Table of Contents

Chapter 1: Machine Learning for Cybersecurity

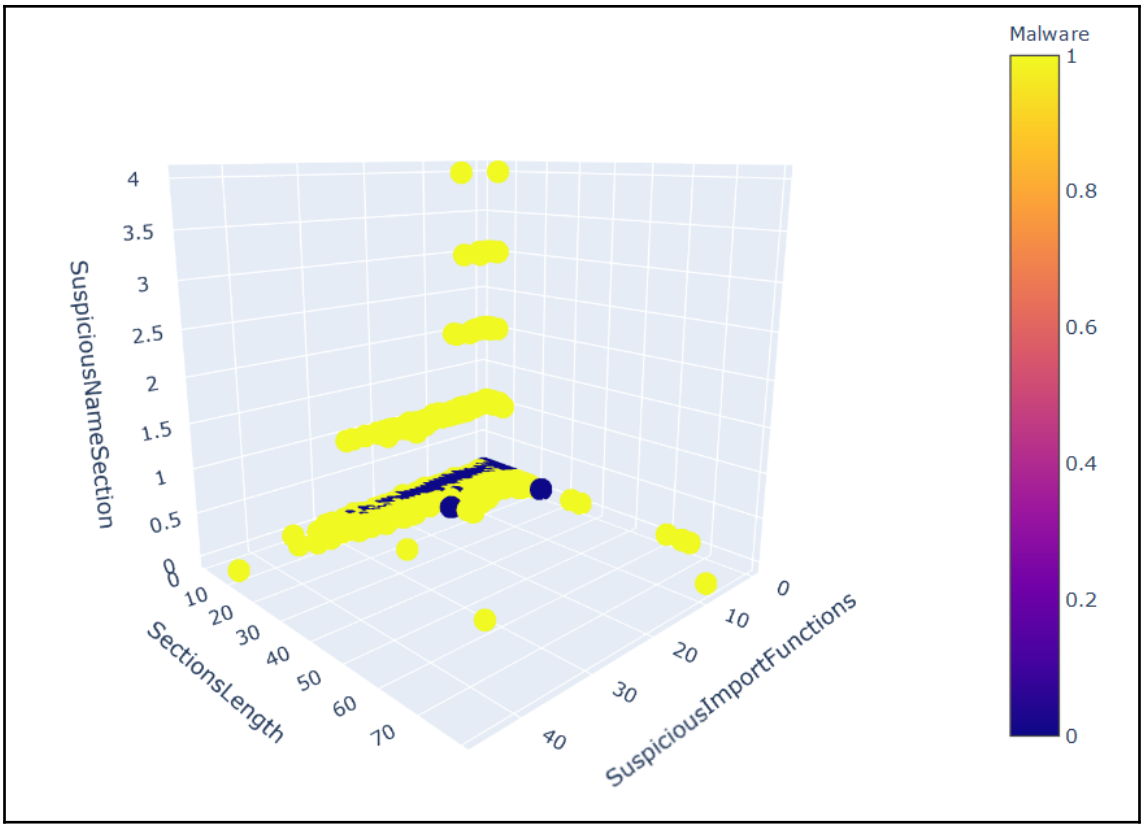
```
print(len(X_train))
print(len(y_train))
print(len(X_val))
print(len(y_val))
print(len(X_test))
print(len(y_test))
```

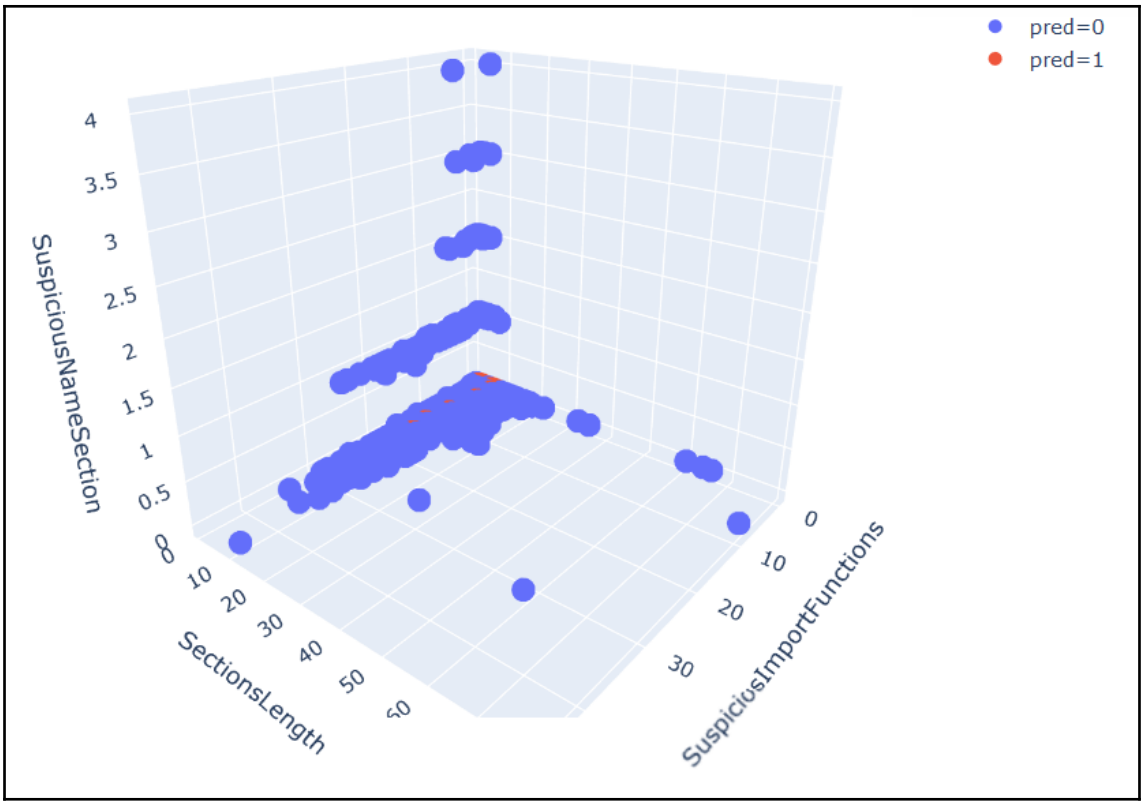
```
81
81
27
27
27
27
```

```
[[2.31170e+04 1.44000e+02 3.00000e+00 ... 7.78240e+04 7.37280e+04
  0.00000e+00]
 [2.31170e+04 1.44000e+02 3.00000e+00 ... 2.94912e+05 0.00000e+00
  3.46112e+05]
 [2.31170e+04 1.44000e+02 3.00000e+00 ... 4.09600e+04 0.00000e+00
  0.00000e+00]
 ...
 [2.31170e+04 0.00000e+00 0.00000e+00 ... 6.14400e+04 0.00000e+00
  0.00000e+00]
 [2.31170e+04 1.44000e+02 3.00000e+00 ... 1.02400e+05 0.00000e+00
  0.00000e+00]
 [2.31170e+04 1.44000e+02 3.00000e+00 ... 5.57056e+05 0.00000e+00
  0.00000e+00]]
```

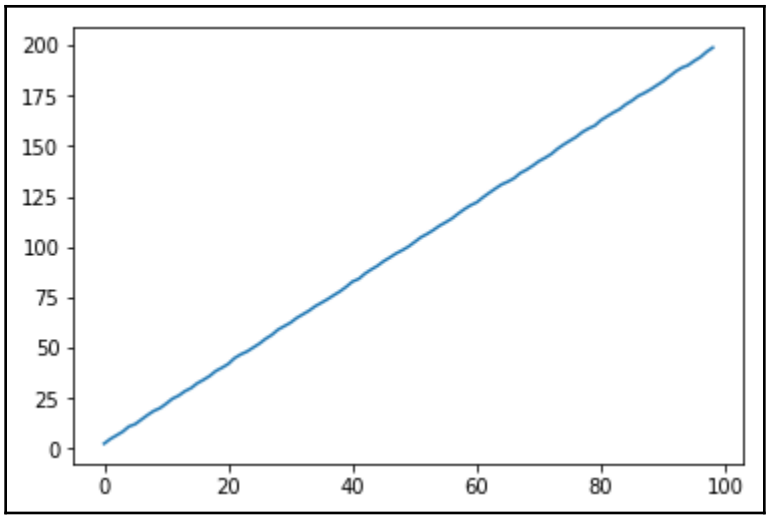
```
[[ 0.         -0.03506542 -0.04751096 ... -0.07054894 -0.0198525
  -0.04066791]
 [ 0.         -0.03506542 -0.04751096 ... -0.03849221 -0.02110877
  -0.02469983]
 [ 0.         -0.03506542 -0.04751096 ... -0.07599254 -0.02110877
  -0.04066791]
 ...
 [ 0.         -0.18093613 -0.04958686 ... -0.07296832 -0.02110877
  -0.04066791]
 [ 0.         -0.03506542 -0.04751096 ... -0.06691988 -0.02110877
  -0.04066791]
 [ 0.         -0.03506542 -0.04751096 ...  0.00021781 -0.02110877
  -0.04066791]]
```

```
[1.13714096e-01 6.04526312e-02 5.35847638e-02 4.95286930e-02
 4.08242868e-02 3.43687925e-02 3.32004002e-02 3.01112226e-02
 2.86901095e-02 2.81624164e-02 2.54807940e-02 2.38845548e-02
 2.22696648e-02 2.05755591e-02 1.82485433e-02 1.73648310e-02
 1.66649078e-02 1.63647194e-02 1.52683994e-02 1.46357930e-02
 1.45790542e-02 1.45535760e-02 1.44699413e-02 1.44154480e-02
 1.42948516e-02 1.39221004e-02 1.35338124e-02 1.33766277e-02
 1.32896667e-02 1.23472302e-02 1.20507834e-02 1.15452214e-02
 1.13731313e-02 1.10939084e-02 1.07062189e-02 1.01649154e-02
 9.90148375e-03 9.61478385e-03 9.17627698e-03 9.04802544e-03
 8.66332999e-03 6.94752252e-03 6.84216033e-03 6.48244001e-03
 5.95005317e-03 5.91335216e-03 5.41615029e-03 5.10640740e-03
 4.83543074e-03 4.45888820e-03 4.29104432e-03 3.82076025e-03
 3.79864324e-03 3.24146447e-03 3.18558571e-03 2.67004617e-03
 2.03201471e-03 1.73591476e-03 1.65758475e-03 1.56708821e-03
 1.38839592e-03 1.20694096e-03 8.20896559e-04 6.92520065e-04
 2.79632267e-04 1.36614783e-04 6.56001071e-06 3.22441346e-07
 1.26534195e-10 5.64125607e-34 5.64125607e-34 5.64125607e-34
 5.64125607e-34 5.64125607e-34 5.64125607e-34 5.64125607e-34
 5.63722303e-34]
```


Malware
1
0.8
0.6
0.4
0.2
0
SuspiciousNameSection
4
3.5
3
2.5
2
1.5
1
0.5
0
SectionsLength
0
10
20
30
40
50
60
70
SuspiciousImportFunctions
0
10
20
30
40



Accuracy: 99.08%


200
175
150
125
100
75
50
25
0
0
20
40
60
80
100

```
from statsmodels.tsa.ar_model import AR

model = AR(time_series)
model_fit = model.fit()
y = model_fit.predict(len(time_series), len(time_series))
print(y)
```

```
[200.46051296]
```

```
model_fit.params
```

```
array([13.52904896,  0.0387842 ,  0.20658747,  0.2626664 , -0.23256276,
        0.1341352 ,  0.13259913,  0.17487147, -0.13811329, -0.02630609,
        0.06267792,  0.13943178,  0.24528964])
```

```
from statsmodels.tsa.arima_model import ARMA

model = ARMA(time_series, order=(0, 1))
model_fit = model.fit(disp=False)
y = model_fit.predict(len(time_series), len(time_series))
print(y)
```

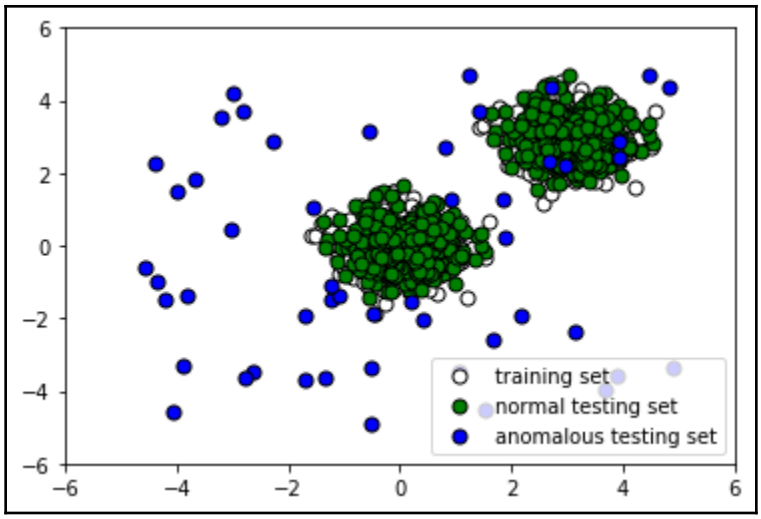
```
[150.594829]
```

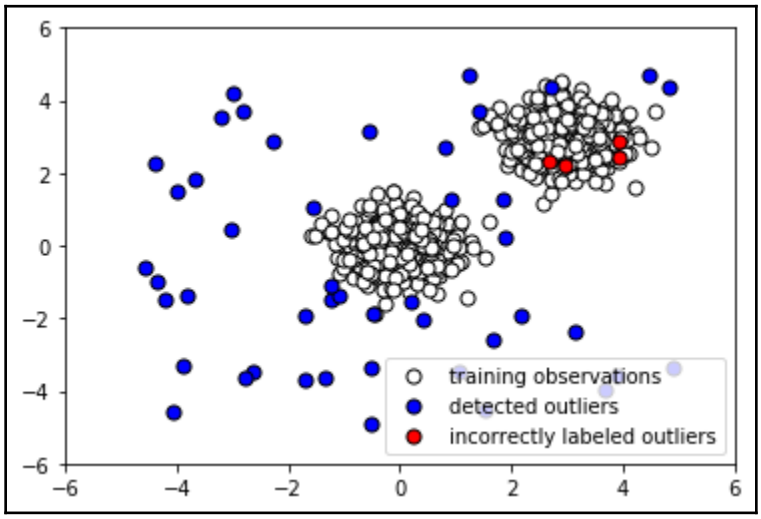
```
model_fit.params
```

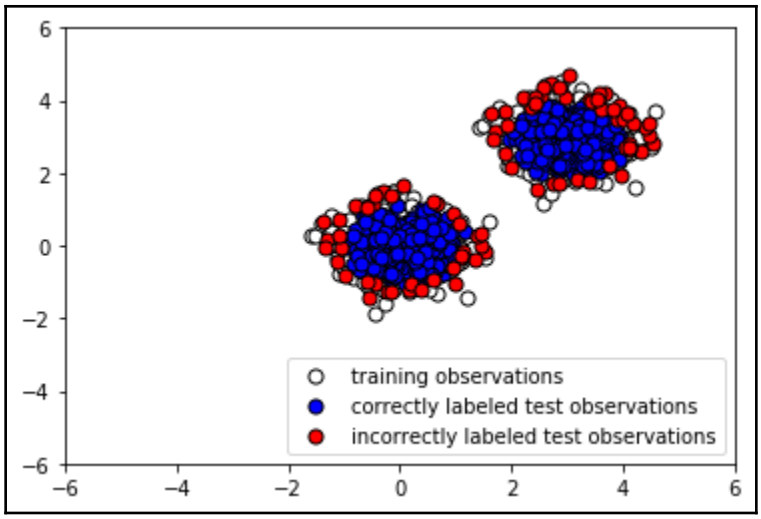
```
array([100.52900385,   0.99994647])
```

```
from statsmodels.tsa.holtwinters import SimpleExpSmoothing

model = SimpleExpSmoothing(time_series)
model_fit = model.fit()
y = model_fit.predict(len(time_series), len(time_series))
print(y)
```

```
[198.58106655]
```


training set
normal testing set
anomalous testing set

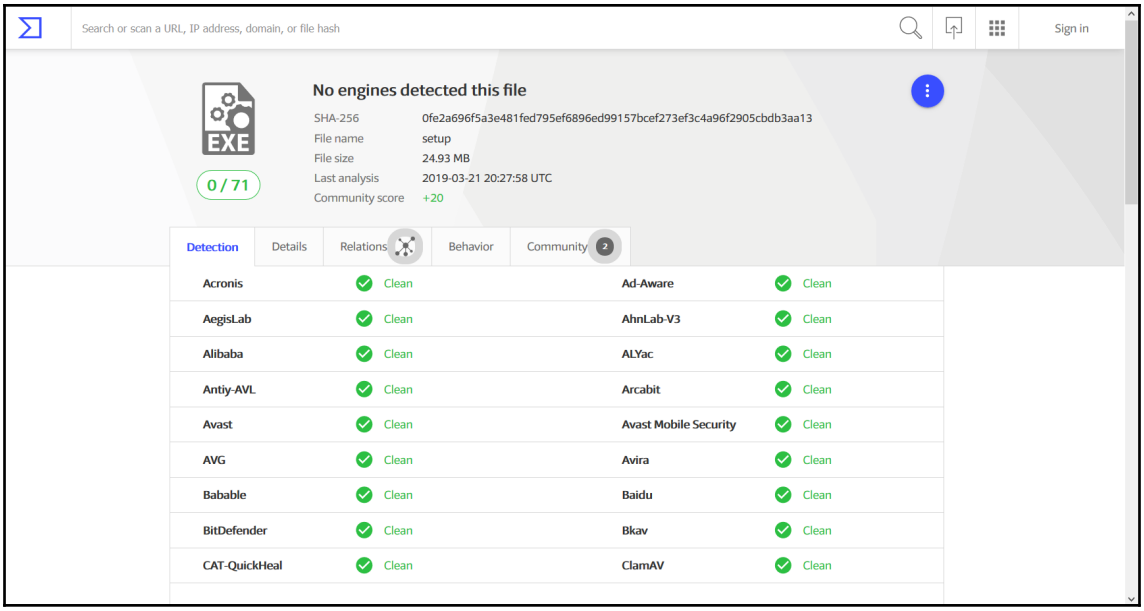

training observations
detected outliers
incorrectly labeled outliers


6
4
2
0
−2
−4
−6
−6
−4
−2
0
2
4
6
training observations
correctly labeled test observations
incorrectly labeled test observations

```
(0, 938273)    0.10023429482560929
(0, 871172)    -0.33044470291777067
(0, 755834)    -0.2806123960092745
(0, 556974)    -0.2171490773135763
(0, 548264)    -0.09851435603064428
(0, 531189)    -0.2566310842337745
(0, 522961)    -0.3119912982467716
(0, 514190)    -0.2527659565181208
(0, 501800)    -0.33044470291777067
(0, 499727)    -0.18952297847436425
(0, 488876)    0.13502094828386488
(0, 377854)    0.22710724511856722
(0, 334594)    -0.25581186158424035
(0, 256577)    0.20949022238574433
(0, 197273)    -0.30119674850360456
(0, 114899)    0.09713499033205285
(0, 28523)     -0.3060506288368513
(1, 960098)    0.09780838928665199
(1, 955748)    -0.2747271490090429
(1, 952302)    0.26070217969901804
(1, 938273)    0.12095603891963835
(1, 937092)    -0.2947114257264502
(1, 927866)    0.21727726371674563
(1, 820768)    -0.11065660403137358
(1, 772066)    -0.14344517367198276
:      :
(180828, 329790)       0.06808618130417012
(180828, 312887)       -0.08249409552977467
(180828, 209871)       0.17685927011939476
(180828, 193711)       -0.14127016157231428
(180828, 181881)       -0.11885031537539834
(180828, 180525)       -0.06925490785130799
(180828, 156500)       -0.20787461071537122
(180828, 148568)       0.1963433059906426
(180828, 82508)        -0.1289257787752738
(180828, 79994)        0.23121076025389292
(180828, 78098)        -0.18205107240120946
(180828, 47738)        0.23121076025389292
(180828, 46353)        0.1045181919567425
(180828, 45900)        -0.09537730182105167
(180828, 45419)        -0.11189579574426382
(180828, 11712)        -0.16947494737589616
(180829, 1026910)      0.4082112914772047
(180829, 975831)       -0.18401193506169794
(180829, 936283)       0.2472007199039777
(180829, 856299)       -0.15436175878438183
(180829, 473183)       -0.41092004816695277
(180829, 464504)       0.2928849862993687
(180829, 251872)       -0.4714000763194845
(180829, 189128)       0.44418614795477124
(180829, 45900)        -0.20102520636796686
```

Chapter 2: Machine Learning-Based Malware Detection

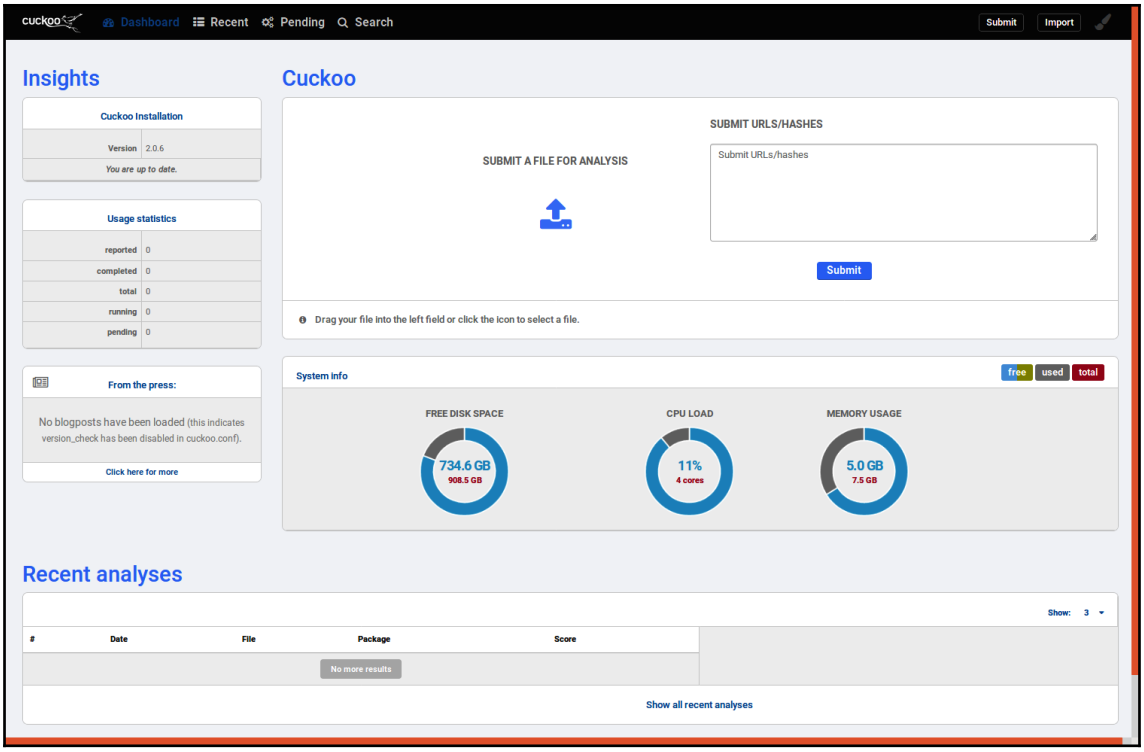
Windows x86-64 executable install	Windows	for AMD64/EM64T/x64	ff258093f0b3953c886192dec9f52763	26140976	SIG

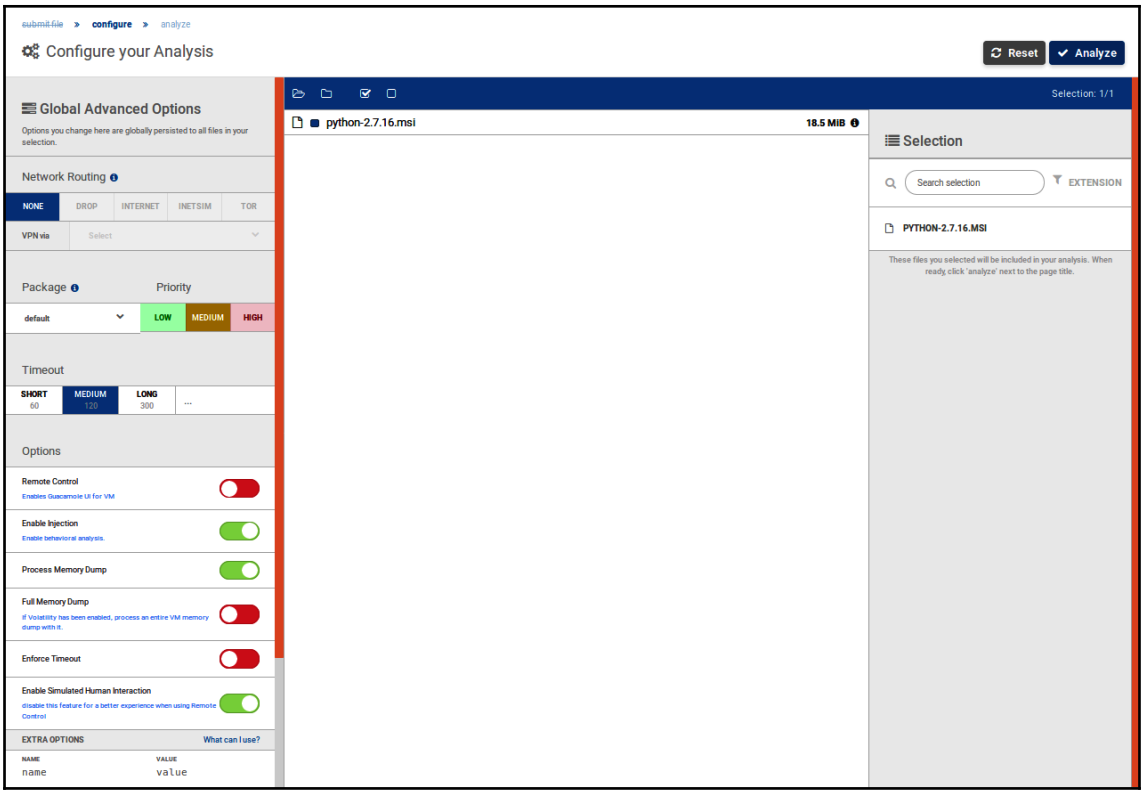


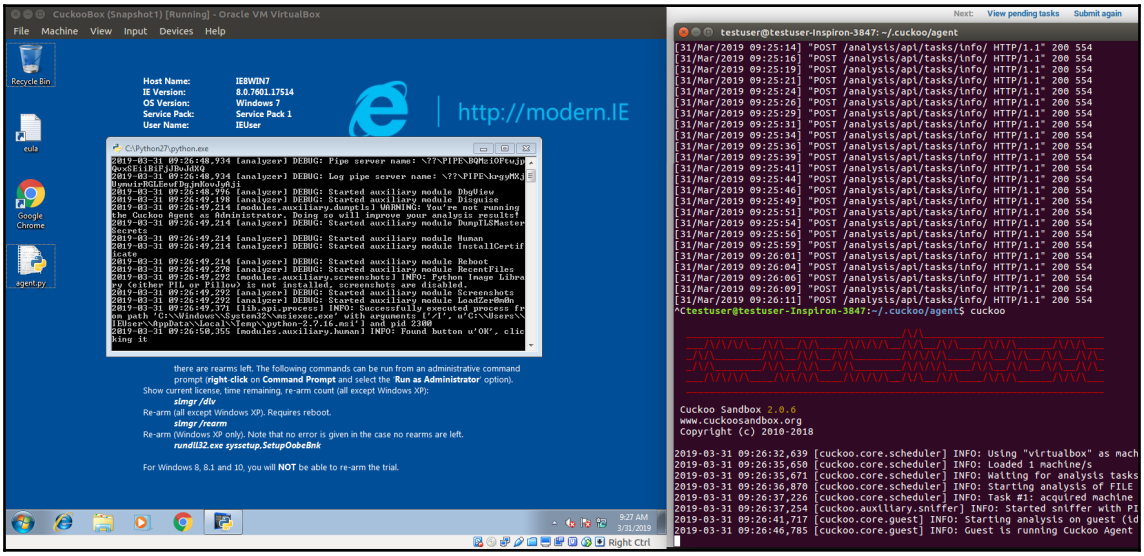
```
b'ADVAPI32.dll'
          0x44b000 b'RegCloseKey'
          0x44b004 b'RegOpenKeyExW'
          0x44b008 b'OpenProcessToken'
          0x44b00c b'AdjustTokenPrivileges'
          0x44b010 b'LookupPrivilegeValueW'
          0x44b014 b'InitiateSystemShutdownExW'
          0x44b018 b'GetUserNameW'
          0x44b01c b'RegQueryValueExW'
          0x44b020 b'RegDeleteValueW'
          0x44b024 b'CloseEventLog'
          0x44b028 b'OpenEventLogW'
          0x44b02c b'ReportEventW'
          0x44b030 b'ConvertStringSecurityDescriptorToSecurityDescriptorW'
          0x44b034 b'DecryptFileW'
          0x44b038 b'CreateWellKnownSid'
          0x44b03c b'InitializeAcl'
          0x44b040 b'SetEntriesInAclW'
          0x44b044 b'ChangeServiceConfigW'
          0x44b048 b'CloseServiceHandle'
          0x44b04c b'ControlService'
          0x44b050 b'OpenSCManagerW'
          0x44b054 b'OpenServiceW'
          0x44b058 b'QueryServiceStatus'
          0x44b05c b'SetNamedSecurityInfoW'
          0x44b060 b'CheckTokenMembership'
```

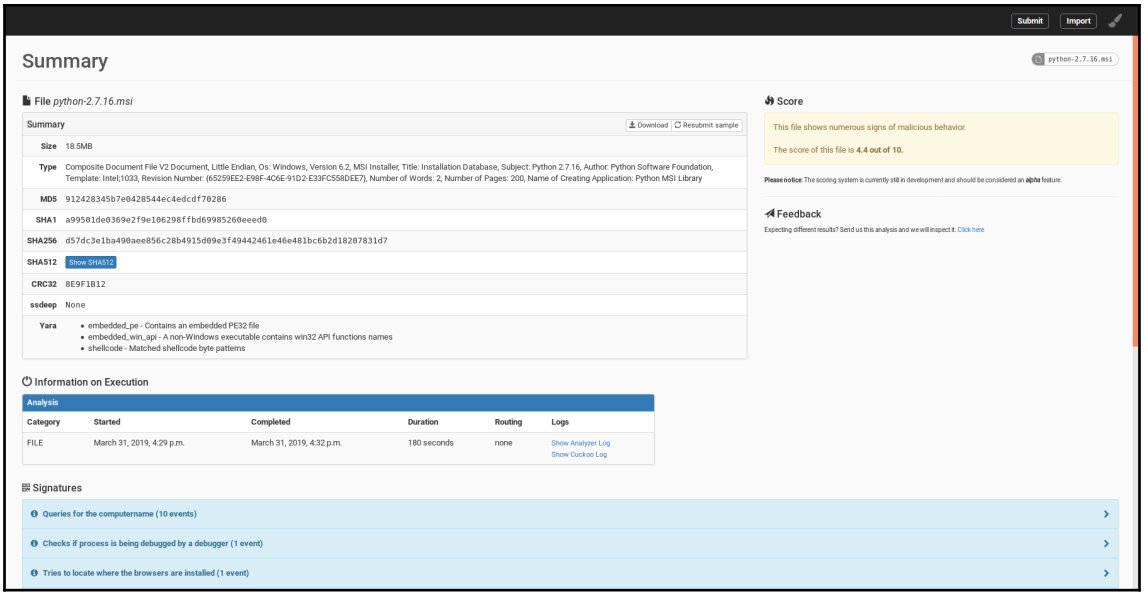
```
b'.text\x00\x00\x00' 0x1000 0x49937 301568
b'.rdata\x00\x00' 0x4b000 0x1ed60 126464
b'.data\x00\x00\x00' 0x6a000 0x1730 2560
b'.wixburn' 0x6c000 0x38 512
b'.rsrc\x00\x00\x00' 0x6d000 0x165f4 91648
b'.reloc\x00\x00' 0x84000 0x3dfc 15872
```

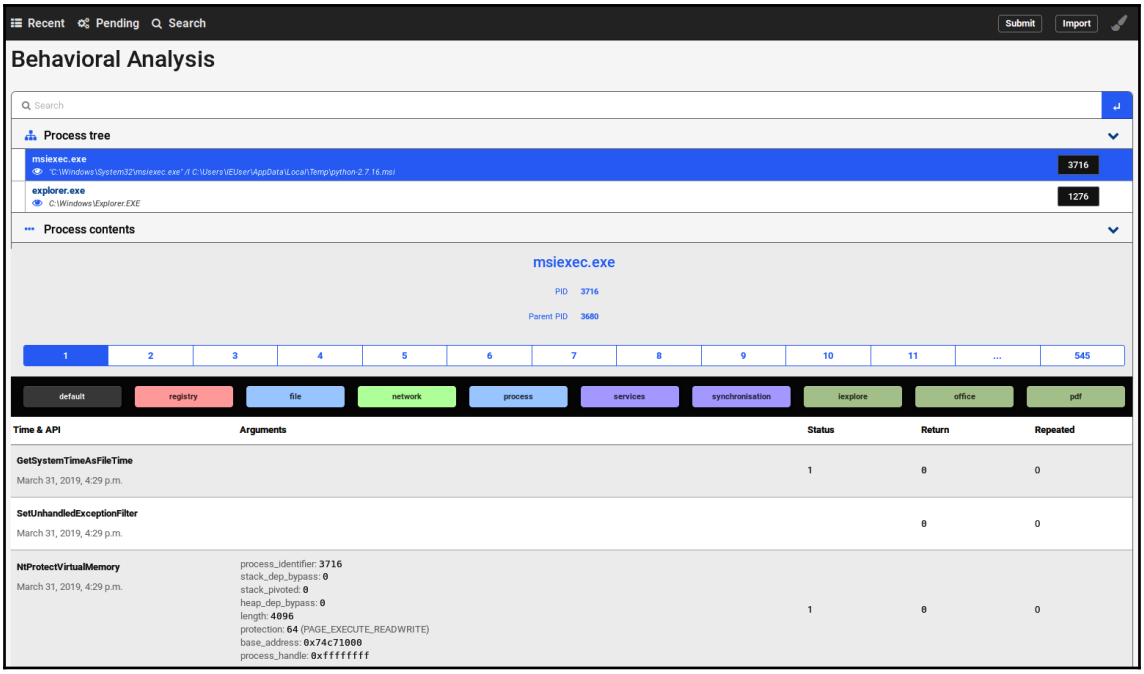
```
In [6]: print(pe.dump_info())

----------DOS_HEADER----------

[IMAGE_DOS_HEADER]
0x0         0x0   e_magic:                       0x5A4D
0x2         0x2   e_cblp:                        0x90
0x4         0x4   e_cp:                          0x3
0x6         0x6   e_crlc:                        0x0
0x8         0x8   e_cparhdr:                     0x4
0xA         0xA   e_minalloc:                    0x0
0xC         0xC   e_maxalloc:                    0xFFFF
0xE         0xE   e_ss:                          0x0
0x10        0x10  e_sp:                          0xB8
0x12        0x12  e_csum:                        0x0
0x14        0x14  e_ip:                          0x0
0x16        0x16  e_cs:                          0x0
0x18        0x18  e_lfarlc:                      0x40
0x1A        0x1A  e_ovno:                        0x0
0x1C        0x1C  e_res:
0x24        0x24  e_oemid:                       0x0
0x26        0x26  e_oeminfo:                     0x0
0x28        0x28  e_res2:
0x3C        0x3C  e_lfanew:                      0x110

----------NT_HEADERS----------

[IMAGE_NT_HEADERS]
0x110       0x0   Signature:                     0x4550

----------FILE_HEADER----------

[IMAGE_FILE_HEADER]
0x114       0x0   Machine:                       0x14C
0x116       0x2   NumberOfSections:              0x6
0x118       0x4   TimeDateStamp:                 0x5A10AD86 [Sat Nov 18 22:00:38 2017 UTC]
0x11C       0x8   PointerToSymbolTable:          0x0
0x120       0xC   NumberOfSymbols:               0x0
```


cuckoo
Dashboard
Recent
Pending
Search
Submit
Import
Insights
Cuckoo Installation
Version 2.0.6
You are up to date.
Usage statistics
reported 0
completed 0
total 0
running 0
pending 0
From the press:
No blogposts have been loaded (this indicates version_check has been disabled in cuckoo.conf).
Click here for more
Cuckoo
SUBMIT A FILE FOR ANALYSIS
SUBMIT URLS/HASHES
Submit URLs/hashes
Submit
Drag your file into the left field or click the icon to select a file.
System info
free
used
total
FREE DISK SPACE
734.6 GB
908.5 GB
CPU LOAD
11%
4 cores
MEMORY USAGE
5.0 GB
7.5 GB
Recent analyses
Show: 3
Date File Package Score
No more results
Show all recent analyses


submit file » configure » analyze
Configure your Analysis
Reset
Analyze
Global Advanced Options
Options you change here are globally persisted to all files in your selection.
Network Routing
NONE
DROP
INTERNET
INETSIM
TOR
VPN via
Select
Package
Priority
default
LOW
MEDIUM
HIGH
Timeout
SHORT
60
MEDIUM
120
LONG
300
Options
Remote Control
Enables Guacamole UI for VM
Enable Injection
Enable behavioral analysis.
Process Memory Dump
Full Memory Dump
If Volatility has been enabled, process an entire VM memory dump with it.
Enforce Timeout
Enable Simulated Human Interaction
disable this feature for a better experience when using Remote Control
EXTRA OPTIONS
What can I use?
NAME
name
VALUE
value
Selection: 1/1
python-2.7.16.msi
18.5 MiB
Selection
Search selection
EXTENSION
PYTHON-2.7.16.MSI
These files you selected will be included in your analysis. When ready, click 'analyze' next to the page title.


CuckooBox (Snapshot1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
eula
Google Chrome
agent.py
Host Name: IEBWIN7
IE Version: 8.0.7601.17514
OS Version: Windows 7
Service Pack: Service Pack 1
User Name: IEUser
http://modern.IE
C:\Python27\python.exe
there are rearms left. The following commands can be run from an administrative command prompt (right-click on Command Prompt and select the Run as Administrator option).
Show current license, time remaining, re-arm count (all except Windows XP):
slmgr /dlv
Re-arm (all except Windows XP). Requires reboot.
slmgr /rearm
Re-arm (Windows XP only). Note that no error is given in the case no rearms are left.
rundll32.exe syssetup,SetupOobeBnk
For Windows 8, 8.1 and 10, you will NOT be able to re-arm the trial.
Right Ctrl
Next: View pending tasks Submit again
testuser@testuser-Inspiron-3847: ~/.cuckoo/agent
[31/Mar/2019 09:25:14] "POST /analysis/api/tasks/info/ HTTP/1.1" 200 554
[31/Mar/2019 09:25:16] "POST /analysis/api/tasks/info/ HTTP/1.1" 200 554
[31/Mar/2019 09:25:19] "POST /analysis/api/tasks/info/ HTTP/1.1" 200 554
[31/Mar/2019 09:25:21] "POST /analysis/api/tasks/info/ HTTP/1.1" 200 554
[31/Mar/2019 09:25:24] "POST /analysis/api/tasks/info/ HTTP/1.1" 200 554
[31/Mar/2019 09:25:26] "POST /analysis/api/tasks/info/ HTTP/1.1" 200 554
[31/Mar/2019 09:25:29] "POST /analysis/api/tasks/info/ HTTP/1.1" 200 554
[31/Mar/2019 09:25:31] "POST /analysis/api/tasks/info/ HTTP/1.1" 200 554
[31/Mar/2019 09:25:34] "POST /analysis/api/tasks/info/ HTTP/1.1" 200 554
[31/Mar/2019 09:25:36] "POST /analysis/api/tasks/info/ HTTP/1.1" 200 554
[31/Mar/2019 09:25:39] "POST /analysis/api/tasks/info/ HTTP/1.1" 200 554
[31/Mar/2019 09:25:41] "POST /analysis/api/tasks/info/ HTTP/1.1" 200 554
[31/Mar/2019 09:25:44] "POST /analysis/api/tasks/info/ HTTP/1.1" 200 554
[31/Mar/2019 09:25:46] "POST /analysis/api/tasks/info/ HTTP/1.1" 200 554
[31/Mar/2019 09:25:49] "POST /analysis/api/tasks/info/ HTTP/1.1" 200 554
[31/Mar/2019 09:25:51] "POST /analysis/api/tasks/info/ HTTP/1.1" 200 554
[31/Mar/2019 09:25:54] "POST /analysis/api/tasks/info/ HTTP/1.1" 200 554
[31/Mar/2019 09:25:56] "POST /analysis/api/tasks/info/ HTTP/1.1" 200 554
[31/Mar/2019 09:25:59] "POST /analysis/api/tasks/info/ HTTP/1.1" 200 554
[31/Mar/2019 09:26:01] "POST /analysis/api/tasks/info/ HTTP/1.1" 200 554
[31/Mar/2019 09:26:04] "POST /analysis/api/tasks/info/ HTTP/1.1" 200 554
[31/Mar/2019 09:26:06] "POST /analysis/api/tasks/info/ HTTP/1.1" 200 554
[31/Mar/2019 09:26:09] "POST /analysis/api/tasks/info/ HTTP/1.1" 200 554
[31/Mar/2019 09:26:11] "POST /analysis/api/tasks/info/ HTTP/1.1" 200 554
^Ctestuser@testuser-Inspiron-3847:~/.cuckoo/agent$ cuckoo
Cuckoo Sandbox 2.0.6
www.cuckoosandbox.org
Copyright (c) 2010-2018
2019-03-31 09:26:32,639 [cuckoo.core.scheduler] INFO: Using "virtualbox" as mach
2019-03-31 09:26:35,650 [cuckoo.core.scheduler] INFO: Loaded 1 machine/s
2019-03-31 09:26:35,671 [cuckoo.core.scheduler] INFO: Waiting for analysis tasks
2019-03-31 09:26:36,870 [cuckoo.core.scheduler] INFO: Starting analysis of FILE
2019-03-31 09:26:37,226 [cuckoo.core.scheduler] INFO: Task #1: acquired machine
2019-03-31 09:26:37,254 [cuckoo.auxiliary.sniffer] INFO: Started sniffer with PI
2019-03-31 09:26:41,717 [cuckoo.core.guest] INFO: Starting analysis on guest (id
2019-03-31 09:26:46,785 [cuckoo.core.guest] INFO: Guest is running Cuckoo Agent

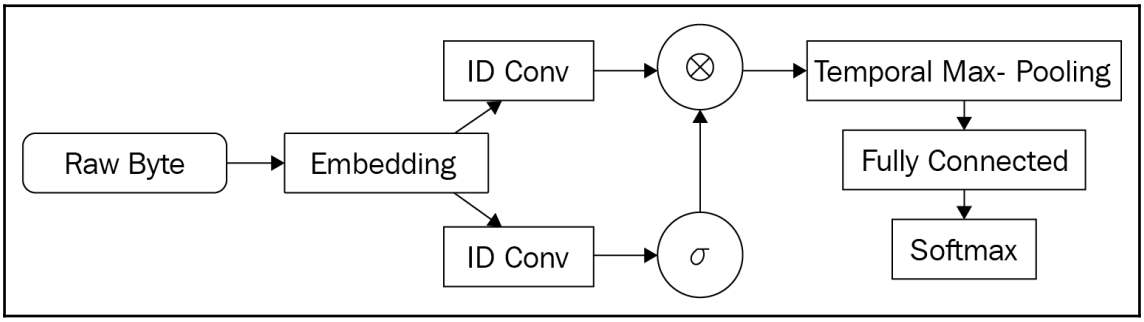

Submit
Import
Summary
python-2.7.16.msi
File python-2.7.16.msi
Summary
Download
Resubmit sample
Size 18.5MB
Type Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, MSI Installer, Title: Installation Database, Subject: Python 2.7.16, Author: Python Software Foundation, Template: Intel;1033, Revision Number: {65259EE2-E98F-4C6E-91D2-E33FC558DEE7}, Number of Words: 2, Number of Pages: 200, Name of Creating Application: Python MSI Library
MD5 912428345b7e0428544ec4edcdf70286
SHA1 a99501de0369e2f9e106298ffbd69985260eeed0
SHA256 d57dc3e1ba490aee856c28b4915d09e3f49442461e46e481bc6b2d18207831d7
SHA512 Show SHA512
CRC32 8E9F1B12
ssdeep None
Yara
embedded_pe - Contains an embedded PE32 file
embedded_win_api - A non-Windows executable contains win32 API functions names
shellcode - Matched shellcode byte patterns
Score
This file shows numerous signs of malicious behavior.
The score of this file is 4.4 out of 10.
Please notice: The scoring system is currently still in development and should be considered an alpha feature.
Feedback
Expecting different results? Send us this analysis and we will inspect it. Click here
Information on Execution
Analysis
Category Started Completed Duration Routing Logs
FILE March 31, 2019, 4:29 p.m. March 31, 2019, 4:32 p.m. 180 seconds none Show Analyzer Log Show Cuckoo Log
Signatures
Queries for the computername (10 events)
Checks if process is being debugged by a debugger (1 event)
Tries to locate where the browsers are installed (1 event)

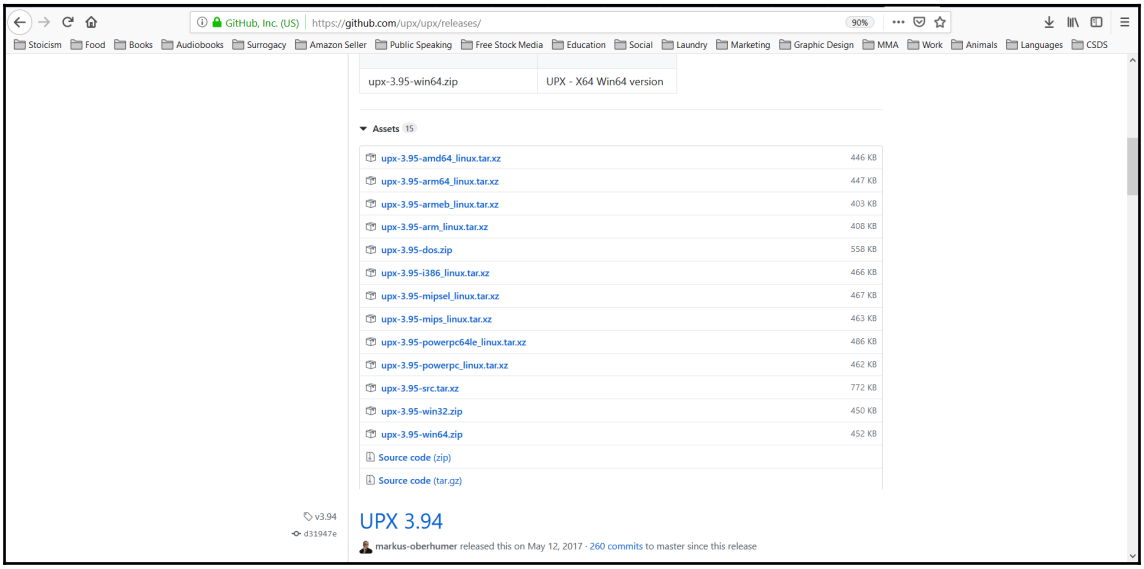

Recent
Pending
Search
Submit
Import
Behavioral Analysis
Search
Process tree
msiexec.exe
"C:\Windows\System32\msiexec.exe" /i C:\Users\EUser\AppData\Local\Temp\python-2.7.16.msi
3716
explorer.exe
C:\Windows\Explorer.EXE
1276
Process contents
msiexec.exe
PID 3716
Parent PID 3680
1 2 3 4 5 6 7 8 9 10 11 ... 545
default registry file network process services synchronisation iexplore office pdf
Time & API Arguments Status Return Repeated
GetSystemTimeAsFileTime
March 31, 2019, 4:29 p.m.
1 0 0
SetUnhandledExceptionFilter
March 31, 2019, 4:29 p.m.
0 0
NtProtectVirtualMemory
March 31, 2019, 4:29 p.m.
process_identifier: 3716
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 0
length: 4096
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x74c71000
process_handle: 0xffffffff
1 0 0

```
0.9840273816314888
[[1222    0    0]
 [  28  502    0]
 [   0    0    1]]
```

Chapter 3: Advanced Malware Detection

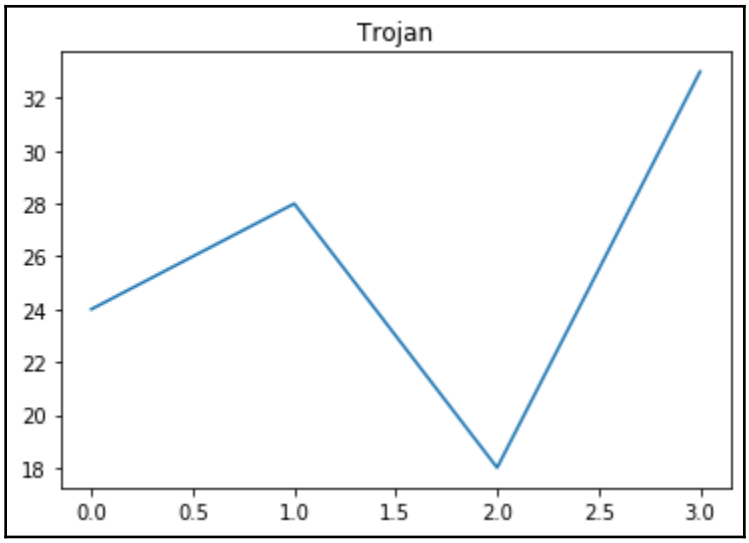
```
0.9605911330049262
[[405  18]
 [ 14 375]]
```

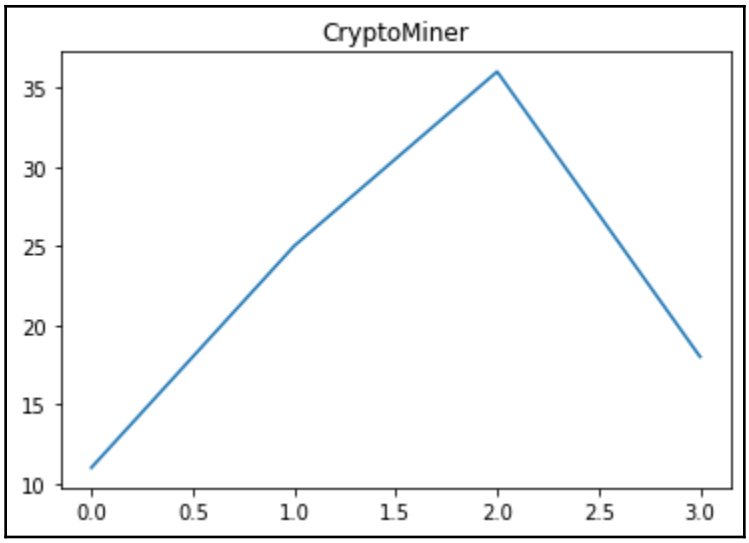


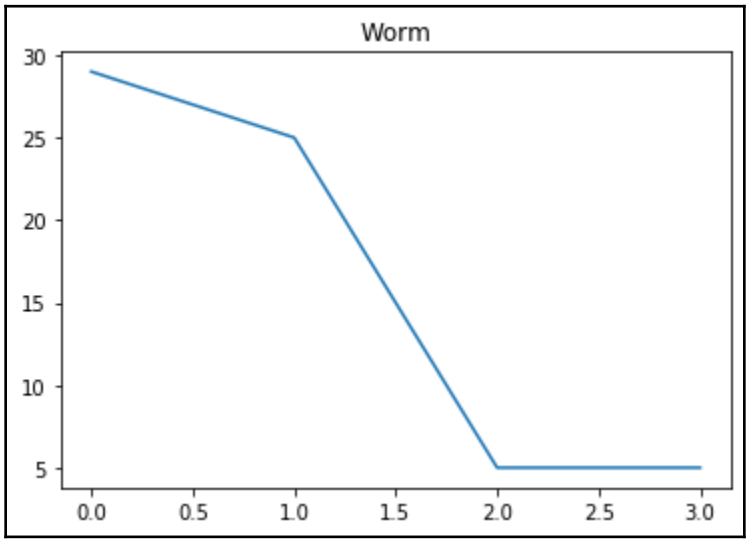


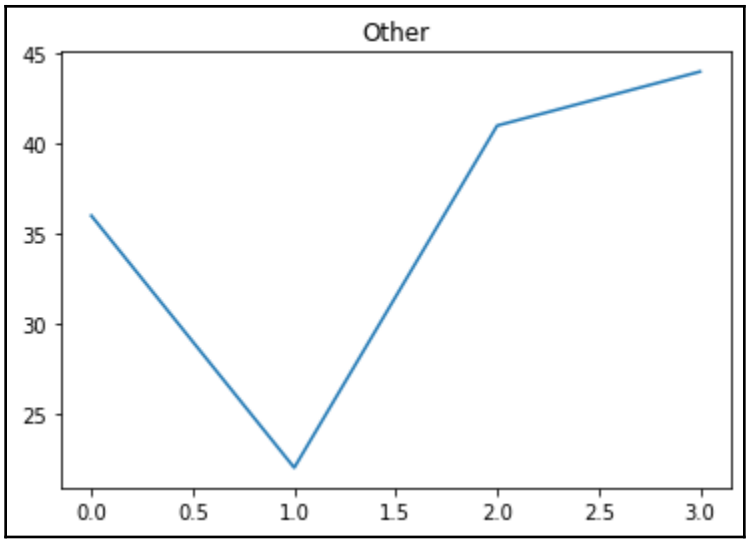
```
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2018
UPX 3.95w       Markus Oberhumer, Laszlo Molnar & John Reiser   Aug 26th 2018

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
   2868536 ->   1746744   60.89%    win64/pe     foofile.exe

Packed 1 file.
```

```
[25]: from sklearn.metrics import confusion_matrix
      confusion_matrix(y_test, y_pred)

[25]: array([[64,  2,  0],
             [ 0, 66,  0],
             [ 0,  0, 66]], dtype=int64)
```




CryptoMiner
35
30
25
20
15
10
0.0
0.5
1.0
1.5
2.0
2.5
3.0


Worm
30
25
20
15
10
5
0.0
0.5
1.0
1.5
2.0
2.5
3.0


Other
45
40
35
30
25
0.0
0.5
1.0
1.5
2.0
2.5
3.0

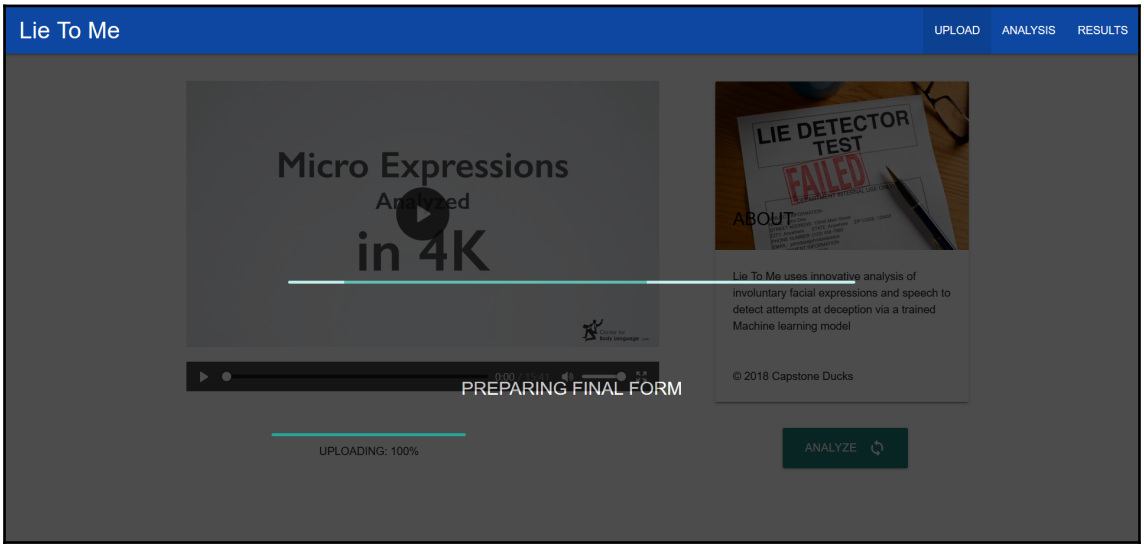
Chapter 4: Machine Learning for Social Engineering

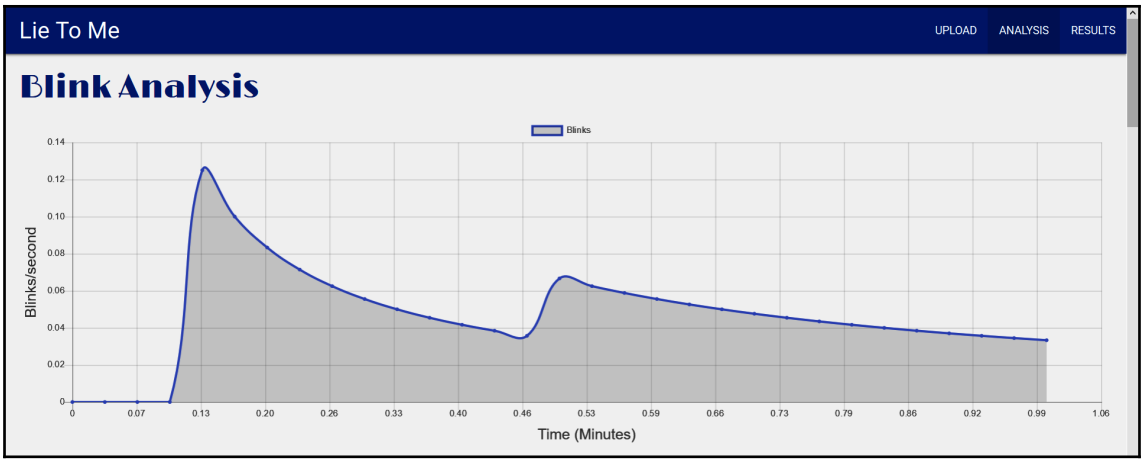

THE MARINE CORPS - LAW ENFORCEMENT FOUNDATION

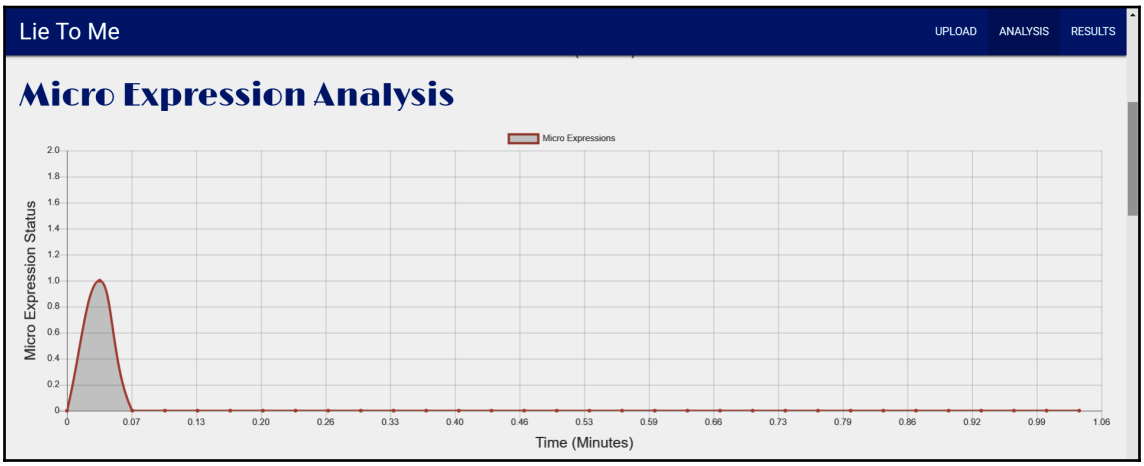

Trump
THE MARINE CORPS - LAW ENFORCEMENT FOUNDATION

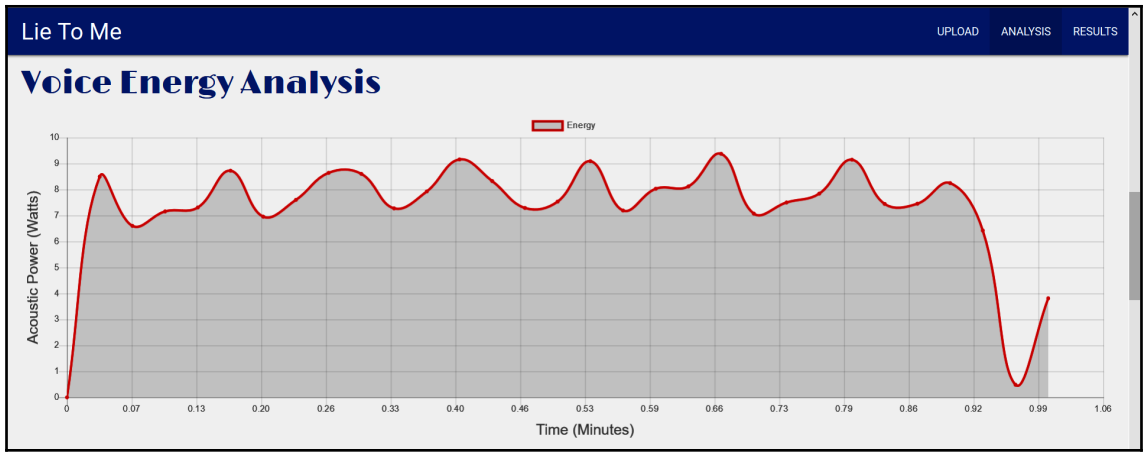

AMERICAN ATHLETIC
AMERICAN ATHLETIC
Navy

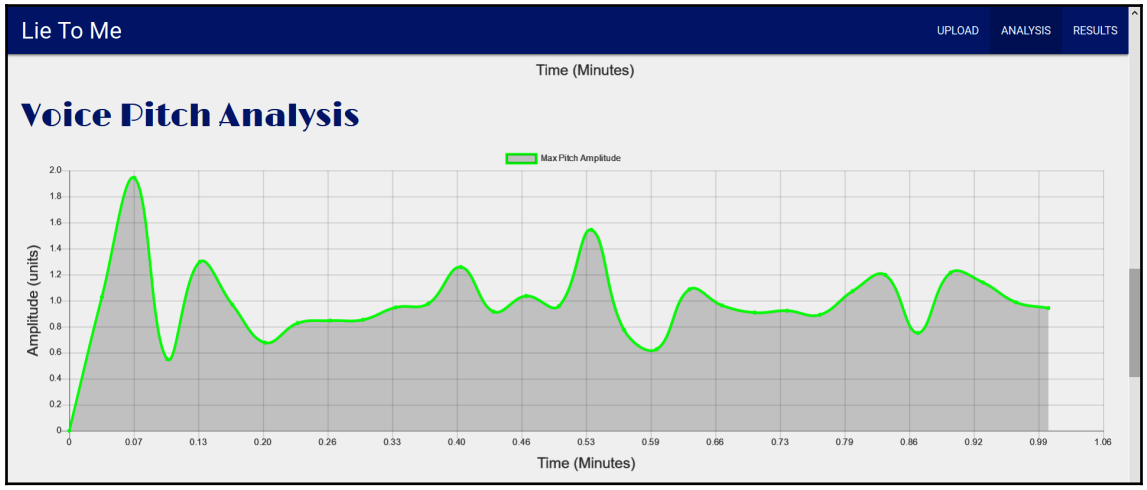

AMERICAN ATHLETIC
AMERICAN ATHLETIC
Navy

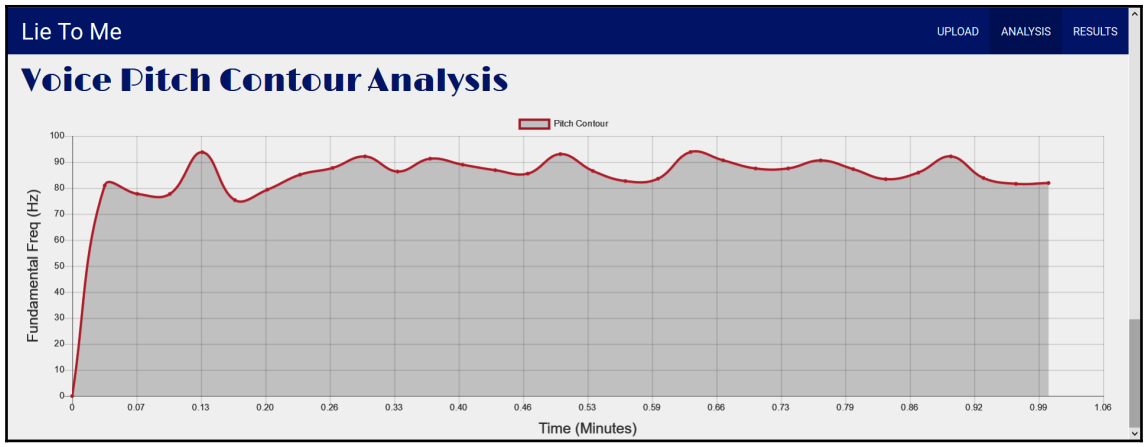

Lie To Me
UPLOAD
ANALYSIS
RESULTS
Micro Expressions
Analyzed
in 4K
LIE DETECTOR
TEST
FAILED
ABOUT
Lie To Me uses innovative analysis of involuntary facial expressions and speech to detect attempts at deception via a trained Machine learning model
© 2018 Capstone Ducks
PREPARING FINAL FORM
UPLOADING: 100%
ANALYZE

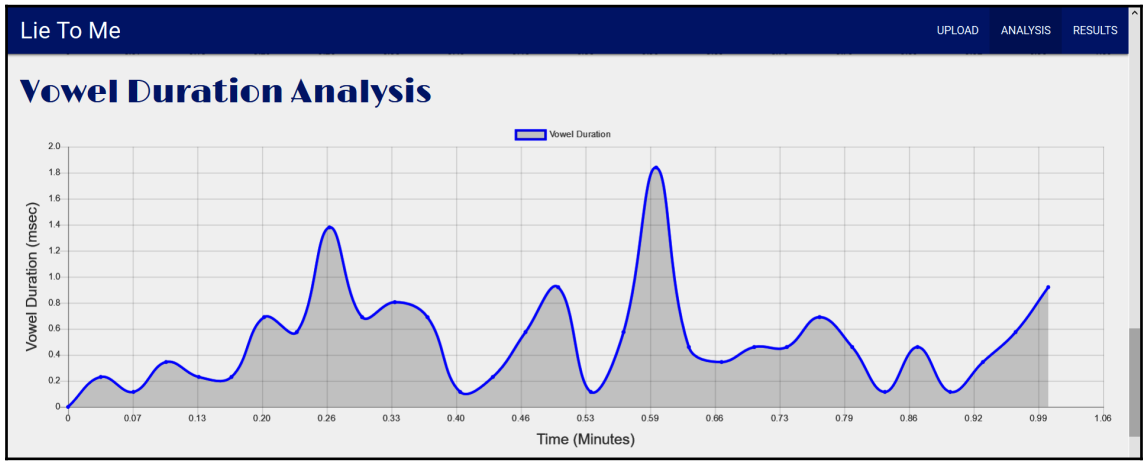

Lie To Me
UPLOAD
ANALYSIS
RESULTS
Blink Analysis
Blinks
Blinks/second
0.14
0.12
0.10
0.08
0.06
0.04
0.02
0
0
0.07
0.13
0.20
0.26
0.33
0.40
0.46
0.53
0.59
0.66
0.73
0.79
0.86
0.92
0.99
1.06
Time (Minutes)


Lie To Me
UPLOAD
ANALYSIS
RESULTS
Micro Expression Analysis
Micro Expressions
Micro Expression Status
2.0
1.8
1.6
1.4
1.2
1.0
0.8
0.6
0.4
0.2
0
0
0.07
0.13
0.20
0.26
0.33
0.40
0.46
0.53
0.59
0.66
0.73
0.79
0.86
0.92
0.99
1.06
Time (Minutes)


Lie To Me
UPLOAD
ANALYSIS
RESULTS
Voice Energy Analysis
Energy
Acoustic Power (Watts)
0
1
2
3
4
5
6
7
8
9
10
0
0.07
0.13
0.20
0.26
0.33
0.40
0.46
0.53
0.59
0.66
0.73
0.79
0.86
0.92
0.99
1.06
Time (Minutes)


Lie To Me
UPLOAD
ANALYSIS
RESULTS
Time (Minutes)
Voice Pitch Analysis
Max Pitch Amplitude
Amplitude (units)
0
0.2
0.4
0.6
0.8
1.0
1.2
1.4
1.6
1.8
2.0
0
0.07
0.13
0.20
0.26
0.33
0.40
0.46
0.53
0.59
0.66
0.73
0.79
0.86
0.92
0.99
1.06
Time (Minutes)


Lie To Me
UPLOAD
ANALYSIS
RESULTS
Voice Pitch Contour Analysis
Pitch Contour
Fundamental Freq (Hz)
Time (Minutes)


Lie To Me
UPLOAD
ANALYSIS
RESULTS
Vowel Duration Analysis
Vowel Duration
Vowel Duration (msec)
Time (Minutes)

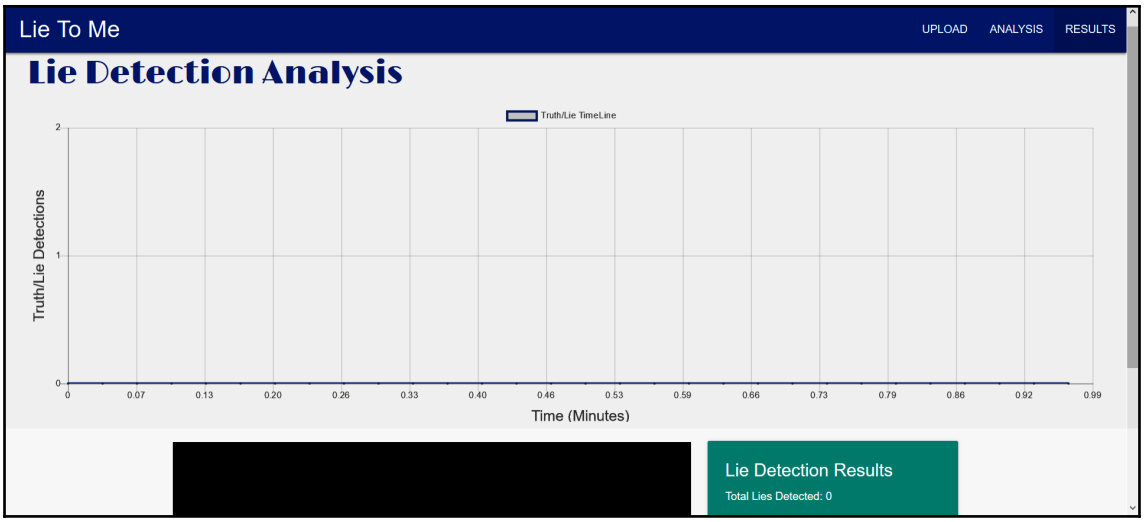
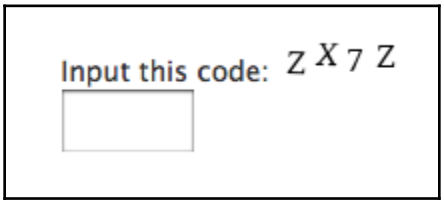
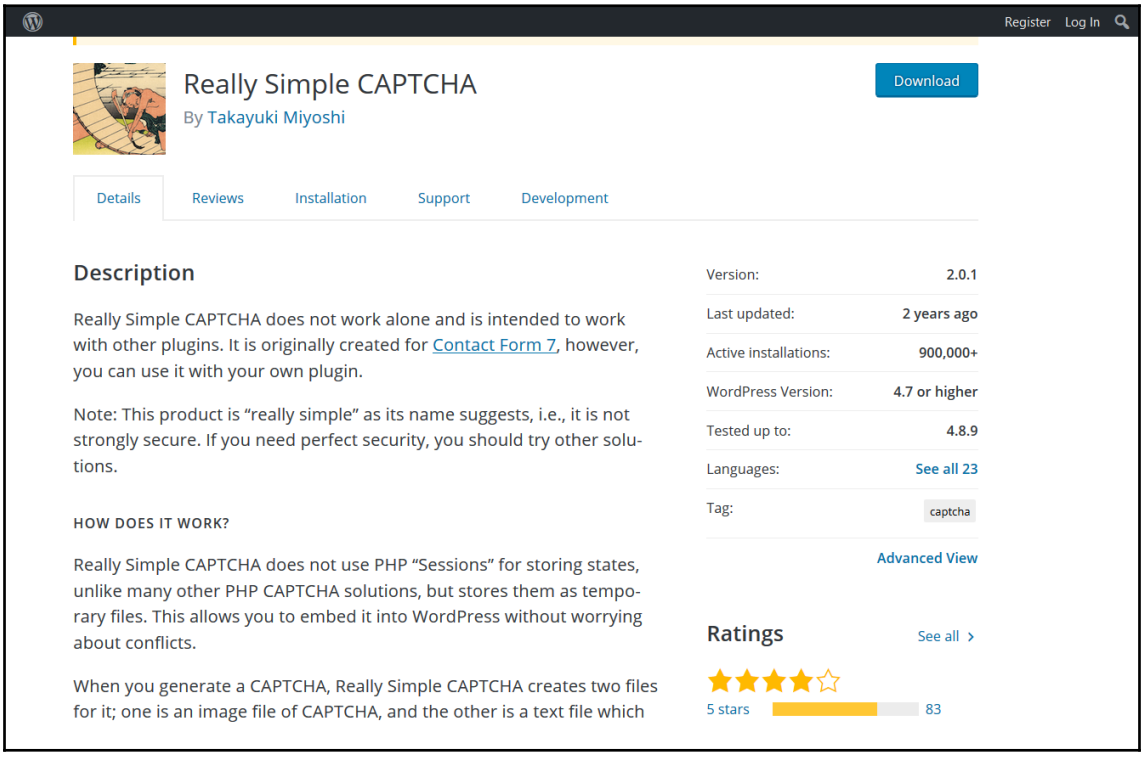

Lie To Me
UPLOAD
ANALYSIS
RESULTS
Lie Detection Analysis
Truth/Lie TimeLine
Truth/Lie Detections
2
1
0
0
0.07
0.13
0.20
0.26
0.33
0.40
0.46
0.53
0.59
0.66
0.73
0.79
0.86
0.92
0.99
Time (Minutes)
Lie Detection Results
Total Lies Detected: 0

Photo	Name	LinkedIn	Facebook	Twitter	Instagram
		GooglePlus	VKontakte	Weibo	Douban
	Bill Gates	Twitter: https://twitter.com/BillGates			

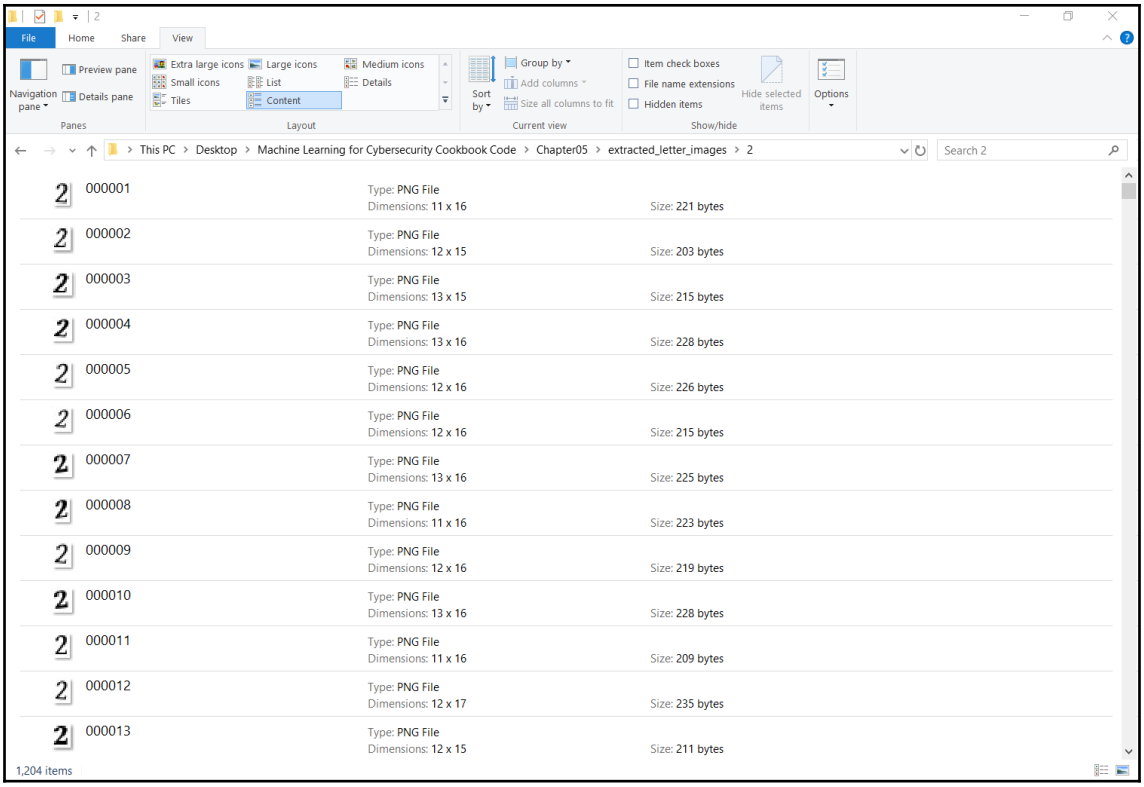
"<SOR>Very nice atmosphere. I had the burger which was delicious. Also, the chicken curry was the b
est in town.<EOR>"
"<SOR>Amazing! My favorite place to go when your in Vegas! And the breakfast and wine are a definit
e place to eat!<EOR>"
"<SOR>Best pizza in town, crispy and crispy and not crazy about the chocolate level of taste. The b
est part is the location too. Their crepes are amazing! A must try, best service . We will be retu
rning several times for wonton soups.<EOR>"
"<SOR>The food was fresh and tasty. I was so impressed by the kids and I loved the fresh chsty. I w
as so impressed by the kids and I loved the fresh ch

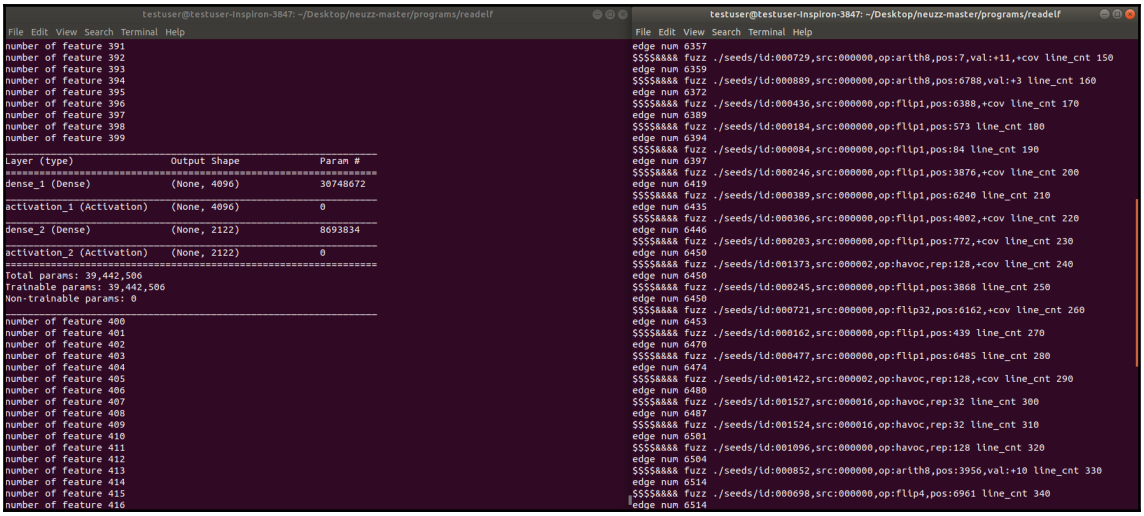
Chapter 5: Penetration Testing Using Machine Learning



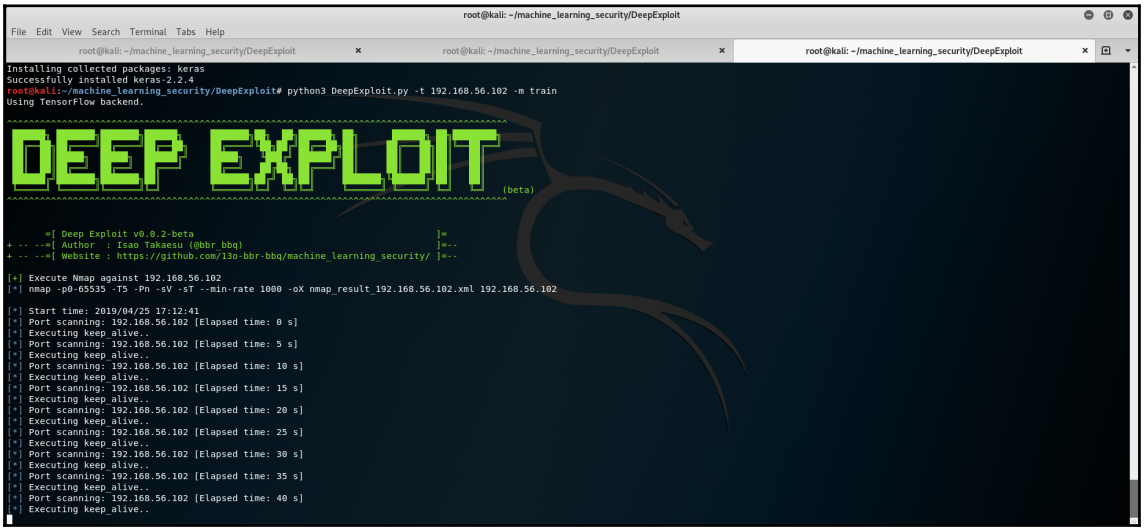


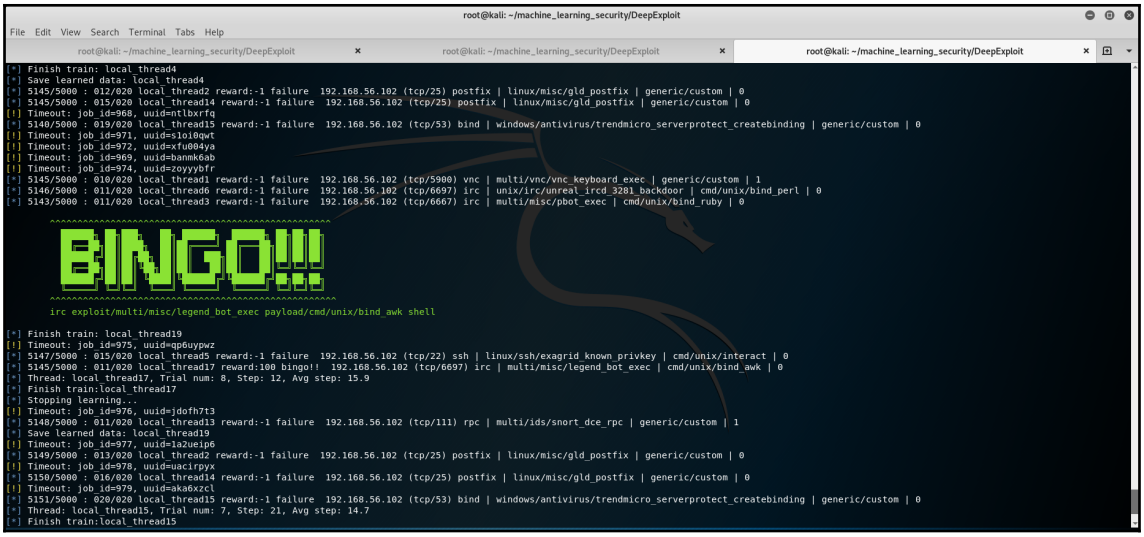
```
 Directory of C:\Users\ETsukerman\Desktop\Machine Learning for Cybersecurity Cookbook Code\Chapter05\extracted_letter_images

04/23/2019  06:17 PM    <DIR>          .
04/23/2019  06:17 PM    <DIR>          ..
04/23/2019  06:19 PM    <DIR>          2
04/23/2019  06:19 PM    <DIR>          3
04/23/2019  06:19 PM    <DIR>          4
04/23/2019  06:19 PM    <DIR>          5
04/23/2019  06:19 PM    <DIR>          6
04/23/2019  06:19 PM    <DIR>          7
04/23/2019  06:19 PM    <DIR>          8
04/23/2019  06:19 PM    <DIR>          9
04/23/2019  06:19 PM    <DIR>          A
04/23/2019  06:19 PM    <DIR>          B
04/23/2019  06:19 PM    <DIR>          C
04/23/2019  06:19 PM    <DIR>          D
04/23/2019  06:19 PM    <DIR>          E
04/23/2019  06:19 PM    <DIR>          F
04/23/2019  06:19 PM    <DIR>          G
04/23/2019  06:19 PM    <DIR>          H
04/23/2019  06:19 PM    <DIR>          J
04/23/2019  06:19 PM    <DIR>          K
04/23/2019  06:19 PM    <DIR>          L
04/23/2019  06:19 PM    <DIR>          M
04/23/2019  06:19 PM    <DIR>          N
04/23/2019  06:19 PM    <DIR>          P
04/23/2019  06:19 PM    <DIR>          Q
04/23/2019  06:19 PM    <DIR>          R
04/23/2019  06:19 PM    <DIR>          S
04/23/2019  06:19 PM    <DIR>          T
04/23/2019  06:19 PM    <DIR>          U
04/23/2019  06:19 PM    <DIR>          V
04/23/2019  06:19 PM    <DIR>          W
04/23/2019  06:19 PM    <DIR>          X
04/23/2019  06:19 PM    <DIR>          Y
04/23/2019  06:19 PM    <DIR>          Z
               0 File(s)              0 bytes
              34 Dir(s)  79,015,010,304 bytes free
```

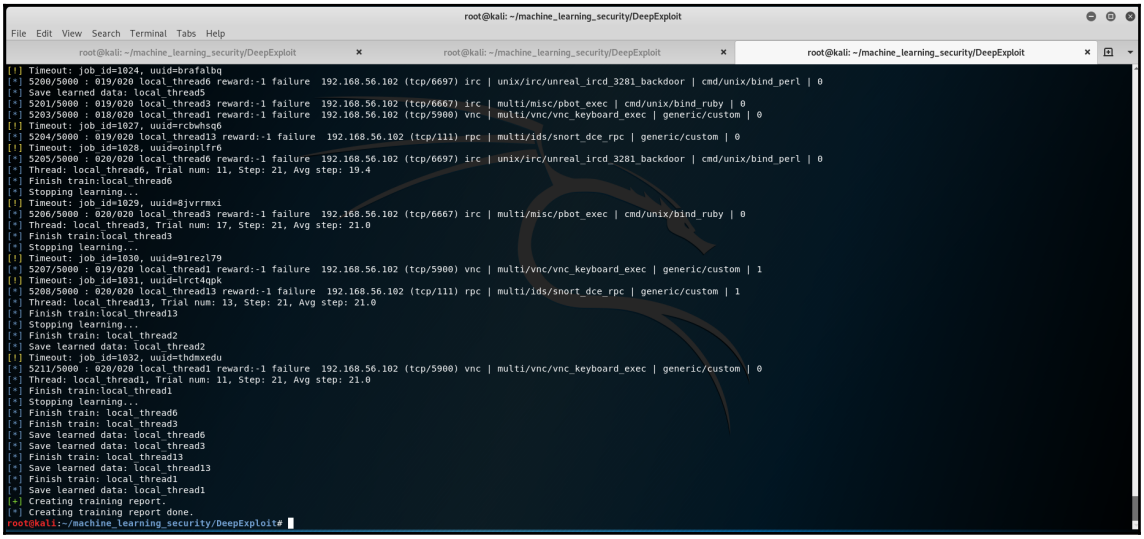

File
Home
Share
View
Navigation pane
Preview pane
Details pane
Panes
Extra large icons
Large icons
Medium icons
Small icons
List
Details
Tiles
Content
Layout
Sort by
Group by
Add columns
Size all columns to fit
Current view
Item check boxes
File name extensions
Hidden items
Hide selected items
Show/hide
Options
This PC › Desktop › Machine Learning for Cybersecurity Cookbook Code › Chapter05 › extracted_letter_images › 2
Search 2
000001 Type: PNG File Dimensions: 11 x 16 Size: 221 bytes
000002 Type: PNG File Dimensions: 12 x 15 Size: 203 bytes
000003 Type: PNG File Dimensions: 13 x 15 Size: 215 bytes
000004 Type: PNG File Dimensions: 13 x 16 Size: 228 bytes
000005 Type: PNG File Dimensions: 12 x 16 Size: 226 bytes
000006 Type: PNG File Dimensions: 12 x 16 Size: 215 bytes
000007 Type: PNG File Dimensions: 13 x 16 Size: 225 bytes
000008 Type: PNG File Dimensions: 11 x 16 Size: 223 bytes
000009 Type: PNG File Dimensions: 12 x 16 Size: 219 bytes
000010 Type: PNG File Dimensions: 13 x 16 Size: 228 bytes
000011 Type: PNG File Dimensions: 11 x 16 Size: 209 bytes
000012 Type: PNG File Dimensions: 12 x 17 Size: 235 bytes
000013 Type: PNG File Dimensions: 12 x 15 Size: 211 bytes
1,204 items


testuser@testuser-Inspiron-3847: ~/Desktop/neuzz-master/programs/readelf
File Edit View Search Terminal Help
number of feature 391
number of feature 392
number of feature 393
number of feature 394
number of feature 395
number of feature 396
number of feature 397
number of feature 398
number of feature 399
Layer (type) Output Shape Param #
dense_1 (Dense) (None, 4096) 30748672
activation_1 (Activation) (None, 4096) 0
dense_2 (Dense) (None, 2122) 8693834
activation_2 (Activation) (None, 2122) 0
Total params: 39,442,506
Trainable params: 39,442,506
Non-trainable params: 0
number of feature 400
number of feature 401
number of feature 402
number of feature 403
number of feature 404
number of feature 405
number of feature 406
number of feature 407
number of feature 408
number of feature 409
number of feature 410
number of feature 411
number of feature 412
number of feature 413
number of feature 414
number of feature 415
number of feature 416
testuser@testuser-Inspiron-3847: ~/Desktop/neuzz-master/programs/readelf
File Edit View Search Terminal Help
edge num 6357
$$$$&&&& fuzz ./seeds/id:000729,src:000000,op:arith8,pos:7,val:+11,+cov line_cnt 150
edge num 6359
$$$$&&&& fuzz ./seeds/id:000889,src:000000,op:arith8,pos:6788,val:+3 line_cnt 160
edge num 6372
$$$$&&&& fuzz ./seeds/id:000436,src:000000,op:flip1,pos:6388,+cov line_cnt 170
edge num 6389
$$$$&&&& fuzz ./seeds/id:000184,src:000000,op:flip1,pos:573 line_cnt 180
edge num 6394
$$$$&&&& fuzz ./seeds/id:000084,src:000000,op:flip1,pos:84 line_cnt 190
edge num 6397
$$$$&&&& fuzz ./seeds/id:000246,src:000000,op:flip1,pos:3876,+cov line_cnt 200
edge num 6419
$$$$&&&& fuzz ./seeds/id:000389,src:000000,op:flip1,pos:6240 line_cnt 210
edge num 6435
$$$$&&&& fuzz ./seeds/id:000306,src:000000,op:flip1,pos:4002,+cov line_cnt 220
edge num 6446
$$$$&&&& fuzz ./seeds/id:000203,src:000000,op:flip1,pos:772,+cov line_cnt 230
edge num 6450
$$$$&&&& fuzz ./seeds/id:001373,src:000002,op:havoc,rep:128,+cov line_cnt 240
edge num 6450
$$$$&&&& fuzz ./seeds/id:000245,src:000000,op:flip1,pos:3868 line_cnt 250
edge num 6450
$$$$&&&& fuzz ./seeds/id:000721,src:000000,op:flip32,pos:6162,+cov line_cnt 260
edge num 6453
$$$$&&&& fuzz ./seeds/id:000162,src:000000,op:flip1,pos:439 line_cnt 270
edge num 6470
$$$$&&&& fuzz ./seeds/id:000477,src:000000,op:flip1,pos:6485 line_cnt 280
edge num 6474
$$$$&&&& fuzz ./seeds/id:001422,src:000002,op:havoc,rep:128,+cov line_cnt 290
edge num 6480
$$$$&&&& fuzz ./seeds/id:001527,src:000016,op:havoc,rep:32 line_cnt 300
edge num 6487
$$$$&&&& fuzz ./seeds/id:001524,src:000016,op:havoc,rep:32 line_cnt 310
edge num 6501
$$$$&&&& fuzz ./seeds/id:001096,src:000000,op:havoc,rep:128 line_cnt 320
edge num 6504
$$$$&&&& fuzz ./seeds/id:000852,src:000000,op:arith8,pos:3956,val:+10 line_cnt 330
edge num 6514
$$$$&&&& fuzz ./seeds/id:000698,src:000000,op:flip4,pos:6961 line_cnt 340
edge num 6514

```
testuser@testuser-Inspiron-3847:~/Desktop/neuzz/programs/readelf$ ./readelf -a crashes/crash_0_001652
readelf: Error: '-a': No such file
ELF Header:
  Magic:   7f 45 4c 46 01 01 01 00 00 00 00 00 00 00 00 00
  Class:                             ELF32
  Data:                              2's complement, little endian
  Version:                           1 (current)
  OS/ABI:                            UNIX - System V
  ABI Version:                       0
  Type:                              DYN (Shared object file)
  Machine:                           MIPS R4000 big-endian
  Version:                           0x0
  Entry point address:               0x0
  Start of program headers:          0 (bytes into file)
  Start of section headers:          0 (bytes into file)
  Flags:                             0x0
  Size of this header:               0 (bytes)
  Size of program headers:           0 (bytes)
  Number of program headers:         0
  Size of section headers:           0 (bytes)
  Number of section headers:         0
  Section header string table index: 0

There are no sections in this file.

There are no sections to group in this file.

There are no program headers in this file.

There is no dynamic section in this file.

There are no relocations in this file.

The decoding of unwind sections for machine type MIPS R4000 big-endian is not currently supported.

Dynamic symbol information is not available for displaying symbols.

No version information found in this file.
readelf: readelf.c:658: find_section: Assertion `filedata->section_headers != NULL' failed.
Aborted
```

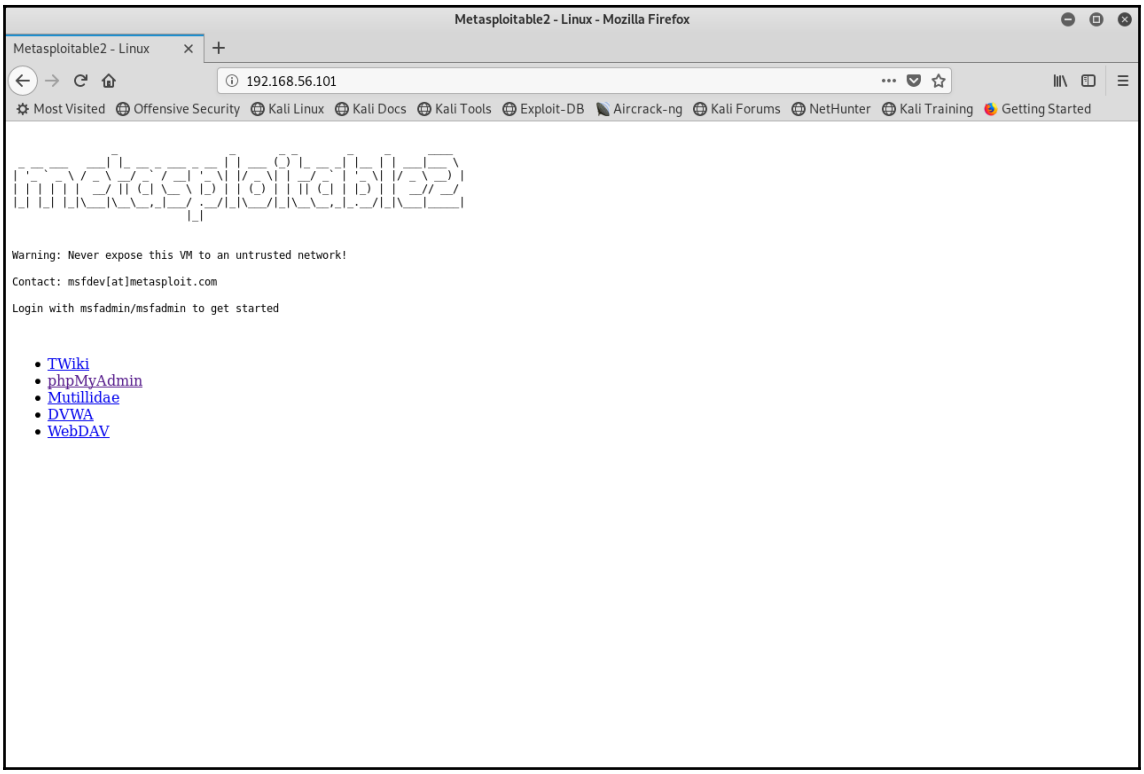



root@kali: ~/machine_learning_security/DeepExploit
File Edit View Search Terminal Tabs Help
root@kali: ~/machine_learning_security/DeepExploit
root@kali: ~/machine_learning_security/DeepExploit
root@kali: ~/machine_learning_security/DeepExploit
[*] Finish train: local_thread4
[*] Save learned data: local_thread4
[*] 5145/5000 : 012/020 local_thread2 reward:-1 failure 192.168.56.102 (tcp/25) postfix | linux/misc/gld_postfix | generic/custom | 0
[*] 5145/5000 : 015/020 local_thread14 reward:-1 failure 192.168.56.102 (tcp/25) postfix | linux/misc/gld_postfix | generic/custom | 0
[!] Timeout: job_id=968, uuid=ntlbxrfq
[*] 5140/5000 : 019/020 local_thread15 reward:-1 failure 192.168.56.102 (tcp/53) bind | windows/antivirus/trendmicro_serverprotect_createbinding | generic/custom | 0
[!] Timeout: job_id=971, uuid=s1oi0qwt
[!] Timeout: job_id=972, uuid=xfu004ya
[!] Timeout: job_id=969, uuid=banmk6ab
[!] Timeout: job_id=974, uuid=zoyyybfr
[*] 5145/5000 : 010/020 local_thread1 reward:-1 failure 192.168.56.102 (tcp/5900) vnc | multi/vnc/vnc_keyboard_exec | generic/custom | 1
[*] 5146/5000 : 011/020 local_thread6 reward:-1 failure 192.168.56.102 (tcp/6697) irc | unix/irc/unreal_ircd_3281_backdoor | cmd/unix/bind_perl | 0
[*] 5143/5000 : 011/020 local_thread3 reward:-1 failure 192.168.56.102 (tcp/6667) irc | multi/misc/pbot_exec | cmd/unix/bind_ruby | 0
BINGO!!!
irc exploit/multi/misc/legend_bot_exec payload/cmd/unix/bind_awk shell
[*] Finish train: local_thread19
[!] Timeout: job_id=975, uuid=qp6uypwz
[*] 5147/5000 : 015/020 local_thread5 reward:-1 failure 192.168.56.102 (tcp/22) ssh | linux/ssh/exagrid known privkey | cmd/unix/interact | 0
[*] 5145/5000 : 011/020 local_thread17 reward:100 bingo!! 192.168.56.102 (tcp/6697) irc | multi/misc/legend_bot_exec | cmd/unix/bind_awk | 0
[*] Thread: local_thread17, Trial num: 8, Step: 12, Avg step: 15.9
[*] Finish train:local_thread17
[*] Stopping learning...
[!] Timeout: job_id=976, uuid=jdofh7t3
[*] 5148/5000 : 011/020 local_thread13 reward:-1 failure 192.168.56.102 (tcp/111) rpc | multi/ids/snort_dce_rpc | generic/custom | 1
[*] Save learned data: local_thread19
[!] Timeout: job_id=977, uuid=ia2ueip6
[*] 5149/5000 : 013/020 local_thread2 reward:-1 failure 192.168.56.102 (tcp/25) postfix | linux/misc/gld_postfix | generic/custom | 0
[!] Timeout: job_id=978, uuid=uacirpyx
[*] 5150/5000 : 016/020 local_thread14 reward:-1 failure 192.168.56.102 (tcp/25) postfix | linux/misc/gld_postfix | generic/custom | 0
[!] Timeout: job_id=979, uuid=aka6xzcl
[*] 5151/5000 : 020/020 local_thread15 reward:-1 failure 192.168.56.102 (tcp/53) bind | windows/antivirus/trendmicro_serverprotect_createbinding | generic/custom | 0
[*] Thread: local_thread15, Trial num: 7, Step: 21, Avg step: 14.7
[*] Finish train:local_thread15


root@kali: ~/machine_learning_security/DeepExploit
File Edit View Search Terminal Tabs Help
root@kali: ~/machine_learning_security/DeepExploit
root@kali: ~/machine_learning_security/DeepExploit
root@kali: ~/machine_learning_security/DeepExploit
[!] Timeout: job_id=1024, uuid=brafalbq
[*] 5200/5000 : 019/020 local_thread6 reward:-1 failure 192.168.56.102 (tcp/6697) irc | unix/irc/unreal_ircd_3281_backdoor | cmd/unix/bind_perl | 0
[*] Save learned data: local_thread5
[*] 5201/5000 : 019/020 local_thread3 reward:-1 failure 192.168.56.102 (tcp/6667) irc | multi/misc/pbot_exec | cmd/unix/bind_ruby | 0
[*] 5203/5000 : 018/020 local_thread1 reward:-1 failure 192.168.56.102 (tcp/5900) vnc | multi/vnc/vnc_keyboard_exec | generic/custom | 0
[!] Timeout: job_id=1027, uuid=rcbwhsq6
[*] 5204/5000 : 019/020 local_thread13 reward:-1 failure 192.168.56.102 (tcp/111) rpc | multi/ids/snort_dce_rpc | generic/custom | 0
[!] Timeout: job_id=1028, uuid=oinplfr6
[*] 5205/5000 : 020/020 local_thread6 reward:-1 failure 192.168.56.102 (tcp/6697) irc | unix/irc/unreal_ircd_3281_backdoor | cmd/unix/bind_perl | 0
[*] Thread: local_thread6, Trial num: 11, Step: 21, Avg step: 19.4
[*] Finish train:local_thread6
[*] Stopping learning...
[!] Timeout: job_id=1029, uuid=8jvrrmxi
[*] 5206/5000 : 020/020 local_thread3 reward:-1 failure 192.168.56.102 (tcp/6667) irc | multi/misc/pbot_exec | cmd/unix/bind_ruby | 0
[*] Thread: local_thread3, Trial num: 17, Step: 21, Avg step: 21.0
[*] Finish train:local_thread3
[*] Stopping learning...
[!] Timeout: job_id=1030, uuid=91rezl79
[*] 5207/5000 : 019/020 local_thread1 reward:-1 failure 192.168.56.102 (tcp/5900) vnc | multi/vnc/vnc_keyboard_exec | generic/custom | 1
[!] Timeout: job_id=1031, uuid=lrct4qpk
[*] 5208/5000 : 020/020 local_thread13 reward:-1 failure 192.168.56.102 (tcp/111) rpc | multi/ids/snort_dce_rpc | generic/custom | 1
[*] Thread: local_thread13, Trial num: 13, Step: 21, Avg step: 21.0
[*] Finish train:local_thread13
[*] Stopping learning...
[*] Finish train: local_thread2
[*] Save learned data: local_thread2
[!] Timeout: job_id=1032, uuid=thdmxedu
[*] 5211/5000 : 020/020 local_thread1 reward:-1 failure 192.168.56.102 (tcp/5900) vnc | multi/vnc/vnc_keyboard_exec | generic/custom | 0
[*] Thread: local_thread1, Trial num: 11, Step: 21, Avg step: 21.0
[*] Finish train:local_thread1
[*] Stopping learning...
[*] Finish train: local_thread6
[*] Finish train: local_thread3
[*] Save learned data: local_thread6
[*] Save learned data: local_thread3
[*] Finish train: local_thread13
[*] Save learned data: local_thread13
[*] Finish train: local_thread1
[*] Save learned data: local_thread1
[+] Creating training report.
[*] Creating training report done.
root@kali:~/machine_learning_security/DeepExploit#

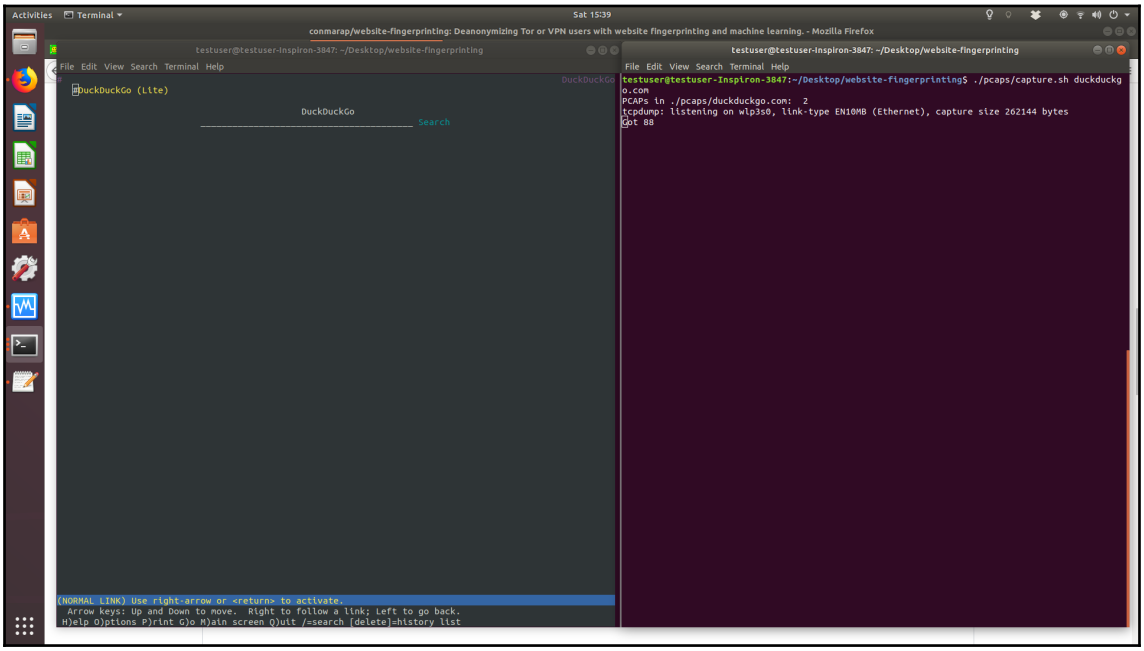
Deep Exploit scan Report

Index	Item	Value
1	IP address	192.168.56.102
	Port number	21
	Source IP address	192.168.56.101
	Product name	vsftpd
	Vuln name	VSFTPD v2.3.4 Backdoor Command Execution
	Type	shell
	Description	This module exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available. This backdoor was removed on July 3rd 2011.
	Exploit module	exploit/unix/ftp/vsftpd_234_backdoor
	Target	0
	Payload	payload/cmd/unix/interact
	Reference	[OSVDB] 73573 [URL] http://pastebin.com/AetT9sS5 [URL] http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
2	IP address	192.168.56.102
	Port number	25
	Source IP address	192.168.56.101
	Product name	postfix
	Vuln name	GLD (Greylisting Daemon) Postfix Buffer Overflow
	Type	shell
	Description	This module exploits a stack buffer overflow in the Salim Gasmi GLD <= 1.4 greylisting daemon for Postfix. By sending an overly long string the stack can be overwritten.
	Exploit module	exploit/linux/misc/gld_postfix
	Target	0
	Payload	payload/generic/shell_bind_tcp
	Reference	[CVE] 2005-1099 [OSVDB] 15492 [BID] 13129 [EDB] 934

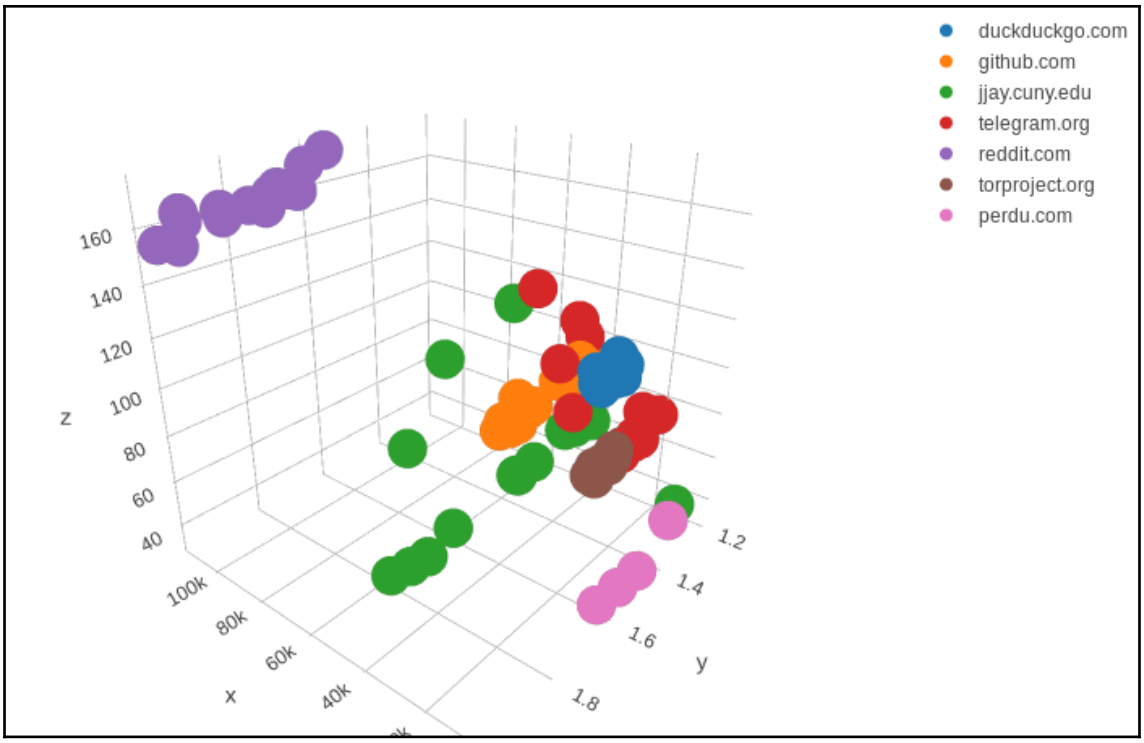


ip_addr	port	cloud_type	method	vendor_name	prod_name	prod_version	prod_trigger	prod_type	prod_vuln	server_header
192.168.56.101	80	Unknown	Crawling	-	-	-	-	-	-	Server: Apache/2.2.8 (Ubuntu) DAV/2
192.168.56.101	80	Unknown	Crawling	php	php	5.2.4	PHP/5.2.4	Language	CVE-2015-8994 CVE-2016-7478 CVE-2008-0599	Server: Apache/2.2.8 (Ubuntu) DAV/2
192.168.56.101	80	Unknown	Crawling	ubuntu	ubuntu_linux	*	(Ubuntu)	OS	CVE-2005-0109 CVE-2004-0882 CVE-2004-0888	Server: Apache/2.2.8 (Ubuntu) DAV/2
192.168.56.101	80	Unknown	Crawling	apache	http_server	2.2.8	Apache/2.2.8	Web	CVE-2016-4975 CVE-2010-0425 CVE-2011-3192	Server: Apache/2.2.8 (Ubuntu) DAV/2

```
et@et-VirtualBox:~/Desktop/website-fingerprinting$ cat config.json
{
  "pcaps": [
    "duckduckgo.com",
    "github.com",
    "jjay.cuny.edu",
    "telegram.org",
    "reddit.com",
    "torproject.org",
    "perdu.com"
  ]
}
```




```
* Parsing configuration
Loading the classifier...
/home/et/.local/lib/python2.7/site-packages/sklearn/base.py:253: UserWarning: Trying to unpickle estimator KNeighborsClassifier from version 0.20.2 when using version 0.20.3. This might lead to breaking code or invalid results. Use at your own risk.
  UserWarning)
OUT: 124, IN: 107, TOTAL: 231, SIZE: 25782, RATIO: 0.862903225806
[[1. 0. 0. 0. 0. 0. 0.]]
[1] Prediction: duckduckgo.com
```



	ack	ack_A	ack_B	bytes	bytes_A	bytes_A_B_ratio	bytes_B	ds_field_A	ds_field_B	duration	...	suffix_is_co.il	suffix_is_com	suffix_is_com.sg	suffix_is_
0	9	5	5	1213	743	0.713924	668	0	0	1.5756	...	0	0	0	
1	9	5	5	1213	743	1.806874	668	0	0	0.6890	...	0	0	0	
2	9	5	5	1213	743	0.103124	668	0	0	0.9852	...	0	0	0	
3	9	5	5	1213	743	1.806874	668	0	0	1.5756	...	0	0	0	
4	9	5	5	1213	743	1.806874	668	0	0	1.5756	...	0	0	0	

5 rows × 298 columns

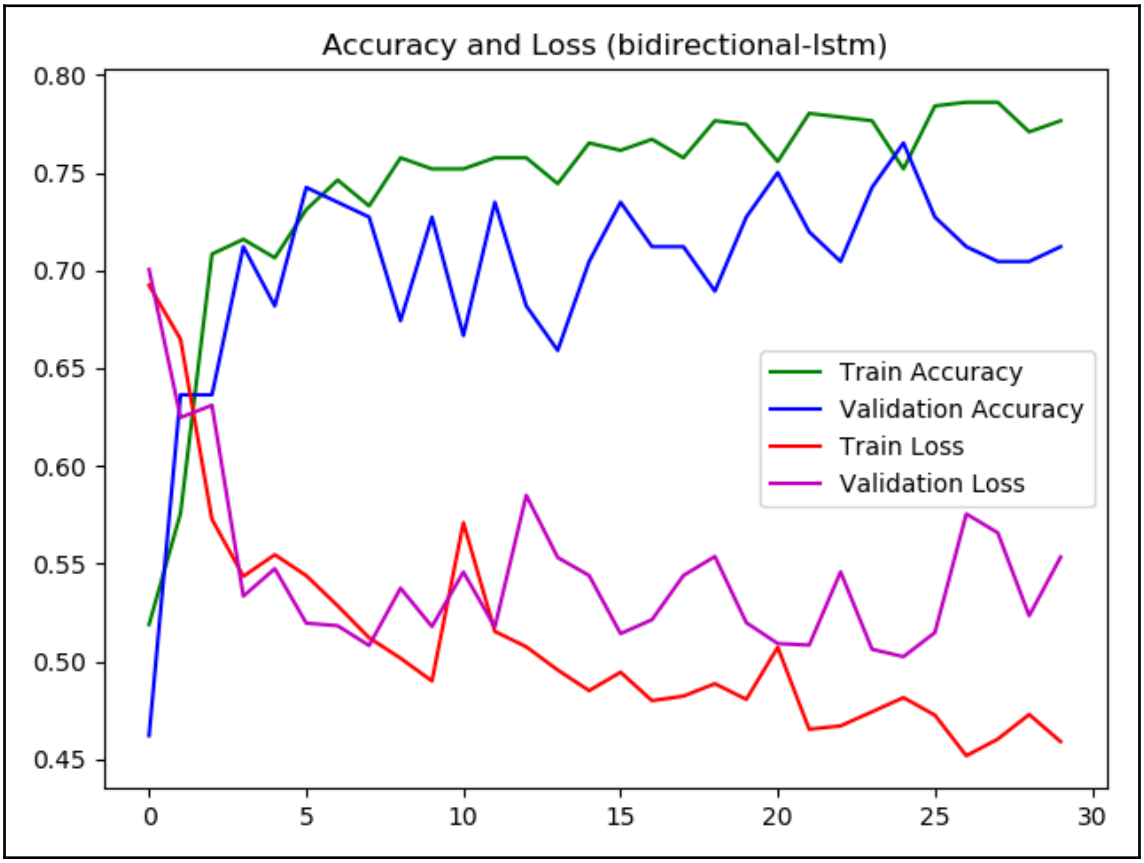
```
et@et-VirtualBox:~/Desktop/keystroke_dynamics-master 2$ python example.py
Choose an option:
  1) create new fingerprint
  2) match text to a existing fingerprint
1



what's your name? Emmanuel
Please write the following text. When you're finished, press Ctrl-C
------------------
Wikipedia is a free-access, free content Internet encyclopedia, supported and hosted by the non-
profit Wikimedia Foundation. Those who can access the site and follow its rules can edit most of
 its articles. Wikipedia is ranked among the ten most popular websites and constitutes the Inter
net's largest and most popular general reference work.
Wikipedia is a free-access, free content Internet encyclopedia, supported and hosted by the non-
profit Wikimedia Foundation. Those who can access the site and follow its rules can edit most of
 its articles. Wikipedia is ranked among the ten most popular websites and constitutes the Inter
net's largest and most popular general reference work.
^C

Finished creating fingerprint!
```

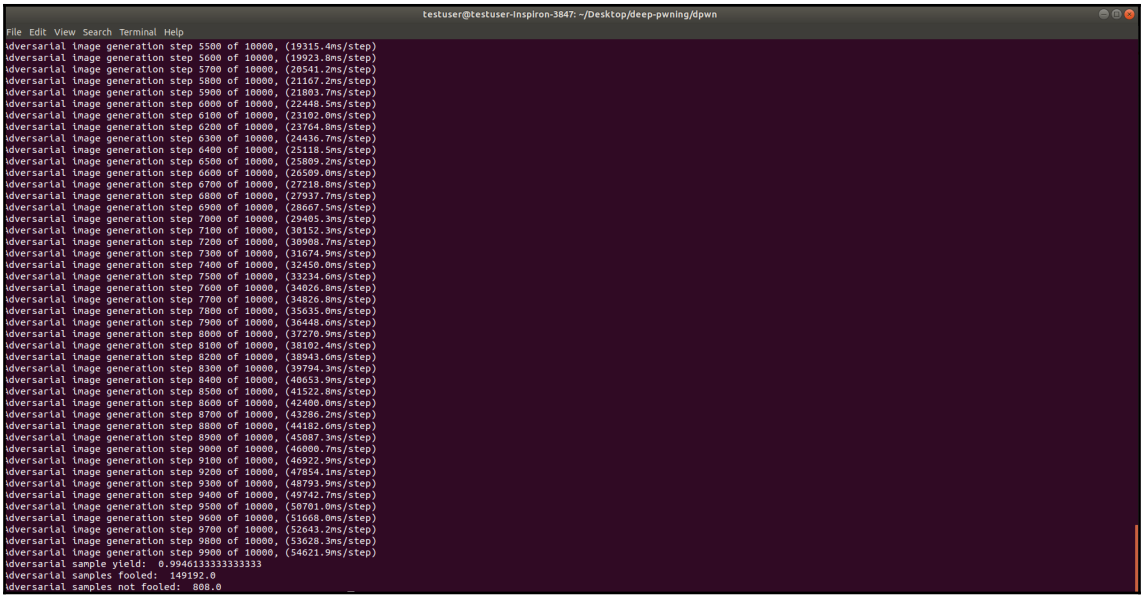
```
et@et-VirtualBox:~/Desktop/keystroke_dynamics-master 2$ python example.py
Choose an option:
  1) create new fingerprint
  2) match text to a existing fingerprint
1



what's your name? Bob
Please write the following text. When you're finished, press Ctrl-C
------------------
Wikipedia is a free-access, free content Internet encyclopedia, supported and hosted by the non-
profit Wikimedia Foundation. Those who can access the site and follow its rules can edit most of
 its articles. Wikipedia is ranked among the ten most popular websites and constitutes the Inter
net's largest and most popular general reference work.
Wikipedia is a free-access, free content Internet encyclopedia, supported and hosted by the non-
profit Wikimedia Foundation. Those who can access the site and follow its rules can edit most of
 its articles. Wikipedia is ranked among the ten most popular websites and consitutes the Intern
et's largest and most popular general reference work.^C

Finished creating fingerprint!
```

```
et@et-VirtualBox:~/Desktop/keystroke_dynamics-master 2$ python example.py
Choose an option:
  1) create new fingerprint
  2) match text to a existing fingerprint
2



Please write the following text. When you're finished, press Ctrl-C
------------------
Wikipedia is a free-access, free content Internet encyclopedia, supported and hosted by the non-
profit Wikimedia Foundation. Those who can access the site and follow its rules can edit most of
 its articles. Wikipedia is ranked among the ten most popular websites and constitutes the Inter
net's largest and most popular general reference work.
Wikipedia is a free-access, free content Internet encyclopedia, supported and hosted by the non-
profit Wikimedia Foundation. Those who can access the site and follow its rules can edit most of
 its articles. Wikiepdia is ranked among the ten most popular websites and constitutes the Inter
net's largest and most popular general reference work.^C

computing similarity for fingerprints:    Fingerprint(Bob)    Fingerprint(NoName)
computing similarity for fingerprints:    Fingerprint(Emmanuel)    Fingerprint(NoName)
Score for Bob: 5.32711338919e-37
Score for Emmanuel: 2.09209471999e-08
Best match:  Emmanuel
```

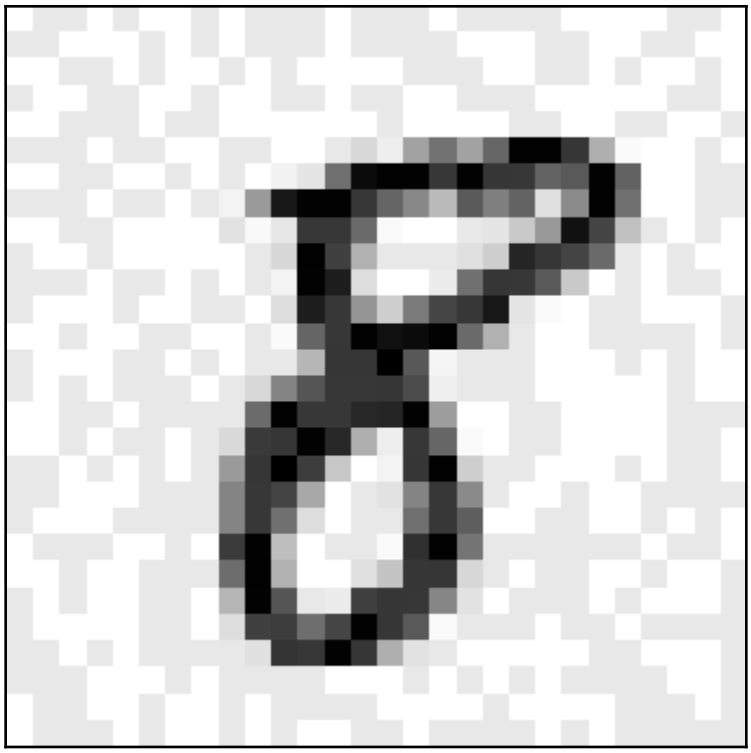
```
Command Prompt
:\Users\ETsukerman\Desktop\Malicious URL Detector\keras-malicious-url-detector>python bidirectional_lstm_train.py
Using TensorFlow backend.
WARNING:tensorflow:From C:\Users\ETsukerman\AppData\Local\Programs\Python\Python37\lib\site-packages\tensorflow\python\framework\op_def_library.py:263: colocate_with (from tensorflow.python.framework.ops) is dep
recated and will be removed in a future version.
Instructions for updating:
Colocations handled automatically by placer.
WARNING:tensorflow:From C:\Users\ETsukerman\AppData\Local\Programs\Python\Python37\lib\site-packages\keras\backend\tensorflow_backend.py:3445: calling dropout (from tensorflow.python.ops.nn_ops) with keep_prob i
s deprecated and will be removed in a future version.
Instructions for updating:
Please use `rate` instead of `keep_prob`. Rate should be set to `rate = 1 - keep_prob`.
WARNING:tensorflow:From C:\Users\ETsukerman\AppData\Local\Programs\Python\Python37\lib\site-packages\tensorflow\python\ops\math_ops.py:3066: to_int32 (from tensorflow.python.ops.math_ops) is deprecated and will
be removed in a future version.
Instructions for updating:
Use tf.cast instead.
Train on 528 samples, validate on 132 samples
Epoch 1/30
2019-04-30 08:29:39.683776: I tensorflow/core/platform/cpu_feature_guard.cc:141] Your CPU supports instructions that this TensorFlow binary was not compiled to use: AVX2
528/528 [==============================] - 6s 11ms/step - loss: 0.6924 - acc: 0.5189 - val_loss: 0.7004 - val_acc: 0.4621
Epoch 2/30
528/528 [==============================] - 5s 10ms/step - loss: 0.6648 - acc: 0.5758 - val_loss: 0.6248 - val_acc: 0.6364
Epoch 3/30
528/528 [==============================] - 4s 8ms/step - loss: 0.5728 - acc: 0.7083 - val_loss: 0.6310 - val_acc: 0.6364
Epoch 4/30
528/528 [==============================] - 5s 9ms/step - loss: 0.5436 - acc: 0.7159 - val_loss: 0.5334 - val_acc: 0.7121
Epoch 5/30
528/528 [==============================] - 5s 9ms/step - loss: 0.5546 - acc: 0.7064 - val_loss: 0.5475 - val_acc: 0.6818
Epoch 6/30
528/528 [==============================] - 4s 8ms/step - loss: 0.5439 - acc: 0.7311 - val_loss: 0.5196 - val_acc: 0.7424
Epoch 7/30
528/528 [==============================] - 4s 8ms/step - loss: 0.5285 - acc: 0.7462 - val_loss: 0.5183 - val_acc: 0.7348
Epoch 8/30
528/528 [==============================] - 4s 8ms/step - loss: 0.5121 - acc: 0.7330 - val_loss: 0.5082 - val_acc: 0.7273
Epoch 9/30
528/528 [==============================] - 4s 8ms/step - loss: 0.5017 - acc: 0.7576 - val_loss: 0.5375 - val_acc: 0.6742
Epoch 10/30
528/528 [==============================] - 4s 8ms/step - loss: 0.4900 - acc: 0.7519 - val_loss: 0.5181 - val_acc: 0.7273
Epoch 11/30
528/528 [==============================] - 4s 8ms/step - loss: 0.5371 - acc: 0.7538 - val_loss: 0.5396 - val_acc: 0.6818
Epoch 12/30
528/528 [==============================] - 4s 8ms/step - loss: 0.4961 - acc: 0.7557 - val_loss: 0.5169 - val_acc: 0.7348
Epoch 13/30
528/528 [==============================] - 4s 8ms/step - loss: 0.5052 - acc: 0.7538 - val_loss: 0.5620 - val_acc: 0.6818
Epoch 14/30
528/528 [==============================] - 4s 8ms/step - loss: 0.4938 - acc: 0.7538 - val_loss: 0.5503 - val_acc: 0.6667
Epoch 15/30
528/528 [==============================] - 4s 8ms/step - loss: 0.4888 - acc: 0.7633 - val_loss: 0.5496 - val_acc: 0.6818
Epoch 16/30
528/528 [==============================] - 4s 8ms/step - loss: 0.4952 - acc: 0.7538 - val_loss: 0.5124 - val_acc: 0.7424
Epoch 17/30
528/528 [==============================] - 4s 8ms/step - loss: 0.4822 - acc: 0.7670 - val_loss: 0.5190 - val_acc: 0.7197
```

```
C:\Users\ETsukerman\Desktop\Malicious URL Detector\keras-malicious-url-detector>python bidirectional_lstm_predict.py
Using TensorFlow backend.
WARNING:tensorflow:From C:\Users\ETsukerman\AppData\Local\Programs\Python\Python37\lib\site-packages\tensorflow\python\framework\op_def_library.py:263: colocate_with (from tensorflow.python.framework.ops) is
recated and will be removed in a future version.
Instructions for updating:
Colocations handled automatically by placer.
WARNING:tensorflow:From C:\Users\ETsukerman\AppData\Local\Programs\Python\Python37\lib\site-packages\keras\backend\tensorflow_backend.py:3445: calling dropout (from tensorflow.python.ops.nn_ops) with keep_prob
s deprecated and will be removed in a future version.
Instructions for updating:
Please use `rate` instead of `keep_prob`. Rate should be set to `rate = 1 - keep_prob`.
2019-04-30 08:42:08.589978: I tensorflow/core/platform/cpu_feature_guard.cc:141] Your CPU supports instructions that this TensorFlow binary was not compiled to use: AVX2
http://naver.com. predicted: 0 actual: 0
http://google.com.hk. predicted: 0 actual: 0
http://reddit.com. predicted: 0 actual: 0
http://newyorkrealestate.eu. predicted: 1 actual: 1
http://siteadvisor.com. predicted: 1 actual: 0
http://google.co.ve. predicted: 0 actual: 0
http://best-cv-templates.com. predicted: 1 actual: 1
http://lademejeanne.fr. predicted: 1 actual: 1
http://vube.com. predicted: 0 actual: 0
http://www.docentesenterrianos.com/coldwellbanker.com/googledoc/index.htm. predicted: 1 actual: 1
http://archive.org. predicted: 1 actual: 0
http://speedtest.net. predicted: 1 actual: 0
http://ikea.com. predicted: 0 actual: 0
http://axebet.com. predicted: 0 actual: 1
http://clickpage.net. predicted: 1 actual: 1
http://clkmon.com. predicted: 0 actual: 0
http://beeg.com. predicted: 0 actual: 0
http://vai.la. predicted: 1 actual: 1
http://google.com. predicted: 0 actual: 0
http://plus.lapvo3.tk. predicted: 1 actual: 1
http://bbc.co.uk. predicted: 0 actual: 0
```






```
File  Edit  View  Search  Terminal  Help
testuser@testuser-Inspiron-3847:~/Desktop/deep-pwning/dpwn/output/mnist/pickle$ python3
Python 3.6.7 (default, Oct 22 2018, 11:32:17)
[GCC 8.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import pickle
>>> advImagesUnpickle = pickle.load(open("generated-adv-images.pkl","rb"))
>>> advImagesUnpickle.shape
(150000, 11)
>>> advImagesUnpickle.iloc[0]
Adversarial Image              [[[[-0.49], [-0.51], [-0.51], [-0.49], [-0.51]...
Gradient                       [[[[ 0.0571566 ]\n [-0.21229117]\n [-0.128913...
Gradient Norm                  [[[0.057156596], [0.21229117], [0.12891318], [...
Gradient Step                                                             0.01
Idx                                                                          0
Image                          [[[-0.5], [-0.5], [-0.5], [-0.5], [-0.5], [-0....
Predicted Label                                                              8
Predicted Label Adversarial                                                  8
Predicted Prob                 [[0.023965867, 0.20235294, 0.0024297407, 0.002...
Predicted Prob Adversarial     [[0.019035637, 0.17733964, 0.0020470265, 0.002...
True Label                                                                   7
Name: 0, dtype: object
>>>
```



cwe119_cgd - Notepad

File Edit Format View Help

```
1 CVE-2010-1444/vlc_media_player_1.1.0_CVE-2010-1444_zipstream.c cfunc 449
ZIP_FILENAME_LEN, NULL, 0, NULL, 0 )
char *psz_fileName = calloc( ZIP_FILENAME_LEN, 1 );
if( unzGetCurrentFileInfo( file, p_fileInfo, psz_fileName,
vlc_array_append( p_filenames, strdup( psz_fileName ) );
free( psz_fileName );
0
----------------------------------
2 CVE-2010-1444/vlc_media_player_1.1.0_CVE-2010-1444_zipstream.c cppfunc 449
char *psz_fileName = calloc( ZIP_FILENAME_LEN, 1 );
ZIP_FILENAME_LEN, NULL, 0, NULL, 0 )
if( unzGetCurrentFileInfo( file, p_fileInfo, psz_fileName,
vlc_array_append( p_filenames, strdup( psz_fileName ) );
free( psz_fileName );
0
----------------------------------
3 CVE-2011-2896/cups_1.4.2_CVE-2011-2896_image-gif.c inputfunc 100
fread(buf, 13, 1, fp);
img->xsize = (buf[7] << 8) | buf[6];
img->ysize = (buf[9] << 8) | buf[8];
ncolors    = 2 << (buf[10] & 0x07);
if (buf[10] & GIF_COLORMAP)
if (gif_read_cmap(fp, ncolors, cmap, &gray))
switch (getc(fp))
fclose(fp);
buf[0] = getc(fp);
if (buf[0] == 0xf9)
gif_get_block(fp, buf);
fread(buf, 9, 1, fp);
if (buf[8] & GIF_COLORMAP)
ncolors = 2 << (buf[8] & 0x07);
if (gif_read_cmap(fp, ncolors, cmap, &gray))
img->xsize = (buf[5] << 8) | buf[4];
img->ysize = (buf[7] << 8) | buf[6];
if (img->xsize == 0 || img->ysize == 0)
img->xsize, img->ysize);
fprintf(stderr, "DEBUG: Bad GIF image dimensions: %dx%d\n",
fclose(fp);
i = gif_read_image(fp, img, cmap, buf[8] & GIF_INTERLACE);
int interlace);
i = gif_read_image(fp, img, cmap, buf[8] & GIF_INTERLACE);
static int      gif_read_cmap(FILE *fp, int ncolors, gif_cmap_t cmap,
fclose(fp);
```

```
C:\Users\ETsukerman\Desktop\Machine Learning for Cybersecurity Cookbook Code\Chapter05\Deep Learning-Based System for Automatic Detection of Software Vulnerabilities>python vuldeepecker_train.py datasets\cwe119
-gd.txt
Using TensorFlow backend.
Found 2697 forward slices and 37056 backward slices

Training model...
Processing gadgets... 39753
WARNING:tensorflow:From C:\Users\ETsukerman\AppData\Local\Programs\Python\Python37\lib\site-packages\tensorflow\python\framework\op_def_library.py:263: colocate_with (from tensorflow.python.framework.ops) is
recated and will be removed in a future version.
Instructions for updating:
Colocations handled automatically by placer.
WARNING:tensorflow:From C:\Users\ETsukerman\AppData\Local\Programs\Python\Python37\lib\site-packages\keras\backend\tensorflow_backend.py:3445: calling dropout (from tensorflow.python.ops.nn_ops) with keep_prob
s deprecated and will be removed in a future version.
Instructions for updating:
Please use `rate` instead of `keep_prob`. Rate should be set to `rate = 1 - keep_prob`.
WARNING:tensorflow:From C:\Users\ETsukerman\AppData\Local\Programs\Python\Python37\lib\site-packages\tensorflow\python\ops\math_ops.py:3066: to_int32 (from tensorflow.python.ops.math_ops) is deprecated and will
be removed in a future version.
Instructions for updating:
Use tf.cast instead.
Epoch 1/4
2019-05-09 12:09:31.071435: I tensorflow/core/platform/cpu_feature_guard.cc:141] Your CPU supports instructions that this TensorFlow binary was not compiled to use: AVX2
16704/16704 [==============================] - 54s 3ms/step - loss: 0.6001 - acc: 0.6640
Epoch 2/4
16704/16704 [==============================] - 54s 3ms/step - loss: 0.5315 - acc: 0.7296
Epoch 3/4
16704/16704 [==============================] - 55s 3ms/step - loss: 0.5083 - acc: 0.7466
Epoch 4/4
16704/16704 [==============================] - 56s 3ms/step - loss: 0.4849 - acc: 0.7597
4176/4176 [==============================] - 5s 1ms/step
Accuracy is... 0.7708333333333334
False positive rate is... 0.3309386973180077
False negative rate is... 0.12739463601532566
True positive rate is... 0.8726053639846744
Precision is... 0.7250298448070036
F1 score is... 0.7920017387524451
```

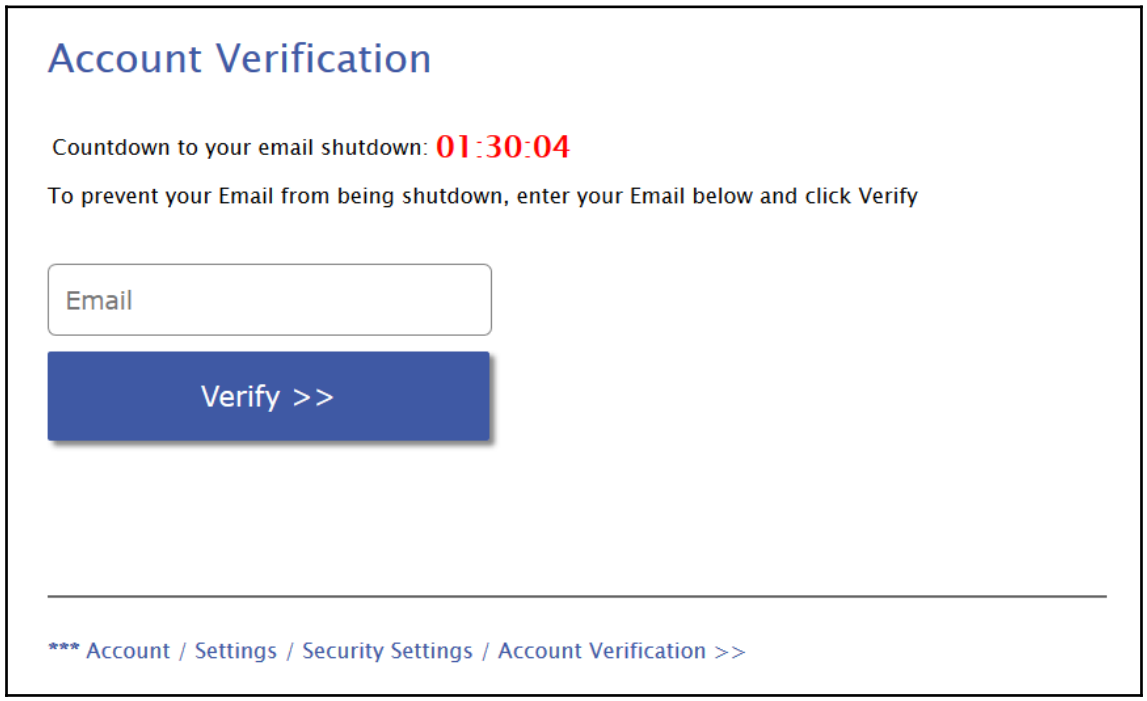
some_gadgets - Notepad

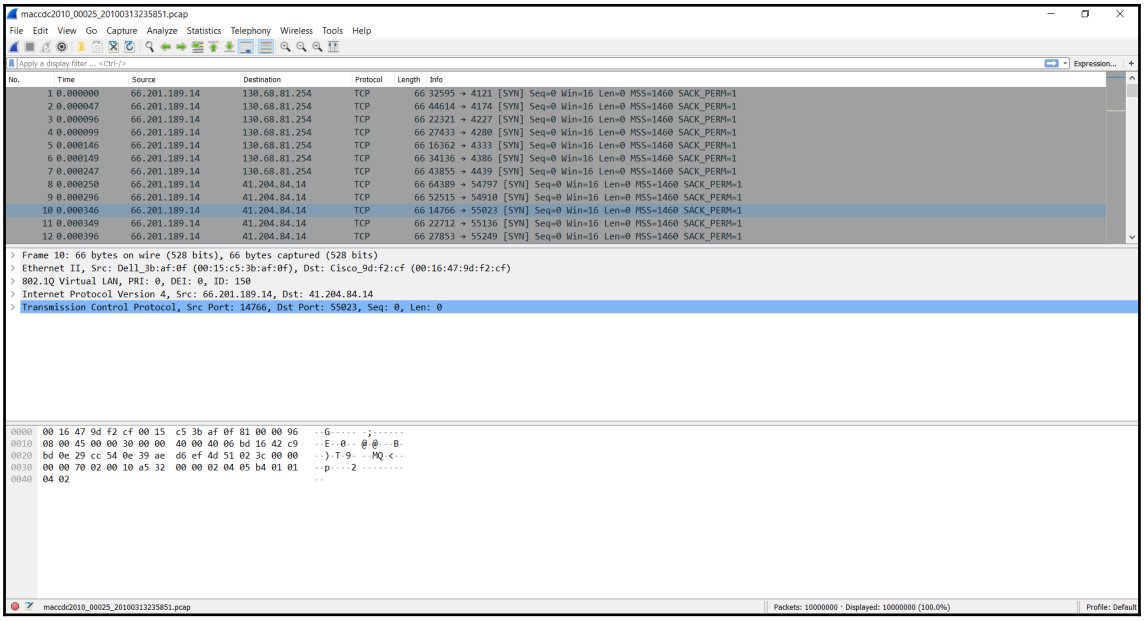
File Edit Format View Help

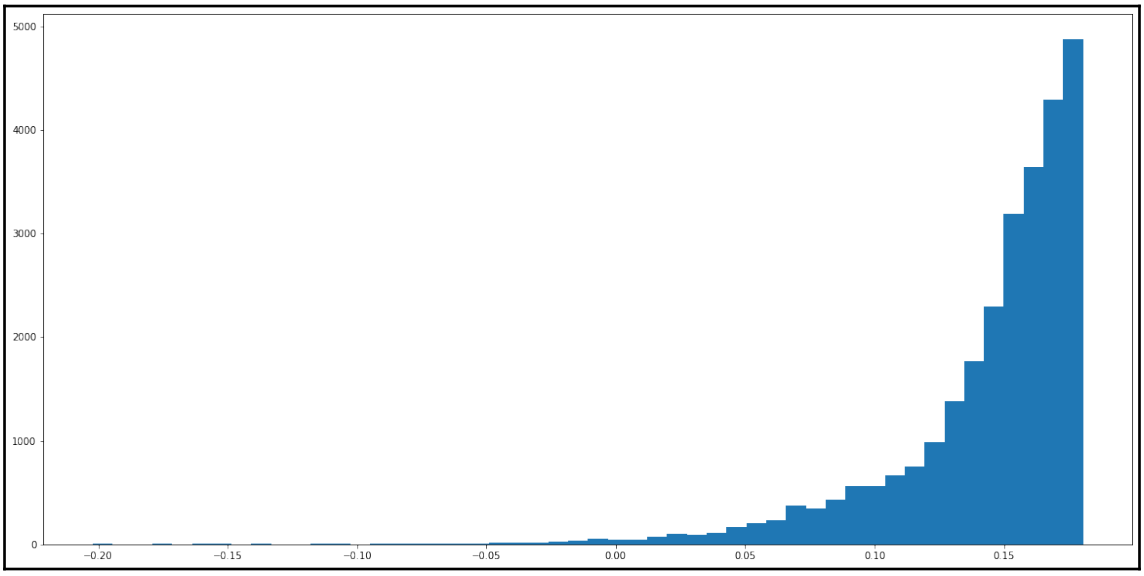
```
4 CVE-2013-1706/Firefox_22.0b6_CVE_2013_1706_toolkit_components_maintenanceservice_workmonitor.cpp cppfunc 111
WCHAR installDir[MAX_PATH + 1] = {L'\0'};
if (!GetInstallationDir(argc, argv, installDir)) {
GetInstallationDir(int argcTmp, LPWSTR *argvTmp, WCHAR aResultDir[MAX_PATH + 1])
wcsncpy(aResultDir, argvTmp[2], MAX_PATH);
WCHAR* backSlash = wcsrchr(aResultDir, L'\\');
0
----------------------------------
5 CVE-2013-1732/Firefox_20.0.1_CVE_2013_1732_layout_generic_nsBlockFrame.cpp cfunc 196
DumpStyleGeneaology(nsIFrame* aFrame, const char* gap)
nsFrame::ListTag(stdout, aFrame);
nsStyleContext* sc = aFrame->GetStyleContext();
printf("%p ", sc);
psc = sc->GetParent();
sc = psc;
printf("%p ", sc);
0
----------------------------------
```

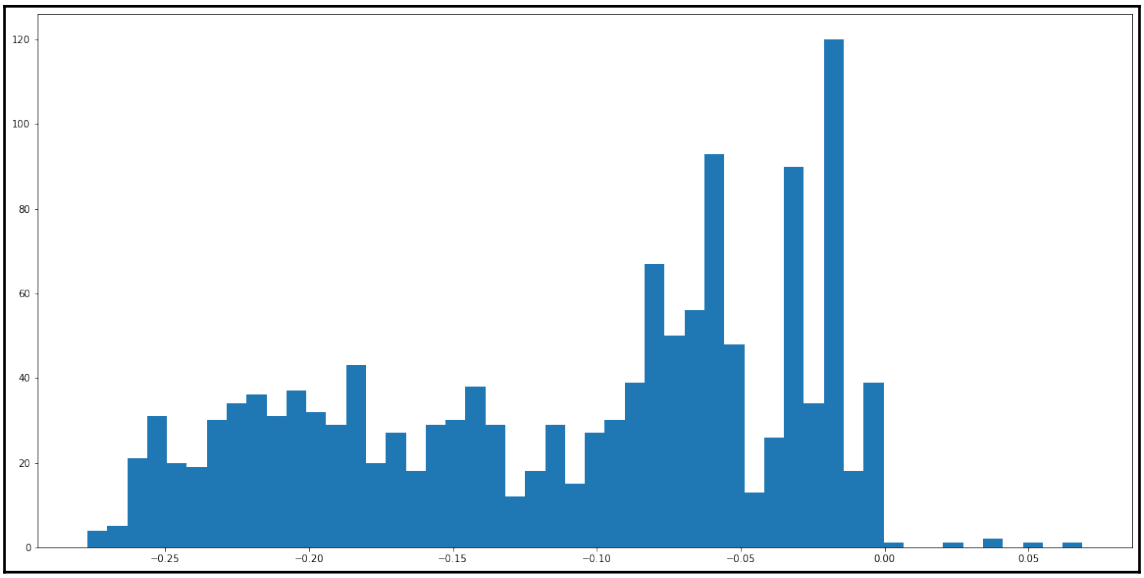
```
C:\Users\ETsukerman\Desktop\Machine Learning for Cybersecurity Cookbook Code\Chapter05\Deep Learning-Based System for Automatic Detection of Software Vulnerabilities>python vuldeepecker_predict.py datasets\some_
gadgets.txt cwe119_cgd_model.h5
Using TensorFlow backend.
Found 0 forward slices and 2 backward slices

Training model...
Processing gadgets... 2
WARNING:tensorflow:From C:\Users\ETsukerman\AppData\Local\Programs\Python\Python37\lib\site-packages\tensorflow\python\framework\op_def_library.py:263: colocate_with (from tensorflow.python.framework.ops) is dep
recated and will be removed in a future version.
Instructions for updating:
Colocations handled automatically by placer.
WARNING:tensorflow:From C:\Users\ETsukerman\AppData\Local\Programs\Python\Python37\lib\site-packages\keras\backend\tensorflow_backend.py:3445: calling dropout (from tensorflow.python.ops.nn_ops) with keep_prob i
s deprecated and will be removed in a future version.
Instructions for updating:
Please use `rate` instead of `keep_prob`. Rate should be set to `rate = 1 - keep_prob`.
2019-05-09 12:21:57.663411: I tensorflow/core/platform/cpu_feature_guard.cc:141] Your CPU supports instructions that this TensorFlow binary was not compiled to use: AVX2
[[1. 0.]
 [1. 0.]]
```

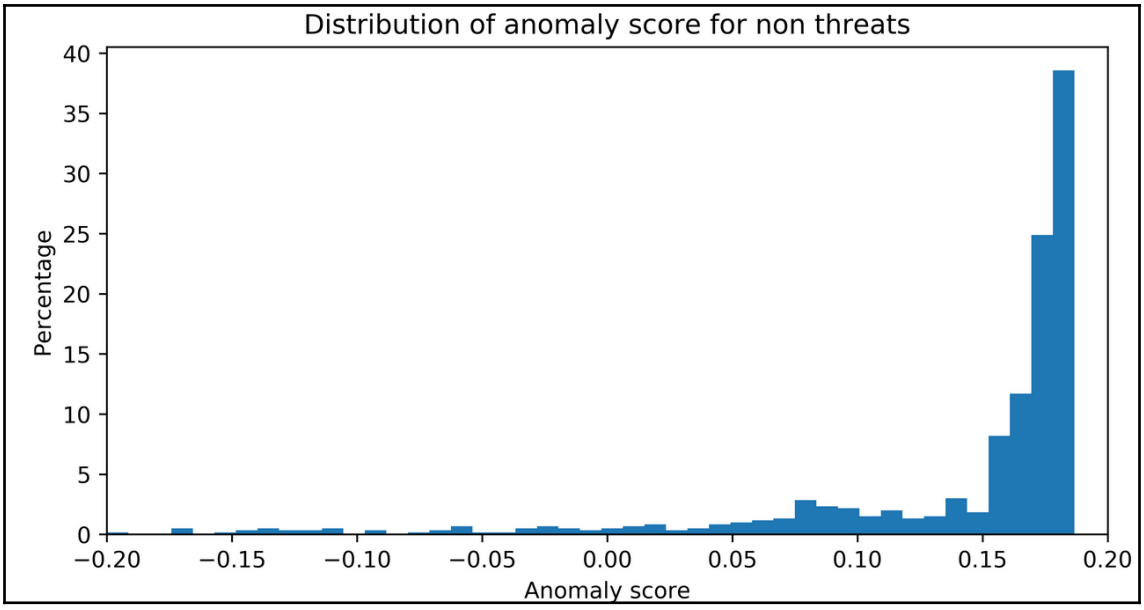
Chapter 6: Automatic Intrusion Detection

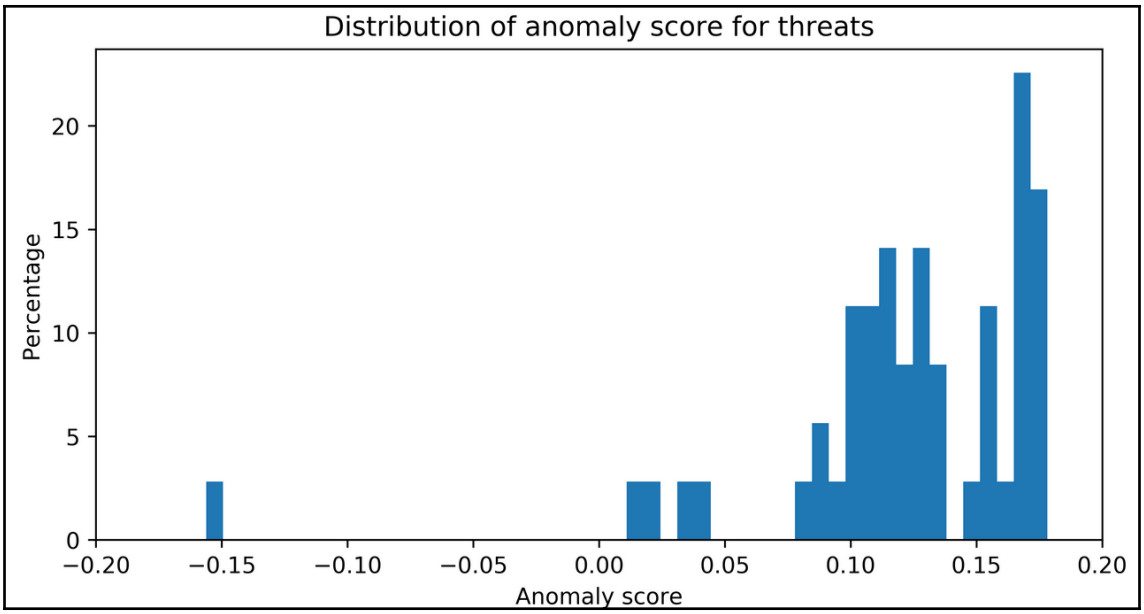



maccdc2010_00025_20100313235851.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
1 0.000000 66.201.189.14 130.68.81.254 TCP 66 32595 → 4121 [SYN] Seq=0 Win=16 Len=0 MSS=1460 SACK_PERM=1
2 0.000047 66.201.189.14 130.68.81.254 TCP 66 44614 → 4174 [SYN] Seq=0 Win=16 Len=0 MSS=1460 SACK_PERM=1
3 0.000096 66.201.189.14 130.68.81.254 TCP 66 22321 → 4227 [SYN] Seq=0 Win=16 Len=0 MSS=1460 SACK_PERM=1
4 0.000099 66.201.189.14 130.68.81.254 TCP 66 27433 → 4280 [SYN] Seq=0 Win=16 Len=0 MSS=1460 SACK_PERM=1
5 0.000146 66.201.189.14 130.68.81.254 TCP 66 16362 → 4333 [SYN] Seq=0 Win=16 Len=0 MSS=1460 SACK_PERM=1
6 0.000149 66.201.189.14 130.68.81.254 TCP 66 34136 → 4386 [SYN] Seq=0 Win=16 Len=0 MSS=1460 SACK_PERM=1
7 0.000247 66.201.189.14 130.68.81.254 TCP 66 43855 → 4439 [SYN] Seq=0 Win=16 Len=0 MSS=1460 SACK_PERM=1
8 0.000250 66.201.189.14 41.204.84.14 TCP 66 64389 → 54797 [SYN] Seq=0 Win=16 Len=0 MSS=1460 SACK_PERM=1
9 0.000296 66.201.189.14 41.204.84.14 TCP 66 52515 → 54910 [SYN] Seq=0 Win=16 Len=0 MSS=1460 SACK_PERM=1
10 0.000346 66.201.189.14 41.204.84.14 TCP 66 14766 → 55023 [SYN] Seq=0 Win=16 Len=0 MSS=1460 SACK_PERM=1
11 0.000349 66.201.189.14 41.204.84.14 TCP 66 22712 → 55136 [SYN] Seq=0 Win=16 Len=0 MSS=1460 SACK_PERM=1
12 0.000396 66.201.189.14 41.204.84.14 TCP 66 27853 → 55249 [SYN] Seq=0 Win=16 Len=0 MSS=1460 SACK_PERM=1
Frame 10: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: Dell_3b:af:0f (00:15:c5:3b:af:0f), Dst: Cisco_9d:f2:cf (00:16:47:9d:f2:cf)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 150
Internet Protocol Version 4, Src: 66.201.189.14, Dst: 41.204.84.14
Transmission Control Protocol, Src Port: 14766, Dst Port: 55023, Seq: 0, Len: 0
0000 00 16 47 9d f2 cf 00 15 c5 3b af 0f 81 00 00 96
0010 08 00 45 00 00 30 00 00 40 00 40 06 bd 16 42 c9
0020 bd 0e 29 cc 54 0e 39 ae d6 ef 4d 51 02 3c 00 00
0030 00 00 70 02 00 10 a5 32 00 00 02 04 05 b4 01 01
0040 04 02
Packets: 10000000 · Displayed: 10000000 (100.0%)
Profile: Default


5000
4000
3000
2000
1000
0
−0.20
−0.15
−0.10
−0.05
0.00
0.05
0.10
0.15


120
100
80
60
40
20
0
−0.25
−0.20
−0.15
−0.10
−0.05
0.00
0.05


Distribution of anomaly score for non threats
Percentage
Anomaly score
40
35
30
25
20
15
10
5
0
−0.20
−0.15
−0.10
−0.05
0.00
0.05
0.10
0.15
0.20



In [104]:
```
df.head()
```

Out[104]:

	0	1	2	3	4	5	6	7	8	9	...	1549	1550	1551	1552	1553	1554	1555	1556	1557	label
0	125	125	1.0	1	0	0	0	0	0	0	...	0	0	0	0	0	0	0	0	0	ad.
1	57	468	8.2105	1	0	0	0	0	0	0	...	0	0	0	0	0	0	0	0	0	ad.
2	33	230	6.9696	1	0	0	0	0	0	0	...	0	0	0	0	0	0	0	0	0	ad.
3	60	468	7.8	1	0	0	0	0	0	0	...	0	0	0	0	0	0	0	0	0	ad.
4	60	468	7.8	1	0	0	0	0	0	0	...	0	0	0	0	0	0	0	0	0	ad.

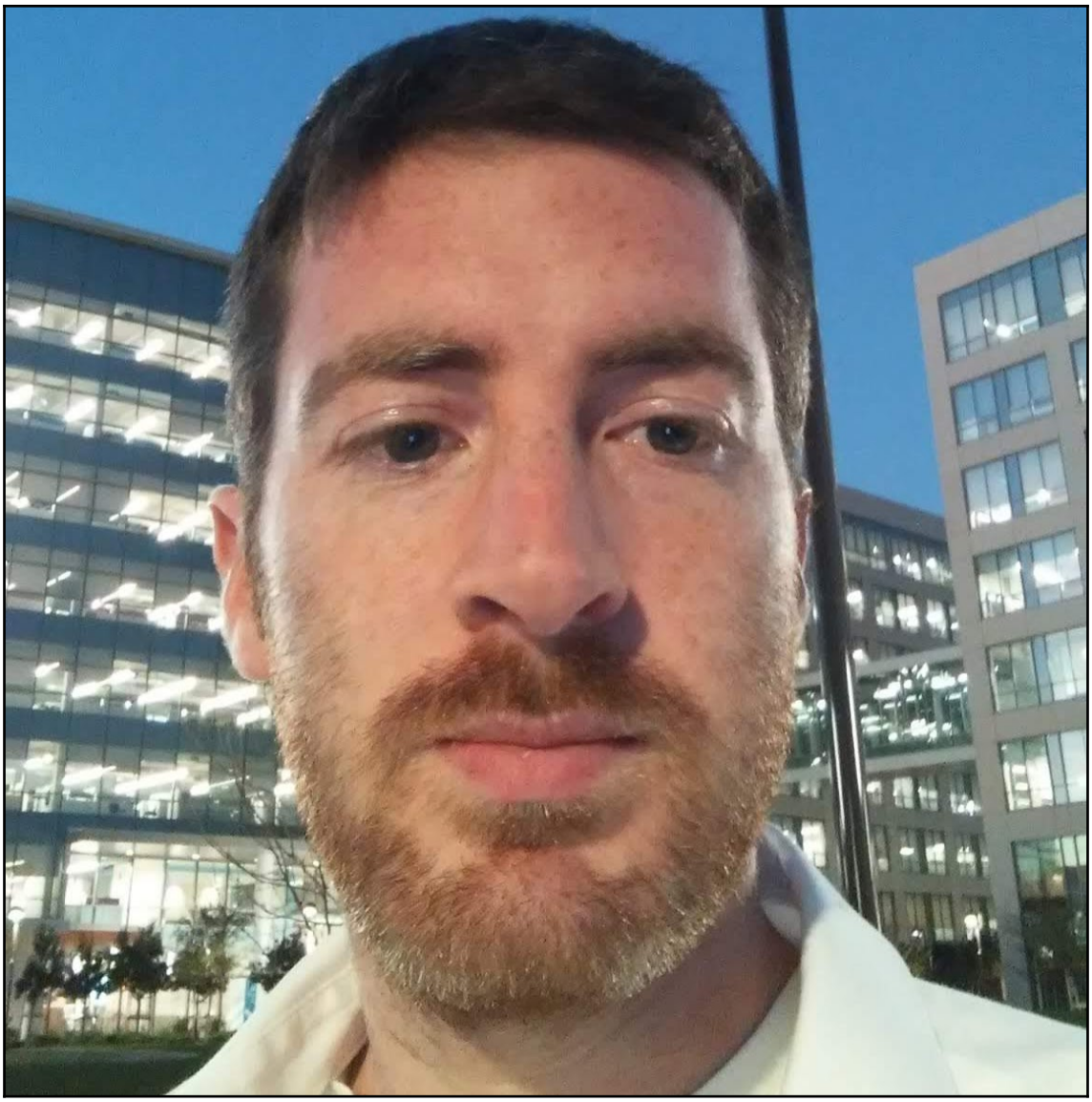
5 rows × 1559 columns

Chapter 7: Securing and Attacking Data with Machine Learning

```
emmanueltsukerman@instance-2:~/PassGAN$ curl -L -o data/train.txt https://github.com/brannondorsey/PassGAN/releases
/download/data/rockyou-train.txt
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   608    0   608    0     0   1601      0 --:--:-- --:--:-- --:--:--  1600
100  164M  100  164M    0     0  3761k      0  0:00:44  0:00:44 --:--:-- 5602k
```

```
emmanueltsukerman@instance-2:~/PassGAN$ python sample.py \
> --input-dir pretrained \
> --checkpoint pretrained/checkpoints/195000.ckpt \
> --output gen_passwords.txt \
> --batch-size 1024 \
> --num-samples 10000
WARNING:tensorflow:From /usr/local/lib/python2.7/dist-packages/tensorflow/python/framework/op_def_library.py:263:
olocate_with (from tensorflow.python.framework.ops) is deprecated and will be removed in a future version.
Instructions for updating:
Colocations handled automatically by placer.
WARNING:tensorflow:From /home/emmanueltsukerman/PassGAN/tflib/ops/conv1d.py:93: calling conv1d (from tensorflow.pyth
on.ops.nn_ops) with data_format=NCHW is deprecated and will be removed in a future version.
Instructions for updating:
`NCHW` for data_format is deprecated, use `NCW` instead
2019-05-11 05:42:30.779382: I tensorflow/stream_executor/cuda/cuda_gpu_executor.cc:998] successful NUMA node read
rom SysFS had negative value (-1), but there must be at least one NUMA node, so returning NUMA node zero
2019-05-11 05:42:30.781860: I tensorflow/compiler/xla/service/service.cc:161] XLA service 0x55f76149c180 executing
computations on platform CUDA. Devices:
2019-05-11 05:42:30.781981: I tensorflow/compiler/xla/service/service.cc:168]   StreamExecutor device (0): Tesla K8
0, Compute Capability 3.7
2019-05-11 05:42:30.810848: I tensorflow/core/platform/profile_utils/cpu_utils.cc:94] CPU Frequency: 2199995000 Hz
2019-05-11 05:42:30.811089: I tensorflow/compiler/xla/service/service.cc:161] XLA service 0x55f761508ca0 executing
computations on platform Host. Devices:
2019-05-11 05:42:30.811232: I tensorflow/compiler/xla/service/service.cc:168]   StreamExecutor device (0): <undefin
ed>, <undefined>
2019-05-11 05:42:30.811599: I tensorflow/core/common_runtime/gpu/gpu_device.cc:1433] Found device 0 with properties
:
name: Tesla K80 major: 3 minor: 7 memoryClockRate(GHz): 0.8235
pciBusID: 0000:00:04.0
totalMemory: 11.17GiB freeMemory: 11.10GiB
2019-05-11 05:42:30.811881: I tensorflow/core/common_runtime/gpu/gpu_device.cc:1512] Adding visible gpu devices: 0
2019-05-11 05:42:32.651256: I tensorflow/core/common_runtime/gpu/gpu_device.cc:984] Device interconnect StreamExecu
tor with strength 1 edge matrix:
2019-05-11 05:42:32.651488: I tensorflow/core/common_runtime/gpu/gpu_device.cc:990]      0
2019-05-11 05:42:32.651612: I tensorflow/core/common_runtime/gpu/gpu_device.cc:1003] 0:   N
2019-05-11 05:42:32.651993: I tensorflow/core/common_runtime/gpu/gpu_device.cc:1115] Created TensorFlow device
b:localhost/replica:0/task:0/device:GPU:0 with 10754 MB memory) -> physical GPU (device: 0, name: Tesla K80, pci bu
s id: 0000:00:04.0, compute capability: 3.7)
WARNING:tensorflow:From /usr/local/lib/python2.7/dist-packages/tensorflow/python/training/saver.py:1266: checkpoint
_exists (from tensorflow.python.training.checkpoint_management) is deprecated and will be removed in a future versi
on.
Instructions for updating:
Use standard file APIs to check for files with this prefix.
2019-05-11 05:42:33.218162: I tensorflow/stream_executor/dso_loader.cc:153] successfully opened CUDA library libcub
las.so.10.0 locally
finished in 3.06 seconds
```

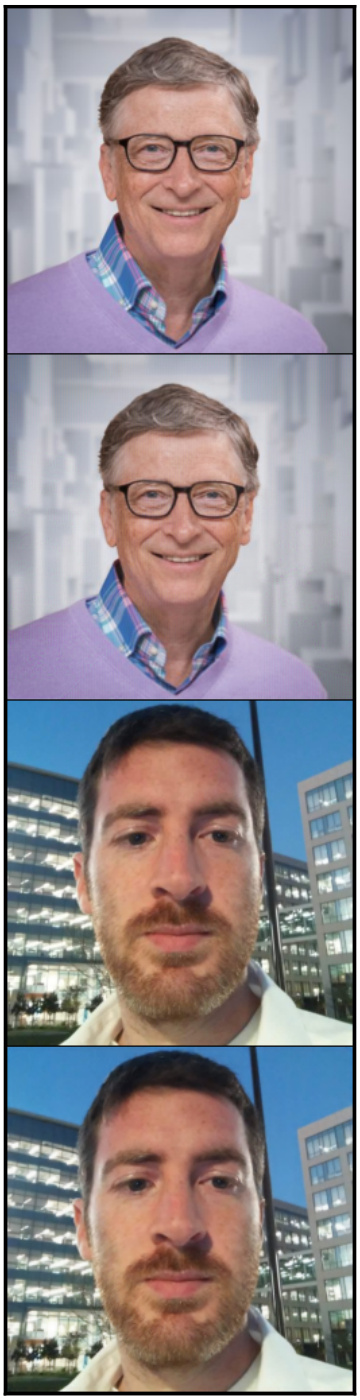
```
emmanueltsukerman@instance-2:~/PassGAN$ head -10 gen_passwords.txt
149032
9101ja
namalo
harrien
teugaj
0122060
notch
yudla1
0105263
mariosa
```

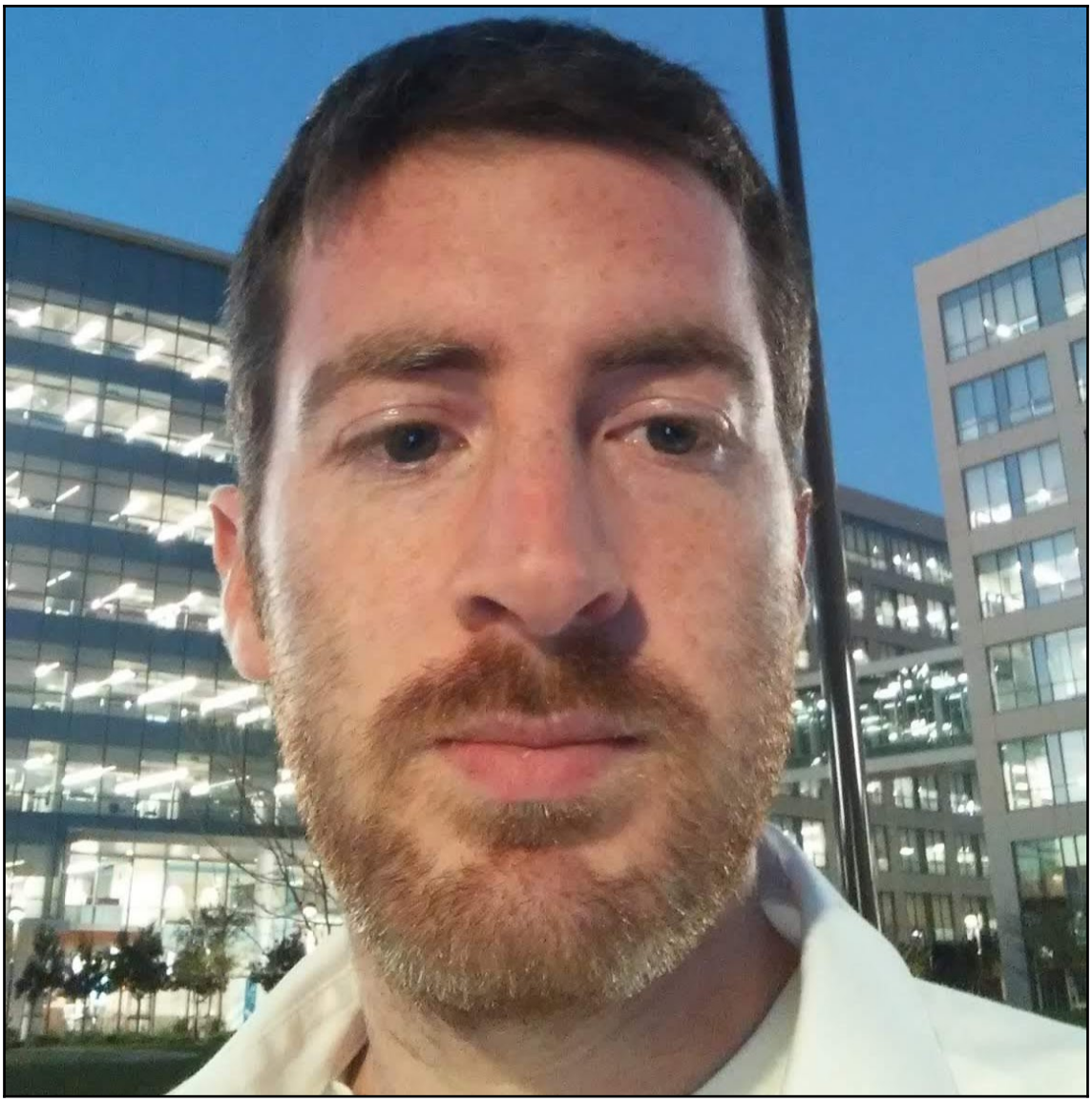


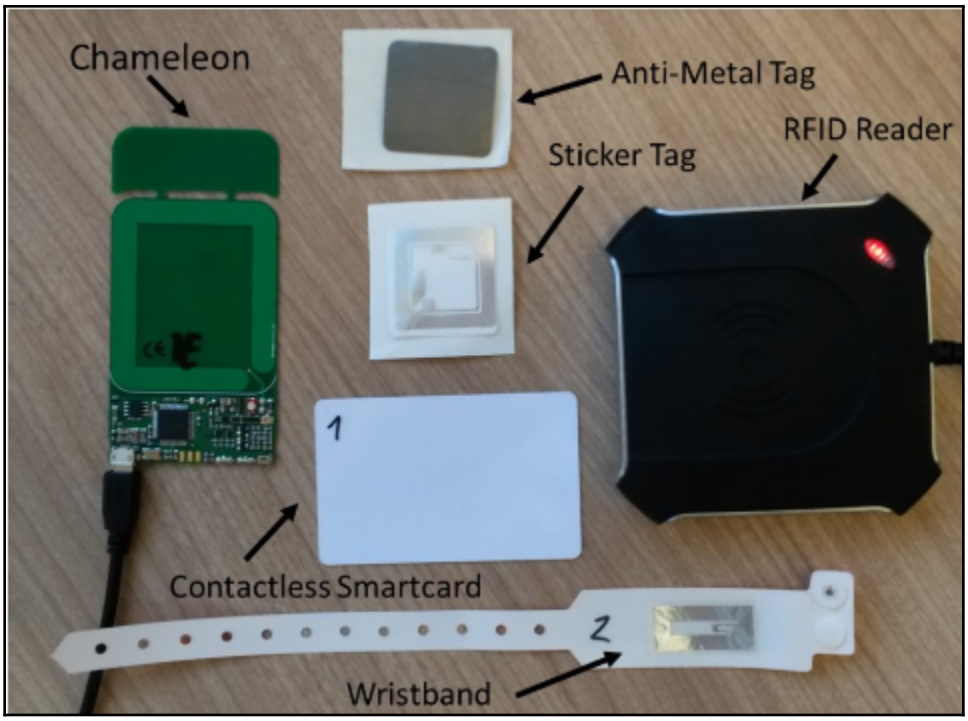
```
emanuel@yokoamainstance 2:~/pyTorch-Deep-Image-Steganography$ CUDA_VISIBLE_DEVICES=0 python3 main.py --test=./example_pics
Namespace(Hnet='', Rnet='', batchSize=32, beta=0.75, beta1=0.5, cuda=True, dataset='train', debug=False, decay_round=10, hostname='instance-2', imageSize=256, logFrequency=10, lr=0.001, ngpu=1, ni
ter=100, outckpts='./training/instance-2_2019-05-11-14_25_31/checkPoints', outcodes='./training/instance-2_2019-05-11-14_25_31/codes', outlogs='./training/instance-2_2019-05-11-14_25_31/trainingLo
gs', remark='', resultPicFrequency=100, test='./example_pics', testPics='./training/instance-2_2019-05-11-14_25_31/testPics', trainpics='./training/instance-2_2019-05-11-14_25_31/trainPics', valid
ationpics='./training/instance-2_2019-05-11-14_25_31/validationPics', workers=8)
UnetGenerator(
  (model): UnetSkipConnectionBlock(
    (model): Sequential(
      (0): Conv2d(6, 64, kernel_size=(4, 4), stride=(2, 2), padding=(1, 1), bias=False)
      (1): UnetSkipConnectionBlock(
        (model): Sequential(
          (0): LeakyReLU(negative_slope=0.2, inplace)
          (1): Conv2d(64, 128, kernel_size=(4, 4), stride=(2, 2), padding=(1, 1), bias=False)
          (2): BatchNorm2d(128, eps=1e-05, momentum=0.1, affine=True, track_running_stats=True)
          (3): UnetSkipConnectionBlock(
            (model): Sequential(
              (0): LeakyReLU(negative_slope=0.2, inplace)
              (1): Conv2d(128, 256, kernel_size=(4, 4), stride=(2, 2), padding=(1, 1), bias=False)
              (2): BatchNorm2d(256, eps=1e-05, momentum=0.1, affine=True, track_running_stats=True)
              (3): UnetSkipConnectionBlock(
                (model): Sequential(
                  (0): LeakyReLU(negative_slope=0.2, inplace)
                  (1): Conv2d(256, 512, kernel_size=(4, 4), stride=(2, 2), padding=(1, 1), bias=False)
                  (2): BatchNorm2d(512, eps=1e-05, momentum=0.1, affine=True, track_running_stats=True)
                  (3): UnetSkipConnectionBlock(
                    (model): Sequential(
                      (0): LeakyReLU(negative_slope=0.2, inplace)
                      (1): Conv2d(512, 512, kernel_size=(4, 4), stride=(2, 2), padding=(1, 1), bias=False)
                      (2): BatchNorm2d(512, eps=1e-05, momentum=0.1, affine=True, track_running_stats=True)
                      (3): UnetSkipConnectionBlock(
                        (model): Sequential(
                          (0): LeakyReLU(negative_slope=0.2, inplace)
                          (1): Conv2d(512, 512, kernel_size=(4, 4), stride=(2, 2), padding=(1, 1), bias=False)
                          (2): BatchNorm2d(512, eps=1e-05, momentum=0.1, affine=True, track_running_stats=True)
                          (3): UnetSkipConnectionBlock(
                            (model): Sequential(
                              (0): LeakyReLU(negative_slope=0.2, inplace)
                              (1): Conv2d(512, 512, kernel_size=(4, 4), stride=(2, 2), padding=(1, 1), bias=False)
                              (2): ReLU(inplace)
                              (3): ConvTranspose2d(512, 512, kernel_size=(4, 4), stride=(2, 2), padding=(1, 1), bias=False)
                              (4): BatchNorm2d(512, eps=1e-05, momentum=0.1, affine=True, track_running_stats=True)
                            )
                          )
                          (4): ReLU(inplace)
                          (5): ConvTranspose2d(1024, 512, kernel_size=(4, 4), stride=(2, 2), padding=(1, 1), bias=False)
                          (6): BatchNorm2d(512, eps=1e-05, momentum=0.1, affine=True, track_running_stats=True)
                        )
                      )
```

```
                    )
                  )
                  (4): ReLU(inplace)
                  (5): ConvTranspose2d(1024, 512, kernel_size=(4, 4), stride=(2, 2), padding=(1, 1), bias=False)
                  (6): BatchNorm2d(512, eps=1e-05, momentum=0.1, affine=True, track_running_stats=True)
                )
              )
              (4): ReLU(inplace)
              (5): ConvTranspose2d(1024, 256, kernel_size=(4, 4), stride=(2, 2), padding=(1, 1), bias=False)
              (6): BatchNorm2d(256, eps=1e-05, momentum=0.1, affine=True, track_running_stats=True)
            )
          )
          (4): ReLU(inplace)
          (5): ConvTranspose2d(512, 128, kernel_size=(4, 4), stride=(2, 2), padding=(1, 1), bias=False)
          (6): BatchNorm2d(128, eps=1e-05, momentum=0.1, affine=True, track_running_stats=True)
        )
      )
      (4): ReLU(inplace)
      (5): ConvTranspose2d(256, 64, kernel_size=(4, 4), stride=(2, 2), padding=(1, 1), bias=False)
      (6): BatchNorm2d(64, eps=1e-05, momentum=0.1, affine=True, track_running_stats=True)
    )
  )
  (2): ReLU(inplace)
  (3): ConvTranspose2d(128, 3, kernel_size=(4, 4), stride=(2, 2), padding=(1, 1))
  (4): Sigmoid()
 )
)
Total number of parameters: 41832067
RevealNet(
  (main): Sequential(
    (0): Conv2d(3, 64, kernel_size=(3, 3), stride=(1, 1), padding=(1, 1))
    (1): BatchNorm2d(64, eps=1e-05, momentum=0.1, affine=True, track_running_stats=True)
    (2): ReLU(inplace)
    (3): Conv2d(64, 128, kernel_size=(3, 3), stride=(1, 1), padding=(1, 1))
    (4): BatchNorm2d(128, eps=1e-05, momentum=0.1, affine=True, track_running_stats=True)
    (5): ReLU(inplace)
    (6): Conv2d(128, 256, kernel_size=(3, 3), stride=(1, 1), padding=(1, 1))
    (7): BatchNorm2d(256, eps=1e-05, momentum=0.1, affine=True, track_running_stats=True)
    (8): ReLU(inplace)
    (9): Conv2d(256, 128, kernel_size=(3, 3), stride=(1, 1), padding=(1, 1))
    (10): BatchNorm2d(128, eps=1e-05, momentum=0.1, affine=True, track_running_stats=True)
    (11): ReLU(inplace)
    (12): Conv2d(128, 64, kernel_size=(3, 3), stride=(1, 1), padding=(1, 1))
    (13): BatchNorm2d(64, eps=1e-05, momentum=0.1, affine=True, track_running_stats=True)
    (14): ReLU(inplace)
    (15): Conv2d(64, 3, kernel_size=(3, 3), stride=(1, 1), padding=(1, 1))
    (16): Sigmoid()
  )
)
```

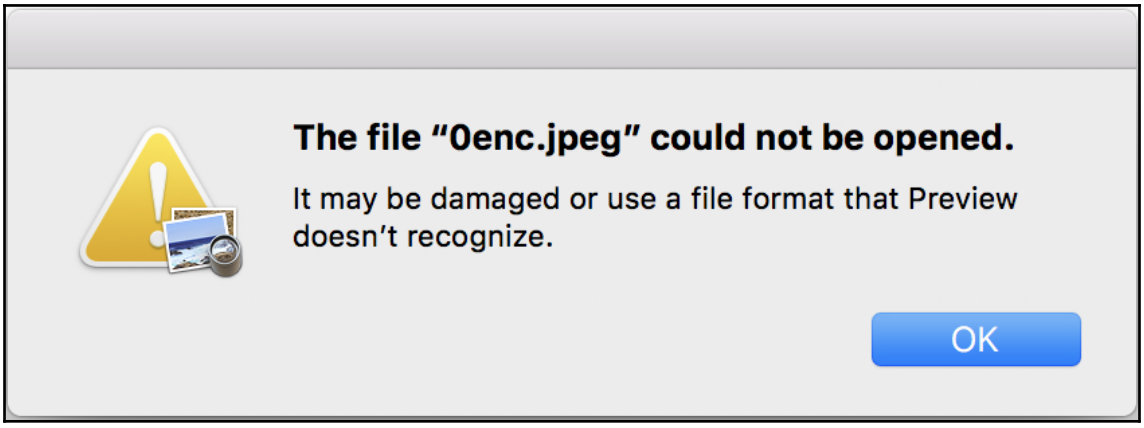
```
Total number of parameters: 742659
################################################## test begin ##################################################
main.py:450: UserWarning: volatile was removed and now has no effect. Use `with torch.no_grad():` instead.
  concat_imgv = Variable(concat_img, volatile=True)  # concat_img as input of Hiding net
main.py:451: UserWarning: volatile was removed and now has no effect. Use `with torch.no_grad():` instead.
  cover_imgv = Variable(cover_img, volatile=True)  # cover_imgv as label of Hiding net
tensor(0.0003, device='cuda:0', grad_fn=<MseLossBackward>)
main.py:461: UserWarning: volatile was removed and now has no effect. Use `with torch.no_grad():` instead.
  secret_imgv = Variable(secret_img, volatile=True)  # secret_imgv as label of R-net
validation[0] val_Hloss = 0.000278      val_Rloss = 0.000178    val_Sumloss = 0.000412  validation time=6.41
################################################## test end ##################################################
##################   test is completed, the result pic is saved in the ./training/yourcompuer+time/testPics/   ######################
```








```
              :convcrypt etsukerman$ python encrypt.py --input_file 0.jpeg --output_file 0enc.jpeg --key_file key
/anaconda3/lib/python3.6/site-packages/h5py/__init__.py:36: FutureWarning: Conversion of the second argument of issubdtype from `float` to `np.floating` is deprecated. In future, it wi
ll be treated as `np.float64 == np.dtype(float).type`.
  from ._conv import register_converters as _register_converters
Using TensorFlow backend.
  0%|                                                                                                                                                  | 0/5 [00:00<?, ?it/s]
2019-05-14 10:44:16.602113: I tensorflow/core/platform/cpu_feature_guard.cc:141] Your CPU supports instructions that this TensorFlow binary was not compiled to use: AVX2 FMA
100%|████████████████████████████████████████████████████████████████████████████████████████████████████████████████████████████████| 5/5 [3:05:39<00:00, 2208.89s/it]
Encryption complete.
```

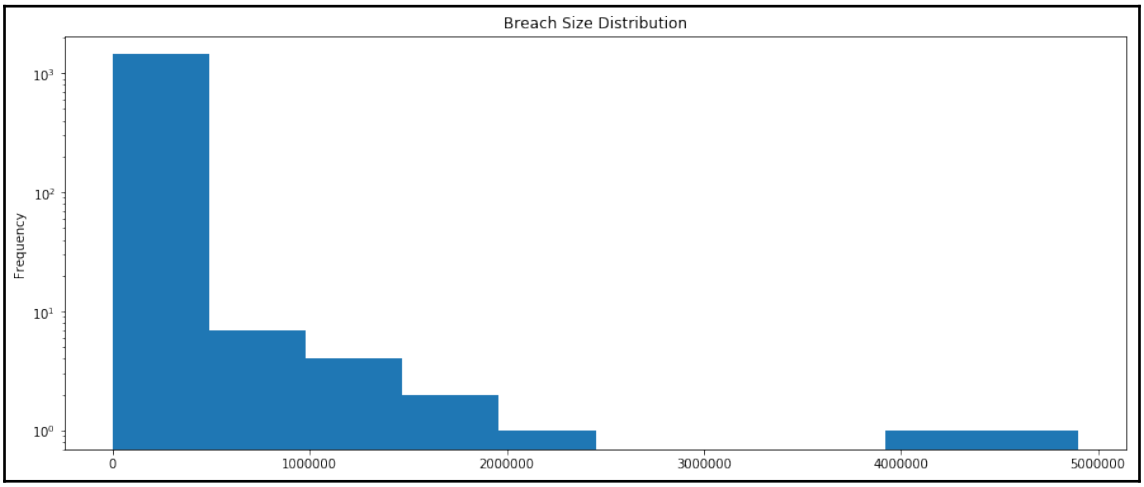


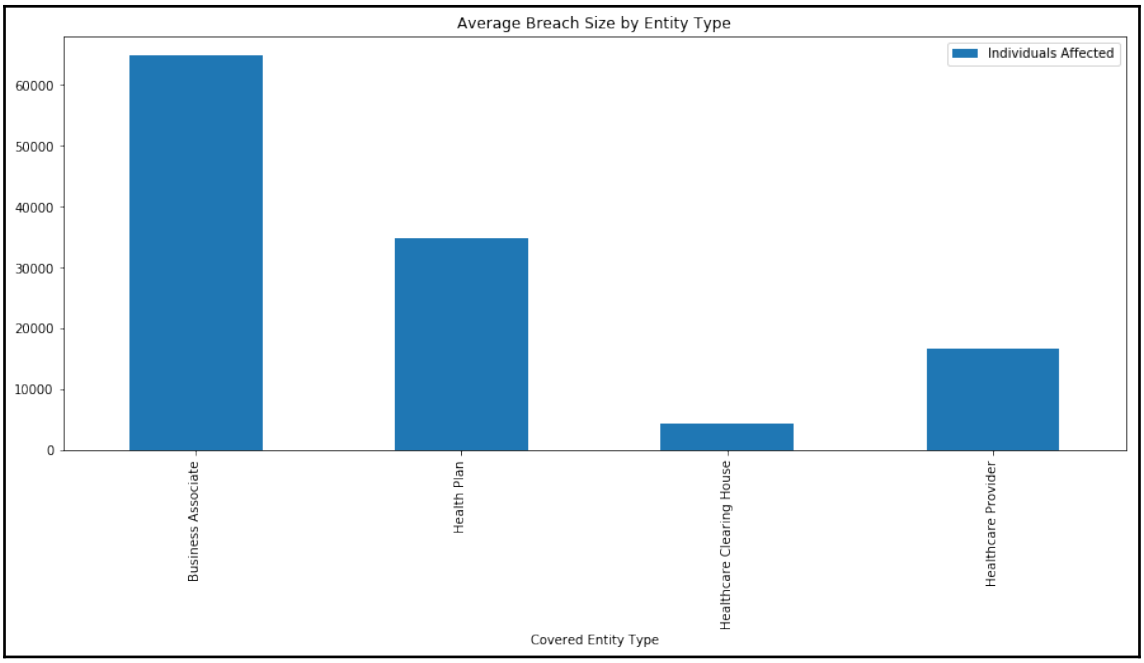
```
In [104]: df.head()
```

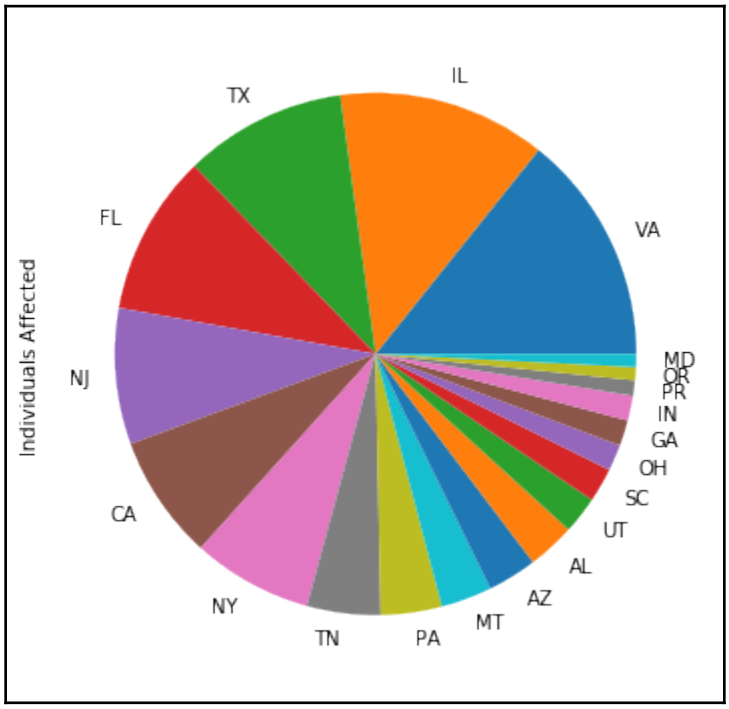
Out[104]:

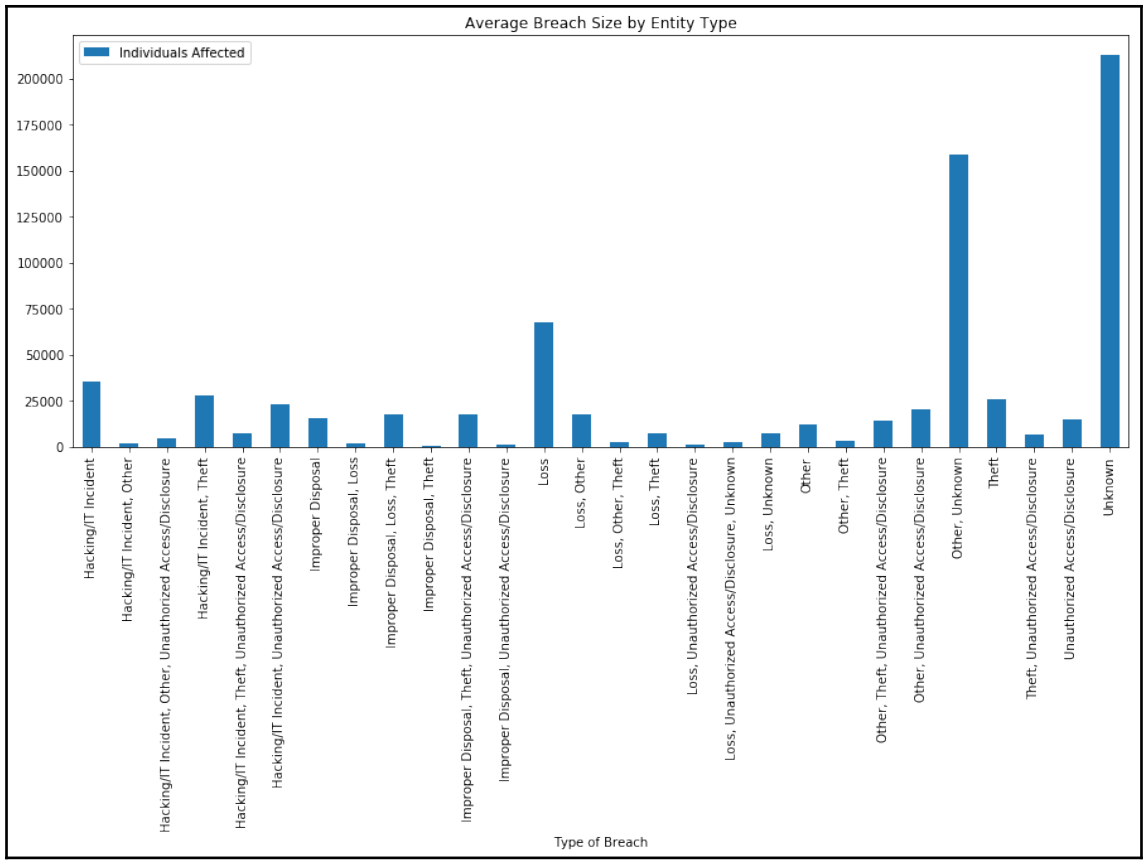
	0	1	2	3	4	5	6	7	8	9	...	1549	1550	1551	1552	1553	1554	1555	1556	1557	label
0	125	125	1.0	1	0	0	0	0	0	0	...	0	0	0	0	0	0	0	0	0	ad.
1	57	468	8.2105	1	0	0	0	0	0	0	...	0	0	0	0	0	0	0	0	0	ad.
2	33	230	6.9696	1	0	0	0	0	0	0	...	0	0	0	0	0	0	0	0	0	ad.
3	60	468	7.8	1	0	0	0	0	0	0	...	0	0	0	0	0	0	0	0	0	ad.
4	60	468	7.8	1	0	0	0	0	0	0	...	0	0	0	0	0	0	0	0	0	ad.

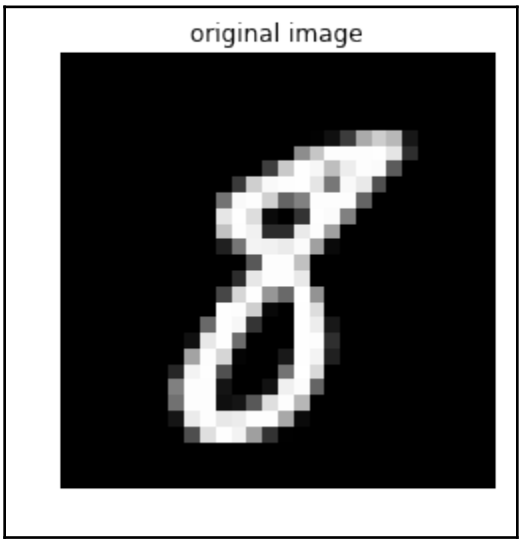
5 rows × 1559 columns

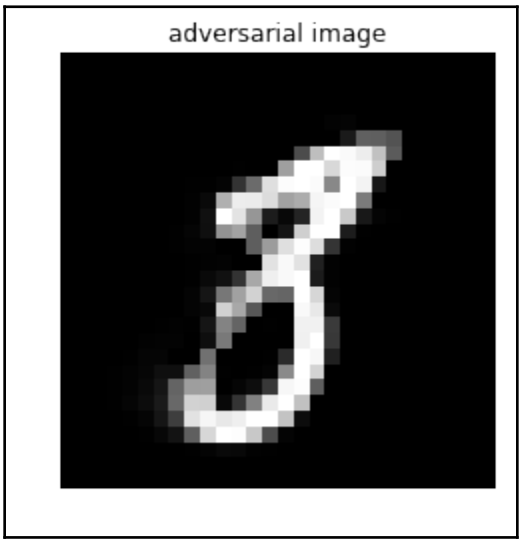


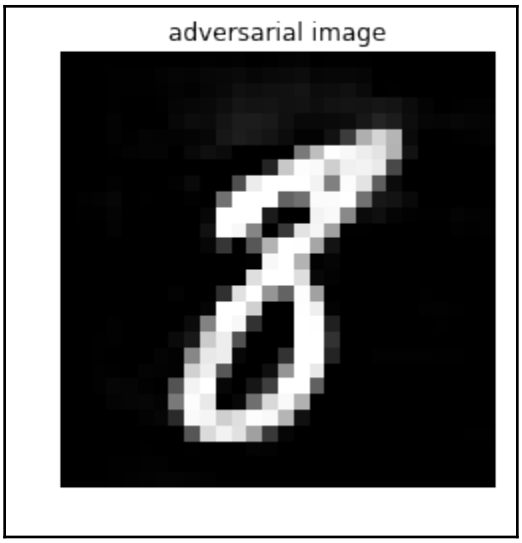

Average Breach Size by Entity Type
Individuals Affected
60000
50000
40000
30000
20000
10000
0
Business Associate
Health Plan
Healthcare Clearing House
Healthcare Provider
Covered Entity Type


Individuals Affected
IL
TX
FL
VA
NJ
MD
OR
PR
IN
GA
OH
SC
UT
AL
AZ
MT
PA
TN
NY
CA


Average Breach Size by Entity Type
Individuals Affected
200000
175000
150000
125000
100000
75000
50000
25000
0
Hacking/IT Incident
Hacking/IT Incident, Other
Hacking/IT Incident, Other, Unauthorized Access/Disclosure
Hacking/IT Incident, Theft
Hacking/IT Incident, Theft, Unauthorized Access/Disclosure
Hacking/IT Incident, Unauthorized Access/Disclosure
Improper Disposal
Improper Disposal, Loss
Improper Disposal, Loss, Theft
Improper Disposal, Theft
Improper Disposal, Theft, Unauthorized Access/Disclosure
Improper Disposal, Unauthorized Access/Disclosure
Loss
Loss, Other
Loss, Other, Theft
Loss, Theft
Loss, Unauthorized Access/Disclosure
Loss, Unauthorized Access/Disclosure, Unknown
Loss, Unknown
Other
Other, Theft
Other, Theft, Unauthorized Access/Disclosure
Other, Unauthorized Access/Disclosure
Other, Unknown
Theft
Theft, Unauthorized Access/Disclosure
Unauthorized Access/Disclosure
Unknown
Type of Breach


original image


adversarial image


adversarial image

Graphics Bundle Ends Here

Index