Color Coded TCP Log

Color Key:

green	Normal TCP connection handshakes
red	Attack activity
yellow	Normal TCP connections failing due to attack

Color as text	No.	Time (in seconds & milliseconds)	Source	Destination	Protocol	Info
green	47	3.144521	198.51.100.23	192.0.2.1	TCP	42584->443 [SYN] Seq=0 Win-5792 Len=120...
green	48	3,195755	192.0.2.1	198.51.100.23	TCP	443->42584 [SYN, ACK] Seq=0 Win-5792 Len=120...
green	49	3,246989	198.51.100.23	192.0.2.1	TCP	42584->443 [ACK] Seq=1 Win-5792 Len=120...
green	50	3,298223	198.51.100.23	192.0.2.1	HTTP	GET /sales.html HTTP/1.1
green	51	3,349457	192.0.2.1	198.51.100.23	HTTP	HTTP/1.1 200 OK (text/html)
red	52	3,390692	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red	53	3,441926	192.0.2.1	203.0.113.0	TCP	443->54770 [SYN, ACK] Seq=0 Win-5792 Len=120...
red	54	3,49316	203.0.113.0	192.0.2.1	TCP	54770->443 [ACK Seq=1 Win=5792 Len=0...
green	55	3,544394	198.51.100.14	192.0.2.1	TCP	14785->443 [SYN] Seq=0 Win-5792 Len=120...
green	56	3,599628	192.0.2.1	198.51.100.14	TCP	443->14785 [SYN, ACK] Seq=0 Win-5792 Len=120...
red	57	3,664863	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
green	58	3,730097	198.51.100.14	192.0.2.1	TCP	14785->443 [ACK] Seq=1 Win-5792 Len=120...
red	59	3,795332	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win-5792 Len=120...
green	60	3,860567	198.51.100.14	192.0.2.1	HTTP	GET /sales.html HTTP/1.1
red	61	3,939499	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win-5792 Len=120...
green	62	4,018431	192.0.2.1	198.51.100.14	HTTP	HTTP/1.1 200 OK (text/html)
green	63	4,097363	198.51.100.5	192.0.2.1	TCP	33638->443 [SYN] Seq=0 Win-5792 Len=120...
red	64	4,176295	192.0.2.1	203.0.113.0	TCP	443->54770 [SYN, ACK] Seq=0 Win-5792 Len=120...
green	65	4,255227	192.0.2.1	198.51.100.5	TCP	443->33638 [SYN, ACK] Seq=0 Win-5792 Len=120...
red	66	4,256159	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...

green 67	5,235091	198.51.100.5	192.0.2.1	TCP	33638->443 [ACK] Seq=1 Win-5792 Len=120...
red 68	5,236023	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
green 69	5,236955	198.51.100.16	192.0.2.1	TCP	32641->443 [SYN] Seq=0 Win-5792 Len=120...
red 70	5,237887	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
green 71	6,228728	198.51.100.5	192.0.2.1	HTTP	GET /sales.html HTTP/1.1
red 72	6,229638	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
yellow 73	6,230548	192.0.2.1	198.51.100.16	TCP	443->32641 [RST, ACK] Seq=0 Win-5792 Len=120...
red 74	6,330539	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
green 75	6,330885	198.51.100.7	192.0.2.1	TCP	42584->443 [SYN] Seq=0 Win=5792 Len=0...
red 76	6,331231	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
yellow 77	7,330577	192.0.2.1	198.51.100.5	TCP	HTTP/1.1 504 Gateway Time-out (text/html)
red 78	7,351323	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
green 79	7,360768	198.51.100.22	192.0.2.1	TCP	6345->443 [SYN] Seq=0 Win=5792 Len=0...
yellow 80	7,380773	192.0.2.1	198.51.100.7	TCP	443->42584 [RST, ACK] Seq=1 Win-5792 Len=120...
red 81	7,380878	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 82	7,383879	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 83	7,482754	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
red 84	7,581629	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
yellow 85	7,680504	192.0.2.1	198.51.100.22	TCP	443->6345 [RST, ACK] Seq=1 Win=5792 Len=0...
red 86	7,709377	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 87	7,738241	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 88	7,767105	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 89	13,895969	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
red 90	13,919832	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 91	13,943695	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
yellow 92	13,967558	192.0.2.1	198.51.100.16	TCP	443->32641 [RST, ACK] Seq=1 Win-5792 Len=120...
red 93	13,991421	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 94	14,015245	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 95	14,439072	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
red 96	14,862899	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...

green 97	14,886727	198.51.100.9	192.0.2.1	TCP	4631->443 [SYN] Seq=0 Win=5792 Len=0...
red 98	15,310554	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 99	15,734381	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 100	16,158208	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
red 101	16,582035	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 102	17,005862	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 103	17,429678	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
red 104	17,452693	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 105	17,475708	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 106	17,498723	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 107	17,521738	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 108	17,544753	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 109	17,567768	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
red 110	17,590783	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 111	18,413795	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 112	18,436807	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 113	18,459819	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 114	18,482831	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 115	18,506655	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 116	18,529667	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 117	18,552679	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
red 118	18,875692	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 119	19,198705	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 120	19,521718	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
yellow 121	19,844731	192.0.2.1	198.51.100.9	TCP	443->4631 [RST, ACK] Seq=1 Win=5792 Len=0...
red 122	20,167744	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 123	20,490757	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 124	20,81377	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
red 125	21,136783	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 126	21,459796	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...

red 127	21,782809	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 128	22,105822	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 129	22,428835	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 130	22,751848	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 131	23,074861	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 132	23,397874	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 133	23,720887	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 134	24,0439	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 135	24,366913	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 136	24,689926	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 137	25,012939	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 138	25,335952	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 139	25,658965	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 140	25,981978	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 141	26,304991	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 142	26,628004	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 143	26,951017	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 144	27,27403	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 145	27,597043	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 146	27,920056	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 147	28,243069	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 148	28,566082	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 149	28,889095	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 150	29,212108	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 151	29,535121	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 152	29,858134	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 153	30,181147	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 154	30,50416	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 155	30,827173	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 156	31,150186	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...

red 157	31,473199	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 158	31,796212	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 159	32,119225	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 160	32,442238	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 161	32,765251	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 162	33,088264	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 163	33,411277	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 164	33,73429	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 165	34,057303	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 166	34,380316	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 167	34,703329	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 168	35,026342	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 169	35,349355	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 170	35,672368	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 171	35,995381	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 172	36,318394	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 173	36,641407	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 174	36,96442	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 175	37,287433	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 176	37,610446	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 177	37,933459	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 178	38,256472	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 179	38,579485	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 180	38,902498	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 181	39,225511	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 182	39,548524	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 183	39,871537	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 184	40,19455	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 185	40,517563	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 186	40,840576	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...

red 187	41,163589	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 188	41,486602	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 189	41,809615	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 190	42,132628	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 191	42,455641	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 192	42,778654	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 193	43,101667	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 194	43,42468	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 195	43,747693	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 196	44,070706	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 197	44,393719	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 198	44,716732	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 199	45,039745	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 200	45,362758	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 201	45,685771	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 202	46,008784	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 203	46,331797	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 204	46,65481	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 205	46,977823	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 206	47,300836	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 207	47,623849	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 208	47,946862	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 209	48,269875	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 210	48,592888	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 211	48,915901	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 212	49,238914	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 213	49,561927	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 214	49,88494	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 214	50,207953	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 214	50,530966	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...

red 214	50,853979	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 214	51,176992	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 214	51,500005	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 214	51,823018	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...