## **Demo: InViz – Instant Visualization of Security Attacks**

Lucas Layman, Nico Zazworka Fraunhofer Center for Experimental Software Engineering College Park, MD, USA {llayman,nzazworka]@fc-md.umd.edu

## **1. INTRODUCTION**

InViz is a desktop tool for visualizing events from network applications, such as webserver application events or syslog events from network appliances such as routers or firewalls. InViz maps properties of events onto graphical objects that move across the screen in real-time as the events occur. For example, our Live Visualization maps types of requested files, the size of the HTTP response, and the HTTP response code to different shapes, magnitudes, and colors of the moving objects (see Figure 1 for an example of the interface). This visualization allows users to search for visual patterns in the flow of events in real time.

The Historical Visualization shows patterns of events over time sorted by event properties, such as the requesting IP. This sorting of events can reveal unique patterns of behavior from different IP addresses. InViz is controlled by the Timeline View and timeline controls, which function much like the standard controls on a DVD or DVR, allowing the user to control the display of the realtime information. The InViz cybersecurity visualizations combine concepts from glTail [1] and CodeVizard [2] to distill large amounts of information into a form more easily palatable to the user.

These visualizations leverage the human capacity for pattern recognition to identify anomalous events. By being able to process this information quickly, humans can also apply their contextual knowledge of the system to eliminate false positives, thus reducing the time to perform rapid/live forensics.

InViz is a functional prototype and has gone through a handful of internal releases, with a project release date of February 2013. A video demonstrating the capabilities of InViz may be found at: <u>http://www.fc-md.umd.edu/inviz/</u>.

## 2. DEMONSTRATION PLAN

We will briefly demonstrate the tool's capabilities on a real-life example take from Fraunhofer CESE's public-facing webserver. We will load the IIS 7.5 webserver application log file into InViz and demonstrate how InViz can quickly and easily identify abnormal patterns of behavior. We will highlight a naïve, scriptbased attack on our webserver that attempted to find a backdoor into an online email application. We will also show attempted accesses to administrative control panels for the phpMyAdmin application. We will also show some other potentially interesting patterns of behavior that are not, necessarily, attacks. We will, of course, limit what we show to the time allotted.

The goal of our demonstration is to focus on ease of use and understandability by security novices, rather than promulgate the tool as an attack detection or forensics silver bullet (which it is not).

Our takeaway is that we hope that InViz will be a useful tool for one or more of the following:

- Narrowing the gap between attack notification and attack resolution by helping users understand log file data more quickly and accurately;
- 2) Lightweight analysis of webserver and router traffic by non-experts;
- 3) Training for security novices to identify attack patterns.

## **3. REFERENCES**

- "glTail.rb realtime logfile visualization", <u>http://www.fudgie.org</u>, 2007.
- [2] N. Zazworka, C. Ackermann, "CodeVizard: a tool to aid the analysis of software evolution", 2010 ACM-IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM '10), Bolzano-Bozen, Italy, Sept. 16-17 2010
- [3] U.S. Department of Homeland Security, "A Roadmap for Cybersecurity Research", <u>http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf</u>, 2009, pp. 90-98.

| File Search Options View   |   |  |  |  |   |  |
|--|---|--|--|--|---|--|
| 📢 🕕 Pause 📕 Stop 🕨   | Timeline view -                                   | <ul> <li>shows aggregated ever</li> </ul>  | nts over time  | e  |   |  |
| 🔊 Timeline   |   |  |  |  |   |  |
| Tue Mar 15 01:19:04 EDT 2011   |   |  |  |  |   |  |
|  |   | *  |  | Tue Mar 15 05  | 21:33 EDT 201   |  |
|  |   |  |  |  |   |  |
| Tue Mar 15 00:07:30 EDT 2011   |   |  |  |  | т   | ue Mar 15 07:59:10 EDT 201   |
| Live Visualization   |   |  |  | odeVizard View   |   |  |
|  |   |  |  |  |   |  |
| Clients/Host Frequent P/A  | Current Speed: 32.0x                              | r/m Requested pages  | roc  | ot   |   |  |
| 106.16.136.13 2.95   | ¢   | 0.72 ./Styles/New item.css<br>0.72 ./Styles/BusinessCards.cs   |  | 209.85.238.120   |   |  |
| 207.218.234.226 0.21   | <u>م</u>  | 0.70 ./Styles/tipTip.css   |  | 207.210.234.226  |   |  |
| 120.0.10.01 0.21   | ¢•  | 0.69 ./News/10-01-2010.aspx  |  | 77.88.27.27  |   |  |
|  | Q   | 0.49 .ustomersAndCollaborators   | 5.35px   | 67.195.115.120   |   |  |
|  | Ø   | 0.46 ./Resources/Resources.ass   | •••  | 128.8.70.132   |   |  |
|  | 0   | 0.27 ./AboutUs.aspx  |  | 128.8.10.81  |   |  |
|  | Ś   | 0.24 ./Jobs.espx   |  | 98.228.212.111   |   |  |
|  | ) (   | 0.21 ./People/HyrnaRegardic.as   | spx  | 00.249.72.53   |   |  |
| 67.195.115.120 3.61  | Ç   | 0.22 ./Styles/General.css<br>0.23 ./Home.aspx  |  | 10 161 12 102  |   | = \  |
| 207.210.234.226 0.21   |   | 0.14 ./Script/animation-box.j:   |  | 109.101.13.192   |   | = '  |
|  |   |  |  |  |   |  |
| 108.18.136.13 2.95<br>128.8.10.81 0.21   |   | 0.13 ./People.aspx<br>0.12 .ges/university_of_icelas   | nd.jpg   | 65.52.110.17   |   |  |
| Live view – Shows even<br>attributes   | nts in real time, mapping to object dimensions    | P.13 ./Propie.aspx<br>0.12 .ges/university_of_fcolar<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_resources<br>versity_of_  | nd.jpg<br>ome.jpg<br>o.pms<br>nt.ong H   | istorical vie  | w – Pattern<br>ed by IP   | s of events over time  |
| Live view – Shows even<br>attributes   | nts in real time, mapping<br>to object dimensions | e.13 ./Propie.aspx<br>e.13   | nd.jpg<br>sme.jpg<br>o.jpmg<br>nt.png  | istorical vie  | w – Pattern<br>ed by IP   | is of events over time   |
| Live view – Shows ever<br>attributes   | nts in real time, mapping<br>to object dimensions | e.13 (Propieranox<br>e.13 (Aroniversity_of_ficial<br>exet/university_of_ficial<br>event (Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Contention)<br>(Con | nd jpg<br>one dag<br>on png<br>nt ong<br>H   | istorical vie<br>sorte   | w – Pattern<br>ed by IP   | is of events over time   |
| Live view – Shows ever<br>attributes   | nts in real time, mapping<br>to object dimensions | <pre>*.13 ./Prople.aspx *.13</pre>   | nd.jpa<br>one.jpg<br>o.pnc<br>nt.png<br>H  | istorical vie<br>sort  | w – Pattern<br>ed by IP   | s of events over time  |
| Live view – Shows ever<br>attributes   | nts in real time, mapping<br>to object dimensions | e.13<br>e.13<br>;event<br>;event<br>Host Name  | nd Jox<br>ane Jog<br>a proc<br>at on A   | istorical vie<br>Sorta   | w – Pattern<br>ed by IP<br>Status   | s of events over time  |
| Live view – Shows even<br>attributes   | nts in real time, mapping<br>to object dimensions | Host Name<br>pool-108-18-136-13.was  | Protocol<br>HTTP/1.1   | istorical vie<br>sorte   | w – Pattern<br>ed by IP<br>Status<br>200  | Event details  |
| Live view – Shows even<br>attributes<br>Event View & Violation View (0)<br>Search:<br>Date/time<br>EDT 2011-Mar-15 01:22:55<br>EDT 2011-Mar-15 01:22:56  | nts in real time, mapping<br>to object dimensions | Host Name     pool-108-18-136-13.was     pool-108-18-136-13.was  | Protocol<br>HTTP/1.1   | Method<br>GET<br>GET   | w – Pattern<br>ed by IP   | Event details  |
| Live view – Shows even<br>attributes<br>Event View & Violation View (0)<br>Search:<br>Date/time<br>EDT 2011-Mar-15 01:22:55<br>EDT 2011-Mar-15 01:22:58  | nts in real time, mapping<br>to object dimensions | +.13         :/Propis.espx           +.13         :scr/university_of_itelan           versity_of_restry  | Protocol<br>HTTP/1.1<br>HTTP/1.1   | Method<br>GET<br>GET<br>GET  | w – Pattern<br>ed by IP<br>Status<br>200<br>200<br>200  | Event details  |
| Live view – Shows ever<br>attributes<br>Event View & Violation View (0)<br>Search:<br>Date/time<br>EDT 2011-Mar-15 01:22:55<br>EDT 2011-Mar-15 01:22:58<br>EDT 2011-Mar-15 01:22:58<br>EDT 2011-Mar-15 01:23:00  | nts in real time, mapping<br>to object dimensions | +.13         :/Propis-appx           +.13         :sex/university_of_itelan           yersity_of_itelan         :lega_pre           isex/university_of_itelan         :lega_pre           :lega_pre         :lega_pre           :lega_pre <td:lega_pre< td="">           :lega_pre</td:lega_pre<>  | Protocol<br>HTTP/1.1<br>HTTP/1.1<br>HTTP/1.1   | Method<br>GET<br>GET<br>GET<br>GET   | w – Pattern<br>ed by IP   | Event details<br>/Competencies.aspx<br>/CustomersAndColli<br>/Resources/Resource<br>/CustomersAndColli   |
| Itin (D.1.50.15)         2.52           Itin (D.1.50.15)         2.55           Itin (D.1.50.15)         501:22:55           Itin (D.1.50.15)         501:22:55           Itin (D.1.50.15)         501:22:56           Itin (D.1.50.15)         501:22:50           Itin (D.1.50.15)         501:22:50           Itin (D.1.50.15)         501:23:00           Itin (D.1.50.15)         501:23:30   | nts in real time, mapping<br>to object dimensions | +.13         :/Propis-seps<br>.sev/estverstr, ad., (.etaa<br>vr.str, ad., (.etaa<br>serv/estverstr, ad., (.etaa<br>vr.str, ad., (.etaa<br>serverstr, ad., (.etaa)<br>serverstr, (.etaa)<br>serverstr, ad., (.etaa)  | Protocol<br>HTTP/1.1<br>HTTP/1.1<br>HTTP/1.1<br>HTTP/1.0   | Method<br>GET<br>GET<br>GET<br>GET<br>GET                                    | w – Pattern<br>ed by IP<br>Status<br>200<br>200<br>200<br>200<br>200<br>200                             | Event details /Competencies.aspx /CustomersAndColli. /Resources/Re |
| Live view - Shows even<br>attributes           Event View ▲ Violation View (0)           Search:           Date/time           EDT 2011-Mar-15 01:22:55           EDT 2011-Mar-15 01:22:56           EDT 2011-Mar-15 01:22:58           EDT 2011-Mar-15 01:22:50           EDT 2011-Mar-15 01:22:50           EDT 2011-Mar-15 01:22:30           EDT 2011-Mar-15 01:22:30           EDT 2011-Mar-15 01:22:30   | nts in real time, mapping<br>to object dimensions | +.13         :/Propis-seps           +.13         :set/est/est/est, of.ictar           event         :set/est/est/est/est/est/est/est/est/est/   | Protocol<br>HTTP/1.1<br>HTTP/1.1<br>HTTP/1.0<br>HTTP/1.0   | Method<br>GET<br>GET<br>GET<br>GET<br>GET<br>GET                             | w – Pattern<br>ed by IP<br>Status<br>200<br>200<br>200<br>200<br>200<br>200<br>404                      | Event details<br>/Competencies.aspx<br>/CustomersAndColli<br>/Resources/Resourci<br>/CustomersAndColli<br>/People/MyrnaRega<br>/Courses.aspx   |
| Live view – Shows ever<br>attributes<br>Event View & Violation View (0)<br>Search:<br>Date/time<br>EDT 2011-Mar-15 01:22:55<br>EDT 2011-Mar-15 01:22:56<br>EDT 2011-Mar-15 01:22:58<br>EDT 2011-Mar-15 01:22:30<br>EDT 2011-Mar-15 01:26:37  | nts in real time, mapping<br>to object dimensions | +.13         :/Propis-seps           +.13         :set/estress           event         vrsity_of_cr          16gs.png         :.16gs.png          170         :.111          111         :.111          111         :.111          111         :.111          111         :.111          111         :.111          111         :.111          111         :.111          1111         :.111          1111         :.111          1111         :.111          1111         :.111          1111         :.111          1111         :.111          1111         :.1111  | Protocol<br>HTTP/1.1<br>HTTP/1.1<br>HTTP/1.0<br>HTTP/1.0   | Method<br>GET<br>GET<br>GET<br>GET<br>GET<br>GET<br>GET                      | w – Pattern<br>ed by IP<br>Status<br>200<br>200<br>200<br>200<br>404<br>200                             | Event details /Competencies.aspx /CustomersAndColli. /Resources/Resourci /CustomersAndColli. /People/MyrnaRega /Courses.aspx /News/10-01-2010.a  |
| Live view – Shows ever.<br>attributes  Event View & Violation View (0) Search: Date/time EDT 2011-Mar-15 01:22:55 EDT 2011-Mar-15 01:22:58 EDT 2011-Mar-15 01:22:58 EDT 2011-Mar-15 01:22:30 EDT 2011-Mar-15 01:26:25 EDT 2011-Mar-15 01:26:25 EDT 2011-Mar-15 01:26:25 EDT 2011-Mar-15 01:26:37 EDT 2011-Mar-15 01:26:37  | nts in real time, mapping<br>to object dimensions | +.13         ://repix-sepx           +.13         :sst/sstresty_of_itetar           sst/sstresty_of_itetar         :sst/sstresty_of_itetar           isst/sstresty_of_itetar         :sst/sstresty_of_itetar           isst/sstresty_of_itetar         :sst/sstresty_of_itetar           isst/sstresty_of_itetar         :sst/sstresty_of_itetar           isst/sstresty_of_itetar         :sst/sstresty_of_itetar           isst/sstresty_of_itetar         :sst/sstresty_of_itetar           isst/sstresty_of_itetar         :sstresty_of_itetar           isst/sstresty_of_itetar         :sstresty_of_itetar           isstresty_of_itetar         :sstresty_of_itetar           pool-108-18-136-13.was         pool-108-18-136-13.was           pool-108-18-136-13.was         207.210.234.226           b3090795.crawl.yahoo.net         b3090795.crawl.yahoo.net  | Protocol<br>HTTP/1.1<br>HTTP/1.1<br>HTTP/1.1<br>HTTP/1.0<br>HTTP/1.0<br>HTTP/1.0<br>HTTP/1.0                           | Method<br>GET<br>GET<br>GET<br>GET<br>GET<br>GET<br>GET<br>GET               | w – Pattern<br>ed by IP<br>Status<br>200<br>200<br>200<br>200<br>200<br>200<br>200<br>200<br>200<br>20  | Event details<br>/Competencies.aspx<br>/CustomersAndColli<br>/Resources/Resource<br>/CustomersAndColli<br>/People/MyrnaRega<br>/Courses.aspx<br>/News/10-01-2010.a<br>/Styles/General.css  |
| Iteratoristic         2:52           131.4.10:41         2:53           131.4.10:41         2:53           Live view – Shows ever<br>attributes         2:54           Event View         ▲ Violation View (0)           Search:         2:55           EDT 2011-Mar-15 01:22:55         EDT 2011-Mar-15 01:22:56           EDT 2011-Mar-15 01:22:56         EDT 2011-Mar-15 01:22:56           EDT 2011-Mar-15 01:22:58         EDT 2011-Mar-15 01:26:30           EDT 2011-Mar-15 01:26:37         EDT 2011-Mar-15 01:26:37           EDT 2011-Mar-15 01:26:37         EDT 2011-Mar-15 01:26:37  | nts in real time, mapping<br>to object dimensions | +.13         ://rept - sept           +.13         :sev/estverstr, set, ictar           *.14         :sev/estverstr, set, ictar           *.15         :sev/estverstr, set, ictar           *.162         :sev/estverstr, set, ictar           pool-108-18-136-13.was         pool-108-18-136-13.was           pool-108-18-136-13.was         :sev           pool-108-18-136-13.was         :sev           207.210.234.226         :sev           b3090795.crawl.yahoo.net         :s3090795.crawl.yahoo.net           b3090795.crawl.yahoo.net         :s03090795.crawl.yahoo.net  | Protocol<br>HTTP/1.1<br>HTTP/1.1<br>HTTP/1.1<br>HTTP/1.0<br>HTTP/1.0<br>HTTP/1.0<br>HTTP/1.0<br>HTTP/1.0               | Method<br>GET<br>GET<br>GET<br>GET<br>GET<br>GET<br>GET<br>GET<br>GET<br>GET | w - Pattern<br>ed by IP<br>Status<br>200<br>200<br>200<br>200<br>200<br>200<br>200<br>200<br>304<br>304 | Event details Competencies.aspx /CustomersAndColli /Resource/Resource/CustomersAndColli /People/MyrnaRega /Courses.aspx /News/10-01-2010.a /Styles/General.css /Styles/tipTip.css  |
| Ideated Stort         203           328.4.10.50.12         203           328.4.10.50.12         203           State 10.11         6.031           Live view - Shows eve:<br>attributes         attributes           Search:  | nts in real time, mapping<br>to object dimensions | +.13         ://rest-seps           +.13         :sev/estverstry, of.(telar           event         :sev/estverstry, of.(telar           -1020.pmg         :.130           -1020.pmg         :.130           -1020.pmg         :.130           -1020.pmg         :.130           -1020.pmg         :.130           -1020.pmg         :.130           -1020.108-18-136-13.was         pool-108-18-136-13.was           pool-108-18-136-13.was         pool-108-18-136-13.was           pool-108-18-136-13.was         207.710.224.226           b3090795.crawl.yahoo.net         b3090795.crawl.yahoo.net           b3090795.crawl.yahoo.net         b3090795.crawl.yahoo.net   | Protocol<br>HTTP/1.1<br>HTTP/1.1<br>HTTP/1.1<br>HTTP/1.0<br>HTTP/1.0<br>HTTP/1.0<br>HTTP/1.0<br>HTTP/1.0<br>HTTP/1.0   | Method<br>GET<br>GET<br>GET<br>GET<br>GET<br>GET<br>GET<br>GET<br>GET<br>GET | w – Pattern<br>ed by IP<br>Status<br>200<br>200<br>200<br>200<br>200<br>200<br>200<br>200<br>200<br>20  | Sof events over time   |
| Ideatestation         2019           333.4.150.13         0.33           Live view - Shows ever<br>attributes         Automatic<br>stributes           Event View         ▲ Violation View (0)           Search:         Date/time           EDT 2011-Mar-15 01:22:55         EDT 2011-Mar-15 01:22:56           EDT 2011-Mar-15 01:22:58         EDT 2011-Mar-15 01:22:58           EDT 2011-Mar-15 01:22:30         EDT 2011-Mar-15 01:26:25           EDT 2011-Mar-15 01:26:25         EDT 2011-Mar-15 01:26:37           EDT 2011-Mar-15 01:26:37         EDT 2011-Mar-15 01:26:37   | nts in real time, mapping<br>to object dimensions | +.13         ://repix-sepx           +.13         :set/entversits, of.(telar           event         :set/entversits, of.(telar          163.pm         :set/entversits, of.(telar          163.pm         :.163.pm          163.pm         :.163.pm          163.pm         :.163.pm          163.pm         :.163.pm          163.pm         :.163.pm          164.pm         :.163.pm          164.stails-13.was         :.164.stails-13.was           pool-108-18-136-13.was         :207.210.234.226           b3090795.crawl.yahoo.net         :3090795.crawl.yahoo.net           b3090795.crawl.yahoo.net         :3090795.crawl.yahoo.net           b3090795.crawl.yahoo.net         :3090795.crawl.yahoo.net           b3090795.crawl.yahoo.net         :3090795.crawl.yahoo.net  | Розбеловина<br>Рготосо<br>НТТР/1.1<br>НТТР/1.1<br>НТТР/1.1<br>НТТР/1.0<br>НТТР/1.0<br>НТТР/1.0<br>НТТР/1.0<br>НТТР/1.0 | Method<br>GET<br>GET<br>GET<br>GET<br>GET<br>GET<br>GET<br>GET<br>GET<br>GET | w – Pattern<br>ed by IP<br>Status<br>200<br>200<br>200<br>200<br>200<br>200<br>200<br>200<br>200<br>20  | Event details<br>/Competencies.aspx<br>/CustomersAndColli<br>/Resources/Resource<br>/CustomersAndColli<br>/People/MyrnaRega<br>/Courses.aspx<br>/News/10-01-2010.a<br>/Styles/Jeneral.css<br>/Styles/ipTip.css<br>/Styles/ipTip.css<br>/Styles/ipTip.css   |
| Ideated at 0         203           328.4.103.12         0.33           Live view - Shows eve:<br>attributes         attributes           Image: State at 100 million view (0)         Search:           Date/time         EDT 2011-Mar-15 01:22:55           EDT 2011-Mar-15 01:22:56         EDT 2011-Mar-15 01:22:56           EDT 2011-Mar-15 01:22:58         EDT 2011-Mar-15 01:22:50           EDT 2011-Mar-15 01:26:30         EDT 2011-Mar-15 01:26:25           EDT 2011-Mar-15 01:26:37         EDT 2011-Mar-15 01:26:37           EDT 2011-Mar-15 01:26:37         EDT 2011-Mar-15 01:26:39 | nts in real time, mapping<br>to object dimensions | +.13         ://repix-sepx           +.13         :set/entversity.of.(tetar           event         vfsity.of.(tetar          16gs.png         :.16gs.png          16gs.png         :.16gs.png          16gs.png         :.16gs.png          16gs.png         :.16gs.png           pool-108-18-136-13.was         pool-108-18-136-13.was           pool-108-18-136-13.was         207.210.234.226           b3090795.crawl.yahoo.net         b3090795.crawl.yahoo.net           b3090795.crawl.yahoo.net         b3090795.crawl.yahoo.net           b3090795.crawl.yahoo.net         b3090795.crawl.yahoo.net  | Protocol<br>HTTP/1.1<br>HTTP/1.1<br>HTTP/1.1<br>HTTP/1.0<br>HTTP/1.0<br>HTTP/1.0<br>HTTP/1.0<br>HTTP/1.0<br>HTTP/1.0   | Method<br>GET<br>GET<br>GET<br>GET<br>GET<br>GET<br>GET<br>GET<br>GET<br>GET | w – Pattern<br>ed by IP<br>200<br>200<br>200<br>200<br>200<br>200<br>200<br>200<br>200<br>20            | so of events over time<br>Event details<br>/Competencies.aspx<br>/CustomersAndColl.<br>/Resources/Resourci<br>/CustomersAndColl.<br>/People/MyrnaRega<br>/Courses.aspx<br>/News/10-01-2010.a<br>/Styles/dusinessCarc<br>/Styles/ipTip.css<br>/Styles/ipTip.css<br>/Styles/ipTip.css<br>/Styles/ipTip.css   |

Figure 1. Screenshot of the InViz prototype processing IIS 7.5 webserver events