# 리눅스 기반 BusyBox 를 사용하는 드론 포렌식 연구

류가연*, 홍득조**
*전북대학교 컴퓨터공학과
**전북대학교 IT 정보공학과
e-mail : gryu720@naver.com

# A Study of Drone Forensics using BusyBox based on Linux

Ga-Yeon Ryu*, Deukjo Hong**
*Dept. of Computer Engineering, Chonbuk University
** Dept. of IT Information Technology, Chonbuk University

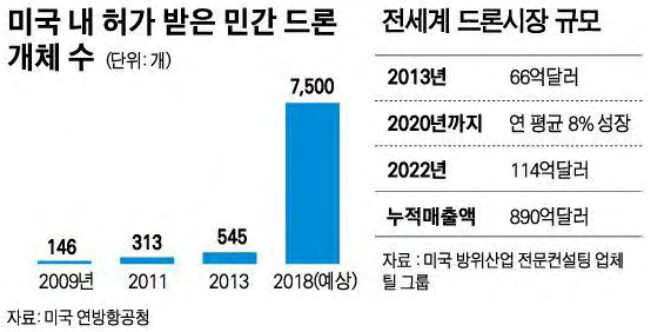
**요 약**

드론 기술이 발전하여 다양한 용도로 활용 가능해지면서 사용 범위와 시장을 더욱 넓혀가고 있다. 또한 사물인터넷(IoT) 시대에 포렌식 적용 대상의 범위가 스마트 워치, 스마트 TV 등 우리 생활에 다양하게 자리잡은 임베디드 시스템으로 확대되고 있다. 본 논문에서는 리눅스 포렌식 아티팩트 분석 기법을 이용하여 Busybox 를 사용하는 드론에 대해 중요 데이터 증거를 수집하는 방법을 제시한다.

## 1. 서론

디지털 포렌식은 사건을 조사하거나 사고의 원인을 파악하기 위해서 각종 기기에 저장되어 있는 디지털 데이터의 생성 원인과 의미를 분석하는 분야이다. 대부분의 정보가 디지털 데이터로 기록되면서 디지털 포렌식의 중요성에 대한 인식이 높아지고 있으며, 사물인터넷(IoT) 시대가 도래하면서 디지털 포렌식 적용 대상의 범위가 가정용 셋탑박스, 스마트 TV, 전자게임기 등으로 빠르게 확장되고 있다[1].

최근 각광받고 있는 무인 항공기 시스템 드론은 군사적 용도로 시작하였으나 감시, 연구개발, 촬영, 범죄수사, 물류 사업 등 다양한 용도로 활용 가능해지면서 사용 범위와 시장을 더욱 넓혀가고 있다. 민간 드론의 개체수가 빠르게 증가함에도 불구하고 안전성 문제가 상용화의 가장 큰 걸림돌이다[2]. 특히, 개인이 사용할 경우 안전사고 발생 위험이 매우 높다. 그렇기 때문에 안전사고 발생 시 책임 소재를 확실히 할 수 있는 제도적 장치가 필요하므로 개인용 드론은 충분히 디지털 포렌식의 적용 대상이 될 수 있다[3].




(그림 1) 미국 내 허가 받은 민간 드론 개체 수

본 논문에서는 드론의 파일 시스템 구조를 분석하고 리눅스 포렌식을 통해 얻을 수 있는 드론의 아티팩트를 정리한다. 이를 위해 리눅스 기반 BusyBox 가 제공하는 드론의 파일 시스템 구조를 분석하고 드론 포렌식을 통해 유효한 증거를 가진 데이터를 수집한다. 또한 드론에 외부 저장 장치 장착 여부에 따라 분석 시나리오를 두 가지로 분류한다.

본 논문의 구성은 다음과 같다. 2 절에서는 드론 분석을 위한 리눅스 포렌식 분석과 BusyBox 등의 관련 기술이 설명되고 3 절에서는 2 절의 리눅스 포렌식 아티팩트 일부의 수집 방법을 적용한 드론 내부에 존재하는 유효한 포렌식 증거의 종류와 수집 방법이 설명된다. 4 절에서는 결론과 함께 향후 연구 계획이 제시된다.

## 2. 관련 기술

### 2.1. AR.Drone 2.0

연구는 세계 무인항공기 매출 2 위인 프랑스 Parrot 사의 AR. Drone 2.0 Elite Edition 으로 진행되었다[4]. 이 드론은 Arm Cortex A8 기반의 Architecture 를 기반으로 동작되는 임베디드 시스템으로 Linux 2.6.32 의 플랫폼을 가지며, 콘솔에서 커널의 Operate Command 를 동작하기 위해 BusyBox 를 이용하여 텔넷 Service 를 제공하고 있다[5]. Wi-Fi 로 스마트폰과 연결하여 조종하며, HD 1280x720 카메라가 부착되어 비행 중에 사진, 동영상 촬영이 가능하다. USB 플래시 드라이브를 추가로 부착하여 비행 중 동영상을 저장할 수 있다.

(그림 2) Parrot 사의 AR.Drone 2.0

### 2.2. BusyBox

BusyBox [6]는 크기 최적화와 제한된 리소스를 염두에두고 작성된 유닉스 유틸리티와 명령어의 압축 파일이다. 제한된 자원을 가진 임베디드 시스템을 위한 완벽한 환경을 제공한다. BusyBox 의 유틸리티는 일반적으로 완전한 기능을 갖춘 GNU 보다 적은 옵션을 가지고 있으나 포함 된 옵션의 함수는 최소 사이즈로 다시 구현되었으며 GNU 와 매우 유사하게 동작한다.

BusyBox 는 매우 모듈화 되어 있기 때문에 컴파일 시 명령을 쉽게 포함하거나 제외 할 수 있다. 임베디드 시스템을 쉽게 사용자 정의 할 수 있다는 장점이 있으며 작동중인 시스템을 만들기 위해서는 /dev 에 장치 노드를 몇 개 추가하고 /etc 에 몇 가지 구성 파일을 추가하고 Linux 커널을 추가한다.

### 2.3. 리눅스 포렌식 수집 정보

리눅스 기반의 드론 구조를 이해하기 위해 리눅스 시스템의 포렌식 수집 정보를 정리한다. 활성시스템 상태에서 얻을 수 있는 정보는 매우 다양하지만 AR. Drone 의 BusyBox 에서 수집 가능한 아티팩트만 조사한다[7].

**<표 1> 리눅스 포렌식 시 수집 대상이 되는 주요 시스템 정보의 위치 및 수집 방법**

| 정보 | 수집 방법 |
|---|---|
| 시스템 명 | /etc/os-release 에서 추출<br>/proc/version<br>uname -a |
| 시스템 시간 | time()함수를 이용하여 time_t 수집 |
| 메모리 용량 | /proc/meminfo 에서 추출 |
| 메모리 상태 | /proc/iomem<br>/proc/vmstat |
| 시스템 구동시간 | uptime<br>/proc/uptime |
| 프로세스 상태 | ps -elf |
| 시스템 사용자 | /etc/passwd uid 수집 |

## 3. 드론 아티팩트 수집

활성시스템 상태에서 드론을 발견했다는 가정하에 드론에서 얻을 수 있는 데이터를 조사한다.
드론과 연결된 PC 의 OS 는 Ubuntu 16.04 LTS 를 사용한다. 텔넷 서비스를 통해 드론과 Wi-Fi 연결 후 루트 디렉토리 내부를 볼 수 있고 ftp 는 /root/data 정보만 제공한다.

### 3.1. 드론의 디렉터리 구조

BusyBox 에서 제공하는 명령어와 유틸리티를 사용하는 드론은 기존 리눅스에 비해 적은 옵션을 갖는다. 메모리 용량이 매우 작아 /data/video/ 비행 기록을 2 개 이상 가지고 있지 않고 매번 덮어 씌우므로 얻을 수 있는 정보가 제한적이다.

```
bin     etc     home    mnt     sbin
data    factory lib     proc    sys
dev     firmware licenses root  tmp
```

(그림 3) 드론 root(/) 디렉터리 구조

**<표 2> 드론에서 수집할 수 있는 주요 시스템 정보의 위치 및 수집 방법**

| 정보 | 수집 방법 | 수집 정보 |
|---|---|---|
| 시스템 명 | /proc/version<br>uname -a | Linux version 2.6.32.9 |
| 시스템 시간 | date | 포렌식 당시 드론 시스템 시간정보 |
| 메모리 용량 | /proc/meminfo | 메모리 정보 |
| 메모리 상태 | /proc/iomem<br>/proc/vmstat | 메모리 상태 |
| 시스템 구동시간 | uptime<br>/proc/uptime | 드론 전원이 켜진 상태의 시간 |
| 프로세스 상태 | top | 실시간 프로세스 |

### 3.2. 외부 저장 장치 없이 드론 비행 시

드론이 촬영한 영상, 사진의 정보는 기본적으로 Parrot 사에서 AR.Drone 을 구동을 위해 제공하는 애플리케이션을 통해 획득할 수 있다. 그러나 스마트폰 갤러리에서 해당 데이터가 삭제된다면 모바일 포렌식을 통해 복구해야 한다.

텔넷서비스를 이용하여 드론 내부에 접속하면 /data/video/boxes 에 비행 기록이 남는다. 기본적으로 메모리 용량이 작아 이전의 비행기록은 알 수 없으나 가장 최근 비행 날짜 및 시간을 파일명으로 제공하므로 드론을 사용한 시간정보를 획득할 수 있다.

```
# cd boxes/
# ls
flight_20170315_161807
# cd flight_20170315_161807/
# pwd
/data/video/boxes/flight_20170315_161807
```

(그림 4) 드론 내부에 존재하는 비행 기록

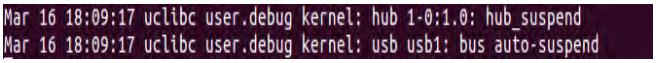
### 3.3. 외부 저장 장치 장착 후 드론 비행 시

USB 플래시 드라이브나 Parrot 사에서 제공하는 GPS 레코더를 장착하면 /data/video 하위 디렉터리로 usb# 폴더가 생성되며 디렉터리 내부에 비행 중 촬영

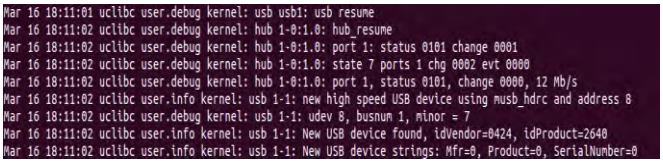
한 동영상을 mp4 파일 형식으로 저장한다. 날짜 및 시간 정보를 획득할 수 있다. GPS 레코더에서 GPS 위치 정보를 수신하므로 촬영된 사진 및 영상에 GPS 위치정보가 자동으로 포함된다.


(그림 5) GPS 레코더 내부 데이터

이처럼 외부 저장 장치를 연결한 후 드론을 사용했을 때에는 스마트폰 이외에 외부 저장 장치에도 미디어 파일이 저장된다. 사용자가 악의적으로 사생활 침해에 해당하는 사진 이나 동영상을 촬영했을 때 외부 저장장치의 마운트 흔적을 발견하는 것은 매우 중요하다. 일반적으로 USB 플래시 드라이브나 GPS 레코더 같은 장치가 마운트되면 /var/log/syslog 에 기록된다. 이 드론의 BusyBox 에는 syslog 가 포함되지 않아 확인할 수 없다. AR.Drone 에서는 /var/log/messages 에 기록되는 커널 로그를 통해 디바이스 마운트 정보를 얻을 수 있다. 실시간으로 tail -f /var/log/messages 명령어를 통해 커널의 이벤트를 확인한다.




(그림 6) USB drive 장착 해제 시 messages




(그림 7) USB drive 연결 시 messages 변화

## 4. 결론 및 향후 연구 계획

본 논문에서는 리눅스 기반 BusyBox 가 제공하는 드론의 파일 시스템 구조를 분석하고 드론 포렌식을 통해 유효한 증거를 가진 데이터를 수집했다.

최근 스마트폰과 드론의 Wi-Fi 연결을 통한 드론 운용방식이 증가하고 있어 스마트폰 앱의 모바일 포렌식을 통해 더 많은 정보를 얻을 수 있을 것으로 예상된다. 사용자가 앱에서 악의적으로 비행기록을 삭제했을 경우에 드론 내부에 완전히 삭제되지 않은 이전의 비행기록이 있는지 메모리 덤프로 확인해 볼 필요가 있다.

또한 상용화된 Parrot 사의 비밥드론이나 다른 무인항공사의 드론 모델에서 얻을 수 있는 정보는 어떤 것이 있는지 대부분의 드론에서 공통적으로 적용될 수 있는 포렌식 도구 개발이 필요하다.

**Acknowledgement**

이 논문은 2017 년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.B0722-16-0006, (창조씨앗-2 단계)암호와 물리계층보안을 결합한 IoT 네트워크 보안 기술 개발)

## 참고문헌

[1] 손성화, 강진혁, 박경준, “드론 무선통신의 개요 및 이슈” 한국통신학회지(정보와통신), 33(2), 93-99, 2016

[2] “드론 대중화를 위해 고민해야 할 부분”, 플래텀 http://platum.kr/archives/48799

[3] “살인병기서 일상으로..드론시대 열린다.” 한국일보 http://www.hankookilbo.com/m/v/0052263768fc4b949fc10332f59d91f1

[4] 이아름, “드론 시장 및 산업 동향,” 융합연구정책센터, 2017

[5] 정인수, 홍득조, “와이파이를 이용하는 드론의 취약점 분석,” 한국컴퓨터정보학회 학술발표논문집, 25(1), 219-222, 2017

[6] BusyBox https://ww9w.BusyBox.net/about.html

[7] 장현수, 손태식, “활성화 리눅스 시스템 정보 수집 도구 설계 및 구현,” 한국디지털포렌식학회, 12 호, 83-95, 2014