Computer and Phone Forensics

Californsics

Califorensics
Don Vilfer, JD, ACE
916-789-1602
Don@Califorensics.com

www.Califorensics.com

Califorensics

WHY DO WE CARE ABOUT FORENSICS?

- Lawyers and Investigators need to be equipped to adequately advise clients or employers.
- You have a duty to prepare your cases for adequate discovery.
- You have a duty to advise your clients/management about their discovery obligations.

INITIAL RESPONSE

- Gather sufficient info to develop a response
- Traditional investigation
- Don't attempt data recovery
- Avoid spoiling the evidence (logs, free space, etc.)
- Consult with someone knowledgeable
- Consider locations of relevant evidence (thumbdrives, router logs, cameras)
- Develop a strategy drawing on your skills and what you will hopefully learn today!

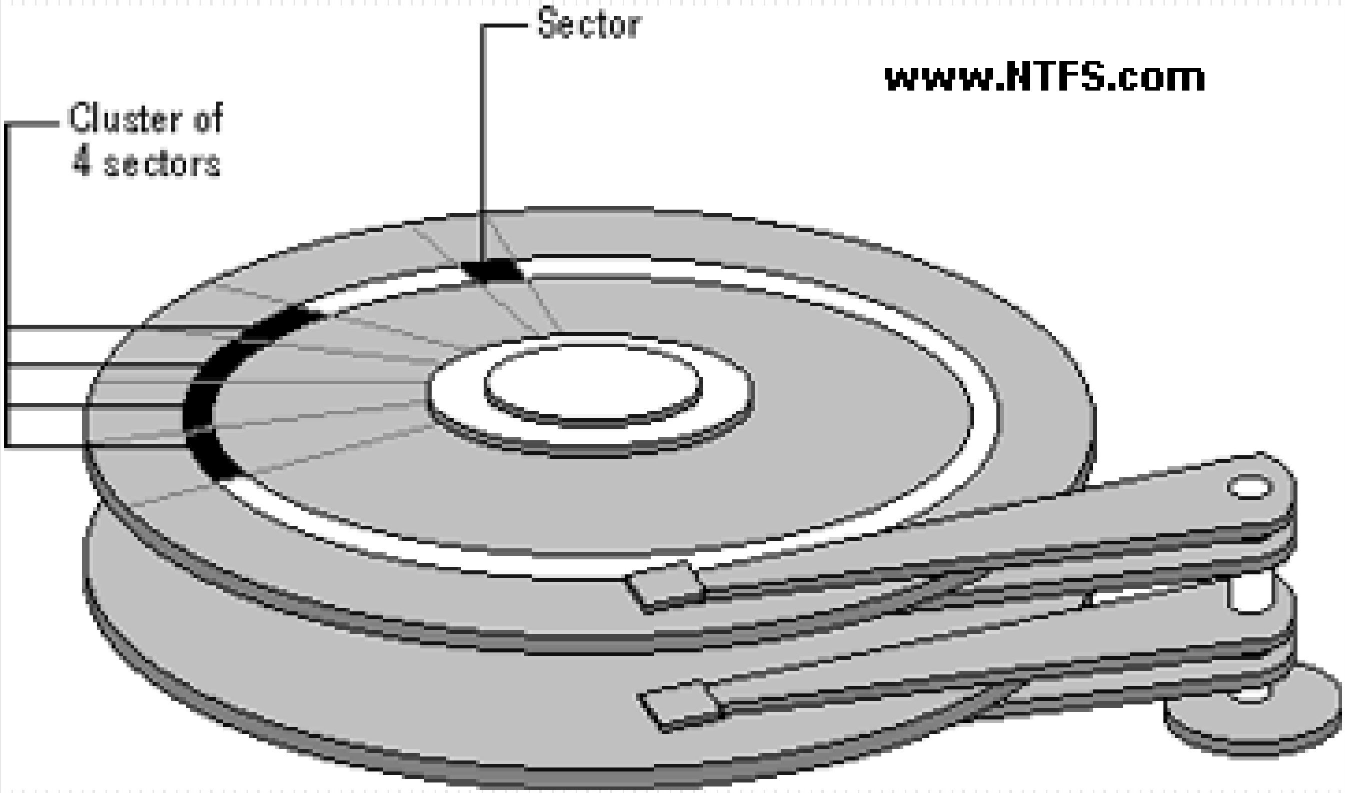
COMPUTER FORENSICS VS. EDISCOVERY

Computer Forensics: the use of specialized techniques for recovery, authentication and analysis of electronically stored data.

Electronic Discovery: the process of locating, searching and securing electronic data to produce as evidence in a legal proceeding.

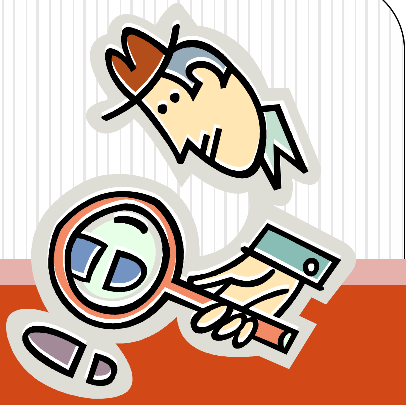
Califorensics

Data Constantly Changes



Califorensics

FORENSIC IMAGE



- The creation of a Forensic Duplicate of the storage media.
- FRE Section 1003: a duplicate is admissible to the same extent as the original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original.

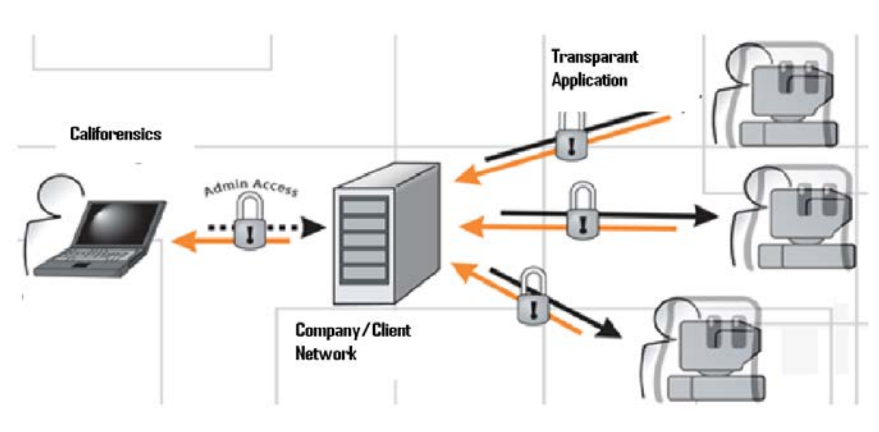
Califorensics

CHARACTERISTICS OF A FORENSIC IMAGE

- Hash Value (Digital Fingerprint)
- Data cannot be changed
- Includes Unallocated Space, Drive Freespace and File Slack
- Difference from Ghost
- Acceptable in court as Best Evidence

FORENSIC IMAGES/DATA ACQUISITION

- Drive Removal and write-blocking
- Live Images
- Boot Disks
- Triage-Live Searching and Acquisition
- Networks-remote imaging (even across the ocean) is possible



Califorensics

BUT, THE USUAL RULES OF EVIDENCE STILL APPLY

- Chain of Custody—must be able to account for the location of the evidence from the moment it was collected.
- Authentication—computer evidence is considered "writings and recordings" under the Rules of Evidence and must be authenticated to be admissible.
- Validation—is it really the same? (Hash files)

Califorensics

WHO WILL DO IT?

- You may want to avoid the in-house IT Professional
- Qualifications: ACE EnCE CFE etc.

FORENSIC PROCESSES (NOW WHAT DO WE DO WITH IT?)

- Review information on the drive
- Recover deleted files.
- Data Carving.
- Searches in free space.
- Recovering web-based e-mail.
- Determining activities on the computer (copying, printing, deleting, burning).
- Break passwords and encryption.

Application to Research Misconduct

- Sources of data.
- Acquiring data from multiple computers and lab equipment.
- Review of Communications (recovery of emails).
- Authenitcating information supplied by the subject of the inquiry.
- Comparison of Digital Images.

PHONES ARE MORE PREVALENT THAN COMPUTERS

Some Statistics

	No. of Phone	% of Pop	Computers
China	1.1B	75%	53M
India	900M	74%	60M
US	327M	104%	223M

WHAT IS RECOVERABLE

- It Depends- dependent on phone OS, model, forensic capabilities
- Email
- Voicemail
- Text Messages
- Location Data- Maps, WiFi, Apps, Photos
- Network Detail

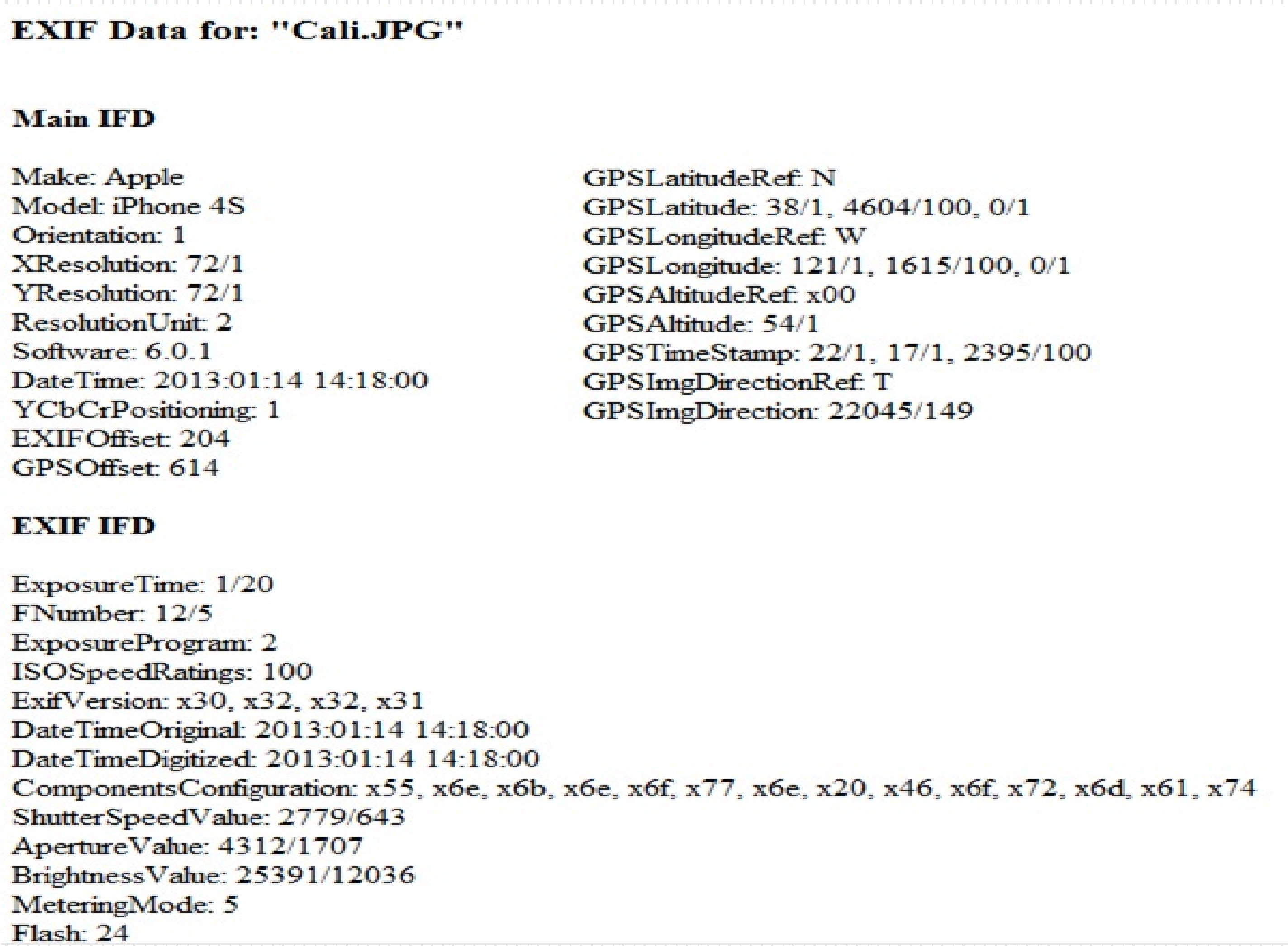
  - local network

  - carrier network (see attached)

Califorensics

Example of Photo Location Data

EXAMPLE OF PHOTO LOCATION DATA



EXIF Data for: "Cali.JPG"

Main IFD

Make: Apple
Model: iPhone 4S
Orientation: 1
XResolution: 72/1
YResolution: 72/1
ResolutionUnit: 2
Software: 6.0.1
DateTime: 2013:01:14 14:18:00
YCbCrPositioning: 1
EXIFOffset: 204
GPSOffset: 614

GPSLatitudeRef: N
GPSLatitude: 38/1, 4604/100, 0/1
GPSLongitudeRef: W
GPSLongitude: 121/1, 1615/100, 0/1
GPSAltitudeRef: x00
GPSAltitude: 54/1
GPSTimeStamp: 22/1, 17/1, 2395/100
GPSImgDirectionRef: T
GPSImgDirection: 22045/149

EXIF IFD

ExposureTime: 1/20
FNumber: 12/5
ExposureProgram: 2
ISOSpeedRatings: 100
ExifVersion: x30, x32, x32, x31
DateTimeOriginal: 2013:01:14 14:18:00
DateTimeDigitized: 2013:01:14 14:18:00
ComponentsConfiguration: x55, x6e, x6b, x6e, x6f, x77, x6e, x20, x46, x6f, x72, x6d, x61, x74
ShutterSpeedValue: 2779/643
ApertureValue: 4312/1707
BrightnessValue: 25391/12036
MeteringMode: 5
Flash: 24

PHONE vs. COMPUTER FORENSICS

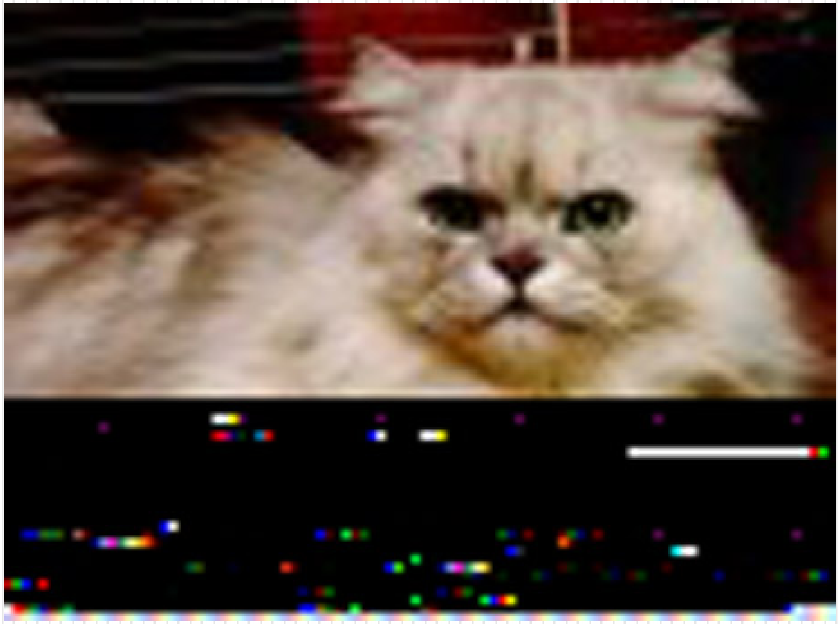
- Flash Storage vs. Disk- wear leveling
- File Systems
- Types of Data
- Security- password, disk wipe, phone encryption

FORENSIC APPROACH’S

- Logical vs. Physical
- SIM
- SD Cards
- Chip Offs
- Backups

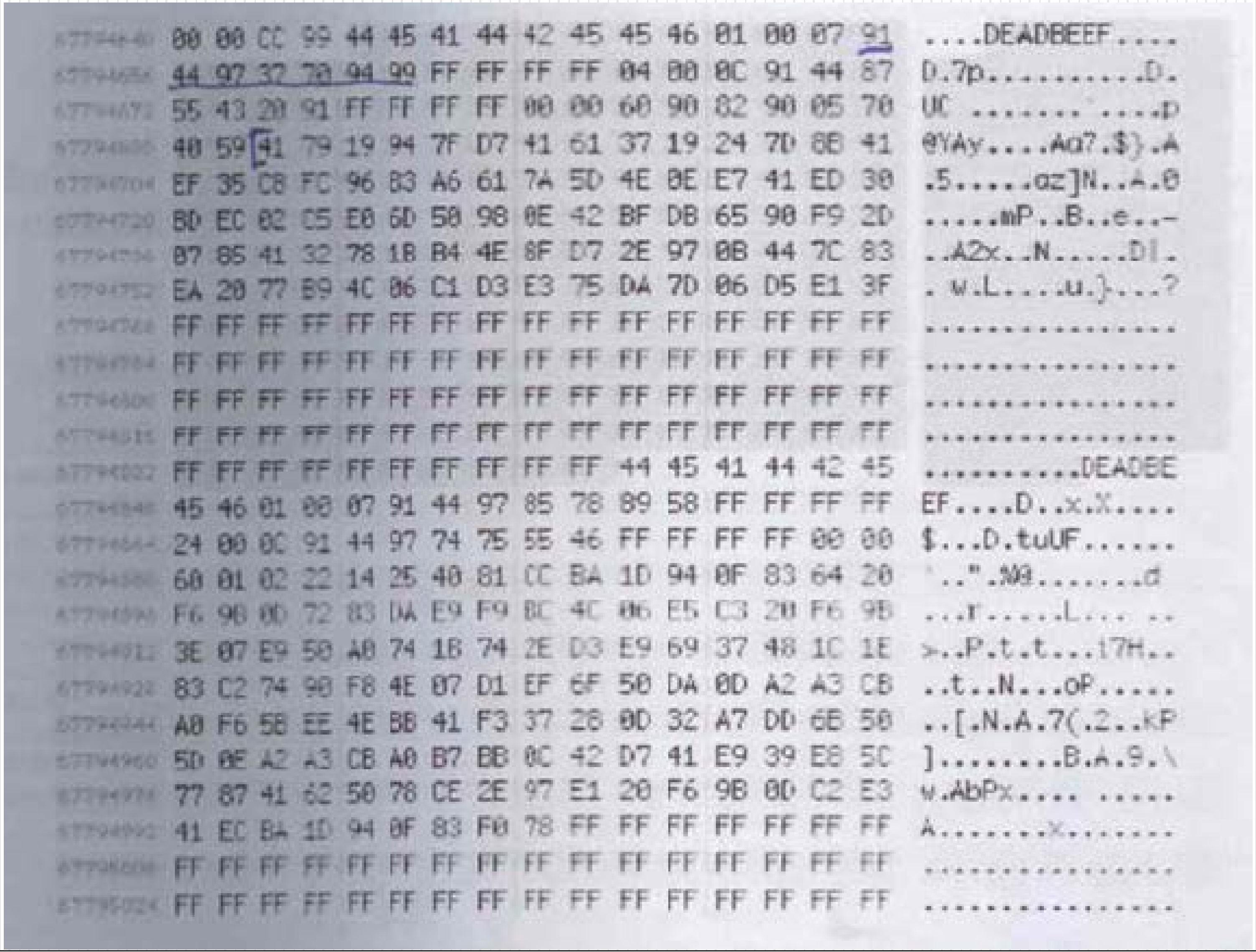
LOGICAL vs. PHYSICAL
DATA CARVING

Data Carved Image



Califorensics

Carved SMS



```
67794640 00 00 CC 99 44 45 41 44 42 45 45 46 01 00 07 91  ....DEADBEEF....
67794656 44 97 37 70 94 99 FF FF FF FF 04 00 0C 91 44 87  D.7p..........D.
67794672 55 43 20 91 FF FF FF FF 00 00 60 90 82 90 05 70  UC ........ ....p
67794688 40 59 41 79 19 94 7F D7 41 61 37 19 24 7D 8B 41  @YAy....Aa7.$}.A
67794704 EF 35 C8 FC 96 83 A6 61 7A 5D 4E 8E E7 41 ED 30  .5......az]N..A.0
67794720 BD EC 02 C5 E0 6D 50 98 0E 42 BF DB 65 90 F9 2D  ......mP..B..e..-
67794736 07 85 41 32 78 18 B4 4E 8F D7 2E 97 0B 44 7C 83  ..A2x..N......D|.
67794752 EA 20 77 E9 4C 06 C1 D3 E3 75 DA 7D 06 D5 E1 3F  . w.L.....u.}...?
67794768 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
67794784 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
67794800 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
67794816 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
67794832 FF FF FF FF FF FF FF FF FF FF 44 45 41 44 42 45  ..........DEADBE
67794848 45 46 01 00 07 91 44 97 85 78 89 58 FF FF FF FF  EF....D..x.X....
67794864 24 00 0C 91 44 97 74 75 55 46 FF FF FF FF 00 00  $...D.tuUF......
67794880 60 01 02 22 14 25 40 81 CC BA 1D 94 0F 83 64 20  `..".%@........d
67794896 F6 98 0D 72 83 DA E9 F9 8C 4C 06 E5 C3 20 F6 9B  ...r.....L... ..
67794912 3E 07 E9 50 A0 74 1B 74 2E D3 E9 69 37 48 1C 1E  >..P.t.t...i7H..
67794928 83 C2 74 90 F8 4E 07 D1 EF 6F 50 DA 0D A2 A3 CB  ..t..N...oP.....
67794944 A0 F6 5B EE 4E BB 41 F3 37 28 0D 32 A7 DD 6B 50  ..[.N.A.7(.2..kP
67794960 5D 0E A2 A3 CB A0 B7 BB 0C 42 D7 41 E9 39 E8 5C  ]........B.A.9.\
67794976 77 87 41 62 50 78 CE 2E 97 E1 20 F6 9B 0D C2 E3  w.AbPx.... .....
67794992 41 EC BA 1D 94 0F 83 F0 78 FF FF FF FF FF FF FF  A........x.......
67795008 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
67795024 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
```

SIM CARDS

Subscriber Identity Module

- Stores Data so the user can be identified on the network
- Can be used to store SMS and contacts
- Portable
- Will contain cell site information
- SIM Clones

SD CARDS

- May contain photos, documents, videos or phone data
- Standard storage media and can be examined as such
- May have data when the phone is inaccessible

Califorensics

CHIP OFFS and JTAG

- When all else fails….

Califorensics

BACKUPS

- Blackberry (ipb)
- i Phone Backup
- Cloud

INITIAL RESPONSE

- Leave It On?
- Passwords
- Faraday Solutions
- Data Cables

You Are Not Paranoid If They Really Are Out To Get You

A Word About Computer Security and Threats

Califorensics

The Costs of Computer Crimes

- Cost is now at over $500 Billion per year (McAfee).
- Average cost to respond and clean up after a successful attack is $1 million (Ponemon Institute).
- Each business is successfully compromised on average twice per week.

Threats from the Inside

- Trade Secret Theft.
- Embarrassment to the Company.
- Embezzlement.
- Blackmail.

Threats from the Outside

- Trade Secret Theft.
- Loss of PII.
- Destruction of data.
- DDOD Attacks.
- Ransomware/Cryptolocker

Threats from the Outside-Solutions

- Trade Secret Theft. (monitor traffic, air gap, disk encryption)
- Loss of PII. (offline, encryption)
- Destruction of data. (backups)
- DDOS Attacks (prepare, communicate, respond and block).
- Ransomware. (expert to decrypt, backups, pay)

Questions?

Califorensics
Don Vilfer, JD, ACE
916-789-1602
Don@Califorensics.com

www.Califorensics.com