정보보호론 #11

침해사고대응 및 디지털 포렌식

Prof. Byung Il Kwak

Review

- IoT 보안
- AI에 대한 이해
- AI의 취약점 유형과 대안
- AI를 이용한 보안

Contents

- 침해 대응
- 디지털 포렌식의 개념과 절차
- 디지털 포렌식의 증거 수집

CONTENTS

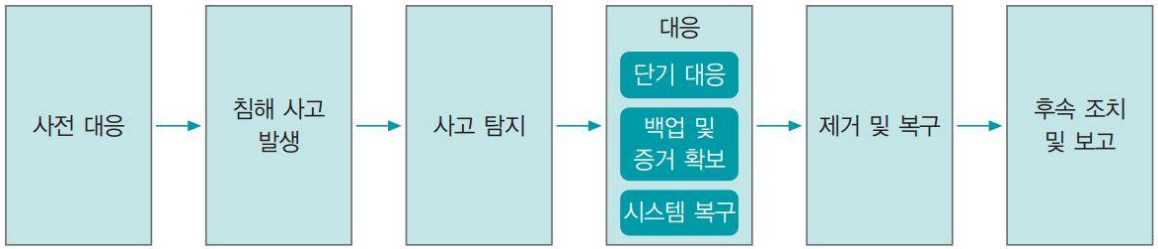
- 침해 대응

침해 대응

- CERT
  - 미국 국방부 고등연구계획국(DARPA)은 컴퓨터와 관련한 침해 사고에 대응하기 위해 CERT를 만듬
    - **CERT**: 범죄자나 의심스러운 사람이 건물에 들어오면 검사한 후 범죄자임이 확인되면 체포하는 건물 경비원과 유사한 역할
  - 정부는 물론이고 일반 기업에서도 CERT와 같은 보안팀을 필요로 함

침해 대응

- CERT
  - CERT의 침해 대응 절차



- 사전 대응
  - 기본적인 사전 대응은 침해 대응 체계를 구축하는 것
  - 이를 위해 가장 먼저 할 일은 CERT를 구성하는 것

침해 대응

- 사전 대응
  - CERT에 필요한 구성원
    - 시스템 운영 전문가
      - 침해 사고가 발생한 시스템의 효율적인 복구를 위해 서비스와 시스템의 관계를 명확하게 이해하고 조치를 취함
    - 대외 언론 및 외부 기관 대응 전문가
      - 침해 사고를 이해하고 언론 및 사이버안전국, 경찰에 적절한 방법으로 대응
    - 법률 팀
      - 침해 사고 대응 과정에서 법적인 문제가 발생했을 때 판단을 내리고 법적인 후속 절차를 밟음
    - 인사 팀
      - 조직 내 구성원의 권리와 책임을 파악하고 침해 사고 대응 과정에서 적절한 조직원을 찾도록 지원

침해 대응

- 사전 대응
  - 침해 사고의 위험 등급
    - 1등급 상황
      - 분산 서비스 거부 공격(DDoS)으로 정상 동작 불가능
      - 침입자에 의해 서버의 중요한 파일이 삭제
      - 악성 프로그램이 실행되어 정상적인 접근 제어에도 다른 경로를 통해 침입자가 지속적인 공격 시도
      - 침입자의 공격에 대한 대응 수단이 없는 경우
    - 2등급 상황
      - 비인가자에 의해 관리자 명령이 실행.
      - 시스템 자원을 불법적으로 사용하는 프로그램이 실행
      - 일반 사용자의 홈 디렉터리에 시스템 파일 존재
      - 일반적이지 않은 숨김 파일 또는 디렉터리 존재
      - 시스템 담당자가 알지 못하는 사용자가 추가 또는 사용자 권한이 임의로 변경
    - 3등급 상황
      - 외부 또는 내부에서 취약점 수집 행위가 계속 발견
      - 외부 또는 내부에서 불법적인 접근 시도가 계속 발견
      - 외부 또는 내부에서 비정상 패킷의 전송량 증가
      - 확산 속도가 빠른 바이러스가 외부에서 발생

침해 대응

- 사전 대응
  - 침해 사고의 위험 등급
    - 2등급 상황
      - 비인가자에 의해 관리자 명령이 실행.
      - 시스템 자원을 불법적으로 사용하는 프로그램이 실행
      - 일반 사용자의 홈 디렉터리에 시스템 파일 존재
      - 일반적이지 않은 숨김 파일 또는 디렉터리 존재
      - 시스템 담당자가 알지 못하는 사용자가 추가 또는 사용자 권한이 임의로 변경
    - 3등급 상황
      - 외부 또는 내부에서 취약점 수집 행위가 계속 발견
      - 외부 또는 내부에서 불법적인 접근 시도가 계속 발견
      - 외부 또는 내부에서 비정상 패킷의 전송량 증가
      - 확산 속도가 빠른 바이러스가 외부에서 발생

침해 대응

- 사전 대응
  - 등급별 대응 절차
    - 1등급 상황 대응 절차
      - 시스템 담당자가 CERT 팀장에게 즉시 보고.
      - 피해를 최소화하기 위해 네트워크의 인터페이스 단절, 전원 공급 중단 등의 **조치 먼저 수행 가능 (상황에 따라 *선 조치 후 보고 가능*)**
    - 2·3등급 상황 대응 절차
      - **비인가 접근 시도 및 정보 수집 행위를 발견**하면 CERT와 함께 해당 **단말기나 IP 조사**하여 소속 **네트워크와 조직 파악**
      - **내부 시스템에서 침입 시도가 발생한 경우**에는 시스템 위치를 확인하여 책**임자와 접속 경위를 조사**
      - **외부 네트워크에서 침입 시도가 발생한 경우**에는 해당 조직의 **시스템 담당자**나 **보안 담당자**에게 해당 IP로부터 **불법적인 접근 시도**가 발생했음을 통보후 협조 요청
      - 외부 네트워크의 침입 시도에 대한 적절한 조치가 이루어지지 않고 위협이 심각한 경우에는 **대외 기관(검찰, 경찰, 한국인터넷진흥원(KISA) 등)에 조사 의뢰**
      - 침입 시도에 대한 대응이 종료되면 **CERT 팀장이 침입 시도 방법, 침입 시도 대응책 등이 포함된 침입 시도 대응 보고서를 작성**하여 담당자에게 전달

침해 대응

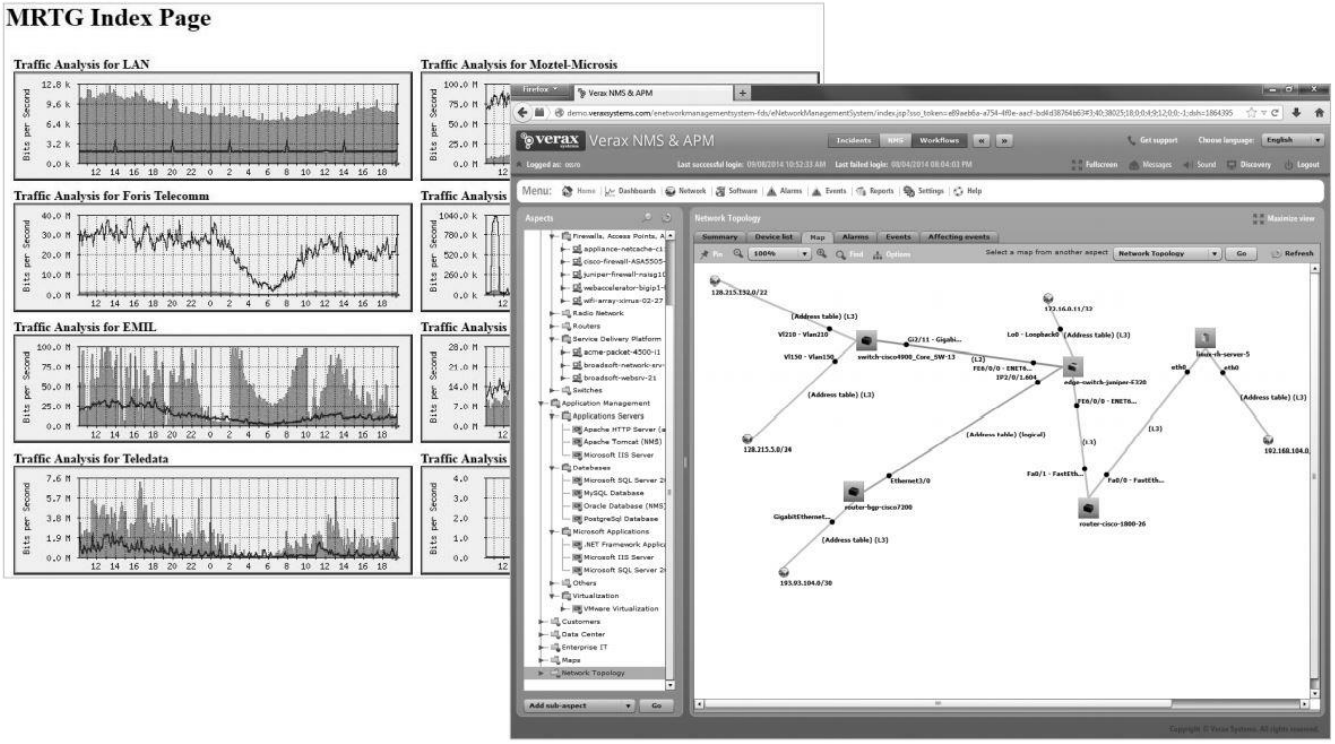
- 사전 대응
  - 침해 대응 체계 점검 사항
    - 조직의 모든 사람이 보안 정책에 대해 알고 있는가?
    - 침해 사고 대응 팀의 모든 구성원은 침해 사고 발생 시 누구에게 보고하고 언론 대응은 어떻게 해야 하는지 충분히 인지하고 있는가?
    - 침해 사고 대응 팀의 모든 구성원은 침해 사고 발생 시 처리해야 할 기술적 절차에 대해 충분히 이해하고 있는가?
    - 침해 사고 대응과 관련한 모든 구성원은 정해진 절차에 따라 주기적으로 훈련을 수행하고 있는가?

침해 대응

- 사고 탐지
  - 사고 탐지의 개요
    - 문제 발생시 침해 사고가 발생한 것인지 확인하는 단계
    - 침해 사고로 확인되면 로그 파일, 오류 메시지 등을 확보, 방화벽, 침입 탐지 시스템을 통해 특정한 절차를 수행
    - 내부의 보고 체계에 따라 책임자에게 보고, 언론 대응이 필요한 경우 대응책 마련
  - 침해 사고 식별 과정에서 확인할 사항
    - 침해 사고 발생 시점은 언제인가?
    - 누가 침해 사고를 발견하고 보고했는가?
    - 침해 사고가 어떻게 발견되었는가?
    - 침해 사고의 발생 범위는 어느 정도인가? 이로 인해 다른 곳이 손상되지는 않았는가?
    - 침해 사고로 인해 기업의 서비스 능력이 손상되었는가?
    - 공격자의 규모와 공격 능력은 어느 정도인가?

침해 대응

- 사고 탐지
  - 침해 사고 발생을 실시간으로 식별하는 과정은 침입 탐지 시스템(IDS)이나 침입 방지 시스템(IPS), 네트워크 트래픽 모니터링 장비(MRTG), 네트워크 관리 시스템(NMS)을 통해 이루어짐



네트워크 트래픽 모니터링 장비와 네트워크 관리 시스템

침해 대응

- 대응
  - 1. 단기 대응
    - 침해 사고가 발생한 시스템이나 네트워크를 식별하고 통제할 수 있는 경우에는 해당 시스템이나 네트워크 연결을 해제 / 차단
    - 대응 수단으로 네트워크 케이블을 뽑는 것과 같은 물리적인 것을 포함하여 방화벽 설정 변경 및 침해 사고 룰 업데이트, 백신 업데이트, 시스템 종료 등이 있음
  - 2. 백업 및 증거 확보
    - 침해 사고 발생 시스템을 초기화하기 전에 백업을 하고 포렌식 절차에 따라 시스템 이미지를 획득
    - 포렌식으로 획득한 증거가 법적 효력을 지니려면 증거 획득과 처리 과정이 적법한 절차를 거쳐야 함
  - 3. 시스템 복구
    - 백도어 등의 악성 코드 제거, 시스템 계정 및 패스워드 재설정, 보안 패치 적용 작업을 거친 뒤 다시 서비스가 가능하도록 시스템을 네트워크에 연결

침해 대응

- 후속 조치 및 보고
  - 침해 사고 식별과 대응 과정에 대해 작성한 문서와 포렌식 과정에서 획득한 자료를 바탕으로 침해 사고 보고서 작성

○○○ 침해 사고 보고

작성자: ○○○

작성일: 2018-○○-○○

(1) 침해 사고 발생 일지: 시간대별로 발생 사실 및 확인 사실을 기록한다.

(2) 사고 원인: 침해 사고가 발생한 원인을 기술한다.

(3) 초기 대처: 침해 사고 시 현황과 그에 따른 대응 내용을 기술한다.

(4) 복구 현황: 보고서 작성 시점의 복구 현황을 기술한다.

(5) 대처 오류 및 해결 방안: 사고 대응 과정에서 잘못한 점과 그에 대한 해결 방안을 강구하여 기술한다.

CONTENTS

- 디지털 포렌식의 개념과 절차

디지털 포렌식의 개념과 절차

- 포렌식의 개요
  - 고대 로마 시대의 포럼이라는 라틴어에서 유래한 말
  - '법의학적인, 범죄 과학 수사의, 법정의, 재판에 관한' 이라는 의미
  - 일반적으로 법정 변론을 위한 과학, 즉 법정과학이나 법과학이라는 개념으로 사용
  - 최근에는 범죄 수사 및 민형사 소송 등 법정에서 사용되는 증거의 수집·보존·분석을 위한 응용과학 분야를 통칭하는 용어로 사용

디지털 포렌식의 개념과 절차

- 포렌식의 개요
  - 디지털 포렌식
    - 법정 제출을 전제로 디지털 환경과 장비를 이용하여 디지털 증거 자료를 수집·분석하는 기술
    - 국제컴퓨터수사전문가협회(IACIS)가 개설한 교육 과정에서 '디지털 포렌식' 이라는 용어가 처음 등장

[Source https://techpad.tistory.com/39]

디지털 포렌식의 개념과 절차

- 디지털 포렌식의 증거
  - 포렌식은 기술 유출, 해킹, 위조, 사이버 테러, 명예훼손이나 업무상 과실, 내부 감사 등에도 사용
  - 포렌식 과정을 통해 획득한 증거가 법적 효력을 지니려면 과학적이고 논리적인 절차와 방법을 거쳐야 함
  - 증거의 개념
    - 직접 증거: 요증 사실(증거에 의한 증명을 요하는 사실)을 직접 증명하는 증거
    - 간접 증거: 요증 사실을 간접적으로 추측하게 해주는 증거
    - 인적 증거: 증인의 증언, 감정인의 진술, 전문가의 의견 등
    - 물적 증거: 범행에 사용한 흉기, 사람의 신체 등

디지털 포렌식의 개념과 절차

- 디지털 포렌식의 증거
  - 전문 증거
    - 포렌식으로 수집된 증거는 간접 증거 (전문 증거)
    - 사실 인정의 기초가 되는 실험을 실험자 자신이 법원에 직접 보고하지 않고 진술서나 진술 기재서를 통해 간접적으로 보고하는 것
    - 전문 법칙을 따르지만, 실험자가 직접 진술하지 않고 실험 결과를 타 인이 전달받아 재진술하는 형태로 제한하여 전문 증거를 인정

(대법원 1999. 9. 3. 선고 99도2317 판결)
컴퓨터 디스켓에 들어 있는 문건이 증거로 사용되는 경우

"위 컴퓨터 디스켓은 그 기재의 매체가 다를 뿐 실질에 있어서는 피고인 또는 피고인 아닌 자의 진술을 기재한 서류와 크게 다를 바 없고 입수 후의 보관 및 출력 과정에 조작의 가능성이 있으며 기본적으로 반대 신문의 기회가 보장되지 않는 점 등에 비추어 그 기재 내용의 진실성에 관하여는 전문 법칙이 적용된다 할 것이고 따라서 형사소송법 제313조 제1항에 의하여 그 작성자 또는 진술자의 진술에 의하여 그 성립의 진정함이 증명된 데 한해 이를 증거로 사용할 수 있다."

디지털 포렌식의 개념과 절차

- 디지털 포렌식의 기본 원칙
  - 정당성의 원칙
    - 모든 증거는 적법한 절차를 거쳐서 얻은 것이어야 하며 위법한 절차로 획득한 증거는 증거 능력이 없음
    - 포렌식도 정당성을 얻기 위한 과정으로 정보 제공 동의서에 서명을 받아야 함

정보 제공 동의서

본인은 ○○○의 정보 자산(개인 정보, 서류, 전자 파일, 저장 매체, 전산망, 전산 장비 등)을 업무 이외의 목적으로 사용하지 않을 것이며 정보 자산 보호 및 유출을 방지하기 위한 목적으로 실시되는 모든 종류의 유·무선 통신에 의한 음향, 문언, 부호 등에 대한 ○○○의 내용 검색에 동의합니다.

년 월 일

성명:

서명 또는 날인:

디지털 포렌식의 개념과 절차

- 디지털 포렌식의 증거
  - 증거 개시 제도
    - 정식 재판이 진행되기 전 공판 준비 절차 단계에서 민사소송은 원고와 피고, 형사 공판은 검사와 피고인 (변호인)이 각자 가지고 있는 증거를 동시에 개시하며 미리 제시하지 않은 증거는 법정에서 원칙적으로 사용하지 못하도록 하는 제도
    - 이로 인해 디지털 포렌식이 대량의 문서나 이메일에서 증거를 찾는 전자 증거 개시(e-Discovery)로 발전

디지털 포렌식의 개념과 절차

- 디지털 포렌식의 기본 원칙
  - 재현의 원칙
    - 증거는 절차를 통해 정제되는 과정을 거칠 수 있는데 이를 법정에 제출하려면 같은 환경에서 같은 결과가 나오도록 재현할 수 있어야 하며, 수행할 때마다 다른 결과가 나온다면 증거로 제시할 수 없음
  - 신속성의 원칙
    - 컴퓨터 내부 정보는 휘발성을 가진 것이 많기 때문에 신속성이 필요
    - 시스템 안의 디스크, 메모리, 응용 프로그램 등의 정보를 얻기 위해서는 신속하고 정확하게 움직여야 함

디지털 포렌식의 개념과 절차

- 디지털 포렌식의 기본 원칙
  - 연계 보관성의 원칙
    - 연계 보관성: 증거를 획득한 뒤에는 이송, 분석, 보관, 법정 제출이라는 일련의 과정이 명확해야 하며 이러한 과정을 추적할 수 있어야 함

연계 보관성 로그표

인계자	인수자	증거 보관 위치 변동 사항	날짜	인계 내용 및 이유
이름: (서명)	이름: (서명)	( )→( )		
이름: (서명)	이름: (서명)	( )→( )		
이름: (서명)	이름: (서명)	( )→( )		
이름: (서명)	이름: (서명)	( )→( )		
이름: (서명)	이름: (서명)	( )→( )		

  - 무결성의 원칙
    - 수집된 증거는 연계 보관성을 가지고 각 단계를 거치는 과정에서 위조·변조되어서는 안 되며 이러한 사항을 매번 확인해야 함
    - 하드디스크의 경우에는 해시 값을 구해서 각 단계마다 값을 확인하여 무결성을 입증할 수 있음

디지털 포렌식의 개념과 절차

- 포렌식 수행 절차
  - 수사 준비
    - 수사를 준비할 때는 장비와 툴을 확보하고 적절한 법적 절차를 거쳐 피의자 또는 수사 대상에 접근해야 함
  - 증거물 획득
    - 증거를 획득하는 사람, 감독하는 사람, 인증하는 사람의 참관하에 다음 절차를 수행해야 함
      - 컴퓨터의 일반적인 하드드라이브를 검사할 때는 컴퓨터 시스템 정보를 기록
      - 복제 작업을 한 원본 매체나 시스템의 디지털 사진을 찍음
      - 모든 매체에 적절한 증거 라벨을 붙임

디지털 포렌식의 개념과 절차

- 포렌식 수행 절차
  - 증거물 획득

포렌식 사용 증거 라벨

증거 획득 날짜	피의자 동의 여부	사건 번호	라벨 번호
	(Yes, No)		
증거에 대한 설명			
증거를 획득한 방법, 장소, 증거의 고유성을 확인할 수 있는 시리얼 번호 등 증거와 관련하여 기록해야 할 일련의 내용을 적는다.			

구분	이름	서명	날짜	연락처
증거를 획득한 사람				
감독한 사람				
검토 책임자				

디지털 포렌식의 개념과 절차

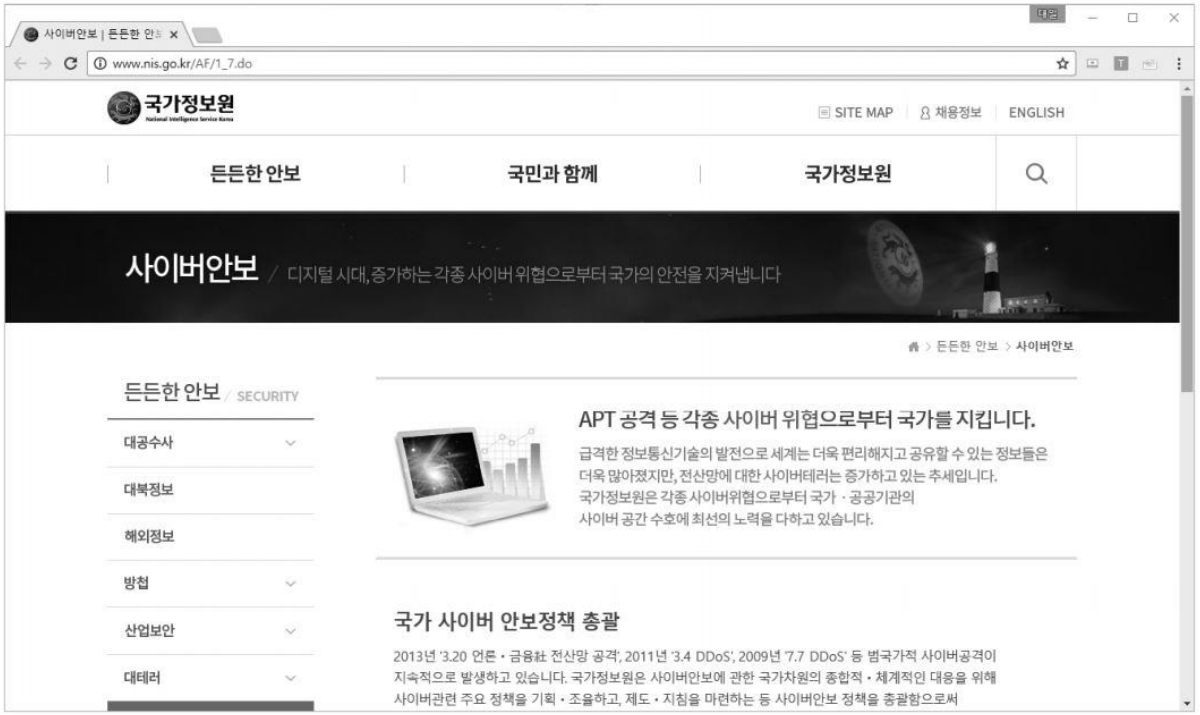
- 포렌식 수행 절차
  - 보관 및 이송
    - 획득한 증거가 연계 보관성을 가지려면 안전한 장소에 보관되어야 함
    - 이송하거나 담당자가 바뀔 때는 문서에 증적을 남겨야 함
  - 분석 및 조사
    - 포렌식 증거를 관리할 때는 최량 증거 원칙을 따름
      - 최량 증거 원칙: 복사본 등의 이차적인 증거가 아닌 원본을 제출하도록 요구하는 영미 증거법상의 원칙
      - 원본이 존재하지 않으면 가장 유사하게 복사한 최초 복제물이라도 증거로 제출해야 함

디지털 포렌식의 개념과 절차

- 포렌식 수행 절차
  - 법원에 제출하는 원본 또는 최초의 복제물은 기본적으로 보관하고 이를 다시 복사한 것을 분석 및 조사해야 함
  - 각 분석 단계에서는 무결성을 확인할 수 있는 정보가 계속 기록되어야 하며 사용 프로그램은 공증 받은 것에 한함
  - 프로그램 내에서 사용된 스크립트는 내용과 실행 단계별 결과가 문서화되어야 함
  - 보고서 작성
    - 분석에 사용한 증거 데이터, 분석 및 조사 과정에서 증거 수집을 위해 문서화한 무결성 관련 정보, 스크립트 수행 결과를 보고서로 작성하여 증거와 함께 제출

디지털 포렌식의 개념과 절차

- 사이버 수사 기구
  - 국가정보원 국가사이버안전센터
    - 2003년의 1·25 인터넷 대란을 계기로 국가 기간 통신망을 보호하기 위해 2004년 2월 설립



국가사이버안전센터

디지털 포렌식의 개념과 절차

❑ 사이버 수사 기구

◘ 국가정보원 국가사이버안전센터

– 국가사이버안전센터의 주요 업무

구분	설명
국가 사이버 안전 정책 총괄	• 국가 사이버 안전 정책 기획·조정 • 국가 사이버 안전 전략 회의 및 대책 회의 운영 • 민·관·군 사이버 안전 정보 공유 체계 구축 운영
사이버 안전 예방 활동	• 국가 정보통신망의 안정성 확인 • 사이버전 모의 훈련 실시 • 정보통신망 보안성 검토 및 안전 측정
국가 사이버 위협 정보 종합 수집·분석·전파	• 주요 기관을 대상으로 24시간 365일 보안 관제 • 위협 수준별 경보 발령 • 보안 분석 정보 배포 • 사이버 안전 관련 기술 개발
침해 사고 긴급 대응, 조사 및 복구	• 사이버 공격 침해 사고 접수 • 사고 조사 및 대책 강구 • 피해 확산 방지 및 복구 지원 • 범정부 합동 조사·복구 지원 팀 구성 및 운영
국내외 사이버 위협 정보 공유 및 공조 대응	• 국내 사이버 안전 전문 기구와 협의체 운영 • 미국, 영국, 프랑스, 독일, 캐나다, 일본 등 선진국과 협력 체계 구축·운영

국가사이버안전센터의 업무

디지털 포렌식의 개념과 절차

- 사이버 수사 기구
  - 대검찰청 첨단범죄수사과
    - 기술 유출 범죄 수사지원센터
      - 산업 기술 유출 범죄 수사 계획을 수립하고 지원
  - 인터넷 관련 범죄 수사 팀
    - 컴퓨터 및 인터넷 관련 장치를 압수 수색, 분석
  - 회계 분석 팀
    - 기업 비리, 회계 부정 등을 조사하기 위해 회계 데이터 압수 수색, 분석하며 관련자 조사
  - 범죄 수익 환수 팀
    - 자금 세탁 범죄를 수사하며 마약, 조직범죄 등의 수익을 추적, 몰수
  - 자금세탁 수사 및 범죄 수익 환수 전담반
    - 경제적 이익 획득과 관련된 범죄 수사 시 관련 증거를 확보하기 위해 금융 계좌 추적, 관련자 조사, 금융정보분석원에서 제공받은 혐의 조사, 거래 정보 및 고액 현금 거래 정보 수사
  - 첨단 범죄 수사 전문 아카데미
    - 각종 첨단 범죄에 효율적으로 대처하는 수사 전문가 양성

디지털 포렌식의 개념과 절차

- 사이버 수사 기구
  - 경찰청 사이버테러대응센터
    - 1995년 10월 해커수사대 이름으로 창설되어 지금까지 운영

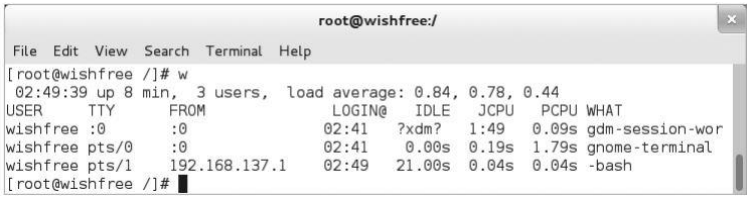
사이버테러 대응센터

CONTENTS

- 디지털 포렌식의 증거 수집

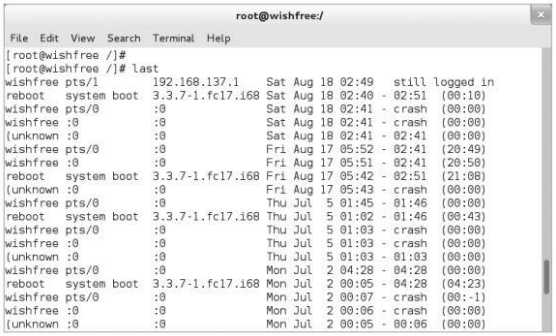
디지털 포렌식 증거 수집

- 시스템 증거 수집
  - 활성 데이터 수집
    - 리눅스(유닉스) 시스템
      - 리눅스에서 현재 세션이 형성되어 있는 사용자를 확인할 때는 **w, who, last** 명령을 사용

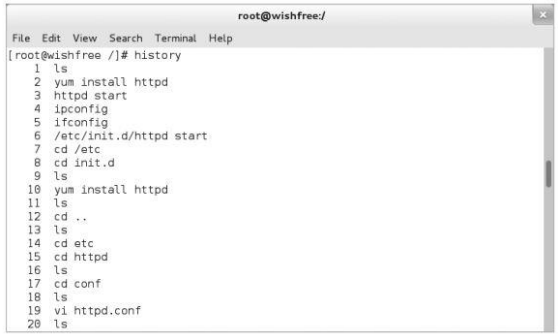


W 명령 실행 결과

      - 최근 접속 기록을 확인할 때는 주로 **last** 명령을 사용



last 명령 실행 결과



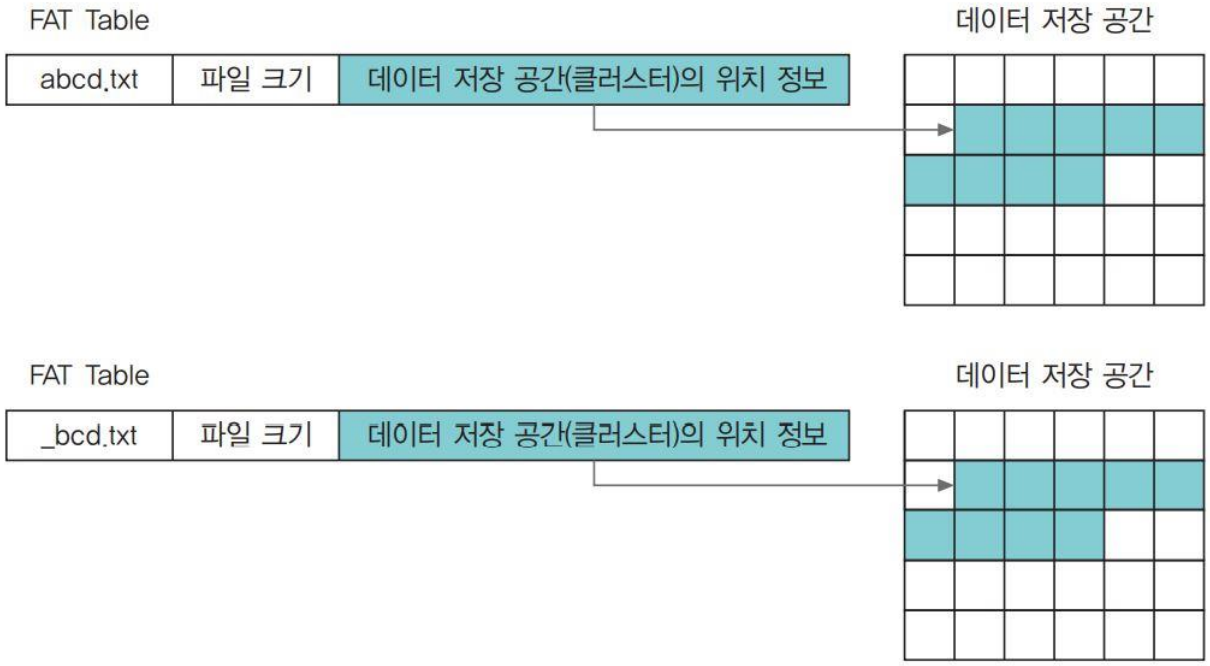
History 명령 실행 결과

디지털 포렌식 증거 수집

- 시스템 증거 수집
  - **시스템 로그 분석**
    - 시스템 로그는 공격자에 의해 삭제될 수 있지만 침해 사고가 발생했을 때 가장 먼저 살펴보아야 할 기본 항목
    - 시스템 로그가 삭제되는 것을 막기 위해 네트워크에 로그 서버를 별도로 둘 수 있음
  - **저장 장치 분석**
    - 먼저 조사 대상 시스템에서 **하드디스크를 떼어냄**
    - 하드디스크는 가장 중요한 기본 증거 데이터이므로 쓰기 금지를 보장하는 장치 연결 이미지 장치를 이용하여 **별도로 준비한 저장 매체에 쓰기를 금지시킨 원본 하드디스크를 복사**함
    - **이미지 획득 작업**은 저장 매체의 모든 **정보를 비트 단위로 복사**
    - 획득한 이미지는 별도의 포렌식용 시스템에서 포렌식 이미지 전용 분석 툴로 분석하므로 삭제된 파일도 일부 복구 가능

디지털 포렌식 증거 수집

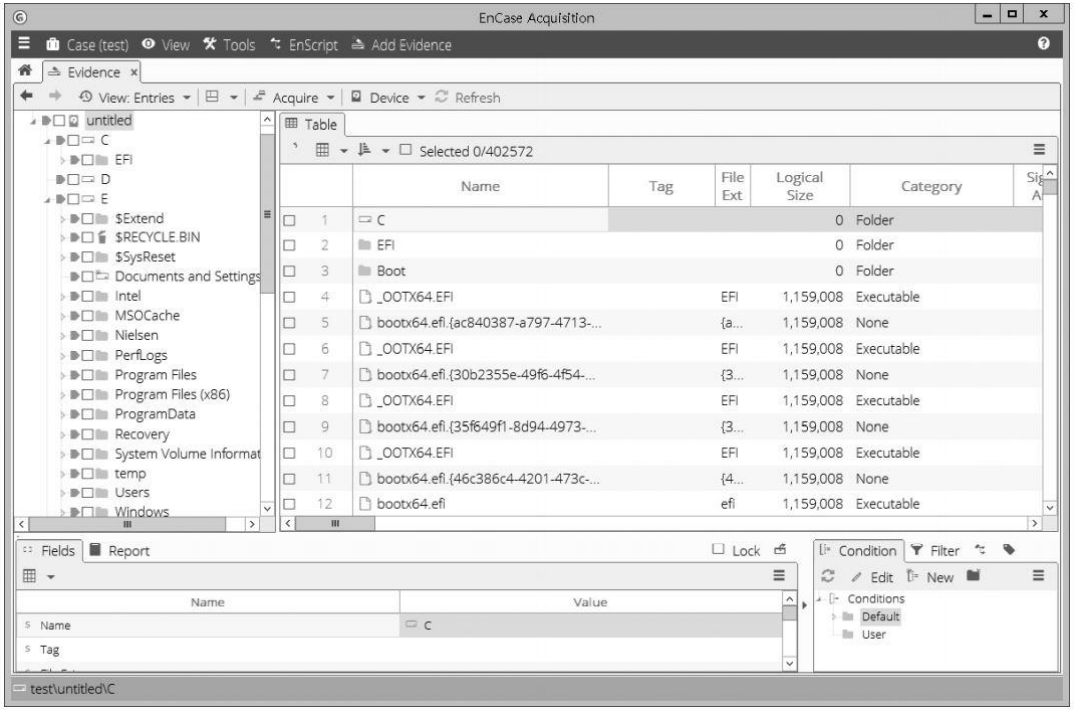
- 시스템 증거 수집
  - 저장 장치 분석
    - 삭제된 파일을 복구할 수 있는 이유는 운영체제에서 파일을 삭제할 때 실제로 해당 데이터를 모두 삭제하는 것이 아니기 때문



파일 삭제 전후 상태

디지털 포렌식 증거 수집

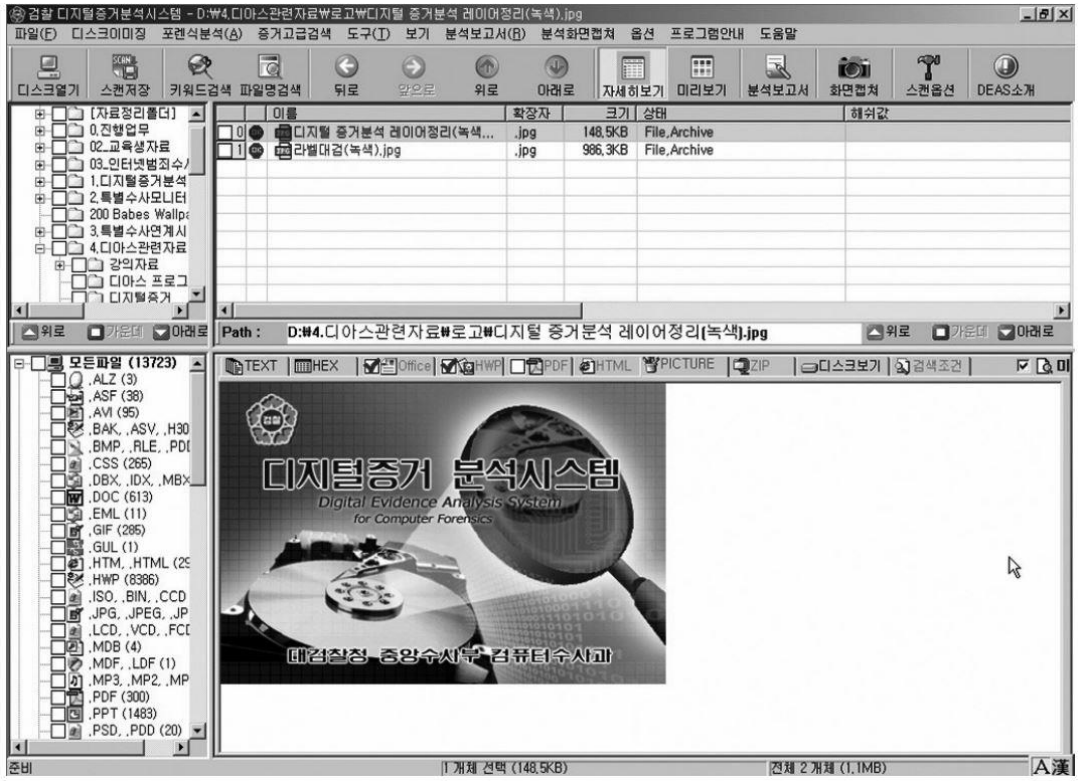
- 시스템 증거 수집
  - EnCase
    - 디지털 포렌식 툴
    - 미국에서 1990년대 후반부터 수많은 사법 기관의 컴퓨터 관련 범죄 수사에 활용



Encase 실행 화면

디지털 포렌식 증거 수집

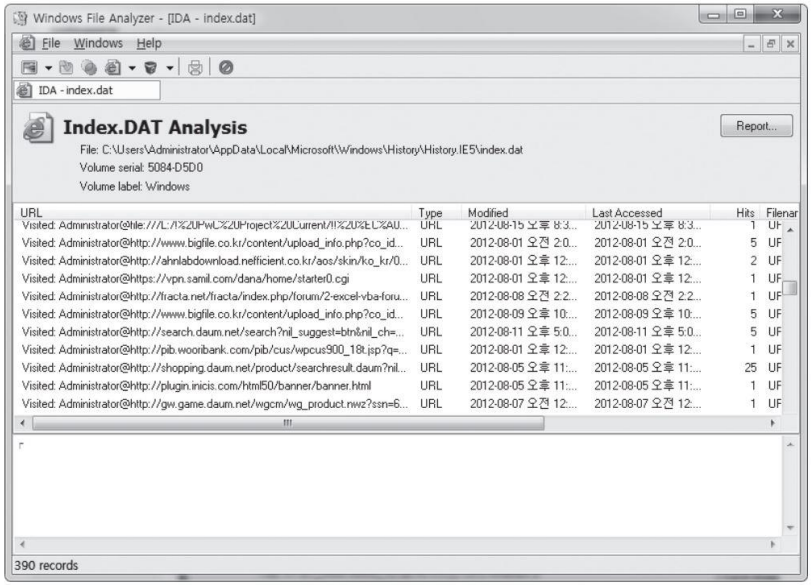
- 시스템 증거 수집
  - DEAS
    - 우리나라는 2002년에 검찰 디지털 증거 분석 시스템(DEAS)을 만들어 사용



DEAS 실행 화면

디지털 포렌식 증거 수집

- 데이터 및 응용 프로그램 증거 수집
  - 이메일 분석
    - 피의자가 여러 명일 때는 서로 주고받은 이메일을 분석하여 범죄 증거 확보 가능
  - 인터넷 분석
    - 시스템에 저장되어 있는 인터넷 브라우저의 쿠키나 index.dat 파일, temp 등으로 방문 사이트 정보를 획득하고 작업 내용 파악 가능



WFA(Window File Analyzer)를 이용한 index.dat 파일 열람

Summary

- 침해 대응
- 디지털 포렌식의 개념과 절차
- 디지털 포렌식의 증거 수집

참고문헌

- 정보 보안 개론 - 한권으로 배우는 핵심 보안 이론, 양대일, 한빛 아카데미

Q & A