

An aerial photograph of the University of California campus, featuring the prominent Sather Tower (Cathedral of Learning) in the center. The foreground is filled with lush green trees, while the background shows a dense urban landscape under a hazy sky. The text is overlaid on the upper portion of the image.

University of California  
2019 Ethics, Compliance and Audit  
Symposium

**REACHING NEW HEIGHTS**



# Computer and Cell Phone Evidence Preservation for Investigations

Don Vilfer, JD  
Digital Evidence Ventures

# Digital Evidence Ventures



**Who we are:** Reformed lawyers, former FBI Agents, assisted by young Brainiacs.

**What we do:** Computer Forensics, Cell Phone Forensics, Research Misconduct Investigations, Fraud Investigations.

# Class Objectives

- Understand the importance of forensic acquisitions.
- Learn the assorted methods of acquiring electronic evidence.
- Understand what evidence can be had from devices.
- Know when to do it yourself and when to engage an expert.

# 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.

# 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

# 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.

# 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)



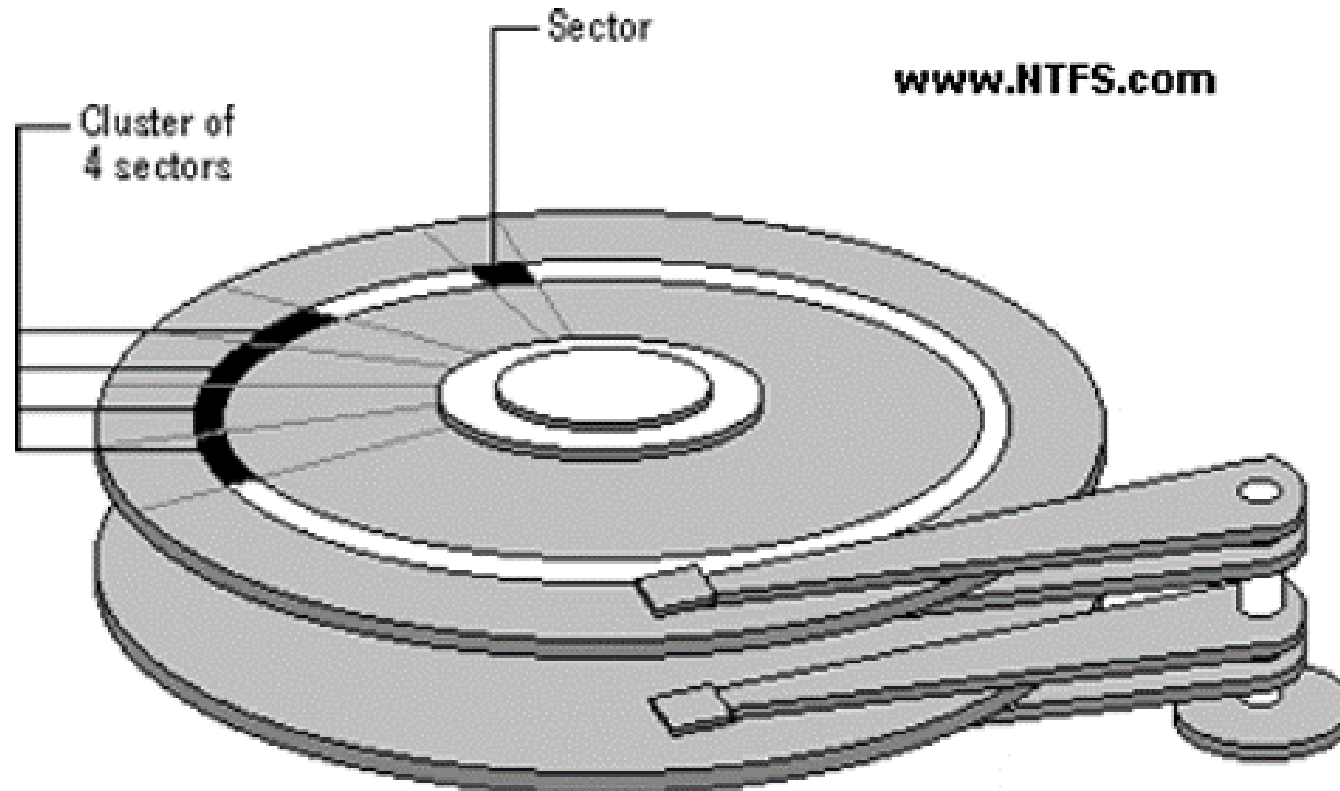
# Paper Evidence of Electronic Data?

[State v. Kolanowski](#), (Wash: Court of Appeals, January 30, 2017). In a case involving the failure to authenticate social media evidence, a criminal defendant unsuccessfully sought to admit a screenshot of Facebook evidence that he maintained would have served as critical impeachment of the prosecutions' main witness. The State successfully argued the screenshot lacked foundation. Metadata that could have been obtained during the collection was not obtained—a simple screenshot did not suffice.

# INITIAL RESPONSE

- Gather sufficient info to develop a response
- Traditional investigation
- Don't attempt data recovery with non-forensic tools
- 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!

# Show me the Data!



# 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

# Drive Removal and Write-Blocking

- Using a physical device to prevent change to the evidence while acquiring a forensic image
- Benefits and Drawbacks



# Live Images

Good for:

- When you cannot shut down the computer/server.
- Encrypted drive.
- Multiple computers.
- When a smear is OK.
- Drawbacks.

# Boot Disks

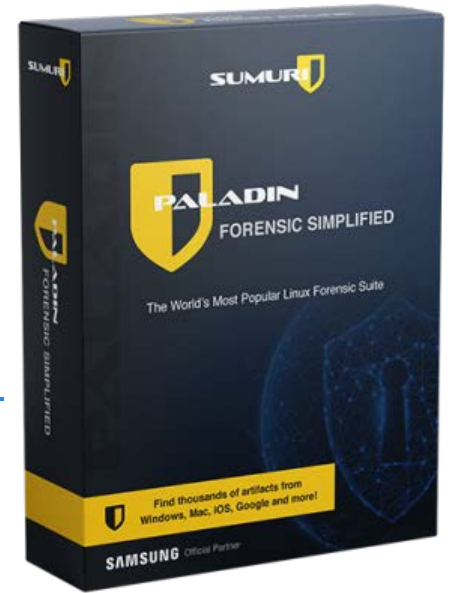
Typically a disk with its own Linux Operating System.

Free (or nearly so) options!

Other tools are included.

Windows FE <https://www.forensicfocus.com/windows-forensic-environment-boot-cd>

[www.sumuri.com](http://www.sumuri.com)



# Triage and Live Searching

Oxford Dictionary: (in medical use) the assignment of degrees of urgency to wounds or illnesses to decide the order of treatment of a large number of patients or casualties

Helpful for many devices or privacy concerns

Relatively recent development

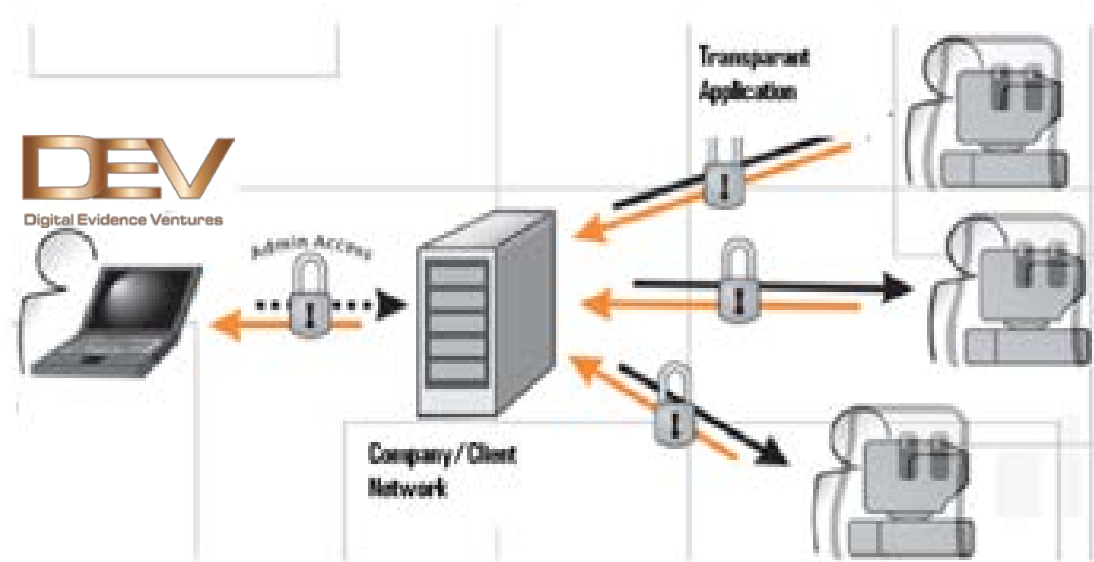
Used by Law Enforcement including Customs





# NETWORK ACQUISITION

- Technique can be used locally or across the internet
- Admin access required
- Good for covert review
- Napa case example
- Tools: FTK Enterprise, F-Response, Hardware
- FTK Imager work-around



# FTK Imager Workflow

AccessData FTK Imager 4.2.0.13

- File
- View
- Mode
- Help
- Add Evidence Item...
- Add All Attached Devices
- Image Mounting...
- Remove Evidence Item
- Remove All Evidence Items
- Create Disk Image...
- Export Disk Image...
- Export Logical Image (AD1)...
- Add to Custom Content Image (AD1)
- Create Custom Content Image (AD1)...
- Decrypt AD1 image...
- Verify Drive/Image...
- Capture Memory...
- Obtain Protected Files...
- Detect EFS Encryption
- Export Files...
- Export File Hash List...
- Export Directory Listing...
- Exit

File List

Name	Size	Type	Date Modified
------	------	------	---------------

Custom Content Sources

Evidence:File System|Path|File Options

# FTK Imager Workflow

The screenshot displays the AccessData FTK Imager 4.2.0.13 application window. The main interface includes a menu bar (File, View, Mode, Help), a toolbar, and a File List pane with columns for Name, Size, Type, and Date Modified. A 'Select Source' dialog box is open in the center, prompting the user to choose an evidence type. The dialog contains the following options:

- Physical Drive
- Logical Drive
- Image File
- Contents of a Folder  
(logical file-level analysis only; excludes deleted, unallocated, etc.)
- Femico Device (multiple CD/DVD)

At the bottom of the dialog, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'. The 'Next >' button is highlighted with a blue border. In the bottom-left corner of the application window, there is a status bar that reads 'For User Guide, press F1'.

# FTK Imager Workflow

The screenshot displays the AccessData FTK Imager 4.2.0.13 application window. The main interface includes a menu bar (File, View, Mode, Help), a toolbar, and a File List pane with columns for Name, Size, Type, and Date Modified. Two dialog boxes are open:

- Create Image**: This dialog box is centered on the screen. It features an "Image Source" field containing the text "\\.\PHYSICALDRIVE2". Below this is a "Starting Evidence Number" field with the value "1". The "Image Destination(s)" field is currently empty. At the bottom of the dialog, there are three buttons: "Add...", "Edit...", and "Remove", followed by an "Add Overflow Location" button. Below these buttons are two checked checkboxes: "Verify images after they are created" and "Precalculate Progress Statistics", and one unchecked checkbox: "Create directory listings of all files in the image after they are created". At the very bottom are "Start" and "Cancel" buttons.
- Select Image Type**: This dialog box is positioned to the right of the "Create Image" dialog. It contains the text "Please Select the Destination Image Type" and a list of radio button options: "Raw (dd)" (which is selected), "SMART", "E01", and "AFF". At the bottom of the dialog are four buttons: "< Back", "Next >", "Cancel", and "Help".

The bottom of the application window shows a status bar with the text "For User Guide, press F1" and a "NUM" indicator.

# FTK Imager Workflow

The screenshot displays the AccessData FTK Imager 4.2.0.13 application window. The main interface includes a menu bar (File, View, Mode, Help), a toolbar, and a 'File List' pane with columns for Name, Size, Type, and Date Modified. Two dialog boxes are open:

- Create Image:** This dialog is used to configure the imaging process. It features an 'Image Source' field containing '\\.\PHYSICALDRIVE2', a 'Starting Evidence Number' field set to 1, and an empty 'Image Destination(s)' list. Below the list are 'Add...', 'Edit...', and 'Remove' buttons, along with an 'Add Overflow Location' button. At the bottom, there are checkboxes for 'Verify images after they are created' (checked), 'Precalculate Progress Statistics' (checked), and 'Create directory listings of all files in the image after they are created' (unchecked). 'Start' and 'Cancel' buttons are also present.
- Evidence Item Information:** This dialog is used to enter metadata for the evidence item. It contains text input fields for 'Case Number:', 'Evidence Number:', 'Unique Description:', 'Examiner:', and 'Notes:'. At the bottom, there are '< Back', 'Next >', 'Cancel', and 'Help' buttons.

The 'Custom Content Sources' pane on the left shows a list of sources with the entry 'Evidence:File System|Path|File' and an 'Options' button. The status bar at the bottom indicates 'For User Guide, press F1' and a 'NUM' indicator.

# FTK Imager Workflow

The screenshot displays the AccessData FTK Imager 4.2.0.13 interface. The main window shows a menu bar (File, View, Mode, Help) and a toolbar. On the left, there is an 'Evidence Tree' pane and a 'Custom Content Sources' pane. The central area is a 'File List' table with columns for Name, Size, Type, and Date Modified. Two dialog boxes are open:

- Create Image**: Shows 'Image Source' as '\\.\PHYSICALDRIVE2' and 'Starting Evidence Number' as 1. It includes buttons for 'Add...', 'Edit...', and 'Remove', along with an 'Add Overflow Location' button. Checkboxes for 'Verify images after they are created' and 'Precalculate Progress Statistics' are checked. There are 'Start' and 'Cancel' buttons at the bottom.
- Select Image Destination**: Shows an empty 'Image Destination Folder' field with a 'Browse' button. The 'Image Filename (Excluding Extension)' field is also empty. 'Image Fragment Size (MB)' is set to 1500. 'Compression' is set to 6. 'Use AD Encryption' is unchecked. Buttons for '< Back', 'Finish', 'Cancel', and 'Help' are at the bottom.

At the bottom left, a footer reads 'For User Guide, press F1'. At the bottom right, a system tray icon shows 'NUM'.

# 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.

# Benefits of Incorporating Cell Phones into Your Investigation

- No longer is it a “he said, she said”
- Establish communication between subjects/witnesses-example
- Provide location during key times
- Prove misconduct (harassment, relationships, use of time, theft)
- Can contain irrefutable evidence
- Many times the evidence is in their own words
- There is often evidence available that cannot be had elsewhere
- Cell Phone data might inform other aspects of the inquiry or develop leads



# Sources of Phone Data

- The phone itself
- Local Backups-not just backing up iTunes
- The cloud-oh, forgot about the cloud
- Service Provider-limitations, but also data that is not available elsewhere

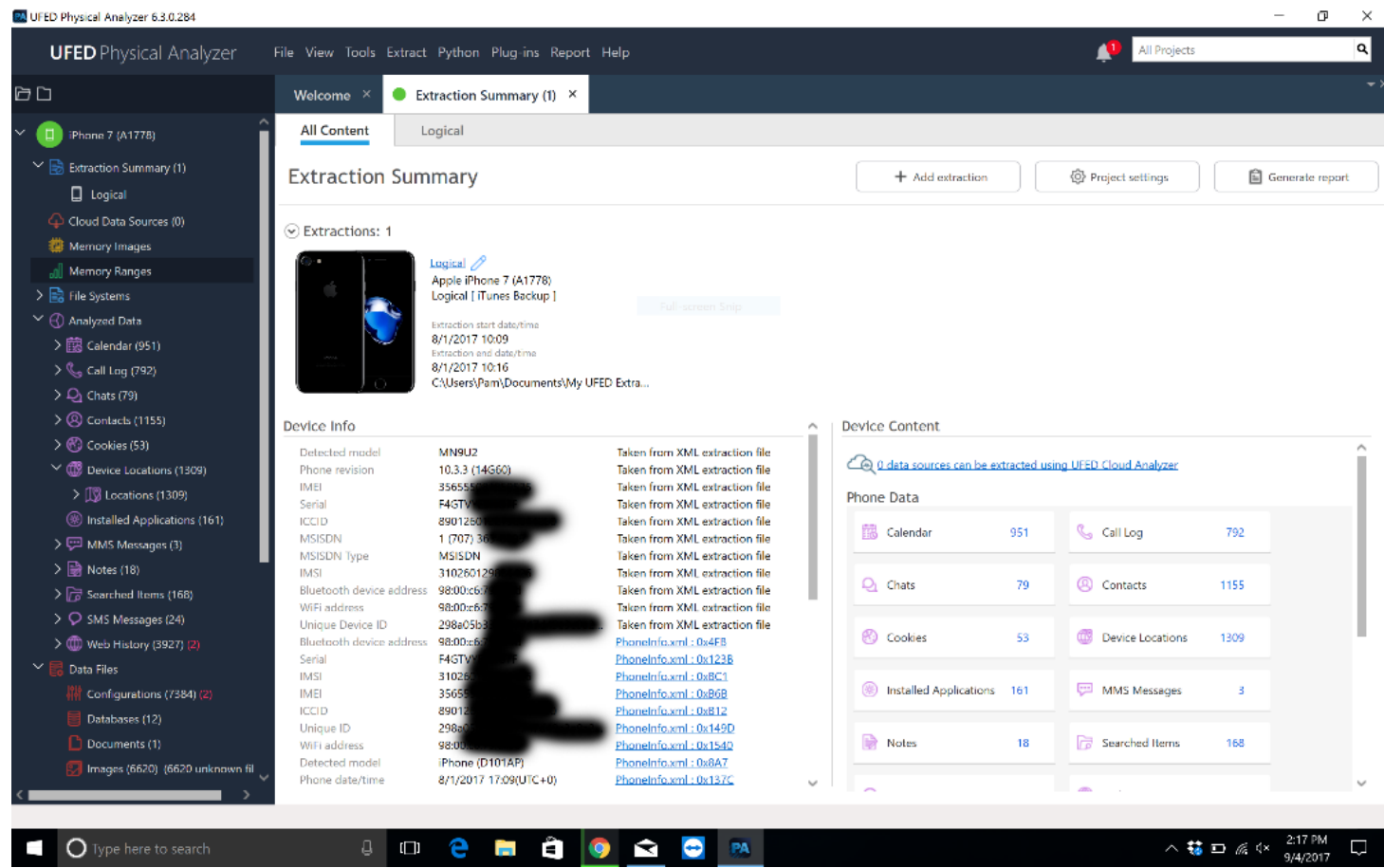
# Forensic Approaches

- **First** protect the data (Faraday bag or foil)
- Logical vs Physical extraction
- SIM card
- SD Cards?
- Chip Off



# Cell Phone Forensics Software

- Cellebrite
- Accessdata-MPE
- Magnet Axion (Acquire)
- Blacklight



# Automated vs Manual Carving (may help decide who does the extraction)



```
67794460 00 00 CC 99 44 45 41 44 42 45 45 46 01 00 07 91 ....DEADBEEF....
67794464 44 97 32 70 94 99 FF FF FF FF 04 00 0C 91 44 87 D.7p.....D.
67794468 55 43 20 91 FF FF FF FF 00 00 60 90 82 90 05 70 UC .....p
6779446C 40 59 41 79 19 94 7F D7 41 61 37 19 24 70 0B 41 @YAy....Aa?.$.A
67794470 EF 35 C8 FC 96 83 A6 61 7A 5D 4E 0E E7 41 ED 30 .5.....az]N..A.0
67794474 8D EC 02 C5 E0 5D 50 98 0E 42 BF D8 65 90 F9 2D .....mP..B..e.-
67794478 87 85 41 32 78 18 B4 4E 8F D7 2E 97 0B 44 7C 83 ..A2x..N.....D|.
6779447C EA 20 77 89 4C 06 C1 D3 E3 75 DA 7D 06 D5 E1 3F . w.L....u.)...?
67794480 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
67794484 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
67794488 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
6779448C FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
67794490 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
67794494 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
67794498 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
6779449C FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
677944A0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
677944A4 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
677944A8 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
677944AC FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
677944B0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
677944B4 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
677944B8 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
677944BC FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
677944C0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
677944C4 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
677944C8 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
677944CC FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
677944D0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
677944D4 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
677944D8 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
677944DC FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
677944E0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
677944E4 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
677944E8 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
677944EC FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
677944F0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
677944F4 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
677944F8 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
67794500 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
67794504 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
```

# The Service Provider

- Limitations on stored data
- Data not had elsewhere
- Ping data and geolocation data
- Transactional records

# Legal Obligations to Collect Cell Data

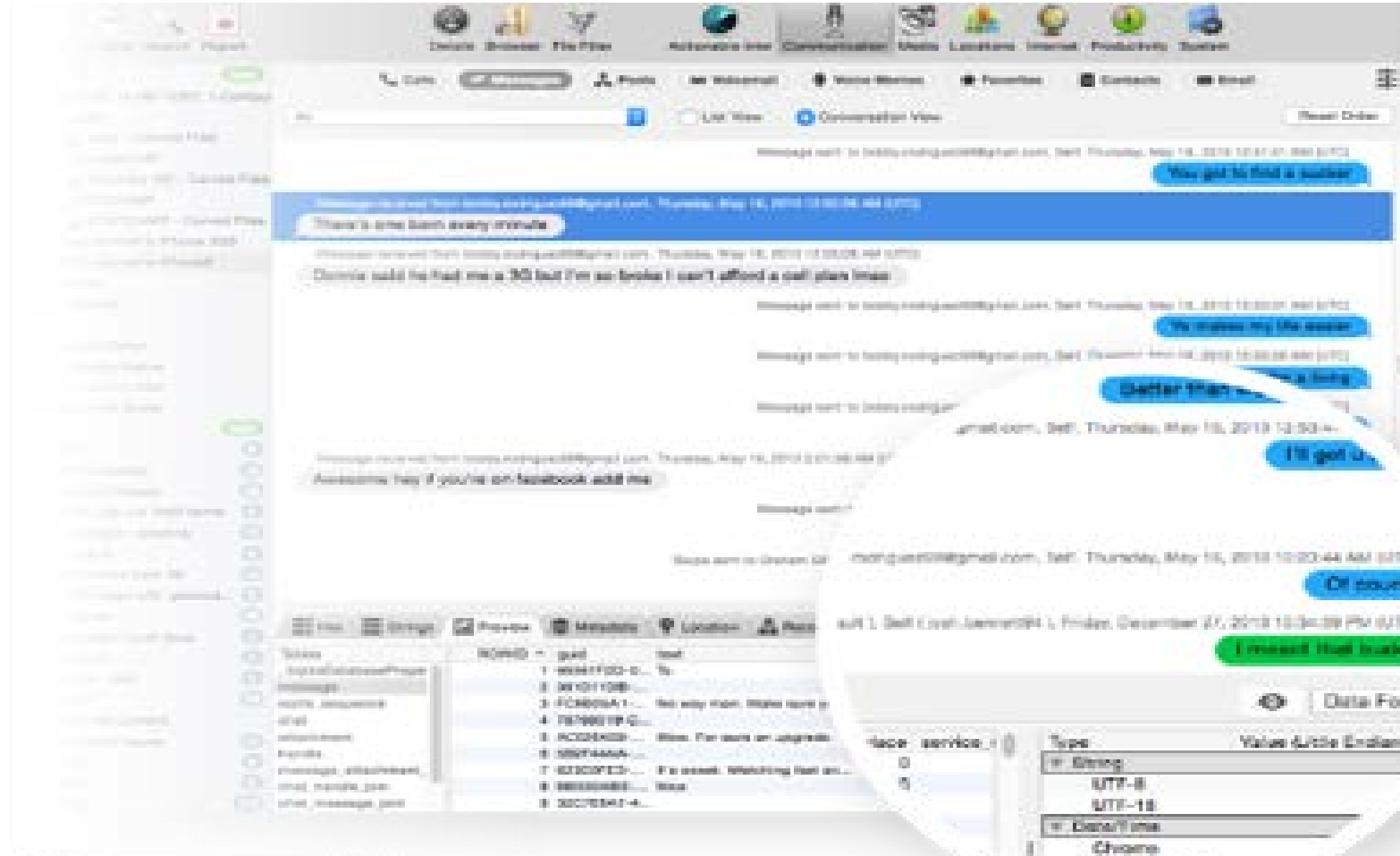
Failure to preserve text messages or other mobile data could result in “death penalty sanctions.” see [Small v. Univ. Med. Center of S. Nevada](#)



# Legal Obligations to Collect Cell Phone Data

Texts and emails sent by public employees on their personal devices or accounts are a matter of public record if they deal with official business. see [\*City of San Jose v. Superior Court\*](#), CA Supreme Court decided March 2, 2017.

# The Product You Want





# Questions?

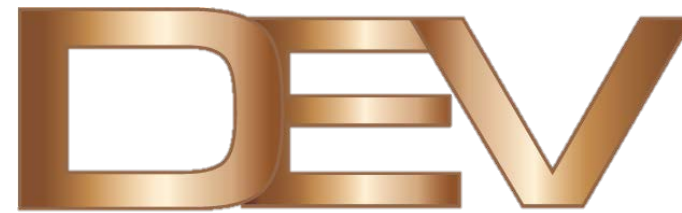
Don Vilfer, JD

Digital Evidence Ventures

1013 Galleria Blvd., suite 280 Roseville, CA 95678

916-883-2020

[don@DigitalEvidenceVentures.com](mailto:don@DigitalEvidenceVentures.com)



Digital Evidence Ventures