VERE SOFTWARE
INVESTIGATIVE TOOLS

Build Context into Your Digital Forensic Exam With Online Evidence

Written by

Vere Software

Contents

Build Context into Your Digital Forensic Exam with Online Evidence

Investigation and Forensics Requirements

Digital forensics is becoming increasingly important in on-site previews. Whether routine checks of offenders on probation or parole, search warrant execution, or in the corporate environment as part of incident response or workplace investigation, both law enforcement and corporate personnel need access to computers when they may contain evidence.

However, “dead” forensics – and even “live” forensics – only capture part of the story of a suspect's activities. Artifacts related to the Internet, social networking sites, online searches, and webmail uncover what the suspect did at just a specific point in time, while live forensics capture what's occurring in the computer's memory (but not on the suspect's online sites) while it is running.

To get a full picture, online evidence is necessary. In fact, the documentation of internet-based evidence is the logical extension of digital forensic examinations.

Social Networking Activity

Social networking updates can reveal not just the subject's activities, but also his or her personal network of friends and associates. Investigators need to be able to document a subject's online activity and compare it to other activities, including cell phone traffic and computer activity. Online activity during a time in question could mean an alibi – or an associate trying to provide a cover; conversely, a break from normal online activity patterns might be compared to computer and cell phone activity to see whether the subject's activity changed there, too.

Cell Phone Evidence Extraction

Data extraction from cell phones is not always easy to document. No commercially available mobile forensic tool recovers all the evidence from a phone, especially when it has been damaged or the data deleted. Mobile forensic examiners have adapted a number of free tools, both online and offline, to adjust for such discrepancies, but because these tools were not made for digital forensics, they have few or no documentation features. As a result, they are easier for savvy defense attorneys to challenge in court.

SOHO Router Interrogation

Not only is it important to document evidence of recent social networking activity; at home, the subject may also have hidden wireless devices routed through their SOHO network. Investigators on-site are often required to determine and document router settings. However, accessing routers and documenting actions usually consists of photographing the computer screen at each step. This is awkward and time-consuming, and as a result, many investigators don't bother.

Vere Software Has the Capabilities You Need

Extend your digital forensics investigation to the Internet. Vere Software's premier product WebCase helps investigators to:

- ✓ verify website archives and social networking artifacts located during a forensic exam.
- ✓ document the current state of those websites and social profiles.
- ✓ compare properly documented online activity to other sources of information collected in the investigation.

WebCase's video function further allows investigators to **record cell phone data extraction** and **SOHO router interrogation**, thereby providing a record of actions that would previously have gone undocumented. This provides investigators with an additional level of process security and documentation.

Context Through Integrated Electronic Exhibits

WebCase automatically dates and time stamps each collected item within a case and hashes the items as they are collected. WebCase's attach function further allows the investigator to store and document other digital evidence items, treating attached files in the same manner it treats other evidence.

This provides the investigator with added assurance that the evidence is documented to an acceptable legal level. The ability to integrate electronic files from many sources – audio and video recordings, word processor documents, spreadsheets, and other digital evidence files – enables investigators to prepare a fully contextual case file, one which enables adequate comparison of cached online activities with the current state of websites and social profiles.

Context Through Full Case Histories

WebCase enables investigators to maintain complete case histories with instant access to all related case information. Forensic examiners can keep collected case data separated and accessible only through their individual user logins. This way, they can document cases without fearing cross contamination.

Context Through Easy to Understand Reports

Preparing internet-based evidence investigation reports the old-fashioned way often requires a major time commitment. With WebCase, investigators simply click a button to generate a browser-based report containing a comprehensive chronology of all events and activities, as well as the evidence that was gathered and any investigators' comments.

WebCase’s reporting function complements existing forensic reports by providing an additional level of evidence collection and documentation. WebCase reports can quickly be burned to CD/DVD right from WebCase without the use of third party applications. This way, examiners can collect data from the Internet on a separate computer, then transfer it to the forensic computer without fear of compromising the forensic machine by going online.

This report, which is similar to those generated from digital forensic tools, contains the collected items along with any attachments. Its easy to view, easy to understand format improves the process of explaining a case to attorneys, judges and jurors.

Vere Software: The Internet Investigations Leader

Vere Software Solutions for Digital Forensics Examinations

Using Vere Software's solutions, you can extend your digital investigations through individual case management and documentation tools. A recognized leader in online investigation documentation, Vere Software's founders based their tools on their years of experience in online investigations and reporting.

Vere Software's proven solutions can help reduce time spent on investigations, improve legal defensibility of online evidence documentation, and help you successfully manage online investigations while reducing employee time and costs. They also reduce the risk of improperly documented internet-based evidence by eliminating the distractions and complexity of documenting online evidence with individual tools not built for investigations.

When the courts review your process, don't be stressed. Vere Software tools place online investigations and documentation fully under your control.

For More Information

To learn more, visit http://www.veresoftware.com/

About Vere Software

Now more than ever, organizations need to work smart and improve efficiency. Vere Software creates and supports online investigations—helping our customers solve every day Internet Investigations challenges faster and easier. Visit www.veresoftware.com for more information.

Contacting Vere Software

VERE SOFTWARE
INVESTIGATIVE TOOLS

PHONE	888-432-4445 (United States and Canada) If you are located outside North America, you can find our reseller on our Web site.
E-MAIL	sales@veresoftware.com
MAIL	Vere Software 4790 Caughlin Parkway #323 Reno, Nevada 89519 USA
WEB SITE	www.veresoftware.com

Contacting Vere Software Support

Vere Software Support is available to customers who have a trial version of a Vere Software product or who have purchased a commercial version and have a valid maintenance agreement.

Vere Software Support provides assistance with our Web self-service.

Visit our forum at http://www.veresoftware.com/forum

Our website gives users of Vere Software products the ability to:

- Search Vere Software's online FAQ
- Download the latest releases, documentation, and patches for Vere Software products
- Request email support
- Manage existing support cases

Copyright Notice

If you have any questions regarding your potential use of this material, contact:

Vere Software
Attn: Legal Department
4790 Caughlin Parkway #323
Reno, Nevada 89519
www.veresoftware.com
email: info@veresoftware.com

Refer to our Web site for regional and international office information.

Trademarks

WebCase "Make the Internet your regular beat" and the Vere Software logo, are trademarks and registered trademarks of Vere Software in the United States of America and other countries. Other trademarks and registered trademarks used in this guide are property of their respective owners.

January 2011