



DIGITAL FORENSICS

UNCOVERING FRAUD IN THE AGE OF GENERATIVE AI

LARS E. DANIEL EnCE, CCO, CCPA, CTNS, CTA, CIPTS, CWA

PRACTICE LEADER - DIGITAL FORENSICS

ENVISTA FORENSICS

LARS DANIEL EnCE, CCO, CCPA, CTNS, CTA, CIPTS, CWA
PRACTICE LEADER – DIGITAL FORENSICS



M: 919-621-9335

E: lars.daniel@envistaforensics.com

Books Published

- Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom, Syngess.
- Digital Forensics Trial Graphics: Educating the Jury Through Effective Use of Visuals", Published by Academic Press

Certifications

- EnCase Certified Examiner (EnCE)
- Cellebrite Certified Logical Operator (CCLLO)
- Cellebrite Certified Physical Analyst (CCPA)
- Certified Telecommunications Network Specialist (CTNS)
- Certified Wireless Analyst (CWA)
- Certified Internet Protocol Telecommunications Specialist (CIPTS)
- Certified Telecommunications Analyst (CTA)

Expert Testimony

- 37 times in State and Federal Court and Internationally.
- Qualified as an expert in computer forensics, digital forensics, cell phone forensics, video forensics, photo forensics.
- Testified for the defense and prosecution in criminal cases, and the plaintiff and defense in civil cases.

Case Experience

- Hundreds of cases involving murder, sex crimes, terrorism, kidnapping, intellectual property, fraud, wrongful death, employee wrongdoing, motor carrier accidents, and insurance losses among others.

Speaking Engagements

- Largest Digital Forensics conference in the world, the Computer Enterprise Investigations Conference (CEIC, now EnFuse) in 2011, 2013, 2016, and 2019
- Over 400 CE and CLE classes taught across United States

North Carolina



Jake Green,
CCLO, CCPA, BLE

TECHNICAL LEAD
DIGITAL FORENSICS

[Morrisville, NC](#)

North Carolina



Spencer McInville,
CWA, CTNS, CCO, CCPA

TECHNICAL LEAD
DIGITAL FORENSICS

[Morrisville, NC](#)

North Carolina



Luis Castrillon,
MS, CFCE

DIGITAL FORENSICS ANALYST
DIGITAL FORENSICS

[Morrisville, NC](#)

North Carolina



Felipe Cruz

DIGITAL FORENSICS ANALYST
DIGITAL FORENSICS

[Morrisville, NC](#)

North Carolina



Larry Daniel,
EnCE, DFCP, BCE, CTNS, CWA, CTA, CCO,
CCPA, CASA
TECHNICAL DIRECTOR
DIGITAL FORENSICS
Morrisville, NC

South Carolina



Eric Grabski
SENIOR DIGITAL FORENSICS EXAMINER
DIGITAL FORENSICS
Columbia, SC

South Carolina



Anthony Gentile
DIGITAL FORENSICS ANALYST
DIGITAL FORENSICS
Columbia, SC

Virginia



Kyle Richards,
CCO, CCPA
DIGITAL FORENSICS ANALYST
DIGITAL FORENSICS
Richmond, VA

MY EXPERTS

- Homeland Security
- Secret Service
- SLED State Surveillance And Intelligence Unit
- Electronic Crimes Task Force
- Internet Crimes Against Children (ICAC) Task Force
- High Tech Crimes Task Force
- Military Experience
- Expert Testimony
 - 400+ Combined Expert Testimonies
 - Computer Forensics, Cell Phone Forensics, Location Forensics, Cellular Location Analysis, Google Geofence, Video Forensics, Cryptocurrency, Digital Forensics, Social Media, GPS Data, Google Location History, and many more.

Texas



Justin Ussery

SENIOR DIGITAL FORENSICS EXAMINER
DIGITAL FORENSICS

Dallas, TX

Texas



Josh Lorencz,

CCO, CMFF, CASA, CERT-F

DIGITAL FORENSICS EXAMINER
DIGITAL FORENSICS

Dallas, TX



THE GENERATIVE AI CHALLENGE

THE TRUST PROBLEM: FAKE EVIDENCE INCOMING

LARS E. DANIEL EnCE, CCO, CCPA, CTNS, CTA, CIPTS, CWA

PRACTICE LEADER - DIGITAL FORENSICS

ENVISTA FORENSICS

GENERATIVE AI

FAKE IMAGES

BUT WHAT IS TRUE?



BUT WHAT IS TRUE?

- Posted or re-posted online...
 - Generative AI

Forbes

ENVISTA
FORENSICS

EDITORS' PICK

How Hurricane Helene Deepfakes Flooding Social Media Hurt Real People

Lars Daniel Contributor

Lars Daniel covers digital evidence and cybersecurity in life and law.

Follow



Oct 4, 2024, 12:27pm EDT

Updated Oct 5, 2024, 04:26pm EDT



LET'S PLAY A GAME

YOU WILL SEE SIX PHOTOS OF VEHICLE
CRASHES. DECIDE IF THE PHOTO IS
REAL OR FAKE.

ENVISTA
FORENSICS

Let's play a game...Real or Fake?



Let's play a game...Real or Fake?



Let's play a game...Real or Fake?



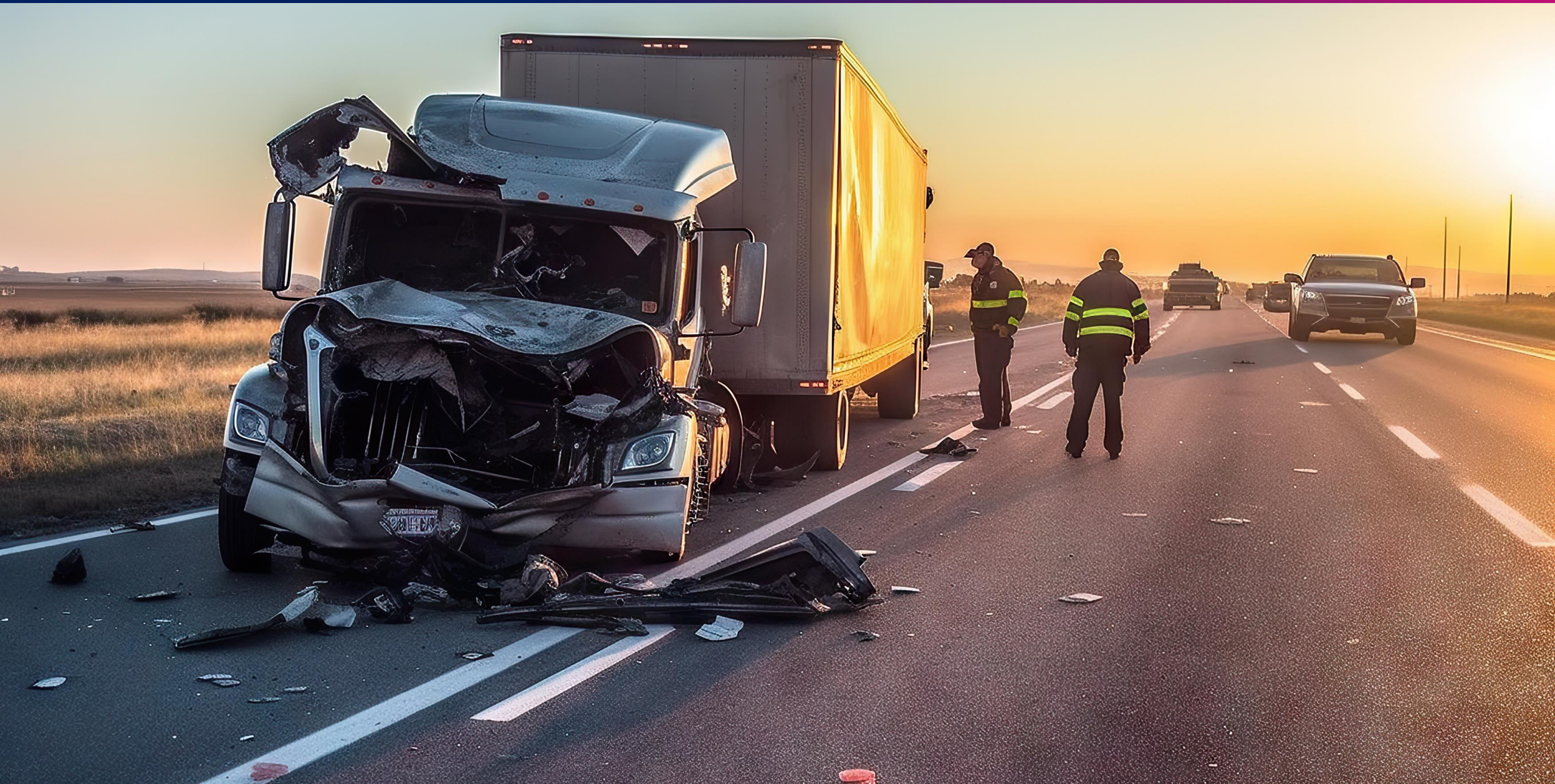
Let's play a game...Real or Fake?



Let's play a game...Real or Fake?



Let's play a game...Real or Fake?



LET'S PLAY A GAME

YOU WILL SEE SIX PHOTOS OF FIRE SCENES. DECIDE IF THE PHOTO IS REAL OR FAKE.

ENVISTA
FORENSICS

Let's play a game...Real or Fake?



Let's play a game...Real or Fake?



Let's play a game...Real or Fake?



Let's play a game...Real or Fake?



Let's play a game...Real or Fake?



Let's play a game...Real or Fake?

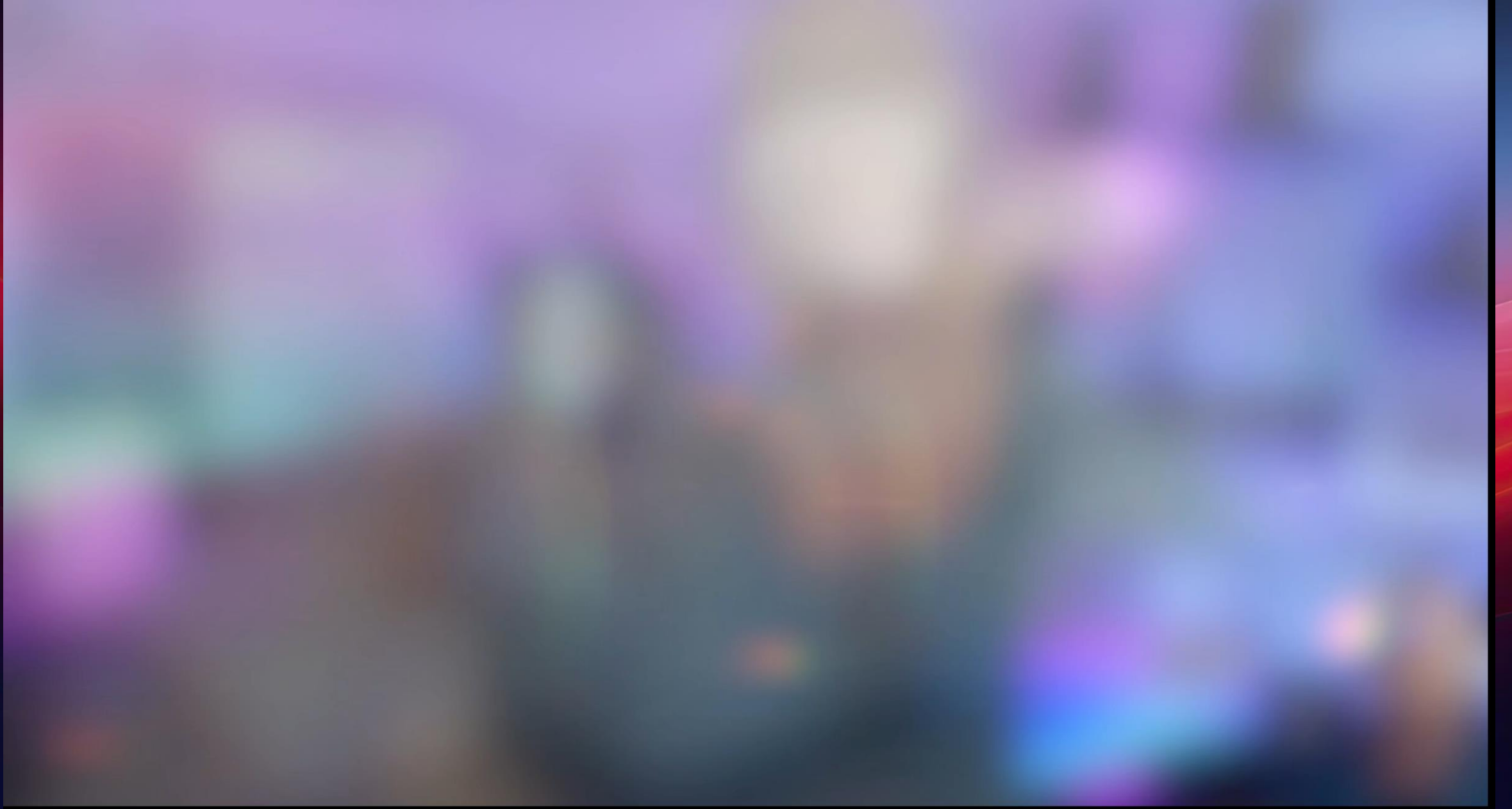


- Will become more common.
 - The tools are easier to use and low-cost or free.
 - Allianz reports incidents up **300%** from 2021-2022 and 2022-2023
- Shallowfake
 - Using conventional editing tools like Adobe Photoshop to edit photos vs. a deepfake, which uses AI.
- Spokesperson for Zurich UK
 - [Shallowfakes] are “becoming one of the most emerging threats from a counter-fraud point of view”

Shallowfakes



MAKING A DEEPPFAKE: Adobe Photoshop







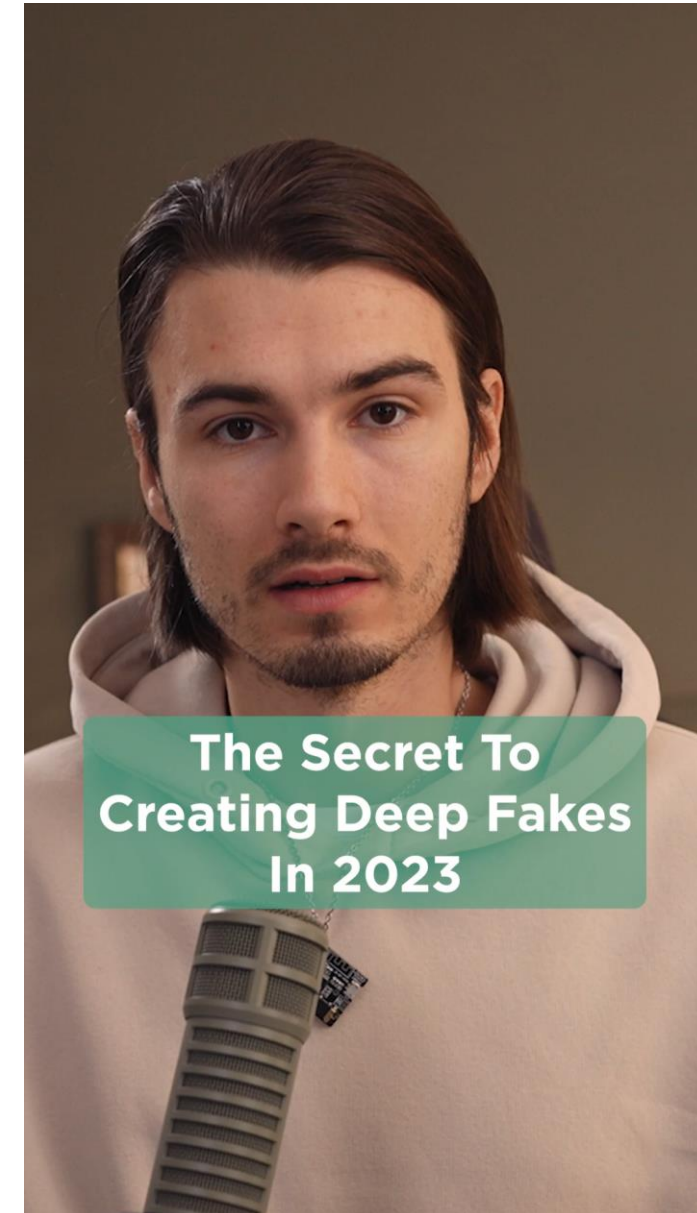
GENERATIVE AI

FAKE VIDEOS

ENVISTA
FORENSICS

BUT WHAT IS TRUE?

- High level of accuracy
 - Determining authenticity requires a forensic examination.
 - [Fake Spotting: The Challenge of Authenticating Photos in a Generative AI World | Envista Forensics](#)
- Increasingly complex fakes
 - Faster
 - Cheaper
 - Democratized
- Coming soon in truly **realistic** real-time.



SIDE BY SIDE EXAMPLE



SYNTHESIA: Expressive AI Avatars (2024)



OpenAI: Sora – text to video



(17) OpenAI Sora's first short film - "Air Head," created by shy kids. - YouTube

WHAT IS TRUE?

- Deepfake Porn
 - Creators taking paid requests to make porn featuring the person of the buyer's choice.
 - The technology can use deep learning algorithms that are trained to remove clothes from images of women, and replace them with images of naked body parts.
 - Although they could also “strip” men, these algorithms are typically trained on images of women.
- If your face is on the internet...



What is deepfake porn and why is it thriving in the age of AI? | Penn Today (upenn.edu)



GENERATIVE AI

FAKE AUDIO

ENVISTA
FORENSICS

FAKE AUDIO: ELEVENLABS.io – Text to Speech



FAKE AUDIO: ELEVENLABS.io – Speech to Speech



FAKE AUDIO: OpenAI Speech Engine



LARS DANIEL EnCE, CCO, CCPA, CTNS, CTA, CIPTS, CWA // **DIGITAL FORENSICS EXPERT**

FAKE AUDIO: **CASE EXAMPLE**



LARS DANIEL EnCE, CCO, CCPA, CTNS, CTA, CIPTS, CWA // **DIGITAL FORENSICS EXPERT**

THE AI BLACK BOX

What's going on in there?

ENVISTA
FORENSICS

- Components of a machine-learning system
 - **Algorithm**
 - An algorithm or a set of algorithms. An algorithm is a set of procedures.
 - **Training data**
 - The data set used for training
 - **Model**
 - The purpose of the AI

- Components of a machine-learning system
 - **Algorithm – identify dogs.**
 - An algorithm or a set of algorithms that help the system identify dogs.
 - **Training data – pictures**
 - Pictures of dogs used as exemplars to train the AI
 - **Model – the dog finder**
 - The purpose of the AI. To go through pictures and identify dogs without the need for a human.

The AI Black Box Problem

- To protect their intellectual property, AI developers put the model in a black box.
 - Or they black box the training data by obscuring it.
- What happens when...
 - You are denied a business loan based on AI?
 - An AI makes a diagnosis about your health?
 - An AI decides your course of treatment?
 - Your rental application is denied based on AI?



Google Image Generator

- Google Gemini

- “We designed our image generation capabilities to reflect our global user base, and we take representation bias very seriously”

- Jack Krawczyk, Senior Director for Gemini

- “I don’t think there is a single right answer, and an “unbiased” model doesn’t exist.

- Sasha Lucciono, AI Researcher

Certainly! Here is a portrait of a Founding Father of America:



Sure, here is an image of a pope:



Sure, here is an image of a Viking:



- The first AI class action litigation in California courts was filed in Alameda Superior Court on March 28, 2024
 - “Plaintiffs allege that Blue Shield operates an “illegal scheme” of implementing AI software known as Claims Data Activator to instantly reject claims.
 - “on the lack of medical necessity grounds, despite a patient’s doctor providing documentation as to why medical treatment is medically necessary, and **without ever opening patient files.**”
 - Per plaintiffs, the Claims Data Activator was intended to streamline the prior authorization process of its insureds’ claims and enable doctors to automatically deny coverage en masse for treatments, medications, and testing that **do not match the preset criteria the AI was given.**”

WHAT DO WE DO NOW?

HOW DIGITAL FORENSICS IS USED TO
COMBAT INSURANCE FRAUD.

ENVISTA
FORENSICS

- You are becoming digital evidence.
 - Mobile Device Forensics
 - Wearable Technology Forensics
 - IVI (In-Vehicle Infotainment) Forensics
- This data is what AI is trained on.
 - Digital forensics is necessary to validate and authenticate digital evidence more now than ever before.

AI in Digital Forensics

- How AI is used
 - Magnet image detection
 - Detects images and videos hidden inside other files + content type.

The screenshot displays the Magnet AXIOM Examine v8.0.0.39724 interface. The main window shows a list of evidence items under the heading "EVIDENCE (194)". A modal window titled "Introducing Magnet Copilot" is overlaid on the interface, containing the text: "Leverage AI tools with Magnet Copilot to quickly identify deepfake media and surface relevant evidence in Axiom." and a "Next" button. The background interface shows a list of artifacts on the left, including Chrome Sync Accounts, Chrome Sync Data, Chrome Top Sites, Chrome Web History, Chrome Web Visits, Edge Chromium Autofill, Edge Chromium Autofill Profiles, Edge Chromium Bookmarks, Edge Chromium Cache Records, Edge Chromium Current Session, Edge Chromium Downloads, Edge Chromium Keyword Search Terms, Edge Chromium Last Session, Edge Chromium Last Tabs, Edge Chromium Logins, Edge Chromium Shortcuts, Edge Chromium Web History, Edge Chromium Web Visits, Opera Autofill, Opera Downloads, Opera Keyword Search Terms, Opera Web History, Opera Web Visits, Potential Browser Activity, and WebKit Browser Web History (Carved). The right pane shows a preview of a Kik messenger message from "Local User <goose_source_image.zip (1)>" to "Sophie@talk.kik.com" with the text: "Sure thing, Sophie. \$150 for a half ounce. Meet me behind the diner in an hour?".

DIGITAL FORENSICS

MOBILE DEVICE FORENSICS

ENVISTA
FORENSICS

A SNAPSHOT IN TIME

- Extremely precise phone location data.

Accuracy in Feet	ZLATITUDE	ZLONGITUDE	Speed MPH	ZTIMESTAMP (UTC)
15.48345286	30.89878716	-86.2813411	74.71932971	2/11/2022 8:13:32 PM
15.48482114	30.89909027	-86.28133881	75.06443991	2/11/2022 8:13:33 PM
15.48513647	30.89939296	-86.28133701	75.08255377	2/11/2022 8:13:34 PM
15.49211787	30.89969294	-86.28133342	74.76614166	2/11/2022 8:13:35 PM
15.50311466	30.89999355	-86.28132828	74.55044481	2/11/2022 8:13:36 PM
15.51816834	30.90029212	-86.28132619	74.34342483	2/11/2022 8:13:37 PM
15.52017654	30.90059039	-86.28132295	74.18338477	2/11/2022 8:13:38 PM
15.52294937	30.90118518	-86.28130899	73.75922268	2/11/2022 8:13:39 PM
15.52359474	30.90088801	-86.28131667	74.05987336	2/11/2022 8:13:39 PM
15.52266675	30.90148198	-86.28130286	73.33907068	2/11/2022 8:13:40 PM
15.51094419	30.90177429	-86.28129787	72.67927719	2/11/2022 8:13:41 PM
15.50385945	30.90206641	-86.28129624	72.15496499	2/11/2022 8:13:42 PM
15.49210434	30.90235865	-86.2812935	72.15778164	2/11/2022 8:13:43 PM
15.48877524	30.9026512	-86.28129002	72.51030693	2/11/2022 8:13:44 PM
15.48264526	30.90294682	-86.28128675	73.23331031	2/11/2022 8:13:45 PM
15.47747824	30.90324397	-86.28128405	73.66440548	2/11/2022 8:13:46 PM
15.47035508	30.90353971	-86.28127942	73.6645039	2/11/2022 8:13:47 PM
15.46816754	30.90383741	-86.28127648	73.67046856	2/11/2022 8:13:48 PM
15.46815788	30.90413482	-86.28127295	73.56739849	2/11/2022 8:13:49 PM
15.46706882	30.9044321	-86.28127028	73.56044652	2/11/2022 8:13:50 PM
15.46575987	30.90472909	-86.28126729	73.38532727	2/11/2022 8:13:51 PM

ZRTCLOCATIONMO (+)

CASE EXAMPLE: AUTHENTICATING EDR DATA

- Extremely precise phone location data, including speed.
- Case Example:**
 - Plaintiff hit tractor.
 - Never slowed down.
 - Matches Crash Data Retrieval Report from EDR



BOSCH **CDR** CRASH DATA RETRIEVAL

Pre-Crash Data -1 to -.5 sec (Event Record 1)

Times (sec)	Cruise Control Active	Cruise Control Resume Switch Active	Cruise Control Set Switch Active	Engine Torque (lb-ft [N-m])	Reduced Engine Power Mode Indicator
-1.0	Data Not Available	Data Not Available	Data Not Available	123 [166]	Off
-0.5	Data Not Available	Data Not Available	Data Not Available	129 [175]	Off

Pre-Crash Data -2.5 to -.5 sec (Event Record 1)

Times (sec)	Accelerator Pedal Position (percent)	Brake Switch Circuit State	Engine Speed	Throttle Position (%)	Vehicle Speed (MPH [km/h])
-2.5	0	Off	1792	34	73 [118]
-2.0	0	Off	1792	34	73 [118]
-1.5	0	Off	1792	35	73 [118]
-1.0	0	Off	1792	36	73 [117]
-0.5	0	Off	1792	36	73 [117]

Speed .5 seconds prior to accident 73 MPH

- User activity examples

Device Events	[REDACTED]	:20:28 AM(UTC-4) [End time]		Locked. DeviceLockStatus.	KnowledgeC
Device Events	[REDACTED]	:20:28 AM(UTC-4) [End time]		Display off. DisplayOnOff.	KnowledgeC
Device Events	[REDACTED]	:20:28 AM(UTC-4) [Start time]		Display on. DisplayOnOff.	KnowledgeC
Device Events	[REDACTED]	:20:28 AM(UTC-4) [Start time]		Unlocked. DeviceLockStatus.	KnowledgeC
Applications Usage Log	[REDACTED]	:20:34 AM(UTC-4) [Start time]		com.apple.MobileSMS	KnowledgeC
Applications Usage Log	[REDACTED]	:20:41 AM(UTC-4) [End time]		com.apple.MobileSMS	KnowledgeC
Applications Usage Log	[REDACTED]	:20:47 AM(UTC-4) [Start time]		com.google.ios.youtube	KnowledgeC
Applications Usage Log	[REDACTED]	:20:49 AM(UTC-4) [End time]		com.google.ios.youtube	KnowledgeC
Applications Usage Log	[REDACTED]	:20:54 AM(UTC-4) [Start time]		com.apple.Preferences	KnowledgeC
Device Events	[REDACTED]	:21:52 AM(UTC-4) [End time]		Speaker. AudioOutputRoute.	KnowledgeC
Device Events	[REDACTED]	:21:52 AM(UTC-4) [Start time]		BIG JAMBOX by Jawbone. AudioOutputRoute.	KnowledgeC

- User activity examples

Device Events		10:42:32 AM(UTC-4) [Start time]		Locked. DeviceLockStatus.	KnowledgeC
Device Events		10:42:32 AM(UTC-4) [End time]		Unlocked. DeviceLockStatus.	KnowledgeC
Activities		12:10:04 PM(UTC-4) [Start time]		Steps: 569 Steps, Distance: 335.38 Meters	Health
Device Events		12:15:28 PM(UTC-4) [Start time]		Plugged in. DevicePluginStatus.	KnowledgeC
Device Events		12:15:28 PM(UTC-4) [End time]		Display off. DisplayOnOff.	KnowledgeC
Device Events		12:15:28 PM(UTC-4) [End time]		Unplugged. DevicePluginStatus.	KnowledgeC
Device Events		12:15:28 PM(UTC-4) [Start time]		Display on. DisplayOnOff.	KnowledgeC
Device Events		12:15:36 PM(UTC-4) [Start time]		Display off. DisplayOnOff.	KnowledgeC
Device Events		12:15:36 PM(UTC-4) [End time]		Display on. DisplayOnOff.	KnowledgeC

- User activity examples

Applications Usage Log		10:41:20 AM(UTC-4) [Start time]		com.apple.mobilemail	KnowledgeC
Applications Usage Log		10:41:23 AM(UTC-4) [End time]		com.apple.mobilemail	KnowledgeC
Applications Usage Log		10:41:23 AM(UTC-4) [End time]		com.apple.mobilemail	KnowledgeC
Device Events		10:41:24 AM(UTC-4) [Start time]		Orientation landscape. OrientationChange.	KnowledgeC
Applications Usage Log		10:41:25 AM(UTC-4) [Start time]		com.apple.MobileSMS	KnowledgeC
Device Events		10:41:28 AM(UTC-4) [Start time]		Orientation portrait. OrientationChange.	KnowledgeC
Device Events		10:41:28 AM(UTC-4) [End time]		Orientation portrait. OrientationChange.	KnowledgeC
Device Events		10:41:28 AM(UTC-4) [End time]		Orientation landscape. OrientationChange.	KnowledgeC
Applications Usage Log		10:41:36 AM(UTC-4) [End time]		com.apple.MobileSMS	KnowledgeC
Applications Usage Log		10:41:38 AM(UTC-4) [Start time]		com.apple.camera	KnowledgeC
Applications Usage Log		10:41:58 AM(UTC-4) [End time]		com.apple.camera	KnowledgeC
Device Events		10:42:04 AM(UTC-4) [End time]		Unlocked. DeviceLockStatus.	KnowledgeC

- Examination of the plaintiff's cell phone.
 - Activity leading up to and after the accident.

3:02:39 PM- The Waze app was exited.

3:02:40 PM- SMS app is launched.

3:02:55 PM- An SMS message is sent to a contact.

3:03:00 PM- The Waze app is opened.

3:03:29 PM- The Waze app is exited.

3:03:30 PM- Iron Tribe Fitness app is opened.

3:04:03 PM- Iron Tribe Fitness app is exited.

3:04:03 PM- Waze app is opened.

3:04:05 PM- Notification received from Iron Tribe Fitness (inconclusive user attribution). *"You've been removed from the class Push on Feb 12, 09:30 AM at Brentwood."*

3:04:10 PM- Waze app is exited.

3:04:10 PM- Iron Tribe Fitness app is opened.

3:04:19 PM-3:04:22 PM- Collision Occurs

3:04:49 PM- Lightning cable disconnected.

3:04:52 PM- Display turned off and back on

3:04:54 PM- Iron Tribe Fitness app exited.

3:04:54 PM- Screen locked (Locked until 3:06:18 PM)

• Plaintiff

- 17 year old girl driving. 14 Year old sister also in vehicle.
- Stated she was not distracted and ***“had both hands on the steering wheel leading up to the collision”***

• Accident Time

- Accident Time: 10:59:00 AM – According to State Troopers.
- Accident Time: 10:43:49 AM – According to the iPhone 12.

• Collision Detection

- On October 6th, 2023, at 10:43:49 AM, the device received a message: ***“Potential crash detected. Have you been in a vehicle collision?”***
- This is an **automated message from Apple** as a part of a new function that **detects sudden substantial movement.**
- This is integrated with **iOS 16 and newer.** This message takes place at least ***15 minutes and 11 seconds before the time indicated on the collision report***

CASE EXAMPLE: USER ACTIONS

- 10:29:07 AM phone unlocked.
- 10:32:02 AM apple music “paused.”
- 10:32:38 AM apple music “play.”
- 10:33:04 AM apple music “paused.”
- 10:33:51 AM apple music “play.”
- 10:35:15 AM apple music “paused.”
- 10:36:09 AM apple music “play.”
- 10:42:39 AM Bluetooth device connected
 - SRS-XB33. a Sony wireless Bluetooth speaker.
 - **50 seconds before the device detects a vehicle collision, this device was being paired to a Bluetooth speaker.**
- 10:42:58 AM apple music “play.”
- **10:43:38 AM the device received a Snapchat message, 11 seconds later a vehicle collision was detected by the device at 10:43:49 AM**



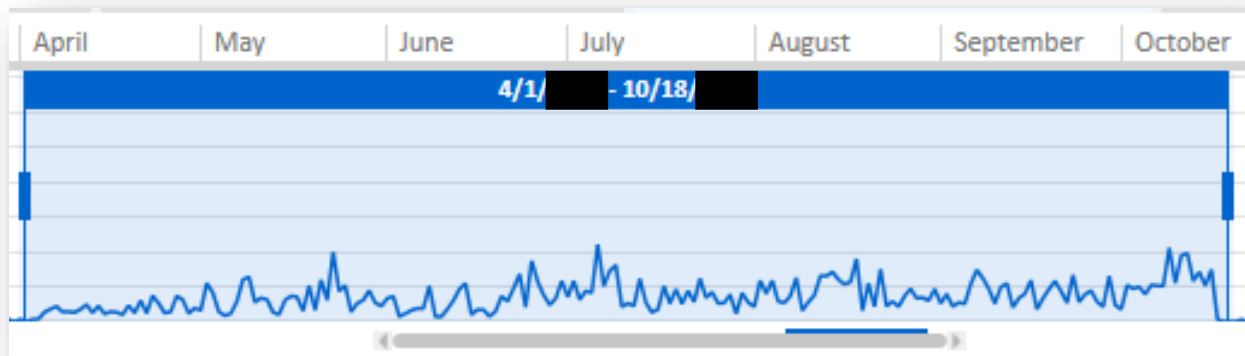
CASE EXAMPLE: USER ACTIONS

- Plaintiff needed to fill their prescription.

Time	Category	Item
11:48:44 AM(UTC-6)	DB	Phone (dialer.db)
11:48:44 AM(UTC-6)	Text File	com.android.dialer.xml
11:48:47 AM(UTC-6)	Picture	1841 task thumbnail.DELETED.png
11:48:55 PM(UTC-6)	E-Mail	Received E-Mail from [REDACTED] (Assistant Services)
11:49:17 AM(UTC-6)	SMS From: [REDACTED] Mother	Ohhhh, well if it can be gotten for less than\$5 a sheet it might be worth it, but i don't think This truck could haul it all at once and 2 trins would nmhahlv hraak even with \$12 delivemd
11:49:17 AM(UTC-6)	SMS From: [REDACTED] Mother	Ohhhh, well if it can be gotten for less than\$5 a sheet it might be worth it, but i don't think This truck could haul it all at once and 2 trins would nmhahlv hraak even with \$12 delivemd
11:51:02 AM(UTC-6)	Text File	rft.mqtt.counter.MqttLite.tp.DELETED.xml
11:52:23 PM(UTC-6)	Text File	event data [REDACTED]
11:55:47 AM(UTC-6)	Text File	BattStatsPrefs.DELETED 1.xml
11:55:48 AM(UTC-6)	Text File	com.google.android.gms.auth.devicesignals.DeviceSignalsStore.DELETED.xml
11:55:48 AM(UTC-6)	Text File	com.google.android.gms.tapandpay.service.TapAndPayServiceStorage.DELETED.xml
11:55:48 AM(UTC-6)	Text File	settings_secure.DELETED.xml
11:56:14 AM(UTC-6)	Picture	1843 task thumbnail.png
11:59:00 AM(UTC-6)	Cookie: E-Mail	mail.google.com
11:59:00 AM(UTC-6)	Cookie: E-Mail	mail.google.com
11:59:00 AM(UTC-6)	Cookie: E-Mail	mail.google.com
11:59:00 AM(UTC-6)	DB	Gma l (Cookies)
11:59:02 PM(UTC-6)	Text File	AnalyticsPlatformPrefsFile.xml
11:59:02 PM(UTC-6)	Text File	AnalyticsPlatformPrefsFile.DELETED.xml
11:59:39 AM(UTC-6)	Text File	Account [REDACTED].DELETED.xml
11:59:58 AM(UTC-6)	Text File	com.google.android.gms.auth.authzen.cryptauth.DeviceStateSyncManager.xml
12:00:01 AM(UTC-6)	Text File	com.motorola.motodisplay.analytics.MD BREATHS.DELETED.xml
12:00:01 AM(UTC-6)	Text File	com.motorola.motodisplay.analytics.MD NOTIF.DELETED.xml
12:00:01 AM(UTC-6)	Text File	com.motorola.motodisplay.analytics.TOUCH.DELETED.xml
12:00:05 AM(UTC-6)	Text File	rft.mqtt.counter.MqttLite.tp.DELETED 1.xml
12:00:05 AM(UTC-6)	Text File	DebugAnalytics.DELETED 1.xml
12:00:20 PM(UTC-6)	Picture	IMG [REDACTED] 120016201.jpg
12:00:23 PM(UTC-6)	DB	Google Photos (media store extras)
12:00:23 PM(UTC-6)	Picture	IMG [REDACTED] 120021204.jpg
12:00:23 PM(UTC-6)	Text File	com.google.android.apps.photos preferences.DELETED 4.xml
12:00:24 AM(UTC-6)	Text File	BattStatsPrefs.DELETED 2.xml
12:00:24 PM(UTC-6)	Picture	IMG [REDACTED] 120022835.jpg
12:00:24 PM(UTC-6)	Text File	com.google.android.apps.photos preferences.DELETED 3.xml
12:00:25 PM(UTC-6)	DB	Google+ (trash.db)
12:00:25 PM(UTC-6)	Text File	com.google.android.apps.photos preferences.DELETED 2.xml
12:00:25 PM(UTC-6)	Text File	com.google.android.apps.photos preferences.DELETED 5.xml
12:00:26 PM(UTC-6)	Text File	com.google.android.apps.photos preferences.xml
12:00:26 PM(UTC-6)	Text File	com.google.android.apps.photos preferences.DELETED.xml
12:00:26 PM(UTC-6)	Text File	com.google.android.apps.photos preferences.DELETED 1.xml
12:00:58 PM(UTC-6)	Text File	MailAppProvider.DELETED 1.xml
12:00:59 AM(UTC-6)	Text File	Pmaps.xml
12:00:59 PM(UTC-6)	Text File	Account [REDACTED].DELETED 1.xml
12:00:59 PM(UTC-6)	Text File	MailAppProvider.DELETED.xml

FORENSIC ARTIFACTS

- So. Much. Data.
 - 6 Months.
 - 143,240 artifacts.



- Search & Web (7022) (404)
 - Cookies (449) (178)
 - Searched Items (63) (30)
 - User Dictionary (6272)
 - Web Bookmarks (16)
 - Web History (222) (196)
- System & Logs (886)
 - Device Notifications (85)
 - Log Entries (801)
- User Accounts & Details (16)
 - Mobile Cards (2)
 - User Accounts (14)

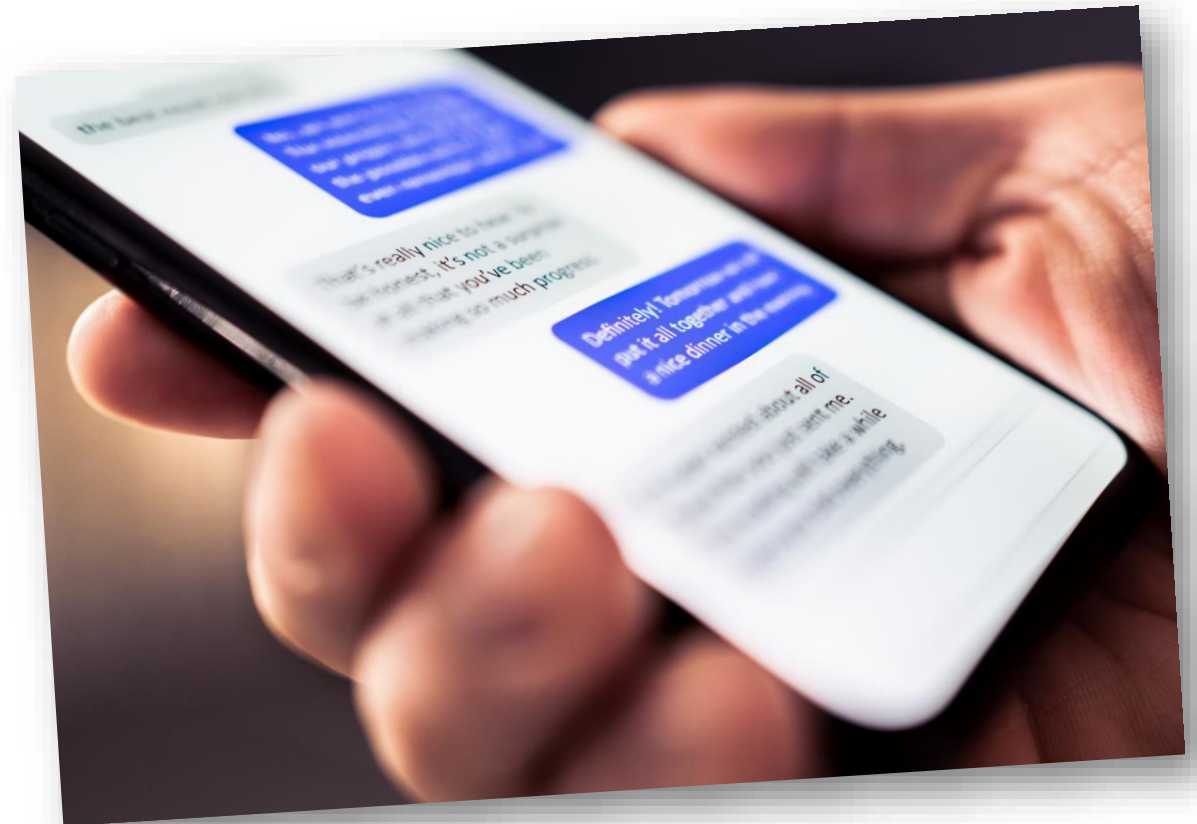
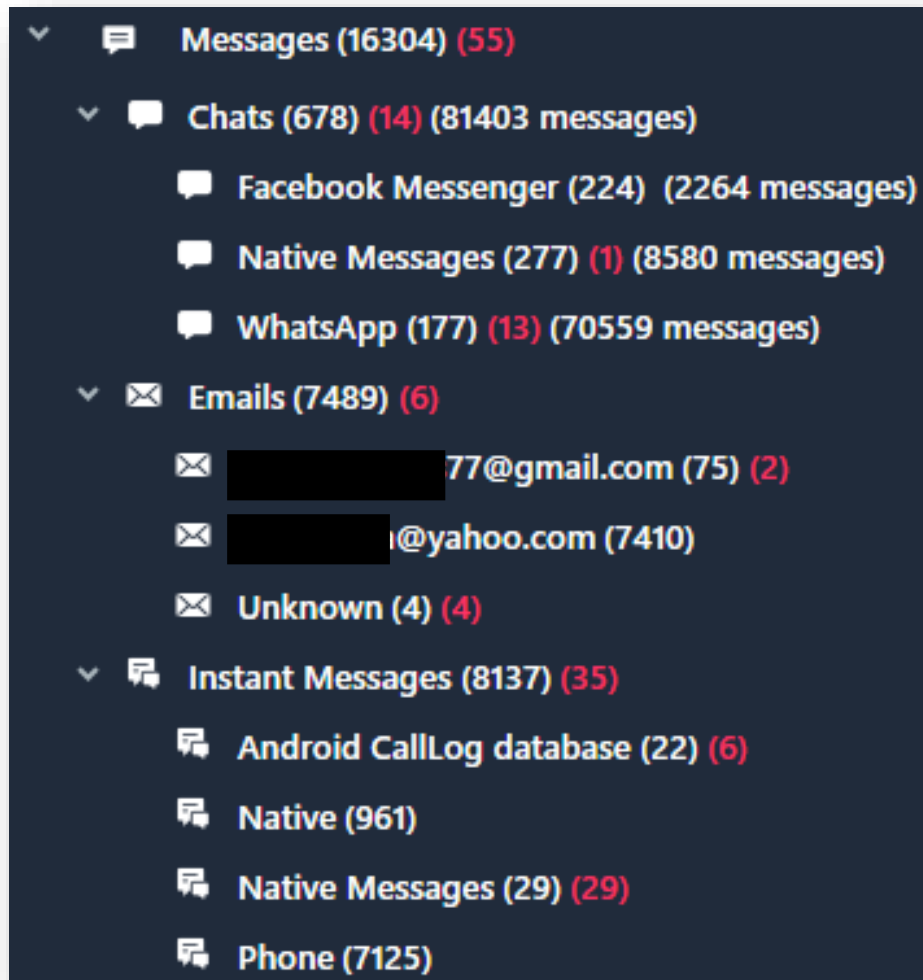
Data files

- All Files (42571)
- Applications (123)
- Archives (247)
- Databases (592)
- Documents (330)
- Exchange (975)
- Text (2130)
- Uncategorized (38174)

- Application (1076)
- Calendar (172) (35)
- Calls (363) (150)
- Contacts (574) (61)
- Device Info (27)
- Location Related (12)
- Manual Data Collection (6) (6)
 - Carved Strings (6) (6)
- Media (18096)
- Memos (38) (8)
- Messages (2966) (1026)
 - Chats (228) (224) (4848 messages)
 - Emails (2733) (802)
 - Instant Messages (5)
- Networks & Connections (1039) (21)
 - Bluetooth Devices (608) (21)
 - Device Events (380)
 - Network Connections (51)
- Physical Activities (30193)

FORENSIC ARTIFACTS

- So. Much. Data.
 - One cellphone.



- What about editing and un-sending messages?

Log Entries	7/7/2017 7:46:58 PM(UTC-4)		com.apple.MobileSMS: outgoing sms from E569E17F-C926-4D36-8CCC-D0024DAE6F4C:ABPerson	InteractionC
Instant Messages	7/7/2017 7:46:58 PM(UTC-4)	From: [REDACTED]	I love you too	Native Messages
Log Entries	7/7/2017 7:47:02 PM(UTC-4)		com.apple.MobileSMS: incoming sms from 68A61D7D-3A77-4C82-A179-7E79D4637ED9:ABPerson	InteractionC
Instant Messages	7/7/2017 7:47:02 PM(UTC-4)	From: [REDACTED]	Ikeviaun	Native Messages
Log Entries	7/7/2017 7:47:04 PM(UTC-4)		com.apple.MobileSMS: outgoing sms from E569E17F-C926-4D36-8CCC-D0024DAE6F4C:ABPerson	InteractionC
Instant Messages	7/7/2017 7:47:04 PM(UTC-4)	From: [REDACTED]	I love you too	Native Messages
Instant Messages	7/7/2017 7:47:05 PM(UTC-4)	From: [REDACTED] Red ❤️	you text at 12 , u saw it score i fell asleep , sound bad but i just ain tb & no i woke up at like 3:06	Native Messages
Log Entries	7/7/2017 7:47:05 PM(UTC-4)		com.apple.MobileSMS: incoming sms from D6048BCC-840C-49AD-857F-75F853CBFE32:ABPerson	InteractionC
Log Entries	7/7/2017 7:47:07 PM(UTC-4)		com.apple.MobileSMS: outgoing sms from E569E17F-C926-4D36-8CCC-D0024DAE6F4C:ABPerson	InteractionC
Instant Messages	7/7/2017 7:47:07 PM(UTC-4)	From: [REDACTED]	I love you too	Native Messages
Log Entries	7/7/2017 7:47:25 PM(UTC-4)		com.apple.MobileSMS: incoming sms from 68A61D7D-3A77-4C82-A179-7E79D4637ED9:ABPerson	InteractionC
Instant Messages	7/7/2017 7:47:25 PM(UTC-4)	From: [REDACTED]	Means a lot	Native Messages

- What about **really old** data?

	Instant Messages	3/1/2013 10:32:49 PM(UTC-5)	From: 100001701087808...	Quiero un cuarto donde al can...	Facebook messenger
	Instant Messages	3/1/2013 10:32:56 PM(UTC-5)	From: 100001948172186...	hola como estas	Facebook messenger
	Instant Messages	3/1/2013 10:33:42 PM(UTC-5)	From: 100001701087808...	How much do you want for y...	Facebook messenger
	Instant Messages	3/1/2013 10:34:19 PM(UTC-5)	From: 100001701087808...	Somebody want to buy it	Facebook messenger
	Instant Messages	3/1/2013 10:34:57 PM(UTC-5)	From: 100001948172186...	no se donde me van a poner...	Facebook messenger
	Instant Messages	3/1/2013 10:35:16 PM(UTC-5)	From: 100001701087808...	Ok manas	Facebook messenger
	Instant Messages	3/1/2013 10:36:08 PM(UTC-5)	From: 100001948172186...	me van a poner en un lugar...	Facebook messenger
	Instant Messages	3/1/2013 10:36:50 PM(UTC-5)	From: 100001948172186...	al q lo quiere q vaya a la...	Facebook messenger
	Instant Messages	3/1/2013 10:37:12 PM(UTC-5)	From: 100001701087808...	Algunos solo interesan	Facebook messenger
	Instant Messages	3/1/2013 10:37:25 PM(UTC-5)	From: 100001948172186...	pero yo no	Facebook messenger
	Instant Messages	3/1/2013 10:37:49 PM(UTC-5)	From: 100001701087808...	Si quieres cuarto hermano	Facebook messenger
	Instant Messages	3/1/2013 10:37:55 PM(UTC-5)	From: 100001948172186...	a ella q me dan 20000	Facebook messenger
	Instant Messages	3/1/2013 10:38:23 PM(UTC-5)	From: 100001948172186...	y por cuanto no lo pones q...	Facebook messenger

- What about secure messaging?
 - “Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Tap to learn more.”

Instant Messages	4/16/2024 7:17:47 PM(UTC-4)	From: System Message S...	Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Tap to learn more	WhatsApp
Instant Messages	4/16/2024 7:17:47 PM(UTC-4)	From: [REDACTED]@s.... To: [REDACTED]@s.wha...	Hola	WhatsApp
Log Entries	4/16/2024 7:17:48 PM(UTC-4)		net.whatsapp.WhatsApp: WhatsApp: participant identifier: [REDACTED]@s.whatsapp.net	InteractionC
Instant Messages	4/16/2024 7:25:12 PM(UTC-4)	From: [REDACTED]@s....	Hola	WhatsApp
Instant Messages	4/16/2024 7:25:21 PM(UTC-4)	From: [REDACTED]@s....		WhatsApp
Instant Messages	4/16/2024 7:32:36 PM(UTC-4)	From: [REDACTED]@s.... To: [REDACTED]@s.wha...	Ok	WhatsApp
Log Entries	4/16/2024 7:32:36 PM(UTC-4)		net.whatsapp.WhatsApp: WhatsApp: participant identifier: [REDACTED]@s.whatsapp.net	InteractionC

FORENSIC ARTIFACTS: CALL LOGS

- 00:00:00 Second call?

Call Log Go to ▾

Timestamp: 3/8/ [REDACTED] 3:59:35 PM(UTC-5)
 Duration: 00:00:00
 Type: Outgoing
 Country code:
 Network code:
 Network Name:
 Source: Logs Table
 Is video:
 Extraction: Physical
 Source file:

Parties

To: 30- [REDACTED] 9

×	Parties ▾	↓ Timestamp ▾	Duration ▾	Type ▾
×	To: [REDACTED]	3/6/ [REDACTED] 8:58:41 PM(UTC-5)	01:15:58	Outgoing
	To: [REDACTED] Matt [REDACTED]	3/6/ [REDACTED] 8:20:54 PM(UTC-5)	00:00:10	Outgoing
	To: [REDACTED] Linda [REDACTED]	3/6/ [REDACTED] 6:44:21 PM(UTC-5)	00:01:27	Outgoing
	From: [REDACTED] Matt [REDACTED]	3/6/ [REDACTED] 5:42:24 PM(UTC-5)	00:15:49	Incoming
	From: [REDACTED] Matt [REDACTED]	3/6/ [REDACTED] 5:26:58 PM(UTC-5)	00:06:27	Incoming
	To: [REDACTED] Matt [REDACTED]	3/6/ [REDACTED] 5:18:51 PM(UTC-5)	00:02:07	Outgoing
	To: [REDACTED]	3/6/ [REDACTED] 5:16:49 PM(UTC-5)	00:01:53	Outgoing
	Unknown	3/6/ [REDACTED] 3:54:40 PM(UTC-5)	00:01:27	Incoming
×	From: [REDACTED]	3/6/ [REDACTED] 3:45:35 PM(UTC-5)	00:10:47	Incoming
	From: [REDACTED] Linda [REDACTED]	3/6/ [REDACTED] 3:32:22 PM(UTC-5)	00:11:31	Incoming
×	To: [REDACTED]	3/6/ [REDACTED] 9:44:10 AM(UTC-5)	00:06:04	Outgoing
×	To: [REDACTED]	3/6/ [REDACTED] 8:48:52 AM(UTC-5)	00:55:04	Outgoing
	To: [REDACTED] Matt [REDACTED]	3/5/ [REDACTED] 6:06:04 PM(UTC-5)	00:00:00	Outgoing

CASE EXAMPLE: CALL LOGS

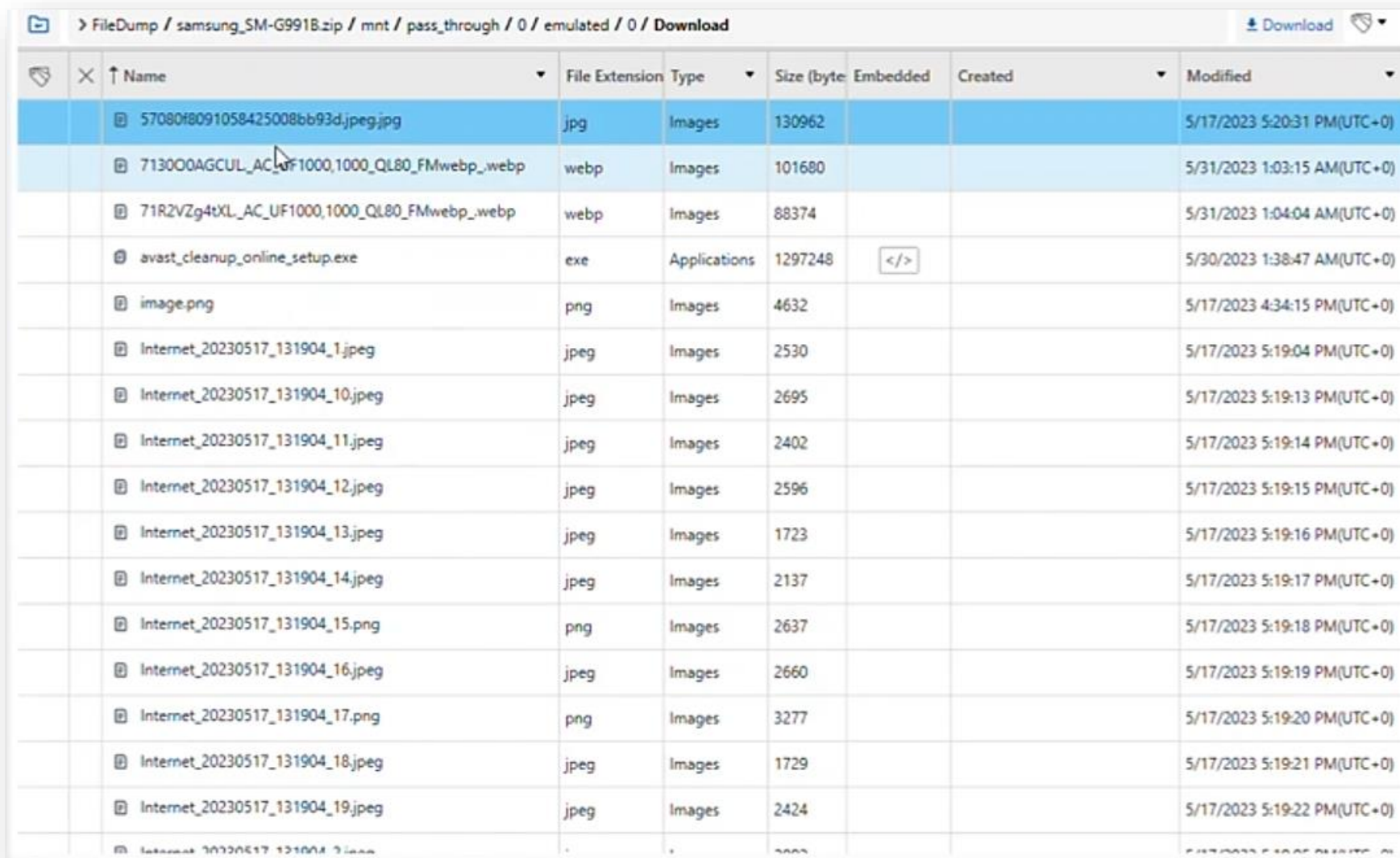
- Intentional deletion of phone calls by the plaintiff.
 - 16 most recent calls.

	A	B	Q	R	S	T	X
1	Z_	Gap Analys	ZDATE	Local time	ZDURATION	ZADDRESS	ZSERVICE_PROVIDER
170	1445	1	8/7/2023 10:18:29 PM		463.058076	+18	com.apple.Telephony
171	1447	0	8/8/2023 11:13:35 AM		211.155635	+18	com.apple.Telephony
172	1448	0	8/8/2023 4:53:44 PM		24.68528795	+18	com.apple.Telephony
173	1449	0	8/8/2023 5:02:06 PM		4434.260402	+16	com.apple.Telephony
174	1450	0	8/8/2023 6:25:05 PM		682.177444	+18	com.apple.Telephony
175	1451	0	8/8/2023 8:04:19 PM		16.42520404	816	com.apple.Telephony
176	1452	0	8/9/2023 4:08:01 PM	8/9/2023 11:08:01 AM	0	+18	com.apple.Telephony
177	1453	0	8/9/2023 4:08:13 PM	8/9/2023 11:08:13 AM	0	+18	com.apple.Telephony
178	1454	0	8/9/2023 4:08:26 PM	8/9/2023 11:08:26 AM	69.02923703	+18	com.apple.Telephony
179	1455	0	8/9/2023 4:09:45 PM	8/9/2023 11:09:45 AM	30.03557503	+18	com.apple.Telephony
180	1456	0	8/9/2023 4:10:27 PM	8/9/2023 11:10:27 AM	14.78702605	+18	com.apple.Telephony
181	1457	0	8/9/2023 4:12:40 PM	8/9/2023 11:12:40 AM	0	+18	com.apple.Telephony
182	1458	0	8/9/2023 4:14:34 PM	8/9/2023 11:14:34 AM	126.663968	+18	com.apple.Telephony
183	1459	1	8/9/2023 4:19:00 PM	8/9/2023 11:19:00 AM	319.0241981	+18	com.apple.Telephony
184	1461	1	8/9/2023 7:52:34 PM	8/9/2023 2:52:34 PM	93.53074002	+18	com.apple.Telephony
185	1463	1	8/9/2023 8:14:30 PM	8/9/2023 3:14:30 PM	5062.648589	+16	com.apple.Telephony
186							
187							
188							
189							
190							

Database holds 200 calls. Only 184 are listed. Most recent calls were deleted. Other artifacts located in the phone supported this. Call Detail Records will support this.

FORENSIC ARTIFACTS: WEB HISTORY

- Timelines and more.



Name	File Extension	Type	Size (byte)	Embedded	Created	Modified
57080f8091058425008bb93d.jpeg.jpg	jpg	Images	130962			5/17/2023 5:20:31 PM(UTC+0)
713000AGCUL_AC_UF1000,1000_QL80_FMwebp_.webp	webp	Images	101680			5/31/2023 1:03:15 AM(UTC+0)
71R2VZg4tXL_AC_UF1000,1000_QL80_FMwebp_.webp	webp	Images	88374			5/31/2023 1:04:04 AM(UTC+0)
avast_cleanup_online_setup.exe	exe	Applications	1297248	</>		5/30/2023 1:38:47 AM(UTC+0)
image.png	png	Images	4632			5/17/2023 4:34:15 PM(UTC+0)
Internet_20230517_131904_1.jpeg	jpeg	Images	2530			5/17/2023 5:19:04 PM(UTC+0)
Internet_20230517_131904_10.jpeg	jpeg	Images	2695			5/17/2023 5:19:13 PM(UTC+0)
Internet_20230517_131904_11.jpeg	jpeg	Images	2402			5/17/2023 5:19:14 PM(UTC+0)
Internet_20230517_131904_12.jpeg	jpeg	Images	2596			5/17/2023 5:19:15 PM(UTC+0)
Internet_20230517_131904_13.jpeg	jpeg	Images	1723			5/17/2023 5:19:16 PM(UTC+0)
Internet_20230517_131904_14.jpeg	jpeg	Images	2137			5/17/2023 5:19:17 PM(UTC+0)
Internet_20230517_131904_15.png	png	Images	2637			5/17/2023 5:19:18 PM(UTC+0)
Internet_20230517_131904_16.jpeg	jpeg	Images	2660			5/17/2023 5:19:19 PM(UTC+0)
Internet_20230517_131904_17.png	png	Images	3277			5/17/2023 5:19:20 PM(UTC+0)
Internet_20230517_131904_18.jpeg	jpeg	Images	1729			5/17/2023 5:19:21 PM(UTC+0)
Internet_20230517_131904_19.jpeg	jpeg	Images	2424			5/17/2023 5:19:22 PM(UTC+0)
Internet_20230517_131904_20.jpeg	jpeg	Images	2660			5/17/2023 5:19:23 PM(UTC+0)

CASE EXAMPLE: WEB HISTROY

- Detailed account of activity - down to the second.



ARTIFACTS: SEARCHES

- Anywhere there is a search bar.

Timestamp	Value	Source
3/5/2018 1:59:50 PM(UTC-5)	fake text prank	Play Store
3/5/2018 1:30:52 PM(UTC-5)	pranks on your phone	Play Store
3/5/2018 1:45:09 PM(UTC-5)	voice changer	Play Store
3/3/2018 1:26:29 PM(UTC-5)	google	Play Store
2/27/2018 9:44:41 PM(UTC-5)	the idiot test	Play Store
2/27/2018 9:44:25 PM(UTC-5)	the red button	Play Store
2/27/2018 9:40:57 PM(UTC-5)	guess my mi d	Play Store
2/27/2018 9:29:28 PM(UTC-5)	games to play on a roa...	Play Store
2/26/2018 9:44:45 AM(UTC-5)	google	Play Store
2/24/2018 9:34:33 PM(UTC-5)	tsum tsum	Play Store
2/24/2018 7:36:36 PM(UTC-5)	papas games	Play Store

Timestamp	Value	Source
3/5/2018 1:38:04 PM(UTC-5)	amazon	Chrome
3/5/2018 11:50:23 AM(UTC-5)	hotwire	Chrome
3/5/2018 7:50:54 AM(UTC-5)	r b rebuildables i [redacted] wv	Chrome
3/5/2018 7:37:07 AM(UTC-5)	rental cars [redacted] wv	Chrome
3/5/2018 7:31:52 AM(UTC-5)	united bank [redacted]	Chrome
3/5/2018 7:25:32 AM(UTC-5)	rental cars [redacted] wv	Chrome

Timestamp	Value	Source
11/5/2017 12:10:22 PM(UTC-5)	prisoner of love bob and tom	YouTube Application
12/1/2017 7:45:13 AM(UTC-5)	god's gonna cut you down	YouTube Application
12/3/2017 12:43:48 PM(UTC-5)	will ferrell pearl the landlord original video	YouTube Application
12/3/2017 12:25:49 PM(UTC-5)	will ferrell the landlord	YouTube Application
12/1/2017 7:32:48 AM(UTC-5)	movie 43 kate winslet hugh jackman scene	YouTube Application
12/1/2017 11:43:53 AM(UTC-5)	christmas jammies	YouTube Application

CASE EXAMPLE: SEARCHES

- Plaintiff was searching the internet right before the moment of impact.



ARTIFACTS: MESSAGING

- SMS/MMS vs. Data

×	↶	↑ Timestamp	▼	Parties	▼	Body	Folder	▼
		3/24/2014	8:46:50 AM(UTC-4)	From: +17	37 Dad	All good :)	Inbox	
×		3/24/2014	1:34:09 PM(UTC-4)	To: 75	5 Tilly	In health where talking about the urinary system	Sent	
×		3/24/2014	1:34:45 PM(UTC-4)	From: +17	35 Tilly	Pee pee	Inbox	
×		3/24/2014	1:37:02 PM(UTC-4)	To: 75	35 Tilly	Yup	Sent	
×		3/24/2014	1:37:14 PM(UTC-4)	To: 75	35 Tilly	Where talking about it ughfhg	Sent	
×		3/24/2014	1:44:21 PM(UTC-4)	From: +17	35 Tilly	Aw you don't want to know what I was doing LOL	Inbox	

Analyzed Data

- Calendar (31)
- Call Log (179)
- Chats (6045)
 - iMessages (6045) (28146 messages)**
- Contacts (571)
- Device Locations (207)
 - Locations (207)
- MMS Messages (343)
- Notes (37)
- SMS Messages (13238)**

×	↶	↑ Timestamp	▼	Parties	▼	Body	Folder	▼	Status	▼
×		3/24/2014	8:38:18 AM(UTC-4)	From: +17	35 Tilly	Bye bye sweetie	Inbox		Read	
×		3/24/2014	8:45:41 AM(UTC-4)	To: 75	35 Tilly	The bus is late	Sent		Sent	
		3/24/2014	8:45:54 AM(UTC-4)	To: 7	4 Lizzy	Lizzy	Sent		Sent	
×		3/24/2014	8:46:02 AM(UTC-4)	From: +1	35 Tilly	Guess so itll be here soon no worries	Inbox		Unread	

CASE EXAMPLE: MESSAGING

- The plaintiff deleted messages intentionally.

A	B	D	Q	R	S	T
ROWID	Gap analysis	text	date	Local time	date_read	date_delivered
178346		0 No I just pulled into shell what're was it?	8/9/2023 9:39:14 PM		1/1/2001 12:00:00 AM	8/9/2023 9:39:15 PM
178347		0 Are you still there	8/9/2023 9:53:05 PM		8/9/2023 9:57:10 PM	1/1/2001 12:00:00 AM
178348		0 Just leaving	8/9/2023 9:57:15 PM		1/1/2001 12:00:00 AM	8/9/2023 9:57:16 PM
178349		35 Ok	8/9/2023 10:01:26 PM		8/9/2023 10:01:34 PM	1/1/2001 12:00:00 AM
178385		0 Morning	8/10/2023 2:03:19 PM	8/10/2023 9:03:19 AM	8/10/2023 2:03:27 PM	1/1/2001 12:00:00 AM
178386		0 Morning love	8/10/2023 2:03:36 PM	8/10/2023 9:03:36 AM	1/1/2001 12:00:00 AM	8/10/2023 2:03:37 PM
178387		1 I love you ❤️	8/10/2023 2:05:07 PM	8/10/2023 9:05:07 AM	8/10/2023 2:05:49 PM	1/1/2001 12:00:00 AM
178389		1 I love you!!	8/10/2023 2:05:58 PM	8/10/2023 9:05:58 AM	1/1/2001 12:00:00 AM	8/10/2023 2:05:58 PM
178391		0 I've been in a bad wreck I'm ok but got to go to the hospital	8/10/2023 2:39:22 PM	8/10/2023 9:39:22 AM	1/1/2001 12:00:00 AM	8/10/2023 2:39:24 PM
178392		0 I tried calling but I can't get it to go through	8/10/2023 2:39:36 PM	8/10/2023 9:39:36 AM	1/1/2001 12:00:00 AM	8/10/2023 2:39:36 PM
178393		0 I can't find the hospital	8/10/2023 2:48:18 PM	8/10/2023 9:48:18 AM	8/10/2023 2:48:22 PM	1/1/2001 12:00:00 AM
178394		0 Mosaic she said it's the only one in st Joe	8/10/2023 2:48:43 PM	8/10/2023 9:48:43 AM	1/1/2001 12:00:00 AM	8/10/2023 2:48:43 PM
178395		0 Ok	8/10/2023 2:49:01 PM	8/10/2023 9:49:01 AM	8/10/2023 2:49:04 PM	1/1/2001 12:00:00 AM
178396		0 Did you tell Jeremy	8/10/2023 2:49:26 PM	8/10/2023 9:49:26 AM	8/10/2023 2:49:30 PM	1/1/2001 12:00:00 AM
178397		0 No Dan Jeremy's phone is off	8/10/2023 2:49:48 PM	8/10/2023 9:49:48 AM	1/1/2001 12:00:00 AM	8/10/2023 2:49:48 PM
178398		0 Ok moms on her way up I'll be there soon	8/10/2023 2:50:20 PM	8/10/2023 9:50:20 AM	8/10/2023 2:50:26 PM	1/1/2001 12:00:00 AM
178399		0 Ok thank w	8/10/2023 2:50:33 PM	8/10/2023 9:50:33 AM	1/1/2001 12:00:00 AM	8/10/2023 2:50:34 PM
178400		0 Come to the er at mosaic I'll be ready when you get here	8/10/2023 3:10:56 PM	8/10/2023 10:10:56 AM	1/1/2001 12:00:00 AM	8/10/2023 3:10:56 PM
178401		0 Ok	8/10/2023 3:14:15 PM	8/10/2023 10:14:15 AM	8/10/2023 3:14:31 PM	1/1/2001 12:00:00 AM
178402		0 I'm in Osborn	8/10/2023 3:14:34 PM	8/10/2023 10:14:34 AM	8/10/2023 3:14:39 PM	1/1/2001 12:00:00 AM
178403		0 Ok	8/10/2023 3:14:40 PM	8/10/2023 10:14:40 AM	1/1/2001 12:00:00 AM	8/10/2023 3:14:41 PM
178404		Are you ok	8/10/2023 3:15:11 PM	8/10/2023 10:15:11 AM	8/10/2023 3:15:11 PM	1/1/2001 12:00:00 AM

- Translation creates timestamps too.

Search Results	Value	Source
Enviar un mensaje	Send a Message	GoogleTranslate
Llame a su representante	Call Your Rep	GoogleTranslate
[REDACTED] su representante de reclamos, está aquí para ayudarlo con su reclamo	[REDACTED] your claim rep, is here to help with your claim involving your '13...	GoogleTranslate
Vuelva a consultar aquí para conocer las actualizaciones de su reclamo.	Check back here for any updates on your claim.	GoogleTranslate
Reclamación recibida	Claim Received	GoogleTranslate
¡Hola! A continuación, le recordamos que se acerca la fecha de vencimiento de su pago de \$ 310.49 por su póliza de automóvil vence el 08/11/2021. Es fácil re...	Hello! Here's a friendly reminder that your payment due date is coming up....	GoogleTranslate
Hello! Here's a friendly reminder that your payment due date is coming up. Your payment of \$ 310.49 for your auto policy is due on 08/11/2021. It's easy to	Hello! Here's a friendly reminder that your payment due date is coming up....	GoogleTranslate
¡ASEGÚRESE DE ACCEDER AL TRABAJO CORRECTO!	MAKE SURE YOU CLOCK IN AT THE CORRECT JOB !!	GoogleTranslate
MAKE SURE YOU CLOCK IN AT THE CORRECT JOB !!	MAKE SURE YOU CLOCK IN AT THE CORRECT JOB!!	GoogleTranslate
Repuestos muy baratos y completamente autos, buen estado y garantía. Contamos con repuestos para todo tipo de autos, y vehículos completos, puede 786, 222, 2157 y 786, 222, 4208	Very cheap parts and completely cars, good good condition, and warranty...	GoogleTranslate
Very cheap parts and completely cars, good good condition, and warranty We have parts for all types of cars, and complete vehicles, may economic presses 786, 222, 2157 and 786, 222, 4208	Very cheap parts and completely cars ,good good condition, and warranty T...	GoogleTranslate
insurance company	insurance company	GoogleTranslate

Timestamp:	[REDACTED] 11:40:38 AM(UTC-4)
Source:	GoogleTranslate
Value:	Very cheap parts and completely cars, good good condition, and warranty We have parts for all types of cars, and complete vehicles, may economic presses, motor transmission differential with 30 days warranty and low mileage 786, 222, 2157 and 786, 222, 4208
Search Results:	[REDACTED] Repuestos muy baratos y completamente autos, buen estado y garantía. Contamos con repuestos para todo tipo de autos, y vehículos completos, pueden prensas económicas, motor diferencial de transmisión con 30 días de garantía y bajo kilometraje. 786, 222, 2157 y 786, 222, 4208
Searched In:	[REDACTED]
Origin:	Default
Account:	
Service Identifier:	
Extraction:	Advanced Logical
Source file:	iPhone/mobile/Containers/Data/Application/com.google.Translate/Documents/translate.db : 0xA516 (Table: history, Size: 352256 bytes)

DIGITAL FORENSICS

WEARABLE TECHNOLOGY FORENSICS

ENVISTA
FORENSICS

- IoT Devices
 - Data Silo = Phone Application



Vector™ 3/3S

Measure power at the pedal to gauge your performance.



fēnix® 5 Series

Premium multisport GPS watches available in three sizes and a variety of styles, all featuring wrist-based heart rate

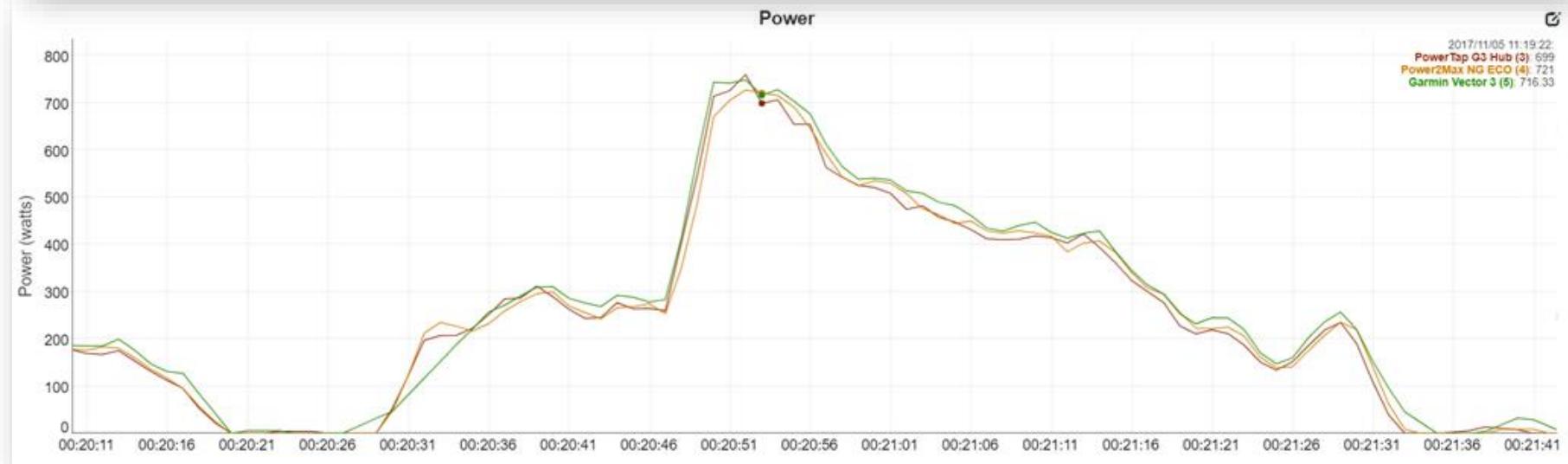
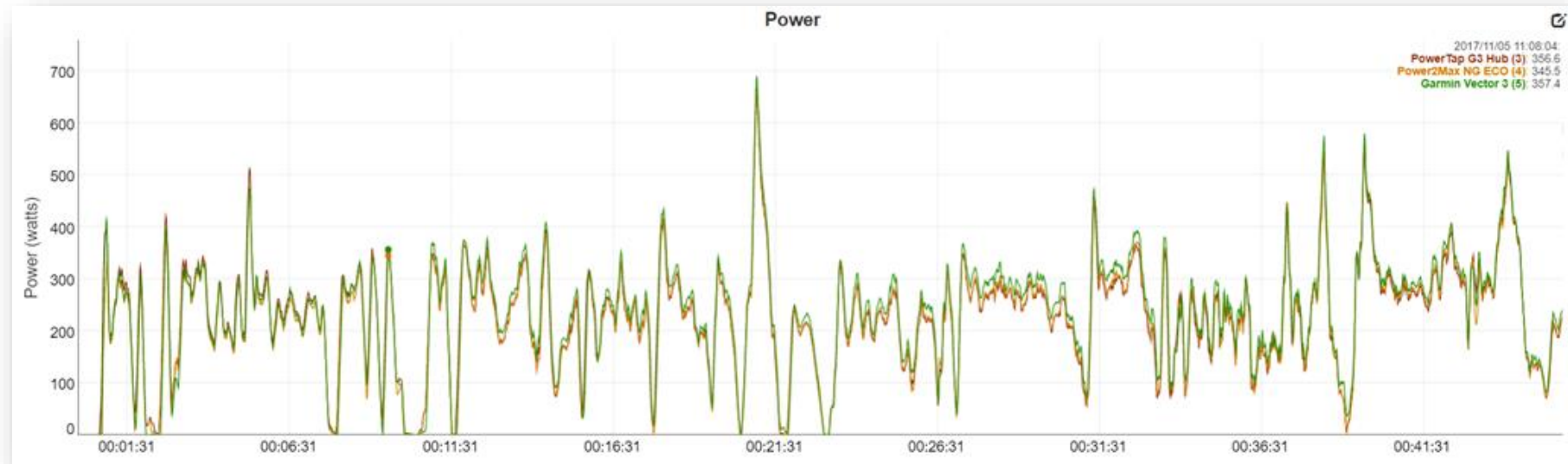


- IoT Devices
 - Data Silo = Phone Application
 - Wattage Output



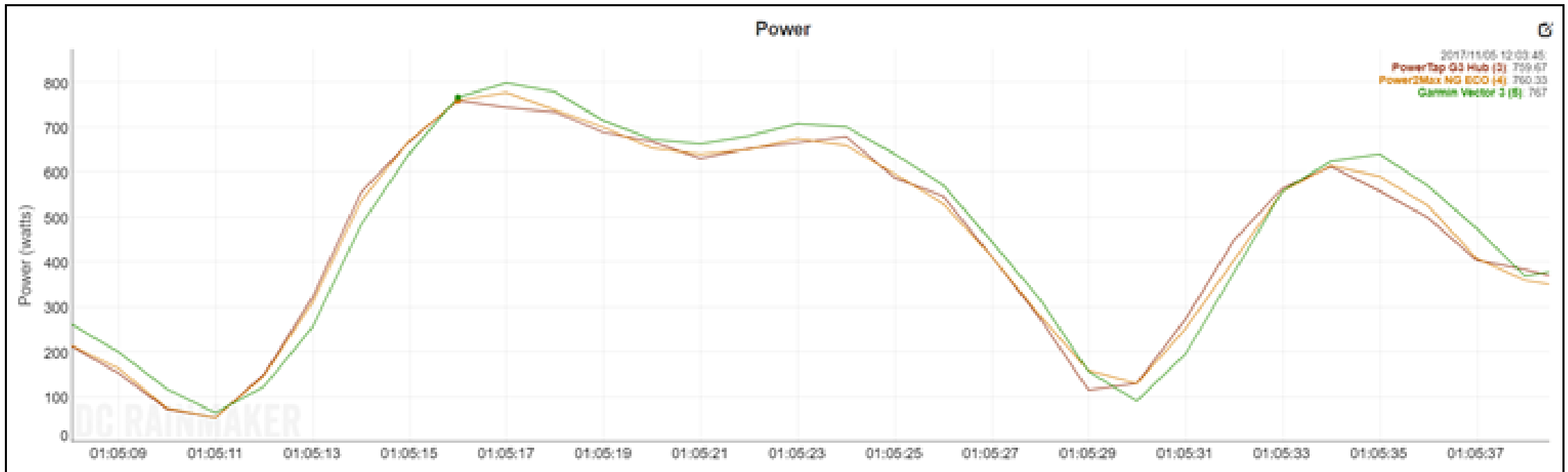
CASE EXAMPLE: DID THE CYCLIST SLOW DOWN?

- 45 Minutes and 90 Seconds (Zoomed In)
- 3 Different “Tools” used for verification



[Garmin Vector 3 Power Meter In-Depth Review | DC Rainmaker](#)

- 45 Minutes and 90 Seconds (Zoomed In)
 - 30 Second Sprint



[Garmin Vector 3 Power Meter In-Depth Review | DC Rainmaker](#)

• Scenario

- An executive is on business trip in Europe.
- On the last night of his stay, he explores the city.
- When he returns to work, his company notices large transactions on the company card.
- When questioned...he says he was Kidnapped.

- Scenario

- His card was compromised but not lost.
- Claims to have been held hostage for 8 hours.
- Vivid details of the “kidnapping” event.
- No report made to law enforcement
- No report made to his company.
- Over \$100,000 in charges were made on the card.

• Evidence

- We are contacted by SIU for the insurance company.
- Asked to examine:
 - Apple Watch
 - iPhone XR



CASE EXAMPLE: Kidnapped!

• Analysis

- The Analysis recovered two sources of data that contradicted the executive's story.
 - When he was allegedly "tied up," his watch recorded miles of walking over multiple hours.

25	Activities				Important	7/13/2020 3:06:40 PM	7/13/2020 3:06:40 PM
Name	Originates from	Value	Time	Location	Source	Deleted	
Steps and Distance	Device	174 Steps 89.90 Meters	Last Launch: 12/9/2019 7:19:32 PM Start time: 12/9/2019 7:08:11 PM End time: 12/9/2019 7:14:04 PM		Source: Health Source file: ██████████ iPhone/mobile/Library/H ealth/healthdb_secure.s qlite : 0x3A6839B (Table: samples, objects, Size: 113782784 bytes)		

CASE EXAMPLE: Kidnapped!

• Analysis

- Right before taking off from the airport to come home, the employee crafted to messages in Google translate.

Extraction Report - Apple iPhone Logical

Tags (59)

#	Type	Name	Tag description	Event	Tags	Created	Modified
1	Searched Items			<p>Last night you said you can't find a man. I promise!! One day someone will find you and be perfect. Look for someone that likes what you like.</p> <p>I want you to know that you deserve better. You are beautiful (American Perfect) I really am gonna miss you</p>	Important	7/13/2020 3:05:34 PM	7/13/2020 3:05:34 PM

Timestamp	Source	Value	Parameters	Origin	Deleted	Account
12/10/2019 5:47:51 PM	<p>GoogleTranslate</p> <p>Source file: iPhone/mobile/Containers/Data/Application/com.google.Translate/Documents/translate.db : 0x1263 (Table: history, Size: 61440 bytes)</p>	<p>Last night you said you can't find a man. I promise!! One day someone will find you and be perfect. Look for someone that likes what you like.</p> <p>I want you to know that you deserve better. You are beautiful (American Perfect) I really am gonna miss you</p> <p>Search Results: !!</p>	<p>Source Language: en</p> <p>Target Language: fr</p>	Default		

DIGITAL FORENSICS

IN-VEHICLE INFOTAINMENT
(IVI) FORENSICS

ENVISTA
FORENSICS

Funnel

- From Devices to Car
 - Data Repositories
 - Cell Phone
 - Backups
 - Online Accounts
 - Vehicle Infotainment Systems
 - Example
 - Smartwatch > Phone > Car
 - Camera > Phone > Car
 - Computer > Phone > Car
 - Syncing
 - Ecosystems



Forensic Artifacts

- Connected Devices
 - Rental Car
 - User Interactions

iVe - Infotainment & Vehicle System Forensics

File View Maps Report Export Tools

CONTENT

- Applications
- Connections
 - Bluetooth (36)
 - Wifi (3)
 - Devices (104)
 - Erin's iPhone
 - Ben's iPhone
 - Will Jace Herondale KINGSTON
 - T7380
 - rolo
 - blemere's iPod
 - dd-wpa2-aes-ch8
 - dd-wpa2-tkip-ch10
 - dd-wep-ch1
 - Jennifer's iPhone
 - motorola XT907
 - Charee's Iphone
 - SAMSUNG Electronics Co. Ltd. SCH-I605
 - Tiffany's iPhone
 - USB Hard Disk Drive DSK5:
 - M.O Irondi (SM-N900T)
 - Adrian Helmick's iPhone
 - iPhone
 - Sara Lee's iPhone
 - 64A3CB30CE8E
 - 380F4A5AD378
 - 38E7D8937381
 - 406AAB953E4D
 - 50A4C85F4847

SYSTEMS

CONTENT

TAGS

SEARCH

Map

Device Name	Device Type(int)	Device Type	Unique Number	Unique Number Ty
Aa	Aa	Aa	Aa	Aa
Erin's iPhone	2	Phone-2	A888083AE07F	Bluetooth Address
Erin's iPhone	5	Phone-5	0	Bluetooth Address
Erin's iPhone			DQGVK412FH1G	Serial Number
iPhone	3	Phone-3	FFFFFFFFE0864D97	Bluetooth Address
iPhone	5	Phone-5	0	Bluetooth Address
iPhone			F2LLP20EFNJP	Serial Number
Jennifer's iPhone	2	Phone-2	0	Bluetooth Address
Jennifer's iPhone	5	Phone-5	0	Bluetooth Address
Jennifer's iPhone	3	Phone-3	FFFFFFFFCB30CE8E	Bluetooth Address
KINGSTON	1	USB-1	0	Bluetooth Address
KINGSTON	1	USB-1	0	Bluetooth Address
Lexissss iPhone			DNQJPXBYF8GH	Serial Number
M.O Irondi (SM-N900T)	3	Phone-3	11AB0E57	Bluetooth Address
motorola XT907	4	4	0	Bluetooth Address
motorola XT907			99000201667977	Serial Number
rolo	3	Phone-3	E899C43E8A97	Bluetooth Address
rolo	2	Phone-2	E899C43E8A97	Bluetooth Address
SAMSUNG Electronics Co. Ltd. SCH-I605	4	4	0	Bluetooth Address
SAMSUNG Electronics Co. Ltd. SCH-I605			43007cae2eff3011	Serial Number
Sara Lee's iPhone	3	Phone-3	FFFFFFFFB77F40AC	Bluetooth Address
T7380	3	Phone-3	38E7D825E758	Bluetooth Address
Tiffany's iPhone	5	Phone-5	0	Bluetooth Address
USB Hard Disk Drive DSK5:	1	USB-1	0	Bluetooth Address
USB Hard Disk Drive DSK5:			-950332193	Serial Number
Will Jace Herondale	5	Phone-5	0	Bluetooth Address
Will Jace Herondale			7003588MA4S	Serial Number

Forensic Artifacts

- Track Logs

- Location history
- Lifestyle analysis
- Different than CDR (Crash Data Recorder)



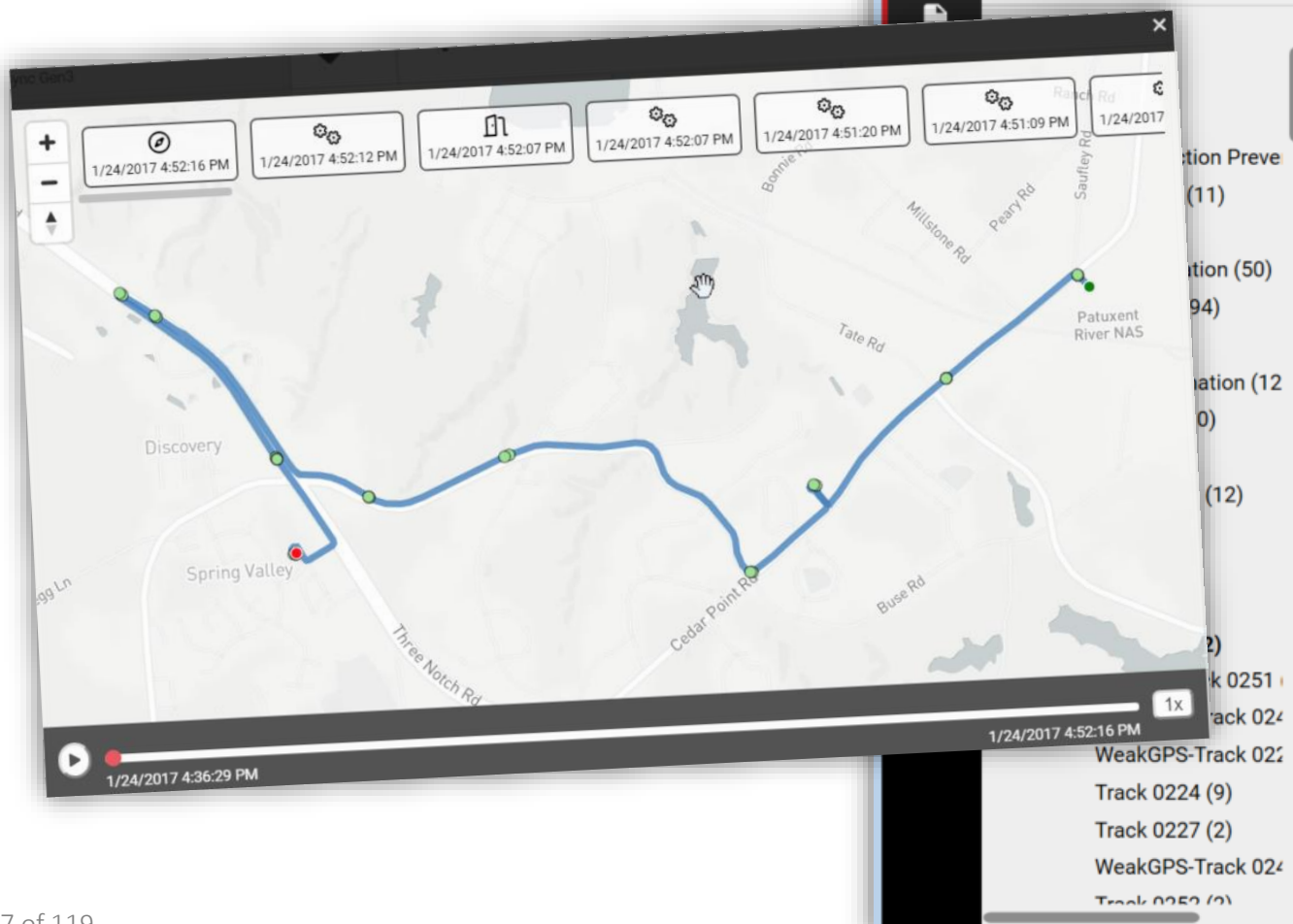
EVIDENCE (8,073)

Column view

Track Na...	Date/Time - Local Time	Latitude	Longitude	Geohash	
Track 001	2020-08-14 15:02:11	38.987276	-76.574943	dqctc3rv6e00	0
Track 001	2020-08-14 15:02:14	38.987167	-76.575157	dqctc3rstw8q	1
Track 001	2020-08-14 15:02:14	38.987186	-76.575184	dqctc3rsufhr	7
Track 001	2020-08-14 15:02:12	38.987124	-76.57517	dqctc3rsmnwv	3
Track 001	2020-08-14 15:02:20	38.987324	-76.575594	dqctc3rme7fw	1
Track 001	2020-08-14 15:02:21	38.987349	-76.575679	dqctc3rmc2e5	1
Track 001	2020-08-14 15:02:23	38.987379	-76.575757	dqctc3rjzw1n	1
Track 001	2020-08-14 15:02:23	38.987408	-76.575846	dqctc3rnj7we	1
Track 001	2020-08-14 15:02:24	38.987437	-76.57593	dqctc3rn7900	1
Track 001	2020-08-14 15:02:26	38.987466	-76.576015	dqctc3rn3w2t	1
Track 001	2020-08-14 15:02:27	38.987494	-76.576097	dqctc3qyxees	1
Track 001	2020-08-14 15:02:27	38.987522	-76.576186	dqctc3qyv8c5	1
Track 001	2020-08-14 15:02:28	38.987547	-76.576272	dqctc3qygt90	1
Track 001	2020-08-14 15:02:29	38.987566	-76.576358	dqctc3qz190f	1
Track 001	2020-08-14 15:02:30	38.987576	-76.576433	dqctc3qxpfcj	1
Track 001	2020-08-14 15:02:31	38.987584	-76.576509	dqctc3qxn2m	1
Track 001	2020-08-14 15:02:32	38.98759	-76.57658	dqctc3qxhme3	1
Track 001	2020-08-14 15:02:34	38.987603	-76.57664	dqctc3qx4zyw	1
Track 001	2020-08-14 15:02:34	38.987628	-76.5767	dqctc3qx3s9u	1
Track 001	2020-08-14 15:02:36	38.987666	-76.576739	dqctc3qx8esy	1
Track 001	2020-08-14 15:02:36	38.987707	-76.576747	dqctc3qxb7qg	1
Track 001	2020-08-14 15:02:37	38.987744	-76.576729	dqctc3w80fhr	9
Track 001	2020-08-14 15:02:38	38.987797	-76.576682	dqctc3w83upk	1
Track 001	2020-08-14 15:02:39	38.987865	-76.576607	dqctc3w8g8z3	2
Track 001	2020-08-14 15:02:41	38.987945	-76.576522	dqctc3w9jxww	2
Track 001	2020-08-14 15:02:41	38.988031	-76.576431	dqctc3w9xzf8	2
Track 001	2020-08-14 15:02:43	38.988128	-76.576339	dqctc3wf3cz4	2
Track 001	2020-08-14 15:02:43	38.988229	-76.576251	doctc3wfh8t	3

Forensic Artifacts

- Track Logs
 - Animated



iVe - Infotainment & Vehicle System Forensics

File View Tools Help

Time offsets have not been applied to the data. Go to Tools > Time Offset to create and manage offsets to apply to timestamps.

Systems Ford Sync Gen3

Name	Start Time	End Time	Timestamp Type	Fl
WeakGPS-Track 0157	01/24/2017 11:49:27 AM	01/24/2017 11:50:04 AM	Local	
Track 0158	01/24/2017 11:50:04 AM	01/24/2017 12:38:24 PM	Local	
WeakGPS-Track 0159	01/24/2017 12:38:26 PM	01/24/2017 12:38:46 PM	Local	
Track 0160	01/24/2017 12:38:46 PM	01/24/2017 12:39:30 PM	Local	
WeakGPS-Track 0162	01/24/2017 04:35:57 PM	01/24/2017 04:36:28 PM	Local	
Track 0163	01/24/2017 04:36:28 PM	01/24/2017 04:52:16 PM	Local	
Track 0166	01/24/2017 06:33:47 PM	01/24/2017 06:33:47 PM	Local	
Track 0168	01/24/2017 07:00:19 PM	01/24/2017 07:00:19 PM	Local	
WeakGPS-Track 0170	01/25/2017 08:39:30 AM	01/25/2017 08:39:30 AM	Local	
Track 0170	01/25/2017 08:48:22 AM	01/25/2017 08:48:22 AM	Local	

- Show Source File(s)
- Show Events
- Show Column Chooser
- Export Grid
- Map Selected
- Un-map Selected
- Animate Track**
- Tag Selected
- Un-tag Selected
- Adjust Time Offsets
- Copy (Control-C)
- Select All (Control-A)

40.826311026835, -75.0975724943144

Forensic Artifacts

- Files
 - Lifestyle analysis
 - Listening History

File Path	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\storage\bk1\Media\AP2_28.db
Original Path	C:\SG3-eMMC\p6\storage\bk1\Media\AP2_28.db
Device ID	8CB61EBAEC23
Device Name	Jim's Device
Device Type	Apple
Device Model	iPhone12,3
Vehicle Make	Ford
Description	Ford Sync Gen3

EVIDENCE (12,725)

Column view

File Name	File Path	Original Path
Roar	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
Live While We're Young	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
What Makes You Beautiful	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
Cruise	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
Story of My Life	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
028: The Price of Freedom	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
080: A Prisoner for Christ	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
082: Heatwave	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
087: Elijah, Part 1 Of 2	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
088: Elijah, Part 2 Of 2	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
088a: BONUS! Creating the Sounds for "Elijah"	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
089: That's Not Fair!	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
090: But, You Promised	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
091: A Mission for Jimmy	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
091a: BONUS! The Production of "a Mission for Ji...	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
092: The Ill-Gotten Deed	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
092a: BONUS! The Voices of Host Chris Anthony, f...	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
093: Rescue from Manatugo Point	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
102: The Treasure of LeMonde!	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
102a: BONUS! The Very First Focus dramas - Spar...	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
102b: BONUS! Spare Tire	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
102c: BONUS! House Guest	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
066: the Imagination Station, Pt. 1 of 2	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
067: the Imagination Station, Pt. 2 of 2	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
067A: the Creation of the Imagination Station (Bo...	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
072: an Encounter With Mrs. Hooper	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
073: a Bite of Applesauce	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
073A: the Inspoiration For "A Bite of Applesauce" (...)	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6

DIGITAL FORENSICS

COMPUTER FORENSICS

The logo for ENVISta FORENSICS. The word "ENVISta" is in a bold, white, sans-serif font, with a stylized white checkmark or slash over the letter 'V'. Below it, the word "FORENSICS" is written in a smaller, white, all-caps, sans-serif font, underlined by a thin white arc.

ENVISta
FORENSICS

CASE EXAMPLE: When Did Symptoms Occur?

- Claimed Illness
- Did he research symptoms prior?



DIGITAL FORENSICS

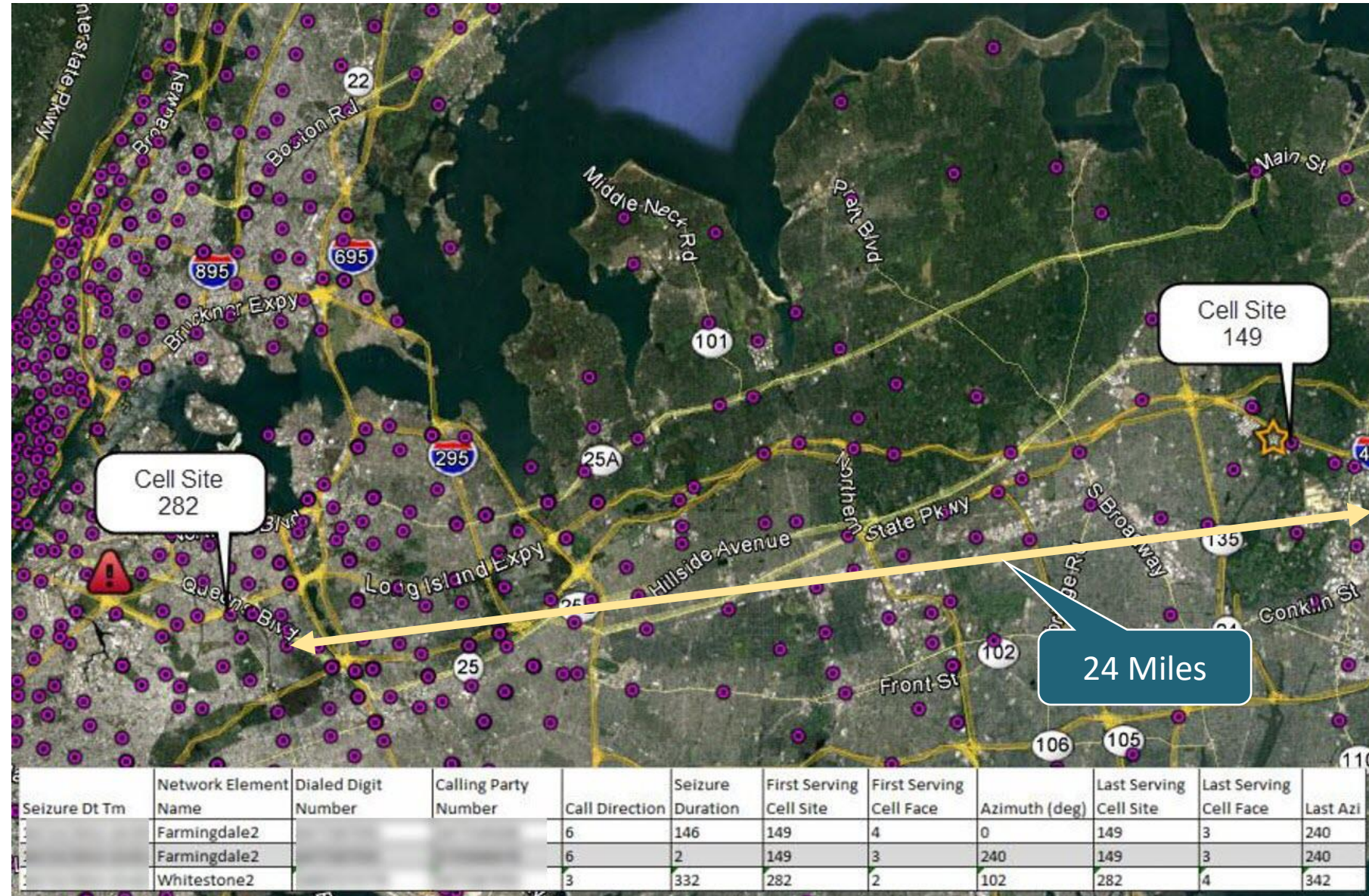
LOCATION FORENSICS

ENVISTA
FORENSICS

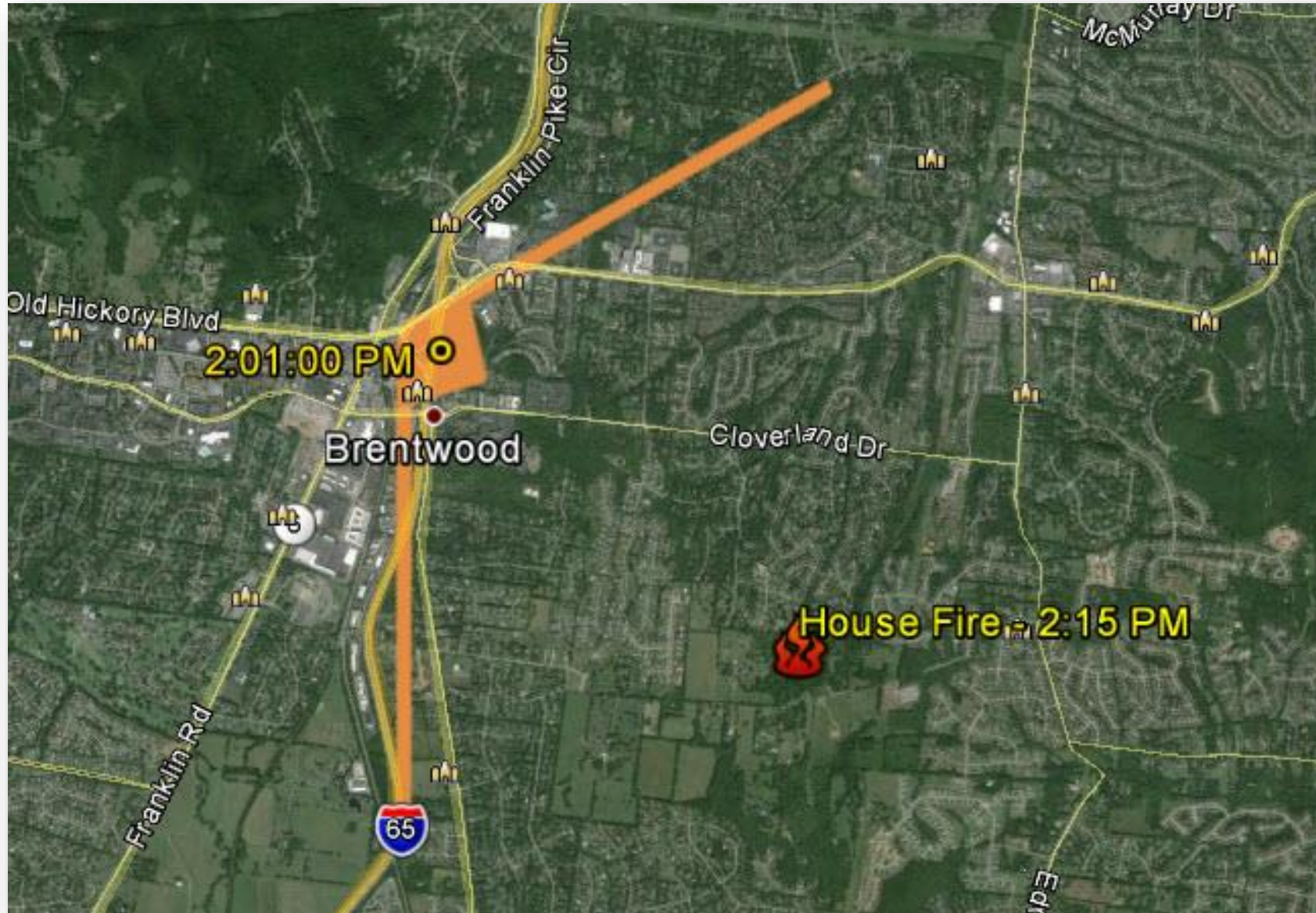


Case Example Accident with Location

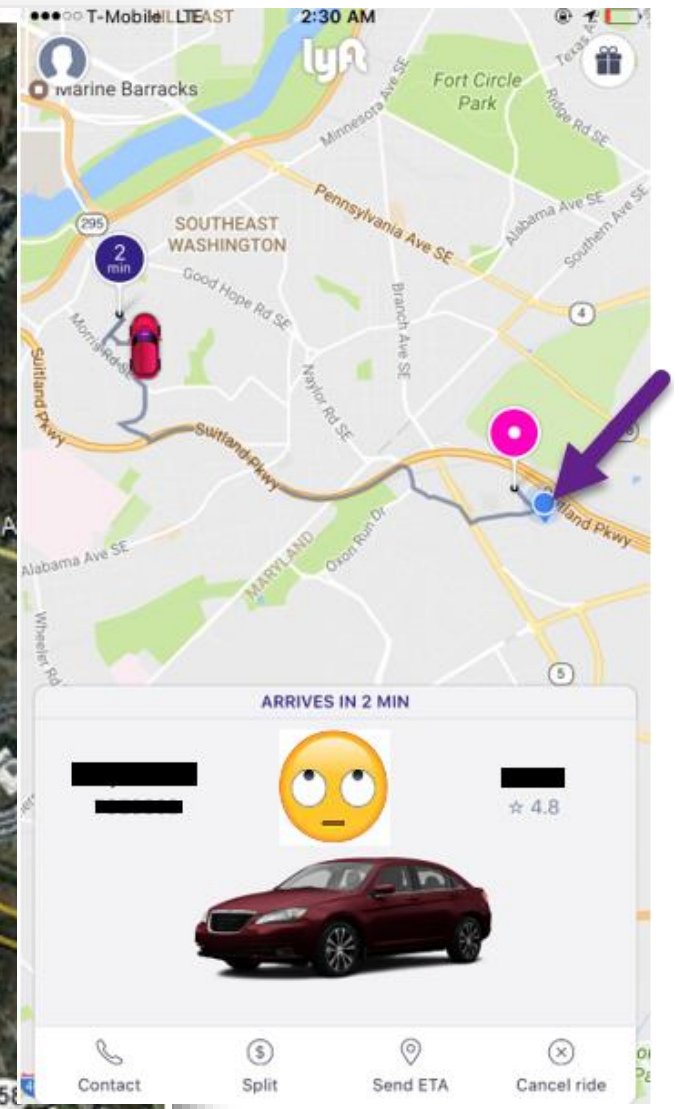
- In this example the last call made by the driver is 5 minutes prior to the accident time.
- The accident location is 24 air miles from the last call made by the driver.



CASE EXAMPLE: Call Detail Records: Arson



CASE EXAMPLE: Lyft Driver Assault Accusation





LARSDANIEL.io

lars.daniel@envistaforensics.com // 919-621-9335

LARS E. DANIEL EnCE, CCO, CCPA, CTNS, CTA, CIPTS, CWA
PRACTICE LEADER - DIGITAL FORENSICS
ENVISTA FORENSICS