Best Practices for Sharing Digital Evidence

This project explored best practices to guide DHS and other federal, state, and local law enforcement investigators and organizations in a wide variety of aspects of digital forensics, and in particular in training and certification programs. Investigations of crimes increasingly involve capturing, storing, analyzing, and sharing digital evidence. The fast-paced growth in digital technologies and evolving laws governing search and seizure and privacy mean that DHS must develop new digital forensic investigative procedures and develop new tools for training its personnel and law enforcement in general in the use of such procedures. The research team looked for best practices for digital forensics that can be immediately applied in investigations and used along with gaps and requirements identified as the basis for developing training materials.

The team worked with the Federal Law Enforcement Training Centers (FLETC) to develop and analyze a survey questionnaire focused on required competencies, training needs, certification, and the importance of various skills for first responders dealing with digital evidence as well as for advanced forensics examiners. Their analysis of survey results identified common training requirements, certifications desired, and the importance of advanced forensics analysis skills across the different kinds of organizations. Separately, they collected information about and categorized digital forensics courses and certifications available to those in the field by type, length, NIST job function, forensics lifecycle area, and more. They have identified gaps in certification and training offered by FLETC and available to DHS, presented available options to fill these gaps, and have also created digital forensics certification pathways based off of our findings. A primary objective of this research has been to contribute to the analysis of cyber forensics training and certification for DHS investigators, the standardizing of cyber forensics training, and the development of a consistent certification program. However, the information gathered could be a start in understanding how to attract and retain cyber professionals to this in-demand area of the government sector.

To request copies of the final reports, please contact cina@gmu.edu