TAGCYBER

opentext™

Transforming Digital Forensics in Law Enforcement

Dr. Edward G. Amoroso
Chief Executive Officer, TAG Cyber
Distinguished Research Professor, NYU

The law enforcement community has been a major consumer of digital forensic tools. As technology evolves toward zero trust and public cloud, law enforcers will require new forensic capabilities from their platform partners for the collection, analysis, and presentation of evidence.

Introduction to Digital Forensics

Modern criminals rely heavily on mobile devices, personal computers, and even cloud-based services to plan and coordinate their unlawful activity. As a result, important evidence will typically exist across criminal devices and systems in the form of logs, emails, texts, files, and images. Law enforcers thus have strong incentives to establish digital forensic capability to obtain desired evidence and to derive other useful data such as device location and usage statistics.

Sadly, a recent example at the US Capital illustrates the central role mobile devices play in providing digital evidence of crimes. The FBI and other law enforcement teams are relying heavily on video and other mobility-based information, mostly posted to social media, to identify and arrest suspected criminals. This is a sad and unfortunate case, but it does demonstrate the general principle here regarding mobile forensics.

For this reason, law enforcers (many of whom shift to corporate investigations teams) both in the United States and other countries, have been a key influencer of digital forensic capabilities. Such influence has been enabled by law enforcers staying up to date on the best available commercial and open-source forensic tools, as well as providing practical guidance and feedback on how existing platforms can be optimized to support their forensic needs, particularly as technology evolves.

This report outlines several key platform issues that the law enforcement community should consider as they develop and optimize their digital forensic needs. The report starts by summarizing the existing baseline capabilities supported in existing commercial platforms, and then continues with a set of recommended features that should be demanded from forensic providers as technology evolves toward zero trust security and public cloud usage.

Digital Data for Law Enforcement

The existing use of digital forensics platforms for law enforcement centers primarily on the collection, preservation, analysis, and reporting of evidence from the devices, systems, and services that are being used by individuals and groups of interest. As such, the forensic tools selected most often by law enforcers have tended to provide support for the most popular digital technologies, since these are likely to arise in the context of an investigation.

As such, it is straightforward to identify the existing baseline device, system, and service feature requirements for digital forensic support of law enforcement. These current and common features, which obviously must integrate with both digital forensic methodologies and law enforcement processes, include the following rich data sources:

Mobiles
In the course of most current law enforcement investigations, the collection of evidence from mobile devices will eventually arise. As a result, digital forensic extraction from mobile devices, usually iPhones or Android devices, has become a staple of law enforcement work during the past decade.

Apps
To support law enforcement investigation, integration with mobile and web apps has become an important functional requirement. This is helpful to investigators who use a toolkit with different application functions to support preservation, analysis, or reporting.

PCs
The collection of evidence from PCs has been the most traditional means for evidence collection, and it continues to the present day. Whether from Windows PCs or Macs, this collection requires tools that can read file systems, directories, memory, and disks, even in the presence of encryption.

Servers
Collecting data from servers traditionally involved seizing physical hardware. This has since evolved to the collection of virtual images, since server technology has progressed considerably in the past few years. This has the advantage of supporting scale, but it requires more modern extraction tools.

Networks
Collecting data from networks is influenced by speed, capacity, and access opportunities. More recently. However, the ubiquity of encrypted data transmission complicates law enforcement access where pre-coordination (e.g., CALEA) has not been arranged.

These primary traditional technologies have been complemented by familiar additional devices targeted by law enforcers such as memory sticks, printers, and other electronic components. The common denominator has been that such technologies might include relevant evidence and must therefore be interrogated in the course of an investigation. Existing platforms are generally quite good in supporting these well-known extraction points.

Integrating Forensics with Investigative Cycle

The modern law enforcer follows standard processes and cycles as they handle digital evidence during criminal investigations. A typical cycle includes three data-centric tasks combined with three analytic and consultative tasks – arranged in a continuous process. The data centric tasks – collect, check, connect, as one might expect, require tight integration with the digital forensic platform in order to support the analytic tasks – construct, consider, consult.

One might view the collect, check, and connect tasks as dealing more with raw data and intelligence, and the construct, consider, and consult tasks as combining data and intelligence into scenarios and conclusions. In each case, however, the underlying platform supporting digital forensics provides essential support to the law enforcer, either through direct, on-demand access to required data, or through stored information to support analysis (see Figure 1).

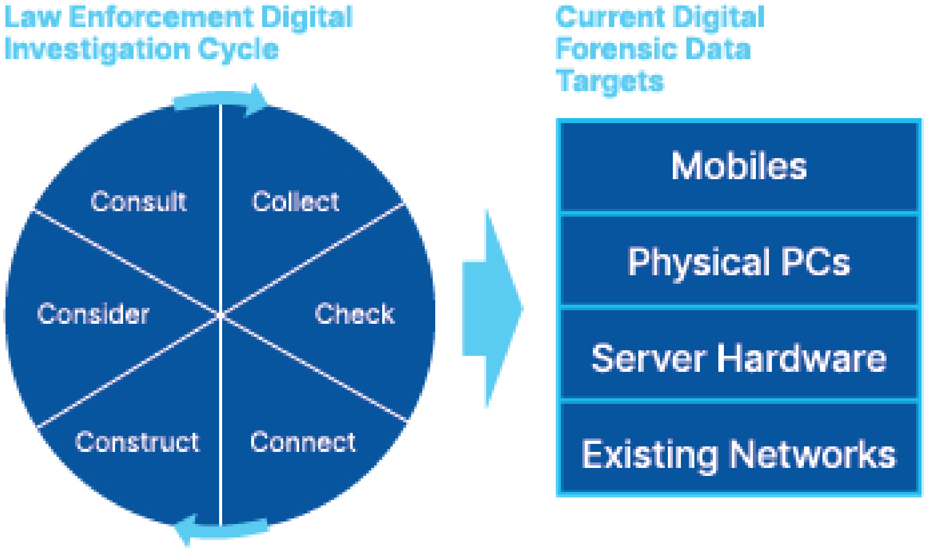


Figure 1. Current Forensic Data Targets in Law Enforcement Investigations

New Forensic Requirements for Law Enforcement

The challenge is that with massively expanding, shifting, and advancing capabilities in modern technologies for both consumers and business, the law enforcement community has had to shift its emphasis for data extraction. This shift extends obviously to the platforms used by law enforcers for digital forensic collection and analysis – and this includes both commercial tools as well as open-source software components.

The most obvious change that is directly relevant to modern digital forensics platforms is that the range of devices, systems, and networks applicable to law enforcement investigation has expanded dramatically. This can be best understood by listing the most significant advances that have occurred in both enterprise computing and consumer-based technologies. Each of these advances introduces new challenges for data-oriented and analysis-oriented tasks:

Shift to Public Cloud

Despite some early hesitation among investigators, an obvious shift has involved increased use of public cloud infrastructure, software, and services. Law enforcers have thus had to expand their focus from enterprise-centric devices, systems, and networks to cloud-based resources managed by third parties such as Microsoft, Google, and Amazon. Digital forensic platforms must therefore include means to lawfully collect, process, and analyze cloud-based data through whatever public or private interfaces are available.

Increase in SaaS-Based Services

An additional shift involves increased use of SaaS-based applications to support business functions such as payroll, finance, and sales. The implication is that many organizations have been able to dissolve entire business functions such as human resources in favor of using a suitable SaaS tool. Digital evidence is thus likely to be stored within these third-party services, which implies that digital forensic platforms must have the ability to lawfully reach into their infrastructure.

Increase in IoT Devices

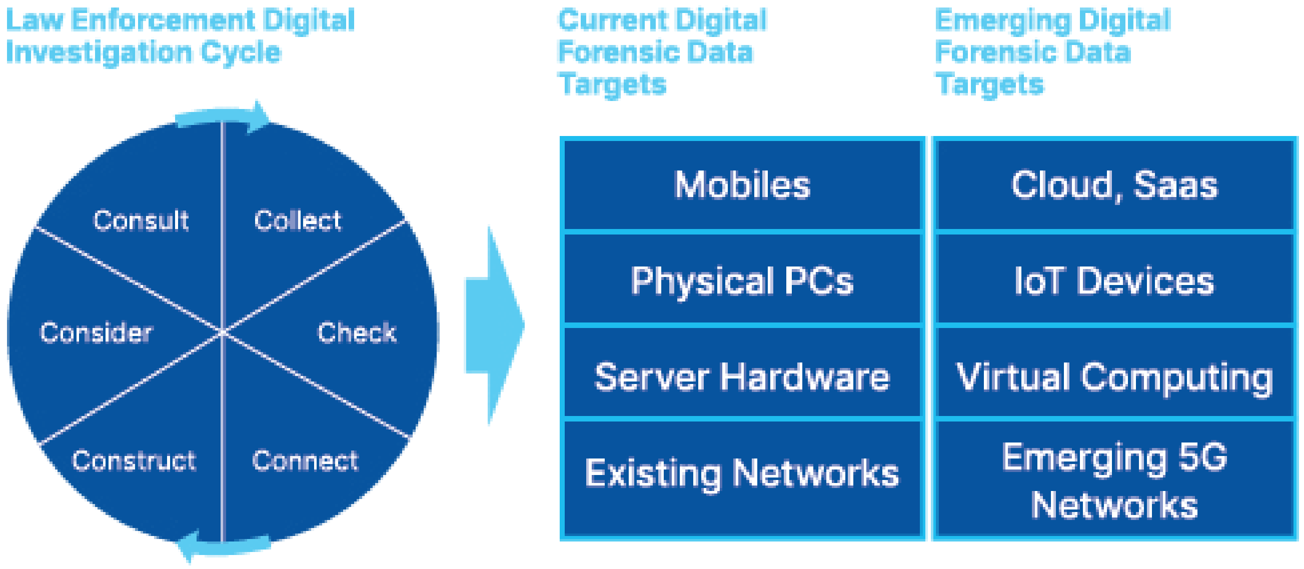
IoT devices tend to generate relevant forensic evidence in situations that involve operational functions. If, for example, some law enforcement case involves use of IoT devices in a factory, manufacturing plant, or industrial facility, then the digital forensic platform would require means to lawfully collect data from the IT or network systems that are monitoring or managing the devices of interest.

Ubiquity of 5G Services

The emergence of 5G wireless infrastructure services will create new connectivity between users, systems, and applications that can extend evidence collection to a larger set of potential targets. This makes sense because 5G services will be so attractive, feature-rich, and ubiquitous that increased connectivity will certainly result. Law enforcement will thus require digital forensic platforms that can lawfully and legally integrate with 5G wireless infrastructure.

Virtualization of Computing

The traditional concept of seizing server hardware to collect evidence has been largely replaced with the virtual equivalent that is more focused on software images. The concept expands dramatically as virtual computing becomes even more prevalent and distributed across global infrastructure. Tools to deal with micro-segmented applications and dynamically provisioned workloads are thus required for law enforcement teams to keep up with modern technology.



Current Digital Forensic Data Targets	Emerging Digital Forensic Data Targets
Mobiles	Cloud, Saas
Physical PCs	IoT Devices
Server Hardware	Virtual Computing
Existing Networks	Emerging 5G Networks

Figure 2. Emerging Forensic Data Targets in Law Enforcement Investigations

Luckily, the law enforcement digital investigative cycle has been sufficiently general in design that little adjustment is required in the various tasks and their respective interaction. Within each task, however, reaching into these new data targets such as cloud and SaaS require new legal, policy, and technical considerations. They also introduce new training requirements for law enforcers, especially ones who have more traditional skills.

Market Landscape: Digital Forensics for Law Enforcement

To assist law enforcement buyers in selecting and procuring the best available digital forensic platforms to support modern digital investigations, the following questions are offered that should be posed to potential commercial providers during the source selection process:

Does the platform support data collection and analysis from public cloud and SaaS?

The platform should demonstrate integration with public cloud services from Amazon, Microsoft, and Google, as well as for popular enterprise SaaS applications such as SAP and Salesforce.

Does the platform support data collection and analysis from IoT devices, including 5G connected?

The platform should demonstrate integration support for data collection from a range of modern IoT and select industrial devices, including ones connected to and supporting 5G infrastructure services.

Does the platform include sufficient capacity to integrate with high-speed network capture?

The platform should demonstrate the ability to handle the data volumes and formats that emerge with high-speed network capture from large backbones and other transport.

Does the platform include integration with tools that crack, decrypt, or cryptanalyze cleartext?

The platform should demonstrate the ability to integrate with cracking, decryption, and cryptanalysis tools, given the increased use of encryption on applications, systems, and networks.

TAGCYBER

About TAG Cyber

Founded in 2016 by Dr. Edward Amoroso, TAG Cyber provides world class research and advisory services, with advanced market reporting for cyber security teams. TAG Cyber's goal is to bridge the communication gap between commercial security vendors and enterprise practitioners. TAG Cyber's insights are delivered through an innovative on-line portal with support for expert on-demand research.

References

[1] DHS Science and Technology Directorate, Cybersecurity Forensics Support for Law Enforcement, https://www.dhs.gov/sites/default/files/publications/Cyber%20Forensics%20Support%20for%20Law%20Enforcement-508_0.pdf