情報保護學會論文誌
第 23 卷 第 1 號, 2013. 2

윈도우 환경에서의 증거 수집 시스템 설계 및 구현에 관한 연구

이 승 원,[1†] 노 영 섭,[2‡] 한 창 우[1]
[1]지식경제사이버안전센터, [2]서울벤처대학원대학교

A Study on the Design and Implementation of an Digital Evidence Collection Application on Windows based computer

SeungWon Lee,[1†] YoungSup Roh,[2‡] Changwoo Han[1]
[1]MKE Cyber Security Center, [2]Seoul Venture University

요 약

침해사고는 시스템 해킹, 바이러스 및 웜, 홈페이지 변조, 자료 유출 등 그 유형이 다양하고, 단순한 바이러스나 웜 등의 유포가 아닌 개인정보 및 기업기밀 정보를 취득하거나 금전적 이득을 취하기 위한 목적으로, 공격자가 사용하는 공격 기법이 고의적인 데이터의 삭제나 변경 등 고도의 은닉 기법을 활용하여 흔적을 남기지 않기 때문에, 정확한 자료를 수집하기가 쉽지 않다. 침해사고 초기 대응시 초동 대응자는 신속한 조사를 수행해야할 필요가 있는 침해위협 또는 범죄와 관련 현장 정보를 취급한다. 이때 체계적인 증거 수집을 위하여 침해사고의 식별에 적합한 디지털 포렌식 프로세스 방법론의 적용이 요구된다.

본 논문에서는 초동 대응자가 효과적인 초기 대응을 위하여, 윈도우 시스템 환경에서의 디지털 포렌식 측면에서 CFFTPM 포렌식 프로세스 모델을 적용하여 사용자 사용 정보, 타임라인 정보, 인터넷 정보 등 증거 수집 기본정보를 분석하고 이에 따라 클라이언트/서버 모델로 증거수집 응용시스템을 설계하고 이를 구현하였다.

ABSTRACT

Lately, intrusive incidents (including system hacking, viruses, worms, homepage alterations, and data leaks) have not involved the distribution of an virus or worm, but have been designed to acquire private information or trade secrets. Because an attacker uses advanced intelligence and attack techniques that conceal and alter data in a computer, the collector cannot trace the digital evidence of the attack. In an initial incident response first responser deals with the suspect or crime scene data that needs investigative leads quickly, in accordance with forensic process methodology that provides the identification of digital evidence in a systematic approach.

In order to an effective initial response to first responders, this paper analyzes the collection data such as user usage profiles, chronology timeline, and internet data according to CFFPM(computer forensics field triage process model), proceeds to design, and implements a collection application to deploy the client/server architecture on the Windows based computer.

Keywords: digital forensics, digital evidence, evidence collection, collection software

접수일(2012년 6월 4일), 수정일(1차: 2012년 7월 27일 , 2차: 2012년 10월 19일, 3차: 2012년 12월 24일), 게재확정일(2013년 1월 15일)

† 주저자, swlee1201@gmail.com
‡ 교신저자, youngs.roh@gmail.com

I. 서 론

최근 침해사고는 단순한 바이러스나 웜 등의 유포가 아닌 개인정보 및 기업기밀 정보를 취득하거나 금전적 이득을 취하기 위한 목적으로 장시간에 걸쳐 지능적이고 다양한 최신의 공격기법이 활용되고 있다. 이에 따라 침해사고의 위협은 점차 증가되고 있으며, 침해 기관의 피해 또한 대형화되어 해당 기관의 존립과도 직결되기도 한다.

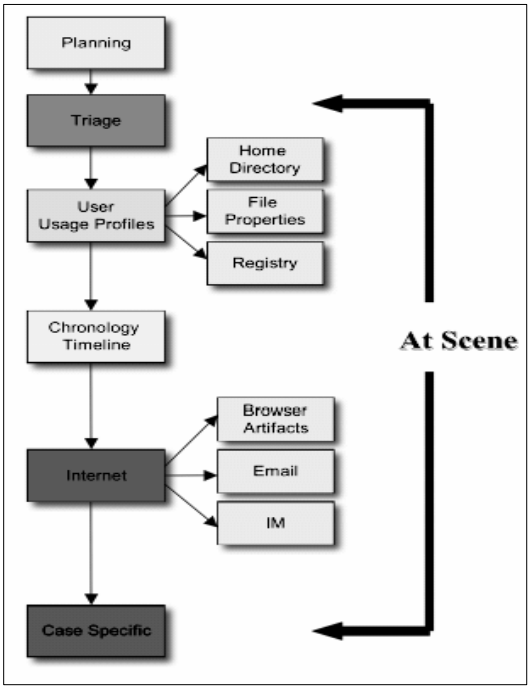
디지털 증거는 쉽게 변경될 수 있고, 특정 악성코드는 고도로 지능화된 은닉기법의 사용으로 특정 프로그램을 시스템 파일처럼 위장하고, 관련 설치 파일을 제거하여 흔적을 남기지 않기도 한다. 디지털 증거의 효과적 분석을 위하여 디지털 포렌식 도구가 점차 필수적으로 사용되고 있다.

일반적인 디지털 포렌식의 절차는 준비, 사고 식별, 데이터 수집, 보관, 조사 및 분석, 보고서 작성 단계로 이루어진다. 침해 사고가 식별되면 증거수집 단계가 진행되는데, 증거 수집 단계에서는 저장 매체, 데이터, 시스템 및 네트워크, 응용 프로그램 등 다양한 정보를 정밀하고 정확하게 수집해야 한다.

본 논문은 먼저 사전 연구된 CFFTPM(Computer Forensic Field Triage Process Model)을 파악한 후에, 윈도우 환경에서 요구분석을 위하여 윈도우 디지털 포렌식을 위한 디지털 증거 수집 기법을 조사하여 관련 스크립트를 분석하고, 적용하는 방법론에 따라 클라이언트/서버 모델을 도입하여 자료 수집 프로그램을 설계하고 구현한다.

II. 적용방법론 사전 연구

Rogers 등은 침해사고 현장에서 실시간으로 분석할 수 있는 CFFTPM을 제안하였다[1]. 이 모델은 [그림 1]과 같이 계획 단계(planning), 분류 단계(triage), 사용자 사용 프로파일 단계(user usage profiles), 타임라인 단계(chronology/timeline), 인터넷 단계(internet), 특정 사례 단계(case specific)로 분류하였다. 사용자 사용 프로파일 단계는 홈 디렉토리(home directory), 파일 특성(file properties), 레지스트리 단계로 세분된다. 인터넷 단계도 브라우저 부산물, 이메일, 인터넷 메신저 단계로 구분된다. CFFTPM은 MS 윈도우 환경을 적용한 정형화된 프로세스 모델로의 정제된 현실세계의 접근법의 공식화로써 현장에서 실시간 정보인 휘발성 및



[그림 1] CFFTPM 단계

비휘발성 데이터를 수집 시에 많이 활용된다. 이 방법론의 특징은 사용할 수 있는 증거를 즉시 찾고, 예민한 자료를 식별하며, 실시간 증거조사를 가이드하며, 잠재적인 혐의를 식별하고, 사회에 대한 공격자의 위해(damage)를 정확하게 접근시킨다.

본 연구에서는 CFFTPM 모델을 적용하는 것을 근간으로 하여 데이터 수집에 대해 설계하여 구현하도록 하는 것을 전제로 한다.

III. 요구사항 분석 관련 연구

3.1 스크립트를 이용한 자료 수집

초기분석 단계에는 현재 구동 중인 프로세스 정보나 네트워크 상태 정보 등 휘발성 정보를 수집해야 한다. 피해 시스템 상황을 파악하기 위해 윈도우 명령어를 사용하여 프로세스, 네트워크, 로그인 정보들을 수집하여 시스템 변경 내용이나 공격자의 흔적을 파악해야 한다.

한국인터넷진흥원에서 2010년 발간한 침해사고 분석 절차 안내서에서 윈도우 사고 분석 시 침해사고 분석은 자료를 수집하는 초기분석, 루트킷 점검, 상세분석, 해킹 프로그램 분석으로 구분하여 스크립트를 제

〔표 1〕 스크립트에 포함된 시스템 분석 모듈

모 듈	각 모듈이 제공하는 정보
date /t	분석 시작/종료 날짜
time /t	분석 시작/종료 시간
uptime	시스템 가동 시간
psinfo -h -s	설치된 핫픽스 및 소프트웨어 목록
pslist -t	현재 프로세스 리스트 출력
listdlls	프로세스들이 사용하는 DLL들 출력
handle	프로세스들이 참조하는 파일 리스트 출력
ipconfig /all	시스템 아이피 정보 수집
netstat -an	서비스 중인 포트 정보 및 연결된 아이피 정보
fport	서비스 중인 포트를 열고 있는 프로그램 정보
promiscdetect	NIC가 promisc 모드로 동작중인지 확인
net user	시스템에 존재하는 계정정보 출력
net localgroup	시스템에 존재하는 그룹정보 출력
net share	시스템 공유 정보
net session	공유자원에 접속한 컴퓨터 정보 출력
nbstat -c	NBT에 연결된 세션 정보 출력
ntlast -f	원격접속 로그 정보 출력

시하였다〔2〕. 초기분석의 데이터 수집 순서로는 시스템 시간 확인, 시스템 정보, 프로세스 정보 확인, 네트워크 정보 확인, 사용자/그룹 확인, 공유와 로그인 정보 확인 등이 있으며 사용되는 명령어 스크립트는 〔표 1〕과 같다〔2,3〕. 또한 공개용 도구를 이용해 정보를 자동으로 수집해 주는 도구를 사용할 수 있으며 수집된 정보를 브라우저로 확인하는 기능을 제공하는 WFT(Windows Forensic Toolchest) 사용을 추천한다.

일반적으로 정보수집 도구로써 수사에 사용되는 포렌식 도구가 사용하는 명령어는 〔표 2〕와 같다〔4,5〕.

〔표 2〕 포렌식 도구의 명령어

포렌식 도구	활성 데이터
pslist	활성화 상태의 윈도우 프로세스 리스트
pslog	현재 로그온 한 윈도우 사용자의 세션 정보
psinfo	로컬 또는 원격 윈도우 시스템 정보
net accounts	사용자 계정 데이터베이스 업데이트/계정의 암호와 로그온에 필요한 사항
net file	서버에 열려있는 모든 공유 파일 이름
route print	로컬 IP 라우팅 테이블 항목
net session	로컬 컴퓨터의 모든 세션 정보
net start	현재 실행 중인 서비스 목록
net user	사용자 계정 추가/수정 및 사용자 계정 정보
net use	컴퓨터 공유 리소스 연결/해제 및 컴퓨터 연결 정보 표시

미 공군 침해사고대응팀에서 사용하는 FRED(First Responder's Evidence Disk)의 배치 프로그램의 내부의 사용 명령어는 〔표 3〕과 같다〔3,6〕.

〔표 3〕 "FRED.bat" 내의 시스템 분석 모듈

모듈	각 모듈이 제공하는 정보
date /t	분석 시작/종료 날짜
time /t	분석 시작/종료 시간
psinfo	로컬 또는 원격 윈도우 시스템 정보
net accounts	사용자 계정 데이터베이스 업데이트/계정의 암호와 로그온에 필요한 사항
net file	서버에 열려있는 모든 공유 파일 이름
route print	로컬 IP 라우팅 테이블 항목
net session	로컬 컴퓨터의 모든 세션 정보
net start	현재 실행 중인 서비스 목록
net use	컴퓨터 공유 리소스 연결/해제 및 컴퓨터 연결 정보 표시
net user	사용자 계정 추가/수정 및 사용자 계정 정보
net view	네트워크 구성원 정보
arp -a	ARP cache 정보
netstat -anr	네트워크 연결상태(라우트 테이블 정보 포함)
psloggedon	로컬 원격 로그온 정보
listdlls	프로세스들이 사용하는 DLL들의 정보
fport/p	포트 정보(번호 기준 오름차순 정렬)
pslist -x	프로세스 정보(메모리 및 쓰레드 정보 포함)
nbtstat -c	NBT에 연결된 세션 정보
dir /s /a:h /t:a c:\	숨김 속성의 디렉터리 및 파일에 대한 정보 (마지막 접근시간 기준 오름차순 정렬)
md5sum c:*.*	c 드라이브의 모든 파일의 MD5값 획득

또한 윈도우 2000 및 XP에서 사용 가능한 휘발성 정보를 수집하는 스크립트의 예로써 〔표 4〕를 제시하고 있다〔7,8〕.

수사의 초동 단계의 분석내용과 비교해서 진전된 연구로는 윈도우 포렌식을 중심으로 디지털 증거의 법적 증명력을 위한 디지털 포렌식에 관한 연구가 있다〔9〕. 윈도우 포렌식 측면에서 주요 프로세스를 식별하였고, 먼저 휘발성 증거의 수집 및 분석, 둘째로 시스템 증거의 수집 및 분석으로 날짜 및 시간 정보 수집, IP 정보의 수집, 시스템 정보의 수집, 공유폴더, 그리고 메모리 덤프, 셋째로 레지스트리 증거 수집 및 분석으로 로그인한 사용자의 Default 폴더 확인, 최근에 열었거나 실행·수정한 문서에 대한 사용 흔적, 최근 네트워크 연결에 대한 사용 흔적, 메신저 정보 확인, 사용자 계정 추가 확인, 바이러스 같은 악성 코

[표 4] 휘발성 정보 수집 스크립트 예

포렌식 도구	활성 데이터
date /t time /t	시스템 시작 날짜와 시간 (시작 시간)
psloggedon	현재 로그온되어 있는 사용자 목록
dir /t:a /o:d /a /s c:\ dir /t:a /o:d /a /s c:\	파일 시스템의 time/date stamp
netstat -na	열려 있는 소캣 목록
fport	열려진 소캣에 대기하고 있는 어플리케이션
plist	현재 동작하는 프로세스 목록
nbstat -c	현재 또는 최근 시스템에 연결했던 시스템들의 목록
date /t time /t	시스템 시작 날짜와 시간(종료 시간)
doskey /historyr	작업 히스토리 기록

드 프로그램 감염 여부, 컴퓨터 정보, 그리고 Office 제품군 최근 사용 내역 보기, 넷째로 윈도우 운영체제별 레지스트리 백업 및 복구로 Regexe(NTResourceKit)와 실행되고 있는 레지스터 정보, 다섯째로는 네트워크 증거 수집 및 분석으로 현재 사용 중인 TCP/UDP에 정보와 ARP 정보 등을 제시하였다.

3.2 웹 브라우저 정보 수집

웹 브라우저는 인터넷 사용 정보를 웹 브라우저 생성 파일에 기록한다. Internet Explorer는 〔그림 2〕와 같이 index.dat 파일에 기록한다[1]. index.dat는 웹에 근거한 e-mail의 접근을 포함(e-mail 내용은 미포함)하여 방문한 인터넷 사이트의 실행 레코드를 내포하고[1], 사용자가 방문한 웹사이트에 대한 쿠키, 히스토리, 인터넷 임시 파일 정보 등이 기록된다[3,10].

IV. 시스템 설계

4.1 설계 개념

4.1.1 설계 방향

수집된 데이터를 디지털 포렌식 전문가가 분석할 수 있도록, 앞에서 제시한 CFFTPM 방법론에 따라 비휘발성 정보까지 수용하여 초기 대응을 위한 디지털 증거 자료의 수집 소프트웨어를 설계한다. 요구사항 분석의 사건 초기 대응 수집 정보 요약을 기준으로 하여 설계한다.

```
==========================================
URL          : http://us.f307.mail.yahoo.com/ym/ShowFolder?rb=Inbox&reset=1&YY=85059
Title        : Yahoo! Mail - xxxxxxxx@yahoo.com
Hits         : 21
Modified Date    : 10/4/2005 9:06:37 PM
Expiration Date  : 10/30/2005 9:06:38 PM
User Name        : xxxxxx
==========================================
This example shows a user accessing their yahoo account for the 21st time on 10/4/2005.
```

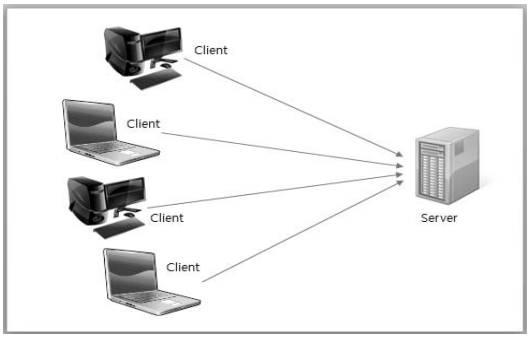
〔그림 2〕 index.dat 예

- 윈도우 환경의 클라이언트/서버 구조의 전용 수집 도구 설계
- 현장에서 사용자가 쉽게 사용하고 성능이 좋은 도구 설계
- 윈도우 명령어와 내부 인터널(Sysinternals)을 사용하고, 관련 데이터는 자동화된 공개용 패키지가 있을 때는 이를 활용토록 설계
- 수집된 데이터는 포렌식 증거로서 법적 효력을 갖도록 MD5 해시값 사용

본 시스템 설계의 한계는 사고발생한 현장의 디지털 증거를 간단히 수집하는 것을 전제로 하기 때문에 사고 유형별로 사고를 분류하여 수집하지 못하고 일괄로 전체 데이터를 수집하는 한계가 있다.

4.1.2 네트워크 구조

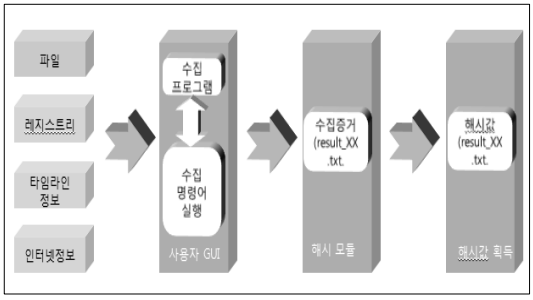
데이터 수집 소프트웨어는 사내망에서 중앙 서버와 수집 대상 PC가 연결되는 단순 클라이언트/서버 개념〔그림 3〕을 도입하여 클라이언트는 수집된 데이터를 MD5 해시를 적용하여 암호화하여 서버에 전송하며, 서버는 수신된 자료를 이중화 복사하여 원본과 사본을 구분하여 보존토록 한다.



〔그림 3〕 클라이언트-서버 구조

4.1.3 구현 방식 및 구성요소

본 프로그램은 .NET 방식 개념을 도입하여 클라이언트/서버 구조의 프로그램을 개발한다. 서버 모듈은 수집된 해시 데이터를 수신하고 이를 이중화시키는 기능을 갖는다. 클라이언트 모듈은 〔그림 4〕와 같이 실행되고 증거의 무결성을 유지하기 위해 MD5 해시 값을 자동으로 계산하여 수집된 증거와 함께 암호화하여 전송되도록 설계한다.



〔그림 4〕 클라이언트 수집 도구의 도식화

4.2 사용자/사용 프로파일

4.2.1 홈 디렉토리

시스템 중요 폴더의 실행파일 목록

윈도우 시스템 폴더(%windir%)와 시스템 관련 폴더(%windir%\system32), 휴지통(Recycler) 폴더 등에 있는 실행 파일(exe, dll) 목록과 해당 파일의 해시 값을 추출한다.

사용자 정보

〔표 5〕의 명령어를 이용하여 공격자에 의해 추가된 그룹이나 사용자가 없는지 확인한다. 특히 관리자 그룹에 속한 사용자 목록은 보다 관심 있게 파악해야 한다.

〔표 5〕 사용자 정보 수집 명령어

명령어	제작사	기능
net user	윈도우 내부명령	사용자 계정 목록 추출
net localgroup Administrators	윈도우 내부명령	관리자 그룹(Administrators)에 속한 사용자 목록 추출
UserProfiles View	NirSoft	시스템에 존재하는 모든 사용자 프로파일 목록 추출

시스템 관련 정보

〔표 6〕의 명령어를 이용하여 OS의 기본 정보 및 보안 업데이트 정보 등과 함께 설치된 소프트웨어 정보를 확인한다. 보안 업데이트 정보는 시스템 취약점을 통해 공격한 정보를 획득할 수 있기 때문에 최종 갱신일자를 확인해야 한다.

〔표 6〕 시스템 관련 정보 수집 명령어

명령어	제작사	기능
psinfo -d	Sysinternals	설치된 OS 종류, 커널 빌드, 물리적 메모리 양, 시스템 설치 날짜 그리고 'd' 옵션을 이용하여 디스크 볼륨 정보 등을 포함한 시스템 정보 추출
wul	NirSoft	'WinUpdatesList' 프로그램을 이용하여 시스템에 설치된 윈도우 업데이트 목록(서비스 팩과 핫 픽스) 추출

4.2.2 파일 특성

시스템에 설치된 프로그램과 윈도우 시작 시 자동으로 시작되는 프로그램 목록

윈도우 시스템에 설치된 프로그램 목록 확인과 윈도우가 시작될 때 자동으로 로딩되는 프로그램은 〔표 7〕의 명령어를 이용하여 확인한다. 일반적으로 윈도우 시작 시 자동으로 실행하는 프로그램은 레지스트리에 등록되어 있다 악성 코드 프로그램을 레지스트리에 등록하여 시스템 부팅 시 자동으로 실행되도록 하므로 분석시 중요한 정보로 인식된다. Sysinternals에서 제공하는 Autorun를 이용하여 확인하기도 한다.

〔표 7〕 프로그램 관련 정보 수집 명령어

명령어	제작사	기 능
myuninstexe	NirSoft	시스템에 설치되어 있는 어플리케이션 목록 추출
WhatInStartupexe	NirSoft	윈도우가 시작할 때 자동으로 로딩되는 어플리케이션별 시작 형태, 명령 구문, 제품명, 파일 버전, 회사명, 레지스트리 위치 등의 정보 추출

프리패치 파일 목록

응용 프로그램이 실행될 때 운영체제에 의해 자동으로 해당 어플리케이션 관련 정보를 프리패치 파일에 저장하게 되는데, 프리패치 파일은 응용 프로그램을

〔표 8〕 Prefetch 파일 목록 수집 명령어

명령어	제작사	기 능
WinPrefetch View	NirSoft	시스템 저장된 Prefetch 파일을 읽어 저장된 정보 추출

다음에 실행할 경우 로딩 시간 최적화를 위해 사용된다. 응용프로그램 사용 횟수 및 마지막 실행 시간 확인을 위해 〔표 8〕의 명령어를 이용하여 확인한다.

4.2.2 레지스트리

프로세스 정보 확인

프로세스 중에는 공격자가 설치한 악성 코드가 실행되거나 침입한 흔적이 존재할 수 있으므로 〔표 9〕의 명령어를 이용하여 확인한다.

〔표 9〕 프로세스 관련 정보 수집 명령어

명령어	제작사	기 능
pslist -t	Sysinternals	현재 시스템에서 실행 중인 프로세스 목록을 't'옵션을 사용하여 트리형태로 추출
CProcessexe	NirSoft	'CurrProcess' 프로그램을 이용 현재 시스템에서 실행 중인 모든 프로세스 목록을 제품명, 버전, 회사명 등 추가적으로 유용한 정보를 함께 출력
ListDllsexe	Sysinternals	프로세스에 의해 로딩된 모든 DLL 목록 추출

시스템에 구성된 서비스와 드라이버 목록

시스템 구성 서비스 목록과 드라이버 목록은 〔표 10〕의 명령어를 이용하여 확인한다. 대부분의 공격자 프로그램이 정상적인 서비스 이름으로 가장하고 있기 때문에 현재 수행되고 있는 서비스 목록을 인식하여 실행 파일 경로가 올바른지 확인해야 한다.

〔표 10〕 프로그램 관련 정보 수집 명령어

명령어	제작사	기 능
serviwin services	NirSoft	'ServiWin' 프로그램을 이용하여 시스템에 설치된 드라이버와 서비스 목록을 추출
serviwin drivers	NirSoft	

이벤트 로그와 USB 히스토리 정보

이벤트 로그는 하드웨어, 소프트웨어 및 시스템 문제를 저장한다. 이벤트 로그는 공격자의 흔적 및 활동 정보를 남기기 때문에 〔표 11〕의 명령어를 이용하여 확인한다. 공격이 있었더라도 공격자는 공격 흔적을 지우기 위해 'ClearEvent' 같은 프로그램을 사용해 이벤트 로그를 삭제할 수 있으므로 이벤트 로그가 남지 않을 수도 있다.

〔표 11〕 event log와 USB History 정보 수집 명령어

명령어	제작사	기 능
psloglist -d 7 -f we	Sysinternals	컴퓨터의 이벤트 로그 내용을 최근 7일간 Error와 Warning 이벤트만 필터링하여 추출
USBDeview	NirSoft	현재 컴퓨터에 연결되어 있는 USB 기기와 예전에 사용되었던 모든 USB 기기 목록 추출

4.3 타임라인 정보

시스템 시간 확인

시스템 시간 확인을 위해서는 〔표 12〕의 명령어를 사용하여 시스템별로 운영되는 고유의 시간을 파악하면 이와 연관되는 시스템 로그시간을 파악할 수 있다. uptime은 시스템 부팅시간을 알려준다.

〔표 12〕 시스템 날짜와 시간 수집 명령어

명령어	제작사	기 능
date /t	윈도우 내부명령	시스템 현재 날짜 출력
time /t	윈도우 내부명령	시스템 현재 시간 출력
uptime	Sysinternals	시스템 가동 시간

최근 파일 목록

윈도우 파일 시스템은 모든 디렉토리나 파일과 관련되어 MAC(mtime, atime, ctime) 정보를 갖는다. 이를 기준으로 하여 최근에 사용한 파일목록을 〔표 13〕의 명령어를 이용하여 확인한다.

〔표 13〕 최근 파일 목록 수집 명령어

명령어	제작사	기 능
RecentFilesView	NirSoft	최근에 사용한 파일 목록 추출

예약된 작업 목록

공격자는 일반적 공격 시간을 정하여 특정 프로그램을 수행하도록 지정하는 경우가 많다. 〔표 14〕의 명령어를 이용하여 예약된 작업 목록을 확인한다.

〔표 14〕 예약된 작업 목록 수집 명령어

명령어	제작사	기 능
schtasks /Query /FO TABLE /V	윈도우 내부명령	예약된 작업 목록 추출

4.4 인터넷 정보

4.4.1 브라우저 부산물(artifacts)

인터넷 브라우저(Internet Explorer) 관련 정보

인터넷 브라우를 통해 특정 사이트를 접속하면 관련 사이트의 페이지는 임시파일에 저장되며 접속한 기록이 히스토리에 남는다. 사용되었던 쿠키도 저장되므로 이러한 파일을 〔표 15〕의 명령어를 이용하여 확인함으로써 공격자의 흔적을 찾아 낼 수 있다.

〔표 15〕 인터넷 브라우저(IE) 관련 정보 수집 명령어

명령어	제작사	기능
iehv	NirSoft	'IEHistoryView' 프로그램을 이용하여 사용자 방문한 모든 URL 목록을 추출
IECache View	NirSoft	'IECacheView' 프로그램을 이용하여 Internet Explorer 캐시 정보를 수집한다 해당 프로그램은 Internet Explorer 캐시 폴더를 읽어 현재 캐쉬에 저장된 파일의 목록을 수집

DNS 설정 파일변조 확인 (hosts)

DNS 설정 파일변조 확인은 '%windir%\system32\drivers\etc\hosts' 파일을 확인한다.

네트워크 정보 확인

피해시스템의 네트워크 정보, 서비스를 열로 있는 응용 프로그램의 정보, 서비스에 연결되어 있는 세션 정보 등은 공격자의 흔적을 추적할 수 있는 주요한 정보로 〔표 16〕의 명령어를 이용하여 확인한다.

〔표 16〕 네트워크 관련 정보 수집 명령어

명령어	제작사	기 능
ipconfig /all	윈도우 내부명령	Network 어댑터별 TCP/IP 통신을 하기 위한 IP주소, Subnet Mask, 기본 Gateway와 같은 모든 설정정보 출력
net session	윈도우 내부명령	현재 시스템에 연결된 모든 세션 정보 출력
net file	윈도우 내부명령	네트워크상에 모든 열린 공유 파일 목록 출력
net share	윈도우 내부명령	현재 시스템의 모든 공유 자원에 대한 목록 출력
net view	윈도우 내부명령	현재 도메인 정보를 공유하는 컴퓨터 목록 출력
nbtstat -c	윈도우 내부명령	NetBIOS 이름과 IP 주소 매핑 정보를 포함하는 NetBIOS 이름 캐쉬 데이터 목록 출력
nbtstat -n	윈도우 내부명령	NetBIOS 어플리케이션에 의해 현재 시스템에 등록된 이름 목록 출력
arp -a	윈도우 내부명령	모든 인터페이스에 대해 현재 ARP(Address Resolution Protocol) cache 테이블 정보를 출력
netstat -ano	윈도우 내부명령	프로토콜 통계 및 현재 TCP/IP 네트워크 연결을 표시하는 netstat 명령에서 모든 연결 및 수신 대기 포트를 표시하는 'a'옵션, 주소 및 포트 번호를 숫자 형식으로 표시하는 'n'옵션 그리고 프로세스 관련 수집 데이터와의 연관성을 위해 각 연결마다 프로세스 ID(PID)를 표시하는 'o'옵션을 같이 사용하여 활성화된 네트워크 연결 목록 추출
cportsexe	NirSoft	netstat 명령으로 확인할 수 있는 정보에 더해 현재 활성화되어 있는 TCP/IP 와 UDP 포트 목록을 비롯하여 프로세스 실행 경로와 생성시간 등의 정보를 확인할 수 있는 'CurrPorts' 프로그램을 이용하여 네트워크 연결 정보 추출

sniffer 작동 유무 확인

〔표 17〕과 같이 확인하여 네트워크 동작이 만약 무차별 모드로 작동하고 있으면 해당 시스템에 스니핑 프로그램이 작동하고 있는 것으로 파악한다. Active filter 상태가 정상(directed, multicast and broadcast)인지 확인하며, sniffer가 작동하지 않더라도 VMWare가 구동 중이면 무차별(promiscuous) 모드가 나타난다.

〔표 17〕 프로세스 관련 정보 수집 명령어

명령어	제작사	기 능
promiscdetectexe	ntsecurity	네트워크 어댑터가 무차별 모드로 작동하고 있는지 유무를 확인할 수 있다.

4.4.2 이메일 정보

이메일 정보

이메일 사용 정보는 이메일 송·수신 정보를 확인할 수 있는 정보로 마이크로소프트사의 아웃룩 프로그램에 대하여 수집한다. 해당 기본 폴더는 C:\Documents and Settings\user\Local Settings\Application Data\Identities\{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX}\Microsoft\Outlook Express이다.

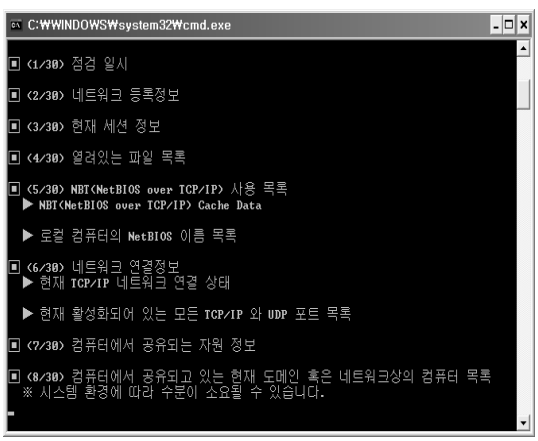
4.4.3 인스턴트 메시징 부산물

메신저 정보

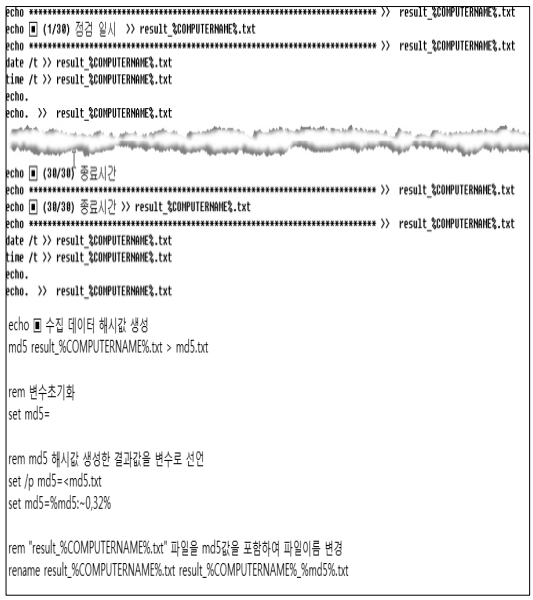
메신저 정보는 상대방과의 실시간 대화와 송·수신을 지원한다. 메신저에서 수집하는 정보는 사용자의 ID, 대화 내용 저장 폴더, 파일 다운로드 폴더, 쿠키 파일 등으로 이루어진다. 메신저는 Nateon, MSN 메신저를 포함시킨다.

V. 시스템 구현 및 평가

5.1 시스템 구현



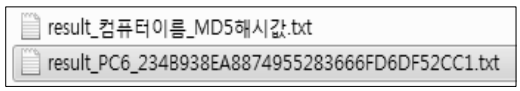
〔그림 5〕 프로그램 실행화면



〔그림 6〕 배치파일 형태

디지털 데이터 수집 프로그램은 클라이언트/서버 구조로 설계한 내용에 따라 구현하였다. 윈도우 시스템에서 제공하는 기본적인 명령어와 'Sysinternals', 'NirSoft' 등에서 제공하는 도구들을 활용하여 정보를 수집한다. 설계 내용을 토대로 스크립트 로그가 〔그림 5〕과 같이 화면에 표시하면서 실행한다.

클라이언트는 〔그림 6〕처럼 배치파일 형태로 실행시간과 함께 수집된 데이터가 저장된다. 저장된 데이터는 〔그림 7〕과 같이 MD5 해시값을 생성하여 암호화되어 서버에 전송된다. 서버는 수집된 데이터의 원본에서 이중화를 위해 사본을 복사한다.



〔그림 7〕 해시값을 포함한 수집데이터 생성

5.2 구현 시스템 평가

5.2.1 기능 평가

사건 초기대응 수집 데이터는 활성 데이터와 비활성 데이터로 구분된다. 이는 고려대학교 디지털포렌식 연구센터에서 작성한 "디지털 증거 처리 가이드라인"의 초기대응 및 데이터수집 항목에서 〔표 18〕과 같이 정의되어 있으며〔11〕, 본 연구에서 설계한 시스템은

이 기준을 만족하고 있다. 활성 데이터 수집은 시간 정보 수집, 물리메모리 및 가상 메모리 수집, 실행 프로세스 수집, 네트워크 정보 수집, 열린 파일 정보(운영체제, IP 설정 정보, 물리 디스크 사용 정보) 수집으로 구분되며, 비휘발성 정보 수집은 파일 및 디렉토리 정보 수집, 운영체제 설정 파일 수집, 인터넷 히스토리 파일 정보 수집, 로그 파일(IIS 로그, Windows 로그 파일, 이벤트 로그 파일), 해시값 계산이 있다.

〔표 18〕 가이드라인 제시 항목

활성 데이터 수집	시간 정보 수집	
	물리 메모리 및 가상 메모리	
	실행 프로세스	
	네트워크 정보	
	열린 파일 정보	
	시스템 정보 및 각종 설정 정보	운영체제 정보
		IP설정 정보
		물리 디스크 사용정보
	사용자 정보	
비활성 데이터 수집	파일 및 디렉토리 정보	
	운영체제 설정 파일	
	인터넷 히스토리 파일	
	로그 파일	IIS로그
		Windows 로그
		이벤트 로그
	해시값 계산	

〔표 19〕 시험 플랫폼

PC 1	
OS	Windows 7 Professional
Physical memory	2014 MB
Processor type	Intel(R) Core(TM)2 Duo CPU E8400 @
HDD 용량	153.28 GB
PC 2	
OS	Microsoft Windows Server 2003 R2
Physical memory	4096 MB
Processor type	Intel(R) Xeon(TM) CPU
HDD 용량	46.57 GB
PC 3	
OS	Microsoft Windows XP
Physical memory	2048 MB
Processor type	Intel(R) Core(TM)2 Duo CPU E7200 @
HDD 용량	146.48 GB
PC 4	
OS	Windows 7 Home Premium
Physical memory	2046 MB
Processor type	Pentium(R) Dual-Core CPU E5700 @
HDD 용량	99.00 GB

5.2.2 성능 평가

본 프로그램은 윈도우 환경의 여러 클라이언트 환경에서〔표 19〕에서 성능을 평가하였는데 실행 후 서버에 도착한 결과를 비교하면 〔표 20〕과 같다. 수집 데이터의 환경에 따라 다르다고 할 수 있으나 결과는 상당히 만족하게 생각된다.

〔표 20〕 실행 결과

단위 : 〔시간:분〕

PC 1		PC 2	
시작시간	종료시간	시작시간	종료시간
11:22	11:25	18:27	18:33
PC 3		PC 4	
시작시간	종료시간	시작시간	종료시간
09:52	09:56	13:03	13:05

5.2.3 종합 평가

현장에서의 포렌식 관점에서 침해사고 분석에서 필요한 다양한 정보가 수집될 수 있도록 추가 사항을 구현하여 정보의 수집 범위가 확대되었다. 허건일 등이 증거수집 모듈 개선에서 제안한〔3〕 네트워크 연결 정보와 프로세스 정보의 통합, 도메인 주소 정보 수집을 추가하였으며, 백은주 등이 연구한 내용〔4,5〕을 포함하였고, 이 두 연구에 비해 클라이언트/서버 구조로 변경하여 증거 보존성을 강화하였고, MD5 해시를 적용함으로써 증거 보존의 원본성과 무결성을 유지하는 진전된 연구 결과를 도출하였다.

본 논문의 독창성은 기능평가에서 언급한 고대 디지털 포렌식연구센터에서 발간한 디지털 증거처리 가이드라인을 만족하면서 윈도우 명령어, 내부 인터널(internals)과 공개된 자동화된 패키지를 활용하여 구체적인 시스템 설계를 통한 시스템을 구현하였다는 점이다. 시스템 성능은 성능 평가에서 비교한 것처럼 다른 포렌식 수집 도구에 비해 현장의 활성 및 비활성 데이터를 매우 빠르게 수집하고 있다. 디지털 포렌식 해결 관점에서 시스템의 특징은 클라이언트는 간단한 클릭만으로 휘발성 및 비휘발성 자료수집이 진행되고

자료수집이 완료되면 자동화된 해시값을 계산하여 해시정보의 생성 및 전송을 수행하고, 서버는 이중화된 데이터를 보관한다. 따라서 본 시스템은 가독성이 있는 데이터를 수집하고 있기 때문에 포렌식 수사에 있어 침해사고 발생시 현장에 포렌식 전문가가 투입되지 않고도 활성 시스템에서 디지털 데이터의 수집을 가능하게 한다.

본 연구된 증거 수집시스템은 EnCase나 FTK (Forensic Tool Kit) 등 디스크 이미지를 생성하는 디지털 자료 취득 상용 도구를 구입하지 않는 침해사고 기관에 배포하여 초동대응 시 사고 현장에서의 디지털 증거 수집용으로 활용될 수 있도록 개발하였으며 디지털 포렌식 분석의 많은 경험을 토대로 설계하였기 때문에 수집된 데이터 분석 시 부족함이 없이 활용되고 있으며 이 도구의 장점은 다음과 같다.

① 수집된 정보는 암호화되고 이중화되어 보존되므로 증거보존의 원본성과 무결성이 유지된다.
② 사본을 가지고 디지털 포렌식 분석 도구를 이용하여 분석하기 위한 초동 대응 증거수집용으로 침해사고대응팀에서 사용하고 있다.
③ 포렌식 지식이 없는 침해사고 기업에서 디지털 증거 수집 시 사용이 가능하다.
④ 신속한 증거수집이 가능토록 구현되었다.
⑤ 증거 수집의 수집에 대한 추가 요구발생에 대해 쉽게 확장될 수 있다.

VI. 결 론

본 논문은 윈도우 시스템 환경 침해사고 식별시 디지털 포렌식 관점에서 침해사고 분석가에 의해 초동대응을 위하여, 신속하게 디지털 증거를 수집할 수 있도록 증거 수집 시스템을 설계하였으며, 설계된 사항에 따라 클라이언트/서버 형태로 구현하였다.

먼저 기존 사전 연구된 현장에서의 포렌식 프로세스 방법론을 검토하였으며, 디지털 데이터 수집도구 요구사항의 분석을 위하여 윈도우 디지털 데이터 수집 스크립트를 파악하였다.

조사된 자료를 기준으로 CFFTPM 모델을 적용하여 사용자 사용 프로파일 단계에는 홈 디렉토리, 파일 특성, 레지스트리 단계에 따라 스크립트를 작성하였고, 타임라인 단계에는 시스템 및 MAC(mtime, atime, ctime)에 대한 스크립트를 작성하였으며, 인터넷 단계에는 브라우저 부산물, 이메일, 인터넷 메신저 정보수집을 위한 스크립트를 작성하였으며, 이는 실제로 클라이언트에서 구현된다. 수집된 정보는 MD5해시 코드를 생성하여 암호화 되어 서버에 전송된다.

본 프로그램은 침해사고가 의심되거나 발생한 해당 기관에 배포하여 신속하게 디지털 증거를 수집하여 그 결과를 디지털 포렌식 분석 전문가에 의해 분석될 수 있도록 초동 단계 도움을 제공하는 데 목적이 있다. 모든 윈도우 OS에서는 사용 가능하나 최신의 64비트용에 대해서는 추가 검증이 필요하며, 향후 개선할 부분으로는 수집하고자하는 활성 및 비활성 데이터의 선택 정보에 따른 분할된 정보의 수집기능 추가와 더불어 P2P 악성코드 분석을 위한 증거 수집 모듈 추가에 대한 연구가 필요하다.

참고문헌

〔1〕 Marcus K Rogers et al, "Computer Forensic Field Triage Process Model," Conference on Digital Forensics, Security and Law, Las Vegas, Nevada, USA, pp. 27-40, April 20-21, 2006.

〔2〕 침해사고 분석 절차 안내서, 방송통신위원회・한국인터넷진흥원, 2010.1.

〔3〕 허건일, 박찬욱, 박원형, 국광호, "윈도우 기반 악성코드 증거 수집 모듈 개선에 관한 연구", 정보・보안 논문지, 제10권, 제3호, pp 61-68, 2010.9.

〔4〕 백은주, 성진원, 임경수, 이상진, "윈도우 활성 시스템상의 디지털 증거수집 도구 설계 및 구현," 정보보안・논문지, 제7권, 제2호, pp 91-100, 2007.6.

〔5〕 백은주, "윈도우 시스템에서의 활성 데이터 수집 도구 설계 및 구현," 석사학위 논문, 고려대학교, pp 8-13, 2007.12.

〔6〕 Special Agent Jesse Kornblum, "Preservation of Fragile Digital Evidence by First Responders," Air Force Office of Special Investigations, pp 1-11, Aug. 2002.

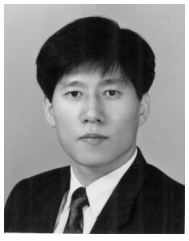
〔7〕 Chris, Kevin, "Incident Response & Computer Forensics," 2nd. ed, McGraw-Hill. pp. 114-115, July 17, 2003.

〔8〕 이석희, 김현상, 이상진, 임종인, "윈도우 시스템에서 디지털 포렌식 관점에서의 메모리 정보 수집 및 분석 방법에 대한 고찰", 정보보호학회 논문지, 16(1), pp 87-96, 2006.2.

〔9〕 송대완, "디지털 증거의 법적 증명력을 위한 디지털 포렌식에 관한연구(Windows Forensic을 중심으로)", 석사학위논문, 한남대학교, pp15-30, 2006.12.
〔10〕 신삼신, "윈도우 파일 시스템의 직접접근을 통한 초기단계 포렌식 증거수집", 석사학위논문, 전남대학교, pp 4-43, 2008.2.
〔11〕 "디지털 증거 처리 가이드라인", 고려대학교 디지털 포렌식연구센터, 2012. http://forensic.korea.ac.kr/sub_guideline/download/guideline_1.pdf

〈著者紹介〉

이 승 원 (SeungWon Lee) 종신회원
1982년 8월: 전남대학교 계산통계학과 졸업
1992년 8월: 고대학교 경영대학원 경영정보 석사
2013년 2월: 서울벤처대학원대학교 유비쿼터스시스템 박사
1982년 12월~1992년 8월 한국전력기술(주) 근무
1992년 8월~현재 한전케이디엔(주) 근무
2011년 2월~현재 지식경제사이버안전센터 사이버대응팀장
〈관심분야〉 CAD/GIS, U-City, 스마트그리드, 융합기술, 정보보호, 정보시스템감리



노 영 섭 (YoungSup Roh) 정회원
1988년 2월: 인하대학교 전자공학과(공학사)
1996년 8월: 한국과학기술원 정보및통신공학과(공학석사)
2005년 2월: 고려대학교 전기,전자,전파공학과(공학박사)
1987년 11월~1998년 2월 : LG전자 미디어통신연구소 선임연구원
1998년 3월~2001년 2월 : 청강문화산업대학교 이동통신과 교수
2001년 3월~2005년 2월 : 주식회사 싸이버뱅크 연구개발부문 상무이사
2005년 3월~2012년 8월 : 서울벤처대학원대학교 유시티.융합기술경영전공 교수
〈관심분야〉 임베디드시스템, 이동통신, IT융합기술, 정보보호

한 창 우 (HanChang Woo) 정회원
2001년 02월: 창원대학교 산업시스템공학과 졸업(공학사)
2001년 03월~현재: 한전KDN(주) 근무
2008년 07월~현재: 지식경제사이버안전센터
〈관심분야〉 정보보호, 디지털포렌식