전자금융사고에서의 디지털포렌식
(and... Military Police Digital Forensic)

Jo YongHyun

khu410@gmail.com

Who am I ?

Previous employment:

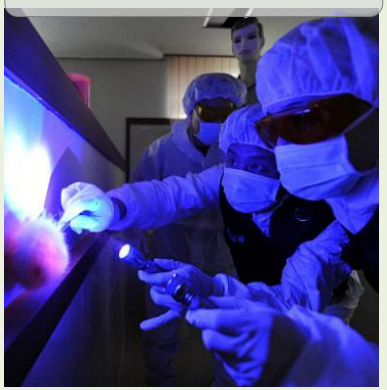
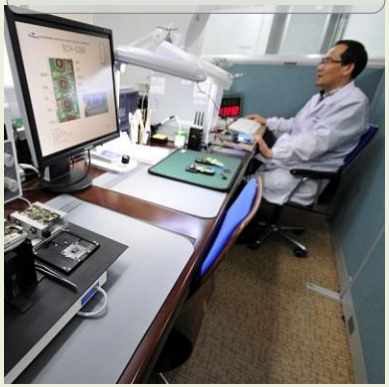
Financial Company Security Manager – 2009-2014
Security Consulting – 2007-2009
Army CID CyberCrime Special Agent – 2000-2007

Total Information Security, Forensic Investigations, & Consulting – 13+ years


전반전
Military Police Digital Forensic
후반전
전자금융사고에서의 디지털포렌식
연장전
Forensic Investigation
vs
Forensic Examination

Military Police Digital Forensic

MISSION

군사법경찰	과학수사	대테러/경호	디지털포렌식
			

군사법경찰관이란

- **제43조(군사법경찰관)** 다음 각 호의 어느 하나에 해당하는 사람은 군사법경찰관으로서 범죄를 수사한다.

1. 헌병과(憲兵科)의 장교, 준사관 및 부사관과 법령에 따라 범죄수사업무를 관장하는 부대에 소속된 군무원으로서 범죄수사업무에 종사하는 사람

2. 법령에 따른 기무부대에 소속된 장교, 준사관 및 부사관과 군무원으로서 보안업무에 종사하는 사람

3. 국가정보원 직원으로서 국가정보원장이 군사법경찰관으로 지명하는 사람

4. 검찰수사관

CASE

애인 토막살해 후 암매장한 군인에 무기징역

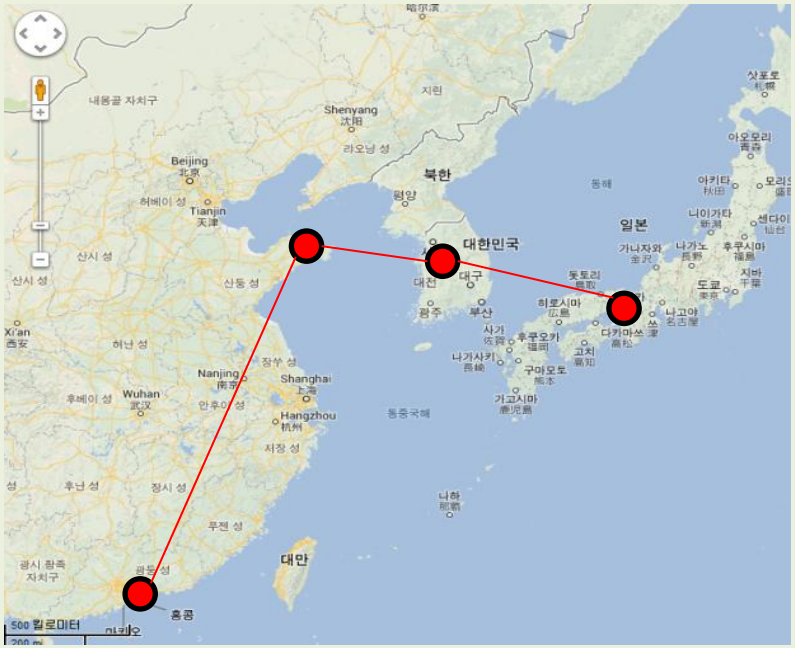
결혼을 약속한 애인을 살해하고 시신을 엽기적인 방법으로 토막내 암매장한 군인에게 무기징역형이 확정됐다. 대법원1부(주심 김지형 대법관)는 살인 및 시체은닉 혐의로 기소된 육군 김모(34) 중사의 상고심에서 무기징역을 선고한 원심을 확정했다고 4일 밝혔다.

김씨는 "말다툼하다 애인이 약을 과다 복용해 스스로 목숨을 끊었는데 너무 놀라 신고하지 못했고, 살인자로 오해받을까봐 시신을 은닉했다"고 주장했다. 국과수 부검 결과 약물복용이 직접적인 사인이 됐는지는 밝혀지지 않았고 김씨의 컴퓨터에서 사건 발생 후 인터넷에서 '자살방조', 'CCTV보존기간' 등의 자료를 검색한 점이 드러났다.

대법원은 "간접증거가 개별적으로는 완전한 증명력을 갖지 못하더라도 종합적으로 봤을 때 증명력이 있다면 범죄사실을 인정할 수 있다"고 밝혔다.

CASE


박안서 소령/육군중앙수사대 과학수사대장
IP 분석을 통해서 범행 장소가 외국인 것을
확인하고 인터폴과 협조해서 현지에 수사관을
파견해 하드디스크와 CCTV 자료를 확보했습니다


Shenyang
Beijing
북한
대한민국
일본
대구
부산
Nanjing
Shanghai
Wuhan
Hangzhou
대만
홍콩

CASE

내일을 봅니다 www.sbs.co.kr - 인쇄하기 - Chrome

w3.sbs.co.kr/news/newsEndPagePrintPopup.do?news_id=N1000037630

뉴스 > 정치

K-2소총 분실부대 수류탄 6발도 없어져

남상석 기자 LIKE 0 최종편집: 2005.12.12

지난 8일 K-2 소총 2정을 분실했던 강원도 고성군 육군 모 부대에서 실탄과 함께 수류탄도 없어진 것으로 알려졌습니다.

육군 관계자는 11일 "K-2 소총 2정을 분실한 율곡부대 예하 모 대대에 대한 정밀조사 과정에서 실탄 700여발과 수류탄 6발이 비는 것으로 나타나 현재 정확한 조사를 벌이고 있다"고 밝혔습니다.

군은 지난 8일 소총만 분실됐다고 설명했지만 실탄 수백발과 수류탄

내일을 봅니다 www.sbs.co.kr - 인쇄하기 - Chrome

w3.sbs.co.kr/news/newsEndPagePrintPopup.do?news_id=N1000046677

뉴스 > 사회

총기탈취 용의자 2명 검거…"은행 털려 했다"

한지연 기자 LIKE 0 최종편집: 2006.01.05

CASE(U.S CID)

Army deploys PC forensics technology in Iraq

Summary: *Equipment and techniques normally associated with resolving business disputes have made their way into post-war Iraq, where the army is using it to find evidence of war crimes*

By Munir Kotadia | September 29, 2003 -- 14:45 GMT (07:45 PDT)

Follow @zdnetaustralia

Comments 0 Votes 0 Like 0 Tweet 0 Share more -

Email Print
Google+ Del.icio.us
Digg StumbleUpon
Reddit Technorati
Pinterest Slashdot

The British Army has revealed that it is using PC forensics te
recovered electronic media to investigate illegal activities un

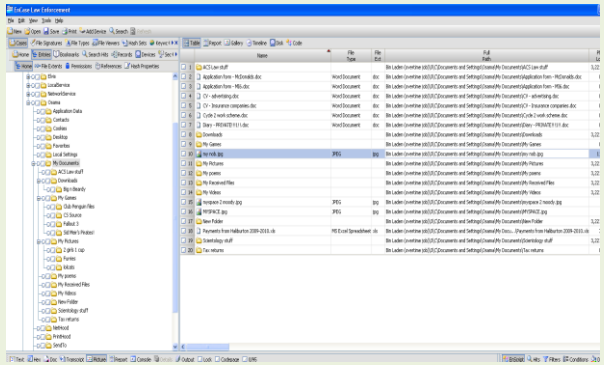
The British Army's Land Information Assurance Group (LIAG)
services -- has been deployed in Iraq since the end of the w
partially destroyed electronic media. The unit is responsible
and emails from all types of electronic storage media in orde
can stand up in court.

"Any evidence gained has to be legally admissible, and we knew that computer forensic techniques were far more thorough than other methods of data analysis," said the LIAG's Major John Pringle in a statement.

Simon Janes, operations manager for computer forensics at data recovery specialist Ibas UK, which provided the army with a "mobile forensics laboratory", said one of the most important requirements for the recovered data was to guarantee that it had not been altered in any way -- a requirement for evidence to be given in court.

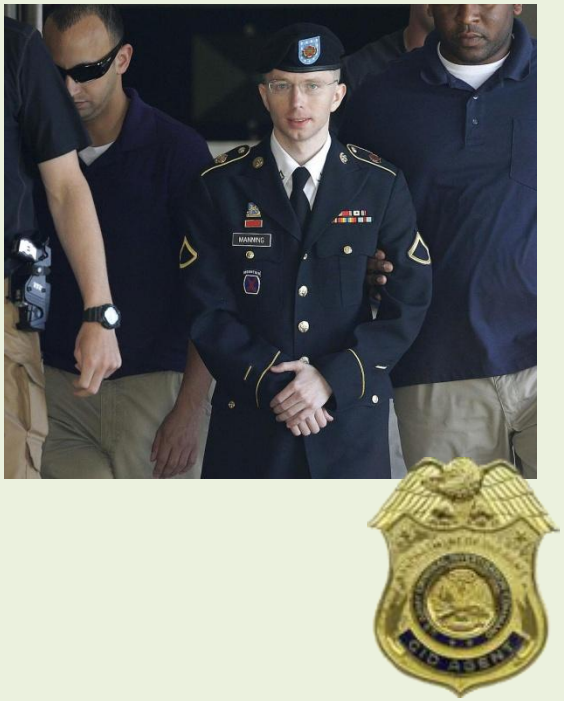
CASE(U.S NACY SEAL)

Terrorist(Bin Laden)



CASE(U.S CID)

Manning, Bradley



UNITED STATES OF AMERICA)
)
v.) STIPULATION OF EXPECTED TESTIMONY
)
Manning, Bradley E.) SA Charles Clapper
PFC, U.S. Army,)
HHC, U.S. Army Garrison,)
Joint Base Myer-Henderson Hall) DATED: 30 May 2013
Fort Myer, Virginia 22211)

It is hereby agreed by the Accused, Defense Counsel, and Trial Counsel, that if Special Agent (SA) Charles Clapper were present to testify during the merits and pre-sentencing phases of this court-martial, he would testify substantially as follows.

1. I am a Special Agent (SA) for the U.S. Army Criminal Investigation Division (CID). Specifically, I work for the CID, Computer Crimes Investigation Unit (CCIU). My current job title is Special Agent in Charge (SAC) of the Arizona Branch Office located at Fort Huachuca, Arizona. As the SAC, I run a two-man office that handles exclusively computer crimes. My job also entails serving as CID's liaison officer for NETCOM. Additionally, I am the liaison officer to the Regional Computer Emergency Response Team (RCERT-CONUS) and to the Theater Network Operations and Security Center (TNOSC). I have served in Arizona as an SA for five years and I have been the SAC for three of the five years.

2. From 1986-1999, I was an enlisted Military Police officer (MP). I served as an Evidence Custodian for the Investigation Section at Fort Lewis, Washington from 1993-1994. After becoming a CID agent in 1999, from 1999-2002, I served as the Computer Crimes Coordinator for the 5th MP Battalion in Kaiserslaughtern, Germany. I was also the Evidence Custodian for the Kaiserslaughtern CID Office from 2001-2002. I served as the Detachment Sergeant and as an Evidence Custodian from 2004-2006 at CCIU on Fort Belvoir, Virginia. In 2007, I was an INSCOM contractor performing forensics for the Army's Computer Emergency Response Team (Army CERT) in the Forensics and Malware Analysis department. I became a civilian Special Agent in Arizona in 2008, and currently serve in this capacity.

전자금융사고 사이버테러와 디지털포렌식

금융 소비자가 인터넷 등의 네트워크를 이용하여 비대면으로 금융업무를 처리하는 것을 의미

전자금융거래법 제2조(정의) "전자금융거래"라 함은 금융회사 또는 전자금융업자가 전자적 장치를 통하여 금융상품 및 서비스를 제공(이하 "전자금융업무"라 한다)하고, 이용자가 금융회사 또는 전자금융업자의 종사자와 직접 대면하거나 의사소통을 하지 아니하고 자동화된 방식으로 이를 이용하는 거래를 말한다.

전자금융거래 인프라가 원인불상 서비스의 본래목적을 저해하는 요인이 발생하면 사회기반 전반에 심각한 영향을 초래

1.경영 손실 비용 발생

카드 재발급 : 286억원

사고 수습 : 173억원

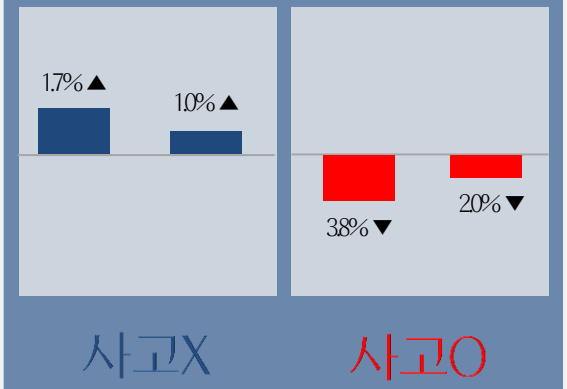
탈회 만회 : 1649억원

소송 패소시 : 1712억원

영업정지 : 172억원

카드 3사 고객정보유출 사건 기준

2.시장 점유율 하락



금융감독원 금융통계정보시스템(2014.5.23)

3. 신뢰 이미지 실추

"I'm Sorry"

More…

금융회사는 전자금융거래법, 전자금융감독규정 등을 중심으로 신용보호법, 정보통신망법, 개인정보보호법을 준수

기업에서 포렌식을 도입하는 이유				
침해사고 분석을 하려구요	정뷰유출 사고조사를 하려구요	내부 감사 목적으로요	외부 감사 사전대응요	다들 하던데요

정책 > 기술

사전대응	사후대응
Event에 대해 사전 대응을 통한 2차 피해 방지 및 확산 차단	진실 규명을 통한 제3의 피해를 최소화하고, 경영진 의사결정 지원

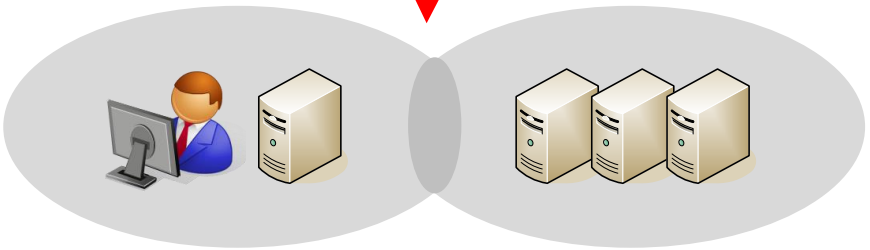
북한에 의한 사이버테러로 국내 언론사, 금융회사, 대북단체 등 전산장비가 파괴되는 등의 피해를 입은 해킹사고

Don’t Foget It

장시간 동안 사전에 준비된 공격 방법과 공격 루트를 통해 기업 내부의 전산망을 거점으로 확보하고 최종공격 감행

① 8개월~1년여간 준비된 공격

②기업 내부 거점 확보



③전산장비 파괴

"나 악성코드"
말 아님...

사이버戰은 국가적 차원에서 지원되고 있으며 미군의 경우 다양한 실전 사례를 바탕으로 전장의 핵심 요소로 부각시키고 있음

해외	구분	북한
IRAQ War(1991)	최초	이라크 전쟁時 사용된 미군의 사이버전 교리 획득, 자체 사이버전 훈련 교범
Cosobo War(1999)	전환기	코소보 사태에서 미군,유고군의 사이버 심리전, 홈페이지 해킹 모니터링
Stuxnet(2010)	정점	내부 폐쇄망에 대한 공격 침투 연구

3.20 사이버테러와 같은 공격 방법은 이미 북한 사이버전 전투 시나리오로 개발되어 연구/준비되고 있었음

과거의 흔적

...[중략]...일단 뚫린 서버들에서 중요한 정보들을 절취하여 프록시서버를 경우하여 빼어가며 흔적을 감추기 위하여 일단 공격을 멈추고 나서 사용된 서버들과 좀비PC의 시스템들을 ***모두 파괴***시키는 가장 강력한 공격시나리오를 실행하려고 한다. ...[이하생략]...

2011.3.28

2013.3.20

北사이버전 전투시나리오는 3개의 기능으로 동작되도록 개발되었고 이러한 공격에 따른 대응 모델 준비가 요구

1.독립적인 공격

7,7 대란에서 활용되었던 기법과 마찬가지로 명령/제어서버 없이 좀비 피시들에 심어놓은 공격코드 자체에 공격시간 동기화 처리부분이 있어 **명령/제어서버의 조종이 없이도 마스터피시의 조종**만으로도 목표 서버에로의 수십만대의 일제 공격이 가능하다.

2.위장/교란

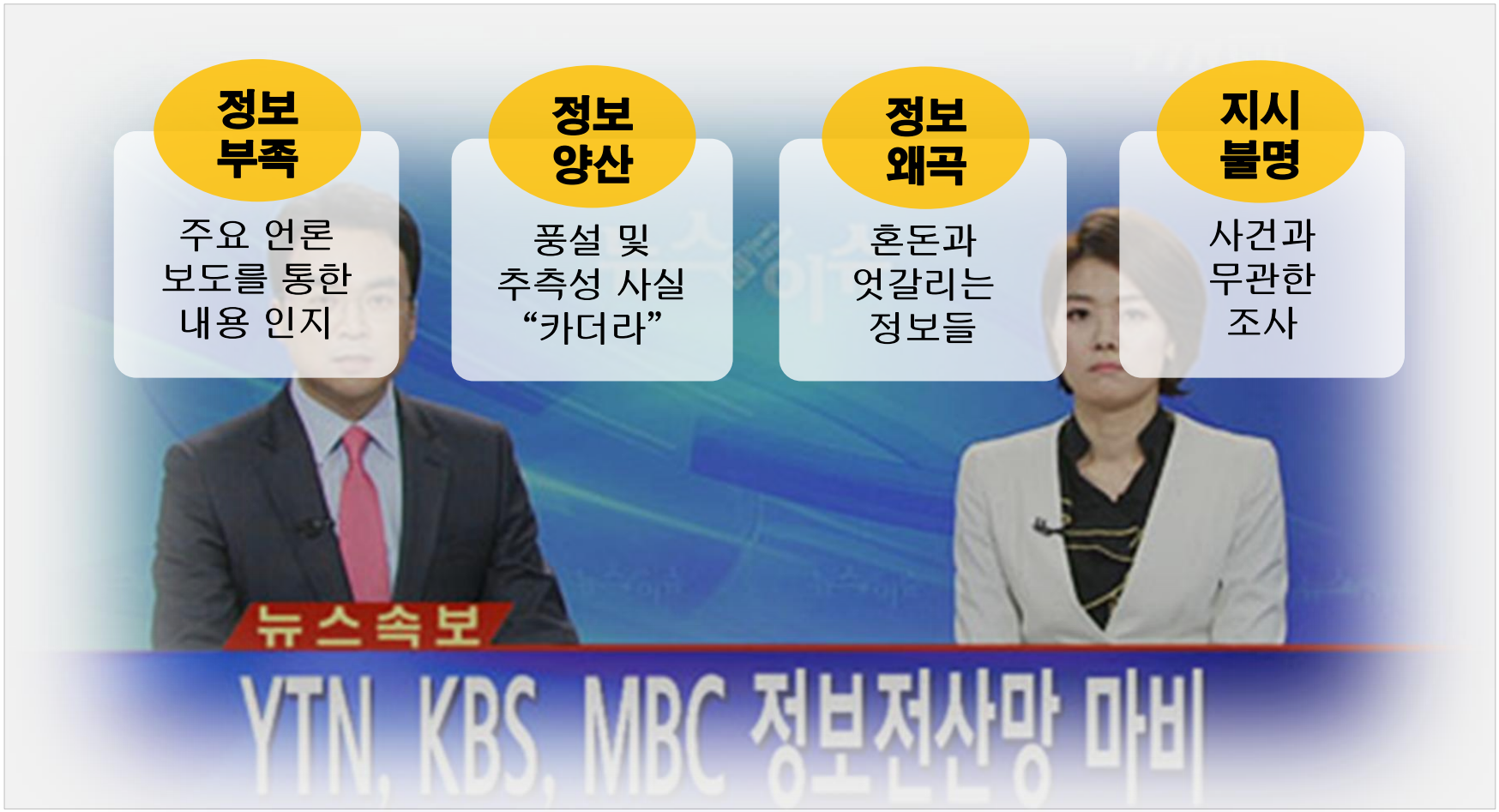
가상적인 명령/제어서버가 존재하는 것으로 위장시켜 **추적 시간을 지연** 시키며 추적자들을 교란

3.파괴

종전 능력관시성 공격으로부터 중요 정보의 절취, 파괴, 시스템의 과부하에 의한 **기능불량 등 가능한 파괴 기술을 활용**

Bigdata Forensic	Anti-Forensic	3rd Evidence Forensic

3.20 사이버테러 발생 직후 혼돈과 오보, SNS의 허위사실 등으로 인해 상황파악이 제대로 되지 않음

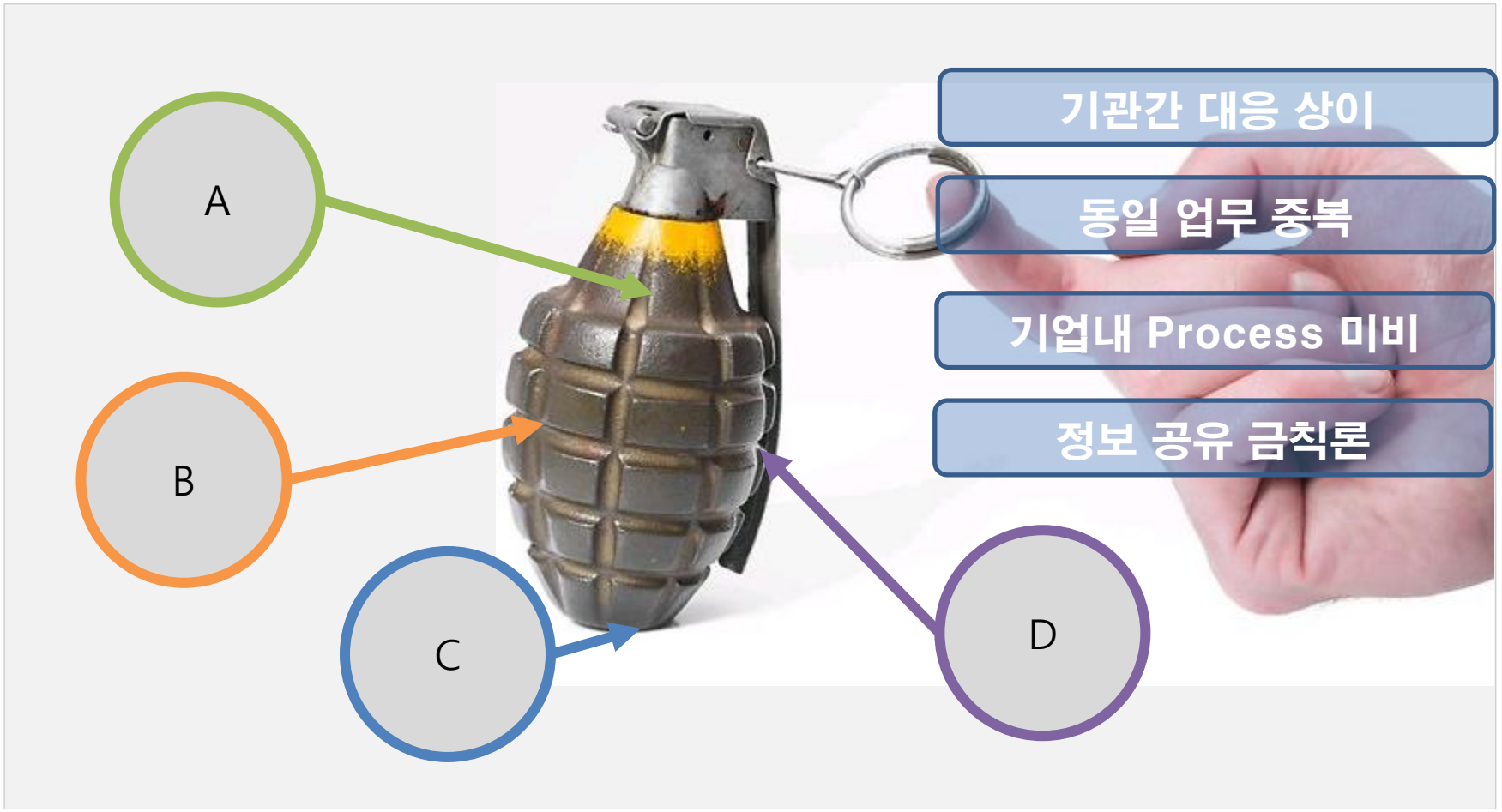


3.20 사이버테러

2013.3.20 13:00~14:00경부터 시작된 HDD 파괴 증상으로 피해 사실을 인지하게 되었으며, 2차 공격은 3.25일부터 발생

- 국내 거점 구축 (2012.6月 ~)
- 기업망 내부 악성코드 감염 (2012.8~12月경)
- 기업망 내부 PC, 서버 해킹
- 전산장비 파괴 (2013.3.20. 13:00~)
- 무차별 악성코드 유포 (2013.3.25~) / 날씨닷컴 등
- 대북.보수단체 서버 파괴 (2013.3.26~)
- 추가 공격(?)

- [결론] 3.20 사이버테러를 통해 본 실체적 진실 규명이란...



Forensic Investigation
vs
Forensic Examination

법집행기관과 민간 기업 MISSION에 따라 상이

- 사법경찰관(리)로써의 법적 권한
- 수사학 및 법률지식
- 전문교육 이수
- 다양한 케이스
- 주기적인 반복 숙달 훈련
- 기술 지원 조직

- 감사 또는 보안 부서
- 수사학 및 법률지식 없음
- 단기교육 이수(벤더, 무료, 학원)
- 케이스別 이해도 낮음
- 훈련 보다는 겸직된 업무에 충실
- Self Study

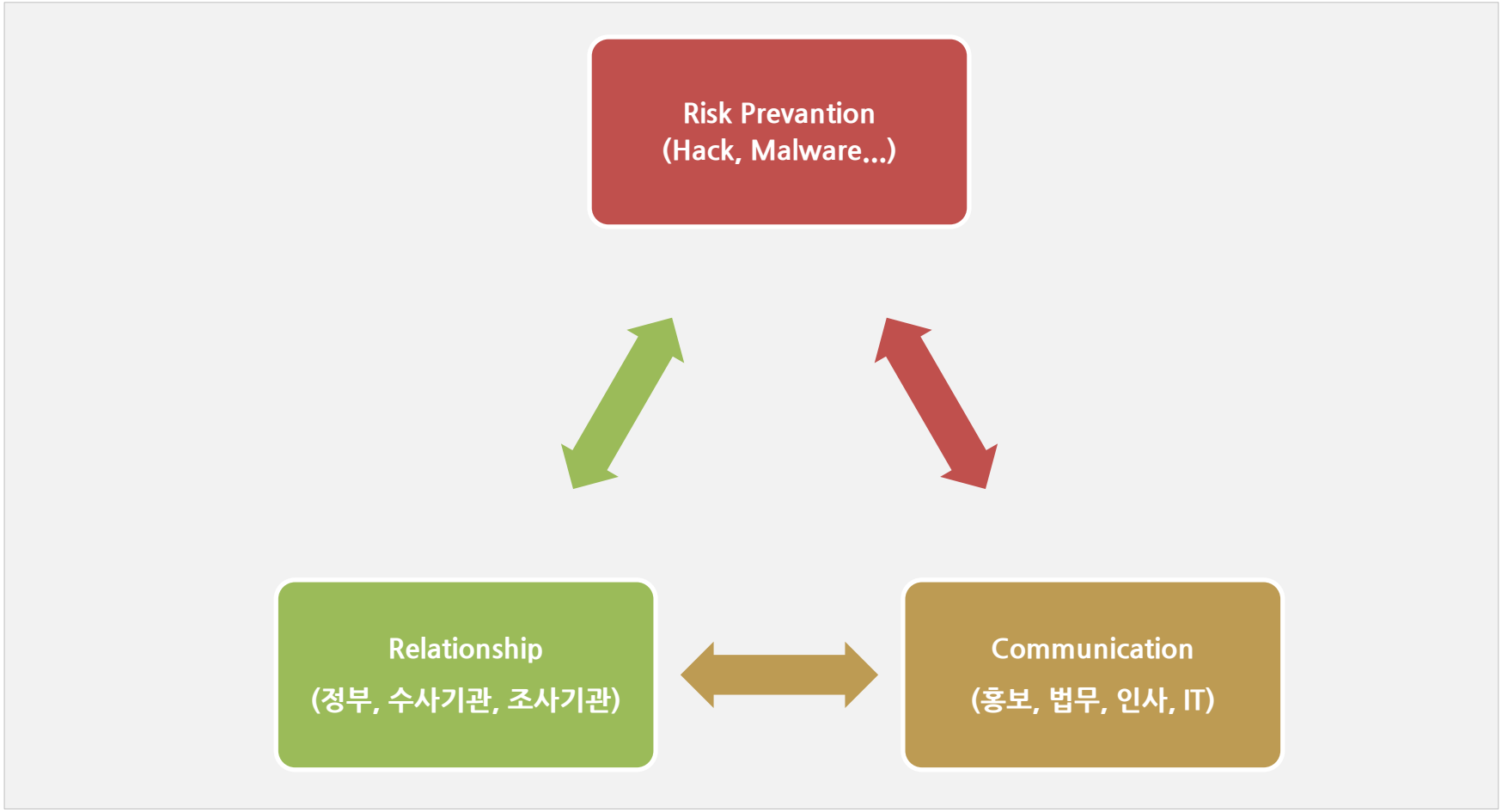
Law Enforcemet	구분	Corporate
기소, 단서수집	목적	가용성, 사고조사
법정 증거	고려사항	가용성
사고이후	환경	Realtime
강제수사, 임의제출	수집	자사자산

Forensic Investigation vs Forensic Examination

디지털포렌식은 2개의 영역(Physical + Digital)에서 얻어진 단서(Evidence)를 조합하여 사건/사고의 실체적 진실을 규명

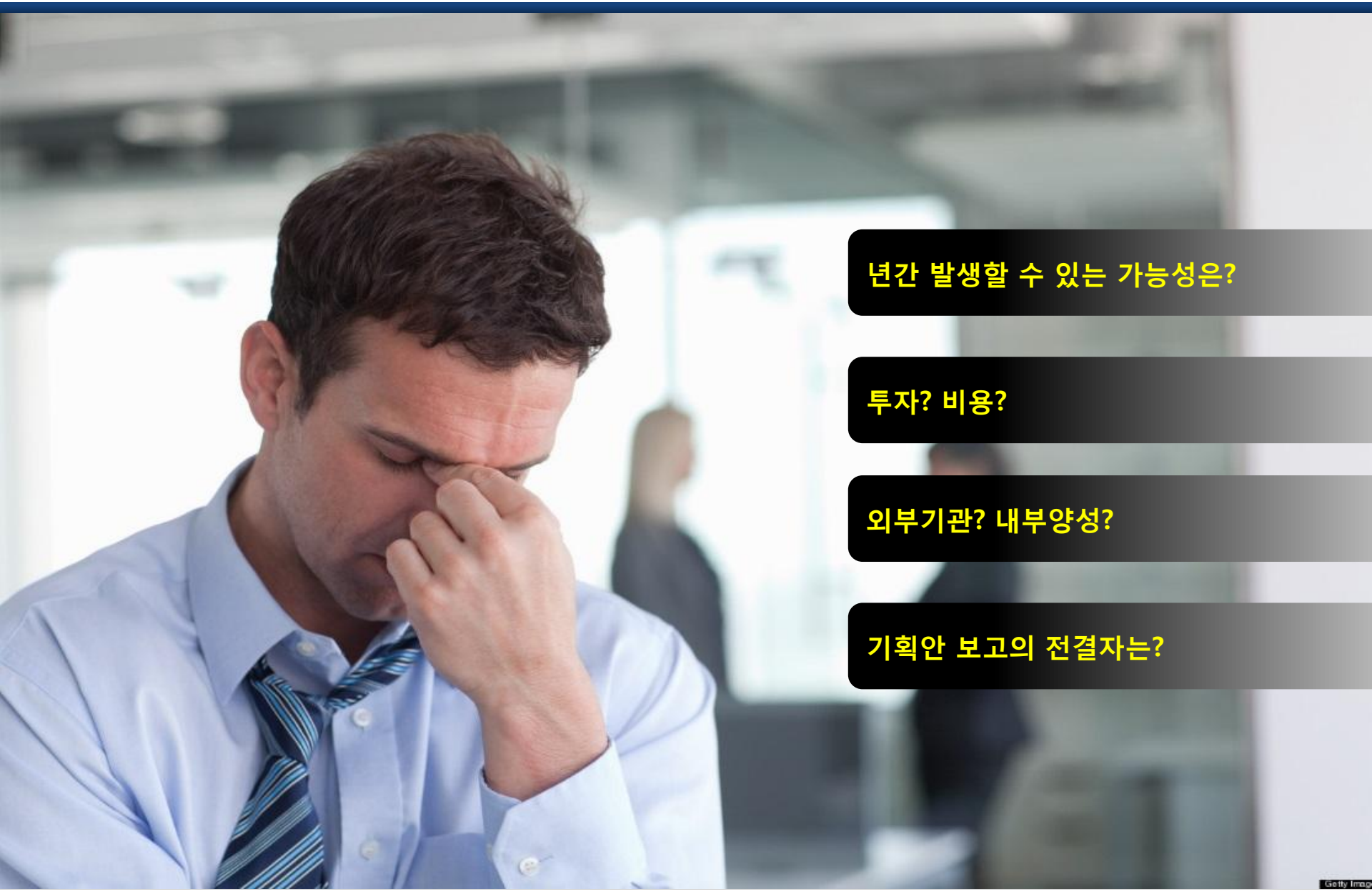
Forensic Investigation vs Forensic Examination

Forensic Investigation vs Forensic Examination



Forensic Investigation vs Forensic Examination

Forensic Investigation vs Forensic Examination



기업의 디지털포렌식이란?

왜?
디지털포렌식이
필요한가?

+

담당부서의
준비사항은?

+

담당자의
고려사항은?

디지털포렌식은
잠재적 Risk를 가시화하여
건전한 경영활동 보장

Question and Answer