


Computer and Phone Forensics

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



www.Calforensics.com

Calforensics

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.

Calforensics

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!

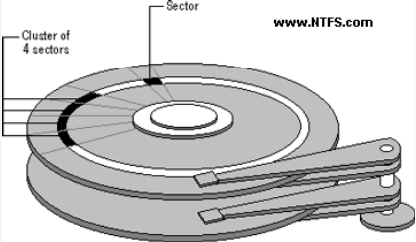
COMPUTER FORENSICS VS. EDISCOVERY

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



The diagram shows a hard drive platter with a central hub and several concentric tracks. A single track is divided into segments labeled 'Sector'. A group of four adjacent sectors is labeled 'Cluster of 4 sectors'. The URL 'www.NTFS.com' is visible in the upper right of the diagram area. The 'Califorensics' logo is at the bottom right.

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

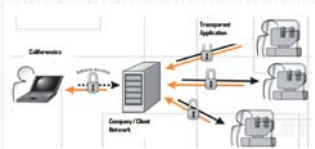
CHARACTERISTICS OF A FORENSIC IMAGE

- 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

Califorensics

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

PRESERVING THE ORIGINAL EVIDENCE FOR EXAMINATION

i.e., To Shutdown Or Not To Shutdown

- RAM-volatile data. Now capable of being forensically captured! Leave computer on if you suspect recent monkey business.
- Hard Drive-reasons to not leave computer on or access files. The evidence changes simply by booting.

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)

Calforensics

WHO WILL DO IT?

- Avoid your client’s IT Professional
- Qualifications: ACE EnCE CFE etc.



Calforensics

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.

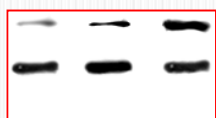
Calforensics

Application to Research Misconduct

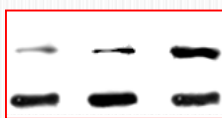
- Sources of data.
- Acquiring data from multiple computers and lab equipment.
- Review of Communications (recovery of emails).
- Authenticating information supplied by the subject of the inquiry.
- Comparison of Digital Images.

Calforensics

ORI Color Overlay of Two Data Sets



Data Set 1



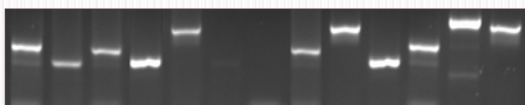
Data Set 2



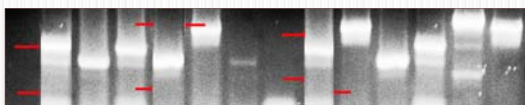
Data Set 2 Over Data Set 1

Calforensics

Adjustments to Bring Out Detail



Original



Equalized

Calforensics

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

Calforensics

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)

Calforensics

Example of Photo Location Data



Calforensics

EXAMPLE OF PHOTO LOCATION DATA

EXIF Data for "Call.JPG"

Main IFD

Make: Apple	GPSLatitudeRef: N
Model: iPhone4S	GPSLatitude: 38.7, 4604/100, 0/1
Orientation: 1	GPSLongitudeRef: W
XResolution: 72/1	GPSLongitude: 121.1, 1615/100, 0/1
YResolution: 72/1	GPSAltitudeRef: s00
ResolutionUnit: 2	GPSAltitude: 54/1
Software: 6.0.1	GPSTimeStamp: 22/1, 17/1, 2395/100
DateTime: 2013:01:14 14:18:00	GPSImgDirectionRef: T
YCbCrPositioning: 1	GPSImgDirection: 22045/149
EXIFOffset: 204	
GPSOffset: 614	

EXIF IFD

ExposureTime: 1/20
FNumber: 12.5
ExposureProgram: 2
ISOSpeedRatings: 100
ExifVersion: s30, s32, s32, s31
DateTimeOriginal: 2013:01:14 14:18:00
DateTimeDigitized: 2013:01:14 14:18:00
ComponentsConfiguration: s55, s6e, s6b, s6e, s6f, s77, s6e, s20, s46, s6f, s72, s6d, s61, s74
ShutterSpeedValue: 2779/643
ApertureValue: 4312/1707
BrightnessValue: 25391/12036
MeteringMode: 5
Flash: 24

Calforensics



Even a Missed Call may be Relevant

Calforensics

PHONE vs. COMPUTER FORENSICS

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

Calforensics

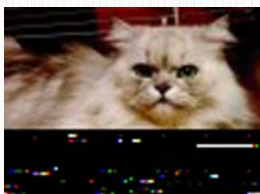
FORENSIC APPROACH'S

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

Calforensics

LOGICAL vs. PHYSICAL DATA CARVING

Data Carved
Image



Calforensics

Carved SMS

```
00 00 CC 20 44 45 41 44 42 45 45 46 01 00 07 21 .....DEADBEF...
44 92 32 70 94 20 FF FF FF FF 04 00 0C 91 44 07 0,7D.....D.
55 43 20 91 FF FF FF FF 00 00 60 90 02 90 05 78 UC.....d
48 59 14 79 19 34 7F 07 41 61 37 19 24 7D 0E 41 @!Ay....A07.$).A
E7 35 C8 FC 96 03 A0 61 7A 5D 4E 0E E7 41 ED 38 .5.....02}B..A.B
00 E0 6C 05 00 58 50 50 0E 4C BF 58 65 90 F9 20 .....wP..B..e..-
07 05 41 52 78 18 04 4E 0F 02 ZE 97 00 44 7C 03 .AD..N.....D..
5A 28 77 89 4C 06 C1 E3 E3 7D 04 70 06 05 E1 3F .wL.....U)...?
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
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

Calforensics

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

Calforensics

CHIP OFFS

- When all else fails....



Calforensics

BACKUPS

- Blackberry (ipb)
- i Phone Backup
- Cloud

Calforensics

INITIAL RESPONSE

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

Calforensics

LIVE FORENSICS DEMO

- What's on Your Phone (or mine)

Calforensics

Questions?

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