Interested in learning more about security?

The SANS Survey of Digital Forensics and Incident Response

Copyright SANS Institute
Author Retains Full Rights
The SANS Survey of Digital Forensics and Incident Response

July 2013
A SANS Whitepaper
Written by Paul Henry, Jacob Williams and Benjamin Wright

Survey Respondents PAGE 3
How and Why They Investigate PAGE 7
What They’re Investigating PAGE 12
Challenges with “New” Technologies PAGE 17
Recommendations PAGE 22
More than 450 participants completed the SANS 2013 Digital Forensics Survey, conducted online during April and May 2013. A primary goal of this survey was to identify the nontraditional areas where digital forensics techniques are used.

In the survey 54% of respondents indicated their digital forensics capabilities are reasonably effective. Although the majority of their investigations still take place on company-issued computers and laptops and internal networks and systems, participants also conduct forensic investigations on virtual and cloud-based systems and other unconventional endpoints. When it comes to investigating these new media types, participants are nearly equally divided among several challenges inherent to such investigations—including a lack of specialized tools, standards and training, and visibility into potential incidents.

A chief finding of the survey was that participants identified deficiencies in standards, tools and training as the fundamental challenges to investigating incidents involving the cloud, mobile devices and other unconventional endpoints. Figure 1 shows the other challenges identified by respondents.

![Figure 1. Primary Challenges of New Devices and Technologies](image-url)
Executive Summary (CONTINUED)

As organizations adopt bring-your-own-device (BYOD) policies and cloud (particularly “public cloud”) technologies, they should ensure that the policies cover digital forensics and incident response (DFIR) in these and other emerging technologies. IT professionals should also engage the advice of their legal teams or consultants so that the policies actually achieve the desired outcomes and protections, while avoiding undesired ones. For instance, some incident response (IR) teams routinely reload compromised workstations without obtaining forensic disk images or memory captures. Although accomplishing the IR goals of containment and eradication, this method undermines the value of evidence that may be required for subsequent legal action.

Forensic investigations of so-called “new” computing devices and media are increasing, affecting enterprise governance (and society in general) more than ever before. Increasingly, these investigations involve technologies such as cloud computing and mobile devices.

To assess the current state of forensic investigations and emerging trends, the SANS Institute conducted this online survey of digital forensics practitioners. The results, summarized in this whitepaper, will help forensic professionals and their clients better prepare for future investigations and allocate resources, while helping guide educators and forensic tools vendors.
The respondents for this survey were numerous and diverse, with more than half representing organizations of 2,000 employees or more. Smaller operations were also well represented; organizations with fewer than 500 employees comprised almost one-third of all responses, as shown in Figure 2.

The results of the survey are representative of a cross-section of organization sizes, not merely those with large budgets for DFIR.
Respondents also came from a range of industries; the largest group (almost one-quarter of survey respondents) was government professionals. Financial, IT services, consultants in forensics and incident response, and education were the next most represented industries, ranging from 9–13% of responses. Figure 3 shows the distribution of respondents’ industries.

![Figure 3. Respondents by Industry](image)

This cross-section of respondents demonstrates the broad interest (and investment) in forensic investigations. It also speaks to the different roles and perceptions they may have regarding digital forensics.
The survey did not break out “Government” respondents by branch, so it is difficult to distinguish law enforcement professionals from other forensic or investigative personnel in public service. Nevertheless, we assume that a substantial share of the 25% of respondents who identified themselves as “Government” (twice as many as any other industry classification) belong to the law enforcement community. We base this in part on the high number of “Government” respondents who selected “Investigator” as their primary role.

Figure 4 shows the breakdown of consultants and staff in the various roles and job titles listed by respondents.

Just as law enforcement professionals have certain definitions and perceptions of digital forensics and related tools, personnel in staff positions will have concerns and goals that differ from those of outside consultants. Consultants can provide value through up-to-date skills and access to specialized equipment and tools that are unavailable to inside staff that may be challenged for resources and time to research the latest tools and techniques. Clearly, the majority of respondents are treated as staff by the organizations they support.

The most well represented work roles identified by respondents were, in descending order: Digital forensics specialist, incident responder, security analyst and investigator.
Figure 5 shows the breakdown among the various types of in-house and outside resources most used for digital investigations, based on how often they are called in; the scale ranges from least used (0) to most used (4).

The close alignment of these numbers may also indicate that many part-time incident responders are borrowed from the IT staff ranks, particularly for small- and medium-sized businesses with fewer resources. Regardless, it is clear that in-house staff is less likely to have forensic training as most have incident response assignments. (See the sidebar “Forensic Investigations Defined” for how we distinguish between forensics and incident response.)

The lower incidences of specially trained forensic and legal professionals (in-house or consultants) indicates that more IT groups are using “forensics” capabilities to respond to incidents than for preserving digital evidence that would stand up in court. This indicates many respondents do not expect to have the results of these investigations challenged in external reviews such as legal or regulatory hearings.

**Forensic Investigations Defined**

For the purposes of our survey, and because the survey base includes professionals from both private and public sectors, with consultants as well as in-house experts, we distinguish between “forensics” and “investigations”:

- We use “forensics” in the sense of searching computer networks and systems for evidence of breach, data loss or other activities.
- In similar fashion, we use “investigations” when referring to the cases our respondents support, such as employee abuse of resources, espionage or financially motivated attacks.
- We define “incident response” (IR) as the identification of a compromise, the containment of the compromise and the eradication of the threat actor from the environment. Because detection often relies on intelligence derived from forensics and eradication can destroy forensic evidence, optimal outcomes are achieved when IR and digital forensics teams work closely together.
The next section of the survey focused on the investigations that survey participants and their organizations conduct.

**Number of Investigations**

Slightly more than 25% of respondents told us they conducted more than 50 investigations in the last two years, with 11% of that 25% conducting more than 100 investigations and 4% conducting more than 500 investigations. A disproportionately large number of those conducting more than 50 investigations identified their industry as “Government.” In fact, those respondents accounted for more than half of those reporting 500 or more cases, possibly working in law enforcement-related forensic labs.

Others conducting large numbers of investigations may be from large-sized forensic/IT consulting services that conduct multiple investigations for their clients. Nevertheless, such responses certainly do not represent the norm; the majority of respondents said they conducted up to 25 investigations in the last two years, as shown in Figure 6.

![Figure 6. Number of Investigations Conducted in Previous Years](image)
Types of Investigations

Respondents were asked to select the reasons their organizations conduct forensic investigations. The responses to this question were telling: Three-quarters of respondents (75%) said they conduct forensic investigations to “find and investigate incidents after the fact.” This follows the pattern of traditional forensic investigations, particularly for law enforcement or legal professionals whose work may be used in court or regulatory proceedings.

However, digital forensics is also useful for investigations in real time. The survey found 57% of respondents reporting that they conduct investigations to “find and investigate incidents as they are occurring.” Real-time digital forensics is increasingly important to IT security professionals grappling with advanced persistent threats (APTs) in their networks, as APTs can be multifaceted in their danger as well as in their attempts to survive. In the survey nearly 50% of respondents are also using forensics to track and remediate APTs, for example.

The range of reasons behind investigations and the relative share of each appear in Figure 7.

This was a multiple-choice answer set, with the ranking occurring based on the number of responses to each option. HR issues, such as investigating employee misuse of resources, were the second most frequently reported reason for conducting forensic investigations. Collecting evidence for legal or regulatory investigations was also frequently cited, which may be related to the large representation of respondents from government, which includes law enforcement with other public sector forensic experts.
Prepared for Legalities?

Considering that 62% of respondents have used digital forensics to investigate “HR issues/employee misuse or abuse” and 57% indicate that they were looking for legal evidence that could hold up in court, organizations would be wise to treat such cases as if they may end up in arbitration or even legal proceedings. This means applying an appropriate degree of rigor in the collection and management of evidence so that the trustworthiness of the evidence can be defended.

The substantial number of respondents who specified evidence collection as an investigative goal also emphasizes the need for sound processes that can withstand challenge under outside scrutiny. Law enforcement has, for years, led the private sector in the use of digital forensics, whether investigating computer-related crimes or more prosaic ones. The evolution of practices and tools in the areas of chain of custody, evidence control, forensic imaging and similar fields is, as a rule, driven by the requirements of police, prosecutors and related investigators.

The need for rigor also applies when conducting forensics for measuring legal or regulatory compliance. In the survey only 40% of respondents reported they use forensic investigations to support regulatory or compliance processes. Regulatory issues are also likely to be reviewed by an outside authority, such as a court, an auditor or a government agency.

Forensics-Derived Intelligence

The survey results also indicate a substantial amount of threat intelligence being derived from forensic data, as more than half of respondents reported that they use forensic investigations to collect intelligence for ongoing and future incidents. Similarly, almost half of respondents use investigations to track and remediate APTs. Because of difficulties in detecting APTs inside corporate networks—in most cases these are reported to victims from an outside source—the ability to proactively use intelligence gathered through forensics and other means is increasingly valuable for incident detection and follow-up, especially where it may provide specific indicators of compromise. This can help identify other assets within the organization (or elsewhere) that may be at risk.

Intelligence and digital forensics have a close-knit, nearly circular relationship. Artifacts discovered with forensic techniques can be used to identify attacks—especially those perpetrated by stealthy APT actors—much earlier and with a higher degree of accuracy than without such techniques. Detecting attacks earlier reduces the scope (and cost) of the subsequent incident response and forensic investigation.
Level of Effectiveness

The good news is that the majority of respondents (74%) feel their overall forensics and incident response capabilities are reasonably (54%) or very (20%) effective. Of the remaining 26%, the overwhelming majority has some sort of DFIR capability while only 3% of respondents have no such capability. Figure 8 shows the distribution of respondents’ self-evaluation of their DFIR efforts.

For those 26% of respondents reporting marginal or zero DFIR effectiveness, we recommend reaching out to their particular industry or trade association for technical guidance and other assistance with investigations that rely on digital forensics. Otherwise, they risk incurring greater liability if mistakes are made during the investigative process.
How and Why They Investigate (CONTINUED)

Extensiveness of Policies

Survey respondents indicated overwhelmingly that their forensics policies and tools are neither up to date nor ready to respond, even in those investigations involving mature forensics processes and tools. Only 29% of the respondents indicated that they have detailed policies and are ready to respond to an incident. The remaining participants indicated that either their policies need to be updated (“partially mission-capable”) or they have none at all, as shown in Figure 9.

The low number of respondents with a “detailed policy” is especially significant because this question specifically addressed forensic capabilities in traditional environments. This brings up the question: If so many respondents feel their policies for traditional environments are deficient, how are they conducting investigations that involve new technologies or unconventional deployments? In the next sections, we discuss new technologies professionals are using in their investigations and how the innovations complement the tried-and-true.
What They’re Investigating

The landscape of digital forensics is rapidly changing, increasingly involving nontraditional devices, platforms, and systems. Survey respondents are obviously scrambling to adapt their efforts to these new environments, given the diversity of device types on which they report conducting investigations.

Cloud on the Horizon

When asked about the types of environments they typically investigate, nearly 60% of respondents stated that they investigate virtual systems and networks; however, only 15% of respondents indicated that they investigate server infrastructure in the cloud, such as Amazon EC2, and only 17% investigate shared collaborative cloud apps, such as Dropbox, as shown in Figure 10.

The disparity between these numbers suggests that assets deployed to the cloud are generally not included in forensic investigations or that respondents may be conflating their virtualized systems with cloud-based ones or focusing on the nature of a system rather than where it is deployed.

Although “the cloud” implicitly relies on virtualized systems, the concepts are not necessarily interchangeable; the virtualized systems can be in a “private” cloud, where the organization owns the hardware supporting the virtualized systems, or in a “public” cloud, where the system provider owns the hardware and rents access in a fashion reminiscent of mainframe time-sharing.

The responses to this question indicating a lower frequency for cloud-related investigations may reflect the relative novelty of such deployments; alternatively, the owner of the hardware in public cloud environments such as Amazon EC2 (typically the provider, rather than the user of the service) may be able to block or merely disregard such inquiries. Organizations whose policies assume physical access to systems in the course of internal investigations should keep this in mind when contracting with cloud and similar service providers.

Nevertheless, the responses show that cloud, mobile and virtual systems are a part of forensic investigations at many organizations and will be a growing part of future investigations.

Figure 10. Devices and Systems Subjected to Investigation

The SANS Survey of Digital Forensics and Incident Response
Nontraditional Platforms

Respondents were asked what percentage of investigations involves nontraditional platforms, specifically virtual or cloud-based resources, mobile devices (with or without BYOD policies) or atypical systems (including embedded systems, game systems, printers and similar devices). The results show that such investigations still represent a small share of the total number (generally, in the 1–5% range), regardless of which technology is involved.

However, 40% of respondents investigated employee-owned mobile devices, while 20% investigated virtualized, cloud-based or other unconventional systems.

For this reason organizations looking to increase forensic investigation capabilities in nontraditional areas should address mobile platforms first. Policies should account for the routine backup of mobile device data to the cloud, potentially through employee-owned accounts. Due to the complications inherent in BYOD environments, organizations should also align policy and training with the adoption of new practices and technologies when creating or reviewing their DFIR strategies.

The tools and techniques used in forensic investigations of traditional platforms are in some ways similar to those used in virtualized and cloud-based environments, but in other ways, may not be suited at all to these newer technologies. Similarly, mobile devices and embedded systems present their own challenges.

Tools for the Cloud

When asked about the tools forensic investigators employ in virtualized and cloud environments, only 16% of respondents indicated they use tools designed specifically for such platforms. Additionally, more than one-third of organizations (36%) use low-tech image captures and screen recordings for investigating virtualized and cloud-based systems, while one-quarter reported that they create their own tools as the need arises. The opportunity cost that comes with creating and maintaining specialty tools in-house can be significant. Figure 11 shows the usage of various tools and techniques among the survey respondents.
These responses suggest that a capability or usability gap exists for custom tools in cloud environments.

Almost one-third of respondents (31%) rely on cloud service providers to collect evidence for them. This practice relieves organizations of the requirement to train on specialized forensics, but it raises concerns about the quality and accessibility of evidence, including:

- How well is the service provider’s staff trained?
- What tools and procedures do staff use?
- What assurance is there that the service provider will respond in a timely fashion when an investigation is required?
- What is the chain of custody?

Organizations should carefully vet cloud service providers that offer evidence collection, to ensure they meet expectations. They should ask service providers to provide assurances about controls, capabilities and obligations in regard to forensic investigations.
Nevertheless, only 16% of respondents reported that they have a service agreement allowing them to conduct forensic investigations in the provider’s environment if the need arises. Organizations that previously overlooked this consideration during their migration to the cloud should evaluate their current requirements and negotiate specific terms with their providers.

**Tools for Mobile/BYOD**

We also wanted to understand the tools and techniques used to investigate mobile/BYOD environments, assuming that these would vary from those used on traditional platforms. Therefore, respondents were asked about the tools and techniques used in their mobile/BYOD device investigations. The most common tools and techniques are acquiring the device filesystem and physical data extraction (62%), followed by interviewing the device owner/user (59%) and forensic acquisition of logical data (55%). Figure 12 shows the tools and resources used to investigate mobile devices, with or without BYOD policies.

![Figure 12. Tools and Resources in Common Use](image-url)
The reliance on acquiring the actual device and recovering physical data from it (a basic digital forensics technique) and on user interviews (an inherently nontechnical solution) may indicate an immaturity of tools (or investigator access to and experience with tools) for mobile/BYOD situations. Alternatively, it may indicate that old-school “gumshoe” work is still fundamental to law enforcement and regulatory investigations.

Only 30% of respondents indicated they retrieve data from a mobile device management (MDM) platform during forensic investigations. This number is probably close to if not exactly congruent with the number of respondents whose organization uses MDM, on the assumption that it is employed in investigations whenever it is available.

Comparing this number to the survey demographics indicates that about one-half of responding organizations with more than 2,000 employees do not employ MDM systems in their investigations. This may indicate that many of the respondents simply don’t encounter mobile devices that are provisioned by (or otherwise in contact with) an MDM platform. For example, investigators reporting themselves as “Government” are far less likely to use MDM logs in investigations involving mobile devices than their peers, employing MDM data in 18% of investigations. Nevertheless, such data can be invaluable during a forensic investigation that involves mobile devices, whether these are company provided or supported through BYOD policies.

Interestingly, more than one-half of respondents use data from network access control (NAC) platforms or network records, such as logs, for analysis. This indicates that these organizations have NAC, egress/exfiltration logs or other network monitoring assets at their disposal for investigators’ use, or organizations performing investigations are more likely to use NAC or related tools in their endpoint monitoring. Nevertheless, mobile devices could be entirely bypassing corporate networks by using cellular or “rogue” Wi-Fi connections, and investigations focusing on a corporate network may miss this traffic.

Government investigators are much more likely to perform forensic investigations on mobile devices than the other types of respondents. Participants were asked to approximate the share of investigations involving mobile devices. The number of respondents reporting that mobile devices were involved in more than 10% of cases was much higher among government investigators than it is for the general population (47% vs. 25%). This seems to indicate that law enforcement personnel—presumably a large portion of the responding investigators who are employed by government—are as likely to encounter mobile devices in their investigations as not. Also, government investigators (whether employed in law enforcement or not) were much more likely than the other respondents to acquire physical or filesystem data, by margins of up to 25%.
Challenges with “New” Technologies

In order to determine what tools and techniques are working for investigations on unconventional platforms and how best to deploy those means of inquiry, the next set of questions asked about respondents’ level of satisfaction with these tools and processes, and the challenges posed by these rapidly evolving technologies.

Much Room for Improvement

Respondents were first asked about their satisfaction with the tools and processes used in forensic investigations of traditional devices and systems, and the dominant answer across all categories (except for “Other”) was “Somewhat satisfied.” This response indicates that forensic tool development has room for improvement in the eyes of the survey respondents, even in well-documented and conventional environments, as shown in Figure 13.

![Figure 13. Tools Used to Investigate Conventional Systems](image)

What tools do you use for investigations on traditional network devices, endpoints and company applications? Check your level of satisfaction with the tools you do use.

- Network data capture/sniffer tools
- Third-party tools specific for legal digital forensics
- Log collection with manual interpretation
- Homememade tools for our specific environment
- SIEM tools
- Log collection with third-party analysis tools
- Intelligence and analytics tools or services
- Tools not specifically designed for investigative use
- Endpoint interceptors
- Other

Very Satisfied
Somewhat Satisfied
Not Satisfied
Challenges with “New” Technologies (CONTINUED)

Log collection dominates the ranking of processes and tools used for investigations, although respondents indicate that logs do not completely satisfy their requirements. In a similar vein, respondents frequently use browsers and screen captures in their investigations, but few respondents (15%) find these sufficient.

Interestingly, two-thirds of survey respondents use homegrown tools tailored to their environment when investigating conventional systems. This was surprising, given the maturity of the tools commonly used in such investigations. However, nearly as many respondents also use third-party tools, and the overall satisfaction with homemade tools is not noticeably different from that for commercial ones.

Other telling observations from this data are that only two-thirds of respondents use a security information and event management (SIEM) product in their work. Of respondents using SIEM tools, 80% are either very or somewhat satisfied with SIEM data for investigations, indicating that SIEM products provide worthwhile evidence for forensic investigations.

Investigations on Unconventional Systems

When asked to cite the primary challenges in responding to incidents involving virtualized, mobile and atypical systems, respondents indicated multiple challenges for each of these technologies and identified five fundamental challenges:

- Legal issues of ownership and privacy
- Lack of standards and tools
- Lack of skills, training and certification
- Lack of established policy
- Lack of visibility

The majority of challenges selected in this survey relate to virtual (including cloud) systems and mobile devices. Respondents reported only about 70% as many challenges for atypical systems as they did for mobile or virtualized systems. This correlates with Figure 10, in which one-fifth of respondents indicated they conducted investigations on atypical systems.
Meanwhile, the type of challenges reported for virtual (including cloud) and mobile systems is nearly identical, as shown in Figure 14.

![Figure 14. Challenges of New Technologies](image)

Normalized responses for “virtual or cloud” hovered near 20%, indicating that all of these challenges are commonly faced by organizations and that the challenges are of equal significance.

**Challenges of Mobile Devices**

Legal issues of ownership and privacy was the main challenge for mobile devices, with 27% of the normalized responses indicating this to be their biggest challenge. “Skills and training” for mobile appears less problematic, being listed in only 17% of the normalized responses. This may indicate that forensic training addresses at least some of the needs related to mobile devices. Keeping in mind the responses illustrated in Figure 12—specifically, more than three-fifths of respondents use a device’s filesystem or physical data in their investigations—while considering these numbers, it may be that “dump and image” of mobile devices isn’t a technical challenge for our respondents.

Nevertheless, if use of data recovered by such means is a priority for an organization, it should ensure that the policies surrounding the use of such tools keeps pace with their technical advancement.

In the case of atypical platforms such as embedded systems and game consoles, the two top challenges were the lack of standards and tools and lack of skills, training or certification (each receiving about 25% of normalized responses). Not surprisingly, legal issues of ownership and privacy was not rated a significant concern for such devices.
Challenges of Virtualized Systems, With or Without the Cloud

When respondents were asked which activities were the most difficult to complete in virtual and cloud environments, the most frequent response (56%) was “imaging the environment.” Respondents reported that disk acquisition (52%) and memory acquisition (40%) are also difficult in cloud environments, as shown in Figure 15.

![Figure 15. Forensics Complicated by New Platforms](image)

Most “infrastructure as a service” (IaaS) providers offer some ability to image disks through volume snapshots, although imaging of memory is rarely available. This suggests that many forensic professionals do not consider memory imaging important when compromises occur in IaaS environments. It may also indicate that the difficulty of obtaining memory images in such cases outweighs their perceived usefulness.

Legal processes (40%), live response (36%) and monitoring for events (30%) are also identified as difficult activities in IaaS-based cloud environments. Some of the respondents who selected “Other” reported that they “only copy content.” The difficulty of obtaining both data access and timely response from third-party providers was a common theme.
Investigative Costs

The scope of an investigation largely controls its cost, and the scope is largely based on the goals of the investigation. Scope isn’t the only factor that affects cost; complexity is another driving factor.

When asked about the scope and cost of their investigations, the majority of respondents (55%) reported that most of their investigations are small, costing less than $50,000. These likely represent investigations that are conducted almost completely in-house, without any need for outside consultants or a substantial commitment from in-house legal teams.

This may also represent investigations that do not involve regulatory oversight and are not intended for use in legal proceedings, such as a find-it-and-fix-it repair. Alternatively, in the case of law enforcement it may indicate investigations where evidence never appears in court, but is used to encourage acceptance of a plea bargain. Figure 16 shows the distribution of reported average costs of investigations.

In the other large group of answers, 37% of respondents reported that the scope of their investigations varied too widely to assign an average cost.

With nearly 8% of the respondents who were able to assign a cost to investigations saying that most cost more than $50,000, it’s clear that the expenses associated with a digital forensics investigation can be varied and complex.

Understanding all of these complexities, particularly at the high end of the scale, is difficult. However, smaller organizations (particularly those with limited budgets) could benefit substantially by considering the costs before they dive into an investigation that relies on digital forensics.
Recommendations

To complement the advice presented in the preceding discussion, we offer a baker’s dozen set of recommendations to the readers of this paper.

1. Respondents indicated that training and certification are challenging for investigations in virtual and cloud environments. As your organization increases its cloud and virtual footprint, ensure that the skills of your forensic investigators keep pace with current technologies.

2. Take inventory of the tools used by your digital forensics staff. Find out which tools are developed in-house and what problems they solve. Leverage existing vendor relationships to close capability gaps in tools, leaving your forensic staff to do what they do best—namely, forensics. The tools at your disposal must provide timely, accurate and insightful analysis to forensic specialists.

3. If your organization uses cloud services, review your SLA for assistance with forensic investigations. If your organization is planning a move to the cloud, ensure that you negotiate an acceptable SLA, establish relevant policies and train team members before the migration. It is important to understand which tools the provider uses in forensic investigations, and the tools’ limitations as well as strengths.

4. Increase the involvement of legal team members in forensic investigations. Many organizations involve the legal team only in investigations they feel are likely to involve law enforcement or be resolved in court. However, every investigation has the potential to end in court proceedings, so legal staff should be consulted in most if not all investigations. The improved working relationships between forensic investigators and legal staff will be an even greater asset when complicated cases arise.

5. Use forensic investigations to identify potential issues before they rise to the level of incidents. Involvement of incident response professionals in daily operations can help detect problems before they are incidents, lowering the overall cost of your forensic staff.

6. Update policies and procedures regarding forensic investigations to account for new policies and technologies. More than half of respondents reported that their policies needed revision.

7. Ensure that your forensic team has input into the creation of the policies they’ll have to implement. Staff will be less likely to correctly implement policies that don’t align with industry best practices.

8. Budget appropriately for forensic investigations. These are understandably expensive, but their true costs are often underestimated, resulting in sticker shock when upper management sees the bills. Educating management now on the factors that affect the cost of forensic investigations will save pain later.

9. Improve visibility into IT security operations. Several survey responses suggest that this is still a problem for many organizations. Enhanced visibility improves the chances of discovering an incident early, neutralizing it and lowering the cost of the investigation.

10. Seek out cross-disciplinary training for personnel who may be involved with investigations. Forensic professionals need to understand law in order to better engage with legal advisors. Lawyers need education about technology and forensic techniques so they can better advise forensic professionals.
11. Vendors must develop tools that are easier to use and that better serve the diverse and changing environments in which investigations now occur. Early and accurate detection is vital to incident response.

12. Vendors also need to develop tools that are more cost-effective than current offerings so that the community does not need to rely so much on custom tools that may be used only once or twice. These tools must support emerging and unconventional platforms such as cloud, embedded, mobile and virtualized systems.

13. New investigative practices will develop as forensic professionals and legal authorities gain more experience with new and unconventional platforms. Everyone in the community should be abreast of the latest cases and practices.
The computing landscape continues to diversify, moving away from PC-derived hardware to include new technologies; mobile devices, BYOD policies and embedded systems complicate many investigations. Cloud and virtualized environments are increasingly part of the picture and present their own challenges.

The survey results indicate that many challenges to digital forensics come with the deployment of these “new” platforms. However, survey participants report that they are already engaging these environments and embracing their challenges with the help of a variety of tools and processes available today. A large percentage of respondents are also relying on home-developed tools and processes, and organizations indicate an equal need for improvement in their own tools as well as the commercial tools available today.

To keep pace, forensic professionals, and the educators and vendors who support them, must redouble their efforts in training and educating their investigators in the legal and technical processes of conducting investigations that involve modern computing technologies.
About the Authors

Paul Henry is one of the world’s foremost global information security and computer forensic experts with more than 20 years’ experience managing security initiatives for Global 2000 enterprises and government organizations worldwide, and is a principal at vNet Security, LLC. Paul also advises and consults on some of the world’s most challenging and high-risk information security projects, including the National Banking System in Saudi Arabia, the Reserve Bank of Australia, the Department of Defense’s Satellite Data Project (USA), and government and telecommunications projects throughout Southeast Asia.

Jacob Williams, a principal consultant at CSRgroup Computer Security Consultants, has more than a decade of experience in secure network design, penetration testing, incident response, forensics and malware reverse engineering. Before joining CSRgroup, he worked with various government agencies in information security roles. Jake is a two-time victor at the annual DC3 Digital Forensics Challenge.

Benjamin Wright is the author of several technology law books, including *Business Law and Computer Security*, published by the SANS Institute. With more than 25 years in private law practice, he has advised many organizations—large and small, private sector and public sector—on privacy, computer security, email discovery and records management, and he has been quoted in publications around the globe, from the *Wall Street Journal* to the *Sydney Morning Herald*. He teaches the law of data security and investigations at the SANS Institute and is a graduate of Georgetown University Law Center.

SANS would like to thank its sponsors:
## Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Oslo 2015</td>
<td>Oslo, NO</td>
<td>Mar 23, 2015 - Mar 28, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS 2015</td>
<td>Orlando, FLUS</td>
<td>Apr 11, 2015 - Apr 18, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>RSA Conference 2015</td>
<td>San Francisco, CAUS</td>
<td>Apr 19, 2015 - Apr 22, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>Security Operations Center Summit &amp; Training</td>
<td>Washington, DCUS</td>
<td>Apr 24, 2015 - May 01, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS London 2015</td>
<td>London, GB</td>
<td>Apr 27, 2015 - May 02, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS SEC401 London</td>
<td>London, GB</td>
<td>Apr 27, 2015 - May 02, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Bahrain 2015</td>
<td>Manama, BH</td>
<td>May 02, 2015 - May 07, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Security West 2015</td>
<td>San Diego, CAUS</td>
<td>May 03, 2015 - May 12, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure India 2015</td>
<td>Bangalore, IN</td>
<td>May 04, 2015 - May 16, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure Europe 2015</td>
<td>Amsterdam, NL</td>
<td>May 05, 2015 - May 25, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS/NH-ISAC Healthcare Cybersecurity Summit</td>
<td>Atlanta, GAUS</td>
<td>May 12, 2015 - May 19, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Pen Test Austin 2015</td>
<td>Austin, TXUS</td>
<td>May 18, 2015 - May 23, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Melbourne 2015</td>
<td>Melbourne, AU</td>
<td>May 18, 2015 - May 23, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS Security Training - Houston</td>
<td>Houston, TXUS</td>
<td>Jun 01, 2015 - Jun 05, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS410 Vienna in Association with IAEA</td>
<td>Vienna, AT</td>
<td>Jun 06, 2015 - Jun 10, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dublin 2015</td>
<td>Dublin, IE</td>
<td>Jun 08, 2015 - Jun 13, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Houston 2015</td>
<td>OnlineTXUS</td>
<td>Mar 23, 2015 - Mar 28, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>