NIST Offers Free Software to Help Agencies Test Computer Forensics Tools

NIST Offers Free Software to Help Agencies Test Computer Forensics Tools

Such a small item, this cellphone dropped by a suspect fleeing at the scene of a failed drug deal. But potentially, this small item could yield vital evidence in preparing a case that would stop the drug deals for good. And the investigators want to be absolutely sure they're using the right version of the right forensic tool that will produce that evidence in a manner that will hold up in court.

They turn to the National Institute of Standards and Technology (NIST) Computer Forensics Tool Testing (CFTT) project to get the help they need to ensure that it will.

Created in 1999 in the early years of the Information Age, CFTT offers computer forensics assistance to law enforcement agencies in two ways: through posting tool testing reports produced by NIST researchers and through offering free Federated Testing software that allows agencies to test tools on their own.

Launched in November 2015 with a version that allows agencies to check disk imaging capabilities, Federated Testing consists of a downloadable Linux CD .iso file. Agencies can burn the file to a blank CD, then use that CD to boot a forensic workstation and

test a tool or tools via a user-friendly interface.

“For 15 years we just did this ourselves, and law enforcement used our reports to help select the appropriate tools,” says Barbara Guttman, leader of the Software Quality Group. “We got to the point where there are so many tools out there, with new versions released all the time to correspond with new versions of mobile devices and new versions of apps, and how can you test all of them? The obvious answer was someone other than NIST has to do some of it or we can’t keep up.”

The Federated Testing software started with disk imaging because the first and most basic step in computer forensics investigations is to make a copy, thus leaving the original intact. NIST added the capability to test mobile forensics data extraction tools in June 2017, and write blocking capability will come online this fall. Agencies can sign up on the CFTT website (https://www.cftt.nist.gov/) to receive notification when a new version becomes available.

In its early months of availability, Version 1.0 of Federated Testing averaged about 35 downloads a month, and with the addition of the mobile forensics suite, that number should increase, says the Software Quality Group’s Ben Livelsberger. During 2017, NIST has provided technical assistance to a public defender’s office in Missouri and officers out of the United Kingdom, indicating agencies are already putting the downloaded software to use. And NIST encourages users to submit copies of their reports via email so that they, too, can be posted on the CFTT website and shared with

other agencies.

“Law enforcement agencies and universities can use it to not only help themselves directly, they can also use it to help each other,” Guttman says. “Sharing information will reduce everybody’s workload, and if we can help each other out, isn’t that a more efficient way of doing things? The result is a big win for law enforcement, and it can also be a big win for the vendor community, because they can use the reports to help them improve their tools.”

Guttman cautions that tools that “work correctly” still aren’t perfect; for example, it’s not possible to recover every single deleted file.

“We say we want the tools to work right, and in order to do that, we first have to define what ‘right’ is. Sometimes all we’re doing is characterizing what they can and can’t do so they can be used effectively,” she says.

The Scientific Working Group on Digital Evidence is developing a soon-to-be-released report that will help support using test reports even if a different version of the tool was tested.

“What they’re really saying is it’s unlikely that major versions will have bugs that will turn out to be relevant to your workload, and if you did extremely specific testing all the time, you’d never get any actual work done,” she says.

The Office of Justice Programs’ National Institute of Justice, along with the Federal Bureau of Investigation and the Department of Defense Cyber Crime Center, provided the original funding. Ongoing funding for the project comes from the U.S. Department of Homeland Security.

To research posted test reports or download the Federated Testing software, visit https://www.cftt.nist.gov. Reports produced prior to March 2013 can be located at here.

For more information, contact Rich Press in the NIST Public Affairs Office at Rich.press@nist.gov.

Article photo: Igor Stevanovic/Alamy Stock Photo