PATHWAY FORENSICS

What Every CPA Needs to Know About Digital Law

September 10, 2018
Texas Society of Certified Public Accountants
Financial Institutions Conference

Presented by: Noel Kersh, EnCE

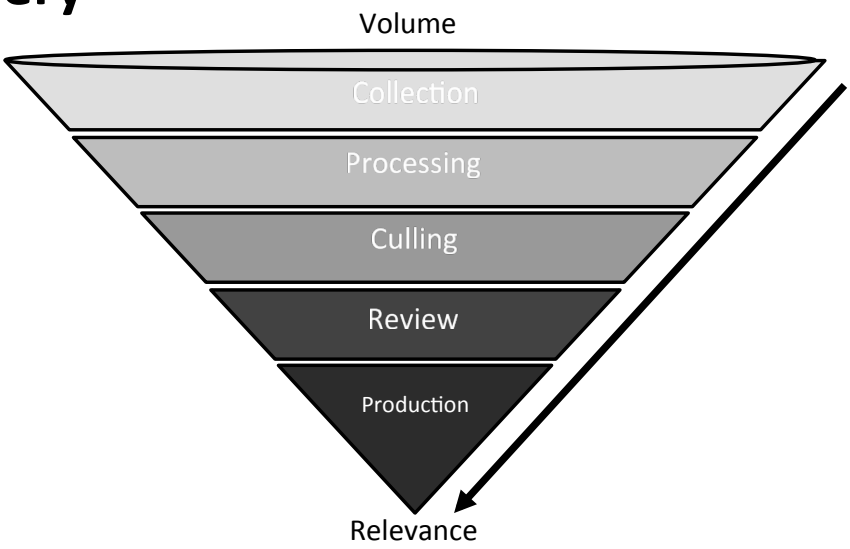
Overview of Today's Session

- Overview of Computer Forensics and eDiscovery
- Litigation Process
- We'll Answer: Why Do I Need to Know This?
- Case Examples
  - Cloud Storage
  - Evidence Spoliation
  - Instant Messaging
  - Evidence Wiping
  - Mobile Devices

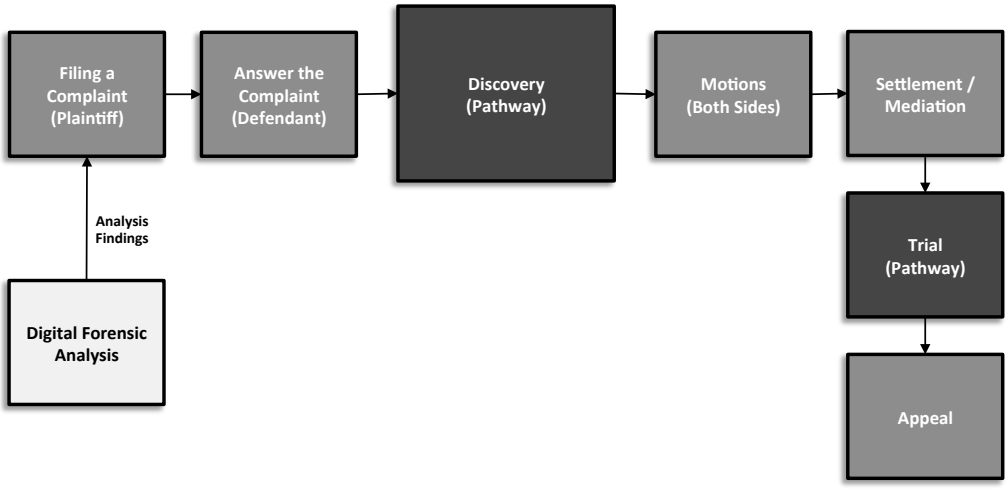
Overview of Computer Forensics

- Computer forensics is a discipline dedicated to the collection of computer evidence for judicial purposes
- Until around the year 2000, Computer Forensics was primarily a law enforcement tool
- From 2000 – present – huge growth in civil litigation application
- As long as there are people doing stupid things on their computer, I'll be busy ☺
- Focus of examinations are at a **micro level** focused on the bits and fragments of data on a device

eDiscovery



Litigation Process



Types of Cases

- Intellectual Property theft
- Employment Matters
  - Harassment, Discrimination, Wrongful Termination
- Business Litigation
  - Partnership contract disputes
- Government Investigations
  - Federal Corrupt Practices Act (FCPA)
- Criminal
- Family Law

Why Do I Need to Know This?

- You may be an advisor to a client that has data stolen from them
- Everybody has a cell phone and a computer
- Do you know what is on your cell phone and computer?
- Most of YOUR documents in business are created and stored electronically, be careful what you put in email.
- Data is often not really deleted
- One of the largest growing areas of litigation – it's not going away

Digital Evidence Sources

If it's electrical – it probably has data.

Electronic Storage Devices

- Desktops, laptops
- Email and file servers
- Network Shares
- Printers/Copy/Fax
- Backup Tapes
- External hard drives
- CD/DVD
- USB flash drives
- SD Cards
- Phone Systems
- DVR

Portable Devices

- Smartphones
- Tablet (iPad)
- Cell phones
- GPS Devices
- Cameras
- Mp3 Players
- Automobile onboard computers

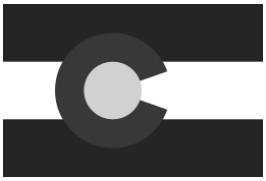
Online Media

- Cloud storage
- Hosted Services
- Virtual Infrastructure
- Websites
- Web based email
- Social media

The Digital Mountain

Searching for a needle in a haystack…

- 1 GB = 158,700 printed pages
- 1 GB fills up 10 bankers boxes and enough to fill up the bed of a pickup
- 50 GB = Almost 8 million printed pages and enough paper to fill up a box truck
- 80 Gigabytes - Nearly 700 miles of printed documents, enough to stretch from Dallas to Denver
- 1 Terabyte (1,000 GB) = 20 box trucks of paper and enough printed documents to stretch from Dallas to Melbourne, Australia (8,750 miles)



Computer Evidence

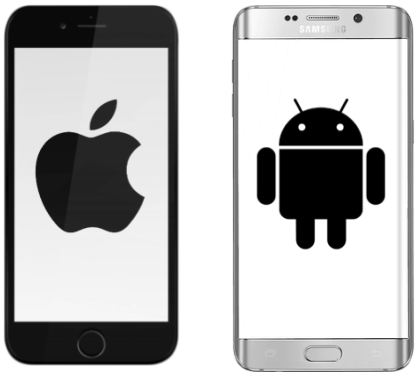
Active and Deleted

- Email
- File Activity (created, accessed, deleted)
- USB Activity
- Internet History
  - Web searches
  - Webmail
- Software Usage
- Instant Messaging
- Mobile Device Backups

Mobile Phone Evidence

Active and Deleted

- Messages: SMS, MMS, Chats, IM
- Call Logs
- Contacts
- Calendar
- Internet History
- Locations
- Pictures/Video
- Voicemail



Case Example 1: Cloud Storage

Once its on the web…it can be anywhere.

- Single Dropbox account shared across all users
- Blocked access to other cloud storage sites
- Employee left to work for competitor
- Used Dropbox login to download 300+ documents

Dropbox

iCloud

Google Drive

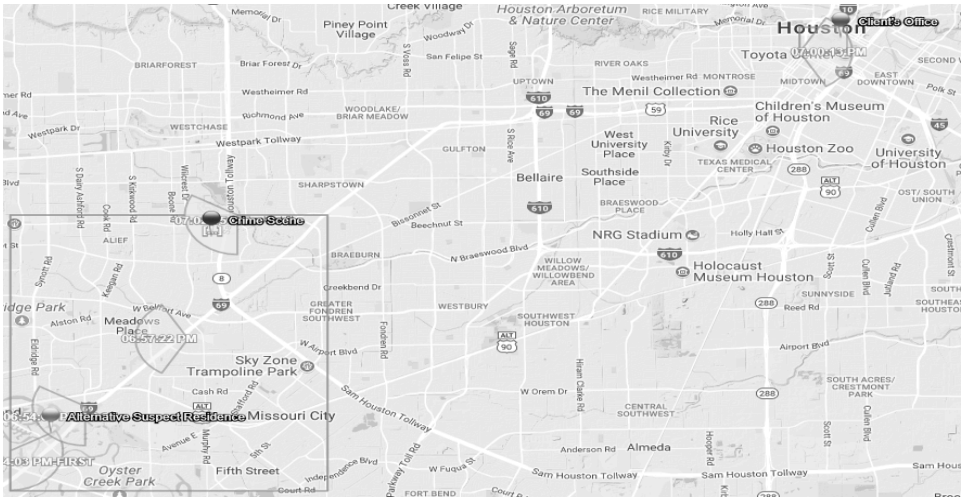
Case Example 2: Mobile Devices

Can you hear me now?

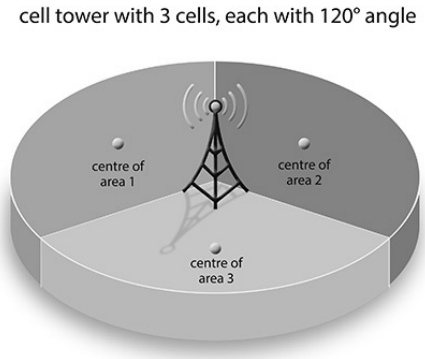
- Client arrested and charged with murder.
- Call Detail Records (CDR) from Cellphone Carrier obtained via warrant.
- CDR showed client was in a different location at time of murder.
- CDR for another suspect was used to place near the crime scene at time of murder.
- Client was released and charges dropped.

Case Example 2: Mobile Devices

Can you hear me now?



Call Detail Records



Retention Periods of Major Cell Providers

	Verizon	AT&T	Sprint / Nextel	T-Mobile
Subscriber Information	3-5 years	Depends on Length of Service	Unlimited	5 years
Call Detail Records	1 year	5-7 years	18 months	2-5 years
Cell Towers Used by Phone for Calls	1 year	From July 2008	18 months	6 months
Text Message (SMS) Records	1 year	5-7 years	18 months; Not Available for Nextel	2-5 years
Text Message (SMS) Content	3-5 days	Not Retained	Not Retained	Not Retained
Cell Towers Used for SMS Transmission	Not Retained	1 year	Varies	180 days

Case Example 3: Webmail

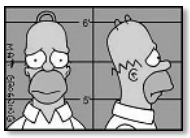
Everybody has a webmail account or three or four…

- Webmail found showing large number of company files sent to home address morning of last day
- Webmail found planning new competing business to be setup including documents sent to Secretary of State to setup new company
- Financials sent to CPA containing accounts not previously disclosed to spouse
- Email received in webmail from former employee under non-solicitation agreement with offer letter attached

Case Example 4: Evidence Spoliation

When a judge says don't delete…you really should not delete.

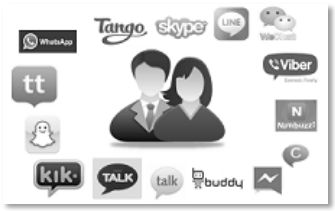
- Forensic analysis on former work computer identified a USB device containing several IP docs
- Specific device requested make, model and serial number of USB determined from the analysis
- Subject's attorney represented the device contained only family photos and recipes
- Analysis showed IP deleted and family photos and recipes added on the morning of the evidence hearing
- Subject later found in contempt and sentenced to 6 months in jail



Case Example 5: Instant Messaging

"Don't worry, this is instant messenger, not email. They won't read this."

- Former employee sued for sexual harassment
- Claimed manager used specific vulgar phrase
- Analysis found instant messages between subject and her boyfriend where she repeatedly used the phrase in a light hearted manner
- Chat analysis report faxed to subject's Counsel – never heard from again



Case Example 6: Evidence Wiping

Not all data wipers are created equally.

- Subject used free application which left details of what was wiped the day before turning over computer
- Computer received in lab with hard drive manufactured 4 years after computer manufactured
- Forensic analysis determined almost 30k files wiped using CCleaner the morning of last day – Former employee admitted he did it – Files never recovered and former employee sanctioned by the court

Case Example 7: Mobile Devices

Can you hear me now?

- Former employee returned company issued phone upon departure
- New company provided employee with a new phone
- Subject used iTunes backup of former company phone to load contacts onto new company phone
- Subject factory reset device before returning to company – Analysis found backup on computer and data (call logs, texts, contacts) extracted from backup

Questions/Comments

PATHWAY FORENSICS

Noel Kersh, EnCE
Principal
nkersh@pathwayforensics.com
(713) 401-3380

14405 Walters Rd., Suite 630
Houston, Texas 77014

www.pathwayforensics.com