Mobile Forensic

January 15, 2009

이경식(rapfer@gmail.com)

목 차

표 목 차

그 림 목 차

I. QPST

1. QPST(Qualcomm Product Support Tool)란?

QPST(Qualcomm Product Support Tool)란 Qualcomm 에서 생산하는 MSM(Mobile Station Modem)을 채용한 임베디드 기기에 대한 NAND Flash Memory 영역을 연결해주는 프로그램을 말한다. 이 프로그램은 본래 리버스 코드엔지니어링을 통한 크랙으로 사업자에게 피해를 줄 수 있고, 일반인이 접근 시에는 해당 기기를 고장 낼 위험이 크기 때문에 일반인에게는 공개를 하지 않는다. 한 때(2005~2006 년경)에 QPST 2.7 버전이 유출됨으로 인해, 많은 국내 사용자들이 불법으로 유료게임을 Cellurar Phone 에 넣는 등 휴대폰사업자에게 손해를 끼치는 문제가 발생하기도 하였다.

2. QPST 의 Forensic 분야에서의 연관성

이 툴이 물론 불법적인 용도로 많이 사용되지만, 실제로 보안분야에서는 상당히 유용한 여러 가지 요소를 가지고 있다.
휴대폰의 경우엔 문자정보부터 시작해서 다양한 정보를 내부 Flash 메모리를 통해 저장을 실시한다. 즉, Forensic 분야의 경우엔 범죄수사 시, 해당 Flash 메모리의 데이터를 이용하여 다양한 용의자의 정보를 얻을 수 있다는 것이다.

II. QPST 사용

1. 필요한 도구

우선 QPST 를 사용하기 위해서는 다음과 같은 요소가 필요하다.

1. 휴대폰(이하 단말기)와 QPST 를 설치한 시스템간에 연결을 위한 드라이버
2. QPST 가 설치된 시스템
3. 연결을 위한 케이블

필자의 경우엔 Windows XP SP3, QPST 2.7 b301, QPST Enabler, LG_CYON_SD370 Model 을 이용해 실습해 보도록 하겠다.

2. 연결 설정

QPST 를 연결하기 위해서는 휴대폰 드라이버를 설치한 상태에서 휴대폰과 PC 가 연결된 Port 가 어떤 건지를 알아둬야 한다. 이는 Windows XP 상에서 Device Manager(devmgmt.msc)를 통해 확인할 수 있다.

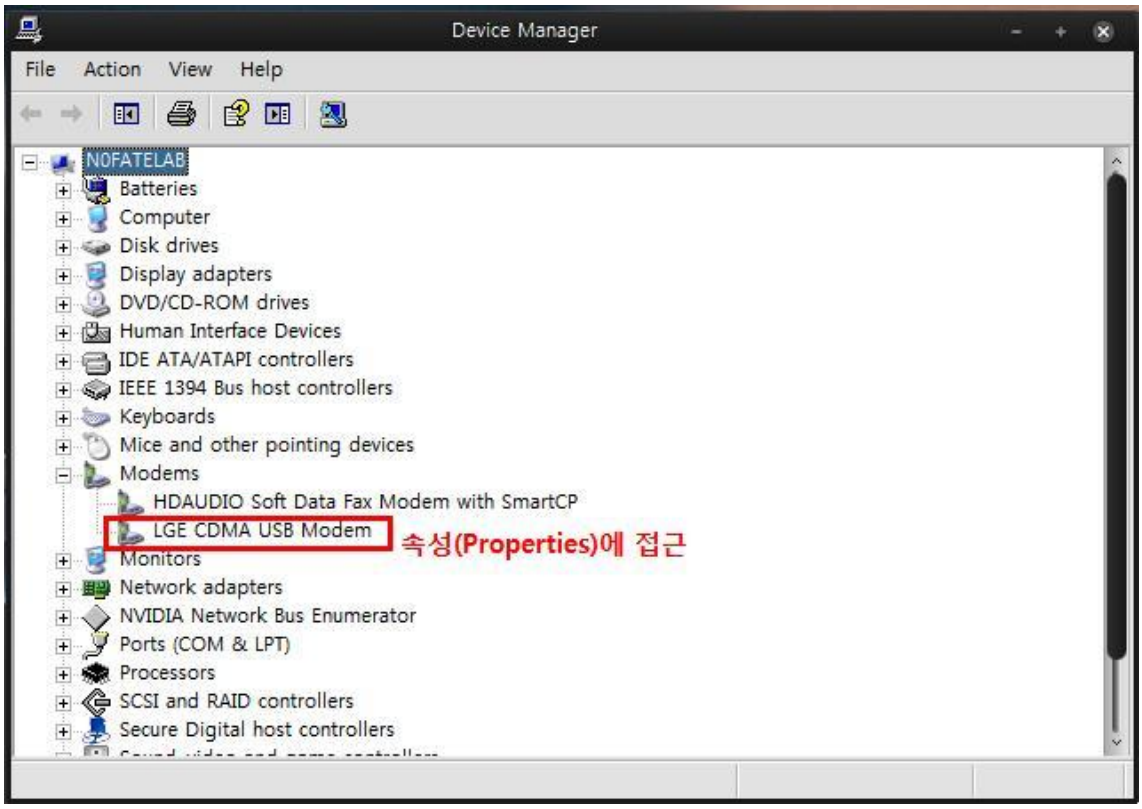


그림 1 - Device Manager

위와 같이 해당 제조사명을 가진 모뎀드라이버의 속성에 접근해 Modem 탭에 접근하면 Port 정보를 알 수 있다.

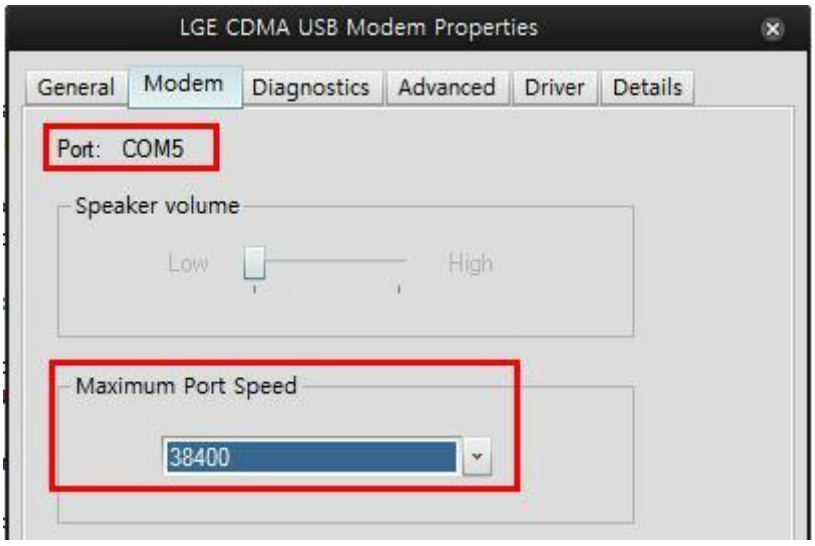


그림 2 - COM Port 정보 확인

위와 같이 COM5 를 사용한다는 정보를 얻을 수 있다. 여기서 Maximum Port Speed 는 38400 으로 설정해 준다. QPST 가 38400 의 속도로 설정하는 것을 권장하기 때문이다. 물론 기본설정으로 돌려도 돌아가는데 지장은 없다. 그럼 이제 QPST 와 연결을 시작해보자.
우선, QPST Configuration 을 실행하고 Ports Tab 에서 Add New Port 를 눌러보면 위에서 확인한 포트가 다른 것을 볼 수 있다.[1]

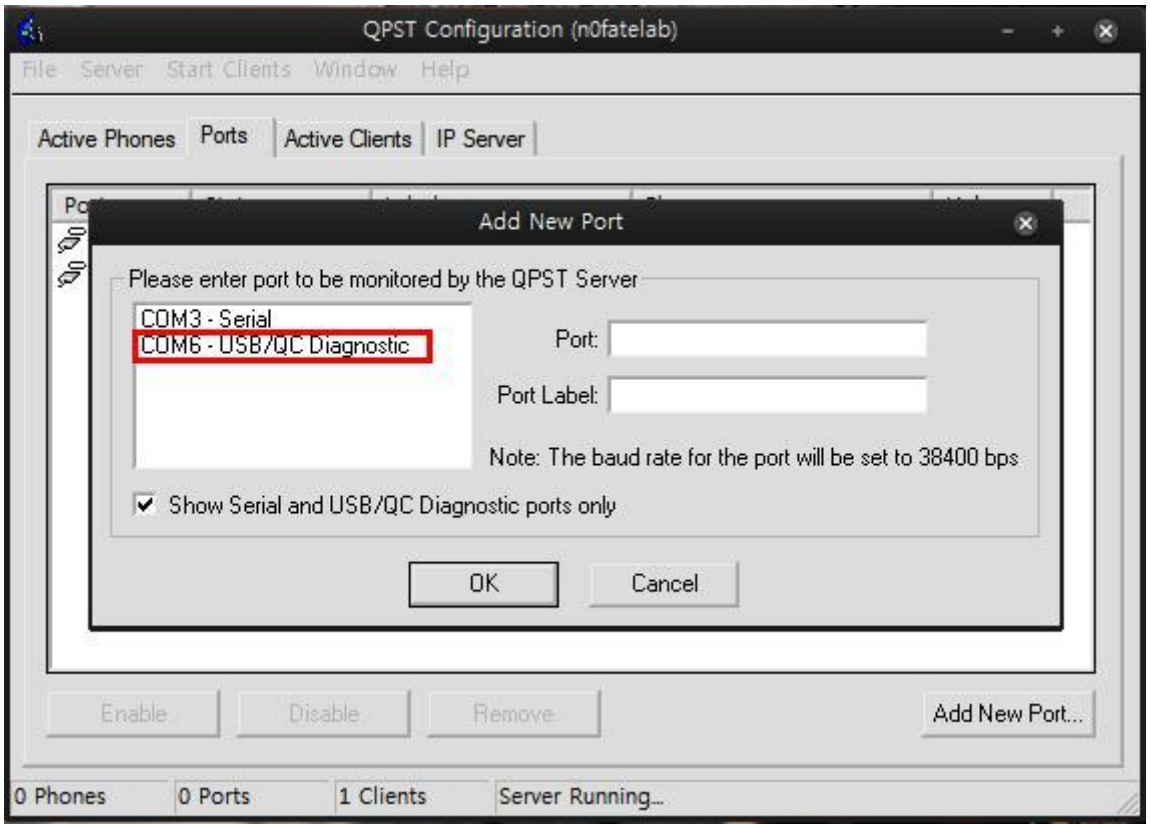


그림 3 - QPST Configuration

여기서 포트가 다른 이유는 Windows 장치관리자에서 보여주는 포트는 USB/QC Data Modem 의 COM 포트 정보이기 때문이다. 실제적으로 QPST 는 Diagnostic Port 를 사용하여 통신을 수행한다. 일반적으로 이 번호는 Data Modem Port 번호의 +-1 의 값을 가지고 있다. 해당 포트를 추가해주고, Active Phones 탭에서 정상적으로 뜨면 올바르게 작동하는 것이다.

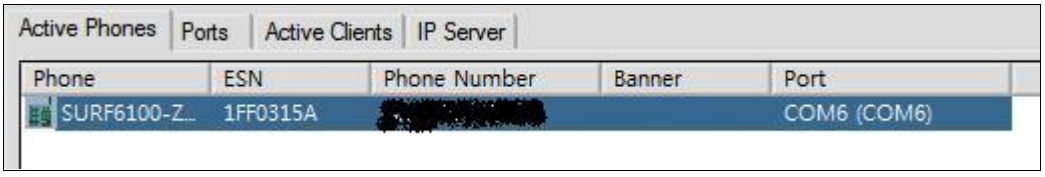


그림 4 - Phone이 정상적으로 연결된 화면

[1] 만약 연결이 에러가 발생한다거나, 뒤에 나올 EFS Explorer구동 시 Partition정보를 얻지 못한다면, QPST Enabler를 통하여 해결하여야 한다. 만약 해결되지 않는다면, 2.7버전에서는 접근할 수 없다.

3. 실습

이제 Start Clients 에서 EFS Explorer 로 해당 단말기의 내부를 들여다 보도록 하자.

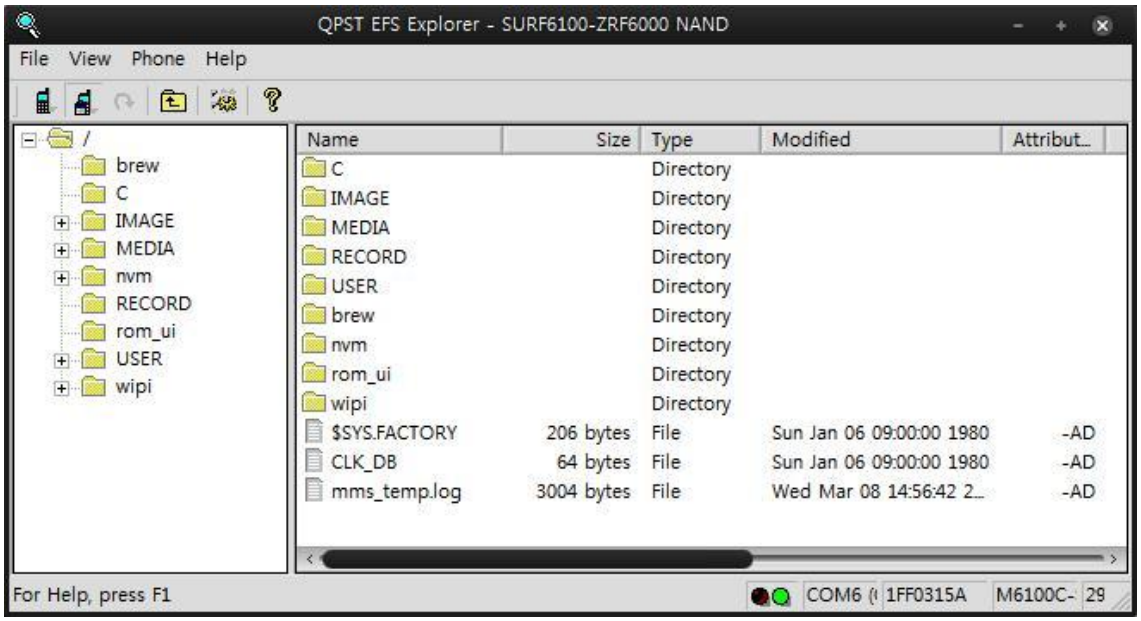


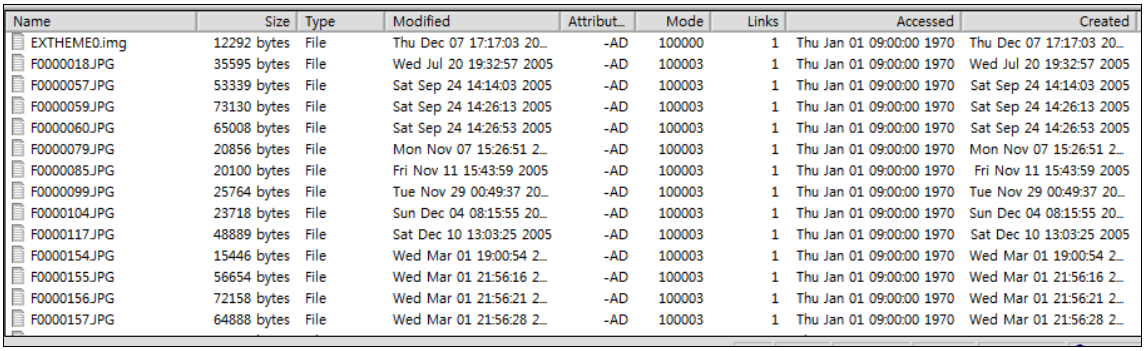
그림 5 - QPST EFS Explorer 구동화면

내부화면은 위와 같다. 이 탐색기를 활용하면, 낸드에 있는 파일을 가져오는 것부터 파일 수정일자까지 확인할 수 있다. 트리의 내용은 다음과 같음을 유추해볼 수 있겠다.

표 1 - Folder Information

Folder name	Comment(*.dat, *.bar)
C	Calculator, Memo, PhoneBook 과 같은 휴대폰 Application(*.pxo)
brew	Mediaplayer 와 같은 BREW Application
IMAGE	Menu 와 같은 곳에 사용되는 이미지파일들을 저장(*.paf)
MEDIA	배경화면, 벨소리 같은 파일들을 저장(*.mmf)
nvm	확인 안됨.
RECORD	SMS, 주소내역, 통화내역, 그룹정보 등의 사용자 정보를 담음(*.dat, *.hd0)
Rom_ui	음악플레이어, 메뉴에 사용되는 TEXT 문자 등의 정보를 가짐(file3)
USER	MP3, 사진파일을 저장
Wipi	WIPI Application 저장

위와 같은 요소들을 가지고 있다. 여기서 주목해야 할 폴더는 RECORD 폴더이다. USER 폴더이다. 이 두 가지 요소는 본래 휴대폰의 정보가 아닌, 사용자가 생성한 정보이기 때문에 매우 가치가 높다고 할 수 있겠다. 예로 USER-PHOTO 폴더에 접근하여 보겠다.



Name	Size	Type	Modified	Attribut...	Mode	Links	Accessed	Created
EXTHEME0.img	12292 bytes	File	Thu Dec 07 17:17:03 20...	-AD	100000	1	Thu Jan 01 09:00:00 1970	Thu Dec 07 17:17:03 20...
F0000018.JPG	35595 bytes	File	Wed Jul 20 19:32:57 2005	-AD	100003	1	Thu Jan 01 09:00:00 1970	Wed Jul 20 19:32:57 2005
F0000057.JPG	53339 bytes	File	Sat Sep 24 14:14:03 2005	-AD	100003	1	Thu Jan 01 09:00:00 1970	Sat Sep 24 14:14:03 2005
F0000059.JPG	73130 bytes	File	Sat Sep 24 14:26:13 2005	-AD	100003	1	Thu Jan 01 09:00:00 1970	Sat Sep 24 14:26:13 2005
F0000060.JPG	65008 bytes	File	Sat Sep 24 14:26:53 2005	-AD	100003	1	Thu Jan 01 09:00:00 1970	Sat Sep 24 14:26:53 2005
F0000079.JPG	20856 bytes	File	Mon Nov 07 15:26:51 2...	-AD	100003	1	Thu Jan 01 09:00:00 1970	Mon Nov 07 15:26:51 2...
F0000085.JPG	20100 bytes	File	Fri Nov 11 15:43:59 2005	-AD	100003	1	Thu Jan 01 09:00:00 1970	Fri Nov 11 15:43:59 2005
F0000099.JPG	25764 bytes	File	Tue Nov 29 00:49:37 20...	-AD	100003	1	Thu Jan 01 09:00:00 1970	Tue Nov 29 00:49:37 20...
F0000104.JPG	23718 bytes	File	Sun Dec 04 08:15:55 20...	-AD	100003	1	Thu Jan 01 09:00:00 1970	Sun Dec 04 08:15:55 20...
F0000117.JPG	48889 bytes	File	Sat Dec 10 13:03:25 2005	-AD	100003	1	Thu Jan 01 09:00:00 1970	Sat Dec 10 13:03:25 2005
F0000154.JPG	15446 bytes	File	Wed Mar 01 19:00:54 2...	-AD	100003	1	Thu Jan 01 09:00:00 1970	Wed Mar 01 19:00:54 2...
F0000155.JPG	56654 bytes	File	Wed Mar 01 21:56:16 2...	-AD	100003	1	Thu Jan 01 09:00:00 1970	Wed Mar 01 21:56:16 2...
F0000156.JPG	72158 bytes	File	Wed Mar 01 21:56:21 2...	-AD	100003	1	Thu Jan 01 09:00:00 1970	Wed Mar 01 21:56:21 2...
F0000157.JPG	64888 bytes	File	Wed Mar 01 21:56:28 2...	-AD	100003	1	Thu Jan 01 09:00:00 1970	Wed Mar 01 21:56:28 2...

그림 6 - PHOTO Folder

위와 같이 여러 사진들과 촬영한 날짜, 접근한 날짜, 수정한 날짜를 확인할 수 있다. 이제 RECORD 폴더를 접근해보자.

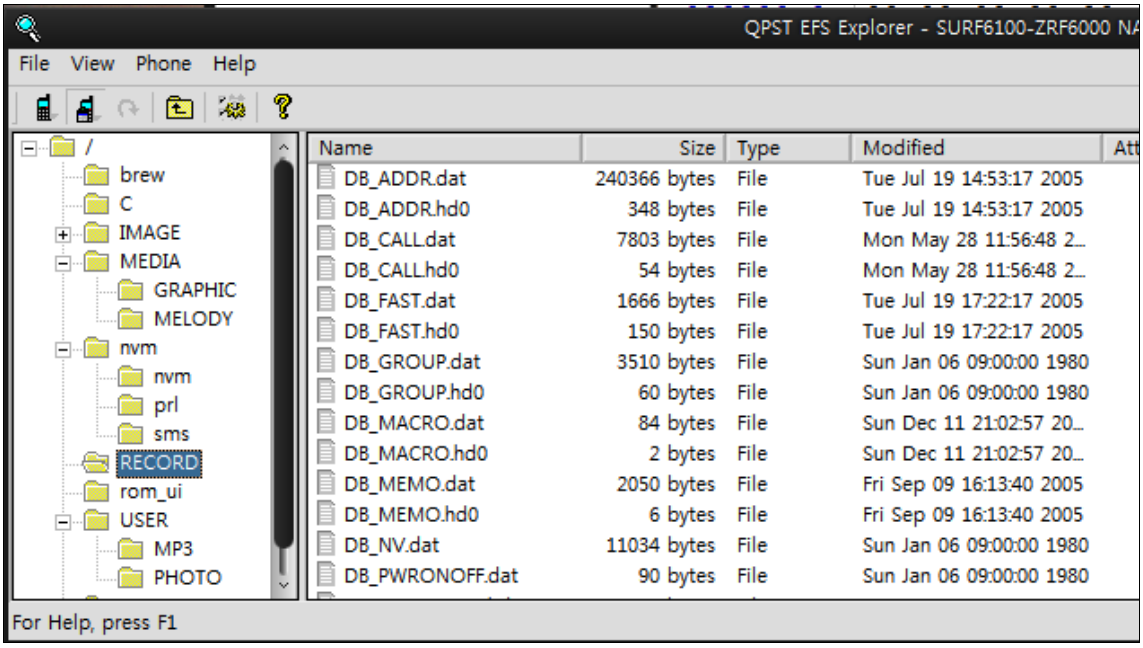


그림 7 - RECORD Folder

RECORD 폴더에도 위에 설명한 것과 같이 사용자에게 중요한 정보를 확인할 수 있다. 모든 data file 은 *.dat, *.hd0 두 개의 파일로 구성되어 있다. 이 중에서 DB_ADDR(사용자 연락처 정보로 추정)되는 것을 다운로드 받아 Hexa Editor[2]로 구동해 보도록 하겠다.

[2] WinHex, UltraEdit

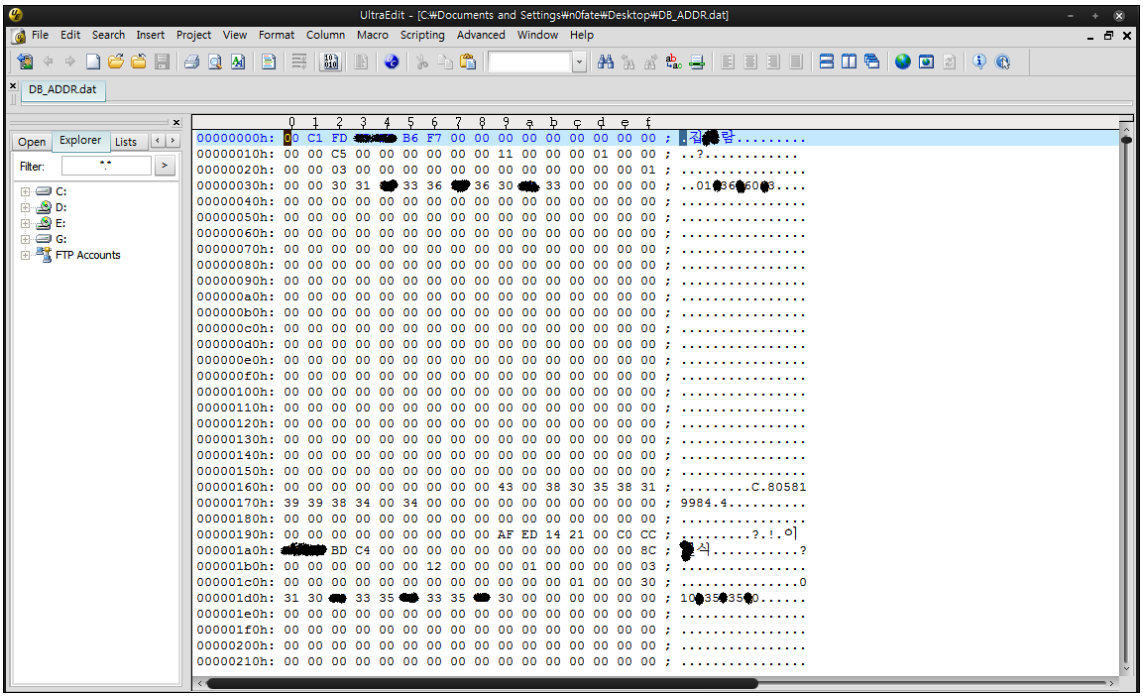


그림 8 - Hexa Editor

이 파일을 보면 순차적으로 저장하는 흔적을 확인할 수 있다. (실제로 부친이 사용했던 휴대폰이며, 실제로도 위와 같은 저장순서를 따랐다.) 여기에서 흥미로운 건 아래의 "집*람"내역이다.

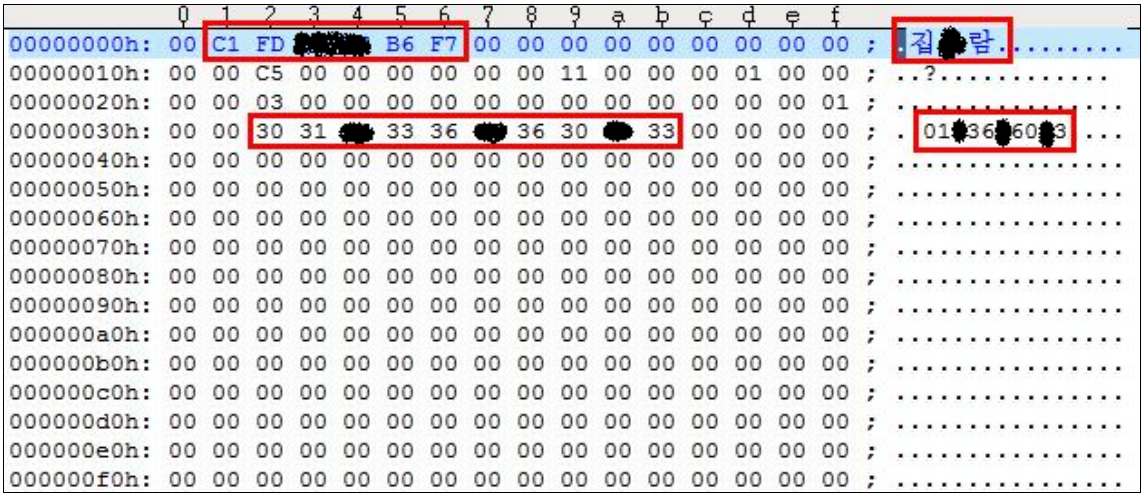


그림 9 - 실제론 삭제하였으나 남아있는 번호내역

위 내용은 실제 휴대폰에는 저장 되어있지 않은 정보이다. 즉, 정해놓은 메모리의 한계치까지 파일사이즈를 늘리면서 번호내역을 추가만하고, 삭제된 번호정보는 UI 상에서는 존재하지 않지만, 파일상에는 그대로 두는 것을 확인할 수 있다.

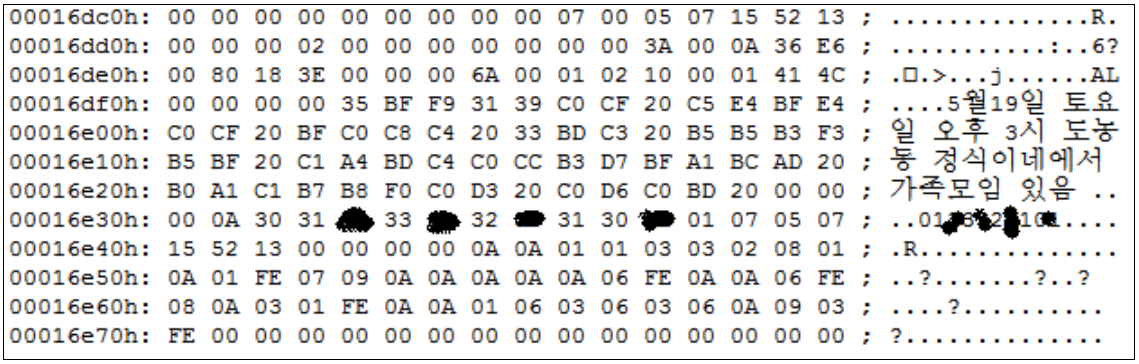


그림 10 - 삭제한 문자가 보관 되어 있는 화면

III. 최종결론

1. 결론

본문의 내용에서와 같이 휴대폰 NAND Flash Memory 상의 데이터는 충분히 Forensic 기술에 이용될 수 있다. 만약, 사용자가 전화번호부, SMS, 통화내역 등을 삭제하는 경우에도, 위의 예제와 같이 파일에는 저장되기 때문에 각각의 필드가 무엇을 의미하는지의 정보를 알아내면 Parsing 하여 결과를 쉽게 산출해 낼 수도 있을 것이다. 이 경험은 Mobile Forensic 이라는 분야가 수사상황에 충분한 도움을 가져다 줄 것이라는 걸 예상해 볼 수 있는 좋은 경험이 된 것 같다.