

# PFP 두번째 이야기

---

*zurum*

*herosdfrc@gmail.com*



- 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





- Other works
  - OCFA
    - <http://ocfa.sourceforge.net/>
  - XIRAF
    - [http://www.forensicinstitute.nl/products\\_and\\_services/forensic\\_products/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

# Concept



- 통합 솔루션 개념 → DIY 플랫폼

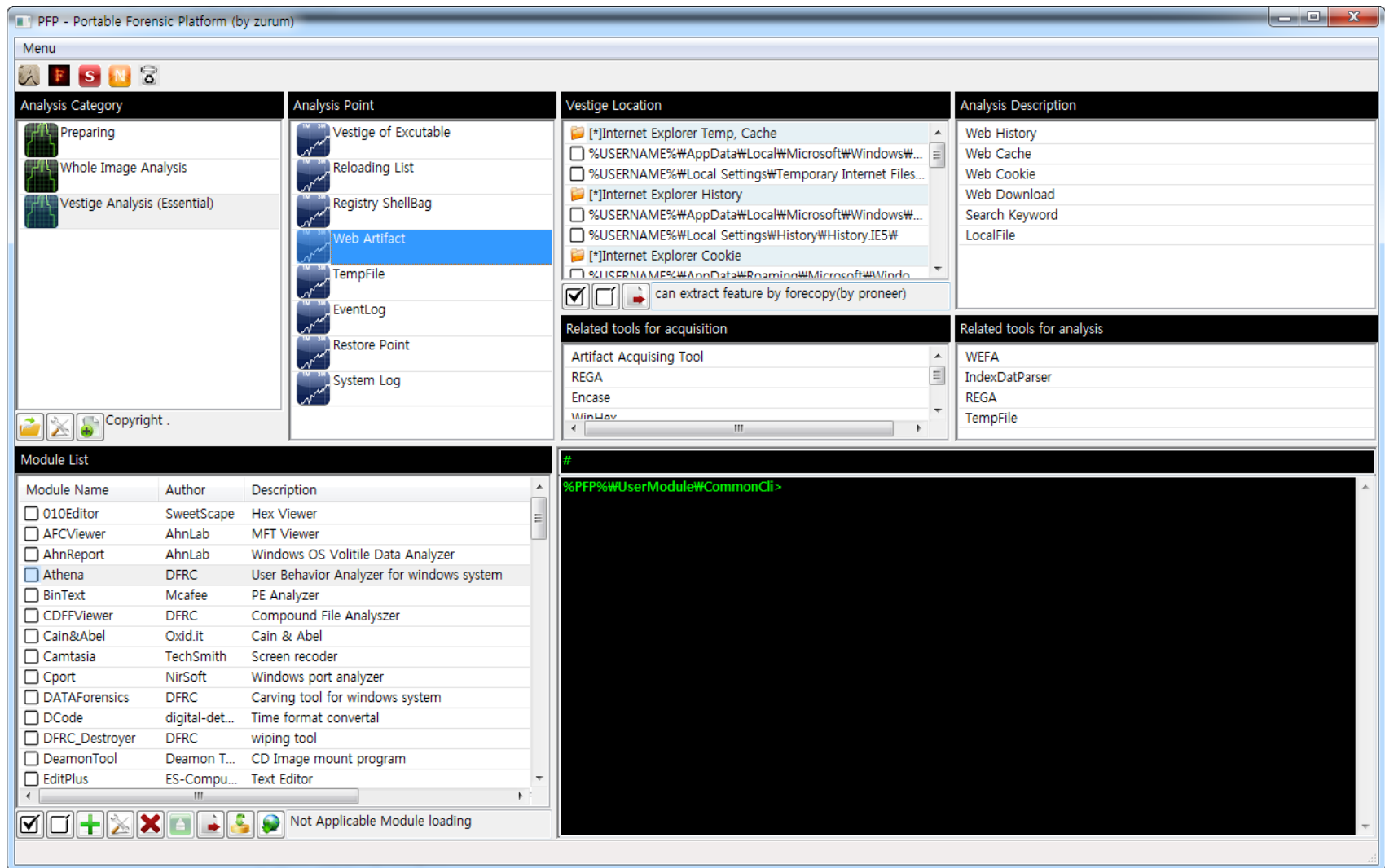




# Concept



- **Manual :** <https://code.google.com/p/portable-forensic-platform/downloads/list>



# The initial screen



PFP - Portable Forensic Platform (by zurum)

Menu

Analysis Category

- Preparing
- Whole Image Analysis
- Vestige Analysis (Essential)

Analysis Point

- Vestige of Executable
- Reloading List
- Registry ShellBag
- Web Artifact
- TempFile
- EventLog
- Restore Point
- System Log

Vestige Location

- [\*]Internet Explorer Temp, Cache
- ☐ %USERNAME%\AppData\Local\Microsoft\Windows\...
- ☐ %USERNAME%\Local Settings\Temporary Internet Files...
- [\*]Internet Explorer History
- ☐ %USERNAME%\AppData\Local\Microsoft\Windows\...
- ☐ %USERNAME%\Local Settings\History\History.IE5\
- [\*]Internet Explorer Cookie
- ☐ %USERNAME%\AppData\Roaming\Microsoft\Windo...
- ☒ ☐ ☐ can extract feature by forecopy(by proneer)

Analysis Description

- Web History
- Web Cache
- Web Cookie
- Web Download
- Search Keyword
- LocalFile

Related tools for acquisition

- Artifact Acquiring Tool
- REGA
- Encase
- WinHex

Related tools for analysis

- WEFA
- IndexDatParser
- REGA
- TempFile

Module List





















| Module Name                                | Author         | Description                               |
|--|----------------|---|
| <input type="checkbox"/> 010Editor         | SweetScape     | Hex Viewer                                |
| <input type="checkbox"/> AFCViewer         | AhnLab         | MFT Viewer                                |
| <input type="checkbox"/> AhnReport         | AhnLab         | Windows OS Volatile Data Analyzer         |
| <input checked="" type="checkbox"/> Athena | DFRC           | User Behavior Analyzer for windows system |
| <input type="checkbox"/> BinText           | Mcafee         | PE Analyzer                               |
| <input type="checkbox"/> CDFVViewer        | DFRC           | Compound File Analyzer                    |
| <input type="checkbox"/> Cain&Abel         | Oxid.it        | Cain & Abel                               |
| <input type="checkbox"/> Camtasia          | TechSmith      | Screen recorder                           |
| <input type="checkbox"/> Cport             | NirSoft        | Windows port analyzer                     |
| <input type="checkbox"/> DATAForensics     | DFRC           | Carving tool for windows system           |
| <input type="checkbox"/> DCode             | digital-det... | Time format convertal                     |
| <input type="checkbox"/> DFRC_Destroyer    | DFRC           | wiping tool                               |
| <input type="checkbox"/> DeamonTool        | Deamon T...    | CD Image mount program                    |
| <input type="checkbox"/> EditPlus          | ES-Compu...    | Text Editor                               |

Not Applicable Module loading

```
#
%PFP%\UserModule\CommonCli>
```

# PFP-List panel



| Analysis Category  | Analysis Point  | Vestige Location   | Analysis Description              |
|--|---|--|-----------------------------------|
|  Preparing                    |  Vestige of Executable |  [*]Internet Explorer Temp, Cache   | Web History                       |
|  Whole Image Analysis         |  Reloading List        | <input type="checkbox"/> %USERNAME%\AppData\Local\Microsoft\Windows\Te...  | Web Cache                         |
|  Vestige Analysis (Essential) |  Registry ShellBag     | <input type="checkbox"/> %USERNAME%\Local Settings\Temporary Internet Files\C...   | Web Cookie                        |
|  |  Web Artifact          |  [*]Internet Explorer History   | Web Download                      |
|  |  TempFile              | <input type="checkbox"/> %USERNAME%\AppData\Local\Microsoft\Windows\His...   | Search Keyword                    |
|  |  EventLog              | <input type="checkbox"/> %USERNAME%\Local Settings\History\History.IE5\W   | LocalFile                         |
|  |  Restore Point         |  [*]Internet Explorer Cookie  |                                   |
|  |  System Log            | <input type="checkbox"/> %USERNAME%\AppData\Roaming\Microsoft\Windows\W...   |                                   |
|  |   | <input type="checkbox"/> %USERNAME%\Cookies\W  |                                   |
|  |   |  [*]Internet Explorer Download  |                                   |
|  |   | <input type="checkbox"/> %USERNAME%\AppData\Roaming\Microsoft\Windows\W...   |                                   |
|  |   |  [*]FireFox Cache, History, Cookie, Download  |                                   |
|  |   | <input type="checkbox"/> %USERNAME%\AppData\Local\Mozilla\Firefox\Profiles\W   |                                   |
|  |   | <input type="checkbox"/> %USERNAME%\Local Settings\Application Data\Mozilla\W...   |                                   |
|  |   |  [*]Chrome Cache, History, Cookie, Download   |                                   |
|  |   | <input type="checkbox"/> %USERNAME%\AppData\Local\Google\Chrome\User D...  |                                   |
|  |   | <input type="checkbox"/> %USERNAME%\Local Settings\Application Data\Google\Chrome\User Data\DefaultW   |                                   |
|  |   |  [*]Safari Cache, History, Cookie, Download   |                                   |
|  |   | <input type="checkbox"/> %USERNAME%\AppData\Local\Apple Computer\Safari\W  |                                   |
|  |   | <input type="checkbox"/> %USERNAME%\Local Settings\Application Data\Apple C...   |                                   |
|  |   |  [*]Opera Cache, History, Cookie, Download  |                                   |
|  |   | <input type="checkbox"/> %USERNAME%\AppData\Local\Opera\Opera\cache\W  |                                   |
|  |   | <input type="checkbox"/> %USERNAME%\AppData\Roaming\Opera\Opera\W  |                                   |
|  |   | <input type="checkbox"/> %USERNAME%\Local Settings\Application Data\Opera\W...   |                                   |
|  |   | <input type="checkbox"/> %USERNAME%\Application Data\Opera\Opera\W   |                                   |
|  |   | <input type="checkbox"/> Registry Hive   |                                   |
|  |   | <input type="checkbox"/> HKU\{USER}\SOFTWARE\Microsoft\Internet Explorer\Main  |                                   |
|  |   | <input type="checkbox"/> HKU\{USER}\SOFTWARE\Microsoft\Internet Explorer\Ty...   |                                   |
|  |   | <input type="checkbox"/> HKU\{USER}\SOFTWARE\Microsoft\Internet Explorer   |                                   |
|  |   | <input type="checkbox"/> HKU\{USER}\SOFTWARE\Microsoft\Windows\CurrentVe...  |                                   |
|  |   | <input checked="" type="checkbox"/> <input type="checkbox"/>  can extract feature by forecopy(by proneer) |                                   |
|  |   | <b>Related tools for acquisition</b>   | <b>Related tools for analysis</b> |
|  |   | Artifact Acquiring Tool  | WEFA                              |
|  |   | REGA   | IndexDatParser                    |
|  |   | Encase   | REGA                              |
|  |   | WinHex   | TempFile                          |



# PFP-List panel(Button in Analysis Category)

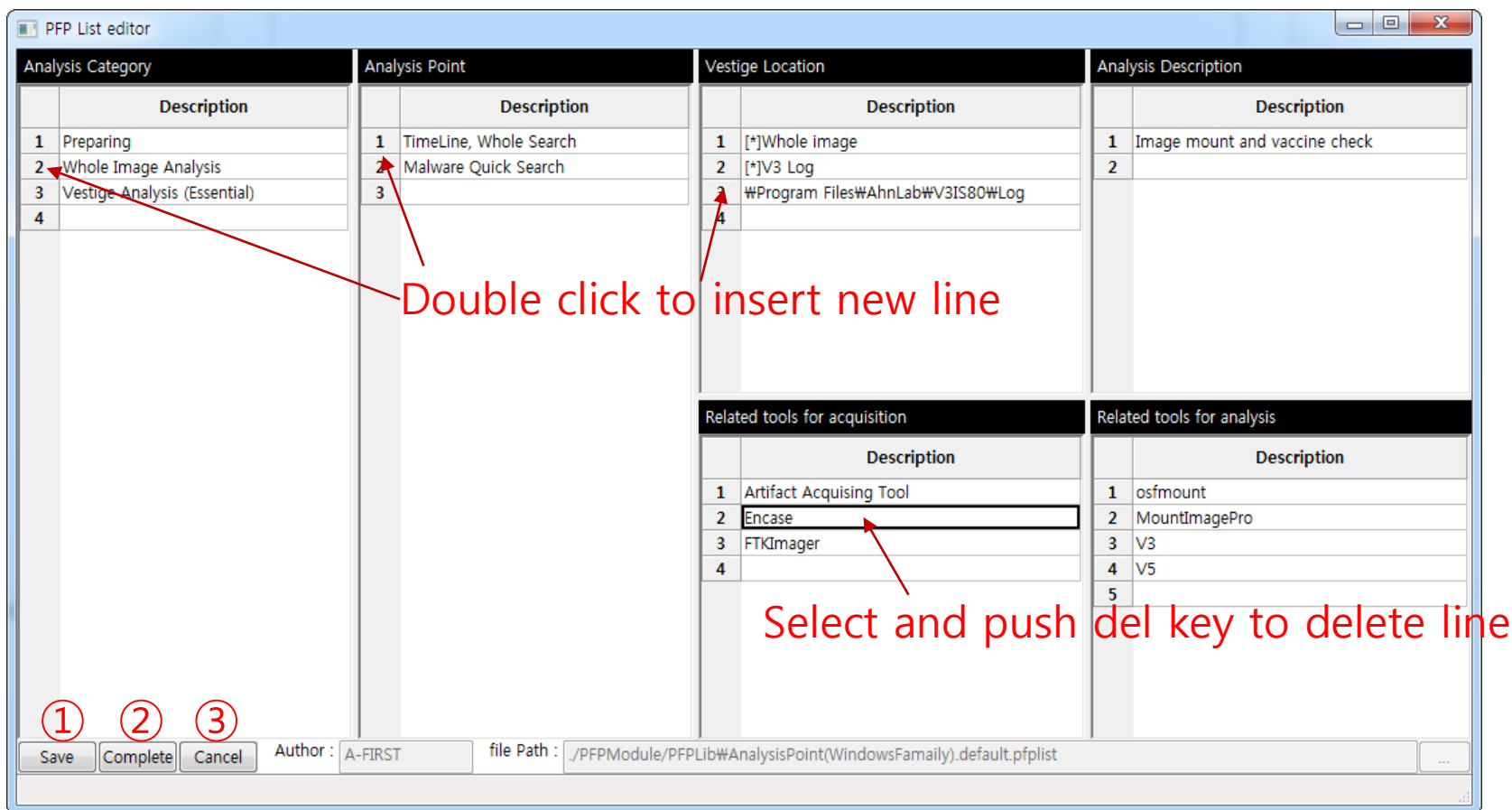


- ① 1. Open File
  - Open another PFP-List(.pfplist) file
- ② 2. Modify File
  - Load PFP-List config window for Modify current .pfplist file
- ③ 3. New
  - Load PFP-List config window for Make New .pfplist file
- ④ 4. Copyright text
  - Copyright text of current PFP-List (.pfplist)

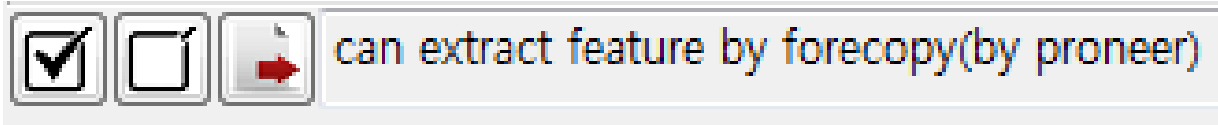
# PFP-List panel(PFP-List Config window)



- ① Save : Save as PFP-List in file Path.
- ② Complete : Save and close the config window
- ③ Cancel : Do not save and close the config window



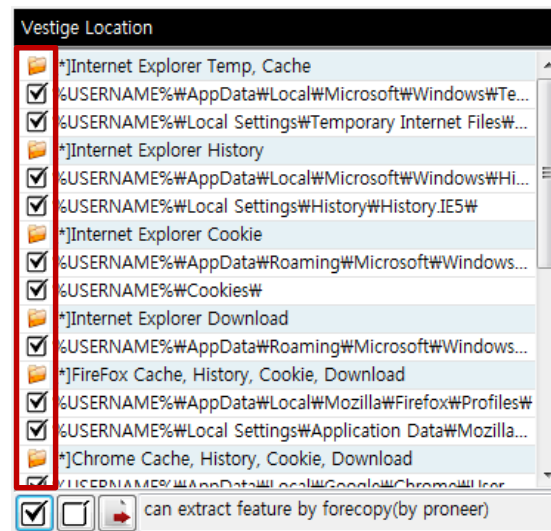
# PFP-List panel(Button in Vestige Location)



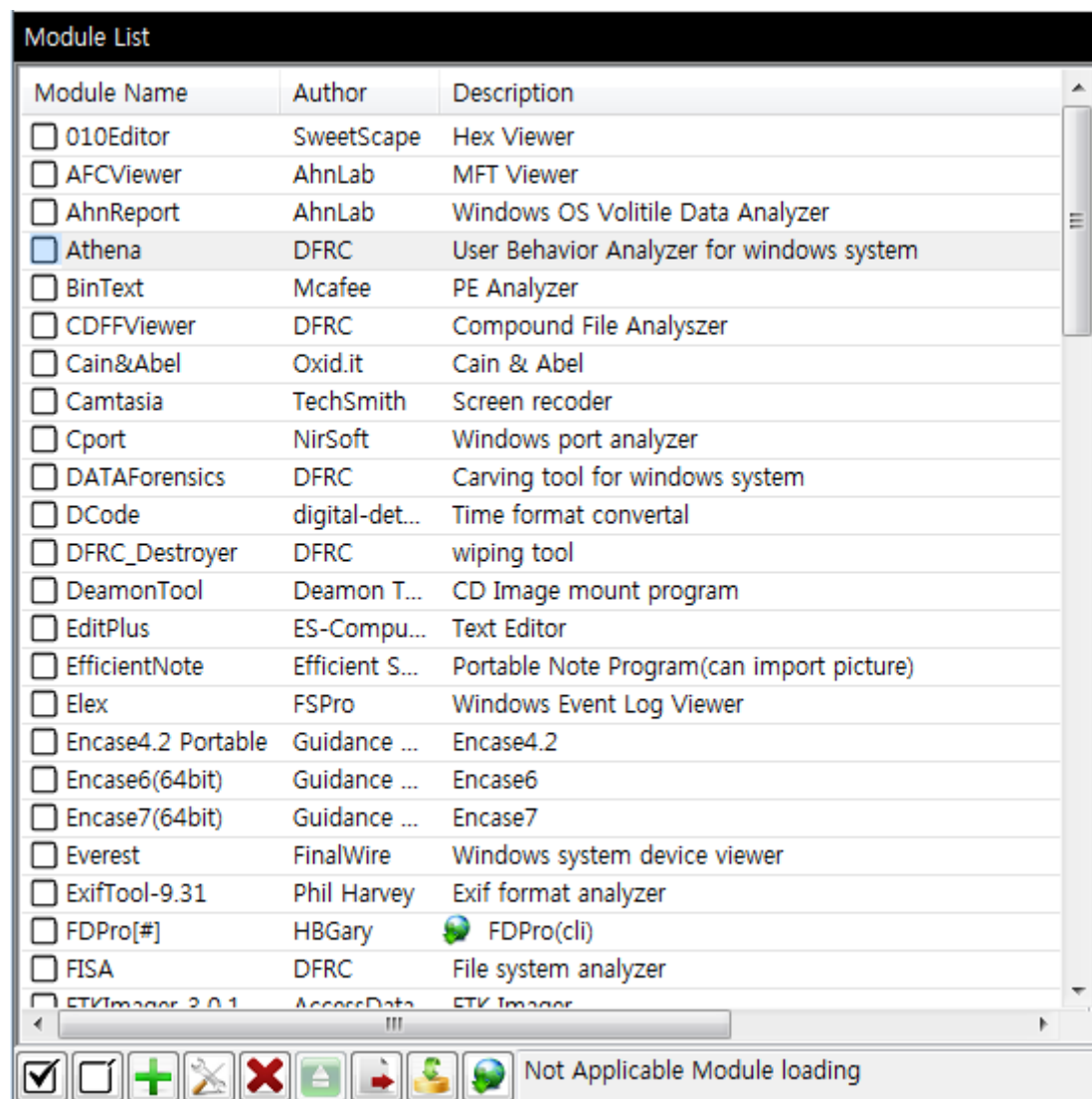
① ② ③

④

- 1. Check All
  - Check all item.
- 2. Release All
  - Release all item.
- 3. Extract artifact(only checked)
  - Forensic copy all checked item using forecopy.
- 4. Status bar



# Module Launcher



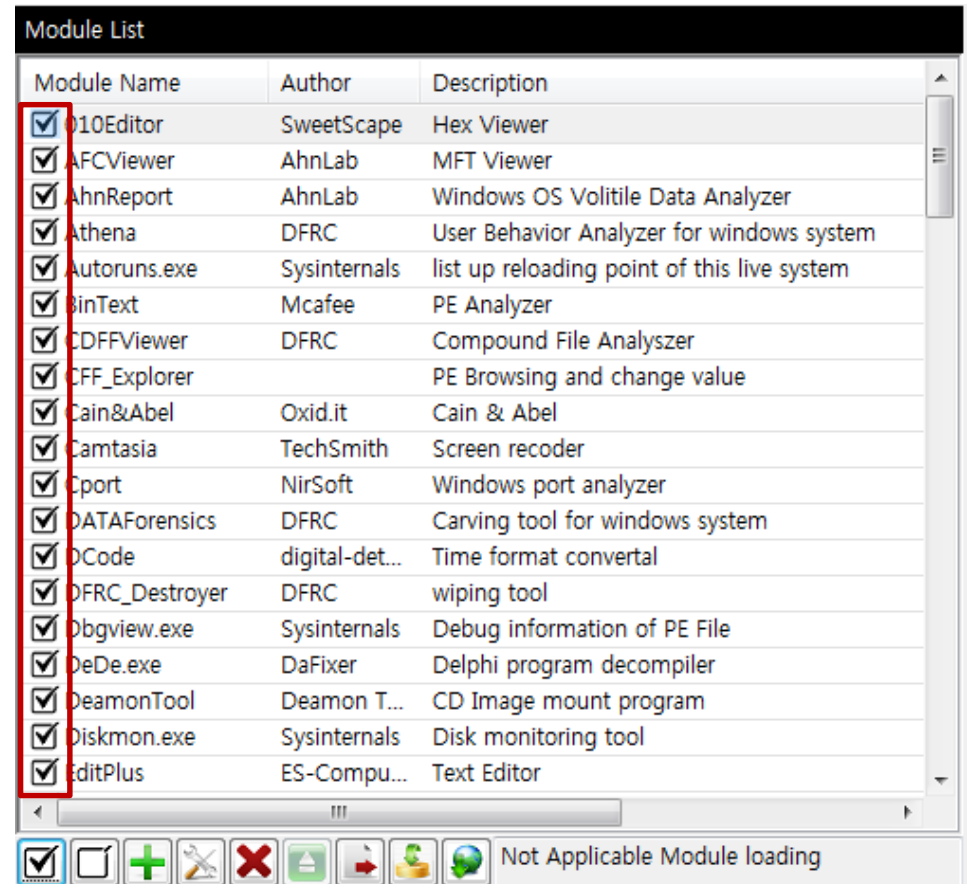


# Module Launcher(Button)



① ②

- 1. Check All
  - Check all modules
- 2. Release All
  - Release all modules



# Module Launcher(Button)



- 3. Insert new module
  - Load Module configure window for new module
- 4. Modify selected module property
  - Load Module configure window for modify selected module

# Module Launcher(Module Config window)



Module Information

Modify Module

Module Path 1 C:\Program Files\Wireshark\Wireshark.exe Browse..

Module Name 2 WireShark(64bit)

Description 3 Network packet monitoring toolhttp://wiresharkdownloads.river

Executable Type 4 gui Platform 5 Windows

Argument 6 Add

7

☐ Module is Portable 8 Default Path 9

☒ Module can analyze specific file format 10

Sample Path 11 Add

Target Extender 12 pcap

Target Signature 13 D4C3

[Optional]

Download Link 14

Help Ok Cancel

# Module Launcher(Module Config window)




1. Module Path : Executable file path of the module
2. Module Name : Module name
3. Description : Module description
4. Executable Type(GUI / CLI / Python)
5. Platform (Windows / Mac OS X / Linux)
6. Argument Input : CLI Module Argument
7. Argument List : CLI Module Argument List
8. Module is Portable : Check, if module is portable
9. Default Path : if module need to be installed, set this field by executable path
10. Module can analyze specific file format
11. Sample Path : Analysis target sample file path
12. Target Extender : Analysis target files' extenders
13. Target Signature : Analysis target files' signature(first 2 byte)
14. Download Link(Optional) : File Link in world wide web



# Module Launcher(Button)



⑤ ⑥

- 5. Delete module
  - Delete checked module into recycle(  )
- 6. Recover deleted module
  - Button is enabled when you click recycle button in toolbar
  - If you want recover some deleted module, then check module for recover and relick recycle button.

# Module Launcher(Button)



⑦ ⑧


- 7. Export module into PFP-Archive(.pfparc)
  - Make .pfparc and insert into module checked
  - .pfparc is made into PFP root folder
- 8. Import Module from PFP-Archive(.pfparc)
  - Select .pfparc
    - ➔ Select module in pfparc what you want to import into your Platform
    - ➔ And relick the Button ⑧

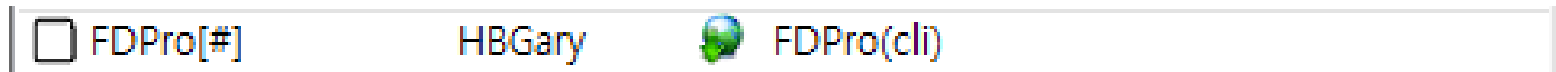
# Module Launcher(Button)



⑨

⑩

- 9. Module Download
  - Download checked module. If it is not downloaded
  - Check icon(  )



- 10 . Status of Module launcher



- Comment
  - You can use system command and binary in the commoncli folder in your PFP by this emulator (not perfect. but sometimes it is useful)

```
%PFP%\UserModule\CommonCLI>ipconfig

Windows IP 구성

이더넷 어댑터 로컬 영역 연결:

    연결별 DNS 접미사. . . :
    링크-로컬 IPv6 주소 . . . : fe80::c01a:7a4e:88c5:6f33%11
    IPv4 주소 . . . . . : 111.2.0.184
    서브넷 마스크 . . . . . : 255.255.255.0
    기본 게이트웨이 . . . . . : 111.2.0.1

이더넷 어댑터 VMware Network Adapter VMnet1:

    연결별 DNS 접미사. . . :
    링크-로컬 IPv6 주소 . . . : fe80::a4b0:408d:545a:4763%13
    IPv4 주소 . . . . . : 192.168.91.1
    서브넷 마스크 . . . . . : 255.255.255.0
    기본 게이트웨이 . . . . . :

이더넷 어댑터 VMware Network Adapter VMnet8:

    연결별 DNS 접미사. . . :
    링크-로컬 IPv6 주소 . . . : fe80::809f:90db:ea4a:328%15
    IPv4 주소 . . . . . : 192.168.237.1
    서브넷 마스크 . . . . . : 255.255.255.0
    기본 게이트웨이 . . . . . :

터널 어댑터 isatap.{50EE7BC3-7EF0-4ACC-8EAF-D1FEB7DD7272}:

    미디어 상태 . . . . . : 미디어 연결 끊김
    연결별 DNS 접미사. . . :

터널 어댑터 6TO4 Adapter:

    연결별 DNS 접미사. . . :
    IPv6 주소 . . . . . : 2002:6f02:b8::6f02:b8
    기본 게이트웨이 . . . . . :

터널 어댑터 Teredo Tunneling Pseudo-Interface:

    미디어 상태 . . . . . : 미디어 연결 끊김
    연결별 DNS 접미사. . . :

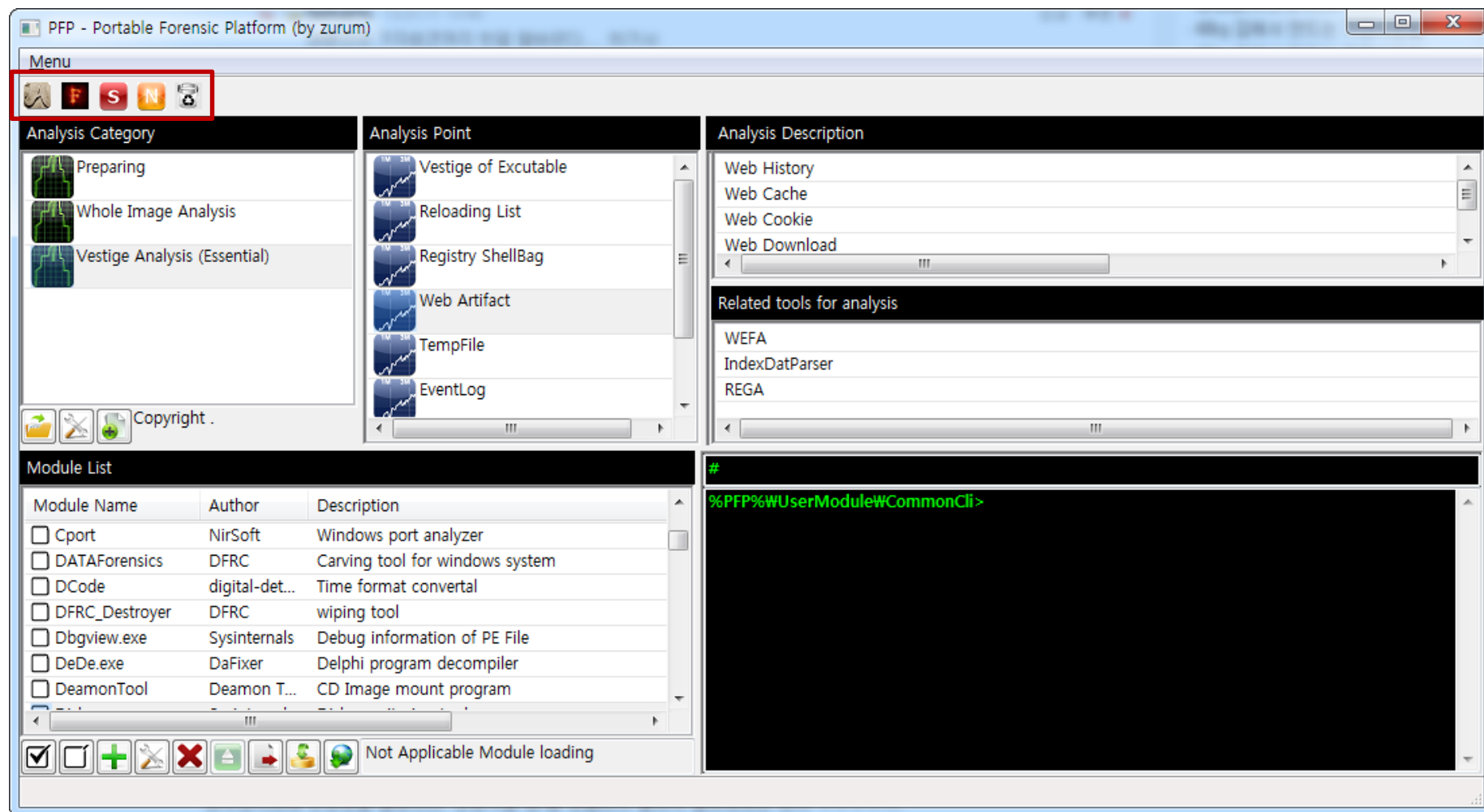
터널 어댑터 isatap.{1EF20580-C4B6-4C4F-A912-84F5FDF78C23}:

    미디어 상태 . . . . . : 미디어 연결 끊김
    연결별 DNS 접미사. . . :

%PFP%\UserModule\CommonCLI>
```



# Toolbar and accelerator

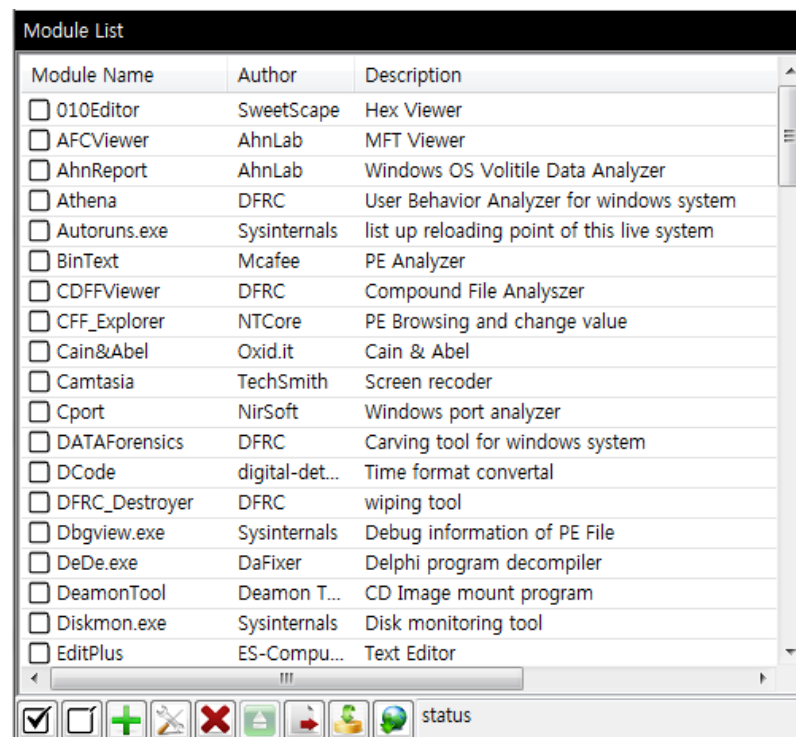


# Toolbar and accelerator



①

- 1. All Module (Ctrl + A)
  - Show all module in your platform

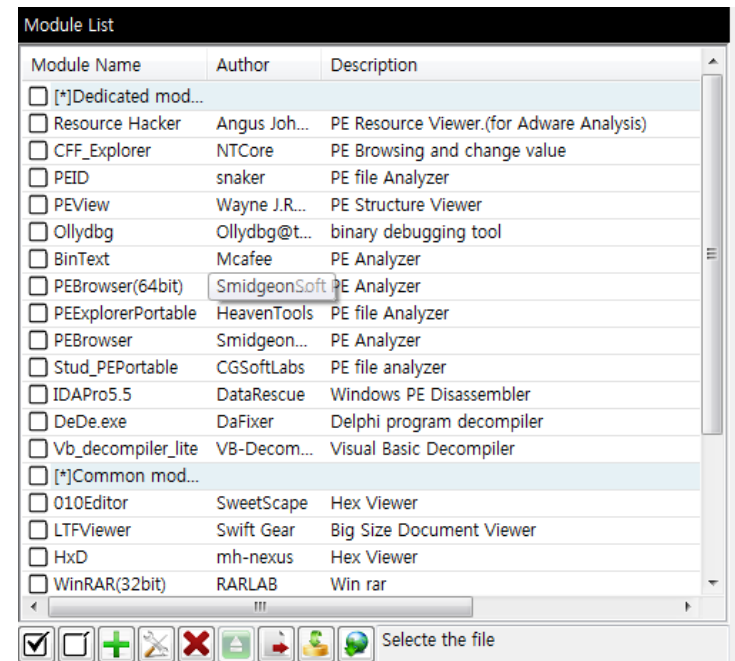
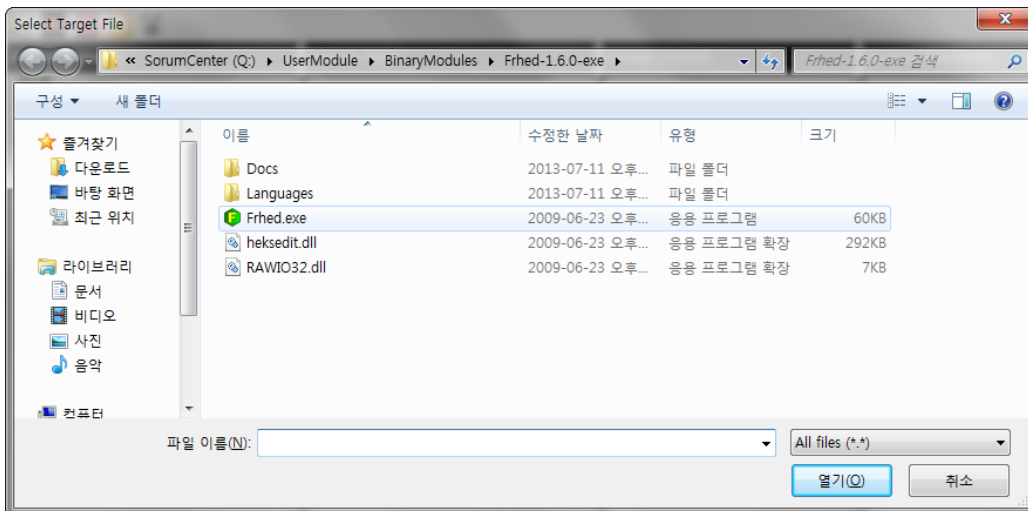


# Toolbar and accelerator



②




- 2. Select File (Ctrl + F)
  - Select file and show related module about selected file





③

- 3. Unit Module (Ctrl + S)
  - Now preparing...

| Module Name  | Author     | Description |
|--|------------|-------------|
|  [Unit] CSVtoSQLite | by Zurum   |             |
|  [Unit] Sample      | by Author  |             |
|  [Unit] Sample2     | by Author2 |             |

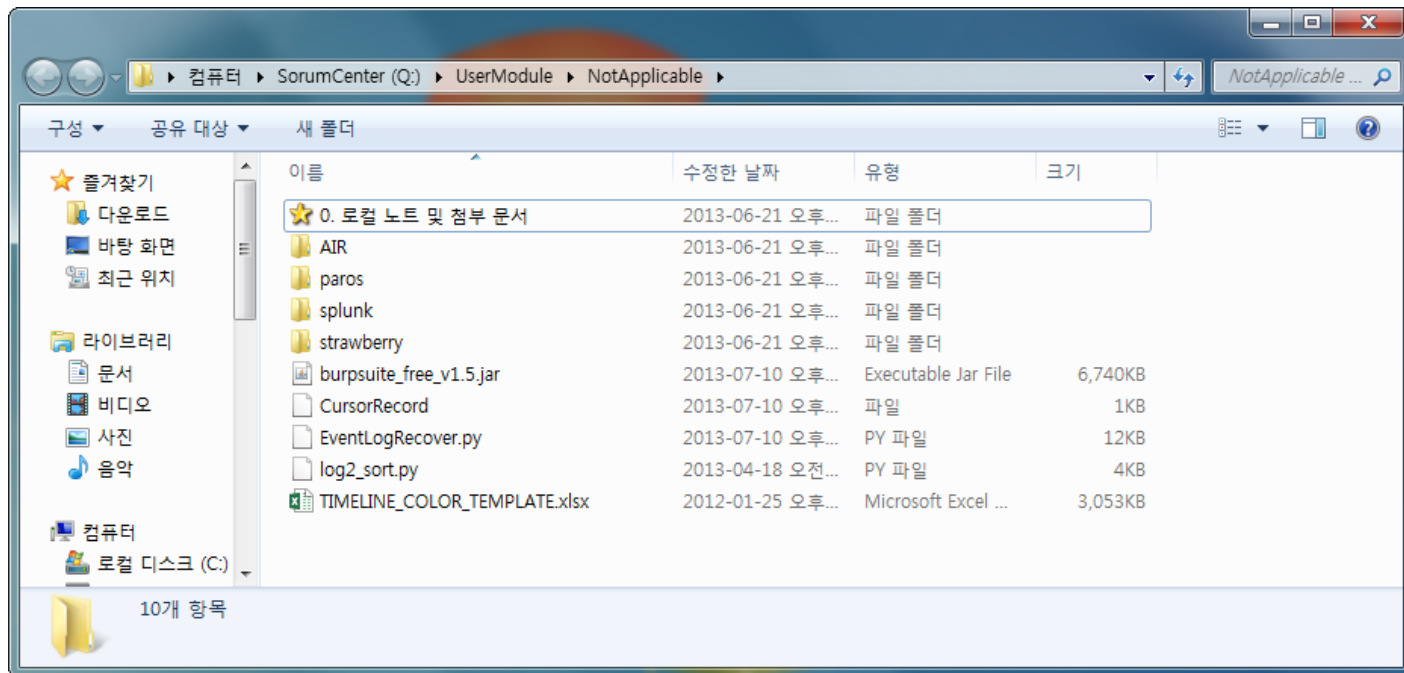


# Toolbar and accelerator



4

- 4. Not Applicable (Ctrl + N)
  - Open folder : %PFPROOT%\UserModule\NotApplicable\

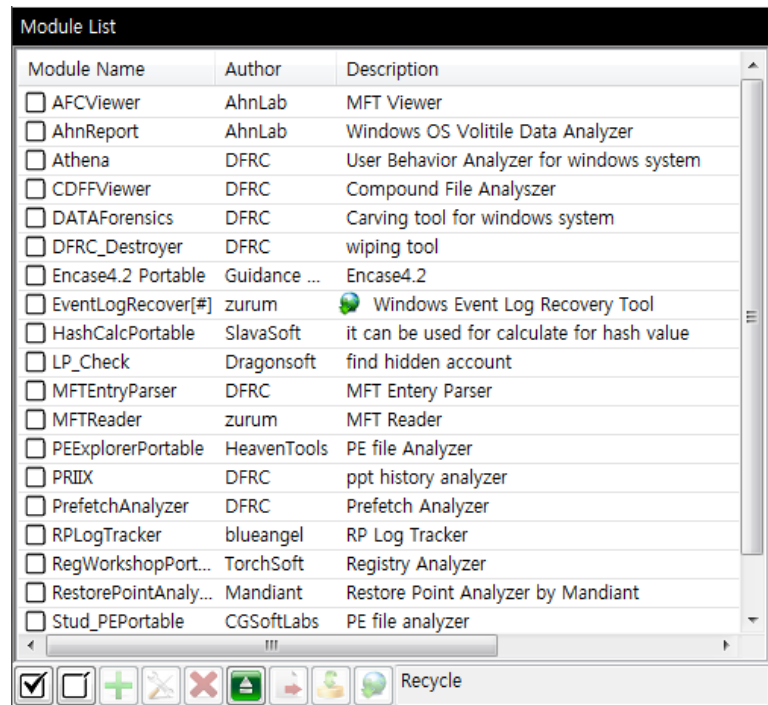


# Toolbar and accelerator



5

- 5. Recycle
  - Show deleted modules and recovery button is enabled





Just replace PFPModule folder of latest version of PFP!!!



- 구현상 예외처리 및 오류수정
- 1.5.0 or 2.0.0
  - Script editor and launcher
  - Cli module(exe, script)의 Module launcher 연동
  - 전용모듈 및 단위모듈 제작, 추가



- Project
  - <http://code.google.com/p/portable-forensic-platform/>

