Cell Phone Forensics Can Play a Key Role in Gathering Intelligence

By Rebecca L. Lewis

Author's Note: *Findings and conclusions reported in this article are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.*

The facility search team completes its first sweep with the newly trained cell phone-sniffing dog, coming up with a bag full of contraband ranging from old-style flip phones to the latest in smartphone technology. Now what? The answers are in a new publication, *Cell Phone Forensics in a Correctional Setting Guidebook*, which suggests how agencies can develop forensics programs for dealing with illegal cell phones.[1]

Many federal and state laboratories are overwhelmed by huge numbers of illegal cell phones. To help, the National Institute of Justice (NIJ) tasked John Shaffer, a retiree from the Pennsylvania Department of Corrections, with leading a three-year effort that culminated in publication of the guidebook. The project also involved a market survey of hardware and software; literature reviews; Internet searches; and meetings with subject matter experts (some experienced in cell phone forensics) and skilled technologists. The project was managed by the Corrections Technology Center of Excellence with funding from NIJ. The team concluded that administrators should implement forensics in their facilities, as well as learn to use all the tools and resources at their disposal. As Joe Russo, director of the Corrections Technology Center of Excellence and one of the guidebook's authors, said, "It is not just about collecting the confiscated phones, putting them in a box and giving the box to charity." It is, most importantly, about retrieving any valuable data that can be used to reduce or eliminate crime.

> **The guidebook's authors believe that as more and more inmates are successfully prosecuted using digital forensic evidence, the ability to recover data may prove to be a deterrent to using cell phones illegally in correctional facilities.**

Understanding the Problem

A common theme emerged from the project: Many corrections professionals share a belief that stopping inmates from using phones, whether through some form of managed access or locating contraband, is all that is needed to address the problem. "You'll often hear people say 'All we have to do is jam them,' or 'If we establish managed access and render them paperweights, that's all we need.' This lack of understanding of the technology is a real concern," said Shaffer. He discovered that many people do not realize that even when you cut off the ability to make a voice call, phones can still be used for a lot of other things such as taking still photographs, making videos, word processing and local text messaging. Some phones also allow the user to select the carrier, thus bypassing managed access systems. All of these things still pose a risk, so the phones should still be considered contraband. Thus, Shaffer always advocates recovering the hardware and conducting a forensic analysis to prevent the loss of potential evidence.

Russo agrees with Shaffer that the mission should not just be to recover the phones, but also to maximize their intelligence value, because the phones contain a great deal of data that could

potentially help uncover criminal acts and lead to arrests. This data can also identify links between inmates and individuals in the community who could, in turn, link to the officers and civilians who smuggle the phones into the facility.

Meeting the Need

Some corrections professionals lack awareness about the potential security intelligence stored on contraband cell phones and the importance of cell phone forensics. The *Cell Phone Forensics in a Correctional Setting Guidebook* gets this message out through an explanation of the evidentiary benefits of a cell phone forensics program; a review of the technology available to help agencies examine contraband cell phones; an outline of the issues involved in starting an internal cell phone forensics program; and a synopsis of relevant legal issues and case law.

Evidentiary benefits. To understand the evidentiary benefits derived from cell phone forensics, correctional administrators need to learn about the types of communication an individual can execute with a cell phone. These various types of communication can generate evidence that will support criminal investigations and can potentially lead to linkages between inmates and individuals in the community. The guidebook's authors believe that as more and more inmates are successfully prosecuted using digital forensic evidence, the ability to recover data may prove to be a deterrent to using cell phones illegally in correctional facilities.

Technology. This section looks at how currently available tools can help examine contraband cell phones. There are four basic options for data recovery: screen captures; logical analysis; physical analysis and a Joint Test Action Group; and chip analysis. Tools are classified according to a pyramid illustration, with techniques becoming more technical, taking longer to use and requiring more training as one moves up the pyramid. The guidebook includes examples of the various types of tools.

Establishing cell phone forensics capability. Agencies considering establishing a cell phone forensics capability need to consider issues such as obtaining funding for both startup and ongoing operations, as well as determining the appropriate technology tools and staffing; requirements for startup and ongoing training; and providing an appropriate physical site.

Implementation. Legal issues and case law need to be considered when establishing cell phone forensics capability, although the authors caution that nothing contained in the guidebook should be construed as legal advice sanctioned by NIJ or the National Law Enforcement and Corrections Technology Center System, of which the Corrections Technology Center of Excellence is a component. Other issues an agency should consider relate to coordination with law enforcement; establishing evidentiary priorities; collection and retention; and the need for policies and procedures.

Lessons learned and success stories. The guidebook provides links to sample policies and procedures, and includes summaries of successful prosecutions. Additional sample policies and procedures are provided in an appendix.

Outlook. Due to the number of devices confiscated, the Federal Bureau of Investigation and state police forensic labs are overwhelmed with a large backlog of requests for analysis, and it is becoming increasingly important for correctional agencies to develop their own internal forensic capacity. However, only about 29 percent of practitioner participants in a July 2013 cell phone webinar indicated their agencies have this capability.[2] To develop that capacity, agencies must make an ongoing commitment to fund staffing, training, equipment and computer hardware and software.

Conclusion

Agencies that make a commitment to developing their own internal forensic capacity will be able to mine data and conduct link analyses with inmate visiting lists and employee/volunteer telephone numbers, and they could potentially develop actionable intelligence that may lead to stopping and/or successfully prosecuting criminal activity. According to Russo, "Developing the internal capacity to examine [contraband cell phones] is probably something that every agency should consider if there is any kind of a cell phone problem. On the other hand, it's not for every agency. If you find only a few in a year, there are external resources your [agencies] can use, and the guide provides information on that, too."

ENDNOTES

[1] Shaffer, J.S. 2014. *Cell phone forensics in a correctional setting guidebook*. Denver, Colo.: Corrections Technology Center of Excellence.

[2] Ibid.

Rebecca L. Lewis is a writer and editor at the National Law Enforcement and Corrections Technology Center.