Network features

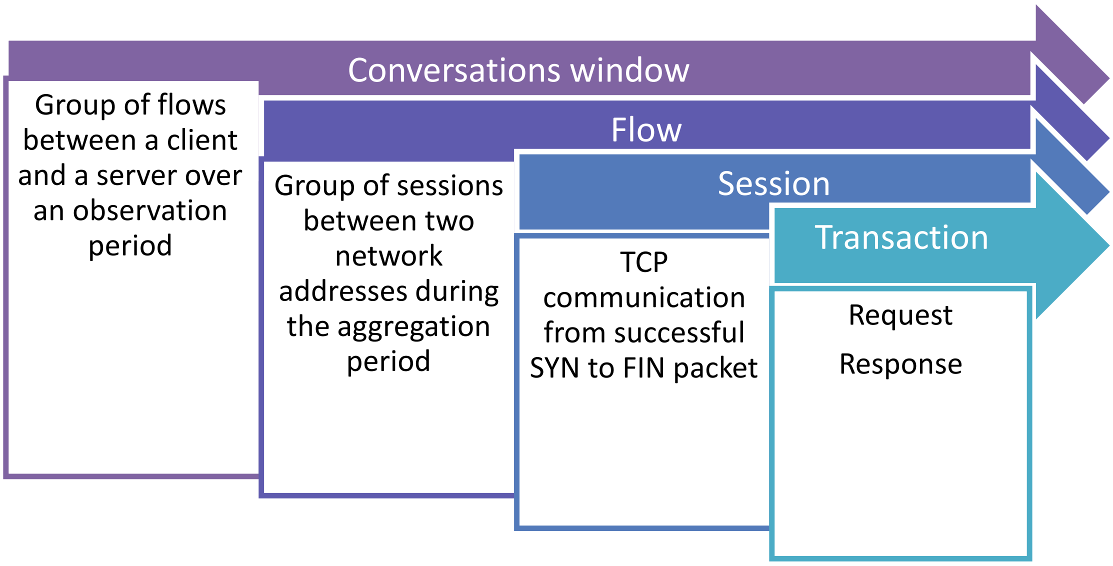
Conversations window
Group of flows between a client and a server over an observation period
Flow
Group of sessions between two network addresses during the aggregation period
Session
TCP communication from successful SYN to FIN packet
Transaction
Request
Response

Figure 1: Data stream encapsulated types

- **Transaction** – represents an interaction between a client and a server. It is a two-way communication: the client sends a request to the server, and the server processes the request and sends a response back to the client. We handle the following types of transactions:
  - An HTTP transaction consists of sending one request and response message between a client and a server
  - A DNS transaction is equivalent to one session with two packets, one for the request and another for the response with the same transaction ID.
  - An SSL transaction is the aggregation of all App-data packets sent from a client to a server and vice versa after a successful handshake step and until the session ends.
- **Session** – A unique 4-tuple consisting of source and destination IP addresses and port numbers.
  - A TCP session begins with a successful handshake, and ends with one of the following: Timeout, packet with the RST or FIN flag from any of the devices.
  - A UDP session consists of all packets sent from a client to a server and from a server to a client until a defined communication idle time is reached.
- **Flow** – A group of sessions between two network addresses (IP pair) during the aggregation period. The aggregation period can be specified by an algorithm as the accurate period of time from the start of the first session in the flow, until the maximum idle time between two sessions. A new flow starts iff the time between the end of a session (the last packet) and the start of a new session (first packet) is more than the defined idle time. The new session is then part of the new flow.
- **Conversation** – A group of flows between a client and a server over an observation period. A conversation can be defined between two network addresses (IP pair) or a group of network resources, (e.g., between two autonomous system).

Full features list

#	Feature	Observation level		Description
1	cw_count_asn	Conversation Window		Number of autonomus sytems participated in communication
2	cw_count_country	Conversation Window		Number of countries participated in communication
3	cw_count_flows	Conversation Window		Number of flows in conversation window
4	cw_dns_bad_additionals_avg	Conversation Window	Average	Number of additional fields in bad DNS response
5	cw_dns_bad_additionals_entropy	Conversation Window	Entropy	Number of additional fields in bad DNS response
6	cw_dns_bad_additionals_firstQ	Conversation Window	First quartile	Number of additional fields in bad DNS response
7	cw_dns_bad_additionals_max	Conversation Window	Maximum	Number of additional fields in bad DNS response
8	cw_dns_bad_additionals_median	Conversation Window	Median	Number of additional fields in bad DNS response
9	cw_dns_bad_additionals_min	Conversation Window	Minimum	Number of additional fields in bad DNS response
10	cw_dns_bad_additionals_stdev	Conversation Window	Standard deviation	Number of additional fields in bad DNS response
11	cw_dns_bad_additionals_sum	Conversation Window	Sum	Number of additional fields in bad DNS response
12	cw_dns_bad_additionals_thirdQ	Conversation Window	Third quartile	Number of additional fields in bad DNS response
13	cw_dns_bad_additionals_var	Conversation Window	Variance	Number of additional fields in bad DNS response
14	cw_dns_bad_answers_avg	Conversation Window	Average	Number of answer fields in bad DNS response
15	cw_dns_bad_answers_entropy	Conversation Window	Entropy	Number of answer fields in bad DNS response
16	cw_dns_bad_answers_firstQ	Conversation Window	First quartile	Number of answer fields in bad DNS response
17	cw_dns_bad_answers_max	Conversation Window	Maximum	Number of answer fields in bad DNS response
18	cw_dns_bad_answers_median	Conversation Window	Median	Number of answer fields in bad DNS response
19	cw_dns_bad_answers_min	Conversation Window	Minimum	Number of answer fields in bad DNS response
20	cw_dns_bad_answers_stdev	Conversation Window	Standard deviation	Number of answer fields in bad DNS response
21	cw_dns_bad_answers_sum	Conversation Window	Sum	Number of answer fields in bad DNS response
22	cw_dns_bad_answers_thirdQ	Conversation Window	Third quartile	Number of answer fields in bad DNS response
23	cw_dns_bad_answers_var	Conversation Window	Variance	Number of answer fields in bad DNS response
24	cw_dns_bad_authoritative_avg	Conversation Window	Average	Number of authoritative fields in bad DNS response
25	cw_dns_bad_authoritative_entropy	Conversation Window	Entropy	Number of authoritative fields in bad DNS response
26	cw_dns_bad_authoritative_firstQ	Conversation Window	First quartile	Number of authoritative fields in bad DNS response
27	cw_dns_bad_authoritative_max	Conversation Window	Maximum	Number of authoritative fields in bad DNS response
28	cw_dns_bad_authoritative_median	Conversation Window	Median	Number of authoritative fields in bad DNS response
29	cw_dns_bad_authoritative_min	Conversation Window	Minimum	Number of authoritative fields in bad DNS response
30	cw_dns_bad_authoritative_stdev	Conversation Window	Standard deviation	Number of authoritative fields in bad DNS response
31	cw_dns_bad_authoritative_sum	Conversation Window	Sum	Number of authoritative fields in bad DNS response

32	cw_dns_bad_authoritative_thirdQ	Conversation Window	Third quartile	Number of authoritative fields in bad DNS response
33	cw_dns_bad_authoritative_var	Conversation Window	Variance	Number of authoritative fields in bad DNS response
34	cw_dns_bad_count	Conversation Window		Number of bad DNS responses
35	cw_dns_bad_count_flags	Conversation Window		Number of unique flags combinations
36	cw_dns_bad_dom_flag	Conversation Window		Dominated DNS flags combination in bad DNS responses
37	cw_dns_bad_queries_avg	Conversation Window	Average	Number of query fields in bad DNS response
38	cw_dns_bad_queries_entropy	Conversation Window	Entropy	Number of query fields in bad DNS response
39	cw_dns_bad_queries_firstQ	Conversation Window	First quartile	Number of query fields in bad DNS response
40	cw_dns_bad_queries_max	Conversation Window	Maximum	Number of query fields in bad DNS response
41	cw_dns_bad_queries_median	Conversation Window	Median	Number of query fields in bad DNS response
42	cw_dns_bad_queries_min	Conversation Window	Minimum	Number of query fields in bad DNS response
43	cw_dns_bad_queries_stdev	Conversation Window	Standard deviation	Number of query fields in bad DNS response
44	cw_dns_bad_queries_sum	Conversation Window	Sum	Number of query fields in bad DNS response
45	cw_dns_bad_queries_thirdQ	Conversation Window	Third quartile	Number of query fields in bad DNS response
46	cw_dns_bad_queries_var	Conversation Window	Variance	Number of query fields in bad DNS response
47	cw_dns_bad_tcp_sess_ratio	Conversation Window		Ratio between number of UDP sessions and bad DNS responses
48	cw_dns_bad_udp_sess_ratio	Conversation Window		Ratio between number of TCP sessions and bad DNS responses
49	cw_dns_good_count	Conversation Window		Number of good DNS responses
50	cw_dns_good_tcp_sess_ratio	Conversation Window		Ratio between number of UDP sessions and good DNS responses
51	cw_dns_good_udp_sess_ratio	Conversation Window		Ratio between number of TCP sessions and good DNS responses
52	cw_dst_ports	Conversation Window		Number of destination ports
53	cw_dst_ports_flows_ratio	Conversation Window		Ratio between number of destination ports and number of flows
54	cw_dst_ports_sessions_ratio	Conversation Window		Ratio between number of destination ports and number of sessions
55	cw_duration	Conversation Window		Conversation window duration
56	cw_flow_bytes_A_avg	Conversation Window	Average	Number of bytes sent by client
57	cw_flow_bytes_A_entropy	Conversation Window	Entropy	Number of bytes sent by client
58	cw_flow_bytes_A_firstQ	Conversation Window	First quartile	Number of bytes sent by client
59	cw_flow_bytes_A_max	Conversation Window	Maximum	Number of bytes sent by client
60	cw_flow_bytes_A_median	Conversation Window	Median	Number of bytes sent by client
61	cw_flow_bytes_A_min	Conversation Window	Minimum	Number of bytes sent by client
62	cw_flow_bytes_A_stdev	Conversation Window	Standard deviation	Number of bytes sent by client
63	cw_flow_bytes_A_sum	Conversation Window	Sum	Number of bytes sent by client
64	cw_flow_bytes_A_thirdQ	Conversation Window	Third quartile	Number of bytes sent by client
65	cw_flow_bytes_A_var	Conversation Window	Variance	Number of bytes sent by client
66	cw_flow_bytes_B_avg	Conversation Window	Average	Number of bytes sent by server

67	cw_flow_bytes_B_entropy	Conversation Window	Entropy	Number of bytes sent by server
68	cw_flow_bytes_B_firstQ	Conversation Window	First quartile	Number of bytes sent by server
69	cw_flow_bytes_B_max	Conversation Window	Maximum	Number of bytes sent by server
70	cw_flow_bytes_B_median	Conversation Window	Median	Number of bytes sent by server
71	cw_flow_bytes_B_min	Conversation Window	Minimum	Number of bytes sent by server
72	cw_flow_bytes_B_stdev	Conversation Window	Standard deviation	Number of bytes sent by server
73	cw_flow_bytes_B_sum	Conversation Window	Sum	Number of bytes sent by server
74	cw_flow_bytes_B_thirdQ	Conversation Window	Third quartile	Number of bytes sent by server
75	cw_flow_bytes_B_var	Conversation Window	Variance	Number of bytes sent by server
76	cw_flow_bytes_avg	Conversation Window	Average	Number of bytes sent and received
77	cw_flow_bytes_entropy	Conversation Window	Entropy	Number of bytes sent and received
78	cw_flow_bytes_firstQ	Conversation Window	First quartile	Number of bytes sent and received
79	cw_flow_bytes_max	Conversation Window	Maximum	Number of bytes sent and received
80	cw_flow_bytes_median	Conversation Window	Median	Number of bytes sent and received
81	cw_flow_bytes_min	Conversation Window	Minimum	Number of bytes sent and received
82	cw_flow_bytes_stdev	Conversation Window	Standard deviation	Number of bytes sent and received
83	cw_flow_bytes_sum	Conversation Window	Sum	Number of bytes sent and received
84	cw_flow_bytes_thirdQ	Conversation Window	Third quartile	Number of bytes sent and received
85	cw_flow_bytes_var	Conversation Window	Variance	Number of bytes sent and received
86	cw_flow_duration_avg	Conversation Window	Average	Flow duration
87	cw_flow_duration_entropy	Conversation Window	Entropy	Flow duration
88	cw_flow_duration_firstQ	Conversation Window	First quartile	Flow duration
89	cw_flow_duration_max	Conversation Window	Maximum	Flow duration
90	cw_flow_duration_median	Conversation Window	Median	Flow duration
91	cw_flow_duration_min	Conversation Window	Minimum	Flow duration
92	cw_flow_duration_stdev	Conversation Window	Standard deviation	Flow duration
93	cw_flow_duration_sum	Conversation Window	Sum	Flow duration
94	cw_flow_duration_thirdQ	Conversation Window	Third quartile	Flow duration
95	cw_flow_duration_var	Conversation Window	Variance	Flow duration
96	cw_flow_packets_A_avg	Conversation Window	Average	Number of packets sent by client
97	cw_flow_packets_A_entropy	Conversation Window	Entropy	Number of packets sent by client
98	cw_flow_packets_A_firstQ	Conversation Window	First quartile	Number of packets sent by client
99	cw_flow_packets_A_max	Conversation Window	Maximum	Number of packets sent by client
100	cw_flow_packets_A_median	Conversation Window	Median	Number of packets sent by client
101	cw_flow_packets_A_min	Conversation Window	Minimum	Number of packets sent by client

102	cw_flow_packets_A_stdev	Conversation Window	Standard deviation	Number of packets sent by client
103	cw_flow_packets_A_sum	Conversation Window	Sum	Number of packets sent by client
104	cw_flow_packets_A_thirdQ	Conversation Window	Third quartile	Number of packets sent by client
105	cw_flow_packets_A_var	Conversation Window	Variance	Number of packets sent by client
106	cw_flow_packets_B_avg	Conversation Window	Average	Number of packets sent by server
107	cw_flow_packets_B_entropy	Conversation Window	Entropy	Number of packets sent by server
108	cw_flow_packets_B_firstQ	Conversation Window	First quartile	Number of packets sent by server
109	cw_flow_packets_B_max	Conversation Window	Maximum	Number of packets sent by server
110	cw_flow_packets_B_median	Conversation Window	Median	Number of packets sent by server
111	cw_flow_packets_B_min	Conversation Window	Minimum	Number of packets sent by server
112	cw_flow_packets_B_stdev	Conversation Window	Standard deviation	Number of packets sent by server
113	cw_flow_packets_B_sum	Conversation Window	Sum	Number of packets sent by server
114	cw_flow_packets_B_thirdQ	Conversation Window	Third quartile	Number of packets sent by server
115	cw_flow_packets_B_var	Conversation Window	Variance	Number of packets sent by server
116	cw_flow_packets_avg	Conversation Window	Average	Number of packets sent and received
117	cw_flow_packets_entropy	Conversation Window	Entropy	Number of packets sent and received
118	cw_flow_packets_firstQ	Conversation Window	First quartile	Number of packets sent and received
119	cw_flow_packets_max	Conversation Window	Maximum	Number of packets sent and received
120	cw_flow_packets_median	Conversation Window	Median	Number of packets sent and received
121	cw_flow_packets_min	Conversation Window	Minimum	Number of packets sent and received
122	cw_flow_packets_stdev	Conversation Window	Standard deviation	Number of packets sent and received
123	cw_flow_packets_sum	Conversation Window	Sum	Number of packets sent and received
124	cw_flow_packets_thirdQ	Conversation Window	Third quartile	Number of packets sent and received
125	cw_flow_packets_var	Conversation Window	Variance	Number of packets sent and received
126	cw_http_count_host	Conversation Window		Number of HTTP hosts
127	cw_sessions_flow_ratio	Conversation Window		Ratio between number of sessions and number of flows
128	cw_src_ports	Conversation Window		Number of source ports
129	cw_src_ports_flows_ratio	Conversation Window		Ratio between number of source ports and number of flows
130	cw_src_ports_sessions_ratio	Conversation Window		Ratio between number of source ports and number of sessions
131	cw_ssl_count_server_name	Conversation Window		Number of SSL servers
132	cw_tcp_analysis_duplicate_ack	Conversation Window		Number of packets with duplicake ACKs
133	cw_tcp_analysis_keep_alive	Conversation Window		Number of Keep Alive packets
134	cw_tcp_analysis_lost_segment	Conversation Window		Number of lost segments
135	cw_tcp_analysis_out_of_order	Conversation Window		Number of packets received out of order
136	cw_tcp_analysis_retransmission	Conversation Window		Number of retransmitted packets

137	cw_tcp_analysis_reused_ports	Conversation Window		Number of reused ports
138	cw_tcp_bytes_A_avg	Conversation Window	Average	Number of bytes sent by client over TCP
139	cw_tcp_bytes_A_entropy	Conversation Window	Entropy	Number of bytes sent by client over TCP
140	cw_tcp_bytes_A_firstQ	Conversation Window	First quartile	Number of bytes sent by client over TCP
141	cw_tcp_bytes_A_max	Conversation Window	Maximum	Number of bytes sent by client over TCP
142	cw_tcp_bytes_A_median	Conversation Window	Median	Number of bytes sent by client over TCP
143	cw_tcp_bytes_A_min	Conversation Window	Minimum	Number of bytes sent by client over TCP
144	cw_tcp_bytes_A_stdev	Conversation Window	Standard deviation	Number of bytes sent by client over TCP
145	cw_tcp_bytes_A_sum	Conversation Window	Sum	Number of bytes sent by client over TCP
146	cw_tcp_bytes_A_thirdQ	Conversation Window	Third quartile	Number of bytes sent by client over TCP
147	cw_tcp_bytes_A_var	Conversation Window	Variance	Number of bytes sent by client over TCP
148	cw_tcp_bytes_B_avg	Conversation Window	Average	Number of bytes sent by server over TCP
149	cw_tcp_bytes_B_entropy	Conversation Window	Entropy	Number of bytes sent by server over TCP
150	cw_tcp_bytes_B_firstQ	Conversation Window	First quartile	Number of bytes sent by server over TCP
151	cw_tcp_bytes_B_max	Conversation Window	Maximum	Number of bytes sent by server over TCP
152	cw_tcp_bytes_B_median	Conversation Window	Median	Number of bytes sent by server over TCP
153	cw_tcp_bytes_B_min	Conversation Window	Minimum	Number of bytes sent by server over TCP
154	cw_tcp_bytes_B_stdev	Conversation Window	Standard deviation	Number of bytes sent by server over TCP
155	cw_tcp_bytes_B_sum	Conversation Window	Sum	Number of bytes sent by server over TCP
156	cw_tcp_bytes_B_thirdQ	Conversation Window	Third quartile	Number of bytes sent by server over TCP
157	cw_tcp_bytes_B_var	Conversation Window	Variance	Number of bytes sent by server over TCP
158	cw_tcp_bytes_avg	Conversation Window	Average	Number of bytes sent and received over TCP
159	cw_tcp_bytes_entropy	Conversation Window	Entropy	Number of bytes sent and received over TCP
160	cw_tcp_bytes_firstQ	Conversation Window	First quartile	Number of bytes sent and received over TCP
161	cw_tcp_bytes_max	Conversation Window	Maximum	Number of bytes sent and received over TCP
162	cw_tcp_bytes_median	Conversation Window	Median	Number of bytes sent and received over TCP
163	cw_tcp_bytes_min	Conversation Window	Minimum	Number of bytes sent and received over TCP
164	cw_tcp_bytes_stdev	Conversation Window	Standard deviation	Number of bytes sent and received over TCP
165	cw_tcp_bytes_sum	Conversation Window	Sum	Number of bytes sent and received over TCP
166	cw_tcp_bytes_thirdQ	Conversation Window	Third quartile	Number of bytes sent and received over TCP
167	cw_tcp_bytes_var	Conversation Window	Variance	Number of bytes sent and received over TCP
168	cw_tcp_count_sessions	Conversation Window		Number of TCP sessions
169	cw_tcp_duration_avg	Conversation Window	Average	Duration of TCP sessions
170	cw_tcp_duration_entropy	Conversation Window	Entropy	Duration of TCP sessions
171	cw_tcp_duration_firstQ	Conversation Window	First quartile	Duration of TCP sessions

172	cw_tcp_duration_max	Conversation Window	Maximum	Duration of TCP sessions
173	cw_tcp_duration_median	Conversation Window	Median	Duration of TCP sessions
174	cw_tcp_duration_min	Conversation Window	Minimum	Duration of TCP sessions
175	cw_tcp_duration_stdev	Conversation Window	Standard deviation	Duration of TCP sessions
176	cw_tcp_duration_sum	Conversation Window	Sum	Duration of TCP sessions
177	cw_tcp_duration_thirdQ	Conversation Window	Third quartile	Duration of TCP sessions
178	cw_tcp_duration_var	Conversation Window	Variance	Duration of TCP sessions
179	cw_tcp_packets_A_avg	Conversation Window	Average	Number of packets sent by client over TCP
180	cw_tcp_packets_A_entropy	Conversation Window	Entropy	Number of packets sent by client over TCP
181	cw_tcp_packets_A_firstQ	Conversation Window	First quartile	Number of packets sent by client over TCP
182	cw_tcp_packets_A_max	Conversation Window	Maximum	Number of packets sent by client over TCP
183	cw_tcp_packets_A_median	Conversation Window	Median	Number of packets sent by client over TCP
184	cw_tcp_packets_A_min	Conversation Window	Minimum	Number of packets sent by client over TCP
185	cw_tcp_packets_A_stdev	Conversation Window	Standard deviation	Number of packets sent by client over TCP
186	cw_tcp_packets_A_sum	Conversation Window	Sum	Number of packets sent by client over TCP
187	cw_tcp_packets_A_thirdQ	Conversation Window	Third quartile	Number of packets sent by client over TCP
188	cw_tcp_packets_A_var	Conversation Window	Variance	Number of packets sent by client over TCP
189	cw_tcp_packets_B_avg	Conversation Window	Average	Number of packets sent by server over TCP
190	cw_tcp_packets_B_entropy	Conversation Window	Entropy	Number of packets sent by server over TCP
191	cw_tcp_packets_B_firstQ	Conversation Window	First quartile	Number of packets sent by server over TCP
192	cw_tcp_packets_B_max	Conversation Window	Maximum	Number of packets sent by server over TCP
193	cw_tcp_packets_B_median	Conversation Window	Median	Number of packets sent by server over TCP
194	cw_tcp_packets_B_min	Conversation Window	Minimum	Number of packets sent by server over TCP
195	cw_tcp_packets_B_stdev	Conversation Window	Standard deviation	Number of packets sent by server over TCP
196	cw_tcp_packets_B_sum	Conversation Window	Sum	Number of packets sent by server over TCP
197	cw_tcp_packets_B_thirdQ	Conversation Window	Third quartile	Number of packets sent by server over TCP
198	cw_tcp_packets_B_var	Conversation Window	Variance	Number of packets sent by server over TCP
199	cw_tcp_packets_avg	Conversation Window	Average	Number of packets sent and received over TCP
200	cw_tcp_packets_entropy	Conversation Window	Entropy	Number of packets sent and received over TCP
201	cw_tcp_packets_firstQ	Conversation Window	First quartile	Number of packets sent and received over TCP
202	cw_tcp_packets_max	Conversation Window	Maximum	Number of packets sent and received over TCP
203	cw_tcp_packets_median	Conversation Window	Median	Number of packets sent and received over TCP
204	cw_tcp_packets_min	Conversation Window	Minimum	Number of packets sent and received over TCP
205	cw_tcp_packets_stdev	Conversation Window	Standard deviation	Number of packets sent and received over TCP
206	cw_tcp_packets_sum	Conversation Window	Sum	Number of packets sent and received over TCP

207	cw_tcp_packets_thirdQ	Conversation Window	Third quartile	Number of packets sent and received over TCP
208	cw_tcp_packets_var	Conversation Window	Variance	Number of packets sent and received over TCP
209	cw_tcp_udp_ratio	Conversation Window		Ratio between number of UDP sessions and number of TCP sessions
210	cw_udp_count_sessions	Conversation Window		Number of UDP sessions
211	cw_udp_dst_ports	Conversation Window		Number of UDP destination ports
212	cw_udp_dst_ports_sessions_ratio	Conversation Window		Ratio between number of UDP destination ports and number of UDP sessions
213	cw_udp_sess_bytes_A_avg	Conversation Window	Average	Number of bytes sent by client over UDP
214	cw_udp_sess_bytes_A_entropy	Conversation Window	Entropy	Number of bytes sent by client over UDP
215	cw_udp_sess_bytes_A_firstQ	Conversation Window	First quartile	Number of bytes sent by client over UDP
216	cw_udp_sess_bytes_A_max	Conversation Window	Maximum	Number of bytes sent by client over UDP
217	cw_udp_sess_bytes_A_median	Conversation Window	Median	Number of bytes sent by client over UDP
218	cw_udp_sess_bytes_A_min	Conversation Window	Minimum	Number of bytes sent by client over UDP
219	cw_udp_sess_bytes_A_stdev	Conversation Window	Standard deviation	Number of bytes sent by client over UDP
220	cw_udp_sess_bytes_A_sum	Conversation Window	Sum	Number of bytes sent by client over UDP
221	cw_udp_sess_bytes_A_thirdQ	Conversation Window	Third quartile	Number of bytes sent by client over UDP
222	cw_udp_sess_bytes_A_var	Conversation Window	Variance	Number of bytes sent by client over UDP
223	cw_udp_sess_bytes_B_avg	Conversation Window	Average	Number of bytes sent by server over UDP
224	cw_udp_sess_bytes_B_entropy	Conversation Window	Entropy	Number of bytes sent by server over UDP
225	cw_udp_sess_bytes_B_firstQ	Conversation Window	First quartile	Number of bytes sent by server over UDP
226	cw_udp_sess_bytes_B_max	Conversation Window	Maximum	Number of bytes sent by server over UDP
227	cw_udp_sess_bytes_B_median	Conversation Window	Median	Number of bytes sent by server over UDP
228	cw_udp_sess_bytes_B_min	Conversation Window	Minimum	Number of bytes sent by server over UDP
229	cw_udp_sess_bytes_B_stdev	Conversation Window	Standard deviation	Number of bytes sent by server over UDP
230	cw_udp_sess_bytes_B_sum	Conversation Window	Sum	Number of bytes sent by server over UDP
231	cw_udp_sess_bytes_B_thirdQ	Conversation Window	Third quartile	Number of bytes sent by server over UDP
232	cw_udp_sess_bytes_B_var	Conversation Window	Variance	Number of bytes sent by server over UDP
233	cw_udp_sess_bytes_avg	Conversation Window	Average	Number of bytes sent and received over UDP
234	cw_udp_sess_bytes_entropy	Conversation Window	Entropy	Number of bytes sent and received over UDP
235	cw_udp_sess_bytes_firstQ	Conversation Window	First quartile	Number of bytes sent and received over UDP
236	cw_udp_sess_bytes_max	Conversation Window	Maximum	Number of bytes sent and received over UDP
237	cw_udp_sess_bytes_median	Conversation Window	Median	Number of bytes sent and received over UDP
238	cw_udp_sess_bytes_min	Conversation Window	Minimum	Number of bytes sent and received over UDP
239	cw_udp_sess_bytes_stdev	Conversation Window	Standard deviation	Number of bytes sent and received over UDP
240	cw_udp_sess_bytes_sum	Conversation Window	Sum	Number of bytes sent and received over UDP
241	cw_udp_sess_bytes_thirdQ	Conversation Window	Third quartile	Number of bytes sent and received over UDP

242	cw_udp_sess_bytes_var	Conversation Window	Variance	Number of bytes sent and received over UDP
243	cw_udp_sess_duration_avg	Conversation Window	Average	Duration of UDP sessions
244	cw_udp_sess_duration_entropy	Conversation Window	Entropy	Duration of UDP sessions
245	cw_udp_sess_duration_firstQ	Conversation Window	First quartile	Duration of UDP sessions
246	cw_udp_sess_duration_max	Conversation Window	Maximum	Duration of UDP sessions
247	cw_udp_sess_duration_median	Conversation Window	Median	Duration of UDP sessions
248	cw_udp_sess_duration_min	Conversation Window	Minimum	Duration of UDP sessions
249	cw_udp_sess_duration_stdev	Conversation Window	Standard deviation	Duration of UDP sessions
250	cw_udp_sess_duration_sum	Conversation Window	Sum	Duration of UDP sessions
251	cw_udp_sess_duration_thirdQ	Conversation Window	Third quartile	Duration of UDP sessions
252	cw_udp_sess_duration_var	Conversation Window	Variance	Duration of UDP sessions
253	cw_udp_sess_packets_A_avg	Conversation Window	Average	Number of packets sent by client over UDP
254	cw_udp_sess_packets_A_entropy	Conversation Window	Entropy	Number of packets sent by client over UDP
255	cw_udp_sess_packets_A_firstQ	Conversation Window	First quartile	Number of packets sent by client over UDP
256	cw_udp_sess_packets_A_max	Conversation Window	Maximum	Number of packets sent by client over UDP
257	cw_udp_sess_packets_A_median	Conversation Window	Median	Number of packets sent by client over UDP
258	cw_udp_sess_packets_A_min	Conversation Window	Minimum	Number of packets sent by client over UDP
259	cw_udp_sess_packets_A_stdev	Conversation Window	Standard deviation	Number of packets sent by client over UDP
260	cw_udp_sess_packets_A_sum	Conversation Window	Sum	Number of packets sent by client over UDP
261	cw_udp_sess_packets_A_thirdQ	Conversation Window	Third quartile	Number of packets sent by client over UDP
262	cw_udp_sess_packets_A_var	Conversation Window	Variance	Number of packets sent by client over UDP
263	cw_udp_sess_packets_B_avg	Conversation Window	Average	Number of packets sent by server over UDP
264	cw_udp_sess_packets_B_entropy	Conversation Window	Entropy	Number of packets sent by server over UDP
265	cw_udp_sess_packets_B_firstQ	Conversation Window	First quartile	Number of packets sent by server over UDP
266	cw_udp_sess_packets_B_max	Conversation Window	Maximum	Number of packets sent by server over UDP
267	cw_udp_sess_packets_B_median	Conversation Window	Median	Number of packets sent by server over UDP
268	cw_udp_sess_packets_B_min	Conversation Window	Minimum	Number of packets sent by server over UDP
269	cw_udp_sess_packets_B_stdev	Conversation Window	Standard deviation	Number of packets sent by server over UDP
270	cw_udp_sess_packets_B_sum	Conversation Window	Sum	Number of packets sent by server over UDP
271	cw_udp_sess_packets_B_thirdQ	Conversation Window	Third quartile	Number of packets sent by server over UDP
272	cw_udp_sess_packets_B_var	Conversation Window	Variance	Number of packets sent by server over UDP
273	cw_udp_sess_packets_avg	Conversation Window	Average	Number of packets sent and received over UDP
274	cw_udp_sess_packets_entropy	Conversation Window	Entropy	Number of packets sent and received over UDP
275	cw_udp_sess_packets_firstQ	Conversation Window	First quartile	Number of packets sent and received over UDP
276	cw_udp_sess_packets_max	Conversation Window	Maximum	Number of packets sent and received over UDP

277	cw_udp_sess_packets_median	Conversation Window	Median	Number of packets sent and received over UDP
278	cw_udp_sess_packets_min	Conversation Window	Minimum	Number of packets sent and received over UDP
279	cw_udp_sess_packets_stdev	Conversation Window	Standard deviation	Number of packets sent and received over UDP
280	cw_udp_sess_packets_sum	Conversation Window	Sum	Number of packets sent and received over UDP
281	cw_udp_sess_packets_thirdQ	Conversation Window	Third quartile	Number of packets sent and received over UDP
282	cw_udp_sess_packets_var	Conversation Window	Variance	Number of packets sent and received over UDP
283	cw_udp_src_ports	Conversation Window		Number of UDP source ports
284	cw_udp_src_ports_sessions_ratio	Conversation Window		Ratio between number of UDP source ports and number of UDP sessions
285	flow_ack	Flow		Number of ACK packets sent and received
286	flow_ack_A	Flow		Number of ACK packets sent by client
287	flow_ack_B	Flow		Number of ACK packets sent by server
288	flow_asn_A	Flow		Number of autonomous systems served as client
289	flow_asn_B	Flow		Number of autonomous systems served as server
290	flow_bidirectional	Flow		Is communication in flow established in both directions
291	flow_bytes	Flow		Number of bytes sent and received
292	flow_bytes_A	Flow		Number of bytes sent by client
293	flow_bytes_A_B_ratio	Flow		Ratio between number of bytes sent and number of bytes received
294	flow_bytes_B	Flow		Number of bytes sent by server
295	flow_country_A	Flow		Number of countries systems served as client
296	flow_country_B	Flow		Number of countries systems served as server
297	flow_daysTime	Flow		When during the day communication was established
298	flow_dns_alexaRank	Flow		DNS response server Alexa rank
299	flow_dns_count_additional_records	Flow		Number of additional fields in DNS response
300	flow_dns_count_addresses	Flow		Number of adresses fields in DNS response
301	flow_dns_count_answer_records	Flow		Number of answer fields in DNS response
302	flow_dns_count_authoritative_records	Flow		Number of authoritative fields in DNS response
303	flow_dns_count_canon_names	Flow		Number of canonical names in DNS response
304	flow_dns_flag	Flow		DNS response flags combinations
305	flow_dns_min_ttl	Flow		DNS response minimal time-to-live
306	flow_dns_pre_bad_requests	Flow		Number of preceding bad DNS responses
307	flow_dns_time	Flow		Time took to receive DNS response
308	flow_ds_field_A	Flow		Differentiated Services (DS) field sent by server
309	flow_ds_field_B	Flow		Differentiated Services (DS) field sent by client
310	flow_dst_ports	Flow		Number of destination ports
311	flow_dst_ports_sessions_ratio	Flow		Ratio between number of destination ports and number of sessions

312	flow_duration	Flow		Conversation window duration
313	flow_http_GET	Flow		Number of HTTP requests submited with GET method
314	flow_http_POST	Flow		Number of HTTP requests submited with POST method
315	flow_http_bytes_avg	Flow	Average	Number of bytes sent by client over HTTP
316	flow_http_bytes_entropy	Flow	Entropy	Number of bytes sent by client over HTTP
317	flow_http_bytes_firstQ	Flow	First quartile	Number of bytes sent by client over HTTP
318	flow_http_bytes_max	Flow	Maximum	Number of bytes sent by client over HTTP
319	flow_http_bytes_median	Flow	Median	Number of bytes sent by client over HTTP
320	flow_http_bytes_min	Flow	Minimum	Number of bytes sent by client over HTTP
321	flow_http_bytes_stdev	Flow	Standard deviation	Number of bytes sent by client over HTTP
322	flow_http_bytes_sum	Flow	Sum	Number of bytes sent by client over HTTP
323	flow_http_bytes_thirdQ	Flow	Third quartile	Number of bytes sent by client over HTTP
324	flow_http_bytes_var	Flow	Variance	Number of bytes sent by client over HTTP
325	flow_http_cookie_count	Flow		Total number of cookie values
326	flow_http_cookie_values_avg	Flow	Average	Number of cookie values
327	flow_http_cookie_values_entropy	Flow	Entropy	Number of cookie values
328	flow_http_cookie_values_firstQ	Flow	First quartile	Number of cookie values
329	flow_http_cookie_values_max	Flow	Maximum	Number of cookie values
330	flow_http_cookie_values_median	Flow	Median	Number of cookie values
331	flow_http_cookie_values_min	Flow	Minimum	Number of cookie values
332	flow_http_cookie_values_stdev	Flow	Standard deviation	Number of cookie values
333	flow_http_cookie_values_sum	Flow	Sum	Number of cookie values
334	flow_http_cookie_values_thirdQ	Flow	Third quartile	Number of cookie values
335	flow_http_cookie_values_var	Flow	Variance	Number of cookie values
336	flow_http_count_host	Flow		Number of hosts
337	flow_http_count_req_content_type	Flow		Number of unique content types used in HTTP request
338	flow_http_count_resp_code	Flow		Number of unique HTTP response codes
339	flow_http_count_resp_content_type	Flow		Number of unique HTTP response content type
340	flow_http_count_transactions	Flow		Number HTTP transaction
341	flow_http_count_user_agents	Flow		Number of unique HTTP user agents
342	flow_http_dom_browser	Flow		Dominated HTTP browser
343	flow_http_dom_browser_ver	Flow		Dominated HTTP browser version
344	flow_http_dom_host_alexaRank	Flow		Dominated host Alexa rank
345	flow_http_dom_is_bot	Flow		Is most of HTTP connections created by known bot
346	flow_http_dom_os	Flow		Dominated operating system

347	flow_http_dom_os_ver	Flow		Dominated operating system version
348	flow_http_dom_req_content_type	Flow		Dominated HTTP request contetn type
349	flow_http_dom_resp_code	Flow		Dominated HTTP response code
350	flow_http_dom_resp_content_type	Flow		Dominated HTTP response contetn type
351	flow_http_has_location	Flow		Is HTTP request has location field
352	flow_http_has_referrer	Flow		Is HTTP request has refferer field
353	flow_http_has_req_content_type	Flow		Is HTTP request has content type field
354	flow_http_has_resp_content_type	Flow		Is HTTP response has content type field
355	flow_http_has_user_agent	Flow		Is HTTP request has user agent field
356	flow_http_inter_arrivel_avg	Flow	Average	HTTP request-response inter arrival time
357	flow_http_inter_arrivel_entropy	Flow	Entropy	HTTP request-response inter arrival time
358	flow_http_inter_arrivel_firstQ	Flow	First quartile	HTTP request-response inter arrival time
359	flow_http_inter_arrivel_max	Flow	Maximum	HTTP request-response inter arrival time
360	flow_http_inter_arrivel_median	Flow	Median	HTTP request-response inter arrival time
361	flow_http_inter_arrivel_min	Flow	Minimum	HTTP request-response inter arrival time
362	flow_http_inter_arrivel_stdev	Flow	Standard deviation	HTTP request-response inter arrival time
363	flow_http_inter_arrivel_sum	Flow	Sum	HTTP request-response inter arrival time
364	flow_http_inter_arrivel_thirdQ	Flow	Third quartile	HTTP request-response inter arrival time
365	flow_http_inter_arrivel_var	Flow	Variance	HTTP request-response inter arrival time
366	flow_http_req_bytes_avg	Flow	Average	HTTP request bytes
367	flow_http_req_bytes_entropy	Flow	Entropy	HTTP request bytes
368	flow_http_req_bytes_firstQ	Flow	First quartile	HTTP request bytes
369	flow_http_req_bytes_max	Flow	Maximum	HTTP request bytes
370	flow_http_req_bytes_median	Flow	Median	HTTP request bytes
371	flow_http_req_bytes_min	Flow	Minimum	HTTP request bytes
372	flow_http_req_bytes_stdev	Flow	Standard deviation	HTTP request bytes
373	flow_http_req_bytes_sum	Flow	Sum	HTTP request bytes
374	flow_http_req_bytes_thirdQ	Flow	Third quartile	HTTP request bytes
375	flow_http_req_bytes_var	Flow	Variance	HTTP request bytes
376	flow_http_resp_bytes_avg	Flow	Average	HTTP response bytes
377	flow_http_resp_bytes_entropy	Flow	Entropy	HTTP response bytes
378	flow_http_resp_bytes_firstQ	Flow	First quartile	HTTP response bytes
379	flow_http_resp_bytes_max	Flow	Maximum	HTTP response bytes
380	flow_http_resp_bytes_median	Flow	Median	HTTP response bytes
381	flow_http_resp_bytes_min	Flow	Minimum	HTTP response bytes

382	flow_http_resp_bytes_stdev	Flow	Standard deviation	HTTP response bytes
383	flow_http_resp_bytes_sum	Flow	Sum	HTTP response bytes
384	flow_http_resp_bytes_thirdQ	Flow	Third quartile	HTTP response bytes
385	flow_http_resp_bytes_var	Flow	Variance	HTTP response bytes
386	flow_http_time_avg	Flow	Average	Time took to HTTP server to return response
387	flow_http_time_entropy	Flow	Entropy	Time took to HTTP server to return response
388	flow_http_time_firstQ	Flow	First quartile	Time took to HTTP server to return response
389	flow_http_time_max	Flow	Maximum	Time took to HTTP server to return response
390	flow_http_time_median	Flow	Median	Time took to HTTP server to return response
391	flow_http_time_min	Flow	Minimum	Time took to HTTP server to return response
392	flow_http_time_stdev	Flow	Standard deviation	Time took to HTTP server to return response
393	flow_http_time_sum	Flow	Sum	Time took to HTTP server to return response
394	flow_http_time_thirdQ	Flow	Third quartile	Time took to HTTP server to return response
395	flow_http_time_var	Flow	Variance	Time took to HTTP server to return response
396	flow_packet_inter_arrivel_A_avg	Flow	Average	Client packets inter arival time
397	flow_packet_inter_arrivel_A_entropy	Flow	Entropy	Client packets inter arival time
398	flow_packet_inter_arrivel_A_firstQ	Flow	First quartile	Client packets inter arival time
399	flow_packet_inter_arrivel_A_max	Flow	Maximum	Client packets inter arival time
400	flow_packet_inter_arrivel_A_median	Flow	Median	Client packets inter arival time
401	flow_packet_inter_arrivel_A_min	Flow	Minimum	Client packets inter arival time
402	flow_packet_inter_arrivel_A_stdev	Flow	Standard deviation	Client packets inter arival time
403	flow_packet_inter_arrivel_A_sum	Flow	Sum	Client packets inter arival time
404	flow_packet_inter_arrivel_A_thirdQ	Flow	Third quartile	Client packets inter arival time
405	flow_packet_inter_arrivel_A_var	Flow	Variance	Client packets inter arival time
406	flow_packet_inter_arrivel_B_avg	Flow	Average	Server packets inter arival time
407	flow_packet_inter_arrivel_B_entropy	Flow	Entropy	Server packets inter arival time
408	flow_packet_inter_arrivel_B_firstQ	Flow	First quartile	Server packets inter arival time
409	flow_packet_inter_arrivel_B_max	Flow	Maximum	Server packets inter arival time
410	flow_packet_inter_arrivel_B_median	Flow	Median	Server packets inter arival time
411	flow_packet_inter_arrivel_B_min	Flow	Minimum	Server packets inter arival time
412	flow_packet_inter_arrivel_B_stdev	Flow	Standard deviation	Server packets inter arival time
413	flow_packet_inter_arrivel_B_sum	Flow	Sum	Server packets inter arival time
414	flow_packet_inter_arrivel_B_thirdQ	Flow	Third quartile	Server packets inter arival time
415	flow_packet_inter_arrivel_B_var	Flow	Variance	Server packets inter arival time
416	flow_packet_inter_arrivel_avg	Flow	Average	Packets inter arival time

417	flow_packet_inter_arrivel_entropy	Flow	Entropy	Packets inter arival time
418	flow_packet_inter_arrivel_firstQ	Flow	First quartile	Packets inter arival time
419	flow_packet_inter_arrivel_max	Flow	Maximum	Packets inter arival time
420	flow_packet_inter_arrivel_median	Flow	Median	Packets inter arival time
421	flow_packet_inter_arrivel_min	Flow	Minimum	Packets inter arival time
422	flow_packet_inter_arrivel_stdev	Flow	Standard deviation	Packets inter arival time
423	flow_packet_inter_arrivel_sum	Flow	Sum	Packets inter arival time
424	flow_packet_inter_arrivel_thirdQ	Flow	Third quartile	Packets inter arival time
425	flow_packet_inter_arrivel_var	Flow	Variance	Packets inter arival time
426	flow_packet_size_A_avg	Flow	Average	Client packets size
427	flow_packet_size_A_entropy	Flow	Entropy	Client packets size
428	flow_packet_size_A_firstQ	Flow	First quartile	Client packets size
429	flow_packet_size_A_max	Flow	Maximum	Client packets size
430	flow_packet_size_A_median	Flow	Median	Client packets size
431	flow_packet_size_A_min	Flow	Minimum	Client packets size
432	flow_packet_size_A_stdev	Flow	Standard deviation	Client packets size
433	flow_packet_size_A_sum	Flow	Sum	Client packets size
434	flow_packet_size_A_thirdQ	Flow	Third quartile	Client packets size
435	flow_packet_size_A_var	Flow	Variance	Client packets size
436	flow_packet_size_B_avg	Flow	Average	Server packets size
437	flow_packet_size_B_entropy	Flow	Entropy	Server packets size
438	flow_packet_size_B_firstQ	Flow	First quartile	Server packets size
439	flow_packet_size_B_max	Flow	Maximum	Server packets size
440	flow_packet_size_B_median	Flow	Median	Server packets size
441	flow_packet_size_B_min	Flow	Minimum	Server packets size
442	flow_packet_size_B_stdev	Flow	Standard deviation	Server packets size
443	flow_packet_size_B_sum	Flow	Sum	Server packets size
444	flow_packet_size_B_thirdQ	Flow	Third quartile	Server packets size
445	flow_packet_size_B_var	Flow	Variance	Server packets size
446	flow_packet_size_avg	Flow	Average	Packets size
447	flow_packet_size_entropy	Flow	Entropy	Packets size
448	flow_packet_size_firstQ	Flow	First quartile	Packets size
449	flow_packet_size_max	Flow	Maximum	Packets size
450	flow_packet_size_median	Flow	Median	Packets size
451	flow_packet_size_min	Flow	Minimum	Packets size

452	flow_packet_size_stdev	Flow	Standard deviation	Packets size
453	flow_packet_size_sum	Flow	Sum	Packets size
454	flow_packet_size_thirdQ	Flow	Third quartile	Packets size
455	flow_packet_size_var	Flow	Variance	Packets size
456	flow_packets	Flow		Total packets
457	flow_packets_A	Flow		Total packets sent by client
458	flow_packets_A_B_ratio	Flow		Ratio between packets sent by client and sent by server
459	flow_packets_B	Flow		Total packets sent by server
460	flow_push	Flow		Total packets with PSH flag
461	flow_push_A	Flow		Total packets with PSH flag sent by client
462	flow_push_B	Flow		Total packets with PSH flag sent by server
463	flow_reset	Flow		Total packets with RST flag
464	flow_reset_A	Flow		Total packets with RST flag sent by client
465	flow_reset_B	Flow		Total packets with RST flag sent by server
466	flow_sess_concurent_avg	Flow	Average	Cuncurent sessions
467	flow_sess_concurent_entropy	Flow	Entropy	Cuncurent sessions
468	flow_sess_concurent_firstQ	Flow	First quartile	Cuncurent sessions
469	flow_sess_concurent_max	Flow	Maximum	Cuncurent sessions
470	flow_sess_concurent_median	Flow	Median	Cuncurent sessions
471	flow_sess_concurent_min	Flow	Minimum	Cuncurent sessions
472	flow_sess_concurent_stdev	Flow	Standard deviation	Cuncurent sessions
473	flow_sess_concurent_sum	Flow	Sum	Cuncurent sessions
474	flow_sess_concurent_thirdQ	Flow	Third quartile	Cuncurent sessions
475	flow_sess_concurent_var	Flow	Variance	Cuncurent sessions
476	flow_sess_duration_avg	Flow	Average	Session duration
477	flow_sess_duration_entropy	Flow	Entropy	Session duration
478	flow_sess_duration_firstQ	Flow	First quartile	Session duration
479	flow_sess_duration_max	Flow	Maximum	Session duration
480	flow_sess_duration_median	Flow	Median	Session duration
481	flow_sess_duration_min	Flow	Minimum	Session duration
482	flow_sess_duration_stdev	Flow	Standard deviation	Session duration
483	flow_sess_duration_sum	Flow	Sum	Session duration
484	flow_sess_duration_thirdQ	Flow	Third quartile	Session duration
485	flow_sess_duration_var	Flow	Variance	Session duration
486	flow_sess_idle_avg	Flow	Average	Idle between sessions

487	flow_sess_idle_entropy	Flow	Entropy	Idle between sessions
488	flow_sess_idle_firstQ	Flow	First quartile	Idle between sessions
489	flow_sess_idle_max	Flow	Maximum	Idle between sessions
490	flow_sess_idle_median	Flow	Median	Idle between sessions
491	flow_sess_idle_min	Flow	Minimum	Idle between sessions
492	flow_sess_idle_stdev	Flow	Standard deviation	Idle between sessions
493	flow_sess_idle_sum	Flow	Sum	Idle between sessions
494	flow_sess_idle_thirdQ	Flow	Third quartile	Idle between sessions
495	flow_sess_idle_var	Flow	Variance	Idle between sessions
496	flow_src_ports	Flow		Number of source ports
497	flow_src_ports_sessions_ratio	Flow		Ration between number of source ports and number of sessions
498	flow_ssl_count_certificates	Flow		Number of SSL certificates
499	flow_ssl_count_client_cipher_algs	Flow		Number of supported SSL cipher algorithms by client
500	flow_ssl_count_client_ciphersuites	Flow		Number of supported SSL ciphersuites by client
501	flow_ssl_count_client_compressions	Flow		Number of supported SSL compressions by client
502	flow_ssl_count_client_elliptic_curves	Flow		Number of supported SSL eliptic curves by client
503	flow_ssl_count_client_key_exchange_algs	Flow		Number of supported SSL key exchange algorithms by client
504	flow_ssl_count_client_mac_algs	Flow		Number of supported SSL mac algorithms by client
505	flow_ssl_count_server_ciphersuite	Flow		Number of supported SSL cipher algorithms by server
506	flow_ssl_count_server_compression	Flow		Number of supported SSL ciphersuites by server
507	flow_ssl_count_server_elliptic_curve	Flow		Number of supported SSL compressions by client
508	flow_ssl_count_server_name	Flow		Number of supported SSL eliptic curves by server
509	flow_ssl_count_transactions	Flow		Number of supported SSL key exchange algorithms by server
510	flow_ssl_count_version	Flow		Number of supported SSL mac algorithms by server
511	flow_ssl_dom_server_ciphersuite	Flow		Number of SSL versions
512	flow_ssl_dom_server_compression	Flow		Dominated SSL ciphersuite
513	flow_ssl_dom_server_elliptic_curve	Flow		Dominated SSL eliptic curve
514	flow_ssl_dom_server_name_alexaRank	Flow		Dominated SSL server name
515	flow_ssl_dom_version	Flow		Dominated SSL version
516	flow_ssl_handshake_duration_avg	Flow	Average	SSL handshake duration
517	flow_ssl_handshake_duration_entropy	Flow	Entropy	SSL handshake duration
518	flow_ssl_handshake_duration_firstQ	Flow	First quartile	SSL handshake duration
519	flow_ssl_handshake_duration_max	Flow	Maximum	SSL handshake duration
520	flow_ssl_handshake_duration_median	Flow	Median	SSL handshake duration
521	flow_ssl_handshake_duration_min	Flow	Minimum	SSL handshake duration

522	flow_ssl_handshake_duration_stdev	Flow	Standard deviation	SSL handshake duration
523	flow_ssl_handshake_duration_sum	Flow	Sum	SSL handshake duration
524	flow_ssl_handshake_duration_thirdQ	Flow	Third quartile	SSL handshake duration
525	flow_ssl_handshake_duration_var	Flow	Variance	SSL handshake duration
526	flow_ssl_ratio_certificate_expired	Flow		Ratio between ssl setions and expired certificates
527	flow_ssl_ratio_client_cipher_algs	Flow		Ratio between ssl setions and client cipher algorithms
528	flow_ssl_ratio_client_ciphersuites	Flow		Ratio between ssl setions and client ciphersuites
529	flow_ssl_ratio_client_elliptic_curves	Flow		Ratio between ssl setions and client eliptic curves
530	flow_ssl_ratio_client_key_exchange_algs	Flow		Ratio between ssl setions and client key exchange algorithms
531	flow_ssl_ratio_client_mac_algs	Flow		Ratio between ssl setions and client mac algorithms
532	flow_ssl_ratio_server_name	Flow		Ratio between ssl setions and server names
533	flow_ssl_req_bytes_avg	Flow	Average	Number of request bytes
534	flow_ssl_req_bytes_entropy	Flow	Entropy	Number of request bytes
535	flow_ssl_req_bytes_firstQ	Flow	First quartile	Number of request bytes
536	flow_ssl_req_bytes_max	Flow	Maximum	Number of request bytes
537	flow_ssl_req_bytes_median	Flow	Median	Number of request bytes
538	flow_ssl_req_bytes_min	Flow	Minimum	Number of request bytes
539	flow_ssl_req_bytes_stdev	Flow	Standard deviation	Number of request bytes
540	flow_ssl_req_bytes_sum	Flow	Sum	Number of request bytes
541	flow_ssl_req_bytes_thirdQ	Flow	Third quartile	Number of request bytes
542	flow_ssl_req_bytes_var	Flow	Variance	Number of request bytes
543	flow_ssl_resp_bytes_avg	Flow	Average	Number of response bytes
544	flow_ssl_resp_bytes_entropy	Flow	Entropy	Number of response bytes
545	flow_ssl_resp_bytes_firstQ	Flow	First quartile	Number of response bytes
546	flow_ssl_resp_bytes_max	Flow	Maximum	Number of response bytes
547	flow_ssl_resp_bytes_median	Flow	Median	Number of response bytes
548	flow_ssl_resp_bytes_min	Flow	Minimum	Number of response bytes
549	flow_ssl_resp_bytes_stdev	Flow	Standard deviation	Number of response bytes
550	flow_ssl_resp_bytes_sum	Flow	Sum	Number of response bytes
551	flow_ssl_resp_bytes_thirdQ	Flow	Third quartile	Number of response bytes
552	flow_ssl_resp_bytes_var	Flow	Variance	Number of response bytes
553	flow_tcp_analysis_duplicate_ack	Flow		Number of packets with duplicake ACKs
554	flow_tcp_analysis_keep_alive	Flow		Number of Keep Alive packets
555	flow_tcp_analysis_lost_segment	Flow		Number of lost segments
556	flow_tcp_analysis_out_of_order	Flow		Number of packets received out of order

557	flow_tcp_analysis_retransmission	Flow		Number of retransmitted packets
558	flow_tcp_analysis_reused_ports	Flow		Number of reused ports
559	flow_tcp_count_sessions	Flow		Number of TCP sessions
560	flow_ttl_A_avg	Flow	Average	TCP packet time-to-live sent by client
561	flow_ttl_A_entropy	Flow	Entropy	TCP packet time-to-live sent by client
562	flow_ttl_A_firstQ	Flow	First quartile	TCP packet time-to-live sent by client
563	flow_ttl_A_max	Flow	Maximum	TCP packet time-to-live sent by client
564	flow_ttl_A_median	Flow	Median	TCP packet time-to-live sent by client
565	flow_ttl_A_min	Flow	Minimum	TCP packet time-to-live sent by client
566	flow_ttl_A_stdev	Flow	Standard deviation	TCP packet time-to-live sent by client
567	flow_ttl_A_sum	Flow	Sum	TCP packet time-to-live sent by client
568	flow_ttl_A_thirdQ	Flow	Third quartile	TCP packet time-to-live sent by client
569	flow_ttl_A_var	Flow	Variance	TCP packet time-to-live sent by client
570	flow_ttl_B_avg	Flow	Average	TCP packet time-to-live sent by server
571	flow_ttl_B_entropy	Flow	Entropy	TCP packet time-to-live sent by server
572	flow_ttl_B_firstQ	Flow	First quartile	TCP packet time-to-live sent by server
573	flow_ttl_B_max	Flow	Maximum	TCP packet time-to-live sent by server
574	flow_ttl_B_median	Flow	Median	TCP packet time-to-live sent by server
575	flow_ttl_B_min	Flow	Minimum	TCP packet time-to-live sent by server
576	flow_ttl_B_stdev	Flow	Standard deviation	TCP packet time-to-live sent by server
577	flow_ttl_B_sum	Flow	Sum	TCP packet time-to-live sent by server
578	flow_ttl_B_thirdQ	Flow	Third quartile	TCP packet time-to-live sent by server
579	flow_ttl_B_var	Flow	Variance	TCP packet time-to-live sent by server
580	flow_ttl_avg	Flow	Average	TCP packet time-to-live
581	flow_ttl_entropy	Flow	Entropy	TCP packet time-to-live
582	flow_ttl_firstQ	Flow	First quartile	TCP packet time-to-live
583	flow_ttl_max	Flow	Maximum	TCP packet time-to-live
584	flow_ttl_median	Flow	Median	TCP packet time-to-live
585	flow_ttl_min	Flow	Minimum	TCP packet time-to-live
586	flow_ttl_stdev	Flow	Standard deviation	TCP packet time-to-live
587	flow_ttl_sum	Flow	Sum	TCP packet time-to-live
588	flow_ttl_thirdQ	Flow	Third quartile	TCP packet time-to-live
589	flow_ttl_var	Flow	Variance	TCP packet time-to-live
590	flow_udp_count_sessions	Flow		Number of UDP sessions
591	flow_udp_dst_ports	Flow		Number of UDP destination ports

592	flow_udp_dst_ports_sessions_ratio	Flow		Ratio between UDP destination ports and number of sessions
593	flow_udp_sess_bytes_A_avg	Flow	Average	Bytes in UDP session sent by client
594	flow_udp_sess_bytes_A_entropy	Flow	Entropy	Bytes in UDP session sent by client
595	flow_udp_sess_bytes_A_firstQ	Flow	First quartile	Bytes in UDP session sent by client
596	flow_udp_sess_bytes_A_max	Flow	Maximum	Bytes in UDP session sent by client
597	flow_udp_sess_bytes_A_median	Flow	Median	Bytes in UDP session sent by client
598	flow_udp_sess_bytes_A_min	Flow	Minimum	Bytes in UDP session sent by client
599	flow_udp_sess_bytes_A_stdev	Flow	Standard deviation	Bytes in UDP session sent by client
600	flow_udp_sess_bytes_A_sum	Flow	Sum	Bytes in UDP session sent by client
601	flow_udp_sess_bytes_A_thirdQ	Flow	Third quartile	Bytes in UDP session sent by client
602	flow_udp_sess_bytes_A_var	Flow	Variance	Bytes in UDP session sent by client
603	flow_udp_sess_bytes_B_avg	Flow	Average	Bytes in UDP session sent by server
604	flow_udp_sess_bytes_B_entropy	Flow	Entropy	Bytes in UDP session sent by server
605	flow_udp_sess_bytes_B_firstQ	Flow	First quartile	Bytes in UDP session sent by server
606	flow_udp_sess_bytes_B_max	Flow	Maximum	Bytes in UDP session sent by server
607	flow_udp_sess_bytes_B_median	Flow	Median	Bytes in UDP session sent by server
608	flow_udp_sess_bytes_B_min	Flow	Minimum	Bytes in UDP session sent by server
609	flow_udp_sess_bytes_B_stdev	Flow	Standard deviation	Bytes in UDP session sent by server
610	flow_udp_sess_bytes_B_sum	Flow	Sum	Bytes in UDP session sent by server
611	flow_udp_sess_bytes_B_thirdQ	Flow	Third quartile	Bytes in UDP session sent by server
612	flow_udp_sess_bytes_B_var	Flow	Variance	Bytes in UDP session sent by server
613	flow_udp_sess_bytes_avg	Flow	Average	Bytes in UDP session
614	flow_udp_sess_bytes_entropy	Flow	Entropy	Bytes in UDP session
615	flow_udp_sess_bytes_firstQ	Flow	First quartile	Bytes in UDP session
616	flow_udp_sess_bytes_max	Flow	Maximum	Bytes in UDP session
617	flow_udp_sess_bytes_median	Flow	Median	Bytes in UDP session
618	flow_udp_sess_bytes_min	Flow	Minimum	Bytes in UDP session
619	flow_udp_sess_bytes_stdev	Flow	Standard deviation	Bytes in UDP session
620	flow_udp_sess_bytes_sum	Flow	Sum	Bytes in UDP session
621	flow_udp_sess_bytes_thirdQ	Flow	Third quartile	Bytes in UDP session
622	flow_udp_sess_bytes_var	Flow	Variance	Bytes in UDP session
623	flow_udp_sess_duration_avg	Flow	Average	UDP session duration
624	flow_udp_sess_duration_entropy	Flow	Entropy	UDP session duration
625	flow_udp_sess_duration_firstQ	Flow	First quartile	UDP session duration
626	flow_udp_sess_duration_max	Flow	Maximum	UDP session duration

627	flow_udp_sess_duration_median	Flow	Median	UDP session duration
628	flow_udp_sess_duration_min	Flow	Minimum	UDP session duration
629	flow_udp_sess_duration_stdev	Flow	Standard deviation	UDP session duration
630	flow_udp_sess_duration_sum	Flow	Sum	UDP session duration
631	flow_udp_sess_duration_thirdQ	Flow	Third quartile	UDP session duration
632	flow_udp_sess_duration_var	Flow	Variance	UDP session duration
633	flow_udp_sess_packets_A_avg	Flow	Average	Packets in UDP session sent by client
634	flow_udp_sess_packets_A_entropy	Flow	Entropy	Packets in UDP session sent by client
635	flow_udp_sess_packets_A_firstQ	Flow	First quartile	Packets in UDP session sent by client
636	flow_udp_sess_packets_A_max	Flow	Maximum	Packets in UDP session sent by client
637	flow_udp_sess_packets_A_median	Flow	Median	Packets in UDP session sent by client
638	flow_udp_sess_packets_A_min	Flow	Minimum	Packets in UDP session sent by client
639	flow_udp_sess_packets_A_stdev	Flow	Standard deviation	Packets in UDP session sent by client
640	flow_udp_sess_packets_A_sum	Flow	Sum	Packets in UDP session sent by client
641	flow_udp_sess_packets_A_thirdQ	Flow	Third quartile	Packets in UDP session sent by client
642	flow_udp_sess_packets_A_var	Flow	Variance	Packets in UDP session sent by client
643	flow_udp_sess_packets_B_avg	Flow	Average	Packets in UDP session sent by server
644	flow_udp_sess_packets_B_entropy	Flow	Entropy	Packets in UDP session sent by server
645	flow_udp_sess_packets_B_firstQ	Flow	First quartile	Packets in UDP session sent by server
646	flow_udp_sess_packets_B_max	Flow	Maximum	Packets in UDP session sent by server
647	flow_udp_sess_packets_B_median	Flow	Median	Packets in UDP session sent by server
648	flow_udp_sess_packets_B_min	Flow	Minimum	Packets in UDP session sent by server
649	flow_udp_sess_packets_B_stdev	Flow	Standard deviation	Packets in UDP session sent by server
650	flow_udp_sess_packets_B_sum	Flow	Sum	Packets in UDP session sent by server
651	flow_udp_sess_packets_B_thirdQ	Flow	Third quartile	Packets in UDP session sent by server
652	flow_udp_sess_packets_B_var	Flow	Variance	Packets in UDP session sent by server
653	flow_udp_sess_packets_avg	Flow	Average	Packets in UDP session
654	flow_udp_sess_packets_entropy	Flow	Entropy	Packets in UDP session
655	flow_udp_sess_packets_firstQ	Flow	First quartile	Packets in UDP session
656	flow_udp_sess_packets_max	Flow	Maximum	Packets in UDP session
657	flow_udp_sess_packets_median	Flow	Median	Packets in UDP session
658	flow_udp_sess_packets_min	Flow	Minimum	Packets in UDP session
659	flow_udp_sess_packets_stdev	Flow	Standard deviation	Packets in UDP session
660	flow_udp_sess_packets_sum	Flow	Sum	Packets in UDP session
661	flow_udp_sess_packets_thirdQ	Flow	Third quartile	Packets in UDP session

662	flow_udp_sess_packets_var	Flow	Variance	Packets in UDP session
663	flow_udp_src_ports	Flow		Number of UDP source ports
664	flow_udp_src_ports_sessions_ratio	Flow		Ratio between UDP source ports and number of sessions
665	flow_urg	Flow		Total packets with URG flag
666	flow_urg_A	Flow		Total packets with URG flag sent by client
667	flow_urg_B	Flow		Total packets with URG flag sent by server
668	flow_weekDay	Flow		Day of the week
669	session_A_port	Session		Client port
670	session_B_port	Session		Server port
671	session_ack	Session		Number of ACK packets sent and received
672	session_ack_A	Session		Number of ACK packets sent by client
673	session_ack_B	Session		Number of ACK packets sent by server
674	session_bytes	Session		Number of bytes sent and received
675	session_bytes_A	Session		Number of bytes sent by client
676	session_bytes_A_B_ratio	Session		Ratio between number of bytes sent and number of bytes received
677	session_bytes_B	Session		Number of bytes sent by server
678	session_ds_field_A	Session		Differentiated Services (DS) field sent by server
679	session_ds_field_B	Session		Differentiated Services (DS) field sent by client
680	session_duration	Session		Session duration
681	session_http_GET	Session		Number of HTTP requests submited with GET method
682	session_http_POST	Session		Number of HTTP requests submited with POST method
683	session_http_bytes_avg	Session	Average	Number of bytes sent by client over HTTP
684	session_http_bytes_entropy	Session	Entropy	Number of bytes sent by client over HTTP
685	session_http_bytes_firstQ	Session	First quartile	Number of bytes sent by client over HTTP
686	session_http_bytes_max	Session	Maximum	Number of bytes sent by client over HTTP
687	session_http_bytes_median	Session	Median	Number of bytes sent by client over HTTP
688	session_http_bytes_min	Session	Minimum	Number of bytes sent by client over HTTP
689	session_http_bytes_stdev	Session	Standard deviation	Number of bytes sent by client over HTTP
690	session_http_bytes_sum	Session	Sum	Number of bytes sent by client over HTTP
691	session_http_bytes_thirdQ	Session	Third quartile	Number of bytes sent by client over HTTP
692	session_http_bytes_var	Session	Variance	Number of bytes sent by client over HTTP
693	session_http_cookie_count	Session		Total number of cookie values
694	session_http_cookie_values_avg	Session	Average	Number of cookie values
695	session_http_cookie_values_entropy	Session	Entropy	Number of cookie values
696	session_http_cookie_values_firstQ	Session	First quartile	Number of cookie values

697	session_http_cookie_values_max	Session	Maximum	Number of cookie values
698	session_http_cookie_values_median	Session	Median	Number of cookie values
699	session_http_cookie_values_min	Session	Minimum	Number of cookie values
700	session_http_cookie_values_stdev	Session	Standard deviation	Number of cookie values
701	session_http_cookie_values_sum	Session	Sum	Number of cookie values
702	session_http_cookie_values_thirdQ	Session	Third quartile	Number of cookie values
703	session_http_cookie_values_var	Session	Variance	Number of cookie values
704	session_http_count_host	Session		Number of hosts
705	session_http_count_req_content_type	Session		Number of unique content types used in HTTP request
706	session_http_count_resp_code	Session		Number of unique HTTP response codes
707	session_http_count_resp_content_type	Session		Number of unique HTTP response content type
708	session_http_count_transactions	Session		Number HTTP transaction
709	session_http_count_user_agents	Session		Number of unique HTTP user agents
710	session_http_dom_browser	Session		Dominated HTTP browser
711	session_http_dom_browser_ver	Session		Dominated HTTP browser version
712	session_http_dom_host_alexaRank	Session		Dominated host Alexa rank
713	session_http_dom_is_bot	Session		Is most of HTTP connections created by known bot
714	session_http_dom_os	Session		Dominated operating system
715	session_http_dom_os_ver	Session		Dominated operating system version
716	session_http_dom_req_content_type	Session		Dominated HTTP request contetn type
717	session_http_dom_resp_code	Session		Dominated HTTP response code
718	session_http_dom_resp_content_type	Session		Dominated HTTP response contetn type
719	session_http_has_location	Session		Is HTTP request has location field
720	session_http_has_referrer	Session		Is HTTP request has refferer field
721	session_http_has_req_content_type	Session		Is HTTP request has content type field
722	session_http_has_resp_content_type	Session		Is HTTP response has content type field
723	session_http_has_user_agent	Session		Is HTTP request has user agent field
724	session_http_inter_arrivel_avg	Session	Average	HTTP request-response inter arrival time
725	session_http_inter_arrivel_entropy	Session	Entropy	HTTP request-response inter arrival time
726	session_http_inter_arrivel_firstQ	Session	First quartile	HTTP request-response inter arrival time
727	session_http_inter_arrivel_max	Session	Maximum	HTTP request-response inter arrival time
728	session_http_inter_arrivel_median	Session	Median	HTTP request-response inter arrival time
729	session_http_inter_arrivel_min	Session	Minimum	HTTP request-response inter arrival time
730	session_http_inter_arrivel_stdev	Session	Standard deviation	HTTP request-response inter arrival time
731	session_http_inter_arrivel_sum	Session	Sum	HTTP request-response inter arrival time

732	session_http_inter_arrivel_thirdQ	Session	Third quartile	HTTP request-response inter arrival time
733	session_http_inter_arrivel_var	Session	Variance	HTTP request-response inter arrival time
734	session_http_req_bytes_avg	Session	Average	HTTP request bytes
735	session_http_req_bytes_entropy	Session	Entropy	HTTP request bytes
736	session_http_req_bytes_firstQ	Session	First quartile	HTTP request bytes
737	session_http_req_bytes_max	Session	Maximum	HTTP request bytes
738	session_http_req_bytes_median	Session	Median	HTTP request bytes
739	session_http_req_bytes_min	Session	Minimum	HTTP request bytes
740	session_http_req_bytes_stdev	Session	Standard deviation	HTTP request bytes
741	session_http_req_bytes_sum	Session	Sum	HTTP request bytes
742	session_http_req_bytes_thirdQ	Session	Third quartile	HTTP request bytes
743	session_http_req_bytes_var	Session	Variance	HTTP request bytes
744	session_http_resp_bytes_avg	Session	Average	HTTP response bytes
745	session_http_resp_bytes_entropy	Session	Entropy	HTTP response bytes
746	session_http_resp_bytes_firstQ	Session	First quartile	HTTP response bytes
747	session_http_resp_bytes_max	Session	Maximum	HTTP response bytes
748	session_http_resp_bytes_median	Session	Median	HTTP response bytes
749	session_http_resp_bytes_min	Session	Minimum	HTTP response bytes
750	session_http_resp_bytes_stdev	Session	Standard deviation	HTTP response bytes
751	session_http_resp_bytes_sum	Session	Sum	HTTP response bytes
752	session_http_resp_bytes_thirdQ	Session	Third quartile	HTTP response bytes
753	session_http_resp_bytes_var	Session	Variance	HTTP response bytes
754	session_http_time_avg	Session	Average	Time took to HTTP server to return response
755	session_http_time_entropy	Session	Entropy	Time took to HTTP server to return response
756	session_http_time_firstQ	Session	First quartile	Time took to HTTP server to return response
757	session_http_time_max	Session	Maximum	Time took to HTTP server to return response
758	session_http_time_median	Session	Median	Time took to HTTP server to return response
759	session_http_time_min	Session	Minimum	Time took to HTTP server to return response
760	session_http_time_stdev	Session	Standard deviation	Time took to HTTP server to return response
761	session_http_time_sum	Session	Sum	Time took to HTTP server to return response
762	session_http_time_thirdQ	Session	Third quartile	Time took to HTTP server to return response
763	session_http_time_var	Session	Variance	Time took to HTTP server to return response
764	session_packet_inter_arrivel_A_avg	Session	Average	Client packets inter arival time
765	session_packet_inter_arrivel_A_entropy	Session	Entropy	Client packets inter arival time
766	session_packet_inter_arrivel_A_firstQ	Session	First quartile	Client packets inter arival time

767	session_packet_inter_arrivel_A_max	Session	Maximum	Client packets inter arival time
768	session_packet_inter_arrivel_A_median	Session	Median	Client packets inter arival time
769	session_packet_inter_arrivel_A_min	Session	Minimum	Client packets inter arival time
770	session_packet_inter_arrivel_A_stdev	Session	Standard deviation	Client packets inter arival time
771	session_packet_inter_arrivel_A_sum	Session	Sum	Client packets inter arival time
772	session_packet_inter_arrivel_A_thirdQ	Session	Third quartile	Client packets inter arival time
773	session_packet_inter_arrivel_A_var	Session	Variance	Client packets inter arival time
774	session_packet_inter_arrivel_B_avg	Session	Average	Server packets inter arival time
775	session_packet_inter_arrivel_B_entropy	Session	Entropy	Server packets inter arival time
776	session_packet_inter_arrivel_B_firstQ	Session	First quartile	Server packets inter arival time
777	session_packet_inter_arrivel_B_max	Session	Maximum	Server packets inter arival time
778	session_packet_inter_arrivel_B_median	Session	Median	Server packets inter arival time
779	session_packet_inter_arrivel_B_min	Session	Minimum	Server packets inter arival time
780	session_packet_inter_arrivel_B_stdev	Session	Standard deviation	Server packets inter arival time
781	session_packet_inter_arrivel_B_sum	Session	Sum	Server packets inter arival time
782	session_packet_inter_arrivel_B_thirdQ	Session	Third quartile	Server packets inter arival time
783	session_packet_inter_arrivel_B_var	Session	Variance	Server packets inter arival time
784	session_packet_inter_arrivel_avg	Session	Average	Packets inter arival time
785	session_packet_inter_arrivel_entropy	Session	Entropy	Packets inter arival time
786	session_packet_inter_arrivel_firstQ	Session	First quartile	Packets inter arival time
787	session_packet_inter_arrivel_max	Session	Maximum	Packets inter arival time
788	session_packet_inter_arrivel_median	Session	Median	Packets inter arival time
789	session_packet_inter_arrivel_min	Session	Minimum	Packets inter arival time
790	session_packet_inter_arrivel_stdev	Session	Standard deviation	Packets inter arival time
791	session_packet_inter_arrivel_sum	Session	Sum	Packets inter arival time
792	session_packet_inter_arrivel_thirdQ	Session	Third quartile	Packets inter arival time
793	session_packet_inter_arrivel_var	Session	Variance	Packets inter arival time
794	session_packet_size_A_avg	Session	Average	Client packets size
795	session_packet_size_A_entropy	Session	Entropy	Client packets size
796	session_packet_size_A_firstQ	Session	First quartile	Client packets size
797	session_packet_size_A_max	Session	Maximum	Client packets size
798	session_packet_size_A_median	Session	Median	Client packets size
799	session_packet_size_A_min	Session	Minimum	Client packets size
800	session_packet_size_A_stdev	Session	Standard deviation	Client packets size
801	session_packet_size_A_sum	Session	Sum	Client packets size

802	session_packet_size_A_thirdQ	Session	Third quartile	Client packets size
803	session_packet_size_A_var	Session	Variance	Client packets size
804	session_packet_size_B_avg	Session	Average	Server packets size
805	session_packet_size_B_entropy	Session	Entropy	Server packets size
806	session_packet_size_B_firstQ	Session	First quartile	Server packets size
807	session_packet_size_B_max	Session	Maximum	Server packets size
808	session_packet_size_B_median	Session	Median	Server packets size
809	session_packet_size_B_min	Session	Minimum	Server packets size
810	session_packet_size_B_stdev	Session	Standard deviation	Server packets size
811	session_packet_size_B_sum	Session	Sum	Server packets size
812	session_packet_size_B_thirdQ	Session	Third quartile	Server packets size
813	session_packet_size_B_var	Session	Variance	Server packets size
814	session_packet_size_avg	Session	Average	Packets size
815	session_packet_size_entropy	Session	Entropy	Packets size
816	session_packet_size_firstQ	Session	First quartile	Packets size
817	session_packet_size_max	Session	Maximum	Packets size
818	session_packet_size_median	Session	Median	Packets size
819	session_packet_size_min	Session	Minimum	Packets size
820	session_packet_size_stdev	Session	Standard deviation	Packets size
821	session_packet_size_sum	Session	Sum	Packets size
822	session_packet_size_thirdQ	Session	Third quartile	Packets size
823	session_packet_size_var	Session	Variance	Packets size
824	session_packets	Session		Total packets
825	session_packets_A	Session		Total packets sent by client
826	session_packets_A_B_ratio	Session		Ratio between packets sent by client and sent by server
827	session_packets_B	Session		Total packets sent by server
828	session_push	Session		Total packets with PSH flag
829	session_push_A	Session		Total packets with PSH flag sent by client
830	session_push_B	Session		Total packets with PSH flag sent by server
831	session_reset	Session		Total packets with RST flag
832	session_reset_A	Session		Total packets with RST flag sent by client
833	session_reset_B	Session		Total packets with RST flag sent by server
834	session_ssl_count_certificates	Session		Number of SSL certificates
835	session_ssl_count_client_cipher_algs	Session		Number of supported SSL cipher algorithms by client
836	session_ssl_count_client_ciphersuites	Session		Number of supported SSL ciphersuites by client

837	session_ssl_count_client_compressions	Session		Number of supported SSL compressions by client
838	session_ssl_count_client_elliptic_curves	Session		Number of supported SSL eliptic curves by client
839	session_ssl_count_client_key_exchange_algs	Session		Number of supported SSL key exchange algorithms by client
840	session_ssl_count_client_mac_algs	Session		Number of supported SSL mac algorithms by client
841	session_ssl_count_server_ciphersuite	Session		Number of supported SSL cipher algorithms by server
842	session_ssl_count_server_compression	Session		Number of supported SSL ciphersuites by server
843	session_ssl_count_server_elliptic_curve	Session		Number of supported SSL compressions by client
844	session_ssl_count_server_name	Session		Number of supported SSL eliptic curves by server
845	session_ssl_count_transactions	Session		Number of supported SSL key exchange algorithms by server
846	session_ssl_count_version	Session		Number of supported SSL mac algorithms by server
847	session_ssl_dom_server_ciphersuite	Session		Number of SSL versions
848	session_ssl_dom_server_compression	Session		Dominated SSL ciphersuite
849	session_ssl_dom_server_elliptic_curve	Session		Dominated SSL eliptic curve
850	session_ssl_dom_server_name_alexaRank	Session		Dominated SSL server name
851	session_ssl_dom_version	Session		Dominated SSL version
852	session_ssl_handshake_duration_avg	Session	Average	SSL handshake duration
853	session_ssl_handshake_duration_entropy	Session	Entropy	SSL handshake duration
854	session_ssl_handshake_duration_firstQ	Session	First quartile	SSL handshake duration
855	session_ssl_handshake_duration_max	Session	Maximum	SSL handshake duration
856	session_ssl_handshake_duration_median	Session	Median	SSL handshake duration
857	session_ssl_handshake_duration_min	Session	Minimum	SSL handshake duration
858	session_ssl_handshake_duration_stdev	Session	Standard deviation	SSL handshake duration
859	session_ssl_handshake_duration_sum	Session	Sum	SSL handshake duration
860	session_ssl_handshake_duration_thirdQ	Session	Third quartile	SSL handshake duration
861	session_ssl_handshake_duration_var	Session	Variance	SSL handshake duration
862	session_ssl_ratio_certificate_expired	Session		Ratio between ssl setions and expired certificates
863	session_ssl_ratio_client_cipher_algs	Session		Ratio between ssl setions and client cipher algorithms
864	session_ssl_ratio_client_ciphersuites	Session		Ratio between ssl setions and client ciphersuites
865	session_ssl_ratio_client_elliptic_curves	Session		Ratio between ssl setions and client eliptic curves
866	session_ssl_ratio_client_key_exchange_algs	Session		Ratio between ssl setions and client key exchange algorithms
867	session_ssl_ratio_client_mac_algs	Session		Ratio between ssl setions and client mac algorithms
868	session_ssl_ratio_server_name	Session		Ratio between ssl setions and server names
869	session_ssl_req_bytes_avg	Session	Average	Number of request bytes
870	session_ssl_req_bytes_entropy	Session	Entropy	Number of request bytes
871	session_ssl_req_bytes_firstQ	Session	First quartile	Number of request bytes

872	session_ssl_req_bytes_max	Session	Maximum	Number of request bytes
873	session_ssl_req_bytes_median	Session	Median	Number of request bytes
874	session_ssl_req_bytes_min	Session	Minimum	Number of request bytes
875	session_ssl_req_bytes_stdev	Session	Standard deviation	Number of request bytes
876	session_ssl_req_bytes_sum	Session	Sum	Number of request bytes
877	session_ssl_req_bytes_thirdQ	Session	Third quartile	Number of request bytes
878	session_ssl_req_bytes_var	Session	Variance	Number of request bytes
879	session_ssl_resp_bytes_avg	Session	Average	Number of response bytes
880	session_ssl_resp_bytes_entropy	Session	Entropy	Number of response bytes
881	session_ssl_resp_bytes_firstQ	Session	First quartile	Number of response bytes
882	session_ssl_resp_bytes_max	Session	Maximum	Number of response bytes
883	session_ssl_resp_bytes_median	Session	Median	Number of response bytes
884	session_ssl_resp_bytes_min	Session	Minimum	Number of response bytes
885	session_ssl_resp_bytes_stdev	Session	Standard deviation	Number of response bytes
886	session_ssl_resp_bytes_sum	Session	Sum	Number of response bytes
887	session_ssl_resp_bytes_thirdQ	Session	Third quartile	Number of response bytes
888	session_ssl_resp_bytes_var	Session	Variance	Number of response bytes
889	session_tcp_analysis_duplicate_ack	Session		Number of packets with duplicake ACKs
890	session_tcp_analysis_keep_alive	Session		Number of Keep Alive packets
891	session_tcp_analysis_lost_segment	Session		Number of lost segments
892	session_tcp_analysis_out_of_order	Session		Number of packets received out of order
893	session_tcp_analysis_retransmission	Session		Number of retransmitted packets
894	session_tcp_analysis_reused_ports	Session		Number of reused ports
895	session_ttl_A_avg	Session	Average	TCP packet time-to-live sent by client
896	session_ttl_A_entropy	Session	Entropy	TCP packet time-to-live sent by client
897	session_ttl_A_firstQ	Session	First quartile	TCP packet time-to-live sent by client
898	session_ttl_A_max	Session	Maximum	TCP packet time-to-live sent by client
899	session_ttl_A_median	Session	Median	TCP packet time-to-live sent by client
900	session_ttl_A_min	Session	Minimum	TCP packet time-to-live sent by client
901	session_ttl_A_stdev	Session	Standard deviation	TCP packet time-to-live sent by client
902	session_ttl_A_sum	Session	Sum	TCP packet time-to-live sent by client
903	session_ttl_A_thirdQ	Session	Third quartile	TCP packet time-to-live sent by client
904	session_ttl_A_var	Session	Variance	TCP packet time-to-live sent by client
905	session_ttl_B_avg	Session	Average	TCP packet time-to-live sent by server
906	session_ttl_B_entropy	Session	Entropy	TCP packet time-to-live sent by server

907	session_ttl_B_firstQ	Session	First quartile	TCP packet time-to-live sent by server
908	session_ttl_B_max	Session	Maximum	TCP packet time-to-live sent by server
909	session_ttl_B_median	Session	Median	TCP packet time-to-live sent by server
910	session_ttl_B_min	Session	Minimum	TCP packet time-to-live sent by server
911	session_ttl_B_stdev	Session	Standard deviation	TCP packet time-to-live sent by server
912	session_ttl_B_sum	Session	Sum	TCP packet time-to-live sent by server
913	session_ttl_B_thirdQ	Session	Third quartile	TCP packet time-to-live sent by server
914	session_ttl_B_var	Session	Variance	TCP packet time-to-live sent by server
915	session_ttl_avg	Session	Average	TCP packet time-to-live
916	session_ttl_entropy	Session	Entropy	TCP packet time-to-live
917	session_ttl_firstQ	Session	First quartile	TCP packet time-to-live
918	session_ttl_max	Session	Maximum	TCP packet time-to-live
919	session_ttl_median	Session	Median	TCP packet time-to-live
920	session_ttl_min	Session	Minimum	TCP packet time-to-live
921	session_ttl_stdev	Session	Standard deviation	TCP packet time-to-live
922	session_ttl_sum	Session	Sum	TCP packet time-to-live
923	session_ttl_thirdQ	Session	Third quartile	TCP packet time-to-live
924	session_ttl_var	Session	Variance	TCP packet time-to-live
925	session_urg	Session		Total packets with URG flag
926	session_urg_A	Session		Total packets with URG flag sent by client
927	session_urg_B	Session		Total packets with URG flag sent by server