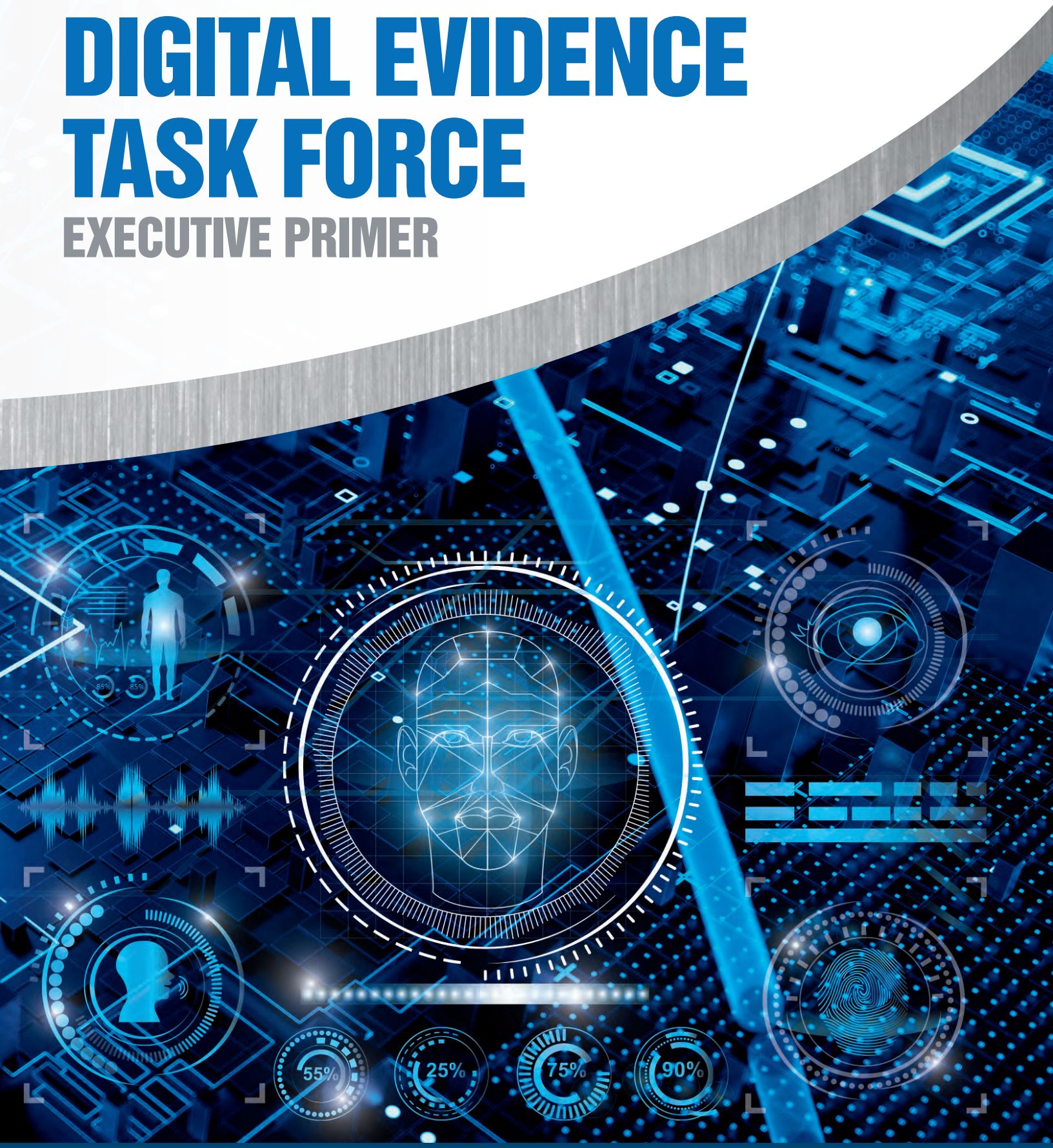
DIGITAL EVIDENCE TASK FORCE

EXECUTIVE PRIMER



IACP
International Association of Chiefs of Police

Overview

The expansion of communications technology means that crime scenes are often digital rather than physical, which poses a growing challenge to investigators. In addition, physical crime scenes—the ones that state and local law enforcement respond to every day—are much more complex than ever before. Crime scenes from homicides, kidnappings, assaults, property crimes and incidents of domestic violence — crimes that impact thousands of victims, families, and communities annually—now, more often than not, include digital evidence.

Properly obtained and analyzed, digital evidence results in more actionable and successful investigations and prosecutions. At the same time, the complexity and sheer volume of digital evidence has greatly impacted law enforcement operations and investigations.

To succeed in this new environment, law enforcement executives need to understand the complexities of digital evidence, consider what policy changes they may need to adopt, and how they can work with both their communities and policy makers to ensure they fully understand the challenge this issue poses for law enforcement.

To assist law enforcement leaders in addressing this issue the International Association of Chiefs of Police (IACP) established the Digital Evidence Task Force (DETF).
The DETF draws on the expertise of the IACP Computer Crimes and Digital Evidence Committee, Forensic Science Committee, and Police Investigative Operations Committee.

Scope of the Problem

Law enforcement encounters digital evidence in numerous ways, including, but not limited to:

- Video and audio files
- Social media posts and aggregated products
- Email and other business communications
- Evidence on computers, mobile devices, and wearables
- Ecommerce and other online financial data
- Sensor data such as license plate readers (LPR), facial recognition, and gunshot detection technology
- Website access logs
- Geolocation information
- Subscriber records for online service providers
- Data from motor vehicle computing systems
- Data from the Internet advertising ecosystem

In addition, the collection, analysis, utilization, and preservation of digital evidence must be managed under the same standards as other types of evidence. As a result, law enforcement must adapt to manage the appropriate handling and use of digital evidence available from a multitude of resources.

Challenges to Law Enforcement

Police executives should be aware of three main ways that law enforcement's access to digital crime scenes can be restricted.

- *Lack of capacity.* This includes issues such as lack of specialized training, specialized equipment, and other investigative resources within the law enforcement agency.
- *Technical barriers to access*. These barriers include unregulated encryption and communications technologies developed outside of a legal framework that allow for lawful access to data and communications.
- *Non-technical barriers.* This includes the imposition of customer notification requirements and legal barriers that arguably heighten the proof required to access evidence.

IACP's Law Enforcement Cyber Center

To assist law enforcement executives in meeting these challenges, the IACP, in cooperation with the Bureau of Justice Assistance and other law enforcement organizations, developed the IACP Law Enforcement Cyber Center (LECC)[1] to serve as a central clearinghouse for detailed resources managed by government, professional organizations, and subject-matter experts. The purpose of this site is to provide executives, senior leadership, and staff access to information, policy and other critical resources related to computer crime, cyber issues, and digital evidence.

1 http://www.iacpcybercenter.org/

Policy Considerations

Law enforcement agencies should consider implementing new or reviewing their existing policy, oversight, and operational controls to ensure that they are positioned to successfully meet the challenges posed by digital evidence. A few key steps are outlined below, in addition, the Law Enforcement Cyber Center provides links to resources which elaborate on these topics and information on further technical detail and support.

1 **Review recommendations from the IACP Technology Policy Framework[2], to include planning, use, and management of any technology in professional policing. This should include policies related to:**

- Technologies that generate, aggregate, and analyze data
- Technologies used to acquire process or handle digital evidence
- Ongoing management review of policies to ensure they are current

2 **Training and proficiency guidelines for all personnel in the collection, preservation, and analysis (where appropriate) of digital evidence, to include**

- First responders
- Investigators
- Crime scene specialists
- Forensic examiners

3 **Standard Operating Procedures and Policies for digital evidence that outline**

- Collection and acquisition
- Marking, documentation, and photography
- Preservation, packaging, and handling
- Storage, security, and accountability
- Access considerations
- Electronic storage considerations
- Disaster recovery and resiliency
- Deviations from policies

4 **Standards for validating proficiency of personnel performing critical digital forensic functions. This should include requiring**

- Certification and recertification of all personnel involved in the acquisition and examination of digital evidence
- Proficiency testing within the context of tools, tasks, conditions, and standards
- Quality review of examiner process and productions
- Process for correction and mitigation of errors

5 **Digital forensic tools, to include**

- Authorization to operate and use various technologies
- Context and limitation of appropriate forensic tools
- Validation and efficacy testing of forensic tools
- Quality review/documentation of tool validation and testing
- Process for correction and mitigation of errors

6 **Digital evidence metrics and impact on operations that address**

- Collection of data to measure use, context, and volume of digital evidence
- Analysis of data to understand specific relevance and importance of digital evidence to various statutes

7 **Challenges presented by new emerging or evolving technologies, such as**

- Cloud data
- Internet of things (connected/smart city technology)
- Social networks
- Vehicle informatics (the computers and systems in cars)

8 **Legal guidelines for digital evidence, such as those related to**

- Development of effective legal process, communications, and resources
- Collection, preservation, and analysis of remote digital evidence from third parties

9 **Protecting law enforcement agency systems against cyber threats from seized evidence, to include**

- General protection from malware, ransomware, and similar threats
- LEA system design to minimize risk to records and evidence
- Cyber security and risk management
- Assessment, evaluation, and testing

10 **Understanding encryption and its operational impact on evidence including**

- Its potential as a barrier to access
- Available legal options/resources for compelling access to encrypted digital evidence
- Available technical options/resources for access to encrypted digital evidence

2 The International Association of Chiefs of Police. (2014). "IACP Technology Policy Framework." https://www.theiacp.org/sites/default/files/all/i-j/IACP%20Technology%20Policy%20Framework%20January%202014%20Final.pdf. As of publication in September 2019, this document is currently being updated.

Going Dark

In addition to the challenges posed by the sheer volume of digital evidence, the issue of "going dark"—law enforcement's decreasing ability to lawfully access and examine digital evidence at rest and evidence in motion due to technical and nontechnical barriers— is increasingly placing public safety at risk.

Law enforcement often lacks the technical ability to access communications and information pursuant to a lawful court order. This inability to access digital communications data not only inhibits access to evidence in federal criminal and terrorism cases, but also keeps state and local law enforcement from being able to do their job effectively.

Unfortunately, current laws which were designed for non-digital communications and the development of new technologies, such as encryption products, which do not allow for third party access put public safety at risk.

Education and Outreach

To assist in addressing these concerns, law enforcement executives need to take the lead in ensuring that the public, private sector companies, and elected officials understand the impact and threat, that digital evidence access and going dark poses to communities. Below are some key points that should be stressed when discussing this issue with the public or elected officials.

- Digital evidence is a critical component in virtually all of today's criminal investigations.
- To safeguard communities, law enforcement needs access to appropriate legal authorities, tools, and training that are necessary to lawfully obtain and use digital evidence.
- Barriers to lawful access, whether technological or non-technological, should be minimized and factored into the development process by service providers and equipment manufacturers.
- Encryption without lawful access to encrypted content is a growing problem for law enforcement. This lack of access means cases are going unsolved, and the public is less safe.
- Policymakers should explore opportunities to enable increased lawful access to digital evidence. A lack of legal authorities regulating the retention and production of digital evidence by technology companies is driving negative public safety outcomes.
- Policymakers need to enact laws that require industry to ensure lawful access to digital evidence when a lawful court order is authorized and needed.
- Policymakers need to encourage industry leaders to identify approaches that protect privacy while still allowing lawful access to stored data and electronic communications that will help law enforcement conduct investigations and apprehend criminals and terrorists.
- Heightened legal requirements and other restrictions on law enforcement access to digital evidence impact law enforcement effectiveness, and therefore should be imposed with careful consideration of the consequences to ensure that law enforcement's ability to protect the public is not unduly impaired.

This document is a product of the IACP Digital Evidence Task Force:

Sandra Spagnoli
Chair, IACP Investigations Policy Council

John Letteney
Chair, IACP Technology Policy Council

David Rausch
Co-Chair, IACP Forensics Committee

John Grassel
Co-Chair, IACP Forensics Committee

James Emerson
Chair, IACP Computer Crimes and Digital Evidence Committee

Thomas Ruocco
Chair, IACP Police Investigative Operations Committee

For More Information, Please Visit

www.theIACP.org/resources/law-enforcement-cyber-center

International Association of Chiefs of Police
44 Canal Center Plaza, Suite 200
Alexandria, VA 22314
703.836.6767 • fax 703.836.4743
www.theIACP.org