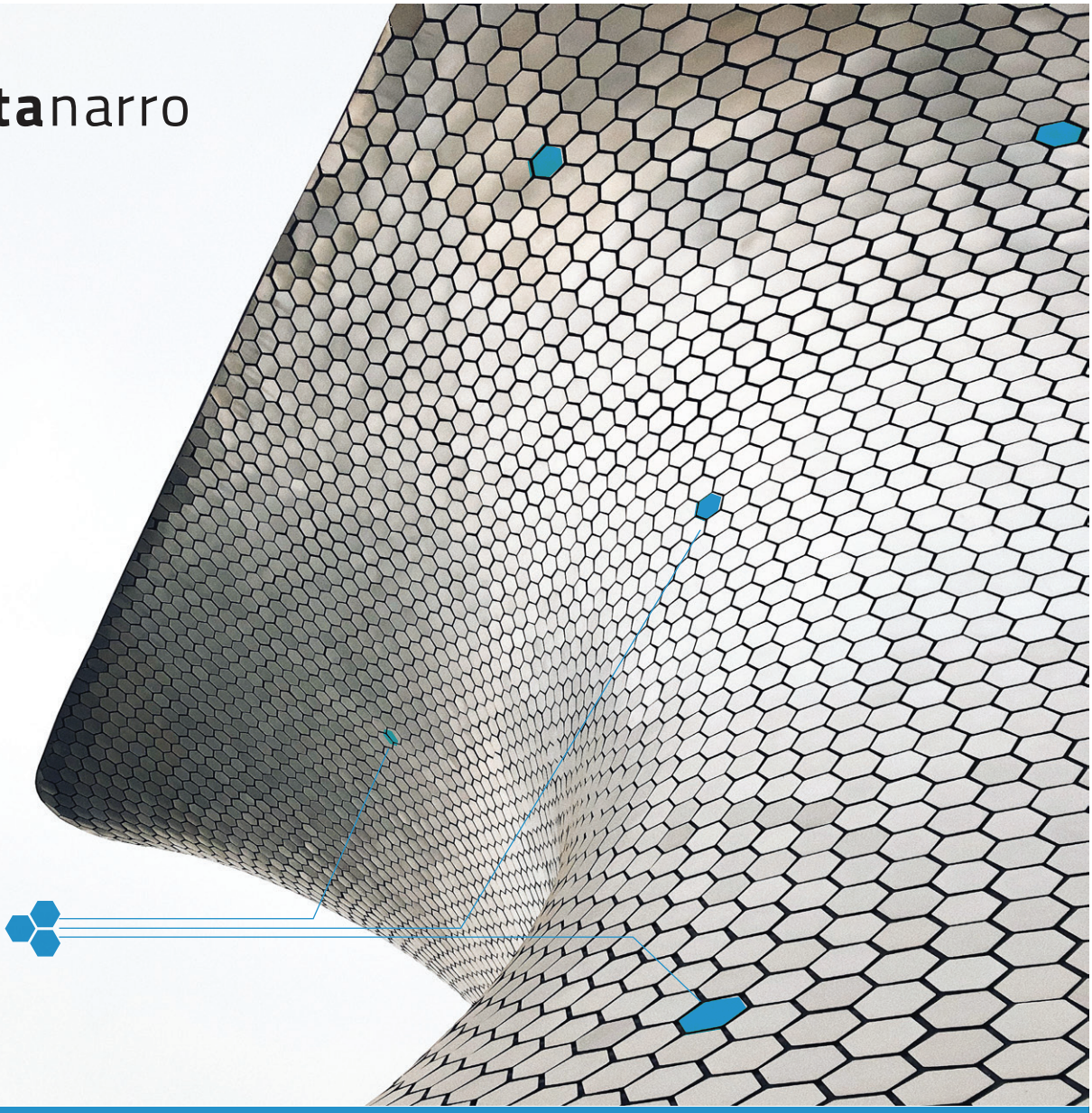
datanarro



THE 2020 ATTORNEY'S GUIDE TO DIGITAL FORENSICS

By Kristian Larsen & Erik Thompson

The 2020 Attorney's Guide to Digital Forensics

INTRODUCTION

The past decade has produced a seismic shift in the world of civil litigation and evidentiary discovery. Whereas digital evidence once played a supporting role, in 2020 it is likely the star player. Smartphones, social media, messaging apps, and an abundance of connected devices are tracking our daily routines and generating mountains of data.

This data, when properly collected and analyzed, can be an invaluable resource for attorneys that need evidence to strengthen a case. As technology has advanced, the potential sources of digital evidence have grown exponentially. By developing a solid understanding of the processes and capabilities of modern digital forensics, informed attorneys can generate a distinct advantage for their clients and cases.

PURPOSE

The purpose of this e-book is to provide attorneys and legal professionals with a contemporary field guide to modern digital forensics. While we'll cover the basics of digital forensics, our goal is to detail recent advances and provide insight into what you can expect in the coming decade. While we may touch on elements of criminal investigations, we will focus on digital forensic applications for civil litigation. Along the way, we'll alert you to new sources of digital evidence, providing you with the awareness to better drive e-discovery efforts for you and your clients.

What Exactly is Digital Forensics?

If we look at the standard definition, we might describe digital forensics as the detailed investigatory examination of digital media to uncover electronic evidence that supports or refutes a hypothesis. As a branch of forensic science, digital forensics follows established processes and procedures that ensure that digital evidence collected during an investigation will maintain credibility and integrity for use in possible legal proceedings.

More importantly, digital forensics tells the story of digital information. Skilled digital forensic investigators can trace the history of files and artifacts to help you build a strong legal argument. How did a file get there? Who had control over that file? Where was it transferred? Investigators can help prove that the defendant had knowledge of a document or that data was transferred to a third-party. Expert digital forensics helps win cases.

Digital Forensics vs. E-Discovery

There is often a bit of confusion between the concepts of digital forensics and e-discovery. Are they the same thing? Are they different concepts altogether? The answer is somewhere in between.

In general, we can say that e-discovery is an activity, typically engaged in civil litigation, that is used to identify and preserve potential digital evidence that resides in the form of **Electronically Stored Information (ESI)**. E-Discovery follows well-established processes that help maintain the integrity of ESI during evidence gathering, and later, through potential litigation.

When digital forensics is engaged in as part of the e-discovery process, it is typically thought of as a subset of that process.

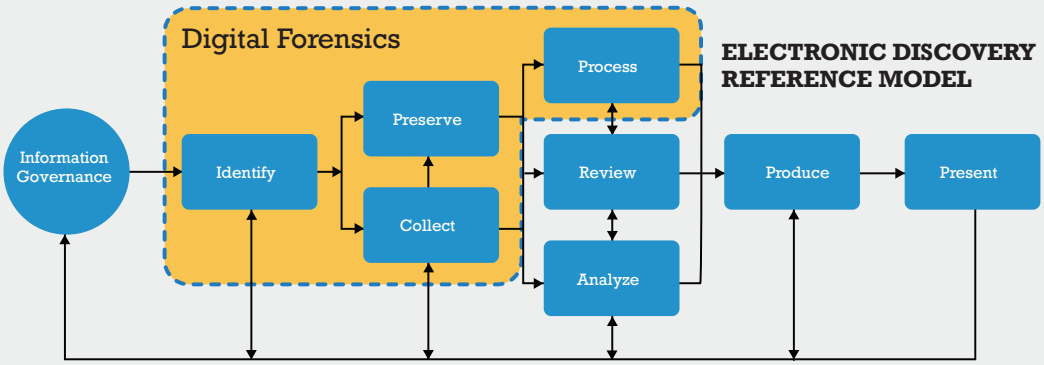


Figure 1: *The above EDRM diagram is a conceptual represention of an e-discovery project. This model breaks down the typical phases of e-discovery. We have highlighted those phases that are most likely to include elements of digital forensics.*

To understand this relationship better, let's refer to the popular **Electronic Discovery Reference Model (EDRM)**. In the diagram above, the various phases of an e-discovery project are broken down. Digital forensics occurs primarily in the **collection** and **preservation** stages, but can also contribute to the **identification** and **processing** stages.

It is important to note that not all e-discovery projects will require digital forensics work. In some e-discovery cases, it is merely enough to request a set of email records from the opposing party. Their IT staff can pull the request information and forward it on. No deep investigative or forensic activities are necessary.

However, discovery requests are rarely that simple. More often than not, parties will need to provide information from a broad set of repositories that include not only email, but messaging, file transfer, website search activities, and more. Some of this information may be readily retrievable, but most of the time it is not. In cases such as these, a digital forensics investigation is recommended.

DIGITAL FORENSICS OFTEN STANDS ALONE

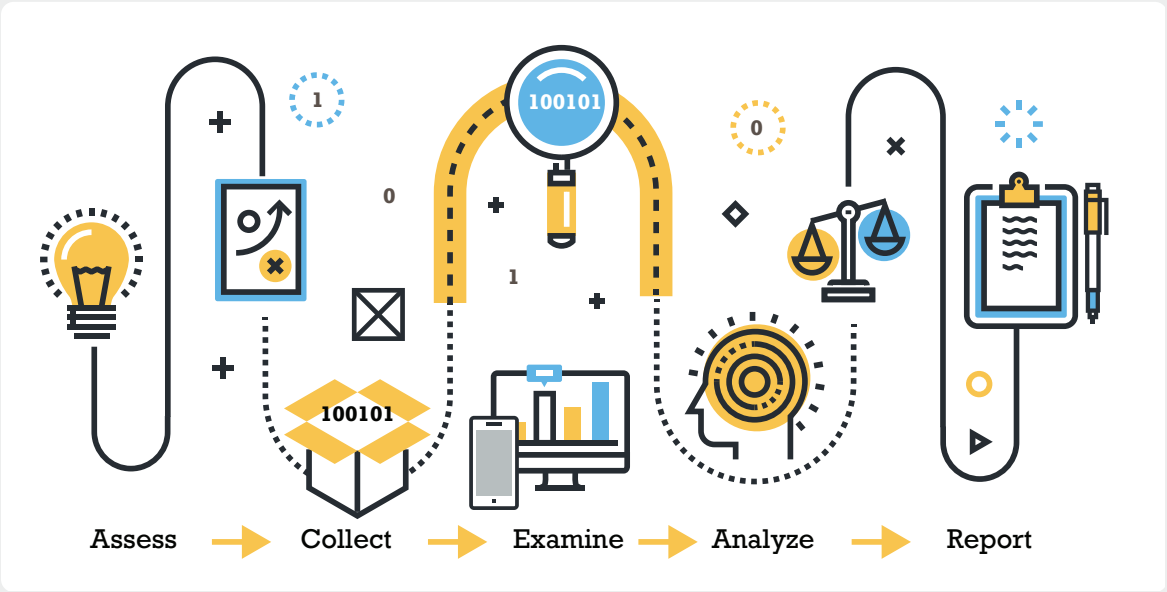
We feel that it is important to mention that while digital forensics may be employed during an e-discovery effort, digital forensics often exists independently from e-discovery. Digital forensics can be used anytime there is a need to recover data or establish the provenance of digital information. Attorneys should employ digital forensics services to help determine the strength of potential litigation or gain insight into drafting a discovery request. Forensic experts can provide strong investigative and analytical resources that can help make or break a case.

The History of Digital Forensics

Many of you may be familiar with the term **computer forensics**. You may be wondering why we now call this field **digital forensics?** The explanation has to do with the fact that we are living in an increasingly digital world.

Computer forensics has its roots in the '60s and '70s, but back then, it was hardly a science. Examinations were performed by system administrators knocking around mainframe computers, operating without any methodology or scientific processes. Over time, national organizations and investigative agencies brought a level of scientific rigor to this emerging field.

While computer forensics may have been an appropriate term for a time, we are now living in an era of interconnected smart digital devices—phones, TVs, speakers, watches, doorbells, and cameras, each with the potential to track and store information about our activities. It's only been about ten years since we saw a big push toward renaming the field. It makes sense—it's simply more appropriate to refer to this field as "digital forensics" as this phrase encompasses a broader range of potential electronic devices and digital platforms.



The 5 Stages of Digital Forensics

Before we get too far along, let's review the five primary stages of a digital forensics investigation. While different organizations may categorize the stages differently, all examinations will include these necessary steps in one form or another.

ASSESSMENT

Whenever civil disputes turn litigious, we always encourage attorneys to bring a digital forensics professional aboard their team. Before any data is ever collected, a digital forensics professional will need to assess the situation and develop a game plan for a forensic investigation.

Ideally, you will have the services of a digital forensics professional before your **meet and confer conference.** These pre-trial meetings can have a dramatic effect on the case and its outcome, so it's important that you have the best possible resource for understanding complex IT infrastructure, data storage, file formats, and production strategies. Guidance from a digital forensics professional can help guide you to the data that is most critical to your case. You'll end up with a plan that enables you get the information you need while lowering the overall cost of collection.

Even if you contract a digital forensics professional later in the game, he or she will need to have a strong understanding of the pending litigation and the types of information that could be useful in supporting or refuting the central claims of the case. If there is already a discovery request in place, the investigator will need to see it. It is critical that the investigator defines what they are looking for and how they intend to collect the data in a manner that is consistent with the **Federal Rules of Civil Procedure (FRCP)**.

WHAT IS A FORENSIC COPY?

The term **forensic copy** typically refers to an exact bit-for-bit copy of the entire physical hard drive, including unallocated and slack space.

However, it is possible to make a forensic copy of drive volumes (like the c: drive), cloud storage accounts, or individual folders.

In these cases, we might be better served if we modify our definition of a 'forensic copy' to be **an accurate replica of the source data in which the metadata and content are not altered.**

A forensic copy is almost always created as a read-only container with self-authentication built into it.

To better understand forensic copies and the technology that enables them, check out this helpful article:

CLICK TO VISIT ARTICLE

Let's suppose that you are asked to investigate a case where an employee is suspected of stealing intellectual property from an employer. It may be obvious to search the accused's computer hard drive, but it is essential to identify other potential sources of information—this may include thumb drives, email, messaging apps, social media accounts, mobile phones, or cloud-based storage. A good digital forensics professional will be able to assess the effort required to examine a broad assortment of digital repositories and can devise a plan to obtain that information. Additionally, the investigator can guide efforts to draft a discovery request or respond to one.

COLLECTION

As a general rule, it is unacceptable to perform digital examination directly on source media that contains potentially discoverable information. Even experienced IT personnel can damage the integrity of an investigation by making informal backups or doing a cursory examination of the source media. A quick peek at a target's emails may trigger events that can delete materials, update metadata, or overwrite information located in unallocated space.

Before any examination can occur, the source media needs to be copied in a way that preserves the integrity of the original. This can be accomplished by making a **forensic copy,** which is usually the first step a forensics investigator will take. A forensic copy will be a 100% faithful replica of the original media and will include all data visible through the file system, as well as data hidden in unallocated space. As this duplicate is created, it is run through an algorithm that calculates a **hash value**, a type of

digital fingerprint that can be used to assure that the forensic copy remains accurate to the source.

A recent amendment to US Federal Rule of Evidence 902 establishes that preserved electronic data should be self-authenticating, which is exactly what creating a forensic copy achieves. The rule provides that properly certified electronic data will carry with it a strong presumption of authenticity. Because the forensic copy is verified to be identical to the original and it is protected against future alteration, it is generally considered to be a more reliable source of truth than the original media, which can be inadvertently altered.

EXAMINATION

Now that we have a forensic copy to work from, we can begin the examination. The goal of this stage is to extract relevant data from the digital haystack of information, preparing for in-depth analysis in the next stage. Using their skill, experience, and specialized tools, the forensic examiner will perform many different actions to gather the data they are looking for.

In this phase, you can expect your investigator to:

- recover deleted information
- parse containers such as mailboxes, computer backups, phone backups, and compressed archives
- retrieve artifacts such as web browser history and web searches
- identify the history of opened files and connected storage devices
- accurately identify file types
- cull unnecessary files such as duplicate and system/application files

Examiners also know that different operating systems and applications leave digital artifacts in a variety of hidden places. While a document may appear to be deleted to the ordinary user, examiners know to check specific directories or system files for duplicates and drafts that can be recovered. They understand that they can examine system resources such as restore points and registry files to find hidden data. For files that don't appear in the active file system, examiners can use a technique called "file carving" to search the unallocated sectors of a hard drive. By searching for specific key signatures, the forensics examiner can target specific file types for recovery.

DENISTING

If you hang around digital forensics long enough, you'll encounter the cryptic term **deNISTing**.

During a typical hard drive search, an investigator will uncover a broad assortment of files present on the computer. Many times, the pool of potentially discoverable material will include standard system or applications files, even though these files will have no relevance to an investigation. DeNISTing is a technique to efficiently remove these files.

NIST is the acronym for **National Institute of Standards and Technology**, a government agency that maintains a project called the **National Software Reference Library.** This library contains the hash values of thousands of traceable computer programs and operating systems. The process of deNISTing removes known application files from the pool of potentially discoverable data.

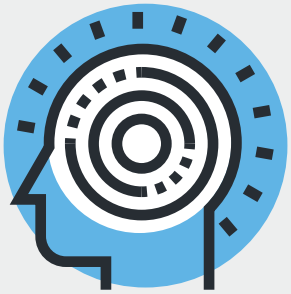
Learn more about deNISTing below.

CLICK TO VISIT ARTICLE

By this stage, the examiner will have a pretty good understanding of the type of data they are looking for, often driven by the professional profile of the computer's primary user. An engineer might store engineering files; a financial advisor may have accounting or banking files. With an encyclopedic understanding of specialized applications and file types, the digital forensics examiner will tailor their search to find the most relevant information.

Before the gathered data is analyzed, it is crucial to reduce the volume of information by intelligently culling files that have no relevance to the investigation. In the process of **deduping**, duplicate versions of files are removed from the collection. Another process that can be used to cull data is informally called **deNISTing**. (See sidebar.)

ANALYSIS



With our data set parsed and consolidated, we are ready to do a deep dive. During this phase, a digital forensics examiner performs an in-depth analysis of the evidence that has been gathered, attempting to interpret the data, draw insights, and ultimately tell a story.

The investigator will use powerful tools to find specific types of data using searches based on keywords, file types, and date ranges, while analyzing a file's content, metadata, datestamps, and more. The examiner will pull the gathered evidence together, correlating timelines, identifying the provenance of key evidence, and providing expert analysis using all available information.

Most people believe that the goal of a forensic investigation is to uncover an electronic "smoking gun," and sometimes that is the case. But more often it is the meticulous analysis of available information that builds a narrative around a discovered piece of evidence that helps win cases.

REPORTING

In the final phase of a digital forensics investigation, the digital forensics professional can prepare a report that documents all relevant findings of the investigation. The **expert report** will describe the activities undertaken during the investigation, providing a timeline that correlates evidence with user activities, supplemented with expert opinions and conclusions.

Once a report is submitted, investigators will often verbally walk a client through the findings. Reports can sometimes be misinterpreted when taken out of context, so it is important to have the investigator explain the results and be available to answer questions.

Sometimes a final report is not desired—once submitted, a report can become discoverable as evidence by the opposing party. Forensics professionals can forgo a formal report and discuss their findings with the client attorneys in order to guide their subsequent examination efforts.

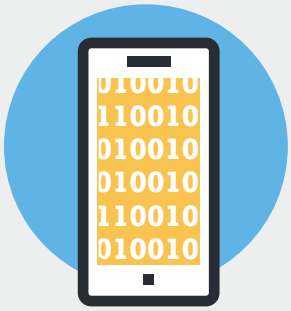
Depending on the needs of the case and the agreement between the parties, digital evidence can be provided in several different ways. In some cases, it is preferable to produce files in their native format. In other cases, it is not. For instance, let's suppose we have a batch of original email files in the .eml format. By themselves, they are not entirely human readable without proper parsing. However, they can be quickly turned into human-readable PDF files during the reporting process.

Should it be necessary, investigators are usually available to provide expert testimony in court. They can attest to their findings and demonstrate proper chain of custody for all evidence produced.

Six Hot Digital Forensics Trends

The field of digital forensics has changed immensely over the last decade. During this time, we've seen the rise of smartphones and tablets along with many other interconnected digital devices. Let's take a look at some of the most important trends that will shape digital forensics as we approach 2020 and beyond.

SMART PHONES



Former FBI director James Comey once stated, "The cell phone is probably the single most important piece of evidence you will find at a crime scene today." Even for those of us working on civil matters, smartphones can yield a wealth of information.

Smartphones have become our indispensable digital companions, traveling nearly everywhere with us. Increasingly, smartphones are the preferred platform that provides us access to email, social media, messaging, and the World Wide Web. Using geolocation information, smartphones can provide us with driving directions or track our exercise activity.

Because of this, smartphones are critical in most digital forensic investigations. There are now a host of powerful tools that allow forensic investigators to capture a wide range of information from modern mobile phones. Information and activities can often be correlated to specific time periods and geographic locations. Because smartphones often make automated backups to computers or cloud storage, data is often preserved longer than most users are aware.

EPHEMERAL APPS

Along with the rise of smartphones, we have seen the emergence of a category of mobiles apps that promise to deliver messages that are temporary in nature. Snapchat pioneered this market, buoyed by a user base of teenagers looking to protect their communications from the prying eyes of parents. Snapchat allows users to share information that is automat-

ically deleted just seconds after it is viewed, minimizing the chance that embarrassing digital content will come back to haunt the user.

Although Snapchat built its base by providing users with a sense of security and freedom, flaws in the system have emerged. Besides the obvious issues of users photographing incoming messages, it has come to light that deleted Snapchat content may be recoverable by using some fairly basic forensic techniques. (**Link:** Read more about recovering SnapChat data.)

Recently, a woman and boyfriend were charged with murder after they conspired to kill the woman's husband to claim life insurance money. What is notable about the case is that the couple plotted the crime over Snapchat which they believed would make it difficult for police to trace. As the case unfolds, it will be interesting to learn about the role that digital forensics plays. (**Link:** Keep up with the Data Narro blog to follow this case.)

INTERNET OF THINGS (IoT)

We are now living in an era of **IoT–the Internet of Things**. In essence, IoT refers to the ecosystem of digital devices that connect to the Internet. Devices that were previously built to perform simple mechanical tasks now have circuits, memory, and sensors that can detect our presence and record information about our lives. Doorbells, speakers, thermostats, watches, TVs, and even toothbrushes have all become "smart," routinely tracking our activities and recording information in the form of metrics, logs, or audio/visual files. In the past decade, the amount of discoverable information generated by the devices in our homes has exploded. Most of us are leaving an invisible trail of digital evidence all around us as we go about our lives.

There is a trade-off that we are making on a daily basis. By embracing modern technology, each of us is implicitly agreeing to give up anonymity in many of our regular activities. While most people believe there is little harm in the digital traces we leave behind, most people don't understand the extent that those digital traces are being captured.

Widely reported in 2018 was the news that a judge in New Hampshire ordered the release of recordings from an Amazon Echo device located in a home where two women were murdered. To those in the digital forensics and e-discovery fields, it's a reminder of just how intertwined our everyday lives have become with a vast assortment of Internet-enabled digital devices.

Our advice? Attorneys should take a more comprehensive view of potential evidence that could be found on current and emerging IoT devices. These devices can hold useful information about a user's location or actions that can be used to strengthen a legal case.

SSDs

As technology progresses, so do the components in a typical computer. Whereas traditional hard drives were the standard, in 2019 it is likely that a modern computer will come equipped with newer **solid-state drives (SSDs)**. Solid-state drives are silicon-chip based and nearly identical to the technology found in flash memory cards. SSDs offers the advantage of a reduced footprint, lightning-fast response times, and lower power consumption. From a forensics point of view, SSDs can be a bit more challenging.

Traditional hard drives rely on rotating magnetic platters in which bits of data are read and written by physically repositioning a read/write head. When a file is deleted, it is often left in place, with only the index pointer to the data being removed. That file will remain in place until it is overwritten when space is needed.

SSDs, on the other hand, require a clean slate to write files. Before new data can be written, write-ready blocks will be created by clearing the data from the needed space. If this data clearing happens soon after a file is marked deleted, this effectively prevents investigators from recovering data sitting in unallocated space. Let's use this analogy: writing to a hard drive is like painting—new data can simply be painted over the old, an SSD operates more like a chalkboard—old data must be erased before new data can be written.

ENCRYPTION

As computer software and hardware manufacturers take consumer privacy concerns seriously, they have started to offer painless ways to automatically encrypt the information that we store or transmit. Whereas encryption used to be a technique only employed by the tech-savvy, everyday consumers can now apply encryption easily. Let's look at a few ways that encryption can be used:

Full-Drive Encryption: Full-drive encryption (FDE) is precisely what it sounds like, a method of encoding an entire drive, effectively obscuring all of its data. It is a relatively simple matter to examine the contents of an unprotected hard drive. But if the drive is encoded with FDE, viewing any files without a decryption key is nearly impossible–the entire drive and its data structure will be completely obfuscated.

In the past, FDE required specialized software and a fair amount of patience. Nowadays, both Apple and Microsoft offer simple methods for consumers to employ FDE. Windows operating systems come with an easy-to-use utility called **BitLocker**; on a Mac, you'll use **FileVault**. Once a drive is encrypted, an investigator's ability to examine data from a drive without a password is severely hampered or, more likely, entirely prevented.

Encrypted Messaging Apps: More and more messaging apps have found a way to differentiate themselves by including end-to-end encryption into their communication offerings. We've seen that while some ephemeral apps have built flawed systems (SnapChat), others have made products fortified with nearly impenetrable security.

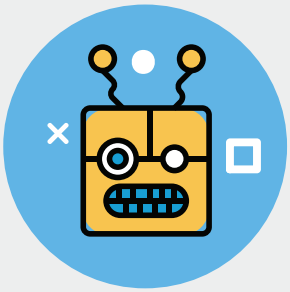
One such product is **Signal** which offers end-to-end encryption for text, video, and voice messaging. This means that even if messages are intercepted during transmission or storage, the captured data is unintelligible. Signal's parent company itself cannot decode the messages or turn them over to authorities, even if subpoenaed. Other secured messaging apps include **Silence**, **Cyphr**, and **Telegram**. Even Facebook's nearly-ubiquitous **Messenger** app has a "secret conversation" feature that offers end-to-end encryption.

File/Folder Encryption: There are many products on the market (**7-Zip**, **AxCrypt**) that allow you to encrypt individual files or folders. These products can prevent unauthorized users from seeing the contents of a protected file. Many times, you don't even need a separate encryption utility. Users of Word, Excel, or Acrobat have options to password-protect their files right from the application menu.

Even if information is encrypted, forensics examiners have techniques to help recover information. Let's suppose a user created, and then encrypted, an Excel spreadsheet. It is helpful to understand that Excel creates periodic backups of active documents in the event of an application crash. While these copies are automatically deleted, they could be recoverable from unallocated space using file carving techniques.

While it may be nearly impossible to crack the file encryption, it may be easier to focus energy on determining the password protecting the information. In civil litigation, gaining access to encrypted media may simply require negotiations between opposing parties.

TAR/AI/MACHINE LEARNING:



The latest hot topic in the world of digital forensics and e-discovery is **technology-assisted review** or **TAR**. While this technology fits better into the realm of e-discovery, it is well worth a mention here. TAR is a software-based approach that aids the document review phase of an e-discovery effort. TAR leverages the power of machine learning to identify and tag potentially responsive materials, significantly reducing the amount of time and effort spent in the most resource-intensive phase of e-discovery.

In earlier iterations of the technology, users were required to tag a set of "seed data" that TAR algorithms could use to analyze and learn from. Current versions of the technology allow users to simply begin tagging responsive documents while the software observes in the background. As new input is generated, the software uses active learning to continually refine the information that it tags as potentially responsive.

As the technology improves, TAR will become more and more efficient at finding relevant documents for review. We expect that this technology will substantially grow in popularity as litigation teams discover the cost-saving advantages of using TAR.

What steps should you take if you need to preserve digital evidence?

At some point in your legal career, it is likely that you will need to guide a client on what steps should be taken to conduct the initial actions in an electronic discovery effort. In this section, we'll cover seven of the major do's and don't to follow when you need to preserve digital evidence for civil litigation. Along the way, we'll include some of the best practices of e-discovery while avoiding some of the most common pitfalls.

Let's use a hypothetical situation to help illustrate our point—it's Monday morning, and you receive a call from your corporate client. They have strong suspicions that their former employee downloaded a cache of company documents shortly before they quit. The documents could be anything, including customer lists, pricing guides, or critical contracts. The company has the ex-employee's laptop in the sales manager's office, and they are thinking about searching his email. What do you tell your client?

#1: DO: ISOLATE THE COMPUTER

The absolute first thing you should advise your client to do is to isolate the machine in question. If it is already off, leave it off. The laptop should be stored in a secure location and steps should be taken to ensure that no one powers it on. If the machine is already on, we advise that you disconnect the computer from the network and leave it on until you can get instructions from a digital forensics examiner. Again, make sure that no one interacts with the machine.

Most people don't realize that the act of booting up or shutting down a computer can affect hundreds of files as the operating system engages in a set of housekeeping tasks when transitioning power states. Metadata can be updated, caches may be purged, and unallocated space can be overwritten.

#2: DON'T: ASK THE IT DEPARTMENT TO HELP

Just because your client has a competent IT department doesn't mean they should be engaged to look for evidence. Even the most well-meaning examination of the computer will alter the data on that hard drive. Opening, reviewing, or copying files can modify crucial underlying metadata that will affect the quality of the discoverable evidence. At this point, performing a search on the employee's computer is like trampling around in an active crime scene.

You need to protect the integrity of the computer data. Before you do any search, a forensic copy of the computer's hard drive must be created. That leads us to step #3.

#3 DO: CALL YOUR DIGITAL FORENSICS PROFESSIONAL

As early as possible, you need to engage a digital forensics expert. Your digital forensics professional will provide you with immediate guidance on the next steps in the process. They will let you know what you need to do with the digital device in question.

Forensic investigators have specialized hardware and software tools that allow them to capture a forensically-sound copy of digital media; the result is an exact bit-for-bit copy of the storage device that will include all visible data as well as all hidden data located in unallocated space.

The forensic copy is preserved along with a hash value, a type of digital signature that can be used to assure that the forensic copy remains 100% faithful to the source. Searches should be performed only on forensic copies of data.

#4 DO: IDENTIFY OTHER POTENTIAL SOURCES OF DATA

In today's world, it's not uncommon for employees to be issued additional digital devices and Internet accounts that should be preserved as well. Hardware might include USB drives, backup drives, phones, tablets, and other smart devices. Internet accounts might consist of cloud storage platforms like DropBox, email platforms, or collaboration software. Your digital forensics professional will have the knowledge and tools to extract information from cloud accounts better than you probably realize.

Additionally, you should catalog any recently retired digital devices. Employees periodically replace laptops and phones — you need to identify these items and determine what data may still be on these devices if they are still available.

#5 DON'T: ABDICATE YOUR RESPONSIBILITY FOR PROVIDING LEGAL GUIDANCE

Attorneys still need to make sure they use proper ethical and legal judgment to guide discovery efforts.

Electronic discovery can bring a Pandora's box of issues. What do you do when you find personal files on the company-issued computer? What if you find the employee has personal accounts loaded on the laptop with login credentials intact? Having inadvertent access to an ex-employee's personal Gmail account, even if loaded on company equipment, doesn't mean that you can review their past or present email activity on that platform.

You will need to exercise caution and decide about what files are fair game for electronic discovery. I would point you to an excellent article from the American Bar Association that will help you understand your ethical and legal obligations during a digital forensics investigation (**Link:** Forensic Examination of Digital Devices in Civil Litigation: The Legal, Ethical and Technical Traps.)

#6 DO: CONTAIN THE SCOPE AND COST

It is essential to make sure that you accurately define the intended scope of the investigation with your chosen digital forensics professional before any forensics work is performed.

You may wish to limit the examination to a cursory search of company emails. Alternatively, you may want to engage in a thorough digital archeology expedition, attempting to unearth deleted files or recover information from hidden data caches. Your digital forensics professional needs to understand your expectations and budget.

You should have a clearly defined statement of work or engagement letter that spells out what actions should be performed and make sure you have a common understanding of the costs of those services. While the scope of work may change based on initial findings (it often does), it is crucial that your digital forensics professional knows what you expect of them.

#7 DO: ENFORCE A CHAIN OF CUSTODY

While all qualified forensics professionals will do this already, it is your responsibility to make sure a proper chain of custody for evidence is maintained. Whenever Data Narro engages in a digital investigation, we take the necessary steps to ensure that our evidence is forensically sound and suitable for admission in a court of law. That means our tools and procedures are forensically-validated. We maintain a proper chain of custody for all the digital equipment we examine—complete with photographs, detailed logs, and physical security. However, it is up to the attorney that guides the discovery process to make sure all parties are complying with rules of evidence.

CONCLUSION

This e-book was intended as a quick primer to help you get started thinking about digital forensics and e-discovery. Please feel free to contact Data Narro if you have any questions concerning digital forensics, e-discovery, or data recovery! We are helpful, friendly, and always willing to help steer legal professionals in the right direction.

STAY UP-TO-DATE: VISIT OUR BLOG TODAY!

Data Narro, LLC is a Wisconsin-based digital forensics and e-discovery consulting firm. DataNarro helps businesses, law firms, and government agencies preserve and recover electronically stored information for investigation, data analysis, and litigation support. We serve our Midwest clients from our headquarters in downtown Milwaukee.

Data Narro, LLC
740 N Plankinton Ave, Suite 730
Milwaukee, WI 53203
www.datanarro.com
info@datanarro.com
(262) 393-1710

About Data Narro
Data Narro, LLC is a Wisconsin-based digital forensics and e-discovery consulting firm. DataNarro helps businesses, law firms, and government agencies preserve and recover electronically stored information for investigation, data analysis, and litigation support. We serve our Midwest clients from our headquarters in downtown Milwaukee.