디지털 포렌식 연구
제7호(2010.11)

불법 사이트 사건 사례를 통한 데이터베이스 증거물 획득 방안

김 진 환† , 장 기 식*, 이 상 진**
경찰청 사이버테러대응센터*
고려대학교 정보보호전문대학원**

Case study of the Efficient Method to locate the Database Server for Finding Digital Evidence in the Illegal Website

Jin-Hwan Kim† , Ki-Sik Chang*, Sang-Jin Lee**
Cyber Terror Response Center, Korean National Police Agency*
Graduate School of Information Management and Security, Korea University**

요 약

최근 수사기관에서는 인터넷상에서 기하학적으로 증가하고 있는 도박사이트, 경마사이트, 음란물 사이트, 사기 쇼핑몰 등과 같은 불법 사이트를 지속적으로 단속하고 있지만 새로운 유형의 미니 선물 거래 사이트, 피싱사이트 등이 생겨나고 수사기관의 추적을 피하기 위한 수법이 날로 발전하고 있어 수사에 많은 어려움을 주고 있다. 이러한 불법사이트들은 대부분 웹서비스를 기반으로 운영되지만 회원정보나 범행관련 거래내역 등 핵심적인 자료들은 데이터베이스에 별도 저장된다. 따라서 불법사이트에 대한 수사는 데이터베이스 서버를 확보하는 것에 중점을 두어야 하며 이 데이터베이스의 확보에 따라 수사의 성공여부를 판가름 할 수 있다.

본 논문에서는 최근 성행하는 미니 선물 거래 사이트에 대한 수사사례를 통해 웹서비스와 어플리케이션, 데이터베이스로 구성된 불법사이트 시스템에 대한 압수수색 절차 및 방법과 데이터베이스를 획득하는 방법을 소개한다.

Keywords : 불법사이트, 웹, 데이터베이스

† 교신저자 : jhkim74@police.go.kr

Ⅰ. 서 론

인터넷 도박이나 경마 등과 같은 사행성 게임 사이트, 사기를 목적으로 하는 온라인 쇼핑몰, 피싱 사이트는 우리나라 현행법을 위반한 불법사이트들로 수사기관에서 지속적으로 단속이 이루어지고 있다. 그러나 최근에는 금융위원회의 인가를 받지 않고 현금을 거래하는 미니 선물 사이트가 새롭게 등장하여 많은 피해자를 양산하고 있다.

이러한 불법사이트들은 대부분 웹 서버와 데이터베이스 서버로 이분화되어 있으며 수사를 진행하기 위해서는 해당 서버들을 모두 압수하여 법원에 증거물로 제출해야 한다. 특히 데이터베이스 서버는 거래내역이나 회원정보 등과 같이 범죄와 관련된 모든 정보를 저장하고 있기 때문에 해당 데이터베이스를 획득하는 것이 수사에 있어 매우 중요한 작업 중의 하나이다.

불법 도박 사이트 경우에는 웹사이트 주소가 포함된 문자메시지를 무차별적으로 송신하여 회원을 모집한다. 웹사이트 주소는 회원들뿐만 아니라 수사기관에도 노출이 되기 때문에 회원 가입 기능과 실제 운영되고 있는 게임 사이트를 안내하는 역할만 하고 있다. 불법 사이트로 판정되어 해당 인터넷 주소가 차단되면 또 다른 웹사이트 주소로 웹서비스를 변경하여 변경된 웹사이트 주소를 회원들에게 통보만 해주면 다시 같은 회원들을 상대로 계속적으로 사이트를 운영할 수 있다. 이런 운영이 가능한 것은 실제 데이터베이스 서버는 단속되지 않고 포워딩 기능만 탑재된 웹사이트가 단속하기 때문이다. 여기에 설령 운영자를 검거되더라도 이에 대한 범죄사실을 구증하는 것이 쉽지 않다.

또한 특정 단체들이 자체적으로 운영하고 있는 사설 웹서비스 경우에는 회원전용 게시판을 운영하면서 허위사실 유포 및 명예훼손 범죄에 해당되는 글을 게시하는 경우가 자주 발생하고 있는데 범죄를 입증하기 위해서는 게시된 글이 저장된 데이터베이스 서버를 특정한 다음 해당 서버를 압수해야하나 해당 서버를 찾지 못해 수사 진행에 있어 많은 어려움을 겪고 있다.

불법사이트를 단속하는 수사기관에서는 범죄자를 검거하기 전에 증거물을 먼저 확보해야 한다. 증거 확보를 위해서는 범죄 구증에 있어 제일 중요한 데이터베이스 서버를 압수해야하나 현실적으로는 데이터베이스 서버를 찾지 못한 상태에서 웹서비스가 운영되는 웹서버 만 찾아 전원을 차단한 후 해당 서버에 장착되어 있는 하드디스크를 복제하거나 이미징 작업을 통해 압수를 진행해왔다. 압수된 웹 서버의 하드디스크를 분석하여 데이터베이스에 대한 정보를 입수하게 되면 다시 동일 장소에서 데이터베이스 서버를 압수하기 위해 운영자에게 통보 후에 데이터베이스 서버의 전원을 내려 다시 하드디스크 복제나 이미징 작업을 진행해왔다. 하지만 여러 차례 수사기관에 검거된 경력이 있는 사이트 운영자들은 이런 압수수색 과정을 통하여 수사기관의 수사 및 압수수색을 눈치 채고 증거자료를 인멸한 후 도주하는 경우가 종종 발생하고 있다.

본 논문에서는 불법 무인가 미니 선물 거래 사이트 수사 사례를 통하여 웹서비스와 데이터

베이스가 연동되는 웹 사이트에 대한 압수수색 절차와 외부에 노출되지 않은 데이터베이스 서버를 찾는 방법을 소개한다.

Ⅱ. 미니선물거래사이트 사건에 대한 수사 사례

2.1 사건개요

[사건개요]

피의자는 2010년 3월 3일부터 2010년 11월 13일까지 금융위원회에서 금융투자업인가를 받지 아니하고 금융투자업을 영위하고, 한국거래소가 개설하는 파생상품시장과 유사한 시설인 A사이트(http://www.XXXXXX.co.kr)을 개설한 것으로, 이 사이트는 도박사이트와 유사하게 범행계좌로 현금을 입금받고 이를 사이버머니로 전환시켜주어 자체 개발한 홈트레이딩시스템 (HTS)을 통해 실제 코스피 200지수에 의해 사설 선물 매매를 하게 하고, 여기에서 발생하는 회원들의 손실금과 수수료 명목으로 1계약당 0.002%를 해당하는 금액을 통해 3억원 상당한 재산상 이득을 취한 것이다.

위 A사이트는 무인가 미니 선물 거래 사이트로써, 웹서버와 HTS(Home Trading System, 온라인 주식매매 프로그램) 어플리케이션 서버, 데이터베이스 서버로 구성되어 있었다. 여타 불법사이트와 마찬가지로 웹서버에는 회원모집 및 가입, 공지사항 등만을 게시하고 있었으며 실제 선물 매매는 별도로 제작한 HTS 클라이언트 프로그램을 배포하여 이를 통해 가상 선물매매를 하게 하고 사이버머니를 출금해 주었다.

그리고 이 사이트에 등록한 회원 정보 및 HTS를 통해 선물매매 정보가 웹페이지와 HTS창에서 모두 보여지므로 이런 정보들이 모두 데이터베이스에 누적해서 관리가 되고 있는 것으로 판단되었다.

2.2 시스템 구성 정보 수집

이 웹서버 주소인 www.XXXXXX.co.kr에 할당된 IP주소와 HTS 어플리케이션 서버는 같은 호스팅업체에서 코로케이션 서비스를 받고 있었다. 이 2개 서버를 상대로 포트 스캐닝을 통해 열린 TCP 포트를 확인한 결과, 데이터베이스 네트워크 서비스 포트로 판단되는 TCP 포트를 발견하지 못하였다.

2.3 압수수색 영장 신청 및 집행

이 웹서버 주소인 www.XXXXXX.co.kr와 HTS 어플리케이션 서버가 운영되고 있는 서버에 대해 법원에 압수수색 영장을 신청하여 집행하였다.

2.3.1 압수수색영장 신청

압수수색할 서버들이 통신자료제공 요청으로 모두 코로케이션 서비스를 받고 있는 것으로 확인되었다. 이는 웹호스팅이나 서버호스팅과 달리 서버들의 소유자가 사이트 운영자로 시스템 자체를 압수해도 무관하지만 이 당시 범죄사실이 구증되지 않은 시점이었기 때문에 계속적으로 운영을 시키면서 이 서버의 하드디스크만 증거자료로 확보하고자 하였다.

[압수수색영장 압수수색할 물건[1]]

웹서버 IP주소 XXX.XXX.XXX.XXX와 HTS서버 IP주소 XXX.XXX.XXX.XXX를 할당받아 운영되고 있는 시스템과 이와 물리적, 네크워크로 연결된 시스템에 대해
- 상기 시스템
- 상기 시스템에 장착된 저장장치
- 상기 시스템에 장착된 하드디스크 복제 및 이미징
- 상기 시스템에 장착된 이동식 저장매체
- 상기 시스템 임대에 대한 계약서 및 비용 결제 내역
- 상기 시스템에 대한 상담 및 작업일지
- 상기 시스템에 설치된 방화벽 로그
- 상기 시스템의 트래픽 모니터링 자료

2.3.2 압수수색영장 집행 및 결과

범죄자인 운영자는 선물 매매가 이루어지는 08:00부터 15:20까지 항시 접속하여 정산 작업을 하기 때문에 시스템 자체를 모두 압수한다면 수사를 눈치채고 증거인멸 및 도주 우려가 상당히 높았다. 그리고 서버 압수에 대해 운영자의 눈을 피하고자 무정전 상태로 이미징 작업을 하고자 하였으나 압수 대상 시스템의 아이디 및 비밀번호를 전혀 알 수 없었다. 따라서 위 압수수색할 물건 사항과 같이 먼저 트래픽 모니터링 자료를 압수하여 시스템 전원을 끄고, 하드디스크를 복제하기 위한 시간대를 선정하였다.

동시에 웹서버와 HTS서버의 하드디스크를 복제하였으며 바로 현장에서 이 2개 서버 하드디스크에서 데이터베이스 서버 위치를 특정해야만 했다. 그래서 웹소스에서 데이터베이스 연결 부분 소스와 HTS 윈도우 서버에서 ODBC/OLE 연결 항목을 검색하였다.

그 결과, [그림 1]와 같이 웹서버 하드디스크 웹소스 폴더 "\web\HTS_ADMIN\common\f_dbconnect.asp" 파일에서 데이터베이스 IP주소를 확인하였다.

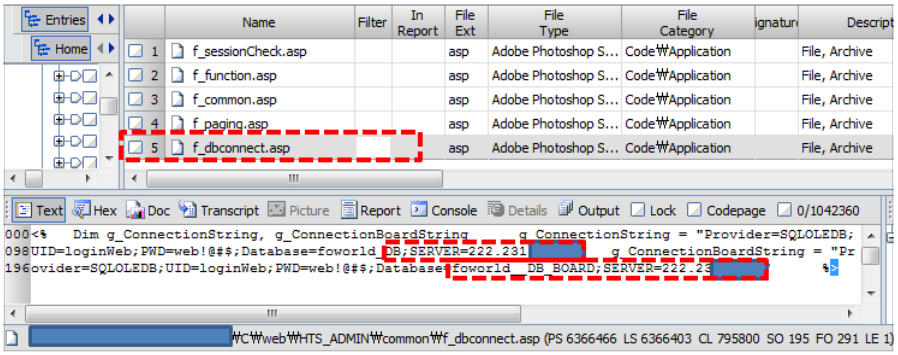

그림 1. 웹서버 f_dbconnect.asp 파일 속성 및 저장 데이터값

[그림 2]와 같이 HTS 서버 하드디스크내 윈도우 ODBC/OLE 항목이 저장되는 레지스트리 "\HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI"[2]에서 같은 데이터베이스 서버 IP주소가 확인되었다.

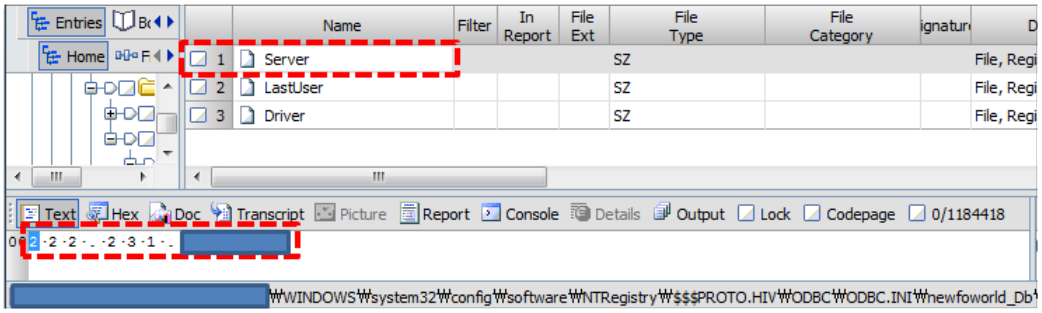

그림 2. HTS서버 ODBC/OLE 등록 레지스트리값

따라서, 위 2개 서버에서 공통적으로 특정된 데이터베이스 서버를 확인한 결과, 예상대로 회원 정보나 선물 매매 내역이 모두 저장되어 있는 데이터베이스가 발견되어 이 서버를 압수하여 증거물로 제출하였다.

Ⅲ. 데이터베이스 획득을 위한 사이트 압수수색 절차 및 방법

외부에 노출된 웹서버와 어플리케이션 서버에 대해 1개의 압수수색 영장를 발부받아 집행 가능하다. 하지만 Ⅱ장 수사사례와 같이 외부에 노출되지 않는 데이터베이스를 1개의 영장으로 획득하는 것은 그리 쉽지가 않다. 일반적으로 소규모 사이트 같은 경우 1개 웹서버, 데이터베이스 서버로 구성되어 있으나 동시 접속자 수가 많은 사이트 같은 경우 로드밸런스 장비(L4)와 함께 다수 웹서버가 존재한다. 여기에서 현장에 나간 수사관이 전에 이런 시스템 구성을 접하지 못하였다면 당황하여 압수수색으로 얻고자 하는 증거자료를 획득하지 못할 경우도 있을 것이다.

따라서 이 장에서 데이터베이스와 연동되는 압수대상 사이트에 대해 압수수색하는 절차와 방법에 대해서 논할 것이다.

3.1 시스템 구성 정보 수집

수사대상 사이트에 대해 압수수색영장을 신청, 집행하기 전에 먼저 시스템의 기본 구성정보를 수집하여 이 점을 고려, 압수수색 영장을 신청해야 한다.

웹서비스 어플리케이션이나 데이터베이스가 각 벤더별로 다양한 버전으로 운영되고 있다. 더불어 현재 거의 모든 사이트들이 자체 회선이나 네트워크 장비, 서버 등을 직접 구성하여 운영하는 경우는 드물고, 거의 대부분 호스팅업체를 통한 서버 임대식으로 사이트를 운영하고 있다.

따라서 호스팅 서비스를 제공하고 있는 업체를 상대로 웹호스팅, 서버호스팅, 코로케이션인지를 먼저 파악한다. 각 서버별로 포트 스캐닝을 통해 동작 운영체제와 데이터베이스 제품명 등을 확인하고 이에 맞는 압수수색 영장을 신청해야 한다.

[표 1]은 각 데이터베이스별로 서비스하고 있는 네트워크 기본 포트번호이다. 물론 Ⅱ장 수사사례처럼 데이터베이스가 외부에 노출 되지 않는 경우가 다반사이지만 이 정보를 기반으로 각 시스템에 포트 스캐닝을 통해 어떤 데이터베이스가 운영되는지 먼저 확인해야 한다.

표 1. 데이터베이스별 네트워크 TCP 서비스 포트[3]

데이터베이스	Default TCP Port
MS-SQL	1433
Oracle	1521
MySQL	3306
PostgreSQL	5432

3.2 압수수색영장 신청 방법 및 유의사항

수사기관에서 강제적으로 증거물을 획득할 수 있는 수단이 바로 압수수색 영장이다. 이 영장은 경찰에서 신청, 검찰에서는 청구하여 법원에서 신청 사항을 모두 검토하고 합당할 때에만 발부된다. 압수수색 영장을 신청할 때는 신청한 압수할 물건외 다른 물건을 동일 영장으로는 압수할 수 없기 때문에 신청단계에서 철저한 검증을 거쳐 신청을 해야한다. 더군다나 외부에 노출되지 않는 데이터베이스 시스템에 대해서 1차, 2차를 거쳐 압수수색영장을 집행한다면 사이트 운영자들도

수사사항에 대해 인지를 하고 증거인멸과 도주를 시도할 것이다.

따라서 1개 압수수색 영장으로 동시에 웹서버 뿐만 아니라 데이터베이스 서버도 같이 압수수색 영장을 집행해야 한다.

본 저자는 [표 2]와 같이 각 호스팅 서비스별로 압수할 물건을 제시한다. 1개 서버에 가상 도메인 주소로 구성, 운영되는 웹호스팅과 서버임대식의 서버호스팅, 장소와 회선만 공급받아 운영되는 코로케이션별로 압수할 물건을 따로 구분하여 신청해야 한다.

표 2. 호스팅 서버별 압수할 물건 작성 예시

서비스구분	압수할 물건 작성 예시
웹호스팅	도메인 sample.co.kr에 대해 - 상기 도메인주소에 저장된 파일 전체 - 상기 도메인주소에서 사용된 데이터베이스 파일 및 백업된 자료 - 상기 도메인주소에 대한 웹로그, FTP, SSH, Telnet 등 시스템 로그 일체
서버호스팅	IP주소 XXX.XXX.XXX.XXX를 할당받아 운영되고 있는 시스템과 이와 물리적, 네크워크로 연결된 시스템에 대해 - 상기 시스템에 장착된 저장장치 - 상기 시스템에 장착된 하드디스크 복제 및 이미징 - 상기 시스템에 장착된 이동식 저장매체 - 상기 시스템 임대에 대한 계약서 및 비용 결제 내역 - 상기 시스템에 대한 상담 및 작업일지 - 상기 시스템에 설치된 방화벽 로그 - 상기 시스템의 트래픽 모니터링 자료
코로케이션	IP주소 XXX.XXX.XXX.XXX를 할당받아 운영되고 있는 시스템과 이와 물리적, 네크워크로 연결된 시스템에 대해 - 상기 시스템 - 상기 시스템에 장착된 저장장치 - 상기 시스템에 장착된 하드디스크 복제 및 이미징 - 상기 시스템에 장착된 이동식 저장매체 - 상기 시스템 임대에 대한 계약서 및 비용 결제 내역 - 상기 시스템에 대한 상담 및 작업일지 - 상기 시스템에 설치된 방화벽 로그 - 상기 시스템의 트래픽 모니터링 자료

3.3 시스템별 데이터베이스 특정 방법

압수수색 영장 집행 현장에서 데이터베이스 시스템을 검색할 수 있는 방법은 크게 휘발성 데이터 수집을 통한 네트워크 세션, 윈도우서버 ODBC 정보 검색, 웹 소스 검색 등 3가지로 나눌 수 있다.

3.3.1 휘발성데이터 수집을 통한 검색

흔히들 해킹 당한 서버를 분석하고자 할 때만 휘발성 데이터를 수집한다. 하지만 가능하다면 불법 사이트 압수시에도 휘발성 데이터를 먼저 수집한 후에 서버를 압수해야 한다.

서버에서 동작하고 있는 프로세스들을 통해 시스템 운영 구성을 파악할 수 있으며 **SSH, Telnet,** 터미널서비스 등 원격에서 접속해 있는 용의자의 **IP**주소를 확인할 수 있다. 네트워크 세션 정보를 통해 데이터베이스 시스템 및 현재 시스템에서 서비스에 접속한 **IP**주소를 확인할 수 있다.

[그림 3]와 같이 현재 웹서버의 네트워크 세션 정보를 통해 [표 1]와 같은 **MySQL** 기본 **TCP** 포트 번호인 **3306**번에 오픈하고 있는 특정 **IP**주소로 다수 접속하는 것이 확인된다. 여기에서 **MySQL**이 설치, 운영되고 있는 데이터베이스의 위치를 알 수 있다.

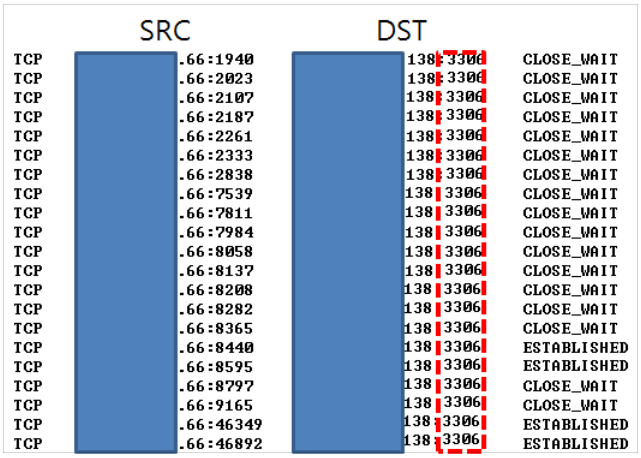

그림 3. 웹서버내 데이터베이스 **MySQL** 연결 세션 정보

하지만 서버를 압수할 당시 아이디와 비밀번호를 알지 못하는 경우가 다반사이다. 이와 같은 경우 데이터베이스와 연결되는 웹서버 앞단에 탭(Tab)장비를 연결하여 [그림 4]와 같이 데이터베이스 서비스 포트와 연결되는 패킷을 수집하면 데이터베이스의 **IP**주소를 특정할 수 있다.

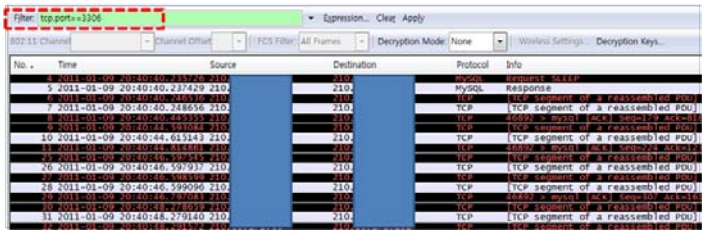

그림 4. **Tab**와 **WireShark**를 이용한 **TCP 3306**번 필터링

3.3.2 윈도우 서버의 ODBC DB 연결정보 검색

도박사이트의 게임서버나 Ⅱ장 사례와 같은 **HTS** 윈도우 어플리케이션 프로그램들은 윈도우의 **ODBC**를 통해 데이터베이스와 연결된다.

윈도우 어플리케이션 프로그램들은 **[표 3]**와 같이 설치된 각 데이터베이스별 드라이브 정보와 함께 서버의 **IP**주소, 아이디, 비밀번호 등을 설정 데이터베이스와 연결된다. 이 윈도우 레지스트리 **\HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI** 하위에 **ODBC**에 설정된 데이터베이스 정보를 확인 할 수 있다.

표 3. 데이터베이스별 윈도우 ODBC DB 설정 정보[4]

DB	ODBC
SQL Server	Driver={SQL Server};*Server=IP*;Database=myDataBase;Uid=myUsername; Pwd=myPassword;
SQL Server 2005	Driver={SQL Native Client};*Server=IP*;Database=myDataBase;Uid=myUsername; Pwd=myPassword;
Oracle	Driver={Microsoft ODBC for Oracle};*Server=IP*;Uid=myUsername; Pwd=myPassword;
MySQL 5.1	DRIVER={MySQL ODBC 5.1 Driver};*Server=IP*;DATABASE=test;UID= myUsername;PWD=myPassword;
Postgre SQL	Driver={PostgreSQL};*Server=IP*;Port=5432;Database=myDataBase;Uid=myUsern ame;Pwd=myPassword;

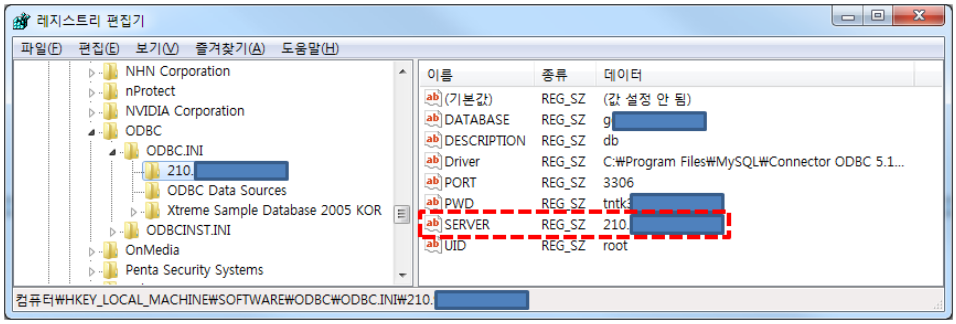

그림 5. MySQL ODBC 설정 정보

3.3.3 웹소스 파일에서 데이터베이스 연결정보 검색

웹 프로그래밍에 사용되는 일반적인 언어 **ASP, PHP, JSP**는 인터프리터로 되어 있으며 "해석기"가 코드를 한줄씩 해석하여 사용자가 이해할 수 있는 문서인 **HTML**로 변환해 준다.

웹 서버내 웹 어플리케이션은 **ASP, PHP, JSP** 언어를 이용하여 코딩되어 있기 때문에 이 웹 서버가 연결되는 데이터베이스 서버의 **IP**주소도 소스 코드에서 문자열로 확인이 가능하다. 그리고 일반적으로 이런 데이터베이스 연결과 같은 소스 코드는 모든 웹페이지에서 사용하기 때문에 공통적으로 사용되는 라이브러리 폴더인 **\common** 등과 같은 폴더명으로 명명된 모듈 폴더에 존재한다. 역시 파일명 **db_connect.asp, dbconn.php, com_dbconnect.jsp** 등과 같이 데이터베이스와 연관된 단어들로 파일명을 생성한다.

따라서 Ⅱ장 수사사례에서 본 것과 같이 웹서버 및 데이터베이스와 연결되는 것으로 추정되는 서버의 하드디스크를 복제 및 이미징 작업을 한 후, 바로 위와 같은 데이터베이스와 연결되는 웹소스 파일을 검색해서 데이터베이스 서버 **IP**주소를 특정하고, 바로 이 서버에 같은 방법으로 압수를 해야한다.

[표 4]와 같은 각 언어별 데이터베이스(**MS-SQL**) 연결 소스와 같이 보통의 소스 코드는 변수로 데이터베이스 서버와 연결 정보를 설정하고, 객체 생성, 설정된 변수를 인자로 함수를 호출하는 구조로 되어 있다. 여기에서 **Server IP** 문자열 값이 우리들이 찾고 있는 데이터베이스의 **IP**주소가 되는 것이다.

표 4. 웹 프로그램 언어별 데이터베이스 연결 소스 파일 예시

웹프로그램 언어	웹 프로그래밍 예시
ASP (mssql 연결)[5]	//DB 연결정보 StrConn = "Provider=SQLOLEDB;*Data Source = DB Server IP*;Initial Catalog=DB명;User ID=myUsername;Password=myPassword" //객체생성 set Conn = server.CreateObject(*"ADODB.Connection"*)
PHP (mssql 연결)[6]	//DB 연결정보 *$hostnaem = DB Server IP* $user_id = myUsername $password = myPassword $DbName = DB명 //객체생성 $Conn = MSSQL_CONNECT(*$hostname*, $user_id, $passworld)
JSP (mssql 연결)[7]	//DB 연결정보 Class.forName("com.mircrosoft.jdbc.sqlser.SQLServerDriver"); String strUrl = "jdbc:microsoft:*sqlserver:DB Server IP*:databasename=DB명"; String strUser_id = myUsername; String strPassword = myPassworld; //객체생성 Connection Conn = DriverManager.getConnection(*strUrl*, sttUser_id, strPassworld);

Ⅳ. 결 론

최근 범죄에 사용된 사이트를 대용량화 되고 있어 1개의 서버에 웹서비스, 데이터베이스를 같이 설치, 운영하는 것이 흔하지 않다. 수사기관에서의 지속적인 단속으로 인해 외부로 노출된 웹서비스는 수시로 압수, 차단되고 있지만 다시 도메인 주소 변경 등을 통해 계속해서 사이트를 운영되고 있다. 그리고 사이트 운영자를 검거했을 때에도 구증 자료가 없어 범죄 행위에 대한 기소가 어려울 때가 많다. 이는 근본적으로 회원 정보나 불법 행위를 저장하고 있는 데이터베이스 서버의 압수를 통한 차단 조치와 증거자료 확보가 미진하기 때문이다. 또한 데이터베이스 자료에 대한 분석을 통해 제출되는 증거자료가 없다면 피의자가 법정에서 부인할시 범죄 행위를 구증하는데 어려움이 있었을 것이다.

이 논문에서 데이터베이스 압수를 중심으로 제시한 압수수색영장 신청 및 집행 방법이 추후 수사기관의 불법 사이트 사건에 활용되길 바란다.

참 고 문 헌

[1] 형사소송법, '영장의 방식' 제114조

[2] Microsoft, "Registry Entries for ODBC Components", MSDN, http://msdn.microsoft.com/en-us/library/ms714818(v=VS.85).aspx

[3] IANA, "Port Numbers", http://www.iana.org/assignments/port-numbers

[4] Microsoft, "ODBC 연결", MSDN, http://msdn.microsoft.com/ko-kr/library/79hh5st2.aspx

[5] Microsoft, "Active Server Pages에서 SQL Server에 액세스하는 방법", MSDN, http://support.microsoft.com/kb/169377/ko

[6] PHP MySQL Tutorial, http://www.php-mysql-tutorial.com/wikis/mysql-tutorials/connect-to-mysql-database.aspx

[7] Microsoft, "JDBC 드라이버로 SQL Server에 연결", MSDN, http://msdn.microsoft.com/ko-kr/library/ms378956(v=SQL.90).aspx

著者紹介

김 진 환(Jin-Hwan Kim)

2000년 2월: 한밭대학교 전자계산학과 학사
2000년 2월~2004년 1월: KCNTech, 한국정보공학 시스템 프로그램 개발
2004년 6월~현재: 경찰청 사이버테러대응센터 수사팀
2009년 3월~현재: 고려대학교 정보경영공학전문대학원 정보보호 석사과정
<관심분야> 사이버 범죄, 디지털 포렌식, 정보보호

장 기 식(Ki-Sik Chang)

1995년 2월 경희대학교 수학과 졸업
1997년 8월 경희대학교 일반대학원 수학과 석사(대수학 전공)
2005년 2월 고려대학교 정보보호대학원 정보보호학과 박사(정보보호 전공)
2006년 2월 ~ 현재 경찰청 사이버테러대응센터(디지털증거분석센터)
<관심분야> 디지털 포렌식, 정보보호, 암호학, 스테가노그래피

이 상 진(Sang-Jin Lee)

1987년 2월: 고려대학교 학사 졸업
1989년 2월: 고려대학교 석사 졸업
1994년 8월: 고려대학교 박사 졸업
1989년 10월~1999년 2월: ETRI 연구원 역임
1999년 10월~현재: 고려대학교 정교수
1997년 12월: 국가안전기획부장 표창
<관심분야> 디지털 포렌식, 모바일 포렌식, 심층 암호, 해쉬 함수