White Paper
May 20, 2019

Digital Evidence Innocence Initiative

Digital Innocence

VERITAS VOS LIBERABIT

Exonerating the Innocent and Preventing Wrongful Convictions with Digital Evidence

Presenting a standardized method for investigating digital evidence to exonerate the innocent and prevent wrongful convictions

Table of Contents

Introduction

This paper highlights the need for a standardized method of investigating digital evidence in post-conviction reviews, as well as, the requirement that this method be applied to pre-trial cases to prevent wrongful convictions from occurring. We will outline the most up-to-date standardized process model for investigating digital evidence, in both pre-trial and post-conviction review cases and present a practical methodology for its application.

In post-conviction cases, using the latest digital forensic knowledge or technology can be substantially more probative. Likewise in pre-trial situations, following a standardized process will ensure reliability and effective representation that can reduce pre-trial incarcerations and prevent future wrongful convictions. By way of comparison, earlier advances in the field of DNA science left the defense community with the onerous task of playing catch-up with understanding this evidence and gaining meaningful access to testing its reliability. As the use of scientific evidence in litigation increased, the case law also evolved until the Supreme Court established the *Daubert* standard for determining the reliability and accuracy of scientific evidence. In conjunction with the *Daubert* decision, professional standards and training requirements emerged to adjust for this phenomenon. But not withstanding this evolution, wrongful convictions continued to occur that are only now being identified and addressed.

Digital Innocence

The Digital Evidence Innocence Initiative (DEII) is the first and only organization in the nation dedicated to exonerating the innocent and preventing future wrongful convictions in cases that involve digital evidence. Combined efforts from the criminal defense and digital forensic community bridge the gap as to the training, collection, and analysis of digital evidence. By sharing knowledge and creating a standardized assessment method, we have identified several areas where the latest forensic technology can reveal new digital evidence. For example, unlocking a previously inaccessible cell phone can produce new evidence. New forensic methods and techniques can also produce previously undiscovered digital evidence. The adoption of a standardized assessment method to re-examine old cases has uncovered new digital evidence. These same standardized methods are now being proactively applied to pre-trial matters to prevent wrongful convictions and to reduce pretrial incarceration.

Parity for Public Defenders

The majority of defendants facing criminal charges are indigent. When the force of local, state, or federal law enforcement is levied against an indigent defendant, it becomes the state or federal government's responsibility to provide each individual with court-appointed representation. A vigorous and independent indigent defense system, funded and resourced in parity with the prosecution, promotes fairness, equal access and reduces the risk of wrongful convictions. The majority of digital forensic examinations are conducted by state or federal labs, and since law enforcement agencies are considered first responders, a significant and disproportionate amount of training and resources is made available to prosecutors and law enforcement personnel compared to what is available to public defenders and its investigators.

Public defenders are also disadvantaged in managing digital evidence because of rapid changes and proliferation of digital devices, budgetary limitations, and lack of equal access to matching training and technology. The defense may be behind because of a lack of early involvement to preserve time-sensitive digital evidence, or they do not have independent forensic resources to analyze the data. The IACP Law Enforcement Cyber Center describes the lack of parity for the defense in their article Understanding Digital Evidence.

An independent, indigent defense system resourced in parity with the prosecution will reduce the risk of wrongful convictions.

Independence for Indigent Defense

Sadly, the criminal justice system has created an infrastructure, whether unintended or not, that does not promote the principals of an independent defense system. The vast majority of state crime labs are under the umbrella of the state police system, and there is an imbalance in the training, access and resources that is provided to prosecutors compared to defense counsel.

Providing Effective Representation

As the use of DNA evidence in criminal prosecutions increased, the need arose to develop standards, access, and training to defense counsel in order to provide effective representation to clients. In today's criminal prosecutions, with the amount and frequency in which digital evidence is generated and used, there is a real need to create standards that the defense counsel must follow to provide what is considered effective representation. The DNA model should be applied to digital evidence and followed accordingly as a parallel course.

The defense team must have the knowledge, training and resources equal to that of law enforcement. Investigators and attorneys must evaluate the potential damaging evidence collected by police investigators and conduct an independent and vigorous investigation and assessment of the digital evidence.

> *There is a real need to create standards that the defense counsel must follow to provide what is considered effective representation.*

Evaluating Digital Evidence From Law Enforcement
Investigators or first responders with limited background and training who rely only on the forensic software for the analysis might not fully understand their findings. These examiners can be challenged on their experience in court because they often draw inaccurate conclusions from their analysis. For that reason, it is important to verify the expert's credentials as an examiner. Also, it is always recommended to consult with your own expert to review the State's evidence to find problems with the State examiner's conclusions.

Dealing with Digital Discovery
Currently, there are no comprehensive electronic discovery rules separate and apart from general discovery requirements in criminal cases. Some legal scholars suggest the existing civil rules in many jurisdictions as they relate to e-discovery as appropriate models to follow in criminal cases, but these civil rules are also not uniformly adopted. Accordingly, discovery rules in both civil and criminal matters need to be updated and/or rewritten to reflect the prevalence of ordinary digital evidence in the majority of cases. In jurisdictions where discovery production is not an issue, the large amounts of digital data that gets dumped on the defense often becomes overwhelming. Not only can the digital evidence correspond to thousands of documents with correlating metadata, making the data set extremely large, it can also be in multiple different formats, requiring the defense team to have the resources and expertise to access the data.

For digital evidence discovery purposes, the defense must know to request and receive a copy of the native forensic evidence file. Printouts or PDFs of the relevant material should not be accepted and are incomplete. Native files will allow access to metadata. This information is not available if you simply accept printed or edited files. Consider due process or *Brady* arguments for cases in which native files might provide exculpatory evidence or information.

Nature & Behavior of Digital Evidence

One of the most critical and important things a defense attorney and/or investigator should know about digital evidence is its extreme time-sensitive nature. Furthermore, this evidence is often inherently fragile, as it may be easily altered, tampered with, or destroyed through improper handling or examination. Therefore, providing effective representation in cases with digital evidence requires the initial assessment of the evidence to be conducted as soon as possible.

Need for Early Case Assessment

Due to the time-sensitive nature of digital evidence, the need for early case assessment goes beyond just having parity in training and resources. Effectiveness of a client requires early involvement by competent advocates to identify, preserve and collect time-sensitive digital evidence for later analysis and reporting.

Equal access to qualified defense experts
will reduce the risk of prejudice to defendants.

Need for a Standardized Training

Digital evidence requires comprehensive knowledge and experience to review all of the material, locate the items of interest, and finally digest and understand the value of the digital data. Even with balanced reciprocal discovery rules, there needs to be parity in ongoing standardized training and available resources for the defense. This should include equal access to qualified experts, to reduce the risk of prejudice to defendants.

Continuing Education

Advancements in technology and emerging case law associated with this type of evidence changes all the time. The defense community needs equal access to continuing education to acquire the latest working knowledge of digital evidence and its use in criminal cases.

The proposition that defense attorneys need to keep up with the latest technologies to provide effective representation to their clients is certainly not novel, but until recently, no satisfactory concepts have been suggested to help guide the defense community on how to achieve this balance when it comes to digital evidence.

Digital Case Assessment Method (DECAM)

DECAM is the first standardized assessment method developed with the combined knowledge and experience of criminal defense investigators and digital forensic experts. This methodology was created specifically for the criminal defense community to proactively investigate cases involving digital evidence using the latest technology, in accordance with the best practices.

Read the DECAM White Paper

> *The first standardized Digital Evidence Case Assessment Method for the Criminal Defense Community.*

DECAM promotes a uniformed application of national standards for the assessment, collection and use of digital evidence, updated to today's technology to ensure consistency in quality, efficiency, and effectiveness in accordance with the Principles of a Public Defense Delivery System.

DECAM provides a comprehensive framework consisting of workflow guides, printable check lists, forms, templates, requests, motions, evidence receipts and logs, the latest cellular provider retention schedule, internet and social media subpoena guides, as well as other critical resources.

Originally, **DECAM** was developed as a proactive way to reliably investigate digital evidence meant to reduce pre-trial incarceration and prevent future wrongful convictions. However, after recognizing the need to apply this method to post-conviction review in cases where digital evidence was a critical factor, it became the genesis for the **Digital Evidence Innocence Initiative.**

DECAM Impact

- To provide a meaningful standardized method for post-conviction review regarding cases involving digital evidence.

- Provide a uniformed standard for assessment and collection of digital evidence to prevent spoliation.

- To provide comprehensive uniformed training, including assessment, collection, and preservation in accordance with the prevailing standards for public defenders and the defense community.

- To provide meaningful access to independent digital forensic resources, training and guidance for public defenders and the defense community.

The ABC’s of DECAM

A proactive and repeatable approach to manage all the different types of digital evidence ensures effectiveness and reliability. The **ABC** method of ***assess, baseline*** and ***collect*** guides the investigator through this process.

The assessment component provides worksheets and flowcharts to identify, locate ,and triage the most time-sensitive data and prevent spoliation. The baseline aspect provides worksheets that capture a reliable record of the basic information needed to access the devices or other sources. The collection section provides investigators with the framework to combine the information gathered during assessment with the best practices to ensure as much of the digital evidence is collected and is in accordance with the standards.

Overcome time-sensitive digital evidence with early case assessment.

Professional Standards

Following an established uniform procedure for managing digital evidence improves the quality and consistency of delivering an effective public defense system. It would also allow reliable, repeatable and accurate guidance to defense counsel as they make key decisions in the most efficient and cost-effective manner without sacrificing quality representation.

Standards and Best Practices For Collection

The collection and examination of digital evidence should be conducted in accordance with the best practices and a quality management system. The prevailing governing standards and best practices are set forth by The Scientific Working Group of Digital Evidence (SWGDE) and The National Institute of Justice (NIJ). These guides establish recommendations for how investigators should handle digital evidence.

Digital Evidence – A Forensic Science Discipline

Similar to other recognized forensic techniques, the scientific community has developed standards and implemented quality management systems for the proper methods of collection and storage of digital evidence. The prevailing quality system standards are set forth by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The current standard for the collection and preservation of digital evidence is ISO/IEC 27037.

Leveraging the Knowledge of Experts

While digital forensic experts should be involved as early as possible, their involvement should go beyond examining digital evidence or evaluating evidence collected by law enforcement. Using digital experts at trial can provide technical guidance in cross-examination of prosecution experts. Experts should also be used to evaluate the state's crime lab's adherence to the ISO Quality System requirements. These standards rely heavily on documentation and allow a greater understanding of what happened with the evidence after it was collected. Bench notes, examiner proficiency reports and quality audit reports are just some of the documents that should be obtained and examined by defense experts. Any knowledge gained will enhance the defense's ability to evaluate how the evidence was handled by laboratory personnel.

Legal Challenges to Handling Digital Evidence

In digital forensics, any interaction with a device can alter its contents, so any part of the process that is not carefully and properly documented can be a point where reasonable doubt is emphasized. Adhering to the best practices process guides the defense in evaluating how the evidence was handled.

Legal Challenges to Collection

Whichever forensic method is used, the examiner must document every step of the process in preparation for possible legal challenges. If documentation is missing, cross-examination can reveal flaws in the process. The expert should be able to confirm that the forensic equipment that was used was properly functioning and that the software they use has been validated.

Also, ask the examiner for verification that the target media contained no information before the forensic copy or forensic evidence file was placed onto the target media. If this documentation does not exist, the examiner cannot be certain that the suspect material came from the defendant's device.

Using Hash Values to Verify Digital Evidence

In computer forensics, hashing is a way to represent a piece of digital evidence with a unique number generated from an algorithm of the contents of the file(s) or the entire device memory. The hash value is like a DNA profile for the whole drive, and it can be used to ensure that no data was altered during the course of the forensic acquisition or analysis.

Conclusion

As technology continues to advance, more data can be accessed that may not have been previously available. Some digital evidence can be found long after it was created, such as Google timeline, while some devices that were unable to be accessed can now be examined. Applying the latest standardized case assessment method helps find more evidence. Applying the latest technology to examine the evidence can lead to the discovery of new digital evidence that can be used to overturn wrongful convictions.

Digital evidence is part of many criminal defense cases and will continue to evolve with advances in technology. Currently, with regards to digital evidence a significant disparity is evident between the resources available to law enforcement and that which is available to public defenders. As a result, criminal defense investigators and attorneys must find a meaningful way to achieve parity and have access to the same training and independent experts to be effective.

Standards and best practices, along with quality system requirements, exist and are available for the collection and use of digital evidence. Using these standards can ensure the reliability of digital evidence collected by the defense as well as the ability to evaluate and challenge digital evidence presented by law enforcement. Practical application of a standardized repeatable method will ensure reliability. The Digital Evidence Case Assessment Method combined with a proactive approach will enable preservation of time-sensitive digital evidence that can reduce pre-trial incarcerations and prevent future wrongful convictions in the first place.

About Digital Innocence

The **Digital Evidence Innocence Initiative (DEII)** was launched in 2019 and is based in Connecticut. **DEII** is an independent organization, founded by a criminal defense investigator, criminal defense attorney, and a certified digital forensic examiner. Initially, the focus was to apply new technology for post-conviction review in cases where the digital evidence was a deciding factor. The initiative evolved to also provide expert forensic services and training for the defense community, and to advance a uniformed national standard for preventing wrongful convictions in cases involving digital evidence.

Founder/Director- Michael Udvardy

The **Digital Evidence Innocence Initiative** was developed in 2018 by Mike Udvardy, a Board Certified Criminal Defense Investigator, creator of the Digital Evidence Case Assessment Method-**DECAM** and owner of IRIS LLC, a Connecticut based criminal defense investigative firm.

Co-Founder - James Oulundsen

Jim Oulundsen is a cross-trained, criminal defense investigator, Encase and Cellebrite Certified digital forensic expert, and Laboratory Manager at ***e*Lab Digital Forensics.** ***e*Lab** is an independent laboratory providing certified digital forensic services exclusively to public defender organizations and Innocence Projects. Our experts provide the widest range of digital forensic services achieving parity with state crime lab capabilities.

Co-Founder - William Paetzold, Esq.

Bill Paetzold is a partner and co-founder of Moriarty, Paetzold & Sherwood and was admitted to the Connecticut and Federal Bar in 1990. He began his career as a Public Defender and worked as a criminalist at the Connecticut State forensic crime Lab. Bill specializes in criminal defense cases in state and federal court involving digital evidence. Bill provides strategic legal consultation to the defense community regarding the effective use of digital evidence in pre-trial cases and post-conviction review.

Curriculum Development

The world is a better place thanks to people who want to help others. Thank you to Chief Investigator Ellen Knight of the Connecticut Division of Public Defender Services for assisting in development of this curriculum and the inspiration for this initiative.

Digital Evidence Innocence Initiative

www.digitalinnocence.com
info@digtialinnocence.com
877-266-3703

FOCUSED ON THE FACTS
I.R.I.S. LLC
Information Retrieval Investigative Services
Licensed Investigators
Certified Digital Forensics

www.irisinvestigation.com
irisllc@irisinvestigations.com
860-522-0001

eLab
DIGITAL FORENSICS
PRACTICAL SOLUTIONS TO DIGITAL EVIDENCE FOR PUBLIC DEFENDERS

Hartford, CT
Springfield, MA
Brattleboro, VT

www.elabforensics.com
info@elabforensics.com
877-266-3703

Nashua, NH
Providence, RI
Maine

MORIARTY, PAETZOLD & SHERWOOD
ATTORNEYS AT LAW

2230 Main Street, Glastonbury, CT
www.mpslawfirm.com
whpaetzold@mpslawfirm.com
860-657-1010