Digital Forensics for Lawyers:
Uncovering Hidden Evidence to Win Your Case

IADC Annual Meeting
July 12, 2022

By: Kristina von der Linden, Bayer AG;
David Patron, Phelps Dunbar LLP, John Unice, bit-x-bit, LLC

Kristina von der Linden
Bayer AG
Compliance
Building Q 26, 0.006
51368 Leverkusen, Germany
kristina.vonderlinden@bayer.com

David L. Patrón
Phelps Dunbar LLP
Canal Place
365 Canal Street, Suite 2000
New Orleans, LA 70130
David.Patron@phelps.com

John Unice
bit-x-bit, LLC
437 Grant St., Suite 1250
Pittsburgh, PA 15219
john.unice@bit-x-bit.com

I. Introduction

Even before the COVID-19 pandemic, the workplace was becoming increasingly globalized by the proliferation of workplace collaboration technology and other tools that enabled colleagues to create, modify, and share information seamlessly across departments, companies and jurisdictions. Coupled with tools such as Slack and WhatsApp, mobile devices (smartphones and tablets) have also become in many ways indispensable to how we work and communicate. As the use of these platforms and devices to conduct business will only continue to grow, so, too will the data sources and volumes that attorneys will need to contend with in the context of investigations and litigation. With the explosion of electronic means by which we all work and communicate, the need to defensibly preserve, identify, cull, review, and make sense of electronic evidence is not going away anytime soon.

While these assets are very effective at helping us create and share information, attorneys often overlook the type (and amount) of information that can be uncovered from various data sources when the need arises. Too often, we think solely about the documents and files to which the custodian had access. But beneath the surface of what a typical user can see or touch lies a trove of information that can often help drive the prosecution, or defense, of various types of matters. This is where the discipline of digital forensics can be leveraged by attorneys to provide more proactive, holistic, and strategic advice to their clients.

As the business world has transitioned to mostly a remote, or hybrid, workforce, one resulting risk is that company data is now spread out beyond the company network or infrastructure. As colleagues change roles within organizations or jump from one company to the next, being able to track and recover important company assets is critical to protecting corporate assets. Global organizations that have employees in various jurisdictions add another layer of complexity to these challenges. Divergent data privacy rules directly impact how attorneys can defensibly (and legally) collect and analyze custodial data sources.

Using the electronic discovery reference model ("EDRM") as approximate guideposts, attorneys with a more informed understanding of digital forensics can better assist their clients in finding and preserving potentially relevant information as well as make sense of what truly lies beneath

the surface of evidence sources such as PCs, smartphones, cloud accounts, and email accounts. Accordingly, the need to know how organizations create information, how to retain potentially relevant evidence, and how to identify what is truly important to a case has become increasingly important.

The nuance that attorneys often disregard, or fail to consider, is the fact that they can add value by helping clients proactively identify where their information is, how it is stored, and how key evidence can be retrieved and analyzed. While this may at first glance seem like a "business" or "IT" problem, it quickly becomes a legal one when a subpoena hits or a lawsuit is filed, triggering the need to issue a legal hold to preserve potentially relevant evidence. Without proper forethought and planning, the client's ability to find, preserve, and identify relevant evidence is severely hampered. In the best case, this means that the company must spend extra time and money finding the evidence it needs for the particular matter. In the worst case, under at least U.S. law, spoliation arguments and claims can follow,[1] leading to monetary sanctions, adverse inference instruction or (in the most egregious of cases) a default judgment.

Courts have repeatedly recognized the importance of preserving and disclosing evidence in discovery. Spoliation occurs not just when evidence is intentionally destroyed, but also when a party failed to take "reasonable" steps and ESI was completely lost that should have been preserved. When intent to deprive is proven, courts can impose the most draconian sanctions, including an adverse inference.[2]

Locating and preserving what is potentially important is only step one in the road to defensible practices. The foregoing thoughts are often relied upon as a crutch by organizations to "save everything, forever," just in case it is needed in a future matter or to avoid any of the adverse effects of spoliation. Rule 26's proportionality standards, to the contrary, direct attorneys to weigh what is relevant in proportion to the cost and expense in reviewing and producing that information.[3] As The Sedona Conference emphasized in its *Commentary on Proportionality in Electronic Discovery (Commentary)*, the scope of discovery is not unlimited.[4]

---

[1] *See Victor Stanley, Inc. v. Creative Pipe, Inc.*, 269 F.R.D. 497 (D. Md. 2010) (noting the importance of Rule 26 proportionality, but imposing strict sanctions for spoliation, to include up to two years in prison, due to the severity of discovery violations).

[2] *See, e.g., Federal Rules of Civil Procedure, Rule 37(e); Alabama Aircraft Industries v. Boeing*, 319 F.R.D. 730 (N.D. Ala. March 9, 2017, *request for interlocutory appeal denied*, 2017 WL 4572484, *15 (N.D. Ala. April 3, 2017) (granting adverse inference where ESI was "intentionally destroyed by an affirmative active which has not been credibly explained.)

[3] *See, e.g., Mach. Sols., Inc. v. Doosan Infracore Am. Corp*., Civil Action No. 3:15-cv-03447-JMC, 2017 U.S. Dist. LEXIS 225277 (D.S.C. May 26, 2017) (analyzing Rule 26's proportionality factors as applied to a number of discovery requests after plaintiffs filed a motion to compel); *D.J.'s Diamond Imps., LLC v. Brown*, No. WMN-11-2027, 2013 U.S. Dist. LEXIS 46730 (D. Md. Apr. 1, 2013) ("Before ordering a party to respond to a discovery request, Rule 26(b)(2)(C) requires the Court to engage in a proportionality analysis and to limit the frequency or extent of discovery otherwise allowed by [the] rules.").

[4] The Sedona Conference, Commentary on Proportionality in Electronic Discovery, 18 Sedona Conf. J. 141 (2017) (hereinafter "The Sedona Commentary").

Once key data sources are collected, attorneys can better serve their clients if they understand the evidence that often lies beneath the surface.

In addition to helping organizations find and collect relevant ESI, thereby serving the dual purpose of avoiding spoliation and meeting discovery obligations, digital forensics can also be used effectively as a "sword" by legal counsel. Depending on the data source, forensics can be used to uncover the "data behind the data." From smartphone forensic images, deleted texts, internet search inquiries, photos, videos, and notes can be recovered. PC forensic images, the user's internet history, document and folder access activity, deletion activity, the use of USB devices, and the use of cloud data sources also can be extracted. These are just a few examples of how attorneys can use forensics to create critical timelines that aid in the prosecution and defense of various types of claims.

Special care should also be taken with how ESI is collected and preserved. Utilizing forensically sound collection techniques can often be used to satisfy the authentication standards under U.S. federal and state rules. Indeed, under F.R.E. 902, ESI collected using forensically sound means can be self-authenticated at trial, obviating the need to call a live witness to testify to authenticity.

With the foregoing as a framework, this paper discusses what digital forensics is (and is not), how the discipline can be broadly applied across various practice areas, and what are the key evidence sources that often lie beneath the surface. We then explain a practical application of digital forensics, and conclude with some tips on how attorneys can ensure that the evidence that is collected is done so in a way that supports admissibility and authenticity at trial.

II. Digital Forensics: What It Is, and What It Is Not

A. Setting the Stage: Digital forensics is the process of identifying, preserving, examining, and documenting digital evidence to be used for legal proceedings.

1. Investigative in nature: includes the analysis of the data (often the most important aspect of forensics). Many practitioners equate forensics with data collection. That perspective is overly narrow and discounts the true value of the discipline.

2. Working with a client's legal team, the forensic experts can help identify what data stores are likely to contain relevant information, advise on the most defensible means to preserve that data, and execute steps to collect that data in ways that retains the most important characteristics of the data sources.

a. Metadata: "Information about information." For a Word file, for example, the metadata will tell you when that document was created, modified, last opened, deleted, or moved.

b. Metadata will also show you how a user interacted with a device or account; it will show you information that is not accessible to the user in the normal course of using the device or account.

3. Forensics is not the same as eDiscovery. While eDiscovery review may follow a forensic review, eDiscovery focuses on finding patterns and key terms/concepts in essentially user-documents (emails, Word documents, Excel, PowerPoint, text messages, and the like). Forensics goes to a deeper level and has a different focus: what can the data tell me about how a user interacted with a file, system, or device?

III. Digital Forensics: Broad Application and Use Cases

A. Practitioners may think that forensics is reserved for criminal matters as it has been popularized in the "CSI" tv show. Not so. The discipline has a wide scope and can be used in multiple civil contexts.

B. Use Cases

1. Employee Unexpectedly Leaves Amid a Critical Project

2. Employee Tenders Resignation, Wants Out of Non-Compete

3. Class Action Litigation

4. Harassment Investigation/Claims

5. Subpoenas/"Dawn Raids" – Limited Response Time

IV. What is a Data Map and Why Is It Important?

A. **Definition:** In the context of the EDRM workflow, a case-specific data map is designed to help an organization identify where corporate records reside, who has access to those systems, how the information is tracked, and ideally how records can be disposed of when their useful life expires.[5] While this topic may seem to be mainly in the purview of IT experts or perhaps the business unit to which the data sets most frequently apply, attorneys would be well-served to work with their clients to understand the locations and types of data potentially relevant to the matters under their purview.

1. There is no magic to the process. The process involves interviewing key record owners, and bringing together core functions such as IT, legal and the impacted business units.

2. Common frameworks: who owns, uses, or views the data; does it contain special or proprietary information requiring additional protection?

[5] Data Mapping, Records and Privacy: Know and Manage Your Information, M. Dederer and M. Sherwin (ARMA Floridan Sunshine Conference) (Feb. 21, 2020)

3. Metadata can also be a helpful indicator when assessing privilege in certain jurisdictions.

V. Common Evidence Sources and How to Collect from Them

A. Once a need to preserve and collect data arises, counsel needs to understand the contours of the demand and whether or not full forensic collections are required. If so, lawyers should keep in mind the common evidence sources discussed below.

B. EU Data Privacy:

1. The basic ideas of EU Data Privacy regulation may be described as follows: To preserve and collect data, the legitimate interests of the corporation doing so must in essence outweigh the privacy rights and freedoms of the data subject, taking into consideration the reasonable expectations of data subjects based on their relationship with the corporation. The latter will typically limit the sources of evidence.[6]

   Key considerations when balancing the different interests may be (among others):

   a. If the investigation is necessary for legal proceedings (including prospective legal proceedings), or to establish, exercise or defend legal rights and obligations,[7] the corporation's interests often qualify as "legitimate" and outweighs data privacy concerns (so long as the investigation is carried out in a reasonable and proportionate manner) – i.e. any interference to any individual's privacy may be justified in light of the seriousness of the matters being investigated, information generated by the investigation is kept secure and, to the extent possible, only used for the purpose of that investigation. Each case requires an individual assessment which should be documented.

   b. If the company carries out an investigation to comply with a mandatory request by an EU/EEA authority "legitimate interest" in favor of processing data is per se assumed (so long as the investigation is being carried out in a reasonable and proportionate manner).[8]

[6] Against that background, it is advisable for corporations to prohibit private use of company devices.
[7] Corporate law in Germany as well as in many other European countries requires the management of a company to establish and maintain an adequate compliance management system. As part of this, the company management is required to get to the bottom of compliance deficits and violations. Failure to conduct an adequate investigation can result in civil liability *vis-a-vis* the corporation, or criminal liability.
[8] It is to be noted that this assumption does not apply, if the regulatory request comes from the US or another non-EU/EEA member state, but a fully-fledged balance-of-interests-analysis must be conducted which eventually may

2. Data protection rules impose restrictions on the transfer of personal data outside of the EU/EAA.

   a. Transfers to countries which are recognized by the European Commission as having an adequate level of data protection (i.e. adequacy decision,[9] e.g. Switzerland, Argentina, Canada to name a few) is not problematic and may happen without further restrictions.

   b. For any other transfers outside the above-mentioned regions further requirements[10] need to be fulfilled. This is relevant for both transfers within a group of companies and transfers outside of a group of companies to third parties (e.g. service providers, public authorities etc.), as no so-called "corporate privilege" exists.

C. **Personal Computers:** a catch-all term for information that is stored electronically, regardless of the media or whether it is in the original format in which it was created, as opposed to stored on paper.

1. Forensic tools can recover metadata unknown to the user

   a. Deleted content: "unallocated" space is where data deleted by the user resides until it is overwritten by other data sources. Once it is overwritten, it is truly gone. But some form of deleted content is often available through the use of forensic tools. User-generated documents (Word, PDF, Excel), web searches and webmail are a few examples of deleted content that can often be recovered.

   b. File(s) accessed: Each time the PC's user opens or interacts with files and folders, the computer's operating system tracks metadata associated with that action. Depending on the context of your investigation or matter, this activity could be critical.

   c. Internet search history: artifacts indicating access to personal email accounts, cloud storage or file sharing platforms are often recoverable.

   d. Whether external storage devices were connected: the insertion of USB devices is often tracked. Some limitations exist (Windows 10,

lead to a conflict of laws as under European Data Privacy Law the interest of the data subject in their personal data not being transferred to a country where the level of data protection is not considered to be adequate will regularly prevail.

[9] Adequacy decisions | European Commission (europa.eu)

[10] A detailed analysis is required taking into account conclusion of standard contractual clauses, the overall level of protection in the country which is the target of the data transfer and so called "supplementary measures" to safeguard the data transfer (e.g. encryption or pseudonymization with the key not being accessible by the recipient of the data); see The CJEU Judgement in the Schrems II Case (europa.eu).

for example, only logs USB insertion activity for approximately 30 days)

2. The PC model may dictate how an image can be created. For example, most Windows devices can be collected through remote means, while Apple computers need to be in the analysts' hands in order for a collection to be completed.

D. **Company-Issued Mobile Devices**:

1. Company-issued mobile devices often have a mobile device management tool ("MDM") installed

   a. MDM restricts backups/collections without the help of IT.

   b. MDM policy may need to be changed to effect a collection.

   c. MDM app may need to be removed to effect a collection.

2. Key takeaway: MDM does not help with data collection from mobile devices.

E. **Personal Mobile Devices**

1. iPhones

   a. Generally easier to collect with some remote options.

   b. iCloud backup (user can create a recent iCloud backup; analyst can then log in remotely to the account and collect the account remotely).

   c. iTunes backup (user can backup his or her device to the iTunes account on a PC, which can then be copied over to a drive using forensic tools).

2. Androids: pretty much always require knowledge of forensic specialist/device in-hand

3. Aside from the logistical requirements of collecting mobile devices, attorneys should be mindful of whether requesting an adversary's personal mobile devices is proportional to the needs of the case under Federal Rule 26. (*Henson v. Turn, Inc.*, 2018 WL 5281629 (N.D. Cal. Oct. 22, 2018) (denying defendant's request for production of plaintiffs' personal smartphones because a full production of the devices would disclose a substantial amount of private data that would be disproportionate to the discovery needs of the case at hand).

F. **Cloud Storage**

1. Cloud storage may be prohibited by policy, but not technically blocked. As a result, these sources can be untracked, unknown, and unmanaged.

2. Collection steps: dictated by the storage application in question.

3. Business-class cloud storage have additional logging available, to address topics such as sharing of data with third parties.

4. Extremely large volumes (100s of GB) could take weeks to collect, so be aware when planning and negotiating deadlines

G. **Corporate/Shared Networks**

1. Often considered "systems of record"

   a. Centrally located and controlled

   b. Secure (settings will often depend on the type of data in the system and whether it contains personal or sensitive information)

   c. Not tied to an individual (an Outlook email account will never be a system of record)

2. Ask the client!

   a. How networks are structured

   b. Who has network access, and how is access controlled

   c. Whether any automated deletion cycles apply (if so, they need to be disabled, or data must be collected, in the event of a legal hold)

H. **External Storage Devices**

1. Employees may be relying on external storage due to convenience or inability to connect to the company's network storage

2. In a remote-imaging situation, the devices may be able to be plugged into the computer being collected (case specific – not a good idea for a defense case involving trade secrets theft)

I. Social Media

1. Slack[11], WhatsApp, Facebook, Instagram, LinkedIn, etc., are commonly used by employees for both sharing work and basic communications

2. eDiscovery "purpose built" tools do exist for most of the popular platforms. Note, however, that as developers frequently change the website's Application Planning Interface, the tools designed to capture web content sometime lag behind these updates. This means that social media and web captures aren't always clean or able to fully capture the desired scope. Furthermore, privacy settings might impede in the collection of certain social media components.

    a. Onna for Slack

    b. WebPreserver and X1 Social Discovery for FB, IG, and LinkedIn, Twitter

3. Certain tools also have built in tools for the extraction and retrieval of materials. Properly framed requests for production can be used to solicit the producing party to use these tools to extract these materials in a forensically defensible way from platforms like WhatsApp, LinkedIn, Google Enterprise, etc.

4. In certain jurisdictions, social media proliferation may also be addressed by the application of proportionality standards.

    Instead of seeking to identify and preserve every possible relevant message or post from a client's social media accounts, lawyers should do as the Sedona Commentary suggests and "focus on the needs of the case." This means conferring with litigation opponents to more readily ensure that relevant social media content is "obtained from the most convenient, least burdensome, and least expensive sources." By cooperatively seeking to isolate high-value content from marginally relevant information, counsel can help alleviate preservation and production burdens associated with social media.

5. Another preservation issue rests with the dynamic nature of most social media content. This is particularly the case with social messaging applications (like Slack, WhatsApp and Snapchat) whose content may be modified or destroyed shortly after being sent or received.

[11] James A. Sherer, Aaron Singer & Ben Barnes, *Picking Up the Slack™ Legal and Information Governance Considerations for New(er) Technologies*, 25 RICH. J.L. & TECH., no. 4, 2019 (discussing how disruptive technologies are utilized within existing legal, regulatory, and ethical frameworks, using Slack as a case study).

J. **Internet of Things**

1. IoT devices are not only the future; they are very much the present.

   a. IoT devices include wireless sensors, software, actuators, computer devices and more. They are attached to a particular object that operates through the internet, enabling the transfer of data among objects or people automatically without human intervention.

   b. Smart home devices: Everything from Amazon Echo and Alexa, to the Nest Thermostat and other connected appliances such as thermostats, lights, security systems, door locks, refrigerators, door bells, and swimming pools are potential sources of data.

   c. Wearables: The Apple Watch and other smartwatches have turned our wrists into smartphone holsters by enabling text messaging, phone calls, and more. And devices such as Fitbit and Jawbone have helped revolutionize the fitness world by giving people more data about their workouts.

   d. Connected Cars: Vehicles can be equipped with Internet access and can share that access with others, just like connecting to a wireless network in a home or office. AT&T – Connected Car: AT&T was the first telecom company to open a connected car research and innovation center.

   e. Corporate Environments: Location information and door badging data can be prevalent on certain company campuses. Knowing the retention periods of these data types can be crucial when gathering evidence.

   f. Data from devices connected to devices has exploded over the past several years and now dwarfs the volume of human communication over the internet. It is estimated that in 2019, IoT data volume represented 99% of all internet traffic (13,600 EB (exabytes)[12] vs. 167 EB of consumer traffic).[13]

2. IoT Is Changing The Landscape Of Discovery?

   a. Attorneys have an ethical obligation to gain a foundational knowledge of what relevant data is available and how it can be

[12] Data volume of internet of things (IoT) connections worldwide in 2019 and 2025," Statista website, 26 October 2020; How the internet of things is driving a new era of e-discovery," Scott Bilbrey, Ernst & Young LLP Forensic & Integrity Services Managing Director, Feb 3, 2021.
[13] Global data volume of consumer IP traffic 2017-2022," Statista website, 28 February 2020.

collected, analyzed and applied in litigation. To meet this obligation, attorneys, with assistance from litigation support and IT professionals, need to make sure they are informed on IoT data and systems so that they can ask the right questions and prioritize the right issues.

b. No longer is it sufficient to consider only human communications and human-generated data. With IoT forensics the first thing to do is to identify the available sources of evidence. The lawyer must establish which devices recorded relevant data. The question that needs to be answered is how IoT interacts with its surroundings. The lawyer can then know which of the possible available sources to use. Before collecting evidence, constraints to data collection (physical, proprietary standards, legal) should be checked.

c. IoT forensics is different from and can be more challenging than traditional digital forensics. Data extraction is made difficult by the limited capabilities of devices, their various interfaces, and their storage formats. While some IoT devices may have permanent storage with familiar file systems and file formats, others might use proprietary file systems and formats. Other devices might not even have permanent memory that holds user data or have limited amount of RAM and transfer all their data immediately. Some may have a limited power supply that severely limits duration or even prevents live forensics. IoT data can be encrypted and is often processed in the cloud located in an unknown location that can be on the other side of the planet.

d. There is a lack of a methodology and framework for IoT forensics. Even in digital forensics there is no single universally accepted methodology, but there are a few that are recognized and used by practitioners and researchers. IoT forensics is still in its infancy and relies on methodologies and frameworks from standard digital forensics that might not be fully adequate. There is a lack of appropriate tools for IoT forensics.

e. Notwithstanding its challenges, IoT brings new sources of evidence to general forensics. IoT records events from the physical environment, which were not recorded and stored before. IoT systems can contain contextual evidence collected without the individual who committed a crime or relevant act being aware. This all happens automatically, without any user interaction as a side effect of the IoT operation.

f. IoT evidence is also harder to destroy. It usually is not just one piece of evidence and it is generally stored in the cloud out of the

reach of people who may want to delete it. Usually suspects are not even aware of the evidence being collected.

g. IoT offers more evidence sources than standard digital forensics. A composite picture of events can be constructed from all the data collected from the IoT systems. For example, the location of a suspect at a particular time can be established by correlating data from different IoT devices from various locations the suspect frequents. Wearable activity monitors can also help identify the approximate location of the suspect.

VI. Typical Forensic Scenario

A. Sam Smith – Lead Scientist at Superior Science

1. Background: Developing key treatment for blockbuster drug. Unhappy with his year-end bonus. Goes on an unplanned vacation, resigns 6 days later, and the company learns shortly thereafter that Smith is now working for a competitor.

2. Digital Forensics – Finding the Truth in Data

B. Key Resources

1. Sam's company-issued PC

   a. Document access

   b. USB device insertion

   c. Use/deletion of webmail

   d. Metadata on Sam's Resume

   e. Sam's iPhone backup

VII. How Do I Ensure I Get Evidence Before a Jury/Decision Makers

A. Admissibility Under US Law: Hearsay Exceptions and Authentication

1. The Basics: ESI is Still "Traditional" in Many Aspects

2. Must Be Relevant (F.R.E. 402)

3. Must Satisfy Original Writing Rule, or Exception (F.R.E. 402)

4. Must Not Be Hearsay or Be Subject to Hearsay Exception (F.R.E. 801/803)

5. Must Not Be Prohibited Under F.R.E. 403

B. Authentication Is Still Required (F.R.E. 901-02)

1. Common Methods of Traditional Authentication Under F.R.E. 901

a. (b)(1): witness with personal knowledge (internal IT delegate)

b. (b)(3): comparison by an expert witness (retained expert)

c. (b)(9): evidence describing a process/system and showing that it produces an accurate result

2. Why Is Authentication So Important?

a. Hash Value: An identifier assigned to a file based on an algorithm (a value so distinctive that the chance of any 2 data sets sharing the same HV are < 1 in a billion)

3. Authentication Under F.R.E. 902(13)

a. Covers certified records generated by an electronic process or system

b. Must have a "qualified person" create a full forensic image of the device

c. Don't wait. Image the device ASAP and put it "on the shelf" for evidence if needed (Risk: waiting for formal discovery to commence, or worse, trial preparation)

d. Keep a copy of the Chain of Custody records (common subject of cross-examination)

4. Self Authentication –F.R.E. 902(14)

a. Certified Data Copied from an Electronic Device, Storage Medium, or File. Data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person ….

b. Certification by a qualified person allows the ESI to be "self-authenticating" without need of further testimony.

c. Notice must be given to the opposing side: if no objection or challenge, the evidence becomes self-authenticating at trial (no need for a live witness)

d. Be sure to work with forensic experts to prevent or eliminate

pretrial challenges.

C. Authentication and Admission of Common Evidence Types

1. Email: Application of Traditional Rules to Leniency

a. Most Common Methods: F.R.E. 901(b)(1) (witness with personal knowledge); F.R.E. 902(11), (12) (business records); F.R.E. 801(d)(2) (statement by party opponent)

b. Key Authentication Factors

i. Circumstantial Evidence: sender's known address; e-signature; similar use of email in other contexts

ii. Forensic info: hash value (think "Bates" number); expert forensic testimony

2. Web Pages

a. Point of Contention: sites are dynamic, so establishing authenticity of historic site info can be challenging

b. IP Addresses: often subpoenaed to identify source of hacker; in some states, must be offered by qualified forensic expert & meet rules 901/803 (regular business activity)

c. "Wayback Machine": Internet Archive stores all websites/can retrieve info from a particular time (expert testimony may still be needed, while some courts take judicial notice; www.archive.org)

3. Text Messages

a. Witness with personal knowledge (conclusive proof not required)

b. Circumstantial Proof:

i. author's ownership/possession of the sending device

ii. author's known phone number

iii. use of phone number on other occasions common use of phrasing/emojis

iv. author acts in accordance with the text

4. Social Media/Internet Chatrooms

a. Authentication can be challenging given that account owners often

use pseudonyms rather than their actual names, and the fact that various parties have access to and can modify information in such environments

b. Circumstantial evidence

i. Testimony from witness(es) who interacted with author on other occasions

ii. Testimony from participant(s) in the subject conversation

iii. Use of screen name by author on other occasions

D. **Using Evidence at EU Proceedings:** Using evidence is not covered by a harmonized EU regulation. In fact, laws regarding the use of evidence differ from country to country and therefore provide a high level of complexity. While some countries provide for a holistic legal framework, in major countries like Germany there is a lack of codified regulations on the performance, legal effects, and admissibility of findings of internal investigations**.**