[DiFoni Study-1주차]

1.디지털 포렌식 유형

1)디스크 포렌식

•정의: 물리적인 저장장치 하드디스크, CD_ROM 등 각종 보조장치의 데이터를 수집하여 분석하는 기법

•방법: 피의자의 컴퓨터에서 물리적인 저장장치를 압수->사본제작->분석 실시 -> "원본=사본"임을 증명하기 위해 해시값을 통해 검증, 무결성 입증

•도구: FTK imager 등

2)인터넷 포렌식

•정의: www와 같은 인턴넷을 통해 응용 프로토콜을 사용하여 증거 수집하는 기법

•방법: 웹 브라우저 히스토리 분석(사이트 간 이동 기록 탐색 기능), 전자우편 헤더분석, IP추적 등 기술->증거 수집

•도구: forensic crane 등

3)모바일 포렌식

•정의: 모바일 장비들을 통해 데이터를 수집하여 분석하는 기법

•방법

3-1)비침습적 방법

-수동 추출: 터치패드, 키패드 사용 ->데이터 탐색

-논리적 추출: 케이블, 블루투스 등을 사용하여 모바일 장치와 포렌식 워크스테이션 간의 연결 설정

-JTAG: 암호화 상태의 소프트웨어로 모바일 장치에서도 데이터 추출 가능하게 함..

-헥스덤프: 플래시 메모리에 저장된 원시정보를 물리적으로 추출하는 방법

3-2)침습적 방법

-칩 오프: 칩을 기기에서 분리하고 칩 리더기를 사용->조사 중인 기기에 저장된 데이터 추출

-마이크로 읽기: 전자현미경의 렌즈를 통해 수동으로 관찰,데이터 분석

•도구: MD-NEXT, Autopsy 등

4)네트워크 포렌식

•정의: 네트워크를 통해 전송되는 패킷으로 데이터&암호 분석하여 조사하는 기법

•방법: 패킷을 실시간, 저장된 형태로 수집->헤더 분석->ip주소,프로토콜 통신 내용 등 이상 행동 탐지->로그분석->세션 재구성-> 이메일, 파일전송 내용 등 복원 ->흐름 분석->시간대별 네트워크 분석

•도구: Volatility 등

5)암호 포렌식

•정의: 암호화된 데이터에서 암호를 분석, 해독,복구하는 기법

•방법: 취약점 분석->키 저장 위치 탐색, 분석->암호키 해시 추출->복호화->복구데이터에 대한 무결성 검사

•도구: Hashcat 등

6)데이터베이스 포렌식

•정의: 데이터베이스 구조 및 저장된 데이터,메타데이터 수집,분석하는 기법.

•방법: 많은 양의 DB조사 증거 수집 계획->데이터베이스 종류 파악->데이터베이스 저장위치, 접근가능성 등 실사 파악->증거의 무결성 확보

•도구: Adminer 등

2.파일 시스템 개념&종류

•개념: 컴퓨터의 운영체제에서 저장장치에 있는 파일을 구성하고 데이터를 저장,탐색, 관리하기 위한 구조

-장점: 단순성, 데이터복구,호환성

-단점: 단편화,고급기능부족

•대표적인 종류

1)FAT: ms_dos/windows 주로 사용된 파일 시스템, 소형 장치나 플래시 메모리에서 주로 사용(FAT16,FAT32 버전o)

2)ext: 리눅스에서 주로 사용하는 파일 시스템(ext2,3,4 등 버전 o)

3)HFS+: macOS에서 사용하는 파일시스템, APFS의 도입으로 점자 대체

4)NTFS: windows에서 사용하는 최신 파일 시스템으로 다양한 고급 기능 지원

5) APFS: macOS, iOS에서 사용하는 최신 파일 시스템, 성능 향상, 데이터 무결성, 암호화 지원

3.해시란?&해시 함수 종류,의미

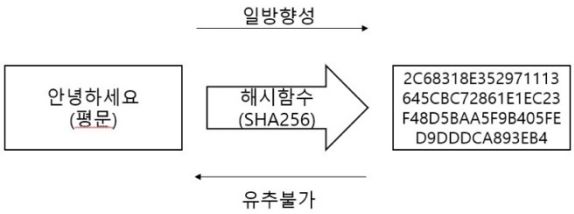
•해시란?

-다양한 길이를 가진 데이터를 고정된 길이를 가진 데이터로 출력한 값

-무결성, 보안성,데이터 저장 속도가 빠르다는 특징O

-원본 데이터를 해시함수로 암호화하여 암호문 생성->암호문 복호화

->원본 데이터 유추X



•해시함수 의미

-해시값은 항상 동일한 길이로 출력

-단방향성(역방향 추적 어려움.)

-충돌저항성O

-눈사태효과(입력 값이 조금만 바뀌어도 해시값이 달라진다.)

•해시함수 종류

1)MD5: 단방향 암호화 방식으로 128비트 해시 값을 생성하는 암호화 해시 함수로, 취약점이 발견되어 현재는 권장X

-입력 데이터 512비트 블록으로 나누기-> 패딩-> 512비트 배수로 맞추기->4개의 32비트 레지스터 초기화->각 블록 64번 라운드-> 해시함수를 통해 처리->최종적으로 레지스터를 이어붙여 128비트 해시 값 생성

2)SHA-1: 최대 2^64비트를 160비트의 해시값을 만든다.

-패딩과정이 MD5와 동일한 방식으로 적용되지만, 나머지 64비트를 big endian 패딩을 한다는 차이가 있음.

-패딩과정->초기 해시값 설정->512블록 32비트로 쪼갬, 80개 워드 생성->80번 반복 과정에서 새로운 해시값 생성 ->최종적으로 160비트-> 값 출력

3) SHA-2: 보안성이 강화된 해시 함수로 256비트 해시 값을 생성하여 현재 많은 시스템에서 표준으로 사용중

-패딩 -> 초기 해시 값 설정 -> 512비트 블록 32비트 워드 분할 및 80개 워드 확장 -> 80번 반복 계산 -> 최종 160비트 해시 값 생성 및 출력