디지털포렌식

> [19반] 정민석_7000

> 작성일: 2025/03/31

목차

범죄 시나리오 설정

[1]의 링크에는 한국형 초음속 전투기 KF-21 관련 내부 개발 자료를 유출한 인도네시아 기술자의 컴퓨터, 휴대전화 등의 저장장치를 압수하였다는 정보가 실려있습니다.

이번 과제에서는 기술자의 저장장치에 유출한 것으로 추정되는 전투기 사진[2]이 담겨있고, 이러한 저장장치를 분석해보겠습니다. 저장장치 C: 드라이브의 볼륨을 축소하여 생성하였습니다. 더하여 해당 논리 드라이브는 아래의 디렉토리 구조로 세팅하였습니다.

```
img/
img/my_img.jpeg
```

이미징 과정 및 정보

1. 저장 장치 훼손을 막기 위하여, 디스크 쓰기 방지를 활성화
2. FTK Imager에서 File→CreateDiskImage 클릭
3. 이미지 생성을 원하는 저장장치 선택
4. Add를 클릭하여 **E01** 선택
5. **Case Number(ex. 오늘 날짜)**등 정보 입력
6. **Image Fragment Size를 0으로 설정** 및 저장할 디렉토리, 이미징 파일명 입력
7. 이미징 파일 생성 완료

- 이미징 파일 생성 시 생성되는 텍스트 파일

```
Created By Exterro® FTK® Imager 4.7.3.81

Case Information:
Acquired using: ADI4.7.3.81
Case Number: 2025-3-30
Evidence Number:
Unique Description:
Examiner:
Notes:

---------------------------------------------------------------

Information for C:\Users\j93es\Desktop\2025-3-30:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Logical
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 802,816
[Physical Drive Information]
 Removable drive: False
 Source data size: 392 MB
 Sector count:    802816
[Computed Hashes]
 MD5 checksum:    bf7b144f236fec1c5b4511b7d96a3ec8
 SHA1 checksum:   18bca2c2e79962307761d6bfd18eca719e59c52e

Image Information:
 Acquisition started:   Sun Mar 30 19:06:01 2025
 Acquisition finished:  Sun Mar 30 19:06:05 2025
 Segment list:
  C:\Users\j93es\Desktop\2025-3-30.E01
 COMPUTED HASH：bf7b144f236fec1c5b4511b7d96a3ec8
 COMPUTED HASH：18bca2c2e79962307761d6bfd18eca719e59c52e

Image Verification Results:
 Verification started:  Sun Mar 30 19:06:05 2025
 Verification finished: Sun Mar 30 19:06:08 2025
```

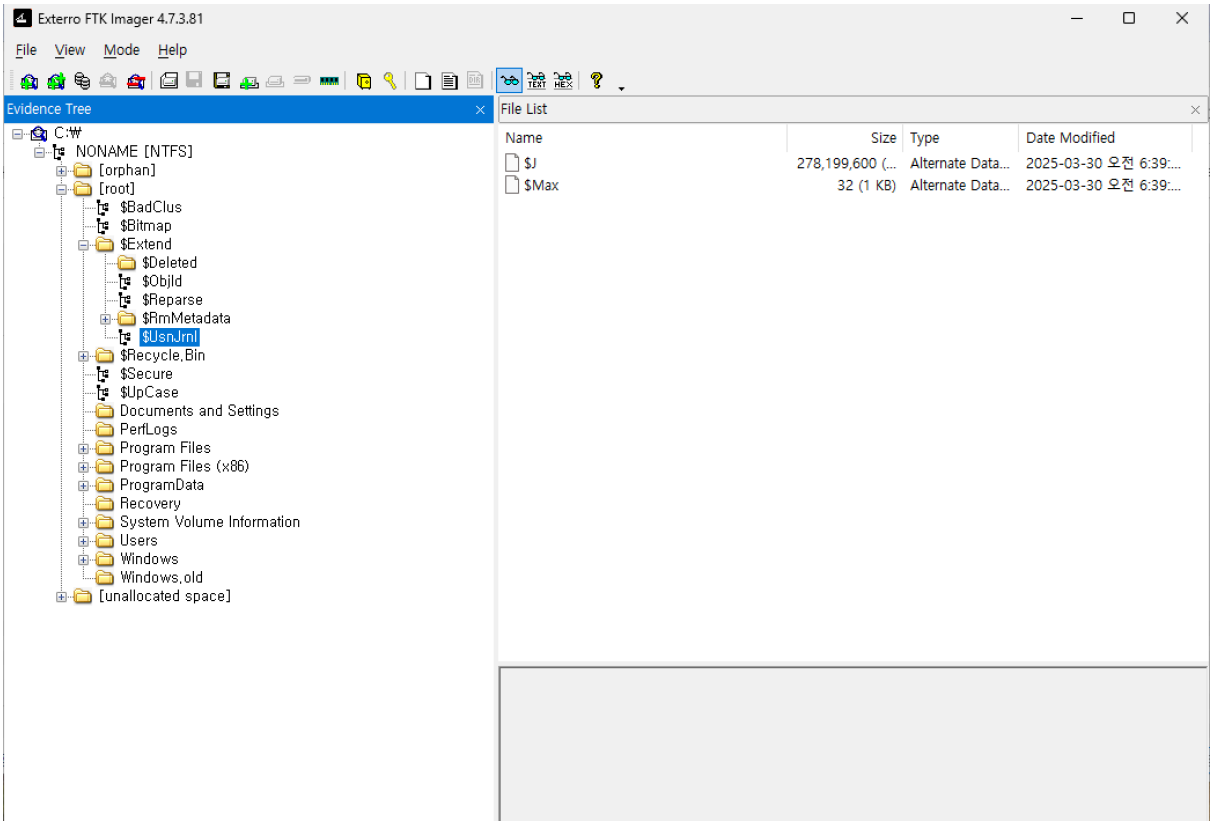
MD5 checksum: bf7b144f236fec1c5b4511b7d96a3ec8 : verified
SHA1 checksum: 18bca2c2e79962307761d6bfd18eca719e59c52e : verified

이미징 파일 분석

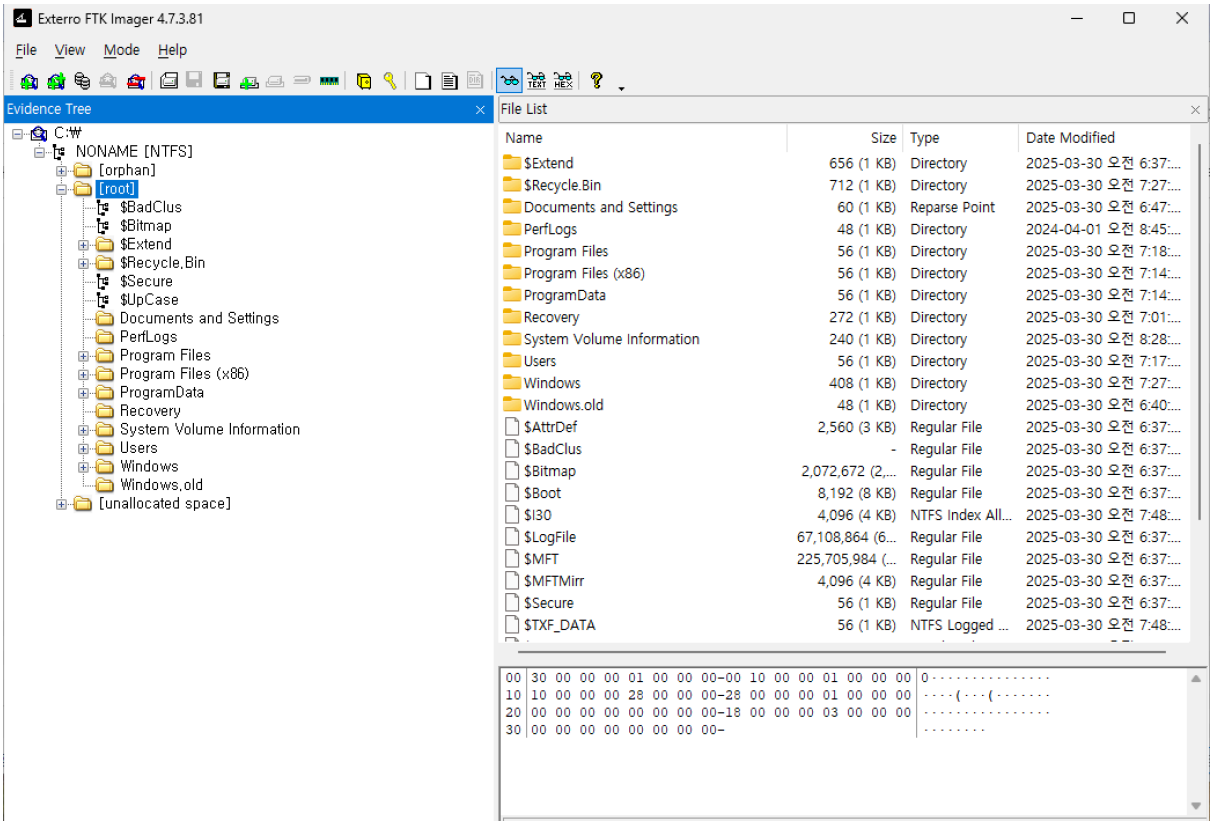
FTK Imager를 통한 파일 추출

MacOS에서 UTM 가상머신으로 윈도우를 실행하는 환경이며 “보호된 운영체제 파일 숨기기” 옵션을 해제하였지만, 논리 드라이브의 $UsrJrnl이 표출되지 않았습니다. 이에 부득이하게 C: 드라이브의 파일로 실습을 진행하였습니다.

- $J 추출



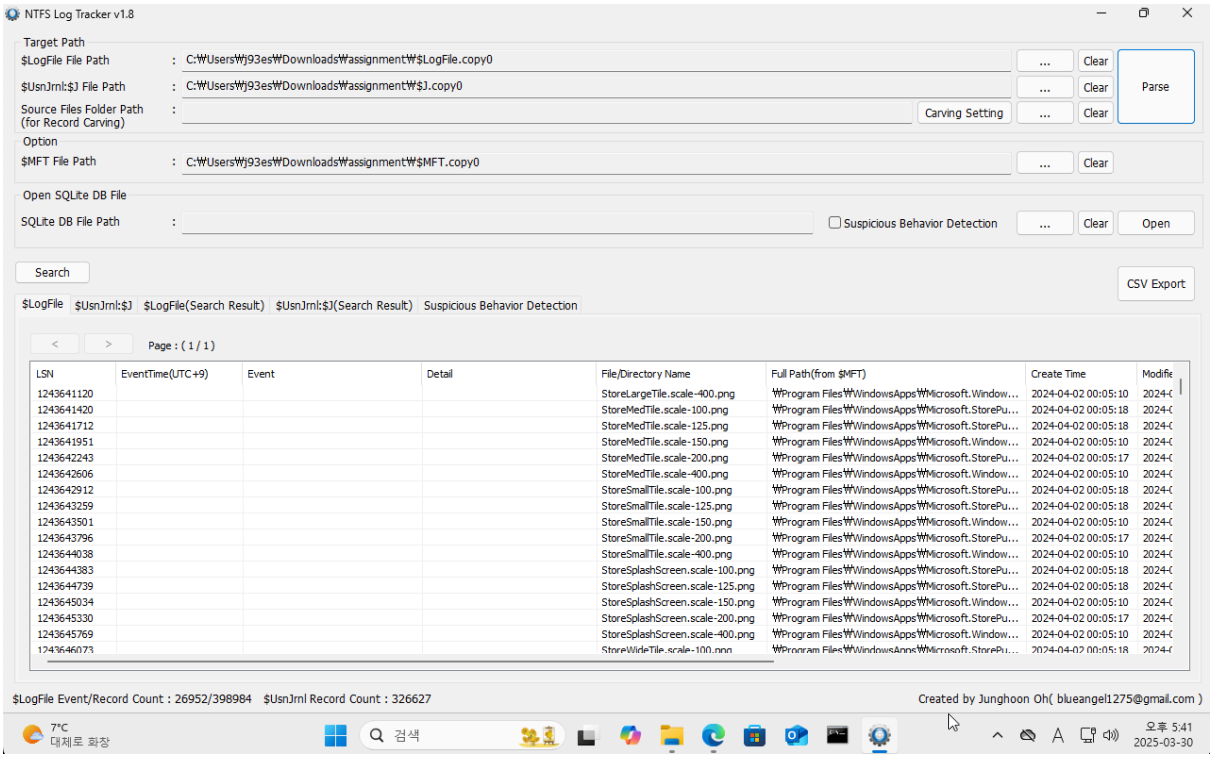
- $LogFile, $MFT 추출



최종적으로 $J, $LogFile, $MFT 파일을 추출하였습니다.

NTFS Log Tracker를 통한 파일 분석

- NTFS Log Tracker에 $J, $LogFile, $MFT를 입력하고 Parse한 결과물



이러한 분석을 통하여 파일이 변경된 이력을 조회할 수 있었습니다.

ExifTool를 통한 이미지 메타데이터 분석

- ExifTool을 통한 exif 출력 결과 중 일부

```
ExifTool Version Number         : 12.36
File Name                       : IMG_6467.jpeg
Directory                       : .
File Size                       : 857 KiB
Zone Identifier                 : Exists
File Modification Date/Time     : 2025:03:30 17:32:57+09:00
File Access Date/Time           : 2025:03:30 17:33:28+09:00
File Creation Date/Time         : 2025:03:30 17:32:56+09:00
File Permissions                : -rw-rw-rw-
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Exif Byte Order                 : Big-endian (Motorola, MM)
Make                            : Apple
Camera Model Name               : iPhone 16
Orientation                     : Horizontal (normal)
X Resolution                    : 72
Y Resolution                    : 72
Resolution Unit                 : inches
Software                        : 18.3.1
Modify Date                     : 2025:03:12 14:57:29
Host Computer                   : iPhone 16
Y Cb Cr Positioning             : Centered
Exposure Time                   : 1/4630
F Number                        : 1.6
Exposure Program                : Program AE
ISO                             : 32
Exif Version                    : 0232
Date/Time Original              : 2025:03:12 14:57:29
Create Date                     : 2025:03:12 14:57:29
Offset Time                     : +09:00
Offset Time Original            : +09:00
Offset Time Digitized           : +09:00
Components Configuration        : Y, Cb, Cr, -
```

exif를 분석한 결과, 사진 촬영자의 기종, 촬영 위치/시각 등의 많은 정보를 확인할 수 있었습니다. 이를 통하여 수사에 도움이 되는 정보를 수집하였습니다.

참고 자료

- [1] https://www.chosun.com/national/2024/03/16/UBM625XQCVDPRJPA2DNSOZRABY/?utm_source=naver&utm_medium=referral&utm_campaign=naver-news
- [2] 직접 촬영한 블랙이글스 공연 사진으로, 군부대 내에서 촬영하여 **해당 사진 및 이미징 파일의 외부 유출은 삼가**해주시길 부탁드리겠습니다.