Digital Investigation Workforce Development

Dennis Allen

March 2012

Software Engineering Institute | Carnegie Mellon

This material is based upon work supported by United States Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

This report was prepared for the

Contracting Officer
ESC/CAA
20 Shilling Circle
Building 1305, 3rd Floor
Hanscom AFB, MA 01731-2125

Table of Contents

Introduction

Many threats face our internet-connected networks today: denial-of-service (DoS) attacks, viruses, worms, spam and phishing emails, physical security threats, exposure of sensitive information, and numerous others. Network defense strategies are continuously playing catch-up to the latest attacks perpetrated by cyber criminals and malicious insiders. Unfortunately, incidents will occur on almost all networks that impact the confidentiality, integrity, or availability of critical data and systems. Furthermore, cyber criminals use obfuscation techniques such as encryption, steganography, anonymous proxies, and even the leasing of computer robot networks (botnets) [Bosworth 2009, pp. 15-30]. When a compromise occurs, system administrators, incident-handling personnel, and digital investigators may all, in some way, be responsible for responding to the event and collecting evidence. Important assets and data must be collected, analyzed, and protected in a forensically sound manner. To ensure that, those responsible for data acquisition, assessment, and reporting must have the necessary knowledge, skills, and experience.

As more and more criminal acts are committed in cyberspace, law-enforcement agencies, businesses, and other organizations must develop new digital investigation capabilities [Kanellis 2006, p. 292]. The intent of this paper is to identify those competencies and what readers must learn about in order to develop them.

Define Program Objectives

A digital investigation program and capability can vary greatly between organizations. Investigators in small law-enforcement organizations may have a minimum set of skills for collecting and preserving evidence. Even then, their knowledge of information systems may be very limited, and their exposure may be confined to only crimes facilitated by computers rather than true cybercrimes that target computers, services, and data. Officers may not have the opportunity to learn the intricacies of computer networks and master operating systems. As a result, the program objectives for these small organizations may never go beyond evidence collection.

Other federal agencies may focus on financial crime or the prevention of child exploitation. With more manpower, financial resources, and jurisdiction, these agencies often institute specific analysis teams while training all personnel to triage cyber incidents. With national and international responsibilities, these law-enforcement agents may be required to gain advanced skills in system and network operations and incident response, in addition to computer forensics. Furthermore, because they are often dealing with criminal cases, more in-depth knowledge is required in legal areas such as federal rules of evidence, search warrants, protection of chain of custody, and expert witness testimony.

Many private organizations rely on internal information technology or security personnel for digital investigations, so they send them to formal education or professional training programs.

Through training, these organizations establish a broad computer forensics baseline capability that can be tapped when cyber incidents occur.

After an organization decides how many investigators it needs and what responsibilities they will have (acquisition, assessment, etc.), it must define exactly how those responsibilities will be carried out. For example, organizations responsible for Health Insurance Portability and Accountability Act (HIPAA) compliance must refine their capabilities to investigate the applications and systems that support processing this sensitive information. They must also know how and when to report compliance-related findings.

Organizations and agencies must anticipate the types of events they will investigate and know how to analyze all devices being used. For example, if all employees have iPhones, the computer forensics team must have the tools and expertise needed to investigate iPhone attacks and threats.

When establishing a digital investigation capability, an organization must align its services and training with its priorities. Technologies are always evolving, and new threats are constantly emerging. Just as defense-in-depth controls should be deployed and tuned over time to protect the organization's most critical assets, digital investigation capabilities must support the acquisition and analysis of mission-critical systems. As incidents occur and organizations learn more, they must refine their program objectives and competencies.

Establish Expertise Levels and Roles

Once an organization defines objectives for its entire program, it can assign specific tasks to team members. Such assignment can occur based on experience or expertise level; for example, entry-level investigators could be designated as apprentices or junior investigators. Then, after they gain the prerequisite skills and proficiency, they could be promoted to journeymen. Similar advancement criteria could lead to advanced or master levels of expertise. Additional responsibilities can be placed on more senior members to mentor and train those more junior. An important point of emphasis here is on assessment and the continuous demonstration of proficiency at each level.

In addition to defining levels of expertise, specific digital investigation tasks can help define team member roles. For example, some individuals may be responsible for the initial response to an incident. Their ability to successfully triage the situation and properly collect all the necessary evidence could dramatically impact the entire investigation. These collection agents must have the necessary skills to determine what digital evidence is needed and how to acquire it safely whether they are system administrators or law-enforcement agents.

After the data is collected, an analysis agent or examiner may get involved. Beyond safe collection and handling procedures, these team members should be proficient with the approved analysis tools and procedures. They should follow an established methodology but have the skills needed to adapt their investigation as circumstances may dictate. They must also be able to perform detailed analysis and provide meaningful reports.

The forensic examiner should be the primary contributor to the final digital investigation report. However, in some situations, the reporting agent may actually be a different member of the team who could be responsible for presenting findings to senior leaders within the organization. Post-mortem details including lessons learned and follow-up actions should be included in the report. The reporting agent must also possess the prerequisite knowledge and skills necessary to provide expert witness testimony in civil and criminal proceedings.

Last, but certainly not least, is the manager/supervisor. This individual is responsible for all aspects of the investigation ensuring that collection, analysis, and reporting functions all occur seamlessly. Quite often, the supervisor is also the reporting agent.

Develop Knowledge and Skills

It is entirely possible for bad investigations to lead to criminal or civil action against the investigating organization [Kanellis 2006, p. 312]. Employee terminations or even criminal punishments can be challenged if evidence is mishandled, misanalyzed, or just plain missing. The expertise of everyone involved could potentially come into question. To ensure success, digital investigation teams should continuously develop their knowledge, skills, and experience in the areas described below.

Baseline Skills

Digital investigators come from varied backgrounds. There are, however, two common scenarios. The first involves traditional law-enforcement agents who have developed computer skills on the job or been assigned to specific cyber-related task forces. The second group consists of information technology (IT) professionals who have a strong computing background and are now advancing into the digital forensics realm. Each group has distinct advantages and challenges.

Traditional law-enforcement agents have a strong understanding of the law. Specifically, they understand federal rules of evidence, chain-of-custody procedures, how to present evidence in court, civil rights protections, and other legal issues governing the search and seizure of various assets. However, most agents do not have the technical education, training, or experience that a computer professional has in areas such as operating systems, desktop and server applications, network devices, communication protocols, and intersystem dependencies. Likewise, the IT specialist has little experience in the areas of law enforcement. To build an effective capability, digital investigators must develop a sound baseline of both skills in IT and knowledge of applicable legal statues.

Technical Skills

Technical skills in the context of this report refer to a minimum amount of knowledge recommended for all digital investigators to effectively acquire and analyze digital evidence. To that end, a computer forensics program should ensure that all team members have a strong understanding, and preferably some experience, in the following areas:

- **operating systems:** Knowing system boot options may provide investigators access to systems when user passwords are unknown. Investigators should understand how files are stored, deleted, and recovered. Familiarity with logging options and how the command history is saved can lead investigators to evidence not readily visible. Having extensive system administrator experience can help analysts determine which processes and files are legitimate, opposed to anomalies that may indicate a compromise. Other important components include memory page files, temporary files, system backup/restore information, password files, and databases like the Windows Registry. These can all provide vital information when analyzed properly.
- **file systems:** Operating systems use a variety of file-system types. Investigators should understand concepts such as file-block size, clusters, compression, encryption options, linking/shortcuts, and file attributes. They should know how file creation, modification, and deletion times are recorded. Having this knowledge supports examination activities and ensures the proper file-system type is selected for the storage of important, and often very large, image files.
- **networking and TCP/IP:** A fundamental understanding of TCP/IP is another requirement. Investigators should be familiar with the format of a TCP/IP packet, IP addressing, MAC addresses, and how internet routing works. Being able to properly identify the source and destination address can lead the investigation in the appropriate direction. Understanding the weaknesses in protocols and attacker obfuscation techniques such as IP spoofing also enhance the investigator's capability.
- **desktop applications:** Many applications such as Microsoft Word and Internet Explorer create temporary files in addition to those related to the operating system. Those temporary files provide backups, histories, and even performance details for the application. The evidence in existing (or deleted) application temporary files may support the investigation. It is important to understand the common files created by these applications, where they are stored, and how to recover deleted versions. Common applications to begin with are Microsoft Excel, Microsoft Word, Microsoft Internet Explorer, Apple Safari, Mozilla Firefox, and Google Chrome.
- **memory image acquisition:** Attackers have access to numerous obfuscation techniques they can use to hide malicious processes, files, and network connections from the operating system. Native system commands can often be fooled by rootkits that hide attacker activity. Extracting memory or RAM to an image file for analysis outside of the operating system may be the only way to detect this hidden activity. Memory acquisition tools are often unique to the operating system and computer architecture. Digital investigators should have trusted, tested, and documented tools for all operating systems they plan to investigate.
- **volatile data acquisition:** Computer system information that is lost upon shutdown is considered *volatile*. System uptime, open network connections, command histories, active users, open files, installed applications, running processes, and file creation,

modification, and access times are all data that should be collected. Investigators should have trusted utilities and processes for acquiring volatile system information.

- **hard drive acquisition:** In addition to rootkits that obfuscate various files, it may not be possible to recover deleted files from unallocated or slack space from a live file system. Acquisition of an entire hard disk or logical volume using a bit-by-bit full duplication method provides a forensically viable option for offline analysis and allows investigators to analyze a hard drive without affecting the original evidence. The hard drive image can be marked "read only" after creation, and analysis can occur on yet another copy using a commercial or open source tool. Investigators should have a trusted tool set and documented procedures to support this activity.
- **log file collection:** Knowing what to collect and how to collect it does not necessarily mean the data will be available. Although many operating systems, networking devices, and applications are capable of writing valuable information to log files, they are often not configured to do so. Nevertheless, it is important for investigators to know how to collect and protect this data because it may, in some cases, contribute greatly to an investigation. Analysts should be aware of common log files such as those in Windows System, Application, and Security Event viewers and the data recorded in /var/log/messages and /var/log/secure on Linux systems. In addition, analysts should know the default log locations and settings for common operating systems and applications and know what information they could provide to support the investigation. Just as with memory images, hard-disk images, and volatile data, the collected log files should be written once, protected, and then copied before the newly duplicated data files are analyzed.
- **storage and transportation:** In addition to write-protecting collected data, analysts should verify the integrity of evidence files using approved hashing algorithms such as MD5 or SHA-2. Appropriate labeling of evidence is also important. To guarantee the physical security of such log files, organizations should maintain a secure storage cabinet or server within a secure location and allow only authorized personnel to access it. Furthermore, when transferring the ownership of collected evidence, analysts should complete and secure the appropriate chain-of-custody paperwork. Organizations should also document procedures for labeling, storing, protecting, and transporting data. All team members must understand the importance of these requirements and adhere to them at all times.
- **trusted tools**: All team members should be proficient with their organizations' approved acquisition, analysis, and reporting tools. In some environments, professional training on approved tools may be necessary to develop the necessary knowledge and skills. In addition to having a baseline competency for each tool, team members should understand what to look for and why. They should be able to verify what each tool can and cannot do and justify the results obtained from the various applications [Kanellis 2006, p. 326].
- **timeline generation:** Generating a timeline of activity from a system or multiple sources can provide analysts with a significant means of data reduction. In addition, analysts can use timelines to determine the timing of malicious activity or even optimize analysis and

reporting [Harlan 2009]. Analysts can use applications like log2timeline,[1] SleuthKit,[2] and other open source digital investigation tools to make this difficult task easier.

Specialty Skills

While it's impossible for digital investigators to know everything there is to know about all systems and applications, they should try to develop a more advanced forensics capabilities in the following areas:

- **mobile computing:** Technology for smartphones and mobile computing devices is evolving rapidly. The convenience and power of lightweight portable devices are making their use in professional computing environments ever more popular. These devices often record call and text message activity and can store gigabytes of information including images, music, movies, and corporate data. Several commercial tools have add-ons to support mobile device forensics. Enhancing this collection and analysis capability in a digital investigation team may be considered mandatory in some organizations.
- **virtualization technologies:** VMWare,[3] Virtual PC,[4] VirtualBox,[5] and other virtual technologies allow organizations to maximize their return on investment for expensive server hardware by deploying multiple virtual computers on one physical system. These applications leverage a virtual machine manager (VMM) or hypervisor to effectively manage computing resources for numerous virtual systems while still isolating critical services and customers to preserve confidentiality. As application service providers, hosting facilities, and organizations begin to leverage these technologies more, the likelihood of an incident occurring in a virtual infrastructure increases. Such an incident may result from the compromise of a hypervisor, the host operating system, or even the guest system. Having the skills needed to safely acquire digital evidence in these architectures could prevent collateral damage to other systems and secure the necessary data.
- **encryption:** Many obfuscation techniques are leveraged by malicious perpetrators. One such option is to encrypt malware files or data in transit. An organization may also implement a legitimate encryption solution to protect assets that process sensitive data. In either case, digital investigators may need to address this challenge by first detecting the presence of encryption. Network analysis tools such as Wireshark[6] can identify encrypted protocols such as SSH, HTTPS, and IPSec. At a minimum, investigators need to detect the source and destination IP addresses of this activity. To help law-enforcement agencies detect the presence of encryption on live systems, the CERT Program at the Carnegie Mellon Software Engineering Institute created the CryptHunter[7] application. CryptHunter can detect mounted, encrypted volumes and whole-disk encryption if implemented on

---

1 For more information, go to http://log2timeline.net.

2 For more information, go to http://sleuthkit.org/.

3 For more information, go to http://www.vmware.com/.

4 For more information, go to http://www.microsoft.com/windows/virtual-pc/default.aspx.

5 For more information, go to http://www.virtualbox.org/.

6 For more information, go to http://www.wireshark.org/.

7 For more information, go to http://www.cert.org/forensics/.

running systems. This information may be critical to the collection agent. Immediate live acquisition of the encrypted drive may be necessary because that volume may not be available again after the system is shut down. Enterprise solutions such as the Windows Encrypting File System (EFS) provide a key escrow system that can allow system administrator accounts to also unlock encrypted volumes. Investigators should have at least a basic understanding of common encryption technologies.

- **wireless networking:** Several technologies expose computing resources to additional risk. Misconfigured Bluetooth devices, insecure Wi-Fi Access Points (APs), and unencrypted Radio Frequency Identification (RFID) communications can all lead to the compromise of sensitive personal and corporate data. While obtaining previous radio communications may not be possible, collecting transaction and authentication logs from devices may provide details of when and how an incident occurred. Understanding the vulnerabilities associated with each technology can also lead a related investigation in the appropriate direction.
- **network appliances:** Investigators can develop specialty skills on specific platforms such as Cisco, Juniper, Nortel, and other common router, firewall, and switch products. Using logging and monitoring features and reliably collecting data can provide investigators with valuable information not readily available during the analysis of a specific compromised host.
- **runtime analysis:** In conjunction with communications protocol knowledge and experience with specific network devices, investigators can benefit greatly by developing runtime analysis skills. Using packet capture solutions and tools like Wireshark and tcpdump, investigators may be able to detect malicious network traffic involving a compromised host or suspected attacker. Those tools might be the only way to detect activity that is otherwise hidden by malicious code on a computer. In addition, these skills can help investigators understand the attacker's mindset and methods for extracting data or executing command and control operations.
- **online games:** Massively Multiplayer Online Role-Playing Games (MMORPGs) like World of Warcraft can be used to facilitate cybercrimes. Incidents include real-world violence extending from virtual conflicts, sexual exploitation of minors through online chat sessions, and even money laundering.[8] In some circumstances, chat histories and communications within the Microsoft Xbox LIVE network, Sony's PlayStation Network, and computer-based games such as World of Warcraft can contain vital evidence to support a digital investigation. As online games become more popular, they become a more common tool for committing cybercrimes. A computer forensics team would benefit from having members experienced in finding and correlating evidence from these activities.

[8] For more information, go to http://www.dfinews.com/article/multiplayer-game-forensics.

Trusted Toolkit

Before a security incident occurs and any evidence collection is done, digital investigators must have a trusted toolkit of applications and procedures to support acquisition and analysis. Being prepared beforehand is crucial. A working knowledge of the tools in the toolkit will aid collection efforts and help identify collection limitations and capabilities.[9]

Several supporting tasks are required when developing a trusted toolkit. First, a test environment must be created. Ideally the hardware, software, and collection scenarios will be comprehensive enough to support any future incidents. If an organization leverages certain virtual technologies, encryption applications, smartphones, or operating systems, the internal digital investigation team can customize the testbed accordingly. Since 100% preparation is unlikely, documenting this testbed is crucial. Investigators should note any variances they see during actual incidents.

Trusted tools may produce different results in new scenarios, and investigators must be prepared to adapt techniques for accomplishing the current task. For example, an approved Windows memory-acquisition tool supports 32-bit, Windows 2003 servers. Once on-site, investigators determine that the compromised machine is a 64-bit version of Windows 2008; therefore, the trusted tool may or may not work. It's best to verify whether it will work beforehand and identify any alternative memory capture techniques that may be necessary. For this reason, designing, implementing, documenting, and using the test environment to develop a trusted toolkit are critical tasks for a digital investigation team.

After the test environment has been established, the tools must be tested. Live-response CDs, volatile collection tools for Linux and Windows, hard-drive imaging applications and hardware, and other computer forensic tools must be evaluated in various scenarios. Analysts can compare documented outcomes to known data elements and vendors' claims to validate a tool's capability. The impact a tool may have on the system being investigated should also be documented. If a tool leverages specific operating system files, it changes the last accessed time of those files and becomes dependent on the compromised system to provide accurate information. With the various obfuscation techniques available to attackers, this dependency can prevent the tool from accurately enumerating the desired information. Documenting and minimizing these dependencies are also important when developing a trusted toolkit.

Situational Awareness

When initially responding to an incident, it is important for investigators to gain situational awareness as soon as possible. In some cases, they might need to video record the actual location or photograph the area before actually collecting digital assets. This recording or photograph may be used as evidence in a legal matter or be referenced later to identify follow-up areas of investigation. First responders will also need to quickly ascertain the supporting staff's level of cooperation and expertise, and possibly collect additional data such as firewall or application logs. This evidence may not be within the original scope of the investigation or the collection agent's

[9] For more information, read *First Responders Guide to Computer Forensics* posted at http://www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

authority. However, identifying the need to collect this data is still important. The cooperation of on-site staff may be necessary to preserve evidence for later collection and analysis.

Situational awareness is a difficult skill to develop. The only true way to grow this capability is through on-the-job training. The next best option is to immerse investigators in training simulations that present them with opportunities to triage and respond to realistic events in a controlled environment. Through the production of training events that replicate previous incidents, computer forensics teams have the opportunity to benefit from the experiences of knowledgeable experts and the lessons they've learned.

Threat Awareness

Due to the dynamic nature of computer threats, information security professionals must stay abreast of the latest news and challenges. Administrators can enhance their defensive controls by analyzing current attacks, motives, and vulnerabilities. Investigators can review reports and lessons learned to enhance their own deductive capabilities. For example, published analysis of new online banking Trojans or other malware may identify new attack vectors or signatures. When investigators encounter a new case with similar characteristics, they can leverage the experience of others to detect or verify their own findings.

Simply understanding popular technology can also prove to be important. As the use of social networking, online gaming, and internet-based productivity applications grow, so too does the risk of attack through these services. Digital investigators should be aware of known malicious incidents involving popular technologies. They should know how to detect them and, if possible, know how to attribute victims and perpetrators.

Analysts can take additional proactive actions to increase threat awareness. Many professional courses are available on computer network attack and defense, penetration testing, and network vulnerability assessment topics. Advanced information security courses provide insight into topics such as steganography, encryption, rootkits, and other methods of concealment. By understanding attack methodology, objectives, and the evidence left behind from offensive activities, digital investigators can better determine evidence possibilities and prioritize their analysis.

Reporting and Presentation

The ability to accurately and expertly record and present digital investigation findings can make the difference in the outcome of a legal investigation. It may also impact an organization's ability to successfully protect against similar incidents in the future. Reporting requirements may vary from organization to organization, but the questions that need to be answered are generally the same:

- What happened?
- How?
- Who were the parties involved?
- What was the impact on the organization?
- Why did the incident occur?
- What can be done to prevent similar events in the future?

Not all investigations require answers to all these questions. Investigators might be able to derive some answers from the facts and evidence they discover, while other answers will come from the conclusions of expert analysis. Including an executive summary in the report is highly recommended. It is written for senior leaders and nontechnical readers, and provides an overview of the case details and findings.

A computer forensics team should develop a template and a detailed list of reporting requirements to ensure that (1) each investigation is executed in a consistent manner that adheres to defined policies and (2) each team member collects all the necessary information and completes all investigation steps.

In some situations, formal reporting of the findings might be necessary, for example, via testimony at a trial. Having a thorough understanding of the findings and an ability to present them clearly can provide the credibility and validation required by management or a judge and jury. For this reason, any team manager or investigation supervisor must develop effective written and oral communication skills.

Legal/Policy Knowledge

When organizations establish a digital investigation capability, they must understand the legal and organizational policies that impact the collection and examination of evidence. In general, traditional law-enforcement agents transitioning into cyber investigations have a better knowledge of legal procedures than IT professionals do. On the other hand, individuals with more industry experience may have a better understanding of Acceptable Use Policies (AUPs) and corporate monitoring policies. All investigators must have baseline knowledge in these areas and develop the skills needed to interpret the application and precedence of this governance on a case-by-case basis.

After being notified of an event, an investigator must determine which evidence to acquire. An internal response team may have broad authority to collect data on numerous sources. In contrast, a law-enforcement agency may need to request a search warrant for a specific component (e.g., a hard drive) on a specific computer, based on demonstrated probable cause of a crime. Once the collection and initial triage begins, investigators might decide that additional evidence must be obtained. Internal forensics teams may have the leeway to pursue these actions, while external investigators and law-enforcement agents may require additional authorization. In many cases, the organization can permit law enforcement to expand the investigation. This consent can make it possible to circumvent the Fourth Amendment, which protects individuals from unauthorized search and seizure.[10] To further support digital investigations by the organization or law enforcement, an organization should have a comprehensive AUP that clearly details what, if any, expectation of privacy is available on its network. Being able to expertly interpret organizational policies and legal statues can significantly aid an investigation.

Not all investigations will lead to criminal or civil legal actions. However, at times, members of the digital investigation team will be required to provide expert witness testimony. Teams can

[10] For more information, go to http://www.drpsecurity.com/digital-crime-laws.

prepare for this activity throughout their own workforce development cycle. First, they can develop a deep understanding of the technologies involved in collecting and analyzing the evidence. Much like instructors or presenters, investigators who understand the collection and analysis procedures, the tools used in the investigation, and the strategies that support all the activities will demonstrate more confidence in their work and findings. Before making a court appearance, investigators can enhance their interpersonal communication skills by participating in mock interviews and leading formal presentations of their findings to senior leaders and customers. Both exercises give investigators practice answering questions in situations of increased pressure and scrutiny.

Industry Certifications

Digital investigators who pursue professional training and certification programs can more readily be introduced as an expert witness in a courtroom because such training can indicate a level of expertise or accreditation. However, the court may not recognize the value of one certification over another. For example, the GIAC Certified Forensic Analyst (GCFA) requires investigators to pass a 150-question test with a score of 69.3% or better,[11] while the International Society of Forensic Computer Examiners (ISFCE) Certified Computer Examiner (CCE) accreditation requires them to complete specific training, have 18 months of professional experience, and pass both written and practical exams.[12] These programs, along with other certifications, provide investigators an opportunity to gain a solid foundation of knowledge in the areas of computer forensics. The depth of knowledge and skills required to pass one certification over another may better prepare investigators for future events. However, the value of one certification over another may or may not come into question in a courtroom. Organizations should evaluate certification programs based on known and/or anticipated investigation and presentation requirements.

Build Proficiency Through Experience

Although formal education and professional training are both important to establishing capability, real-world experience is required to develop proficiency. It may take months, or even years, for an investigator to gain the necessary expertise to truly be effective. To speed up this learning process, investigation teams should seek opportunities to develop, evaluate, and enhance their capability in comprehensive digital forensics scenarios and live-fire exercises.

The CERT Program's approach to cybersecurity workforce development builds knowledge, skills, and experience in a continuous cycle of professional development. Each phase focuses on building a specific area of development that is leveraged and supplemented by the next phase of development. The end goal is for cybersecurity professionals to use relevant knowledge, skills, and experience to successfully and effectively perform their jobs [May 2010]. This approach is especially applicable to the development of digital investigation capabilities.

---

[11] For more information, go to http://www.giac.org/certification/certified-forensic-analyst-gcfa.

[12] For more information, go to https://www.isfce.com/process.htm.

Experience is required to truly be effective and successful in computer forensics. Situational awareness increases through exposure to numerous events and through growing skills from previous lessons learned. Through immersion in training scenarios based on real-world events and threats, investigators can enhance their ability to identify, collect, and analyze important evidence. Using repeatable training scenarios, teams can continuously develop skills even though team members may start with varied levels of experience.

CERT XNET is a next-generation cybersecurity training and simulation platform that can help digital investigators build their experience. XNET offers a unique solution by providing organizations with convenient and continuous access to realistic, hands-on cyber-training scenarios. [13] Using dynamically deployed computers and network infrastructure, real-time security events and scenarios are available to digital investigators through an easy-to-use, isolated, web-based portal. Numerous computer forensics scenarios exist within a comprehensive training library that can facilitate the growth of entire investigative teams as well as individuals.

Conclusion

The first step in developing a digital investigation capability is to create a comprehensive workforce development plan with clear objectives based on the organization's priorities and available resources. An organization must continuously build upon the knowledge, skills, and experience of its staff to enhance the capability and effectiveness of its digital investigation unit. Three learning paradigms support the building of knowledge, skills, and experience: (1) formal education through colleges and universities, (2) professional training through organizations such as the CERT Program or the SANS Institute, and (3) good old-fashioned, on-the-job-training [Kanellis 2006, p. 320]. To become proficient, investigators might needs months or even years of on-the-job training. Solutions like the XNET training and simulation platform are emerging to speed up this learning process and enhance computer forensics capabilities.

After investigators complete training, the effectiveness of that training must be evaluated, along with the resulting capabilities. Organizations should use feedback from these evaluations to refine future training plans [Kanellis 2006, p. 329]. Beyond training review, lessons learned from actual events should be incorporated into workforce development. They can provide input into new iterations of risk analysis and management programs, and better prepare organizations for future attacks [Blum 2010].

Finally, having a development program for a digital investigation workforce supports career progression and advancement. Career goals may be established for junior analysts to advance to journeyman or senior/master levels. Individuals may want to expand their baseline knowledge and skills to become subject matter experts in specialty areas such as encryption, virtualization, or mobile computing forensics. Team leader, supervisor, or manager roles may focus learning efforts on communication and presentation skills, along with enhanced understanding of legal issues and organizational policies.

---

[13] For more information, go to http://xnet.cert.org.

Bibliography

URLs are valid as of the publication date of this document.

[Blum 2010]
Blum, J. "The Art of Forensic Analysis." *ISSA Journal* (August 2010): 36-44.

[Bosworth 2009]
Bosworth, S.; Kabay, M. E.; & Whyne, E. *Computer Security Handbook* (5th ed.). John Wiley & Sons, 2009.

[Harlan 2009]
Harlan, C. "Windows Timeline Analysis, Building a Timeline, Part2." *Hackin9 4*, 6 (June 2009): 46-49.

[Kanellis 2006]
Kanellis, P.; Kiountouzis, E.; Kolokotronis, N.; & Martakos, D. *Digital Crime and Forensic Science in Cyberspace*. Idea Group Inc., 2006.

[May 2010]
May C. & Hammerstein, J. *The CERT Approach to Cybersecurity Workforce Development* (CMU/SEI-2010-TR-045). Software Engineering Institute, Carnegie Mellon University, 2010. http://www.sei.cmu.edu/library/abstracts/reports/10tr045.cfm