법과 과학

2019년 3월호

과학수사의 중심

대검찰청 과학수사부

CONTENTS

속기 업무 매뉴얼 제작·배포

법과학분석과 속기사 손자현

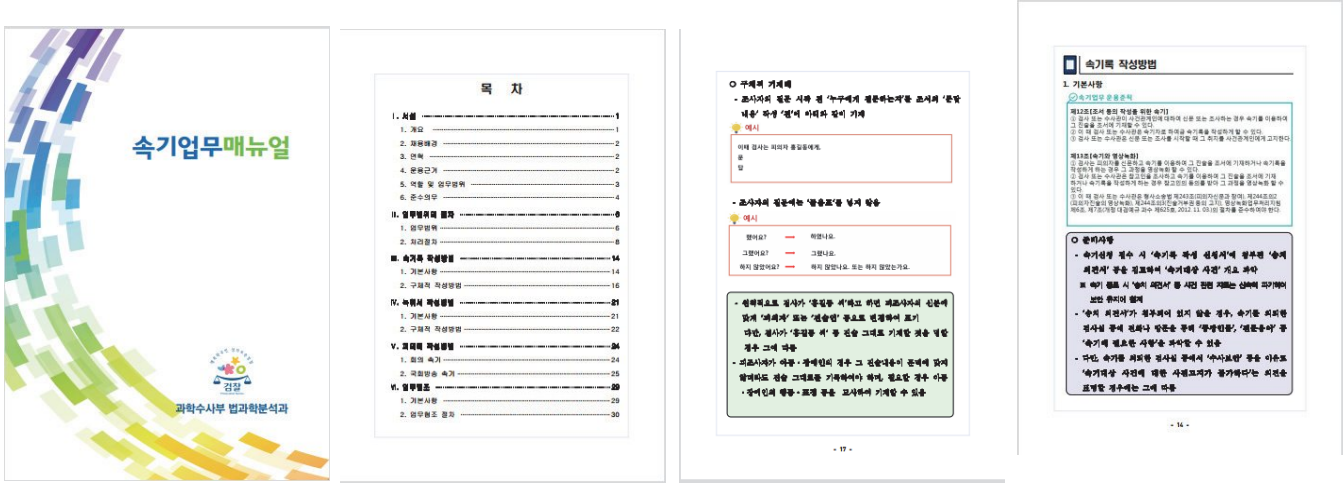
“신규속기사도 이 매뉴얼 하나면...”

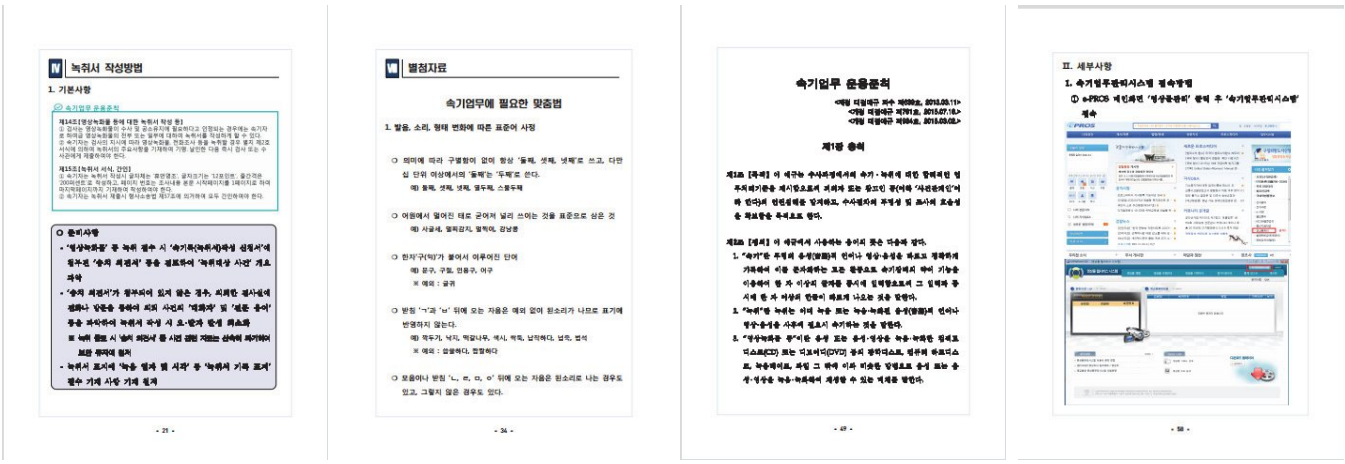
검찰에 속기사를 도입한지 10년, 28명의 시작으로 현재 전국 청에는 106명의 속기사가 수사업무 지원에 힘쓰고 있습니다. 그간 속기업무 절차 및 범위와 속기록·녹취서의 구체적 작성방법 등에 대한 가이드가 없어서 교육에도 한계가 있었고, 올해 24명의 신규 속기사를 증원하면서 명확한 가이드가 필요한 시점이었습니다.

이에 법과학분석과 영상녹화팀은 신규속기사도 빠르게 습득하여 업무에 적용할 수 있는 실무매뉴얼을 제작하게 되었습니다.

2018년 11월에 개최되었던 전국 속기사 워크숍에서 일선청 속기사의 업무처리 실태 등 현장의 목소리를 들으며 그를 바탕으로 자료를 수집하였습니다.

1월에 속기업무매뉴얼 초안이 완성되어 일선 의견조회를 실시하였고, 이를 바탕으로 수정에 들어갔습니다. 2월 말, 드디어 속기업무매뉴얼이 완성되어 3월 배포를 하게 되었습니다.





주요 내용을 소개하자면, 검찰 속기사 제도의 연혁과 운용근거를 설명하였고, 속기업무 준칙에 정해진 속기업무의 범위와 절차를 정리하고, 준수의무도 함께 넣어 기본적으로 꼭 알고 있어야 하는 업무의 범위 및 의무를 이해하기 쉽게 정리하였습니다.

그 다음으로는 업무 절차에 대한 설명을 하였습니다. 업무처리 흐름도를 넣어 속기 신청부터 제출까지 보기 쉽게 절차를 확인할 수 있습니다.

매뉴얼의 꽃인 속기록·녹취서의 구체적 작성방법에는 적절한 예시를 통해 검찰 속기업무를 처음 하는 신규속기사도 이해할 수 있도록 하였습니다. 그밖에 회의 속기 방법 설명과 속기사 여러 명이 협동하여 하는 실시간 속기 등에 대한 방법도 기재하여 업무에 큰 도움이 될 것으로 예상됩니다.

별첨자료에는 업무에 필요한 맞춤법과 양식을 넣어서 매뉴얼 하나면 완벽하게 속기업무를 할 수 있도록 노력하였습니다.

매뉴얼을 통해 속기업무에 대한 시행착오를 줄여 나가며, 속기업무가 보다 활성화 되고 조직 내부에서 수사지원의 한 축으로 발전하였으면 좋겠습니다.

속기업무매뉴얼을 위해 힘써주신 분들 감사합니다.

우즈베키스탄 디지털포렌식팀 설립 관련 국외출장

디지털수사과 수사관 박연재

디지털 증거 분석 이제는 필수인 시대!

대검찰청 디지털수사과 디지털포렌식연구소에서는 국제협력단(KOICA)과 함께 <CIS 과학수사 역량강화 사후관리 현장사업:우즈베키스탄 과학수사센터 디지털포렌식 역량강화 사업>을 2018. 10.부터 2019. 2.까지 성공리에 수행하였습니다.

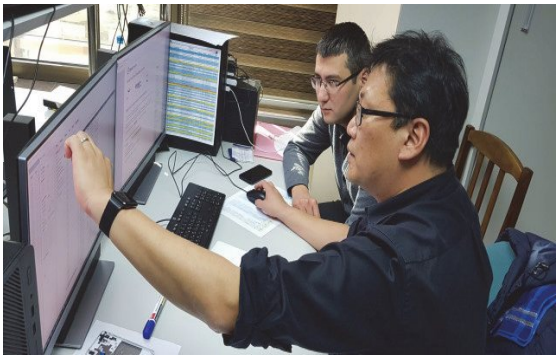
우즈베키스탄하면 떠오르는 단어가 어떤 것이 있으신가요? 혹자는 미녀들의 나라라고 부르기도 하고, 다른 누군가는 실크로드의 중심지 또 다른 누군가는 구소련이 붕괴되면서 생겨난지 얼마되지 않은 아직은 개발이 매우 필요한 나라라고 생각하기도 합니다. 이처럼 다양한 의미로 와닿는 우즈베키스탄에 디지털포렌식센터(MFC, Main Forensics Center)가 개소되었고, 중앙아시아 최초의 디지털수사 분야 전문가를 배출한 기쁜 소식을 전해드리고자 이렇게 지문으로 인사를 드립니다. 디지털수사과에서 우즈베키스탄 현장지원 사업경과는 아래의 표와 같습니다.

- 아 래 -

기간	사업 내용
2016. ~ 2018.	CIS과학수사 역량강화 초청연수
2018. 6.	우즈베키스탄 현지컨설팅
2018. 7.	한국국제협력단 사후관리 현장사업 선정 공모
2018. 9.	대검찰청 디지털수사과 현장사업 기관 선정
2018. 10.	우즈베키스탄 현장사업 관련 사전조사 및 현지컨설팅
2018. 11.	1차 모바일포렌식 기술교육
2019. 2.	2차 모바일 포렌식 기술교육 및 성과보고회 개최

특히 이번 사업은 2018. 10.부터 2019. 2.까지 우즈베키스탄이 디지털수사를 함에 있어서 이론교육과 더불어 실무교육을 진행하여 디지털포렌식 분석 기법 역량 강화 요청, 우즈베키스탄의 형사소송법 개정 및 디지털포렌식 증거물에 관한 규정 제정에 대한 법정비 지원 요청, 모바일 포렌식과 관련한 기자재 전달이 금번 사후관리 사업에 주를 이루었습니다. 우즈베키스탄 사후관리 사업 1차 출장기간(18.10.28. ~ 11.3.)에는 우즈베키스탄 현지 기자재, 도서, 형사소송법, 예규 등에 대한 내무부 사전 조사와 우즈베키스탄 현지 사용 폰에 대한 통계자료, 앱 사용 현황 등 디지털포렌식 환경 조성을 위한 외부인자에 대한 조사를 실시하였습니다. 기본적인 기자재와 도서 등이 구비되어 있지 못하고, 법률적으로 디지털포렌식에 대한 내용이 전무하였으며, 스마트폰에 대한 시장점유율은 삼성, 화웨이, 샤오미, 아이폰, 엘지 순으로 그리고 앱에 대한 점유율은 텔레그램, IMO, 페이스북 메신저, 왓츠앱, VKONTACT 등 한국과 유사하지만 특이한 앱에 대한 점유율이 높았습니다. 또한 범죄 유형별로는 강력사건, 경제범죄, 마약사건 등 스마트폰을 도구로 행해지는 범죄가 증가하는 추세라는 것을 확인하였습니다.

2차 출장기간(2018. 11. 25. ~ 12. 8.) 1차 실무교육에는 형사소송법상 감정서를 작성할 수 있는 전문가 양성(국제 인증 자격증 취득), 디지털 증거 수집 절차 교육 및 매뉴얼 작성, 모바일 포렌식 획득 분석 중 삼성, 엘지, 아이폰에 대한 집중 교육을 진행하였으며, 분석은 텔레그램 위주로 진행하였습니다.



이러한 교육의 성과로 2명의 국제 인증 자격증 취득(중앙 아시아 최초), 실제 사건(살인사건) 증거물 분석으로 살해동기 확인하여 기소할 수 있는 증거 분석, 디지털 포렌식 관련 기자재 전달(모바일 획득도구, 분석 노트북, 차폐봉투, 도서, 모바일 분해도구, 모바일 충전도구 등), 디지털 포렌식 증거 수집 절차 매뉴얼 초안 작성이라는 쾌거를 이루었습니다.

3차 출장기간(2019. 2. 17.~ 2. 23.) 2차 실무교육에는 모바일 포렌식 획득 분석 중 화웨이, 샤오미에 대한 집중 교육을 진행하였으며, 특히 교육 마지막 날인 2. 20.에는 대검찰청 과학수사부장님이 직접 교육생에게 수료증과 국제공인 자격증 수여식을 진행 하였으며, 2. 21.에는 성과보고회를 개최하였습니다. 성과보고회는 당초 예상 했던 인원 70여 명을 훨씬 웃도는 110여 명이 참석을 했으며, 권용우 주 우즈베키스탄 한국대사, 손성일 코이카 우즈베키스탄소장, 조남관 과학수사부장, 박현준 디지털수사과장 뿐만 아니라 타지예프 대검찰청 차장검사, 예브가니 우즈베키스탄 검찰아카데미 원장, 나일 과학수사센터장을 비롯한 루스탐 검찰 아카데미 부원장, 이남야노프 타슈켄트 검찰청 차장검사, 마디예프 타슈켄트 중요 경제범죄부장 뿐만아니라 국가투자위원회, 기무사, 국방부 등 여러 공직자들이 다수 참여하여 디지털포렌식의 중요성과 확산 가능성에 대해 긍정적인 평가를 가질 수 있었습니다. 행사가 종료된 후 우즈베키스탄 내무부 과학수사센터장이 디지털포렌식 연구소 이인수 소장, 서도정 수사관, 박연재 수사관에게 감사패를 증정하였으며, 성과보고회는 UZ Report, MY5, 내무부 홍보실 등에서 언론보도 자료를 냈으며, 과학수사부장님의 개별 인터뷰도 진행이 되었습니다.

이러한 열기가 채 가시기도 전에 타슈켄트 검찰청에서 세미나 발표자료에 대한 강의 요청이 들어와서 다시한번 타슈켄트 검찰청에서 강의를 진행하였으며, 50여명의 현직검사를 대상으로 실무 교육까지 완료하였습니다. 이렇게 숨가빴던 우즈베키스탄 과학수사센터 디지털포렌식 역량강화 사업을 완료하였습니다.

우즈베키스탄의 관광도시 중 사마르칸트에 아프라시압 궁전지 벽화의 사절단에 고구려인이 있었다는 사실로 미루어볼 때 우즈베키스탄은 어느 날 갑자기 알게 된 나라라기보다 오랜기간 우리와 함께 교류하고 있었던 나라였습니다. 이러한 우즈베키스탄과 향후에 디지털포렌식의 발전과 기술교류 등을 통해 양국간의 우호증진, 사법공조 등 보다 넓은 미래를 향해 함께 나아가길 기대해봅니다.

Postda

2019-yil 2

ХАЛҚАРО ҲАМКОРЛИК

РАҚАМЛИ ЭКСПЕРТИЗА — ЗАМОН ТАЛАБИ

Жорий йилнинг 17–22 февраль кунлари Корея Республикаси Бош прокурори ўринбосари, Эксперт-криминалистика департаменти бошлиғи, бош айбловчи Чо Нам Кван бошчилигидаги делегация Ўзбекистон Республикасида бўлди.

Ташрифдан кўзланган мақсад рақамли экспертиза, хусусан, мобил қурилмалардаги маълумотларни тиклаш ва таҳлил қилиш жараёнларини батафсил ўргатиш мақсадида иккинчи техник семинарни ўтказиш эди. Илк семинар ўтган йилнинг 25 ноябридан 7 декабригача Ўзбекистон Республикаси ИИВ ЭКБМ негизида бўлганди.

Таъкидлаш жоизки, рақамли экспертиза жиноятларни тергов қилишда муҳим ўрин тутади. Бу криминалистик имкониятларнинг ўсиши, компьютер қувватининг ортиши ҳамда маълумотларни сақлаш технологияларининг узлуксиз ривожланиши билан изоҳланади.

Қурилмалардан, яъни компьютер, смартфон, планшет, серверлар, шунингдек, турли маълумотлар-ни сақловчи ва ташувчи воситалар (каттиқ диск, компакт-диск, флэш-тўплагич)дан маълумот йиғиш анчагина қулайлик туғдирмоқда.

Рақамлаштиришга ўтиш рақамли маълумотларни самарали таҳлил қилиш учун электрон тергов воситаларидан янада кенг фойдаланишга хизмат қилади. Мазкур йўналиш яқинда ташкил этилганига қарамай, уни ўзлаштириш борасида кореялик ҳамкасблар кўмагида катта ютуқлар қўлга киритилди. Хусусан, рақамли экспертиза ўтказиш бўйича замонавий, синовдан ўтган методикани таҳлилий салоҳиятни мустаҳкамлаш этишди, шунингдек, экспертларимиз ўзлаштирган билим ва кўникмалар текширилди.

Ташрифнинг тўртинчи куни Ўзбекистон Республикаси Ички ишлар вазири ўринбосари, полковник Р. Эргашев делегация раҳбари Чо Нам Кван билан учрашди. Унда Ўзбекистон Республикаси ИИВ ЭКБМда рақамли экспертизани янада ривожлантириш истиқболлари муҳокама этилди. Жумладан, Корея Республикаси Бош прокуратураси мутахассислари тергов ва суд жараёнида тўпланган ашёвий далилларнинг

ҳамда зарурий жиҳозлар ва дастурий таъминотлар рўйхатини тақдим этишда кўмаклашишмоқда.

ИИВ ЭКБМ ва Корея Республикаси Бош прокуратураси ўртасидаги расмий келишувга мувофиқ, делегация аъзолари, яъни бош айбловчи Чо Нам Кван, рақамли тергов бўлими директори Пак Жен Жун, рақамли тергов тадқиқот институти директори Ли Ин Су, рақамли тергов терговчилари Со До Чжонг, Пак Ен Жэ, Сон Жи Ан вазирлик ходимларининг мобил қурилмалар экспертизаси соҳасидаги малакасини ошириш мақсадида бир қатор тренинглар ўтказишди.

Семинарлар доирасида «Xiaomi» русумли мобил қурилмаларидаги маълумотлар, таҳлили ва рақамли далилларни олишни ўргатиш бўйича тренинглар ташкил этилди. Ўқув жараёнида иштирокчилар бирничи техник ўқув натижалари бўйича рақамли кўринишлари билан ишлаш шунингдек, далилларнинг мазкур кўриниши юзасидан ўтказилган тадқиқот бўйича хулоса бериш учун экспертиза тадқиқотлари ўтказишда улардан келгусида суд жараёнида фойдаланишнинг қонуний жиҳатларига тўхталиб ўтишди.

Тажриба алмашиш ва мутахассисларни ўқитиш зарурати алоҳида қайд этилди. Полковник Р. Эргашев ушбу йўналишда яқиндан ҳамкорлик қилиш ва муносабатларни янада ривожлантиришга умид билдирди.

Учрашув сўнгида ҳамкорликни жадал давом эттириш, янада ривожлантириш борасида келишиб олинди.

Ташриф якунида делегация аъзолари учун Тошкент шаҳрининг диққатга сазовор жойларига саёҳат уюштирилди.

Азиза БАҲОДИРОВА, лейтенант.
Содиқ ҲАКИМОВ олган суратлар.

СЕМИНАР-ТРЕНИНГ

<우즈베키스탄 현지 언론 보도 사진>

『알아두면 좋은 과학수사 상식』 ①

사이버수사 용어 요모조모

대검찰청 검찰연구관 김영미

사이버 범죄란 사이버 공간을 이용한 전통적인 범죄와 사이버 공간 등장으로 새롭게 발생한 범죄를 생각할 수 있습니다. 2001년 출범한 최초의 사이버 범죄 국제협약인 유럽평의회 사이버범죄협약은 사이버범죄 유형을 ① 시스템의 기밀성, 무결성, 유용성에 대한 범죄, ② 컴퓨터 관련 범죄, ③ 콘텐츠 관련 범죄, ④ 저작권 침해 범죄로 구별하고 있습니다.

사이버 범죄에서는 다양한 용어가 나와 약간 어리둥절해질 수 있는데요. 이번 달에는 이러한 용어들을 정리해 보겠습니다.

IP(Internet Protocol)란 인터넷에 연결된 컴퓨터에 부여된 고유식별 값을 말합니다. 이러한 고유식별 값은 숫자로만 구성되어 있어 사람이 쉽게 기억하고 입력할 수 있도록 만들어진 주소 체계를 도메인(domain)이라고 합니다.

또한 인터넷 도박 사건 등등에서 종종 활용할 수 있는 MAC 주소가 있습니다. MAC은 'Media Access Control'로서, 컴퓨터 네트워크 카드에 부여된 고유식별 값입니다. IP와

MAC은 인터넷 사용자를 추적할 때 사용하는 방법으로 알려져 있습니다.

패킷은 정보기술에서 패킷 방식의 네트워크가 전달하는 데이터의 형식화된 블록입니다. 패킷을 지원하지 않는 통신 연결은 단순히 바이트, 문자열, 비트를 독립적으로 연속하여 데이터를 전송할 뿐입니다. 데이터가 패킷으로 형식이 바뀌면 네트워크는 장문의 메시지를 더 효과적이고 신뢰성 있게 보낼 수 있습니다. 우리가 컴퓨터에 정보를 입력하면 대부분 패킷에 담겨서 IDC(인터넷데이터센터)에 도달하게 됩니다. 그래서 IDC에 도달하게 된 패킷 과정을 따라 IP나 MAC을 확인하여 정보 입력자를 확인하게 되는 것입니다.

그런데 이렇게 IP를 추적하기 어렵게 소위 IP 세탁을 하게 되는 경우가 있습니다. VPN(Virtual Private Network, 가상 사설망)은 당초는 기업의 비용 절감과 보안 목적으로

사용되던 가상 네트워크인데 VPN을 거치면 IP 주소가 변경되어 추적이 어려워집니다. 프록시(Proxy) 서버도 마찬가지 역할을 하고 있습니다.

흔히 사이버 공격으로 APT(Advanced Persistent Threat)를 이야기하는데요. 해커가 다양한 취약점을 이용하여 특정 기업이나 조직의 네트워크에 지속적으로 가하는 공격을 말하며, 지능형 지속 공격이라고 합니다.

악성코드란 사용자가 원하지 않는 일을 몰래 하는 코드(소프트웨어)로 해외에서는 'Malicious(악의적인)'와 'Software(소프웨어)'의 합성어로 'Malware'라고 부릅니다. 악성코드 관련 국내 법률의 대표적인 예는 정보통신망 이용촉진 및 정보보호 등에 관한 법률을 들 수 있습니다. 악성코드는 기밀자료나 정보를 유출하거나, 협박이나 금전 요구형(이른바

랜섬웨어 Ransomware), 개인 금융정보 탈취형(파밍(Pharming) 악성코드) 등 다양합니다. 최근 악성코드는 이메일, 웹사이트 방문, 업데이트 서버 해킹, 설치프로그램 변조 등을 통해 유포되고 있습니다. 여기서 백도어(Backdoor)라고 하는 말이 등장하는데, 허가받지 않은 사용자가 정상적인 인증과정을 거치지 않고도 컴퓨터 시스템에 접속할 수 있도록 만들어 놓은 뒷문, 즉 보안우회접속지점을 말합니다. 본래는 시스템 관리자나 설계자에 의해 외부에서도 시스템을 원격으로 점검할 수 있도록 고의로 백도어를 만들어 두었는데, 점차 해커가 시스템 침입에 성공 후 다음에 쉽게 접속할 수 있도록 만들어 놓는 보안 우회 접속지점으로 사용되었습니다.

스피어피싱(Spear Phishing)은 불특정 다수를 대상으로 하는 피싱과 달리 특정기관의 내부 직원을 표적으로 삼아 계정정보를 탈취하거나 악성코드를 감염시키기 위한 피싱 시도를 말합니다.

그렇다면 흔히들 말하는 피싱(Phishing)과 파밍(Pharming)의 차이점은 무엇일까요.

피싱은 수사기관, 금융기관 등에서 보낸 이메일, SMS로 위장하여 사용자로 하여금 가짜 사이트에 접속하도록 유도한 뒤 개인정보, 금융정보를 탈취하는 방식임에 반하여, 파밍은 악성코드로 사용자의 컴퓨터를 감염시켜 도메인 서버 주소를 변경함으로써 사용자가 정상적인 사이트 주소를 입력하더라도 가짜 사이트로 자동 접속되도록 유도하는 수법입니다.

스미싱(Smishing)은 문자메시지와 피싱의 합성어로 인터넷 접속이 가능한 스마트폰의 문자메시지를 이용한 피싱 수법입니다.

쿠키(Cookie)는 인터넷 사용자가 웹 사이트를 방문할 때 사용자의 컴퓨터에 자동으로 설치되는 작은 임시 파일입니다. 웹 사이트는 쿠키를 사용하여 방문자에 대한 정보를 저장하고, 쿠키를 이용하여 사용자에게 편리한 웹 서핑 환경을 제공해 줍니다. 레지스트리(Registry)란 시스템 하드웨어, 설치된 프로그램 및 설정, 컴퓨터에 있는 각 사용자 계정의 프로필 등에 대한 중요한 정보가 저장되는, 윈도우를 운영하는데 필수적인 데이터베이스 역할을 하고 있습니다. 아티팩트(artifact)란 시스템이 운영되면서 사용자 또는 운영체제에 의해 남게 되는 모든 흔적을 의미합니다.

로그 추적때 UTC라는 단어를 보게 되는데요. UTC(Universial Time Coordinated)는 국제 사회가 사용하는 과학적 시간의 표준을 말합니다. UTC는 전 세계를 25개 시간 구역

으로 나누어 표시하고, 한국은 UTC+9, 즉 기준시보다 9시간이 더 빠르다고 보면 됩니다.

마지막으로 토르, 딥웹에 대해서 이야기해 보려 합니다. 토르(TOR)는 파이어폭스(firefox) 기반의 브라우저로 'The Onion Routing'의 약자입니다. 본래는 미국 해군 연구소의 '3G 어니언 라우팅 프로젝트'라는 이름으로 시작되었고, 주요 목적은 정부의 온라인 통신 내용을 보호하기 위함이었습니다. 토르 네트워크는 수천 개의 어니언 라우터(중계서버)로 구성되고, 각각의 중계서버는 패킷이 어디서 출발했는지, 최종 목적지가 어딘지 알 수 없고, 패킷은 여러 겹으로 암호화 되어 전송되는데 각 중계서버를 통과할 때마다 한 꺼풀씩 복호화되어 다음 중계서버로 이동합니다. 이러한 토르 네트워크는 적게는 몇 개부터 수백, 수천 개의 중계 서버로 구성되고, 패킷의 이동 경로에 관한 정보는 주기적으로 삭제되고 각 중계서버를 지나면서 IP가 변경되는 등 전체 통신을 추적하거나 분석할 수 없도록 구성되어 추적이 쉽지 않습니다.

딥웹(deep web)은 외부에 노출되지 않도록 만들어진 네트워크로 다중 프록시 우회 등 익명성이 보장된 토르 브라우저를 통해서만 접속할 수 있도록 인터넷 주소 암호화 기술이 적용된 네트워크입니다. 일반 검색엔진으로는 딥웹 사이트를 찾을 수 없습니다.

이 외에도 많은 생소한 용어가 있는데요. 다음 기회에 더 설명해 드리겠습니다.

『알아두면 좋은 과학수사 상식』 ①

미국, 이렇게나 많은 기관이...

법과학연구소장 이승환

나라마다 과학수사를 책임지고 있는 법과학기관들의 규모, 형태 등은 매우 다양하여 좋은 모델을 찾아 벤치마킹하는 것은 국내의 법과학을 발전시킬 수 있는 소중한 자료일 것입니다. 여러분들이 이미 많이 알고 계실 것으로 생각합니다만 흩어져 있던 정보를 한 데 모으는 취지에서 세계의 법과학기관에 대해 소개하는 글을 연재하고자 하며 이번 호에는 미국부터 시작하고자 합니다.

미국하면 떠오르는 법과학기관은 미연방수사국(FBI) Laboratory Division 정도이겠지만 이번 호는 법과학기관 전체의 현황을 살펴볼까 합니다. 여러분은 얼마나 많은 법과학기관이 미국에 존재한다고 생각하십니까? 2014년 기준으로 무려 409개의 공공 법과학기관이 있으며 이 통계는 민간기업은 제외된 것이니 실제는 훨씬 더 많은 법과학서비스기관이 있다고 할 것입니다.

TABLE 9
Annual operating budget for publicly funded forensic crime labs, by type of jurisdiction and number of full-time employees, 2014

	Number of labs	Annual operating budget (in millions)
All labs	409	$1,680
Type of jurisdiction		
Federal	39	$302
State	193	796
County	98	306
Municipal	79	277
Number of full-time employees*		
100 or more	27	$568
50–99	51	416
25–49	90	378
10–24	134	262
9 or fewer	107	56

Source: Bureau of Justice Statistics, Census of Publicly Funded Forensic Crime Laboratories, 2014.

연방기관이 존재하는가 하면 주(洲) 정부가 관할하는 기관도 있고 더 작은 단위인 카운티 혹은 더 작게 시(市)에 속한 기관들도 존재합니다. 그 규모도 천차만별이어서 100명이상의 대규모 기관은 27개로 전체의 7%정 도이며 50명 이상인 기관수를 합쳐도 20%정도에 머무릅니다. 나머지 80%는 중소규모의 인원을 가진 기관이며 인원이 10명이 안되는 기관이 전체의 1/4정도를 차지하고 있습니다. 주의깊게 살펴볼 점은 연방기관만 해도 39개에 달하며 50개 주로 이루어진 미국에서 주단위 기관이 무려 193개에 이른다는 점입니다. 이러한 점은 미국에서는 법과학 기능을 가진 정부 부처가 매우 많다는 것을 의미합니다. 예를 들어 한 주내에서도 경찰과 법무부가 서로 다른 법과학기관을 가지고 있고 이와는 별개로 법의검시관 사무소도 독립적인 법과학 서비스를 하는 식입니다. 우리나라에서는 법과학 예산이나 인원 논의 시 법과학기관의 중복 문제가 늘 거론되지만 미국의 예만 보더라도 이것은 타당하지 않은 논리라는 것을 쉽게 알 수 있습니다. 법과

학기관의 연 예산을 모두 합치면 약 17억불(약 1조 7천억원) 정도 된다고 합니다. 100명 이상의 인원을 가진 기관이 평균 연 210억원, 50명이상 기관이 연 80억원 정도, 그 이하 기관들이 연 40억원 정도의 예산으로 법과학서비스를 운영하고 있습니다. 미국의 GDP가 우리나라의 약 13배에 해당하는 것으로 알려져 있는데 이를 감안한다 해도 우리나라의 전체 법과학 예산보다는 훨씬 규모가 큰 것으로 짐작됩니다.

409개의 기관에서 모든 분야의 법과학을 다루고 있지는 않습니다.

TABLE 2
Functions performed by publicly funded forensic crime labs, by type of jurisdiction, 2014

Forensic function	Federal	State	County	Municipal
Controlled substances	55%	87%	86%	71%
Crime scene	42	48	51	75
Digital evidence	54	10	20	36
Firearms/toolmarks	27	58	60	58
Forensic biology casework	27	71	68	42
Forensic biology from convicted offender/arrestee samples	12	25	9	4
Impressions	26	43	46	35
Latent prints	67	53	62	88
Questioned documents	34	12	12	14
Toxicology	9	48	52	36
Trace evidence	57	53	50	29
Number of labs	39	193	98	79

Note: See appendix table 2 for standard errors.
Source: Bureau of Justice Statistics, Census of Publicly Funded Forensic Crime Laboratories, 2014.

일반적으로 나타나는 특징은 단위가 작은 기관일수록 수사에 직접 필요한 법과학분를 많이 다루는 것을 볼 수 있습니다. 전체적으로 마약, 규제물질류 등의 분석을 담당하는 분야를 가장 많이 포함하고 있습니다. 최근에 중요도가 매우 높아진 디지털증거분야는 제일 작은 단위에서도 상대적으로 많이 다루고 있지만 연방 단위의 기관에서 가장 많이 맡고 있습니다. 이 통계에서 디지털 증거는 우리 과학수사부의 디지털 및 사이버 수사과의 업무에 영상, 음성분석을 합친 정도로 생각되는데 연방기관에서 신흥 디지털포렌식 분야가 많이 이루어지는 것을 알 수 있습니다. 반면에 수사에서 활용도가 아주 높은 DNA분야는 의외로 다루고 있는 기관이 많지 않습니다. 아마도 운영비가 많이 들고 아직도 기술적으로 전문성이 높은 분야라는 인식이 있지 않나 생각합니다. 사건현장증거에 대한 DNA감정은 카운티나 시의 소규모 기관에서 많이 다루고 대규모 기관일수록 DNA DB관련 업무가 많은 것이 나타나고 있습니다.

그렇다면 법과학에 종사하는 인력의 숫자는 어느 정도나 될까요?

TABLE 10
Number of full-time employees in publicly funded forensic crime labs, by type of jurisdiction, 2002, 2005, 2009, and 2014

Type of jurisdiction	2002	2005	2009	2014
All labs	11,000	12,200	13,100	14,300
Federal	2,000	2,400	2,300	2,100
State	5,300	5,600	6,100	6,600
County	1,900	2,200	2,500	2,900
Municipal	1,900	2,000	2,200	2,700
Number of labs	351	389	411	409

Note: Estimates include both full-time and part-time employees, with a weight of 0.5 assigned to part-time employees. Numbers are rounded to nearest hundred. Detail does not sum to total due to rounding. See appendix table 10 for standard errors.
Source: Bureau of Justice Statistics, Census of Publicly Funded Forensic Crime Laboratories, 2002, 2005, 2009, and 2014.

2014년 통계에 의하면 14,300명의 정규직이 법과학기관에 근무하는 것으로 나타나고 이 중 약 80% 이상이 감정을 담당하거나 관리하는 기술인력으로 나타나고 있습니다. 인구의 수가 우리나라의 6배 정도인 점을 감안할 때 우리나라는 아직도 법과학 전문인력의 저변이 매우 취약하다는 것을 알 수 있습니다.

14,300 여명의 인력이 일년에 접수하는 감정물의 양은 2014년 기준 380만점 정도에 이르며 이 중 처리된 양은 360만점 정도라고 합니다. 단순하게 산술적으로 계산해 보면 1인당 일년에 처리하는 감정물 점수가 250여 점이라는 수치를 얻는데 업무의 법과학 분야별 특성이나 통계 기준의 차이를 감안해도 1인당 1천점이 훨씬 넘는 우리나라가 감정업무에 대한 부담이 훨씬 높은 것으로 나타납니다. 그럼에도 불구하고 미국 내 전체 감정 지연 현상이 아직도 문제가 되고 있으며 2014년 말 기준, 57만점 정도의 처리되지 않은 채 지연되고 있는 감정물이 있다고 합니다. 또한, 40%에 가까운 기관들은 접수된 감정물의 일부를 민간 등 외부로 아웃소싱 의뢰하기도 한다하니 우리나라와는 많은 차이가 존재하는 것 같습니다.

TABLE 5
Percent of requests for services received by publicly funded forensic crime labs, by type of jurisdiction, 2014

Type of request	Federal	State	County	Municipal
All requests	100%	100%	100%	100%
Controlled substances	27	33	40	31
Crime scene	--	--	9	17
Digital evidence	2	--	--	3
Firearms/toolmarks	--	3	5	10
Forensic biology casework	2	9	9	13
Forensic biology from convicted offender/arrestee samples	39	36	1	4
Impressions	--	--	--	--
Latent prints	24	4	10	12
Questioned documents	1	--	--	--
Toxicology	4	14	25	9
Trace evidence	1	1	2	1
Total requests received*	254,000	2,164,000	775,000	589,000

Source: Bureau of Justice Statistics, Census of Publicly Funded Forensic Crime Laboratories, 2014.

미국의 법과학 감정에 대한 규정이나 절차는 우리나라에 비해 많이 엄격하다는 사실에 비추어보면, 감정처리에 더 많은 시일이 소요된다는 것은 업무를 게을리한다기 보다는 감정의 정확성과 절차의 적합성을 매우 중시하는 단면에서 기인하는 것이라고 생각합니다. 외국의 법과학 전문가들과 얘기를 나눌 때 우리나라의 감정처리 기간이나 일인당 감정처리 건수를 얘기하면 '그 말이 사실이냐'고 종종 놀라곤 합니다. 우리나라가 과학수사 기술이 발전했다고 많은 나라에서 믿고 있는 현실에서 그리 자랑할 만한 일은 아닌 것 같습니다. 그만큼 허술한 면도 있을 수 있다는 얘기니까요. 국가적으로 조금 더 많은 관심과 투자가 체계적으로 이루어져야 하지 않을까요.

다음에는 미국의 대표적인 법과학 기관들에 대해 소개하고자 합니다.

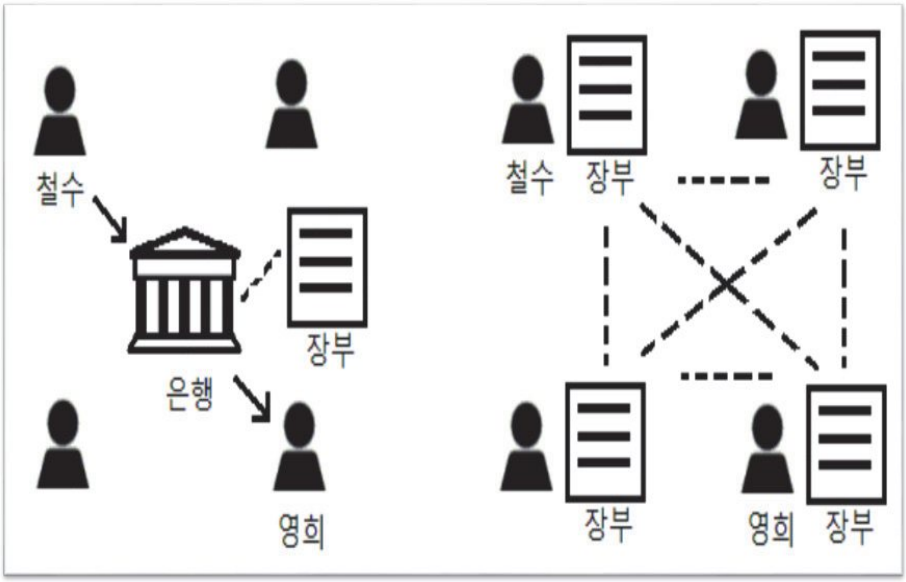
『블록체인·가상화폐에 대해 알아보자』 ①

블록체인 및 가상화폐 개념

사이버수사과 수사관 최훈제

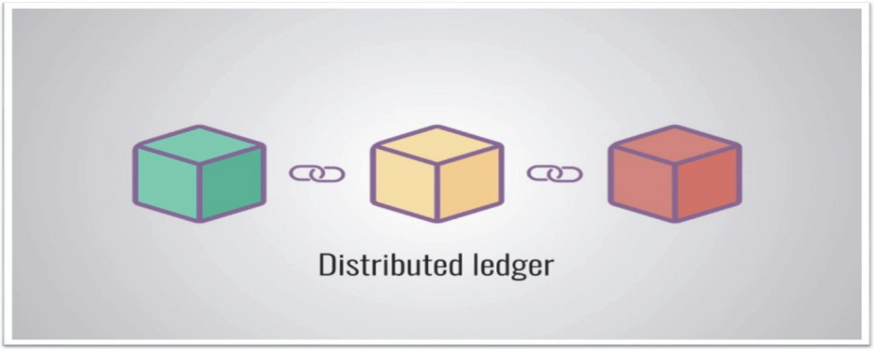
블록체인은 현재 우리나라 여러 공공기관에서 사용하거나 개발하고 있습니다. 서울 노원구 지역화폐, 관세청 출통관 서비스, 농림수산식품부 농산물 원산지 증명 시범 서비스, 의료기록 관련 증명서 발급 서비스, 중앙선거관리위원회 블록체인기반 투표시스템, 한국조폐공사 모바일 고향사랑 상품권 등 많은 분야에서 사용되고 있을 뿐만 아니라 에스토니아 전자영주권 발급, 영국 복지연금 프로젝트 등 해외에서도 다양하게 활용[1]되고 있습니다.

이번 연속기획의 첫 번째 내용으로 블록체인과 블록체인의 대표적인 기술인 비트코인 가상화폐의 개념에 대해 알아보도록 하겠습니다.

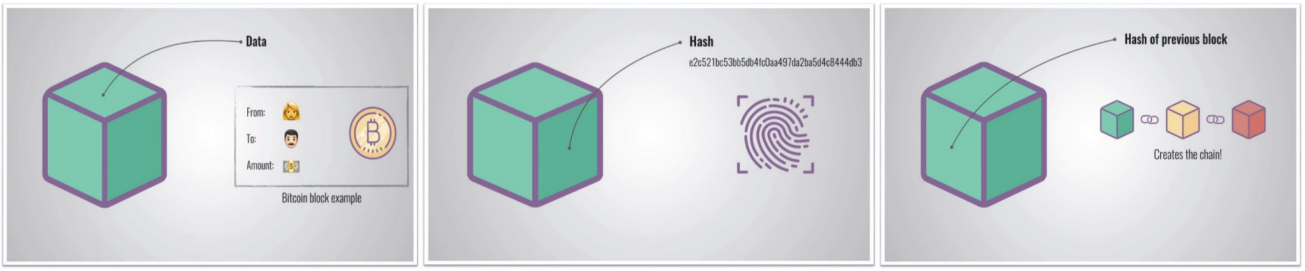


블록체인은 분산원장(Distributed ledger)입니다. 은행과 같이 신뢰할 수 있는 중앙기관이 보관·관리했던 거래내역이 담긴 장부를 중앙기관이 없이 모든 사람이 동일한 장부를 보관·관리하는 것입니다.

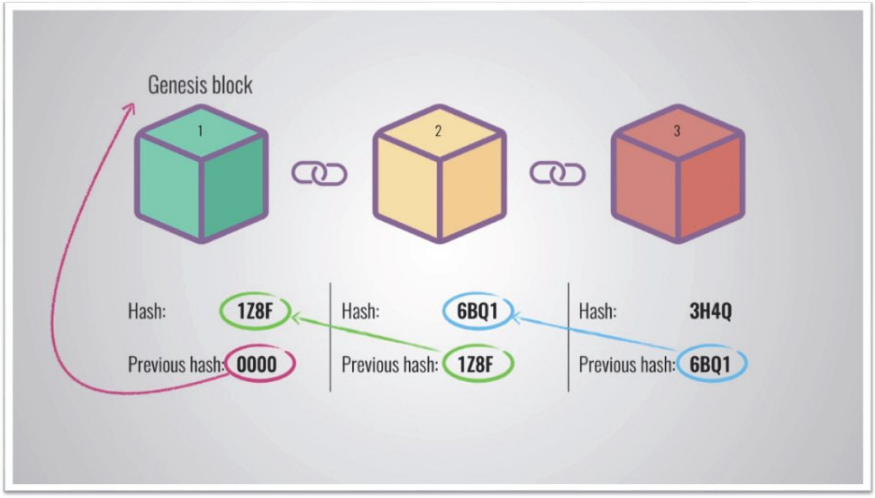
1) 2018. 10. 행정안전부 발간 디지털 공공서비스 혁신길잡이(가이드북, '공공서비스, 디지털기술로 날다')



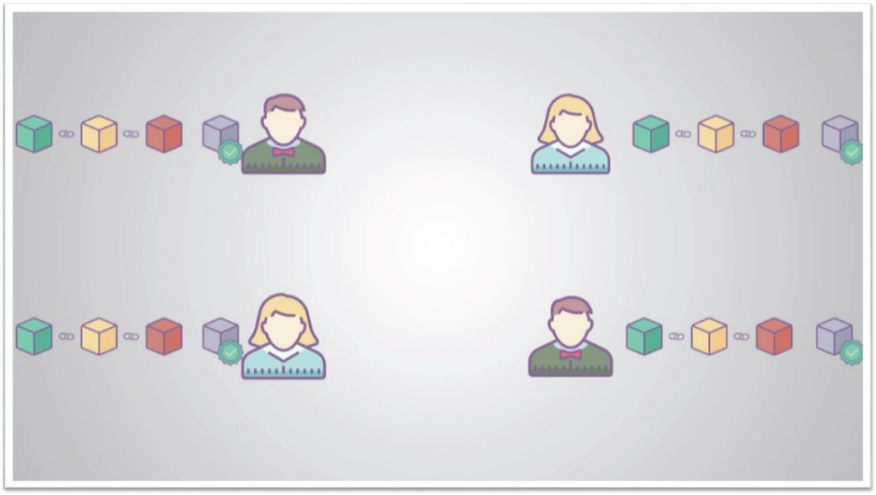
블록체인 전체는 하나의 장부이고 각 블록은 장부의 한 페이지에 해당합니다. 장부에 거래내역을 기입하고 페이지를 다 채우게 되면 다음 페이지로 넘어가게 되듯이 하나의 블록에 거래내역을 저장하고 거래내역이 다 저장된 블록은 다음 블록으로 연결되게 됩니다.



하나의 블록은 거래내역에 해당하는 데이터, 거래내역의 무결성을 보장하는 블록의 해시값, 전체 거래내역의 무결성을 보장하기 위한 이전 블록의 해시값을 가지고 있습니다.

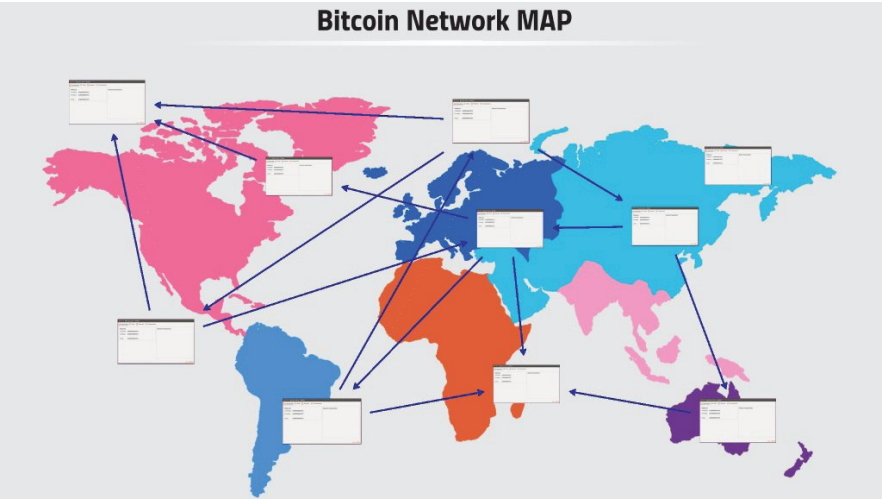


각 블록은 해시값을 통해 서로 연결되어 있기 때문에 전체 거래내역에 대한 무결성을 보장하게 됩니다.



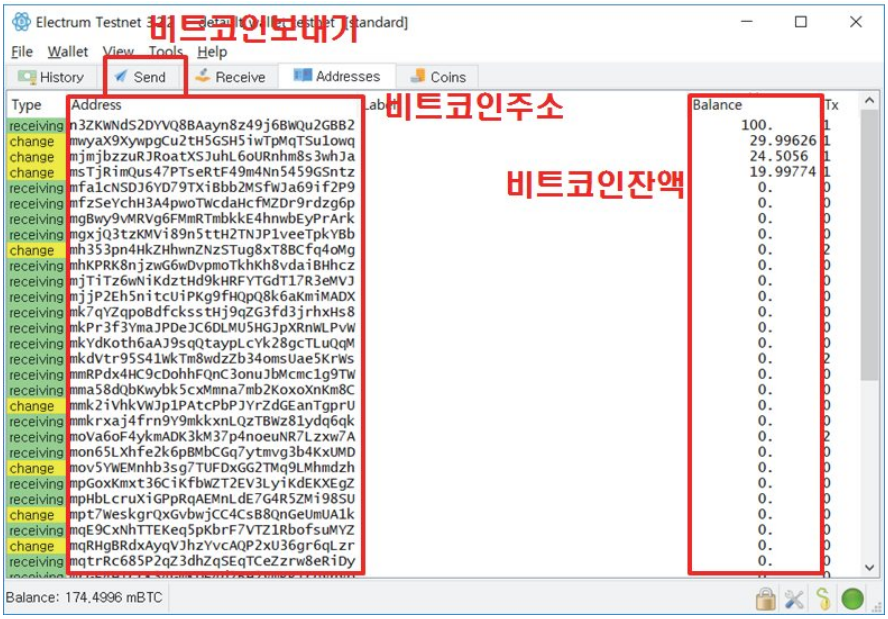
블록체인 참여자들은 이 전체 블록체인을 각자의 컴퓨터에 저장하고 해시값을 확인함으로써 거래의 신뢰성을 보장합니다.[2)]

다음으로 거래내역이 생성되고 블록에 포함되는 과정을 통해 지갑, 트랜잭션, 채굴에 대해 알아 보겠습니다.



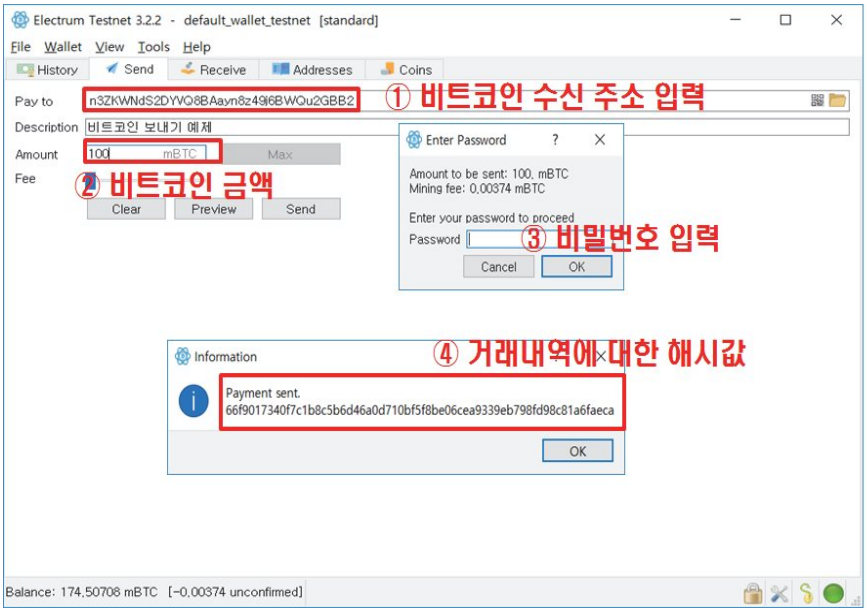
비트코인 블록체인에 참여하기 위해서는 흔히 지갑이라고 불리는 클라이언트 프로그램을 설치함으로써 참여할 수 있습니다. 지갑을 설치한 참여자는 P2P 네트워크를 통해 가까운 참여자들 끼리 연결되어 거래내역과 블록체인을 공유하게 됩니다.

2) 그림출처 : https://www.youtube.com/watch?v=SSo_EIwHSd4&t=17s, http://learnmeabitcoin.com

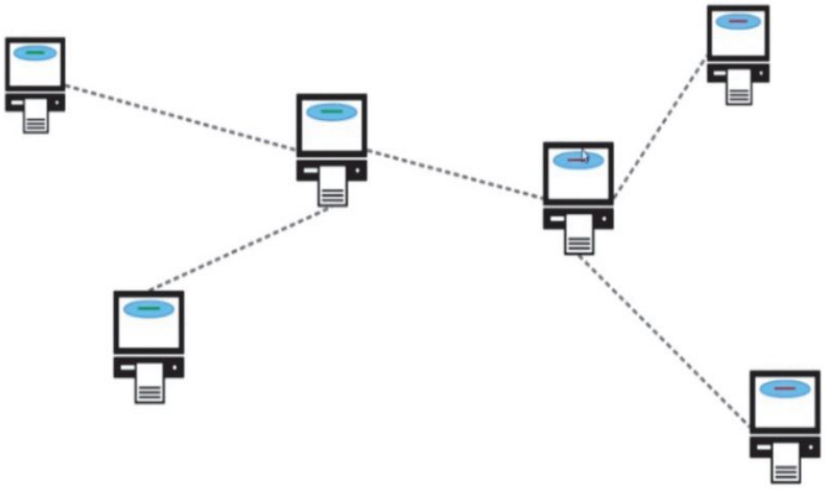


지갑 프로그램은 개인 컴퓨터에 설치되며 블록체인 네트워크에 참여하여 비트코인 보내기 및 받기, 잔액 확인, 개인키 관리 등의 기능을 합니다. 위의 그림과 같이 하나의 지갑은 여러 개의 비트코인 주소를 사용하게 되며 각 주소마다 비트코인이 들어있습니다.

참고로 가상화폐 거래소는 거래소에 이런 지갑 프로그램을 설치하여 사용자들이 직접 지갑 프로그램을 설치하지 않고도 비트코인을 주거나 받을 수 있는 서비스를 제공하는 것입니다.

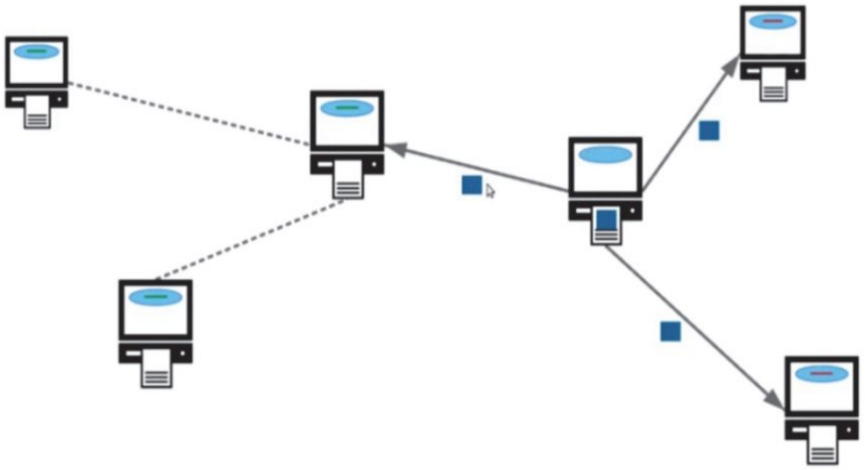


지갑 프로그램을 통해 비트코인을 상대방에게 보내게 되면 트랜잭션이라고 하는 해당 거래에 대한 거래내역이 생성됩니다.



새롭게 생성된 거래내역은 블록체인 네트워크를 통해 참여자들에게 전파되어 공유되게 됩니다. 아직 해당 거래는 장부에 포함된 상태는 아니며 따라서 해당거래는 신뢰성이 보장되는 상태가 아닙니다.

채굴자는 새로 생성되어 전파된 거래내역들을 모아 장부의 새로운 페이지에 기입하여 한 페이지를 채웁니다. 하지만 채굴자들은 많고 각자 새로운 페이지를 생성하기 때문에 가장 먼저 숙제를 푼 채굴자의 페이지만이 장부에 포함 될 수 있고 그 대가로 일정량의 비트코인을 받게 됩니다. 이 과정을 채굴이라고 합니다.



채굴을 통해 새로 생성된 페이지는 블록체인 네트워크를 통해 참여자들에게 전파되고 새로운 페이지를 받은 참여자들은 기존 장부에 새로운 페이지를 추가하게 되어 모든 참여자들이 동일한 장부를 소유하게 됩니다.

이렇게 새로 생성된 거래내역들이 새로운 페이지에 기입되고, 새로운 페이지가 추가된 장부가 다수의 참여자들에게 전파되어 저장 되었을 때 비로소 해당 거래내역은 신뢰할 수 있게 됩니다.

지금까지 블록체인과 가상화폐의 개념에 대해 간단히 알아보았습니다. 이론적인 부분은 다소 생소하고 어려울 수 있지만 개념과 본질에 대한 이해가 있어야 가상화폐 관련 사건에 대한 정확한 법리를 구성하는데 도움이 될 수 있을것 같습니다.

다음 호에서는 거래내역과 주소에 대해 좀 더 알아보도록 하겠습니다. 추가적으로 궁금한 사항에 대해 의견을 주시면 다음 호 내용에 반영하도록 하겠습니다.

『사건 속 법의학 이야기』 ③

91세 노모 성폭행 살인사건

서울대학교 법의학 교수 유성호

그는 어려서부터 작은 시골 동네에서 소문난 골칫덩어리였다. 위에 형과 누나는 과부인 어머니를 도울 요량으로 초등학교만 졸업하고 바로 타지로 나가 일을 하여 가계에 보탬이 되도록 작은 돈이나마 송금했다. 형과 누나는 자신들보다 10살 이상 어린 늦둥이인 막내를 고등학교까지 마치게 하고 싶었다. 그러나 그는 공부에 도통 관심이 없었으며, 동네에서 잦은 사고를 일으켰다. 처음에는 자신보다 어린 아이들의 코 묻은 돈을 빼앗더니, 이후로는 동네 빈 집에 들어가 돈을 훔치기까지 했다. 동네 사람들은 그를 처음에는 혼내고 타일렀지만, 그의 덩치가 커짐에 따라 두려워하여 아무 말도 하지 않게 되었다. 그는 고등학교를 중퇴하고 집에 남아 동네에서 잡일을 하고 돈을 받아 술을 먹는 일을 반복하며 지냈다.

그는 점차 자신의 처지를 비관하며 그 원인을 이제는 늙어버린 노모에게 돌렸다. 그는 폭언과 상습적 폭행을 노모에게 저지르는 패륜도 서슴지 않았다. 보다 못한 동네 이웃은 그에게 몰려가 그가 떠나기를 요구했다. 그는 술에 취한 채 동네를 떠났다.

수년 만에 그가 돌아왔다. 늙수그레하고 이마에 주름이 가득한 그의 얼굴을 보고 동네 사람들은 그가 험하고 거친 일을 했음을 짐작했다. 그는 아무런 인사도 없이 곧바로 노모가 살고 있는 집으로 향했다. 이제는 너무 늙어 허리가 굽고 거동이 불편한 노모는 큰아들이 가끔 들여다보며 돌보고 있었다. 노모가 10년 만에 찾아온 막내아들을 보고 반가워하는 것을 이웃 주민이 보았다. 그리고 그가 떠나는 모습은 아무도 보지 못했다.

다음날 노모는 자신의 집 좁은 마루에 누워 사망한 상태로 발견되었다. 경찰이 출동하여, 이웃 주민에게 전일 아들이 찾아왔다는 진술을 확보했다. 신속하게 부검이 시행되었다. 불쌍한 여인의 사망원인은 목을 손으로 조른 질식사인 액사로 판단하였다. 그런데 여성의 왼쪽 손목과 왼쪽 아래팔을 잡아 제압한 흔적이 관찰되었고, 노모의 성기 부위에 멍과 열창이 관찰되었다.

멍은 기본적으로 생활반응이다. 생활반응(Vital Reaction)이란 시신에 있는 손상이 생전(生前)에 생긴 것인지를 판단할 수 있는 기준으로 대표적인 것이 피하출혈, 즉 멍이다.

멍은 앞서도 언급하였듯이 혈관이 터지면 혈관 속에 있던 혈액이 흘러나오지만 혈압이 걸리지 않으므로 양은 생전 손상에 비하여 훨씬 적고, 혈액이 응고되지도 않는다. 따라서 응혈된 출혈이 있다면 이 손상은 생전에 생긴 것이다. 또한 성기 부위의 열창도 사후 손상이라면 적게 벌어지며 출혈이 거의 관찰되지 않는데 시신에서는 상처가 크게 벌어지면서 주변 응혈이 관찰되었다. 노모의 시신에서는 생활반응에 합당한 응혈된 출혈과 열창이 확인되었다.

그러나 경찰은 사망 후에 시신을 추행했다는 아들의 진술을 듣고 존속살인죄와 사체오욕죄[死體汚辱罪]로 검찰에 송치하였다. 피의자인 아들은 형, 형수가 거동이 불편한 피해자를 돌보기 힘들어하는 것을 보고 피해자를 목 졸라 살해한 후, 문득 사망한 피해자 등에 욕창이 있었는지 궁금하여 피해자의 등을 보려다가 성적 충동을 느껴 피해자 음부에 손가락을 넣게 되었다고 주장했다. 그러나 변사체의 목뿐만 아니라 음부, 얼굴, 팔다리 등에도 다수의 좌상 및 출혈이 확인된 데 의문을 가지고 전면적인 재수사에 착수하면서, 대검에서 지정한 당청 법의학 자문위원인 필자에게 의뢰가 온 것이었다.

검찰에서 주목한 것은 생활반응[1]이었다. 시체에 있는 손상이 생전(生前)에 생긴 것인지를 판단할 수 있는 소견이 생활반응이다. 만약 뜨거운 물에 데면 그 부위가 빨갛게 되고(발적), 물집이 생긴다(수포). 이는 열에 대하여 생체만 보이는 반응이고, 따라서 시체에서 이런 발적이나 수포를 보았다면 아직 생존하였을 때 열에 데었다고 볼 수 있다.

생활반응의 양상을 다음과 같이 설명할 수 있다.

첫째, 시체에서도 혈관이 터지면 혈관 속에 있던 혈액이 흘러나오지만 혈압이 걸리지

---

1) 만약 뜨거운 물에 데면 그 부위가 빨갛게 되고(발적), 물집이 생긴다(수포). 이는 열에 대하여 생체만 보이는 반응이고, 주검에서 이런 발적이나 수포를 보았다면 아직 생존하였을 때 열에 데었다고 단정할 수 있다. 이처럼 외부로부터 작용한 자극에 대하여 생체로서 반응한 결과로 나타난 변화를 사후에 확인할 수 있는 것을 생활반응이라 한다. 생활반응 중 국소적으로 나타나는 생활반응(Local Vital Reaction)으로 맨눈으로도 확인할 수 있는 소견은 다음과 같다.
① 출혈(出血, hemorrhage, bleeding); 혈관이 터지면 온몸을 돌고 있던 혈액은 혈압 때문에 혈관 밖으로 흘러나온다. 이것이 출혈이다. 출혈된 혈액이 고여 덩어리를 이루면 혈종(血腫, hematoma)이라 한다.
② 창상의 벌어짐(gaping of wound); 개방 손상은 피부나 근육이 수축하므로 벌어진다.
③ 염증성 변화(inflammatory reaction)나 치유 기전(wound healing)의 개시; 살아있을 때에 외력이나 감염을 받은 조직은 염증성 변화(발적, 종창 등)나 조직의 재생(섬유아세포의 증식, 결합조직의 생성 등)이 일어난다.
전신 생활 반응 (Systemic Vital Reaction)으로는 다음과 같은 소견이 있다.
① 빈혈(貧血, anemia); 손상 부위에서 다량 출혈하면 전신적 빈혈이 생긴다.
② 전색증(栓塞症, embolism); 손상 부위에서 생긴 지방 방울(fat droplet)이나 공기방울(air bubble), 작은 조직 조각이 색전으로 작용하여 혈관을 막고 있으면 이는 손상을 받을 때 혈류가 있었음을 의미한다.
③ 외래 물질의 전신분포 및 배설; 마신 술은 전신 각 장기에 분포하고 일부는 대사되어 소변으로 배설되는 것도 역시 일종의 생활반응이다.
④ 속발성 염증; 외상을 받은 후에 생긴 전신성 염증, 즉 패혈증, 균혈증.
⑤ 이물질 흡인; 익사(溺死)때 마신 물에 들어있던 플랑크톤이 전신 장기에 분포하거나, 소사(燒死)때 기관과 기관지에 검댕이 있거나, 두개골 바닥 골절 때 혈액을 흡입하였다면 이는 호흡 운동의 결과로 생긴 것이며 전신성 생활 반응이다.
⑥ 헤모글로빈(血色素)의 변화; 일산화탄소 중독이나 화재사망 사례에서 보는 카르복시헤모글로빈(carboxyhemoglobin, COHb)이나, 청산 중독 때의 cyanhemoglobin, 황화수소(H2S) 중독 때의 methemoglobin이 전신 퍼진 것은 생활반응이다.

않으므로 양은 생전 손상에 비하여 훨씬 미량이며, 혈액이 응고되지도 않는다. 따라서 응혈된 출혈이 있다면 이 손상은 생전에 생긴 것이며, 또한 흘러내린 혈흔이 있다면 생활반응의 하나로 중요하다. 같은 맥락으로 사후에 생긴 골절에는 출혈이 없다. 둘째, 생전에 생긴 개방성 손상은 탄력섬유가 수축하여 창구가 크게 벌어지며 주변부에 출혈을 동반하지만 사후 손상은 적게 벌어지며 출혈이 거의 관찰되지 않는다. 피해자인 노모에서는 ① 음부의 질어귀오목(vestibular fossa of vagina)의 출혈을 동반한 열창(裂創, laceration)[2]과 ②소음순(labium minus)의 피하출혈, ③현장에서 망인의 속옷에서 혈흔이 확인되었다. 따라서 소음순의 피하출혈 및 질어귀오목의 열창에 의해 속옷에서 흘러내린 혈액 등은 모두 생활반응의 국소적 소견으로 합당하다고 판단하며, 그 손상의 정도와 양상을 고려한다면 생전 손상이라고 판단하였다.

또한 피해자에게 발견된 다른 부위의 피하출혈은 ❶아래턱부위에서 표피박탈을 동반한 피하출혈, ❷목 부위에 표피박탈(爪痕)을 동반한 피하출혈, ❸양쪽 팔꿈치부위, 양쪽 아래팔부위, 양쪽 손목부위, 오른손 둘째손가락 바닥쪽 면의 피하출혈, ❹왼쪽 넓적다리 뒤쪽 부위의 피하출혈이었다. 이들 모두는 그 양태를 살피건대, 사망 전에 발생한 최근의 출혈이다. 특히 팔에서 관찰되는 부위는 방어흔[3]으로 추정할 수 있는 소견이라고 판단하였다. 결국 재판에서도 필자가 증인으로 출석하여 상처의 형태, 손상 정도, 출혈의 양을 기반으로 생활반응이 있음을 지적하였다.

결국, 피의자의 주장에만 의존하여 존속살인죄와 사체오욕죄 혐의로 송치된 이 사건은 법의학적 자문을 바탕으로 한 재수사 과정을 거쳐 사건의 실체가 밝혀졌다. 이에 법원도 피고인의 강간등살인의 혐의를 인정하여 무기징역을 선고하였다.

2) 피부가 지나치게 당겨져(伸展) 탄성 한계를 넘어 피부가 찢어진 상태이다.
3) 가해자의 공격을 손으로 잡거나, 팔로 막으려는 과정에서 생기는 손상이다. 주로 손바닥, 팔의 척골(尺骨, 자뼈) 쪽에서 관찰된다.

『과학수사 우수 논문 소개』

화웨이 스마트폰 백업 프로토콜

디지털수사과 수사관 박연재

디지털 증거물이 있는 곳에 연구개발이 있다!

대검찰청 디지털수사과 디지털포렌식연구소에서는 Digital Investigation 28호(2019. 3.)에 화웨이 스마트폰 백업파일에 대한 복호화 방안(Decrypting password-based encrypted backup data for Huawei smartphones)을 기고하였습니다.

최근 스마트폰의 시장은 급성장을 거듭하고 있으며, 매우 많은 사람들이 사용을 하고 있습니다. 한 스마트폰 시장 업체 조사 결과, 삼성(31%), 애플(23%), 화웨이(8%), 샤오미(8%)를 점유하고 있는 것으로 나타났습니다. 특히나 한국은 중국과 인접국가이므로 중국산 스마트폰(샤오미, 화웨이 등)을 구매하기 쉽고, 그로 인하여 범죄에 이용하는 경우도 빈번하게 발생하고 있습니다. 이러한 시장점유율로 인하여 디지털포렌식 분석 불가를 최소화하기 위해 2018년도에 디지털포렌식 연구소에서는 현재 상용화 및 기술개발이 완료된 삼성 스마트폰, 엘지 스마트폰의 백업프로토콜의 후속으로 화웨이 스마트폰에 대한 백업프로토콜에 대해 연구를 수행하였습니다.

스마트폰 백업 프로토콜이란 스마트폰에 저장된 데이터를 다른 개체(PC, 외장 메모리, 다른 스마트폰 등)에 보관, 재사용 등을 목적으로 옮기는 것을 의미합니다. 이렇게 백업 프로토콜을 이용하여 획득하는 방식을 디지털 포렌식적으로는 라이브 획득 혹은 로지컬 획득(논리 획득)이라고 칭합니다. 이와 반대개념으로 임베디드(기계적 혹은 전자적 장치 등을 데이터에 접근하여 획득하는 방식)방식, 우회부팅(정상적인 부팅이 아닌 복구모드, 업데이트 모드 등을 활용하여

디스크 저장장치에 접근하는 방식)방식이 있고, 이러한 획득 방식을 물리 획득 혹은 피지컬 획득이라고 칭합니다. 하지만 이러한 물리 획득은 패턴락이나 진입 비밀번호를 알지 못하는 경우에도 획득을 할 수 있고 분석도 가능하였으나, 안드로이드 보안강화(안드로이드 버전 6.0버전 이상)가 되면서, 디스크 전체에 대한 암호화(FDE, Full Disk Encryption) 기술 적용, 파일 기반 암호화(File Base Encryption) 기술 적용이 보편화, 기본 설정화 되면서 메모리 데이터를 가져온다고 하더라도 암호해독을 하지 못해 정상적인 데이터 분석을 할 수 없는 상황이 되어 부득이 스마트폰 백업 프로토콜을 사용하여 모바일 포렌식 획득을 진행하게 되었습니다.

백업프로토콜은 앞서 말한대로 스마트폰에 저장된 데이터를 다른 매체로 옮겨서 저장하는 것을 의미하고, 스마트폰 백업은 크게 두 가지 경우로 나누어질 수 있습니다. 첫 번째는 스마트폰 자체 저장공간에 저장하는 경우와 다른 하나는 스마트폰과 연결된 PC에 저장하는 경우가 있습니다. 스마트폰 자체에 저장하는 경우도 연구과제에 포함이 되어 있었으나, 지면 배분 문제로 금번에는 PC에 저장하는 경우로 국한해서 소개해드리겠습니다. PC에 저장하는 백업프로토콜을 사용하기 위해서는 우선 화웨이에서 제공하는 HiSuite라는 프로그램을 이용해야합니다. 그 이유는 특정 데이터를 주고 받기 위해서는 통신 규약대로 파일을 주고 받아야하는데 화웨이의 폰이 PC와 데이터 전송을 하기 위해서 화웨이에서 정한 통신 규약대로 주고 받아야 하기 때문입니다. 이러한 백업프로토콜의 경우 백업할 때 암호를 설정하는 방식과 암호를 설정하지 않는 방식으로 진행할 수 있으며, 백업 저장 방식은 암호 설정 및 파일 종류에 따라 다르게 저장되는 것을 아래의 표에서 확인하실 수 있습니다.

	DB 파일	APK 파일	미디어 등 파일
암호화 설정 O	O	X	O
암호화 설정 X	O	X	X

표 1. HiSuit를 통한 백업 시 암호화 설정에 따라 암호화 되는 파일의 종류

이러한 실험 결과 DB 파일은 백업을 진행할 시 암호와는 무관하게 암호화가 되고, 미디어 파일은 암호화 설정을 한 경우에만 암호화가 진행되는 것을 확인하였습니다. DB 파일은 모바일포렌식의 핵심인 전화기록, 문자, 카카오톡, 텔레그램 등 사용자가 생성한 내용이 대부분인 것으로 이 파일에 대해 암호화 알고리즘을 찾고, 복호화를 하는 것이 이번 연구과제의 핵심 주제입니다.

암호화 진행 방식은 암호키 생성 → 파일 암호화 → 백업 노트 생성의 과정으로 진행되는 것을 확인하였고, 여기에서 사용하는 함수는 OpenSSL과 advapi32를 사용하는 것을 확인하였습니다. 세부적으로 암호화 키는 사용자가 입력하는 패스워드를 해시함수를 이용하여 해시값으로 처리하고, 이렇게 생성된 해시값 중 일부를 암호화 키로 이용하게 됩니다. 이렇게 암호화키가 생성이 되면 파일 암호화를 진행하고, 암호화를 진행하는 함수는 특정 계산식이 포함된 함수로 계산 횟수를 매회 랜덤하게 계산하여 암호화를 진행하게 됩니다. 이러한 결과는 특정 파일에 저장이 되어, 이것을 근거로 암호화에 사용된 키값을 확인할 수 있으며, 또한 이러한 키값이 올바르게 생성된 값인지를 검증하는 절차도 포함이 되어있는 것을 확인하였습니다. 또한 프로그램의 버전 및 안드로이드의 버전에 따라 적용되는 함수가 다르다는 점도 확인하였으나, 세부적인 함수와 알고리즘에 대해서는 기술유출 등이 있으므로 밝히지 못하는 점 깊은 양해를 부탁드립니다.

또한 이러한 알고리즘에 대한 연구 수행 후, 역으로 암호화된 파일에 암호화 알고리즘을 역순으로 대입하여 복호화를 진행하게 하여 암호화된 DB파일에 대해 평문화를 진행하는 데 성공하였습니다. 미디어 등의 파일에 대한 암호화는 DB 파일과 다소 다른 부분이 있었으나, 대체로 간단한 정도의 암호화 과정을 거치고 있으므로 복호화를 하는 데는 큰 어려움이 없습니다.

이러한 결론이 도출되기 위한 가장 큰 전제는 백업파일과 관련한 모든 파일에 대해 수집이 가능해야한다는 것입니다. 물론 모든 파일이 없다고 하여 복호화를 못하는 것은 아니지만 암호화 키값을 찾기 위해 수백시간 수천시간의 시간비용이 들어갈 수 있습니다. 하지만 핸드폰을 압수하여 디지털포렌식팀에서 증거물 획득 및 분석을 진행한다는 전제에서는 특정 파일이 누락될 가능성은 매우 희박하다고 볼 수 있습니다. 이 프로그램은 현재 디지털포렌식 연구소에서 자체 개발중인 MFA 4.0에 탑재가 되어 화웨이 제조사에서 만든 스마트폰에 대해서는 획득 및 분석이 가능하게 되었습니다. 물론 대검찰청 및 거점청 디지털포렌식 수사지원팀에서도 화웨이 스마트폰에 대한 증거물 획득과 분석은 가능합니다. 다만 이번 연구가 모바일 포렌식에만 국한된 연구과제가 아닌 PC 압수수색 시 스마트폰 사용자의 자의적인 백업 파일을 발견하였을 경우, 특정 상용툴 제조사의 도움 없이 대검찰청 자체적인 기술만으로도 화웨이폰의 백업 파일을 복호화하여 증거로써 사용가능하다는 데에 더 큰 의의가 있지 않을까 하는 생각을 합니다. 앞으로 디지털포렌식 연구개발팀은 더 많은 증거를 획득하기 위한 연구개발에 힘쓸 것을 약속드립니다.

과학수사 대학(원)생 아이디어 공모전 입상작 소개 ③

- 최우수상 광주과학기술원 윤여경 -

과학수사기획관실 수사관 김희정

대검찰청 과학수사부에서는 2018. 10. 31. 개관 10주년을 기념하여 한국연구재단과 공동 주관으로 『4차산업혁명 시대의 과학수사 대학(원)생 아이디어 공모전』을 진행하였습니다.

공모작 총 60건 중 입상작 8건은 아래와 같습니다.

훈격	공모분야	대학명	제출자	작품명
대상	법과학분석	상명대학교	서건하외 1	영상촬영물에서의 생리 신호 모니터링 및 얼굴 표정 특징 기반 인공지능 심리분석 애플리케이션
최우수상	법과학분석	광주과학기술원	석영웅	범죄현장에서 미량의 시료로부터 신원 감별이 가능한 신속 DNA 분석용 휴대용 페이퍼 칩 시스템
최우수상	디지털수사	고려대	윤여경외 1	Cloud 기반의 WebOS 모바일 기기 압수 및 분석 방안
우수상	디지털수사	고려대	한승현	빅데이터 기반 유사범죄 해결방안에 대한 경우의 수 제시 및 추론
우수상	법과학분석	경북대	최다솜외 1	GAN 알고리즘을 적용한 쪽(조각) 지문 복구
우수상	사이버수사	성균관대	양성호외 2	가상화폐 익명성 추적을 위한 빅데이터 기반 이상거래탐지시스템 구축방안
우수상	기타	중앙대	이은지외 2	가상 범죄현장의 인공지능 범죄자 아바타
우수상	법과학분석	동아대	유홍연외 2	자연어처리를 이용한 담화 분석 기반의 과학수사 보조 시스템

이번호에는 최우수상 수상작을 소개합니다.

○ 제출자 : 고려대학교 윤여경

○ 제목 : Cloud 기반의 WebOS 모바일 기기 압수 및 분석 방안

공모전 제안서

『4차 산업혁명 시대의 과학수사 대학(원)생 아이디어 공모전』
아 이 디 어 개 요

분 야	□ 법과학분석 ■ 디지털수사 □ 사이버수사 □ 기타 과학수사 관련 자유주제
제안명	Cloud 기반의 WebOS 모바일 기기의 압수 및 분석 방안 (ChromeBook을 중심으로)
제안 배경	기존의 스마트폰과 PC에 대한 포렌식 방법으로, Cloud와 동기화하는 WebOS 형태의 모바일 기기에 대한 증거수집은 쉽지 않다. 그 이유는 동일 기기 다중 사용자의 기기에 대한 보안과 Cloud의 자료 이동성 때문이다. 그러므로 WebOS 모바일 기기에 맞는 증거수집 절차와 방법이 필요하다.
주요 내용	WebOS 모바일 기기는 인터넷과 Cloud 서비스를 기반으로 개발되었기 때문에 보안이 우수하고, 기기의 시스템 영역에 대한 접근이 어렵다. 그러므로, 기기의 일반사용자 모드와 관리자 모드로 나누어 증거수집 절차와 방법을 실행하고 수집한 증거를 분석하여 수사에 활용한다. · 일반사용자 모드의 접근 범위와 한계점 - 인터넷 사용과 안드로이드 앱만 실행 가능 - 시스템 영역에 접근 불가 【Chrome 브라우저의 Internal Chrome Pages를 이용한 수집 + Cloud】 · 관리자 모드에서 증거수집과 분석 방법 - 인터넷 사용과 안드로이드 앱만 실행 가능 - 시스템 영역 접근 가능 - 사용자 영역 암호화 【Chrome 브라우저 영역, Android Container 영역 수집 + Cloud】
기대 효과 (요약)	비용절감, 편리성, 보안성, 증거인멸의 용이성 때문에 Cloud 서비스가 범죄의 수단으로도 많이 사용되고 있지만 그에 대한 수사와 증거수집을 위한 접근이 어렵다. 하지만 Cloud 기반의 사용자 단말을 통하여 논리적인 증거수집과 Cloud에 보관하고 있는 자료의 선별 수집으로 이에 대한 문제를 해결하고, WebOS 모바일 기기에 대응하고자 한다.

『4차 산업혁명 시대의 과학수사 대학(원)생 아이디어 공모전』

아 이 디 어 제 안 서

1. 개 요

고속통신과 모바일 기기, 웹기술의 발전과 Cloud의 보안성, 경제성, 편리성으로, IT 환경이 Cloud 기반의 Web OS 기기로 이동하고 있다. 구글은 Google Cloud기반의 Chrome OS가 탑재된 Chromebook를 개발하였고, MS는 Azure 기반의 윈도우10과 오피스365를 융합한 윈도우 가상 데스크톱 이라는 Cloud OS를 발표하였다. 또한 이런 저비용, 보안성, 편리성, 증거인멸의 용이성 때문에 Cloud Computing이 범죄의 수단이나 도구로 많이 이용되고 있다.

하지만 Cloud 기반의 모바일 기기들은 시스템 영역에 접근하기 어렵고, 자료를 Clolud와 동기화하기 때문에 증거 수집이나 자료 확보가 쉽지 않다. 또한 현장 중심의 과학수사와는 다르게 압수나 임의 제출된 압수물을 분석하는 사무실 중심의 포렌식 방법으로는 그에 대한 대응이 더욱 어렵다.

2. 추진 목표 및 전략

수사기관의 포렌식 방법이나 절차를 변화하는 IT환경과 기기 특성에 맞게 바꿔야 한다. 이제는 모바일 기기의 보안성과 Cloud의 대중화로 기기 자체에 저장되는 증거 자료는 줄어들고 있고, 라이브 상태에서 자료를 추출하는 것이 일반적이 되었다.

그러므로, 압수대상에 따라 현장에서부터 증거 수집과 포렌식을 통한 분석 및 선별 압수하는 절차와 방법이 필요하다. 특히, Cloud 기반의 Web OS 기기를 압수하는 경우에는 포렌식 방법이나 절차를 현장까지 확대하여 대응할 필요가 있다.

3. 주요 내용

1. 크롬북의 특징

가. 크롬북 소개

크롬북은 외형적으로 컨버터블 노트북 형태이고, 일반적인 사양은 Intel Processor, 4-8GB 메모리, 터치스크린, 32-64GB eMMC, WebCam, Wifi, Bluetooth, USB Type-C, MicroSD Por를 지원한다.

크롬북에서 인식 가능한 외부기기의 파일시스템은 FAT(FAT16, FAT32, exFAT), NTFS, HFS+(Read only), UDF(Read only), ISO9660(Read only), MTP(Media Transfer Protocol) 등을 지원하고, 내부적으로 Ext4를 사용한다. 마이크로소프트 오피스(doc, docx, xls, xlsx, ppt, pptx), 영상(3gp, avi, mov, mp4, mkv, ogv, ogg, oga, webm, m4v, m4a, wav), 사진(bmp, gif, jpg, jpeg, png, webp), 압축(zip, rar) 파일을 사용할 수 있다.

데스크탑 PC와 다르게 전원을 켜고 약 7초 만에 부팅이 되고 로그인 화면을 보여준다. 등록된 구글 계정으로 로그인할 수 있으며 부팅시 마다 인터넷을 통해 업데이트와 보안패치를 확인하고 필요한 경우 업데이트를 한다. 부팅이 완료된 후 기본적으로 설치되어있는 소프트웨어는 크롬OS(브라우저), Gmail, 유투브, 구글드라이브, 구글독스, 구글 플레이스토어, 크롬 웹스토어를 지원하며 윈도우와 같은 탐색기를 통해 구글 드라이브를 온·오프라인으로 사용할 수 있다.

크롬북은 PC와는 다르게 부팅과정에서 중복을 제거하고 시작프로그램이 없어 부팅 속도가 빠르고, 펌웨어부터 시작되는 부팅과정에서 단계별로 보안키로 인증을 하고 변조 유무를 확인하기 때문에 보안성도 우수하다.

나. 크롬 OS 소개

크롬OS는 젠투(Gentoo Gentoo Linux : 자유오픈소스 소프트웨어로 바이너리 형태의 배포판으로 지원되지 않고 컴파일해서 직접설치) 리눅스 기반의 웹OS로, monolithic kernel을 사용하기 때문에 micro kernel에 비해 실행속도는 빠르지만 커널에 새로운 서비스를 추가 확장하는 것이 어렵고, 서비스 충돌시 전체 시스템에 영향을 줄 수 있다. 크롬OS의 아키텍처는 Firmware, System-level(linux kernel)과 user-land software, Chromium과 window manger 크게 3가지 구성요소로 나누어진다.

2. 데이터 수집

포렌식 관점에서 크롬북 자료를 수집하는 경우 크게 3가지로 나눌 수 있다. 첫 번째는 일반사용자(루팅이 안된 상태) 환경에서 자료를 수집하는 경우이고(시스템 영역 접근 불가), 두 번째는 관리자 권한(루팅된 상태)이 획득 가능하여 시스템과 사용자 영역에 접근하여 자료를 수집하는 경우이다. 세 번째는 클라우드 기반의 웹OS 형태이므로, 브라우저에서 클라우드 접속 계정과 암호가 저장되어 있는 경우 구글 드라이브와 이메일, 구글Docs에 자동접속이 가능하여 자료를 수집할 수 있다. 크롬 OS에서 주로 사용하는 브라우저 탭은 탭별로 샌드박스 형식으로 운영되기 때문에 상호 접근이 안되고, 사용자도 관리자 권한을 획득하지 않고는 시스템 영역에 접근할 수 없다.

가. 일반사용자 모드에서 데이터 수집(Live)

일반사용자 모드에서 접근할 수 있는 부분은 인터넷 브라우저, 사용자 로컬저장 영역과 설치된 안드로이드 앱 등이다. 관리자권한 상승이 없는 상황에서 데이터 접근과 수집은 매우 제한적이나 크롬북은 웹기반의 크롬OS 운영체제이므로 크롬브라우저의 Internal Chrome Pages를 통해서 데이터를 수집해야한다. 개발자에게 상세 정보를 제공하도록 설계된 크롬브라우저 내부페이지 이지만 일반사용자 모드에서도 브라우저를 통해 접근이 가능하여 데이터 수집에 사용할 수 있다.

주소창에 “chrome://about” 또는 “chrome://chrome-urls” 을 입력하게 되면 사용가능한 Chrome URLs 목록이 표시되고 이중에서 포렌식 관점에서 수집 가능한 정보의 종류와 목록을 아래 표와 같이 정리하였다.

표 1. Chrome URLs List

Category	Chrome URLs	Collection Info
Systme	version	OS, Platform, Firmware, User profile path, JavaScript info
Web	bookmarks	Chrome Bookmakrs
Systme	device-log	Network(Wifi), Bluetooth,Login, Power Event log
Web	extensions	Webstore Apps
Web	history	Chrome history
System	network	Wifi connetion info
Web	predictors	과거접속 정보를 이용한 자동완료 예측 목록
Web	quota-internals	chrome directory에서 domain별 디스크 사용 정보
Web	settings	Chrome 설정 정보, 사이트 저장암호
System	supervised-user-internals	chrome 사용자 정보
Systme & Web	sync-internals	OS 버전 history, ChromeWeb App, favicon, Typed URLs, Bookmarks
System	system	OS, Network, Device, WebApp, logcat, netlog, netstat, Wifi, ps, syslog, system_files info, threads, trim, kernel, clobber log etc
Web	thumbnails	Top sites URLs thumbnails

위와 같은 Internal Chrome Pages를 통해서 크롬OS 정보, 히스토리, 북마크, 크롬웹스토어 설치 앱, 네트워크, 사용자 정보 등을 mhtml 형식dmfh 수집할 수 있다. 클라우드와 연동되는 웹OS이므로 클라우드 정보도 수집이 가능하다. Chrome URLs 중 'chrome://version' 으로 크롬OS와 'chrome://settings/passwords' 로 저장된 웹페이지의 주소와 계정, 암호도 수집이 가능하다.

그림 1. 크롬OS 정보(좌), 사이트 저장 계정/암호 (우)

현장에서 라이브로 크롬북의 자료를 선별 수집하는 경우 탐색기를 통해서 온·오프라인에 따라 구글 드라이브의 파일을 수집할 수 있고, 자동접속 설정이 되어 있는 경우 구글Docs, 지메일, 구글킵(메모)에 접속하여 자료수집이 가능하다.

나. 개발자모드에서 논리적 데이터 수집(Logical export)

데이터 수집은 크게 크롬 OS 시스템, 구글 플레이스토어 설치앱, 크롬 브라우저와 크롬 웹앱, 저장파일 영역으로 구분되고 관련 디렉토리로 구분할 수 있는데, System은 시스템, 네트워크, 블루투스, Trim, 타임존 정보 등으로 운영체제가 부팅되고 운영되는 부분과 관련된 정보이다. Android App는 사용자가 구글플레이 스토어를 통해서 앱을 설치하는 경우 앱들이 저장되는 위치이다. Chrome Browser는 사용자의 인터넷 사용기록과 관련된 브라우저 저장위치, Chrome Web App은 크롬웹스토어를 통해서 브라우저에 Extension app형태로 설치되는 웹앱이 저장되는 위치이고, Media는 사용자 저장공간에 저장하는 사진, 영상, 오디오 파일인 멀티미디어 데이터를 저장하는 로그파일이다. 이와 같이 수집해야 하는 대상 위치 디렉토리를 기준으로 아래 표2.와 같이 정리하였다.

표2. 논리데이터 수집 위치(개발자모드)

Category	Path	Artifact
System	var/log	system log
	home/.shadow/UID/mount/user/	bash history
	var/lib/	trim info, timezone, bluetooth
Android App	/home/.shadow/UID/mount/root/android-data/data/	Contact, SNS, calender Media,
Chrome Browser	/home/.shadow/UID/mount/user/	History, Cache, Bookmark, Saved ID/Pass, etc
Download files	/home/.shadow/UID/mount/user/Downloads	
Chrome Web App	/home/.shadow/UID/mount/user/Extensions	WebApp Info

크롬 OS도 리눅스와 같이 kernel을 통해 디바이스와 사용자 영역까지 연결한다. 물론 안드로이드 스마트폰처럼 구글 플레이스토어를 지원하여 앱을 다운받아 설치와 실행을 할 수 있다. 이는 크롬 OS가 Android container를 갖고 있기 때문이다. 크롬북의 시스템과 디바이스에 대한 수집 가능한 로그와 데이터를 아래 표3.과 같이 정리하였다.

표 3. Chrome OS 시스템 정보 수집 위치(개발자모드)

Data	Path (/var, /home/.shadow, /etc)
BIOS 정보	/var/log/bios_info.txt
Chrome OS 버전 정보	/etc/os-release (os-release.d) /var/lib/crash_reporter/os-release /var/lib/crash_reporter/lsb-release
초기화, 루팅 정보	/var/log/clobber.log /var/log/clobber-state.log
TPM, 암호키 인증, P_UUID 정보	/var/log/debug_vboot_noisy.log
시작,종료, 절전 모드 시간	/var/log/eventlog.txt /var/log/metrics/shutdown.(date)
Wifi, SSID, IP 정보	/var/log/netlog (net.1~.log) /var/cache/shill/default.profile /.shadow/UID/mount/root/shill/shill.profile
터미널 사용기록	/var/log/secure (secure.1~)
MicroSD, USB mount 기록	/var/log/message (message.1~)
터미널 실행 명령어 기록	/home/.shadow/UID/mount/user/.bash_history
Bluetooth 정보	/var/lib/bluetooth/(S_MAC)/(D_MAC)/info
Trim 시간/상태 정보	/var/lib/trim/stateful_trim_data /var/lib/trim/statreful_trim_state
TimeZone 설정 정보	/var/lib/timezone/localtime

크롬북에서 안드로이드 플레이스토어를 처음부터 지원한 것은 아니다. OS 버전업과 구글의 정책이 변경되면서 안드로이드 앱을 지원하게 된 것이며 스마트폰과 비슷한 Android-data 하위 폴더구조를 갖고 있다. 하지만 크롬북은 스마트폰처럼 유심을 사용하여 전화통화, 문자메시지를 보낼 수 없다는 것이 스마트폰과 가장 큰 차이점이다. 통화기록, SMS/MMS, 이메일 정보를 제외하고, 구글앱과 멀티미디어 관련 정보를 주로 수집한다. 수집 가능한 데이터와 정보를 아래 표4.와 같이 정리하였다.

표 4. Android App 관련 정보 수집 위치(개발자모드)

Data	Path (/home/.shadow/UID/mount/root/android-data/data)
Google Play Store Apps	/data/(Application package name)/database /data/(Application package name)/cache /data/(Application package name)/files
Locale / Timezone	/property/persis.sys.locale /property/persis.sys.timezone
Multimedia files	/data/media/0/DCIM /data/media/0/Documents /data/media/0/Download /data/media/0/(SNS download files)
Multimedia log	/data/com.android.providers.media/databases/external.db
Contacts	/data/com.android.providers.contacts/databases/contacts2.db
Calendar	/data/com.android.providers.calendar/database/calendar.db
Google drive	/data/com.google.android.apps.docs/database/DocList.db /data/com.google.android.apps.editors.docs/database/DocList.db

사용자 측면에서 보면 클라우드와 인터넷 접속을 하는 경우 Android Container의 브라우저나 앱을 설치하여 사용할 수 있지만 이미 사용이 가능하게 구성된 크롬 브라우저를 통해서 구글 클라우드와 인터넷 접속을 하는 경우가 일반적이다. 크롬 웹스토어에서 설치된 웹앱과 클라우드, 인터넷 접속과 관련된 아티팩트를 수집할 수 있는 위치와 내용을 아래 표5.와 같이 정리하였다.

표 5. Chrome browser 관련 정보 수집 위치(개발자모드)

Data	Path (home/.shadow/UID/mount/user)
Web Artifacts	/Bookmarks, /Cookies, /Cache, /History, /Login Data, /Network Action Predictor, /QuotaManager,
Google Profile Image	/Accounts/Avatar Images/ID
Download files	/Downloads
Web Store Apps	/Extensions/(Web App_ID)

3. 데이터 분석

가. 사용자 모드에서 수집한 라이브 데이터 분석

일반사용자 모드인 경우 권한상승이 되지 않기 때문에 시스템 영역에는 접근할 수 없다. 그러므로 수집할 수 있는 정보는 극히 제한적이다. 라이브 상태에서 "chrome://chrome-urls" 를 통해 수집한 정보와 사용자 로컬저장 영역에서 추출한 파일, 온·오프라인 경우 탐색기를 통한 구글 드라이브에서 수집 가능한 파일 뿐이다.

Internal Chrome Pages에서 수집 가능한 자료는 크롬북 바이오스와 크롬 OS 상세정보, 사용자 계정 정보, 웹접속기록, 웹다운로드 파일목록, 블루투스 정보, 디바이스 로그, 클라우드 프린터, 크롬 웹스토어에서 설치된 앱정보, 네트워크(Wifi) 정보, Top Sites (썸네일), 자동 로그인 사이트와 계정, 암호, 마지막 로그인 사이트의 세부정보, 부팅 로그, 초기화 정보, 디바이스 정보, net log, power log, Trim log 등 크롬북과 OS, 사용자 계정, 웹히스토리, 웹앱 설치정보, 구글 드라이브 주요 로그를 확인할 수 있다.

나. 크롬 브라우저 수집 파일 분석(개발자모드)

크롬북의 인터넷 사용기록이 저장되는 곳으로 위치는 '/home/.shadow/(UID)/mount/user' 에 기록된다. 증거수집 표5.의 내용을 참고하여 분석한다. 인터넷 History, Cache, Bookmarks. Avatar image, Chrome WebApp 설치목록, Downloads 파일, 로그인 저장페이지의 주소, 계정, 암호 등을 수집할 수 있다.

Chrome WebApp Store에서 설치된 앱은 '/user/Extensions' 의 하위 폴더를 생성하며 설치가 되는데 폴더명으로 웹스토어에서 조회를 하면 정확한 앱을 확인할 수 있다. 수집한 SQLite 형식의 파일은 도구를 사용하여 복원 작업 후 정보를 분석한다.

다. Android Container 파일 분석(개발자모드)

구글플레이 스토어에서 다운받은 앱들을 설치하고 운영되는 곳이다. 구글 플레이스토어에서 크롬북을 처음부터 지원한 것은 아니며 크롬 OS 53버전 이후부터 지원하기 시작하였다. 크롬북에서 Android Container 는 안드로이드 앱이 운영되는 부분을 말한다. 크롬북에서 안드로이드 시스템 저장위치는 '/home/.shadow/(UID)/mount/root/android-data/data/' 폴더 이하에서 생성된다. 안드로이드 스마트폰 폴더구조와 유사하다. 안드로이드 스마트폰과의 차이점은 유심칩을 사용하지 않는다는 것이다.

/app, /data, /dalvic-cache, /media, /misc 폴더는 안드로이드 스마트폰과 같은 구조로 저장된다. 이 중 /misc에서 다바이스 관련 로그는 확인되지 않는다. 증거수집에서 중요하게 확인해야하는 폴더는 /data, /media 이다.

안드로이드 기본앱과 구글 플레이스토어에서 다운 받아 설치 저장되는 위치인 /data 하위 폴더에서 SQLite 파일을 선별하여 DB파일에서 데이터를 레코드 복구 및 추출하여 정보를 분석한다.

/media 폴더는 크롬북의 WebCAM, 카카오톡이나 텐센트 같은 SNS 앱에서 다운로드 받은 파일 등이 저장되는 공간으로 이곳에 저장된 파일을 추출하여 분석할 필요가 있다. 크롬북의 WebCAM으로 촬영하여 저장되는 파일의 기본형식은 사진파일은 'IMG_일자_시간.jpg' 형식이고, 동영상 파일은 'VID_일자_시간.webm'으로 각각 ./Pictures와 ./Movies 폴더에 저장된다. /media 폴더 이하에 각 저장되는 사진, 영상파일은 external.db 파일에 로그가 저장되고, 사진이나 영상 파일을 삭제해도 해당 레코드가 바로 삭제되지 않는다.

_id	_data	_size	format	parent	date_added	date_modified	mime_type
	Click here to define a filter						
25	/storage/emulated/0/Download/Screenshot 2018-09-08 at 18.13.19.png	502952	14347	8	1536398000	1536397999	image/png
26	/storage/emulated/0/Download/Screenshot 2018-09-08 at 18.13.39.png	208343	14347	8	1536398020	1536398019	image/png
27	/storage/emulated/0/Android	(null)	12289	0	(null)	1536379324	(null)
28	/storage/emulated/0/Android/data	(null)	12289	27	(null)	1536379426	(null)
29	/storage/emulated/0/Android/data/com.google.android.gms	(null)	12289	28	(null)	1536379324	(null)
30	/storage/emulated/0/Android/data/com.google.android.gms/files	(null)	12289	29	(null)	1536400363	(null)
31	/storage/emulated/0/Android/data/com.google.android.gms/files/gmsnet2.jpg	159	14337	30	1536581546	1536400363	image/jpeg
33	/storage/emulated/0/Download/Screenshot 2018-09-27 at 00.24.14.png	1326791	14347	8	1537975455	1537975454	image/png
34	/storage/emulated/0/Download/Screenshot 2018-09-29 at 20.57.45.png	371737	14347	8	1538222267	1538222266	image/png
35	/storage/emulated/0/Download/Screenshot 2018-09-29 at 21.27.20.png	746799	14347	8	1538224041	1538224040	image/png
36	/storage/emulated/0/Android/data/org.telegram.messenger	(null)	12289	28	(null)	1537976140	(null)
37	/storage/emulated/0/Android/data/org.telegram.messenger/cache	(null)	12289	36	(null)	1538402584	(null)
38	/storage/emulated/0/Android/data/org.telegram.messenger/cache/2_71217939 5279716704.webp	73812	14336	37	1538406372	1538402446	image/webp
39	/storage/emulated/0/Android/data/org.telegram.messenger/cache/713417809_ 21399.webp	10790	14336	37	1538406372	1538402446	image/webp

그림2. data/com.android.providers.media/databases/external.db

4. 크롬북의 데이터 수집 및 분석 절차

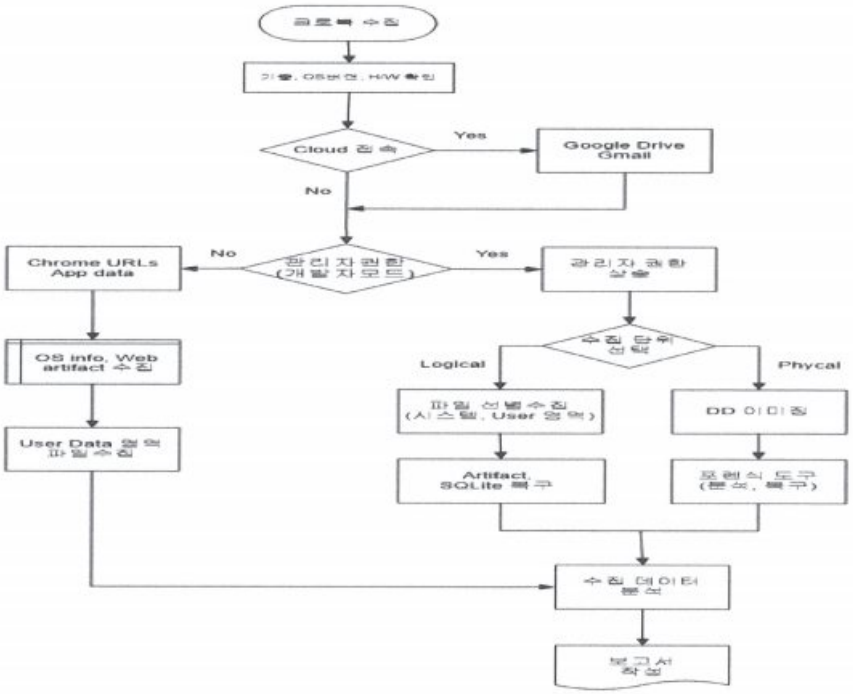
크롬북과 같은 클라우드 기반의 웹OS 형태의 모바일 기기는 동일기기의 다중 사용자를 염두에 두고 개발되었다. 그렇기 때문에 데이터 수집단계에서부터 클라우드 환경을 고려해야 한다. 크롬북의 기종, OS 버전 등 정보를 확인하고, 라이브 상태에서 클아우드가 접속 가능한 상태인지를 확인하여 구글 드라이브, 지메일, 구글독스에 대한 자료를 수집한다.

일반사용자와 관리자 모드에 따라서 증거수집 방법을 달리해야 하기 때문에, 일반사용자 모드에서는 웹브라우저를 이용하여 시스템 로그, 사용자 정보를 수집하고, 사용자 영역에서는 로컬스토리지에 저장된 파일을 수집한다.

관리자모드(개발자)가 가능한 상태에서는 Logical과 Physcial로 나누어지는데 크롬북은 Ecryptfs 암호화 파일시스템을 사용하기 때문에 로지컬에서 디렉토리나 파일 단위로 추출하는 것이 좋다.

3가지 영역으로 구분하여 수집하는 하는데, 첫 번째는 'home/.shadow/(UID)/mount'를 기준으로 'user' 폴더 이하의 ChromeOS와 두번째는 'root/android-data/data' 폴더 이하의 Android-Container 영역, 세 번째는 사용자의 로컬파일 저장영역(구글 드라이브 오프라인 포함)으로 구분해서 증거를 수집한다.

이렇게 수집한 시스템 로그와 SNS, History, Contact, Cache, Calendar, External, Download SQLite 파일 등은 포렌식 도구를 사용하여 복구 및 분석하고, 사용자 영역과 클라우드에서 수집한 문서, 영상, 사진 파일과 같이 분석하여 보고서를 작성한다.



[크롬북 데이터 수집·분석 절차]

4. 아이디어의 가치

Cloud 기반의 Web SO가 탑재된 모바일 기기 중 Chromebook을 제외하고 대중적인 기기는 아직 없다. Chromebook은 동일 기기 다중사용자 환경을 위한 모바일 기기로 사용자 간의 privacy 침해를 막기 위해 보안성이 우수하므로, 증거수집이 어렵다. 이런 모바일 기기특성을 고려하여 전체적인 증거수집 방법과 절차에 대한 프레임워크는 연구된 것이 없다. 실질적으로 현장에서부터 이런 절차와 방법을 고려하여 적용한다면 선별압수 요건은 물론 기기를 통한 Cloud의 자료까지 수사의 범위를 확대할 수 있을 것으로 본다.

5. 기대효과

인터넷이나 국외 Cloud를 이용한 범죄의 경우 사실상 국제공조가 어렵다. 각 국가 간의 법과 정책이 다른 부분도 있겠지만 사이버의 특성 때문에 범죄현장이 국내가 아닌 국외가 많고 수집해야할 자료 또한 국외 서버에 있는 경우가 대다수이다. 이런 경우 증거수집이나 수사 진행이 어렵고, 관련 클라우드 기반의 모바일 기기를 압수하여도 기존의 포렌식 방법으로는 자료 추출이나 분석이 쉽지 않다.

지금까지 디지털 기기에 대한 포렌식 방법은 현장에서 압수된 스마트폰, PC, 디스크 등을 복제하고, 복구하여 분석하는 절차로 진행한다. 하지만 크롬북의 경우 현장에서 라이브 상태로 증거수집을 하는 경우 더 많은 자료를 수집할 수 있었고, 암호화와 보안성 때문에 기존의 사무실에서 진행하는 포렌식 절차를 수행하는 것만으로는 이런 환경의 모바일 기기에 대한 분석과 자료수집이 어렵다. 이제는 물리적, 논리적 획득에 의한 포렌식 보다는 Live 환경의 적극적인 포렌식으로 전환할 필요가 있다. 기기 특성에 맞게 방법을 바꾸고, 모바일 기기를 이용하여 Cloud까지 접근할 수 있다면 수사의 범위와 증거 확보의 가능성을 좀 더 높일 수 있을 것으로 기대한다.

『영화로 본 수사관 일기』 ⑬ <아이캔스피크>

- 오늘도 검찰청 최전방을 지키고 있습니다만

서울남부지검 수사관 강현식

악성(惡性)[명사] :

① 악한 성질, ② 어떤 병이 고치기 어렵거나 생명을 위협할 정도로 심함.

민원인(民願人)[명사] :

행정기관에 민원의 처리를 요구하는 자연인 또는 단체.

제가 검찰에 입사한 후 지청을 거쳐 처음으로 일다운 일을 했던 부서가 바로 서울중앙지검 사건과 종합민원실이었습니다. 그것도 5번 창구. 담당업무는 민원서류 접수 및 출국금지. 민원실 맨 오른쪽 끄트머리에 앉아서 하루종일 온갖 민원인들이 가져오는 서류를 접수받아 접수인을 날인하고, 중간중간 출국금지 요청서 결재를 위해 해당 검사실을 오가는 업무를 7개월 정도 맡았었습니다.

"종합민원실은 해당 검찰청의 얼굴이다"라는 말씀을 어디선가 들은 기억이 있는데, 그 말의 무게 때문인지는 몰라도 항상 웃는 얼굴로 대하려고 노력했지만, 거기서 만난 거대한 존재 때문에 번번히 좌절하고 번민에 빠졌던 생각이 나서 지금에 와서는 웃음이 나기도 합니다.

검찰청에서 근무하는 사람이라면 누구나 알고 있는 그 거대한 존재. 바로 '악성 민원인'인데요. 앞서 언급한대로 '악성'과 '민원인'의 사전적 의미를 합치면 '악성민원인'이란, '악한 성질을 가진 민원처리 요구자'라고 정의할 수 있겠지만, 쉽게 뜻하자면 '말도 안되는 트집을 잡으며 민원 담당자를 시종일관 괴롭게 하는 민원인'이라고 할 수 있을 겁니다. 특히, 제가 근무했었던 서울중앙지검 종합민원실은 한국의 대표 검찰청답게 그 규모만큼이나 엄청난 수의 악성민원인을 수도없이 만날 수 있었던 곳이었습니다. 혹자는 '악성민원인들의 배움터', '악성민원인의 성지'라고 할 정도로 타 청에서 악명을 드높이는 민원인들이 세를 늘려가면서 서울중앙지검 종합민원실을 몇 시간동안 점령(?)하면서 담당 직원들을 힘들게 한 적도 있었습니다.

영화 <아이캔스피크>는 잘 알려진 대로 위안부로 끌려갔었던 아픈 기억을 가지고 있는 옥분이라는 할머니가 주민센터 공무원에게 영어를 배워 미국까지 건너가 몸소 피해사례를 널리 알렸던 실화를 바탕으로 했던 작품이었습니다. 다만, 저는 영화 끝에 전해져오는 감동도 진하게 느꼈었지만, 영화 초반부에 나왔던 상황이 보는 내내 상당히 인상적이었습니다. 온 동네를 휘저으며 무려 8,000건에 달하는 민원을 넣고, 원칙에 어긋난 행정이라고 느낄 경우 매일같이 주민센터를 찾아가서 공무원들을 괴롭히는 주인공 옥분의 모습에서 지난날 종합민원실에서 보았던 악성민원인들이 오버랩되었기 때문이지요.

그런데, 한 가지 재미있는 사실은 제가 6개월이란 시간을 들여 배웠던 악성민원인 응대법을 <아이캔스피크>에서도 고스란히 보여주고 있었다는 점이었습니다. 시간이 걸리더라도 얘기를 들어주는 것. 사실 들어보면 그리 어렵지 않은 방법이지만, 결코 쉽지 않은 것이 바로 이 방법이기도 합니다. 매번 바쁜 시간에 찾아와서 아무 말 없이 데스크 위에 떡하니 100장이 넘는 고소장을 올려놓고 접수를 요구하고, 원본을 복사해달라고 하면서, 동시에 기다리기가 매우 무료하니 커피를 줘야하지 않느냐며 으름장을 놓는 등 악성민원 요구사항 3종 세트를 발동하는 민원인에게 시간이 걸리더라도 얘기를 들어주기란 여간 어려운 일이 아니기 때문

입니다.

저를 매번 찾아오던 여성 민원인 한 분이 있었습니다. 모자를 썼으며, 매우 많은 양의 서류뭉치가 들어 있을 법한 백팩을 메고, 비도 오지 않는 날씨에 긴 우산까지 들고 왔던 분이었습니다. 그 분이 와서 하는 일은 매번 민원서류를 제출하는 제 담당창구로 와서 내용도 전혀 바뀌지 않은 고소장을 내밀며 사본을 해달라는 것이었습니다.

처음에는 친절모드를 가동하여 요구사항을 들어주었는데, 옆자리 선배는 저에게 이렇게 말해주었습니다.

"저 아줌마, 조심해야 돼. 해주기 시작하면 끝이 없어."

아니나 다를까, 그 민원인은 그 다음 날에 "내가 접수한 고소장을 3부 복사해달라", 또 그 다음날은 "내가 접수한 고소장을 5부 복사하고 낱장마다 접수인을 다 찍어줘라"는 등 기하급수적으로 요구사항이 늘어나기 시작했고, 급기야 저는 화를 이기지 못하고 이렇게 쏘아붙였죠. "저기....맨날 오셔서 저한테 왜 이러시는 거예요?" "너 이름 뭐냐? 국민신문고라고 알지? 너 거기 한 번 데뷔해볼래?"

"항상 민원인을 친절하게 대해야 한다"라는 말은 민원실 근무직원에게는 마치 잠언처럼 늘 지켜야하는 것이어야 하지만, 그들도 엄청난 스트레스 속에 살아가는 감정노동자라는 사실도 한번쯤 알아주셨으면 좋겠다는 생각이 듭니다. 사실 그들이야말로 검찰청 최일선을 지키는 당당한 검찰수사관이니까요.

YTN science

[사이언스 CSI] 국민의 생명과 재산을 지킨다! 'NDFC 화재수사팀'

2019-03-04

■ 강정기 / 대검찰청 화재수사팀 수사관

[앵커]

화재사건은 다른 사건과 달리 목격자도 찾기 힘들고 증거가 훼손되기 쉬워서 사건의 진실을 밝히기가 쉽지 않다고 합니다. 하지만 객관적이고 과학적인 분석을 통해 억울한 사건을 해결하는 분들이 있다고 하는데요.

오늘 사이언스 CSI에서는 '실체적 진실을 밝히는 대검찰청 화재수사팀'에 대해 알아보겠습니다. 강정기 수사관과 함께합니다. 어서 오세요.

대검찰청에 화재수사를 전담하는 팀이 있다는 것이 조금은 생소한데요. 어떤 팀인지 소개 부탁드립니다.

[인터뷰]

대검찰청 화재수사팀은 검찰청에서 화재나 폭발사건에 대해 수사나 재판 중 사실관계를 명확히 해야 할 사건이 있을 경우에 수사지원을 하는 업무를 담당하고 있습니다. 좀 더 구체적으로 말씀드리면 검사

가 화재사건을 수사하면서 기소 여부를 결정하거나, 기소하여 재판 중인 사건에 대해서 실체적 진실을 밝히기 위해서 수사지원을 의뢰하게 됩니다. 그러면 화재수사팀에서는 현장 감식, 재연실험, 컴퓨터 시뮬레이션 등 다양한 기법을 통해 감정하는 업무를 담당하고 있습니다.

[앵커]

저는 일반적으로 화재를 수사한다고 하면 일단 소방서나 국과수 감식이 떠오르는데요. 화재수사팀과는 어떻게 다른 건가요?

[인터뷰]

많은 분들이 그렇게 생각하고 있습니다. 일단 말씀하신 소방, 경찰, 국과수 등은 1차, 초동조사기관으로 생각하시면 됩니다. 화재가 발생한 즉시 현장에 투입되어 발화지점과 발화 원인을 찾는 것이 주 업무라 생각하시면 됩니다. 반면 화재수사팀은 2차 감정기관으로, 형사사건이 검찰로 송치된 후 피의자나 피해자의 행위를 밝히는 것이 더 중요한 업무입니다. 빈번하게 발생하는 사건으로 말씀드리면, 두 사람이 한 공간에 있다가 유류화재가 발생했을 경우 초동조사에서는 현장을 감식하면서 탄화 패턴을 분석하고 유류의 성분을 감정하여 '휘발유를 이용한 방화'로 판단을 하게 됩니다.

하지만 대검 화재수사팀에서는 휘발유에 의한 방화인 것은 알겠는데 그러면 누가 불을 냈는지 알기 위해서 피의자와 피해자의 화상 부위 분석하고, 피의자의 진술 여부 분석 등을 통해서 누가 휘발유를 뿌렸고 누가, 어떤 방법으로 불을 붙였는지 밝히는 등 피의자와 피해자의 행위를 분석하는 것입니다. 즉, 초동 조사기관과 대검 화재수사팀은 조금은 다른, 상호보완적인 업무를 하고 있다고 보시면 되겠습니다.

[앵커]

차이가 있군요. 2차 감정기관인 만큼, 화재사건이 대검 화재수사팀에 가기까지는 상당한 시간이 걸릴 것 같은데요. 그러면 아무래도 현장에 대한 조사는 불충분할 수도 있지 않을까요?

[인터뷰]

아무래도 화재 발생 직후 현장 감식을 하는 것보다는 어려운 부분이 있습니다. 하지만 초동조사기관에서 촬영한 사진 등을 참고로 현장을 재구성하면 사건 발생 당일 있었던 일을 추정할 수 있습니다.

한 사례를 말씀드리면, 2002년도에 화재 사망 사건이 발생하고 약 9년이 지난 후 재수사한 사건이 있었습니다. 가정집에서 불이 나 4살 아이가 숨진 사건으로 사건 발생 당시에는 형광등 누전으로 인한 화재로 내사종결 되었습니다. 그런데 9년 후 당시 아이 아버지와 동거했던 여성이 '아이의 아버지가 아이의 몸에 휘발유를 뿌리고 불을 질러 살해했다'는 내용으로 투서를 한 것입니다.

[앵커]

9년이나 지났으면 증거나 흔적도 많이 사라졌을 것 같아요.

[인터뷰]

네, 그렇죠. 피의자는 처음에는 완강히 부인했으나 나중에는 방에 휘발유를 뿌린 사실에 대해서는 인정

을 했습니다. 하지만 끝까지 아이의 몸에는 휘발유를 뿌리지 않았다고 주장했습니다. 현장은 화재 후 방치되어 저희가 갔을 때는 이미 폐허가 되어 있었습니다. 하지만 화재 발생 직후 촬영한 사진과 비교하며 기둥과 벽, 그리고 출입문의 위치를 특정하자 중요한 사실이 확인되었습니다.

[앵커]

뭔가요?

[인터뷰]

피해자는 화재 발생 당시 출입문에 가장 가까이 있었음에도 탈출을 하지 못하였습니다. 또한, 피해자는 침대 밑에서 발견되었음에도 화염과 반대 방향에서 두개골 개방골절과 신체 소실이 발생한 것입니다. 이것은 피의자가 피해자의 좌측 머리 쪽에 휘발유를 부었다는 명백한 증거이며 재판부에서도 이를 받아들여 피고인에게 중형을 선고했습니다. 이처럼 시간이 지난 현장에서도 사건의 핵심적인 사실이 남아 있을 수 있어서 아무리 오래된 현장이라 하더라도 반드시 확인할 필요가 있습니다.

[앵커]

그렇군요. 앞서 현장감식뿐만 아니라 여러 다양한 기법을 활용한다고 말씀해주셨는데요. 먼저 재연실험은 어떻게 이루어지나요?

[인터뷰]

재연실험은 사건마다 다르고 방법은 팀 회의에 의해 결정됩니다. 우선은 피의자가 주장하는 사실과 수사기관에서 추정하는 사실에 대해서 실험을 통해 누구의 말이 과학적으로 타당한지를 확인합니다. 그리고 두 주장과는 상관없이 수사 기록상 확인되는 여러 사실과 화재 역학에 비추어 사건 발생 당일 일어났을 것으로 추정되는 사실에 실험하게 됩니다.

그리고 만약, 피의자가 담뱃불에 의해 화재가 발생했다고 주장한다면 담배꽁초 한 개를 놓고 불이 나는지를 보는 것이 아닌 두 개, 세 개까지 두고 화재 발생 여부를 실험합니다. 이는 조건에 따라 화재 발생 여부가 달라질 수 있으므로 최대한 피의자에게 유리하게 실험을 진행하는 것입니다.

[앵커]

그러니깐 최대한 공정성을 기하려는 느낌이 있네요. 그렇다면 컴퓨터 시뮬레이션은 어떻게 이뤄지나요?

[인터뷰]

컴퓨터 시뮬레이션은 건축물 내 화염 확산 속도 분석 등 실물 재연실험이 어려운 사건에 대해서 실시합니다. 대학연구팀의 도움을 받아 실시하며 주로 FDS 프로그램을 이용합니다. FDS 프로그램은 미국국립표준기술연구소 NIST에서 개발한 화재해석 전용 프로그램입니다. 대학연구팀에 컴퓨터 시뮬레이션을 의뢰할 때는 객관적인 결과를 담보하기 위해 구획공간의 크기, 가연물, 점화원 등 시뮬레이션을 위한 필요 최소한의 정보만 제공합니다. 화재의 성상이 어떠했는지를 미리 알고 조건을 부여한다면 그 시뮬레이

션 결과는 신뢰하기 어렵기 때문입니다.

[앵커]

그동안 처리했던 사건 중 가장 기억에 남는 사건이 있다면 어떤 것인가요?

[인터뷰]

모 시사 프로그램에도 방영되었던 2011년에 발생했던 사건입니다. 동거녀와 돈 문제로 다투다가 동거녀와 그 딸이 있는 방 앞 복도에 휘발유를 뿌리고 방화하여 두 사람을 살해한 사건이 있었습니다. 1심 재판부는 공소사실을 모두 인정하여 징역 20년을 선고했습니다.

그런데 항소심에서 새로운 증거도 없고 달라진 사실관계도 없음에도 갑자기 피고인에게 무죄를 선고한 것입니다. 화재 발생 당시 피고인은 양쪽 다리와 팔, 얼굴에 일부 화상을 입었을 뿐인데 재판부는 마당에 있다가 화재 난 사실을 인지하고 피해자들을 구하다가 화상을 입었다는 피고인의 주장을 신빙성이 있다고 판단했는데요. 또한, 피고인에게 나타난 화상을 방화자의 화상으로 보기 어렵다고 본 것입니다.

[앵커]

그러면 어떤 실험을 통해서 결과를 밝혀내신 건가요?

[인터뷰]

네, 일단은 피고인이 주장하는 현장을 모델로 했습니다. 그리고 안에 뿌린 것으로 추정되는 휘발유 양의 절반을 뿌렸습니다. 그리고 마네킹을 현장에 통과시켰습니다. 실험결과 세트 내부는 약 1,000도를 넘었고요. 실험세트를 통과한 마네킹에 설치한 온도 계측기는 900도까지 상승했으며 불덩어리가 되었습니다. 즉, 피고인의 주장대로 피해자들을 구하기 위해서 화재현장을 통과했다면 피고인은 전신 3도 이상의 화상을 입어야 한다는 결론에 도달한 것입니다.

[앵커]

그러면 항소심에서 결과가 뒤집혔나요?

[인터뷰]

항소심에서 무죄가 선고됐고 이 사건은 이미 대법원으로 가있는 상태였습니다. 그래서 우리 팀은 화재역학에 따른 감정서를 제출했고 실험 결과로 2차 감정서를 제출한 것입니다. 그래서 대법원에서는 유죄취지의 파기환송을 했고 파기환송심에서는 팀 감정 결과와 법정증언을 주요이유로 설명하며 1심과 같은 징역 20년을 선고하였습니다.

[앵커]

얘기만 들어도 어렵지만, 보람도 있을 것 같은데 언제 가장 보람을 느끼시나요?

[인터뷰]

화재사건은 워낙 복잡, 다양하기 때문에 진실을 밝히는 것이 쉽지 않습니다. 목격자는 없고, 증거는 불

에 타고, 소화를 위해 뿌려진 물에 의해 현장이 훼손되기 때문입니다.

또한, 화재사건은 전기, 화학, 물리, 건축 심지어 법의학까지 관계되며 주변은 늘 위험이 도사리고 있습니다. 이런 과정 속에서 우리 팀에서 작성한 감정서가 진실을 밝히고, 진실을 밝힘으로써 억울한 사람을 풀어줄 수 있는 사건이 있을 때 가장 큰 보람을 느낍니다.

[앵커]

사실 많은 분들이 잘 모르고 있는 팀일 수도 있지만, 오늘 이 시간을 통해서 노고에 대해 많이 알아가셨으면 하는 바람이 생깁니다.

지금까지 대검찰청 화재수사팀 강정기 수사관과 함께했습니다. 고맙습니다.

“회삿돈 4억 원 증발”… 과학수사로 밝힌 ‘가짜 전표“

2019-02-24

회삿돈 수억 원을 빼돌려 집과 외제차를 사들인 회사원이 검찰에 붙잡혔습니다.

그런데 이 직원, 가짜 회계 전표로 회사 대표에게 누명까지 씌우려다가 과학 수사에 덜미가 잡혔습니다.

최주현 기자의 보도입니다.

[리포트]

사라진 회삿돈 4억 원을 찾아 나선 수사 검사는 계좌추적 끝에 집과 외제차까지 사들인 경리 직원 B씨를 용의자로 꼽았습니다.

하지만, B 씨는 대표 서명이 담긴 금전 출납 전표 60여 장을 내놓으며, 도리어 "범인은 회사 대표 A씨"라고 지목했습니다.

미궁에 빠질뻔한 상황, 대검 과학수사부의 문서감정이 진실을 밝혀냈습니다.

'가수금 577만여 원'이라고 적힌 문제의 전표에 가시광선보다 강한 빛을 쐈더니, 지워졌던 '상여금' 1천1백만여 원'이라는 글자가 드러난겁니다.

발행연도를 2017년에서 2015년으로 바꿔치기 한 사실도 탄로났습니다.

전표 69장 중 68장이 '가짜'였습니다.

연필 글씨를 지우고 전표를 위조했지만, 종이 사이에 배어 든 연필심 자국을 강한 빛으로 찾아낸 겁니다.

[박윤상 / 창원지검 마산지청 검사]

"법 과학 분석을 하지 못했다면 진실을 밝혀내지 못했을 겁니다."

검찰은 횡령 혐의에 사문서 위조 혐의를 추가해 B씨를 재판에 넘겼습니다.

세계 최고의 과학수사