# SQL Server Forensics

***dorumugs***

***dorumugs@gmail.com***

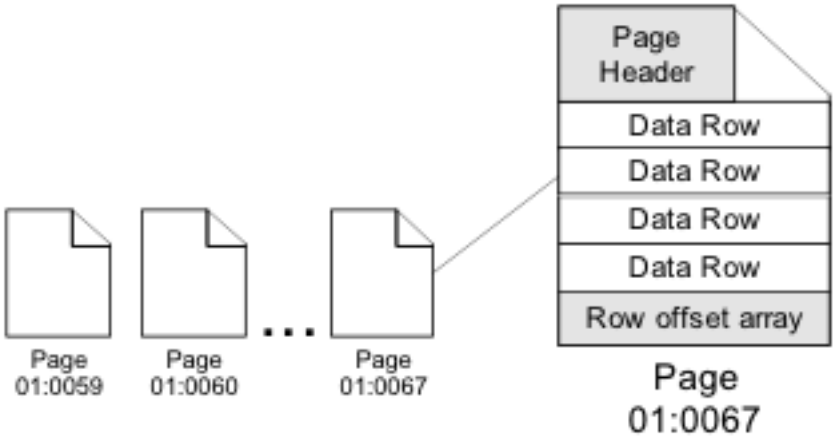
***Reference :*** *Forensic Analysis of a SQL Server 2005 Database Server, SANS*

# SQL Server Forensics

- ***Databases Files***
- Database Configurations
- Data Acquisition
- Database Analyze
- Deleted Row
- WFTSQL

## Databases Files

- 데이터 파일들은 실제 데이터를 담고 있다.
- 데이터 파일은 확장자 mdf 파일을 말한다.
- 기본적으로 아래와 같은 경로에 존재한다.
  - C:₩Program Files₩Microsoft SQL Server₩MSSQL.1₩MSSQL₩Data₩
- 파일명은 "<database>.mdf" 와 같다.
- 여러 데이터 페이지로 구성되어 있다.



## Databases Files

- Data Rows는 다양한 크기를 가지고 있다.
- Log files은 Transactions에 사용되는 데이터를 담고 있으며, Database를 복구하는데 사용한다.
- 물리적으로 존재하는 Log files은 여러 Virtual Log Files(VLF)로 구성 되어 있다.


- 물리적 Log Files은 확장자 ldf를 사용하며, 기본 경로는 아래와 같다.
  - C:₩Program Files₩Microsoft SQL Server₩MSSQL.1₩MSSQL₩Data₩
- 하나의 VLF는 Transaction log Unit과 같다.

## Databases Files

- **Important Transaction Log Columns**
  - Operation - 수행된 작업
  - Transaction ID - Transaction 구분자
  - Page ID - Transaction에 의해 영향받은 Data Page
  - Slot ID - Transaction에 의해 영향받은 Data Page의 Row
  - Offset in Row - Transaction에 의해 영향받은 Data Page의 첫번째 위치
  - SPID - Server Process 구분자
  - Begin Time - Transaction이 시작된 시간
  - Transaction Name -Active transaction의 유형
  - End Time - Transaction이 끝난 시간
  - RowLog Contents 0 - Transaction에 의해 업데이트된 값
  - RowLog Contents 1 - Disk에 씌여진 값

# SQL Server Forensics

- Databases Files
- ***Database Configurations***
- Data Acquisition
- Database Analyze
- Deleted Row
- WFTSQL

## Database Configurations

- **Logging Configuration**
  - 로깅은 성공 로그와 실패 로그를 전부 저장해야 한다.
  - 확인방법
    - ✓ 명령어 : SQLCMD.EXE -S 127.0.0.1 -e -s "," -Q "xp_loginconfig"
    - ✓ Login mode : Mixed => Windows / Account
    - ✓ Audit level : all => Success / Failed(Default)

```
name                          ,config_value
------------------------------,----------------------------
login mode                    ,Mixed
default login                 ,guest
default domain                ,ESALECO
audit level                   ,all
set hostname                  ,false
map _                         ,domain separator
map $                         ,NULL
map #                         ,-
```

## Database Configurations

- **User List**
  - 로그인에 사용되는 사용자 목록을 보여준다.
  - 확인방법
    - ✓ 명령어 : SQLCMD.EXE -E -Q "select name,type_desc,create_date,modify_date from sys.sql_logins order by create_date,modify_date"

```
name                  type_desc     create_date             modify_date
--------------------- ------------- ----------------------- -----------------------
sa                    SQL_LOGIN     2003-04-08 09:10:35.460 2012-01-25 11:48:10.530
dorumugs              SQL_LOGIN     2012-01-25 14:38:33.630 2012-01-25 14:38:34.160

(2 rows affected)
```

## Database Configurations

- **Active Transaction Log 확인**
  - 활성화된 Transaction Log를 확인한다.
  - 확인방법
    - ✓ 명령어 : SQLCMD.EXE -S 127.0.0.1 -e -s "," -Q "dbcc loginfo"

```
dbcc loginfo
FileId     ,FileSize           ,StartOffset        ,FSeqNo     ,Status     ,Parity,CreateLSN
-----------,-------------------,-------------------,-----------,-----------,------,----------------------------------------
          2,             253952,               8192,        195,          0,    64,                                     0
          2,             262144,             262144,        194,          0,   128,                                     0
          2,             262144,             524288,        196,          0,   128,         190000000035200448
          2,             262144,             786432,        197,          0,   128,         191000000013600274
          2,             262144,            1048576,        198,          2,   128,         191000000021600452

(5 rows affected)
DBCC 실행이 완료되었습니다. DBCC에서 오류 메시지를 출력하면 시스템 관리자에게 문의하십시오.
```

2 == Active / 0 == Recoverable or unused

## Database Configurations

- **Data Files와 Log Files 위치**
  - Database가 사용하는 Data Files와 Log Files 경로를 파악한다.
  - 확인방법
    - ✓ 명령어 : sqlcmd.exe -S 127.0.0.1 -e -s "," -Q "sp_helpdb wizmall(Database 명)"

```
sp_helpdb wizmall
name                ,db_size      ,owner
------------------,------------,------------------------------------------------------------
wizmall             ,     20.06 MB,DORUMUGS-TEDSZ8\Administrator

name                ,fileid,filename
------------------,------,------------------------------------------------------------------
wizmall_Data        ,     1,C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data\wizmall_Data.mdf
wizmall_Log         ,     2,C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data\wizmall_log.ldf
```

## Database Configurations

- **중요 설정 내용 확인**
  - Trace를 Logging하는지, xp_cmdshell을 사용하는지 확인한다.
  - 확인방법
    - ✓ 명령어 : SQLCMD.EXE -S 127.0.0.1 -e -s "," -Q "select * from sys.configurations"

```
1 == enable
0 == disable
select * from sys.configurations
configuration_id,name                                   ,value
----------------,---------------------------------------,---------------
          1568,default trace enabled                    ,1
          1569,blocked process threshold                ,0
          1570,in-doubt xact resolution                 ,0
          1576,remote admin connections                 ,0
         16384,Agent XPs                                ,1
         16385,SQL Mail XPs                             ,0
         16386,Database Mail XPs                        ,0
         16387,SMO and DMO XPs                          ,1
         16388,Ole Automation Procedures                ,0
         16389,Web Assistant Procedures                 ,0
         16390,xp_cmdshell                              ,0
         16391,Ad Hoc Distributed Queries               ,0
         16392,Replication XPs                          ,0

(62개 행 적용됨)
```

# SQL Server Forensics

- Databases Files
- Database Configurations
- ***Data Acquisition***
- Database Analyze
- Deleted Row
- WFTSQL

## Data Acquisition

- **수집 중요도 계산**
  - 10 - (Significance Rating) + (Volatility rating) = Priority

| Item | Importance | Volatility | Priority |
|---|---|---|---|
| SQL Server Connections & Sessions | 5 | 5 | **0** |
| Transaction Log(s) | 5 | 4 | **1** |
| SQL Server Logs | 4 | 3 | **3** |
| SQL Server Database Files | 3 | 2 | **5** |
| System Event Logs | 2 | 2 | **6** |

## Data Acquisition

- Netstat Information
- Active Transaction Log
- DBCC Log
- Database Plan Cache
- Additional Database Plan Cache
- Database Data Files & Logs
- Default Trace Files
- SQL Server Error Logs
- Windows Event Logs

## Data Acquisition

- **Netstat Information**
  - Connection 및 Session 내역을 확인
  - 수집 방법
    - ✓ 명령어 : netstat -ano

## Data Acquisition

- **Active Transaction Log**
  - 수집 방법
    - ✓ 명령어 : SQLCMD.EXE -S 127.0.0.1 -e -s "," -Q "select * from ::fn_dblog(NULL,NULL)"
      - NULL,NULL : 현재 데이터베이스의 모든 Transaction Log를 출력
      - Default,Default : NULL,NULL과 동일

## Data Acquisition

- **DBCC Log**
  - 수집 방법
    - ✓ 명령어 : SQLCMD.EXE -S 127.0.0.1 -e -s "," -Q "dbcc log(wizmall, 3)"
      - 0 : 최소한의 정보(Operation, Context, Transaction id)
      - 1 : 0보다 많은 정보(Flags, Tags, row length, description)
      - 2 : 1보다 많은 정보(Object name, index name, page id, slot id)
      - 3 : Operation에 따른 모든 정보
      - 4 : 3 + Current transaction logs의 row에 대한, hexadecimal dump

## 수집 데이터

- **Database Plan Cache**
  - 정상적이지 않은 명령어 확인
  - 수집 방법
    - ✓ 명령어 : SQLCMD.EXE -S 127.0.0.1 -e -s "," -Q "select * from sys.dm_exec_cached_plans cross apply sys.dm_exec_sql_text(plan_handle)"

## 수집 데이터

- **Additional Database Plan Cache**
  - 수집방법
    - ✓ 명령어 :
      - SQLCMD.EXE -S 127.0.0.1 -e -s "," -Q "select * from sys.dm_exec_query_stats"
      - SQLCMD.EXE -S 127.0.0.1 -e -s "," -Q "select * from sys.dm_exec_cached_plans cross apply sys.dm_exec_plan_attributes(plan_handle)"

## Data Acquisition

- **Database Data Files & Logs**
  - MDF
    - ✓ DATA PAGEs로 구성
    - ✓ 실질적인 Data Row를 저장
  - LDF
    - ✓ 물리적 Transaction Log를 저장
  - 수집 방법
    - ✓ 방법
      - 서비스 OFF 후, 데이터를 수집
      - Dcfldd를 사용하여, Hash 값을 생성하면서 복사
    - ✓ 위치 : ₩₩Microsoft SQL Server₩MSSQL.1₩MSSQL₩DATA₩*.MDF | *.LDF

## Data Acquisition

- **Default Trace Files**
  - 권한에 의해 제한된 명령을 수행할 때, 로그를 저장
    - ✓ 예 : 사용자 추가, 권한 상승 등
    - ✓ DDL Operations이 Database에 접근할 때도 로그를 저장
      - DDL : 데이터 정의어 (SCHEMA, DOMAIN, TABLE, VIEW, INDEX를 정의 및 변경, 삭제)
      - DML : 데이터 조작어 (SELECT, INSERT, DELETE, UPDATE 명령어와 같이 저장된 데이터를 처리)
      - DCL : 데이터 제어어 (COMMIT, ROLLBACK, GRANT, REVOKE와 같이 데이터 베이스 관리를 목적으로 사용)
  - 수집 방법
    - ✓ 명령어 : SQLCMD.EXE -S 127.0.0.1 -e -s "," -Q "select * from fn_trace_gettable('C:₩Program Files₩Microsoft SQL Server₩MSSQL.1₩MSSQL₩LOG₩log_6.trc',default) order by starttime"
    - ✓ 위와 같이 수집은 되나, **SQL Server Profiler**로 확인한 결과와 차이가 존재함

## Data Acquisition

- **SQL Server Error Logs**
  - SQL Server의 재시작 시간
  - 사용자 접속 성공 / 실패 내역
  - 수집 방법
    - ✓ 위치 : ₩₩Microsoft SQL Server₩MSSQL.1₩MSSQL₩LOG₩ERRORLOG

## Data Acquisition

- **Windows Event Logs**
  - Default 경로
    - ✓ Windows XP / 2003 : C:₩windows₩system32₩config
    - ✓ Windows Vista / 7 : C:₩windows₩system32₩winevtlogs
  - 수집 방법
    - ✓ 명령어 :
      - psloglist.exe /accepteula –g Syslog.evt system
      - psloglist.exe /accepteula –g Seclog.evt security
      - psloglist.exe /accepteula –g Applog.evt application

## Database Analyze

- **조사 순서**
  - Error Log에서 SQL Server의 재시작 시간과 사용자 접속 시간 파악
  - Trace Log로 추가된 계정이나 권한이 상승된 내역 확인
    - ✓ 의심되는 SPID(서비스 제공 식별자(쿼리를 실행한 프로세스 ID)를 확인
  - 의심 SPID 기준으로 Transaction Log 확인
    - ✓ Transantion Log는 "LOP BEGIN XACT"로 시작, "LOP COMMIT XACT"로 끝을 나타냄
    - ✓ 시작과 끝 사이에 수정, 삭제 등과 같은 내역이 존재함
    - ✓ 의심 SPID의 수정 및 삭제의 Transaction ID와 Page ID, Slot ID를 확인함
  - 확인된 Page ID는 아래와 같은 명령어로 확인
    - ✓ dbcc page (<database명>, 페이지 ID, 페이지 파일 번호, Print option)
      - Print option 1은  Page header를 요청함
      - 예> dbcc page(wizmall, 1, 211, 1)

# SQL Server Forensics

- Databases Files
- Database Configurations
- Data Acquisition
- ***Database Analysis***
- Deleted Row
- WFTSQL

## Database Analysis

- **조사 순서**
  - Page Header에서 Object ID를 확인
    - ✓ 확인된 Object ID는 아래 명령어로 확인
      - Select * from sysobjects where id="Object_ID"
    - ✓ 해당 Object ID에 대한, 스키마 확인
      - "SELECT sc.colorder, sc.name, st.name as 'datatype', sc.length FROM syscolumns sc, systypes st WHERE sc.xusertype = st.xusertype and sc.id = **"Object ID"** ORDER BY colorder"
  - Slot ID에서 Row offset 만큼 이동 후, 수정되거나 추가, 삭제된 내용 확인
    - ✓ 기존에 입력되어 있는 값을 관리자에게 확인할 수 있을 경우, 분석에 용이함
  - Transaction Log의 Row Log0과 Row Log1의 값을 비교하여, 변경 전과 변경 후를 확인

## Database Analysis

- **Row Log**
  - 수정
    - ✓ 해당 Transaction Log에서 Row Log 0[변경 전]과 Row Log 1[변경 후]을 비교하여 확인 가능
  - 삽입
    - ✓ 해당 Transaction Log의 Slot ID를 확인하여 어떠한 데이터가 삽입되었는지 확인 가능
  - 삭제
    - ✓ 해당 Transaction Log에서 Page Header를 확인하면, "m_ghostRecCnt = 0" 을 확인할 수 있음
    - ✓ 해당 Transaction Log의 Slot ID를 확인하여 어떠한 데이터가 삭제되었는지 확인 가능
    - ✓ 쓰레기 값을 청소하는 프로세스로 인해 데이터가 오래 살아 있지는 않고 새로운 값으로 덮어씌어질 가능성이 높음

# SQL Sever Forensics

- Databases Files
- Database Configurations
- Data Acquisition
- Database Analysis
- ***Deleted Row***
- WFTSQL

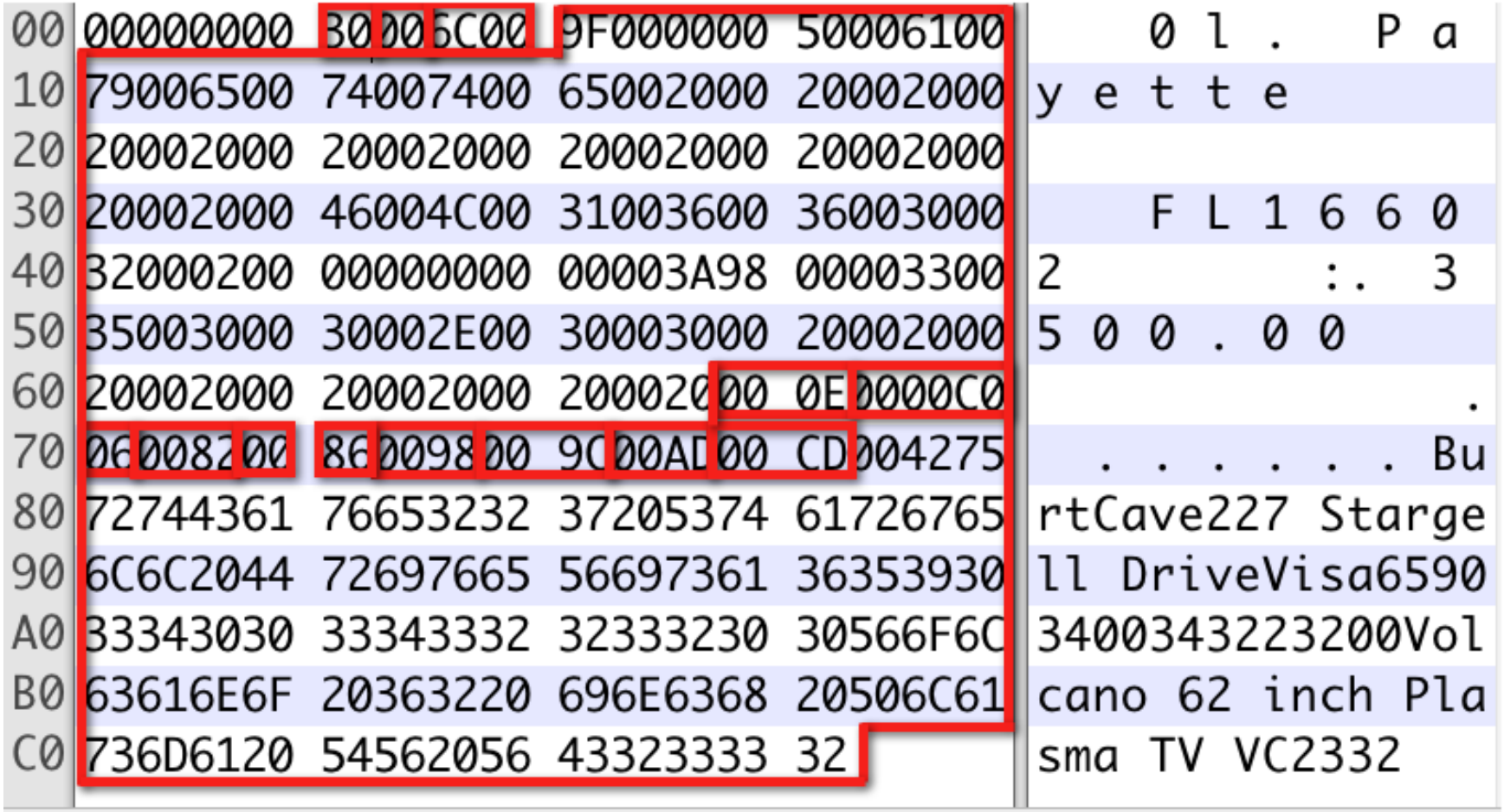
## Deleted Row

- **Row Log Format**


| Item | 할당 크기 | 설명 |
|---|---|---|
| 1 | 1 byte | Data row 속성을 표현하는 status bit A |
| 2 | 1 byte | SQL 2005에서 사용 X |
| 3 | 2 byte | Item 4에 대한 Offset |
| FLC | 모든 고정 크기의 column들에 대한 길이 | Fixed Columns |
| 4 | 2 byte | Data Row에 있는 Column들의 전체 갯수 |
| 5 | 각각의 Row Column에 대한 1bit | Null Bitmap |
| 6 | 2 byte | Variable Columns 갯수 |
| 7 | 2 byte | Variable Columns 의 각각의 길이 |
| VLC | 유동 길이를 가진 모든 column들에 대한 길이 | Variable Columns |

## Deleted Row

- Row Log Format



| | | | | | |
|---|---|---|---|---|---|
| 00 | 00000000 | 30006C00 | 9F000000 | 50006100 | 0 l . P a |
| 10 | 79006500 | 74007400 | 65002000 | 20002000 | y e t t e |
| 20 | 20002000 | 20002000 | 20002000 | 20002000 | |
| 30 | 20002000 | 46004C00 | 31003600 | 36003000 | F L 1 6 6 0 |
| 40 | 32000200 | 00000000 | 00003A98 | 00003300 | 2 : . 3 |
| 50 | 35003000 | 30002E00 | 30003000 | 20002000 | 5 0 0 . 0 0 |
| 60 | 20002000 | 20002000 | 20002000 | 0E0000C0 | . |
| 70 | 06008200 | 86009800 | 9C00AD00 | CD004275 | . . . . . Bu |
| 80 | 72744361 | 76653232 | 37205374 | 61726765 | rtCave227 Starge |
| 90 | 6C6C2044 | 72697665 | 56697361 | 36353930 | ll DriveVisa6590 |
| A0 | 33343030 | 33343332 | 32333230 | 30566F6C | 340034322320Vol |
| B0 | 63616E6F | 20363220 | 696E6368 | 20506C61 | cano 62 inch Pla |
| C0 | 736D6120 | 54562056 | 43323333 | 32 | sma TV VC2332 |

## Deleted Row

- **Deleted Row's Page Header**
  - "m_ghostRecCnt = 0" 은 물리 data page에서 이미 삭제되었다는 것을 나타냄
  - 물리적으로 Data가 삭제된 경우, Transaction Log의 Row Log 0에서 확인 가능

```
Page @0x043D0000

m_pageId = (1:344)                    m_headerVersion = 1                   m_type = 1
m_typeFlagBits = 0x4                  m_level = 0                           m_flagBits = 0x8200
m_objId (AllocUnitId.idObj) = 78      m_indexId (AllocUnitId.idInd) = 256
Metadata: AllocUnitId = 72057594043039744
Metadata: PartitionId = 72057594039042048                                   Metadata: IndexId = 1
Metadata: ObjectId = 245575913        m_prevPage = (1:190)                  m_nextPage = (1:191)
pminlen = 108                         m_slotCnt = 27                        m_freeCnt = 2876
m_freeData = 6899                     m_reservedCnt = 0                     m_lsn = (16:3626:1)
m_xactReserved = 0                    m_xdesId = (0:818)                    m_ghostRecCnt = 0
m_tornBits = -1097693874
```

# SQL Server Forensics

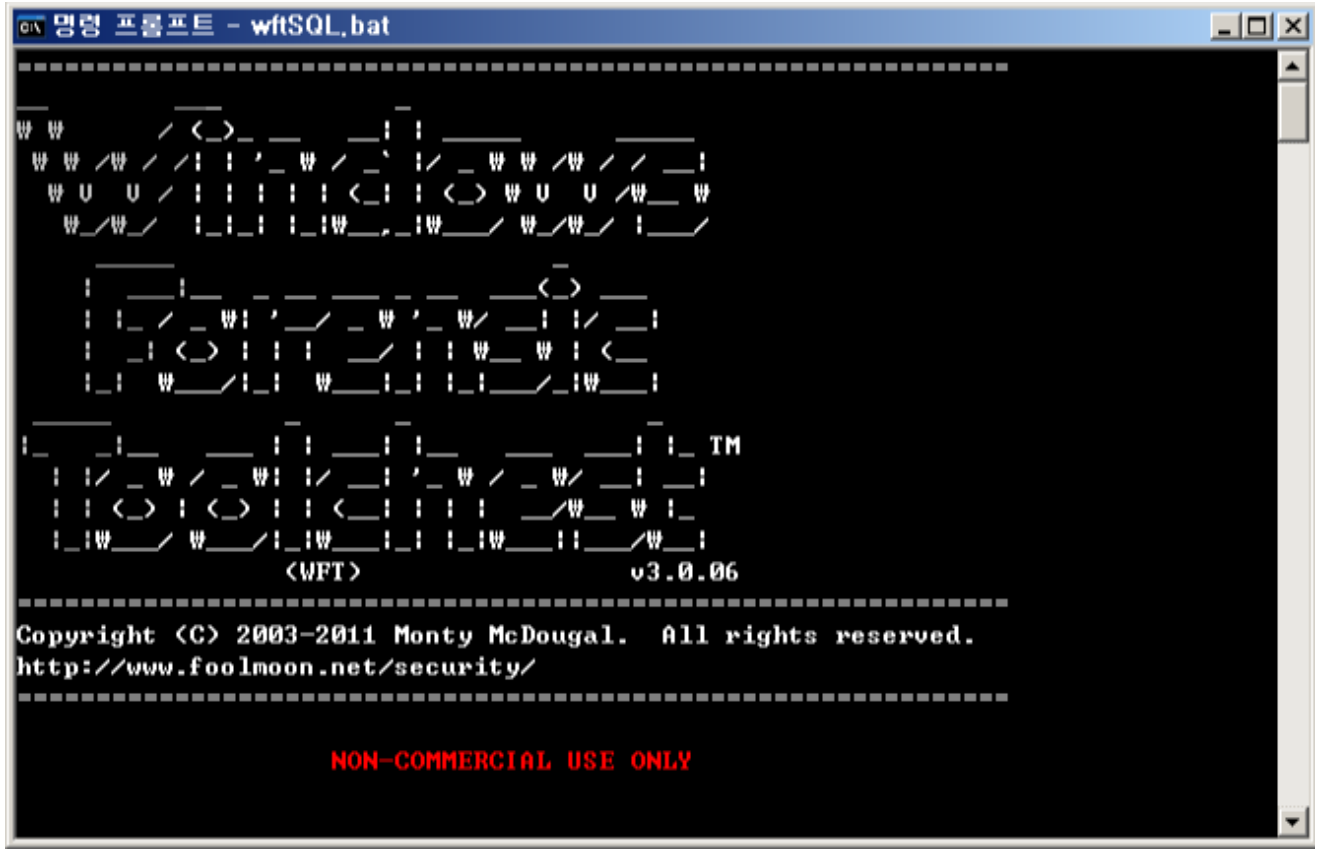
- Databases Files
- Database Configurations
- Data Acquisition
- Database Analysis
- Deleted Row
- ***WFTSQL***

## WFTSQL

- **WFTSQL**
  - 기존에 존재하는 WFT에서 SQL분석에 맞게 설정된 스크립트
  - 사용되는 바이너리와 설정파일들은 WFTHASH와 MD5로 검증
  - WFT는 침해대응에 필요한 바이너리를 사용하여 휘발성 및 비휘발성 데이터를 수집
  - WFT는 SQLCMD.EXE와 쿼리 스크립트를 사용하여 데이터베이스 로그를 수집
  - WFT.exe는 만료 기간이 정해져 있으며, 지속적으로 아래 홈페이지에서 다운로드 가능하다.
    - ✓ http://www.foolmoon.net/security/wft/
  - 사용 가능한 OS
    - ✓ Windows NT / 2K/ XP/ 2K3/ Vista / Win 7

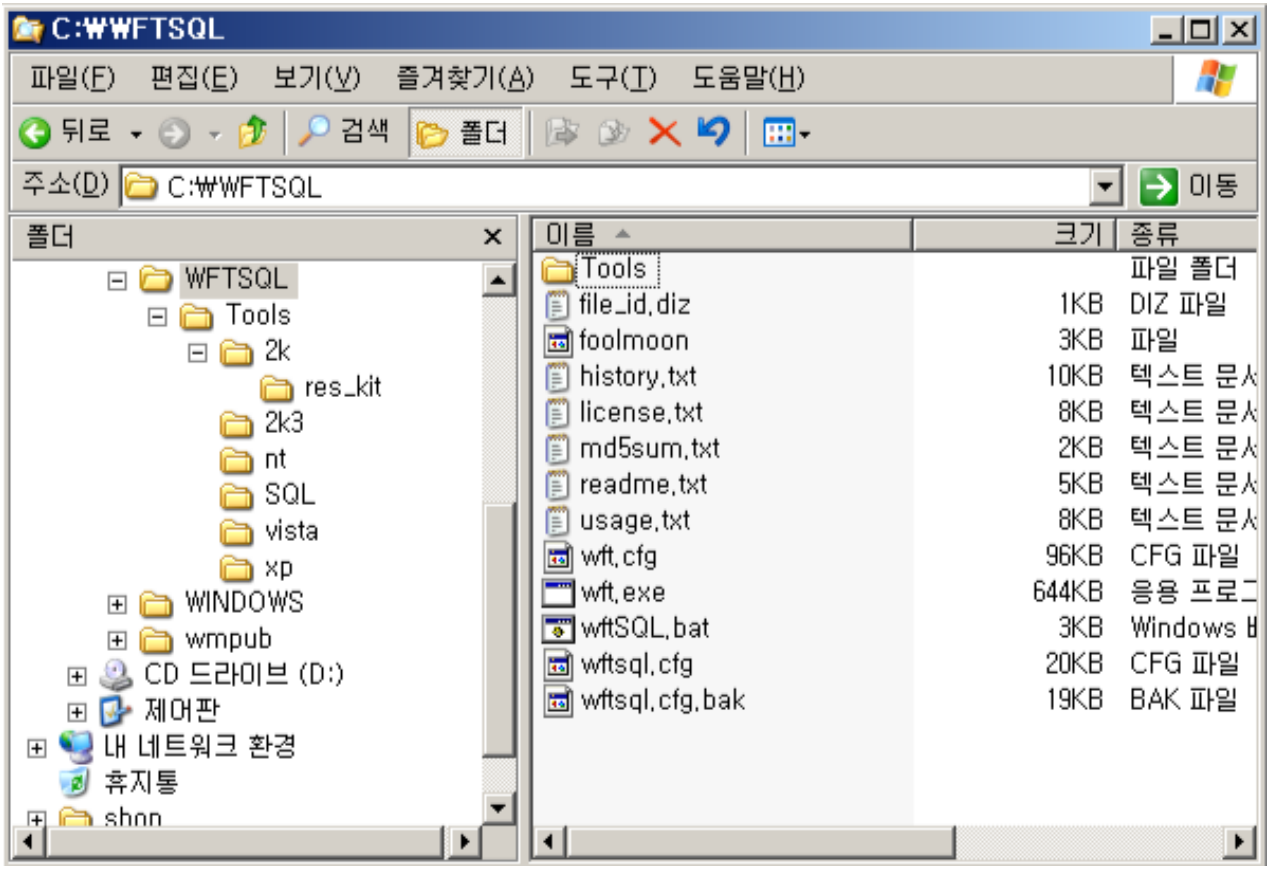
## WFTSQL

- **WFTSQL Script**



## WFTSQL

- **WFTSQL 구성**

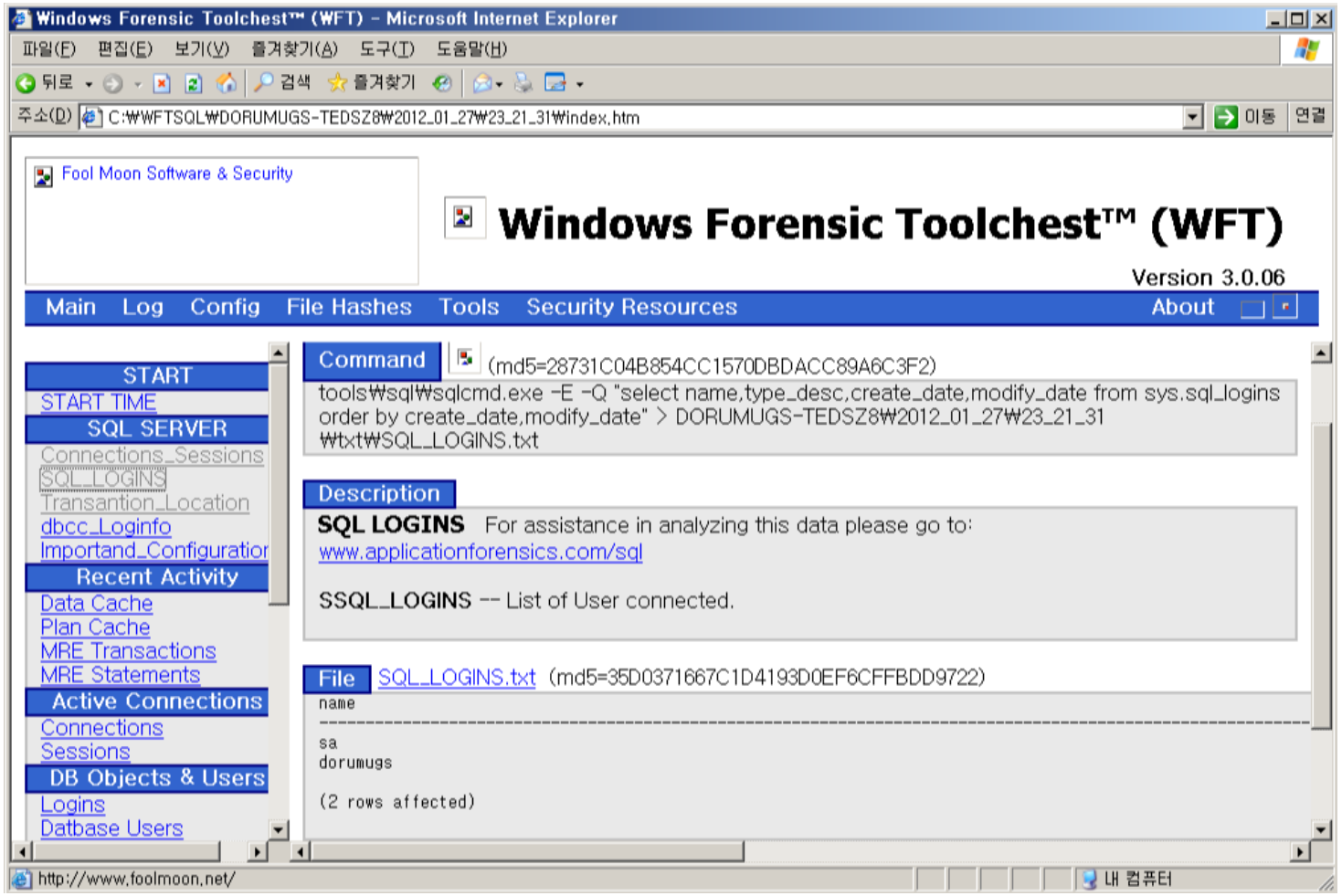


## WFTSQL

- **WFTSQL 구성**
  - WFTSQL
    - ✓ WFT.exe 및 WFT에 사용되는 Config files
  - 2K / 2K3 / nt / vista / xp
    - ✓ 시스템에서 사용되는 명령서 (EX : cmd.exe)
  - SQL
    - ✓ WFTSQL.bat가 사용하는 SQL 스크립트
    - ✓ SQLCMD.exe 및 SQLCMD.exe가 사용하는 라이브러리

## WFTSQL

- WFTSQL 결과



# 질문 및 답변