아시아 지역의 디지털 포렌식 트렌드

김범진 @PLAINBIT

PLAINBIT

Contents

발표자 소개

김범진 이사

Certifications

- CCO, CCPA

Education

- 2008.05 : MBA (Entrepreneurship), 뱁슨 컬리지, F.W.Olin Graduate School of Business, 미국
- 2007.12 : MBA (교환학생), 칭화대학교, 중국
- 2002.05 : 학사, 컴퓨터 과학, 로체스터 대학교, 미국

History

- 2024.06 - 현재 : (주) 플레인비트, 사업개발 이사, 싱가포르 법인장
- 2021.08 - 현재: 성균관대학교 과학수사학과 겸임교수
- 2023.06 - 2024.05: (주) BHSN, LegalTech 영업 이사
- 2022.01 - 2024.05: (주) 플레인비트, eDiscovery 외부 컨설턴트
- 2021.11 - 2023.05: Favorite Medium Korea, 한국지사 대표
- 2021.10 - 2021.11: 프론테오 코리아, eDiscovery 및 Legal AI팀 전무
- 2009.02 - 2021.10: Interasia Corporation (홍콩 & 싱가폴), Co-founder - eDiscovery 및 LegalTech 사업 총괄
- 2002.08 - 2006.08: (주) 그라티브, 솔루션 개발자

아시아 디지털 포렌식 동향

PLAINBIT

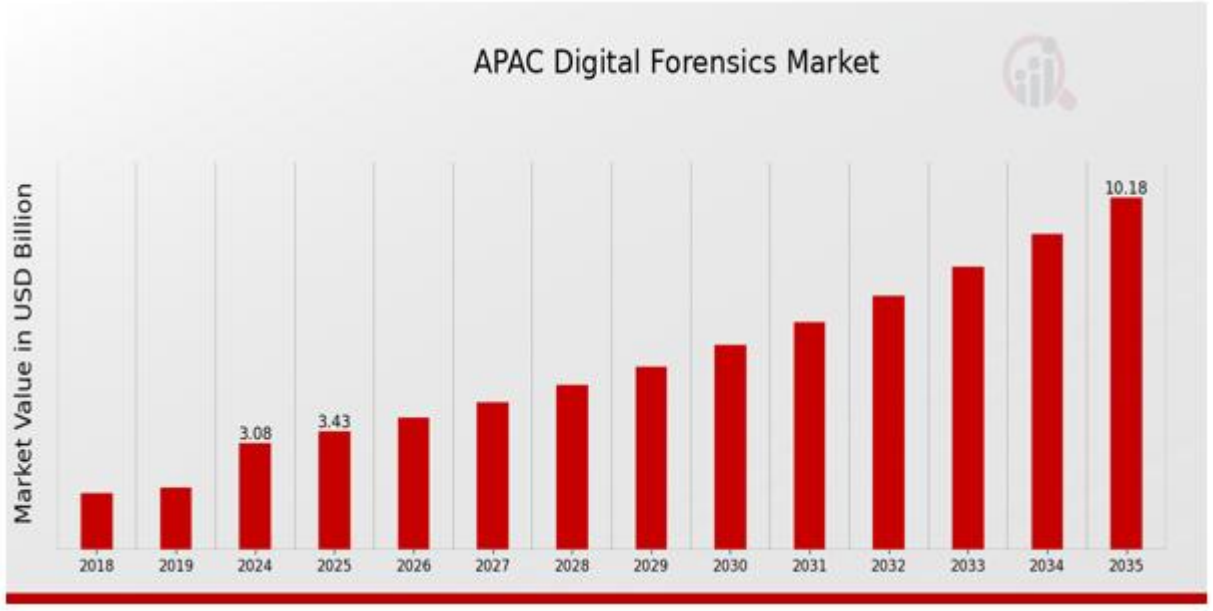
Why Asia?

아시아는 디지털 포렌식의 핫스팟

- 전 세계 사이버 범죄의 45% 이상이 아시아에서 발생
- 디지털 경제 성장률, 세계 평균의 2배 수준
- 동남아의 초고속 디지털화
  - 매일 약 12만명의 새로운 인터넷 사용자 증가
  - 디지털 경제는 2030년까지 최대 2조 달러 규모로 성장 예상
- 클라우드·핀테크·스마트시티 확산 → 증거 폭증
- 각국의 데이터 보호법 강화로 '법+기술 포렌식' 중요성 급증

아시아 지역의 디지털 포렌식 시장 규모 및 성장세

- 아시아·태평양(APAC) 지역 산업 성장 전망: 2024년 30억 달러 → 2035년 101억 달러 이상
- 연평균 성장률(CAGR): 약 11.5%
- 주요 성장 시장: 인도, 중국, 싱가포르, 베트남
- 성장 요인: 사이버 범죄 증가, 규제 강화, 인공지능(AI) 및 사물인터넷(IoT)의 확산



출처: https://www.marketresearchfuture.com/reports/apac-digital-forensics-market-57420

아시아 지역의 위협 현황

- 지정학적 긴장 심화
  - 남중국해, 중국-대만, 태국등의 국경 분쟁
  - 미중 관세 갈등
  - 북한, 중국, 러시아 간 연대 강화
- 주요 통계:
  - 2023: 동남아 지역 기업 대상 사이버 공격 **4,300만 건**
  - 2024: 싱가포르 침해 사고의 **71.4%가 제3의 협력기업**을 통해 발생
  - 주요 피해 산업 변화
    - ✓ 2023: 제조업, 금융(BFI), 기술·미디어·통신(TMT)
    - ✓ 2024: TMT, 금융(BFI), 공공 부문

SG	Manufacturing	Professional services	TMT	**Financial services**	Real estate
MY	Manufacturing	**Government**	TMT	Professional services	Retail
ID	TMT	**Financial Services**	**Government**	Energy	Manufacturing
SK	**Government**	TMT	Manufacturing	**Financial services**	Defence
AU	TMT	Engineering & construction	Retail	**Government**	**Financial services**
GCR	TMT	Manufacturing	Professional services	Healthcare	**Financial Services**

출처: Ensign Infosecurity, Cyber Threat Landscape 2024

SG	BFI	Business & Professional Services	Hospitality	Retail	TMT
MY	Automotive & Mobility / Defence & Law Enforcement / Energy & Utilities	BFI	Hospitality	Public Sector	TMT
ID	BFI	Defence & Law Enforcement	Hospitality	Public Sector	TMT
SK	Aviation	BFI	Public Sector	TMT	Transport
AU	Aviation	BFI	Public Sector	TMT	Transport
GCR	BFI	Healthcare	Public Sector	TMT	Transport

출처: Ensign Infosecurity, Cyber Threat Landscape 2025

새로운 개인정보 보호 및 데이터 주권 법률과 그 영향

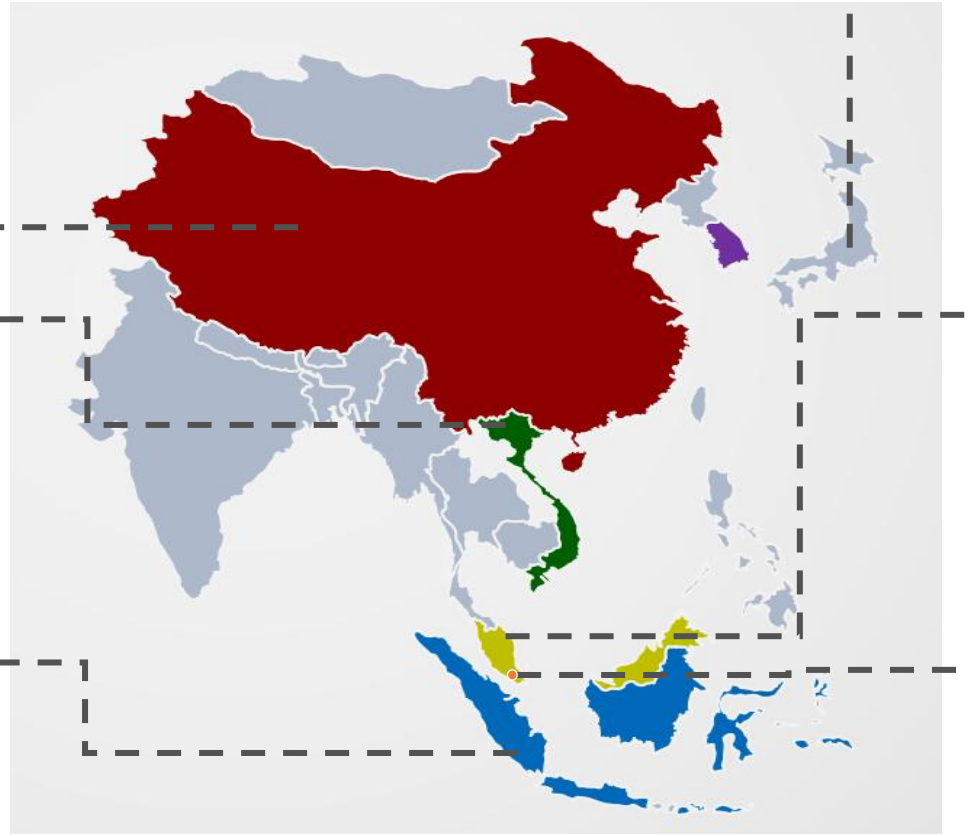
국가별 법안들은 지속적으로 개정 중

중국

사이버보안법 개정 (2025.09)
- 강력한 데이터 현지화
- 높은 법적 책임

일본

능동적 사이버 방어법 제정 (2025.05)
형사절차법의 디지털화 법안 승인 (2025.02)
새로운 총리 – 사이버보안 중점 예정



베트남

전자거래법 (2023년 개정, 2024.07 시행)
사이버보안법 (2019년 시행, 2025년 개정)
개인정보보호법 (2026.01 시행)

Malaysia

사이버보안법 (2024.8.26 시행)
개인정보보호법 개정안 (2025.1.1부터 단계적 시행)
형사소송법 및 형법 개정안 (2024년) – 온라인 사기 및 자금동결 중심

인도네시아

개인정보보호법 (2022년 제정)
전자정보거래법 (2024.01 시행)

Singapore

사이버보안법 개정안 2024 (2024.05.07)
- 범위를 CII에서 Non-Provider-Owned CII 및 STTC (임시 보안위험 관리대상 시스템)로 확대

국가별 포렌식 특이점

다양한 포커스

- 중국
  - 미국 제재로 인해 해외 포렌식 제품을 사용할 수 없어서 독자적으로 다양한 포렌식 제품을 개발 (Meiya Pico, DataPort Tiko등)
  - 상당한 수준의 포렌식 제품을 개발
- 홍콩 및 싱가포르
  - 영미법 기반의 eDiscovery 절차를 위한 디지털 포렌식 시장
- 일본
  - 국가 사법 기관 이외의 디지털 포렌식은 회계 법인/법무 법인 중심의 내부 조사, 감사가 민간에서 가장 큰 시장
  - 미국 소송에 따른 eDiscovery 서비스 기업들
- 동남아
  - 저렴한 포렌식 툴 사용: Magnet, EnCase등도 잘 없음
  - 모바일 포렌식: Oxygen, Belka등 제품 활용
  - 지역에 대한 락이 없는 제품 선호
- 인도네시아 - 디지털 샤리아 포렌식
  - 세계 최대 무슬림 국가, 디지털 샤리아 금융 확대.
  - 샤리아 원칙(진실성, 신의) 따라 디지털 증거와 분석 강조.
  - 샤리아 규정과 디지털 포렌식 기술의 조화 및 표준화가 발전 방향

모바일 중심의 사회

아시아는 주요 증거는 스마트폰

- 아시아 지역은 한국, 중국, 일본 등 수십 여종의 스마트폰을 다양하게 사용 → 같은 안드로이드 폰이어도 포렌식 툴 미지원 가능
  - Xiaomi, Oppo, Huawei, OnePlus, Hitachi, Sharp, Sony, Panasonic, HTC, Asus, Honor, Vivo, ZTE
- 메신저 복구 수요 급증
  - 한국: 카카오
  - 일본, 대만, 태국: 라인
  - 중국: WeChat
  - 베트남: Zalo
  - 캄보디아, 미얀마: Telegram
  - 필리핀: 페이스북 메신저
  - 싱가포르, 홍콩등 그 외: WhatsApp
- 앱 데이터 및 GPS, 통화기록 등 교차분석 강화

디지털 포렌식의 미래

PLAINBIT

디지털 포렌식의 혁신

PLAINBIT

AI, Cloud, Blockchain

01 증거 검토 자동화

- AI와 머신러닝이 방대한 증거 데이터를 효율적으로 분석
- 숨겨진 패턴을 찾아 핵심 정보를 신속하게 식별
- 포렌식 절차의 정확성과 속도를 동시 향상

02 딥페이크 탐지

- 첨단 기술로 딥페이크와 인공 신원을 식별
- 조작된 영상·음성 데이터를 정밀 분석
- 법정 제출 증거의 진정성을 보장하고 사기 수사 신뢰도 강화

03 클라우드 포렌식의 적응과 진화

- 국가 간 데이터 분산으로 인한 수집·관리 문제 대응
- 국제 표준과 법적 절차 준수로 증거 무결성 확보
- 수사기관 간 협업을 통한 안전한 클라우드 증거 관리

04 블록체인 및 암호화폐 포렌식

- 250종 이상의 암호화폐 거래를 실시간 모니터링
- 불법 거래 탐지 및 탈취·세탁 자산의 추적 강화
- DeFi 모니터링과 스마트 계약 감사로 위험 사전 차단
- 양자컴퓨팅을 활용한 프라이버시 코인 해독 시도

Challenge & Opportunity

PLAINBIT

Challenge

AI & 딥페이크
- 합성 미디어로 증거 진위 검증 복잡
- AI 탐지 도구로 콘텐츠 진본성 확인 필요

블록체인 & 암호화폐
- 암호화폐 활용한 랜섬·자금세탁 증가
- 지갑 추적 및 온-체인 활동 분석 필수

클라우드 & 가상화
- AWS, Azure, GCP 사고 증가
- Multi-tenancy·관할권·로그 접근이 주요 과제

양자 컴퓨터
- 기존 암호화 체계 무력화 가능성
- 포스트-양자 암호에 대한 대응 필요

Opportunity

AI 도구들
- 합성 아티팩트 탐지
- 로그·악성코드 분석 속도 향상

블록체인
- 투명하고 변경 불가능한 원장
- 거래 추적 및 행위자 연계 가능

클라우드 포렌식
- 세부 로그·스냅샷 확보 (e.g., AWS CloudTrail)
- 신속한 보존 및 확장형 분석 지원

양자 컴퓨터
- 포렌식 패턴 인식 성능 향상 가능
- 포스트-양자 암호를 활용하여 증거 보안 강화

디지털 포렌식 전문가의 미래

진화하는 역량 (Evolving Skillset)

클라우드 포렌식, 블록체인 추적, AI 기반 증거 검증,
그리고 랜섬웨어 복호화 기술 분야의 전문성을 개발 필요

국제 협력 (International Collaboration)

국경을 넘어 다양한 국가의 지역 파트너 및
법집행기관과 협력하되,
법을 위반하지 않는 방식으로 협업의 중요성

사전 대응형 포렌식 (Proactive Forensics)

사고가 일어나기 전에 포렌식 대응 체계를 준비하고,
사후 분석 중심에서 **사전 대비 중심의 포렌식 체계**로
전환

MITRE ATT&CK 매핑

포렌식 결과를 MITRE ATT&CK 전술과 연계하여
공격자의 행동 패턴을 이해하고 탐지·대응 역량을 강화

침해(Compromise)가 사고(Incident)로 연결되지 않아야 합니다.

PLAINBIT