# Advanced Forensic Log File Analyzer

*Cyfin's employee Web-use forensic reports help you find relevant evidence faster, dramatically reducing the time to analyze terabytes of log data. Comprehensive, actionable, and accurate, these forensic reports supply specific Web-use information with reliable metrics, detailed audit reports, and Smart Engine analytics to anyone in the legal community.*

## Smart Engine Analytics

- Makes technical data easy to consume and manager-ready.
- Utilizes precise algorithms to present accurate and up-to-date Web-use data.
- Distinguishes between user clicks (visits) and unsolicited traffic (hits).
- Analyzes large volumes of data over long periods of time.

**Audit Detail For ID "Technical Services Department/Banning, Payton (payton)"**

Report Filters: All

Banning, Payton (payton)

| Count Extra ID | | Date Time | Category Name | Size | Web Page |
|---|---|---|---|---|---|
| 1) | 10.10.30.99 | Jul 27, 2016 6:35:43 PM | Video Streaming | 232 B | http://youtube.com/fido-1/66320-1?catalo |
| 2) | 10.10.30.99 | Jul 27, 2016 6:36:32 PM | Video Streaming | 2.5 K | http://youtube.com/fido-1/numitm-10/262 |
| 3) | 10.10.30.99 | Jul 27, 2016 6:39:11 PM | Video Streaming | 8.2 K | http://youtube.com/fido-1/1966609-99600 |
| 4) | 10.10.30.99 | Jul 27, 2016 6:39:43 PM | Video Streaming | 126 B | http://youtube.com/fido-1/2626561-1 |
| 5) | 10.10.30.99 | Jul 27, 2016 6:40:35 PM | Video Streaming | 14 B | http://youtube.com/fido-1/numitm- 10/262 |
| 6) | 10.10.30.99 | Jul 27, 2016 6:41:13 PM | Search Engines | 1.6 K | http://www.algonet.se/htbin/wrapcount?u |
| 7) | 10.10.30.99 | Jul 27, 2016 6:41:13 PM | Search Engines | 12.8 K | http://www.algonet.se/~lewa/bbw.html |
| 8) | 10.10.30.99 | Jul 27, 2016 6:41:23 PM | Search Engines | 175 B | http://www.algonet.se/htbin/wrapcount?u |
| 9) | 10.10.30.99 | Jul 27, 2016 6:43:05 PM | IT Services | 2.4 K | http://hem.passagen.se/lewa/lew.html |
| 10) | 10.10.30.99 | Jul 27, 2016 6:43:14 PM | IT Services | 3.2 K | http://hem.passagen.se/lewa/ew.html |
| 11) | 10.10.30.99 | Jul 27, 2016 6:46:32 PM | Search Engines | 1.8 K | http://www.algonet.se/~lewa/bbwhem.htm |
| 12) | 10.10.30.99 | Jul 27, 2016 6:46:37 PM | Search Engines | 154 B | http://www.algonet.se/htbin/wrapcount?u |
| 13) | 10.10.30.99 | Jul 27, 2016 6:47:40 PM | Social Media | 932 B | F-http://linkedin.com/fido-1/numref-6/135 |
| 14) | 10.10.30.99 | Jul 27, 2016 6:47:48 PM | High Tech | 5.3 K | http://hpcc920.external.hp.com/ |
| 15) | 10.10.30.99 | Jul 27, 2016 6:47:59 PM | High Tech | 226 B | http://www.hp.com/ |
| 16) | 10.10.30.99 | Jul 27, 2016 6:48:06 PM | Social Media | 67.3 K | F-http://linkedin.com/fido-1/numitm-10/13 |
| 17) | 10.10.30.99 | Jul 27, 2016 6:48:24 PM | Education/Reference | 22.8 K | http://www.info.cornell.edu/cuhomepage/ |
| 18) | 10.10.30.99 | Jul 27, 2016 6:52:15 PM | Education/Reference | 163 B | http://www.cornell.edu/zchimes/home.htr |

Goodridge, Marianne (mgood)

| Count Extra ID | | Date Time | Search Engine | Size | Terms |
|---|---|---|---|---|---|
| 1) | 10.10.30.90 | Jul 28, 2017 1:22:56 PM | Yahoo | 310 B | c.j. midi productions |
| 2) | 10.10.30.90 | Jul 28, 2017 3:53:36 PM | Yahoo | 3.1 K | midihits.com |
| 3) | 10.10.30.90 | Jul 28, 2017 3:53:58 PM | Yahoo | 297 B | midihits |

AYoung-Shee, Minh (minh)

| Count Extra ID | | Date Time | Search Engine | Size | Terms |
|---|---|---|---|---|---|
| 1) | 10.10.20.50 | Jul 28, 2017 3:54:24 PM | Yahoo | 6.9 K | r/c engines |
| 2) | 10.10.20.50 | Jul 29, 2017 7:15:22 AM | Google | 15 K | 0-290 engine |
| 3) | 10.10.20.50 | Jul 29, 2017 7:16:31 AM | Google | 15.3 K | aircraft and 0-290 |
| 4) | 10.10.20.50 | Jul 29, 2017 12:03:41 PM | Yahoo | 6.4 K | winzip |
| 5) | 10.10.20.50 | Jul 29, 2017 12:53:17 PM | Yahoo | 8.9 K | aircraft for sale |

Loftug, Mirel K. (mirel)

| Count Extra ID | | Date Time | Search Engine | Size | Terms |
|---|---|---|---|---|---|
| 1) | 10.10.30.109 | Jul 27, 2017 1:42:42 PM | Yahoo | 9.3 K | hardrock |
| 2) | 10.10.30.109 | Jul 27, 2017 1:52:29 PM | Yahoo | 303 B | hardrock cafes |
| 3) | 10.10.30.109 | Jul 29, 2017 11:47:31 AM | Yahoo | 8.5 K | windjammer |
| 4) | 10.10.30.109 | Jul 29, 2017 12:26:13 PM | Yahoo | 6.2 K | windstar |

Litt Monica R. (mlitt)

| Count Extra ID | | Date Time | Search Engine | Size | Terms |
|---|---|---|---|---|---|
| 1) | 10.10.30.215 | Jul 27, 2017 9:13:09 AM | Yahoo | 10.1 K | web page design |
| 2) | 10.10.30.215 | Jul 27, 2017 9:24:36 AM | Yahoo | 10.2 K | corel |
| 3) | 10.10.30.215 | Jul 27, 2017 5:31:14 PM | Yahoo | 302 B | lingonberries |

Morgan, Claudia (morganc)

| Count Extra ID | | Date Time | Search Engine | Size | Terms |
|---|---|---|---|---|---|
| 1) | 10.10.30.19 | Jul 23, 2017 8:14:35 AM | Yahoo | 4.8 K | company |
| 2) | 10.10.30.19 | Jul 27, 2017 1:52:40 PM | Yahoo | 307 B | the frankline mint |
| 3) | 10.10.30.19 | Jul 27, 2017 2:11:50 PM | Yahoo | 315 B | franklin mint collectible |

## Detailed User Audits

- Show activity by entire organization, groups, users, and categories.
- Get accurate, actionable, manager-ready detailed reports.
- See the exact search terms entered by users and their search time.
- Determine how much time a user spends online.
- View Web content most frequently visited by a user.
- Dramatically reduce analysis time of your organization's Web use.
- Comply with government and industry regulations such as CIPA and HIPAA.

**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- |
| 3) | 10.10.30.99 | Jul 27, 2016 10:46:11 AM | Anonymous/Public Proxy | 439 B | F-http://wwwiso.is.anonymizer.con |
| 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.h |
| 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://www.anonymizer.com/ |
| 12) | 10.10.30.99 | Jul 27, 2016 5:55:38 PM | Pornography | 3.3 K | http://lisanne.com/obroads/ladies1 |
| 13) | 10.10.30.99 | Jul 27, 2016 5:55:40 PM | Pornography | 0 B | http://lisanne.com/obroads/ladies1 |
| 14) | 10.10.30.99 | Jul 27, 2016 5:55:59 PM | Pornography | 924 B | http://lisanne.com/obroads/ob1.htr |
| 15) | 10.10.30.99 | Jul 27, 2016 5:56:21 PM | Pornography | 707 B | http://lisanne.com/obroads/ob2.htr |
| 16) | 10.10.30.99 | Jul 27, 2016 5:56:34 PM | Pornography | 709 B | http://lisanne.com/obroads/ob3.htr |
| 17) | 10.10.30.99 | Jul 27, 2016 5:56:50 PM | Pornography | 708 B | http://lisanne.com/obroads/ob4.htr |
| 18) | 10.10.30.99 | Jul 27, 2016 5:57:00 PM | Pornography | 708 B | http://lisanne.com/obroads/ob5.htr |

## Hits vs. Visits

- Most accurate visit algorithm in the industry.
- Visits give uncluttered, relevant Web activity detail based on user clicks.
- Visits are a critical component to understanding human behavior.
- Hits consist of unsolicited traffic and are not a reliable tracking metric on their own.

## Cyfin Forensic Features

- Quick and easy setup and implementation.
- Time-saving, categorized audit reports detailing individual user Web activity.
- Ability to run ad hoc reports increasing analysis speed.
- Server-based, storing log file data and providing critical evidence not residing on user's system.
- Log file independent, analyzing a multitude of log file formats from different systems.
- Highly customizable licensing based on investigative case or usage.

## Reliable Source of Evidence

- Ability to utilize various secure gateways for evidence.
- Court-cited investigation platform.
- 25+ years' proven investigation history.
- Trusted by large government and commercial organizations such as:
  - John Hopkins
  - Health Choice Network
  - Canadian National Railway
  - U.S. Postal Service Office of Inspector General

## Audit Detail Reports

| User Audit Detail | Get a detailed analysis of a single user or IP. |
|---|---|
| Category Audit Detail | Get a detailed analysis of a user's activity in a particular category. |
| Search Terms Audit Detail | View search terms that a user entered on popular search sites. |
| Legal Liability Detail | View the sites accessed by a user that pose a legal liability risk. |
| Denied Detail | View the specific URLs to which a user was denied access. |

## Installation & Eval Support

When needed, Wavecrest provides consultation and advice via telephone, live chat, remote, or e-mail at no charge during the free trial period.

## Flexible VM Deployment

Cyfin Forensic Virtual Appliance is ready to be downloaded and installed on your VM server. We support both VMware and Microsoft Hyper-V environments. Our VMware-compatible files can be imported into many VM systems in the industry.

Cyfin Forensic Virtual Appliance can also be deployed on Hyper-V which is built into Windows versions 8 and later, a common operating system that you are already familiar with. Hyper-V is also included in Windows Server. There is nothing to purchase when deploying on Hyper-V.

*Since 1996, Wavecrest Computing has provided business and government clients with reliable, accurate employee Web-access security, monitoring, and analytics 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–monitoring VPN use, following roaming and remote users, managing and monitoring Web usage for hybrid work environments, comprehensive reporting on Microsoft 365 use, and more. Focused on our customer's needs–reducing liability risks, improving productivity, managing cloud services, saving bandwidth, and controlling costs. Wavecrest has clients worldwide, including Canadian National Railway, Johns Hopkins, Goodyear, USPS Office of Inspector General, Chevron, Health Choice Network, and a growing list of enterprises and government agencies. For more information on our company, products, and partners, visit www.wavecrest.net.*

**Wavecrest Computing**
904 East New Haven Avenue
Melbourne, FL 32901
toll-free: 877-442-9346
voice: 321-953-5351
sales@wavecrest.net

**www.wavecrest.net**