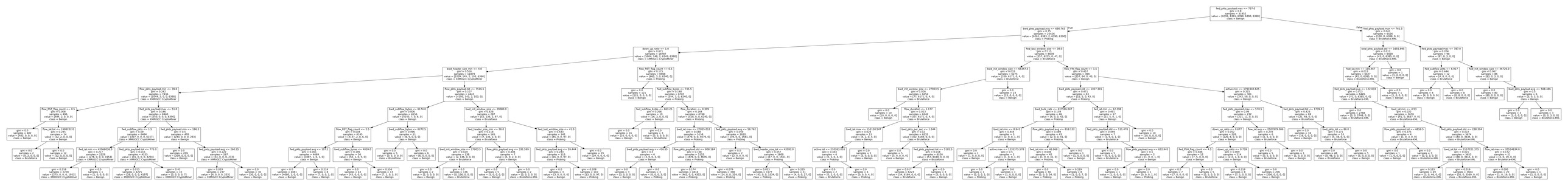

fwd_pkts_payload.max <= 737.0
gini = 0.8
samples = 31952
value = [6391, 6391, 6390, 6390, 6390]
class = Benign

bwd_pkts_payload.avg <= 690.763
gini = 0.75
samples = 25426
value = [6261, 6383, 2, 6390, 6390]
class = Probing

True fwd_pkts_payload.max <= 761.5
gini = 0.041
samples = 6526
value = [130, 8, 6388, 0, 0]
class = Bruteforce-XML

False

down_up_ratio <= 1.0
gini = 0.671
samples = 18787
value = [5904, 148, 2, 6343, 6390]
class = XMRIGCC CryptoMiner

fwd_last_window_size <= 39.0
gini = 0.115
samples = 6639
value = [357, 6235, 0, 47, 0]
class = Bruteforce

bwd_header_size_min <= 4.0
gini = 0.516
samples = 11879
value = [5239, 145, 2, 103, 6390]
class = XMRIGCC CryptoMiner

flow_RST_flag_count <= 0.5
gini = 0.175
samples = 6908
value = [665, 3, 0, 6240, 0]
class = Probing

flow_pkts_payload.min <= 39.0
gini = 0.242
samples = 7436
value = [1044, 2, 0, 0, 6390]
class = XMRIGCC CryptoMiner

flow_pkts_payload.tot <= 7516.5
gini = 0.107
samples = 4443
value = [4195, 143, 2, 103, 0]
class = Benign

flow_RST_flag_count <= 0.5
gini = 0.008
samples = 496
value = [494, 2, 0, 0, 0]
class = Benign

fwd_pkts_payload.max <= 51.0
gini = 0.146
samples = 6940
value = [550, 0, 0, 0, 6390]
class = XMRIGCC CryptoMiner

gini = 0.0
samples = 482
value = [482, 0, 0, 0, 0]
class = Benign

flow_iat.tot <= 1998232.0
gini = 0.245
samples = 14
value = [12, 2, 0, 0, 0]
class = Benign

gini = 0.0
samples = 2
value = [0, 2, 0, 0, 0]
class = Bruteforce

gini = 0.0
samples = 12
value = [12, 0, 0, 0, 0]
class = Benign

fwd_subflow_pkts <= 1.5
gini = 0.09
samples = 6464
value = [307, 0, 0, 0, 6157]
class = XMRIGCC CryptoMiner

fwd_pkts_payload.min <= 196.5
gini = 0.5
samples = 476
value = [243, 0, 0, 0, 233]
class = Benign

fwd_iat.min <= 42066036.0
gini = 0.217
samples = 2229
value = [276, 0, 0, 0, 1953]
class = XMRIGCC CryptoMiner

fwd_pkts_payload.tot <= 775.0
gini = 0.015
samples = 4235
value = [31, 0, 0, 0, 4204]
class = XMRIGCC CryptoMiner

gini = 0.216
samples = 2228
value = [275, 0, 0, 0, 1953]
class = XMRIGCC CryptoMiner

gini = 0.0
samples = 1
value = [1, 0, 0, 0, 0]
class = Benign

gini = 0.013
samples = 4225
value = [28, 0, 0, 0, 4197]
class = XMRIGCC CryptoMiner

gini = 0.42
samples = 10
value = [3, 0, 0, 0, 7]
class = XMRIGCC CryptoMiner

gini = 0.0
samples = 209
value = [209, 0, 0, 0, 0]
class = Benign

fwd_pkts_payload.avg <= 260.25
gini = 0.222
samples = 267
value = [34, 0, 0, 0, 233]
class = XMRIGCC CryptoMiner

gini = 0.033
samples = 237
value = [4, 0, 0, 0, 233]
class = XMRIGCC CryptoMiner

gini = 0.0
samples = 30
value = [30, 0, 0, 0, 0]
class = Benign

bwd_subflow_bytes <= 6174.0
gini = 0.006
samples = 4156
value = [4143, 7, 0, 6, 0]
class = Benign

bwd_init_window_size <= 29080.0
gini = 0.628
samples = 287
value = [52, 136, 2, 97, 0]
class = Bruteforce

flow_RST_flag_count <= 2.5
gini = 0.004
samples = 4145
value = [4137, 2, 0, 6, 0]
class = Benign

bwd_subflow_bytes <= 6272.5
gini = 0.496
samples = 11
value = [6, 5, 0, 0, 0]
class = Benign

fwd_pkts_payload.avg <= 107.1
gini = 0.001
samples = 4089
value = [4087, 1, 0, 1, 0]
class = Benign

bwd_subflow_bytes <= 4039.0
gini = 0.195
samples = 56
value = [50, 1, 0, 5, 0]
class = Benign

gini = 0.0
samples = 4081
value = [4080, 1, 0, 0, 0]
class = Benign

gini = 0.219
samples = 8
value = [7, 0, 0, 1, 0]
class = Benign

gini = 0.0
samples = 43
value = [43, 0, 0, 0, 0]
class = Benign

gini = 0.556
samples = 13
value = [7, 1, 0, 5, 0]
class = Benign

gini = 0.0
samples = 5
value = [0, 5, 0, 0, 0]
class = Bruteforce

gini = 0.0
samples = 6
value = [6, 0, 0, 0, 0]
class = Benign

fwd_header_size_min <= 26.0
gini = 0.118
samples = 145
value = [7, 136, 2, 0, 0]
class = Bruteforce

fwd_last_window_size <= 41.0
gini = 0.433
samples = 142
value = [45, 0, 0, 97, 0]
class = Probing

bwd_init_window_size <= 27903.5
gini = 0.029
samples = 138
value = [2, 136, 0, 0, 0]
class = Bruteforce

flow_pkts_payload.avg <= 331.599
gini = 0.408
samples = 7
value = [5, 0, 2, 0, 0]
class = Benign

gini = 0.0
samples = 2
value = [2, 0, 0, 0, 0]
class = Benign

gini = 0.0
samples = 136
value = [0, 136, 0, 0, 0]
class = Bruteforce

gini = 0.0
samples = 5
value = [5, 0, 0, 0, 0]
class = Benign

gini = 0.0
samples = 2
value = [0, 0, 2, 0, 0]
class = Bruteforce-XML

fwd_pkts_payload.avg <= 59.444
gini = 0.243
samples = 113
value = [16, 0, 0, 97, 0]
class = Probing

gini = 0.0
samples = 29
value = [29, 0, 0, 0, 0]
class = Benign

gini = 0.0
samples = 3
value = [3, 0, 0, 0, 0]
class = Benign

gini = 0.208
samples = 110
value = [13, 0, 0, 97, 0]
class = Probing

gini = 0.0
samples = 121
value = [121, 0, 0, 0, 0]
class = Benign

fwd_subflow_bytes <= 745.5
gini = 0.148
samples = 6787
value = [544, 3, 0, 6240, 0]
class = Probing

fwd_subflow_bytes <= 663.25
gini = 0.266
samples = 19
value = [16, 3, 0, 0, 0]
class = Benign

flow_duration <= 0.309
gini = 0.144
samples = 6768
value = [528, 0, 0, 6240, 0]
class = Probing

gini = 0.0
samples = 16
value = [16, 0, 0, 0, 0]
class = Benign

gini = 0.0
samples = 3
value = [0, 3, 0, 0, 0]
class = Bruteforce

bwd_iat.max <= 27835.012
gini = 0.168
samples = 5158
value = [479, 0, 0, 4679, 0]
class = Probing

fwd_pkts_payload.avg <= 56.762
gini = 0.059
samples = 1610
value = [49, 0, 0, 1561, 0]
class = Probing

bwd_pkts_payload.avg <= 416.65
gini = 0.5
samples = 6
value = [3, 0, 0, 3, 0]
class = Benign

flow_pkts_payload.std <= 808.184
gini = 0.168
samples = 5152
value = [476, 0, 0, 4676, 0]
class = Probing

gini = 0.0
samples = 3
value = [3, 0, 0, 0, 0]
class = Benign

gini = 0.0
samples = 3
value = [0, 0, 0, 3, 0]
class = Probing

gini = 0.174
samples = 4814
value = [462, 0, 0, 4352, 0]
class = Probing

gini = 0.079
samples = 338
value = [14, 0, 0, 324, 0]
class = Probing

gini = 0.0
samples = 2
value = [2, 0, 0, 0, 0]
class = Benign

bwd_header_size_tot <= 42092.0
gini = 0.057
samples = 1608
value = [47, 0, 0, 1561, 0]
class = Probing

gini = 0.053
samples = 1577
value = [43, 0, 0, 1534, 0]
class = Probing

gini = 0.225
samples = 31
value = [4, 0, 0, 27, 0]
class = Probing

bwd_init_window_size <= 65347.5
gini = 0.033
samples = 6275
value = [100, 6171, 0, 4, 0]
class = Bruteforce

flow_FIN_flag_count <= 1.5
gini = 0.457
samples = 364
value = [257, 64, 0, 43, 0]
class = Benign

bwd_init_window_size <= 27903.5
gini = 0.026
samples = 6252
value = [77, 6171, 0, 4, 0]
class = Bruteforce

gini = 0.0
samples = 23
value = [23, 0, 0, 0, 0]
class = Benign

gini = 0.0
samples = 10
value = [10, 0, 0, 0, 0]
class = Benign

flow_duration <= 1.177
gini = 0.023
samples = 6242
value = [67, 6171, 0, 4, 0]
class = Bruteforce

bwd_iat.max <= 153158.547
gini = 0.628
samples = 11
value = [5, 2, 0, 4, 0]
class = Benign

bwd_pkts_per_sec <= 1.344
gini = 0.02
samples = 6231
value = [62, 6169, 0, 0, 0]
class = Bruteforce

active.tot <= 210263.016
gini = 0.444
samples = 6
value = [0, 2, 0, 4, 0]
class = Probing

gini = 0.0
samples = 5
value = [5, 0, 0, 0, 0]
class = Benign

gini = 0.0
samples = 2
value = [0, 2, 0, 0, 0]
class = Bruteforce

gini = 0.0
samples = 4
value = [0, 0, 0, 4, 0]
class = Probing

gini = 0.0
samples = 5
value = [5, 0, 0, 0, 0]
class = Benign

fwd_pkts_payload.tot <= 5185.5
gini = 0.018
samples = 6226
value = [57, 6169, 0, 0, 0]
class = Bruteforce

gini = 0.017
samples = 6223
value = [54, 6169, 0, 0, 0]
class = Bruteforce

gini = 0.0
samples = 3
value = [3, 0, 0, 0, 0]
class = Benign

bwd_pkts_payload.std <= 1057.315
gini = 0.471
samples = 63
value = [15, 5, 0, 43, 0]
class = Probing

active.min <= 1791942.625
gini = 0.315
samples = 301
value = [242, 59, 0, 0, 0]
class = Benign

bwd_bulk_rate <= 437596.047
gini = 0.159
samples = 46
value = [4, 0, 0, 42, 0]
class = Probing

fwd_iat.min <= 12.398
gini = 0.491
samples = 17
value = [11, 5, 0, 1, 0]
class = Benign

bwd_iat.min <= 8.941
gini = 0.444
samples = 3
value = [2, 0, 0, 1, 0]
class = Benign

flow_pkts_payload.avg <= 618.132
gini = 0.089
samples = 43
value = [2, 0, 0, 41, 0]
class = Probing

gini = 0.0
samples = 1
value = [1, 0, 0, 0, 0]
class = Benign

active.max <= 1235375.578
gini = 0.5
samples = 2
value = [1, 0, 0, 1, 0]
class = Benign

gini = 0.0
samples = 1
value = [0, 0, 0, 1, 0]
class = Probing

gini = 0.0
samples = 1
value = [1, 0, 0, 0, 0]
class = Benign

fwd_iat.min <= 46.968
gini = 0.046
samples = 42
value = [1, 0, 0, 41, 0]
class = Probing

gini = 0.0
samples = 1
value = [1, 0, 0, 0, 0]
class = Benign

gini = 0.0
samples = 34
value = [0, 0, 0, 34, 0]
class = Probing

gini = 0.219
samples = 8
value = [1, 0, 0, 7, 0]
class = Probing

fwd_pkts_payload.std <= 111.478
gini = 0.449
samples = 7
value = [1, 5, 0, 1, 0]
class = Bruteforce

gini = 0.0
samples = 10
value = [10, 0, 0, 0, 0]
class = Benign

gini = 0.0
samples = 5
value = [0, 5, 0, 0, 0]
class = Bruteforce

flow_pkts_payload.avg <= 622.945
gini = 0.5
samples = 2
value = [1, 0, 0, 1, 0]
class = Benign

gini = 0.0
samples = 1
value = [1, 0, 0, 0, 0]
class = Benign

gini = 0.0
samples = 1
value = [0, 0, 0, 1, 0]
class = Probing

fwd_pkts_payload.max <= 570.5
gini = 0.09
samples = 232
value = [221, 11, 0, 0, 0]
class = Benign

fwd_pkts_payload.tot <= 1739.0
gini = 0.423
samples = 69
value = [21, 48, 0, 0, 0]
class = Bruteforce

down_up_ratio <= 0.677
gini = 0.052
samples = 226
value = [220, 6, 0, 0, 0]
class = Benign

flow_iat.avg <= 2507979.086
gini = 0.278
samples = 6
value = [1, 5, 0, 0, 0]
class = Bruteforce

fwd_PSH_flag_count <= 4.5
gini = 0.486
samples = 12
value = [7, 5, 0, 0, 0]
class = Benign

down_up_ratio <= 0.739
gini = 0.009
samples = 214
value = [213, 1, 0, 0, 0]
class = Benign

gini = 0.0
samples = 7
value = [7, 0, 0, 0, 0]
class = Benign

gini = 0.0
samples = 5
value = [0, 5, 0, 0, 0]
class = Bruteforce

gini = 0.219
samples = 8
value = [7, 1, 0, 0, 0]
class = Benign

gini = 0.0
samples = 206
value = [206, 0, 0, 0, 0]
class = Benign

gini = 0.0
samples = 5
value = [0, 5, 0, 0, 0]
class = Bruteforce

gini = 0.0
samples = 1
value = [1, 0, 0, 0, 0]
class = Benign

gini = 0.0
samples = 16
value = [16, 0, 0, 0, 0]
class = Benign

bwd_pkts_tot <= 86.0
gini = 0.171
samples = 53
value = [5, 48, 0, 0, 0]
class = Bruteforce

gini = 0.0
samples = 48
value = [0, 48, 0, 0, 0]
class = Bruteforce

gini = 0.0
samples = 5
value = [5, 0, 0, 0, 0]
class = Benign

bwd_pkts_payload.std <= 1655.895
gini = 0.013
samples = 6428
value = [43, 0, 6385, 0, 0]
class = Bruteforce-XML

fwd_pkts_payload.max <= 787.0
gini = 0.204
samples = 98
value = [87, 8, 3, 0, 0]
class = Benign

fwd_iat.min <= 116.467
gini = 0.013
samples = 6427
value = [42, 0, 6385, 0, 0]
class = Bruteforce-XML

gini = 0.0
samples = 1
value = [1, 0, 0, 0, 0]
class = Benign

fwd_pkts_payload.avg <= 122.033
gini = 0.013
samples = 6426
value = [41, 0, 6385, 0, 0]
class = Bruteforce-XML

gini = 0.0
samples = 1
value = [1, 0, 0, 0, 0]
class = Benign

gini = 0.0
samples = 2748
value = [0, 0, 2748, 0, 0]
class = Bruteforce-XML

bwd_iat.min <= 4.53
gini = 0.022
samples = 3678
value = [41, 0, 3637, 0, 0]
class = Bruteforce-XML

flow_pkts_payload.tot <= 6856.5
gini = 0.375
samples = 4
value = [1, 0, 3, 0, 0]
class = Bruteforce-XML

fwd_pkts_payload.std <= 238.394
gini = 0.022
samples = 3674
value = [40, 0, 3634, 0, 0]
class = Bruteforce-XML

gini = 0.0
samples = 1
value = [1, 0, 0, 0, 0]
class = Benign

gini = 0.0
samples = 3
value = [0, 0, 3, 0, 0]
class = Bruteforce-XML

bwd_iat.tot <= 2157221.375
gini = 0.021
samples = 3653
value = [38, 0, 3615, 0, 0]
class = Bruteforce-XML

flow_iat.max <= 20534634.0
gini = 0.172
samples = 21
value = [2, 0, 19, 0, 0]
class = Bruteforce-XML

gini = 0.115
samples = 49
value = [3, 0, 46, 0, 0]
class = Bruteforce-XML

gini = 0.019
samples = 3604
value = [35, 0, 3569, 0, 0]
class = Bruteforce-XML

gini = 0.095
samples = 20
value = [1, 0, 19, 0, 0]
class = Bruteforce-XML

gini = 0.0
samples = 1
value = [1, 0, 0, 0, 0]
class = Benign

fwd_subflow_pkts <= 6.917
gini = 0.444
samples = 12
value = [4, 8, 0, 0, 0]
class = Bruteforce

fwd_init_window_size <= 46720.0
gini = 0.067
samples = 86
value = [83, 0, 3, 0, 0]
class = Benign

gini = 0.0
samples = 4
value = [4, 0, 0, 0, 0]
class = Benign

gini = 0.0
samples = 8
value = [0, 8, 0, 0, 0]
class = Bruteforce

gini = 0.0
samples = 80
value = [80, 0, 0, 0, 0]
class = Benign

bwd_pkts_payload.avg <= 508.486
gini = 0.5
samples = 6
value = [3, 0, 3, 0, 0]
class = Benign

gini = 0.0
samples = 3
value = [3, 0, 0, 0, 0]
class = Benign

gini = 0.0
samples = 3
value = [0, 0, 3, 0, 0]
class = Bruteforce-XML