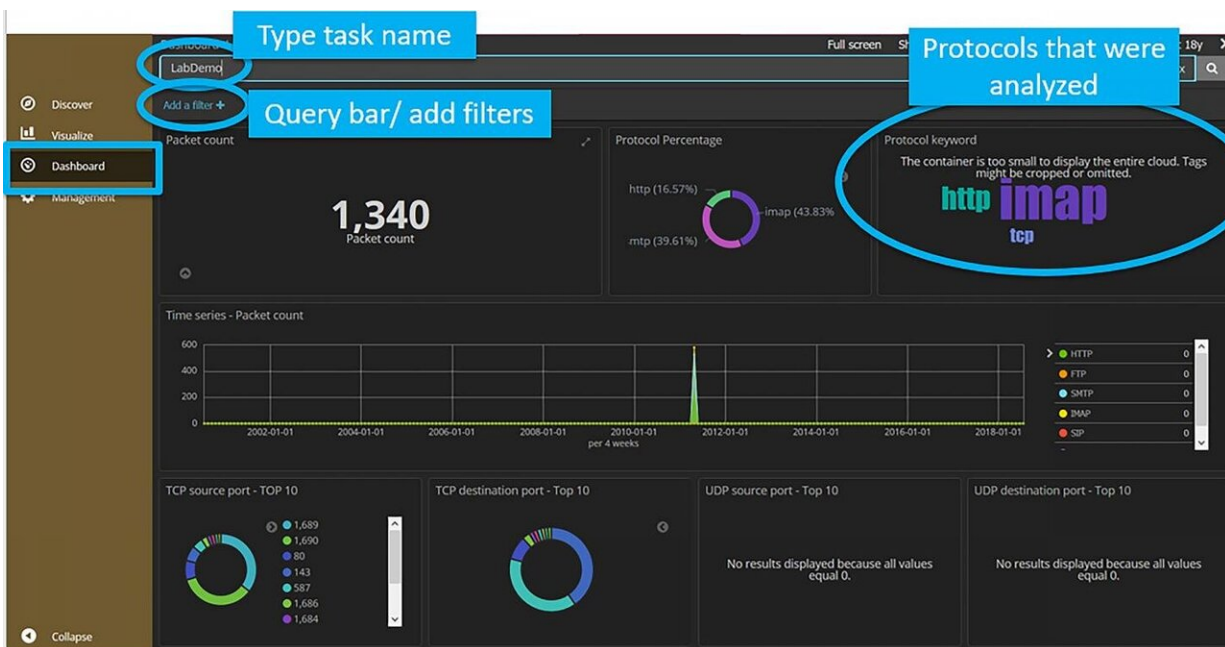


Cyber toolkit a 'complete package' for detectives, companies

March 3 2020, by Chris Adam



The Purdue Toolkit for Selective Analysis and Reconstruction of Files (FileTSAR) brings together in one complete package the top open source investigative tools used by digital forensic law enforcement teams. Credit: Kathryn Seigfried-Spellar/Purdue University

A growing number of law enforcement agencies from across the world want to use Purdue University technology to help them track down cybercriminals with a toolkit that also can help companies stop insider threats and technology-facilitated abuse.

Purdue cybersecurity experts developed the all-in-one toolkit, called the Toolkit for Selective Analysis and Reconstruction of Files (FileTSAR), to help detectives solve cybercrimes.

"FileTSAR allows [forensic investigators](#) to capture, selectively analyze and reconstruct files from [network traffic](#)," said Kathryn Seigfried-Spellar, an associate professor of computer and [information technology](#) in the Purdue Polytechnic Institute, who helps lead the research team.

"The main functions of this tool are capturing data flows and providing a mechanism to selectively reconstruct documents, images, email and VoIP conversations."

VoIP is Voice over Internet Protocol, a means of making [phone calls](#).

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.

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.

More than 100 law enforcement agencies from across the world have requested access to the technology, which is being licensed through the Purdue Research Foundation Office of Technology Commercialization.

"Knowing that we created an affordable tool that will help law enforcement with their network forensic investigations is incredibly rewarding," Seigfried-Spellar said.

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 HTCUC is housed in Purdue's Discovery Park.

The project was funded by the National Institute of Justice and made available for three years to [law enforcement agencies](#).

Provided by Purdue University

Citation: Cyber toolkit a 'complete package' for detectives, companies (2020, March 3) retrieved 2 May 2024 from <https://techxplore.com/news/2020-03-cyber-toolkit-package-companies.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.