논문 2013-2-6

정보기기 하드웨어 감정에서 디지털 포렌식

이규대*

Digital Forensics on the Handheld Devices

Kyu-Tae Lee*

요 약

디지털 포렌식은 정보장비에서 디지털 자료의 변형관계를 정보체계적으로 분석 규명함으로써 법적 증거의 가치를 갖도록 스마트폰 및 휴대폰, PDA, PC, 서버 등에서 데이터를 수집 분석하는 디지털 정보검출을 의미한다. 디지털정보는 파일형태로 가공 배포되는 특징으로, 간단한 조작으로 생성, 복제, 변경, 삭제, 전송 및 원격지에서의 변형이 가능하다. 따라서 변형된 정보가 법적인 증거효력을 갖게 하기 위해서는 전문성이 적용된 절차와 방법이 필요하다. 정보기기 하드웨어는 프로세서 기반으로 제작되고 운영되는 특징이 있어 프로세서의 하드웨어 구성, PCB 배치, 프로그램의 파일구조 등에 있어 설계자의 고유한 습성이 포함되는 경향이 있다. 본 연구에서는 정보기기 하드웨어를 복제 및 도용시 해당기기의 제작과정을 단계적으로 추적하여, 의도적인 도용의 증거가 되는 특징을 검출하는 방법 및 증거로 활용성이 있는 포렌식정보를 활용하는 가능성을 제시한다.

Abstract

To trace and verify an illegal usage of IT technology, digital forensics are known as an usefull approach. The digital forensics is a procedure of criminal investigation for assure of legal ability by scientific analysis in electronic equipment. smart phone is the one of the best mobile IT devices. Evidence in digital form is the way of doing to create, reproduce, modify, remove, transport Thus, specific procedures and methods are required to achieve legal evidences. A hardware device has special processor and interface modules for it's own function under designers characteristics. An application program has it's own useful program utility and file structures. On forensics, it should be evaluated on the hardware and source code. This paper shows how to make forensics evidence on the hardware devices as it comes illegal property in ownership.

키워드 : 하드웨어 감정, 정보기기, 회로설계 포렌식, 파일구조 포렌식

1. 서 론

IT 최근 정보기기 증거 확보방법으로 사용되고 있는 디지털 포렌식은 디지털 기기의 메모리, 디스크 등을 분석하여 범행 행각이나 증거, 기록 등을 분석해 내는 행위를 말한다. 현대의 정보화 사회는 생활의 많은 부분에 디지털기기가 설치 운영되고 있으며, 이 기기에 사용자, 사용시

* 공주대학교 정보통신공학부
(email: ktlee@kongju.ac.kr)
접수일자: 2013.12.02 수정완료: 2013.12.20

간, 작업내용, 이동상황 등 모든 내용들이 기록되도록 운영되고 있기 때문에 유사시에 이를 활용한 추적이 가능한 환경을 제공한다. 거리에 설치된 CCTV, 대중교통내 CCTV, 대중교통 승차시 교통카드 TAG, 회사 출입할 때 현관 CCTV, SNS, 휴대폰 문자메시지, 메신져 등 모든 행위가 서버에 또는 개별 단말기에 기록되고 있다.

디지털 포렌식 기술은 이러한 저장된 정보를 활용하여 범죄 예방, 검거에 도움을 주기위한 기술이다.[1]

최근 새로운 기능의 IT 정보기기가 개발되면서, 활용도가 높은 정보기기의 경우 이를 무단 동요하거나, 개발자의 일부가 이직하여 유사한 기기를 생산 판매함으로써 원 저작권자의 지적재산권을 침해하는 경우가 발생되고 있다.

이런 유형의 분쟁시 유사기기의 소프트웨어와 하드웨어를 비교 감정을 수행하게 되는데, 소프트웨어는 기능이나 소스코드의 유사성을 판단하여 도용여부를 판단한다. 하드웨어의 경우 많은 부분이 공지된 회로나 부품을 사용하는 경우가 많아, 도용의 여부를 판단하는데 어려움이 있어 왔다.

본 연구에서는 하드웨어 감정시 유사한 부품과 회로를 사용하여 구현한 경우, 디지털포렌식 방법으로 원저작권자의 저작권을 판단하는 근거로 사용될 수 있는 부분을 제시하였다.

2. 정보기기 하드웨어

정보기기의 핵심인 프로세서는 초기의 8bit/16bit 컨트롤러에 제한된 동작을 하도록 하는 소프트웨어가 탑재된 시스템이었으나 이후 고성능 마이크로프로세서와 Digital Signal Processing (DSP) 칩의 등장으로 사용영역이 넓어지고 그에 따른 소프트웨어도 발달하게 되었다.

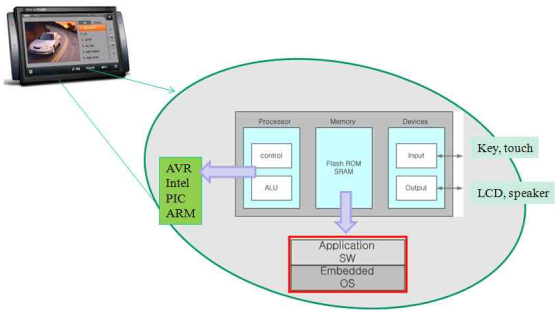


그림 1. 정보기기 시스템 구조

2.1 시스템구성요소

(1) 마이크로프로세서

마이크로프로세서는 버스 동작을 제어하고, 계산을 실행하며 결정을 한다. 마이크로프로세서는 프로그램이 가능하며, 시퀀스 명령에 의해 제어된다. 명령은 데이터 전송명령, 산술과 논리 명령, 프로그램 제어 명령 등의 3가지 형태를 갖는다. 이때 소스코드로 작성된 마이크로프로세서 명령 시퀀스를 프로그램 또는 소프트웨어라고 부른다.

(2) 메모리

기억장치로 사용되는 메모리는 마이크로프로세서의 프로그램과 데이터를 저장하기 위한 것으로 시스템에 적용되는 여러 가지 형식의 메모리 디바이스가 있으며 버스 시스템에 접속한 메모리를 메인 메모리라고 부른다. 메모리의 종류에는 사용의 유용성에 따라 RAM, ROM, EPROM, FlashROM등이 있다.

(3) I/O 장치

I/O 장치는 마이크로컴퓨터와 외부와의 인터페이스를 제공하는 LCD display, 키패드, 터치스

크린 등의 기능을 포함한다. 최근 새롭게 개발되는 정보기기는 새로운 I/O 모듈의 개발에 따라, 휴먼 인터페이스기능과 네트워크나 머신 인터페이스가 부가되면서 발전하고 있다.

(4) 소프트웨어

정보기기 시스템은 일반적인 시스템과는 달리 특정한 작업만을 하도록 설계되며 초기의 임베디드 시스템은 운영체제가 필요 없이 사람이 순차적인 프로그램을 작성해서 실행하고 중간에 인터럽트가 발생되는 경우에 서비스 프로그램을 수행하고 돌아오는 구조로 동작한다. 이전의 시스템들은 주로 간단하고 단순한 순차적인 작업에 관련되었기 때문에 OS의 필요성이 없었으나 최근의 시스템 개발 분야에서는 기능이 많아지고, 네트워크나 멀티미디어가 요구되면서 시스템이 해야 할 일들도 많아지고 복잡해 졌기 때문에 순차적인 프로그램 작성이 매우 어렵게 되었다. 따라서 시스템에서도 운영체제의 개념이 필요하게 되었고 실시간이라는 요소를 만족해야 했으므로 실시간 운영체제가 정보기기 시스템에 도입되었던 것이다. 지금도 실시간 OS를 채택하여 개발된 제품들이 점점 늘어나고 있다. 이제는 많은 시스템에서 그 목적에 맞게 실시간 운영체제를 적절하게 사용하고 있다.

최근의 IT 기술은 마이크로프로세서의 가격이 낮아지고 소형화 및 고성능화가 진행됨에 따라 제품 경쟁력의 핵심이 H/W 생산 기술에서 S/W 최적화 기술로 이동하는 추세로 임베디드 S/W가 탑재된 기기의 가치가 H/W보다는 S/W에 의해 좌우되는 방향으로 발전하고 있다. 초창기 S/W는 간단한 제어 프로그램만으로 산업용 기기를 제어하는데 그쳤으나, 최근에는 멀티미디어 처리와 같은 점차 복잡한 기능을 위해 멀티태스크 및 네트워크기능을 제공하는 실시간 OS를 이용하고 있다.

(5) 프로그램의 특징

- 실시간 처리 지원: 입력장치의 신호 및 내부 처리결과를 바로 출력
- 고신뢰성: 다양한 환경에서 안정된 동작
- 최적화 기술 지원: 임베디드 시스템은 크기, 가격 및 발열 등을 이유로 제한된 H/W 자원으로 구성되기 때문에 임베디드 S/W는 경량화, 저전력 지원, 자원의 효율적 관리 등의 측면에서 H/W에 최적화되는 기술을 지원해야 한다.
- 특정 시스템 전용: 범용 데스크탑 또는 서버에서 실행되는 패키지 소프트웨어와 달리 특정 시스템의 실행을 목적으로 개발되는 S/W이다.
- 네트워크 및 멀티미디어 처리기능 지원: 임베디드 시스템들이 단독형 시스템뿐만 아니라 유무선 네트워크를 통해 연결될 수 있어야 하고, 멀티미디어 정보를 처리하는 기술이 필요한 디지털 TV, PDA 및 스마트폰 등과 같은 임베디드 시스템을 지원해야 한다.
- 다양한 솔루션과 개발 도구 필요: 다양한 기종과 규격의 마이크로프로세서에 최적화된 별도의 솔루션이 동시에 제공되어야 하며, 임베디드 S/W 애플리케이션을 빠르고 안정되게 개발하기 위해 사용하기 쉬운 개발 도구가 필요하다.

3. 정보기기 포렌식

정보기기를 개발하는 하드웨어 기술자는 요구사항을 만족하는 기능을 구현하기 위해 상업용으로 개발된 다양한 인터페이스 부품을 사용하게 된다. 이때 인터페이스작업을 위한 지원으로 표준회로도를 제공하는 경우가 많다. 따라서 동일한 부품을 사용하는 개발자들은 유사한 프로그램과 회로도를 작성하게 되는 특징이 있다. 그러나 실제 구현에 있어서는 정보기기의 디자인과 사용

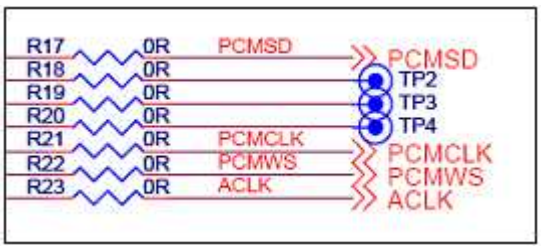
자 취급을 용이하게 하기위해 부품의 배치, PCB 설계등이 개발자 고유의 창작성으로 제작된다.

따라서 유사한 기능의 정보기기의 경우 원 개발자의 고유한 특징을 포렌식 자료로 활용하게 되면, 기존의 유사도 감정의 정확도를 향상할 수 있는 장점이 있다.

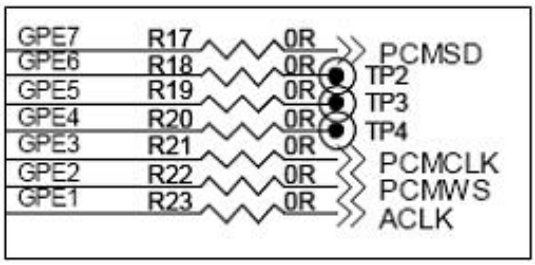
다음은 동일한 기능의 하드웨어 구성 정보기기에서 두 장치의 유사성을 검증시 나타날 수 있는 저작권자의 고유 특징점을 예시한다.

(1) 동일한 포트의 사용예

일반적으로 정보기기용 프로세서에는 사용가능한 포트가 다수 있으며(A,B,C,D,E,F,G) 있으며, 동일한 포트가 사용되는 경우라도, PCMSD, PCMCLK, PCMWS 등이 동일하게 연결된 경우를 보인다.



a) 원본

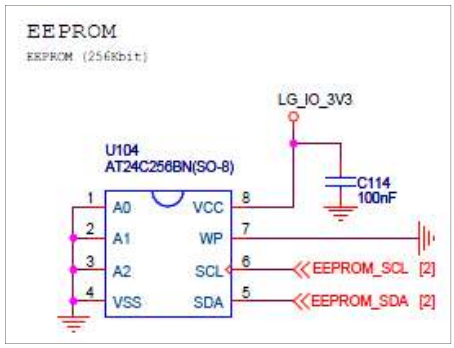


b) 비교본

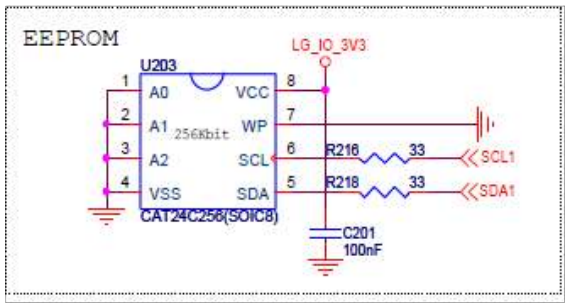
그림 2. 동일포트 사용예

(2) 동일 데이터의 전달방향 사용예

기억장치로 사용되는 직렬 EEPROM 의 경우를 보면 그림과 같다. 유사 부품의 사용과 연결선의 니모닉을 명명하는 과정이 동일한 특성을 보이는 경우 저작자의 원본회로를 도용하는 증거로 활용이 가능한 특징을 보인다.



a) 원본



b) 비교본

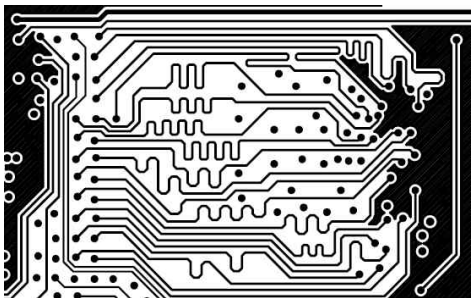
그림 3. 동일 데이터 전달방향 사용예

(3) PCB 패턴의 동일 라우팅 사용예

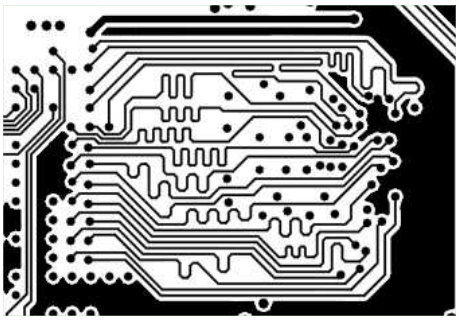
PCB의 설계는 핵심부품의 배치 및 연결선의 이동이 설계자 마다 다르기 때문에 동일성을 갖기 어려운 특징이 있다. 그림과 같이 두 개의 PCB 패턴에서 보면, 두 PCB의 연결점과 연결선

이동과정이 동일한 모습을 보인다. 또한 PCB 기판설계에서 배선연결의 꺾임이나 각도, 연결된 거리 등도 동일한 경우를 보인다.

위의 예에서 나타나듯이 동일하게 보이는 회로와 PCB의 패턴에서 개발자 고유의 포렌식 자료를 검출할 수 있음을 알 수 있다.



a) 원본



b) 비교본

그림 4. 수동소자의 동일 배치 사용예

동일한 기능을 보이는 회로임에도 구현과정에서 동일할 확률이 작은 상황이 재연되는 경우를 분류하여 포렌식 정보로 활용하게 되면, 도용의 의미가 없어 보이는 하드웨어 감정에서 원 개발자의 저작권을 보호하는 방법으로 활용될 수 있다.

4. 결 론

하드웨어의 개발은 인터페이스 부품들이 모듈화 되고 있어서 동일하거나 유사한 부품을 사용하는 경우가 증가하고 있다. 이때 동일한 부품과 회로를 사용하여 구현하더라도 개발자의 아이디어에 따라 다른 PCB 패턴이 만들어지거나, 부품의 배치에 고유의 특이점이 내재되는 특징이있다. 본 연구에서는 이러한 특징점을 포렌식 정보로 활용하는 방법을 제시하였다.

감정의 특이점을 정의함으로써 정보기기 하드웨어의 분쟁시, 회로가 동일하고, 사용된 부품이 동일한 경우도 원 개발자의 저작권이 보호되는 방법으로 활용될 수 있을 것으로 보인다.

참 고 자 료

[1] 정익래, 홍도원, 정교일; 디지털포렌식 기술 및 동향; 전자통신동향분석 제22권; 2007. 2
[2] 홍도원; 디지털 포렌식 기술; 한국전자통신연구원; 2007
[3] 임경수, 박종혁, 이상진; 디지털포렌식 현황과 대응방안; 보안공학연구논문지, 2008. 11
[4] 류희수; 정보보호: 디지털 세상의 CSI, 그 가능성은?, 정보통신진흥협회, 2007
[5] 조용현; 디지털 포렌식을 위한 절차와 도구의 중요성; (주)시큐아이닷컴 CERT팀, 2007
[6] 김도완, 윤영선; SW소스코드 저작권보호를 위한 통합 가이드; 컴퓨터프로그램보호위원회, 2009. 4
[7] 길연희, 홍도원; 디지털 포렌식 기술과 표준화 동향; IT standard & test TTA journal, 2008, 8
[8] 변정수; 한국형 디지털 증거분석 표준화: 경찰청 디지털 증거처리 표준가이드라인 및 증거분석 전문매뉴얼의 고찰; 디지털 포렌식 연구 창간호, 2007. 11
[9] 방효근, 신동명, 정태명; 소프트웨어 포렌식: 프로그램 소스코드 유사성 비교 및 분석을

중심으로; 디지털 포렌식 연구 창간호, 2007. 11
[10] 전상덕, 홍동숙, 한기준; 디지털 포렌식의 기술 동향과 전망; 정보화정책; 2006. 11
[11] 전병태, "프로그램 복제도 감정기법 및 감정비 산출에 관한 연구" 프로그램심의조정위원회 결과보고서 2002.
[12] 이규대, "임베디드시스템의 이진코드 추출 및 분석", 한국소프트웨어감정평가학회 논문지, 5권1호, pp27-38, 2009.5.

저 자 소 개

이 규 대(Kyu-Tae Lee)

1984 고려대 전자공학과 졸업
1986 고려대 전자공학과 석사
1991 고려대 전자공학과 박사
2001 미 죠지아텍 교환 교수
2006 미 일리노이주립대 교환 교수
2007~2009 한국전자통신연구원 이동통신연구소 초빙연구원
'92. 3 ~현재 : 공주대 정보통신공학부 교수
<관심분야> 회로 및 시스템, 신호처리, VLC