디지털 포렌식의 챌린지

PLAINBIT

#1. (현재) 디지털 포렌식 분석 환경의 문제점

- ✓ 디지털 데이터의 출처가 매우 다양해지고 있다.
- ✓ 늘어나는 디지털 데이터만큼 분석 인력을 확보하기 어렵다.
- ✓ 대부분의 분석이 기본적인 내용 확인인 것에 반해 투입되는 인력은 전문가로 구성되어 있다.
- ✓ 분석 건마다 전처리 작업의 기다림과 많은 수동적인 클릭이 동반된다.
- ✓ 디지털포렌식 업무의 숙련도가 빠르게 향상되지 않는다.
- ✓ 분석을 위한 인프라가 특정 조직과 특정 사건에 집중되어 있다.

이 문제는 더 많은 사람이나
컴퓨팅 리소스로 해결할 수 있는
문제가 아니다.

기술과 자동화가 답이다.

#2. 디지털 데이터와 증거 능력

DEAD

LIVE

aws

Azure

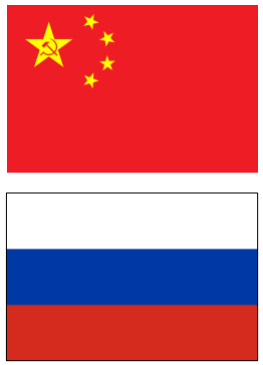
Google Cloud

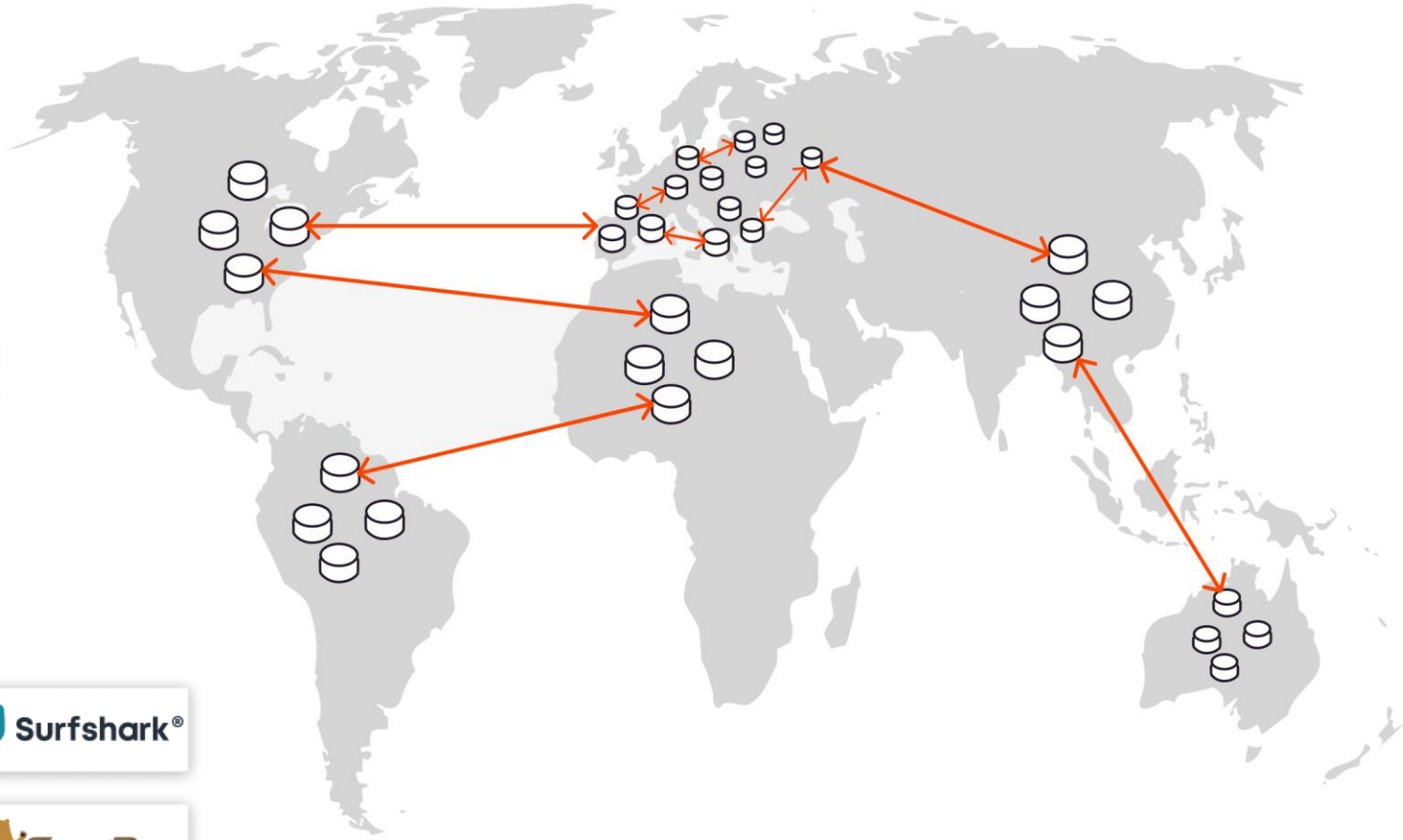
NHN Cloud

NAVER Cloud

kt Cloud

#3. 네트워크 추적의 한계





ExpressVPN
NordVPN
avast
Surfshark
IVPN
VPN Unlimited
GOOSEVPN
TunnelBear
IPVANISH VPN
elo .net
FrootVPN
AstrillVPN
Invisible browsing VPN
blackVPN
Perfect Privacy
vyprvpn by golden frog

#4. 디지털 포렌식과 AI

이미지 영상 분석 – 얼굴 인식, 객체 탐지, 텍스트 인식 등

자연어 처리 – 이메일, 채팅 로그, SNS 게시글 등을 분석해 자동 분류

LLM을 활용한 **디지털 포렌식 챗봇**

이상 행동 탐지 – 사용자 아티팩트를 분석해 비정상 행위 탐지

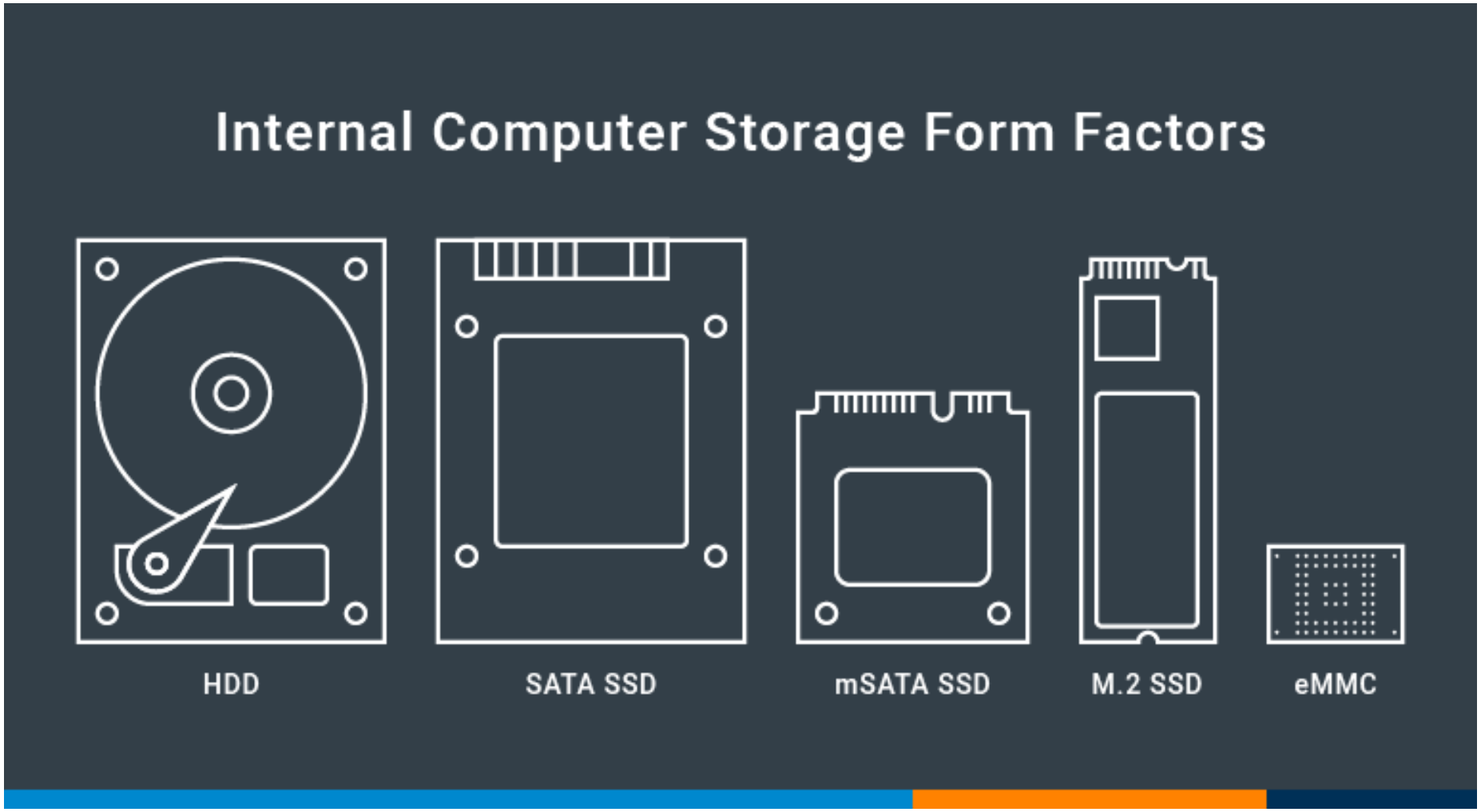
데이터 복구 – 대용량의 데이터 처리의 자동화 및 효율화, 은닉 탐지

데이터 분석 및 분류 – 방대한 양의 문서,이미지,이메일을 빠르게 분류

증거 연관성 분석 및 매핑 – 다양한 소스의 데이터의 연관성 + 매핑

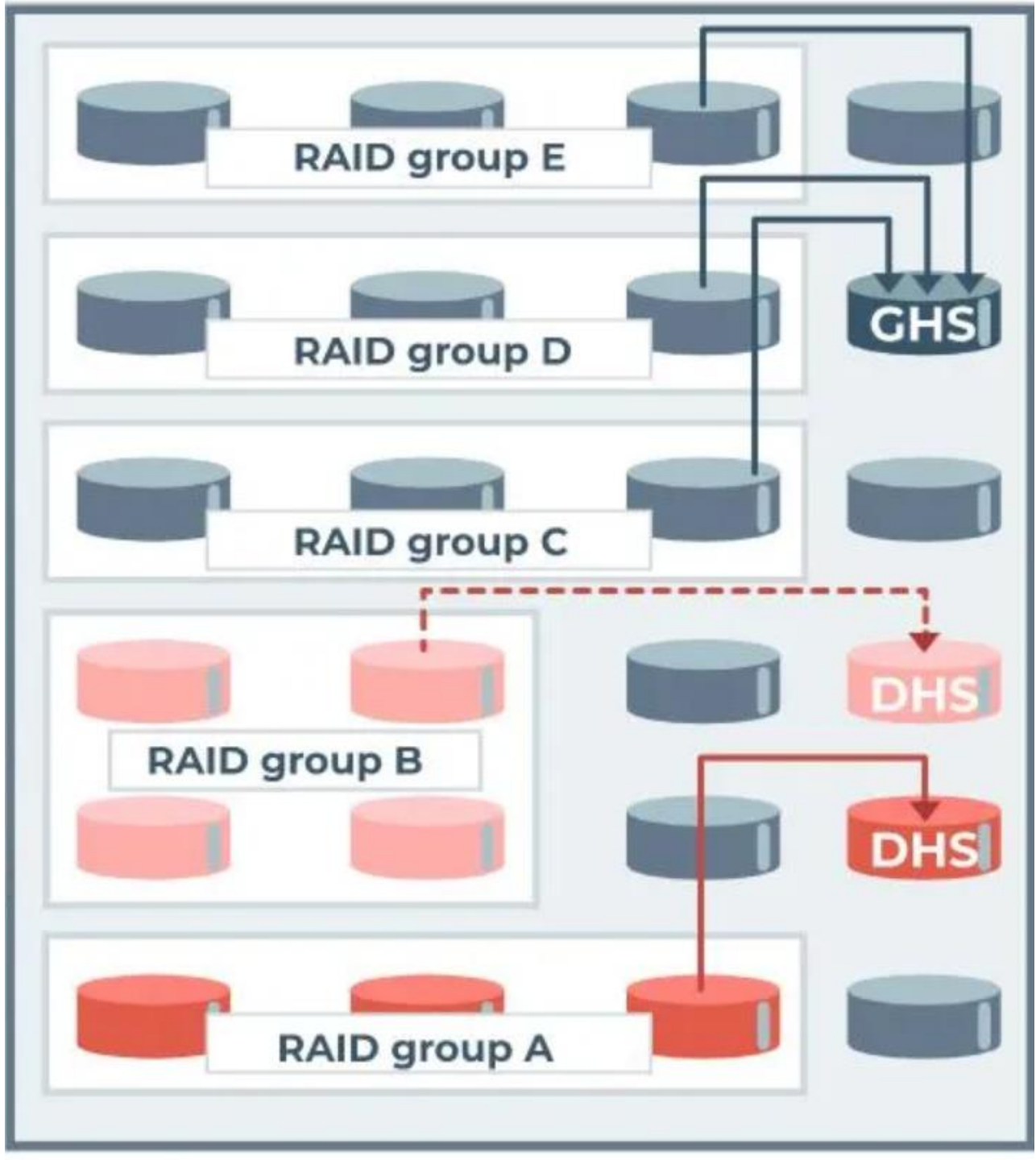
사회적 네트워크 분석 – SNS, 채팅 등에서 사회적인 관계성 분석

#5. 데이터 복구의 어려움


Internal Computer Storage Form Factors
HDD
SATA SSD
mSATA SSD
M.2 SSD
eMMC

#6. 다양한 스토리지 관련 기술

- SAN, DAS, NAS
- RAID(SHR,0,1,5,50E,6,10,F1), JBOD
- LVM, Dynamic Disk(LDM)
- CoreStorage, Time Machine
- Virtual Disk(VMWare,Hyper-V,XEN)
- FileValut2, BitLocker, LUKS, eCryptFS



#7. 멀티미디어 포렌식의 한계

데이터 양과 처리 속도 – 대량의 사진, 비디오 파일 처리에 높은 컴퓨팅 자원 필요

디지털 조작 탐지의 어려움 – Deepfake가 일반화되고, 정교한 조작 기술의 발전

저화질 영상과 손상된 데이터 – 세부 정보가 손실되어 인물 식별과 이벤트 재구성의 어려움

다양한 코덱과 포맷 – 독자 규격의 사용도 많아 모든 포맷을 다루는 도구의 부족

법적, 윤리적 문제 – 분석 과정에서 개인정보나 사생활 침해의 문제가 발생

인간 해석의 한계 – 최종 판단에 주체인 전문가의 주관적인 요소가 개입될 가능성이 높음

AI 기반 분석의 신뢰성 문제 – 잘못된 탐지, 오탐, 데이터셋의 편향, 훈련 부족의 문제점

#8. 민간 디지털 포렌식과 책임감

KOREA LABORATORY ACCREDITATION SCHEME
KOLAS
REFERENCE MATERIAL PRODUCER NO.