Computer Forensic: The Choice between Certified and Non-Certified Personal

Lt. Gary R. Ellsworth

Abstract

Ever since the beginning of the digital age, law enforcement agencies have been behind the curve when it comes to digital forensic. When personal computers started on the scene, law enforcement agencies have always been reactive in the approach to solving crime dealing with digital evidence. Each agency has to determine how to deal with the recovery of digital evidence and storage. Are they going to send out the digital media or process at their forensic lab. Is the examiner going to be a civilian or a certified law enforcement person, how much money will be submitted into this new unit and what will be the results? Many agencies are facing this dilemma. Research has shown that the massive amount of information media that is available is too much for just one person. The way a unit is established will determine its course and future. This paper will ~~only~~ assist in providing insight for that decision.

Introduction

This research paper is looking into what is needed to start up a computer forensic unit for a small to medium law enforcement agency. When this author was involved with starting a computer forensic unit, there was little information on the cost, whom should be selected to staff the unit and what training would be needed to successfully complete a case. Most articles and research deals with what computer forensic, also known as digital forensic, is but never really focuses on the necessary elements.

In an article from Craig D. Ball (2006), the author stated that you need “The Seven E’s.” Mr. Ball described them as:

1. Exploration
2. Education
3. Experimentation
4. Experience
5. Exchange
6. Equipment
7. Earning

These seven elements are related in every article about a computer forensic examiner. They may not come right out and state the seven E’s, but they suggest the same concept. Whether a department or company chooses to use civilian employees compared to certified employees, the same training is going to be employed.

In most articles and research that has been reviewed, each refer to a forensic team, but do not deal with the issue of whether they should be civilian or certified. At the very start of a computer forensic unit, administrators need to decide what type of unit they will have: Either proactive units, where computer forensic team members will do online investigations, investigate fraud complaints dealing with digital media and literally investigate the case from start to finish or will the agency just do forensic examinations on computer media and transfer the information to a secondary investigator to finish the process.

The cost factor of running a computer forensic unit depends on which direction the administration wants. The cost of training a person, cost of equipment, and finally how long this person will be staying in a forensic unit must be considered. These cost factors should be factored into the plan before a decision is made. In this economy, where the budget is tight, this research will give options on other approaches to whether they should be civilian or certified officers.

Literature Review

In every article researched, each author has come up with the same information on who to look for, education needed and continuing education. Craig Ball, in his article “How do I become a Computer Forensic Specialist?” does the best job in putting together the necessary steps for an investigator, whether civilian or certified. Mr. Ball lays out the “Seven E’s.”

Exploration: A good forensic examiner is self taught. The examiner can build and repair a computer. They investigate other programs to see how they work and experiment with settings to see what the outcome will be.

1. Education: Every forensic examiner is eager to learn from others. The examiner is eager to learn from other people regarding how they achieved their results.
2. Experimentation: Even when an examiner learns new techniques, he wants to try it himself/herself and try to get the same results. The examiner may try to change the technique to find out which way is better or what would happen.
3. Experience: This takes time. After several examinations and classes/college courses, the examiner gets to the point that they can talk in common terms to get the information to the proper people who will understand what is being said.
4. Exchange: This is where the networking comes into effect. Speaking to other examiners about techniques they have learned while working different forensic investigation. With the

amount of different digital media on the market, one person could not remember everything.

5. Equipment: The equipment used is a costly affair. When computer forensic start out in the early 90's, a hex editor and a writer blocker was a cheap fast way to conduct an examination. With Hard drives reaching 2 terabytes, more sophisticated software must be employed. Some of the forensic software can run into the thousands of dollars. Also, the equipment needed to copy the media along with storing the information could also run into the thousands of dollars
6. Earning: Whether you are a civilian or certified person, wages are important. If someone else offers more money, than the chances a trained person will leave and take a better position increase.

Christine Vecchio-Flaim wrote in her article "Developing a Computer Forensics Team," that a team can't be built overnight. Ms. Vecchio-Flaim stated that it is difficult to find skilled forensic specialists because of the training and experience needed to become a forensic examiner. Ms. Vecchio-Flaim states the person must have education, experience and know their equipment. It takes time and practice to achieve this goal. She mainly says the best people to use are IT professionals. They understand how an operating system works.

Methods

A questionnaire survey was send by electronic mail to 20 law enforcement agencies south of Central Florida. The survey will give two indications The second will give a general overall trend of computer forensic examiners performing examinations for their agencies.

Results

There was a return of 50 percent of survey questionnaire returned.

1. Does your agency have a Computer Crimes Unit?
    a. Yes 40%
    b. No 60%
2. Does your agency send out your Forensic digital devices?
    a. Yes 40%
    b. No 60%
3. How big is your agency?
    a. Less than 100 members 10%
    b. 101 to 300 members 40%
    c. 301 to 600 members
    d. 601 and up members 50%
4. Does your unit investigate a computer crime from start to closure?

a. Yes 80%
b. No 20%

5. How many sworn officers are conducting forensic examinations?
    a. 0 to 1 70%
    b. 2 to 4 20%
    c. 5 to 6 10%
    d. 7 or more
6. How many non sworn officers are conducting forensic examinations?
    a. 0 to 1 90%
    b. 2 to 4 10%
    c. 5 to 6
    d. 7 or more
7. What are the average years of service for your examiners have in your unit?
    a. 0 to 1 40%
    b. 2 to 4 20%
    c. 5 to 6 20%
    d. 7 or more 20%
8. What type of examinations does your unit perform? (check all that apply)
    a. Computers (Mac or PC) 20%
    b. Cell phones
    c. Storage devices 20%
    d. All the above 60%
9. List any other comments you think would assist in this survey? (example-Our forensic examiners are required to be Certified or non certified and attend a number of classes.)

In this open end question, most of the agencies that do conduct computer forensic examinations, listed that training and obtaining a certification was important to their unit. The agencies that send out their examinations send to other agencies that have certified examiners like FDLE, or other larger agencies.

Discussion

After reviewing the returned surveys, there is one main topic that each agency that does have computer forensic examiners has to be well educated in computer forensics. Each agency wants their examiners to be certified by an forensic organization like EnCase, and International Association of Computer Investigative Specialists. Most agencies have certified law enforcement officers currently conducting computer forensic examinations. There was one agency that was currently starting a computer forensic unit with one non-certified member. There is a problem with this survey that each agency is facing and that it is the stereotype that only certified law enforcement officers can conduct a computer forensic examination. Currently, major universities are currently adding computer forensic courses to their courses. Some have developed a required course study that would give a person a degree in Computer Forensic

Recommendations

Should an agency have a computer forensic unit? According to the survey, an agency with less than 300 personal should not have a computer forensic unit. The cost of equipment and personal could make the idea of having a computer forensic unit a costly budget line on a department's budget. Devoting the necessary man hours and attending the necessary computer forensic courses, along with obtaining certification to qualify a person to examine a computer correctly would take a person about a year and a major investment in funds.

This question would be better answered by the agency. If the agency is treating their computer forensic unit like a crime scene unit, with the examiner just looking at acquiring the data and then giving the information to a detective to investigate further, then a non-certified member is the best choice. If the agency requires all computer related crimes be investigated by a member of a unit, you would have to have more than one person. Most likely you would have two to three members. Two of the members could be non-certified. They would be the members that did the data mining and presented the information to the certified member. The certified member would be the person that actually investigates the crime itself. This goes back to the same recommendation that started the discussion, the computer crime unit, based on economic factors; a civilian could perform the necessary investigation and pass the information to a certified member who could follow up on the investigation. This certified member could also investigate other crimes such as burglaries, thefts, frauds and other associated crimes. This would be the most cost effective use of funds for an agency.

Gary Ellsworth has worked with the Charlotte County Sheriff's Office since 1989. He has worked in several divisions to include Patrol, Criminal Investigation, Major Crimes Unit, Economic Crime Unit and Computer Forensic Unit. Gary currently is a Lieutenant supervising the Criminal Investigation and Computer Forensic Unit for Charlotte County. Gary has a bachelor's degree in Criminal Justice from St. Leo University.

References

Ball, C. (2006). *How do I become a computer forensic specialist?* Retrieved from http://www.craigball.com/Becoming%20a%20Computer%20Forensic%20examiner.html

Leigland, R, & Krings, A. (2004). A formalization of digital forensics. *International journal of digital evidence*, *3*(2), Retrieved from http://www.utica.edu/academic/institutes/ecii/publications/articles/aob8472c-d1d2-8f98-8f7597844cf74df8.pdf

Rowlingson, R. (2005, May). An Introductio to forensic readiness planning. *NISCC*, (27), Retrieved from http://www.cpni.gov.uk/docs/re-20050621-00503.pdf

Meyers, M, & Rogers, M. (2004). Computer forensics: meeting the challenges of scientific evidence. Retrieved from http://cerias.purdue.edu/assets/pdf/bibtex_archive/2005-18.pdf

Michaud, D. (2001). Adventures in computer forensics. Retrieved from http://www.sans.org/reading_room/whitepapers/incident/adventures_in_computer_forensics_638?show=638.php&cat=incident

Stacy, H, & Lunsford, P. (2006). Computer forensics for law enforcement. Retrieved from http://www.inforsecwriters.com/tex_resources/pdf/Forensics_HStacy.pdf

Vecchio-Flaim, C. (2001). Developing a computer forensics team. *Security Reading Room*, Retrieved from http://www.sans.org/reading_room/whitepapers/incident/developing_a_computer_forensics_team_628?show=628.php&cat=incident

Yasinsac, A., Erbacher, R.F., Marks, D.G., Politt, M.M. & Sommer, P.M. (2003, July). Computer forensics education. *The IEEE Security and Privacy, 1(4)*, 15-23. ISSN: 1540-7993.

Yngvar, S, & Frode, S. (2005). Digital forensics research. *Telektronikk*, Retrieved from http://www.telenor.com/telektronikk/volumes/pdf/1.2005/page_092-097.pdf