Lawyer's Guide to Understand Computer Forensics and Best Practices for Engaging and Working with Digital Forensic Experts

Speakers:

Yoav Griver, Partner, Zeichner Ellman & Krause LLP

Mathea Bulander, Partner, Redgrave LLP

Brian Dykstra, President & CEO, Atlanta Data Forensics

Disclaimer

- This is not legal advice nor should it be considered legal advice.
- This presentation and the comments contained therein represent only the personal views of the participants, and do not reflect those of their employers or clients.
- This presentation is offered for educational and informational uses only.

(c) 2021 Lexeprint Inc. All Rights Reserved.

Speakers



Yoav Griver
Partner
Zeichner Ellman & Krause LLP



Mathea Bulander
Partner
Redgrave LLP



Brian Dykstra
President & CEO
Atlanta Data Forensics

(c) 2021 Lexeprint Inc. All Rights Reserved.

Agenda

- Overview of Digital Forensics
- 5 Stages of Digital Forensics
- Digital Forensics Report
- Evaluation of a Forensics Report
- Considerations for a good Digital Forensics Report
- Rules of Evidence
- Tips for every Attorney when collecting electronic evidence

(c) 2021 Lexeprint Inc. All Rights Reserved.



Overview of Digital Forensics

(c) 2021 Lexeprint Inc. All Rights Reserved.



What is Digital Forensics?

- Digital Forensics can be defined as the detailed investigatory examination of digital media to uncover electronic evidence that supports or refutes a hypothesis.
- It follows processes and procedures that ensure that digital evidence collected during an investigation will remain credible with integrity for use in possible legal proceedings.
- Digital Forensics narrates the story of digital information.

(c) 2021 Lexeprint Inc. All Rights Reserved.



What is Digital Forensics?

- Expert digital forensics can help you win your cases.
  - They can 'help to prove that the defendant had knowledge of a document or that data was transferred to a third-party.'
- They can usually answer the following questions:
  - How did a file get there?
  - Who had control over that file?
  - Where was it transferred?

(c) 2021 Lexeprint Inc. All Rights Reserved.



Cardinal Rules of Evidence Handling

- ✓ Only use tools and methods that have been tested and evaluated to validate their accuracy, repeatability and reliability
- ✓ Handle the original physical evidence as little as possible to avoid inadvertently modifying the original data
- ✓ Establish and maintain a defensible chain of custody – include pictures
- ✓ Document everything done – it didn't happen if it's not in your notes
- ✓ Never exceed the limits of your personal knowledge – ask for help

(c) 2021 Lexeprint Inc. All Rights Reserved.

Forensics Investigation Methods

Methods used by investigators must achieve these objectives:

- Protect digital evidence from alteration
- Discover all responsive files
- Recover deleted files & hidden files
- Create timelines & “searchable” terms
- Access protected or encrypted files
- Use steganalysis to identify hidden data
- Document their work so others can independently reproduce findings made
- Comply with all privacy regulations
- Analyze data in unallocated and slack space
- Have a chain of custody process that will survive a no-nonsense audit
- Whenever possible, use write-blockers when acquiring evidence
- Follow a forensic protocol when analyzing evidence
- Provide expert testimony or consultation

(c) 2021 Lexeprint Inc. All Rights Reserved.

Chain of Custody Procedures

Handling of e-evidence must follow the *three C's of evidence*: care, control, and chain of custody

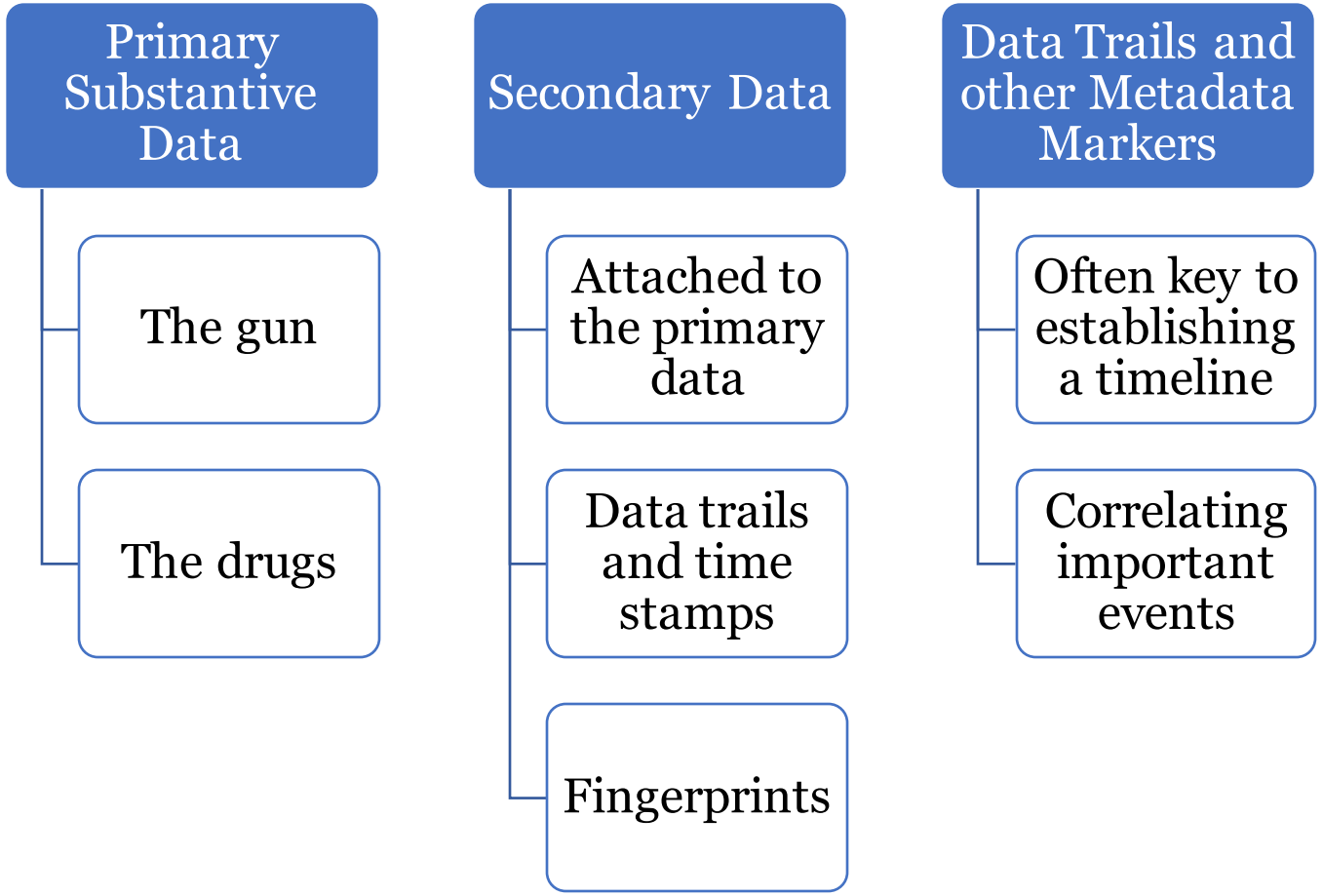
Chain of Custody Procedures:

- Keep an evidence log that shows:
  - Who identified the location of the physical evidence? How was it acquired? Was it a live or static acquisition?
  - Who acquired the evidence? When was it acquired? What form of labeling was used to identify the evidence?
  - What are the technical details of the source of the evidence? (make, model, mfg., serial number, capacity, etc.)
  - What is the MD5 hash value of the digital evidence acquired?
  - Who was authorized to surrender it for analysis? Does the forensic evidence contain data protected by privacy regs?
  - Record dates of when items are released to anyone and when they are returned
- Restrict access to evidence using 24x7 monitored security system
- Place original hard drive in an evidence locker – protect from fire, water and theft
- Perform all forensics on an exact duplicate image, never on the original data

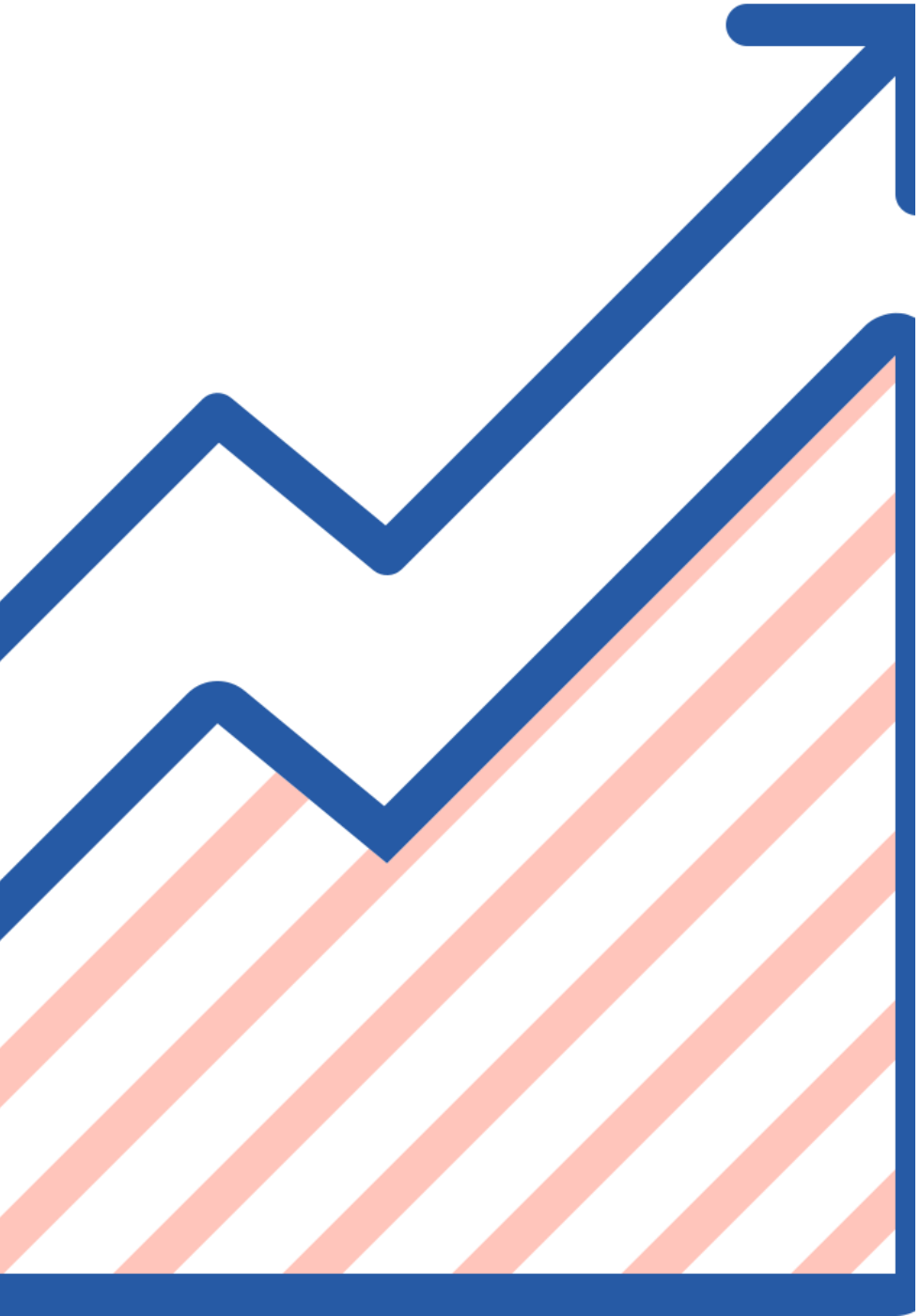
(c) 2021 Lexeprint Inc. All Rights Reserved.

What Goes into a Forensic Investigation?

Digital Forensics in a Traditional Forensics Context



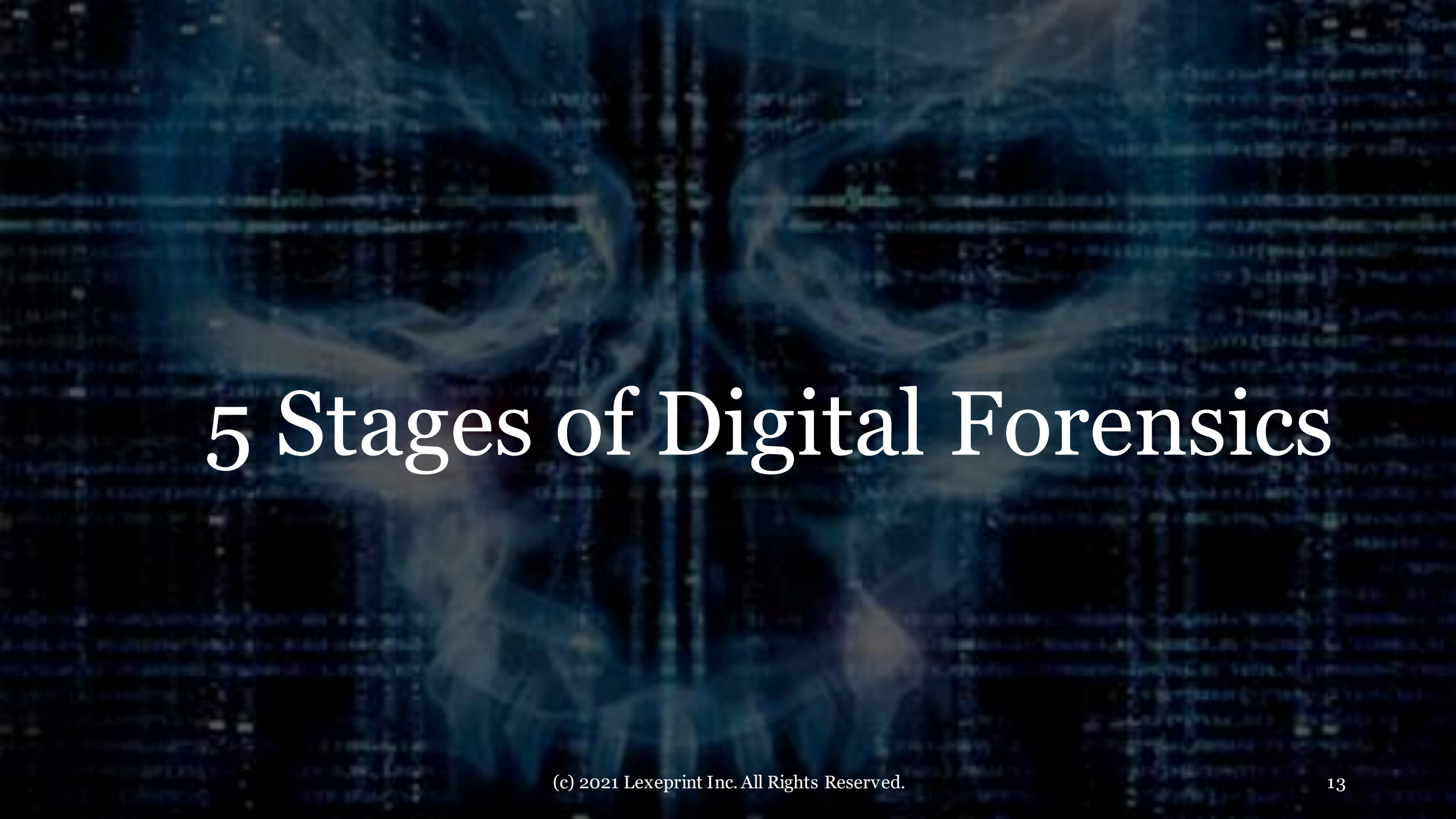
(c) 2021 Lexeprint Inc. All Rights Reserved.



Trends that Shaped Digital Forensics in 2020

- Smart phones
- Ephemeral Apps – such as Snapchat
- Internet of Things (IoT) - the ecosystem of digital devices that connect to the Internet
- SSDs
- TAR/AI/Machine Learning
- Cloud Forensics

(c) 2021 Lexeprint Inc. All Rights Reserved.



5 Stages of Digital Forensics

(c) 2021 Lexeprint Inc. All Rights Reserved.



I. Assessment/Identification of Evidence

- Attorneys are encouraged to bring a digital forensics professional onboard their team when civil disputes turn litigious. Ahead of any data collection, digital forensics professionals will need to assess the situation and develop a strategy for a forensic investigation.
- Digital forensics can provide you with a very helpful guide to the data that will be most critical to your case. This will allow you to form a plan that allows you to retrieve the information you need while lowering the overall cost of collection.
- It will be crucial for the investigator to define what they are looking for and how they intend to collect the data as you will need to ensure that it is consistent with the Federal Rules of Civil Procedure (FRCP).

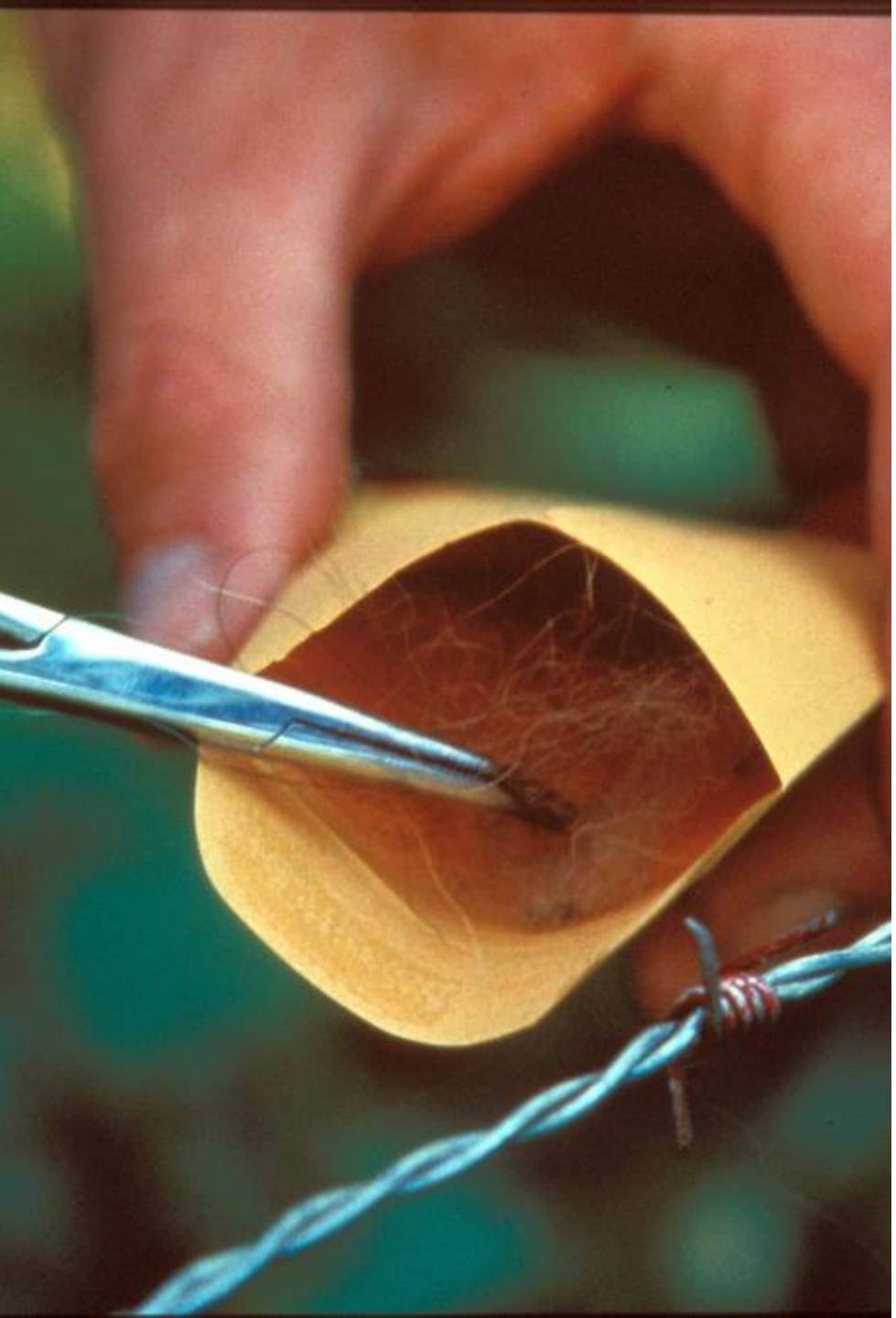
(c) 2021 Lexeprint Inc. All Rights Reserved.



I. Assessment/Identification of Evidence

- Example of a scenario where assessment of evidence by a digital forensics' investigator is crucial:
  - You are asked to investigate a case where an employee is suspected of stealing intellectual property from an employer.
  - It will be essential to identify potential sources of information – such as pen drives, email, messaging apps, social media accounts, cell phones, or cloud-based storage. A competent digital forensics professional will be able to assess the effort that is required to examine a broad assortment of digital archives and construct a plan that can obtain that information.
  - Furthermore, they can guide efforts to draft a discover request or response to one.

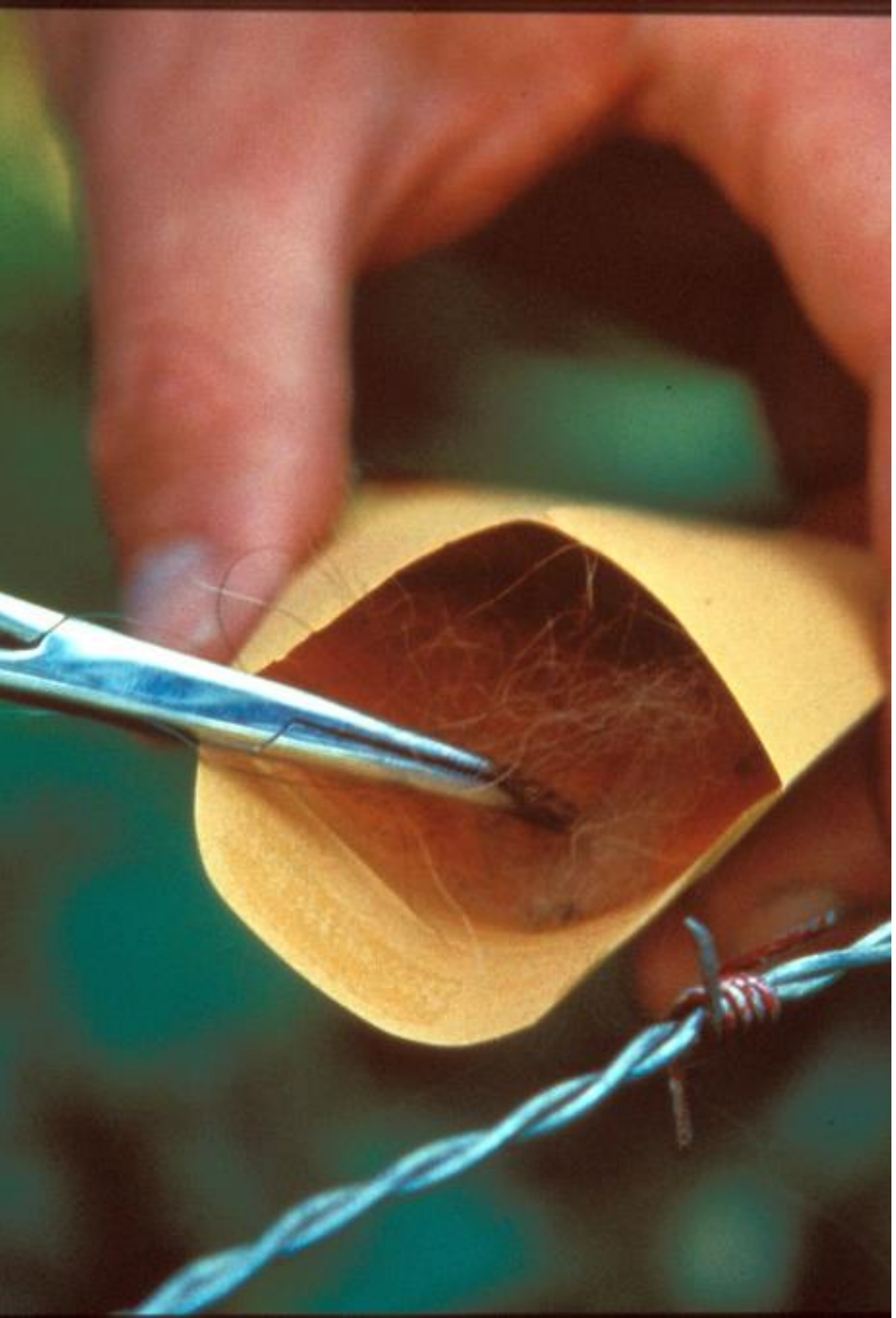
(c) 2021 Lexeprint Inc. All Rights Reserved.



II. Collection of Evidence

- The source media needs to be copied in a way that preserves the integrity of the original before any examination can take place. If this is not done properly, the integrity of an investigation can be damaged. [1]
- This can be achieved by making a **forensic copy.** A forensic copy is an 'exact bit-for-bit copy of the entire physical hard drive.'

(c) 2021 Lexeprint Inc. All Rights Reserved.



II. Collection of Evidence

- **Update to the law:**
- Recent Amendment to **US Federal Rule of Evidence 902**:
  - This recent amendment 'establishes that preserved electronic data should be self-authenticating.' This is what creating a forensic copy accomplishes.
  - The rule stipulates that properly certified electronic data will carry with it a strong presumption of authenticity. This is due to the fact the forensics copy is verified to be identical to the original and it is protected against future alteration.
  - It is widely considered as a more reliable source of truth than the original media as it can be inadvertently altered.

(c) 2021 Lexeprint Inc. All Rights Reserved.



III. Examination of Evidence

- The aim of examination is to extract relevant data from the digital haystack of information to prepare it for in-depth analysis, which is the next stage in digital forensics.
- You can expect your investigator to do the following:
  - recover deleted information;
  - parse containers such as mailboxes, computer backups, phone backups, and compressed archives;
  - retrieve artifacts such as web browser history and web searches;
  - identify the history of opened files and connected storage devices;
  - accurately identify file types; and
  - cull unnecessary files such as duplicate and system/application files."

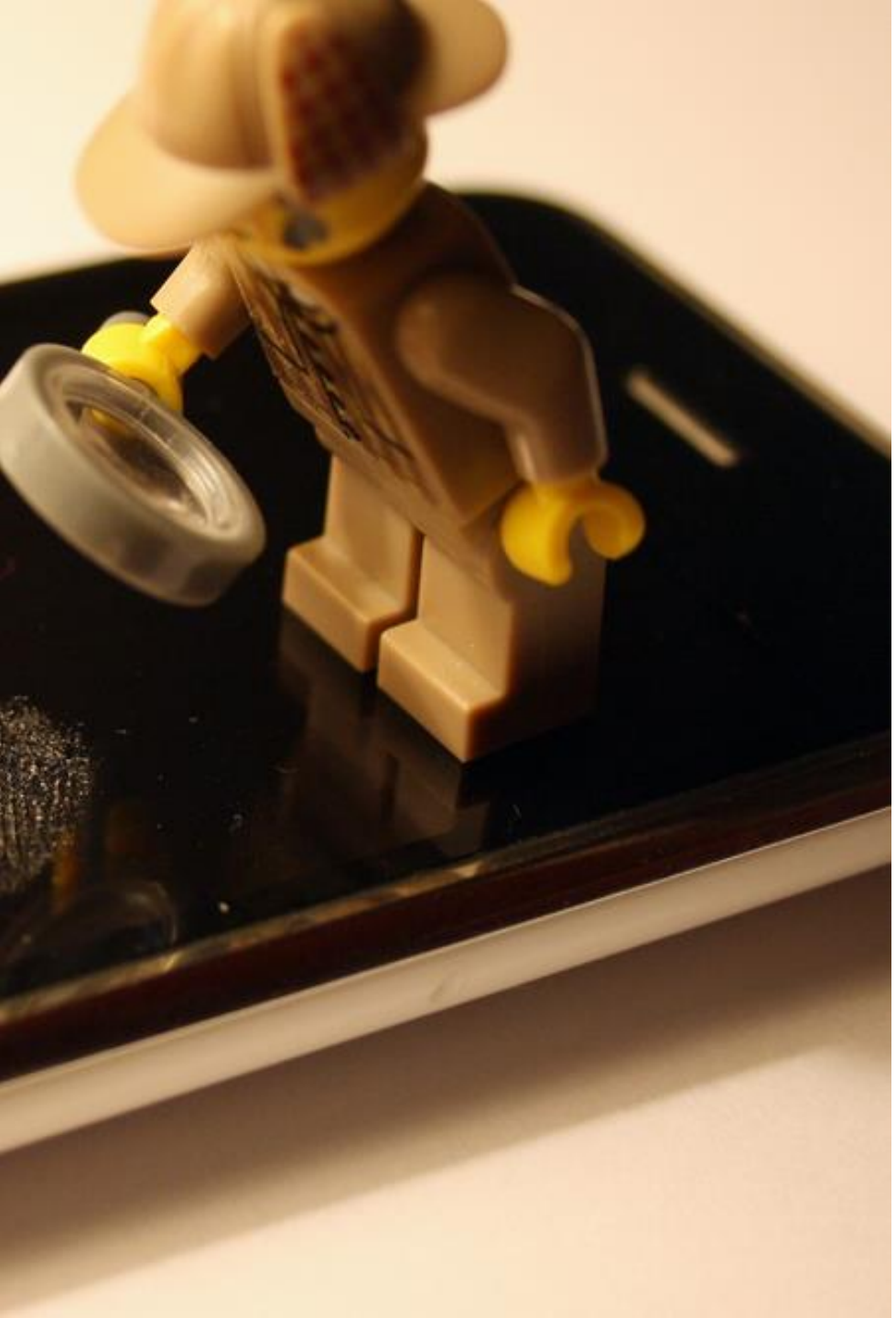
(c) 2021 Lexeprint Inc. All Rights Reserved.



III. Examination of Evidence

- Forensics specialists know that while a document may appear to be deleted, they can check specific directories or system files for duplicates and drafts that can be recovered. They can examine system resources such as restore points and registry files to find hidden data.
- At this stage, the specialists will have a sufficient understanding of the type of data that they are looking for.
- It is critical to reduce the volume of information by intelligently culling files that have no relevance to the investigation.
- Two processes that will be utilized in this stage are: **deduping** and **deNisting**.

(c) 2021 Lexeprint Inc. All Rights Reserved.



IV. Analysis of Evidence

- At this stage, digital forensics examiners perform an in-depth analysis of the evidence that has been gathered thus far. They will attempt to interpret the data, draw insights and ultimately tell a story.
- 'The examiner will pull the gathered evidence together, correlating timelines, identifying the provenance of key evidence, and providing expert analysis using all available information.'
- The aim of a forensic investigation is usually the 'meticulous analysis of available information that builds a narrative around a discovered piece of evidence that helps win cases.'

(c) 2021 Lexeprint Inc. All Rights Reserved.



V. Reporting & Documentation of Evidence

- In this final stage, digital forensics professionals prepare a report that documents all relevant findings of the investigations.
- The expert report will describe the following:
  - Activities undertaken during the investigation;
  - A timeline that correlates evidence with user activities;
  - Expert opinions; and
  - Conclusions

(c) 2021 Lexeprint Inc. All Rights Reserved.



V. Reporting & Documentation of Evidence

- It is crucial to have the investigator explain the results and findings and be readily available to answer any relevant questions.
- Not all cases will require a final report as once one is submitted, it may become discoverable as evidence by the opposing party. A formal report and discussion can take place with the client's attorneys to guide their subsequent examination efforts.
- Each case will be different. Thus, depending on specifics and the agreement between parties, the digital evidence may be provided in several different ways. [1]

(c) 2021 Lexeprint Inc. All Rights Reserved.



Digital Forensics Report

(c) 2021 Lexeprint Inc. All Rights Reserved.

What is a Digital Forensics Report?

Facts discovered and opinions formed need to be documented and referenced to their sources because they are more likely to withstand judicial scrutiny.



(c) 2021 Lexeprint Inc. All Rights Reserved.



Structure of a Digital Forensics Report

1. Brief summary of information
2. Tools used in the investigation process, including their purpose and any underlying assumptions associated with the tool
3. Evidence Item #1 (For example A's work computer)
   a. Summary of evidence found on Employee A's work computer
   b. Analysis of relevant portions of Employee A's work computer
      I. Email history
      II. Internet search history
      III. USB registry analysis
   c. Repetition of above steps for other evidence items (which may include other computers and mobile devices, etc.)
4. Recommendations and next steps for counsel to continue or cease investigation based on the findings in the report

(c) 2021 Lexeprint Inc. All Rights Reserved.



Report Procedures

- All reports of the investigation should be prepared with the understanding that they will be scrutinized by others in excruciating detail.
- The investigator should never comment on the guilt or innocence of an involved party.
- Only the facts of the investigation should be presented; opinions must be avoided where possible. Exceptions pivot on binary functions that have multiple possible outcomes to the extent that even the original developers are unsure what may happen in scenario X.

(c) 2021 Lexeprint Inc. All Rights Reserved.

Lexeprint



Evaluation of a Forensics Report

(c) 2021 Lexeprint Inc. All Rights Reserved.

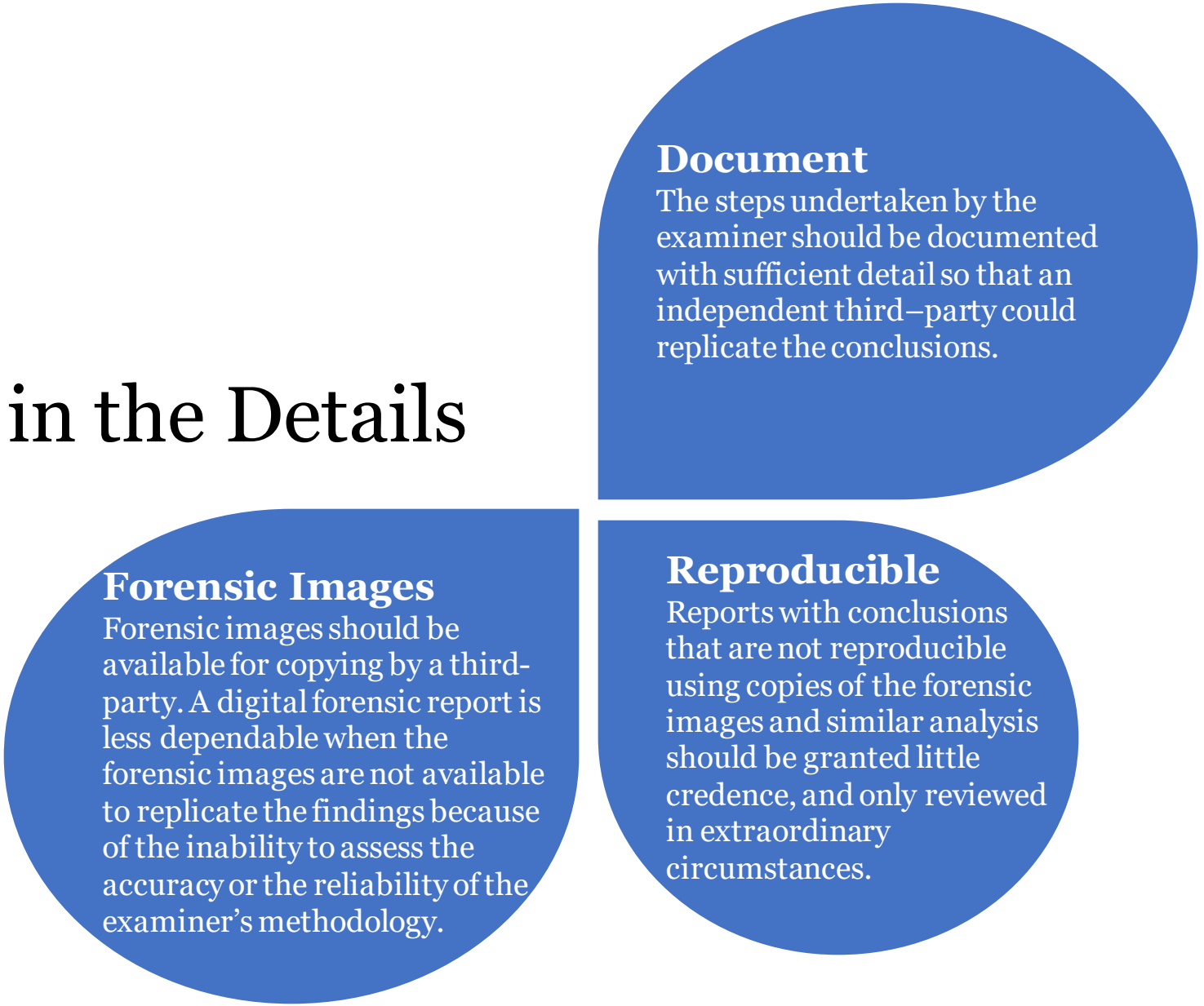


Not All Forensic Examiners are Created Equal…

- The last several years have seen significant improvements in the methodologies necessary to analyze digital evidence.
- This has led to a process that is structured so that years of experience and training are no longer necessary to produce a digital forensics report.
- Cause and Effect: this has led to an increased number of forensic examiners and lowered costs, but also reduced the depth of knowledge held by the average forensic examiner.
- All forensic examiners are not created equal!
- Going with the cheapest option could cost you more in the end

(c) 2021 Lexeprint Inc. All Rights Reserved.

The Devil is in the Details



(c) 2021 Lexeprint Inc. All Rights Reserved.

Qualifications + Experience...



(c) 2021 Lexeprint Inc. All Rights Reserved.



Considerations for a Good Digital Forensics Report

(c) 2021 Lexeprint Inc. All Rights Reserved.

Key Things to Look for…..

Too Much Information

- Report should not volunteer superfluous information

All findings should be accurately qualified for:

- Limitations of the tool(s) used
- Applicability of the current technology and industry-standard best practices
- Methodology or techniques, such as search criteria or formulae
- Scope of the investigation

(c) 2021 Lexeprint Inc. All Rights Reserved.



Check for Information Overload

- The report should provide a cohesive and logical framework on its face.
- It should not delve into the underlying technical minutiae.
- Are there hundreds of digital items in the body of the report that distract from the underlying conclusions?

(c) 2021 Lexeprint Inc. All Rights Reserved.

Rules of Evidence

(c) 2021 Lexeprint Inc. All Rights Reserved.



US Federal Rule of Evidence 902

- The amendment to Rule of Evidence 902, establishes that preserved electronic data should be self-authenticating.
  - *"(13) Certified Records Generated by an Electronic Process or System. A record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11).*
  - *(14) 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 that complies with the certification requirements of Rule (902(11) or (12). The proponent also must meet the notice requirements of Rule 902 (11)."*

(c) 2021 Lexeprint Inc. All Rights Reserved.



Federal Rule of Evidence 702

A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:

- (a) the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;
- (b) the testimony is based on sufficient facts or data;
- (c) the testimony is the product of reliable principles and methods; and
- (d) the expert has reliably applied the principles and methods to the facts of the case.

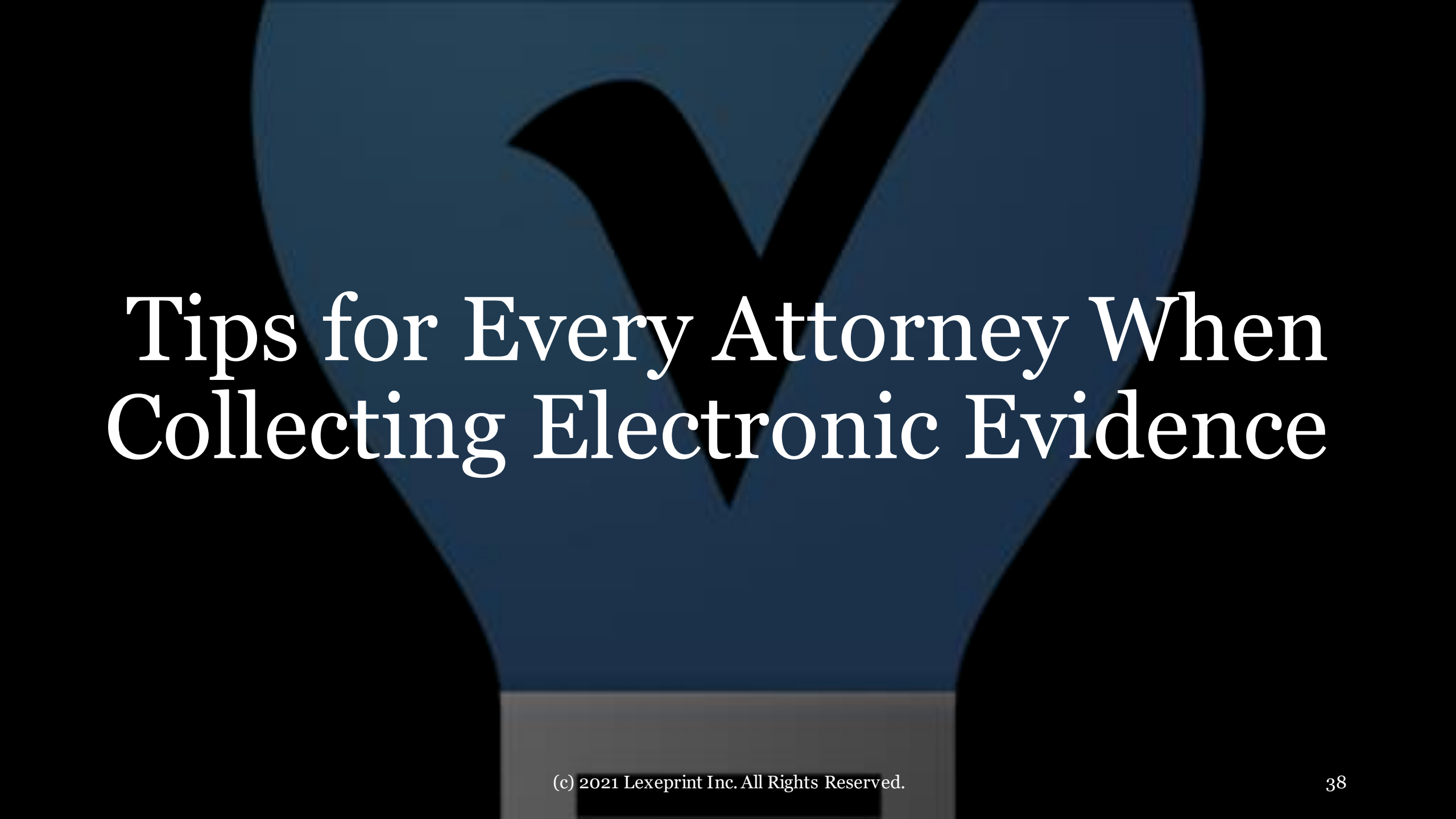
(c) 2021 Lexeprint Inc. All Rights Reserved.



Current State: *Nucor Corp v. Bell*

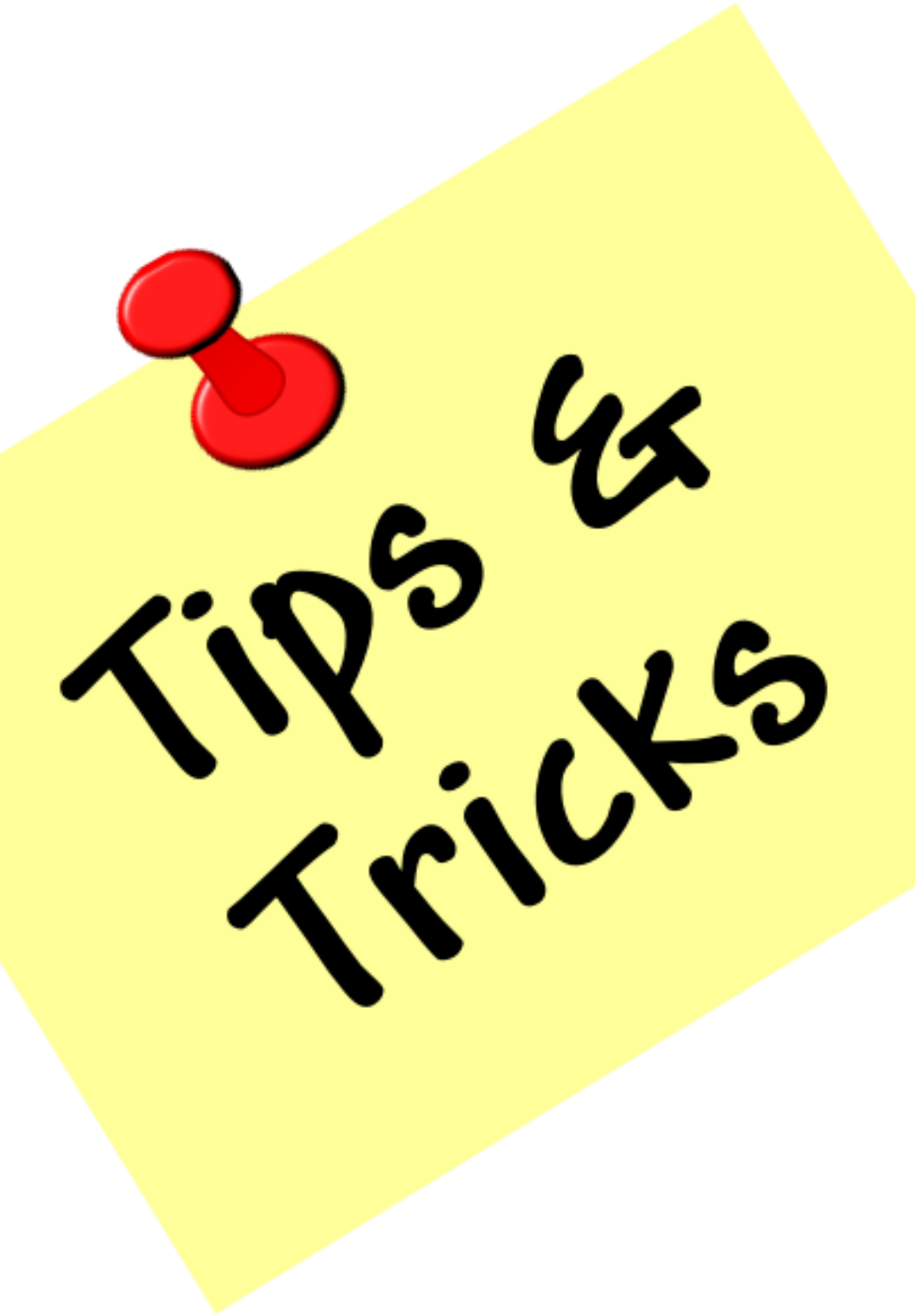
- An expert offered testimony on evidence that the opposing party had used a non-traceable wiping program to clear evidence from a laptop.
- The spoliation case was based on the examination of a hard drive with large blocks of zeroes surrounded by data.
- The court denied a motion to exclude the expert's testimony, finding that the method used by the expert sufficiently filled the analytical gap between the data and the opinion.
- **With a nod to the *Daubert* factors, the court noted that the expert had tested a hypothesis as to how the blocks of zeroes had appeared on the drive and, had replicated the pattern of zeroes.**
- The court also admitted evidence resulting from a test that was found to be capable of repetition, because the expert had thoroughly documented each step in the test to establish that data had been written to the hard drive in the predicted manner.

(c) 2021 Lexeprint Inc. All Rights Reserved.



Tips for Every Attorney When Collecting Electronic Evidence

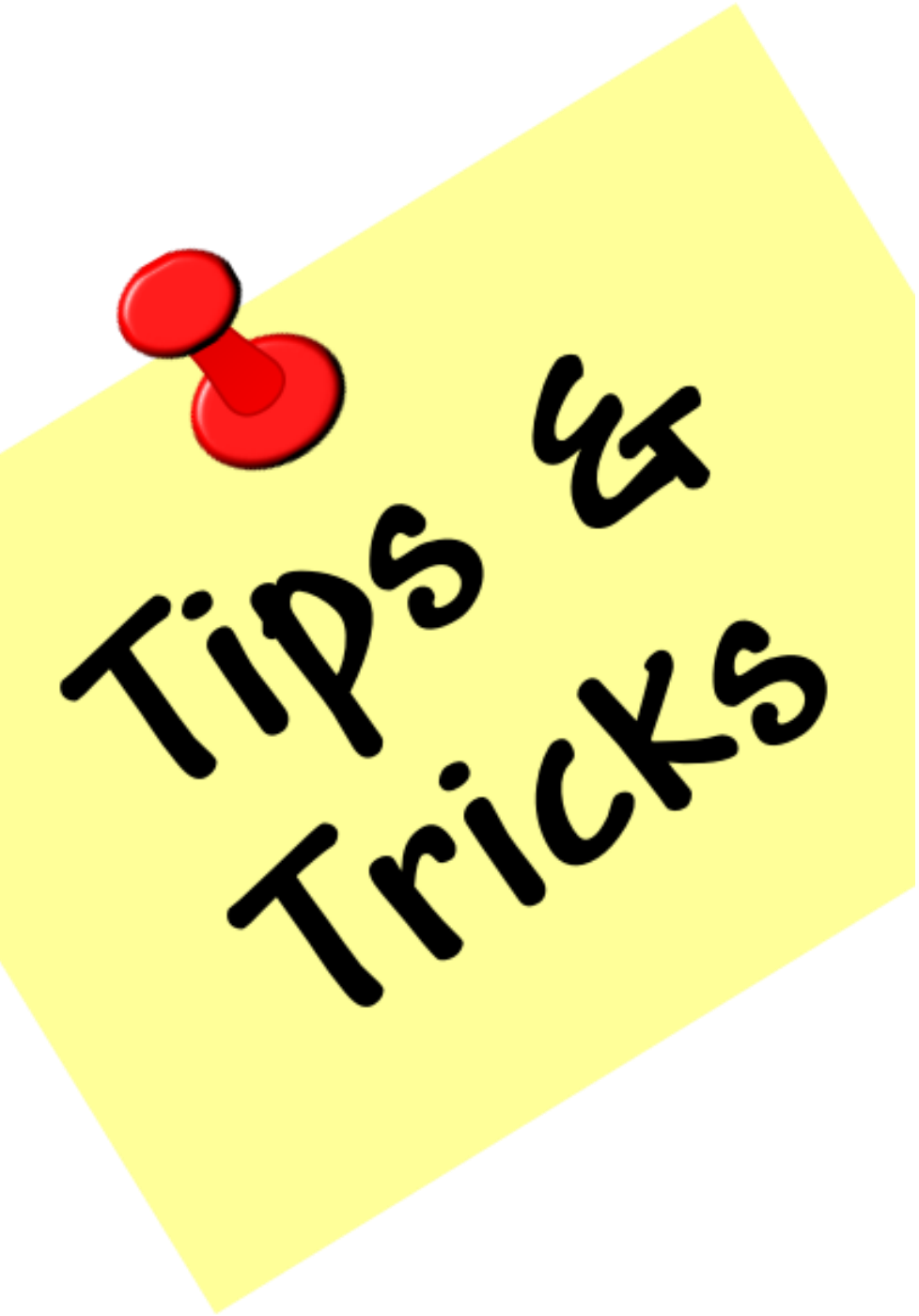
(c) 2021 Lexeprint Inc. All Rights Reserved.



Tips when Collecting Electronic Evidence

- Isolate the computer
  - The laptop should be stored in a safe location and steps should be taken to ensure that no one powers it on if it is already off.
- Do not seek the help of the IT Department
  - Even the most well-meaning examination of the computer can alter the data on the hard drive. The integrity of the computer's data needs to be protected. A forensic copy of the computer's hard drive must be created first!
- Contact your digital Forensics Professional
  - You should engage with a digital forensics expert as soon as possible.

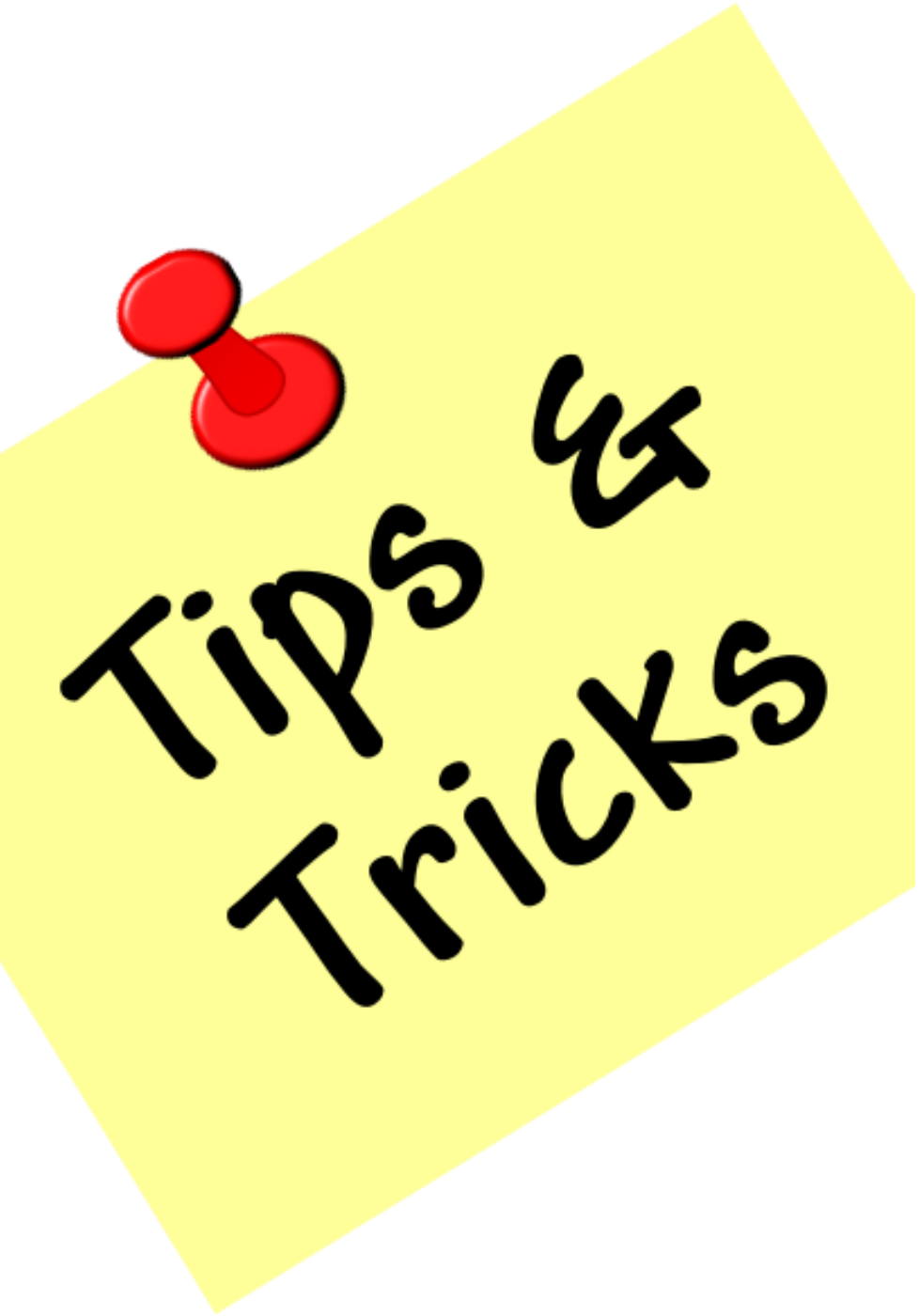
(c) 2021 Lexeprint Inc. All Rights Reserved.



More Tips

- Identify other potential sources of data
  - In 2021, it should not be uncommon for employees to be issued additional digital devices and internet accounts that need to be preserved as well. Hardware can include USB drives, phones, tablets, etc.
- Do not relinquish your responsibility for providing legal guidance!
  - Attorneys must ensure that they continue to use proper ethical and legal judgment to guide discovery efforts.

(c) 2021 Lexeprint Inc. All Rights Reserved.



More Tips

- Incorporate the scope and cost
  - Ensure you accurately define the intended scope of the investigation with your chosen digital forensics professional before any forensic work has been performed
- Implement a chain of custody
  - It is your responsibility to ensure that you make a proper chain of custody for evidence. Ensure that it is suitable and sound for admission in a court of law.

(c) 2021 Lexeprint Inc. All Rights Reserved.

Questions?

(c) 2021 Lexeprint Inc. All Rights Reserved.

Contact Us



Yoav Griver
Email: Ygriver@zeklaw.com
Phone: 212-826-5338
URL: www.zeklaw.com/attorney/yoav-m-griver

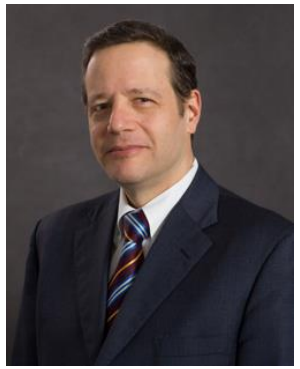


Brian Dykstra
Email: brian.dykstra@atlanticdf.com
URL: atlanticdf.com



Mathea Bulander
Email: mbulander@redgravellp.com
Phone: (612) 746-5031
URL: https://www.redgravellp.com

(c) 2021 Lexeprint Inc. All Rights Reserved.



Yoav Griver
Partner, Zeichner Ellman & Krause LLP

Contact:
P: 212-826-5338
E: Ygriver@zeklaw.com
URL: www.zeklaw.com/attorney/yoav-m-griver

Yoav M. Griver is a partner in the firm's litigation group where he specializes in representing clients in complex commercial matters.

Prior to joining ZEK, Yoav was Litigation Counsel to Weil, Gotshal & Manges LLP, where he litigated a variety of commercial and intellectual property matters for clients in the banking, credit, transportation, insurance, computer software and electronic industries. Before that, Yoav prosecuted banking conspiracy, stock fraud and other cases on behalf of the Israeli Ministry of Justice where he was a member of the Ministry's Economics Unit.

Yoav's many proud moments as a trial attorney include successfully defending Hitachi America in the longest customs fraud trial in the history of the Court of International Trade; successfully defending MasterCard in a multi-district putative class action against claims that MasterCard was responsible under RICO for internet gambling; recovering a verdict on behalf of a class of minority schoolchildren in a prominent civil rights case; successfully defending GMAC in a class action alleging violations of RICO, the Sherman Act, state and federal credit repair organization statutes, and state UDAP statutes; and successfully defending Tellium Inc. in a protracted case involving allegations of breach of contract, unjust enrichment, and fraud upon the United States Patent and Trademark Office.

Yoav has written on a wide variety of legal topics for such publications as The Business Lawyer, The Consumer Financial Services Law Report, The Consumer Financial Law Quarterly Report, and the Journal of Proprietary Rights. He received his J.D. with honors, Order of the Coif, from the University of Texas School of Law in 1991, where he was a member of the Texas International Law Journal, and his B.B.A. with honors from the University of Texas in 1988.

Outside the office, Yoav volunteers his time to the Lawyers' Committee for Civil Rights Under Law and the Office of the Appellate Defender. Yoav also is an Adjunct Professor at NYU. Together with Anthony I. Giacobbe, Jr., of our New York office, he teaches a course at NYU on Sports Law. He resides in Manhattan with his wife.

(c) Law and Forensics 2018. All Rights Reserved



Mathea Bulander
Redgrave LLP – Partner
Contact:
E: mbulander@redgravellp.com
W: (612) 746-5031
URL: https://www.redgravellp.com

Mathea defends the Firm's Fortune 100 companies in complex litigation, including class actions, insurance disputes, antitrust matters, and multi-district litigation. She is a leader and strategic advisor to clients in cases where technologies intersect with the law, the rules of evidence, and rules of civil procedure. As an eDiscovery advocate, Mathea represents clients in state and federal courts on issues of discovery strategy and electronic evidence, and provides strategic counsel regarding legal holds and preservation, fact investigations, witness preparation, motions practice, conferral strategy, and document production and admissibility.

Some of Mathea's recent work experience includes:

- Leading appellate briefing teams and helping prepare lead counsel for arguments in matters addressing discovery issues, including lead responsibility for briefing issues regarding proportionality. Appearance as second chair in oral argument before the Supreme Court of Texas that resulted in a favorable resolution regarding an issue of first impression
- Coordinating and defending consistent discovery production strategies across putative class action matters in multiple state jurisdictions for large national client
- Representing a client in significant multi-district litigation concerning discovery compliance and privilege review issues where the production involved more than two million documents produced and the initial logging of over sixty thousand documents
- Preparing corporate 30(b)(6) witnesses to testify regarding the accessibility of data in complex customer management systems, tools available to query the data, and document retention policies

Outside of the courtroom, Mathea is a key advisor regarding litigation readiness, information governance, and data disposition strategies. Mathea was recognized by the Profiles in Diversity Journal in its 2019 "Women Worth Watching" annual list.

ORGANIZATIONAL INVOLVEMENT & MEMBERSHIPS:
Mathea serves on the Executive Committee for the Computer & Technology Law Section of Minnesota State Bar Association and is a member of The Sedona Conference® Working Group on Electric Document Retention and Production. She also serves as a volunteer attorney for the Children's Law Center of Minnesota.

EDUCATION:
Mathea received her J.D., cum laude, from William Mitchell College of Law and a B.A. from Macalester College. She is admitted to practice in Minnesota.



Brian Dykstra
Atlanta Data Forensics – President & CEO
Contact:
E: brian.dykstra@atlanticdf.com
URL: atlanticdf.com

Mr. Dykstra has over 19 years experience in investigations, computer forensics, incident response, network and wireless security testing and information security. Mr. Dykstra was previously the CIO and Director of Professional Education at Mandiant, Inc. where he was responsible for the development and management of numerous advanced computer security and cybercrime investigation courses.

Before founding Atlantic Data Forensics (formerly Jones Dykstra and Associates, Inc.), Mr. Dykstra was the CIO & Director of Professional Education and a founding member of Mandiant, where he was responsible for the development and management of numerous advanced computer security and cybercrime investigation courses. While at Mandiant, Mr. Dykstra annually trained over 400 FBI Cyber Crime agents as well as many state and local investigators through a series of highly acclaimed cybercrime investigation courses. As Mandiant's Chief Information Officer (CIO), Mr. Dykstra was also responsible for all planning, budgeting, implementation and security of the corporate information infrastructure. Prior to becoming a co-founder of Mandiant (formerly known as Red Cliff Consulting, LLC), Mr. Dykstra was a Senior Program Manager at Communications Technologies where he led commercialization efforts of computer security and managed services business groups; supervised the secure remote management of UNIX and Windows customer and network systems, and provided technical oversight for business development efforts and technical assistance to commercial and government sales groups. An enabling factor was his prior experience as the Senior Director of Managed Services at Apex Digital Services and Viaken Systems, Inc. where he managed scientific research networks worth over $9 million, and designed and implemented a Network Operations Center (NOC) and scientific computing system staging area valued over $3 million.

Prior to employment at Apex/Viaken, Mr. Dykstra was the Director of Technical Operations at Sytex, Inc where he co-developed a two-week computer intrusion response course for the Federal Bureau of Investigation. Not only did Mr. Dykstra teach on-site at the FBI Academy at Quantico for over one year where he trained hundreds of FBI Special Agents in computer crime investigations, he has also trained hundreds of students from the United States Air Force, State Department, Central Intelligence Agency and of Office of the Inspector General in computer crime, intelligence analysis and criminal investigations. He also received a Letter of Appreciation from the Director of the Federal Bureau of Investigation for investigative support to the international network intrusion investigation known as "Moonlight Maze." Prior to joining SYTEX, Mr. Dykstra was a Counterintelligence Special Agent with the United States Army's Military Intelligence Branch where he specialized in investigations and operations, to include information warfare and Technical Surveillance Counter Measures.

Don’t Fall Behind: A Cybersecurity Guide for Law Firms

This concise guide offers steps all law firms, small and large, should take to protect their networks and data against cyber attacks.

Buy Now

By Daniel B. Garrie

Available on Amazon as an eBook or paperback.