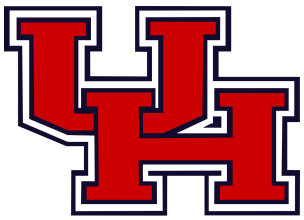
OS Fingerprinting using ML

Short Summary Report

Author

Shanto Roy

Department of Computer Science
University of Houston



April, 2021

Feature Selection and Classification for Operating System Fingerprinting by Analyzing Captured Network Packets

Shanto Roy
University of Houston
Houston, Texas
sroy10@uh.edu

ABSTRACT

The project is about fingerprinting operating systems using different multi-class classification algorithms. I tried to look into required features for OS fingerprinting and find accuracy of different classifiers based on different labeling (base OS platform, e.g., Windows vs OS versions, e.g., Win 7,8,10). The accuracy is almost 100% if labeled as base platform only (Windows, Ubuntu, macOS). However, the accuray is lower when labeled as the OS version (see below in the Ground Truth section).

KEYWORDS

OS Fingerprinting, Machine Learning, Multi-class Classification

1 INTRODUCTION

Operating system fingerprinting is the most important part of performing passive reconnaissance by an attacker as OS identification leads to vulnerability detection and exploit selection. Milestone I provided a probability-based belief update approach in a compromised network where cyber deception is not present. The work focused on passive fingerprinting to identify a network node configuration based on packet analysis. However, Milestone II report presents a deep insight regarding OS identification through analyzing different features of network packets and using classification algorithms to predict those OS. Code and basic documentation can be accessed in the Github repo [1].

In this work, the following research questions are addressed:

Q1. **OS fingerprinting features:** What are the important features to consider while identifying an OS?
Q2. **Classification Algorithms:** Which classification algorithms are more suitable to classify proper OS?
Q3. **OS Version Identification:** How better the classifiers perform while identifying OS versions?

While trying to answer the research questions, the primary contribution of the project is as follows:

- Selecting features based on ranking algorithms for OS identification
- Testing the performance of different multi-class classification algorithms for OS fingerprinting
- Finding out how TCP/IP stack implementation changes across the versions of the same OS

[1] https://github.com/shantoroy/OS_fingerprinting_using-ML

Outline. The rest of the report is organized as follows: Section 2 presents the necessary definition and details of widely used passive reconnaissance techniques and tools. Section 3 presents the data extraction, feature selection, and classifier selection procedures. Section 4 discuss different results and findings of the feature selection and model accuracy of the classifiers followed by concluding remarks.

2 BACKGROUND

2.1 Fingerprinting:

Fingerprinting is a method of analyzing response packets to determine the operating system, application version (e.g., web server), or network protocol (e.g., SNMP). Often, the operating system and/or the application reply with packets that expose the platform and version in the packet header. If this is not the case due to kernel patching (changed headers), blackholing (dropped packets/RST segments), or packet filtering (dropped packets for certain flags), then adversaries can look into the TCP/IP stack for further information [3]. Usually, operating systems set different values in the TCP/IP packet fields/flags depending on their version and architecture. Therefore, adversaries can analyze the response packets, compare the values against a dataset of various operating systems and versions, and identify the OS version (e.g., APT32 [2]).

2.2 OS Fingerprinting

Most of the tools prioritize two features (TTL and Window Size) to identify operating systems. A few other tools consider some other features, e.g., option fields such as SYN, ACK, or RST bit. Figure 1 presents a few example operating systems with the TTL and default window size values.

2.3 Literature Review

Hagos et al. provided an interesting OS fingerprinting approaches using machine learning to analyze different TCP traffics [4, 5]. They used the TCP traces to fingerprint remote OSes and achieved a fair accuracy while fingerprinting the OSes. They fingerprinted four computer OSes such as Linux, Unix, Windows, and macOS. They also fingerprinted two mobile OSes such as Android and IOS. They used SVM, KNN, Naive Bayes, and Random Forest classifiers and deep neural network (MLP and LSTM) to classify the operating systems.

Table 1: TTL and WS Variation for different OS

OS	TTL	WS
Linux 2.4 and 2.6	64	5840
Google customized Linux	64	5720
Linux kernel 2.2	64	32,120
FreeBSD	64	65,535
OpenBSD, AIX 4.3	64	16,384
Windows 2000	128	16,384
Windows XP	128	65,535
Windows 7, Vista, and Server 8	128	8,192
Cisco Router IOS 12.4	255	4,128
Solaris 7	255	8,760
MAC	64	65,535

Another similar work was performed by Song et al. [6] who used machine learning to fingerprint different OSes. They initially looked into a number of features that could be useful to fingerprint an OS. They were able to fingerprint Linux, AIX, Windows, and macOS and achieved aaround 90% accuracy using KNN, ANN, and Decision Tree classifiers.

Both of the most recent works focused on achieving accuracy for the base operating systems only. In this work, I have tried to find out the accuracy for the versions as well.

3 METHODOLOGY

This section provides information regarding the used dataset, initial data processing, labeling, feature selection process, and the list of used multi-class classifiers used in this project to classify the operating systems.

3.1 Dataset

I used a small part of the CIC-IDS2017 dataset [1] which is an intrusion detection dataset and has captured traffic in the network for seven days in a week.

```
ip_dict = {
     '192.168.10.51': 'Ubuntu server 12',
     '192.168.10.19': 'Ubuntu 14.4',
     '192.168.10.17': 'Ubuntu 14.4',
     '192.168.10.16': 'Ubuntu 16.4',
     '192.168.10.12': 'Ubuntu 16.4',
      '192.168.10.9': 'Win 7',
      '192.168.10.5': 'Win 8.1',
      '192.168.10.8': 'Win Vista',
     '192.168.10.14': 'Win 10',
     '192.168.10.15': 'Win 10',
     '192.168.10.25': 'macOS'
}
```

3.2 Initial Data Process

From the dataset, I extracted a small portion of data packet that still has a few thousands of instances of each operating system for faster workflow. Looking at the variation of data it seemed sufficient for me to identify OS.

Before performing the feature analysis, I extracted a number of fields from all packets to create a CSV file from the PCAP files. The following code is used to extract features mentioned after the $-e$ options. The details is provided in Appendix A.6.

3.3 Data Labeling

To label the data using the ground truth information, I intended to test four types of labeling:

- considering all OS versions
- considering only Windows versions
- considering only Ubuntu versions
- considering no version at all (labeling as base operating systems only), e.g., considering Win 7, 8, Vista, and 10 as "Windows"

3.4 Feature Selection Algorithms

I used the following feature ranking algorithms to identify best features for OS fingerprinting.

- Univariate Selection (ANOVA f-val, Chi-Squared)
- Recursive Feature Elimination
- Extra Tree Classifier for feature importance

Based on the results, I have selected the following features to consider for OS classification (Result in Appendix A.1).

- ip.flags.df
- ip.ttl
- ip.len
- tcp.seq
- tcp.ack
- tcp.len
- tcp.hdr_len
- tcp.flags.fin
- tcp.flags.syn
- tcp.flags.reset
- tcp.flags.push
- tcp.flags.ack
- tcp.window_size

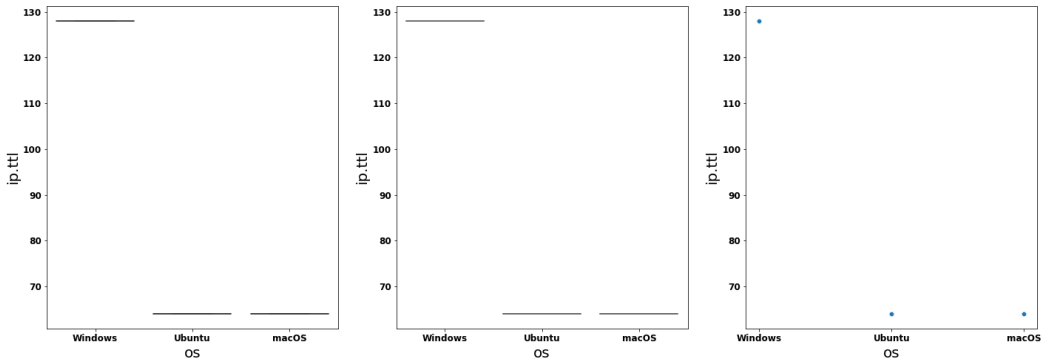


Figure 1: IP TTL

3.5 Classification Algorithms

I have tested the following multi-class classification algorithms to identify the OS classes.

- Logistic Regression Classifier
- K-Neighbor Classifier
- SVM (Linear) Classifier
- SVM (RBF) Classifier
- Naive Bayes Classifier
- Decision Tree Classifier
- Random Forest Classifier

4 RESULTS

In this section, first, I provide an insight into the feature values across different OS, and then I provide the performance of different classifiers for OS fingerprinting.

4.1 Feature Information

The following figures represents some of the interesting features that have variations across packets. To depict the data, each figure includes three types of visualization (box plot, violin plot, and scatter plot) of the same features across Ubuntu, Windows, and macOS. Figure 1, 2, 3, 4, and 5 presents the values of TTL, window size, TCP header length, TCP length, and IP length respectively across the operating systems.

4.2 Performance of Different Classifiers

Table 2 presents the precision, recall, and F1-score of different classifiers while fingerprinting the operating systems. From the table, we can see that Decision Tree and Random Forest outperforms other classifiers and achieve almost 100% accuracy while identifying the base operating systems.

Table 3 presents the accuracy of the classifiers while labeling the dataset in four different ways:

- **All OS versions**: the classifiers naturally performs worst while detecting the OS versions as we know in most cases there is no change in the basic TCP/IP implementation for these OS kernels.
- **Win versions, Ubuntu, macOS**: here, I consider Windows versions (7,8,Vista, and 10), however labeling all Ubuntu versions as "Ubuntu". The achieved accuracy slightly improves over the achieved accuracy while considering all versions.
- **Ubuntu Versions, Win, macOS**: here, I consider Ubuntu versions (12,14.4, and 16.4), however labeling all Windows versions as "Windows". The achieved accuracy is a lot higher (over 90%) than the achieved accuracy while considering all versions or Windows versions.
- **Base OS only**: I get almost 100% accuracy while labeling all packets as only the base operating system (Windows, Ubuntu, macOS).

Based on the achieved accuracy, we can conclude that it is more difficult to differentiate between Windows versions rather than differentiating the Ubuntu versions. That means, the TCP/IP stack implementation is almost similar all the way for Windows 7, 8, Vista, and 10. In contrast, there is quite a remarkable difference in the TCP/Ip stack implementation while upgrading Ubuntu to a newer versions.

5 CONCLUSION AND FUTURE WORKS

In this work, we see machine learning is quite useful while fingerprinting particular operating systems. The primary observation is that it is always better to classify base operating systems rather than classifying exact versions as it can provide as the latter can provide many false positives or false negative results. Without hyperparameters tuning, Decision Tree and Random Forest classifiers provides the best accuracy while identifying operating systems.

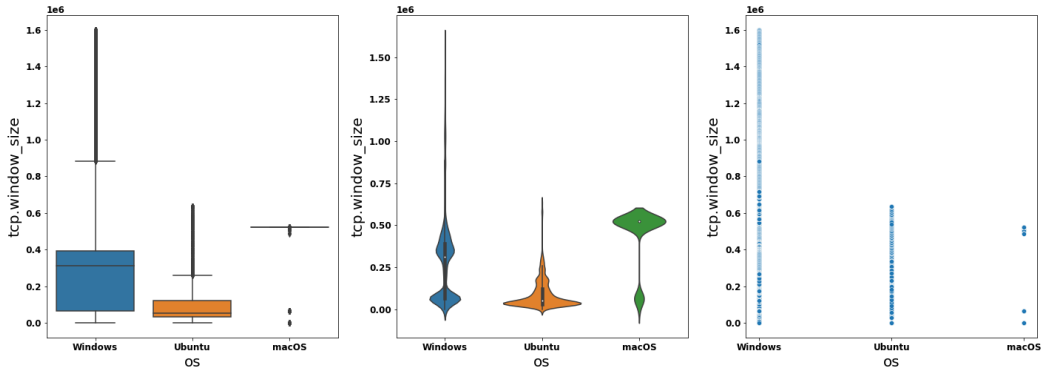


Figure 2: TCP Window Size

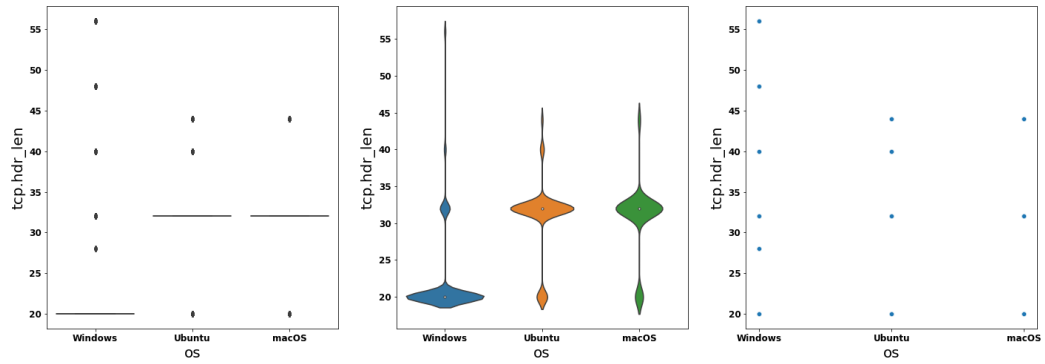


Figure 3: TCP Header Length

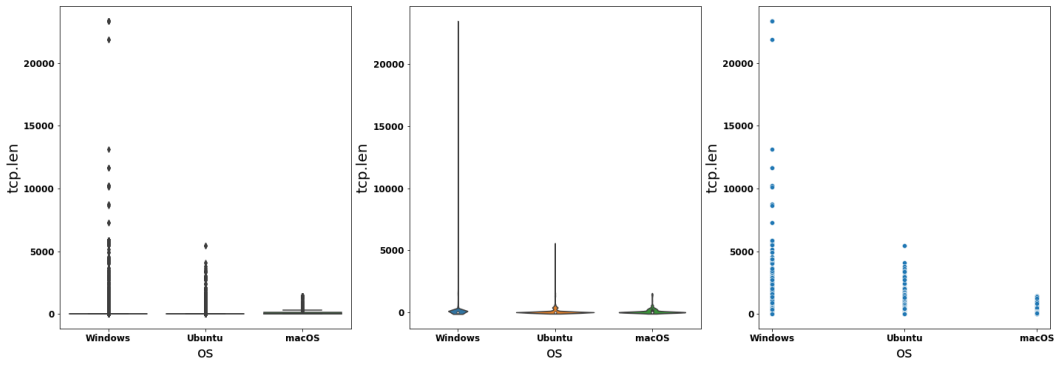


Figure 4: TCP Length

In future, I plan to collect network packets of mobile OSes (Android and IOS) to see how that works. In addition to that, I plan to use deep learning to classify the OSes as well using MLP and LSTM classifiers.

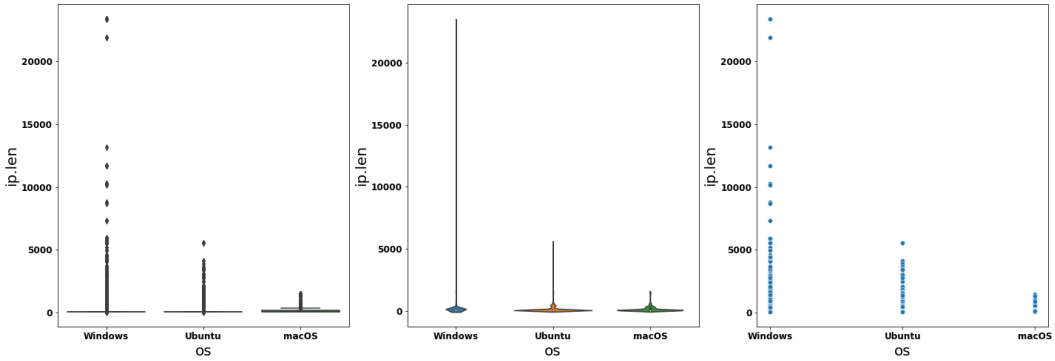


Figure 5: IP Length

Table 2: Performance of Different Classifiers for OS Fingerprinting

	precision						recall						f1-score					
OS/ Classifiers	**LR**	**KNN**	**SVM**	**NB**	**DT**	**RF**	**LR**	**KNN**	**SVM**	**NB**	**DT**	**RF**	**LR**	**KNN**	**SVM**	**NB**	**DT**	**RF**
Ubuntu	0.97	1	0.98	0.97	1	1	0.99	1	1	0.94	1	1	0.98	1	0.99	0.96	1	1
Windows	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
macOS	0.93	0.98	0.98	0.75	1	0.99	0.87	0.99	0.89	0.86	1	1	0.9	0.98	0.93	0.8	1	1

Table 3: Accuracy for different Labeling (Base OS vs OS Versions)

	Accuracy (Approximate)					
Labeling/ Classifiers	**LR**	**KNN**	**SVM**	**NB**	**DT**	**RF**
All OS Versions	63%	85%	74%	51%	91%	90%
Win versions, Ubuntu, macOS	63%	86%	75%	58%	92%	91%
Ubuntu Versions, Win, macOS	98.46%	99.17%	98.63%	91.53%	99.72%	99.65%
Base OS only	99.43%	99.91%	99.6%	98.72%	100%	99.98%

REFERENCES

[1] [n.d.]. IDS 2017 | Datasets | Research | Canadian Institute for Cybersecurity | UNB. https://www.unb.ca/cic/datasets/ids-2017.html. (Accessed on 05/01/2021).

[2] Assaf Dahan. 2017. Operation Cobalt Kitty. Cybereason, https://cdn2.hubspot.net/hubfs/3354902/Cybereason%20Labs%20Analysis%20Operation%20Cobalt%20Kitty.pdf.

[3] Balaji Ganesan. 2004. *TCP/IP stack fingerprinting for patch detection in a distributed Windows environment.* Master's thesis. West Virginia University.

[4] Desta Haileselassie Hagos, Martin Løland, Anis Yazidi, Øivind Kure, and Paal E Engelstad. 2020. Advanced Passive Operating System Fingerprinting Using Machine Learning and Deep Learning. In *2020 29th International Conference on Computer Communications and Networks (ICCCN)*. IEEE, 1–11.

[5] Desta Haileselassie Hagos, Anis Yazidi, Øivind Kure, and Paal E Engelstad. 2020. A Machine Learning-based Tool for Passive OS Fingerprinting with TCP Variant as a Novel Feature. *IEEE Internet of Things Journal* (2020).

[6] Jinho Song, ChaeHo Cho, and Yoojae Won. 2019. Analysis of operating system identification via fingerprinting and machine learning. *Computers & Electrical Engineering* 78 (2019), 1–10.

A APPENDIX

A.1 Feature Selection

```
##############################
####### f_classif, chi2 ######
##############################

Feature          Score
ip.hdr_len       nan
ip.flags.rb      nan
ip.flags.df      nan
ip.flags.mf      nan
ip.frag_offset   nan
ip.ttl           inf
tcp.hdr_len      7921.654399363424
tcp.ack          1858.7058726039422
tcp.flags.push   578.4962673016072
tcp.seq          168.18967000816457
tcp.flags.ack    88.44752170371562
tcp.flags.reset  60.42841951134094
tcp.flags.syn    32.62172871161581
tcp.flags.fin    17.276021320268978
ip.len           13.263547401719991
tcp.len          6.8090954402126
tcp.flags.urg    nan
tcp.flags.cwr    nan
tcp.window_size  2145.669002838123
tcp.urgent_pointer nan

Feature          Score
ip.flags.rb      nan
ip.flags.mf      nan
ip.frag_offset   nan
tcp.ack          25275293139.172764
tcp.seq          7182603.694913036
ip.ttl           244888.86595956332
ip.len           53387.914239702135
tcp.len          42262.466675598946
tcp.hdr_len      22747.661397528627
tcp.flags.push   973.2027209183278
tcp.flags.reset  119.9386965936998
tcp.flags.syn    63.02861453125354
tcp.flags.fin    33.70395901070399
tcp.flags.ack    6.138201995570768
ip.hdr_len       0.0
ip.flags.df      0.0
tcp.flags.urg    nan
tcp.flags.cwr    nan
tcp.window_size  1039563734.5629808
tcp.urgent_pointer nan
```

```
##############################
############# RFE ############
##############################
Feature           Support
ip.hdr_len        1
ip.flags.rb       0
ip.flags.df       1
ip.flags.mf       0
ip.frag_offset    0
ip.ttl            1
ip.len            1
tcp.seq           1
tcp.ack           1
tcp.len           1
tcp.hdr_len       1
tcp.flags.fin     0
tcp.flags.syn     0
tcp.flags.reset   0
tcp.flags.push    1
tcp.flags.ack     1
tcp.flags.urg     0
tcp.flags.cwr     0
tcp.window_size   0
tcp.urgent_pointer 0

Feature           Rank
ip.hdr_len        1
ip.flags.df       1
ip.ttl            1
ip.len            1
tcp.seq           1
tcp.ack           1
tcp.len           1
tcp.hdr_len       1
tcp.flags.push    1
tcp.flags.ack     1
tcp.window_size   2
tcp.flags.syn     3
tcp.flags.fin     4
tcp.flags.reset   5
tcp.flags.cwr     6
tcp.flags.urg     7
ip.frag_offset    8
ip.flags.mf       9
ip.flags.rb       10
tcp.urgent_pointer 11

##############################
#### ExtraTreesClassifier ####
##############################
Feature           Importance
```

```
ip.ttl             0.7130620664096162
tcp.window_size    0.12035736760824285
tcp.hdr_len        0.08655425685285494
tcp.ack            0.032291006943969844
ip.len             0.015774823356295112
tcp.seq            0.015221847797222635
tcp.flags.push     0.006592398775936251
tcp.len            0.0029166163290636994
tcp.flags.ack      0.0026267480400964656
tcp.flags.syn      0.002163405515025841
tcp.flags.reset    0.0013875724350276468
tcp.flags.fin      0.0010518899366486006
ip.hdr_len         0.0
ip.flags.rb        0.0
ip.flags.df        0.0
ip.flags.mf        0.0
ip.frag_offset     0.0
tcp.flags.urg      0.0
tcp.flags.cwr      0.0
tcp.urgent_pointer 0.0
```

A.2 Classification Reports (Considering Windows Versions Only)

```
Total number of packets:  48962

### Logistic Regression Classifier ###
Classification Report:
              precision    recall  f1-score   support

      Ubuntu       0.97      0.98      0.98      1424
      Win 10       0.57      0.97      0.72      4536
       Win 7       0.38      0.10      0.16      1368
     Win 8.1       0.50      0.00      0.00      1872
   Win Vista       0.75      0.07      0.13       300
       macOS       0.91      0.87      0.89       293

    accuracy                           0.64      9793
   macro avg       0.68      0.50      0.48      9793
weighted avg       0.61      0.64      0.53      9793


Confusion Matrix:
[[1400    0    0    0    0   24]
 [   0 4414  120    1    1    0]
 [   0 1224  139    0    5    0]
 [   0 1798   72    1    1    0]
 [   0  243   36    0   21    0]
 [  38    0    0    0    0  255]]

Precision:  63.6168691922802 %


### K-Neighbors Classifier ###
Classification Report:
              precision    recall  f1-score   support

      Ubuntu       1.00      1.00      1.00      1424
      Win 10       0.89      0.91      0.90      4536
       Win 7       0.69      0.76      0.73      1368
     Win 8.1       0.85      0.78      0.82      1872
   Win Vista       0.71      0.42      0.53       300
       macOS       0.98      0.99      0.98       293

    accuracy                           0.87      9793
   macro avg       0.85      0.81      0.83      9793
weighted avg       0.87      0.87      0.86      9793


Confusion Matrix:
[[1418    0    0    0    0    6]
 [   0 4147  242  125   22    0]
 [   0  218 1040   94   16    0]
 [   0  239  153 1468   12    0]
```

```
 [   0   75   62   38  125    0]
 [   3    0    0    0    0  290]]

Precision:  86.67415500867966 %


### Support Vector Classifier (linear) ###
Classification Report:
              precision    recall  f1-score   support

      Ubuntu       0.97      0.99      0.98      1424
      Win 10       0.56      1.00      0.72      4536
       Win 7       0.00      0.00      0.00      1368
     Win 8.1       0.00      0.00      0.00      1872
   Win Vista       0.00      0.00      0.00       300
       macOS       0.96      0.87      0.91       293

    accuracy                           0.63      9793
   macro avg       0.42      0.48      0.44      9793
weighted avg       0.43      0.63      0.50      9793


Confusion Matrix:
[[1413    0    0    0    0   11]
 [   0 4536    0    0    0    0]
 [   0 1368    0    0    0    0]
 [   0 1872    0    0    0    0]
 [   0  300    0    0    0    0]
 [  38    0    0    0    0  255]]

Precision:  63.351373430001026 %


### Support Vector Classifier (rbf) ###
Classification Report:
              precision    recall  f1-score   support

      Ubuntu       0.98      1.00      0.99      1424
      Win 10       0.66      0.98      0.79      4536
       Win 7       0.77      0.19      0.31      1368
     Win 8.1       0.87      0.47      0.61      1872
   Win Vista       1.00      0.15      0.26       300
       macOS       0.98      0.89      0.93       293

    accuracy                           0.75      9793
   macro avg       0.88      0.61      0.65      9793
weighted avg       0.78      0.75      0.71      9793


Confusion Matrix:
[[1418    0    0    0    0    6]
 [   0 4426   20   90    0    0]
```

```
 [    0 1065   266    37     0     0]
 [    0  930    61   881     0     0]
 [    0  254     0     1    45     0]
 [   33    0     0     0     0   260]]

Precision:  74.50219544572654 %


### Naive Bayes Classifier ###
Classification Report:
              precision    recall  f1-score   support

      Ubuntu       0.97      0.94      0.96      1424
      Win 10       0.61      0.82      0.70      4536
       Win 7       0.31      0.14      0.19      1368
     Win 8.1       0.30      0.04      0.07      1872
   Win Vista       0.10      0.37      0.15       300
       macOS       0.75      0.86      0.80       293

    accuracy                           0.58      9793
   macro avg       0.51      0.53      0.48      9793
weighted avg       0.55      0.58      0.53      9793


Confusion Matrix:
[[1339    0    0    0    0   85]
 [    0 3707  195  116  518    0]
 [    0  852  186   47  283    0]
 [    0 1403  152   76  241    0]
 [    0  116   62   11  111    0]
 [   40    0    0    0    0  253]]

Precision:  57.918921678750124 %


### Decision Tree Classifier ###
Classification Report:
              precision    recall  f1-score   support

      Ubuntu       1.00      1.00      1.00      1424
      Win 10       0.91      0.96      0.94      4536
       Win 7       0.86      0.80      0.83      1368
     Win 8.1       0.90      0.86      0.88      1872
   Win Vista       0.83      0.61      0.70       300
       macOS       1.00      1.00      1.00       293

    accuracy                           0.92      9793
   macro avg       0.92      0.87      0.89      9793
weighted avg       0.92      0.92      0.92      9793


Confusion Matrix:
```

```
[[1424    0    0    0    0    0]
 [   0 4377   74   76    9    0]
 [   0  173 1099   82   14    0]
 [   0  177   73 1608   14    0]
 [   0   70   25   23  182    0]
 [   0    0    0    0    0  293]]

Precision:  91.72878586745634 %


### Random Forest Classifier ###
Classification Report:
              precision    recall  f1-score   support

      Ubuntu       1.00      1.00      1.00      1424
      Win 10       0.90      0.96      0.93      4536
       Win 7       0.85      0.77      0.81      1368
     Win 8.1       0.89      0.84      0.86      1872
   Win Vista       0.82      0.57      0.67       300
       macOS       0.99      0.99      0.99       293

    accuracy                           0.91      9793
   macro avg       0.91      0.85      0.88      9793
weighted avg       0.90      0.91      0.90      9793


Confusion Matrix:
[[1422    0    0    0    0    2]
 [   0 4365   80   83    8    0]
 [   0  222 1048   83   15    0]
 [   0  208   81 1568   15    0]
 [   0   77   19   34  170    0]
 [   2    0    0    0    0  291]]

Precision:  90.51363218625549 %
```

A.3 Classification Reports (Ubuntu Versions Only)

```
Total number of packets:  48962

### Logistic Regression Classifier ###
Classification Report:
                  precision    recall  f1-score   support

     Ubuntu 14.4       0.91      0.99      0.95      1329
     Ubuntu 16.4       0.00      0.00      0.00        80
Ubuntu server 12       0.00      0.00      0.00        15
         Windows       1.00      1.00      1.00      8076
           macOS       0.93      0.87      0.90       293

        accuracy                           0.98      9793
       macro avg       0.57      0.57      0.57      9793
    weighted avg       0.98      0.98      0.98      9793


Confusion Matrix:
[[1311    0    0    0   18]
 [  80    0    0    0    0]
 [  15    0    0    0    0]
 [   0    0    0 8076    0]
 [  38    0    0    0  255]]

Precision:  98.45808230368631 %


### K-Neighbors Classifier ###
Classification Report:
                  precision    recall  f1-score   support

     Ubuntu 14.4       0.97      0.98      0.97      1329
     Ubuntu 16.4       0.67      0.50      0.57        80
Ubuntu server 12       0.47      0.53      0.50        15
         Windows       1.00      1.00      1.00      8076
           macOS       0.98      0.99      0.98       293

        accuracy                           0.99      9793
       macro avg       0.82      0.80      0.81      9793
    weighted avg       0.99      0.99      0.99      9793


Confusion Matrix:
[[1298   19    6    0    6]
 [  37   40    3    0    0]
 [   6    1    8    0    0]
 [   0    0    0 8076    0]
 [   3    0    0    0  290]]

Precision:  99.17287858674564 %
```

```
### Support Vector Classifier (linear) ###
Classification Report:
  _warn_prf(average, modifier, msg_start, len(result))
                 precision    recall  f1-score   support

     Ubuntu 14.4       0.91      1.00      0.95      1329
     Ubuntu 16.4       0.00      0.00      0.00        80
Ubuntu server 12       0.00      0.00      0.00        15
         Windows       1.00      1.00      1.00      8076
           macOS       0.98      0.87      0.92       293

        accuracy                           0.99      9793
       macro avg       0.58      0.57      0.57      9793
    weighted avg       0.98      0.99      0.98      9793


Confusion Matrix:
[[1324    0    0    0    5]
 [  80    0    0    0    0]
 [  15    0    0    0    0]
 [   0    0    0 8076    0]
 [  38    0    0    0  255]]

Precision:  98.59083018482589 %


### Support Vector Classifier (rbf) ###
Classification Report:
                 precision    recall  f1-score   support

     Ubuntu 14.4       0.91      1.00      0.95      1329
     Ubuntu 16.4       0.00      0.00      0.00        80
Ubuntu server 12       0.00      0.00      0.00        15
         Windows       1.00      1.00      1.00      8076
           macOS       0.98      0.89      0.93       293

        accuracy                           0.99      9793
       macro avg       0.58      0.58      0.58      9793
    weighted avg       0.98      0.99      0.98      9793


Confusion Matrix:
[[1323    0    0    0    6]
 [  80    0    0    0    0]
 [  15    0    0    0    0]
 [   0    0    0 8076    0]
 [  33    0    0    0  260]]

Precision:  98.631675686715 %
```

```
### Naive Bayes Classifier ###
Classification Report:
                  precision    recall  f1-score   support

     Ubuntu 14.4       0.94      0.43      0.59      1329
     Ubuntu 16.4       0.12      0.75      0.21        80
Ubuntu server 12       0.04      0.80      0.07        15
         Windows       1.00      1.00      1.00      8076
           macOS       0.91      0.85      0.88       293

        accuracy                           0.92      9793
       macro avg       0.60      0.77      0.55      9793
    weighted avg       0.98      0.92      0.93      9793


Confusion Matrix:
[[ 567  429  307    0   26]
 [   0   60   20    0    0]
 [   0    3   12    0    0]
 [   0    0    0 8076    0]
 [  38    6    0    0  249]]

Precision:  91.5347697334831 %


### Decision Tree Classifier ###
Classification Report:
                  precision    recall  f1-score   support

     Ubuntu 14.4       0.99      0.99      0.99      1329
     Ubuntu 16.4       0.87      0.86      0.87        80
Ubuntu server 12       0.92      0.73      0.81        15
         Windows       1.00      1.00      1.00      8076
           macOS       1.00      1.00      1.00       293

        accuracy                           1.00      9793
       macro avg       0.96      0.92      0.93      9793
    weighted avg       1.00      1.00      1.00      9793


Confusion Matrix:
[[1318   10    1    0    0]
 [  11   69    0    0    0]
 [   4    0   11    0    0]
 [   0    0    0 8076    0]
 [   1    0    0    0  292]]

Precision:  99.72429286224855 %


### Random Forest Classifier ###
```

```
Classification Report:
                    precision    recall  f1-score   support

      Ubuntu 14.4       0.98      0.99      0.99      1329
      Ubuntu 16.4       0.90      0.79      0.84        80
Ubuntu server 12        0.92      0.73      0.81        15
          Windows       1.00      1.00      1.00      8076
            macOS       0.99      0.99      0.99       293

         accuracy                           1.00      9793
        macro avg       0.96      0.90      0.93      9793
     weighted avg       1.00      1.00      1.00      9793


Confusion Matrix:
[[1319    7    1    0    2]
 [  17   63    0    0    0]
 [   4    0   11    0    0]
 [   0    0    0 8076    0]
 [   3    0    0    0  290]]

Precision:  99.65281323394262 %
```

A.4 Classification Reports (All OS Versions)

```
Total number of packets:  48962


### Logistic Regression Classifier ###
Classification Report:
                  precision    recall  f1-score   support

     Ubuntu 14.4       0.91      0.98      0.94      1329
     Ubuntu 16.4       0.00      0.00      0.00        80
Ubuntu server 12       0.00      0.00      0.00        15
          Win 10       0.57      0.97      0.72      4536
           Win 7       0.38      0.10      0.16      1368
         Win 8.1       0.50      0.00      0.00      1872
       Win Vista       0.75      0.07      0.13       300
           macOS       0.91      0.87      0.89       293

        accuracy                           0.63      9793
       macro avg       0.50      0.37      0.36      9793
    weighted avg       0.59      0.63      0.52      9793


Confusion Matrix:
[[1304    0    0    0    0    0    0   25]
 [  80    0    0    0    0    0    0    0]
 [  15    0    0    0    0    0    0    0]
 [   0    0    0 4413  121    1    1    0]
 [   0    0    0 1224  139    0    5    0]
 [   0    0    0 1798   72    1    1    0]
 [   0    0    0  243   36    0   21    0]
 [  38    0    0    0    0    0    0  255]]

Precision:  62.626365771469416 %


### K-Neighbors Classifier ###
Classification Report:
                  precision    recall  f1-score   support

     Ubuntu 14.4       0.97      0.98      0.97      1329
     Ubuntu 16.4       0.67      0.50      0.57        80
Ubuntu server 12       0.47      0.53      0.50        15
          Win 10       0.89      0.91      0.90      4536
           Win 7       0.69      0.76      0.73      1368
         Win 8.1       0.85      0.78      0.82      1872
       Win Vista       0.71      0.42      0.53       300
           macOS       0.98      0.99      0.98       293

        accuracy                           0.86      9793
       macro avg       0.78      0.73      0.75      9793
    weighted avg       0.86      0.86      0.86      9793
```

```
Confusion Matrix:
[[1298   19    6    0    0    0    0    6]
 [  37   40    3    0    0    0    0    0]
 [   6    1    8    0    0    0    0    0]
 [   0    0    0 4147  242  125   22    0]
 [   0    0    0  218 1040   94   16    0]
 [   0    0    0  239  153 1468   12    0]
 [   0    0    0   75   62   38  125    0]
 [   3    0    0    0    0    0    0  290]]

Precision:  85.93893597467579 %


### Support Vector Classifier (linear) ###
Classification Report:
                  precision    recall  f1-score   support

     Ubuntu 14.4       0.91      1.00      0.95      1329
     Ubuntu 16.4       0.00      0.00      0.00        80
Ubuntu server 12       0.00      0.00      0.00        15
          Win 10       0.56      1.00      0.72      4536
           Win 7       0.00      0.00      0.00      1368
         Win 8.1       0.00      0.00      0.00      1872
       Win Vista       0.00      0.00      0.00       300
           macOS       0.98      0.87      0.92       293

        accuracy                           0.62      9793
       macro avg       0.31      0.36      0.32      9793
    weighted avg       0.41      0.62      0.49      9793


Confusion Matrix:
[[1324    0    0    0    0    0    0    5]
 [  80    0    0    0    0    0    0    0]
 [  15    0    0    0    0    0    0    0]
 [   0    0    0 4536    0    0    0    0]
 [   0    0    0 1368    0    0    0    0]
 [   0    0    0 1872    0    0    0    0]
 [   0    0    0  300    0    0    0    0]
 [  38    0    0    0    0    0    0  255]]

Precision:  62.44256101296845 %


### Support Vector Classifier (rbf) ###
Classification Report:
                  precision    recall  f1-score   support

     Ubuntu 14.4       0.91      1.00      0.95      1329
     Ubuntu 16.4       0.00      0.00      0.00        80
```

```
Ubuntu server 12       0.00      0.00      0.00        15
          Win 10       0.66      0.98      0.79      4536
           Win 7       0.77      0.19      0.31      1368
         Win 8.1       0.87      0.47      0.61      1872
       Win Vista       1.00      0.15      0.26       300
           macOS       0.98      0.89      0.93       293

        accuracy                           0.74      9793
       macro avg       0.65      0.46      0.48      9793
    weighted avg       0.76      0.74      0.69      9793


Confusion Matrix:
[[1323    0    0    0    0    0    0    6]
 [  80    0    0    0    0    0    0    0]
 [  15    0    0    0    0    0    0    0]
 [   0    0    0 4426   20   90    0    0]
 [   0    0    0 1065  266   37    0    0]
 [   0    0    0  930   61  881    0    0]
 [   0    0    0  254    0    1   45    0]
 [  33    0    0    0    0    0    0  260]]

Precision:  73.53211477586031 %


### Naive Bayes Classifier ###
Classification Report:
                   precision    recall  f1-score   support

     Ubuntu 14.4       0.94      0.43      0.59      1329
     Ubuntu 16.4       0.12      0.75      0.21        80
Ubuntu server 12       0.04      0.80      0.07        15
          Win 10       0.61      0.82      0.70      4536
           Win 7       0.31      0.14      0.19      1368
         Win 8.1       0.30      0.04      0.07      1872
       Win Vista       0.10      0.37      0.15       300
           macOS       0.91      0.85      0.88       293

        accuracy                           0.51      9793
       macro avg       0.42      0.52      0.36      9793
    weighted avg       0.54      0.51      0.48      9793


Confusion Matrix:
[[ 567  429  307    0    0    0    0   26]
 [   0   60   20    0    0    0    0    0]
 [   0    3   12    0    0    0    0    0]
 [   0    0    0 3707  195  116  518    0]
 [   0    0    0  852  186   47  283    0]
 [   0    0    0 1403  152   76  241    0]
 [   0    0    0  116   62   11  111    0]
 [  38    6    0    0    0    0    0  249]]
```

```
Precision:  50.73011334626775 %


### Decision Tree Classifier ###
Classification Report:
                  precision    recall  f1-score   support

     Ubuntu 14.4       0.99      0.99      0.99      1329
     Ubuntu 16.4       0.90      0.86      0.88        80
Ubuntu server 12       0.92      0.73      0.81        15
          Win 10       0.91      0.96      0.94      4536
           Win 7       0.86      0.80      0.83      1368
         Win 8.1       0.90      0.86      0.88      1872
       Win Vista       0.83      0.61      0.70       300
           macOS       1.00      1.00      1.00       293

        accuracy                           0.91      9793
       macro avg       0.91      0.85      0.88      9793
    weighted avg       0.91      0.91      0.91      9793


Confusion Matrix:
[[1320    8    1    0    0    0    0    0]
 [  11   69    0    0    0    0    0    0]
 [   4    0   11    0    0    0    0    0]
 [   0    0    0 4372   79   75   10    0]
 [   0    0    0  173 1101   82   12    0]
 [   0    0    0  177   75 1606   14    0]
 [   0    0    0   70   25   23  182    0]
 [   1    0    0    0    0    0    0  292]]

Precision:  91.42244460328807 %


### Random Forest Classifier ###
Classification Report:
                  precision    recall  f1-score   support

     Ubuntu 14.4       0.99      0.99      0.99      1329
     Ubuntu 16.4       0.88      0.84      0.86        80
Ubuntu server 12       0.92      0.73      0.81        15
          Win 10       0.90      0.96      0.93      4536
           Win 7       0.85      0.77      0.81      1368
         Win 8.1       0.89      0.83      0.86      1872
       Win Vista       0.80      0.56      0.66       300
           macOS       1.00      1.00      1.00       293

        accuracy                           0.90      9793
       macro avg       0.90      0.84      0.86      9793
    weighted avg       0.90      0.90      0.90      9793
```

```
Confusion Matrix:
[[1319    9    1    0    0    0    0    0]
 [  13   67    0    0    0    0    0    0]
 [   4    0   11    0    0    0    0    0]
 [   0    0    0 4364   78   81   13    0]
 [   0    0    0  223 1048   86   11    0]
 [   0    0    0  216   78 1560   18    0]
 [   0    0    0   71   31   30  168    0]
 [   0    0    0    0    0    0    0  293]]

Precision:  90.1664454201981 %
```

A.5 Classification Reports (Base OS only)

```
Total number of packets:  48962


### Logistic Regression Classifier ###
Classification Report:
              precision    recall  f1-score   support

      Ubuntu       0.97      0.99      0.98      1424
     Windows       1.00      1.00      1.00      8076
       macOS       0.93      0.87      0.90       293

    accuracy                           0.99      9793
   macro avg       0.97      0.95      0.96      9793
weighted avg       0.99      0.99      0.99      9793


Confusion Matrix:
[[1406    0   18]
 [   0 8076    0]
 [  38    0  255]]

Precision:  99.42816297355253 %


### K-Neighbors Classifier ###
Classification Report:
              precision    recall  f1-score   support

      Ubuntu       1.00      1.00      1.00      1424
     Windows       1.00      1.00      1.00      8076
       macOS       0.98      0.99      0.98       293

    accuracy                           1.00      9793
   macro avg       0.99      1.00      0.99      9793
weighted avg       1.00      1.00      1.00      9793


Confusion Matrix:
[[1418    0    6]
 [   0 8076    0]
 [   3    0  290]]

Precision:  99.90809762074952 %


### Support Vector Classifier (linear) ###
Classification Report:
              precision    recall  f1-score   support

      Ubuntu       0.97      0.99      0.98      1424
```

```
      Windows       1.00      1.00      1.00      8076
        macOS       0.96      0.87      0.91       293

     accuracy                           0.99      9793
    macro avg       0.98      0.95      0.97      9793
weighted avg       0.99      0.99      0.99      9793


Confusion Matrix:
[[1413    0   11]
 [   0 8076    0]
 [  38    0  255]]

Precision:  99.49964260185847 %


### Support Vector Classifier (rbf) ###
Classification Report:
              precision    recall  f1-score   support

      Ubuntu       0.98      1.00      0.99      1424
     Windows       1.00      1.00      1.00      8076
       macOS       0.98      0.89      0.93       293

    accuracy                           1.00      9793
   macro avg       0.98      0.96      0.97      9793
weighted avg       1.00      1.00      1.00      9793


Confusion Matrix:
[[1418    0    6]
 [   0 8076    0]
 [  33    0  260]]

Precision:  99.60175635658123 %


### Naive Bayes Classifier ###
Classification Report:
              precision    recall  f1-score   support

      Ubuntu       0.97      0.94      0.96      1424
     Windows       1.00      1.00      1.00      8076
       macOS       0.75      0.86      0.80       293

    accuracy                           0.99      9793
   macro avg       0.91      0.93      0.92      9793
weighted avg       0.99      0.99      0.99      9793


Confusion Matrix:
[[1339    0   85]
```

```
 [    0 8076     0]
 [   40     0   253]]

Precision:  98.72357806596548 %


### Decision Tree Classifier ###
Classification Report:
              precision    recall  f1-score   support

      Ubuntu       1.00      1.00      1.00      1424
     Windows       1.00      1.00      1.00      8076
       macOS       1.00      1.00      1.00       293

    accuracy                           1.00      9793
   macro avg       1.00      1.00      1.00      9793
weighted avg       1.00      1.00      1.00      9793


Confusion Matrix:
[[1424     0     0]
 [    0 8076     0]
 [    0     0   293]]

Precision:  100.0 %


### Random Forest Classifier ###
Classification Report:
              precision    recall  f1-score   support

      Ubuntu       1.00      1.00      1.00      1424
     Windows       1.00      1.00      1.00      8076
       macOS       0.99      1.00      1.00       293

    accuracy                           1.00      9793
   macro avg       1.00      1.00      1.00      9793
weighted avg       1.00      1.00      1.00      9793


Confusion Matrix:
[[1422     0     2]
 [    0 8076     0]
 [    0     0   293]]

Precision:  99.97957724905545 %
```

A.6 PCAP to CSV

Used code to convert pcap to CSV file.

```
tshark -r thursday.pcap -T fields -E header=y -E separator=, -E quote=d -E occurrence=f \
-e ip.version -e ip.hdr_len -e ip.tos -e ip.id -e ip.flags -e ip.flags.rb -e ip.flags.df \
-e ip.flags.mf -e ip.frag_offset -e ip.ttl -e ip.proto -e ip.checksum -e ip.src -e ip.dst \
-e ip.len -e ip.dsfield -e tcp.srcport -e tcp.dstport -e tcp.seq -e tcp.ack -e tcp.len \
-e tcp.hdr_len -e tcp.flags -e tcp.flags.fin -e tcp.flags.syn -e tcp.flags.reset \
-e tcp.flags.push -e tcp.flags.ack -e tcp.flags.urg -e tcp.flags.cwr -e tcp.window_size \
-e tcp.checksum -e tcp.urgent_pointer -e tcp.options.mss_val > thursday.csv
```