

제 3장 디지털 증거 분석기법

4. 인터넷 브라우저

각각의 브라우저들은 사용자의 인터넷 행위에 대해서 파일 형태로 저장
해당 파일 분석을 통해 사용자가 방문한 사이트 주소(히스토리), 사용한 이메일,
검색한 키워드, 캐시 등을 확인 가능

4.1. 구글 크롬(Chrome)

구글에서 제작하여 배포하는 브라우저 프로그램 크롬은 안정성과 효율적인 인터페이스에
중점을 두고 있음

크롬을 이용해 인터넷 행위를 수행하면 해당 내용이 파일에 저장됨

대표적 파일들은 크롬의 'Default'에 저장됨

'Login Data', 'Last Session', 'Visited Links', 'Top Sites' 등의 아티팩트 파일들이 저장됨

4.2. 마이크로소프트 엣지(Edge) / 인터넷 익스플로러(IE 10)

윈도우에 포함된 기본 웹 브라우저이며 엣지의 경우 윈도우 10 이후로 탑재된 웹 브라우저
인터넷 익스플로러의 경우 4~9버전까지 'index.dat' 파일에 브라우저 사용 정보들을
저장하였고 IE 10으로 넘어오면서 데이터베이스 파일 형식으로 전환됨

엣지 브라우저는 인터넷 익스플로러와 히스토리 파일을 같이 사용

사이트 정보를 'WebCacheV01.dat' 파일에 저장

4.3. 파이어폭스(Firefox)

모질라에서 개발한 오픈 소스 웹 브라우저이며 최초 개발 당시 'Phoenix' 라는 이름을
사용하다 'Firebird'로 변경한 뒤 최종적으로 현재의 이름으로 불리움

방문한 사이트의 기록을 'places.sqlite' 파일에 저장하고 'SQLite' 데이터베이스 형식을 사용

파이어폭스 26.0부터 다운로드 받은 파일 목록도 'places.sqlite'에 함께 기록됨

4.4. 사파리(Safari)

애플에서 개발한 기본 웹 브라우저로 Mac OS와 iOS에 사용되며 윈도우 용으로도
개발되어 윈도우 OS에서 설치하여 사파리 브라우저를 사용 가능(2012.5.9.일 출시된 5.1.7
버전 이후로 더 이상 지원 안함)

접속한 사이트들에 대한 정보는 'History.plist' 파일에 저장하며 바이너리 타입의
'plist' 파일로 별도의 도구를 이용해서 내용을 확인해야 함

5. 이메일

5.1. 웹메일(Webmail) 서비스

웹 브라우저를 통해 웹 페이지에서 전자우편을 전달하는 서비스
대표적으로 ‘핫메일’, ‘야후’, ‘지메일’ 등이 있으며 국내에는 ‘네이버’, ‘다음’, ‘네이트’ 등

5.2. PC 이메일 응용프로그램

응용프로그램이 PC에 이메일 데이터를 파일 형태로 저장함
해당 파일들을 분석하여 사용자의 송수신 이메일, 일정, 주소록 등의 데이터 확인 가능

5.2.1. 모질라 썬더버드(Mozilla Thunderbird)

다양한 플랫폼에서 사용할 수 있는 이메일 클라이언트(프로그램)
마이크로소프트의 아웃룩 프로그램, Gmail, 다음, 네이버 메일등을 지원함
다른 PC에서 사용한 메일에 대한 프로필 파일 연동가능, 새로운 프로필에서 사서함
데이터 정의 가능

5.2.2. 마이크로소프트 아웃룩(Microsoft Outlook)

마이크로소프트에서 개발한 개인 정보 관리자 응용프로그램의 메일 클라이언트
오피스 97부터 기본적으로 수록되었으며 메일 기능, 달력, 일정 및 연락처 관리 등을 포함
두 가지 모드로 온라인 모드와 캐시된 모드로 사용할 수 있으며 아웃룩을 Exchange
Server로 구성하면 사용자 사서함 파일을 만듦
이 파일은 컴퓨터의 로컬하드 드라이브에 저장되며 Exchange 서버와의 연결이 불가능한
경우 오프라인 모드에서도 작업 가능

제4장

1. 논리적 디스크 쓰기금지

* Windows 레지스트리 편집기를 이용한 쓰기 방지

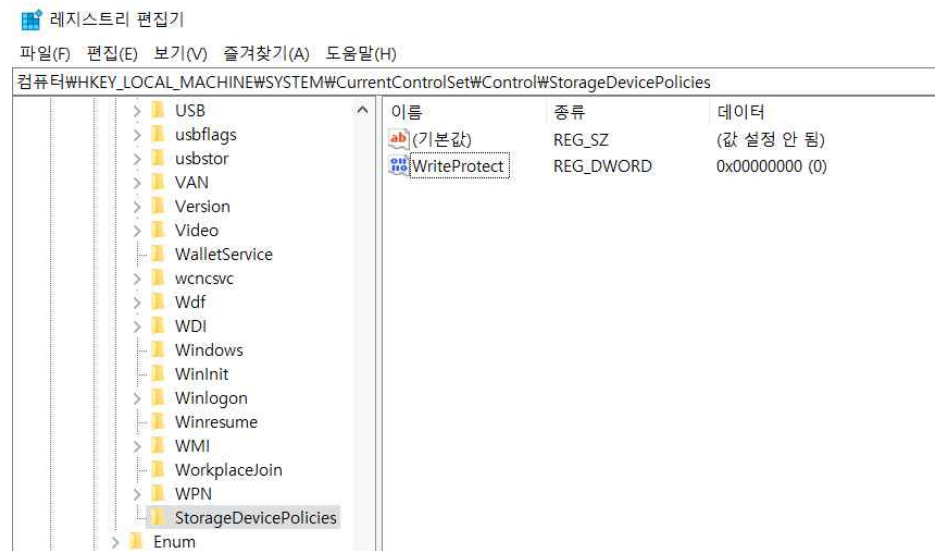
1) 레지스트리 편집기 실행



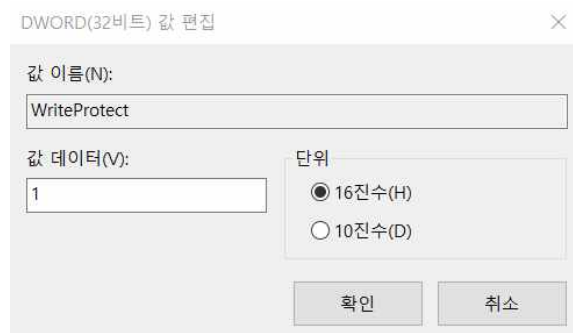
2) HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control 우 클릭 - 새로 만들기 - 키 선택하여 StorageDevicePolicies 생성



3) StorageDevicePolicies 우 클릭 - 새로 만들기 - DWORD 선택해 WriteProtect 생성



4) 값 데이터 : 쓰기방지 해지(0x00000000) / 쓰기방지 설정(0x00000001)

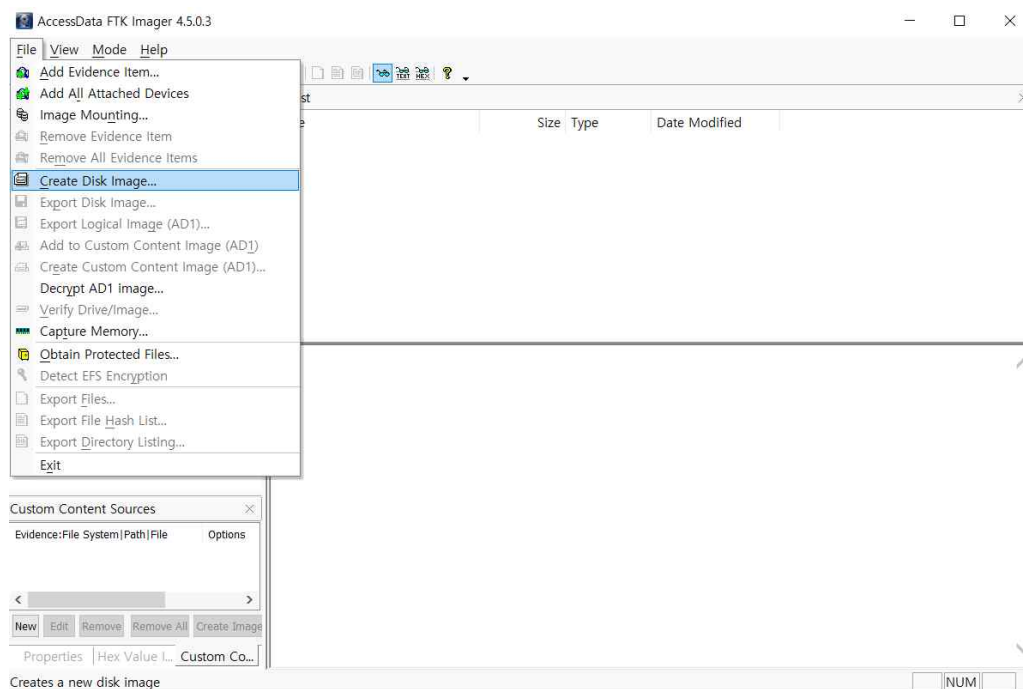


5) 이미 장착되어 있는 USB는 쓰기방지 설정이 적용되지 않음,
분석용 USB는 레지스트리 수정 후에 장착

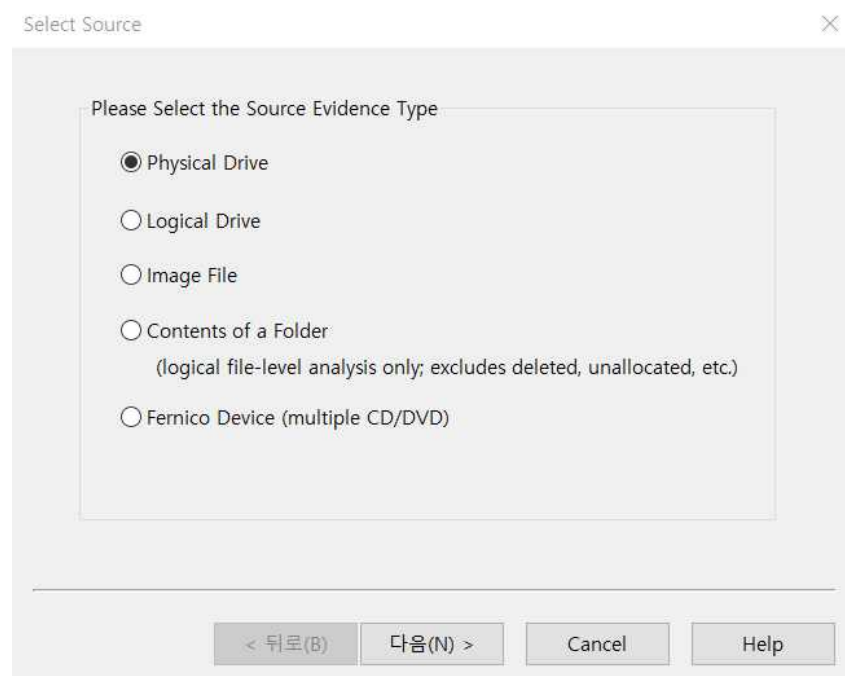
2. 사본이미지 생성

* FTK Imager를 사용한 사본이미지 생성

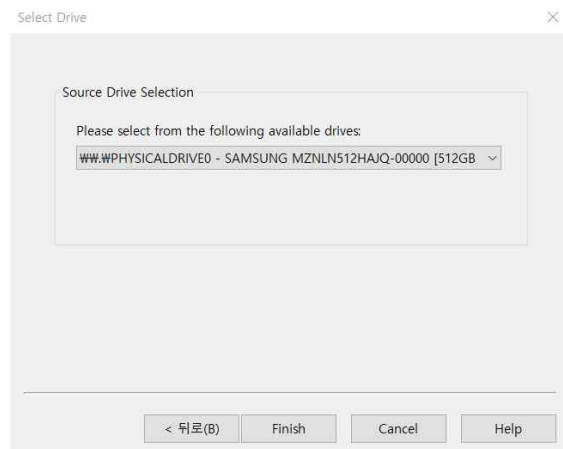
1) FTK Imager - Create Disk Image 실행



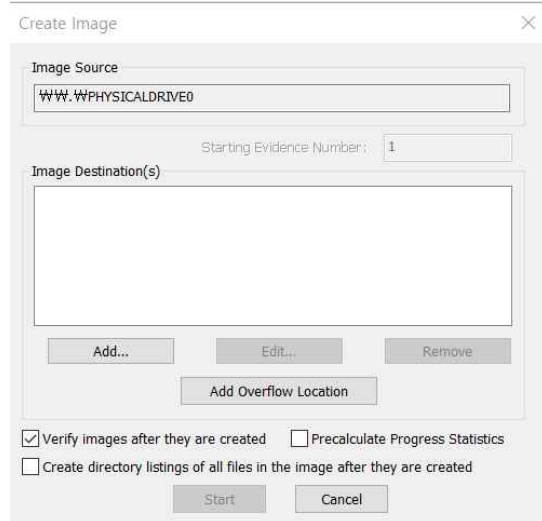
2) 물리적 드라이브를 선택해 원본 매체 전체를 사본이미지 생성



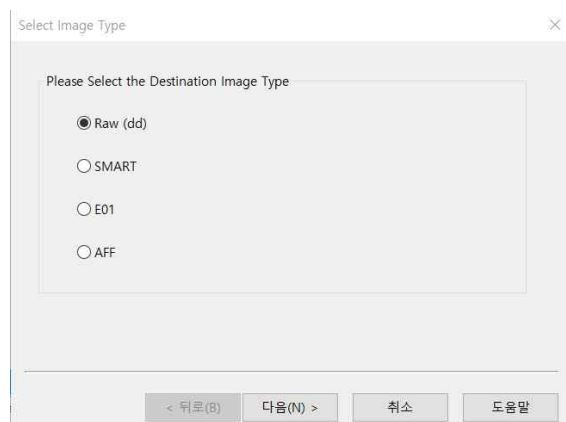
3) 분석대상 USB 선택



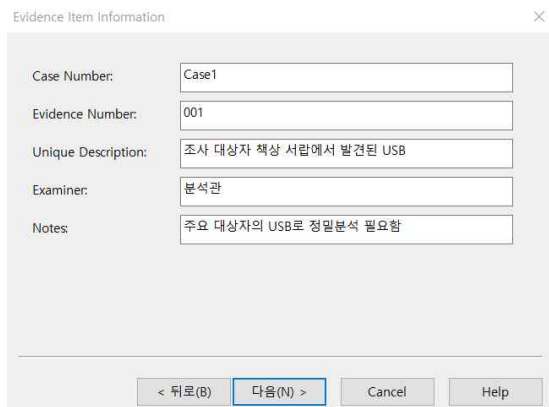
4) Add 버튼을 눌러 이미지 타입 선택



5) 경우에 따라 파일 시스템이 손상되거나 조작되어 있으면 원시(dd) 방식으로 덤프 (이미지 타입은 통상적으로 E01을 선택)



6) 기본 정보를 입력, 내용 기재안해도 상관 없음



Evidence Item Information

Case Number: Case1

Evidence Number: 001

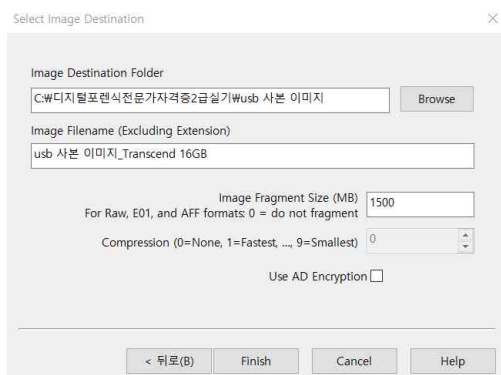
Unique Description: 조사 대상자 책상 서랍에서 발견된 USB

Examiner: 분석관

Notes: 주요 대상자의 USB로 정밀분석 필요함

< 뒤로(B) 다음(N) > Cancel Help

7) 사본이미지가 저장될 경로, 파일명 지정, Fragment Size 설정
(0으로 설정하면 단일 파일로 생성)



Select Image Destination

Image Destination Folder: C:\디지털포렌식전문가자격증2급실기\usb 사본 이미지 Browse

Image Filename (Excluding Extension): usb 사본 이미지_Transcend 16GB

Image Fragment Size (MB): 1500
For Raw, E01, and AFF formats: 0 = do not fragment

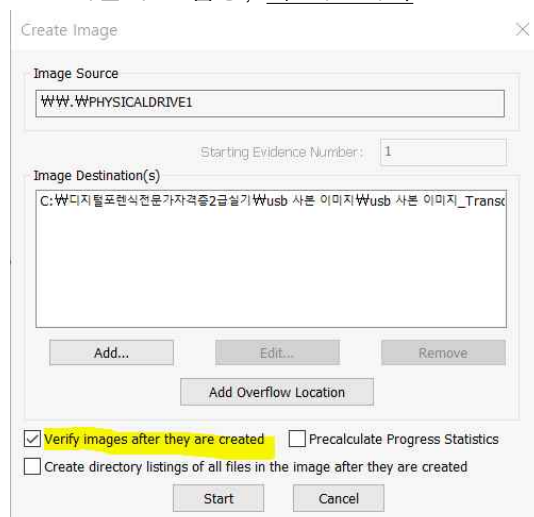
Compression (0=None, 1=Fastest, ..., 9=Smallest): 0

Use AD Encryption ☐

< 뒤로(B) Finish Cancel Help

8) 시작 누르면 사본이미지 생성됨

‘이미지 작성 후 이미지 확인 옵션’ 체크 시 사본이미지 생성 후에 해시값을 한번 더
계산하고 검증, 꼭 체크하기



Create Image

Image Source: \\W.W\PHYSICALDRIVE1

Starting Evidence Number: 1

Image Destination(s): C:\디지털포렌식전문가자격증2급실기\usb 사본 이미지\usb 사본 이미지_Transcend 16GB

Add... Edit... Remove

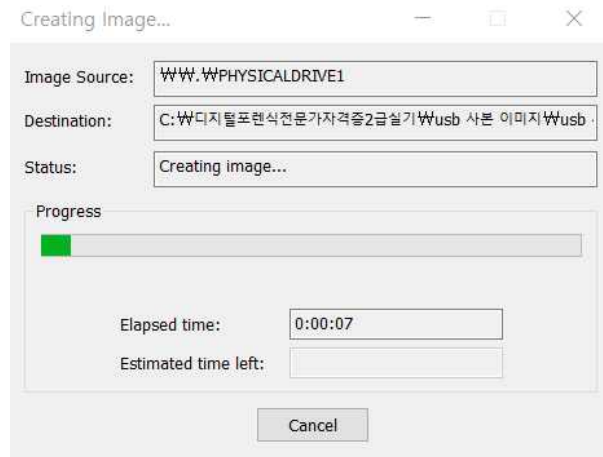
Add Overflow Location

☒ Verify images after they are created ☐ Precalculate Progress Statistics

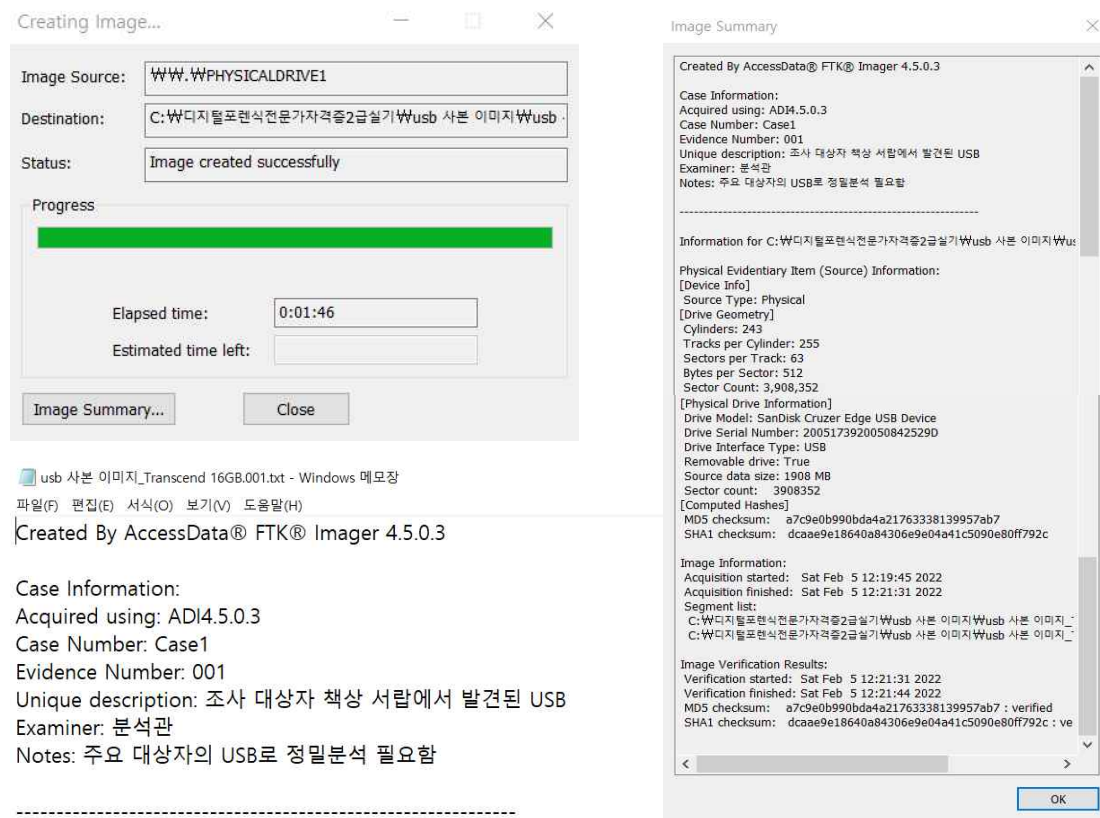
☐ Create directory listings of all files in the image after they are created



Start Cancel

9) 사본이미지 생성 진행 화면



10) 사본이미지 생성 완료후 ‘Image Summary’누르거나
사본이미지 생성 디렉토리에 있는 txt파일에서 정보확인 가능
(사본이미지의 해시값은 MD5, SHA1 알고리즘으로 생성)



이름	수정한 날짜	유형	크기
 usb 사본 이미지_Transcend 16GB.001	2022-02-05 오후 12:21	압축(.001) 파일	1,536,000KB
 usb 사본 이미지_Transcend 16GB.001.txt	2022-02-05 오후 12:21	텍스트 문서	2KB
 usb 사본 이미지_Transcend 16GB.002	2022-02-05 오후 12:21	002 파일	418.176KB