


Emerging Technology: Criminal Law & Evidence

CHRISTINA MILLER
ASSOCIATE CLINICAL PROFESSOR OF LAW
SUFFOLK LAW


 > [News](#) > Digital Forensics: Window Into the Soul

Digital Forensics: Window Into the Soul

June 10, 2019 | [C.M "Mike" Adams, EnCE](#)

 [Tweet](#)

 [Share](#)

 [Email](#)

Digital forensics, much like DNA, can be the key to unlocking unbiased truth. It offers its own patterns and "codes" that the examiner can link directly to a person. We have heard the rumblings. Our ubiquitous digital devices are "today's DNA."

Just as DNA evidence revolutionized investigations in the 1990s, digital forensics is now becoming the best science, the leading tool, and our most powerful weapon for use in the ever-evolving criminal landscape.

However, one major difference is that a prosecutor would have an easy time proving that a suspect was never separated from his DNA. This is much less certain for one's digital forensics presence, no matter how profoundly the defense attorney might argue otherwise.

The pitfall comes when, for whatever reason, an error occurs. In digital forensics errors are usually the result of at least two, or more, mistakes. Let's examine one critical error spawned by smaller mistakes within the Casey Anthony case. In this case a mother, Casey Anthony, was accused of murdering her own daughter, Caylee Anthony. The prosecution and the defense had their own digital forensics examiners. They independently generated almost the same information but arrived at different conclusions.

Casey's defense attorney, Jose Baez, gave the jury what it needed the most. A viable alternative suspect, to wit George Anthony, Casey's father. Per the timeline George and Casey were home when the following Google searches were initiated ...

- Chloroform
- Chest trauma
- Internal bleeding
- How to make chloroform

However, there was one more critical search which, if the jury had known about, might have pushed them to vote guilty on the murder charge. While sources disagree on the exact term, they all agree that the search was



Criminal Law

Criminal Procedure

Evidence

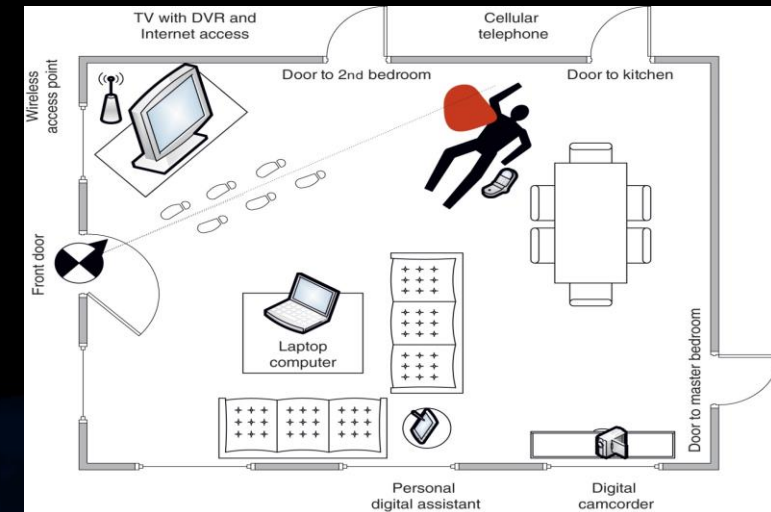
Nature of Proof



Constitutional Investigations



Evidentiary Value & Limitations



****Educating the Investigators & Factfinders****

Digital Evidence



WHAT IS IT?



HOW DO YOU GET IT?



HOW DO YOU USE IT?



Digital Evidence: What Is It?

- Computer Hard Drive: Written & Deleted Data
- Server & Cloud Data
- App Data
- Blackbox & Car Communications (OnStar)
- Video/Audio/Photos
- Metadata
- AND Much, Much MORE!



What can be provided From Phone Itself?



- Saved Items (email, docs, images, text ...)
- Created Items
- Deleted Items
- Changed or Altered Items
- Hidden or Encrypted Items
- Dates and Times
- User Logs
- E-Mail
- Documents
- Images
- Metadata (EXIF)

Name	Outlook
Logical Size	4,096
Category	Unknown
Signature Analysis	Unknown
Last Accessed	04/23/20 12:46:21 AM (-4:00 Eastern Daylight Time)
File Created	06/27/19 06:08:44 PM (-4:00 Eastern Daylight Time)
Last Written	04/23/20 12:46:21 AM (-4:00 Eastern Daylight Time)
Is Indexed	-
MD5	e603f066cd01d8a49d99bdcfeb2d1eef
SHA1	ef5fe77bbfe9a732ebb1b598a7678ac7ca8727a1
Item Path	E01Capture\C\Users\Dropbox\Outlook
True Path	E01Capture\C\Users\Dropbox\Outlook
Description	Folder, Archive
Entry Modified	04/23/20 12:46:21 AM (-4:00 Eastern Daylight Time)
File Acquired	05/11/20 11:04:06 AM (-4:00 Eastern Daylight Time)
Initialized Size	4,096
Physical Size	4,096
Starting Extent	0C-C4060763



Cloud Content

- Calls & Texts
- Photographs
- **App Data**
- GPS
- Contacts
- Accounts
- Metadata
- And on, and on, and on....

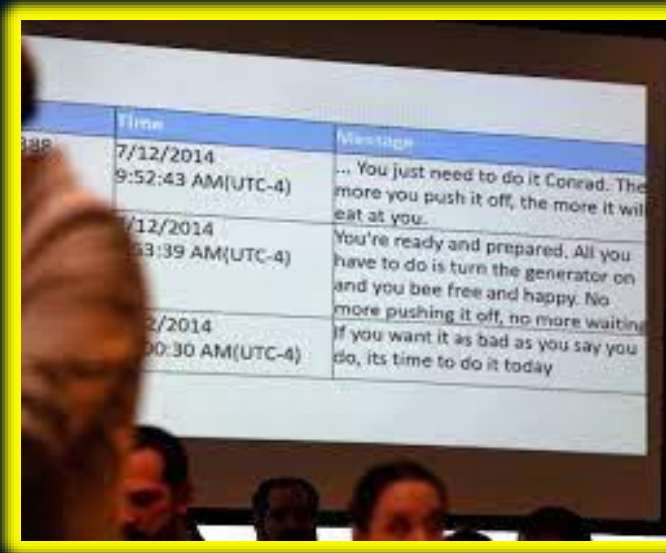
Name	Outlook
Logical Size	4,096
Category	Unknown
Signature Analysis	Unknown
Last Accessed	04/23/20 12:46:21 AM (-4:00 Eastern Daylight Time)
File Created	06/27/19 06:08:44 PM (-4:00 Eastern Daylight Time)
Last Written	04/23/20 12:46:21 AM (-4:00 Eastern Daylight Time)
Is Indexed	-
MDS	e603f066cd01d8a49d99bdcfeb2d1eef
SHA1	ef5fe77bbfe9a732ebb1b598a7678ac7ca8727a1
Item Path	E01Capture\C\Users\Dropbox\Outlook
True Path	E01Capture\C\Users\Dropbox\Outlook
Description	Folder, Archive
Entry Modified	04/23/20 12:46:21 AM (-4:00 Eastern Daylight Time)
File Acquired	05/11/20 11:04:06 AM (-4:00 Eastern Daylight Time)
Initialized Size	4,096
Physical Size	4,096
Starting Extent	0C-C4060763

Digital Evidence: Criminal Law

Act



Intent



Causation

From: Kevin Weinman <cybercriminal@email.com>
Sent: Friday, August 5, 2022 11:51 AM
To: Payroll
Subject: Friday, Aug 5, 2022



[EXTERNAL EMAIL]

Patty,

I would like to change/modify my direct deposit information to be effective for the next pay date, What details do you need so you can help me change it?

Regards

Kevin C. Weinman

FRAUD



<https://www.latimes.com/california/story/2021-05-04/3-men-dead-in-anaheim-car-crash-driver-found-after-fleeing-the-scene>

(1) ID: What pieces of digital evidence will help identify the driver?

(2) Crimes: What crimes could the government allege?

(3) Elements: How will the digital evidence support the elements of the crimes?



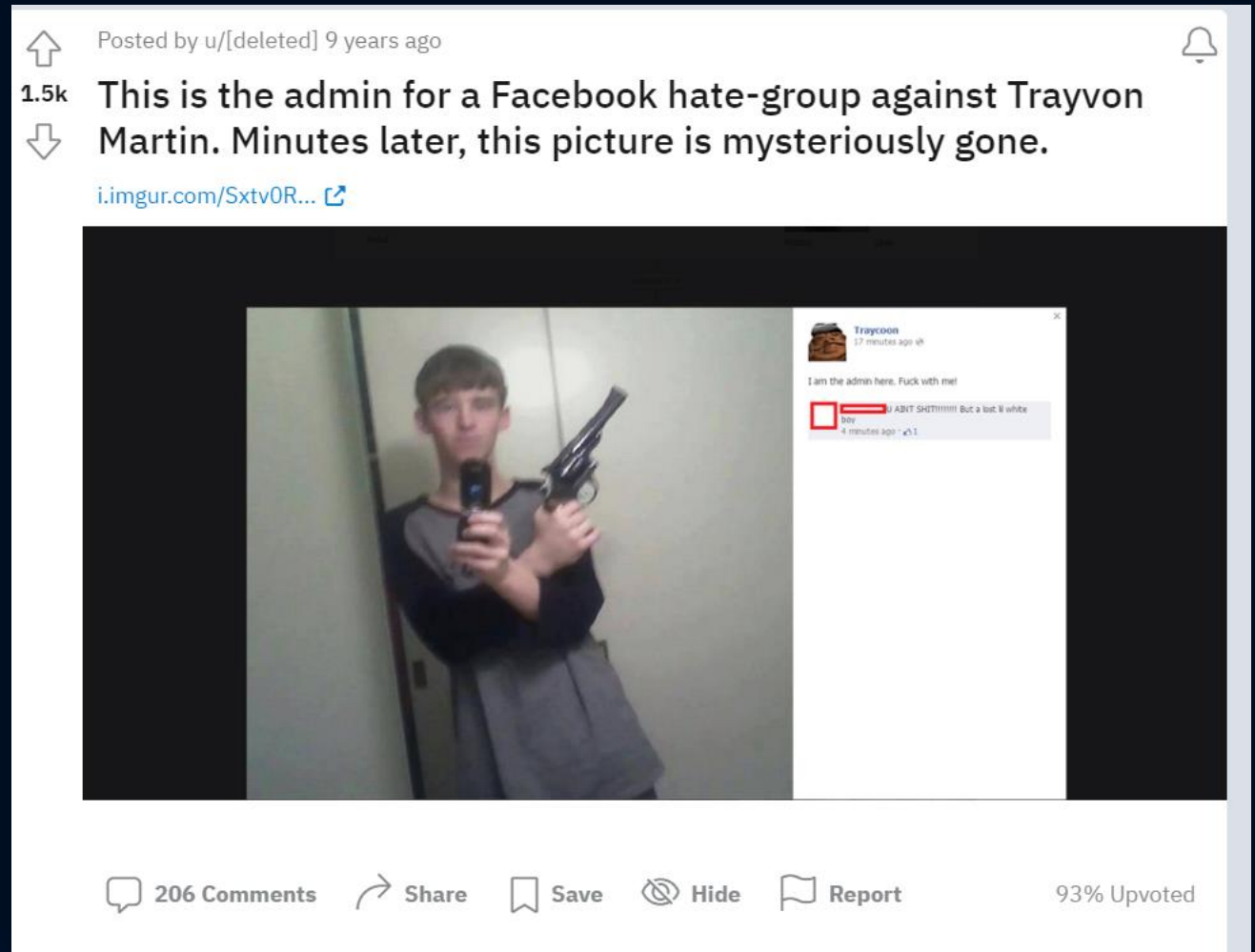
Opportunity #1: Criminal Law

Integrate Cybercrime & Digital Evidence

- Act
 - Cybercrime
- Intent
 - Texts, Emails, Video
- Causation
 - Fraudulent E-mails
 - Texts Induce Action



Criminal Procedure: Stop, Seize, & Search



App Searches



Company App Search Methods

1st Preserve: Freeze Orders (Stored Communications Act or Court Order) [18 U.S.C. Chapter 121 §§ 2701–2712](#)

2nd Procure & Search:

- Administrative or Grand Jury Subpoenas or Court Order for Subscriber Information (SCA & ECPA & state-by-state)¹
- Content of Communications: Search Warrant or Exigency
- Witness Examination (Investigator, Officer, Forensic Examiner)

3rd Privacy of Investigation:

- Protective (A/K/A Non-Disclosure Orders) [18 U.S.C. § 2705\(b\)](#)

¹ [Sample D Order \(justia.com\)](#)

Nexus?

CELL PHONE SEARCH

Commonwealth v. Snow, 486 Mass. 582 (2021)



- D called GF to ask her to retrieve car soon after crime & repeatedly called re: car
- GF had improbable explanation for having rented the car at all (she owned a car)
- Evidence of premeditation (change of clothes)
- Co-D communicating with victim, reasonable inference used cells to communicate with Co-venturer
 - ****Proof of shared mental state****
- NOTE: Joint Venture is Insufficient

Particularity & Scope?

- No time restriction given in issuing warrant: warrant “impermissibly broad”
- Where no time restriction, automatically overbroad because facts point to a particular time
- REMEDY: Partial Suppression (Remanded)

CELL PHONE SEARCH

Commonwealth v. Snow, 486 Mass. 582 (2021)





IMSI Catchers & Geofencing

- IMSI Catchers (International mobile subscriber identity): Mimics a cell tower in order to force all nearby cell phones to connect to it.
- Geofencing: (Typically) Data from cell towers for a defined area and time period are analyzed to ID devices.**



** See *United States v. Chatrie*, 590 F. Supp. 3d 901 (E.D. Va. March 3, 2022)

** Lower Court Documents: [https://www.nacdl.org/Content/United-States-v-Chatrie,-No-3-19-cr-130-\(E-D-Va-\)](https://www.nacdl.org/Content/United-States-v-Chatrie,-No-3-19-cr-130-(E-D-Va-))

Social Network Searches

Commonwealth v. Carrasquillo, 489 Mass. 107 (February 7, 2022)

Privacy? Democracy?

- Conversational Privacy: “Think and act creatively and constructively”
- Associational Privacy: Develop & maintain personal relationships
 - ** “joys, profound sorrows, & minutiae of everyday life that previously would have been discussed ... in privacy of ... homes now generally are shared electronically using social media” **

Subjectively Reasonable?

Objective Reasonable?

Social Network Searches

Fourth Amendment Questions:

- Geo-location data: If you “tag” yourself at a location, do you have an expectation of privacy?
- Does the same warrant requirement for text messages apply to private messages sent via social networking sites?
- What about once-public, now deleted social media content?
- Do expectations vary depending on owner of hardware?
- Does the proliferation of these sites change normative expectations of privacy?
- Does compliance with the terms of service impact expectations of privacy?



Digital Surveillance

Commonwealth v. Mora, 485 Mass. 360 (2020)

Mosaic Theory

- “Color of a single stone depicts little, but by stepping back one can see a complete mosaic.”¹
- Reasonable Expectation of Privacy in Aggregated Digital Data Collected over Time by Government and Third-Parties.
- Focuses on Sustained Electronic Monitoring of Public Movements and Activities.

¹ *Commonwealth v. McCarthy*, 484 Mass. 493, 504 (2020).





<https://www.latimes.com/california/story/2021-05-04/3-men-dead-in-anaheim-car-crash-driver-found-after-fleeing-the-scene>

What Should Happen Next?



Analyze the three-P's for one key piece of digital evidence in your case? Recommend how it would legally be:

- 1) preserved
- 2) procured and searched, and
- 3) privacy protected (or not).

TEAMS 1 & 4: DRUG & GUN CASE

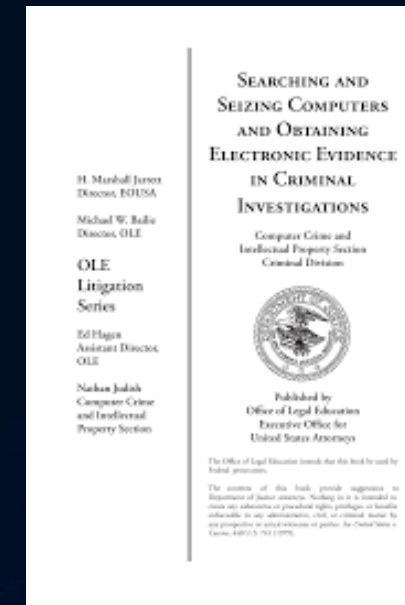
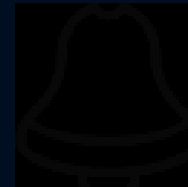
TEAMS 2 & 3: MOTOR VEHICULAR HOMICIDE CASE

Opportunity #2: Criminal Procedure

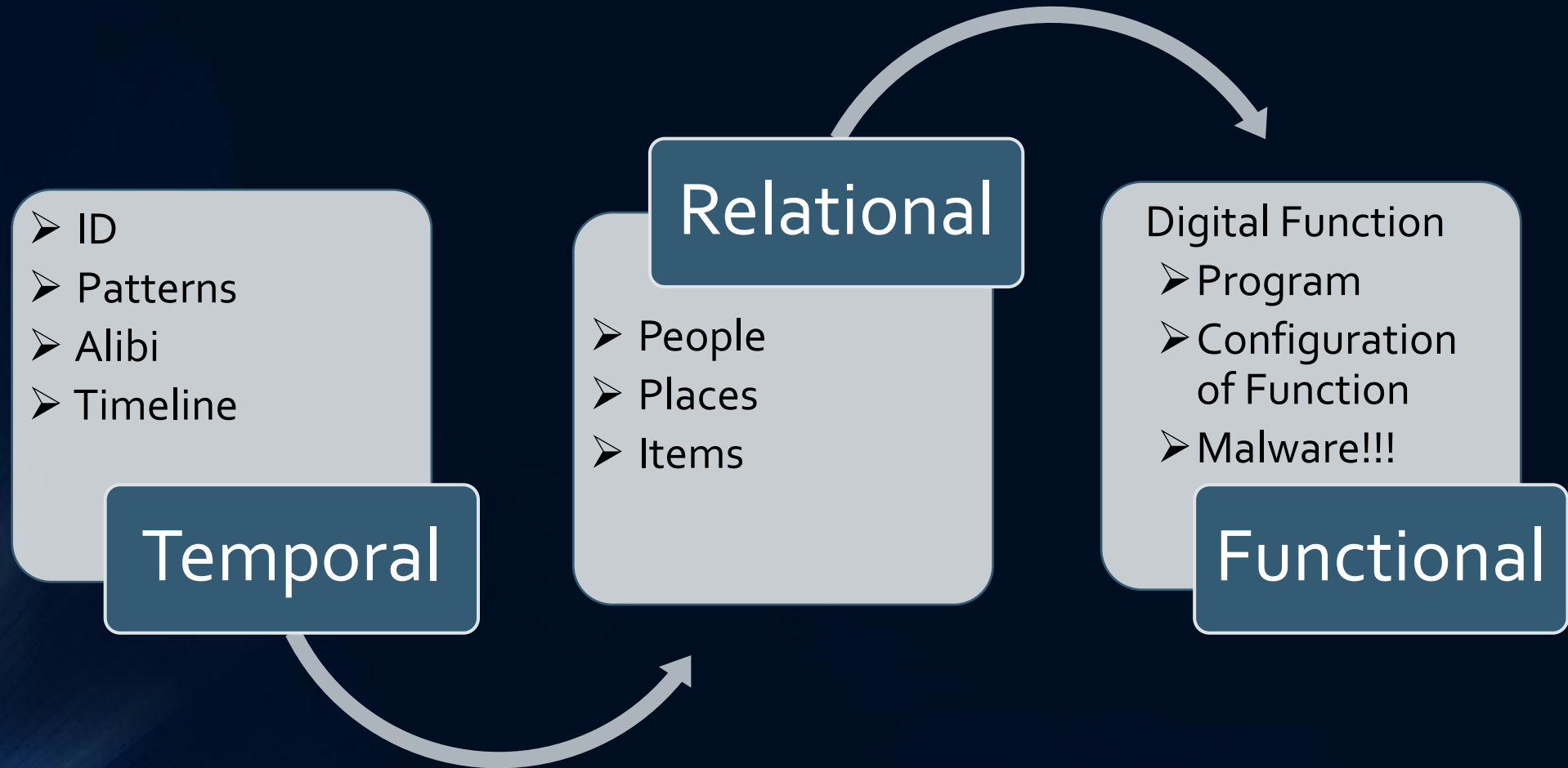
- Reasonable Expectation of Privacy
- Nexus of Items Sought to Evidence
- Particularity & Scope of Search:
 - Expected to be Located at the Time the Warrant Issues (Durable vs. Stale)

CloudGavel's Electronic Warrants Solution

The solution for law enforcement, prosecutors, judges



Evidentiary Analysis



Adapted From: Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science and the Internet* (Elsevier Inc. 2011)

FRE 902: Digital evidence

“(13) **Certified Records Generated by an Electronic Process or System.** A record generated by an electronic process or system **that produces an accurate result**, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). ...

(14) **Certified Data Copied from an Electronic Device, Storage Medium, or File.** Data copied from an electronic device, storage medium, or file, **if authenticated by a process of digital identification**, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12).”

Mass. G. Evid: Article XI, § 1119: Digital evidence

§1119(b) Application of law:

“The same principles of evidence law that apply to traditional documentary evidence apply to digital evidence in courtroom and virtual proceedings. Digital evidence admissible in a courtroom is admissible in a virtual proceeding.”

Climb Mountains of Admissibility



Authentic

Authentic

- ☐ ID author(s) of computer stored document?
- ☐ The same as when created/recorded as now?
 - ☐ Has not undergone significant change that matters

Emails & Texts: Authentication

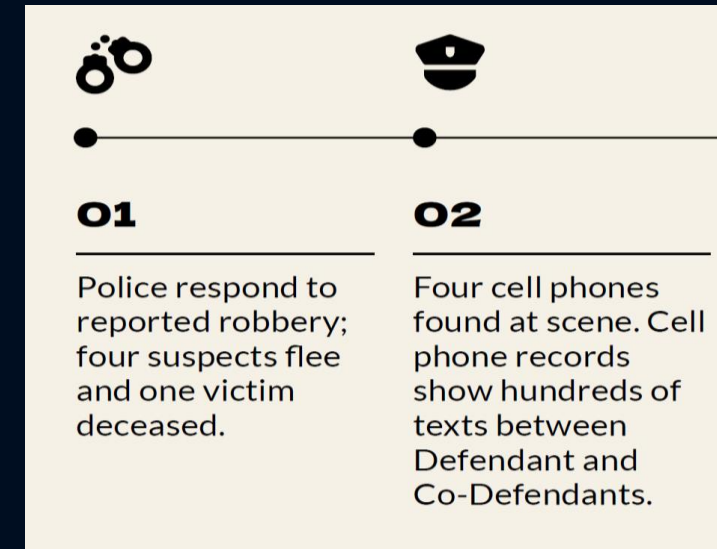
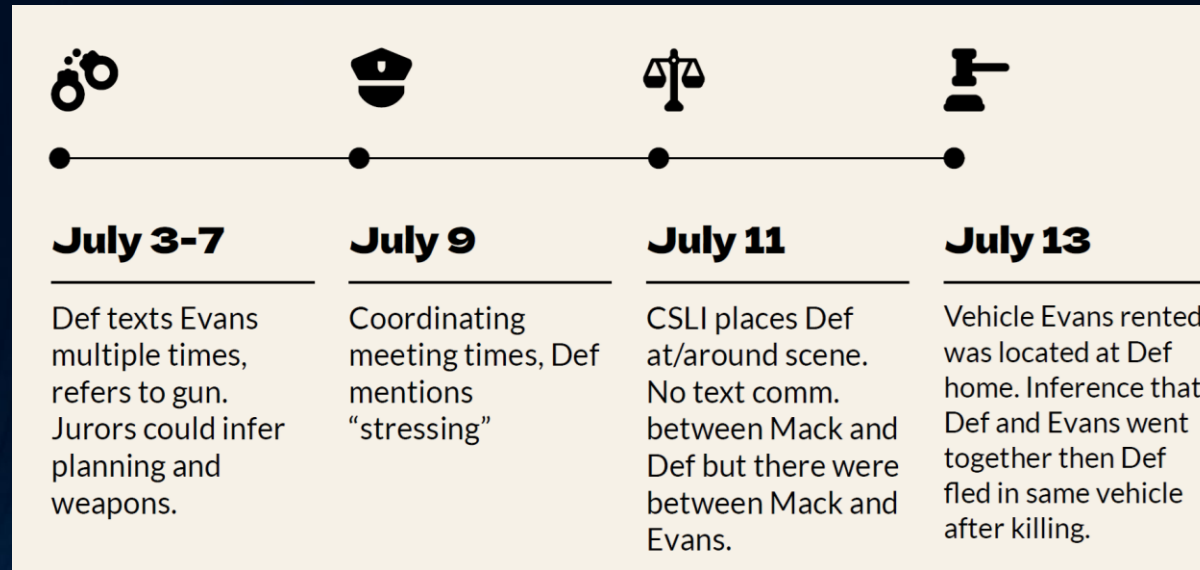
Commonwealth v. Purdy, 459 Mass. 442 (2011)

Online communications must have “confirming circumstances” to establish that they are “what [their] proponent claims [them] to be.”

- Chain of Custody: route of message + sender had primary access to computer
- Content of e-mail: refers to matters of which the writer would be aware (self-authenticating)
- Recipient used the reply function to respond (includes sender’s original message)
- Subsequent action: sender takes action consistent with content (after sending or receiving)

Authentication SODSI: "Some Other Dude Sent It"

Commonwealth v. Webster, 480 Mass. 161 (2018)



Insufficient Proof it's Co-Perp's Phone! Not associated with him & no one said it was his number

- Phone data indicated user had communications with defendant, co-defendants, and person with same name that co-perp told police is the name of his mother.
- Street name was "trigger" and number in co-perpetrator's phone as TR.
- All four men involved in robbery communicated by cell with each other and other's numbers were clear on record.
- Only one number left. Circumstantial evidence supported reasonable inference that final number was co-perp.

Same as When Found: Forensics



<https://youtu.be/RdwcUXij6HM>

Cases

All Users

Default

DPaparc

Appli

Cook

Desk

Favc

Loca

My D

B

C

D

D

Table

Gallery

Timeline

Report

	Name	Filter	File Ext	File Type	File Category	Signature
<input type="checkbox"/>	41 telephone company...		doc	Word Document	Document	
<input type="checkbox"/>	42 TelephoneCompani...		doc	Word Document	Document	
<input type="checkbox"/>	43 _ODO.TXT		TXT	Text	Document	
<input type="checkbox"/>	44 TUCOFS - The Ultim...		htm			
<input type="checkbox"/>	45 FBI Academy.ppt		ppt	MS Powerpoint Templa	Document\Presentatio	
<input type="checkbox"/>	46 _AMPLE.DOC		DOC	Word Document	Document	
<input type="checkbox"/>	47 _WRL0001.TMP		TMP	Windows Temporary	Windows	
<input checked="" type="checkbox"/>	48 _AMPLE.DOC		DOC	Word Document	Document	
<input type="checkbox"/>	49 Sample.jpg		jpg	JPEG	Pictures	
<input type="checkbox"/>	50 samplebefore.bmp		bmp	Bitmap Image	Pictures	

```

01050 .....
01155 .....
01260 .....
01365 Ã40Ã·p.....í·0·ý.....
01470 .....Û...This is a demonstration of recovering d
01575 eleted files and photos from a seized computer. When people delete files and empty their recycling bin th
01680 e information is not removed from the computer. The only thing that is removed is the header of the file
01785 the data remains on the hard drive. At some point the data may be over written, but with the size of har
01890 d drives today it still remains. As you type in word or excel the program automatically saves your wor
01995 k ever so many minutes and dumps this in unallocated space of the drive and we can find remnants of the l
02100 etter or work in unallocated clusters. March 6, 2003 .....
02205 .....
02310 .....

```

Authentication & Relevance



- ☐ Is Computer Generated Data Reliable?
 - ☐ Data Reliable¹
 - ☐ Reasonable Inference Tested ²
- ☐ Need Expert?
 - ☐ Testing Results
 - ☐ Interpretation
 - ☐ Anomalous Behavior
 - ☐ Absence Evidence
 - ☐ Technical

¹ FRE 901(b)(9) "*Evidence About a Process or System*. Evidence describing a process or system and showing that it produces an accurate result."

² *Commonwealth v. Davis*, 487 Mass. 448 (2021)

Event Recreation & Multimedia Presentations

The History of Forensic Animation in the Courtroom

November 16, 2022



by Jason Fries, CEO of 3D Forensic, and Sean Daly, Director of Public Relations, 3D Forensic

Court cases have always relied on visual aids to break down complex incidents. This once entailed using hand-drawn illustrations or photographs to communicate key aspects of a case. This was the standard throughout most of the 20th century until computers streamlined the litigation process. Storing, sharing, and communicating case material became instant and cleaner with this innovation.

As computer and visual technology advanced, the potential for forensic visualization grew through animation. Today, it is common for accidents and critical incidents to be demonstrated through digital animation so audiences can clearly see the critical factors of incidents. Through years of legal and technological refinement, animation has become the standard in modern forensic visualization.

Early years

Forensic animation first took shape in the American court system in 1988 with the tragic Delta 191 plane crash in Dallas, TX. This crash killed 137 people and occurred because the flight crew was unaware of severe weather near the runway. The trial for this case would become the longest major aviation trial in US history, taking 14 months to litigate.

Z-Axis, a Colorado-based firm, was recruited by the Department of Justice to demonstrate the path of the plane as well as the forces acting upon it. The production itself took two years to complete and cost about \$250,000. Compared to modern 3D animations, this animation was very simple but laid the groundwork for demonstrating complex issues to an audience of lay people.

The second notable admission of courtroom animation was the criminal case of Jim Mitchell's homicide of his brother Artie in 1991 in Corte Madera, CA. This production became the first animation to be used in a criminal trial in the United States. Prosecutors worked with Alexander Jason of ANITE Group to produce an animation of the shooting based on ballistics and a 911 phone call from Artie's girlfriend at the time. Despite questions about the production's assertions of timing, this animation blazed a path for modern ballistic and shooting visualizations.



Accident reconstruction example

Hearsay

Hearsay

Hearsay = Computer-Stored Evidence:


Records/documents that were created by a human,
stored in electronic form

VS

Not Hearsay = Computer-Generated Evidence:

Direct output of computer program

Defenses



Train and CertifyManage Your TeamSecurity AwarenessResourcesGet Involved


Home > Blog > Analysis of e-mail and appointment falsification on Microsoft Outlook/Exchange

Robert-Jan Mora


Analysis of e-mail and appointment falsification on Microsoft Outlook/Exchange

August 26, 2009

Summary

In digital forensic analysis it is sometimes required to be able to determine if an e-mail has or has not been falsified. In this paper a review of certain Outlook Message Application Programming Interface (MAPI)  is provided which can help in determining falsified e-mails or altered appointments in an Microsoft Outlook/Exchange environment.

About the libpst Project

In 2008 Joachim Metz a forensic investigator at Hoffmann Investigations started the libpst project. At that time the best source about the Personal Folder File (PFF) format in the public domain was the libpst  project. The libpst project dated back to 2002 and had been contributed and maintained by David Smith, Joe Nahmias, Brad Hards and Carl Byington.

However the libpst, at that time, wasn't a library and had no support for recovering deleted items in PST and OST

Subscribe to SANS

Receive curated news & security awareness

Your Email...

Select your country

By providing this info I agree to the processing of my personal data by SANS according to our [Privacy Policy](#).

[SANS Digital Forensics and Incident Response Blog | Analysis of e-mail and appointment falsification on Microsoft Outlook/Exchange | SANS Institute](https://www.forensictmag.com/592144-New-Technology-Creates-Digital-Alibis/)

New Technology Creates 'Digital Alibis'

November 18, 2022 | Michelle Taylor Editor-in-Chief

 Tweet  Share  Email

If you have a map app and location services enabled on your phone, it pretty much knows where you are 24/7/365. Well, it knows where it is—not necessarily you.

That's a problem when it comes to alibis for law enforcement. Confirming a personal device was in a specific place at a specific time is easy, confirming that the owner of said device was also there is not as easy.

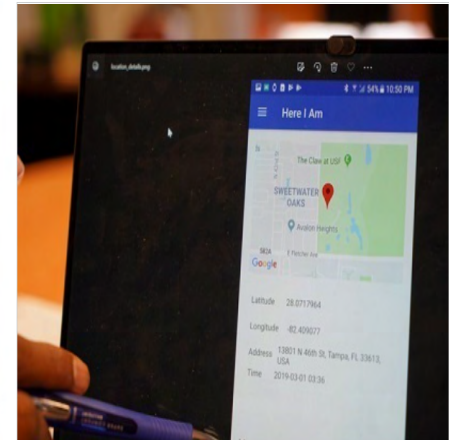
After years of research, computer science experts Sriram Chellappan and Balaji Padmanabhan concluded the most efficient way to overcome this hurdle would be to combine a person's voice with the location, date and time—a foolproof way for someone to prove they were at a specific place at a certain time.

"When law enforcement is investigating a crime, it is very common for those who are detained to be unable to generate verifiable alibis and that becomes a critical liability," said Chellappan. "They can't return to work, may lose their job and as a result, lose their income. I thought there must be a way to fix this and prove people's true location, when needed."

Chellappan and Padmanabhan's collaboration resulted in a patented technology called "Here I Am," which creates an unforgeable, encrypted digital certificate on a user's cellular device. The University of South Florida professors are currently in the process of licensing the technology.

"Most location authentication technologies today mainly authenticate a device, such as a phone, but not the user. Nothing like this exists," said Padmanabhan. "If companies with reliable location identification can offer this as a service, then individual users can easily generate their own authentication as needed."

In the prototype, a Here I Am user initiates a request to generate an authentication certificate. The user is then prompted to read a message out loud. While reading, the user's device will record their voice, which is paired by a server with the date, time and precise location data to create a cryptographically verifiable certificate that forever preserves the information on the user's device.



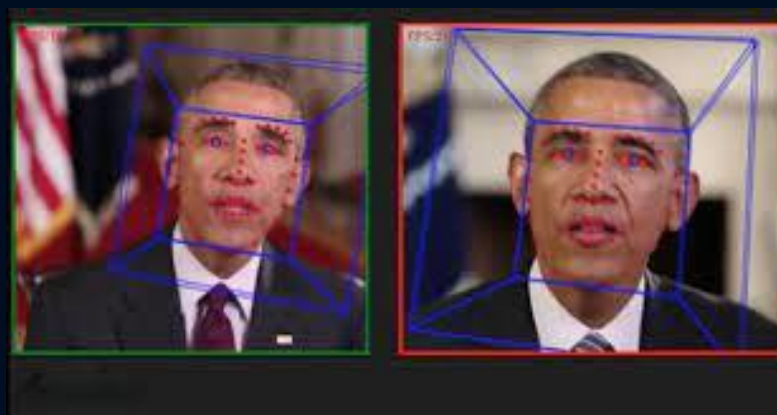
The Here I Am app, developed by two University of South Florida researchers, can accurately confirm an individual's identity and location using their voice, creating a digital alibi. Credit: University of South Florida

<https://www.forensictmag.com/592144-New-Technology-Creates-Digital-Alibis/>

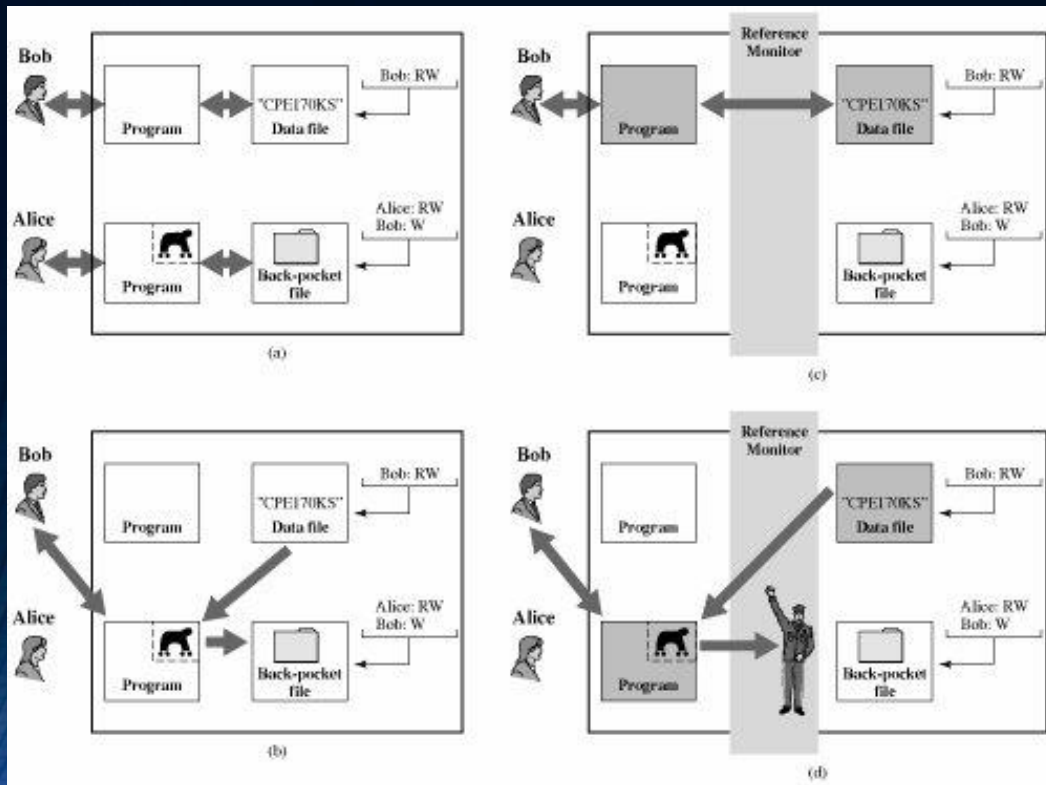
Digital Alibi: Long Shot



Deepfakes



Set Up by Malware¹



<https://flylib.com/books/en/3.190.1.165/1/>

How Digital Analysts Manage the Impact of Malware

February 04, 2022 | Heather Mahalik, Senior Director of Digital Intelligence

[Tweet](#) [Share 3](#) [Share](#) [Email](#)

co-authored by Jean-Philippe Noat, Senior Director of Strategic Advisory Services/International, Cellebrite

Malware plagues just about all organizations – from major financial services companies and healthcare facilities, down to mom-and-pop shops and sole-proprietor businesses. Law enforcement agencies and digital forensics labs aren't immune to the disruptive and dangerous effects of malware either. Even analysts and examiners who are savvy about detecting and avoiding cyber attacker exploits, such as phishing emails with links that lead to malware, must grapple with devices and files that may have malware, and might infect other digital tools in the lab setting.

Fortunately for analysts and examiners, their own know-how, along with protections built into Digital Intelligence software and hardware solutions, can protect their workflows and the wider law enforcement team from falling victim to malware. (Digital Intelligence is the data collected and preserved from digital sources and data types – such as smartphones, computers, and the cloud – and the process by which agencies collect, review, analyze, manage, and obtain insights from this data to more efficiently run their investigations.)

Why worry about malware?

For law enforcement agencies working to bring criminals to justice and protect citizens, the dangers of malware go beyond corrupted files and stolen data. If the digital evidence process isn't secured against malware – and if the processes are not documented – defense attorneys gain a foot in the door to protest the legitimacy of evidence. Defense could claim that text messages or emails attributed to a suspect could have been altered by malware, and that someone else in fact created those messages. That's a long-shot argument, but it's enough to raise doubt in a jury.

Examiners need to anticipate tough questions about malware protection and document the steps taken to prevent malware infections in systems that touch digital evidence. The steps and tips below can help law enforcement teams demonstrate that proper protocols have been followed to guard against malware and maintain the chain of custody.

Check for malware immediately after extracting data from a mobile device.



Heather Mahalik, Senior Director of Digital Intelligence & Jean-Philippe Noat, Senior Director of Strategic Advisory Services/International, Cellebrite, "How Digital Analysts Manage the Impact of Malware" (Feb. 2022) <https://www.forensicmag.com/3425-Featured-Article-List/583193-How-Digital-Analysts-Manage-the-Impact-of-Malware/>

Josh Duggar¹



“His activity was found in connection with an undercover investigation involving a file-sharing program”

- geolocated the computer to Duggar's car lot and then
- matched the timing of the image downloads to times Duggar was at the lot.
- including “times when Duggar was the “only paid employee on the lot.”

Defense Expert testified:

- “internet network [where downloaded illegal images] was so insecure” that anyone could hijack “his computer to remotely watch child porn in a so-called 'hit and run attack.’
- She described a scenario whereby a remote user, or hacker, could potentially log on, do something nefarious, then quickly log off again without the account holder ever knowing.
- Likening Duggar's network to a house, she said: 'All of its doors are unlocked. Anyone can come in and they can do what they want.’”

¹ [Josh Duggar found guilty in child sex abuse image trial \(nbcnews.com\)](https://www.nbcnews.com/news/10284627/Josh-Duggar-Computer-forensics-expert-says-Duggars-internet-network-insecure.html) & <https://www.dailymail.co.uk/news/article-10284627/Josh-Duggar-Computer-forensics-expert-says-Duggars-internet-network-insecure.html> & <https://www.dailymail.co.uk/news/article-10284627/Josh-Duggar-Computer-forensics-expert-says-Duggars-internet-network-insecure.html>

Opportunity #3: Evidence

- Authentication & Relevance
 - ID
 - Reliable
 - Trustworthy
- Digital Defenses
- Expertise





<https://www.latimes.com/california/story/2021-05-04/3-men-dead-in-anaheim-car-crash-driver-found-after-fleeing-the-scene>



<https://twitter.com/i/status/1389691159237201924>

How a Determined Detective Caught a Cyberstalker

[High School Stalker Caught by Detective |
Reader's Digest \(rd.com\)](#)



Other Instructive Cases

- [Italian Mafia Fugitive Caught In Spain Thanks to Google Maps - The New York Times \(nytimes.com\)](#)
- [Doctor arrested in death of Boston delivery truck driver shot, killed in Vermont \(wcvb.com\)](#)
- [He Built a Home to Survive a Civil War. Tragedy Found Him Anyway.](#)

General Online Resources

- Digital Forensics (forensicmag.com)
 - Subscribe to their eNewsletter: On the Scene and in the Lab - Forensic® (forensicmag.com)
- National Institute of Justice (NIJ): Publications re: Digital Evidence Forensics
- American Academy of Forensic Sciences (aafs.org)
- Massachusetts Digital Evidence Consortium: Digital Evidence Guide for First Responders

Criminal Procedure: Investigation Resources

- United States Secret Service: Best Practices for Seizing Electronic Evidence [Electronic Evidence – Guide for First Responders \(publicintelligence.net\)](https://publicintelligence.net/electronic-evidence-guide-for-first-responders)
- National Institute of Justice: Forensic Examination of Digital Evidence: A Guide for Law Enforcement <https://www.ncjrs.gov/pdffiles1/nij/199408.pdf>
- National Institute of Justice: Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition <https://www.ncjrs.gov/pdffiles1/nij/219941.pdf>
- National Institute of Justice: Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders <https://www.ncjrs.gov/pdffiles1/nij/227050.pdf>
- Department of Justice: Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations <http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf>

Evidence: DE in the Courtroom

- National Institute of Justice: Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors
<https://www.ncjrs.gov/pdffiles1/nij/211314.pdf>
- **DFS101: 5.3 Digital Investigation Procedure**
https://www.youtube.com/watch?v=ZTZ_GnFR-GE
- Authenticating Digital Evidence, 69 Baylor L. Rev. 1 (Winter 2017).
- Mass. G. Evid. [Article XI: Section 119: Digital Evidence](#)
- Jury Instructions: [3610 Authentication of Digital Evidence.docx \(mass.gov\)](#)

Learn More

- ❑ Find a TA or RA with IT or Digital Experience
- ❑ Talk to an “Expert” Inside or Outside of Your Institution
- ❑ Watch a CLE on the Subject

<https://www.mcle.org/product/catalog/code/2190126P01>



Product Number: 2190126P01

CLE Credits, earn up to:
3 substantive credits, 0 ethics credits
CLE Credit Note

[Print Brochure](#)

[Add to Favorites List](#) ▼

The Investigative Art of Digital Forensics

Finding and using the information hidden in electronic devices

Choose Date/Location:



In-Person Program

Wednesday, 3/27/2019, 9:30 am – 12:30 pm, MCLE Conference Center, Ten Winter Place, Boston



Live Webcast

Wednesday, 3/27/2019, 9:30 am – 12:30 pm, Live Webcast, www.mcle.org, Live Webcast



Recorded Webcast

Wednesday, 4/10/2019, 2:00 pm – 5:00 pm, Recorded Webcast, www.mcle.org, Recorded Webcast

Registration for this program is closed

Also Available:



MP3 Download [Add to Cart](#)

Includes downloadable supporting materials.
\$245.00; Sponsor Members \$220.50; New Lawyers \$122.50
Free for OnlinePass subscribers.



On Demand Webcast [Add to Cart](#)

Includes downloadable supporting materials.
\$245.00; Sponsor Members \$220.50; New Lawyers \$122.50
Free for OnlinePass subscribers.



Related eLectures

See Agenda below to purchase individual video segments from this program.
Price per video: \$65.00; Sponsor Members \$58.50; New Lawyers \$32.50
Free for OnlinePass subscribers.

Christina Miller
Associate Clinical Professor
cmiller3@suffolk.edu

