**jz2791 Jihao Zhang**

**COMS 4180 Network Security Programming Assignment 2**

Problem 1.

a.

prog1: C/C++. In Strings, it contains the “vector::\_M\_insert\_aux” string

prog2: C/C++. In Strings, it contains the “memcmp”, “vector::\_M\_insert\_aux” strings.

prog3: C/C++. In Strings, it contains the “memcmp”, “malloc”, “atoi” strings.

prog4: C/C++. After unpacking with UPX, contains “memcmp” strings.

prog5: Java. In strings, it contains the “java/util/ArrayList”, ”java/lang/StringBuilder” strings.

prog6: Python. In strings, it contains the “/usr/lib/python2.7/site packages/scapy/layers/ntp.pyR” string.

b.

prog1 and prog2 are similar. Their fuzzy hashes matches at 69. Their ngram counting are also similar as listed in part c.

prog1.hash:prog1 matches prog2.hash:prog2 (69)

prog3 and prog4 are the same after unpacking prog4.

prog1, prog3 and prog2, prog3 are similar in the way that their top ngram counting overlaps significantly.

c.

• list the 20 bytes (1-grams) in hex that occur the most along with a count of each:

prog1:

[('0x0', 16631),

 ('0x48', 3359),

 ('0xff', 3146),

 ('0x5f', 1730),

 ('0x89', 1710),

 ('0x45', 1572),

 ('0x53', 1026),

 ('0x74', 1019),

 ('0x8b', 888),

 ('0xe8', 868),

 ('0x61', 850),

 ('0x49', 702),

 ('0x72', 683),

 ('0xc7', 659),

 ('0x40', 658),

 ('0x8d', 619),

 ('0x65', 550),

 ('0x69', 537),

 ('0x31', 476),

 ('0x63', 473)]

prog2:

[('0x0', 16916),

 ('0x48', 2778),

 ('0xff', 2472),

 ('0x5f', 1728),

 ('0x89', 1481),

 ('0x45', 1407),

 ('0x53', 1031),

 ('0x74', 1022),

 ('0x61', 841),

 ('0xe8', 745),

 ('0x8b', 709),

 ('0x49', 709),

 ('0x72', 677),

 ('0x40', 577),

 ('0x65', 543),

 ('0x69', 535),

 ('0xc7', 528),

 ('0x31', 480),

 ('0x63', 465),

 ('0x73', 451)]

prog3:

[('0x0', 19211),

 ('0x48', 2902),

 ('0xff', 2304),

 ('0x5f', 1857),

 ('0x89', 1612),

 ('0x45', 1439),

 ('0x74', 1012),

 ('0x8b', 841),

 ('0xe8', 826),

 ('0x53', 797),

 ('0x65', 743),

 ('0x61', 684),

 ('0x49', 667),

 ('0x40', 634),

 ('0xc7', 615),

 ('0x69', 602),

 ('0x72', 589),

 ('0x6f', 523),

 ('0x63', 489),

 ('0x6e', 455)]

prog4:

[('0x0', 515),

 ('0x17', 293),

 ('0x7', 230),

 ('0xff', 194),

 ('0x5f', 186),

 ('0x1', 181),

 ('0x10', 175),

 ('0x20', 174),

 ('0x8', 169),

 ('0x1f', 163),

 ('0x48', 162),

 ('0x3', 159),

 ('0xb0', 154),

 ('0x2', 150),

 ('0xf', 144),

 ('0xc', 144),

 ('0x2f', 139),

 ('0x6', 138),

 ('0x4', 137),

 ('0x40', 137)]

prog5:

[('0x0', 202),

 ('0x61', 71),

 ('0x1', 48),

 ('0x2f', 41),

 ('0x74', 34),

 ('0x6e', 34),

 ('0x72', 29),

 ('0x69', 29),

 ('0x6c', 28),

 ('0x67', 26),

 ('0x6a', 24),

 ('0x65', 24),

 ('0x76', 22),

 ('0x7', 19),

 ('0x4c', 16),

 ('0xa', 14),

 ('0x6f', 13),

 ('0xc', 13),

 ('0x53', 13),

 ('0x28', 12)]

prog6:

[('0x0', 1004),

 ('0x74', 147),

 ('0x64', 121),

 ('0x73', 102),

 ('0x65', 98),

 ('0x1', 89),

 ('0x69', 81),

 ('0x2', 63),

 ('0x70', 58),

 ('0x61', 57),

 ('0x2f', 56),

 ('0x3', 54),

 ('0x72', 52),

 ('0x79', 45),

 ('0x28', 44),

 ('0x6e', 43),

 ('0x6c', 42),

 ('0x52', 41),

 ('0x63', 40),

 ('0x4', 34)]

• list the top 20 2-grams in hex along with a count for each for a slide of 1 and a slide of 2 (there are 2 top 20 lists of 2-grams for each program)

slide of 1:

prog1:

[('0x0', 12375),

 ('0xffff', 1670),

 ('0x4889', 1597),

 ('0x488b', 810),

 ('0xff48', 759),

 ('0x89c7', 581),

 ('0xc7e8', 581),

 ('0x488d', 532),

 ('0x8b45', 477),

 ('0x4000', 439),

 ('0x5374', 406),

 ('0x48', 401),

 ('0x4953', 322),

 ('0x5f', 316),

 ('0x8d85', 291),

 ('0x7249', 288),

 ('0x5f5a', 270),

 ('0x4545', 245),

 ('0xd00', 236),

 ('0x800', 229)]

prog2:

[('0x0', 12804),

 ('0x4889', 1386),

 ('0xffff', 1313),

 ('0x488b', 679),

 ('0xff48', 550),

 ('0x89c7', 472),

 ('0xc7e8', 472),

 ('0x5374', 406),

 ('0x4000', 397),

 ('0x8b45', 377),

 ('0x488d', 340),

 ('0x48', 326),

 ('0x4953', 322),

 ('0x5f', 318),

 ('0x7249', 288),

 ('0x5f5a', 271),

 ('0x4545', 245),

 ('0xd00', 241),

 ('0x800', 224),

 ('0x6169', 210)]

prog3:

[('0x0', 14818),

 ('0x4889', 1489),

 ('0xffff', 1231),

 ('0x488b', 751),

 ('0x89c7', 547),

 ('0xc7e8', 546),

 ('0x8b45', 477),

 ('0x4000', 475),

 ('0x48', 399),

 ('0xff48', 338),

 ('0x5f', 313),

 ('0x6f72', 265),

 ('0x5f5a', 262),

 ('0x4545', 244),

 ('0xd00', 243),

 ('0x800', 237),

 ('0x5374', 234),

 ('0xf848', 227),

 ('0x488d', 220),

 ('0xd', 218)]

prog4:

[('0x0', 214),

 ('0x3c97', 25),

 ('0xffff', 21),

 ('0x4dd3', 18),

 ('0x200', 17),

 ('0x344d', 16),

 ('0x4000', 15),

 ('0x699a', 14),

 ('0xd334', 14),

 ('0x2', 13),

 ('0x973c', 13),

 ('0xff0f', 13),

 ('0xff17', 13),

 ('0x2083', 12),

 ('0x830c', 12),

 ('0xa669', 12),

 ('0x1414', 11),

 ('0x40', 10),

 ('0x4889', 10),

 ('0x6017', 9)]

prog5:

[('0x100', 45),

 ('0x0', 35),

 ('0x6e67', 22),

 ('0x7661', 22),

 ('0x6176', 21),

 ('0x6a61', 21),

 ('0x612f', 20),

 ('0x616e', 15),

 ('0x700', 15),

 ('0x2f6c', 14),

 ('0x672f', 14),

 ('0x696e', 14),

 ('0x6c61', 14),

 ('0xc00', 12),

 ('0x4c6a', 11),

 ('0x5374', 11),

 ('0x7269', 11),

 ('0x7472', 10),

 ('0xa00', 10),

 ('0x1', 9)]

prog6:

[('0x0', 535),

 ('0x64', 86),

 ('0x200', 52),

 ('0x300', 52),

 ('0x74', 49),

 ('0x100', 44),

 ('0x73', 41),

 ('0x400', 31),

 ('0x52', 27),

 ('0x7079', 27),

 ('0x83', 25),

 ('0x500', 23),

 ('0x7c', 21),

 ('0x2800', 20),

 ('0x600', 20),

 ('0x800', 20),

 ('0x700', 19),

 ('0x28', 18),

 ('0x65', 18),

 ('0x6e74', 17)]

slide of 2:

prog1:

[('0x0', 6506),

 ('0xffff', 1007),

 ('0x4889', 819),

 ('0x488b', 459),

 ('0x4000', 376),

 ('0xff48', 371),

 ('0xc7e8', 307),

 ('0x488d', 274),

 ('0x89c7', 274),

 ('0x5374', 216),

 ('0xd00', 210),

 ('0x8b45', 203),

 ('0x48', 195),

 ('0x2200', 191),

 ('0x800', 185),

 ('0xe10', 166),

 ('0x41', 165),

 ('0x430d', 164),

 ('0x8602', 164),

 ('0x1c00', 160)]

proj2:

[('0x0', 6717),

 ('0xffff', 837),

 ('0x4889', 734),

 ('0x488b', 399),

 ('0x4000', 362),

 ('0xff48', 262),

 ('0xc7e8', 253),

 ('0x89c7', 219),

 ('0xd00', 215),

 ('0x5374', 201),

 ('0x2200', 191),

 ('0x800', 181),

 ('0x5f', 175),

 ('0xe10', 167),

 ('0x41', 166),

 ('0x430d', 165),

 ('0x488d', 165),

 ('0x8602', 165),

 ('0x1c00', 162),

 ('0x4953', 162)]

prog3:

[('0x0', 7730),

 ('0xffff', 801),

 ('0x4889', 735),

 ('0x488b', 440),

 ('0x4000', 402),

 ('0xc7e8', 276),

 ('0x89c7', 271),

 ('0xd00', 217),

 ('0x48', 214),

 ('0x8b45', 207),

 ('0x2200', 196),

 ('0x800', 185),

 ('0x41', 176),

 ('0xe10', 176),

 ('0x430d', 174),

 ('0x8602', 174),

 ('0xff48', 167),

 ('0x1c00', 166),

 ('0x5f', 162),

 ('0x5548', 151)]

prog4:

[('0x0', 117),

 ('0x3c97', 24),

 ('0x200', 12),

 ('0x4000', 10),

 ('0x4dd3', 9),

 ('0xffff', 9),

 ('0x2083', 8),

 ('0x699a', 8),

 ('0x100', 7),

 ('0x4889', 7),

 ('0x6572', 7),

 ('0x70f', 7),

 ('0xd334', 7),

 ('0xff17', 7),

 ('0x11b', 6),

 ('0x344d', 6),

 ('0x6017', 6),

 ('0x830c', 6),

 ('0x1414', 5),

 ('0x1964', 5)]

prog5:

[('0x100', 27),

 ('0x0', 17),

 ('0x6176', 16),

 ('0x612f', 15),

 ('0x6e67', 13),

 ('0x700', 12),

 ('0x6c61', 11),

 ('0x4c6a', 8),

 ('0x696e', 8),

 ('0x2f53', 6),

 ('0x7472', 6),

 ('0x1', 5),

 ('0x15', 5),

 ('0x6a61', 5),

 ('0x6e74', 5),

 ('0x7269', 5),

 ('0x7661', 5),

 ('0xa00', 5),

 ('0xb00', 5),

 ('0x200', 4)]

prog6:

[('0x0', 271),

 ('0x64', 44),

 ('0x200', 28),

 ('0x300', 24),

 ('0x100', 22),

 ('0x74', 22),

 ('0x83', 18),

 ('0x400', 17),

 ('0x52', 16),

 ('0x73', 15),

 ('0x500', 13),

 ('0x7079', 12),

 ('0x7c', 12),

 ('0x2800', 11),

 ('0x800', 11),

 ('0x28', 10),

 ('0x900', 10),

 ('0x600', 9),

 ('0x700', 9),

 ('0x7273', 9)]

list the 20 3-grams in hex along with the count of each for a slide of 1 and a slide of 3 (there are 2 top 20 lists of 3-grams for each program).

Slide of 1:

Prog1:

[('0x0', 9485),

 ('0xffff48', 734),

 ('0x89c7e8', 581),

 ('0x4889c7', 577),

 ('0x488b45', 470),

 ('0xff4889', 333),

 ('0x400000', 328),

 ('0x488d85', 291),

 ('0x48', 277),

 ('0x5f5a', 268),

 ('0xffffff', 249),

 ('0xff488d', 234),

 ('0x80000', 226),

 ('0xfeffff', 221),

 ('0xd00', 208),

 ('0x4889', 206),

 ('0x5f5a4e', 204),

 ('0x22', 188),

 ('0x2200', 187),

 ('0x22000d', 183)]

prog2:

[('0x0', 9967),

 ('0xffff48', 540),

 ('0x89c7e8', 472),

 ('0x4889c7', 468),

 ('0x488b45', 368),

 ('0x400000', 329),

 ('0x5f5a', 269),

 ('0x48', 241),

 ('0xff4889', 240),

 ('0x80000', 222),

 ('0xd00', 210),

 ('0x5f5a4e', 204),

 ('0xffffff', 195),

 ('0x488d85', 193),

 ('0x22', 188),

 ('0x2200', 187),

 ('0x22000d', 183),

 ('0x537434', 176),

 ('0x746f72', 173),

 ('0x347061', 171)]

prog3:

[('0x0', 11807),

 ('0x4889c7', 546),

 ('0x89c7e8', 546),

 ('0x488b45', 456),

 ('0x400000', 344),

 ('0xffff48', 338),

 ('0x5f5a', 262),

 ('0x48', 251),

 ('0x80000', 235),

 ('0xd00', 217),

 ('0x746f72', 210),

 ('0x22', 197),

 ('0x4889', 194),

 ('0xffffff', 193),

 ('0x2200', 192),

 ('0x1c0000', 187),

 ('0x22000d', 187),

 ('0x5f5a4e', 187),

 ('0x4889e5', 178),

 ('0xc0708', 177)]

prog4:

[('0x0', 136),

 ('0x3c973c', 13),

 ('0x973c97', 12),

 ('0x200', 8),

 ('0xd3344d', 8),

 ('0x2', 7),

 ('0x344dd3', 7),

 ('0x4000', 7),

 ('0x4dd334', 7),

 ('0x555058', 7),

 ('0xa6699a', 7),

 ('0xffffff', 7),

 ('0x20000', 6),

 ('0x40', 6),

 ('0x400000', 6),

 ('0x10000', 5),

 ('0x141414', 5),

 ('0x20830c', 5),

 ('0x830c32', 5),

 ('0x1', 4)]

prog5:

[('0x617661', 21),

 ('0x6a6176', 21),

 ('0x0', 20),

 ('0x76612f', 20),

 ('0x2f6c61', 14),

 ('0x612f6c', 14),

 ('0x616e67', 14),

 ('0x6c616e', 14),

 ('0x6e672f', 14),

 ('0x4c6a61', 11),

 ('0x72696e', 11),

 ('0x537472', 10),

 ('0x100', 8),

 ('0x672f53', 8),

 ('0x696e67', 8),

 ('0x747269', 8),

 ('0x2f5374', 7),

 ('0x284c6a', 5),

 ('0x3b0100', 5),

 ('0xb00', 5)]

prog6:

[('0x0', 272),

 ('0x73', 41),

 ('0x74', 39),

 ('0x30000', 28),

 ('0x52', 25),

 ('0x280000', 19),

 ('0x28', 18),

 ('0x40000', 17),

 ('0x2800', 16),

 ('0x60000', 14),

 ('0x740300', 14),

 ('0x640200', 13),

 ('0x657273', 13),

 ('0x740400', 13),

 ('0x10000', 12),

 ('0x20000', 12),

 ('0x6402', 12),

 ('0x80000', 12),

 ('0x10064', 11),

 ('0x50000', 11)]

slide of 3:

prog1:

[('0x0', 3239),

 ('0xffff48', 240),

 ('0xd00', 207),

 ('0x4889c7', 189),

 ('0x22', 187),

 ('0x89c7e8', 173),

 ('0x488b45', 159),

 ('0xff4889', 122),

 ('0x488d85', 102),

 ('0x48', 91),

 ('0x5f5a', 90),

 ('0x80000', 77),

 ('0x5f5a4e', 75),

 ('0x4889', 74),

 ('0xfeffff', 72),

 ('0xffffff', 71),

 ('0xff488d', 68),

 ('0x12', 65),

 ('0x347061', 61),

 ('0x48897d', 61)]

proj2:

[('0x0', 3409),

 ('0x2200', 187),

 ('0xffff48', 187),

 ('0x4889c7', 169),

 ('0x89c7e8', 149),

 ('0x488b45', 123),

 ('0x1200', 112),

 ('0x5f5a', 83),

 ('0x48', 82),

 ('0x5f5a4e', 78),

 ('0x80000', 77),

 ('0xff4889', 73),

 ('0xfdffff', 63),

 ('0x4889e5', 62),

 ('0x746f72', 61),

 ('0x410e10', 59),

 ('0x48897d', 59),

 ('0x860243', 59),

 ('0x347061', 58),

 ('0x537434', 58)]

proj3:

[('0x0', 3968),

 ('0x89c7e8', 212),

 ('0x2200', 191),

 ('0x4889c7', 176),

 ('0x488b45', 149),

 ('0xffff48', 111),

 ('0x48', 91),

 ('0x5f5a', 91),

 ('0x80000', 74),

 ('0x1200', 69),

 ('0x4889', 68),

 ('0x746f72', 68),

 ('0xffffff', 66),

 ('0x2430d', 64),

 ('0x4889e5', 64),

 ('0x5f5a4e', 64),

 ('0xe1086', 64),

 ('0x1c0000', 59),

 ('0x41', 59),

 ('0x70800', 59)]

proj4:

[('0x0', 43),

 ('0x3c973c', 5),

 ('0x20000', 4),

 ('0x20830c', 4),

 ('0x4000', 4),

 ('0x83eefc', 4),

 ('0x8b1e48', 4),

 ('0x973c97', 4),

 ('0xa6699a', 4),

 ('0x11db8a', 3),

 ('0x200', 3),

 ('0x344dd3', 3),

 ('0x41ffd3', 3),

 ('0x4dd334', 3),

 ('0x555058', 3),

 ('0x699aa6', 3),

 ('0x196490', 2),

 ('0x1a00a0', 2),

 ('0x211f1c', 2),

 ('0x24007', 2)]

proj5:

[('0x6a6176', 10),

 ('0x612f6c', 8),

 ('0x616e67', 8),

 ('0x76612f', 7),

 ('0x6c616e', 5),

 ('0x0', 4),

 ('0x2f5374', 4),

 ('0x3b0100', 4),

 ('0x4c6a61', 4),

 ('0x537472', 4),

 ('0x617661', 4),

 ('0x72696e', 4),

 ('0x10016', 3),

 ('0x673b29', 3),

 ('0x100', 2),

 ('0x10000', 2),

 ('0x15284c', 2),

 ('0x170000', 2),

 ('0x2d284c', 2),

 ('0x2f4f62', 2)]

proj6:

[('0x0', 96),

 ('0x73', 13),

 ('0x74', 12),

 ('0x52', 10),

 ('0x30000', 9),

 ('0x6402', 8),

 ('0x8302', 8),

 ('0x740300', 7),

 ('0x2800', 6),

 ('0x280000', 6),

 ('0x8400', 6),

 ('0x60000', 5),

 ('0x617965', 5),

 ('0x6403', 5),

 ('0x740700', 5),

 ('0x7c0200', 5),

 ('0x10000', 4),

 ('0x10c01', 4),

 ('0x28', 4),

 ('0x61636b', 4)]