



**Phelco Technologies, Inc**  
**eBusiness Solutions**

156 E. Market Street, 7<sup>th</sup> Floor

Indianapolis, IN 46204

Phone: 317.898.0334

Fax: 317.536.3743

[www.phelco.com](http://www.phelco.com)

MBE | WBE | DBE | ACDBE | 8(a) | SDB

# **PHELCO BRIEF:**

## **DIGITAL FORENSICS SECURITY**

### *Education*

DEFINED: Digital forensics (a.k.a., e-forensics / computer forensics) "is the discipline that combines elements of law and computer science to collect, preserve and analyze data from computer systems, networks, wireless devices, portable media players and memory devices in a way that is admissible as evidence in a court of law."

Forensic Examinations have become a critical component to ensuring stability and security of businesses, organizations, educational institutions and government agencies. Complete and comprehensive data recovery solutions for law enforcement, attorneys, corporations, schools and universities, financial & insurance institutions and government organizations has become a significant technique that is considered a significant part of management.

Typical types of data requested statewide by schools or other academic institutions for a digital forensic examination include: email usage, website history, cell phone usage, cellular & VOIP phone usage, file activity history, file creation or deletion, chat history, account login/logout records, and more. These data requests are likely instrumental in detecting security risks for an institution, because they will identify areas of concern and potential leaks in security filters.

When accompanied with an appropriate Legal Plan and Operational Continuity Plan, Phelco is able to prove a well-rounded solution for virtually any stage or process involved in examining, storing, recovering and securing data. Phelco's Digital Forensic services are handled by a team of active and experienced legal agents and law enforcement investigators who possess significant experience for each of their respective areas of expertise.

It is important to note that even the most experienced I.T. professional, may not be as familiar with producing data using forensic methodology - making the found data acceptable in a court of law. In addition, (should the case arise) the examiner must also be able to give expert testimony to the forensic procedures and results of the examination in a court of law.

#### **RELEVANT EXAMPLES:**

- Recovery of lost or damaged student data;
- eDiscovery of unlawful or improper use of network resources or the Internet by students or faculty;
- Investigations into unlawful or improper content being copied, accessed or produced on school computers or when connected to the school network;
- Investigations into harassment or other improper or unlawful communications by or between faculty, staff, administration and students - by means of cellular or VOIP phones, emails, chats, website or social network posts (MySpace, Facebook, YouTube, etc.) or any other means of digitally transferred or stored media;
- Investigations into improper or unlawful access to restricted files or directories by internal or external hacking attempts;
- Investigations into critical incident threats or actions against individuals, groups or facilities - including school bomb threats, student bullying, school shootings and vandalism;
- Proactive security audits of I.T. policy and procedures - ensuring that legal requirements are met.