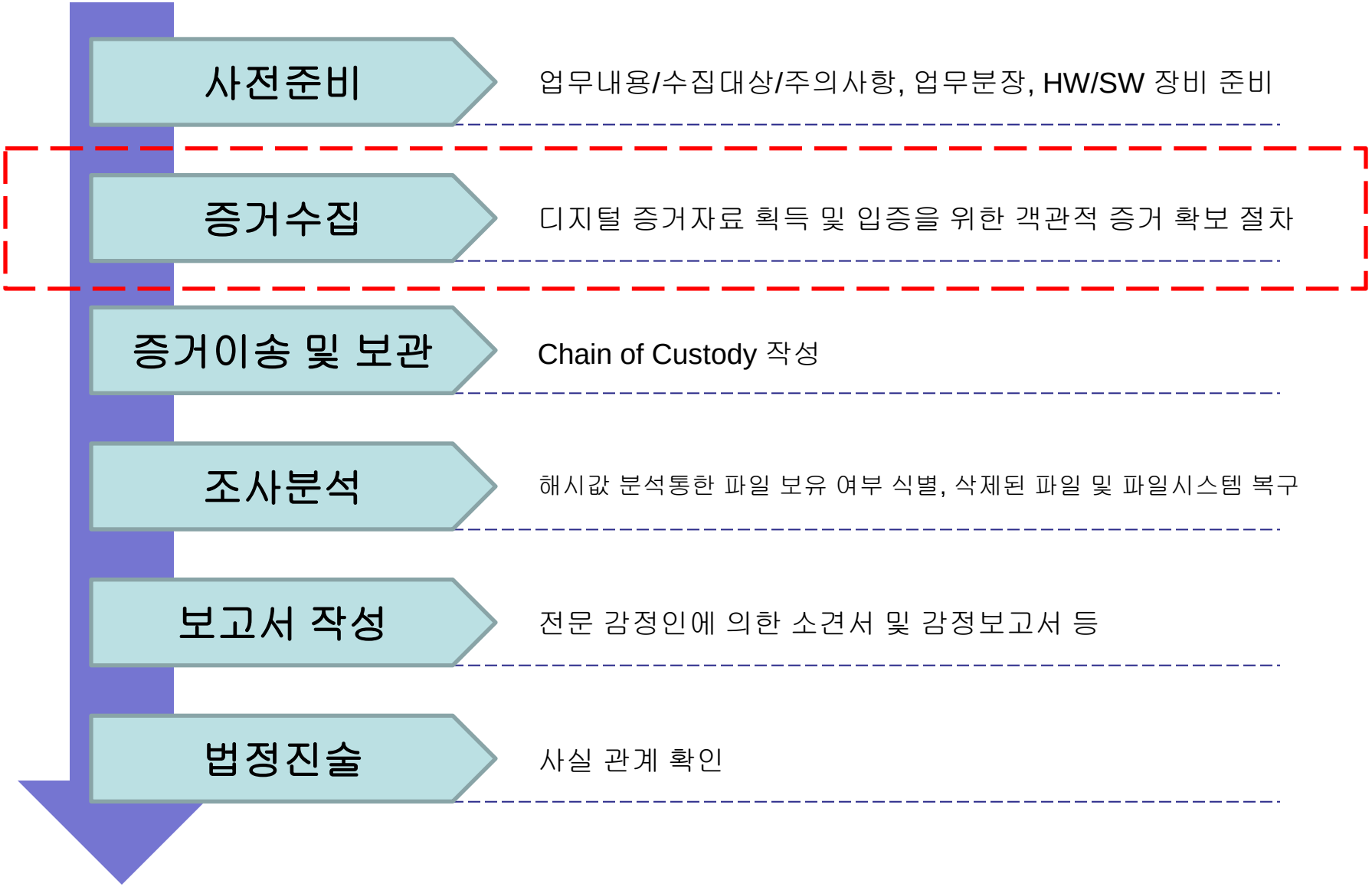
컴퓨터보안 실습

포렌식 실습(실습10)

조사 분석 – 라이브 포렌식

디지털포렌식 절차


사전준비
업무내용/수집대상/주의사항, 업무분장, HW/SW 장비 준비
증거수집
디지털 증거자료 획득 및 입증을 위한 객관적 증거 확보 절차
증거이송 및 보관
Chain of Custody 작성
조사분석
해시값 분석통한 파일 보유 여부 식별, 삭제된 파일 및 파일시스템 복구
보고서 작성
전문 감정인에 의한 소견서 및 감정보고서 등
법정진술
사실 관계 확인

라이브 포렌식 정의

[범죄 현장] [현장 보존] [현장 증거 수집(지문, 혈흔 …)]

- **실제 현장 사건 발생 시, 현장 보존 & 현장 증거 수집에 따라 사건 해결 가능성이 달라짐**

http://victorypi.com/services/computer-forensics-deleted-data-recovery/

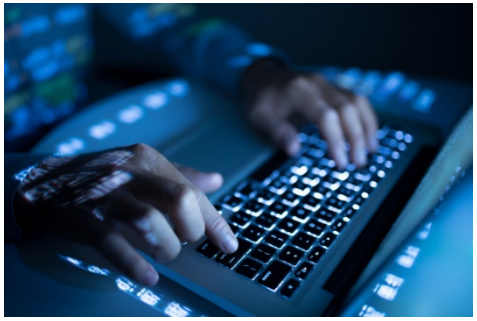
라이브 포렌식 정의

- 개인 관련 사건의 경우, USB, 노트북, 스마트 폰 등 디지털기기 현장에서 인계 또는 압수

- 증거 훼손 최소화 위해 개인용 디지털 기기의 경우 대부분 전원을 끈 상태로 수집 및 분석

↓

- 기업의 경우 침해사고의 조사를 위해 전원을 임의로 끄거나 중지시킬 수 없음



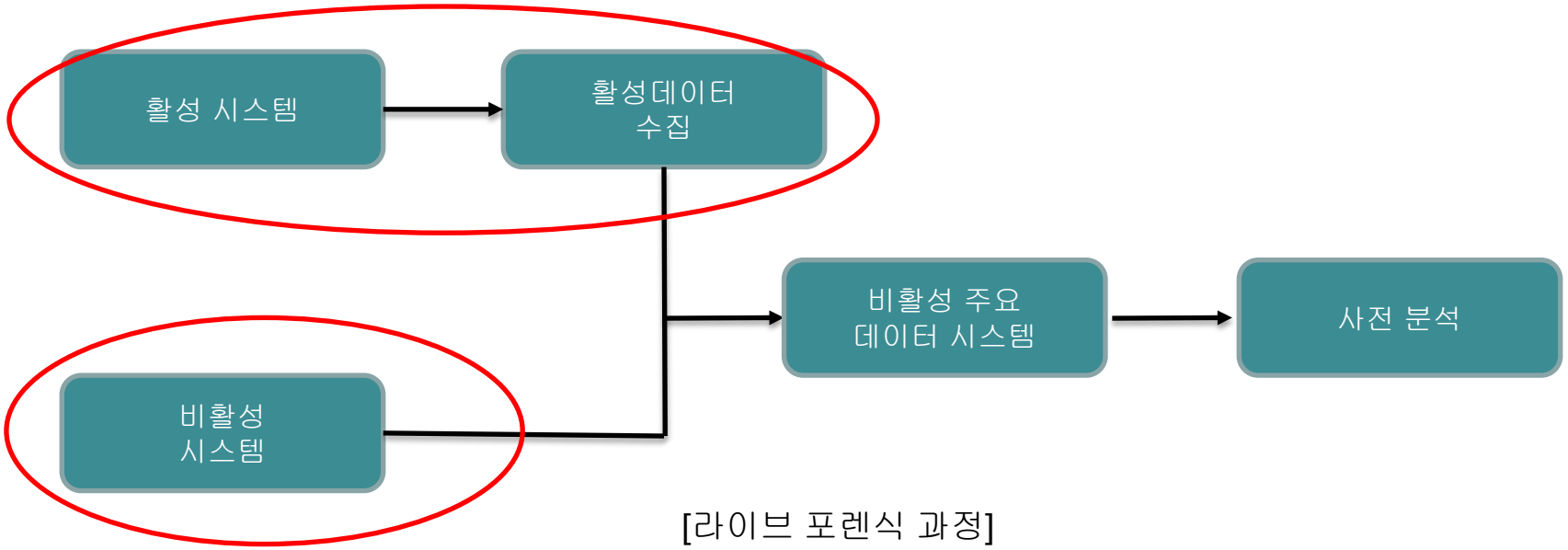
→

라이브 포렌식 진행

- 라이브 포렌식 : 컴퓨터 및 전자기기가 동작중인 상태에서 빠른 시간 안에 얻을 수 있는 자료들을 수집하고 분석하여 증거가 될 수 있는 정보를 찾아내는 기술

http://victorypi.com/services/computer-forensics-deleted-data-recovery/

라이브 포렌식 절차



[라이브 포렌식 과정]

- **활성시스템과 비활성 시스템으로 나누어 증거 수집**
- **데이터의 분석 보다는 활성 상태에서 수집 가능한 모든 데이터를 최대한 수집하는 데 초점**

활성 시스템 및 휘발성 데이터

- **활성 시스템(Live System) :** 전원에 연결되어 정상적으로 가동 중인 시스템
- **휘발성 데이터 : RAM**과 같은 휘발성 메모리에 저장되어**,** 전원이 꺼지면 사라지는 데이터

- **휘발성 데이터(활성 데이터) 종류**
  - 실행 중인 프로세스
  - 연결 중인 프로세스
  - 현재 로그인 사용자
  - 현재 시스템 리소스 상황
  - 현재 전송 중인 패킷
  - 클립보드에 저장된 데이터
  - 기타

활성 데이터 수집 고려사항

- 공개되고 검증된 **CLI (Command Line Interface)** 도구를 사용해 수집해야 함

→ 최소한의 명령어 이용으로 증거 훼손 최소화

- 단일 도구 보다는 여러 도구로 중복 수집 필요

→ 각 도구마다 시스템 정보를 불러오는 방식과 출력방식이 다르기 때문

- 모든 명령어는 독립적으로 실행되어야 함

→ 시스템이 악성코드로 감염되었을 경우 기본명령 이용 시 손상 발생 가능성, 정적으로 컴파일해간 명령어 준비

- 수집한 활성 데이터와 덤프한 물리메모리를 비교해보는 작업 필요

→ 기본 명령어로는 은닉된 프로세스 파악 불가능, 물리메모리 덤프하여 실제 교차 검증 필요

활성 데이터 수집 툴

Windows Software

There are many Windows memory acquisition tools. Most of them will not work on Windows Vista or 7, as user prog tools acquire physical memory by first installing a device driver, so administrative privileges are needed.

We have edited this list so that it only includes current tools:

Belkasoft Live RAM Caputer

This free forensic tool, unlike many others, works in kernel-mode, which allows bypassing proactive anti-debuggir reliable results compared to user-mode tools.

Designed specifically for computer forensics. Fully portable, runs off a flash drive, produces uncompressed raw bir Server. 32 and 64-bit drivers are included.

https://belkasoft.com/ram-capturer

WindowsSCOPE Cyber Forensics, available at http://www.windowsscope.com

Can capture, analyze, graph in depth physical and virtual memory codes and structures

Proprietary and standard formats (windd), snapshot repository, snapshot comparison

All Windows OSs (XP, Vista, 7, 8/8.1, 10), 32 and 64 bit supported

Available via node-locked license and cloud rental

Phantom Probe USB based fetch

CaptureGUARD PCIe card and ExpressCard for hardware-assisted DRAM acquisition

CaptureGUARD Gateway enables DRAM acquisition of locked computers

Launched in 2011

winen.exe (Guidance Software - included with Encase 6.11 and higher)

included on Helix 2.0

http://forensiczone.blogspot.com/2008/06/winenexe-ram-imaging-tool-included-in.html

Mdd (Memory DD) (ManTech)

http://sourceforge.net/projects/mdd

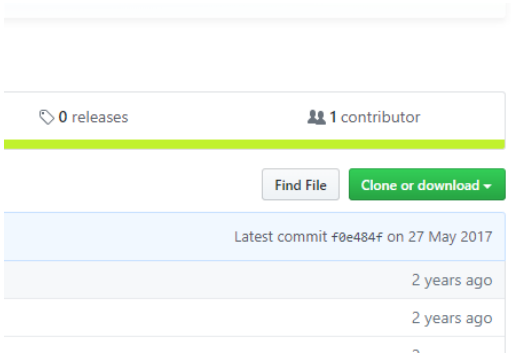
http://www.forensicswiki.org/wiki/Tools:Memory_Imaging#Windows_Software

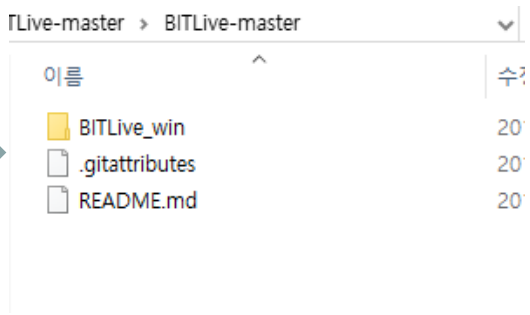
(실습) 활성 데이터 수집

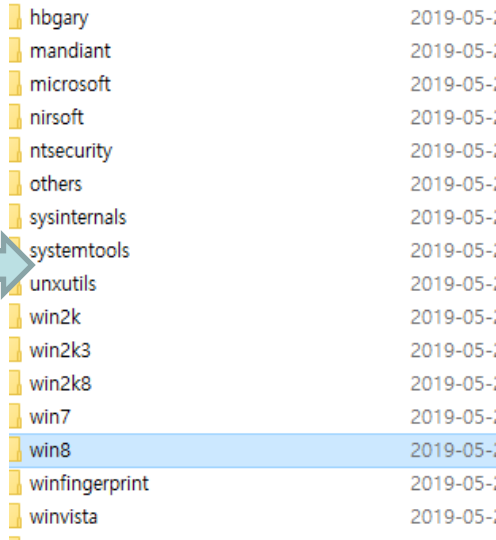
1. 실습준비

1). https://github.com/Plainbit/BITLive

→ Plainbit 사, BITLive_win 툴 다운로드



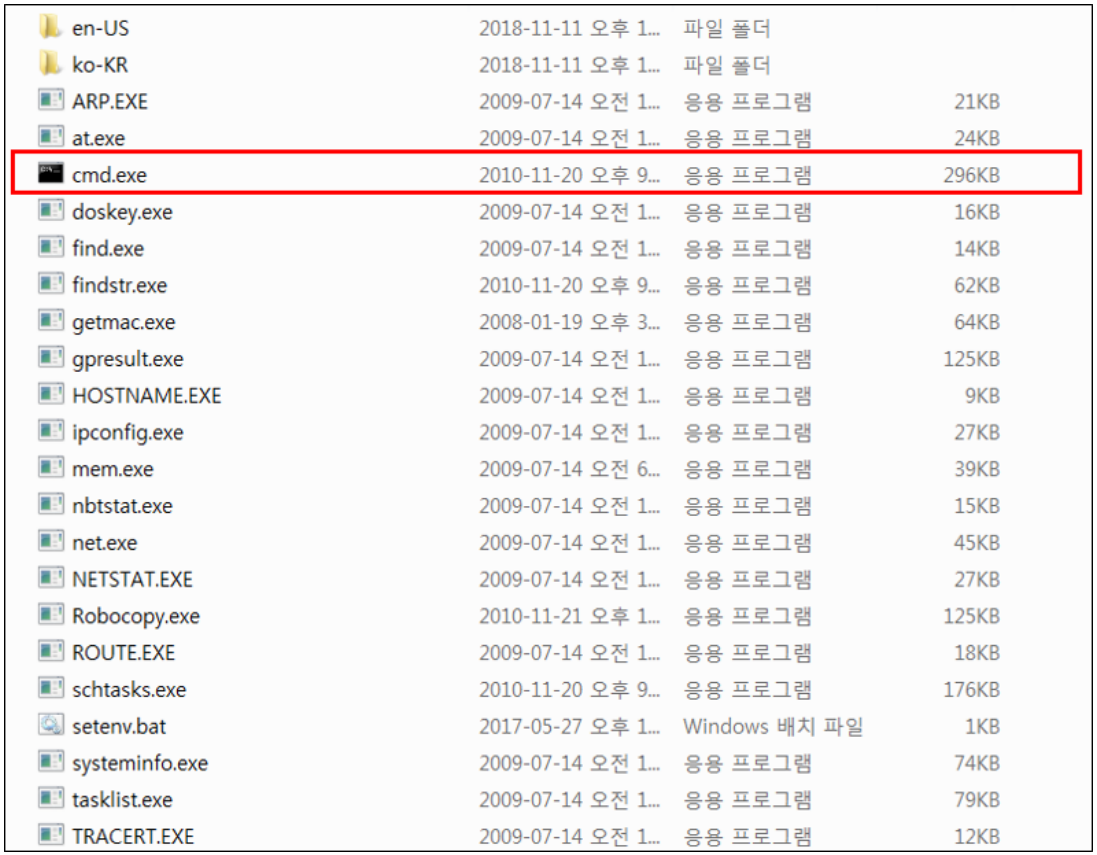




- 압축 해제 후 Win 7 폴더로 이동

(실습) 활성 데이터 수집

2. 해당 폴더에 있는 독립 cmd 실행



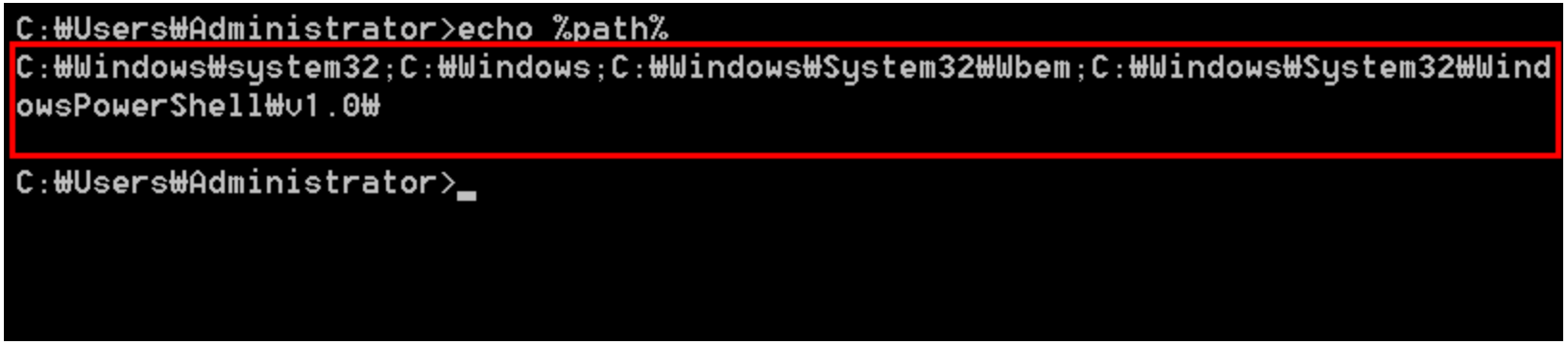
en-US	2018-11-11 오후 1...	파일 폴더	
ko-KR	2018-11-11 오후 1...	파일 폴더	
ARP.EXE	2009-07-14 오전 1...	응용 프로그램	21KB
at.exe	2009-07-14 오전 1...	응용 프로그램	24KB
cmd.exe	2010-11-20 오후 9...	응용 프로그램	296KB
doskey.exe	2009-07-14 오전 1...	응용 프로그램	16KB
find.exe	2009-07-14 오전 1...	응용 프로그램	14KB
findstr.exe	2010-11-20 오후 9...	응용 프로그램	62KB
getmac.exe	2008-01-19 오후 3...	응용 프로그램	64KB
gpresult.exe	2009-07-14 오전 1...	응용 프로그램	125KB
HOSTNAME.EXE	2009-07-14 오전 1...	응용 프로그램	9KB
ipconfig.exe	2009-07-14 오전 1...	응용 프로그램	27KB
mem.exe	2009-07-14 오전 6...	응용 프로그램	39KB
nbtstat.exe	2009-07-14 오전 1...	응용 프로그램	15KB
net.exe	2009-07-14 오전 1...	응용 프로그램	45KB
NETSTAT.EXE	2009-07-14 오전 1...	응용 프로그램	27KB
Robocopy.exe	2010-11-21 오후 1...	응용 프로그램	125KB
ROUTE.EXE	2009-07-14 오전 1...	응용 프로그램	18KB
schtasks.exe	2010-11-20 오후 9...	응용 프로그램	176KB
setenv.bat	2017-05-27 오후 1...	Windows 배치 파일	1KB
systeminfo.exe	2009-07-14 오전 1...	응용 프로그램	74KB
tasklist.exe	2009-07-14 오전 1...	응용 프로그램	79KB
TRACERT.EXE	2009-07-14 오전 1...	응용 프로그램	12KB

- cmd 와 커맨드 명령 파일들이 "win7" 디렉토리에 있는 것을 알 수 있음
- 이유는 증거 수집시 수집 대상 pc의 cmd가 악성인지 아닌지 판단할 수 없기 때문

(실습) 활성 데이터 수집

3. cmd 환경변수 설정

HEX	80
DEC	128



- 명령어 입력시 cmd 환경변수 그대로 적용되므로 변경 필요
- 현재 환경변수 확인 --> echo % path%

(실습) 활성 데이터 수집

3. cmd 환경변수 설정

```
Live-master₩BITLive_win> setenv.bat
```

```
================================================================
1. You have to go to the parent folder.
2. Run BITLive_win.bat.

22:50:14.01 C:₩Users₩Administrator₩Desktop₩tool₩tool₩BITLive_win₩win7> echo %pat
h%
win7₩;hbgary₩;mandiant₩;microsoft₩;moonsols₩;nirsoft₩;ntsecurity₩;sysinternals₩;
systemtools₩;unxutils₩;winfingerprint₩;wireshark₩;others₩;

22:50:54.35 C:₩Users₩Administrator₩Desktop₩tool₩tool₩BITLive_win₩win7>
```

- 환경변수 설정 위해 'setenv.bat' 실행 → setenv.bat
- 정상적으로 변경되었는지 확인 → echo %path%

(실습) 활성 데이터 수집

4. 활성 데이터 수집

```
 3:44:29.27 C:₩Users₩PC_H₩Downloads₩BITLive-master₩BI
Please enter the case name : movestok06
Please enter the examiner's name : YH
Do you want to acquire physical memory? (y or n) y
Do you want to acquire Non-volatile data? (y or n) y
```

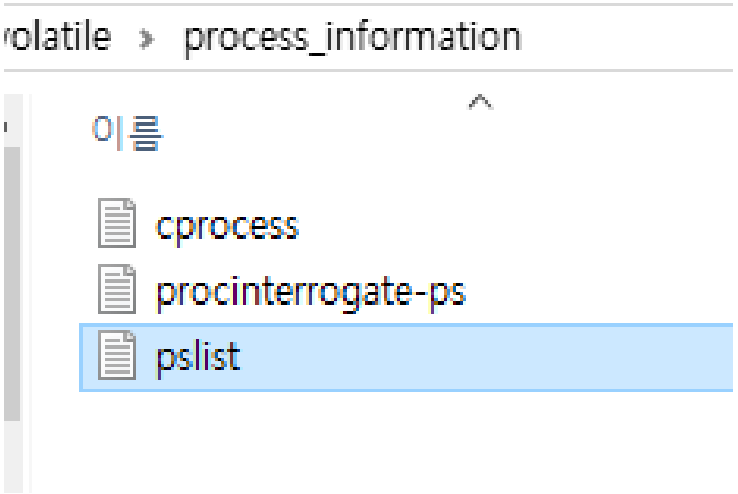
```
Do you want to acquire Non-volatile data? (y or n) y

************************************************
*         PLAINBIT Incident Response Kit       *
************************************************
### FIRST OF ALL, START ACQUIRING PREFETCH AND RECENTFILECACHE
Created "non_volatile" directory in C:₩movestok06₩DESKTOP-AKBSE4G₩
2019-05-27  3:52:47.62 - Acquiring Prefetch files ...
2019-05-27  3:53:27.39 - Acquiring RecentFileCache.bcf, Amcache.hve ...
### START ACQUIRING VOLATILE
Created "volatile" directory in C:₩movestok06₩DESKTOP-AKBSE4G₩
# START ACQUIRING NETWORK INFORMATION
Created "network_information" directory in C:₩movestok06₩DESKTOP-AKBSE4G₩vol
2019-05-27  3:53:42.89 - Acquiring arp cache table ...
2019-05-27  3:53:43.77 - Acquiring network Status ...
2019-05-27  3:53:44.45 - Acquiring routing Table ...
```

- 증거 정보는 C:\에 Case명으로 저장됨
- 휘발성 정보는 volatile에서 확인 가능

(실습) 활성 데이터 수집

5. 활성 데이터 확인



- 해당 case 폴더에서 활성화 정보 확인
- ~~ volatile\process_information 에서 tlist-s를 캡처하여 bgwon214@gmail.com로 제출

참고문헌

- 정보 보안 개론[개정3판], 양대일 저, 한빛미디어, 2018, 1.
- 디지털 포렌식 개론(2판), 이상진 저, 이룬 출판사, 2015. 5.
- 컴퓨터보안, William Stalling 저, 한티미디어, 2016. 8
- 정보보안과 사이버 해킹의 기초, 김경신 저, 2016. 8
- RFC 3227, Guidelines for Evidence Collection and Archiving
- NIST Special Publication 800-86, Guide to Integrating Forensic Techniques into Incident Response
- http://www.forensicswiki.org/wiki/Tools:Memory_Imaging#Windows_Software

Q & A