

# 사이버범죄의 대응강화를 위한 디지털 포렌식 수사 활용방안

오세연  
세명대학교 경찰행정학과 조교수

## The application of digital forensic investigation for response of cyber-crimes

Sei-Youen OH

Dept. of Police Administration, Semyung University Korea

요 약 본 논문에서는 최근 증가하고 있는 다양한 사이버범죄에 대한 대응강화를 위해 국내에서 발생하고 있는 사이버범죄의 발생현황과 경찰청의 디지털 포렌식 활용실태를 살펴 본 후 사이버범죄의 수사과 범인검거에 있어 좀 더 효율적으로 활용할 수 있는 사이버범죄 대응 디지털 포렌식 모델을 제안하고자 한다.

이 모델은 디지털 포렌식 분석기를 통하여 수집된 데이터를 언어지원시스템에 의해 다양한 개별언어를 표준화된 데이터로 처리하고, 처리된 데이터는 범죄혐의를 입증하는데 있어 법적 증명력이 있는지 여부를 검토하여 법적증명력이 있다고 분석된 데이터들은 다시 경찰 등의 수사기관에 알려주게 되어 신속한 수사를 가능하게 한다. 또한 수사기관은 파일시스템에 직접 접근하여 디지털 증거능력 여부를 조회 확인 할 수 있게 함으로써 보강수사에 대한 수사절차와 시간을 최소화 하고, 디지털 포렌식에 의해 분석된 데이터는 디지털 포렌식 저장기에 다시 저장하여 모아진 데이터를 통해 향후 범죄예측과 예방에 활용하게 함으로써 궁극적으로는 사이버범죄 감소의 효과를 가져 올 수 있다.

주제어 : 사이버범죄, 디지털 포렌식, 범죄수사, 온톨로지, 디지털 포렌식 범죄수사.

**Abstract** This study will show the digital forensic model which fights against cyber-crimes to prepare various cyber-crimes. The digital forensic model will be more useful about the investigation of cyber-crimes and arresting criminals after researching the uses of the digital forensic model and cyber-crime rates in South Korea. This model conduct the standardized data with various languages by the language support system through the digital forensic analyzer. This model will send the data to law enforcement reviewing whether or not we ought to prove criminal charges.

Moreover, law enforcement can access the file system to find out admissibility of evidence. And this model simplifies lawful investigation about additional investigation. The data, which is conducted and saved by the digital forensic system, will be helpful to protect against the future crimes because of the data.

**Key Words** : Digital Forensic, Cyber-Crimes, Criminal Investigation, Ontology, Digital Forensic Criminal Investigation.

Received 12 February 2015, Revised 25 March 2015  
Accepted 20 April 2015  
Corresponding Author: Sei-Youen Oh (Semyung University,  
Police Administration)  
Email: s092724@naver.com.

ISSN: 1738-1916

© The Society of Digital Policy & Management. All rights reserved. This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (<http://creativecommons.org/licenses/by-nc/3.0>), which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

## 1. 서론

20세기 후반부터 사이버공간의 활용을 통한 활동이 활발해지면서 사이버공간은 해킹, 사기 등의 사이버범죄에 불법적으로 이용되고 있으며 최근 들어서는 IS테러리스트들을 모집하는 방안의 한 방법으로까지 활용되면서 심각한 국제적 사회문제로 발전하고 있다. 이러한 사이버범죄는 익명성, 전문성, 기술성, 반복성 등의 특징을 가지고 공간의 제약 없이 이루어진다는 점에서 우리나라만의 문제가 아닌 국제적문제로 바라볼 필요가 있다.

사이버범죄의 발생추이를 살펴보면 전통적 범죄보다 더 급격한 형태로 증가하고 있으며 최근 10년간 무려 두 배가 넘는 범죄가 발생하고 있다. 더불어 그 피해의 심각성과 규모도 매우 크기 때문에 각 국가 간의 강력한 국제적인 대응방안이 강구되어야 하는 실정이다. 우리나라의 경우 사이버범죄에 대하여 사이버대응센터를 설치하여 사이버범죄에 대응하고 있다. 하지만 사이버범죄의 발생추이와 다양한 범죄기술 양상의 발달로 고도의 전문화 되어진 인력을 필요로 하고 있지만 아직 부족한 상태이며, 사이버상이라는 특성을 감안할 때 증거수집과 관련하여서도 디지털 포렌식의 활용방안이 적극적으로 모색되어야 하지만 지속적인 기술개발과 예산지원 등이 부족한 실정이다. 따라서 다양한 디지털매체의 발달과 사용으로 인한 다양한 사이버 범죄에 대응하기 위해서는 디지털 포렌식을 활용한 수사지원체계가 강화되어야 할 것이다.

이를 위해 우선 사이버범죄의 개념 및 유형 그리고 디지털 포렌식의 범죄수사처리절차에 대하여 살펴본 후 사이버범죄의 유형별 발생현황과 우리나라 경찰의 디지털 포렌식 활용실태를 알아보고, 이를 통하여 사이버범죄에 보다 효과적으로 대응하기 위한 디지털 포렌식 수사 활용방안에 대하여 제시해 보고자 한다.

## 2. 사이버범죄와 디지털 포렌식

### 2.1 사이버범죄의 정의

사이버범죄에 대한 학문적인 명확한 정의는 없지만 일반적으로 사이버공간에서 이루어지는 범죄행위로서 일반적으로 인터넷 같은 정보통신망을 연결된 컴퓨터시

스템이나 이들을 매개로 형성된 사이버공간을 중심으로 발생하는 범죄행위를 총칭하는 개념이다[1].

또 다른 정의를 살펴보면 사이버범죄란 개념이 아직은 불확정의 신조어로 학교폭력, 가정폭력, 지하철키폭죄 등과 같은 범죄가 행해지는 장소를 부각시킬 목적으로 가상의 사이버공간을 장소화 하여 호칭 하는 것으로 나아가 컴퓨터나 네트워크가 사용되지 않는 범죄라 하더라도 특정범죄에 디지털증거가 관련되어 있을 때 이를 광의의 사이버범죄에 포함시킨다는 견해도 있다[2].

이러한 사이버범죄의 유형으로는 경찰청에서 분류한 기준을 중심으로 살펴보면 그 범행목적에 따라 해킹, 바이러스 등의 사이버테러형범죄와 전자상거래 사기, 불법복제, 사이버폭력, 개인정보침해 등의 일반사이버 범죄로 크게 구분할 수 있다[3]. 또한 사이버범죄의 특징은 기존의 범죄와 달리 비대명성, 익명성, 전문성과 기술성, 시간과 공간의 무제약성, 상당한 재산피해와 빠른 전파성, 발각과 원인규명의 어려움 등의 특징을 가지고 있다[4].

따라서 본 논문서에서 사이버 범죄라 하는 것은 '인터넷을 비롯한 사이버공간과 같은 정보통신망으로 연결된 컴퓨터 시스템이나 이들을 매개로 한 사이버 공간에서 시간과 공간을 초월하여 빠른 시간 내에 불특정 다수인에게 해를 끼치는 범죄행위'라고 정의 할 수 있다.

### 2.2 디지털 포렌식

디지털 포렌식이란 디지털증거를 저장하는 정보기에 내장된 디지털자료를 근거로 삼아 그 정보기기를 매개체로 하여 발생한 어떠한 행위의 사실관계를 규명하고 증명하는 일체의 절차를 말한다. 다시 말해 디지털 증거를 수집, 운반, 분석하여 범죄와 관련된 정보를 획득하고 법정에서 유죄의 증거로 사용하기 위한 일련의 과정으로 1991년 미국 포틀랜드에서 열린 IACIS (International Association of Computer Specialists)에서 처음 사용되었다[5].

디지털 포렌식은 범죄수사의 일환으로 사용되어지기 때문에 디지털 증거를 수집하는 절차는 일반적인 증거물에 적용되는 법률절차를 그대로 적용하며, 디지털 매체의 특성으로 인한 추가적인 조치가 필수적이다. 디지털 포렌식의 대상이 되는 디지털 매체나 데이터는 비가시성, 변조가능성, 복제용이성, 휘발성의 특징이 있기 때문에 최초수집에서 보관까지 각 매체별 특징에 맞는 적절한

조치가 필요하며 이러한 과정과 절차가 준수되었다는 사실을 수사기관이 입증해야 한다[6]. 또한 최근에는 디지털 포렌식의 수사가 컴퓨터뿐만 아니라 개인 휴대폰에서 사건과 관련된 정보를 수집하고 삭제된 데이터를 복원하는 작업이 필수적으로 수행되고 있다[7]. 예를 들어 성폭행 살인사건과 같은 형사사건에서 용의자의 휴대폰에 있는 이미지 파일을 탐색하고 복구하여 피해자의 사진이 없는지를 조사하여 사건의 해결실마리를 찾는 기본적인 수사의 단계로까지 자리 잡고 있다[8]. 디지털 포렌식과 관련되어진 연구 분야는 디지털 증거수집과 관련된 절차적인 문제에 대한 연구와 다양한 디지털 데이터를 분석하는 기법에 관한 연구가 주를 이루고 있고[9, 10, 11] 특히 최근에는 모바일기기 등의 다양한 저장매체의 대중화와 클라우드, 가상시스템 등의 등장으로 각각의 매체와 데이터의 유형에 따른 조사, 분석방법에 대한 연구도 진행되고 있다[12, 13, 14].

따라서 사이버공간에서의 기술의 발달과 범죄의 다양성으로 인하여 컴퓨터, 스마트폰, 테블릿 PC 등과 같은 디지털 기기에서 증거를 수집하고 분석하여 범죄혐의를 입증하는데 사용되는 수사방법 중 하나로 범죄발생 시 적시적절하게 활용된다면 범죄수사에 더욱 효과적일 것이다.

### 2.3 사이버범죄의 발생 현황

경찰청에서는 사이버범죄를 사이버테러형범죄와 일반사이버범죄로 구분하고 있고 이에 대한 발생현황과 검거현황을 살펴보면[Table. 1]과 같다[15].

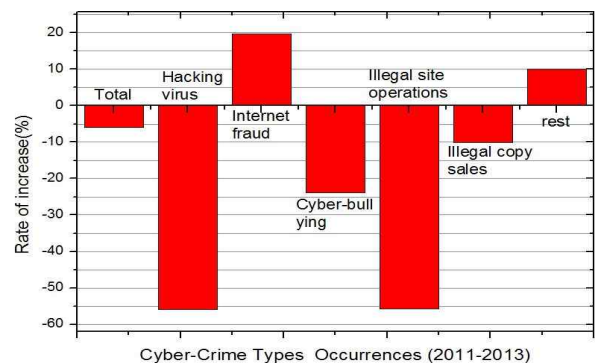
사이버범죄는 2011년 총116,961건에서 2013년 155,366건 발생하여 2011년에 비해 2013년에 32.8%가 증가하였지만 검거에 있어서는 2011년 91,496건에서 2013년 86,105건으로 2011년에 비해 2013년도에 -5.8% 감소한 것으로 나타나 사이버범죄의 발생은 증가하고 있으나 이에 대한 검거가 제대로 이루어지고 있지 않음을 알 수 있다[15]. 이는 사이버범죄의 특성상 전문성과 기술성을 요하고 있어서 일선 수사경찰관들이 수사현장에 도착하여도 전문성이 부족하여 파일과 데이터베이스를 누락시키는 등 적절한 방법으로 디지털 증거를 수집하지 못하고 있기 때문에 사이버범죄 발생 증가 대비 검거 현황이 감소한 것일 것이다.

<Table 1> Cyber-Crime Occurrences and Arrested Current States(2011-2013)

Type	Total		
	Occurrences	Arrest	
		Number	personnel
2011	116,961	91,496	95,795
2012	108,223	84,932	86,513
2013	155,366	86,105	92,621

또한 사이버범죄의 유형별 발생 현황을 살펴보면 [Fig. 1]과 같다[15].

2013년에 발생한 사이버범죄 유형을 보면 인터넷 사기가 39,282로 가장 많았고, 그 다음으로 불법복제판매, 사이버폭력, 해킹바이러스 순으로 많이 발생하는 것을 알 수 있다[15]. 특히 지난 3년 동안 사이버범죄의 유형 중 다른 범죄는 지속적으로 감소하는데 비해 인터넷 사기는 유일하게 계속적으로 증가하여 2011년 32,803건에서 2013년 39,286건으로 2011년에 비해 2013년 19.7%가 증가한 것으로 나타났다. 이는 최근 인터넷과 스마트폰, 테블릿PC 등의 디지털 매체를 이용하여 언제 어디서든 인터넷 쇼핑 등이 가능해지면서 인터넷 사기가 증가하고 있음을 알 수 있다. 이러한 상황을 반영하듯이 2008년부터 2011년 5월까지 경찰청 디지털매체 분석현황을 살펴보면 2008년 2,864개에서 2011년 6,247개로 2008년 기준 118% 증가하였다. 또한 디지털매체 분석 중 PC노트 분석이 2011년 1,394개로 가장 많은 비율을 차지했고 특히, 스마트폰과 휴대폰 분석은 2008년 47개에서 2010년 1,611개로 3,327% 증가하여 디지털매체 분석지원에 있어서 가장 높은 증가폭을 보였다[3].



[Fig. 1] Cyber-Crime Types Occurrences (2011-2013)

### 3. 사이버범죄와 디지털 포렌식 활용제안

위의 국내 사이버범죄의 발생현황과 경찰청의 디지털 포렌식 이용현황에서도 알 수 있듯이 사이버범죄의 국내 발생은 꾸준히 증가하고 있지만 기술적인 측면의 지원과 정책적인 수사절차추진상의 상이한 문제 등으로 인하여 이에 대한 검거가 제대로 이루어지지 않고 있다.

이러한 사이버 범죄의 증가는 현행 사이버 범죄 수사에 있어 다음과 같은 문제점이 있기 때문이다.

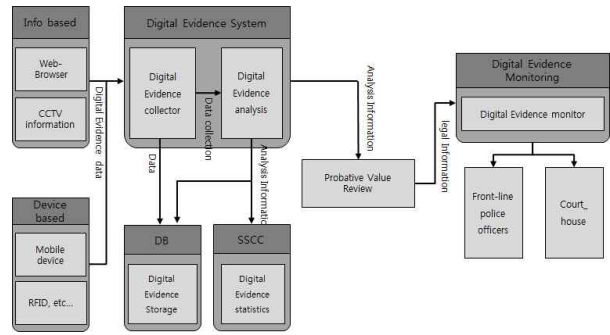
우선, 사이버범죄 수사 시 각종 디지털 포렌식 도구들은 각각 개별적인 특성에 맞추어 이용한 수사기법을 사용하였기 때문에 사이버 범죄의 시간적 제약이라는 특성과 수사절차상의 인권침해 등의 문제로 인하여, 수사상 필요한 여러 단계를 지나다 보면 증거가 없어지거나 누락되어 사이버범죄에 대한 증명력확보는 물론 범죄검거의 기회를 놓치게 된다.

또한 사이버범죄수사에 있어 디지털 포렌식은 전문적인 기술과 지식을 요하기 때문에 전문 분석관만이 디지털 증거물을 다루게 된다. 그러나 실질적으로 범인검거를 하고 현장에서 활동하고 있는 일선경찰관들이 디지털 포렌식을 수사하는 과정에서 직접적으로 연계하여 효과적으로 활용할 수 없다는 문제점이 있다.

마지막으로 사이버 범죄 수사 시 이용된 디지털 증거 자료들을 저장하여 향후 발생 되어질 범죄를 예측하는데 활용할 수 있는 제도적 장치가 없기 때문에 발생 가능한 범죄의 유형 등을 예측할 수 없다는 점이다.

따라서 이러한 여러 가지 문제점을 바탕으로 사이버 범죄에 대응강화를 위한 다음과 같은 디지털 포렌식 활용방안에 대하여 제시하고자 한다.

개별적인 디지털 포렌식의 분석과 이용보다는 온톨로지 등을 구축한 시스템 형식의 디지털 포렌식 체계가 갖추어 수집 증거에 대한 무결성, 신뢰성 등의 적법성 여부를 판단하여 증거의 증명력을 입증함으로써 범죄수사의 시간을 단축하고 사이버범죄에 대한 범인 검거율을 높일 수 있다. 따라서 사이버범죄 대응 온톨로지 형식의 디지털 포렌식 시스템의 구축설계는 다음의 [Fig. 2]와 같다.



[Fig. 2] Proposal Model of Ontology Digital Forensic for Response of Cyber-Crimes

디지털 증거 수집기를 통해 사이버범죄와 관련하여 영장에 의해 합법하게 압수, 수색할 수 있는 웹 브라우저, CCTV, 모바일 기기, RFID 등으로부터 디지털 증거 자료를 수집한다. 이렇게 합법하게 수집한 자료는 디지털 증거 분석기와 데이터베이스로 전송하게 된다.

디지털 증거 분석기는 디지털 증거 수집기로부터 전송받은 사이버범죄와 관련된 데이터를 분석하여 정보를 만들고 만들어진 정보를 데이터베이스와 디지털 증거식 통계처리기로 전송하게 된다. 데이터베이스에는 디지털 증거 분석기를 통해 처리된 정보와 디지털 증거 수집기를 통해 수집된 데이터를 함께 저장한다.

디지털 증거 분석기를 통해 처리된 정보를 다시 디지털 증거 수집기에 저장하는 이유는 향후 유사범죄가 발생할 경우 기존의 디지털 분석 데이터를 통해 범죄수사의 시간을 단축하고, 이중으로 번거롭게 드는 시간의 단축과 동시에 경제비용을 줄일 수 있게 하기 위함이다. 또한 축적된 정보를 바탕으로 이를 분석하여 앞으로 발생하게 될 범죄를 예측하고 이러한 범죄에 대하여 수사하는데 많은 도움을 줄 뿐 아니라 사이버범죄 이외에도 다른 범죄수사에 활용 될 수 있을 것으로 예상된다.

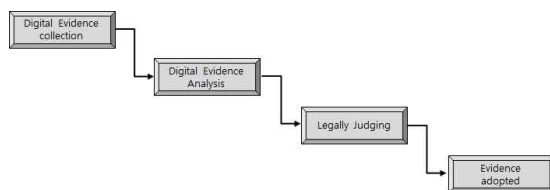
디지털 포렌식 분석기는 분석한 정보에 대하여 법적 증명력 여부를 판단하기 위해 증명력검토 판단기로 분석한 정보를 전송하게 된다.

디지털 증거 분석기가 전송한 정보를 받은 법적 증명력 검토 판단기는 전송받은 정보가 적법한 절차에 의해 신뢰성과 수집된 증거에 대한 무결성을 갖고 있다고 판단되면 증거 추적기로 정보를 전송하여 디지털 증거 정보가 사이버범죄 수사에 활용될 수 있게 하고, 이러한 증

명령 검토에 적법하지 않다면 사실상 데이터의 활용이나 법적 증거로 사용될 수 없으므로 폐기한다.

디지털 증거 분석기로부터 분석 정보를 받은 디지털 증거통계처리기는 필요한 종류의 통계 데이터를 생성하게 된다. 디지털 증거 통계처리기는 기존 정보들을 활용하여 과거 사건들에 대한 유형별 증감분석이나 사건해결 비율 등의 통계자료를 통해 현황을 확인하고, 향후 발생 가능한 범죄유형을 유추할 수 있도록 지원하게 한다.

마지막으로 디지털 증거의 증명력여부가 확보되면 디지털 증거 모니터를 통하여 일선경찰관과 검사 모두가 실시간으로 조회하거나 볼 수 있도록 하여 사이버범죄가 시간을 다투는 범죄이니만큼 추가보강 압수, 수색이 필요한 경우 바로 수사 할 수 있도록 지원하게 하여 불필요한 절차를 생략하게 할 수 있다.



[Fig. 3] Digital forensic process

#### 4. 제안 모델의 평가

사이버범죄에 대한 디지털 증거수집 절차와 분석을 통하여 범죄현의를 입증하는데 있어 증명력 여부의 확보는 범죄수사에 무엇보다 중요하며 이후 범죄수사에 대한 절차를 간소화하고 추가의 데이터 증거를 확보할 수 있게 하는데 영향을 미치게 됨으로 무엇보다 중요한 부분이라고 할 수 있다. 그러나 현행 사이버범죄 수사와 디지털 포렌식 시스템은 이러한 점에 한계가 있어 이를 보완하기 위한 필요성이 절실하다고 보여 진다.

이에 본 연구에서 제안한 모델을 토대로 사이버 범죄 수사에 활용하게 된다면 우선 제안되어진 온톨로지 형식의 디지털 포렌식 수사는 언어지원시스템을 통하여 다양한 언어 데이터를 표준화되어진 언어 데이터로 처리 할 수 있게 함으로써 일률적인 데이터 처리를 가능하게 하여 수집된 디지털 매체의 증명력 여부를 검토하게 되고 이는 전문가에게 번역을 맡기고 다시 데이터의 수사상

증명력이 있는지를 확인해야 되는 이중적인 일을 한 번에 처리할 수 있게 되면서 신속한 사이버범죄 수사를 실행 할 수 있게 된다.

다음으로는 사이버범죄에 대한 디지털 포렌식 수사가 현재 일선 경찰관들의 사이버범죄 수사 과정의 절차와 연계하여 사용하는 것이 힘들었다면 제안된 모델을 통하여 디지털 증거 분석기에서 처리되어진 데이터들이 법적 증명력이 인정된 경우 디지털 증거 모니터를 통해 수사 기관에 알리게 되고 수사기관은 파일시스템에 접근하여 디지털 매체의 증거능력여부를 직접 조회 확인하여 추가 보강 수사에 대한 절차상의 시간을 축약하여 빠른 시간 내에 범죄자를 검거 할 수 있게 되어 범죄감소라는 효과를 가져 올 수 있다.

마지막으로 처리되어진 디지털 증거 데이터는 다시 한 번 디지털 증거 저장기에 저장함으로써 향후 발생 될 범죄의 증감 여부와 범죄의 유형 등을 예측 할 수 있는 데이터로써 활용하게 되고 이는 비슷한 유형의 범죄가 발생 될 경우 시간의 단축은 물론이고, 범죄의 예측을 통한 범죄예방에 도움을 줄 것이다.

### 5. 결론 및 제언

#### 5.1 연구의 한계

본 연구는 국내에서 발생하고 있는 사이버범죄의 증가현상에 따른 효과적인 대응방안을 강구하고자 사이버 범죄의 발생현황과 디지털 포렌식의 이용실태를 살펴보고 수사상 문제점을 분석하여 향후 사이버범죄에 대해 디지털 포렌식을 활용한 좀 더 효율적인 수사방법과 방향에 대하여 제시하였다.

하지만 본 연구에서는 사이버범죄 수사에 대한 온톨로지 형식의 디지털 포렌식 모델을 제안하는데 있어 디지털 증거 데이터의 증명력 여부를 검토하여 정책적인 방향과 활용여부만을 제시하고 있기 때문에 많은 사례나 다양한 자료를 확보하여 타당성 검증은 통한 기술적인 측면에서 여러 분야의 다양한 사이버 범죄에 대응하는데 어느 정도 한계가 있다고 보여 진다.

#### 5.1 연구의 제언

사이버범죄에 대한 지능화와 다양한 수법의 증가로

인하여 디지털 포렌식 수사의 성장과 활용범위는 매우 넓고 새로운 분야에 대한 활발한 연구들도 진행되어지고 있다. 하지만 대부분의 연구가 각각의 성격이 다른 범죄에 대하여 디지털 증거를 분석하여 증거로 제시하는 정도의 모델을 연구하고 있어 제시된 디지털 데이터의 증명력확보에 문제점을 가지게 되고, 수사에 사용되어진 디지털 증거 데이터를 향후 발생하게 될 범죄를 예측하는데 사용 하지 않고 있어 디지털 증거 데이터의 범죄예측 활용에 대한 한계가 있었다. 따라서 본 논문은 이러한 문제점을 고려하여 사이버범죄 대응강화를 위한 온톨로지 형식의 디지털 포렌식 모델을 제안하여 디지털 증거 데이터의 증명력 여부 검토에 대한 분석을 추가하고 이후 분석 데이터를 저장하게 하여 향후 범죄예방에도 기여할 수 있게 하였다.

그러나 위의 연구의 한계에서 언급한 것을 토대로 앞으로의 연구에서는 실무사례를 통하여 기술적 측면의 효용성을 검증하고 일선의 수사담당자들이 좀 더 쉽게 활용할 수 있는 시스템의 추가개발과 이를 뒷받침해 줄 수 있는 다양한 정책적 방향도 세부적으로 마련되어야 한다.

## REFERENCES

- [1] Sang-Woon Kim, Hyun-Bin Jo, Prevention Methods of Cyber-crimes using the Private Security, The Korea Contents Association, Vol. 13, No. 3, pp. 141-151, 2012.
- [2] Won-Geun Yang, Nature of cyber crime and the investigation direction, Investigation research, 2006.
- [3] Bong-Gyu Song, Suk-Hun Chang. The Actual Condition of Police Digital Forensic and Its Solutions for Improvement, Korean Police Studies Review, Vol. 12, No. 2, pp.115-142, 2013.
- [4] Jeong-Wan, The Recent Situation of Cybercrime and the Legal Measurements. Hongik University Legal Research Center, Vol. 10, No. 1, pp. 195-224, 2009.
- [5] Han-Kuk. Yun, Sang-Hoon. Lee, Digital Forensics Ontology for Intelligent Crime Investigation System, Journal of Korea Society of Computer and Information, Vol. 19, No. 12, pp.161-169, 2014.
- [6] Sang-Jin. Lee. Introduction to Digital Forensics. Iroon. 2010.
- [7] Kyung-Soo Lim, Jong-Hyuk Park, Sang-Jin Lee, Trend and Challenges of Current Digital Forensics, Journal of Security Engineering, Vol. 5, No.4, pp. 47-58, 2008.
- [8] Kyung-Soo Lim et al, A Study on the Information Interchanging of Forensic Investigation in Knowledge Management System, Journal of Korea Institute of Information Security and Cryptology, Winter Symposium, pp. 35-53, 2007.
- [9] Kwang-Hun Cho, Improvement of the Issues in Search and Confiscation of Digital Evidence, Seoul Law Review, Vol. 21, No.3, pp. 699-738, 2013.
- [10] Young-Ho Kim, Dae-Sung Lee, The Problem Point and Improvement Program of the Scene Search and Seizure of Digital Evidence at Practical Affairs, Communication Engineering, Vol. 17, No.11, pp. 2595-2601, 2011.
- [11] Byong-Sun Kwack, A study on Problems and Improvements of Digital Forensic Investigation, Law Review, Vol. 23, No.2, pp. 171-191, 2013.
- [12] Byong-Sun Kwack, A study on Problems and Improvements of Digital Forensic Investigation, Law Review, Vol. 23, No.2, pp. 171-191, 2013.
- [13] Sang-Hee Jang et al, Digital Forensic Investigation of Virtual Desktop Infrastructure, Journal of Korea Institute of Information Security and Cryptology Vol. 23, No.2, pp. 203-212, 2013.
- [14] Se-Hwan Park, Young-Soo Chol, Jong-Kyu Park, Technology Trend on Image File Carving, Journal of the Institute of Electronics and Information Engineers, Vol. 37, No.6, pp. 1428-1431, 2014.
- [15] Korean National Police Agency, Statistical Yearbook of the Police, 2013.

오 세 연(Oh, Sei Youen)



- 2009년 9월 : 동국대학교 경찰행정학과 (경찰학박사)
- 2014년 1월 ~ 현재 : 한국경찰연구학회 여성이사
- 2015년 3월 ~ 현재 : 한국치안행정학회 운영위원
- 2014년 7월 ~ 현재 : 충청소방학교 자문위원
- 2013년 3월 ~ 현재 : 세명대학교 경찰행정학과 조교수
- 관심분야 : 범죄학, CPTED 등
- E-Mail : s092724@naver.com