Beratung

Circumstantial evidence, the ugly duckling of eDiscovery

04. August 2022, von Gaïa Leblanc

Introduction

As eDiscovery usually focuses on user generated content (such as emails and documents), data related to a person's behavior (such as Internet searches and history, phone calls and locations) is often overlooked. While that type of data is at the core of a computer forensic investigation, eDiscovery tends to disregard it as an "ugly duckling".

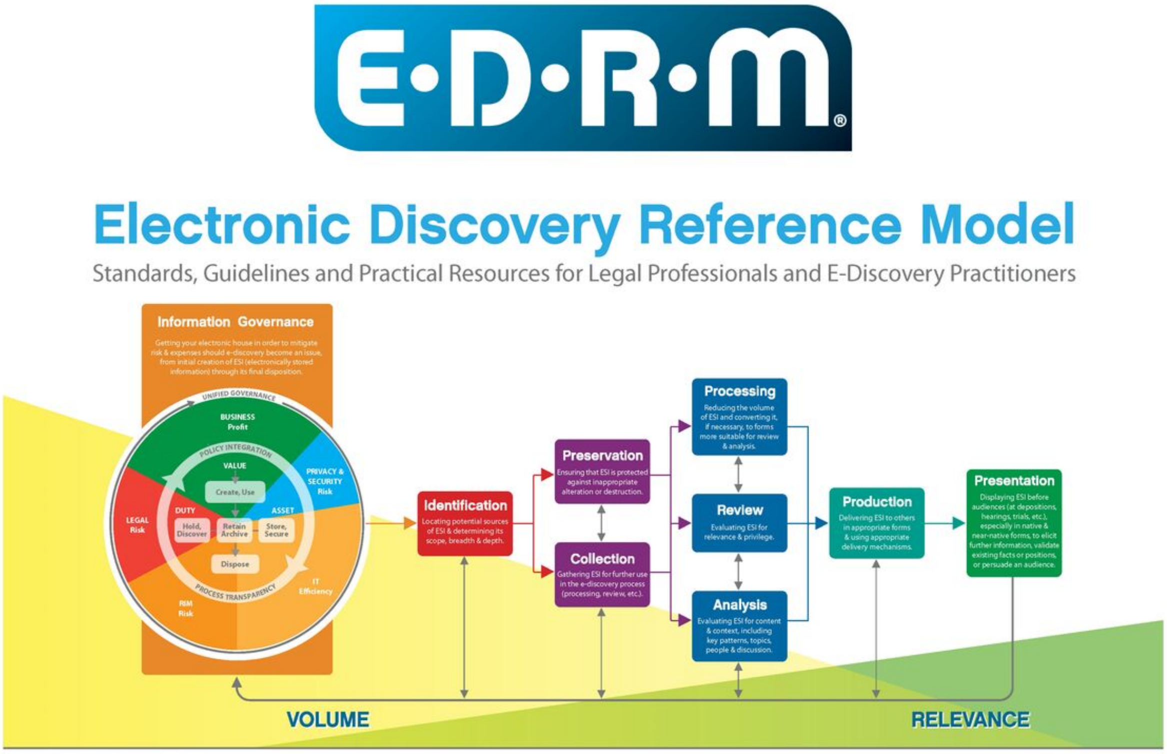
This article explores why and discusses tangible solutions to help legal teams leverage circumstantial electronic evidence in their investigations, which can prove remarkably useful.

The ugly duckling of eDiscovery

eDiscovery and forensic investigations

eDiscovery workflows typically include the collection, processing, review and production of emails and other easily human-readable files gathered from a custodian’s devices. Chat conversations are also getting the spotlight.

Legal teams will generally instruct technical staff to gather what they want to see, and proceed with a document review in a renowned software. This method sounds safe and familiar, but may only reveal the tip of the iceberg. We all know the devil is in the details.



E·D·R·M®

Electronic Discovery Reference Model

Standards, Guidelines and Practical Resources for Legal Professionals and E-Discovery Practitioners

Information Governance

Getting your electronic house in order to mitigate risk & expenses should e-discovery become an issue, from initial creation of ESI (electronically stored information) through its final disposition.

Identification

Locating potential sources of ESI & determining its scope, breadth & depth.

Preservation

Ensuring that ESI is protected against inappropriate alteration or destruction.

Collection

Gathering ESI for further use in the e-discovery process (processing, review, etc.).

Processing

Reducing the volume of ESI and converting it, if necessary, to forms more suitable for review & analysis.

Review

Evaluating ESI for relevance & privilege.

Analysis

Evaluating ESI for content & context, including key patterns, topics, people & discussion.

Production

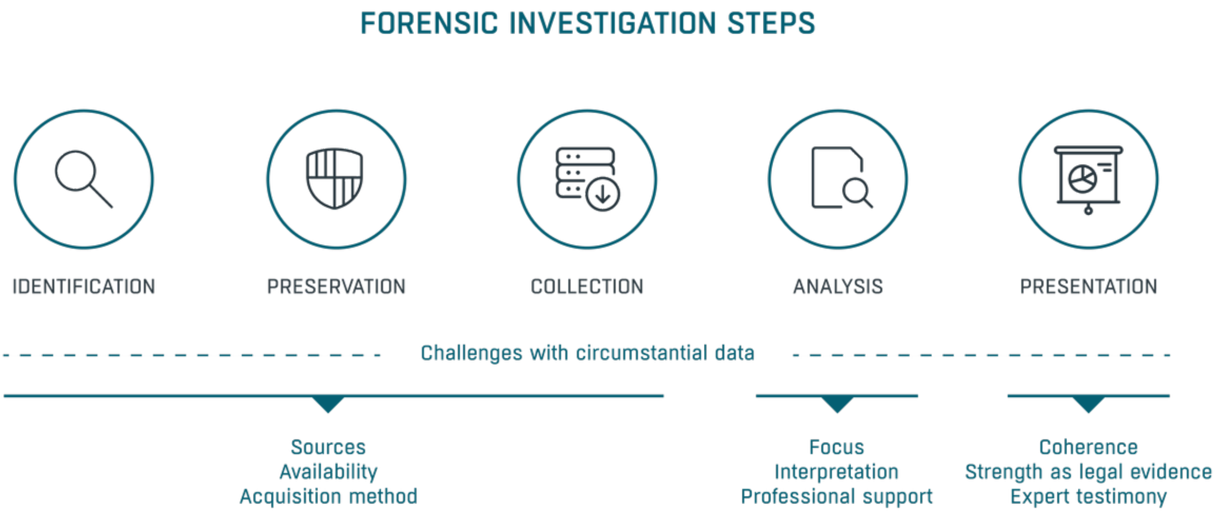
Delivering ESI to others in appropriate forms & using appropriate delivery mechanisms.

Presentation

Displaying ESI before audiences (at depositions, hearings, trials, etc.), especially in native & near-native forms, to elicit further information, validate existing facts or positions, or persuade an audience.

Download the EDRM poster directly from the EDRM Global Advisory Council website

On the other hand, forensic methods will find artefacts, traces of incidents and evidence on any digital device with the capability to store data. In general, trained professionals conduct the digital analysis using specialized software, and their rigorous techniques enable the resulting evidence to meet the legal standards. The normal steps share common ground with eDiscovery, they are the identification, preservation, collection, analysis and presentation of data.



Challenges with circumstantial data

What is out there?

The context surrounding the facts obviously matters in any litigation or investigation. For example, chat messages combined with - apparently harmless – deleted items, meetings and phone calls can completely change the perspective.

New data types and sources, such as data from the Internet of Things (IoT) and from personal apps, begin to make their way into the investigations. A vibrant example is the smartwatch FitBit data used to prove movements of suspects or victims in criminal cases, and relevant in health and product liability disputes. (i)

This type of data may seem difficult to grasp and identify. There is a mountain of data and metadata available in the world that surrounds us. Identifying what exists, knowing where it is stored and how to acquire it are the first challenges.

Effective and efficient analysis

One additional challenge is the time required for traditional forensics. A computer contains many little details where it is easy to get lost, and an analysis without the right focus or direction can be extremely time-consuming.

Some logistical issues such as software licensing, malware and hardware requirements may also influence the process. It is true that circumstantial data will probably appear messy and uneasy to read in a standard eDiscovery tool. Details and formats will not display well, and - of upmost importance - this data will almost certainly not be responsive to keyword searches or concept clustering. This data does not “speak” textually by itself. It requires analysis and interpretation to reveal its secrets.

Solid evidence

When it comes to producing such evidence at Court, it induces further challenges. Facts are straight forward, but interpretation of traces and metadata are more debatable. Furthermore, a strict production format is often not appropriate for such data, and evidence traceability brings higher complexity.

For example, how can a system log prove that Mr. Defendant received the whistleblowing alert but deleted it? One must demonstrate why this becomes evidence with solid supporting data. The opposing party might challenge the assumptions. (ii) Explaining and simplifying technical concepts from computer science will probably be necessary when addressing the Judge, the arbitrators or the other participants in the case. The testimony of the expert who conducted the analysis might be required. (iii)

Dealing with circumstantial evidence may appear burdensome for legal teams and require external expert support. However, recognizing its potential and combining it with traditional eDiscovery can generate a lot of value. With the appropriate preparation, collaboration and tools, it can shed light on many litigious situations.

Make it a swan

Step by step

Legal teams can successfully manage and use circumstantial electronic evidence. It only requires recognizing it for what it is, i.e. **different** data, and therefore apply different techniques to it.

Like in many other fields, preparation is key. This means to put in place strong project management and methodologies. Clear communication channels, defined objectives and timelines, and carefully crafted iterative review phases will be helpful.

> “Preparation is key. This means to put in place strong project management and methodologies.”

One could start an eDiscovery project by working with easy data sources, like interviews and traditional review of emails, and then use the basic knowledge acquired to quick start the circumstantial analysis. With enough reference material, it is possible to dive deeper and look into events that are more precise, correlate people, leverage data analytics and dig into new data sources.

Get your expert involved

Field experience and appropriate tools will help link traditional eDiscovery with circumstantial digital evidence. A solid collaboration is a game changer to cross-reference the results. Legal teams can see their service provider as a robust ally when it comes to circumstantial data. Their skill set and knowledge will help identify, collect, prepare and review the right data in the right way.

Too often, legal teams tend to keep the service provider away from the facts at stake in the case. A more collaborative approach may provide better results. Asking questions to your experts, identifying with them potential gaps in the flow of information, discussing options about the usable types of data and merging technical and legal knowledge could really make your investigation bulletproof.

> “A more collaborative approach may provide better results.”

It might be efficient to use the eDiscovery results to formulate specific questions that the expert will attempt to answer with artefact analysis and other forensic approaches adding the expected value to the evidence available in the case.

Expert forensic practitioners can use specialized software to work on data that does not fit well in traditional eDiscovery platforms. They are capable of conducting the analysis and data interpretation required to bring this evidence to Court and they can testify.

Ask for it

Let’s also discuss solidifying the exchange and production protocols (especially in Europe compared to United States or Canada). They often request only very basic metadata and data sources. (iv) Still today, plain PDF productions are sometimes called for. These completely strip off the metadata and simply discard data types that are not printable, such as audio, heavy spreadsheets or database entries.

Slowly, a shift in the industry is happening. As an example, the Council of Europe issued guidelines about electronic evidence in 2019 mentioning: “**Courts should be aware of the probative value of metadata and of the potential consequences of not using it**”.(v)

> “Courts should be aware of the probative value of metadata and of the potential consequences of not using it.[v]”

The Sedona Conference - a well-known authority guiding the eDiscovery professionals - also issued relevant comments on the discovery of social media (vi) and ephemeral messaging (vii), and also points to weighty publications by its Technology Resource Panel members on wearable devices (viii) and the Internet of Things. (ix) It shows the way to data sources other than emails and chat messages.

The lawyers, the judicial system and the public become more aware of the existence and possibilities offered by data in multiple forms. This movement can be encouraged by specifically referring to new data types and sources, extensive metadata and native productions in agreements between parties. If circumstantial evidence can be relevant for your case, **ask for it**.

Conclusion

Just like in the Danish tale, the “ugly duckling” of eDiscovery can find its perfect place to shine. Circumstantial digital evidence simply needs to be treated with the appropriate methods and corresponding tools.

Review by contract lawyers of massive amounts of system logs or applying search terms on phone call data will not be effective, but working on this data with a forensic mindset and a more analytical approach can be a gold mine of new evidence.

Becoming comfortable with circumstantial evidence will strengthen the investigation results of legal teams. Skilled forensic examiners will help to cross-reference it with other known facts and legal teams can see their digital service providers as expert allies.

To learn more, read the article published by Rogier Teo, Swiss FTS CEO, about bridging the gap between unstructured and structured data in the GoingDigital Magazine: Careful planning and use of the right tools - Deutscher AnwaltSpiegel.

For more detailed information about our services in digital forensics, please contactIrène Wilson, Director at Swiss FTS.

info@swiss-fts.com | +41 43 266 78 50 (Zurich) | +41 21 510 53 80 (Lausanne)

Footnotes

(i) See for example: Jurors in 'Fitbit Murder' Trial Convict Man of Killing Wife | U.S. News® | US News; and Bartis v. Biomet, Inc., No. 4:13-CV-00657 (E.D. Mo. May 24, 2021).

(ii) For example, in HCC INS. HOLDINGS, INC. V. FLOWERS
(N.D. GA. JANUARY 30, 2017), a compelling US competition case, the typical movements of data (updating, copying, moving and deleting files) and the standard use of different software by the defendant were analyzed and compared, before and after the discovery order, to see if anything uncommon arose. The use of "cleaning" programs on the defendant's computer was also uncovered, as well as the use of external drives plugged into the company system by the defendant. However, it was not enough to prove "misappropriation" of trade secrets.

(iii) For example in this Canadian case, Droit de la famille — 211908, 2021 QCCS 4295 (CanLII), the Fitbit evidence submitted was expressly rejected because of the absence of an expert opinion on its reliability.

(iv) For some examples of how metadata can affect a case, read JAVO BEVERAGE CO., INC. v. CALIFORNIA EXTRACTION VENTURES, INC., Dist. Court, SD California 2020 about the importance of file paths, Lee v. TREES, INC., Dist. Court, D. Oregon 2017 where metadata was used to prove that text messages presented as evidence were in fact fabricated, and Lawrence v. City of New York, Dist. Court, SD New York 2018 where metadata was used to prove that some photographs were taken long after the relevant events, referenced in The Importance of Metadata in Digital Forensics and eDiscovery (forensicdiscovery.expert).

(v) Electronic Evidence in Civil and Administrative Proceedings, Guidelines, adopted by the Committee of Ministers of the Council of Europe on 30 January 2019, as proposed by the European Committee on Legal Co-operation (CDCJ, ISBN 978-92-871-8929-5).

(vi) The Sedona Conference, Sedona Canada Commentary on Discovery of Social Media, 23 SEDONA CONF. J. 79 (forthcoming 2022).

(vii) The Sedona Conference, Commentary on Ephemeral Messaging, 22 SEDONA CONF. J. 435 (2021).

(viii) Your Employee May Be Wearing His Alibi—Or Your Evidence, Warren G. Kruse II, Consilio, April 2020.

(ix) The Internet of All Things: Collecting the Right Data For Your Case by Warren Kruse, Paul McVoy and Kevin Chang (February, 2017).

Gaïa Leblanc

Gaïa Leblanc is eDiscovery Project Manager at Swiss FTS. She previously worked as a lawyer at a leading global firm in business law and as eDiscovery Consultant for an engineering firm where she developed experience with complex eDiscovery matters.

Swiss FTS AG | www.swiss-fts.com | +41 43 266 78 50 | info@swiss-fts.com

https://swiss-fts.com/blog/circumstantial-evidence-the-ugly-duckling-of-ediscovery