New NIST forensic tests to ensure high-quality copies of digital evidence

December 13 2017

Credit: Skylar Kang from Pexels

Data found on a suspect's computer, cell phone or tablet can prove to be crucial evidence in a legal case. A new set of software tools developed at the National Institute of Standards and Technology (NIST) aims to make

sure this digital evidence will hold up in court.

The software suite, referred to collectively as federated testing tools, is designed to help law enforcement and forensic practitioners with a critical early step in evidence collection: making a copy of the data from a seized electronic device. Because a suspect's guilt or innocence can hang in the balance, both the prosecution and the defense must agree that the digital forensic process did not introduce any unseen errors into the data, and that the methods they are using work as expected.

Extracting and copying data is a risky process because of the rapidly shifting digital landscape that we and our devices inhabit. Confronting the practitioners are all the differences in data and format that can exist between one device and the next—because of the sheer number of different manufacturers, and because of the frequent software updates pushed to various makes and models.

"It's hard to keep up," said Barbara Guttman, one of the suite's developers at NIST's Computer Forensics Tool Testing project. "You don't want to risk your copying software failing when you try to get data from some new computer that is critical to your case. So, we created these tools to help ensure that the copying software works effectively and transparently."

The federated testing tools allow authorities to run tests in advance on their digital forensic software to make sure ahead of time that it will not fail them when a suspect's personal computer, media or device arrives in the forensic science lab. Guttman describes the suite as the three most critical tools for evidence acquisition and preservation, each addressing one aspect of the copying process.

One tool tests software for copying computer disks, while another tests mobile device data extraction software. These two test protocols were

available previously, but the suite is now completed with a new third test for "write blockers," which are a sort of one-way valve for data-copying software. An effective write blocker allows data to flow only from the seized device to the copying computer, not the other way around. Later updates to the suite will address additional forensic functions, Guttman said.

The full suite is a freely available Linux file that anyone can download and burn to a blank CD. They can use the disk to boot their workstation and test their copying tools via a user-friendly interface.

The NIST software also allows different forensics labs to exchange the results of their tests with each other, so that they can share the burden of exploring how well a copying method works on a specific platform and operating system. Running copying software through its paces generates a report that disparate organizations can share among themselves or with the world, allowing them to indicate whether they found anomalies during the testing or not.

"Pooling these traceable results will mean less work for any given lab or organization," Guttman said. "We don't require they share the tests, but a rising tide should raise all boats."

Guttman cautioned that the tools will not ensure that a copying or digital forensic process is flawless, only that the results of the job are clearly visible to anyone.

"Evidence doesn't have to be complete to be admissible," she said. "The key here is that copying does not introduce errors into the data that no one can see."

Interest in federated testing will go beyond law enforcement agencies, Guttman added. Any organization that performs forensics, such as civil

law firms and corporate enforcement offices, will find a use for the test suite.

This story is republished courtesy of NIST. Read the original story here.

Provided by National Institute of Standards and Technology