Forensic Accounting

By Mary-Jo Kranacher, CPA/CFF, CFE

Chapter 10
Using Information Technology for Fraud Examination and
Financial Forensics

LEARNING OBJECTIVES

10-1 Discuss the two major approaches for testing IT system controls.
10-2 Describe CAATTs and explain what they are used for.
10-3 Explain the purpose of computer forensics.
10-4 Identify some computer functions that can make recovering deleted files more difficult.
10-5 Describe how e-discovery rules impact the storage of e-mail and other electronic files.
10-6 Identify functions used by data extraction and analysis software to highlight red flags of fraud.
10-7 Recognize the two categories of data mining and knowledge discovery software.
10-8 Explain the role that graphics play in an investigation.
10-9 Describe the purpose of timelines in an investigation.
10-10 Discuss how case management software may be used in an investigation.

True/False

10-T/F #1. An information technology (IT) audit consists of (1) planning, (2) tests of controls, and (3) substantive tests.
Answer: True

10-T/F #2. The source documents that support the electronic data systems do not need to be pre-numbered and used in sequence.
Answer: False

10-T/F #3. There are two major ways to test IT systems - the “black-box” approach, and the “white-box” approach, which utilizes a relatively small dataset to test the system.
Answer: True

10-T/F #4. Generally, a warrant or subpoena is not required to obtain digital evidence.
Answer: False

10-T/F #5. The simple act of turning on a confiscated computer, digital camera, cell phone, PDA, etc. may make all the evidence on that digital device inadmissible in a courtroom.
Answer: True
10-T/F #6. Recovering deleted files is not considered difficult, provided that the file has not been overwritten or corrupted and that the drive has not been repartitioned or reformatted.
Answer: True

10-T/F #7. An activity that can enhance the ability to recover deleted files is the “Defrag” command.
Answer: False

10-T/F #8. Restoring data and files is a more sophisticated approach to recovering deleted files.
Answer: True

10-T/F #9. Once data sectors on computer files have been overwritten, generally a computer forensic specialist can still recover the files.
Answer: False

10-T/F #10. Data mining and knowledge discovery software is generally classified into two general categories: public domain and commercial applications.
Answer: True

10-T/F #11. IDEA can read, display, analyze, manipulate, sample, and extract data from files obtained from many sources in only one format.
Answer: False

10-T/F #12. ACL and IDEA are examples of commercially available data mining software.
Answer: True

10-T/F #13. Benford’s Law can be used as an indicator of potential fraud.
Answer: True

10-T/F #14. An association matrix is not useful for identifying major players who are central to an investigation and to identify linkages between those players.
Answer: False

10-T/F #15. Preparing link charts is a way to represent the associations, linkages, and other important relationship graphically.
Answer: True

10-T/F #16. Case management software can be used in a number of situations to manage cases and case data.
Answer: True
10-T/F #17. Validation controls detest input errors by flagging those transactions that fall within accepted ranges.
Answer: False

10-T/F #18. Record validation can include reasonableness checks, sequences checks, and other checks.
Answer: True

10-T/F #19. Output controls address how to monitor waste and how to identify who is responsible for data accuracy, report distribution, and end-user controls.
Answer: True

10-T/F #20. The acronym MICE signifies fraud motivations such as money, intellectualism, coercion, and ego.
Answer: False

**Multiple Choice**

10-M/C #1. An information technology (IT) audit consists of all EXCEPT
A. planning,
B. tests of controls,
C. substantive tests,
D. qualitative tests.
Answer: D

10-M/C #2. The general framework for viewing IT risks and controls include all the following EXCEPT
A. IT Operations
B. Systems Maintenance
C. Human Resource Management
D. Electric Commerce
Answer: B

10-M/C #3. Which of the following is not considered CAATTs (Computer-Aided Audit Tools and Techniques) software:
A. Microsoft Dynamics GP
B. IDEA
C. ACL
D. Picalo
Answer: A
MC Graphic 10-4

10-M/C #4. The graphic 10-4 is called a(n):
A. Association matrix
B. Link chart
C. Familial chart
D. Grouping chart

Answer: B

MC Graphic 10-5

10-M/C #5. The graphic 10-5 is called a(n):
A. Association matrix
B. Link chart
C. Familial chart
D. Grouping chart

Answer: A

10-M/C #6. Which of the following would be considered a batch control for payroll?
A. A total on FICA taxes withheld.
B. A total on Federal Income taxes withheld.
C. A total on employee hours.
D. A total on state income tax withheld.
10-M/C #7. Which of the following would be normally be detected as an input error in payroll processing?
A. An alphabetic character in the employee hours field.
B. Overtime hours above 10 hours for an individual employee.
C. Zero hours for a long time employee.
D. The addition of a new employee.
Answer: A

10-M/C #8. An example of an input error that would likely be caught by a validation control in payroll processing would be:
A. Overtime hours above 10 hours for an individual.
B. Zero hours for a long time employee.
C. 90 hours worked by one employee in one week.
D. The addition of a new employee
Answer: C

10-M/C #9. The assertions of management related to financial statements include all of the these EXCEPT:
A. The existence of assets and transactions.
B. The completeness of the transactions.
C. Proper disclosure of all rights and obligations.
D. Assurance of future profitability.
Answer: D

10-M/C #10. Which of the following is NOT a tool to collect digital evidence?
A. Road MASSter
B. Encase
C. HDD Regenerator
D. Microsoft Dynamics GP
Answer: D

10-M/C #11. One of the major functions of data security and privacy tools such as Privacy Suite is to:
A. Copy files
B. Rename files
C. Overwrite files
D. Recycle files
Answer: C

10-M/C #12. The functions of data extraction and analysis software tools includes all EXCEPT:
A. Sorting  
B. Input into payroll system  
C. Verifying multiples of a number  
D. Correlations analysis  

Answer: B

10-M/C #13. The functions of data extraction and analysis software tools includes all EXCEPT:  
A. Compliance verification  
B. Input into inventory system  
C. Duplicate searches  
D. Correlation analysis  

Answer: B

10-M/C #14. Duplicate searches in data extraction and analysis software could be used to discover:  
A. Invoices that have been paid twice  
B. Missing employees  
C. Missing invoices  
D. Stolen inventory  

Answer: A

10-M/C #15. Compliance verification in data extraction and analysis software could be used to discover all EXCEPT:  
A. Credit approvals for customer credit limits by credit manager  
B. Excessive per diem amounts on employee expense accounts  
C. Criminal background searches on prospective employees  
D. Insuring that middle managers do not exceed company mandated budget limits  

Answer: C

10-M/C #16. Verifying multiples of a number in data extraction and analysis software could be used to discover all EXCEPT:  
A. Recalculation of invoice totals  
B. Reimbursement rates for mileage  
C. Paycheck amounts for hours worked  
D. Embezzled petty cash  

Answer: D

10-M/C #17. Correlation analysis in data extraction and analysis software could be used to discover all EXCEPT:  
A. Correlations where none existed previously  
B. Non-existent inventory
C. Correlations that currently exist
D. How variables move in the same direction

Answer: B

10-M/C #18. In data analysis and extraction software, the types of queries conducted on the general ledger would include everything EXCEPT:
A. Calculating financial ratios
B. Select specific journal entries for analysis
C. Age counts receivable in various formats
D. Create actual to budget comparison reports

Answer: C

10-M/C #19. In data analysis and extraction software, the types of queries conducted on accounts receivable would includes everything EXCEPT:
A. Identifying debits to expense accounts
B. Create a list of customer limit increases
C. Age accounts receivable in various formats
D. Identify gaps in the sequence of invoice numbers

Answer: A

10-M/C #20. In data analysis and extraction software, the types of queries conducted on sales analysis would include everything EXCEPT:
A. Analyze sales returns and allowances
B. Selecting specifying journal entries for analysis
C. Summarize trends by customers type
D. Create reports on customer demand

Answer: B

10-M/C #21. This type of graphic allows the investigator to analyze the movement of goods services, people and money:
A. Gantt chart
B. Link chart
C. Association matrix
D. Flow diagram

Answer: D

10-M/C #22. This type of graphic organizes information about events chronologically to determine what has occurred:
A. Link chart
B. Association matrix
C. Timeline
D. Flow diagram

Answer: C
10-M/C #23. The software product Analyst’s Notebook I2 would be classified as:
A. Data analysis and extraction software
B. Case management software
C. Electronic spreadsheet
D. Data presentation software

Answer: B

**Short Answer Essay**

10-SAE #1. List five assertions of management in respect to financial statements.

Answer: The assertions of management related to financial statements include the following:
1. The existence of assets and transactions.
2. The completeness of the transactions reflected in the financial statements and related notes.
3. Proper disclosure of all rights and obligations associated with assets and liabilities.
4. The valuation of transactions and balances reflected in the financial statements are reasonable.
5. Proper financial statement presentation and disclosure of the related notes.

10-SAE #2. List two commercial data extraction and analysis software and list four functions of this software.

Answer: ACL and IDEA are two commercial software programs. The available functions include the following:
- Sorting
- Record selection and extraction
- Joining files
- Multi-file processing
- Correlation analysis
- Verifying multiples of a number
- Compliance verification
- Duplicate searches
- Vertical ratio analysis
- Horizontal ratio analysis
- Date functions
• Recalculations
• Transactions and balances exceeding expectations

10-SAE #3. List and describe three graphical techniques used to support the forensics professional.

Answer: One of the first graphical tools is an association matrix for identifying major players who are central to an investigation and to identify linkages between those players. Linkages can take the form of names, places, addresses, phone numbers, etc. Although all of these data are documented as preliminary evidence electronically in some software tool, such as Excel, Access, or even Word, the association matrix is a starting point for reflecting some of the most important data in a simplified format.

Link charts are another way to represent the associations, linkages, and other important relationships graphically. They help graphically describe linkages between entities: people, businesses, and “organizations” (in quotes because some organizations, including gangs, consortiums of drug dealers, and organized criminal enterprises, are probably not listed with the Secretary of State’s records but may act and operate like many legitimate business entities). Link charts therefore create a graphic representation of known and suspected associations among businesses, individuals, organizations, telephone numbers, addresses, e-mail accounts, Web sites, etc. that are potentially involved in criminal activity.

The next type of graphic is the flow diagram. It allows the investigator to analyze the movement of events, activities, and commodities—to see what that flow means in relation to a suspected criminal activity. The flow diagram can be used for the following:
• To illustrate the operation of the illegal movement of goods, services, people, money, etc.
• To present the activities that precede a suspected criminal act
• To show the flow of criminal goods, cash flows, and profits
• To illustrate and describe a money-laundering scheme
• To present changes in organizational structure over time
• To illustrate the flow of cash, information, or documents through an organization
**Critical Thinking Exercise**
A married couple goes to a movie. During the movie, the husband strangles the wife. He is able to get her body home without attracting attention.

How is this possible?

Answer: The male action portraying the husband kills the female actress portraying the wife.

**Text Review Questions**

10-TRQ #1. What are the two major approaches for testing IT system controls?

Answer: First, the IT systems can be audited around. This is often referred to as the “black-box” approach, according to which the professional relies on interviews and flow charts to develop an understanding of the systems but primarily tests the integrity of the data and the system by reconciling inputs to outputs. The second alternative is the “white-box” approach, which utilizes a relatively small dataset to test the system. Some of the tests performed include authenticity, accuracy, completeness, redundancy, access audit trail, and rounding error tests.

10-TRQ #2. What is meant by the acronym CAATTs and what are they used for?

Answer: CAATTs (Computer-Aided Audit Tools and Techniques) can assist with the testing of the IT systems control environment. They are used to detect and report on potentially fraudulent transactions.

10-TRQ #3. What is computer forensics?

Answer: Computer forensics involves using specialized tools and techniques to image and capture data and information, housed on computer hardware and embedded in software applications, so that the integrity and chain of custody of such evidence is protected and can be admitted into a court of law.

10-TRQ #4. What computer functions can make recovering deleted files more difficult?

Answer: An activity that can severely reduce the ability to recover deleted files is the “Defrag” command. Defrag, or defragmenting the hard drive, is a method of reorganizing the computer hard drive so that the unused space is allocated for the most efficient data storage.

10-TRQ #5. How do e-discovery rules have an impact on the storage of e-mail and other electronic files?
New e-discovery rules require organizations to be able to provide e-mail and other electronic files that go back in time in a manner similar to that of paper files. So the probability of e-mail and other deleted file recovery in an e-discovery environment is greatly enhanced.

10-TRQ #6. What functions are used by data extraction and analysis software to highlight red flags of fraud?

- Answer: Sorting
- Record selection and extraction
- Joining files
- Multi-file processing
- Correlation analysis
- Verifying multiples of a number
- Compliance verification
- Duplicate searches
- Vertical ratio analysis
- Horizontal ration analysis
- Date functions
- Recalculations
- Transactions and balances exceeding expectations

10-TRQ #7. What are the two categories of data mining and knowledge discovery software?

Answer: Data mining and knowledge discovery software is generally classified into two general categories:
- Public domain/shareware/freeware: available free, or for a nominal charge, through Web sites, ftp sites, and newsgroups. Some of the more common freeware includes Picalo, SAOimage, Super-Mongo, Tiny Tim, and xv. Many shareware programs, such as WINKS v4.62, allow users a trial period, after which a fee must be paid to reactivate the software. Freeware and shareware programs can be located through Internet search engines and through software download services. In some cases—research prototypes/beta versions or free software in the development stages—users are asked to review performance, report malfunctions, etc.
- Commercial applications: general release products, usually with technical support and warranty

10-TRQ #8. What role do graphics play in an investigation?

Answer: Graphics have at least three distinct roles in an investigation.
- First, they can be used as an investigative tool. By visually putting together linkages, flows, timelines, and other graphics, the investigator can gain insight
into the case, possibly seeing the case in ways that he or she had not previously considered.

- Second, graphics can also help the investigator to identify holes in the case or problem areas where further investigation is required. For example, the graphics might suggest that persons with opportunity have not been properly eliminated as suspects. Similarly, graphics can be used to identify questions that need to be answered in order to wrap up a case. Graphical representations of the data, like spreadsheets and examination of raw data, such as source documents, can facilitate critical thinking by facilitating consideration of the case from differing perspectives.

- Third, graphics can be useful to communicate investigative findings, conclusions, and results.

10-TRQ #9. What is the purpose of timelines in an investigation?
Answer: A timeline organizes information about events or activities chronologically to determine what has or may have occurred and the impact that these actions have had on the activity under investigation.

10-TRQ #10. How is case management software used in an investigation?
Answer: Case management software can be used in a number of situations to manage cases and case data, organize it in meaningful ways, and even present information for use in reports or during testimony. Sophisticated, complicated, and complex cases can benefit from the use of case management software.