

DHS Science and Technology Directorate

Cybersecurity Forensics Support for Law Enforcement

Keeping pace with cyber criminals

In recent years, computers and portable media devices (e.g., cell phones, GPS devices) have become indispensable to the planning, coordination and execution of criminal activities. These devices may contain vital evidence—such as user information, call logs, locations, text messages, emails, images or audio and video recordings—that could lead to the arrest of criminals. However, law enforcement agencies often do not have the tools or technologies to keep up with the constantly evolving hardware and software these devices use. Law enforcement officials require scientific and technological support to stay abreast of the latest technologies and analyze information stored on these devices.

New tools analyze evidence recorded in digital devices

The Department of Homeland Security (DHS) Science and Technology Directorate's (S&T) Cybersecurity Forensics project develops solutions for law enforcement in the daily investigation of threats. S&T created this project to address the specific needs of DHS law enforcement components, as well as to collaborating with investigators at various federal, state and local agencies. The project involves efforts in the persistent areas of cyber forensics, including mobile device forensics, GPS forensics, data acquisition and analysis, first responder crime-scene computer triage, high-speed data capture and deep packet inspection, gaming system live capture, and law enforcement technology information exchange.



Project requirements originate from the Cyber Forensics Working Group (CFWG), led by S&T's Cyber Security Division, which is composed of representatives from federal, state and local law enforcement agencies. CFWG members meet bi-annually to discuss capability gaps, pri-



oritize the areas of most immediate concern to focus technology development, provide requirements and participate as test and evaluation partners for prototype technologies.

In addition to CFWG members, the National Institute of Standards and Technology's Computer Forensics Tool Testing Steering Committee, the Federal Bureau of Investigation-sponsored Scientific Working Group on Digital Evidence, and the Defense Cyber Crime Center are strongly involved in the requirements vetting and testing phases of this project.

Law enforcement officers will have the technology needed to investigate cyber crimes

The tools developed through this project will significantly improve capabilities for law enforcement agencies to address cyber-related crimes and will be used in investigative casework immediately following project transition. The delivered tools are designed to fit seamlessly into existing operations at customer agencies without disruption.

Transitioning technologies

- 2013: Transitioned mobile device flash memory chip acquisition tools
- 2013: Transitioned Blackthorn3[®] GPS analysis tools and provided training and licenses to 80 additional customers
- 2014: Distribute disposable mobile phone tutorials free of charge to law enforcement

Performers

- Berla Corporation, Millersville, Maryland
- S34A Inc., Reston, Virginia
- Basis Technology, Cambridge, Massachusetts
- National Institute of Standards and Technology Gaithersburg, Maryland



**Homeland
Security**

Science and Technology

To learn more about Cybersecurity Forensics, contact sandt-cyberliaison@hq.dhs.gov.