Forensic Analyzer

Input Log Files Configuration Files Time Filter Debug Level Help

Forensic Analyzer Parameters:

Input Log Files: --input=apache-access1000000.log=APACHE-ACCESS1000000

Config Files: --conf=associatedActivitiesAcrossAllLogs.conf

Fixed & Time: --notail --parseEventTime --parsedTimeOrder --debug=3

Optional Params: --intevents

START ANALYZING

List of activities across all log files by IP:

54.204.185.160:
lide.cb.cz 54.204.185.160 - - [22/Jan/2017:11:02:14 +0100] "GET /
lide.cb.cz 54.204.185.160 - - [22/Jan/2017:11:02:14 +0100] "GET /
lide.cb.cz 54.204.185.160 - - [30/Jan/2017:11:02:14 +0100] "GET /
lide.cb.cz 54.204.185.160 - - [30/Jan/2017:11:02:14 +0100] "GET /

82.142.105.1:
cb.cz 82.142.105.1 - - [24/Jan/2017:15:01:58 +0100] "GET /praha4/velryba/ HTTP/1.1" 200 7130
cb.cz 82.142.105.1 - - [24/Jan/2017:15:02:00 +0100] "GET /praha4/velryba/wp-content/themes/twentythirteen/genericons/genericons.css?ver=3.03 HTTP/1.1" 200 19329
cb.cz 82.142.105.1 - - [24/Jan/2017:15:02:00 +0100] "GET /praha4/velryba/wp-content/themes/twentythirteen/style.css?ver=2013-07-18 HTTP/1.1" 200 11142
cb.cz 82.142.105.1 - - [24/Jan/2017:15:02:00 +0100] "GET /praha4/velryba/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1 HTTP/1.1" 200 4014
cb.cz 82.142.105.1 - - [24/Jan/2017:15:02:00 +0100] "GET /praha4/velryba/wp-includes/js/jquery/jquery.js?ver=1.12.4 HTTP/1.1" 200 33766
cb.cz 82.142.105.1 - - [24/Jan/2017:15:02:00 +0100] "GET /praha4/velryba/wp-includes/js/wp-emoji-release.min.js?ver=4.7.1 HTTP/1.1" 200 4230
cb.cz 82.142.105.1 - - [24/Jan/2017:15:02:00 +0100] "GET /praha4/velryba/wp-content/themes/twentythirteen/js/functions.js?ver=20160717 HTTP/1.1" 200 1803
cb.cz 82.142.105.1 - - [24/Jan/2017:15:02:00 +0100] "GET /praha4/velryba/wp-includes/js/wp-embed.min.js?ver=4.7.1 HTTP/1.1" 200 751
cb.cz 82.142.105.1 - - [24/Jan/2017:15:02:00 +0100] "GET /praha4/velryba/wp-content/uploads/2014/09/cropped-b-236_joni_tabor13.jpg HTTP/1.1" 200 145809
cb.cz 82.142.105.1 - - [24/Jan/2017:15:02:00 +0100] "GET /praha4/velryba/wp-content/themes/twentythirteen/images/search-icon.png HTTP/1.1" 200 422
cb.cz 82.142.105.1 - - [24/Jan/2017:15:02:00 +0100] "GET /praha4/velryba/wp-content/themes/twentythirteen/images/dotted-line.png HTTP/1.1" 200 80
cb.cz 82.142.105.1 - - [24/Jan/2017:15:02:02 +0100] "GET /favicon.ico HTTP/1.1" 200 318
cb.cz 82.142.105.1 - - [24/Jan/2017:15:02:05 +0100] "GET /praha4/velryba/2017/01/tabor-2017/ HTTP/1.1" 200 5011
cb.cz 82.142.105.1 - - [24/Jan/2017:15:02:06 +0100] "GET /praha4/velryba/wp-includes/js/comment-reply.min.js?ver=4.7.1 HTTP/1.1" 200 589
cb.cz 82.142.105.1 - - [24/Jan/2017:15:02:06 +0100] "GET /praha4/velryba/wp-content/uploads/2014/10/cropped-20140703_1557591.jpg HTTP/1.1" 200 91756
cb.cz 82.142.105.1 - - [24/Jan/2017:15:03:17 +0100] "GET /praha4/velryba/2017/01/fotky-z-podzimek/ HTTP/1.1" 200 4612
cb.cz 82.142.105.1 - - [24/Jan/2017:15:03:19 +0100] "GET /praha4/velryba/fotogalerie/podzimky-2016/ HTTP/1.1" 200 5896
cb.cz 82.142.105.1 - - [24/Jan/2017:15:03:20 +0100] "GET /praha4/velryba/wp-content/plugins/nextgen-

Finished

Analysis finished in 0 hours, 6 minutes, 25 seconds, 19 miliseconds.

OK