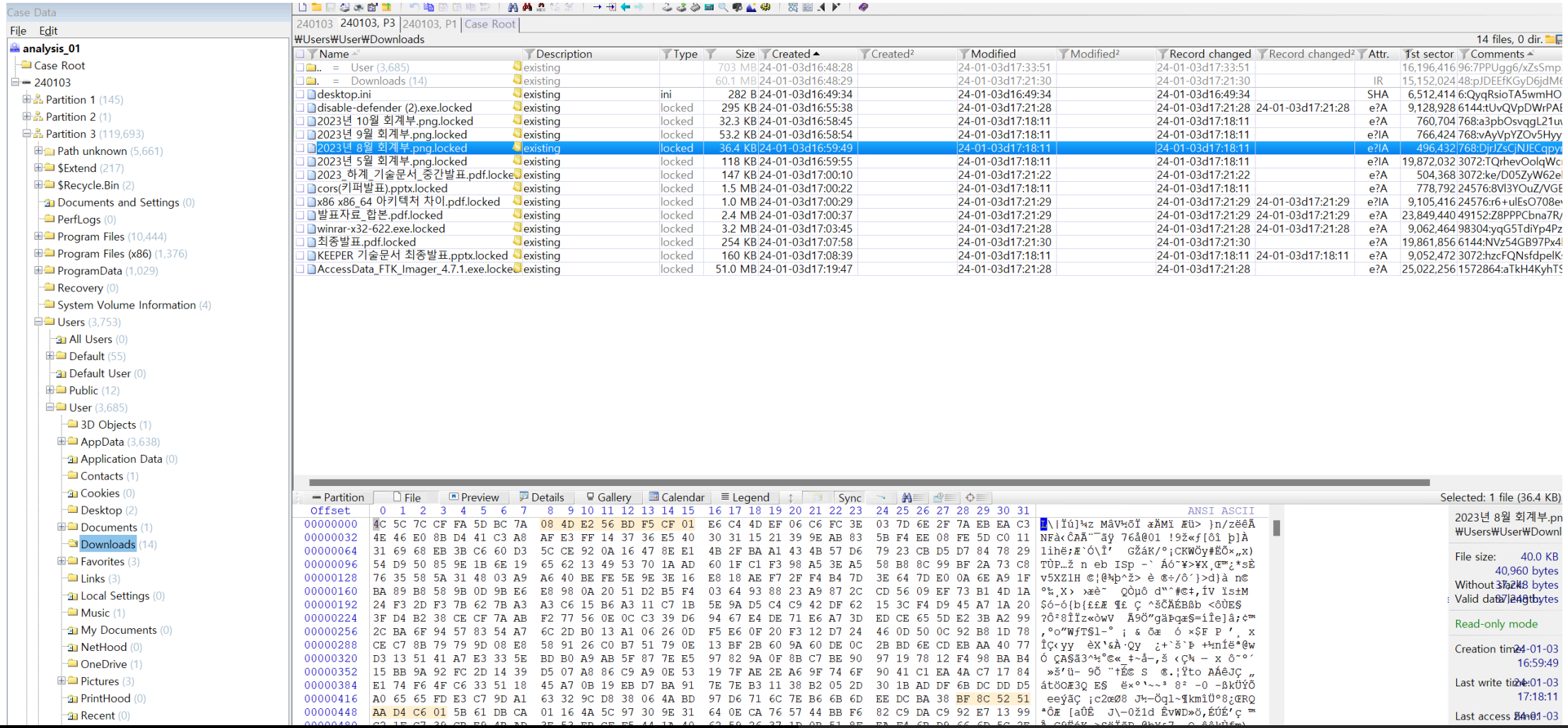
X-Tensions

X-Ways Forensics

- 포렌식에서 자주 사용되는 통합 도구, 타 도구에 비해 적은 리소스 사용 → 그러나 다양한 기능 존재



X-Ways Forensics

 # 통합 포렌식 도구

통합이라고 제목은 붙였지만 보통의 분석 대상이 이미지 파일이기 때문에 이미지 파일을 해석하고 파일시스템 구조를 확인할 수 있는 도구를 메인으로 사용한다. 이런 도구는 파일시스템 뿐만아니라 주요 아티팩트의 해석 기능도 지원한다. 오픈소스인 TSK (The Sleuth Kit) 기반의 Autopsy도 있지만 안정성이 떨어져 원활한 분석을 하려면 상용 도구를 사용하자.

Tool	Description
X-Ways Forensics (WinHex)	파일시스템의 상세한 구조까지 모두 직접 확인가능하고 필터링과 검색 기능이 뛰어나며 무엇보다도 가볍다. 파일시스템 해석 기능만 필요하다면 WinHex 제품으로도 충분하다.
Magnet AXIOM	아티팩트 분석 기능과 레코드 복구 기능이 탁월한 도구로 파일시스템에 대한 이해 없이도 쉽게 사용 흔적을 확인할 수 있다. 하지만, 아티팩트 구조와 해석 방법에 대한 정확한 이해가 있어야 정확한 판단이 가능하다.

In A Nutshell

X-Ways Forensics, the forensic edition of WinHex, is a powerful and affordable integrated computer forensics environment with numerous forensic features, rendering it a powerful disk analysis tool: capturing free space, slack space, inter-partition space, and text, creating a fully detailed drive contents table with all existing and deleted files and directories and even alternate data streams (NTFS), Bates-numbering files, and more. Picture gallery, file preview, calendar/timeline display. Also serves as a low-level disk imaging and cloning tool that creates true mirrors (including all slack space) and reads most drive formats and media types, and supports drives and files of virtually unlimited size (even terabytes on NTFS volumes!).

X-Ways Forensics and WinHex can natively interpret and show the directory structure on FAT, NTFS, Ext2/3, Reiser, CDFS, and UDF media and image files. It performs safe recoveries on hard disks, memory card, flash disks, floppy disks, ZIP, JAZ, CDs, DVDs, and more. It incorporates several automated file recovery mechanisms and allows to conveniently recover data manually. WinHex provides sophisticated, flexible and lightning-fast simultaneous search functions that you may use to scan entire media (or image files), including slack, for deleted files, hidden data and more. Via physical access, this can be accomplished even if a volume is undetectable by the operating system e.g. due to an unknown or a corrupt file system.

[1] https://blog.plainbit.co.kr/dforensics-specialist-tools/

[2] https://www.x-ways.net/winhex/forensics.html

X-Ways Forensics

X-Ways Forensics comprises all the general and specialist features known from WinHex, such as...

- Disk cloning and imaging
- Ability to read partitioning and file system structures inside raw (.dd) image files, ISO, VHD, VHDX, VDI, and VMDK images
- Complete access to disks, RAIDs, and images more than 2 TB in size (more than 2^{32} sectors) with sector sizes up to 8 KB
- Built-in interpretation of JBOD, RAID 0, RAID 5, RAID 5EE, and RAID 6 systems, Linux software RAIDs, Windows dynamic disks, and LVM2
- Automatic identification of lost/deleted partitions
- Native support for FAT12, FAT16, FAT32, exFAT, TFAT, NTFS, Ext2, Ext3, Ext4, CDFS/ISO9660/Joliet, UDF
- Superimposition of sectors, e.g. with corrected partition tables or file system data structures to parse file systems completely despite data corruption, without altering the original disk or image
- Access to logical memory of running processes
- Various data recovery techniques, lightning fast and powerful file carving
- Well maintained file header signature database based on GREP notation
- Data interpreter, knowing 20 variable types
- Viewing and editing binary data structures using templates
- Hard disk cleansing to produce forensically sterile media
- Gathering slack space, free space, inter-partition space, and generic text from drives and images
- File and directory catalog creation for all computer media
- Easy detection of and access to NTFS alternate data streams (ADS)
- Mass hash calculation for files (Adler32, CRC32, MD4, ed2k, MD5, SHA-1, SHA-256, RipeMD-128, RipeMD-160, Tiger-128, Tiger-16, Tiger-192, TigerTree, ...)
- Lightning fast powerful physical and logical search capabilities for many search terms at the same time
- Recursive view of all existing and deleted files in all subdirectories
- Automatic coloring for the structure of FILE records in NTFS
- Bookmarks/annotations
- Runs under Windows FE, the forensically sound bootable Windows environment, e.g. for triage/preview, with limitations
- Support for high DPI settings in Windows
- Ability to analyze remote computers in conjunction with F-Response
- ...

$^1% https://www.x-ways.net/forensics/index-m.html

X-Tensions

X-Ways Forensics에서 플러그인으로 확장할 수 있게 제공하는 API[1]

Among other things, X-Tensions allow you to:

- read from a disk/partition/volume/image
- retrieve abundant information about each file and directory in the volume snapshot
- read from any file
- add new objects to the volume snapshot, e.g. attach results of translations, decryption, decoding etc.
- bookmark/classify/categorize files by assigning them to report tables
- add free text comments to files
- run searches
- process, validate and delete search hits
- create and fill evidence file containers
- add events to the event list
- retrieve information about evidence objects
- add evidence objects to the currently loaded case
- and do practically *everything else that is possible with a Windows program*! (thanks to the Windows API)

C++ function definitions and sample projects (updated Apr 2021)
Delphi function definitions and 5 sample projects (updated May 2023)
Project in C with source code
32-bit demo, 64-bit demo (updated June 2016)

Plug-in for Python 3.10 with sample scripts (64-bit, from Jan 2023)

[1] https://www.x-ways.net/forensics/x-tensions/api.html

플러그인 조사

X-Ways Forensics X-Tensions

- Exponent - MobileMedia (Youtube)
- xwf-yara-scanner
- a5hlynx - xt_fuzzy, xt_entropy
- PolitoInc - X-Ways-VirusTotal-Extension, X-Ways-Metadefender-extension (Youtube)
- Kuiper Forensics - XT_Image, XT_RAW
- 4Discovery - X-Ways BeyondCompare X-Tension
- ...

Exponent

- X-Ways Forensics 하나의 도구에서 모든 분석을 진행하자는 아이디어[1]
  - 종합 포렌식 도구는 불필요하게 많은 기능이 있고 그로 인해 **매우 무겁다**.
  - 윈도우와 모바일을 분석한다고 했을 때 특화된 도구들이 나눠져있기 때문에 분석 시간 또한 **2배**로 늘어난다.
    → 키워드를 검색한다고 했을 때 각각의 도구에서 검색을 진행해야 한다.
    - 모바일 분석: Magnet AXIOM, MD-NEXT 등
    - 윈도우 분석: X-Ways Forensics, Magnet AXIOM, EnCase 등
- X-Ways Forensics에서 모바일을 분석하는 기능을 추가해보자!
  - 예를 들어 이미지를 검색할 때 각각의 도구에서 검색하지 않고 X-Ways Forensics에서 확인하자.

Tool	Description
X-Ways Forensics (WinHex)	파일시스템의 상세한 구조까지 모두 직접 확인가능하고 필터링과 검색 기능이 뛰어나며 무엇보다도 가볍다. 파일시스템 해석 기능만 필요하다면 WinHex 제품으로도 충분하다.

[1] https://www.apiforensics.com/blogs/announcing-exponent-1-0.asp
[2] https://blog.plainbit.co.kr/dforensics-specialist-tools/

Exponent

Development Roadmap: What's In Store?

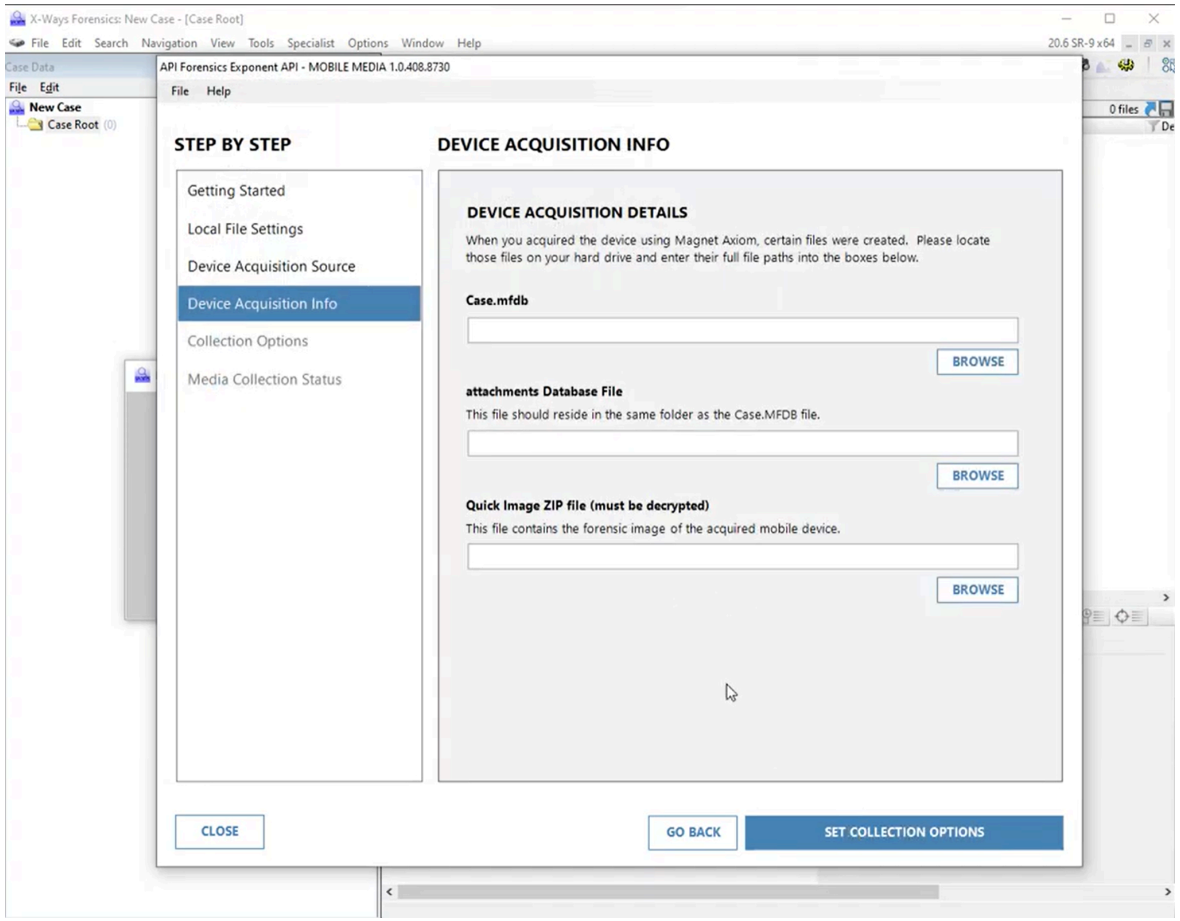
Exponent™ was created to be a continually evolving and expanding library that extends and simplifies the discovery and reporting capabilities of DFIR type investigations using X-Ways Forensics. New features that are currently under consideration or already under development include:

- Windows Artifacts
- SQLite Database
- Browser Artifacts
- Cyber Forensic Artifacts
- Cloud Artifacts (too many to list)

> *Exponent is all about extending the features, functionalities and capabilities of X-Ways Forensics so that forensic practitioners don't have to keep switching between different tools: one for desktop, one for mobile devices and a handful of other smaller niche tools. We know that examiners will always need to have more than one tool in their toolbox. It has long been a practice to have similar tools on-hand for purposes of validation and comparison of results.*

- 향후 계획을 보면 윈도우에서 활용되는 각각의 도구들도 통합할 예정인 것 같다.

Exponent - MobileMedia



- AXIOM의 분석 기능이 뛰어난 것은 부정할 수 없다.
  → AXIOM의 분석 결과를 X-Ways Forensics에서 활용할 수 있게 하자.

xwf-yara-scanner

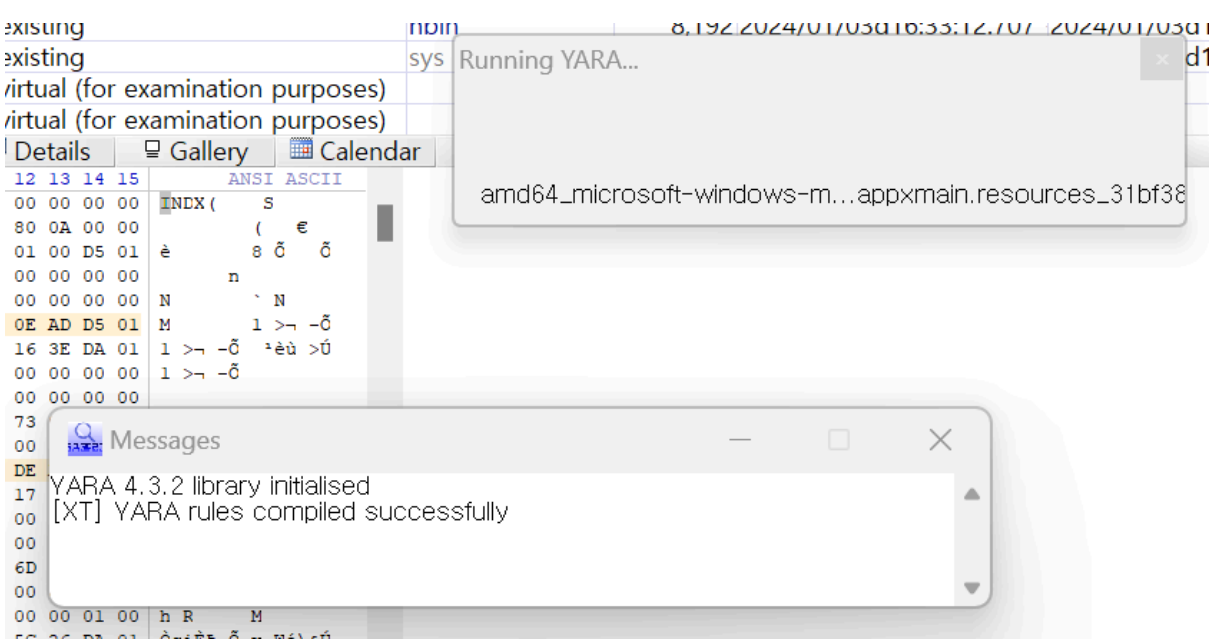
- CrowdStrike에서 Yara[1]를 X-Ways Forensics에서 사용하기 위해 만든 플러그인
- 디렉토리 브라우저에서 플러그인을 실행하면 Yara rule을 요구하며 rule에 매칭된 파일들을 보여준다.

```
rule png_test
{
  strings:
    $a = {89 50 4E 47} // PNG Header
  condition:
    $a at 0
}
```

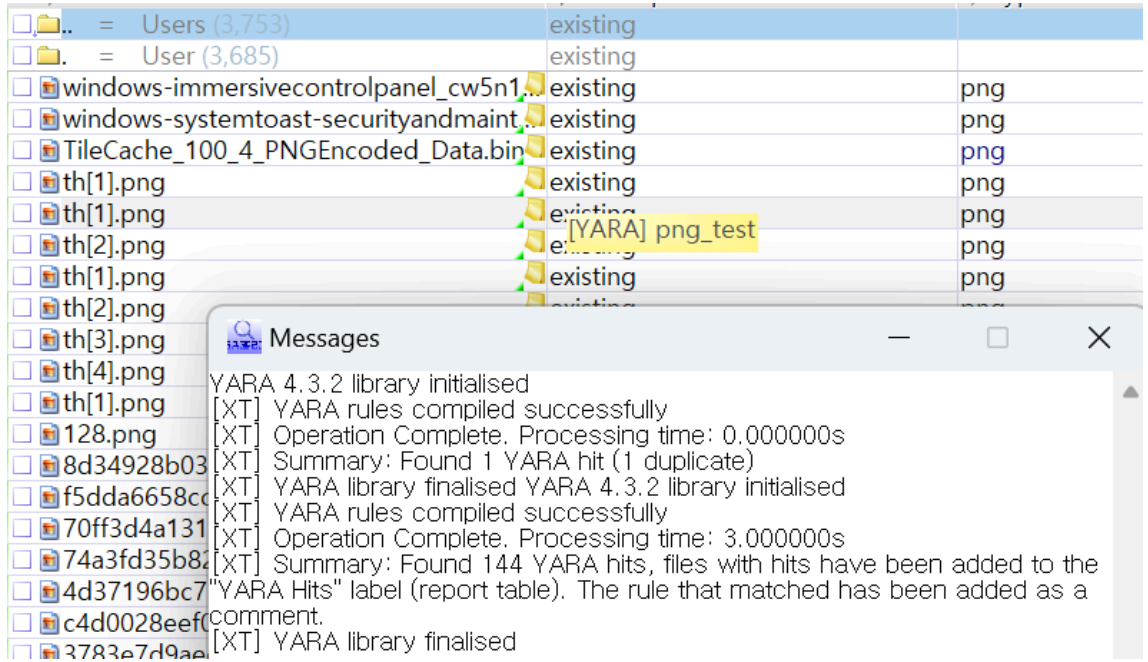
- PNG 시그니처로 테스트 진행

[1] Yara는 패턴 매칭 도구이다. 악성코드 유사도 분석에서 많이 활용되며, 분석 보고서에서 yara rule을 공유하는 것을 볼 수 있다. Virustotal Intelligence에서 yara rule을 사용하여 악성코드를 탐지한다.

xwf-yara-scanner



플러그인 실행 중



플러그인 실행 결과

- X-Ways Forensics에서 이미지(ex: E01) 파일을 올린 후에 플러그인을 사용하면 흐름이 깨지지 않고 분석에 도움을 줄 것 같다. (일반적인 경우에는 이미지 파일을 마운트한 후 터미널 창을 띄우고 yara를 실행해야 하며, 추출할 때도 탐지 결과를 번갈아 가면서 봐야 한다.)

xwf-yara-scanner

```
/* https://virustotal.github.io/yara/ */
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        threat_level = 3
        in_the_wild = true

    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"

    condition:
        $a or $b or $c
}
```

- 악성코드의 특징들을 rule로 만들어서 사용한다.

xt_fuzzy, xt_entropy

- xt_fuzzy: 퍼지 해시를 계산해주는 플러그인 (`Comments` - 계산 결과)
  - 파일명은 다르지만 유사한 기능을 하는 악성코드들을 찾을 때 활용할 수 있다.

240103, P3

₩Users₩User₩AppData₩Local₩Temp 32+4=36 files, 21+1=22 dir.

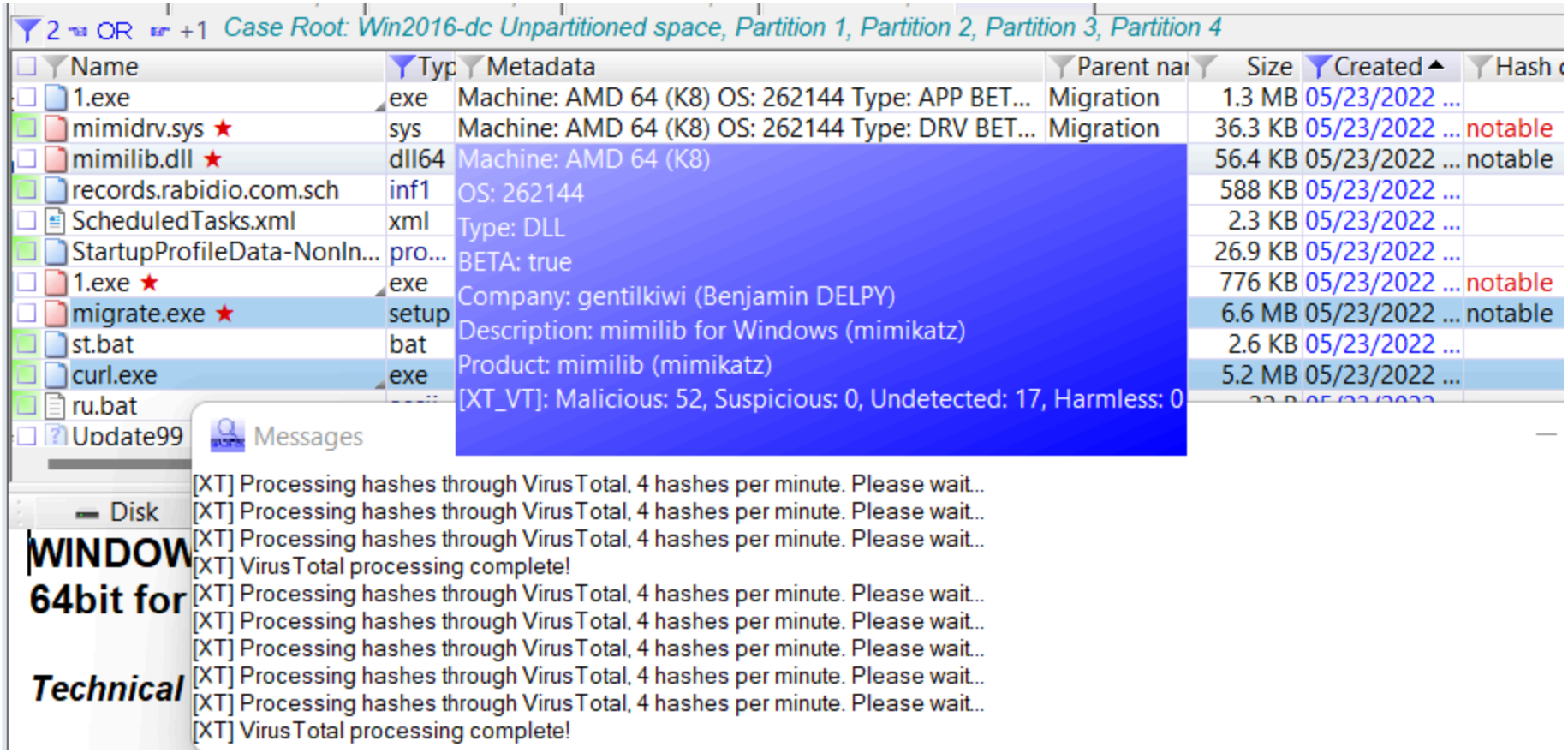
Name	Description	Type	Size	Created	Modified	Record changed	Attr.	1st sector	Comments
.. = Local (3,523)	existing		664,270,...	2024/01/03d16:48:29.085	2024/01/03d16:49:53.257	2024/01/03d16:49:53.257		3,830,128	48:pJRl9Ui1hWUiYlu7Czft3jtZjFJoZ74Z+pzfvYzIXhPo0l:1Ym1Y53JMH
. = Temp (172)	existing		129,159,...	2024/01/03d16:48:29.085	2024/01/03d17:35:27.793	2024/01/03d17:35:27.793		15,153,992	192:MonQzHU9AXA9A+AbAVAXphlaLBULpOLp0wLpx08Lp9TYzcl/Tgd...
gviBFQRfUYKg.exe	existing	exe	212,480	2024/01/03d17:21:14.590	2024/01/03d17:21:14.621	2024/01/03d17:21:14.621	A	851,688	3072:gM+lmsolAIrRuw+mqv9j1MWLQmMTmmsolNIrRuw+mqv9j1MWLQ...
pOcZproCkop9.exe	existing	exe	212,480	2024/01/03d17:11:14.526	2024/01/03d17:11:14.573	2024/01/03d17:11:14.573	A	85,504	3072:mM+lmsolAIrRuw+mqv9j1MWLQeMTmmsolNIrRuw+mqv9j1MWL...
dd_vcredist_amd64_202...	existing	log	134,848	2024/01/03d16:53:16.203	2024/01/03d16:53:17.328	2024/01/03d16:53:17.328	A	8,906,992	3072:nAmjA9d66666HHHHHHHHPQYB3pMJVPx39cL51:5j
dd_vcredist_x86_20240...	existing	log	139,772	2024/01/03d16:53:13.531	2024/01/03d16:53:13.985	2024/01/03d16:53:13.985	A	19,916,872	3072:qe5jzGfffffffffOOOO/I/6NhWdnneQ3p8rRS:Vj
0lAjDNgXOrFO.exe	existing	exe	212,480	2024/01/03d17:18:07.214	2024/01/03d17:18:07.245	2024/01/03d17:18:07.245	A	3,519,824	3072:yM+lmsolAIrRuw+mqv9j1MWLQWMTmmsolNIrRuw+mqv9j1MWLQ...
LqozVnjzOVrN.exe	existing	exe	212,480	2024/01/03d17:15:38.863	2024/01/03d17:15:38.879	2024/01/03d17:15:38.879	A	23,759,480	3072:yM+lmsolAIrRuw+mqv9j1MWLQWMTmmsolNIrRuw+mqv9j1MWLQ...
ifi2UtAXWPKT.exe	existing	exe	212,480	2024/01/03d17:12:15.171	2024/01/03d17:12:15.202	2024/01/03d17:12:15.202	A	23,906,152	3072:yM+lmsolAIrRuw+mqv9j1MWLQrMTmmsolNIrRuw+mqv9j1MWLQA...

- xt_entropy: 엔트로피를 계산해주는 플러그인 (`Comments` - 계산 결과)
  - 암호화, 난독화된 파일들을 찾을 때 활용할 수 있다. (엔트로피 값이 비정상적으로 높다.)

Name	Description	Type	Size	Created	Modified	Record changed	Attr.	1st sector	Comments
.. = Users (3,753)	existing		738,875,...	2019/12/07d18:03:44.539	2024/01/03d17:10:05.399	2024/01/03d17:10:05.399	R	20,280,920	1.4087179161253904
. = User (3,685)	existing		737,307,...	2024/01/03d16:48:28.960	2024/01/03d17:33:51.486	2024/01/03d17:33:51.486		16,196,416	3.7727379599675990
AccessData_FTK_Imager_4.7.1.exe.locked	existing	locked	53,465,4...	2024/01/03d17:19:47.399	2024/01/03d17:21:28.407	2024/01/03d17:21:28.407	e?A	25,022,256	7.9999951487529559
발표자료_합본.pdf.locked	existing	locked	2,500,896	2024/01/03d17:00:37.443	2024/01/03d17:21:29.860	2024/01/03d17:21:29.876	e?A	23,849,440	7.9998617554202429
winrar-x32-622.exe.locked	existing	locked	3,306,976	2024/01/03d17:03:45.197	2024/01/03d17:21:28.986	2024/01/03d17:21:28.989	e?A	9,062,464	7.9998289590919338
tmpE8D0.tmp	existing	cab1	27,107,4...	2024/01/03d16:52:18.646	2024/01/03d16:52:18.852	2024/01/03d16:52:18.852	TA	16,196,120	7.9998260606824605
tmp91A.tmp	existing	cab1	27,107,4...	2024/01/03d16:52:26.915	2024/01/03d16:52:27.106	2024/01/03d16:52:27.106	TA	19,647,520	7.9998260606824605
x86 x86_64 아키텍처 차이.pdf.locked	existing	locked	1,092,576	2024/01/03d17:00:29.742	2024/01/03d17:21:29.318	2024/01/03d17:21:29.321	e?IA	9,105,416	7.9996514316569609
cors(키퍼발표).pptx.locked	existing	locked	1,529,408	2024/01/03d17:00:22.217	2024/01/03d17:18:11.400	2024/01/03d17:18:11.400	e?A	778,792	7.9994416388741163

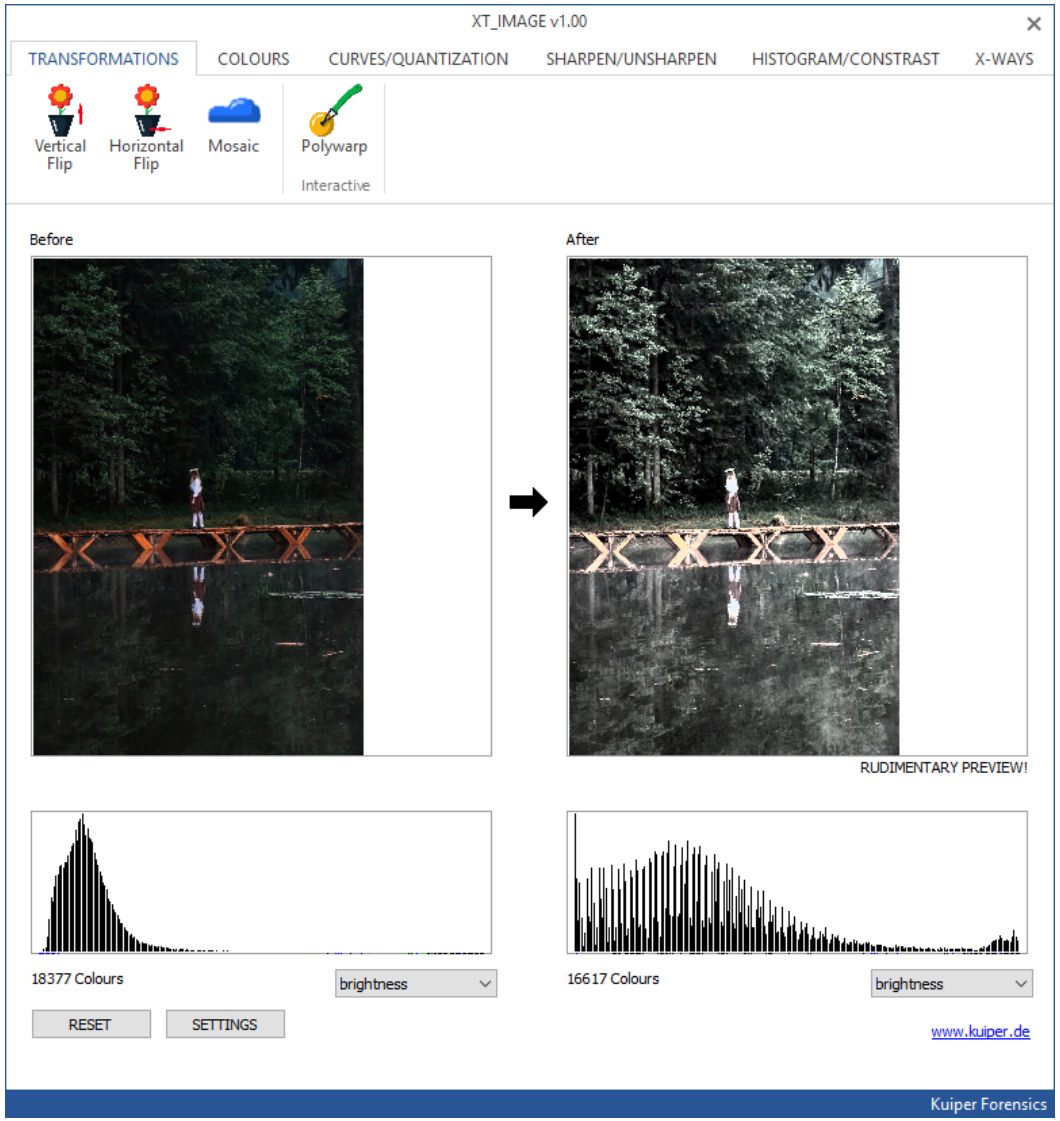
X-Ways-VirusTotal-Extension

- 이미지 파일에 존재하는 파일들을 Virustotal에 요청하여 악성 파일인지 알려주는 플러그인

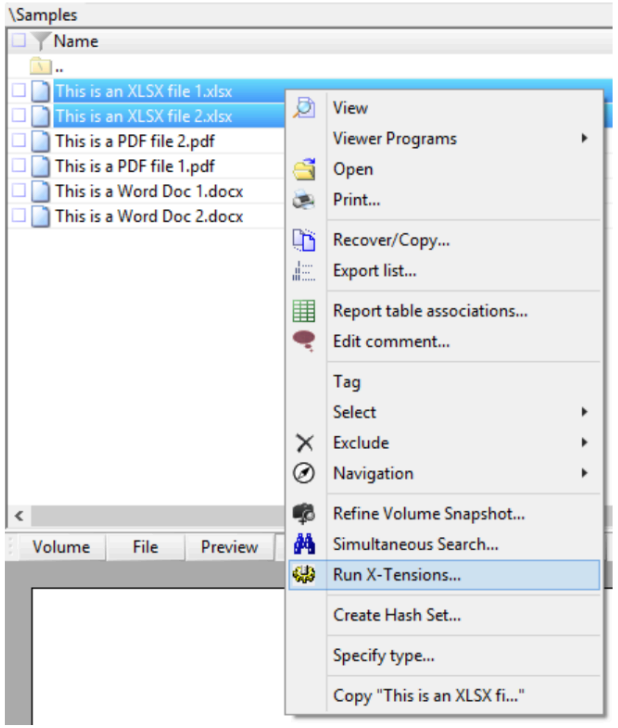


[1] https://www.politoinc.com/post/enhancing-digital-forensics-with-x-ways-x-tensions-virustotal-plugin

XT_Image

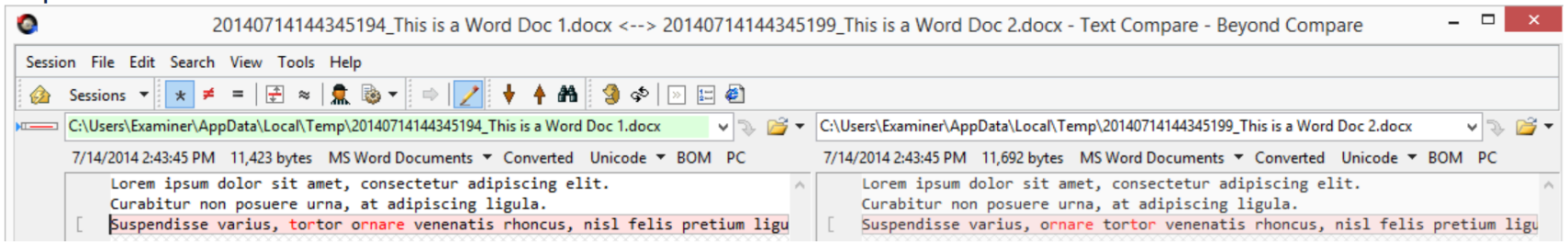

XT_IMAGE v1.00
TRANSFORMATIONS
COLOURS
CURVES/QUANTIZATION
SHARPEN/UNSHARPEN
HISTOGRAM/CONSTRAST
X-WAYS
Vertical Flip
Horizontal Flip
Mosaic
Polywarp
Interactive
Before
After
RUDIMENTARY PREVIEW!
18377 Colours
brightness
16617 Colours
brightness
RESET
SETTINGS
www.kuiper.de
Kuiper Forensics

X-Ways BeyondCompare X-Tension



Samples

Comparison of 2 Word Documents



API 공부

X-Ways Forensics X-Tensions API Documentation

X-Ways Forensics Image I/O API Documentation

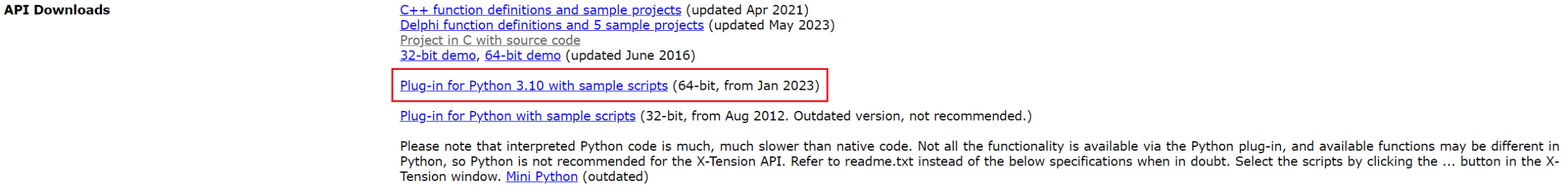
XT_* functions that you may export

XWF_* functions that you may call

- TED SMITH
  - Introduction to X-Tensions for X-Ways Forensics for Beginners
  - New Export Options and XWF_OpenItem Additional Flags for X-Ways Forensics

X-Tension - Python 사용하기

- 최근에 Python 3을 지원하는 dll 파일이 추가되었다.
  - `Python 2.7` → `Python 3.10` 지원 - 2023. 01



API Downloads

C++ function definitions and sample projects (updated Apr 2021)
Delphi function definitions and 5 sample projects (updated May 2023)
Project in C with source code
32-bit demo, 64-bit demo (updated June 2016)

Plug-in for Python 3.10 with sample scripts (64-bit, from Jan 2023)

Plug-in for Python with sample scripts (32-bit, from Aug 2012. Outdated version, not recommended.)

Please note that interpreted Python code is much, much slower than native code. Not all the functionality is available via the Python plug-in, and available functions may be different in Python, so Python is not recommended for the X-Tension API. Refer to readme.txt instead of the below specifications when in doubt. Select the scripts by clicking the ... button in the X-Tension window. Mini Python (outdated)

- 이전에는 C++, Pascal, Python 2.7 등을 사용해야 했다.

X-Tension - Python 사용하기

- 플러그인에서 사용하는 `PyQt5`, `PySide6` 등 라이브러리 사용 불가
- Python 사용에 문제가 있다. (잦은 버그와 팅김 현상 존재)

```
[XT] Failed to execute import Hyara_xways
[XT] Failed to execute Hyara_xways.XT_Init(2030, 1, 724626, 186136576)bad argument type for built-in operation
[XT] Failed to execute Hyara_xways.XT_Prepare(48786320, 49530336, 0, 0)
[XT] Failed to execute Hyara_xways.XT_Finalize(48786320, 49530336, 0, 0)bad argument type for built-in operation
[XT] Failed to execute Hyara_xways.XT_Done(0)
```

```
[XT] Running "About" functions for selected Python scripts:
[XT] Failed to execute Hyara_xways.XT_Prepare(48851856, 49595872, 0, 0)
[XT] Failed to execute Hyara_xways.XT_Finalize(48851856, 49595872, 0, 0)bad argument type for built-in operation
An exception of type 216 (page protection fault, high or unknown impact) occurred at offset 7FFFFF7A5CE3. The problem was noted in the file "C:₩X-Ways_Forensics 20.3 SR-4₩error.log".
```

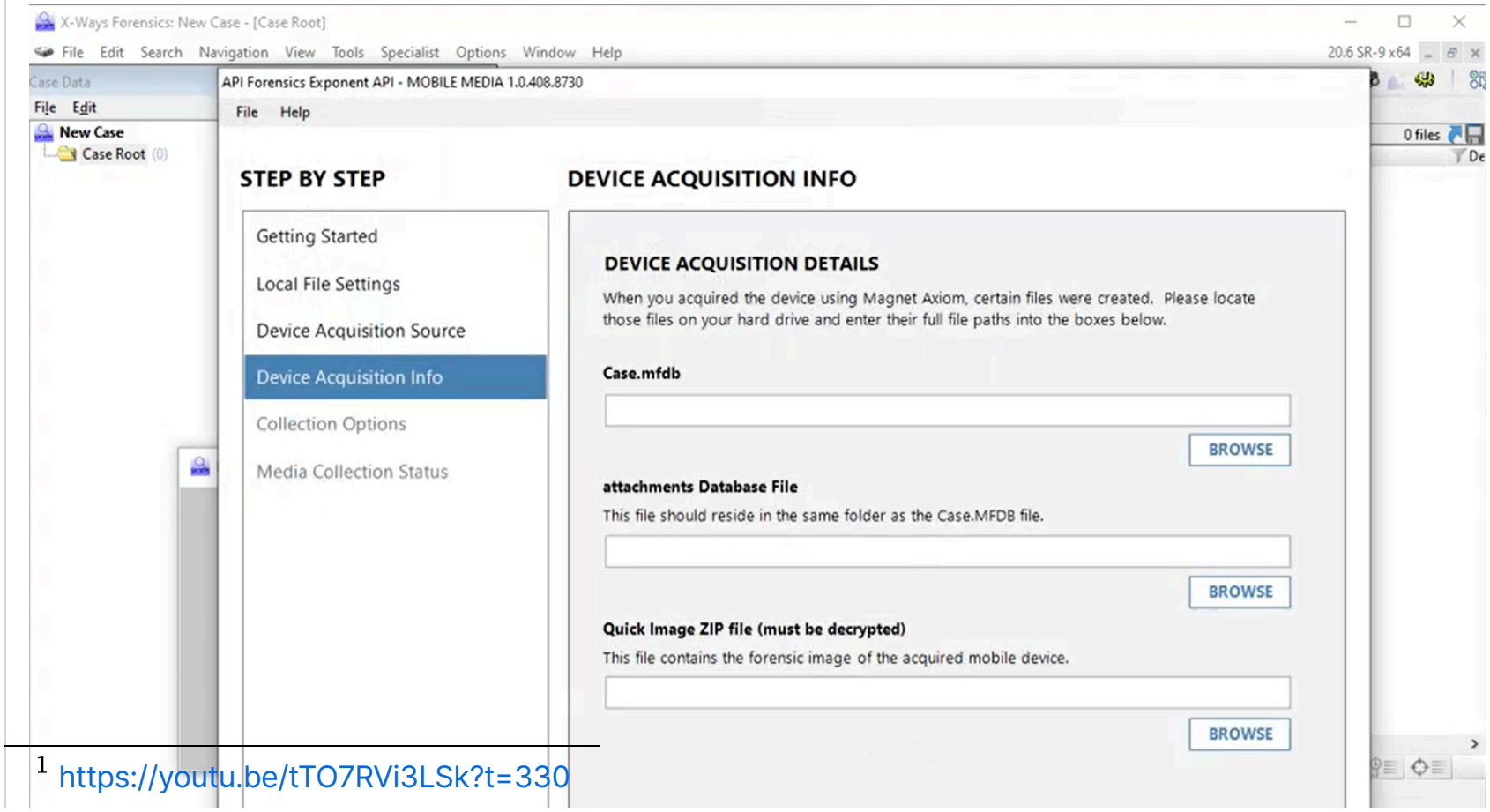
- **결론: 아직 Python 지원이 매우 미흡하다.** → 메인으로 지원하는 `C++`, `Pascal`을 사용해야 한다.

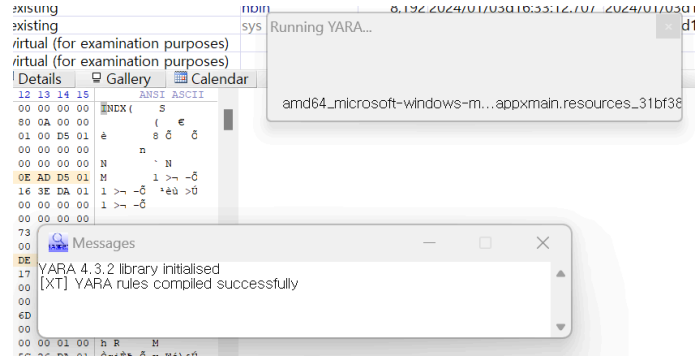
C++ function definitions and sample projects (updated Apr 2021)
Delphi function definitions and 5 sample projects (updated May 2023)

- GUI로 개발한 X-Tension 플러그인이 거의 없었지만 어떻게 만들었는지 알아봤다.

GUI 플러그인 분석

- X-Tension 플러그인으로 제작된 GUI 도구들 정리
  - API Forensics[1]: WinForm을 사용하는 것으로 보인다.

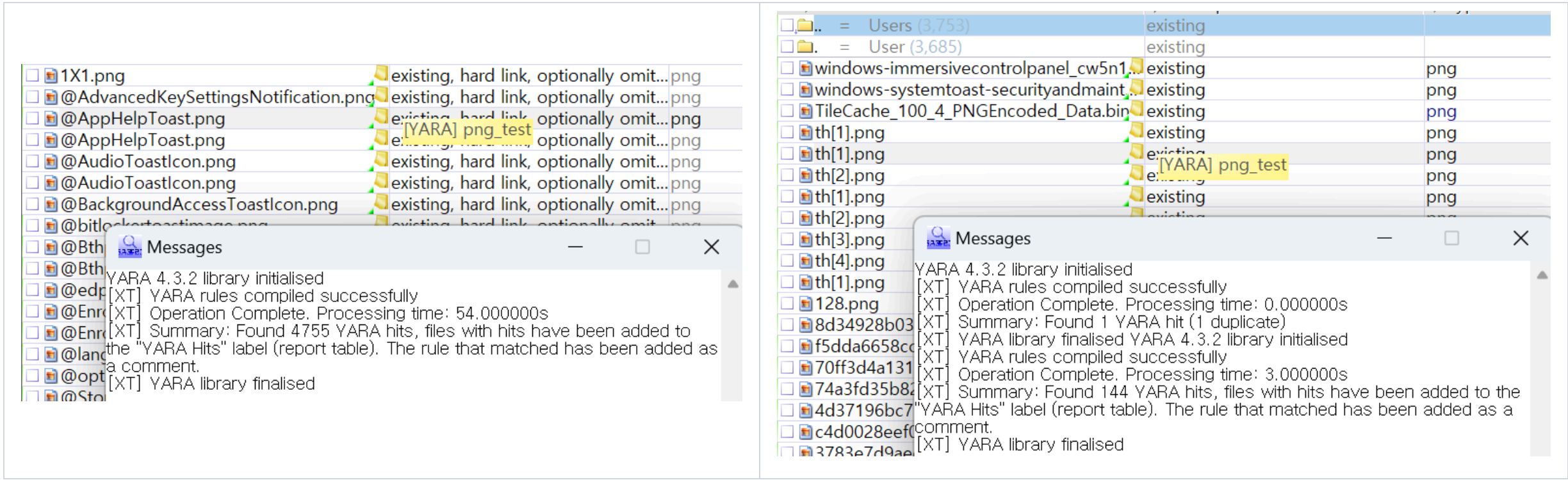




[1] https://youtu.be/tTO7RVi3LSk?t=330

GUI 플러그인 분석

- X-Tension 플러그인으로 제작된 GUI 도구들 정리
  - Kruiper[1]: C++ MFC를 사용하는 것으로 보인다. (`CString` , `CWnd` 등 함수 사용 확인)



[1] https://youtu.be/tTO7RVi3LSk?t=330

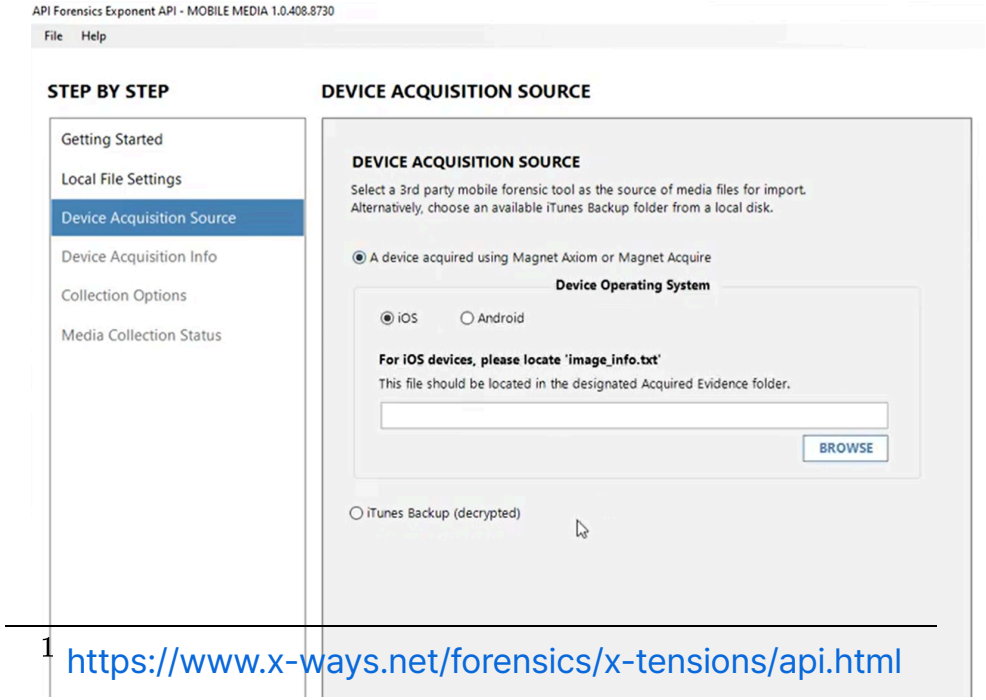
MFC? WinForm? Pascal?

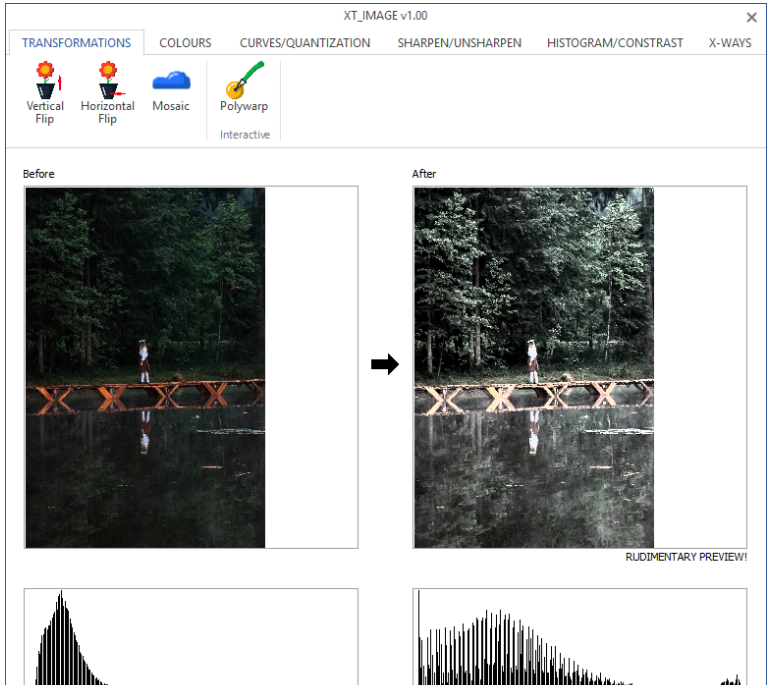
- Windows API를 통해 거의 모든 프로그램을 만들 수 있다는 것은 맞는 말이다.[1]

```
[XT] Running "About" functions for selected Python scripts:
[XT] Failed to execute Hyara_xways.XT_Prepare(48851856, 49595872, 0, 0)
[XT] Failed to execute Hyara_xways.XT_Finalize(48851856, 49595872, 0, 0)bad argument type for built-in operation
An exception of type 216 (page protection fault, high or unknown impact) occurred at offset 7FFFFF7A5CE3. The problem was noted in the file "C:₩X-Ways_Forensics 20.3 SR-4₩error.log".
```

  - 그러나 언어 지원 미흡으로 인해 진입 장벽을 높게 만든다.

    → Python은 버그가 많고 C++을 사용해야 하며, GUI를 구현하려면 MFC, WinForm 등을 사용해야 함





[1] https://www.x-ways.net/forensics/x-tensions/api.html

MFC? WinForm? Pascal?

To answer your question, X-Ways is written in C++ and our X-Tensions are written in C# with WinForms.

The C++ functions have to be ported to the language of choice used to develop the X-Tensions.

Everything you need is documented at the x-ways.net website.

Most of the other X-Tensions provide compact dialog windows (if any) to keep with the X-Ways Forensics interface.

Providing a GUI to the X-Tensions was important for us because it provides better interaction and visualization of the activities and feature configurations.

- 발표 이후에 이메일을 통해 물어본 결과, API Forensics에서는 C# winform으로 개발한다고 한다.
- GUI 도구를 개발하면 더 나은 기능과 시각화 등을 제공할 수 있다고 한다.
    - 지금까지 개발된 X-tension은 X-Ways 인터페이스, 대화창에 맞춰져 있다.