2024년 2/4분기

정보보호 인적자원개발위원회(ISC)

ISSUE REPORT

디지털포렌식 전문인력 양성 및 거버넌스 구축 방안

정보보호 인적자원개발위원회
Information Security Industrial Skills Council

CONTENTS

정보보호 인적자원개발위원회 사무국 02-6748-2011, 2039 | mhr0327@kisia.or.kr

본 이슈리포트는 군산대학교 법행정경찰학부 권양섭 교수, 성균관대학교 과학수사학과 김기범 교수가 작성하였습니다.

요약

□ 논의 배경

- ○ 국내 디지털포렌식 시장은 2016년 401억원에서 2021년 537.3억원으로 연평균 약 482억원의 규모로 추정되고, 최근 6년간 약 34% 증가한 것으로 추산되며, 2022년에서 2031년까지 총 10년간 연평균 약 668억원의 규모일 것으로 전망
- ○ 경찰청의 디지털포렌식 건수는 2019년 56,440건에서 2023년 79,433건으로 최근 5년간 총 22,993건(40.7%) 증가
- ○ 디지털포렌식은 법과학분야 전문영역으로, 법과 기술 능력이 모두 요구되는 융복합 영역, 사회적 책임성과 높은 직업윤리가 요구되는 분야로 발전
- ○ 디지털포렌식은 범죄 수사에서뿐만 아니라 각종 행정조사, e-디스커버리, 기업 내부감사, 민간 디지털포렌식 서비스 등에서 폭넓게 활용

□ 국내 디지털포렌식 전문인력 양성 현황

- ○ 대학에서 디지털포렌식 학과를 운영하는 사례는 아직까지 없고, 전공 형태로 군산대학교, 한림대학교, 동서대학교에서 운영 중
- ○ 대학원은 맞춤형 석사과정을 통합하여 일반·전문·특수 대학원으로 서울대·고려대·동국대·성균관대·동서대 등에서 디지털포렌식 관련 학과와 전공 운영
- ○ 한국인터넷진흥원은 매년 '최정예 정보보호 전문인력 양성(K-Shield)' 일환으로 디지털포렌식 교육과정 운영
- ○ 디지털포렌식 분야는 법학과 공학의 융복합 영역으로써 법절차, 기술, 디지털포렌식 TOOL 활용 능력을 요구하고 있으므로 융복합 교육과정의 운영을 통해 전문인력 양성 필요

□ 국내·외 디지털포렌식 자격제도 및 NCS 운영 현황

- ○ (사)한국포렌식학회와 한국인터넷진흥원이 공동으로 '디지털포렌식 전문가 자격'을 발행하고 있으며 수사기관에서는 자체적인 전문수사관 인증제도 운영
- ○ 우리나라에서는 디지털포렌식 자격증이 민간공인자격 형태로 1개만 운영되고 있지만, 미국 등 선진국에서는 다양한 형태의 디지털포렌식 자격제도 운영
- ○ 디지털포렌식 수요가 증가하고 디지털포렌식 직무에 대한 표준이 사회적으로 요구되어 2020년 디지털포렌식 국가직무능력표준(NCS, National Competency Standards) 개발·배포

□ 디지털포렌식 거버넌스 구축과 입법적 과제

- 수사기관, 조사기관, 정부부처, 연구소, 민간기업 등 다수 이해관계자의 등장으로 기능과 역할 구분을 통한 발전 방안 마련이 필요하며, 디지털포렌식은 국가안보와 직결 및 형사사법 역량과 신뢰도를 결정짓는 요소로 작용하고 있는 동시에, 계속 등장하는 기술적 난제 대응과 시장/산업 경쟁력 확보가 필요하므로 거버넌스 구축 필요
- 유비쿼터스 컴퓨팅 환경이 확대됨에 따라 디지털 데이터를 수집하는 과정에서 법률적 한계에 봉착하는 상황 발생
- 디지털포렌식은 범죄수사와 같은 공공영역뿐만 아니라 민간영역에서도 다양하게 활용되고 있으므로 무분별한 디지털포렌식 업체의 난립을 방지하기 위해서라도 시급히 인력 수행자격에 대한 기준 마련 필요
- 미국 및 선진국에서는 디지털포렌식 기술 및 절차와 관련하여 다양한 보고서 및 가이드라인을 제작하여 배포하고 있으며, 우리나라도 이와 같은 기술 표준의 제작·배포 시급
- 도구 검증은 디지털포렌식에 의해 수집된 증거의 진정성을 담보할 수 있는 전제조건이므로 국가가 직접 도구 검증을 위한 제도 신설 필요

□ 시사점 및 제언

- 디지털포렌식 수요와 중요성을 고려할 때 고등교육기관에서 전문인력을 양성해야 하며, 정부는 대학에 예산을 지원하여 전문인력을 양성할 수 있는 환경 조성 필요
- 우리나라에서는 1개의 디지털포렌식 자격만 운영되고 있으므로, 공신력 있는 기관에서 디지털포렌식 관련 자격을 개발하여 전문가로서의 위상과 신뢰성이 담보된 자격제도 운영 필요
- 디지털포렌식 거버넌스 구축을 위해서는 우선적으로 디지털포렌식의 주요 요소라고 볼 수 있는 법절차, 자격, 기술 표준, 도구 검증에 관한 입법이 필요하며, 거버넌스 운영을 위해서는 국가가 디지털포렌식 부문을 주도적으로 견인해 나가는 것이 타당

I.

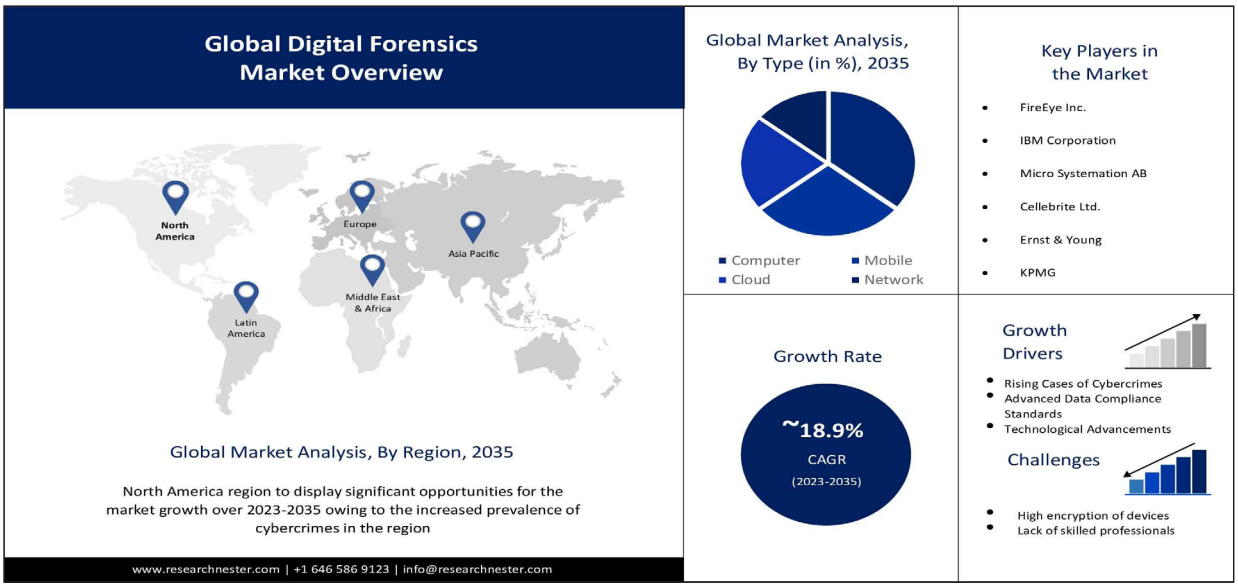
논의 배경

Ⅰ 논의 배경

1. 디지털포렌식 수요현황

○ 정보분석社인 Research Nester는 디지털포렌식 시장규모에 대해 2023~2035년간 연평균 성장률(Compound Annual Growth Rate, CAGR) 약 18.90% 성장 전망[1)]

▪ 구체적으로 2022년 110억 달러에서 2035년 860억 달러까지 확대될 것으로 예측



[그림 1] 디지털포렌식 시장 규모 예측(2023-2035)

○ 국내 디지털포렌식 시장은 2016년 401억원에서 2021년 537.3억원으로 연평균 약 482억원으로 추정되고, 최근 6년간 약 34% 증가한 것으로 추산[2)]

▪ 2022년에서 2031년까지 총 10년간 연평균 약 668억원으로 전망

○ 경찰청의 디지털포렌식 건수는 2019년 56,440건에서 2023년 79,433건으로 최근 5년간 총 22,993건(40.7%) 증가[3)]

▪ 대검찰청의 디지털포렌식 건수는 2012년 5,921건에서 2016년 13,172건으로 4년간 약 122% 증가[4)]

1) Research Nester 홈페이지, https://www.researchnester.com/kr/reports/digital-forensics- market/4832(최종확인 2024.6.25.)
2) 백현정, 「디지털포렌식 시장추산 및 예측에 관한 연구」, 성균관대학교 과학수사학과(대학원) 석사학위, 2022, 43p.
3) 경찰청 통계자료(2024)
4) 대검찰청 통계자료(2017)

○ HM컴퍼니가 2022년 국내 200여개 기업 내부감사인을 대상으로 디지털포렌식의 필요성에 대해 설문조사한 결과, 총 22.4%가 '매우 필요'하다고 응답하였고, 디지털포렌식 수행을 위한 환경구축은 약 58.2%가 '아니오'라고 응답[5)]

▪ 디지털포렌식에서 애로사항은 '전문인력 부족'(33.3%), 경영진의 반대(19.5%), 높은 비용(18.5%), 피감부서 반발(18.5%), 기대이하 성과(10.2%) 순 응답

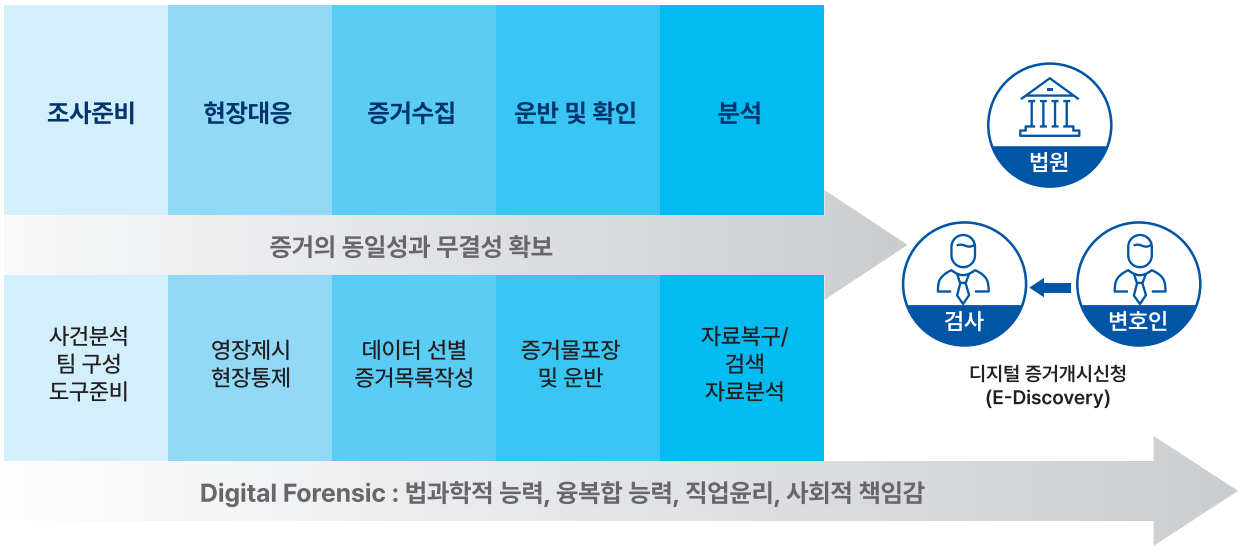
2. 디지털포렌식 영역의 전문성

○ 디지털포렌식은 단순히 디지털 기기나 저장매체 등에서 삭제된 데이터를 복구하거나 필요한 자료를 추출하는 작업이 아니며, 디지털정보를 통해 사실을 입증하는 법과학의 한 분야로 전문영역에 해당

○ 컴퓨터 등 IT 기술능력뿐만 아니라 법절차에 대한 전반적인 이해를 요구하고 있다는 점에서 법과 기술능력이 모두 요구되는 융복합 영역에 해당

○ 범죄 수사나 행정조사에 있어서는 유죄와 위법행위를 판단할 수 있는 증거를 제공한다는 점에서 사회적 책임이 높은 영역에 해당

○ 타인의 사생활과 비밀의 자유를 침해할 수 있는 정보를 다룬다는 점에서 높은 직업윤리와 비밀준수의무를 부담하는 영역에 해당



[그림 2] 디지털포렌식 수행절차와 전문성

5) 조세일보 보도(2022.3.31.), "내부감사에 디지털포렌식·리뷰 플랫폼 필요해", https://m.joseilbo.com/ news/view.htm?newsid=450527#_enliple(최종확인 2024.6.25.)

3. 디지털포렌식 활용 분야

○ 범죄 수사

▪ 모든 수사는 디지털에서 시작하여 디지털로 끝난다는 말이 있듯이 범죄 수사에 있어서 디지털포렌식은 필수적인 수사 방법이며 모든 범죄 사건의 해결에 결정적인 역할 수행

○ 행정조사

▪ 공정거래위원회, 국세청, 감사원, 고용노동부 등에서는 행정조사를 진행하는 과정에서 디지털포렌식을 활용하고 있으며, 각각의 기관에는 수사기관 못지않은 디지털포렌식 장비와 인력 구비

○ e-디스커버리[6)]

▪ 우리나라의 민사소송에서는 아직 e-디스커버리가 도입되지 않았으나 미국 등 선진국에서는 e-디스커버리 제도가 민사소송 등에서 시행되고 있으며, e-디스커버리 과정에서 디지털포렌식 기술과 절차 활용

○ 기업 내부감사

▪ 기업 내의 부정행위, 갑질·성희롱, 징계 조사 등에서도 디지털포렌식이 활용되고 있으며, 기업의 업무환경이 모두 디지털화됨에 따라 일반적인 기업의 내부감사에서도 디지털포렌식 활용

○ 민간 디지털포렌식 서비스

▪ 민사소송에서의 증거 제출, 내부 징계에서의 반박 자료 등 특정 행위나 사실관계를 입증하기 위해 디지털포렌식 민간기업에 분석을 의뢰하는 경우 증가 추세

6) e-디스커버리(e-Discovery, Electronic Discovery)는 민사소송이나 형사소송에서 전자적으로 저장된 정보(ESI, Electronically Stored Information)를 수집, 보존, 검토, 분석, 제출하는 절차를 의미, 미국 등의 민사소송에서는 법원의 e-디스커버리 명령을 위반할 경우, 다양한 제재 조치가 적용될 수 있으며, 이는 소송의 결과에 중대한 영향을 미칠 수 있기 때문에 모든 당사자는 e-디스커버리 규정을 엄격히 준수해야 함

II.

국내 디지털포렌식 전문인력 양성 현황

II 국내 디지털포렌식 전문인력 양성 현황

1. 대학(원) 운영현황

○ 정규 대학(원) 교육과정

▪ 대학에서 디지털포렌식 학과를 운영하는 사례는 아직 없으며, 전공 형태로 군산대학교, 한림대학교, 동서대학교에서 운영 중

연번	학교명	학과/전공명
1	군산대학교	법행정경찰학부+컴퓨터소프트웨어학부(디지털포렌식융합전공)
2	동서대학교	정보보호학과+경찰행정학과(사이버경찰보안융합연계전공)
3	한림대학교	융합과학수사학과(경찰과학수사융합전공)

[표 1] 대학의 디지털포렌식 전공 운영 현황

▪ 대학원은 일반·전문·특수 대학원으로 고려대·동국대·성균관대·동서대 등에서 디지털포렌식 관련 학과와 전공 운영 중

연번	학교명	대학원	학과/전공명
1	경찰대학	치안대학원(일반)	미래치안과학융합학과
2	고려대학교	정보보호대학원(전문)	정보보호학과(디지털포렌식 전공)
3	동국대학교	경찰사법대학원(특수)	과학수사학 전공
4	동국대학교	국제정보보호대학원(특수)	사이버포렌식 전공
5	동서대학교	일반대학원	디지털포렌식학과
6	성균관대학교	일반대학원	과학수사학과(디지털포렌식 전공)
7	한림대학교	융합과학수사학과(일반)	융합과학수사학과

[표 2] 대학원 디지털포렌식 관련 학과·전공 현황

○ 맞춤형 대학원 교육과정

▪ 대검찰청은 서울대에, 경찰청은 고려대·연세대·성균관대 중에서 사업자를 선정하여 디지털포렌식에 대한 맞춤형 석사과정 운영 중

학교	서울대학교 [7]	연세대학교 [8]	고려대학교 [9]	성균관대학교 [10]
학과명	융합과학기술대학원 (수리정보과학과)	정보대학원 (디지털포렌식과정)	정보보호대학원 (디지털포렌식학과)	일반대학원 (디지털포렌식학과)
교과목	• 정보보호이론 • 디지털포렌식 • 디지털포렌식 실습 및 특강 • 디지털증거법 • 정보보호법 • 소프트웨어 및 시스템 보안 • 수리암호 • 컴퓨터학 • 수리정보과학 특강	• 정보보호 이론 • 디지털포렌식 연구방법론 • 디지털포렌식 실무 • 디지털포렌식 고급 • 디지털증거 관련 법률과 정책 • 사이버 법률과 정책 • 최신 사이버 범죄론 • 악성코드 분석과 역공학 • 침해사고 분석 및 대응 • 가상자산과 금융보안 등	• 정보보호이론 • 디지털포렌식개론 • 디지털포렌식실무 • 윈도우포렌식 • 디지털증거법 • 사이버법률 • 사이버범죄조사기법 • 침해사고대응관리 • 악성코드 및 역공학 • 전문가증언 • 암호화폐 등	• 정보보호 이론 • 디지털포렌식 세미나 • AI와 디지털포렌식 • 디지털포렌식기술 • 디지털포렌식법제 • 사이버포렌식판례 • 사이버범죄수사 • 침해사고 대응

[표 3] 국내 맞춤형 석사과정으로 디지털포렌식학과 운영 현황

2. 정부지원 사업

○ 교육훈련

- 한국인터넷진흥원은 매년 '최정예 정보보호 전문인력 양성(K-Shield)' 일환으로 디지털포렌식 교육과정 운영 중[11]
- 세부적으로 △침해사고 로그분석을 위한 디지털포렌식, △포렌식을 활용한 기업보안사고 대응, △디지털포렌식 현장대응 감사기법, △디지털포렌식 분석기법 실습, △디지털포렌식 관리자 과정, △인증서 취득과정(디지털포렌식 분야) 운영

7) 서울대학교 홈페이지, https://mis.snu.ac.kr/academic/subjects.php (최종확인, 2024.6.26.)
8) 연세대학교 홈페이지, https://gsi.yonsei.ac.kr/course/c9.asp (최종확인, 2024.6.25.)
9) 고려대학교 홈페이지, https://gss.korea.ac.kr/ime/about/curriculum.do (최종확인, 2024.6.26.)
10) 성균관대학교 홈페이지, https://skb.skku.edu/forensic/under/under_course01.do (최종확인, 2024.6.26.)
11) 한국인터넷진흥원 홈페이지, https://www.kisa.or.kr/402/form?postSeq=2384#fnPostAttachDownload (최종확인, 2024.6.26.)

연번	과정명	훈련시간	정원	교육비(원)	훈련일정
1	침해사고 로그분석을 위한 디지털포렌식	18H(3일)	15	71,130	1차 5/27(월)-29(수) 2차 6/19(수)-21(금)
2	포렌식을 활용한 기업보안사고 대응	21H(3일)	15	83,370	1차 4/15(월)-16(수) 2차 5/22(수)-24(금) 3차 6/12(수)-14(금)
3	디지털포렌식 현장대응 감사기법	18H(3일)	15	71,460	1차 8/7(수)-9(금)
4	디지털포렌식 분석기법 실습	18H(3일)	15	71,390	1차 9/30(월)-10/2(수) 2차 10/23(수)-24(금)
5	디지털포렌식 관리자 과정	18H(3일)	15	71,460	1차 9/4(수)-6(금) 2차 9/30(월)-10/2(수)
6	인증서 취득과정(디지털포렌식 분야)	4H(1일)	10	15,800	1차 11/8(금)

[표 4] K-Sheild 디지털포렌식 관련 교육 과정(2024)

○ 국가 연구개발(R&D)[12]

연번	과제명	주무기관	수행기관	기간
1	해양사고 디지털증거 무결성 및 증거능력 확보를 위한 항해장비 포렌식 기법 개발	해양경찰청	ETRI	2019-2022
2	자율주행 차량제어 주체판별을 위한 디지털 포렌식 원천기술 연구	과학기술정보통신부	한림대학교	2022-2025
3	인공지능 기술 활용 디지털증거 분석기법 개발	〃	동국대학교	2022-2025
4	디지털 환경에서의 증거인멸행위 증명 및 대응기술 개발	〃	성균관대학교	2024-2027
5	AI 저작권침해 콘텐츠 식별·탐지를 위한 저작권 포렌식 수집 도구 기술 개발	한국콘텐츠진흥원	〃	2024-2025
6	한류콘텐츠 보호를 위한 국제공조수사 협력 체계 기술 개발	〃	〃	2024-2026

[표 5] 디지털포렌식 분야 국가 연구개발(R&D) 현황(예시)

12) 국가과학기술지식정보서비스 홈페이지, https://www.ntis.go.kr/(최종확인, 2024.6.26.)

3. 디지털포렌식 교육과정의 특성

○ 융복합교육과정 구성

- 디지털포렌식 분야는 법학과 공학의 융복합 영역으로써 법절차, 기술, 디지털포렌식 TOOL 활용 능력을 요구하고 있으므로 융복합 교육과정 운영을 통해 전문인력 양성 필요

[그림 3] 디지털포렌식의 융복합 요소

○ 법·절차 관련 지식

- 디지털포렌식은 디지털 기기나 저장매체에서 타인의 데이터를 수집·분석하는 일련의 절차로써 관련 법률 준수
- 따라서 법절차와 관련된 지식이 필수적으로 요구되며 관련 법률에는 형법, 형사소송법, 개인정보 보호법, 정보통신망법, 통신비밀보호법, 전기통신사업법 등 존재

○ 기술 관련 지식

- 디지털 기기나 저장매체를 분석하기 위해서는 컴퓨터 및 네트워크 등 IT 관련 기술 습득 필요
- 기본적으로 컴퓨터 시스템의 기본 구조와 작동 원리, 프로그래밍 언어를 학습할 필요가 있으며, 컴퓨터 네트워크, 운영체제, 데이터베이스, 컴퓨터 보안, 파일시스템 등의 교과목 학습 필요

○ 디지털포렌식 TOOL 활용 능력

- 디지털포렌식은 개발된 TOOL을 활용하여 데이터를 수집·분석하는 분야로써 기본적으로 디지털포렌식 TOOL을 활용할 수 있는 능력 필요
- 신뢰성이 검증된 TOOL을 사용해야 하며, 복제기(Falcon) 등 하드웨어 장비와 EnCase, FTK 등 분석 소프트웨어 사용 방법 학습 필요

III.

국내·외 디지털포렌식 자격제도 및 NCS 운영 현황

Ⅲ 국내·외 디지털포렌식 자격제도 및 NCS 운영 현황

1. 국내·외 디지털포렌식 자격제도

○ 국내 자격제도

▪ (사)한국포렌식학회와 한국인터넷진흥원이 공동으로 '디지털포렌식 전문가 자격' 발급[13)]

구분	시험과목
디지털포렌식 전문가 1급	• (실기) 디스크포렌식, 네트워크포렌식, 데이터베이스포렌식, 모바일포렌식, 침해사고 대응 포렌식 • (필기) 증거법
디지털포렌식 전문가 2급	• (실기) 디지털포렌식 기초실무 • (필기) 컴퓨터 구조와 디지털저장매체, 파일시스템과 운영체제, 응용프로그램과 네트워크의 이해, 데이터베이스, 디지털포렌식 개론

[표 6] 디지털포렌식 전문가 1급·2급 운영 현황

▪ 대검찰청은 2016년부터 각 수사 분야의 전문성을 지닌 검찰 수사관을 선발하는 '공인전문수사관 인증제도(디지털포렌식 포함)' 운영

▪ 경찰청은 '전문수사관 인증제'에서 디지털포렌식 제도 운영

대분류	기능	인증분야		
죄종별	사이버 수사 (16)	가상자산추적수사	디도스	랜섬웨어
		메신저피싱	몸캠피싱	사이버개인정보침해
		사이버국제공조	사이버도박	사이버명예훼손
		사이버사기	사이버성폭력 불법유통망수사	사이버저작권침해
		아동성착취물 신분위장수사	악성프로그램	피싱·파밍
		해킹		

13) (사)한국포렌식학회 디지털포렌식 자격검정시험 홈페이지, https://exam.forensickorea.org/bbs/user.php? user_type=examinfo (최종확인, 2024.6.26.)

대분류	기능	인증분야		
증거분석	과학수사 (8)	범죄분석	법최면수사	수중과학수사
		영상분석	폴리그래프	화재감식
		현장감식	혈흔분석	-
	사이버 (5)	IoT기기포렌식	디스크포렌식	모바일포렌식
		악성코드포렌식	영상기기포렌식	-

[표 7] 전문수사관 인증 분야(2022)

○ 해외 자격제도

자격증명	기관	내용
Certified Computer Examiner (CCE)	International Society of Forensic Computer Examiners (ISFCE)	디지털 증거 수집, 분석, 보고 기술에 대한 인증
Certified Forensic Computer Examiner (CFCE)	International Association of Computer Investigative Specialists (IACIS)	법 집행 기관에서의 디지털 포렌식 수사 기술 인증
GIAC Certified Forensic Examiner (GCFE)	Global Information Assurance Certification (GIAC)	컴퓨터 포렌식 분석, 데이터 복구, 사건 대응 기술 인증
GIAC Certified Forensic Analyst (GCFA)	Global Information Assurance Certification (GIAC)	고급 디지털 포렌식 분석, 사건 대응, 침해 조사 기술 인증
Certified Cyber Forensics Professional (CCFP)	International Information System Security Certification Consortium (ISC)	사이버 포렌식 수사, 증거 수집, 법적 절차에 대한 전문 지식 인증
EnCase Certified Examiner (EnCE)	OpenText	EnCase 포렌식 소프트웨어를 사용한 디지털 증거 분석 기술 인증.
Certified Digital Forensics Examiner (CDFE)	Mile2	디지털 포렌식 수사, 증거 수집, 분석 기술 인증.
Certified Hacking Forensic Investigator (CHFI)	EC-Council	해킹 사고 분석, 디지털 증거 수집, 사건 대응 기술 인증
AccessData Certified Examiner (ACE)	AccessData	AccessData 포렌식 도구를 사용한 디지털 증거 분석 기술 인증
Professional Certified Investigator (PCI)	ASIS International	조사 기법, 증거 수집, 윤리 기준에 대한 전문 지식 인증
CyberSecurity Forensic Analyst (CSFA)	CyberSecurity Institute	디지털 포렌식 분석, 침해 사고 대응 기술 인증

[표 8] 해외 디지털포렌식 관련 자격제도 현황

2. 디지털포렌식 NCS 운영 현황[14)]

○ 개요 및 직무정의

- 디지털포렌식 수요가 증가하고 디지털포렌식 직무에 대한 표준이 사회적으로 요구되어 2020년 디지털포렌식 직무능력표준(NCS, National Competency Standards) 개발·배포
- 직무정의를 "디지털포렌식은 디지털 기기에서 발생된 특정 행위의 사실 관계를 규명하고, 추후 법정에서 증거 자료로 인정될 수 있도록 요건을 갖추어 과학적 방법으로 증거물을 수집, 이동, 보존, 분석, 제출, 검증하는 일"로 정의

○ 능력단위

순번	능력단위	능력단위 정의
1	조사계획 수립	조사 계획 수립이란 사고를 접수하여 유형을 파악하고 대상과 범위를 확정한 후 조사계획을 수립하는 능력
2	현장 조사	현장 조사란 현장을 파악한 후 통제하고, 증거를 식별하여 현장에서 필요한 분석을 하는 능력
3	증거 수집	증거 수집이란 디지털기기에서 조사 목적에 맞게 데이터를 수집하고 수집결과를 검증할 수 있는 능력
4	증거 관리	증거 관리란 수집된 디지털 증거의 현황을 파악하고 절차에 따라 관계자에게 인계하며 보관 장소를 유지하고 관리하는 능력
5	증거 추출	증거 추출이란 수집된 증거물을 검사하고 복구하여 사건 관련 데이터를 추출하는 능력
6	증거 분석	증거 분석이란 운영체제/애플리케이션, 네트워크, 코드, 데이터베이스로부터 추출한 증거를 분석하는 능력
7	증거 제출	증거 제출이란 분석 절차와 결과를 문서화하고 의뢰자에게 제출한 후 법정이나 해당기관에서 증언하는 능력

[표 9] NCS 디지털포렌식 능력단위

○ 능력단위별 능력단위요소와 수행준거

능력단위	능력단위요소	수행준거
조사계획 수립	사고 접수하기	1.1 디지털 증거 수집, 분석 요청에 따라 사고를 접수할 수 있다. 1.2 접수된 사고의 발생 시간, 위치와 같은 사고 정보를 기록할 수 있다. 1.3 기록한 정보에 따라 사고 유형을 분류하고, 사건 접수서를 작성할 수 있다.

14) 국가직무능력표준(NCS) 홈페이지, www.ncs.go.kr

능력단위	능력단위요소	수행준거
조사계획 수립	사전 조사하기	2.1 사건 접수서에 기록된 정보에 따라 조사 대상의 네트워크 구성, 시스템 유형, 규모, 운영체제와 같은 전산 환경 정보를 사전에 조사할 수 있다. 2.2 사전에 조사된 정보에 따라 주요 조사 대상을 선정할 수 있다. 2.3 사전 조사 결과에 따라 사전 조사 결과서를 작성할 수 있다.
	계획 수립하기	3.1 사전 조사 결과서에 따라 주요 조사 대상을 확인하고, 조사 대상의 증거 수집에 필요한 하드웨어, 소프트웨어, 관련 장비를 선정할 수 있다. 3.2 사전 조사 결과서에 따라 증거분석 방법을 선정할 수 있다. 3.3 조사된 정보에 따라 예산 산정, 인력 구성, 일정 계획을 수립하고, 조사 계획서를 작성할 수 있다.
현장 조사	현장 파악하기	1.1 현장관계자에게 조사 권원(權原)을 제시하고 협조를 요청할 수 있다. 1.2 조사계획서에 따라 유형을 파악하고, 사건조사에 필요한 사람을 상대로 면담지를 작성할 수 있다. 1.3 현장에 있는 수집 대상물의 위치를 상세히 스케치할 수 있다. 1.4 훼손되거나 사라질 가능성이 있는 증거들을 촬영하여 보존할 수 있다.
	현장 통제하기	2.1 현장에서 조사에 방해가 되거나 불필요한 사람을 사건 현장에서 통제할 수 있다. 2.2 조사 대상 현장에 대한 출입 통제영역을 설정할 수 있다. 2.3 조사 대상과 관련 있는 디지털기기를 확보하고 네트워크 통신을 제어할 수 있다.
	현장증거 식별하기	3.1 조사 계획에 따라 현장의 조사 대상 디지털기기를 특정할 수 있다. 3.2 은닉된 디지털기기나 시스템 등에 연결되었던 디지털저장매체를 발견·식별할 수 있다. 3.3 현장에 있는 메모지, 각종 출력문서 등 사건과 관련성 있는 물리적 증거물을 확인할 수 있다.
	현장 분석하기	4.1 현장에서 식별된 디지털기기의 휘발성 정보를 분석할 수 있다. 4.2 조사 계획에 따라 로그정보를 분석할 수 있다. 4.3 분석된 결과에 따라서 초동분석 보고서를 작성할 수 있다.
증거 수집	증거 식별하기	1.1 디지털기기 유형에 따른 디지털 저장매체를 식별할 수 있다. 1.2 디지털 저장매체에서 사건과 관련된 파일을 선별할 수 있다. 1.3 교체하거나 은닉된 수집 대상을 식별할 수 있다.
	증거 수집하기	2.1 조사 목적에 맞는 수집 방법을 결정할 수 있다. 2.2 디지털기기에서 라이브 데이터를 수집할 수 있다. 2.3 디지털 저장매체에서 선별된 데이터를 수집할 수 있다. 2.4 디지털 저장매체를 복제하거나 이미징할 수 있다.
	동일성 확인하기	3.1 수집된 증거물의 동일성을 확인할 수 있다. 3.2 수집된 증거물의 목록을 작성하여 교부할 수 있다. 3.3 수집된 증거물을 봉인할 수 있다. 3.4 수집 과정 및 결과에 대한 보고서나 확인서를 작성할 수 있다.

능력단위	능력단위요소	수행준거
증거 관리	증거물 인계하기	1.1 수집된 증거물을 안전하게 포장할 수 있다. 1.2 포장된 증거물을 무결성이 훼손되지 않도록 운반할 수 있다. 1.3 운반된 증거물을 관계자에게 인계할 수 있다. 1.4 운반된 증거물을 관리대장이나 시스템에 등록할 수 있다.
	증거 보관하기	2.1 수집된 증거의 무결성이 훼손되지 않도록 보관할 수 있다. 2.2 증거의 입출고 내역을 포함한 현황을 체계적으로 추적하고 관리할 수 있다. 2.3 증거자료 복사본을 절차에 따라 정보보호 처리 후 교부할 수 있다.
	보관소 관리하기	3.1 보관소 정·부책임자를 지정하고 출입자 명부를 작성할 수 있다. 3.2 증거의 안전한 관리를 위하여 기술적 보안조치를 할 수 있다. 3.3 증거 보관소의 유지를 위하여 주기적으로 안전성을 점검하고 관련 규정을 개선하고 관리할 수 있다.
증거 추출	증거물 검사하기	1.1 수집된 디지털기기에서 디지털 저장매체를 분리할 수 있다. 1.2 수집된 증거물의 물리적 손상여부를 판별하여 기록할 수 있다. 1.3 디지털 저장매체에 보호조치가 있는지 확인할 수 있다. 1.4 검사 결과에 대한 보고서를 작성할 수 있다.
	물리적 복구하기	2.1 증거 디지털 기기가 고장으로 정상적으로 동작하지 않을 경우, 부품 확보와 수리를 할 수 있다. 2.2 증거 디지털 기기의 정상적인 동작이 어려운 경우, 디지털 저장매체를 물리적으로 분리하거나 우회 읽기를 할 수 있다. 2.3 증거 디지털 저장매체의 물리적 손상이 확인된 경우, 복구 장비나 수작업으로 복구를 할 수 있다. 2.4 디지털 기기에 시스템 보안이나 사용자 인증키 등의 보호조치가 적용되어 디지털 저장매체에 접근이 불가한 경우, 이를 우회하거나 무력화할 수 있다.
	증거사본 생성하기	3.1 증거물의 사본을 생성하는데 적합한 디지털 저장매체를 준비할 수 있다. 3.2 준비된 디지털 저장매체에 증거물의 사본을 생성할 수 있다. 3.3 증거물의 원본과 생성된 사본의 동일성을 확인할 수 있다.
	파일시스템 복구하기	4.1 생성된 사본의 파일시스템을 구분할 수 있다. 4.2 준비된 파일시스템의 정상 여부를 구분할 수 있다. 4.3 백업영역을 이용해 비정상 파일시스템을 복구할 수 있다. 4.4 숨겨지거나 암호화된 증거물을 식별하고 해제 할 수 있다.
	데이터 추출하기	5.1 조사계획서에 따라 사고와 관련된 데이터를 구분할 수 있다. 5.2 조사계획서에 따라 사고와 관련된 데이터를 추출할 수 있다. 5.3 조사계획서에 따라 삭제되거나 손상된 데이터를 확인하고 복구할 수 있다. 5.4 추출된 결과에 따라 목록과 보고서를 작성할 수 있다.

능력단위	능력단위요소	수행준거
증거 분석	운영체제/ 애플리케이션 분석하기	1.1 사건과 관련된 유의미한 데이터를 선별할 수 있다. 1.2 운영체제에 의해 생성된 데이터를 분석할 수 있다. 1.3 애플리케이션에 의해 생성된 데이터를 분석할 수 있다. 1.4 분석 결과를 검토하여 분석 보고서를 작성할 수 있다.
	네트워크 분석하기	2.1 수집된 네트워크 데이터를 필요한 기준에 따라 분류할 수 있다. 2.2 특정 서비스 실행과 연관된 네트워크 프로토콜 패턴과 패킷 내용을 분석할 수 있다. 2.3 네트워크와 보안장비의 설정내역 및 로그를 분석할 수 있다. 2.4 분석 결과를 검토하여 분석 보고서를 작성할 수 있다.
	코드 분석하기	3.1 코드를 역어셈블하여 정적 분석을 수행할 수 있다. 3.2 악성코드 분석 방법을 이해하고 (정적 분석과 동적 분석) 도구를 사용할 수 있다. 3.3 코드의 동작방식과 그 동작 결과로 발생된 영향을 분석할 수 있다. 3.4 분석 결과를 검토하여 분석 보고서를 작성할 수 있다.
	데이터베이스 분석하기	4.1 복구 도구를 이용하여 데이터베이스에서 삭제된 레코드를 복구할 수 있다. 4.2 데이터베이스 접속 프로그램을 사용하여 로그 정보를 수집할 수 있다. 4.3 로그파일을 분석하여 사용자 및 시간대별 데이터 접근 및 조작 내역을 분석할 수 있다. 4.4 분석 결과를 검토하여 분석 보고서를 작성할 수 있다.
	안티포렌식 분석하기	5.1 안티포렌식 기술과 사용된 도구를 판별할 수 있다. 5.2 안티포렌식 기법별로 원래의 데이터를 복구하여 분석할 수 있다. 5.3 분석 결과를 검토하여 분석 보고서를 작성할 수 있다.
증거 제출	보고서 작성하기	1.1 제출 기관의 서식 및 일반원칙을 고려하여 보고서 작성 계획을 수립할 수 있다. 1.2 분석과정에서 사용한 도구와 수행절차, 분석결과를 파악할 수 있다. 1.3 원본무결성 보존을 위해 취해진 조치와 분석된 증거를 확인하는 방법을 파악할 수 있다. 1.4 분석과정과 결과를 재검토하여 분석보고서 기준에 맞게 전문가 소견을 작성할 수 있다.
	보고서 제출하기	2.1 보고서를 뒷받침할 수 있는 증거와 분석 산출물을 선별할 수 있다. 2.2 보고서의 내용을 의뢰자에게 설명할 수 있다. 2.3 보고서와 관련 자료를 승인절차를 거쳐 제출할 수 있다. 2.4 보고서 부본과 관련 자료 사본을 생명주기에 따라 보관하고 파기할 수 있다.
	증언하기	3.1 전문가 증언에 관한 절차를 파악할 수 있다. 3.2 분석보고서를 이해하고, 쟁점을 도출할 수 있다. 3.3 객관적 사실과 주관적 견해를 구분하여 증언할 수 있다. 3.4 분석결과에 대해 필요할 경우 재현할 수 있다.

[표 10] NCS 디지털포렌식 능력단위요소 및 수행준거

IV.

디지털포렌식 거버넌스 구축과 입법적 과제

Ⅳ 디지털포렌식 거버넌스 구축과 입법적 과제

1. 디지털포렌식 거버넌스 구축 필요성 및 방안

○ 거버넌스 필요성

- 다수의 이해관계자의 등장으로 기능과 역할 구분을 통한 발전 방안 마련
  - · 경찰, 검찰, 군, 공수처, 해양경찰, 특사경등 다수 수사기관 활용
  - · 선관위, 감사원, 노동부, 공정위, 관세청, 특허청, 서울시, 경기도 등 조사기관 가세
  - · 공공/연구기관, 감정기관, 표준기관, 학계, 기업, 법무/회계법인, 시민단체 참여
  - · 형사소송, 정보통신, 정보보호에서 행정조사, 인공지능, 가상자산, 개인정보 등 확장
- 국가안보와 직결되고, 형사사법 역량과 신뢰도를 결정짓는 요소로 작용
- 계속 등장하는 기술적 난제 대응과 시장/산업 경쟁력 확보

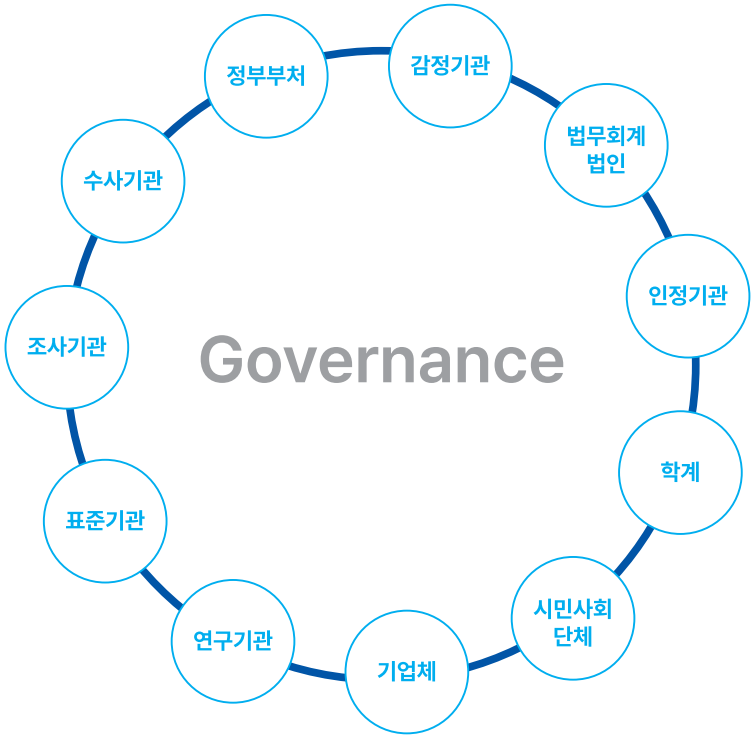
○ 입법동향

- 2017년 과학수사기본법안 연구용역(치안정책연구소)
- 2017년 김승희 의원, "법과학기술육성 법안" 발의·폐기(20대)
- 2019년 디지털증거의 인증 및 포렌식감정에 관한 법률(안) 연구용역(국과수)
- 2022년 조수진 의원, "디지털포렌식산업육성 및 지원에 관한 법률안" 발의·폐기(21대)

  ※ 디지털포렌식산업 육성을 위한 종합대책, 위원회(총리실 소속), 사업자 허가·영업 정지 요건, 재정지원, 실태조사 등

○ 구축방안 : 디지털포렌식발전방안 법률 마련

- 제정목적 : 수사역량과 산업육성 중에서 선택
- 적용범위 : 디지털포렌식 단독 또는 법과학/과학수사 통합방안 검토
- 거버넌스 : 총리실, 행안부, 법무부, 과기부, 경찰청, 대검찰청 중에서 결정
- 영업형태 : 디지털포렌식 사업자에 대해 자유업, 신고업, 허가업으로 규정할 지 검토
- 기타–실태조사, 연구개발 지원, 국제협력 등 포함



[그림 4] 디지털포렌식 관련 이해관계자 현황

2. 디지털포렌식 관련 입법 과제

○ 법절차 관련

- 유비쿼터스 컴퓨팅 환경이 확대됨에 따라 디지털 데이터를 수집하는 과정에서 법률적 한계에 봉착하는 상황 발생
- 디지털증거의 취약성과 대량성, 네트워크 관련성이 증거수집에 있어서 많은 문제를 초래함에 따라, 전세계적으로 이와 같은 문제를 해결하기 위해 사이버범죄협약의 가입국이 계속하여 늘어나고[15] 있으며 미국에서는 클라우드법(CLOUD Act, Clarifying Lawful Overseas Use of Data Act)이 제정·시행
- 우리나라도 2022년 사이버범죄협약 가입의향서를 제출하였고, 2023년 정식 가입 초청서를 받은 상태로 사이버범죄협약에서 요구하고 있는 입법적 사항을 형사소송법 등에 반영해야 할 시점
- 디지털증거 수집의 효율성뿐만 아니라 디지털포렌식은 수사과정에서의 피압수자의 사생활의 비밀과 자유, 정보에 대한 자기결정권, 사실상의 평온권을 침해할 수 있으므로 비례의 원칙에 근거한 수행 절차 마련 필요

15) 2024년 현재 75개국이 사이버범죄협약에 가입하였으며, 20개국이 초청되었음
(https://www.coe.int/en/web/cybercrime/the-budapest-convention (최종확인, 2024.06.25.)

○ 인력 수행자격 관련

- 디지털포렌식 절차를 통해 수집·분석된 데이터가 유효한 사실입증의 자료로 사용되기 위해서는 자료의 동일성과 무결성, 신뢰성 인정 필요
- 자료의 동일성과 무결성, 신뢰성을 인정받기 위해서는 일정한 수준의 자격을 가진 사람이 디지털포렌식을 수행해야 하며, 자격요건을 마련하여 국가 관리 시급
- 디지털포렌식은 범죄수사와 같은 공공영역뿐만 아니라 민간영역에서도 다양하게 활용되고 있으므로 무분별한 디지털포렌식 업체의 난립을 방지하기 위해서라도 시급히 인력 수행자격에 대한 기준 마련 필요

○ 기술 표준 관련

- 사실관계를 증명해 주는 데이터는 유무죄를 판단함에 있어서 중요한 자료가 될 수 있으므로 데이터의 수집과 분석에 활용한 기술은 자료의 신뢰성을 담보하는데 중요 역할 수행
- 미국[16] 및 선진국에서는 디지털포렌식 기술 및 절차와 관련하여 다양한 보고서 및 가이드라인을 제작하여 배포하고 있으며, 우리나라도 이와 같은 기술 표준 제작·배포 필요

○ 도구 검증 관련

- 형사재판뿐만 아니라 민사재판에서 디지털포렌식에 의해 수집된 증거가 유효하게 사용되기 위해서는 증거의 신뢰성이 전제되어야 하고, 증거의 신뢰성은 도구의 검증 담보 필요
- 미국에서는 NIST CFTT(Computer Forensics Tool Testing Program)을 통해 디지털포렌식 도구의 검증을 위한 표준화된 테스트 방법을 제공하며, 도구의 신뢰성과 정확성 평가
- 도구 검증은 디지털포렌식에 의해 수집된 증거의 진정성을 담보할 수 있는 전제조건이므로 국가가 직접 도구 검증을 위한 제도 마련 필요

16) NIST (National Institute of Standards and Technology), FBI (Federal Bureau of Investigation), NIJ (National Institute of Justice) 등이 있음

V.

시사점 및 제언

V 시사점 및 제언

1. 디지털포렌식 전문인력 양성 부문

- 공공분야뿐만 아니라 민간 영역에서도 디지털포렌식 수요는 매년 증가하고 있으나 전문인력 양성을 위한 환경은 매우 열악
- HM컴퍼니가 기업 내부감사인을 대상으로 실시한 설문조사 결과에 따르면 응답자의 33.3%가 지적한 디지털포렌식에서 가장 큰 애로사항은 전문인력 부족
- 디지털포렌식 전문인력을 양성하는 대학도 학부 과정 3곳(군산대, 동서대, 한림대), 대학원 과정 6곳(경찰대, 고려대, 동국대, 동서대, 성균관대, 한림대) 등에 불과, 정부지원사업으로 양성하는 수준
- 디지털포렌식 수요와 중요성에 고려할 때 고등교육기관에서 전문인력을 양성해야 하며, 정부는 대학에 예산을 지원하여 전문인력을 양성할 수 있는 환경 조성 필요

2. 디지털포렌식 자격제도 부문

- 해외에서는 디지털포렌식과 관련하여 다양한 자격제도가 운영되고 있는 반면, 우리나라에서는 한국포렌식학회에서 운영하고 있는 디지털포렌식전문가 자격이 유일
- 수사기관에서는 내부적인 전문수사관 인증제를 통해 자격을 부여하고 있으나 수사기관 자체의 교육은 신뢰성을 담보할 수 없으므로 공신력 있는 기관에서 디지털포렌식 관련 자격을 개발하여 전문가로서의 위상과 신뢰성이 담보된 자격제도를 운영 필요

3. 디지털포렌식 거버넌스 구축 부문

- 디지털포렌식은 법절차, 자격, 기술 표준, 도구 검증의 체계가 구축되었을 때 절차의 신뢰성과 데이터의 진정성 확보 가능
- 디지털포렌식 거버넌스 구축을 위해서는 우선적으로 디지털포렌식의 주요 요소라고 볼 수 있는 법절차, 자격, 기술 표준, 도구 검증에 관한 입법이 필요하며, 거버넌스 운영을 위해서는 국가가 디지털포렌식 부문을 주도적으로 견인해 나가는 것이 타당

참고문헌

(사)한국포렌식학회 디지털포렌식 자격검정시험 홈페이지, https://exam.forensickorea.org/

Research Nester 홈페이지, https://www.researchnester.com/kr/reports/digital-forensics- market/4832

경찰청 통계자료(2024)

고려대학교 홈페이지, https://gss.korea.ac.kr/ime/about/curriculum.do

국가과학기술지식정보서비스 홈페이지, https://www.ntis.go.kr/

국가직무능력표준(NCS) 홈페이지, www.ncs.go.kr

대검찰청 통계자료(2017)

백현정, 「디지털포렌식 시장추산 및 예측에 관한 연구」, 성균관대학교 과학수사학과(대학원) 석사학위, 2022.

서울대학교 홈페이지, https://mis.snu.ac.kr/academic/subjects.php

성균관대학교 홈페이지, https://skb.skku.edu/forensic/under/under_course01.do=

연세대학교 홈페이지, https://gsi.yonsei.ac.kr/course/c9.asp

유럽평의회 홈페이지. https://www.coe.int/en/web/conventions/home

조세일보 보도(2022.3.31.), "내부감사에 디지털포렌식·리뷰 플랫폼 필요해", https://m.joseilbo.com/ news/view.htm?newsid=450527#_enliple

한국인터넷진흥원 홈페이지, https://www.kisa.or.kr/402/form?postSeq=2384#fnPostAttachDownload

정보보호 인적자원개발위원회
Information Security Industrial Skills Council

ISSUE REPORT

(05717) 서울특별시 송파구 중대로 135, IT벤처타워 서관 14층
정보보호 인적자원개발위원회