Journal of Forensic & Investigative Accounting
Vol. 4, Issue 1, 2012

Integrating Generalized Audit Software and Teaching Fraud Detection in Information Systems Auditing Courses

Constance M. Lehmann*

ABSTRACT

The purposes of this paper are to: 1) describe the integration of generalized audit software (GAS)—specifically, IDEA—in an information systems auditing course, 2) to illustrate the data mining capabilities of IDEA in two fraud detection cases and, 3) make recommendations regarding the effective integration of the software in other auditing or fraud/forensic classes. The first fraud case presented here illustrates the use of data mining techniques to detect unauthorized users in the system (Unauthorized Users), and the second illustrates detection of unauthorized payments (Unauthorized Payments).

Keywords: Generalized Audit Software (GAS), IS auditing, fraud detection, cases.

Acknowledgements: The author would like to thank Carolyn Newman and Phyllis Erickson of Audimation Services, Inc. for their support and assistance in providing data, training and advice for this project. In addition, Carolyn Strand Norman provided helpful comments and suggestions to improve this manuscript. The feedback from participants at the AIS Educators Conference (2010) and the Forensic and Investigative Accounting Mid-Year Meeting (2011) improved the case materials and teaching notes significantly, as did the comments/suggestions from two anonymous reviewers. The data for the fraud detection cases was provided by Audimation Services, Inc. during a workshop and is available from the author. Permission to use screenshots from the IDEA software and workbook provided by Audimation Services, Inc., (a business partner of CaseWare IDEA, Inc.), the sole provider of IDEA Data Analysis Software and product support in the United States (http://www.audimation.com).

* The author is Associate Professor of Accounting at the University of Houston-Clear Lake.

INTRODUCTION

The proliferation of fraud cases in the financial services (e.g., Bernie Madoff, Jerome Kervial of Societe Generale) and other industries (e.g., Enron) has resulted in the desire to hire auditors with fraud detection and forensic skills. The importance of having these skills in-house for many companies as part of their internal audit function is also being discussed.[1] This is in addition to calls to integrate technology into the accounting curriculum for the last two decades. Albrecht and Sack (2000) suggested the importance of curriculum change by integrating technology to avoid producing accounting graduates unable to operate in our technologically advancing profession. The purposes of this paper are to a) describe the integration of generalized audit software (GAS)—specifically, IDEA—in an information systems auditing course, b) illustrate the data mining capabilities of IDEA in two fraud detection cases developed for the course developed by the author and, c) make recommendations as to the integration of the software in other auditing or fraud/forensic classes. The graduate-level information systems auditing course described here integrates the IDEA software throughout the semester to teach fraud detection and analysis techniques, tying in the use of the software with the lecture and discussion material.

Ahadiat (2008) discusses the Association to Advance Collegiate School of Business International (AACSB) and AICPA requirements that students acquire experience with technology tools in use in the profession. Their survey suggested that while accounting information systems classes made some use of computer labs for class meetings and data analysis software assignments, auditing classes did not make use of

[1] This issue was discussed during the panel discussion (current security issues) at the October 20, 2010 Information Systems Audit and Control Association (Houston Chapter) meeting.

these. Many times, instructors are reluctant to integrate software into a class that already has more than enough topic coverage requirements to fill a semester. The addition of a new software package with its associated learning curve can be intimidating. Smith-David, Maccracken, and Reckers (2003) point out that the high costs, along with the non-assured rewards of adding software to the course account for the reluctance of instructors to implement technology, particularly if instructors do not feel that they are "technology-savvy." While Smith-David *et al.* (2003) specifically addresses the integration of technology into introductory accounting courses, their comments also apply to courses such as auditing, fraud/forensic classes, and /or information systems auditing. This is especially true for instructors trying to develop a new course who do not have the time and/or resources to develop software-based assignments.

Our university's experience with Audimation Service's Academic Partnership Program has provided our students with a competitive edge when they interview for jobs in the fraud examination profession.[2] This paper discusses how the IDEA software was integrated into a graduate-level information systems auditing (IS Auditing) class, which uses hands-on fraud detection and analysis exercises throughout the semester. Included here are two fraud cases developed by the author. This paper also provides suggestions to help instructors integrate data extraction software into any auditing or fraud/forensic auditing class.

BACKGROUND

Scheiner and Kiger (1983) were some of the first to encourage the integration of GAS into an auditing elective course. The Auditing Section Education Committee of the

[2] CaseWare IDEA, Inc. of Canada develops the software. Audimation Services (www.audimation.com) is the US distributor of the IDEA software

American Accounting Association (the Committee) (2000-2001) discussed changes in the topic coverage in information systems auditing courses since the Groomer and Heintz (1994) study. Of the eleven syllabi for IS auditing courses reviewed, nine (81.8 percent) covered computer-assisted audit tools/techniques, as compared to 36.1 percent in the earlier Groomer and Heintz study. In addition, the Committee noted that 36.4 percent of the IS auditing classes were covering fraud and substantive testing of the revenue and purchasing cycles. The IDEA software integrates especially well in these areas. The ability of the software to perform data mining and data extractions with a user-friendly, menu-driven format helps the students use hands-on techniques to apply what they are learning in the auditing class.

While Janvrin, Bierstaker, and Lowe (2008) show that the professional auditors in their sample use audit information technology for certain procedures, such as sampling, analytical procedures, and report writing, their respondents did not indicate frequent use of audit IT for fraud review. This was in contrast to the respondents' indication of the importance of auditing applications for fraud review. Janvrin *et al*. (2008) recommend that the audit firms expand the use of audit applications, and suggested that those setting auditing standards address the use of auditing applications in the areas of fraud review. Pearson and Singleton (2008) lament that accounting education has not kept up with the innovations in fraud and forensic auditing. The IDEA software is an excellent data mining tool that illustrates fraud detection techniques. For example, the software can analyze large sets of data, and can perform Benford's analysis or other extractions to detect fraud (e.g., determining if terminated employees are still logging in to the system).

Three years ago, a graduate-level IS auditing elective course was developed incorporating the recommended topics from the ISACA Model Curriculum for a basic IS auditing course. References used to develop class materials included the Certified Information Systems Auditor (CISA) review materials, trade publications, older IT Audit textbooks, and recent articles from the *ISACA Journal*. The materials for the course currently include a trade publication on IT Auditing and a custom book that includes auditing and forensic topics, as well as recent articles from the *ISACA Journal, Internal Auditor, Fraud Magazine,* and the *Wall Street Journal* dealing with IT and fraud auditing topics. The recommended topic coverage in the course ties in well with the IDEA workbook, as each chapter in the workbook covers a partial audit of a business process. Exhibit 1 is an excerpt from the course syllabus, illustrating how the IDEA software is integrated into the course topics covered.

Course Learning Objectives and Integration of the IDEA Software

The learning objectives of the IS Auditing course include providing the student with the information to:

1. Apply core concepts of IS auditing
2. Recognize legislation, rules, and regulations related to IS auditing
3. Analyze the unique risks of information technology and information assets
4. Acquire experience conducting portions of business process audits and interpreting results using the IDEA software. This experience includes writing formal audit reports discussing the audit findings, potential risk exposures, and recommendations to management.

5. Learn basic techniques for fraud detection in the areas of disbursements and system access

The students are introduced to the software during a lab session conducted during the third week of class. There are five IDEA assignments in the course: three require the students to work through the three audit chapters in the IDEA workbook (accounts receivable, accounts payable, and inventory), and two are fraud detection assignments developed by the author (one addressing unauthorized users and the other addressing unauthorized payments). Each assignment is completed by the individual students and takes them approximately 2-5 hours each.

Features of the IDEA Software

The IDEA educational version includes a workbook, the software CD (with related data files), online access to a case (with data files), and technical support for both students and instructors.[3] The workbook is organized by audit. Each chapter includes step-by-step instructions with screen shots and check figures for the audit of the area. At the beginning of each section is an introduction to the audit (including instructions for importing the necessary data files), followed by a description of the potential risks of the area, the implications of that risk, and the management assertions addressed by mitigation of that risk (see Exhibit 2). Each section of the workbook also contains an audit program, which the students are required to fill out and turn in (Exhibit 3). Students must also write an audit report discussing the audit findings, potential risk exposures, and

[3] Instructors who enter into an academic partnership with Audimation receive a free copy of the software (limited to 5,000 records), the IDEA workbook, and the case study. The school is allowed to load the software on its network as well. The workbook data files are included on the CD included with the package. Version 8.4 is the current version, which is compatible with Windows 7. Audimation provides the workbook and the software to the students for about $35 (plus any bookstore markup).

recommendations to correct the deficiencies noted. For the assignments discussed here, the students go through the workbook on their own to prepare to work the business process audits. For an instructor new to integrating IDEA into their class, they can use the workbook chapters as assignments early in the semester, and then complete the two fraud assignments included here (as is suggested in the schedule shown in Exhibit 1).

The IDEA workbook illustrates the use of IDEA for many tests typically performed during a fraud audit—e.g., random/stratified samples, extractions of high or low value items, tests for duplicate checks, gap detection, Benford's analysis, joining databases with a common data field, and aging analysis.

Another feature of IDEA is the history file. This file records all of the actions performed by the user in a particular working folder (i.e., audit) and can be printed out as an "audit trail" for the instructor to review. Items cannot be deleted from the history file, but comments can be added to help future users replicate and/or understand the procedures performed by previous users. This file can be viewed any time the software is open in that working folder. An excerpt from a history file is illustrated in Exhibit 4.

Pedagogy

The simplest way to integrate the IDEA software for fraud detection in an auditing course is to tie the chapters in the IDEA workbook to the business process audit discussions, as shown in Exhibit 1. The requirement that the students fill out the audit program and interpret their results requires them to consider the implications of their results on the risk assessment for the area. For example, if the results indicate that some disbursements were made on Saturday or Sunday, this might not necessarily indicate

fraudulent activity (e.g., if the company is open seven days a week), but should be investigated further, particularly if the client does not normally conduct business on the weekends. The resultant risk exposure from unauthorized disbursements could be substantial, and recommendations of controls to limit this activity could be made once the investigation of noted exceptions is completed.

While an instructor might choose to use the data provided with the IDEA software, instructors can develop their own assignments using other data, which allows the students to use the workbook as a reference.[4] With the fraud detection cases discussed here, the data mining capabilities of IDEA are illustrated, allowing an instructor to integrate a discussion of fraud detection and forensic investigation. The two fraud detection cases developed for the graduate IS auditing course are described in the section entitled "Fraud Cases Using IDEA."

Benefits of Integrating IDEA into the Course

Besides addressing the issues mentioned in the Committee's report, the benefits of integrating IDEA into IS auditing course include:

- Hands-on knowledge of a popular GAS, resulting in a more interactive approach to teaching auditing techniques and tools
- Practice using audit programs, performing a risk assessment, and applying audit objectives
- Development of written communication skills because of the requirement to write an audit report based on the findings

[4] Audimation's Academic Partnership currently works with professors using IDEA in their courses to provide an online forum where professors can share developed cases and data files with other professors who are members of the Academic Partnership (http://www.audimation.com/academic.cfm).

- Practice in the use of data mining techniques utilized in fraud detection
- Low cost of software and materials (free to instructors and universities, inexpensive to students)
- Software compatibility with most university networks; software can also be used by the students on their home or office computers
- The software is easy to learn, has excellent technical support, and discounted supplemental training for educators is available through Audimation Services
- Providing the students with a competitive advantage during interviews because of their experience in using auditing software, performing actual fraud detection procedures, and analyzing their results[5]

Limitations of the IDEA Software

In our experience as a university, there have been very few problems with using the IDEA software over the last nine years. The software works well on institutional networks, and the students have no difficulty loading IDEA on their personal computers. To become fairly conversant in the software requires a 2-4 hour investment of an instructor's time to learn the software (the best way to do that is to work through the workbook). There are no licensing problems with the educational version, although an instructor who wants to introduce the use of IDEA for large databases might find the 5000 record limitation of the educational version of the software to be an issue. The newest versions of IDEA have added the ability to import SAP databases and are

[5] The IDEA software is being used by many accounting firms and internal audit departments throughout the world.

compatible with Windows 7 operating systems. Importing text files is still somewhat challenging, but the learning curve for this procedure not steep.

Grading

These cases are used in the class as individual assignments, requiring submission of the required materials by each student. The students receive credit for handing in the correct printouts and submitting their electronic files via the course support website. Exhibit 5 shows the breakdown of the scores for the various assignments. Since screen shots and check figures are provided in the IDEA workbook, the total points allocated to the assignments from the workbook are lower than those for the fraud cases (for which the workbook is a reference). Exhibit 6 shows the rubrics for the "Unauthorized Users" and "Unauthorized Payments" cases (described below), allowing the instructor to assess student learning of basic fraud detection skills.

Student Feedback

Student feedback on the use of the IDEA software has been very positive. In the formal evaluations, the students rated the use of the software highly and wrote comments indicating that the hands-on applications made the course more interesting and helped them understand the concepts they were learning. Since there is no auditing or accounting information systems prerequisite for the course, the knowledge levels vary among the students. In the three years the course has been taught at our university, there has not been a single negative student comment about the IDEA software. We even had a student taking the course who detected fraud (using IDEA) while auditing a client during his

internship with a small accounting firm. Student comments with regard to these cases have been very positive, as students enjoy the "investigative" nature of the assignments. The average score on the formal evaluations for the item "involving students in hands-on projects" has averaged 4.8 (out 5). Examples of individual comments include, "lots of projects and hands-on cases that were interesting," "this course really made auditing interesting. I really liked using IDEA to do the fraud assignments."

Recommendations for Utilizing the IDEA Software in Other Courses

Integrating the IDEA software in other classes can be accomplished quite easily. Our university has been using the IDEA software in various classes since 2002. For example, we have integrated this software into an undergraduate accounting elective that teaches the students advanced spreadsheet skills and applications of IDEA in auditing. We also introduce the IDEA software in the graduate-level accounting information systems course to encourage students to take higher-level electives to develop their skills with the software beyond the basics taught in the workbook. Most types of databases can be easily imported into IDEA (e.g., DB files, Access files, Excel spreadsheets, SAP files). As an instructor becomes more comfortable using the software, he/she can develop new assignments using other data.

The IDEA software can also be utilized in a fraud or forensic auditing class because of the data mining techniques available for detecting disbursement, receipts, payroll, travel expense account, and fixed asset fraud. Other universities have used the software in internal auditing classes (emphasizing the fraud detection features of IDEA).

In addition, add-ons are available for the software to allow the user to utilize advanced sampling and statistical methods such as trend analysis and correlation analysis.

The use of IDEA to illustrate data mining techniques in fraud detection teaches students to detect and analyze potential signals of fraudulent activity, which ties in directly with the requirements of the Statement on Auditing Standards (SAS) No. 99. SAS No. 99 requires that the audit teams document discussion of the risk of potential material misstatement due to fraud by the client. SAS No. 99 also requires that the team consider fraud risks when determining the analytical review procedures performed, and requires that the auditors communicate their fraud concerns to management, the audit committee, and other concerned parties. The requirement that the students interpret their audit findings and compose an audit report discussing those findings helps the students learn to identify what can go wrong in disbursements or access control functions.

The next section discusses two basic fraud detection cases developed by the author using the IDEA software and Excel data files.[6]

FRAUD DETECTION CASES USING IDEA

Students are very aware of the proliferation of fraud in the corporate world, and they are very interested in learning how to detect fraud. Both of the cases described here are set up as fraud detection audits. The cases deal with testing for unauthorized system access (Case 1) and testing for unauthorized payments (Case 2). The Excel data files (available from the author) include the Employee Master File, the Supplier Master File (Supplier File), the Active Users Directory File, the Payroll Most Current Period File, the

[6] Data files were initially provided by Audimation Services during a professional meeting training session. These data files were modified to expand the assignments. Data available from the author or Audimation Services at www.audimation.com .

Accounts Payable File (AccPay for fraud), and the Customer Invoice File. The cases include a risk assessment with related management assertions to be tested, and an audit program that includes references to the section(s) in the IDEA workbook for the procedures.

Audit Objectives of the Unauthorized Users Audit (Case 1)

The students are given the following information for the Unauthorized Users case:

You have been put in charge of the fraud detection audit for your client. The key risks associated with unauthorized access to the computer system, the business and audit implication of those risks, and the audit assertions that could be addressed by testing are shown in Exhibit 7.

The audit program for this case (Exhibit 8) should be completed as you perform your tests. Please turn in printouts of your results, the properly filled out/initialed audit program/audit procedures sheet, along with an audit report discussing your audit findings.

Appendix A in the Teaching Notes includes a description of the audit objectives/tests to be completed, narrative of the commands (with screen shots) necessary to perform each test, as well as screen shots of the results for each of the tests. The instructor can use the Appendix as an answer key and/or as lab notes to aid in teaching the students how to use the software.

Audit Objectives for Unauthorized Payments Audit (Case 2)

The students are given the following information for the Unauthorized Payments case:

You have been put in charge of the fraud detection audit for your client. The key risks associated with unauthorized payments in accounts receivable, accounts payable and payroll, the business and audit implication of those risks, as well as the audit assertions that could be addressed by testing can be found in Exhibit 9.

The audit program for this case (Exhibit 10) should be completed as you perform your tests. Please turn in printouts of your results, the properly filled out/initialed audit program/audit procedures sheet, along with an audit report discussing your audit findings.

Appendix B in the Teaching Notes includes a description of the audit objectives/tests to be completed, narrative (with screen shots) of the commands to perform each test, as well as screen shots of the results for each of the tests.[7] The instructor can use the Appendix as an answer key and/or as lab notes to aid in teaching the students how to use the software. Note that with both of these cases, once the students analyze their findings and put together an audit report, they have a better understanding of not only the specific exceptions, but also can identify any patterns that have emerged as the result of their tests. The instructor might even suggest the students develop follow-up procedures (e.g., the same person, "HMV," shows up as the person authorizing suspicious transactions that show up on the results of several of the tests from the Unauthorized Payments case. Follow-up investigation procedures might recommend a combination of interviews and source document collection.)

Concluding Remarks

It is essential that our students enter the profession with skills gained from hands-on experience with technology. Since many of our students enter public accounting or

[7] PDF files with the full results for both cases are available from the author.

internal auditing, experience utilizing data extraction software and analyzing results is a valuable and marketable skill. Many students are interested in learning methods to detect fraud, and being able to give them examples of how to use a tool such as IDEA to detect suspicious patterns and trends can give them an edge when they go on interviews. It also helps them develop a "trust-but-verify" attitude as they objectively review business processes and conduct their evidence-gathering tests.

REFERENCES

Albrecht, W. and R. Sack. 2000. *Accounting Education: Charting the Course Through a Perilous Future*, Sarasota, FL: AAA.

Ahadiat, N. (2008). "Technologies Used in Accounting Education: A Study of the Frequency of Use Among Faculty." *Journal of Education for Business*, January/February: 123-133.

American Institute of Certified Public Accountants. Statement on Auditing Standards No. 99. *Consideration of Fraud in a Financial Statement Audit (Supersedes SAS No. 82)*, effective for audits for periods beginning on or after December 15, 2002.

Auditing Section Education Committee of the American Accounting Association (2000-2001). "Challenges to Audit Education for the 21st Century: A Survey of Curriculum, Course Content, and Delivery Methods." *Issues in Accounting Education*, 18 (3): 241-263.

CaseWare, IDEA, Inc. (distributed by Audimation Services, Inc.) 2009. *IDEA Data Analysis Software for IDEA Version 8 Workbook (with software version 8.4).* CaseWare IDEA, Inc.: Toronto, Canada.

Janvrin, D., J. Bierstaker, and D. J. Lowe. 2008. "An Examination of Audit Information Technology Use and Perceived Importance." *Accounting Horizons*, 22 (1): 1-21.

Lehmann, C. M., C. D. Heagy, and C. Norman. 2007. "The Evaluation of Application Controls in Accounting Software: A Short Instructional Case." *Journal of Information Systems*, 21 (2): 87-98.

Pearson, T. A., and T. Singleton. 2008. "Fraud and Forensic Accounting in the Digital Environment." *Issues in Accounting Education*, 23 (4): 545-559.

Scheiner, J. H. and J. E. Kiger. 1983. "Generalized Audit Software: A Classroom Approach." *Issues in Accounting Education*, 1983 (1): 123-132.

Smith David, J., H. Maccracken, and P.M.J. Reckers. 2003. "Integrating Technology and Business Process Analysis into Introductory Accounting Courses." *Issues in Accounting Education*, 18 (4): 417-425.

EXHIBIT 1
Excerpt from Syllabus (Spring Semester 2009)[8]

02/09	Handout	**CLASS 3**: IT CONTROLS and USING COMPUTER ASSISTED AUDIT TOOLS AND TECHNIQUES (CAATS)/**IDEA LAB** * Audit Evidence Process (CAATs)	**Introduction to IDEA software in the lab (2nd half of class)**
02/16	Handout	**CLASS 4**: CONDUCTING THE IT AUDIT/AUDITING THE REVENUE PROCESS * Audit Planning Process * Audit Evidence Process LAB TIME TO WORK ON REVENUE PROCESS ASSIGNMENT	Bakshi (2004)
02/23	Handout	**CLASS 5**: AUDITING THE PURCHASING PROCESS/AUDITING THE INVENTORY PROCESS * Audit Planning Process * Audit Evidence Process LAB TIME TO WORK ON PURCHASING PROCESS/INVENTORY ASSIGNMENT	**IDEA Chapter 2 (A/R audit) due**
03/02	Davis chapters 3, 12, handout	**CLASS 6**: IT DEPLOYMENT RISKS, SDLC, and ENTITY-LEVEL CONTROLS/introduction to **PEACHTREE (Application Controls)** * Information Management and Usage * Development, Acquisition and Maintenance of Information Systems: System Development Life Cycle (from handout) * Impact of IT on the Business Processes and Solutions Entity-level control audits (chapter 3 in Davis book)	Hettigei (2005) **IDEA Chapter 3 (A/P audit) due**
03/09		**MID-TERM EXAM**	
03/16		**SPRING BREAK: NO CLASSES**	
03/23	Davis chapter 4, pages 83-105	**CLASS 7:** MANAGING THE IT FUNCTION AND DATA CENTERS Data center audit objectives and procedures Basic IT function organization (centralized v. distributed data processing): audit objectives and procedures Database issues: audit objectives and procedures • IS/IT Management (from Chapter 2 of CISA) LAB TIME TO WORK ON PEACHTREE CONTROLS ASSIGNMENT	Malik (2006) **IDEA Chapter 4 (Inventory audit) due**

04/20	Custom: pages 109-140, 176-218	**CLASS 11:** FRAUD AND FORENSIC AUDITING/DATA MINING TECHNIQUES LAB TIME TO WORK ON SECOND FRAUD ASSIGNMENT	10 Truths About Fraud (WebCT), Singleton (2006) ("What every auditor should know about cyberforensics") **IDEA unauthorized users due**
04/27	Same as above	**CLASS 12:** FRAUD AND FORENSIC AUDITING	Cilli (2005), Moynihan (2008), Johnstone and Wong (2008), Taylor (2008) **IDEA unauthorized payments due**

[8] In the most recent 15-week semesters, the IDEA workbook chapter assignments have been replaced with business process audits (revenue/accounts receivable, payables/payroll, and inventory/travel expense audits) developed by the author and available through the IDEA Academic Partnership webpage (membership required for access). The process audit discussions are covered after the class addressing fraud and forensic auditing (now class 5). The IDEA workbook is used as a reference by the students for the process audit assignments. The most current syllabus is available from the author upon request.

EXHIBIT 2
Example of IDEA Workbook Risk Assessment: Accounts Receivable Audit (Adapted from IDEA Workbook for Version 8)

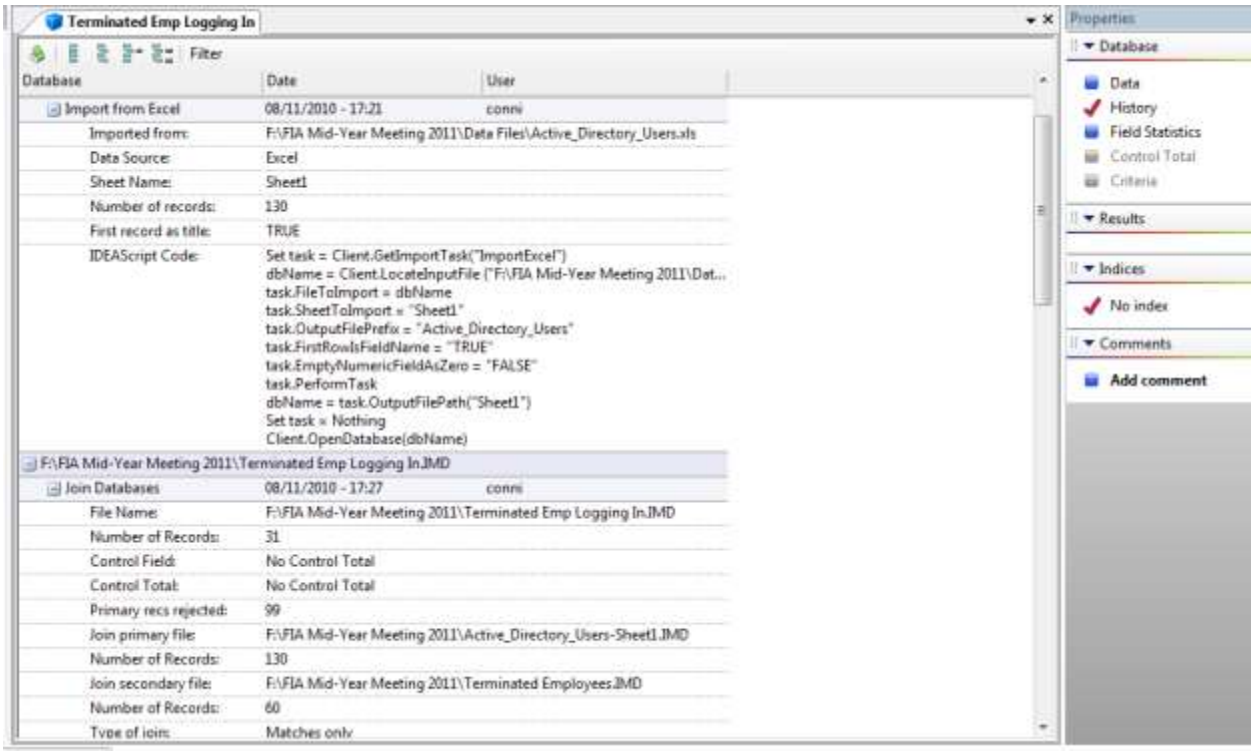
Risk	**Implications**	**Audit Objectives**
1. The file is incorrectly consolidated or summed	Items could be omitted, or the listed items may not be included in the totals reported in the financial statements. The Accounts Receivable could be overstated or understated depending on the direction of the error.	Completeness, Accuracy
2. Foreign currency transactions are not translated correctly.	Management may not be aware of the impact of transactions in foreign currency and may fail to take steps to manage currency risks. The Accounts Receivable could be overstated of understated depending on the direction of the error	Accuracy
3. Credit is granted to customers that are likely to default	The business will sell goods to parties from which they will not be able to collect cash. This has potential implications on liquidity and bad debt expenses.	Valuation
4. Customers are double-billed.	Double billing can negatively affect customer satisfaction. Also, revenues and receivables would be overstated.	Existence, Validity, Valuation
5. Accounts Receivable are invalid or incorrectly stated.	Accounts could be entirely or partly invalid. Partially invalid accounts may be the result of delays in processing transactions of errors in applying credits and payments to accounts. Fictitious accounts could be due to fraud.	Existence, Validity, Accuracy
6. Improper allocation of credits and payments.	Improper allocation of payments to accounts could affect the aging of the Accounts Receivable and this would affect management's ability to determine an effective course of action for handling the customer's account, e.g., sales to customers could be blocked or the customer sent to a collection agency even though the customer is current.	Existence, Validity, Accuracy
7. Accounts Receivable is not properly aged.	If the aging of the Accounts Receivable is not correct, then management may fail to take action on overdue accounts in a timely manner and permit sales to poor credit risks. Also, the calculation of the allowance for doubtful accounts and bad debt expense would be affected.	Valuation
8. A significant percentage of the receivables is concentrated in a few customers.	The business could be exposed to a combination of credit and liquidity risks if these large customers do not pay their debts in a timely fashion. Also, the company may be deemed to be economically dependent on the identified customers, and this may need to be noted in the financial statements.	Presentation
9. Improper classification of amounts	If a credit balance is classified as an AR instead of an AP, then it could distort the current ratio which could be part of a debt covenant.	Presentation

EXHIBIT 3
Example of Audit Program from IDEA Workbook: Accounts Receivable Audit
(Adapted from IDEA Workbook Version 8)

Auditing Procedures	Assertions	Work done by (initials)	Test Ref	Extent of Testing
1. Obtain the data files from the client and load onto the PC. Load IDEA and create a project for Accounts Receivable for Bright IDEAs, Inc.			2.3	
2. Agree the total of Accounts Receivable: a) Import the Accounts Receivable details, b) Check the total, c) Compute the field statistics, and d) Reconcile the control totals to the trial balance.	 C C C V		 2.5 2.7 2.8 2.9	
3. Select a sample for detailed testing and confirmation.	E O		2.10	
4. Prepare an aged accounts analysis to review the profile of debtors.	V		2.11	
5. Identify old and large accounts for detailed testing.	E V		2.12	
6. Identify all credit notes.	V		2.13	
7. Prove calculations: a) Calculations of net value and b) Totals by account.	V		 2.14 2.15	
8. Identify accounts exceeding their credit limit: a) Import the Customer Master File and b) Extract balances over their approved limit.	V		 2.16.1 2.16.2	

Key to Assertions: Completeness, Existence, Ownership, Valuation, Presentation

EXHIBIT 4
Excerpts from an IDEA History File



Second Page:

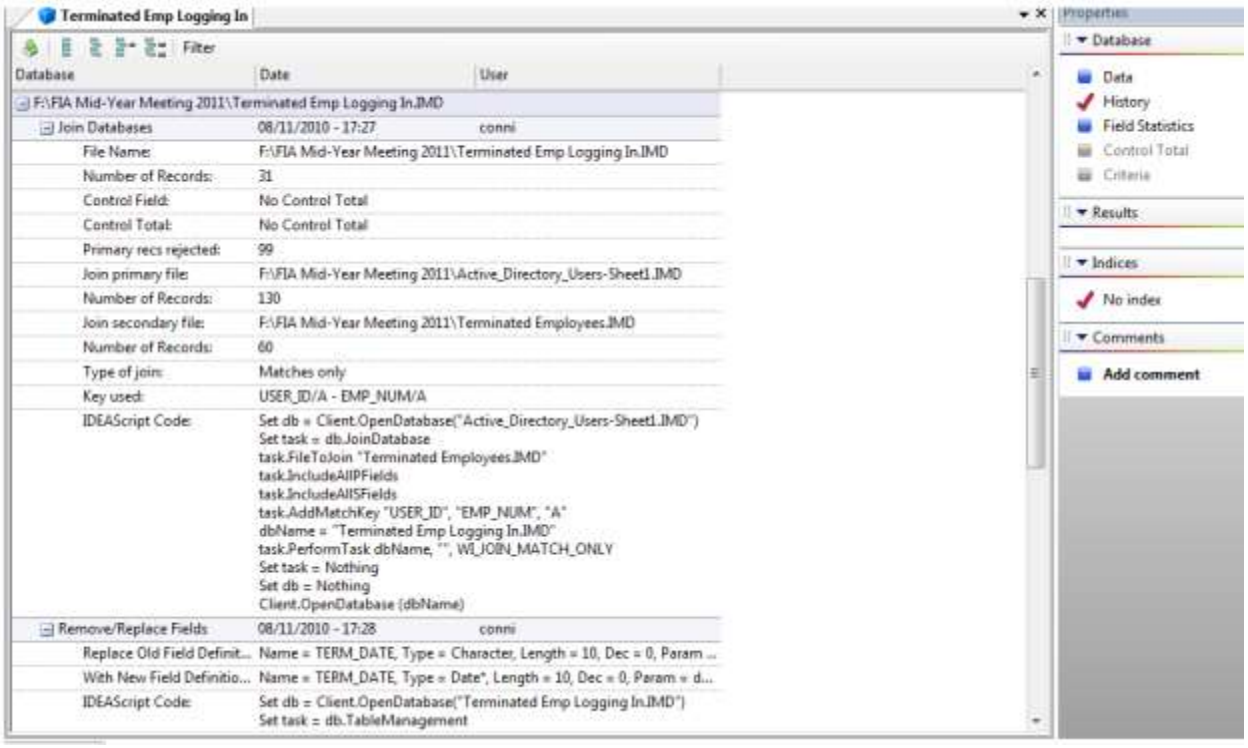


EXHIBIT 5
Example of Point Allocations for IDEA Assignments (Spring Semester 2009)

Name of Assignment/Case	Due Date	Number of Possible Points
IDEA chapter 2 (A/R)	02/23	10
IDEA chapter 3 (A/P)	03/02	10
IDEA chapter 4 (Inventory)	03/23	10
Peachtree Controls Assignment^	03/30	20
Auditing after SOX case	04/06	10
IDEA unauthorized users	04/20	20
IDEA unauthorized payments	04/27	20
Total Possible Points		100*

*Out of a total of 500 points in the course. The mid-term and final count 100 points each, the online quizzes (based on CISA practice questions) count for a total of 100 points, and the in-class group cases account for the remaining 100 points.

^ **Note:** The Peachtree Controls Assignment is adapted from Lehmann, Heagy, and Norman (2007) and the Auditing after SOX case is a written assignment (e.g., non-computerized).

EXHIBIT 6
Grading Rubrics for Unauthorized Users and Unauthorized Payments Cases

Panel A: Unauthorized Users

Rubric for IDEA: Unauthorized Users

Class ACCT 5335
Semester

IDEA Assignment
Number of Points: 20

Student ID	Name/date in title of audit (1 point)	4 Required Reports (2 each/8 points total)	Audit program prepared and properly filled out/signed off (2 points)	The interpretation of audit findings (8 points)	Printout of history file (1 point)

Panel B: Unauthorized Payments

Rubric for IDEA: Unauthorized Payments

Class ACCT 5335
Semester

IDEA Assignment
Number of Points: 20

Unauthorized Payments

Student ID	Name/date in title of audit (0.5 points)	The 10 required reports (1 each/10 points total)	Audit program prepared and properly filled out/signed off (1 point)	The interpretation of audit findings (8 points)	Printout of history file (0.5 points)

EXHIBIT 7
Risk Assessment for Unauthorized Users Case

You have been put in charge of the fraud detection audit for your client. Below are the risks associated with unauthorized access to the computer system. Below are the key risks, the business and audit implication of those risks, and the audit assertions that could be addressed by testing.

Unauthorized Users Audit Risk	**Implications**	**Assertions**
Terminated employees have been Logging into the system	Unauthorized access by terminated employees could cause misstatement of assets, destruction of data, improper monitoring/ updating of access	Validity, Accuracy Existence
Terminated employees are listed as vendors in the A/P master file	Improper vendor could represent diversion of company funds, indicating fraud	Existence, Validity
System log-ins on days/times the company is closed	Unauthorized access might indicate an intent to commit fraud	Existence, Validity

EXHIBIT 8
Audit Program for Unauthorized Users Case

From the available/possible tests, the audit manager has decided on the appropriate tests/procedures for you to complete.

Objective	Auditing Procedures	Work Done By Initials	Test Ref.	Extent of Testing
1	Import the employee and active directory user files (both Excel files) using the FILE/IMPORT ASSISTANT. Extract terminated employees using direct extraction with DIRECT EXTRACTION function. DIRECT EXTRACTION for TERM-DAT <> "" gives a list of terminated employees WINDOW/WORKBOOK/TILE allows you to look at both files simultaneously. Be sure to use the Terminated Employee file. Joining Active Directory and Terminated Employee Files (includes terminated employees) DATA/FIELD MANIPULATION to check that the format of USER-ID and EMP_NO are same format JOIN Active Directory Users and Terminated Employee files A DIRECT EXTRACTION can be used to determine if the last login date is greater than the termination date (use DATA/FIELD MANIPULATION to make sure both fields are date formats). If they are not the same An 8 digit date is in the format YYYYMMDD and an 10-digit date is in The DD/MM/YYYY.		Section 3.10.4 Section 3.15.2 Section 3.10.4	
2	Create a DIRECT EXTRACTION under the Employee file of terminated employees. Use IMPORT ASSISTANT to import the Suppliers file. Use the JOIN function to create a report of Suppliers who are also terminated employees		Section 3.10.4	
3	Use a DIRECT EXTRACTION of the Active Directory Users file to determine log-ins on weekends (use @dow function, Sunday = 1, Saturday = 7)		Section 3.10.4	

EXHIBIT 9
Risk Assessment for Unauthorized Payments Case

Unauthorized Payments Audit **Risk**	**Implications**	**Assertions**
Accounts Receivable Non-sequential customer invoice numbers	Invoices issued out of order could result in accounts receivable misstatement	Completeness
Accounts Payable Payments to fictitious vendors	Improper set up of vendors could result in fraudulent payments being made to outside parties	Validity, Existence
Vendors with P.O. box addresses, rather than street addresses	Could indicate an invalid/fictitious vendor could result in fraudulent payments and/or misstatement of accounts payable	Valuation
Payments on Saturday or Sunday	Payments made when the company is closed could suggest processing errors or fraud	Existence, Validity
Duplicate payments	Overpayment to vendors, overstates expenses	Validity, Valuation
Vendor and employee names/addresses are the same/similar	This could represent a diversion of funds or could be the result of contract labor arrangements	Existence, Validity
Multiple companies with the same address	Might be a means to double-pay vendors for the same materials or services, causing losses to the company from overpayment	Completeness, Validity
Invoices created slightly below the review threshold	Could indicate collusion with insider, or desire to avoid having someone review invoice that is higher than the PO, might result in company overpaying for materials	Validity, Valuation
Payroll Excessive hours worked	Could indicate "ghost" employees, or employees fraudulently reporting overtime not performed, overstates payroll expenses	Valuation, Validity
Salary payments to non-existent or terminated employees	Overstatement of payroll expenses	Valuation, Validity

EXHIBIT 10
Audit Program for Unauthorized Payments Case

Objective	Auditing Procedures	Work Done by (Initials)	Test Ref.	Extent of Testing
1	Ensure "customer invoices" is the active file INVOICE field contains the check number, make sure INVOICE field is numeric Perform GAP DETECTION task and report results		Section 3.12 Section 3.12 Section 3.12	
2	Ensure that "supplier master file" and "accpay file for fraud" have been properly imported Join databases with common key(use "no secondary match" or use "matches only"); perform necessary extraction to determine unauthorized suppliers and report results as in section 3.15		Section 3.15 Section 3.15	
3	Ensure that "supplier master file" is the active file DIRECT EXTRACTION on the Supplier file to find all suppliers with PO addresses, rather than street addresses (extraction: ADDRESS1 = "P.O.".OR. ADDRESS1="PO".OR.ADDRESS1="P O"). Report results		Section 3.10.4	
4	Ensure "accpay file for fraud" is the active file Perform DIRECT EXTRACTION to find all invoices paid on Saturday or Sunday and report results		Section 3.10.4	
5	Ensure all employees and supplier files are the active files Perform JOIN DATABASES function to determine employees and vendors with the same name and report results. Determine employees and vendors with same addresses (match on ADDRESS and ADDRESS1, respectively		Section 3.15.2	
6	Ensure "accpay file for fraud" is the active file Perform ANALYSIS/DUPLICATE KEY/DETECTION to identify duplicate payments and report results		Section 3.11	
7	Ensure "supplier master file" is active file Perform DATA/SORT to sort suppliers by addresses and analyze results			
8	Ensure "accpay file for fraud" is the active file Perform a DIRECT EXTRACTION to extract invoice amounts between $29000 and $30000 (which is the threshold for a higher level review for payment) and report results		Section 3.9	

Exhibit 10 (continued)

Objective	Auditing Procedures	Work Done by (Initials)	Test Ref.	Extent of Testing
9	Import the "payroll most current period" file Perform a DIRECT EXTRACTION to create a report of all employees who worked more than 40 hours in the most recent week		Section 3.15	
10	Import the "employee master file", determine "payroll most current period" is the active file. Join the two files Perform an extraction of all terminated employees from the combined file For terminated employees, compare the termination date with the date of the paycheck Determine whether any current payees are not listed on the current employee file (note that this will include terminated employees) Report results of your analysis		Section 3.15	

TEACHING NOTES

Using the Cases

The two fraud detection cases (Unauthorized Users and Unauthorized Payments) are given as individually-completed out of class assignments. These cases are assigned during the fraud/forensic investigation portion of the graduate information systems auditing course (IS auditing), but could easily be incorporated in an internal auditing, fraud/forensic auditing, or regular auditing class. Since the IDEA software is introduced early in the semester for our IS auditing course, and the students must work through the workbook, they are familiar with the software by the time these cases are due later in the semester. An alternative to assigning the cases as an out of class assignment is to present the cases in a lab for the students.

The IDEA software is loaded on our University server, and can be purchased (with the workbook) by the students for a reasonable price. The data files needed for these cases are all Excel 2003 files which are easily imported into IDEA. With these data files, the instructor can adjust the data in Excel to change or adjust the case results, or can expand the audit procedures.

Appendix A contains the "answer key/lab instructions" for completing the audit procedures for the Unauthorized Users case. Appendix B contains the "answer key/lab instructions" for completing the audit procedures for the Unauthorized Payments case. These include screen shots to help with instruction.

Analyzing Audit Findings

Requiring the students to analyze their findings in a report is meant to help them to reflect on and communicate their results, as they would in a real audit. Several studies document that writing assignments can enhance the learning experience (e.g., Libby and Frederick 1990, Stocks *et al.* 1992, Baird *et al.* 1998, Koepppen 2000, Riordan *et al.* 2000, Larkins 2001, Messmer 2001, Ashbaugh *et al*. 2002, and May and May 2003). Entry-level auditors must document their findings clearly on their audit workpapers. Stocks *et al.* (1992) suggested that "writing to learn" activities in accounting classes provides a way to solidify concepts and enhance understanding by compelling the students to concisely summarize a problem or issue covered in class. The students in the IS auditing class must write an audit report (discussing the scope, executive summary, potential risk exposures, findings, and recommendations) to the instructor. This writing assignment further enhances learning by including the following requirements specified by Stocks *et al*. (1992):

- Provides a purpose, i.e., requires students to examine their findings and compile that information into a concise memo interpreting their results,
- Indicates the proposed audience, i.e., their instructor (supervisor), and
- Specifies the type of assignment, i.e., "reflective memos"/audit reports for both cases. As recommended by Stocks *et al.* (1992), the students are also provided with grading rubrics for the cases in advance.

Baird *et al.* (1998) found the students' perceptions of learning were higher in classes with "writing to learn" assignments than in the control class (with no writing assignments). Riordan *et al.* (2000) found evidence that writing skills of accounting

students improved with a "writing across the curriculum approach." This corresponds to more recent requirements for improving written communication skills required by professional organizations such as state societies of CPAs, and accrediting bodies such as the AACSB. The audit report requirement in these cases should encourage the students to reflect on the implications of their audit findings, and help them develop skills in concisely interpreting and communicating their results.

REFERENCES

Ashbaugh, H., K. Johnstone, and T. Warfield. 2002. Outcome assessment of a writing-skill improvement initiative: Results and methodological implications. *Issues in Accounting Education*, 17 (2): 123-149.

Baird, J., R. Zelin II and L. Ruggle. 1998. Experimental evidence on the benefits of using "writing to learn" activities in accounting courses. *Issues in Accounting Education*, 13(2): 259-276.

Koeppen, D. 2000. Writing for success: Some tips for the accountant. *The National Public Accountant,* 45 (7): 48-49.

Larkins, E. 2001. Developing a clearer and stronger writing style. *The National Public Accountant,* 46 (7): 42-45.

Libby, R. and D. Frederick. 1990. Expertise and the ability to explain audit findings. *Journal of Accounting Research*, (Autumn): 348-367.

May, C. and G. May. 2005. *Effective Writing: A Handbook for Accountants*, 7th Edition. Upper Saddle Hall, NJ: Prentice Hall.

Messmer, M. 2001. Enhancing your writing skills. *Strategic Finance,* 82 (7): 8-9.

Riordan, D., M. Riordan and M. Sullivan. 2000. Writing across the accounting curriculum: An experiment. *Business Communications Quarterly*, 63(3): 49-59.

Stocks, K., T. Stoddard, and M. Waters. 1992. Writing in the accounting curriculum: Guidelines for professors. *Issues in Accounting Education*, 7(2): 193-204.

APPENDIX A
Answer Key/Lab Notes for Instructor: Unauthorized Users Case

Objectives for case 1 (unauthorized users)

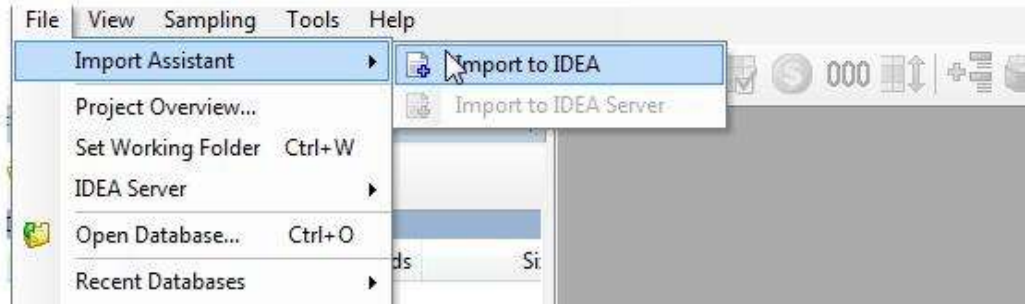
1. To determine whether terminated employees have been logging into the system (use Active Directory File and Terminated Employee File, refer to section 3.15.2 in IDEA book)
2. To determine whether terminated employees are listed as vendors in the A/P master file (use Terminated Employee File and Supplier Master File and match criteria should be "Address1")
3. To determine if there are system log ins on days/times the company is closed (use Active Directory File, see section 3.13, section 3.10.4 in IDEA book)

NOTE: The students must turn in printouts of their results (including history file), the properly filled out/initialed audit program/audit procedures sheet, along with an audit report memo addressed to the instructor interpreting their findings.

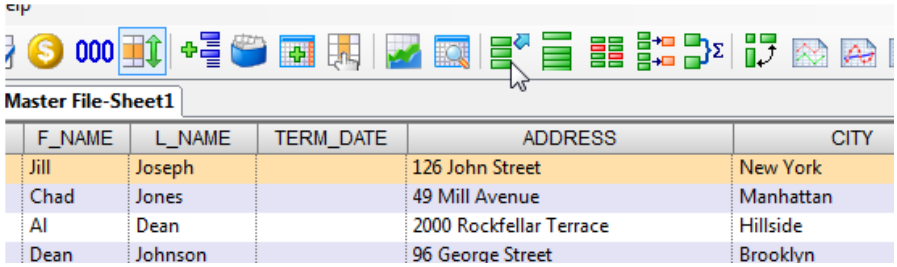
APPENDIX A (continued)

Objective 1
Set Working Folder as "Unauthorized Users Audit" from "Jan 1, 2007 – Dec 31, 2007".

Import the Employee Master File and Active Directory File (both Excel files) using the FILE/IMPORT ASSISTANT. Import as Excel file, with first row as field names.



Extract terminated employees using direct extraction with DIRECT EXTRACTION. Name the file "terminated employees".

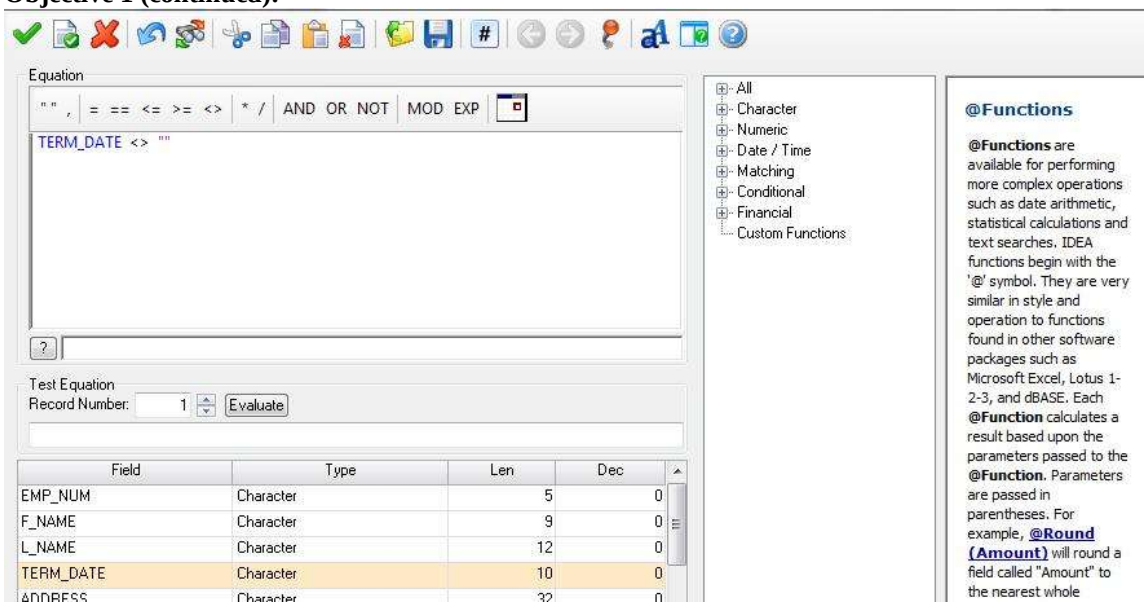


F_NAME	L_NAME	TERM_DATE	ADDRESS	CITY
Jill	Joseph		126 John Street	New York
Chad	Jones		49 Mill Avenue	Manhattan
Al	Dean		2000 Rockfellar Terrace	Hillside
Dean	Johnson		96 George Street	Brooklyn

DIRECT EXTRACTION for TERM_DAT <> "" (termination date not equal to blank) gives you a list of terminated employees (name this extraction "terminated employees"). There are 60 terminated employees.

APPENDIX A (Continued)

Objective 1 (continued):



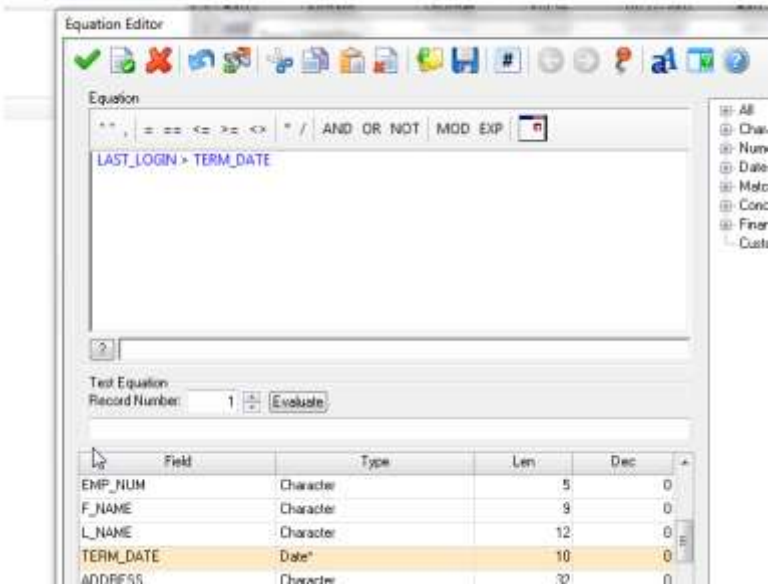
Join the Active Directory File (primary) with the terminated employees file (secondary) and match USER_ID and EMP_NUM (both should be in the (C) format).

Here are the first 30 (of 31) results:

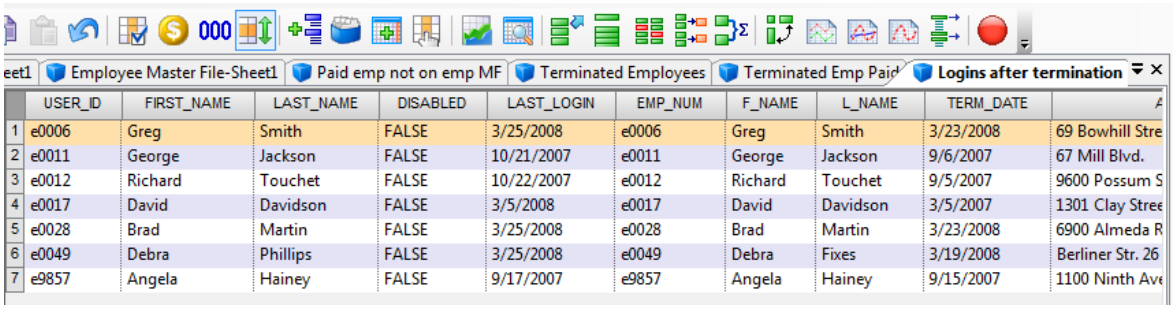
APPENDIX A (Continued)

Objective 1 (continued)

A DIRECT EXTRACTION can be used to determine if the last login date is greater than the termination date (use DATA/FIELD MANIPULATION or right click on the data and choose "field manipulation", TERM_DATE should be "date" formatted "dd/mm/yyyy").



Here are the results:

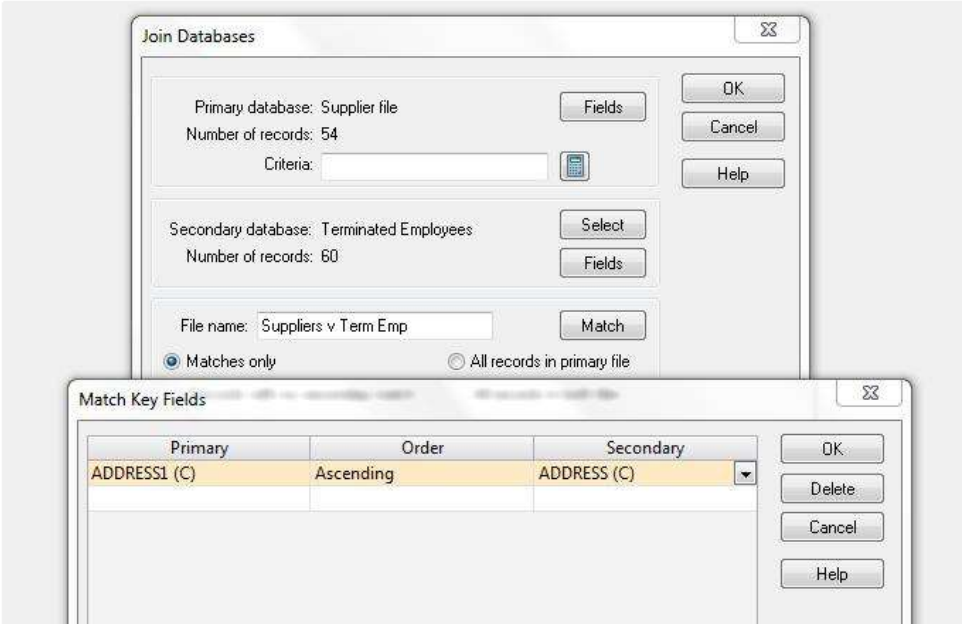


	USER_ID	FIRST_NAME	LAST_NAME	DISABLED	LAST_LOGIN	EMP_NUM	F_NAME	L_NAME	TERM_DATE	
1	e0006	Greg	Smith	FALSE	3/25/2008	e0006	Greg	Smith	3/23/2008	69 Bowhill Stre
2	e0011	George	Jackson	FALSE	10/21/2007	e0011	George	Jackson	9/6/2007	67 Mill Blvd.
3	e0012	Richard	Touchet	FALSE	10/22/2007	e0012	Richard	Touchet	9/5/2007	9600 Possum S
4	e0017	David	Davidson	FALSE	3/5/2008	e0017	David	Davidson	3/5/2007	1301 Clay Stree
5	e0028	Brad	Martin	FALSE	3/25/2008	e0028	Brad	Martin	3/23/2008	6900 Almeda R
6	e0049	Debra	Phillips	FALSE	3/25/2008	e0049	Debra	Fixes	3/19/2008	Berliner Str. 26
7	e9857	Angela	Hainey	FALSE	9/17/2007	e9857	Angela	Hainey	9/15/2007	1100 Ninth Ave

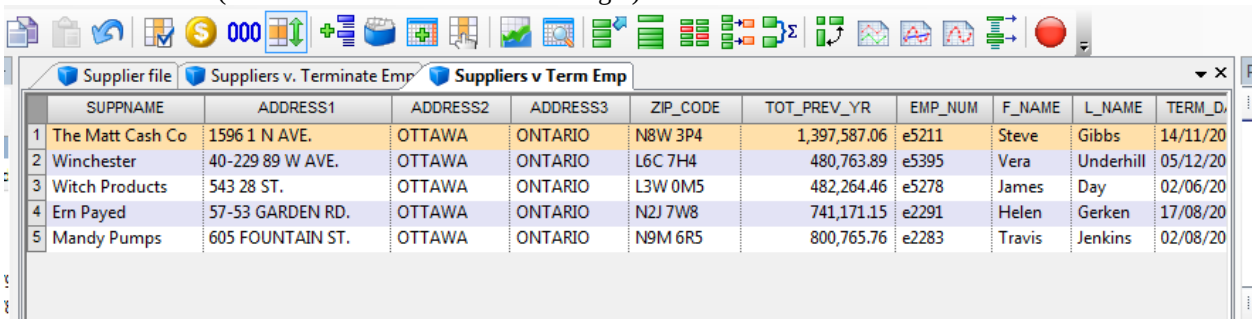
APPENDIX A (Continued)

Objective 2

Use the IMPORT ASSISTANT to import the Supplier File. Use the JOIN function to create a report of suppliers who are also terminated employees. The primary database is the Supplier file, the secondary database is the Terminated Employees extraction file; match criteria should be ADDRESS1 in the Supplier File and ADDRESS in Terminated Employee extraction file (matches only).



Here are the results (does not show all columns to the right):



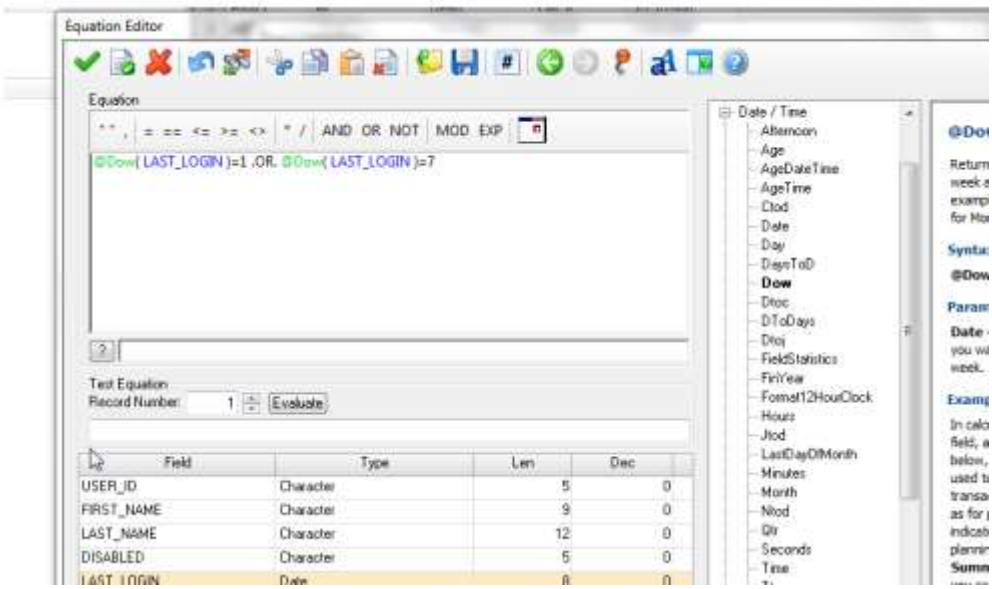
Supplier file | Suppliers v. Terminate Emp | Suppliers v Term Emp

	SUPPNAME	ADDRESS1	ADDRESS2	ADDRESS3	ZIP_CODE	TOT_PREV_YR	EMP_NUM	F_NAME	L_NAME	TERM_D
1	The Matt Cash Co	1596 1 N AVE.	OTTAWA	ONTARIO	N8W 3P4	1,397,587.06	e5211	Steve	Gibbs	14/11/20
2	Winchester	40-229 89 W AVE.	OTTAWA	ONTARIO	L6C 7H4	480,763.89	e5395	Vera	Underhill	05/12/20
3	Witch Products	543 28 ST.	OTTAWA	ONTARIO	L3W 0M5	482,264.46	e5278	James	Day	02/06/20
4	Ern Payed	57-53 GARDEN RD.	OTTAWA	ONTARIO	N2J 7W8	741,171.15	e2291	Helen	Gerken	17/08/20
5	Mandy Pumps	605 FOUNTAIN ST.	OTTAWA	ONTARIO	N9M 6R5	800,765.76	e2283	Travis	Jenkins	02/08/20

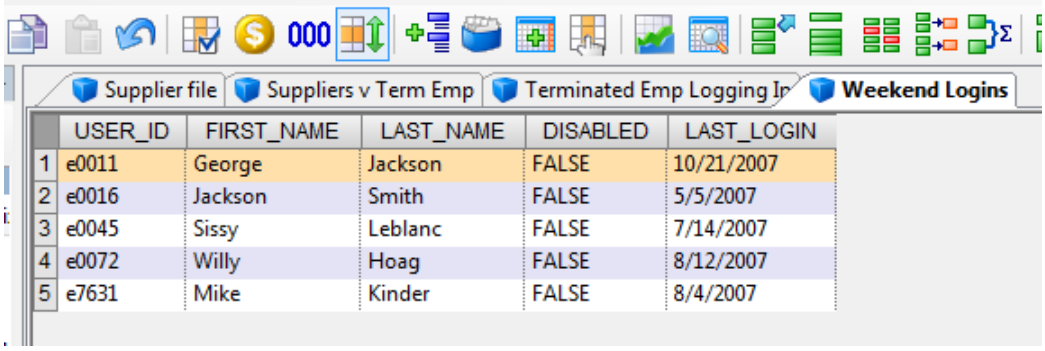
APPENDIX A (continued)

Objective 3

Use a DIRECT EXTRACTION as follows from the Active Directory_Users File to determine log-ins on weekends. Note that the extraction name should be "Weekend Logins". The extraction should be built as indicated below using the DATE/TIME function "dow" (or "day of week"; the software will input it as "@dow"). Be sure to use the "Insert Field" bar rather than try to type in the field name. The numbers "1" and "7" indicate the days of the week: 1 = Sunday, 7 = Saturday.



Here are the results:



	USER_ID	FIRST_NAME	LAST_NAME	DISABLED	LAST_LOGIN
1	e0011	George	Jackson	FALSE	10/21/2007
2	e0016	Jackson	Smith	FALSE	5/5/2007
3	e0045	Sissy	Leblanc	FALSE	7/14/2007
4	e0072	Willy	Hoag	FALSE	8/12/2007
5	e7631	Mike	Kinder	FALSE	8/4/2007

APPENDIX B
Lab Notes for Instructor: Unauthorized Payments Case
(PDF files with results available from author)

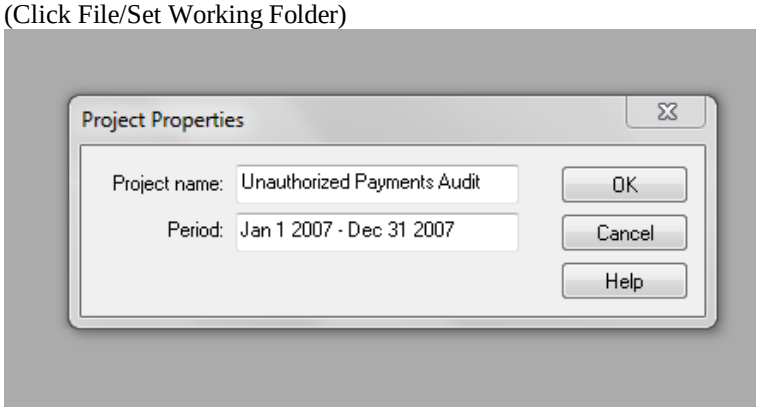
Objectives for Case 2 (unauthorized payments):

1. Checking for sequential invoice numbers (refer to section 3.12)
2. To analyze payments to fictitious vendors (Supplier File, see section 3.15)
3. Checking for vendors with P.O. box addresses, rather than street addresses (Supplier Master File, extract "P.O." "P O" and "PO")
4. Noting payments on Saturday or Sunday
5. Comparing vendor and employee names (merge Supplier Master File and Employee Master File using match keys "L_Name" of employees, SUPPNAME for vendor). Also determine if employees and vendors have same addresses (match keys Employee: Address, Vendor: Address1)
6. Testing for duplicate payments (Accounts Payable, section 3.11)
7. Noting multiple companies with the same address (sort Supplier Master File by address)
8. Noting invoices slightly below the review threshold (Accounts Payable, section 3.9, set threshold)
9. Testing for excessive hours worked (need Payroll Most Current Period, extract hours > 40)
10. Testing for salary payments to non-existent or terminated employees (Payroll Most Current Period and Master Employee File—cleaned up with only current employees, section 3.15)

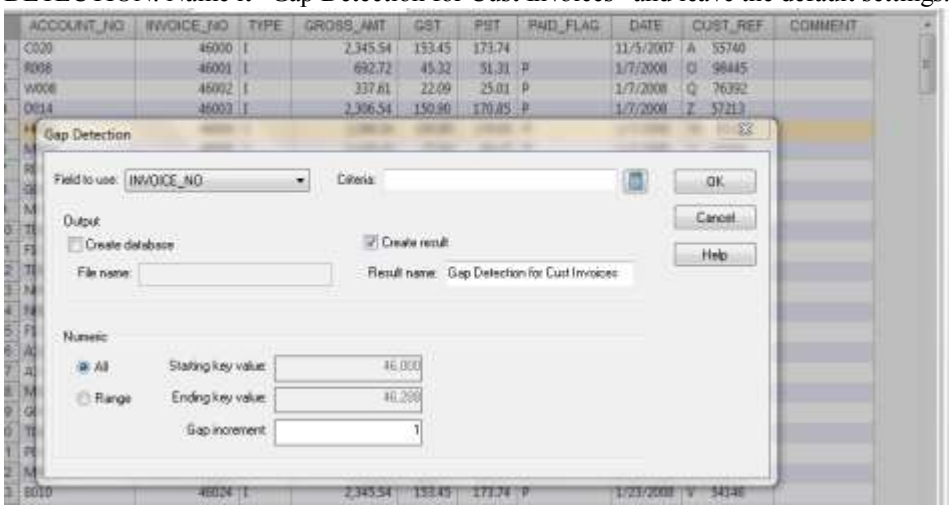
NOTE: The students must turn in printouts of their results (including history file), the properly filled out/initialed audit program/audit procedures sheet, along with an audit report addressed to the instructor interpreting their findings

APPENDIX B (continued)

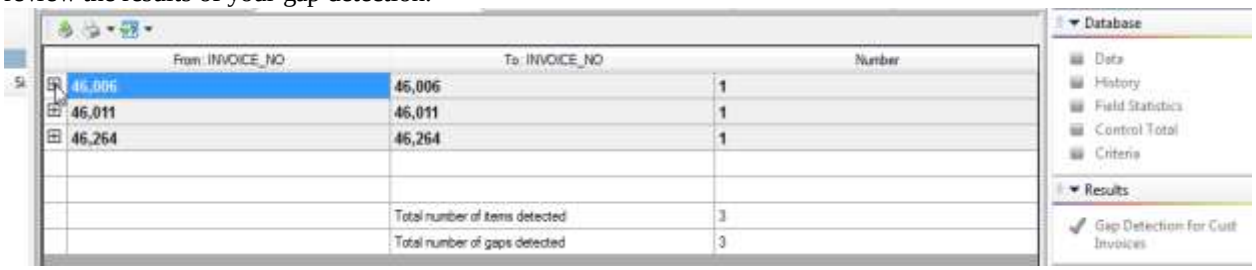
Objective 1
Set the Working Folder to "Unauthorized Payments Audit" with the dates "Jan 1 2007 – Dec 31 2007" (Click File/Set Working Folder)



Import the Customer Invoices File. Right click on the data, select FIELD MANIPULATION. Change the "Invoice" field to "numeric". Select the GAP DETECTION icon on the tool bar or select ANALYSIS/GAP DETECTION. Name it "Gap Detection for Cust Invoices" and leave the default settings.



The report will show up initially in the window. To see which invoice numbers are missing, click on the "+". You can return to the data by clicking on "Data" in the properties bar on the right hand side of the screen. The "Results" section of the properties bar on the right hand side of the screen can be selected to review the results of your gap detection.

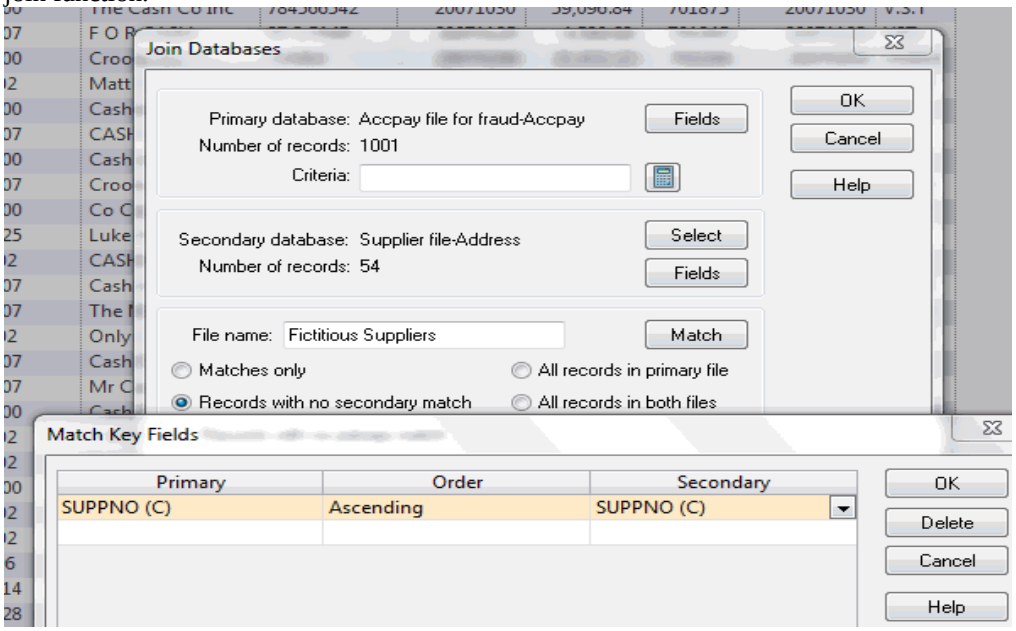


You can also double-click on the "Invoice" column to have the records automatically put in numeric order (ascending). Click on the right side of the column heading and they will be sorted in descending order.

APPENIDX B (Continued)

Objective 2

Import the Accpay File for Fraud File. Join the ACCPAY FILE FOR FRAUD (primary database) with the Supplier File (secondary database). Call this joined file "Fictitious Suppliers". Match on "SUPPNO" for both files and use the "no secondary match" choice when selecting your match preference to perform the join function.



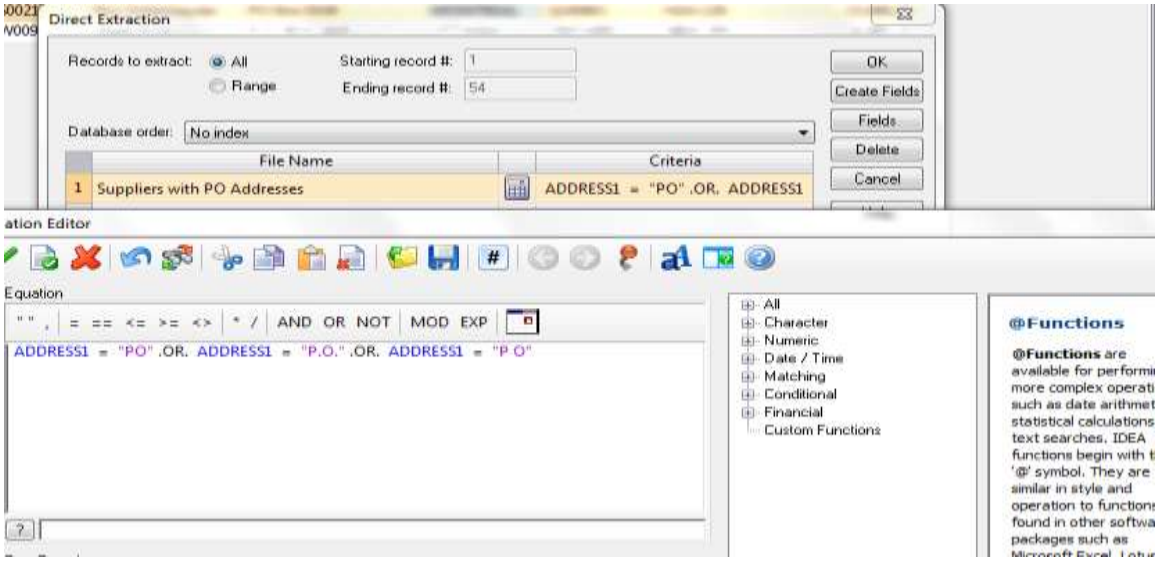
The results should look like this.

	SUPPNO	PAYEE	INVOICE	INV_DATE	AMOUNT	CHECK	PAY_DATE	AUTH
1	M100	M Cash Inc	UP-76409	20071001	75,000.00	701774	20071008	HMV
2	M100	The Cash Co Inc	784566542	20071030	59,096.84	701875	20071030	V.S.T
3	M100	Crooks Inc	PI7683	20070208	21,632.22	701046	20070209	H.M.V.
4	M100	Cashonly	UY-9371	20070426	2,792.72	701270	20070430	HV
5	M100	Cash Inc	CS - 717 -97	20070913	75,000.00	701728	20070914	VST
6	M100	Co Cash Inc	T5352	20071017	75,000.00	701849	20071019	V.S.T
7	M100	Cash Back Inc	CB3456	20071117	2,922.78	701927	20071118	H.M.V.
8	M100	Matt Cash & Co	In879-97	20070624	190,071.38	701443	20070628	HMV

APPENDIX B (Continued)

Objective 3

Do a DIRECT EXTRACTION on the Supplier File to find all suppliers with PO/P.O. addresses, rather than street addresses (ADDRESS1 = "PO" .OR. ADDRESS1 = "P.O." .OR. ADDRESS1= "P O").



Here are the results:

Accpay | Customer invoices-Acc_rec | Payroll most current period-Sheet1 | Fictitious Suppliers | Supplier file | **Suppliers with PO Addresses**

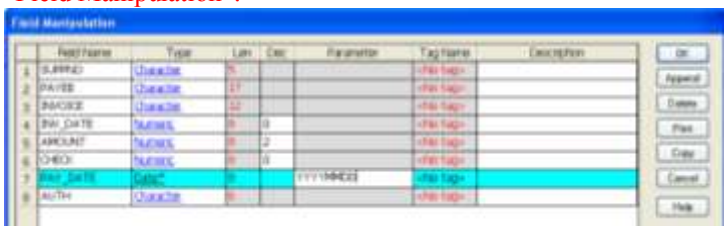
	SUPPNO	SUPPNAME	ADDRESS1	ADDRESS2	ADDRESS3	ZIP_CODE	TOT_PREV_YR
1	J0016	Jackson Smith	PO BOX 12	EDMONTON	ALBERTA	T5J 7M1	509,816.54
2	L555	Anita Lozano	PO BOX 153-89	OTTAWA	ONTARIO	P0Z 5K8	4,836.21
3	M129	Allison Milo	PO Drawer 13	TORONTO	ONTARIO	M1T 7S4	1,258.47
4	S0021	Roy Schexnayder	PO Box 5538	MONTREAL	QUEBEC	H2A 1Z6	15,486.25
5	W009	Wash N Go	P.O. BOX 1820	OTTAWA	ONTARIO	N8W 3P4	14,985.23

APPENDIX B (continued)

Objective 4

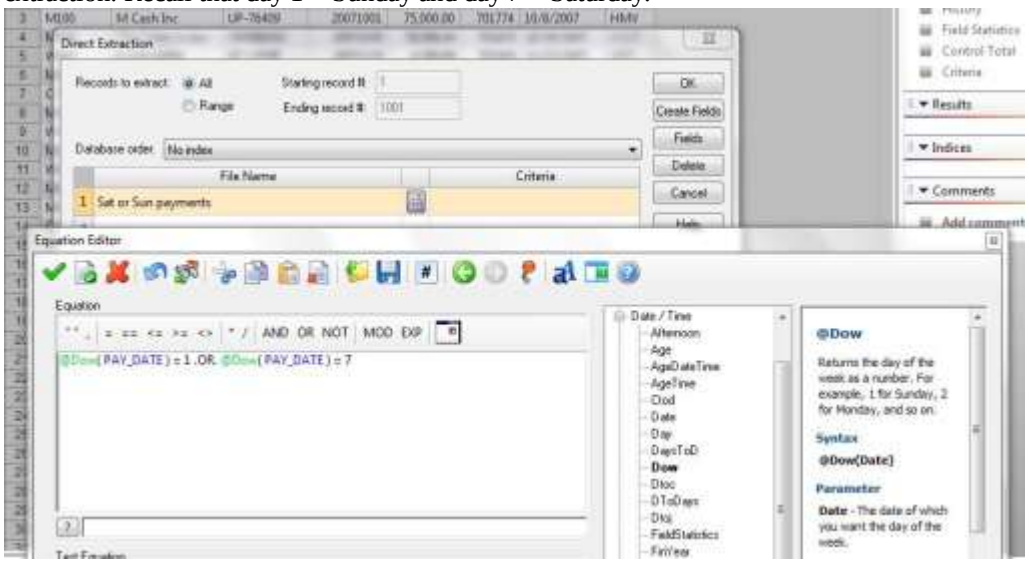
Use the DIRECT EXTRACTION described in section 3.10.4 of the workbook to find all invoices paid on Saturday or Sunday. (Use AccPay for Fraud file)

Note: PAY_DATE should be changed its format to DATE as below by right clicking on data and choosing "Field Manipulation":



This can be done by right clicking on the data, selecting "Field Manipulation" and changing the PAY_DATE" to DATE format with "YYYYMMDD" as the parameter.

Call your extraction "Sat or Sun payments" and use the "dow" DATE/TIME function when building the extraction. Recall that day 1 = Sunday and day 7 = Saturday.



Here is a partial list of the results (there are 42 weekend payments):

Supplier file | Suppliers v Term Emp | Terminated Emp Logging In | Weekend Login | Sat or Sun payments

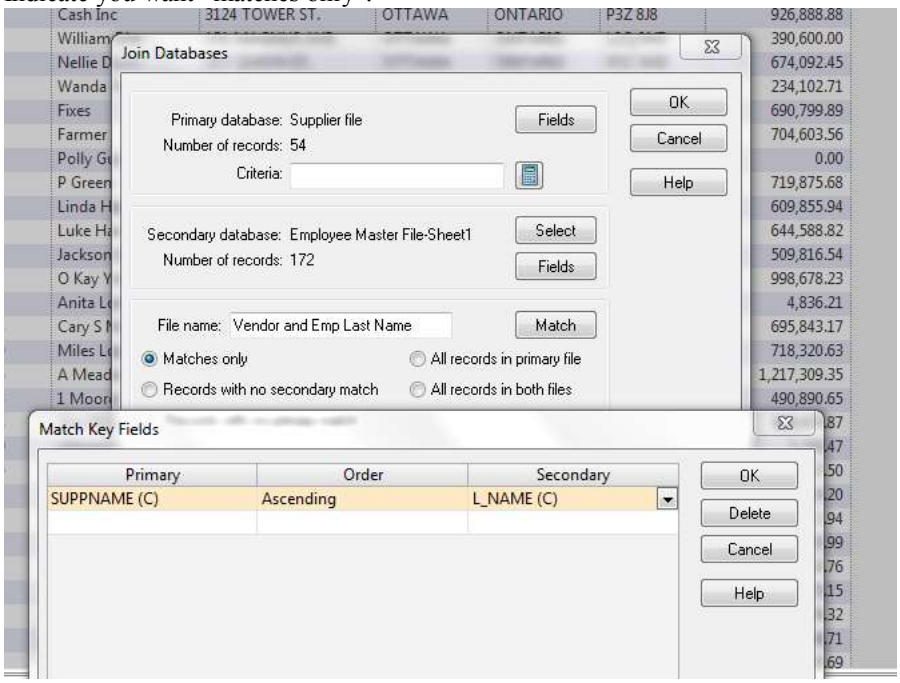
	SUPPNO	PAYEE	INVOICE	INV_DATE	AMOUNT	CHECK	PAY_DATE	AUTH
1	W007	Matt Cash Co	879-97	20070407	83,516.79	701218	4/7/2007	V.S.T
2	W007	I M A Crook	97 2089.29J	20070609	14,432.19	701391	6/10/2007	HV
3	C202	Matt Cash	51726	20070304	6,242.74	701117	3/4/2007	HMV
4	M025	Luke Hair	51498	20070208	50,067.31	701027	2/10/2007	HV
5	M100	Cash Back Inc	CB3456	20071117	2,922.78	701927	11/18/2007	H.M.V.
6	M014	Kurt N Upp	123489	20070411	15,906.20	701294	5/6/2007	VMH
7	F130	Farmer	14653	20070606	177.41	701451	7/1/2007	CW
8	W007	Trevor Wills	TJ9775	20070910	44,035.95	701789	10/6/2007	HMV
9	N001	Microcomputers	5900MCC	20071029	3,038.95	701941	11/24/2007	HMV
10	B008	A Meadow	117 - 2411	20071031	97,454.56	701944	11/25/2007	HMV
11	M025	Luke Hair	3012 BNA	20071114	12,400.19	701985	12/8/2007	H.M.V.
12	M025	Luke Hair	51505	20070124	79,500.00	701073	2/17/2007	H.M.V.
13	W011	Witch Products	25G	20070207	21,650.08	701118	3/4/2007	HMV
14	R007	Philip Upp Garage	1374/21	20070307	2,174.63	701201	4/1/2007	HMV
15	P009	P Green	566743T	20070320	67,059.93	701236	4/15/2007	HMV
16	R008	Phillippa Pail	97/1267/A	20070325	28,842.89	701250	4/21/2007	WJT
17	M020	Luke Hair	2879 BNA	20070416	47,092.73	701314	5/13/2007	HMV
18	C202	Cary S Matic	CS - 607 -97	20070417	19,182.60	701317	5/13/2007	HMV
19	P007	Nellie Dunn	000517CJW	20070429	16.80	701352	5/27/2007	H.M.V.
20	T007	Round Table	BUR1366-G	20070627	260.06	701519	7/22/2007	HMV
21	H014	Honor Toze	659898	20070723	21,131.83	701644	8/19/2007	HMV
22	F130	1 Moore	IN 6508 97	20070801	9,337.45	701676	8/26/2007	HMV
23	B010	Carter Bout	971061A	20070909	30,536.55	701787	10/6/2007	HMV
24	T006	Ronnie Biggs	7899500	20070917	78,605.73	701813	10/14/2007	HMV
25	F123	Edward Zoff	99799ABC	20070115	2,713.16	701052	1/13/2007	HMV
26	Z001	Miles Long	FR-972 42	20070127	3,649.83	701094	2/24/2007	HMV
27	F130	1 Moore	IN 6446 97	20070127	24,163.78	701096	2/24/2007	CW
28	M025	L Hair	232 A2Z	20070212	5,033.83	701146	3/11/2007	HMV
29	F130	Farmer	14677	20070701	8,384.50	701569	7/29/2007	HMV
30	P010	P Green	566817T	20070702	19,647.86	701571	7/29/2007	HMV
31	F128	Edward Zoff	99833ABC	20070902	2,546.59	701760	9/30/2007	H.M.V.

APPENDIX B (Continued)

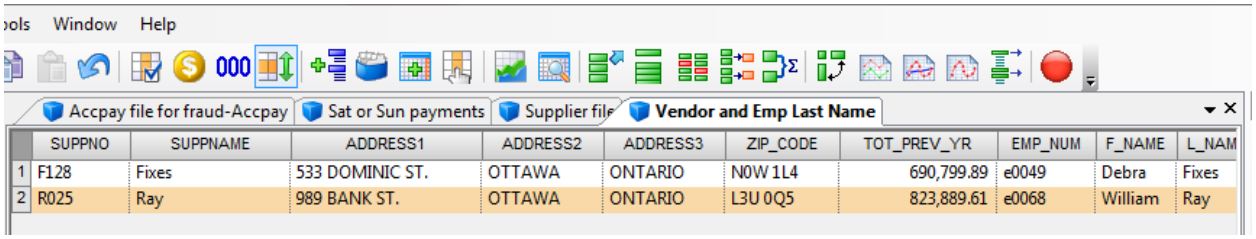
Objective 5

The Supplier file should be the active file.

Use the JOIN DATABASES function to determine employees and vendors with the same names. The Supplier file is the primary file and the Employee Master File is the secondary. Call this join "Vendor and Emp Last Name". (Match criteria should be "SUPP_NAME" of supplier and "L_NAME" of employees). Indicate you want "matches only".



The results look like this (note that Debra Fixes is a terminated employee)

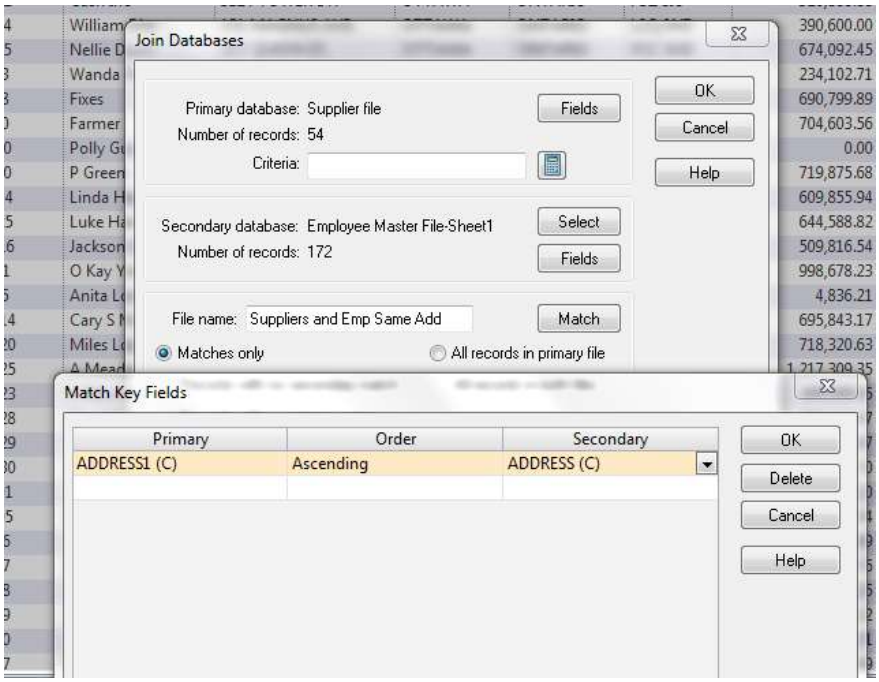


	SUPPNO	SUPPNAME	ADDRESS1	ADDRESS2	ADDRESS3	ZIP_CODE	TOT_PREV_YR	EMP_NUM	F_NAME	L_NAM
1	F128	Fixes	533 DOMINIC ST.	OTTAWA	ONTARIO	N0W 1L4	690,799.89	e0049	Debra	Fixes
2	R025	Ray	989 BANK ST.	OTTAWA	ONTARIO	L3U 0Q5	823,889.61	e0068	William	Ray

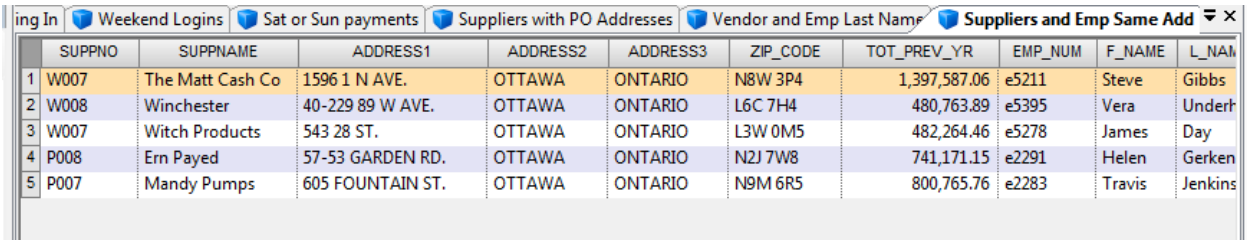
APPENDIX B (Continued)

Objective 5 (continued):

To determine if any of the employees and vendors have the same addresses, perform an join databases of Supplier File (primary database) and Employee Master File (secondary database). Match on ADDRESS1 (Supplier File) and ADDRESS (Employee Master File), matches only. Name the file "Suppliers and Emp Same Address."



Here are the results (missing some of the right-most columns):



ing In | Weekend Logins | Sat or Sun payments | Suppliers with PO Addresses | Vendor and Emp Last Name | **Suppliers and Emp Same Add**

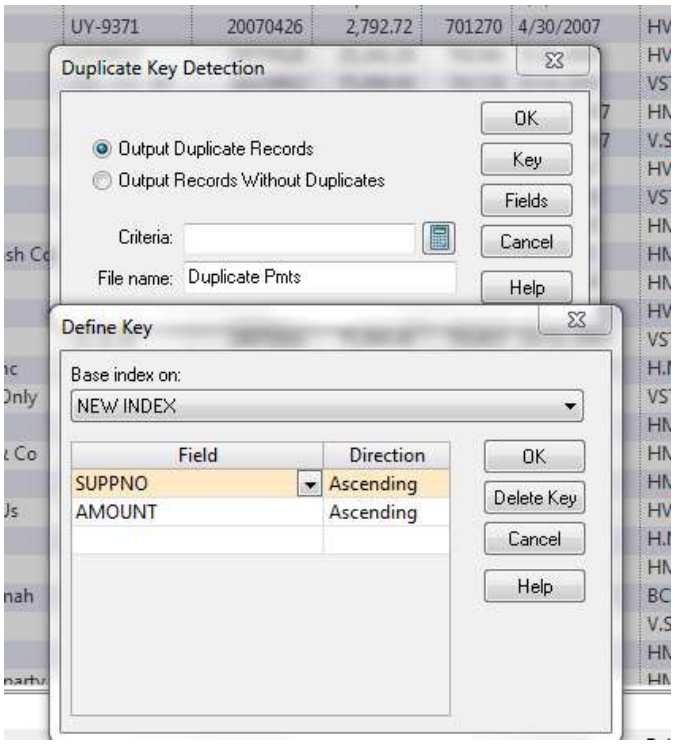
	SUPPNO	SUPPNAME	ADDRESS1	ADDRESS2	ADDRESS3	ZIP_CODE	TOT_PREV_YR	EMP_NUM	F_NAME	L_NAI
1	W007	The Matt Cash Co	1596 1 N AVE.	OTTAWA	ONTARIO	N8W 3P4	1,397,587.06	e5211	Steve	Gibbs
2	W008	Winchester	40-229 89 W AVE.	OTTAWA	ONTARIO	L6C 7H4	480,763.89	e5395	Vera	Underh
3	W007	Witch Products	543 28 ST.	OTTAWA	ONTARIO	L3W 0M5	482,264.46	e5278	James	Day
4	P008	Ern Payed	57-53 GARDEN RD.	OTTAWA	ONTARIO	N2J 7W8	741,171.15	e2291	Helen	Gerken
5	P007	Mandy Pumps	605 FOUNTAIN ST.	OTTAWA	ONTARIO	N9M 6R5	800,765.76	e2283	Travis	Jenkins

APPENDIX B (continued)

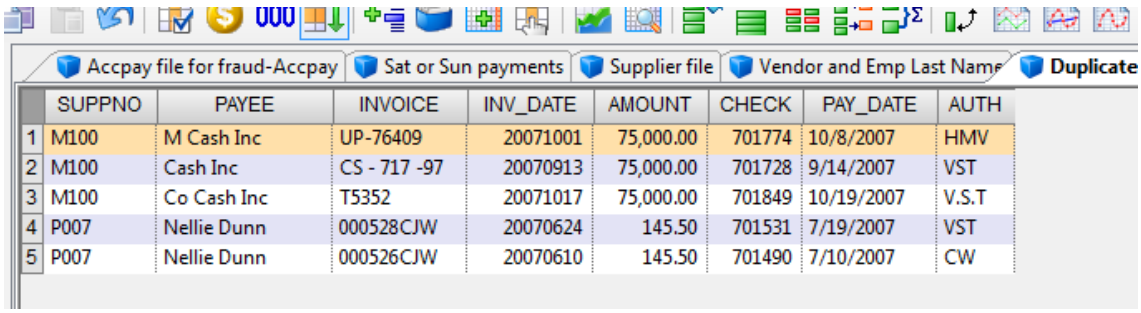
Objective 6

Accpay for Fraud file should be the active file.

Use the ANALYSIS/DUPLICATE KEY/DETECTION (or use duplicate key detection icon on toolbar) to identify duplicate payments. Call this analysis "Duplicate Pmts". Click "Key" and base index on "SUPPNO" and "AMOUNT". Click OK/OK to produce the output of duplicate records.



Here are the results:



	SUPPNO	PAYEE	INVOICE	INV_DATE	AMOUNT	CHECK	PAY_DATE	AUTH
1	M100	M Cash Inc	UP-76409	20071001	75,000.00	701774	10/8/2007	HMV
2	M100	Cash Inc	CS - 717 -97	20070913	75,000.00	701728	9/14/2007	VST
3	M100	Co Cash Inc	T5352	20071017	75,000.00	701849	10/19/2007	V.S.T
4	P007	Nellie Dunn	000528CJW	20070624	145.50	701531	7/19/2007	VST
5	P007	Nellie Dunn	000526CJW	20070610	145.50	701490	7/10/2007	CW

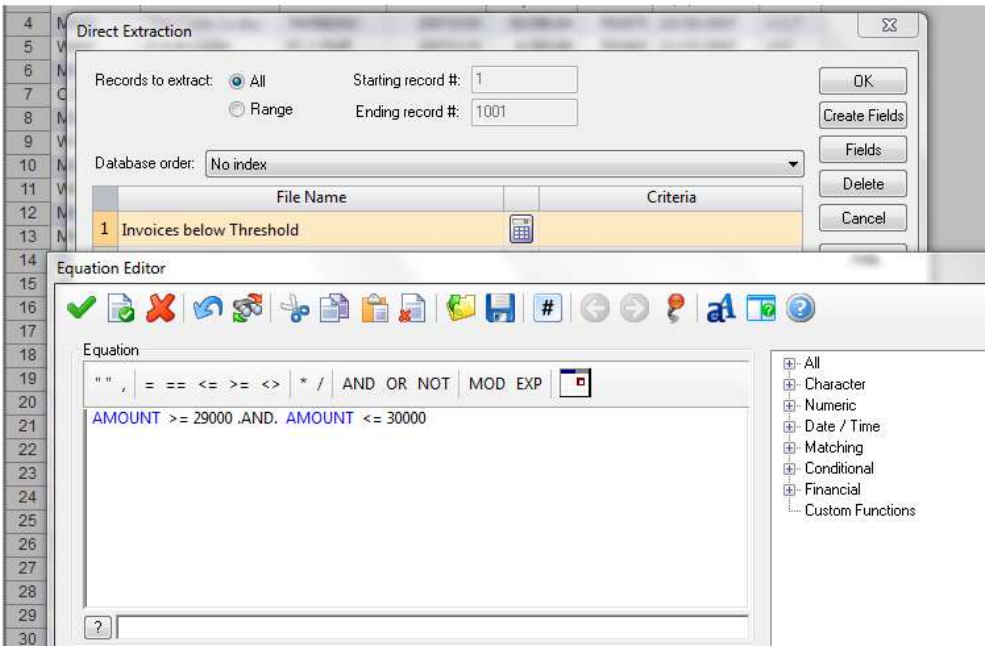
APPENDIX B (continued)

Objective 7
The Supplier File should be the active file

Use the DATA/SORT function to sort suppliers by addresses (ADDRESS1) OR double click on the column you want to sort.

Objective 8
The Accpay File for Fraud is the active file.

Use the DIRECT EXTRACTION function to extract invoice amounts between $29000 and $30000 (which is the threshold for a higher level review for payment). Call this extraction "Invoices below Threshold" and create the extraction as shown below:



Here are the results:

Accpay file for fraud-Accpay | Sat or Sun payments | Supplier file | **Invoices below Threshold**

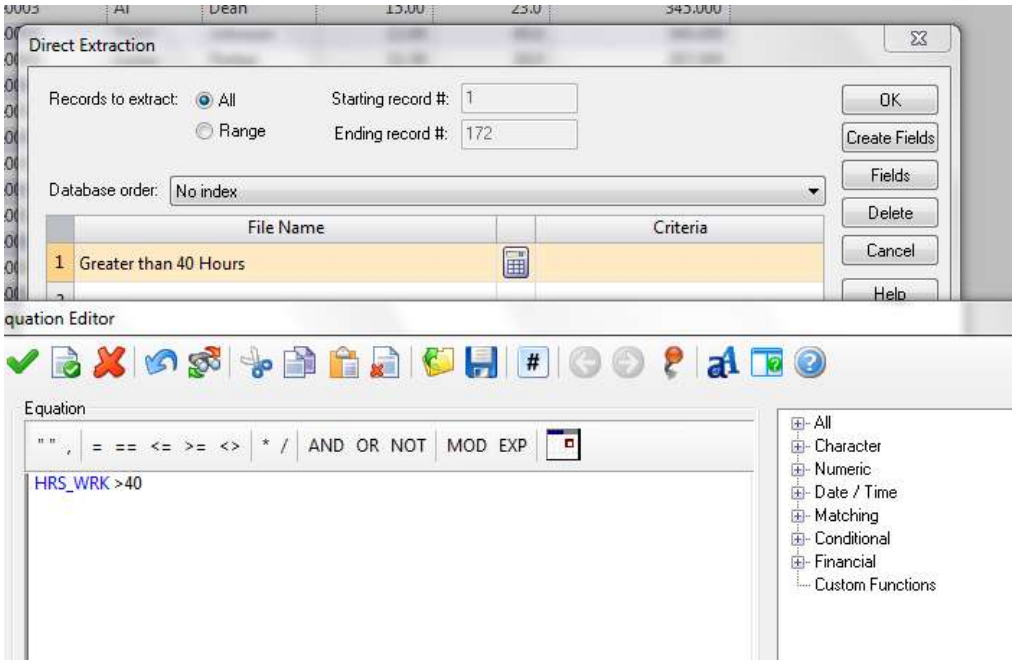
	SUPPNO	PAYEE	INVOICE	INV_DATE	AMOUNT	CHECK	PAY_DATE	AUTH
1	P009	P Green	566701T	20070115	29,990.31	701058	2/14/2007	BC
2	T009	Truckstop	97 2061.29J	20070603	29,339.05	701442	6/28/2007	WJT
3	Z001	Miles Long	FR-985 62	20070408	29,232.42	701288	5/4/2007	HV
4	F123	Denise Bent	81373	20070923	29,188.20	701832	10/19/2007	HMV
5	R025	Ray	55009/10	20071001	29,616.37	701866	10/29/2007	WJT
6	F128	Ern Payed	82 162 1	20070728	29,527.27	701684	8/23/2007	WJT
7	W011	Witch Products	21G	20070113	29,033.80	701047	Error	HMV
8	F123	Dick Tate	35266DUF	20070624	29,982.12	701522	7/23/2007	CW
9	R020	Polly Gunn	L-1321/68	20070630	29,626.00	701540	7/26/2007	HMV
10	W020	Witch Products	54G	20070918	29,463.41	701826	10/16/2007	BC
11	K001	Jackie Tupp	917341	20070131	29,976.77	701109	3/1/2007	VMH
12	W020	Witch Products	39G	20070530	29,691.39	701444	6/28/2007	WJT
13	R008	Penny Cillin	100255	20071007	29,686.09	701886	11/5/2007	V.S.T
14	D025	Chimps Teaparty	147939CTR	20071016	29,415.50	701923	11/14/2007	HV

APPENDIX B (Continued)

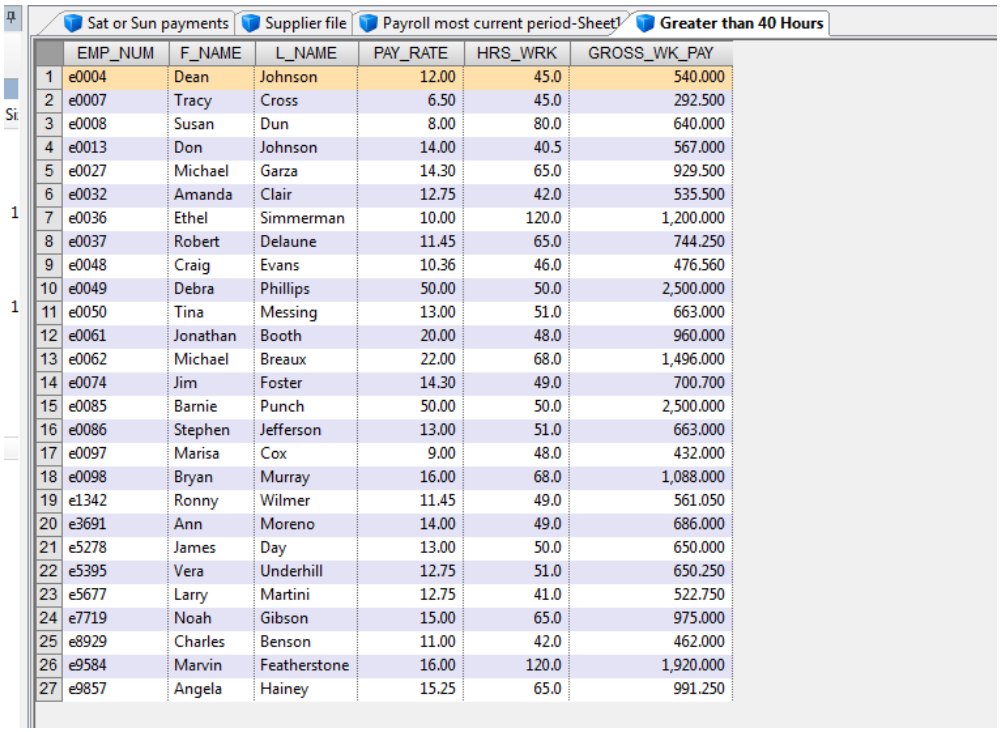
Objective 9

Use the IMPORT ASSISTANT to import the Payroll Most Current Period file.

Perform a DIRECT EXTRACTION to create a report of all employees who worked more than 40 hours last week. Call this extraction "Greater than 40 Hours" and create the extraction as shown below:



Here are the results:



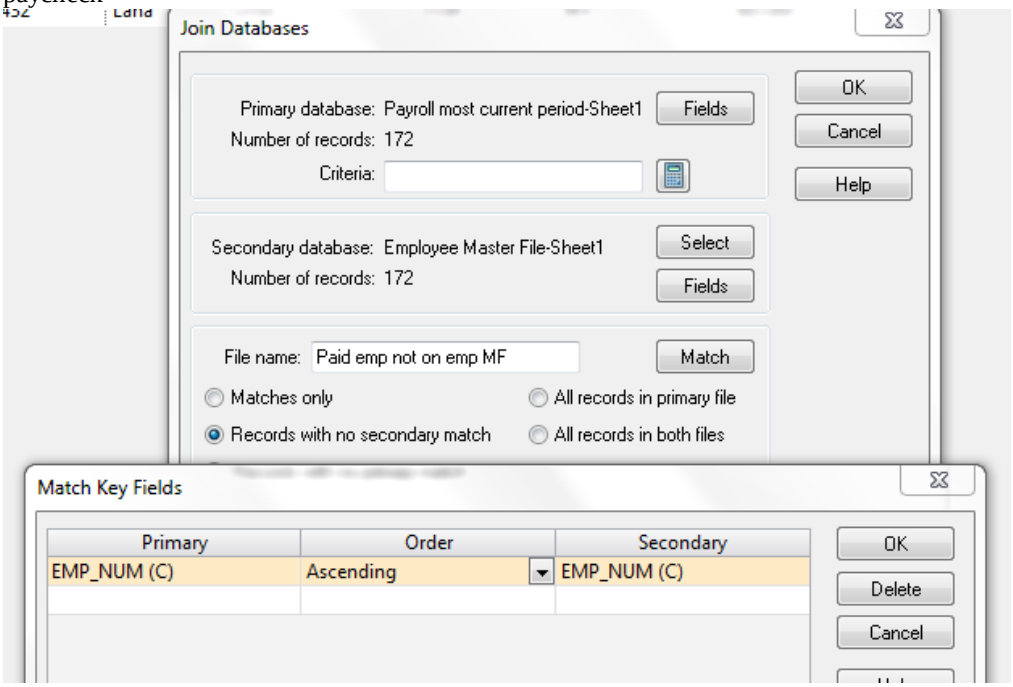
Sat or Sun payments | Supplier file | Payroll most current period-Sheet1 | **Greater than 40 Hours**

	EMP_NUM	F_NAME	L_NAME	PAY_RATE	HRS_WRK	GROSS_WK_PAY
1	e0004	Dean	Johnson	12.00	45.0	540.000
2	e0007	Tracy	Cross	6.50	45.0	292.500
3	e0008	Susan	Dun	8.00	80.0	640.000
4	e0013	Don	Johnson	14.00	40.5	567.000
5	e0027	Michael	Garza	14.30	65.0	929.500
6	e0032	Amanda	Clair	12.75	42.0	535.500
7	e0036	Ethel	Simmerman	10.00	120.0	1,200.000
8	e0037	Robert	Delaune	11.45	65.0	744.250
9	e0048	Craig	Evans	10.36	46.0	476.560
10	e0049	Debra	Phillips	50.00	50.0	2,500.000
11	e0050	Tina	Messing	13.00	51.0	663.000
12	e0061	Jonathan	Booth	20.00	48.0	960.000
13	e0062	Michael	Breaux	22.00	68.0	1,496.000
14	e0074	Jim	Foster	14.30	49.0	700.700
15	e0085	Barnie	Punch	50.00	50.0	2,500.000
16	e0086	Stephen	Jefferson	13.00	51.0	663.000
17	e0097	Marisa	Cox	9.00	48.0	432.000
18	e0098	Bryan	Murray	16.00	68.0	1,088.000
19	e1342	Ronny	Wilmer	11.45	49.0	561.050
20	e3691	Ann	Moreno	14.00	49.0	686.000
21	e5278	James	Day	13.00	50.0	650.000
22	e5395	Vera	Underhill	12.75	51.0	650.250
23	e5677	Larry	Martini	12.75	41.0	522.750
24	e7719	Noah	Gibson	15.00	65.0	975.000
25	e8929	Charles	Benson	11.00	42.0	462.000
26	e9584	Marvin	Featherstone	16.00	120.0	1,920.000
27	e9857	Angela	Hainey	15.25	65.0	991.250

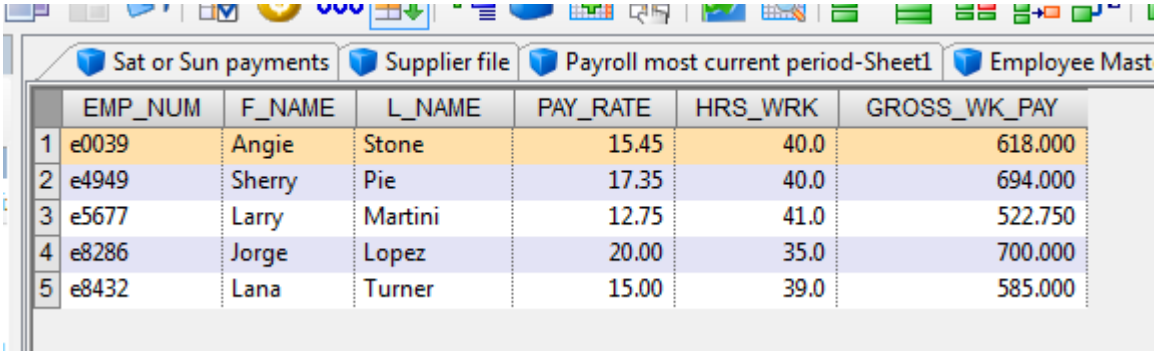
APPENDIX B (continued)

Objective 10
Payroll Most Current Period and the Employee Master Files should be the active files.

To determine the non-existent/terminated employees getting paid, do a "join databases" and get only those payees not listed in the current employee database (note that this will include terminated employees. This can be done by joining Payroll Most Current Period (primary database) and Employee Master File (secondary database). Call this "Paid emp not on emp MF". Perform the join choosing "records with no secondary match" and match on EMP_NO to determine terminated/non-existent employees who received a paycheck

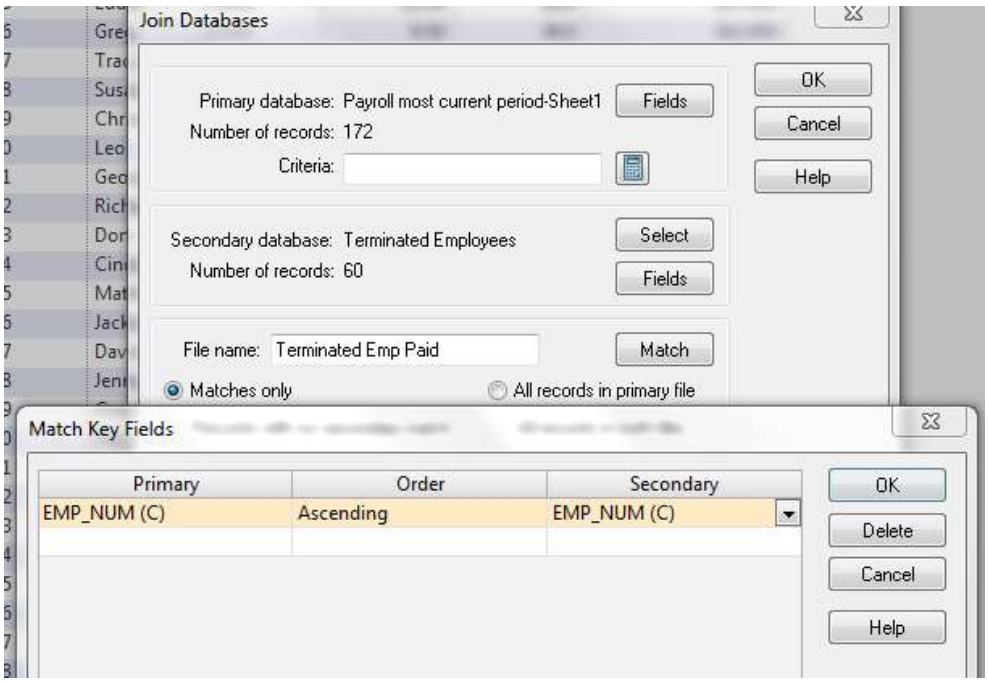


Here are the results:



	EMP_NUM	F_NAME	L_NAME	PAY_RATE	HRS_WRK	GROSS_WK_PAY
1	e0039	Angie	Stone	15.45	40.0	618.000
2	e4949	Sherry	Pie	17.35	40.0	694.000
3	e5677	Larry	Martini	12.75	41.0	522.750
4	e8286	Jorge	Lopez	20.00	35.0	700.000
5	e8432	Lana	Turner	15.00	39.0	585.000

Terminated Employees and Payroll Most Current Period should be the active files. Perform a JOIN DATABASES to determine terminated employees who received a paycheck in the current period (see illustration below), by setting Payroll Most Current Period as primary, Terminated Employees as secondary and choosing "Matches Only". Name this database "Terminated Emp Paid".



This results in the terminated employees who received a paycheck for the current period (all 60 of the terminated employees were paid). You would then go and compare the termination date with the date of the paycheck (e.g., it might have been their final paycheck). You could do an extraction asking for the employees whose termination date was less than the payroll date (latter is not provided in this example). Then all that would be left would be the terminated employees who continue to receive paychecks (like the guy in "Office Space" who received paychecks for two years after he was laid off!)

APPENDIX B (continued)

If you were interested in only the non-existent employees who were paid, you can do a join databases using your previous extraction ("non-existent or terminated employees") as the primary database, and the Terminated Employees extraction file as the secondary database. Match on "records with no secondary match" on EMP_NUM, to indicate you only want those in the non-existent or terminated employees that are not in the terminated employee list.