

PFP

Portable Forensic Platform

zurum

E-mail : herosdfrc@gmail.com

By Zurum

목차

- ✓ 개요
- ✓ 구성요소
- ✓ 구조 (Structure)
- ✓ 튜토리얼

개요

- 동기
 - 모듈의 관리, 배포, 개발(재사용성 등)에 관한 불편
 - 숙련된 분석가들의 노하우 축적, 공유 문제
 - 개발, 분석환경 구축에 따른 초보 분석가들의 포렌식 진입장벽 완화
- 목적
 - 연구와 개발환경 통합
 - 멀티 운영체제 동일 인터페이스
 - 개발, 분석, 연구 편의
 - 노하우 축적 틀 제공
 - 다양한 포렌식 분석 모듈의 유기적 활용
- 조건
 - 모듈의 플랫폼 종속성 탈피
 - 모듈간 독립성
 - 모듈 재사용성
 - 모듈 교체 편의성
 - 포터블 분석 패키지
 - 자체 개발 환경 제공
 - 효율적인 공유 시스템



개요

- Other works
 - OCFA
 - <http://ocfa.sourceforge.net/>
 - XIRAF
 - http://www.forensicinstitute.nl/products_and_services/forensic_products/xiraf/
 - Open Source Digital Forensics
 - <http://www2.opensourceforensics.org/tools>
 - Pyrtf
 - <http://www.web2py.com/examples/static/sphinx/gluon/gluon.contrib.pyrtf.html>
 - DFF
 - <http://www.digital-forensic.org/en/>
 - OSF
 - <http://www.osforensics.com/download.html>
 - SIFT
 - <http://computer-forensics.sans.org/community/downloads#over>
- 완성된 Kit, 벤더 종속성
 - ➔ 분석가의 커스터마이징 불가능 or 매우 불편

개요

- 통합 솔루션 개념 → DIY 플랫폼



개요



By Zurum

구성 요소

- 분석 모듈
- 관리 DB
- 공유 시스템
- 모듈 호출 시스템

구성 요소

- 분석 모듈
 - 포렌식 모듈
 - 포렌식 조사 모듈의 분류
 - Binary Modules
 - » CLI Based
 - » GUI Based
 - Setup Files
 - Script(python)
 - 혼용하여 사용 시 모듈간 미묘한 차이로 사용상 불편 야기
 - 구동 방법
 - 구동 경로
 - 설치 여부 등
- ➔ 각각의 모듈이 특성에 맞게 플랫폼에 탑재될 수 있도록 구성

구성 요소

- 분석 모듈

- 단위 모듈 / API (Unit Module)

- 동일한 코드(또는 함수)의 반복적인 사용 경험
 - 특정 코드만 구동, 결과를 확인하고 싶은 경험
 - ➔ " 함수만 들고 다니며 사용할 수 있을까?".

```
def Forensic_FolderCopy(self, ImagePath = "" , FolderPath = "" , ExtractFolder = "" , depth = 0):  
  
    Platform = sys.platform  
  
    if ImagePath == "" or FolderPath == "":  
        print "Select Extract Path"  
        ExtractFolder = tkFileDialog.askdirectory()  
  
        print "Select Target Folder"  
        FolderPath = tkFileDialog.askdirectory()  
  
        TokenizedResult = FolderPath.split(':')  
  
        print "Selected Folder: " , FolderPath  
  
        if 'darwin' in Platform:  
            ImagePath = '/dev/rdisk0s2'  
            FolderPath = FolderPath  
            FolderPath += '/'  
  
        elif 'win' in Platform:  
            ImagePath = "\\.\\"+TokenizedResult[0]+": "  
            FolderPath = TokenizedResult[1]  
            FolderPath += '/'
```

구성 요소

- 분석 모듈
 - 플랫폼 전용 모듈(PFP Module)
 - 플랫폼에 내장된 Python 분석 도구
 - 특정 행위를 자동, 반복적으로 수행하기 위한 단위 모듈의 모음

구성 요소

• 관리 DB

No	ModuleName	ModulePath	ExecutableType	ExecuteCount	Description	OS	Category	AnalysisType	TargetExtender	TargetSignature	isPortable	isInstalled	InstallFilePath
Click here to define a filter													
1	putty	./UserModule/BinaryModules/putty.exe	gui	4	terminal tool	win	live	network			y		
2	010Editor	C:\Program Files (x86)\010 Editor v3\010Editor.exe	gui	26	Hex Viewer	win	death, live	support	allfile	allfile	n	y	./UserModule/Setupfiles/010Editor/010EditorInstaller305.exe
3	0xED	./UserModule/BinaryModules/0xED.app	gui		Hex Viewer for Mac OS X	mac	live, death	support	allfile	allfile	y		
4	AFCViewer	./UserModule/BinaryModules/MFTView/AFCViewer.exe	gui	1	MFT Viewer(by Ahnlab)	win	live	os, file	\$MFT	4649	y		
5	Ahn Report	./UserModule/BinaryModules/AhnReport/AhnRptV.exe	gui	2	Windows OS Volatile Data Analyzer(by Ahnlab)	win	live, death, acquisition	volatile, file, network	arc	4152	y		
6	Athena	./UserModule/BinaryModules/Athena(DFRC Behavior Analyzer)/Athena.exe	gui		User Behavior Analyzer for windows system (by DFRC)	win	live, death, acquisition	os			y		
7	BinText	./UserModule/BinaryModules/bintext303/bintext.exe	gui	3	PE Analyzer	win	death, live	file	exe, scr, dll, cpl, ocx, obj, sys, drv	4D5A	y		
8	Camtasia	C:\Program Files (x86)\TechSmith\Camtasia Studio 7\CamtasiaStudio.exe	gui	1	Screen recoder	win	util	util	allfile	allfile	n	y	./UserModule/Setupfiles/Camtasia Studio 7.0.0/Camtasia Studio 7.0.0.exe.msi
9	Cport	./UserModule/BinaryModules/Currport/cports.exe	gui	1	Windows port analyzer	win	live	network, os			y		
10	DATAForensics	./UserModule/BinaryModules/DATAForensics(DFRC Carving Tool)/DATAForensics.exe	gui	1	Carving tool for windows system(by DFRC)	win	live, death, acquisition	storage			y		
11	DCode	./UserModule/BinaryModules/DCode(Time Convert).exe	gui		Time format convertal	win	live, death	support	allfile	allfile	y		
12	DFRC_Destroyer	./UserModule/BinaryModules/DFRC_Destroyer.exe	gui		wiping tool (by DFRC)	win	live	file	allfile	allfile	y		
13	DeamonTool	C:\Program Files (x86)\DAEMON Tools Lite\DTLite.exe	gui	1	CD Image mount program	win	util	util	iso	4344303031	n	y	./UserModule/Setupfiles/daemon4355-lite/daemon4355-lite.exe
14	EditPlus	C:\Program Files (x86)\EditPlus 3\editplus.exe	gui	1	Text Editor	win	live, death	support	allfile	allfile	n	y	./UserModule/Setupfiles/Editplus/epp300.exe
15	Elex	C:\Program Files (x86)\Event Log Explorer\wex.exe	gui	29	Windows Event Log Viewer	win	live, death	os, file	evt, evtx	3000,456C	n	y	./UserModule/Setupfiles/elex_setup(Windows Event Logs Viewer)/elex_setup(Windows Event Logs Viewer).exe
16	Encase4.2 Portable	./UserModule/BinaryModules/EnCase 4.2(Cracked Portable Encase)/encase.exe	gui		Encase4.2	win	live, death, acquisition	storage			y		
17	Encase6(64bit)	C:\Program Files\EnCase6\Encase.exe	gui	7	Encase6	win	live, death, acquisition	storage			n	y	./UserModule/Setupfiles/EnCase Forensic

<Filter is Empty>

구성 요소

- 관리 DB (Field 정의)

Field Name	정의	조건
ModuleName	모듈의 이름	
ModulePath	모듈의 실행 경로	설치용의 경우 기본 경로
Version	모듈 버전	Reserved
ExecuteCount	실행된 횟수	모듈 호출 시 카운트, 카운트 높은순으로 출력
Description	모듈 설명	
OS	구동 환경	windows, mac, linux 中 택 1
Category	사용 분류	live, death, util, acquisition(다중 선택 가능)
AnalysisType	분석 대상	file, support, util, os, network, storage, memory, volatile app의 경우 관련된 파일이 들어온 경우에만 호출
TargetExtender	분석 대상 확장자	분석 대상이 file, os인 경우에 설정
TargetSignature	분석 대상 시그니처	분석 대상이 file, os인 경우에 설정
isPortable	포터블 구동 여부	
isInstalled	인스톨 필요 여부	isPotable과 배타적 설정
InstallFilePath	설치파일 경로	isInstalled 가 TRUE일 경우만 설정
ExecutableHash	파일 해쉬	포터블의 경우 실행파일, 설치용인 경우 설치파일의 해쉬
isUsed	사용 여부	x 인 경우 모듈 로딩 x

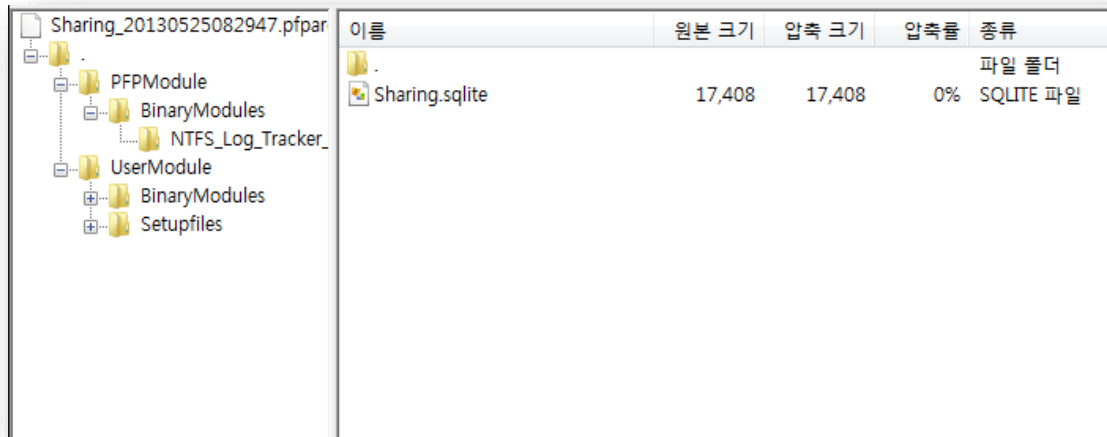
구성 요소

- 공유 시스템

- 목적 :

- 조직내 분석 환경 통일
 - 플랫폼 적용 모듈에 대한 공유 활성화

- PFP Archive



- .pfparc 생성 및 사용

- <http://portable-forensics.blogspot.kr/2013/05/pfp-pfparc.html>

구성 요소

- 모듈 호출 시스템
 - 목적 : 상황에 따른 직관적 모듈 호출
 - Prototype에 적용된 호출 시스템
 - 조사 절차에 따른 호출
 - 침해사고 조사, 증거 채취(부정 조사)
 - + 절차 제작 기능(Do It Yourself)
 - 모듈 자체 호출
 - 모듈 이름 검색
 - 상황별 분류에 따른 호출
 - 전체 목록에서의 호출
 - 분석 대상(파일)과 관련된 모듈 호출
 - 분석 대상 파일을 선택할 경우, 관련된 모든 분석 모듈 목록을 출력
 - 파일에 대한 다각적 분석에 용이하도록 구성
 - 단위 모듈 호출

구성 요소

- 모듈 호출 시스템
 - Prototype에 적용된 호출 시스템

```
AnalysisPoint(WindowsFamily).txt - 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

==Format=====
#Analysis Point
#
#Artifact Location
#Acquisition Tools
#Analysis Target
#Analysis Tools
==Format=====

#####
#Preparing#
#####

Data Acquisition
Artifact Location
Disk Image
Artifact
Registry Hive
Memory(In Live)
Live Data(In Live)

Acquisition Tools
AhnReport
AhnForensic
FDPro
Win32dd
Win64dd
AIF
REGA
RegWorkshop

Analysis Target
Collect data for forensic analysis

Analysis Tools

Live, Network
Artifact Location
Live Command(Batch)
Physical Memory
Registry Hive

HKLM\SYSTEM\ControlSet000\Services\LanmanServer\Shares
HKLM\SYSTEM\Software\Microsoft\Windows NT\CurrentVersion
HKLM\SYSTEM\Software\Microsoft\Windows NT\CurrentVersion
HKLM\SYSTEM\ControlSet000\Control\ComputerName\Active
HKLM\SYSTEM\ControlSet000\Control\TimeZoneInformation
HKLM\SYSTEM\Software\Microsoft\Windows NT\CurrentVersion

0060970EAC(F9)Count
HKLM\SYSTEM\Software\Microsoft\Windows NT\CurrentVersion
HKLM\SYSTEM\ControlSet000\Control\FileSystem

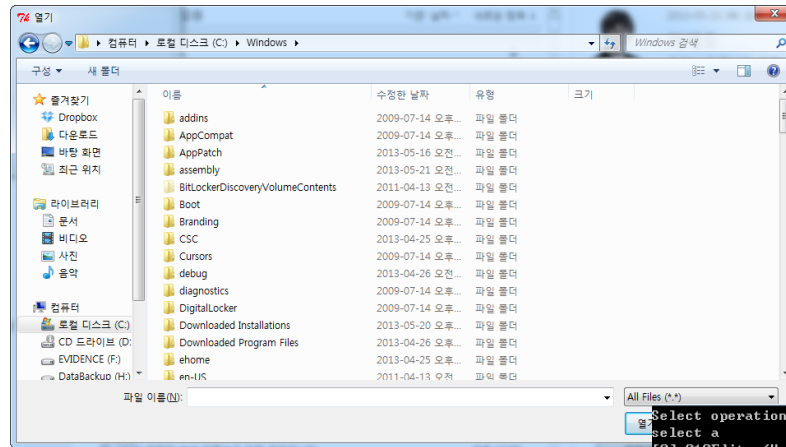
Acquisition Tools
AhnReport
AhnForensic
FDPro
Win32dd
Win64dd
AIF
REGA
RegWorkshop

Analysis Target
Any vestiges of live data

Analysis Tools
AhnReport
AhnForensic
RedLine
Volatility
MEMA
AIF
RegWorkshop
REGA

#####
#Whole Image Analysis#
#####

TimeLine, Whole Search
Artifact Location
Whole Image
Main Artifact
```



```
Select operation : f
select f
Selected File: Q:\cmd(32bit).exe

[*]Dedicated module List is following
[0].BinText<PE Analyzer>
[1].LoadPE<PE Viewer>
[2].PE Explorer<PE file Analyzer>
[3].PEID<PE file Analyzer>
[4].PEView<PE Structure Viewer>
[5].Stud_PE<PE file analyzer>

[*]Common module List is following
[6].WinHex<Hex Viewer (acceptable for disk view)>
[7].LITViewer<Big Size Document Viewer>
[8].HashCalc(it can be used for calculate for hash value)
[9].osfMount(Windows Disk Mount Program)
[10].ofsmount(64bit)<Windows Disk Mount Program>
[11].010Editor<Hex Viewer>
[12].HxD<Hex Viewer>
```

```
Select operation : a
select a
select 1
[0].010Editor<Hex Viewer>
[1].AFCViewer<MFT Viewer>
[2].Ahn Report<Windows OS>
[3].Athena<User Behavior>
[4].BinText<PE Analyzer>
[5].CDFFViewer<Compound File System Viewer>
[6].Encase4.2 Portable<Encase4.2>
[7].FTK Imager portable<FTK Imager>
[8].forecopy<File raw copy>
[9].DATAForensics<Carving>
[10].DCode<Time format cd>
[11].Athena<User Behavior>
[12].DeamonTool<CD Image>
[13].forecopy<File raw copy>
[14].Elex<Windows Event Log>
[15].Encase4.2 Portable<Encase4.2>
[16].Encase6<64bit><Encase6>
[17].FDPro<Memory Dump tool>
[18].win64dd<Windows Memory Dump Tool>
[19].FDPro<Memory Dump tool (by Mandiant)>
[20].FISA<File system analyzer>
[21].FTK Imager<FTK Imager>
[22].FTK Imager portable<FTK Imager portable>
[23].HBGary<Expensive memory forensic tool(need dongle)>
[24].HashCalc(it can be used for calculate for hash value)
[25].HexWorkshop<Hex Viewer>
[26].HxD<Hex Viewer>
[27].JPEGenoop<exif format analyzer>
[28].LP_Check<Find hidden account>
[29].LITViewer<Big Size Document Viewer>
[30].LoadPE<PE Viewer>
[31].MEMA<Memory dump file analyzer (by DFRC)>
```

```
#####
#Preparing#
#####

[0] Data Acquisition
[1] Live, Network

#####
#Whole Image Analysis#
#####

[2] TimeLine, Whole Search
[3] Malware Quick Search

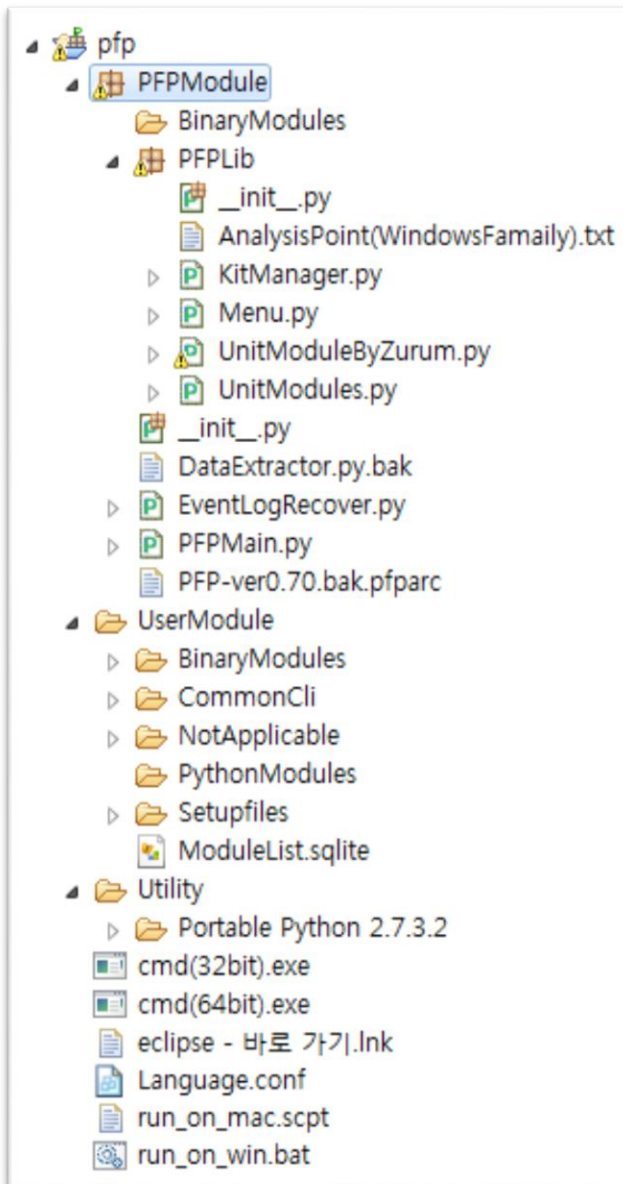
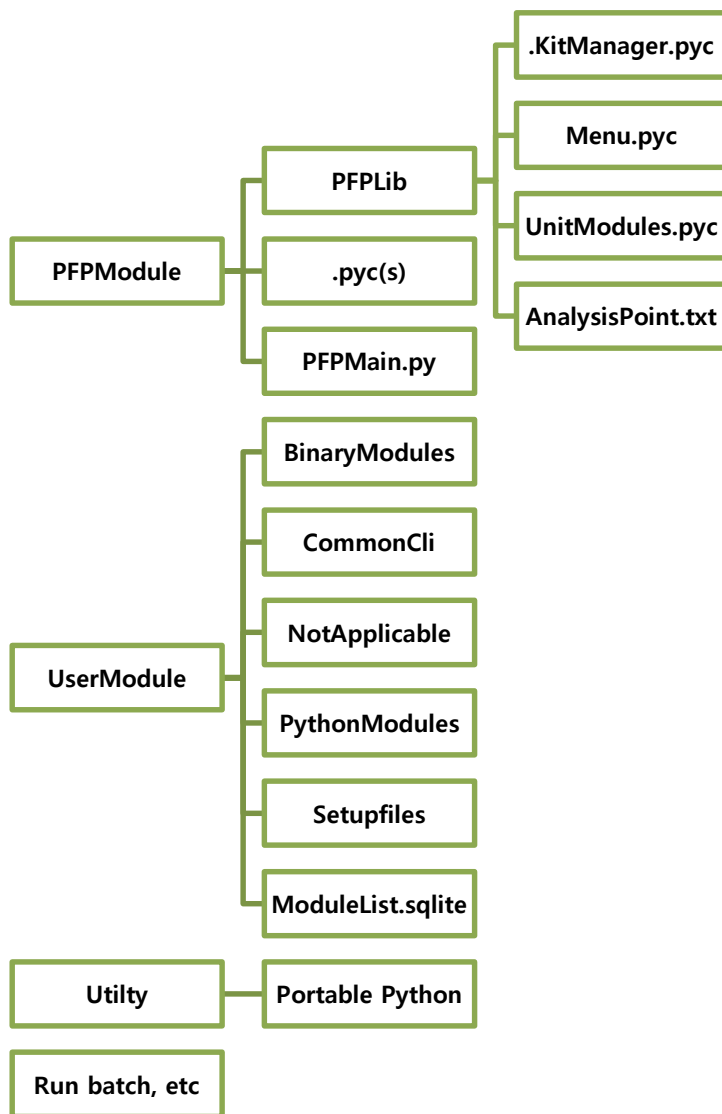
#####
#Vestige Analysis (Essential)#
#####

[4] Vestige of Executable
[5] Reloading List
[6] Registry ShellBag
[7] Web Artifact
[8] TempFile
[9] EventLog
[10] Restore Point
[11] System Log

Select module (number):
```

구조

- 전체 구조



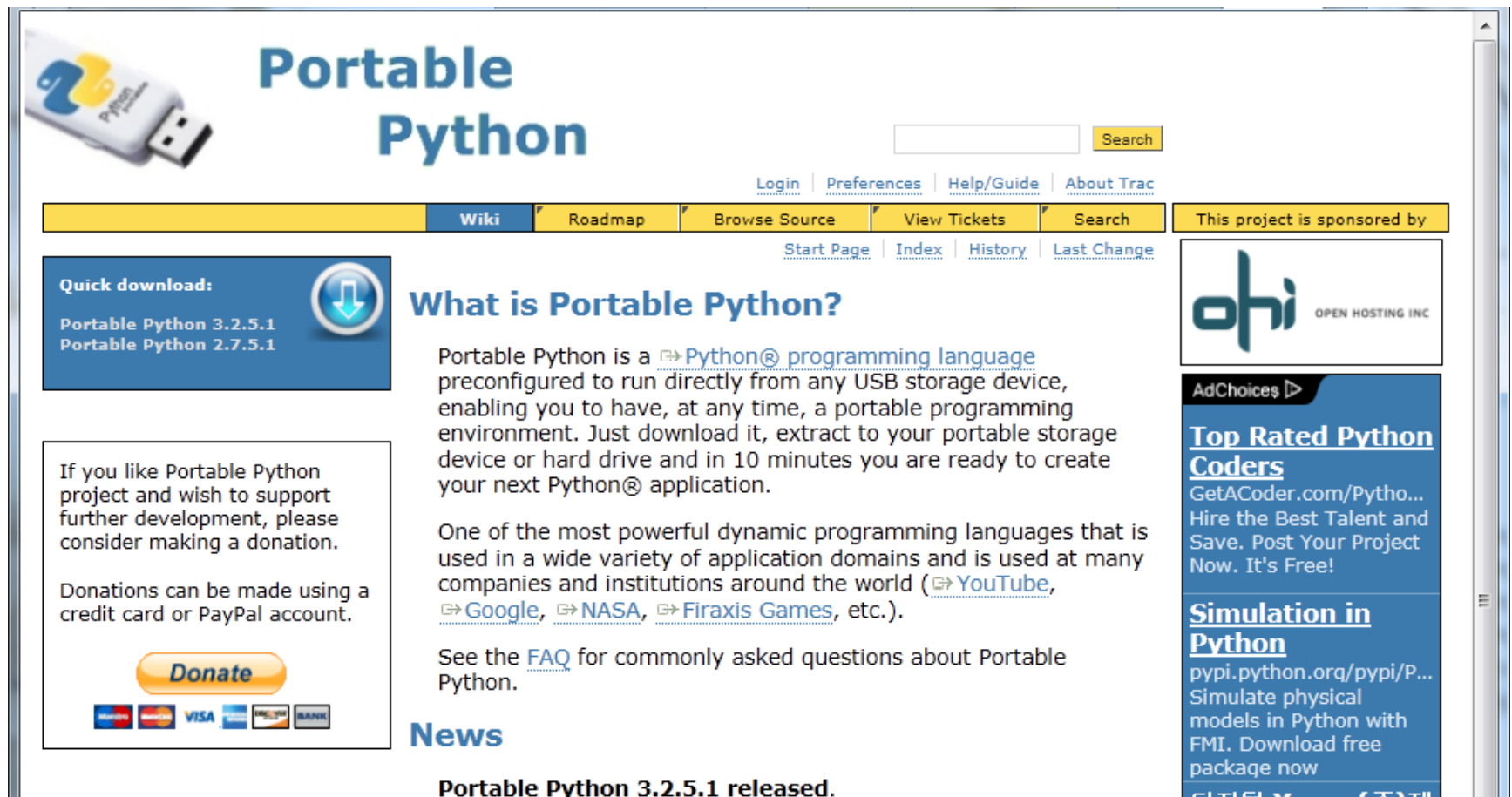
구조

- Modules

모듈 구분	요소	설명
PFPMModule	BinaryModules	PFP 기본 탑재 모듈 중 Python 이외의 언어로 제작된 실행파일
	PFPLib	PFP 기본 동작 코드 와 단위 모듈 클래스, AnalysisPoint.txt
	.pyc	PFP 전용 모듈
UserModule	BinaryModules	타 그룹 혹은 벤더에서 제작한 Portable Binary 모듈
	PythonModules	타 그룹 혹은 벤더에서 제작한 Python 모듈
	SetupFiles	설치를 필요로하는 모듈의 설치파일 (default.txt 포함 필수)
	ModuleList.sqlite	PFP에 탑재된 모든 모듈을 관리하는 데이터베이스(SQLite)
	CommonCli	CLI 모듈에 대한 관리 편의를 위한 폴더
	NotApplicable	현재 버전에 적용되지 못하는 모듈들(차후 개선안 모음)

구조

- Utility
 - Portable Python



The screenshot shows the homepage of the Portable Python project. At the top left is a USB drive icon with the Python logo. The title "Portable Python" is in large blue font. A search bar and "Search" button are on the right. A navigation bar includes links for Login, Preferences, Help/Guide, and About Trac. Below this is a yellow bar with links for Wiki, Roadmap, Browse Source, View Tickets, and Search. A sidebar on the left contains a "Quick download" section with links to Portable Python 3.2.5.1 and 2.7.5.1, a "Donate" button, and a list of payment methods (Visa, MasterCard, etc.). The main content area features the heading "What is Portable Python?" followed by a paragraph explaining that it is a Python programming language preconfigured to run from USB storage. Below this is another paragraph stating it is one of the most powerful dynamic programming languages. A "News" section at the bottom mentions "Portable Python 3.2.5.1 released." On the right side, there is a section for "Top Rated Python Coders" and "Simulation in Python" with links to external resources.

Portable Python

Quick download:
Portable Python 3.2.5.1
Portable Python 2.7.5.1

If you like Portable Python project and wish to support further development, please consider making a donation.

Donations can be made using a credit card or PayPal account.

Donate

Visa MasterCard American Express Discover PayPal

What is Portable Python?

Portable Python is a [Python® programming language](#) preconfigured to run directly from any USB storage device, enabling you to have, at any time, a portable programming environment. Just download it, extract to your portable storage device or hard drive and in 10 minutes you are ready to create your next Python® application.

One of the most powerful dynamic programming languages that is used in a wide variety of application domains and is used at many companies and institutions around the world ([YouTube](#), [Google](#), [NASA](#), [Firaxis Games](#), etc.).

See the [FAQ](#) for commonly asked questions about Portable Python.

News

Portable Python 3.2.5.1 released.

This project is sponsored by

ohi OPEN HOSTING INC

AdChoices

Top Rated Python Coders

GetACoder.com/Pytho...
Hire the Best Talent and Save. Post Your Project Now. It's Free!

Simulation in Python

pypi.python.org/pypi/P...
Simulate physical models in Python with FMI. Download free package now

동작

- 범용 명령
 - f = select file
 - 'keyword = find module by name
 - c = open terminal (CommonCli Folder)
 - n = Open Explorer (Not Applicable)
 - s = Self Test
 - a = show all
 - d = DB Configure

동작

- 조사 환경
 - I = Analysis Point list

```
AnalysisPoint(WindowsFamily).txt - 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)
=====Format=====
=Analysis Point
= Artifact Location
= Acquisition Tools
= Analysis Target
= Analysis Tools
=====Format=====
#####
# Preparing #
#####
Data Acquisition
Artifact Location
Disk Image
Artifact
Registry Hive
Memory(in Live)
Live Data(in Live)
Acquisition Tools
AhnReport
AhnForensic
FDPro
Win32dd
Win64dd
AIR
REGA
RegWorkshop
Analysis Target
Collect data for forensic analysis
Analysis Tools
Live, Network
Artifact Location
Live Command(Batch)
Physical Memory
Registry Hive
HKLM\SYSTEM\ControlSet00X\Services\LanmanServer\Shares
HKLM\SYSTEM\Software\Microsoft\Windows\CurrentVersion\
HKLM\SYSTEM\Software\Microsoft\Windows NT\CurrentVersion\
HKLM\SYSTEM\ControlSet00X\Control\ComputerName\Active
HKLM\SYSTEM\ControlSet00X\Control\Windows
HKLM\SYSTEM\ControlSet00X\Control\TimeZoneInformation
HKLM\SYSTEM\Software\Microsoft\Windows\CurrentVersion\
006097DEACF9\Count
HKLM\SYSTEM\Software\Microsoft\Windows\CurrentVersion\
HKLM\SYSTEM\Software\Microsoft\Windows\CurrentVersion\
Acquisition Tools
AhnReport
AhnForensic
FDPro
Win32dd
Win64dd
AIR
REGA
RegWorkshop
Analysis Target
Any vestiges of live data
Analysis Tools
AhnReport
AhnForensic
RedLine
Volatility
MEMA
AIR
RegWorkshop
REGA
#####
# Whole Image Analysis #
#####
TimeLine, Whole Search
Artifact Location
Whole image
Main Artifact
```

```
#####
# Preparing #
#####
[0] Data Acquisition
[1] Live, Network

#####
# Whole Image Analysis #
#####
[2] TimeLine, Whole Search
[3] Malware Quick Search

#####
# Vestige Analysis (Essential) #
#####
[4] Vestige of Executable
[5] Reloading List
[6] Registry ShellBag
[7] Web Artifact
[8] TempFile
[9] EventLog
[10] Restore Point
[11] System Log

Select module (number):
```


Project

- Project
 - <http://code.google.com/p/portable-forensic-platform/>
- Blog
 - <http://portable-forensics.blogspot.kr/>
- Google 검색
 - Portable Forensics

Thank you

By Zuram