DHS Science and Technology Directorate

Cyber Security Division Cyber Security Forensics Project

Law enforcement agencies need to keep pace with the technologies criminals are using

The role of computers and portable media devices such as cell phones and GPS units in criminal and terrorist activity has increased significantly in recent years. In most cases, these devices contain vital evidence, including user information, call logs, location, text messages, email, images and audio and video recordings.

Law enforcement agencies require scientific and technological support to analyze the information stored in constantly evolving hardware and software, which is becoming more indispensable to the planning, coordination and execution of criminal and terrorist acts.

Developing new tools to analyze evidence from digital devices

The U.S. Department of Homeland Security (DHS) Science and Technology Directorate's (S&T) Cyber Security Forensics project develops solutions law enforcement can use to investigate criminal and terrorist activity. This project addresses the specific needs of DHS law enforcement components, and also collaborates with investigators from a variety of federal, state and local agencies and international partners. The project encompasses efforts in the persistent areas of cyber forensics, including mobile device forensics, GPS forensics and data acquisition and analysis.

Project requirements originate from the Cyber Forensics Working Group (CFWG), led by S&T's Cyber Security Division (CSD), part of the Homeland Security Advanced Research Projects Agency. The CFWG is composed of representatives from federal, state and local law enforcement agencies who meet biannually to discuss capability gaps, prioritize the areas of most immediate concern to focus technology development, provide requirements and participate as test-and-evaluation partners for prototype technologies.

Through this project, S&T CSD co-funds the National Institute of Standards and Technology's Computer Forensics Tool Testing Steering Committee and Scientific Working Group on Digital Evidence. Both groups provide additional input to S&T on research needs in the law enforcement community.

Law enforcement officers receive the technologies needed to investigate cybercrimes

The tools developed though this project are significantly improving the capabilities of law enforcement agencies, which use the new solutions in investigative casework immediately following project transition to address criminal activity. Most importantly, the delivered tools are designed to fit seamlessly into existing operations at customer agencies.

Transitioning technologies

- **2014:** Tutorials outlining disposable mobile phone data acquisition were distributed free of charge to law enforcement
- **2016:** Expansion of modules for open-source digital forensics platform for law enforcement was completed
- **2017:** Final version of vehicle forensics tool providing a solution for more 10,000 vehicle makes and models was released
- **Ongoing:** National Software Reference Library Computer Forensics Tool Testing, Computer Forensics Reference Dataset provide resources and standards to the broader digital forensic community

Performers

- Basis Technology
- Mississippi State University
- National Institute of Standards and Technology
- VTO Inc.
- Partnership with New Zealand Department of Internal Affairs

To learn more about Cyber Security Forensics, contact SandT-Cyber-Liaison@HQ.DHS.GOV