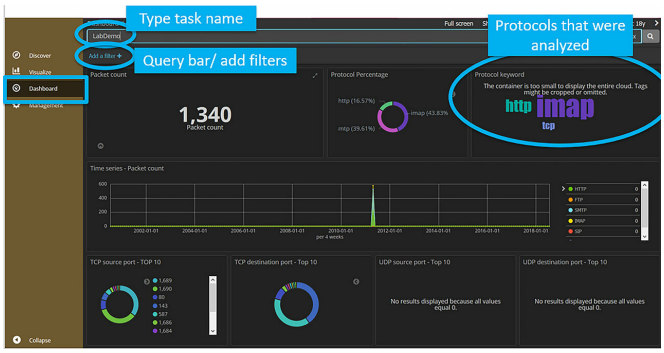
An all-in-one cyber toolkit for criminal investigations

7 March 2019, by Chris Adam



Purdue University cybersecurity experts have developed an all-in-one toolkit for criminal investigations, making it easier to follow a criminal's digital footprint. Credit: Kathryn Seigfried-Spellar/Purdue University

Cybercriminals can run, but they cannot hide from their digital fingerprints.

Still, cybercrimes reached a six-year high in 2017, when more than 300,000 people in the United States fell victim to such crimes. Losses topped $1.2 billion.

Now, Purdue University cybersecurity experts have come up with an all-in-one toolkit to help detectives solve these crimes. Purdue has a reputation in this area—it is ranked among the top institutions for cybersecurity.

"The current network forensic investigative tools have limited capabilities—they cannot communicate with each other and their cost can be immense," said Kathryn Seigfried-Spellar, an assistant professor of computer and information technology in the Purdue Polytechnic Institute, who helps lead the research team. "This toolkit has everything criminal investigators will need to complete their work without having to rely on different network forensic tools."

The toolkit was presented in December 2018 during the IEEE International Conference on Big Data.

The Purdue team developed its Toolkit for Selective Analysis and Reconstruction of Files (FileTSAR) by collaborating with law enforcement agencies from around the country, including the High Tech Crime Unit of Tippecanoe County, Indiana. The HTCU is housed in Purdue's Discovery Park.

FileTSAR is available free to law enforcement. The project was funded by the National Institute of Justice.

The Purdue toolkit brings together in one complete package the top open source investigative tools used by digital forensic law enforcement teams at the local, state, national and global levels.

"Our new toolkit allows investigators to retrieve network traffic, maintain its integrity throughout the investigation, and store the evidence for future use," said Seunghee Lee, a graduate research assistant who has worked on the project from the beginning. "We have online videos available so law enforcement agents can learn the system remotely."

FileTSAR captures data flows and provides a mechanism to selectively reconstruct multiple data types, including documents, images, email and VoIP sessions for large-scale computer networks. Seigfried-Spellar said the toolkit could be used to uncover any network traffic that may be relevant to a case, including employees who are sending out trade secrets or using their computers for workplace harassment.

"We aimed to create a tool that addressed the challenges faced by digital forensic examiners when investigating cases involving large-scale computer networks," Seigfried-Spellar said.

The toolkit also uses hashing for each carved file to

maintain the forensic integrity of the evidence, which helps it to hold up in court.

More information: Raymond A. Hansen et al, File Toolkit for Selective Analysis & Reconstruction (FileTSAR) for Large-Scale Networks, *2018 IEEE International Conference on Big Data (Big Data)* (2019). DOI: 10.1109/BigData.2018.8621914