

변 론 요 지 서

사 건 2018노4088

정보통신망이용촉진및정보보호등에관한법률위반(명예훼손)등

피 고 인 변희재 외 3

위 사건에 관하여 피고인들의 변호인은 다음과 같이 이 사건 태블릿PC의 조작과 관련하여 새로이 발견된 증거들을 제출합니다.

I. 의견서의 목적

이 사건 태블릿PC의 조작과 관련하여 피고인 측의 주장을 뒷받침하고 검사측 주장을 반박할 수 있는 새로운 증거들이 다수 발견되었습니다. 새로운 증거들은 모두 이 사건 태블릿PC에 대한 국과수의 감정결과를 바탕으로 분석한 것입니다. 확실한 과학적 근거를 가진 새로운 증거들인 만큼 항소심 재판 과정에서 이에 대한 충분한 증거조사가 이루어져야 하고 검사 측이 이러한



증거들에 대해 합리적으로 반박하지 못한다면 그에 따른 불이익은 모두 검사 측에게 돌아간다는 점을 명확히 하고자 합니다.

II. 고소인 측에 의한 이 사건 태블릿PC의 조작

1. 카카오톡 닉네임 ‘선생님’ 설정시점

가. 구체적인 내용

JTBC는 카카오톡에 설정된 ‘선생님’이라는 닉네임이 이 사건 태블릿PC가 최서원의 것이라는 핵심 근거라는 취지로 2016. 10. 26. 뉴스룸에서 방송한 바 있습니다.

태블릿PC 사용자가 자신의 카톡 닉네임을 ‘선생님’으로 설정했는데, 최서원이 과거 유치원 원장 경력이 있고 선생님이란 호칭으로 자주 불렸으므로 카톡의 ‘선생님’은 곧 최서원 스스로 설정한 것이며, 따라서 태블릿PC는 최서원의 것이라는 논리입니다.

이러한 논리가 가능하려면 카톡 닉네임 ‘선생님’은 태블릿PC가 실제 사용되었던 2012. 6. 22.부터 2014. 4. 1. 기간 사이에 설정된 것이어야 합니다. 하지만 국과수의 태블릿PC 감정 시스템파일정보에 따르면, 이는 사실이 아닌

것으로 드러나고 있습니다.

태블릿PC에 저장된 `com.android.contacts_preferences.xml`은 사용자 연락처에 대한 환경설정을 저장하는 파일입니다. 예를 들어 태블릿PC 사용자가 자신의 카톡 닉네임을 변경할 경우 이 파일에 반영이 되면서 수정이 일어납니다.

따라서 `com.android.contacts_preferences.xml`의 과거 백업 파일들을 살펴 보면, 카톡이나 연락처 등에서 어떤 변화들이 있었는지 그 이력을 알아볼 수 있는 것입니다. 이 사건 태블릿에서 주목할 백업 파일은 2016년 10월 22일에 생성된 파일들입니다.

선택 여부	파일 경로	파일 이름	크기	날짜
□	문서/com.	.contacts_preferences.xml.bak(70).xml	1.25 KB	2016-10-22 20:22:20
□	문서/com.	.contacts_preferences.xml.bak(71).xml	1.25 KB	2016-10-22 20:22:20
✓	문서/com.	.contacts_preferences.xml.bak(72).xml	1.25 KB	2016-10-22 20:22:20
✓	문서/com.	.contacts_preferences.xml.bak(73).xml	1.19 KB	2016-10-22 20:22:20
□	문서/com.	.contacts_preferences.xml.bak(74).xml	1.19 KB	2016-10-22 20:22:20
□	문서/com.	.contacts_preferences.xml.bak(75).xml	1.21 KB	2016-10-22 20:22:20
□	문서/com.	.contacts_preferences.xml.bak(76).xml	1.19 KB	2016-10-22 20:22:20

[그림1-1-1] 2016. 10. 22.에 생성된 `com.android.contacts_preferences.xml`의 백업파일들

이날 16시 30분부터 20시 22분 20초까지 생성된 백업 파일에는 ‘선생님’ 이란 닉네임이 보이지 않았습니다(그림 1-1-2). 그러나 20시 22분 30초에 생성된 백업 파일을 보면, 처음으로 닉네임 ‘선생님’ 이 등장한다는 사실을



알 수 있습니다(그림 1-1-3).

```
1 <?xml version='1.0' encoding='utf-8' standalone='yes' ?>
2 <map>
3 <int name="filter.count" value="0" />
4 <int name="saveTab" value="2" />
5 <null name="filter.id" />
6 <boolean name="filter.groupReadOnly" value="false" />
7   <string name="defaultContactBrowserSelection-0 com.google.zixi9876@gmail.com
8     -1">content://com.android.contacts/contacts/lookup/3657if2d9e158c157c28/1</string>
9   <null name="filter.accountType" />
10  <null name="filter.accountName" />
11  <null name="filter.groupSourceId" />
12    <string name="defaultContactBrowserSelection-id">content://com.android.contacts/contacts
13      /lookup/3657f60a9cbe609c4978d/12</string>
14    <string name="defaultContactBrowserSelection-2-1">content://com.android.contacts
15      /contacts/lookup/0r5-AA20AA70AA92AA40AA70AA92AA38AA48AA9C/5</string>
16  <int name="groupFilterIndex" value="0" />
17  <int name="filter.type" value="-15" />
18  <int name="filter.groupFilterIndex" value="0" />
19  <null name="filter.groupSystemId" />
20  <boolean name="filter.autoAdd" value="false" />
21    <string name="defaultContactBrowserSelection-15-1">content://com.android.contacts
22      /contacts/lookup/0r4-AA20AA70AA92AA44AA48AA7AAA32AA62_3903f53137254/4</string>
23  <null name="filter.groupTitle" />
24  <long name="filter.groupId" value="-1" />
25 </map>
```

[그림 1-1-2] 2016년 10월 22일 20시 22분 20초에 생성된 백업 파일



```
1 <?xml version='1.0' encoding='utf-8' standalone='yes' ?>
2 <map>
3 <int name="filter.count" value="0" />
4 <int name="saveTab" value="2" />
5 <null name="filter.id" />
6 <boolean name="filter.groupReadOnly" value="false" />
7   <string name="defaultContactBrowserSelection-0-com.google.zixi9876@gmail.com">
8     -1</string>
9   <string name="filter.accountType">com.kakao.talk</string>
10  <string name="filter.accountName">선생님</string>
11  <null name="filter.groupSourceId" />
12    <string name="defaultContactBrowserSelection-id">content://com.android.contacts/contacts
13     /lookup/3657f60a9cbe609c4978d/12</string>
14    <string name="defaultContactBrowserSelection-2-1">content://com.android.contacts
15     /contacts/lookup/0r5AA20AA70AA92AA40AA70AA92AA38AA48AA90/5</string>
16    <int name="groupFilterIndex" value="0" />
17    <int name="filter.type" value="0" />
18    <int name="filter.groupFilterIndex" value="12" />
19    <null name="filter.groupSystemId" />
20    <boolean name="filter.autoAdd" value="false" />
21      <string name="defaultContactBrowserSelection-15-1">content://com.android.contacts
22       /contacts/lookup/0r4-AA20AA70AA92AA44AA48AA7AAA32AA62_3903f53137254/4</string>
23      <string name="filter.groupTitle">선생님</string>
24      <long name="filter.groupId" value="-1" />
25    </map>
```

[그림 1-1-3] 2016년 10월 22일 20시 22분 30초에 생성된 백업 파일에 ‘선생님’ 처음 등장

나. 증거의 취지

1) 증명력 탐핵

우선, 닉네임 ‘선생님’은 이 사건 태블릿PC가 최서원의 것임을
뒷받침하는 증거로서의 증명력이 없다고 할 것입니다. 닉네임 ‘선생님’은

고소인 측이 이 사건 태블릿PC를 점유하는 동안에 조작된 내용이기 때문입니다.



2) 사실의 적시에 해당

무엇보다도, 닉네임 ‘선생님’이 고소인 측에 의해 조작되었다는 사실은 이 사건 태블릿PC의 무결성이 심각하게 훼손되어 애초에 박근혜 전 대통령의 공무상비밀누설죄의 증거로서 쓰일 수 없음을 뒷받침합니다. 피고인 측은 이 사건 태블릿PC 내의 파일들에 대한 조작이 이루어졌고 그에 따른 심각한 무결성의 훼손으로 인해 이 사건 태블릿PC는 박근혜 전 대통령의 공무상비밀누설죄의 증거로서 쓰일 수 없음을 주장하였는데, 이는 결국 모두 진실한 사실의 적시에 해당함이 명백합니다.

3) 고소인 측의 증거위조

마지막으로, 닉네임 ‘선생님’은 고소인 측이 이 사건 태블릿PC를 점유하는 동안에 생성된 것이므로 형법 제155조 제1항의 증거위조죄에 해당합니다.

2. ‘L’ 자 패턴 설정 시점

가. 구체적인 내용

이 사건 태블릿PC에는 잠금 패턴이 설정되어 있습니다. 2016. 10. 25.
실시된 검찰의 포렌식 결과에 따르면, 태블릿PC의 잠금 패턴은 대문자 L자형입니다. 따라서 2016. 10. 18. 태블릿PC 발견 당시 JTBC 김필준 기자가 어떻게 잠금 패턴을 봄 것인지 의문이 들 수밖에 없습니다. 훗날 JTBC는 이렇게 해명합니다.

출처 | 미디어워치에 대한 손석희-JTBC의 2차 고소장(2017년 12월 19일) 84쪽

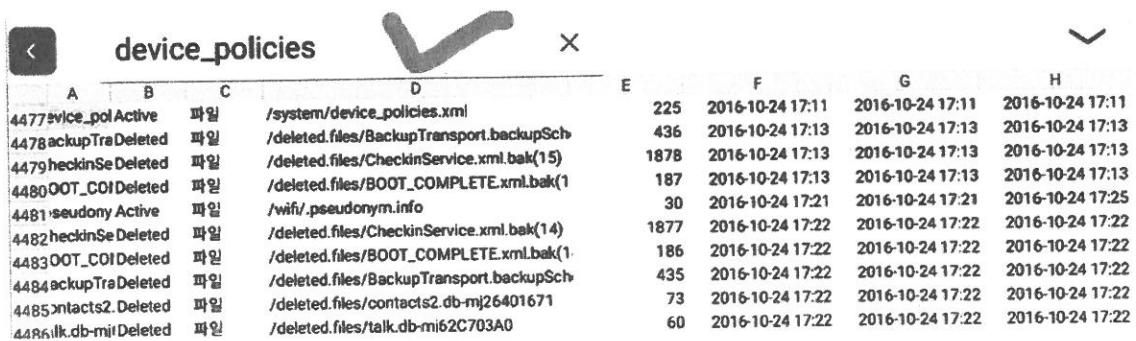
먼저, 2016.10.18. 더블루케이 사무실에서 '최순실의 태블릿PC'를 처음 발견한 JTBC 김필준 기자는 자신과 그의 여자친구가 평소에 사용하는 잠금 패턴이 L자여서 무심코 'L'자 형태로 비밀번호를 눌러 봤더니 바로 열린 것입니다. 김필준 기자는 이러한 사실을 자신의 휴대전화 포렌식(한컴지앤디 분석)을 통해 확인하여 검찰에 관련 증거로 제출한바 있습니다. 지극히 운이 좋았던 것입니다.

김필준은 자신은 물론 여자친구까지 당시 휴대전화 잠금 패턴이 L자였고, 그래서 잠겨져있던 태블릿에 무심코 L자 패턴을 그려봤더니 운 좋게 단번에 열렸다는 것입니다. 이 논리에 따르면, 2016. 10. 18. 태블릿PC 발견 당시에도 잠금 패턴이 L자였다는 것인데, 이 역시 사실이 아닌 것으로 드러나고 있습니다.

국과수의 시스템파일정보 분석결과에 나오는 `device_policies.xml` 파일이 그 근거입니다. 이 파일을 분석하면 사용자가 잠금 설정을 생성 또는 수정했던 시점, 잠금의 형태(비밀번호, 잠금 패턴, 영문자) 등을 정확히 알 수 있

습니다.

전문가의 분석 결과, 이 파일의 최종 수정일시는 2016년 10월 24일 17시 11분이며(그림 1-2-1), 이때의 잠금 형태는 5자리의 ‘잠금 패턴’이라는 사실이 밝혀졌습니다(그림 1-2-2). 국과수 포렌식의 한컴 GMD 분석결과에 따르면, 그 5자리 값은 ‘03678’인 것으로 확인됩니다(그림 1-2-3). 이는 잠금 패턴 L자형이라는 뜻입니다.



A	B	C	D	E	F	G	H
4477service_pol Active	파일	/system/device_policies.xml		225	2016-10-24 17:11	2016-10-24 17:11	2016-10-24 17:11
4478 backupTraDeleted	파일	/deleted.files/BackupTransport.backupSch		436	2016-10-24 17:13	2016-10-24 17:13	2016-10-24 17:13
4479 heckinSe Deleted	파일	/deleted.files/CheckinService.xml.bak(15)		1878	2016-10-24 17:13	2016-10-24 17:13	2016-10-24 17:13
4480 OOT_COI Deleted	파일	/deleted.files/BOOT_COMPLETE.xml.bak(1)		187	2016-10-24 17:13	2016-10-24 17:13	2016-10-24 17:13
4481 seudonym Active	파일	/wifi/.pseudonym.info		30	2016-10-24 17:21	2016-10-24 17:21	2016-10-24 17:25
4482 heckinSe Deleted	파일	/deleted.files/CheckinService.xml.bak(14)		1877	2016-10-24 17:22	2016-10-24 17:22	2016-10-24 17:22
4483 OOT_COI Deleted	파일	/deleted.files/BOOT_COMPLETE.xml.bak(1)		186	2016-10-24 17:22	2016-10-24 17:22	2016-10-24 17:22
4484 backupTraDeleted	파일	/deleted.files/BackupTransport.backupSch		435	2016-10-24 17:22	2016-10-24 17:22	2016-10-24 17:22
4485 contacts2 Deleted	파일	/deleted.files/contacts2.db-mj26401671		73	2016-10-24 17:22	2016-10-24 17:22	2016-10-24 17:22
4486 ilk.db-mj Deleted	파일	/deleted.files/talk.db-mj62C703A0		60	2016-10-24 17:22	2016-10-24 17:22	2016-10-24 17:22

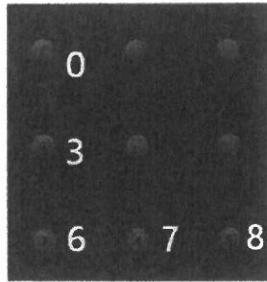
[그림 1-2-1] device_policies.xml의 수정일시가 2016년 10월 24일 17시 11분으로 나온다.

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<policies>
<active-password quality="65536" length="5" uppercase="0" lowercase="0"
letters="0" numeric="0" symbols="0" nonletter="0" recoverable="false" />
</policies>
```

[그림 1-2-2] device_policies.xml을 보면, 10월 24일 17시 11분에 설정된 패스워드는 5자리이다.

활성	이전 Sim의 네트워크 제공	SKTelecom	USIM 정보
비고	/system/SimCard.dat		
활성	데더링	아이디 : AndroidHotspot5783	데더링
활성	화면 잠금 패턴	03678	화면 잠금 패턴

[그림 1-2-3] 10월 24일 17시 11분에 설정된 암호는 ‘잠금 패턴’이며, 그 값은 03678이다.



[그림 1-2-4] 잠금 패턴 03678은 L자형을 의미한다.

따라서 이 사건 태블릿PC는 2016년 10월 24일 17시 11분에 잠금 패턴이 L자형으로 변경됐다는 결론을 내릴 수 있습니다. 바꿔 말하면 그 이전의 잠금 설정은 L자 패턴이 아니었다고 판단되는 것입니다.

나. 증거의 취지

1) 증명력 탄핵

우선, 고소인 측은 입수경위와 관련하여 우연하게 ‘L’ 자 패턴을 입력하여 이 사건 태블릿PC의 잠금장치를 해제하였다고 주장하고 있는데 이는 허위임이 명백합니다. 이 사건 태블릿PC의 파일을 조작하는 방식으로 입수경

위를 날조하고 있음이 드러난 이상, 고소인 측이 주장하는 입수경위 전반을 신빙할 수 없습니다.

2) 사실의 적시에 해당

무엇보다도, ‘L’ 자 패턴이 고소인 측에 의해 사후적으로 조작되었다는 사실은 이 사건 태블릿PC의 무결성이 심각하게 훼손되어 애초에 박근혜 전 대통령의 공무상비밀누설죄의 증거로서 쓰일 수 없음을 뒷받침합니다. 피고인 측은 이 사건 태블릿PC 내의 파일들에 대한 조작이 이루어졌고 그에 따른 심각한 무결성의 훼손으로 인해 이 사건 태블릿PC는 박근혜 전 대통령의 공무상비밀누설죄의 증거로서 쓰일 수 없음을 주장하였는데, 이는 결국 모두 진실한 사실의 적시에 해당함이 명백합니다.

3) 고소인 측의 증거 위조

마지막으로, ‘L’ 자 패턴은 고소인 측이 이 사건 태블릿PC를 점유하는 동안에 생성된 것이므로 형법 제155조 제1항의 증거위조죄에 해당합니다.

3. 김필준의 잠금장치 해제 방법

가. 구체적인 내용

2016. 10. 18. 태블릿PC 발견 당시, 태블릿의 잠금 설정은 L자 패턴이 아니었습니다. 그렇다면 김필준은 이날 오후 3시 32분경, 과연 어떤 방법으로 태블릿의 잠금을 해제했는지 또 다른 의문이 생길 수밖에 없습니다.

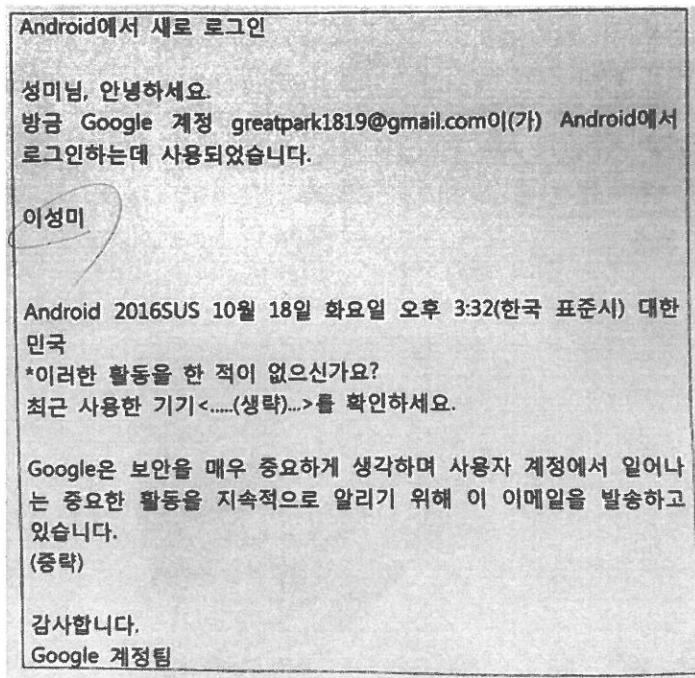


발견 당시 태블릿PC의 운영체제는 안드로이드 3.2 버전입니다. 지금 기준으로 한참 구 버전인 이 운영체제에서는 의외의 방법으로 잠금을 해제할 수 있는, 일종의 버그(프로그램 오류)가 있었습니다. 당시 안드로이드는 사용자가 잠금 패턴 해제를 5회 실패하면 구글 계정에 로그인하라는 입력 화면을 띠웠고, 이때 구글 아이디와 패스워드를 정확하게 입력하면 잠금이 풀리도록 되었습니다.

문제는 해당 기기와 전혀 무관한 구글 계정으로 로그인을 해도 잠금이 풀린다는 점이었습니다. 구글 계정만 갖고 있으면 누구라도 남의 스마트기기를 잠금 해제하는 게 가능하다는 것입니다. 이러한 보안상의 취약점은 이후 안드로이드 버전에서 해당 기기에 등록된 구글 계정으로 로그인할 때에만 잠금이 풀리도록 개선되었습니다.

이렇게 본다면 김필준도 2016년 10월 18일 오후 3시 32분경 구글 계정에 로그인을 하는 방법으로 잠금 패턴을 건너뛰고 태블릿PC를 열 수 있었다는 추정이 가능합니다. 이때 사용한 메일 계정이 바로 greatpark1819@gmail.com입니다.

전문가 분석에 따르면, 태블릿PC의 accounts.db라는 파일을 분석한 결과, 2016년 10월 18일 오후 3시 32분 구글 계정 greatpark1819가 태블릿PC에 새롭게 등록된 사실이 밝혀졌습니다. 로그인과 거의 동시에 태블릿의 잠금이 풀렸고, 구글 서버는 자동 보안메일을 greatpark1819 계정으로 발송했습니다.(그림 1-3-1) 이 사건 태블릿PC를 이전에 로그인한 적이 없는 새로운 기기로 인식했기 때문입니다.



[그림 1-3-1] 2016년 10월 18일 오후 3시 32분 이 사건 태블릿PC로 처음 greatpark1819에 로그인을 하자, 곧바로 보안메일이 도착했다.

중요한 것은 김필준이 이날 greatpark1819에 수동으로 로그인을 했다는 점입니다. 하지만 JTBC 측은 greatpark1819 메일 계정의 경우, 태블릿을 켜기만

하면 자동 로그인이 되는 계정이기 때문에 따로 아이디와 패스워드를 몰라도 접속 가능했다는 해명을 하고 있습니다.

하지만 이는 앞서 언급했던 accounts.db 파일로 반박이 가능합니다. greatpark1819가 태블릿PC에 ‘새롭게 등록된 시점’이 2016년 10월 18일 오후 3시 32분으로 나오기 때문입니다. 그 이전에는 이 태블릿PC를 통해 greatpark1819에 로그인한 적이 없다는 뜻입니다. 따라서 김필준이 이날 첫 로그인을 할 때만큼은 수동 로그인이었다고 결론지을 수 있습니다. 이는 김필준이 사전에 누군가에게서 아이디(greatpark1819)와 패스워드를 건네받은 것이라는 추론에 이르게 합니다.

나. 증거의 취지

1) 증명력 탐핵

우선, 고소인 측은 입수경위와 관련하여 우연하게 ‘L’ 자 패턴을 입력하여 이 사건 태블릿PC의 잠금장치를 해제하였다고 주장하고 있는데 이는 허위임이 명백합니다. 이 사건 태블릿PC의 파일을 조작하는 방식으로 입수경위를 날조하고 있음이 드러난 이상, 고소인 측이 주장하는 입수경위 전반을 신빙할 수 없습니다.

2) 고소인 측의 위증

무엇보다도, 김필준의 위증이 확실시됩니다. 이 사건 태블릿PC의 발
견 당시 잡금 장치가 ‘L’ 자 패턴이 아니었을 뿐 아니라, 메일 계정을 통해
잡금장치를 무력화하는 방식은 ‘L’ 자 패턴을 입력하여 정상적으로 잡금장치
를 해제하는 방식과는 너무나도 극명하게 차이가 나므로 단순한 기억의 오류
라고는 도저히 볼 수 없고, 따라서 김필준은 기억에 반하는 사실을 적극적으
로 날조해내었다고 볼 수밖에 없습니다.

3) 입수과정에서 고소인 측의 불법행위

덧붙여, 고소인 측은 이 사건 태블릿PC의 입수과정에서 형법 제316조
제2항 전자기록등내용탐지죄를 저질렀다고 봄이 타당합니다. 이 사건 태블릿
PC의 잡금 장치를 메일 계정을 통해 무력화하는 방식으로 해제하여 내부에 저
당된 정보를 열람한 것은 기술적 수단을 이용하여 잡금장치를 풀어 저장된 정
보를 열람하는 경우에 정확히 해당되기 때문입니다.

4. 시스템파일에 대한 인위적 접근

가. 구체적인 내용

2016년 10월 22일 이 사건 태블릿PC에는 다량의 시스템파일이 수정
또는 삭제되는 일이 발생했습니다. JTBC 측은 태블릿의 일반적인 구동이나 자
동업데이트로 인한 자연적인 현상이었다고 주장하고 있습니다.

하지만, 국과수 시스템파일정보 분석결과를 살펴보면 이 사건 태블릿PC의 일반적인 구동 혹은 앱의 자동업데이트 등에 의해 자연적으로 이루어졌다고 볼 수 없는 인위적인 행위들이 확인됩니다. 특히, 그러한 인위적인 행위들이 루팅권한을 획득하거나 소스코드편집(프로그래밍)을 통해 루팅권한을 우회하지 않고서는 불가능한 데이터베이스파일 내지 시스템파일에 대한 수정 또는 삭제 등의 방식으로까지 이루어지고 있습니다.

국과수의 파일포렌식 및 시스템파일정보 분석결과에 따르면, 2016년 10월 22일 오전 2시 24분경 IT 전문 지식을 갖춘 것으로 추정되는 누군가가 이 사건 태블릿PC를 사용한 혼적이 나옵니다. 이 사람이 SW 프로그래밍에 사용되는 소스코드 편집기나 태블릿PC 프로그래밍 관련 전문 포럼 등의 사이트에 접근한 결로 봄에서는 JTBC의 일개 기자가 아닐 확률이 높습니다(그림 1-4-1).

1054	첨상			2012-05-25 18:17:27	2016-10-22 02:24:23	2012-05-25 18:17:27
		<ul style="list-style-type: none">- 파일 경로 : /Media/data/com.android.email/cache/webviewCacheChromium- 크기 : 3.7KB [3,839 Bytes]- 유형 : JPG- 시각 Offset : 0x00015000- 해시값 [SHA1] : DB4F47451EA0B17B173A1A63FA115751B41EC20 (data_3_00004.jpg)				
1055	첨상			2012-05-25 18:17:27	2016-10-22 02:24:23	2012-05-25 18:17:27

	- 해시값 (SHA1) : 49E476948220BFA6BFC053268D6C342390636EF4 (data_2_00006.jpg)				
1057	정상	 NEWS	2012-06-25 18:17:27	2016-10-22 02:24:23	2012-06-25 18:17:27
- 파일 경로 : /Media/data/com.android.email/cache/webviewCacheChromium - 크기 : 2.8KB (2,913 Bytes) - 유형 : JPG - 시작Offset : 0x0001E000 - 해시값 (SHA1) : 6704BE4289B92AC4A2BF9B6B5EE467BFA6FAA2BE (data_2_00007.jpg)					
1058	정상		2012-06-25 18:17:27	2016-10-22 02:24:23	2012-06-25 18:17:27
- 파일 경로 : /Media/data/com.android.email/cache/webviewCacheChromium - 크기 : 2.5KB (2,604 Bytes) - 유형 : JPG - 시작Offset : 0x00021000 - 해시값 (SHA1) : 67D8C48DC7FE95877D0E4E4CA1F4BD2172BD1739 (data_2_00008.jpg)					
1059	정상	[REDACTED]	2012-06-25 18:17:27	2016-10-22 02:24:23	2012-06-25 18:17:27

	- 파일 경로 : /Media/data/com.android.email/cache/webviewCacheChromium - 유형 : JPG - 시작Offset : 0x0005C000 - 해시값 (SHA1) : 3456D74009654B296E794C061597A32038836126 (data_2_00022.jpg)				
1074	정상		2012-06-25 18:17:27	2016-10-22 02:24:23	2012-06-25 18:17:27
- 파일 경로 : /Media/data/com.android.email/cache/webviewCacheChromium - 크기 : 3.5KB (3,574 Bytes) - 유형 : JPG - 시작Offset : 0x0005E000 - 해시값 (SHA1) : 00A61497CEC389146D7B7461A72DD23F76665D76 (data_2_00023.jpg)					

529 / 1644
Mobile Forensics
DIGITAL MOBILE EVIDENCE ANALYSIS RESULT

	- 파일 경로 : /Media/data/com.android.email/cache/webviewCacheChromium - 크기 : 3.5KB (3,572 Bytes) - 유형 : JPG - 시작Offset : 0x00060000 - 해시값 (SHA1) : 87ECA3E756A722185-B97D8CAF2456DE87406B0B (data_2_00024.jpg)				
1075	정상		2012-06-25 18:17:27	2016-10-22 02:24:23	2012-06-25 18:17:27
- 파일 경로 : /Media/data/com.android.email/cache/webviewCacheChromium - 크기 : 3.5KB (3,572 Bytes) - 유형 : JPG - 시작Offset : 0x00060000 - 해시값 (SHA1) : 87ECA3E756A722185-B97D8CAF2456DE87406B0B (data_2_00024.jpg)					

[그림 1-4-1] IT 전문 지식을 갖춘 누군가가 프로그래밍 관련 사이트에 접근한 흔적들

이러한 접근에 뒤이어 곧바로 이메일이나 시스템폴더 및 로그, 지도 정보, 다운로드 기록, 계정 정보 등과 관련된 데이터베이스 파일 내지 시스템파일을 수정하거나 삭제한 기록이 등장합니다.

fx /deleted.files/EmailProvider.db

A	B	C	D	E	F	G	H
이름	상태	종류	경로	크기	생성 일시	접근 일시	수정 일시
2613	EmailProv Deleted	파일	/deleted.files/EmailProvider.db	225280	2011-01-01 9:02	2011-01-01 9:02	2016-10-22 2:24
2614	logs.db Active	파일	/data/com.sec.android.provider.logspro	221184	2011-01-01 9:02	2011-01-01 9:02	2016-10-22 2:24
2615	data_2 Active	파일	/data/com.android.email/cache/webviewC	1056768	2012-06-25 18:17	2012-06-25 18:17	2016-10-22 2:24

fx /data/com.sec.android.provider.logsprovider/databases/logs.db

A	B	C	D	E	F	G	H
이름	상태	종류	경로	크기	생성 일시	접근 일시	수정 일시
2614	logs.db Active	파일	/data/com.sec.android.provider.logspro	221184	2011-01-01 9:02	2011-01-01 9:02	2016-10-22 2:24 1845
2615	data_2 Active	파일	/data/com.android.email/cache/webviewC	1056768	2012-06-25 18:17	2012-06-25 18:17	2016-10-22 2:24 1845
2616	tombstone Active	폴더	/tombstones	4096	2012-07-02 12:39	2012-07-02 12:39	2016-10-22 2:25 A598
2617	tombstone Active	파일	/tombstones/tombstone_04	19888	2016-10-22 2:25	2016-10-22 2:25	2016-10-22 2:25 228C
2618	shared_prefs Active	폴더	/system/shared_prefs	4096	2012-07-02 16:45	2012-07-02 16:45	2016-10-22 2:25 0C37

fx /data/com.google.android.apps.maps

A	B	C	D	E	F	G	H
이름	상태	종류	경로	크기	생성 일시	접근 일시	수정 일시
2639	com.google.Active	폴더	/data/com.google.android.apps.maps	4096	2011-01-01 9:01	2011-01-01 9:01	2016-10-22 2:31 A3E
2640	cache_vts Active	파일	/media/Android/data/com.google.andro	27648	2016-10-22 2:31	2016-10-22 2:31	2016-10-22 2:31 B93C
2641	cache_rgts Active	파일	/media/Android/data/com.google.andro	22528	2016-10-22 2:31	2016-10-22 2:31	2016-10-22 2:31 B0A1
2642	DriveAbou Active	파일	/data/com.google.android.apps.maps/sha	116	2016-10-22 2:31	2016-10-22 2:31	2016-10-22 2:31 2B94
2643	databases Active	폴더	/data/com.google.android.apps.maps/dat	4096	2012-06-22 12:19	2012-06-22 12:19	2016-10-22 2:31 906F

/deleted.files/accounts.xml.bak(4)

A	B	C	D	E	F	G	H
1	이름	상태	종류	크기	생성 일시	접근 일시	수정 일시
2661	accounts.xml Deleted	파일	/deleted.files/accounts.xml.bak(4)	3513	2016-10-22 10:23	2016-10-22 10:23	2016-10-22 10:23 1DD1
2662	inode_06F Deleted	파일	/deleted.files/inode_06F93D00	204	2016-10-22 10:23	2016-10-22 10:23	2016-10-22 10:23 6F04
2663	inode_07C Deleted	파일	/deleted.files/inode_07D54A00	217	2016-10-22 10:23	2016-10-22 10:23	2016-10-22 10:23 70DA
2664	EmailProv Deleted	파일	/deleted.files/EmailProviderBody.db-shm!	32768	2011-01-01 9:02	2011-01-01 9:02	2016-10-22 10:23 93D6
2665	inode_08C Deleted	파일	/deleted.files/inode_08C04500	32768	2011-01-01 9:02	2011-01-01 9:02	2016-10-22 10:23 585D
2666	shared_pref Active	플더	/data/com.iloen.melon.tablet/shared_pref	4096	2011-01-01 9:02	2011-01-01 9:02	2016-10-22 10:23 116A

[그림 1-4-2] 이메일이나 시스템폴더 및 로그, 지도 정보, 계정 정보 등 관련 시스템파일들이 수정 또는 삭제된 기록들

전문가 분석에 따르면 해당 소스코드 편집기는 데스크톱PC 또는 노트북에서만 사용할 수 있었습니다. 따라서 JTBC 측의 누군가가 이 사건 태블릿PC를 데스크톱PC에 연결하고, 데스크톱PC에서 소스코드 편집기를 실행하여 이 사건 태블릿PC의 데이터베이스 파일이나 시스템파일을 수정 또는 삭제하였을 가능성을 추론해 볼 수 있습니다.

나. 증거의 취지

1) 사실의 적시에 해당

우선, 이 사건 태블릿PC의 데이터베이스파일이나 시스템파일이 소스코드편집(프로그래밍)등에 의해 인위적으로 수정 또는 삭제되었을 가능성이 매우 크다는 사실은, 이 사건 태블릿PC 내의 파일들이 고소인 측의 인위적인 개입에 의해 조작되었고 그에 따라 무결성이 심각하게 훼손되어 박근혜 대통령의 공무상비밀누설죄의 증거로 쓰일 수 없음을 의미합니다. 따라서

이 사건 태블릿PC 내의 파일들이 조작되고 그에 따라 무결성이 침해되었다는 피고인 측의 주장은 결코 허위사실의 적시가 아니고 진실한 사실이거나 진실이라고 믿을 충분한 근거가 있는 때에 해당함이 명백합니다.

2) 개별 파일들의 무결성 훼손

무엇보다도, 이 사건 태블릿PC 전체의 무결성 뿐 아니라, 파일 단위의 무결성 또한 훼손되었다는 점이 드러났습니다. 상기 피고인 측이 제시한 파일시스템정보 상의 기록들은 모두 일반적인 구동 내지 자동업데이트에 의해서는 결코 이루어질 수 없고 프로그래밍 방식에 의해서만 가능한 데이터베이스파일들 혹은 시스템파일들의 인위적인 삭제 또는 수정 내역입니다. 따라서 검사 측은 더 이상 구동 내지 자동업데이트에 의해 시스템파일들이 삭제 또는 수정되었다고 주장해서는 안 될 것입니다.

나아가, 이 사건 태블릿PC에 관한 국과수 감정회보서 35면, 36면에 따르면 일반적인 구동 내지 자동업데이트는 이 사건 태블릿PC 전체의 무결성을 훼손하는 근거가 될 뿐, 결코 개별적인 파일들의 무결성을 인정하는 근거가 되는 것이 아닙니다. 국과수 감정회보서의 취지는 일반적인 구동만으로도 이 사건 태블릿PC 전체의 무결성은 쉽게 훼손되기 때문에 개별 파일들의 경우 무결성이 인정되기 위해서는 국과수가 제공한 파일시스템정보와 포렌식 분석 결과를 종합적으로 고려하여 파일마다 개별적으로 입증을 하라는 취지입니다.

따라서 검사 측이 이 사건 태블릿PC 내의 파일들 또한 무결성이 인정된다고 주장하기 위해서는 피고인 측이 제시한 기록들을 포함하여 2016.

10. 18. 발견 이후 변경된 것으로 확인되는 전체의 시스템파일 내지 데이터베이스파일들이 인위적으로 변경된 것이 아니라는 점을 국과수의 감정결과를 근거로 구체적이고 합리적으로 입증해야 할 것입니다.

3) 고소인 측의 증거인멸

덧붙여, 고소인 측은 형법 제155조 제1항의 증거인멸죄를 저질렀다고 봄이 타당합니다. 고소인 측은 이 사건 태블릿PC 내의 시스템파일 내지 데이터베이스파일을 소스코드편집을 통해 인위적으로 수정 또는 삭제하였을 가능성이 매우 높기 때문입니다.

5. 장승호 사진파일의 다운로드

가. 구체적인 내용

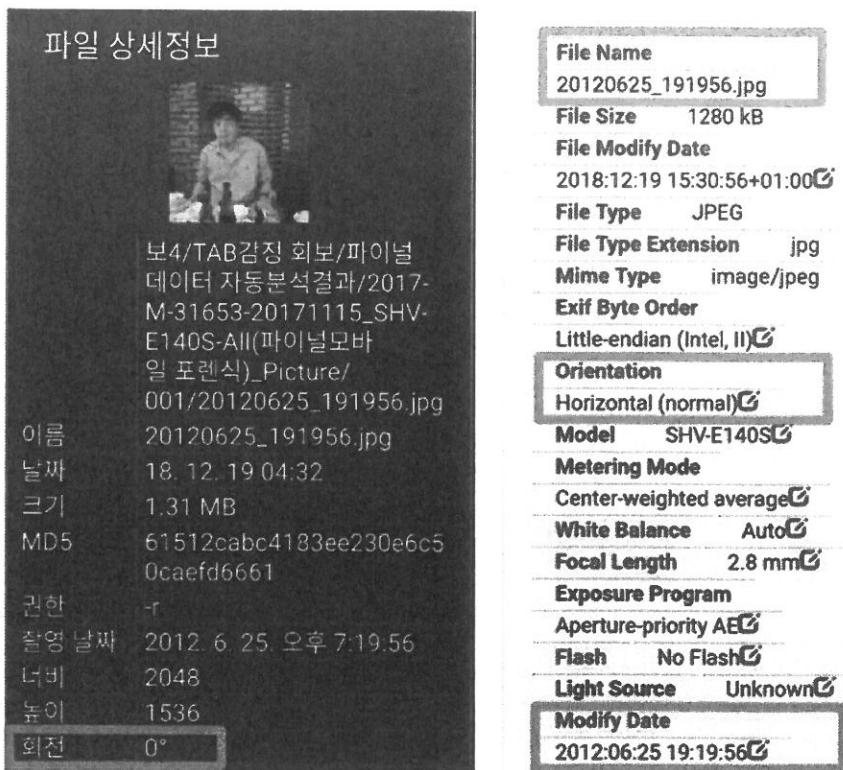
이 사건 태블릿PC에 저장돼 있는 장승호 사진파일(20120625_191956.jpg)은 국과수 포렌식 감정에서도 언급하듯이 메타데이터가 수정되어 원본이 아닌 것으로 판정되었습니다. 태블릿PC로 촬영된 나머지 16장의 사진들과 달리 촬영 당시 생성된 사진파일 그대로 저장되어 있는 것이 아니라는 뜻입니다.

이에 대해 국과수 감정회보서 44면에서는 해당 장승호 사진파일은 사용자에 의해 삽입 또는 생성된 파일이라고 적시하고 있습니다.

국과수 나기현 공업연구관은 하나의 가능성으로서 ‘사진회전가설’을 제시했습니다. 사진을 회전시키면서 보는 경우 원본파일에 덮어쓰기가 되면서 원본이 아닌 새로운 파일이 생성된 것처럼 기록에 남을 수 있다는 주장입니다. 이 가설은 변희재의 태블릿PC 명예훼손 재판 1심에서 검사가 원용하기도 했던 주장으로, 태블릿 발견 당시 김필준이 무심코 장승호 사진을 회전시켜 발생한 현상인 것처럼 사소하게 치부되었습니다.

하지만 분석결과, 해당 장승호 사진은 회전되지 않은 것으로 드러났습니다. 사진파일의 회전 여부를 알 수 있는 분석 프로그램으로 살펴본 결과 해당 사진의 회전 각도는 0도로 나온 것입니다.

구체적으로 장승호 사진의 Orientation값은 ‘Horizontal(normal)’으로 나왔습니다. 여기서 Orientation은 사진파일의 현재 회전 상태를 사진이 촬영된 최초의 상태와 비교하여 각도로 표시해주는 항목입니다. 그 값이 Horizontal(normal)이라는 것은 처음 상태에서 전혀 회전되지 않았다는 의미입니다.



[그림 1-5-1] 장승호 사진파일(20120625_191956.jpg)은 회전되지 않은 것으로 밝혀졌다.

사진이 회전된 게 아니라면, 장승호 사진파일의 메타데이터가 어떤 이유로 수정된 것인지 또 다른 가능성을 찾아야 하는 상황입니다. 이 분야 전문가가 제시한 의견에 따르면, 이메일이나 문자메시지, 카카오톡 등에서 다운로드 받은 사진이라면 촬영 당시에 기록된 메타데이터가 누락된 채 전송될 수 있습니다.

따라서 현재 남은 가장 유력한 가능성으로 장승호 사진파일은 이메일이나 문자메시지, 카카오톡 등을 통해 전송받아서 이 사건 태블릿에 저장되었다고 추론할 수 있습니다. 요컨대, 인위적으로 삽입된 사진이라고 봄이 타당합니다.

나. 증거 취지

1) 사실의 적시에 해당

우선, 사진이 회전되지 않았다는 사실은 사진이 회전에 따라 생성되었을 가능성을 배제하는 것이고 피고인 측이 주장한 바와 같이 사진이 삽입되었음을 의미합니다. 따라서 장승호 사진이 삽입되었다는 피고인 측의 주장은 허위사실의 적시가 아니라 진실한 사실의 적시에 해당합니다.

2) 고소인 측의 증거인멸

다음으로, 고소인 측이 이 사건 태블릿PC를 보유하고 있던 기간 중에 해당 장승호 사진이 다운로드 되는 방식 등으로 삽입되었으므로 그러한 고소인 측의 삽입행위는 형법 제155조 제1항의 증거위조에 해당합니다.

6. 고소인 측이 제시한 입수영상의 조작가능성

가. 구체적인 내용

1) 장승호 사진 파일

상기 장승호 사진파일의 경우 JTBC측이 2016. 10. 18. 이 사건 태블릿PC를 최초로 발견할 당시에 촬영하였다고 주장하면서 제시된 구동영상에서 수차례 회전되는 것으로 나타나는데 이상에서 살펴본 바와 같이 해당 사진파일은 회전된 적이 없음이 분명합니다. 그러므로 이러한 사실은 구동영상 전체가 2016. 10. 18. 이 사건 태블릿PC를 최초로 발견할 당시에 실제로 촬영된 것이 아니고 불상의 시점에 인위적으로 상황을 설정하여 촬영한 영상들을 편집하여 만든 영상이라는 점을 뒷받침하는 증거가 됩니다.

2) 카카오톡 닉네임 ‘선생님’

카카오톡 닉네임 ‘선생님’이 등장하는 시점 또한 구동영상이 조작되었음을 뒷받침하는 증거가 됩니다. 2016. 10. 18. 당시에 촬영되었다고 주장되는 구동영상에는 분명히 카카오톡 닉네임 ‘선생님’이 등장합니다. 하지만, 국과수 시스템파일정보 분석결과에 따르면 카카오톡 닉네임 ‘선생님’은 2016. 10. 22. 20시 22분 30초부터 등장함을 확인할 수 있습니다. 따라서 이러한 사실은 JTBC측이 제시한 구동영상이 2016. 10. 18. 당시에 실제로 찍힌 것이 아니라 2016. 10. 22. 이후 불상의 시점에 인위적으로 상황을 설정하여 촬영한 영상들을 편집하여 만든 영상이라는 점을 뒷받침하는 증거가 됩니다.

나. 증거의 취지

1) 증거위조죄(형법 제155조 제1항) 혹은 모해증거위조죄(형법 제155조 제3항)

모해증거위조죄의 경우 피의자 또는 피고인이 된 자에게 불

리하도록 새로운 증거를 만드는 경우에 성립합니다.(2008도12127판결 참조)

따라서 장승호 사진을 회전시키는 부분이나 카카오톡 닉네임 ‘선생님’
이 등장하는 부분이 변희재 고문 외 3인 등에 대한 수사가 진행된 이후에
조작한 부분이라면 모해증거위조죄에 해당하나 그렇지 않으면 단순한 증
거위조죄에만 해당할 것입니다.

2) 무결성 훼손

대법원 2018. 3. 15. 선고 2014도11448 판결, 서울고등법원
2014. 8. 21. 선고 2014노1268 판결, 서울중앙지방법원 2014. 4. 25. 선고
2013고합805 판결 등의 구체적인 설시내용을 적용하여 보면 다음과 같습
니다. 해당 구동영상은 현장에서 촬영된 원본이 편집되는 등의 인위적 개
작 없이 원본의 내용 그대로 복사하여 사본으로 만든 것이 아니고, 영상
촬영자가 원본 확인 및 편집에 동석하지 아니하였으며, 원본 파일이 변개
되지 않은 상태에서 복사되었음을 인정할 만한 봉인 등의 조치를 하지 않
았을 뿐 아니라, 원본의 일정부분을 편집을 통해 인위적으로 삭제·소멸시
켰고, 나아가 원심에서는 해당 구동영상파일의 조작여부에 관한 감정 등이
전혀 이루어지지 않았기 때문에 조작여부를 판단할 수 없는 상태임이 명

백합니다. 그러므로 해당 구동영상은 2016. 10. 18. 당시에 이 사건 태블릿 PC가 촬영되었다는 점을 입증하는데 있어 증거로서 쓰일 수 없습니다.

7. 대용량 앱의 설치 기록

가. 구체적 내용

국과수 파일포렌식 분석결과를 살펴보면, 이 사건 태블릿PC에는 2012. 2. 23. 공장출하 당시 ARBook이라는 앱의 원본설치 파일이 .apk 형태로 들어있던 것으로 확인됩니다.

[ARBook.apk.ZIP]						
번호	정상	파일 경로	ZIP	크기	시작Offset	파싱값 (SHA1)
185	ARBook.apk.ZIP	/Media/app	ZIP	1980-01-01 AM 12:00:00	13.6MB (14,250,732 Bytes)	0x00000000

그리고 이 원본설치 파일이 2016. 10. 20. 저녁 8시 경에 설치된 것으로 확인됩니다. 이 파일의 원본날짜가 공장출하 시와 동일하므로, 자동업데이트가 아닌 사용자가 임의로 2016. 10. 20. 저녁 8시 경에 설치한 것으로 볼 수 있습니다.

583	정상	업티미 디어 모 그	/mnt/sdcard/ARBook/r xdata	4096	2016-10-20 PM 08:52:10	2016-10-20 PM 08:22:19
-----	----	------------------	-------------------------------	------	---------------------------	---------------------------

S08	항상		MP4	2016-10-20 PM 08:22:22	2016-10-20 PM 08:22:24
· 파일 경로 : /Media/data/com.samsung.arbook/ARBook/sample · 크기 : 3.9MB (4,049,647 Bytes) · 시작Offset : 0x00000000 · 해시값 (SHA1) : 176438ACA362FB99F241540ECC4C7F1E8D3F4A15 (ar_sample.mp4)					

나. 증거의 취지

1) 무결성 확손

문제는 이러한 대용량 앱을 설치할 경우 하드디스크의 물리적 공간을 크게 차지할 확률이 높아지고, 그 차지하는 공간에 과거 삭제된 정보들이 있을 때 그 위에 새로운 정보가 덮어쓰기 됨에 따라 포렌식 감정으로도 삭제된 로그기록을 완벽하게 복원해 낼 수 없다는 점입니다. 바로 이러한 점 때문에 디지털증거의 경우 그것을 발견하는 순간부터 어떠한 기능적 활동도 일어나지 않은 상태가 유지되어야 무결성이 확보되고 증거로 쓰일 수 있는 것입니다.

디지털증거는 생성・복제・삭제가 용이한 특성으로 인해 수사와 재판의 과정에서도 까다로운 절차를 통해 무결성을 확보하도록 되어 있습니다. 서울중앙지법 전자정보 압수수색영장에 관한 실무운영 지침, 대검예규 제805호 등이 따라야 할 적법절차입니다. 이러한 절차적 규범은 원칙적으로 수사자가 수사기관 내지 법원이지만 무결성의 확보라는 원칙

에서 볼 때에는 사인에 의해서도 반드시 지켜지지 않으면 안 되는 규범입니다. 해당 규범이 오로지 수사기관 내지 법원만을 구속한다면 사인에 의해 심하게 오염된 디지털증거가 임의제출의 방식으로 법정에 그대로 들어오기 때문입니다.

2) 고소인 측의 증거인멸

고소인 측이 대용량 앱의 설치를 통해 과거 삭제된 로그기록들이 포렌식에 의해서도 완벽히 복원되지 않을 수 있다는 점을 인식하고, ARBook 앱을 인위적으로 설치한 것이라면 형법 제155조 제1항의 증거인멸죄에 해당할 것입니다.

III. 검찰에 의한 이 사건 태블릿PC의 조작

1. 구체적인 내용

가. 2016. 10. 31. 검찰의 루트 폴더에 대한 권한 획득

국과수 파일시스템정보 분석결과를 보면, 제일 첫머리에 해당하는 제2행에 '/' 표시가 있으며 2016년 10월 31일 오후 2시 47분에 수정된 것으로 기록되어 있습니다.

파일시스템...
2017-M-31653...



C	D	E	F	G	H	
1	종류	감지	생성일시	접근일시	수정일시	
2	폴더	/	40%	1970-01-01 9:00	1970-01-01 9:00	2016-10-31 14:47
3	폴더	/lost+found	40%	1970-01-01 9:00	1970-01-01 9:00	1970-01-01 9:00
4	폴더	/media	40%	2011-01-01 9:00	2011-01-01 9:00	2016-10-22 0:18
5	폴더	/media/ReadersHub	40%	2011-01-01 9:00	2011-01-01 9:00	2011-01-01 9:00
6	폴더	/media/ReadersHub/Books	40%	2011-01-01 9:00	2011-01-01 9:00	2011-01-01 9:00
7	파일	/media/ReadersHub/Books/TextorefreeD	34053	2011-01-01 9:00	2011-01-01 9:00	2011-01-01 9:00
8	파일	/media/ReadersHub/Books/TextorefreeD	2071185	2011-01-01 9:00	2011-01-01 9:00	2011-01-01 9:00
9	파일	/media/ReadersHub/Books/TextorefreeD	33535	2011-01-01 9:00	2011-01-01 9:00	2011-01-01 9:00
10	파일	/media/ReadersHub/Books/TextorefreeD	492873	2011-01-01 9:00	2011-01-01 9:00	2011-01-01 9:00

[그림 2-1-1] 제2행에 '/' 표시가 있으며, 2016년 10월 31일 오후 2시 47분에 수정되었다.

전문가의 분석에 따르면, 이는 10월 31일 오후 2시 47분에 검찰의 누군가가 태블릿PC의 ‘루트 권한’을 획득했다는 의미입니다. 루트 권한이란 특정 기기나 소프트웨어 등을 사용하여 안드로이드 운영체제의 가장 깊숙한 곳에 있는 핵심부인 루트(root) 폴더에 대한 권한을 획득하는 것을 의미합니다.

이러한 권한을 획득하면 이 사건 태블릿PC에 존재하는 거의 모든 파일에 접근하여 수정할 수 있고, 그에 따른 로그기록을 남기지 않을 수도 있습니다. 국과수 감정회보서 34면에 표현된 바에 따르면, 이는 시스템 접근권한 탈취에 해당하는데 이 사건 태블릿PC에 대한 검찰 포렌식이 종료되고 6일 후에 벌어진 일입니다.

이렇듯 국과수 파일시스템정보 분석결과의 제일 첫머리에 루트 권한이 탈취된 사실이 명백히 확인됨에도 국과수는 시스템 접근권한의 탈취가 없었다고 감정회보서에 적시하고 있어 이 부분에 있어서는 국과수의 오류라고 보아야 합니다.

여하튼 루트 권한을 획득한 이후 검찰은 어떠한 흔적도 남기지 않고 이 사건 태블릿PC를 조작할 수 있는 상태를 만들었습니다. 그 결과 똑같은 태블릿PC임에도 2016년 10월 25일에 실시된 검찰 포렌식 보고서와, 2017년 11월에 실시된 국과수 감정회보서에 나오는 사용자 파티션의 해시값이 서로 다릅니다.

포렌식 보고서 28번 파티션의 해시값 비교

1. 국과수 회보 해시

1) SHA1
A1C4BD3532D24CC8540DDF5219281417DE07448C

2) MD5
edb47a398bbae1c21cbac9453c34d349

2. 검찰 보고서 해시

MD5
5db883725394c1c199520b00858f90b9

[그림 2-1-2] 해시값이 달라지지 않아야 하지만, 검찰의 포렌식 이후 국과수가 다시 포렌식을 할 때에는 해시값이 바뀐 것으로 드러났다.

이는 검찰이 2016년 10월 31일 루트 권한을 획득하여 이 사건 태블릿PC에 대해 조작을 하지 않았다면 결코 발생할 수 없는 현상이라 할 것입니다.

나. 각종 데이터베이스파일 내지 시스템파일의 변경기록

실제 이날 오후 2시 47분 검찰이 루트 권한을 탈취한 이후, 약 2분

의 시간¹⁾ 동안 이 사건 태블릿PC의 시스템파일들이 대거 변경된 기록들이 나타납니다.

이름	상태	종류	경로	크기	생성 일시	접근 일시	수정 일시
qmux_client_socket_185	Active	기타	/radio/qmux_client_socket_185	0	2016-10-31 14:47	2016-10-31 14:47	2016-10-31 14:47
inode_00620200	Deleted	파일	/deleted.files/inode_00620200	3145768	2011-01-01 9:01	2011-01-01 9:01	2016-10-31 14:47
inode_00620300	Deleted	파일	/deleted.files/inode_00620300	3145768	2011-01-01 9:01	2011-01-01 9:01	2016-10-31 14:47
.pcsync_stream	Active	기타	/pcsync_stream	4096	1970-01-01 9:00	1970-01-01 9:00	2016-10-31 14:47
persist.radio.adb_log_on	Active	파일	/property/persist.radio.adb.log.on	0	2016-10-31 14:47	2016-10-31 14:47	2016-10-31 14:47
persist.radio.mem_leak_debug	Active	파일	/property/persist.radio.mem_leak_debug	1	2016-10-31 14:47	2016-10-31 14:47	2016-10-31 14:47
persist.radio.data_adb_log_on	Active	파일	/property/persist.radio.data_adb.log.on	1	2016-10-31 14:47	2016-10-31 14:47	2016-10-31 14:47
persist.radio.voip_enabled	Active	파일	/property/persist.radio.voip_enabled	1	2016-10-31 14:47	2016-10-31 14:47	2016-10-31 14:47
proxy_tether_connect_socket	Active	기타	/radio/proxy_tether_connect_socket	0	2016-10-31 14:47	2016-10-31 14:47	2016-10-31 14:47
proxy_qmux_connect_socket	Active	기타	/radio/proxy_qmux_connect_socket	0	2016-10-31 14:47	2016-10-31 14:47	2016-10-31 14:47
inode_0062C700	Deleted	파일	/deleted.files/inode_0062C700	32768	2016-10-25 11:22	2016-10-25 11:22	2016-10-31 14:47
efs1.bin	Active	파일	/qcks/efs1.bin	3145768	2011-01-01 9:01	2011-01-01 9:01	2016-10-31 14:47
efs2.bin	Active	파일	/qcks/efs2.bin	3145768	2011-01-01 9:01	2011-01-01 9:01	2016-10-31 14:47
temp.dump	Active	파일	/qcks/temp.dump	3145728	2011-01-01 9:01	2011-01-01 9:01	2016-10-31 14:47
efs3.bin	Active	파일	/qcks/efs3.bin	3145768	2011-01-01 9:01	2011-01-01 9:01	2016-10-31 14:47
entropy.dat	Active	파일	/system/entropy.dat	4096	2011-01-01 9:01	2011-01-01 9:01	2016-10-31 14:47
inode_008C6F00	Deleted	파일	/deleted.files/inode_008C6F00	102128	2016-10-31 14:47	2016-10-31 14:47	2016-10-31 14:47
statsbin.bak	Deleted	파일	/deleted.files/statsbin.bak	900	2016-10-31 14:47	2016-10-31 14:47	2016-10-31 14:47
statusbin.bak	Deleted	파일	/deleted.files/statusbin.bak	1482	2016-10-31 14:47	2016-10-31 14:47	2016-10-31 14:47
packages.xml	Active	파일	/system/packages.xml	165625	2016-10-31 14:47	2016-10-31 14:47	2016-10-31 14:47
packages.list	Active	파일	/system/packages.list	10759	2016-10-31 14:47	2016-10-31 14:47	2016-10-31 14:47
packages-stopped.xml	Active	파일	/system/packages-stopped.xml	226	2016-10-31 14:47	2016-10-31 14:47	2016-10-31 14:47
accounts.xml	Active	파일	/system/qsync/accounts.xml	3513	2016-10-31 14:47	2016-10-31 14:47	2016-10-31 14:47
databases	Active	폴더	/data/com.android.providers.settings/databases	4096	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:47
settings.db	Active	파일	/data/com.android.providers.settings/databases/:/	57344	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:47
settingsdb-wal	Active	파일	/data/com.android.providers.settings/databases/:/	0	2016-10-31 14:47	2016-10-31 14:47	2016-10-31 14:47
settingsdb-shm	Active	파일	/data/com.android.providers.settings/databases/:/	32768	2016-10-31 14:47	2016-10-31 14:47	2016-10-31 14:47
property	Active	폴더	/property	4096	2011-01-01 9:00	2011-01-01 9:00	2016-10-31 14:47
backup	Active	폴더	/backup	4096	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:47
pending	Active	폴더	/backup/pending	4096	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:47
processed	Active	파일	/backup/processed	204	2016-10-31 14:47	2016-10-31 14:47	2016-10-31 14:47
persist.sys.profiler_ms	Active	파일	/property/persist.sys.profiler_ms	1	2016-10-31 14:47	2016-10-31 14:47	2016-10-31 14:47

1) 루트 권한을 획득하는 즉시 이 사건 태블릿PC 내부의 파일들이 변경된 기록을 알 수 없게 되는 것이 아니고 그렇게 되기까지는 다소간의 시간이 걸리게 됩니다. 국과수가 제공한 파일시스템정보 상에는 2016. 10. 31. 오후 2시 47분 루트권한을 획득한 이후 약 2분 정도의 시간 동안에 변경된 각종 데이터베이스파일 내지 시스템파일이 존재함을 확인할 수 있습니다.

이름	상태	종류	경로	크기	생성 일자	최근 일자	수정 일자
journal-1995247881tmp	Active	파일	/backup/pending/journal-1995247881tmp	55	2016-10-31 14:47	2016-10-31 14:47	2016-10-31 14:47
downloads.db-shm	Active	파일	/data/com.android.providers.downloads/databases/	32768	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:47
akmd_set.txt	Active	파일	/misc/akmd_set.txt	311	2012-06-22 14:15	2012-06-22 14:15	2016-10-31 14:47
telephony.db-shm	Active	파일	/data/com.android.providers.telephony/database	32768	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:47
cache	Active	폴더	/data/com.google.android.location/cache	4096	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:47
inode_007BBC00	Deleted	파일	/deleted/files/inode_007BBC00	32768	2011-03-22 4:27	2011-03-22 4:27	2016-10-31 14:47
launcher.db-shm	Active	파일	/data/com.android.launcher/databases/launcher	32768	2011-03-22 4:27	2011-03-22 4:27	2016-10-31 14:47
shared_prefs	Active	파일	/data/com.google.android.backup/shared_prefs	4096	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:47
contacts2.db-shm	Active	파일	/data/com.android.providers.contacts/databases/	32768	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:47
BackupTransport.backupSchedule	Active	파일	/data/com.google.android.backup/shared_prefs/l	424	2016-10-31 14:47	2016-10-31 14:47	2016-10-31 14:47
BackupTransport.restoreSchedule	Active	파일	/data/com.google.android.backup/shared_prefs/l	217	2016-10-31 14:47	2016-10-31 14:47	2016-10-31 14:47
qmux_connect_socket	Active	기타	/radio/qmux_connect_socket	0	2016-10-31 14:47	2016-10-31 14:47	2016-10-31 14:47
wallpaper_info.xml	Active	파일	/system/wallpaper_info.xml	173	2016-10-31 14:47	2016-10-31 14:47	2016-10-31 14:47
radio	Active	폴더	/radio	4096	2011-01-01 9:00	2011-01-01 9:00	2016-10-31 14:47
MT_shared_pref.xml.bak	Deleted	파일	/deleted/files/MT_shared_pref.xml.bak	213	2016-10-31 14:47	2016-10-31 14:47	2016-10-31 14:47
inode_0083C500	Deleted	파일	/deleted/files/inode_0083C500	32768	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
mmssms.db-shm	Active	파일	/data/com.android.providers.telephony/database	32768	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
nvmmac.info	Active	파일	/nvmmac.info	17	2011-01-01 9:00	2011-01-01 9:00	2016-10-31 14:48
inode_0076FE00	Deleted	파일	/deleted/files/inode_0076FE00	21032	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
inode_0075FE00	Deleted	파일	/deleted/files/inode_0075FE00	21032	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
inode_0075SE00	Deleted	파일	/deleted/files/inode_0075SE00	21032	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
inode_0074AE00	Deleted	파일	/deleted/files/inode_0074AE00	21032	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
inode_0074E200	Deleted	파일	/deleted/files/inode_0074E200	21032	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
inode_0073BE00	Deleted	파일	/deleted/files/inode_0073BE00	21032	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
inode_0072E600	Deleted	파일	/deleted/files/inode_0072E600	21032	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
pending.bin	Active	파일	/system/9ync/pending.bin	492	2016-10-31 14:47	2016-10-31 14:47	2016-10-31 14:48
databases	Active	폴더	/data/com.android.providers.contacts/databases	4096	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
.mac.info	Active	파일	/mac.info	18	2012-07-07 11:37	2012-07-07 11:37	2016-10-31 14:48
wpa_supplicant.conf	Active	파일	/misc/wifi/wpa_supplicant.conf	423	2012-07-13 19:18	2012-07-13 19:18	2016-10-31 14:48
contacts2.db-mj1336945A	Deleted	파일	/deleted/files/contacts2.db-mj1336945A	73	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48
EmailProvider.db-shm	Deleted	파일	/deleted/files/EmailProvider.db-shm	32768	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
databases	Active	폴더	/data/com.android.email/databases/EmailProvid	4096	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
EmailProvider.db-shm	Active	파일	/data/com.android.email/databases/EmailProvid	32768	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48

이름	상태	종류	경로	크기	생성 일자	최근 일자	수정 일자
EmailProviderBody.db-shm	Deleted	파일	/deleted/files/EmailProviderBody.db-shm	32768	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
EmailProviderBody.db-shm	Active	파일	/data/com.android.email/databases/EmailProvid	32768	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
EmailProvider.db-mj764AC1B1	Deleted	파일	/deleted/files/EmailProvider.db-mj764AC1B1	132	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48
EmailProvider.db-mj09C95C69	Deleted	파일	/deleted/files/EmailProvider.db-mj09C95C69	132	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48
launcher.db	Active	파일	/data/com.android.launcher/databases/launcher	96304	2011-03-22 4:27	2011-03-22 4:27	2016-10-31 14:48
launcher.db-wal	Active	파일	/data/com.android.launcher/databases/launcher	32992	2011-03-22 4:27	2011-03-22 4:27	2016-10-31 14:48
inode_008EB000	Deleted	파일	/deleted/files/inode_008EB000	32768	2012-06-22 12:09	2012-06-22 12:09	2016-10-31 14:48
calendar.db	Active	파일	/data/com.android.providers.calendar/databases	176128	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
downloads.db	Active	파일	/data/com.android.providers.downloads/databas	36864	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
calendar.db-shm	Active	파일	/data/com.android.providers.calendar/databases/	32768	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
SYSTEM_BOOT@1477892885708	Active	파일	/system/dropbox/SYSTEM_BOOT@14778928857C	254	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48
RR_NPONp	Active	파일	/log/RR_NPONp	1632	2011-01-01 9:01	2011-01-01 9:01	2016-10-31 14:48
databases	Active	폴더	/data/com.sec.android.providers.downloads/data	4096	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
sisDownloads.db	Active	파일	/data/com.sec.android.providers.downloads/data	20480	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
osp.db	Active	파일	/data/com.osp.app.signin/databases/osp.db	28672	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
sisDownloads.db-wal	Active	파일	/data/com.sec.android.providers.downloads/data	0	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48
sisDownloads.db-shm	Active	파일	/data/com.sec.android.providers.downloads/data	32768	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48
cache	Active	폴더	/data/com.sec.readershelf/cache	4096	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
webView.db-shm	Active	파일	/data/com.sec.readershelf/databases/webview.db	32768	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
media.db	Active	파일	/data/com.sktelecom.hoppin/tablet/databases/m	53248	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
mmssms.db	Active	파일	/data/com.android.providers.telephony/database	135168	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
melon.info	Active	파일	/media/melon.info	128	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
inode_0083CA00	Deleted	파일	/deleted/files/inode_0083CA00	32768	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
internal.db-shm	Active	파일	/data/com.android.providers.media/databases/in	32768	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
dropbox	Active	폴더	/system/dropbox	8192	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
inode_00868E00	Deleted	파일	/deleted/files/inode_00868E00	21032	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
inode_0086TE00	Deleted	파일	/deleted/files/inode_0086TE00	21032	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
inode_00859E00	Deleted	파일	/deleted/files/inode_00859E00	21032	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
inode_00852E00	Deleted	파일	/deleted/files/inode_00852E00	21032	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
inode_0084BE00	Deleted	파일	/deleted/files/inode_0084BE00	21032	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
inode_00843E00	Deleted	파일	/deleted/files/inode_00843E00	21032	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
inode_00837E00	Deleted	파일	/deleted/files/inode_00837E00	21032	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
googleSettings.gdb	Active	파일	/data/com.google.android.gsf/databases/google	28672	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48

이름	상태	종류	경로	크기	생성 일시	접근 일시	수정 일시
googlesettings:db-journal	Active	파일	/data/com.google.android.gsf/databases/google	0	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
shared_prefs	Active	폴더	/data/com.google.android.gsf/shared_prefs	4096	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
r1z_data_db	Active	파일	/data/com.google.android.partnersetup/database	32768	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
shared_prefs	Active	폴더	/data/com.google.android.partnersetup/shared_p	4096	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
EventLogService.xml.bak	Deleted	파일	/deleted.files/EventLogService.xml.bak	242	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48
EventLogService.xml	Active	파일	/data/com.google.android.gsf/shared_prefs/Eve	242	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48
R1Z.xml	Active	파일	/data/com.google.android.partnersetup/shared.p	300	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48
ApplicationHidingPreferences.xml	Active	파일	/data/com.google.android.partnersetup/shared.p	114	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48
event_log@1477892891117.txt	Active	파일	/system/dropbox/event_log@1477892891117.txt	34	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48
event_data@1477892891137.txt	Active	파일	/system/dropbox/event_data@1477892891137.txt	63	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48
inode_008A2B00	Deleted	파일	/deleted.files/inode_008A2B00	32768	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
alarms.db-shm	Active	파일	/data/com.android.deskclock/databases/alarms.d	32768	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
databases	Active	폴더	/data/com.google.android.gm/databases	4096	2012-06-25 18:35	2012-06-25 18:35	2016-10-31 14:48
mailstore.zix9876@gmail.com.db	Active	파일	/data/com.google.android.gm/databases/mailsto	200704	2012-06-25 18:35	2012-06-25 18:35	2016-10-31 14:48
mailstore.zix9876@gmail.com.dt	Active	파일	/data/com.google.android.gm/databases/mailsto	0	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48
mailstore.zix9876@gmail.com.mt	Active	파일	/data/com.google.android.gm/databases/mailsto	32768	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48
shared_prefs	Active	폴더	/data/com.google.android.gms/shared_prefs	4096	2013-05-17 11:05	2013-05-17 11:05	2016-10-31 14:48
auth_recovery_state.xml	Active	파일	/data/com.google.android.gms/shared_prefs/auth	468	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48
Device.info	Active	파일	/media/Tstore/Temp/Device.info	101	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
inode_008B8100	Deleted	파일	/deleted.files/inode_008B8100	32768	2012-06-25 18:40	2012-06-25 18:40	2016-10-31 14:48
shared_prefs	Active	폴더	/data/com.android.settings.mt/shared_prefs	4096	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
external.db-journal(1)	Deleted	파일	/deleted.files/external.db-journal(1)	12824	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48
external.db-journal(2)	Deleted	파일	/deleted.files/external.db-journal(2)	12824	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48
MT_shared_pref.xml	Active	파일	/data/com.android.settings.mt/shared_prefs/MT_	212	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48
databases	Active	폴더	/data/com.android.providers.media/databases	4096	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
external.db	Active	파일	/data/com.android.providers.media/databases/e	352256	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
badge.db	Active	파일	/data/com.sec.android.provider.badge/databases	20480	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
external.db-journal	Deleted	파일	/deleted.files/external.db-journal	12824	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48
inode_00911B00	Deleted	파일	/deleted.files/inode_00911B00	32768	2012-06-22 12:09	2012-06-22 12:09	2016-10-31 14:48
webview.db-shm	Active	파일	/data/com.android.browser/databases/webview.c	32768	2012-06-22 12:09	2012-06-22 12:09	2016-10-31 14:48
off.p	Active	파일	/log/off.p	384	2012-06-24 0:23	2012-06-24 0:23	2016-10-31 14:48
inode_0093E100	Deleted	파일	/deleted.files/inode_0093E100	1090	2012-06-24 0:23	2012-06-24 0:23	2016-10-31 14:48
sync	Active	폴더	/system/sync	4096	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48

이름	상태	종류	경로	크기	생성 일시	접근 일시	수정 일시
status.bin	Active	파일	/System/sync/status.bin	1432	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48
stats.bin	Active	파일	/System/sync/stats.bin	900	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48
sockets	Active	폴더	/misc/wifi/sockets	4096	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
system	Active	폴더	/system	4096	2011-01-01 9:01	2011-01-01 9:01	2016-10-31 14:48
usagestats	Active	폴더	/system/usagestats	4096	2011-01-01 9:01	2011-01-01 9:01	2016-10-31 14:48
dmapppmgr.db	Active	파일	/system/dmapppmgr.db	32768	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
UinboxProvider.db	Active	파일	/data/com.sec.android.sociehub/databases/Uinb	32768	2012-06-22 12:09	2012-06-22 12:09	2016-10-31 14:48
batterystats.bin	Active	파일	/system/batterystats/bin	103440	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48
usage-20161031	Active	파일	/system/usagestats/usage-20161031	416	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48
inode_0096A100	Deleted	파일	/deleted.files/inode_0096A100	32768	2012-06-25 18:40	2012-06-25 18:40	2016-10-31 14:48
webview.db-shm	Active	파일	/data/com.nhn.android.search/databases/webvie	32768	2012-06-25 18:40	2012-06-25 18:40	2016-10-31 14:48
talk.db-mj04EE7F0	Deleted	파일	/deleted.files/talk.db-mj04EE7F0	60	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48
talk.db-journal(1)	Deleted	파일	/deleted.files/talk.db-journal(1)	12906	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
talk.db-journal(2)	Deleted	파일	/deleted.files/talk.db-journal(2)	12906	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
talk.db-mj3643B73	Deleted	파일	/deleted.files/talk.db-mj3643B73	60	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48
talk.db-mj5C1A1375	Deleted	파일	/deleted.files/talk.db-mj5C1A1375	60	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48
talk.db-mj35127F84	Deleted	파일	/deleted.files/talk.db-mj35127F84	60	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48
talk.db-mj24CED60A	Deleted	파일	/deleted.files/talk.db-mj24CED60A	60	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48
talk.db-mj6AF4AB3E	Deleted	파일	/deleted.files/talk.db-mj6AF4AB3E	60	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48
talk.db-mj422EE482	Deleted	파일	/deleted.files/talk.db-mj422EE482	60	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48
talk.db-mj648250AC	Deleted	파일	/deleted.files/talk.db-mj648250AC	60	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48
databases	Active	폴더	/data/com.google.android.gsf/databases	4096	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
talk.db-journal	Deleted	파일	/deleted.files/talk.db-journal	8802	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
talk.db	Active	파일	/data/com.google.android.gsf/databases/talk.db	81920	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
talk.db-journal	Active	파일	/data/com.google.android.gsf/databases/talk.db	0	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48
dumpstate_shutdown.txt	Active	파일	/log/dumpstate_shutdown.txt	1095	2012-06-24 0:23	2012-06-24 0:23	2016-10-31 14:48
talk.db-mj4DC14423	Deleted	파일	/deleted.files/talk.db-mj4DC14423	60	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48

[그림 2-1-3] 검찰의 루트 권한 탈취 직후, 시스템파일들이 대거 변경된 기록이 나타난다.

검찰에 의해 무단으로 수정되었던 주요 시스템파일을 살펴보면, 연락처 및 통화기록, 문자메시지, 메일, 각종 파일 다운로드 관련 정보(dropbox,

downloads.db), 태블릿PC의 고유한 기기 정보인 맥 정보(.mac.info), 위치·지역·시간 값(persist.sys.profiler_ms)에 관련된 파일 등이 변경되었습니다.

문서파일 또는 사진과 연관된 데이터베이스 파일들도 변경되었으며, 이 사건 태블릿PC에 대한 이미지 파일이 백업(efs.bin, backup)되거나, 외부저장장치 내지 데스크톱PC 등과 연결되어 동기화된 경우(sync)도 나타나고 있을 뿐만 아니라, 시스템폴더 내의 파일까지 변경된 기록이 확인되고 있습니다.

예컨대 zixi9876 메일계정의 보관함은 검찰이 이 태블릿PC로 이메일을 새롭게 송수신하거나 삭제하지 않는 이상 데이터베이스 (mailstore.zixi9876@gmail.com.db) 파일의 변동이 있을 수 없음에도 해당 파일의 변경이 발생²⁾하였습니다. 더구나 파일 크기도 이전에 비해 현저히 작아져 있습니다.³⁾

2) 국과수 포렌식 분석결과에 따르면 2016. 10. 31.에는 메일이 송수신된 기록이 나타나지 않습니다.

3) 만일 해당파일이 자동업데이트에 따른 백업파일이라고 한다고 보더라도 사용자의 메일 보관함에 있는 메일을 함부로 수정 또는 삭제할 일은 절대로 없는 것이고 당연히 원상태로 복원하게 됩니다. 그렇다면, 2016. 10. 31. 해당파일은 이전의 해당파일과 크기가 같아야 할 것인데 해당파일의 크기는 이전에 비해 현저히 작아져 있습니다. 따라서 해당파일은 자동업데이트에 따른 백업파일이라고 볼 수 없습니다.

데이터	경로
연락처	/data/data/com.android.providers.contacts/databases/contacts2.db
통화 기록	/data/data/com.android.providers.contacts/databases/contacts2.db
SMS/MMS	/data/data/com.android.providers.telephony/databases/mmssms.db
일정	/data/data/com.android.providers.calendar/databases/calendar.db
메일 목록	/data/data/com.google.android.email/databases/EmailProvider.db
메일 내용	/data/data/com.google.android.email/databases/EmailProviderBody.db
웹 히스토리	/data/data/com.android.browser/databases/browser.db
웹 쿠키	/data/data/com.android.browser/databases/webview.db
웹 캐시	/data/data/com.android.browser/databases/webviewCache.db
알람	/data/data/com.google.android.deskclock/databases/alarm.db
미디어 위치	/data/data/com.android.providers.media/databases/external-숫자.db
다운로드	/data/data/com.android.providers.downloads/databases/downloads.db
시스템 설정	/data/data/com.android.providers.settings/databases/settings.db
GPS 캐시	/data/data/com.android.browser/app_geolocation/CachedGeoposition.db
구글지도 검색어	/data/data/com.google.android.apps.maps/databases/search_history.db
구글지도 북마크	/data/data/com.google.android.apps.maps/files/DATA_STARING
Wi-Fi 리스트	/data/misc/wifi/wpa_supplicant.conf
Wi-Fi Mac 캐시	/data/data/com.google.android.location/files/cache.cell
기지국 Cell 캐시	/data/data/com.google.android.location/files/cache.cell
사진, 동영상	/sdcard/dcim/camera/

[그림 2-1-4] 검찰이 루트 권한 탈취 이후 연락처, 통화기록, 메일 등을 변경한 정황이 드러났다.

2. 증거의 취지

가. 무결성 훼손

디지털증거의 경우에는 생성·복제·삭제가 용이한 특성으로 인해 발견 순간부터 어떠한 형태의 인위적 개입이 없이 그 상태 그대로 법정에 현출될 때에만 증거로서 쓰일 수 있습니다. 이를 형사소송법 상 디지털 증거의 무결성이라 일컫고 있고 판례와 관계 법령⁴⁾의 규율에 따라 이러한 디지털증거에 고유한 증거능력 인정요건이 구체화되고 있습니다. 검찰은 수사기관으로서 이러한 디지털증거의 취급에 있어 무결성의 확보를 위한 상기의 적법한 절차에 대해 상세히 알아야 하고 그를 철저히 준수하여 디지털증거를 취급해야 할 것입니다.

그럼에도 불구하고 위에서 살펴본 바와 같이 검찰은 루트폴더에 관한 권한을 획득함으로써 그러한 적법절차를 정면으로 위반하고 있습니다. 루트폴더에 대한 권한을 획득한다는 것은 어떠한 흔적도 없이 이 사건 태블릿PC 내의 모든 파일을 수정 또는 삭제할 수 있다는 의미로서 이보다 더 한 무결성 훼손은 없습니다.

4) 서울중앙지법 전자정보 압수수색영장에 관한 실무운영 지침, 대검예규 제805호 등이 대표적입니다.

나. 이 사건 태블릿PC 내의 개별 파일들의 무결성 확인

루트폴더에 대한 권한을 획득하는 방식의 광범위하고 근본적인 형태의 무결성 확인은 이 사건 태블릿PC 전체의 무결성 차원에서 뿐만 아니라, 이 사건 태블릿PC 내의 개별 파일들에 대해서도 무결성이 확인되어 증거로서의 가치가 없다고 볼 결정적이고 중대한 근거가 됩니다. 루트 권한의 획득은 사실상 이 사건 태블릿PC의 내의 거의 모든 파일에 대해 수정기록을 남기지 않은 채 접근·수정할 수 있게 만들기 때문입니다.

예컨대, 상기에서 분석한 바와 같이 다운로드 기록이나 위치·장소·시간 등에 관한 파일에 대한 수정기록이 존재하는데, 이러한 점은 어떠한 문서파일의 다운로드 여부 내지 다운로드 시점이 조작되었을 가능성 이 있다는 것입니다. 따라서 중국특사단 의원 추천 파일의 경우, 검사의 주장 및 박근혜 전 대통령의 1심 판결과 달리, 2016. 10. 31. 이후 국과수 감정 이 이루어지기 전 불상의 시점에 다운로드 여부에 관한 조작이 일어났을 가능성이 충분히 있으므로 중국특사단 의원 추천 파일이 특정 시점에 다운로드 된 것이라는 사실을 확정할 수는 없는 것입니다.

이렇듯, 무결성 침해가 광범위하고 흔적 없이 이루어질 수 있는 루트권한의 획득이 명백히 확인됨에도 불구하고 이 사건 태블릿PC 내의 개별 파일들에 대해 무결성이 당연히 인정되고 그러한 파일들의 존재를 근거로 어떠한 사실을 확정할 수 있다고 보는 것은 사실상 디지털증거의 무결

성에 관한 법리나 적법절차 그리고 증거에 의한 사실인정을 모조리 포기하는 것과 다를 바가 없습니다. 요컨대, 이 사건 태블릿PC 전체의 무결성은 물론 내부의 파일들에 대한 무결성 또한 확보되지 않는다고 봄이 타당할 것입니다.

다. 검찰의 증거인멸

루트권한의 획득은 이 사건 태블릿PC에 대하여 최대한 흔적 없이 위조 내지 변조하려는 고의를 가지지 않는 이상 절대 하지 않는 행위입니다. 즉, 루트권한의 획득 사실은 증거위조 내지 변조 의사의 충분조건인 것입니다. 따라서 검찰이 검찰 포렌식 이후 루트권한을 획득하였다는 사실이 명백함에도 불구하고 증거위조 내지 변조죄에 대한 수사가 이루어지지 않는다면 이는 명백히 수사기관의 직무유기로 해당할 것입니다. 보다 근본적으로는 특검법의 제정에 의해 면밀하고 집중적인 수사가 이루어져야 할 부분입니다.

특히, 검찰이 루트폴더에 대한 권한을 획득한 행위는 단순한 증거인멸이 아니라 형법 제155조 제3항의 모해증거인멸에 해당한다고 봄이 타당합니다. 2008도12127판결에 따르면 ‘피의자’로 볼 수 있기 위해서는 수사기관이 범죄사실을 인지하고 수사가 개시되었을 것을 필요로 합니다. 2016. 10. 24. 당시에 이미 이 사건 태블릿PC를 통하여 청와대문서가 열람되고 수정되었다는 본격적인 언론보도가 이루어졌고 2016. 10. 24. 오후 7시

경 검찰은 고소인 측으로부터 이 사건 태블릿PC를 임의제출 받았으며 다음 날 이 사건 태블릿PC에 대한 검찰 포렌식을 마쳤음을 고려할 때, 2016. 10. 31. 경에는 이미 박근혜 전 대통령의 공무상비밀누설죄에 대한 검찰의 인지가 있었고 수사 또한 이루어졌다고 봄이 타당합니다.

IV. 결 어

위 열거한 사항들은 이 사건 태블릿PC의 조작과 관련하여 피고인 측의 주장 을 뒷받침하는 중요한 증거들로, 이 사건 태블릿PC에 대한 국과수의 감정결 과 밝혀진 부분입니다. 현명하신 재판부께서 위와 같은 점들을 결코 간과하지 마시고 고소인과 검찰 측의 증거조작 행위에 관하여 납득할만한 석명을 하여주실 필요가 있다고 사료됩니다.

2019. 4. .

피고인들의 변호인

변호사

이 동 환



서울중앙지방법원 제4-2형사부(나) 귀중