C11 An Analysis of Digital Forensic Units

Kaitlyn Gurule, BS, Purdue University, 401 N Grant Street, West Lafayette, IN 47907; Kathryn C. Seigfried-Spellar, PhD*, Purdue University, Computer and Information Technology, 401 N Grant Street, West Lafayette, IN 47907; and Marcus Rogers, PhD, Purdue University, 401 N Grant Street, West Lafayette, IN 47907*

After attending this presentation, attendees will have learned about the operations of digital forensic units, what can be improved upon, and what tactics have succeeded.

This presentation will impact the forensic science community by providing a basis point for analyzing digital forensic units and also confirms the findings of previous research within the digital forensic community.

Computer technology is growing rapidly, and law enforcement has seen an increase in the number of criminal cases that involve digital evidence. Nearly all crimes, including both cybercrimes and traditional crimes, include some type of digital media.[1,2] In fact, it is becoming more common to see multiple forms of digital evidence in a single criminal case, such as texts from a mobile phone, travel coordinates on a GPS, and saved photos on a computer.

Law enforcement agencies are having a difficult time processing all of the digital media in an effective and efficient manner.[1] As the volume of digital data increases, so does the amount of time it takes to examine the data for evidence, resulting in a backlog. In addition, this backlog is exacerbated when there are multiple parties involved with multiple digital devices.[3] Thus, law enforcement is overwhelmed with the number of cases that involve digital evidence, as well as the number of devices and variety of devices which may be involved in a single case, adding to the backlog of cases.[2]

In order to overcome the backlog created by cases involving digital evidence, some states have created computer crime or digital forensic units that investigate and/or process the digital evidence obtained in criminal cases. For the purposes of this study, specialized cybercrime units were defined as units that work only on digital media forensics and complete the forensic investigation within their own unit. Non-specialized units were defined as any other unit that did not fit the specialized unit criteria. The current study assessed the effectiveness of specialized vs. non-specialized units.

Two surveys were completed: a phone interview and an online questionnaire. Twelve specialized and eight non-specialized units completed the phone interview. Eight specialized and eight non-specialized units completed the online survey. The data was aggregated and anonymized so the respondents felt comfortable reporting information about their units. Respondents answered a variety of questions about the unit, such as the unit's history (e.g., Why was it created? What were the original goals?), their past and/or current backlog, number of cases worked, and types of digital evidence examined, just to name a few. The study suggested the specialized units operated more effectively than the non-specialized units. This study also revealed the lack of knowledge regarding standard procedures/best practices in digital forensics, as well as the lack of consistency in the standards reported among the cybercrime units community. Finally, the current study also supported previous research regarding the need for more training, funding, and personnel in digital forensics.

Reference(s):

1. Clifford R.D. (2011). Cybercrime: *The investigations, prosecution and defense of a computer-related crime (Third ed.)*. Durham, NC: Carolina Academic Press.

2. Easttom C. (2014). *System forensics, investigation, and response (Second ed.).* Burlington, MA: Jones and Bartlett Learning.
3. Goodison S.E., Davis R.C., Jackson, B.A. (2015). *Digital evidence and the U.S. criminal justice system*. Priority Criminal Justice Needs Initiative.

Cyberforensics, Digital Media, Cybercrime