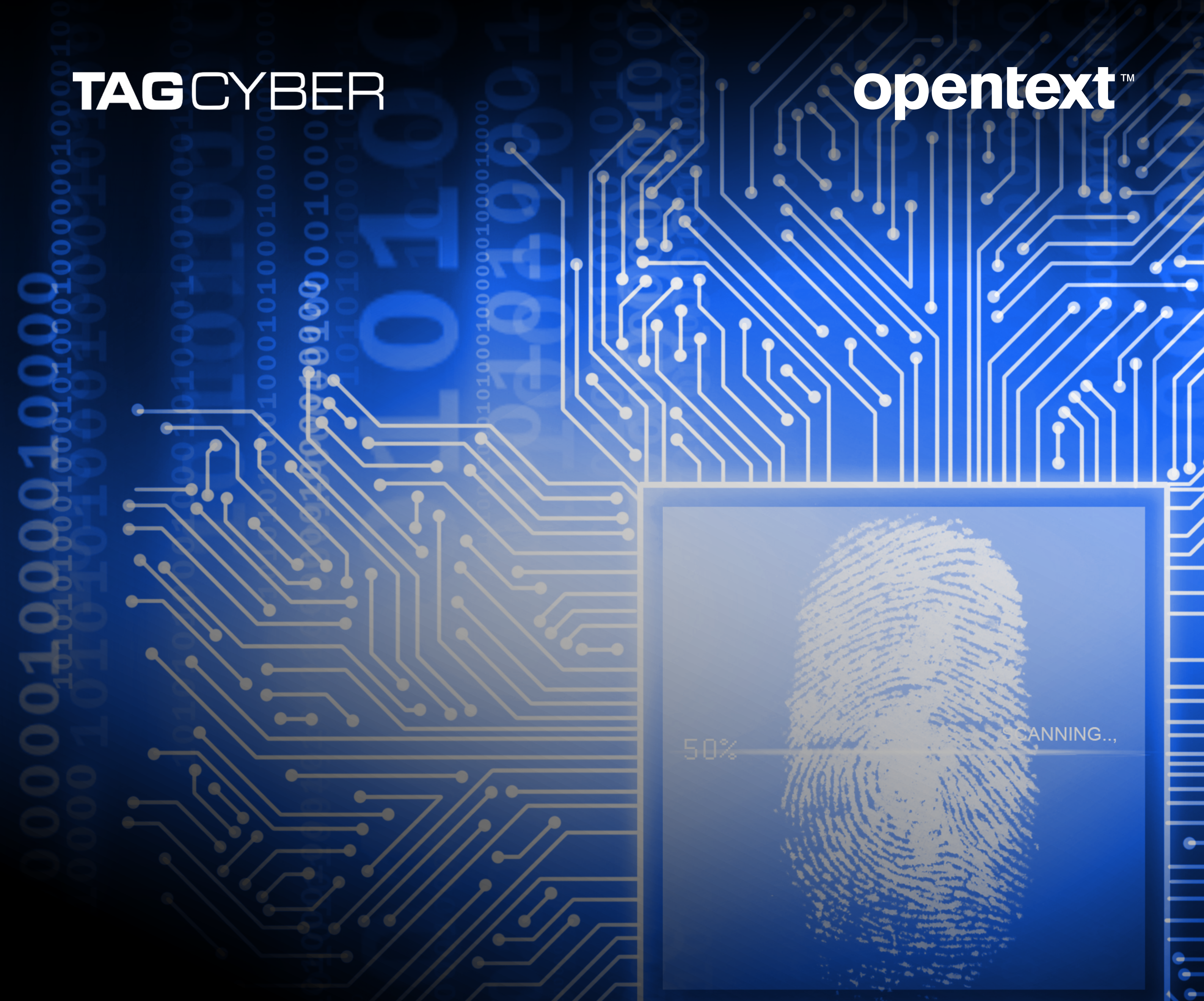
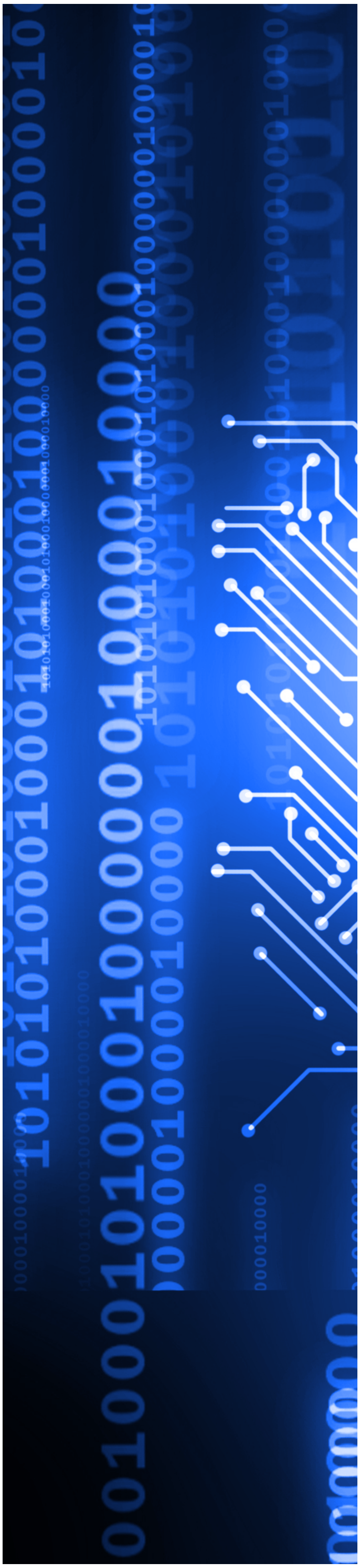


Information Assurance and Digital Forensics: A Deepening Relationship

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

Modern digital forensics provides essential technical support for eDiscovery tasks. This interaction, referred to as information assurance in some contexts must also take into account the shift in data and information processing toward multi-cloud and off-network devices, systems, and applications.



Introduction to Enterprise eDiscovery

The familiar process of eDiscovery, which can be thought of as a subset to information assurance, involves the discovery and preservation of electronically stored information by officials, usually as part of some legal procedure such as a lawsuit. Other regulatory instruments such as the Freedom of Information Act (FOIA), GDPR in the UK, and others around the world also commonly prompt eDiscovery-like activity by data owners. International eDiscovery can be especially complex, given the challenges of location, local laws, and even culture.

The typical eDiscovery process starts with a legal representative obtaining authority from a court to request that a data owner identify and preserve some designated artifact. This is often easier requested than done, because not every business enterprise has a good understanding and inventory of their data objects. The eDiscovery process is particularly challenging when designated objects are stored in a public cloud (see NIST guidance on this issue for eDiscovery [1]).

As one would expect, subsequent eDiscovery process steps will require the use of automated platform tools for digital forensic review, analysis, and preservation. This is especially important in cases where the requested artifacts cannot be easily identified or reviewed. In the best circumstances, the digital forensic tool will be selected with future eDiscovery requirements in mind – and this note is designed to help enterprise teams follow this desired path.

Data Discovery and Risk Management

Laptops, desktops, servers, Internet of Things (IoT) devices, and content repositories represent the backbone of a modern organization. The data on these components drive business; precise visibility into and control of their stored information is thus critical to expose, understand, and manage risks. Maintaining control of information has never been more challenging. Employees are creating, editing, transmitting, and deleting information every day – which underscores the importance of such data to the eDiscovery process.

Organizational data will also exist across multiple hyperscalers such as Google, Microsoft, and Amazon – so highly distributed workforces are using numerous cloud repositories to collaborate with partners and peers. To solve for this challenge, organizations are beginning to use data discovery platforms to reach across the entire data estate in a comprehensive and defensible manner. From inside counsel and compliance to information security teams, the entire organization benefits from a complete understanding of sensitive data usage and locations. Inside counsel must meet comprehensive discovery obligations in a timely manner.

Compliance teams need to enforce internal policies and ensure that medical, financial, and customer data remains private and protected. Information security teams must understand which areas of IT infrastructure represent likely targets for insider or external threats. Implementing data discovery based on forensic principles is the only approach that delivers the visibility and control required to uncover relevant electronically stored information (ESI) accurately and completely and reveal sensitive data risks, no matter how well hidden.

Digital Forensics for Enterprise eDiscovery

In addition to the importance of data discovery in the context of risk management, it is important for enterprise teams to understand the forensic requirements for eDiscovery. Luckily, this is a mature process generally well-understood by practitioners and generally supported by a partnership between IT operations teams, CISO-led security teams, and legal counsel. Popular reference models exist to help guide and organize the various eDiscovery tasks, including how they interact and feedback to the information governance base (see Figure 1).

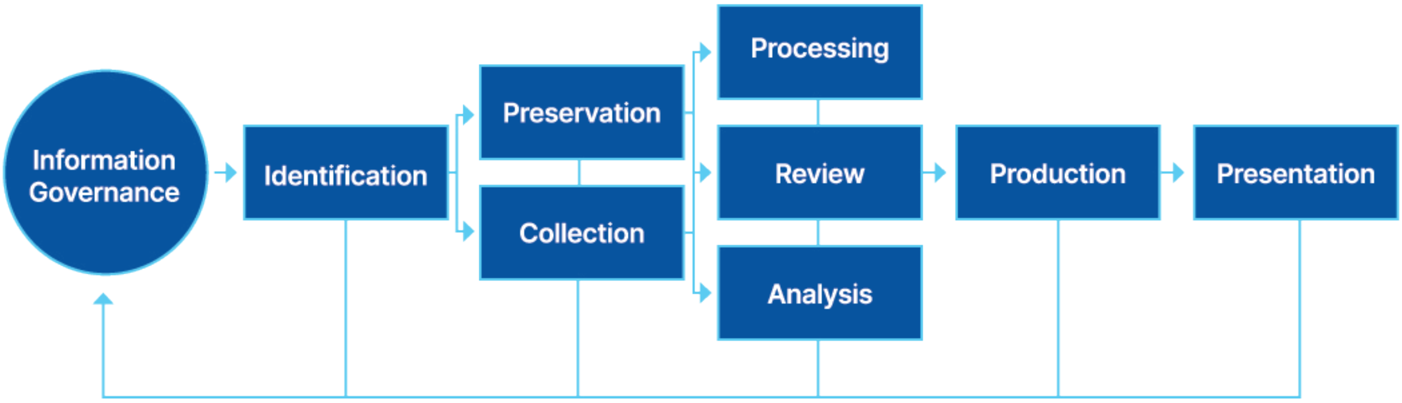


Figure 1. Familiar eDiscovery Reference Model

Despite the familiarity of the information governance, identification, preservation, collection, and other tasks involved in eDiscovery, two new considerations have arisen that require attention during eDiscovery due to the on-going changes occurring in modern technology and enterprise. The first involves the massive shift of enterprise computing to public cloud services and the second involves the growing need for digital forensic support during eDiscovery.

Shift to Public Cloud

The shift for most enterprise computing, including for third parties, to off-network use of systems and applications usually involves heavy reliance on public cloud services from companies such as Amazon, Google, and Microsoft. It also includes increased use of SaaS-based capabilities from companies such as Salesforce and SAP. To that end, the eDiscovery process must be extended to include coverage across this new infrastructure.

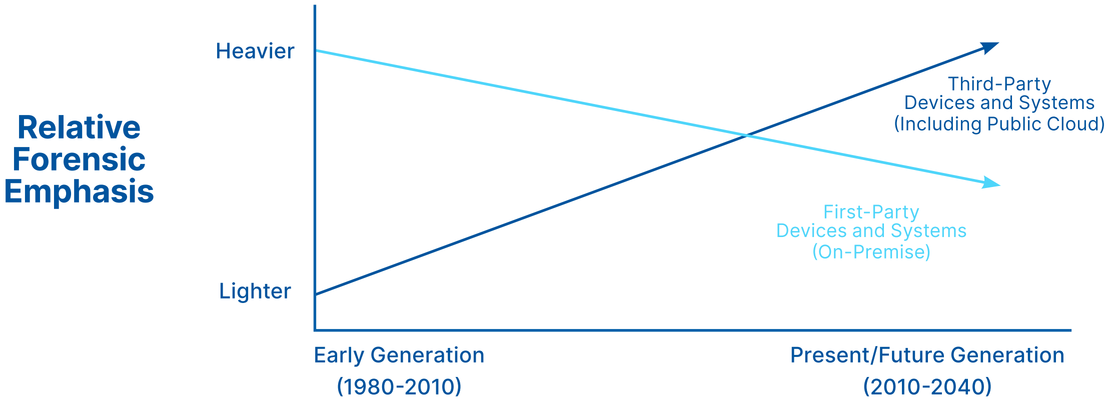


Figure 2. Extending eDiscovery to Public Cloud

Need for Digital Forensics

A corresponding shift in modern enterprise computing involves less obvious extraction of data from desired devices, systems, applications, and services. To that end, modern digital forensic support is more critical than ever in supporting the eDiscovery needs of an enterprise. Commercial platforms for digital forensics must have tight integration with the eDiscovery process and toolset – and this must extend to use of public cloud services.

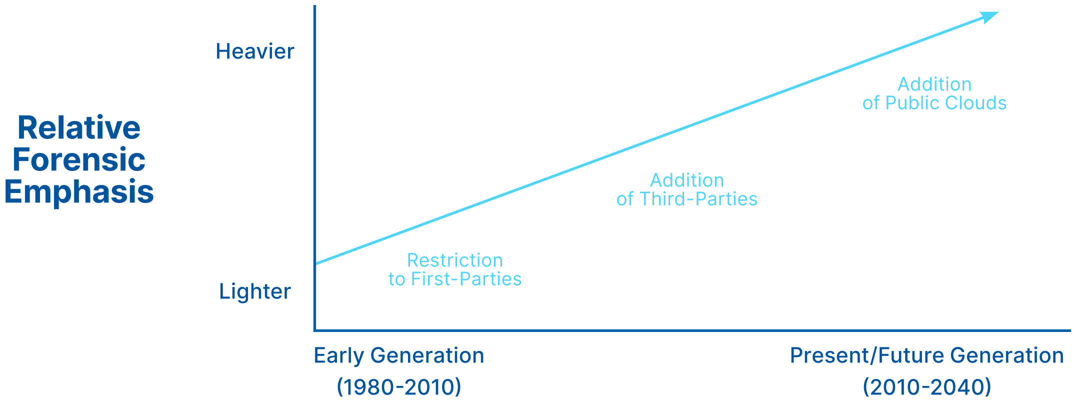


Figure 3. Extending Digital Forensics to Public Cloud

Market Landscape: Information Assurance and Enterprise eDiscovery

The challenge in selecting a commercial platform for modern digital forensics involves ensuring the correct set of requirements to support the evolving eDiscovery needs of the enterprise. To that end, we offer below a set of questions that can assist teams with proper source selection of a commercial platform partner. Each question tracks closely with the reference model introduced above.

How does the digital forensic platform provide support for the information governance component of eDiscovery?

The objective of good enterprise information governance should be to maximize policy, process, and control transparency to support on-going business operations and digital transformation. This implies that for organizations who support information governance properly, the corresponding use of digital forensics to collect, preserve, and analyze designated data should be relatively straightforward.

The challenge, however, is that most organizations struggle with information governance, which implies that the digital forensic platform must compensate for any weaknesses. This includes forensic platform capability to discover and collect electronically stored information in enterprise environments where storage, retention, and other forensic relevant information might not be optimal.

How does the digital forensic platform provide support for the identification task in eDiscovery?

The primary task for the forensic platform in the context of identification is to assist in the more subtle discovery of electronically stored information on devices and systems for which this might not be immediately evident. Increasingly, forensic support is needed to discover critically important data that might be hidden, deleted, or even intentionally destroyed by a malicious insider. The modern digital forensic platform must support this objective.

How does the digital forensic platform provide support for the collection and preservation tasks in eDiscovery?

The collection and preservation of electronically stored information comprises important tasks to support the needs of a given legal procedure. The digital forensic platform must support the need to extract data and preserve it without change or damage to preserve key evidence. This task requires coordination between the forensic platform and other IT tools used for collection and preservation.

How does the digital forensic platform provide support for the processing, review, and analysis tasks in eDiscovery?

The processing, review, and analysis of electronically stored data will generally be performed through a combination of automated and human activity. Integrating the digital forensic platform into this analysis ecosystem thus requires procedural coordination for the human analysts, as well as automated interfaces (usually an application programming interface) for sharing data between the forensic platform and other analytic tools.

How does the digital forensic platform provide support for the production and presentation tasks in eDiscovery?

The final tasks in support of the eDiscovery process include production and presentation of collected and analyzed results. This can be informal, such as for internal managers, or more formal, such as in support of depositions, trials, or court hearings. As such, the digital forensic platform must include capabilities to integrate findings into such production and presentation activities by the eDiscovery team.

References

[1] NIST Information Technology Laboratory, 5.5 eDiscovery, updated March 23, 2018.
https://www.nist.gov/itl/55-ediscovery