마약사건 수사에서 디지털 포렌식 활용에 대한 연구

- 현장수사관 중심으로 -

2019년 12월

서울대학교 융합과학기술대학원

수리정보학과 디지털포렌식 전공

김 종 엽

마약사건 수사에서 디지털 포렌식 활용에 대한 연구

- 현장수사관 중심으로 -

지도교수 천 정 희

이 논문을 석사 학위논문으로 제출함

2019년 12월

서울대학교 융합과학기술대학원

수리정보과학과 디지털포렌식학 전공

김 종 엽

김종엽의 석사 학위논문을 인준함

2019년 12월

위 원 장 안 정 호 (인)

부위원장 천 정 희 (인)

위 원 박 상 준 (인)

요약(국문초록)

스마트 폰 등 디지털 기기의 보급 확대와 인터넷 서비스의 발달로 SNS를 통하여 마약을 판매하고 구입하는 시대가 되었다. 디지털 기기를 이용하여 서로 연락을 주고받은 후 매수자는 비트코인이나 대포통장으로 대금을 입금하고 판매자는 마약이 숨겨진 장소를 사진으로 찍어 전송하는 등 서로 만나지 않고도 매매가 가능하여 대한민국은 지금 전례 없는 마약이 성행하고 있다.
그러나 마약수사는 짧은 시간에 해당 범인을 검거하고 윗선까지 검거해야 하므로 범죄자들이 사용하는 디지털 기기에 대한 분석이 반드시 있어야 하고 그 분석을 위해서는 디지털 포렌식이 필요하다. 디지털 기기는 필연적으로 그 흔적을 남기기에 수사를 하는 과정에서 디지털 포렌식을 통하여 결정적 증거를 발견하고 사건을 해결하는 경우가 많아 여러 사례를 통하여 디지털 포렌식이 마약사건에서 어떻게 활용되고 있는지 알아보고 신속한 수사를 위해 마약사건 유형별로 디지털 기기에 대한 우선 조사순위를 정립하고 범죄자의 안티포렌식 행위는 어떤 것이 있는지 살펴보고자 한다.

뿐만 아니라 디지털 포렌식이 마약수사에 있어 없어서는 안 될 중요한 수사도구 이지만 디지털 포렌식을 통하여 확보된 디지털 증거는 변조용이성과 취약성 등의 특징이 있어 그 취급에 상당한 주의를 기울여야 한다.
하지만 마약수사는 대부분 긴급을 요하는 사건이 많아 디지털 포렌식 수사관과 함께 현장에 나가기 어렵기 때문에 현장수사관들이 범인검거와 신병관리 및 현장보존, 마약 증거물 압수뿐만 아니라 디지털 증거를 적법하게 확보하는 것도 필수적인 절차임에도 불구하고 현재 여건을 보면 현장수사관들은 디지털 증거 처리에 대한 지식이 많이 부족한 실정이다. 따라서 현장수사관의 효율적인

디지털 기기 수집절차가 무엇인지 알아본다.
이와 더불어 현장수사를 중점으로 하는 마약수사관에게도 디지털 포렌식 관련 교육을 받을 수 있는 기회를 확대해야하며 장기적으로는 마약수사를 전담 분석하는 디지털 포렌식 팀을 신설하여 마약수사의 역량을 향상시킬 필요가 있다.

주요어 : 마약수사, 디지털 포렌식, 안티포렌식, 다크웹, 디지털 기기, 증거활용, 킬스위치
학 번 : 2018-23946

목 차

표 목 차

그 림 목 차

Ⅰ. 서 론

1. 연구의 목적

마약류가 개인과 사회에 미치는 영향을 고려할 때, 최근 급속하게 국제화·광역화·조직화되고 있는 마약 범죄로부터 우리 사회 및 구성원을 보호하기 위해서는 마약범죄에 엄정하게 대처하여야 할 필요가 있다.
최근 서울의 유명클럽에서 발생한 폭행사건이 마약사건으로 번지며 마약류범죄에 대한 사회적 관심이 고조되고 있다. 경찰은 이를 계기로 마약류 등 약물이용범죄에 대한 집중단속에 들어가 올해 2. 25. ~ 5. 24.까지 3개월간 관련사범 3,994명을 검거하고 이 가운데 920명을 구속했다고 발표했다.[1] 2013년 9,765명이었던 마약류사범은 급격히 증가하여 2016년 14,214명으로 조사되었으며 2017년 14,123명, 2018년 12,613명으로 지난 3년간은 보합세로 보이지만 전체적으로 보면 증가추세에 있다.[2]

이러한 마약사범의 증가는 스마트폰 등 디지털 기기의 보급 확대와 소셜 네트워크서비스(SNS)의 대중화, 클라우드 컴퓨팅 기술, 유튜브 등 인터넷 기반 서비스와 스마트폰 등 모바일 기기를 사용할 수 있는 환경이 확대되어 많은 정보를 시간과 장소에 구애받지 않고 접할 수 있게 되었고, 그런 환경의 변화가 마약사범의 증가를 가능하게 만들었다. 뿐만 아니라 위와 같은 환경의 변화는 마약수사의 환경도 변화시켜 마약사범에 대한 수사방법을 과거와 다르게 변화시켰다.
즉 과거 판매자와 구입자가 직접만나 음성적으로 마약을 매매하는 방식에서 현재는 SNS(텔레그램, 위챗, 카카오톡, 구글 메신저 등)를 통한 **비대면 방식**[3](일명 '던지기', '드랍')으로 마약에 대한 매매와 유통방식이

1) 구효송, 신승균, '마약류 범죄의 문제와 대응방안' 2019. 6. 21. 116면.
2) 대검 마약류 범죄백서, 2018
3) SNS로 마약을 구입하고 싶다는 메시지를 받으면 특정 계좌(주로 대포통장)로 돈을 송금 받은 후, 판매자가 마약이 숨겨진 장소를 사진과 함께 알려주면 구입자가

서서히 바뀌는 추세다.
마약범죄자들이 비대면 방식의 마약매매를 하기 위해서는 휴대전화, 컴퓨터 등 디지털기기를 필연적으로 사용하여야 하고 그 디지털기기 내부에는 범죄자가 관련 내용들을 삭제하더라도 반드시 그 흔적이 남기에 범죄자들이 통제할 수 없는 영역인 디지털 기기에 축적된 데이터를 정밀 분석하면 효율적인 범죄 수사가 가능하다. 이러한 분야를 디지털 포렌식이라 한다.[4)]
이렇듯 디지털 포렌식은 마약사건에서 빠질 수 없는 중요한 증거획득 방법임에도 불구하고 현장수사관의 포렌식에 대한 이해의 부족과 포렌식 전문 수사관의 부족으로 초동수사의 성패를 가를 수 있는 범죄현장에서 포렌식 전문수사관의 부재는 현장수사관이 적법한 디지털 기기 수집과 초동수사를 동시에 진행해야 하는 업무 부담감이 있고 이러한 수사 환경에서 문제점이 발생될 수 있다.

또한, 마약사건은 긴급하게 발생하는 경우가 많고 신속하게 사건을 처리해야 되는 경우가 빈번하다. 신속하게 사건을 해결하기 위해서는 빠른 시간 내에 유의미한 증거를 발견해야 되고 그러기 위해서는 디지털 포렌식이 필수적인바, 디지털 포렌식이 마약사건 해결에 기여한 수사사례를 살펴보고 디지털 포렌식을 이용하여 마약사건 수사과정에서 효과적이고 신속하게 사건을 처리할 수 있는 활용 방안을 모색해야 한다. 아울러 디지털 포렌식 수사관이 없는 경우 적절한 디지털 기기의 수집절차가 무엇인지 제안하고 피의자의 안티포렌식 행위는 어떤 것들이 있고 그것을 차단할 방법은 무엇인지 알아본다.

2. 연구의 범위 및 방법

2.1. 연구 범위

거기에 가서 마약을 찾아가는 방식으로 매매함.
4) 이상진. 디지털 기반의 첨단 과학수사기술. 한국과학기술단체총연합회. 2013. 28면

본 연구는 여러 범죄 중 마약사건으로 그 범위를 한정하여 디지털 포렌식이 활용된 사례를 살펴보고 디지털 포렌식이 마약사건 해결에 효과적으로 기여할 수 있는 방안을 제안한다. 총 6장으로 구성하였다.
제1장 서론에서는 연구를 하게 된 목적과 연구범위를 살펴본다.
제2장에서는 마약과 마약수사는 무엇이며 일반수사와의 차이점을 알아보고, 마약수사의 현실에 대해 살펴본다.
제3장에서는 마약수사 현장의 문제점과 그 문제점을 해결하기 위해 디지털 포렌식의 필요성을 살펴보고 설문조사를 통하여 마약수사관이 디지털 포렌식에 대한 필요성을 어느 정도 공감하고 있는지, 포렌식이 마약수사에 얼마나 사용되는지에 대한 인식을 데이터화 시켜 마약수사에 있어서 디지털 포렌식의 필요성을 강조하였다.
제4장에서는 디지털 포렌식을 활용한 마약사건 수사사례를 통하여 디지털 포렌식이 사건수사에 어떻게 이용되었는가와 그 시사점을 알아본다.
제5장에서는 마약사건 수사 시 디지털 기기에 대한 효율적인 조사방법이 무엇이고, 사건유형별로 디지털 기기 우선 조사순위와 현장수사관의 효과적인 디지털 기기 수집절차 방안 모색, 피의자의 안티포렌식 행위의 유형과 그 대응방안 등 전반적인 마약사건의 수사절차를 제언한다.
제6장에서는 본 연구의 결론을 제시하고 연구결론을 통하여 마약수사관이 앞으로 디지털 포렌식을 마약수사에 어떻게 활용할 것인가에 대한 의견 및 마약수사가 앞으로 나아가야할 방향을 제시한다.

2.2. 연구방법

연구방법으로는 마약사건의 이론적 배경을 설명하기 위해 문헌연구와 사례연구, 설문조사 등을 통하여 마약사건에서 디지털 포렌식을 보다 효과적으로 이용 할 수 있는 방안을 연구한다.

■ 문헌연구
마약수사와 디지털 포렌식의 관계를 알아보고자 디지털 포렌식에 대한

국내외 선행자료를 참고하였으며 마약과 관련된 연구자료를 참고하였다.

■ 사례연구
디지털 포렌식이 마약사건에 적용된 유의미한 사례를 선별하여 해당 사건에서 디지털 포렌식이 주는 시사점을 정리하였다.

■ 설문조사
마약수사부서에 근무하는 수사관들을 상대로 디지털 포렌식에 대한 인식과 디지털 포렌식이 마약수사에 어떻게 이용되고 도움을 받았는지에 대해 설문조사하여 신뢰 높은 연구결과를 도출하였다.

Ⅱ. 마약수사와 현실

마약수사에 있어 디지털 포렌식이 어떻게 활용되는지 파악하기 위해서는 먼저 마약과 마약수사는 무엇이고 다른 수사와의 차이점이 무엇인지 알아봐야할 필요성이 있고, 마약수사의 현실을 그 수사방법적인 측면에서 과거와 현재로 나누어 비교해 봄으로써 앞으로 마약수사가 어떻게 진행될 것인지 예상해 본다.

1. 마약류 정의 및 종류

마약(narcotics)이란 용어는 무감각을 의미하는 그리스어 'narkotikos'에서 유래된 것으로 수면 및 혼미를 야기해 통증을 완화시키는 물질을 말하며, 그 동안 '마약'이라는 용어가 좁은 의미의 마약, 향정신성의약품, 대마를 총괄하는 의미로 혼용되어 왔으나 최근에는 이들을 총칭하는 표현으로 '마약류'라는 용어를 사용하고 있다.

마약류는 일반적으로 천연마약, 합성마약, 향정신성의약품, 대마 등으로 분류된다.

천연마약에는 코카인, 양귀비, 아편, 모르핀, 코테인 등이 있고,

합성마약에는 메치딘계, 그 구조의 유사성에 따라 페치딘(pethidine)계, 메사돈(methadone)계, 모르피난(morphinane)계, 아미노부텐(aminobuten)계, 벤조모르판(benzomorphan)계 등 5종으로 분류되며 그 중 페치딘계와 메사돈계가 가장 널리 남용되고 있다.

그 다음 **향정신성의약품**으로는 메트암페타민(일명 '필로폰, 히로뽕'), MDMA[5], LSD[6], 야바[7], GHB[8](일명 '물뽕') 등이 있으며 마지막으로 **대마**류에는 대마초와 해시시[9] 등이 있다[10].

2. 마약수사의 정의 및 특징

마약수사란, 마약을 그 대상으로 마약을 국외에서 국내로 운반하는 밀수입자와 국내·외에서 인터넷과 다크웹, SNS 등으로 판매하는 자 및 이러한 경로를 통하여 마약을 구매하는 자를 추적하여 검거하고 범죄수익을 환수하는 일련의 과정에 대한 수사를 말한다.

마약수사의 특징을 파악하기 위해서는 먼저 마약범죄의 특성을 잘 이해할 필요가 있다. 마약범죄의 특성은 모든 국가에서의 이동 및 소지자체가 금지되어 있기에 **거래의 은밀성**이 있고 단 한 번의 사용으로도 중독의 위험이 높아 그 **재범의 비율이 높고** 투약의 경우 피해자와 피의자가 동

---

5) 일명 '엑스터시'라 불리는 흥분제와 환각제 역할을 하는 암페타민계 화합물

6) 일명 'acid'라 하는데, 필로폰의 300배, 코카인의 100배에 달하는 효과가 있다.

7) 태국어로 '미친약'의 뜻으로 필로폰과 카페인이 혼합되어 있다.

8) 무색, 무취의 중추신경제로 '물이나 술에 타먹는 히로뽕'이란 말로 일명 '물뽕'이라 한다. 데이트 강간 약물로 불리기도 한다.

9) 대마초로부터 채취한 대마수지를 건조시켜 여러 형태로 제조한 것

10) 대검찰청 홈페이지, 검찰활동 중 마약조직범죄수사.

일하여 수사기관에 신고하기를 꺼려하기에 **암수범죄화**[11] 되어 있다.
이러한 이유로 마약수사는 범죄에 대한 사전정보가 입수되지 않으면 적발이 어려워 정보원 또는 유관기관과의 협조가 반드시 필요하고 다른 사건들에 비해 불시에 발생할 가능성이 높다. 또한 범죄자의 재범 비율도 높아 마약전과자의 꾸준한 관리가 필요하며 피의자를 검거한 후에도 해당 피의자에게 마약을 판매하거나 구입한 또 다른 피의자를 검거해야 되기에 사건이 단발성으로 끝나지 않는 등 여러 가지 특징이 있다.

3. 일반수사와 차이점

마약수사가 다른 수사와의 차이점은 피해자가 없다는 것이다. 예를 들어 살인사건의 경우 살인을 한 가해자와 살인을 당한 피해자가 있고, 강도 사건의 경우에도 폭행·협박으로 금전을 강취하는 가해자와 피해자가 있기 마련인데, 마약사건의 경우 마약을 판매하는 가해자도 그 마약을 구매하는 피해자도 서로 필요에 의한 목적으로 그 관계가 성립되기 때문에 가해자와 피해자라는 수식어를 붙이기가 곤란하다.
(누군가가 나쁜 목적을 가지고 몰래 마약을 먹이는 경우에는 마약을 투약한 사람이 범죄에 대한 고의가 없어 피해자라고 할 수 있겠지만 이 경우는 논외로 한다.)
이러한 이유로 범죄에 대한 신고가 거의 없고 범죄의 흔적을 밝히기가 매우 어렵다. 이것이 마약사건이 가지는 다른 사건과의 가장 큰 차이점이다.

뿐만 아니라, 사건의 긴급성도 그 뚜렷한 특징 중 하나인데, 위와 같이 마약사건의 경우 사건의 은밀성, 점조직화, 암수범죄화 등으로 인해 수사기관이 사건을 직접 인지하기가 어려운 부분이 있어 정보원들의 사전정보나 유관기관의 협조에 의존성이 높은 편이다. 물론 피의자를 조사하다

11) 해당 범죄가 실제로 발생하였으나 수사기관에 인지되지 않거나 수사기관에 인지되어도 용의자 신원파악 등이 해결되지 않아 공식적 범죄통계가 집계되지 않는 범죄.(위키피디아)

가 다른 피의자를 인지할 수 도 있지만 그것이 실제로 쉬운 일은 아니다. 그리고 그 정보가 시간적 여유를 주고 나오는 것이 아니라면, 즉 갑자기 정보원들에게 신고전화가 걸려 와서 마약거래가 성사 되었다던가, 외국에서 국내로 마약을 들어오면서 유관기관에 적발되는 경우처럼 사전 대비 없이 범죄자를 발견하면 거의 긴급체포로 이어져 다른 범죄에 비해 긴급체포 비율이 높은 편이다. 예를 들어 2019. 10.말 현재 인천지검에서 마약사건 관련하여 체포한 피의자건수는 총 64명으로 그 중 긴급체포건수가 53명이고 체포영장에 의한 체포건수가 11명으로 긴급체포 건수가 약 83%에 이른다. 최근 수사기관에서 피의자의 인권보호 등으로 긴급체포를 지양하고 있지만 마약사건은 사건의 긴급성이라는 특수성 때문에 긴급체포의 비중이 높다는 것도 일반 사건과 구분된다.

4. 마약수사의 현실

마약은 일제 강점기 조선총독부가 의사에게 모르핀 사용을 무제한 허용하여 많은 중독자가 생긴 것을 기반으로 해방이후 혼란한 시대를 틈타 일반에게 더욱 확대되었고[12] 1957년 마약법이 제정되고 현재에 이르기까지 사회 문제로 끊임없이 인식되고 있다. 하지만 계속해서 그 사용인구와 사용량은 늘어날 뿐 수사기관이 나서서 이를 제대로 해결하지 못하고 있다.

이러한 이유는 첫 번째로 수사방식의 문제다. 마약사범들은 대부분 음성적으로 마약거래를 하고 있어 수사기관이 적극적으로 범죄자와 범죄현장을 발견하기 어렵다. 마약사범의 경우 피의자와 피해자의 구분이 없기 때문에 수사기관에 신고 되는 비율도 낮아 대부분 정보원의 진술이나 유관기관의 협조에 의존하여 사건을 진행한다. 하지만 정보원 자체도 마약을 취급하는 사람들이 대부분이고 자신의 이익을 위해 수사기관을 이용할 뿐 사회정의를 위해서 정보를 주는 것이 아니기 때문에 수사기관의

12) 조석연, 해방이후의 마약문제와 사회적 인식(해방과 정부수립 초기를 중심으로). 2012. 11. 7. 310면.

입장에서도 그렇게 입수한 정보를 이용하기가 불편한 것이 사실이며 유관기관에 연락하여 정보를 달라고 애원할 수 도 없는 입장이다.
하지만 수사기관 입장에서는 마약범죄에 대한 사소한 정보하나가 수사의 중요한 단서가 될 수 있어 위와 같은 사실을 인식하면서도 정보원 또는 유관기관의 정보에 의존할 수밖에 없다. 즉 적극적으로 마약사범 근절을 위해 수사를 하기 보다는 수동적인 수사가 될 수밖에 없다는 뜻이다.
또한 범죄자를 검거하더라도 윗선에 대해 진술 하지 않으면 다른 중요한 증거를 확보할 수 있는 방법이 없어 확대수사가 될 수 없기에 위와 같은 환경에서는 마약사범을 근절하기에는 근본적으로 어려움이 많았다.

그러나 최근 마약수사 방식에 큰 변화가 찾아왔다. 이는 인터넷 환경이 변화하고 개인의 디지털 기기의 사용이 확대되어 인터넷으로 마약을 구입하는 시대가 도래됨에 따라 범죄자의 디지털 기기만 확보한다면 과거의 범행뿐만 아니라 현재와 미래에 대한 범행을 들여다 볼 수 있게 되었다. 따라서 검거된 범인이 윗선에 대해 굳이 말하지 않더라도 범인이 가지고 있던 디지털 기기를 분석할 수 만 있다면 해당 범죄자가 가지고 있던 범죄의 전말을 밝혀낼 수 있는 환경이 마련되었다.
과거 밝혀내지 못했던 범행사실도 지금은 시대의 변화로 디지털 기기를 분석하여 해당 범행 사실을 밝히는 것이 가능하고, 만약 피의자가 해당 디지털 기기에서 범죄와 관련된 부분을 삭제하더라도 그 기기에 대한 디지털 포렌식을 하면 복원이 가능하기에 큰 문제가 없다.

그러나 마약수사 현실을 범죄현장과 관련하여 디지털 포렌식의 관점에서 살펴본다면, 현장의 대부분은 디지털 포렌식 수사관이 참여할 수 없는 구조다. 이것은 마약수사의 특징이 긴급성에 있는 이유에 기인(起因)한다. 언제, 어디서, 어떻게 발생할지 예견할 수 없어 포렌식 전문 수사관의 지원을 요청할 수 없을 뿐만 아니라 발생한 사건이 늦은 밤이나 새벽이라면 포렌식 수사관의 신속한 지원을 기대하기가 어렵다. 사실 지원요청의 문제가 아니라 긴급을 다투는 상황에서 원거리에 있는 포렌식 수사관을

요청하고 현장 도착까지 소요되는 시간이 마약수사관에게 주어지지 않는다. 이런 상황에서 현장수사관은 범인체포, 신병관리, 압수된 마약을 관리하고 향후 디지털 포렌식으로 보강증거나 다른 공범 등을 찾기 위해 피의자가 사용하던 휴대전화 등 디지털 기기를 압수해야 한다. 하지만 압수 시 유의사항 등에 대한 교육을 받지 못한 수사관이 대부분이고 적절한 디지털 기기의 압수는 수사관 개인의 역량에 맡겨지고 있는 실정이다. 따라서 현장에서 마약수사관이 범할 수 있는 문제점이 무엇인지 고찰해 볼 필요가 있다.

Ⅲ. 현장의 문제점과 디지털 포렌식의 필요성

1. 마약수사 현장의 문제점

대검예규인 디지털 증거의 수집·분석 및 관리규정을 살펴보면,

『디지털 증거의 수집·분석 및 관리 규정(대검예규 제991호)』

제11조 (디지털 증거 분석 등 지원요청)

③ 정보저장매체 등에 대한 지원요청의 경우에는 별지 제3호 서식의 "정보저장매체 제출 및 이미징 등 참관여부 확인서"를 작성하고, 정보저장매체 등을 다음 각 호의 절차에 따라 봉인한 후 이를 지원 담당부서에 송부한다.

다만, 긴급을 요하는 등 부득이한 경우에는 정보저장매체를 기타 신뢰할 수 있는 형식으로 봉인하여 송부하되 별지 제6-1호 서식의 "압수(임의제출)물 송부지"를 작성하여 부착하는 등 요청번호, 요청기관, 내용물, 수량 등의 기재가 누락되지 않도록 유의한다.

1. 정보저장매체 등을 훼손 또는 변경의 우려가 없는 봉투에 넣는다.
2. 별지 제5-1호 서식의 “압수물 봉인지”를 작성하여 피압수자, 「형사소송법」 제121조 및 제123조에서 정하는 참여인(이하 ‘피압수자 등’이라고 한다) 또는 임의제출자의 확인·서명을 받은 다음 위 봉투에 부착한다.
3. 별지 제6-2호 서식의 “충격방지봉투”에 요청번호, 요청기관, 내용물, 수량 등의 정보를 기재한다.
4. 봉인한 정보저장매체와 작성한 “정보저장매체 제출 및 이미징 등 참관여부 확인서” 사본을 충격방지봉투에 함께 넣은 후 직접 또는 우송 기타 적절한 방법으로 디지털 포렌식팀에 송부한다.

제20조 (정보저장매체 등의 운반)

정보저장매체 등을 운반할 경우에는 정전기 차단, 충격방지 등의 조치를 취하여 그 매체가 파손되거나 기억된 정보가 손상되지 않도록 주의하여야 한다.

위 규정에 의하면 정보저장매체를 압수한 후 봉인 시 압수물 송부지에 대한 유의점에 대해서는 규정하고 있으나 현장수사관이 압수과정에서 유의할 점과 적절한 압수방법이 무엇인지에 대해서는 규정하고 있지 않다. 또한 제20조에 정보저장매체 등을 운반할 경우에는 정전기 차단을 요구하고 있지만 어떤 방법이 정전기 차단에 효율적인지와 그 방법이 무엇인지에 대해서는 기재가 없어 디지털 포렌식 교육을 받지 못한 현장수사관의 입장에서는 위 규정을 이해하고 획일적으로 실천하기가 어렵다.

따라서 첫 번째 문제점은 수사현장에서 관련교육과 전문 인력 부족에서 오는 수사관의 업무에 대한 부담의 가중이다. 대부분 사건에서는 디지털 포렌식 전문수사관이 동행하여 디지털 기기를 적법절차에 따라 압수하고 압수된 디지털 기기에 대해 분석 후 그 분석결과서가 사건담당 수사관에게 전달된다. 그러나 마약사건은 위에서 언급한 것처럼 긴급을 요하는 경우가 많아 사전에 포렌식 수사관을 요청하여 함께 현장에 가는 경우가 거의

없다. 따라서 사건현장에서 마약수사관이 범인체포, 신병관리, 압수된 마약류관리 이외에 범인이 사용하는 디지털 기기도 적법하게 압수하여 보관한 후 포렌식 수사관에게 전달하여야 한다. 디지털 포렌식에 대한 학습이 부족한 수사관이 압수된 디지털 기기를 무결성, 신뢰성 등을 인식하면서 보관에 주의를 기울여야 하는데 이 모든 것을 잘 소화하기가 어려울 뿐만 아니라 이를 해결하기 위한 교육의 기회가 자주 주어지는 것도 아니다.

「검·경 수사권 조정 합의문」[13]

> 4. 검사의 수사권 및 사법경찰관과의 수사경합 시 해결기준
>
> 나. ① 검사는 경찰, 공수처 검사 및 그 직원의 비리사건, 부패범죄, 경제·금융범죄, 공직자범죄, 선거범죄 등 특수사건(구체적 내용은 별지와 같다) 및 이들 사건과 관련된 인지사건(위증·무고 등)에 대하여는 경찰과 마찬가지로 직접적 수사권을 가진다.

두 번째는 수사능력 배양의 어려움이다. 최근 검·경 수사권 조정안으로 인해, 검찰의 강력사건에 대한 직접수사가 어려워지면서 마약사건을 다양하게 접해봐야 할 초급 수사관들이 경험할 수 있는 사건의 수가 급격하게 줄어들었고 경험 많은 수사관들은 검경 수사권 조정안으로 사기가 저하되어 마약수사 업무에 대한 관심과 열의가 많이 사라졌다.
현재 디지털 포렌식이 마약수사에서 중요한 증거획득의 방법으로 등장하였지만 디지털 포렌식에 대한 이해가 부족한 선임 수사관과 상대적으로 경험이 부족한 초급 수사관이 변화된 환경에 빠르게 적응하여 신속하게 사건을 해결하는데 어려움이 많다.

---

13) 청와대 보도자료『검경수사권 조정 합의문 서명식 개최』2018. 6. 21.

2. 디지털 포렌식의 필요성 등장

위와 같은 대표적인 문제를 해결하기 위해서는 범죄현장에 디지털 포렌식 수사관이 없어도 피의자로부터 디지털 기기를 적절하게 압수하는 방법을 공유하고 수사사례를 통하여 디지털 포렌식이 마약수사에 어떻게 활용되었는지를 간접적으로 경험해 본다면 수사관의 수사능력을 조금이라도 향상시킬 수 있을 것이고 여기에 더해 마약사건 피의자들이 자주 사용하는 안티포렌식 행위에는 어떤 것들이 있고 그것을 방어 할 수 있다면 수사관의 개인역량이 향상될 것이다.

이런 모든 것들이 디지털 포렌식과 연결되어 있고 디지털 포렌식에 대한 광범위한 이해와 사용만이 그 어려움을 해결할 수 있는 결정적인 요소가 된다. 디지털 기기의 대량보급과 5G 같은 인터넷 환경은 우리 사회의 많은 변화를 가져왔고 앞으로도 많은 변화를 가져다 줄 것이다. 이는 더 이상 범인을 특정하고 범인의 집 앞이나 자주 가는 술집, PC방에서 잠복하는 방법으로는 효과적인 마약퇴치가 어렵다는 의미다. 물론 범인을 검거하기 위해서는 위와 같은 행동이 필요하나 이는 범인 한명만 검거하기에 족한 방법이고 그 원천적 뿌리를 뽑기 위해서는 검거한 피의자의 윗선에 윗선과 하선의 하선을 모두 검거할 기술적인 요소가 있어야 한다. 그러기 위해서는 디지털 포렌식이 반드시 필요하다. 비대면 방식의 마약 매매방법에서는 범죄자가 필연적으로 휴대전화 등 디지털 기기를 이용할 수밖에 없고 디지털 기기의 특성상 범죄의 흔적이 고스란히 그 기기에 녹아있다. 단 한명의 체포만으로도 범죄현장에 없었던 공범 범죄자를 체포할 수 도 있고 피의자의 여죄를 밝혀낼 수 도 있다.
이처럼 과거에는 직접 범죄현장에 잠복하여 범죄가 발생하는 그 순간을 포착하여 범죄자를 체포하고 관련증거를 확보하였다면 지금은 범죄가 발생하는 순간을 놓치더라도 디지털 기기만 확보한다면 디지털 포렌식을 통해 의미 있는 증거를 확보할 가능성이 높아졌다. 따라서 포렌식 분석으로 범죄자가 어디서, 누구로부터 구입했는지 등을 추적하다 보면 관련 범죄

자들을 한 명씩 파악할 수 있고 최초 마약을 유포하거나 마약을 밀수입한 자를 검거할 수 있다. 이는 과거에 비해 마약 총책을 검거하는 비율이 상대적으로 높아 졌으며, 절대적으로 디지털 포렌식이 마약수사에 미치는 순기능이자 필요성이라고 할 수 있다.
디지털 포렌식은 마약수사에 있어서 필요한 증거를 밝혀내는데 유용한 방법이지만 피의자로부터 압수한 모든 디지털 기기에 대해 포렌식 분석을 하다보면 시간이 지체되어 수사의 골든타임을 놓치는 우(愚)를 범한다. 따라서 마약수사에 주로 사용되는 디지털 증거의 유형을 살펴보고 사건에 맞는 디지털 기기에 대한 포렌식을 요청하는 것이 더욱 효과적이다.

디지털 포렌식이 마약수사에 있어 결정적인 역할을 하고 있지만 실제 현장수사관은 디지털 포렌식에 대해 얼마나 알고 있고 그 필요성을 얼마나 체감하고 있는가에 대해 실제 마약수사관을 대상으로 설문조사를 실시하였다.

3. 설문조사

3.1. 설문조사의 목적, 범위, 방법

현장수사를 담당하는 마약수사관들을 대상으로 디지털 포렌식이 마약수사에 미치는 영향과 어떠한 포렌식을 주로 요청하는지, 마약사건에서 디지털 포렌식이 차지하는 비중 등을 알아본다.

검찰청 마약수사관 및 특별사법경찰관으로 근무하고 있는 수사관 총 42명을 상대로 인적 네트워크를 활용하여 설문조사를 실시하였고 설문 대상자들은 모두 마약수사에 경험이 있는 수사관들을 대상으로 실시하였다.

설문지는 크게 응답자의 근무지와 근무년수, 디지털 포렌식 관련성에 대한 설문으로 구성되어 있고 전국에 걸쳐 설문조사를 실시하는 조사의 특성상

대면조사와 비대면 조사를 병행했다.

3.2. 설문조사의 결과

【마약사건 수사에 있어서 디지털 포렌식의 비중 관련】

■ 마약수사를 하면서 디지털 포렌식을 요청한 경험이 있는가에 대한 질문에 ①‘있다’ 95.2%, ② ‘없다’ 4.8%

■ 디지털 포렌식이 마약사건 해결에 있어 중요한 역할을 하는가에 대한 질문에 ①‘매우 그렇다’ 90.5%, ②‘그렇다’ 9.5%

■ 디지털 포렌식을 통하여 수사에 중요한 단서를 찾은 경험이 있는가에 대한 질문에 ①‘있다’고 답변한 비율이 100%를 차지하여 마약수사관들은 마약수사에 있어서 디지털 포렌식이 매우 중요한 부분을 차지한다고 인식하고 있다.

구분	세부문항	빈도	%	유효 %
유효	① 있다	40	95.2	95.2
	② 없다	2	4.8	4.8
	소계	42	100.0	100.0
결측	무응답	0	0	
합계		42	100.0	

［표 3-1］ 디지털 포렌식을 요청한 경험

구분	세부문항	빈도	%	유효 %
유효	① 매우 그렇다	38	90.5	90.5
	② 그렇다	4	9.5	9.5
	③ 보통	0	0	0
	④ 그렇지 않다	0	0	0
	⑤ 매우 그렇지 않다	0	0	0
	소계	42	100.0	100.0
결측	무응답	0	0	
합계		42	100.0	

〔표 3-2〕 디지털 포렌식 역할의 중요성

구분	세부문항	빈도	%	유효 %
유효	① 있다	40	100	100
	② 없다	0	0	0
	소계	40	100.0	100.0
결측	무응답	2	2	
합계		42	100.0	

〔표 3-3〕 디지털 포렌식을 이용 수사에 중요한 단서를 찾은 경우

【마약수사관의 디지털 포렌식에 대한 인식정도】

■ 디지털 포렌식에 대한 교육을 받은 사실이 있는가에 대한 질문에 ② ‘없다’ 100%,

■ 범죄현장에서 디지털 기기 등 정보저장매체의 적절한 수집과정에 대한 교육받은 사실이 있는가에 대한 질문에 ②‘없다’ 100%를 차지하여 현장에 있는 마약수사관들은 디지털 포렌식에 대한 교육을 전혀 받지 못한 것을 알 수 있다.

구분	세부문항	빈도	%	유효 %
유효	① 있다	0	0	0
	② 없다	42	100	100
	소계	42	100.0	100.0
결측	무응답	0	0	
합계		42	100.0	

〔표 3-4〕 디지털 포렌식 교육 이수 여부

구분	세부문항	빈도	%	유효 %
유효	① 있다	0	0	0
	② 없다	42	100	100
	소계	42	100.0	100.0
결측	무응답	0	0	
합계		42	100.0	

〔표 3-5〕 정보저장매체의 적절한 수집과정에 대한 교육 이수 여부

【기타 사항】

■ 마약사건 현장에서 디지털 포렌식 수사관과 함께 수사를 진행한 경험이 있는가에 대한 질문에 ②‘없다’ 100%,

■ 위 항의 응답에 ‘없다’를 선택한 대상자 중 그와 같은 이유는 무엇인가에 대한 질문에 ①‘사건이 언제 발생할지 몰라 미리 신청을 할 수 없다’ 71.5%, ②‘포렌식 수사관이 부족해서 시간을 맞추기 어려울 것 같아서 19%, ③’포렌식 수사관이 필요 없어서‘ 9.5%,

■ 어떤 디지털 기기에 대해 포렌식을 요청했는가에 대한 질문에(복수선택) ①'휴대전화' 83.4% ②'노트북' 6.2% ③'테블릿 PC' 10.4%를 차지하였다.

구분	세부문항	빈도	%	유효 %
유효	① 있다	0	0	0
	② 없다	42	100	100
	소계	42	100.0	100.0
결측	무응답	0	0	
합계		42	100.0	

〔표 3-6〕 디지털 포렌식 수사관과 함께 수사를 진행한 경험

구분	세부문항	빈도	%	유효 %
유효	① 사건이 언제 발생할지 몰라 신청 못함	30	71.5	71.5
	② 포렌식 수사관이 부족해서 시간을 맞추기 어려울 것 같아서	8	19	19
	③ 포렌식 수사관이 필요 없어서	4	9.5	9.5
	④ 기타	0	0	0
	소계	42	100.0	100.0
결측	무응답	0	0	
합계		42	100.0	

〔표 3-7〕 위 응답에서 '없다'를 선택한 대상자 중 그와 같은 이유에 대한 답변

구분	세부문항	빈도	%	유효 %
유효	① 휴대전화	40	83.4	83.4
	② 노트북	3	6.2	6.2
	③ 테블릿 PC	5	10.4	10.4
	④ 데스크 탑	0	0	0
	⑤ USB 메모리, 외장하드	0	0	0
	⑥ 기타	0	0	0
	소계	48	100.0	100.0
결측	무응답	0	0	
합계		48	100.0	

[표 3-8] 포렌식 요청한 디지털 기기의 종류(복수선택)

3.3. 설문조사 분석

마약수사관들은 수사를 하면서 대부분 디지털 포렌식을 요청한 경험이 있고 디지털 포렌식이 마약사건 해결에 중요한 역할을 한다고 인식하고 있었으며, 디지털 포렌식을 통하여 수사의 중요한 단서를 찾은 경험이 있다고 응답하였다.

그러나 대부분 디지털 포렌식 교육수강의 경험이 없고 디지털 기기에 대한 적절한 수집과정에 대해서도 교육을 받은 사실이 전무하였으며, 마약사건 현장에서 디지털 포렌식 수사관과 함께 수사를 진행한 경험이 없다고 하였다. 이와 같이 대답한 주된 이유는 사건이 언제 발생할지 몰라 미리 신청을 할 수 없다는 것이 주된 이유로 나타났다.
위와 같은 설문조사를 통해서 디지털 포렌식이 마약사건수사에서 중요한 역할을 하고 있음에도 불구하고 수사관들이 관련교육을 제대로 받지 못해 사건현장에서 문제가 발생할 가능성이 높음을 알 수 있다.

Ⅳ. 디지털 포렌식 및 디지털 증거 활용 사례

1. 수사 기능별 디지털 포렌식 사용 유형

수사는 그 업무에 따라 경제범죄를 수사하는 부서와 교통사고를 수사하는 부서, 성폭력을 수사하는 부서 등 다양한 수사부서가 있고 이에 따른 범죄의 행태와 수사방법 및 디지털 포렌식 활용하는 분야가 달라진다.
위에서 언급한 부서는 주로 디지털 포렌식을 활용하는 부서로써 그 유형을 살펴보면, 아래 표와 같다.

기업수사	서버 삭제자료·숨김 자료 복구
교통수사	CCTV, 블랙박스 영상 복원
성폭력수사	몰래 카메라 영상증거 복원
마약수사	휴대전화 삭제기록 복원

〔표 4-1〕 부서별 빈번하게 사용되는 디지털 포렌식 유형

기업수사에서는 기업의 전산서버에서 각종 회계자료나 이메일, 기업자료가 저장된 파일서버로부터 데이터를 확보·분석하고, 교통수사에서는 삭제된 CCTV를 복원하거나 차량에 있는 블랙박스 영상을 복원, 성폭력수사에서는 소형카메라나 휴대전화를 이용하여 상대방의 동의 없이 촬영된 영상을 복구한다. 또한 마약수사에서는 범죄와 관련된 삭제된 자료를 휴대전화에서 복구하여 수사에 이용한다.

2. 디지털 포렌식을 활용한 마약수사 사례

2.1. 남미에서 대량 코카인 밀수사건

브라질 상파울루를 출발하여 아랍 에미레이트 두바이를 거쳐 인천국제공항에 도착한 루마니아인 피의자가 소지하고 있던 노트북의 내피 양쪽 벽면에 코카인 1.2kg이 은닉된 사실을 적발, 코카인이 들어 있는지 몰랐다고 범행을 전면 부인하는 피의자를 휴대전화 디지털 포렌식을 이용 공범과 범행일체를 밝혀내어 구속기소 한 사례다.

피의자는 브라질 언어를 몰라서 노트북 가방을 브라질에서 친구가 대신 구입해 주었다고 진술하며 그 가방에 코카인이 왜 들어 있는지 모르겠다고 부인하는 상황이었다. 이후 피의자의 휴대전화에 대한 디지털 포렌식 분석결과 ①삭제된 메시지에서 피의자가 코카인을 준 공범에게 '불법적인 물건을 가지고 입국하다가 한국에서 걸리면 감옥 가는 것이 아니냐'라고 질문한 내용, ②물건 배달 후 커미션에 대한 이야기를 공범과 주고받은 내용, ③한국에 머물 호텔을 직접 사이트(billigfüge.de)를 휴대전화를 통해 예약했다고 진술하였으나 피의자의 진술과 달리 복원된 휴대전화에서 위 사이트를 직접 접속한 기록을 발견하지 못한 점 등을 밝혀내 피의자와 공범간의 범행모의에 관한 것들을 확보하는데 성공한 사례다.

이 사례에서 주로 이용한 디지털 증거는 SNS다. 수천 개에 달하는 독일어와 영어로 표기된 SNS를 번역기로 돌려가며 그 내용을 해석 하는데 많은 시간이 소요되었다.

2.2. 대만에서 대량 필로폰 밀수사건

대만 폭력조직에서 조직원들이 SNS 등을 통해 불특정 일반인 27명을 금전으로 회유 또는 협박하여 비닐로 소분한 대량의 필로폰을 피의자의

신체에 붙이는 방법으로 대만에서 국내로 필로폰 약 62kg을 밀수, 이중 22명을 구속기소한 사례다.(필로폰 62kg은 약 200만 명이 동시에 투약할 수 있는 양으로 소매가 기준 2,080억 원 상당임)

피의자들은 공범으로부터 필로폰을 건네받을 때, 그 장소에 눈을 가리고 가는 경우가 대부분이어서 대만 현지에 있는 총책이나 조직원들의 이름과 필로폰을 건네받은 장소 등을 모른다고 일관했다. 피의자들의 휴대전화를 디지털 포렌식하여 삭제 된 데이터를 복원한 결과, 한국에 있는 호텔 사진과 필로폰 운반의 최종목적지 등 공범과 대화한 내용을 확보했다. 대부분 페이스 타임과 위챗 등으로 대만에 있는 책임자가 피의자들에게 필로폰을 운반·알선·판매를 지시하는 형태였다.
주목할 만한 사항으로는 대만 현지 조직원이 피의자들에게 휴대전화(아이폰)를 지급하고 비행기에서 내려 입국장을 통과할 때까지 페이스 타임으로 실시간 현지상황을 영상으로 체크했고, 세관 공무원에게 적발되는 순간 대만 현지에서 원격조종으로 휴대전화를 초기화 시켜 포렌식으로 복원할 수 없어 수사과정에 어려움이 있었다.

이는 일종에 피의자의 '안티포렌식' 행위로써 현장 수사관은 위와 같은 피의자의 행동을 미연에 방지해야 하므로 이러한 상황이 발생할 경우 현장에서 어떻게 처리해야 할지를 아래에 별도로 설명하겠다.

이 사례에서 유용하게 사용한 디지털 증거는 사진이다. 공범 간에도 서로 모르는 사람이라고 진술하였으나 각 공범자의 휴대전화를 압수하여 분석한 결과 동일인이 보낸 호텔사진이 각 휴대전화에서 복원되어 공범으로 특정하고 사건해결에 도움이 되었다.

2.3. 미국에서 대마초 및 대마오일 카트리지 밀수사건

최근 매스컴을 통해서 외국에서 생활한 전력이 있는 재벌 3~4세와 해외

유학생들 사이에 대마성분이 들어간 카트리지를 전자담배에 끼워 피는 것이 유행하여 많은 종류의 대마오일 카트리지가 국내로 밀수입 되고 있다. 본 건은 피의자가 미국에서 대마오일이 함유된 카트리지와 대마초를 국내로 밀수한 사건으로 피의자는 모든 범행사실을 자백하고 선처와 함께 공범은 없다고 주장한 사례였다.

그러나 휴대전화 포렌식 분석결과 여자친구와 카카오 톡에서 대마초와 대마오일에 대한 대화내용이 발견되어 피의자의 여자친구를 공범으로 의심하였고, 이 후 조사에서 여자친구와 공범관계를 추궁하였으나 여자친구는 본 건 마약과 아무런 관련이 없다고 주장하였다.
그러나 복원된 사진에서 여자친구가 대마오일 카트리지를 들고 있는 사진과 대마를 흡연한 뒤 기분에 대해 피의자와 주고받은 대화내용, 대마를 피우는 동영상 및 마약 운반여부를 묻는 메시지 등이 확보되어 이를 추궁한 끝에 자백을 받아내고 여자친구와 공범관계를 밝혀내는 중요한 증거가 된 사례였다.

이 사례에서 가장 유용했던 디지털 증거는 동영상이다. 20대에서 30대 초반의 성인 남녀가 휴대전화를 수년간 사용하다 보면 그 휴대전화 안에 저장되어 있거나 포렌식을 통해 복원된 메일과 SNS, 사진은 수백에서 수천 건에 달한다. 이러한 자료를 하나씩 분석하면서 사건과 관련된 증거를 찾으려면 많은 시간이 필요하다.
하지만 동영상은 사진에 비해 수사시간을 획기적으로 절약할 수 있다. 그 이유는 사진에 비해 영상의 개체수가 적고, 마약거래의 상대방은 사진보다 현물과 일시를 특정할 수 있는 동영상 전송을 선호함에 따라, 동영상 촬영일자 전후의 SNS를 추적하면 마약거래와 관련된 메시지들을 빠르게 확인할 수 있어 증거확보에 대한 시간을 단축시킨다.

2.4. 합성대마 밀수사건

최근 온라인을 통해 마약류를 구매하는 경우가 증가하고 있는 추세다. 본 건은 외국사이트에서 합성대마를 주문한 피의자를 체포하였으나 합성대마를 주문한 사실이 없고 외국에 있는 친구가 일방적으로 보낸 것이라고 범행을 부인한 사례다.

외국 인터넷 사이트에서 마약류를 구입해서 국내 배송 받는 방법으로 밀수하는 경우가 증가하고 있다. 마약이 들어 있는 소포가 세관에 적발되면 세관직원, 우체국직원, 마약수사관들이 함께 배송지로 가서 피의자를 체포하는데 이것을 실무에서는 **'통제배달'**이라고 한다. 최근 마약류를 매매하는 사이트에서 통제배달을 의식하여 적발될 경우를 대비해 적절한 변명과 조치법을 알려주기도 한다. 통제배달 후 범인을 체포하면 이전에 검거했던 피의자와 같은 말로 변명하는 사례가 반복된다.
이러한 이유로 현장에서 적발하더라도 차후에 자기 것이 아니라고 변명하는 경우가 부지기수여서 범행입증에 많은 어려움이 있다. 이때 디지털 포렌식은 피의자의 범행입증을 위해 매우 중요한 수단으로 작용한다. 본 사건의 경우 피의자가 가지고 있던 노트북을 포렌식하여 접속기록을 확인, 마약류를 판매하는 외국사이트에 접속한 기록이 적발되어 자백을 받은 사례다.
따라서 통제배달을 가는 현장수사관들은 피의자가 범행을 부인하는 경우 반드시 피의자의 휴대전화나 노트북 등 디지털기기 확인이 필수다. 특히 휴대전화만 압수하고 노트북이나 데스크탑을 소홀히 여기지 않도록 주의해야 한다.
이 사례에서 가장 유용했던 디지털 증거는 메일이다. 해당 사이트 관리자와 주고받은 메일을 확인하고 그 시간 때에 접속기록도 확인하여 피의자를 추궁하여 자백을 받아낸 사안이다.

2.5. 마약 투약사건

피의자는 캄보디아에서 필로폰을 투약하고 국내로 입국하려고 캄보디아 국제공항에 대기하는 동안 환각증세로 소란을 피워 해당 국가 이민경찰에서 대한민국 대사관으로 신고하여 국내로 인계된 사안으로, 공항에 도착한 피의자가 '이순신 장군과 이야기 한다고 말을 하며 웃고, 횡설수설하고 소리를 지르고 크게 웃다가 또 다시 괴성을 지르는 등' 마약 투약자가 환청, 환각증세를 보이는 모습과 흡사하였으나 피의자는 필로폰 투약자체를 부인한 사례다.

피의자는 환각상태가 지속되어 혼자서 엉뚱한 소리를 하고 창문을 바라보며 누군가와 대화를 하는 등 조사자체가 불가능하였으나 피의자의 휴대전화에 대해 디지털 포렌식으로 분석결과, 카카오톡에서 피의자에게 캄보디아행 비행기 티켓과 호텔비, 체류비 등을 제공한 윗선과의 대화내용이 있었고 그 대화에서 필로폰을 암시하는 내용을 발견했다. 또한, 포렌식 분석을 통해 남자친구로 추정되는 사람의 전화번호를 발견, 남자친구를 설득한 끝에 '피의자가 외국에서 마약과 관련된 일이 있었던 것 같다'는 내용의 진술을 청취하였다. 피의자의 남자친구는 피의자가 마약전력이 있다는 것을 인지하고 있었으며 피의자가 누군가의 제안으로 캄보디아로 여행을 가게 되었는데 그 불상자가 피의자에게 비행기 티켓과 호텔비, 체류비 등을 지급한 것을 피의자의 친구를 통해 이미 알고 있었다고 진술하였다.

이렇듯 피의자의 환각상태가 지속되어 피의자를 상대로 더 이상 수사를 진행할 수 없었지만 피의자의 휴대전화 분석과 남자친구의 진술을 통해 사건을 종결할 수 있었던 사례다.

3. 증거의 활용 및 디지털 증거의 사례별 활용 방법

범죄수사에 있어 현장을 보존하고 그 현장에서 관련 증거를 확보하고 그

증거를 통해 범죄자와 사건사이에 인과관계를 밝혀내는 것이 대략적인 수사의 흐름이다. 하지만 증거를 발견하더라도 그 증거와 범행사이에 인과관계를 밝혀내지 못한다면 증거를 발견하고도 피의자의 유죄를 입증하지 못한다. 따라서 그 증거를 어떻게 활용할 것인가도 수사에 있어서 매우 중요하다.

3.1. 물리적·생물학적 증거의 활용

프랑스의 에드몽 로카르드(Edmond Locard, 1877~1966)에 의해 “모든 접촉은 흔적을 남긴다(EveryContact Leaves a Trace)”라는 말로 표현되는 로카르드의 교환 원칙(Locard′s Exchange Principle)이 범죄수사에서 자주 인용되고 사용된다.
이는 어떤 범죄현장이든지 범인의 흔적이 어딘가에는 남아있으니 범죄수사에 있어서는 범죄현장을 잘 보존하고 분석하는 것이 범인을 특정하고 검거하기 위해서 가장 우선시 되어야 한다는 것이다. 그는 법과학 실험실을 만들어 실제 사건의 현장에서 발견되는 토양, 먼지 등의 미세증거물을 분석하여 동일성 여부를 판단, 범죄와의 관련성을 밝힘으로써 자신의 주장을 증명하였다. 그 후 체계적인 연구와 분석이 진행되어 학문적 틀을 갖추고 꾸준히 범죄수사에 이용되고 있다.

최근 유전자 지문이라고 불리는 DNA의 대조 방법으로 영구미제사건으로 남아 있던 화성연쇄살인사건의 용의자가 특정하였다. DNA 분석기법은 1984년 영국의 유전학자인 알렉 제프리스(Alec Jeffreys, 1950~)에 의해 개발되었으며 현재 범죄수사에 있어 없어서는 안 될 중요한 과학수사기법으로 자리 잡았다. 생물학적 증거물은 범인을 확증할 수 있는 수단이기 때문에 매우 중요하다. 즉, 범죄 현장에서 발견되는 눈에 보이지도 않는 증거물에서 범인의 유전자형을 성공적으로 검출하고 용의자와 비교함으로써 범인을 확인할 수 있다.
모든 범죄현장은 아무리 미세하다고 할지라도 범인의 행동으로 인해

조금은 변화된다. 이 때문에 우리는 범죄자의 신원을 확인하고 위치를 파악하여 정의를 구현 할 수 있다.

그러나 과학의 발달로 위 DNA분석에 버금갈 만큼 중요한 수사기법이 있는데 그것이 디지털 포렌식 분석기법이다. 이 디지털 포렌식으로 디지털 증거를 확보하고 수사에 활용하면 더 많은 범죄를 밝혀낼 수 있다.

3.2. 디지털 증거의 활용

마약사건은 갈수록 광역화·조직화·대형화 추세와 끊임없는 신종마약류의 개발과 보급 등으로 그 진압을 더욱 어렵게 만들고 있다. 갈수록 거래 수법이 지능화 되고 있고 국경 없는 인터넷을 통한 거래의 확산은 이미 국제사회에 큰 고민거리가 된지 오래다. 디지털 기기의 사용이 일상화된 지금 전통적인 수사방식으로 증거를 확보하여 사건을 해결하기란 여간 어려운 것이 아니다. 누구든 간에 동작 중인 디지털 기기의 시스템을 다루게 되면 해당 시스템은 반드시 변화가 발생한다. 즉 디지털 기기를 사용하는 범인은 반드시 그 흔적을 남기기 마련이고 그 흔적을 통해 수사단서를 발견하고 범인을 검거한다.

예를 들어 스마트 폰 SNS를 확인한다면 공범간의 대화내용을 알 수 있고, 인터넷 검색으로 범행방법 및 범인이 저지른 사건기사를 확인했는지 여부를 알 수 있을 뿐만 아니라, 사진촬영 또는 인터넷에서 사진 내려받기로 해당 범죄장소 확인, 네비게이션 이동내역 확인으로 범행장소를 특정 하는 등 마약수사에 있어서 디지털 증거의 중요성은 갈수록 높아지고 있다.

그러나 디지털 증거의 활용도가 높아지면서 디지털 증거에 대한 법원의 판단도 갈수록 엄격해 지고 있다. 최근 법원은 '前국정원장 자택 화염병 투척 사건'과 관련하여 그 판결에 주된 증거인 CCTV 영상들의 수집 과정 중

‘동일성과 무결성’을 확보하는 과정에 문제가 있다고 판단, 해당 CCTV의 증거능력을 부정하고 구속기소 된 피고인에 대해 무죄를 선고하였다.[14)]

따라서 디지털 증거를 수사에 활용하기 위해서는 그에 앞서 그 디지털 기기의 수집절차과정에 수사관들의 주의가 요구된다.

3.3. 디지털 증거의 사례별 활용 방법

마약사건은 크게 마약밀수, 매매, 투약으로 나눌 수 있고, 각 범죄유형 마다 디지털 기기를 이용하는 패턴에 차이가 있다. 이는 디지털기기에 개인의 일상과 사생활이 집약되어 있어 이를 분석하면 각 유형에 해당하는 피의자들이 디지털기기를 범죄에 어떻게 이용하는지 알 수 있다. 그 사용패턴의 차이점을 이용 수사에 활용한다.

---

14) 디지털 저장매체 압수물인 디지털 저장매체로부터 출력된 문건이 증거로 사용되기 위해서는 디지털 저장매체 원본에 저장된 내용과 출력된 문건의 동일성이 인정되어야 하고, 그 동일성이 인정되기 위해서는 디지털 저장매체 원본이 압수된 이후 문건 출력에 이르기 까지 변경되지 않았음이 담보되어야 하고(무결성), 특히 디지털 저장매체 원본에 변화가 일어나는 것을 방지하기 위해 디지털 저장매체 원본을 대신하여 디지털 저장매체에 저장된 자료를 ‘하드카피’·‘이미징’한 매체로부터 문건이 출력된 경우에는 디지털 저장매체 원본과 ‘하드카피’·‘이미징’한 매체 사이에 자료의 동일성이 인정되어야 한다고 판시한 대법원 2007도7267 판결을 인용하여 위 사건의 수사관들이 파일을 복사한 USB에 대한 봉인조치를 취하지 않았던 점, 위 사건 복사 파일 및 복사 파일을 스마트폰 카메라로 재촬영한 파일이 USB 내지 스마트폰카메라 저장장치에서 수사관들의 컴퓨터로 복사됨에 있어 그 복사된 수사관의 컴퓨터의 저장장치에 대한 봉인조치가 이루어지지 않았던 점, 수사관들이 디지털 증거수집에 관한 교육을 별도로 받은 적이 없고, 위 사건 복사 파일에 관하여 CCTV 원본 영상 파일의 해쉬값과 재촬영 파일에 관하여 스마트폰 카메라에 저장된 재촬영본 원본 파일의 해쉬값을 추출하여 기록하여 놓지 않은 점 등을 근거로 증거능력을 인정하지 않았다(서울중앙지방법원 2013고합805 현주건조물방화미수, 화염병등의처벌에관한법률위반 2014. 4. 25. 선고)
임정완, 살인사건 수사에서의 디지털포렌식의 활용방안에 관한 연구, 고려대학교 정보보호대학원. 2015. 6면

■ 밀수 사건

마약류의 대량 밀수는 주로 공항이나 항만을 통해 국내로 밀반입되고 최근 국내로 들어오는 대량 밀수사건의 경우 피의자가 대부분 국내에 연고가 없는 외국이어서 입국 후 빠른 시간 내에 피의자로부터 밀수된 마약을 건네받는 공범이 있다. 이들은 전화번호 등 개인신상의 노출을 서로 꺼려하는 경향이 있어 직접 연락해서 만나기보다는 제 3자를 통해 서로 만날 장소나 일시를 제공받는다. 따라서 휴대전화는 통화목적이 아닌 주로 사진과 SNS로 사용한다. 이러한 피의자의 휴대전화를 압수하면 통화내역이 거의 없는 경우가 많다.

피의자로부터 마약을 현장에서 압수하더라도 거기에 만족하지 말고 피의자의 디지털 기기를 확보 한 후 지체 없이 포렌식을 통해서 삭제된 이메일 및 SNS의 대화내용을 복구하여야 한다. 대화한 사람이 누구인지, 범행계획의 수립과 검거되었을 경우를 대비한 범행 부인에 대한 모의과정이 있었는지 파악하여 상선 또는 공범의 존재확인이 필수다.
또한 공범이 미리 국내로 입국한 후 출입국 공무원들의 점검강도가 소홀한 시간대를 파악하고 마약을 전달할 장소, 머물 호텔 등을 사전에 점검하여 사진으로 촬영, 직접 마약을 밀반입하는 피의자에게 사전에 사진 등으로 알려주는 경우가 많다. 그러므로 수사 시 통화내역 분석에 초점을 두지 말고 복원된 사진들을 통해 공범 또는 조력자를 만나는 일시, 장소 등을 발견하는데 중점을 두어야 한다.

이후 복원된 SNS 등 데이터를 분석하여 피의자의 범행동기가 단순 채무관계인지 아니면 돈을 벌기위한 자발적 범행참여인지, 폭력조직의 자금 확보가 목적인지 등을 확인하여야 한다. 또한 해당 마약이 우리나라를 경유하여 제3의 국가로 다시 반출되는 범행여부를 판단하여 국제공조가 필요한 수사인지도 신속히 파악하여야 한다.
특히, 마약사건의 경우 단순 투약자나 판매자를 검거하기 보다는 총책

즉, 최종 윗선을 검거하여 마약류의 국내밀수를 원천 차단해야 되기 때문에 해당 패턴을 기억하여 골든타임을 놓치지 말고 빠르게 수사를 진행해야 한다.

위에서 소개한 수사사례 중 대만에서 필로폰 밀수입한 사건의 경우 피의자의 휴대전화에 호텔사진을 확인, 그 호텔에 잠복한 후 공범자 중 일부를 체포한 사례다.

■ 판매·투약 사건

최근 마약 판매의 트렌드는 '던지기(드랍)'이다. 이는 위에서 잠시 설명한 바와 같이 판매자와 구매자가 서로 대면하지 않고 SNS를 통해 서로 정보를 교환한 후 매도자가 비트코인이나 금전을 제공받으면 마약을 숨겨 놓은 특정장소를 사진으로 전송하는 방법이다.
직접 만날 수 없으니 매수자의 입장에서는 판매자가 돈만 받고 물건을 넘기지 않을 것을 대비해 인터넷으로 '드랍'에 대해 많은 정보를 검색한다. 또한 매수자는 마약을 구매하기 전 인터넷으로 마약을 나타내는 은어나 낱말 등을 검색하는 경우가 많기 때문에(예를 들어 필로폰을 나타내는 '아이스, 얼음, 작대기, 빙두', 대마를 나타내는 '떨, 허브') 휴대전화나 컴퓨터 등에서 접속기록을 확인하는 것이 중요하다. 무엇을 검색하였고 어디에 접속하였는지에 대해 반드시 확인하여야 한다. 이는 피의자가 범행을 부인하더라도 추궁하는데 유용하게 사용되기 때문이다.

일반 구글이나 네이버 뿐 만 아니라 최근에는 다크웹을 통하여 마약을 매매하는 경우가 많기 때문에 다크웹 접속기록도 확인해야 한다. 대부분 마약 판매자와 매수자는 위와 같이 행동을 반복하므로 이를 확인한다면 범죄와 직·간접적으로 관련된 내용을 알 수 있다. 이러한 패턴들을 염두에 두고 수사관은 피의자의 혐의입증에 적극 활용해야 한다.

Ⅴ. 디지털 포렌식 활용을 위한 제언

1. 사건 유형별 디지털 기기 조사 우선순위 설정

1.1. 필요성

현대사회에 살고 있는 사람들은 과거에 비해 많은 디지털 기기를 소유하고 있다. 그 디지털 기기를 이용하여 사람들과 소통하면서 인간관계를 넓혀 가고 필요한 정보를 획득하여 삶의 질을 향상시키고 있다. 그러나 디지털 기기의 광범위한 보급과 사용을 범죄의 측면에서만 본다면 많은 시간과 기술적 어려움이 있어 그 만큼 수사관의 피로도가 높아지는 것이 사실이다. 마약수사에 있어서 모든 디지털 기기를 동순위에 두고 수사하기 보다는 유형별로 나누어 포렌식 전문인력이 부족한 현실에 입각한 대안을 마련하고자 한다.

사건을 수사하면서 증거수집에 대한 우선순위를 둔다는 것이 자칫 빈틈을 보이는 증거수집으로 판단할 수 있으나, 마약사건에서는 저 마다 다른 특성이 있기에 유형별로 나누어 디지털 기기에 대해 그 우선순위를 정해야 한다. 그 것이 체포부터 구속영장을 청구하고 기소하기까지 부족한 시간을 조금이라도 효율적으로 사용할 수 있는 방법이다.

1.2. 공항 및 항만을 통한 마약 밀수사건

공항 및 항만을 통한 마약밀수사건에서 1차적 우선순위는 당연 '휴대전화'다. 기술이 발전하는 만큼 휴대전화의 성능이 컴퓨터에 버금갈 정도로 향상되었다. 휴대전화에는 대량의 개인정보들을 담고 있을 뿐만 아니라 보안수준도 매우 높다. 휴대전화의 디지털 포렌식을 통해 범행의 동기와 방법,

공범의 유무, 범행자금의 흐름, 전과유무 등 다양한 내용을 확인 할 수 있다.
특히, 외국인의 경우 마약을 전달한 직후 본국으로 돌아가는 경우가 많아 총책으로부터 휴대전화를 제공받는 경우가 대부분이어서 공범과의 대화내용은 필연적이다. 비록 피의자가 태블릿 PC나 노트북을 보유하고 있더라도 거기에는 개인적인 내용이 많이 저장되어 있고 범죄와 관련된 유의미한 자료는 부재할 확률이 높다. 따라서 체포 후 구속영장을 청구하기 전까지 48시간이라는 짧은 시간에 피의자가 가지고 있는 디지털 기기를 모두 디지털 포렌식으로 복구·분석하는 방법은 한계가 있다.

1.3. 인터넷을 통한 마약밀수 사건

인터넷을 통한 마약밀수사건의 1순위는 '노트북 또는 데스크 탑 컴퓨터'다. 최근에는 인터넷 사이트에서 마약을 주문하여 자택으로 배달받는 사례가 많다. 휴대전화로는 다양한 정보의 검색 또는 장문의 이메일, 사진자료를 전송하기가 컴퓨터보다 불편하다. 이 때문에 국내·외 사이트에서 마약류를 구입하는 범죄자들은 휴대전화보다는 노트북과 태블릿 PC 등을 선호함에 따라 이와 같은 사례에서는 노트북 등을 우선하여 포렌식하여야 한다.
휴대전화를 통해서 마약을 주문할 확률이 없는 것은 아니지만 그 만큼 사용가치가 떨어지기 때문에 짧은 시간에 확실한 정보를 알아내기 위해서는 노트북 등을 먼저 포렌식 하는 것이 효율적이다. 간혹 휴대전화만 압수해서 피해자가 범행사실을 부인하고 휴대전화 포렌식에서 주문한 내역을 찾지 못하는 경우가 있으니 반드시 주의해야한다.

1.4. 마약 단순 판매 및 투약자 사건

마약 단순 판매사범과 투약사범을 검거할 때 우선순위는 '1.2'항과 같다. 다만 마약 단순 판매자와 투약자 검거 시에는 메시지가 아닌 사진에 중점을 두어야 한다. 최근 주된 마약 매매의 방식은 '드랍'이라고 위에서 설명한 바

있다.
따라서 판매자는 거의 마약이 숨겨져 있는 사진을 주소와 함께 구입자에게 메시지를 보내고, 매수자는 메시지를 확인한 후 내역을 삭제하기 전에 그 사진을 별도로 백업해 놓는 경우가 많다. 삭제된 메시지는 복원이 안 되면 의미가 없지만 매수자의 카메라에서 직접 촬영하지 않은 사진이면서 담벼락 또는 바위사진과 같은 장소를 특정할만한 자료를 확보한다면 추궁의 증거로 사용하는 것 도 좋은 방법이다.

1.5. 대마재배 사건

가끔 대마를 직접 재배하여 판매하는 경우가 있다. 이는 보편화 되지 않은 사례로 최근 주거용 오피스텔을 임차하여 대마를 직접 재배하고 판매한 유형이다. 대마를 직접 재배하기 위한 재배일지, HSP[15]전구 온도사항 체크, 대마의 발육상태 등을 사진으로 찍어 보관한 후 판매할 때 이용하기 위해서 이러한 데이터를 작성하는 경우가 많다. 이 때 주로 데스크 탑을 많이 사용한다. 노트북을 사용할 수 도 있지만 재배기계와 연동을 위해서는 용량과 사용이 좀 더 편리한 데스크 탑이 유용하다. 따라서 이와 같은 사례에서는 데스크 탑을 1순위로 확인하여야 한다.
위 와 같은 내용을 정리하면 아래와 같다.

휴대전화	⇒	태블릿 PC 및 노트북	⇒	데스크 탑
1. 공항, 항만 밀수사건 1. 단순 판매 및 투약사건		1. 인터넷을 통한 마약 밀수사건		1. 대마 재배 사건

〔표 5-1〕 사건 유형별 디지털 기기 조사 우선순위

15) hps(high pressure sodium, 고압나트륨) 전구는 씨앗의 초기발아용 및 식물성장 촉진용 등으로 활용되는 조명장치

1.6. 소결

수사에 있어서 빠지지 않고 증거를 수집하고 그 증거를 활용하여 유죄의 확정적인 증거로 사용하면 좋겠지만 애석하게도 체포부터 구속영장 청구 시까지 허용되는 시간이 너무 짧다.(물론 피의자를 구속하는 것이 수사의 목적이 되어서는 안 되겠지만 마약사건에서는 공범이 있을 수밖에 없는 실정이어서 불구속 수사를 하는 경우 공범에게 연락하는 등 수사에 혼선을 줄 수 있다.)
위에서 언급한 것처럼 마약사건은 일반 사건처럼 미리 사전영장을 받고 체포 한 뒤 수사를 진행하는 경우보다는 대부분 예고가 없고 불시에 발생하는 사례가 많다. 위 48시간 안에 유의미한 증거를 수집하고, 피의자 조사를 하고, 수사보고서를 작성하는 등 기록을 만들기 위해서는 48시간은 매우 제한적이다. 단시간에 최대한 많은 정보를 획득하고 영장을 청구하려면 '디지털 기기에서 어떠한 증거를 가장 효율적으로 수집할 수 있을까?'를 고민해야한다. 이러한 이유로 위 와 같은 사례에 알맞은 디지털 기기 조사의 우선순위와 그 이유를 제안해 보았다.

2. 범죄현장에서 효율적인 디지털 기기 수집절차 방안

2.1. 현장수사관의 디지털 기기 수집 시 발생하는 문제점

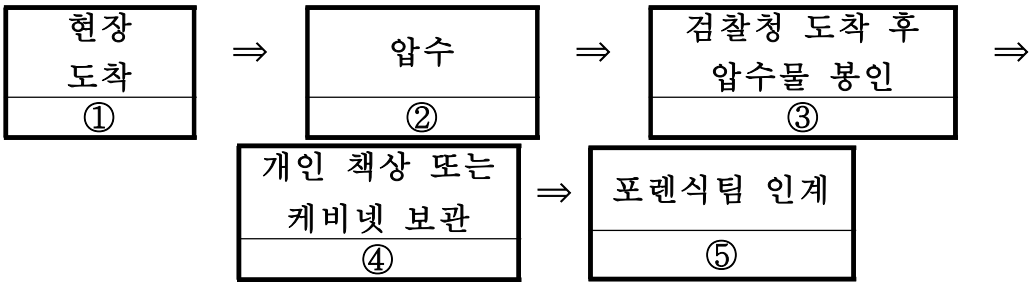
디지털 증거의 압수수색의 절차에서 일반적으로 ①필요한 정보의 저장매체를 찾아 압수하는 단계와 ②그 저장매체에서 다시 필요한 정보를 인식하기 위한 행위의 단계를 절차적으로 구분하는 것이 필요하다.[16]

일반적으로 포렌식 수사관과 함께 압수수색을 할 경우 ①,②를 디지털 포렌식 수사관이 담당한다. 대형사건의 경우 포렌식 수사관과 함께 범죄

16) 이완규, 디지털 증거 압수수색과 관련성 개념의 해석, 2013년. 112면

현장으로 가는 경우가 많지만, 마약범죄는 그 특성상 언제 발생할지 모르기 때문에 항시 포렌식 수사관과 함께 범죄현장에 나갈 수 없는 문제점이 있다. 현장수사관은 ①의 단계 뿐 만 아니라 ②의 단계로 넘어가기 위해 압수된 증거물을 잘 보관하고 무결성과 신뢰성이 깨어지지 않도록 적절한 절차적 조치가 필요하다.

그러나 대부분 현장수사관들은 포렌식에 대한 지식이 부족하여 압수된 디지털 기기를 보관하고 이를 포렌식 수사관에게 전달하는 과정까지 효율적으로 집행하기 위한 절차적 과정의 정립이 필요하다. 현재 현장에서 압수물을 수집하여 포렌식 수사관에게 전달되는 과정은 아래와 같다.



〔표 5-2〕 압수물이 포렌식 팀에 전달되는 과정

현장 수사관들의 경험으로 현장도착과 압수과정은 능숙하게 해결하고 있으나 현장에서 압수물을 거의 봉인하지 않는 다는 것이 문제점이다. 예를 들어 현장에서 피의자의 전화기를 압수한 후, 임의로 전화기에 있는 내용들을 살펴보고 사무실로 복귀한 후 피의자가 조사 받는 동안 다른 수사관은 휴대전화에 있는 자료들을 살펴보면서 필요한 증거들을 찾는다.

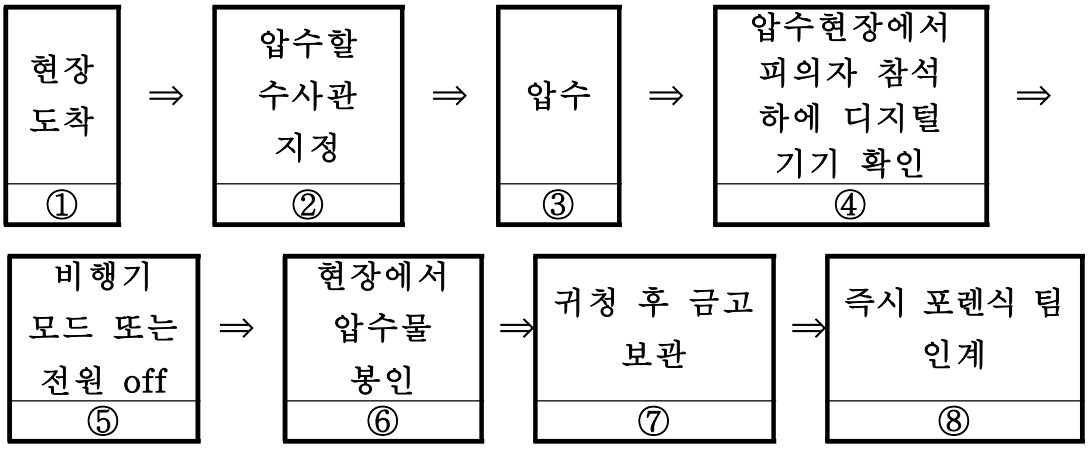
이때 조사받고 있는 피의자의 참여가 있을 수 없다. 디지털증거의 무결성 유지와 신뢰성과 관련하여 과연 이렇게 얻은 증거가 증거능력이 있을지 의문이다. 현장에서 즉시 봉인된 압수물이 아닌 피의자 조사종료 또는 익일 피의자를 소환하여 압수물 봉인절차를 진행한 후 그 증거물을 포렌식팀에 인계하는 경우가 종종 있다.

디지털 증거 수집 및 분석규정(대검예규 410호)에 따르면 제7조에 **'디지털 포렌식 수사관 등에 의한 압수·수색 조항'이 있는데 그 조항에는**

‘디지털 기기 등의 압수수색검증은 포렌식 수사관 또는 실무교육을 받은 직원이 하여야 한다. 다만, 긴급을 요하는 경우에 일반 직원이 대신할 수 있다고 규정하고 있다’ 고 규정한다. 그러나 위 규정에는 일반 수사관이 압수할 때 어떤 절차에 따라서 하라는 규정이 없다. 실무교육을 수료한 수사관이라면 별 문제가 없겠지만 현실은 그런 교육을 받지 못한 수사관이 훨씬 더 많아 현장에서 실수가 많이 일어날 수밖에 없는 구조다. 따라서 마약수사를 하는 현장수사관들이 범행현장에서 압수물을 수집할 때 유의해야 되는 사항과 절차들을 아래와 같이 제시해 보았다.

2.2. 현장수사관의 효율적인 디지털 기기 수집절차 방안

(포렌식 수사관이 없는 경우)



〔표 5-3〕 효율적인 디지털 기기 수집 절차 방안

① 현장에 도착한 수사관은 피의자가 사용하는 휴대전화 등 디지털 기기가 있는 지 확인하고 그 디지털 기기를 영장 없이 긴급압수 할 것 인지, 임의제출 받을 것인지 결정한다. 물론 영장 없이 압수를 하기 위해서는 긴급체포나 현행범체포가 선행되어야 한다. 이때 주의할 점은 빨리 체포여부를 결정하여야 한다는 것이다. 왜냐하면 체포 전에는 영장 없이 압수할 수 없어 전과가 많은 범죄자들은 압수되기 전에 휴대전화에 있는 관련 증거들을 삭제하는 경우가 많기 때문이다.

② 현장 도착 직후 선임팀장이 압수물을 관리할 수사관을 미리 지정하는 것이 필요하다. 왜냐하면 현장의 어수선한 분위기 때문에 아래 ③같은 일들이 많이 일어나기 때문에 누군가는 책임감 있게 처음부터 끝까지 압수물을 챙겨야 한다.(포렌식 수사관이 함께 간다면 필요 없을 단계이지만 그렇지 않은 경우에 반드시 해야 한다.)

③ 긴급압수하기로 하였다면 그 취지를 설명하고 피의자로부터 휴대전화를 압수한다. 이때 주의할 점은 마약전과가 많은 피의자들은 변호사를 선임한다는 이유로 휴대전화를 돌려받아 공범과의 대화내용을 삭제하거나 범행기록이 있는 관련 어플을 삭제하기도 한다. 따라서 변호사 선임을 핑계로 휴대전화를 돌려달라고 요구 한다면 수사관의 휴대전화를 사용하게 하던지, 아니면 수사관이 직접 피의자의 휴대전화에 연락처를 입력하고 피의자가 가급적 스피커로 통화하도록 유도해야 한다.(임의제출 받는 사례는 제외한다)

④ 마약사건에서는 체포 후 구속영장을 청구하기 까지 시간이 고작 48시간이기에 현장 수사관은 최대한 빨리 보강증거를 찾으려고 한다. 하여 수사관은 압수당시부터 지속적으로 피의자의 휴대전화를 들여다보며 증거를 보강하는 사례가 많다. 이는 압수와 동시에 휴대전화의 전원을 차단하거나 비행기 모드로 바꾸는 것을 선행하여야 한다는 지식의 부재다. 그리고 피의자의 참여하에 이루어지는 것이 아니기 때문에 문제가 될 수 있기 때문에 위 절차를 통해 피의자의 참여하에 휴대전화 등을 살펴보는 것이 좋다. 그렇지 않으면 향후 재판에서 증거능력에 문제가 되거나 휴대전화 전원이 계속 켜져 있어 ⑤와 같은 위험에 장시간 노출될 수 있다.

⑤ 전원이 켜져 있을 경우 수신되는 데이터로 인해 기존 데이터가 덮어씌워지거나 원격 삭제로 복구가 불가능하게 된다. 이러한 상황을 방지하기 위해 압수 후 배터리를 반드시 분리하여야 한다. 그러나 배터리 분리가 불가능한 아이폰 등은 종료기능을 통해 전원을 차단하거나 유심칩 분리

또는 비행기 탑승 모드로 전환하여야 한다. 그렇지 않으면 공범이 데이터를 원격으로 삭제하기도 한다. 데이터의 원격삭제 방법은 수사관에게 참고가 될 수 있어 아래에서 따로 설명하겠다.

⑥ 현장에서 휴대전화를 압수하더라도 곧바로 압수물봉인지에 봉인하거나 정보저장매체 등 제출확인서를 작성을 생략하고 사무실에 복귀하여 조사를 마친 뒤에 하는 경우가 다반사다. 심지어 피의자가 구속된 이후 압수물을 봉인하고 디지털 포렌식팀에 맡긴 경우도 있다. 이 경우 재판과정에서 피의자 측에서 무결성 등을 주장한다면 법적 증거로 채택되기가 어렵다. 이에 현장수사관은 반드시 압수 즉시 봉인하고 정보저장매체 등 제출확인서를 받아야 하며 휴대전화 확인이 필요하다면 반드시 피의자의 입회절차를 거쳐야 한다.

⑦ 금요일 오후나 주말에 압수하는 등 특별한 사정으로 압수즉시 증거물을 포렌식팀에 전달하기 어려운 사정이라면, 반드시 금고 또는 자물쇠가 있는 캐비넷에 보관해야한다. 이는 압수물이 멸실되거나 충격으로 인해 압수물이 손상되는 것을 방지하기 위함이다. 실제 압수물에 대한 관리부족으로 압수물을 잃어버린 후 찾은 경우가 종종 있다. 이러한 것을 방지하기 위해서라도 위에서 언급한 수사팀원 중 1인을 압수물을 전담 보관자로 지정하는 것도 좋은 방법이다.

⑧ 압수물을 포렌식팀으로 넘기기 전에 확인해야 하는 절차가 있다. 첫 번째는 봉인지가 손상되었는지 확인해야 한다. 압수물 봉인지는 특수처리가 되어 있어 일회성 접착만 허용한다. 따라서 재차 접착한 흔적이 발견되면 그 흔적으로 인하여 포렌식팀에서 분석거부를 할 수 있으므로 전달하기 전 봉인상태를 재확인할 필요가 있다.
두 번째는 정보저장매체 등 제출 확인서에 제출자, 제출일시, 장소, 기기의 종류, 제조사 등의 기재 및 피의자 참관여부를 반드시 확인하여야한다. 이때 피의자의 참관 의사표시가 있다면 포렌식팀과 일정을 조율하여 피

의자에게 통보하면 된다. 하지만 참관여부를 생략했다면 향 후 파일 추출과정에서 당사자의 참여가 보장되지 않았다는 사유로 재판상 증거능력에 문제가 될 수 있다.

제안한 절차 과정이 일반 포렌식 수사관이 하는 과정과 비슷하다고 생각할 수 도 있지만 현장수사관에게는 증거물을 압수하는 단계부터 포렌식 수사관에게 전달하는 과정까지 세심한 절차와 과정이 필요하다.

3. 안티포렌식 유형 및 대응

3.1. 안티포렌식 정의

안티포렌식(Anti-Forensics)을 한마디로 정의할 수 없지만 '포렌식 도구, 수사 및 수사관의 분석을 방해하기 위한 도구와 기술'[17] 또는 포렌식 기술에 대응하여 자신에게 불리하게 작용할 가능성이 있는 증거물을 차단하려는 일련의 활동[18] 정도로 정의할 수 있다.

3.2. 마약범죄자들의 안티포렌식 행위

안티포렌식은 단순히 정보 은닉행위부터 파일와이핑[19]과 디가우징[20] 같은 데이터 삭제방법 등 다양한 방법이 있다. 하지만 대부분 마약사건의 범죄자들은 이러한 기술적 안티포렌식 행위보다는 범죄행위 시 또는 검거

17) 신원, 안티포렌식 기법 분석을 통한 안티포렌식 대응 방안, 보안공학 연구 논문지 통권 42호, 2014. 12. 5. 606면.
18) DIGITAL FORENSICS WIKIPEDIA, ,안티포렌식 정의 및 설명, 위키피디아
19) 디렉토리 엔트리 정보를 가지고 있는 영역과 해당 클러스터의 디스크 영역에 난수나 0으로 중복하여 덮어쓰는 기법, 오미경, 디지털 증거 선별 압수·수색에 따른 문제점 해결을 위한 기술적 방안 연구, 서울대학교 융합과학기술대학원 2018. 16면
20) 강한 자기장을 이용해 하드디스크를 지워 복구가 안되게 만드는 기술(위키피디아)

직후, 본능적으로 본인의 범죄에 대한 증거를 인멸하는 행위, 수사기관이 자신의 범죄와 관련된 정보수집을 방해하거나 어렵게 하는 행위, 범죄자들끼리 사용하는 메세지를 암호화 하는 행위 등이 대부분이다.

예를 들어 휴대전화에 있는 범행과 관련되는 대화내용 또는 관련 어플을 삭제하는 경우가 많다. 특히 마약범죄자들은 복원이 어려운 '텔레그램'이라는 어플을 범죄에 많이 활용한다. 검거 직후 어수선한 틈을 타서 해당 어플을 삭제하거나 메시지 내용을 삭제 한다면 향후 범죄혐의 입증이 어려울 수 있으므로 휴대기기 압수 후 전원OFF 또는 비행기 모드로 전환해야한다. 더 나아가 다크웹을 이용하여 마약을 판매하거나 범죄자들 상호간에 암호화된 메시지를 주고받는 것도 수사기관의 범죄정보 확인을 어렵게 한다는 차원에서는 범죄자들의 안티포렌식 행위의 한 예라고 볼 수 있다.

위에서 예를 들었던 대만 사건에서 페이스 타임을 이용한 아이폰 원격조종 초기화 사례와 다음에 설명할 다크웹과 GPG 메시지를 사용한 마약매매 사례 등 최근 안티포렌식 행위가 증가하고 있으니 본 사례를 통해 수사에 참고하기 바란다.

3.3. 원격 데이터 초기화(Kill Switch) 및 대응방안

'킬 스위치'란 스마트폰 분실 및 도난으로 인한 피해를 최소화하기 위해 스마트폰 제조사가 단말기 제조 단계에서 도난방지 소프트웨어를 탑재하여 분실 및 도난 시 원격제어 또는 사용자 설정을 통하여 스마트폰을 사용할 수 없는 상태로 만들어 버리는 기능을 말한다. '킬 스위치'를 켜면 원래 주인이 비밀번호를 입력하기 전까지 절대 해당 기기를 사용할 수 없다. 그러나 최근 범죄자들이 킬 스위치의 본래 목적이 아닌 범죄혐의에 대한 증거를 인멸하는 수단으로 악용되고 있어 주의가 요구된다.[21]

21) 이주호·이종협, 휴대폰 킬스위치(Kill Switch) 기능에 대한 범죄악용에 따른

얼마 전 인천 00고등학교 3학년 학생이 수학시험 문제지를 훔친 것이 적발되어 그 학생이 사용하던 휴대전화를 압수하였는데 이 휴대전화에서 수학 문제지가 파일형태로 발견되자 해당 학생이 원격으로 해당 파일을 지운 혐의를 받고 있다는 내용의 뉴스가 나왔다.[22] 뿐만 아니라 위 사례 중 대만에서 대량의 필로폰을 몸에 은닉하고 국내에 도착하여 공항을 빠져나오면서 아이폰 페이스 타임을 이용하여 공범과 통화를 하다가 적발되자 공범이 원격으로 데이터를 삭제해 버린 사례처럼 범죄자는 수사관이 생각하는 것 보다 훨씬 자기방어에 철저하다.

이런 문제를 해결하기 위해 최근 국외에서는 원천적으로 범죄현장에서부터 전자통신을 차단할 수 있는 곳에 증거물을 넣어 포렌식 실험실로 운반하고 있다. 예를 들면 패러데이 백(Faraday Bag)이 있는데 여기에 증거물을 보관하면 모바일 장치를 외부 전파접촉으로부터 보호할 수 있다. 이 백은 전자파를 차단하기 위해 고안된 '차폐가방'의 일종이다.[23] 이 가방을 사용하면 네트워크가 원천적으로 차단되어 킬 스위치가 작동할 수 없기 때문에 범죄현장에 포렌식 수사관이 없는 경우에도 유용하게 사용할 수 있다.

그러나 일부 능력이 뛰어난 범죄자들은 더 지능적인 수법으로 자신들의 휴대폰이 압수당할 경우 좀 더 지능화된 킬 스위치 작동을 위하여 무선 네트워크 연결감지 도구를 설치한다. 그래서 실제 압수당했을 경우 설치된 툴에서 휴대폰이 충전기에 연결되어 있으나 아무런 사용이 없고 미리 설정한 시간만큼 무선 연결이 없는 것으로 감지되면 바로 초기화를 실행해 버린다. 이른바 일정시간 동안 전자파가 감지되지 않으면 스스로 '킬스위치가'가 작동되어 자폭장치 역할을 함으로써 휴대폰을 초기화 시키는 것이다.

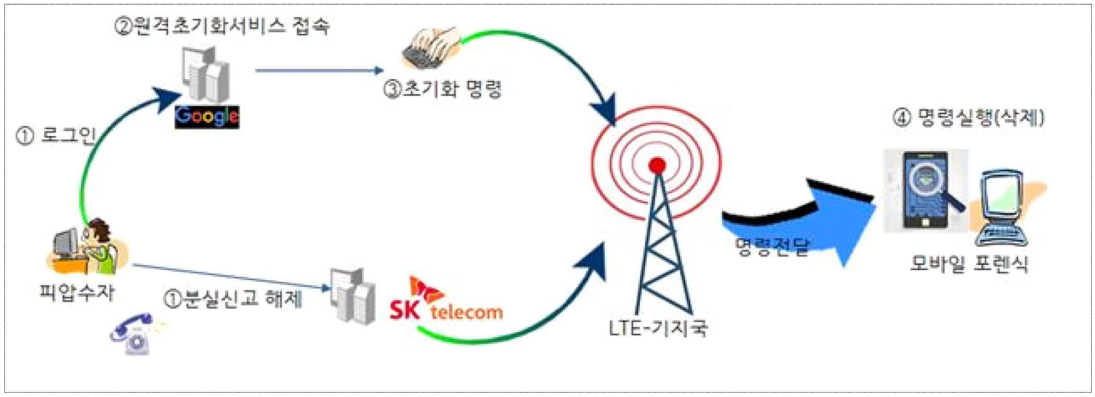
대책, 국방부조사본부, 2017. 12. 12. 256면

22) '시험지 빼내고 해킹으로 증거인멸, 컴퓨터 영재 오리발' MBC 뉴스, 2016. 7. 24.

23) 이주호·이종협, 휴대폰 킬스위치(Kill Switch) 기능에 대한 범죄악용에 따른 대책, 국방부조사본부, 2017. 12. 12. 256면

한편, 범죄자는 증거를 삭제하기 위한 다른 방안으로 통신사에 분실신고를 할 수 있다. 만약 분실신고를 한다면 압수된 휴대폰의 시스템 설정정보 자체가 비활성화 되어버린다. 포렌식이 가능하려면 압수된 폰에서 데이터를 추출해야 하는데 그러기 위해서는 공장초기화방지모드(일명 'FRP[24] LOCK' 모드)가 'OFF'전환이 필수적이다.
FRP 설정 값을 ON에서 OFF로 전환하려면 전원을 켠 다음 환경설정(OEM 잠금해제)값을 변경해야 한다. 하지만 휴대폰 상태가 모두 활성화 되어 있을 때만 이 모든 것이 가능하다. 그러나 범죄자가 분실신고를 한 상태라면 해당 화면이 자동으로 비활성화 되어 FRP LOCK 자체를 풀 수 없어 결과적으로 포렌식이 어렵다.

피의자가 자신의 휴대폰이 압수당한 후 고의로 분실신고를 하고 거기에 '킬 스위치'까지 실행했다면 어떻게 될 것인지 고찰해 볼 필요가 있다.



〔그림 5-1〕 킬 스위치 명령어가 유입되는 과정

위 그림에서 보면 피압수자는 자신의 집이나 또는 특정장소에서 웹페이지를 통해 킬 스위치 서비스에 접속하여 삭제 명령을 실행하는 한편, 범죄자는 수사관의 요구로 통신사에 분실신고 해제를 요청하였다고 가정하자. 데이터를 획득하려는 수사관은 분실해제 요청이 된 걸 확인하기 위해 압

24) 공장초기화 방지(Factory Reset Protect)

수한 휴대폰의 전원을 켤 것이다. 분실신고가 해제되었다는 것을 확인하기 위해서는 휴대폰을 켜야 기지국으로부터 해제 명령이 전달된다. 그런데 해제명령을 받는 순간 위 그림처럼 '킬스위치(원격초기화명령)'도 같이 유입되면서 해당 휴대폰은 데이터가 삭제가 동시에 실행된다.[25]

피의자가 원격으로 증거인멸을 시도할 경우 현장 수사관은 데이터 통신을 차단함으로써 1차적 보호는 가능하다. 이런 점에서 두 가지만 유의해도 '킬 스위치' 작동은 예방할 수 있다.
첫 번째 현장에서 휴대폰 등 디지털 기기를 압수할 경우 패러데이 백 같은 것을 사용하여 전파를 차단하는 방법, 두 번째 데이터 통신이 차단되는 차폐실에서 작업을 하는 방법이 있겠지만 마약수사 현장마다 차폐실을 마련할 수 없는 입장이다. 현장수사관은 휴대폰을 압수하면 전원을 끄거나 비행기 모드로 바꾸고 전파 차단백에 압수물을 보관한 후 디지털 포렌식 수사관에게 전달하면 된다. 이렇게 하기 위해서는 최일선 부서에 전파 차단백 보급이 선행 되어야 한다.

킬 스위치는 마약범죄 뿐만 아니라 일반범죄에도 자주 사용되고 있지만 현장수사관들은 킬 스위치가 무엇인지도 모르고 압수한 휴대폰에 아무런 사용 흔적이 없으면 피의자의 휴대폰에는 처음부터 아무런 디지털 기록이 없다고만 생각한다. 실제로 현장에서 휴대전화를 압수하여 사무실에 들어와 휴대전화를 보면 공기계처럼 아무것도 없는 경우도 있었다. 하지만 이것이 피의자의 안티포렌식 행위라고 생각하는 마약수사관이 과연 얼마나 있을지 생각하게 된다.

---

25) 이주호·이종협, 휴대폰 킬스위치(Kill Switch) 기능에 대한 범죄악용에 따른 대책, 국방부조사본부, 2017. 12. 12. 261면

패러데이 백

〔그림 5-2〕 전차파 차단이 가능한 패러데이 백

구분		기능 및 작동방식	적용기기 및 부가기능
제조사	삼성	· Reactivation Lock -기기에서 사전 설정 -공장초기화시 자동 작동	· 적용기기: 갤럭시 S5 모델부터 적용 · 웹(http://findmymobile.samsung.com)과 연동되어 원격 제어 - 단말잠금, 데이터 삭제, 위치 찾기 등
제조사	LG	· 기기에서 사전 설정 · 공장초기화시 자동 작동	· 적용기기: G3 모델부터 적용 · 웹(http://lge.mcafeemobilesecurity.com)과 연동되어 원격 제어 - 단말잠금, 데이터 삭제, 위치 찾기 등
	팬택	· V-Protection -기기에서 사전 설정 -USIM 제거 후 재부팅 시 자동 작동	· 적용기기: 베가 No 6, 베가 아이언, 시크릿노트, 시크릿 업 등 · 웹(http://www.pantechservice.co.kr)과 연동되어 원격 제어 - 잠금, 데이터 삭제, 통화내역 확인 등
	애플	· Activation Lock -기기에서 사전 설정 -공장초기화시 자동 작동	· 적용기기 : 아이폰(4,4S,5,5S,5C) · 원격제어(Find My iPhone) 웹서비스 운영 - 단말잠금, 데이터 삭제, 위치 찾기 등

〔표5-4〕 휴대폰 회사별 킬 스위치 탑재 현황[26)]

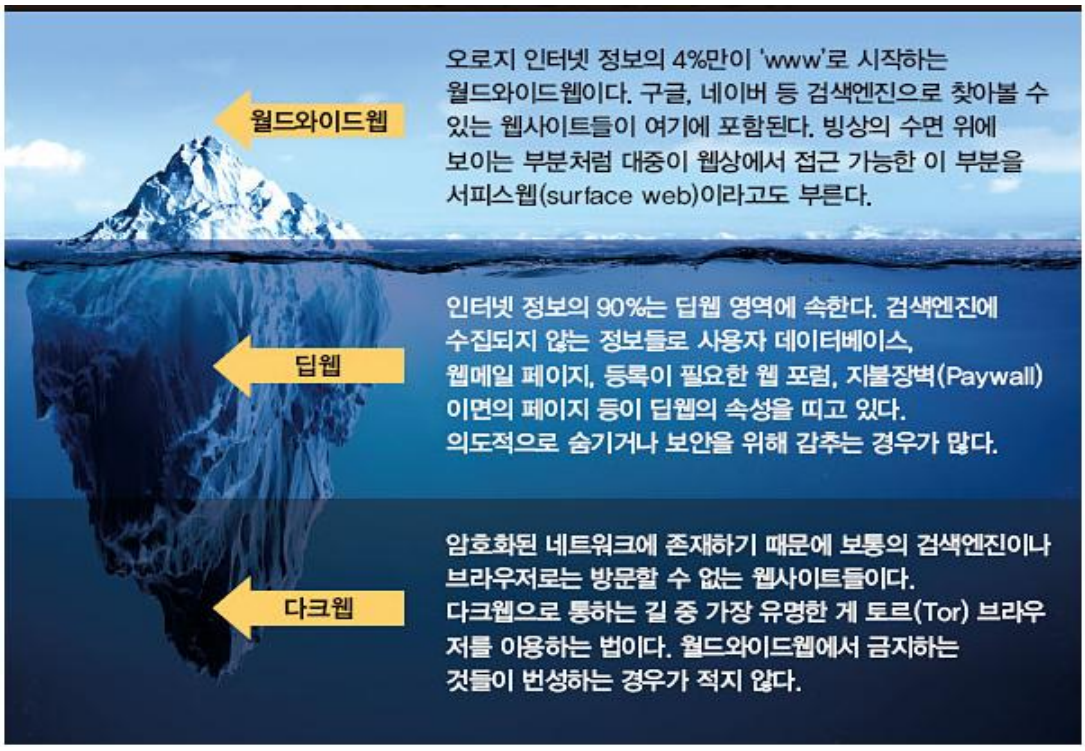
모든 휴대폰이 킬 스위치 기능을 갖고 있는 것이 아니므로 위 그림에 킬 스위치가 가능한 회사별 휴대폰 기종을 찾아보았다.

3.4. 다크웹(Dark Web) 및 보안메시지 사용

다크웹은 IP 추적이 불가능하도록 고안된 '은닉 인터넷 망'으로 일반웹 브라우저가 아닌 특정 브라우저를 통해서만 접속이 가능한 웹,[27)] 또는

26) IT 정보/뉴스, 휴대폰분실, 도난 및 해외 밀반출 피해 해결방법-킬스위치, 2017. 6. 23. https://newsroom76.tistory.com/52

‘인터넷 암시장’으로 다중 프록시를 사용하여 IP주소 등이 은닉되어 있는 고도로 익명화된 사설 네트워크(Private Network)를 일컫는다. 특정 브라우저를 통해서만 접근이 가능한 웹[28]으로 우리가 흔히 사용하는 경로로는 들어갈 수 없는 매우 은밀한 웹으로 정의하면 된다. 그림으로 쉽게 나타내면 아래와 같다.



〔그림 5-3〕 웹 사이트 구분[29]

다크웹에서는 마약, 총기, 아동포르노 등 일상에서 쉽게 접할 수 없는 다양한 물건들이 거래되고 있다. 그중에서 마약은 다른 어떤 물건보다 많이 거래되고 있는데 그 이유는 다크웹이 암호화된 네트워크에 존재하

27) 서울중앙지검 보도자료. 2018. 12. 21.
28) NEWSTOF. 마약·총기·포르노 유통되는 ‘다크웹’... 한국어 사이트 수 ‘세계 3위’ 2019. 3. 25.
29) chosun.com 사회. 범죄 온상 어둠의 웹사이트 ‘다크웹’을 아시나요. 2019. 10. 27.

기 때문이다. 다크웹으로 통하는 길 중 가장 유명한 것이 **토르(TOR, The Onion Router)** 브라우저 인데 이 토르에서 가장 많은 불법 사이트가 마약과 관련된 사이트이다.

아래 그림을 보면 무기거래 사이트가 42개, 불법 포르노 사이트가 122개, 마약거래 사이트가 무려 423개로 무기거래에 사이트에 약 10배에 해당하는 수치다.

다크웹 '토르'의 불법 사이트 현황

구분	웹사이트수
마약 거래 사이트	423
불법 금융	327
기타 불법	198
극단주의	140
불법 포르노	122
불법적 다크웹 연결 사이트	118
해킹	96
불법적 소셜네트워크	64
무기거래	42
폭력	17
총합	1547

[그림5-4] 다크웹 토르의 불법 사이트 현황30)

[그림 5-5] 다크웹에서 마약판매를 홍보하고 있는 글

30) 파이낸셜 뉴스. 국내서 차단한 범죄·마약정보 '다크웹'서 줄줄 샌다. 2016. 10. 28.

이처럼 많은 마약사이트들이 다크웹에 존재하고 있고 그 사이트를 통해 마약이 국내에 확산되고 있다. 그리고 마약범죄자들은 암호화된 보안 메시지를 사용하는데 대표적으로 GPG[31]메시지가 있다. GPG 메시지로 마약 매수 주문을 받고 그 대금을 '에스크로'[32] 방식으로 걸어 놓은 뒤 대마를 특정장소에 '드랍'(드랍방식은 위에서 설명한 바 있어 자세한 것은 생략한다.)하고 매수자가 이를 수령하면 판매자는 일정금액을 수수료로 차감한 후에 판매대금을 받는다.

피의자들은 공범이 수사기관에 검거되면 GPG 키가 저장된 컴퓨터 하드를 숨기거나 폐기하기도 하니 유의해야 한다.

3.5. 아이폰 텔레그램 어플 복원 방법

텔레그램은 러시아 최대 사회관계망 서비스(SNS)인 '브이깐딱제(VK)를 설립한 니콜라이 두로프와 파벨 두로프 형제가 2013년 개발한 오픈소스 메신저다. 이 텔레그램은 보안이 우수하여 삭제되면 복원이 어렵다는 이유로 일반 범죄자들뿐만 아니라 마약범죄자들이 이 어플을 많이 사용한다. 텔레그램은 포렌식을 하더라도 삭제된 데이터가 복원이 되지 않아 수사가 매우 어렵다. 하지만 최근 아이폰에 설치된 텔레그램을 기술적으로 복원하기 어려워 압수영장을 이용하여 텔레그램 메시지를 획득·분석한 사례를 소개한다.

아이폰의 최신 기종은 실제 DB 파일이 기기에 저장되어 있음에도 불구하고 백업 기능을 허용하지 않아 DB 파일 획득·분석이 불가하다. 하지만, PC 텔레그램이나 안드로이드 스마트폰의 경우 DB 파일이 존재하면 획득 가능한 방법을 우회 활용함으로써 정보를 획득한 사례다.

최근 수원지방검찰청에서 수사관이 피의자로부터 압수한 아이폰에 대

31) GNU Privacy Guard, 데이터와 통신을 암호화하고 서명할 수 있는 무료 툴
32) 구매자와 판매자 간 신용관계가 불확실할 때 제3자가 상거래가 원활히 이루어질 수 있도록 중계를 하는 매매 보호 서비스(네이버 지식백과)

해 비밀번호 해제를 요구하자 피의자가 이를 거부하였고, 압수영장을 근거하여 그의 아이폰 유심칩을 다른 공기계에 삽입, 그 아이폰(테스트폰)을 개통한 후 텔레그램 PC 버전을 컴퓨터에 설치, 간단한 인증절차를 걸쳐 텔레그램 서버로부터 해당 자료를 압수하였다.

위와 같은 방법을 사용하기 위해서는 압수수색검증 영장이 필요한데 압수수색검증 영장 청구 시 '압수할 물건'에 압수방법을 다음과 같이 특정 하여 영장을 발부받아 집행하여야 한다.

압수방법 기재예시
전화번호 '010-0000-####'를 이용하여 인증한 피의자의 텔레그램 계정과 관련하여 텔레그램 서버에 저장된 백업 파일 중 이 사건 범죄사실과 관련 있는 대화 목록, 문자메시지 등 대화내용, 첨부파일(사진, 동영상, 녹음파일, 문서 등)
압수·수색 방법
텔레그램 PC 버전의 로그인 입력 창에 피의자가 사용하던 '010-0000-####' 휴대폰 번호로 개통, 휴대전화로 전송된 인증번호를 텔레그램 PC버전에 입력하여 텔레그램 서버에 저장되어 있는 자료를 컴퓨터로 다운로드 받음

텔레그램 분석 필요성이 있는 경우, **『앞의 압수방법 기재예시를 참고하여 수사팀에서 영장을 청구하여 영장이 발부 되면 피의자에게 참관절차를 고지하고 반드시 참관 확인서를 작성하여야 한다.』** 아이폰에서 사용중인 USIM을 추출하여 안드로이드 폰에 삽입 후 텔레그램을 설치하여 인증절차를 거쳐 텔레그램을 분석 진행해야 한다.
단, 대화방의 대화내역 동기화가 이루어지지 않기 때문에 **압수가 필요한 대화방에 대해서는 스크롤을 이용 전체 데이터를 선택하여 내려 받아야**

한다. 그렇지 않을 경우, 각 채팅방별 마지막 대화만 획득이 되어 원활한 증거수집이 이루어지지 않음에 각별히 유의해야 한다. 텔레그램 비밀 대화방의 경우 **기기 인증 방식**이므로 다른 기기에서 획득이 되지 않는다.[33]

Ⅵ. 결　　론

오늘날 디지털 기기의 대량 보급과 인터넷 환경의 변화는 범죄수사의 측면에 많은 영향을 미치고 있는데 이는 마약사건에 있어서도 예외가 아니다. 특히, 마약사건의 경우 인터넷을 통한 대량 판매의 길이 열려 과거와는 비교할 수 없을 정도로 그 수요가 폭발적으로 증가하였다. 이는 마약거래에 대한 접근성이 용이해졌기 때문이다. 즉, 과거 마약거래는 주로 마약판매자와 구입자가 비밀스럽게 직접 만나 음성적으로 매매하는 방식이었다면, 현재는 개인의 디지털 기기를 이용하여 인터넷 웹사이트, 다크 웹사이트 등을 통해 마약판매상과 접촉하고 대금지급 방법의 다양화가 보편화되었기 때문이다.

이러한 사이버 세상의 범죄를 밝혀내기 위해서는 그에 사용된 디지털기기를 수집하고 그 기기에 대한 디지털 포렌식을 통해 증거를 확보하여 수사에 활용하여야 한다.

그러나 디지털 증거는 변조용이성 및 취약성 등의 특징으로 인해 취급에 주의가 필요하고 반드시 수집단계부터 전문 교육을 받은 포렌식 수사관이 참여하여야 한다. 그러나 현재 마약수사의 현실을 보면 마약수사의 긴급성과 포렌식 수사관의 부족으로 인해 디지털 포렌식에 대한 지식이 부족한 현장수사관이 디지털 기기를 수집하고 초동수사를 동시다발적으로 진행

33) 대검 디지털수사과 디지털 포렌식 연구소. 아이폰 텔레그램 우회 압수〔압수영장〕방법, 2019. 3.

해야 되기에 실수가 발생할 수 있다.

뿐만 아니라, 긴급체포가 주를 이루는 마약수사에서 48시간 내에 구속영장을 청구하고 공범을 검거하려면 빠른 시간 내에 관련증거를 수집하고 보강증거도 확보해야 한다. 하지만 디지털 포렌식 분석이 늦어지면 위에서 언급한 긴급성에 적절하게 대응하기 어렵고 수사가 지연되는 만큼 실체적 진실에 도달할 수 없다.

따라서 본 논문은 마약수사를 하는 현장수사관의 관점에서 마약사건의 긴급성에 대응하고 변화된 마약수사 환경에 익숙하지 못한 수사관이 디지털 포렌식을 통한 증거확보를 효과적으로 하기 위해 디지털 포렌식을 활용한 마약사건의 수사사례를 살펴보았다. 그 사례를 통해 디지털 포렌식이 마약수사에 어떻게 이용되었는지를 확인하였고, 긴급성을 요하는 마약사건에서 증거를 신속하게 확보하는데 필요한 유형별 디지털 기기 우선 조사순위를 명확히 하였다. 한편 범죄현장에 포렌식 전문 수사관의 참여가 없는 경우 발생할 수 있는 문제점과 그 해결을 위해 현장수사관의 효율적인 디지털 기기 수집절차를 제안하고 피의자의 안티포렌식 행위와 그 대응방안을 분석했다.

현재 마약수사의 환경은 많이 변화되었고 그 변화에 대응하기 위해서는 디지털 포렌식이 필수요소임을 현장수사관도 인식하고 있으나 관련교육이 정착화 되지 않았고, 이러한 이유로 디지털 포렌식에 대한 지식이 많이 부족한 것이 사실이다. 이는 마약수사관들의 설문을 통하여 디지털 포렌식의 필요성과 중요성을 재차 확인하였다.

예산과 인력이 부족하겠지만 검찰에서도 마약수사관의 디지털 포렌식 교육을 확대시키고, 포렌식 전문수사관으로 활동할 수 있는 기회를 제공할 필요가 있다.

끝으로 마약수사를 담당하는 국가기관으로 검찰청, 경찰청, 해양경찰청, 관세청, 국정원 등 많은 기관들이 있지만 각 기관은 정보를 공유하여 사건을 해결하기 보다는 실적으로 서로 경쟁하고 있는 실정이다. 마약범죄는 안일하게 대처하게 되면 **반드시 국가적 문제로 결부된다**. 따라서 각 기관들은 사건유형별로 처리한 수사내용 및 그 사례에 이용된 디지털 포렌식 기술과 디지털 증거의 사용례 등을 공유하여 디지털 포렌식에 대한 이해가 부족한 현장수사관들의 한계를 극복하고, 궁극적으로는 마약 수사기관들을 대상으로 공유할 수 있는 통합시스템을 도입함으로써 국내로 밀반입되는 마약퇴치에 적극 대응해야 할 것이다.

참 고 문 헌

임정완, 살인사건에서 디지털 포렌식 활용방안에 관한 연구, 석사학위논문, 고려대학교, 2015.

권오걸, 디지털 증거의 개념 특성 및 증거능력 요건, IT와 법연구, 2011.

이완규, 디지털 증거 압수수색과 관련성 개념의 해석, 연구논문, 2013.

이상진, 디지털 기반의 첨단 과학수사기술, 한국과학기술단체총연합회, 2013.

조석연, 해방 이후의 마약문제와 사회적 인식(해방과 정부수립 초기를 중심으로), 사학연구, 2012.

이승호, 경찰 수사상 디지털 포렌식 활용도 제고를 위한 기능분류체계 구축 연구, 석사학위논문, 연세대학교, 2018.

남재성, 경찰의 마약류 범죄수사 효율화 방안, 사회과학연구 17(1), 2010.

이가윤, 디지털 증거의 압수수색에 관한 연구, 한국컴퓨터정보학회 학술발표논문집 22(2), 2014.

임장일, 軍 수사에서 디지털 증거의 활용방안, 석사학위논문, 한양대학교 행정대학원, 2010.

김범식, 디지털증거 압수수색 및 증거능력의 쟁점과 과제, 국회입법조사처, 2016.

이주호·이종협, 휴대폰 킬스위치(Kill Switch) 기능에 대한 범죄악용에 따른 대책, 국방부조사본부(서울 04383), 2017.

김윤섭·박상용, 형사증거법상 디지털 증거의 증거능력(증거능력의 선결요건 및 전문법칙의 예외요건을 중심으로), 형사정책연구 26(2), 2015.

사법정책연구원·손지영·김주석, 디지털 증거의 증거능력 판단에 관한 연구, 〔JPRI〕 연구보고서 2015(8), 2015.

오미경, 디지털 증거 선별 압수·수색에 따른 문제점 해결을 위한 기술적 방안 연구(동형암호를 이용하여), 석사학위논문, 서울대학교, 2019.

윤혜령, 빅 데이터를 활용한 마약유통 인식에 관한 연구, 석사학위논문, 성균관대학교, 2018.
조정우, 마약류 투약자 중심의 마약수사 실효성에 관한 연구, 한국범죄심리연구 제15권 제2호(2019): 53-66, 2019.
구효송·신승균, 마약류 범죄의 문제와 대응방안, 한국범죄심리연구 제15권 제2호(2019): 113-126, 2019.
이보영·이무선, 마약범죄 처벌의 정당성, 법학연구 47, 2012.
대검찰청, 알기쉬운 디지털 포렌식 Q&A, 2015.
채희선, 마약청정국의 위상이 흔들린다 : 대한민국 마약을 말하다 연속보도 2019년 4월 18일~6월 7일 보도, SBS, SBS A&T, 방송기자 49, 2019.
대검예규 제991호, 디지털 증거의 수집·분석 및 관리규정, 2019.
대검찰청, 마약류범죄백서, 2018.
대검찰청, 『2018년 마약류 범죄백서』 발간, 보도자료, 2019.
이덕환, 이덕환의 과학세상(407) 과학수사, 디지털 타임즈 2013.
대검 디지털수사과 디지털 포렌식 연구소, 아이폰 텔레그램 우회 압수〔압수영장〕방법, 2019.
chosun.com 사회, 범죄 온상 어둠의 웹사이트 '다크웹'을 아시나요. 2019. 10. 27.