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

UNIVERSITY OF CALIFORNIA Ethics, Compliance & Audit Symposium
REACHING NEW HEIGHTS

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)

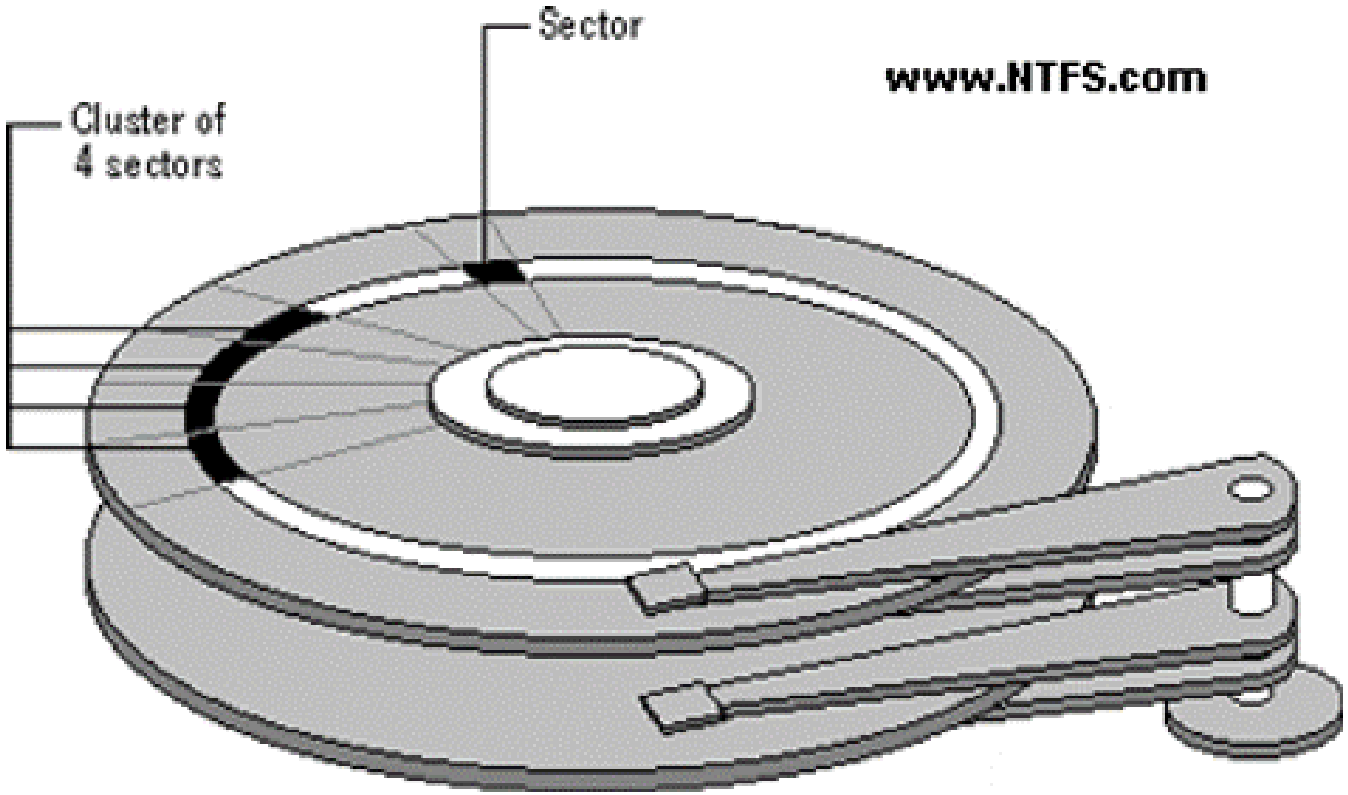
Paper Evidence of Electronic Data?

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

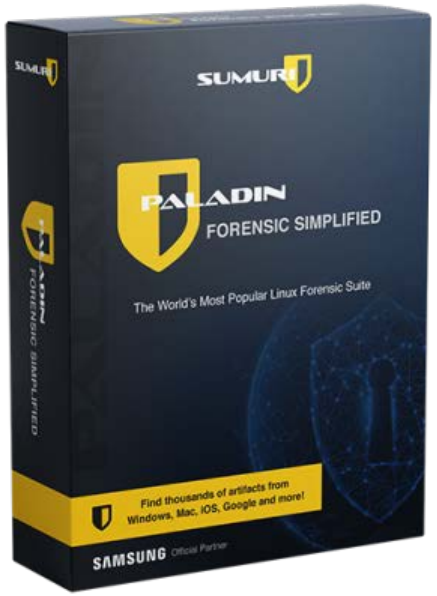
- Using a physical device to prevent change to the evidence while acquiring a forensic image
- Benefits and Drawbacks

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.

www.sumuri.com

Free (or nearly so) options!

Other tools are included.

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

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

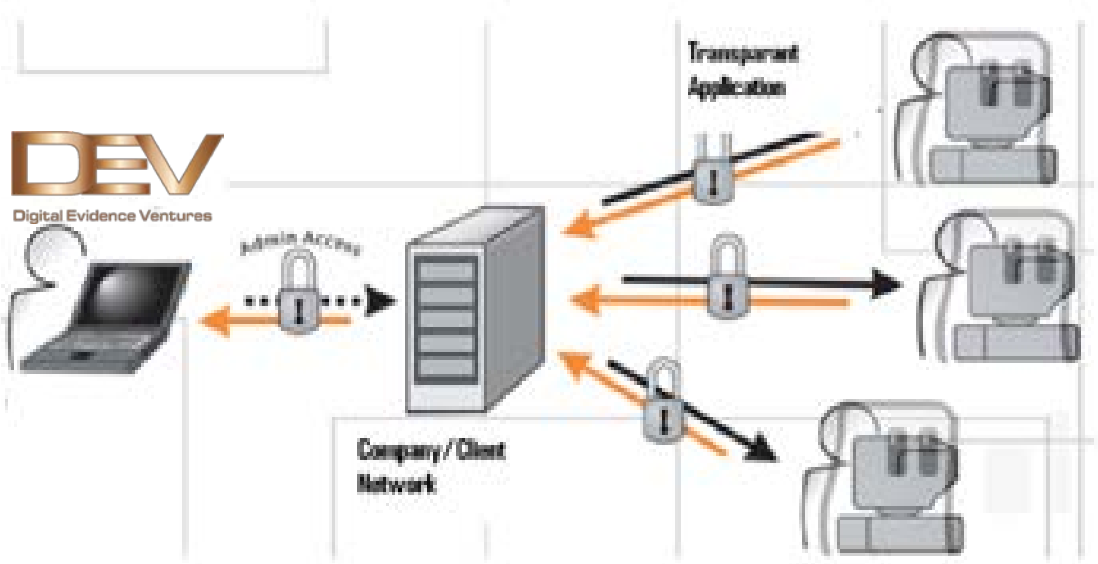
Used by Law Enforcement including Customs

NETWORK ACQUISITION

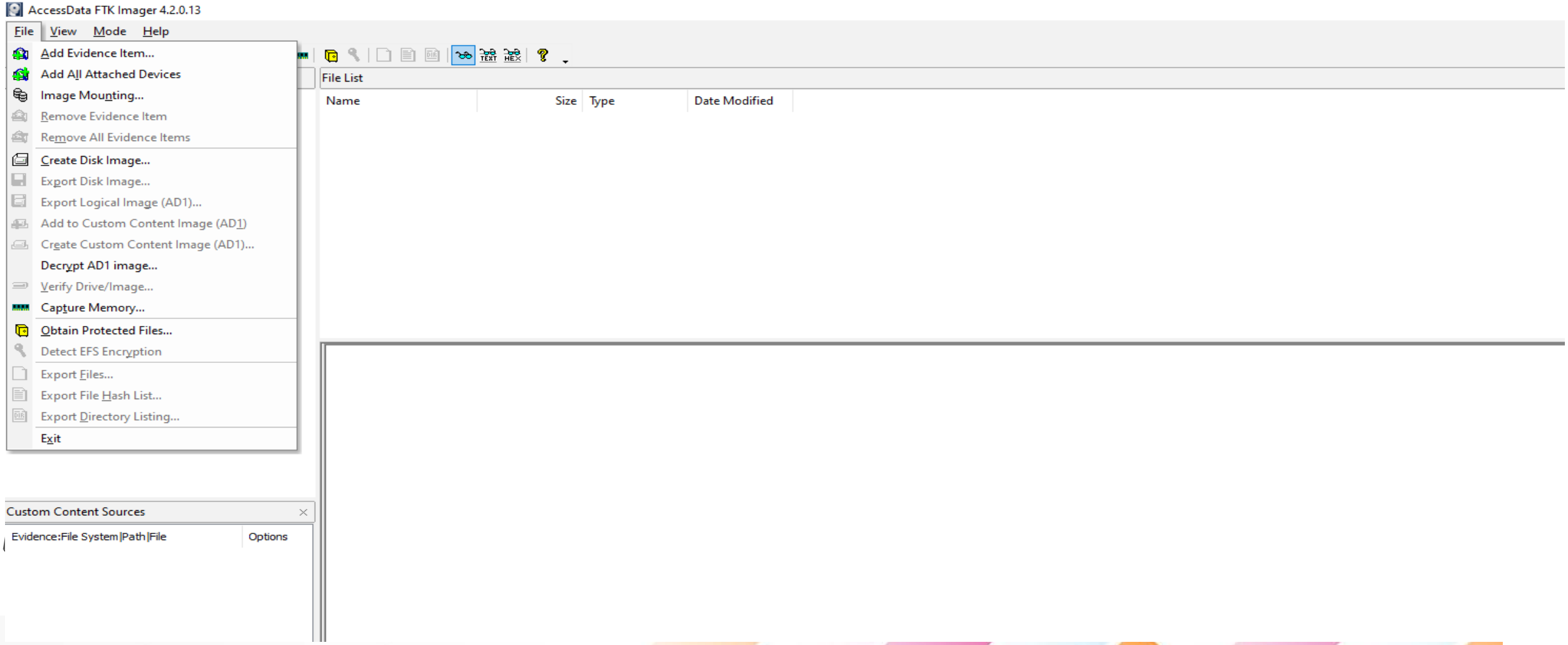
- Technique can be used locally or across the internet
- Admin access required
- Good for covert review
- Napa case example
- Tools: FTK Enterprise,

F-Response, Hardware

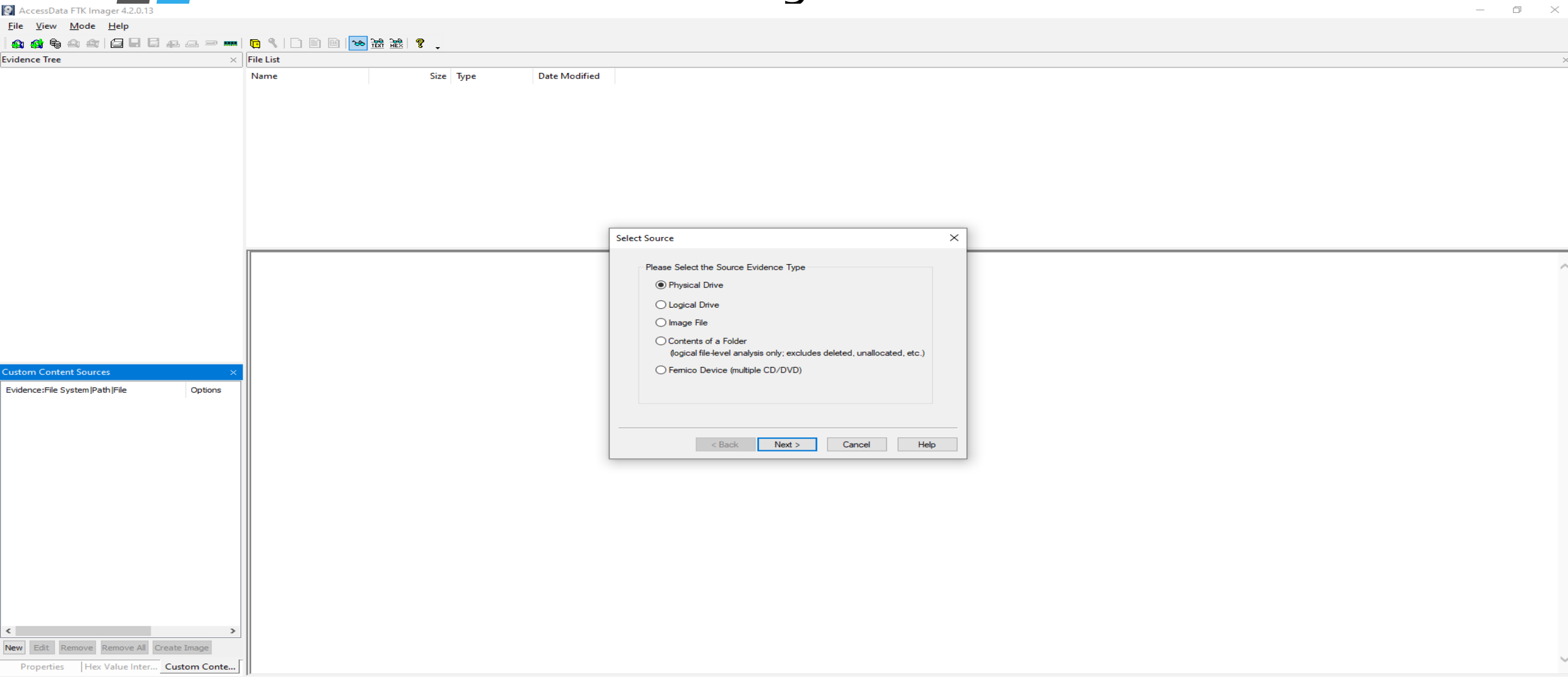
- FTK Imager work-around



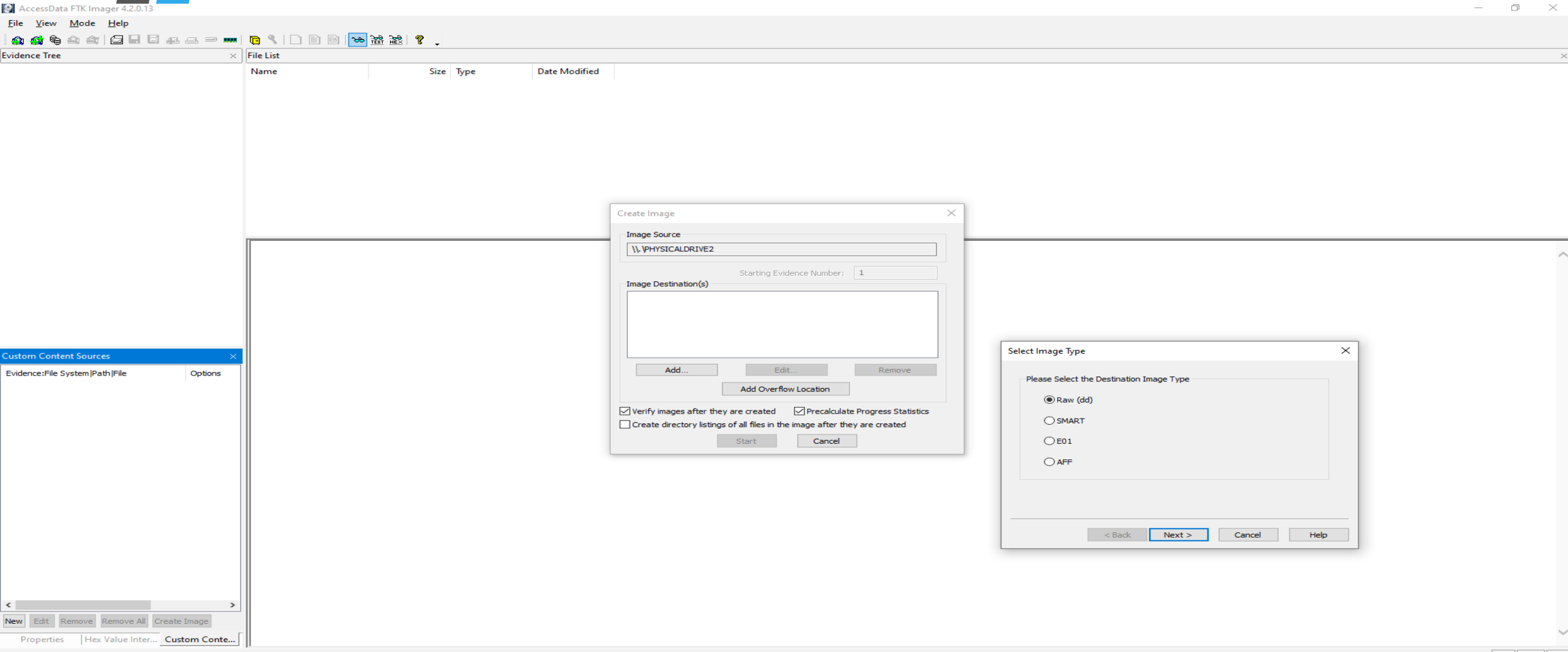
FTK Imager Workflow



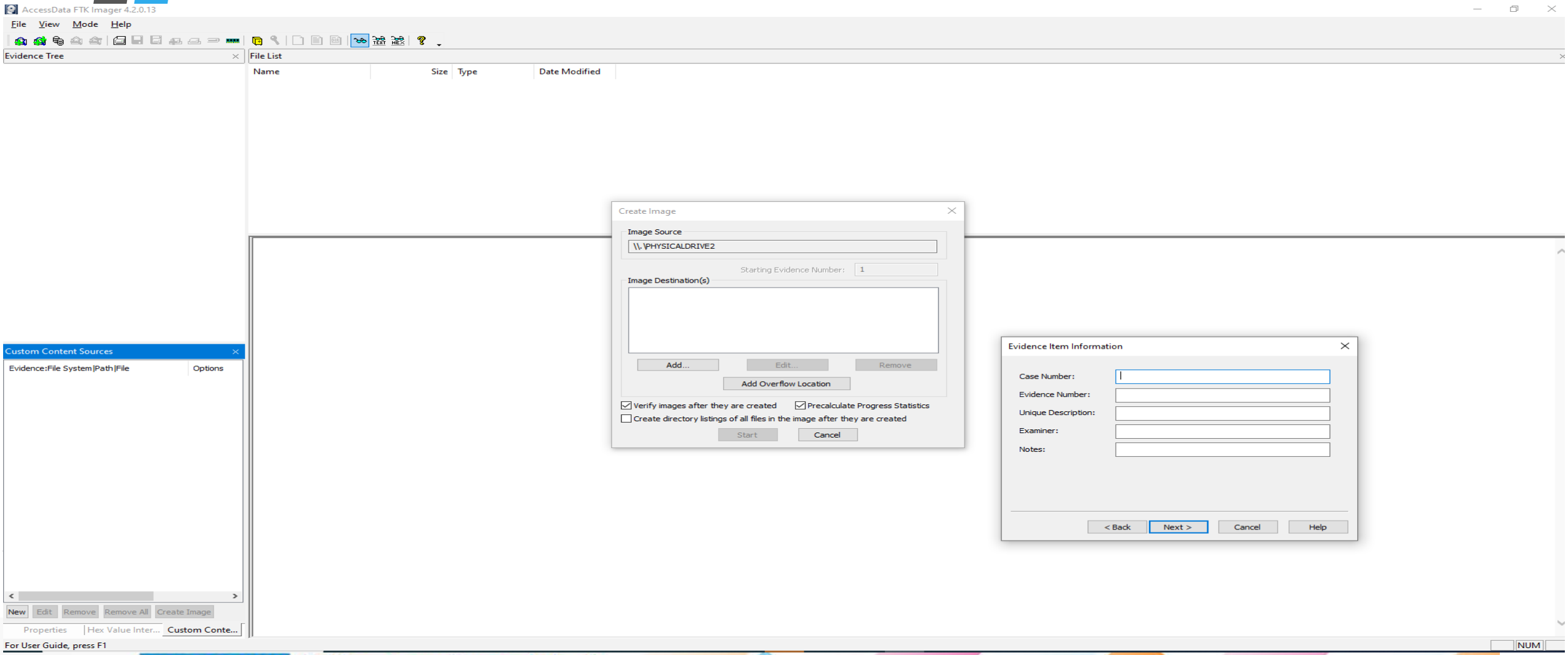
FTK Imager Workflow



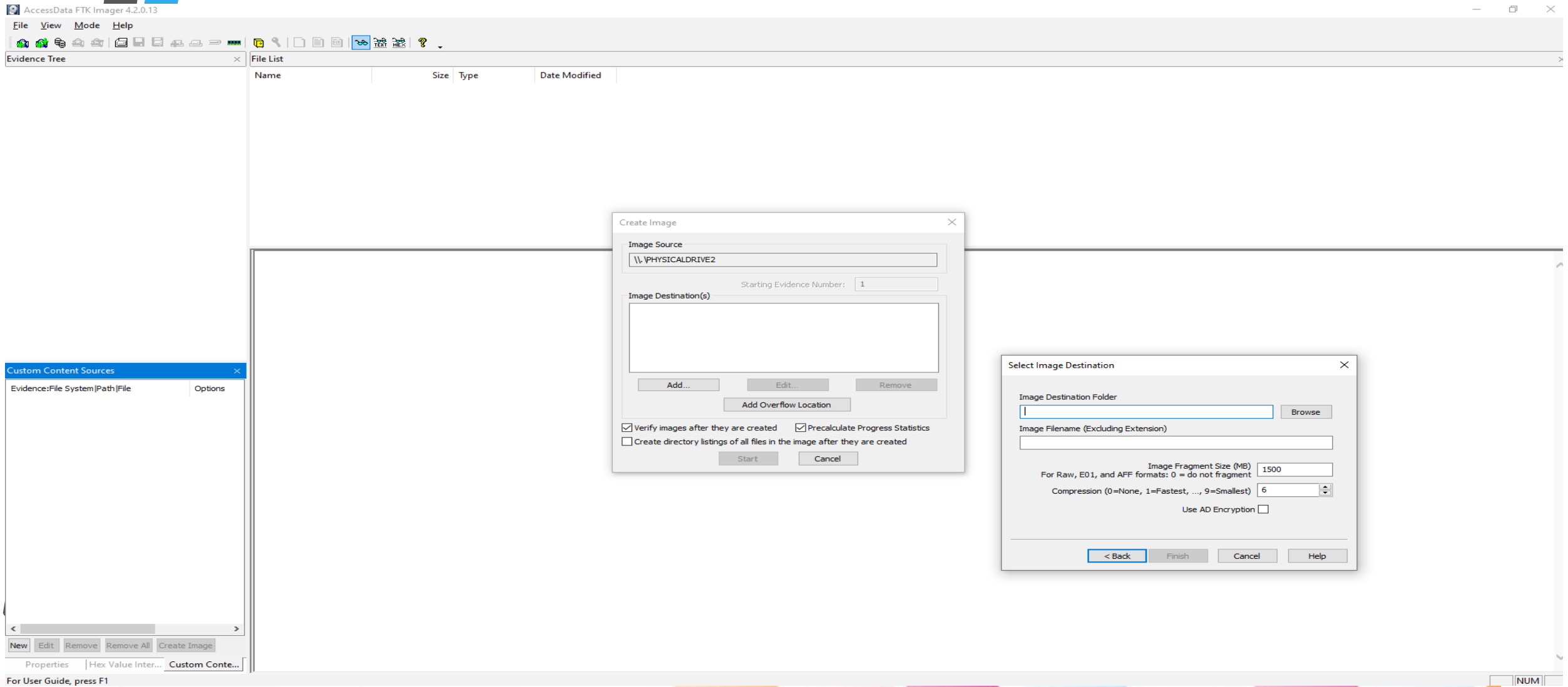
FTK Imager Workflow



FTK Imager Workflow



FTK Imager Workflow



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

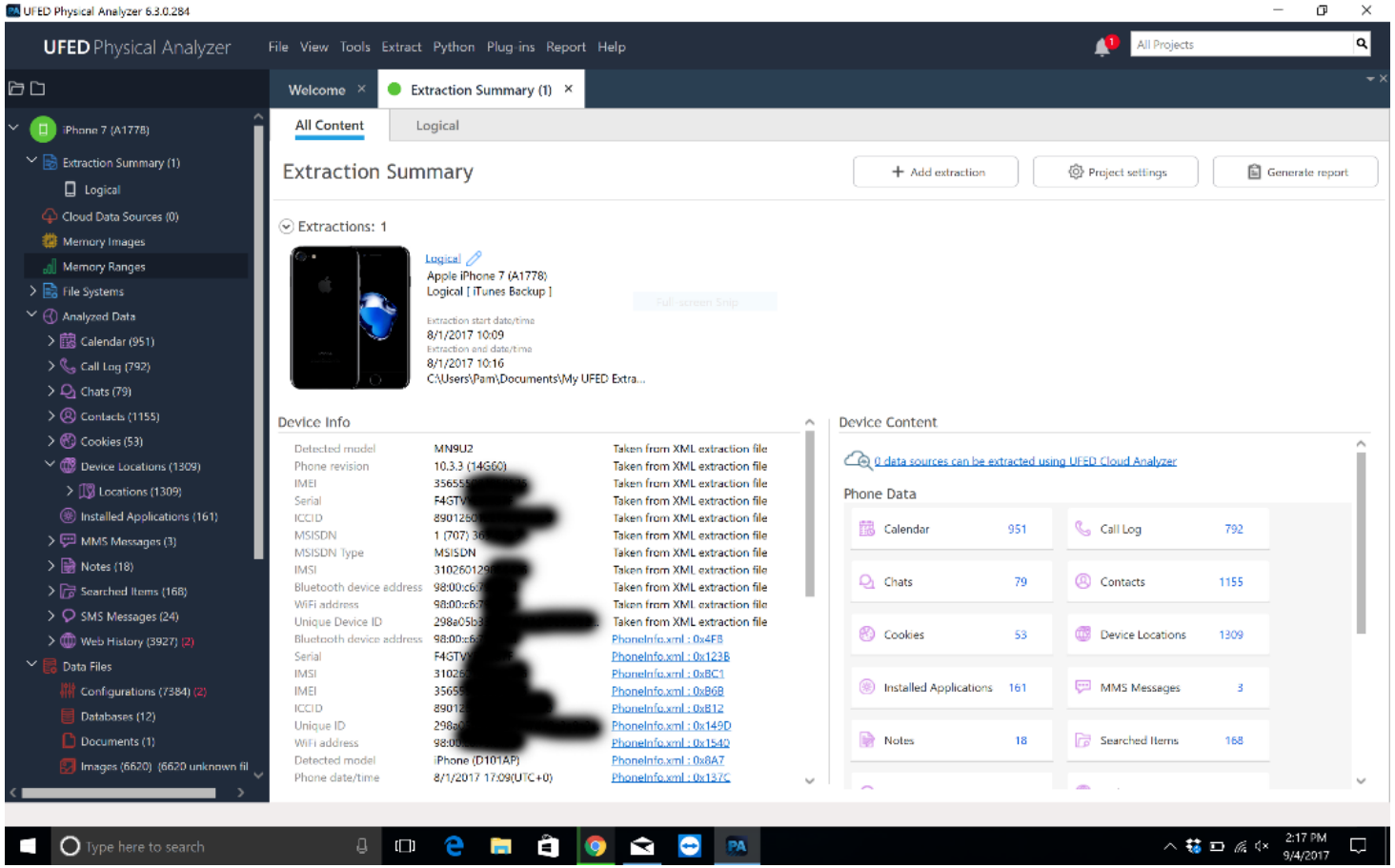
- The phone itself
- Local Backups-not just backing up iTunes
- The cloud-oh, forgot about the cloud
- Service Provider-limitations, but also data that is not available elsewhere

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 Axiom (Acquire)
- Blacklight



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

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

The Service Provider

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

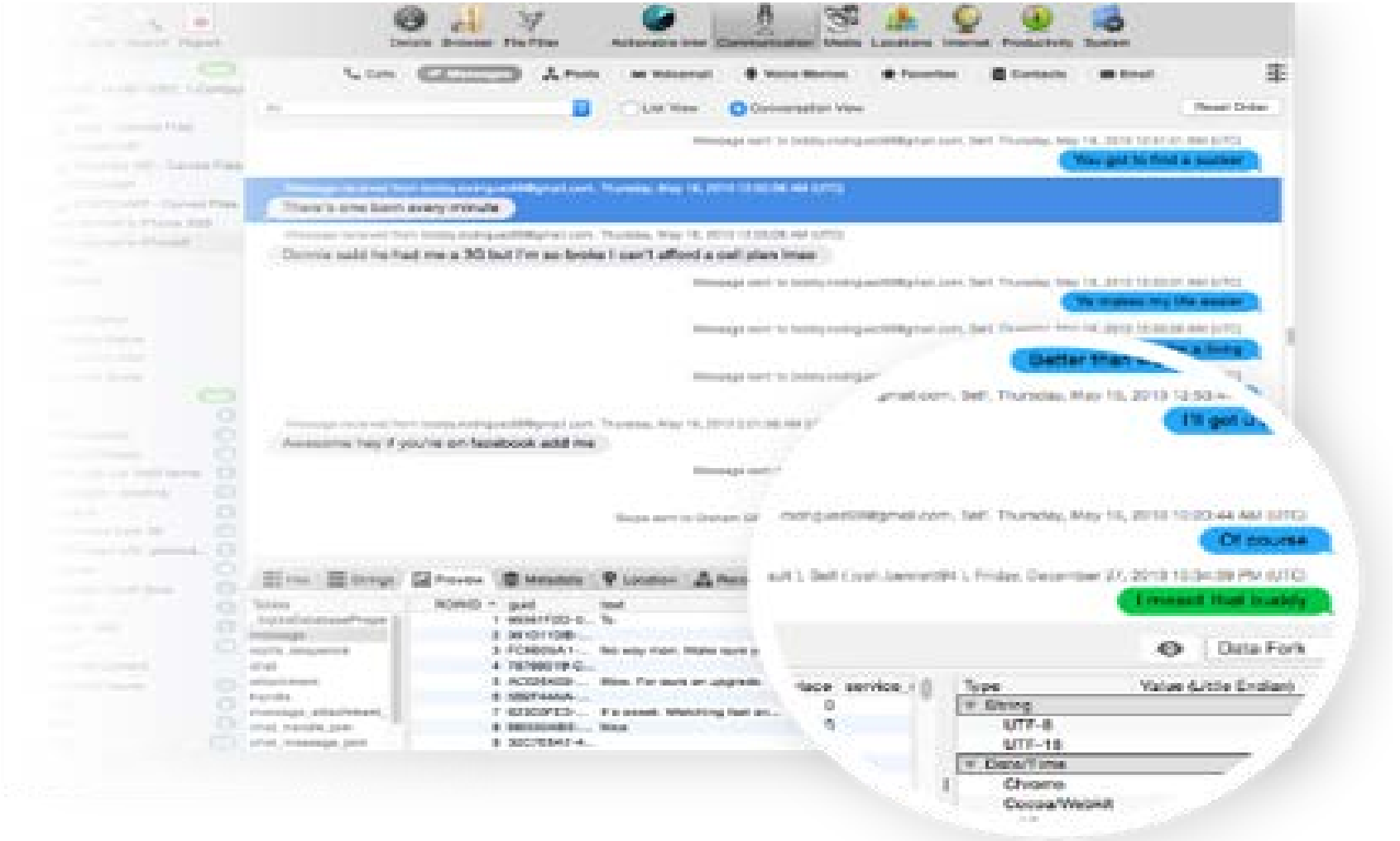
Legal Obligations to Collect Cell Data

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