디지털포렌식연구실 소개

Digital Forensic Research Center

2023-08-14

손 지 훈 (Hunjison)

esby9774@gmail.com

dfrc
Digital Forensic Research Center

목 차

- 발표자 소개
- 디지털포렌식연구센터(DFRC)
- 대학원 진학의 장단점

발표자 소개

발표자 소개

“열심히 배워서 남 주기”

- **학력**
  - 2020, 경찰대학 법학과 졸업
  - 2022~, **고려대학교 정보보호대학원**
- **활동**
  - 2019, BoB 8기 취약점 분석 트랙 수료
  - 2020, BoB 총동문회 & 뉴스레터 편집장
  - 2022~, F_Active, Hackyboiz 팀원
- **수상/자격증**
  - 2020, 정보처리기사 & 정보보안기사
  - 2021, 네이버 버그바운티 3건
  - 2021/2023 CCE 공공부문 본선 진출
  - 2022 디지털포렌식챌린지 수상
- **발표/강의**
  - 2021, 경찰수사연수원 외래 강사
  - 2021/2022, 해킹캠프 컨퍼런스
  - 2022, 코드엔진 컨퍼런스
  - 2022, 코드게이트 컨퍼런스
  - 2022/2023, **인프런 온라인 강의/교재**
- **논문**
  - SCI 2편
    - 2022 FSIDI, 2023 DFRWS
  - KCI 2편 (2019, 2022)

디지털포렌식연구센터 (DFRC)

고려대학교 디지털포렌식연구센터

Digital Forensic Research Center

- **설립 목적**
  - 사이버 범죄, 해킹, 침해사고 및 각종 범죄 수사 시 활용 가능한 실질적이고 선도적인 디지털 포렌식 기술 / 정책 / 절차 연구

- **연혁**
  - 2002년: 디지털 포렌식 연구 시작
  - 2003년: 국내 첫번째 디지털 포렌식 연구실 설립
  - 2008년: 디지털포렌식연구센터로 승격

- **구성원**
  - 지도교수: 이상진 교수님 (법, 정책), 박정흠 교수님 (기술)
  - 연구원(풀타임): 총 34명
    - 박사과정·수료: 9명 / 석사과정: 25명 (군위탁 2명, 경위탁 1명)

고려대학교 디지털포렌식연구센터

Digital Forensic Research Center

- **지도 교수 (이상진 교수님 – 법, 정책)**
  - 교수 | 고려대학교 정보보호대학원
  - 센터장 | 고려대학교 정보보호연구원 디지털포렌식연구센터
  - 전문위원회 위원 (정보통신분야 산업기술보호) | 산업통상자원부
  - 자문위원 | BoB (Best of the Best) Program, KITRI
  - 원장 | 고려대학교 정보보호대학원
  - 회장 | 한국디지털포렌식학회 (2011 ~ 2017)
  - 회장 | 한국정보보호학회 디지털포렌식연구회 (2012 ~ 2013)
  - 교수 | 고려대학교 자연과학대학 (1999 ~ 2001)
  - 연구원 | 한국전자통신연구원(ETRI) (1989 ~ 1999)
- **주요 수상 내역**
  - 제 3회 대한민국 사이버치안 대상 (대통령 표창)

고려대학교 디지털포렌식연구센터

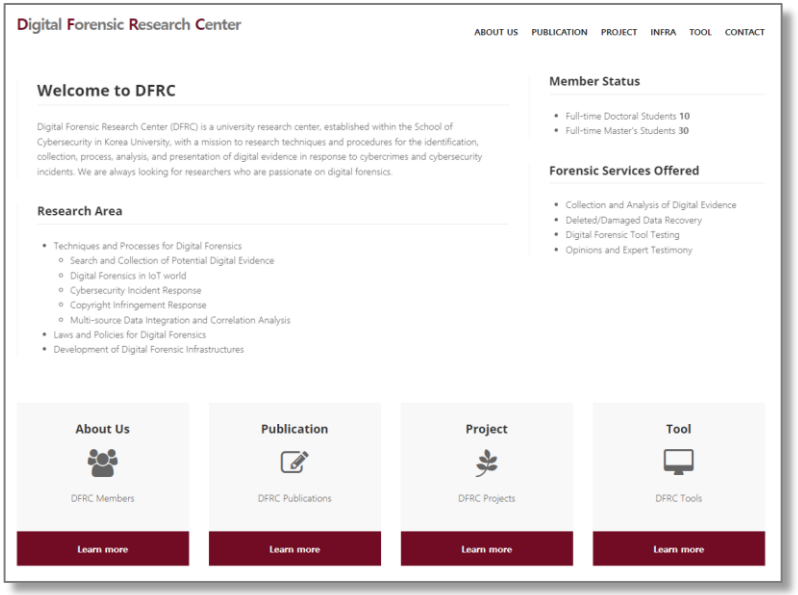
Digital Forensic Research Center

- **지도 교수 (박정흠 교수님 – 기술)**
  - 부교수 | 고려대학교 정보보호대학원
  - 부 센터장 | 고려대학교 정보보호연구원 디지털포렌식연구센터
  - 위원회 구성원 | DFRWS (Digital Forensics Research Conference) APAC
  - 리뷰어 | Forensic Science International: Digital Investigation
  - 멘토 (디지털포렌식) | BoB (Best of the Best) Program, KITRI
  - 학술 위원 | 한국디지털포렌식학회 (Korean Digital Forensics Society)
  - 공동 연구원(Collaborator) | National Institute of Standards and Technology [NIST]
  - 연구원 | National Institute of Standards and Technology [NIST] (2015 ~ 2018)
  - 박사 | 고려대학교 정보보호대학원 (2014)
- **주요 수상 내역**
  - 우승 | DFRWS (Digital Forensics Research Conference) Challenge (2013)
  - 우승 | DC3 (U.S. Department of Defense Cyber Crime Center) Challenge (2009)

고려대학교 디지털포렌식연구센터

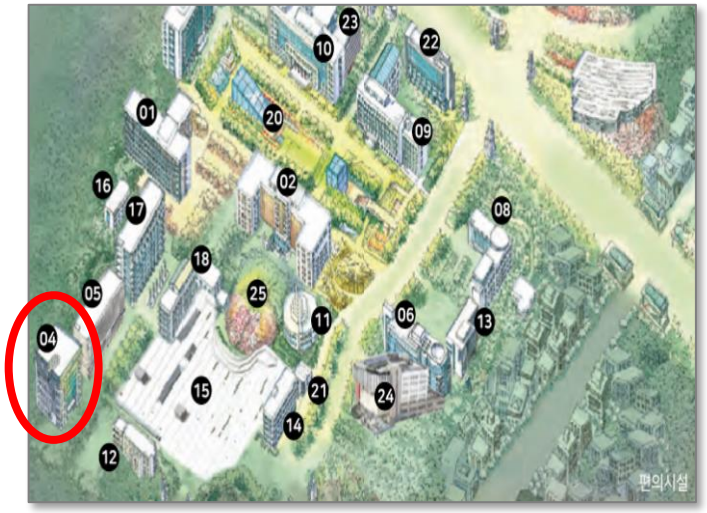
Digital Forensic Research Center

- **홈페이지**
  - http://dfrc.korea.ac.kr/



- **연구센터 위치**
  - 고려대학교 자연계캠퍼스 로봇융합관 405호

- **연락처**
  - 전화번호: 02-3290-4738
  - E-Mail: koreauniv.dfrc@gmail.com

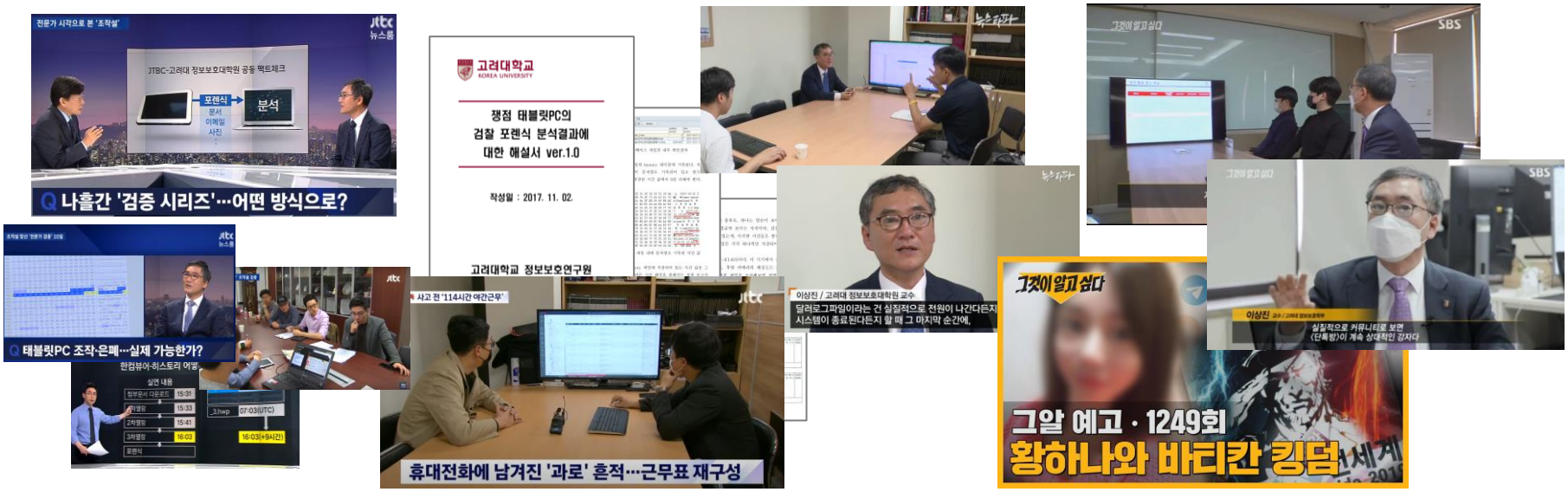


Digital Forensic Research Center

- **연구 성과**
  - **연구 실적**
    - 디지털 포렌식 관련 연구 논문 발표 및 게재(국외 135건, 국내 188건)
    - 디지털 증거 수집 보존 가이드라인 외 표준화 5건
    - 연구 과제 수행 – 최근 40개 이상
      - 주요 수사기관 – 대검찰청, 국정원, 경찰청, 국군방첩사령부 등
      - 주요 연구기관 – ETRI, NSR, ADD, KISA 등
  - **센터 실적**
    - 디지털 포렌식 교육 – 경찰청, 국정원, 대검찰청, 군·민간 기업, 해외 등
    - 디지털 증거 감정 수행 – 150건 이상
    - 수상
      - DFRWS Forensic Challenge 우승 1회, 준우승 2회
      - DC3 Forensic Challenge 대상 2회
      - 2016 스마트그리드 보안 해커톤 대회 1위
      - 2019 디지털 포렌식 아이디어 최우수상 2회, 우수상 1회 (대검, 한국저작권보호원)

Digital Forensic Research Center

- **주요 언론 인터뷰 및 사건 분석**
  - (2017.10.) 최순실 태블릿 보도 의혹 관련 검증 및 해설서 공개
  - (2019.08.) 세월호 선박 내 DVR 동작 상태 검증
  - (2020.04.) [탐사보도 세븐 (104회)] 조주빈 덫에 걸려든 VIP들
  - (2021.02.) SBS 그것이알고싶다 – 상태와 쭈라 (황하나와 바티칸 킹덤의 비밀)
  - (2022.11.) JTBC 뉴스룸 – [단독] 2주간 '114시간 야근'…SPC 끼임사 노동자 '과로' 흔적



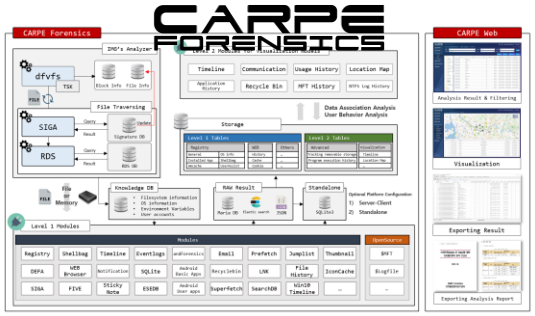
연구 분야

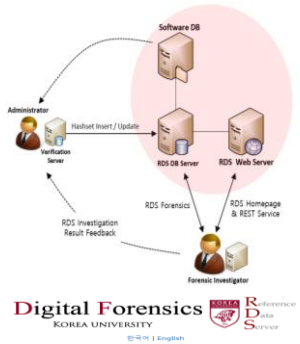
디지털 포렌식 정책 및 표준

- 디지털 증거 처리 절차, 기술 표준화
- 디지털 포렌식 기술 로드맵 수립 등

디지털 포렌식 인프라

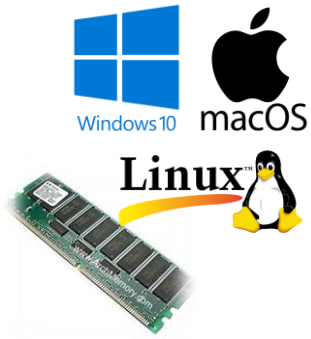
- 포렌식 분석 자동화 시스템 개발, 포렌식 교육시스템 개발
- 포렌식 위키, 참조 데이터 세트, 도구 검증 데이터 세트 등





시스템 포렌식

- 윈도우/리눅스/맥 시스템 포렌식
- 활성 시스템 포렌식



모바일 포렌식

- Android, iOS 등 데이터 수집, 복구, 분석
- 악성 앱 및 앱 데이터 분석

연구 분야

IoT 포렌식

- 스마트 스피커 분석
- 웨어러블 기기 분석

데이터베이스/대용량 저장장치 포렌식

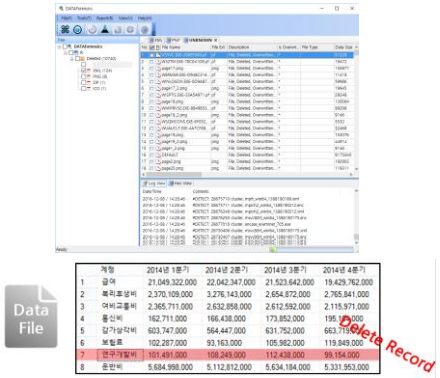
- ORACLE, MSSQL, MySQL, NoSQL 포렌식
- NAS 데이터 수집, RAID 재조합

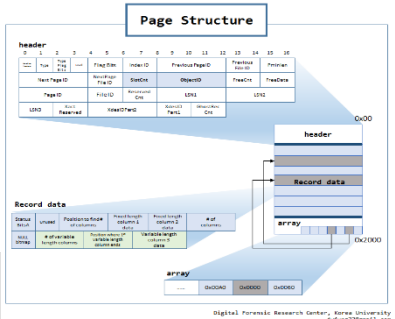
이미지 및 영상 데이터 포렌식

- 블랙박스, CCTV 분석
- 영상 데이터 파편 복구 및 재조합

데이터 복구

- 운영체제 아티팩트/주요 파일 복구
- 데이터베이스 복구





디지털포렌식연구센터 주요 연구과제

- **디지털 포렌식 통합 시스템 개발**
  - (2018.05. ~ 2020.12.) 디지털 포렌식 통합 플랫폼 개발 (CARPE Forensics)
  - (2014.06. ~ 2015.12.) 손상된 CCTV, 블랙박스의 복원 및 통합 뷰어 개발
  - (2012.10. ~ 2017.07.) 대용량 저장장치 조사용 포렌식 시스템 개발
- **디지털 포렌식 분석 기법 개발**
  - (2022.04. ~) 인공지능 기술 활용 디지털증거 분석 기법 개발
  - (2021.07. ~) 안티-포렌식 기술 대응을 위한 데이터 획득 및 분석 기술 연구
  - (2020.07. ~ 2021.09.) 문서형 악성코드 탐지 기술 연구
  - (2019.08. ~) 해양사고 현장 디지털증거물 무결성 및 증거능력 확보를 위한 항해장비 디지털 포렌식 기법 개발
- **보안 취약점 분석 연구**
  - (2016.04. ~ 2019.09.) 최신 APT 방식의 사이버침해 기술 연구 & 사이버 모의 훈련 기술 연구 & 사이버전 지휘통제를 위한 사이버 공격 기법 연구
  - (2015.07. ~ 2017.10.) 임베디드 기기 취약성 분석 및 공격 코드 개발
- **디지털 포렌식 인프라 구축**
  - (2021.05. ~ 2021.11.) 경찰 디지털포렌식 도구 검증체계 구축을 위한 추진전략 연구
  - (2017.04. ~ 2017.11.) 국방 사이버 포렌식 체계 개선 연구
  - (2016.06. ~ 2016.12.) 디지털 포렌식 온라인교육 콘텐츠 개발
  - (2015.05. ~ 2015.11.) 한국형 디지털증거 표준 관리모델 연구

디지털포렌식연구센터 주요 연구과제 (.. ing)

- **디지털 포렌식 분석 기법 개발**
  - (2023.01. ~) 모바일 진단 로그 분석
  - (2022.04. ~) 인공지능 기술 활용 디지털증거 분석 기법 개발
  - (2021.07. ~) 안티-포렌식 기술 대응을 위한 데이터 획득 및 분석 기술 연구
  - (2019.08. ~) 해양사고 현장 디지털증거물 무결성 및 증거능력 확보를 위한 항해장비 디지털 포렌식 기법 개발

- **보안 취약점 분석 연구**
  - (2023.01. ~) 펌웨어 취약점 분석 기술 개발
  - (2022.12. ~) 사이버 타겟 침투 및 원격 무력화 기술 개발

- **디지털 포렌식 정책 · 법제**
  - (2023.01. ~) 논리 이미지 표준화 (내부 과제)

배출 인력


국가정보원
NATIONAL INTELLIGENCE SERVICE


KRX
한국거래소
KOREA EXCHANGE


HYUNDAI


LINE


SK on


SAMSUNG


SAMSUNG SDS


검찰
PROSECUTION SERVICE


금융보안원
FINANCIAL SECURITY INSTITUTE


금융결제원


KOREAN NATIONAL POLICE AGENCY


NSR
국가보안기술연구소
National Security Research Institute


HYUNDAI
AutoEver


KIM & CHANG


Deloitte.

대학원 진학의 장단점

대학원 진학의 장단점

솔직히 대학원 뭐가 부족하냐. 하고 싶은 공부하게 해줘, 월급도 줘, 논문 지도해 줘, 기숙사도 줘, 프로젝트 경험도 쌓게 해줘, 학계 인맥도 쌓게 해줘, 집에 보내 줘, 살려줘 등등

2017. 12. 1. 오후 4:45

리트윗 **4,204**회 마음에 들어요 **713**회

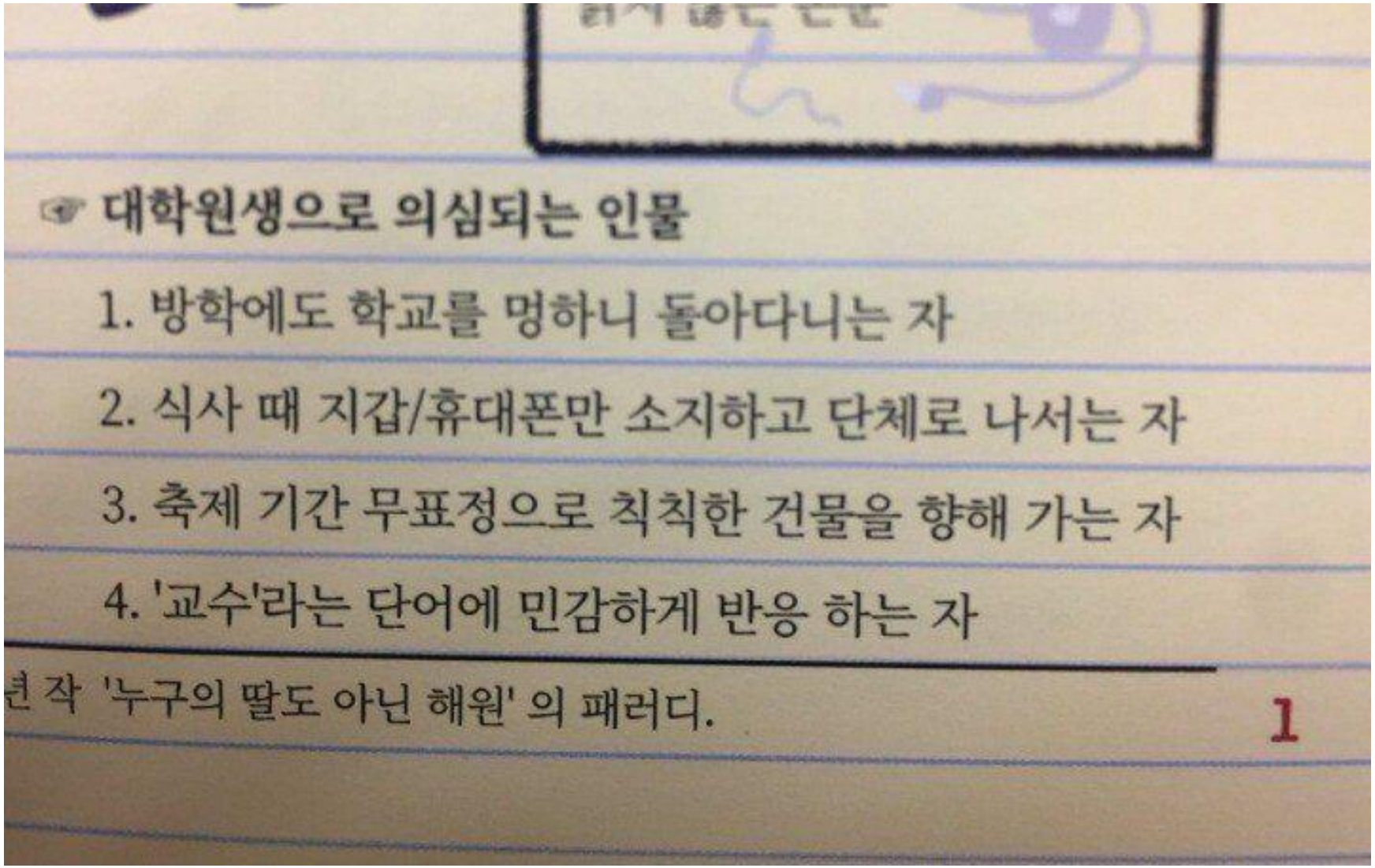
필라이트 홍보맨 @soleratido · 1일
@MikiBear_ 님, @x_nuk 님에게 보내는 답글
대학원, 죽여주네요!

1 383 41

어떤 미키베어는 반달곰이다 @MikiB... · 1일
완전 죽여주죠

210 25

대학원 진학의 장단점


대학원생으로 의심되는 인물
1. 방학에도 학교를 멍하니 돌아다니는 자
2. 식사 때 지갑/휴대폰만 소지하고 단체로 나서는 자
3. 축제 기간 무표정으로 칙칙한 건물을 향해 가는 자
4. '교수'라는 단어에 민감하게 반응 하는 자
년 작 '누구의 딸도 아닌 해원' 의 패러디.
1

대학원 진학의 장단점

지극히 개인적인 대학원의 장단점

- **장점**
  - 진로
    - 국가 차원의 대규모 과제에 참여할 수 있는 기회, 가능성
    - 개인이 원하는 주제를 자유롭게 연구할 수 있는 환경
  - 취업
    - 학벌세탁 & 전공세탁 가능
    - 일정 수준 이상의 직장 취업에 유리한 위치
    - 박사 학위 취득 시에 학계 진출 가능(교수 or 연구소)
  - 생활
    - 충분한 연구비 & 괜찮은 연구 환경 (연구실 by 연구실)
- **단점**
  - 대학원.

THANK YOU
for Listening!

dfrc
Digital Forensic Research Center

Questions?