Raw Data Forensics

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

Raw Data Tree groups Raw Data files in folders according to the 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 N Raw Data	Files	Flows			
🖯 🗮 Raw Files	Show Sel	ected Select All			
🖯 🕞 Aug - 2014		-11	-		
🖶 🔛 14. Aug	Select	File	Size		
8 📴 14h		2014-08-14-14-45-00 mls	40.25 1/8		
2014-08-14-14-50-00	8	2014-08-14-14-50-00 //6	40.9 1/8		
2014-08-14-14-55-00.n		2014-08-14-14-55-00 //6	39.66 MB		
🗟 🔚 1Sh		2014-08-14-15-00-00 rds	37.81 MB		
2014-08-14-15-00-00.n		2014-06-14-15-05-00 //16	37.1 MB		
2014-08-14-15-05-00.0		2014-06-14-15-10-00 //16	35.45 1/8		
2014-08-14-15-15-00.n		2014-08-14-15-15-00.nfe	35.83 MB		
2014-08-14-15-20-00.n		2014-00-14-15-20-00.nm	34.95 1/8		
2014-08-14-15-25-00.n		2014-00-14-15-25-00.nm	35.63 MB		
2014-08-14-15-35-00.n		2014-00-14-15-20-00.nm	34.73 1/8		
2014-08-14-15-40-00.n		2014-00-14-15-25-00-10	35.45.103		
		2014-08-14-15-40-00 //18	35.48 149		
		Page 1 of 1 🔻 🔊 🗐	1-12 / 12		

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

Sequest Indexits	and Hannes X thear		Filtering		Grouping					Sorting	A Dep	
Start Time	End Time	Duration	Sec IP U	Sec Poet 0	DSI D	DSLINET O	Pestocal O	T05 ()	TCP Flegs O	Plans 1	Packets	Bales
9-07-2019 15:20:27.979	29-07-2019 15-20:27.979	8.0 MC	90.	42540	29.	26015	6	264	5			-
947-311915-2038-11	29-07-2019 18:28:28.11	8.0 MC	95.	50309	28.	31306	12	364	0004	1		122
9-67-28 29 15:20:27.895	29-07-2019 15:20:27.995	8.0 MC	22.	\$117	79.	25256	12	129	0004			442
947-3119 15:20:27.855	29-07-2019 15:20:27.555	8.0 MC	20	46350	79.	264	12	129	0004	1		31
947-31191522027.871	29-07-2019 15:20:27.971	8.0 MC	139.1	46423	10.	40925	6	264	5			40
947-311935-20.28.87	29-07-2019 15:20:20.07	8.0 MC	66.	23713	10.	\$2	9	129	0004	1		20
9-67-38 19 15:20:27.544	29-07-2019 15:20:27.544	8.0 MC	124.1	\$7110	163.	2111	6	129	5			44
947-311915-20:20.30	29-07-2019 15:28:30.62	2.42 HC	123.	3490	10	29022	9	129	0004	1		96
947-3119 15:20:20.43	29-07-2019 15:28:29.40	8.0 MC	46.	\$4510	10.	9060	9	129	0004			260
947-3119 15:20:27.800	29-07-2019 15:28:27.960	8.0 MC	77.	\$117	79.	25356	9	129	0004	1		445
947-3119 15:20:27.963	29-07-2019 12:28:27.963	8.0 MC	£92.	53	10	21302	9	254	0004			346
947-31191520-20.03	29-07-2019 15-28:29.00	8.0 mc	32.	45005	10.	9000	6	129	5	1		40
947-3119 15:20:20.37	29-07-2019 10:20:20.37	8.0 mc	77.	\$117	79.	25356	9	129	0004			442
947-31191520-30.37	29-07-2019 10:20:20.37	8.0 mc	77.	\$117	29.	25356	9	129	0004	1		442
947-3119 15:20:27.890	29-07-2019 10:28:29.77	0.79 MC	212		153.			129	0004			250
947-3119 15:20:20.20	29-07-2019 15:28:29.20	8.0 mc	77.	\$117	79.	25356	9	120	0004	1		445
947-3119 (5:20:20.26	29-07-2019 12:22:28.26	8.0 mc	115.	17796	153.	60001	6	120	5			40
947-311915-20:20.34	29-07-2019 10:28:28.24	8.0 MC	77.1	\$117	79.	25356	9	120	0004	1		444
947-3119 (5:29:29.33	29-07-2019 12:28:29.55	8.0 mc	173.	443	1672	\$3223	6	120	10			53
947-311915-20:20.74	29-07-2019 10:28:28.74	8.0 MC	192.	\$4905	147.5	445	6	354	5			40
947-3119 (5:29:26.76	29-07-2019 12:22:28-76	8.0 MC	77.	\$117	79.	25356	9	120	0004			441
947-01915-00:0515	29-07-2019 10:20:20.45	8.0 mc	77.4	55746	1477	53	10	354	1014			72
9-17-31 19 15:20:27.897	29-07-2019 10-20:27.997	8.0 mc	77.2	5117	79.	25356	10	120	1014			439
947-319 (5:29:35.95	29-07-0019 10:20:20:55	8.0 mc	77.	5117	29.	25356	10	125	1014			444
948-3119 10 30:09 105	12-02-2012 12:29:53.521	65.796 pec	172	1990	122	63261	12				402	200.500

Clicking on Bidirectional button provides expanded filtering on two pairs of columns:

Src IP and Dst IP

• Src Port and Dst Port

When you enable Bidirectional filtering, filter will be applied not only on filtered column, but also on bidirectional pair of that column. With this option enabled it is easier to find records for some IP address /port without knowledge if that IP address/port is source or destination. In example below, user is searching for one address and one port as source. With Bidirectional option enabled, result where that IP or port are destination will be also returned.

Report Balrecto	Manes X Clear			¥ ¥	<u>í</u>	× .						A 14
Start Time	End Time	Duration	5rc 32 O	Sec Peet O	Doi 19 O	Dst Pert O	Protocel O	T05 0	TCP Flegs O	Flows	Packets	Eates
1072030343408.446	22-07-2228 14:34-08.478	0.32 sei	173.16.0.71	255890	172.16.3.211	181	17	0	none			207
147-2020 14-34-08-446	22-07-2228 14:34-08.478	0.32 sec	172.16.3.211	181	173.16.0.71	35589	17	0	none			241
147-319 143430.77	22 07 29 29 14 34 30 77	0.0 set	173.16.0.71	45532	172 10 4 211	181	17	0	none			72
147-319 143430.77	22-07-2919 14:34:30.77	0.0-sec	172.16.3.211	141	172 18 0.71	49332	17	0	none			24
47-2119 14:39:59.402	22-07-2919-14-40(01.432	2.0 sec	172.16.0.71	400	172.16.3.227	151	17	0	A		2	290
47-2119 14 39:53.425	22-07-2919 14:40:05.995	4.158 sec	172.16.0.71	404	172 16 5 229	151	17	0	A		4	780
47-2119 14:39:59.402	22-07-2919 14:40:65.576	4.144 MC	172.16.0.71	37732	172.15.5.228	151	17	0	A		4	780
47-2119 14:30:50.406	22-07-2919 14:40:03.576	4.140 MC	172.15.0.71	41384	172.15.3.226	151	17	0	A		4	644
47-2119-14-40:03-402	22-07-2919 14:40:03.432	0.0 sec	172.15.0.71	53836	172.15.3.222	151	12	0	A			226
17-2119 14:40:03.406	22-07-2919 14:40:03.436	0.0 mc	172.15.0.71	55312	172.15.3.225	151	12	0	A			2.90
17-2119 14:40:03.406	22-07-2919 14:40:03.600	0.172 mc	172.15.0.71	57713	172.15.13.5	151	12	0	A		6	3,576
17-2019 14:40:00.456	22-07-2919 14:40:03.455	0.0 mc	172.15.3.225	151	172.16.0.71	55312	12	0	A		1	235
17-20129-14140103-460	22-07-22:29 14:40:02.405	0.15 840	172.15.0.71	60225	147.91.5.290	151	12	0	A		2	3,180
07-2019 14:40:03.464	22-07-22/29 14:40(02).464	0.0 мс	172.16.3.222	161	172.16.0.71	\$28.76	12	0	A		1	252
17-2010-14-40/02-468	22-07-22/29 14:40(02).416	0.8 840	172.16.0.71	57234	172.16.0.3	161	12	0	A		2	891
ET-2010 14-40-03-480	22-07-2229 14:40(02.504	0.24 and	172.16.0.71	67115	172.16.4.251	161	12	0	A		2	790
17-2019-14-40-03-900	22-07-2219 14-40-03.512	0.12 sec	172.16.4.251	161	172.16.0.71	\$7115	12	0	Δ.		3	834
17-2029-24-40-02-448	22-07-2229 14-40-03.780	0.132 sec	173.16.0.71	35390	173.16.13.4	181	17	0	A		4	2,889
17-2019 14:35:35.428	22-07-2228 14-40-05-428	6.0 sei	173.18.0.71	36.799	173.18.3.204	181	17	0	A		4	2,618
67-2019 14:40:03:402	22 07 23 29 14 40 05 432	2.0 sei	173.18-0.71	80093	173.16.3.223	181	17	0	A		2	430
17-2019 14:40-03.456	22-07-2219 14-40-05-436	2.0 sec	173.16.0.71	40473	172.16.3.224	183	12	0	A		2	290
17-2019 14:40-05.512	22-07-2219 14-40-05-516	2.4 sec	173.16.0.71	34022	172.16.4.213	163	12	0	A		2	3,294
17 21 29 14:40-03.515	22-07-2919 14:40:05:520	2.4 mm	172.18-0.71	48.383	172.16.4.254	151	17	0	A		2	1,290
17 21 19 14 49:03 894	22-07-2919 14:40:05.805	2.4 sec	172.18-0.71	40061	172.16.13.3	151	12	0	A		2	1,326
47-2119 14:40:07.402	22-07-2919 14:40:07.412	0.0 mm	172.16.0.71	538.10	122.16.3.44	151	12	0	A		1	355

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.

On this page:

- Inspecting Raw Data
- Exporting Raw Data

Request Edvecto	nal Ramon X Clear										A Dep	,et
Start Time	End Time	Deratice		Sec IP O	Sic Port	0	Del IP O	Dst Part O	Pretacel O	105.0	TCP Flags O	
22-67-3019 14 58:21,776	22-07-2019 14:50-21.776	6.0 HC	28			62.		771	109		A.	
2247-3049 14 58:21,704	22407-2018 14:59:21 794	6.0 mc	:57.5	print on	wTTPS	62		49445	102	0	42	
22-07-3019 14 58:21,700	22-07-2019 14:59:21.792	6.4 mc	:22		33725	B17900-12-/3		016	109	0	A	
22-47-3049 14 58:21,796	22-07-2018 14:59:21.796	6.0 mc	:22.1		4015	HIPPOD (2)/7		016	0.09	0	A	
22-47-3049 14 58:21,796	22-07-2019 14:59:21 796	6.0 mc	27.1		45204	62.		25635	109	0	A	
22-47-3049 14 58:21,796	22-07-2018 14:59:21.796	6.0 mc	:22.1		29655	101		1062	0.09	0	A	
22-67-3019 14 58:21.815	22-07-2018 14:50-21.016	6.0 HC		107403-23-73	58363		anapyrawa.com	HTPS	102	0	A	
22-07-2019 14 58:21.424	22-07-2018 14:59:21-804	6.0 mc	:22		49445		content.com	HTPS	102	0	A	
22-47-3049 14 58:21.436	22407-2018 14:50:21.048	8.4 mc	:22		57187	BINGD-13-78		016	LOP	0	A	
247-209 14 51:21.840	22407-2018 14:50:21.048	6.0 MC	172		565 22	INFRC0-12-78		016	LOP	0	Α.	
22-47-3019 14 58:21.936	22-07-2018 14:50:21.906	6.0 HC		anaconava.com				50363	102	0	A	
22-47-3019 14 58:21.976	22-07-2018 14:50:21.976	6.0 MC	_	101410-01-71	Paddross	255		HTTPS	102	0	Α.	
22-07-3019 14:58:21.976	22-07-2018 14:50:21.976	6.0 MC		apres.cs.m	eganization:	Amazon Technologies Inc.		HTTPS	102	0	A	
22-07-3019 14:58:21.904	22-07-2018 14:50:21.904	6.0 MC	:22		etwork Range:	54. 53		016	LOP	0	Α.	
22-07-3209 34 58:06.744	22-07-2018 14:50:21.7%	15.32 mc	172.1		ountry:	Contract Statistic		0005	102	0	5	
22-07-3019 14:58:24.68	22-07-2018 14:50:38,768	6.632.000	172.1		base erant	abusedtamazonavs.com		14008	102	0	AR.	
22-07-3019 14:58:24.324	22-07-2018 14:50:38,756	6.402.000	128.		2000	12.1		4001	102	0	A ¹	
22-07-3019 14:58:24.795	22-07-2018 14:50 38,702	5.956 pec		0100.01/1	54034		.anagonava.com	HTPS	102	0	APROF	
22-07-3109 14:58:24.000	22-07-2018 14:50-38,728	5.040 and		anazonevit.com	WTTPS	82.		54034	102	0	APSE	
22-07-3089 34 58:06.744	22-07-2018 14:50-21.792	15.40 mc	172.1		64409	22.		2005	102	0	5	
22-07-3019 14:58:07.496	22-07-2018 14:50-21.556	14.50 mc	172.		4011	172.		4001	102	0	5	
22-07-3019 14:58:28:524	22-07-2018 14:50 38.624	3.128 eec		107403-02-78	\$5540	801603-0L/8		H5-5Q.	102	0	A24	
22-07-3019 14:58:30.56	22-07-2018 14:50-38, 104	£.40 and		anaprest of	m HTTPS	82.		8003	109	0	A24	
22-07-2019 14:58:20.56	22-07-2018 14:50 28.56	8.0 HIC		KOMINGE OD JIE	\$8700		VINCENTRAL CON	HTMS	109	0	AF.	
22-07-2019 14:50:20.424	22-07-2018 14:50 28,768	6.12N pec		2008/2 (2 12	50890	1000 CT (T		MI-5/1	1/2	0	4212	

If you want to see detailed description for fields in some columns all you need to do is to move mouse cursor over some IP address or port. Provided information is actually detailed description from Display Names section in Settings.

npest Biles	load Henry X G	*										A Esper
Sec IP O	Sec Part O	Del IP O	Ost Pert O	Protecol O	T05 0	TCP Flegs ()	Hims	Peckets	Tates	Throughput	Exporter O	Interface In
72.04.4.200	0	172.16.4.291	2048			A		20	140	8.14596	172.18.4.201	
72.08.4.200	35791	172.06.4.201	181	17		Δ			121		172.16.4.211	
12.06.071	0	172.36.4.251	2048			Δ.		1	400	4.410ps	172.16.4.211	
72.08.4.200	0	172.06.4.201	2048			Δ		10	840	0.410ps	172.16.4.211	
72.34.4.208	38823	172.36.4.281	583	17		A			121		172.16.4.211	
11.0.41	38596	172.36.4.281	583	17		Δ		2	7 Incenter - 177	16479 Care 105 Salte	www.1000.Sethuase.0717	CS-ACADOTICE PROFESSION
72.36.4.205	38284	172.36.4.281	583	17		A			IL ML Venice 12	ATSITIA PELEASE SCIETA	AME INZ	
72.36.4.205	0	172.36.4.251	2048			Δ		10	p- Technical Supp	ert hilly.//www.cbce.ce	mitecharaport	
11.0.0.11	0	172.36.4.251	2048			A		13	¹ Carepled Tue	17-hep-10 1208 by and	HE SHARE	
72.36.4.205	36383	172.36.4.251	583	17		A			101		22.16.4.211	1
72.36.4.205	0	172.36.4.251	2048			A		10	840	9.140ps	173.16.4.211	
11.0.0.0	0	172.36.4.251	2048			A		8	400	5.110ps	173.16.4.211	
11.0.0.0	46243	172.36.4.251	383	17		A		2	780	35.5Xbps	173.16.4.211	
72.36.4.305	33906	172.36.4.251	181	17		A			321		173.16.4.211	
17.08.071	0	172.16.4.251	2048			A		5	430	5.2 Hop	173.16.4.251	
72.36.4.305	0	172.16.4.251	2048			A		30	1,688	783.0 hps	172.16.4.251	
72.36.4.305	55839	172.16.4.251	181	17	1	A			121		172.16.4.251	
72.86.71	0	172.16.4.251	2948			A		5	430	5.2 Hop	172.16.4.251	
72.86.71	36771	172.16.4.251	181	17	1	A		2	780	34,790pp	172.16.4.251	
72.36.4.205	0	172.16.4.251	2948			A		10	840	13.490pp	172.16.4.251	
72.36.4.205	45826	172.16.4.251	151	17	1	A			321		172.16.4.251	
72.36.4.205	47573	172.16.4.251	151	17	1	A			121		172.16.4.251	
72.86.71	0	172.16.4.251	2946		1	A		15	1,250	611,2000	172.16.4.251	
72.36.4.205	0	172.16.4.251	2948		1	A		10	840	0.5Hbps	172.16.4.251	
72.860.71	40391	172.95.4.251	161	12	1		1	2	280	72.1 i/hm	122.16.6.203	1

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).

Exporting Raw Data

(i)

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.

Report (Mirectio	nel Harres X Gear											
Start Time	End Time	Duration	Sec IP O	Src Port O	Det IP O	Dot Port O	Protocol O	TOS O	TCP Flogs O	Flores	Peckets	Dytes
11-07-2019 20-49-09-190	25-07-0039-23-49-09-175	0.25 sec	172.16.3.211	261	172.16.0.71	38216	17	0	nare			245
11-07-2010 2010-2018	21-07-3010-23-52-28-425	0.8 smi	172.16.3.211	43779	172.16.1.201	8200	4	0	1			60
11-07-0010 23-40-30-250	21-07-3110-23-49-30-311	0.1 sm	172.16.3.211	28.1	172.16.4.201	32298	17	0	nare			79
11-07-0010 23-40-30-287	21-07-3119-23-49-30-388	0.1 sm	172.16.3.211	28.1	172.16.0.71	49002	17	0	nare			79
11-07-0010 20:02:30.389	21-07-3119-23-32-30-344	0.139 and	172.16.3.211	3666	172.16.0.71	40268	4	0	APR P		1	1,348
11-07-0010 23:30:00.334	21-CP-3019-23-55-00-118	0.1 441	172.16.3.211	28.1	172.16.4.201	32004	17	0	nare			79
11-07-2010 23:33:00.394	21-07-3019-23.53:00.382	0.188 and	172.16.3.211	3666	172.16.0.71	41218	4	0	APR P		1.00	1,205
11-07-0219 23:35:00.404	21-07-3019-23.55(00.996	0.172 (e)(172.16.3.211	3666	172.16.0.71	4946	4	0	APR P		1.00	1,205
11-07-2010 23:35:00.436	21-07-3019-23.55(00.304	0.68 and	172.16.3.211	22	172.16.0.71	42228	4	0	1712		8	1,389
11-07-2010 23:34:39.412	21-07-3019-23-34-39-412	0.0 and	172.16.3.211	28.1	172.16.4.201	49622	17	0	A			79
11-07-0219 23:34:39.494	21-07-3019-23.55(00.308	0.824 and	172.16.3.211		172.16.4.201			0	A		10	340
11-07-2019 23:35:00.360	21-07-3019-23.55(00.300	0.0 and	172.36.3.211	23990	172.16.0.71	2088	17	0	A			964
11-07-2010 23:35:00.372	21-07-3019-23.55(00.372	0.0 and	172.16.3.211	23990	172.16.4.217	2088	17	0	A			964
11-07-2010 23:35:00.372	21-07-3019-23.55(00.372	0.0 and	172.36.3.211	23990	172.16.1.47	2065	17	0	A			964
11-07-2010 23:56:00.372	21-07-3019-23.55(00.372	0.0 acc	172.16.3.211	23990	172.16.4.203	2065	17	0	A			964
11-07-2010 23:56:00.372	21-07-3019-23.55(00.372	0.0 acc	172.16.3.211	23990	172.16.2.83	2065	17	0	Α.			964
11-07-2019 22:55:00.372	21-07-3019-23.55(00.372	0.0-840	172.16.3.211	23990	172.16.4.239	2065	17	0	Α.			964
11-07-2019 22:55:00.372	21-07-3019-23.55(00.372	0.0-840	172.16.3.211	23990	172.16.4.201	2065	17	0	Α.			964
11-07-2019 22:55:00.372	21-07-3019-23.55(00.372	0.0440	172.16.3.211	23990	172.16.4.214	2065	17	0	Α.			964
11-07-2019 22:55:00.372	21-07-3019-23.55(00.372	0.0-000	172.16.3.211	23990	172.16.4.212	2065	17	0	Α.		2	1,828
11-07-2019 22:55:00.372	21-07-3019-23.55(00.372	0.0440	172.16.3.211	23990	172.16.4.230	2065	17	0	Α.			964
1-07-2019 22:55:00.372	21-07-0009-23.55:00.372	0.0 MC	172.16.3.211	29990	172.16.2.192	2065	10	0	Α.			964
11-07-2019 22:55:00.372	21-07-0009-23.55:00.372	0.0 MC	172.16.3.211	29990	172.16.4.215	2065	10	0	Α.			964
1-07-2019 22:55:00.372	25-67-30 29 23 55:00.372	0.0 MC	172.16.3.211	23990	172.16.4.205	2055	13	0	Α.			964
11-07-2019 22:55:00.372	21-07-2019 23 55:00.172	0.0 MC	172.16.3.211	29990	172.16.4.212	2055	12	0	Δ.			964

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

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**.

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