Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.32, NO.4, Aug. 2022 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2022.32.4.723

안보사건에서 스테가노그라피 분석 및 형사법적 대응방안

오 소 정,[1†] 주 지 연,[1] 박 현 민,[1] 박 정 환,[3] 신 상 현,[4] 장 응 혁,[5] 김 기 범[2‡]
[1,2]성균관대학교 과학수사학과 (대학원생, 교수), [3]KDI국제정책대학원 (전문원),
[4]헌법재판소 (헌법연구원), [5]계명대학교 (교수)

Analysis of Steganography and Countermeasures for Criminal Laws in National Security Offenses

SoJung Oh,[1†] JiYeon Joo,[1] HyeonMin Park,[1] JungHwan Park,[3] SangHyun Shin,[4]
EungHyuk Jang,[5] GiBum Kim[2‡]
[1,2]Sungkyunkwan University (Graduate Student, Professor),
[3]KDI School (Associate Researcher), [4]Constitutional Court of Korea (Researcher),
[5]Keimyung University (Professor)

요 약

스테가노그라피는 테러, 간첩 등 국가안보를 위협하는 범죄에 비밀통신 수단으로 활용되고 있다. 정보통신기술 발전에 따라 기술도 고도화되고 있고, 범죄자들은 자체적으로 프로그램을 제작하여 사용하고 있다. 하지만 스테가노그파리 관련내용이 공개되지 않아 수사기술 개발과 형사법적 대응에 한계가 있다. 따라서 본 논문에서는 스테가노그라피 수사를 위하여 탐지와 해독과정을 살펴보고 대법원에서 유죄판결 받은 김목사 간첩사건을 중심으로 수법을 분석하였다. 김목사 간첩사건은 사전에 약속된 스테고 키를 활용한 대칭 스테가노그라피를 사용하였고 다중 보안장치를 사용한 고도화된 수법을 사용하고 있었다. 형사법적 쟁점은 ① 관련성, ② 참여권, ③ 공개재판 등 3가지 문제에 대하여 검토하였다. 본 연구가 수사기관이 스테가노그라피에 대한 분석기법을 발전시키는데 출발점이 되기를 기대한다.

ABSTRACT

Steganography is being used as a means of secret communication for crimes that threaten national security such as terrorism and espionage. With the development of computers, steganography technologies develop and criminals produce and use their own programs. However, the research for steganography is not active because detailed information on national security cases is not disclosed. The development of investigation technologies and the responses of criminal law are insufficient. Therefore, in this paper, the detection and decoding process was examined for steganography investigation, and the method was analyzed for 'the spy case of Pastor Kim', who was convicted by the Supreme Court. Multiple security devices were prepared using symmetric steganography using the pre-promised stego key. Furthermore, the three criminal legal issues: (1) the relevance issue, (2) the right to participate, and (3) the public trial issue a countermeasure were considered in national security cases. Through this paper, we hope that the investigative agency will develop analysis techniques for steganography.

Keywords: Steganography, Steganalysis, National Security, Digital Forensics, Criminal Investigation

Received(06. 03. 2022), Modified(07. 14. 2022), Accepted(07. 23. 2022)

† 주저자, mira0809@naver.com
‡ 교신저자, freekgb02@gmail.com(Corresponding author)

I. 서 론

스테가노그라피(Steganography)는 2001년 알카에다(Al-Qaeda)가 9.11테러에 사용하면서 전 세계에 알려지기 시작하였다[1]. 주로 간첩, 테러, 산업기술유출 등 국가안보를 위협하는 범죄에 통신수단으로 사용하고 있다. 역사적으로 볼 때, 1차 세계대전에서 독일의 스파이 '마타하리'가 프랑스군의 향후 계획을 음표에 숨겨 보고하면서 기습에 성공하였고 당시 프랑스군 20만명이 사망한 사례가 있다[2]. 2008년 유럽에서 이슬람 테러리스트들이 아동성착취물 사이트에 테러지령을 숨겨 통신수단으로 활용하였다[3]. 최근에는 사진, 문서 등에 해킹 명령어나 악성코드를 은닉하는 방법으로 방화벽과 침입차단시스템을 우회하여 사이버공격을 감행하기도 한다[4]. 2011년 최초로 사이버공격에 사용된 악성코드 '두쿠'가 출현하고[5], Hwp문서, Microsoft문서의 특징을 이용한 표적형 악성코드를 유포하는 은닉기술이 유행하고 있다. 또한 아동성착취물, 불법촬영물, 마약, 랜섬웨어 등을 거래하는 데에 악용하기도 한다[6]. 정보통신기술과 결합하면서 우리나라에서도 2013년 일명 '왕재산 간첩사건'[7]을 시작으로 2015년 '통합진보당 간첩사건'[8], 2017년 '김목사 간첩사건'[9]과 'PC방 간첩사건'[10] 등에서 활발하게 사용되었다. 스테가노그라피 특성상 일반사건보다는 안보사건에서 보다 활발히 사용되고 있다. 안보사건은 국민안전에 직접적인 위해가 될 수 있어 새로운 위협요인이 되고 있다.

하지만 수사기관은 스테가노그라피의 탐지와 해독에 대한 전문성이 부족한 실정이다. 구동 원리나 범죄 수법에 관한 기술정보가 공개되지 않아 연구도 미흡하다. 안보위협 요소를 사전에 차단하지 못하고 관련 수사기법을 발전시키지 못하고 있다. 현장 압수·수색에서 엄격한 절차를 요구하고 한정된 시간 내 탐지해야 하기 때문에 관련성 판단에 애로가 있다.(형사소송법 제106조제1항, 제215조) 정보저장매체를 반출하여 탐지 및 해독하는 과정에서 참여권 보장으로 보안기술이 공개되는 문제도 있다.(동법 제123조) 또한 공개된 법정에서 탐지 및 해독기술을 공개해야 하는지 문제가 발생한다.

따라서 본 논문에서는 안보사건에서 스테가노그라피 생성 및 해독 원리, 수사기관의 압수수색 절차와 방법을 분석하고 형사법적 대응방안을 제시하고자 한다. 특히, 스테가노그라피 수사과정 등을 소개하고, 2017년 대법원에서 유죄판결을 받은 일명 '김목사 간첩사건'을 중점으로 분석하고자 한다. 먼저, 제2장에서 스테가노그라피의 개념과 생성, 해독기술의 원리에 대해 살펴본다. 제3장에서는 대법원 판결을 바탕으로 압수·수색 과정, 범죄수법 등을 분석하여 시사점을 도출한다. 마지막으로 제4장에서 수사현장에서 발생할 수 있는 형사법적 쟁점에 대한 대응방안을 제시한다.

II. 스테가노그라피의 생성 및 탐지이론

2.1 스테가노그라피 개념 및 구동

스테가노그라피는 '정보를 숨기는 절차나 과정'[11], '정보를 감추거나 보이지 않게 하는 방법'[12], '데이터 은닉기법 중의 하나'[2], '기존의 자료에 암호화된 메시지를 넣는 기법'[13], '비가시적 통신의 기법과 과학'[14], '메시지의 탐지를 방지하는 방식으로 정보를 숨기는 기술'[15] 등으로 정의되고 있다. 정보를 숨긴다는 측면에서 암호와 유사하나 비밀메시지 존재 자체를 인지하지 못하게 한다는 측면에서 차이가 있다. 또한 비밀통신 기술로 복호화 방법을 공유하고 있는 관계자만 정보 교환이 가능하다.

스테가노그라피는 커버파일(Cover File)에 비밀메시지를 은닉하여 스테고파일(Stego File)을 생성하는 기술을 말한다[Fig.1]. '커버파일' 은 비밀메시지를 숨기는데 사용하는 위장할 파일을 의미하고, 주로 풍경사진, 신문기사 등의 내용으로 JPG, Docx, Hwp형식을 사용한다. '스테고파일'은 스테가노그라피가 적용된 커버파일을 의미한다. 따라서 제3자는 비밀메시지를 인지하지 못한 채 커버파일의 표면적인 내용만 인식할 수 있다.

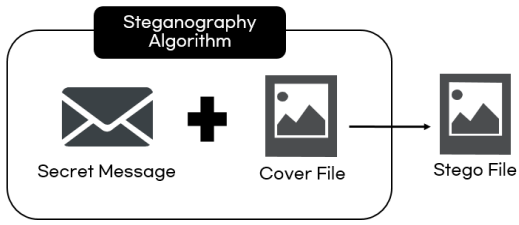


Fig. 1. Basic Procedure for Steganography

2.2 스테가노그라피 생성

스테가노그라피 생성기술은 2000년대에 들어 커버파일이 디지털화되면서 비약적인 발전을 이룩하였다. 2004년 인터넷상에 공개된 스테가노그라피 프로그램은 유·무료를 포함하여 약 100여개가 존재하였으나[12], 2014년 약 500여개 이상으로 10년간 5배 이상 증가하였다[16]. 과거보다 운영체제 환경도 다양화되어 해킹·악성코드 등 사이버 공격과 연계된 범죄수단으로 활발하게 사용되고 있다[17].

생성기술은 크게 치환(Substitution System), 변환영역(Transform Domain), 통계(Statistical), 대역확산(Spread Spectrum), 왜곡(Distortion), 생성데이터(Carrier Data) 등이 있다. 먼저 ① 치환은 커버파일의 잉여비트나 불용되는 비트를 비밀메시지로 치환하여 생성하는 기술이다. 많은 상용 프로그램이 이미지 및 그레이스케일 이미지에 8비트, 24비트를 사용하는 LSB(Least Significant Bit Embedding) 치환기법을 사용한다[18]. 파일의 이미지 픽셀을 구성하는 각 바이트 영역의 최하위 비트를 은닉데이터의 비트로 교체하는 방법이다[2]. 우리나라에서 발생하였던 대부분의 간첩사건은 치환기술을 활용하고 있다. ② 변환영역은 데이터의 입출력 및 교환 과정에서 일어나는 신호처리의 과정에서 메시지를 은닉하는 기법이다. 실시간으로 전달되는 데이터를 시각적으로 변화가 없도록 하면서 동시에 비밀메시지를 숨겨야 한다. 고도의 기술이 요구되어 최근 급속도로 발전하고 있는 기술이다. ③ 통계는 이미지의 통계적 특성을 이용하여 변조하거나 변경한다[19]. 구체적으로 커버파일을 임의의 구간으로 나눈 후, 1비트를 삽입하여 통계적인 변화를 발생시킨다. 즉, 비밀메시지의 비트에 따라 신호에 특성을 부여하여 변화가 생기는 구간을 '1'로, 변화가 없는 구간을 '0'으로 코딩하는 방식이다[20]. ④ 대역확산은 좁은 대역폭을 가진 신호를 넓은 대역폭을 가진 신호에 숨기는 방법이다. 커버파일의 데이터를 연속적으로 이동시키는 것으로 비밀키와 잡음생성기(Noise Generator)를 이용하여 비밀메시지를 마치 자연적인 잡음처럼 삽입한다. 비밀메시지 데이터가 커버파일의 특정영역으로 몰리는 것을 방지하여 탐지되는 것을 어렵게 한다. ⑤ 왜곡은 비밀메시지 삽입을 위하여 커버파일에 의도적인 왜곡을 일으키는 방식이다. 마지막으로 ⑥ 생성은 커버파일을 사용하지 않고, 비밀메시지에서 바로 스테고파일을 생성하는 방법이다. 스팸, 편지 등 거짓으로 메시지를 작성하여 일반적인 메시지로 보이게 하며 복호화할 수 있는 키를 소유하고 있는 관계자만 해독할 수 있다.

2.3 스테가노그라피 탐지와 해독

스테가노그라피 탐지 및 해독은 일반적으로 숨기는 기술을 역으로 수행하는 것으로 '스테그어날리시스(Steganalysis)'라고 한다. 스테가노그라피가 적용된 데이터에 대한 검출 및 분석하는 기술을 통칭하는 개념이다[21]. 탐지는 대상 파일이 스테고파일임을 인지하는 과정이고, 해독은 그 파일에서 비밀메시지를 추출하는 과정으로 보통 동시에 이루어진다. 스테가노그라피는 메시지를 정상영상에 맞추어 각 픽셀별로 숨길 수 있는 확률을 계산하며 의사난수를 이용하여 숨길 위치를 정한다. 이때, 그 키를 송·수신자 간에 공유함으로써 수신자는 스테고파일을 탐지하고 비밀메시지를 획득하여 해독하게 된다.

스테그어날리시스 방법은 크게 Visual Attack, 통계분석 등으로 구분할 수 있다. Visual Attack은 비밀메시지의 데이터가 무작위로 삽입되어 원본데이터와 구별해내기 어려운 경우 사용한다. 보통 LSB 및 팔레트 분석과 영상색상을 활용하여 미세한 변화를 감지하여 탐지한다. 즉, 이미지 변환이나 흐림의 정도를 식별하는 시각적 공격방법으로 LSB 영상분석, 이미지 변환 등에 사용된다. 통계분석은 카이스퀘어공격(Chi-square Attack)과 LSB랜덤분포조사 등이 있다. 전자는 비밀메시지를 커버파일에 암호화하여 숨기면 LSB에서 통계적 특징이 사라지는 성질을 이용하고, 후자는 LSB 분포형태를 중심으로 탐지한다. 카이스퀘어공격은 파일에서 특정 데이터나 구조 등에 비트가 관측된 빈도가 일반적으로 발견돼야 하는 기대 빈도와 일치하는지 확인한다. 특히, 스테가노그라피에서는 변조된 이미지를 감지하기 위해 이웃한 RGB 값을 기반으로 비교한다[22]. 대부분 이 방법을 사용하여 비밀메시지의 존재 여부를 판단하지만 미세한 크기의 메시지를 인지하기에는 부족한 면이 있어 숨긴 위치를 제대로 찾아낼 수 없다. 마지막으로 LSB랜덤분포조사의 가장 기초적인 방법은 시그니처를 활용하는 것으로 디스크가 파일을 읽는 방식과도 관련이 있다. 디스크는 파일의 구조 중, 데이터의 시작과 끝을 알리는 시그니처를 식별하여 읽게 되며 사용자에게 시각화해준다. 이와 같은 특징을 역으로 분석하여 파일에서 정해진 시그니처를 확

인하거나 헤더 등 구조 중 시각적 영향을 주지 않는 부분을 분석하면 스테고파일임을 인지할 수 있다.

최근 스테그어날리스는 기계학습 기반의 방법론을 적극 도입하고 있다[13][21]. 인공지능은 학습을 통해 얻어낸 알고리즘으로 ① 다양한 기법으로 생성한 스테고파일에 대한 무작위 실험(Blind Steganalysis)[23], ② 사용된 스테가노그라피의 알고리즘 분석(Targeted Steganalysis)[24], ③ 스테고파일을 생성하는 프로그램 및 시스템의 취약점을 이용하는 방법(System Attack)으로 탐지를 시도한다. 이를 활용하면 수사기관은 용의자가 어떠한 방법으로 비밀통신을 했을지 모를 때, 사용한 프로그램을 알고 있을 때, 도구의 취약점을 이용해 스테고파일을 탐지할 때 사용할 수 있다[25]. 또한 테러·범죄조직들이 스테가노그라피를 적극적으로 사용함에 따라 스테고파일을 탐지하는 프로그램 개발과 방법에 대한 연구도 꾸준히 진행되고 있다. 김현재등(2008)은 기존의 딥러닝을 이용한 검출기법의 한계점을 극복하기 위해 단적인 스테가노가라피 탐지기법이 아닌 융합 탐지 모델을 제시하였다[21]. 김재영등(2012)은 SPAM 기반의 영상 스테그어날리시스 기술을 사용하여 단일영상만 분석하여 범용적으로 사용하는데 한계가 있다는 기존 연구의 문제점을 극복하였다[26]. 기계학습 기반의 스테그아날리시스 모델은 스테고영상과 정상영상에서 차이가 나타나는 부분의 특징을 학습하여 구별하게 된다[21]. 일반적으로 커버 및 스테고파일에서 추출한 샘플 자체를 훈련데이터로 활용하여 그 기법에는 정확한 탐지가 될 수 있도록 하는 방식을 채택하고 있다[27]. 다만, 이러한 프로그램들이 모든 기법을 탐지할 수 없어 주요증거를 모두 확보할 수 없다. 또한 원본파일 없이 탐지가 가능한지 여부, 시그니처가 존재하는지 여부, 분석대상 시스템에 특정 프로그램 흔적이 존재하는지 여부에 따라 탐지 가능성이 다르게 나타난다.

III. 김목사 간첩사건의 스테가노그라피 기술분석

3.1 사건개요

김목사 간첩사건은 2011년 4월부터 2015년 11월까지 북한 대남공작조직 225국 소속 공작원에 포섭되어 국가보안법위반 혐의로 대법원에서 유죄판결을 받은 사건이다[9][28][29]. 검찰은 국가보안법상 찬양·고무등, 회합·통신등, 편의제공, 자진지원·금품수수한 혐의로 기소하였다. 1심법원[28]은 공소사실 중 이적표현물 소지에 대해 일부 무죄를 선고하였고, 2심법원[29]은 원심의 유죄판결 부분에서 일부 회합·통신등 및 편의제공도 무죄를 선고하였다. 1심에서 징역 4년형을 선고받았고 2심에서 징역 3년으로 감형되어 대법원에서 최종 확정되었다.

3.2 압수·수색 과정

2015년 국가정보원과 검찰은 압수·수색영장을 발부받아 피고인의 신체, 지갑 등에 소지하고 있던 정보저장매체를 압수하였다. 이때, 피고인 등 관계자에게 정보저장매체를 확인시켜주는 등 압수·수색 전 과정에 참여를 요청하였지만 거절하였다. 압수목록과 압수 증명서를 교부하였으나 수령확인 서명 및 날인도 거부하였다. 압수는 Micro SD 카드 3개, USB 4개, LG 노트북의 SSD 1개, 노트북 1대, 하드디스크 1개, 삼성 외장하드 S2 1개, CD 1개, LG사와 애플사 등 스마트폰 3대, 아이패드 에어2 1대, 갤럭시 탭 1대 총 17개로 각각 이미징하거나 이미징이 불가능한 경우 원본을 반출하였다[Table 1].

Table 1. List of Seized Digital Devices

No	Device	Detail
1	Micro SD card (No.122) 16G, SAMSUNG EVO, MBMPAGVDDD CE-P	- found at defendant's wallet.(2015. 11. 13. around 00:48) - seized the original and calculated hash by imaging.(around 11:25)
2	Micro SD card (No.123) 16G, S/N MBMSAGVDDD CW-P	- found by searching defendant's shirt pocket.(around 00:48) - seized the original, calculated hash by imaging.(around 12:37)
3	USB (No.124) HP 4G, v165w, S/N: AA0000 0000 003498	- seized at defendant's motorcycle seat's under space. (around 07:53 ~ 07:59) - sealed up and moved to defendant's residence and asked for confirmation cooperation to defendant and his wife - seized original and calculated hash by imaging.(around 09:20)
4	SD card (No.125) SONY, CHDC036GA	- found at a pile of coins inside the ashtray of defendant's car. (around 06:15 ~ 06:30)

5	USB (No.126) HP, 4G, S/N:AA0000 0000 000102	- seized each of the original. calculated hash by imaging.(around 07:59)
6	LG Notebook SSD (No.127) 128G, LG13Z94 Imaging File	- found at defendant's car(around 06:15~06:30) - seized the original and calculated hash by imaging.(around 12:37)
7	USB (No.128) 8G, Sandisk Blade Cruzer	- found at space in front of transmission of defendant's car.(around 06:15~06:30) - seized the original and calculated hash by imaging.(around 08:45)
8	USB (No.129) 32G, DUCO	- found at the living room of defendant's residence.(around 01:11~03:59) - seized the original and calculated hash by imaging.(around 13:16)
9	TOSHIBA Notebook (No.130) 120G, S/N 180XT018T Imaging File	- found at the living room of defendant's residence.(around 01:11~03:59) - seized after making 2 copies by imaging and return the original.(around 06:30)
10	Hard Disk (No.131) 40G, ○○○	- found at the living room of defendant's residence.(around 01:11~03:59) - error occurred during imaging, carried out the original by external company for recovery.(around 13:35)
11	SAMSUNG External Hard Drive S2(No.132) 500G	- found at storage box located at defendant's motorcycle seat's under space.(around 07:53~07:59) - seized the original and calculated hash by imaging.(around 12:30)
12	CD (No.133)	- found at the bookcase next to bookshelf at defendant's residence. - seized the original and calculated hash by imaging.(around 08:30)
13	Smart Phone No.134) LG-F300S, S/N 310KPDT0024778	- seized which was found in the body of defendant.
14	IPAD Air2 (No.135) A-1566, S/N DLXP4CCEGSV Y Imaging File	- found inside the backpack located at defendant's car's passenger seat. - seized the two images and returned the original to the defendant.(around 11:35)
15	GALAXY Tab (No.136) SHW-M500W, S/N R34D600A76V	- found inside the backpack located at defendant's car's passenger seat.
16	Smart Phone (No.137) SHV-E330S, S/N R33D60V7PBA Imaging File	- found and seized at the ceiling of defendant's residence located upper side of bookshelf which arranged at the surface of a wall of living room.
17	IPHONE 6 Plus (No.138) A-1524, IMEI : 35437063388512 Imaging File	- found at the inside pocket of defendant's top while searching defendant's body. - seized the two images and returned the original to the defendant.(around 11:20)

대법원은 압수한 다수의 정보저장매체에서 자체 제작한 프로그램으로 스테가노그라피를 생성하여 북한과 통신·연락한 사실을 인정하고 있다[9][28][29]. 암호화된 '국외(국내)여행신청 및 계약서'라는 제목의 'info.docx' 파일에는 구체적인 프로그램 사용설명서, 이메일 주소 교체이용과 관련된 약속사항 등이 기재되어 있었다[29][Table 2]. 국가정보원은 압수물에 대하여 각각 2015. 11. 14.~ 2015. 11. 29.경 선별압수를 수행하였다. 피고인에게 선별 과정에 대해 참여 의사를 물었으나 거부하여 압수·수색 과정의 동일한 참관인을 참여시키고, 종료 후 선별된 파일들에 대한 해시값을 산출하여 확인시켰다. 판결문에서는 어떤 압수물에서 스테가노그라피가 발견되었는지 구체적으로 설명하고 있지 않지만 피고인들이 자체 제작한 프로그램이 들어있는 USB(No.4)을 주고 받았고 이 프로그램의 기동방법을 제시하고 있는 'info.docx' 파일을 전달받았다는 사실을 명시하고 있다. USB(No.4)에는 'info.docx' 파일이 있었고 이 역시 스테가노그라피로 생성된 파일로 해독한 결과, 2011년 11월자 북한의 지령문을 확보하였다. 동일한 압수물에서 '고난주간 설교' 제목의 'to you.docx', 'to you7-7.docx' 파일을 발견하여 해독해 대북보고문임을 확인하였다. Micro SD(No.2)에서 본문이 "이스라엘 백성들에게..."로 시작하는 'to you11-12.docx' 파일을 확인하고, 해독한 결과 대북보고문을 확보하였다.

한편, USB(No.5)에서 스테가노그라피 생성을 위해 자체 제작한 주요프로그램 2개 중 'SETUP.EXE'도 확인하였고, 이를 수행하기 위하여 '남조선·전국련합·민주로총' 등 북한식 용어와 '위대한 령도자 김정일 동지·위대한 수령 김일성 동지' 등 북한을 찬양하는 500여개 이상의 문구가 포함되어 있었다[28]. 이 프

로그램들로 해독한 문서 파일의 내용으로 확인한 바 '분기마다 사용할 이메일주소와 암호'를 파악하였다[30]. 국가정보원은 이메일주소 10개에 대해 압수·수색영장을 발부받았으나 실제 수색할 수 있는 계정은 1개로 스테가노그라피가 사용되었는지 의심은 가지만 직접적인 관련성을 파악할 수 없어 2차 선별하기 위해 이메일 전체를 압수하였다[28]. 전체 보관함에서 피고인과 225국 소속의 간첩들이 주고받은 이메일을 총 17건 발견하고 첨부파일에 스테가노그라피 프로그램으로 제작된 것으로 의심되는 15건에 대해 출력 및 저장하는 방법으로 압수하였다. 이때, 이메일주소와 암호를 활용한 압수·수색에 대해 피고인은 위법수집 증거라고 주장하였으나 법원은 받아들이지 않았다.

Table 2. Steganography Manual 'info.docx'

NO		Contents
The First Operation (Manual of Program no° 1)	ⓐ	- Preparation for using program Make document to send but do not exceed capacity over 5K. If exceeding over 5K, Compress and make under 5K(ZIP) using compression program after finishing first operation.
	ⓑ	- Activation Method SISVGADRIVER - Open README.TXT file at AGPPACK folder. Copy string《THIS PACKAGE INCLUDE FOUR PARTS.》at contents written in the notepad. Next, activate SETUP.EXE file. When 《Please wait a moment》 string appears at screen, it is successfully activated.
	ⓒ	Dispatch Select OUT and add starting number at ID. Next, press BROWS button, read draft file and press START button. Then dispatch progress and operation completes.
	ⓓ	Starting number to use next time appears at the lower part of the program.(For example if 82 appears, then give 82)
	ⓔ	File will be created as RESUIT.TXT at the folder contained draft file before. Read work file by selecting IN and press BROWS button. Then press START button.
	ⓕ	Caution Avoid using overlapped number Important contents(Word such as Name, Age, Organization name, Region, Area can be tied with angle bracket and make double.
	ⓖ	Preparation for activating program - Text file : under 5K which gained by no.1 program work. - (RAR) file : already owned by promising mutually before
The Second Operation (Manual of Program no° 2)	ⓖ	- Promised password and starting number (Our company decided A's birth(1963) as password to avoid complexity) - Prepare WORD DOC file
	ⓗ	When preparing DOC file WORD OPTION(OPTION) - SAVE - Check all the last three spaces. WINDOWS standard typeface should not be used for DOC file typeface. Should made to become《Hancom Batang》, 《Hancom Dodum
	ⓘ	Finally when work is done, file that ( ) mark attached will be formed again newly under DOC file was located, and should send this file.
	ⓙ	Activate Program Double click the BORAMI customer management - Manual, TXT Double click - Select from customer management sales management to range from graduation etc. to blank case then copy it and double click the AUTORUN.EXE. Find again BORAMI customer management here and program will be appeared after double clicking SETUP.IMX (In the program, the first button is to send, the second button is to receive, the third number is to use, the fourth is to put the mutually promised password, and the first box below is to put the first file, the second box is to put the RAR file, and the third box is to put the DOCX) After putting required things, click START then SUCCESS message will be appeared.
	ⓚ	Manual until now is top secret data, therefore this manual should be deleted after a fully gets it and USB that contains these contents should be destroyed physically.

3.3 스테가노그라피 수법

3.3.1 설계

스테가노그라피 수법분석은 'info.docx'파일을 중심으로 분석하였다[Table 2]. 이 사건에서 스테가노그라피는 SETUP.EXE(이하, 프로그램1)과 SETUP.IMX(이하, 프로그램2)을 제작하여 생성하였다. 프로그램1은 난수 변환기능을 수행하고 커버파일로 텍스트 파일을 활용한다. 프로그램2의 기능은 명시되어 있지 않지만 도크파일을 커버파일로 사용한다. 이때, 5KB를 초과하였다면 프로그램1 동작 이후에 ZIP형식으로 압축하여야 한다고 하는 것으로 보아 프로그램2는 은닉 가능한 영역이 5KB까지만 수용할 수 있는 특별한 커버파일을 사용하거나 프로그램 자체에서 용량을 제한하는 것으로 보인다(Table 2. ⓐ). 이와 같은 특징들을 종합하면 [Fig. 2]와 같은 스테가노그라피 수법을 사용하였다고 정리할 수 있다.

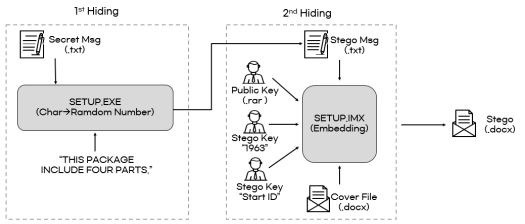


Fig. 2. Creation of Steganography

추가로 피고인은 조직원 및 상부조직에 보고하고 지령을 받기 위하여 이메일을 활용하였는데 이때, 첨부한 스테고파일의 이름에 일정한 규칙이 있었다. 'to you7-7.docx'은 7월 7일자 대북보고문이자 2013년 7월 7일에 약속된 외국계 이메일로 첨부한 파일이고 'to you11-12.docx'은 11월 12일자 대북보고문이자 2015년 11월 12일에 첨부한 파일이다. 즉, to you는 대북보고문을 피고인이 상부에 전달하기 위해 첨부할 때 사용하는 명칭이고 그 뒤의 대시(-)를 기준으로 왼쪽은 월(Month), 오른쪽은 일(Day)을 의미할 것이다.

3.3.2 1차 은닉단계

프로그램1을 구동하기 위해서는 SISVGADRIVER 폴더 아래 AGPPACK폴더에 위치한 지정된 텍스트파일(README.TXT)을 열람한다. 내용 중, "THIS PACKAGE INCLUDE FOUR PARTS" 라는 문자열을 복사한다(Table 2. ⓑ). 이 상태에서 프로그램1의 제목인 SETUP.EXE를 실행해야 정상적으로 기동한다고 하는 것으로 보아 복사한 데이터를 일시적으로 보관하고 있는 클립보드를 자동으로 접속함으로써 실행되는 구조로 보인다.

발신을 위해서 'OUT' 버튼을 선택하고 'ID' 칸에 시작번호를 입력한 후, 'BROW' 버튼을 눌러 비밀메시지를 불러들인다(Table 2. ⓒ). 시작번호는 직전에 스테고파일을 생성할 때, 확인된 번호를 입력해야 한다(Table 2. ⓓ). 이때, 수기로 작성하는 시작번호가 틀릴 수 있기 때문에 중복하여 입력하지 않도록 주의한다(Table 2. ⓕ). 프로그램1의 결과 파일 형식은 텍스트 파일로 산출되고, 그 이름은 비밀메시지가 있던 폴더에 RESULT.TXT로 항상 생성되는 것으로 보인다(Table 2. ⓔ). 스테고파일은 제작할 때마다 동일한 이름으로 생성되므로 이를 구분할 수 있도록 시작번호로 번호체계를 사용하는 것으로 보인다.

한편, 프로그램1은 문자를 숫자로 자동 변환하는 난수 변환기능을 수행한다. 일반적으로 난수는 무작위 숫자를 나타내는데 통신을 위해 제작한 프로그램이라면 반드시 규칙이 있었을 것이다. 첫 번째 가능성은 한글을 숫자로 변환하기 위해서 각 자음과 모음을 2바이트의 숫자에 대입하는 것이다. 예컨대, ㄱㄴㄷㄹ 등 자음에 순서대로 00,01,02,03..을 대입하고 ㅏㅑㅓㅕㅗ 등 모음에는 10,11,12,13..을 대입하는 것과 같이 각각의 자음과 모음에 숫자를 2바이트씩 배정하는 방법이다. 두 번째는 가나다라..등 글자 자체를 특정 숫자로 대입하는 것이다. 암·복호화 규칙이 전자보다는 후자가 비교적 수월하기 때문에 후자를 선택했을 가능성이 더 높아 보인다.

3.3.3 2차 은닉단계

프로그램2 구동 역시 프로그램1과 유사한 과정을 거친다. 먼저, '보라미고객관리' 폴더에서 지정된 파일을 열람하여 "고객관리 판매관리...학교졸업 등"이라는 문구까지 선택하고 복사한다. 직후, AUTORUN.EXE를 실행한 상태에서 보라미고객관리 폴더 내부에 저장되어 있는 SETUP.IMX을 실행해야 한다(Table 2. ⓙ). AUTORUN.EXE는 프로그램2를 실행하기 위해 백그라운드에서 실행하고 있어야 하는 보조프로그램으로 보인다. 이때, 프로그램2를 통해 최종 스테고파일을 제작하기 위하여 사전에 준비해야 하는 사항들이 있다. 먼저, 프로그램1에서 생성된 텍스트파일 형식의 스테고파일(이때, 5KB가 넘는다면 ZIP형식으로 압축해야 한다.)과 상호 간에 가지고 있는 RAR형식 파일, 약속된 비밀번호, 프로그램1에서 활용한 시작번호, 커버파일인 도크파일이 필요하다(Table 2. ⓖ). 이때, 도크파일의 서체를 제한하고 있으며 특정 저장 옵션을 활성화하도록 한다(Table 2. ⓗ). 비밀번호의 경우, 복잡성을 줄이기 위해 A의 생년도인 '1963'으로 통일한다고 명시하고 있으므로 특정 숫자가 지정되어 있다(Table 2. ⓖ). 이와 관련해서는 법원에서 피고인의 SNS 가입자 정보에 1963년생으로 기재한 것을 확인한 것과 부합하므로 A는 피고인으로 확인된다고 언급한 바 있다. 프로그램2의 스테고파일은 커버파일인 도크형식의 파일이 위치한 동일한 폴더에 '( )' 표시가 붙은 파일이고, 이를 송부하라고 명시하고 있다(Table 2. ⓘ). 이것으로 보아 스테고파일의 형식도 도크파일로 판단된다.

3.3.4 소결

과거 스테가노그라피는 그림과 그림을 합성하거나 삽입하는 등 비교적 단순하고 잘 알려진 방식을 사용하였다면 2010년대 들어서는 암호기법을 혼합한 고도의 기술을 사용하고 있는 추세이다. 북한이 자체 제작한 스테가노그라피 프로그램도 생성과 복호화 절차가 복잡하고 탐지 및 해독이 되지 않도록 설계하고 있다. 'info.docx'파일[Table 2]은 극비자료로 숙지 후 삭제하고 USB는 물리적으로 파괴하라고 지시하고 있음(Table 2. ⓚ)에도 피고인은 보유하고 있다가 적발되었다. 각 사건마다 스테고파일의 이름에 날짜 등을 넣어 규칙성을 보이고 있다. 명명규칙은 협의사실에 대한 관련성을 파악할 수 있어 검색, 색인 등의 방법으로 디지털포렌식에 활용할 수 있을 것이다. 다만, 명명규칙을 따르지 않는 경우가 발생하고 자체 제작한 프로그램과 추가로 상용화된 암호화 프로그램을 활용하여 2-3중으로 보안에 신경쓰고 있다. 통합진보당 내란선동 간첩사건에서도 이메일 암호화 프로그램인 PGP(Pretty Good Privacy)와 하드디스크를 통째로 암호화할 수 있는 프로그램인 트루크립트(Truecrypt)를 사용하여 3중 보안장치를 마련하였다[31].

종합하여 살펴볼 때, 수사기관은 한정된 시간 내에 탐지하여 사건과 관련성을 입증해내기 쉽지 않다. 스테가노그라피 수법이 공개되지 않지 않아 기술연구와 탐지에 한계가 있다. 형사소송법과 국가보안법에서도 안보사건에 대하여 예외를 두고 있지 않다. 이처럼 스테가노그라피는 기술뿐만 아니라 형사법적 측면에서도 다양한 쟁점 검토가 필요한 시점이 되었다.

IV. 스테가노그라피 수사에서 형사법적 쟁점

4.1 스테고파일의 관련성 판단

스테가노그라피는 한정된 시간 내 현장에서 탐지·수색하기 어렵다. 그렇다고 관련성 없는 파일까지 압수할 경우, 위법하게 수집한 증거가 될 수 있다. 김목사 간첩사건에서도 피고인은 압수·수색영장에 기재된 범죄혐의와 관련 없는 자료까지 전부 추출하였다며 위법하다고 주장하였다[28]. 왕재산 간첩사건에서도 정보저장매체에 대한 압수·수색 과정에서 관련성 문제가 논란이 되었다[32]. 서울중앙지방법원은 "각 영장 발부의 사유로 된 혐의 사실이 많고 각 압수·수색 장소에서 디지털 저장매체가 많게는 60여 개에 이를 정도로 다수 압수되었으므로 현장에서 범죄사실의 관련성이 있는 전자정보만을 구분해 내는 것은 현실적으로 불가능하였던 것"으로 보이고 "일부 보안USB에는 암호가 설정되어 있어 현장에서 그 내용을 지득할 수 없었으며, 삭제 파일의 복구 등 추가적 분석이 필요하였던 것으로 보이는 점 등을 인정할 수 있고, 이를 종합하여 보면 저장매체 자체를 직접 혹은 하드카피나 이미징 등 형태로 반출한 것에는 부득이한 사유가 있었음이 인정된다"며 피고인들의 주장을 배척하였다[32].

형사소송법은 피고사건과 '관계가 있다고 인정할 수 있는 것에 한정'하여 증거물 또는 몰수할 것으로 사료하는 물건을 압수할 수 있다고 규정하고 있다(제106조 제1항). 사건과의 관련성은 압수·수색의 대상과 범위를 결정하는 중요한 기준이나 그 개념이 다소 모호하다. 특히, 유체물과 달리 디지털증거는 대용량인 경우가 많은 상태에서 열람해야 관련성을 확인할 수 있어 프라이버시 침해가 발생할 수 밖에 없다[33]. 사건과의 관련성인 객관적 관련성, 증거와 수사대상자 간의 인적 관련성인 주관적 관련성, 협의사실 발생 시점과의 근접성인 시간적 관련성으로 세분화할 수 있다[33]. 대법원은 객관적 관련성에 대해 "압수수색영장에 기재된 협의사실 자체 또는 그와 기본적 사실관계가 동일한 범행과 직접 관련되어있는 경우는 물론 범행 동기와 경위, 범행수단과 방법, 범행 시간과 장소 등을 증명하기 위한 간접증거나 정황증거 등으로 사용될 수 있는 경우에도 인정될 수 있다"라고 한 후, "압수·수색영장에 기재된 협의사실의 내용과 수사의 대상, 수사 경위 등을 종합"하여 구체적·개별적 연관 관계가 필요하다고 보았다[34]. 인적 관련성에 대해서는 압수·수색영장에 기재된 대상자의 공동정범이나 교사범 등 공범이나 간접정범은 물론 필요적 공범 등에 대해서도 인정될 수 있다고 하였다[35].

종합하면, 스테가노그라피 탐지는 관련성 판단과 선별압수에 많은 쟁점을 야기할 수밖에 없다. 현실적으로 압수·수색 현장에서 스테가노그라피를 선별하여 압수하기 쉽지 않다. 따라서 안보사건의 경우, 암호나 스테가노그라피 사용 흔적이 있고 다른 감청자료 등에서 스테가노그라피를 사용한 증거가 발견될 경우 선별압수의 예외를 제한적으로 허용해야 할 것이다. 예컨대, 수사기관이 동일사건의 다른 영장으로 집행한 이메일에서 스테가노그라피 대화 내용이 발견되었거나 전기통신감청으로 스테가노그라피를 사용하는

흔적을 포착한 경우, 정보저장매체에 스테가노그라피에 대한 도구가 발견되거나 사용방법 등에 대한 검색기록이 확인되는 경우를 고려할 수 있다. 이러한 내용들이 발견되었을 경우에는 사전에 압수·수색영장에 선별압수에 대한 예외의 방식으로 압수하겠다는 내용을 포함시키는 것도 방법이다. 이러한 방법으로 집행하더라도 사후적으로 선별압수과정에서 참여권 보장, 위법수집증거 배제, 준항고 제도 등을 통하여 남용을 통제할 수 있을 것이다. 수사기관은 관련성 논란을 최소화하기 위해 스테가노그라피 사용 흔적을 채증하고, 탐지·해독이 가능한 고도의 기술을 개발해야 할 것이다.

4.2 분석 및 해독과정에서 참여권 보장

스테가노그라피를 이용한 안보사건에서 탐지 및 해독과정에 대한 참여권을 어디까지 보장해야 하는지 논란이 된다. 참여권은 피고인·피의자나 그 변호인이 법원 또는 수사기관의 압수·수색 영장 집행현장에 참여할 수 있는 소송법상 권리를 말한다[36]. 형사소송법은 검사, 피고인 또는 변호인은 압수·수색영장의 집행에 참여할 수 있고(제121조), 영장을 집행함에는 미리 집행의 일시와 장소를 검사, 피고인 또는 변호인에게 통지하도록 규정하고 있다.(제122조) 즉, 참여권은 수사절차 전반에서 보장하고 있다. 일례로 통합진보당 내란선동 간첩사건에서 정보저장매체 일부에서 암호화 프로그램이 사용된 정황이나 북한원전으로 보이는 파일이 삭제된 흔적을 확인하고, 전부 복제하여 압수하였다[37]. 그러나 피고인들은 반출하여 분석하는 과정에 참여시키지 않고 해독하여 증거를 수집한 부분에 대해 검사가 제출한 증거들이 위법하게 수집하였다고 주장하였고 대법원은 "전자정보가 담긴 저장매체 자체를 수사기관 사무실 등으로 옮겨 이를 열람 혹은 복사하게 되는 경우도 그 전체 과정을 통하여 피압수·수색 당사자나 그 변호인의 계속된 참여권 보장, 피압수·수색 당사자가 배제된 상태에서의 저장매체에 대한 열람·복사 금지, 복사대상 전자정보 목록의 작성·교부 등 압수·수색의 대상인 저장매체 내 전자정보의 왜곡이나 훼손과 오·남용 및 임의적인 복제나 복사 등을 막기 위한 적절한 조치가 이루어져야만 그 집행 절차가 적법"한 것으로 볼 수 있다고 판시하였다[38].

한편, 수원지방법원은 현장 압수 외의 과정에서 정보저장매체를 분석하는 것에 대한 피고인 등의 참여권에 대해 "수사관들이 저장매체를 전부 복제하여 압수한 후 해독된 암호로 암호화된 파일을 복호화하거나 삭제된 파일을 복구하고 영장에 기재된 범죄혐의 관련 전자정보를 탐색하여 이를 문서로 출력하는 과정 역시 전체적으로 위 영장 집행의 일환에 포함된다"고 하며 "피고인과 변호인에게 집행의 일시와 장소를 통지하여 참여권을 보장하지 않은 것은 형사소송법 제122조 본문, 제121조를 위반한 영장 집행"이라고 하였다[37]. 즉, 저장매체 자체를 복구·복제하거나 삭제된 파일을 복원하고 암호를 풀어 복호화하는 과정 역시 영장 집행의 일환이라고 판시한 것이다[39]. 분석과정에서 피고인이나 변호인에게 참여하도록 통지하지 않아 문제가 제기된 사건에서도 국가정보원 직원들은 암호해독 과정은 수사기밀에 해당하므로 압수수색 집행이 완료된 후 압수물의 분석과정에 피고인측 참여는 필요하지 않다는 취지로 증언하였다[37]. 대법원은 수사기관이 분석하는 과정에서 피고인측의 참여권을 보장하지 않은 것을 위법하나 현장에서 절차상 위법 없이 정당하게 증거를 수집하였고 서명하에 봉인하는데도 위법성이 없었으며 그 증거의 증거능력을 배제하는 것이 헌법과 형사소송법이 형사소송에 관한 절차 조항을 마련하여 적법절차의 원칙과 실체적 진실 규명의 조화를 도모하고 이를 통하여 형사 사법의 정의 실현 취지에 반하는 결과를 초래하는 것으로 평가되는 예외적인 경우로 인정하여 유죄증거로 사용할 수 있다고 판단하였다[37][40].

종합하면, 스테가노그라피 분석과정에 피고인 등을 참여시키면 수사기밀이 공개될 우려가 있는 것은 사실이다. 하지만 수사현장에서 분석할 경우 프로그램 형태로 구동되기 때문에 그것만으로 관련기술이 완전히 공개된다고 보기 어렵다. 나아가 수사기관이 관련기술의 공개가 최소화되는 방향으로 프로그램을 설계할 수도 있다. 따라서 수사현장에서 압수·수색할 경우 참여권을 충분히 보장하되 압수·수색이 종료된 이후 분석과정에는 참여권이 제한하는 것이 바람직하다.

4.3 재판과정에서 분석 및 해독기술 공개

국가안보와 관련된 범죄를 다루는 재판에서 스테가노그라피 탐지와 해독기술 등 수사기밀이 노출될 우려가 있다. 공개재판주의는 헌법에서 명시한 원칙으로 재판의 공정성과 투명성을 보장하는데 기여한다. 법원조직법 제57조제1항에서는 국가의 안전보장·안녕질서 또는 선량한 풍속을 해할 우려가 있는

때에는 결정으로 이를 공개하지 않을 수 있다며 예외 조항을 두고 있다. 김목사 간첩사건에서도 스테가노그라피로 암호화된 대북연락문의 복호화 과정을 설명하고 실연하는 증인신문이 비공개로 진행되어 논란이 되었다[28]. 검사는 수사기관이 스테가노그라피를 탐지하고, 해독하여 증거를 수집하는 과정이 공개되면 그 자체가 국가안전에 적절하지 않는다는 취지로 재판의 비공개를 신청하였다[28]. 서울고등법원도 수사기관의 탐지 및 해독기술이 상당한 수사기밀에 해당할 수 있고, 외부에 공개될 경우 국가안보를 해할 우려가 있다고 보아 적법한 조치로 판단되었다[29].(헌법 제27조제3항, 제109조, 법원조직법 제57조제1항) 왕재산 간첩사건에서도 피고인은 원심의 일부 증인신문에 대한 비공개 결정이 없었음에도 국가안전을 해할 우려가 있다는 사유만으로 재판을 정당한 사유 없이 비공개로 진행한 것은 위법하다 주장하였다[41].

대법원은 피고인들이 공개재판을 받을 권리를 침해한 절차적 위법이 있다고 인정하면서도 공판기일 전 검사가 증인신문 과정에서 스테가노그라피로 생성된 증거물을 해독하는 과정과 다른 증거목록의 검증을 병행하겠다는 내용의 입증계획서를 제출한 바 있고, 국가안전 보장을 위하여 비공개 증인신문 등의 조치가 필요하다는 의견서를 제출한 점을 인정하여 심리 전체의 비공개 결정은 재판공개 규정에 따라 이루어진 적법한 조치로 판단하였다[7].

종합하면 수사기관의 스테가노그라피 해독기술이 일반에게 공개됨에 따라 악용할 소지가 있다. 예컨대, 해독기술을 변조하여 anti-decrypto를 개발하고 범죄에 활용될 가능성도 배제할 수 없다. 따라서 스테가노그라피 탐지와 해독기술은 수사기밀에 해당하고 국가안보에 영향을 미치기 때문에 공개재판의 예외를 허용할 필요가 있다.

V. 결 론

북한의 스테가노그라피 기술은 이미지, 문서 등 파일의 특정 구조를 이용한 단순삽입, 수정을 넘어 이제는 정해진 커버파일과 스테고 키 등 고도화된 첨단기능을 갖춘 프로그램으로 진화하고 있다. 구동하기까지의 절차조차 상당히 복잡하고 상용화된 암호화 프로그램을 활용하여 보안 수준이 높아지고 있다. 그래서 수사기관이 증거를 수집하지 못하거나 해독방법을 확보할 수 없는 경우도 발생한다. 나아가, 실시간 탐지시스템 등 개발이 미비하여 스테가노그라피를 유사한 수법으로 사용하고 오랫동안 국내에서 활동을 유지할 수 있는 여건이 마련됐다. 따라서 본 논문에서는 스테가노그라피 생성·탐지기술을 살펴 김목사 간첩사건을 대상으로 압수·수색과정과 수법에 대해 분석하였다. 또한 안보사건에 발생하는 형사법적 쟁점인 관련성문제, 참여권문제, 공개재판문제에 대해 살펴보았다. 안보사건에서는 선별압수 예외를 제한적으로 허용하고 참여권을 최대 보장하되 탐지·해독기술을 활용한 분석과정에서는 예외가 허용되어야 한다. 마지막으로 수사기관의 분석기술은 수사기밀에 해당하고 국가안보에 영향을 미치기 때문에 공개재판의 예외를 허용할 필요가 있다.

북한의 스테가노그라피 수법이 진화함에 따라 다양한 가능성을 대비하여 관련 기술을 확보해야 한다. 스테가노그라피와 암호에 대해 복호화명령을 도입할 것인지, 수사기관의 분석결과와 해독 프로그램에 대한 신뢰성은 어떻게 입증할 것인지에 대한 연구도 필요하다. 특히, 2024년 대공수사권 이관에 따라 첨단기술을 개발하고 수사기법과 지침, 절차를 준비해야 할 것이다. 본 연구가 수사기관의 스테가노그라피 분석기법과 형사법적 쟁점을 연구하는데 기초자료로 활용되기를 기대해 본다.

References

[1] NBC NEWS, "FBI: Russian spies hid codes in online photos", http://www.nbcnews.com/id/38028696/ns/technology_and_science-science/t/fbi-russian-spies-hid-codes-online-photos/#.XNdsf-UzZhE (Last Check 2021. 10. 21.)

[2] Jo Jae-Ho and Jeong Kwang-Sik, "Anti-forensics", episteme, 2018.

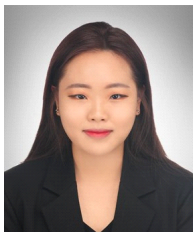
[3] Donga, "Use of Children's Porno Site as a Contact Channel for Islamic Terrorists", https://news.naver.com/main/read.naver?mode=LSD&mid=sec&sid1=104&oid=020&aid=0002000820 (Last Check 2022. 3. 4.)

[4] Dmitri Alperovitch, "Revealed: Operation Shady RAT", McAfee, 2011; Hon LAU, The Truth Behind the Shady RAT, Symantec, 2011, Avaliable: https:

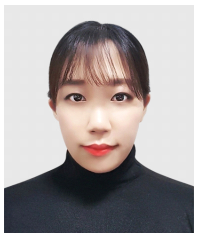
//www.symantec.com/connect/blogs/truth-behind-shady-rat (Last Check 2021.10.27.)
[5] Mcfree, "McAfee Lab Threat Report", June, 2017.
[6] Eric Cole, Ronald L. Krutz, James Conley, "Network Security Bible", 2004.
[7] Supreme Court, "Decision 2013도2511", Decided July 26, 2013.
[8] Supreme Court, "Decision 2014도10978" Decided Jan. 22, 2015.
[9] Supreme Court, "Decision 2017도9747" Decided Nov. 29, 2017.
[10] Supreme Court, "Decision 2017도12643" Decided Oct. 31, 2017.
[11] Merrill Warkentin, Ernst Bekkering, and Mark B. Schmidt, "Steganography: Forensic, Security, and Legal Issues," Journal of Digital Forensics, Security and Law, vol 3, no. 2, p. 17, 2008.
[12] G.C. Kessler, "An Overview of Steganography for the Computer Forensics Examiner", Forensic Science Communications, vol 6, no. 3, pp. 1-29, 2004.
[13] Huayong Ge, Huang Mingsheng, and Wang Qian, "Steganography and Steganalysis based on digitalimage," Image and Signal Processing (CISP), pp. 252-255, 2011.
[14] M.M. Sadek, A.S. Khalifa, and M.G. Mostafa, "Video steganography: a comprehensive review," Multimedia Tools and Applications, vol. 74, no. 17, pp. 7063-7094, 2015.
[15] N.F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," IEEE computer, vol. 31, no. 2, pp. 26-34, 1998.
[16] Mohsen Bazyar and Rubita Sudirman, "A Recent Review of MP3 Based Steganography Methods," International Journal of Security and Its Applications, vol. 8, no. 6, pp. 405-414, 2014.
[17] Jennifer Newman et al., "Can stego images from a mobile phone stego app be detected?," International Forensic Science Error Management Symposium, July 2017.
[18] Jessica Fridrich, Miroslav Goljan, and Rui Du. "Reliable detection of LSB steganography in color and grayscale images," In Proceedings of the 2001 workshop on Multimedia and security: new challenges (MM&Sec '01). Association for Computing Machinery, New York, pp. 27-30, 2001.
[19] M. Kharazi, H.T. Sencar, and N. Memon, "Image steganography: Concepts and practice," WSPC/Lecture Notes Series: 9in x 6in, pp. 1-49, 2004.
[20] S.C. Katzenbeisser. Information Hiding Techniques for Steganography and Digital Watermarking Illustrated Edition, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, pp. 43-78, 2000.
[21] Kim Hyunjae, Lee Jaekoo, Kim Gyuwan and Yoon Sungroh, "Generalized Steganalysis using Deep Learning," Journal of Korean Institute Of Information Scientists and Engineers, 23(4), pp. 244-249, 2017.
[22] Ji Seon-su, "Detecting Steganographic Contents Using EWM Statistics," Journal of Korea Society Of Industial Information Systems, 13(3), p. 58, 2008.
[23] M.H. Menori and R. Munir, "Blind steganalysis for digital images using support vector machine method," International Symposium on

Electronics and Smart Devices (ISESD), pp. 132-136, 2016.
〔24〕 G.J. Babu and R. Sridevi, "Contemporary stegnalysis schemes for reliable detection of stega-nography," International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp. 2013-2016, 2017.
〔25〕 Oh So-Jung, Joo Ji-Yeon, Park Hyun-Min, Park Jung-Hwan, Shin Sang-Hyun, Jang Eung-Hyuk and Kim Gi-Bum, "Steganography Analysis and Criminal Legal Issues at investigation," Winter Conference of the Korean Digital Forensics Society, 2021
〔26〕 Kim Jae-young, Park Han-hoon and Park Jong-il, "Experimental Verifi-cation of the Versatility of SPAM-based Image Steganalysis," Journal of Broadcast Engineering, 23(4), pp. 526-535, 2018.
〔27〕 J. Fridrich and J. Kodovsky, "Rich Models for Steganalysis of Digital Images," in IEEE Transactions on Information Forensics and Security vol. 7, no. 3, pp. 868-882, 2012.
〔28〕 Seoul Central District Court, "Decision 2016고합538, 558(Merged)", Decided Dec. 15, 2016.
〔29〕 Seoul High Court, "Decision 2017노23" Decided June 13, 2017.
〔30〕 Lee Chang-Hyun, "A Review of Criminal Procedure Cases of the Korean Supreme Court in 2017," Human Right and Justice, (473), pp. 43-46, 2018.
〔31〕 Kim Gi-Bum, "A Study on the Improvement of Digital Forensics Capacity for Steganography," KOREA ASSOCIATION FOR INFORMEDIA LAW, research presentation, May 2019.
〔32〕 Seoul Central District Court, "Decision 2011고합1131, 1143, 1144, 1145, 1146(Each Merged)" Decided Feb. 23, 2012.
〔33〕 Lee Wan-kyu, "Search and Seizure of the Digital Evidence and the Concept of Relevancy". Korean Lawyers Association Journal, 62(11), pp. 91-162, 2013.
〔34〕 Supreme Court, "Decision 2019도14341", Decided Feb. 13, 2020.
〔35〕 Chang Eung-Hyeok, "the Study of Interpretation and Issues about Relevancy Requirement of Seize Warrant", Journal of Criminal Law, pp. 235-260, 2020.
〔36〕 Lee Jin-Kuk, "Kleine Bemerkungen zur Tragweite des Teilnahmerechts der Betroffenen bei der Beschla-gnahme und Durchsuchung der elektronischen Informationen", Legal Research Institute of Ajou University, 11(4), p. 331, 2018.
〔37〕 Suwon District Court, "Decision 2013고합620,624(Merged),699(Merged),851(Merged)" Decided Feb. 17, 2014.
〔38〕 Supreme Court, "Decision 2009모1190" Decided May 26, 2011.
〔39〕 Seoul High Court, "Decision 2014노762" Decided Oct 11, 2014.
〔40〕 Supreme Court(En banc), "Decision 2007도3061", Decided Nov. 15, 2007.
〔41〕 Seoul High Court, "Decision 2012노805" Decided Feb. 8, 2013.

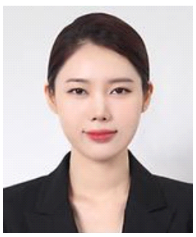
〈저자소개〉



오 소 정 (SoJung Oh) 학생회원
2019년 2월: 상명대학교 컴퓨터과학과 졸업
2020년 3월~현재: 성균관대학교 과학수사학과 석사수료
2020년 7월~현재: (사)한국디지털포렌식학회 간사
〈관심분야〉 디지털포렌식, 사이버범죄수사, 모바일포렌식, 다크웹추적 등



주 지 연 (JiYeon Joo) 학생회원
2018년 2월: 조선대학교 법학과 졸업
2020년 12월: 한국여성인권진흥원 디지털성범죄피해자지원센터 팀원
2021년 2월~현재: 성균관대학교 과학수사학과 석사과정
2022년 7월~현재: 정보통신정책연구원 연구원
〈관심분야〉 디지털포렌식, 사이버범죄수사, 디지털 성범죄, 형사법, 국제공조수사 등



박 현 민 (HyeonMin Park) 학생회원
2016년 8월: 백석대학교 정보보호학과 졸업
2018년 9월~현재: 성균관대학교 석박통합과정 수료
2020년 1월~4월: 대전선거관리위원회 디지털포렌식요원
〈관심분야〉 디지털포렌식, 사이버범죄수사, 안티포렌식, 보이스피싱, 가상자산포렌식 등

박 정 환 (JungHwan Park) 정회원
2010년 2월: 아주대학교 정보및컴퓨터공학과 졸업
2013년 2월: 제주대학교 법학전문대학원 석사
2022년 2월: 성균관대 과학수사학과 박사(디지털포렌식)
2022년 1월~현재: KDI 국제정책대학원 인권센터
〈관심분야〉 디지털포렌식, 디지털 성범죄, 사이버범죄수사, 인권침해조사 등

신 상 현 (SangHyun Shin) 정회원
2016년 8월: 고려대학교 법학과 석사(형법)
2019년 2월: 독일 뮌스터대학교 법학과 LL.M.(형사법)
2020년 12월: 독일 뮌스터대학교 법학과 박사(Dr. jur.)(형사법)
2021년 5월~현재: 헌법재판소 헌법연구원
〈관심분야〉 형법, 형사소송법, 형사정책, 비교법

장 응 혁 (EungHyuk Chang) 정회원
1996년 2월: 경찰대학 행정학과 졸업
2010년 3월: 일본 도쿄대학교 법학정치학과 석사
2015년 2월: 고려대학교 법학과 박사
〈관심분야〉 형법, 형사소송법, 형사정책, 비교법 등

김 기 범 (GiBum Kim) 종신회원
1997년 2월: 경찰대학 행정학과 졸업
2009년 2월: 고려대학교 정보보호대학원 공학석사
2017년 2월: 고려대학교 정보보호대학원 공학박사
2014년~2020년: 경찰대학 경찰학과 교수요원
2020년 3월~현재: 성균관대학교 과학수사학과(디지털포렌식) 부교수
〈관심분야〉 경찰, 디지털포렌식, 사이버범죄수사, 정보보호, 국제개발협력 등