[별첨1] 대검 예규 제805호 위반 상세내용

※ 이 사건 태블릿PC를 포렌식 분석한 2016. 10. 25. 시점에 적용되었던 **대검찰청 예규 제805호 '디지털포렌식 수사관의 증거 수집 및 분석 규정' 2015. 7. 16. 개정판**을 기준으로 합니다.

1. '대검 예규 제805호' 제9조 3항 위반

제9조 (지원요청)

① 일선 검찰청의 부장검사(부가 없는 지청의 경우 지청장)는 디지털 증거의 압수·수색·검증이 필요한 경우에는 디지털수사과장 또는 그의 위임을 받은 검찰공무원(이하 '디지털수사과장 등'이라고 한다)에게 메신저, 전화, 검찰메일 등의 방법으로 지원을 요청한다. <개정 2015. 7. 16.>

② 일선 검찰청 검사, 검찰수사관 등은 수사 또는 공소유지 등을 위하여 필요한 경우 디지털수사과장 등 또는 거점청 디지털포렌식팀 담당 검사에게 다음 각 호의 지원을 요청할 수 있다.

1. 디지털 증거의 분석·현출 <개정 2015. 7. 16.>
2. 제1호 내지 디지털 증거의 압수·수색·검증과 관련된 기술적 자문
3. 제1호 내지 디지털 증거의 압수·수색·검증과 관련된 법정 증언

③ **제1항, 제2항의 지원요청은 디지털수사통합업무관리시스템에 등록한다.** 다만, 제1항의 경우에는 디지털수사과장 등과 협의하여 결정된 지원내용 등을 디지털수사통합업무관리시스템에 등록한다. <개정 2015. 7. 16.>

제9조 3항에 따르면, 검사가 디지털수사과장 등에게 포렌식을 요청할 때에는 **'디지털수사통합업무관리시스템(이하 통합관리시스템)'**에 지원요청 내용을 필히 등록해야 합니다. 하지만 이 사건의 경우 검사가 송지안 수사관에게 지원요청을

하면서, 통합관리시스템에 등록하지 말 것을 특별히 지시했다는 것입니다.

2012년 개정 예규까지는 긴급을 요할 경우 통합관리시스템에 등록하지 않고 일단 메신저 등으로 지원요청부터 할 수 있는 예외조항이 있었지만, 그렇다고 해도 **긴급성이 소멸된 뒤에는 시스템에 등록하라고 규정했습니다.** 즉 등록하는 시점만 잠시 연기할 수 있을 뿐이지, 통합관리시스템에 등록하는 것은 필수라는 의미입니다. 이같은 예외조항은 2015. 7. 16. 개정 예규에서는 아예 삭제되었습니다.

따라서 이 사건 태블릿의 경우처럼 2016. 10. 25. 당시는 물론 지금까지도 통합관리시스템에 아무런 내용을 등록하지 않은 건 어떠한 사유도 감안하기 어려운 명백한 내규 위반입니다. 이처럼 포렌식 검증의 첫 단계인 '지원요청'에서부터 통합관리시스템에 등록하지 않았기 때문에, 이후 모든 포렌식 과정에서 현출된 자료나 근거 기록이 아무 것도 남지 않는 초유의 상황이 벌어진 것입니다.

2. '대검 예규 제805호' 제9조 4항 위반

제9조 (지원요청)

④ 제2항 제1호의 지원을 요청할 경우에는 정보저장매체 등을 훼손 또는 변경의 우려가 없는 봉투에 넣은 다음 **피압수자 또는 임의제출자의 확인·서명**을 받은 별지 제1호 서식의 **압수물 확인지를 위 봉투에 부착하고**, 별지 제2호 서식의 **압수물 봉인지를 이용하여 위 봉투를 봉인한 후 피압수자 또는 임의제출자의 확인·서명을 받아** 별지 제4호 서식의 정보저장매체 등 제출 확인서 사본과 함께 직접 또는 우송 기타 적절한 방법으로 대검찰청 디지털수사과 또는 각 거점청 디지털포렌식팀에 송부하여야 한다. 다만, 긴급을 요하는 등 부득이한 경우에는 다른 형식으로 봉인한 후 확인·서명을 받을 수 있다. <본항 신설 2015. 7. 16.>

제9조 4항에 따르면, 검사가 디지털수사과장 등에게 증거물을 전달하기까지 훼손 또는 변경의 우려가 없는 봉투에 증거물을 넣고 보관해야 하는데, 봉투 겉면에는 피압수자(임의제출자)의 확인·서명을 받은 압수물 '확인지'가 부착되어 있어야 합니다. 또한 피압수자(임의제출자)의 확인·서명이 있는 압수물 '봉인지'로 봉투 입구를 봉인해야 합니다. 긴급을 요하는 예외적인 경우에도 확인·서명과 봉인만큼은 필수입니다.

하지만 이 사건 태블릿의 경우, 피압수자(임의제출자)의 확인·서명도 받지 않았고, 제대로 봉인하지 않은 일반 봉투에 담아 송지안 수사관에게 넘겼다고 합니다. 이 역시 명백한 예규 위반입니다.

3. '대검 예규 제805호' 제19조 위반

> **제19조 (정보저장매체 등의 등록 및 책임자등의 참여)**
> ① 제15조 제1항 단서의 압수·수색의 경우 및 제9조 제2항의 분석 의뢰를 받은 경우에는 대상 정보저장매체 등의 **봉인을 해제한 후** 이에 기억된 정보에 대하여 **이미지 파일로 복제하여, 이를 디지털수사통합업무관리시스템에 등록**하고, 대상 정보저장매체 등은 **재봉인**하여 지원요청자에게 **인계**한다. <개정 2015. 7. 16.>

디지털 증거물을 복제한 이른바 '사본화(이미징) 파일'은 대검 예규 제805호 제19조에 따라 필히 통합관리시스템에 등록해야 합니다. 송지안 수사관에 따르면, 사본화 파일은 증거물의 무결성이나 신뢰성이 재판에서 문제가 될 경우 검찰 측이 내놓을 수 있는 원본 자료의 역할을 한다고 합니다. 따라서 통합관리시스템은 일종의 원본 보관용 시스템이라는 것입니다. 그만큼 사본화 파일의 통합관리시스템 등록은 필수입니다.

하지만 이 사건 태블릿의 경우, 검사의 지시에 따라 고의로 사본화 파일을 통합관리시스템에 등록하지 않았으며, 포렌식 종료 뒤 외장하드에 담겨 검사에게 전달한 것이 전부라고 합니다. 지금도 사본화 파일은 통합관리시스템에 등록되어 있지 않습니다. 이는 예규 위반을 넘어 검사의 직무유기, 증거인멸 정황이라고 할 수 있습니다. 디지털 증거물의 신뢰성, 무결성을 따질 수 있는 근거 자체를 은폐한 행위이기 때문입니다.

4. '대검 예규 제805호' 제22조 1항 위반

> 제5장 디지털 증거의 분석
> **제22조 (이미지 파일 등에 의한 분석)**
> ① 디지털 증거의 분석은 디지털수사통합업무관리시스템에 등록된 이미지 파일로 한다.

제22조 1항에 따르면, 포렌식은 디지털 증거물을 직접 분석하는 게 아니라, 증거물의 사본화(이미징) 파일을 분석하도록 되어 있습니다. 이는 증거물의 훼손·변경을 막기 위한 조치입니다. 그리고 포렌식에 사용될 사본화 파일은 통합관리시스템에 등록된 상태여야 합니다.

하지만 이 사건 태블릿의 경우, 처음부터 사본화 파일을 통합관리시스템에 등록하지 않았기 때문에, 대검 예규를 위반한 상황에서 포렌식 분석을 강행한 것으로 볼 수 있습니다.

5. '대검 예규 제805호' 제26조 1항 위반

> **제26조 (디지털 증거의 압수물 관리)**
> ① 디지털증거관리책임자 등은 해당 사건 주임검사가 **디지털수사통합업무관리시스템에 등록된 디지털 증거의 압수조서** 등 서류의 작성 및 입증서류의 구비가 용이하도록 필요한 조치를 취하여야 한다.

제26조 1항은 디지털 증거물의 압수조서 등 갖가지 서류를 통합관리시스템에 등록했다는 것을 전제로 한 규정입니다. 즉 압수조서 같은 서류들도 통합관리시스템에 등록돼 있어야 하는 것입니다. 하지만 이 사건 태블릿의 경우, 지원요청 단계부터 통합관리시스템에 등록하지 않았기 때문에 당연히 어떠한 서류나 자료도 시스템에 등록되지 않았습니다.

6. '대검 예규 제805호' 제24조 1항 위반

> **제24조 (분석결과 통보)**
> ① 디지털포렌식 수사관은 디지털 증거의 분석을 종료한 때에는 **분석보고서를 디지털수사통합업무관리시스템에 등록하고**, 지원요청자에게 통보하여야 한다. 다만, 긴급을 요하는 경우에는 구두 또는 전화 등 기타 방법으로 분석결과를 통보할 수 있으며, **긴급성이 소멸된 경우 즉시 분석보고서를 디지털수사통합업무관리시스템에 등록하여야 한다.**

제24조 1항에 따르면, 분석을 종료한 때에는 담당 포렌식 수사관이 분석보고서를 작성하여 통합관리시스템에 등록해야 합니다. 다만 긴급을 요할 경우 분석결과를 지원요청자에게 먼저 통보하고 등록을 잠시 미룰 수는 있지만, 이 경우에도 긴급성이 소멸되었다면 즉시 시스템에 등록해야 합니다.

하지만 이 사건 태블릿의 경우, 포렌식 소프트웨어가 자동 출력하는 데이터를 단순 나열한 문서가 전부여서 사실상 분석보고서라고 보기 어려운 수준입니다. 지원 요청할 당시 검사는 송 수사관에게 구체적으로 태블릿의 무엇을 분석해야 하는지 알려주지도 않았다고 합니다. 이로 인해 송 수사관은 전문가로서의 견해를 담은 분석보고서를 작성하지 않았으며, 당연히 통합관리시스템에도 등록하지 않았습니다.

실상은 이랬지만, 2016. 10. 24. 태블릿을 확보한 검찰은 이후에 마치 전문적인 분석을 통해 태블릿의 실사용자가 최서원으로 밝혀진 것처럼 수시로 언론에 흘리는 행태를 보였습니다. 최서원이 실사용자라는 결론을 정해놓고서 이에 부합하는 듯한 극히 일부 데이터만 선택해서 끼어 맞춘 수준을, 마치 대단한 첨단 과학수사로 전부 밝혀낸 것처럼 국민들의 눈을 속였던 것입니다.

7. '대검 예규 제805호' 제5조 위반

> 제5조 (디지털 증거의 신뢰성 유지)
> 디지털 증거는 **그 수집 및 분석 과정에서 이용된 도구와 방법의 신뢰성**이 유지되어야 한다.

제5조에서 말하는 증거물의 수집 및 분석 과정을 이 사건 태블릿에 적용한다면, 2016. 10. 24. 오후 7시 30분경 태블릿이 검찰에 임의제출된 시점부터, 2016. 10. 25. 오후 5시 15분경 포렌식 분석, 같은날 밤 태블릿이 재봉인되어 지원요청한 검사에게 인계되기까지 모든 과정이라고 할 수 있습니다.

앞서 언급한 바와 같이 디지털 증거물은 입수되자마자 훼손·변경의 우려가 없는 봉투에 담겨 피압수자(임의제출자)의 확인·서명이 기입된 압수물 봉인지로 밀봉

된 상태여야 하고, 봉투 겉면에는 피압수자의 확인·서명이 있는 압수물 확인지도 부착되어 있어야 합니다.

해당 증거물을 넘겨받은 포렌식 수사관은 증거물의 밀봉 상태를 확인하고 분석을 위해 봉인 해제를 하는데, 이같은 과정 전부를 사진이나 동영상으로 촬영해 놓아야 합니다. 그 뒤 사본화 과정도 촬영해야 하고, 사본화(이미징) 파일은 통합관리시스템에 등록해야 합니다. 포렌식 분석이 종료된 뒤에는 증거물은 다시 재봉인한 상태에서 지원요청자에게 인계해야 합니다.

결국 제5조가 말하는 도구와 방법의 '신뢰성'이라는 것은, 이 모든 과정에서 규정을 제대로 지켰느냐의 문제입니다. 하지만 이 사건 태블릿의 경우, 예규를 대부분 어긴 가운데 신뢰성을 담보할 수 있는 객관적인 근거나 현출물을 남기지 않거나, 일부 남겼더라도 통합관리시스템에 등록하지 않았습니다. 따라서 제5조에서 말하는 신뢰성은 이 사건 태블릿에서는 전혀 찾아볼 수 없는 것입니다.

8. '대검 예규 제805호' 제12조 위반

> 제12조 (과잉금지원칙 준수)
> 디지털 증거를 **압수·수색·검증**할 때에는 수사에 필요한 최소한의 범위에서 실시하여야 하고, **모든 과정에서 적법절차를 엄격히 준수하여야 한다.**

제12조는 디지털 증거물을 압수·수색·검증하는 모든 과정에서 적법 절차를 엄격히 준수해야 한다는 조항입니다. 대검 예규 제805호에서 규정한 모든 의무 조항에 대해 제12조는 **'적법 절차'**라고 명시하였습니다. 하지만 이 사건 태블릿의 경우, 거의 모든 규정을 고의로 지키지 않았기 때문에 객관적으로 **'불법 포렌식'**이라고 규정할 수 있습니다.

9. '대검 예규 제805호' 제4조 위반

> **제4조 (디지털 증거의 무결성 유지)**
> 디지털 증거는 **압수·수색·검증한 때로부터 법정에 제출하는 때까지 훼손 또는 변경되지 아니하여야 한다.**

제4조는 검찰이 디지털 증거물을 입수한 시점부터 봉인, 봉인해제, 사본화, 포렌식, 재봉인, 법정 제출 때까지 증거물의 훼손 또는 변경이 있으면 안 된다는 의무 조항이자, 증거물의 '무결성' 유지라는 대검 예규 제805호의 대원칙을 제시하고 있습니다.

하지만 이 사건 태블릿의 경우, 검사가 증거물을 입수하였다면 곧바로 봉인부터 한 뒤 아무런 접촉을 하지 않아야 함에도, 증거물의 '무결성'을 지키려는 노력은 처음부터 할 생각이 전혀 없었다는 것이 드러났습니다.

구체적으로 2016. 10. 24. 오후 7시 30분경 태블릿이 검찰에 임의제출된 직후 노승권 당시 서울중앙지검 1차장은 JTBC 기자와 문자를 주고받으며 태블릿을 임의로 접촉·구동하는가 하면(**별첨2 사례①**), 2016. 10. 25. 오후 5시 14분 포렌식 분석이 있기까지 태블릿을 켜놓은 채 지속적으로 구동시키고(**별첨2 사례②**), 포렌식 분석 30분 전까지 검사는 문서파일 30여건을 열람하였습니다(**별첨2 사례③**).

이같은 사실은 민원인의 재판에 제출된 증거와 2017. 11. 15. 이 사건 태블릿을 재차 검증한 국과수의 포렌식 감정결과에 고스란히 포착되었습니다. JTBC와 검찰은 태블릿의 내부 파일이 2016. 10. 24. ~ 10. 25. 대거 변경된 사실에 대해 태블릿을 켰을 때 자동 발생하는 현상이라고 주장하지만, 이는 **문서파일까지 열람한 기록(별첨2 사례③)** 하나만으로 반박이 가능합니다.

이같은 고의적인 무결성 훼손으로 인해 2017. 11. 15. 작성된 국과수 감정서는 **"태블릿 전체에 대한 무결성이 유지되지 않음"**이라고 적시하였습니다(**별첨2 사례④**), 만일 무결성이 유지되었다면 검찰이 포렌식할 때의 해시값과 1년 뒤 국과수가 재차 포렌식할 때의 해시값이 똑같이 유지되어야 하지만, 이 사건 태블릿의 경우 해시값이 바뀌어 버렸습니다(**별첨2 사례⑤**).

해시값이 바뀐 결정적인 이유는, 재봉인되어 밀봉 상태로 있어야 할 태블릿이 2016. 10. 31. 오후 2시 47분경 무단으로 다시 켜져 시스템파일에 대거 수정·삭제가 벌어진 일 때문인 것으로 추정됩니다(**별첨2 사례⑥**).

검찰은 2016. 10. 25. 포렌식 분석을 완료하였고, 이날 사본화 파일까지 만들었기 때문에 6일이 지난 2016. 10. 31. 태블릿을 다시 꺼내서 켤 이유가 없었습니다. 만일 미진한 부분을 보강 검증하고자 했다면, 이미 만들어놓은 사본화 파일을 활용해야 하는 것입니다. 그럼에도 봉인된 태블릿을 다시 꺼내서 구동시켰다는 것은 **불순한 목적의 증거조작**까지 의심해야 할 상황입니다.

디지털 포렌식 과정에서 준수해야 할 대검찰청 예규 제805호 '디지털포렌식 수사관의 증거 수집 및 분석 규정' 제4조, 제5조, 제9조 3항, 제9조 4항, 제12조, 제19조, 제22조 1항, 제24조 1항, 제26조 1항의 총체적인 위반