



Digital Forensic



23 고은이

PRESENTATION

INDEX

1. 디지털 포렌식이란?
2. 네트워크 증거 수집
3. 호스트 기반 증거 획득





Digital Forensic

범죄수사에서 적용되고 있는 과학적 증거 수집 및 분석기법의 일종으로, 각종 디지털 데이터 및 통화기록, 이메일 접속기록 등의 정보를 수집·분석하여 범행과 관련된 증거를 확보하는 수사기법을 말한다.



디지털 포렌식 프레임워크의 여섯 가지 기본 요소



- 식별
- 보존
- 수집
- 조사
- 분석
- 제출

증거 수집

네트워크 증거 수집



사고를 조사하는 동안 이용할 수 있는 주요한 증거 자료는 인터넷의 네트워크 진입/출구 지점이다. 피해 입은 네트워크에 따라 트래픽은 방화벽이나 인터넷 프록시 또는 둘 다를 통과하는 경우가 생긴다. 따라서 방화벽과 인터넷 프록시는 사고 대응 담당자에게 아주 중요한 증거 자료를 제공한다.

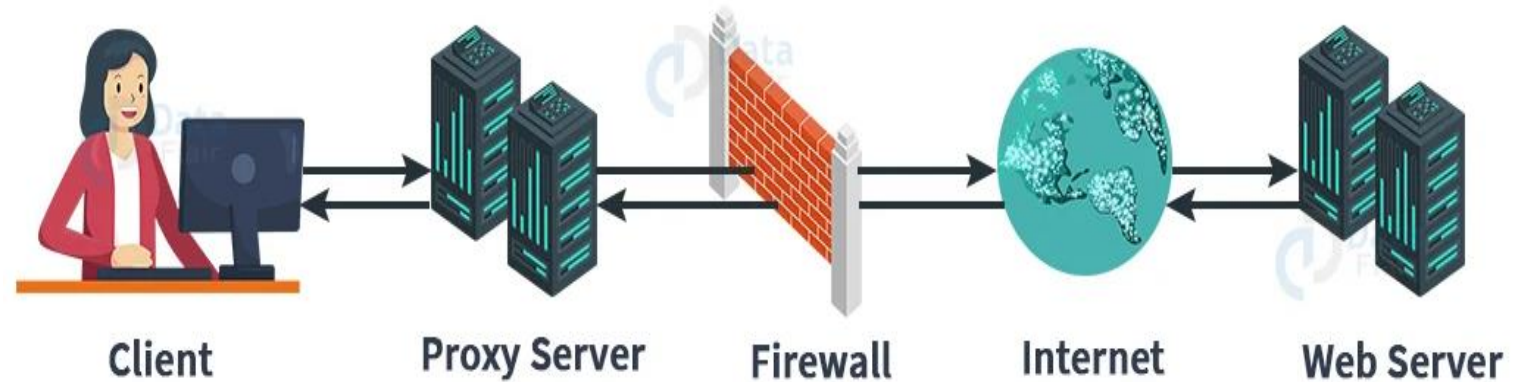
증거 수집

방화벽



차세대 방화벽의 대부분은 거부/허용 규칙을 IDS 또는 IPS와 결합하는 동시에 응용 프로그램에 대한 네트워크 액세스를 제어하고 이는 사고 발생 중에 활용할 수 있는 중요한 증거 소스를 생성한다. 사고 대응자는 방화벽이 제공하는 일련의 기능들과 특징 데이터를 철저히 파악하고 이해해야 한다.

증거 수집



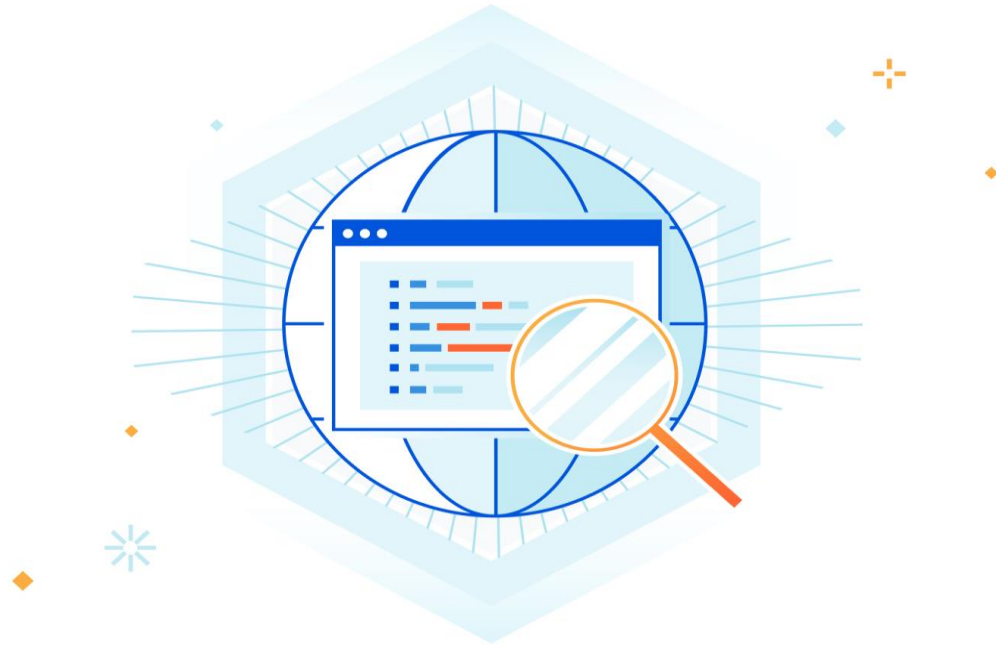
웹 프록시 서버

HTTP 및 HPPTS 요청에 웹 프록시 서버를 이용하는 조직이라면 외부 사이트에 접속한 적이 있는 내부 네트워크에 시스템에 대한 기록을 갖게 되고 이 기록으로 다운로드 된 악성 코드나 악성 프로그램의 위치를 식별할 수 있다.

(악성 코드와 유사한 전술을 사용하는 c2트래픽에서도 추가적인 정보를 얻을 수 있다.)

증거 수집

패킷 캡처



네트워킹 트래픽 캡처는 사고를 완전하게 파악하는데 중요한 역할을 한다. 일부 네트워크 기기들은 추가 분석을 위한 트래픽 캡처에 활용할 수 있는 tcpdump와 같은 프로그램을 가지고 있다. tcpdump는 패킷 캡처를 목적으로 설계된 명령 행 기반 도구다. 이것은 네트워크나 스위치에 물리적으로 접근 할 필요가 없고 원격으로 설정할 수 있다.

패킷 캡처

tcpdump -h

tcpdump

기본 도움말 메뉴에 접근

```
root@ubuntu:~# tcpdump -h
tcpdump version 4.9.3
libpcap version 1.8.1
OpenSSL 1.1.1 11 Sep 2018
Usage: tcpdump [-aAbdDefhHIJKlLnNOpqStuUvxX#] [-B size] [-c count]
               [-C file_size] [-E algo:secret] [-F file] [-G seconds]
               [-i interface] [-j tstamptype] [-M secret] [--number
               [-Q in|out|inout]
               [-r file] [-s snaplen] [--time-stamp-precision precision]
               [--immediate-mode] [-T type] [--version] [-V file]
               [-w file] [-W filecount] [-y datalinktype] [-z postro
               [-Z user] [expression]
```

tcpdump의 기본 설정은 사용 가능한 모든 인터페이스에서 트래픽을 캡처하는 것이다.

패킷 캡처

tcpdump -D

tcpdump

tcpdump가 트래픽을 캡처 할 수 있는 인터페이스 목록을 생성

```
root@ubuntu:~# tcpdump -D
1.ens33 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.bluetooth0 (Bluetooth adapter number 0)
5.nflog (Linux netfilter log (NFLOG) interface)
6.nfqueue (Linux netfilter queue (NFQUEUE) interface)
7.usbmon1 (USB bus number 1)
8.usbmon2 (USB bus number 2)
```

트래픽 캡처에 ens33 및 lo
인터페이스가 사용될 수 있음을
보여준다.

패킷 캡처

`sudo tcpdump -i ens33 -v`

tcpdump

ens33에 위치한 이더넷 인터페이스에서 일반적인 세부 정보의 수준으로 기본 캡처를 구성할 수 있다.

```
root@ubuntu:~# sudo tcpdump -i ens33 -v
tcpdump: listening on ens33, link-type EN10MB (Ethernet), capture size 262144 bytes
23:41:40.127384 IP (tos 0x0, ttl 255, id 11763, offset 0, flags [none], proto UDP (17), length 125)
    192.168.0.112.mdns > 224.0.0.251.mdns: 0 [2q] [1au] PTR (QU)? _companion-link._tcp.local. PTR
(QU)? _sleep-proxy._udp.local. (97)
23:41:40.140006 IP (tos 0x0, ttl 64, id 44172, offset 0, flags [DF], proto UDP (17), length 81)
    ubuntu.46569 > bns1.hananet.net.domain: 38443+ [1au] PTR? 251.0.0.224.in-addr.arpa. (53)
23:41:40.153527 IP (tos 0x0, ttl 249, id 64343, offset 0, flags [DF], proto UDP (17), length 154)
    bns1.hananet.net.domain > ubuntu.46569: 38443 NXDomain 0/1/1 (126)
23:41:40.155934 IP (tos 0x0, ttl 64, id 44173, offset 0, flags [DF], proto UDP (17), length 70)
    ubuntu.46569 > bns1.hananet.net.domain: 38443+ PTR? 251.0.0.224.in-addr.arpa. (42)
23:41:40.160845 IP (tos 0x0, ttl 250, id 64851, offset 0, flags [DF], proto UDP (17), length 127)
    bns1.hananet.net.domain > ubuntu.46569: 38443 NXDomain 0/1/0 (99)
```

-i는 tcpdump에 어떤 인터페이스에서 패킷 캡처를 수행할 것인지 명령

-v는 패킷 캡처 할 때 보여주는 세부 정보의 수준 설정

패킷 캡처

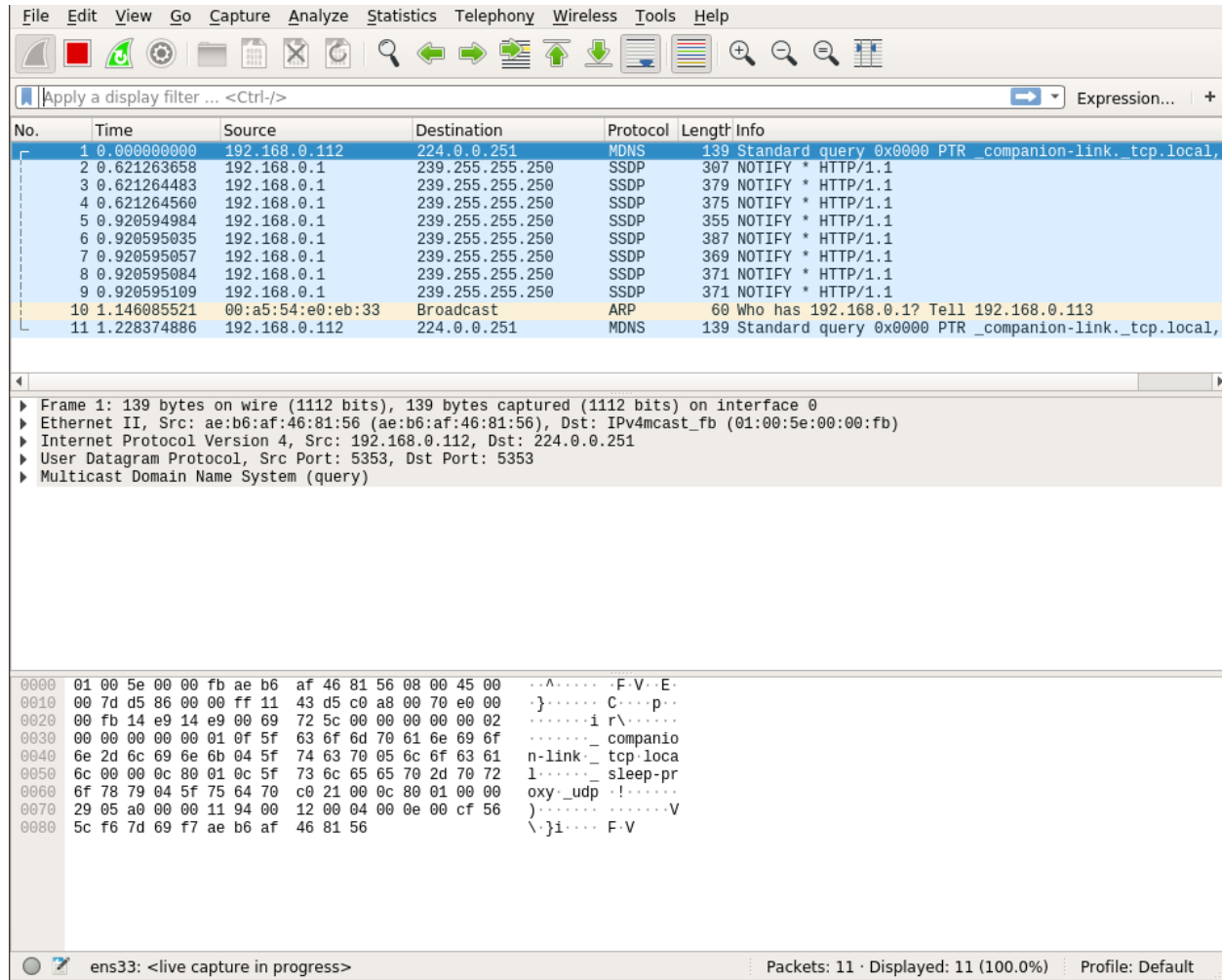
`sudo tcpdump -i ens33 -vvv -w ping_capture`

tcpdump

이전의 패킷 캡처를 파일로 출력한다.

```
root@ubuntu:~# sudo tcpdump -i ens33 -vvv -w ping_capture
tcpdump: listening on ens33, link-type EN10MB (Ethernet), capture size 262144 by
^C77 packets captured
77 packets received by filter
0 packets dropped by kernel
```

캡처를 중지 하려면 **Ctrl + C**를 누른다.



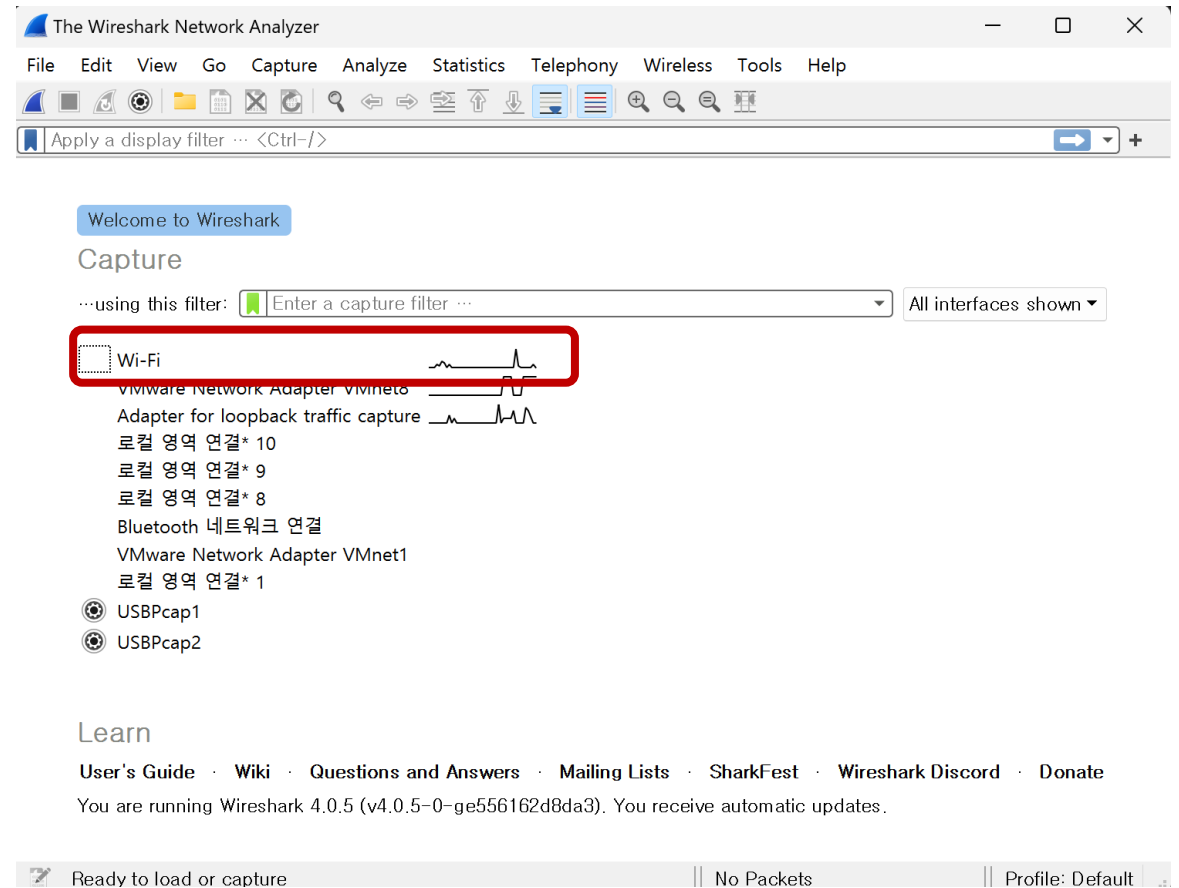
Wireshark를 통해 파일을 열 수 있다.

패킷 캡처

Wireshark

관리자 권한으로 실행한다.

트래픽을 처리하고 있는 것으로 표시되는 3개의
인터페이스 중 주목해서 봐야 하는 것은 Wi-Fi
인터페이스다.

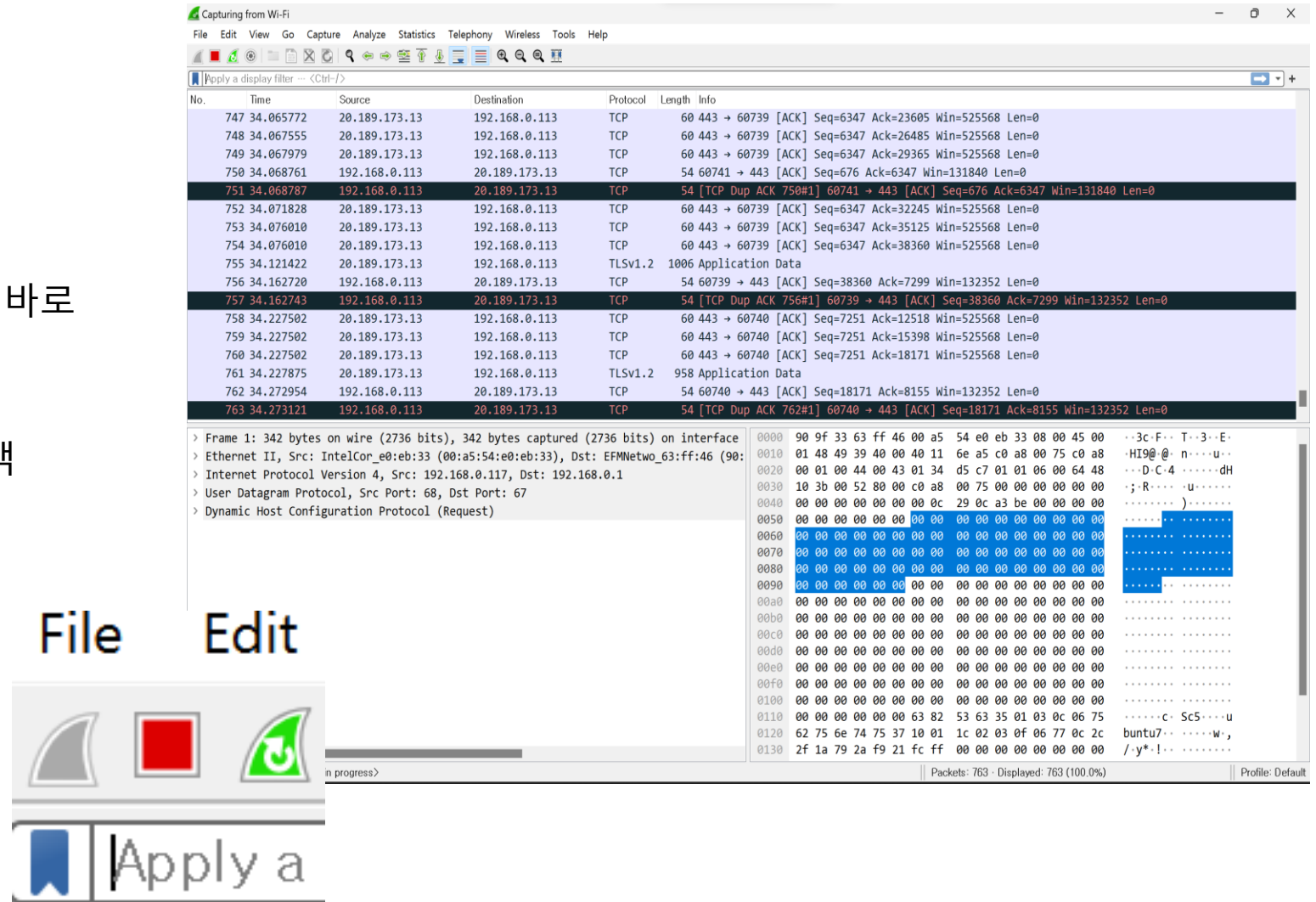


패킷 캡처

Wireshark

tcpdump 와 달리 캡처가 분석을 위해 바로 화면으로 출력된다.

캡처를 중지하려면 왼쪽 상단에 빨간색 버튼을 누르면 된다.





호스트 기반 증거 획득

호스트 시스템은 자주 악의적인 공격의 표적이 된다.
호스트 시스템은 네트워크에서 또는 추가적인 공격을 위한 피벗 포인트 또는 위협 행위자의 최종 목표를 만드는데 거점 확보가 가능한 초기 표적이다.
따라서 사고 대응 분석가는 호스트 시스템에 대한 조사 준비를 갖춰야 한다.

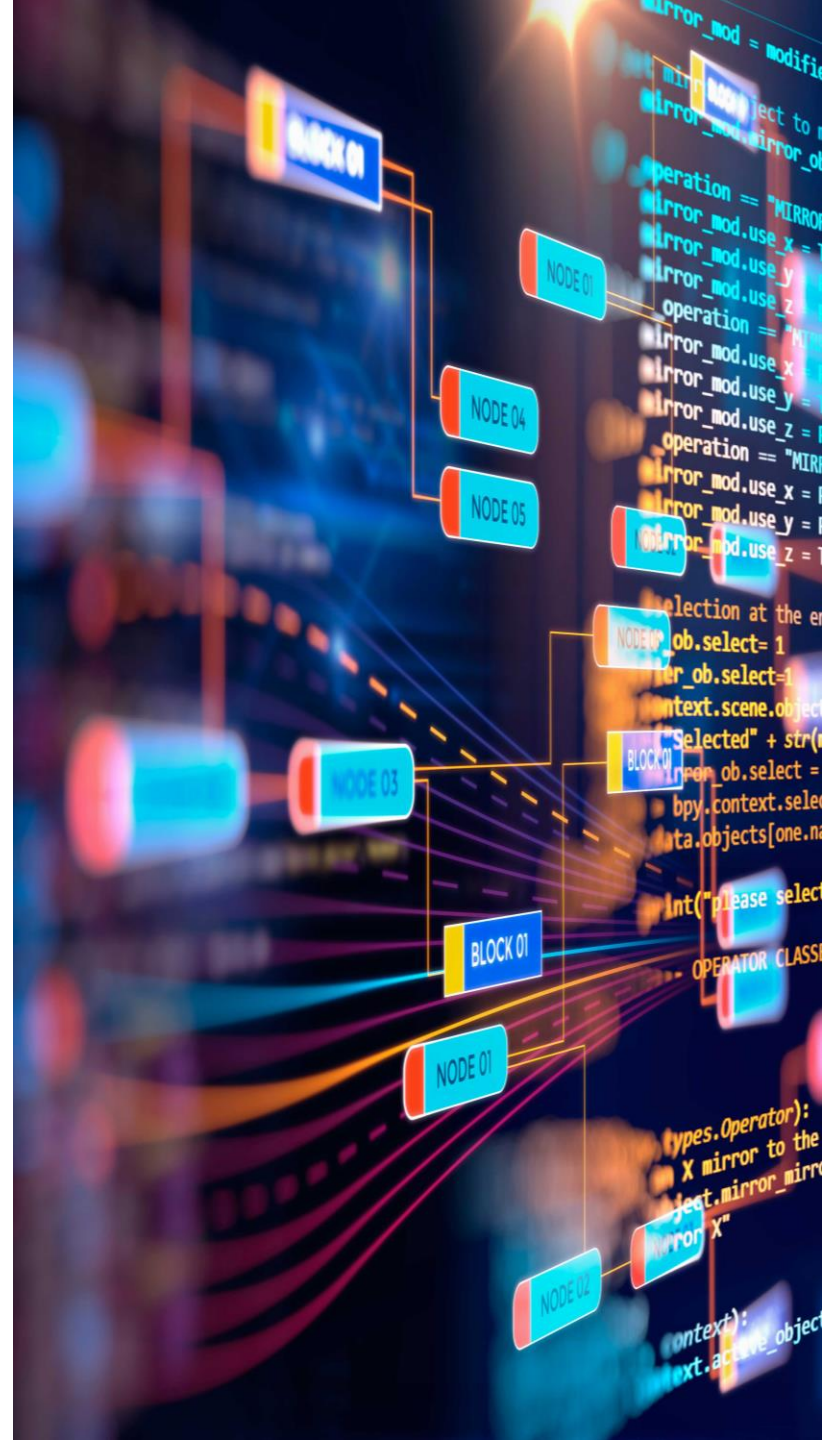
마이크로 소프트 윈도우와 같은 운영체제는 응용 프로그램 실행, 파일 변경, 사용자 계정의 추가 과정에서 다양한 증거 아티팩트를 남겨 사고 대응 분석가가 평가할 수 있는 활동의 흔적을 남긴다.





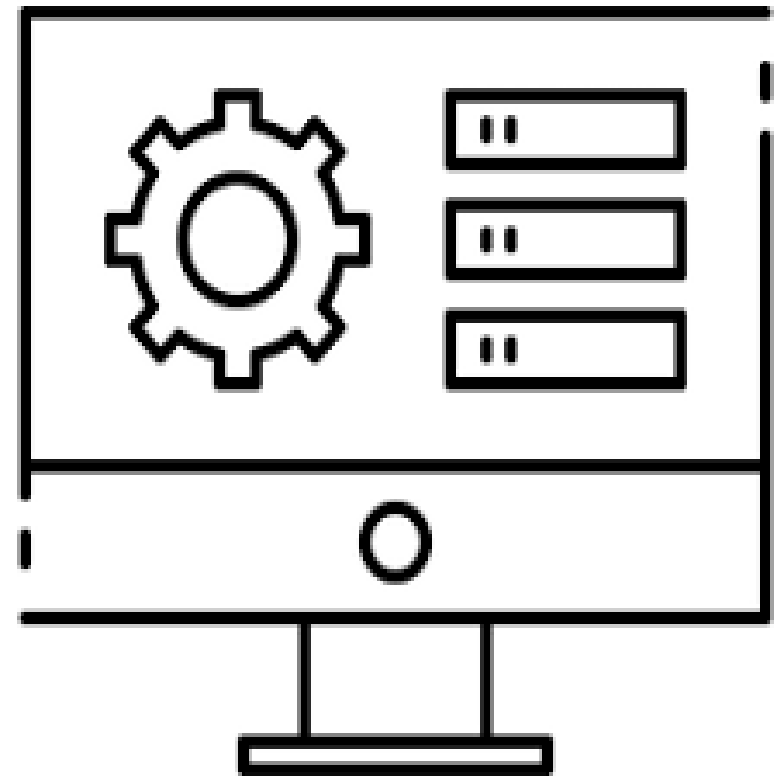
휘발성

시스템의 전원이 꺼질 때 손실되는 데이터를 휘발성 데이터라고 한다. 휘발성은 로그오프나 정전과 같은 변화가 있고 나서 호스트 시스템의 데이터가 어떻게 유지/관리 되는지 설명하는데 사용된다. 휘발성 데이터는 CPU 또는 라우팅 테이블, ARP 캐시의 데이터 일 수 있다. 가장 중요한 휘발성 데이터 중 하나는 시스템에서 현재 실행되고 있는 메모리다. 악성 코드 감염과 같은 사고를 조사할 때 라이브 시스템의 메모리가 아주 중요하다. 악성 코드는 시스템의 메모리 내에서 많은 주요 증거를 남기는데, 이 메모리가 손실 되는 경우 사고 대응 분석자가 할 수 있는 방법이 거의 없다.



비 휘발성

비 휘발성 데이터는 하드 드라이브에 저장되는 데이터로서 컴퓨터 전원이 꺼진 후에도 계속 유지된다. 악성 코드가 메모리에 증거를 남기는 동안 비 휘발성 메모리에는 증거 가치가 있는 항목들이 여전히 존재한다.



증거 획득 순서를 정할 때 고려해야 할 디지털 증거

중앙 처리 장치,
레지스터

랜덤 액세스 메모리

페이지 파일
또는
스왑 파일

스토리지 드라이브

증거 수집 절차

01

시스템과 일반
장치 촬영

02

시스템 전원 확인

03

실행 메모리 확보

04

파일 레지스트리
및 로그 확보

05

시스템 전원
플러그 제거

06

시스템 모델 및
일련번호 캡처

07

하드 드라이브
모델 및 일련번호
캡처

08

시스템에서 하드
디스크 정보를
사라시키기
방지 백업

09

모든 조치 문서화

휘발성 메모리 획득

보안 사고에서 많은 양의 증거는 손상 가능성이 있는 시스템 메모리 안에 들어있다. 흔적 증거는 종종 손상된 시스템의 메모리에서 발견되기 때문에 시스템 전원을 끄고 하드 드라이브를 제거하기 전에 실행 메모리를 확보하는 것이 중요하다.

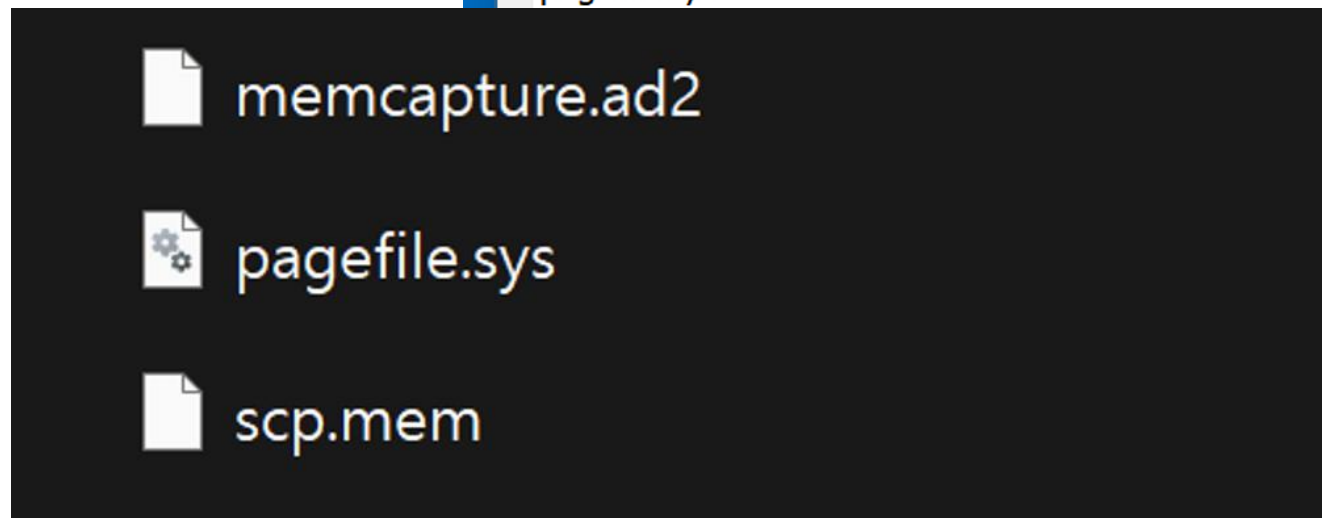
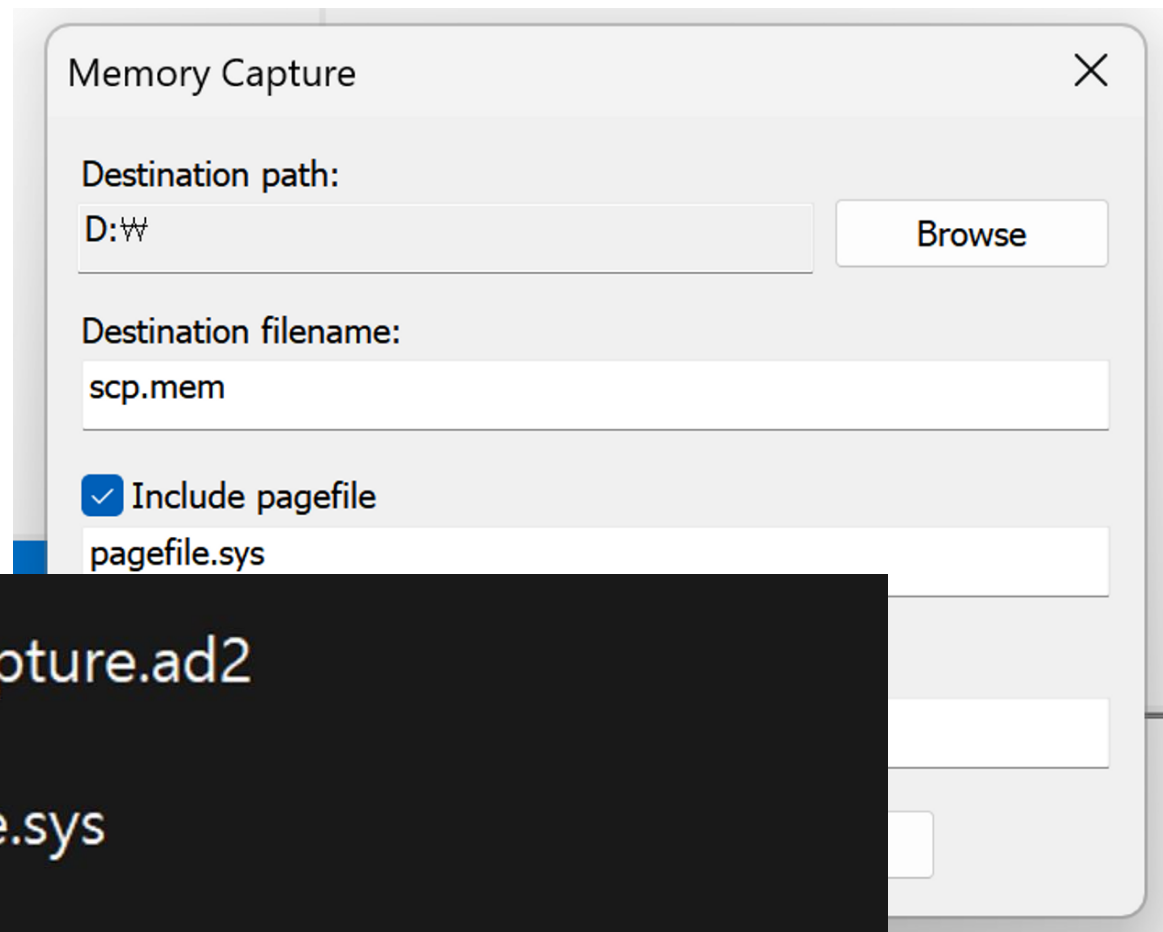


로컬 획득

FTK Imager

FTK Imager 실행 후 file에 들어가
Capture Memory 클릭

파일 이름 입력

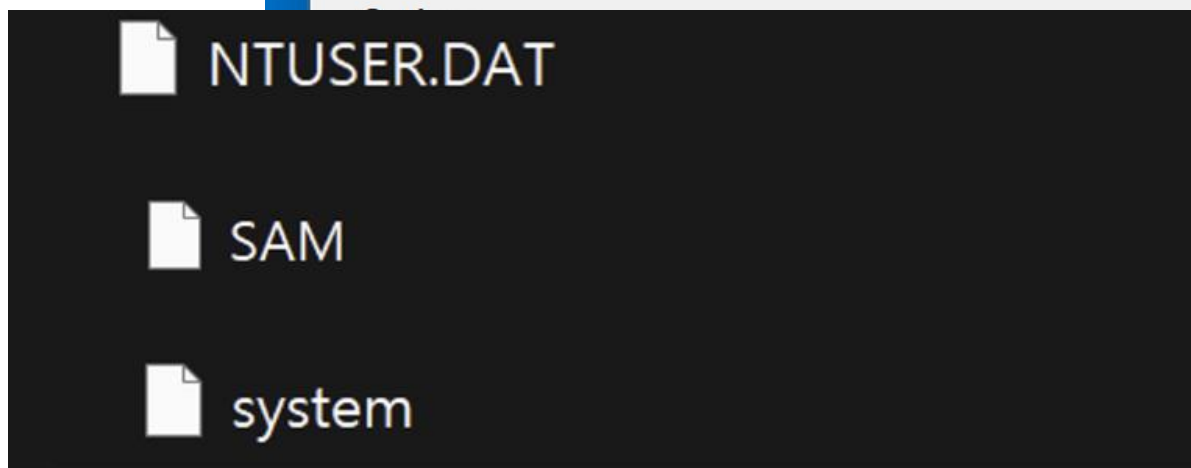
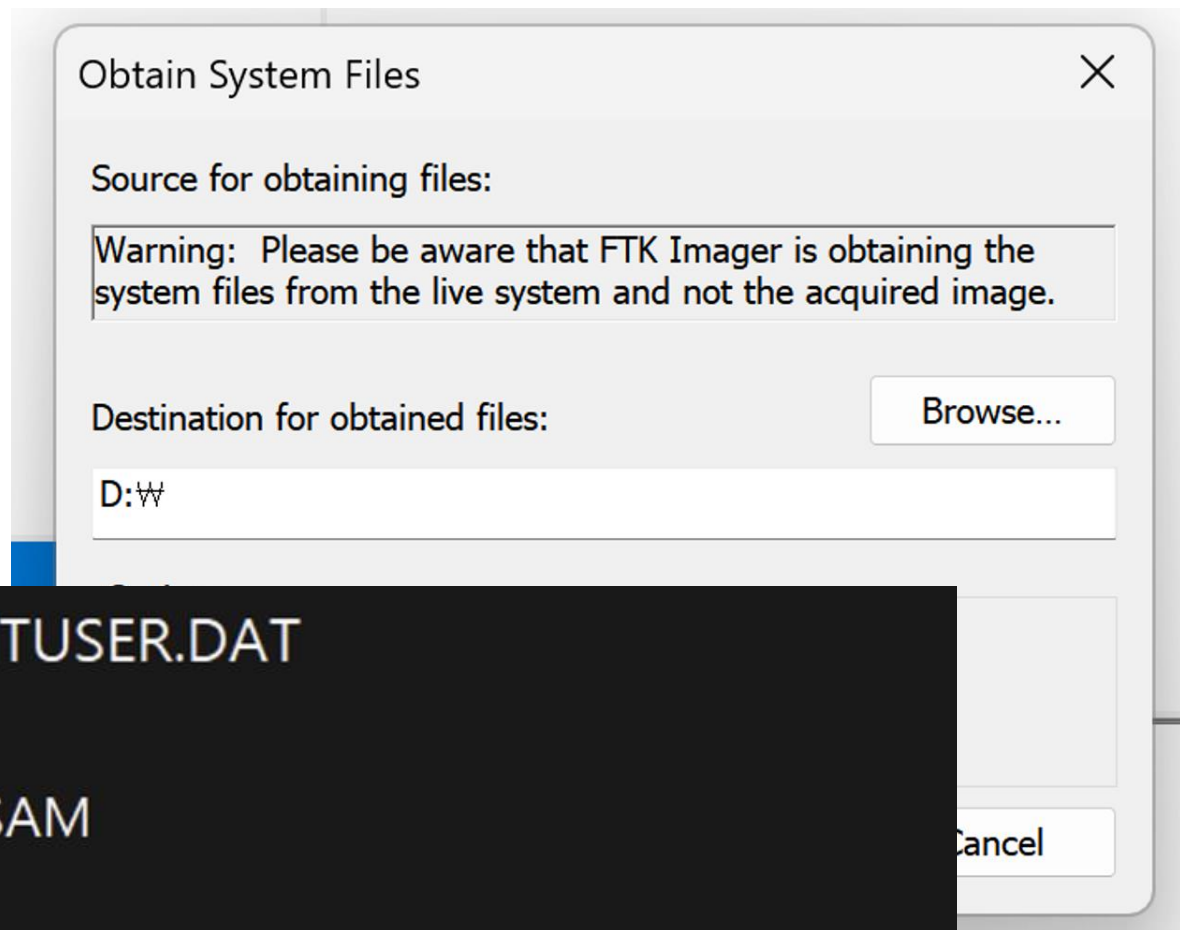


비 휘발성 증거 획득

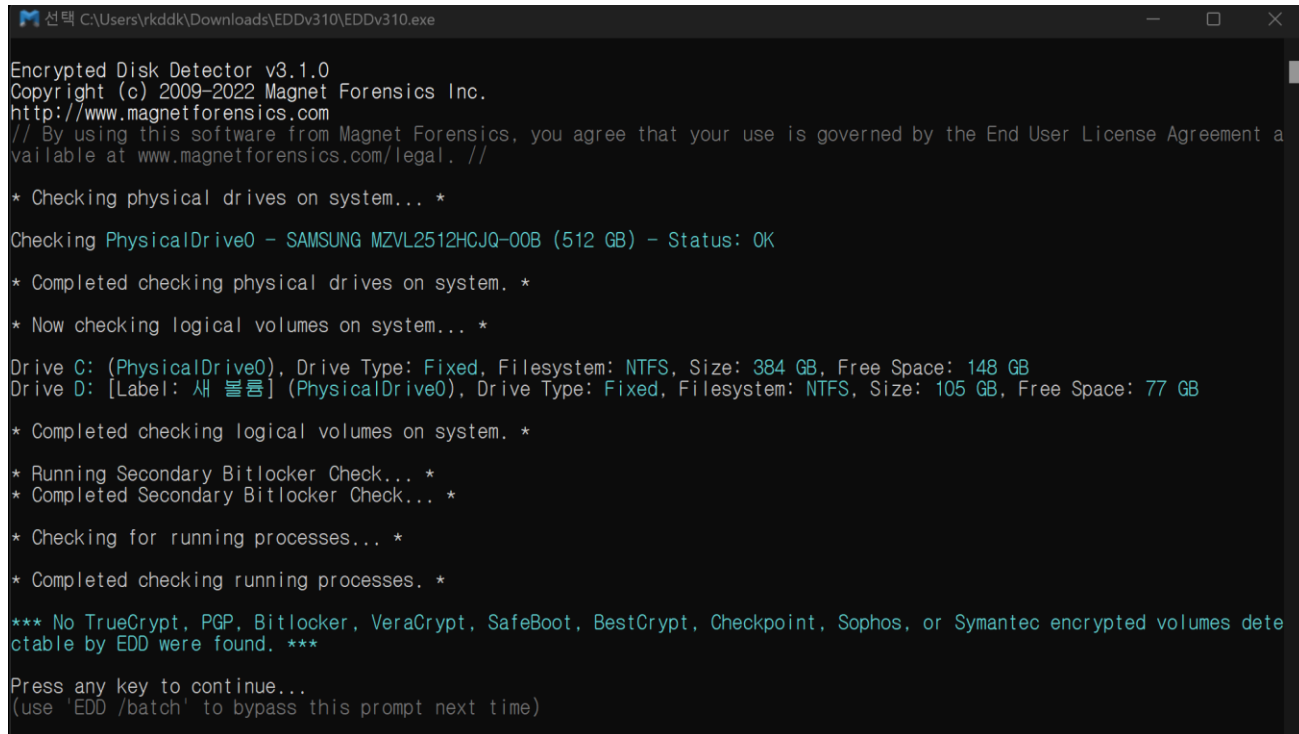
FTK Imager

FTK Imager 실행 후 file에 들어가
Obtain Protected Files 클릭

레지스트리 및 암호 데이터가
증거 폴더로 전송된다.



암호화 확인



```
선택 C:\Users\ykddk\Downloads\EDDv310\EDDv310.exe
Encrypted Disk Detector v3.1.0
Copyright (c) 2009-2022 Magnet Forensics Inc.
http://www.magnetforensics.com
// By using this software from Magnet Forensics, you agree that your use is governed by the End User License Agreement a
vailable at www.magnetforensics.com/legal. //

* Checking physical drives on system... *
Checking PhysicalDrive0 - SAMSUNG MZVL2512HCJQ-00B (512 GB) - Status: OK
* Completed checking physical drives on system. *
* Now checking logical volumes on system... *
Drive C: (PhysicalDrive0), Drive Type: Fixed, Filesystem: NTFS, Size: 384 GB, Free Space: 148 GB
Drive D: [Label: 새 볼륨] (PhysicalDrive0), Drive Type: Fixed, Filesystem: NTFS, Size: 105 GB, Free Space: 77 GB
* Completed checking logical volumes on system. *
* Running Secondary Bitlocker Check... *
* Completed Secondary Bitlocker Check... *
* Checking for running processes... *
* Completed checking running processes. *

*** No TrueCrypt, PGP, Bitlocker, VeraCrypt, SafeBoot, BestCrypt, Checkpoint, Sophos, or Symantec encrypted volumes dete
ctable by EDD were found. ***

Press any key to continue...
(use 'EDD /batch' to bypass this prompt next time)
```

Magnet Forensics의 도구를 통해 어떤 암호화가 사용되고 있는지 확인 할 수 있다.



Thank you