JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 27 No. 10, pp. 115-121, October 2022
https://doi.org/10.9708/jksci.2022.27.10.115

The Trends and Prospects of Mobile Forensics Using Linear Regression

Sang-Yong Choi*

*Professor, Dept. of Cyber Security, Yeungnam University College, Daegu, Korea

[Abstract]

In this paper, we analyze trends in the use of mobile forensic technology, focusing on cases where mobile forensics are used, and we predict the development of future mobile forensics technology using linear regression used in future prediction models. For the current status and outlook analysis, we extracted a total of 8 variables by analyzing 1,397 domestic and foreign mobile forensics-related cases and newspaper articles. We analyzed the prospects for each variable using the year of occurrence as an independent variable, seven variables such as text (text message usage information), communication information (cell phone communication information), Internet usage information, messenger usage information, stored files, GPS, and others as dependent variables. As a result of the analysis, among various aspects of the use of mobile devices, the use of Internet usage information, messenger usage information, and data stored in mobile devices is expected to increase. Therefore, it is expected that continuous research on technologies that can effectively extract and analyze characteristic information of mobile devices such as file systems, the Internet, and messengers will be needed As mobile devices increase performance and utilization in the future and security technology.

▸ **Key words**: Mobile Forensic, Cyber Crime, Forensic Tools, Logistic Regression, Prospect

[요 약]

본 논문에서는 모바일 포렌식이 활용된 사례를 중심으로 모바일 포렌식 기술 활용의 동향을 분석하고, 이를 기반으로 미래 예측 모델에 사용하는 선형 회귀 분석을 사용하여 미래 모바일 포렌식 기술의 발전을 전망한다. 현황과 전망분석을 위해 국외 및 국내 모바일 포렌식 관련 사례 및 신문 기사 등 1,397개를 분석하여, 발생 연도를 포함하는 총 8개의 변수를 추출하였다. 발생 연도를 독립 변수로 하고, 텍스트(문자메시지 사용정보), 통신정보(휴대전화 통신정보), 인터넷 사용정보, 메신저 사용정보, 저장된 파일, GPS, 기타 등 7개의 변수를 종속변수로 하여 각 변수에 대한 전망분석 결과 모바일 기기의 다양한 활용 측면 중 인터넷 사용정보, 메신저 사용정보, 모바일 기기에 저장된 데이터 등의 분야에 대한 활용이 증가할 것으로 예상된다. 따라서, 향후 모바일 기기의 성능과 활용성 증가 및 보안기술 향상에 따라 파일시스템, 인터넷, 메신저 등 모바일 기기의 특성 정보를 효과적으로 추출하고 분석할 수 있는 기술에 관한 연구가 지속적으로 필요할 것으로 예상된다.

▸ **주제어**: 모바일 포렌식, 사이버 범죄, 포렌식 도구, 선형 회귀, 전망

• First Author: Sang-Yong Choi, Corresponding Author: Sang-Yong Choi
*Sang-Yong Choi (spikechoi@ync.ac.kr), Dept. of Cyber Security, Yeungnam University College
• Received: 2022. 09. 28, Revised: 2022. 09. 28, Accepted: 2022. 10. 18.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

ICT 기술의 발전에 따라 디지털 기기의 활용이 증가하고 있고, 이는 사용자 편의성을 증가시키는 반면, 디지털 기기를 사용한 범죄 또한 증가시키고 있다. 디지털 기기를 이용한 범죄를 해결하기 위하여 다양한 디지털포렌식 기술이 개발 및 활용되고 있으며 디지털포렌식의 분야는 모바일 포렌식, 디스크 포렌식, 메모리 포렌식 등 다양한 종류가 있다. 최근에는 스마트폰이나 웨어러블 기기 등 모바일 기기들을 사용하는 빈도가 증가하고 있으며 최근에 일어난 대표적인 사례를 살펴보면 텔레그램을 이용하거나, 기밀 자료를 태블릿에 보관하는 등 사이버 범죄에서 모바일 기기가 사용되는 사례가 많아지고 있다. 사이버 범죄 해결을 위해 수사기관에서는 모바일 포렌식 도구를 활용하고 있지만, 암호화 등 기술적인 측면, 기기 파손 등 환경적인 측면에서 한계가 존재하여 완벽하게 복구하지 못하는 것이 현실이다. 더욱이 미래사회가 발전하면서 모바일 포렌식의 활용성은 증가할 것을 예상해보면, 더 완전한 복구를 위해 필요한 모바일 포렌식의 분야를 예상하여 기술 개발을 위해 집중할 필요가 있다.

본 논문에서는 모바일 포렌식이 활용된 다양한 사례를 분석하여 모바일 포렌식이 활용 분야를 분석하고, 분석된 데이터를 활용하여 선형회귀분석 모델에 적용하여 미래 모바일 포렌식의 기술 전망을 분석하여, 미래 모바일 포렌식 기술의 발전 방향을 제안하고자 한다. 본 논문에서는 2장에서 모바일 포렌식의 정의와 모바일 포렌식의 기술, OS(Operation System) 별 모바일 포렌식 도구 등 기술현황 및 현재 국내 및 해외에서 연구 중인 몇 가지 모바일 포렌식 기술을 조사하고 분석한다, 3장에서는 모바일 포렌식이 활용된 약 1,379건의 사례를 조사하여 각 사례에서 활용된 모바일 포렌식의 분야를 분석하고 데이터 세트를 구성한다. 이후, 미래 예측 모델에 자주 사용되는 회귀분석 모델 중 선형 분석을 활용하여 향후 모바일 포렌식의 전망을 예측한다.

II. Related Work

1. Mobile Forensic

모바일 포렌식은 디지털포렌식의 한 분야로, 조사 대상이 되는 스마트폰, 전자수첩 태블릿, 디지털카메라 등 디지털 증거에 저장된 데이터를 추출 혹은 복원하는 기법을 말한다. 모바일 포렌식을 위한 데이터 수집 방법에는 물리적 추출(수집)과 논리적 추출(수집)로 분류할 수 있다[1].

1.1 Physical Extraction

물리적 추출 기술은 모바일 장치 내에 포함된 플래시 메모리 칩에서 모든 데이터를 캡처하는 기술로서 파일시스템을 비트 단위 복사본으로 생성하며 할당되지 않은 공간에도 액세스하여 모든 데이터를 획득할 수 있다. 일반적으로 물리 추출은 JTAG(Joint Test Action Group)케이블로 접속한다[2].

1.2 Logical Extraction

논리적 추출 기술은 모바일 장치에서 파일과 폴더를 추출하는 기술로, 컴퓨터와 동기화시키기 위하여 제조업체의 API(Application Program Interface)를 사용한다. API를 사용하기 때문에 할당되지 않은 공간에는 액세스할 수 없어 휴대전화기의 파일만 복구할 수 있다. 일반적으로 논리 추출은 기기에 접근하기 위해 Bluetooth, 적외선 혹은 케이블을 사용한다[2].

2. Mobile Forensics Technology and tools

2.1 Mobile Forensic Technology

일반적으로 모바일 포렌식에 사용하는 기술은 수동 추출, 잠금장치 우회, 무차별 대입 획득, 논리 추출, 파일시스템 추출, 16진수 덤프, 시스템 내 프로그래밍(ISP), 칩 오프, 마이크로 리드, 클라우드 데이터 수집 등이 있다[3].

수동 추출은 가장 단순한 방법으로 모바일 기기의 잠금을 해제하여 직접적으로 데이터를 추출하는 방식이다. 잠금장치 우회는 잠금 데이터를 삭제 혹은 부팅 프로세스 수정 등 시스템의 취약성을 사용하며 장치가 AFU(After First Unlock) 상태일 때만 사용할 수 있다. 무차별 대입 획득은 PIN 코드를 무한 반복하여 데이터를 획득하는 방식이다. 논리 추출은 USB, Bluetooth 등을 통해 포렌식 하드웨어 혹은 워크스테이션에 연결하여 데이터를 추출하는 방식이다. 파일시스템 추출은 IOS, 안드로이드 등 운영체제별 파일시스템 구조를 분석하여 데이터를 추출하는 방식이며, 비휘발성 메모리에 저장된 데이터를 비파괴적 방법으로 전체 혹은 부분 파일시스템 데이터를 획득하는 방식이다. 16진수 덤프는 코드나 부트로더를 스마트폰에 업로드하여 메모리를 스마트폰에서 컴퓨터로 덤프시켜 데이터를 추출하는 방식으로 삭제 파일을 복원할 수 있다. 시스템 내 프로그래밍은 메모리 판독기를 회로 기판의 칩에 연결하여 액세스한 후, 대상 메모리의 비트 단위 복사본을 생성하는 맞춤형 부트로더를 사용하는 방식이다. 칩

오프는 물리적으로 메모리칩을 제거하여 다른 스마트폰으로 옮겨 데이터를 추출하는 방식으로 기술적으로 까다롭고 메모리칩이 손상되면 추출할 수 없다는 특성이 있으며, JTAG를 사용하여 읽어온다. 마이크로 리드는 칩에서 표시되는 데이터를 수동으로 해석하는 작업으로, 전자 현미경 등을 사용하여 물리적 게이트를 분석한 후 게이트 상태를 0과 1로 변환하여 ASCII 문자로 결정하여 판독하는 방식이다. 이 방식을 사용하기 위해서는 플래시 메모리 및 파일시스템에 대한 광범위한 지식과 교육이 필요하다. 클라우드 데이터 수집은 최근 공급업체에서 제공하는 클라우드 서버에도 모바일 데이터를 저장하기에 해당 업체의 클라우드 서버에 접근하여 데이터를 수집하는 방식으로, 일종의 데이터 마이닝으로 볼 수 있다[4-7].

2.2 Mobile Forensic Tools

모바일 포렌식에서 대표적인 Toolkit은 주로 Android OS와 IOS를 대상으로 하는 툴킷이 주를 이루고 있으며, BlackBerry 같은 OS, 모조 전화기와 같은 비표준 모바일 장치, 중국 칩셋으로 제조된 전화기를 전문적으로 포렌식을 할 수 있게끔 지원을 해주는 툴도 있다. OS에 따른 세부적인 모바일 포렌식 툴은 Table. 1과 같다.

Table 1. Mobile Forensic Tools

Name	Target OS		
	Android	IOS	Etc
Cellebrite UFED[11]	o	o	x
Oxygen Forensics Suite[10][11]	o	x	x
Mobile Phone Examiner Plus[10]	o	o	o
Xry[11]	o	o	x
Lantern[9]	x	o	x
Elcomsoft ios Forensic Toolkit[14]	x	o	x
Belkasoft Evidence Center[15]	o	o	x
Mobiledit Forensic Express[8][9][11]	o	o	x
Micro Systemation XRY[11]	o	o	x
msab(xry)	o	o	x
Encase[8]	o	o	x
FTK[8]	o	o	x
AFLogical OSE[16]	o	x	x
Andriller[11]	o	o	x
FTK Imager Lite[8]	o	o	x
NowSecure Forensics Community Edition[11]	o	o	x
Android Data Extraactor Lite (ADEL)[17]	o	x	x
WahtsApp Xtract[12]	o	o	x
Bulk Extractor[18]	o	x	x

3. Trends in Mobile Forensic Technology Research

현재 모바일 포렌식 기술의 문제점 등을 개선하기 위해서 부 채널 분석, 결함 주입, SoC(System-on-Chip)리버스 엔지니어링, DPE(Distributed Processing Engine)같은 기술들이 연구되고 있다.

부채널 분석은 집적 회로가 기판에서 작동할 때 관련 정보가 전류를 타고 흐르거나 전자기 방출의 형태로 누출될 수 있는 것에서 착안하여, 암호화키와 같은 정보 획득하여 데이터 추출한다. 결함 주입은 불법적인 동작 유발을 목적으로 컨트롤러 장치의 입력을 조작하는 기술로 전원 공급 장치 글리칭, 부족 공급, 전자기 신호 전송 및 광빔 주입 등의 기술을 사용한다. 이는 부트 시퀀스 공격이라고 할 수 있으며, 높은 권한을 가진 코드 추출 등을 위하여 사용한다. SoC 리버스 엔지니어링은 SoC 내부에 물리적 접근을 통해 내부 회로를 검사하는 방식으로, 반도체를 확인하는 방식이다. DPE는 분산된 데이터를 네트워크를 통해 여러 대의 컴퓨터에 나누어 처리하는 시스템으로, 대용량 디지털 저장매체에 대해 효율적인 분석이 가능하다. 파일 카빙 기법은 시그니처 정보를 알아야 수집한 데이터의 이미지 파일을 재조합할 수 있지만, 암호화된 디지털 이미지의 경우 시그니처 정보가 없으므로, 메타데이터와 같은 부가정보가 없는 데이터의 단편 조각 간 인접-상관도를 측정하고 재조합하여 주는 기술이라고 하며, Header/Footer, Header/File Size, Header/Ram Slack, 파일구조 검증 4가지 기법이 존재한다[4-5].

III. Analysis of Mobile Forensics Technology Prospects Using Cases

1. Prediction Methodology

1.1 KDD Analysis Methodology

KDD(Knowledge Discovery in Database) 분석 방법론은 1996년 Fayyad가 소개한 방법론으로 데이터를 통해 통계적 패턴이나 지식을 찾을 수 있도록 정리한 데이터마이닝 프로세스이다. 데이터마이닝, 기계학습, 인공지능, 패턴인식, 데이터 시각화에서 응용될 수 있는 구조를 갖추고 있다. KDD 분석 방법론은 데이터 셋 선택, 데이터 전처리, 데이터 변환, 데이터마이닝, 결과 평가로 이루어져 있다[19].

1.2 CRISP-DM Analysis Methodology

CRISP-DM 방법론은 전 세계에서 가장 많이 사용되는데이터 마이닝 표준 방법론으로 단계, 일반과제, 세부과제, 프

로세스 실행 등의 4가지 레벨로 구성된 계층적 프로세스 모델이다. CRISP-DM의 절차는 Data Understanding, Data Preparation, Modeling, Evaluation, Deployment, Business Understanding과 같이 6단계로 구성되며, 각 단계는 순차적으로 진행되는 것이 아니라, 필요에 따라 단계 간의 반복 수행을 통해 분석의 품질을 향상시킨다[9].

1.3 Linear Regression Analysis - Regression curve

선형 회귀는 다양하게 연구되고, 널리 사용되고 있는 회귀분석 기법이며 종속변수 y와 한 개 이상의 독립 변수(또는 설명 변수) x와의 선형 상관관계를 모델링 하는 분석기법이다. 선형 예측 함수를 사용해 회귀식을 모델링 하며, 알려지지 않은 파라미터는 데이터로부터 추정한다.

선형 회귀는 여러 사용 사례가 있지만, 값을 예측하는 것이 목적일 경우, 선형 회귀를 사용해 데이터에 적합한 예측 모형을 개발한다. 개발한 선형 회귀식을 사용하여 y가 없는 x값에 대해 y를 예측하기 위하여 사용할 수 있다. 일반적으로 다음과 같이 최소제곱법(least square method)을 사용해 선형 회귀 모델을 세운다.

$$y_i = \beta_1 \chi_{i1} + \cdots + \beta_p \chi_{ip} + \epsilon_i = \chi_i^T \beta + \epsilon_i, i = 1, \ldots, n,$$

주어진 식에서 $^{\beta_i}$는 각 독립 변수의 계수이며, p는 선형 회귀로 추정되는 모수의 개수이다. T는 전치를 의미하고, $\chi_i^T \beta$는 χ_i와 β의 내적을 의미한다. ϵ_i는 오차항, 오차항 변수로, 관찰되지 않은 확률 변수이며, 종속변수와 독립변수 사이에 오차를 의미한다. 이것이 선형 회귀라 불리는 것은, 종속변수가 독립 변수에 대해 선형 함수(1차 함수)의 관계에 있을 것이라 가정하기 때문이다. 선형 회귀는 데이터를 통해 미래를 예측하고자 할 때 주로 사용된다. 비용 예측, 고정 투자 예측, 재고 관리 예측, 필요 유동 자산 예측, 노동 수요 예측, 노동 공급 예측 등에 선형 회귀를 사용할 수 있다. 이러한 이유로 본 논문 연구에서는 전망분석을 위해 선형회귀분석법을 선택했다[20].

2. Mobile Forensics Forecast Analysis

데이터 셋은 Table. 2와 같이 국내 법원, 해외 법원, 국내 기사에 나와 있는 사례들을 조사하여 총 1,397개를 생성하였으며, 분석에 사용된 변수는 발생 연도, 텍스트(SMS 사용정보), 통신정보(휴대전화 통신정보), 인터넷 사용정보, 메신저(SNS) 사용정보, 저장된 파일, GPS, 기타 앱 및 악성코드를 포함하는 Etc 등 Table. 3과 같이 총 8개로 구성하였다. Table. 3의 Total Count는 연도에 관계

Table 2. RAW Data

No	Year	Text	Call	Internet	Messenger/ SNS	Data	GPS	Etc	Source
1	1992	1	1	0	0	0	0	0	https://casetext.com/case/us-v-slater-7
2	2000	0	0	0	0	0	0	0	https://caselaw.findlaw.com/nc-court-of-appeals/1201672.html
3	2002	0	0	0	0	0	0	0	https://www.post-gazette.com/news/crime-courts/2019/10/02/scott-tyree-alicia-kozakiewicz-sex-offender-sentenced-violating-parole-pittsburgh-harrisburg/stories/201910020149
4	2002	0	0	0	0	0	0	0	https://casetext.com/case/com-v-kelley-3
5	2004	0	1	0	0	0	1	0	https://casetext.com/case/united-states-v-mahon-3
6	2004	1	0	0	0	0	0	0	https://casetext.com/case/people-v-cunnigham
7	2005	0	0	0	0	0	0	0	https://www.biography.com/news/btk-killer-dennis-rader-timeline
8	2005	0	0	0	0	0	0	0	https://law.justia.com/cases/alabama/court-of-appeals-criminal/2010/08-1767.html
9	2005	0	0	0	0	0	0	0	https://casetext.com/case/state-v-bettis-2
10	2006	0	1	0	0	0	0	0	https://casetext.com/case/people-v-vu-5
					~~				
1373	2019	0	0	1	0	0	0	0	https://www.edaily.co.kr/news/read?newsId=03630966622491544&mediaCodeNo=257&OutLnkChk=Y
1374	2019	0	0	0	0	1	0	0	https://www.usmbc.co.kr/article/iVJKLte0Yytvc
1375	2019	0	0	1	0	0	0	0	http://www.mediajeju.com/news/articleView.html?idxno=316715
1376	2019	0	0	0	0	1	0	0	https://www.chosun.com/site/data/html_dir/2019/06/05/2019060502171.html?utm_source=naver&utm_medium=original&utm_campaign=news
1377	2019	0	0	0	0	0	0	0	https://www.news1.kr/articles/?3639867
1378	2019	1	1	0	0	0	0	0	https://news.kbs.co.kr/news/view.do?ncd=4218491&ref=A
1379	2019	0	0	0	0	0	0	0	https://newsis.com/view/?id=NISX20190612_0000678706&cID=10810&pID=10800

Table 3. Variables and Total Count

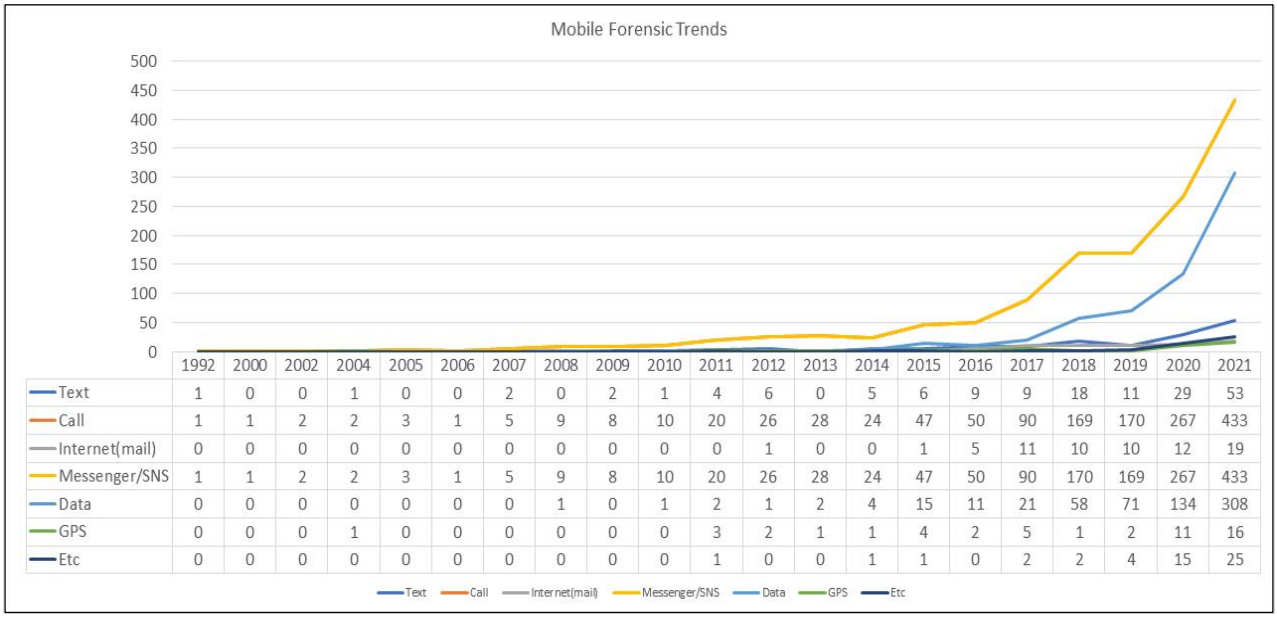
Variables	Value	Total Count
Year	20XX	1,379
Text	1,0	158
Call	1,0	153
Internet(mail)	1,0	73
Messenger/SNS	1,0	202
Data	1,0	633
GPS	1,0	53
Etc	1,0	51

없이 총 1,379건의 사례 가운데 해당 변수가 사용된 횟수를 나타낸다. 분석대상 총 1,379건의 사례 중 모바일 포렌식에서 가장 많이 사용된 정보는 Data임을 알 수 있으며, Messenger, Text, Call 등의 정보가 모바일 포렌식에 많이 사용되었다.

수집한 데이터를 연도별, 분야별로 확인한 결과 Fig. 1과 같이 Call, Messenger(SNS), Data 등의 정보에 대한 포렌식 빈도가 최근들어 급격하게 상승하고 있는 것을 확인할 수 있었다. 이는 최근 스마트 기기의 보급률 및 사용률 증가에 따른 현상인 것으로 분석된다. 특이할 만한 점은 모든 모바일 포렌식 모든 분야가 증가하고 있는 것을 확인할 수 있다.

독립 변수는 향후 포렌식 분야를 추정하기 위하여 범죄 발생 연도로 지정하였다. 종속변수에는 모바일 기기 포렌식에 사용된 기술범위의 전망을 예측하기 위해 나머지 변수를 모두 사용하였다. 독립 변수에는 모두 발생 실제 연도를 기입하였으며 종속변수는 참이면 1, 거짓이면 0으로 표시하였다.

선형회귀분석 알고리즘을 이용하여 모바일 포렌식의 기술 전망을 분석한 결과 텍스트와 Call 정보는 Fig. 2, Fig. 3에서 보여주는 것처럼 사용 빈도가 점차 감소할 것으로 예상된다. 이는 최근에는 전화 통화보다 카카오톡, 텔레그램 등 SNS의 활용이 증가함에 따른 것에 기인한 것으로 분석된다. 반면 Fig. 4 ~ Fig. 7에 보이는 바와 같이 인터넷(email 포함) 사용정보와 Messenger/SNS, Data, Etc 등의 정보는 시간이 지나갈수록 사용률이 높아지는 것을 확인할 수 있었다. 특히 두드러진 증가세를 보이는 분야는 Messenger/SMS와 저장된 파일을 의미하는 Data 분야이다. 이는 최근 업무의 환경이 카카오톡, 텔레그램과 Facebook, Instagram 등 SNS를 활용하는 빈도가 높아짐에 기인하는 것으로 예상되며, 모바일 기기의 성능이 향상되고, 활용성이 높아짐에 따라 모바일 기기에 저장되는 파일과 데이터의 양 또한 증가할 것으로 예상되는 것에 기인하는 것으로 분석된다. 따라서 향후 모바일 포렌식의 기술은 모바일 기기를 컴퓨터시스템과 같은 요소로 인정하고 모바일 기기의 파일시스템을 추출하는 기술, 모바일 기기 응용프로그램 디버깅 또는 리버싱 기술과 같은 모바일 기기에 특화된 디지털포렌식 기술개발이 지속적으로 필요할 것으로 전망한다. 그래프에서 관심 있게 보아야 할 다른 측면은 악성코드를 포함한 기타 앱 분석의 필요성이 증가하고 있다는 점이다. 이는 과거와는 달리 모바일용 악성코드가 증가하고, 다양한 앱이 출시됨에 따라 향후 모바일 악성코드 분석기술 또한 필요할 것으로 예상할 수 있다.



	1992	2000	2002	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Text	1	0	0	1	0	0	2	0	2	1	4	6	0	5	6	9	9	18	11	29	53
Call	1	1	2	2	3	1	5	9	8	10	20	26	28	24	47	50	90	169	170	267	433
Internet(mail)	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	5	11	10	10	12	19
Messenger/SNS	1	1	2	2	3	1	5	9	8	10	20	26	28	24	47	50	90	170	169	267	433
Data	0	0	0	0	0	0	0	1	0	1	2	1	2	4	15	11	21	58	71	134	308
GPS	0	0	0	1	0	0	0	0	0	0	3	2	1	1	4	2	5	1	2	11	16
Etc	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	2	2	4	15	25

Fig. 1. Mobile Forensic Trends

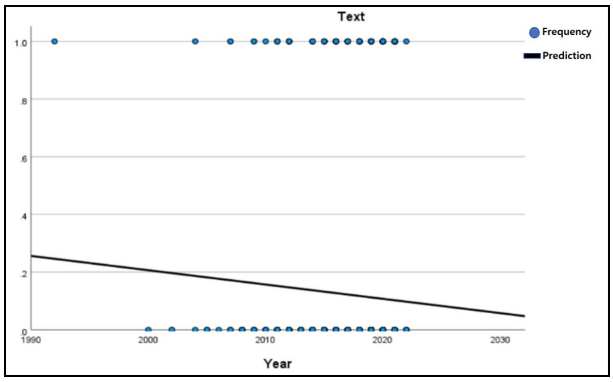


Fig. 2. Text

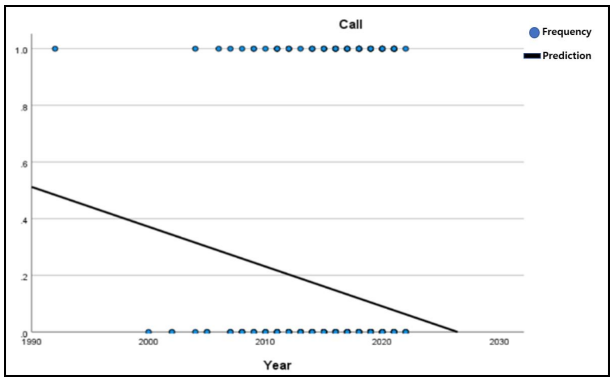


Fig. 3. Call

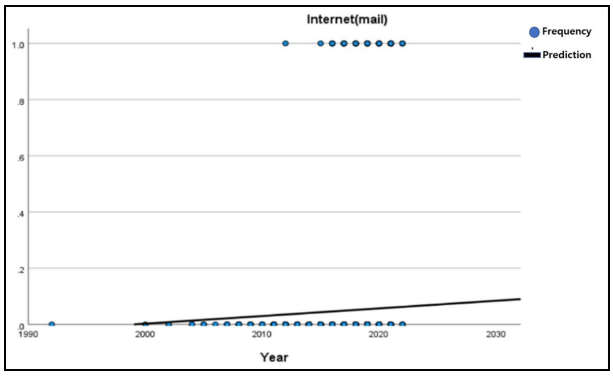


Fig. 4. Internet

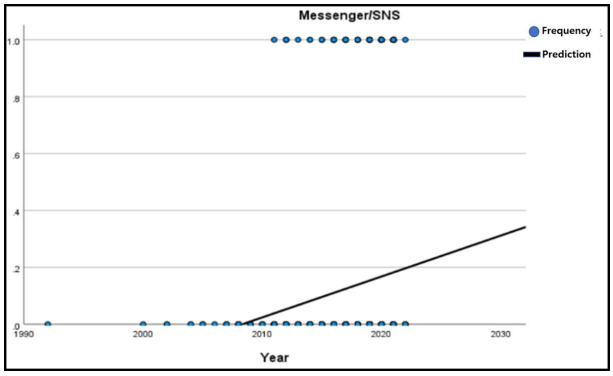


Fig. 5. Messenger/SNS

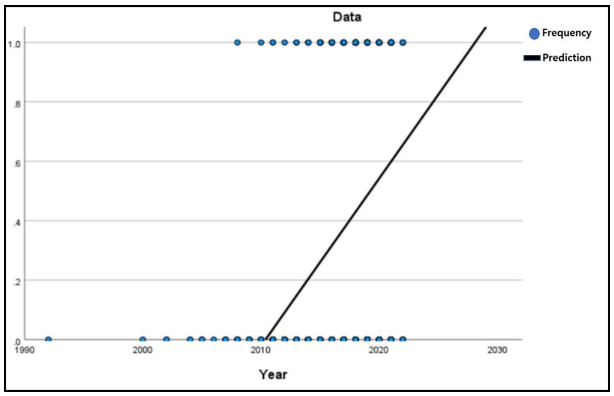


Fig. 6. Data

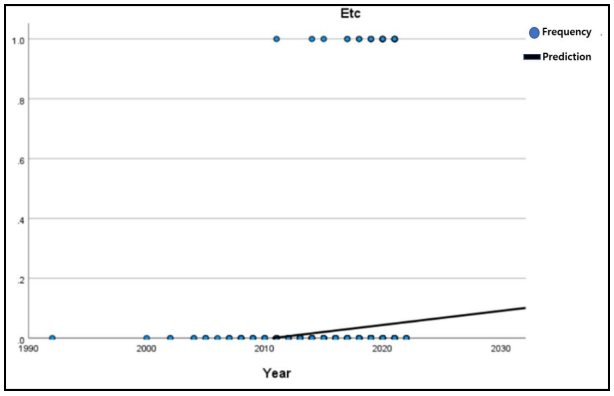


Fig. 7. Etc

IV. Conclusions

ICT 기술이 발전함에 따라 모바일 기기의 범죄 사용 빈도가 증가하는 반면에 모바일 포렌식 기술에 대한 발전 속도는 이를 따라가지 못하고 있다. 본 논문에서는 모바일 포렌식에 관한 다양한 사례를 조사하고, 사례분석 결과를 기반으로 선형회귀분석 모형을 사용하여 미래 모바일 포렌식의 기술적 발전 방향을 예측하였다. 예측 결과 모바일 포렌식에서는 Data를 추출하는 기술, Messenger/SNS 포렌식 기술 등에 대한 지속적인 연구와 기술개발이 필요할 것으로 예상되었다. 다만, 데이터 셋을 구성할 때 국내·외 법원 판례 및 기사에서 자료를 조사하였지만, 존재하는 모든 사례를 조사할 수 없어 데이터 셋에 한계가 있었다. 향후 보다 많은 데이터 셋을 구성하여 예측분석 모형을 만든다면 더 정확한 예측이 가능할 것으로 예상된다. 또한, 조사한 정보에 따르면 여러 국가 및 기관 등에서 서로 다른 표준을 지정하고 다양한 포렌식 도구들을 활용하여 데이터를 추출해 증거로 사용하고 있다. 모바일 포렌식에 사용되는 기술과 도구가 다르며 추출할 수 있는 데이터 역시

차이가 있기 때문에 모바일 포렌식에 대한 기술표준 등에 관한 연구도 지속되어야 할 것이다.

ACKNOWLEDGEMENT

This work was supported by the Yeungnam University College Research Grants in 2021

REFERENCES

[1] Fakhar Imam, Common mobile forensics tools and techniques, https://resources.infosecinstitute.com/topic/common-mobile-forensics-tools-techniques/

[2] Tript, What is JTAG & Chip-Off Forensics?, https://www.octodigitalforensics.com/what-is-jtag-chip-off-forensics/

[3] Satish Bommisetty, Rohit Tamma, Heather Mahalik, "Practical Mobile Forensics" Packt Publishing, chapter1 Section 4, July, 2014

[4] Aya Fukami, Radina Stoykova, Zeno Geradts, “A new model for forensic data extraction from encrypted mobile devices”, Forensic Science International: Digital Investigation, Vol. 38, Sep. 2021. DOI : https://doi.org/10.1016/j.fsidi.2021.301169

[5] Yi Jeong Hoon, Park Dea Woo, "A Study on Mobile Forensic Extraction Methods of Cellular and Smart Phone", Journal of Korea Society of Digital Industry and Information Management, Vol.6 No.3,, pp..79-89, Sep. 2010. DOI : https://doi.org/10.17662/ksdim.2010.6.3.079

[6] Kevin Curran, Andrew Robinson, Stephen Peacocke, Sean Cassidy, "Mobile Phone Forensic Analysis", International Journal of Digital Crime and Forensics, Vol. 2, No. 3 Volume 2, Issue 3, Article 2, pp.15~27, Sep. 2010. DOI : https://doi.org/10.4018/jdcf.2010070102

[7] Yoon Kyung-Bae, Chun Woo-Sung, Park Dea-Wo, "Forensic Evidence of Search and Seized Android and Windows Mobile Smart Phone", Journal of the Korea Institute of Information and Communication Engineering, Vol. 17, No. 2, pp..323-331, Feb. 2013. DOI : https://doi.org/10.6109/jkiice.2013.17.2.323

[8] Oluwafemi Osho, Sefiyat Ohida, "Comparative Evaluation of Mobile Forensic Tools", International Journal of Information Technology and Computer Science, Volume 8, Issue 1, pp. 74-83, Jan. 2016. DOI : https://doi.org/10.5815/ijitcs.2016.01.09.

[9] Utkarsha Shukla, Bishwas Mandal, Kiran Kasula, "Perlustration on Mobile Forensics Tools", Computer Networks and Inventive Communication Technologies, pp. 1225-1231. Apr. 2021 DOI : https://doi.org/10.1007/978-981-15-9647-6_97

[10] Ritika Lohiya, Priya John, Pooja Shas, "Survey on Mobile Forensics", International Journal of Computer Applications, International Journal of Computer Applications, Vol. 118, No.16, pp. 6-11, May, 2015. DOI : https://doi.org/10.5120/20827-3476

[11] Nihar Ranjan Roy, Anshul Kanchan Khanna, Leesha Aneja, "Android phone forensic: Tools and techniques", 2016 International Conference on Computing, Communication and Automation (ICCCA), pp. 605-610, Apr. 2016. DOI : https://doi.org/10.1109/CCAA.2016.7813792

[12] Rusydi Umar, Imam Riadi, Guntur Maulana Zamroni, "Mobile Forensic Tools Evaluation for Digital Crime Investigation", International Journal on Advanced Science, Engineering and Information Technology, Vol. 8, No. 3, pp. 949-955, 2018. DOI : https://doi.org/10.18517/ijaseit.8.3.3591

[13] Ana Lucila Sandoval Orozco, Jocelin Rosales Corripio, David Manuel Arenas González, Luis Javier García Villalba, "Theia: a tool for the forensic analysis of mobile devices pictures", Computing Vol. 98 No.12 , pp. 1251~1286, Jan. 2016. DOI : https://doi.org/10.1007/s00607-015-0482-5

[14] Elcomsoft, https://www.elcomsoft.com/DS/Datasheet_Mobile.pdf

[15] Belkasoft, https://belkasoft.com/x

[16] Open source Android Forensics app and framework, https://github.com/nowsecure/android-forensics

[17] Android Data Extractor Lite, https://github.com/mspreitz/ADEL

[18] Bulk Extractor, https://github.com/simsong/bulk_extractor

[19] Leekangjoon, “Traditional data analytics methodologies.: KDD, CRISP-DM”, https://www.2e.co.kr/news/articleView.html?idxno=301010

[20] Wikipedia, “linear regression”, https://ko.wikipedia.org/wiki/%EC%84%A0%ED%98%95_%ED%9A%8C%EA%B7%80

Authors

Sang-Yong Choi received his B.S. degree in Mathematics and M.S. degree in Computer Science, both from Hannam University in 2000 and 2003, and Ph.d degree in Interdisciplinary of Information Security from Chonnam National University in 2014, Dr. Choi is a assistant professor at the Dept. of Cyber Security in Yeungnam University College, Daegu, Korea. His research interests are in web security, network security and cloud computing security.