

# DHS Science and Technology Directorate

## Cyber Security Division - Cyber Security Forensics

### Law enforcement agencies need to keep pace with technologies criminals use

The role of computers and portable media devices (e.g. cell phones, GPS devices) in criminal and terrorist activity has increased significantly in recent years. Used as such, these devices may 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 stay abreast of the latest technologies to analyze information stored in constantly evolving hardware and software as they become 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&T) Cyber Security Forensics project develops solutions for law enforcement in the daily investigation of criminal and terrorist activity. This project addresses the specific needs of DHS law enforcement components and collaborates with investigators at a wide variety of federal, state and local agencies and international partners. The project involves efforts in the persistent areas of cyber forensics including: mobile device forensics, GPS forensics, data acquisition and analysis, and law enforcement technology information exchange.



Project requirements originate from the Cyber Forensics Working Group (CFWG), led by S&T's Cyber Security Division (CSD), which is composed of representatives from federal, state, and local law enforcement agencies. CFWG members meet bi-annually 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 (NIST) Computer Forensics Tool Testing Steering Committee and the Scientific Working Group on Digital Evidence. Both of these groups provide additional input for S&T on research needs in the community.

### 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 criminal activity and will be used in investigative casework immediately following project transition. The delivered tools are intended to fit seamlessly into existing operations at customer agencies without disruption.

### Transitioning technologies

- 2014: Disposable mobile phone tutorials distributed free of charge to law enforcement
- 2015: Expansion of modules for open source digital forensics platform for law enforcement
- 2015: Transition of solid state memory software and hardware
- Ongoing: Updated release of vehicle infotainment and navigation forensics tool

### Performers

- Berla Corporation
- Pacific Northwest National Laboratory
- Basis Technology
- National Institute of Standards and Technology



**Homeland Security**

Science and Technology

To learn more about Cyber Security Forensics, contact Megan Mahle, Program Manager.