Computer forensics laboratory

Running Head: COMPUTER FORENSICS LABORATORY COMPUTER FORENSICS LABORATORY By Processes Involved in Computer Forensics Laboratory Computer forensics is a discipline that integrates aspects of law and computer in the process of data collection and assessment from " computer systems, networks, wireless communications, and storage devices" in a manner that does not violate procedural laws on admissibility (US-CERT 2008). It involves the processes of preservation, identification, extraction and documentation. Computer forensics are conducted either offline or online. An offline analysis necessarily means conducting examination of a computer system while it is powered down and an online analysis while it is powered on. The first one is preferable, but there are instances when it is impossible to conduct it in such a manner as in cases when the system needs to be continuously powered on. During an offline analysis, copies of the hard drive are made to ensure that no data is lost and during a powered on forensics analysis, the investigator takes and collects as much evidence as he can take (Craiger 2006, p. 5). Since the goal of computer forensics is to gather and obtain evidence that may be presented in court against a suspect in a crime, it is important that the processes undertaken abide by the Federal rules of evidence that govern the admissibility of evidence. There are three steps with which computer forensics is undertaken: one, make an exact digital copy of the original evidence to ensure that the latter is untouched and unaltered; two, validate that the copy is an exact replica of the original, and, three, analyze the digital copy. The exact physical copy of the evidence is called bit-stream image, forensic duplicate or forensic image and is done by removing the hard disk from the source computer and attaching it to the investigator’s forensic machine with the following security measures: using a write-blocker to ensure that no data is written to it in the process, and; setting the jumper setting of the source drive to slave to prevent any change of files. As an alternative, the network acquisition method may be used where the source computer is access by the forensics computer through a network connection. Verification of the copy involves the use of a one-way hash algorithm called the MD5 cryptographic hash (Craiger 2006, pp. 6-7, 9-13). Analysis done in computer forensics laboratory may be classified as logical or physical. Logical analysis looks at the evidence from a file system perspective using system tools such as file manager, file viewer and the like. On the other hand, physical analysis entails an examination of the evidence from a purely physical perspective and uses tools such as the hex editor. For example, in the examination of the source hard disk, logical analysis confines the examination to clusters allocated to a file, but a physical analysis entails looking not only at allocated space, but also on unallocated and slack spaces (Craiger 2006, pp. 18-49). The first thing to do in the analytical process is to reduce the space to be searched for efficiency and accuracy. This could be done through processes called hash analysis and signature analysis. Hash analysis entails sifting through and distinguishing between known and notable files. Known files are ignored, while notable files, such as hacking tools and child pornography, are scrutinized. On the other hand, signature analysis distinguishes between documents and their types, and images. If the goal of the investigation is to obtain pornographic images as evidence against the suspect, then the appropriate file signature, such as JPEG, for images must be identified. In searching for specific forensic image, searches may be made using keywords and particular types of files such as email, web-mail as well as looking for computer footprints in the swap file, index. dat file, cookies, INFO2 for deleted files, temporary files, print spool files and similar files (Craiger 2006, pp. 18-49). The Laboratory: Services and Training Offered The San Diego Regional Computer Forensics Laboratory is the nearest computer forensic laboratory to the state of Hawaii. This laboratory offers the following services: on-site seizure and collection; duplication, storage and preservation of computers and related evidence; forensic examination of digitally stored media, and; courtroom testimony. The San Diego RCFL offers courses to law enforcement agents that are geared to train them in seizing, collecting and analyzing computer evidence as well as other specialized areas of computer forensics such as internet intrusion and computer forensics software. Course descriptions include: forensic tool kit for investigators; image scan training; introduction to MySpace and other social networking websites; seizing and handling of digital evidence; internet crimes and tracing, and; N-DEx class description (San Diego RCFL 2011). The San Diego RCFL facilities include a 25-student computer workstations, with Dell precision Workstation 650, networked by Ghost Station as well as peripherals such as 42’ plasma monitor, a projector, 2 Whiteboards, a VCR, DVD player and broadcasting capability provided by Robotel (San Diego RCFL 2011). As for job opportunities, an interested party does not apply directly to the San Diego RCFL nor does the latter ‘ hire’ employees. An interested applicant must be nominated by any of the participating agencies of which he or she is gainfully employed. The detail usually lasts for 2 years (RCFL 2011). The participating agencies to the San

Diego RCFL to which the applicant must be an employee of are: California Highway Patrol; Carlsbad Police Dept; Chula Vista Police Dept.; Department of Homeland Security-Immigration and Customs Enforcement; El Cajon Police Dept.; FBI; La Mesa Police Dept.; National City Police Dept.; Oceanside Police Dept.; San Diego District Attorney’s Office; San Diego Police Dept.; San Diego Sheriff’s Dept.; US Attorney’s Office; DHS-Customs and Border Protection (San Diego RCFL 2011). References: Craiger, J. P. (2206). Computer Forensics Procedures and Methods. RCFL (2011). Employment Opportunities with RCFLs. San Diego RCFL (2011). Regional Computer Forensics Laboratory. US-CERT (2008). Computer Forensics.