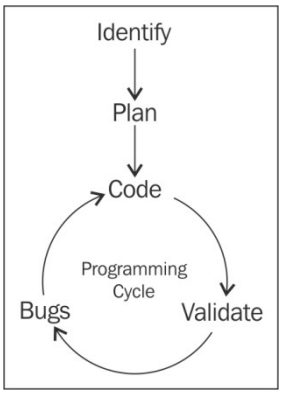
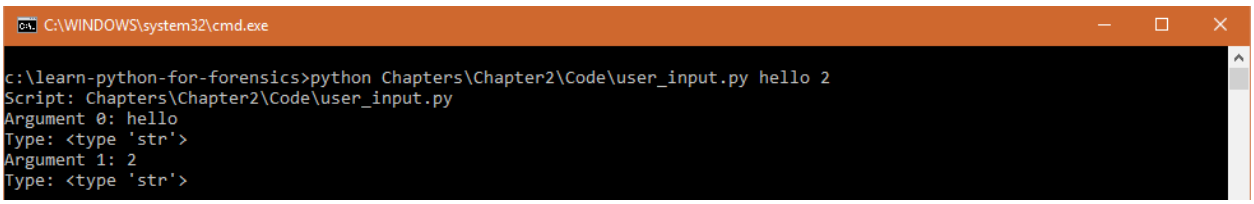
Chapter 1

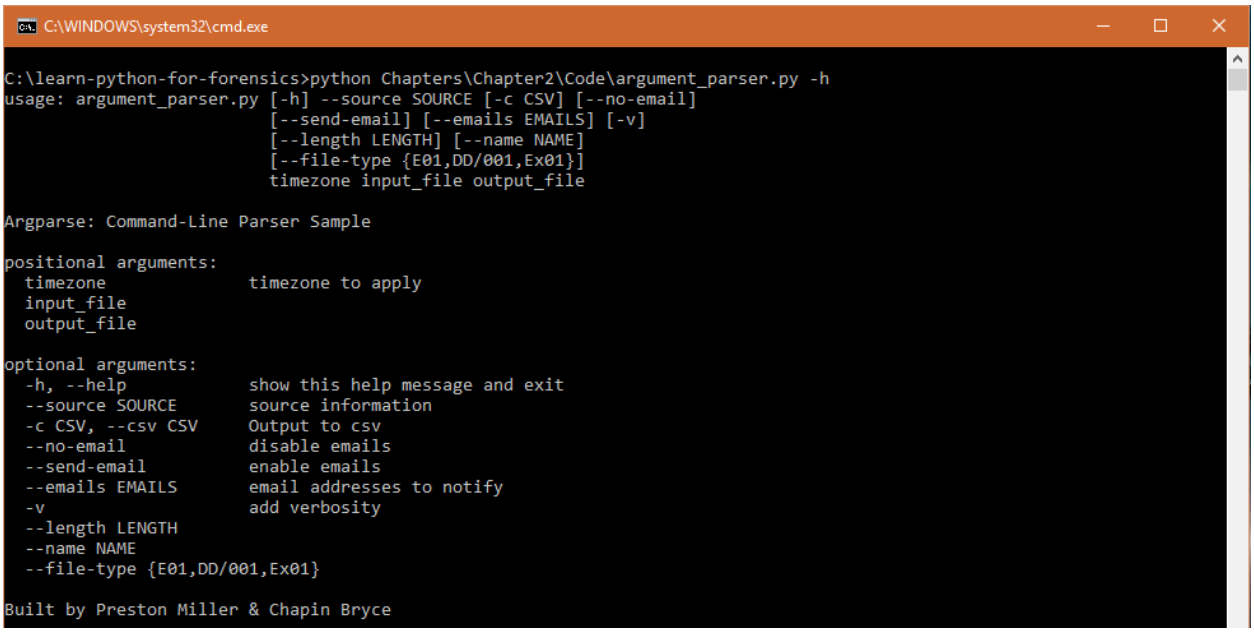



```
C:\WINDOWS\system32\cmd.exe

C:\learn-python-for-forensics>python Chapters\Chapter1\Code\hello.py
Hello World!
```

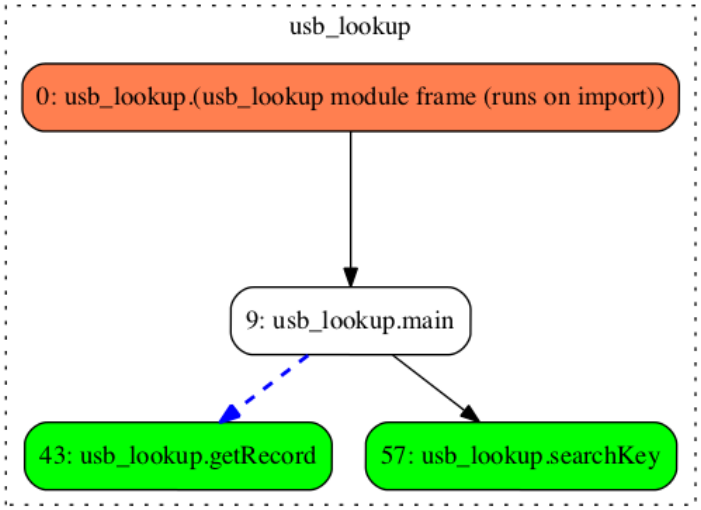
Chapter 2

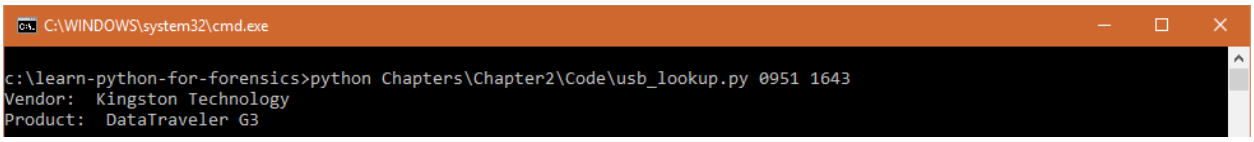

C:\WINDOWS\system32\cmd.exe
c:\learn-python-for-forensics>python Chapters\Chapter2\Code\unix_converter.py
Unix timestamp to convert:
>> 1445401740
10/21/2015 04:29:00 AM UTC


C:\WINDOWS\system32\cmd.exe
c:\learn-python-for-forensics>python Chapters\Chapter2\Code\user_input.py hello 2
Script: Chapters\Chapter2\Code\user_input.py
Argument 0: hello
Type: <type 'str'>
Argument 1: 2
Type: <type 'str'>

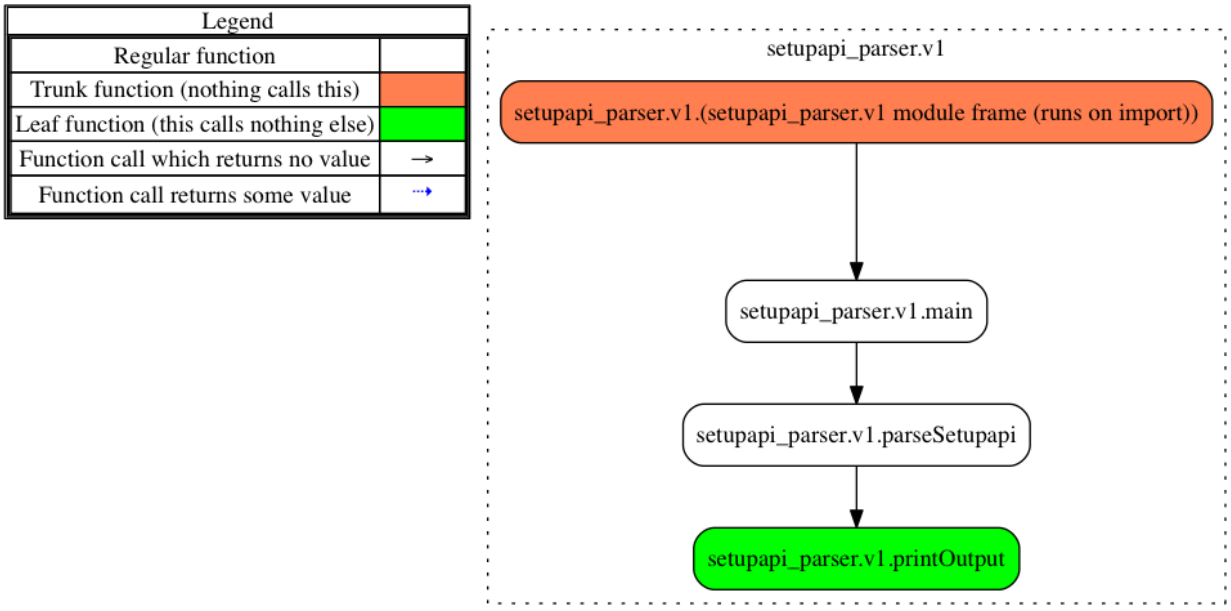

C:\WINDOWS\system32\cmd.exe
C:\learn-python-for-forensics>python Chapters\Chapter2\Code\argument_parser.py -h
usage: argument_parser.py [-h] --source SOURCE [-c CSV] [--no-email]
[--send-email] [--emails EMAILS] [-v]
[--length LENGTH] [--name NAME]
[--file-type {E01,DD/001,Ex01}]
timezone input_file output_file
Argparse: Command-Line Parser Sample
positional arguments:
timezone timezone to apply
input_file
output_file
optional arguments:
-h, --help show this help message and exit
--source SOURCE source information
-c CSV, --csv CSV Output to csv
--no-email disable emails
--send-email enable emails
--emails EMAILS email addresses to notify
-v add verbosity
--length LENGTH
--name NAME
--file-type {E01,DD/001,Ex01}
Built by Preston Miller & Chapin Bryce

Legend	
Regular function	
Trunk function (nothing calls this)	
Leaf function (this calls nothing else)	
Function call which returns no value	→
Function call returns some value	⇢

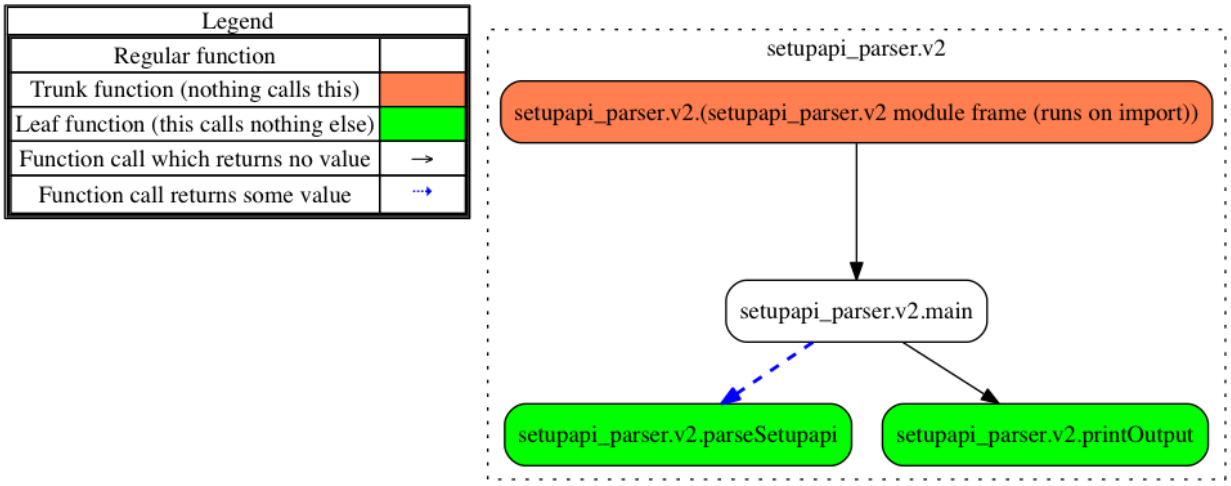




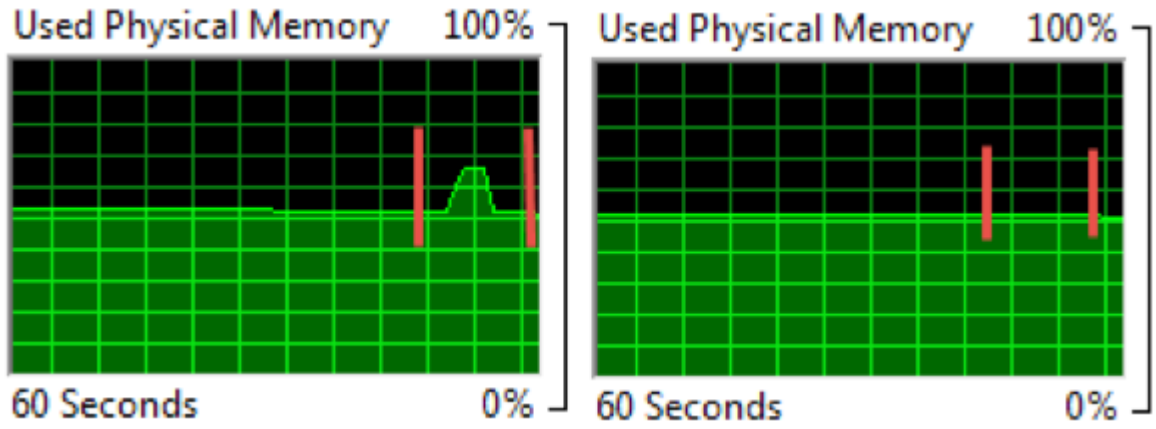
Chapter 3

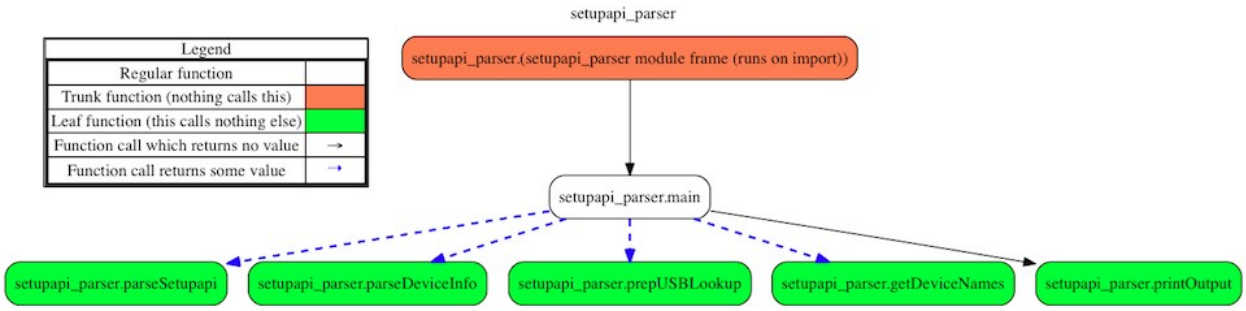



```
C:\WINDOWS\system32\cmd.exe

c:\learn-python-for-forensics>python Chapters\Chapter3\Code\setupapi_parser.v1.py
====================
SetupAPI Parser,  0.01
====================
Device: USB\VID_0E0F&PID_0008\000650268328]
First Install: 2016/03/10 14:59:53.099
Device: USB\VID_0E0F&PID_0003&MI_00\7&2a7d3009&0&0000]
First Install: 2016/03/10 14:59:53.317
Device: USB\VID_0E0F&PID_0003&MI_01\7&2a7d3009&0&0001]
First Install: 2016/03/10 14:59:53.317
```



```
C:\WINDOWS\system32\cmd.exe

C:\learn-python-for-forensics>python Chapters\Chapter3\Code\setupapi_parser.v2.py setupapi.dev.log
====================
SetupAPI Parser,  0.02
====================

Device: usb\vid_0e0f&pid_000b\6&103465e1&0&1]
First Install: 2016/03/10 14:59:49.604

Device: usb\vid_0e0f&pid_0002\6&b77da92&0&2]
First Install: 2016/03/10 14:59:49.994

Device: usb\vid_0e0f&pid_0003\6&b77da92&0&1]
First Install: 2016/03/10 14:59:50.306
```

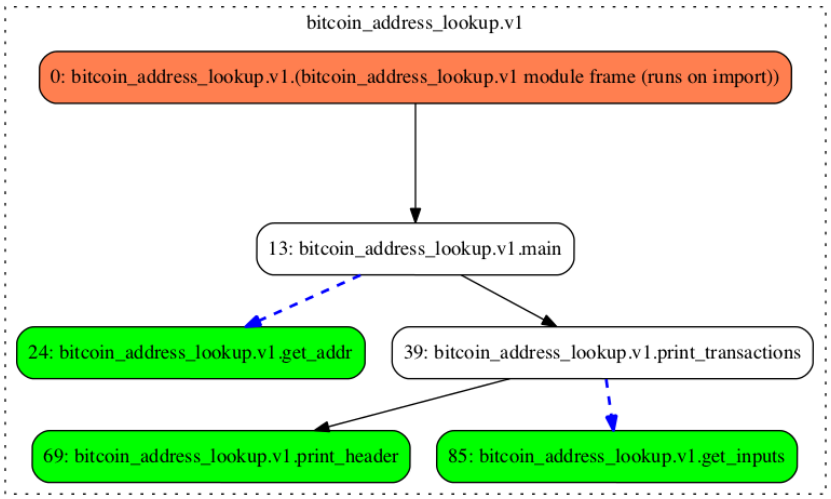





```
C:\WINDOWS\system32\cmd.exe

C:\learn-python-for-forensics>python Chapters\Chapter3\Code\setupapi_parser.py setupapi.dev.log
--------------
First Installation Date: 2016/03/10 14:59:49.604
Product ID: 000b
UID: 6&103465e1&0&1
Product Name: Unknown
Vendor Name:  VMware, Inc.
Vendor ID: 0e0f
Revision:
--------------
First Installation Date: 2016/03/10 14:59:49.994
Product ID: 0002
UID: 6&b77da92&0&2
Product Name:  Virtual USB Hub
Vendor Name:  VMware, Inc.
Vendor ID: 0e0f
Revision:
--------------
```

Chapter 4

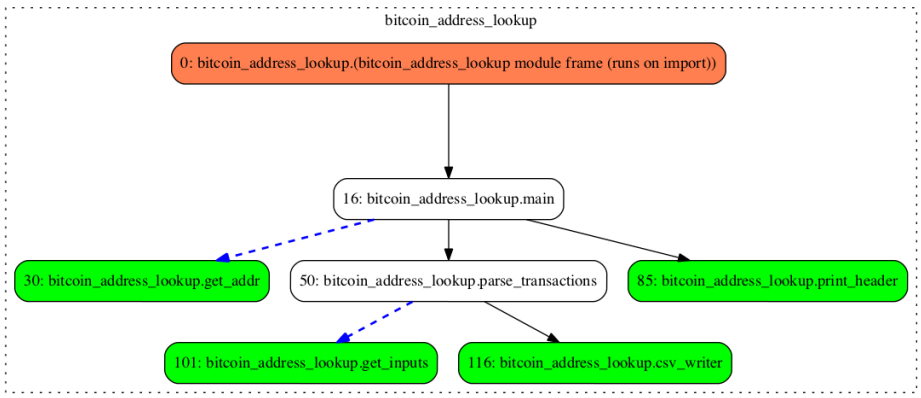
Legend	
Regular function	
Trunk function (nothing calls this)	
Leaf function (this calls nothing else)	
Function call which returns no value	→
Function call returns some value	⇢




```
C:\WINDOWS\system32\cmd.exe

C:\learn-python-for-forensics>python Chapters\Chapter4\Code\bitcoin_address_lookup.v1.py 125riCXE2MtxHbNZkRtExPGAfbv7LsY
3Wa
======================
Bitcoin Address Lookup,  0.01
======================

Address: 125riCXE2MtxHbNZkRtExPGAfbv7LsY3Wa
Current Balance: 0.00000000 BTC
Total Sent: 0.80000000 BTC
Total Received: 0.80000000 BTC
Number of Transactions: 25
======================

Transactions
Transaction #0
Transaction Hash: 467a944dd0d7ed0bc41948675b48296094f04cbe035e048d6fa01c4eb5bb29c9
Transaction Date: 09/20/2015 11:56:24 PM
1J6bKdNo49s4c6fAjFFZgJLCgGphQrPvYM & 1FKGLnDiDa1b3dv8gimUJYAh8MzCo4Rook & 125riCXE2MtxHbNZkRtExPGAfbv7LsY3Wa & 1GxTRccWA
3DztJasEtBG1wm7pEcT7NogTE --> 1CbQp7zhUWbDeBSQTeeD6XnWNdH2GDYP1P (2.16686450 BTC)
1J6bKdNo49s4c6fAjFFZgJLCgGphQrPvYM & 1FKGLnDiDa1b3dv8gimUJYAh8MzCo4Rook & 125riCXE2MtxHbNZkRtExPGAfbv7LsY3Wa & 1GxTRccWA
3DztJasEtBG1wm7pEcT7NogTE --> 1GxTRccWA3DztJasEtBG1wm7pEcT7NogTE (0.25110936 BTC)
======================

Transaction #1
Transaction Hash: 399e3bc8b051def19a725888e2eb316c6247f8033fe4b875dd998f3ae42a6ff1
Transaction Date: 09/20/2015 10:17:58 PM
125riCXE2MtxHbNZkRtExPGAfbv7LsY3Wa --> 3HdbKdofxudExko4KPjAPgp4Jsy1Jy7fkq (0.00021762 BTC)
125riCXE2MtxHbNZkRtExPGAfbv7LsY3Wa --> 125riCXE2MtxHbNZkRtExPGAfbv7LsY3Wa (0.51281430 BTC)
======================
```

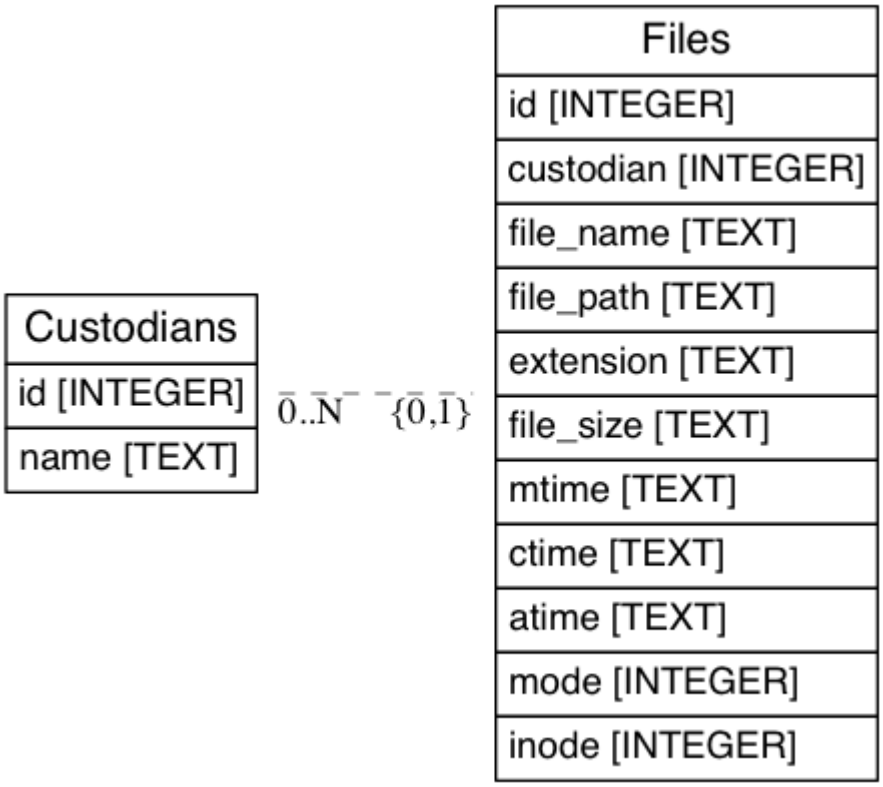
```
btc_addr_lookup - Notepad
File  Edit  Format  View  Help
2016-03-18 00:40:39,999 | INFO | Starting Bitcoin Address Lookup v.0.02
2016-03-18 00:40:39,999 | DEBUG | System win32
2016-03-18 00:40:39,999 | DEBUG | Version 2.7.6 (default, Nov 10 2013, 19:24:18) [MSC v.1500 32 bit (Intel)]
2016-03-18 00:40:40,002 | INFO | Initiated program for 125riCXE2MtxHbNZkRtExPGAfbv7LsY3Wa address
2016-03-18 00:40:40,002 | INFO | Obtaining JSON structured data from blockchain.info
2016-03-18 00:40:40,473 | INFO | Printing account and transaction data to console.
```

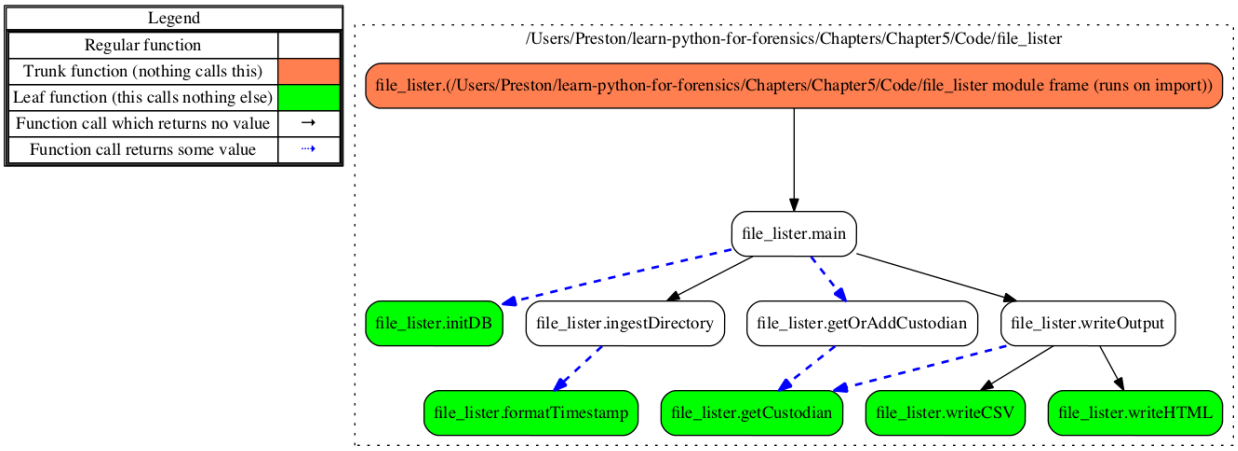
Legend	
Regular function	
Trunk function (nothing calls this)	
Leaf function (this calls nothing else)	
Function call which returns no value	→
Function call returns some value	⇢



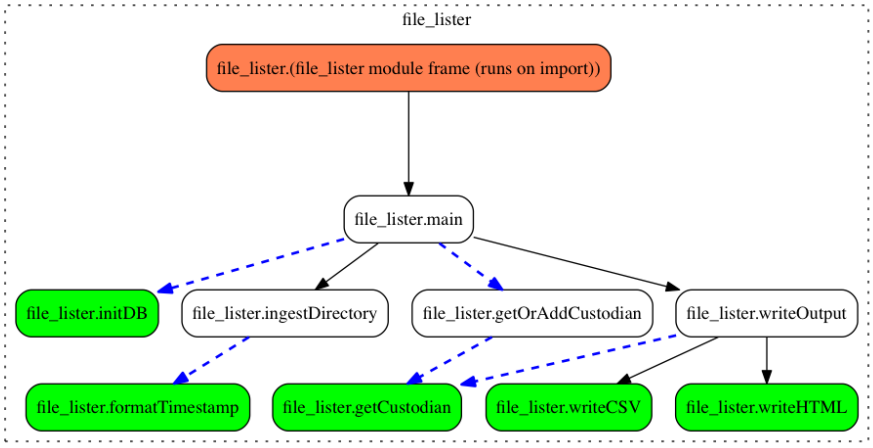
A	B	C	D	E	F	G
Index	Date	Transaction Hash	Inputs	Outputs	Values	Total
0	9/20/15 23:56	467a944dd0d7ed0bc41948675b48296094f04cbe035e048d6fa01c4eb5bb29c9	1J6bKdNo49s4c6fAjFFZgJLCgGphQrPvYM 1FKGLnDiDa1b3dv8gimUJYAh8MzCo4Rook 125riCXE2MtxHbNZkRtExPGAfbv7LsY3Wa 1GxTRccWA3DztJasEtBG1wm7pEcT7NogTE	1GxTRccWA3DztJasEtBG1wm7pEcT7NogTE 1CbQp7zhUWbDeBSQTeeD6XnWNdH2GDYP1P	0.25110936 2.1668645	2.41797386
1	9/20/15 22:17	399e3bc8b051def19a725888e2eb316c6247f8033fe4b875dd998f3ae42a6ff1	125riCXE2MtxHbNZkRtExPGAfbv7LsY3Wa	125riCXE2MtxHbNZkRtExPGAfbv7LsY3Wa 3HdbKdofxudExko4KPjAPgp4Jsy1Jy7fkq	0.5128143 0.00021762	0.51303192
2	9/20/15 20:11	4e569e655f322db5c7f9dcf7cd859b95766f5fe958007a354db5ef9e06018917	125riCXE2MtxHbNZkRtExPGAfbv7LsY3Wa	3GtGscT34cjR2Jay9UqcYMNwu7xA9GDYUX 125riCXE2MtxHbNZkRtExPGAfbv7LsY3Wa	0.00051253 0.51313192	0.51364445
3	9/20/15 18:08	9032592a133bddd3270b449a3b6a90698accb7836f03be6e35224352b1fab58e	125riCXE2MtxHbNZkRtExPGAfbv7LsY3Wa	125riCXE2MtxHbNZkRtExPGAfbv7LsY3Wa 18EdCZ7netnin52Mug6UjtZGSZUgdXUXu5	0.51374445 4.068e-05	0.51378513
4	9/20/15 16:35	f00febdc80e67c72d9c4d50ae2aa43eec2684725b566ec2a9fa9e8dbfc449827	125riCXE2MtxHbNZkRtExPGAfbv7LsY3Wa	12ytXWtNpxaEYW6ZvM564hVnsiFn4QnhAT 125riCXE2MtxHbNZkRtExPGAfbv7LsY3Wa	0.001 0.51388513	0.51488513
5	9/20/15 15:17	e3d4ac28233722bf1094f90a86f4eee2c19c8baa8a62dccc93c4b70197016884	125riCXE2MtxHbNZkRtExPGAfbv7LsY3Wa	125riCXE2MtxHbNZkRtExPGAfbv7LsY3Wa 3FdYMAYiFn9Ns2vGBBmRrfRXSk2VWyXoJA	0.51498513 0.00019896	0.51518409
6	9/20/15 13:07	876fe602c635936509a13e61dceacf522242b5bc02b5df0068497d9824d33dbb	125riCXE2MtxHbNZkRtExPGAfbv7LsY3Wa	125riCXE2MtxHbNZkRtExPGAfbv7LsY3Wa 1Gqt16gd2amyPL2pxMzqmTytCDxh63x8sR	0.51528409 1.434e-05	0.51529843

Chapter 5


Custodians
id [INTEGER]
name [TEXT]
0..N
{0,1}
Files
id [INTEGER]
custodian [INTEGER]
file_name [TEXT]
file_path [TEXT]
extension [TEXT]
file_size [TEXT]
mtime [TEXT]
ctime [TEXT]
atime [TEXT]
mode [INTEGER]
inode [INTEGER]


Legend
Regular function
Trunk function (nothing calls this)
Leaf function (this calls nothing else)
Function call which returns no value
Function call returns some value
/Users/Preston/learn-python-for-forensics/Chapters/Chapter5/Code/file_lister
file_lister.(/Users/Preston/learn-python-for-forensics/Chapters/Chapter5/Code/file_lister module frame (runs on import))
file_lister.main
file_lister.initDB
file_lister.ingestDirectory
file_lister.getOrAddCustodian
file_lister.writeOutput
file_lister.formatTimestamp
file_lister.getCustodian
file_lister.writeCSV
file_lister.writeHTML

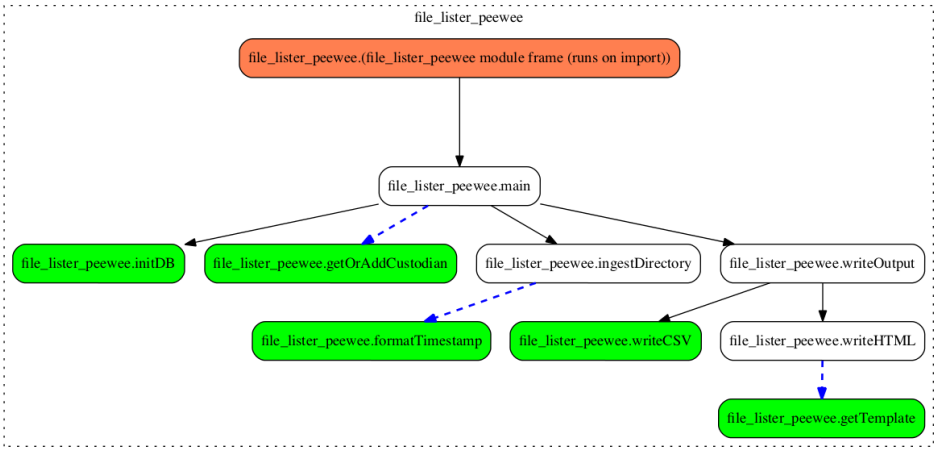
Legend	
Regular function	
Trunk function (nothing calls this)	
Leaf function (this calls nothing else)	
Function call which returns no value	→
Function call returns some value	⇢

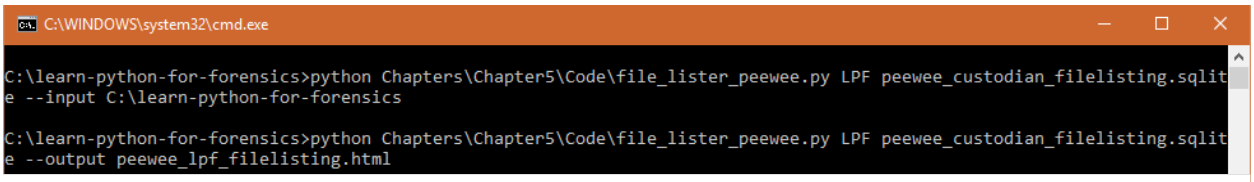



```
C:\WINDOWS\system32\cmd.exe

C:\learn-python-for-forensics>python Chapters\Chapter5\Code\file_lister.py LPF custodian_filelisting.sqlite --input C:\l
earn-python-for-forensics

C:\learn-python-for-forensics>python Chapters\Chapter5\Code\file_lister.py LPF custodian_filelisting.sqlite --output lpf
_filelisting.csv
```

	A	B	C	D	E	F	G	H	I	J	K
1	id	custodian	file_name	file_path	extension	file_size	mtime	ctime	atime	mode	inode
2	1	1	.gitignore	C:\\learn-python-for-forensics\\.gitignore		57	4/3/2016 18:16	4/3/2016 18:16	4/3/2016 18:16	100666	0
3	2	1	custodian_filelisting.sqlite	C:\\learn-python-for-forensics\\custodian_filelisting.sqlite	.sqlite	3072	4/4/2016 21:58	4/4/2016 21:58	4/4/2016 21:58	100666	0
4	3	1	custodian_filelisting.sqlite-journal	C:\\learn-python-for-forensics\\custodian_filelisting.sqlite-journal	.sqlite-journal	2576	4/4/2016 21:58	4/4/2016 21:58	4/4/2016 21:58	100666	0
5	4	1	file_lister.log	C:\\learn-python-for-forensics\\file_lister.log	.log	680	4/4/2016 21:58	4/4/2016 21:58	4/4/2016 21:58	100666	0
6	5	1	ISSUE_TEMPLATE.md	C:\\learn-python-for-forensics\\ISSUE_TEMPLATE.md	.md	1257	4/3/2016 18:16	4/3/2016 18:16	4/3/2016 18:16	100666	0
7	6	1	line_numbers.py	C:\\learn-python-for-forensics\\line_numbers.py	.py	420	4/3/2016 18:16	4/3/2016 18:16	4/3/2016 18:16	100666	0
8	7	1	NTUSER.DAT	C:\\learn-python-for-forensics\\NTUSER.DAT	.DAT	1310720	4/3/2016 18:16	4/4/2016 0:06	4/4/2016 0:06	100666	0
9	8	1	ntuser_userassist.xlsx	C:\\learn-python-for-forensics\\ntuser_userassist.xlsx	.xlsx	14802	4/4/2016 0:07	4/4/2016 0:07	4/4/2016 0:07	100666	0
10	9	1	README.md	C:\\learn-python-for-forensics\\README.md	.md	55	4/3/2016 18:16	4/3/2016 18:16	4/3/2016 18:16	100666	0
11	10	1	reference.docx	C:\\learn-python-for-forensics\\reference.docx	.docx	40149	4/3/2016 18:16	4/3/2016 18:16	4/3/2016 18:16	100666	0
12	11	1	rot13.py	C:\\learn-python-for-forensics\\rot13.py	.py	1468	4/3/2016 18:16	4/4/2016 0:01	4/4/2016 0:01	100666	0

Legend	
Regular function	
Trunk function (nothing calls this)	
Leaf function (this calls nothing else)	
Function call which returns no value	→
Function call returns some value	⇢

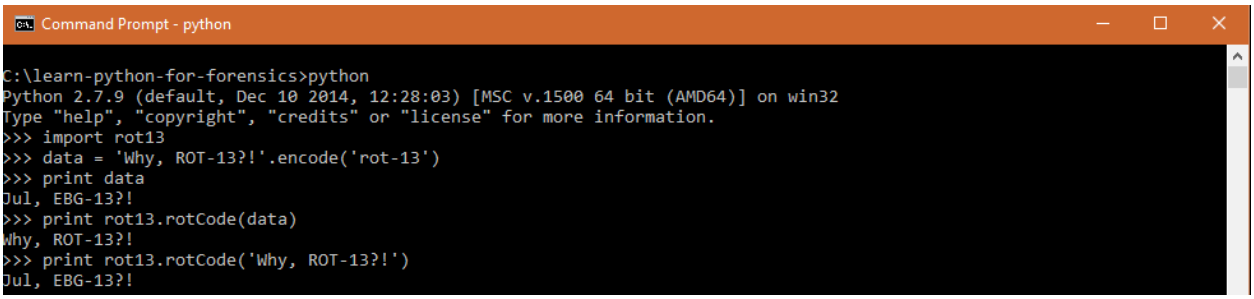


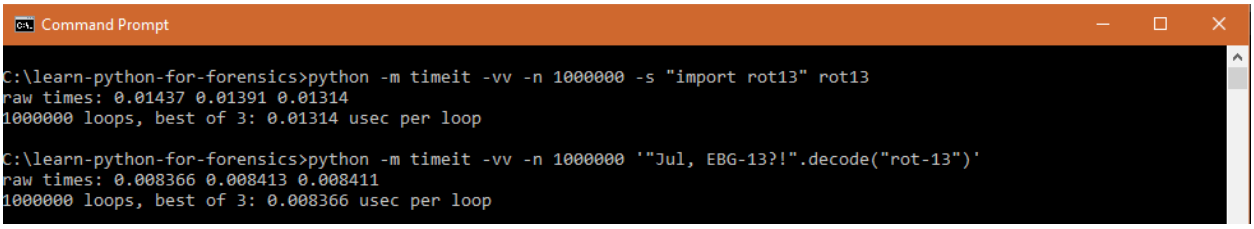


File Listing for Custodian 1, LPF

Id	Custodian	File Name	File Path	File Extension	File Size	Created Time	Modified Time	Accessed Time	Mode	Inode
1	LPF	.gitignore	C:\learn-python-for-forensics\.gitignore		57	2016-04-03 18:16:25.942755	2016-04-03 18:16:25.943245	2016-04-03 18:16:25.942755	100666	0
2	LPF	custodian_filelisting.sqlite	C:\learn-python-for-forensics\custodian_filelisting.sqlite	.sqlite	96256	2016-04-04 21:58:47.664950	2016-04-04 21:58:48.074615	2016-04-04 21:58:47.664950	100666	0
3	LPF	file_lister.log	C:\learn-python-for-forensics\file_lister.log	.log	3505	2016-04-04 21:58:47.663949	2016-04-04 21:59:11.339528	2016-04-04 21:58:47.663949	100666	0
4	LPF	ISSUE_TEMPLATE.md	C:\learn-python-for-forensics\ISSUE_TEMPLATE.md	.md	1257	2016-04-03 18:16:27.040920	2016-04-03 18:16:27.041411	2016-04-03 18:16:27.040920	100666	0
5	LPF	line_numbers.py	C:\learn-python-for-forensics\line_numbers.py	.py	420	2016-04-03 18:16:27.045424	2016-04-03 18:16:27.045916	2016-04-03 18:16:27.045424	100666	0

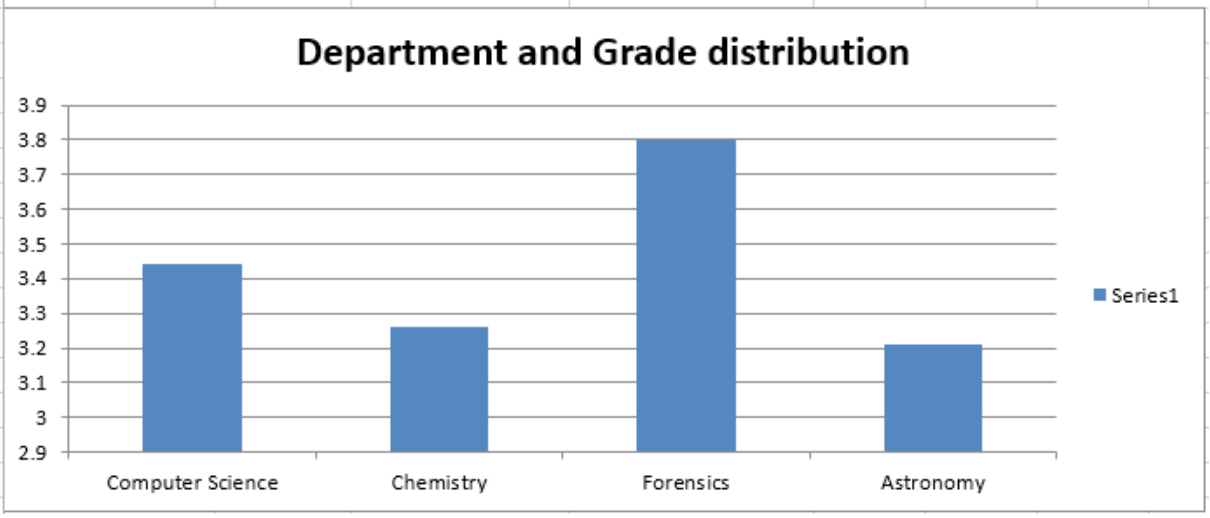
Chapter 6



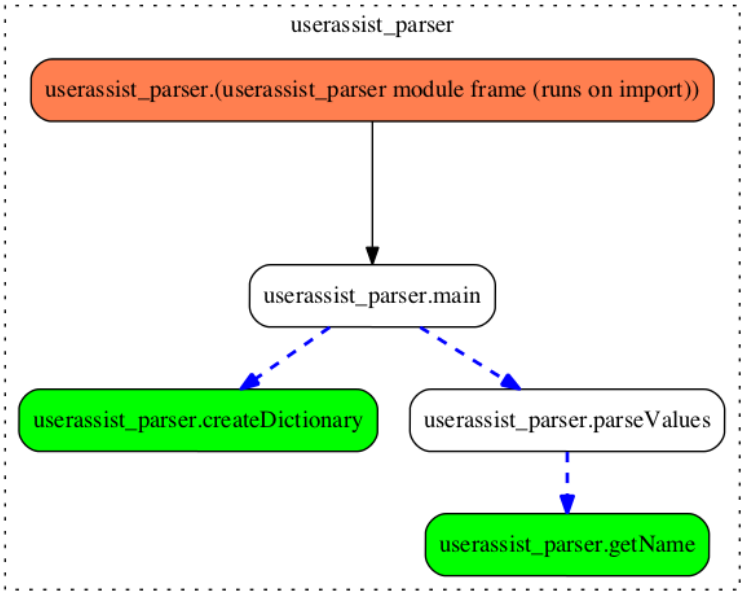


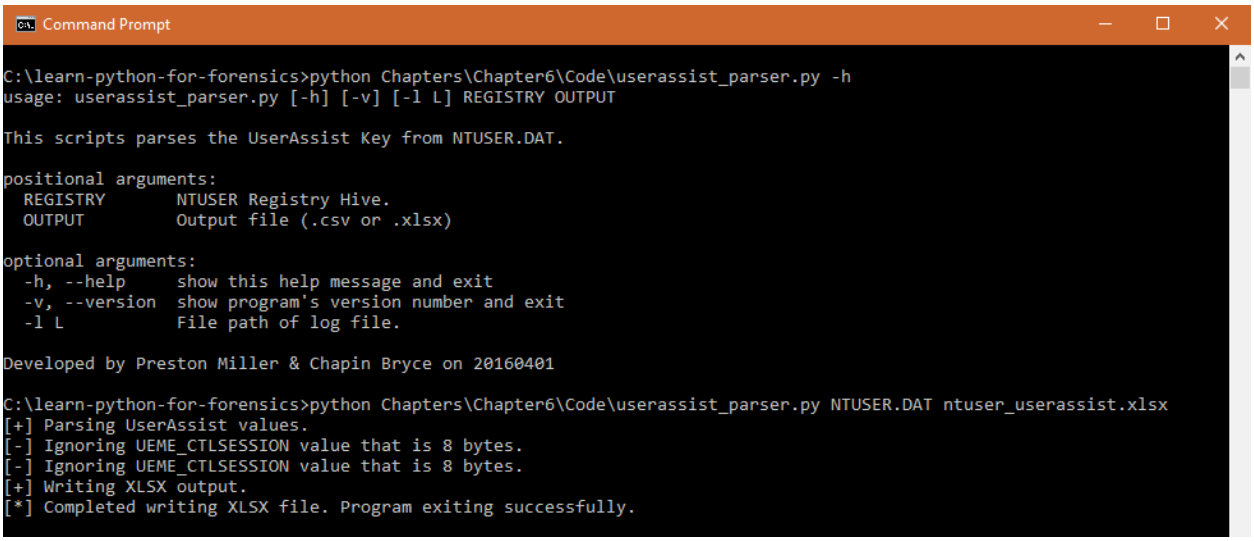
	A	B	C	D
1	Department	Students	Cumulative GPA	Final Date
2	Computer Science	235	3.44	07/23/15 06:00:00 PM
3	Chemistry	201	3.26	07/25/15 09:30:00 AM
4	Forensics	99	3.8	07/23/15 09:30:00 AM
5	Astronomy	115	3.21	07/19/15 03:30:00 PM

Department	Students	Cumulative GPA	Final Date
Computer Science	235	3.44	07/23/15 06:00:00 PM
Chemistry	201	3.26	07/25/15 09:30:00 AM
Forensics	99	3.8	07/23/15 09:30:00 AM
Astronomy	115	3.21	07/19/15 03:30:00 PM



Legend	
Regular function	
Trunk function (nothing calls this)	
Leaf function (this calls nothing else)	
Function call which returns no value	→
Function call returns some value	⇢

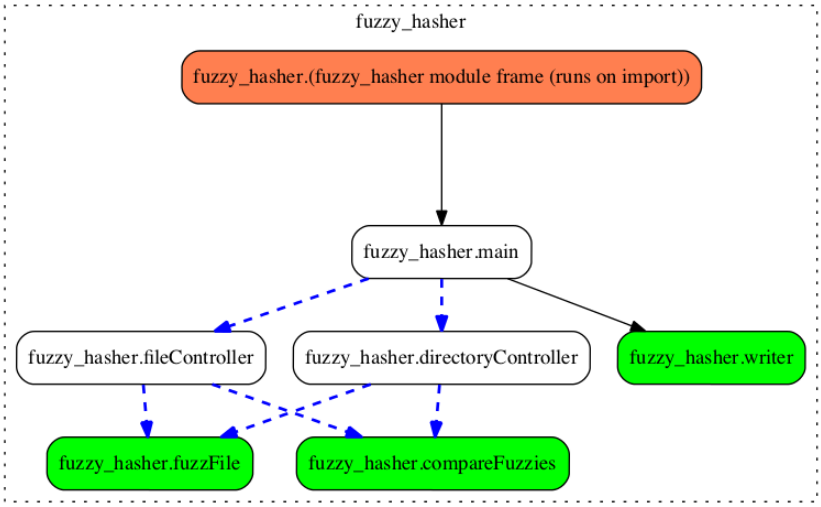


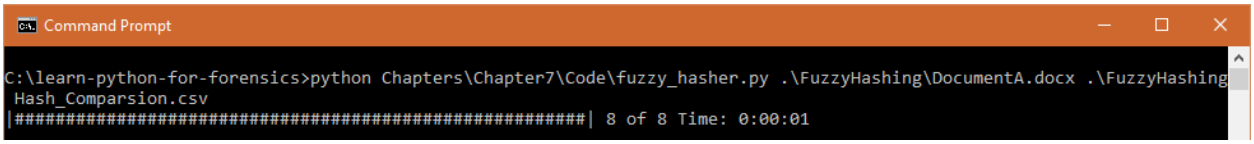

Command Prompt
C:\learn-python-for-forensics>python Chapters\Chapter6\Code\userassist_parser.py -h
usage: userassist_parser.py [-h] [-v] [-l L] REGISTRY OUTPUT
This scripts parses the UserAssist Key from NTUSER.DAT.
positional arguments:
REGISTRY NTUSER Registry Hive.
OUTPUT Output file (.csv or .xlsx)
optional arguments:
-h, --help show this help message and exit
-v, --version show program's version number and exit
-l L File path of log file.
Developed by Preston Miller & Chapin Bryce on 20160401
C:\learn-python-for-forensics>python Chapters\Chapter6\Code\userassist_parser.py NTUSER.DAT ntuser_userassist.xlsx
[+] Parsing UserAssist values.
[-] Ignoring UEME_CTLSESSION value that is 8 bytes.
[-] Ignoring UEME_CTLSESSION value that is 8 bytes.
[+] Writing XLSX output.
[*] Completed writing XLSX file. Program exiting successfully.

Chapter 7

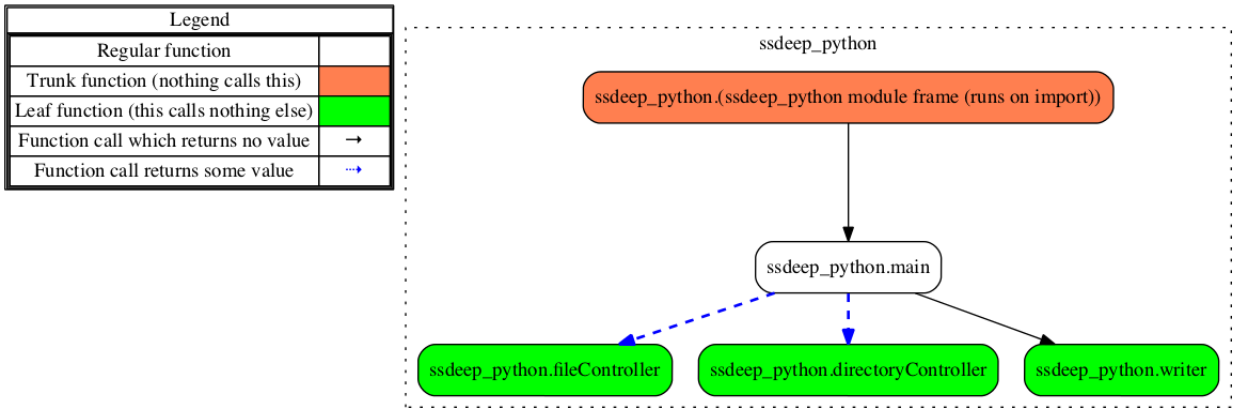
Name	Date modified	Type	Size
DocumentA	12/11/2015 10:19 ...	Microsoft Word D...	40 KB
DocumentB	12/11/2015 10:19 ...	Microsoft Word D...	40 KB
DocumentC	12/11/2015 10:20 ...	Microsoft Word D...	45 KB
Email Header Demo	1/20/2014 6:36 PM	Microsoft Word D...	15 KB
FTK Imager Overview	1/30/2014 12:15 AM	Microsoft PowerP...	1,812 KB
Internet Lab Practical	9/13/2014 5:27 PM	Microsoft Word D...	16 KB
Notes	9/14/2014 12:31 PM	Text Document	2 KB
Notes_Feb2	2/2/2015 1:24 PM	PDF File	162 KB

Legend	
Regular function	
Trunk function (nothing calls this)	
Leaf function (this calls nothing else)	
Function call which returns no value	→
Function call returns some value	⇢





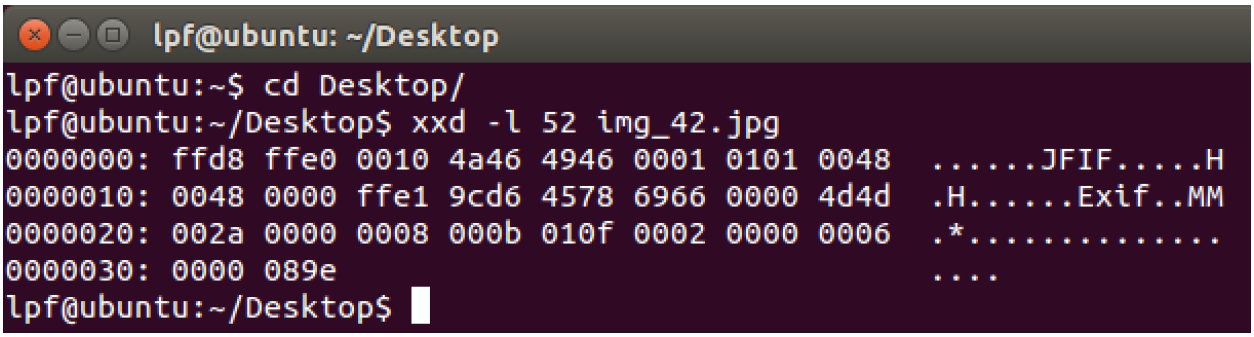
	A	B	C	D	E
1	file path	similarity	matching segments	known file total segments	comparison total segments
2	rand1A.file	100	1046028	1046028	1046028
3	rand1B.file	99.9935948	1045961	1046028	1046026
4	rand2.file	0.47857228	5006	1046028	1046060

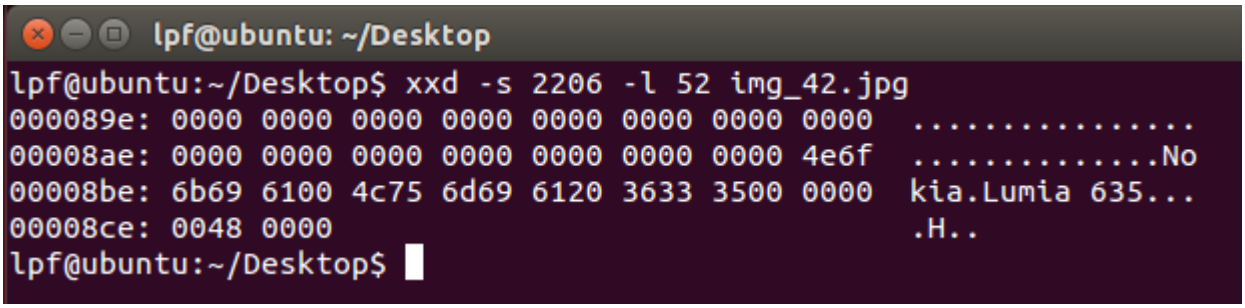


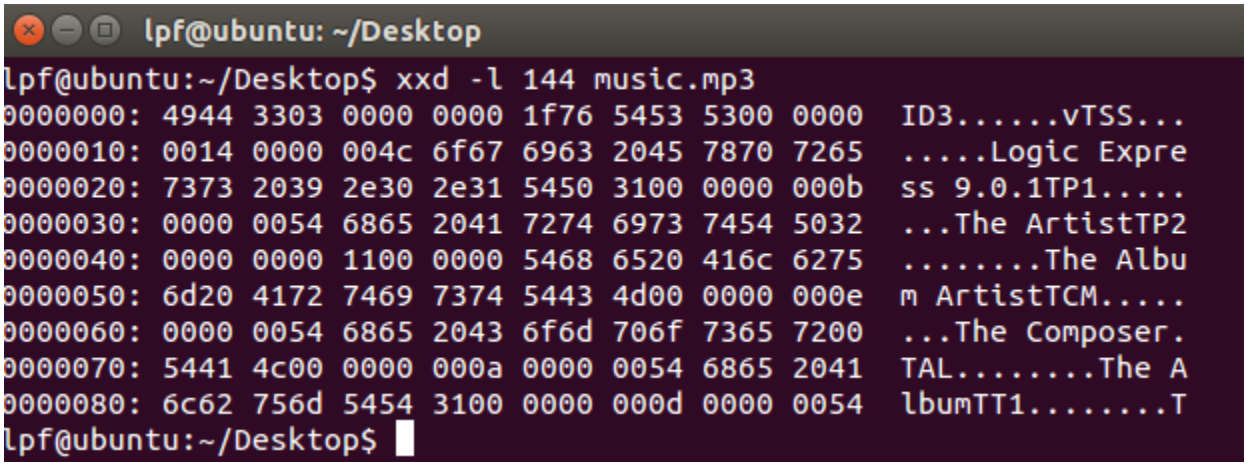

```
pmiller@ubuntu: ~/learn-python-for-forensics/Chapters/Chapter7/Code
pmiller@ubuntu:~/learn-python-for-forensics/Chapters/Chapter7/Code$ python ssdee
p_python.py DocumentA.docx ~/FuzzyHashing/ ~/Desktop/ssdeep_output.csv
|############################################################| 8 of 8 Time: 0:00:00
pmiller@ubuntu:~/learn-python-for-forensics/Chapters/Chapter7/Code$
```

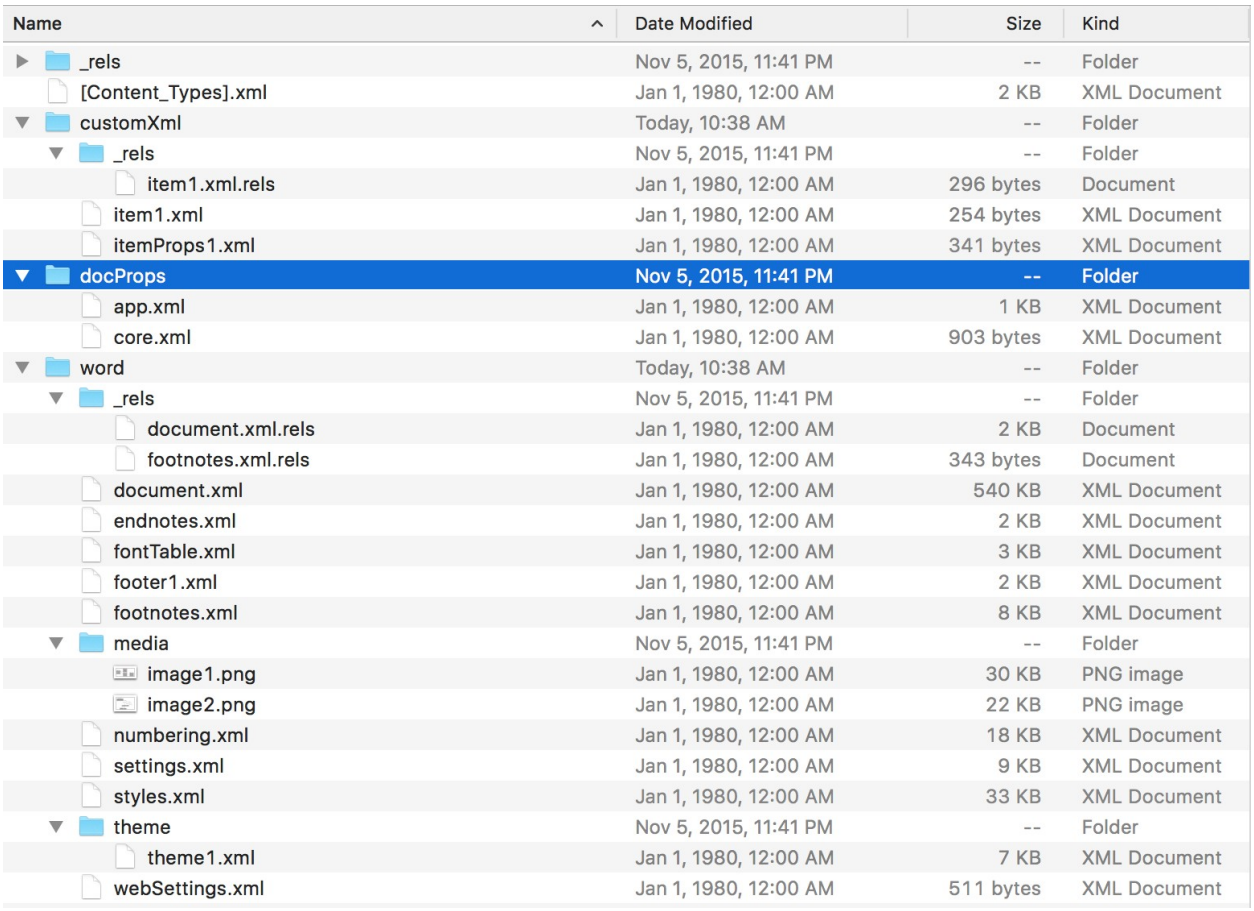
file_path	similarity
rand1A.file	100
rand1B.file	94
rand2.file	0

Chapter 8


lpf@ubuntu: ~/Desktop
lpf@ubuntu:~$ cd Desktop/
lpf@ubuntu:~/Desktop$ xxd -l 52 img_42.jpg
0000000: ffd8 ffe0 0010 4a46 4946 0001 0101 0048 ......JFIF.....H
0000010: 0048 0000 ffe1 9cd6 4578 6966 0000 4d4d .H......Exif..MM
0000020: 002a 0000 0008 000b 010f 0002 0000 0006 .*..............
0000030: 0000 089e   ....
lpf@ubuntu:~/Desktop$


lpf@ubuntu: ~/Desktop
lpf@ubuntu:~/Desktop$ xxd -s 2206 -l 52 img_42.jpg
000089e: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00008ae: 0000 0000 0000 0000 0000 0000 0000 4e6f ....No
00008be: 6b69 6100 4c75 6d69 6120 3633 3500 0000 kia.Lumia 635...
00008ce: 0048 0000   .H..
lpf@ubuntu:~/Desktop$

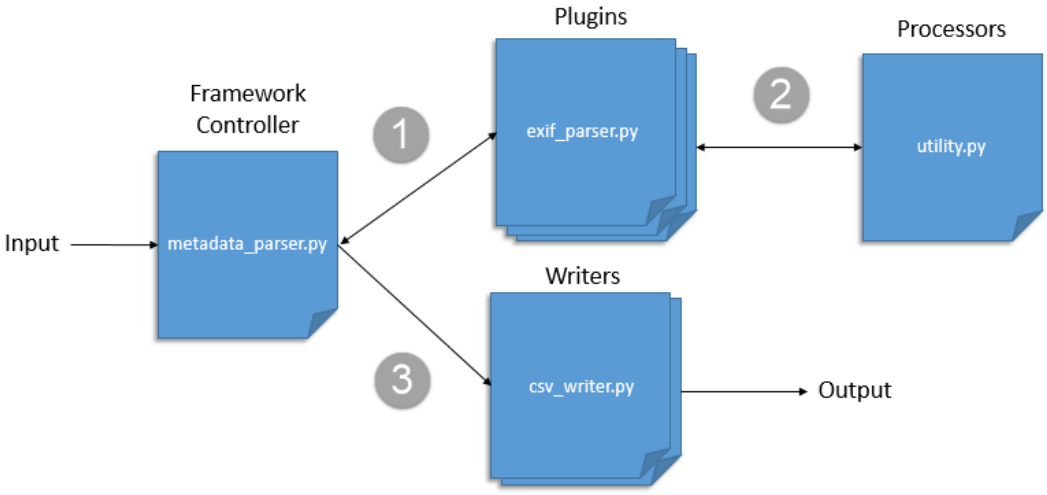

lpf@ubuntu: ~/Desktop
lpf@ubuntu:~/Desktop$ xxd -l 144 music.mp3
0000000: 4944 3303 0000 0000 1f76 5453 5300 0000 ID3......vTSS...
0000010: 0014 0000 004c 6f67 6963 2045 7870 7265 .....Logic Expre
0000020: 7373 2039 2e30 2e31 5450 3100 0000 000b ss 9.0.1TP1.....
0000030: 0000 0054 6865 2041 7274 6973 7454 5032 ...The ArtistTP2
0000040: 0000 0000 1100 0000 5468 6520 416c 6275 ....The Albu
0000050: 6d20 4172 7469 7374 5443 4d00 0000 000e m ArtistTCM.....
0000060: 0000 0054 6865 2043 6f6d 706f 7365 7200 ...The Composer.
0000070: 5441 4c00 0000 000a 0000 0054 6865 2041 TAL........The A
0000080: 6c62 756d 5454 3100 0000 000d 0000 0054 lbumTT1........T
lpf@ubuntu:~/Desktop$



core.xml

core.xml 〉 <cp:contentStatus>

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<cp:coreProperties xmlns:cp="http://schemas.openxmlformats.org/package/2006/metadata/core-properties" xmlns:dc=
    "http://purl.org/dc/elements/1.1/" xmlns:dcterms="http://purl.org/dc/terms/" xmlns:dcmitype="http://purl.org/
    dc/dcmitype/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><dc:title>Metadata Title</dc:title><dc:
    subject>Digital Forensics</dc:subject><dc:creator>Preston Miller</dc:creator><cp:keywords>Embedded Metadata,
    EXIF, ID3, Office documents, XML</cp:keywords><dc:description>Embedded metadata stores a great deal of
    information about forensically relevant files!</dc:description><cp:lastModifiedBy>Preston Miller</cp:
    lastModifiedBy><cp:revision>4</cp:revision><dcterms:created xsi:type="dcterms:W3CDTF">2015-11-06T03:15:00Z</
    dcterms:created><dcterms:modified xsi:type="dcterms:W3CDTF">2015-11-06T04:36:00Z</
    dcterms:modified><cp:category>Book Category</cp:category><cp:contentStatus>Complete</cp:contentStatus></cp:
    coreProperties>
```



DMS GPS Coordinates

Python Format: Degree Minute Second ((40, 1), (40, 1), (58475, 1000))

Simplified Format: 40, 40, 58.475

DMS to Degree Conversion

Formula:

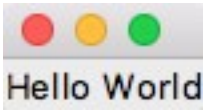
$$Degree + \frac{Minute}{60} + \frac{Second}{3600} \quad \text{(Degree > 0)}$$

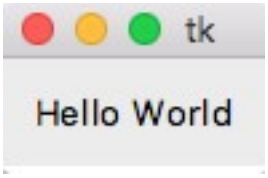
$$Degree - \frac{Minute}{60} - \frac{Second}{3600} \quad \text{(Degree < 0)}$$

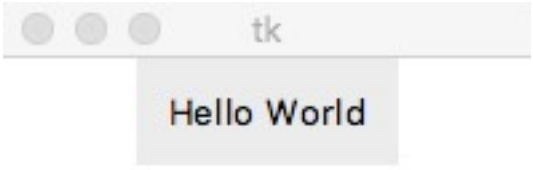
Example:

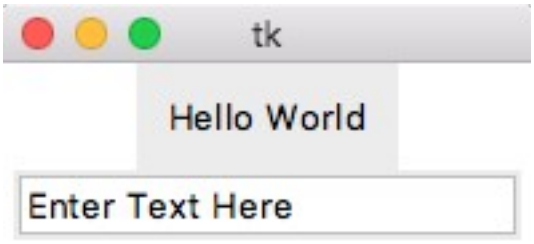
$$40 + \frac{40}{60} + \frac{58.475}{3600} = \boxed{40.68291}$$

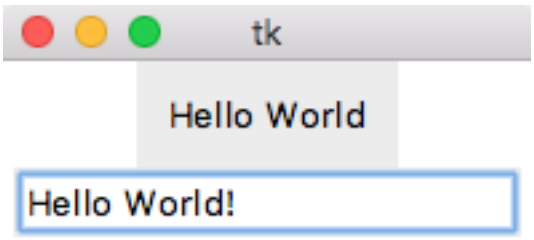
Chapter 9



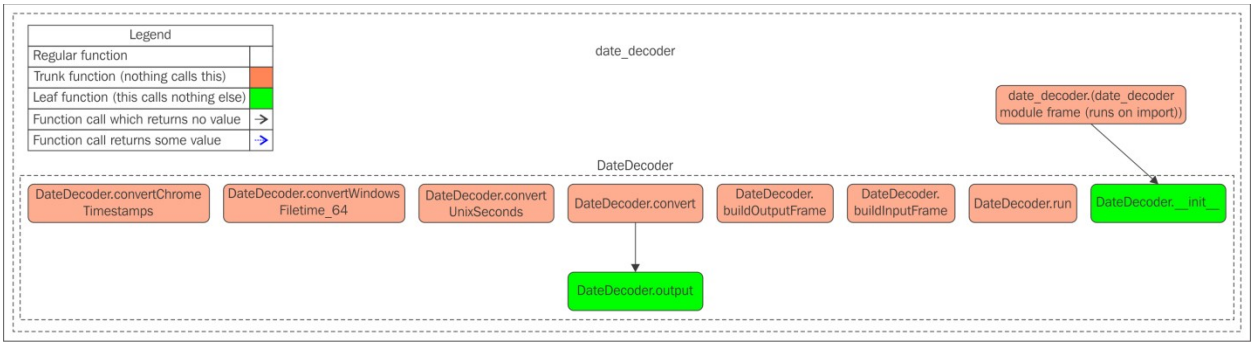


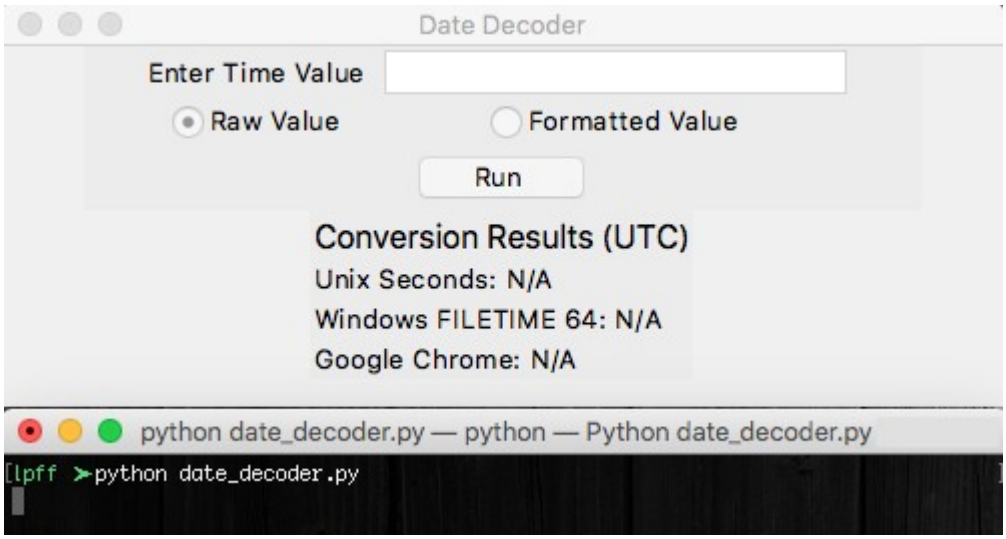


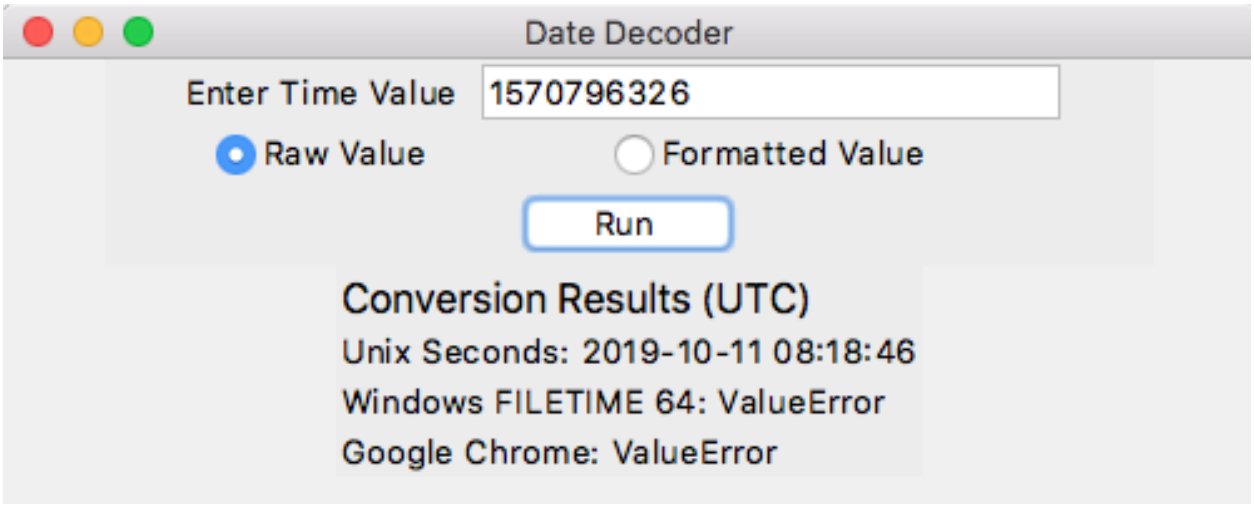

tk
Hello World
Enter Text Here

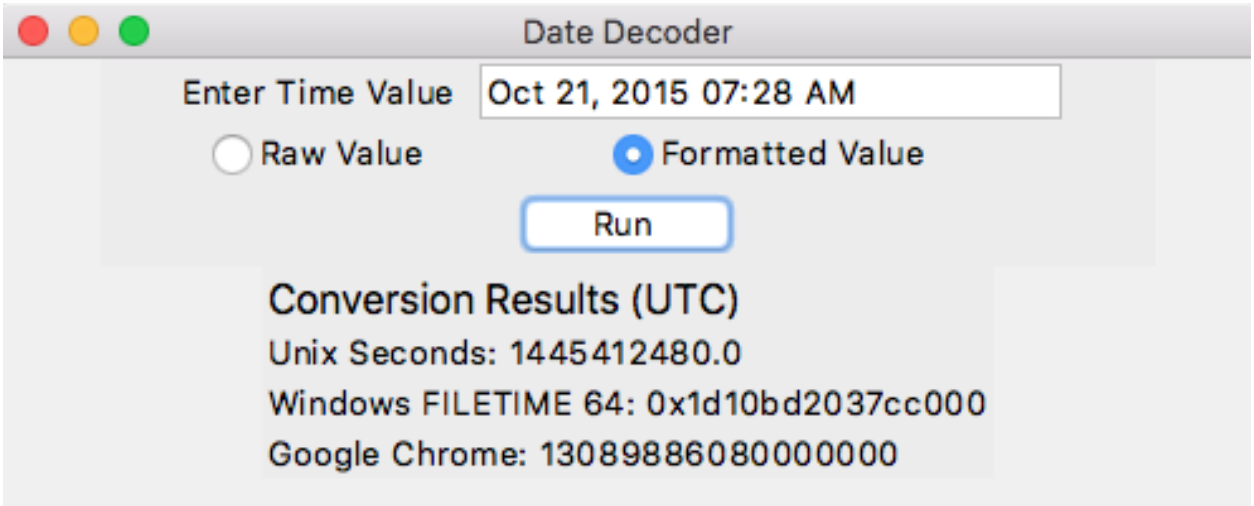

tk
Hello World
Hello World!


tk
Hello World
Enter Text Here
Go

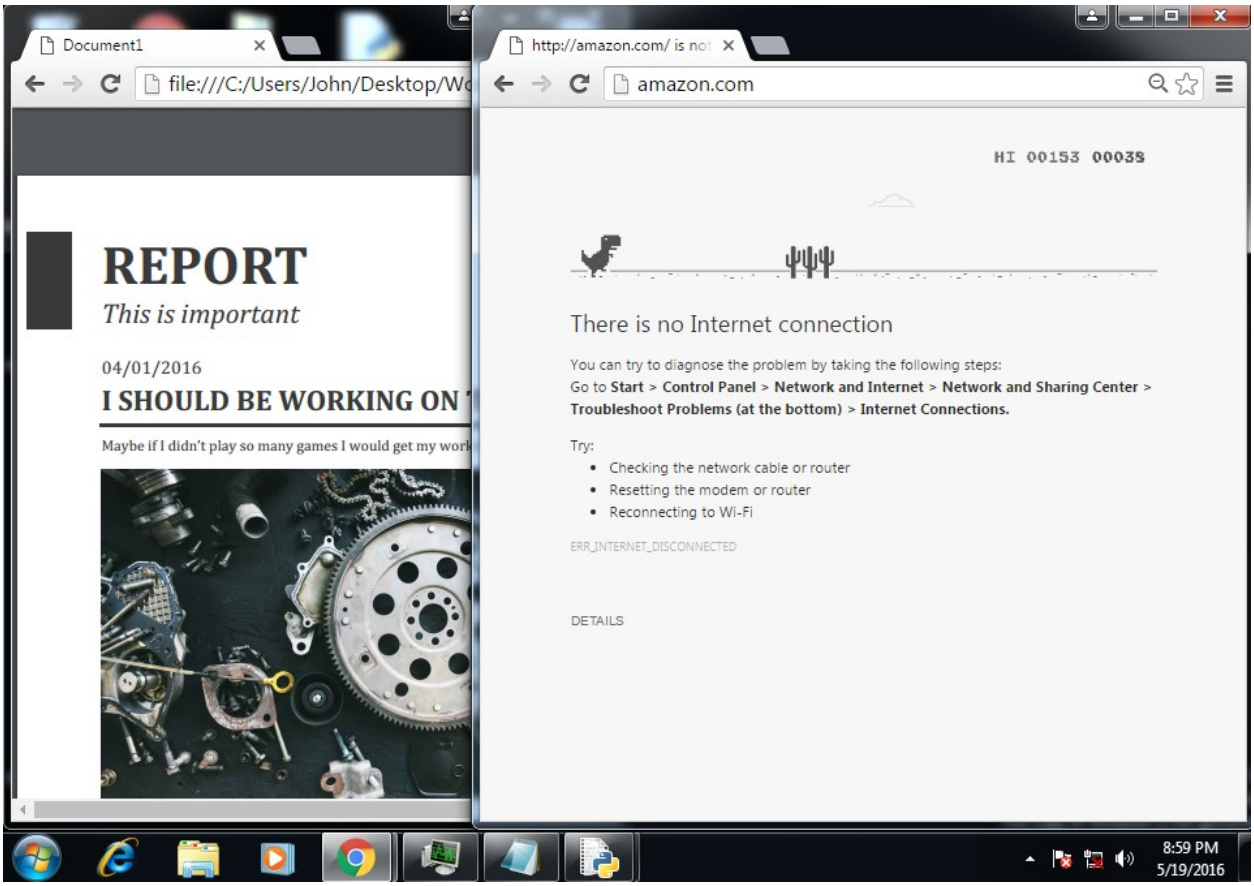

Legend
Regular function
Trunk function (nothing calls this)
Leaf function (this calls nothing else)
Function call which returns no value
Function call returns some value
date_decoder
date_decoder.(date_decoder module frame (runs on import))
DateDecoder
DateDecoder.convertChrome Timestamps
DateDecoder.convertWindows Filetime_64
DateDecoder.convert UnixSeconds
DateDecoder.convert
DateDecoder. buildOutputFrame
DateDecoder. buildInputFrame
DateDecoder.run
DateDecoder.__init__
DateDecoder.output


Date Decoder
Enter Time Value
Raw Value
Formatted Value
Run
Conversion Results (UTC)
Unix Seconds: N/A
Windows FILETIME 64: N/A
Google Chrome: N/A
python date_decoder.py — python — Python date_decoder.py
[lpff ➤python date_decoder.py


Date Decoder
Enter Time Value
1570796326
Raw Value
Formatted Value
Run
Conversion Results (UTC)
Unix Seconds: 2019-10-11 08:18:46
Windows FILETIME 64: ValueError
Google Chrome: ValueError


Date Decoder
Enter Time Value
Oct 21, 2015 07:28 AM
Raw Value
Formatted Value
Run
Conversion Results (UTC)
Unix Seconds: 1445412480.0
Windows FILETIME 64: 0x1d10bd2037cc000
Google Chrome: 13089886080000000

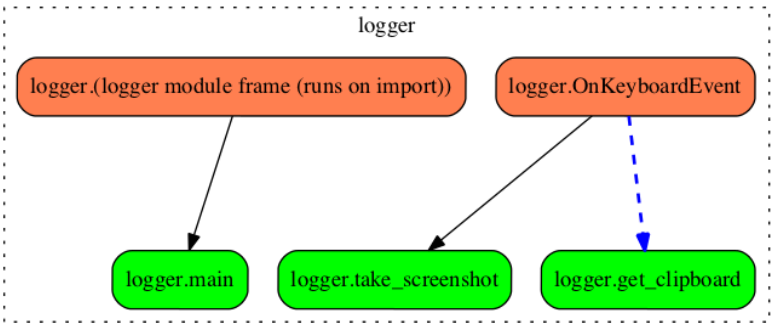
Chapter 10


Document1
file:///C:/Users/John/Desktop/Wo
REPORT
This is important
04/01/2016
I SHOULD BE WORKING ON
Maybe if I didn't play so many games I would get my work
http://amazon.com/ is not
amazon.com
HI 00153 00038
There is no Internet connection
You can try to diagnose the problem by taking the following steps:
Go to Start > Control Panel > Network and Internet > Network and Sharing Center > Troubleshoot Problems (at the bottom) > Internet Connections.
Try:
Checking the network cable or router
Resetting the modem or router
Reconnecting to Wi-Fi
ERR_INTERNET_DISCONNECTED
DETAILS
8:59 PM
5/19/2016

C:\Windows\system32\cmd.exe - python

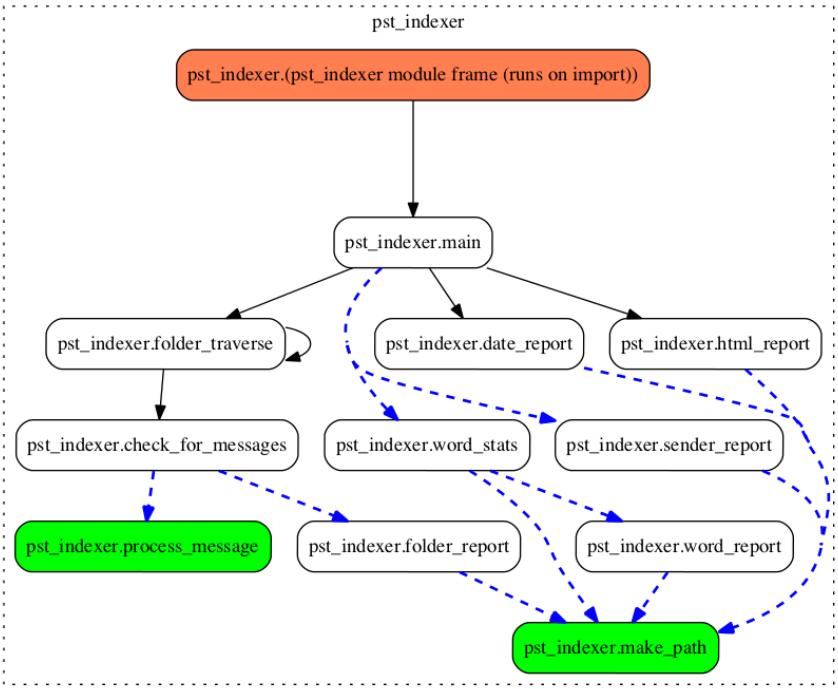
```
>>> import wmi
>>> c = wmi.WMI()
>>> process_watcher = c.Win32_Process.watch_for("creation")
>>> while True:
...     print process_watcher()
...

instance of Win32_Process
{
        Caption = "calc.exe";
        CommandLine = "\"C:\\Windows\\system32\\calc.exe\" ";
        CreationClassName = "Win32_Process";
        CreationDate = "20160519230520.795611-240";
        CSCreationClassName = "Win32_ComputerSystem";
        CSName = "HOME";
        Description = "calc.exe";
        ExecutablePath = "C:\\Windows\\system32\\calc.exe";
        Handle = "3460";
        HandleCount = 53;
        KernelModeTime = "0";
        MaximumWorkingSetSize = 1380;
        MinimumWorkingSetSize = 200;
        Name = "calc.exe";
        OSCreationClassName = "Win32_OperatingSystem";
        OSName = "Microsoft Windows 7 Ultimate |C:\\Windows|\\Device\\Harddisk0\
\Partition2";
        OtherOperationCount = "60";
        OtherTransferCount = "56";
        PageFaults = 1880;
        PageFileUsage = 4336;
        ParentProcessId = 1396;
        PeakPageFileUsage = 4336;
        PeakVirtualSize = "66723840";
        PeakWorkingSetSize = 7464;
        Priority = 8;
        PrivatePageCount = "4440064";
        ProcessId = 3460;
        QuotaNonPagedPoolUsage = 5;
        QuotaPagedPoolUsage = 123;
        QuotaPeakNonPagedPoolUsage = 5;
        QuotaPeakPagedPoolUsage = 123;
        ReadOperationCount = "1";
        ReadTransferCount = "60";
        SessionId = 1;
        ThreadCount = 2;
        UserModeTime = "0";
        VirtualSize = "66723840";
        WindowsVersion = "6.1.7601";
        WorkingSetSize = "7643136";
        WriteOperationCount = "0";
        WriteTransferCount = "0";
};
```

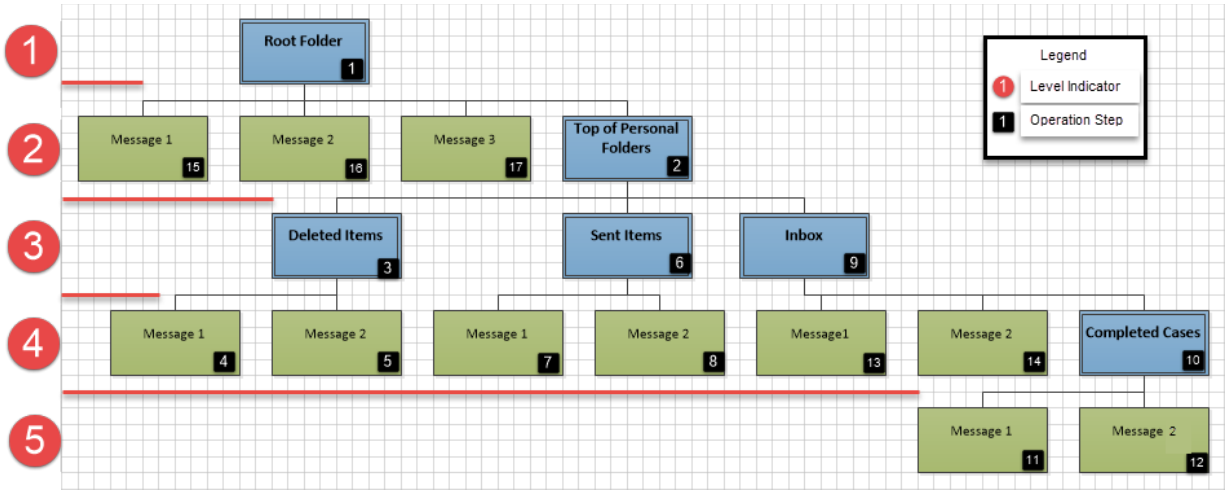
Legend	
Regular function	
Trunk function (nothing calls this)	
Leaf function (this calls nothing else)	
Function call which returns no value	→
Function call returns some value	⇢



Chapter 11

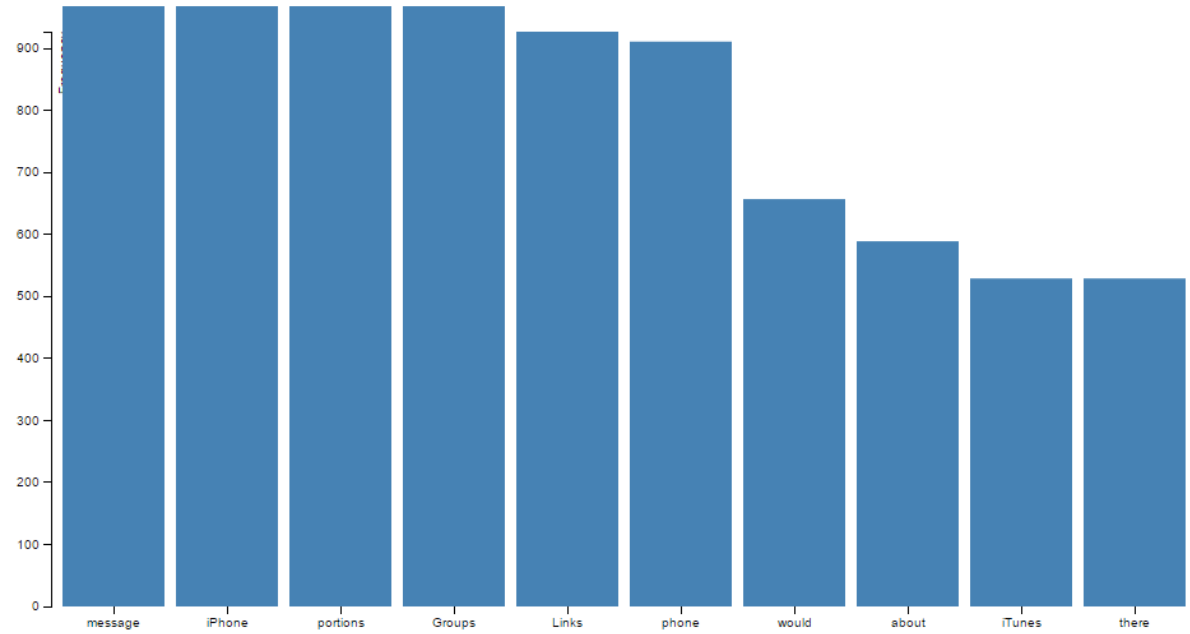
Legend	
Regular function	
Trunk function (nothing calls this)	
Leaf function (this calls nothing else)	
Function call which returns no value	→
Function call returns some value	⇢



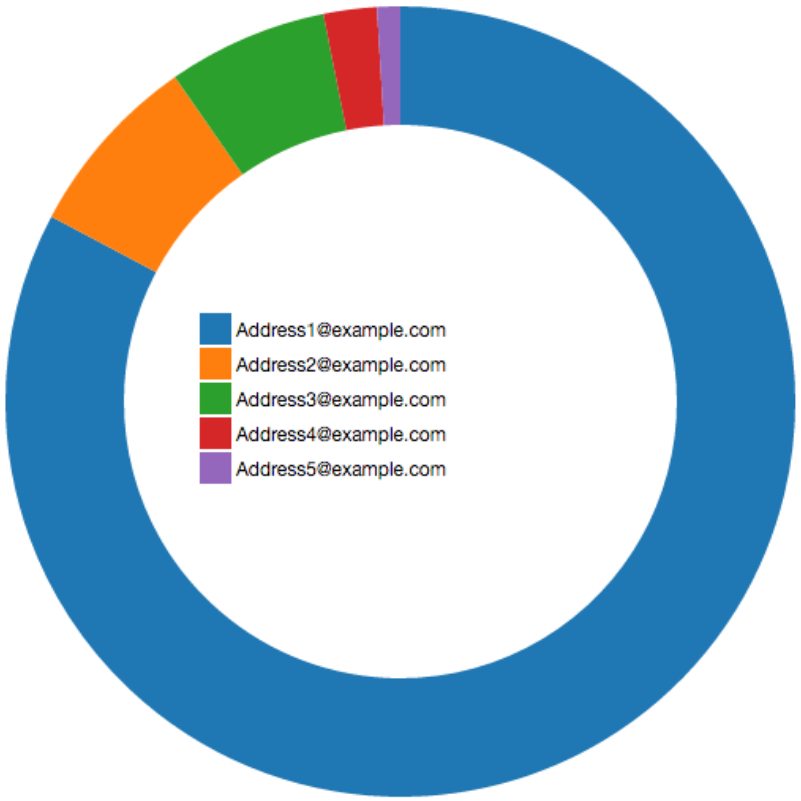


PST Report

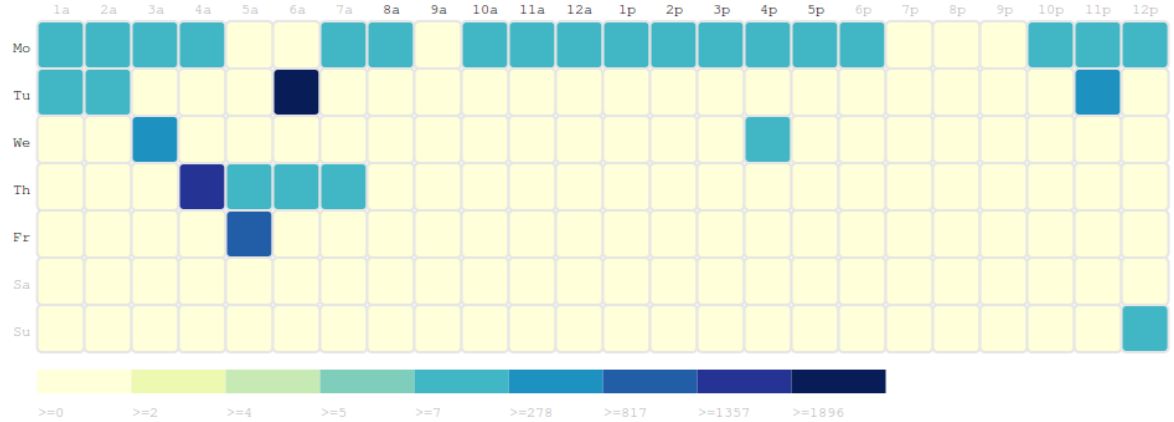
Top 10 words in Example.pst



Top 5 Senders in Example.pst



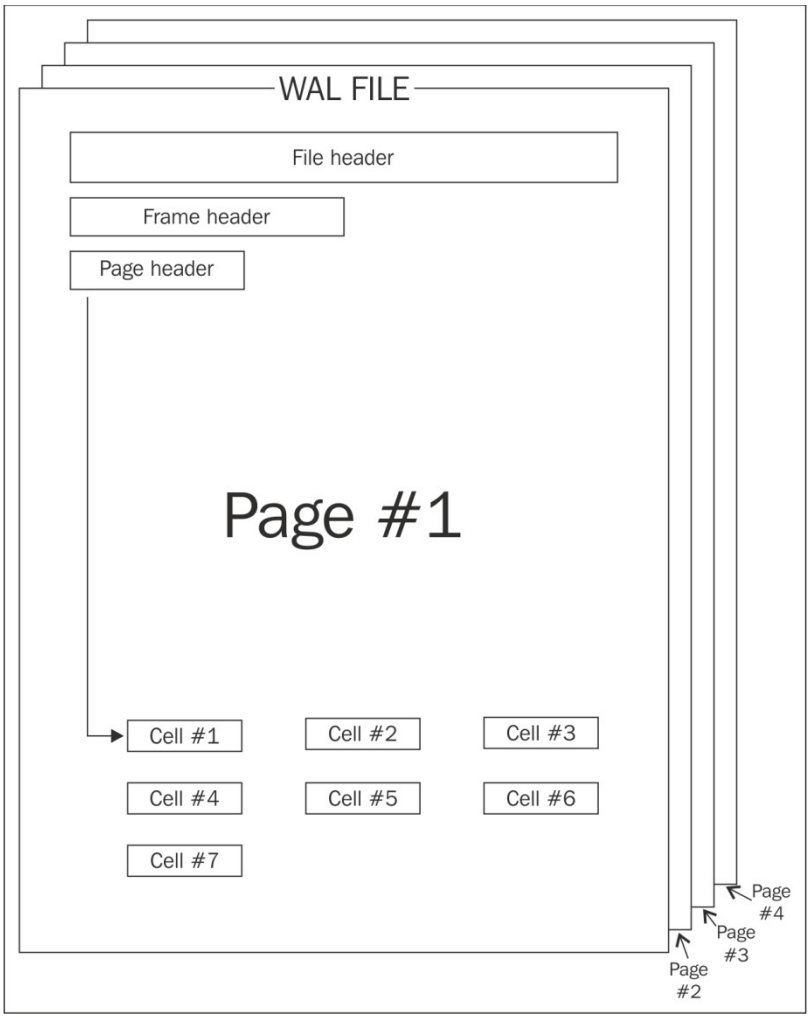
Heatmap of all date activity in Example.pst




```
lpff@ubuntu $ python pst_indexer.py example.pst example_output/ --title "Example Report"
lpff@ubuntu $ _
```

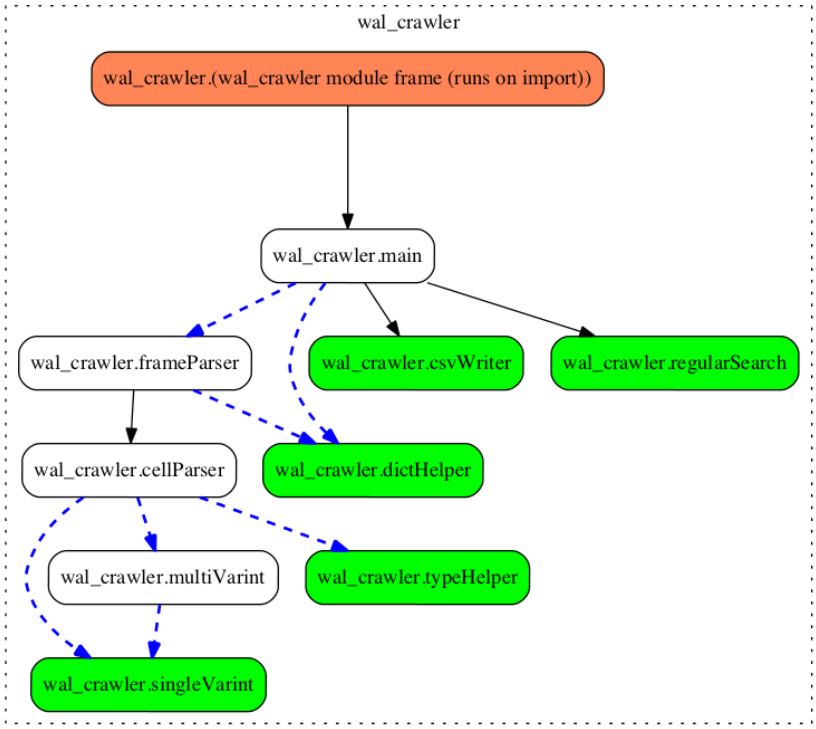
Chapter 12

Name	Date Modified	Size
Ch11.md	Today, 5:35 PM	3 KB
Code	Today, 3:21 PM	--
Images	Today, 1:14 PM	--
superuser.sqlite	Today, 5:36 PM	45 KB
superuser.sqlite-shm	Today, 5:37 PM	33 KB
superuser.sqlite-wal	Today, 5:37 PM	Zero bytes



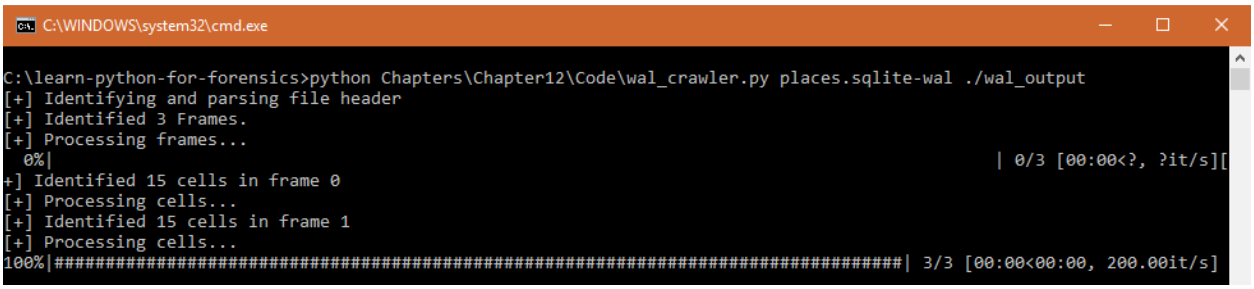
```
C:\WINDOWS\system32\cmd.exe - python
C:\learn-python-for-forensics>python
Python 2.7.9 (default, Dec 10 2014, 12:28:03) [MSC v.1500 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> from tqdm import tqdm
>>> from time import sleep
>>> for x in tqdm(range(100)):
...     sleep(1)
...
 84%|#################################################################           | 84/100 [01:24<00:16,  1.01s/it]
```

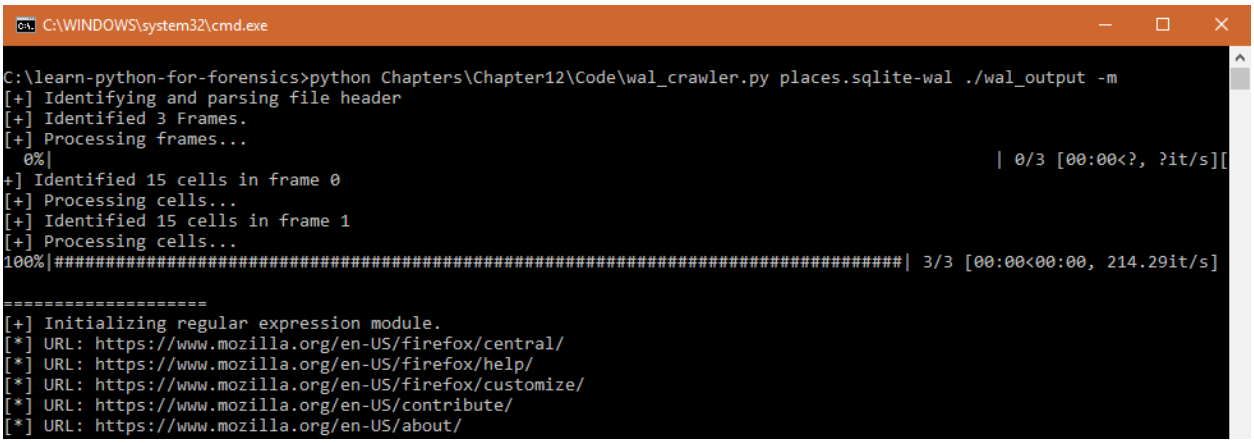
Legend	
Regular function	
Trunk function (nothing calls this)	
Leaf function (this calls nothing else)	
Function call which returns no value	→
Function call returns some value	⇢




```
C:\WINDOWS\system32\cmd.exe - python  Chapters\Chapter12\Code\wal_crawler.py places.sqlite-wal ./wal_output
C:\learn-python-for-forensics>python Chapters\Chapter12\Code\wal_crawler.py places.sqlite-wal ./wal_output
[+] Identifying and parsing file header
> c:\learn-python-for-forensics\chapters\chapter12\code\wal_crawler.py(166)dictHelper()
-> return keys._asdict(keys._make(struct.unpack(format, data)))
(Pdb)
```

A	B	C	D	E	F	G	H	I	J
Frame	Salt-1	Salt-2	Frame Offset	Cell	Cell Offset	ROWID	Data		
0	-977652151	1343711549	32	0	32293	3	NULL (RowId?)	https://www.mozilla.org/en-US/firefox/central/	NULL (RowId?)
0	-977652151	1343711549	32	1	32204	4	NULL (RowId?)	https://www.mozilla.org/en-US/firefox/help/	NULL (RowId?)
0	-977652151	1343711549	32	2	32110	5	NULL (RowId?)	https://www.mozilla.org/en-US/firefox/customize/	NULL (RowId?)
0	-977652151	1343711549	32	3	32023	6	NULL (RowId?)	https://www.mozilla.org/en-US/contribute/	NULL (RowId?)
0	-977652151	1343711549	32	4	31941	7	NULL (RowId?)	https://www.mozilla.org/en-US/about/	NULL (RowId?)
0	-977652151	1343711549	32	5	31887	8	NULL (RowId?)	place:sort=8&maxResults=10	NULL (RowId?)
0	-977652151	1343711549	32	6	31739	9	NULL (RowId?)	place:folder=BOOKMARKS_MENU&folder=UNFILED_BOOKMARKS&folder=TOOLBAR&queryType=1&sort=12&maxResults=10&excludeQueries=1	NULL (RowId?)
0	-977652151	1343711549	32	7	31677	10	NULL (RowId?)	place:type=6&sort=14&maxResults=10	NULL (RowId?)
0	-977652151	1343711549	32	8	32631	11	NULL (RowId?)	https://search.yahoo.com/yhs/search?p=anarchist+cookbook&ei=UTF-8&hspart=mozilla&hsimp=yhs-002	anarchist cookbook - - Yahoo Search Results
0	-977652151	1343711549	32	9	31395	12	NULL (RowId?)	http://r.search.yahoo.com/_ylt=A0LEVi8mfW9WcocAdMQnnIIQ;_ylu=X3oDMTByOHZyb21tBGNvbG8DYmYxBHBvcwMxBHZ0aWQDBHNlYwNzcg--/RV=2/RE=1450175910/RO=10/RU=http%3a%2f%2fwww.anarchistcookbook.com%2f/RK=0/RS=ZhsJ4ecMNDt20UAz0ei1XlFqkJQ-	NULL (RowId?)
0	-977652151	1343711549	32	10	32439	13	NULL (RowId?)	http://www.anarchistcookbook.com/	Anarchist Cookbook | Government is not the solution to our problem; government is the problem.


C:\WINDOWS\system32\cmd.exe
C:\learn-python-for-forensics>python Chapters\Chapter12\Code\wal_crawler.py places.sqlite-wal ./wal_output
[+] Identifying and parsing file header
[+] Identified 3 Frames.
[+] Processing frames...
0%| | 0/3 [00:00<?, ?it/s][
+] Identified 15 cells in frame 0
[+] Processing cells...
[+] Identified 15 cells in frame 1
[+] Processing cells...
100%|##########| 3/3 [00:00<00:00, 200.00it/s]

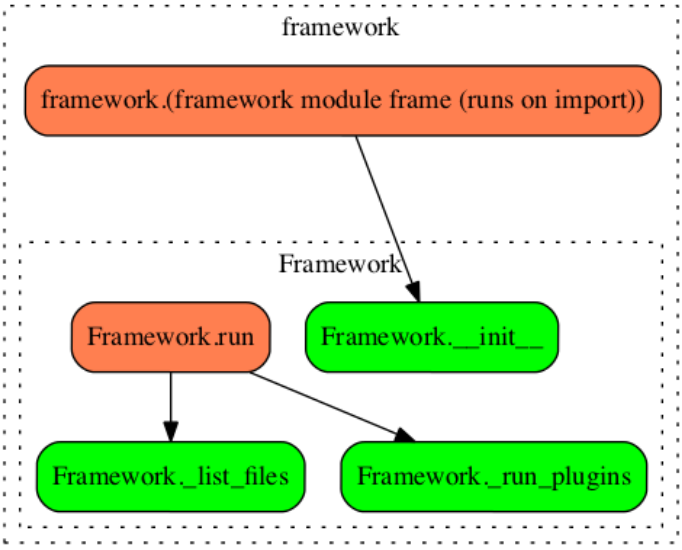

C:\WINDOWS\system32\cmd.exe
C:\learn-python-for-forensics>python Chapters\Chapter12\Code\wal_crawler.py places.sqlite-wal ./wal_output -m
[+] Identifying and parsing file header
[+] Identified 3 Frames.
[+] Processing frames...
0%| | 0/3 [00:00<?, ?it/s][
+] Identified 15 cells in frame 0
[+] Processing cells...
[+] Identified 15 cells in frame 1
[+] Processing cells...
100%|##########| 3/3 [00:00<00:00, 214.29it/s]
==========
[+] Initializing regular expression module.
[*] URL: https://www.mozilla.org/en-US/firefox/central/
[*] URL: https://www.mozilla.org/en-US/firefox/help/
[*] URL: https://www.mozilla.org/en-US/firefox/customize/
[*] URL: https://www.mozilla.org/en-US/contribute/
[*] URL: https://www.mozilla.org/en-US/about/

Chapter 13

```
>>> print '\033[31m' + '31 is the ANSI color code for red'
31 is the ANSI color code for red
>>> print '\033[39m' + '39 will reset our foreground color to default'
39 will reset our foreground color to default
>>> print '\033[47; 31m' + 'We can supply multiple options by separating them wi
th the semicolon. The last option must be immediately followed by "m"'
We can supply multiple options by separating them with the semicolon. The last o
ption must be immediately followed by "m"
```

```
>>> import colorama
>>> print colorama.Fore.RED + 'Red foreground text'
Red foreground text
>>> print colorama.Fore.RED + colorama.Back.GREEN + 'Red foreground text and gre
en background'
Red foreground text and green background
>>> print colorama.Style.RESET_ALL

>>> print 'Back to defaults'
Back to defaults
```

Legend	
Regular function	
Trunk function (nothing calls this)	
Leaf function (this calls nothing else)	
Function call which returns no value	→
Function call returns some value	⇢

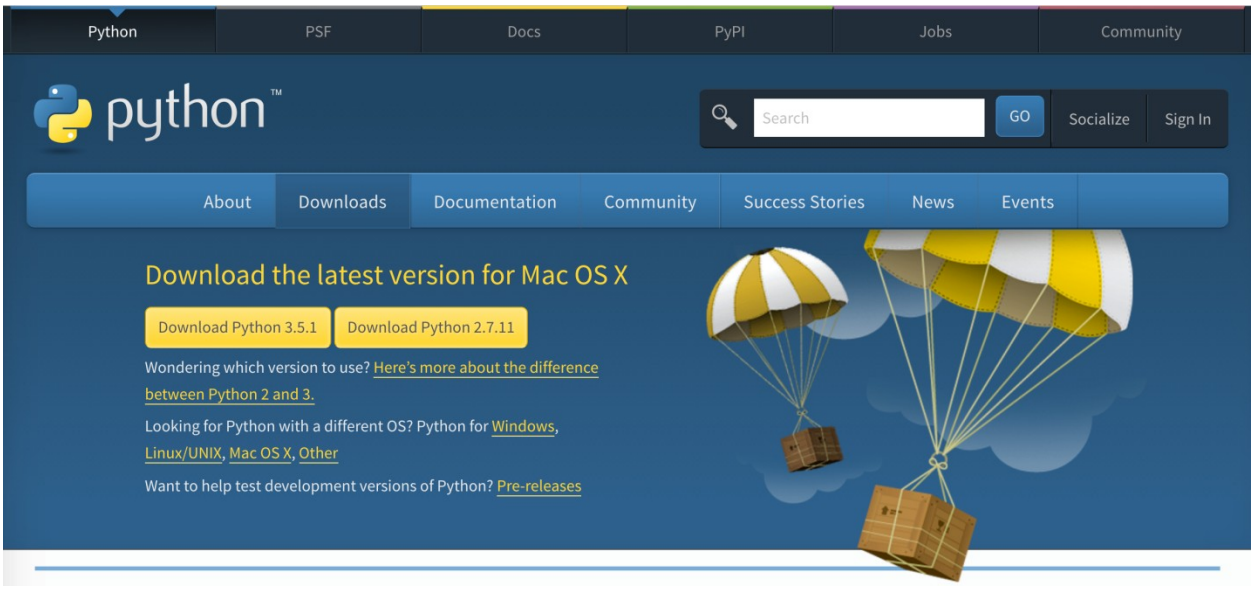


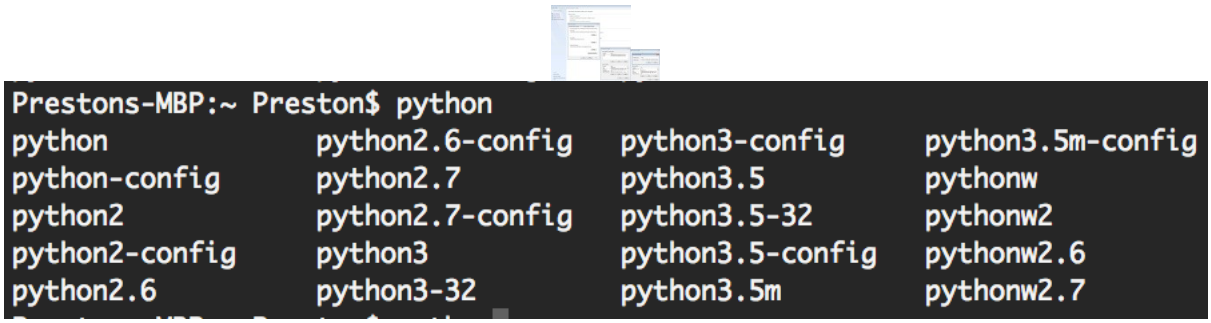
Code — -bash — 80×24

```
[Prestons-MBP:Code Preston$ sudo python framework.py /Users/Preston/Documents/ /U]
sers/Preston/Desktop/output/
[+] Initializing framework v0.01
 ______                                          _
 |  ___|                                        | |
 | |_ _ __ __ _ _ __ ___   _____      _____  _ __| | __
 |  _| '__/ _` | '_ ` _ \ / _ \ \ /\ / / _ \| '__| |/ /
 | | | | | (_| | | | | | |  __/\ V  V / (_) | |  |   <
 \_| |_|  \__,_|_| |_| |_|\___| \_/\_/ \___/|_|  |_|\_\


[+] Indexing /Users/Preston/Documents/
[+] Executing wal_crawler plugin
[*] Plugin wal_crawler completed at 02/07/2016 14:40:42
[+] Writing results of wal_crawler plugin
[+] Executing setupapi plugin
[*] Plugin setupapi completed at 02/07/2016 14:40:42
[+] Writing results of setupapi plugin
[+] Executing userassist plugin
[*] Plugin userassist completed at 02/07/2016 14:40:42
[+] Writing results of userassist plugin
[+] Executing exif_metadata plugin
[*] Plugin exif_metadata completed at 02/07/2016 14:40:42
```

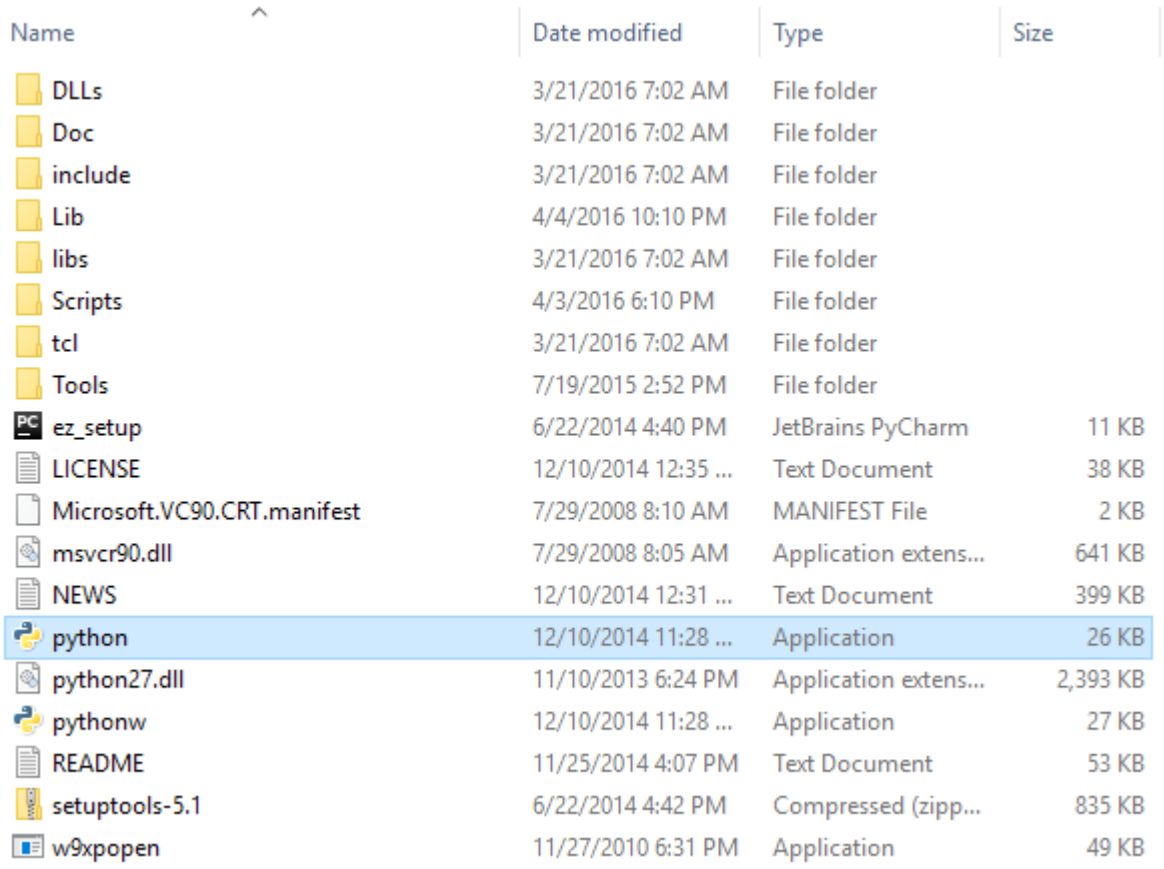
Name	Size	Date Modified
▼ metadata	--	Today, 2:41 PM
exif_metadata.csv	40 KB	Today, 2:40 PM
exif_metadata.kml	3 KB	Today, 2:40 PM
office_metadata.csv	7 KB	Today, 2:40 PM
▼ setupapi	--	Today, 2:41 PM
setupapi.csv	962 bytes	Today, 2:40 PM
▼ userassist	--	Today, 2:41 PM
userassist.csv	77 KB	Today, 2:40 PM
▼ wal	--	Today, 2:41 PM
wal_crawler.csv	307 KB	Today, 2:40 PM

Appendix A


Python
PSF
Docs
PyPI
Jobs
Community
python™
Search
GO
Socialize
Sign In
About
Downloads
Documentation
Community
Success Stories
News
Events
Download the latest version for Mac OS X
Download Python 3.5.1
Download Python 2.7.11
Wondering which version to use? Here's more about the difference between Python 2 and 3.
Looking for Python with a different OS? Python for Windows, Linux/UNIX, Mac OS X, Other
Want to help test development versions of Python? Pre-releases


Prestons-MBP:~ Preston$ python
python
python-config
python2
python2-config
python2.6
python2.6-config
python2.7
python2.7-config
python3
python3-32
python3-config
python3.5
python3.5-32
python3.5-config
python3.5m
python3.5m-config
pythonw
pythonw2
pythonw2.6
pythonw2.7

Appendix B



Name	Date modified	Type	Size
DLLs	3/21/2016 7:02 AM	File folder	
Doc	3/21/2016 7:02 AM	File folder	
include	3/21/2016 7:02 AM	File folder	
Lib	4/4/2016 10:10 PM	File folder	
libs	3/21/2016 7:02 AM	File folder	
Scripts	4/3/2016 6:10 PM	File folder	
tcl	3/21/2016 7:02 AM	File folder	
Tools	7/19/2015 2:52 PM	File folder	
ez_setup	6/22/2014 4:40 PM	JetBrains PyCharm	11 KB
LICENSE	12/10/2014 12:35 ...	Text Document	38 KB
Microsoft.VC90.CRT.manifest	7/29/2008 8:10 AM	MANIFEST File	2 KB
msvcr90.dll	7/29/2008 8:05 AM	Application extens...	641 KB
NEWS	12/10/2014 12:31 ...	Text Document	399 KB
python	12/10/2014 11:28 ...	Application	26 KB
python27.dll	11/10/2013 6:24 PM	Application extens...	2,393 KB
pythonw	12/10/2014 11:28 ...	Application	27 KB
README	11/25/2014 4:07 PM	Text Document	53 KB
setuptools-5.1	6/22/2014 4:42 PM	Compressed (zipp...	835 KB
w9xpopen	11/27/2010 6:31 PM	Application	49 KB