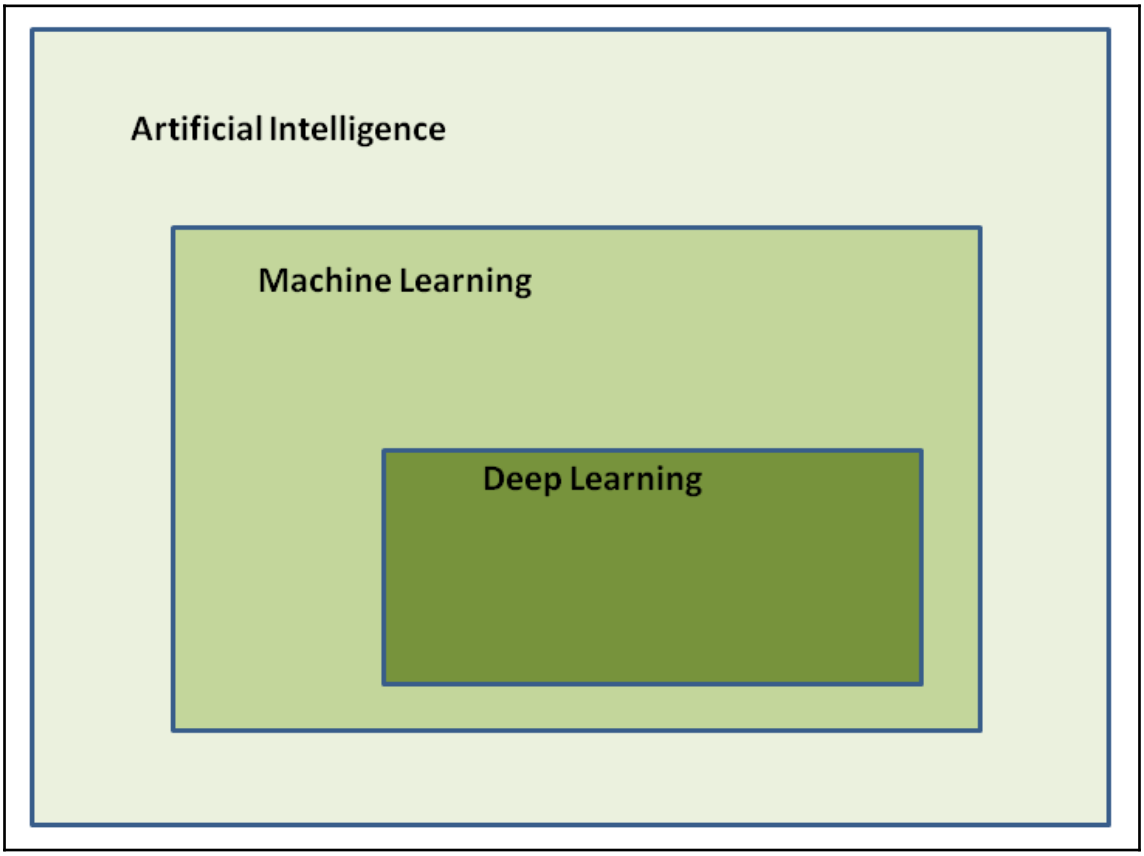
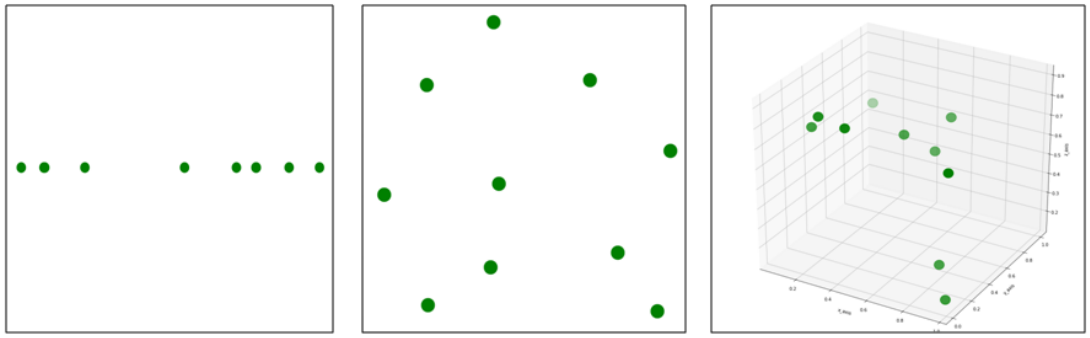
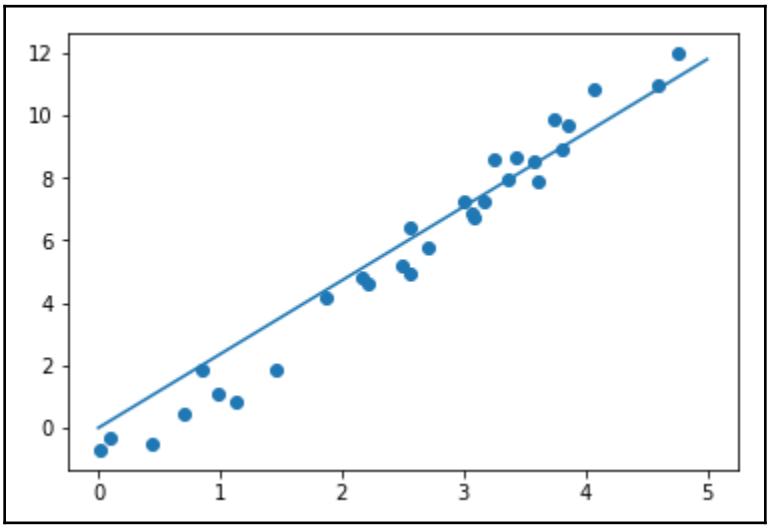
Chapter 1: Introduction to AI for Cybersecurity Professionals

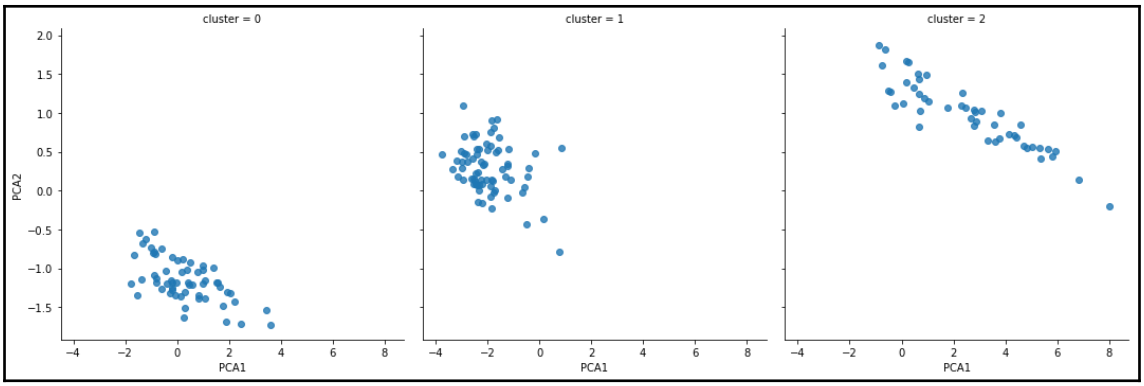


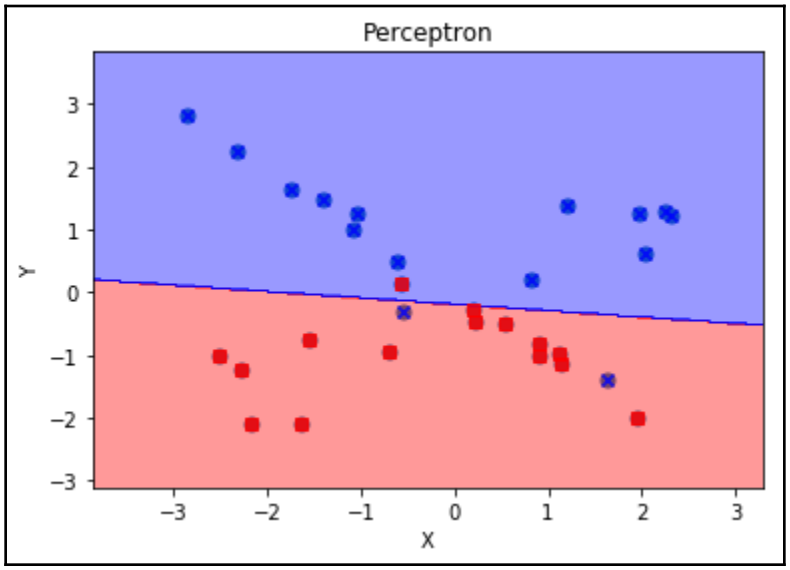
The “Curse of Dimensionality”



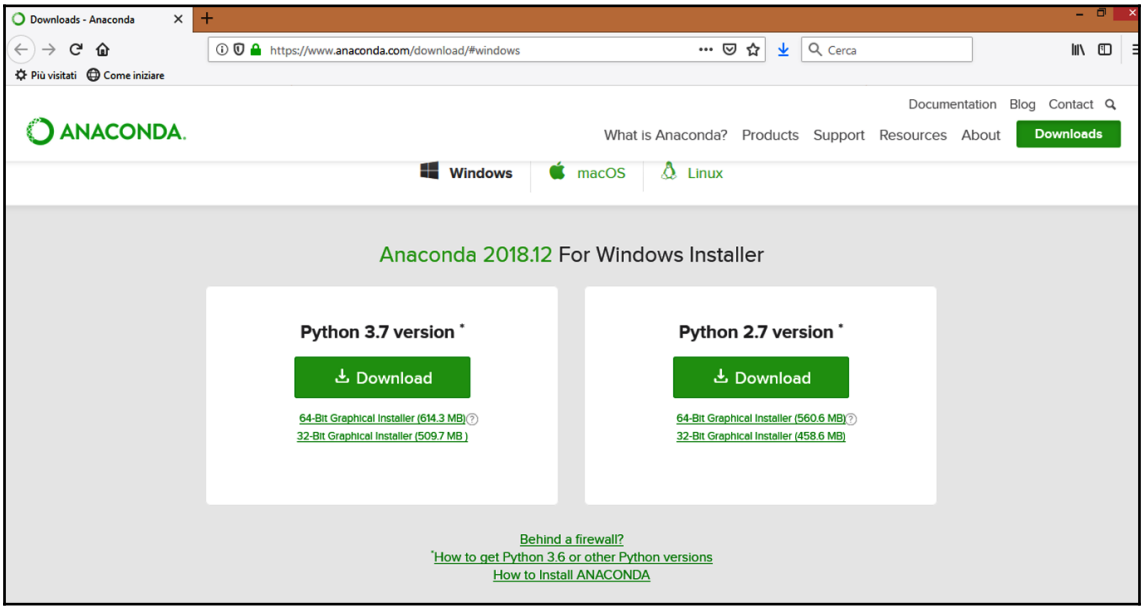
1 dimension 2 dimensions 3 dimensions

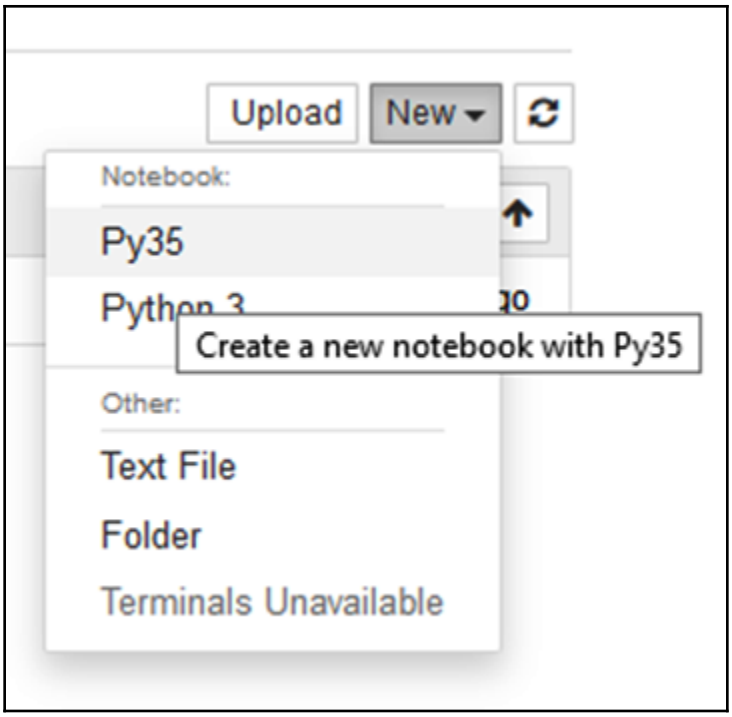


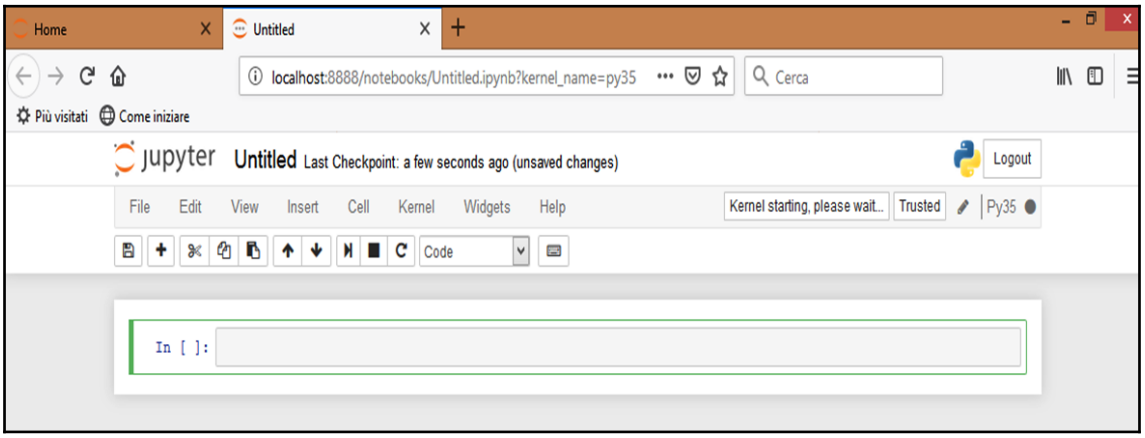

cluster = 0
cluster = 1
cluster = 2
PCA2
PCA1
PCA1
PCA1

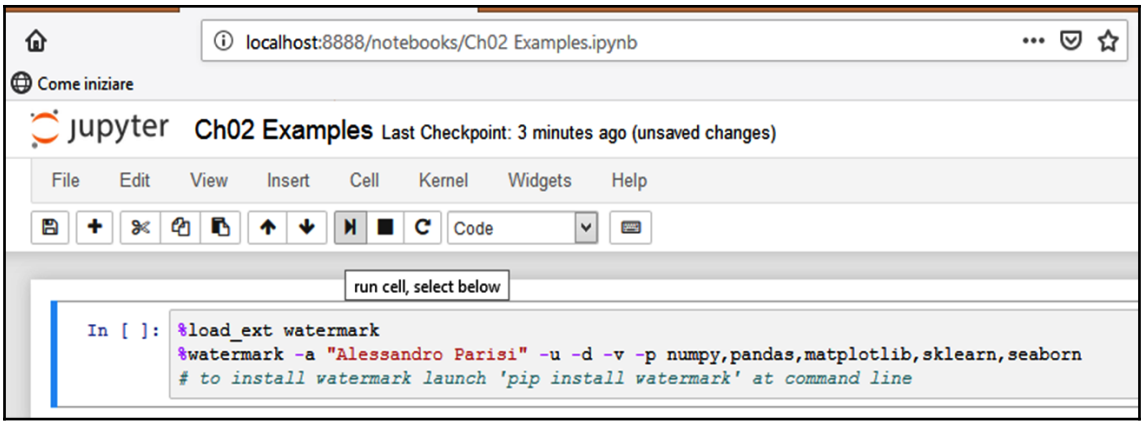

Perceptron
Y
X

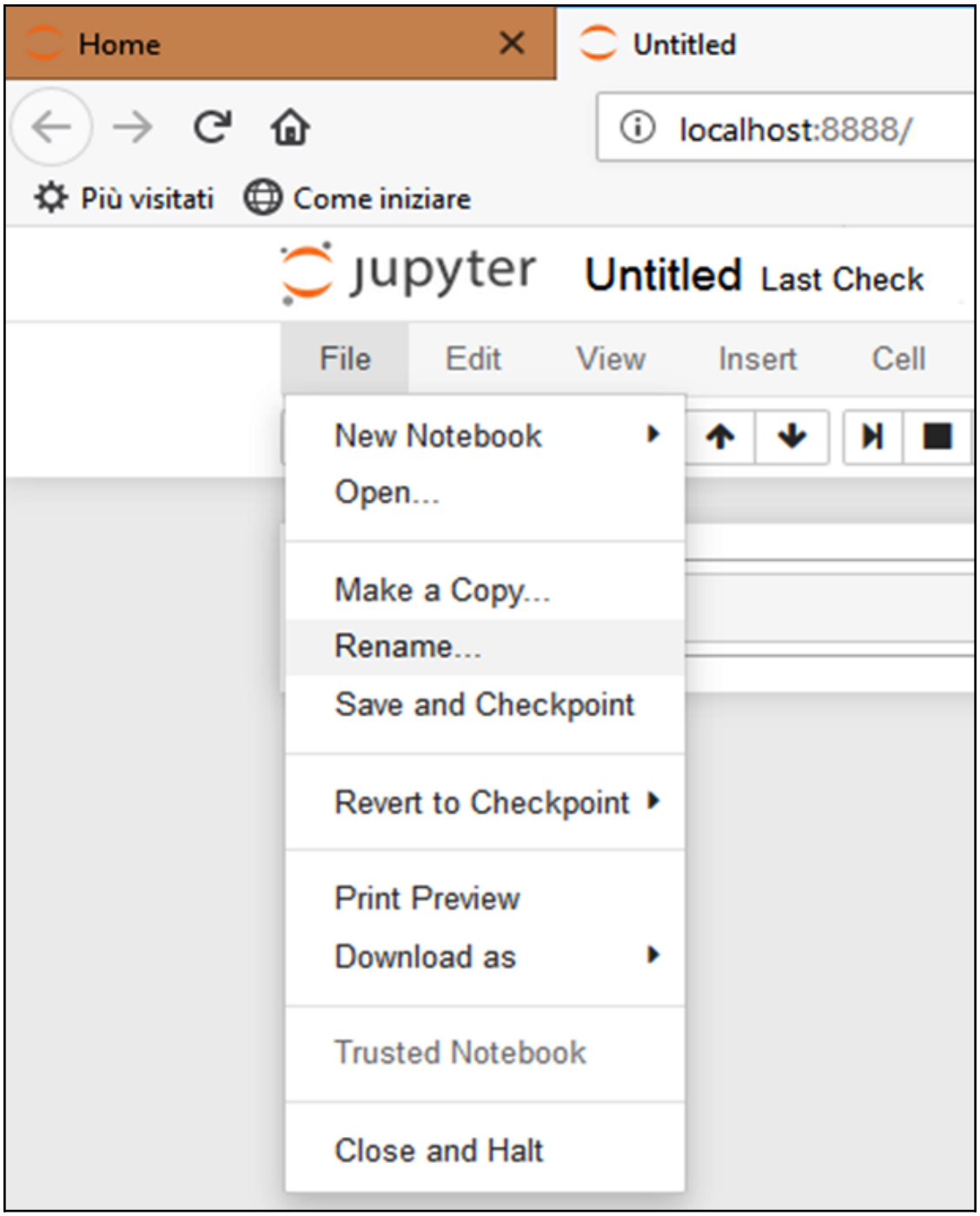
Chapter 2: Setting Up Your AI for Cybersecurity Arsenal

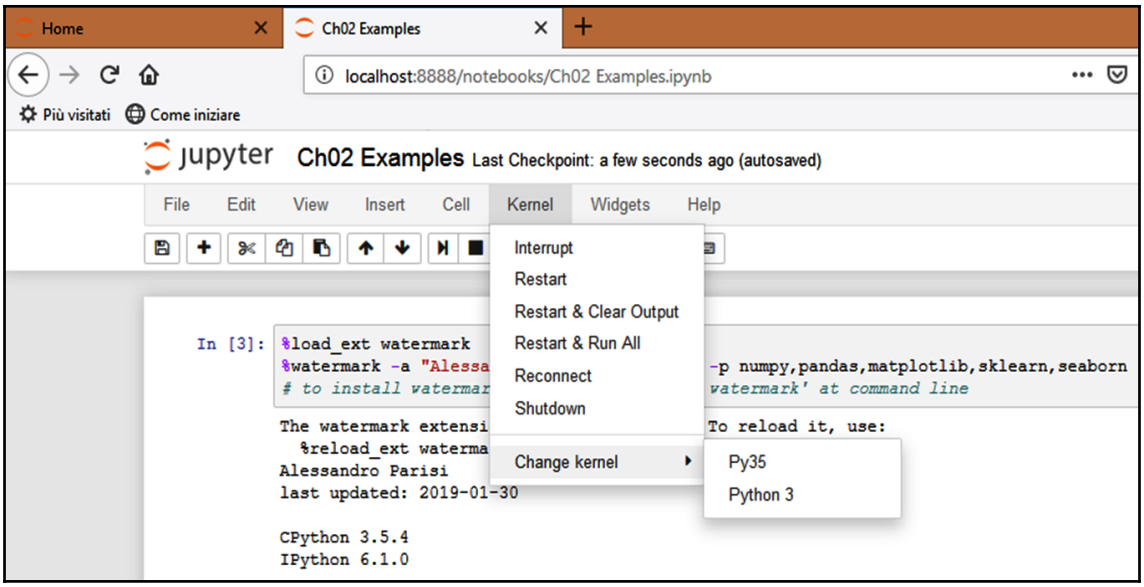


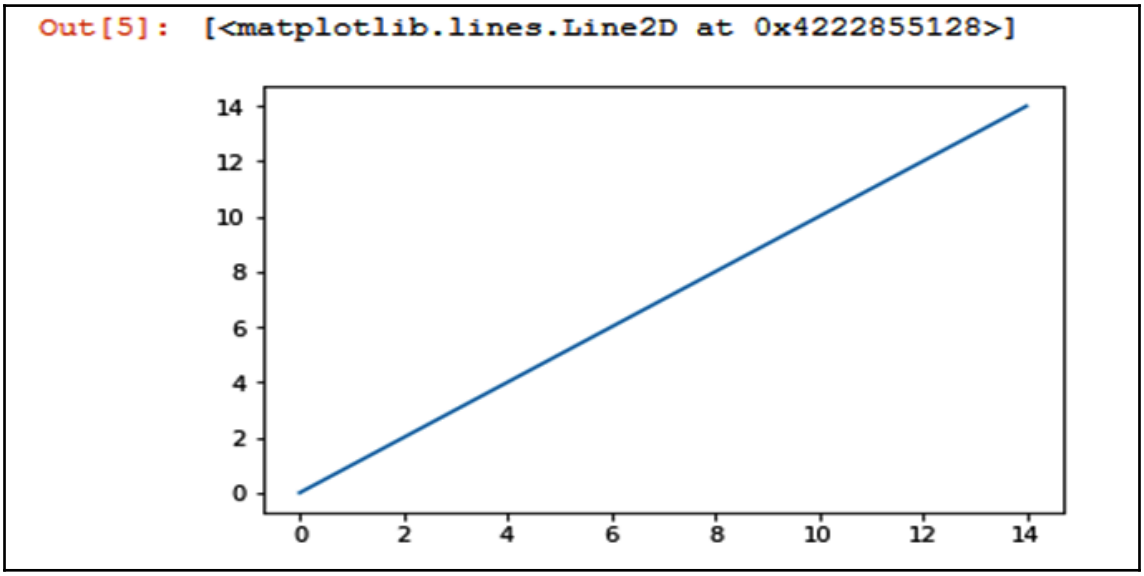

Upload
New
Notebook:
Py35
Python 3
Create a new notebook with Py35
Other:
Text File
Folder
Terminals Unavailable


Home
Untitled
localhost:8888/notebooks/Untitled.ipynb?kernel_name=py35
Cerca
Più visitati
Come iniziare
jupyter
Untitled
Last Checkpoint: a few seconds ago (unsaved changes)
Logout
File
Edit
View
Insert
Cell
Kernel
Widgets
Help
Kernel starting, please wait...
Trusted
Py35
Code
In [ ]:


localhost:8888/notebooks/Ch02 Examples.ipynb
Come iniziare
jupyter
Ch02 Examples
Last Checkpoint: 3 minutes ago (unsaved changes)
File
Edit
View
Insert
Cell
Kernel
Widgets
Help
Code
run cell, select below
In [ ]:
%load_ext watermark
%watermark -a "Alessandro Parisi" -u -d -v -p numpy,pandas,matplotlib,sklearn,seaborn
to install watermark launch 'pip install watermark' at command line


Home
Untitled
localhost:8888/
Più visitati
Come iniziare
jupyter
Untitled
Last Check
File
Edit
View
Insert
Cell
New Notebook
Open...
Make a Copy...
Rename...
Save and Checkpoint
Revert to Checkpoint
Print Preview
Download as
Trusted Notebook
Close and Halt

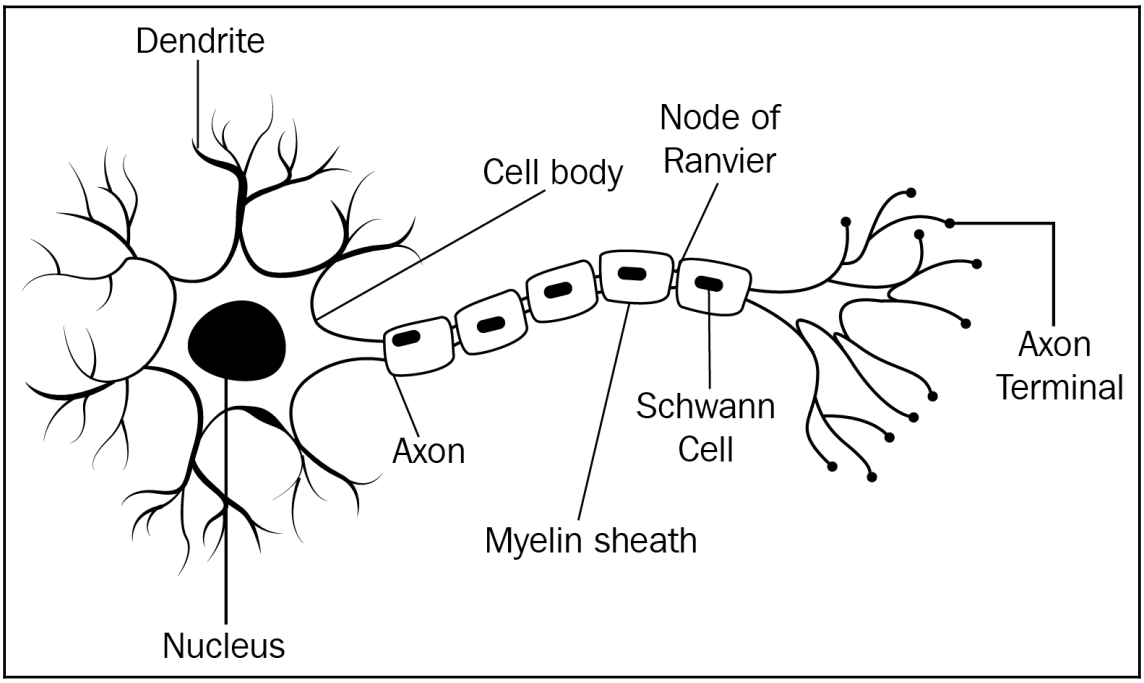

Home
Ch02 Examples
localhost:8888/notebooks/Ch02 Examples.ipynb
Più visitati
Come iniziare
jupyter
Ch02 Examples
Last Checkpoint: a few seconds ago (autosaved)
File
Edit
View
Insert
Cell
Kernel
Widgets
Help
Interrupt
Restart
Restart & Clear Output
Restart & Run All
Reconnect
Shutdown
Change kernel
Py35
Python 3
In [3]:
%load_ext watermark
%watermark -a "Alessa
to install watermar
-p numpy,pandas,matplotlib,sklearn,seaborn
watermark' at command line
The watermark extensi
%reload_ext waterma
To reload it, use:
Alessandro Parisi
last updated: 2019-01-30
CPython 3.5.4
IPython 6.1.0

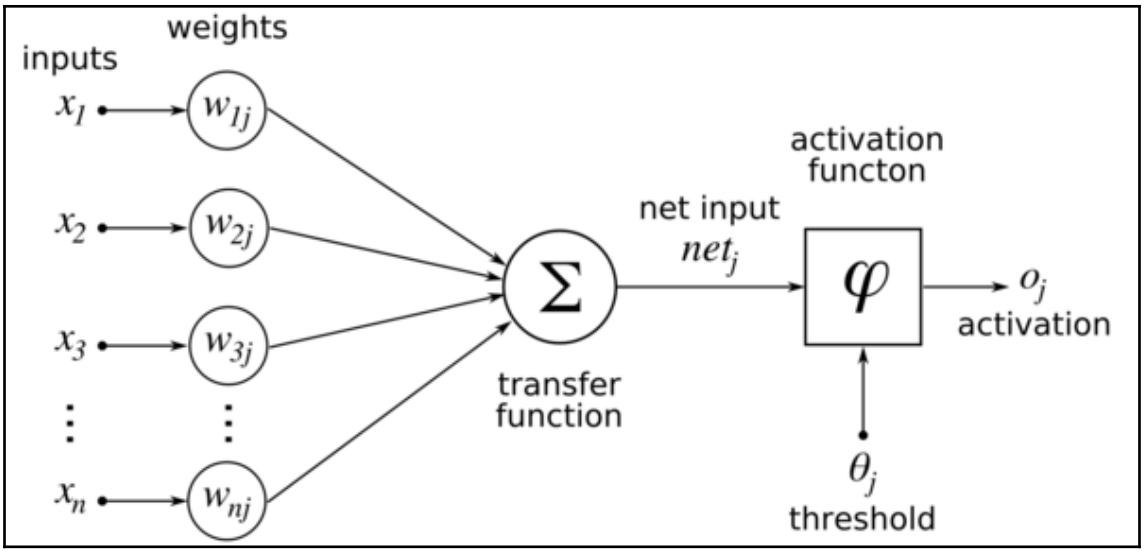

Out[5]: [<matplotlib.lines.Line2D at 0x4222855128>]
14
12
10
8
6
4
2
0
0
2
4
6
8
10
12
14

Out[7]:

	sepal length (cm)	sepal width (cm)	petal length (cm)	petal width (cm)
count	150.000000	150.000000	150.000000	150.000000
mean	5.843333	3.057333	3.758000	1.199333
std	0.828066	0.435866	1.765298	0.762238
min	4.300000	2.000000	1.000000	0.100000
25%	5.100000	2.800000	1.600000	0.300000
50%	5.800000	3.000000	4.350000	1.300000
75%	6.400000	3.300000	5.100000	1.800000
max	7.900000	4.400000	6.900000	2.500000

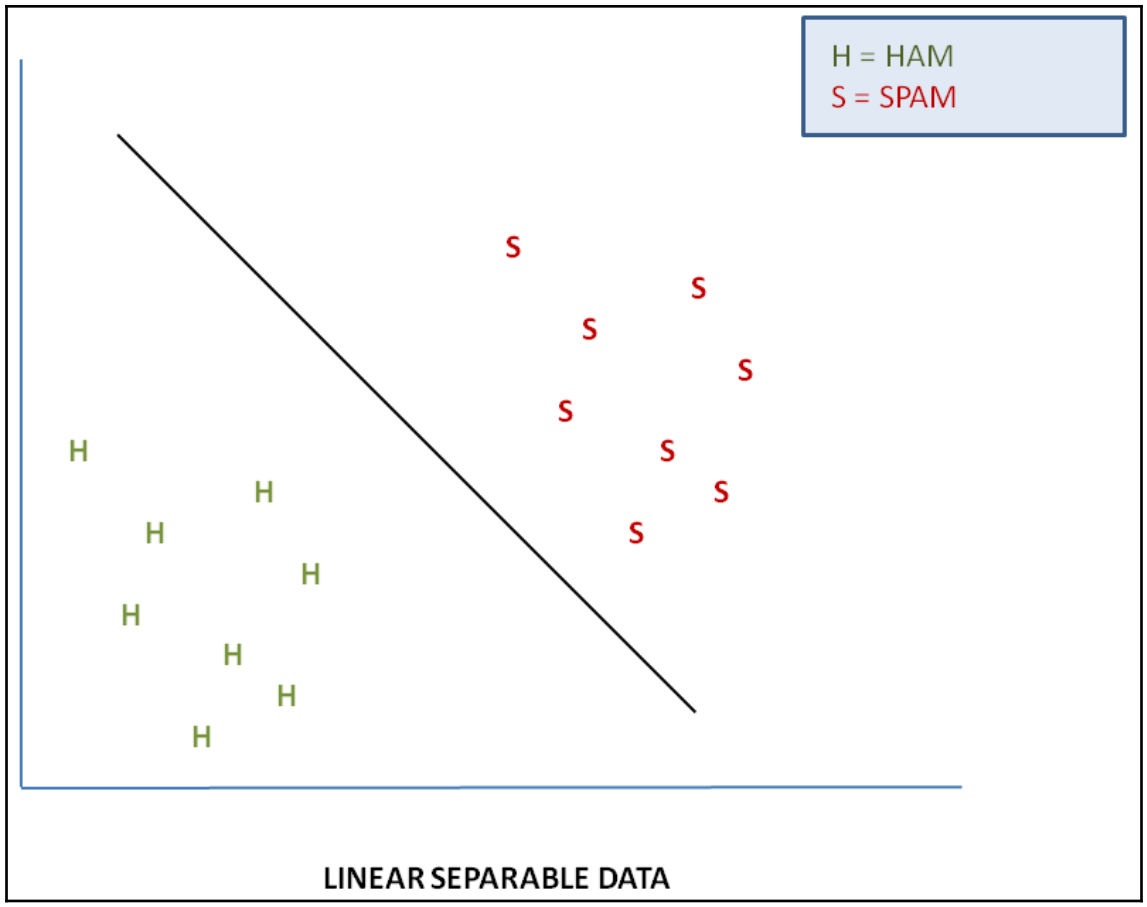
Chapter 3: Ham or Spam? Detecting Email Cybersecurity Threats with AI



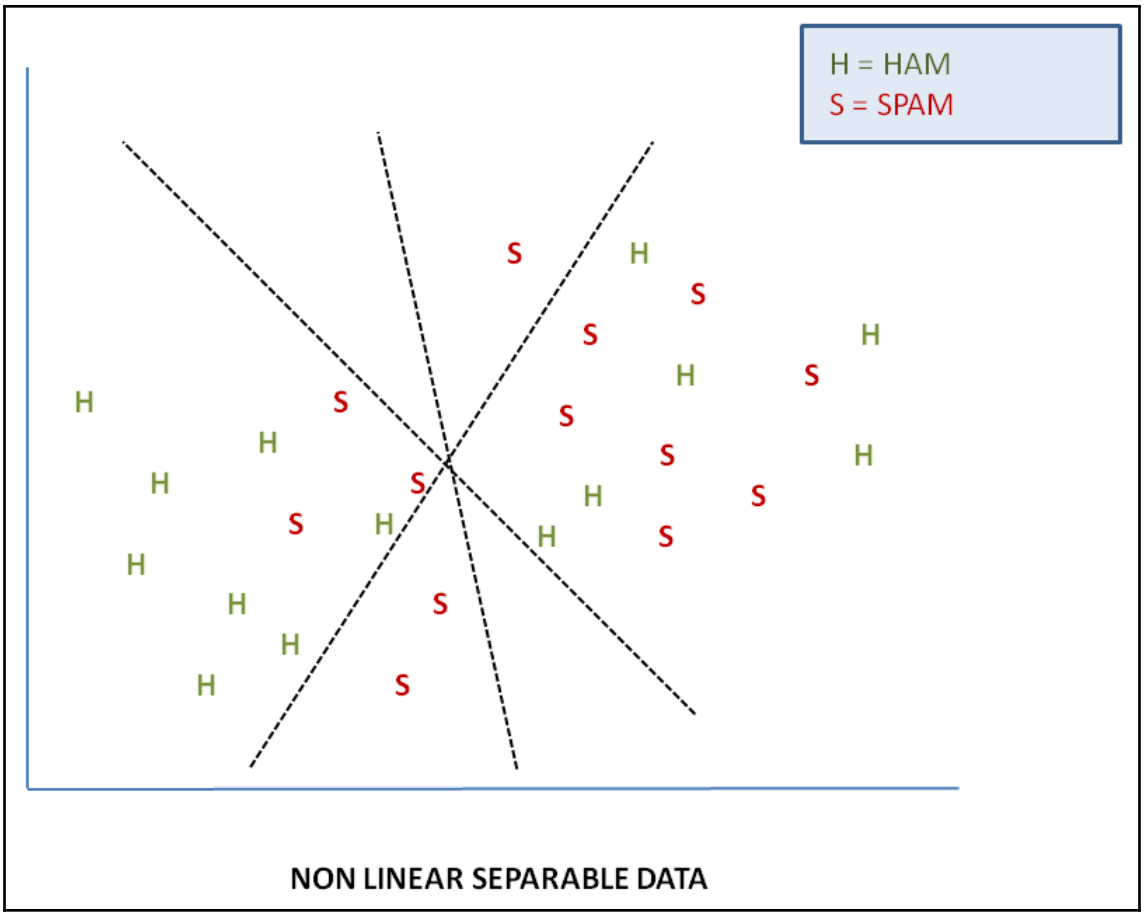


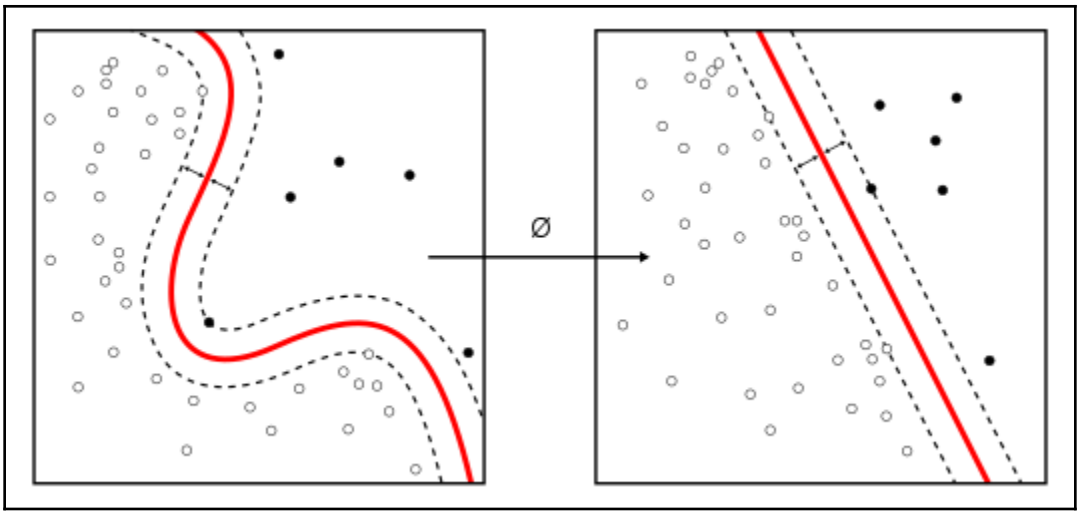
Email	Buy	Sex	Spam or Ham?
1	1	0	H
2	0	1	H
3	0	0	H
4	1	1	S

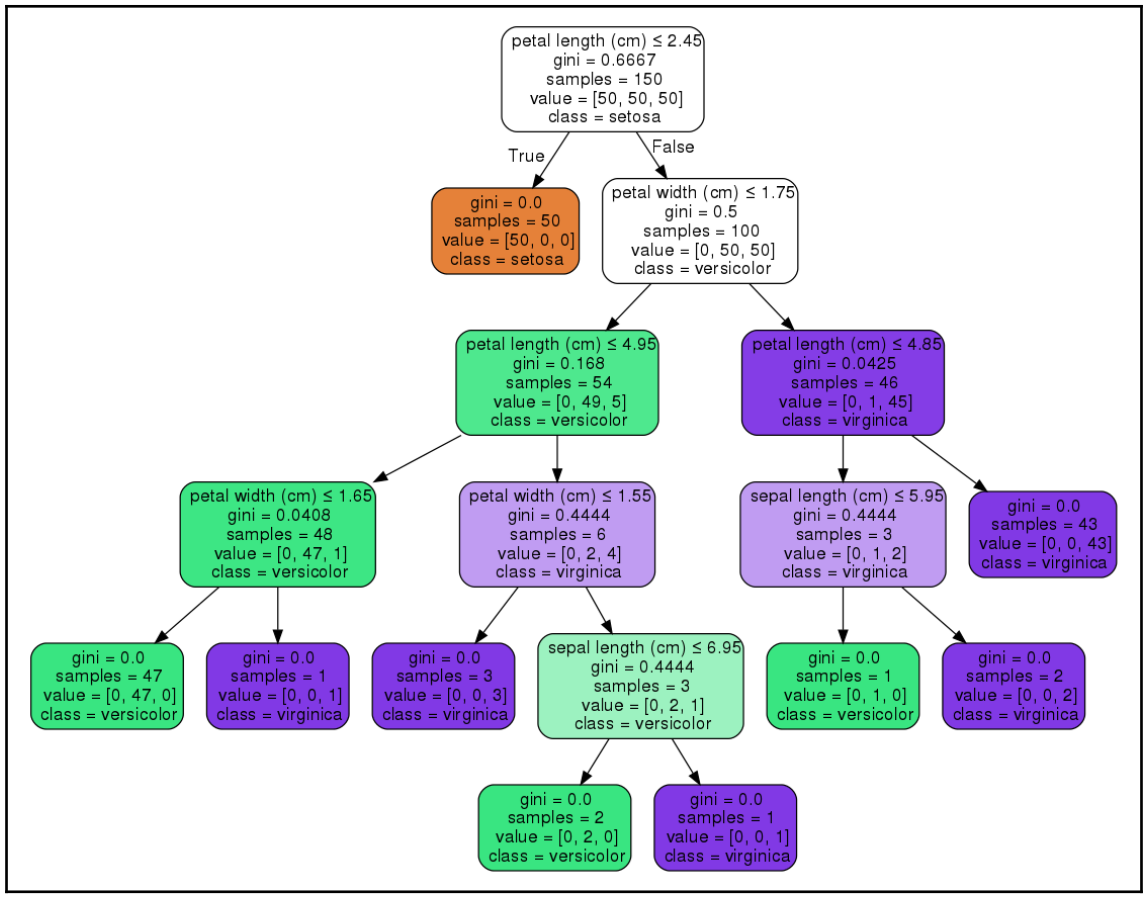
Email	B	S	2B + 3S	Spam or Ham?
1	1	0	2	H
2	0	1	3	H
3	0	0	0	H
4	1	1	5	S



LINEAR SEPARABLE DATA

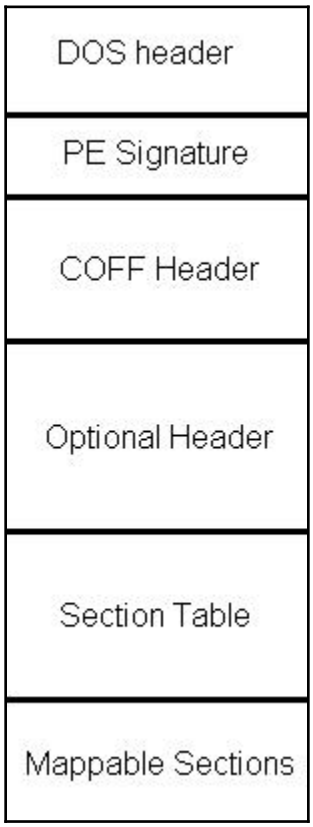

H = HAM
S = SPAM
NON LINEAR SEPARABLE DATA

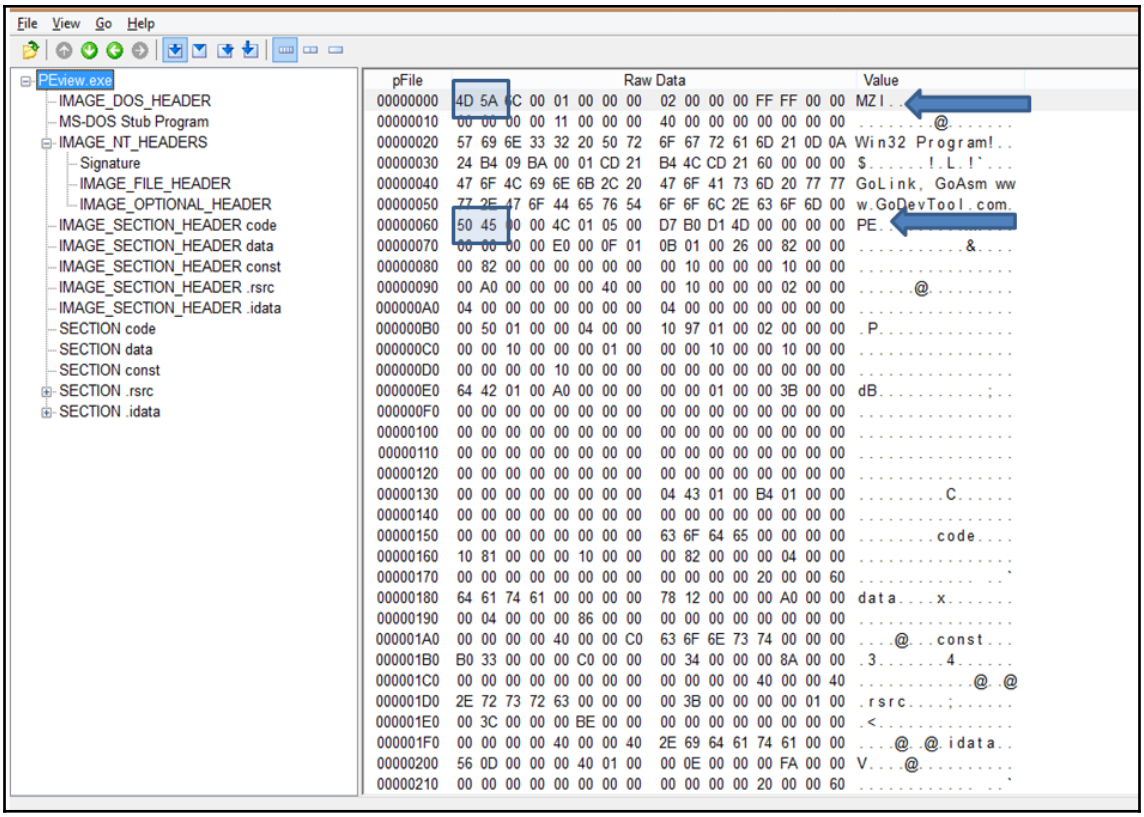

Ø

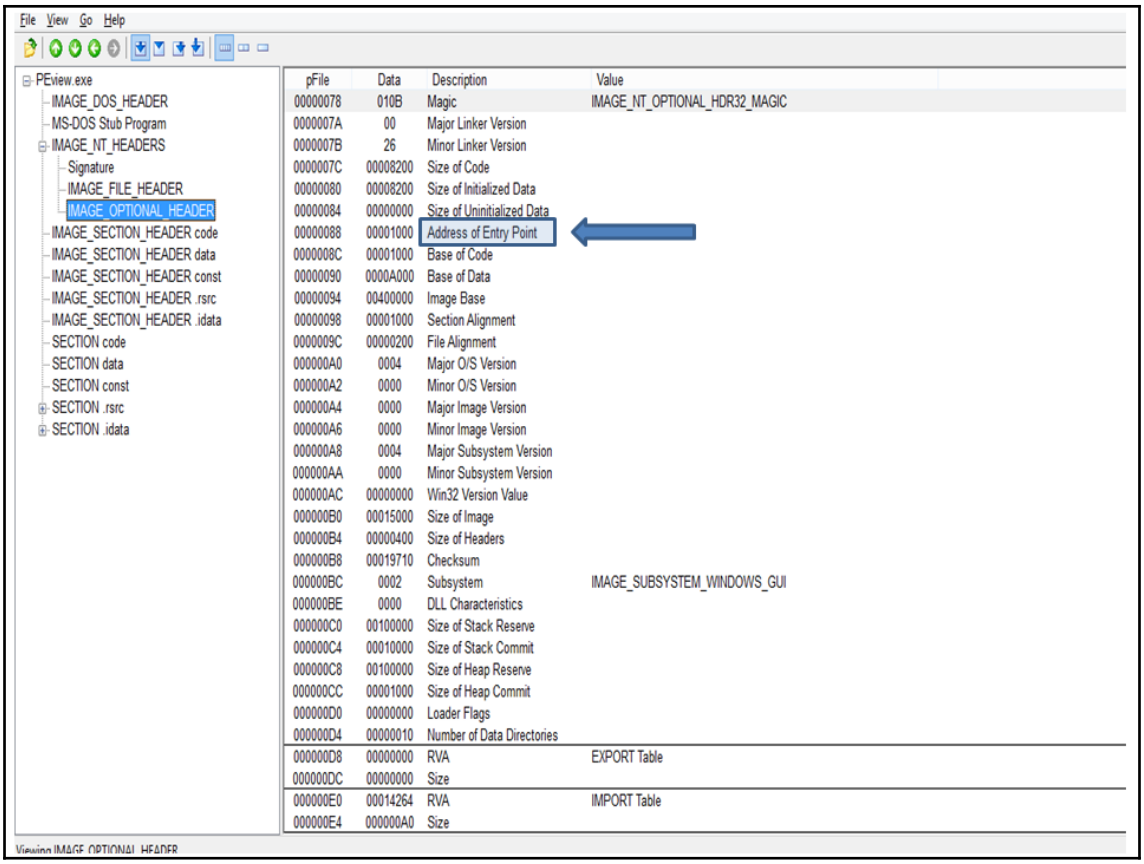



```
print (classification_report(sms['type'][:len(predictions)], predictions))
             precision    recall  f1-score   support

        ham       0.87      0.90      0.89      3382
       spam       0.15      0.11      0.13       519

avg / total       0.80      0.80      0.80      3901
```

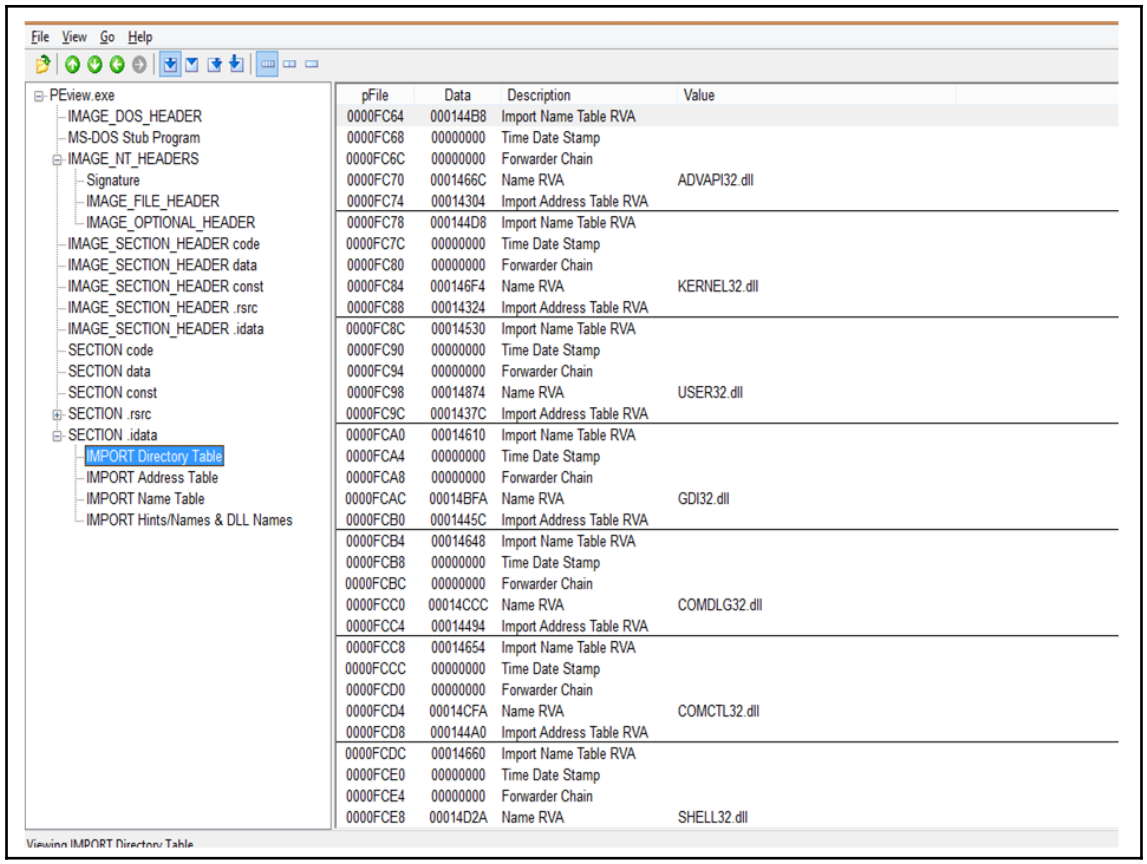
Chapter 4: Malware Threat Detection

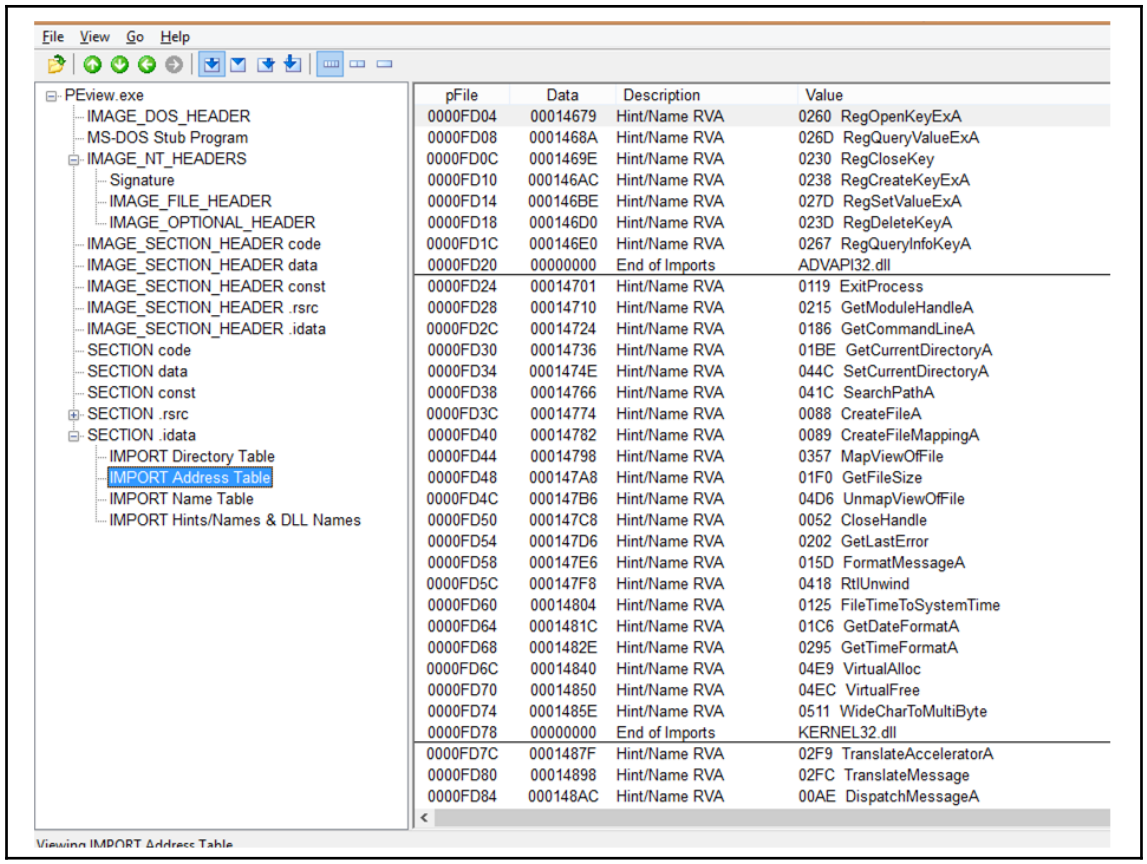


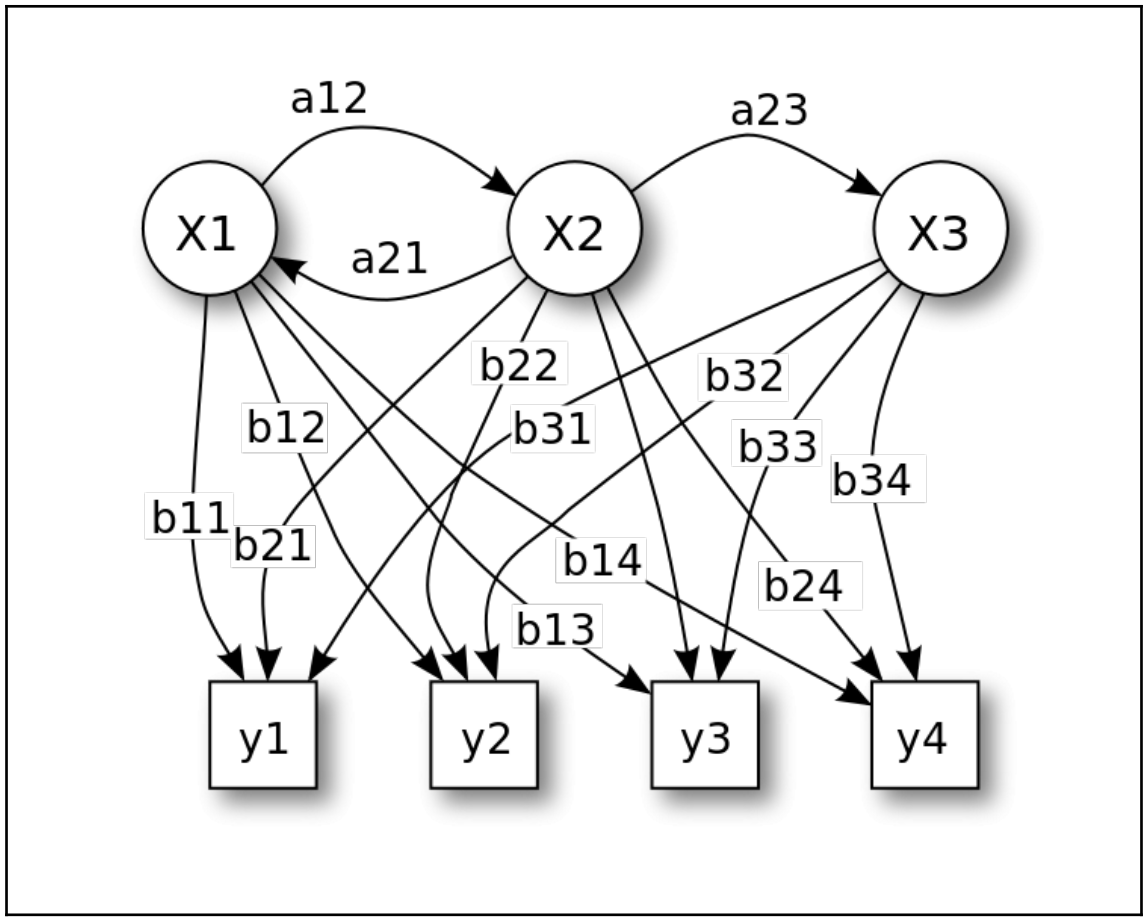

File View Go Help
PEview.exe
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
Signature
IMAGE_FILE_HEADER
IMAGE_OPTIONAL_HEADER
IMAGE_SECTION_HEADER code
IMAGE_SECTION_HEADER data
IMAGE_SECTION_HEADER const
IMAGE_SECTION_HEADER .rsrc
IMAGE_SECTION_HEADER .idata
SECTION code
SECTION data
SECTION const
SECTION .rsrc
SECTION .idata
pFile Raw Data Value
00000000 4D 5A 4C 00 01 00 00 00 02 00 00 00 FF FF 00 00 MZL.
00000010 00 00 00 00 11 00 00 00 40 00 00 00 00 00 00 00 ....@.
00000020 57 69 6E 33 32 20 50 72 6F 67 72 61 6D 21 0D 0A Win32 Program!..
00000030 24 B4 09 BA 00 01 CD 21 B4 4C CD 21 60 00 00 00 $.....!.L.!`...
00000040 47 6F 4C 69 6E 6B 2C 20 47 6F 41 73 6D 20 77 77 GoLink, GoAsm ww
00000050 77 2E 47 6F 44 65 76 54 6F 6F 6C 2E 63 6F 6D 00 w.GoDevTool.com.
00000060 50 45 00 00 4C 01 05 00 D7 B0 D1 4D 00 00 00 00 PE..L.....M....
00000070 00 00 00 00 E0 00 0F 01 0B 01 00 26 00 82 00 00 .....&....
00000080 00 82 00 00 00 00 00 00 00 10 00 00 00 10 00 00 ....
00000090 00 A0 00 00 00 00 40 00 00 10 00 00 00 02 00 00 ......@.........
000000A0 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 ....
000000B0 00 50 01 00 00 04 00 00 10 97 01 00 02 00 00 00 .P..............
000000C0 00 00 10 00 00 00 01 00 00 00 10 00 00 10 00 00 ....
000000D0 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 ....
000000E0 64 42 01 00 A0 00 00 00 00 00 01 00 00 3B 00 00 dB.....;..
000000F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000130 00 00 00 00 00 00 00 00 04 43 01 00 B4 01 00 00 ....C......
00000140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000150 00 00 00 00 00 00 00 00 63 6F 64 65 00 00 00 00 ....code....
00000160 10 81 00 00 00 10 00 00 00 82 00 00 00 04 00 00 ....
00000170 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 ....`
00000180 64 61 74 61 00 00 00 00 78 12 00 00 00 A0 00 00 data....x.....
00000190 00 04 00 00 00 86 00 00 00 00 00 00 00 00 00 00 ....
000001A0 00 00 00 00 40 00 00 C0 63 6F 6E 73 74 00 00 00 ....@...const...
000001B0 B0 33 00 00 00 C0 00 00 00 34 00 00 00 8A 00 00 .3.......4......
000001C0 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 ....@..@
000001D0 2E 72 73 72 63 00 00 00 00 3B 00 00 00 00 01 00 .rsrc....;......
000001E0 00 3C 00 00 00 BE 00 00 00 00 00 00 00 00 00 00 .<..............
000001F0 00 00 00 00 40 00 00 40 2E 69 64 61 74 61 00 00 ....@..@.idata..
00000200 56 0D 00 00 00 40 01 00 00 0E 00 00 00 FA 00 00 V....@..........
00000210 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 ....`

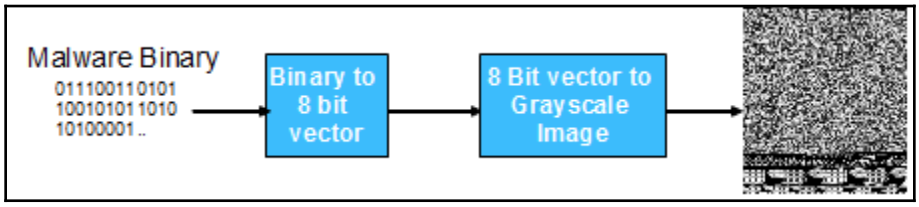

File View Go Help
PEview.exe
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
Signature
IMAGE_FILE_HEADER
IMAGE_OPTIONAL_HEADER
IMAGE_SECTION_HEADER code
IMAGE_SECTION_HEADER data
IMAGE_SECTION_HEADER const
IMAGE_SECTION_HEADER .rsrc
IMAGE_SECTION_HEADER .idata
SECTION code
SECTION data
SECTION const
SECTION .rsrc
SECTION .idata
pFile Data Description Value
00000078 010B Magic IMAGE_NT_OPTIONAL_HDR32_MAGIC
0000007A 00 Major Linker Version
0000007B 26 Minor Linker Version
0000007C 00008200 Size of Code
00000080 00008200 Size of Initialized Data
00000084 00000000 Size of Uninitialized Data
00000088 00001000 Address of Entry Point
0000008C 00001000 Base of Code
00000090 0000A000 Base of Data
00000094 00400000 Image Base
00000098 00001000 Section Alignment
0000009C 00000200 File Alignment
000000A0 0004 Major O/S Version
000000A2 0000 Minor O/S Version
000000A4 0000 Major Image Version
000000A6 0000 Minor Image Version
000000A8 0004 Major Subsystem Version
000000AA 0000 Minor Subsystem Version
000000AC 00000000 Win32 Version Value
000000B0 00015000 Size of Image
000000B4 00000400 Size of Headers
000000B8 00019710 Checksum
000000BC 0002 Subsystem IMAGE_SUBSYSTEM_WINDOWS_GUI
000000BE 0000 DLL Characteristics
000000C0 00100000 Size of Stack Reserve
000000C4 00010000 Size of Stack Commit
000000C8 00100000 Size of Heap Reserve
000000CC 00001000 Size of Heap Commit
000000D0 00000000 Loader Flags
000000D4 00000010 Number of Data Directories
000000D8 00000000 RVA EXPORT Table
000000DC 00000000 Size
000000E0 00014264 RVA IMPORT Table
000000E4 000000A0 Size

Index	Description
0	Exported functions
1	Imported functions
2	Resources
3	Exception informations
4	Security informations
5	Base relocation table
6	Debug informations
7	Architecture specific data
8	Global pointer
9	Thread local storage
10	Load configuration
11	Bound imports
12	Import address table
13	Delay load imports
14	COM runtime descriptor

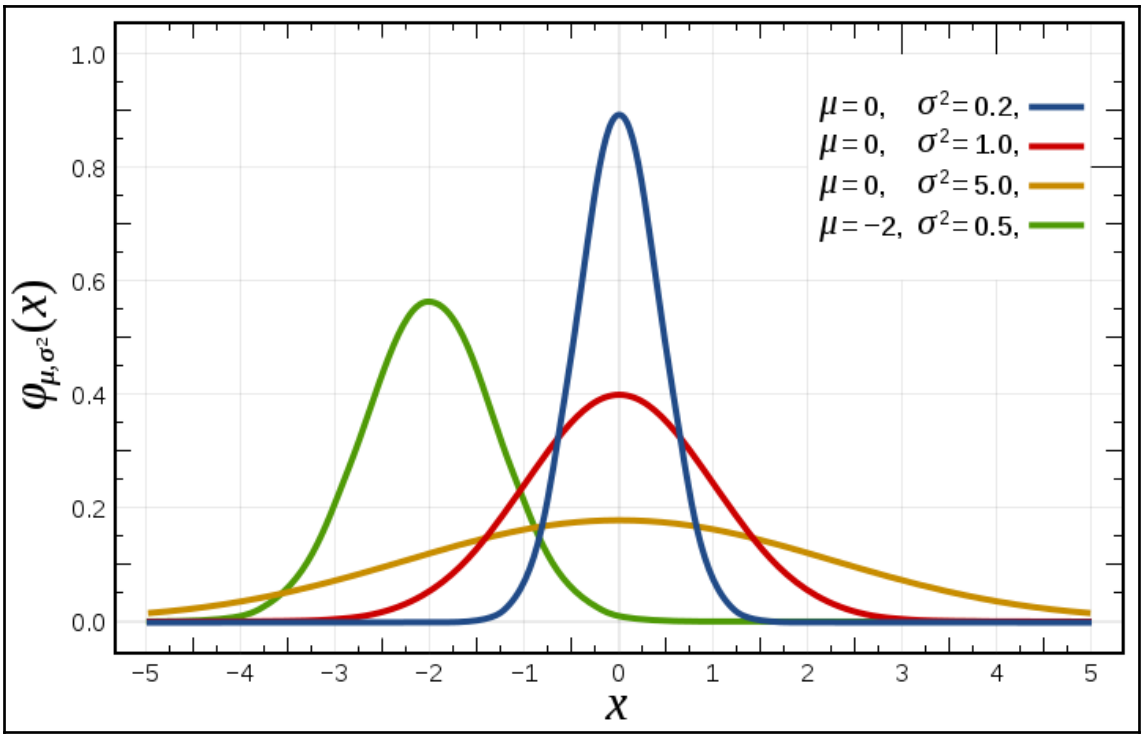

File View Go Help
PEview.exe
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
Signature
IMAGE_FILE_HEADER
IMAGE_OPTIONAL_HEADER
IMAGE_SECTION_HEADER code
IMAGE_SECTION_HEADER data
IMAGE_SECTION_HEADER const
IMAGE_SECTION_HEADER .rsrc
IMAGE_SECTION_HEADER .idata
SECTION code
SECTION data
SECTION const
SECTION .rsrc
SECTION .idata
IMPORT Directory Table
IMPORT Address Table
IMPORT Name Table
IMPORT Hints/Names & DLL Names
pFile Data Description Value
0000FC64 000144B8 Import Name Table RVA
0000FC68 00000000 Time Date Stamp
0000FC6C 00000000 Forwarder Chain
0000FC70 0001466C Name RVA ADVAPI32.dll
0000FC74 00014304 Import Address Table RVA
0000FC78 000144D8 Import Name Table RVA
0000FC7C 00000000 Time Date Stamp
0000FC80 00000000 Forwarder Chain
0000FC84 000146F4 Name RVA KERNEL32.dll
0000FC88 00014324 Import Address Table RVA
0000FC8C 00014530 Import Name Table RVA
0000FC90 00000000 Time Date Stamp
0000FC94 00000000 Forwarder Chain
0000FC98 00014874 Name RVA USER32.dll
0000FC9C 0001437C Import Address Table RVA
0000FCA0 00014610 Import Name Table RVA
0000FCA4 00000000 Time Date Stamp
0000FCA8 00000000 Forwarder Chain
0000FCAC 00014BFA Name RVA GDI32.dll
0000FCB0 0001445C Import Address Table RVA
0000FCB4 00014648 Import Name Table RVA
0000FCB8 00000000 Time Date Stamp
0000FCBC 00000000 Forwarder Chain
0000FCC0 00014CCC Name RVA COMDLG32.dll
0000FCC4 00014494 Import Address Table RVA
0000FCC8 00014654 Import Name Table RVA
0000FCCC 00000000 Time Date Stamp
0000FCD0 00000000 Forwarder Chain
0000FCD4 00014CFA Name RVA COMCTL32.dll
0000FCD8 000144A0 Import Address Table RVA
0000FCDC 00014660 Import Name Table RVA
0000FCE0 00000000 Time Date Stamp
0000FCE4 00000000 Forwarder Chain
0000FCE8 00014D2A Name RVA SHELL32.dll
Viewing IMPORT Directory Table

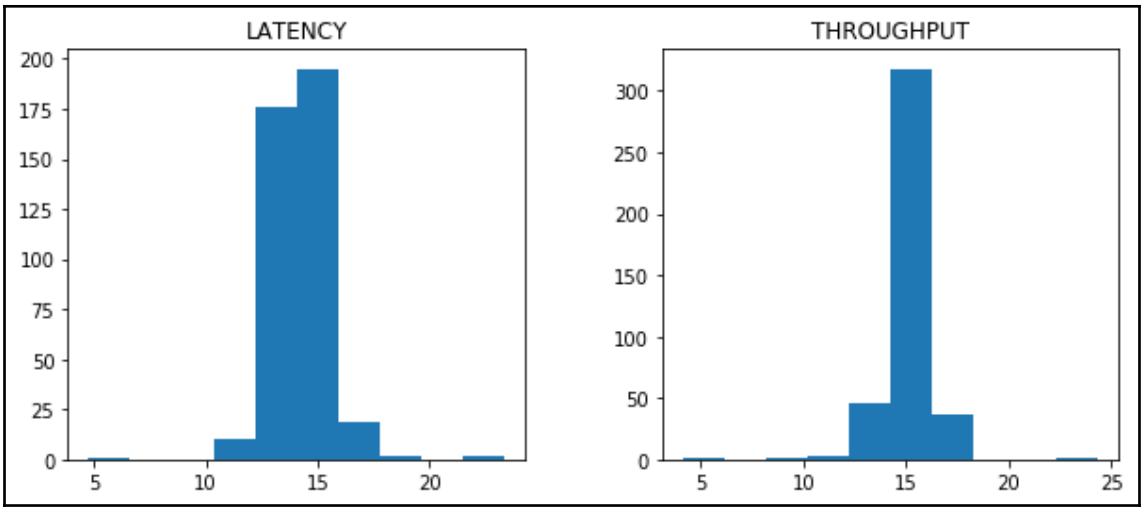

File View Go Help
PEview.exe
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
Signature
IMAGE_FILE_HEADER
IMAGE_OPTIONAL_HEADER
IMAGE_SECTION_HEADER code
IMAGE_SECTION_HEADER data
IMAGE_SECTION_HEADER const
IMAGE_SECTION_HEADER .rsrc
IMAGE_SECTION_HEADER .idata
SECTION code
SECTION data
SECTION const
SECTION .rsrc
SECTION .idata
IMPORT Directory Table
IMPORT Address Table
IMPORT Name Table
IMPORT Hints/Names & DLL Names
pFile Data Description Value
0000FD04 00014679 Hint/Name RVA 0260 RegOpenKeyExA
0000FD08 0001468A Hint/Name RVA 026D RegQueryValueExA
0000FD0C 0001469E Hint/Name RVA 0230 RegCloseKey
0000FD10 000146AC Hint/Name RVA 0238 RegCreateKeyExA
0000FD14 000146BE Hint/Name RVA 027D RegSetValueExA
0000FD18 000146D0 Hint/Name RVA 023D RegDeleteKeyA
0000FD1C 000146E0 Hint/Name RVA 0267 RegQueryInfoKeyA
0000FD20 00000000 End of Imports ADVAPI32.dll
0000FD24 00014701 Hint/Name RVA 0119 ExitProcess
0000FD28 00014710 Hint/Name RVA 0215 GetModuleHandleA
0000FD2C 00014724 Hint/Name RVA 0186 GetCommandLineA
0000FD30 00014736 Hint/Name RVA 01BE GetCurrentDirectoryA
0000FD34 0001474E Hint/Name RVA 044C SetCurrentDirectoryA
0000FD38 00014766 Hint/Name RVA 041C SearchPathA
0000FD3C 00014774 Hint/Name RVA 0088 CreateFileA
0000FD40 00014782 Hint/Name RVA 0089 CreateFileMappingA
0000FD44 00014798 Hint/Name RVA 0357 MapViewOfFile
0000FD48 000147A8 Hint/Name RVA 01F0 GetFileSize
0000FD4C 000147B6 Hint/Name RVA 04D6 UnmapViewOfFile
0000FD50 000147C8 Hint/Name RVA 0052 CloseHandle
0000FD54 000147D6 Hint/Name RVA 0202 GetLastError
0000FD58 000147E6 Hint/Name RVA 015D FormatMessageA
0000FD5C 000147F8 Hint/Name RVA 0418 RtlUnwind
0000FD60 00014804 Hint/Name RVA 0125 FileTimeToSystemTime
0000FD64 0001481C Hint/Name RVA 01C6 GetDateFormatA
0000FD68 0001482E Hint/Name RVA 0295 GetTimeFormatA
0000FD6C 00014840 Hint/Name RVA 04E9 VirtualAlloc
0000FD70 00014850 Hint/Name RVA 04EC VirtualFree
0000FD74 0001485E Hint/Name RVA 0511 WideCharToMultiByte
0000FD78 00000000 End of Imports KERNEL32.dll
0000FD7C 0001487F Hint/Name RVA 02F9 TranslateAcceleratorA
0000FD80 00014898 Hint/Name RVA 02FC TranslateMessage
0000FD84 000148AC Hint/Name RVA 00AE DispatchMessageA
Viewing IMPORT Address Table

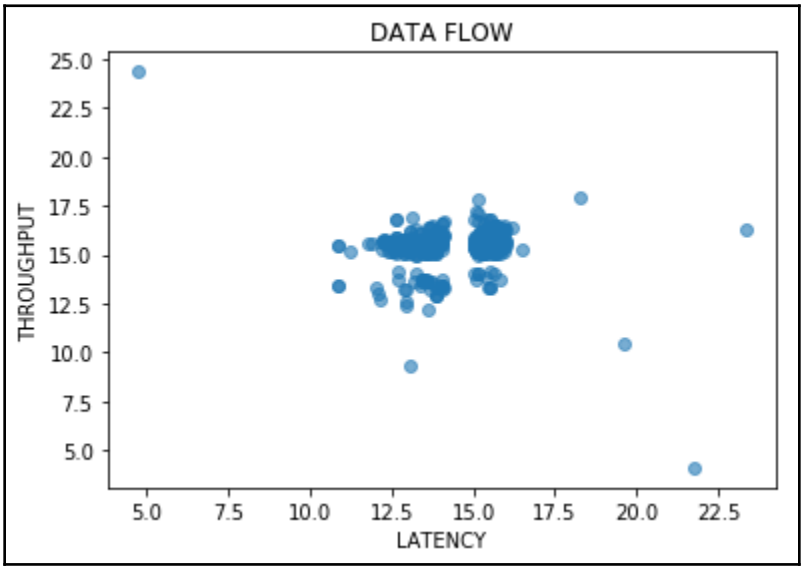

a12
a23
X1
X2
X3
a21
b22
b32
b12
b31
b33
b34
b11
b21
b14
b24
b13
y1
y2
y3
y4

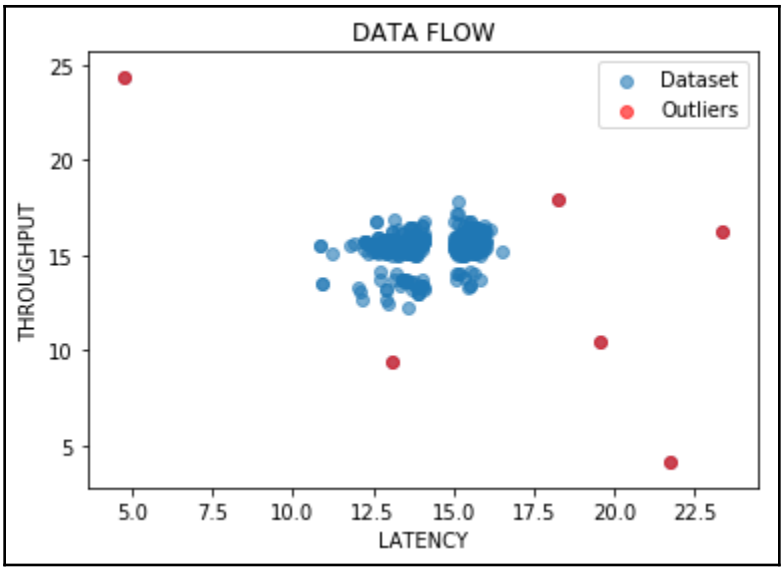

Malware Binary
011100110101
100101011010
10100001..
Binary to 8 bit vector
8 Bit vector to Grayscale Image

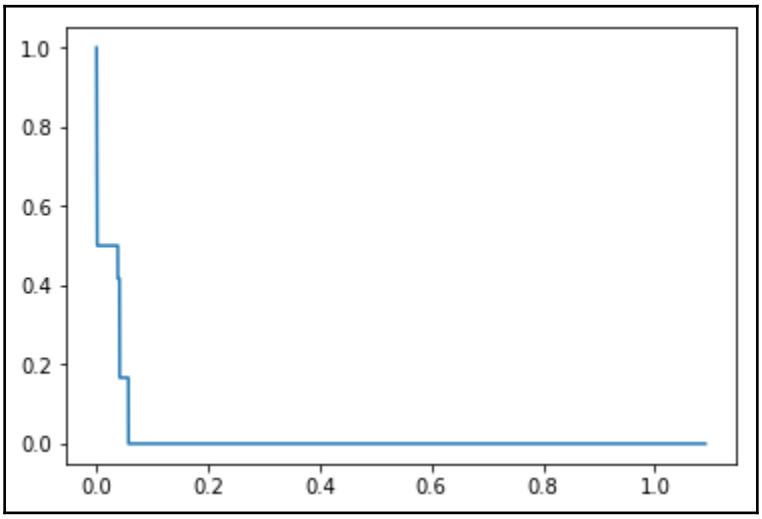
Chapter 5: Network Anomaly Detection with AI

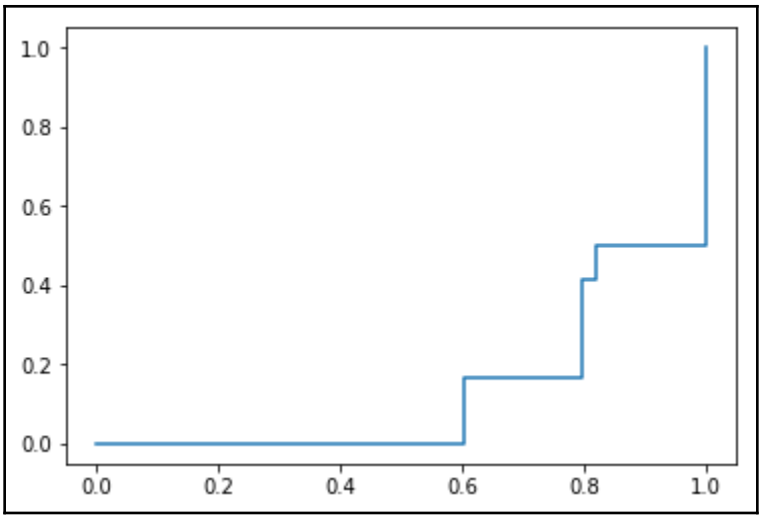



LATENCY
200
175
150
125
100
75
50
25
0
5
10
15
20
THROUGHPUT
300
250
200
150
100
50
0
5
10
15
20
25

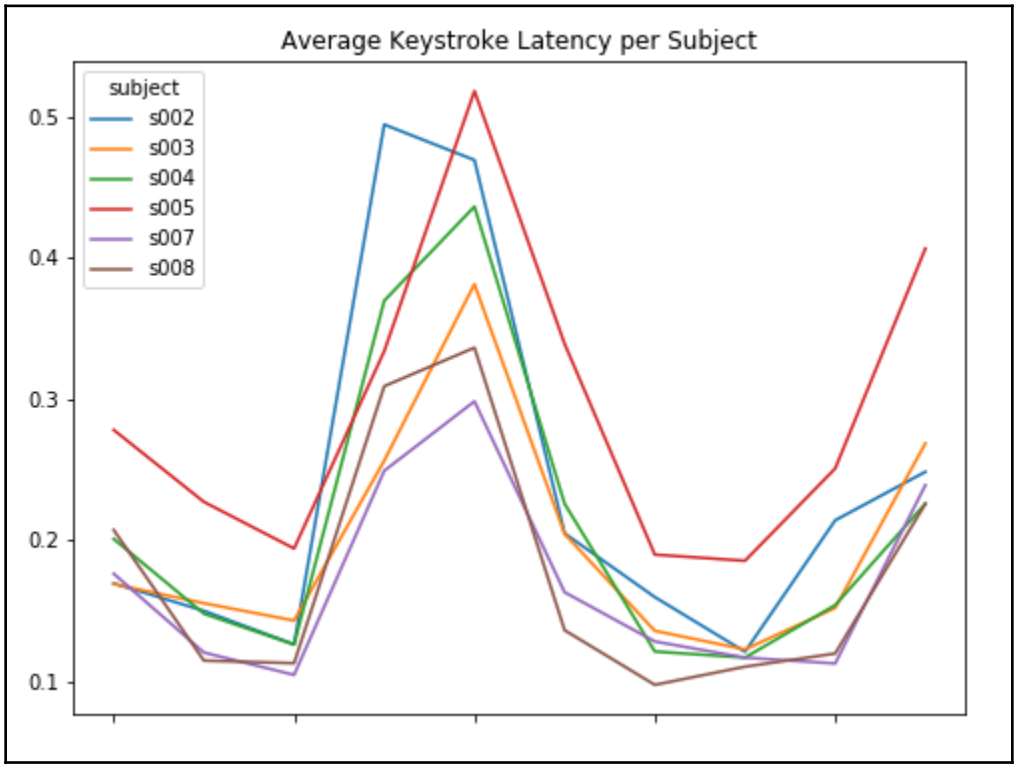

DATA FLOW
25.0
22.5
20.0
17.5
15.0
12.5
10.0
7.5
5.0
THROUGHPUT
5.0
7.5
10.0
12.5
15.0
17.5
20.0
22.5
LATENCY

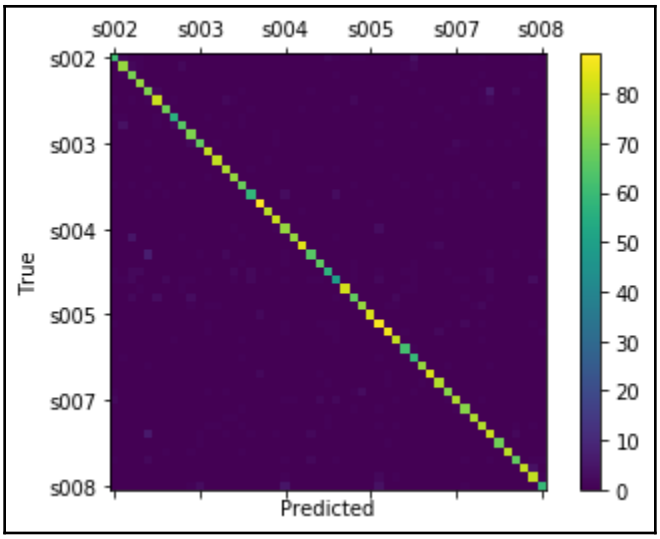

DATA FLOW
Dataset
Outliers
THROUGHPUT
LATENCY
25
20
15
10
5
5.0
7.5
10.0
12.5
15.0
17.5
20.0
22.5

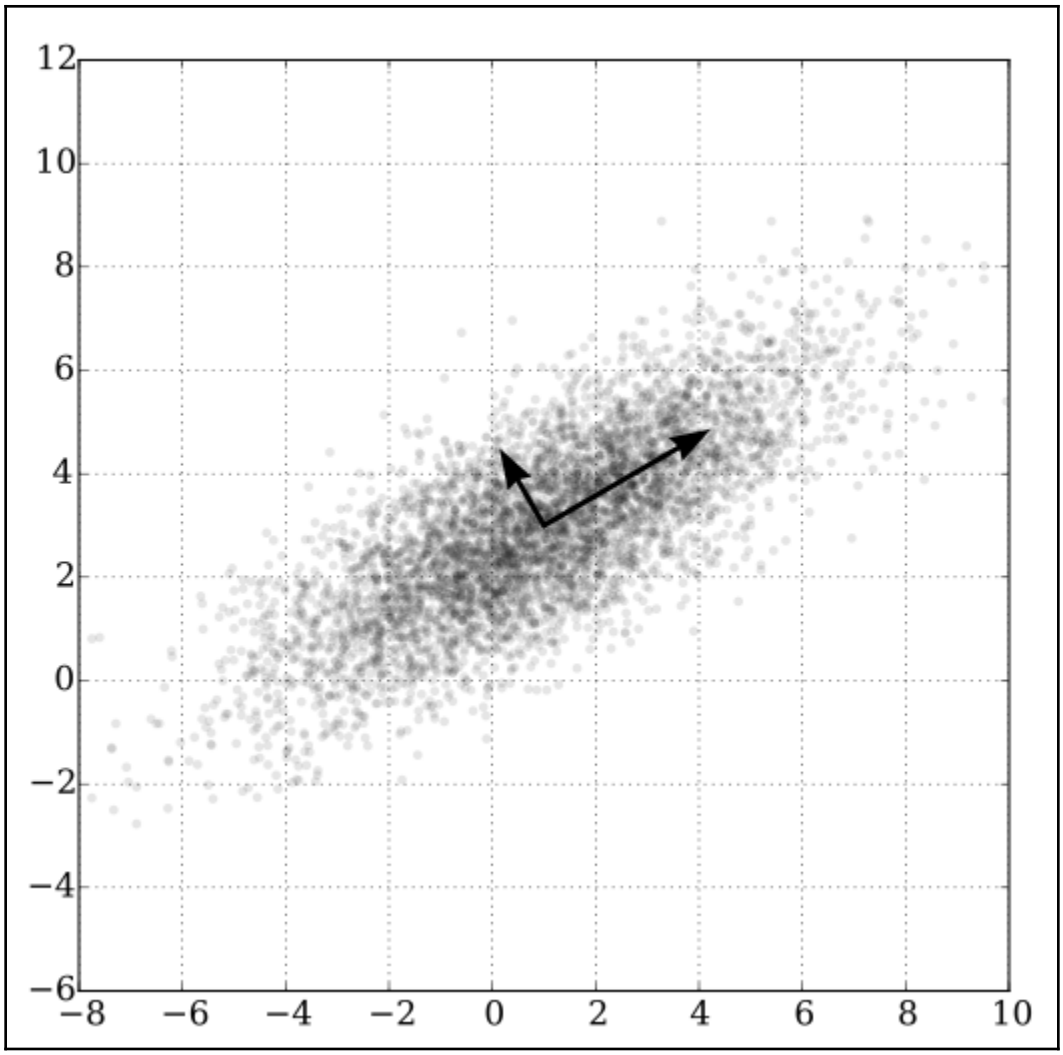

1.0
0.8
0.6
0.4
0.2
0.0
0.0
0.2
0.4
0.6
0.8
1.0

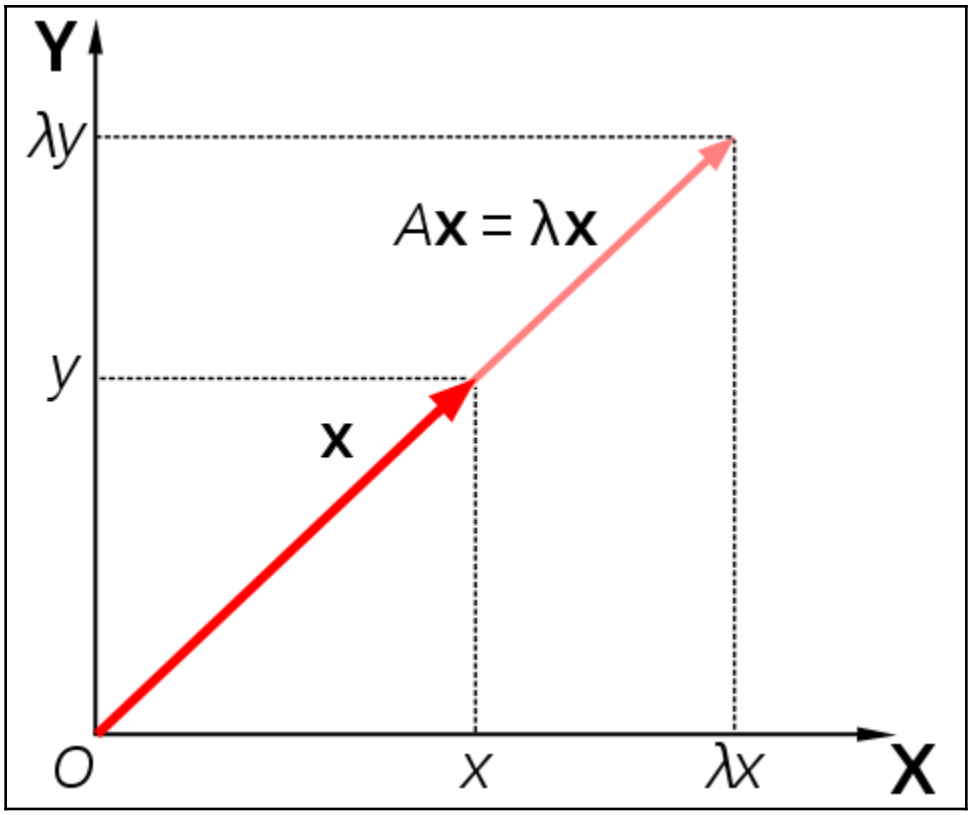

1.0
0.8
0.6
0.4
0.2
0.0
0.0
0.2
0.4
0.6
0.8
1.0

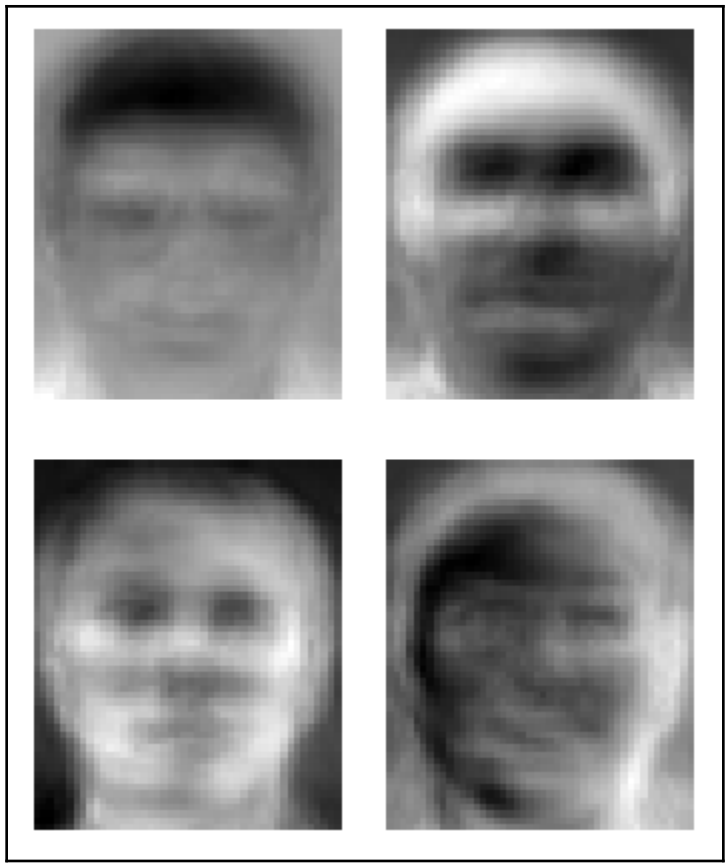
Chapter 6: Securing User Authentication



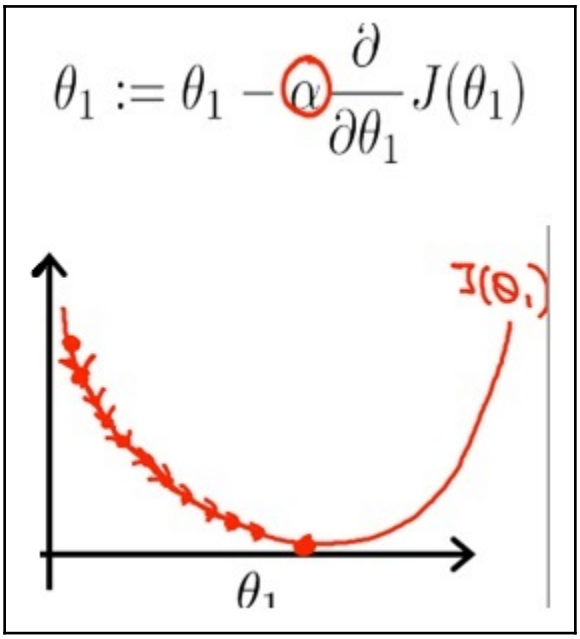

s002
s003
s004
s005
s007
s008
True
Predicted
80
70
60
50
40
30
20
10
0

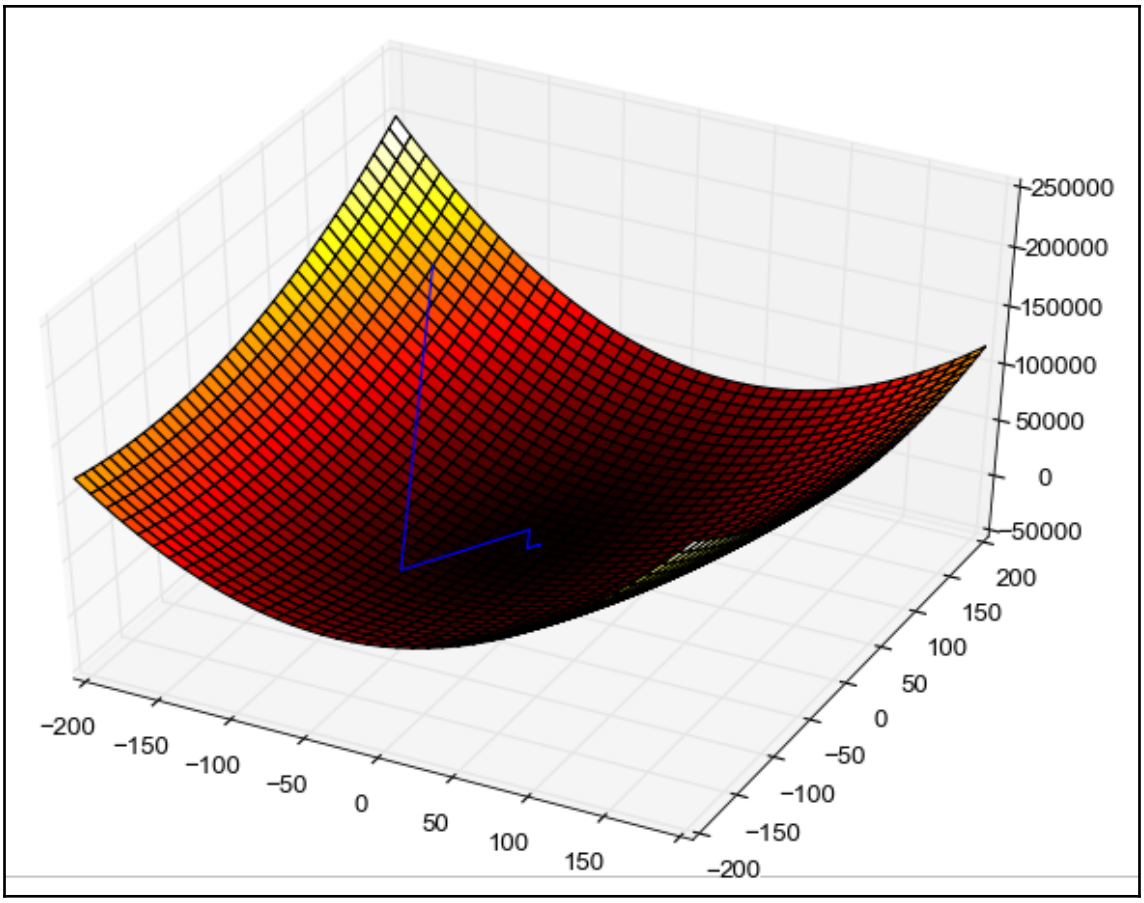

12
10
8
6
4
2
0
−2
−4
−6
−8
−6
−4
−2
0
2
4
6
8
10

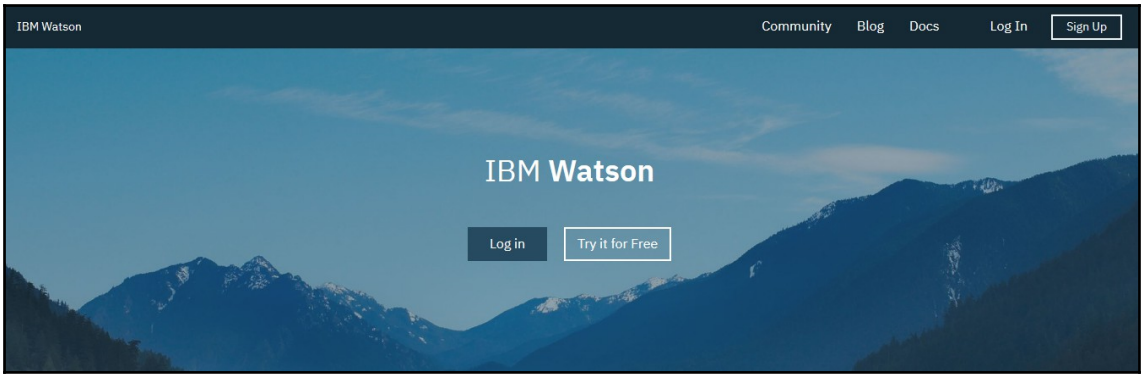

Y
λy
Ax = λx
y
x
O
x
λx
X

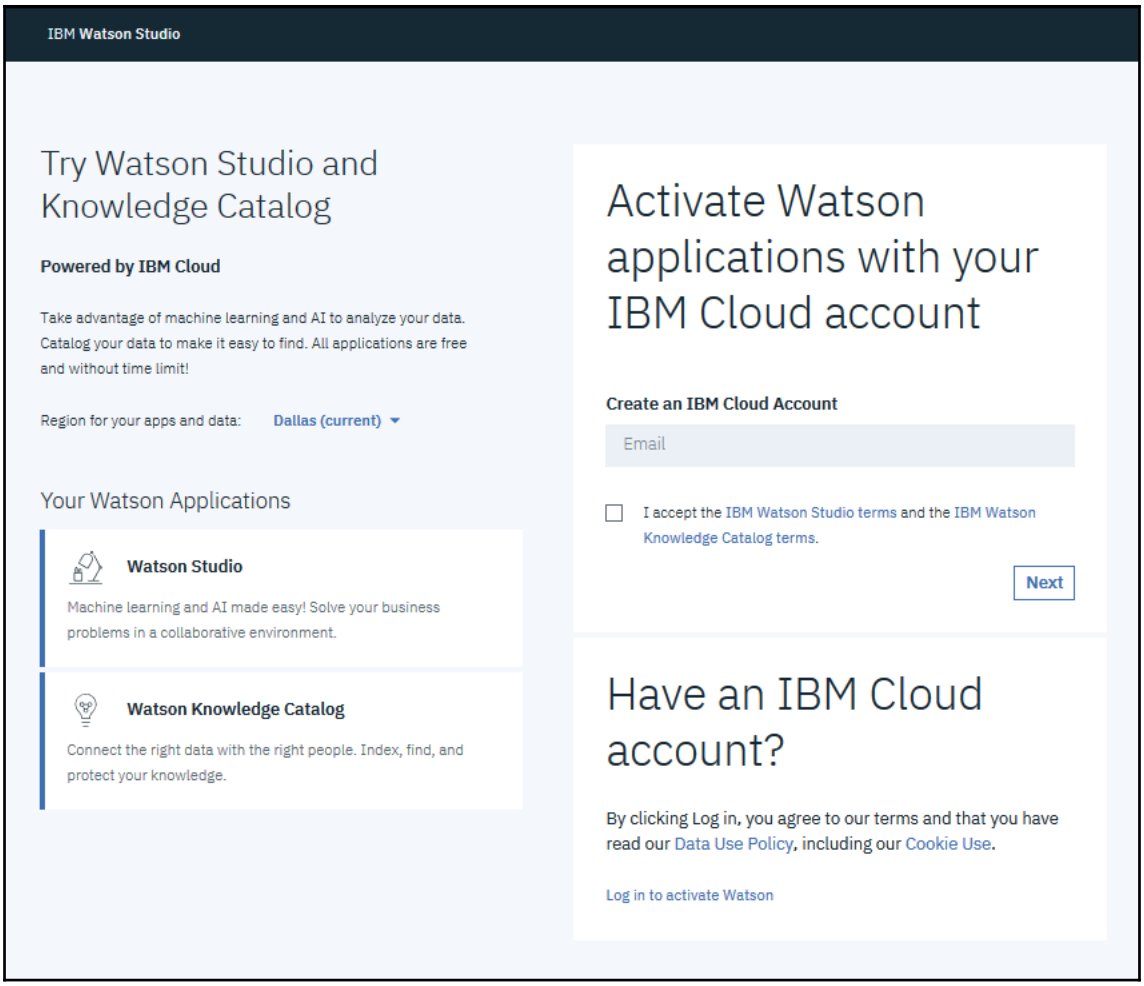


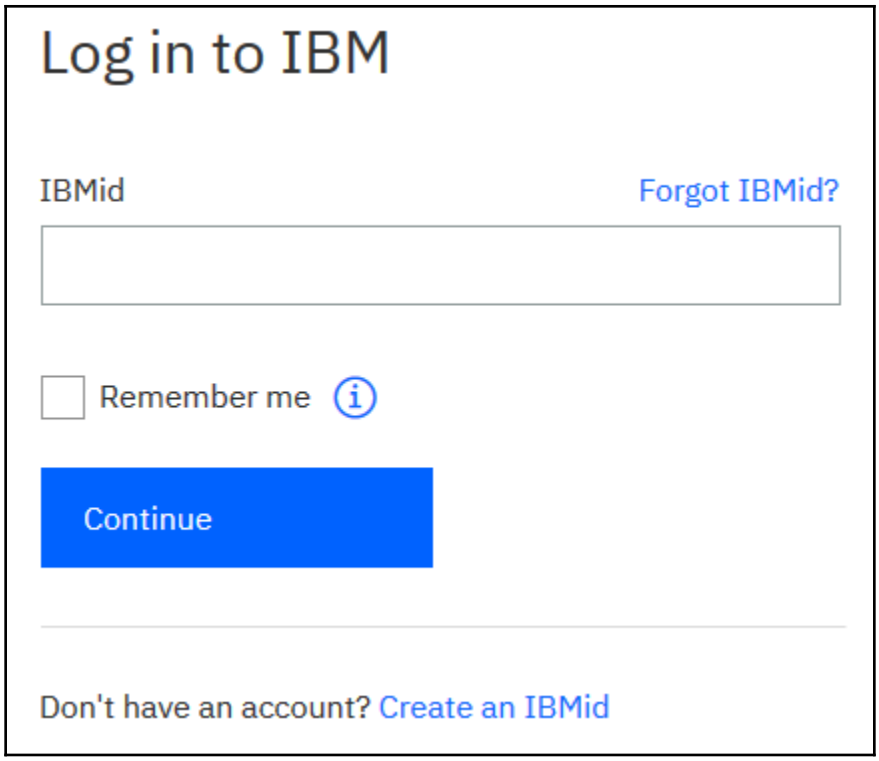
Chapter 7: Fraud Prevention with Cloud AI Solutions

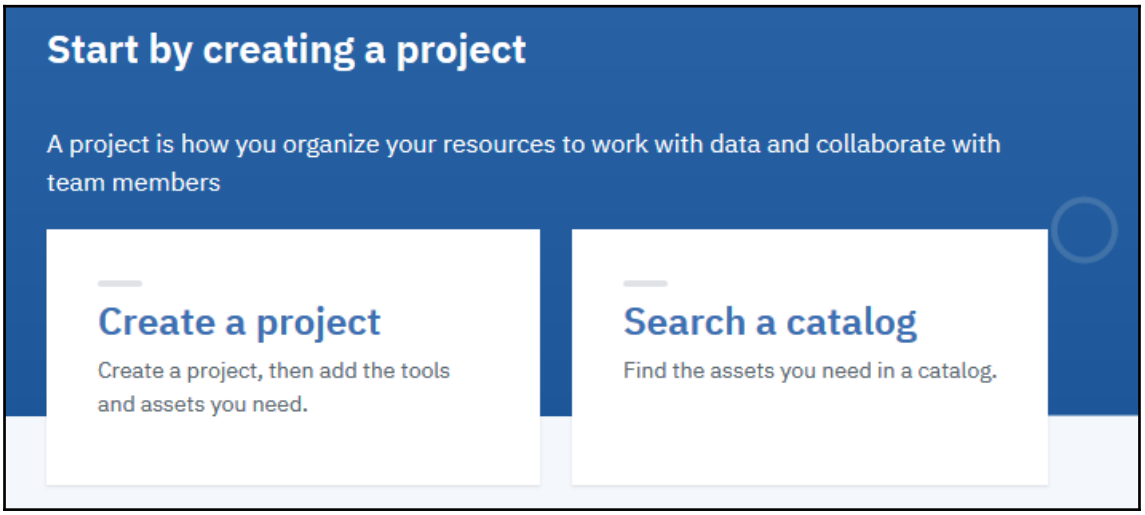


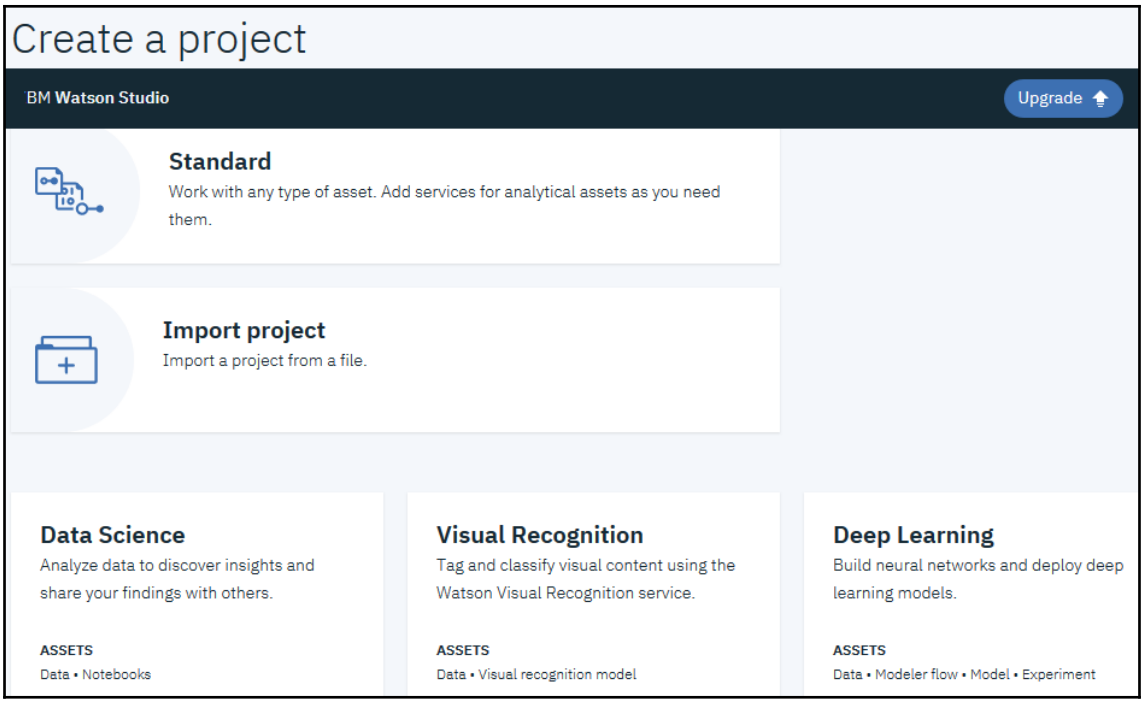

250000
200000
150000
100000
50000
0
−50000
200
150
100
50
0
−50
−100
−150
−200
−200
−150
−100
−50
0
50
100
150

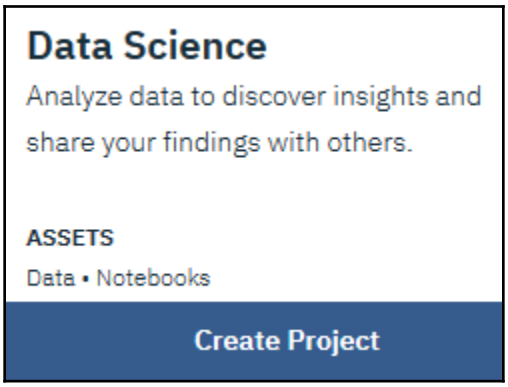

IBM Watson
Community
Blog
Docs
Log In
Sign Up
IBM Watson
Log in
Try it for Free

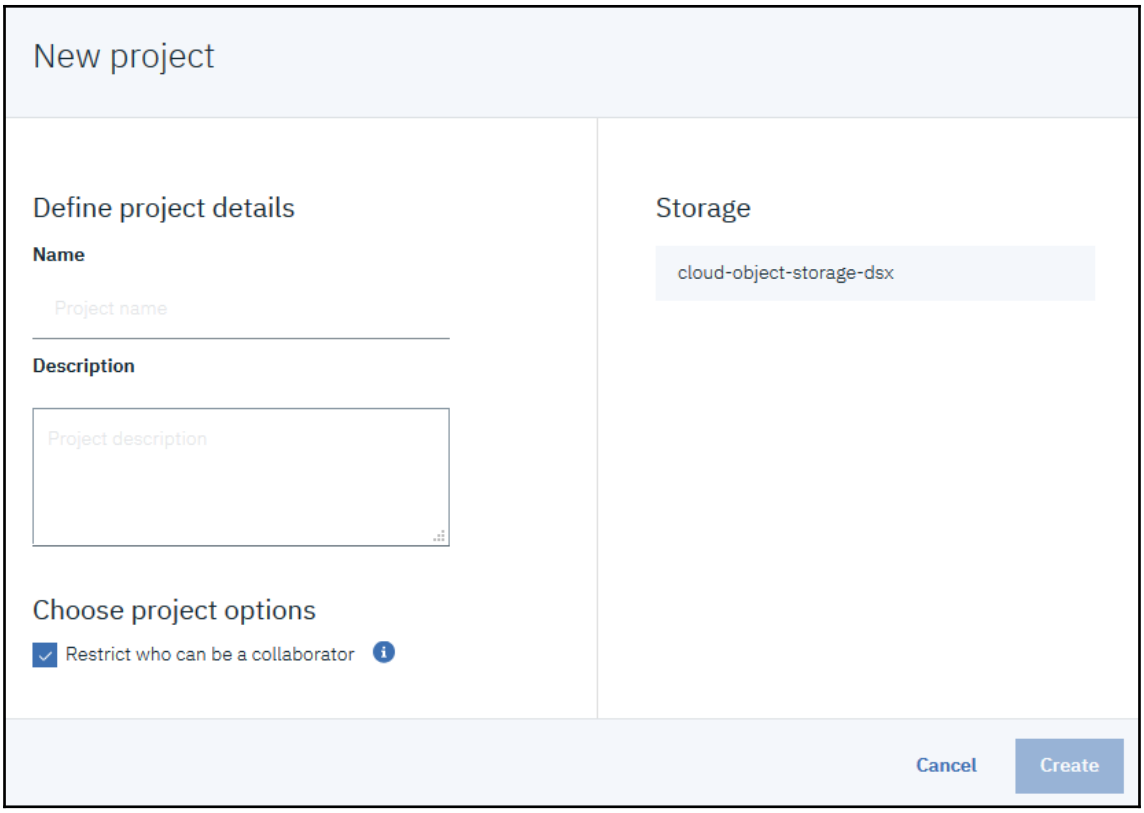

IBM Watson Studio
Try Watson Studio and Knowledge Catalog
Powered by IBM Cloud
Take advantage of machine learning and AI to analyze your data. Catalog your data to make it easy to find. All applications are free and without time limit!
Region for your apps and data:
Dallas (current)
Your Watson Applications
Watson Studio
Machine learning and AI made easy! Solve your business problems in a collaborative environment.
Watson Knowledge Catalog
Connect the right data with the right people. Index, find, and protect your knowledge.
Activate Watson applications with your IBM Cloud account
Create an IBM Cloud Account
Email
I accept the IBM Watson Studio terms and the IBM Watson Knowledge Catalog terms.
Next
Have an IBM Cloud account?
By clicking Log in, you agree to our terms and that you have read our Data Use Policy, including our Cookie Use.
Log in to activate Watson

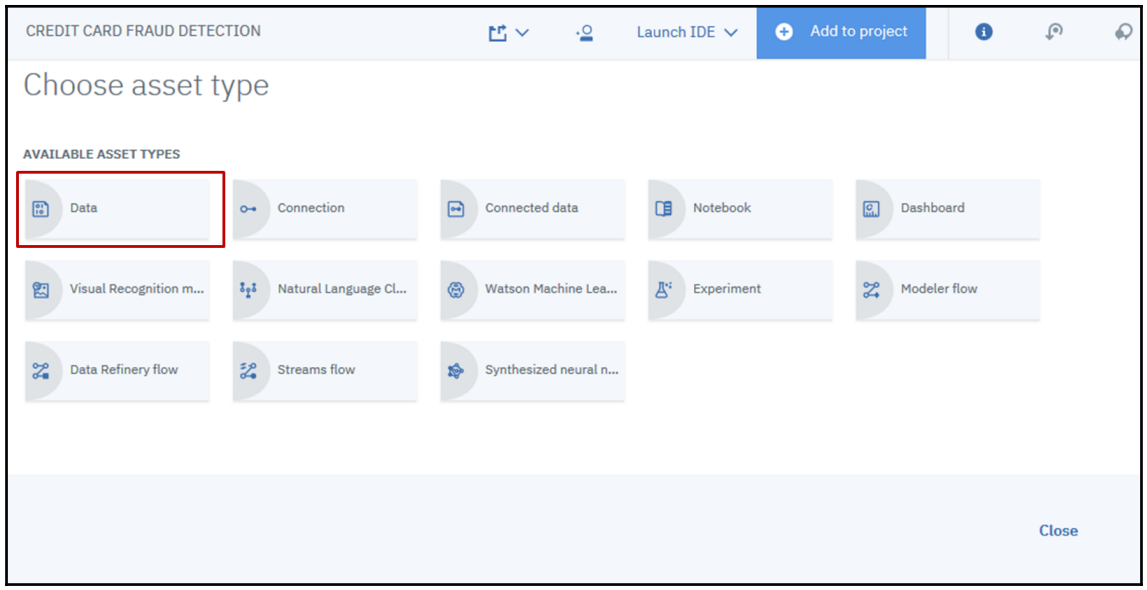

Log in to IBM
IBMid
Forgot IBMid?
Remember me
Continue
Don't have an account? Create an IBMid

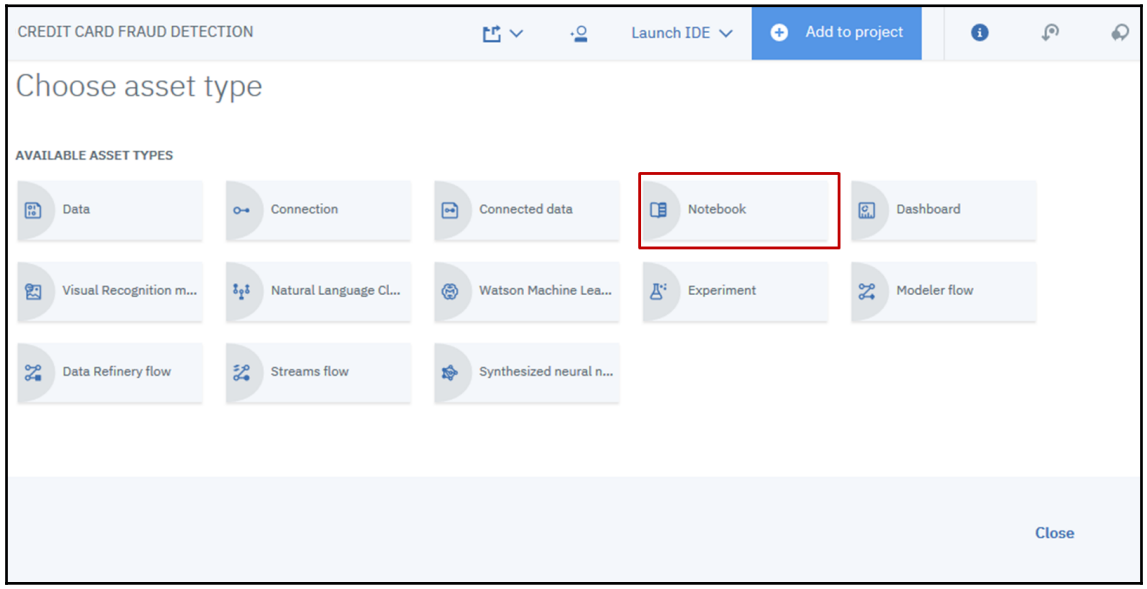

Start by creating a project
A project is how you organize your resources to work with data and collaborate with team members
Create a project
Create a project, then add the tools and assets you need.
Search a catalog
Find the assets you need in a catalog.

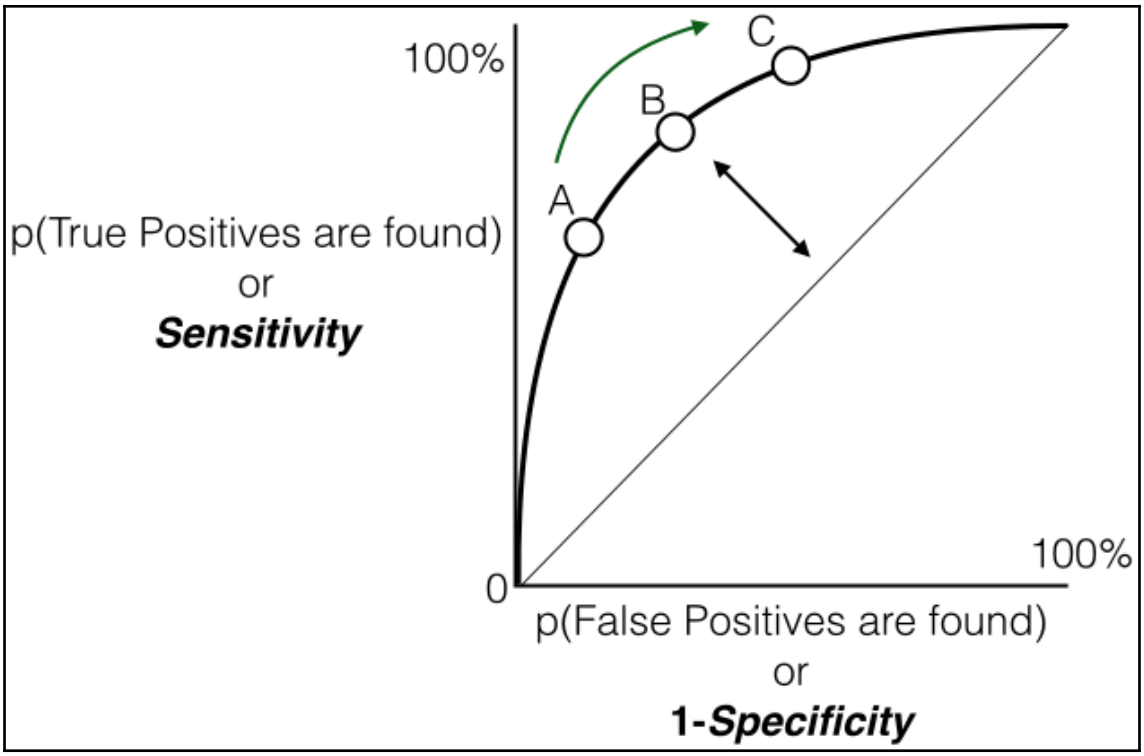

Create a project
BM Watson Studio
Upgrade
Standard
Work with any type of asset. Add services for analytical assets as you need them.
Import project
Import a project from a file.
Data Science
Analyze data to discover insights and share your findings with others.
ASSETS
Data • Notebooks
Visual Recognition
Tag and classify visual content using the Watson Visual Recognition service.
ASSETS
Data • Visual recognition model
Deep Learning
Build neural networks and deploy deep learning models.
ASSETS
Data • Modeler flow • Model • Experiment


Data Science
Analyze data to discover insights and share your findings with others.
ASSETS
Data • Notebooks
Create Project

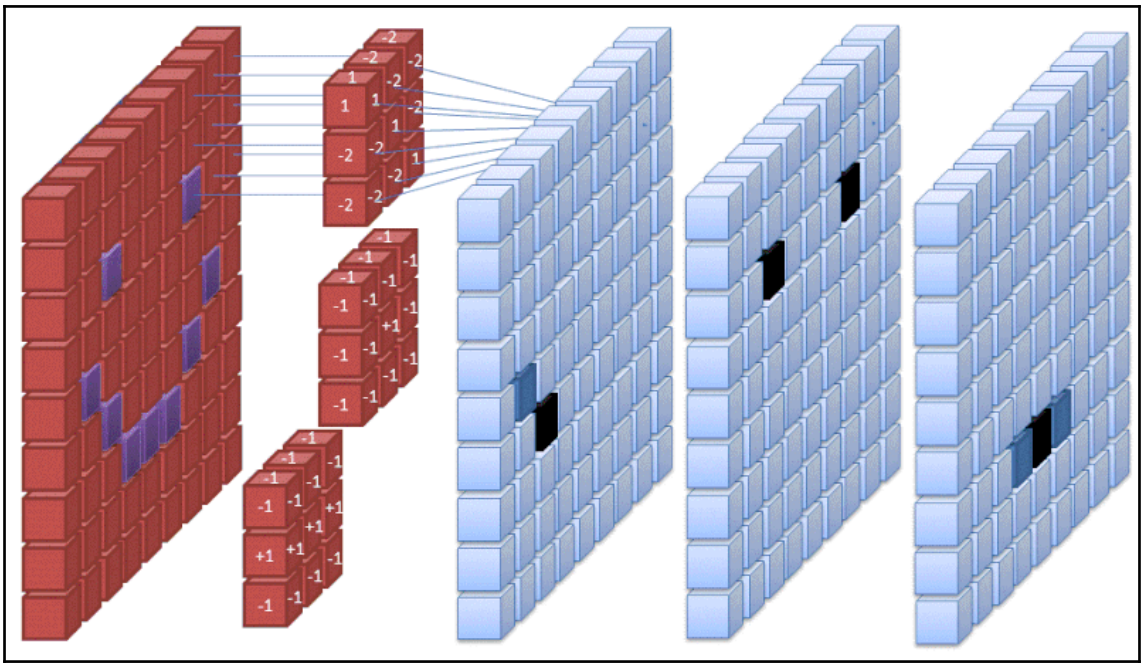

New project
Define project details
Name
Project name
Description
Project description
Choose project options
Restrict who can be a collaborator
Storage
cloud-object-storage-dsx
Cancel
Create

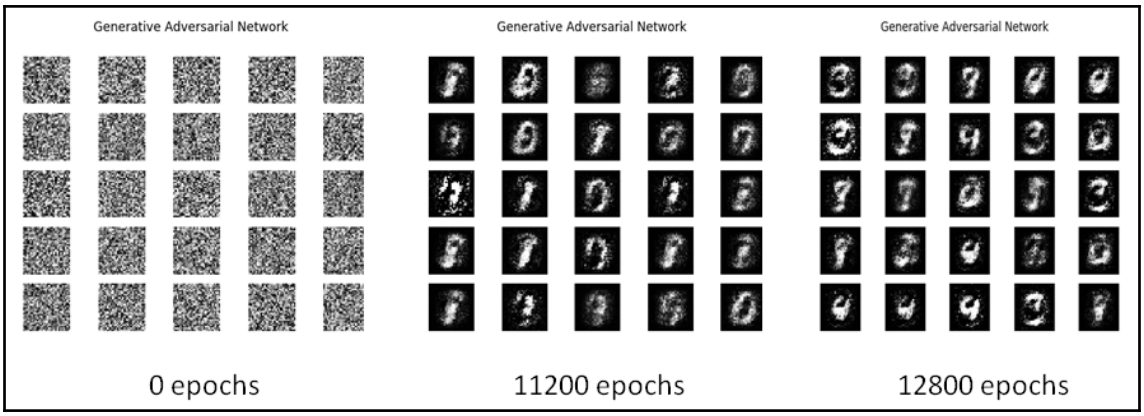

CREDIT CARD FRAUD DETECTION
Launch IDE
Add to project
Choose asset type
AVAILABLE ASSET TYPES
Data
Connection
Connected data
Notebook
Dashboard
Visual Recognition m...
Natural Language Cl...
Watson Machine Lea...
Experiment
Modeler flow
Data Refinery flow
Streams flow
Synthesized neural n...
Close

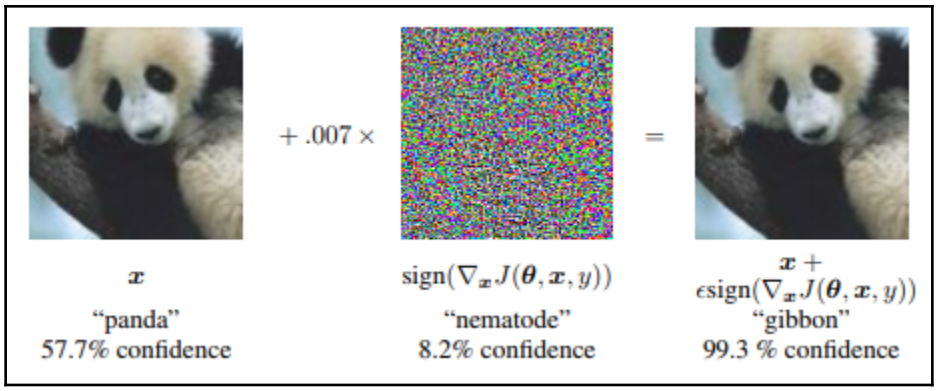

CREDIT CARD FRAUD DETECTION
Launch IDE
Add to project
Choose asset type
AVAILABLE ASSET TYPES
Data
Connection
Connected data
Notebook
Dashboard
Visual Recognition m...
Natural Language Cl...
Watson Machine Lea...
Experiment
Modeler flow
Data Refinery flow
Streams flow
Synthesized neural n...
Close


100%
C
B
A
p(True Positives are found)
or
Sensitivity
0
100%
p(False Positives are found)
or
1-Specificity

Chapter 8: GANs - Attacks and Defenses






+ .007 ×
=
$\boldsymbol{x}$
"panda"
57.7% confidence
sign($\nabla_{\boldsymbol{x}} J(\boldsymbol{\theta}, \boldsymbol{x}, y)$)
"nematode"
8.2% confidence
$\boldsymbol{x} +$
ϵsign($\nabla_{\boldsymbol{x}} J(\boldsymbol{\theta}, \boldsymbol{x}, y)$)
"gibbon"
99.3 % confidence

Chapter 9: Evaluating Algorithms

Ordinal Encoding example:

Original encoding	Ordinal encoding
Low	1
Medium	2
High	3

One-Hot Encoding example:

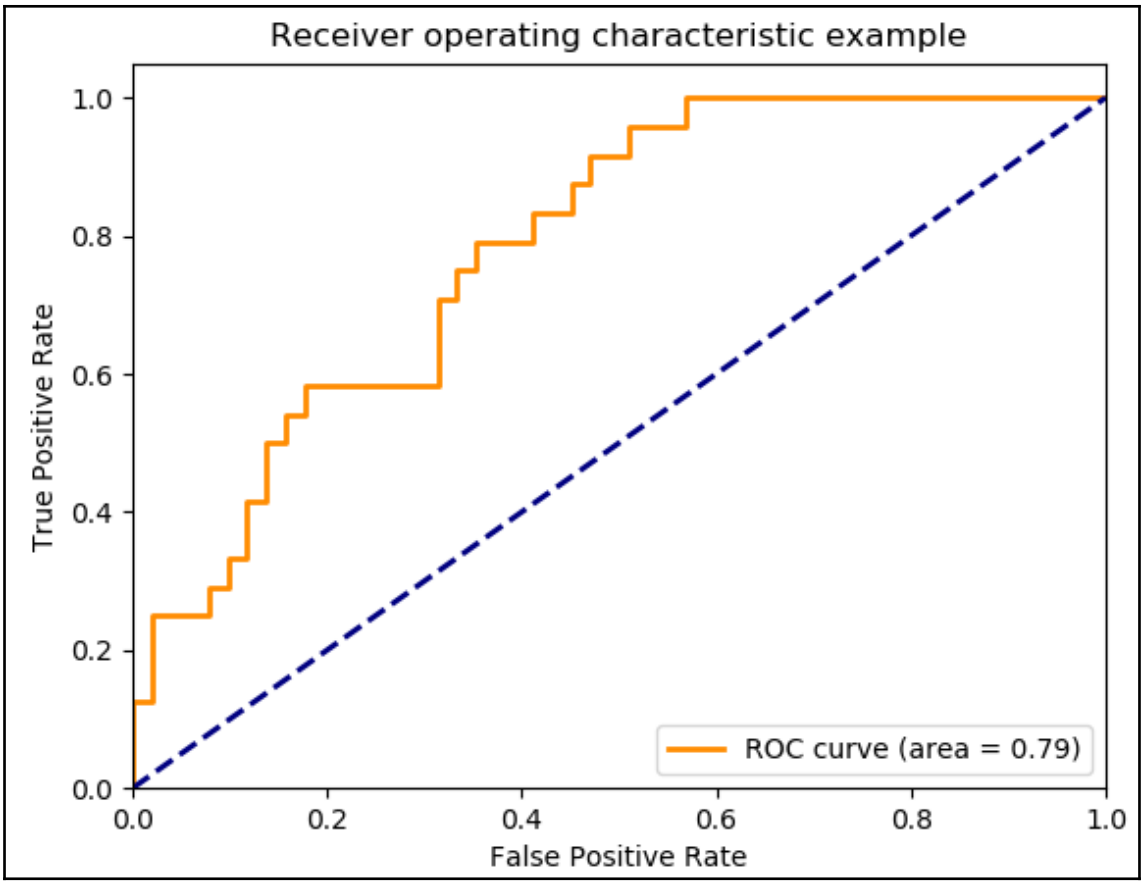
State	B1	B2	B3
England	1	0	0
France	0	1	0
Germany	0	0	1

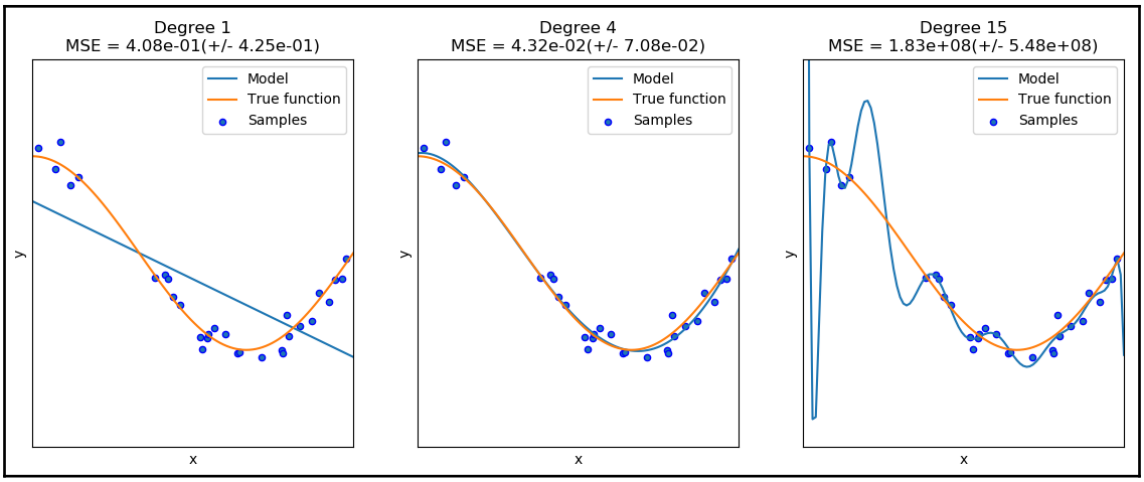
Dummy Encoding example:

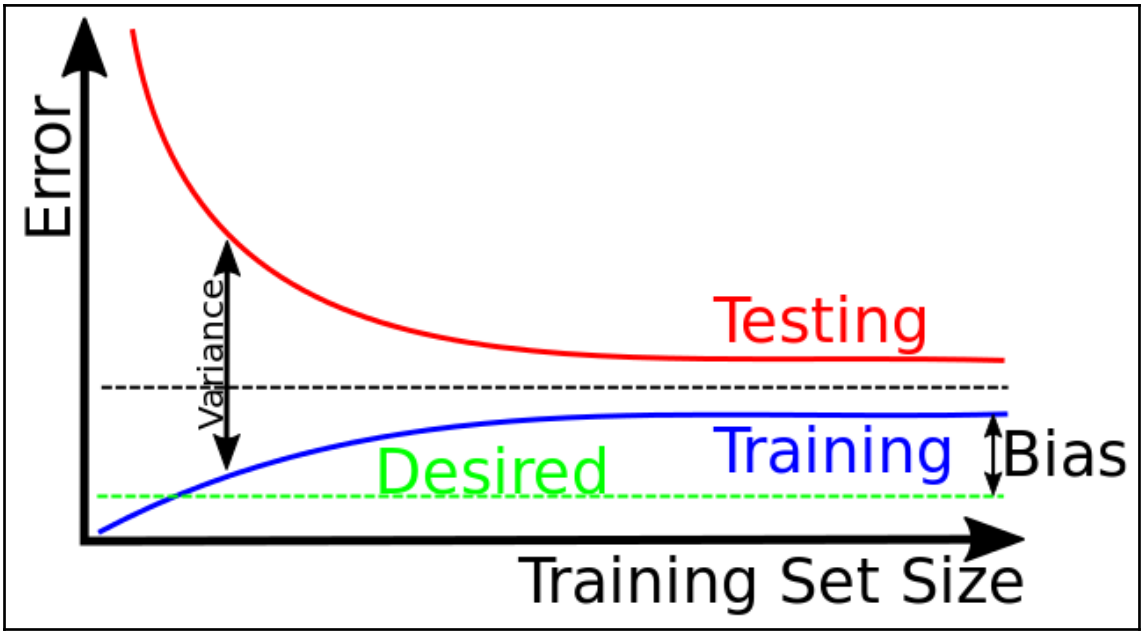
State	B1	B2
England	1	0
France	0	1
Germany	0	0

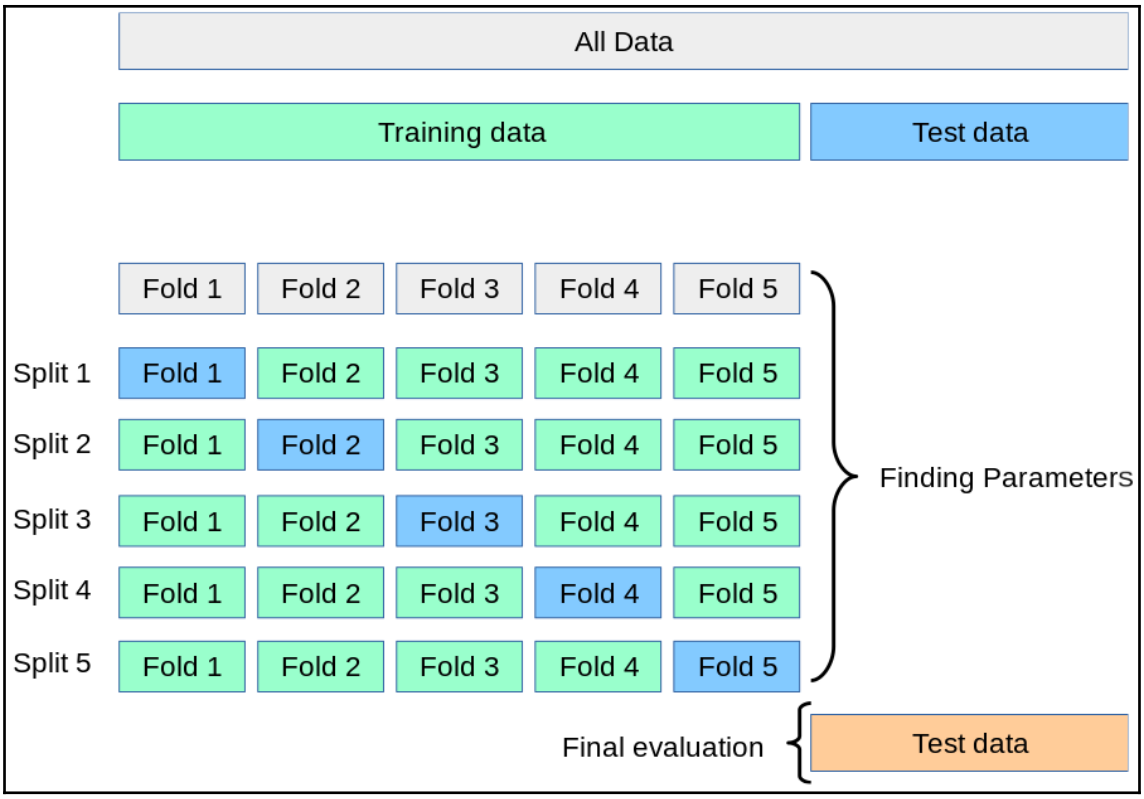
Confusion Matrix:

Predicted	Actual Fraud	Actual Not Fraud
Fraud	True Positive (TP)	False Positive (FP)
Not Fraud	False Negative (FN)	True Negative (TN)


Receiver operating characteristic example
True Positive Rate
False Positive Rate
0.0
0.2
0.4
0.6
0.8
1.0
ROC curve (area = 0.79)


Degree 1
MSE = 4.08e-01(+/- 4.25e-01)
Degree 4
MSE = 4.32e-02(+/- 7.08e-02)
Degree 15
MSE = 1.83e+08(+/- 5.48e+08)
Model
True function
Samples
x
y


Error
Variance
Testing
Training
Bias
Desired
Training Set Size


All Data
Training data
Test data
Fold 1
Fold 2
Fold 3
Fold 4
Fold 5
Split 1
Split 2
Split 3
Split 4
Split 5
Finding Parameters
Final evaluation
Test data

Chapter 10: Assessing your AI Arsenal