B3 Understanding the Costs of Conducting Computer Forensic Examinations

Douglas G. Elrick, BA, Digital Intelligence, 17165 West Glendale Drive, New Berlin, WI 53151*

After attending this presentation, attendees will be able to accurately evaluate, compute, and budget the needed costs of digital forensic examiners. Whether starting a new unit or expanding an existing one, costs can be effectively estimated.

This presentation will impact the forensic community by providing managers and directors an introduction to the computer technology and practices of this forensic discipline, a guide for budgeting and planning to adequately equipment, and examples of the types of cases examiners will face.

Attendees of this presentation will learn about real costs associated with computer forensic examinations and will come away with an understanding and appreciation for the necessary types hardware, software, facilities, and training requirements for this newly recognized scientific discipline. A comparison of the commonly used forensic applications and hardware will be given. This will be helpful in the purchasing and budgetary development process for both managers and experienced practitioners.

Costs for conducting computer forensic examinations can be broken down into four main categories; hardware, software, facilities, and training. While these categories are similar in other forensic disciplines, the need for continuing updates is more apparent and pronounced in the computer field. Typical hardware and software startup costs requirements based upon a two-person section will range between $30,000 and $100,000. This presentation will highlight this range and describe the factors involved in the cost differentiations. Specific software programs and hardware devices will be addressed in a manner to present a perspective and comparison of the many features. A listing of what is considered "industry standard" applications based upon functionality will be provided along with a variety of lesser known and often less expensive or free alternatives. What must also be factored into the overall cost will be the need for annual updates of licenses and hardware changes. Many of the current forensic software packages are offering (some are requiring) annual subscription services for their products in order to receive updates and fixes. Hardware lifecycles are running approximately three years before upgrades are necessary. New types of storage media is a big reason for required upgrades. For example, when new interfaces to hard drives or new flash media types are developed the forensic workstation must be capable of connecting to it. This can often be accomplished through relatively inexpensive adapters. In other circumstances, it may require complete upgrades to the internal components of the computer. Approximately $10,000 a year may be necessary to cover these updates.

With regard to the facilities needed for digital forensics, while the data collection and inventory of the physical components of the submitted evidence are done in a traditional laboratory environment with the ability to address any chemical or biological contamination, the forensic computer analysis is typically accomplished at a desk location. The desk location should still be a part of the laboratory with all of its security and controls, but should be in an isolated place. Due to the nature of the data displayed, which is often child pornography, the examination should be conducted in an area where viewing is limited to the examiner and not to any passerby. The examination may also require considerable concentration and the work area should allow for minimal distraction.

Unlike most other forensic disciplines where the methods of analysis and identification are continually improving but the evidence itself has remained the same, with computer information the form of the evidence is consistently changing and evolving. This frequent change necessitates updated training. Continuing education is essential in order for examiners to stay abreast of new technologies and methodologies. Software and hardware providers offer regularly scheduled training updates and there are several computer forensic associations that provide methodology training each year. For state and local law enforcement grant-funded training opportunities are available. A minimum number of hours should be twenty hours per year, per examiner, as this meets the educational requirements of several industry certifications. This would provide the most basic of updates. A preferred number would be 80 hours, budgeted at $20,000 a year for two examiners.

Managers and directors who are not familiar with the computer technology and practices of this forensic discipline will have a guide for budgeting and planning to adequately equipment and provide for the types of cases examiners will face. Experienced examiners will be presented with an analysis of commonly used programs, hardware and training options.

Computer Forensics, Budget, Costs

* *Presenting Author*