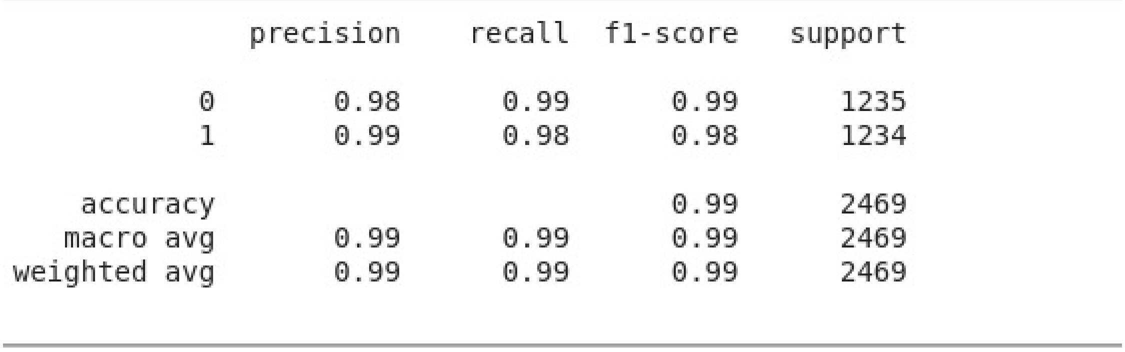
HACKIITK2020-Round-1

1. **Static Malware Analysis:**
   We considered 11 DLLs; 97 function calls mostly used by malware
   We used Random Forest Classifier and achieved the following:

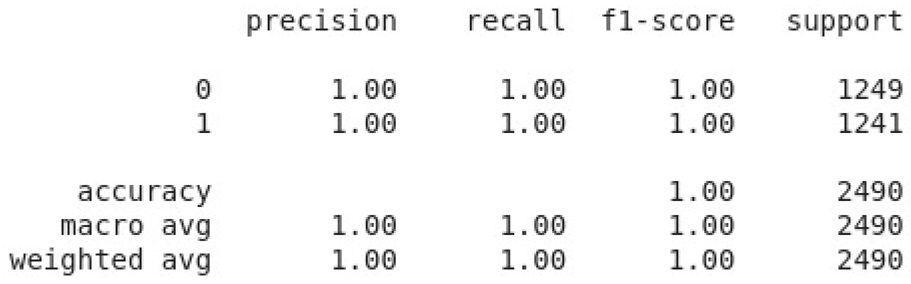


```
              precision    recall  f1-score   support

           0       0.98      0.99      0.99      1235
           1       0.99      0.98      0.98      1234

    accuracy                           0.99      2469
   macro avg       0.99      0.99      0.99      2469
weighted avg       0.99      0.99      0.99      2469
```

2. **Dynamic Malware Analysis:**
   We considered 16 features related to files, directories, reg_keys, top 35 file extensions with their modifications, top 257 API calls with hit rate, top 16 API call categories, top 112 cuckoo signatures.
   We used Random Forest Classifier and achieved the following:



```
              precision    recall  f1-score   support

           0       1.00      1.00      1.00      1249
           1       1.00      1.00      1.00      1241

    accuracy                           1.00      2490
   macro avg       1.00      1.00      1.00      2490
weighted avg       1.00      1.00      1.00      2490
```

We built classifiers for static and dynamic analysis respectively.