Forensic Investigation of Employee Internet Activity

Introduction

Computer or digital forensics involve forensic investigations that recover data from computers and other technological devices, such as servers, to solve a crime or find evidence of misconduct. Depending upon the employer and the investigation, forensic investigators may have to examine a single computer hard drive, a corporate e-mail server, a large network, or terabytes of data. Some common situations that call for forensic investigations are intellectual property theft, employment disputes, fraud, inappropriate e-mail and Internet use in the workplace, and violations of regulatory compliance laws. These situations pose greater risks for any company. Losses are more than financial in nature and can potentially damage the company's reputation.

Increased dependence on the Internet and computers among corporate organizations and government institutions have extensively resulted in a rise in cyber crime and fraud. As a result, computer forensic tools are primarily used in both criminal law and private investigations to determine, examine, and recover evidence or digital data related to computer fraud and crime, as well as civil matters. For investigations of Internet activity, finding the right tool may be a challenge. Forensic investigators need a tool that can read a variety of raw log files and quickly analyze them. However, many Web log file tools only read their own specific log files and do not break down the data into elements such as visits, hits, and Web content categories.

Some tools are limited to the examination of the user's computer hard drive, for example, a tool that is used to read local files containing the user's Web browsing history and cache, or an undetectable keylogger that captures keyboard keystrokes. Ideally, the user's Web activity log files should reside outside of his computer system, for example, on a server, providing a critical source of evidence versus data that is analyzed locally and could potentially be wiped or tampered with. Forensic investigators would want to use a server-based tool along with their user system tool. This tool would provide detailed user Internet activity, verify any evidence investigators find locally, and identify any gaps or inconsistencies in the local data. With a server-based tool, historical log data exists, and depending on a company's archive policy, investigators can quickly "go back in time" to review past patterns and searches in Internet activity.

To support your forensic investigations of Internet use, Wavecrest offers Cyfin, an advanced forensic log file analyzer that processes a multitude of log file formats, allows you to run quick ad hoc reports, produces categorized audit reports detailing individual user Web activity, stores log file data on a server, and much more.

Benefits of a Cyfin Implementation

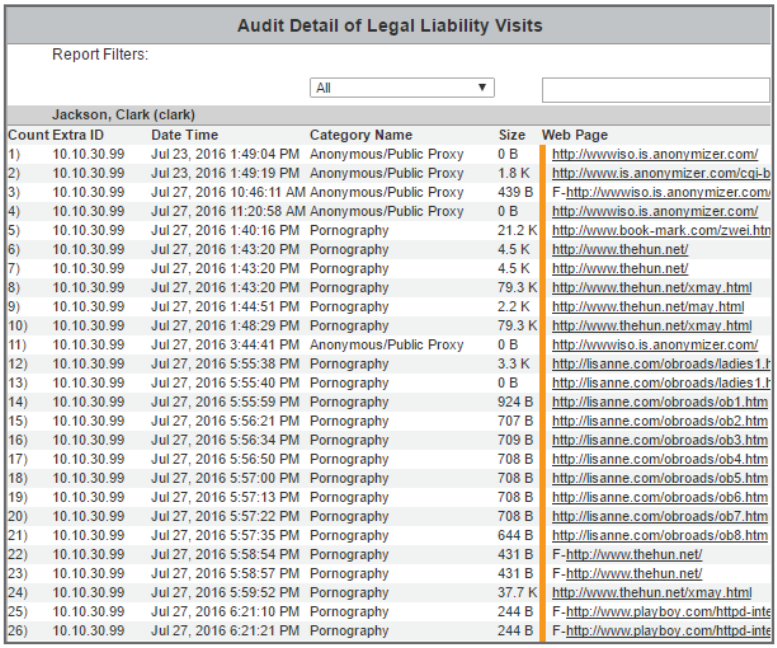
Ease of Installation

Cyfin is easily installed by starting a wizard and following the on-screen instructions. After installing the product, a few steps will get the product up and running. The screens are intuitive, reducing your setup time and giving you access to information as quickly as possible.

Detailed Forensic Reports

Cyfin's employee Web-use forensic reports deliver a comprehensive analysis of user activity including their visits, search terms, and inappropriate sites. These low-level audit reports allow forensic investigators to get a detailed analysis of a single user's visits including the site's category and full URL, view search terms that a user entered on popular search sites such as Google, view users who accessed sites that pose a legal liability risk, and see specific URLs to which a user was denied.

The forensic reports include User Audit Detail, Category Audit Detail, Search Terms Audit Detail, Legal Liability Detail, and Denied Detail and can be quickly run as ad hoc reports saving you time in your investigation. As shown in the figures below, report elements include user, IP address, date/time, category name, URL, search engine, and search term. Reports also provide the number of visits by hour, category classification, and category, as well as total visits/hits, total denied visits, and total legal liability visits/hits.



Audit Detail of Legal Liability Visits

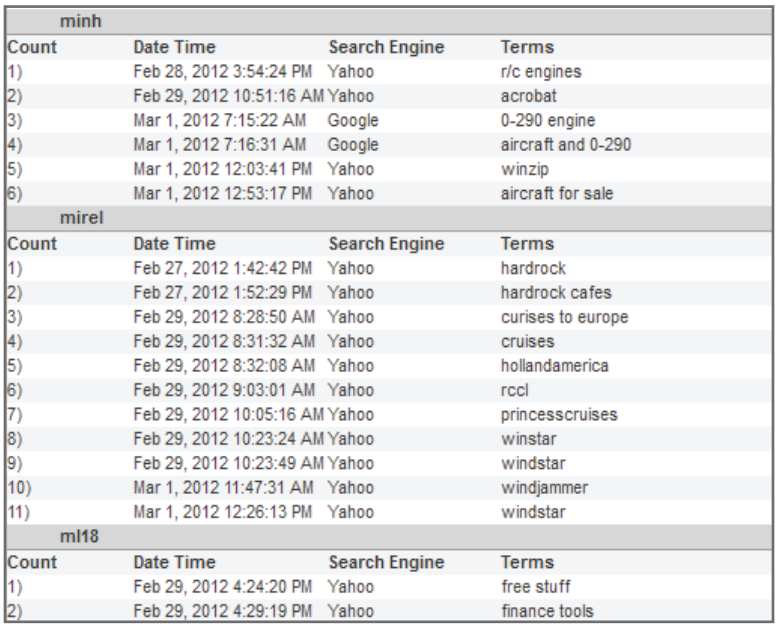
Report Filters:

All

Jackson, Clark (clark)

Count	Extra ID	Date Time	Category Name	Size	Web Page
1)	10.10.30.99	Jul 23, 2016 1:49:04 PM	Anonymous/Public Proxy	0 B	http://wwwiso.is.anonymizer.com/
2)	10.10.30.99	Jul 23, 2016 1:49:19 PM	Anonymous/Public Proxy	1.8 K	http://www.is.anonymizer.com/cgi-b
3)	10.10.30.99	Jul 27, 2016 10:46:11 AM	Anonymous/Public Proxy	439 B	F-http://wwwiso.is.anonymizer.com/
4)	10.10.30.99	Jul 27, 2016 11:20:58 AM	Anonymous/Public Proxy	0 B	http://wwwiso.is.anonymizer.com/
5)	10.10.30.99	Jul 27, 2016 1:40:16 PM	Pornography	21.2 K	http://www.book-mark.com/zwei.htn
6)	10.10.30.99	Jul 27, 2016 1:43:20 PM	Pornography	4.5 K	http://www.thehun.net/
7)	10.10.30.99	Jul 27, 2016 1:43:20 PM	Pornography	4.5 K	http://www.thehun.net/
8)	10.10.30.99	Jul 27, 2016 1:43:20 PM	Pornography	79.3 K	http://www.thehun.net/xmay.html
9)	10.10.30.99	Jul 27, 2016 1:44:51 PM	Pornography	2.2 K	http://www.thehun.net/may.html
10)	10.10.30.99	Jul 27, 2016 1:48:29 PM	Pornography	79.3 K	http://www.thehun.net/xmay.html
11)	10.10.30.99	Jul 27, 2016 3:44:41 PM	Anonymous/Public Proxy	0 B	http://wwwiso.is.anonymizer.com/
12)	10.10.30.99	Jul 27, 2016 5:55:38 PM	Pornography	3.3 K	http://lisanne.com/obroads/ladies1.h
13)	10.10.30.99	Jul 27, 2016 5:55:40 PM	Pornography	0 B	http://lisanne.com/obroads/ladies1.h
14)	10.10.30.99	Jul 27, 2016 5:55:59 PM	Pornography	924 B	http://lisanne.com/obroads/ob1.htm
15)	10.10.30.99	Jul 27, 2016 5:56:21 PM	Pornography	707 B	http://lisanne.com/obroads/ob2.htm
16)	10.10.30.99	Jul 27, 2016 5:56:34 PM	Pornography	709 B	http://lisanne.com/obroads/ob3.htm
17)	10.10.30.99	Jul 27, 2016 5:56:50 PM	Pornography	708 B	http://lisanne.com/obroads/ob4.htm
18)	10.10.30.99	Jul 27, 2016 5:57:00 PM	Pornography	708 B	http://lisanne.com/obroads/ob5.htm
19)	10.10.30.99	Jul 27, 2016 5:57:13 PM	Pornography	708 B	http://lisanne.com/obroads/ob6.htm
20)	10.10.30.99	Jul 27, 2016 5:57:22 PM	Pornography	708 B	http://lisanne.com/obroads/ob7.htm
21)	10.10.30.99	Jul 27, 2016 5:57:35 PM	Pornography	644 B	http://lisanne.com/obroads/ob8.htm
22)	10.10.30.99	Jul 27, 2016 5:58:54 PM	Pornography	431 B	F-http://www.thehun.net/
23)	10.10.30.99	Jul 27, 2016 5:58:57 PM	Pornography	431 B	F-http://www.thehun.net/
24)	10.10.30.99	Jul 27, 2016 5:59:52 PM	Pornography	37.7 K	http://www.thehun.net/xmay.html
25)	10.10.30.99	Jul 27, 2016 6:21:10 PM	Pornography	244 B	F-http://www.playboy.com/httpd-inte
26)	10.10.30.99	Jul 27, 2016 6:21:21 PM	Pornography	244 B	F-http://www.playboy.com/httpd-inte

Legal Liability Detail Report



minh			
Count	Date Time	Search Engine	Terms
1)	Feb 28, 2012 3:54:24 PM	Yahoo	r/c engines
2)	Feb 29, 2012 10:51:16 AM	Yahoo	acrobat
3)	Mar 1, 2012 7:15:22 AM	Google	0-290 engine
4)	Mar 1, 2012 7:16:31 AM	Google	aircraft and 0-290
5)	Mar 1, 2012 12:03:41 PM	Yahoo	winzip
6)	Mar 1, 2012 12:53:17 PM	Yahoo	aircraft for sale
mirel			
Count	Date Time	Search Engine	Terms
1)	Feb 27, 2012 1:42:42 PM	Yahoo	hardrock
2)	Feb 27, 2012 1:52:29 PM	Yahoo	hardrock cafes
3)	Feb 29, 2012 8:28:50 AM	Yahoo	curises to europe
4)	Feb 29, 2012 8:31:32 AM	Yahoo	cruises
5)	Feb 29, 2012 8:32:08 AM	Yahoo	hollandamerica
6)	Feb 29, 2012 9:03:01 AM	Yahoo	rccl
7)	Feb 29, 2012 10:05:16 AM	Yahoo	princesscruises
8)	Feb 29, 2012 10:23:24 AM	Yahoo	winstar
9)	Feb 29, 2012 10:23:49 AM	Yahoo	windstar
10)	Mar 1, 2012 11:47:31 AM	Yahoo	windjammer
11)	Mar 1, 2012 12:26:13 PM	Yahoo	windstar
ml18			
Count	Date Time	Search Engine	Terms
1)	Feb 29, 2012 4:24:20 PM	Yahoo	free stuff
2)	Feb 29, 2012 4:29:19 PM	Yahoo	finance tools

Search Terms Audit Detail Report

Server-Based Evidence

Cyfin is server-based where log files are stored on the server and do not reside on the user's system. Since the server would be restricted to IT administrators or other authorized personnel, the log data on the server is a critical source of Web-use evidence for the investigator, especially if the user's system has been tampered with.

Multiple-Log-File Analyzer

Cyfin is designed to process and analyze terabytes of log data daily. It is log file independent meaning that it can process a multitude of log file formats regardless of proxy server, firewall, or gateway device. Cyfin's log file analyzer is wizard-driven providing automatic log file analysis and detection, that is, it automates the process of importing log data from hundreds of common network devices. The data is transformed into useful information to deliver meaningful, detailed reports.

URL Categorization

Categorization is the process of determining the types of content provided by Web sites and grouping those sites into content categories. Typical Web content categories are Shopping, Sports, and Financial. Those that address legal liability risks include Fantasy Sports, Gambling, Illegal Drugs, Malware, and Pornography. The Wavecrest reporting process assigns categories to individual Web sites for use in the report-generation process. For example, the category assigned to www.espn.com is "Sports." When you create reports, you can choose the specific category (or categories) whose Web activity you want to assess. With 70-plus standard categories and an unlimited number of custom categories, Cyfin categorizes all Web activity so that investigators can easily find the evidence they need.

Licensing Per Investigation

Wavecrest understands that forensic investigations can be sporadic assignments, and investigators are only tasked when a user has come under suspicion from a complaint or a common situation calls for a forensic investigation. As mentioned earlier, these situations include intellectual property theft, fraud, and inappropriate e-mail and Internet use in the workplace. Therefore, our licensing model is flexible and highly customizable based on investigative case or product usage.

Conclusion

Due to increasing security concerns across different industries, such as law enforcement, defense, banking, health care, information technology, and education, the market for computer or digital forensics is witnessing substantial growth. Wavecrest has over 20 years of proven history addressing forensic requirements across various industries. Cyfin is a court-cited, forensic investigation solution capable of significantly reducing case investigative times by allowing you to gather and analyze pertinent evidence in a rapid, cost-effective manner.

Whether you are a large organization with an internal Investigations department or an independent Forensics Investigator, you will experience a significant increase in productivity which equates to decreased cost per investigation. In addition to identifying evidence faster with Cyfin, pinpoint supporting relevant activity that may be of value and have more time to focus on the actual investigation.

About Wavecrest Computing

Since 1996, Wavecrest Computing has provided business and government clients with reliable, accurate employee Web-access security, employee Web-use monitoring and analytics, and Cloud Access Security Broker (CASB) solutions. IT specialists, HR professionals, and business managers trust Wavecrest's Cyfin® and CyBlock® products to manage employee Internet usage with today's distributed workforce in mind–reducing liability risks, improving productivity, managing cloud services, saving bandwidth, and controlling costs.

Wavecrest has over 3,000 clients worldwide, including Blue Cross Blue Shield, MillerCoors, National Grid, Rolex, Siemens, Superior Court of California, U.S. Dept. of Veterans Affairs, and a growing list of global enterprises and government agencies. For more information on our company, products, and partners, visit www.wavecrest.net.

WAVECREST
COMPUTING

Wavecrest Computing
904 East New Haven Avenue
Melbourne, FL 32901
toll-free: 877-442-9346
voice: 321-953-5351
fax: 321-953-5350