[DiFoni Study-3주차]

1.디스크이미징•메모리덤프

•디스크이미징: 저장장치의 모든 물리적 데이터를 파일 형태로 만드는 작업을 의미. 파일 복사 시 디스크의 모든 섹터를 복사하여 포렌식 분석, 데이터 백업 및 시스템 복구에 적합.

•메모리덤프: RAM에 저장되어 있는 데이터를 특정 시점에 메모리에 파일로 저장. 컴퓨터 오류의 원인 분석, 보안 취약점에 활용.

	디스크이미징	**메모리덤프**
대상 저장장치	비휘발성 저장장치	RAM에서 실행 중인 데이터 휘발성 정보
백업 목적	시스템,데이터 백업 장애 복구, 증거 보존	오류 원인 분석 침해사고 대응
백업/복구	전체 백업, 포맷 완벽 복구 가능	특정 시점의 상태 스냅샷 시스템 복구 직접 활용 부적합
복사 방식	바이트 단위, 섹터 단위 전체 복제	RAM 메모리 영역 전체 스냅샷 파일로 저장
데이터 변경 여부	정적데이터	동적데이터
데이터 보존	모든 데이터 원본 보존 (삭제,숨김,포맷된 파일 포함)	실시간 메모리 정보 보존 (암호화 키, 프로세스)
도구	FTK imager, Autopsy 등	Voiatility, FTK imager, HxD 등

•디스크이미징 과정(FTK imager 툴 사용)	**•메모리덤프 과정(FTK imager 툴 사용)**
1) 이미징 할 디스크 생성 2) 증거 수집 형태 선택 (대부분 물리적 디스크에서 이미징 수행) - Physical drive : 모든 디스크를 이미징 - Logical drive : 파디션, 부분적인 디스크 이미징 3) 이미징 수행하려는 물리디스크 선택 4)이미징할 디스크 이미지 파일 종류 선택 5)사건번호, 증거번호, 분석가 이름 등 정보 입력 6)이미징 후 이미징 된 디스크 저장 위치, 이름 저장 7)모든 설정 완료->start	1)파일->capture memory 선택 2)덤프 파일을 저장할 경로, 파일명 지정 3)옵션 선택 4)capture memory 버튼 클릭->현재 시스템 RAM 내용을 파일로 저장 5)설정 경로에 메모리 덤프 생성 6)Volatility 도구로 분석 가능

2.윈도우 아티팩트 조사

:윈도우 운영체제와 관련된 다양한 기능, 프로그램 사용하면서 자동으로 생성되는 흔적을 말한다.

윈도우 운영체제는 사용자의 활동을 다양한 파일과 로그로 기록하며 포렌식 도구들을 통해 추출, 분석되어 사용자 행위의 타임라인을 재구성하거나, 시스템 침해 사고 조사, 악성코드 활동 추적, 증거보존 등에 활용.

- 대표적인 윈도우 아티팩트

:레지스트리, 프리페치, 로그파일

점프리스트 등

3.웹 포렌식, 웹 아티팩트 조사 (캐시, 역사, 쿠키, 다운로드 목록)

•웹 포렌식: 웹 브라우저, 웹 서버 등에 남겨진 아티팩트를 수집, 분석하여 필요한 증거를 찾는 과정

1)Cache

• 웹 사이트 접속 시, 방문 사이트의 데이터를 자동으로 다운로드하는 데이터로, 기존에 방문했던 웹 사이트를 재방문하면 기존에 다운로드 했던 데이터는 다시 로딩하지 않고 캐시에서 불러 접근 속도를 높인다.

2)History

•사용자가 방문한 웹사이트의 접속 정보로, 웹사이트 방문 시 웹사이트 정보를 분류하여 저장한다.

3)Cookie

•웹사이트에서 사용자의 하드디스크에 저장시켜 놓는 사용자에 관한 데이터이며, HTTP 통신에서 접속 상태를 유지할 수 있도록 사용자의 정보를 잠시 저장해두는 임시장소를 말한다.

4)Dowload list

•사용자가 임의로 선택하여 다운로드 한 파일을 말하며, 다운로드 된 파일들과 구분된다.

5)웹 브라우저에 따른 로그파일의 경로

•internet explorer

-index.dat 로그 파일 구조

-경로를 살펴보면 download list를 제외한 나머지는 index.dat과 동시에 다른 파일들도 포함하고 있다.

Artifacts	Path
History	C:\Users\[Uername]\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat C:\Users\[Uername]\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist##################\index.dat
Cache	C:\Users\[Uername]\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat C:\Users\[Uername]\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5*.*
Cookie	C:\Users\[Uername]\AppData\Roaming\Microsoft\Windows\Cookies\index.dat C:\Users\[Uername]\AppData\Roaming\Microsoft\Windows\Cookies\
download list	C:\Users\[Uername]\AppData\Roaming\Microsoft\Windows\IEDownloadHistory\index.dat
관련 툴	
[Public] Web Browser IECookiesView IEHistoryView IECacheView MyLastSearch BrowsingHistoryView WEFA	

•microsoft edge

-WebCacheV01.dat 파일 저장

-ESE Database구조

Artifacts	Path
Database URL, History	C:\Users\[Uername]\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat
Cache	C:\Users\[Username]\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb38bbwe\AC\#!xxx17)\MicrosoftEdge\Cache\
Cookie	C:\Users\[Username]\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb38bbwe\AC\#!xxx\MicrosoftEdge\Cookies\
Temporary Files	C:\Users\[Username]\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb38bbwe\AC\Temp
Recovery.dat	C:\Users\[Username]\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb38bbwe\AC\MicrosoftEdge\User\Default\Recovery\Activ

•Chrome

-Cache 제외 SQLite Database 형태 저장

-History 데이터베이스 안에 download list 정보 포함

-Cache는 **data_x** 파일 저장

Artifacts	Path
History(download list)	C:\Users\[Uername]\AppData\Local\Google\Chrome\User Data\Default\History C:\Users\[Uername]\AppData\Local\Google\Chrome\User Data\Default\History\History Index
Cache	C:\Users\[Uername]\AppData\Local\Google\Chrome\User Data\Default\Cache
Cookie	C:\Users\[Username]\AppData\Local\Google\Chrome\User Data\Default\Cookies
관련 툴	
[Public] Web Browser ChromeHistoryView ChromeCacheView MyLastSearch BrowsingHistoryView WEFA	

•Firefox

-Cache 제외한 데이터들이 SQLite database(sqlite) 파일로 존재

Artifacts	Path
History	C:\Users\[Uername]\AppData\Roaming\Mozilla\Firefox\Profiles\.default\places.sqlite
Cache	C:\Users\[Username]\AppData\Local\Mozilla\Firefox\Profiles\\Cache_CACHE_MAP_XXX
Cookie	C:\Users\[Username]\AppData\Roaming\Mozilla\Firefox\Profiles\.default\cookies.sqlite
download list	C:\Users\[Username]\AppData\Roaming\Mozilla\Firefox\Profiles\.default\download.sqlite
관련 툴	
[Public] Web Browser MozillaCookieView MozillaHistoryView MozillaCacheView MyLastSearch BrowsingHistoryView WEFA	

•Safari

-Chrome과 FireFox와는 반대로 Cache 파일이 SQLite Database 형태로 존재

Artifacts	Path
Database URL, History	C:\Users\[Uername]\AppData\Roaming\Apple Computer\Safari\History.plist
Cache	C:\Users\[Username]\AppData\Local\Apple Computer\Safari\Cache.db
Cookie	C:\Users\[Username]\AppData\Roaming\Apple Computer\Safari\Cookies\Cookies.plist
download list	C:\Users\[Username]\AppData\Roaming\Apple Computer\Safari\Downloads.plist
관련 툴	
[Public] Web Browser SafariHistoryView SafariCacheView MyLastSearch BrowsingHistoryView WEFA	

•Opera

-Cache 제외한 데이터들이 .dat 파일로 저장

Artifacts	Path
History	C:\Users\[Uername]\AppData\Roaming\Opera\Opera\global_history.dat
Cache	C:\Users\[Username]\AppData\Local\Opera\Opera\cache\dcache4.url
Cookie	C:\Users\[Username]\AppData\Roaming\Opera\Opera\cookies4.dat
download list	C:\Users\[Username]\AppData\Roaming\Opera\Opera\download.dat
관련 툴	
[Public] Web Browser OperaCacheview WEFA	