A journalist from South Africa recently wrote to me with a series of interesting questions about forensics and I had such fun answering that I got his permission to post his questions and my answers in this column and the next.

> I'm looking for information and opinion on the ins and outs of the world of computer forensics. Maybe you would be interested in commenting for the story? I could email you specific questions.<

Hmm, I'm not a forensics expert, but I'll copy some of my colleagues who are so they can contribute to your research if they have time.

First, some general resources.


You may find some good resources in my CJ341 CyberLaw and Cybercrime course lectures at

http://www.mekabay.com/courses/academic/norwich/cj341/lectures.htm

In particular, I recommend looking at

http://www.mekabay.com/courses/academic/norwich/cj341/05_Forensic_Framework.ppt

http://www.mekabay.com/courses/academic/norwich/cj341/09_Remnants.ppt

http://www.mekabay.com/courses/academic/norwich/cj341/15_Using_Forensic_Utilities.ppt

> What do the people who work with computer forensics do and how do they do it?<

They collect and secure digital evidence for use in analyzing the occurrence, nature, mechanisms and perpetrators of computer security violations, some of which may be crimes. They understand how information is created and stored in different kinds of digital media and they use specialized procedures and programs to safeguard data against damage and to find relevant data. They also understand the legal requirements for proper chain of custody of evidence as well as restrictions on investigative techniques that are required for effective use in legal proceedings, if any.

> What sort of tricks do cyber criminals use to cover their tracks?<

Depending on whether criminals have physical access to computer systems they are manipulating, they can
* use false or temporary identifiers to launch attacks;
* route their attack through several compromised systems to obscure their trail of IP addresses in the packets they generate;
* create IP packets with falsified headers;
* use someone else's compromised ID on the target computer or network;
* falsify or delete log files (if they can gain root access);
* store information in difficult-to-get-to parts of disks such as slack space.

>How do the experts side-step logic bombs and get to the truth?<

Most forensic examiners find out if there is an uninterruptible power supply (UPS) on the computer side of the power cord; if there is not, they pull the plug to stop the computer dead without allowing any shutdown procedures that might result in damage programmed by the criminal. If there is a UPS feeding the computer directly, it may be necessary to do some work with wire cutters inside the computer casing -- assuming there are no booby traps.

Once the computer has been halted, the forensic examiner typically removes the disk drive(s) and makes bit-for-bit images (copies) on to non-erasable media. These copies are preserved as primary evidence along with the original disk drive if possible. It's also possible to make a bit for bit copy onto a similar hard disk for experimental work. Using forensic utilities, the investigators then searches the entire contents of the disk(s) duplicate(s) looking for interesting information. The hard disk may contain a swap file; that can show part or all of the contents of live memory (RAM) at the time of the last copy to disk before the system was halted. The swap file and therefore have evanescent information that would not normally be seen on disk such as display or print buffers, passwords in transit through data communications channels, and so on.

More in the next article.

* * *

A Master’s degree in the management of information assurance in 18 months of online study from Norwich University – see

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2004 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.