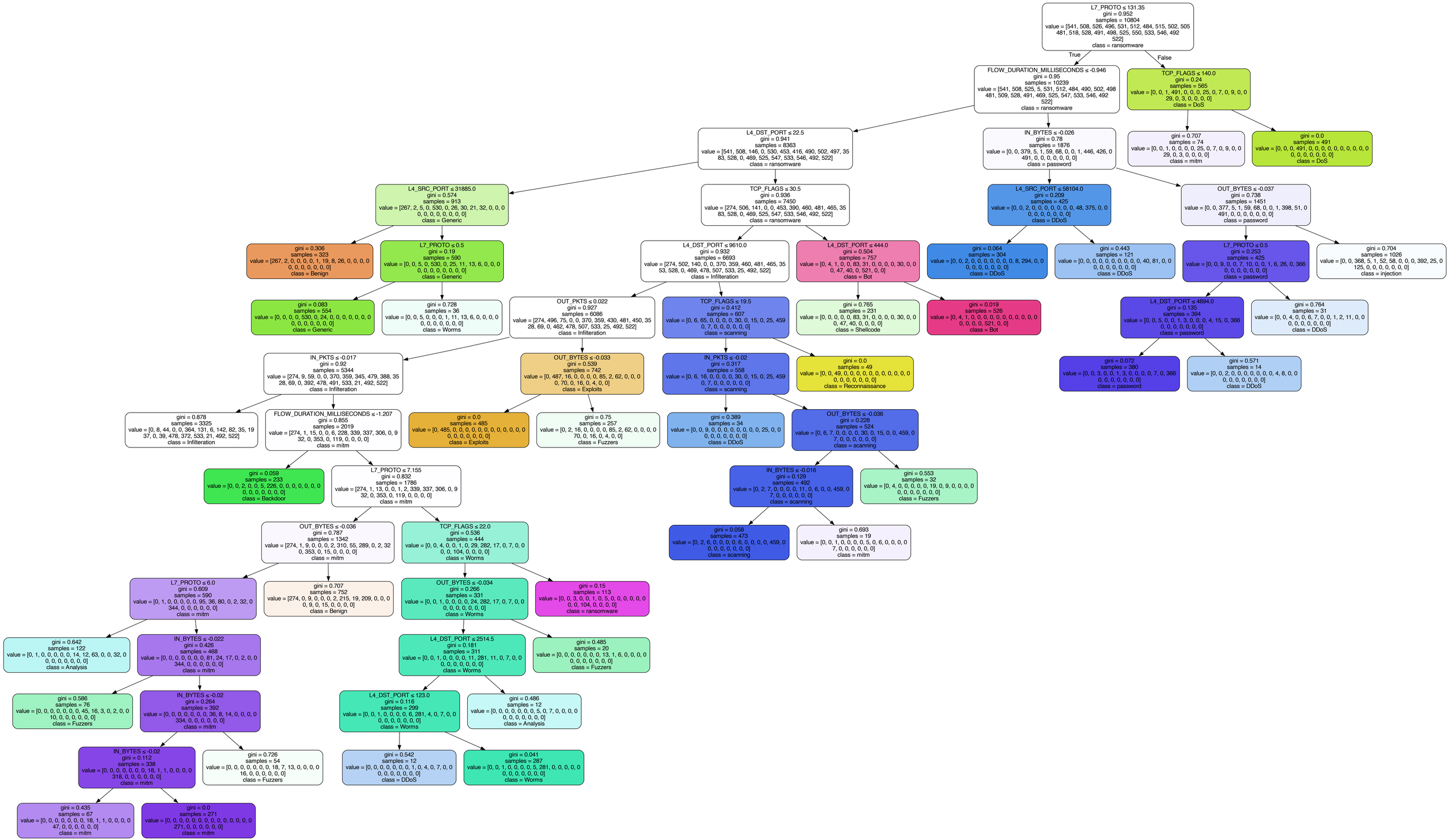
L7_PROTO ≤ 131.35
gini = 0.952
samples = 10804
value = [541, 508, 526, 496, 531, 512, 484, 515, 502, 505 481, 518, 528, 491, 498, 525, 550, 533, 546, 492 522]
class = ransomware
True
False
FLOW_DURATION_MILLISECONDS ≤ -0.946
gini = 0.95
samples = 10239
value = [541, 508, 525, 5, 531, 512, 484, 490, 502, 498 481, 509, 528, 491, 469, 525, 547, 533, 546, 492 522]
class = ransomware
TCP_FLAGS ≤ 140.0
gini = 0.24
samples = 565
value = [0, 0, 1, 491, 0, 0, 0, 25, 0, 7, 0, 9, 0, 0 29, 0, 3, 0, 0, 0, 0]
class = DoS
L4_DST_PORT ≤ 22.5
gini = 0.941
samples = 8363
value = [541, 508, 146, 0, 530, 453, 416, 490, 502, 497, 35 83, 528, 0, 469, 525, 547, 533, 546, 492, 522]
class = ransomware
IN_BYTES ≤ -0.026
gini = 0.78
samples = 1876
value = [0, 0, 379, 5, 1, 59, 68, 0, 0, 1, 446, 426, 0 491, 0, 0, 0, 0, 0, 0, 0]
class = password
gini = 0.707
samples = 74
value = [0, 0, 1, 0, 0, 0, 0, 25, 0, 7, 0, 9, 0, 0 29, 0, 3, 0, 0, 0, 0]
class = mitm
gini = 0.0
samples = 491
value = [0, 0, 0, 491, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 0, 0, 0, 0, 0, 0, 0]
class = DoS
L4_SRC_PORT ≤ 31885.0
gini = 0.574
samples = 913
value = [267, 2, 5, 0, 530, 0, 26, 30, 21, 32, 0, 0, 0 0, 0, 0, 0, 0, 0, 0, 0]
class = Generic
TCP_FLAGS ≤ 30.5
gini = 0.936
samples = 7450
value = [274, 506, 141, 0, 0, 453, 390, 460, 481, 465, 35 83, 528, 0, 469, 525, 547, 533, 546, 492, 522]
class = ransomware
L4_SRC_PORT ≤ 58104.0
gini = 0.209
samples = 425
value = [0, 0, 2, 0, 0, 0, 0, 0, 0, 0, 0, 48, 375, 0, 0 0, 0, 0, 0, 0, 0, 0]
class = DDoS
OUT_BYTES ≤ -0.037
gini = 0.738
samples = 1451
value = [0, 0, 377, 5, 1, 59, 68, 0, 0, 1, 398, 51, 0 491, 0, 0, 0, 0, 0, 0, 0]
class = password
gini = 0.306
samples = 323
value = [267, 2, 0, 0, 0, 0, 1, 19, 8, 26, 0, 0, 0, 0 0, 0, 0, 0, 0, 0, 0]
class = Benign
L7_PROTO ≤ 0.5
gini = 0.19
samples = 590
value = [0, 0, 5, 0, 530, 0, 25, 11, 13, 6, 0, 0, 0 0, 0, 0, 0, 0, 0, 0, 0]
class = Generic
L4_DST_PORT ≤ 9610.0
gini = 0.932
samples = 6693
value = [274, 502, 140, 0, 0, 370, 359, 460, 481, 465, 35 53, 528, 0, 469, 478, 507, 533, 25, 492, 522]
class = Infilteration
L4_DST_PORT ≤ 444.0
gini = 0.504
samples = 757
value = [0, 4, 1, 0, 0, 83, 31, 0, 0, 0, 0, 30, 0, 0 0, 47, 40, 0, 521, 0, 0]
class = Bot
gini = 0.064
samples = 304
value = [0, 0, 2, 0, 0, 0, 0, 0, 0, 0, 8, 294, 0, 0 0, 0, 0, 0, 0, 0, 0]
class = DDoS
gini = 0.443
samples = 121
value = [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 40, 81, 0, 0 0, 0, 0, 0, 0, 0, 0]
class = DDoS
L7_PROTO ≤ 0.5
gini = 0.253
samples = 425
value = [0, 0, 9, 0, 0, 7, 10, 0, 0, 1, 6, 26, 0, 366 0, 0, 0, 0, 0, 0, 0]
class = password
gini = 0.704
samples = 1026
value = [0, 0, 368, 5, 1, 52, 58, 0, 0, 0, 392, 25, 0 125, 0, 0, 0, 0, 0, 0, 0]
class = injection
gini = 0.083
samples = 554
value = [0, 0, 0, 0, 530, 0, 24, 0, 0, 0, 0, 0, 0, 0 0, 0, 0, 0, 0, 0, 0]
class = Generic
gini = 0.728
samples = 36
value = [0, 0, 5, 0, 0, 0, 1, 11, 13, 6, 0, 0, 0, 0 0, 0, 0, 0, 0, 0, 0]
class = Worms
OUT_PKTS ≤ 0.022
gini = 0.927
samples = 6086
value = [274, 496, 75, 0, 0, 370, 359, 430, 481, 450, 35 28, 69, 0, 462, 478, 507, 533, 25, 492, 522]
class = Infilteration
TCP_FLAGS ≤ 19.5
gini = 0.412
samples = 607
value = [0, 6, 65, 0, 0, 0, 0, 30, 0, 15, 0, 25, 459 0, 7, 0, 0, 0, 0, 0, 0]
class = scanning
gini = 0.765
samples = 231
value = [0, 0, 0, 0, 0, 83, 31, 0, 0, 0, 0, 30, 0, 0 0, 47, 40, 0, 0, 0, 0]
class = Shellcode
gini = 0.019
samples = 526
value = [0, 4, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 0, 0, 0, 0, 521, 0, 0]
class = Bot
L4_DST_PORT ≤ 4894.0
gini = 0.135
samples = 394
value = [0, 0, 5, 0, 0, 1, 3, 0, 0, 0, 4, 15, 0, 366 0, 0, 0, 0, 0, 0, 0]
class = password
gini = 0.764
samples = 31
value = [0, 0, 4, 0, 0, 6, 7, 0, 0, 1, 2, 11, 0, 0 0, 0, 0, 0, 0, 0, 0]
class = DDoS
IN_PKTS ≤ -0.017
gini = 0.92
samples = 5344
value = [274, 9, 59, 0, 0, 370, 359, 345, 479, 388, 35 28, 69, 0, 392, 478, 491, 533, 21, 492, 522]
class = Infilteration
OUT_BYTES ≤ -0.033
gini = 0.539
samples = 742
value = [0, 487, 16, 0, 0, 0, 0, 85, 2, 62, 0, 0, 0 0, 70, 0, 16, 0, 4, 0, 0]
class = Exploits
IN_PKTS ≤ -0.02
gini = 0.317
samples = 558
value = [0, 6, 16, 0, 0, 0, 0, 30, 0, 15, 0, 25, 459 0, 7, 0, 0, 0, 0, 0, 0]
class = scanning
gini = 0.0
samples = 49
value = [0, 0, 49, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 0, 0, 0, 0, 0, 0, 0]
class = Reconnaissance
gini = 0.072
samples = 380
value = [0, 0, 3, 0, 0, 1, 3, 0, 0, 0, 0, 7, 0, 366 0, 0, 0, 0, 0, 0, 0]
class = password
gini = 0.571
samples = 14
value = [0, 0, 2, 0, 0, 0, 0, 0, 0, 0, 0, 4, 8, 0, 0 0, 0, 0, 0, 0, 0, 0]
class = DDoS
gini = 0.878
samples = 3325
value = [0, 8, 44, 0, 0, 364, 131, 6, 142, 82, 35, 19 37, 0, 39, 478, 372, 533, 21, 492, 522]
class = Infilteration
FLOW_DURATION_MILLISECONDS ≤ -1.207
gini = 0.855
samples = 2019
value = [274, 1, 15, 0, 0, 6, 228, 339, 337, 306, 0, 9 32, 0, 353, 0, 119, 0, 0, 0, 0]
class = mitm
gini = 0.0
samples = 485
value = [0, 485, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 0, 0, 0, 0, 0, 0, 0]
class = Exploits
gini = 0.75
samples = 257
value = [0, 2, 16, 0, 0, 0, 0, 85, 2, 62, 0, 0, 0, 0 70, 0, 16, 0, 4, 0, 0]
class = Fuzzers
gini = 0.389
samples = 34
value = [0, 0, 9, 0, 0, 0, 0, 0, 0, 0, 0, 25, 0, 0 0, 0, 0, 0, 0, 0, 0]
class = DDoS
OUT_BYTES ≤ -0.036
gini = 0.228
samples = 524
value = [0, 6, 7, 0, 0, 0, 0, 30, 0, 15, 0, 0, 459, 0 7, 0, 0, 0, 0, 0, 0]
class = scanning
IN_BYTES ≤ -0.016
gini = 0.129
samples = 492
value = [0, 2, 7, 0, 0, 0, 0, 11, 0, 6, 0, 0, 459, 0 7, 0, 0, 0, 0, 0, 0]
class = scanning
gini = 0.553
samples = 32
value = [0, 4, 0, 0, 0, 0, 0, 19, 0, 9, 0, 0, 0, 0 0, 0, 0, 0, 0, 0, 0]
class = Fuzzers
gini = 0.058
samples = 473
value = [0, 2, 6, 0, 0, 0, 0, 6, 0, 0, 0, 0, 459, 0 0, 0, 0, 0, 0, 0, 0]
class = scanning
gini = 0.693
samples = 19
value = [0, 0, 1, 0, 0, 0, 0, 5, 0, 6, 0, 0, 0, 0 7, 0, 0, 0, 0, 0, 0]
class = mitm
gini = 0.059
samples = 233
value = [0, 0, 2, 0, 0, 5, 226, 0, 0, 0, 0, 0, 0, 0 0, 0, 0, 0, 0, 0, 0]
class = Backdoor
L7_PROTO ≤ 7.155
gini = 0.832
samples = 1786
value = [274, 1, 13, 0, 0, 1, 2, 339, 337, 306, 0, 9 32, 0, 353, 0, 119, 0, 0, 0, 0]
class = mitm
OUT_BYTES ≤ -0.036
gini = 0.787
samples = 1342
value = [274, 1, 9, 0, 0, 0, 2, 310, 55, 289, 0, 2, 32 0, 353, 0, 15, 0, 0, 0, 0]
class = mitm
TCP_FLAGS ≤ 22.0
gini = 0.536
samples = 444
value = [0, 0, 4, 0, 0, 1, 0, 29, 282, 17, 0, 7, 0, 0 0, 0, 104, 0, 0, 0, 0]
class = Worms
L7_PROTO ≤ 6.0
gini = 0.609
samples = 590
value = [0, 1, 0, 0, 0, 0, 0, 95, 36, 80, 0, 2, 32, 0 344, 0, 0, 0, 0, 0, 0]
class = mitm
gini = 0.707
samples = 752
value = [274, 0, 9, 0, 0, 0, 2, 215, 19, 209, 0, 0, 0 0, 9, 0, 15, 0, 0, 0, 0]
class = Benign
OUT_BYTES ≤ -0.034
gini = 0.266
samples = 331
value = [0, 0, 1, 0, 0, 0, 0, 24, 282, 17, 0, 7, 0, 0 0, 0, 0, 0, 0, 0, 0]
class = Worms
gini = 0.15
samples = 113
value = [0, 0, 3, 0, 0, 1, 0, 5, 0, 0, 0, 0, 0, 0 0, 0, 104, 0, 0, 0, 0]
class = ransomware
gini = 0.642
samples = 122
value = [0, 1, 0, 0, 0, 0, 0, 14, 12, 63, 0, 0, 32, 0 0, 0, 0, 0, 0, 0, 0]
class = Analysis
IN_BYTES ≤ -0.022
gini = 0.426
samples = 468
value = [0, 0, 0, 0, 0, 0, 0, 81, 24, 17, 0, 2, 0, 0 344, 0, 0, 0, 0, 0, 0]
class = mitm
L4_DST_PORT ≤ 2514.5
gini = 0.181
samples = 311
value = [0, 0, 1, 0, 0, 0, 0, 11, 281, 11, 0, 7, 0, 0 0, 0, 0, 0, 0, 0, 0]
class = Worms
gini = 0.485
samples = 20
value = [0, 0, 0, 0, 0, 0, 0, 13, 1, 6, 0, 0, 0, 0 0, 0, 0, 0, 0, 0, 0]
class = Fuzzers
gini = 0.586
samples = 76
value = [0, 0, 0, 0, 0, 0, 0, 45, 16, 3, 0, 2, 0, 0 10, 0, 0, 0, 0, 0, 0]
class = Fuzzers
IN_BYTES ≤ -0.02
gini = 0.264
samples = 392
value = [0, 0, 0, 0, 0, 0, 0, 36, 8, 14, 0, 0, 0, 0 334, 0, 0, 0, 0, 0, 0]
class = mitm
L4_DST_PORT ≤ 123.0
gini = 0.116
samples = 299
value = [0, 0, 1, 0, 0, 0, 0, 6, 281, 4, 0, 7, 0, 0 0, 0, 0, 0, 0, 0, 0]
class = Worms
gini = 0.486
samples = 12
value = [0, 0, 0, 0, 0, 0, 0, 5, 0, 7, 0, 0, 0, 0 0, 0, 0, 0, 0, 0, 0]
class = Analysis
IN_BYTES ≤ -0.02
gini = 0.112
samples = 338
value = [0, 0, 0, 0, 0, 0, 0, 18, 1, 1, 0, 0, 0, 0 318, 0, 0, 0, 0, 0, 0]
class = mitm
gini = 0.726
samples = 54
value = [0, 0, 0, 0, 0, 0, 0, 18, 7, 13, 0, 0, 0, 0 16, 0, 0, 0, 0, 0, 0]
class = Fuzzers
gini = 0.542
samples = 12
value = [0, 0, 0, 0, 0, 0, 0, 1, 0, 4, 0, 7, 0, 0 0, 0, 0, 0, 0, 0, 0]
class = DDoS
gini = 0.041
samples = 287
value = [0, 0, 1, 0, 0, 0, 0, 5, 281, 0, 0, 0, 0, 0 0, 0, 0, 0, 0, 0, 0]
class = Worms
gini = 0.435
samples = 67
value = [0, 0, 0, 0, 0, 0, 0, 18, 1, 1, 0, 0, 0, 0 47, 0, 0, 0, 0, 0, 0]
class = mitm
gini = 0.0
samples = 271
value = [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 271, 0, 0, 0, 0, 0, 0]
class = mitm