2019 Annual Conference
March 13 -15 2019
Orlando, FL

Litigation in The Modern Age:
Will Today's Technology Be Tomorrow's Claim Investigation?

I. General Forensic and Procedural Principles

Digital evidence permeates every aspect of the average person's life in today's society. No matter what you are doing these days, there is probably a digital footprint being created that contains some type of digital evidence that can be recovered. Sending an email, writing a document, taking a picture with your digital camera, surfing the web, driving in your car with the GPS on; all of these activities create digital evidence.

Digital Forensics

Digital forensics is the application of forensic science to electronic evidence in a legal matter. While there are many different sub-disciplines and many types of devices, communication, and storage methods around today, the basic tenets of digital forensics apply to all of them. These tenets encompass four areas: Acquisition, Preservation, Analysis, and Presentation. Each of these areas includes specific forensic processes and procedures.

Acquisition

Acquisition is the first step in the forensic process and is critical to ensure the integrity of the evidence. As acquisition is the first contact with the evidence, it is the point where evidence is most likely to be damaged or destroyed. Simply turning on a computer can lead to the modification of hundreds of evidentiary items including files, date and time stamps, introduction of new internet history and the destruction of files that could be recovered from areas of the hard drive that are in the area of unallocated space.

Preservation

As evidence is collected, it must be preserved in a state that is defendable in court. Preservation is the process of creating a chain of custody that begins prior to collection and ends when evidence is released to the owner or destroyed. Any break in the chain of custody can lead to questions of the validity of the evidence. Additionally, preservation includes keeping the evidence safe from intentional destruction by malicious persons or accidental modification by untrained personnel.

Analysis

Analysis is the process of locating and collecting evidentiary items from evidence that has been collected in a case. In a case involving spousal infidelity, the evidence that must be located can include emails and chat logs between the spouse and their paramour. In a fraud case, financial records would be the target of the analysis, as well as the possible deletion of records involving financial transactions. In a child pornography case, locating contraband pictures and movies would be the target of the examination. Each case is unique in this respect as the circumstances surrounding each case can vary widely, not only in the evidence being sought, but also in the approach used to perform the analysis. The analysis portion is also the area where the individual skills, tools used, and the training of the forensic examiner have the greatest impact on the outcome of the examination. Considering that electronic evidence appears in so many forms and comes from so many disparate locations and devices, training and experience of the examiner begins to have an ever-greater impact on the success of the examination.

The analysis phase is also where the greatest disparity begins to become a factor between the skills and approach of a "computer expert" and a computer or digital forensics expert. While a computer expert may understand many aspects of computer usage and data, a properly trained forensic expert will be well versed in recovering data as well as proper investigative techniques.

Presentation

Presentation of the examiner's findings is the last step in the process of forensic analysis of electronic evidence. This includes not only the written findings or forensic report, but also the creation of affidavits, depositions of experts and court testimony. There are no hard and fast rules or standards for reporting the results of an examination. Each agency or private entity may have its own particular guidelines for reporting. However, forensic examination reports should be written clearly, concisely and accurately, explaining what was examined, the tools used for the examination, the processes used by the examiner and the results of that examination. The report should also include the collection methods used, including specific steps taken to protect and preserve the original evidence and how the verification of the evidence was performed.

Who Establishes Best Practices?

Guidelines published by the National Institute of Justice and the Association of Chiefs of Police set minimal standards for the collection and preservation of digital evidence. These guidelines are developed with the participation of law enforcement, government, academic, and industry practitioners. The best practices are then propagated to the industry through publications and digital forensic training programs. Certifications for persons in the field, such as the EnCase Certified Examiner (EnCE), the Computer Certified Examiner (CCE), the Access Certified Examiner (ACE), the Computer Forensics Certified Examiner (CFCE) and the GIAC Certified Forensic Analyst (GCFA), to name a few, reinforce these best practices by ensuring that the person being certified has a grasp of the proper procedures to correctly collect and preserve electronic evidence.

Who Should Be Following Best Practices?

Anyone who proposes to work as a computer or digital forensics examiner should always follow the established best practices in the field. This is vitally important in a field where the results of the examiner's actions are to be used to provide evidentiary findings based on the collection, preservation, and analysis of evidence. Failing to follow accepted best practices leaves the work of the forensic examiner open to challenge and the possibility of the evidence collected being suppressed. The very least of the results of failing to adhere to accepted minimal best practices in the collection and preservation of evidence can cast doubt on the skills and qualifications of the examiner and the entirety of the examiner's work and potential testimony.

Summary of Best Practices

Best practices apply to the collection and preservation of evidence. These are the two critical parts of ensuring that evidence will be accepted in a court of law as being authentic and an accurate representation of the original evidence. Modification of evidence, either intentionally or accidently can have a devastating effect on the entire case. Understanding best practices is critical for the legal professional so that attorneys and judges can properly assess the authenticity of the evidentiary findings. This is also critical for business and information technology professionals to understand that even if they are preserving evidence for the possibility of future litigation, these practices must be followed to protect the evidence.

If we look at preserving evidence as the over-arching part of the collection and acquisition of digital evidence, we can see that the need to protect and preserve evidence begins BEFORE anything is collected, copied or analyzed, and ends only at the final disposition of evidence. Whether that final disposition is to return the items collected to the owner, permanent seizure of the items by the government or the destruction of that evidence via a destruction order, the preservation of the evidence must persist. In the digital forensic field, preservation is the overall protection of evidence, while acquisition is the actual act of making forensic copies of digital evidence either from hard drives, some other physical media or live memory.

II. Legal Considerations for Securing Information and Data

Preservation Notices

When faced with a claim involving a scene where critical evidence may be altered or destroyed, a timely preservation notice should be sent to all parties involved. The letter need not be long or complicated. Rather it should be simple, direct and to the point. The recipient should be placed on notice that the electronic data and evidence should be preserved. The notice should inform the recipient that if the data is not preserved, he or she may face a claim of spoliation.

Restraining Orders

If you learn that data is about to be destroyed and that data is critical to your case, a motion seeking a restraining order may be filed. The motion should be done via an emergency basis and the opposing party should be given notice. A preservation notice should also be served. It has the added benefit of court's oversight. However, timely access to the court can be an issue.

Subpoena Duces Tecum

A subpoena duces tecum is a writ issued by a court through counsel to compel production of evidence by a witness under penalty for failure. The requests for items must be specifically spelled out and a witness has a right to object.

Rules of Evidence Regarding Admissibility

Simply stated the rules surrounding the admissibility of evidence are to make sure that the evidence placed before a jury is reliable. Today, eyewitness testimony can be enhanced, corroborated or refuted by a technical data that comes in a myriad of forms: cell phone recordings, GPS data, emails, text messages, comments on social media sites and even Twitter. How then is a Judge supposed to deal with newly developed types of evidence that did not exist when the rules of evidence were formulated? The answer is that Judge will require that the party offering evidence lay a foundation which shows that the evidence is reliable before it is placed before the trier of fact.

The first step in establishing the proper foundation is authenticate the data. That is, the proponent must show that the evidence is what it is represented to be. For example, a witness may testify that she is familiar with the image taken from a drone and identify the items shown in the imagery. The evidence must also be relevant. That is, it must have a tendency to either prove or disprove a fact at issue in the case. Note that the evidence must not contain *hearsay* which is an out of court statement offered to prove the truth of the matter asserted. If the aforementioned drone imagery contained a soundtrack, the Judge may allow the image but preclude the statements that go along with the image. That is, allow the video to play with the sound turned down. Finally, the probative value of the evidence must outweigh any prejudicial effect.

Spoliation

The most critical aspect of any successful investigation is the preservation of evidence for use at trial. In *Landry v. Charlotte Motors Cars, LLC,* District Court of Appeal of Florida, Second District, 2017, the Court reiterated the severe sanctions for spoliation of evidence: "Generally speaking, sanctions may be appropriate when a party has spoliated, lost, or misplaced evidence. League of Women Voters of Fla. v. Detzner, 172 So. 3d 363, 391 (Fla. 2015). Spoliation is defined as "[t]he destruction, or significant and meaningful alteration of [evidence]," Vega v. CSCS Int'l, N.V., 795 So. 2d 164, 167 n.2 (Fla. 3d DCA 2001) (quoting Black's Law Dictionary 728 (5th ed. 1983)); or "the failure to preserve property for another's use as evidence in pending" or reasonably foreseeable litigation, id. (quoting Jay E. Rivlin, Note, Recognizing an Independent Tort Action will Spoil a Spoliator's Splendor, 26 Hofstra L.Rev. 1003, 1004 (1998)). See also Aldrich v. Roche Biomedical Labs., Inc., 737 So. 2d 1124, 1125 (Fla. 5th DCA 1999) (similar definition); *Spoliation*, Black's Law Dictionary 1620 (10th ed. 2014) (defining spoliation as "[t]he intentional destruction, mutilation, alteration, or concealment of evidence"). Evidence is deemed "lost" when it is "beyond the possession and custody of its owner and not locatable by diligent search." *Lost*, Black's Law Dictionary 1089 (10th ed. 2014).

To guard against spoliation, ensure that your experts carefully observe legal protocols concerning the preservation of evidence when removing evidence for the scene, and during subsequent storage and testing. Written agreements should be obtained among all potentially interested parties whenever feasible prior alteration of evidence (including removal from scene). Obtain a court protective order when agreement cannot be reached. Consult with legal counsel and your experts early on about this crucial issue - the credibility of your expert testimony can be weakened or destroyed by the mishandling of evidence.

III. Drones-Unmanned Aircraft Vehicle (UAV) and Aerial Imagery

In the past, experts placed themselves in danger to fully document a scene in dangerous and in some cases untenable conditions. In some cases, documentation from above required the costly retention of actual aircraft to overfly, when permitted, a large scene. Though said aircraft would provide overview photography, the detailed documentation would be limited. Today, UAV's have become an integral tool for documenting a scene safely, quickly and with great precision. UAV's are used in many different claims' scenarios including in fire and explosions, accident reconstructions, damage assessment and water intrusion.

UAV's are an economical tool for the expert and can easily be outfitted with high-resolution cameras or thermal imaging technology. The camera systems today allow an expert to identify and document items that are crucial to an investigation with such clarity that even a manufacturer's label can be read from a drone. Detailed measurements can be obtained from an overfly that will allow a scaled diagram to be completed in a matter of minutes. Evidence identification and documentation has become possible in the harshest of conditions as a result of drone technology.

The Federal Aviation Administration (FAA) has implemented regulations for small drones weighing less than 55 pounds. Part 107 of FAA regulations requires that all drones be registered through the automated registration system. An operator must be at least 16 years old who holds a remote pilot certificate with a small UAS rating or be under the direct supervision of a person who holds such a certificate that is attained through a written test.

Anyone acting as a pilot in command must insure that the drone is safe before flying, must make the drone available for FAA inspection and report any operation that results in a serious injury or property damage exceeding $500.00. There are designated airspaces throughout the US that are restricted such as areas immediately adjacent to airports. An operator must be aware of these designated airspace of operation and obtain any necessary waivers and permissions to fly.

IV. Artificial Intelligence (AI)

Artificial intelligence is the science of creating and developing intelligent machines that work and react like humans. This technology can and is being used to both replace humans or collaborate with humans. For example, artificial intelligence has been shown to be better at document review than real lawyers based upon testing performed by LawGeex, "For the study, 20 human attorneys were pitted against LawGeex's AI in reviewing 5 NDAs. The controlled conditions of the study were designed to resemble how lawyers would typically review and approve everyday contracts. After two months of testing, the results were in: the AI finished the test with an average accuracy rating of 94 percent, while the lawyers achieved an average of 85 percent. The AI's highest accuracy rating on an individual test was 100 percent, while the highest rating a human lawyer achieved on a single contract was 97 percent."[1]

[1] https://futurism.com/ai-contracts-lawyers-lawgeex

AI has also been shown to be comparable or better at than humans at spotting eye disease[2] and detecting earthquakes[3], however, AI also creates complications when it comes to determining liability when an incident does occur, not to mention the cybersecurity risks associated with AI. Example scenario: Traffic lights are run by artificial intelligence to improve efficiency. Driverless cars are also run by artificial intelligence. These two systems must synthesize in order to operate correctly and without error. If an accident does occur at an intersection, determining fault could be problematic, it could be:

1. Coding error by a programmer for either the driverless vehicle or the traffic light systems.
2. Purchased code from a 3rd party vendor used one party when creating their software
3. An operating system crash that the applications are run on
4. A physical failure of a part related to the vehicle or traffic system
5. Firmware coding (making the hardware speak to the software) issue that caused physical or software failure from a 3rd party vendor.

V. Global Positioning System (GPS)

How GPS Works

Each satellite in the system transmits navigation data toward the Earth that contains the position of the satellite, a time stamp 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.

In order 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.

In order 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 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.

[2] https://futurism.com/medical-ai-may-better-spotting-eye-disease-real-doctors/

[3] https://www.theverge.com/2018/2/14/17011396/ai-earthquake-detection-oklahoma-neural-network

A connected GPS unit is one that has a cellular radio built into the unit. Some examples of this are the navigation systems currently available in many vehicles that use the On-Star or Microsoft Sync systems.

These units have the ability to make phone calls, receive real time traffic alerts, and search for local shopping deals, find movie times and other functions.
Since many of these units will also allow Bluetooth connections to smart phones, they can contain phone call logs and contact lists. And depending on the phone and unit, they can even receive text messages.

Preservation of GPS data
GPS units are radios that receive data from radio signals transmitted by GPS satellites. This means that in order to properly handle a GPS unit for evidence collection, the unit should be handled in a windowless room and inside a Faraday bag that will block any radio signals from reaching the unit. This is especially important in the case of units that have the Assisted GPS (AGPS) feature. The AGPS system allows the unit to receive information from the cellular phone system to help it more accurately determine its location in areas where a clear view of the sky is a problem.

VI. Smart Devices Smartwatches and Fitness Trackers

Internet connectivity is finding its way into physical devices at an ever-increasing rate. This interconnectivity is making our lives more convenient, but at the expense of extensive data collection about us, and also increase security risks to both electronic and physical assets. These wearable devices are part of the Internet of Things (IoT).

There are unique preservation collection and preservation issues related to IoT data, as collecting the information is often done through cutting-edge or nontraditional methods within the digital forensics' community. Most data related to IoT devices can be recovered and collected from the devices themselves, computers, and cell phones, and how these devices act as "repositories" of data coming from IoT devices.

Wearable technology, such as fitness trackers, can contain information about a person such as their heartrate, sleep quality, activity, including both normal activity such as walking and vigorous activity like exercising, among other data types. This information can be very personal and can be used for many forms of analytics to determine content viewing times, routes of travel, markers of healthiness and disease, or if your claims of physical activity match reality.

Social Media

The revenue for social media websites and applications usually comes primarily from advertising. If the websites were locked down with privacy and security as their main objective, it would inhibit their ability to have maximum user traffic. While enhanced privacy options are available with these websites, for the users themselves there is always a trade off when these security measures are employed. Usually, when a user places enhanced privacy or security on their information the convenience of using the social media outlets can be decreased. In our experience, with almost all forms of digital information and devices, people tend to err on the side of convenience. Typically, the more security that is in place, the harder it is to share your information with others, which makes it more difficult to connect with people in social media websites and applications. Since the primary purpose of social networking is in fact to network with others, it is not difficult to understand why someone might risk their information for the sake of convenience, if they even consider privacy to be a priority in the first place at all. Some common social media include Facebook, Instagram, LinkedIn, Snapchat, YouTube, Blogs, Twitter, Hanzo.

Social Media as Evidence

Social media evidence works best when it is a part of a body of evidence, meaning that it is usually optimal to use that information in conjunction with evidence gathered from other sources, such as cell phones and computers. However, an examination can be performed successfully with only the information available from social networking sites and other information available online.

Connecting Evidence from a Device to Social Media Evidence

During the process of a computer or cell phone examination, it is common to find information pertaining to the social media activity of a person. A computer for example can store information about social media websites in internet history and unallocated space. While only a limited amount of information might be available on the computer regarding social media activity, if pertinent information is found, such as usernames or an email address; that information can then in turn be used in the process of a social media examination to find information about the person of interest online.

Case Example / Wrongful Termination Case

The following case example illustrates this; we were retained in a civil case by a company in the position of defendant. They were being sued for wrongfully terminating an employee. By examining this employee's computer, we were able to find numerous email addresses belonging to him that were previously unknown. We were then able to use these email addresses to find usernames belonging to him. These usernames were associated with social media accounts. This allowed us to locate his activity on message boards where he posted questionable content. This then led to us being able to associate an email address with him from the forum information. This email address was used in the registering of a website domain name, which was a point of contention in the case. The collection of the online information was a direct result of information located on the person's computer.

VII. Surveillance

Video and image evidence must be handled with great care, and any examinations or enhancements performed must be thoroughly documented. If the evidence is not received in the most viable format and preserved correctly, or if the examiner does not perform the forensic examination properly, it is possible to jeopardize the evidence. With surveillance footage becoming more common due to the availability of home systems that are both affordable and require a low amount of technical sophistication to install, the prevalence of such evidence has increased dramatically over the past few years. While surveillance footage is more common, the means by which is it collected, examined, and if necessary, are enhanced, are of paramount importance.

Documentation is paramount when examining video and photo evidence. The Law Enforcement/Emergency Services Video Association explains the necessity of proper and thorough documentation as follows:

> "The best way to ensure the reliability of the video evidence is to have standard operating procedures (SOPs) in place. SOPs assist the forensic video analyst in maintaining proper records of the processes used to examine the evidence and that the processes are performed in a scientifically appropriate and uniformed manner. Records should be complete enough that a similarly experienced and trained individual, working with the same technology, could reproduce similar results."[4]

Just as with computer evidence, an examiner dealing with video and photo enhancement needs to document everything they do in the process of their examination so that another expert can duplicate the results. Without this documentation, it would be extremely difficult and inefficient for another examiner to duplicate the results, if it could be done at all. Improper documentation also calls into question the viability of what the examiner produces in forensic analysis or enhancement, as the improper handling of video and image evidence can create visual information that did not exist in the original video or image, known as artifacts.

VIII. Imaging

A magnetic resonance imaging (MRI) scan is a common medical procedure. An MRI uses a strong magnetic field and radio waves to create detailed images of the organs and tissues within the body. A computerized tomography (CT) scan combines a series of X-ray images taken from different angles around the body and uses computer processing to create cross-sectional images (slices) of the bones, blood vessels and soft tissues inside the body. CT scan images provide more detailed information than a regular X-rays.

Fluoroscopy is a type of medical imaging that shows a continuous X-ray image on a monitor, much like an X-ray movie. During a fluoroscopy procedure, an X-ray beam is passed through the body. The image is transmitted to a monitor so the movement of a body part or of an instrument or contrast agent ("X-ray dye") through the body can be seen in detail.

The use of images from these diagnostic scans can dramatically assist a jury in understanding an expert's testimony. For example, in a case involving a serious auto accident, it was undisputed that plaintiff sustained a head injury. As time progressed, plaintiff's cognitive condition worsened to the point where he needed institutional care for the rest of his life. Several physicians argued that plaintiff had chronic **traumatic** encephalopathy (CTE) brought about by the accident. This disease has become well know because it is found in NFL players. Our expert vehemently disagreed stating that a degenerative **neurological disease** caused the dementia. He was able to use MRI and CT scans to show the development and progression of what is known as "cerebral atrophy" over time. He chose three pictures of horizontal images of

[4] Law Enforcement/Emergency Services Video Association (LEVA), *Guidelines for the Best Practice in the Forensic Analysis of Video Evidence.* http://www.leva.org/pdf/BestPractices forVideoEvidence.pdf

plaintiff’s brain at the same level (just above the eyes). The three pictures had been gleaned from scans taken at various times both pre- and post-accident. They clearly demonstrated that the brain’s ventricles and sulci became bigger and that more cortical brain cells were lost over time. This progression was wholly inconsistent with a traumatic injury and showed that the dementia was an organic degenerative disease - either Alzheimer’s Disease or frontotemporal dementia. Neither of these diseases could have been caused by the auto accident.

The case was challenging because the plaintiff was making a simple causation argument that was familiar to the jurors. We needed something to get the jurors attention and convince them that the simple answer was not the correct one. The medical technology provided the rebuttal that we needed.

The case study demonstrates the following practical pointers:

- Be thorough in your investigation of prior medical records as it was the exhaustive and thorough gathering of medical records that provided the key scans for our expert to compare.
- Be sure to provide your expert with all medical records to protect him or her on cross examination.
- Finally, make sure that all portions of the piece of evidence to be shown to the jury have proper foundations.

Matteport’s 3D cameras captures any loss in its entity, including its exact dimensions, with no ability to inadvertently alter images or measurements. It is a comprehensive loss documentation for contents, automatic floor plan creation for use in Xactimate, and sharing with adjusters, estimators, and consultants.