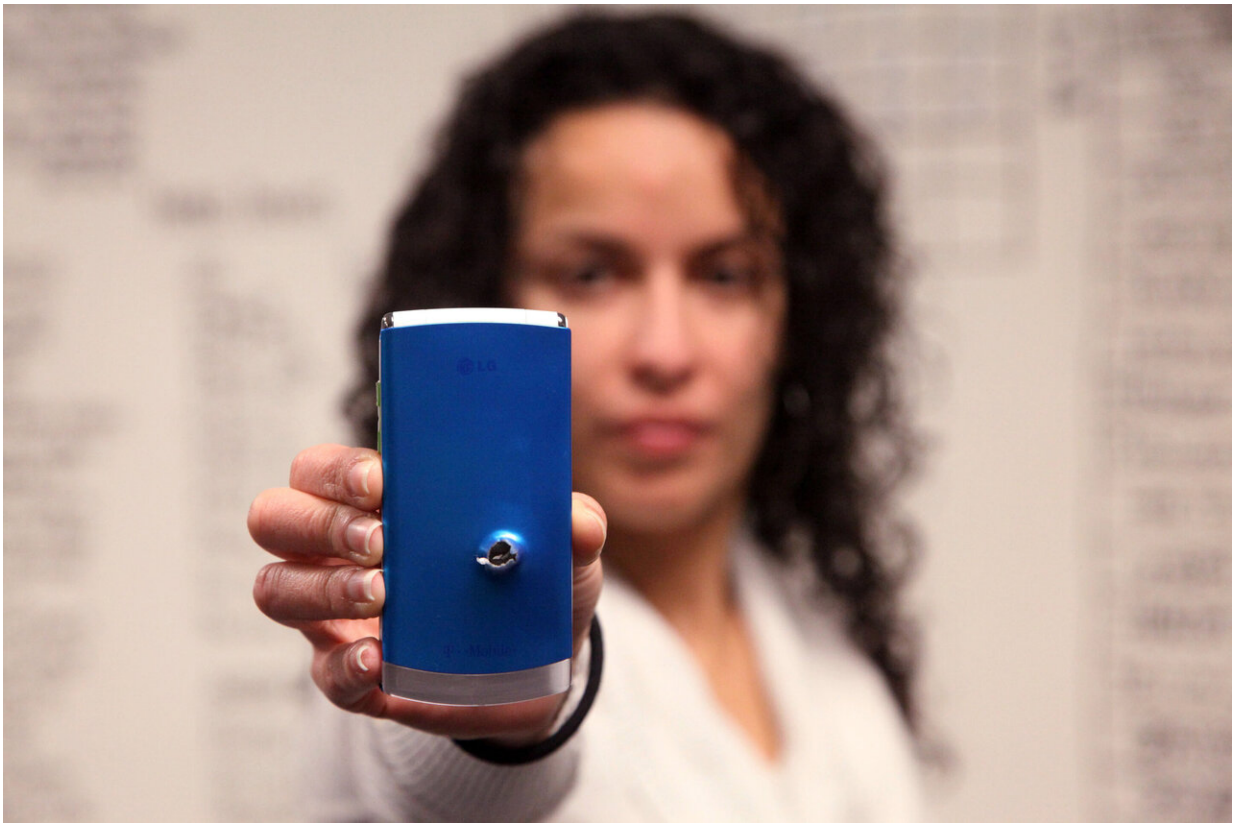
Forensic methods for getting data from damaged mobile phones

January 29 2020, by Rich Press



NIST computer scientist Jenise Reyes-Rodriguez holds a mobile phone that has been damaged by gunfire. Credit: R. Press/NIST

Criminals sometimes damage their mobile phones in an attempt to destroy evidence. They might smash, shoot, submerge or cook their

phones, but forensics experts can often retrieve the evidence anyway. Now, researchers at the National Institute of Standards and Technology (NIST) have tested how well these forensic methods work.

A damaged phone might not power on, and the data port might not work, so experts use hardware and software tools to directly access the phone's memory chips. These include hacking tools, albeit ones that may be lawfully used as part of a criminal investigation. Because these methods produce data that might be presented as evidence in court, it's important to know if they can be trusted.

"Our goal was to test the validity of these methods," said Rick Ayers, the NIST digital forensics expert who led the study. "Do they reliably produce accurate results?"

The results of the NIST study will also help labs choose the right tools for the job. Some methods work better than others, depending on the type of phone, the type of data and the extent of the damage.

The study addresses methods that work with Android phones. Also, the study covered only methods for accessing data, not decrypting it. However, they can still be useful with encrypted phones because investigators often manage to get the passcode during their investigation.

NIST computer scientist Jenise Reyes-Rodriguez uses the JTAG method to acquire data from a damaged mobile phone. Credit: R. Press/NIST

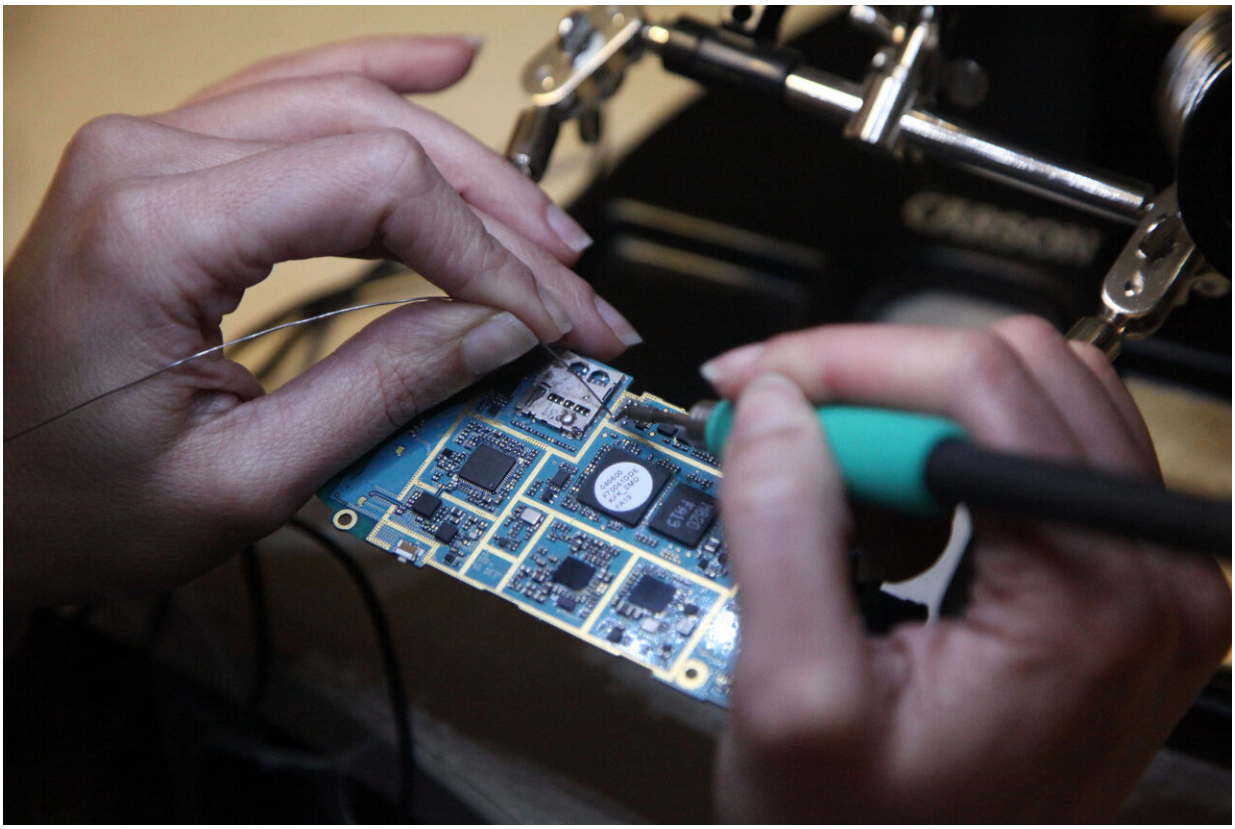
To conduct the study, NIST researchers loaded data onto 10 popular models of phones. They then extracted the data or had outside experts extract the data for them. The question was: Would the extracted data exactly match the original data, without any changes?

For the study to be accurate, the researchers couldn't just zap a bunch of data onto the phones. They had to add the data the way a person normally would. They took photos, sent messages and used Facebook, LinkedIn and other social media apps. They entered contacts with multiple middle names and oddly formatted addresses to see if any parts would be chopped off or lost when the data was retrieved. They added GPS data by driving around town with all the phones on the dashboard.

After the researchers had loaded data onto the phones, they used two methods to extract it. The first method takes advantage of the fact that many circuit boards have small metal taps that provide access to data on the chips. Manufacturers use those taps to test their circuit boards, but by soldering wires onto them, forensic investigators can extract data from the chips. This is called the JTAG method, for the Joint Task Action Group, the manufacturing industry association that codified this testing feature.

Chips connect to the circuit board via tiny metal pins, and the second method, called "chip-off," involves connecting to those pins directly. Experts used to do this by gently plucking the chips off the board and seating them into chip readers, but the pins are delicate. If you damage them, getting the data can be difficult or impossible. A few years ago, experts found that instead of pulling the chips off the circuit board, they could grind down the opposite side of the board on a lathe until the pins were exposed. This is like stripping insulation off a wire, and it allows access to the pins.

"It seems so obvious," said Ayers. "But it's one of those things where everyone just did it one way until someone came up with an easier way."



Digital forensics experts can often extract data from damaged mobile phones using the JTAG method. Credit: R. Press/NIST

The chip-off extractions were conducted by the Fort Worth Police Department Digital Forensics Lab and a private forensics company in Colorado called VTO Labs, who sent the extracted data back to NIST. NIST computer scientist Jenise Reyes-Rodriguez did the JTAG extractions.

After the data extractions were complete, Ayers and Reyes-Rodriguez used eight different forensic software tools to interpret the raw data, generating contacts, locations, texts, photos, social media data, and so on. They then compared those to the data originally loaded onto each phone.

The comparison showed that both JTAG and chip-off extracted the data without altering it, but that some of the software tools were better at interpreting the data than others, especially for data from social media apps. Those apps are constantly changing, making it difficult for the toolmakers to keep up.

The results are published in a series of freely available online reports. This study, and the resulting reports, are part of NIST's Computer Forensics Tool Testing project. Called CFTT, this project has subjected a wide array of digital forensics tools to rigorous and systematic evaluation. Forensics labs around the country use CFTT reports to ensure the quality of their work.

"Many labs have an overwhelming workload, and some of these tools are very expensive," Ayers said. "To be able to look at a report and say, this tool will work better than that one for a particular case—that can be big advantage."

Provided by National Institute of Standards and Technology

Citation: Forensic methods for getting data from damaged mobile phones (2020, January 29) retrieved 18 April 2024 from https://techxplore.com/news/2020-01-forensic-methods-mobile.html