

디지털 포렌식, 어디까지 왔나?

JK Kim

CEO & Founder

Plainbit Co., Ltd.



1. 포렌식 환경 변화
2. 수집 관련 이슈
3. 분석 관련 이슈

포렌식 환경 변화

국내 기업 - 호스트/네트워크 기반 솔루션

- 과거 해외 제품 리셀러에서 벗어나 자체 제품 개발 및 신규 서비스 모색



- 해외 포렌식 제품 리셀링 + 포렌식 전문 교육



- 해외 포렌식 제품 리셀링 + 자체 정보감사 제품
- 더존비즈온 합병 → 해외 컨설팅(포렌식 랩 구축)



- 해외 포렌식 제품 리셀링 + 포렌식 전문 교육



국내 기업 - 모바일 솔루션

- 모바일 포렌식 업계의 춘추전국시대

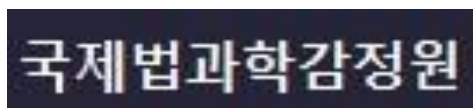


mobile



국내 기업 – 서비스 분야

- 포렌식 기반 다양한 서비스가 생겨남!!
 - 디지털 증거 분석 서비스
 - 침해사고 분석 서비스



포렌식 환경 변화

국내 인력 수요의 변화

감사

Knowledge :

작성지

- 서버, 네트워크 장비, 기술 이해
- Global 보안 트렌드, 국
- 국내 개인정보보호법, 등

Skill :

- (필수) 웹/모바일 취약점
- (필수) Linux/Unix/Win
- (필수) 보안 취약점 진단
- (필수) 보안 취약점 트러
- (추가) 정보보호 관리체

기타 (필요 자격, 어학능력, 해)

- 국내/외 해킹대회 수상
- 리버스엔지니어링, Dig
- C, Java, Python 프로그
- CISA, CISSP, SIS, PMI
- 영어회화능력 우수자 등
- 법학전공자로 학위 소지자 또

[업무내용]

- 침해사고 분석

* 디스크 포렌식을 통한 침해원인 및 문제점 도출

* 악성코드 분석을 통한 특징 및 증상 도출

- 보안위협 분석

* 국내외 신규취약점 및 유흥에 대한 분석 및 조사

- 그룹 내 침해사고 분석

- 국내외 SW 취약점 분석

[자격요건]

- 8년 이상 경력

- Digital Forensics (EnCase)

- Malware Reverse Engineering 경험

- Networking 관련지식

- Languages: Assembly / Java / Python / C / javascript 무대

- Certification: EnCE, GREM, GCFA, CHFI 무대

- 악성코드분석 유경험자 무대

- 디지털포렌식 자격증 보유자 무대

- 침해사고분석 유경험자 무대

- 네트워크관련 자격증보유자 무대

- 영어가능자 무대

- 외국인 지원 가능

포렌식 랩 구축 서울시, 디지털포렌식센터 개설

한국형 모덜더존비즈온, 브루나이에 포렌식센터 수출

오만 무스카트에 '조'입력시간 | 2015.12.07 16:42 | 김관용 기자 kky1441@

기자의 다른 기사보기

머니투데이 진달래 기자 |

독자의견



기사

소셜

▶ 팔자주름 1회 시술로 90살까지 유지??

미래창조과학부가 한

온과 함께 진행한 오'브루나이 정부투자 보안회사ITPSS와 계약

개소식을 열었다고 1 25만 달러 규모 국가 디지털 포렌식 센터 컨설팅 사업 수행

이날 오전 10시(현지 [이데일리 김관용 기자] 더존비즈온(012510)(25,000원)이 동남아에 포렌식센터를 수출하는 쾌거를 이
오만 정보기술청장, ▲ 350 +1.42%)이 동남아에 포렌식센터를 수출하는 쾌거를 이
오만한국대사, 송정수 됐다. 더존비즈온은 올 초 오만 디지털 포렌식 센터 구축
지털포렌식센터장 등 사업을 통해 국내 최초로 포렌식 센터 대규모 해외 수출
(1028만 달러 규모) 기록을 세운바 있다.

이번 사업은 미래부도 더존비즈온은 총 25만 달러(2.8억 원) 규모의 브루나이
사를 통해, 실제 프로 국가 디지털 포렌식 센터 컨설팅 사업을 수주해 브루나이
다. ITPSS와 계약 체결을 완료했다고 7일 밝혔다.



도구/인력 인증

도구/장비

인증

한국형 CFTT



인력

인증

디지털포렌식전문가자격

EnCE (GuidanceSoftware)

GCFE (GIAC)

GCFA (GIAC)

CHFI (EC-Council)

CCFP (ISC)²

포렌식 학과 개설

- **현장형 실무 인재 양성을 목표로 설립!!**
 - **군산대학교** 법학+컴퓨터공학 (디지털포렌식전공)
 - **동국대학교** 국제정보대학원 정보보호학과 (사이버포렌식전공)
 - **상명대학교** 경영대학원 사이버보안경영학과 (포렌식과정)
 - **서울전문학교** 정보보호계열 포렌식보안과정
 - **서울호서전문학교** 사이버해킹보안과 (포렌식과정)
 - **영산대학교** 사이버경찰학과 (포렌식과정)
 - **전주기전대학** 포렌식정보보호과
 - **한국IT전문학교** 정보보호학과 사이버포렌식과정

구글의 노력 +_+



수집 관련 이슈

증거 수집과 무결성 – 형사소송법 106조 3항, 피압수자 참여권 (1/2)

제106조(압수)

③ 법원은 압수의 목적물이 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체(이하 이 항에서 "정보저장매체등"이라 한다)인 경우에는 **기억된 정보의 범위를 정하여 출력하거나 복제하여 제출받아야 한다**. 다만, 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 **현저히 곤란하다고 인정되는 때에는 정보저장매체등을 압수할 수 있다**. <신설 2011.7.18.>

- 압수 집행종료 시점은 언제인가?
 - 수사기관 사무실로 옮긴 후, 전자정보를 탐색하는 과정 ➔ 압수.수색영장 집행의 일환
- 압수과정에서 지켜져야 할 것은?
 - 피압수자의 참여권 보장
 - 압수 후 피압수자에게 압수목록 교부

증거 수집과 무결성 – 형사소송법 106조 3항, 피압수자 참여권 (2/2)



원본과 증거 능력 (1/4)

'원세훈 前 국정원장 집에 화염병 투척' 무죄 선고 법원 "증거 불충분... CCTV 파일 위변조 가능성"

기사등록 : 2014.04.27 15:41

-가 +가

서울중앙지법 형사24부(부장 김용관)는 국가정보원 대선개입 의혹과 관련해 원세훈 전 원장의 집에 화염병을 투척한 혐의(현존건조물방화미수) 등으로 기소된 시민단체 활동가 임모(37)씨에 대해 "증거가 불충분하다"는 이유로 무죄를 선고했다고 27일 밝혔다. 검찰이 유력한 증거로 제시한 폐쇄회로(CC)TV 동영상 파일의 위변조 가능성이 높아 유죄를 인정하기 어렵다는 취지다.

임씨는 지난해 5월5일 오전 6시20분쯤 서울 관악구 남현동 원 전 원장의 집 마당에 시너를 넣어 불 붙인 소주병 두 개를 던지고 달아난 혐의로 기소됐다. 당시 화염병은 정원 나무에 걸려 땅에 떨어지면서 꺼졌지만, 검찰은 원 전 원장 집 주변에 설치된 방범용 CCTV와 주변 가게의 CCTV 등에서 확보한 영상을 복사 혹은 재촬영해 이를 근거로 임씨를 재판에 넘겼다.

그러나 재판부는 "이 사건의 주요 증거인 CCTV와 관련, 디지털 증거로 사본이 제출될 경우 동일성과 무결성이 인정돼야 한다"며 "CCTV 저장장치에서 수사관 USB 등으로 최소 2~3회 이상 복사되는 과정에서 파일을 담은 저장장치를 전혀 봉인하지 않는 등 복사파일의 동일성과 무결성을 인정할 수 없다"고 밝혔다. 디지털 자료는 변조 가능성이 높은 만큼 증거능력은 동일성 여부 등을 엄격히 따져야 한다는 대법원 판례를 따른 것이다.

원본과 증거 능력 (2/4)

■ 원본이라면 무결성과 동일성이 인정되는가?

- (조건) – 원본일 경우 수정하기 어려워야 한다!!
- CCTV 원본 저장매체에 있는 영상 VS. USB로 복사된 영상
- SD 카드에 있는 블랙박스 영상 VS. 별도 저장매체로 복사된 영상

■ 멀티미디어 데이터의 변조 식별 가능성

- 데이터 일부를 조작하거나 중간 영상 프레임을 삭제하는 경우 ➔ 어느 정도(?) 식별 가능
- 영상의 뒷부분을 잘라버리는 경우 ➔ 식별 불가능

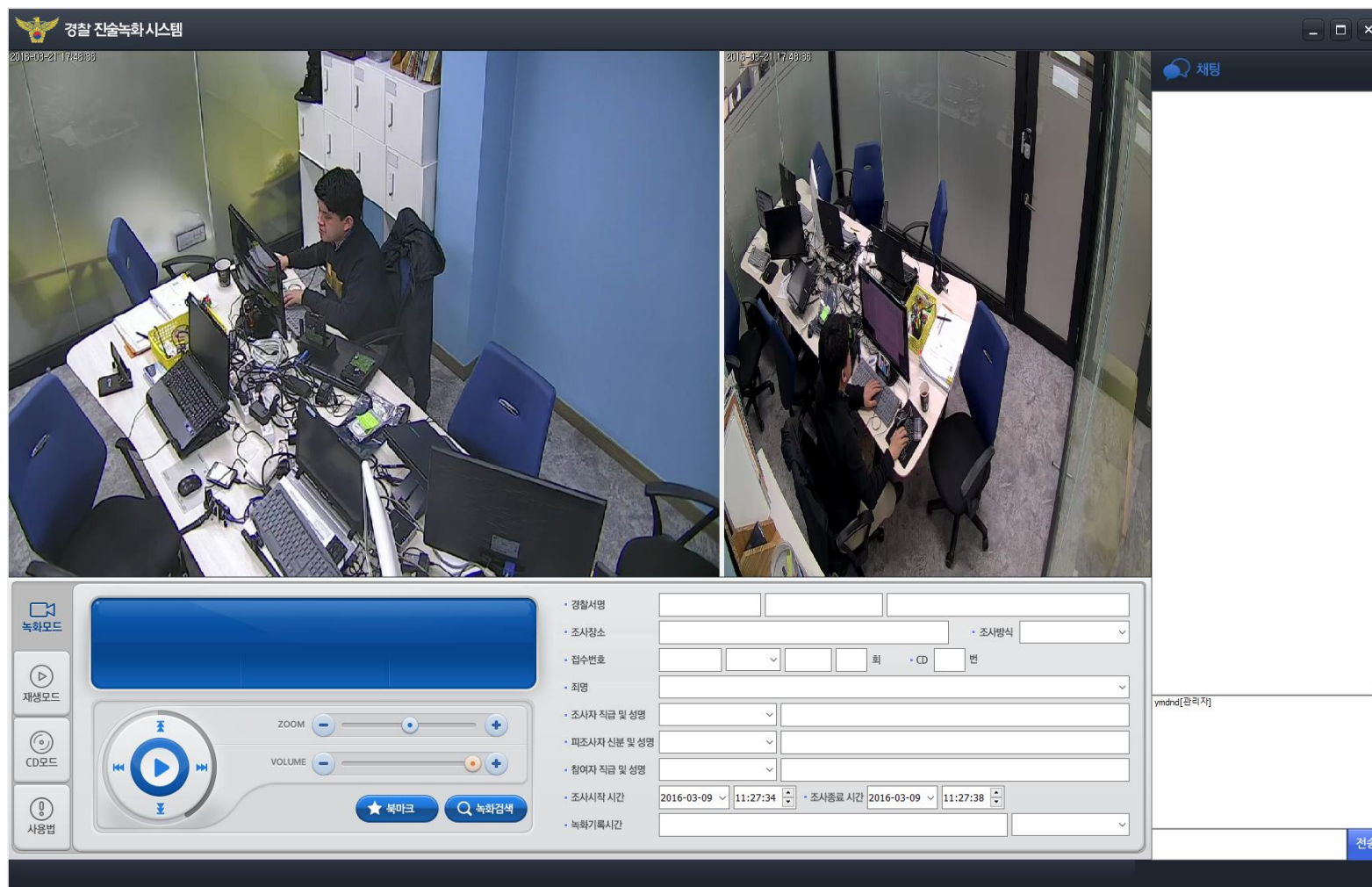
원본과 증거 능력 (3/4)

■ 원본이 증거능력을 가지려면!!

- 원본 데이터가 그 시스템에서 생성되었는지 증명이 필요!!
- 운영체제라면 포렌식 아티팩트로 증명 가능
- 단순히 데이터를 저장하는 방식인 경우(블랙박스, CCTV 등)는?
- 원본성을 증명할 수 있는 추가적인 방법 마련 필요!!
 - ✓ 블랙박스 데이터 위/변조 방지 기능

원본과 증거 능력 (4/4)

■ 영상 위/변조 방지 기능 예



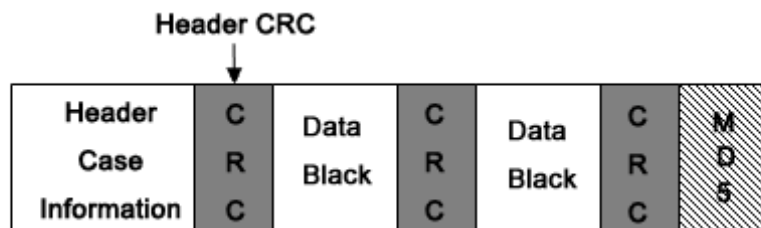
라이브 데이터와 증거 능력

■ 증거 능력 이슈 (DEAD vs. LIVE)

- 자기 디스크 형식의 저장매체 → DEAD 상태 가능!!
- 반도체 형식의 저장매체 → DEAD 상태 불가능!!

■ 왜 모바일 데이터 수집에는 관대한가?

■ EWF(Expert Witness Format)이 만들어진 이유?



안드로이드 – 녹스(KNOX) (1/2)

- 안드로이드 스마트폰 데이터 수집 방법
 - **MANUAL** 수집
 - **S/W** 기반 수집
 - ✓ Logical – Content Provider
 - ✓ Logical - ADB Backup
 - ✓ Physical – Rooting Exploitation + USB Debugging Mode
 - ✓ Physical – AP/BL Exploitation
 - ✓ Physical – Custom Recovery Image (Flashing)
 - **H/W** 기반 수집
 - ✓ JTAG
 - ✓ Chip-Off + Re-balling

Samsung Knox



스마트폰 라이브 수집?

- 안드로이드 폰도 아이폰처럼 FDE가 적용된다면?

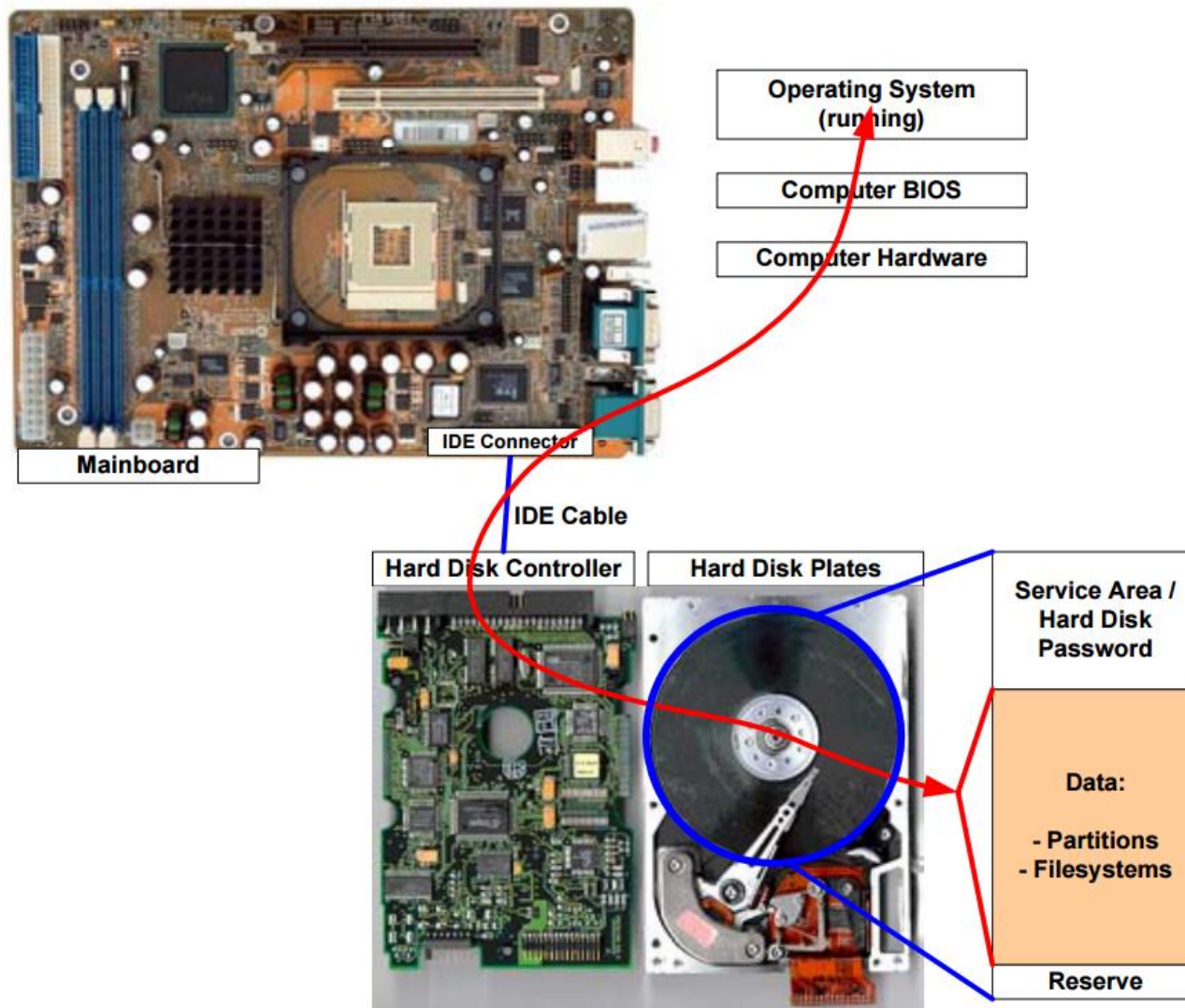


The screenshot shows the Android Security website. The top navigation bar includes the 'android' logo and links for 'Source', 'Devices', 'Security' (highlighted in green), and 'Compatibility'. On the left, a sidebar lists various security topics: 'Overview', 'Bulletins', 'Authentication', 'Keystore', 'Trusty TEE', 'Full Disk Encryption' (highlighted with a blue background and an upward arrow), 'SELinux', and 'Verified Boot'. The main content area features the title 'Full Disk Encryption' in large, multi-colored text. Below it, a section titled 'What is full disk encryption?' provides a definition: 'Full disk encryption is the process of encoding all user data on an Android device using an encrypted key. Once a device is encrypted, all user-created data is automatically encrypted before committing it to disk and all reads automatically decrypt data before returning it to the calling process.' At the bottom, another section titled 'What we've added for Android 5.0' is partially visible.

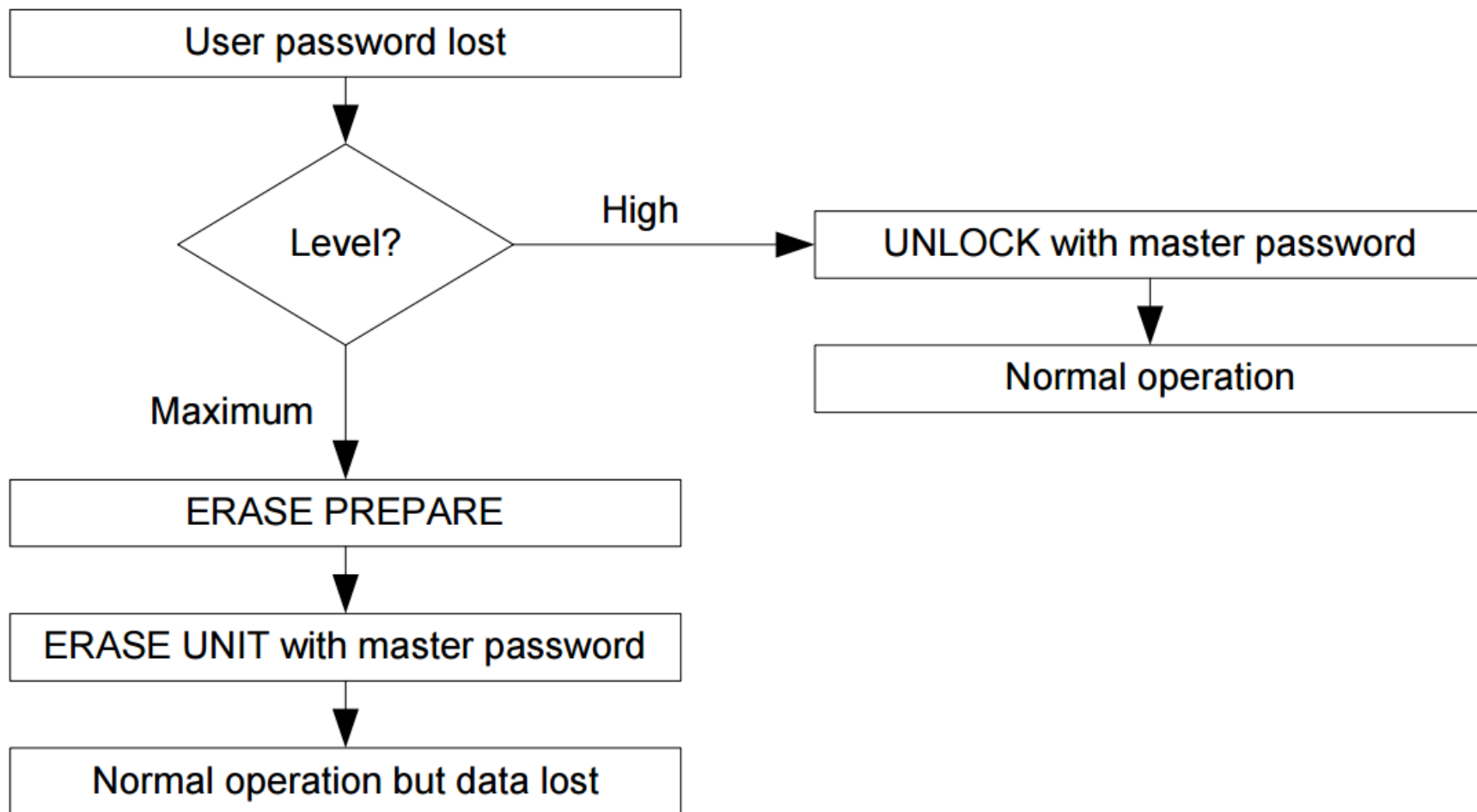
드라이브 락(LOCK)

- 최근 하드디스크는 패스워드 설정 기능 제공 (not BIOS)
 - BIOS를 이용한 설정
 - 3rd Party 도구를 이용한 설정
- 설정된 패스워드는 **HDD SA(Service Area)** 영역에 저장
- **2가지 패스워드**
 - 사용자 패스워드 (User Password), 사용자가 설정한 패스워드
 - 마스터 패스워드 (Master Password), 제조사에서 미리 설정한 패스워드
- **사용자 패스워드 설정 방법**
 - **ATA COMMAND** : SECURITY SET PASSWORD

드라이브 락(LOCK)



드라이브 락(LOCK)



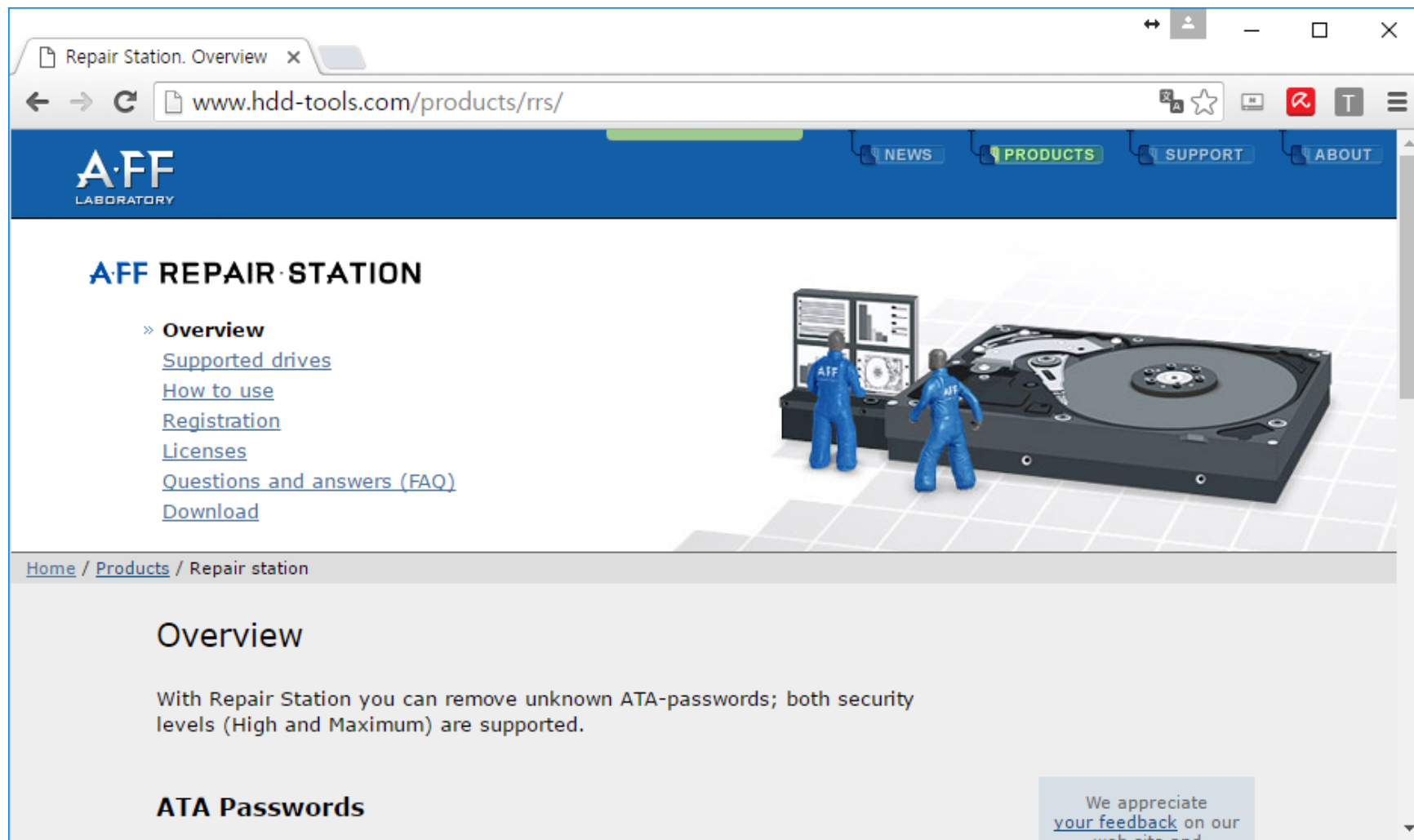
드라이브 락(LOCK)

- ATA SECURITY 모드 명령어 제한

Command	Locked
IDENTIFY DEVICE	Executable
IDENTIFY PACKET DEVICE	Executable
READ SECTOR(S)	Command aborted
READ SECTOR(S) EXT	Command aborted
READ STREAM DMA EXT	Command aborted
READ STREAM EXT	Command aborted
READ VERIFY SECTOR(S)	Command aborted
READ VERIFY SECTOR(S) EXT	Command aborted
SECURITY DISABLE PASSWORD	Command aborted
SECURITY SET PASSWORD	Command aborted

드라이브 락(LOCK)

- A-FF REPAIR STATION (\$49.95 for 1 unlock)



The screenshot shows a web browser window displaying the A-FF REPAIR STATION product page. The browser's address bar shows the URL www.hdd-tools.com/products/rrs/. The website has a blue header with the A-FF LABORATORY logo and navigation links for NEWS, PRODUCTS, SUPPORT, and ABOUT. The main content area features the title "A-FF REPAIR STATION" and a list of links: Overview, Supported drives, How to use, Registration, Licenses, Questions and answers (FAQ), and Download. To the right of the links is a 3D illustration of a hard drive with two small figures in blue suits standing next to it. Below the links, a breadcrumb trail reads "Home / Products / Repair station". The "Overview" section contains the text: "With Repair Station you can remove unknown ATA-passwords; both security levels (High and Maximum) are supported." At the bottom, there is a section titled "ATA Passwords" and a feedback message: "We appreciate your feedback on our website and".

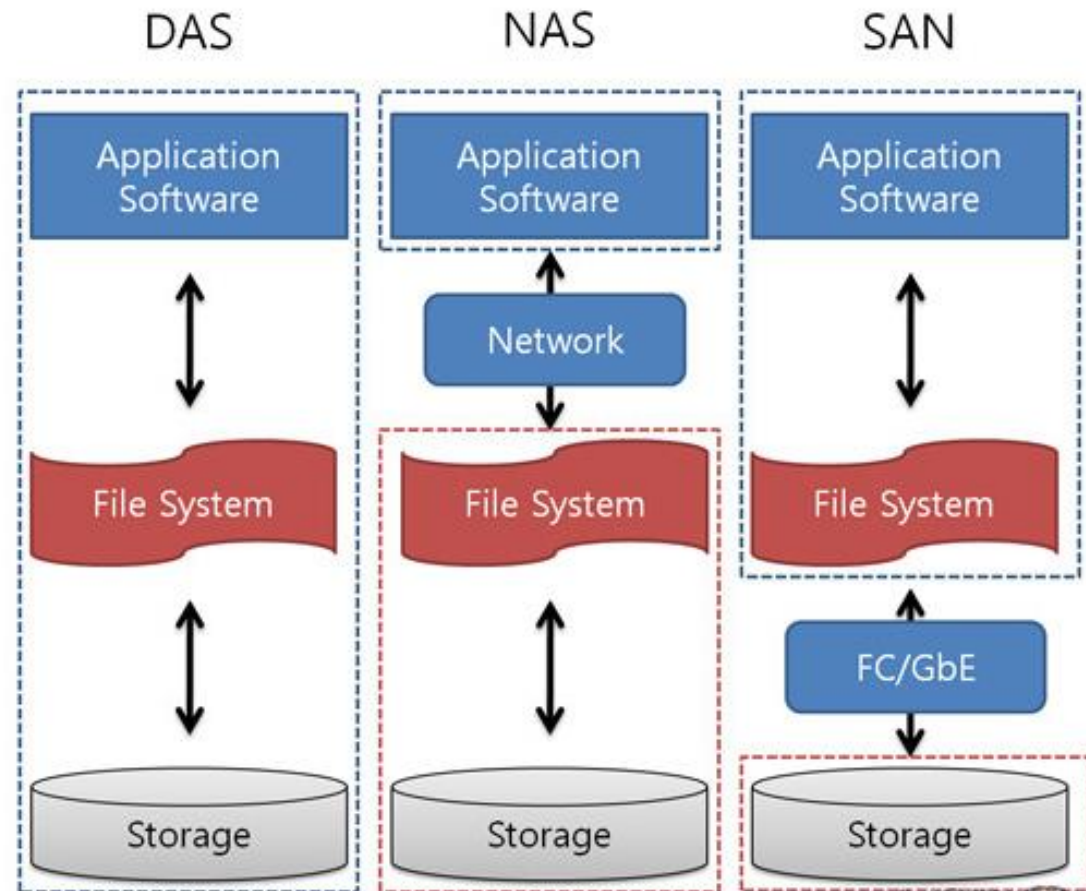
엔터프라이즈 저장매체 데이터 수집

■ 엔터프라이즈 스토리지

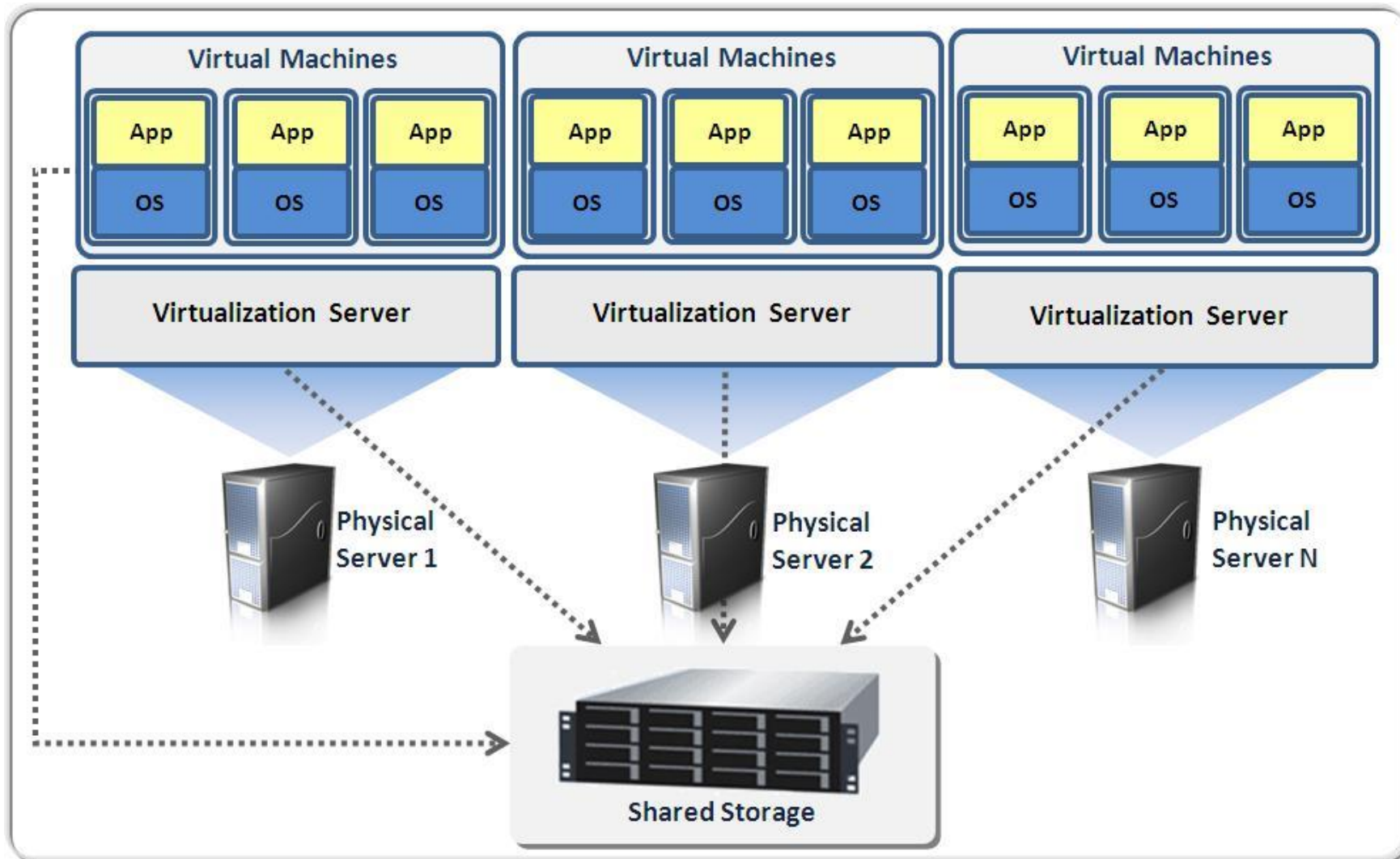
- DAS, NAS
- IP(iSCSI) SAN, FC SAN

■ 엔터프라이즈 스토리지 구성

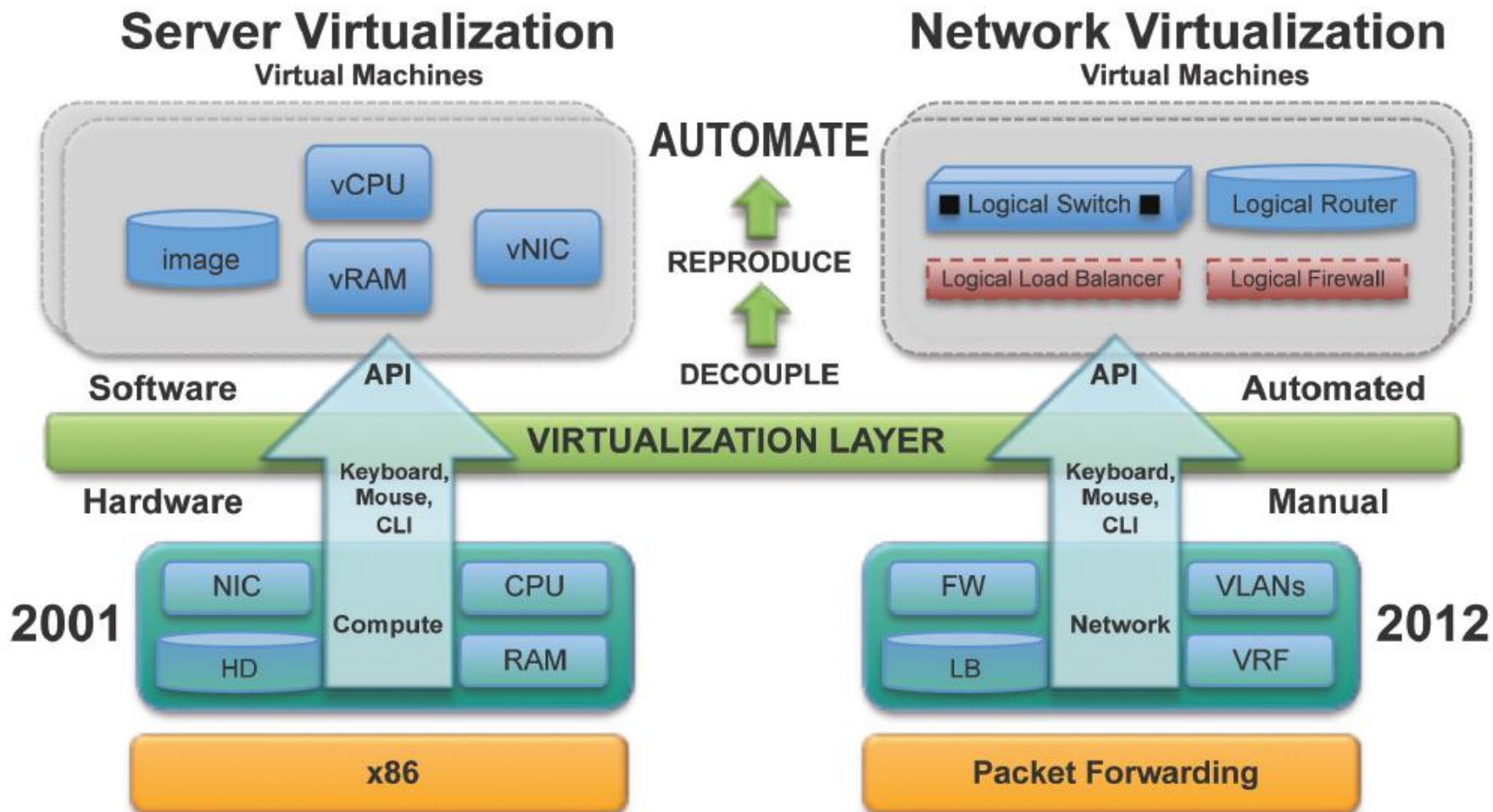
- RAID (S/W, H/W)
- LVM
- JBOD



가상화 환경 (1/2)



가상화 환경 (2/2)



라이브 포렌식 활용 증가 (1/3)

■ 디스크 포렌식 장점

- 삭제된 흔적 파악 가능
- 알려지지 않은 흔적 파악 가능
- 최후 스킵 사용 가능 (키워드, 패턴 검색 등)

■ 디스크 포렌식 단점

- 디스크 획득 시간이 오래 걸림 → 분석 시간도 오래 걸림
- FILELESS 악성코드의 등장

■ 식별만 빠르게 된다면, 빠른 분석을 위해 라이브 포렌식 필요!!

라이브 포렌식 활용 증가 (2/3)

■ 라이브 포렌식 장점

- 빠른 데이터 수집 가능 → 빠른 분석
- 비즈니스 연속성에 영향을 미치지 않고 대응 가능
- DEAD 상태로 갈 수 없는 시스템 대응
- 최근 일어난 일을 정확히 알 수 있음 (안티안티포렌식)
- 인코딩, 암호화, 실행압축된 데이터를 비교적 쉽게 분석

■ 라이브 포렌식 단점

- 디스크 기반 데이터 분석의 한계
- 식별 능력이 부족하거나 대응이 느릴 경우 활동도가 크게 떨어짐!!

■ 조직의 목적에 따라 라이브 포렌식을 적극 활용하는 추세!!

라이브 포렌식 활용 증가 (3/3)

■ 실시간 라이브 포렌식 활용

- 기존 시스템 이벤트 + 포렌식 아티팩트 모니터링
- 네트워크 기반 보안 제품 개념 → 호스트 기반으로...

■ 실시간 라이브 포렌식 이슈

- 호스트 자원 사용의 최소화
- 수집된 이벤트의 규칙(룰) 생성
- 일석이조의 효과를 볼 수 있도록 수집 데이터 선별

원격 포렌식 활용 증가 (1/2)

- **포렌식 분석팀 + 랩을 갖추기는 했는데... → 업무 리소스의 대부분은 데이터 수집**
 - 부서간 물리적인 거리가 있는 경우
 - 전국 단위의 지사를 보유하고 있는 경우

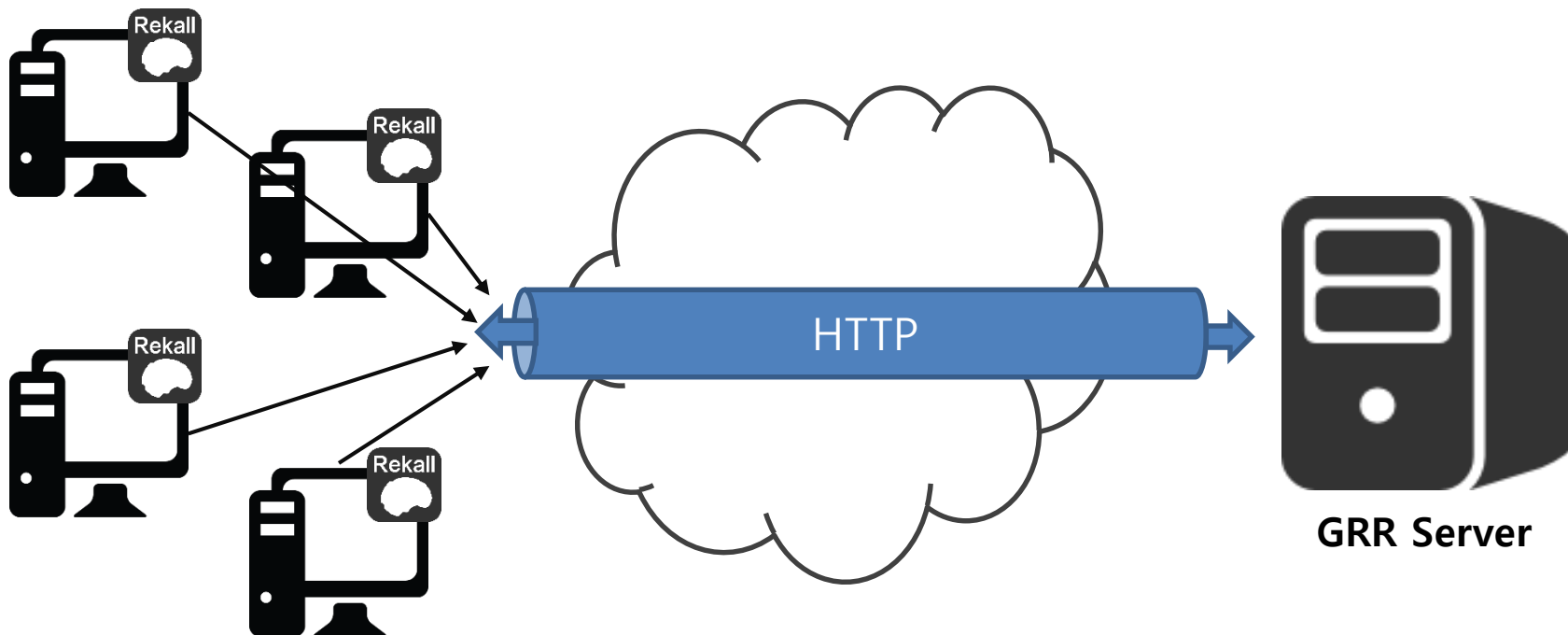
- **원격 포렌식의 이점!!**
 - 물리적으로 거리가 먼 시스템의 포렌식 아티팩트를 바로 수집 가능
 - 필요한 경우 저장매체 이미징도 가능 (네트워크 속도에 기반, 업무 연속성 고려)
 - 빠른 수집으로 빠른 분석 가능
 - 불필요한 업무 리소스를 최소화

- **원격 포렌식 효과를 높이려면 식별 노력을 높이고, 빠른 대응 절차를 마련해야 함!!**

원격 포렌식 활용 증가 (2/2)

■ 원격 포렌식 활용 이슈

- 사고 당한 시스템을 인터넷에 연결시켜줘야 하는가?
- 전송 과정에 데이터 노출은 없는가?
- 라이브 포렌식 + 원격 포렌식 ➔ ReKall + GRR Rapid Response



분석 관련 이슈

포렌식 복구 연구

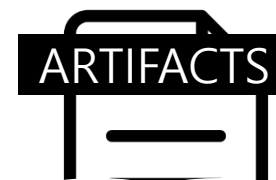
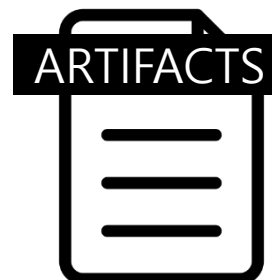
■ 일반 복구

- 데이터 복구 분야에서 일반화
- 문서 파일, 동영상 파일, 그림 파일, 이메일 파일 등



■ 포렌식 복구

- 포렌식 아티팩트 파일 복구
 - ✓ 프리패치, 레지스트리, 바로가기 파일, 메타데이터 등
- 포렌식 레코드 복구
 - ✓ DB 레코드, 레지스트리 레코드 등
 - ✓ 손상되었지만 포렌식적 의미가 있는 데이터



안티안티포렌식

■ 안티포렌식 기술의 일반화

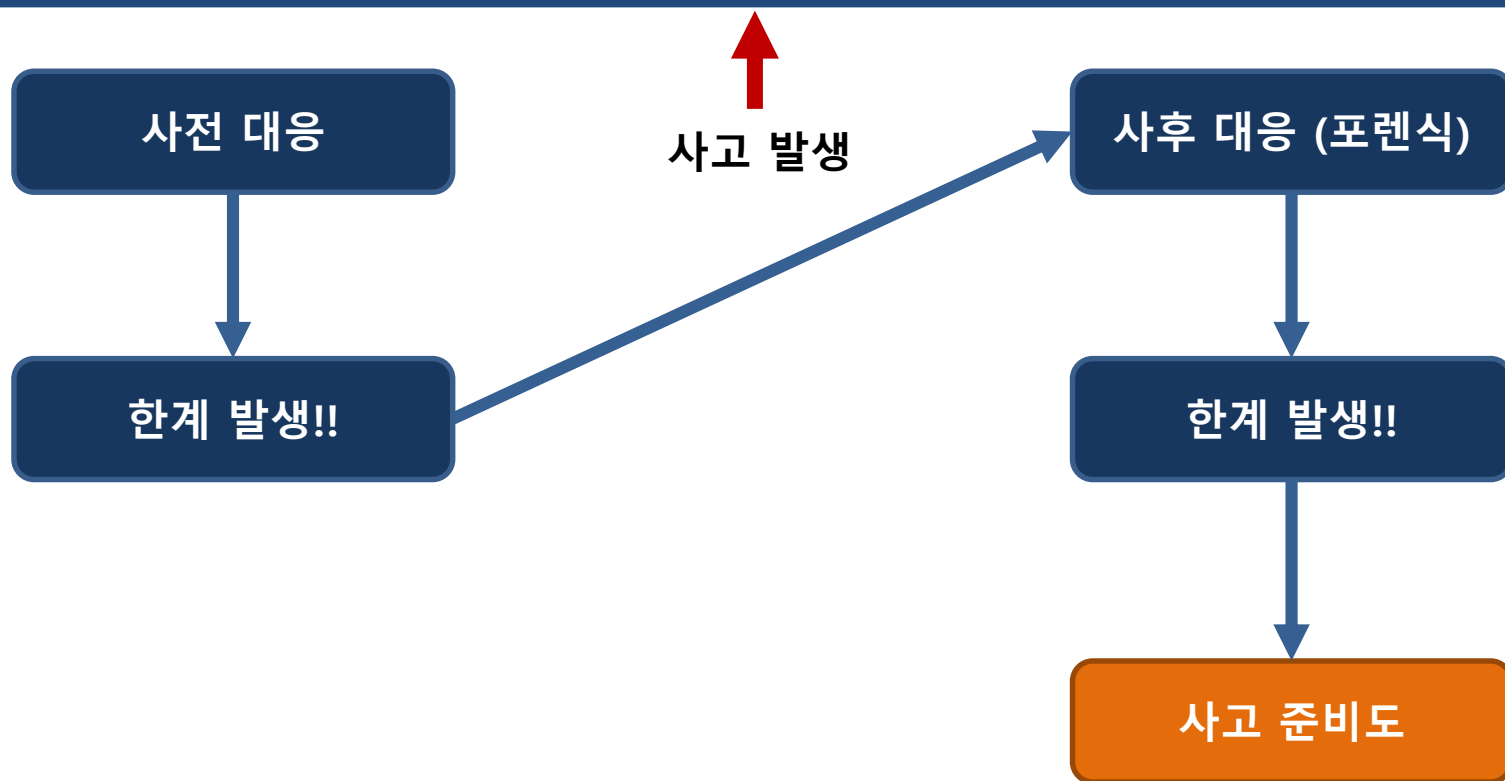
안티포렌식	안티안티포렌식
데이터 삭제	데이터 복구
데이터 은닉, 루트킷	은닉 탐지
암호화, 인코딩, 난독화	암호 분석, 디코딩, 난독화 해제
시간 조작, 메타데이터 조작	통합 분석
흔적 최소화	라이브 포렌식
자연 현상	빠른 대응

■ 효과적 안티안티포렌식

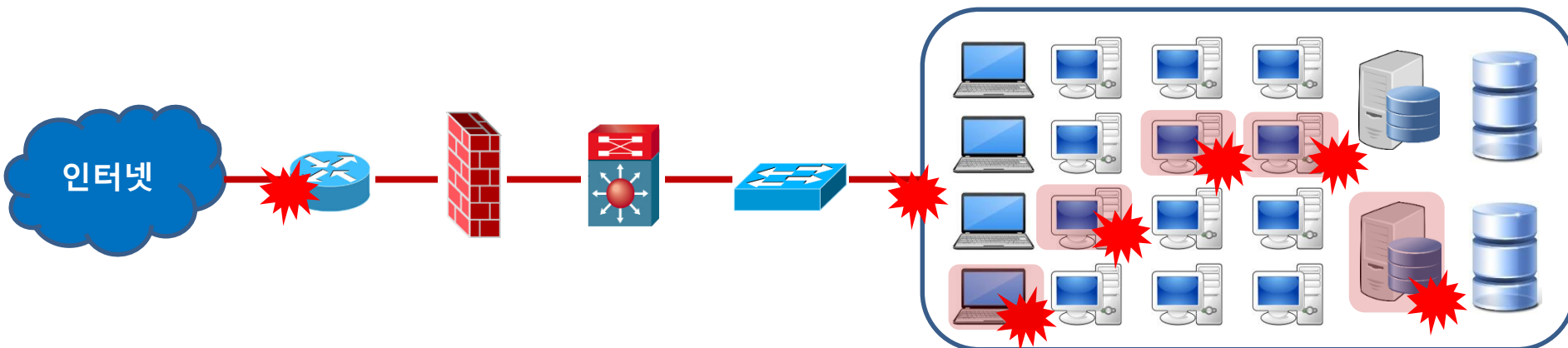
- 상시 모니터링 강화 + 대응 절차 고도화 (골든 타임 준수)

사고 준비도

기술로 어렵다면 정책으로 보완하라!!



포렌식 아티팩트 분석 수준



침해 유입 지표

- 웹 브라우저 → DBD
- ActiveX, Java Applet
- (스피어) 피싱 메일
- (외부) 저장매체
- 클라우드, 소스공유, FTP

침해 실행 지표

- 프리패치/RecentFileCache
- 호환성 캐시
- 바로가기, 점프 목록
- 파일시스템 로그, VSC
- 레지스트리
- WER, AV 로그

침해 전파 지표

- 네트워크 스캔
- ARP 스니핑, 스푸핑
- PTH (Pass The Hash)
- PTP (Pass The Pass)
- 스피어 피싱 메일
- 관리 서버 악용

침해 지속 지표

- 악성코드 선호 경로
- 악성코드 선호 파일명
- 작업스케줄러
- 자동실행 목록
- 시간 조작
- 루트킷/슬랙 공간

타임라인 분석

최근 데이터 분석 흐름

- 타임라인 분석 + 인덱스 엔진 + 시각화

- 타임라인

- plaso

- 인덱스 엔진 사용

- SPLUNK
- ELASTIC SEARCH

- 시각화

- Timesketch
- Kibana



