Network Security Project 2 Report

1. What model or algorithm you use?

   I used rule-based method because after I manually inspect all the data, I found that in “Execution process ID” in “Sysmon.xml” of different person are different and in “Example Test”, I found that “Execution process ID” are identical if the data belongs to the same person.

   According to above 2 discovered features, I used a dictionary to store the mappings of “Execution process ID” and “Person 1-6” so that every time a new data comes in, I only have to extract its “Execution process ID” to determine which person owns these data.

2. Anything interesting you find or problems you encounter in the whole process?

   The interesting things is that at the beginning I thought that this will be hard to choose which feature to use, but there’s a bug or something that “Execution process ID” itself is enough for me to decide these data belongs to which person.

   Problems I encountered is that in real world “Execution process ID” will change every time when the computer restart, so this method certainly can not adapt to the real world scenario and can only fit in this particular situation.