PI magazine.com

professional investigator magazine

$9.95

January/February 2023

HOW TO BUILD A TASKFORCE FROM A WHIM AND A CALL

INTERNATIONAL MISSING PERSONS CASE STUDY

CONDUCTING COHABITATION INVESTIGATIONS

FOLLOWING THE MONEY: CREDIT CARD LAUNDERING SCHEMES

CRIME SCENE MANAGEMENT 101

THE UNDERCOVER PRIVATE INVESTIGATOR

Perspectives on Electronic Evidence Management

BY **ROBERT B. FRIED,** SENIOR VICE PRESIDENT & GLOBAL HEAD OF FORENSICS AND INVESTIGATIONS, SANDLINE GLOBAL
RYAN PARTHEMORE, SAAS EVANGELIST, CELLEBRITE

There are different standards, considerations, and perspectives regarding the documentation and management of electronic evidence. Ideally, a digital forensic practitioner who handles or interacts with evidence understands the various workflows and requirements that ensure that the data can be tracked throughout the lifecycle of an investigation.

BE CAREFUL HOW YOU HANDLE THAT

Evidence handling is an important aspect of evidence management, and proper protocols must always be followed. It is important to remember that physical evidence may be in play on the physical device itself. Trace evidence such as fingerprints, hair, fibers, and touch DNA, which are often present on electronic devices, may be vital to an investigation and should not be overlooked. Forensic practitioners are trained in how to identify, preserve, and collect a wide array of evidence types and should be engaged to assist when necessary.

CHOOSING THE PROPER STORAGE CONTAINER

Electronic evidence has a necessary companionship with a storage container; data does not exist without some type of storage involved. Storage containers are not all equal and choosing one means that you assume the risks and limitations of that container type. This decision always has implications, but the stakes are far greater with electronic evidence.

For example, USB thumb drives are relatively inexpensive, and frequently utilized to store electronic evidence. It is important to consider the capacity of the USB thumb drive, if it will be utilized as a storage container; is it large enough to store the electronic evidence? USB flash drives employ chip-based flash memory with an expected lifespan expressed in read/write cycles; therefore, it has a finite number of usages, and it is impossible to know when it may begin to fail. Many thumb devices come with a two (2) year warranty, with an anticipated life expectancy under ten (10) years. It is not uncommon for the warranty of a USB thumb drive, used to store electronic evidence, to expire during an ongoing investigation. It is always possible for a USB thumb drive that is in physical storage to become inoperable. If device failure occurs, you may get reimbursed financially, but what about your electronic evidence?

Specialized training courses provide digital forensic practitioners the skills necessary to remove the flash memory from USB thumb drives for subsequent forensic analysis. Having personally enrolled in such a course, I recall that the instructor provided the students with new USB thumb drives, from a bulk purchase, for this hands-on exercise. Some of us wondered what data may be recovered from the new USB thumb drives! Ultimately, I came to realize that USB thumb drives purchased in bulk, are often made from recycled flash memory. Therefore, it may be difficult to gauge a device's untold read/write cycles, and its anticipated lifespan, if such a device was to be utilized for storing critical electronic evidence.

USB thumb drives can be used to transfer data between computers; they were designed for short-term storage. Similarly, optical discs such as Blu-ray and DVD degrade over time, rendering them unreadable. Optical storage is also susceptible to physical damage, such as scratches. Therefore, optical media should not be utilized to store electronic evidence.

In recent years, cloud storage has become a viable option for evidence storage. When coupled with a secure evidence management solution, cloud storage becomes the frontrunner for the storage of electronic evidence. In fact, a properly architected cloud-based solution is every bit as secure as a physical evidence storage site, while easily outpacing on-premises solutions in durability. Files uploaded to a cloud service are commonly replicated to ensure redundancy before the upload is reported successful. If you are dealing with a large volume of data, cloud-based solutions can assist in controlling costs without the need to continually expand storage, which is the case with on-premises storage.

It is important to keep in mind that electronic evidence is data, not a storage container. It's up to the investigator to seek guidance from a digital forensic practitioner to choose the most appropriate storage container for the long-term storage of electronic evidence, to ensure its viability during an investigation.

DATA PROTECTION IN TRANSIT & AT REST

The scope of an investigation may involve the collection and review of highly sensitive information, including Personally Identifiable Information (PII) and Intellectual Property (IP). Our clients entrust us with their most important data, and it is our duty to protect their data while in transit and at rest. Whenever possible, electronic evidence should be hand-carried, transported using a reputable shipping or courier service, with tracking, and any data target media utilized should be encrypted. For example, transporting electronic evidence in checked baggage during air travel is not recommended. If a client wants to transfer data electronically, it is recommended to utilize a Secure File Transfer solution.

DOCUMENTATION IS ESSENTIAL

As investigators, we all know that investigations take time. Throughout the life cycle of an investigation, chain of custody documentation must be maintained for any evidence collected. This essential documentation records information regarding the transfer of possession between parties who have physically handled or have interacted with the evidence. Chain of custody documentation can be maintained via a hard-copy document or electronically. Regardless of the format used, for each transfer that occurs, the date and time, the names, and signatures (including those generated electronically) of the parties involved, and the purpose of the transfer is recorded.

It is important to remember that evidence is not relevant, and therefore not admissible, without end-to-end chain of custody. The same rules of evidence apply whether the evidence is physical or electronic, as the court makes no distinction. It is therefore important for evidence to be physically secured and not carried around in briefcases and case folders or tossed in a filing cabinet. Each party who accesses the electronic evidence is part of the chain of custody, just as if they moved physical evidence from one point to another. Their actions are a link in the electronic chain of custody, and if that activity cannot be properly accounted for, the evidence is open to objection to relevance.

THE EMERGENCE OF INVESTIGATIVE MANAGEMENT SOLUTIONS

Technological advancements have allowed forensic laboratories to implement investigative management solutions, to supplement or replace paper-based systems. The best solutions are designed by forensic practitioners with experience in the laboratory, and who adhere to strict evidence handling protocols, allowing records about evidence to be maintained in a defensible and efficient manner. Previously, hard-copy documentation was solely maintained, and often not equipped to address the nuances of electronic evidence. Now, information can be scanned or entered in a central repository, often located in the cloud, and only accessible by team members who will be assisting with the investigation.

Often, an investigation involves a team of stakeholders, including investigators, examiners, counsel, and other specialists. One common issue regarding electronic evidence management is that everyone needs a copy. In such scenarios, we often find ourselves dealing with numerous untracked copies of electronic evidence. The loss of control of a copy can negatively impact the investigation and potentially impart liability on the stakeholders.

An investigative management solution can allow all stakeholders to share critical information, and manage physical and electronic evidence, including its collection, submission, management, and examination, throughout an investigation's lifecycle - ensuring that the evidence is relevant, properly documented, and therefore admissible.

KEY POINTS TO REMEMBER

When encountering electronic evidence during an investigation, it is important to remember the following:

- A digital forensic practitioner can choose the most appropriate storage container to ensure its viability during an investigation.
- Electronic evidence should be protected while in transit and at rest.
- Evidence is not admissible without end-to-end chain of custody.
- A properly architected cloud-based investigative management solution is every bit as secure as an on-premises solution. PI

Robert B. Fried is a seasoned expert and industry thought leader, with over twenty years of experience performing data collections and forensic investigations of electronic evidence. He is the Senior Vice President and Global Head of Sandline Global's Forensics and Investigations practice. In this role, Robert leads the day-to-day operations of the practice, overseeing the forensic services offered to the firm's clients, including data collections, forensic analysis, expert testimony, and forensic consultation. Previously, Robert held senior-level positions within the digital forensic practices at global professional services firms. Additionally, Robert was a Computer Crime Specialist at the National White Collar Crime Center (NW3C), where he developed and instructed computer forensic and investigative training courses for federal, state, and local law enforcement agencies. He attained a BS and MS in Forensic Science, and certificates in Law Enforcement Science, Computer Forensic Investigation, and Information Protection and Security from the University of New Haven. Robert serves on the Board of Advisors for the Masters in Investigations program at the University of New Haven. He holds and actively maintains the following industry certifications: Access Data Certified Examiner (ACE), Certified Forensic Computer Examiner (CFCE), EnCase Certified Examiner (EnCE), GIAC Certified Forensics Analyst (GCFA), Chainalysis Cryptocurrency Fundamentals Certification (CCFC), Chainalysis Reactor Certification (CRC), and C4 Certified Bitcoin Professional (CBP). Robert is a licensed Professional Investigator in Michigan and is a licensed Private Investigator in New York. He is a frequent speaker at industry events, has been a guest on industry podcasts, and has been published in several professional publications. Robert is the author of Forensic Data Collections 2.0: The Guide for Defensible & Efficient Processes. Additionally, he is the author of PI Magazine's CyberSleuthing Department, where he shares insightful content on topics relating to digital forensics, eDiscovery, data privacy, and cybersecurity.

Ryan Parthemore joined Cellebrite as a SaaS evangelist following his extended tenure within law enforcement. A veteran in the industry, Ryan has over 20 years of experience as a patrol officer, detective, and technical lead in a government digital forensics laboratory. During his time in law enforcement, Ryan has completed hundreds of hours of training in digital forensics, performed thousands of digital forensics examinations, represented his unit through ANAB ISO 17025 accreditation, and testified as an expert witness in state and federal court. Ryan moved to Cellebrite to utilize his expertise to help others in law enforcement find more effective ways to resolve cases.