

Scenario

Management in a large brokerage firm was notified by a whistle blower that several of the brokers were electronically providing insider trading information to their friends. Management contracted with an external Computer Forensics company to work with its IT department to covertly look into the allegation. The computers of the brokers were examined. Incriminating emails concerning stock sales and pending mergers were discovered. The brokerage firm's attorney reviewed the results and turned over the pertinent evidence to the local district attorney. The brokers were subsequently indicted for violation of SEC rules and regulations and a trial date was set by the court. All the incriminating evidence was digital which was recovered from computers. The Computer Forensics examiner who examined the computers was called to testify in court regarding his analysis. He is being cross-examined by one of the broker's attorneys:

Q: "Can you describe to the court how you became involved in this case?"

A: "Our company was contracted to work with the IT department. I was assigned to examine the computers of several of the brokers. They were suspected of illegal insider trading. I was to search for anything that would substantiate this claim."

Q: "Can you describe to the court how you went about conducting this examination?"

A: "I brought my forensic computer on-site. Using a write-blocker, I imaged the hard drives of the broker's computers onto my portable 1.5 TB hard drive array. I also imaged their user accounts from their SAN. I returned to my own company and began the examination."

"I created an archive of the images and exported them to DVD's. After that, I opened the images and recovered some deleted folders. The images were searched with several forensic tools, using specific keywords pertaining to the brokers and their friends.

"From the hard drive images I found emails containing information related to stock sales, pending mergers, and price quotations. They all had non-departmental addresses and were in unallocated areas on the hard drives."

"From the user accounts, I found similar emails with non-departmental addresses. A couple of the emails also contained text stating that a percentage of the profits should go to the brokers for providing the insider information. After finding this information, I exported the digital data to CD's, wrote up a report and turned both over to the client's legal department."

Q: "How long have you been employed by your company?"

A: “About three years.”

Q: “Could you describe in more detail to the court your education and training background?”

A: “I have a degree in Computer Science. Prior to my present job, I worked as a System Administrator at the local school board for about four years. I was responsible for maintaining the computer network.

“As part of my duties, I often had to recover data that teachers deleted from their computers.”

“I’ve attended networking training classes provided by both software and hardware vendors and am certified as a CISSP. Additionally, I am certified in Network+, and A+ and am awaiting certification as an MCSE. I’ve attended introductory and intermediate level Computer Forensic courses provided by the vendor of the imaging software we use.”

Q: “Did any of your certification courses contain specific information about Computer Forensic analysis?”

A: “Not specifically. Computer Forensics does not really involve anything more than examining computer hard drives to extract or find information.”

Q: “Can you describe your specific training in Computer Forensic analysis that qualifies you as an expert to have performed this examination?”

A: “The introductory course covered how computers work, basic file systems, and how to use the imaging software. The intermediate course covered how to recover deleted folders and partitions, advanced keyword searches, how to recover artifacts and more detailed ways to use the forensic software. I received a certificate of completion for both courses.”

Q: “Before you began to do Computer Forensic analysis in your current job, did you take a ‘Competency Test’?”

A: “I am not sure what you mean by ‘taking a Competency Test’.”

Q: “A Competency Test is a test used to evaluate an examiners ability to perform work in a technical area prior to performing independent analysis.”

“The question relates to whether or not you were given some media to analyze, such as a floppy disk or a hard drive containing known data, to evaluate your technical skills prior to working cases.”

A: “No one needed to evaluate my technical abilities. I have a Computer Science degree, a number of certifications, and attended two computer Forensics training courses.”

Q: “Do you undergo annual Proficiency Testing?”

A: “I am not familiar with the terminology.”

Q: “I’ll explain. Proficiency Testing is a reliable method of verifying that a laboratory’s technical procedures are valid and that the quality of each examiner’s work is being maintained. At the time the examiner takes a proficiency test, he is unaware of the results.”

“Were you ‘Proficiency Tested’ at any time during the three years you have been in your current job?”

A: “No I was not. However, I would like to state for the record that I do not believe I need to take a Proficiency Test because I have a degree and many certifications and know how to do computer analysis.”

Q: “The procedures that you previously described to image data and examine the email accounts, are they written down and documented?”

A: “No. Nor do they need to be since they are simple and straight-forward.”

Q: “Have the procedures been ‘Verified’ or ‘Validated’ by you or someone else in your company?”

A: “I do not know what those terms mean.”

Q: “Verification and Validation are analytical processes to establish the reliability of a procedure prior to using the procedure in casework. Have you or someone else ‘verified’ or ‘validated’ your procedures?”

A: “I have not and no one else in the company has done so. Let me also say that they do not need to be since they are common procedures used by many examiners.”

Q: “What Standards and Controls did you use during the examinations you performed?”

A: “I am not sure what you mean by those terms.”

Q: “Let me explain their meaning and purpose. A Standard is ‘a prepared sample that has known properties that is used as a control during forensic analyses’.”

“A Control is ‘an appropriate standard used when testing physical evidence that is designed to verify that a procedure is working correctly and the results are valid’.”

“Standards and Controls must be used when analyzing physical evidence as a means to demonstrate that scientific principles and quality assurance practices were followed.”

“Their use ensures that the methods, procedures, and instrumentation are functioning correctly, and that the results obtained are accurate, reliable, and repeatable.”

“I’ll ask the question again. What Standards and Controls did you use to ensure that your write-blocker and software tools were working correctly?”

A: “None.”

Q: “Why not?”

A: “I’ve never heard of having to use Standards and Controls when examining digital evidence. Now that I think about it, I am not sure that they are needed since the write blocker and the imaging software was tested by the vendors before we purchased them. That should be more than sufficient to know that they work properly.”

Q: “Do you know if the software you used in this analysis was flawed or contained any ‘bugs’?”

A: “I am not aware of any.”

Q: “How do you update your software?”

A: “My forensic computer is connected to our internal network which is connected to the Internet. On several occasions, I have gone to the vendor web sites and download available updates.”

Q: “After you download a software update, do you test it in any way before you use it in analysis?”

A: “No. Why would I need to? Updates of software either fix problems associated with the previous version or provide enhanced capabilities. The vendor would already have tested it before they made it available for download to be sure that it worked correctly.”

Q: “Where did you perform this analysis?”

A: “In the Computer Forensics examination area which is located in our headquarters building.”

Q: “How many people have access to that area?”

A: “All the other examiners and department members.”

Q: “Before you turned the results of your analysis over to the legal counsel, did anyone ‘Technically Review’ your analytical notes?”

A: “No.”

Q: “Why not?”

A: “As I previously testified, I know how to perform this type of analysis. So, there would be no need for anyone else to review what I did in this case.”

Q: “One last question. Is your Computer Forensics unit ‘Accredited’?”

A: “All the examiners have certifications of some type, but I am not sure what you mean by ‘Accredited’.”