Regular paper http://dx.doi.org/10.13067/JKIECS.2013.8.6.855

안드로이드 스마트폰을 위한 앤티-포렌식 도구들의 활용성

문필주*

On the Availability of Anti-Forensic Tools for Android Smartphones

Phil-Joo Moon*

요 약

스마트폰은 컴퓨팅 능력 향상, 전송속도의 고속화, 다양한 애플리케이션의 활용 등을 통해 실생활에 매우 유익하게 사용되고 있다. 반면에 스마트폰을 이용한 범죄가 증가하고 있으며, 앤티-포렌식 도구들을 사용하여 스마트폰 메모리의 데이터를 고의로 삭제하는 경우도 발생하고 있다. 본 논문에서는 안드로이드 스마트폰 상에서 사용되는 앤티-포렌식 도구들을 조사 및 분석하여 앤티-포렌식 도구들의 특성과 기법을 연구한다. 또한, 상용 포렌식 도구인 Oxygen Forensic Suite를 이용하여 앤티-포렌식 도구들이 제공하는 기능들의 활용성을 검증하는 실험을 실시한다.

ABSTRACT

Smartphone is very useful for use in the real life through the improvement of computing power, faster data rate and the variety of applications. On the other hand, using the smartphone has been exposed to a lot of crime. Also, it occurs attempting to delete a data of smartphone memory by anti-forensic tools. In this paper, we investigate and analyze the anti-forensic tools used in the Android smartphone to study the characteristics and techniques of anti-forensic tools. In addition, experiments are performed to validate the availability of anti-forensic tools by the Oxygen Forensic Suite that is a commercial forensic tool.

키워드

Digital Forensics, Anti-Forensic, Smart Phone, Android
디지털 포렌식, 앤티-포렌식, 스마트폰, 안드로이드

Ⅰ. 서 론

최근 국내 스마트폰의 사용자는 3천만 명에 이른다고 한다. 이는 전 국민의 60%이상이 이미 스마트폰은 이용 하고 있다는 통계이다. 스마트폰은 컴퓨팅 능력 향상, 전송속도의 고속화, 다양한 부가기능 및 애플리케이션의 개발을 통해 대용량 디지털 멀티미디어 정보의 전달과 이용이 빈번하게 이루어지면서, 이동하면서 업무와 실생활에 사용하는 시간이 많아짐에 따라 관련된 정보를 전달하고, 편리한 생활을 하는 반면에 이를 이용한 많은 범죄에도 노출되고 있다. 스마트폰을 통한 범죄는 디지털 무선 정보에 대한 공격과 침해사고를 유발하고, 사회적 경제적 문화적 피해를 발생시킨다.

* 교신저자 (corresponding author) : 평택대학교 정보통신학과(pjmoon@ptu.ac.kr)
접수일자 : 2013. 04. 11 심사(수정)일자 : 2013. 05. 20 게재확정일자 : 2013. 06. 20

스마트폰 사용의 증가로 인하여 범죄자들에게 노출되어지고 있고, 실제로 많은 범죄에 이용되어지고 있다. 또한 스마트폰에 저장된 자료들로 부터 증거들을 수집 및 분석하여 수사에 활용할 수 있는데 이러한 자료가 디지털 증거로 사용되기 위해서는 원본성과 무결성이 입증되어야 한다.

최근에는 사용하고 있는 스마트폰의 운영체제를 초기화해 데이터를 완전하게 삭제하는 애플리케이션이 등장하고 있다. 이러한 애플리케이션들은 스마트폰 사용자가 자신이 사용하던 스마트폰을 증거물로 제출하면서 스마트폰 메모리에 저장된 데이터를 고의로 삭제하는 기능을 제공한다. 현재 출시된 스마트폰 데이터 삭제 애플리케이션을 이용하여 스마트폰 운영체제를 초기화하면 애플사의 iOS는 복원이 불가능하고, 안드로이드 운영체제는 상당부분 복원이 불가능한 것으로 알려져 있다[1].

앞에서 언급한 바와 같이 스마트폰에 저장된 자료들로부터 디지털 증거들을 수집하여 분석된 자료가 증거로 보장되기 위하여 원본성과 무결성을 입증하여 수사에 활용하는 과정을 디지털 포렌식(Forensics)라고 한다. 이와는 반대로 디지털 증거들을 수집 및 분석하는 과정을 방해하거나 수집, 분석된 자료가 증거로 사용되도록 하지만 원본성과 무결성을 저해하는 과정을 앤티-포렌식(Anti-Forensics) 이라고 한다.

본 논문에서는 스마트폰의 운영체제를 양분하고 있는 iOS와 안드로이드 중 안드로이드를 탑재한 스마트폰에서 사용되는 앤티-포렌식 도구들을 조사 및 분석하여 앤티-포렌식 도구들의 특성과 기법을 연구하고자 한다. 이러한 연구결과는 새로운 앤티-포렌식 도구의 설계에 도움을 줄 뿐만 아니라 새로운 연구 방향 설정하는데 기여하리라고 생각한다. 또한, 대표적인 상용 포렌식 도구인 Oxygen Forensic Suite를 사용하여 앤티-포렌식 도구들이 제공하는 기능들의 활용성을 검증하기 위한 실험을 실시하였다.

II. 배경: 디지털 포렌식과 앤티-포렌식

2.1 디지털 포렌식

포렌식은 “법정의”, “과학수사의”라는 의미를 갖는다. 포렌식은 범죄와 관련된 분야에 사용되어 지문, 모발, DNA감식, 변사체 검시 등이 주류를 이루었다.

디지털 포렌식은 PC, PDA, SERVER , MOBILE 등의 디지털 기기를 이용하여 범죄에 사용되거나 디지털 장비 속에 저장된 디지털 자료를 근거로 어떤 행위의 사실관계를 규명하여 사법기관에 제출하거나 증명하는 것을 말한다. 디지털 포렌식은 디지털 데이터 획득, 데이터의 분석, 증거의 추출, 보존, 표현 등의 과정들로 구성된다[2].

IT 기술의 발전 및 급격한 정보화 사회로의 변화는 정보의 디지털화를 가속시켜서 컴퓨터 관련 범죄뿐 만 아니라 일반 범죄에서도 중요 증거 또는 단서를 컴퓨터와 같은 디지털 정보기기 내에 보관하는 경우가 증가함에 따라, 범죄 규명 및 증거를 확보하기 위해 디지털 포렌식 기술이 필요로 하게 되었다.

디지털 포렌식은 검찰, 경찰 등의 국가 수사기관에서 범죄 수사에 활용되며, 일반 기업체 및 금융회사 등의 민간분야에서도 디지털 포렌식 기술의 필요성이 증가하고 있다. 예로써, 디지털 포렌식 기술은 보험사기 및 인터넷 뱅킹 피해보상에 대한 법적증거자료수집, 내부 정보유출방지 및 회계감사 등의 내부보안강화에 활용이 가능하다.

2.2 디지털 앤티-포렌식

디지털 앤티-포렌식은 디지털 증거를 방해하거나 파괴하는 행위로 정의된다. 디지털 앤티-포렌식 기술들은 데이터 파괴, 데이터 은닉, 데이터 조작, 데이터의 출처 제거 등 네 가지 분야로 분류된다[3].

데이터 파괴는 데이터를 사용하지 못하게 하거나 조사를 진행하지 못하게 한다.

데이터 은닉은 디지털 증거를 조사관에 보이지 않게 한다. 증거를 보이지 않도록 하는 암호화나 스테가노그래피(Steganography) 등의 방법을 사용하며, 스테가노그래피의 경우에는 텍스트 메시지나 이미지 파일을 이미지 파일, 비디오 파일, 오디오 파일 등에 숨겨 데이터를 은닉하는 기능을 제공한다.

데이터 조작은 거짓된 정보를 제공하게 한다. 이 정보로 인해 올바른 포렌식 과정에서 벗어나도록 잘못된 정보나 우회 정보를 제공한다.

데이터의 출처 제거는 증거의 출처를 제거함으로써 증거로 사용될 정보의 생성을 원칙적으로 막을 수 있다.

안드로이드 스마트폰의 앤티-포렌식 도구들은 안드로이드 운영체제의 기능성을 이용하여 생성되어진다[4].

III. 앤티-포렌식 도구들의 활용성 실험

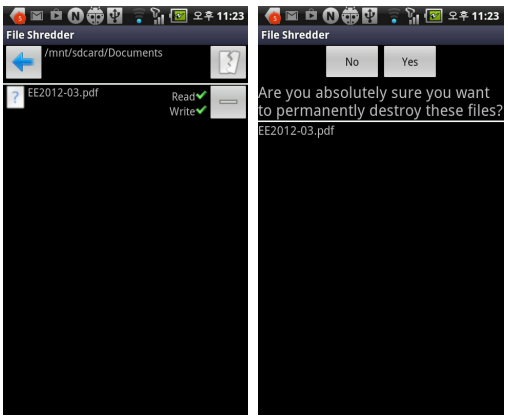
본 장에서는 안드로이드 스마트폰에서 사용 가능한 앤티-포렌식 도구들을 서술한다[5]. 또한 앤티-포렌식 도구들이 제공하는 기능들에 대한 활용성을 검증하기 위하여 상용 포렌식 도구인 Oxygen Forensic Suite[6]를 사용한다. Oxygen Forensic Suite는 스마트폰을 위한 포렌식 소프트웨어로 스마트폰 데이터의 논리적 획득 기능을 제공한다. 실험에 사용한 모바일 기기는 안드로이드 운영체제를 사용하고 있는 팬택의 IM-A690S SKY 스마트폰이다.

3.1 파일 분쇄

파일 분쇄(File Shredding)는 데이터가 증거로 사용되지 않도록 완벽하게 파괴하는 방법이다. 파일 분쇄 앱을 사용한 후의 데이터는 복구가 불가능하다.

File Shredder[7] 앱은 스마트폰에서 파일들을 영구히 제거하기 위해 사용된다. 선택한 파일에 랜덤 데이터를 반복하여 다시 쓰기 함으로써 파일을 삭제하는 방식이다.

그림 1은 File Shredder에서 EE2012-03.pdf 파일을 선택하여 삭제하는 화면으로 선택한 파일을 영구적으로 삭제할 것인지는 묻고 있다.



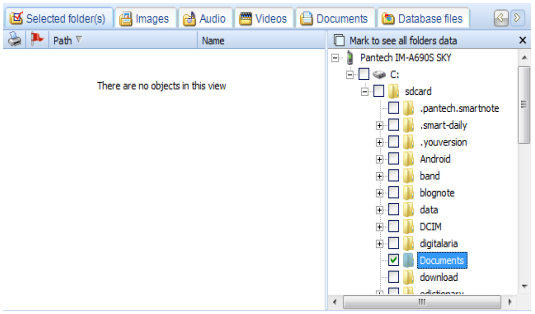


그림 1. File shredder의 파일 삭제 화면
Fig. 1 File shredder's file deletion screen

삭제한 파일은 /mnt/sdcard/Documents 폴더에 존재 했었다. Oxygen Forensic Suite를 실행하여 이 폴더를 확인해 보니 파일이 완벽하게 삭제되어 있음을 알 수 있었다. File Shredder라는 앤티-포렌식 도구이 제대로 동작하고 있음을 알 수 있다.

3.2 암호화

암호화(Encryption)는 쌍방간에 안전한 통신을 위해 데이터를 숨기는 방법이다.

LUKS manager[8] 앱은 안드로이드 기기에서 가상 폴더를 암호화한다. 이 앱을 동작하기 위해서는 실행되는 안드로이드 기기가 루팅되어야 한다. 이 가상 폴더들은 마운트, 언마운트, 생성, 삭제할 수 있다.

3.3 스테가노그래피

스테가노그래피(Steganography)는 미디어 파일, 문서 파일, 실행 파일 등에 디지털 정보를 숨기는 것을 말한다. 이미지나 오디오, 비디오 파일과 같은 미디어 파일은 파일의 용량이 크기 때문에 스테가노그래피로 사용하기에 유리하다.

StegDroid Alpha[9] 앱은 오디오 파일을 생성하면서 이 오디오 파일에 비밀 텍스트 메시지를 숨길 수 있다. 또한 이 앱을 통해 비밀 메시지를 추출할 수 있으며, 보안을 추가적으로 더 강화하기 위해 패스워드를 이용하여 암호화할 수 있다.

그림 2는 StegDroid Alpha를 실행하여 특정 파일에 텍스트를 삽입 후 인코딩하는 화면을 나타낸다.

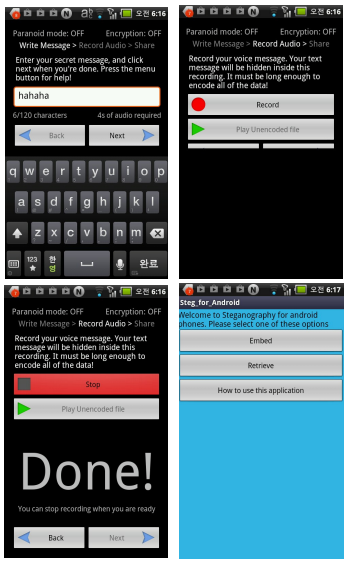


그림 2. StegDroid Alpha의 실행 화면
Fig. 2 StegDroid Alpha execution screen

그림 3은 Oxygen Forensic Suite에서 실험에 사용한 스마트폰의 파일 리스트를 나타내는 화면이다. 앞에서 StegDroid Alpha를 사용하여 특정 이미지 파일에 특정 텍스트를 숨길 때 사용했던 이미지 파일을 나타낸다.

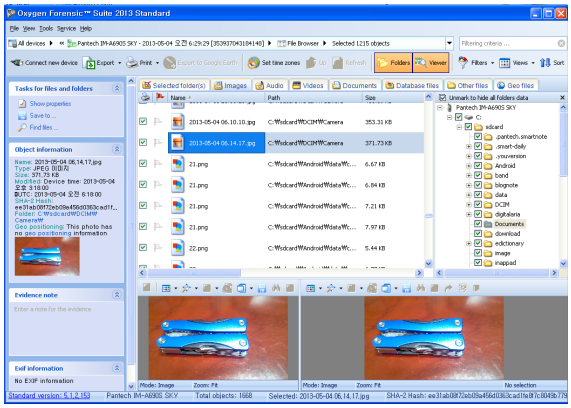
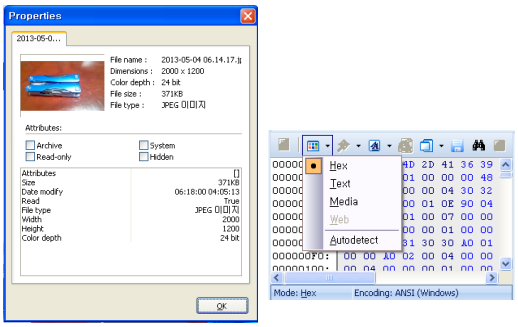


그림 3. Oxygen Forensic Suite의 파일 리스트
Fig. 3 Oxygen Forensic Suite's file list

그림 4의 (a)는 선택한 이미지 파일의 세부 정보를 나타내고, 그림 4의 (b)는 선택한 이미지 파일의 내용을 Hex 형태로 나타내고 있다.



(a) (b)

그림 4. 이미지 파일의 (a) 세부정보와 (b) 표현 방법 화면
Fig. 4 Image file's (a) Properties and (b) Display list screen

그림 5는 이미지 파일 내에서 특정 텍스트를 찾는 화면을 나타낸다. 앞에서 사용한 앱인 StegDroid Alpha를 사용하여 특정 텍스트를 찾고 있다.

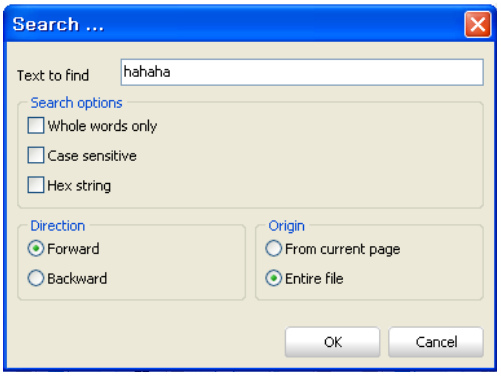


그림 5. 이미지 파일의 텍스트 검색 화면
Fig. 5 Image file's text search screen

그림 6은 검색결과를 나타내는 화면으로 찾고자 하는 텍스트를 찾지 못했다는 것을 나타낸다. 앞에서 StegDroid Alpha를 사용하여 텍스트를 이미지 파일에 숨겨 놓았는데 그것을 찾지 못했다는 것을 나타낸다. 이것은 StegDroid Alpha라는 앤티-포렌식 도구가 성공적으로 그 역할을 수행하여 상용 포렌식 도구인 Oxygen Forensic Suite를 이용하여 디지털 증거를 찾을 수 없도록 하고 있다는 것을 나타낸다.

표 1. 안드로이드 스마트폰에 대한 앤티-포렌식 도구들의 비교
Table 1. Comparison of anti-forensic tools for android smartphone

Application	Anti-forensic Technicque	Classification	Applied Objects	Features
File Shredder	File Wiping	Destroying Data	File, Folder	- Delete files by overwriting them with random data - Can work in the background
LUKS Manager	Encryption	Hiding Data	Folder	- Offers encryption to virtual folders - Virtual folder can be mounted, unmounted, created and deleted as required
StegDroid Alpha	Steganography	Hiding Data	Audio File	- Encodes text messages into an audio file - Provides group multicasting message - Reduce the file size by 33%
MobiStego	Steganography	Hiding Data	Image File	- Encodes text messages into an image file - Created image files can be sent by MMS - Only applicable to low-resolution image file
Steganography Application	Steganography	Hiding Data	Audio, Image File	- Encodes text messages into an image file - Encodes images into an audio and image file
Fake GPS Location	Spoofing	Counterfeiting Data	Location Information	- Faking the current GPS position of the smartphone - Provides 'autostart' options at boot time available

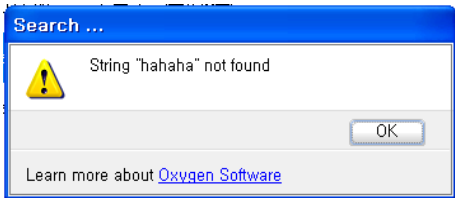


그림 6. 텍스트 검색 결과 화면
Fig. 6 Text search result screen

MobiStego[10] 앱은 텍스트 메시지를 이미지 파일에 숨길 수 있으며, 이 이미지 파일을 MMS로 전송할 수 있다. 이 앱은 낮은 해상도의 이미지 파일에만 적용이 가능하다.

Steganography Application[11] 앱은 텍스트 메시지를 이미지 파일에 숨길 수 있다. 또한, 이미지 파일을 이미지와 비디오 파일들에 숨길 수 있다. 이 앱은 이미지 파일에서 숨겨진 텍스트를, 이미지와 비디오 파일들에서 숨겨진 이미지를 검색할 수 있다. 그림 7은 특정 이미지 파일과 메시지를 이미지 파일에 숨기는 작업을 나타낸다. 또한, 특정 파일을 숨길 때 암호를 설정하도록 하여 숨긴 파일을 다시 나타낼 때 암호를 사용할 수 있도록 한다.

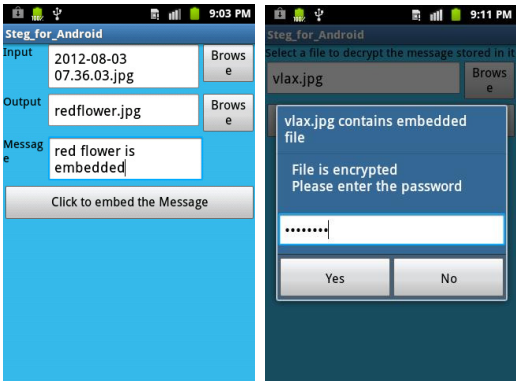


그림 7. Steganography application 화면
Fig. 7 Steganography application screen

3.4 정보 변조

정보 변조는 현재 사용 중인 스마트폰의 정보를 변조하여 다른 사용자들에게 거짓 정보를 나타내는 것을 말한다. 정보 변조의 대표적인 경우가 거짓된 위치 정보이다. 위치 정보는 다양한 소셜 네트워크 서비스나 맵 애플리케이션에서 사용한다. 이러한 애플리케이션에서 다른 사용자에게 자신의 위치를 거짓되게 알릴 수 있도록 한다.

Fake GPS Location[12] 앱은 현재 사용 중인 스마트폰의 현재 GPS 위치를 거짓으로 설정할 수 있게 해준다.

Ⅳ. 앤티-포렌식 도구들의 비교

본 장에서는 앞에서 설명한 안드로이드 플랫폼 상에서 사용되는 앤티-포렌식 도구들에 관하여 비교 및 분석을 하였다. 표 1은 안드로이드 플랫폼의 스마트폰에서 적용된 앤티-포렌식 기법들을 비교하여 요약해 놓은 것이다. 대부분의 안드로이드 스마트폰 앤티-포렌식 도구들은 무료로 제공되고 있다.

앤티-포렌식 도구들은 데이터 파괴, 데이터 은닉, 데이터 사기 등의 분야 등으로 분류될 수 있다.

데이터 파괴 분야는 적용대상에 따라 폴더 또는 폴더와 파일의 조합된 형태로 분류되어지며, 특성상 안드로이드 스마트폰이 루팅된 상태이어야 적용이 가능하다.

데이터 은닉 분야는 적용된 앤티-포렌식 기법에 따라 암호화나 스테가노그래피로 분류되며, 적용 대상에 따라 오디오 파일, 이미지 파일, 비디오 파일 등으로 구분할 수 있다.

Ⅴ. 결 론

본 논문에서는 현재 사용 중인 안드로이드 스마트폰을 대상으로 앤티-포렌식 도구들을 활용하여 데이터를 삭제하거나, 숨기거나, 속이는 일이 가능함을 나타내었다. 또한 앤티-포렌식 도구들을 비교 및 분석하여 적용된 앤티-포렌식 기술과 분류 방법들을 정립하였다. 이러한 연구결과들은 새로운 앤티-포렌식 도구의 설계 및 개발과 추후 연구방향을 제시하는데 많은 기여를 할 것으로 생각된다. 또한, 앤티-포렌식 도구들의 활용성을 검증하기 위하여 상용 포렌식 도구로 실험한 결과 File Shredder와 StegDroid Alpha에서 제공하는 기능이 완벽하게 수행됨을 확인할 수 있었다.

향후에는 다양한 모바일 플랫폼 상에서 앤티-포렌식 도구들을 활용한 기술들을 보다 상세하게 분석하여 앤티-포렌식 기법들에 대한 대응책을 연구해야 한다. 또한, 디지털 증거들이 삭제되거나, 숨겨지거나, 속이는 용도로 사용되는 것을 방지하기 위한 포렌식 측정 방법에 대한 연구도 진행되어야 할 것이다.

참고 문헌

[1] SmartPhone Data Deletion App…, http://www.etnews.com/news/computing/security/2726510_1477.html.

[2] Carrier, B., “Defining digital forensic examination and analysis tools”, International Journal of Digital Evidence, Vol. 1, pp. 1-10, 2002.

[3] Harris, R., “Arriving at an anti-forensics consensus : Examining how to define and control the anti-forensics problem”, The International Journal of Digital Forensics & Incident Response, Vol. 3, pp. 44-49, 2006.

[4] Distefano, A., Me, G., & Pace, F., “Android anti-forensics through a local paradigm”, Digital Investigation, 7(Suppl.), pp. 83-94. 2010.

[5] Ioana Sporea, Benjamin Aziz, Zak McIntyre, “On the Availability of Anti-Forensic Tools for Smartphones”, International Journal of Security, Vol. 6, Issue 4, 2012.

[6] Oxygen, “Oxygen Forensic Suite”, http://www.oxygen-forensic.com/.

[7] File Shredder, https://play.google.com/store/apps/details?id=net.fizzl.fileshredder&hl=ko

[8] LUKS manager, https://play.google.com/store/apps/details?id=com.nemesis2.luksmanager&hl=ko

[9] StegDroid Alpha, https://play.google.com/ store/apps/details?id=uk.ac.cam.tfmw2.stegdroid&hl=ko

[10] MobiStego, https://play.google.com/store/apps/details?id=it.mobistego&hl=ko

[11] Steganography Application,https://play.google.com/store/apps/details?id=com.preethi.bits.steganography&hl=en
[12] Fake GPS Location, https://play.google.com/store/apps/details?id=com.lexa.fakegps&hl=ko
[13] Gyu-An Lee, “A Study on Maritime Digital Forensic with Neccesity”, The Journal of the Korea Institute of Electronic Communication Sciences , Vol. 3, No. 4, pp. 204-209, 2008.
[14] Gyu-An Lee, “A Study on Influence of Korea-EU FTA Ratification upon Legal Service and Forensic Investigation”, The Journal of the Korea Institute of Electronic Communication Sciences, Vol. 6, No. 5, pp. 684-688, 2011.
[15] Gyu-An Lee, “A Study on Casino Embezzlement Incident Analysis and Forensic Investigation Technology”, The Journal of the Korea Institute of Electronic Communication Sciences, Vol. 6, No. 1, pp. 105-110, 2011.

저자 소개

문필주(Phil-Joo Moon)

1988년 숭실대학교 전자계산학과 졸업(공학사)
1991년 숭실대학교 대학원 컴퓨터학과 졸업(공학석사)
1998년 숭실대학교 대학원 컴퓨터학과 졸업(공학박사)
1988년~2001년 ETRI 책임연구원(팀장)
2001년~현재 평택대학교 정보통신학과 교수
※ 관심분야 : 엑세스망기술, 인터네트워킹, 모바일 애플리케이션, 네트워크보안, 모바일 포렌식