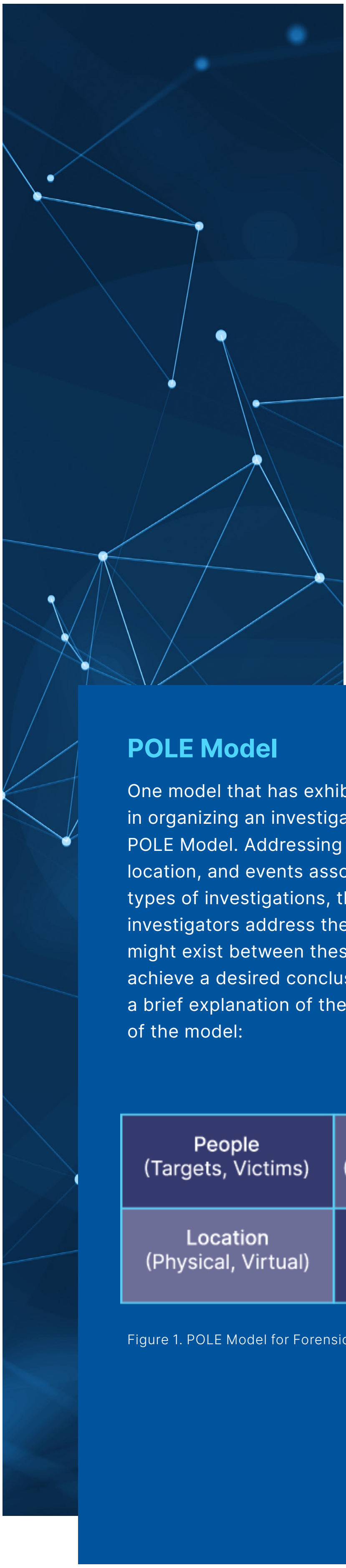
TAG CYBER

opentext™

Modernizing Enterprise Forensic Investigation

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

Enterprise security teams agree that insider threats represent the greatest malicious threat to their critical resources. Modern enterprise forensic investigation now includes off-network, chain of custody, and cloud measures to address this significant and growing risk. This paper introduces the discipline and includes questions to assist in selection of a suitable commercial forensic platform.



Introduction to Modern Enterprise Forensic Investigation

Developing a modern cyber investigative infrastructure and set of strategies is an essential component of enterprise incident response planning. This is easier said than done, so security teams are advised to learn as much as they can about how the process of modern enterprise forensic investigation has evolved. They are also advised to select commercial platforms that ensure good coverage and support during investigations. This report is intended to help on both fronts.

Modern enterprise security teams will generally agree on the need for proactive security to prevent breaches, detection-based security to observe incidents while they proceed, and reactive security to support incident response after a breach. These are familiar considerations for working security professionals, and they form the backbone for security compliance frameworks such as the NIST 800-53 Rev 5 requirements [1]. They also help to provide context for current forensic investigative methods.

Current Forensic Investigation Models

Many conceptual models exist to help organize the many decades (even centuries) of experience and insights developed by traditional investigators [2]. Such models allow the expertise developed by police forces, negotiators, and other experts working on traditional crimes and incidents such as terrorism and kidnapping into corporate situations such as cybercrimes, data theft, privacy violations, digital breaches, and enterprise attacks. Two representative models are briefly introduced below.

POLE Model

One model that has exhibited great usefulness in organizing an investigation is the so-called POLE Model. Addressing the persons, objects, location, and events associated with different types of investigations, the model helps investigators address the relationships that might exist between these different entities to achieve a desired conclusive outcome. Here is a brief explanation of the various components of the model:

People (Targets, Victims)	Objects (Evidence, Artifacts)
Location (Physical, Virtual)	Events (Scans, Reviews)

Figure 1. POLE Model for Forensic Investigation

Persons

These include the targeted victims, individual or group, of a given breach or incident. They can also include the threat actors, enterprise defenders, and other individuals or groups relevant to an incident.

Objects

These include any information or other artifacts that provide evidence of the breach. This includes devices, systems, networks, and other data repositories available either in real-time or after the fact as part of a log trail or archive.

Locations

These include the virtual and physical attributes that help designate where attacks originate, traverse, proceed, and conclude. This can include domains, cloud services, networks, and various other locational data of interest.

Events

These include the specific actions that occur during the breach, as well as during the investigation. Maintaining a tally of the breach, as well as all tasks being performed by investigators during their review work is essential to developing an accurate conclusion.

Extraction Model

One key consideration in modern enterprise forensic investigation is the importance of extraction in the context of the POLE model. Entity and information extraction represent the primary objectives in most investigations, so process models must be developed to guide the forensic team through the required steps. Several models have been proposed [3], but the essential elements of any process model for extraction include the following determining steps:

Stage 1
Determining access methods

Stage 2
Mitigating access risks

Stage 3
Discovering information importance

Stage 4
Data extraction

Stage 5
Storing and querying extracted information

Stage 6
Application validation

As one might expect, investigators must collect data in each of these areas and then establish detailed connection, dependencies, data flows, or other relations between the entities. This is best done proactively and in real-time, but most enterprise teams tend to perform investigations as part of response actions after something has occurred. Behavioral conclusions can be drawn from this type of analysis, because people, objects, location, and events are the key indicators in a compromise.

Required Capabilities for Modern Enterprise Forensic Investigation

The modern enterprise forensic investigator must ensure that their processes are supported by suitable tools, systems, and infrastructure that match up with the type of attacks that occur today. Regulator challenges also drive the need to support investigations in modern, work-from-home infrastructure. This implies that the old methods of seizing devices and reviewing them locally and off-line simply do not cover the types of breaches being investigated by modern cyber investigators.

Since computer forensics is a relatively mature discipline, most enterprise teams have a baseline set of requirements that they expect from their vendors. Little change would be expected, therefore, in the forensic support necessary to collect data from and analyze computers, workstations, and networks. Similarly, most legal and reporting requirements are unlikely to change with advances in modern cyber infrastructure including cloud.

With these on-going changes in technology and architecture, however, several forensic capabilities must be updated to reflect the current typical enterprise. Below are three new capabilities that must exist in the platforms used today by cyber forensic experts and their associated investigative processes. Enterprise teams should be aware of these changes, including how they will influence vendor selection and process design.

Off-Network Analysis

With massive changes in how employees, contractors, and third-party teams support enterprise work, forensic methods must make the necessary adjustments to support investigations. The biggest change is the increase in off-network and off-VPN cases, especially with massive work-from-home initiatives, that will typically arise in the context of an incident. This implies that the forensic platform and associated processes must be capable of collecting, analyzing, and processing off-network devices and systems.

One means by which this off-network and off-VPN analysis can be supported is through agnostic hosting capability for any digital forensic platform. In short, the platform and its associated tools must be deployable wherever necessary. This will require the ability to seamlessly connect to the existing tools and systems in the off-network environment of interest. Public cloud infrastructure (see below) is one of the more obvious cases for such required interaction.

Modern Chain of Custody

A second change involves the chain of custody requirements investigators rely on to work cases, especially in the context of the POLE model. Since chain of custody involves tracking versions, releases, configurations, and other status of objects, modern methods such as DevOps, which incorporate rapid automation and fast Agile process steps, tend to complicate tracking and measurement. Investigative platforms must therefore include support for such custody-based identification and analysis.

For chain of custody to work best, the digital forensic platform must integrate with existing ecosystem tools such as SIEM or SOAR platforms. This implies that the platform should support application programming interface (API)-based collection of information. It should also have the ability to work via connectors or integrations with security tools such as the security information and event management (SIEM) system or any security operations-related tools.

Cloud Infrastructure

Perhaps the most obvious capability required for modern enterprise forensic investigations is the shift in emphasis to cloud. When artifacts and other objects are hosted in public or hybrid clouds, tracking their status, including chain of custody, can be tough to manage. This is particularly true in outsourced or SaaS-based situations where a third party is managing major aspects of some system or workload of interest. Many of these cloud forensic challenges are explained in a recent NIST document [3].

The primary functional consideration is that the digital forensic platform must have the ability to pull cloud-hosted data seamlessly from the local environment. This can include storage objects in services such as Amazon Web Services, Microsoft Azure, and Google Cloud Platform, or it can include interfaces to SaaS-based services that host relevant information. Obviously, if cloud infrastructure data is required, then the forensic team might need to coordinate directly with the cloud hosting security team.

Market Landscape for Modern Enterprise Forensic Investigation

In the early days of computer forensics, investigators had to make use of whatever tools were available, and this often involved open source utilities that were acceptable, but perhaps not optimal to a given security case. Windows, Macintosh, UNIX, and mobile environments were the primary target environments, and experts relied on empirical guidance from other practitioners to learn the best means for supporting forensic work [4].

Today, the commercial marketplace is mature and vibrant for enterprise forensic investigation support. The challenge, in fact, is no longer whether a useful software tool exists to handle the cyber investigative needs of an enterprise team. Rather, security forensic experts today must decide on the optimal suite of tools and services that can support their practical needs to address investigations and insider threats [5] in a cost-effective manner.

To assist with this decision, we offer below a set of questions (grouped into traditional and augmented) that can be used to guide selection of the right set of commercial vendors for forensic investigatory support. The goal here is to assist the enterprise investigator; but law enforcement officials, regulatory teams, examiners, researchers, consultants, executives, and even commercial vendors should also benefit from the questions we include.

Traditional | *What is your capability for standalone computer devices, workstations, and networks?*

Modern forensics certainly extends to cloud and other non-traditional infrastructure, but any commercial platform must maintain work-class capability to deal with evolving devices, next-generation software, and evolving device form factors. Enterprise buyers should make sure their selected commercial partner maintains focus on these foundational concerns.

Traditional | *How does your platform support duplication and hashing to validate collected versions?*

Key requirements during any digital forensic investigation include the ability to duplicate artifacts, and to validate the correctness and accuracy of collected or copied versions. Hashing is a common means for performing this vital task, and any selected platform must demonstrate its capability in this essential aspect of digital forensics.

Traditional | *Does your platform include support to demonstrate repeat instances of an analysis?*

An additional key requirement for digital forensics is that an analysis must be easily demonstrable as a repeat instance. This is especially important for law enforcement, where an analysis will serve as legal evidence, but it is just as essential to enterprise instances where insider consequence or other related incident response actions will hinge on demonstrated confidence in the analysis.

Augmented | *Does your platform integrate with major cloud providers such as AWS, GPC, and Azure?*

A new consideration for digital forensic platform selection involves checking how well the tools can integrate with popular public cloud services. Just about every enterprise uses cloud services from Amazon, Google, and Microsoft, but if other cloud services (e.g., IBM) are being used, then these should be included in any source selection materials sent to prospective forensic vendors.

Augmented | *Does your platform integrate with major SaaS vendors such as SAP, Oracle, and Salesforce?*

A similar requirement is needed for hosted, SaaS-based services that might be in use by the enterprise. This commonly includes services from SAP, Oracle, and Salesforce, but just as with public cloud services, if other SaaS-based services are in use (e.g., ADP, Gusto), then these should be included in any solicitation materials for prospective forensic platforms.

Augmented | *How do you support modern chain of custody across multi-cloud environments?*

The chain of custody requirement is certainly not new for digital forensic experts, but with the introduction of cloud, SaaS, and other non-traditional infrastructure components (including in use by third parties), establishing an unbroken chain of custody can be challenging. Any selected digital forensic platform must have utilities to support this vital task.

Augmented | *Does your tool integrate with a modern threat intelligence vendor or data source?*

Threat intelligence has become particularly important to provide context to the digital forensic analyst. Any prospective forensic platform provider must therefore demonstrate either pre-integrated alliances with good threat intelligence vendors or must include an open interface through which intelligence feeds might be integrated by the enterprise.

Augmented | *Does your tool integrate with modern endpoint security solutions?*

Digital forensics benefits from tight integration with endpoint security tools. In most cases, this will require connection between the forensic platform and the existing commercial endpoint agent. In some cases, however, your digital forensic solution vendor might offer its own endpoint security solution. If you choose this route, it can ensure more commonality in information formats during investigations.

References

[1] Security and Privacy Controls for Systems and Organizations, NIST SP 800-53 Rev 5, September 2020. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[2] Séamus Ó Ciardhuáin, "An Extended Model of Cybercrime Investigations," International Journal of Digital Evidence, Volume 3, Issue 1, 2004. https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B70121-FD6C-3DBA-0EA5C3E93CC575FA.pdf

[3] Timothy Pavlic, et al, "Developing a Process Model for the Forensic Extraction of Information from Desktop Search," The Journal of Digital Forensics, Security, and Law, Volume 3, Number 1, 2008. https://commons.erau.edu/cgi/viewcontent.cgi?article=1036&context=jdfsl

[3] NIST Cloud Computing Forensic Science Challenges, NISTIR 8006, August 2020. https://csrc.nist.gov/publications/detail/nistir/8006/final

[4] Handbook of Digital Forensics and Investigation, Eoghan Casey (ed.), AP, 2010. https://www.amazon.com/Handbook-Digital-Forensics-Investigation-Eoghan/dp/0123742676

[5] Dawn Capelli, et al, The CERT Guide to Insider Threats, Pearson Publishing, 2012. https://www.amazon.com/CERT-Guide-Insider-Threats-Information/dp/0321812573