BISC 2023

Digital Forensic Framework for Decentralized Storage Services

연구 소개 / 해외 컨퍼런스 후기 / 해외 논문 작성법 / 연구실 홍보

손 지 훈
(8기 취약점 분석)

Korea University
School of Cybersecurity

DFRC Korea University
Digital Forensic Research Center

발표자 소개

손지훈 (hunjison)

- **학력**
  - 2020, 경찰대학 졸업
  - 2022~, **고려대학교 정보보호대학원**
- **활동**
  - 2019, BoB 8기 취약점 분석 트랙 수료
  - 2020, BoB 총동문회 & 뉴스레터 편집장
  - 2022~, F_Active, Hackyboiz 팀원
  - 2022~, 디지털포렌식연구센터 연구과제 3개 참여
- **수상/자격증**
  - 2020, 정보처리기사 & 정보보안기사
  - 2021, 네이버 버그바운티 3건
  - 2021/2023 사이버공격방어대회(CCE) 본선
- **논문**
  - 해외: SCI 저널 2편
    - 2022년, 모바일 메신저 안티-포렌식 분석
      2023년, 탈중앙화 스토리지 포렌식
  - 국내: KCI 1편
    - 2022년, 암호화폐 지갑 포렌식 아티팩트 분석
- **발표/강의**
  - 2021, 경찰수사연수원 외래 강사
  - 2021/2022, 해킹캠프 컨퍼런스
  - 2022, 코드엔진 컨퍼런스
  - 2022, 코드게이트 컨퍼런스
  - 2022/2023, 인프런 온라인 강의/교재 업로드

Table of Contents

Keywords

DFRWS APAC 2023

Decentralized Storage Services

대.. 학.. 원.. ?

DFRWS APAC 2023 참가 후기

DFRWS APAC 2023 참가 후기

DFRWS APAC 2023

DFRWS APAC 2023 참가 후기

DFRWS APAC 2023

DFRWS APAC 2023 참가 후기

DFRWS APAC 2023

연구 소개

IF-DSS

- DFRWS 컨퍼런스 논문은 FSIDI 저널(SCI, Q1)에도 자동으로 게재

Forensic Science International: Digital Investigation 46 (2023) 301611

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

DFRWS 2023 APAC - Proceedings of the Third Annual DFRWS APAC

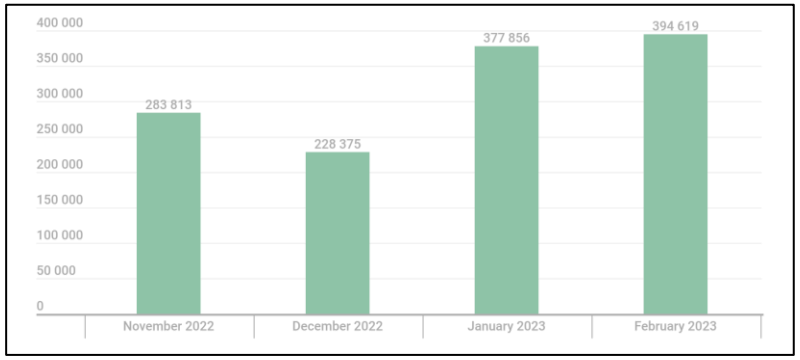
IF-DSS: A forensic investigation framework for decentralized storage services

Jihun Son [a], Gyubin Kim [b], Hyunwoo Jung [c], Jewan Bang [d], Jungheum Park [a,*]

[a] School of Cybersecurity, Korea University, 145 Anam-Ro, Seongbuk-Gu, Seoul, South Korea
[b] AlpineLab, 169-16 Gasan Digital 2-ro, Geumcheon-gu, Seoul, South Korea
[c] AhnLab, 220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, South Korea
[d] Cyber Investigation Bureau, National Office of Investigation, Korean National Police Agency, Seoul, South Korea

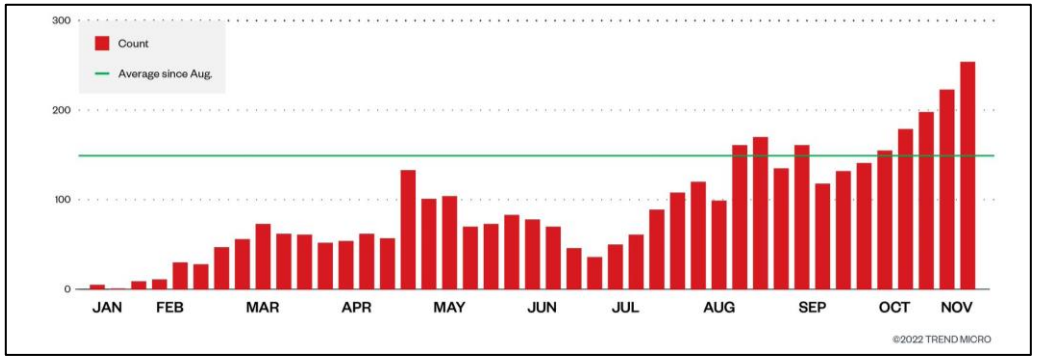
Decentralized Storage Services

- **IPFS**(InterPlanetary File System)**와 같은 P2P 기반의 파일 공유 네트워크**
  - 최근 피싱, 악성코드 유포 등에 많이 사용되며, 그 추세가 증가하고 있음

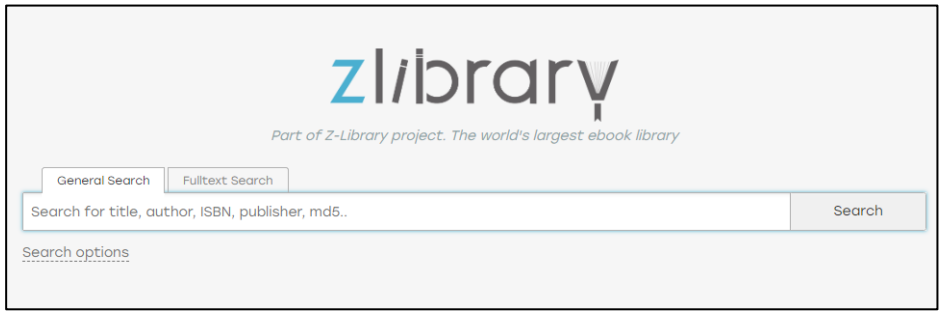


Kaspersky

Trend Micro



  - Z-Library와 같은 콘텐츠 불법 유포에도 활발히 이용

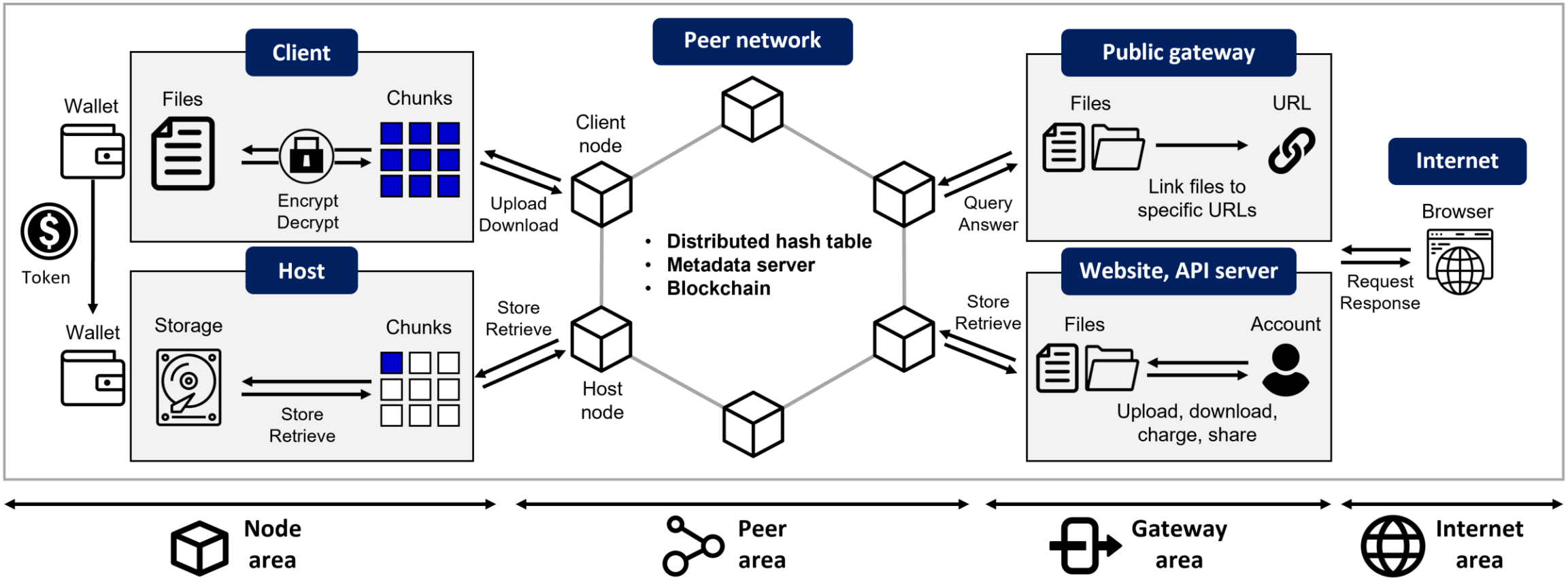


https://www.kaspersky.com/about/press-releases/2023_scammers-go-interplanetary-using-decentralized-file-system-in-their-campaigns
https://www.trendmicro.com/ko_kr/research/22/l/web3-ipfs-only-used-for-phishing---so-far.html

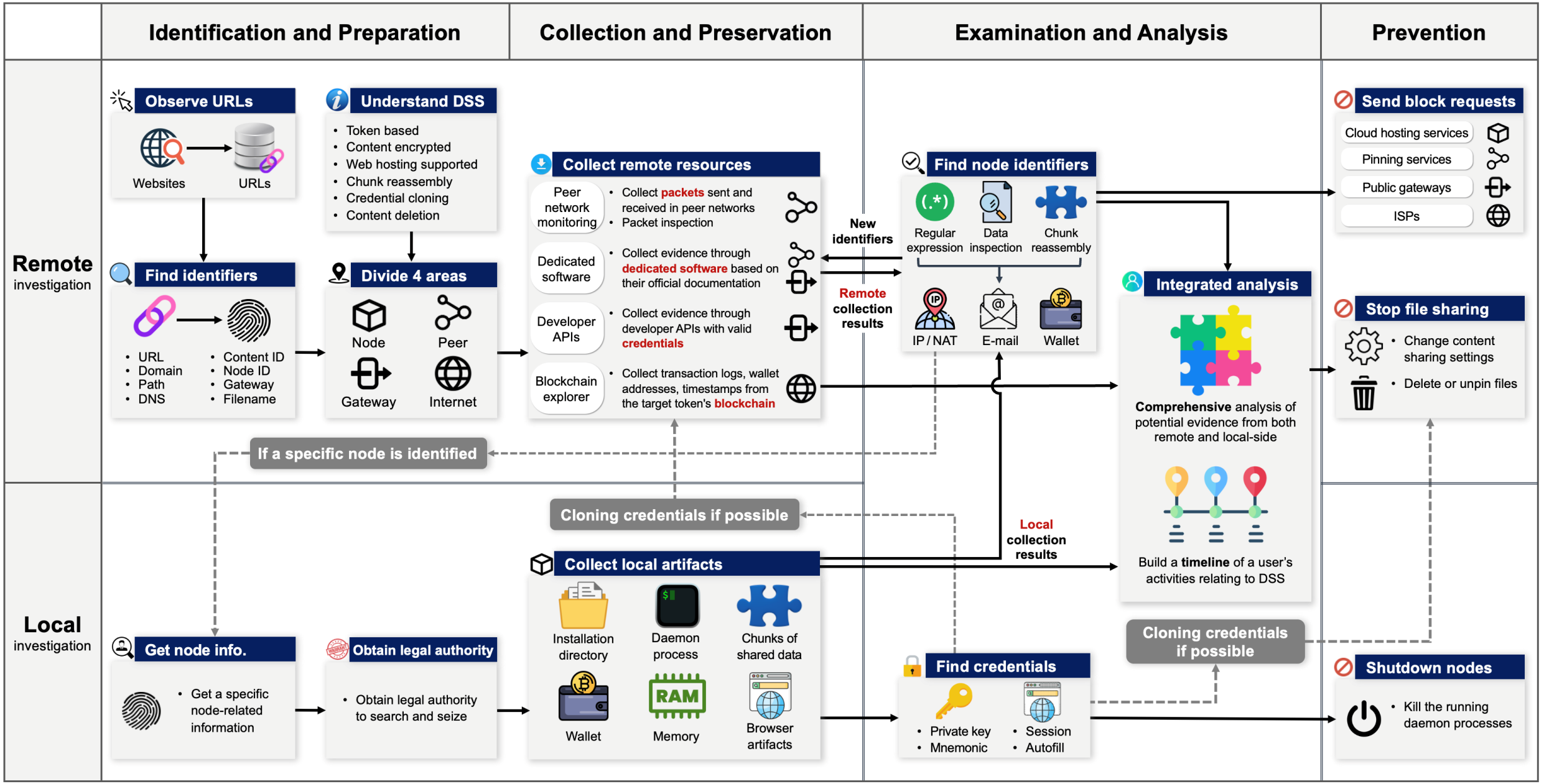
Decentralized Storage Services

- 탈중앙화 & 검열회피성 → 데이터 수집 어려움

  데이터 삭제 불가 & P2P, 인터넷을 통한 콘텐츠 유포 → 데이터 확산 쉬움



연구 소개


Identification and Preparation
Collection and Preservation
Examination and Analysis
Prevention
Remote investigation
Local investigation
Observe URLs
Websites
URLs
Understand DSS
Token based
Content encrypted
Web hosting supported
Chunk reassembly
Credential cloning
Content deletion
Find identifiers
URL
Domain
Path
DNS
Content ID
Node ID
Gateway
Filename
Divide 4 areas
Node
Peer
Gateway
Internet
Collect remote resources
Peer network monitoring
Collect packets sent and received in peer networks
Packet inspection
Dedicated software
Collect evidence through dedicated software based on their official documentation
Developer APIs
Collect evidence through developer APIs with valid credentials
Blockchain explorer
Collect transaction logs, wallet addresses, timestamps from the target token's blockchain
New identifiers
Remote collection results
Find node identifiers
Regular expression
Data inspection
Chunk reassembly
IP / NAT
E-mail
Wallet
Integrated analysis
Comprehensive analysis of potential evidence from both remote and local-side
Build a timeline of a user's activities relating to DSS
Send block requests
Cloud hosting services
Pinning services
Public gateways
ISPs
Stop file sharing
Change content sharing settings
Delete or unpin files
If a specific node is identified
Cloning credentials if possible
Local collection results
Collect local artifacts
Installation directory
Daemon process
Chunks of shared data
Wallet
Memory
Browser artifacts
Get node info.
Get a specific node-related information
Obtain legal authority
Obtain legal authority to search and seize
Find credentials
Private key
Mnemonic
Session
Autofill
Cloning credentials if possible
Shutdown nodes
Kill the running daemon processes

연구 소개

Case Study: 피싱 URL 배포 노드 추적

공개 피싱 URL 수집
(3,662/61,528)

식별자 추출

Type1 URL https://{gateway}/{content_id}/{filename}

https://ipfs.io/Qma... d4e/test.html

https://cloudflare-ipfs.io/Qma... d4e/test.html

Type2 URL https://{content_id}.{gateway}/{filename}

https://baf...brm.ipfs.dweb.link/test.html

https://baf...brm.ipfs.w3s.link/test.html

Type3 URL https://{subdomain}.{gateway}/{filename}

TXT "dnslink=/ipfs/{content_id}"

https://billowing-fire-5940.on.fleek.co/test.html

```
$ dig +answer TXT "_dnslink.billowing-fire-5940.on.fleek.co"
```

TXT "dnslink=/ipfs/Qma9...d4e"

노드 IP 추적

```
$ ipfs dht findprovs bafybe                                  x4k3laufqqfjdo7qfr7zx6e
12D3Koo                                                      dteAh4iF3RR8W1z
12D3Koo                                                      cgYftRRXzVbTrPF
12D3Koo                                                      r2XUKHhEUnfLWX1
$ ipfs dht findpeer 12D3Koo                                  r2XUKHhEUnfLWX1
/ip4/127.0.0.1/tcp/4001
/ip4/167.       .90/udp/4001/quic/p2p/12D3Koo                fkWYdSB1PauqiJT/p2p-circuit
/ip4/127.0.0.1/udp/4001/quic
/ip6/::1/tcp/4001
/ip4/167.       .90/tcp/4001/p2p/12D3Koo                     fkWYdSB1PauqiJT/p2p-circuit
/ip4/192.168.0.134/tcp/4001
/ip6/::1/udp/4001/quic
/ip4/149.       .133/udp/4001/quic/p2p/12D3Koo               1HC8hxHy6r2FjDa/p2p-circuit
/ip4/192.168.0.134/udp/4001/quic
/ip4/149.       .133/tcp/4001/p2p/12D3Koo                    1HC8hxHy6r2FjDa/p2p-circuit
```

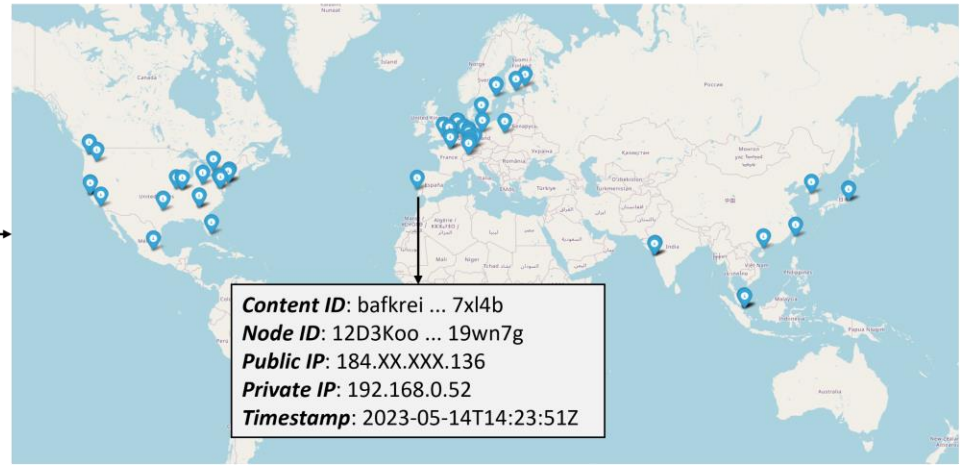
Content ID

Node ID

Public and private IP address of content provider nodes

List of IP addresses

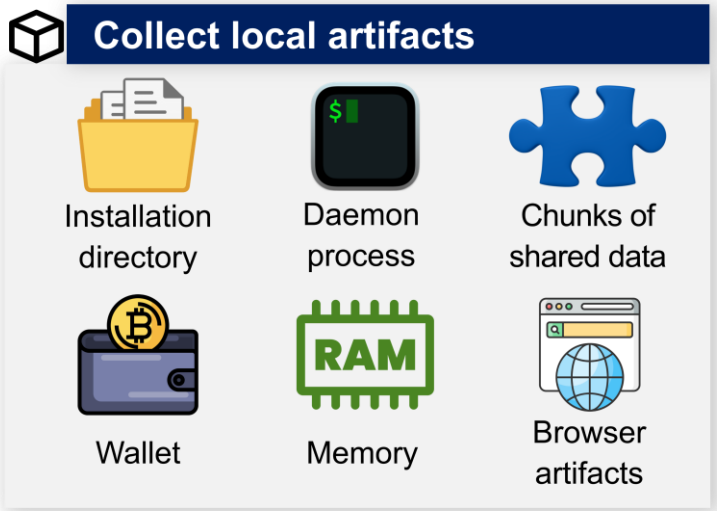
```
107       .221
34.       6.79
44.       .128
3.9       21
54.       .204
34.       .62
54.       1.175
204       52.61
54.       9.182
52.       .25
54.       0.74
107       5.189
```

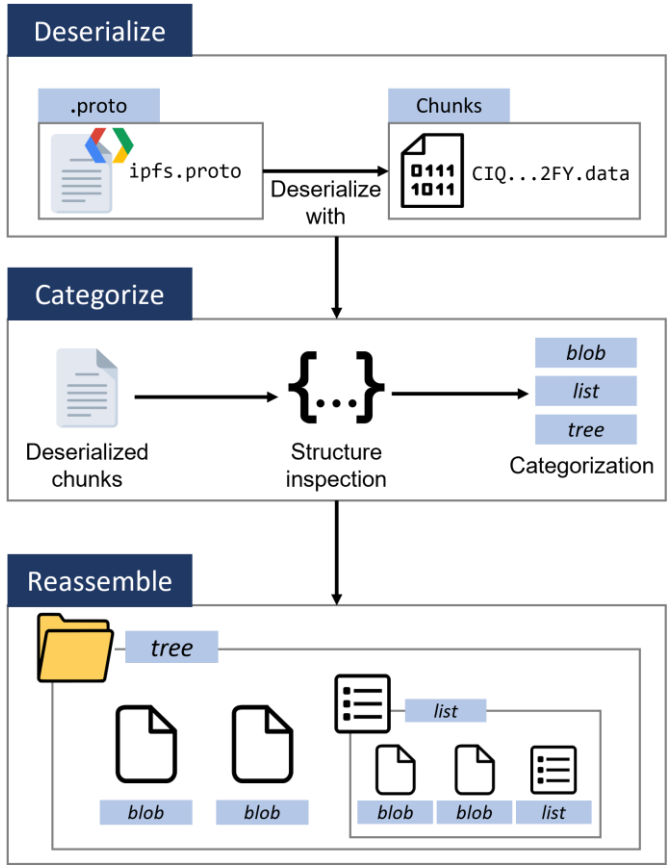


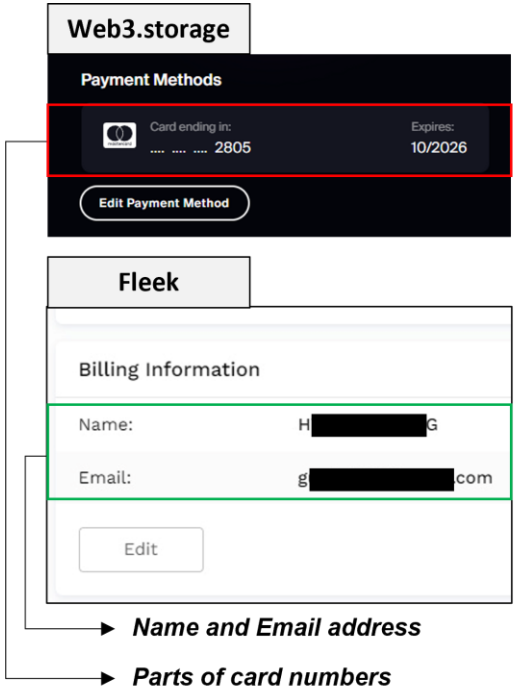
연구 소개

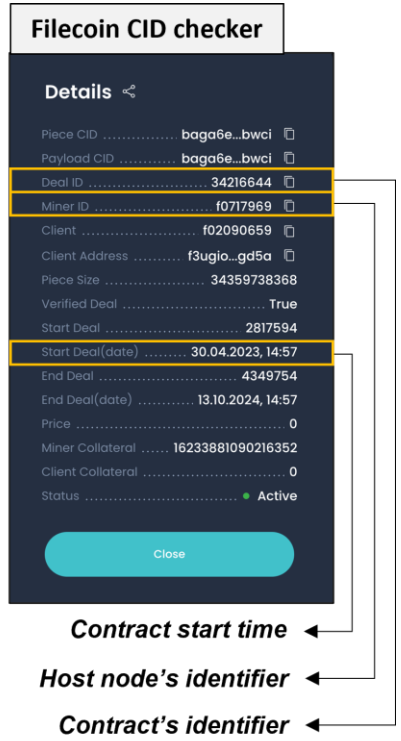
Case Study: 대규모 파일 공유 노드에서의 로컬 아티팩트 분석

대규모 파일 공유 노드 압수수색 → 캐시 재조합을 통한 파일 복원 → 사용자 데이터 수집









연구 소개

Other contributions..

- 7개의 DSS 서비스에 대한 6개의 포렌식적 특징 비교 분석

Table 1
Comparison table between seven well-known DSSs in consideration of six forensics-related features.

Features	IPFS	Filecoin based	BTFS	Internet Computer	Storj	Sia	Arweave based
Cryptocurrency	N/A	Filecoin (FIL)	BitTorrent (BTT)	Internet Computer (ICP)	Storj (STORJ)	SiaCoin (SC)	Arweave (AR)
Data encryption	No	No	No	No	Yes	Yes	No
Web hosting	Yes	Depends	Yes	Yes	Yes	No	Depends
Chunk reassembly	Yes	No	Yes	No	No	No	No
Credential cloning	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Content deletion	No	No	No	Yes	Yes	Yes	No

*N/A means there is no cryptocurrency based.

- 유사한 연구와의 비교

Table 2
Summary of comparative study with the existing digital forensic investigation frameworks.

Subject	Ref	Year	Preparation	Collection				Examination		Prevention
			Understand four area of the DSS	Node area	Peer area	Gateway area	Internet area	Chunk reassembly	Using credentials	Practical methods for prevention
Cloud	Chung et al.	2012		✓		✓			✓	
	Yang et al.	2022		✓		✓			✓	
P2P	Liberatore et al.	2010		✓	✓					
	Scanlon et al., 2015	2015		✓	✓					
	Teing et al.	2017		✓	✓					
DSS	Balduf et al.	2022			✓	✓				
	IF-DSS	Proposed	✓	✓	✓	✓	✓	✓	✓	✓

해외 논문 작성 방법

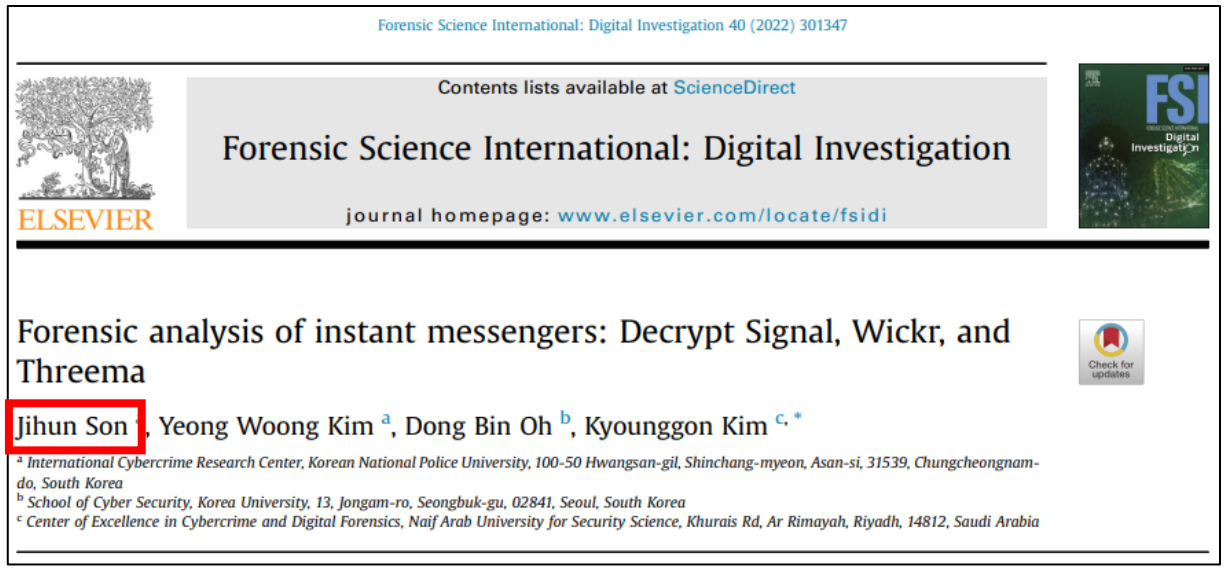
도.. ㄷ망... 도망쳐....!!!!!

해외 논문 작성 방법

WHY? 해외 논문인가?

- 확실히 검증된 성과이면서 사라지지 않는 실적

2022년 (with 김경곤 멘토님)



Forensic Science International: Digital Investigation 40 (2022) 301347

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

ELSEVIER

Forensic analysis of instant messengers: Decrypt Signal, Wickr, and Threema

Jihun Son [a], Yeong Woong Kim [a], Dong Bin Oh [b], Kyounggon Kim [c, *]

[a] International Cybercrime Research Center, Korean National Police University, 100-50 Hwangsan-gil, Shinchang-myeon, Asan-si, 31539, Chungcheongnam-do, South Korea
[b] School of Cyber Security, Korea University, 13, Jongam-ro, Seongbuk-gu, 02841, Seoul, South Korea
[c] Center of Excellence in Cybercrime and Digital Forensics, Naif Arab University for Security Science, Khurais Rd, Ar Rimayah, Riyadh, 14812, Saudi Arabia

2023년 (with 박정흠 멘토님)

Forensic Science International: Digital Investigation 46 (2023) 301611

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

ELSEVIER

DFRWS 2023 APAC - Proceedings of the Third Annual DFRWS APAC

IF-DSS: A forensic investigation framework for decentralized storage services

Jihun Son [a], Gyubin Kim [b], Hyunwoo Jung [c], Jewan Bang [d], Jungheum Park [a, *]

[a] School of Cybersecurity, Korea University, 145 Anam-Ro, Seongbuk-Gu, Seoul, South Korea
[b] AlpineLab, 169-16 Gasan Digital 2-ro, Geumcheon-gu, Seoul, South Korea
[c] AhnLab, 220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, South Korea
[d] Cyber Investigation Bureau, National Office of Investigation, Korean National Police Agency, Seoul, South Korea

- 기술적 난이도 + 논리적 전개 + 분야에 대한 전반적 이해

해외 논문 작성 방법

논문투고.log

- **2022년 FSIDI 저널**
  - 2020.03 ~ 2020.05 기존 연구
  - 2021.05 ~ 2021.09 연구 마무리 + 논문 작성 / 투고
  - 2021.12 논문 리뷰 (Minor Revision): 약 4개월 만
  - 2022.01 논문 재투고 & 논문 게재 확정 (Accept)
  - 2022.02 논문 게재
- **2023년 DFRWS 컨퍼런스**
  - 2022.12 ~ 2023.03 연구 진행
  - 2023.03 ~ 2023.05 연구 마무리 + 논문 투고
  - 2023.07 논문 리뷰 (Accept) 및 수정 사항 반영
  - 2023.10 컨퍼런스 발표 및 논문 게재

해외 논문 작성 방법

논문 작성 과정

- **주제 선정**
  - 같은 주제로 최소 10편 이상은 읽어보자

    → **"빈 틈 찾기"**
- **연구 진행**
  - 중꺽마.. 안 되는게 정상이야..

    오히려 좋아..

- **논문 작성**
  - 일단 뭐라도 쓰기, 완벽주의 버리기
- **논문 투고 및 수정**
  - 악으로 깡으로 버티자

논문 작성 도구

- **논문 검색**
  - Google Scholar, ~~sci-hxx~~
- **학회 정보**
  - (순진한 목소리로) 교수님 어디 낼까요?
  - CFP wiki, SCImago ..
- **영어 번역**
  - ♡Chat GPT ♡, ☆DeepL ☆
- **Latex 작성 관련**
  - (조심스럽게) 혹시.. 예전에 작성하신 Latex 있나요?

https://velog.io/@hunjison/해외-논문을-써보자
https://velog.io/@hunjison/해외-논문을-써보자-실전편

연구실 홍보

연구실 홍보

대.. 학.. 원.. ?


그래 나는
대학원생
나는 대학원생이다
왜라는 것은
필요하지 않다
시키니까 할 뿐이다


사, 살려줘..
대학원생은
사람이 할 짓이 아냐..
괜찮으세요?!
털썩!
박사..왜 내가
박사를 한다고 했지?
논문
졸업

연구실 홍보

대.. 학.. 원.. ?


누가
하라고 함?
누칼협?


알명수
122화 독도 도전할 명수
캐리어
보관장소
Cafe 미당 Restaurant
(중요한 건 꺾였는데도 그냥 하는 마음)

연구실 홍보

Digital Forensic Research Center

- **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)

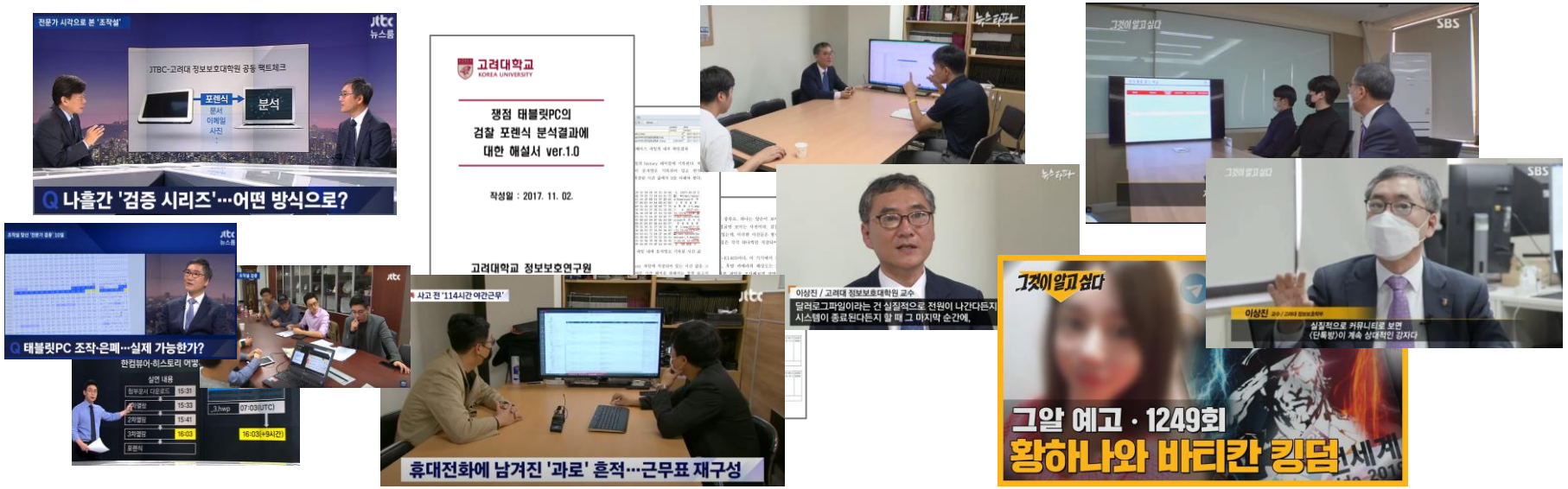
이상진 교수님(법, 정책)

박정흠 교수님(기술)

연구실 홍보

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



연구실 홍보

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

연구실 홍보

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
- **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)

연구실 홍보

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.

THANK YOU

Korea University
Digital Forensic Research Center

sns	facebook, linkedin ..
email	esby9774@gmail.com