value
Model Manufacturer	Nokia
Model Name	Nokia 6101
Model Number	NSE-1
Model Version	05.24
Model Date	05-10-05
Model IMEI	490548309433782
Program timestamp	7/12/2006 1:15:02 PM

Not always conclusive…

Last Interaction with Suspect

- **Device Timestamp**


What do providers keep…

Subscriber Database

- **Subscriber Databases are keep by the cellular networks (with some exceptions and additions depending on the carrier)**
  - **Subscriber name and address**
  - **Billing information**
  - **Telephone Number (MDN – MIN)**
  - **IMSI**
  - **IMEI/ESN**
  - **SIM serial (if applicable – located on card itself)**
  - **PIN/PUK**
  - **Subsidy lock**
  - **Services**

  ***Prepaid services are not required to be identified**

CDRs

- **Call Detail Records are produced every time a customer makes a call or sends a text message.**

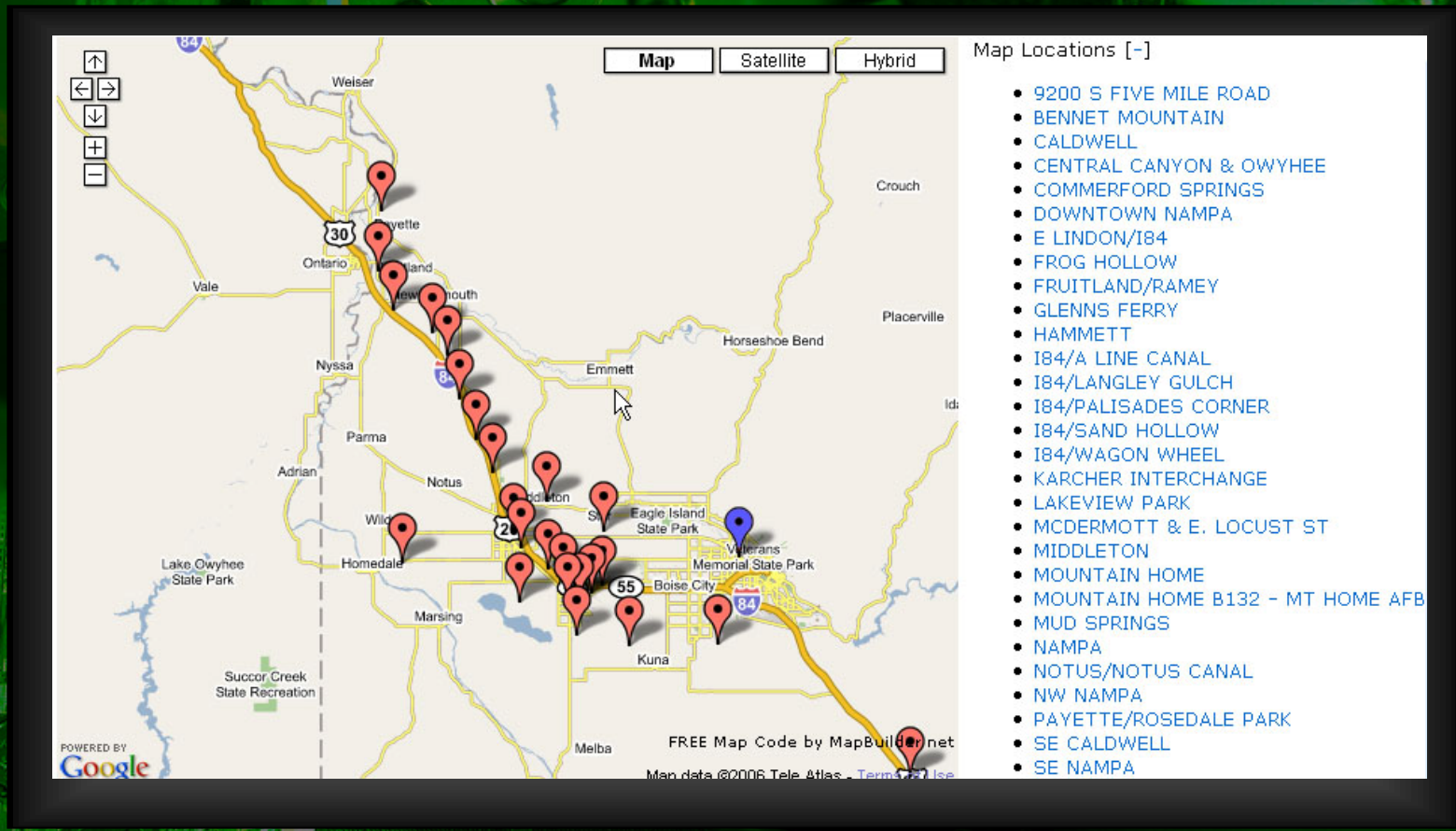
DATA THAT CAN BE OBTAINED

- **Cell Sites utilized (Origination and Termination)**
- **Originating MDN**
- **Termination MDN**
- **Dates and times of calls**
- **Duration of Call**
- **Direction of Call**
- **Switch (Base station) of Origination**

Obtaining Provider Data

- **Methods are dependant as to information you are requesting.**
  - **Letter of Preservation (90 days)**
  - **Subscriber information and billing information – SUBPOENA, 2703(d),SW**
  - **Call History including date and times (Historical) –Subpoena, 2703(d), SW**
  - **Towers, GPS, Live (SMS,MMS,Convo) – 2703(d) or SW**

CDR Applied


Map
Satellite
Hybrid
Weiser
Ontario
Vale
Nyssa
Parma
Adrian
Notus
Homedale
Lake Owyhee State Park
Marsing
Succor Creek State Recreation
Melba
Kuna
Boise City
Eagle Island State Park
Veterans Memorial State Park
Crouch
Placerville
Horseshoe Bend
Emmett
30
84
55
20
POWERED BY Google
FREE Map Code by MapBuilder.net
Map data ©2006 Tele Atlas
Map Locations [-]
9200 S FIVE MILE ROAD
BENNET MOUNTAIN
CALDWELL
CENTRAL CANYON & OWYHEE
COMMERFORD SPRINGS
DOWNTOWN NAMPA
E LINDON/I84
FROG HOLLOW
FRUITLAND/RAMEY
GLENNS FERRY
HAMMETT
I84/A LINE CANAL
I84/LANGLEY GULCH
I84/PALISADES CORNER
I84/SAND HOLLOW
I84/WAGON WHEEL
KARCHER INTERCHANGE
LAKEVIEW PARK
MCDERMOTT & E. LOCUST ST
MIDDLETON
MOUNTAIN HOME
MOUNTAIN HOME B132 - MT HOME AFB
MUD SPRINGS
NAMPA
NOTUS/NOTUS CANAL
NW NAMPA
PAYETTE/ROSEDALE PARK
SE CALDWELL
SE NAMPA

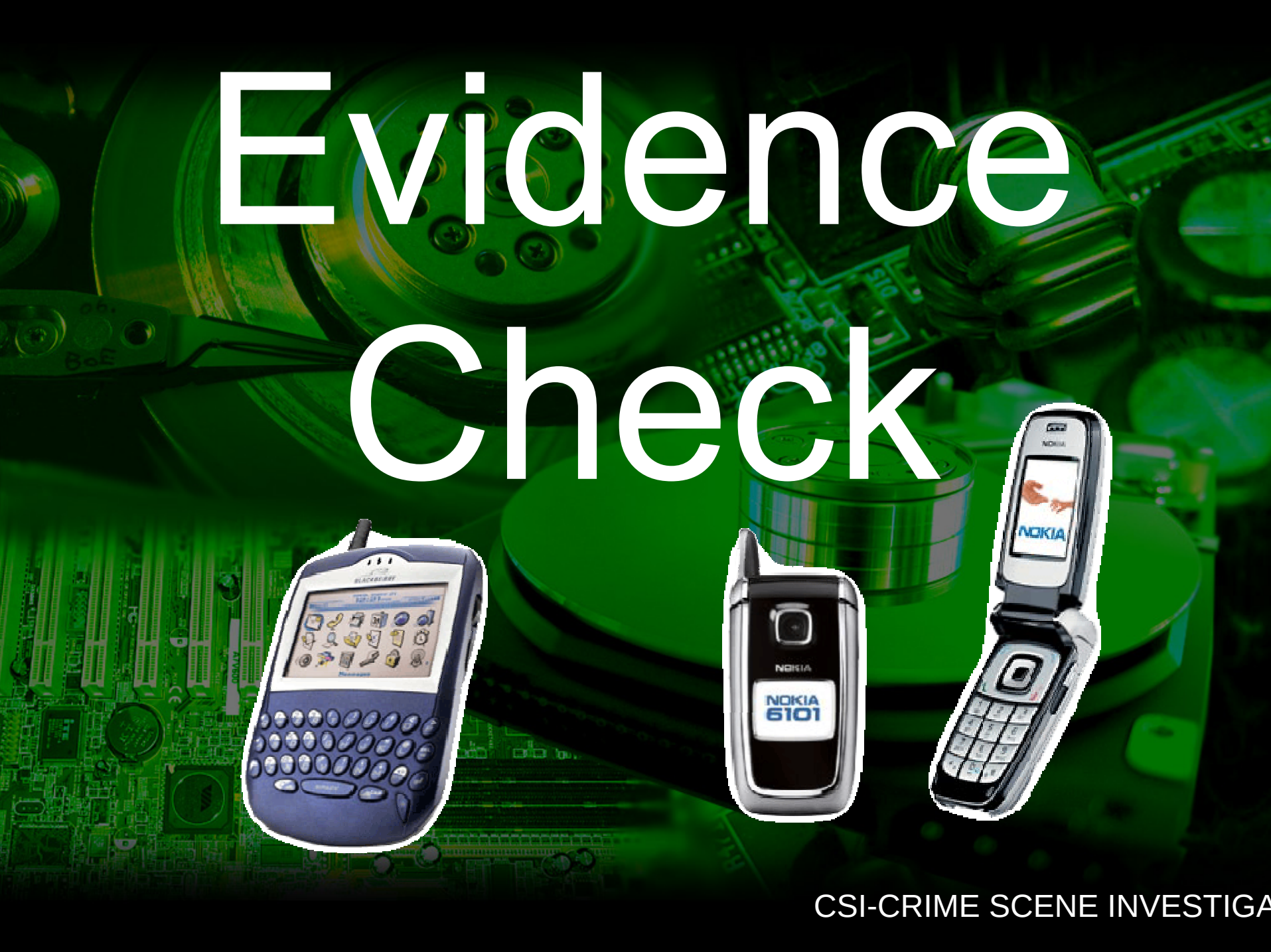
The BIG Questions

- **Who were his accomplices?**
  - **Where to start?**
    - **Address Books**
    - **Text Messages**
    - **Instant Messaging**
    - **E-mail**
    - **Call Records**

The BIG Questions

- **Do we have the evidence to prosecute?**
  - **Where to start?**
    - **Acquisition**
    - **Cross Reference Evidence**
      - **Where do they link together?**

Evidence Check



Evidence Check

CSI-CRIME SCENE INVESTIGA

Types of iPods

- **iPod**
- **iPod Mini**
- **iPod Shuffle**
- **iPod Photo**
- **iPod Nano**
- **iPod Video**

Software

- **Default Software**
  - **iTunes is the default software for controlling your iPod**
- **Other Software**
  - **Anapod is software that can be used to control your iPod but has some added features**
- **Default Software**
  - **Various other software can be found by googling “iPod software”**

File Systems

- **Default File Systems run on the iPod**
  - **HFS+ (Macintosh's Hierarchical File System)**
  - **FAT32 (Microsoft's File Allocation Table)**

- **Alternate File Systems**
  - **FAT16 (Microsoft's File Allocation Table)**
  - **Ext2, Ext3 (Extended File System)**

How This Effects Law Enforcement

- **iPods Can Contain Evidence**
  - **Photos**
  - **Trade Secrets / Espionage**
  - **Hidden Files**
  - **Hacking Tools**
  - **Sky is the Limit**

Podcasting

- **What is a Podcast?**
  - **A Podcast can be either video or audio file that has been pre-recorded and plays on the iPod**

- **How is this relevant to law enforcement?**
  - **Evidence can be hidden in a podcast or be the podcast itself**

Linux Boot CDs and iPod

- **Linux Boot CDs**
  - **Can be used with the iPod.**
  - **Linux Boot CDs leave no trace on HD**
  - **Can create persistent home directory on iPod**
- **Popular boot CDs**
  - **Knoppix STD**
  - **Helix**
  - **Ubuntu**

Hacking Tools on the iPod

- **Hacking tools can be run from the iPod.**
  - **Metasploit**
  - **Exploits**

- **Evidence can be brought back to the iPod for safe keeping.**

Small Linux Distributions

- **Flavors of bootable Linux under or 50mb can run on the iPod**
  - **Damn Small Linux**
  - **Runt**
  - **Puppy**

Response

- **Ways of Imaging the iPod**
  - **Write Blocking Device**
    - **USB Registry Hack**
  - **Linux DCFLDD / DCCIDD**
  - **Forensic Imaging Tools**
    - **Paraben Forensic Replicator**
    - **Encase**
    - **AccessData FTK Imager**

Forensic Tools for Analysis

- **Forensic tools for analyzing iPods**
  - **Brian Carrier's Sleuthkit and Autopsy**
  - **Guidance Software EnCase**
  - **AccessData FTK**
  - **Paraben P2**

Baseline: What is Normal

- **Files typically found on the iPod**
  - **Calendar**
  - **Contacts**
  - **Notes**
  - **iPod_Control**
  - **iPod_Prefs**
  - **iTunes**

What is Not Normal?

- **Mismatched file extensions**
  - **File extensions that don't match the file type**
- **Hidden or improper named Files**
  - **Files named something innocuous**
  - **Suspiciously named files such as "hax0r"**
- **Too many partitions**
  - **iPods with more than 2 partitions could be suspicious**
- **Non-standard file systems**
  - **File systems other than FAT32 or HFS could be suspicious**

Do we have a verdict?

Amber Schroader
amber@paraben.com
&
Tyler Cohen
tylercohen78@gmail.com