Interplay of Digital Forensics in eDiscovery

Sundar Krishnan *skrishnan@shsu.edu*
Department of Computer Science
Sam Houston State University
Huntsville, TX, USA

Narasimha Shashidhar *karpoor@shsu.edu*
Department of Computer Science
Sam Houston State University
Huntsville, TX, USA

Abstract

Digital forensics is often confused with eDiscovery (electronic discovery). However, both the fields are highly independent of the other but slightly overlap to assist each other in a symbiotic relationship. With decreasing costs of cloud storage, growing Internet speeds, and growing capacity of portable storage media, their chances of being used in a crime have grown. Sifting through large volumes of evidential data during eDiscovery or forensically investigating them requires teams from both these fields to work together on a case. In this paper, the authors discuss the relationship between these disciplines and highlight the digital forensic skills required, sub-disciplines of digital forensics, the possible electronic artifacts that can be encountered in a case, and the forensic opportunities relative to the eDiscovery industry. Lastly, the authors touch upon the best practices in digital evidence management during the eDiscovery process.

Keywords: Digital Forensics, eDiscovery, Electronically Stored Information (ESI), Security, Evidence Management.

1. INTRODUCTION

When a civil lawsuit is filed, both the parties in the lawsuit engage in a pre-trial process known as “discovery”. During this process, each party may request documents and other evidence from the other or compel the other to produce such evidence using subpoenas or other legal instruments.

When such documents or evidence are in an electronic/digital format, this process is known as eDiscovery. Any potentially relevant digital evidence deemed necessary by either party may be subject to the eDiscovery process. This corpus of electronic/digital documents or other evidence is known as Electronically Stored Information (ESI). When civil litigation is reasonably anticipated by an organization or individual, they are expected to preserve prospective ESI from destruction. If/When litigation commences, eDiscovery follows wherein each party may be required to declare their ESI relevant to the case. Suppose the other party to the litigation requests this ESI for their own case preparation, the other party may produce this ESI in its original format if it seems related to the case, not privileged, within reasonable costs, and is reasonably accessible. Such ESI may not always be readily available and may need skilled professionals to forensically extract it from electronic devices. Thus, digital forensic professionals may participate alongside Discovery teams from both parties in forensically producing ESI during litigation. Parties to the case may engage digital forensic professionals on both sides if needed to assist in forensically producing ESI and also in validating the other’s ESI production methods.

Initially, the field of digital forensics was limited to personal computer disks. However, over the last few decades as computers have become connected through networks (local and the Internet) coupled with the growth of the cloud and smart devices such as smartphones, Internet Of Things

(IoT), smart medical devices, smart energy grids, smart wearables, etc., personal computer forensics has now grown into digital forensics to encompass the investigation and analysis of these smart devices. The field of digital forensics has also expanded to include network forensics as well, which focuses on investigating networks for security breaches, hacking attempts, and data theft. In the last few decades, federal/state criminal investigators, global corporations, law firms, and private/public enterprises have relied on digital forensic investigators to investigate issues involving criminal activities, intellectual property theft, patent infringement, data theft, misconduct, and embezzlement. A digital forensic professional is someone who has a desire to follow the evidence, thereby assisting the lead investigators by identifying and analyzing digital clues from a pile of digital evidence. Digital forensic experts require a specialized skills to investigate various platforms such as the Internet, computers, smartphones, cloud, IoT, medical devices, accounting data, etc. To become a part of a digital forensic team, a digital forensic professional needs to coordinate with different teams in the investigation. Other teams in an investigation may be from law enforcement when in criminal cases and eDiscovery teams when in non-criminal (civil) litigation. Digital forensic professionals can be called to provide their expert testimony in litigations and thus will need to be an expert in his/her skills. A forensic protocol is the agreed-upon set of investigation steps that a forensic team will follow to acquire, segregate, analyze, and present the information from the digital evidence relevant to the specific legal case. During the eDiscovery process, digital forensics activity is usually visible in the initial stages of the EDRM lifecycle. The volume of digital artifacts for a legal case can be enormous and sometimes in terabytes depending on the size of the case and the depth of investigation. Not all the digital artifacts from a pile of potential evidence (ESI) is in plain sight. Thus, forensic teams assist the eDiscovery, para-legal, and legal teams in uncovering the case digital artifacts of interest. This volume of forensically extracted/acquired digital data is then further weeded to align with the investigation. Figure 1 outlines the typical growth of forensically extracted/acquired digital artifacts (evidence) for a legal case. The “collection and preservation” stage of the EDRM process would typically see the most growth of digital artifacts from digital forensic activity. Each legal case has its own digital forensic effort requirement, and thus costs of employing this skilled team can hugely vary. The eDiscovery industry can be complicated with technical and logistical challenges routinely found in large eDiscovery projects that can test even the most experienced digital forensic examiner [1].

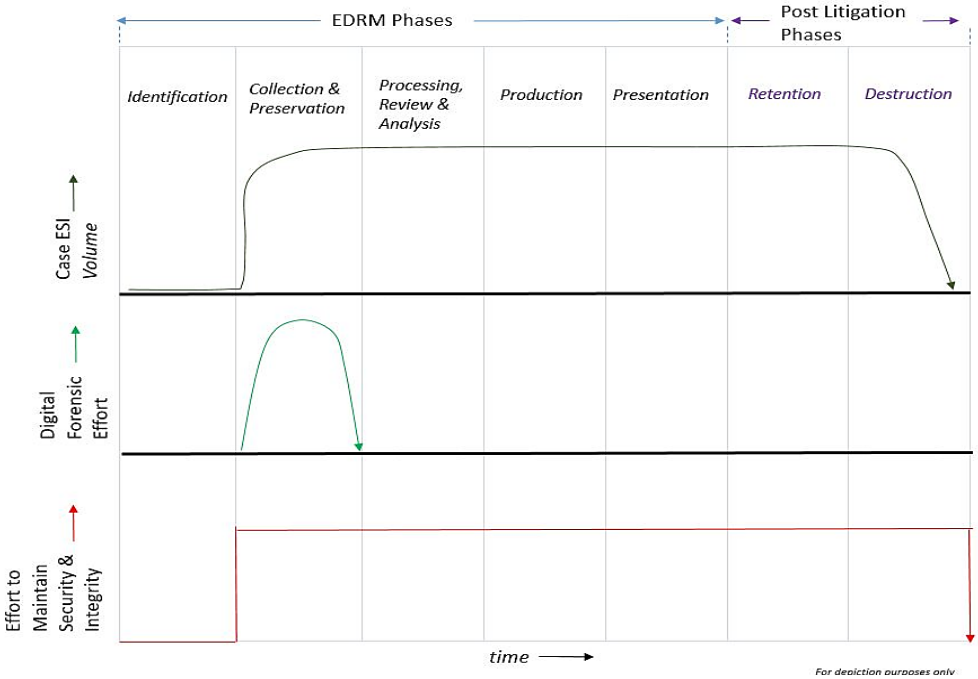

FIGURE 1: Typical growth in volume of digital forensic evidence (electronic stored information) in a legal case setting.

Unlike digital forensics, eDiscovery is not used to acquire, analyze, or investigate data forensically. However, eDiscovery serves to gather and organize information that everyone can view, access and duplicate. This information may be forensically acquired or extracted from data sources within the scope of the investigation. During litigation, eDiscovery teams (or firms) can be subpoenaed to provide testimony on the methods they used when collecting data off electronic data sources [2]. During reviewing and analysis of data, digital forensic teams assist eDiscovery teams and may work alongside an organization's in-house Information Technology team if applicable to the legal case. The work-products of both the teams are electronic data of interest to the legal case. However, both teams refrain from providing legal advice or interpretations of this electronic data unless specifically asked for by the legal counsel.

Typically, digital forensic teams are sub-groups within the eDiscovery team assigned to a legal case. Using digital forensic skills, they can acquire digital data from electronic data sources while maintaining security and integrity. Once electronic data of interest is forensically acquired, it is then forwarded to the eDiscovery team, who then go about with their tasks of sorting, arranging and presenting the data to the legal counsel. This allows the legal counsel to perform their own thorough reviews with this data to arrive at their interpretations and arguments. The legal counsel may always collaborate with the eDiscovery teams and the digital forensic professionals for clarifications on the data. In an example of a family law case that hinges on a question of infidelity, the digital forensics team may be required to produce a transcript or log of communications between the two parties. A typical 40 year old adult sends and receives over 1,500 text messages every month, so extracting these texts and presenting them (transcripts) with appropriate forensic-level feedback can be lengthy and time-consuming [3], [4]. With a tleast 97% of smartphone owners' texting regularly [5], both parties (with access to smartphone devices) may have much more data for this legal case from the use of other texting applications and from the activity on dating sites. The eDiscovery team, attorneys and other paralegals must then review all these transcripts to draw any relevant conclusions about intent or relationships. In this article, the authors take a deductive approach to explain the interplay of digital forensics within eDiscovery and touch upon typical expectations of a digital forensic professional when working with eDiscovery teams on a legal case.

2. RELATED WORK

As we continue to embrace technology in our daily life and work, it is highly likely that digital forensic experts and their forensic reports will become increasingly important to litigation. Legal case evidence in the form of digital artifacts in the modern age sometimes necessitates digital forensics as such evidence is not readily accessible for use in legal arguments. Holley et al. [1] state that during the eDiscovery process of a legal case, digital forensic examiners play crucial roles as technical advisors, hands-on collectors, and analysts. Attoe [6] compares the workflows of eDiscovery (EDRM) and digital forensics and concludes that they share common workflow similarities. He also concludes that eDiscovery is more focused on text examinations with minimal attention to graphic images, while digital forensics is dictated by type of investigation. Digital forensics is a subset of the eDiscovery process in civil litigations. In criminal cases, a report from a digital forensic expert is often prepared at the end of a forensic investigation. Garrie et al. [7] provide a report evaluation framework that would need to be adjusted by following the underlying facts of the dispute. However, in civil cases, during eDiscovery, forensic experts also provide raw evidence unearthed from digital sources so that it can be stored along with the case ESI for analysis and subsequent interpretation. All forms of ESI such as text, graphic images, browser activity, and chat messages are typical sources of evidence and maybe subject to eDiscovery. While defining a "typical" case-load (matter) ESI as a strenuous exercise in a world of Big Data, eDiscovery effort can deal with tons of data per legal case [8]. As organizations address concerns in responding to eDiscovery requests, Ward et al. [9] propose recommendations for the design and development of an electronic records management (EDRM) policy. In this paper, we elaborate on the role of digital forensic examiners and the types of evidence that they may encounter as part of the eDiscovery process. This paper also describes common areas for

attention and suggests best practices for both new and experienced digital forensic examiners as they safely navigate the tricky minefield of eDiscovery.

3. DIGITAL EVIDENCE

Litigation these days often involves digital evidence or Electronically Stored Information (ESI) [10]. Digital evidence or electronic evidence is any digital information stored or transmitted in a digital form that may be used by a party in a court case. Since the last two decades, the legal world, digital forensic professionals, and eDiscovery service providers have all become comfortable working with traditional types of digital evidence (e.g., email, text messages, spreadsheets, word processing files). However, technology evolves rapidly, and so does the complexity in legal cases, especially due to the increasing growth in the use of technology across the globe. Not all digital evidence can easily offer digital data of interest for the case. Thus, digital forensics plays a key role in sound extraction of digital data and its subsequent analysis. This section discusses evidence sources, identification, forensic extraction, types of forensic artifacts encountered and the specialization required in the various sub-disciplines of digital forensics.

3.1 Rules of Evidence

The Federal Rules of Evidence (FRE) [11], as well as the Federal Rules of Civil Procedure (FRCP) [12], were codified to guide legal parties and courts on the admission of evidence. While the FRCP and FRE were developed to outline the procedure in federal courts, many state courts have adopted similar rules. In addition, case law and opinions issued by courts have also guided parties in determining the admissibility of evidence [13]. However, there are five basic rules of evidence [14], [15] that are generally accepted and can be applied to digital evidence, namely;

a) Admissible – This is the most basic rule of evidence validity and importance. Certain legal and technical requirements (such as search and seizures, warrants, etc.) must be met to ensure the admissibility of digital evidence in a court of law. Evidence must be preserved and gathered in such a way that it is relevant to the case and can be admissible in court.
b) Authentic – Evidence relates to an incident in a relevant way. A digital forensic subject matter expert should be able to explain to the court on the origin of the evidence.
c) Complete (no tunnel vision) – Evidence must be related to the incident in a relevant way, else, it cannot be used to prove anything. Evidence should reflect the whole story and not be incomplete.
d) Collection of evidence should be limited to one perspective of the incident. Not only should we collect evidence that can prove a suspect's malicious actions, but also evidence that could prove their innocence (Exculpatory evidence).
e) Reliable – Evidence collected should be reliable. Evidence collection, analysis, and handling procedures must not cast doubt on its authenticity and veracity.
f) Believable – Evidence should be clear, easy to understand, and believable by a jury. A digital forensic subject matter expert must be able to explain to the court with clarity and conciseness on the processes used to examine evidence and the steps followed to preserve its integrity.

From a digital forensics view, certain legal and technical requirements must be met to ensure the admissibility of digital evidence. For the satisfaction of the legal requirement, courts examine the legal authorization to conduct searches and seizures of digital data (evidence), its relevance, authenticity, integrity, and reliability. With respect to technical requirements, courts critically examine the digital forensic procedures and tools used to extract, preserve, and analyze digital evidence. The accreditation of digital forensic laboratories, the qualifications of the digital forensic experts working on the case along with their submitted reports are also taken into account by the courts. Antwi-Boasiako et al. [16] propose an assessment framework that encapsulates the essential technical and legal requirements to determine evidence admissibility. The digital forensic relevance of the digital evidence is assessed by whether the digital evidence links or rules out a connection between the suspect, the target, and the crime scene during the case window (timeline). The forensic relevance assessment should also consider supporting or refuting

the testimony of the suspect, witness or victim. Similarly, forensic relevance of evidence should also provide investigated leads undertaken on the suspect's method of operation, and show that a crime has indeed taken place (corpus delicti) [17].

3.2 Forensic Data Sources

Virtually every form of electronic data (ESI) can be subject to eDiscovery. Few common data sources for forensics during eDiscovery are listed below.

a) Cloud-based Applications
b) Cloud Storage
c) Active Storage, Offline Storage (Archives and Backups)
d) Digital Devices Smartphones & Tablets PCs/Laptops
e) CCTVs Navigation and Global positioning systems (GPS)
f) Internet of Things (IoT Devices)
g) Networks
h) Medical devices
i) DarkWeb
j) Industrial Machinery
k) Automobiles

Digital forensic professionals may perform on-site investigations to identify, collect and preserve data if the data source is not mobile or cannot be detached as a stand-alone device for off-site investigations. While it is one thing to identify and preserve various forms of electronic data, it's often quite another to go out and collect it all. Different data sources have different levels of accessibility, design-constraints, and present other collection challenges [18]. In eDiscovery, we call this phase as "collection", which may involve forensic imaging and logical acquisition by forensic professionals. In some instances, third-party digital forensic professionals may be required to establish an external/remote connection for forensic work. Sometimes, specific data may be readily available and may not need any forensic skills for extraction. In such cases, employees in the Information Technology department of the organization may assist with its collection and would forward the same to the eDiscovery team. As the collection of data completes, preservation starts until the data destruction stage post completion of litigation.

3.3 Digital Forensics Sub-Disciplines in eDiscovery

Digital forensics is a maturing scientific field with many sub-disciplines involved in the eDiscovery industry. Digital Forensic Research Workshop (DFRWS) defines digital forensics as;

"The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering their construction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations." [19]

Since digital evidence may be stored, processed, and transmitted over various digital devices, safely acquiring data off these devices and systems to be admissible in a legal setting (court) needs refined skills and experience. During eDiscovery, forensic professionals assist eDiscovery teams, paralegals and legal professionals in acquiring and extracting electronic information. Each digital forensic sub-discipline needs technical and procedural skills pertaining to that field in addition to the knowledge of common digital forensic processes, namely; preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation. Thus, irrespective of the sub-discipline involved, forensic professionals assisting eDiscovery teams must be adequately trained and vetted before working on the evidence of a legal case. Few other skills of digital forensic professionals' are investigative, computing, and presentation skills (expert witness). Below are a few sub-disciplines of digital forensics that may depend on the legal case and eDiscovery needs.

a) Disk & Storage Devices Forensics – involves traditional digital forensics that is well documented involving disk acquisition, extraction, etc. Storage devices may include SD Cards, USB drives, portable storage media, etc. An understanding of file-system design, operating system(s) involved, and architecture is a must.

b) Network Forensics – involves conducting forensics on the digital networks that link various devices – both within an organization's private networks and over the Internet. A field that is well documented and practiced. Often overlaps with network security and administration and requires an in-depth knowledge of network protocols, security, and network infrastructure. Another focus area of network forensics is on the various network devices (routers, switches, firewalls, etc.) that enable networks to function.

c) Cyber & Cloud Forensics – involves forensics of the Internet and cloud with a deep understanding of cloud architecture and storage, networks, network communication protocols, etc. This sub-discipline considerably overlaps with cyber security and incident investigations. Possible limitations in this area of digital forensics are the inherent geographical laws that come into play due to the cloud design and location of cloud services/servers. Another potential hurdle to grapple are the legal contracts and Service Level Agreements (SLAs) between cloud service providers and users.

d) Mobile Device Forensics – involves forensics on mobile devices, smartphones and tablets. The focus is on the data stored on these devices that can also be encrypted. Since these devices are "mobile", additional focus lies on user/owner privacy and overcoming access controls.

e) IoT Forensics – involves forensics on Internet-of-Thing (IoT) devices like connected devices, smart home devices (smart – speakers, doorbells, doors, lights, thermostats, home security, cameras, and other home appliances), building automation etc. Relatively a new field of digital forensics that involves several new technologies and poses privacy challenges.

f) Accounting Forensics – involves digital forensics in financial and accounting practices related to fraud, money laundering, etc. Although considered a branch of forensics, it may also reside as a sub-discipline of digital forensics, as, much of finance and accounting these days is undertaken via software applications, computing devices, and mobile devices such as smartphones. This field would need skills related to computer forensics, smartphone forensics, accounting forensics and accounting knowledge.

g) Crypto currency Forensics – involves forensics of crypto currencies with an in-depth understanding of crypto currency technology such as blockchains, crypto currency transactions, crypto currency exchanges, etc. An upcoming area of digital forensics that also involves network and mobile forensics.

h) Medical Device Forensics – involves forensics of medical devices (such as infusion pumps, digital pacemakers) in the healthcare industry (both networked and stand-alone devices). This field requires an in-depth understanding of the workings of medical devices, their associated software applications, network protocols used by them, etc. An upcoming area of digital forensics that would need to focus on the many vendor-specific devices and their delicate interplay with human life.

i) Wearable Forensics – involves digital forensics on devices that are smart (over the network, wireless and Internet-enabled) and worn on the body. Smart wearable devices are found in fashion, textiles, jewelry, virtual reality headsets, gaming gloves, footwear, fitness trackers, implantables, etc. and are increasingly favored both in personal life and at workplaces. This sub-discipline of digital forensics is relatively new while posing technology and privacy challenges.

j) Dark-Web Forensics – involves digital forensic investigations of the Dark-Web. Such investigations often pertain to criminal cases. This sub-discipline is of digital forensics is relatively new while requiring extensive Internet and network skills. Since it largely deals with the cloud, geographical limitations in investigations may apply.

k) Social Media Forensics – involves digital forensic investigations of Social Media on the Internet. Websites for social interactions, chat rooms, few professional networking websites, smartphone applications, and web-enabled applications largely constitute the surface area of the sources. This sub-discipline of digital forensics can encounter large unstructured data volumes that may need forensic extraction of data over the Internet, browsers, and computer disks and from mobile platforms such as smartphones. Social media forensics caters to both criminal and civil litigations.

l) Industrial Systems Forensics – involves digital forensic investigations of Industrial systems and controls such as smart-grid components, SCADA systems, and Programming Logic Controllers (PLC). This sub-discipline of digital forensics is relatively new, although these systems have existed for ages. Often forensics in this field would cater to espionage and cyber-attacks, leading to criminal investigations.

3.4 Digital Forensic Artifacts

During a criminal investigation, forensic professionals from a federal or state lab usually perform forensic analysis of these artifacts. However, in civil litigation, digital forensics professionals participate in the investigation either from law firms or from outsourced private companies. Digital forensic investigation effort usually is part of the eDiscovery process before the case is argued in the courts. In this section, few common artifacts (evidence) of interest to forensic investigators are discussed. These artifacts are of common interest in any type of investigation, but the following discussion focus is on civil litigations.

3.4.1 Acquisition and Collection of Forensic Artifacts

During eDiscovery, digital forensic professionals work under the guidance of the eDiscovery team, scope of discovery, legal scope, and attorneys. Digital devices, media, and raw digital data are few sources from a case ESI that can be considered for forensic evidence extraction. A forensic protocol following established forensic standards and procedures should be established and approved before undertaking the forensic acquisition of the device. Forensic methods used to acquire and collect from a device may be intrusive (physical extraction), logical or manual. Any intrusive forensics may result in alteration of the physical attributes of the digital device and may thus destroy the evidence. Thus, all forensic tools used must be legally acceptable, updated for the latest versions, calibrated, tested, and vendor supported. Forensic procedures used must be pre-approved, rehearsed, and any deviations must be documented. Artifacts collected from these procedures are then shared with the eDiscovery teams and attorneys.

3.4.2 Metadata

The “meta” in metadata means “beyond” and is used to indicate the presence of “data beyond the data”. In the world of digital forensics, metadata is the structured data found embedded within electronic files. Metadata is often automatically created and updated by the application handling the file, or Malware, or the operating system, unless manually updated by a human. Every electronic file has metadata associated with it and can be useful depending on the type of file and the type of investigation.

Larry et al. [20] describe common sources of metadata are from the file system, documents, pictures and from the Internet, such as web page metadata and browser metadata. Document metadata is stored inside a document that provides many details such as authorship, file hashes, last accessed timestamp, last modified timestamp, the time taken to edit, and even the computer on which the document was created. Document metadata details can vary between documents created by office suite products such as Microsoft Office, WordPerfect Office, etc. Program code that can also be considered as a document, too, has metadata within it. A picture file can contain

the pixel data, created timestamp, camera details, lens details, geographical coordinates, etc. An audio/video file may contain Artist, Album, Track title, Genre, Video bitrate, etc. When a file can be edited/processed by multiple applications, only commonly accessed metadata fields of the file are updated by these applications. Metadata is usually not visible at first sight when someone opens the file via an application software [21]. Unless this metadata was not tampered with by suspects in a legal case, metadata can be valuable for forensic investigators as they provide a hidden layer of data that the common user would not notice.

In webpages of a website, metadata can be found within the "source code" of the web page and is in the form of meta-tags, title-tags, page titles, page headers, and meta-descriptions [20]. Metadata is the data (keywords) that describe the contents of the webpage. Figure 3 highlights a few such meta-tags that constitute the metadata of the webpage. Metadata is used in page content and HTML tags for two reasons [22], namely; 1) To help readers scan the page to decide if they want to read it. 2) To help search engines find the page. Figure 2 describes the categorization of metadata in webpages. Most browsers allow any user to view the metadata by viewing the source code of the webpage (via browser menu options). While this metadata can be helpful to search engines for content categorization and webpage ranking, forensic investigators can ascertain few other clues, such as the programming language used, page rendering intent, targeted search engines, static content or dynamic generation, etc. This also highlights the limitation that webpage metadata is of limited value in a forensic examination. On the other hand, Internet browsers that render websites and webpages are of interest to forensic investigators as browser metadata can be used extensively as forensic evidence in all kinds of cases. Examples of browser metadata is the history, stored passwords and other browser settings. File System Metadata usually resides in the internal files of a filesystem. For example, in the NTFS file system, the $MFT, $Secure) files contain metadata. In Windows® XP Operating System, File Explorer allowed us to edit the metadata (author name, comments, and keywords) of any file type or folder. However, in Windows® Vista and later Windows® versions, this has been possible only for certain types of files, such as MS Office® documents, JPEG images, and MP3 audio files [21]. File system metadata such as file permissions (read/write), file status (active versus deleted), and information about whether a file is resident or nonresident can be useful in the right forensic context. However, one aspect of file system metadata that often draws the most attention to forensic investigators is the date and timestamp (locale) information [23]. Forensic examiners must also be aware of special circumstances affecting datetime stamps and help place these dates and times within the investigation context to plot a timeline.

Placement	Used By
META tags	Search engines
TITLE tags	Search engines
Headings	• Readers • Search engines
Content	• Readers • Search engines

FIGURE 2: Webpage Metadata [22].

```
<!DOCTYPE html>
<html lang="mul" class="no-js">
<head>
<meta charset="utf-8">
<title>Wikipedia</title>
<meta name="description" content="Wikipedia is a free online encyclopedia, created and edited by volunteers around the world and hosted by the Wikimedia Foundation.">
<script>
document.documentElement.className = document.documentElement.className.replace( /(^|\s)no-js(\s|$)/, "$1js-enabled$2" );
</script>
<meta name="viewport" content="initial-scale=1,user-scalable=yes">
<link rel="apple-touch-icon" href="/static/apple-touch/wikipedia.png">
<link rel="shortcut icon" href="/static/favicon/wikipedia.ico">
<link rel="license" href="//creativecommons.org/licenses/by-sa/3.0/">
<style>
.sprite{background-image:url(portal/wikipedia.org/assets/img/sprite-46c49284.png);background-image:linear-gradient(transparent,transparent),url(portal/wikipedia.org/as
</style>
<style>
html{font-family:sans-serif;-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%;font-size:62.5%}body{margin:0}article,aside,details,figcaption,figure,footer,header
</style>
<link rel="preload" as="image" href="portal/wikipedia.org/assets/img/sprite-46c49284.svg">
<link rel="preconnect" href="//upload.wikimedia.org">
</head>
```

FIGURE 3: Meta Tags in Wikipedia homepage [view-source: https://www.wikipedia.org/].

In the eDiscovery process, metadata is crucial to plot the timelines of digital artifacts to determine their inclusion/exclusion to the legal case. Other attributes of metadata can help ascertain the subjects/actors who accessed them, their state (available/archived/deleted), applications that last processed the files, devices that created them, etc. In short, metadata can provide a wealth of information to the legal team and should not be overlooked. Metadata should be extracted, processed, analyzed, and preserved by skilled forensic experts as nonprofessional interpretations may incorrectly elucidate this data relative to the investigation/legal-case. Care should be taken not to casually open digital artifacts (evidence) once collected as any such actions can instead update metadata of these digital artifacts, thus, altering evidence state and integrity.

3.4.3 Timestamp Data

Often, timeline data from digital artifacts (evidence) of the legal case will need to align to the case timelines. In an example of a family law case that hinges on a question of infidelity, digital data immediately prior to the window of alleged infidelity of either party will be of most interest and not of digital data from childhood or youth days. In short, digital forensic investigators would not want to uncover SMS texts from an entirely different time/date than what the legal case or investigation is dealing with (follow forensic protocol for the case). Timeline analysis is an important component for visualizing information (actions/events) obtained from digital artifacts. Figure 4 describes a visual plot of events on a timeline graph [24]. Using multiple clues from the evidence pile (ESI), a behavioral profile of the suspect can be created based on the timeframes of when the suspect is definitely at home and not at home, browser activity, through cameras, cell tower information, or witnesses. Luckily for us, all digital data is time-stamped (user or system created) and missing timestamps can be considered as red herrings (suspicious). All file systems, irrespective of the device, offer a vast amount of time-stamped data making timeline analysis a powerful and viable technique for forensic analysts. Following the defined forensic protocol, care should be taken to align timestamps to an agreed-upon time zone often in accordance with the legal case. Timeline visualizations can easily get complicated when rendering on a graphical tool, so care should be taken to render based on key digital artifacts that solidify the case arguments.

FIGURE 4: A sample timeline analysis of events [24].

3.4.4 Geo-location Data

Crime happens all over the world, and applying geographical coordinates to suspects has been key to many investigations for centuries. In the past, before Global Positioning System (GPS) data was available on a person or a device, eyewitnesses pinned suspects to streets, a castle, or a field. Alternatively, crime was described to have taken place at a generalized geographical location – say besides a riverbank. Since the last few decades, with the availability of navigation devices and having GPS on our smartphones, cars, drones, and IoTs, forensically retrieving geographical data from these devices can plant the suspect at that location, given the fact that the suspect was carrying the device all along. Geo-location forensics (forensic Geoscience) refers to the application of geography or earth science to forensic investigations [25]. Navigation data (GPS based) is critical in other logistic-related legal cases involving movable assets like ships, cars, planes, etc. Technologies like WiFi network positioning, Bluetooth, and cell tower triangulation can also augment geo-location data. Often, we can see one's location-specific advertisements when browsing websites due to HTML5 support and the use of various Internet-based geo-location services like Google Latitude [26], [27], [28]. Many GPS spoofing Apps on smartphones are freely available and a Global Navigation Satellite System (GNSS) jamming equipment can cost about $300 [29]. Thus, digital forensic investigators should be aware of location spoofing Apps on smartphones that spoofing GPS data [29]. Also, GPS inaccuracy in urban locales can interfere with the accuracy of location data.

In an example of a family law case that hinges on a question of infidelity, determining the location of the suspects via their mobile devices, tablets, IoT devices, cars, or IP address can help place/map the suspect at a geographical location. The suspect may have been walking by a street, in a restaurant or staying at a resort. This data, along with other investigation data, can prove or disprove the suspect's digital geographical footprint. Aligning geo-location data to activity timelines (say their location on Valentine's Day) can help visualize suspects' movements. Extracting this digital data from digital devices during eDiscovery is critical for legal case analysis and argument preparation.

3.4.5 Digital Media Data

Often media (audio, video, images, and photos) data constitute crucial elements of evidence in a legal case. The volume of media data has greatly increased due to availability of cheap smartphones, audio-video devices and the growing capacity of on-board storage on such devices. Growth in media technology (hardware and software) has vastly improved their quality and resolution. Coupled with easy accessibility to telecommunication technology for Internet availability and low-cost cloud storage options have led to a recent spurt in volumes of media

created by humans. Also, their editing and management has become simple, with plenty of freely available software tools on the Internet. This growth in the volume of audio, video, images/photos data makes digital forensics a key aspect during eDiscovery. Increasingly audio, video, and images/photos data is created on mobile devices, and extracting such data would need mobile device forensic skills. As there is a possibility for such data to be stored in the cloud, digital forensic skills may need to include cloud forensics and network forensics. Since this data can be shared and downloaded into computers and other storage devices, additional digital forensic skills may be needed, such as computer (disk) forensics and storage device (USB/SD Card) forensics. Digital forensic analysis of mobile devices comes with their own challenges [30], and overcoming them would need skills, tools, and time. For a legal case, the eDiscovery team would work closely with digital forensic professionals to identify evidence of interest and their sources.

Wikipedia defines audio forensics as the field of forensic science that relates to the acquisition, analysis, and evaluation of sound recordings that may be presented as admissible evidence in a court of law [31]. Audio evidence can occur in the form of music, human voice, voices of animals, machinery, etc. Digital forensic analysis of audio files falls under audio engineering and needs highly skilled audio specialists working in a forensic audio laboratory. Common audio evidence can be either in analog or digital format like sensitive law-enforcement recordings, 911 emergency calls, audio from smartphones, DVD, video, CCTV, voice from videos on social media, audio files on computer disk storage or memory card, etc. On one of the Watergate recordings seized, specialists identified an 18.5-minute section of noise that brought together some of the world's leading audio experts for its analysis [32], [33]. Many significant forensic audio investigation lessons were learned from Watergate and some of the techniques and types of equipment applied are still utilized today. Speech enhancement algorithms can vastly improve the quality of speech in an audio file, however for reliable audio/speech authentication, a better noise estimation method is desirable [34]. Few goals of audio forensics are establishing the authenticity of audio evidence, performing enhancement of audio recordings to improve speech intelligibility and the audibility of low-level sounds (like background noise), interpreting and documenting sonic evidence such as identifying talkers, transcribing dialog, acoustic environment in which the audio recording was made, identifying traces of coding or transcoding, establishing phonetics, voice biometrics and reconstructing crime or accident scenes and timelines [35]. Other cases for audio forensics is around aircraft, submarines, ships and weapon audio signatures, but this would be mostly fall under the military domain.

From doorsteps to driveways, convenience stores to fast-food restaurants, malls to banks, traffic intersections to parks, CCTV systems are virtually everywhere. With the propagation of cell phones and smartphones coupled with cameras on bikes, cars, trains, buses, etc., video cameras are everywhere, resulting in massive video recordings that may be shared and stored for long in the cloud. We are living in a world surrounded by cameras that record most of our moves. Most of the videos for these cameras are in digital formats. Analog video systems are rapidly becoming a recording technology of the past; however, many are still in use today employing magnetic tapes for storage. If a system uses analog tape, the digital forensic investigator should bear in mind that every playback of the tape will degrade the recorded images [36]. Careful write protection measures must be taken to prevent it from being accidentally recorded over. The digital forensic investigator should note the make and model of the recording device, storage limitations/conditions, storage options on device (on-board/cloud), and other important details about the recording system (e.g., how many cameras are connected and recording, whether it is recording in time-lapse mode, the current time/date, and the time/date on the recorder's display). It is also preferable to sketch the cameras' positions relative to the crime scene. In an example of a family law case that hinges on a question of infidelity, any videos or audio that can be acquired from their smartphones, home PCs, etc. can be of use for litigation arguments. Conversations of interest, videos supporting infidelity are common pieces of evidence that would be of interest. During evidence presentation (playback) in court, care should be taken to play the video or audio in its native format unless required. Any enhancements or modifications should be documented and presented alongside the evidence. Depending on the grueling/sensitive details in the evidence, redaction of certain segments of the audio or video are usually agreed by the

prosecuting and opposing legal teams prior to presentation in court. Un-redacted versions of the evidence may be made available to the jury if needed. Thus, both versions of the evidence (redacted and un-redacted) should be preserved along with backups of true copies. Depending on the circumstance, the surroundings, and the witnesses who may have been present, several different audio/video recordings of an event may be available to the digital forensic investigators. Even if the recording does not appear to be very clear or useful, all relevant data (video footage, voice) should be collected for processing. Proven forensic enhancement techniques employed by skilled forensic professionals can help recover details pertinent to the investigation or legal case. In audio forensic investigations involving languages uncommon to the region or investigation team, a forensic phonetician working with an independent translator who speaks that language may be required. A true copy of the audio and video files should then be made for all future viewing, preserving the original video evidence.

3.4.6 Access Control, Data and Logs

Access control is often reported as broken in real-world practices due to design issues, policy misconfigurations, deployment, and maintenance. Very often an enterprise's access control realm is managed by many administrators without comprehensive organizational policies and industry standards. However, due to the increased focus on Cybersecurity these-days, enterprises are continuously made aware of this important security control by leveraging strong identity verification and credentialing. In our personal lives, access to data and devices is a common occurrence through passwords, passcodes, biometrics and pin-codes. User's access to devices and computers is one of the key interests of digital forensic professionals and incident forensic investigators. Questions such as when was the last time of access, who accessed the data/device, how was the data/device accessed, etc., form the elementary lines of questioning.

Log files are an extremely valuable piece of information that are created by a computer, network devices, server, or file system. With declining storage costs and growing storage media on the device and in the cloud, the level/depth of logging has improved in the last decades. Networks, applications, browsers, and file systems often log events, actions and errors. This data can be helpful to digital forensic investigators as logs can be easily parsed and usually contain running timestamps. In an example of a family law case that hinges on a question of infidelity, the access mechanisms of the suspects are of interest along with the logs of their activity. A simple check of their passwords (passwords containing a partner/friend Date of Birth or name) may weakly allude to infidelity, while shared access with another partner/friend may strongly allude to infidelity. Call logs, browser history logs, App logs, smartphone system logs, etc. can provide valuable insight to the investigation.

3.4.7 Browser, Internet and Dark-Web Data

In many legal cases (civil or criminal), Internet usage data acquired from the browser of the suspect has proven to be a valuable source of information. The keywords used by the suspect on search engines, the website(s) visited, browser cookies, stored passwords, browser cache, coupled with the time of visit is often used in legal arguments as evidence. Various digital forensic tools have been proposed for extracting data from a browser. Each browser has its own architecture and storage design. Also, it's not uncommon to find a suspect using more than one browser. These days, Internet activity is used in court to portray the suspect's state of mind [37]. Most web browsers provide an erase function for log information such as the cache, history, cookies, and download list [38]. It's important to note that forensic investigations can be difficult when users erase browser data or surf the Internet in private mode or when browsers use TOR based routers.

Internet data as evidence can be categorized into three different types and likely to be the subject of an inquiry into their authenticity: data posted on a website by the site's owner, data posted on a website by others with the owner's consent (chat room participants or social-media postings), and data posted on a website by others without the owner's consent (content due to hacker activity) [39]. Various forensic approaches have been proposed to glean information from social media sites [40], [41] and microblogging sites like Pinterest and Tumblr [42]. However, suspects can

anonymize their on-line identify by using pseudo names, avatars or aliases while on the Internet, thereby impacting forensic investigations. In such cases, investigators fallback on additional data such as network and locale details, behavior patterns, etc. to profile and identify the suspect.

The Dark Web and Deep Web can offer a ton of evidence, but in many instances, they may quickly evolve into criminal investigations. The Deep Web refers to the non-indexed website pages, while the Dark Web refers to pages which are both non-indexed and involved in illegal activity. Given the nature of anonymous access that it offers, users and website operators can remain anonymous or untraceable. Typically data that ends up in these parts of the Internet world are considered nefarious as websites in the Dark-Web often deal in new cyber exploits, Malware, compromised credentials, social security numbers, child-porn, crypto currencies and contraband. While the eDiscovery process can be scaled to address the Dark-Web and Deep-Web, evidentiary data from these realms of the Internet must be acquired through skilled forensic and security professionals. Browsers that assist with accessing websites on the Dark-Web and Deep-Web can be technically challenging to forensically analyze due to their support for anonymity. However, once data is acquired from this world of the Internet, they can be treated as any Internet data for forensic and eDiscovery analysis.

In an example of a family law case that hinges on a question of infidelity, the browser history or cookies may show the husband was hiding marital assets at an offshore bank in the name of his friend/partner. Similarly, the partner/wife's Internet usage can show that she shopped for certain gifts for her friend/partner. Such data when pieced together can show probable cause or be treated as circumstantial evidence during legal arguments.

3.4.8 Passwords, Certificates, Keys, Digital Signatures

Often sensitive data is given priority for forensic management over security control technology-related artifacts such as passwords, SSL client certificates, digital signatures, and cryptographic digital keys. These may be part of the evidence pile but are crucial in accessing evidence if it so happens that evidence is secured with such technologies. Since the last decade, Mobile Device Management (MDM) platforms are used extensively to remotely provision devices, manage applications and enforce mobile device policies. Only by managing the mobile devices as closely as a desktop (at an organization premises), can the enterprise trust the device as an extension of its network [43]. Such management platforms rely on digital certificates often base on public-key encryption technology. Digital certificates are also used to protect websites, VPNs, wireless networks and other applications. Mobile devices issued by enterprises or BYOD (bring-your-own-device) usually have digital certificates deployed on these devices to manage them and limit user access on enterprise networks and resources [44]. Some of these security control artifacts like SSL certificates can be time-sensitive, but care should be taken when decrypting/unlocking digital evidence when it is coupled with such security technology. Decrypted digital evidence should then be stored securely and separately with multiple layers of authentication controls, while, digital artifacts from their security controls (passwords, certificates, keys, wallets and digital signatures) should be stored separately on a managed keystore, password vaults or Public Key Infrastructure (PKI) platform.

In an example of a family law case that hinges on a question of infidelity, if the suspect has a password that unlocks the smartphone, the password should be used by digital forensic professionals during eDiscovery process to carefully unlock the smartphone and the locking feature should then be disabled on the smartphone device to safely put it through various forensic tests. This allows the disuse of the password and it can be safely stored/documented as part of the evidence analysis (smartphone) documentation. Similarly, if the suspect has data (say compromising photos with a partner/friend) that is encrypted with a private key, forensic professionals may decrypt the data with the private key to then safely work with the decrypted data. The private key should not be used to encrypt back the evidence unless required. The private key should then be stored within a cryptographic digital key management platform/solution. Likewise, if the suspect uses digitally signed certificates to establish secure communication (say Virtual Private Networks, secure Wi-Fi, secure email) for mobile/Internet

Applications (say email, banking, bitcoin wallets, dating or adult Apps), these digital certificates should be acquired from the smartphone device and placed in a secure certificate management platform/solution. We need to note that these certificates may be revoked by the issuing authority or may expire over time. Other public/private keys will also need to be similarly safeguarded.

3.4.9 Intellectual Property - Patents, Copyrights, Trademarks, Trade Secrets, Industrial Designs, Geographical Indications

Administered by the United States Patent and Trademark Office (USPTO), patents are legal protections granted for tangible inventions. A patent grants “the right to exclude others” from using or selling the protected invention for a specific period of time. Copyrights are legal protections granted for “original works of authorship” such as music, literature, pictures, designs, graphics, sound recordings, architectural works, and other artistic expressions. Trademarks are legal protections that safeguard the names, phrases, logos, and symbols that identify the producer of specific goods or services. Geographical indications and appellations of origin are signs used on goods that have a particular geographical origin. An industrial design constitutes the three-dimensional ornamental or aesthetic aspect of an article. In the U.S., in addition to these federal protections, each state has its own law to protect “trade secrets” — the proprietary recipes, formulas, compositions, and processes that provide a competitive edge of a product in the marketplace. Altogether, federal and state laws are complex enough to set standards across the globe.

Unless already in the public domain, sensitive information like unpublished patent designs, Intellectual Property (IP), copyrights, trademarks, trade secrets, etc. should be forensically acquired for eDiscovery from information systems/ devices and managed with strict privacy and security controls. While such data is often in the form of digital data and files, there can be physical (movable/immovable) artifacts that may also fall in this realm. A high level of data complexity, usually involving multiple parties, custodians, experts and document sources and formats are common during eDiscovery in Intellectual Property (IP) or patent infringement cases. In IP litigation, where data concerns the proprietary process or trade secrets of an organization, the risk of a data breach is compounded by the potential release of privileged information to legal opponents or the public. Post digital forensic extraction of such data from (database systems, computer disks, etc.) every step of litigation is both an exercise in privacy, cyber security and corporate strategy. In spite of the overall complexity of these cases, standard litigation deadlines must still be met, making review speed with minimal errors and efficiency, critically essential factors in IP legal cases. Intellectual Property forensic investigations for theft are handled differently than criminal cases, since it requires a deep dive into data movement over networks, harvesting data from devices and strong expertise in IP theft investigations. Such investigations can be time-consuming and may need a detailed understanding of the IP in question.

In an example of a legal case that hinges on a question of copyright infringement by another company on its website, digital forensic investigators must isolate the questionable website data and then work with legal teams to assist in verifying the alleged misuse of copyright. Digital Forensic evidence would typically include website data, website logs, page design aspects, etc. An example of an avenue for copyright violations is the video-sharing web platform YouTube, where the platform is constantly forensically monitored for music/video copyright violations due to users uploading content.

3.4.10 Databases

Mention of databases in eDiscovery discussions can be for various reasons; 1. As a storage repository (database platform) for ESI (digital data, digital documents, images, videos, etc.). 2. As a source/evidence for eDiscovery (database forensics) purposes as outlined by The Sedona Conference Database Principles [45]. 3. As a searchable corpus of case-related data from various U.S. state and federal courts like K&L repository [46]. 4. As possible temporary storage repositories during the analytical processing of ESI. 5. As storage repositories extracted by Digital Forensic tools. Example; MySQL database files found on a smartphone.

This section discusses databases as a source of evidence for eDiscovery purposes. The Sedona Conference Database Principles [45] is an in-depth document that discusses this topic as databases are structured, and legal professionals may not be that technology savvy to deal with database technology, and Structured Query Language (SQL) queries. Most companies use and maintain database systems that run their organization systems. Similar databases in smaller sizes also exist on our mobile devices. Information stored in such databases (such as raw data, graphs, images, videos, digital keys) differs fundamentally from discrete unstructured data as they are in a structured format and normalized in their schema design. While structured data is arguably easier to search during eDiscovery when compared to unstructured data, special skills are required when working with databases as their schema design can often be complicated. When a database is part of the evidence pile, digital forensic investigators must look beyond the single database to the other applications that use the database, such as business intelligence systems, marketing applications, payrolls, human resources, insurance, employee benefits, etc. A mere search query may not result in accurate results (data) unless the schema layout is well understood by a database-savvy forensic professional. This area of expertise has given rise to the sub-discipline of digital forensics, namely database forensics.

Databases from platforms such as Microsoft SQL Server, Oracle, Microsoft Access, Informix, Lotus Notes, PostgreSQL, and DB2 are usually popular in organizations, while mobile devices usually contain databases using MySQL, SQLite, MariaDB, MongoDB, etc. Of recent, there have been numerous databases (including NoSQL) gaining popularity such as RethinkDB, OrientDB, ArangoDB, Cassandra, Couchbase, MarkLogic, LocustDB, Redis, ClickHouse, etc. Big data and real-time web applications often used NoSQL databases. NoSQL databases support SQL-like query languages and lack the ability for joins in queries, making the database schema design to be different than relational databases. A digital device or an organization server that are part of the case ESI may also host multiple types of databases. Such wide choices of databases can be challenging to database forensic professionals as they need to be skilled across many types of databases for the case. Few database product vendors have started to assist with eDiscovery tasks by offering additional product features that can assist with searches, classification, labeling, and reporting data in these databases [47], [48]. Database forensics may also leverage data analytics helping the eDiscovery team to sort through large amounts of structured data to identify relevant information, interpret relationships between large data sets, seek-and-compare among data to identify anomalies within databases, analyze data points, and support subject matter experts, such as forensic accountants, and damages experts working on antitrust, financial, or accounting matters [49].

3.4.11 Financial Data

It is often said that the most effective way to conduct an investigation is to follow the money. Financial data investigation is a branch of forensics known as forensic accounting. Forensic accounting is a combination of traditional accounting techniques and investigative techniques used to discover financial crimes. One of forensic accounting's key functions is to explain the nature and extent of a financial crime to the courts. Since the last two decades, banking, finance, and organization accounting has been largely executed by financial systems/platforms such as SAP, Salesforce, Oracle Financials, etc. They often integrate well with the stock market (stock exchange) and support custom accounting practices across geographies. Forensic accounting professionals investigate cases of tax fraud, money, determine the value of a business, laundering, and other financial criminal activity. They are not financial auditors and are usually called in when an organization or federal regulators/agencies suspect financial wrongdoing. Increasingly, they are also called upon to perform preventative work by advising, designing systems, and procedures for both private companies and the government to limit fraud. Professionals in the financial forensics field are highly skilled and are required to have a bachelor's degree in accounting as well as be a Certified Public Accountant (CPA). Forensic accountants may also be certified by the American Board of Forensic Accounting. Forensic accountants must have a solid knowledge of the audit process, financial systems, business administration, techniques for analyzing data for fraud detection, and more. They must be detail-oriented, good with numbers, have strong critical thinking skills, and be skilled at picking

irregularities out of a pattern. Although they work with digital systems and data on computers, spreadsheets, etc., they are not typically the digital forensic professionals to extract financial data of interest from computer disks, the Internet, etc. This stage of data acquisition and extraction is still the job of traditional digital forensic professionals. Thus, it is safe to say that traditional digital forensics and forensic accounting professions are separate skilled spheres with little in common unless they are working as a team during eDiscovery for litigation purposes or when investigating a data breach. In an example of a legal case led by federal agencies involving fraud investigation on alleged fraud and corruption by a whistleblower (employee) of an organization, forensic professionals (both digital forensics and accounting/finance forensics) work with legal teams to first plan on the scope of an investigation followed by data (evidence) gathering, analysis, and reporting. Based on the allegations by the whistleblower, the organization may also engage an in-house team to assist the federal agencies and simultaneously conduct their own internal investigation. Typical preliminary steps taken by the organization being investigated would include;

a) Alerting in-house legal team to engage with the federal agencies in the litigation.
b) Removing access to company servers and devices for the suspected wrongdoers.
c) Activate additional monitoring and logging on financial systems.
d) Possible suspension of employment for the suspected wrongdoers.
e) Alerting the organization Information Technology Team to monitor any suspicious deletion, copying or transfer of data.

Financial data (mostly in digital form) is gathered by both digital forensic and accounting/finance forensic professionals and are then analyzed along with the legal team to ascertain fraud or corruption as alleged by the whistleblower (employee) of the organization. Typical digital forms of financial data in the case ESI include spreadsheets, transaction files, and data extracted from financial systems via search queries, system log data, system audit data and user access data.

3.4.12 Crypto Currency Data

A crypto currency (or cryptocurrency) is a digital asset that serves as an alternative to traditional currencies of the world. It has been a decade since the Bitcoin Network was launched, and the very first crypto currency was released for use [50]. Since then, many variants of crypto currencies have evolved for public use like, Ethereum, Ripple, Tether, Binance, Litecoin, Monero, etc. Over the years, while they have gained popularity, and in spite of their many advantages, they have also gained tremendous notoriety, making them an illegal means of exchange in many countries [51], [52], [53]. In May 2019, The Wall Street Journal had reported that more than $1.7 billion in crypto currency had been stolen from exchanges around the world [54]. Crypto currencies provide new opportunities for money launderers through the partial anonymity they can provide and the lack of centralized supervision. Accordingly, forensic accounting has also moved into address crypto currencies. Usually, a crypto currency is stored in “wallets” accessible by private keys and traded across crypto currency exchanges and transactions involving this currency is tracked and stored in a ledger (computerized database). Most crypto currency transactions are publicly viewable on a blockchain ledger, which provides the public key addresses, amounts, and timestamp associated with each transaction. Thus, crypto currency forensics is a specialized skill that involves digital forensic professionals with knowledge of accounting forensics, network forensics, mobile forensics, computer forensics, blockchain technology, cryptography, crypto currency exchanges, and cyber-security. Ediscovery in this field would take crypto forensic investigators across computer networks in other countries and may involve cross-border co-operation. Crypto currency forensics can be challenging for traditional accounting forensic professionals migrating into this field, mostly due to the technology involved. Few challenges can be listed as below [55];

a) Understanding how value is exchanged in a given crypto currency transaction.
b) Most financial institutions lack a business strategy or related controls for crypto currencies.

c) Investigations that involve crypto currency have the potential to become complex international issues, as they often cross geographies and involve high-risk locations abroad where financial controls are weak or nonexistent.
d) Identifying the source of funds can be difficult and complex in the crypto currency ecosystem.
e) Technology challenges in determining crypto currency wallet provider/payer, network forensics, computer forensics, mobile forensics, transaction identity, blockchain technology, identifying beneficiaries, forensic accounting analytics, crypto currency exchange mechanisms, cloud forensics, crypto currency mining, crypto currency ledgers, and cyber security.
f) Recovering crypto currency assets can be challenging due to scare success in prior recoveries.
g) Criminals commonly obfuscate transaction details and IP addresses in an effort to launder crypto currency assets.

Crypto currency forensics is highly technology-driven and multiple crypto currency specific tools need to be forensically documented as “wallets” can reside on computers as well as on mobile devices. Doran [56] conducts a forensic investigation for evidence of bitcoin mining on a computer and outlines various artifacts that a forensic investigator would look into when investigating a mining case. Ediscovery would largely depend on findings of crypto currency forensic professionals and this can run into many legal roadblocks due to cross border legal complexity. Needless to say, in such instances, eDiscovery can be time-consuming and expensive given the skilled resources required and the cross-border laws to address. Crypto currency is here to stay and continues to redefine the way governments, financial institutions, banks, and citizens across the globe define ‘money’.

In an example of a family law case on divorce that hinges on a question of infidelity, any hidden crypto currency assets of spouse/partner can be considered financial assets and part of the divorce settlement. The eDiscovery process assisted by crypto currency forensic professionals would help trace crypto currency assets, tax return filings, and transactions from crypto-wallets and capture such data in the financial intake process. If the spouse/partner is suspected to hiding crypto currencies, eDiscovery process will need to investigate further if crypto currency has been parked elsewhere to avoid disclosure during divorce proceedings/settlement. This would entail harvest crypto currency transaction data from crypto currency ledgers, exchanges and tracking crypto currency transactions over a period o time to establish a case. In California, spouses owe each other a fiduciary duty to disclose all assets/debts and duty of the highest good faith and fair dealing. Thus, if one spouse/partner is hiding a crypto currency asset from the other, and it is later found, the aggrieved spouse has a strong legal claim to recover 100% of that asset [57]. Likewise, other states in the U.S. have similar laws. However, since the crypto currency industry is largely unregulated by traditional government laws and extends beyond country borders, federal law enforcement and other international regulatory agencies may get involved in crypto currency transactions if found suspect and undeclared on tax fillings.

3.4.13 Social Media Data

Social media data can be considered as a combination of digital data from media posts, tweets, likes, comments/conversations, profile page visits, and timestamps, re-tweets, embedded images/ video/icons/gif, and their hyperlinks, message replies, forwarded recipients, etc. People (subjects/actors) involved in these ancillary data may also have a link to the suspect’s social media data, and thus their profile data may also be needed for an investigation. This raises the question as to how much deep and wide an digital forensic investigator should cast his/her net when investigating the suspects’ social media data. The answer would lie in the data harvesting tools involved and the investigation itself, but gleaning ancillary data should be a scalable task when needed. As overlooking data key to the investigation can happen, it would be safe to extract as much as related data as possible, depending on the processing tool’s capability. Analytical (statistical) processing of this data into a visual timeline and possible clusters/patterns can be tremendously helpful for the investigation and during legal presentations.

In an example of a family law case that hinges on a question of infidelity, social media data can be a cookie jar of evidence. These days, with the rising access via smartphones to the Internet and social networking sites, mobile devices would be a common source to forensically investigate, followed by computers/laptops used by the parties of the case. Other digital sources of information for this case may be public cameras at places they visited, social media postings of their friends, Google Maps street view data [58], [59], their Internet footprints like product reviews, social networking sites likes/dislikes, comments to other's postings, etc. can all provide clues to build their profile, a story, an alibi, and provide valuable information to legal arguments. All this digital data is often forensically extracted/scrapped from social media websites, cloud storage, their devices, and the Internet. Once extracted, depending on the technology use of the parties, this data may result in large volumes of data (thousands of files and gigabytes/terabytes in size) for culling and analysis (analytics and correlation). Coupled with implementing Artificial Intelligence algorithms/techniques, such volumes can be analyzed by eDiscovery teams in shorter timeframes.

4. FORENSIC EVIDENCE MANAGEMENT IN EDISCOVERY

Digital forensic evidence can be considered digital assets to a legal entity, and their management can be challenging due to many reasons. This section deals with few focus areas on forensic evidence management and safe disposal options.

4.1 Evidence Integrity

Once digital evidence is forensically collected, eDiscovery teams begin their reviews and analysis using various software tools. This can cause a change in evidence state, thereby impacting evidence integrity. While such analysis techniques are the backbone of the eDiscovery process, care must be taken to log all state changes that occur against the evidence. For example, forensically extracted emails from a Mail Exchange server are further subject to analysis by the eDiscovery team. All eDiscovery analysis tasks must involve write blockers or employ read-only mechanisms to prevent accidental compromise of emails (evidence).

4.2 Evidence - Data Acquisition and Extraction

Acquisition and extraction are often confused in digital forensics. Acquisition (logical and physical) is the process of collecting digital evidence from electronic media. There are four methods for acquiring data: disk-to-disk copy, disk-to-image file, logical disk-to-disk file, and sparse data copy of a file or folder. The term extraction is typically referred to data extractions that do not recover deleted data or include a full bit-by-bit copy of the evidence. Acquisition of each type of device has its own techniques and challenges. Care should be taken to identify a forensic plan before starting out on the forensic process. Preference should be given to the device OEM (original equipment manufacturer) application programming interface for data extractions. For digital forensics of social media websites or when working with cloud storage, third-party tools used should be vetted by the industry, and the process should be verified.

4.3 Evidence - Preservation & Retention

Evidence preservation is the process of preserving digital evidence at a secure physical location so that it cannot be changed or altered. Only well-preserved evidence can be presented for legal proceedings. Preservation of electronic evidence is the first step when litigation has been filed, will soon be filed, or an investigation is needed [60]. The federal courts have recognized evidence preservation as a common law duty that arises even before a claim is filed and have asserted their power to impose sanctions on the breach of this duty [61]. Every federal court to have confronted the issue of evidence preservation has held that the duty of preservation arises prior to the initiation of litigation [62], [63], [64]. Litigants have an "uncompromising duty to preserve" what they know or reasonably should know will be relevant evidence in a future or pending lawsuit, even though no eDiscovery request or order to preserve the evidence has been made [65]. Federal Rule of Civil Procedure (FRCP) Rule 26 and Rule 37(e), outline the requirement that litigants specifically address the issue of ESI preservation as part of their conference and discovery plans [66]. FRCP Rule 26 also highlights the thorny issue of evidence preservation in

the modern digital age and how critical it is for litigants to be vigilant right from the earliest possible stage as part of their pre-litigation preservation duties. The FRCP Rule 26 also emphasizes how important it is for the parties to address and discuss evidence preservation issues early in the case and work cooperatively to sort through them. However, even under the existing case law, determining when the duty to preserve has been triggered under FRCP Rules, and the scope of that duty often remains challenging [67]. Keeping this in mind, we focus on evidence preservation duties and processes once it is identified as part of a legal case ESI.

Electronic evidence (ESI) may be readily accessible (such as files on a storage drive or emails) or may need forensics to extract from devices (such as smartphone browsing data, residual data, computer disks, or accounting data). Either way, electronic evidence (ESI) preservation pertaining to a case is often achieved through the combination of policies, standards, security controls, and periodic security risk assessments. Information technology programs such as disaster-recovery, data retention coupled with organization-level policies and standards are often the backbone of programs that assist with the preservation. Security controls such as access controls, data encryption, and data leak/loss prevention (DLP) controls are often deployed after periodic assessments of vulnerabilities and risk. Compliance programs such as periodic audits, privacy assessments, and Data Protection Impact Assessment (DPIA) are also required depending on local laws applicable. Management of the above programs, monitoring of case ESI data, and security controls can be part of maintenance activities that can get costly. While the general rule is that a party generating data must bear the costs of preserving and producing it, few courts have adopted a balancing test to determine which party needs to bear these sometimes staggering costs [68], [69]. Figure 5 highlights few policies that can be created towards evidence retention and preservation in a legal case setting.

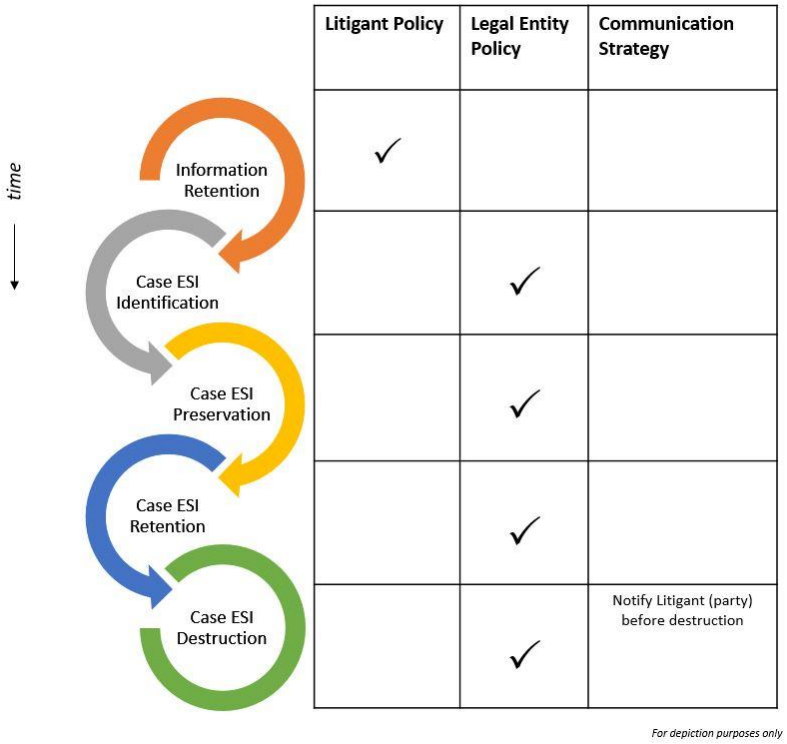

FIGURE 5: Policies regarding retention and preservation in a legal case setting.

Often preservation of ESI may be undertaken within the organization's (litigants) storage infrastructure or at the legal entity's storage infrastructure. Various third parties may have ESI that an organization may be deemed to be in control of (due to contractual relationship, shared drives) and consequently may fall within the company's preservation obligation [70]. Arbitrarily deleting

digital documents without proper archival or failing to retrieve digital records when needed can increase a company's risk of legal liability. To minimize this risk, many organizations employ a data retention process to aid in eDiscovery and digital forensics. These days, since cloud storage is attractive in many ways and is cost-effective, the cloud could very well be the storage location for a case's ESI. The period of preservation of ESI depends on the case and pragmatic concerns ranging from whether the enterprise has governmentally mandated reporting requirements to how much storage space the organization has. Regardless of whether an organization is involved in litigation, a stated document retention policy is necessary. The policy should reference standards that delve into the preservation of technology controls (technical and non-technical) and should reference periodic audits. "Spoliation" is the willful destruction or significant alteration of case evidence (ESI), or the failure to preserve ESI for another's use as evidence in pending or reasonably foreseeable litigation [69]. Sanctions for Spoliation of evidence are wide-ranging and completely in the hands of the court.

4.4 Evidence - Security

Enforcement of a managed security program throughout the preservation phase of a case can help secure case ESI during its lifecycle. Provision of security controls such as access controls, logging, encryption, hashing, risk assessments, vulnerability assessments is mandatory when working with case evidence. Data leak/loss prevention controls have to be deployed to alert on data breaches. Audit and log trails from eDiscovery tools can help track user activity in addition to implementing multi-factor authentication. Encryption of data while at rest and transit is to be followed. Implementing Identity and Access Management (IDAM), Incident Response Management, and data privacy techniques such as pseudonymization, tokenization, redaction, masking, etc., can greatly help to secure PII or PHI within the case ESI. Security best practices for case hardware evidence (devices) may follow procedures similar to law enforcement agencies, such as placing hardware in a secure environment and creating a chain of custody. A security policy is the teeth and the hammer for the previously discussed data security controls. A data breach incident insurance can help protect against cyber risks.

4.5 Evidence - Privacy Management

Data privacy and security are two essential constituents of a successful case ESI data protection strategy. Where data privacy and security begin to differ is in whom or what they are protecting data from. Privacy is concerned with ensuring the data that any given organization collects, processes, stores, or transmits is according to applicable laws and with the consent from the owner of that data. Not all the data (of its owner) may be sensitive; however, isolating sensitive data for applying privacy controls can be challenging. With increasing privacy concerns across the globe, privacy of evidence can be challenging while adhering to these laws and regulations such as PCI DSS, GDPR, CCPA, HIPAA, etc. A data management program in an organization can greatly assist with classifying data and selecting privacy controls to manage it.

4.6 Evidence - Destruction

Digital evidence destruction is the last stage in the case ESI lifecycle. While the final stages of eDiscovery deals with the production and presentation of key evidence from the case ESI, destruction of evidence happens when litigation is fully concluded. In civil cases, spoliation (destruction) of evidence possessed by a party (intentionally or negligently) can result in the court granting the opposing party a jury instruction allowing the jury to infer that the destroyed evidence as favorable to the opponent. This discourages the destruction of the relevant evidence in civil litigation [71]. However, in criminal cases, if the defendant were to destroy evidence relevant to the offense charged, the defendant would almost certainly be charged with obstruction of evidence.

Destruction of evidence (intentionally or negligently) prior to litigation conclusion can be legally complicated, and thus any destruction is to be performed through instructions from the legal team overseeing the case. Approvals from the case legal team must be internally sought before evidence destruction. The case ESI data owner would be the final authority who authorizes destruction. All steps taken to destroy must be documented, and industry standards applied to

delete residual data off ESI storage locations must be followed. Residual data on storage devices cannot be retrieved even when using modern forensic techniques when adequate industry-approved data destruction processes are employed [10]. Internal policies on communicating with the litigant/client prior to destruction is recommended. In cloud storage, adequate language in the contracts with cloud service providers should be included so that destruction can be undertaken by them and validated by the case ESI data owner. Verification and validation of the destruction process must be part of the standard operating procedures. Organization-level data management policies (that of legal entity or litigant) should clearly define data retention, and destruction guidelines and standards followed. In case of negligent/accidental spoliation of case ESI, the legal team and management should be immediately notified. Thus, stakes are high around evidence destruction, and care must be taken to undertake it after necessary approvals and should follow industry standards.

5. CONCLUSION

Digital forensics in the world of eDiscovery is often key to uncover case evidence that may otherwise be in a hidden state. With the growth of digital evidence in non-criminal litigation, digital forensic professionals are called upon to work with large teams of attorneys, paralegals, and eDiscovery professionals. Often a team of digital forensic professionals work under the guidance of the case eDiscovery team leadership. They need to understand their role in such environments and possible tasks being assigned. Digital forensic professionals need to have a deep understanding of the case scope, be team players and possess sound forensic skills for the success of the case. Skilled personnel in digital forensics and eDiscovery have to work in tandem on the case to assist attorneys in preparing case arguments and maybe even be called upon to testify in court regarding the techniques, and conclusions undertaken in their work. This article highlights the interplay of digital forensics and eDiscovery disciplines and the expectations of digital forensic professionals when working with the eDiscovery teams. As part of future work, we propose cataloging select legal cases wherein forensically uncovered digital evidence was found to be critical to the case outcome and thereby highlighting the lessons learned from each case towards digital forensic best practices.

6. REFERENCES

[1] J. O. Holley, P. H. Luehr, J. R. Smith, and J. J. Schwerha. (2010), “Electronic discovery”, in Handb. Digit. Forensics Investig. Elsevier Ltd, ch. 3, pp. 63–133.

[2] “Key Differences Between eDiscovery and Digital Forensics,” [Online]. Available: https://teris:com/key-differences-betweenediscovery-and-digital-forensics/ , 2012, [Accessed September 05, 2020].

[3] R. Chozick, “How To Align Your Forensics Support to Your Case Timeline — Flashback Data,” [Online]. Available: https://www:flashbackdata:com/how-to-align-your-forensicssupport-to-your-case-timeline/ , 2018, [Accessed September 04, 2020].

[4] K. Burke, “107 Texting Statistics That Answer All Your Questions,”[Online]. Available: https://www:textrequest:com/blog/textingstatistics-answer-questions/, 2016, [Accessed September 05, 2020].

[5] A. Smith. (2015), “U.S. Smartphone Use in 2015 — Pew Research Center”, [Online]. Available: https://www:pewresearch:org/internet/2015/04/01/us-smartphone-use-in-2015/ [Accessed October 30, 2020].

[6] R. Attoe. (2015), “Digital forensics in an eDiscovery world,” in Digit. Forensics, Threat. Best Pract., ch. 6, pp. 85–98.

[7] D. Garrie and J. D. Morrissy. (2014), “Digital Forensic Evidence in the Courtroom: Understanding Content and Quality,” Northwest. J.Technol. Intellect. Prop., vol. 12, no. 2,

[Online]. Available: https://scholarlycommons:law:northwestern:edu/njtip/vol12/iss2/5 , [Accessed October 10, 2020].

[8] S. Krishnan and N. Shashidhar, (2019), "eDiscovery Challenges in Healthcare", Int. J. Inf. Secur. Sci., vol. 8, no. 2, [Online]. Available: https://www.ijiss.org/ijiss/index.php/ijiss/article/view/374 , [Accessed October 10, 2020].

[9] B. T. Ward, C. Purwin, J. C. Sipior, and L. Volonino. (2009 September), "Recognizing the impact of E-discovery amendments on electronic records management", Inf. Syst. Manag., vol. 26, no. 4, pp. 350–356, [Online]. Available: https://www:tandfonline:com/doi/abs/10:1080/10580530903245721 , [Accessed October 7, 2020].

[10] S. Krishnan, A. Neyaz, and N. Shashidhar, (2019), "A Survey of Security and Forensic Features In Popular eDiscovery Software Suites", International Journal of Security (IJS) vol.10, no.2, pp 16-30, [Online]. Available: https://www.cscjournals.org/library/manuscriptinfo.php?mc=IJS-152#MCAI, [Accessed October 10, 2020].

[11] "Federal Rules of Evidence — Federal Rules of Evidence — US Law — LII / Legal Information Institute." [Online]. Available: https://www:law:cornell:edu/rules/fre , [Accessed October 7, 2020].

[12] "Federal Rules of Civil Procedure — Federal Rules of Civil Procedure — US Law — LII / Legal Information Institute." [Online]. Available: https://www:law:cornell:edu/rules/frcp , [Accessed October 7, 2020].

[13] "Admissibility of Digital Evidence in Court," [Online]. Available: https://www:atlanticdf:com/blog/2017/12/18/admissibilityof-digital-evidence-in-court/ , 2017, [Accessed October 8, 2020].

[14] J. R. Vacca, "THE RULES OF EVIDENCE", in Computer Forensics: Computer Crime Scene Investigation, Charles River Media; 1st edition, p. 124., 2005, [Accessed October 8, 2020].

[15] S. Bommisetty, R. Tamma, and H. Mahalik. (2014), "Rules of evidence," in Practical. Mobile Forensics, ch 1, p. 23., [Accessed October 8, 2020].

[16] A. Antwi-Boasiako and H. Venter. "A model for digital evidence admissibility assessment", Advances in Digital Forensics XIII., vol.511. Springer New York LLC, pp. 23–38. [Online]. Available: https://link:springer:com/chapter/10:1007/978-3-319-67208-3 2 , 2017, [Accessed October 8, 2020].

[17] M.-H. Maras and M. D. Miranda. (2017 January), "Overlooking forensic evidence? A review of the 2014 International Protocol on the Documentation and Investigation of Sexual Violence in Conflict", Glob. Secur. Heal. Sci. Policy, vol. 2, no. 1, pp. 10–21, [Online]. Available: https://www:tandfonline:com/doi/abs/10:1080/23779497:2017:1281088 , [Accessed October 1, 2020].

[18] "Data Collection - Basics of E-Discovery Guide." [Online]. Available: https://www:exterro:com/basics-of-e-discovery/data-collection/ , [Accessed September 11, 2020].

[19] B. Carrier, "Defining Digital Forensic Examination and Analysis Tools", in Digit. Forensic Res. Work., [Online]. Available: https://www:dfrws:org/sites/default/files/session-files/presdefiningdigital forensic examination and analysis tools:pdf , 2001 , [Accessed September 12, 2020].

[20] L. Daniel and L. Daniel, Digital Forensics for Legal Professionals, Elsevier Inc., [Online]. Available: https://www:sciencedirect:com/book/9781597496438/digital-forensics-for-legal-professionals , 2012 , [Accessed September 12, 2020].

[21] N. A. Hassan and R. Hijazi. (2017), Data Hiding Techniques in Windows OS. Elsevier, [Online]. Available: https://www:sciencedirect:com/book/9780128044490/data-hiding-techniques-in-windows-os , [Accessed September 12, 2020].

[22] K. Redshaw, "What is Metadata in Web Writing?" [Online]. Available: https://www:kerryr:net/webwriting/metadata what is:htm , [Accessed September 14, 2020]

[23] R. D. Pittman and D. Shaver. (2010 January), "Chapter 5 - Windows Forensic Analysis", in Handbook of Digital Forensics and Investigation. Elsevier Ltd, pp. 209–300.

[24] D. Palmer, E. Blackburne, T. Lemoine, X. Zhang, K.R. Choo. (2020), "DFRWS IoT Forensic Challenge Report 1," in Digital Forensic Education: An Experiential Learning Approach, pp. 13–28. [Online]. Available: https://link:springer:com/chapter/10:1007/978-3-030-23547-52#citeas , [Accessed September 14, 2020].

[25] A. Tillekens, N.-A. Le-Khac, and T.-T. Pham-Thi, "A Bespoke Forensics GIS Tool", [Online]. Available: http://arxiv:org/abs/1704:03452 , April 2017, [Accessed September 12, 2020].

[26] S. Gilbertson, "Google Latitude Broadcasts Your Location — WIRED", [Online]. Available: https://www:wired:com/2009/02/googlelatitude/ , 2009, [Accessed September 15, 2020].

[27] C. Tilbury, "SANS Digital Forensics and Incident Response Blog — Big Brother Forensics: Device Tracking Using Browser-Based Artifacts (Part 1) — SANS Institute", [Online]. Available: https://www:sans:org/blog/big-brother-forensicsdevice-tracking-using-browser-based-artifacts-part-1/ , 2019, [Accessed September 18, 2020].

[28] S. J. Vaughan-Nichols, "FAQ: How Google Latitude locates you — Computerworld", [Online]. Available: https://www:computerworld:com/article/2530970/faq--howgoogle-latitude-locates-you:html, 2009, [Accessed September 17, 2020].

[29] C4ADS, "Above Us Only Stars — Exposing GPS Spoofing in Russia and Syria," Tech. Rep., [Online]. Available: https://www:c4reports:org/aboveusonlystars , 2019, [Accessed September 17, 2020].

[30] Krishnan, S., Zhou, B., & An, M. K. (2019). Smartphone Forensic Challenges. International Journal of Computer Science and Security (IJCSS), 13(5), 183. [Online]. Available: http://www:cscjournals:org/manuscript/Journals/IJCSS/Volume13/Issue5/IJCSS-1501:pdf , [Accessed September 18, 2020].

[31] "Audio forensics - Wikipedia." [Online]. Available: https://en:wikipedia:org/wiki/Audio forensics, [Accessed September 18, 2020].

[32] P. Manchester, "An Introduction To Forensic Audio." [Online]. Available: https://www:soundonsound:com/techniques/introduction-forensicaudio , [Accessed September 19, 2020].

[33] "Watergate" and Forensic Audio Engineering." [Online]. Available: http://www:aes:org/aeshc/docs/forensic:audio/watergate:tapes:introduction:html , [Accessed September 19, 2020].

[34] S. Ikram and H. Malik. (2010), "Digital audio forensics using background noise," IEEE International Conference on Multimedia and Expo, ICME 2010, pp. 106–110. [Online]. Available: https://ieeexplore.ieee.org/document/5582981 , [Accessed September 20, 2020].

[35] "What is Audio Forensics? Recordings used in Litigation." [Online]. Available: https://www:audioforensicexpert:com/what-isaudio-forensics/ , [Accessed September 20, 2020].

[36] National Forensic Science Technology Center, "A Simplified Guide To Forensic Audio and Video Analysis", Forensic Science Simplified [Internet] USA., [Online]. Available: http://www.forensicsciencesimplified.org/av/, September 2013, [Accessed September 19, 2020].

[37] B. Schneier, "Web Activity Used in Court to Portray State of Mind - Schneier on Security." [Online]. Available: https://www.schneier.com/blog/archives/2014/07/web_activity_us.html , July 2014, [Accessed September 19, 2020].

[38] J. Oh, S. Lee, and S. Lee. (2011 August) "Advanced evidence collection and analysis of web browser activity", in The Proceedings of the Eleventh Annual DFRWS Conference, vol. 8, no., pp. S62–S70, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1742287611000326 , [Accessed September 21, 2020].

[39] G. S. Bellas, "Internet Evidence: How to Authenticate Evidence From the Internet Under the New Illinois Rules of Evidence." [Online]. Available: https://www:bellas-wachowski:com/internet-evidence-howto-authenticate-evidence-from-the-internet:html , [Accessed September 19, 2020].

[40] A. Majeed, H. Zia, R. Imran, and S. Saleem. (2016 January), "Forensic analysis of three social media apps in windows 10," in 2015 12th Int. Conf. High-Capacity Opt. Networks Enabling/Emerging Technol. HONET-ICT 2015. Institute of Electrical and Electronics Engineers Inc., [Accessed September 19, 2020].

[41] M. N. Yusoff, A. Dehghantanha, and R. Mahmod. (2017 January), "Forensic Investigation of Social Media and Instant Messaging Services in Firefox OS: Facebook, Twitter, Google+, Telegram, OpenWapp, and Line as Case Studies," in Contemp. Digit. Forensic Investig. Cloud Mob. Appl.Elsevier Inc., pp. 41–62. , [Accessed September 19, 2020].

[42] B. McFadden, E. Balasubramani, and W. E. Miebaka. (2020), "Forensic Analysis of Microblogging Sites Using Pinterest and Tumblr as Case Study," in Zhang X., Choo KK. Digit. Forensic Educ. Stud. Big Data. Springer, Cham, pp. 243–279. [Online]. Available: https://link:springer:com/chapter/10:1007/978-3-030-23547-5 13 , [Accessed September 19, 2020].

[43] DigiCert, "Why digital certificates are essential for managing mobile devices," 2020. [Online]. Available: https://www:digicert:com/resources/solution-brief/why-digitalcertificates-are-essential-for-managing-mobile-devices-05-04-20:pdf , [Accessed September 20, 2020].

[44] J. Marchi, "7 Reasons to Use Digital Certificate for Mobile Authentication," 2016. [Online]. Available: https://www:globalsign:com/en/blog/using-digital-certificates-for-mobile-authentication , [Accessed September 22, 2020].

[45] T. S. Conference, "The Sedona Conference Database Principles, Addressing the Preservation and Production of Databases and Database Information on Civil Litigation," in Sedona Conf. Work. Gr. Electron. Doc. Retent. And Production, [Online]. Available:

https://thesedonaconference:org/sites/default/files/publications/171-216DatabasePrinciples 0.pdf , 2014 , [Accessed September 22, 2020].

[46] "Searchable e-Discovery Case Log." [Online]. Available: https://ediscovery:klgates:com/ , [Accessed September 22, 2020].

[47] "SQL Data Discovery & Classification – SQL Server — Microsoft Docs." [Online]. Available: https://docs:microsoft:com/en-us/sql/relational-databases/security/sqldata-discovery-and-classification?view=sql-server-ver15&tabs=t-sql , [Accessed September 22, 2020].

[48] "Automated Oracle data discovery and classification from Netwrix." [Online]. Available: https://www:netwrix:com/oracle data discovery.html , [Accessed September 22, 2020].

[49] "Database Discovery — iDS." [Online]. Available: https://idiscoverysolutions:com/database-discovery , [Accessed September 23, 2020].

[50] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Tech. Rep. [Online]. Available: https://bitcoin:org/bitcoin:pdf , [Accessed September 25, 2020].

[51] D. Stroukal and B. Nedvědová, "Bitcoin and other cryptocurrency as an instrument of crime in cyberspace," Proc. Bus. Manag. Conf., 2016. [Online]. Available: https://ideas.repec.org/p/sek/ibmpro/4407036.html , [Accessed September 27, 2020].

[52] C. A. Vyas and M. Lunagaria, "Security Concerns and Issues for Bitcoin," Tech. Rep. [Online]. Available: https://en:bitcoin:it/wiki/ , [Accessed September 27, 2020].

[53] E. Lam, "Binance Hack: 7,000 Bitcoin Worth $40 Million Stolen By Hackers - Bloomberg", [Online]. Available: https://www:bloomberg:com/news/articles/2019-05-08/crypto-exchange-giant-binance-reports-a-hack-of-7-000-bitcoin , 2019, [Accessed September 27, 2020].

[54] S. Russolillo, "Hackers Swipe More Than $40 Million of Bitcoin From Cryptocurrency Exchange - WSJ", [Online]. Available: https://www:wsj:com/articles/hackers-swipe-more-than-40-million-ofbitcoin-from-cryptocurrency-exchange-11557296830?tesla=y , 2019, [Accessed September 27, 2020].

[55] R. A. Musiala, T. M. Goody, V. Reynolds, L. Tenery, M. McGrath, C. Rowland, and S. Sekhri. (2020 March), "Cryptocurrencies: Forensic techniques to meet the challenge of new fraud and corruption risks, [Online]. Available: https://www.aicpa.org/content/dam/aicpa/interestareas/forensicandvaluation/newsandpublications/downloadabledocuments/eye-on-fraud-cryptocurrency-202003.pdf , [Accessed October 4, 2020].

[56] M. Doran, "A Forensic Look at Bitcoin Cryptocurrency," SANS Inst. Inf. Secur. Read. Room, [Online], Available: https://www.sans.org/reading-room/whitepapers/forensics/paper/36437 , 2020, [Accessed October 4, 2020].

[57] "Cryptocurrency and Forensic Accounting of Marital Assets," 2019. [Online]. Available: https://experts-blog:com/2019/01/28/cryptocurrency-and-forensic-accounting-of-marital-assets-in-divorce/.

[58] A. O'Leary, "Google Maps causes divorce after husband spots 'cheating' wife cuddling another man", [Online]. Available: https://www:mirror:co:uk/news/weird-news/google-maps-causesdivorce-after-13396055 , 2018, [Accessed October 5, 2020].

[59] M. Hohman, "Man Divorces Wife After Catching Her Cheating on Google Maps", [Online]. Available: https://people:com/home/man-catches-wife-cheating-google-maps-street-view-they-divorce/, 2018, [Accessed October 5, 2020].

[60] “E-Discovery & Digital Forensics - Data Preservations.” [Online]. Available: https://www:avansic:com/Services/DataPreservation/, [Accessed October 5, 2020].

[61] S. Scheindlin. (2010), “UNIV. OF MONTREAL PENSION PLAN v. Banc of Am. SEC., 685 F. Supp. 2d 456”, [Online]. Available: https://www:courtlistener:com/opinion/1881971/univ-of-montreal-pension-plan-v-banc-of-am-sec/ , [Accessed October 5, 2020].

[62] J. Koppel. (2012), “Federal Common Law and the Courts’ Regulation of Pre-Litigation Preservation,” SSRN, [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2154484 , [Accessed October 5, 2020].

[63] A. Kuperman. (2010), “Case Law on Elements of a Potential Preservation Rule, Memorandum to the Discovery Subcommittee,” pp. 5–17, [Online]. Available: https://www:uscourts:gov/sites/default/files/case law on elements of a potential preservation rule.pdf , [Accessed October 5, 2020].

[64] “Advisory Committee on Civil Rules, Agenda Book,” pp. 101–107, [Online]. Available: http://www:uscourts:gov/uscourts/RulesAndPolicies/rules/AgendaBooks/Civil/CV2011-11:pdf , 2011 , [Accessed October 5, 2020].

[65] M. E. Bale, “Trial Bar News,” Schwartz Semer. Atty. Law, [Online]. Available: https://www:schwartzsemerdjian:com/trialbar-news/evidence-preservation-and-litigation-holds , 2016 , [Accessed October 5, 2020].

[66] “Rule 26. Duty to Disclose; General Provisions Governing Discovery — Federal Rules of Civil Procedure — US Law.” [Online]. Available: https://www:law:cornell:edu/rules/frcp/rule 26 , [Accessed October 9, 2020].

[67] S. V. Ettari, “Reasonable Anticipation of Litigation Under FRCP 37(e): Triggers and Limits,” KRAMER LEVIN Naft. FRANKEL LLP, 2017, [Accessed October 10, 2020].

[68] “McPeek v. Ashcroft - 202 F.R.D. 31 (D.D.C. 2001)”, [Online]. Available: https://casetext:com/case/mcpeek-v-ashcroft-3 , 2001, [Accessed October 5, 2020].

[69] FindLaw Attorney Writers, “Delete At Your Peril: Preserving Electronic Evidence During The Litigation Process,” FindLaw, [Online]. Available: https://corporate:findlaw:com/litigation-disputes/delete-at-your-peril-preserving-electronic-evidence-during-the:html , 2018, [Accessed October 5, 2020].

[70] “E-Discovery Basics: Preservation of ESI, Part 2 (Vol. 1, No. 6),” [Online]. Available: https://www:gibsondunn:com/e-discoverybasics-preservation-of-esi-part-2-vol-1-no-6/[71] “Reforming Rules on Government Destruction of Evidence.” [Online]. Available: https://www:greenspunlaw:com/blog/governmentdestruction-of-evidence:cfm , 2011, [Accessed October 5, 2020].