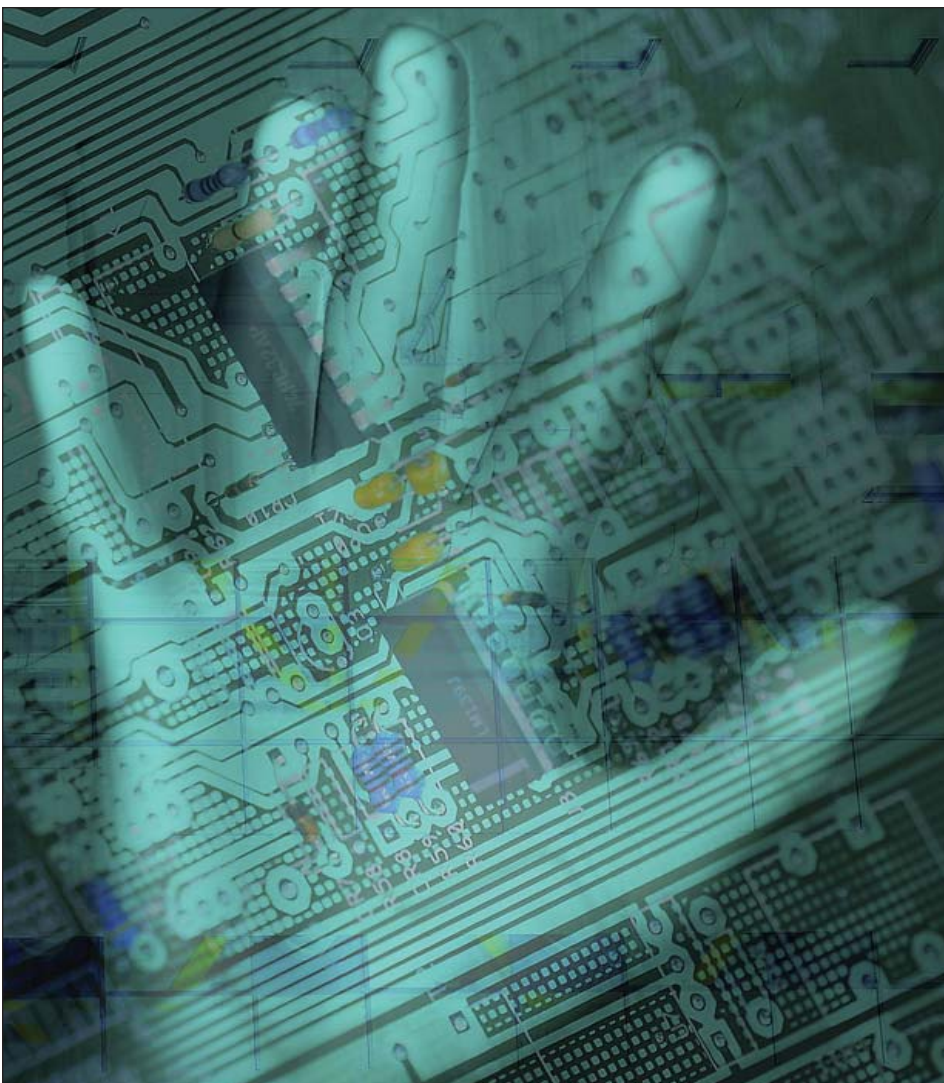


St. Louis Technology News

THE TECHNOLOGY SPIRIT OF ST. LOUIS™

TECHNOLOGY SOLUTIONS AND STRATEGIES FROM ISPIRIAN, SYLLOGISTEKS® AND ULTRATECH

The Dark Side of Forensics



Anti-forensics helps the bad guys destroy digital evidence and evade detection. Or not.

Criminals have long used many techniques to thwart investigators, from wearing gloves to avoid leaving fingerprints to disposing of weapons and other evidence. As electronic data has become key evidence in a wide range of investigations, some wrongdoers have begun using “anti-forensics” in an attempt to cover their tracks — or simply out of spite.

The term “anti-forensics” refers to a variety of software tools and techniques designed to make it difficult for a computer forensic examiner to find suspect data, or to render potential evidence inadmissible in a court of law. While it sounds as though it belongs in the realm of cybercrime, anti-forensics is often found in employment-related cases. Finding evidence of anti-forensics

Continued on page 2

The Dark Side of Forensics

can escalate what would be simple administrative discipline to civil lawsuits or even criminal charges.

“Many investigations hinge upon the use of file system metadata — the details of where a file is stored, how big it is, when it was last modified, etc. Forensic examiners use metadata to find deleted and hidden files, and attorneys use metadata to help prove their case,” said Tom Smith, a forensic scientist with Ispirian Computer Forensics and a member of the American College of Forensic Examiners Institute (ACFEI).

“Anti-forensics tools can be used to hide files and change file system metadata, causing an investigator to overlook crucial evidence. And many of these anti-forensics tools are easy to use and readily available commercially and on hacker Web sites, making it likely that an investigator will run up against this problem in a variety of circumstances.”

How the Bad Guys Hide Evidence

Anti-forensics tools were once the domain of criminals with significant technical know-how. Like hacking tools, however, anti-forensics software has become much more user-friendly, enabling even novices to evade investigators by means of data destruction, hoping to render digital evidence irrecoverable and inadmissible in a court of law. As a result, anti-forensics has grown so rapidly that computer forensic examiners have struggled to keep pace.

Some popular anti-forensics tools are designed to confuse data searches by creating nonsensical metadata. For example, there are tools that can change the timestamp of a file to make it look like it was created in 2047, last accessed in 2022 and last modified in 1963. Because of the vast amount of data stored on the typical hard drive, computer forensic examiners naturally focus their searches on files created or modified during a time period relevant to the investigation. When the timestamp has been manipulated in this manner, searches based on date-related metadata become extremely difficult.

Anti-forensics can also be used to manipulate active files and residual data that would otherwise be recoverable from file slack and unallocated drive space. One popular tool slices up files and inserts them into other files, making it appear that the files are simply corrupted. Without knowledge of how the file was split up, the computer forensic examiner cannot easily re-create the data sets.

“Digital information can also be inserted into files where you wouldn’t expect to find that kind of data,” said Smith. “Just as a criminal might disguise his appearance, these techniques disguise evidence as images, videos and other types of files. They can be stored and even transmitted without simple detection.”

However, wily criminals don’t have to use anti-forensics software to hinder investigations. Bad guys can hide data

quite easily by partitioning a hard drive and encrypting the resulting partitions, then partitioning and encrypting again.

“Forensics tools may view the information on the second encrypted partition as random digital junk,” Smith said. “This illustrates why forensic examiners must not be reliant solely on computer programs or scripts to perform their investigations, but must have a thorough understanding of file systems, operating systems and obfuscation methods used by the wrongdoers.”

How Investigators Fight Back

St. Louis-based Ispirian’s experienced computer forensic examiners are wise to the ways of anti-forensics. However, anti-forensics can still slow down investigations to the point that key evidence is uncovered too late or at too great an expense to assist an attorney with a case. Worse, investigators may never be able to determine who manipulated the metadata, making it difficult to prove spoliation of evidence.

“Luckily, the same problems that make e-discovery challenging also make anti-forensics difficult,” said Smith. “Today’s hard drives can store so much data that it’s extremely difficult for the bad actor to find and alter all of the individual files that can make or break a case. Our experts have the knowledge and experience to find any evidence left behind.”

It’s true that an individual engaged in ongoing fraudulent activity could use anti-forensics deliberately to hide incriminating evidence along the way. While that could make serious crimes difficult to uncover, Smith is confident that computer forensic experts will ultimately prevail.

“Yes, the bad guys are getting pretty sophisticated, but the good guys are learning new tricks as well,” Smith said. “As anti-forensic tools and techniques become more prevalent and easier to use, computer forensic examiners are finding ways to ensure that key electronic evidence can be recovered and lawbreakers can be brought to justice.”

St. Louis Technology News

Copyright © 2009 CMS Special Interest Publications.

All rights reserved.

Editorial Correspondence:

4941 S. 78th E. Ave., Tulsa, OK 74145

Phone (800) 726-7667

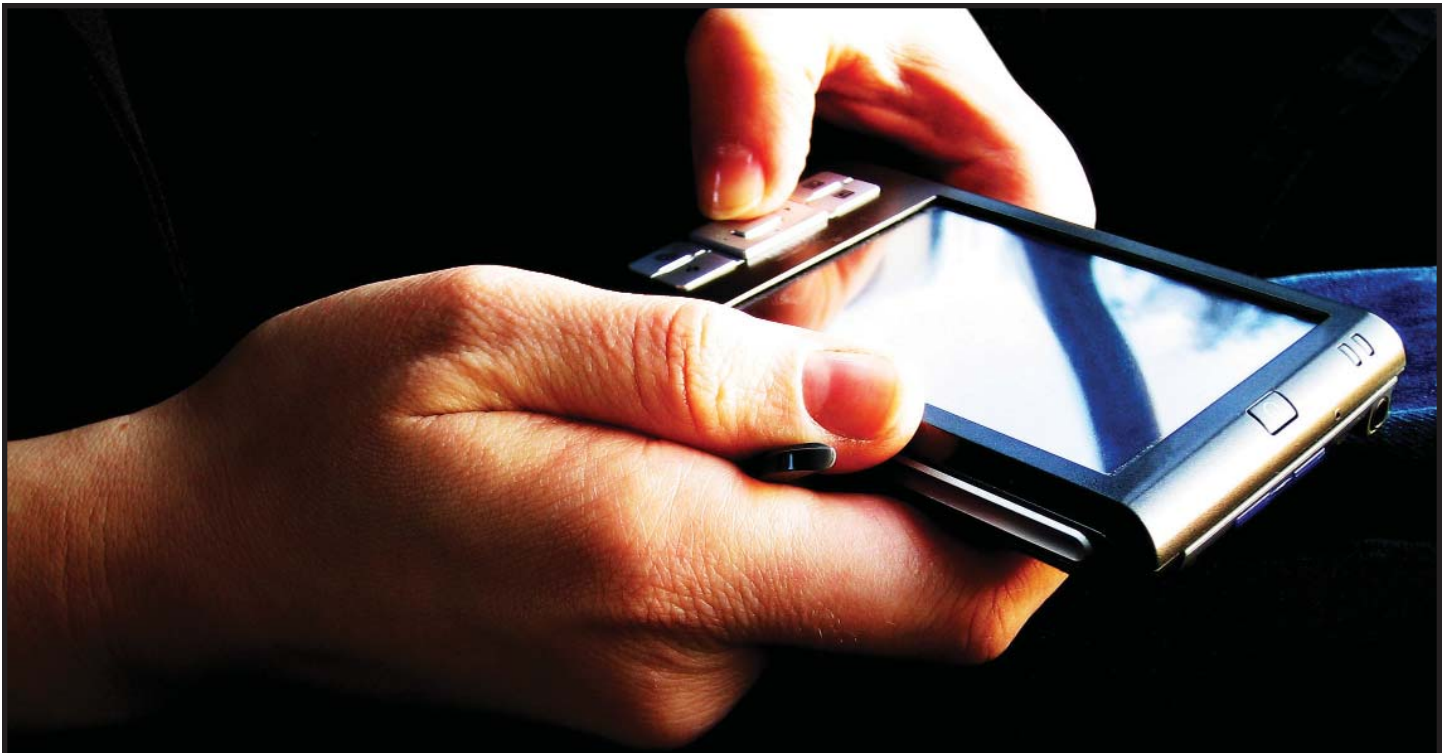
Fax (918) 270-7134

Change of Address:

Send updated address label information to the above address.

Some parts of this publication may be reprinted or reproduced in nonprofit or internal-use publications with advance written permission.

St. Louis Technology News is published by CMS Special Interest Publications. Printed in the U.S.A. Product names may be trademarks of their respective companies.



Funny, it doesn't look like a smoking gun.

Cell phones, GPSs, PDAs and other handheld devices have become practically indispensable as business and personal productivity tools these days. In many cases, they can also be repositories of a variety of dirty little secrets in the form of data, text messages and photographs. As such, they have become increasingly important in a broad range of criminal and civil investigations.

Handheld devices are really tiny computers with their own operating systems, file systems, file formats and methods of communication.

Performing a forensic examination on one of these devices takes special software and special knowledge of the way they work, as well as where possible evidence could be stored.

Ispirian Incorporated's computer forensic experts have the specialized tools, training and expertise to properly identify, collect and protect evidentiary data from handheld devices. Call us today to learn more.



*Ispirian is a member
of the High Technology
Crime Investigation
Association (HTCIA).*



Ispirian Incorporated
Chesterfield, MO 63017
Ph: 636.898.1093
Fax: 636.594.2000