



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



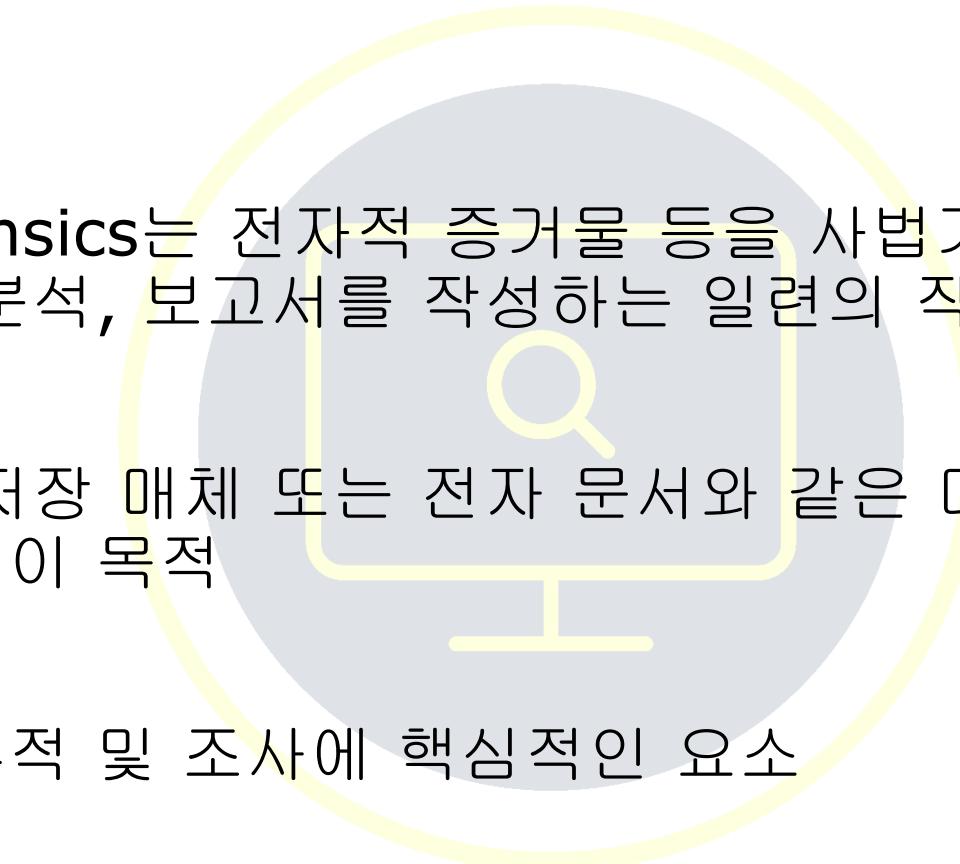
디지털 포렌식이란?

- ☞ 디지털기기를 매개체로 하여 발생한 특정 행위의 사실 관계를 법정에서 **규명하고 증명하기 위한 절차와 방법**이다.
- ☞ 기존의 혈흔, 지문 등의 아날로그 증거와는 다르게 **디지털 데이터는 쉽게 복제가 가능하고 변조할 수 있는 등의 특징**을 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

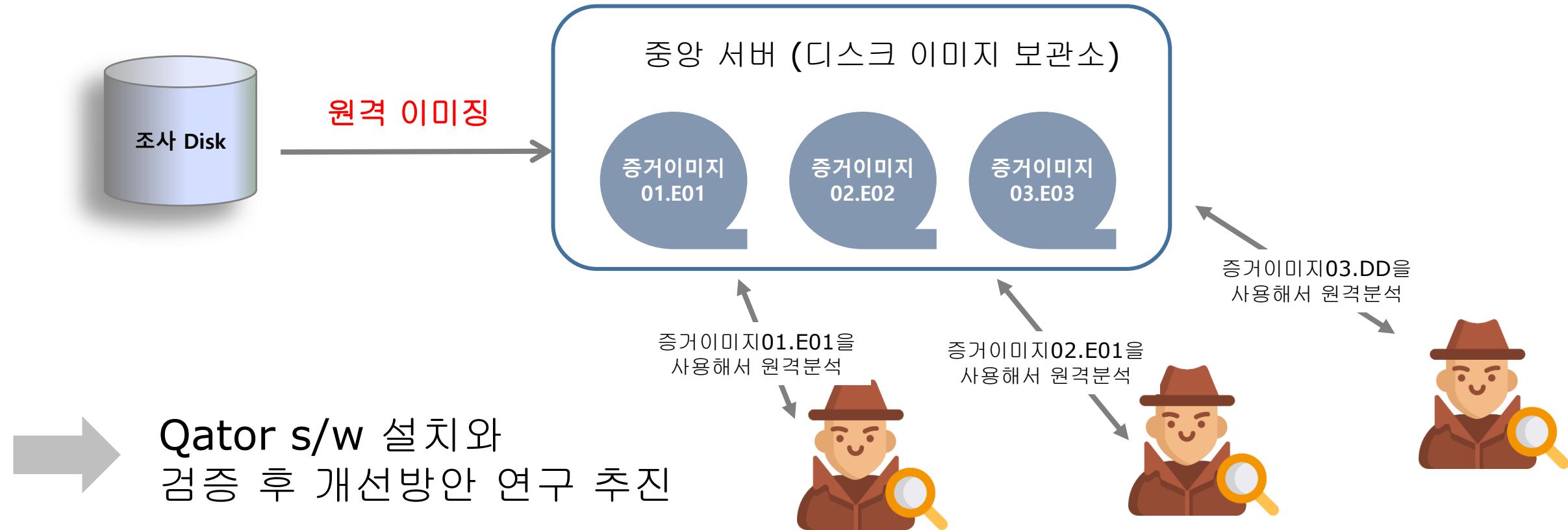
* 수집 이벤트의 휘발성으로 발생 위치에서 분석 및 보안 상태 점검

* 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



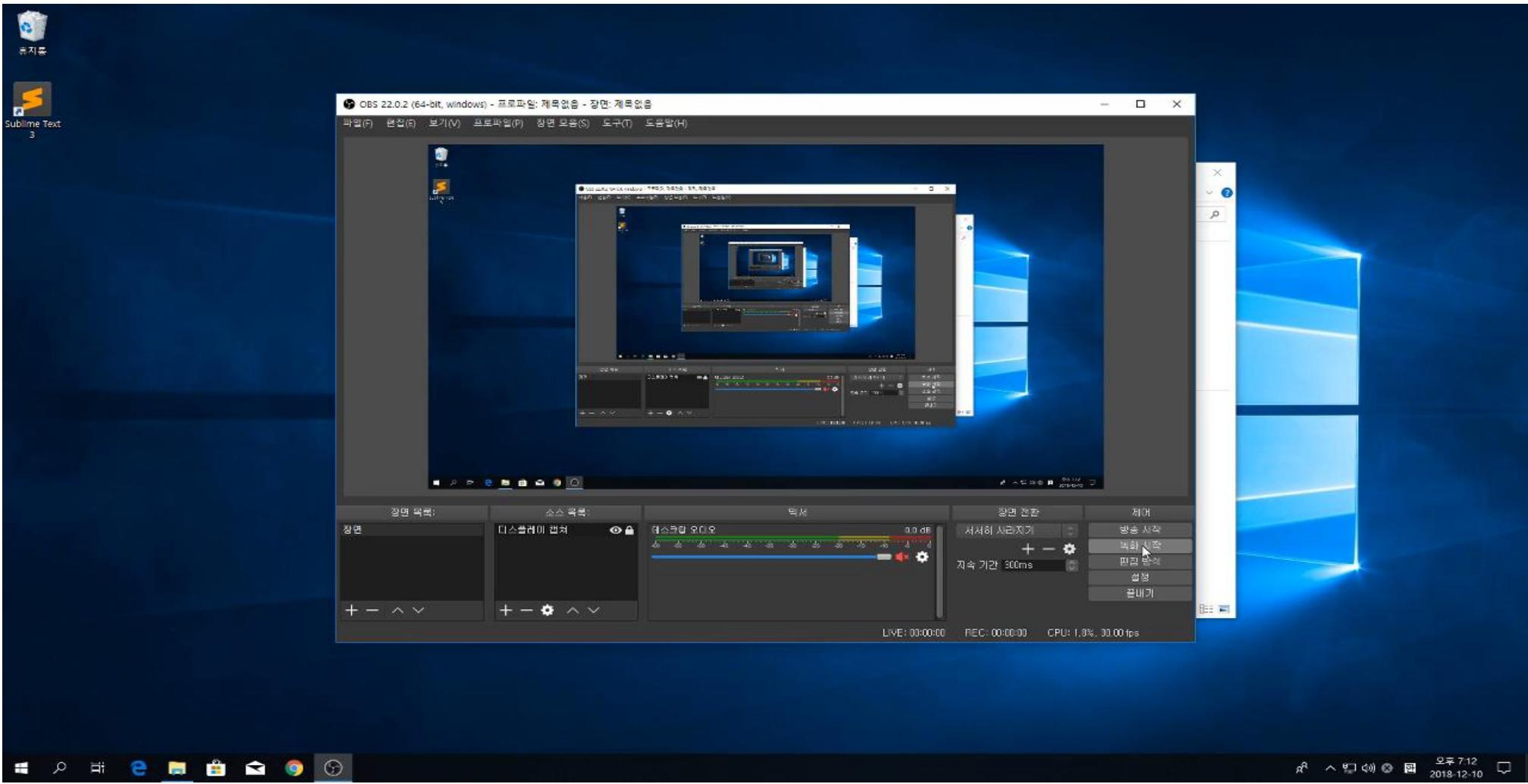
원격 포렌식 분석 도구 Qator



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

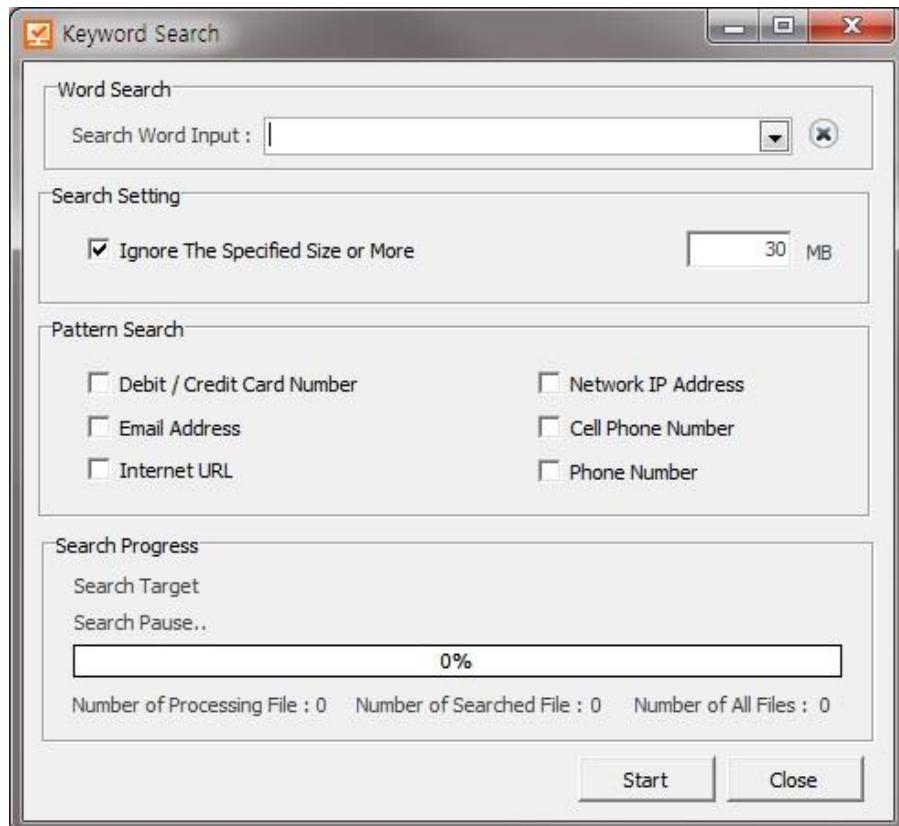
Qator 설치



Qator 기능

□ 검색

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



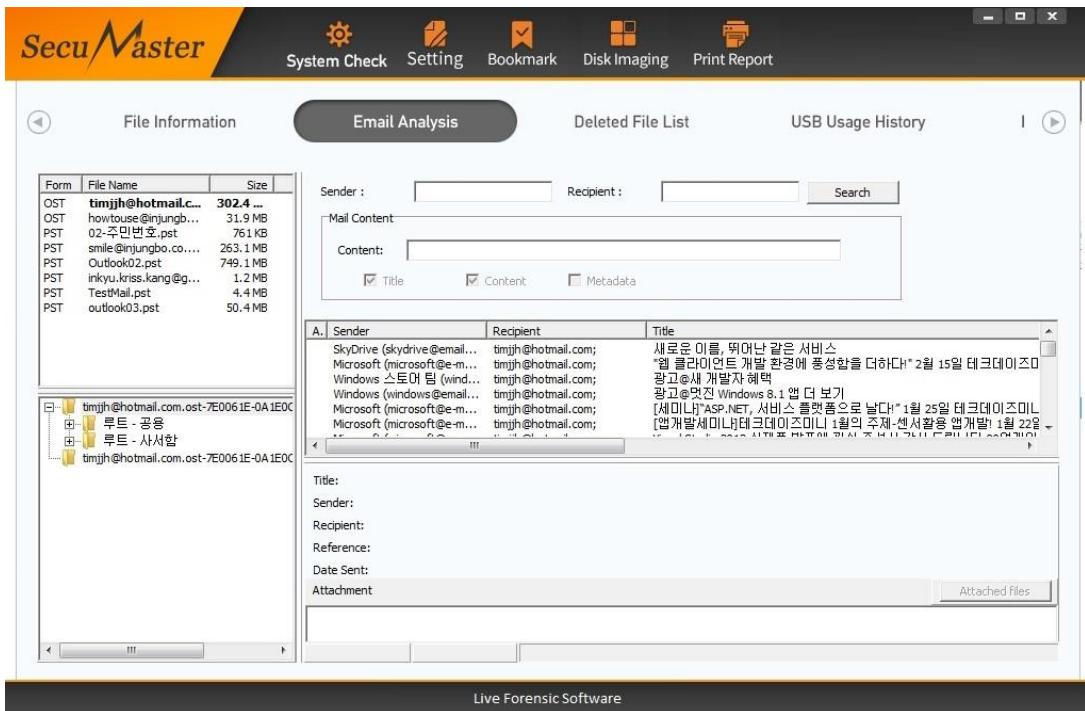
The screenshot shows the SecuMaster software interface. The top menu includes 'System Check', 'Setting', 'Bookmark', 'Disk Imaging', and 'Print Report'. The main area has tabs for 'tion', 'Network and Sharing Information', 'Process List', 'PC Security Analysis', and 'Search Result', with 'Search Result' being the active tab. The search results table lists files found with the keyword 'test'. The columns are 'File Name', 'Searched Keyword', 'Searched File...', and 'Path'. The table contains numerous entries, mostly starting with 'C:\Windows\'. At the bottom of the table are 'Export(Excel)' and 'Add Bookmark' buttons. A footer at the bottom right reads 'Live Forensic Software'.

File Name	Searched Keyword	Searched File...	Path
ListDevices.txt	teSt	1	C:\NVIDIA\DisplayDriver\296.10\WinVista_Win7\International\Display.Drive...
TEST_Parse_type_Paragra...	teSt	1	C:\Program Files\Embarcadero\RAD Studio\7.0\source\unit\Contrib\XP...
TEST_SyncToken.txt	teSt	1	C:\Program Files\Embarcadero\RAD Studio\7.0\source\unit\Contrib\XP...
SiteTemplates.txt	teSt	2	C:\Program Files\Embarcadero\RAD Studio\7.0\objRepos\
CacheSize.txt	teSt	1	C:\Windows\Installer\W\patchCache\Managed\000041099100214000000000...
edu.txt	test	1	C:\Users\Smiler\Documents\리모트운 받은 파일\
bdedeploy.txt	teSt	1	C:\Program Files\Common Files\Borland Shared\BDE\EN\
bdedeploy.txt	teSt	2	C:\Program Files\Common Files\Borland Shared\BDE\
license.txt	teSt	2	C:\Program Files\Opera\locale\en\
README.txt	teSt	1	C:\Users\Guest\AppData\Roaming\Subversion\
COPYING.txt	teSt	1	C:\Users\Smiler\Downloads\fws_4.3.0.0_bin_30\fws_4.3.0.0_bin_30\
ToolbarTopSitesTemplate.pdf	teSt	4	C:\Program Files\Safari\resources\
eula.1031.txt	teSt	4	C:\Windows\Microsoft.NET\Framework\v2.0.50727\Microsoft Visual J# 2.0 R...
eula.1033.txt	test	4	C:\Windows\Microsoft.NET\Framework\v2.0.50727\Microsoft Visual J# 2.0 R...
eula.1041.txt	teSt	4	C:\Windows\Microsoft.NET\Framework\v2.0.50727\Microsoft Visual J# 2.0 R...
EmbeddableGUITestRunner...	teSt	4	C:\ProgramData\{2D559015-4C05-4AE5-8C8B-7E13E1AB09D}\unit\26760...
readme.txt	teSt	4	C:\ProgramData\{2D559015-4C05-4AE5-8C8B-7E13E1AB09D}\unit\26760...
testNextToken.txt	test	8	C:\ProgramData\{2D559015-4C05-4AE5-8C8B-7E13E1AB09D}\unit\26760...
TestSuiteReg.txt	teSt	4	C:\ProgramData\{2D559015-4C05-4AE5-8C8B-7E13E1AB09D}\unit\26760...
test_Get_Token.txt	test	85	C:\ProgramData\{2D559015-4C05-4AE5-8C8B-7E13E1AB09D}\unit\26760...
CnSMR.txt	teSt	1	C:\Program Files\CnPack\CnWizards\Lang\1049\
CnWizards.txt	teSt	1	C:\Program Files\CnPack\CnWizards\Lang\1049\
CnideBRTool.txt	teSt	1	C:\Program Files\CnPack\CnWizards\Lang\1031\
CnManageWiz.txt	teSt	3	C:\Program Files\CnPark\CnWizards\Lang\1031\

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

No.	Process Name	User	Description	Path	Priority	Start Time
1	smss.exe	WWNT AUTHO...	smss.exe	\Windows\Wsys...	Normal	2016-09-08 오전 1...
2	csrss.exe	WWNT AUTHO...	Client Server Runtime Process	C:\Windows\Wsys...	Normal	2016-09-08 오전 1...
3	wininit.exe	WWNT AUTHO...	Windows 시작 응용 프로그램	C:\Windows\Wsys...	High	2016-09-08 오전 1...
4	csrss.exe	WWNT AUTHO...	Client Server Runtime Process	C:\Windows\Wsys...	Normal	2016-09-08 오전 1...
5	services.exe	WWNT AUTHO...	서비스 및 컨트롤러 응용 프로그램	C:\Windows\Wsys...	Normal	2016-09-08 오전 1...
6	lsass.exe	WWNT AUTHO...	Local Security Authority Process	C:\Windows\Wsys...	Normal	2016-09-08 오전 1...
7	lsm.exe	WWNT AUTHO...	로컬 세션 관리자 서비스	C:\Windows\Wsys...	Normal	2016-09-08 오전 1...
8	winlogon.exe	WWNT AUTHO...	Windows 로그온 응용 프로그램	C:\Windows\Wsys...	High	2016-09-08 오전 1...
9	svchost.exe	Unknown	Host Process for Windows Services	C:\Windows\Wsys...	Normal	2016-09-08 오전 1...
10	nvvsvc.exe	WWNT AUTHO...	NVIDIA Driver Helper Service, Versio...	C:\Windows\Wsys...	Normal	2016-09-08 오전 1...
11	svchost.exe	Unknown	Host Process for Windows Services	C:\Windows\Wsys...	Normal	2016-09-08 오전 1...
12	MspfEng.exe	Unknown	Antimalware Service Executable	c:\Program Files\W...	Normal	2016-09-08 오전 1...
13	svchost.exe	Unknown	Host Process for Windows Services	C:\Windows\Wsys...	Normal	2016-09-08 오전 1...
14	svchost.exe	WWNT AUTHO...	Host Process for Windows Services	C:\Windows\Wsys...	Normal	2016-09-08 오전 1...
15	svchost.exe	WWNT AUTHO...	Host Process for Windows Services	C:\Windows\Wsys...	Normal	2016-09-08 오전 1...
16	AUDIOG.DXE	Unknown	Windows 오디오 장치 그래프 드라이버	C:\Windows\Wsys...	Normal	2016-09-08 오전 1...
17	svchost.exe	Unknown	Host Process for Windows Services	C:\Windows\Wsys...	Normal	2016-09-08 오전 1...
18	svchost.exe	Unknown	Host Process for Windows Services	C:\Windows\Wsys...	Normal	2016-09-08 오전 1...
19	spoolsv.exe	Unknown	Spooler SubSystem App	C:\Windows\Wsys...	Normal	2016-09-08 오전 1...
20	nvdsync.exe	WWNT AUTHO...	NVIDIA User Experience Driver Com...	C:\Program Files...	Normal	2016-09-08 오전 1...
21	nvvsvc.exe	WWNT AUTHO...	NVIDIA Driver Helper Service, Versio...	C:\Windows\Wsys...	Normal	2016-09-08 오전 1...
22	svchost.exe	Unknown	Host Process for Windows Services	C:\Windows\Wsys...	Normal	2016-09-08 오전 1...
23	smrwrite.exe	WWNT AUTHO...	Adobe Acrobat\Ivista Service	C:\Program 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

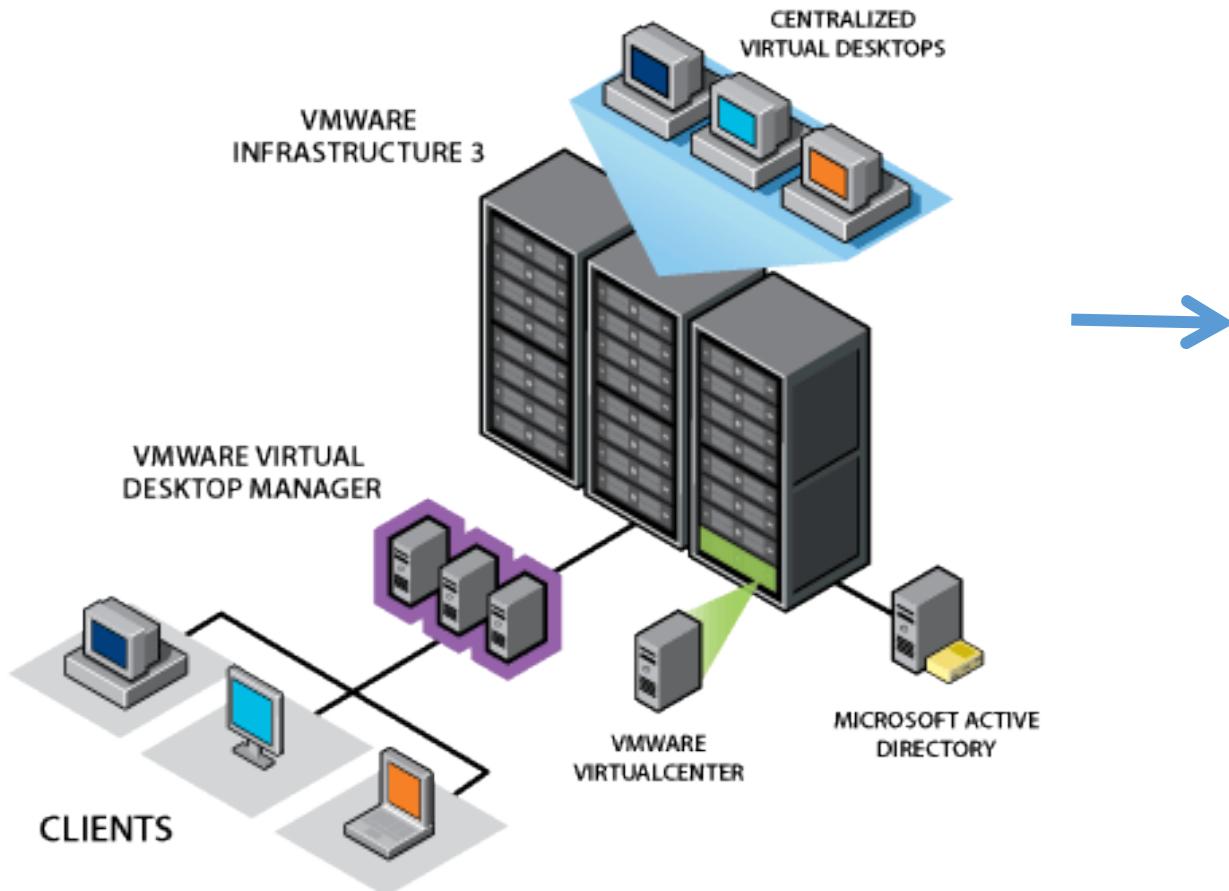


향후 계획

- 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 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 **TOOL**로 사용시 신뢰성이 보장된 서비스 제공 가능

Q & A

THANK YOU

Thanks to 선홍

Thanks to 윤종문 교수님