1.1 ~ 1.2 디지털 증거를 증거로 사용하기 위한 부분에 대해 서술하고 A씨의 디스크를 이미징 하시오.

1.1 디지털 증거가 증거로 사용되기 위한 조건

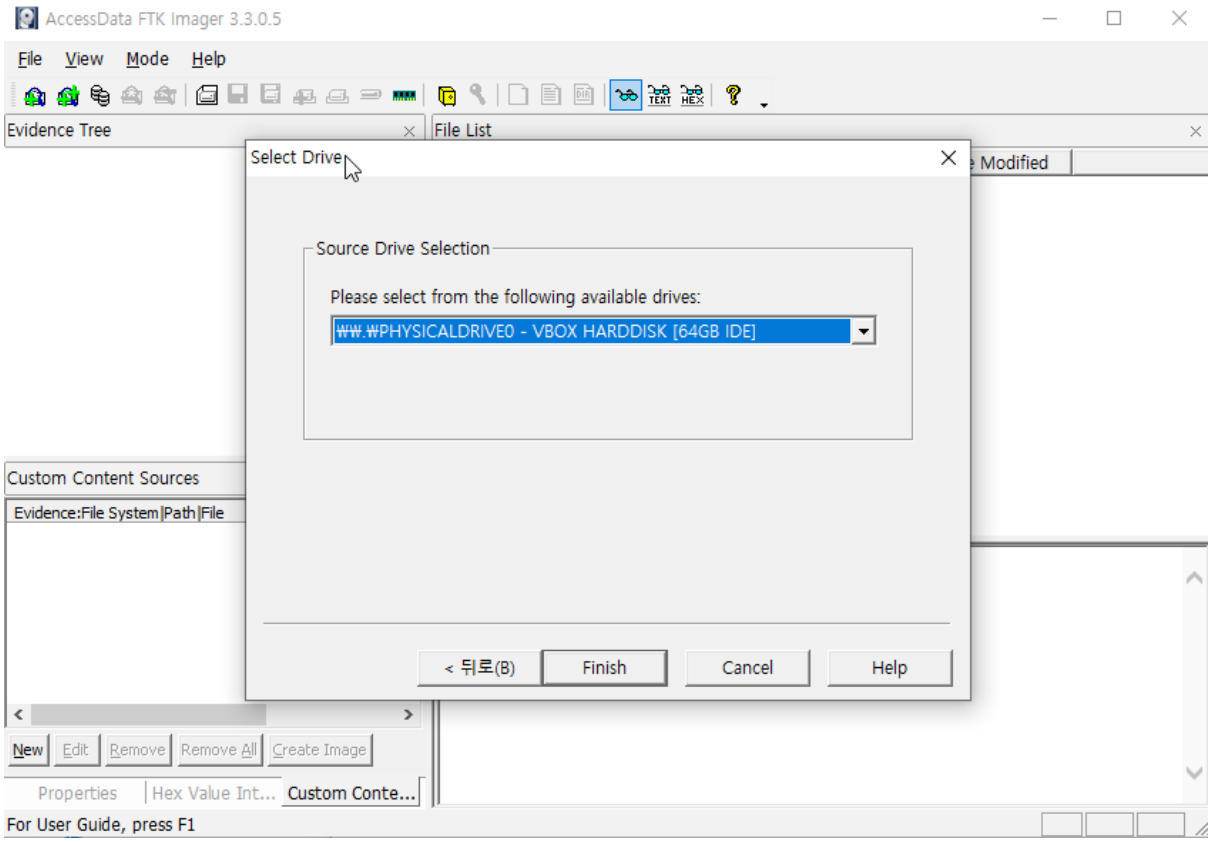
- 무결성을 확보한다.
디지털 증거는 위변조가 쉬운 특성을 가지므로, 최초 수집 시점부터 법정 제출까지 변경되지 않았음을 입증해야 한다. 이를 위해 해시값(SHA-256 등)을 비교하여 데이터의 동일성을 확인한다.

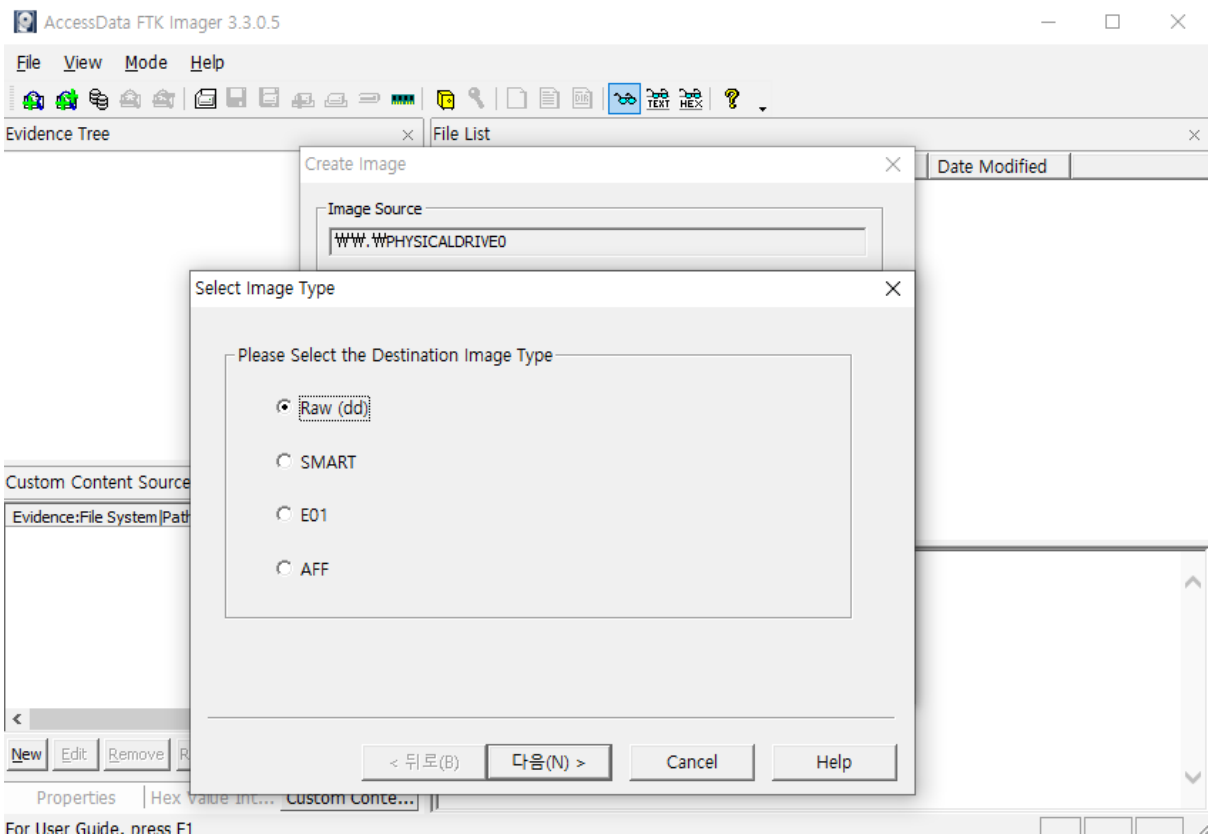
- 진정성을 보장한다.
디지털 증거가 특정한 사람에 의해 특정 시점에 생성되었음을 입증할 수 있어야 한다. 이를 위해 생성자, 생성 시점 등의 메타데이터를 확보하고, 수집부터 제출까지의 이력을 체계적으로 기록하여 증거의 연계 보관(Chain of Custody)을 유지한다.

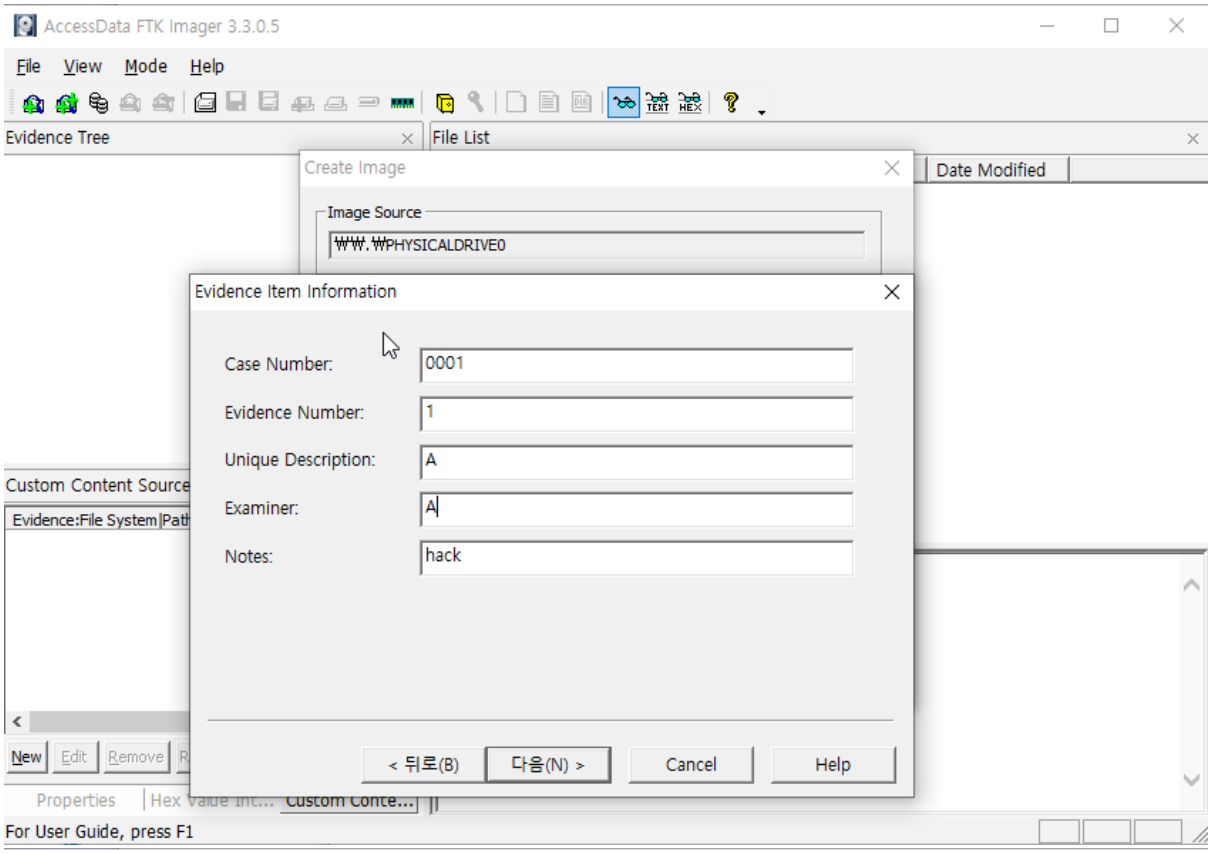
- 신뢰성을 확보한다.
수집과 분석에 사용되는 도구와 절차가 신뢰할 수 있는 방법으로 수행되었음을 보장한다. 포렌식 전문가는 공인된 장비와 도구를 활용하여 표준화된 절차에 따라 작업을 수행한다.

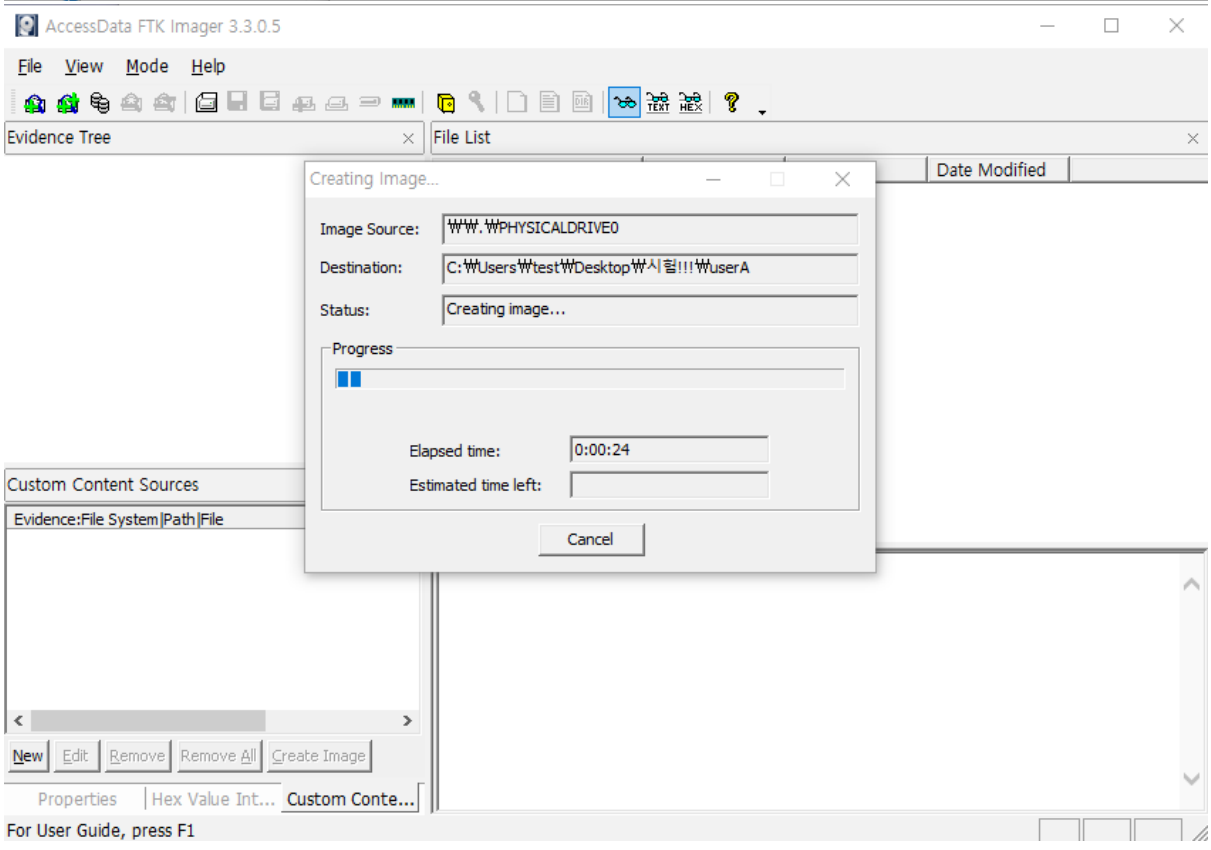
- 원본성을 유지한다.
원본 데이터를 손상 없이 보관하며, 분석은 복제본을 통해 수행한다. 복제본은 원본과 동일한 해시값을 가지도록 이미징 기술을 활용하여 생성한다.

1.2 디스크 이미징


AccessData FTK Imager 3.3.0.5
File View Mode Help
Evidence Tree
File List
Modified
Select Drive
Source Drive Selection
Please select from the following available drives:
₩₩.₩PHYSICALDRIVE0 - VBOX HARDDISK [64GB IDE]
< 뒤로(B)
Finish
Cancel
Help
Custom Content Sources
Evidence:File System|Path|File
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Int...
Custom Conte...
For User Guide, press F1


AccessData FTK Imager 3.3.0.5
File View Mode Help
Evidence Tree
File List
Date Modified
Create Image
Image Source
₩₩.₩PHYSICALDRIVE0
Select Image Type
Please Select the Destination Image Type
Raw (dd)
SMART
E01
AFF
< 뒤로(B)
다음(N) >
Cancel
Help
Custom Content Source
Evidence:File System|Path
New
Edit
Remove
Properties
Custom Conte...
For User Guide, press F1


AccessData FTK Imager 3.3.0.5
File View Mode Help
Evidence Tree
File List
Date Modified
Create Image
Image Source
₩₩.₩PHYSICALDRIVE0
Evidence Item Information
Case Number: 0001
Evidence Number: 1
Unique Description: A
Examiner: A
Notes: hack
< 뒤로(B)
다음(N) >
Cancel
Help
Custom Content Source
Evidence:File System|Path
New
Edit
Remove
Properties
Hex Value Int...
Custom Conte...
For User Guide, press F1


AccessData FTK Imager 3.3.0.5
File View Mode Help
Evidence Tree
File List
Date Modified
Creating Image...
Image Source: ₩₩.₩PHYSICALDRIVE0
Destination: C:₩Users₩test₩Desktop₩시험!!!₩userA
Status: Creating image...
Progress
Elapsed time: 0:00:24
Estimated time left:
Cancel
Custom Content Sources
Evidence:File System|Path|File
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Int...
Custom Conte...
For User Guide, press F1

2.1 ~ 2.3 이미징 후 수집된 증거를 다양한 분석 도구를 활용하여 분석하고 분석 보고서를 작성하시오.

- wow.pcap

1. Ann의 이메일 주소 : sneakyg33k@aol.com

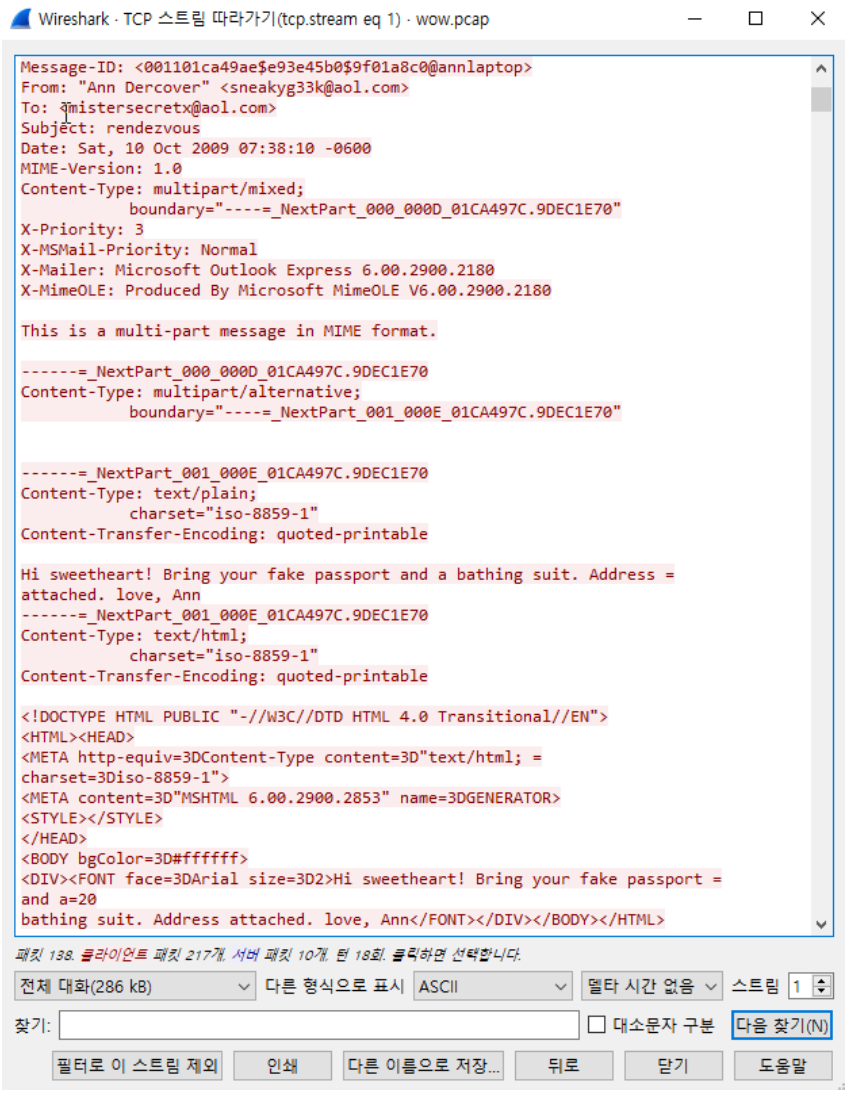
2. Ann의 이메일 password : NTU4cjAwbHo=(base64) 558r00lz(복호화)

3. Ann의 secret lover의 이메일 주소 : mistersecretx@aol.com

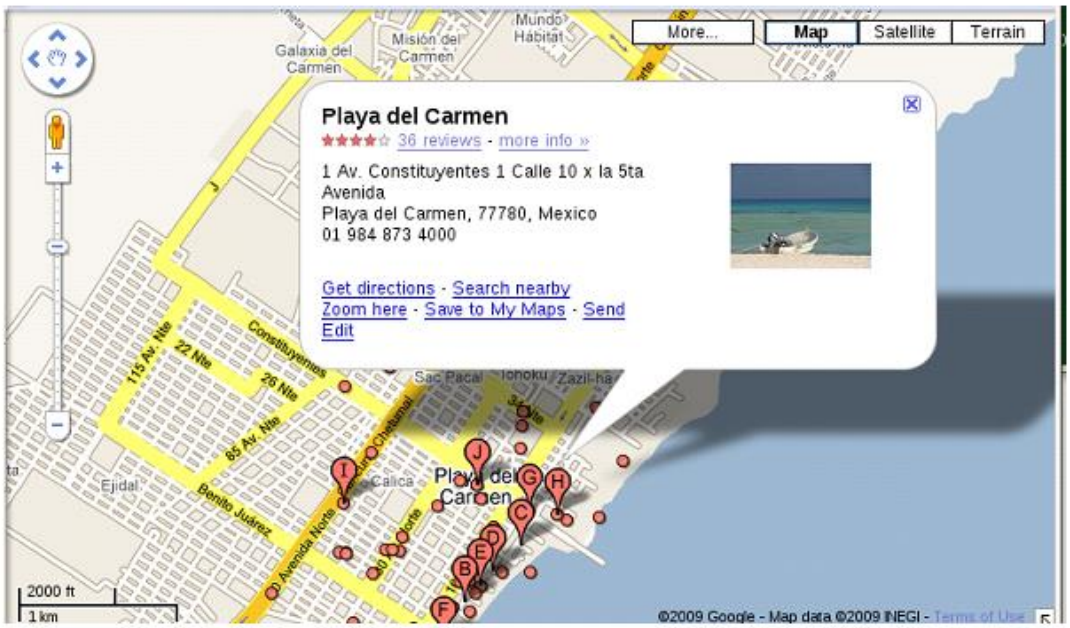
4. Ann이 secret lover에게 가져오라고 한 2개의 items : fake passport / bathing suit

5. Ann이 secret lover에게 보내준 attachment의 NAME : secretrendezvous.docx

6. 비밀 만남 CITY와 COUNTRY : Playa del Carmen, Mexico

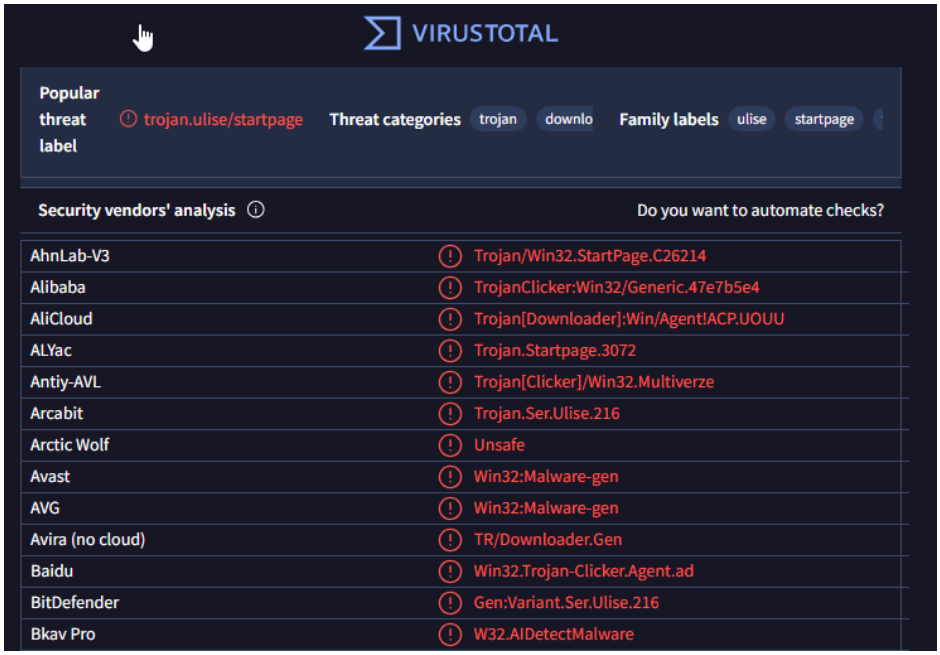


Meet me at the fountain near the rendezvous point. Address below. I'm bringing all the cash.

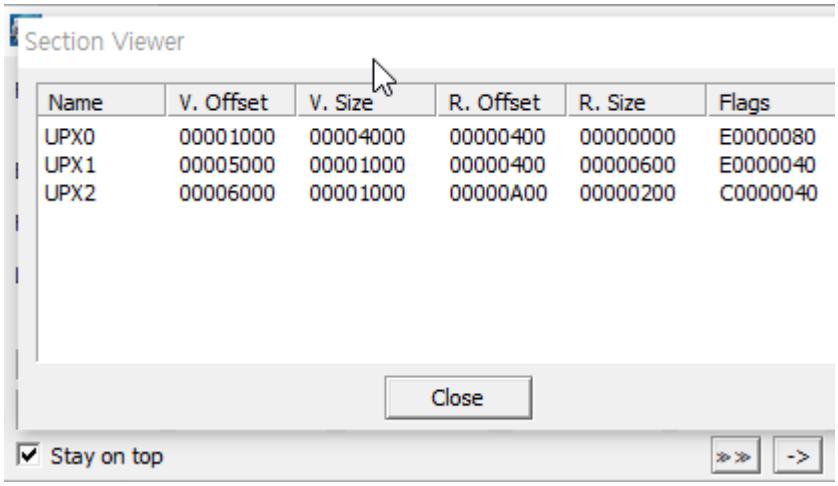


- **hack.exe**

1. 기초분석 : virustotal / 패킹 / 난독화 여부

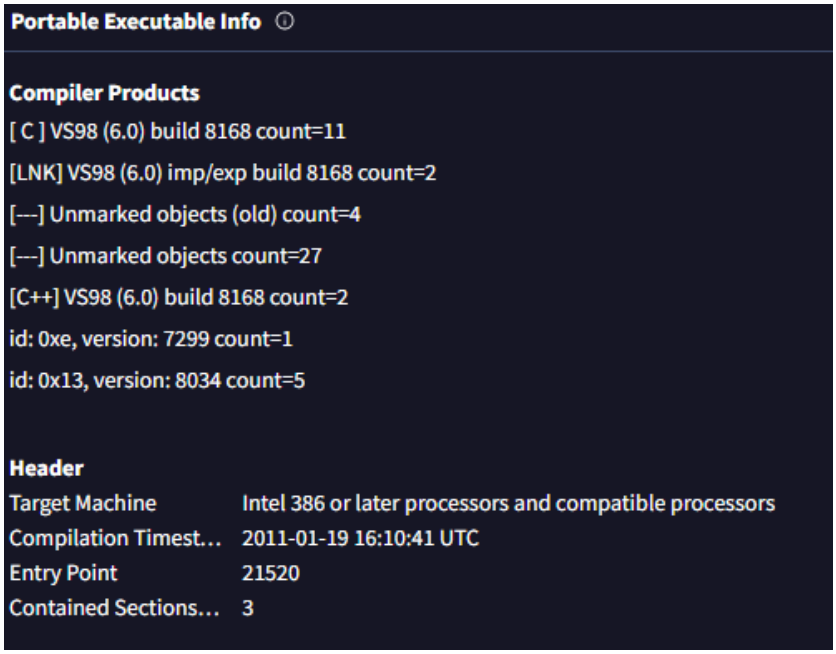


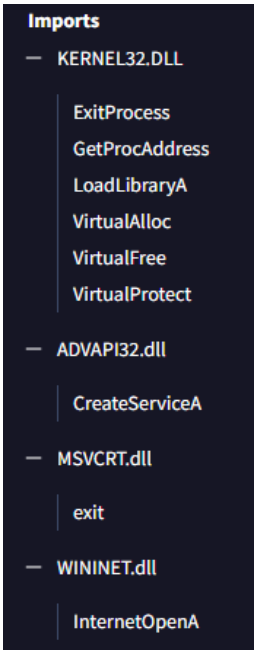
virustotal 사이트에서 Trojan 바이러스, 난독화가 되어있다는 것을 확인



PEiD를 이용해 패킹이 되어있는 것을 확인

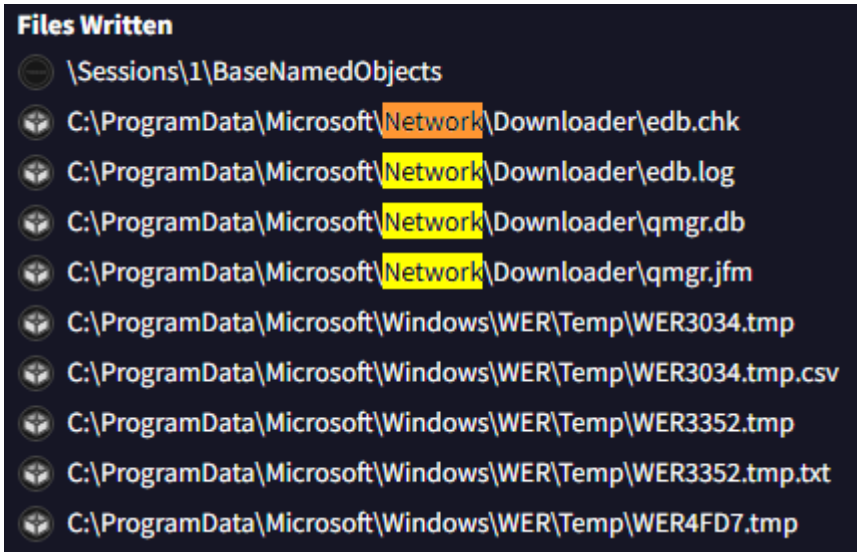
2. 컴파일 날짜 / 실행 시 import





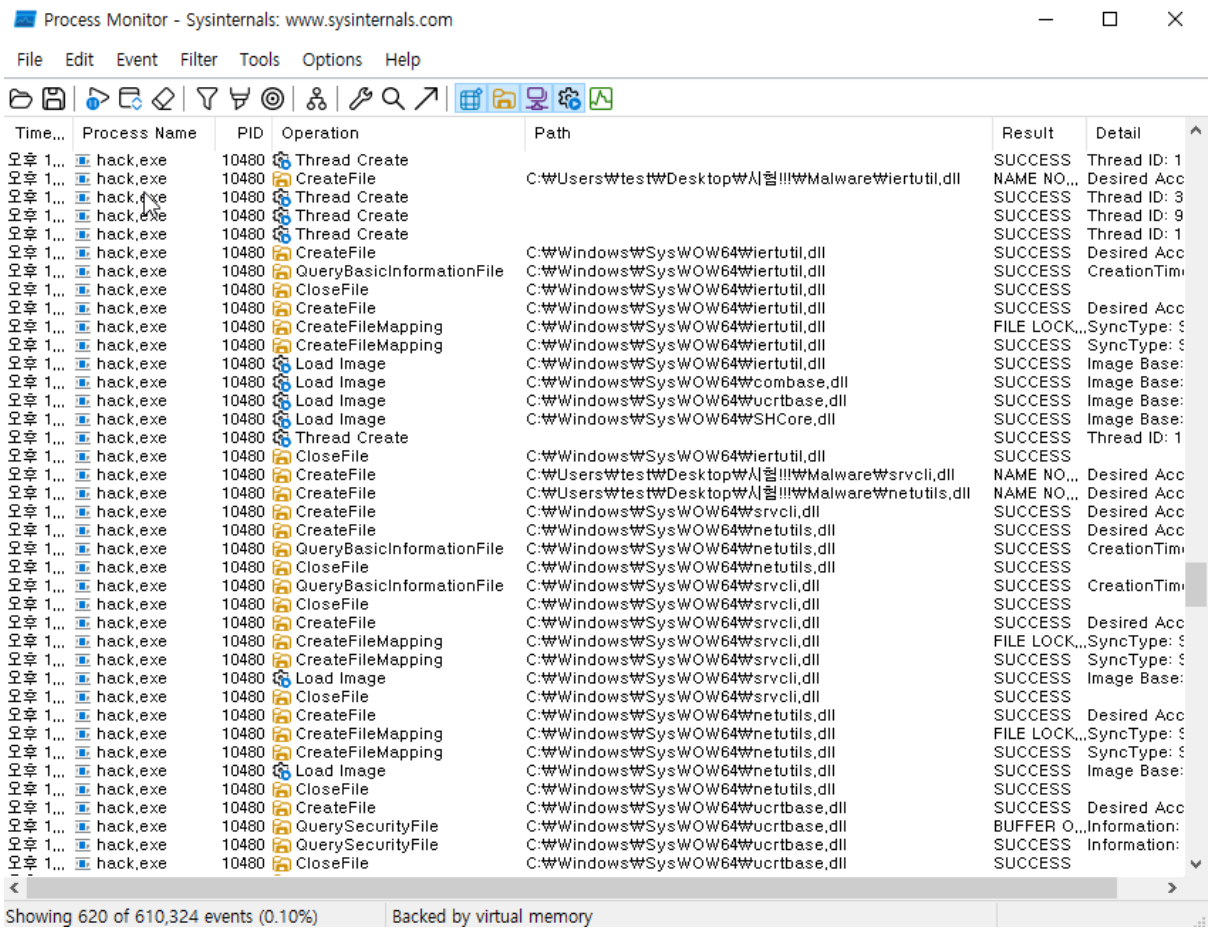
날짜와 어떤 방식으로 import되는지 확인

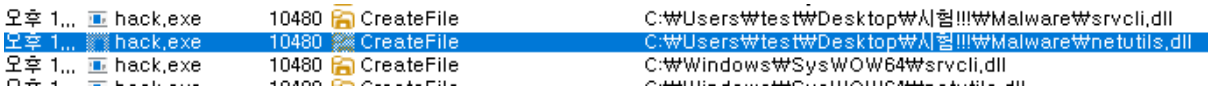
3. 호스트 또는 네트워크 기반 증거 표시



로컬 시스템 내에서 활동한 호스트 기반 증거들

4. 동적 분석 / 영향





procmon으로 모니터링 해 보니 hack.exe가 독립적인 스레드를 생성, 다른 보안 DLL을 로드하려고 시도중인 것을 확인. netutils.dll을 생성한 것을 보아 정상적인 이름을 가진 악성 dll을 폴더에 숨겨둔 것을 확인할 수 있다.

이는 악성 루틴을 별도로 돌릴 가능성이 있고 보안 속성을 읽어 우회와 자기 복제의 가능성이 있음