**안티 포렌식 분석 보고서**

**분석자 : 박지원**

**디지털 포렌식 분석 보고서**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **접수일자** | | 2022.06.03 | | | | |
| **분석번호** | | 20220603 | | | | |
| **관리번호** | | 2022.06.03 | | | | |
| **분석대상** | **분석기간** | 2022.05.30 17:50~2022.06.03 15:30 | | | | |
| **분석자(소속)** | 박지원 (백석대학교 정보보호학과) | | | | |
| **분석장소** | 자택 | | | | |
| **분석대상** | UTM 내 windows | | | | |
| **요청사항** | **요청기관** | 백석대학교 디지털 포렌식스 교수님 | | | | |
| **요청사항** | 가상화 시스템을 이용한 윈도우 설치 후 부팅하고 정상적인 사용 이후에 디지털 증거 분석을 통해 사용과정을 추정한 것을 분석 | | | | |
| **분석결과** | **분석대상** | UTM 내의 windows 파일 | | | | |
| **분석도구** |  | | | | |
| **분석내용** | **No** | **구분** | **Before** | **After** | **비고** |
| A |  |  |  |  |
| B |  |  |  |  |
| C |  |  |  |  |
| D |  |  |  |  |
| E |  |  |  |  |
| F |  |  |  |  |
| G |  |  |  |  |
| ※ 상세 분석 내용 참조 | | | | | |

**별첨1. 분석번호(2019관리-제13호) 상세 분석 내용**

**1. 디지털 저장매체/기기 정보**

A. 외관 상태

- 가상 시스템으로 겉으로 보여지는 외관은 없으나

해당 가상 시스템을 실행하는 노트북의 상태로 서술.

- 외관상 특이사항 없음

B. 하드디스크 정보

- 모델명/시리얼 번호 : macOS Monterey ver 12.2.1

- 용량 : 512GB

- 칩 : apple M1

C. 휘발성 수집 단계

- USB 내의 파일들은 휘발성이 있기 때문에 복제해 원본 파일을 건들지 않고 사본 파일로 로그 및 정보를 수집하고자 함.

**3. 분석 도구**

A. 분석용 컴퓨터 주요 정보 : 위의 디지털 저장매체와 정보 동일함.

- 운영체제(OS)/모델 : Unix / MacBook Air (M1,2020)

- CPU/MB : M1

- HDD1/2 : FVFHM0G7Q6M1

- RAM : 자체 내장 16GB

- 네트워크와 분리하여 독립적으로 운영 및 분석 예정

B. 분석 도구/프로그램

- 파일 뷰어 : 위드용 프로그램, MS 오피스....

**4. 분석 방법 및 내용**

A. 표준시각과 시간 차이 확인

- 파일에 기록된 시각은 피감사자의 컴퓨터 시작을 변경하지 않는다는 가정 하에 분석하였으며 정확한 시간을 판단하기 위해서는 이미지를 생성한 컴퓨터 본체의 CMOS 시간을 대조하여 확인해야 함

B. 휘발성 자료 수집

- 원본 파일의 변형을 방지하고자 복제된 파일에서 정보를 수집함.

**5. 분석 과정**

**6. 분석 결과**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No** | **구분** | **Before** | **After** | **비고** |
| A |  |  |  |  |
| B |  |  |  |  |
| C |  |  |  |  |
| D |  |  |  |  |

A. 확장자 변경

- 분석 과정 및 결과 사진

B. 파일헤더 변경

- 분석 과정 및 결과 사진

**7. 분석 결과 요약**

작성일 : 2022.06.03

분석자 : 박 지 원 (인)