

# 사고(실시간) 대응



*JK Kim*

*@pr0neer*

*forensic-proof.com*

*proneer@gmail.com*

1. 실시간 대응 (Live Response)
2. 사전 준비 (Advance Preparation)
3. 휘발성 데이터 수집 방안 (A Method of acquiring Volatile Data)
4. 휘발성 데이터 수집 절차 (A Process of acquiring Volatile Data)
5. 휘발성 데이터 (Various Volatile Data)
6. 비휘발성 데이터 (Various Non-volatile Data)
7. 윈도우 배치 스크립트 (Windows Batch Script)

# 실시간 대응

*Security is a people problem...*

## 실시간 대응이란?

- **실시간 대응 (Live Response)**
  - 현장에서 조사 대상 시스템을 접했을 경우 취해야 하는 대응 방법
  - 시스템의 규모, 종류, 상태에 따라 적절한 대응 방안이 필요함
  - 시스템에 따른 현장에서의 외부 대응은 문서화 가능
  - But, 시스템 내부의 휘발성 정보를 수집하는 것은 시스템의 상태에 따라 매우 다름
  - 같은 부류의 운영체제이더라도 버전, 배포판, 서비스팩, 패치에 따라 수집하는 방법이 다름
  - 따라서,
    - 적절한 대응을 위해서는 세부적인 시스템 별 대응 방안에 대한 문서화 필요
    - 다양한 환경에 대한 경험을 통한 노하우 습득 및 전수
    - 자신만의 판단이 아닌 2명 이상의 전문가에 의한 통합적인 판단이 요구됨

## 실시간 대응시 시스템 종료 방법

- **전통적인 디지털 포렌식 방법론**
  - 서버용 시스템일 경우, 시스템에서 지원하는 안전한 종료 방식 사용 (Windows NT/2003/2008, HP-UX 등)
  - 개인용 시스템일 경우, 시스템 본체 뒤에서 전원 코드 바로 분리
- **최근 디지털 포렌식 방법론**
  - 현장 시스템이 활성 상태일 경우, 획득할 수 있는 최대한의 휘발성 데이터 수집 후 시스템 종료
  - 휘발성 데이터 수집 시 시스템 무결성에 대한 고려 필요

## 실시간 대응 필요성

- 시스템의 휘발성 데이터를 통해서만 얻을 수 있는 정보가 존재
- 사고 후 계속 활성 상태가 유지된 시스템이라면, 휘발성 데이터는 사건 상황을 가장 잘 표현해 줄 수 있는 정보
- 대규모의 서버와 같이 시스템을 강제 종료할 수 없는 환경이 존재

## 실시간 대응시 고려사항

- “원본에 대한 영향을 최소화”
  - 실시간 대응에 사용하는 도구나 저장매체는 원본에 최소한의 영향을 미쳐야 함
- 로카르드 교환 법칙 (Locard's Exchange Principle)
  - “접촉한 두 물체 간에는 반드시 교환이 일어난다”
  - [http://en.wikipedia.org/wiki/Locard's\\_exchange\\_principle](http://en.wikipedia.org/wiki/Locard's_exchange_principle)

## 실시간 대응시 고려사항 – 시스템 구성 요소

- **메모리**
  - 실시간 대응 도구를 사용할 경우 원본 시스템 메모리에 영향
- **네트워크**
  - 네트워크를 통한 수집 시 네트워크 정보와 관련된 데이터에 영향
- **프리패치/슈퍼패치**
  - 프로그램 실행시 프리패치/슈퍼패치 파일의 생성 및 수정이 발생
- **레지스트리**
  - 도구의 실행, 외부 저장매체 연결 등의 시스템 행위로 인해 레지스트리 변경
- **DLL**
  - 정적 라이브러리나 자체 DLL을 사용하지 않을 경우 원본 시스템의 DLL 영향
- **로그 정보**
  - 시스템의 로그 기록 수준에 따라 실시간 대응시 로그 정보에 영향



# 사전 준비

*Security is a people problem...*

## 사전 준비 고려사항

- **도구 및 장비의 선택**

- 다양한 시스템 환경에 대응이 가능하도록 각 시스템에 맞는 도구 및 장비 보유
- 실시간 대응에 사용하는 도구는 적법절차를 통해 획득 및 사용이 이루어져야 함
- 시스템에 영향을 최소한으로 미치는 도구가 적합
- 불법소프트웨어나 악성코드에 감염되지 않아야 함

- **도구 및 장비의 테스트**

- 선택한 도구 및 장비가 실제 대상 시스템에서 잘 동작하는지 사전에 테스트
- 환경에 따라 도구 및 장비의 사용이 달라져야 하므로 정확한 사용 방법 숙지
- 도구 및 장비에서 지원하는 다양한 옵션 사용, 매뉴얼 숙지
- 예) `\\W.\\PhysicalDrive0`, `\\Device\\PhysicalMemory`

## 사전 준비 고려사항

- 문서화

- 선택한 도구 및 장비의 철저한 기록 (도구 해쉬값 및 장비 상태 등)
- 시스템 환경에 따른 도구 및 장비 테스트 후 해당 결과 기록
- 시스템에 어떤 영향을 미치는가?
- 시스템에 영향을 아예 없앨 수 있는가? 그렇지 않다면 정확한 문서화가 필요

- 실시간 대응 인원

- 도구 및 장비도 이미 검증이 된 (예, CFTT) 것을 사용해야 하지만 대응 인원의 경우에도 자격 검증
- 보통 인원에 대한 자격 검증은 경력이나 자격증으로 이루어짐

# 휘발성 데이터 수집 방안

*Security is a people problem...*

## 휘발성 데이터 수집 방안

- **시스템 스크립트 사용**
  - 시스템 스크립트는 시스템 셸에서 지원하는 기본 기능이므로 시스템에 최소한의 영향
  - 윈도우 셸 스크립트, 리눅스 셸 스크립트
  - 셸 환경도 시스템에서 지원하는 셸이 아닌 별도로 구성할 필요 (예; cmd.exe, bash 등)
- **정적라이브러리를 사용하는 수집 도구**
  - 스크립트가 아닌 별도의 실행 파일을 사용할 경우, 정적 컴파일 필요
- **시스템 유틸리티 및 미리 검증된 유틸리티를 스크립트를 사용해 동작 시킨 후 데이터 수집**

## 휘발성 데이터 전송 방안

- **네트워크를 통한 전송**
  - Netcat/Crycat과 같은 도구를 이용하여 수집된 데이터를 외부로 전송
  - 해당 도구가 시스템에 미치는 영향은 사전에 문서화
- **외부 저장매체를 통한 전송**
  - USB, CD 등을 통해 수집한 휘발성 데이터 저장
  - 자신이 만든 스크립트를 이용하거나 별도의 상용 도구 사용
  - 상용 도구
    - Guidance's EnCase Portable
    - AccessData's Live Response®
    - Microsoft's COFEE (Computer Online Forensic Evidence Extractor)

# 휘발성 데이터 수집 방안

## 실습 #1 – Netcat/Crycat 이용 포렌식 데이터 전송

- 서버 컴퓨터 설정

```
nc -v -l -p "port" > "filename"  
ex) C:\> nc -v -l -p 9999 > evidence.txt
```

- 클라이언트 설정

```
nc "server IP" "server port"  
ex) C:> acquire.bat | nc 192.168.0.1 9999
```

- 클라이언트 이미징 데이터 전송

```
C:\> dd if=\\.\PhysicalMemory | nc 192.168.0.1 9999
```

- Ref. [http://computer-forensics.sans.org/community/papers/forensic-validity-netcat\\_124](http://computer-forensics.sans.org/community/papers/forensic-validity-netcat_124)

# 위발성 데이터 수집 절차

*Security is a people problem...*



## 휘발성 데이터 수집 절차

- 휘발성 순서에 관한 참고 문서
  - RFC 3227, Guidelines for Evidence Collection and Archiving
    - <http://tools.ietf.org/html/rfc3227>
  - NIST Special Publication 800-86, Guide to Integrating Forensic Techniques into Incident Response
    - <http://csrc.nist.gov/publications/PubsSPs.html>
- 휘발성(활성) 데이터는 시스템의 메모리로부터 수집할 수 있는 정보
- 휘발성 데이터의 종류에 따라 휘발성은 다름

# 휘발성 데이터 수집 절차

## 휘발성 데이터 수집 절차

- 휘발성 데이터의 수집 순서

실전 윈도우 포렌식	RFC 3227	NIST SP 800-86
물리적 메모리	레지스터, 캐시	네트워크 연결 정보
네트워크 연결 정보	라우팅 테이블, ARP 캐시	로그온 세션
프로세스 정보	프로세스 정보	물리적 메모리
열린 파일 목록	물리적 메모리	프로세스 정보
로그온 사용자(세션)	임시 파일 시스템	열린 파일
열린 TCP/UDP 포트 정보	디스크	네트워크 설정 경보
프로세스와 포트 맵핑	원격 로그인과 모니터링 데이터	시스템 시간
라우팅 테이블	물리적 설정, 네트워크 토폴로지	N/A
네트워크 인터페이스	기타 저장장치	N/A

# 휘발성 데이터

*Security is a people problem...*

## 휘발성 데이터 수집시 고려사항

- OS 권한 상승
  - 디지털 포렌식 도구들은 대부분 관리자 권한이 필요
  - 일반 사용자 권한의 환경이라면 관리자 권한으로 실행
    - Runas /user:<관리자 계정> "실행 프로그램"
    - Ex) Runas /user:administrator "f:\Live Response\trust\_cmd.exe"
    - 관리자 아이디/비번이 필요

## 휘발성 데이터 목록

- 시스템 시간
- 네트워크 연결 정보
- 프로세스 목록
- 로그인 사용자
- DLL 목록
- 핸들
- 열린 파일
- 열린 포트와 프로세스 매핑
- 명령 히스토리
- 서비스 목록
- 네트워크 인터페이스 정보
- 내부 라우팅 테이블
- 예약된 작업
- 클립보드 내용
- 네트워크 드라이브와 공유 폴더
- 넷바이오스 정보
- 프로세스 덤프
- 물리메모리 덤프

## 휘발성 데이터 목록

- 시스템 시간 (1)
  - 사고 조사시 수집해야 하는 가장 중요한 정보 중 하나
  - 수집에 소요된 시간 기록
  - 기본적인 시간 외 조사 시스템의 설정 시간대 (UTC) 수집
  - 명령 프롬프트를 이용한 수집일 경우 date, time 명령 사용



```
C:\Windows\system32\CMD.exe
C:\Users\wpr0neer>date /t & time /t
01/14/2011 Fri
05:01 PM
```

- 별도의 프로그램을 사용할 경우 시스템 시간을 얻을 수 있는 라이브러리 사용
  - localtime()
  - gmtime()
  - WMI → Win32\_OperatingSystem → Localdatetime

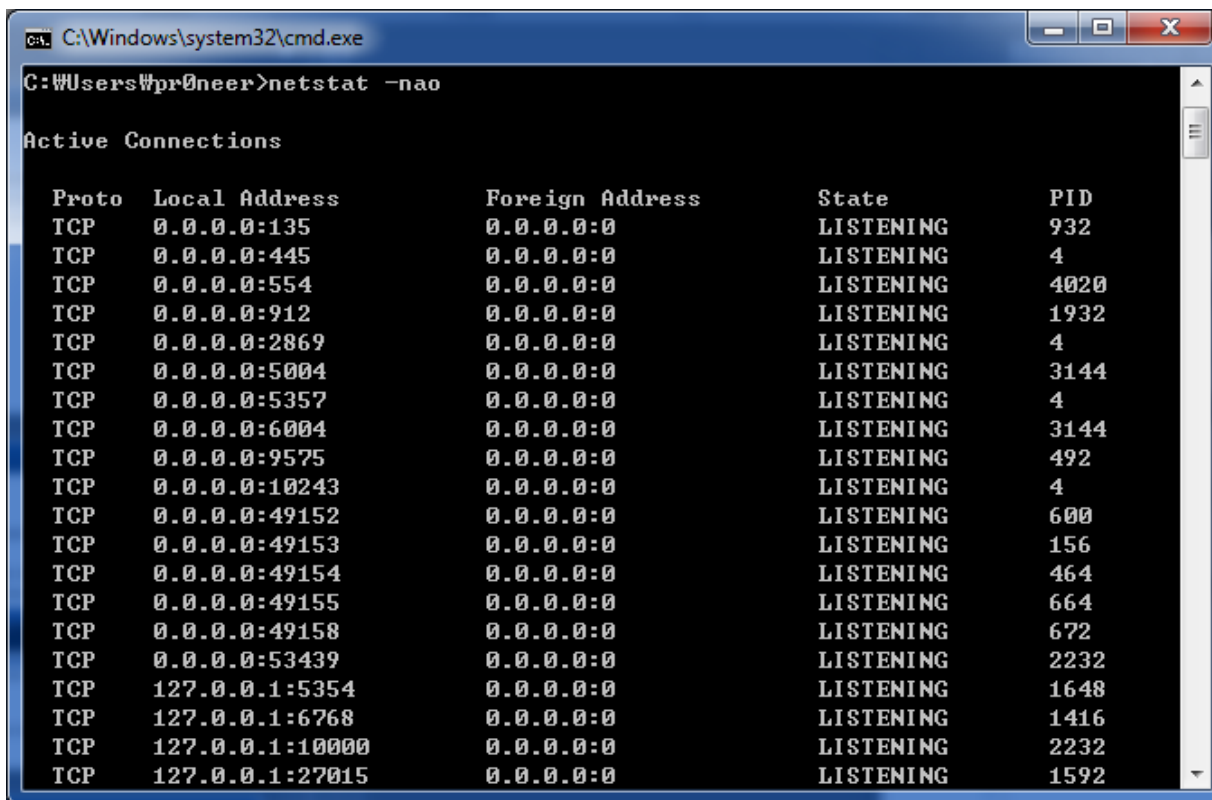
## 휘발성 데이터 목록

- **WMIC**
  - Windows Management Instrumentation Command-line
  - WMI 정보를 확인할 수 있는 명령 인터페이스
  - wmic.exe를 이용해 다양한 WMI Class 정보 획득 가능
  - Ex)
    - wmic:root\Wmi> **os get installdate**
    - wmic:root\Wmi> **os get currenttimezone**
    - wmic:root\Wmi> **os get localdatetime**
    - wmic:root\Wmi> **os get serialnumber**

# 휘발성 데이터

## 휘발성 데이터 목록

- 네트워크 연결 정보 (2)
  - 현재 시스템과 연결된 네트워크 정보 수집
  - Ex) netstat -nao



```
C:\Windows\system32\cmd.exe
C:\Users\Wpr0neer>netstat -nao

Active Connections

Proto Local Address          Foreign Address         State       PID
TCP   0.0.0.0:135             0.0.0.0:0               LISTENING   932
TCP   0.0.0.0:445             0.0.0.0:0               LISTENING   4
TCP   0.0.0.0:554             0.0.0.0:0               LISTENING   4020
TCP   0.0.0.0:912             0.0.0.0:0               LISTENING   1932
TCP   0.0.0.0:2869            0.0.0.0:0               LISTENING   4
TCP   0.0.0.0:5004            0.0.0.0:0               LISTENING   3144
TCP   0.0.0.0:5357            0.0.0.0:0               LISTENING   4
TCP   0.0.0.0:6004            0.0.0.0:0               LISTENING   3144
TCP   0.0.0.0:9575            0.0.0.0:0               LISTENING   492
TCP   0.0.0.0:10243           0.0.0.0:0               LISTENING   4
TCP   0.0.0.0:49152           0.0.0.0:0               LISTENING   600
TCP   0.0.0.0:49153           0.0.0.0:0               LISTENING   156
TCP   0.0.0.0:49154           0.0.0.0:0               LISTENING   464
TCP   0.0.0.0:49155           0.0.0.0:0               LISTENING   664
TCP   0.0.0.0:49158           0.0.0.0:0               LISTENING   672
TCP   0.0.0.0:53439           0.0.0.0:0               LISTENING   2232
TCP   127.0.0.1:5354          0.0.0.0:0               LISTENING   1648
TCP   127.0.0.1:6768          0.0.0.0:0               LISTENING   1416
TCP   127.0.0.1:10000         0.0.0.0:0               LISTENING   2232
TCP   127.0.0.1:27015        0.0.0.0:0               LISTENING   1592
```



## 휘발성 데이터 목록

- 프로세스 목록 (3)
  - 악의적인 프로세스나 현재 실행되고 있는 프로그램 파악
  - **Tlist**
    - Microsoft Debugging Tools에 포함된 도구
    - Ex) tlist -v, tlist -c, tlist -s, tlist -t, tlist -m
  - **Tasklist**
    - 윈도우 기본 명령
    - Ex) tasklist -v
  - **Pstlist**
    - <http://technet.microsoft.com/en-us/sysinternals/bb896682>
    - Ex) pstlist

## 휘발성 데이터 목록

- **로그온 사용자 (4)**
  - 시스템에 연결된 로컬 및 원격 사용자 목록
  - **Net Sessions**
    - 윈도우 내장 명령
    - Ex) net sessions
  - **PsWithLoggedOn**
    - <http://technet.microsoft.com/en-us/sysinternals/bb897545>
    - Ex) psloggedon
  - **LogonSessions**
    - <http://technet.microsoft.com/en-us/sysinternals/bb896769>
    - Ex) logonsessions

## 휘발성 데이터 목록

- **DLL 목록 (5)**
  - 프로세스가 사용하는 DLL 목록
  - **ListDLLs**
    - <http://technet.microsoft.com/en-us/sysinternals/bb896656>
    - Ex) listdlls "processname or PID"

## 휘발성 데이터 목록

- **핸들(Handle) (6)**
  - 프로세스가 시스템에서 열고 있는 다양한 핸들 확인
  - 파일, 포트, 레지스트 키, 쓰레드 핸들
  - **Handle**
    - 윈도우 기본 명령
    - Ex) handle [-a] [-p <process>:<pid>]

## 휘발성 데이터 목록

- **열린 파일 (7) cont'd**
  - 프로세스가 열고 있는 파일 확인
  - 해당 프로세스에 의해 생성, 수정, 삭제가 가능
  - 파일, 포트, 레지스트 키, 쓰레드 핸들
  - **Net file**
    - 윈도우 기본 명령
    - 외부 사용자가 열고 있는 파일 목록
    - Ex) net file
  - **Openfiles**
    - 윈도우 기본 명령 (XP pro 이상)

## 휘발성 데이터 목록

- 열린 파일 (7)
  - Psfile
    - <http://technet.microsoft.com/en-us/sysinternals/bb897552>
    - 원격에서 열린 파일 목록
    - Ex) psfile

## 취발성 데이터 목록

- **열린 포트와 프로세스 매핑 (8)**
  - 프로세스가 열고 있는 포트 확인
  - 해당 프로세스에 의해 생성, 수정, 삭제가 가능
  - **Netstat**
    - 윈도우 기본 명령
    - Ex) netstat -anob
  - **Fport**
    - <http://www.mcafee.com/us/downloads/free-tools/fport.aspx>
    - 윈도우 NT4, 2000, XP 에서만 동작
    - Ex) fport

## 휘발성 데이터 목록

- 명령 히스토리 (9)
  - 사용자가 셸을 통해 실행한 명령
  - **Doskey**
    - 윈도우 기본 명령
    - Ex) doskey -history



## 휘발성 데이터 목록

- 서비스 목록 (10)
  - 시스템에 등록된 모든 서비스 목록과 세부 정보
  - **PsService**
    - <http://technet.microsoft.com/en-us/sysinternals/bb897542>
    - Ex) psservice

## 휘발성 데이터 목록

- **네트워크 인터페이스 정보 (11)**
  - 시스템의 네트워크 인터페이스 정보 (IP, MAC, Gateway, DNS 등)
  - **Ipconfig**
    - 윈도우 기본 명령
    - Ex) ipconfig /all
  - **PromiscDetect**
    - <http://ntsecurity.nu/toolbox/promiscdetect/>
    - Ex) promiscdetect

## 휘발성 데이터 목록

- 내부 라우팅 테이블 (12)
  - 시스템 라우팅 테이블 목록
  - **Netstat**
    - 윈도우 기본 명령
    - Ex) netstat -r

## 휘발성 데이터 목록

- 예약된 작업 (13)
  - 시스템에 자동으로 예약된 작업으로 일부 악성코드들에 의해 악용
  - **At**
    - 윈도우 기본 명령
    - Ex) at

## 휘발성 데이터 목록

- **클립보드 내용 (14)**
  - 클립보드 내용은 메모리에만 존재
  - 조사 현장에 신속 대응했을 경우 용의자의 마지막 행위를 파악하는데 도움
  - **Clipboard Viewer**
    - 윈도우 기본 명령 (XP 이하 버전)
    - Ex) clipbrd
  - **Pclip**
    - <http://unxutils.sourceforge.net/>
    - Ex) pclip

## 휘발성 데이터 목록

- **네트워크 드라이브와 공유 폴더 (15)**
  - 공유된 네트워크(다른 사용자)의 폴더나 드라이브 확인
  - 조사 현장에 신속 대응했을 경우 용의자의 마지막 행위를 파악하는데 도움
  - **Net**
    - 윈도우 기본 명령
    - Ex) net use

## 휘발성 데이터 목록

- **넷바이오스 이름 (16)**
  - 공유된 네트워크(다른 사용자)의 폴더나 드라이브 확인
  - **Nbtstat**
    - 윈도우 기본 명령
    - Ex) nbtstat [-c] [-a ip\_address]

## 휘발성 데이터 목록

- 프로세스 덤프 (17)

- 특정 프로세스의 메모리 영역은 해당 프로세스의 프로그램 코드, 변수, DLL 목록 등의 다양한 부가 정보 포함
- Userdump
  - <http://www.microsoft.com/downloads/en/details.aspx?FamilyID=E089CA41-6A87-40C8-BF69-28AC08570B7E&displaylang=en>
  - Ex) userdump PID "dump\_file\_name"



## 휘발성 데이터 목록

- 물리메모리 덤프 (18)

- 휘발성 데이터는 모두 물리메모리 데이터를 기반으로 표현되는 정보
- 이론적으로 물리메모리만으로 모든 휘발성 데이터를 표현할 수 있다면 이상적
- ➔ 활성 시스템에서 물리메모리만 수집하면 되므로 무결성 훼손 최소화
- 현재 이 부분에 대한 지속적인 연구가 진행
- But, 운영체제 버전, 서비스팩, 패치에 따라 물리메모리 구조가 변경되기 때문에 변화에 맞춰 연구가 지속되기 어려움
- 자세한 물리메모리 덤프 방안은 이후 “메모리 포렌식” 부분에서 살펴봄

# 비휘발성 데이터

*Security is a people problem...*

## 비휘발성 데이터 수집이 필요한 이유

- 최근 디지털 포렌식 환경에서는 실시간 대응에서 비휘발성 데이터도 수집 필요
- 비휘발성 데이터는 저장매체 이미징 후에 분석하는 것이 원칙
- 하지만, 최근 저장매체의 대용량화로 저장매체 이미징 시간이 매우 오래걸림
- 따라서, 이미징 전에 우선 분석이 필요한 비휘발성 데이터 수집 필요
- 우선 분석 결과를 기반으로 이미징된 저장매체의 분석 방향 설정

## 실시간 대응이 필요한 비휘발성 데이터 목록

- **파일시스템 메타데이터**
  - NTFS MFT, FAT Directory Entry 등
- **레지스트리 하이브**
  - %WINDIR%\system32\config\System
  - %WINDIR%\system32\config\Sam
  - %WINDIR%\system32\config\Security
  - %WINDIR%\system32\config\Software
  - %WINDIR%\system32\config\Default
  - %USER PROFILE%\NTUSER.DAT

## 실시간 대응이 필요한 비휘발성 데이터 목록

- 프리패치/슈퍼패치
  - %WINDIR%\Prefetch
- 이벤트 로그
  - 레지스트리 : HKEY\_LOCAL\_MACHINE\SYSTEM\services\eventlog\ 하위 키값 확인
- 웹 브라우저 사용 흔적
  - Internet Explorer, FireFox, Safari 등
  - 쿠키, 히스토리 등의 정보
- 그밖에 로그
  - IIS 로그, Setuplog.txt, Setupact.log, Setupapi.log, Netsetup.log, 작업 스케줄러 로그, 방화벽 로그 등

# 윈도우 배치 스크립트

*Security is a people problem...*

## 배치 스크립트

```
Echo off
REM This is a sample to acquire volatile data.
REM Usage : Windows_LiveResponse.bat "investigator" "file"

echo.
echo ***** Start Live Response *****
echo Investigator : %1

echo ### Live Response by %1 > %2
echo. >> %2
echo ----- Start Date/Time ----- >> %2
date /t >> %2
time /t >> %2
echo. >> %2
echo ----- Step 1 - Network Connection Info ----- >> %2
netstat -nao >> %2
echo ----- Step 1 - End ----- >> %2
echo. >> %2
echo ----- Step 2 - Network Connection Info ----- >> %2
pslist /accepteula >> %2
echo ----- Step 2 - End ----- >> %2
echo.
echo ----- The End ----- >> %2

... ..
```

## 실습 #2 – 윈도우 휘발성 데이터 수집 배치 스크립트 작성

- 앞서 살펴본 18가지 휘발성 데이터 중 "1~16"번 데이터를 수집하는 배치 스크립트 작성
- 스크립트는 2개의 인자를 가짐
  - 첫 번째 인자 : 조사관 이름
  - 두 번째 인자 : 수집한 데이터를 저장할 파일
- 수집 시작과 끝에 시간 정보 기록



