As I mentioned in a previous columns, there’s a new set of draft documents from the Computer Security Resource Center (CSRC) of the US National Institute of Standards and Technology (NIST) <http://csrc.nist.gov/publications/drafts.html>. Readers who are corporate information security officers investigating possible violations of policy and law enforcement officials investigating possible crimes may need to extract data from the multi-purpose devices that are, curiously, still referred to as “mobile phones.” For example, the Nokia Web site <http://www.nokiausa.com/phones/comparephones/1,8392,fltr=1|ordr=3,00.html> shows checkboxes for selecting devices equipped with

- Bluetooth® technology
- Camera (basic)
- Camera (2 megapixels or more)
- Downloadable ring tones
- FM radio
- Games
- Multimedia messaging
- MP3 player
- Speakerphone
- Video recorder
- Voice dialing
- Web browser.

When suspects use such devices, searching them for evidence becomes as necessary as searching their (other) computers.


Authors Wayne Jansen and Rick Ayers have prepared a 98-page document with the following structure:

1. Introduction
2. Background
3. Forensic tools
4. Procedures and principles
5. Preservation
6. Acquisition
Appendix C is an 11-page guide showing a generalized data-extraction process packed with screenshots from a variety of data-acquisition tools. It has the following subsections:

1. Connection identification
2. Device identification
3. Data selection
4. Acquisition
5. Phonebook entries
6. Call log entries
7. Message entries
8. Calendar entries
9. (U)SIM {UMTS [Universal Mobile Telecommunications System] Subscriber Identity Module} data
10. Picture entries
11. Searching
12. Reporting.

This work is a solid introduction to the terminology, tools and methods for forensic analysis of mobile communications devices; it will serve a wide range of users including instructors and students in industry and academic courses that focus on digital forensic investigations. I will certainly be recommending it as a reference in the upcoming Digital Forensic Investigations elective of the Norwich University Master of Science in Information Assurance (MSIA) program.

If readers have comments for improvement of the documents, they can submit them to <mailto:sp800-101@nist.gov?Subject=Comments%20SP800-101> by September 29, 2006.”

* * *


M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.msia.norwich.edu> at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2006 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.