Anay Gupta
CSE 494: AI for Cyber Security
Shakarian - Friday 1 pm
February 8th, 2019

CSE 494 Lab 2 Exercises

1. Hash 1: 297529814d8d292594a1981fad30daa6
   a. Initialized data size = **237568**
   b. Code size = **61952**
   c. File type = **Win32 EXE**

   Hash 2: a30863f1a404bc2f735cc9ad862e85a9
   a. Initialized data size = **696320**
   b. Code size = **28672**
   c. File type = **Win32 EXE**

   Hash 3: 2e0c328aae6abfb19bf02e0fbc5dea93
   a. Initialized data size = **0**
   b. Code size = **24576**
   c. File type = **Win32 EXE**

2. a. Product Version Type = **Categorical** (can be allocated into different recurring categories).
   b. Image Version Type = **Ordinal** (can be allocated into different categories but with order — distance matters)
   c. File Type Type = **Categorical** (can be allocated into different recurring categories).

3. Initialized Data Size Means:
   Teslacrypt = 638268.952381
   dridex = 773436.952381
   locky = 405731.555556
   xtreme = 75288.380952

4. Hash 1: 297529814d8d292594a1981fad30daa6
   Entry point n grams: {'0x': 1, '4a': 1, '7e': 1, 'a': 1, 'e4': 1, 'x7': 1}
   Sorted n grams: [(u'a', 1), (u'e4', 1), (u'7e', 1), (u'4a', 1)]
   Hash 2: a30863f1a404bc2f735cc9ad862e85a9
   Entry point n grams: {'0': 1, '0x': 1, '5c': 1, '70': 1, 'c7': 1, 'x5': 1}
   Sorted n grams: [(u'0', 1), (u'c7', 1), (u'5c', 1), (u'70', 1)]
   Hash 3: 2e0c328aae6abfb19bf02e0fbc5dea93
   Entry point n grams: {'0': 1, '00': 1, '0x': 1, '40': 1, '4f': 1, 'f4': 1, 'x4': 1}
   Sorted n grams: [(u'4f', 1), (u'0', 1), (u'00', 1), (u'f4', 1), (u'40', 1)]