1. 디스크 이미징 이란? + 메모리 덤프란? (두개의 차이점도 작성)

디스크 이미징은 저장 장치의 모든 데이터를 그대로 복사하여 동일한 상태의 디스크 이미지를 생성하는 과정. 디스크의 모든 섹터를 복사하기에 숨겨진 파일이나 삭제된 데이터까지 포함 가능. 다라 데이터 보존 및 복구를 위해 활용되는 강력한 기술.

	디스크 이미징	**디스크 복제**
복사 방식	디스크 전체를 하나의 이미지 파일로 저장	원본 디스크를 새로운 디스크로 복제,
데이터 저장 형태	단일 이미지 파일	별도의 저장 장치에 복제
백업 및 보존	데이터 보관 및 복원 용이	즉시 사용 가능한 형태로 저장
포렌식 분석 가능	삭제된 파일, 숨겨진 데이터 포함	원본 디스크와 동일한 상태 유지

(활용 사례)

디지털 포렌식	범죄 수사 및 법적 증거 분석
데이터 백업	전체 디스크 데이터를 백업하여 데이터 손실 방지
시스템 복구	운영 체제 및 설정을 포함한 복구용 이미지 생성
보안 분석	악성코드 및 랜섬웨어 감염 분석
데이터 마이그레이션	새로운 디스크로 데이터 이전

(과정)

1. 디스크 준비: 원본 디스크와 저장할 공간을 준비
2. 이미징 소프트웨어 실행: 전용 소프트웨어를 사용하여 디스크 이미징 수행
3. 이미지 저장 및 검증: 이미지 파일을 저장하고 무결성 검사 수행
4. 복구 및 분석: 필요 시 이미지를 이용하여 데이터 복구 또는 분석 진행

(도구)

Clonezilla	오픈소스 기반 디스크 복제 및 백업 도구
Acronis True Image	강력한 백업 및 복구 기능을 제공하는 상용 소프트웨어
Macrium Reflect	빠르고 안정적인 디스크 이미징 및 복구 지원
FTK Imager	디지털 포렌식 분석에 사용되는 전문적인 디스크 이미징 도구
dd(Linux 명령어)	리눅스에서 사용되는 기본적인

	디스크 이미징 명령어

(장점)

- 전체 데이터 보존 : 삭제된 데이터가지 포함하여 원본을 완전히 사용 가능
- 빠른 복구 가능 : 시스템 장애 발생 시 신속한 복구 가능
- 법적 증거 보존 : 법적 절차에서 증거로 활용 가능
- 멀티 플랫폼 지원 : 다양한 운영 체제에서 활용 가능

(단점)

- 대용량 저장 공간 필요 : 전체 디스크를 복사하기에 큰 저장 공간 필요
- 시간 소요 : 디스크 크기에 따라 이미지 생성 시간이 오래 걸릴 가능성 존재
- 보안 위험 : 디스크 이미지가 유출될 경우 민감한 정보가 노출될 가능성

*쓰기방지

원본을 반드시 “읽기 전용”으로 연결. 이미징 장비나 소프트웨어에서 읽기 행위만을 수행하도록 지정한다고 해도 펌웨어나 운영체제의 동작 과정에서 언제, 어떻게 원본 디스크에 영향을 주는 행위가 발생할 지는 예측 불가능.

메모리 덤프는 메모리에 저장된 휘발성 데이터를 비휘발성 데이터로 저장한 데이터. 메모리에 저장된 데이터는 시간의 경과에 따라서 실시간으로 변화, 수행한 시각에 저장되어 있는 데이터만이 메모리 덤프의 결과.

2. 윈도우 아티팩트 조사

윈도우 시스템에서는 다양한 이벤트와 활동의 결과로 데이터 파일 또는 기타 유형의 파일 생성. 이런 파일을 윈도우 아티팩트, 일반적으로 불필요하거나 정리해야 할 대상으로 간주. 아티팩트는 프로그램 실행, 시스템 업데이트, 파일 복사 및 이동, 프로세스 종료 등 다양한 상황에서 생성 가능.

3. 웹 포렌식이란? + 웹 아티팩트 조사 (Cache, History, Cookie, Download List)

웹 포렌식은 웹 브라우저를 통해 생기는 아티팩트들을 수집하고 분석하는 것. 웹 로그를 통해 분석하는 과정.

웹 브라우저 : 웹 서버에서 쌍방향 통신하는 HTML문

서나 파일과 연동하고 출력하는 응용 소프트웨어.

Cache : 웹 사이트 접속 시 방문 사이트로부터 데이터를 자동으로 다운받는 데이터. 이를 통해 재접속 시 다시 다운받지 않고 다운 받았던 데이터를 통해 빠르게 접근 가능. 이미지파일, 텍스트파일, 아이콘 HTML파일, XML파일, 스크립트 등. / 다운로드 URL, 다운로드 시간, Cache 데이터 파일명, Cache 데이터 크기, Cache 데이터 위치 등의 정보 확보 가능. Html 형태로 저장된 캐시의 경우 메일 본문의 가능성이 존재, 바로 열어보기 가능

(Internet Explorer) 다운로드된 캐시는 Temporary Internet 파일 형태로 저장되며 index.dat 파일은 해당 폴더 내 파일들의 Cache 인덱스를 저장. 수집 방법으로는 Content.IE5 폴더 아래, index.dat을 수집하거나 Content.IE5 아래의 모든 폴더를 수집하는 방식.

(Chrome) 캐시 정보의 경우 'data_0' 파일에 데이터 인덱스 정보를 data_1, data_2, data_3 파일과 나머지 파일에 캐시 데이터가 저장, 수집 방법으로 Cache 폴더 아래 모든 파일을 수집.

(Firefox) Cache Map File, Separate Cache Data Files, Three Cache Block Files와 같이 3가지 구조로 구성. Cache Map File(_CACHE_)에는 각 Cache 인덱스 정보가 저장, 이러한 인덱스 정보를 바탕으로 Meta 데이터와 Separate Cache Data Files와 Three Cache Bloch Files에 저장. 수집 방법으로 Cache 폴더 아래, _CACHE_MAP_, _CACHE_001_, _CACHE_002_, _CACHE_003_ 파일 수집하거나 Cache 포더 아래, 모든 폴더 수집을 수집.

(Safari) 데이터, 인덱스 정보 모두 SQLite Database인 Cache.db 파일에 저장. 수집 방법으로 Safari 폴더 아래, Cache.db 파일을 수집.

(Opera) 인덱스 정보는 dcache4.url 파일에 저장, 데이터 정보는 cache 폴더 아래, 각 서브 폴더에 파일 형태로 저장. 수집 방법으로 cache 폴더 아래, dcache4.url 파일 수집하거나 cache 폴더 아래, 모든 서브 폴더 수집을 수집.

History : 사용자가 방문한 웹 사이트의 접속 정보. 사용자의 편의를 위해서 제공된 것으로 예전에 방문한 사이트를 다시 방문하고자 할 때 원별이나 일별 목록으로 확인을 통해 접근 가능. URL 입력창에 직접 주소를 입력하는 직접 접근과 링크를 통해 접근하는 간접 접근 형식으로 분류. / 방문사이트 URL, 방문 시간, 방문 횟수, 웹 페이지 제목 등의 정보 확보 가능. 방문 URL 내에 GET 방식으로 포함된 인자값을 분석하여 검색어 정보와 아이디, 패스워드 추출 가능.

(Internet Explorer) History.IE5 폴더 아래에 index.dat 파일의 형태로 저장. 해당 폴더 안에는 다른 폴더들이 존재하는데 해당 기간에 속한 히스토리의 정보 포함. 수집 방법으로 index.dat 파일을 수집하거나 폴더 안에 있는 서브 폴더까지 함께 수집하는 방법.

(Chrome) SQLite Database 파일 형태로 각각 저장되며 History 정보의 경우 History에 저장. 월별 정보가 'History Index 〈년-월〉' SQLite 파일로 저장, 수집 방법으로 Default 폴더 아래, History, history Index 〈년-월〉, Cookie 파일 수집.

(Firefox) SQLite Database 파일 형태로 각각 저장. places.sqlite에 저장, 수집 방법은 〈Random〉.default 아래 places.sqlite 파일을 수집.

(Safari) 데이터, 인덱스 정보 모두 SQLite Database인 Cache.db 파일에 저장, 정보는 Plist 파일 형태로 History.plist에 저장. 수집 방법으로 Safari 폴더 아래, Cache.db 파일을 수집, Safari 폴더 아래 History.plist 파일 수집.

(Opera) global_history.dat에 저장. 수집 방법으로 Opera 폴더 아래의 각 파일들을 수집.

Cookie : 웹 사이트에서 사용자의 하드디스크에 저장 시켜놓는 사용자에 관한 데이터. 웹 사이트에서 사용자별 서비스를 제공하기 위해 사용. 자동 로그인 기능, 쇼핑몰 사이트의 장바구니 등의 기능을 사용하는데 활용. / 호스트, 경로, 쿠키 수정 시간, 쿠키 만료 시간, 이름, 값 등의 정보 확보 가능. 경로를 통해 사용한 서비스를 유추가 가능, 쿠키 수정시간을 통해 해당 사이트에 마지막으로 접속한 시간 확인 가능. 이름이나 값을 통해 로그인 아이디 정보에 획득이 가능, 사용자의 Unique ID등을 확인 가능.

(Internet Explorer) 실제 쿠키 정보는 계정명@호스트명.txt 형식의 쿠키 파일 안에 저장, index.dat 파일은 쿠키 파일들의 인덱스 정보를 저장. 수집 방법으로 Cookies 폴더 아래 index.dat를 수집하거나 폴더 아래의 모든 텍스트 파일을 수집하는 방법.

(Chrome) SQLite Database 파일 형태로 각각 저장되며 Cookie 정보는 Cookie에 저장. 수집 방법으로 Default 폴더 아래, History, history Index 〈년-월〉, Cookie 파일 수집.

(Firefox) SQLite Database 파일 형태로 각각 저장. cookies.sqlite에 저장, 수집 방법은 〈Random〉.default 아래 cookies.sqlite 파일을 수집.

(Safari) 데이터, 인덱스 정보 모두 SQLite Database인 Cache.db 파일에 저장, 정보는 Plist 파일 형태로 Cookies.plist에 저장. 수집 방법으로 Safari 폴더 아래, Cache.db 파일을 수집, Safari 폴더 아래 Cookies.plist 파일 수집.

(Opera) cookies4.dat에 저장. 수집 방법으로 Opera 폴더 아래의 각 파일들을 수집.

Download List : 사용자가 의도적으로 선택해서 자신의 컴퓨터로 내려 받은 파일에 대한 정보를 리스트화 해놓은 것. 사용자의 의도와는 관계없이 받아지는 캐시와는 구분 되는 것으로 사용자의 편의를 위하여 제공되는 기능. 목록을 통해 이미 다운 받았던 파일을 다시 다운 받기 가능. / 파일의 저장 경로, 소스 URL, 파일 크기, 다운로드 시간, 다운로드 성공 여부 등의 정보 확보 가능.

(Internet Explorer) IE 9 이후부터 존재하는 기능, IEDownloadhistory 폴더 아래 index.dat 수집하면 됨.

(Chrome) SQLite Database 파일 형태로 각각 저장되며 Download 정보의 경우 History에 같이 저장. History 정보와 함께 'History' SQLite 파일 안에 저장. 수집 방법으로 Default 폴더 아래, History, history Index <년-월>, Cookie 파일 수집.

(Firefox) SQLite Database 파일 형태로 각각 저장. downloads.sqlite에 저장, 수집 방법은 <Random>/default 아래 downloads.sqlite 파일을 수집.

(Safari) 데이터, 인덱스 정보 모두 SQLite Database인 Cache.db 파일에 저장, 정보는 Plist 파일 형태로 Downloads.plist에 저장. 수집 방법으로 Safari 폴더 아래, Cache.db 파일을 수집, Safari 폴더 아래 Downloads.plist 파일 수집.

(Opera) download.dat에 저장. 수집 방법으로 Opera 폴더 아래의 각 파일들을 수집.

OS 버전	정보	경로
Windows 2000, XP	Cache	%Profile%₩Local Settings₩Temporary Internet Files₩Content.IE5₩index.dat %Profile%₩Local Settings₩Temporary Internet Files₩Content.IE5₩<Random>₩<모든 파일>
	History	%Profile%₩Local Settings₩History₩History.IE5₩index.dat %Profile%₩Local Settings₩History₩History.IE5₩<기간>₩index.dat
	Cookie	%Profile%₩Cookies₩index.dat %Profile%₩Cookies₩<모든 텍스트 파일>
	download	없음
Windows Vista, 7	Cache	%Profile%₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩Content.IE5₩index.dat %Profile%₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩Content.IE5₩<Random>₩<모든 파일>
	History	%Profile%₩AppData₩Local₩Microsoft₩Windows₩History₩History.IE5₩index.dat %Profile%₩AppData₩Local₩Microsoft₩Windows₩History₩History.IE5₩<기간>₩index.dat
	Cookie	%Profile%₩AppData₩Roaming₩Microsoft₩Windows₩Cookies₩index.dat %Profile%₩AppData₩Roaming₩Microsoft₩Windows₩Cookies₩<모든 텍스트 파일>
	download	%Profile%₩AppData₩Roaming₩Microsoft₩Windows₩IEDownloadHistory₩index.dat (IE 9 부터 존재)

OS 버전	정보	경로
Windows 2000, XP	Cache	%Profile%₩Local Settings₩Application Data₩Google₩Chrome₩User Data₩Default₩Cache₩<모든 파일>
	History	%Profile%₩Local Settings₩Application Data₩Google₩Chrome₩User Data₩Default₩History %Profile%₩Local Settings₩Application Data₩Google₩Chrome₩User Data₩Default₩History Index <년-월>
	Cookie	%Profile%₩Local Settings₩Application Data₩Google₩Chrome₩User Data₩Default₩Cookies
	download	%Profile%₩Local Settings₩Application Data₩Google₩Chrome₩User Data₩Default₩History
Windows Vista, 7	Cache	%Profile%₩AppData\Local\Google\Chrome\User Data\Default\Cache\
	History	%Profile%₩AppData₩Local₩Google₩Chrome₩User Data₩Default₩History %Profile%₩AppData₩Local₩Google₩Chrome₩User Data₩Default₩History₩History Index <년-월>
	Cookie	%Profile%₩AppData₩Local₩Google₩Chrome₩User Data₩Default₩Cookies
	download	%Profile%₩AppData₩Local₩Google₩Chrome₩User Data₩Default₩History

OS 버전	정보	경로
Windows 2000, XP	Cache	%Profile%₩Local Settings₩Application Data₩Mozilla₩Firefox₩Profiles₩<Random>.default₩Cache₩_CACHE_MAP_ 외 3개 파일 %Profile%₩Local Settings₩Application Data₩Mozilla₩Firefox₩Profiles₩<Random>.default₩Cache₩<모든 폴더>
	History	%Profile%₩Application Data₩Mozilla₩Firefox₩Profiles₩<Random>.default₩places.sqlite
	Cookie	%Profile%₩Application Data₩Mozilla₩Firefox₩Profiles₩<Random>.default₩cookies.sqlite
	download	%Profile%₩Application Data₩Mozilla₩Firefox₩Profiles₩<Random>.default₩downloads.sqlite
Windows Vista, 7	Cache	%Profile%\AppData\Local\Mozilla\Firefox\Profiles\<Random>\Cache_CACHE_MAP_(같은 폴더 안의 모든 파일 필요)
	History	%Profile%\AppData\Roaming\Mozilla\Firefox\Profiles\<Random>.default\places.sqlite
	Cookie	%Profile%\AppData\Roaming\Mozilla\Firefox\Profiles\<Random>.default\cookies.sqlite
	download	%Profile%₩AppData₩Roaming₩Mozilla₩Firefox₩Profiles₩<Random>.default₩download.sqlite

OS 버전	정보	경로
Windows 2000, XP	Cache	%Profile%₩Local Settings₩Application Data₩Apple Computer₩Safari₩Cache.db
	History	%Profile%₩Application Data₩Apple Computer₩Safari₩History.plist
	Cookie	%Profile%₩Application Data₩Apple Computer₩Safari₩Cookies₩Cookies.plist
	download	%Profile%₩Application Data₩Apple Computer₩Safari₩Downloads.plist
Windows Vista, 7	Cache	%Profile%₩AppData₩Local₩Apple Computer₩Safari₩Cache.db
	History	%Profile%₩AppData₩Roaming₩Apple Computer₩Safari₩History.plist
	Cookie	%Profile%₩AppData₩Roaming₩Apple Computer₩Safari₩Cookies₩Cookies.plist
	download	%Profile%₩AppData₩Roaming₩Apple Computer₩Safari₩Downloads.plist

OS 버전	정보	경로
Windows 2000, XP	Cache	%Profile%₩Local Settings₩Application Data₩Opera₩Opera₩cache₩dcache4.url
	History	%Profile%₩Application Data₩Opera₩Opera₩global_history.dat
	Cookie	%Profile%₩Application Data₩Opera₩Opera₩cookies4.dat
	download	%Profile%₩Application Data₩Opera₩Opera₩download.dat
Windows Vista, 7	Cache	%Profile%₩AppData₩Local₩Opera₩Opera₩cache₩dcache4.url
	History	%Profile%₩AppData₩Roaming₩Opera₩Opera₩global_history.dat
	Cookie	%Profile%₩AppData₩Roaming₩Opera₩Opera₩cookies4.dat
	download	%Profile%₩AppData₩Roaming₩Opera₩Opera₩download.dat