

Computer Forensic Services and the CPA Practitioner



2010-2012
Forensic Technology Task Force
Ron Box
Margaret Daley
Carl Hoecker
Joel Lanz
Charles Reid
Donna Tamura

A special thank you to Al Lewis and Robert Sha for their contributions and assistance to the authors of this white paper.
In addition, members of the 2011-2012 AICPA Forensic and Valuation Services Executive Committee and the Forensic and Litigation Services Committee provided review to the authors and AICPA staff.

Table of Contents

Executive Summary.....	4
Introduction	6
Part I	9
What is Computer Forensics?	9
The Role of Technology and Computer Forensics in Supporting the Forensic Accountant.....	10
The Benefits of Computer Forensics and Data Analysis.....	11
Challenges Encountered In Providing Computer Forensic Services	13
Part II	15
Planning Computer Forensics Engagement.....	15
What is the Objective of a Computer Forensic Engagement?.....	16
Legal Parameters.....	17
Setting Expectations for Computer Forensics	20
Relationship Between Data Size and Documents.....	21
Locating ESI	22
Where Can Data Reside?.....	22
What Kind of Data Potentially Resides on a Computer?	22

Forensic Accountant	24
Execution of the Computer Forensic Engagement	24
Examination of the Device(s) to be Collected	25
Expertise	26
Quality and Management Controls	26
Part III	27
Is the Imported Data Complete and Accurate?	27
Can the Requisite Skills of the Forensic Accountant and Technology Be Combined to Deliver Engagement Results?	28
Can the Forensic Accountant Obtain the Data in the Format Needed?	29
Does the Data Extracted Need to Be Normalized or Cleansed?	30
What Type of Inquiries Can Be Performed With Data Analysis?	30
What Tools Are Available to the Forensic Accountant to Analyze Data?.....	32
Data Analysis Versus Data Mining	34
Conclusion	34
Appendix A.....	35
The Computer Forensic Engagement – A Case Study.....	35
The Tiered Approach	36
Static Forensic Examination.....	36
Analysis.....	39



This white paper was prepared to provide background for CPAs wishing to learn more about forensic technology services and represents the views of the AICPA's Forensic & Litigation Services Committee – Forensic Technology Task Force. This white paper does not establish standards, preferred practices or approaches, nor is it to be used as legal advice or as a substitute for professional judgment. Other approaches, methodologies, procedures and presentations may be appropriate in a particular matter because of the widely varying nature of litigation services and jurisdictional procedures and protocols, as well as specific or unique facts about each client and engagement. Readers are encouraged to consult with legal counsel regarding laws and local court requirements that may affect the material contained in this special report.

Executive Summary



The forensic accountant has an obligation to adhere to all applicable professional standards, laws and regulations when performing professional services that include the use of computer forensics.

Forensic technology services include computer forensics and related data analytic services as well as evidence and discovery management services (“e-discovery” or “EDM”). Although this white paper will discuss each of these, the primary objective of this white paper is to provide background for consideration by CPA professionals (herein referred to as “forensic accountant(s)”) when providing computer forensic services. Forensic accountants who hold the Certified in Financial Forensics (CFF®) credential and/or the Certified Information Technology Professional (CITP®) credential are uniquely positioned to use multi-faceted technologies to efficiently and effectively analyze and review large volumes of disparate digitalized data commonly referred to as electronically stored information (“ESI”). As the term is used in this white paper, computer forensics describes the discipline of gathering and analyzing ESI in a manner that is forensically sound. Computer forensics is different from “e-discovery,” a term that typically refers to a broad spectrum of activities including the collection, preservation, processing, analysis, production, hosting and review of ESI.

The use of computer forensics is not only growing in importance in today’s digital age, its application also is increasing in complexity. The forensic accountant has an obligation to adhere to all applicable professional standards, laws and regulations when performing professional services that include the use of computer forensics. In addition, it is the forensic accountant’s responsibility to understand which standards, laws and regulations may apply to a specific engagement. The professional standards that apply include the AICPA Code of Professional Conduct and the AICPA Statement on Standards for Consulting Services (SSCS No. 1).

In this white paper, the increased role of computer forensics is discussed in three parts.

Part I: Exploring what is encompassed by computer forensics; the role of technology and computer forensics in supporting the forensic accountant; the benefits of computer forensics and data analysis; and challenges in providing computer forensic services.

Part II: Discussion on considerations in planning the computer forensic engagement; defining the objectives of a computer forensic engagement; locating or finding ESI; and execution of the engagement.

Part III: Discussion on the importance of technologies and methodologies that can be used to evaluate the data once acquired; considering completeness and accuracy of the data prior to processing it for review; formatting and cleansing issues; and data analysis tips along with describing tools that can help the forensic accountant.

Appendix A: Provides a computer forensic engagement case study

Computer forensics is a complex practice area and it is impractical to discuss in this white paper how the use of computer forensics can impact all forensic accountants. This white paper is intended to provide the forensic accountant and other interested parties with a basic understanding of the complexities involved in a computer forensic engagement and may benefit the following constituents:

- Forensic accountants providing forensic litigation services including those providing investigative, dispute or proactive risk management services
- CPAs practicing as independent auditors who need to comply with SAS99, including the analysis of non-standard manual
- Internal auditors or company management responsible for electronic data analysis and risk management
- Attorneys who want to understand the expectations of CPAs performing these services
- Audit committee and board of director members wanting to understand basic concepts of computer forensics and its impact on electronic data gathering and analysis in an investigative setting

Beyond this white paper, the forensic accountant can find a wealth of additional guidance and insights in other bodies of knowledge, including:

- Other writings developed within the [CFF body of knowledge](#)
- Other writing developed within the [CITP body of knowledge](#)



This white paper is intended to provide the forensic accountant and other interested parties with a basic understanding of the complexities involved in a computer forensic engagement.



Every organization should consider its vulnerabilities and assess the benefits of having a basic forensic skill set capable of proactively managing fraud risks, detecting fraud, and putting in place a responsible process to respond to allegations of fraud and the knowledge of when to engage a forensic professional to take over the investigation and carry it to a productive conclusion.

Introduction

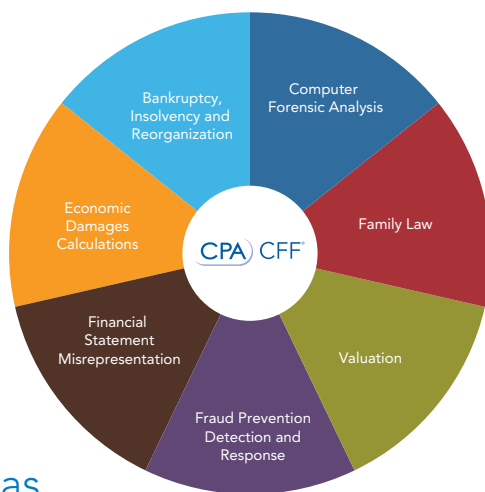
Computer forensics and the use of forensic technology have become more commonplace in today's complex business environments. CPAs in public practice, business and industry, government, and not-for-profit organizations can all benefit from a fundamental understanding of computer forensics as it may apply to fraud prevention, investigations, litigation and dispute matters, and other forensic-related services.

The initial discovery of fraud, or at least the suspicion of fraud, can sometimes be determined by company personnel without the involvement of outside professionals capable of in-depth forensic analysis. Every organization should consider its vulnerabilities and assess the benefits of having a basic forensic skill set capable of proactively managing fraud risks, detecting fraud, and putting in place a responsible process to respond to allegations of fraud and the knowledge of when to engage a forensic professional to take over the investigation and carry it to a productive conclusion. These basic skills may include records management practices and the impact on investigations; knowledge of legal issues that may impact the investigation of potential fraudulent conduct; understanding basic evidence preservation practices so as to not compromise the integrity or contaminate evidence; and the development of protocols to address instances of alleged fraudulent conduct.

The increasing digitalization of information and resulting complex and disparate technology environments; the overwhelming amounts of digital information; and the ever changing investigative landscape, underscore the importance of forensic accountants having a base-level understanding of computer forensics and the benefits of using data analytic and technology

tools. An increasing number of forensic accountants are developing specializations and are obtaining the CFF and CITP credentials. The AICPA has enabled member CPAs to gain a sound understanding of forensic and technology issues through these credentials and the resources related to the bodies of knowledge. In fact, when viewed in combination, both the CFF and CITP credentials provide a very broad structure encompassing forensic accounting techniques and pertinent information technology skills. Given that a great deal of fraud occurs through the use of technology, persons possessing the skill set represented by the CFF and CITP credentials are able to provide an understanding of how computer based fraud can occur and can be prevented and detected.

The CPA with specialized forensic accounting skills may focus on various areas of practice as depicted below in the CFF body of knowledge wheel.



CFF Niche Areas

The CITP is trained in the specific skills represented by the CITP body of knowledge and encompasses areas of focus presented on the wheel below. This body of knowledge includes technology issues that represent a strong foundation in the hardware, software, and techniques used in computer forensics. These skills, when combined with the CFF body of knowledge, form an excellent foundation for forensic analysis.

Although this combined body of knowledge represents a broad set of specific technology skills and processes, it can be thought of in terms of a process that requires continuous re-evaluation of risk, information management and business intelligence, evaluation, testing and reporting, internal controls and IT general controls.

Technology can be used to facilitate fraud. Computer-facilitated fraud takes advantage of the ubiquitous nature of technology in conducting business in the 21st century. Enormous



CITP Niche Areas

amounts of money are moved around the globe every day, and a knowledgeable thief can take advantage of vulnerabilities inherent in many IT operating systems, tools and processes. Cybercrime poses a potentially significant risk that should be considered by most organizations. The sheer scope of the Enron case is believed to be the largest computer forensics case in history.¹ Organizations may find it helpful to utilize specialists in information security to devise and maintain countermeasures to mitigate the security risks of doing business electronically.

Fraud often is perpetrated by an organization's own employees and may include fraudulent financial reporting, asset misappropriation or general fraudulent misconduct. Individuals who perpetrate fraud have access to confidential information and the systems employed by the organization in the normal course of business. They understand the vulnerabilities of an organization's system of internal controls. There typically are three conditions present when a fraud occurs: opportunity, pressure or incentive and rationalization (see SAS 99). A well designed internal control system includes controls to prevent, detect and respond to fraud risks and is a good way to mitigate fraud risks. While the possibilities of overriding internal controls always are present, the use of computer forensics in analyzing electronic information and transactional activity may be useful in the detection of fraudulent activities. Even an organization with a well-designed system of internal controls may fall victim to fraud if they do not establish effective monitoring and detection measures.

¹ For further information see usatoday.com/money/energy/enron/2002-02-19-forensic-detectives.htm#more. And google.com/search?q=enron+computer+forensics&ie=UTF-8&oe=UTF-8&hl=en&client=safari



Part I

What Is Computer Forensics?

The U.S. Department of Justice defines computer forensics as “the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events. ... Many argue whether computer forensics is a science or art. The argument is unnecessary. The tools and methods are scientific and are verified scientifically, but their use necessarily involves elements of ability, judgment and interpretation. Hence, the word “technique” often is used to sidestep the unproductive science/art dispute.”²

Digital media comes in many forms, including the hard drives found in personal computers, external drives, telephones, smartphones, PDAs and telephone voice mail systems. Computer forensics typically are performed to determine what activity took place on a particular device by a user or to restore previously deleted or corrupted data. Computer forensics commonly is performed during a fraud investigation because the results can provide a roadmap as to what the key players involved likely knew, when they were likely to know it, the documents to which they had access, actions taken, with whom they communicated, and whether they appeared to try to hide their actions. The Internet history, web-based email, lost or deleted files, logging and registry files are examples of data the forensic accountant can utilize as evidence in their engagements.

Computer forensics commonly is performed during a fraud investigation because the results can provide a roadmap as to what the key players involved likely knew, when they were likely to know it, the documents to which they had access, actions taken, with whom they communicated, and whether they appeared to try to hide their actions.

² Source: U.S. Department of Justice. United States Attorney’ Bulletin, January 2008. [justice.gov/usao/eousa/foia_reading_room/usab5601.pdf](https://www.justice.gov/usao/eousa/foia_reading_room/usab5601.pdf)

The Role of Technology and Computer Forensics in Supporting the Forensic Accountant

Depending upon the scope and predication of the engagement, any of the seven forensic investigation techniques³ may rely significantly on ESI. The following are a few examples. In conducting electronic surveillance, the forensic accountant may design computer-assisted audit techniques known as continuous monitoring to proactively analyze financial transactions and identify anomalies in the transactional data such as excessive activities or amounts of electronic fund transfers as they are being processed. In conducting undercover operations, “honeypots”⁴ can be designed and incorporated into information security protection strategies to deceive potential electronic thieves and gather evidence to support further prosecution. When analyzing financial transactions, data mining techniques also can be used to identify relationships between data examined, enabling the discovery of suspicious trends or improprieties. The analysis of financial transaction patterns to credit card activity is an example of this type of investigative technique that can help prevent and reduce the potential for fraud.

An abundance of data creates both challenges and opportunities for the forensic accountant. The sheer volume, for example, of databases within and outside the investigated company provides the forensic accountant with unmatched capabilities to interrogate and analyze data for unusual patterns or anomalies. The challenge for the forensic accountant is to control and harness this information as well as to conduct and complete thorough investigations in a timely fashion. This challenge is exacerbated by the explosion of additional sources that require time and diligence to properly conduct the forensic engagement.

In conducting undercover operations, “honeypots” can be designed and incorporated into information security protection strategies to deceive potential electronic thieves and gather evidence to support further prosecution.

³ Forensic Procedures and Specialists: Useful Tools and Techniques, AICPA, 2006, pp.3-6. Please refer to this AICPA publication for further details and definitions relating to each of the seven techniques

⁴ [en.wikipedia.org/wiki/Honeypot_\(computing\)](https://en.wikipedia.org/wiki/Honeypot_(computing))

The opportunity for leveraging technology to analyze data for the purposes of fraud detection and investigations has long been recognized. In the landmark study “Managing the Business Risk of Fraud: A Practical Guide,” the authors identified how data analysis, continuous auditing and monitoring techniques, and other related technology tools can be used to detect fraudulent activity. The study described data analysis as using “technology to identify anomalies, trends and risk indicators within logic populations of transactions ... And to identify relationships amongst people organizations and events.”

Rather than initially focusing on technology, the forensic accountant should clearly define the engagement objectives, and based on the scope, determine how computer-assisted data analysis can be used to conduct or facilitate the engagement. Forensic accountants sometimes believe data analysis can only be used when extensive amounts of information are examined. Although cost benefits should be considered, many data analysis tools provide the forensic accountant with high-level analysis information with only minimal need for programming experience. These types of analyses can assist the forensic accountant in determining the direction or relevancy of further detailed data analysis strategies to support the engagement’s objectives. For example, once downloaded into a data analysis tool, a quick analysis that includes stratification of amounts or transaction types including identifying duplicate records or missing information can be performed with minimal programming skills or involvement. This high-level information can also be used by legal teams in determining overall strategies in pursuing litigation. It also is important to define under whose direction the tools will be used and to what extent, if any, they will be protected under attorney client privileges.

The Benefits of Computer Forensics and Data Analysis

Imagine having to analyze hundreds of thousands or even millions of line items of journal entries, invoice items, receipts and disbursements. How would the forensic accountant identify items to test or further analyze for certain risk elements? Without the benefits of computer-assisted data analysis, the forensic accountant would be looking for a needle in a haystack. Today, with the sophistication of powerful software and the technological ability to extract large amounts of data, 100% of the population of information may be analyzed. Data can be retrieved from a company’s general ledger system, sales databases, time and expense systems, network drives, user files, various types of logs such as web logs, building access logs, and essentially anywhere electronic data resides. Some of the benefits of incorporating data analysis include:

- The ability to reduce or even eliminate sampling risk
- The comparison of relevant types of data from different systems or sources to show a more complete picture



Without the benefits of computer-assisted data analysis, the forensic accountant would be looking for a needle in a haystack. Today, with the sophistication of powerful software and the technological ability to extract large amounts of data, 100% of the population of information may be analyzed.



Forensic accountants can use computer forensics by electronically analyzing manual journal entries, and using analytical tools to identify anomalies and potential areas of risk.

- The ability to easily trend relevant data over periods of time; fluctuations in trending lines can be analyzed further for false positives and potential risk factors
- The quick identification and extraction of certain risk criteria from the entire data population for further analysis
- The testing for effectiveness of the control environment and policies in place by identifying attributes that violate rules
- The identifying trends of which company personnel, consultants and forensic accountants were unaware

SAS No. 99 (SAS 99), Consideration of Fraud in a Financial Statement Audit, discusses an auditor's responsibility to further address the risk of management override of controls. Paragraph 61 states, "The auditor's procedures for testing journal entries and other adjustments will vary based on the nature of the financial reporting process. ... When information technology (IT) is used in the financial reporting process, journal entries and other adjustments might exist in only electronic form. Electronic evidence often requires extraction of the desired data by an auditor with IT knowledge and skills or the use of an IT specialist ... it may be necessary for the auditor to employ computer-assisted audit techniques ... to identify the journal entries and other adjustments to be tested."⁵

In today's environment, the forensic accountants often assist auditors in their audits through SAS 99 procedures. Forensic accountants can use computer forensics by electronically analyzing manual journal entries, and using analytical tools to identify anomalies and potential areas of risk. Forensic accountants may also assist in the testing of supporting documentation for the higher risk manual journal entry areas to better understand the potential risks. Doing so also helps further tailor data analyses to either gain comfort that the journal entries were recorded properly, or identify errors or irregularities. In certain higher risk scenarios, forensic accountants may even design procedures associated with the review of emails. Such procedures may include developing the list of search terms and custodians as well as analyzing the actual output of the email searches.

⁵ Source: Statement of Auditing Standards No. 99, Consideration of Fraud in the Financial Statement Audit, paragraph 61

Challenges Encountered in Providing Computer Forensic Services

If the benefits of using computer forensic techniques and methodologies in support of a forensic engagement are so abundant, it would benefit the forensic accountant to incorporate computer forensic techniques into their engagements to the extent possible. Similar to other project planning activities and investments, the forensic accountant must evaluate the ability and upfront investment to satisfy the objectives of the engagement in the most effective and efficient way. Even if electronic evidence can often be obtained quickly and thoroughly and abundant opportunities exist through analyzing electronic data, these advantages and opportunities need to be evaluated in terms of the risk involved and the ability of the forensic accountant to mitigate these risks. Following are issues that forensic accountants might consider in incorporating data analysis into their forensic engagement strategy.

Obtaining the electronic data poses challenges for the forensic accountant. Even when the appropriate legal permissions are obtained, accessing the data and making sure it is the relevant data can be challenging. For example, was sufficient data maintained on the systems to properly analyze trends over the appropriate time period to be investigated? Many times the forensic accountant will find that the data may not be in one location or that there may be various iterations of the data located on different mediums. Data contained in one database may not correspond to data maintained another. In this instance, the forensic accountant will need to determine how to identify and extract the data most relevant to the analysis. In other situations, the data may or may not be available in an appropriate version that can be used to conduct data analysis. For example, databases that store data in proprietary databases do not facilitate examination by non-related data extraction or other analysis tools. The data could also be stored in a format or medium that may need to be converted to perform various data analyses. Frequently, this can include an electronic file, such as PDF, that needs to be converted to a file format that can be used to perform data analysis.

Obtaining the electronic data poses challenges for the forensic accountant. Even when the appropriate legal permissions are obtained, accessing the data and making sure it is the relevant data can be challenging.

In these situations, the forensic accountant will benefit from adhering to the various evidence custody practices discussed in this white paper, including maintaining appropriate chain of custody and working with forensic images of the data, not the raw data. It is important in these situations that the forensic accountant document, step-by-step, how the data were collected, how the data were normalized and how the data were converted from their original format to data that were subsequently used in the engagement. Such documentation is critical in demonstrating compliance with the chain of custody and protecting the forensic accountant from any challenges that may be made regarding the evidence.

Another challenge in obtaining the data can sometimes be the various silos that may exist in large organizations. When subpoenas or production requests are involved, the organization should take appropriate actions to comply with the subpoena. However, sometimes the forensic accountant may be engaged to conduct preliminary or internal assessments or investigations prior to the matter becoming a formal legal proceeding, or in the absence of a documentation preservation request or subpoena. In these cases, it is not uncommon for individuals within such organizations to try to protect their data. Preserving the integrity of the data and navigating through such political minefields is something the forensic accountant needs to plan as they develop their strategies and project budgets. This planning may involve coordination with legal counsel.

Also contributing to the complexity of providing computer forensic services are national and international privacy laws and regulations. Such regulations require that the forensic accountant carefully evaluate the need to obtain confidential personal information. If required, the forensic accountant may need to implement safeguards to mitigate the risk of data breaches, and gather only the data that may be considered incidental to the engagement. If such information is obtained, the forensic accountant will need to implement appropriate data security and protective strategies to minimize the threat of unauthorized disclosure and use of such information.⁶

Such regulations require that the forensic accountant carefully evaluate the need to obtain confidential personal information.

⁶ For further information see aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/Pages/Generally%20Accepted%20Privacy%20Principles.aspx



Part II

Planning Computer Forensics Engagement

Preparation and planning are important to meeting the objectives of a computer forensic engagement. Proper planning allows the forensic accountant to meet the engagement objectives, satisfy standards and produce solid, defensible results. The engagement scope, understanding of the forensic accountant's role, and clarifying deliverables to be issued should be agreed upon at the outset of the engagement. To that end, the forensic accountant will need to arrange for access to various information and documents that are needed from the client. Expectations of the computer forensic engagement should be established with the client.

When conducting a forensic engagement, it is wise to consider how technology has been used in an organization, including use by individuals that are of interest to the forensic accountant. Many fraud cases have been solved by determining who a key player had access to certain information and/or tried to delete documents or data. Computer forensics can provide critical intelligence as to what the computer user knew, when they knew it, whether they transmitted information to other parties and whether they tried to cover their tracks by intentionally deleting data or documents.

Prior to conducting a computer forensic engagement, it is imperative that the forensic accountant understand the scope of the forensic engagement, including the engagement's objectives and how the results will be used. This section will cover the nature of computer forensics and describe best practices for conducting these examinations.

When conducting a forensic engagement, it is wise to consider how technology has been used in an organization, including use by individuals who are of interest to the forensic accountant.



While computer forensic engagements can be useful in many situations, understanding the context of the engagement plays a key role in helping the forensic accountant clarify the engagement objectives.

Computer forensics can provide information on the computer's user activity such as dates and times the computer was in use and what websites were visited. It can also provide granular information on actions taken on particular documents stored on a device such as the date a letter was amended, when a PowerPoint was created or who originally created a presentation or contract. It also is important to ensure that proper chain of custody and documentation are deployed in order to authenticate the results of the examination and withstand challenges to the conduct of the engagement and resulting conclusions.

Better practices in computer forensics are systematic rather than ad-hoc. A systematic computer forensic analysis is characterized by:

- Applying sound and repeatable methodologies
- Using practices that have historically withstood challenge
- Using forensic software that generally is accepted in the forensic profession
- Using methods that yield reproducible results
- Developing comprehensive documentation

What Is the Objective of a Computer Forensic Engagement?

While computer forensic engagements can be useful in many situations, understanding the context of the engagement plays a key role in helping the forensic accountant clarify the engagement objectives. Potential computer forensic engagements may relate to fraud prevention and detection control assessments; bankruptcy-related investigations and consultations; dispute advisory assistance (i.e., family law, valuation assistance, non-testifying privileged consulting, and expert services and damages calculation); and investigations (that is financial reporting and security investigations, regulatory compliance investigations and misappropriation of assets) to name a few. Requests for computer forensic assistance come from a variety of sources including corporate security professionals, internal and external audit teams, in-house counsel, outside law firms and individuals.

There are a number of commercially available forensic software tools that can assist a forensic accountant in providing computer forensic services, and it is important to remain knowledgeable about such tools and the distinctive advantages of using them, including remaining up to date on version upgrades and new solutions. To this end, the forensic accountant may find it helpful to use information distributed by organizations such as the National Institute of Justice (NIJ) Electronic Crime Technology Center of Excellence. The NIJ Electronic Crime Portfolio is working to build and sustain the electronic crime investigation, digital evidence collection and digital evidence examination capacity of the criminal justice community throughout the United States.



Legal Parameters

Before embarking on an engagement, it is important to consider the legal issues that are relevant to each case. Factors to consider include:

- Are the data being collected pursuant to a subpoena?
- Is the engagement team working at the direction of counsel, under privilege?
- Is the expert fully qualified and licensed where necessary and providing a sound opinion? For example, could the forensic accountant sustain challenges?
- Does state law require that the data be collected and analyzed by a licensed private investigator?
- If data are being collected internationally, is the engagement team familiar with international privacy laws?
- Does the forensic accountant or client have legal authority to gather the data? To whom does the data belong? Are there privacy concerns?
- Will the scope of the examination be limited to only relevant data?

- Are there Fifth Amendment or self-incrimination considerations?
- Is there an expectation that data may be located on the devices that would require reporting to law enforcement authorities (child pornography, national security issues)?

It is best to discuss these issues with legal counsel prior to beginning a computer forensics engagement to make sure that all relevant legal requirements are met and that the protocols are designed to ensure compliance.

When starting a computer forensics engagement, the forensic accountant should obtain initial facts and documents prior to beginning the work. This involves confirming with the client the following: (1) the nature and scope of the engagement; (2) the computer systems and technology involved and (3) the expected end deliverable. The following is a list of intake questions that the forensic accountant may want to consider:

- What is the nature of the engagement, (i.e., investigation, dispute, regulatory compliance assessment)?
- What is the nature of the matter – civil, criminal or regulatory proceeding?
- What is the relevant date range of activity?
- What are the corporate departments that are impacted? Accounting? Legal? Marketing? Executive suite?
- What are the known key documents?
- Are there copies of any litigation, subpoenas or other relevant legal papers that can be produced for the forensic accountant?
- Is the data subject to any preservation order or requirement?
- What is the monetary value/issue in controversy?
- Does the person requesting the examination have the legal authority to possess and examine the equipment?

- What is the expected scope of the examination? How many devices? What type? Will data have to be collected from a computer network?
- What is the identification and contact information of the investigative team?
- What important information is known to the investigative team to date, such as known associates, account numbers, key emails, product names, etc.?
- What computer systems and technology will be examined? Types of computers (Mac, PCs or others), type of servers (Outlook, SQL), smartphones (iPhone or BlackBerry)?
- What is the number, make, model and storage capacity of every device or media to be examined?
- Who is the key point of contact with the client's internal IT department?
- What operating systems, email systems, application and document management systems are in use?
- What, if any, encryption tools are in use?
- What is the nature and type of structured data stores to be analyzed?
- Is there a data map of the network?
- What, if any, prior forensic work has been performed?
- What are the relevant corporate policies (privacy, confidentiality, IT security and usage)?
- What are the usernames, passwords and employee numbers?
- What is the personal identifiable information of the users (such as date of birth, SSN)?
- What access level was each user granted?



A decision to not include certain information in the scope of the forensic accountant's work may affect the overall integrity of the engagement and should be carefully considered.

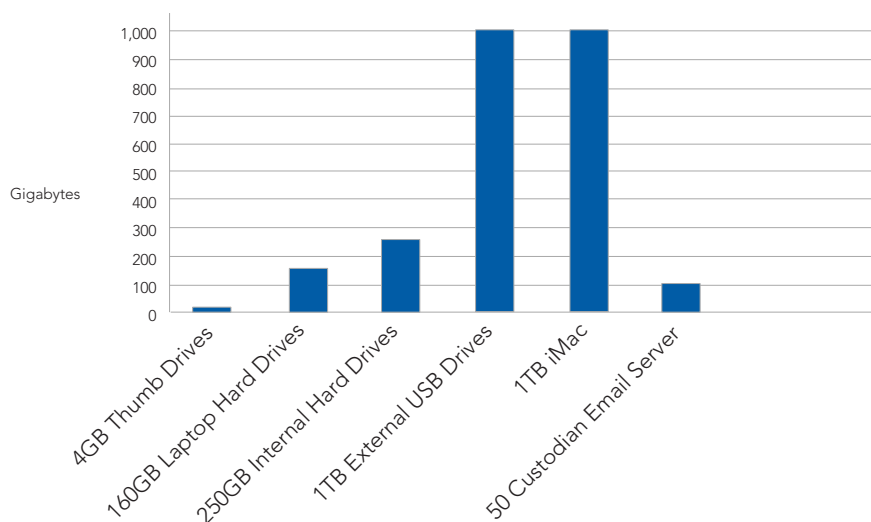
Setting Expectations for Computer Forensics

At the beginning of the engagement, it is important for the forensic accountant to discuss the timing, budget and scope expectations. The amount and location of the data, how it is maintained and the number of locations to be visited will significantly affect the cost of the work and may create significant delays in completing the engagement. In addition, certain types of inactive data, such as backup tapes or orphaned systems, may be so expensive to examine that the cost/benefit of conducting the examination may not be reasonable.

A decision to not include such information in the scope of the forensic accountant's work may affect the overall integrity of the engagement and should be carefully considered. It may also be appropriate to defer examination of such data pending the findings of an initial phase of the investigation.

Developing budgets in advance of doing the work is advisable. One important driver of the engagement's budget is the volume of data to be analyzed. For example, most laptops have about 50 gigabytes of storage. Newer model computers may have more than 500 gigabytes of storage, and sophisticated users can have external hard drives with several terabytes of data. Few people outside the IT world understand the magnitude of one terabyte of data and the time required to examine that level of data. For example, 20 gigabytes of data, if printed, would be a library floor of academic journals. One hundred gigabytes would be the equivalent of 50,000 trees made into paper and printed. A terabyte of data would be an entire academic research library. The print collection of the U.S. Library of Congress totals two terabytes.

Average Storage Device Capacities*



*Data extrapolated from New Egg.com and store.apple.com

Relationship Between Data Size and Documents

In summary, a significant factor in assessing the cost factor in analyzing computer data is driven by how much data exists and where it resides. One example is that one additional computer to be examined is not the primary determining factor in assessing cost – it's how much storage there is associated with that computer. A computer with a terabyte of data is quite different from a laptop with only 50 gigabytes of storage. Acquainting the investigative team with this distinction is a key element in the management of expectations and in the development of budgets.

Days can be spent processing data incorrectly (such as emails without attachments) and when the errors are found, the work may need to be redone completely. The most cost-effective way to conduct an examination is to build in quality-control checks along the way to ensure the data has been captured, analyzed and processed accurately.

It's also important to stress that results are far from predictable. Processing and analyzing electronically stored information is fraught with peril. Data may be corrupted, processing problems that can cause serious delays in analysis and production errors are extremely common. *Days can be spent processing data incorrectly (such as emails without attachments) and when the errors are found, the work may need to be redone completely. The most cost-effective way to conduct an examination is to build in quality-control checks along the way to ensure the data has been captured, analyzed and processed accurately.* This testing may seem unnecessary to the casual observer, but they are indeed necessary. Due to the nature of electronic data, the question is not whether delays or unexpected challenges will occur, but rather, what type of obstacles will be faced and how will they be handled to cause the least delay and cost.

A final work product can be a forensic report, an oral report, or an affidavit. It is important to know prior to beginning the engagement, the information that is critical to the engagement and how the findings are going to be captured in the final work product.



To further understand the value of potential evidence that resides in electronic form, the forensic accountant should, in addition to the information (text, numbers and graphics) in a data file, understand the process used by computing devices in creating electronically stored information and the digital artifacts created during the process.

Locating ESI

Where Can Data Reside?

Data of forensic interest can be found on just about any device that is used to store data. This includes the following commonly used equipment:

- Laptop computers
- PCs and workstation printers
- Fax machines
- IP telephones
- Personal digital assistants
- Cell phones
- Scanners
- Copiers
- iPods and MP3 players
- Mainframes and servers
- Removable disks
- Solid state storage
- Thumb-drives
- Tapes
- CDs and DVDs
- Email – server or remotely stored
- Voicemail on telephone systems
- Recycle bin
- Instant messenger
- Data stored in the cloud (“cloud”)

What Kind of Data Potentially Resides on a Computer?

To further understand the value of potential evidence that resides in electronic form, the forensic accountant should, in addition to the information (text, numbers and graphics) in a data file, understand the process used by computing devices in creating electronically stored information and the digital artifacts created during the process. Generally, each step used by a computer is recorded and stored either as metadata or artifacts on the storage media. Metadata is structured information that describes, explains, locates or otherwise makes it easier to retrieve, use, or manage an information resource. Metadata often is called data about data or information about information. (niso.org/publications/press/UnderstandingMetadata.pdf, National Information Standards Organization).

A partial list of data file process steps is outlined below. Each step is associated with a potential electronic artifact that may, if recovered, be useful to the forensic accountant.

Step in data file	Potential recoverable metadata or artifact
File is created	Date, type of file (MS Word, Excel, text, etc.)
File stored	Date, location
File modified	Date, location
File deleted	File may still exist on storage media
Deleted file recovered	Partial artifact may exist

Forensic Accountant



Just like the weapon in a crime scene, electronic information can be compromised if it is handled improperly, leaving the findings made by the forensic accountant subject to criticism.

Execution of the Computer Forensic Engagement

Once scope, timing, budget and work product expectations have been clarified, the forensic accountant should develop a work plan that will include the process by which data will be identified and collected. A critical element of the plan is to detail the chain of custody of all data to be collected and analyzed. Just like the weapon in a crime scene, electronic information can be compromised if it is handled improperly, leaving the findings made by the forensic accountant subject to criticism.

A forensic accountant whose expertise is in the technology field, generally uses a chain of custody form that normally captures the following information:

- Name and signature of the person(s) providing the device and collecting the device
- The location of each device specific to its physical location within a room, room number and address
- Description, including make, model number, serial number and condition of every device collected
- The date and time each device was collected
- A case/project number, item number that is marked on the device and the initials of the person marking the device. Due care should be taken not to damage the device. Alternative methods include grouping small items into a sealed and marked bag
 - If being transported, the devices are packaged in antistatic wrapping to avoid loss of magnetic media.
 - All packaging is sealed to show protection from tampering

Once transported to a secure environment for examination, each device collected should be stored in a secure evidence locker or facility. This can be as elaborate as a secure vault or as simple as a locked cabinet. Anyone seeking to examine the device must then "sign out" the device by providing a date and time the evidence was removed along with the name and signature of the person removing the evidence. It is important to maintain the chain of custody once it has been established. Even tiny missteps in protocol can impact the credibility of the entire examination.

Examination of the Device(s) to Be Collected

The next step of the planning is to determine how to examine the device. A number of forensic methodologies are available to a forensic accountant to deploy in any given matter. The following steps describe commonly used methods from least invasive to most invasive.

Initial Response: The steps of evaluating the reported incident or anomaly in a triage mode to determine whether further computer forensics methods should be deployed. This may involve gathering available, preliminary information, such as identifying the individuals with knowledge; determining computers, devices, and software involved, and assessing magnitude of damages. Other considerations are securing or isolating the systems, conferring with counsel, and notifying those responsible for the entity's governance.

Forensic Preview: A cursory, high-level review of the entity's information technology assets involved to determine whether data exists or whether further forensic methods are practical, required, or desirable. A typical forensic preview engagement might involve scanning a computer or device for the existence of some type of data. For example, the law enforcement community uses a software program to determine if there are images on a computer that are consistent with pornography.

Static Forensics: Forensic processes performed by the forensic accountant against static data in order to support the engagement. Most forensic engagements, where a report or testimony is required, are performed in this manner. This involves taking an image of a hard drive and then analyzing that drive in a secure environment. The forensic image cannot be altered and is a mirror image of the original hard drive.

Live Forensics: Forensic processes performed against live or dynamic data. A typical live forensics scenario would involve performing a forensic process on a computer, usually a server, which is considered critical to the performance or sustainability of a company and therefore cannot be powered off. Collecting the data from a server often results in "overcollection" – collecting data that are not relevant to the engagement. If a company's entire email server is collected, for example, many user accounts will be on the copy that are not relevant to the engagement. In circumstances involving structured data such as accounting, or Human Resources records, obtaining the entire server may be necessary in order to run customized reports. Overcollection can be expensive, so in the case of servers, it's vital to have a detailed plan so the forensic accountant knows what portions of a server to collect if the entire server is not necessary.

Expertise

When the need for conducting a computer forensic examination is identified, many companies will ask that their own internal IT department do the work. While this can be a significant cost savings over hiring an outside expert, a number of important questions need to be asked prior to determining that this is appropriate. First and foremost, is the in-house IT resource knowledgeable in conducting a forensic examination? While most IT professionals know how to “ghost” or copy a hard drive, this is substantially different from collecting data in a forensically sound manner. It is important that the forensic accountant determines whether the in-house IT professional has been trained in using forensic software and how much experience they have in the area. Just as a person would not hire a divorce lawyer to argue a death penalty case, all IT professionals do not have the same skill set. The integrity of data may be severely compromised if not collected and handled by professionals with appropriate competencies.

Quality and Management Controls

Good practices in computer forensic examinations, as with consultations and attestations, call for the forensic accountant to establish a quality and management control process. Good practices in computer forensic examinations, as with consultations and attestations, call for the forensic accountant to establish a quality and management control process.

- Was the engagement completed and reported in a timely manner?
- Were the results thorough and adequately documented?
- What level of evidence was required? Beyond a reasonable doubt, preponderance of evidence, etc.?
- Was the client satisfied with the results?
- To what extent was professional judgment used?
- Were engagement performance metrics attained?
- Was an assessment of data reliability performed?
- Was there adequate planning and supervision of evidence gathering and referencing?
- Was there compliance with applicable professional standards and expectations?



Part III

In Part III, we discuss the importance of technologies and methodologies that can be used to evaluate the data once acquired, while considering completeness of data, preparing the data for use in analysis, performing inquiries and data analysis, and tools available to the forensic accountant in analyzing the data.

Is the Imported Data Complete and Accurate?

After overcoming the technology challenges identified above, the forensic accountant needs to ensure that the records provided are accurate and complete. Frequently, data that the forensic accountant gathers come from different systems and therefore, the forensic accountant could be at risk of missing pertinent information. Additionally, data can often be categorized into accounts that may not have been properly extracted during the collection process, potentially limiting the analysis of relevant accounts. These are just a couple of examples of potential challenges one might experience when collecting data. Regardless of the source of information, there are various methods of testing whether the data received is complete and has been normalized in a way that would be acceptable to the adjudicating authority.



The forensic accountant can also request a sample of records, typically the first 100, to be printed out to confirm understandings of layouts and data.

Completeness testing can range from reading and understanding the programming script used to extract the population of data to the reconciliation of processing metrics. To assess completeness and accuracy, the forensic accountant could request a number of records that can be used to compare the converted information with what would be expected. One comparison is to calculate hash values of all the records converted and compare them to predetermined values prior to conversion. This also can be performed on designated field and column totals. If an IT specialist is assisting in collecting data, it may often be helpful for the forensic accountant to be present to watch the extraction process. Often the forensic accountant may notice additional fields of interest to include in the population of the data to be extracted that would otherwise have been missed. Watching and understanding the logic of the script used to extract the data also helps to gain comfort with completeness; i.e., date ranges are proper, account ranges are what the forensic accountant is looking for, etc. The forensic accountant can also request a sample of records, typically the first 100, to be printed out to confirm understandings of layouts and data.

When used in a forensic engagement, the standard of care and the number of procedures required to perform these reviews will be significantly greater and will need to be appropriately documented. Each conversion will require its own controls based on the risks of the conversion and importation. It is the forensic accountant's responsibility to ensure the complete and accurate conversion of the data files and to ensure that the materials they are working with meet the quality control requirements of the particular engagement.

Can the Requisite Skills of the Forensic Accountant and Technology Be Combined to Deliver Engagement Results?

Even if the above obstacles can be overcome, the ability to successfully integrate investigative and technology skills is paramount to achieving desired engagement objectives. In many situations, the forensic accountant may seek certain information but may not have the requisite knowledge to obtain that information. Unfortunately, the technologist assisting the forensic accountant may not have the requisite skills or intuition to interrogate suspected data or initiate queries that can achieve engagement objectives. As a result, an overall data analysis plan should be developed to ensure that forensic procedures are performed based on needs rather than skills.

For example, many forensic accountants begin their data analysis activities by looking at one record or table. Based on the information contained, potential data analysis routines may be identified that may be of interest. What may not be realized is that the data may need to be derived from a variety of databases or related tables. For example, this may include "joining" tables in order to facilitate analysis. Of greater challenge to many forensic accountants is the need to convert data into a format that can readily be electronically analyzed.

Many question the need and level of information technology expertise required to perform data analysis. In reality, the performance of data analysis itself will be intuitive to many forensic accountants already familiar with using electronic spreadsheets. The challenge from a technology perspective is the ability to identify where the data resides, how to access the data, and how to convert the data into a format that can be used by one of the data analysis tools identified above.

Can the Forensic Accountant Obtain the Data in the Format Needed?

In an ideal situation, the forensic accountant will request data be provided in a format that will facilitate easy conversion to a data analysis programs with which they are familiar. If given this format, the forensic accountant can then import directly into their data analysis program and begin the process of preparing for inquiries. For example, many forensic accountants are very comfortable working in the Excel or ASCII format. This allows them to analyze data in a tool with which they already are familiar and if using data analysis software, it provides for a very easy import and conversion of data into the requisite format to use the data analysis program. In these situations, hours incurred in performing data analysis are used exclusively to perform the requisite inquiries rather than the overhead investment of converting data into a usable format.

To facilitate the interoperability of data used or stored by proprietary systems that may have challenging data storage formats, commercially available software tools are available such as the Microsoft-developed Open Database Connectivity (ODBC).

To facilitate the interoperability of data used or stored by proprietary systems that may have challenging data storage formats, commercially available software tools are available such as the Microsoft-developed Open Database Connectivity (ODBC). As described on Microsoft's website, "ODBC is Microsoft's strategic interface for accessing data in a heterogeneous environment of relational and non-relational database management systems. Based on the Call Level Interface specification of the SQL Access Group, ODBC provides an open, vendor-neutral way of accessing data stored in a variety of proprietary personal computer, minicomputer and mainframe databases. ODBC alleviates the need for independent software vendors and corporate developers to learn multiple application programming interfaces. ODBC now provides a universal data access interface. With ODBC, application developers can allow an application to concurrently access, view and modify data from multiple, diverse databases."⁷ ODBC further facilitates the ability of the forensic accountant to convert the requisite data into an appropriate form.

⁷ <http://support.microsoft.com/kb/110093> visited on 2/20/2010



When identifying data fields to normalize, there are a variety of issues of which to be aware. Certain software tools such as Excel, Text Pad and ASAP Utilities can assist the forensic accountant with the normalizing process.

Does the Data Extracted Need to Be Normalized or Cleansed?

The data that the forensic accountant plans to use should be scrutinized for normalization of fields and type of data. The forensic accountant may find that normalizing and/or cleaning up of the data is necessary. Normalizing and/or cleaning up the data are the process of standardizing the information received in order to analyze the data in an efficient way. For example, if a data set contains transaction dates in the format of both “mm/dd/yy” and “dd/mm/yy,” these dates would have to be normalized to read in a consistent way for the forensic accountant to analyze and understand when a transaction took place. Additionally, if a dataset contains transaction amounts in multiple currencies, creating a column to translate all amounts into one denomination (i.e., U.S. dollar) will allow the forensic accountant to view and analyze the data in a logical way.

When identifying data fields to normalize, there are a variety of issues of which to be aware. Certain software tools such as Excel, Text Pad and ASAP Utilities can assist the forensic accountant with the normalizing process.

What Type of Inquiries Can Be Performed With Data Analysis?

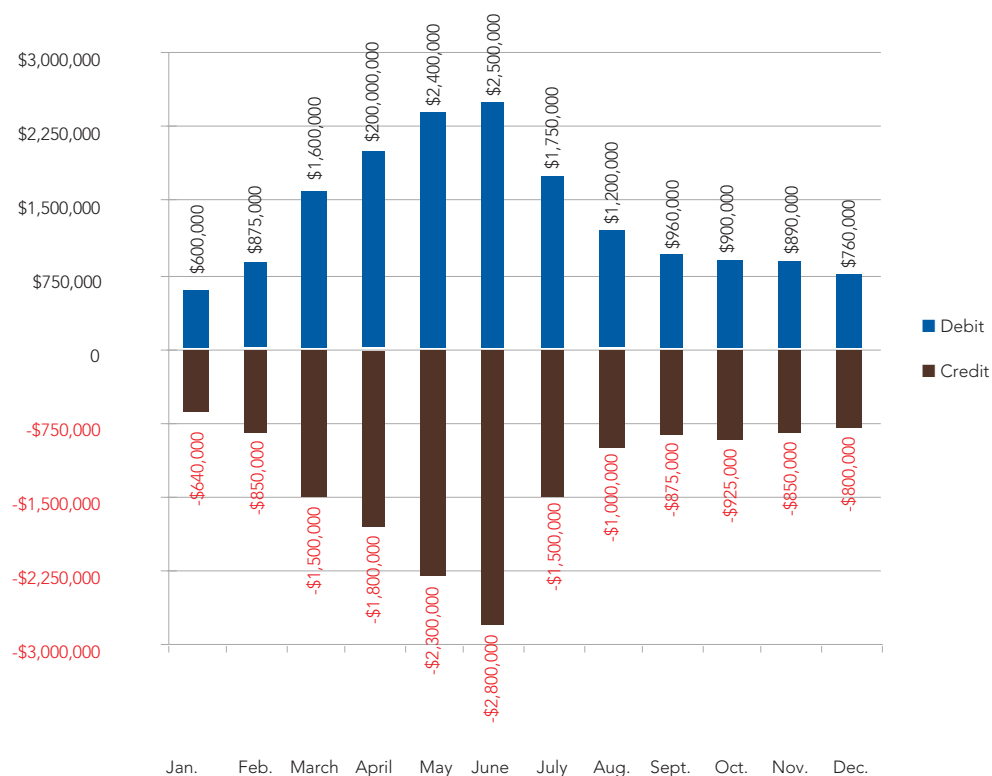
Once the relevant data has been obtained, evaluated for completeness, normalized and cleaned, the forensic accountant can then begin to analyze the information. Understanding the types of information contained in the population will help the forensic accountant with ideas for the types of analyses that can be performed. For example, if the population contains user identification information and the time and day that the entries were made, the forensic accountant can summarize or analyze the data by entries made by person, the time of day/week/holidays, and so forth. It is often helpful to look at the data in different ways such as a summary with similar types of information; graphically to identify trends and anomalies; or at a detailed level.

SAS No. 99 identifies some of the characteristics of fraudulent entries or adjustments when looking at non-standard manual journal entries, including entries made to unrelated, unusual, or seldom-used accounts; entries made by individuals who typically do not make journal entries; end of period or post-closing entries; entries having little or no description; entries made before or during the preparation of financial statements that do not have account numbers; round dollar amount entries or amounts with a consistent ending number (SAS 99, paragraph 61).⁸

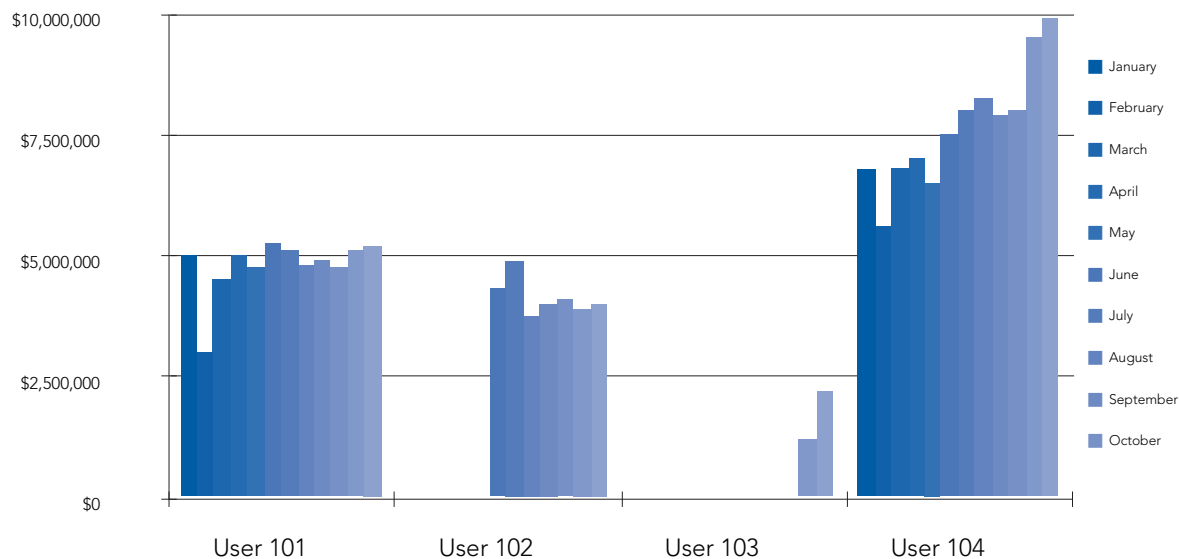
⁸ Source: Statement of Auditing Standards No. 99, paragraph 61 which can be found at aicpa.org/standards

Graphing data helps the forensic accountant and others viewing the data (such as other professionals and clients) understand trends of the business and to identify anomalies. Anomalies are not necessarily indicators of fraud, but simply oddities occurring in a business may be indicators of certain risk factors. Further detailed analysis of anomalies will help those viewing the data understand why the anomalies exist; the business logic of why the anomaly exists; or if there can be potential risks associated with the anomaly. Benford's law has been promoted as a useful tool for the detection of fraud. The tool uses statistical theory and digital analysis to identify anomalies in data sets. Oftentimes the results of such analysis are summarized in graphical form. Some examples of graphing that show trends and anomalies follow.

In the graphic illustration of trending certain accounts by month, the forensic accountant may want to view the details of the data for the months of April, May and June, as the forensic accountant may view these months as anomalous.



Account trending by month or period



Entries made by user identification

Viewing entries made by user identification can help the forensic accountant to validate their knowledge of the number of users with access to record entries, and the volume of entries being recorded. In the graphic illustration above, User 103 may be a new user, or it could be anomalous, in which case the details of entries made by User 103 can be reviewed for potentially inappropriate types of entries.

A very powerful aspect of analyzing data electronically is the ability for the forensic accountant to extract and identify all transactions containing certain risk traits. As risk areas are identified or transactions appear to have been recorded in error, the forensic accountant can further analyze if the “error” occurs multiple times or if the dollar amount of the “errors” is material.

Analyzing data electronically can enhance the way the forensic accountant performs risk analyses while doing proactive work, or while performing engagements in a reactive setting, as well as how auditors audit. Understanding the trends in the data, analyzing anomalies, eliminating false positives, and further investigating or analyzing risk areas helps the forensic accountant to further risk focus the approach to the engagement.

What Tools Are Available to the Forensic Accountant to Analyze Data?⁹

A number of tools are available to the forensic accountant that can assist with data analysis initiatives.

⁹ This section refers to data analysis only and no other software, e.g., case management that can be used to support forensic investigations, e.g., case management

TYPE	DESCRIPTION	EXAMPLES
Basic Productivity Software	The forensic accountant may use common software used for other business purposes. Typically, the forensic accountant will need to acquire intermediate and some advanced expertise of the product.	Excel, Access
Excel/Office Add-on Data Analysis Software	Intuitive programs that provide users with easy-to-use utilities that leverage Excel and other Microsoft products to perform data analysis. Excellent price performance, enabling users new to data analysis to experiment with potential benefits without incurring significant implementation or training expenses.	ActiveData, TopCaats
Data Analysis Software	Comprehensive data analysis programs that support various investigative activities, including conversion of multiple electronic formats into a format that can be used.	IDEA, ACL
Specialty Software	Special purpose software to facilitate advanced data analysis inquiry or special investigative purposes, e.g., data mining, security and access.	WizSoft, SAS, SPSS, Qualys



The forensic accountant who holds both the CFF and CITP credentials has the skill set that best positions them to evaluate the requirements and to identify appropriate resources as necessary.

Data Analysis Versus Data Mining

One of the challenges involved in implementing data analysis is that, in many situations, the forensic accountant needs to define the type of exception conditions they seek. After obtaining the data, the forensic accountant needs to specify the specific condition. For example, in looking at the data obtained, the forensic accountant would need to define the specific field, e.g., accounts payable, and the amount that may meet specific criteria that could identify an exception requiring follow up. However, this approach assumes that the forensic accountant has reason to suspect certain patterns of unusual activity and that by subjecting all transactions to review, fraudulent activities can be identified by thorough and effective inquiries that test the subjected data for these trends.

Data mining can be an answer to the challenges faced by the forensic accountant above. Using mathematical algorithms, data are analyzed to predict relationships between various fields in the record, as well as future trends and behaviors. For example, an accounts payable file may be analyzed and relationships between fields such as employee-initiated the transaction, date and transaction amount, address and amount, can be determined. Algorithms determine and assign a probability for that relationship. If 98% of transactions have a certain relationship that can be predicted and 2% do not and represent anomalies within the file, this 2% would be of interest to the forensic accountant.

Data mining is far from a perfect science. Because anomalies have been identified, the anomalies alone do not indicate that a potential transaction is fraudulent. Forensic accountants may be frustrated by the number of false negatives that arise while running data mining techniques. One interesting approach is to combine both data analysis and data mining. By subjecting the data to data mining first, trends can be identified that then can be analyzed by data analysis tools.

Conclusion

Forensic accountants are becoming increasingly familiar with forensic technology and methodologies used in both proactive and reactive forensic engagements. As the use of computer forensic analysis, e-discovery and forensic data analysis often is a necessary component of a forensic engagement, the forensic accountant should consider various issues and challenges as discussed in this white paper. This white paper discusses many of the more common challenges that may be encountered by the forensic accountant. Lastly, the forensic accountant who holds both the CFF and CITP credentials has the skill set that best positions them to evaluate the requirements and to identify appropriate resources as necessary.



Appendix A

The Computer Forensic Engagement – A Case Study

The following case provides a hypothetical situation in which a forensic accountant adds value. Further, it illustrates the approach that the forensic accountant might undertake in obtaining digital evidence, as outlined previously in this document.

Case Scenario: The computer user, Joe Suspect, is a program manager for ABC Industries. Joe has been with the company for 10 years and although he moved up the ranks rapidly in his first five years, he has only received inflationary bonuses for the past five years. Joe is a gregarious, bright, computer-savvy person. The company's CFO has noticed strange activity over the past six months. Specifically, shipping expenses have increased more than 60%, yet no attributable increase in revenue was found. Based on the delivery service pickup tickets, the CFO believes that Joe Suspect was responsible for the increase in accounts payables. Not wanting to alert Suspect, the CFO alerted the company's general counsel, who subsequently contacted a local computer forensics expert, Mary, a forensic accountant, and explained the scenario. The general counsel wants Suspect's company computer (a 250 gig Dell laptop) analyzed to determine whether it contains any evidence indicating Suspect misused the company's assets. The general counsel provides a letter authorizing access to Joe's company's computer.

The Tiered Approach

Mary, a forensic accountant, and the general counsel agree to use a tiered approach in this case. In this approach, Mary develops an incident response and forensic preview plan to collect system and user artifacts to determine if further analysis is warranted. After understanding the results of the first two steps, the general counsel may determine more analysis is needed and static forensics, a more deliberate process, might be undertaken. Mary would then gain physical access to Suspect's computer at his place of work. Usually this would be done after hours so as not to tip off suspect that an engagement is under way. Finally, the general counsel also could decide to have Mary conduct a live capture of data on Suspect's computer, which would potentially collect volatile data and system and user artifacts.¹⁰

First Steps: Mary conducted the incident response and forensic preview. Her initial, cursory keyword and string searches of Suspect's computer revealed information indicating Suspect's recent Internet activity at websites known for "off shore" banking and gambling, ABC Industries has no "off shore" banking relationships. Upon completing the search, Mary powered off suspect's computer to preserve all data that may be relevant to the engagement.

Mary informed the general counsel the next day and they agree to escalate the engagement by conducting a full static forensic analysis of Suspect's computer.

Static Forensic Examination

Now that the forensic accountant has been retained to perform a static forensic examination of Suspect's computer, additional documentation and protocols come into play. These include:

- Document and photograph the scene and any related and subsequent activities
- Consider disassembling and removing the hard drive (consider taking a picture of the forensic scene prior to disassembling)
- Make a forensic image using tools that have been validated for consistency and reliability, such as EnCase or FTK. The output of the tool must meet the validation of any or all of the accepted hashing algorithms, md5¹¹, SHA1 and SHA256. Once the hashed image(s) have been determined to match, this serves as the baseline qualifier that the forensic process, at no time, changed the data on the electronic media in any way

¹⁰ Artifacts are the remnants of whole or partially deleted files that can still remain on the drive. (Source: U.S. DOJ, Searching and Seizing Computers Manual, page 62) [justice.gov/criminal/cybercrime/ssmanual/02ssma.pdf](https://www.justice.gov/criminal/cybercrime/ssmanual/02ssma.pdf)

¹¹ Prosecutors who seek to introduce electronic records obtained from seized storage media using a validation or authentication process. For example, a prosecutor introducing a hard drive seized from a defendant's home and data from that hard drive may employ a two-step process. First, the prosecutor may introduce the hard drive based on chain of custody testimony or its unique characteristics (e.g., the hard drive serial number). Second, prosecutors may consider using the "hash value" or similar forensic identifier assigned to the data on the drive to authenticate a copy of that data as a forensically sound copy of the previously admitted hard drive. Source: U.S. DOJ Searching and Seizing Computers Manual. [cybercrime.gov/ssmanual/05ssma.html](https://www.cybercrime.gov/ssmanual/05ssma.html)

- Make a master working copy, which is an exact duplicate of the original evidence (the forensic image), as validated through the aforementioned hashing process. Creating a master working copy further reduces the risk of spoiling the data, if the original media become inaccessible for any reason, and it can serve as best evidence in court. An additional copy of this “master” should be created, which is the “working copy.” The working copy is the media that will be analyzed by the forensic accountant, thus eliminating the chance of inadvert alteration of the original evidence
- Deploy analysis tools on the working copy. There are a wide variety of computer analysis tools for today’s forensic accountant. These tools can be divided into the following categories: open source, internal proprietary and commercial. Further categorization can be made as to the completeness or scope of the tools, some tools perform isolated functions and others group functionality to perform a complete forensic examination. Regardless of the tools used, the forensic accountant strives to collect and collate information pertinent to the system, the user(s), and the allegation(s). Generally speaking, this information is obtained within the file system as intact files, cached files, previously deleted files and/or files that has been deleted and partially overwritten

In our example, these files are discovered through conducting keyword searches, which are words directly related to the information being sought to fulfill the objectives of the engagement. Keyword searches are crucial to most computer forensic examinations and need to be carefully planned and implemented for best results. In addition, email analysis can provide insight and help determine activities contemporaneous to the suspicious incident, such as what is being said and sent to whom, where and when. Lastly, for the purposes of this example, the Internet history is an important consideration. Internet history can demonstrate the user’s online searches, what websites were being visited and how often.

Once the keyword search was fully employed, Mary the forensic accountant identified the following relevant information on Suspect’s computer:

- An email to the State Corporation Commission with an attachment registering XYZ Corporation, a corporation with two shareholders, Joe Suspect’s spouse and daughter
- Various emails from Joe to various companies with attachments that are invoices for computer equipment and consulting from XYZ Corp



Keyword searches are crucial to most computer forensic examinations and need to be carefully planned and implemented for best results.

- XYZ Corporation State registration from hard drive
- Various invoices to the company that were created on Suspect's hard drive
- Various spreadsheets indicating revenue detail for XYZ Corporation that were created on Suspect's hard drive
- Internet favorites identifying XYZ Corporation's website

Following the keyword search, the next thing is analysis followed by the documentation of observations and recommendations.

Following the keyword search, the next thing is analysis followed by the documentation of observations and recommendations.

**Analysis:**

Once the search terms have been executed, the files that are “hits” to those terms are examined in more detail. In our hypothetical situation, Mary the forensic accountant found that the email identified above to the state corporation commission contained metadata indicating that Suspect created it on his computer and sent it through company’s email system.

The invoices attached to the email identified in the previous section’s second bullet match the invoices that forensic accountant determined were created on Suspect’s computer. These emails were also sent on the company’s email system. Forensic accountant also determined from log files and metadata, that the spreadsheets identified in the previous section’s fifth bullet were prepared on Suspect’s company computer. These documents indicate that XYZ Corporation, an entity set up by and involving Suspect’s family, was doing business with ABC Industries.



Once the conclusions have been reached, the forensic accountant should report her results consistent with the client's expectations.

In this instance, the forensic accountant could conclude that the artifacts (emails, invoices, documents) indicate fraudulent invoices were created on and sent from Suspect's computer. This critical information will help the general counsel determine whether the Suspect was in fact involved in a fraudulent scheme of his employer. Should the general counsel conduct further investigation, and discover additional questionable transactions or documents, Mary could use such information and further examine the working copy of Suspect's computer.

Once the conclusions have been reached, the forensic accountant should report her results consistent with the client's expectations. In this regard, the forensic accountant is no different from any expert and their report also is subject to ethical and professional standards of care.

In this case, live data capture was not used. At this point, the general counsel of ABC Industries has received Mary's report and, absent future litigation of this matter, forensic accountant has completed her computer forensic engagement.



T: 888.777.7077 | E: info@aicpa.org | W: aicpa.org