Digital Forensics Services

Contents

Computer Forensics

Computer forensics is the oldest of the sub-disciplines that make up digital forensics. Computers are often the main source of digital evidence in civil litigation cases, and with good reason. Computers can contain a massive amount of useful information in a case in and of themselves. They can also contain

useful information about other devices like USB thumb drives, cell phones, digital cameras, portable hard drives, server shares, and cloud data. Almost all devices at one point or another circle around back to a computer. For instance, to create a backup of the information on your cell phone, it can be connected to the computer. The same is true if you want to get the pictures off a digital camera or USB thumb drive.

Computer forensics consists of examining evidence found on a computer hard drive and, in some instances, the examination of data on other hardware components within the computer, like the memory. The foundation of computer forensics is data recovery, and much of this sub-discipline revolves around that aspect.

While cell phones have surpassed computers as the primary form of evidence in most case types, computers still reign supreme in many forms of civil litigation. It is hard to imagine working without the use of technology today, and the hyper-connectivity of businesses is only accelerating. This connectivity requires computers, servers, and peripheral electronic devices to facilitate our modern work environment.

While this connectivity can increases the efficiency and quality of our work, along with it comes challenges, mostly surrounding the protection of sensitive data.

Confidential customer lists, proprietary information, and executive strategy documents are being transferred out of an organization by employees, or former employees, as we speak. These transfers do not require technical sophistication. Filesharing applications, cloud-based services, messaging applications, and personal email accounts can all be used to exfiltrate data. Sometimes these activities are intended by the employee, and at other times, it is done by accident or by an automated process of the computer. In all of these instances, a computer forensic examination would be needed to determine the root cause.

The Envista Difference: Computer Forensics Experts

Envista's computer forensics experts ensure that no stone goes unturned. We can assist in any phase of the digital forensics examination and have the forensic technology, certifications, and experience to provide the best outcomes for our clients, regardless of the amount or variety of data sources and the trajectory of the case. No matter what, our experts treat every case like it will go to court.

Our digital forensics experts come from law enforcement, military intelligence, and private companies. With this combined experience, both from a variety of backgrounds and thousands of computers examined, our experts can be trusted with your most complex and sensitive litigation matters.

Data Preservation

The forensic technology and methods utilized by our experts ensure that the data is preserved in such a way that it is defensible in courts and in accordance with digital forensic best practices and industry standards.

Data Collection

Even if your matter is complex, with data in multiple locations and formats, our team has the people-power and technology to comprehensively gather the relevant data for analysis.

Data Recovery

At the heart of digital forensics is data recovery. Regardless if the data has been deleted, manipulated, or corrupted, our team has the expertise to recover data in a forensically sound and defensible manner.

Forensic Analysis

Even if you recover mountains of data, it often needs to be analyzed, interpreted, and explained to stakeholders. We leave no relevant stone unturned in our examinations, and we strive to explain these findings in plain language.

Expert Testimony

Our experts have the certifications, credentials, education, experience, and expert testimony history to serve as credible expert witnesses in your case.

Cell Phone Forensics Certifications Our Expert Hold Include:

- Magnet Forensics Certified Examiner (MCFE)
- Certified Expert in Cyber Investigations (CECI)
- Encase Certified Examiner (EnCE)
- Digital Forensics Certified Practitioner (DFCP)
- Certified Blacklight Examiner (CBE)
- Certified Computer Examiner (CCE)
- Certified Forensic Investigation Professional (CFIP)
- Certified Mac Forensics Specialist (CMFS)
- OSForensics Certified Examiner (OSFCE)

- Certified Information Systems Security Professional (CISSP)

Cell Phone Forensics

Today's smartphones can perform functions that were possible only with a computer just a few years ago. In fact, the tables have turned. Many applications are only supported on phones, with developers choosing to ignore cross-platform development for computers entirely, and this is understandable. While you may use your computer at work and at other intermittent times throughout the day, you don't have constant access all the time as you do to the phone in your pocket, the constant companion.

Cell phones are used to make calls and send texts to transferring money and storing confidential documents. Cell phones store millions of data records in the form of emails, messages, pictures, location data, financial information, and thousands of others. Much of this data can be recovered even if it has been deleted.

Mobile Device Forensics

Our experts are certified and highly experienced in mobile device forensics. Coupled with access to state-of-the-art forensic hardware and software, our team possesses the technology and expertise to provide comprehensive consultation and analysis to help you achieve the best possible outcome in your case.

Our cell phone forensics experts can recover, analyze and report on the following common data types, among thousands of others:

- Text Messaging
- Social Media
- Location History
- Internet Activity
- Search Activity
- Email Communication
- Photos and Videos
- Voice Calls
- Application Data
- Biometric Data

- Financial Data

Cell Phone Forensics Certifications Our Expert Hold Include:

- XRY Certified Examiner (XRY)
- Cellebrite Certified Operator (CCO)
- Cellebrite Certified Physical Analyst (CCPA)
- Cellebrite Advanced Smartphone Analysis (CASA)
- Cellebrite Certified Mobile Examiner (CCME)

The Mobile Device Forensic Examination Process

Digital evidence is fragile and volatile. Improper handling of a mobile phone can alter or destroy the evidence contained on the device. Further, if the mobile phone is not handled following digital forensics best practices, it can be impossible to determine what data was changed and if those changes were intentional or unintentional. To protect the evidence and prevent spoilation, mobile devices need to be analyzed using mobile device forensic tools by a trained examiner.

The initial handling of digital evidence can be divided into four phases composed of identification, collection, acquisition, and preservation.

Identification

The identification phase's purpose and scope are to identify the digital evidence relevant to the case that possibly spans multiple devices, systems, servers, and cloud accounts. With a mobile phone, the data is not isolated only to the device. The data contained in the device can be synced to cloud storage or another mobile device or backed up onto a computer,

Identification also requires comprehensive documentation. Documentation is critical throughout the entire investigative process, but especially in the beginning, as a mistake here can taint the evidence. The acquisition phase gives us a perfect snapshot in time (forensic copy) of how the data exists. Since identification is the first step and before the acquisition, mistakes made here are carried out throughout the process.

Collection

The collection phase denotes gathering physical devices, such as the smartphone and other mobile devices. Since digital evidence can span multiple devices, systems, and servers, It can become more complicated than securing more traditional forensic evidence. There are vital functions that should be performed to protect the evidence:

Isolate Device Users

The primary goal of the collection process, other than ensuring all relevant electronic items are collected, is to protect digital evidence from contamination. One way this is done is by isolating the devices from their respective users until a forensic acquisition of the mobile device can be performed. While in their custody, the user could delete, create, or change data before the forensic acquisition (the perfect snapshot in time of the mobile phone data) is performed at their whim. They also could factory reset or wipe the device, permanently destroying some data or potentially everything on the mobile phone.

Isolate Devices

Along with isolating the mobile phone from the user, we also need to isolate the device itself. By design, mobile phones are intended for communication, and they are continually sending and receiving data even when they are on the bedside table charging overnight. If data transmission occurs, even with no person physically touching the phone, data can be lost, changed, or destroyed.

Isolation of the device itself is achieved by eliminating all forms of data transmission, including the cellular network, Bluetooth, wireless networks (WiFi), and infrared connections. By isolating the phone from all networks, the mobile phone is prevented from receiving any new data that would cause other data to be deleted, or worse, overwritten.

Preservation

The mobile phone's integrity and the data on it need to be established to ensure that evidence is admissible in court. First, a chain of custody is necessary. The second is a hash calculation of the mobile phone data.

Chain of Custody

Evidence preservation aims to protect digital evidence from modification. This begins with the mobile phone's proper handling by first responders, investigators, crime scene technicians, digital forensic experts, or anyone else who touches the device. A chain of custody must be maintained throughout the lifecycle of a case to demonstrate this.

Mathematical Hashing Algorithm

The forensic data collection process from the mobile device is better called a "forensics extraction," as data is extracted from the device instead of a perfect bit-for-bit copy of the evidence item. With the mobile phone powered on, the forensic software cannot access some areas of data. However, data that is inaccessible because the mobile device is powered on is usually of little to no value evidentiarily. Following the forensic copying comes the hashing process. A mathematical algorithm is run against the copied data, producing a unique hash value. This hash value can be thought of as a digital fingerprint, uniquely identifying the copied evidence exactly as it exists at that point in time.

Acquisition

The acquisition process is where a digital forensic examiner acquires, or forensically copies, the data from a mobile device. There are different methods of acquisition; some of these methods include:

Logical Extraction

A logical extraction of data from a mobile phone collects the files and folders contained on the device without any unallocated space. While what is commonly called "deleted space" is not recovered, deleted data on a mobile phone can be recovered using forensic tools and methods via a logical extraction. This data comes in the form of various database files, especially SQLite. Typically, data collected via a logical extraction includes messaging, pictures, video, audio, contacts, application data, some location data, internet history, search history, social media, and more.

File System Extraction

In effect, a file system extraction is an extension of a logical extraction4. This extraction collects much of the same data as a logical extraction and additional file system data. A file system

extraction allows the forensic tool to access the internal memory of the mobile phone. Accessing the internal memory means the forensic software can collect system files, logs, and database files from the device that a logical acquisition cannot.

These additional files allow for more deleted data recovery from database files and more data related to application usage on the device. Most applications store their data in database files on a mobile phone. Simply put, since a file system extraction recovers more of these database files, more deleted inside of those files can be recovered.

Physical Extraction

The physical extraction of a mobile phone captures the entirety of the device's data, including all files, user content, deleted data, and unallocated space. While this extraction method is the most extensive, it is also the least supported. Like the forensic imaging of a computer hard drive, a physical extraction creates a bit-by-bit copy of the mobile phone's entire contents.

With a bit-by-bit copy, the logical and file system data are recovered, as well as unallocated space. This allows for the recovery of deleted data from database files and unallocated space. Deleted data that otherwise would be inaccessible to a forensic examiner is now available for recovery, including location information, email, messages, videos, photos, audio, applications, and just about any other data contained on a mobile phone.

Backup Files

When you connect your mobile phone to a computer to make a backup of your device, it creates a file. This file can be ingested into cell phone forensics software and analyzed just like a forensic extraction of a mobile phone. Even if someone deleted the mobile phone data or the phone is missing, hope is not lost. The backup file can still contain the evidence you need in the case.

Cloud Data

Mobile phone forensic companies have developed tools that allow for accessing and acquiring data in the cloud. Cellebrite, the leading mobile phone forensic tool provider, can collect cloud data from cloud backups and the actual cloud-based applications themselves. While a forensic image of a mobile phone is a potential gold mine of evidence, the ability to use the mobile phone information to find even more evidence in the cloud is a significant force multiplier.

Reporting

If requested by the client, a report will be prepared of the data contained on the mobile device. Sometimes, it makes the most sense for our examiners to export all of the data from a cell phone for counsel's review. We do this in such a way to make it as accessible as possible, with the ability to search and filter the data.

In other instances, a more in-depth report is needed. Situations where this commonly arises are when timelines and what particular forensic artifacts, or data types, need to be explained to tell the story of what happened in a case.

Expert Testimony

Expert testimony is the culmination of everything that goes into a mobile device forensic examination, from consultation, acquisition, analysis, reporting, and finally to the courtroom. Selecting the expert with the appropriate technical expertise and experience is vital. Still, just as important is the expert's ability to explain technical concepts, forensic procedures, and digital artifacts in plain language. The use of jargon and acronyms is detrimental to the triers of fact. At the end of the day, if an expert has an airtight analysis but cannot communicate effectively to a judge and jury, the words are meaningless. When selecting an expert, choose the one you can have a conversation with. If that expert cannot explain technical details to you in an accessible way, they likely don't understand what they are talking about themselves.

Location Forensics

Our technology is tracking us, and this location data can be a major factor in many types of investigations. Given the connected world we live in, people may not be aware of the fact that everything they do, and nearly everywhere they go, their phones or devices can potentially track it. Unless someone is willing to forgo technology altogether, they will almost certainly be creating location data that can be utilized as evidence.

Not only do our devices record more information about our location history, but they are also recording more kinds of location data. The sources of location information are no longer reserved for GPS units and phone records. Your mobile phone is recording your location activity so it can act as a personal assistant, able to inform you when traffic is heavy when it predicts your about to leave for work. Your digital camera includes geolocation coordinates in the

metadata of the pictures you take. The infotainment system in your car can be recording where you go, even if you have no location set for navigation. And this is only scratching the surface.

Given the breadth of location evidence sources, and the depth of complexity for each individual source, our digital forensics division has a dedicated team of certified experts who specialize in location forensics.

Cellular Location Analysis

Despite the increased prevalence of call detail records being used in cases, both for determining historic location (or CSLI -Cell Site Location Information), or user activity, many are still unaware of how valuable this information can be in litigation or investigative matters.

What is a Call Detail Record?

A call detail record contains transactions between a cell phone and the wireless phone network. These transactions are automatically collected by the wireless phone company's equipment and stored for a period of time, anywhere from a few months to years, depending on the wireless company's policies.

The fact that call detail records are created as the result of the customer's phone using the wireless phone company's network provides legal proof that the service (voice, data, and text) is being provided. This means that if you call the wireless company and complain about not getting any service, they will pull your call detail records to see if that is actually the case.

Each call detail record contains technical details about each transaction your phone has with the wireless phone company's network, such as the date and time of the phone call or text message. Each record may also contain the starting and ending cell tower used for a phone call and, in some cases, text messages and data sessions.

How Call Detail Records Are Used

Determining Historic Location

Call detail records can contain the cell tower used for a phone call and in some cases, text messages and even data transmissions. This associates a phone call/text with a cell tower

location. By associating the activity with a cell tower, it is possible to determine an approximate location. This location information is often used in the establishment or discrediting of an alibi. However, beware that each type of transaction, voice, data, or text, may have different timestamps, and location information that is or is not reliable. You need an expert to assist you through that process.

Show "User" Activity

Determining user activity in a distracted driving accident is becoming an increasingly hot topic, both in civil and criminal cases arising from motor vehicle accidents.

Compared to a cell phone, call detail records have a limited set of information. This makes them easier for legal counsel to obtain. While a cell phone will tell you more, call detail records can still tell you a great deal of information related to voice calls, call forwarding, and text message and data transactions for particular service providers.

How to Get Call Detail Records

Call detail records can be obtained via subpoena to the wireless phone company. Example subpoena language can be found in our **Digital Forensics Resource Packet.** This guide also informs you what to expect to receive from different providers, be it Sprint, AT&T, Verizon, Metro PCS, or others.

The Envista Difference: Cellular Location Analysis

Envista's cell phone location experts are industry leaders on the subject of cellular technology evidence. This process is used to identify the location of a phone in question, typically used in a matter of litigation.

There is an increased prevalence of Call Detail Records (CDRs) used in legal cases to determine the historical location and user activity of a person of interest. Despite this, many are not be fully aware of how this information can make or break a litigated case or investigative matter. This type of evidence needs to withstand all forms of scrutiny, and choosing the proper expert is vital. Our cell phone location experts have worked on numerous, well-known, high-profile legal cases and are here to answer any questions, provide a thorough analysis, and help you uncover the truth.

GPS Forensics

Location data is often of great interest in litigation when attempting to establish or challenge an alibi. Today, almost every smartphone has a GPS receiver. This GPS data is used to track your location even when you are not utilizing navigation software or applications. It uses this information to provide you with restaurant recommendations near you, tag your Instagram photos with the geo-location data, allow you to see who is near you from your LinkedIn network, or give you a heads up on how long the drive home might take with current traffic.

Other than the mobile phone, GPS devices today include personal GPS devices and auto, aviation, and marine devices. Envista has certified GPS examiners on staff who can properly collect data from GPS devices in a forensically sound manner and analyze the data using state-of-the-art forensic tools and mapping technology.

Understanding Global Positioning System (GPS) Forensics

With GPS, each satellite in the system transmits navigation data toward the Earth that contains the satellite's position, a timestamp, and the health of the satellite. When a GPS device can receive signals from at least three satellites at once, the device itself can calculate its position in two dimensions, latitude and longitude. This process is called triangulation.

For a GPS device to calculate its position vertically for altitude, it must be able to receive signals from at least four satellites at the same time. This process is called trilateration.

The satellite signal data is refreshed every thirty seconds, once at the top of the minute and the bottom of the minute.

For the device to calculate its position, it needs to know the position of each of the satellites, the time it took for the signal to reach the device itself, and whether the satellite is healthy. Since the satellite travels at a known velocity, the data provides enough information for the device to perform the calculations.

The data contained in the signal is used by the GPS device to perform calculations not only for a position but also for direction (orientation) and speed. Bear in mind that direction and speed are derived values based on how the device is programmed to perform the calculations. Since device software is proprietary, the exact method and accuracy of the derived calculations can vary by manufacturer and model.

While the most basic GPS units only record waypoints and track points, GPS-enabled cellular phones and connected GPS units can contain a great deal more data that may be of evidentiary value.

Information from GPS Devices Can Include:

- Historic Locations
- Favorite Locations
- Trackpoints (locations where the GPS has been)
- Tracklogs (Complete list of Trackpoints the unit has created)
- Waypoints (locations where the user was physically and saved as a location of interest)
- Routes (custom series of Waypoints created by a user to navigate in a specific order)

Forensic Radio Frequency Verification (Drive Testing)

Worldwide, juries are presented with a Call Detail Record (CDR) and cell phone location information as part of trial evidence. This information can sometimes exonerate or convict an accused. However, today, many verdicts are under review worldwide due to improper analysis of cellular CDRs. Specific verification techniques can help further confirm the accuracy and completeness of a CDR analysis; these survey techniques are called forensic radiofrequency verification, often referred to as drive testing.

What is Forensic Radio Frequency Verification (Drive Testing)?

Forensic radio frequency verification, commonly referred to as drive testing, is performed using specialized techniques, hardware, and software, to collect data on radio frequencies in an area of interest. Our location forensics experts use this data to determine the actual coverage area of a cell tower and its sectors. From there, they can create what's known as a propagation, or coverage map, for a specific tower. With that information, it is easier to pinpoint and determine if a cell tower has optimal service for a phone that may be reviewed as part of a legal investigation.

The Value of Radio Frequency Surveys (Drive Testing)

When we receive information concerning CDRs, we only know the tower and sector in which a phone was connected at a particular time. Radiofrequency engineering data is not provided to an examiner. Using a drive test, the examiner can now see:

- Areas of the tower that are stronger than others
- Areas that have hot spots (or cell tower coverage that bleeds into others, creating spots of coverage that allow someone to connect to a cell tower farther away than expected)
- Areas that may not have coverage
- Other factors that may have affected signal coverage such as nearby wooded areas, bodies of water, large buildings, or topography

In other words, we can determine in much greater detail the likelihood of a cell phone connecting to a particular location. This data is used to validate claims concerning a person's location or challenge it if the radio frequency data collected through drive testing doesn't coincide with the mapping from call detail records alone.

The Envista Forensics Difference

Envista Forensics is one of only a handful of private companies that have access to the forensic software and hardware needed to perform forensic radiofrequency verification surveys.

Our experts are certified in cell phone forensics, cellular networking, and global positioning system forensics. Collectively, our location forensics team has provided expert witness testimony dozens of times.

Forensic Video Recovery and Enhancement

At the heart of digital forensics is the ability to recover data and to do so in a way that protects the original evidence. Today, video evidence is captured and contained on various devices, including digital video recorders (DVRs), mobile phones, personal cameras, home security systems, and body-worn cameras.

From private homes and vehicles to commercial businesses and government facilities, the use of video surveillance has never been more commonplace. The chances that an event critical to

an investigation will be caught on video have increased exponentially. To have the highest opportunity for success, digital video footage must be collected and protected according to digital forensics best practices and industry standards.

Forensic Video Recovery Experts

Our experts have extensive experience, including expert testimony, regarding collecting, preserving, and analyzing digital video evidence. Even when a DVR unit looked to be damaged beyond repair through fire or water damage, we have successfully recovered the digital video.

Comprehensive knowledge of forensic video data recovery processes, coupled with specialized digital forensics expertise, is the reason why our team has recovered video data in cases when others have failed.

Collecting and Protecting Digital Video Evidence

The digital video should be acquired and preserved based on the source of video footage and how it originated. Collecting data from a digital video recorder is different than collecting video from the cloud or a mobile phone.

Digital Video Recorders

A digital video recorder (DVR) is a physical unit installed in a location that records video footage onto a hard drive contained inside the device. It is common for a DVR to record video footage for a certain amount of time and then begin overwriting itself with new video footage. Although digital forensics is heavily focused on data recovery, the overwriting of data with new data does, in fact, constitute true deletion.

Further, how the video is exported out of the device is of paramount importance. If the video evidence is not exported in the most viable format and preserved correctly, or if the examiner does not perform the forensic examination properly, it is possible, and likely, to jeopardize the evidence. For example, if the video footage is exported in a low-quality format, and then the DVR overwrites the video footage of interest, the best evidence, high-quality video, can no longer be obtained.

An examiner performing forensic video recovery needs to thoroughly document their examination process so that another expert can duplicate the results. Without this documentation, it would be complicated and inefficient for another examiner to replicate the

results if it could be done at all. If the work cannot be duplicated, it calls into question the veracity of the evidence. It ultimately leaves it vulnerable to claims of spoliation, intentional, or unintentional due to ineptitude.

To protect the DVR evidence, our process includes:

- Creating a forensic image (which is simply a copy) of the hard drive inside the DVR to preserve the original evidence.
- When possible, we clone the data from the forensic image onto a new hard drive to use as a working copy.
- From the working copy, which is exactly the same as the original evidence hard drive, we recover and export the video footage using forensic hardware and software.
- All exports of the video footage are done in the highest possible quality available. This process is extensively documented to demonstrate that our examination produced the best evidence.

Body-Worn Cameras

The video footage from body-worn cameras can be contained in cloud-based applications and storage or at a physical location on a server or computer. In either instance, the video footage from these devices is usually contained inside proprietary software.

The benefit of these proprietary applications is that they usually have an audit log that cannot be modified or changed. However, the difficultly with body-worn camera applications includes gaining access to the video and these audit logs.

Having an understanding and familiarity with these systems is extremely beneficial during an examination. Our team of experts has first-hand knowledge of these devices and systems. Many have worn these cameras while serving in law enforcement before joining Envista and/or through direct analysis and data acquisition from these devices while working on various cases.

Smart-Home Surveillance Systems

Integrating smart home surveillance systems that connect to the cloud (remote storage) has revolutionized the consumer market for video surveillance systems. For a few hundred dollars or less, a home surveillance system can be installed by a layperson or homeowner in an afternoon. This video surveillance is usually of high definition quality with multiple recording cameras that can capture activity both at the home and on the street, the house next door, and more.

Further, since these are IoT devices, the video can exist and be collected from multiple locations, including a local computer, cell phone, or a cloud user account associated with the surveillance system. However, as with all forms of video surveillance, new or old, it is critical that the evidence is handled appropriately.

Depending on how the smart home surveillance system is installed and set up, it might only keep video footage for a short period of time before deleting it. When it becomes apparent that the recorded video could be of evidentiary value, it should be collected immediately by a qualified examiner. It also needs to be collected in a way that ensures the video is of the highest quality possible.

Forensic Video Enhancement and Analysis

Our Practice Leader, Lars Daniel, is our in-house expert providing photo and video forensics services. His qualification specific to this area are as follows:

I have over twenty years of experience in data recovery, information technology, graphic design, and digital video and image editing. I started working in digital forensics in 2009. I have been working solely in digital forensics for twelve years, and I have thousands of hours of experience in this area.

I am the co-author of *Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom*, published by Syngess, an imprint of Elsevier Publishing. I am also the co-author of the book *Digital Forensics Trial Graphics: Educating the Jury Through Effective Use of Visuals*, Published by Academic Press. My forthcoming book, "*The Attorneys Field Guide to Digital Forensics: Mobile Phones," will be released in early 2022.*

I authored chapter 38, *Video and Photo Evidence,* in my book *Digital Forensics for Legal Professionals.*

I hold numerous certifications in Digital Forensics, including the EnCase Certified Examiner (EnCE), Cellebrite Certified Operator (CCO), Cellebrite Certified Physical Analyst (CCPA), Certified Telecommunications Network Specialist (CTNS), Certified Wireless Analyst (CWA), Certified Internet Protocol Telecommunications Specialist (CIPTS), and the Certified Telecommunications Analyst (CTA) certifications.

I have provided training to my peers at the largest and most prominent annual digital forensics conference, the Computer Enterprise and Investigations Conference (CEIC), in 2011 and 2013, and 2016 and 2019 after the conference was rebranded as Enfuse

I have qualified as an expert witness and testified in state and federal courts, qualifying as a digital forensics expert, computer forensics expert, cell phone forensics expert, video forensics expert, and photo forensics expert. In addition, I have testified for both the defense and prosecution in criminal trials and the plaintiff and defense in civil trials. As it pertains to photo and video forensics, I have qualified as an expert in photo forensics three times and video forensics five times.

I have over 500 hours of training specific to digital forensics, including 20 hours of instruction from the Law Enforcement & Emergency Services Video Association International, Inc. I also received 29 credit hours of education from the University of North Carolina at Pembroke in fine art, digital art, and media integration.

I have trained many thousands of attorneys and claims professionals with over 300 classes taught, providing CLE (Continuing Legal Education) and CE (Continuing Education) classes Across the United States. Specific to photo and video forensics, I have provided CLE and CE training seventeen times.

Internet of Things (IoT) Forensics

Fitness trackers, smart appliances, connected vehicles, and even entire smart cities, hyper-connectivity is the future. This future means that more data than ever will be collected concerning our habits, location, activities, health, and financial information. Virtues and vices will be stored electronically, and when data is collected and stored, it can often be recovered using forensic tools and methodology.

Our digital forensics experts are trained and experienced in analyzing various forms of IoT devices. They have been, and continue to be, ahead of the curve on technological developments, from cellular location, to radio frequency verification surveying, to in-vehicle infotainment forensics. Our team is dedicated to providing exceptional service to our clients,

which can only be accomplished by being ready to face new sources of digital evidence head-on, with a passion for extensive research and training.

What Is The Internet Of Things? (IoT)

In plain language, the Internet of Things is composed of anything that is connected to the internet. This means that a cow with a chip in its ear is as much a part of the Internet of Things as a mobile phone, computer, smartwatch, or connected vehicle.

Some electronics collect and disseminate data, such as an activity tracker that uses sensors to gather and transmit heart rate activity and steps. However, this data is usually not stored on the device itself. It is sent to a device, or data repository, with the processing power and storage capacity to handle the information that the device has collected. These repositories, like computers and mobile phones, have long been examined for evidence, which is where the use of a digital forensic examiner comes into play.

There are unique issues surrounding IoT data preservation and collection, as collecting the information sometimes must be done through cutting-edge or non-traditional methods within the digital forensic community. In these instances, it is paramount that the data collection be done in a way that complies with the best evidence rules and acceptable industry standards for digital forensics when dealing with novel forms of evidence.

Common IoT Devices

Both consumer and commercial products are undergoing a hyper-connectivity revolution. They all collect data, and much of that data can be of evidentiary value. This data can be extracted and collected using state-of-the-art forensic hardware and software from devices such as:

- Smart Home Assistants
- Smart Appliances
- Connected Vehicles
- Fitness Trackers
- Smart Watches
- Home Surveillance
- Home Security Systems
- Smart Doorbells
- Robot Cleaners
- Drones

Vehicle Infotainment and Telematics Forensics

Many are familiar with Event Data Recorders (EDR) in vehicles. These devices record engineering data that can be useful when investigating a traffic incident. However, other data can be recovered from vehicles, and this data is becoming as comprehensive, if not more, than the data recoverable from Event Data Recorders.

This data is from the In-Vehicle Infotainment system in the vehicle. This is the actual screen in the center console that a user interfaces with, usually through a touchscreen, to select music, call or text, utilize applications, or navigate.

For hundreds of models of vehicles, digital forensic technology exists that allows the data from the In-Vehicle Infotainment system to be collected and analyzed. The information contained in the system includes data such as:

- Navigation history
- social media feeds
- emails
- text messages
- Bluetooth connections
- whether the vehicle's lights were on and off
- if the driver was turning volume or tuning knobs, opening a window, locking or unlocking doors, gear indicators
- Location and track points

This type of information can be critical for human factors experts to determine if a driver was distracted. For instance, were they selecting music on the touchscreen at the time of an accident, or were they reaching over to turn the tuning knob?

Also, imagine a scenario where a phone that was critical to a case had been lost or the data wiped. What if there are no cloud backups of the phone, and the phone was never backed up to a computer? There is still one place to look for the data; the car. When a user syncs a cell phone to a vehicle, it copies over contact lists, messages, emails, chat apps, and more depending on the vehicle and model of the phone. These are the types of things our experts can investigate to help uncover key evidence for a case or a claim.

END