Inspecting Raw Data (Flow Records)

Raw Data files store flow records exported in a 5-minute interval.

Raw Data Tree groups Raw Data files in folders according to day/hour/minute. Selecting a node from the tree allows inspection of specific Raw Data files.

Inspecting Raw Data

To inspect Raw Data:

- 1. Go To NetFlow > Raw Data > Files
- 2. **Specify time period** in Time Window. The main panel and Raw Data Tree will show gathered files
- 3. Select files you want to inspect from the Main Panel (or alternatively, select a single file from Raw Data Tree)
- 4. Click Show Selected

| | | | | Last Hour | |
|-----------------------|----------|-------------------------|----------|-----------|--|
| Top II Raw Data | Files | Flows | | | |
| 🖯 🛗 Raw Files | Show Sel | lected Select All | | | |
| 8 🔚 14. Aug | Select | File | Size | | |
| 0 🔛 14h | | 2014-00-14-14-45-00.10 | 40.25 MB | | |
| 2014-08-14-14-50-00. | | 2014-00-14-14-00-00.458 | 40.9 MD | | |
| 2014-08-14-14-55-00. | | 2014-00-14-14-05-00.xtg | 39.66 MD | | |
| 8 📴 15h | | 2014-00-14-10-00-00.458 | 37.81 MB | | |
| 2014-08-14-15-00-00.0 | | 2014-00-14-15-05-00.xtg | 37.1 MB | | |
| 2014-08-14-15-10-00.0 | | 2014-05-14-15-10-00.xts | 35.45 MB | | |
| 2014-08-14-15-15-00. | | 2014-08-14-15-15-00.418 | 35.83 MB | | |
| 2014-08-14-15-20-00. | | 2014-08-14-15-20-00.419 | 34.95 MB | | |
| 2014-08-14-15-25-003 | | 2014-08-14-15-25-00.458 | 35.63 MB | | |
| 2014-08-14-15-35-00. | | 2014-08-14-15-30-00.45 | 34.73 MB | | |
| 2014-08-14-15-40-00. | | 2014-08-14-15-35-00.419 | 36.45 MB | | |
| | | 2014-08-14-15-40-00.419 | 35.48 MB | | |
| | | Page 1 of 1 w > > | 1-12/12 | | |

Raw Data table shows flow records from the selected Raw Data file(s). Data can be filtered, grouped and sorted the by almost any field (source IP address, Bytes, Protocol etc.).

| Discount (Ramon) | Details X Clear | | Filtering | | Grouping | | | | | | | Soline | A Deport |
|-------------------------|-------------------------|-------------|-----------------|------------|-----------------|------------|------------|-------|-------------|-------|---------|---------|----------|
| Start Time | End Time | Duration | SCHO | SIC PART O | Dil 19 0 | Did Part O | Protocol O | TON O | TCP Flags O | Flows | Packets | Eyter v | The |
| 10 10 2014 EX 42 17 ME | 22 10 2014 08 44 56 500 | 115.002 444 | 172.16.2 140 | 33030 | 107 28 349 204 | 4CI | | 0 | AP93 | | 11 | 2,488 | 187.3 0 |
| 12-10-2014 09:43 15:12 | 22.13.2014 09.44 55.534 | 101.402 set | 172.16.2.163 | 55505 | 105.160.165.140 | 443 | 6 | 0 | 4295 | | 91 | 2,579 | 2013-0 |
| 22-10-2014 39:44.46.268 | 22+0-2014/08/44/50:588 | 10.220 HH | 172.16.2.19 | \$5064 | 213.180.204.90 | -80 | 6 | 0 | 4258 | | | 729 | 5000 |
| 22-10-2014 23:44 46.458 | 2210-2014/08/44/36 879 | 10.220 MM | 213 190 204 80 | 80 | 172.18.2.19 | 30004 | | 0 | AP27 | | | 671 | 323.2 0 |
| 12-10-2014 09-44-96 712 | 22.10.2014/09/44/06 712 | 1.0 we 0.1 | 148 201 75 148 | 80 | 172.16.2.144 | 54116 | 6 | 0 | 17 | | | 40 | |
| 22-10-2014 88:44:27:202 | 22+0-2014/08:44:57:598 | 30.564 sec | 172.95.567 | 36477 | 108.168 106 253 | 643 | 6 | 0 | 4912 | | 95 | 2,588 | 660.00 |
| 12-10-2014 28 44 27 492 | 2210-2014-28-44 57 568 | 20.70-846 | 108.100.108.253 | 443 | 172163.67 | 26177 | 6 | 0 | AP24 | | 14 | 0,209 | 1,7 100 |
| 12-10-2014/09/39 58-64 | 22.10.2014/09/39/08.64 | 1.0 sm | 172.16.0.8 | 64475 | 82 817 194 2 | 83 | 12 | 0 | 4 | | | 41 | |
| 12-18-2014 09:39-58 108 | 22-10-2014/09:44:05:412 | 270.004 set | 172.16.2.148 | \$7554 | 74,925,205,938 | 5238 | 6 | | A | | | 287 | 8.5 804 |
| 2-10-2014 28:29 58:184 | 2210-2014/08/44/20 108 | 2704.640 | 032515409 | 12915 | 172.16.2.104 | 1819 | 6 | 0 | 49 | | 26 | 12,356 | 324.60 |
| 2 / 0 2014 29 39 18 428 | 22 10 2014 08 42 31 864 | 103.000 and | 172.16.0.4 | 83013 | 82,817,194,2 | 13 | 17 | 0 | A | | 3 | 192 | 10.010 |
| 0.48-2014 09:39-58 828 | 23-10-2014/09-44 43-558 | 284,656 see | 74.125.135.125 | \$222 | 172.16.2.108 | 407.0 | 6 | 0 | 40 | | 9 | 3,500 | 103.76 |
| 2-18-2014 88:39-58 828 | 22-10-2014/08/44 43:008 | 264.300 sec | 172.16.2.108 | 46712 | 74,925,135,125 | 5222 | 6 | 0 | 49 | | 10 | 515 | 54.400 |
| 2 10 2014 28 44 33 464 | 22102014084438379 | 3.112.005 | 14020170.140 | 10 | 172.18.2.144 | 54182 | | 0 | AP28 | | | 805 | 831.00 |
| 2.10.2014 09 44 40 12 | 23.10.2014/09.44/05/284 | 16.232 set | 172.95.2.19 | 64990 | 193.109.245.48 | 80 | 6 | 0 | 4257 | | 0 | 1,203 | 582.04 |
| 0-18-001408-44.40.52 | 22-10-2014/08:44:55:100 | 15.125 840 | 172.95.239 | 54001 | 190.109.045.48 | -50 | 6 | | 4917 | | | 1.101 | \$2546 |
| 2-10-2014 28 44 40 52 | 22-10-2014 28:44:56:32 | 15.900 Mil | 172.16.2.19 | 54992 | 192.109.240.48 | 80 | 6 | 0 | APDE | | 28 | 1,745 | 873.60 |
| 2.10.2014 28 44 43 12 | 22.10.2014 08 44 66 32 | 15.880 ses | 172.16.2.19 | 84900 | 193.109.246.48 | 82 | 6 | 0 | 42.07 | | 13 | 1,017 | 101.04 |
| 0-18-2014 33:44.40.58 | 22-10-2014/08:44:55:102 | 9576444 | 172.95.239 | 54004 | 100.109.245.48 | -50 | 6 | 0 | 4912 | | 15 | 1,391 | 990.00 |
| 2-10-2014 38:44 40 728 | 22-10-2014 28:44:50 252 | 16.222 846 | 193.109.248.48 | 80 | 172.16.2.19 | 54890 | 6 | 0 | AP24 | | 15 | 0,307 | 4.4300 |
| 2 /0.2014 08 44 43 120 | 22 10 2014 08 44 56 260 | 16.140 ani | 193.109.248.48 | 10 | 172.18.2.19 | 54991 | 6 | 0 | 1222 | | 12 | 7,392 | 3.7 834 |
| 0.10.0014 09.44 40.120 | 23-10-2014/09:44:55:104 | 15.054 set | 103.100.248.48 | 80 | 172.16.2.19 | 54992 | 6 | 0 | 4252 | | 41 | 45,382 | 22,7 19 |
| 2-10-2014 33:44.40.524 | 22-10-2014/08:44:50:108 | 15.595 840 | 193.109.248.48 | 80 | 172.16.2.19 | 54995 | 6 | 0 | APS/ | | 14 | 6.367 | 4.5 Hbp |
| 2 10 2014 28 44 40 324 | 22 10 2014 08 44 56 200 | 18.70 and | 193 109 248 48 | 10 | 172.16.2.19 | 5404 | | 0 | AP27 | | 18 | 14,102 | 7.0139 |
| 12-10-2014 09-44 40 916 | 23-10-2014/09-44-07 180 | 16.264 see | 172.95.239 | 99002 | 108,168,157,176 | 80 | 6 | 0 | 4212 | | | 655 | 302.2% |

Clicking on **Names** button provides IP address resolution. If you move your mouse cursor over specific IP address you can see Whols information about that host.

| Files Flows | | | | | | | | | |
|-------------------------|-------------------------|-------------|----------------------------------|------------------|--|----------------------------------|------------|--|--|
| () Request Names | Details X Clear | | | | | | | | |
| Start Time | End Time | Duration | Src IP O | Src Port O | Dst IP O | Dst Port O | Protocol O | | |
| 17-03-2016 02:54:57.708 | 17-03-2016 02:54:57:804 | 0.96 sec | shelart sereco cors | 52676 | 01.127.144 | SSH | TOP | | |
| 17-03-2016 02:54:57.888 | 17-03-2016 02:54 57.995 | 0.105 sec | shelart screco co.rs | 55010 | 57.129.4 | 55H | TOP | | |
| 17-03-2016 02:59:55:796 | 17-03-2016 02:59:56.44 | 0.248 sec | 6.0.45 | 55136 | 5.113.12 | HTTP | TCP | | |
| 17-03-2016 02:59:55.808 | 17-03-2016 02:59:56:924 | 1.116 sec | 22-238-119 static isp telekom ra | | | | | | |
| 17-03-2016 02:59:55.904 | 17-03-2016 02:59 56:540 | 0.636 sec | 12-20-103 STARC RD MMKOTT IS | IP address 178.2 | 22.230.119 | | | | |
| 17-03-2016 02:59:55.916 | 17-03-2016 02:59:56:164 | 0.248 sec | .113.12 | Description | TELEKON SRBIJA, ADSL users Takovska 2 11000 BELGRADE SERBIA | | | | |
| 17-03-2016 02:59:57:224 | 17-03-2016 02:59 57 520 | 0.296 sec | intelant speeco co.rs | Country: | Serbia | | | | |
| 17-03-2016 02:54:58.72 | 17-03-2016 02:54:58.360 | 0.200 640 | shelart sceeco.co.rs | Network Range: | TO-ZZZZADA.117 TELECON SB013A, ASSL users Takovska 2 11 Serola Ange: 170,222,0.0 - 178,222,255,255 TELECON-K (4440) 110,224,66 111,224,66 17771 Jaa-7/64,54660 17771 | | | | |
| 17-03-2016 02:54:58:252 | 17-03-2016 02:54:58:716 | 0.464 sec | insistelant serece cors | | (1000) | | | | |
| 17-03-2016 02:54:58:424 | 17-03-2016 02:59:55:568 | 297.144 sec | ma-7x54 soneco.co.rs | 51427 | 118 234.66 | 17771 | UDP | | |
| 17-03-2016 02:54:58.516 | 17-03-2016 02:59:58.464 | 299.948 sec | 18.234.66 | 17771 | ana-7x64 screece.co.rs | \$1427 | UDP | | |
| 17-03-2016 02:54:58:544 | 17-03-2016 02:59:42:56 | 283.512 sec | pc.soneco.co.rs | 63383 | h-f188.1e100.net | 5228 | TCP | | |
| 17-03-2016 02:54:58:548 | 17-03-2016 02:59:55:532 | 295.964 sec | ema-7x64 soneco.co.rs | 51427 | 254.151.86 | 59168 | UDP | | |
| 17-03-2016 02:54:58:584 | 17-03-2016 02:59:42:36 | 283.452.5e0 | 100 - 1188. 1e 100 net | 5228 | -pc.soreco.co.rs | 63383 | TCP | | |
| 17-03-2016 02:54:58:588 | 17-03-2016 02:58:59.480 | 240.892 sec | sonece /s | IMAP4 | 16.3.91 | 49433 | TCP | | |
| 17-03-2016 02:54:58.588 | 17-03-2016 02:58 59.692 | 241.104 sec | 6.3.91 | 49433 | r soneco rs | IMAPA | TCP | | |
| 17-03-2016 02:54:58.788 | 17-03-2016 02:59:27.608 | 268.900 sec | shelart soreco.co.rs | 0 | 6-60-103 static isp.telekom.rs | 2048 | ICMP | | |
| 17-03-2016 02:59:56:796 | 17-03-2016 02:59 57 520 | 0.724 sec | -237-180 static top telekom ra | 55H | pahelant soneco.co.rs | 59168 | TCP | | |
| 17-03-2016 02:59:58.104 | 17-03-2016 02:59:58.356 | 0.252 640 | manishelart soeco.co.rs | 46305 | 6-63-221 static isp.telek.om.rs | SSH | TOP | | |
| 17-03-2016 02:59:58:216 | 17-03-2016 02:59 58:284 | 0.68 sec | institution service core | 45745 | 222.246.173 | MS Office antipiracy/DirectAdmin | TOP | | |
| 17-03-2016 02:54:59 200 | 17-03-2016-02-54-50-555 | 0.775 xec | shelped appears no ra | 55401 | 222 245 253 | 55H | TOP | | |

In order to enable IP address resolution, your NetVizura server should have local or remote commu nication with DNS server (for Hostname) and Internet access (for Whois information). Raw Data table can be exported as a CSV file in order to present captured netflow records as a report to a third party or for further analysis.

To export Raw Data, click on the the Export button in the upper right corner of the Raw Data Table.

| | C Request Names | Details X Clear | | | | | | | A Expo | | |
|---|-------------------------|-------------------------|-------------|----------|------------|----------|------------|------------|--------|--|--|
| | Start Time | End Time | Duration | Src IP O | Src Port O | Dst IP O | Dst Port O | Protocol O | TOS | | |
| | 22-10-2014 09:42:57.940 | 22-10-2014 09:44:56:500 | 118.500 sec | 163 | 59896 | 49.204 | 443 | 6 | 0 | | |
| | 22-10-2014 09:43:15.12 | 22-10-2014 09:44:56:504 | 101.492 500 | 163 | 59898 | 105.140 | 443 | 6 | 0 | | |
| | 22-10-2014 09:44:46:360 | 22-10-2014 09:44:58:580 | 10.220 sec | 19 | 55064 | 204.90 | 80 | 6 | 0 | | |
| | 22-10-2014 02:44:46:456 | 22-10-2014 09:44:58:676 | 10.220 sec | 304.90 | 80 | .19 | 55084 | 6 | 0 | | |
| | 22-10-2014 09:44:56.712 | 22-10-2014 09:44:56.712 | 0.0 sec | 45.148 | 00 | .144 | 54116 | 6 | 0 | | |
| > | 22-10-2014 09:44:27:232 | 22-10-2014 09:44:57:596 | 30.364 sec | 67 | 36177 | 106.253 | 443 | 6 | 0 | | |
| | 22-10-2014 09:44 27:492 | 22-10-2014 09:44:57.568 | 30.78 sec | 166.253 | 443 | .67 | 36177 | 6 | 0 | | |
| | 22-10-2014 09:39 58:44 | 22-10-2014 09:39:58.44 | 0.0 sec | 10.004 | 64478 | 94.2 | 53 | 17 | 0 | | |
| | 22-10-2014 09:39:58.108 | 22-10-2014 09:44:28:412 | 270.304 sec | 143 | 57581 | 06.188 | 5228 | 6 | 0 | | |
| | 22-10-2014 09:39:58.184 | 22-10-2014 09:44:28:188 | 270.4 sec | 1.09 | 12975 | .164 | 1619 | 6 | 0 | | |
| | 22-10-2014 09:39:58:428 | 22-10-2014 09:42:31.984 | 153.558 sec | 4 | 53013 | 94.2 | 53 | 17 | 0 | | |
| | 22-10-2014 09:39 58 820 | 22-10-2014 09:44:43:656 | 284.836 sec | 13.125 | 5222 | 108 | 49712 | 6 | 0 | | |
| | 22-10-2014 09:39:58.820 | 22-10-2014 09:44:43:608 | 284.788 sec | 103 | 49712 | 30.125 | 5222 | 6 | 0 | | |
| | 22-10-2014 09:44:53.464 | 22-10-2014 09:44:58:576 | 5.112 500 | 76.148 | 80 | .144 | 54152 | 6 | 0 | | |
| | 22-10-2014 09:44:40:52 | 22-10-2014 09:44:56:284 | 18.232 sec | 19 | 54960 | 248.48 | 80 | 6 | 0 | | |
| | 22-10-2014 09:44:40:52 | 22-10-2014 09:44:56:180 | 16.128 sec | 19 | 54991 | 246.43 | 80 | 6 | 0 | | |
| | 22-10-2014 09:44:40.52 | 22-10-2014 09:44:56:32 | 15.980 sec | 19 | 54992 | 245.43 | 80 | 6 | 0 | | |



Grouping, filtering and sorting the raw data table will affect the CSV as well. This will also make a CSV file much smaller.

Depending on the amount of data, export can last a couple of minutes (i)

Depending on your browser settings, browser may ask you were to save the file or it will save the file to a default folder (usually **Downloads** folder). Some spreadsheet software may ask you which separator to use when opening the file - select Comma.