김일성종합대학학보(력사, 법률)
주체106(2017)년 제63권 제4호

콤퓨터망범죄와 관련한 전자자료의 수집과 분석에서 나서는 중요요구

신 정 민

위대한 령도자 **김정일**동지께서는 다음과 같이 교시하시였다.

《사건취급처리에서 과학성과 객관성, 신중성을 보장하자면 무엇보다도 과학적인 증거에 기초하여 사실관계를 정확히 밝혀야 합니다.》(《**김정일**선집》 증보판 제10권 123페지)

발생된 모든 범죄사건들은 반드시 과학적이며 객관적인 증거들에 기초하여 증명되여야 한다. 과학적이며 객관적인 증거가 없거나 불충분한 증거를 가지고 사실관계를 확정하려고 한다면 필연적으로 추측과 억측, 선입견과 주관주의가 작용하게 되며 결국 사건의 진상을 전면적으로 완전하게 밝혀낼수 없다.

다른 모든 범죄와 마찬가지로 콤퓨터망범죄를 적발조사하자면 그에 필요한 증거들을 충분히 수집하여 리용하여야 한다.

콤퓨터망범죄가 정보통신기술을 비롯한 과학기술을 리용하여 감행되는 범죄인것으로 하여 콤퓨터망범죄조사는 일반범죄사건에서처럼 손흔적, 발흔적과 같은 범죄자가 남긴 물리적흔적보다도 콤퓨터나 련관된 전자설비들에 남아있는 전자자료에 의한 조사를 기본으로 하여 진행되게 된다.

일반적으로 전자자료는 여러가지 정보를 매개의 규칙에 따라 수자화하여 콤퓨터에서 처리하기 쉬운 형식으로 표현한것인데 여기서 말하는 전자자료는 콤퓨터망범죄사건과 련관된 문자, 수값, 기호, 음성, 정지화상, 동화상 등의 수자화된 자료를 의미한다.

그런데 전자자료를 독립적인 증명수단으로 볼수 없는 조건에서 발생된 콤퓨터망범죄사건을 과학적으로 해명하기 위하여서는 사건과 련관된 전자자료들을 충분히 수집하고 그에 대한 분석을 진행하여 그 결과를 증거로 리용하여야 한다. 그러므로 수집된 전자자료에 대한 분석결과가 증거로서의 가치를 가지게 하기 위하여서는 수집과 분석에서 나서는 중요요구를 잘 알고 그에 기초하여 전자자료의 수집과 분석을 진행하여야 한다.

콤퓨터망범죄와 관련한 전자자료의 수집과 분석에서 나서는 중요요구는 무엇보다먼저 전자자료의 수집과 분석에서 법적요구를 철저히 지키는것이다.

전자자료의 수집과 분석과정에 법적요구를 철저히 지키는것은 수집과 분석을 통해 얻어진 결과가 증거로 리용되도록 하기 위한 필수적요구이다. 만일 전자자료의 수집과 분석을 법적요구를 지키지 않고 진행한다면 그 과정에 찾아낸 자료들이 증거로서의 효력을 상실하게 된다.

콤퓨터망범죄에서 전자자료는 순수 기술적자료가 아니라 콤퓨터망범죄사건해결에 절실한 의의를 가지는 증거자료인것만큼 전자자료의 수집과 분석은 형사소송법에 규제된 증거수집의 일반적요구에 따라 진행할수 있다.

전자자료의 수집과 분석에서 법적요구를 철저히 지키는데서 중요한것은 우선 법에서

규정한 사건담당 일군들과 해당 부문의 감정인, 전문가들이 전자자료의 수집과 분석을 맡아 진행하도록 하는것이다.

콤퓨터망범죄와 관련한 전자자료의 수집은 콤퓨터망범죄의 기술적특성으로 하여 사건담당자들과 전문기술일군들에 의하여 진행된다.

오늘날 정보기술의 비약적인 발전과 콤퓨터와 콤퓨터망이 사회생활의 모든 분야에서 광범히 리용되고있는것으로 하여 콤퓨터망범죄사건들이 수많이 발생하고있다. 이러한 콤퓨터망범죄사건들을 과학적으로 밝혀내자면 다른 모든 범죄사건들과 마찬가지로 사건을 직접 담당한 사건담당자들이 사건해결에 필요한 증거뿐아니라 전자자료를 주동적으로 찾아내기 위한 활동을 진행하며 찾아낸 전자자료를 리용하여 해당 사건의 진상을 과학적으로 밝혀내기 위한 소송상의 임무를 수행하게 된다.

일반범죄사건들과 달리 콤퓨터망범죄사건조사는 정보기술을 비롯한 발전된 과학기술적지식과 수단을 필수적으로 요구한다. 그런데 사건담당자들만이 전자자료수집을 진행하는 경우 사건과 련관된 전자자료를 원만히 수집하지 못할수 있다.

그러므로 콤퓨터망범죄와 관련한 전자자료의 수집은 사건을 담당한 법일군들과 함께 전문분야의 감정인, 전문가들이 진행하여야 한다.

콤퓨터망범죄와 관련한 전자자료의 분석은 수집된 전자자료에 대한 과학기술적해명을 진행하는 감정인의 소송법적 및 기술실무적인 활동이다.

콤퓨터망범죄조사에서 전자자료에 대한 분석을 진행하는 목적은 수집된 전자자료를 리용하여 사건을 과학적으로 해명하자는데 있다.

실례로 수집된 홈페지열람리력에 대한 분석을 통하여 범죄자가 언제, 어떤 사용자이름과 암호를 가지고 어떤 내용의 홈페지를 몇번 열람하였는가를 해명할수 있으며 체계일지에 대한 분석을 통하여서는 범죄자가 어떤 콤퓨터와 IP주소로 언제부터 언제까지 망에 침입하였는가 하는 문제들을 해명할수 있다.

전자자료들에 대한 분석은 전문과학기술지식을 필요로 하는만큼 사건담당자가 아닌 전문기술일군들에 의하여 진행된다. 이러한 활동을 소송법적으로는 감정이라고 한다.

전자자료들에 대한 분석이 전문기술일군들에 의하여 진행된다고 하여 그 활동이 순수 기술적활동인것은 아니다.

전자자료에 대한 분석 역시 하나의 감정활동인것만큼 형사소송법에 규정된 감정절차와 요구를 지켜야 하며 따라서 이것은 단순한 기술활동이 아니라 소송법적활동으로 된다.

전자자료의 수집과 분석에서 법적요구를 철저히 지키는데서 중요한것은 또한 전자자료의 수집과 분석과정에 공민의 헌법적권리와 리익이 침해되지 않도록 하며 비밀을 철저히 보장하는것이다.

콤퓨터망범죄의 주요한 특성의 하나는 범죄자가 침해대상에 물리적으로 접촉하지 않고 감행된다는것이다.

범죄자가 범죄현장에 접근하지 않고 수십～수천km 떨어진 곳에서도 콤퓨터망의 도움으로 범죄를 감행할수 있는것으로 하여 콤퓨터망범죄에서 사건현장은 범죄자가 범죄행위를 감행한 현장과 망공간에서 사건과 련관된 전자자료를 수집할수 있는 현장, 범죄의 후과가 발생한 현장으로 구분할수 있다.

전자자료의 수집이 이처럼 지리적으로 넓고 복잡한 환경에서 진행되고 분석과정에는

개별적공민의 사적비밀과 같은 자료들을 알수 있게 되는것만큼 공민의 헌법적권리와 리익이 침해되지 않도록 하는것이 중요하다.

콤퓨터망범죄사건에서는 사건과 련관되는것으로 의심되는 전자자료가 있을 때에만 전자자료의 수집과 분석의 대상으로 삼아야 한다.

전자자료는 대체로 콤퓨터의 하드디스크나 기억기를 비롯한 대용량기억기에 기억되여있다. 이러한 대용량자료들에는 사건과 관련된 자료뿐아니라 전혀 무관계한 자료들도 포함되여있다. 그러므로 어떤것은 사건과 관련된 자료이고 어떤것은 무관계한 자료이며 어떤것은 범죄자가 남겨놓은《범죄흔적》이라는것을 구분하여 전자자료의 수집과 분석을 진행하여야 한다.

이와 함께 전자자료의 수집과 분석과정에 비밀을 철저히 보장하여야 한다.

전자자료들은 모두 전자기매질속에 보관되여있는 수자화된 자료들이므로 독립적으로 존재할수도 있지만 대다수는 다른 자료들과 함께 존재하게 된다.

전자자료와 사건과의 련관성은 일반적으로 그 자료에 대한 분석을 진행하기 전에는 잘 알수 없는것만큼 감정인은 분석을 진행하는 과정에 사건과 련관된 전자자료뿐아니라 련관이 전혀 없는 자료들에 대하여서도 알게 된다. 이 경우 감정인은 사건과 련관이 없는 전자자료에 대하여서는 철저한 비밀을 보장하여야 한다.

콤퓨터망범죄와 관련한 전자자료의 수집과 분석에서 나서는 중요요구는 다음으로 전자자료의 수집과 분석에서 과학성을 철저히 보장하는것이다.

전자자료의 수집과 분석에서 과학성을 철저히 보장한다는것은 전자자료의 수집과 분석을 발전된 과학기술수단에 의거하여 진행함으로써 수집과 분석과정에 전자자료에 그 어떤 변화도 일어나지 않도록 한다는것을 말한다.

범죄자들은 현대과학이 이룩한 성과들을 저들의 범죄행위에 교묘하게 도용하고있으며 단순한 방법으로는 밝혀내기 어려운 교활한 범죄수법들을 적용하고있다. 이러한 범죄자들의 책동을 짓부시고 범죄를 신속정확히 적발처리하자면 반드시 과학적인 방법들과 현대적인 기술수단들을 리용하여 과학적이며 객관적인 증거들을 수집하여야 한다.

전자자료는 수자화된 자료인것으로 하여 사람의 감각기관으로는 그 존재여부에 대하여 확인할수 없는 자료이다. 그러므로 전자자료의 수집과 분석에서 종래의 전통적인 방법이나 낡은 기술기재, 수단들이 아니라 고도로 발전하고있는 정보기술을 비롯한 과학기술성과들을 도입한 기술기재, 설비들을 리용할 때만이 과학적으로 신속정확히 조사할수 있다.

전자자료의 수집과 분석에서 과학성을 철저히 보장하는데서 중요한것은 우선 과학성이 검증된 과학기술수단만을 리용하는것이다.

콤퓨터망범죄의 급속한 전파와 그 엄중성에 대처하여 콤퓨터망범죄를 적발조사하기 위한 연구사업이 활발히 벌어져 여러 나라들에서 자기 식의 쏘프트웨어 및 하드웨어제품들을 부단히 연구개발하고있다. 이러한 조건에서 개발제품들을 마음대로 리용할것이 아니라 반드시 해당 분야에서 그 과학성이 철저히 검증된 과학기술적수단을 리용하여야 한다.

전자자료수집과 분석을 위한 과학기술수단에는 사진기와 촬영기, 읽기대면부, 비트렬복사도구, 검사부호계산도구, 종합전자자료회복, 탐색, 분석프로그람과 전자자료원천보관설비, 전자자료검사전용콤퓨터 등이 있다.

사진 혹은 촬영은 증거고착수법의 하나로서 콤퓨터망범죄현장에서 수집한 각종 증거

물(콤퓨터, 기억디스크들, 망관련설비들, 각종 전자설비들)들에 대하여 영상적형식으로 고착시켜 사건조사에서 증거로서 리용할수 있게 한다.

읽기대면부는 수자읽기기술을 리용하여 전자자료가 변경, 파괴, 삭제되지 않도록 보호하는 기능을 수행하며 전자자료의 수집과정의 완전성과 객관성을 담보한다.

수집한 전자자료에 대한 분석결과와 수집한 원본전자자료와의 대조검사를 할 때에는 반드시 읽기대면부를 통하여 전자자료의 원시성과 완전성, 분석하는 사람이 무의식적으로 검사도중 전자자료의 변경, 복사 혹은 삭제 등의 조작을 진행하지 않도록 담보해주어야 한다.

비트렬을 복사하는 도구는 기억기에 보관되여있는 전자자료를 비트별로 복사하는 기능을 수행한다.

비트렬복사는 자료복사와 엄밀한 의미에서 차이난다. 사람들이 일상적으로 말하는 복사의 제일 작은 단위는 화일이지만 비트렬복사에서는 1대 1의 전면복제화상이다. 실례로 하드디스크 1의 자료내용 2를 빈하드디스크 3에 복제하면 하드디스크 1과 3의 내용은 다 2로 되는데 이때 하드디스크 3에 대한 자료회복조작을 진행하여 얻은 자료는 자료내용 3과 완전히 같지 않을수 있다. 비트렬복사조작은 하드디스크 1과 3에 대하여 그 어떤 회복자료도 다 2로 하며 두개의 하드디스크의 검사부가 완전히 같다는것을 담보해준다.

검사부호의 대조는 비트렬복사기술의 정확한 재현과정과 전자자료를 보존하는데 쓰인다. 이 기능은 검사부호 Hash값을 통해 실현할수 있다.

전자자료수집과 분석에 리용되는 Encase 등 종합적이고 강력한 기능을 갖춘 전자자료회복, 탐색, 분석프로그람과 같은 종류의 종합적인 프로그람들은 전자자료현시, 탐색, 회복, 제공, 자료검사, 분석, 영상 등 여러 기능을 매우 정확하게 수행할수 있다.

전자자료원천보관설비는 주로 수집된 전자자료에 대한 분석을 진행한 다음 그 원천(하드디스크, 기억기, 전자설비 등)들을 강한 자기마당의 영향이나 습기, 먼지 등과 같은 외부적영향으로부터 안전하게 보관하기 위하여 필수적으로 구비하여야 할 설비이다.

전자자료검사전용콤퓨터는 자료검사분석에 전문적으로 쓰이는 콤퓨터이며 일반적으로 2대를 리용하여야 한다. 한대는 호상련결망에 련결하고 다른 한대는 보통 분석을 진행할 때에만 쓰이며 다른 망과는 련결하지 않고 전문적으로 분석자료의 비밀을 보장하는데만 쓰인다.

전자자료의 수집과 분석에서 과학성을 철저히 보장하는데서 중요한것은 또한 전자자료의 수집과 분석과정에 원본자료에 그 어떤 변화도 가져오지 않도록 하는것이다.

전자자료의 수집과 분석에서는 전자자료의 원천으로 되는 물리적증거(하드디스크, 기억기 등)를 먼저 수집한 다음 그로부터 전자자료의 수집과 분석을 진행한다.

그런데 전자자료는 물리적증거보다 쉽게 삭제, 파괴, 변경될수 있는 특성을 가지고있는것으로 하여 수집된 원본증거물들을 그대로 리용한다면 수집과 분석과정에 원본증거물속에 보관되여있는 전자자료들이 쉽게 삭제, 변경, 파괴될수 있다.

이렇게 되면 여기에서 수집한 전자자료는 더이상 사건과의 아무러한 련관관계도 가질수 없으며 이에 대한 분석결과는 증거로서의 가치를 상실하게 된다.

그러므로 전자자료의 수집과 분석에서는 원본자료를 그대로 리용할것이 아니라 반드시 그 예비복사본을 리용하여야 한다.

전자자료의 복제기술은 자료내용의 손실을 가져오기때문에 자료가 기억공간속에서

보관위치가 변하지 않게 하기 위하여서는 원본기억기의 비트렬형식으로 예비복사본을 만들어야 한다.

콤퓨터망범죄와 관련한 전자자료의 수집과 분석에서 나서는 중요요구는 다음으로 전자자료의 수집과 분석을 전면적으로 신속히 진행하는것이다.

전자자료의 수집과 분석에서는 우선 전자자료의 수집과 분석을 전면적으로 진행하는것이 중요하다.

전자자료의 수집과 분석을 전면적으로 진행한다는것은 각이한 측면에서 빠짐없이 수집하여 그에 대한 분석을 진행한다는것을 말한다.

사건담당자들과 해당 부문의 감정인, 전문가들은 될수록 전자자료에 대한 수집과 분석을 전면적으로 진행하여 얻어진 전자자료들이 호상 련관되고 정확성을 담보해주도록 하여야 한다.

일반적으로 콤퓨터망범죄사건에는 항상 사건과 련관이 있는 여러가지 전자자료들이 포함된다. 매 전자자료는 각이한 측면에서 각이한 속성을 가지고 사건과 련관이 있다. 실례로 피해자에게 보내여온 전자우편을 통하여 범죄혐의자의 전자우편주소와 IP주소를 알아낼수 있으며 체계일지를 통하여서는 범죄자가 피해자의 콤퓨터에 침입한 시간, 탈퇴한 시간 등을 알아낼수 있는데 이러한 사실들은 사건을 밝히는데 도움이 되는 증거자료들이다.

특히 전자자료에 대한 수집을 전면적으로 진행하는것이 중요하다. 전자자료에 대한 수집을 전면적으로 진행하는것은 수집된 전자자료에 대한 분석을 전면적으로 진행하기 위한 전제로 된다.

전자자료에 대한 수집에서는 전자자료의 원천으로 되는 물리적증거(하드디스크, 기억기 등)수집에 선차적인 힘을 돌리며 수집된 물리적증거로부터 사건과 련관된 전자자료들을 빠짐없이 수집하여야 한다.

전자자료수집일군들은 때때로 많은 량의 전자자료가운데서 일부 섬세한 전자자료를 홀시하고있는데 정보기술환경에서는 이런 전자자료들이 수없이 존재한다. 그러므로 전자자료수집에서는 반드시 전자자료의 원천을 구체적으로 검사하고 다방면적이고 다각적으로 전자자료를 수집하여야 하며 그에 대한 분석을 전면적으로 진행하여야 한다.

이렇게 할 때만이 수집된 전자자료의 정확성과 사건과의 련관관계를 구체적으로 밝혀낼수 있으며 수집된 모든 전자자료들을 사건의 다른 증거와 결합하여 호상 검증하여 모순된 전자자료를 배제하고 최종적으로 사건을 밝혀낼수 있다.

전자자료의 수집과 분석에서는 또한 전자자료의 수집과 분석을 신속히 진행하는것이 중요하다.

일반적으로 발생사건수사에서는 범죄가 발생하면 제때에 범죄현장을 보존한 다음 신속히 현장검증과 군중료해사업을 진행하여 사건해명에 필요한 증거자료들을 수집하고 그에 기초하여 사건수사를 진행해나간다. 콤퓨터망범죄사건인 경우에 사건해명에 리용되는 전자자료의 기술적특성으로 하여 전자자료의 수집과 분석을 신속히 진행하는 문제는 더욱더 중요한 문제로 나선다.

전자자료의 수집과 분석을 신속히 진행한다는것은 사건과 련관된 전자자료들이 그 어떤 요인으로 변경, 파괴, 삭제되기 전에 필요한 모든 자료들을 수집하여 분석을 진행한

다는것을 말한다.

전자자료는 기본적으로 정보체계운행과정에 자동적으로, 실시간적으로 생성되는데 일정한 시간의 운행과정을 거치면 정보체계가 달라지게 되고 그 결과 전자자료의 변화를 일으킬수 있다. 례하면 망의 리력정보와 체계일지는 모두 크고작은 변화를 일으킬수 있으며 이런 정보는 시간이 지남에 따라 사건과의 련관관계를 정확하게 반영할수 없게 된다.

그러므로 전자자료의 수집은 일정한 시기성을 가지며 수집대상을 확정한 후에는 될수록 빨리 전자자료를 수집하고 그것이 어떠한 파괴와 손실도 받지 않도록 보장해야 한다. 전자자료형성으로부터 수집에 이르는 시간이 오랠수록 전자자료의 변화는 점점 더 커지게 된다.

실례로 IP주소는 항상 사건과 련관된 콤퓨터의 위치를 확정하는데 리용되지만 이런《망주소》는 신분증과는 달리 모든 가입자들과 고정적인 련관관계를 주지 않는다. 임의의 콤퓨터는 망에 련결된 후 한개의 IP주소가 자동적으로 할당되는데 이 콤퓨터가 망에서 탈퇴한 후 이 IP주소는 새로 망에 련결된 다른 콤퓨터에 분배될 가능성이 매우 크다. 그러므로 제때에 전자자료를 수집하여야 수집된 전자자료가 사건과의 련관성을 담보할수 있게 된다.

전자자료의 수집과 분석을 신속히 진행하자면 물리적인 증거들을 수집하여 그로부터 전자자료들을 수집하고 분석을 진행하는것과 함께 실시간전자자료수집을 진행하는것이 중요하다.

현대정보통신기술의 우점의 하나는 전송속도가 대단히 빠른것이다. 정보통신기술은 수십~수백km 떨어져있는 사람들사이의 통신을 즉시 그리고 신속히 보장한다. 그 결과 정보는 대단히 빠른 속도에서 전달되고 회수되며 인터네트에서 자료는 초단위에서 수천km를 지나 전송된다. 콤퓨터망범죄는 이러한 높은 통신속도를 리용하여 대단히 높은 속도에서 감행된다.

그러므로 콤퓨터망범죄가 감행된 후 전자자료의 수집과 분석을 진행하는것도 중요하지만 가능한껏 침입검출체계, 방화벽 등의 쏘프트웨어들과 기술기재들을 리용하여 실시간적으로 전자자료들을 수집하고 그에 대한 분석을 진행하는것이 효과적이다.

모든 법일군들은 콤퓨터망범죄와 관련한 전자자료의 수집과 분석에서 나서는 중요요구를 똑바로 알고 콤퓨터망범죄와의 투쟁을 과학적인 방법론을 가지고 벌려나감으로써 사건취급처리에서 과학성과 객관성, 신중성을 보장해나가야 할것이다.

실마리어 콤퓨터망범죄, 전자자료