



Web Site Forensics

*Enabling IT departments and
helpdesk agents to track down
problems on your web site*

Metronome Labs, LLC.
425 First Avenue
Pittsburgh, PA 15219
+1 (412) 434-4911
www.metronomelabs.com

IT Forensics

Quickly find and troubleshoot visitor problems even on dynamic pages

Understanding your web visitors' problems

Keeping your web site running and your visitors happy is critical. Finding a problem is like looking for a needle in a haystack and most of the time you cannot repeat it. You need to be able to quickly understand what your visitor actually experienced and what went wrong. Better still, if you can catch and alert your staff immediately when there is a problem you take immediate action to keep your visitors coming back. When you have found the problem, you need to know how many times it has occurred to decide its severity.

Metronome Capture tracks what your visitors are doing and what they are experiencing in real-time. Metronome Examine provides a powerful search capability that enables you to quickly find a visitor session and see detailed information about every pageview and hit they experienced in their visit.

You get built-in real-time statistics about your user activity and how your web site is performing, traffic levels, visitors, errors etc. and you can easily build real-time reports to monitor key metrics.

Metronome Capture – rich, secure and convenient data capture

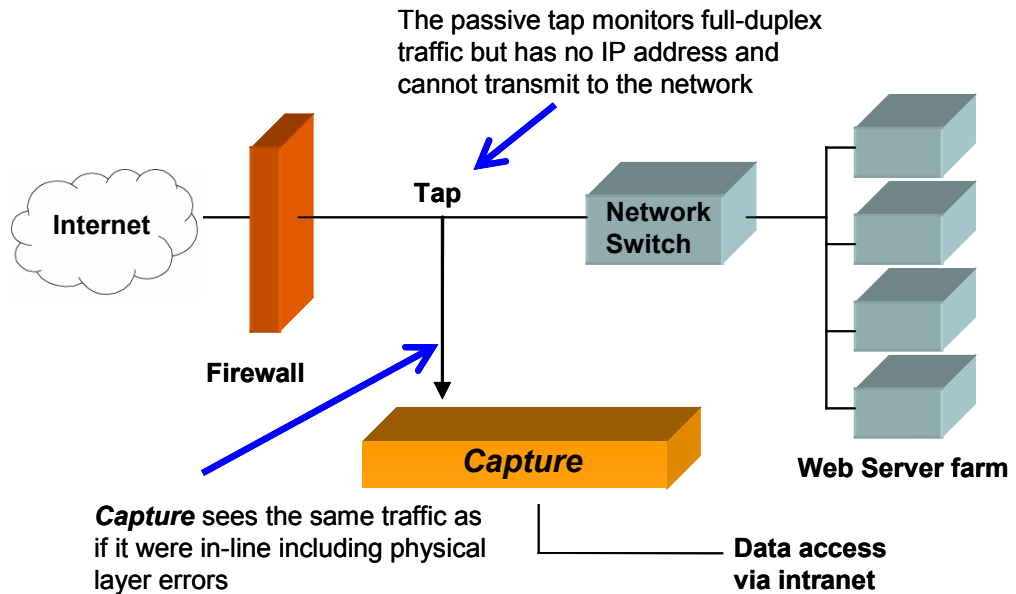
Metronome Capture collects visitor and server activity, filters and sessionizes the data and keeps it all inside your firewall.

The Metronome Capture appliance is placed inside your firewall before your load balancer. It passively listens to all the traffic to and from your site regardless of which server actually handles the request. It collects all your clickstream data at one central location, even when you have multiple servers and domains.

Metronome Capture sees all of the traffic flowing between your visitors and web servers (including the IP packets) so it sees the acknowledgements to requests plus the low level errors that the server never sees. This enables Metronome Capture to calculate every detail of the transaction including precise load times for the HTML and each of its components. Even if your graphics are served by a third party such as Akamai, the true page load times are calculated.

Metronome Capture automatically groups page views and hits into visitor sessions using a sophisticated algorithm and links them together with a unique session ID. The data is available immediately.

Capture can even capture the actual HTML that was served so that problems in dynamic HTML can be diagnosed.

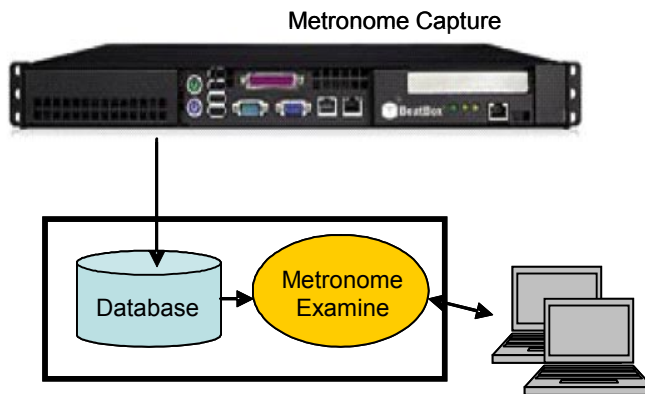


Metronome Examine - Search and destroy

Search for problem visits using any combination of search criteria

When there is a problem on your site, Metronome Examine enables you to quickly search for a visitor session using any criteria, such as logon name and date. You can use multiple search criteria. You can search for all sessions with a particular attribute or problem such as any session with a page that took longer than 20 seconds to download.

Find all visits that had a similar problem



Metronome Examine Architecture

You can then drill down to the pageviews and hits for any session to see exactly what pages and graphics the visitor saw, how long they took to load, which servers supplied them, and so on. Examine will even store the actual HTML that was served.

Metronome Examine :: Hits For Page View 1 in Session 09BBC47A3F6C11DBAB2100A0C95C12B7 - Microsoft In...

File Edit View Favorites Tools Help

QUERY SESSIONS PAGE VIEWS HITS SETTINGS ADMIN LOGOUT

Session ID: 09BBC47A3F6C11DBAB2100A0C95C12B7

Start: 09-08-2006 14:58:37 End: 09-08-2006 14:58:49
 User ID: - Website: default
 Pages: 2 Hits: 21
 Client IP: 202.142.114.25 Duration: 12s
 HTTP Version: HTTP/1.1
 Referrer: http://www.google.com/search?hl=en&lr=&rls=com.microsoft%3Aen-US&q=tlr+decrypt
 User Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 1.1.4322; InfoPath.1)

Seq: 1 In Session ID: 09BBC47A3F6C11DBAB2100A0C95C12B7

Date: 2006-09-08 14:58:37 Status: 200
 Page Title: ::BeatBox Technologies :: SSL & TLS Decryption::
 URL: http://www.beatboxtech.com/technology/ssl.php?;-
 Hits: 12 # Cancelled: 0
 Bytes Sent: 9191 Page Bytes: 23962
 Load Time: 5.4779s HTML Time: 0.8021s
 Num Redirects: 0 Redirect Time: 0s
 HTTP Transaction: [View](#)

Hits

Date	Seq	Tot Time	URL	Post Content	Server IP	Method	SSL	Status	Se
2006-09-08 14:58:37	1	1.209	http://www.beatboxtech.com/technology/...	-	192.168.2.2	GET	N	200	1.
2006-09-08 14:58:39	2	0.448	http://www.beatboxtech.com/css/css.css...	-	192.168.2.2	GET	N	200	0.
2006-09-08 14:58:40	3	0.3919	http://www.beatboxtech.com/images/1x1...	-	192.168.2.2	GET	N	200	0.
2006-09-08 14:58:40	4	0.4389	http://www.beatboxtech.com/images/ho...	-	192.168.2.2	GET	N	200	0.
2006-09-08 14:58:41	5	0.3801	http://www.beatboxtech.com/images/sol...	-	192.168.2.2	GET	N	200	0.
2006-09-08 14:58:41	6	0.4275	http://www.beatboxtech.com/images/pro...	-	192.168.2.2	GET	N	200	0.
2006-09-08 14:58:41	7	0.3599	http://www.beatboxtech.com/images/tec...	-	192.168.2.2	GET	N	200	0.
2006-09-08 14:58:41	8	0.3838	http://www.beatboxtech.com/images/par...	-	192.168.2.2	GET	N	200	0.
2006-09-08 14:58:42	9	0.3767	http://www.beatboxtech.com/images/abo...	-	192.168.2.2	GET	N	200	0.
2006-09-08 14:58:42	10	0.3784	http://www.beatboxtech.com/images/con...	-	192.168.2.2	GET	N	200	0.
2006-09-08 14:58:43	11	0.424	http://www.beatboxtech.com/images/nav...	-	192.168.2.2	GET	N	200	0.
2006-09-08 14:58:43	12	0.441	http://www.beatboxtech.com/images/bbl...	-	192.168.2.2	GET	N	200	0.

SSL Encryption

Capture's decodes secure data so that you can get a complete view of your visitor

Metronome Capture can decode SSL traffic so you can track your visitors in and out of secure areas of your site. Since Metronome Capture is secure behind your firewall, there is no security risk.

Metronome Capture performs decryption is software and supports sites that use multiple RSA keys. It can also be used with FIPS compliant SSL acceleration cards available from vendors such as nCipher.

Improve performance

Triggering Events

Set alerts to tell you when known problem sequences occur

Metronome Capture enables you to define events on hits, pageviews and visits so you can detect any event and get an immediate alert, tag the record in the database or add it to an error report. This enables you to trap known problems when they occur. Basic events could be pageload times greater than 20 seconds or any sever error or error page. The event can capture not only the page but also the session in which it occurred. You can continually improve the reliability and effectiveness of your site by adding event rules as you discover problems that tend to recur on your site. All errors can also be stored to database tables or custom log files and requested as XML.

Metronome Web Console

Real-time reports monitor traffic, performance and errors from any web browser

In addition to the Metronome Examine forensics, Capture has a web console that allows you to monitor your traffic and other metrics in real-time. Standard reports instantly show you the number of visitors on your site, traffic rates, timing information and error counts. You can configure real-time reports from any of the standard or custom fields that are being collected. Reports typically show aggregated data about what is happening on your web site now. This might be the longest page load times, stickiest pages, error pages served by you servers, etc. The reports show up-to-the second information and can be refreshed every few seconds. They are viewed through your web browser.

Geo location

Instantly know where your visitors are coming from.

Metronome Capture uses an integrated database from Quova® to instantly pinpoint each visitor's physical location (country, state, city) and identify their connection information (ISP, network carrier and connection speed). You will know where your visitors are coming from. Often, response problems are not your fault. You can monitor connection latency from different cities to troubleshoot response problems. You can extend this with events for real-time fraud detection applications.

Technical

Technical

Metronome Capture is a Linux application that is shipped in a dual processor, dual core server configuration in a 1U rack-mounted unit. It can also be supplied as a software application to load on your own hardware. Its multi-threaded architecture distributes work evenly across multiple processors, allowing a single appliance to scale to the full line speed of both copper and gigabit fiber networks.

Metronome Capture uses a passive network TAP to promiscuously collect packets. The appliance ports cannot transmit data and have no IP address so they cannot be interrogated. The network TAP is typically inserted between the load-balancing switch and an edge router. This TAP maintains a hard-wired connection between the two devices so that the flow of traffic is not delayed and a failure of the TAP (e.g. due to a power loss) will not cause a network outage. Since the tap prevents routing into the appliance, it does not introduce a security risk. TAPs are widely used, inexpensive devices supplies but many networking hardware vendors (e.g. Datacom). Capture also supports the use of spanning (SPAN) ports which are often available on routers and repeating hubs.

Metronome Examine application typically runs on an additional computer on either Linux or Windows. For sites with lower traffic, both applications can be run on a single dual CPU/dual-core Linux machine.

A Revolution in Web Forensics

Metronome captures your visitors' experience from your network traffic inside your firewall. There are no security or privacy concerns and little maintenance. Metronome Examine enables you to quickly find problem sessions and understand what actually happened. The powerful rule engine enables you to close the loop and raise the alarm immediately should the problem occur again.

About Metronome Labs

Based in Pittsburgh, Pennsylvania, Metronome Labs LLC is a value-added reseller of BeatBox Capture from HP which has embedded the technology in some of its products. Metronome Labs develops value-added products including solutions for web analytics, IT forensics and web data capture and loading. There are about 250 Capture appliances installed, including major retail sites like QVC. For more information, visit the web site at www.metronomelabs.com.