법과 과학

2019년 4월호

과학수사의 중심

대검찰청 과학수사부

C O N T E N T S

방화 및 폭발조사의 선진기법 세미나 참석

법과학분석과 수사관 김일두

대검찰청 법과학분석과 화재수사팀 김일두 수사관은 2019년 3월 9일부터 3월 17일까지 미국화재조사관협회(NAFI ; National Association of Fire Investigators) 주관 '2019년도 방화 및 폭발조사의 선진기법 훈련 및 세미나'에 참석하기 위해 미국 워싱턴주 시애틀에 다녀왔습니다.

<화재 선진기법 훈련 및 세미나 개최 장소>

<NAFI 협회장과의 만남>

NAFI는 1961년에 창립된 미국 비영리단체로서 화재, 폭발, 방화, 소송(화재사건) 등에 관련된 일에 종사하는 회원들에게 화재조사 관련 기술을 개선하고 최신 기술과 더욱 수준 높은 지식을 제공하기 위해 설립되었습니다. 주로 국제 자동차 화재·폭발·방화 조사, 국제 화재·방화·폭발 조사, 화재 조사 심포지엄 등의 프로그램을 운영합니다.

회원은 화재조사관, 변호사, 소방관, 공무원, 보험회사 관계자, 손해사정인, 군인, 공학 기술자, 화학학자, 금속학자, 연구관, 기타 화재조사와 관련된 세계 60여 개 국의 업무종사자들로 구성되어 있습니다.

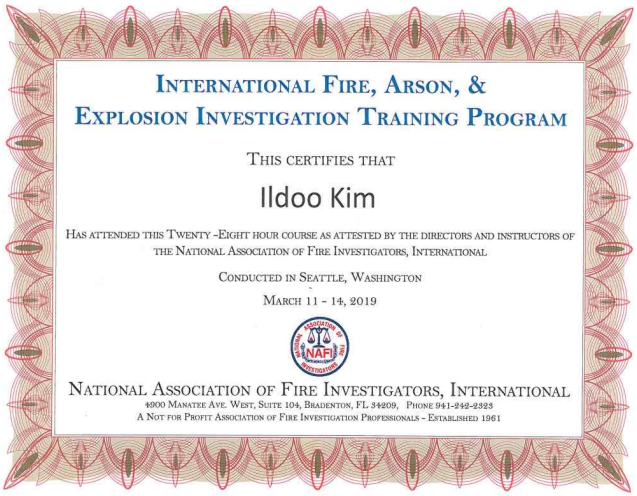
방화 및 폭발조사의 선진기법 훈련 및 세미나 일정에서 오리엔테이션, 화재현장에서의 사진촬영 기법, 화재패턴, 발화지점 및 발화원인 연구, 전기화재 연구, 폭발·방화 분석기법 연구 등에 대한 학습과 토론에 참석하고, CFEI(미국화재폭발조사관) 자격시험에 응시하는 등 다양한 일정에 적극적으로 참여하였습니다.

이번 화재 훈련 및 세미나는 화재사건에 대한 과학적인 이론과 접근 방법에 대한 체계적인 소개로 화재수사에 대한 지식을 쉽게 이해할 수 있게 하여 화재수사에 적극 활용할 수 있게 하는 좋은 계기가 되었습니다.

특히 Ronald Hopkins 교수(NAFI 협회장)와의 장시간 토론은 폭발 메커니즘에 대한 이해와 향후 실험 방향을 설정할 수 있는 지침이 되었고, 귀국 후 화재수사에 대한 연구 및 재연실험 방향 설정 시 많은 도움이 되었습니다.

또한, CFEI(Certified Fire & Explosion Investigator ; 미국화재폭발조사관) 자격 취득을 통해 대검찰청 화재수사팀에서 작성하는 감식보고서 등에 대한 신뢰성 및 신빙성을 높이는 발판을 마련하였습니다.

앞으로도 대검찰청 화재수사팀은 화재수사에 대한 고급 정보와 전문지식을 배울 수 있는 국제 화재 훈련 및 세미나에 참석할 수 있는 기회를 적극 활용하여 대검찰청 화재수사팀이 명실상부한 세계 최고의 화재수사 전문기관으로 자리매김 할 수 있도록 최선을 다하겠습니다.



INTERNATIONAL FIRE, ARSON, & EXPLOSION INVESTIGATION TRAINING PROGRAM

THIS CERTIFIES THAT

Ildoo Kim

HAS ATTENDED THIS TWENTY-EIGHT HOUR COURSE AS ATTESTED BY THE DIRECTORS AND INSTRUCTORS OF THE NATIONAL ASSOCIATION OF FIRE INVESTIGATORS, INTERNATIONAL

CONDUCTED IN SEATTLE, WASHINGTON

MARCH 11 - 14, 2019

NATIONAL ASSOCIATION OF FIRE INVESTIGATORS, INTERNATIONAL

4900 MANATEE AVE. WEST, SUITE 104, BRADENTON, FL 34209, PHONE 941-242-2323

A NOT FOR PROFIT ASSOCIATION OF FIRE INVESTIGATION PROFESSIONALS - ESTABLISHED 1961

<훈련 및 세미나 참석 수료증>

NATIONAL CERTIFICATION BOARD

THE UNDERSIGNED HAS BEEN EVALUATED AND FOUND TO MEET THE STANDARDS OF THE NATIONAL CERTIFICATION BOARD. THIS CERTIFICATION HAS BEEN DULY LISTED IN THE NATIONAL CERTIFICATION REGISTRY OF THE NATIONAL ASSOCIATION OF FIRE INVESTIGATORS, INTERNATIONAL

Ildoo Kim

Certified Fire and Explosion Investigator

Number: 24108-13760

Effective: 03/14/2019

THE NATIONAL ASSOCIATION OF FIRE INVESTIGATORS INTERNATIONAL IS A NON PROFIT ORGANIZATION INCORPORATED IN JUNE, 1961. ITS PRIMARY PURPOSES ARE TO INCREASE THE KNOWLEDGE AND IMPROVE THE SKILLS OF PERSON ENGAGED IN THE INVESTIGATION OF FIRES, EXPLOSIONS, ARSON, SUBROGATION, AND RELATED FIELDS, OR IN THE LITIGATION WHICH ENSUES FROM SUCH INVESTIGATION.

NATIONAL ASSOCIATION OF FIRE INVESTIGATORS, INTERNATIONAL

4900 MANATEE AVENUE WEST

SUITE 104

BRADENTON, FL 34209

<CFEI 자격증>

전국 청 대상 영상녹화 조사 설명회

법과학분석과 수사관 김재순

법과학분석과에서는 2019년 3월 18일부터 4월 18일까지 전국 28개 지검 및 차치지청을 방문하여 검사 및 수사부서 수사관을 대상으로 '영상녹화조사에 대한 이해와 활용방안'이라는 주제로 영상녹화조사 설명회를 진행하였습니다.

2004년 영상녹화제도가 도입된 이래로 2018년까지 약 300억 원의 예산을 투입하여 전국 검찰청에 영상녹화조사실을 꾸준히 확대 설치하고, 지속적인 활성화 방안을 수립하여 시행해 왔습니다.

그동안의 활성화 노력으로 상승추세를 보이던 영상녹화 실시율이 2017년 16.3%를 정점으로 2018년 11.4%, 2019년 1월 9.5%로 하락하였습니다. 이에 일선 청을 직접 방문하여 '영상녹화의 필요성 및 활용 기법'을 공유하여 장기적이고 실효성이 있는 영상녹화 활성화 계기를 마련하고 일선 청의 영상녹화에 대한 의견 및 건의사항을 청취하여 제도개선에 적극 반영하기 위해 설명회를 진행하게 되었습니다.

일부 청에는 조남관 과학수사부장님과 심우정 과학수사기획관님이 참석해 주셨고, 모두 말씀을 통해 설명회를 계기로 영상녹화 등 효율적인 조사 방식에 대해 공감해 주시기를 바라고, 영상녹화에 대한 의견이나 불편사항에 대해 건의를 수렴하여 제도개선 등에 적극 반영하겠다고 당부 말씀을 하면서 강의에 활력을 불어넣어주셨습니다.

설명회는 약 1시간 10분의 강의와 질의응답 순으로 진행이 되었고, 주무부서장인 이정환 법과학분석과장님이 강의를 직접 진행하였습니다.

영상녹화제도의 연혁을 시작으로 일선에서 영상녹화를 잘 하지 않는 이유, 조사는 왜 하는지, 조서는 왜 받는지, 조서가 가장 적합한 수단인지 등 근본적인 물음에 대한 의견을 제시하고, 일선 청에서 영상녹화를 잘 활용하지 않는 이유에 대한 분석 및 사례별 영상녹화 조사의 구체적인 활용 방법(예시)에 대한 설명을 하였습니다.

특히 조사의 기본은 듣기이며, 조서 작성으로 인해 듣기에 집중하지 못하는 점을 꼬집으면서 듣기의 가장 효율적인 방법은 영상녹화라는 점을 강조하였고, 강의에 참석하신 많은 분들이 조사의 기본은 듣기라는 부분에 대해 깊게 공감하였습니다.

일선 청 간부님들을 비롯하여 많은 분들이 참석을 해 주셨고, 강의가 끝나고 난 이후에는 공인인증서 로그인, 녹화물 CD제작 등 절차의 번거로움, 일체형 녹화실 설치 요청, 영상녹화 본증화의 필요성, 음성 텍스트 변환 기술 도입 요청, 신규 검사 및 수사관에 대한 교육 필요성 등 많은 의견을 제시해 주었습니다.

법과학분석과에서는 수렴된 의견을 바탕으로 일선 청에서 영상녹화를 편리하게 할 수 있도록 영상녹화시스템 개선 등 제도 개선을 위해 노력하겠습니다.

타깃형 디지털 및 사이버수사 검사교육 참석 후기

서울동부지검 검사 이승현

인터넷과 스마트폰이 우리 삶의 일부가 된 요즘, 범죄를 수사하고 공판에서 유죄 판결을 이끌어 내는 데 있어 디지털증거와 사이버 공간에 존재하는 각종 정보를 수집·분석하는 것은 사건의 경중을 떠나 당연하고도 필수적인 일이 되었습니다.

저는 이번 기회에 체계적이고 집중적인 배움의 시간을 갖기로 마음먹고, 2019. 4. 3.부터 4. 5.까지 3일간 대검 NDFC에서 실시된 제3기 디지털·사이버수사 실습과정에 참여하였습니다. 마침 대검 마당에 가득한 개나리꽃과 봄햇살은 따뜻한 미소로 저를 맞아 주었습니다.

첫째 날에는 가장 먼저 '디지털 압수수색의 쟁점 및 활용'이라는 주제로 디지털 증거의 종류 및 특징, 디지털증거 수집·분석 및 관리 절차 전반, 디지털 증거 압수수색 절차 및 유의사항을 개관한 강의를 들었습니다. 디지털 증거 수집을 위한 사전 정보 파악부터 압수 영장 등 증거 수집 방법, 분석 후 폐기에 이르기까지 전 과정과 주요 쟁점을 한 눈에 볼 수 있는 그림으로 가르쳐 주시니 명쾌하게 이해가 되었습니다. 그리고 이어서 '디지털 포렌식

이미징 기법', '모바일 포렌식 활용법' 및 'IDEAS 활용법'에 대해 차례로 배웠습니다.

둘째 날에는 '디지털 압수수색 과정에서 적법절차준수와 인권보호'라는 주제로, 선별 압수와 당사자 참여를 점점 강조하는 방향으로 발전해온 디지털 증거 관련 주요 판례 흐름에 대해 공부하고, 전날 배운 대로 다양한 사례를 통해 IDEAS를 이용하여 통화내역, 계좌내역을 분석해 보는 실습 시간을 가졌습니다. IDEAS 실습은 유익할 뿐 아니라 재미까지 더하여져, 참으로 알찬 커리큘럼이라고 생각하였습니다.

마지막 날에는 '사이버수사 활용실무'라는 주제로, 네트워크 분석, 악성코드 및 로그 분석, 빅데이터 분석, 이메일 분석, 가상화폐 분석 등 다양한 사이버수사 기법을 통해 성공적 수사를 이끌어낸 사례들을 배우고, 이와 관련하여 '사이버수사지원시스템 활용법' 및 '통신수사 활용 실무', '사이버수사 증거확보 및 분석 방법'에 대해 공부하였습니다. 사이버공간이라는 가상의 공간에서 이루어지는 정보의 이동을 화물의 이동에 비유해서 배우니 평소 헷갈렸던 기본 개념들을 세우는 데 큰 도움이 되었습니다.

이 날에는 조남관 과학수사부장님과 함께 대검 구내식당 아름채에서 맛있는 음식을 먹으며 즐거운 소통의 자리도 가졌습니다. 일선 청 검사들의 애로사항을 귀기울여 들어 주시고 용기를 북돋워 주신 부장님께 진심으로 감사하다는 말씀을 드리고 싶습니다.

이번 강의를 통해 끊임없이 발전하는 신종 기술과 이에 따른 신종 범죄에 대응하여 열정적으로 연구하고 고민하는 대검 과학수사부의 노력을 보았습니다. 스마트폰 수출, 반도체 생산, 컴퓨터 보급률 등을 비롯한 정보화 시설 세계 1위의 디지털 인프라를 구축했고 인터넷 인구 2,700만 명에 이르는 명실상부한 세계 최강의 IT강국인 우리 한국이 디지털·사이버수사 분야에서도 신속하고 효과적인 수사와 인권보호라는 두 가지 가치를 모두 조화롭게 구현해 냄으로써 세계 최고가 될 것이라는 확신이 들었습니다.

3일 간의 교육을 마치고 햇빛이 찬란한 대검을 나서면서, 색다른 뿌듯함과 보람을 느꼈습니다. 이 후기를 쓰면서 다시 한번 그 보람을 느낄 수 있었기에 행복하고 감사합니다.

제2회 전국 청 과학수사 화상회의 개최

과학수사기획관실 수사관 이정민

대검찰청 과학수사부는 지난 4월 11일 NDFC 6층 국제회의장에서 '제2회 전국 청 과학수사 화상회의'를 개최하였습니다. 전국 청 과학수사 화상회의는 현장 중심의 과학수사 지원, 일선과의 소통을 위해 분기마다 개최되는 회의로서 실제 수사과정에서 활용한 과학수사 기법에 대해 소개하고 실시간으로 전국 청 직원들과 수사기법을 교류하는 등 과학수사 활성화에 기여하고 있습니다.

조남관 과학수사부장은 회의 인사말에서 일선과 과학수사부의 소통창구인 '첨단·과학수사 커뮤니티' 활동 계획, 과학수사 활용 절차와 노하우를 한 눈에 보기 쉽도록 정리한 '알기 쉬운 과학수사 TIP' 발행 소식, 전국 청 상대 영상녹화 설명회 소식 등을 소개하며 과학수사부가 일선의 과학수사 역량을 키워나가는데 많은 노력을 기울이고 있으며, 일선에서도 과학수사에 많은 관심과 애정을 가져주기를 당부하셨습니다.

이번 회의에서는 총 4건의 과학수사 우수사례 발표가 있었습니다. 마산지청 박윤상 검사는 회사자금을 횡령한 직원이 전표를 조작한 사실을 문서감정으로 밝혀낸 사례를 발표하였고, 서울중앙지검 정혁 검사는 범행 도구에 대한 DNA재감정을 통해 계획 살인을 입증한 사례를, 서울중앙지검의 최성규 검사는 알코올중독에 의한 내인사로 암장될 우려가 있던 단순 변사 사건에 대해 피의자의 휴대전화를 확보·분석해서 폭행치사 사건의 실체를 밝힌 사례를, 서울동부지검 반지 검사는 네이버 광고담당자를 사칭하여 네이버 파워링크에 노출시켜주겠다고

속인 업체를 적발·구속한 사례를 발표해주었습니다.

순번	발표검사	사례개요
1	**박윤상** (마산지청)	·3년간 회사자금 약 4억 2천만 원을 횡령한 혐의로 불구속 송치된 **피의자가 범행을 부인하며 제출한 전표가 조작된 사실**을 **문서감정을 통해 밝혀내 추가 인지하여 직구속** 후 기소한 사례로 문서감정을 통해 실체적 진실을 밝혀냄
2	**정혁** (서울중앙)	·피의자는 피해자로부터 칼로 위협을 당하여 위 칼을 빼앗아 피해자를 찔렀다고 주장하며 살인의 고의를 부정하였으나, 대검에 **범행도구인 칼에 대해 재감정 의뢰**(경찰에서는 피의자, 피해자 DNA미검출)하여 칼 손잡이에서 피의자와 피의자 여자친구 DNA존재를 확인하여 **범행도구 출처를 규명하는 등 과학수사기법을 적극 활용**하여 사안의 실체를 밝힌 사례
3	**최성규** (서울중앙)	·알코올중독에 의한 내인사로 **암장될 우려가 있었던 단순변사사건에 대해 직접 검시**를 통해 **타살 정황을 확인**하고, 피의자의 집에 설치된 CCTV(스마트홈캠) 영상이 이미 삭제되어 복구 불가하였으나 이와 연결된 피의자 휴대전화를 분석하여 '피해자의 몸에 멍으로 보이는 자국 및 이불 위의 혈흔 사진, 울고 있는 피해자 사진' 등 **중요 증거**를 **확보하고, 이를 토대로 범행 자백을 이끌어 낸 사례**
4	**반지** (서울동부)	·영세사업자를 상대로 **네이버 광고담당자 등을 사칭**하여 네이버로 오인하게 한 다음 **정액요금 납부 시 네이버 파워링크에 노출시켜주겠다고 속여** 721개 업체로부터 합계 850,216,100원을 편취한 공동대표 2명을 구속기소하고, 임직원 5명을 불구속 기소한 사례

각 사례 발표 후에는 실시간 크라우드소싱 플랫폼을 활용해 전국 청 검사 · 수사관들이 사건별 수사시 착안사항 및 수사기법 등 다양한 질의 응답으로 열띤 분위기가 이어졌습니다. 특히, 정혁 검사는 범행 도구의 재감정을 통한 감정결과가 사건 해결의 결정적 계기가 되었고, 범행 도구 재감정을 하게 된 것은 이전 과학수사 화상회의에 참석 경험을 통해 착안한 것이라고 설명하여 과학수사 화상회의가 실제 수사 시 도움이 되고 있다는 사실에 담당자로서 더욱 뿌듯하고 보람이 느껴진 회의였습니다.

우수사례 발표가 모두 끝난 후에는 디엔에이·화학분석과에서 앞으로 있을 총선 등에 대비하여 선거법 위반·뇌물수수 관련 DNA감정 의뢰방법, 마약류 감정물 포장 개선 협조사항을 안내하였습니다.

앞으로도 대검찰청 과학수사부에서는 일선과의 소통을 통해 현장 중심의 과학수사 지원이 이루어질 수 있도록 최선을 다하겠습니다. 과학수사 화상회의는 7월에도 개최 예정이니 관심있는 직원들의 많은 참여를 바랍니다.

2019. SECON(세계 보안 엑스포) 출장후기

법과학분석과 수사관 박민우

지난 2019. 3. 7.(목) 법과학분석과 영상분석실(윤성빈 연구사, 박민우 수사관)에서는 한국인터넷진흥원, 한국전자통신연구원 등 33여개의 기관 및 단체가 포함된 산업통산자원부가 인증한 보안전문 국제 전시회인 "**SECON 2019 세계 보안 엑스포**"에 다녀왔습니다.

그림 1. 세계 보안 엑스포 전시회 전경

SECON이란 International Security Exhibition & Conference의 약자로 최신 IT 변화에 따른 보안기술과 트렌드를 한 자리에서 직접 경험하고 살펴볼 수 있는 **아시아 유일의 통합 보안전시회**로서, 올해에는 12개국 433개의 기업과 1,006개 부스가 참가한 가운데 지난 2019. 3. 6.(수)부터 2019. 3. 8.(금)까지 일산 KINTEX 제1전시장에서 개최되었습니다.

이번 SECON 2019에서는 최근 떠오르고 있는 인공지능, 빅데이터, 사물인터넷과 ICT 등 최신 IT 환경 변화에 따른 보안 트렌드 및 새롭게 출시되는 CCTV 및 블랙박스 등의 보안 관련 신제품과 최신 기술을 확인할 수 있었으며, 세부적으로는 '영상보안솔루션', '사회안전시스템 및 지능형 교통시스템', '출입통제솔루션', 'IT보안', '사물인터넷(IoT) 보안' 등의 주제로 구성되어 각 부스별로 최신 트렌드 기술을 적용한 많은 사례들을 만나볼 수 있었습니다.

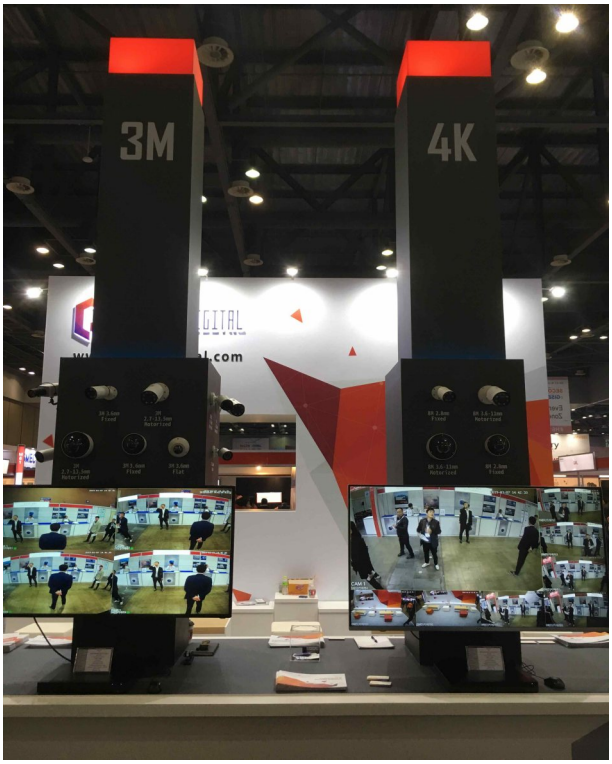


그림 2. 국내 영상보안솔루션 기술 업체 사례

첫 번째로, **국내·외 영상보안솔루션 기술 동향** 부분에서는, CCTV 등 영상 수집 장치로부터 입수되는 영상에서 사람, 차량 등 감시 대상물을 구분 및 인식하고, 이들의 패턴을 분석하여 감시목적(침입, 폭력, 화재, 연기, 배회, 투기, 도난 등)에 부합되는 이벤트가 발생될 때, 해당 정보를 즉각 감시자에게 전달하는 솔루션 기술 동향을 전시 하였습니다.

본 기술들에서는, 딥러닝 기법의 사용으로 높은 객체 인식률 보장, 탐지된 이벤트 객체의 크기 및 속도 분류, 현장 별 알맞은 민감도 설정 기능, 탐지 객체 속성 설정 기능(사람 / 차 / 속도 / 크기 등) 등 여러 기능들의 적용을 통해 영상보안솔루션 기술들의 성능을 극대화하였습니다.

그림 3. 지능형 교통 시스템 기술 업체 사례

두 번째로, **사회안전시스템 및 지능형 교통 시스템 기술 동향** 부분에서는, 대량의 녹화 영상에서 관심대상을 빠르게 찾아주고, 사람과 차량의 통행량 및 교통량을 실시간으로 계수하고 통계를 제공하는 기술 동향을 전시하였습니다.

본 기술들에서는, 사람 및 차량의 통행량 계수 기능, 차선 별 다중 계수 기능, 시간, 주간, 월 별 전체 통행량 통계 기능, 다수의 고정형 카메라와 한 개의 PTZ 카메라 조합에 의한 실시간 교통량 추적 기능, 인식한 객체를 자동 추적하는 기능 등 다수의 기술 적용을 통한 지능형 교통 및 사회안전 시스템 성능의 극대화를 이루었습니다.

이외에도, 출입통제솔루션, IT보안/정보보호, 사물인터넷(IoT) 보안, 홈시큐리티솔루션, 스마트 시티솔루션 등의 기타 보안 관련 장비 관람 및 기술 동향을 수집하였습니다.

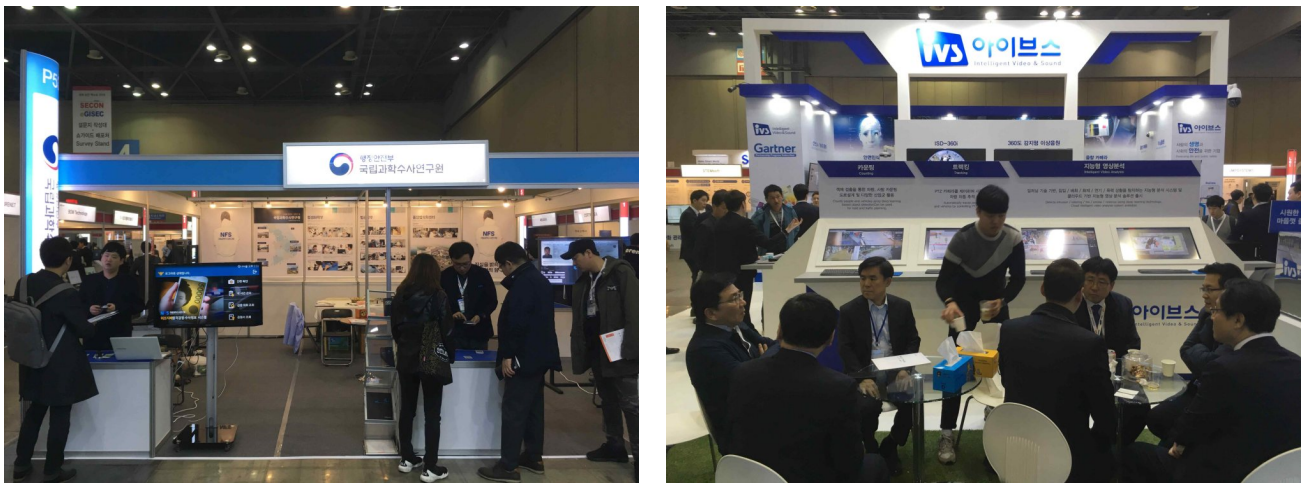


그림 4. 기타 IT보안/정보보호 및 지능형 영상분석 보안 솔루션 업체 사례

이번 전시회에서 제공된 기술들은 실제 현장에서의 사고 위험 감지 대상물을 인식하고, 이들의 패턴을 분석하여 해당 정보를 감시자에게 1차적으로 전달해주는 CCTV 카메라 등의 보안 기기들이 많이 전시되었습니다. 하지만, 실제 이들의 정보는 현장에서의 감시 목적으로 개발된 기기가 대다수였으며, 실제 영상분석을 위한 업무에 바로 적용하는 것은 현실적으로 많은 어려움이 있음을 깨달을 수 있었습니다. 이를 위해, 향후 영상분석 업무에 적용할 수 있는 연구 개발 가능성에 대하여 여러 학계 및 관련 연구소들과 지속적으로 의논하고 협의해 나갈 예정입니다.

끝으로, 이번 전시회를 통해 국내·외 영상보안솔루션 기술 동향 흐름의 파악 및 기타 보안 관련 장비 기술 동향 수집을 통한 관련 분야 인적 네트워크를 강화할 수 있었던 계기가 되어서 너무나 유익한 시간이었으며, 앞으로도 대검찰청 법과학분석과 영상분석실에서는 최신 기술 트렌드를 직접 확인할 수 있는 기회를 적극 활용하여 선제적 영상분석 기술 개발에 앞서 나갈 수 있도록 계속해서 노력하겠습니다.

CODEGATE 2019 참석

사이버수사과 수사관 최승진

스마트시티를 위한 블록체인과 보안기술의 발전을 한눈에 보다!

현재 세상은 랜섬웨어 해킹 공격, 암호화폐를 이용한 투자사기 및 자금세탁 등 새롭게 탄생한 신종 기술을 이용한 사이버범죄에 직면하고 있습니다. 나날이 발전하고 일상생활의 적용영역이 넓어지고 있는 정보통신기술이 모든 국민들에게 편리함을 제공하는 한편, 사이버 공격으로 인한 불편함을 동시에 제공하기도 합니다.

요즘 관심이 많은 블록체인 기술은 국회 및 기업체가 블록체인 산업 육성을 위한 법률안 발의 등을 통해 활발히 논의되고 있습니다. 여기서 가장 큰 또 하나의 걱정거리는 일상 생활로 파고든 신기술로 인한 민감한 개인정보 유출 등 '보안'이라 하겠습니다.

피할 수 없는 대세인 신기술 응용인 '창'은 보안이라는 믿음직한 '방패'가 없으면 단번에

허물어질 수 있습니다. 이들은 상호 보완적일 수 밖에 없습니다.

2019. 3. 27.(수) 서울 삼성동 코엑스몰에서 개최된 제12회 2019 코드게이트 행사는 신기술과 보안의 적절한 조화를 다루었습니다. 대검찰청은 과학수사부 조남관 검사장님과 이덕진 사이버수사과장님이 초청되어 개회식에 참석하였습니다.

이번 행사의 주제는 '스마트시티를 위한 블록체인과 보안'입니다. 곧 닥칠 미래의 모습인 스마트시티, 자율주행 자동차 등은 곧 현실화될 모델이고, 블록체인 또한 산업분야 곳곳에서 응용될 싱싱한 재료입니다. 이에 걸맞게 보안 이슈도 반드시 다뤄야할 주제일 것입니다.

코드게이트 주요 행사는 크게 두 가지로 나뉩니다. 첫째는 해킹방어대회이고, 둘째는 테크니컬 세션입니다. 테크니컬 세션은 보안과 블록체인 두 개 세션으로 나눠서 운영합니다.

해킹방어대회는 본선 진출한 3개 부문(일반, 대학생, 주니어) 50개 팀은 총 상금 6500만원을 두고 겨루는 대회로, 예선전에는 총 97개국 6,000여명이 참가하였습니다. 온라인 예선전에는 가상의 블록체인 시스템과 암호화폐 거래소를 해킹하는 문제가 출시되어 뜨거운 해킹 실력을 겨뤘습니다. 최종 일반부 우승은 지난해 우승팀인 한국의 '앙진모띠' 팀이 거머쥐었고, 2등과 간발의 차이로 문제를 풀어 승리하는 발군의 실력을 보여주었습니다.

테크니컬 세션 중 '보안'세션은 '디지털 ID사기 방지를 위한 차세대 보안' 등 신종 위협에 대한 대응방안을 논하였고, '블록체인'세션은 스마트시티 보안과 블록체인, 블록체인 타겟 공격에 대한 대응, 암호화폐 거래 추적 수사기법 등을 주제로 발표가 있었습니다.

주요 프로그램으로 블록체인 원리부터 암호화폐까지 한눈에 확인가능한 '블록체인 역사관', 암호화폐 거래소의 취약점을 찾는 '거래소 해킹 체험존', 스마트 계약 플랫폼의 취약점 유형과 공격방법을 소개하는 '스마트 컨트랙트 체험존', 다양한 스마트 기기의 해킹 사례와 직접 체험할 수 있는 'IoT 해킹 체험존' 등이 설치되어 방문객의 눈길을 끌었습니다.

대검 과학수사부장님은 여러 참석자분들과 IT체험관을 직접 둘러보시면서 최근 이슈에 대한 의견을 나누는 등 많은 관심을 보이셨습니다.

이번 코드게이트는 시대의 변화가 얼마나 빠른지 한눈에 알려주는 뜻깊은 행사였습니다.

특히 각 정부기관, 공공기관, IT기술을 선도하는 기업체들이 한 자리에 모여 정보를 교환하고 공감대를 형성할 수 있는 좋은 기회였습니다.

『알아두면 좋은 과학수사 상식』 ②

사이버 범죄 협약과 CLOUD ACT

대검찰청 검찰연구관 김영미

사이버 수사를 하다보면 해외 서버를 근거로 활동하는 범죄자 때문에 추적에 애를 먹기 쉽습니다. 범행도구를 애써 은닉할 필요 없이 사이버 공간에서는 클릭 하나로 중요한 증거자료를 삭제하기가 더 쉽습니다. 삭제하기 전에 증거를 확보해야 하는데 해외에 있는 데이터라면 정말 난감해지는 거죠. 정식으로 형사사법공조를 거치면 6개월에서 1년이 넘어가게 되니까요. 그 사이에 증거는 인멸되고 범죄자는 사라지게 될 것입니다.

정보통신업체들의 서버에 저장되는 전자정보가 급증하면서 이들 업체는 많은 데이터센터를 구축하고 있습니다. 그런데 마이크로소프트는 고객의 데이터를 전 세계 약 40개 이상 나라에 설치한 약 100개 이상 데이터센터를 통해 처리하고 있습니다. 구글은 이용자의 의사와 무관하게 데이터를 조각내어 전 세계 약 수십 개의 데이터센터 사이에서 정기적으로 이동시키기고 있습니다. 그 결과 확인해야 할 데이터가 어디에 있는지조차 파악하기 어려워지고 있는 것이 현 실정입니다. 사이버 범죄에서 관할의 의미를 전통적인 의미로 접근할

수 없는 이유입니다.

세계 각국은 이러한 사이버 범죄의 특수성에 대한 인식에 공감대를 형성하고 있는데요. 그렇다면 사이버 범죄에 있어서는 국경을 초월하여, 관할권에 구애받지 않고 증거가 사라지기 전에 보전 조치를 하고 접속로그나 가입정보 등을 파악하여 범죄자를 추적하는 방법에 대해 현재 어떠한 해결 방안이 마련되어 있을까요

우리 나라는 아직 가입되어 있지 않으나 사이버 범죄 협약이 대표적입니다. 사이버 범죄 협약은 '18. 10. 기준 미국, 영국, 독일, 프랑스, 일본 등 61개국이 가입되어 있어 러시아, 중국을 제외하고 주요국들 대다수가 가입된 국제 협약입니다. (OECD 총 36개국 중 우리나라와 뉴질랜드만이 가입을 하지 않고 있습니다)

1985년 유럽평의회(Council of Europe)는 '유럽형사문제위원회'를 구성하여 사이버 범죄와 관련된 논의를 시작하였습니다. 유럽평의회는 1997년 '사이버범죄전문가 회의'(The Committee of Expert on Crime in Cyberspace, PC-CY)를 설치하였고, 위 회의에서 사이버 범죄에 관한 국제협약 체결이 논의되어 2001년 11월 헝가리 부다페스트에서 유럽평의회 회원국 26개 회원국과 미국, 캐나나, 일본, 남아프리카공화국 등이 서명에 참가하여 2004년 7월 1일 발효되었습니다. 헝가리 부다페스트에서 서명되어, 일명 부다페스트 협약이라 불리게 되기도 하였습니다.

사이버 범죄 협약은 사이버범죄와 관련하여 가입국이 기본적으로 갖추어야 할 실체법 및 절차법을 규정하고 효율적인 국제협력 체계를 수립하는데 그 목적이 있습니다.

사이버범죄협약을 가입하게 되면 컴퓨터 데이터를 신속히 보존 조치할 수 있고, 트래픽 데이터의 경우 신속한 보전 및 일부 제공도 가능하며, 긴급한 경우 공조 방식을 간이화하여 신속하게 증거를 받아볼 수 있습니다. 트래픽 데이터란, 컴퓨터 시스템을 통한 통신과 관련하여 통신망의 일부를 구성하는 컴퓨터 시스템에 의해 생성되는 송수신처, 경로, 일시, 크기, 시간 또는 통신 서비스 유형을 나타내는 컴퓨터 데이터, 즉 통신 내용과 무관한 통신 자체와 관련된 자료를 말합니다.

협약 가입으로 인해 확보할 수 있는 이점을 나타내는 주요 조항은 다음과 같습니다.

제16조 저장된 컴퓨터 데이터의 신속한 보전

1. 컴퓨터 시스템을 통해 저장된 특정한 컴퓨터 데이터(트래픽 데이터 포함)

가 특별히 손실되거나 변경될 수 있다고 인정될 만한 특별한 사정이 있는 경우, 각 당사국은 자국의 권한 있는 기관이 이러한 컴퓨터 데이터를 신속히 보전할 수 있도록 명령하거나 이와 유사한 방법으로 확보할 수 있도록 필요한 입법 및 그 밖의 그 밖의 조치를 취해야 한다.

2. 전항과 관련하여 당사국이 어떤 자에게 그가 소유하거나 관리하고 있는 저장된 특정 컴퓨터 데이터를 보전하도록 명령하는 경우, 해당 당사국은 최대 90일까지 필요한 기간 동안 그가 해당 컴퓨터 데이터의 무결성을 유지한 채 보전하도록 하고 권한 있는 기관에게 제공할 수 있도록 필요한 입법 및 그 밖의 조치를 취해야 한다. 각 당사국은 그러한 명령이 연속하여 연장되게 규정할 수 있다.

3. 각 당사국은 국내법에 따라 규정된 기간 동안 컴퓨터 데이터를 보관 또는 보전하고 있는 자가 위 절차를 비밀리에 수행하도록 하는 데 필요한 입법 및 그 밖의 조치를 취해야 한다.

제17조 트래픽 데이터의 신속한 보전 및 일부 제공

1. 각 당사국은 제16조에 따라 보전되어야 할 트래픽 데이터와 관련하여, 각호의 사항을 위해 필요한 입법 및 그 밖의 조치를 취해야 한다.

가. 하나 또는 그 이상의 서비스 제공자가 해당 통신 중개에 관여하고 있는지 여부에 관계없이 트래픽 데이터의 신속한 보전이 가능하도록 보장, 그리고

나. 당사국이 해당 서비스 제공자와 통신 경로를 확인할 수 있는데 충분한 트래픽 데이터를 당사국의 권한 있는 기관이나 그 기관이 지명한 자에게 신속히 제공될 수 있도록 보장

2. 이 조에 규정된 권한과 절차는 제14조와 제15조의 규정에 따른다.

제29조 저장된 컴퓨터 데이터의 신속한 보전

1. 당사국은 컴퓨터 데이터의 수색 또는 유사한 방식의 접근, 압수 또는 유사한 방식의 확보, 제공을 위해 공조를 요청하고자 하는 경우, 다른 당사국

에게 그 영토 내에 있는 컴퓨터 시스템에 저장된 컴퓨터 데이터를 신속히 보전해 줄 것을 요청할 수 있다.

2. 제1항의 요청은 다음 각 호의 사항을 특정해야 한다.

가. 보전을 요청하는 기관

나. 수사 또는 형사절차의 대상인 범죄 및 관련 사실의 개요

다. 보전이 필요한 저장된 컴퓨터 데이터 및 범죄와의 관련성

라. 저장된 컴퓨터 데이터의 관리자 또는 컴퓨터 시스템의 위치를 특정할 수 있는 일체의 자료

마. 보전의 필요성

바. 당사국이 수색 또는 유사한 방식의 접근, 압수 또는 유사한 방식의 확보, 제공을 위해 공조를 요청하고자 한다는 취지

3. 요청을 받은 다른 당사국은 자국법에 따라 그 데이터의 신속한 보전을 위한 적절한 모든 조치를 취해야 한다. 공조 요청에 대해 회신을 할 경우, 쌍방가벌성이 그 보전을 이행하기 위한 요건으로 되어서는 아니 된다.

4. 제2조 내지 제11조에 규정된 범죄 이외의 범죄와 관련하여 컴퓨터 데이터의 수색 또는 유사한 방식의 접근, 압수 또는 유사한 방식의 확보, 제공을 위한 공조 요청에 대하여 그 회신 조건으로서 쌍방가벌성을 요구하는 당사국은 제공 당시 쌍방가벌성 요건이 충족될 수 없다고 믿을만한 이유가 있는 경우 제29조에 따른 보전 요청을 거절할 권리를 유보할 수 있다.

5. 또한 다음 각 호의 경우에 한해서 보전 요청을 거절할 수 있다.

가. 요청을 받은 당사국이 요청 대상 범죄가 정치범죄 또는 그와 관련된 범죄로 판단하는 경우, 또는

나. 요청을 받은 당사국이 주권, 안보, 공공질서 또는 다른 중요한 이익을 침해할 가능성이 있다고 판단하는 경우

6. 요청을 받은 당사국은 보전 조치로 인해 컴퓨터 데이터의 장래 효용성을 담보하지 못하거나 요청 당사국의 수사에 대한 기밀성을 위협 또는 기타 수사

상 장애가 발생할 것이라고 판단되는 경우, 그 사실을 요청 당사국에 즉시 통보하여 요청 당사국이 공조 요청을 계속할지 여부를 결정할 수 있도록 해야 한다.

7. 요청 당사국이 컴퓨터 데이터의 수색 또는 유사한 방식의 접근, 압수 또는 유사한 방식의 확보, 제공을 위해 공조를 요청할 수 있도록 제1항의 요청에 따른 일체의 보전은 최소 60일 동안 되어야 한다. 요청에 대한 결정이 있을 때까지 그 데이터는 계속 보전되어야 한다.

제30조 보전된 트래픽 데이터의 신속한 제공

1. 특정 통신과 관련된 트래픽 데이터를 보전하기 위해 제29조에 따른 요청을 처리하는 과정에서, 요청을 받은 당사국이 다른 국가의 서비스 제공자가 그 통신에 관련된 것이 발견된 경우, 요청을 받은 당사국은 그 서비스 제공자와 통신 경로를 확인하기 위해 충분한 트래픽 데이터를 요청 당사국에 신속히 제공해야 한다.

2. 제1항에 따른 트래픽 데이터의 제공은 다음 각 호의 사유에 한해 보류될 수 있다.

가. 요청을 받은 당사국이 요청 대상 범죄가 정치범죄 또는 그와 관련된 범죄로 판단하는 경우

나. 요청을 받은 당사국이 주권, 안보, 공공질서 또는 다른 중요한 이익을 침해할 가능성이 있다고 판단하는 경우

사이버범죄협약은 불법 접속, 불법 감청, 데이터 침해, 시스템 방해, 장치 남용, 컴퓨터 관련 위조, 컴퓨터 관련 사기, 아동음란물 관련 범죄, 저작권 및 인접권 관련 범죄에 대하여 적용됩니다.

사이버 범죄에 효율적으로 대처하기 위해서는 우리 나라도 하루 빨리 사이버 범죄 협약에 가입할 필요가 있습니다.

한편 미국에서는 연방 수사당국이 Microsoft에 마약 거래에 추정되는 이메일 정보를 요구하였으나, MS는 해당 정보가 미국 내가 아닌 아일랜드에 있는 서버에 저장되어 있기

때문에 SCA(Stored Communication Act)에 기반한 영장의 효력이 미치지 않는다고 다투는 사건이 발생하였습니다. 이 다투는 과정에서 2018. 3. 23. 시행된 연방법인 CLOUD(Clarifying Lawful Overseas Use of Data) Act는 미국 기업(U.S.-based technology companies)은 그 데이터가 해외에 있을 경우라도 영장(warrant)이나 제출명령(subpoena)에 의해 데이터 제공의무가 있다고 규정하여 분쟁을 입법적으로 해결하였습니다.

또한 미국과 행정협정을 체결하는 외국 정부의 경우, 미국 ISP(인터넷 서비스 업체)에게 전자정보를 직접 요청할 수 있는 이른바, 호혜성의 원칙이 적용됩니다. 우리 나라가 체결하게 된다면 우리 나라 수사기관이 미국 구글 등에게 전자 정보를 직접 요청하여 받아볼 수 있으나, 한편으로 미국 수사기관도 우리 나라 네이버에 직접 전자 정보 등을 요청하여 받아볼 수 있게 되는 것입니다. 다만 법원으로부터 발부받은 영장 등의 근거 서류가 필요한 것은 당연합니다.

미국 기업은 위 법률로 인하여 역외에 보유한 데이터를 제출하는 것에 대한 민사상 손해배상 등 책임에서 벗어날 수 있게 되었다고 하면서 법률 제정을 대부분 환영하였습니다. 즉 명확한 법률 제정이 클라우드 시장의 활성화에 기여할 수 있다는 시사점도 있다할 것입니다.

우리 나라도 빠르게 변화하는 사이버 수사의 흐름에 발맞출 필요가 있다할 것입니다. 관련 법률을 정비하고 국제 협약 등에 적극적 가입을 검토해야 합니다.

『세계의 법과학 기관』 ②

미국 FBI Laboratory Division

법과학연구소장 이승환

세계에서 가장 권위있는 법과학 기관을 한 손에 꼽자면 늘 들어가는 기관은 미 연방수사국의 Laboratory Division(Lab. Div.) 일 것입니다. 워싱턴 남쪽으로 100km 이내에 위치한 콴티코라는 미 해병기지 구역 내에 위치하는 이 기관은 연면적 16,000 여평에 이르는 규모로 3개의 빌딩이 연이어 붙어 있는 형태로 되어 있습니다. FBI 연수원(Academy)도 인근에 있는 이 곳은 가끔 부대 에서 훈련 중 발생하는 포탄 소리를 제외하면 적막하리만치 조용하고 사방을 둘러봐도 잔디와 나무 밖에 보이지 않는 곳입니다. 매우 다양한 법과학 분야의 감정 및 연구가 이 안에서 이루어지고 있지만 홈페이지나 어딜 찾아봐도 기관의 특성인지 정확한 인원 규모와 조직도는 찾을 수가 없습니다. 2010년 이전에 찾아갔을 때 감정이나 연구에 전념하는 정규직 종사자(기술 테크니션을 제외한)가 500여명 이란 말을 들었으니 지금은 늘어나 있겠지요. 정규직은 과학전문가와 특별수사관(special agent)의 두 직제로 이루어져 있다고 합니다. 다루고 있는 법과학 분야는 현장수사인 CSI를 포함해 전 분야를 망라하고 있다고 해도 좋을 만큼 다양하지만 언어번역 서비스, 폴리그래프,

디지털포렌식, 오디오 및 영상분석은 FBI 내 다른 관련 부서로 흩어져 있습니다.

세계 최고의 시설을 자랑하는 이 건물도 처음부터 있었던 것은 아니고 어느 기관이나 그렇듯 FBI 법과학부서도 영욕의 역사를 거쳐 오늘에 이르렀습니다. FBI의 법과학 실험실은 1934년, 아주 작은 규모로 워싱턴 시내의 법무부 건물에서 시작되었습니다. 그러다 1974년 FBI가 독립 빌딩으로 이전하면서 Lab. Div.도 이곳으로 옮겨오며 연구 시설인 FSRTC만 콴티코로 이주를 하였습니다. 그러다가 2004년에야 지금의 건물이 완공되어 현재의 모습을 갖추기 시작했는데 여기에는 재미있는(?) 사연이 있습니다. 1992년쯤 책임자급 특별수사관으로 근무하던 Whitehurst 박사라는 사람이 FBI의 법과학 서비스는 오류 투성이라고 폭로를 해버린 것입니다. 그 원인은 전문가라고는 하지만 많은 사람이 FBI의 특별수사관 직함을 가지고 있는 상황에서 중립적인 감정이 나올 리 없고 물적 투자도 열악하여 신뢰성 있는 결과를 기대하기 어렵다고 입장을 밝혔습니다. 당시는 뛰어난 정확성으로 스포트라이트를 받던 DNA감정에 의해 기존에 행해지던 모발이나 섬유의 형태분석, 치흔, 공구흔 등의 흔적 분석 증거의 오류 사례가 속속 밝혀지던 시기였습니다. FBI가 쉬쉬하고 있는 동안 그는 오류 사례들을 폭로해버렸습니다.

전화위복이라고 할까요? 이때부터 미FBI는 Lab. Div.의 발전에 많은 관심과 투자를 기울이고 일련의 변혁 작업을 시작했는데 여기에는 특별수사관의 비율을 점차 줄이는 일, 새로운 시설로의 이전, FBI 법과학 서비스의 전 분야 ISO 인정(accreditation) 등이 포함되어 있었고 이런 정책에 힘입어 오늘의 건물이 들어서게 된 것입니다.

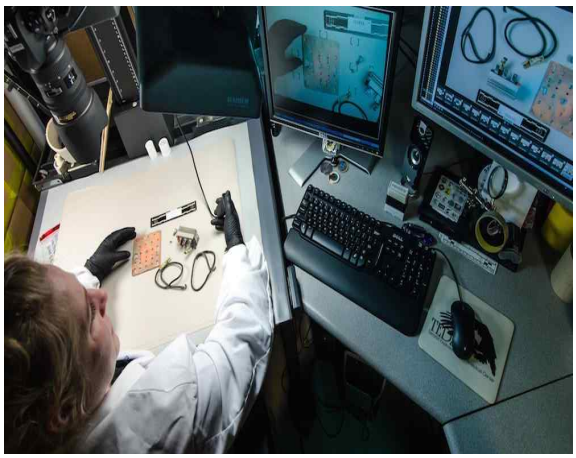
1992년 당시 저는 방문과학자(visiting scientist)로 콴티코에 있는 연구시설인 FSRTC에서 우리나라에 FBI의 DNA감정 기술을 도입하기 위해 연구 중이었는데 동료 중 하나가 이런 문제가 현재 FBI에서 터졌다는 말을 들은 적이 있습니다. 그저 모든 분야가 세계 최고일 것이라 생각했던 저에게는 상당히 충격적으로 들렸던 기억이 있습니다.

Lab. Div.이 이전하는 시점인 2004년에 FBI는 법과학에서 또 한 번의 치욕적인 역사를 맞습니다. 스페인에서 많은 인명을 살상한 열차 폭발사고가 났는데 당시 9.11의 악몽에서 벗어나지 못한 FBI 감정관들은 잘못된 지문 감정으로 엉뚱한 이슬람계 사람을 범인으로 지목했던 것입니다. 세계적인 뉴스가 되어버린 이 사건으로 FBI Lab. Div.의 자긍심은 또 한번 상처를 입게 되었고 이로 인해 미국 내 법과학 전체의 문제를 돌아보도록 미 의회가 제안하는 계기가 되었습니다. 그 결과 미국의 법과학에 대한 개선 프로젝트는 아직도

진행 중입니다.

2010년 이전에 FBI Lab.Div.은 10여개가 넘는 법과학 분야에서 각 기관 실무대표로 구성된 기술협의체(scientific working group)의 주축으로서 활동을 해왔지만 현재 이 기능은 표준기술원(NIST)으로 넘어가 있는 상태입니다. FBI가 세계 최고 수준의 법과학 기술을 구가하고 있으면서도 정확성에 대한 논란과 회의는 지금도 계속되고 있고 이것은 법과학에 종사하는 우리도 늘 염두에 두어야하는 점이라는 것은 분명합니다.

필요는 투자를 낳습니다. FBI Lab.Div.에 속해 있으면서도 자랑하고 있는 별도의 특별 건물이 있는데 TEDAC(Terrorist Explosive Device Analysis Center)이라 명명한 사제



폭발물 센터입니다. 이 기관은 FBI를 필두로 국방부, 국토안보부, 마약국 등 관련 기관 종사자들이 합쳐 테러 및 폭발물 정보에 대응하는 곳입니다. 9.11에 놀란 미국 정부가 많은 예산을 투입해 지은 건물로 Lab. Div.이 이전하기도 전인 2003년에 콴티코에 완공이 되었습니다. 현재는 유럽 각국도 테러에 대비한 별도의 부서를 법과학 기관 내에 많이 두고 있는데 각국의 벤치마킹 대상이 되어 있고 관련 정보교환의 중심이 되어 있다고 합니다.

1992년에 DNA기술 공동연구를 위해 3개월 동안 FBI의 감정관들과 지낸 적이 있습니다. 이들이 자신의 직장에 대해 가지는 자부심은 정말로 대단한 것이었습니다. 또한 모든 기술 노하우나 정보 교환에 매우 개방적이고 적극적이어서 선두에 있는 기관의 여유가 느껴지기도 했습니다. 많은 굴곡이 있었지만 FBI Lab.Div.이 미국 내 400여개나 되는 법과학 기관을 리드하는 중심에 있으며 세계를 선도하는 역할의 일부를 담당하고 있다는 것은 분명하다고 할 것입니다.

폭행치사인가 폭행죄인가?

서울대학교 법의학 교수 유성호

사례 1.

일요일 저녁 근무를 마친 후 노동의 고단함을 술을 마시며 달래고 있었다. 그날은 회사 대청소가 있던 날로 청소를 끝내고 회사에서 제공한 삼겹살을 안주로 몇 되지 않는 근로자들이 모여 독주인 이과두주와 막걸리로 술잔을 기울이고 있었다. 평소 주간조와 야간조로 나뉘어 일을 하던 터에 별로 교류가 많지 않았던 이들이 모처럼 한자리에 모였다. 술잔이 돌고 취기가 오르자 시시껄렁한 농담과 고성이 오고 갔다.

야간조에서 작업지시 등을 맡고 있던 조선족 장 씨(46세)는 중국에 있는 빚을 갚으려 이 공장에 취업해 일을 하고 있었다. 술자리에서 갑자기 장 씨가 사람들에게 다음날의 업무를 지시했다. 고압적인 장 씨의 태도가 김 씨(60세)의 눈에 거슬렸다. 김 씨는 주간조에 속해 있었기 때문에 평소 장 씨와 교류가 잦지는 않았다.

"야, 너는 나보다 나이도 어린데 어디 나이 많은 사람에게 지시를 할 수 있냐?"

얼큰히 술에 취한 김 씨가 장 씨에게 언짢은 듯 말했다. 이어서 "내가 아직까지 너보다 힘이 세다"라고 말하며 장 씨의 왼손을 있는 힘껏 쥐었다. 화가 난 장 씨가 얼굴색 하나 바꾸지 않고 자신의 손을 쥐고 있는 김 씨의 손을 꽉 잡고는 "내가 더 세다"라고 말하며 뿌리쳤다.

잠시 적막이 감도나 싶더니 말릴 틈도 없이 싸움이 시작되었다. 김 씨가 분한 얼굴로 계속해서 장 씨에게 달려들었지만 계란으로 바위 치는 격이었다. 압도적 힘의 차이가 분명히 느껴졌다. 주먹이 오가는 것처럼 보였지만 사실상 김 씨가 장 씨에게 일방적으로 맞고 있는 상황이었다. 술자리에 있던 나머지 사람들이 하나 둘 자리를 떴다.

이미 장 씨에게 얼굴을 10여대 이상 맞은 김 씨는 씩씩거리며 장 씨의 기숙사 방까지 따라오며 계속해서 싸움을 걸었다. 방에서 나가라는 장 씨의 말에 김 씨는 장 씨의 침대 위에 누워버렸다. 질린 얼굴을 한 장 씨가 김 씨를 둔 채 김 씨의 기숙사 방으로 들어갔다.

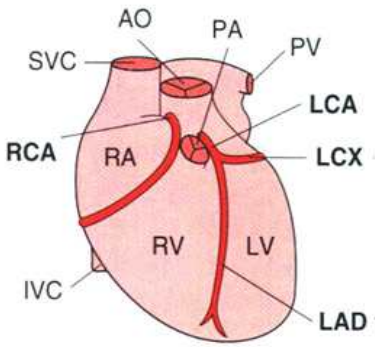
저녁 무렵 마신 술 때문에 목이 타고 화장실에 가고 싶어진 장 씨가 눈을 떴다. 낯선 느낌이 드는 방이었다. 복도를 지나 화장실을 다녀온 장 씨가 자신의 방에 들어가니 침대 위에 김 씨가 누워있었다. 어제 밤의 일들이 빠르게 스쳐갔다. 자신의 방까지 따라와 드러누운 김 씨에게 욕을 퍼붓고는 자신이 김 씨의 방에 가서 잤던 것이었다. 자신의 침대에 누워있는 김 씨를 보니 울컥 짜증이 났다. 끈질긴 영감 같으니라고. 작게 혀를 차며 김 씨를 흔들어 깨웠다. 김 씨의 몸에 손을 대자 정신이 번쩍 드는 기분이었다.

방에 불을 켜고 사람들을 깨운 뒤 119를 불렀다. 이미 김 씨가 사망한 후였다.

맞아서 퉁퉁 부은 김 씨의 시신을 보면 폭행으로 인한 사망처럼 보였다. 하지만 피의자 신문에서 장 씨는 '자신과 싸우다 넘어져서 죽은 것 같다', '술을 마시고 가다가 정신을 못 차리고 스스로 벽에 부딪혀 죽은 것 같다'는 이야기를 하며 자신의 폭행으로 김 씨가 죽은 것이 아님을 강하게 주장하였다.

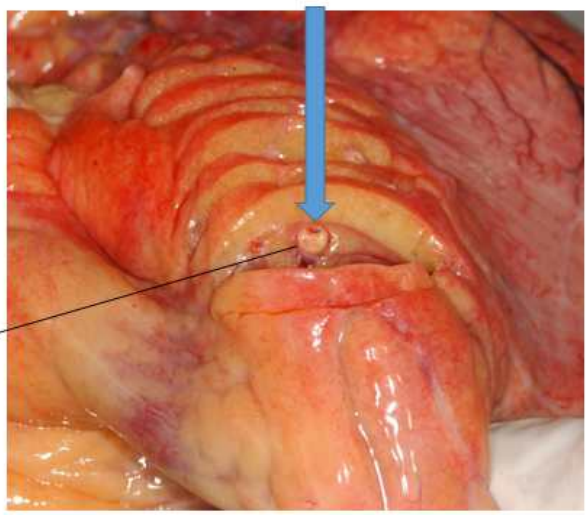
이틀 후 김 씨의 부검결과가 나왔다. 관상동맥 3개의 주된 분지에서 40~60%정도의 폐색이 동반된 중등도의 죽상 동맥경화가 나타났다는 점, 갑상연골의 골절이나 전경부 외표의 액흔이 없다는 점에서 경부압박질식사가 아님이 밝혀졌다. 또한 여러 부위의 출혈이 인정되나 사인으로 보기에는 미흡하다는 점, 사인으로 판단할 만한 다른 질병이나 손상이 없다는 점, 알코올 농도가 0.269%의 고도 명정상태로 특기할 약독물이 검출되지 않았다는 점 등을 종합하여 볼 때 김 씨는 '허혈성 심장질환'과 관련한 사망이라는 결론이었다.

심장의 앞쪽 모습



RCA: 오른쪽 심장동맥(관상동맥)
LAD: 왼쪽 심장동맥 앞내림가지
LCX: 왼쪽 심장동맥 휘돌이 가지

실제 심장동맥 경화 소견



담당 검사는 이러한 부검 소견과 사망원인의 인과관계를 보다 확실하게 하기 위해 서울대학교 법의학교실에 자문을 의뢰했다. 자문 결과 얼굴의 피하출혈과 이마 및 관자 부위의 출혈이 심장동맥의 경화로 인한 심장동맥병인 허혈성 심장질환[1]의 직접 발병원인이 될 수는 없는 것이었다. 다만, 허혈성 심장질환은 외인으로 유발될 수 있는 질병이고, 장 씨의 폭행과 김 씨의 사망이 시간적으로 밀접하므로 장 씨의 폭행이 기왕증인 관상동맥 경화증에 악영향을 끼쳐 허혈성 심장질환으로 발증 하였을 가능성을 배제하기는 곤란했다. 즉, 폭행과 사망의 인과관계는 인정될 수 있었다. 그러나 관상동맥경화증의 특성상 장 씨가 김 씨의 지병을 알고 있었다고 보기 어렵고, 몸싸움을 할 당시에도 얼굴을 수회 때린 것으로 사망을 예견할 수 있었다고 보기는 어렵다는 취지에서 폭행치사 부분을 불기소 하고 폭행죄로 기소하게 되었다.

본 사건의 경우 피해자에게도 범행의 발생 및 피해 확대에 상당한 책임이 있다는 점 등이 고려되어 징역 4월에 집행유예 1년의 형이 선고되었다.

사례 2.

여름 낮 시골 마을 회관에서는 동네사람들이 모여 화투판을 벌이고 있었다. 화투를 치러 간 남편이 돌아오지 않자 A는 직접 남편을 찾으러 회관으로 갔다. 부인에게 대충 말을 둘러대며 손에서 화투장을 놓지 않는 윤 씨의 옆에는 거하게 술을 마신 서 씨가 앉아 있었다. 남편에게 잔소리를 하는 A를 향해 서 씨가 욕을 퍼붓기 시작했다. 사람들 앞에서 입에 담기 힘든 욕설을 듣고 A의 얼굴이 벌겋게 달아올랐다. A의 손가락질을 피하려던 서 씨가 엉덩방아를 찧으며 넘어졌다. 뒤에 놓여있던 선풍기를 깔고 앉으며 넘어지자 선풍기가 찌그러지고 말았다. 주위의 분위기가 냉랭하게 식었다. 화투를 칠만한 분위기가 아니었다. 자신 때문에 선풍기가 찌그러졌으니 집에 있는 선풍기를 가져다 놓겠다며 A가 마을회관을 벗어났다. 윤 씨가 A를 따라갈 생각으로 급히 일어서 허둥지둥 슬리퍼를 신었다. 넘어졌다 일어난 서 씨가 윤 씨의 뒤를 따르며 계속해서 A를 욕했다.

---

1) 허혈심장질환(한국표준질병·사인 분류표에서 I20~I25)이란 심장동맥이 좁아지거나 막히게 되어 심장근육에 충분한 혈액 공급이 이루어지지 못할 때 나타나는 병으로 임상적으로는 협심증, 급성심근경색, 후속심근경색(subsequent myocaridal infarction)과 그의 합병증 및 급사 등의 형태로 나타난다. 쉽게 생각하면, 심장 스스로에게 산소와 영양분을 공급하는 심장동맥(관상동맥이라고도 한다)이 동맥경화에 의해 좁아진 상태를 허혈성 심장질환이라고 부른다. 이것을 흔히 심장동맥병이라고도 일컫는다.

사람들이 질린 표정을 하고 있었지만 서 씨의 이러한 술버릇은 이미 동네에서 유명했다. 윤 씨가 참는데도 한계가 있었다. 화가 머리끝까지 치민 윤씨는 "왜 남의 식구에게 욕을 하냐"고 하며 서 씨의 어깨를 확 밀었다.

술에 취해 휘청거리던 서씨가 '꽁' 하는 둔탁한 소리를 내며 뒤로 넘어졌다. 놀란 윤 씨의 눈이 커졌다. 방에 완전히 드러누운 서씨는 5분 정도 그대로 누워 있었다. 버럭 화를 내며 자신의 분을 이기지 못한 듯 신발을 신고 나와 마을회관 앞에 있는 컨테이너로 향했다. 서 씨는 왼손으로 기둥모서리를 잡고 오른손으로 컨테이너를 짚은 후 스스로 쿵쿵 소리가 날 정도로 머리를 부딪혔다. 서 씨의 앞이마 부근에 피가 흘렀다.

다음날 서 씨가 병원에 입원했다는 소식이 들렸다.

입원 후 몇 차례 수술을 거쳤지만 서 씨의 상태는 점점 나빠져 갔다. 서 씨가 입원해 있는 동안 윤 씨는 병원비 명목으로 600만 원 정도를 건넸다. 수술이 거듭될수록 병원비는 눈덩이처럼 불어갔다. 그렇게 6개월이 지난 후 서 씨가 사망했다는 소식이 들렸다.

서 씨의 사망진단서에 적힌 직접사인은 간경화에 의한 '다발성 장기부전'이었다. 이대로라면 윤 씨의 책임은 폭행에 한정되는 것이었다. 하지만 법의학자의 소견은 달랐다.

서울대학교 법의학교실에 의뢰한 자문에서는 피해자의 원사인[2]을 두부손상(아주 심한 양측 전두부와 측두극에 뇌좌상과 경막하 출혈)으로 제시하였다. 뇌사에 빠진 상태에서 병원에 오래 있다 보면 결국 몸이 점점 약해져 패혈증이나 다발성 장기부전으로 사망하게 되는 것이 보통이며, 이 경우에는 뇌손상에 의해 사망한 것으로 보는 것이 바람직하다는 의견을 받았다. 즉, 서 씨의 사망원인을 간경화가 아닌 뇌출혈에 의한 것으로 본 것이다. 다만 서 씨의 경우 후두부의 손상보다는 전두부의 손상이 주요원인이었다.

하지만 윤 씨는 서 씨의 어깨를 밀었고 서 씨는 뒤로 넘어졌었다. 오히려 이마 쪽의 충격은 서 씨가 컨테이너에 자해한 부분에 의해 생겼을 가능성이 커보였다. 단순히 표면적 사실과 상처만 보았을 때 전두부의 손상이 윤 씨에 의한 것이라 하기는 어려웠다.

하지만 법의학의 세계에서 뒤로 넘어진 것에 의해 전두부가 손상되는 현상은 그리 새롭거나 이상한 일이 아니었다. 이미 수 세기 전부터 머리를 가격하면 가격 부위에 뇌좌상이

2) 원사인(原死因; Underlying COD)은 (a) 직접 사망에 이르게 한 일련의 사건을 일으킨 질병이나 손상 또는 (b) 치명적 손상을 일으킨 사고나 폭력의 상황으로 정의한다.

생기고 넘어져 머리를 땅에 부딪히면 충격부위의 반대쪽에 좌상이 생긴다는 사실이 널리 알려져 왔다. 비유적으로 말하면 뒤로 넘어져도 코가 깨질 수 있는 것이었다.

결국 이 사건은 대측충격손(countre-cou injury)[3]에 의한 양측 전두부와 측두극에 뇌좌상과 경막하 출혈이 주요사인이었다. 이로써 윤 씨의 폭행과 서 씨의 사망사이에는 인과관계가 인정되었고 폭행치사로 기소되어 징역 1년 6월에 집행유예 3년의 선고를 받게 되었다.

3) 머리에 가해진 충격에 의하여 뇌 조직과 두개골이 부딪쳐 생기는 손상은 충격 부위에 생기는 것과 그 반대쪽에 생기는 것이 법의학적으로 외상의 상황을 아는 데 매우 중요하다. 뇌좌상의 기전에 대하여 이미 수 세기 전부터 머리에 가격하면 가격 부위에 뇌좌상이 생기고, 넘어져 머리를 땅에 부딪치면 충격 부위에는 손상이 없고 그 반대쪽에 좌상이 생긴다는 사실이 알려졌다. 후자의 가장 좋은 예가 뒤로 넘어졌을 때 심한 좌상이 전두엽과 측두엽의 끝에 생기는 것이다. 가격한 부위에 뇌좌상이 생기는 것(충격 좌상, coup contusion)은 비교적 쉽게 설명할 수 있으나, 반대쪽에 생기는 대측충격좌상(counter-coup contusion)은 쉽게 설명하기 어려우나(약 6개의 설명 이론이 있음), 실제 자주 발생하는 손상이다. 2017년 문제가 되었던 백남기 농민 사건에서도 대측충격손상에 의해 뇌의 경막하출혈과 뇌의 앞쪽 전두엽과 측두엽 끝에 뇌좌상이 발생하였다.

『영화로 본 수사관 일기』 ⑭ <인생은 아름다워>
- 아이의 언어를 이해한다는 것은 얼마나 어려운 일인가

서울남부지검 수사관 강현식

여러분은 아이들에게 '검찰'을 어떻게 설명하고 계신가요? 저도 처음에 "아빠 직업은 경찰이야?"라는 아이의 질문을 받고 대답도 하지 않은 채 우물쭈물 했었습니다. 경찰은 쉽게 설명할 수 있을 것 같은데, 경찰과 검찰이 어떻게 다른지, 검찰이 하는 일은 뭔지에 대해서 솔직히 말해서 마땅히 설명할 말이 떠오르지 않았거든요.

"검찰은 경찰에 수사지휘를 하며, 공소유지 역할을 할 뿐만 아니라 필요한 경우 인지수사를 하기도 한다"는 말을 아이가 쉽게 이해할만한 용어로 순화할 말이 얼른 생각나지 않았기에 그냥 "경찰관 아저씨가 도둑을 잡으면 그 도둑을 혼내줘야 할지, 실수로 물건을 훔친 불쌍한 사람인지 확인하는 사람이 검찰이야"라고 말해버렸습니다. 억지로 아이에게 아빠의 직업에 대하여 이해하도록 강제하는 것보다는 그 방법이 나을 것 같아서였습니다. 조금 더 시간이 지나면 아이도 검찰이 어떤 일을 하는지 이해하게 되길 바라면서요.

이탈리아 배우 로베르토 베니니가 연출한 영화 <인생은 아름다워>를 개봉관에서 보았던 게

1999년이었으니까 벌써 20년이 다 되어갑니다. 당시에는 결혼도 하기 전인 대학생 신분이었으니 아이를 둔 아버지의 심정이 어떠할지 가늠조차 하지 못하였는데, 얼마 전 재개봉한 영화를 다시 보니 새삼 느껴지는 바가 있었습니다. 그 때 느끼지 못했던 감정의 결이 나이를 먹으니 달라진 탓일까요.

영화 속 주인공 귀도는 그림같은 연애를 마치고 아내, 아들과 행복한 나날을 보내던 중 가족 모두가 나치 수용소에 강제로 끌려가게 됩니다. 자유를 박탈당했다는 사실에 대하여 비관하고 있을 새도 없이 아들에게 그런 현실을 알려주어야 하는 가장 '귀도'. 그는 처형당하는 순간까지도 아들에게 인생은 아름다운 것이라는 사실만 알려주려는 듯 마치 행진하듯이 처형장으로 걸어갑니다. "아들아, 아무리 현실이 힘들어도 인생은 아름다운 거란다"라는 말을 남긴 채 말이죠.

영화를 보는 순간 검찰이라는 직업을 이해시키려고 애썼던 순간들이 부끄럽기 시작했습니다. 아이는 검찰이 뭘 하는 직업인지 궁금했던 것이 아니라, 검찰이라는 직업을 가진 아빠가 어떤 일을 하는지 궁금했던 것이라는 사실을 너무 늦게 알아챘기 때문이지요. 때로는 아이의 언어를 이해한다는 것이 얼마나 어려운지를, 벌써 어른이 되어 하루하루 매너리즘에 괴로워하는 연배가 된 지금에 와서야 깨닫게 됩니다. 그냥 "나쁜 사람을 벌주는 직업이야"라는 말보다 아직 세상은 얼마나 아름다운지 알려주는 게 더 시급할 수도 있음을 오늘 저는 영화 <인생은 아름다워>에서 다시 배워갑니다.

과학수사 대학(원)생 아이디어 공모전 입상작 소개 ④

- 우수상 고려대학교 한승현 -

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 우수상 수상작을 소개합니다.

○ 제출자 : 고려대학교 한승현

○ 제목 : 빅데이터 기반 유사범죄 해결방안에 대한 경우의 수 제시 및 추론

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	빅데이터 기반 유사범죄 해결방안에 대한 경우의 수 제시 및 추론
제안 배경	4차 산업혁명은 과거 '정보화'가 차지했던 영역을 인공지능(AI) 기반의 '지능화'로 업그레이드하는 것이다. 즉, 4차 산업혁명의 성공여부는 인공지능 수준과 직결된다고 볼 수 있다. 여기서 AI와 빅데이터를 과학수사 중 디지털 수사에 접목시키면 어떨까? 하는 생각을 해보았다. 검찰의 수사기록들을 빅테이터로 가정한다면 수사기록 기반 AI는 시간적 소요가 많이 되는 복잡한 수사과정을 효율적으로 단축시킬 수 있으며 보다 객관적인 판단이 될 수 있을 것이라 생각하였다.
주요 내용	검찰 수사기록 빅데이터 기반 AI가 있다고 가정한다면, 사건이 발생하자마자 유사범죄들에 대한 정보를 추출하고, 이를 분석하여 사건의 해결방안과 관련된 경우의 수를 제시할 수 있을 것이다. 또한, 어떤 방향으로 우선적으로 수사를 진행할지에 대해 예측이 가능할 것이며, 이를 통해 더욱 정교한 추론이 가능하다는 것이 제안의 핵심이다. 제안 이전에 빅데이터에 대한 정의, 특성 그리고 수사기록에 대한 정의, 현재 수사기록의 보존과 폐기현황, 끝으로 빅데이터 분석기법인 사례기반추론(CBR)에 대한 설명과 가상의 현실적용을 기반으로 제안을 하였다. 빅데이터 기반 시스템이 개발되더라도 이보다 시스템이 효율적으로 사용되기 위해서 꼭 필요한 것은 각 기관과의 협업관계 구축이다. 검찰 · 경찰 · 법원 · 법무부와 같은 기관들이 범죄예방 및 해결을 위해 서로 유기적인 협력이 반드시 이루어져야 할 것이다.
기대 효과 (요약)	검찰은 형벌권에 기초한 법 집행기관으로서 범죄 수사를 총괄 지휘하고 기소를 담당하는 수사기관이다. 수사기관이 궁극적으로 추구해야할 가치는 공정한 수사와 이에 근거한 판결이다. 빅데이터 분석 체계는 수사과정 속에서 객관성과 논리성을 제공할 수 있고 실패와 손실의 확률을 줄일 수 있을 것이다. 결론적으로 공정한 수사와 판결이 가능해 질 것이다.

『4차 산업혁명 시대의 과학수사 대학(원)생 아이디어 공모전』

아 이 디 어 제 안 서

1. 개 요

2016년 1월 스위스 다보스포럼에서 세계경제포럼 창시자 '클라우스 슈밥'은 4차 산업혁명 이라는 단어를 처음 세계 속에 선보였다. 이 단어는 순식간에 전 세계 속으로 퍼져나갔고 지금은 일반적인 상식용어가 되었다.

4차 산업혁명은 과거 '정보화'가 차지했던 영역을 인공지능(artificial intelligence) 기반의 '지능화'로 업그레이드하는 것이다. 즉, 4차 산업혁명의 성공여부는 인공지능 수준과 직결된다고 볼 수 있다. 최근 인공지능은 학습을 위해 많은 양의 데이터가 필요한데 이때, **빅데이터**의 영향을 크게 받는다. 빅데이터가 활발하게 이용되는 환경이 조성된다면 기계학습을 통해 인공지능의 알고리즘이 더욱 정교하게 개선될 것이고 이로 인해 얻어지는 파급력은 상상이상 일 것이다.

그렇다면, 빅데이터란 무엇인가? 단순하게 대용량 자료를 의미하는 것은 절대 아니다. 조직의 내외부에 존재하는 다양한 데이터를 수집, 처리, 저장하여 목적에 맞게 분석하여 유의미한 지식을 추출하고 이를 조직의 전략적 의사결정에 활용하거나 비즈니스 모델 개선 등에 활용하는 행위를 포괄적으로 가리키는 용어이다.

앞서 설명한 AI와 빅데이터를 과학수사 중 디지털 수사에 접목시킬 수 있다. 검찰의 수사기록들을 빅데이터로 활용하여 AI를 통해 시간적 소요가 많이 되는 복잡한 수사과정을 효율적으로 단축시킬 수 있다.

위 디지털 수사를 실제 사건이었던 2015년 10월 27일에 발생한 '창원 무학산 살인사건'에 적용해 볼 수 있다.

당시 경찰은 피해자의 시체가 발견된 무학산 인근을 중심으로 수사를 하였고 추가적으로 제보 전단을 무학산 인근 등산로에 배포 · 국립과학수사연구원에 DNA 분석도 의뢰했지만 단서를 찾지 못했다. 또한, 수사 중에 무고한 사람이 용의자로 지목되기도 하였다.

이 사건의 담당검사는 이전, 이와 비슷한 유형의 '시신없는 육절기 살인' 사건을 해결한 경험이 있었고 당시, 경찰서에 보관된 육절기를 대검찰청 디지털포렌식센터에 재감정을 의뢰하도록 지휘하여 사건을 해결하였다.

'무학산 살인사건' 또한 당시의 경험을 바탕으로 피해자 유류물에 대한 대검찰청 DNA 재감정을 의뢰하였고 이 과정에서 진범을 찾을 수 있었다.

'무학산 살인사건' 의 범인을 검거하는데 약 190여일이 걸렸다. 당시 경찰은 요원을 확대 편성하면서 현상금 1000만원을 내건 공개수사를 하였고 목격자 등 관련 증거 확보를 위해 전단지 3만부를 제작·배포하였으며 주민 제보 확인과 창원관제센터, 무학산 주변 CCTV 분석, 인터넷 사이트 및 통신수사를 실시했다.

만약 검찰 수사기록 빅데이터 기반 AI가 있었다고 가정한다면, 사건이 발생하자마자 유사범죄들에 대한 정보를 추출하고, 이를 분석하여 사건의 해결방안과 관련된 경우의 수를 제시할 수 있을 것이다. 또한, 어떤 방향으로 우선적으로 수사를 진행할지에 대해 예측이 가능할 것이며, 이를 통해 더욱 정교한 추론을 적용할 수 있었을 것이다.

위와 같은 절차로 수사가 진행되었다면 사건에 소비되는 시간적·비용적 지출을 크게 줄일 수 있었을 것이며 수사과정에 피해를 입는 시민들의 불편함까지 줄일 수 있었을 것이다.

사건 해결의 핵심은 대검찰청 디지털포렌식센터의 기술력을 통한 증거확보와 검사의 수사지휘를 통해 수사상 오류를 신속히 구제해준 사례이기도 하지만 그 보다 중요한 것은 피의자에 대한 범죄사실과 증거 관계를 명백히 하여 검찰 송치·공소 유지 등에 필요한 부분에 대해 검찰과 협력 체제를 보다 세밀하게 구축해야 된다는 것이다.
(※ 위 예시를 통하여 수사과정에 경찰은 잘못하였고, 검사가 잘했다는 것을 말하는 것은 아니다.)

즉, 검찰 수사기록 빅데이터 기반 AI를 통해 검찰과 경찰의 협력체제를 좀 더 보완하여 수사과정에 소요되는 기타 여러 가지 비용들을 최소화 하는 것이 핵심이며, 수사기록들이 빅데이터로써 활용가능성과 잠재성을 인식하고 추후 미래에 보다 발전된 수사방향에 관한 가능성을 제안한다.

2. 추진 목표 및 전략

ⅰ. 빅데이터의 개념에 대한 이해
ⅱ. 빅데이터의 특징에 대한 이해
ⅲ. 미래사회의 특성과 빅데이터의 역할이란?
ⅳ. 검찰 수사기록이란?
ⅴ. 검찰 사건 접수와 수사기록
ⅵ. 수사기록의 보존과 폐기
ⅶ. 빅데이터 분석 기법 - 사례기반추론(Case-Based Reasoning)
ⅷ. 사례기반추론을 통한 유사범죄 해결방안에 대한 경우의 수 제시 및 추론

3. 주요 내용

ⅰ. 빅데이터의 개념에 대한 이해

빅데이터는 정형화(structured)된 데이터, 반정형화(semi-structured) 데이터, 비정형(unstructured)데이터로 구분할 수 있다.

정형화된 데이터는 일정한 규칙을 갖고 체계적으로 정리된 데이터를 의미한다. 예를 들어 매년 통계청에서 발표하는 통계자료, 각종 과학적 데이터 등이 이에 해당되며, 그 자체로 의미 해석이 가능하고 바로 활용할 수 있는 정보를 내포하고 있다.

반정형화된 데이터는 아래아한글이나 마이크로소프트 워드 등으로 작성된 데이터를 의미하며 표나 그림이 될 수도 있지만 일반적으로 문자로 서술된 정보를 담고 있다.

비정형화된 데이터는 개인, 집단, 사회, 국가 등과 관련된 주제를 스마트 미디어 이용자들이 상호 의견을 교류함으로써 생산되는 정보이다.

이러한 빅데이터는 해당 데이터를 분석하고 처리함으로써 기존의 데이터에서 볼 수 없었던 새로운 의미를 산출하게 한다. 따라서 중요한 것은 형식적인 데이터 소스 내에서 외부로 새로운 가치를 창출할 수 있느냐 하는 것이다.

결국 새로운 가치와 의미를 산출하기 위해서는 축적된 데이터를 갖고 무엇을 분석할 것인가에 대한 문제제기가 필요하다. 이에 **마이닝**과 연결되는데, **빅데이터의 마이닝**은 정형 데이터마이닝, 텍스트마이닝, 웹 마이닝 그리고 소셜마이닝을 통해 현실 마이닝에 도달해야 한다. 현실 마이닝을 통해 예측할 수 있는 데이터들이 산출되어 사후 대책이 아니라 사전 방지 시스템을 만들 수 있다.

ⅱ. 빅데이터의 특징에 대한 이해

빅데이터는 5V로 대표되는 규모(Volume), 다양성(Variety), 속도(Velocity), 정확성(Veracity), 가치(Value) 등 5가지 구성요소를 갖추어야 한다. 특정 규모(big volume) 이상을 빅데이터로 칭하는 것을 넘어서 원하는 가치(big value)를 얻을 수 있을 정도로 상대적인 해석을 해야 하는 것이다.

<빅데이터의 5가지 구성요소(5V)>

구분	주요내용
규모(Volume)	· 기술적인 발전과 IT의 일상화가 진행되면서 해마다 디지털 정보량이 기하급수적으로 폭증 → 제타바이트(ZB) 시대로 진입
다양성(Variety)	· 텍스트 이외의 멀티미디어 등 비정형화된 데이터 유형의 다양화
속도(Velocity)	· 사물 정보, 스트리밍 정보 등 실시간성 정보증가 · 실시간성으로 인한 데이터 생성, 이동 속도의 증가

정확성(Veracity)	· 빅데이터의 특성상 방대한 데이터들을 기반으로 분석을 수행 · 데이터 분석에서 질이 높은 데이터를 활용하는 것이 분석의 정확도에 영향을 줌
가치(Value)	· 빅데이터 분석을 통해 도출된 최종 결과물은 기업이 현재 당면하고 있는 문제를 해결하는데 통찰력 있는 유용한 정보를 제공

ⅲ. 미래사회의 특성과 빅데이터의 역할

미래사회의 특성	빅데이터의 역할
불확실성 → **통찰력**	· 여러 가지 가능성에 대한 시나리오 시뮬레이션 · 다각적인 상황이 고려된 통찰력을 제시 · 다수의 시나리오로 상황 변화에 유연하게 대처
리스크 → **대응력**	· 환경, 모니터링 정보의 패턴 분석을 통한 위험 징후 포착 · 이슈를 사전에 인지 · 분석하고 빠른 의사결정과 실시간 대응 지원
스마트 → **경쟁력**	· 대규모 데이터 분석을 통한 상황 인지, 인공지능 서비스 등 가능
융합 → **창조력**	· 타 분야와 결합을 통한 새로운 가치창출 · 향상 및 시행착오 최소화

ⅳ. 검찰 수사기록이란?[1]

수사기록이란? 사건과 관련된 개개의 수사서류들이 종이로 출력되어 편철되어 있는 것이라고 할 수 있다. 수사서류란? 수사기록을 구성하고 있는 개개의 서류를 말한다.
검찰수사실무상 수사과나 검사실에서 통상적으로 사용되는 주요 수사서류에 대해서 대검찰청 검찰사관 수사실무 집필위원회, 검찰수사관 수사실무에 따라 다음과 같이 정리할 수 있다.

[수사단계별 구분]

내사단계	정보보고, 내사결과보고, 진정서, 진술서, 진술조서, 범죄경력조회서
입건 및 수사실행단계	진술서, 고소 · 고발장, 전과입력카드, 피의자신문조서, 진술조서, 진술서, 실황조서, 압수조서, 사실조회, 수사보고서, 출석요구서, 구속영장신청서 등
송치단계	송치서표지, 의견서, 압수물총목록, 기록목록, 피의자통계원표 등
검찰수사단계	사경수사단계에서 사용되는 서류 외에 수사촉탁 의뢰서, 우편진술서, 수사지휘서, 소재수사지휘, 구속영장청구서 등

1) 수사기록에 관한 정보를 찾을 수 없어 논문, '빅데이터로서 수사기록 보존 · 폐기에 관한 연구', 서울대학교 융합과학기술대학원 수리정보과학과 디지털포렌식전공 홍승아, 참고하였습니다.

검사결정단계	공소장 자료, 석방지휘서, 출국정지 및 해제, 지명수배 및 수배해제의뢰서 등

[문서의 성격에 따른 구분]

소송행위적 의사표시적 문서의 성격	고소 · 고발장, 고소 · 고발취소장, 합의서, 공소장, 구속영장신청 등
보고서적 성격	의견서, 범죄발생 및 검거보고서, 수사보고서 등
증거서류의 성격	피의자신문조서, 진술조서, 진술서, 자술서, 실화조서, 사실조회서류, 전과조회서, 진단서, 호적등본 등
기타문서	기록표지, 기록목록 등

[수사방법에 따른 구분]

임의수사방식	피의자신문조서, 진술조서, 출석요구서, 사실조회서류 등
강제수사방식	구속영장, 압수수색영장, 증거보전신청, 증인신문청구서 등

v. 검찰 사건 접수와 수사기록[2)]

수사가 개시되면 그 건에 대한 기록이 생성되기 시작한다. 수사의 개시란? 내사, 인지(입건), 수사의 실행, 사건송치 및 수사종결로 이어지는 수사 단계 중 입건 단계로서 수사기관인 검사가 사건을 수리하여 사건번호를 부여한 후 그 사건의 담당검사가 정해지거나 사법경찰관이 하나의 사건을 사건접수부에 등재하는 절차를 마치는 단계부터를 말한다. 따라서 입건 단계에서 사건을 수리하여 사건번호가 부여되면 사건으로서 수사가 진행되고 그에 대한 수사기록이 만들어지는 것이다.

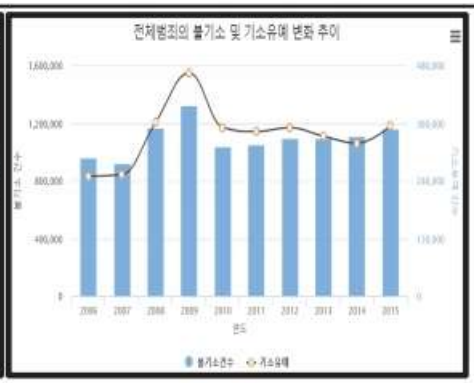
'검찰사건사무규칙' 에 근거하여 사건 수리 사유가 발생하면 사건을 접수하여 수리한 후 사건의 전산입력 진행번호로서 건건이 일련번호를 붙임으로 원칙적으로 1개의 수사기록 당 1개의 사건번호가 부여된다.[3)]

아래 [그림 1,2][4)]는 '전체범죄의 기소 및 구공판 변화추이' 와 '전체범죄의 불기소 및 기소유예 변화 추이' 이다. 이와 같이 접수, 처리되는 수사기록이 데이터화 되어 매해 축적되어 보존 · 관리 된다고 할 때 그 형식적 · 내용적 측면의 방대한 규모에서 '빅데이터' 로서의 가치가 생성될 것이다.

2) 논문, '빅데이터로서 수사기록 보존 · 폐기에 관한 연구', 서울대학교 융합과학기술대학원 수리정보과학과 디지털포렌식전공 홍승아. 참고.

3) 검찰사건사무규칙 제2조 (수리사유) 참고.

[그림 1]



[그림 2]

vi. 수사기록의 보존과 폐기[5]

과거 '수사기록'은 단지 커다란 데이터로 창고에 보존되다가 일정 기간 후 폐기되었지만 데이터를 분석하여 새로운 가치를 발굴해내는 환경이 마련된다면 형사 정책적으로 중요한 도구가 될 수 있다.

형사사건의 수사기록은 최종적으로 검찰청에서 보존하게 되는데 '검찰보존사무규칙'에서는 수사기록이라는 용어를 사용하지 않고 '사건기록'이라고 한다. 사건기록[6]이란? 수사·재판 및 그에 부수되는 기록이라고 정의하고 있다.

사건기록은 재판확정기록, 불기소사건기록, 진정·내사사건기록, 영상녹화물로 구분된다. 불기소사건의 경우 검찰청의 불기소 결정에 의해 종결되어 곧바로 검찰청에서 보존되지만 확정기록은 기소되어 법원에서 재판과정을 거쳐 최종적으로 검찰청으로 오게 된다. (※ 추가적인 보존에 관한 사항은 각주[7]로 정리)

기록은 보존 기간 동안 보존하고 보존 기간이 만료하면 소속검찰청 장의 허가를 받아 폐기하여야 하는데 실무상 연 1회 정기적으로 기록 폐기를 하고 있다.

또한 형사사법정보시스템에서 시스템 부하로 인한 비효율적인 측면이 존재한다는 문제 제기로 영구보존 및 폐기의 대상이 되는 전자문서를 구분하여 재판서, 결정문, 공소장, 의견서 등 통합검색을 통해 공유하는 문서의 경우 원 사건기록 폐기 후에도 정보 공유의 필요성이 있으므로 영구 보존하며 이를 제외한 일반사건의 기록에 편철되는 전자문서는 원 사건기록 폐기 시에 해당 전자문서도 함께 폐기하고 있다.

기록폐기는 불필요한 기록을 적시에 폐기하여 보존의 효과를 증대시키는 중요한 기록 관리의 영역이다. 검찰청의 수사기록 폐기도 증거로서 보존되어야 할 중요기록이

4) 범죄와 형사사법 통계정보, 주요 범죄 유형별 동향, 전체범죄 검찰 처리현황 참고.

5) 논문, '빅데이터로서 수사기록 보존·폐기에 관한 연구', 서울대학교 융합과학기술대학원 수리정보과학과 디지털포렌식전공 홍승아. 참고.

6) 검찰보존사무규칙 제2조(정의).1.

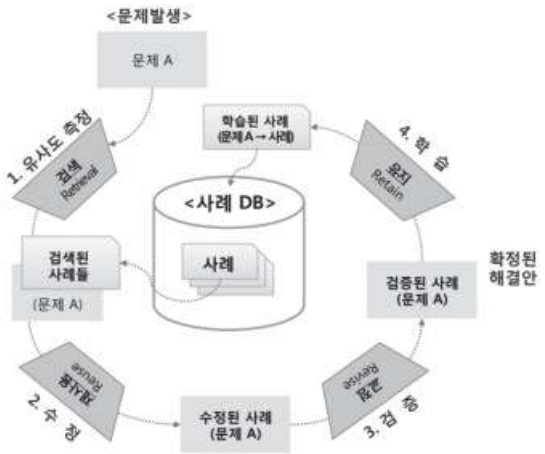
7) 검찰보존사무규칙 제7조(관련사건에 관한 불기소사건기록의 보존), 제8조(보존기간), 제10조(보존기간), 제15조(입건처리로 종결된 내사사건기록의 보존), 제16조(보존기간), 제17조의3(영상녹화물의 보존), 제18조(보존기간)

불필요한 기록과 혼합되어 손상, 분실될 것을 우려한 적극적인 기록관리 행위로 행해져 왔다고 할 수 있으며 보존 방식 또한 마찬가지이다.

반도체 가격의 하락과 오픈소스 기반 분석도구의 발전을 통해 적은 비용으로 데이터 저장이 가능해지고 분석 기술의 지속적 발달 가능성을 미루어 짐작해보면 4차 산업시대에 데이터 폐기란 말이 과연 맞는 것인지 다시 한 번 생각해 볼 필요가 있다.

ⅶ. 빅데이터 분석 기법 - 사례기반추론(Case-Based Reasoning)

사례기반추론**(CBR)**이란 과거에 있었던 사례들의 결과를 바탕으로 새로운 사례의 결과를 예측하는 기법이다. 과거에 발생한 문제는 미래에 다시 비슷한 형태의 문제로 발생할 가능성이 높고 새로운 문제를 해결할 수 있는 정답이 과거의 문제를 해결했던 정답과 유사할 것이라는 가정이다. 과거 사례들을 저장해 둔 사례기반으로부터 해결하고자 하는 새로운 사례와 가장 유사한 사례를 검색한 후, 유사 사례의 해결책을 바탕으로 당면한 문제의 해결책을 제안하는 과정으로 진행된다. 이 때 제안된 해결책은 필요에 따라 적절히 수정된 후에 주어진 문제를 풀기 위해 재사용되며 이렇게 해결된 새로운 사례는 추후 다른 문제 해결에도 도움이 될 수 있도록 새로운 사례로 사례기반에 저장된다.



[그림 3] 사례기반추론과정 4R 프로세스

사례기반추론(CBR)의 이용은 위 **[그림3]**과 같은 4단계 과정을 거친다.

1) 검색(Retrieve)

대상문제가 주어지면, 사례 데이터베이스에서 그것을 풀기에 적절한 사례들을 검색한다. 하나의 사례는 문제와 그 해결 방법 그리고 그 해결방법이 어떻게 유도되었는지에 대한 설명 등으로 구성된다. CBR 시스템의 효과를 결정짓는 가장 중요한 단계이다. 이 단계에서 '어떤 원리로 유사 사례들을 선별해서, 이들을 조합해, 추천 결과를 만들어 낼 것인가?' 하는 것에 따라 CBR 시스템 성능이 크게 변화하기 때문이다.

때문에 사례간 유사도를 어떻게 측정할 것인가, 추천 결과를 도출할 때 유사 사례는 얼마나 결합할 것인가 하는 등의 문제는 전통적으로 주요 CBR의 연구주제로 자리매김하여 왔다.

2) 재사용(Reuse)

이전의 사례로부터 대상 문제의 해결방법을 연결한다. 새로운 상황에 맞추기 위해 필요한 만큼 해결 방법을 적응시키는 것을 포함한다.

3) 수정(Revise)

이전의 해결방법을 대상의 상황에 연결시킨 후, 그 새로운 해결방법을 실세계에서 테스트하고, 필요하다면 수정한다.

4) 유지(Retain)

해법이 성공적으로 대상 문제에 적용된 후에 그러한 경험이 사례 데이터베이스에 새로운 사례로서 저장된다.

일반적으로 다른 주요 인공지능기법들은 문제와 해법 사이의 일반적인 관계를 도출하여 이를 기반으로 추론하는 원리로 이루어져 있어, 비교적 정형화된 문제 해결에만 적합하고, 지식도 지속적으로 개신되기 어려운 구조적인 한계를 가지고 있다.

하지만 사례기반추론**(CBR)**은 과거에 축적된 정보만 있으면, 어떤 문제든 해결이 가능하므로 복잡하거나 비구조화된 문제를 해결하는데 유리하며, 지식기반을 지속적으로 업데이트 할 수 있다는 측면에서 상대적으로 우수하다고 할 수 있다.

ⅷ. 사례기반추론을 통한 유사범죄 해결방안에 대한 경우의 수 제시 및 추론

개요에서 언급하였던 '무학산 살인사건' 을 통해 CBR을 적용시킬 수 있다. 문제 발생은 무학산 살인사건으로 설정하고, 이 수사를 담당하는 검사는 임의의 A검사로 이 사건을 해결해야한다는 가정으로 시작한다.

A검사는 회상할 수 있는 가장 적절한 경험은 그가 증거도 많이 있고 유력한 용의자도 바로 검거하여 사건이 큰 문제없이 해결된 사건이었을 것이다.

하지만 이번 사건은 경찰 측에서도 여러 방법을 시도하였지만 장기간 동안 용의자를 찾지 못하였으며 국립과학수사연구원 DNA 분석에서도 단서가 나오지 않아 사건이 미궁으로 빠질 수 있었다.

이때 A검사는 수사기록 빅데이터를 이용한 CBR을 통해 현재 상황을 검색하여 현재 사건과 가장 유사한 과거 사건들을 알 수 있을 것이다. CBR을 통해 현재 상황과 가장 유사한 '시신없는 육절기 살인' 사건을 찾을 수 있을 것이고 이 사건에서 대검찰청 디지털포렌식센터 DNA 감정을 통해 사건을 해결할 수 있었다는 사실을 빠르게 알 수 있었을 것이다.

A검사는 CBR을 통해 현재 상황과 유사한 과거 사건의 데이터를 통해 해결책을 보다 빠르게 얻을 수 있었고 즉각적으로 대검찰청 디지털포렌식센터에 현 사건의 증거물에 대한 DNA 감정을 진행하였을 것이다.

정상적으로 사건이 흘러갔다면 감정관들이 여러 유류물 중 등산용 장갑을 통해 실제 범인을 검거할 수 있었을 것이다.

하지만 만약에 핵심 증거물이었던 등산용 장갑이 심각하게 훼손되어 검정을 할 수가 없던 상황이 온다는 가정을 한다면 증거로 제출된 여러 유류물 중에서 장갑 다음으로 우선순위가 높은 증거물을 채택하여 그 물품을 대상으로 DNA 감정을 하였을 것이다.

이런 상황이 오게 된다면 사건을 해결하는 과정에서 새로이 발견한 것을 기록할 수 있으며, 이를 통해 축적된 사건이 많아지게 될 것이고 다른 임의의 검사가 이와 비슷한 부류의 사건을 맡게 된다면 복잡한 문제를 비교적 적은 정보로도 의사결정, 문제해결이 가능해 질 것이다.

이와 같이 가정을 통해 설명한 내용들이 빅데이터 기반 사례기반추론(CBR)을 통해 유사사건들의 경우의 수 제시 및 추론이 가능하다는 것을 가상의 시나리오로 이해와 경험을 할 수 있었다.

4. 아이디어의 가치[8)]

빅데이터 기반 범죄예측 및 예방은 이미 현실 속에서 많이 이루어지고 있다.

서울 영등포구에서 여성 대상 성범죄 예측과 사전 예방을 위한 시스템이 구축되고 있다. 2018년 9월, 영등포구와 KT는 범죄예방을 위한 **도시환경설계(CPTED) 플랫폼 개발**을 마치고 하반기 중 본격적으로 가동한다고 밝혔다. CPTED는 도시환경을 재설계해 안전한 도시를 구현한다는 개념으로, 우선 여성 대상 성범죄 예방에 초점이 맞춰졌다. 성범죄와 관련성이 높은 각종 데이터를 수집한 뒤 빅데이터 분석 기법으로 영등포 지역 곳곳에 안전도 등급을 매기는 게 핵심이다.

CPTED에는 영등포경찰서가 보유하고 있는 지역별 성폭력 발생률, 성범죄자 거주지 등 범죄 관련 데이터와 KT가 추출한 밤 9시부터 새벽 3시까지 영등포 지역 내 여성 유동인구 정보, 영등포구청 주민등록 시스템으로 확보한 여성 1인가구 거주지 등이 들어가 있다.

입력된 데이터를 놓고 AI 기반 기계학습(머신러닝) 시스템이 각 데이터가 '안전도'에 미치는 영향을 스스로 분석한다. 안전도를 떨어뜨리거나 높이는 요소들에 대해 계산하면서 영등포 지역의 거리 10m 단위마다 1~5단계의 안전 등급을 매긴다.

범죄가 가장 발생하지 않을 곳을 1등급으로 하여 안전등급을 매기게 된다. 안전에 영향을 미치는 요소에 가중치를 끊임없이 조정하면서 최대한 정확도를 높이는 머신러닝 기술이 적용되었다.

영등포구에서는 안전도가 높은 곳으로 분류되는 지점을 중심으로 여성안심귀갓길 여성안심택배함, 여성안심지킴이집 등이 집중 재배치된다. 또한 범죄 취약 지역에는 CCTV를 증설하고 순찰을 강화한다.

8) 한국일보, '빅데이터로 범죄 예측... 한국판 '마이너리티 리포트' 구축한다', 맹하경 기자, 자료참고

이처럼 올해 당장 빅데이터 기반 범죄예측 및 예방이 현실 속에서 이루어지는 것을 알 수 있다. 하지만 이 제안서에서 말하는 빅데이터 기반 유사범죄 해결 및 추론은 앞서 설명한 기술과는 다르다.

빅데이터 기반 범죄예측 및 패턴분석은 범죄를 수사하고 순찰 및 진압, 단속, 공공질서의 유지 등 업무를 수행하는 경찰의 역할에 더 부합하다고 볼 수 있다.

빅데이터 기반 CBR 방법을 통한 해결방안 제시 및 추론은 수사 자료를 기반으로 최종적으로 수사 및 결정을 하는 검찰의 역할에 더 부합한다고 볼 수 있다. 바로 이 부분이 기존의 빅데이터 기술과의 차이점이다.

수사기록이라는 문서 특성상 빅데이터의 특징인 5V에 부합하지 않을 수 있다. 또한 데이터가 거대해질수록 개인정보를 비롯한 수많은 위험성이 동반되기에 무턱대고 빅데이터 기반 인공지능 시스템을 구축하는 것은 쉬운 일이 아니다.

하지만 지금 이 순간에도 축적되고 있는 수사기록이란 데이터를 빅데이터라는 관점에서 바라볼 때 큰 잠재성이 있는 정보로 바라보는 것이 중요하며 그 속에서 새로운 가치를 찾을 수 있다면 수사적 관점에서 더욱 큰 발전이 있을 것이다.

5. 기대효과

4차 산업의 빅데이터 기반 인공지능 서비스는 일상생활을 포함하는 거의 모든 영역에서 유용하게 활용될 수 있다. 기업입장에서의 빅데이터 분석 체계는 더 나은 의사결정을 통해 비용 감소, 매출 증대, 새로운 제품 · 서비스 개발이라는 가치를 창출시킬 수 있다.

그렇다면 검찰에서 빅데이터 분석 체계는 현실 도입시 궁극적으로 어떤 도움을 가져다 줄 수 있는가?

검찰은 형벌권에 기초한 법 집행기관으로서 범죄 수사를 총괄 지휘하고 기소를 담당하는 수사기관이다. 수사기관이 궁극적으로 추구해야할 가치는 공정한 수사와 이에 근거한 판결일 것이다.

이런 점을 미루어 보았을 때 빅데이터 분석 체계는 수사과정 속에서 객관성과 논리성을 제공할 수 있고 실패와 손실의 확률을 줄일 수 있다.

4차 산업시대가 진행 중인 현 시점에서 빅데이터 도입의 중요성 인식 및 검토는 충분히 할 것이다. 하지만 도입의 목적이 무엇인지에 대해 명확히 하는 것이 중요하다. 검찰의 경우엔 과거의 경험과 감이 아닌 객관적 자료에 근거하여 보다 나은 의사결정을 통해 수사를 진행하기 위하여 필요한 것이다.

수사기록 빅데이터 기반 시스템이 개발되기 위해선 앞서 설명한 수사기록 보존 · 폐기에 대한 법 규정도 개정할 필요가 있고, 개발 이후엔 수사와 관련한 관계기관 간 긴밀한 협업체계를 구축하는 것 또한 매우 중요하다.

수사착수부터 개시, 진행, 재판까지의 순서가 기관과의 협업, 그리고 빅데이터 시스템을 통한 과학적 · 객관적 분석 및 판단은 분명 보다 나은 공정한 수사로 이끌 것이라고 확신한다.

YTN science

[사이언스 CSI] 보이지 않는 흔적까지 찾는다! 디지털포렌식

2019-04-01

■ 이인수 / 대검찰청 디지털 포렌식 연구소 소장

[앵커]

최근 디지털 기술의 발달로 위조나 해킹 등 사이버 범죄가 기승을 부리고 있습니다. 사이버 범죄의 해결사로 디지털 포렌식이 주목받고 있는데요,

오늘 사이언스 CSI에서는 '보이지 않는 흔적까지 찾아내는 디지털 포렌식'에 대해 알아보겠습니다. 대검찰청 과학수사부 디지털수사과 디지털 포렌식 연구소 이인수 소장과 함께합니다. 어서 오세요.

최근 논란이 되고 있는 일부 연예인들의 불법 촬영물 공유 혐의를 비롯해서요. 여러 사이버 범죄를 수사할 때 디지털 포렌식 기법을 사용해서 증거물을 확보했다는 말을 듣곤 합니다. 여기서 말하는 디지털 포렌식, 정확히 어떤 건가요?

[인터뷰]

디지털 포렌식도 과학수사라는 커다란 영역 안에 있는 한 분야로 그 수사 대상이 디지털 기기인 경우를 말합니다. 다시 말씀드리면 정보 저장 매체에 저장된 디지털 정보로부터 범죄 관련 증거를 추출하고 분석하여 법정에 증거로 제출하는 기술과 절차를 통칭한다고 말할 수 있습니다. 현대사회에서는 디지털 기기와 정보기술을 통해 정보를 기록하고 소통하다 보니 다양한 범죄의 정보도 정보 저장 매체에 저장되고 있어서 수사기관 입장에서 범죄 단서를 확보하는 중요한 수단으로 활용하고 있습니다. 디지털 포렌식은 결국 사람이 아니라 디지털 기기에 저장된 데이터를 바탕으로 진실을 찾기 위한 수사기법이라고 할 수 있으며, 증거를 기반으로 수사하는 방식이기 때문에 인권을 보호하는 데에도 중요한 역할을 하고 있습니다.

[앵커]

디지털 기기 내에 있는 정보를 분석해서 수사에 핵심이 될 수 있는 단서를 확보하는 게 디지털 포렌식 기법이라는 말씀이신데요. 디지털 기기라고 하면 떠오르는 게 휴대전화나 노트북을 들 수 있을 것 같습니다. 주로 어떤 디지털 기기를 분석하시나요?

[인터뷰]

디지털 포렌식은 전통적으로 분석 대상 기기와 방법에 따라 컴퓨터 포렌식, 모바일 포렌식, 데이터베이스 포렌식, 네트워크 포렌식 등으로 구분하고 있습니다. 최근에는 새로운 기기가 출현하고 있고 데이터의 저장 위치도 변화되고 있어, IoT 포렌식, 클라우드 포렌식 등 새로운 포렌식 분야로 그 범위가 확장되고 있습니다.

[앵커]

디지털 기기나 저장 위치에 따라 분야가 나뉜다는 말씀이신데요. 전통적인 방식이 컴퓨터 포렌식과 모바일 포렌식이라고 하셨습니다. 우선 이 분야부터 설명해주시죠.

[인터뷰]

데스크톱이나 노트북, USB, 외장 하드디스크 등을 분석하는 컴퓨터 포렌식팀에서는 개인이 사용하는 윈도나 맥 같은 운영체제를 분석합니다. 파일의 생성, 수정, 삭제 시간 등 다양한 응용프로그램의 사용 이력을 PC를 통해 작업하는 동안 생성된 각종 로그 데이터 등을 분석하고요. 삭제된 파일을 복원하거나 삭제 행위들에 대한 흔적 분석을 주로 하고 있습니다. 모바일 포렌식팀은 마찬가지로 스마트폰, 태블릿 PC 등을 대상으로 각종 앱에 기록된 내용과 다양한 접속 흔적 등을 살펴보고 있고요. 고장 나거나 파손되거나 침수되어 정상 작동하지 못하는 휴대전화에서 데이터를 추출하고 복구하여 데이터 분석을 지원하고 있습니다.

[앵커]

증거를 훼손하거나 조작하려는 부분도 확인할 수 있다는 말씀이신데요. 그럼 디지털 포렌식 연구소에는 또 어떤 일을 담당하고 계신가요?

[인터뷰]

기업의 전산 서버에서 각종 회계자료나 이메일, 기업 자료가 저장된 파일 서버를 대상으로 데이터를 확보하고 분석하고 있고요. 그 외에도 암호를 해독하거나 새로운 디지털 포렌식 기법을 연구하기도 하고, 전문인력 양성 교육과 해외 기술 전파를 담당하기도 합니다.

[앵커]

정말 다양한 연구와 수사를 통해서 범죄 해결에 한몫을 하고 계신데, 혹시 기억에 남는 사건이 있다면 들어보고 싶은데요.

[인터뷰]

30대 회사원이 폭행으로 살해돼 가로수 밑에서 발견되었는데, 가로수 밑에 담배꽁초를 찾아 DNA 조사를 한 결과 주변 불량배가 지목되었습니다.

진술을 통해 피의자로 송치되었는데, '담배꽁초와 시신이 같이 있었다는 사실만으로 피의자를 단정시킬 수 없지 않나?'라는 의심을 하게 되었습니다. 디지털 증거를 살펴보며 분석한 결과, 친구들과의 채팅 내용이 암호화되어 담겨 있었는데, 이를 해독하여 내용과 시간을 분석해 송치된 피의자가 범인이 아니었다는 걸 증명했습니다.

[앵커]

또 다른 사건이 있나요?

[인터뷰]

또, 통합진보당 당내 경선에서 벌어진 대리투표사건이 있었습니다. 휴대전화로 전송된 인증번호를 넘겨받아 인터넷 전자 투표를 대신했는데요. 특정 후보를 뽑기 위해 대리투표를 해 경선 업무를 방해한 혐의로 재판에 넘겨졌습니다. 이 사건이 진행될 때 데이터가 압수되었는데 해당 데이터가 모두 암호화되었고 어떤 방식으로 암호화되었는지 확인할 방법이 없었습니다. 결국, 오랜 분석 후에도 결과가 도출되지 않아

실패하였다고 수사팀에 통보하고 종결할 수밖에 없었는데요. 포기하기가 너무 아쉬워서 알고리즘의 조각을 한 번만 더 맞춰보겠다는 생각으로 다시 시도하기를 반복한 끝에 숨겨진 조각 퍼즐이 맞추어져 모든 데이터를 해독하고 내용을 파악하여 수사팀에 통보하였을 때 가장 뿌듯하였습니다.

[앵커]

들어보니깐 피의자의 무죄를 증명하시기도 했고 유죄를 이끌어 낸 사건을 말씀해주셨는데요. 하지만 요즘은 최첨단 IT 기술이 발달하면서 점점 더 범죄 행위를 밝혀내는 게 어려지고 있다는 생각이 듭니다. 수사하시면서 가장 힘들거나 어려운 부분이 있다면 어떤 것인가요?

[인터뷰]

결국, 저희의 업무도 일반 수사업무와 같이 숨기는 자와 찾는 자의 싸움이라고 볼 수 있는데요. 다만 그 대상과 수단이 정보기술이라는 차이만 존재합니다. 그런데 언론과 인터넷 등을 통해 디지털 증거를 은닉하는 기법이 너무 많이 알려져서 데이터를 확보하고 분석하는 것도 어렵고 복잡해지고 있는 것이 사실입니다. 또한, 하루가 멀다 하고 기술은 변화하고 진화하고 있어서 끊임없는 현장 기술의 변화, 추이 조사와 연구개발이 수반되어야 합니다. 디지털 포렌식은 검찰뿐만이 아니라 경찰, 특별사법경찰 등 다양한 수사기관과 조사 감독기관에서도 필수적으로 도입하고 활용되고 있습니다. 지난 10년간은 기관별로 특성에 맞게 발전시켜왔지만, 저희가 닥친 문제는 한 기관의 노력만으로는 해결하기 어려운 상태입니다. 따라서 국가 차원에서 전문 인력 양성과 전문 도구의 연구, 개발, 검증, 서비스의 구축과 활용 측면에서 적극적 노력이 필요할 때라고 보고 있습니다.

[앵커]

갈수록 교묘해지고 어려워지는 사건의 해결을 위해서 기술과 인력양성을 말씀하셨습니다. 이런 부분에 대응하기 위해 어떤 대안을 마련하고 있으신가요?

[인터뷰]

검찰은 빅데이터 처리기술을 활용해 대량의 디지털 증거에서 보다 빠르고 정확하게 범죄 단서를 찾기 위해 'iDEAS'라고 불리는 통합 디지털 증거분석 시스템을 개발하여 운영하고 있습니다. 향후 인공지능 기술과 접목을 통해 진화시킬 예정이며 이를 클라우드 서비스 형태로 국가 수사기관과 공동 활용할 수 있는 방안을 마련하고 있습니다. 또한, 당면한 문제를 구체적으로 파악하고 실천 방안을 마련하기 위해 국가 차원의 디지털 포렌식 지원 클라우드 센터를 구축하려고 하고 있습니다. 국가 수사기관이 공동으로 연구하고 개발된 기술과 서비스를 활용할 수 있는 토대를 만들기 위해 여러 정부 부처와 협력을 강화하고 있습니다. 최근 저희의 지난 경험과 지식을 해외에 전파하기 위해 코이카, 법무연수원과 협력하여 CSI 국가, 몽골, 동남아시아와의 교류를 확대하고 있으며 우즈베키스탄의 경우에는 우즈베키스탄 정부와 협력

하여 디지털 수사과를 설립하였고 전문 인력을 양성해 현재 실제 수사에 투입되어 좋은 결과를 내고 있기도 합니다.

[앵커]

해외로 진출한 건 한국 과학수사의 위상을 높일 수 있겠다는 생각도 들고요. 이렇게 디지털 포렌식의 역할에 대해서 들어봤는데 개인적으로 소장님의 앞으로의 계획이나 바람이 있다면 들어보고 싶은데요.

[인터뷰]

아직은 보람보다는 책임감 때문에 굉장히 무겁게 느끼며 살고 있습니다. 다만 피의자의 범죄행위를 정확히 증명한 경우에 보람이 있기도 하지만 개인적으로는 고소사건에서 누명을 쓴 무고를 밝혀낼 때가 더욱 보람을 느끼는 거 같습니다. 앞으로의 계획이 있다면 의사가 인간의 생명을 다룬다고 하면 수사는 어느 한 사람의 인생과 깊숙이 관련된 업무라고 생각합니다. 정확하고 신중한 분석을 통해 실체적 진실을 발견하기 위해 필요한 부분만을 정확히 추적하고 도려낼 수 있도록 연구에 매진할 생각입니다.

[앵커]

제가 사전에 소장님 인터뷰를 봤는데 어제는 됐는데, 오늘은 안 될 수도 있는 게 디지털 포렌식이라는 말씀을 하셨더라고요. 정말 그만큼 고충과 책임감이 느껴지는 답변이었습니다. 디지털 포렌식에 대해서도 정부의 지원과 국민적인 관심이 필요한 때가 아닌가 싶습니다,

지금까지 대검찰청 과학수사부 디지털 수사과 디지털 포렌식 연구소 이인수 소장님과 함께했습니다. 오늘 말씀 고맙습니다.

세계 최고의 과학수사