



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 forensics**는 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 현장에서 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

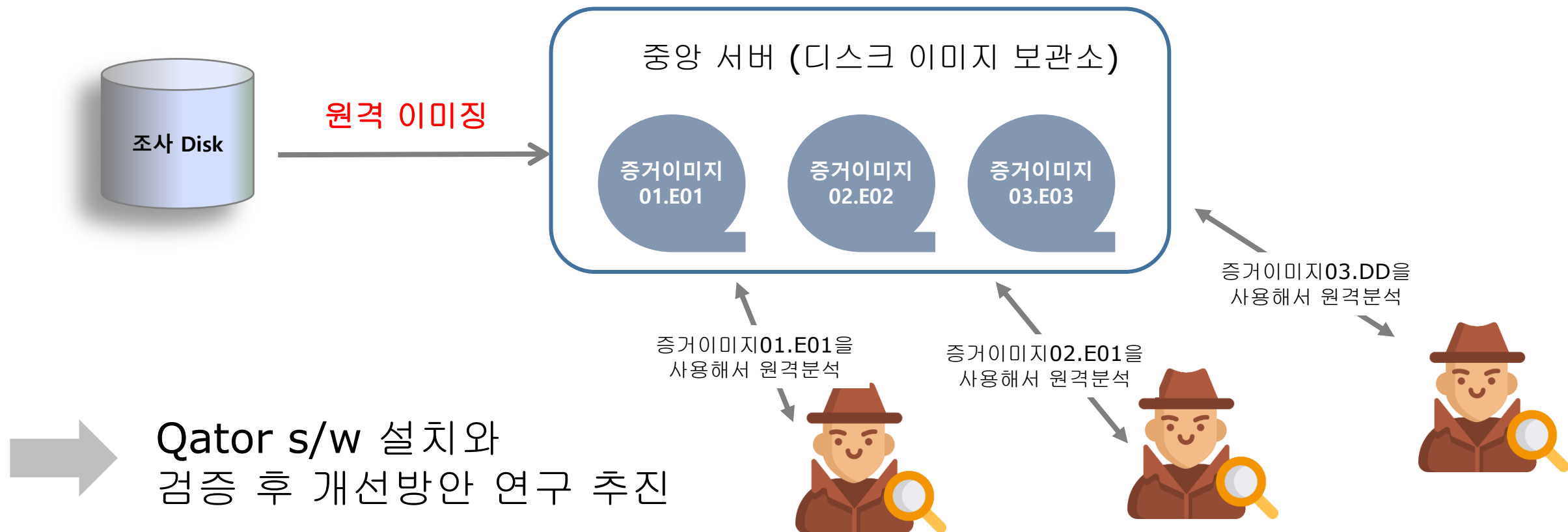
* 무결성 확보와 검증을 위한 원격 형태 방안 필요성 대두



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



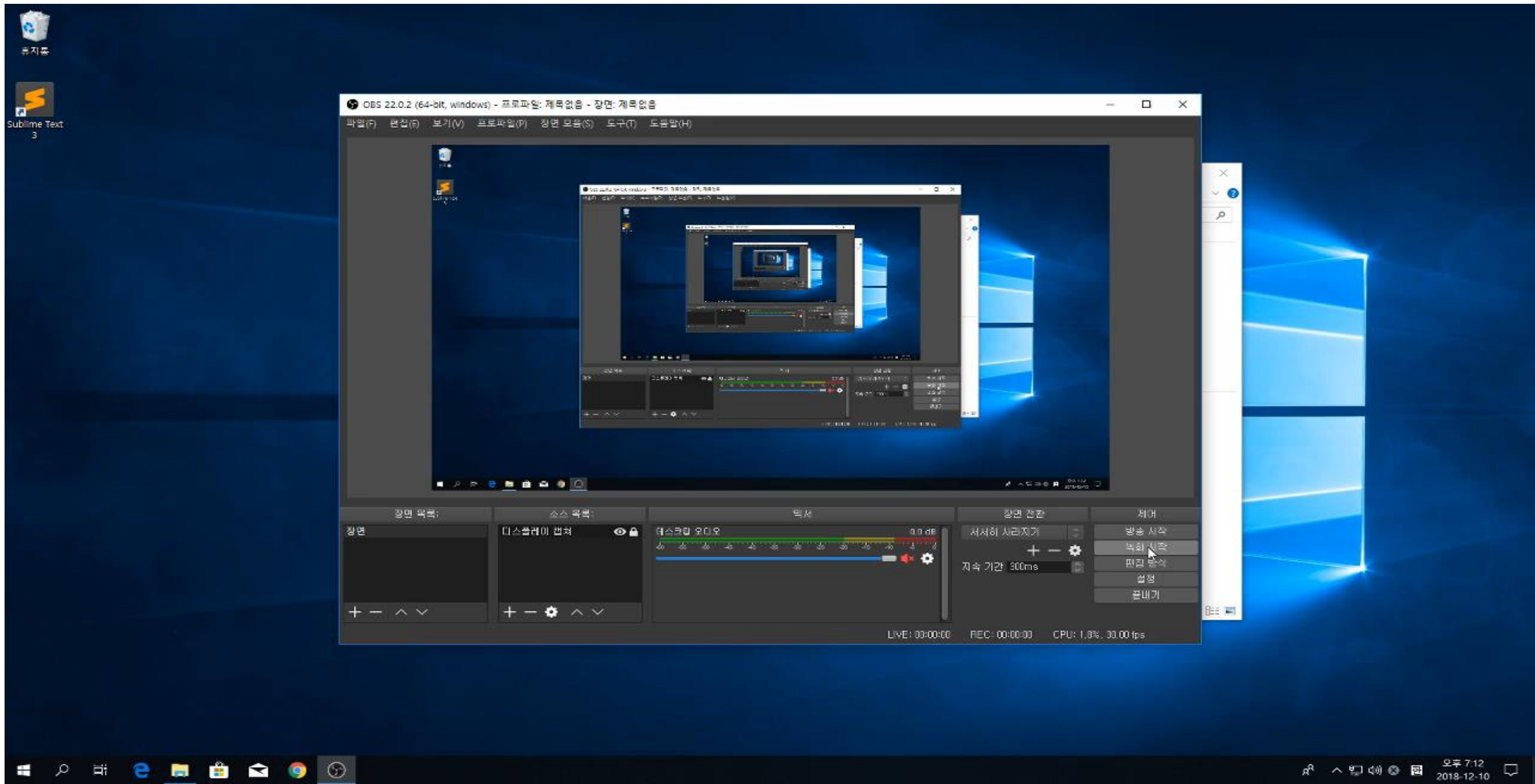
원격 포렌식 분석 도구 Qator



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

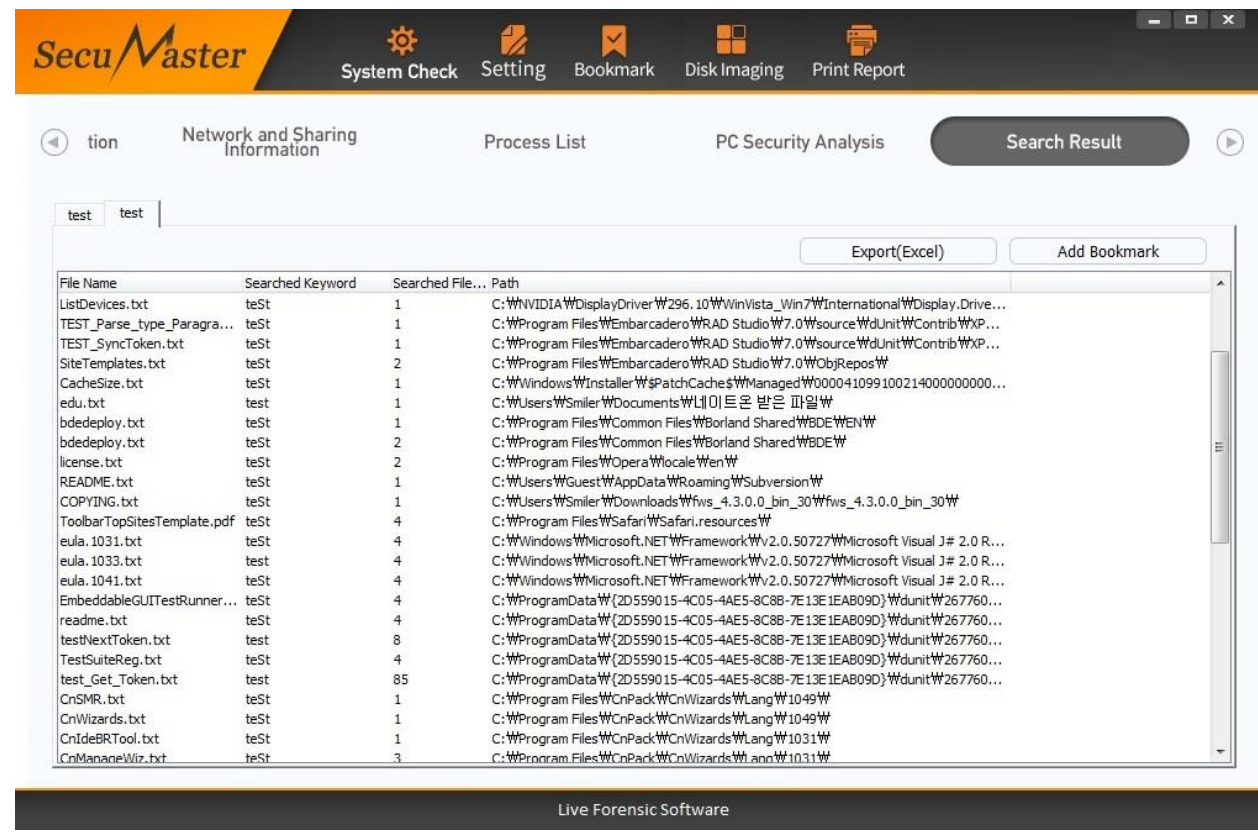
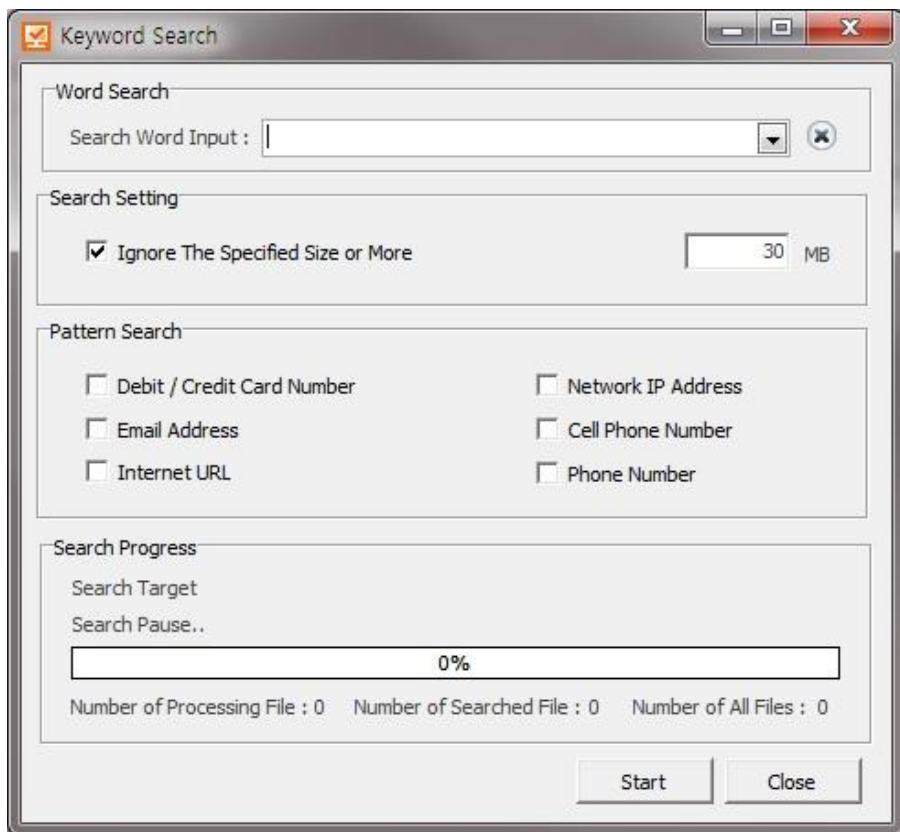
Qator 설치



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

The screenshot shows the 'Email Analysis' tab in the SecuMaster application. On the left, a table lists PST files with columns for 'Form', 'File Name', and 'Size'. The main area displays search filters for 'Sender' and 'Recipient', and a 'Mail Content' search box. Below this, a table shows search results with columns for 'A. Sender', 'Recipient', and 'Title'. The bottom section shows the details of a selected email, including 'Title', 'Sender', 'Recipient', 'Reference', 'Date Sent', and 'Attachment'.

Form	File Name	Size
OST	timjh@hotmail.c...	302.4 ...
OST	howtouse@injunb...	31.9 MB
PST	02-주민번호.pst	761 KB
PST	smile@injungbo.co...	263.1 MB
PST	Outlook02.pst	749.1 MB
PST	inkyu.kriss.kang@g...	1.2 MB
PST	TestMail.pst	4.4 MB
PST	outlook03.pst	50.4 MB

A. Sender	Recipient	Title
SkyDrive (skydrive@email...)	timjh@hotmail.com;	새로운 이를 뛰어난 같은 서비스
Microsoft (microsoft@e-m...)	timjh@hotmail.com;	"웹 클라이언트 개발 환경에 호성함을 더하다" 2월 15일 테크데이즈D
Windows 스토어 팀 (wind...)	timjh@hotmail.com;	광고@새 개발자 혜택
Windows (windows@email...)	timjh@hotmail.com;	광고@멋진 Windows 8.1 앱 더 보기
Microsoft (microsoft@e-m...)	timjh@hotmail.com;	[세미나]"ASP.NET, 서비스 플랫폼으로 날다" 1월 25일 테크데이즈D
Microsoft (microsoft@e-m...)	timjh@hotmail.com;	[앱개발세미나]테크데이즈D 1월의 주제-센서 활용 앱개발! 1월 22일

The screenshot shows the 'Process List' tab in the SecuMaster application. It displays a table of running processes with columns for 'No.', 'Process Name', 'User', 'Description', 'Path', 'Priority', and 'Start Time'. The table lists various system and application processes, including smss.exe, csrss.exe, wininit.exe, services.exe, lsass.exe, sm.exe, winlogon.exe, svchost.exe, nvsvc.exe, and others.

No.	Process Name	User	Description	Path	Priority	Start Time
1	smss.exe	WWWNT AUTHO...	smss.exe	WSystemRootWSy...	Normal	2016-09-08 오전 1...
2	csrss.exe	WWWNT AUTHO...	Client Server Runtime Process	C:WWindowsWsys...	Normal	2016-09-08 오전 1...
3	wininit.exe	WWWNT AUTHO...	Windows 시작 응용 프로그램	C:WWindowsWsys...	High	2016-09-08 오전 1...
4	csrss.exe	WWWNT AUTHO...	Client Server Runtime Process	C:WWindowsWsys...	Normal	2016-09-08 오전 1...
5	services.exe	WWWNT AUTHO...	서비스 및 컨트롤러 응용 프로그램	C:WWindowsWsys...	Normal	2016-09-08 오전 1...
6	lsass.exe	WWWNT AUTHO...	Local Security Authority Process	C:WWindowsWsys...	Normal	2016-09-08 오전 1...
7	sm.exe	WWWNT AUTHO...	로컬 세션 관리자 서비스	C:WWindowsWsys...	Normal	2016-09-08 오전 1...
8	winlogon.exe	WWWNT AUTHO...	Windows 로그인 응용 프로그램	C:WWindowsWsys...	High	2016-09-08 오전 1...
9	svchost.exe	Unknown	Host Process for Windows Services	C:WWindowsWsys...	Normal	2016-09-08 오전 1...
10	nvsvc.exe	WWWNT AUTHO...	NVIDIA Driver Helper Service, Versio...	C:WWindowsWsys...	Normal	2016-09-08 오전 1...
11	svchost.exe	Unknown	Host Process for Windows Services	C:WWindowsWsys...	Normal	2016-09-08 오전 1...
12	MsMpEng.exe	Unknown	Antimalware Service Executable	c:WProgram FilesW...	Normal	2016-09-08 오전 1...
13	svchost.exe	Unknown	Host Process for Windows Services	C:WWindowsWsys...	Normal	2016-09-08 오전 1...
14	svchost.exe	WWWNT AUTHO...	Host Process for Windows Services	C:WWindowsWsys...	Normal	2016-09-08 오전 1...
15	svchost.exe	WWWNT AUTHO...	Host Process for Windows Services	C:WWindowsWsys...	Normal	2016-09-08 오전 1...
16	AUDIODG.EXE	Unknown	Windows 오디오 장치 그래픽 격리	C:WWindowsWsys...	Normal	2016-09-08 오전 1...
17	svchost.exe	Unknown	Host Process for Windows Services	C:WWindowsWsys...	Normal	2016-09-08 오전 1...
18	svchost.exe	Unknown	Host Process for Windows Services	C:WWindowsWsys...	Normal	2016-09-08 오전 1...
19	spoolsv.exe	Unknown	Spooler SubSystem App	C:WWindowsWsys...	Normal	2016-09-08 오전 1...
20	nvxdsync.exe	WWWNT AUTHO...	NVIDIA User Experience Driver Com...	C:WProgram Files...	Normal	2016-09-08 오전 1...
21	nvsvc.exe	WWWNT AUTHO...	NVIDIA Driver Helper Service, Versio...	C:WWindowsWsys...	Normal	2016-09-08 오전 1...
22	svchost.exe	Unknown	Host Process for Windows Services	C:WWindowsWsys...	Normal	2016-09-08 오전 1...
23	smss.exe	WWWNT AUTHO...	Adobe Acrobat Update Service	C:WProgram Files...	Normal	2016-09-08 오전 1...

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

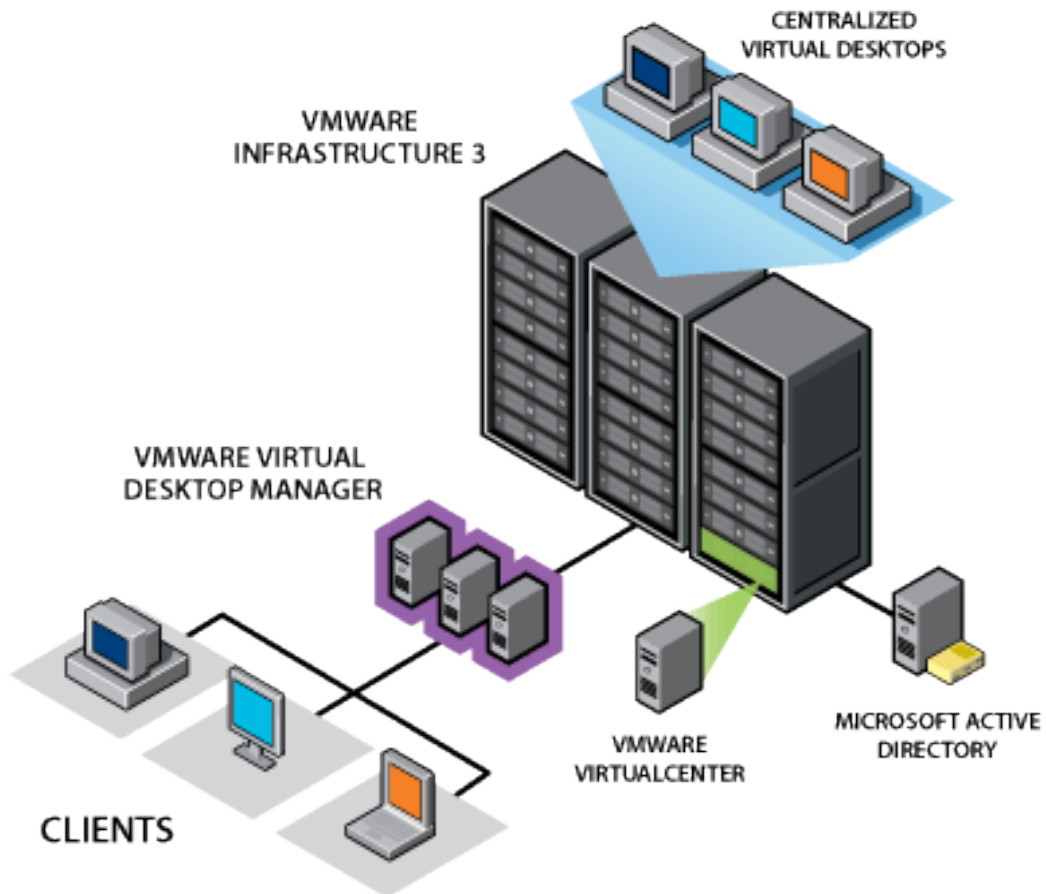
향후 계획

- 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 이용하는 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