Journal of Forensic & Investigative Accounting
Vol. 1, Issue 2

Computer-based Proactive Fraud Auditing Tools

Gary J. Cook
Lynn H. Clements [*]

Deterrence and detection of fraud has been a concern for a long time, but the collapse of Enron created a new era of concern over the detection of fraud. Fraudsters continue to stay one step ahead of fraud auditors, and the use of computers to accomplish fraud is growing. In response, fraud auditors have been slow in acknowledging the importance of computerized tools in detecting fraud and to use them in fraud auditing.

There are numerous computerized fraud detection tools, some of which were developed specifically for fraud auditing, such as Forensic and Case Management, and many multi-purpose tools that can be utilized in uncovering fraud. We have become concerned about the lack of use of the best tools available to fraud auditors, whether they are external auditors, internal auditors, accounting managers, or forensic specialists.

There are inconsistencies in the application of the terms, "auditing," "fraud auditing," and "forensic accounting." This article begins with an explanation of the three concepts, followed by a review of the similarities and differences between proactive and reactive fraud auditing. We then present our analysis of the three phases of fraud auditing and a model representing those phases, based upon the Albrecht *et al.* (2006, 162) deductive approach to fraud auditing.

In this article, we present a number of computerized tools available to fraud auditors, an analysis of the tools currently used, and the tools recommended for use in each of the three phases of fraud auditing. In order to accomplish our task, we conducted a search of available

[*] The authors are, respectively, Associate Professor of IT Management and Professor of Accounting at Florida Southern College.

tools and have reported our findings in this paper. We also surveyed fraud auditors as to the tools they are familiar with and not familiar with, those they own, and those they currently use. We conclude with our recommendations for the best tools to use in each phase of fraud auditing.

LITERATURE REVIEW

Financial Auditing, Fraud Auditing, and Forensic Accounting

The terms financial auditing, fraud auditing, and forensic accounting are sometimes used more or less interchangeably and, although there are similarities, there are differences as well. Financial auditing and fraud auditing are similar in that frauds are often financial crimes, necessitating a certain amount of financial auditing. There are differences between the two, however. Financial auditing is recurring, general, and non-adversarial, with the purpose of rendering an opinion on financial statements or other information. Fraud auditing is nonrecurring, specific, and adversarial, with the purpose of finding enough evidence to determine whether fraud has occurred and if so, who committed the fraud (Wells 2005). Forensic accounting can be broadly divided into two domains: litigation services and investigative accounting, which includes but is not limited to fraud auditing (Crumbley *et al.* 2007).

Proactive vs. Reactive Fraud Auditing

Traditionally, a fraud audit began when a whistleblower reported an economic crime, or when the auditors had the good fortune of selecting a fraudulent transaction during statistical sampling. This method of fraud auditing, identified as reactive fraud auditing, begins with the awareness that a potential fraud has been committed. However, if a fraud is permitted to continue for years, the amount of the loss increases, the chance of recovery is significantly reduced, and oftentimes, the money has been spent. A better fraud detection strategy is to stop

the fraud as early as possible, limit the amount of the loss, and insure the maximum amount of recovery (Davia *et al.* 2000, 253). This requires proactive techniques.

"To proactively search for fraud is to search for symptoms of fraud" (Davia *et al.* 2000, 59). Advances in technology have caused a paradigm shift from reactive to proactive fraud auditing. Proactive fraud auditing begins with the identification of frauds that may be occurring.

Once a fraud auditor has identified the fraud type he or she plans to search for, there are several methods of proactive searching available. Albrecht *et al.* (2006, 158-159) identified two inductive methods and one deductive method used in conducting proactive fraud audits.

Inductive detection methods (e.g., commercial data-mining software and digital analysis) search for anomalies that suggest fraud exists, without identifying a particular type of fraud suspected. Inductive methods have a low cost, but produce so much data, or "red flags," that it is often too costly to investigate them all. Therefore, fraud auditors often prefer a deductive approach.

The deductive method proposed by Albrecht *et al.* (2006, 162) has a higher cost than the inductive methods, but generally produces good results. The deductive approach follows a five-step process: (1) Obtain a good understanding of the business, (2) understand the types of frauds most likely, (3) determine the symptoms of those most likely frauds, (4) use databases and other computerized technology tools to search for those symptoms, and (5) follow up on the symptoms to determine their cause(s).

Proactive fraud search begins with a good understanding of the business and its systems. "Fraud rarely, if indeed ever, is discovered with all of its details intact, neatly wrapped in a package ready for prosecution. Rather, it is usually found in bits and pieces of evidence, which

constitute a case of fraud when assembled" (Davia *et al.* 2000, 59). So, where does a fraud auditor begin?

"Proactive fraud auditors do not simply enter an employer's or client's office location and begin looking for fraud. To begin searching for fraud proactively, auditors must select a specific type of fraud to hunt for. Some proactive fraud auditors are specialists and search for only one type of fraud. By concentrating in one type of fraud, they become expert at catching their quarry" (Davia *et al.* 2000, 54.) The search may end with no findings of fraud indicia. Or, the search may provide sufficient evidence that the fraud auditor finds predication of fraud.

"*Predication* is the totality of circumstances that would lead a reasonable, professionally trained, and prudent individual to believe a fraud has occurred, is occurring, and/or will occur"(Wells 2005, 5). "In other words, predication is the basis for undertaking a fraud investigation. Without predication, the target might be able to sue for real or imaginary damages" (Crumbley *et al.* 2007, 5-6, 7).

The Three Phases of Fraud Auditing

We posit that there are three phases of fraud auditing. Our analysis of fraud auditing begins with the Albrecht *et al.* (2006, 162) five-step deductive method, as previously described in this article. We have found that fraud auditing can be divided into three phases: fraud search, fraud investigation, and fraud detection. Fraud search can be further subdivided into three steps (the first three steps in the Albrecht method): identify specific fraud risks, identify symptoms of those risks, and search for those symptoms. In summary, we propose to arrange the five Albrecht steps into three phases:

Phase One: Fraud Search

1. Identify specific fraud risks
2. Identify symptoms of those risks
3. Search for those symptoms

Phase Two: Fraud Investigation

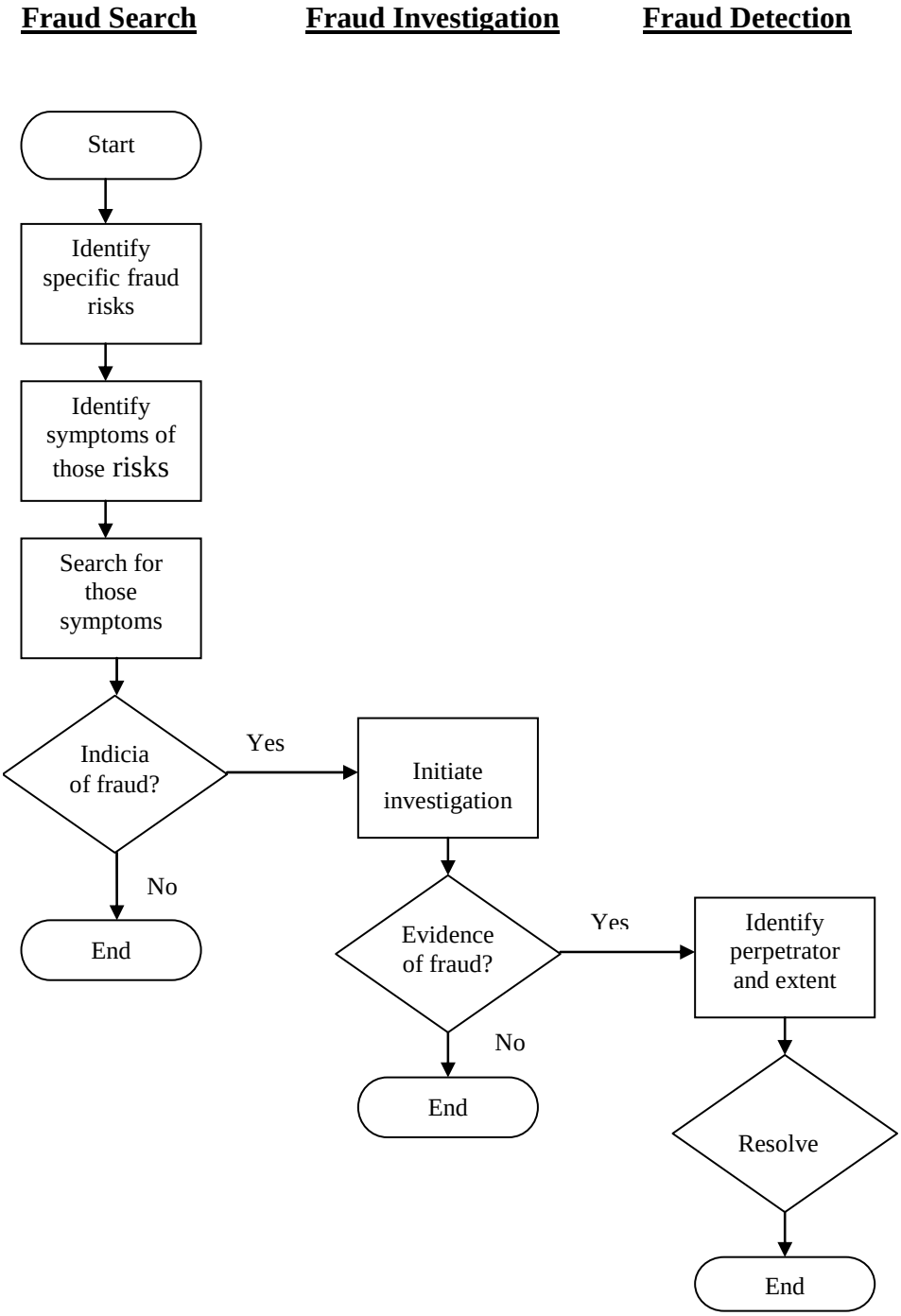
4. If symptoms are found (predication), initiate investigation of the evidence

Phase Three: Fraud Detection

5. If evidence of fraud is found, identify the perpetrator(s) and the extent of the fraud

Based upon our analysis of the three phases, we propose the following model:

Fraud Audit Model



Proactive Fraud Auditing Begins in Phase One: Fraud Search

Fraud audits may begin in any of the three phases. However, to begin a fraud audit upon predication of fraud (in the second phase) or upon the discovery of fraud (in the third phase) is reactive. If and when predication is found, the proactive auditing becomes reactive. A proactive fraud audit, then, begins in the first phase.

A proactive fraud audit may begin in one of two ways. First, a financial statement auditor proactively searches for fraud in order to comply with SAS 99, as required by the American Institute of CPAs (AICPA). Second, a company may choose to engage a fraud auditor, without any expectation of fraud, in the hopes of preventing fraud by providing employee awareness about the company's lack of tolerance for fraud and/or because of a general fear that fraud does exist. Whatever the reason for the proactive audit, proactive fraud auditing is on the rise because of its obvious benefits at lowered costs. Whether the proactive fraud auditor uses surprise audits, or the audit is announced and made widely known to the employees of an organization, a proactive fraud audit should be organized and follow a plan of action with well-defined procedures.

Many proactive detection techniques require the use of computer technology, and most are enabled by commercial software. The two major problems of computerized tools, however, are (1) where to find them, and (2) which one(s) to use.

Our research questions are as follows:

R_1: What computerized tools are available to proactively search for fraud?

R_2: What computerized tools are fraud auditors using in searching for fraud?

R_3: Which tool(s) should fraud auditors use in searching for fraud?

RESEARCH QUESTION #1: WHAT COMPUTERIZED TOOLS ARE AVAILABLE TO PROACTIVELY SEARCH FOR FRAUD?

There are many computerized tools available from a variety of vendors. A lengthy search, provided in Table 1, revealed an extensive, though not comprehensive, listing of available tools. We have arranged the available tools into five classifications: (1) General Purpose Tools, (2) Audit/Fraud Extensions, (3) Data Mining/Data Analysis Tools, (4) Forensic Tools, and (5) Case Management and Reporting Tools (See Table 1).

General Purpose Tools

General purpose tools, such as MS Access and MS Excel, are tools that are not specifically intended for fraud auditing but can still be useful. In fact surveys repeatedly show that MS Excel is widely used by internal auditors and fraud auditors (see, e.g. www.acl.com/pdfs/IIA_Survey_Summary.pdf and our survey, discussed below). Other Microsoft Office products, such as Access, Visio, and Word can also be used in various ways in fraud audits. Open Office is a free open source office suite that includes Calc, Base, Draw, and Writer; products that are very similar to Microsoft Office. Crystal Reports is a report creation tool that supports the delivery of Web-based or application-embedded professional reports. It can be used to extend the capabilities of Microsoft Office or Open Office and is included with tools such as ACL.

Spreadsheet Professional provides development tools for building, testing, documenting, and using spreadsheets. These kinds of tools can be very useful given the widespread occurrence of significant errors in spreadsheets today (see, e.g. www.spreadsheetinnovations.com/Sarbanes-Oxley.htm).

TeamMate is audit management software for internal audit departments. Included is an electronic work paper system and tools for tracking audit issues, risk assessment, scheduling, and time and expense tracking.

Audit/Fraud Extensions

Tools such as ActiveData for Excel (ADE) and ActiveData for Office (ADO) are add-ons that extend the capabilities of MS Excel and MS Access and are intended for fraud auditing as well as financial auditing and other types of analyses. ADE uses MS Excel and extends the regular spreadsheet manipulations that MS Excel provides. An audit log can be created using MS Excel-based comments. ADO is based on tables and uses the MS Jet database engine, and supports the use of SQL database queries for analysis. A full step-by-step audit log can be created automatically.

The types of analyses provided by these tools include: appending/merging files, calculating field functions, Benford's Law tests, identification of duplicates, exporting files, extracting/filtering, identification of gaps, indexing/sorting, joining/merging/relating data, sampling of data, and summarizing of data.

Data Mining/Data Analysis Tools

Traditionally, data mining has been described as using statistical analysis and machine learning techniques to search for previously unknown and potentially useful patterns, trends, anomalies, and relationships in collections of structured data. More recently, vendors and academicians have used the term to describe relatively unstructured searches using products usually thought of as data analysis tools. According to Albrecht, for example, data mining

involves using tools such as IDEA or ACL to search for anomalies or unexpected patterns or relationships in data. With these kinds of searches suspicious patterns do not provide evidence of fraud, merely symptoms of possible fraud. A problem with this approach, whether data analysis tools or data mining tools are used, is that a large number of false positives may be identified requiring further manipulation of the data. In many cases there is no way to eliminate these false positives (Albrecht 2006, 110-111).

In proactive data analysis, a structured approach is followed. Specific fraud symptoms are identified and a search is made for those symptoms. For example, a search for phantom vendors might involve matching a vendor master file with an employee master file and comparing items like telephone numbers, addresses, tax ID numbers, etc., especially for accounts payable personnel (Wells 2005, 120).

In addition to the capabilities listed above for the audit/fraud extensions, tools in this category are capable of many other types of analyses. For example, Wells (2005) identifies more than 170 types of analyses, such as searching for:

- Phantom employees by comparing payroll records with HR employee files
- Payments split into smaller amounts within 90 percent of approval levels
- Invoices paid on irregular days or dates
- Gaps in check sequences
- Duplicate invoices
- Paid invoices with amounts exceeding authorization levels

Forensic Tools

Forensic tools are intended for use in investigations such that the findings will have application in a court of law, which includes the ability to demonstrate that electronic evidence has not been accidentally altered or intentionally tampered with. Typical capabilities of forensic tools include the following:

- Examining Windows, Unix, and Linux file systems
- Previewing all files, including deleted or hidden files, without altering the data on the disk, including file metadata
- Creating bitstream copies of disks and packaging the bitstream for transfer to other media, such as CDs or DVDs
- Aiding in the recovery of deleted, lost, and formatted data from hard drives, diskettes, ZIP discs, USB hard drives, and other removable devices
- Using a hash comparison to find known illegal files or identify known good files

Case Management and Reporting Tools

These tools can be useful in all phases of fraud auditing in various ways. They can be particularly helpful if a fraud audit proceeds from the fraud search phase to the fraud investigation phase, and into the fraud detection phase. CaseMap, for example "makes it easy to organize, evaluate and explore the facts, the cast of characters, and the issues in a case, and is designed for use on all types of cases and by all types of litigators and investigators" (www.casesoft.com/casemap/casemap.asp).

RESEARCH QUESTION #2: WHAT COMPUTERIZED TOOLS ARE FRAUD AUDITORS USING IN SEARCHING FOR FRAUD?

An online survey (see Appendix A) was developed using SurveyMonkey (www.surveymonkey.com) and administered by an email solicitation to members of a local chapter of the Association of Certified Fraud Examiners, members of the Florida Audit Forum, and members of the Association of Local Government Auditors. There were 152 respondents. According to our survey the most commonly used tools are MS Word and MS Excel, with 99.3% and 98.7% respectively of respondents reporting that they use them frequently or occasionally. Next most common is MS Access at 55%, followed by MSVisio at 40.3%, ACL at 31.3%, and Crystal Reports at 17%. The remaining tools were all below 10%, including ActiveData for MS Excel (9.8%), TeamMate (9.7%), IDEA (8.7%), Open Office (7.5%), Undelete for Windows (4.7%), SPSS (4.1%), ActiveData for Office (3.5%), Analyst's Notebook and Monarch (2.7%), and Encase (2.6%). With the exception of Access, ACL, MS Excel, and Word, the most common response was "not familiar with." (See Table 2).

RESEARCH QUESTION #3: WHICH TOOL(S) SHOULD FRAUD AUDITORS USE IN SEARCHING FOR FRAUD?

Answering the first two research questions naturally led to a third question, "Which tool is the best?" In attempting to generalize an answer, we realized that the answer to the question depends upon the purpose and goals of the audit. In this section, we recommend computerized tools for each of the three phases and conclude with recommendations that differ based upon the type of fraud auditor.

Recommendations for Specific Computerized Tools in Phases 1a and 1b

In the first two steps of phase one, "Identify Specific Fraud Risks" and "Identify Symptoms of those Risks," MS Word, MS Visio, and case management tools such as Analyst's

Notebook or CaseMap, can be used to document and diagram fraud risks and symptoms. In addition, case management tools can be used throughout a fraud audit to manage and document the case.

Recommendations for Specific Computerized Tools in Phase 1c

In the third step of phase one, "**Search for Those Symptoms,"** the tool(s) used depends upon whether the suspected fraud involves misstatement of financial statements, or if it involves misappropriation of assets or corruption.

If the suspected fraud involves misstatement of financial statements, an analysis of those financial statements typically involves vertical percentage analysis, horizontal percentage analysis, and/or ratio analysis. Spreadsheet software is appropriate and useful for these kinds of analyses. If the analysis will include a search of transaction and related data, then other considerations come into play, as discussed below.

If the suspected fraud involves misappropriation of assets or corruption, then analyses of transactions and related detail data about, for example, employees, vendors, customers, and assets are needed. This requires extracting data or searching for data in databases, spreadsheets, e-mails, and other types of documents. For these analyses, *entire populations* of data should be examined, *not just samples*. Fraudulent activities may involve a relatively small number of transactions which could be easily overlooked with sampling.

If the fraud search is to be conducted by an auditor who will turn the audit over to a fraud auditor in the event predication is found, then general purpose tools such as MS Access and MS Excel can be appropriate and useful. Purpose-built tools such as ACL and IDEA, however, have the potential to significantly increase productivity, and about 40 percent of the respondents to our

survey reported using these tools either frequently or occasionally. However, a considerable amount of time for training and experimentation is required to fully realize these productivity gains.

If the same person or team that conducts the search phase will also conduct the investigation and detection phases, then it makes more sense to use the same tools in the search phase as will be used in the investigation and detection phases.

Recommendations for Specific Computerized Tools in Phase Two: Fraud Investigation

If the search phase turns up sufficient evidence to suspect fraud (predication) then a fraud investigation should be initiated. There are particular issues to consider in phase two, which involves investigating the evidence, including how to maintain the chain of custody over evidence, and the legal ramifications of evidence come into play if criminal or civil charges will be brought (Wells 2005, 6). In addition, the fraud auditor must be able to demonstrate that the evidence has not been altered in order to be admissible in a court of law.

Probably the most widely used tool for this stage is Excel. However, in a whitepaper entitled “Spreadsheets: A High- Risk Tool for Data Analysis” three main shortcomings are described:

- Lack of data integrity – values may be altered deliberately or accidentally
- Potential for errors – errors in input, logic, data interfaces, and use
- Not in line with standard IT regimes for critical applications – documentation, testing, and version control

Similarly, Metz (2007) identifies five common spreadsheet risks: (1) Unskilled users, (2) lack of guidelines for spreadsheet preparation, (3) data entry and recycling, (4) spreadsheet errors, and (5) loss of data.

Given these issues, it is questionable whether Excel is an appropriate tool for fraud investigation. On the other hand, with data analysis tools such as ACL or IDEA, the original data is read only and cannot be altered by the software. In addition, ACL and IDEA automatically generate a read-only log of each step of the analysis.

Recommendations for Specific Computerized Tools in Phase Three: Fraud Detection

This phase requires a more in depth analysis than phase 2 to identify the extent of the fraud, but would involve the same analysis tools. In addition, identification of the perpetrators often involves interviewing various people. Case management tools can be used to document the results of these interviews and diagram the links or connections among the various parties involved.

Recommendations that Differ Based on the Type of Fraud Auditor

If the fraud search is to be conducted by an auditor who will turn the audit over to a fraud auditor in the event predication is found, then general purpose tools such as MS Access and MS Excel can be appropriate and useful. Purpose-built tools such as ACL and IDEA, however, have the potential to significantly increase productivity, and 40 percent of the respondents to our survey reported using these tools either frequently or occasionally.

If the same person or team that conducts the search phase will also conduct the investigation and detection phases, then it makes more sense to use the same tools in the search phase as will be used in the investigation and detection phases.

Our recommendations are summarized in Table 3 (See Table 3).

CONCLUSIONS

We found fraud auditors are not using the best tools available to them for detecting fraud. Our review of computerized tools for use in proactive fraud auditing is not an exhaustive list, but it is an extensive listing of the strongest tools in the industry. Sadly, many fraud experts are unfamiliar with some of the best tools.

Many fraud auditors continue to limit themselves to reactive fraud auditing. There will always be a need for reactive audits (i.e., when the whistle is blown or fraud is suspected, and the call comes for an investigation). However, with the strength of available computerized tools, proactive fraud auditing has become more expedient and very cost-beneficial.

One area of future research is to determine why fraud auditors are not using the best tools available to them, and/or why they are not searching for better tools to use. Another area of future research is to report on new tools as they become available. A third future research area is the reason(s) for not performing proactive audits. A final area of future research is to extend the survey to a sample of Certified in Financial Forensics (CFF). Since one of the CFF objectives is to "enhance the quality of forensic services CFFs provide," we propose the CFF should have a good knowledge of computerized detection tools and be using them to their greatest extent (AICPA).

The biggest problem with proactive fraud auditing is the possibility a fraud exists that is of a different type than the one the auditor selected for his or her search. To mitigate that problem, “more experienced auditors carefully schedule fraud types to be audited a year or more in advance, to ensure that ultimately they address all fraud types they wish to visit" (Davia 2000, 56). We would add that using the proper tools for fraud detection will help in fraud discovery. It is our hope that auditors, internal auditors, accounting managers, and forensic specialists alike will develop the skills necessary to continue the fight against fraud by using the best tools available.

References

AICPA. Certified in Financial Forensics. Available at: http://fvs.aicpa.org/Memberships/Overview+of+Certified+in+Financial+Forensics+Credential.htm

Albrecht, W.S., C. Albrecht, and C. Albrecht. 2006. *Fraud Examination & Prevention*. Mason, OH: Thomson Southwestern.

Crumbley, D.L., L.E. Heitger, and G.S. Smith. 2007. *Forensic and Investigative Accounting, 3rd ed.* Chicago: CCH.

Davis, H.R. 2000. *Fraud 101: Techniques and Strategies for Detection*. NY: John Wiley & Sons, Inc.

Davia, H.R., P. C. Coggins, J.C. Wideman, and J. T. Kastantin. 2000. *Accountant's Guide to Fraud Detection and Control, 2nd edition*. NY: John Wiley & Sons, Inc.

Metz, L. R. (2007) Five Spreadsheet Risks and How to Control Them, *IT Audit Vol. 10*. Available at: www.theiia.org/ITAudit/index.cfm?iid=563&catid=21&aid=2833.

Spreadsheets: A High- Risk Tool for Data Analysis, ACL White Paper, 2006.

Wells, J.T. 2003. Sherlock Holmes, CPA, Part 1. *Journal of Accountancy Online*, August 2003. Available at: http://www.aicpa.org/pubs/jofa/aug2003/wells.htm

Wells, J.T. 2005. Principles of Fraud Examination. Hoboken, NJ: John Wiley & Sons, Inc.

www.acl.com/pdfs/IIA_Survey_Summary.pdf

www.casesoft.com/casemap/casemap.asp

Appendix A: Online Questionnaire in SurveyShare.com for a period of time at

http://www.surveymonkey.com/s.aspx?sm=YovWXJaEbTNhJfOq5R_2bsmg_3d_3d

Computer-Aided Fraud Examination

Please indicate your relative familiarity with the following computer-based tools

1. General Purpose Tools

	Not familiar with	Own but do not use	Familiar with but do not own	Use occasionally	Use frequently
Crystal Reports	O	O	O	O	O
MS Access	O	O	O	O	O
MS Excel	O	O	O	O	O
MS Word	O	O	O	O	O
MS Visio	O	O	O	O	O
Open Office	O	O	O	O	O
Spreadsheet Professional	O	O	O	O	O
TeamMate	O	O	O	O	O

2. Audit/Fraud Examination Extensions

	Not Familiar with	Own but do not use	Familiar with but do not own	Use occasionally	Use frequently
ActiveData for Excel	O	O	O	O	O
ActiveData for Office	O	O	O	O	O

3. Data Mining/Data Analysis Tools

	Not familiar with	Own but do not use	Familiar with but do not own	Use occasionally	Use frequently
ACL	O	O	O	O	O
IDEA	O	O	O	O	O
Monarch	O	O	O	O	O
NetMap Analytics	O	O	O	O	O
Picalo	O	O	O	O	O
SAS	O	O	O	O	O
SPSS	O	O	O	O	O
SPSS Clementine	O	O	O	O	O

4. Forensic Tools

	Not familiar with	Own but do not use	Familiar with but do not own	Use occasionally	Use frequently
Data-Sniffer	O	O	O	O	O
EnCase	O	O	O	O	O
Forensic Toolkit	O	O	O	O	O
ProDiscover	O	O	O	O	O
Snap!Recovery	O	O	O	O	O
Undelete for Windows	O	O	O	O	O

5. Case Management and Reporting Tools

	Not familiar with	Own but do not use	Familiar with but do not own	Use occasionally	Use frequently
Analyst's Notebook	O	O	O	O	O
CaseMap	O	O	O	O	O
NetMap	O	O	O	O	O
MAGNUM	O	O	O	O	O

Table 1: COMPUTERIZED TOOLS AVAILABLE TO PROACTIVELY SEARCH FOR FRAUD

General Purpose Tools:

- Crystal Reports
- MS Access
- MS Excel
- MS Word
- MS Visio
- Open Office
- Spreadsheet Professional
- TeamMate

Forensic Tools:

- EnCase
- Forensic Toolkit
- Undelete for Windows
- Data-Sniffer
- ProDiscover
- Snap!Recovery

Audit/Fraud Examination Extensions:

- ActiveData for Excel
- ActiveData for Office

Case Management and Reporting Tools:

- Analyst's Notebook
- CaseMap
- NetMap
- MAGNUM

Data Mining/Data Analysis Tools:

- Audit Command Language (ACL)
- Interactive Data Extraction and Analysis (IDEA)
- Monarch
- NetMap Analytics
- Picalo
- SAS

Table 2
Computer-Aided Fraud Examination
Survey Results

	Not familiar with	Own but do not use	Familiar with but do not own	Use occasionally	Use frequently
General Purpose Tools					
Crystal Reports	**50.3%**	8.8%	23.8%	14.3%	2.7%
MS Access	6.7%	26.8%	11.4%	**36.2%**	18.8%
MS Excel	0.0%	0.0%	1.3%	6.0%	**92.7%**
MS Word	0.7%	0.0%	0.0%	2.0%	**97.3%**
MS Visio	**34.9%**	10.7%	14.1%	23.5%	16.8%
Open Office	**83.8%**	0.7%	8.1%	6.8%	0.7%
Spreadsheet Professional	**92.6%**	0.7%	6.0%	0.0%	0.7%
TeamMate	**65.3%**	0.7%	24.3%	0.7%	9.0%
Audit/Fraud Examination Extensions					
ActiveData for Excel	**73.4%**	3.5%	13.3%	6.3%	3.5%
ActiveData for Office	**85.5%**	1.4%	9.7%	2.8%	0.7%
Data Analysis/ Data Mining Tools					
ACL	29.3%	2.0%	**37.3%**	21.3%	10.0%
IDEA	**45.6%**	2.7%	43.0%	4.0%	4.7%
Monarch	**70.0%**	3.3%	24.0%	2.0%	0.7%
NetMap Analytics	**92.0%**	0.0%	8.0%	0.0%	0.0%
Picalo	**93.3%**	0.0%	6.7%	0.0%	0.0%
SAS	**69.6%**	0.7%	27.7%	1.4%	0.7%
SPSS	**73.0%**	1.4%	21.6%	2.7%	1.4%
SPSS Clementine	**91.8%**	0.7%	7.5%	0.0%	0.0%

	Not familiar with	Own but do not use	Familiar with but do not own	Use occasionally	Use frequently
Forensic Tools					
Data-Sniffer	**83.3%**	0.0%	16.7%	0.0%	0.0%
EnCase	**74.5%**	0.0%	22.8%	1.3%	1.3%
Forensic Toolkit	**83.2%**	0.7%	14.1%	1.3%	0.7%
ProDiscover	**96.6%**	0.0%	3.4%	0.0%	0.0%
Snap!Recovery	**95.8%**	0.0%	4.2%	0.0%	0.0%
Undelete for Windows	**83.8%**	1.4%	10.1%	4.7%	0.0%
Case Management/ Reporting Tools					
Analyst's Notebook	**88.0%**	0.0%	9.3%	0.7%	2.0%
CaseMap	**83.3%**	0.7%	14.7%	1.3%	0.0%
NetMap	**89.2%**	0.0%	10.8%	0.0%	0.0%
MAGNUM	**91.8%**	0.0%	8.2%	0.0%	0.0%

Table 3
Computer-Aided Fraud Examination
Recommendations for Specific Tools By Fraud Examination Phase

Phase	1a	1b	1c	2	3
Tool					
Access, Base			•	•	
Excel, Calc			•		
Visio, Draw	•	•			
Word, Writer	•	•		•	•
Spreadsheet Pro			•	•	
TeamMate	•	•	•	•	•
Audit/FE Extensions			•	•	•
Data Mining/Data Analysis			•	•	•
Forensic			•	•	
Case Management	•	•	•	•	•

The opinions of the authors are not necessarily those of Louisiana State University, the E.J. Ourso College of business, the LSU Accounting Department, or the Editor-In-Chief.