2018 CCIT Project

Remote 기반 memory 분석 감사 (audit) 체계 연구

- **Computer Forensics** 구조 기반

발표자

- 정보보호학과 조예림

Contents

- Computer Forensics 정의
- 연구의 필요성
- 연구 개념
- 원격 포렌식 분석도구 Qator
- 향후 진행 계획 - 연구 개념도

디지털 포렌식이란?

- 디지털기기를 매개체로 하여 발생한 특정 행위의 사실 관계를 법정에서 규명하고 증명하기 위한 절차와 방법이다.
- 기존의 혈흔, 지문 등의 아날로그 증거와는 다르게 디지털 데이터는 쉽게 복제가 가능하고 변조할 수 있는 등의 특징을 가진다.
- 디지털 데이터가 증거 능력을 갖도록 하기 위해 사전 준비부터 데이터 수집, 이동, 분석, 검증, 법정 증명 과정 동안 검증된 절차와 방법이 요구된다.

컴퓨터 포렌식

- Computer forensics는 전자적 증거물 등을 사법기관에 제출하기 위해 데이터를 수집, 분석, 보고서를 작성하는 일련의 작업
- 컴퓨터 시스템, 저장 매체 또는 전자 문서와 같은 디지털 자료의 현재 상태를 설명하는 것이 목적
- 사이버 범죄자 추적 및 조사에 핵심적인 요소

연구 필요성

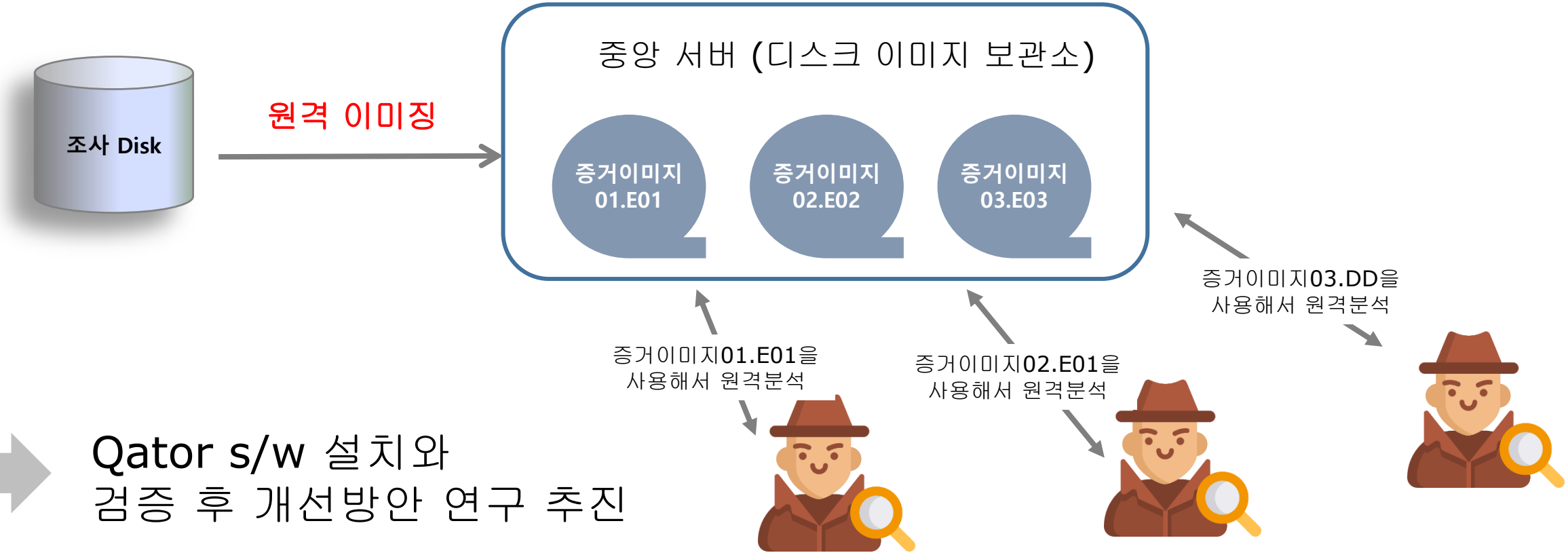
- 사고 현장에서의 내부 감사 및 정보 기술 유출 사고 조사시 (디지털 포렌식) 운용자 위주 감사 분석 및 해석 증거물로서 판단 오류 행위 발생 가능

* 효율적인 디지털 증거 수집 대응 방안 요구
* 정보 유출 사건 발생 시 초기 대응 요구
* 수집 이벤트의 휘발성으로 발생 위치에서 분석 및 보안 상태 점검
* 무결성 확보와 검증을 위한 원격 형태 방안 필요성 대두

원격 조사에 의한 다각화 분석으로 포렌식 행위 사고 분석 및 사전 예방 체계 구현 방안 연구

연구 개념

- 일반적인 포렌식 분석 도구는 조사자 단독으로 분석을 해야 함
- 다수의 조사자에 의한 원격 디스크 이미지 분석으로 객관적 조사 가능



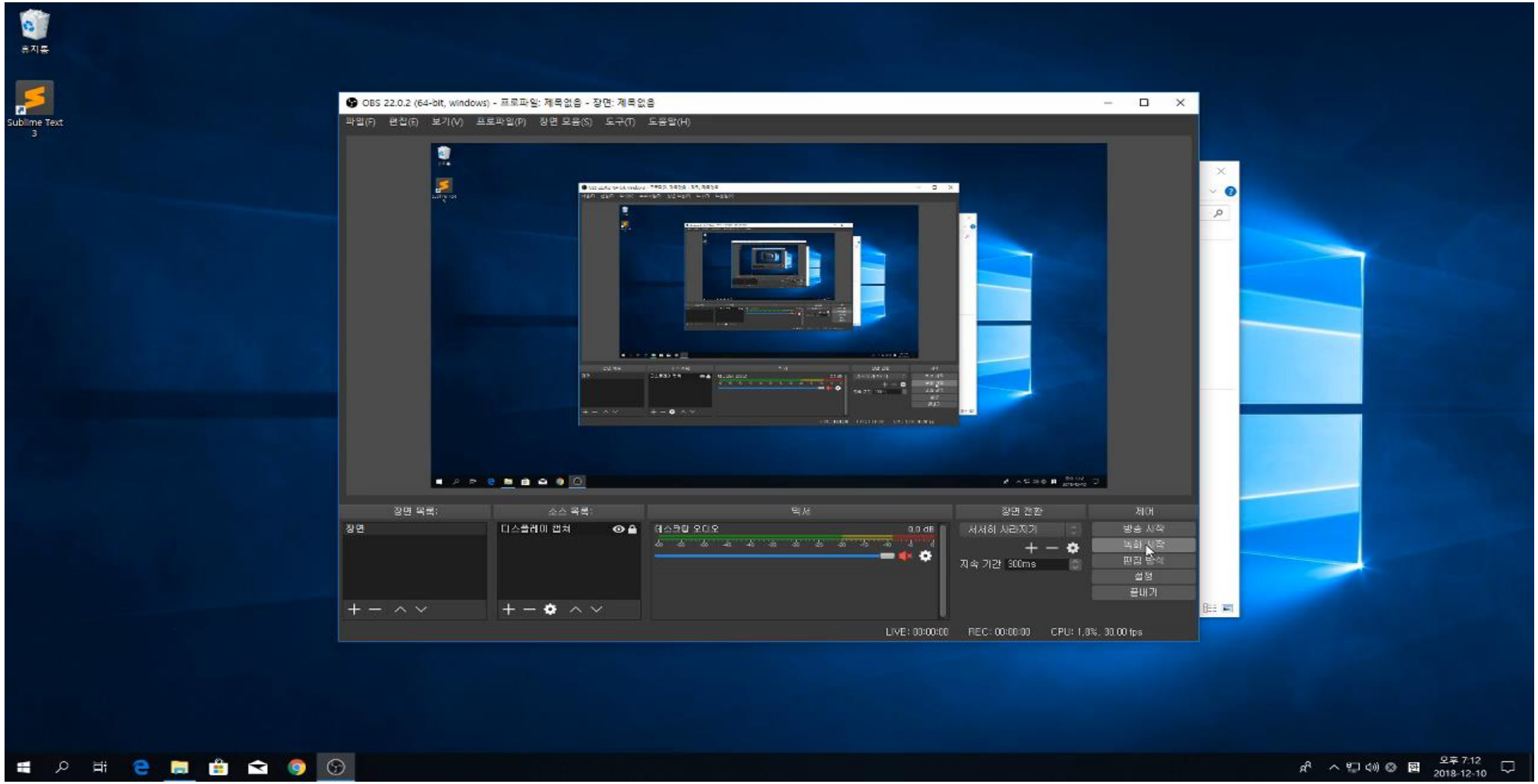
Qator s/w 설치와
검증 후 개선방안 연구 추진

원격 포렌식 분석 도구 Qator

Qator 기능

1. 원격 디스크 조사
2. 삭제 파일 조사
3. 검색
4. 원격 디스크 이미징
5. 인덱스 생성 및 검색
6. 실시간 조사
7. 사용자 환경 수집
8. 웹 히스토리 분석

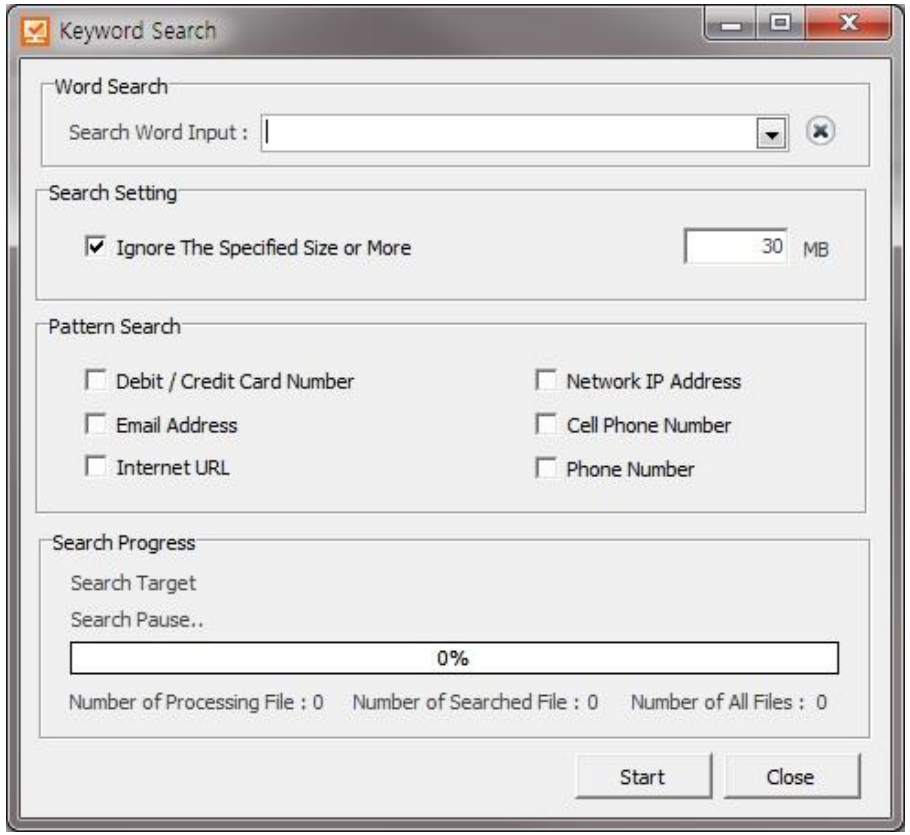
Qator 설치

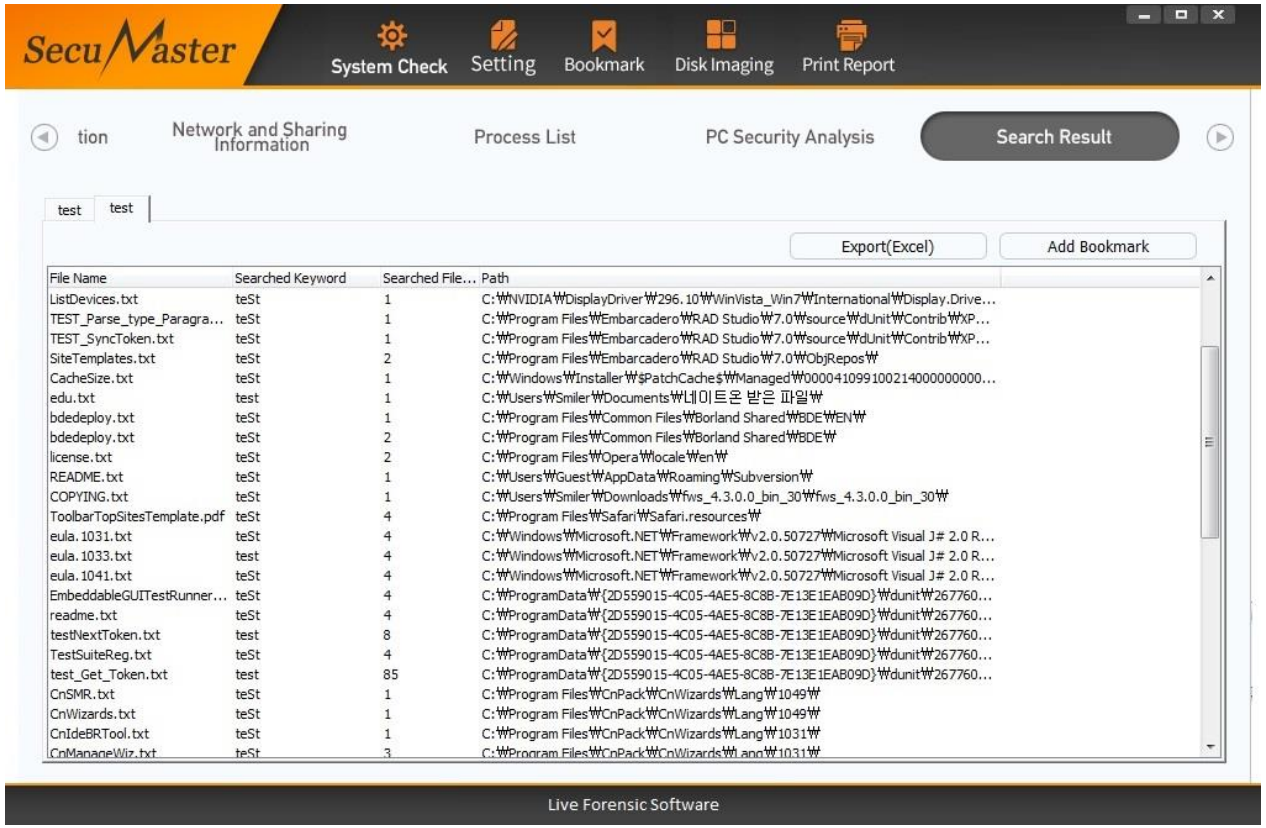

휴지통
Sublime Text 3
OBS 22.0.2 (64-bit, windows) - 프로파일: 제목없음 - 장면: 제목없음
파일(F) 편집(E) 보기(V) 프로파일(P) 장면 모음(S) 도구(T) 도움말(H)
장면 목록:
장면
소스 목록:
디스플레이 캡처
믹서
데스크탑 오디오
0.0 dB
장면 전환
서서히 사라지기
지속 기간 300ms
제어
방송 시작
녹화 시작
편집 방식
설정
끝내기
LIVE: 00:00:00
REC: 00:00:00
CPU: 1.3%, 30.00 fps
오후 7:12
2018-12-10

Qator 기능

❑ 검색

- 원하는 키워드를 파일 이름 및 파일 내용에서 검색.
- 검색 후 내용 확인 및 복사가 가능.

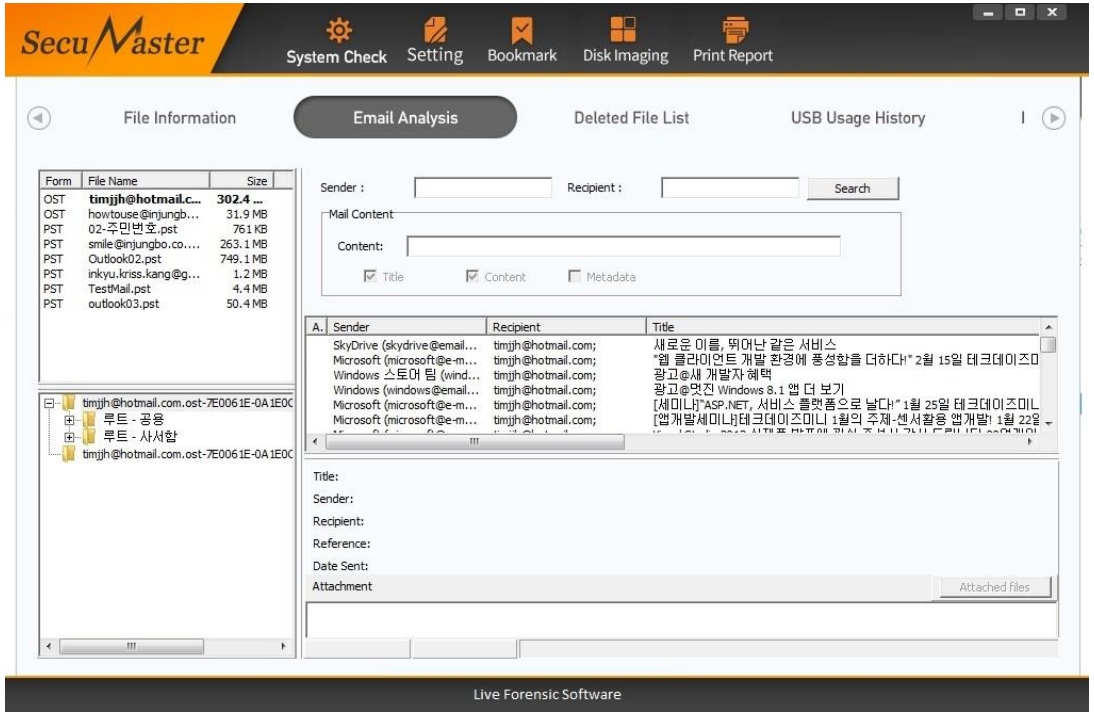




Qator 기능

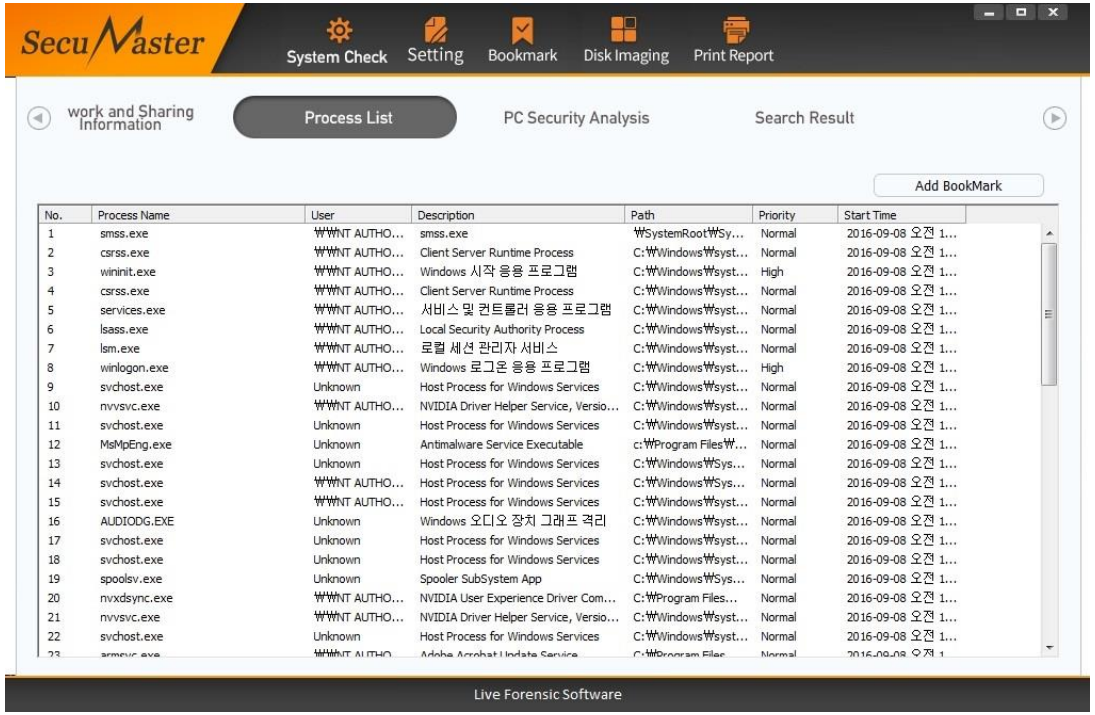
❑ 이메일 분석

- 이메일 파일에 대한 분석을 합니다. 메시지 내용 검색 및 첨부파일 확인 및 검색이 가능.



❑ 메모리 분석

- 조사 대상 시스템에서 동작중인 프로세스의 메모리에 대한 분석 및 전체 메모리에 대한 분석이 가능



Qator 적용 효과

- 원격 포렌식으로 사전 중요 기밀 자료유출 발생 최소화
- 중요 기밀 자료의 유출사고가 발생시 수집/자료 분석을 위해 원격 분석 등의 다각화 기능을 통한 효율적 조사 및 검증 가능
- 잠재적인 소송 대응 기업의 리스크를 최소화할 수 있는 유리한 증거 자료 확보 가능 예상
- 정기적/상시적 보안 조사를 통해 자료 유출 사고 사전 예방

향후 계획

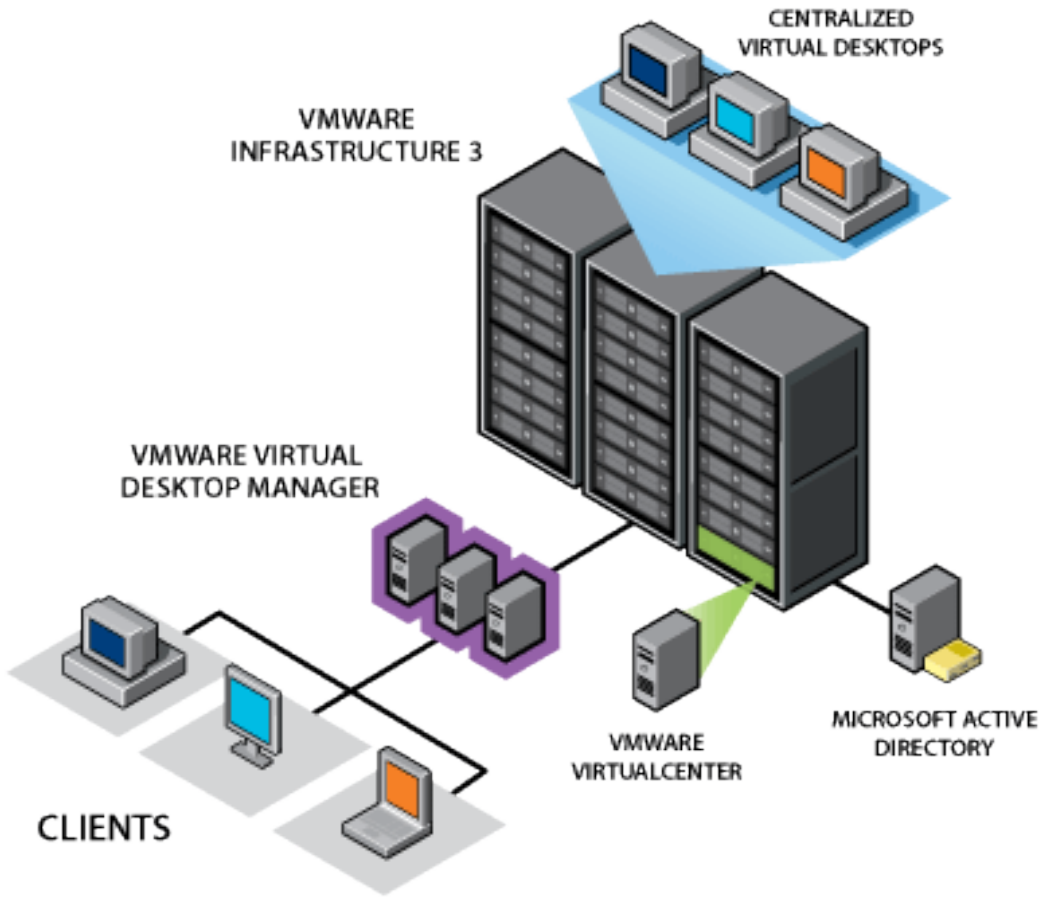
- 원격 포렌식 툴에 기반 추가 기능 검토 및 연구

- 가상화 통합 서버(VDI) 상호 API 연동 연구

*** VDI(Virtual Desktop Infrastructure: 서버를 데이터 센터에 두고 필요할 때 로그인 하여 운용하는 가상의 데스크톱 제공 개념)**

가상화 통합 서버 (VDI) + 원격 포렌식 연구 개념도

가상화 S/W 환경에서의 원격 포렌식 운용 체계 구현



예상되는 기대효과

- 국내최초 가상화 환경에서의 원격 포렌식 구성 및 운용으로 관련기술 검증에 대한 리딩 역할 가능
- 해당 클라우드 환경 구성시 서비스 요구자에 대한 유료화 서비스로 사업성 기대효과 제공
- 가상화 자체에 대한 무결성 검증 TOOL로 사용시 신뢰성이 보장된 서비스 제공 가능

Q&A

THANK YOU

Thanks to 선홍

Thanks to 윤종문 교수님