



고려대학교
KOREA UNIVERSITY

쟁점 태블릿PC의 검찰 포렌식 분석결과에 대한 해설서 ver. 1.4

작성일 : 2017. 12. 13.

**고려대학교 정보보호연구원
디지털포렌식연구센터**

목 차

1. 배경	1
2. 이메일을 이용한 다운로드 파일에 대한 설명	3
3. 한컴뷰어-히스토리의 열람시간에 대한 설명	5
4. 셀카사진에 대한 설명	8
5. contact2.db-wal 파일에 대한 설명	9
6. 카카오톡 메시지 암호화 주장에 대한 설명	13
7. 자동 생성 파일에 대한 설명	15
8. 앱 접속 기록에 대한 설명	19
9. 썸네일(Thumbnail)에 대한 설명	22
10. 자동 로그인 기능에 대한 설명	24
11. ar_sample.mp4 파일에 대한 설명	25
12. 검찰 보고서의 970, 1805, 1871 사진 파일에 대한 설명 ...	27
13. 웹 캐시 파일에 대한 설명	34
14. 이메일 수신/발신 시간의 역전현상에 대한 설명	38

1. 배경

2016년 10월 18일, JTBC에서 입수하여 검찰에 제출한 쟁점 태블릿PC¹⁾에 대한 포렌식 분석 보고서(이하 검찰 보고서로 칭함)를 근거로 하여 조작설이 퍼지고 있다. 이 중 상당수는 디지털 기기의 동작 원리와 포렌식 도구의 특성을 잘못 이해하여 발생한 것으로 보인다.

본 해설서는 정확한 사실에 근거하여 전체적인 내용을 살펴봄으로써 제기된 의혹을 해소하기 위해 작성되었다. 이 해설서를 작성하기 위해 쟁점 태블릿PC와 동일한 기종의 태블릿PC(갤럭시 탭 8.9 LTE)에 사용 시점에 근접한 앱(어플리케이션)²⁾을 설치하여 재현 실험을 하였다.

이 해설서에서 다루고자 하는 대상은 갤럭시 탭에 저장되어 있는 디지털 데이터이며, 그 데이터가 어떠한 방식으로 생성되었는지 설명하고자 한다. **실사용자를 추정하려고 작성하는 것이 아님을 유념해 주기 바람**며, 본 해설서에 대한 불필요한 논쟁이 없기를 바란다.

참고로 디지털 기기, 특히 태블릿PC와 같이 무선 네트워크로 연결되어 있는 기기는 켜져 있으면 사용자가 아무런 조작을 하지 않아도 계속해서 데이터가 생성되거나 변경된다. 그래서 디지털 기기의 내부 데이터에 대해 포렌식 조사를 하기 위해서는 데이터가 변경되지 않는 보존 조치를 취한 후에 조사하는 것이 원칙³⁾이다. 이러한 원칙은 수사기관이 데이터를 수집한 이후에 적용되는 것으로, 디지털 포렌식을 모르는 일반 사용자가 내용을 확인하기 위해 디지털 기기를 작동시키면서 발생하는 데이터의 변경 부분은 전문능력을 보유한 수사기관이 정상적인 것인지 또는 의도적인 위변조인지 조사해야 한다.

다만 불필요한 논란을 피하기 위해서라도 이 해설서를 읽는 모든 분들은 **향후 법정 소송과 같이 중요한 데이터가 있다면 먼저 대상이 되는 디지털 데이터를 보존한 후에 내용을 분석하기** 바란다.

-
- 1) 일명 ‘최순실 태블릿PC’로 말해지고 있으나, 사용자에 대한 선입견을 없애기 위해 본 해설서에서는 쟁점 태블릿PC로 언급하고자 한다.
 - 2) 본 연구팀은 쟁점 태블릿PC의 데이터를 직접 확인할 수 없어서 가장 근접한 것으로 추정되는 앱을 설치하여 실험하였다.
 - 3) 무결성 원칙이라 말하며, 사건 조사를 하기 위해 수집한 디지털 데이터는 수집이 완료된 이후에는 어떠한 변경도 있지 않아야 함을 의미한다. 보통 디지털 기기에 있는 모든 데이터를 비트별로 동일하게 복제하는 과정(이미징이라 함)을 거쳐 보존하며, 이 데이터의 지문과 같은 역할을 하는 해쉬 값을 계산하여 별도 보관함으로써 데이터가 변경되지 않았음을 입증한다.

본 해설서는 월간조선 2017년 11월호(vol. 452)에 ‘최순실 것으로 알려진 태블릿PC, 검찰 포렌식 보고서 全文 입수’에서 제기된 의혹을 중심으로 살펴보고자 한다. 또한 본 해설서 ver1.0의 발표 이후에 질의받은 내용에 대해서도 설명하고자 한다.

2. 이메일을 이용한 다운로드 파일에 대한 설명

이메일에 첨부되어 있는 파일은 두 가지 방법으로 확인한다. 첨부된 파일을 다운로드하지 않고 열어보기만 하는 경우와 첨부된 파일을 다운로드 받은 후에 열어보는 경우가 있다. 전자의 방법으로 확인하는 경우에는 첨부파일이 캐시 디렉터리에 저장되며, 후자의 방법은 다운로드 디렉터리에 저장된다.

- 캐시 디렉터리 경로 : /data/data/com.android.email/cache/,
/data/media/Android/data/com.android.email/cache/
- 다운로드 디렉터리 경로 : /data/media/Download/

위의 저장경로는 쟁점 태블릿PC 기준이며, 대상 기기 또는 안드로이드 버전 등에 따라 상이할 수 있다.

그리고 이메일의 첨부파일을 열람 또는 다운로드하기 위해서는 이메일 앱(기본 이메일 앱, 지메일 앱, 네이버 메일 앱 등)을 이용하거나, 웹 브라우저를 이용하여 웹메일 서비스를 제공하는 도메인에 직접 접근하여 진행할 수 있다.

어떠한 방식을 사용하던지 간에 동일한 파일명을 가지는 첨부파일을 다운로드하는 경우에는 저장되는 파일명이 (파일명)-(숫자).* 규칙이 적용되어 저장되는데 동일한 이름을 가지는 파일이 증가할수록 숫자도 1씩 증가하여 기존의 파일과 구분될 수 있도록 저장된다. 예를 들어, “첨부파일.hwp” 파일이 태블릿PC에 저장되어 있으면, 이러한 파일명의 파일을 추가로 다운로드받는 경우 “첨부파일-1.hwp” 으로 저장되고, 또다시 다운로드 받으면 “첨부파일-2.hwp” 의 파일명으로 디렉터리에 저장된다.

또한, 이메일 앱을 이용하면, 캐시나 다운로드 디렉터리에 저장되는 파일명이 첨부파일의 이름과 동일하지만, 웹 브라우저를 이용하면 첨부파일 이름에서 한글이 포함된 부분(유니코드 인코딩 부분)이 “_” (언더바)로 변경되어 저장되는 특징이 있다. 예를 들어, 첨부파일의 이름이 “첨부파일.hwp” 인 파일을 다운로드하면 캐시 디렉터리나 다운로드 디렉터리에 저장되는 파일

명은 “_hwp” 로 저장된다.

따라서 검찰 보고서 20 쪽부터 21 쪽의 175번부터 181번 파일은 차례대로 웹브라우저 앱을 이용하여 첨부파일을 다운로드받은 것이다. 여기서 _hwp, _-1.hwp, _-2.hwp, ... 로 첨부파일로 저장되는 이유는 파일명이 한글이어서 위에서 언급한 것처럼 _hwp로 저장하고 계속해서 동일한 이름의 파일이 저장되기 때문에 -1, -2와 같은 일련번호가 붙게 된 것으로 보인다. 검찰 보고서에 기록된 해당 파일의 생성시간은 [표 1]과 같으며 순차적으로 저장된 것을 알 수 있다. 이 파일들이 동일한지 여부는 데이터를 확인해야 판단이 가능하다. 본 해설서는 첨부파일이 저장되는 방식에 대해서만 확인하였다.

[표 1] 해당 한글파일의 시간정보

파일명	만든 날짜	수정한 날짜	엑세스한 날짜
_hwp	2014-03-27 PM 07:20:52	2014-03-27 PM 07:20:53	2014-03-27 PM 07:20:52
_-1.hwp	2014-03-27 PM 07:21:06	2014-03-27 PM 07:21:07	2014-03-27 PM 07:21:06
_-2.hwp	2014-03-27 PM 07:21:32	2014-03-27 PM 07:21:33	2014-03-27 PM 07:21:32
_-3.hwp	2014-03-27 PM 07:23:14	2014-03-27 PM 07:23:14	2014-03-27 PM 07:23:14
_-4.hwp	2014-03-27 PM 07:25:01	2014-03-27 PM 07:25:01	2014-03-27 PM 07:25:01
_-5.hwp	2014-03-27 PM 07:25:09	2014-03-27 PM 07:25:10	2014-03-27 PM 07:25:09
_-6.hwp	2014-03-27 PM 07:27:20	2014-03-27 PM 07:27:21	2014-03-27 PM 07:27:20

[관련기사]

- 주간조선, '최순실 태블릿PC' 마지막 사용자는?4)

4) http://news.chosun.com/site/data/html_dir/2017/10/20/2017102002528.html

3. 한컴뷰어-히스토리의 열람시간에 대한 설명

한컴 오피스 파일(.hwp 파일)을 태블릿PC에서 열람하려면 열람할 수 있는 앱이 있어야 한다. 현재 구글 플레이(Google Play, 안드로이드 앱을 다운로드할 수 있는 서비스를 제공)에서는 한컴오피스 파일을 열람할 수 있는 ‘한컴오피스 viewer 앱’이 제공되고 있지만, 쟁점 태블릿PC를 사용한 시점에서는 이 앱이 아니고, 과거에 제공되던 한컴뷰어 앱이다.

본 연구팀에서는 구글 플레이에서 다운로드받은 앱이 아니라, 디지털 포렌식 관련 종사자로부터 받은 한컴뷰어 앱 버전 1.6과 Apkpure⁵⁾에서 한컴뷰어의 패키지명인 “kr.co.hancom.hancomviewer.androidmarket”으로 검색하여 다운로드받은 버전 2.2.1을 이용하여 재현 실험을 진행하였다. 앞서 언급한 두 가지 버전의 한컴뷰어 앱을 참고용으로 게시하므로 누구든지 의문사항이 있을 경우에는 직접 실험해 보길 권한다. (다운로드 링크 : <http://forensic.korea.ac.kr/tablet.html>)

한컴뷰어 앱은 SQLite 데이터베이스 파일 형식으로 history 파일을 저장하며, 열람한 파일명과 마지막으로 열람한 시간을 기록한다. history 파일의 저장경로와 내부 데이터는 아래와 같다.

- history 경로 : /data/data/kr.co.hancom.hancomviewer
.androidmarket/databases/history

[표 2] history 파일의 내부 데이터

구분(컬럼명)	저장된 데이터 의미
path	열람한 파일 경로와 파일명
position	알 수 없음
time	문서파일을 마지막으로 읽은 시간

5) 과거에 사용되던 앱을 다운로드받을 수 있도록 서비스를 제공하는 사이트, <https://apkpure.com>

rowid	path	position	time
(empty)	(empty)	(empty)	(empty)
6	/mnt/sdcard/Download/_3.hwp	0	2017-10-31 12:58:06
7	/mnt/sdcard/Download/드레스덴연설문실험용2.hwp	0	2017-10-31 15:56:37
8	/mnt/sdcard/Download/드레스덴연설문실험용1-2.hwp	0.3614487	2017-10-31 15:56:44

[그림 1] history 데이터베이스 파일의 내부 확인결과

열람한 파일의 정보는 history 파일의 history 테이블에 기록된다. 저장하는 시간 값은 UTC⁶⁾+0인 시간이 문자열로 기록되어 있고 한국시간(UTC+9)으로 변환하기 위해서는 저장된 시간 값에서 9를 더해야 한다.

00003F10	BA 6B A1 39 32 30 31 37	2D 31 30 2D 33 31 20 5A	k 2017-10-31 Z
00003F20	08 05 81 01 07 33 2F 6D	6E 74 2F 73 64 63 61 72	3/mnt/sdcard/Download/드레스덴연설문실험용1-2.hwp
00003F30	64 2F 44 6F 77 6E 6C 6F	61 64 2F EB 93 9C EB A0	드레스덴연설문실험용2.hwp
00003F40	88 EC 8A A4 EB 8D B4 EC	97 B0 EC 84 A4 EB AC B8	2017-10-31 15:56:44
00003F50	EC 8B A4 ED 97 98 EC 9A	A9 31 2D 32 2E 68 77 70	3/mnt/sdcard/Download/드레스덴연설문실험용1-2.hwp
00003F60	3F D7 21 F9 BA 6B A1 39	32 30 31 37 2D 31 30 2D	2017-10-31 15:56:44
00003F70	33 31 20 31 35 3A 35 36	3A 34 34 4F 07 04 7D 08	3/mnt/sdcard/Download/드레스덴연설문실험용2.hwp
00003F80	33 2F 6D 6E 74 2F 73 64	63 61 72 64 2F 44 6F 77	2017-10-31 15:56:37
00003F90	6E 6C 6F 61 64 2F EB 93	9C EB A0 88 EC 8A A4 EB	3/mnt/sdcard/Download/드레스덴연설문실험용1-2.hwp
00003FA0	8D B4 EC 97 B0 EC 84 A4	EB AC B8 EC 8B A4 ED 97	2017-10-31 15:56:37
00003FB0	98 EC 9A A9 32 2E 68 77	70 32 30 31 37 2D 31 30	3/mnt/sdcard/Download/_3.hwp
00003FC0	2D 33 31 20 31 35 3A 35	36 3A 33 37 32 06 04 43	2017-10-31 12:58:06
00003FD0	08 33 2F 6D 6E 74 2F 73	64 63 61 72 64 2F 44 6F	
00003FE0	77 6E 6C 6F 61 64 2F 5F	33 2E 68 77 70 32 30 31	
00003FF0	37 2D 31 30 2D 33 31 20	31 32 3A 35 38 3A 30 36	
00004000	0A 0F A1 00 03 0F 44 00	0F 44 0F C0 0F 64 00 00	

[그림 2] history 데이터베이스 파일 내에 문자열로 기록된 시간 값

FINALMobile Forensics5는 history 파일에 저장되어 있는 시간 값을 그대로 출력하는 것으로 판단되며, 올바른 시간 해석을 위해서는 검찰 보고서에 출력된 시간 값에 9를 더한 한국시간으로 변경해야 한다.

검찰 보고서의 한컴뷰어 히스토리 기록은 총 75건이며 시중에 공개된 검찰 보고서에는 한컴뷰어 히스토리의 첫 장표가 누락되어 1번 항목부터의 열람시간을 알 수는 없으나 2016년 10월 22일, 10월 23일, 10월 24일, 10월 25일 동안 순차적으로 열람되었고 드레스덴 연설문도 이 과정에서 열람되었을 것이다.

6) UTC(Universal Time Coordinated) : 협정 세계시, 국제사회가 사용하는 시간의 표준

[표 3] 한컴뷰어 열람 시간 예시

번호	파일명	열람시간
38	/mnt/sdcard/Download/11일차서울유세문-2.hwp	2016-10-24 AM 10:13:25
39	/mnt/sdcard/Download/_.hwp	2016-10-24 AM 10:13:52
40	/mnt/sdcard/Download/육영수여사 제38주기 추도식 인사말씀.hwp	2016-10-24 AM 10:14:05
41	/mnt/sdcard/Download/육영수여사 제38주기 추도식 인사말씀-7.hwp	2016-10-24 AM 10:14:25
42	/mnt/sdcard/Download/_-2.hwp	2016-10-24 AM 10:14:45
43	/mnt/sdcard/Download/_-6.hwp	2016-10-24 AM 10:14:51
44	/mnt/sdcard/Download/전국 축산인 한마음 전진대회 축사-2.hwp	2016-10-24 AM 10:32:55

[관련기사]

- 월간조선, [단독] 윤상직 의원 “검찰의 ‘최순실 태블릿PC’ 포렌식 프로그램 오류있다!” 7)
- 월간조선, [특종2탄] 독일 드레스덴 연설문 파일 날짜의 의문⁸⁾

7) http://monthly.chosun.com/client/mdaily/daily_view.asp?idx=1943&Newsnumb=2017101943



8) http://monthly.chosun.com/client/mdaily/daily_view.asp?idx=1811&Newsnumb=2017101811

4. 셀카 사진에 대한 설명

최순실과 관련된 파일은 두 가지 종류로, 하나는 양손이 보이는 사진이고 또 다른 하나는 손이 안 보이고 얼굴만 보이는 사진이다. 검찰 보고서에는 똑같은 사진 여러 개를 확인할 수 있는데, 이러한 사진들은 썸네일로 저장되어 있는 것들이고 실제로 원본 파일은 각각 하나씩만 저장되어 있다. (937번, 963번)

쟁점 태블릿PC의 모델명은 SHV-E140S이다. 이 기기에서 전방 카메라의 해상도는 1600×1200만 지원하고, 후방 카메라의 해상도는 2048×1536, 1024×768를 지원한다. 그래서 원본 파일을 조사해보면 전방 카메라로 찍은 것과 후방 카메라로 찍은 것을 구분할 수 있다.

최순실의 양손이 보이는 사진(937번)은 해상도가 2048×1536이기 때문에 후방 카메라로 찍은 것(셀카 사진 아님)이고, 손이 안 보이고 얼굴만 보이는 사진(963번)은 해상도가 1600×1200이기 때문에 전방 카메라로 찍은 것(셀카 사진)이다. 그리고 두 사진 파일의 저장경로로 미루어 보아 쟁점 태블릿PC를 이용하여 촬영되었을 것으로 판단된다.

937	정상		1.1 MB (1, 113 .08 0 B yte s)	JP G	2012:06:2 5 19:17:4 8	카메라 제조업체 : SAMSUNG 카메라 모델 : SHV -E140S 높이 : 1536, 너비 : 2048	20120625_191 748.jpg	2012-06-2 5 19:17:4 8	2012-06-2 5 19:17:4 9	2012-06-2 5 19:17:4 8	0x000 00000
- 파일 경로 : /FAT/media/DCIM/Camera/20120625_191748.jpg											
963	정상		602 .7K B (617 .15 9 B yte s)	JP G	2012:06:2 5 19:19:1 3	카메라 제조업체 : SAMSUNG 카메라 모델 : SHV -E140S 높이 : 1200, 너비 : 1600	20120625_191 914.jpg	2012-06-2 5 19:19:1 4	2012-06-2 5 19:19:1 4	2012-06-2 5 19:19:1 4	0x000 00000
- 파일 경로 : /FAT/media/DCIM/Camera/20120625_191914.jpg											

[그림 3] 937번, 963번 사진에 대한 검찰 보고서 내용

5. .db-wal 파일에 대한 설명

contacts2.db⁹⁾는 안드로이드 운영체제를 사용하는 스마트폰이나 태블릿 PC에서 연락처를 저장하기 위해 사용되는 SQLite 형식의 데이터베이스 파일이다. 사용자와 사용자가 추가한 연락처의 전화번호, 이메일 주소, 프로필 사진, 저장한 시간, 수정한 시간 등이 저장된다.

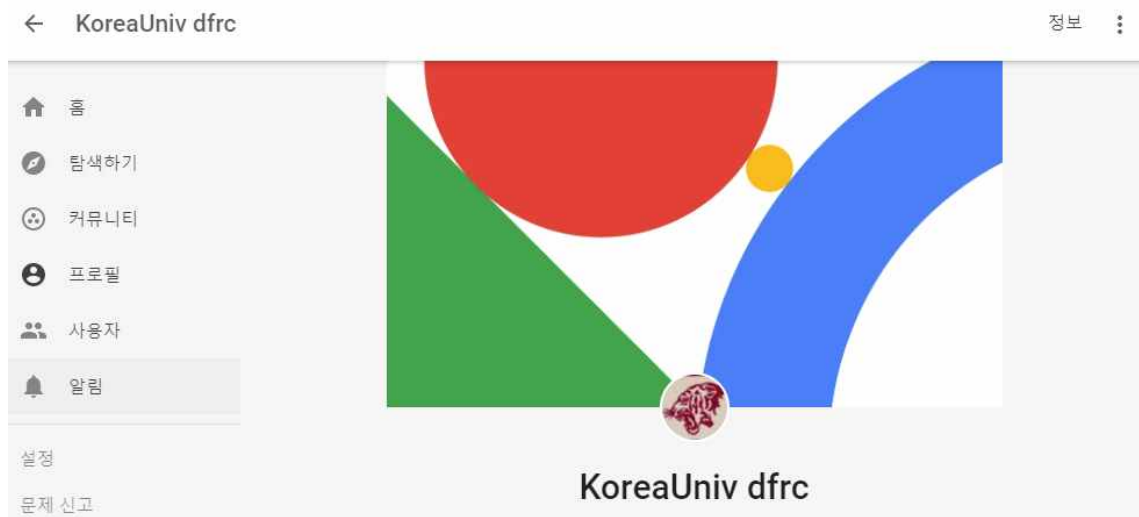
SQLite 형식의 데이터베이스 파일은 데이터 저장과정의 안정성을 위해 동작 중에 임시파일을 만들어 사용하는데, 그 임시파일의 이름은 (파일명).db-wal 파일로 부여된다. 즉, .db-wal 파일은 SQLite 형식의 데이터베이스가 정상적으로 사용되기 위해서 생성하는 임시파일이고, .db 파일이 닫히면 삭제되는 파일이다(단, 안드로이드 기기에서는 삭제되지 않아 디지털 포렌식 조사할 때 유용한 정보를 추출할 수 있다). 이러한 현상은 PC에서 MS워드를 열었을 때 ~\$(파일명).docx 파일이 임시파일로 생성되는 것과 유사한 원리이다. 즉, MS워드 문서파일을 수정하기 위해서 파일을 열었을 때는 임시파일이 생성되고 파일을 저장한 후에는 삭제되는 것과 유사한 원리이다.

.db-wal에는 연락처 record에 대한 transaction 로그가 기록된다. 로그는 연락처 데이터(이름, 번호, 닉네임, 연동된 SNS의 상태메시지, 이메일 등)가 변경되거나 변경을 시도하는 경우에 기록된다. transaction 로그는 연락처가 동기화되면서 새로운 연락처가 기기에 생성되거나 기존 연락처가 삭제 및 갱신될 때 기록되기도 하고, 사용자가 임의로 연락처를 생성, 삭제, 갱신하는 경우 혹은 연락처와 연동된 SNS의 계정 정보가 변경될 때 기타 어플리케이션에서 연락처에 접근해서 데이터가 수정될 때 등 다양한 경우에 기록된다.

.db-wal에 기록된 사진(2번부터 53번)은 위와 같은 여러 가지 이유로 인해 임시로 기록된 사진이며 contact2.db 파일에 저장되어 있는 사진은 1번이다. .db-wal에 해당 사진이 기록된 이유는 검찰 보고서만으로는 알 수 없고 정확한 원인을 파악하기 위해서는 쟁점 태블릿PC의 데이터를 조사해야 한다.

9) contacts2.db 경로 : /data/data/com.android.providers.contacts/databases/contacts2.db

구글의 프로필 사진은 구글 플러스 프로필 사진과 지메일 프로필 사진으로 구분된다. 구글 플러스에 프로필 사진이 있어도 지메일에 프로필 사진을 설정하면, 이메일과 연락처에 관련된 곳에서는 지메일 프로필 사진이 적용된다. 이를 실험하여 확인하기 위해서 설정한 구글 플러스의 프로필 사진은 [그림 4]이며, 지메일의 프로필 사진은 [그림 5]와 같다.



[그림 4] 실험용 구글 플러스 프로필 사진



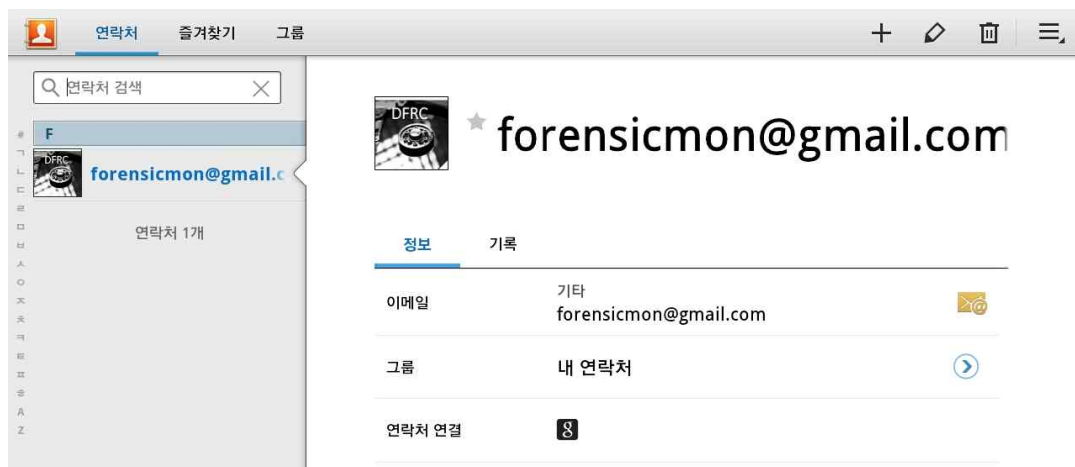
[그림 5] 실험용 지메일 프로필 사진

연락처에 사진이 저장되는 실험을 위해 먼저 실험용 지메일 계정에서 이메일 주소(forensicmon@gmail.com)를 주소록에 추가하였다. 그 이후, 쟁점 태블릿PC와 동일한 모델의 기기에서 실험용 지메일 계정으로 로그인하여 동기화하였다.



[그림 6] 구글 주소록에 저장되어 있는 메일 주소와 상대방 프로필 사진

그 결과, 구글 주소록에서는 [그림 6]과 같이 구글 플러스 프로필 사진이 저장된다. 이렇게 상대방의 지메일 주소를 구글 주소록에 추가한 후에, 태블릿 PC에서 계정 동기화를 하면, 태블릿PC의 연락처에는 [그림 7]과 같이 상대방의 지메일 프로필에서 설정한 사진이 저장된다. 최종적으로 contacts2.db 에는 지메일 프로필 사진이 저장된다.



[그림 7] 태블릿PC에 자동으로 동기화된 연락처



[그림 8] contacts2.db에 저장된 시간 정보

추가적으로 contacts2.db 파일 내부에는 최초 동기화된 시간과 최종 수정된 시간이 기록되어 있다. contacts2.db 내에 있는 ‘raw_contacts’ 테이블의 ‘sync3’ 컬럼에는 최초 동기화된 시간이 UTC+0 적용되어 저장되어 있으며, ‘last_time_modified’ 컬럼에는 최종 수정된 시간이 Unix Time 형태로 저장되어 있다. 해당 테이블에 저장되어 있는 정보를 통해 자동으로 동기화된 연락처, 최초 동기화된 시간, 최종 수정된 시간을 확인할 수 있다.

따라서 쟁점 태블릿PC의 데이터를 분석하면 논란이 되는 사진이 언제 태블릿PC에 저장되었는지 추정할 수 있을 것이다.

[관련기사]

- 미디어워치, 김수민 사진 53장, 박근혜캠프 SNS팀 태블릿PC라는 ‘결정적 증거’¹⁰⁾
- 월간조선, [특종8탄] 포렌식 보고서, 최순실 태블릿PC 안의 카카오톡 메시지 내용 암호화¹¹⁾

10) <http://www.mediawatch.kr/news/article.html?no=252534>

11) http://monthly.chosun.com/client/mdaily/daily_view.asp?Idx=1863&Newsnumb=2017101863

6. 카카오톡 메시지 암호화 주장에 대한 설명

디지털 기기에서 데이터를 삭제하면 동작 속도를 빠르게 하기 위해 삭제했다고 표시만 하고, 원 데이터는 그대로 유지하는 경향이 있다¹²⁾. 이러한 특성을 이용하여 삭제된 데이터를 복구할 수 있는데, 많은 포렌식 도구들이 삭제된 데이터를 복구하는 기능이 포함되어 있다.

디지털 기기를 많이 사용하다보면 삭제된 데이터가 다른 데이터로 덮어써지게 되는데, 이러한 경우에는 해당 데이터를 복구할 수 없으며, 덮어써지지 않은 부분은 삭제된 데이터의 파편 형태로 존재하게 된다.

이러한 삭제된 데이터의 파편은 포렌식 분석 도구로 해석하지 못할 수 있다. 일부 도구에서는 그 부분을 분석가에게 알려주기 위해서 해당 비트열을 그대로 보여주도록 동작하며 FINALMobile Forensics5 역시 그러한 도구로 판단된다.

22	삭제	수신	2018-06-03 PM 12:10:11	00 0C 19 16 14 04 00 00 00 02 00 00 00 0C 19 7F 18 06 00 00 00 0C 19 7F 18 03 00 03 00 03 00 04 00 05 00 00 00 0C 19 00 19 04 00 05 18 03 00 00 00 02 00 00 00 00 19 04 00 03 00 00 00 00 19 04 00 04 00 00 00 02 00 00 00 00 19 0C 19 03 00 00 00 0E 19 03 00 04 00 00 00 04 00 00 00 0E 19 03 00 04 00 EF 18 08 00 00 00 0E 19 C9 01 04 00 04 00 05 18 05 18 05 18 05 18 03 00 00 00 0E 19 C2 13 0F 19 00 00 04 00 00 00 0E 19 D6 18 04 00 04 00 02 00 00 00 0E 19 F0 18 02 00 00 00 0E 19 FC 18 02 00 00 00 0E 19 09 19 03 00 00 00 0E 19 09 19 FF 12 00 00 04 00 00 00 0E 19 09 19 BC 17 D0 13 04 00 00 00 0E 19 0A 19 A3 17 03 00 06 00 00 00 0E 19 0A 19 A3 17 03 00 05 18 09 18 05 00 00 00 0E 19 0A 19 A3 17 03 00 09 18 00 00 03 00 00 00 0E 19 0A 19 F0 18 00 00 04 00 00 00 0E 19 0A 19 F0 18 A3 17 02 00 00 00 0E 19 05 18 01 00 00 00 11 19 00 00 03 00 00 00 11 19 06 18 04 00 00 00 03 00 00 00 14 19 04 00 04 00 00 00 02 00 00 00 20 19 15 19 01 00 00 00 26 19 00 00 02 00 00 00 26 19 00 00 02 00 00 00 38 19 A3 01 03 00 00 00 38 19 A3 01 8E 12 00 00 01 00 00 00 3C 19 00 00 02 00 00 00 3C 19 8E 12 03 00 00 00 43 19 A3 01 8E 12 00 00 02 00 00 00 4F 19 04 00 05 00 00 00 4F 19 03 13 05 00 8E 12 FF 12 00 00 02 00 00 00 53 19 00 00 03 00 00 00 57 19 04 00 04 00 00 00 02 00 00 00 57 19 74 02 01 00 00 00 68 19 00 00 07 00 00 00 6C 19 8E 12 04
----	----	----	------------------------	--

[그림 9] 검찰 보고서 438페이지 내용 중 일부(카카오톡-메시지)

한편, 데이터가 암호화되면 모든 데이터가 랜덤하게 보이며 특정 바이트가 반복되는 형태로 나타나지 않는다. 따라서 [그림 9]와 같이 특정 바이트가 많이 있는 비트열은 암호화한 데이터가 아니라, 포렌식 분석 도구가 해석하

12) 삭제 방식에 따라 복구되지 않는 경우도 있다.

지 못한 데이터를 분석가에게 알려주기 위해 출력된 것으로 판단된다. (본 연구팀에서는 FINAL Mobile Forensics5을 보유하고 있지 않으므로 재현 실험을 진행하지 못하였다.)

Address ▼	Data	
00837634 - 00837848	09 C7 00 D7 45 00 01 19 00 05 05 00 02 09 01 09 08 00 81 39 00 08 08 ...	
06414350 - 06417939	00 0...	
06357038 - 06357041	00 00 00 00	
06283308 - 06283420	00 0...	

00000000:	09 C7 00 D7 45 00 01 19	00 05 05 00 02 09 01 09	.??.....
00000010:	08 00 81 39 00 08 08 08	09 08 01 01 00 00 00 00	..?.....
00000020:	00 00 00 00 08 00 00 00	00 00 00 00 00 00 05 08
00000030:	02 21 19 01 00 08 08 08	09 08 08 08 00 00 00 08	!......
00000040:	08 08 08 08 05 09 08 01	08 77 30 31 39 31 31 34w019114
00000050:	01 4E 9E 4D D9 B8 01 4E	9E 4D D9 B8 10 02 FF 5B	.N摸.N摸.. [
00000060:	4C 47 20 55 2B 5D 20 28	4C 54 45 20 36 32 29 20	LG U+] (LTE 62)
00000070:	EA B8 B0 EB B3 B8 EB 8D	B0 EC 9D B4 ED 84 B0 20	接접보?것??
00000080:	36 2E 30 30 47 42 20 EC	A4 91 20 38 30 25 28 34	6.00GB 以?80% (4
00000090:	2E 38 32 47 42 29 EC 9D	B4 EC 83 81 EC 9D 84 20	.82GB) ?억??

[그림 10] Oxygen Forensic SQLite Viewer 분석 결과

[그림 10]은 Oxygen Forensic SQLite Viewer ver. 2.3.0.8을 이용하여 문자메시지 파일에서 삭제된 데이터를 복구한 결과이다. 여기서도 삭제된 데이터의 일부가 파편 형태로 존재함을 알 수 있다.

[관련기사]

- 미디어워치TV, 변희재 ‘태블릿 PC 조작 특검법 발의 100% 가능’ 13)

13) <http://www.mediawatch.kr/news/article.html?no=252444>

7. 자동 생성 파일에 대한 설명

안드로이드 운영체제가 탑재된 시스템은 전원이 켜지기만 하더라도 자동으로 생성되는 파일이 있다. 이 파일들은 기기가 켜져 있을 때, 사용자가 삽입 또는 생성한 파일이 아니라 시스템이 자동으로 생성하며, 이러한 형태의 파일을 조사해 본 결과 [표 4]와 같다.

[표 4] 안드로이드 기기에서 자동으로 생성하는 파일의 종류

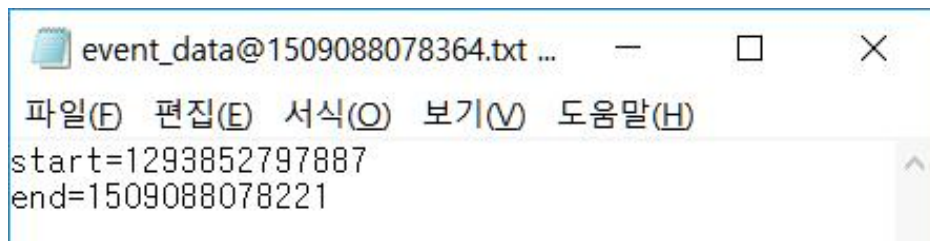
저장경로와 파일명	설 명
/data/system/dropbox/ event_data@(숫자).txt	기기가 켜져 있을 때, 자동으로 생성되는 파일이다. 파일 내용에 기록되어 있는 시간은 유닉스 시간(UNIX time) 이다.
/data/system/dropbox/ event_log@(숫자).txt	
/data/system/dropbox/ system_boot@(숫자).txt	기기가 부팅되는 시점에 자동으로 생성되는 파일이다. 파일 내용은 기기의 빌드정보, 하드웨어 정보, 커널 버전 등이 저장되어 있다.
/data/data/.drm/.playready/ devicefriendlyname.txt	기기에서 운영체제의 업데이트가 진행될 때 생성되는 파일이다. 쟁점 태블릿PC와 유사한 초기 안드로이드 버전에서만 관찰되었다.
/data/misc/wifi/ ipconfig.txt	Wi-fi에 연결될 때 관련 정보가 저장되는 파일이다.
/data/misc/ akmd_set.txt	기기에 내장된 중력 센서에서 변화가 감지될 때(태블릿을 기울여 가로/세로 모드가 바뀔 때)의 기록이 저장되어 있다.
/data/log/ dumpstate_shutdown.txt	기기를 강제로 종료할 때 발생한 로그를 저장하는 파일이다. 기기가 종료되는 시점이 기록되어 있다.

* 저장경로에 포함되어 있는 dropbox는 클라우드 스토리지 서비스와 무관하다.

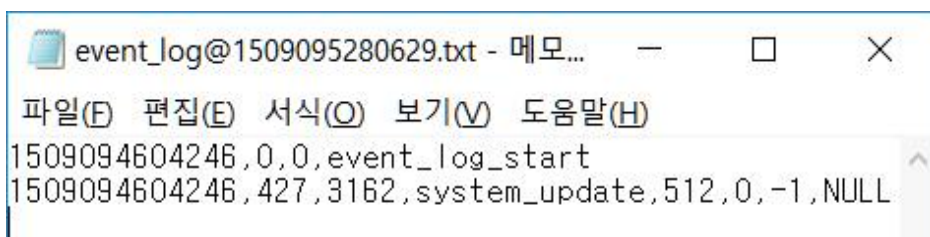
** 저장경로나 파일명, 파일의 생성 여부는 대상 기기에 따라 상이할 수 있다.

이 파일들이 생성되는 원인은 정확하게 파악하지 못하였지만, 안드로이드 기기를 소지하고 있다면 누구든지 자신이 삽입 또는 생성하지 않은 파일들이 저장되어 있음을 확인할 수 있다.

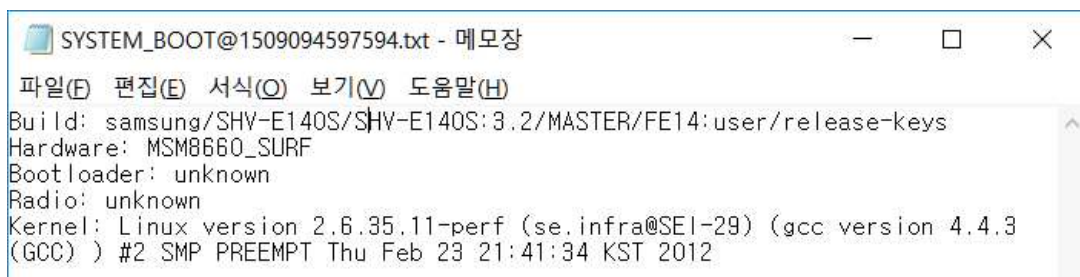
본 연구팀에서는 쟁점 태블릿PC와 동일한 모델의 기기를 이용하여 재현 실험을 통해 event_data@(숫자).txt 파일과 event_log@(숫자).txt 파일이 생성됨을 확인하였다. 또한 안드로이드 운영체제를 사용하는 갤럭시 노트3, 갤럭시 노트4, 갤럭시 노트5, 갤럭시 S6, 갤럭시 S6 edge 모델에서도 자동으로 생성되었으며, 이러한 파일들의 내용은 [그림 11-16]과 같다.



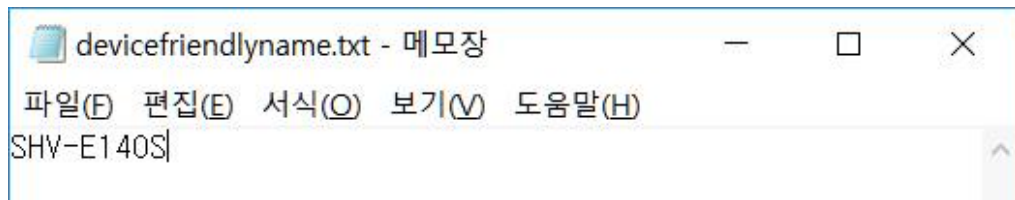
[그림 11] event_data@(숫자).txt 파일 내용(예시)



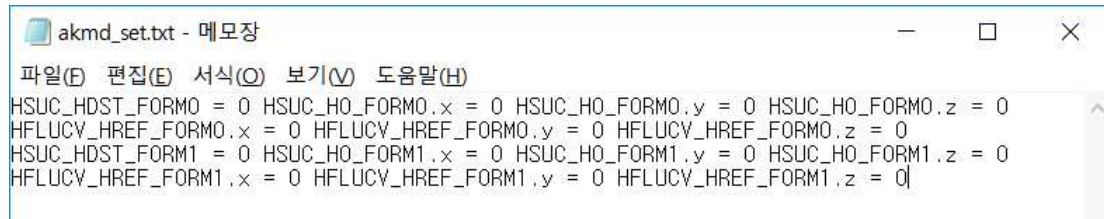
[그림 12] event_log@(숫자).txt 파일 내용(예시)



[그림 13] system_boot@(숫자).txt 파일 내용(예시)



[그림 14] devicefriendlyname.txt 파일 내용(예시)



[그림 15] akmd_set.txt 파일 내용(예시)



[그림 16] dumpstate_shutdown.txt 파일 내용(예시)

추가적으로 자동 생성파일이 최근에 사용한 시간에 따라 얼마나 생성되는지 조사하여 쟁점 태블릿PC에 저장되어 있는 파일의 개수와 비교하였다. 비교 결과는 [표 5]와 같으며, 검찰 보고서의 결과와 유사함을 알 수 있다.

[표 5] 자동 생성 파일의 생성 빈도를 비교한 결과

구 분		기간 (시간)	event_data@(숫자).txt (개)	event_log@(숫자).txt (개)
대 조 군	갤럭시 노트3	15	25	3
	갤럭시 노트4	49	94	6
	갤럭시 노트5	72	68	14
	갤럭시 S6	222	82	13
	갤럭시 S6 edge	71	138	22
대조군 평균		85.8	81.4	11.6
갤럭시탭 8.9 LTE (쟁점 태블릿PC와 동일한 기종)		72	146	2

8. 앱 접속 기록에 대한 설명

태블릿PC에 설치되어 있는 앱을 사용한 흔적은 SQLite 형식의 데이터베이스 파일인 /data/system/ 경로의 dmappmgr.db 파일에 저장된다. dmappmgr.db 파일은 [표 6]과 같이 앱을 사용한 흔적을 저장한다. 이 파일은 업데이트 30분 이후 다른 앱이나 서비스를 사용할 경우 갱신되며 사용자가 구글 플레이를 통해서 설치한 앱 외에도 기본적으로 동작하고 있는 앱을 포함하여 그 사용 흔적을 저장한다.

[표 6] /data/system/dmappmgr.db 파일의 내부 데이터

구분(컬럼명)	저장된 데이터 의미
pkgname	동작시킨 앱 이름
lastlaunchtime	앱이 실행된 시간
lastpausetime	앱이 구동되는 중에 뒤로가기 버튼이나 홈버튼을 눌러서 일시중지된 시간
applastservicestarttime	마지막으로 앱의 서비스가 시작한 시간
applastservicestoptime	마지막으로 앱의 서비스가 멈춘 시간
launchcount	앱을 동작시킨 횟수
totalusagetime	앱이 동작한 총 시간

* 서비스(Service)¹⁴⁾ : 안드로이드의 백그라운드에서 동작하는 컴포넌트

* 각 컬럼에서 저장하는 데이터의 의미를 파악한 결과, 약 30분을 주기로 앱의 구동 여부를 확인하고 변경사항이 생겼을 경우 데이터베이스 파일에 저장되어 있는 내용을 갱신하거나 추가하는 것으로 확인하였다.

14) <https://developer.android.com/guide/components/services.html?hl=ko>

본 연구팀은 쟁점 태블릿PC와 동일한 기종의 태블릿PC를 이용하여 태블릿PC를 공장 초기화한 후, 캘린더 앱을 2017.10.28. 15:21:30에 1회 동작시키고 멈추도록 하였다. 그리고 2017.10.28. 16:04:07에 다시 동작시켰다. dmappmgr.db 파일의 내부 데이터는 [그림 17]과 같은 변화가 있었다.

이 데이터베이스 파일이 저장하는 데이터는 앱의 구동과 관련하여 가장 마지막 시간만 저장한다는 특징이 있다. 갱신되기 전에 저장하던 데이터는 삭제된다. 따라서 앱의 사용내역을 확인하기 위해서는 앱을 동작시킨 횟수, 앱이 동작한 총 시간과 같은 다른 정보를 참고하여야 한다.

_id	pkgname	lastpausetime	applastservicestarttime	applastservicestoptime	totalusagetime	launchcount	lastlaunchtime
Click here to define a filter							
15	com.google.android.location	(null)	1509171806180	1509172890645	(null)	(null)	(null)
16	com.sktelecom.dm	(null)	1509171131313	1509171131388	(null)	(null)	(null)
17	com.skt.skaf.Z0000SLOAD	(null)	1509170964998	1509172890755	(null)	(null)	(null)
18	com.sec.phone	(null)	1509170942485	1509172890830	(null)	(null)	(null)
19	com.sec.android.app.factorytest	(null)	1509170956802	1509172890874	(null)	(null)	(null)
20	com.sec.android.widgetapp.weathernewsclck	(null)	1509171154664	1509172890922	(null)	(null)	(null)
21	com.sec.android.app.sns	(null)	1509170945400	1509172890974	(null)	(null)	(null)
22	com.qualcomm.wiper	(null)	1509170942581	1509172891022	(null)	(null)	(null)
23	com.google.android.partnersetup	(null)	1509171858645	1509172891070	(null)	(null)	(null)
24	com.android.exchange	(null)	1509171693305	1509172891147	(null)	(null)	(null)
25	com.sec.android.providers.downloads	(null)	1509172301106	1509172891196	(null)	(null)	(null)
26	com.android.systemui	(null)	1509170934968	1509172891247	(null)	(null)	(null)
27	com.android.providers.calendar	(null)	1509171690561	1509171691568	(null)	(null)	(null)

↓ 2017.10.28 15:21:30 (UTC+9)

_id	pkgname	lastpausetime	applastservicestarttime	applastservicestoptime	totalusagetime	launchcount	lastlaunchtime
Click here to define a filter							
15	com.google.android.location	(null)	1509174203368	1509176247360	(null)	(null)	(null)
16	com.sktelecom.dm	(null)	1509176209944	1509176210007	(null)	(null)	(null)
17	com.skt.skaf.Z0000SLOAD	(null)	1509174233697	1509176247401	(null)	(null)	(null)
18	com.sec.phone	(null)	1509174218183	1509176247437	(null)	(null)	(null)
19	com.sec.android.app.factorytest	(null)	1509176038102	1509176247462	(null)	(null)	(null)
20	com.sec.android.widgetapp.weathernewsclck	(null)	1509174325754	1509176247498	(null)	(null)	(null)
21	com.sec.android.app.sns	(null)	1509174221696	1509176247518	(null)	(null)	(null)
22	com.qualcomm.wiper	(null)	1509174218326	1509176247538	(null)	(null)	(null)
23	com.google.android.partnersetup	(null)	1509174229722	1509176247564	(null)	(null)	(null)
24	com.android.exchange	(null)	1509174275328	1509176247619	(null)	(null)	(null)
25	com.sec.android.providers.downloads	(null)	1509176209672	1509176247603	(null)	(null)	(null)
26	com.android.systemui	(null)	1509174198672	1509176247643	(null)	(null)	(null)
27	com.android.providers.calendar	(null)	1509174247362	1509176247660	(null)	(null)	(null)

↓ 2017.10.28 16:04:07 (UTC+9)

[그림 17] dmappmgr.db 파일의 내부 데이터 변화(앱 재동작 전후)

위에서 말한 것처럼 동일한 앱의 이전 정보는 저장하지 않고 삭제되기 때문에 삭제된 데이터가 존재한다면, 최신 정보로 업데이트되는 과정에서 기존에 저장하고 있던 데이터가 삭제된 것이다.

따라서 검찰 보고서 336페이지부터 337페이지의 상태 정보가 ‘삭제’인 데이터는 의도적으로 앱을 삭제한 것이 아니라, 앱의 사용 정보가 갱신되면서 삭제된 이전 정보이다. 만약 JTBC가 새롭게 부팅하였을 때 앱이 업데이트되는 동작이 진행되었다면 검찰 보고서의 분석내용은 자연스러운 결과로 판단된다.

[관련기사]

- 한국경제, ‘최순실 태블릿PC’ 등장 1년... 여전한 논란들¹⁵⁾
- 월간조선, 최순실 태블릿 속 카카오톡 대화명 ‘선생님’은 최순실이 아닌 김한수 전 청와대 행정관¹⁶⁾

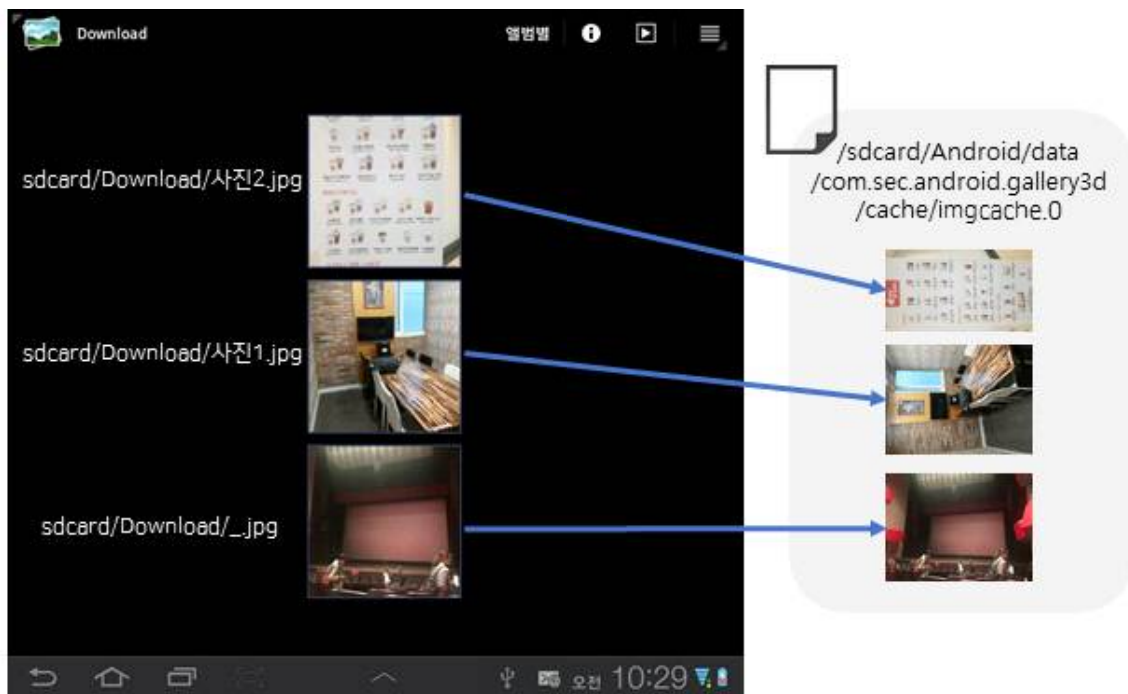
15) <http://news.hankyung.com/article/2017102344401>

16) http://monthly.chosun.com/client/mdaily/daily_view.asp?Idx=1831&Newsnumb=2017101831

9. 썸네일(Thumbnail)에 대한 설명

썸네일은 그래픽 파일의 이미지나 동영상 파일의 일부 장면을 원본보다 작은 이미지로 소형화한 것을 말하며, 미리보기 목적으로 갤러리, 웹브라우저, 메신저 등 대부분의 서비스에서 활용된다.

스마트폰에서 촬영한 사진을 확인할 수 있는 갤러리 앱도 마찬가지로 썸네일 파일을 생성하고 관리한다. 썸네일의 저장경로는 앱별로 상이하다. 쟁점 태블릿 PC의 경우 갤러리 앱의 썸네일 파일은 /sdcard/Android/data/com.sec.android.gallery3d/cache/에 저장되어 있다. 각 이미지 파일에 대한 썸네일은 imgcache.0 또는 imgcache.1 파일의 내부에 저장되어 있다.



[그림 18] 원본 이미지 파일과 썸네일 사이의 관계도(예시)

imgcache는 안드로이드 시스템에서 갤러리 앱이 처음으로 썸네일을 만들 때 생성된다. 생성된 후로는 갤러리 앱이 썸네일을 imgcache에 추가하는 방식으로 동작하므로 썸네일이 추가되면 imgcache 파일은 수정시간만 변경된다. [표 7]에서 확인할 수 있듯이 imgcache.0의 생성시간은 사진1.jpg의 생성시간인 15시 27분 보다 늦은 15시 28분이나 사진2.jpg와 _3.jpg의 생성

시간은 이보다 늦은 시간이다. 따라서 사진1.jpg 파일이 저장된 이후 갤러리 앱으로 열람하면서 imgcache.0 파일이 생성되면서 사진1.jpg 파일의 썸네일이 추가되었고, 그 이후 다른 이미지 파일의 썸네일이 추가된 것을 알 수 있다. 즉, imgcache.0 파일의 수정시간은 원본 사진 파일들의 생성·수정시간보다 늦은 시간임을 알 수 있다.

갤러리 앱에서 imgcache에 썸네일을 추가하는 시간은 사용자의 행위 이후 내부 프로그램에 의해 결정되기 때문에 정확하게 변경되는 시간은 알 수 없지만 마지막으로 사진파일을 열람한 이후에 imgcache 파일의 수정시간이 갱신된다.

[표 7] 사진 파일과 썸네일의 시간 정보 예시

파일명	생성시간	수정시간
imgcache.0	2017/10/28 15:28:29	2017/10/28 15:51:51
사진1.jpg	2017/10/28 15:27:22	2017/10/28 15:27:23
사진2.jpg	2017/10/28 15:29:16	2017/10/28 15:29:16
_3.jpg	2017/10/28 15:31:42	2017/10/28 15:31:43

따라서 imgcache.0 파일의 시간정보로부터 사진파일이 생성된 시간을 추정하는 것은 잘못된 판단이며 원본 파일의 시간 정보로부터 확인해야 한다.

[관련기사]

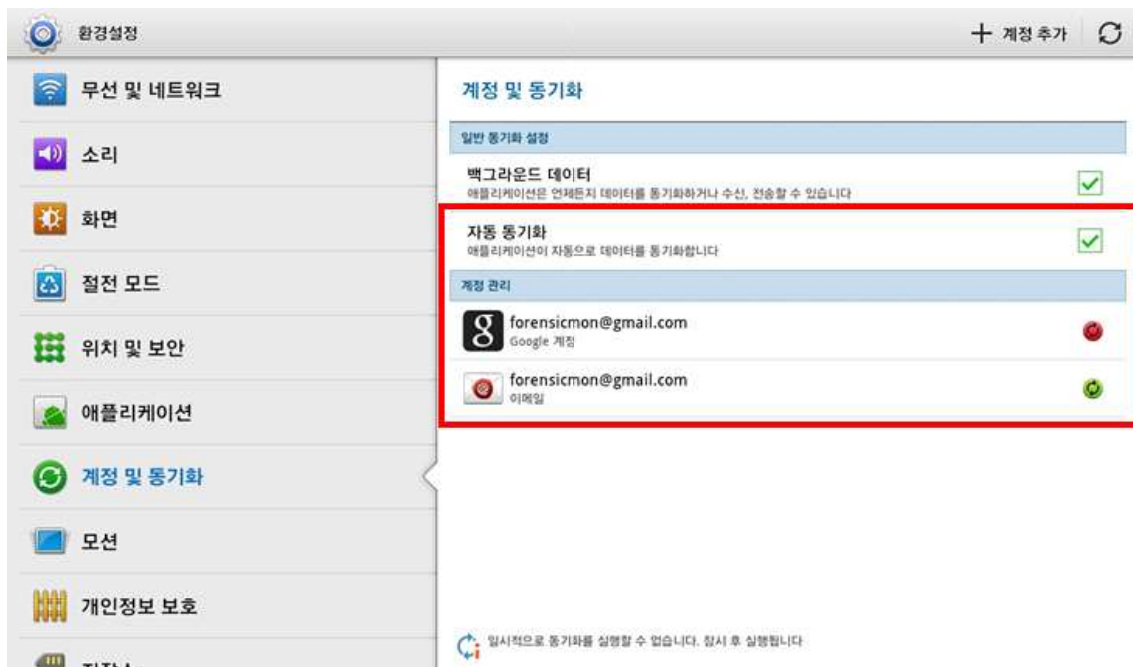
- 국제신문, 태블릿 PC 보도 1년, 김진태 “최순실 태블릿 PC 조작” 공방 보니¹⁷⁾

17) <http://www.kookje.co.kr/news2011/asp/newsbody.asp?code=0100&key=20171024.99099007716>

10. 자동 로그인 및 동기화 기능에 대한 설명

안드로이드 기기에서는 클라우드 서비스나 페이스북과 같은 SNS에 접근할 때 매번 아이디와 패스워드를 입력하지 않아도 접근하게 해주는 자동 로그인 기능이 있다.

대부분 구글 계정의 자동 로그인 기능을 설정하여 사용한다. [그림 19]는 별도의 아이디와 패스워드 정보 없이도 자동 접속될 수 있게 계정 관리에 자동 로그인이 활성화된 상태이며, 추가적으로 해당 계정에 존재하는 데이터를 자동 동기화할 수 있도록 자동 동기화 기능도 선택된 상태이다.



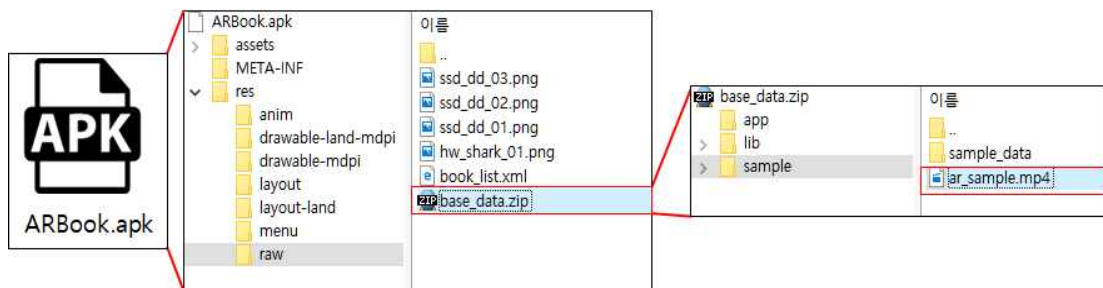
[그림 19] 갤럭시탭 8.9 LTE 모델의 동기화 설정 항목

검찰 보고서 403페이지의 2016년 10월 18일 오후 3시32분27초에 수신한 메일은 보안이 강화된 구글의 정책에 의해 새로운 기기에서 로그인이 되었을 경우 자동적으로 발송되는 메일이다. 쟁점 태블릿PC의 자동 동기화 기능이 활성화되어 있어 해당 계정으로 발송된 메일이 태블릿에 저장된 것으로 보인다. 따라서, JTBC에서 아이디와 패스워드 정보를 직접 입력하여 수신한 메일은 아니다.

11. ar_sample.mp4 파일에 대한 설명

ARBook 앱은 증강현실 기술을 활용하여 책의 이미지를 애니메이션으로 보여주는 앱이다. 이 앱은 쟁점 태블릿PC와 동일한 모델에 기본으로 설치되어 있으며 태블릿PC를 공장초기화 하여도 삭제되지 않고 남아있다.

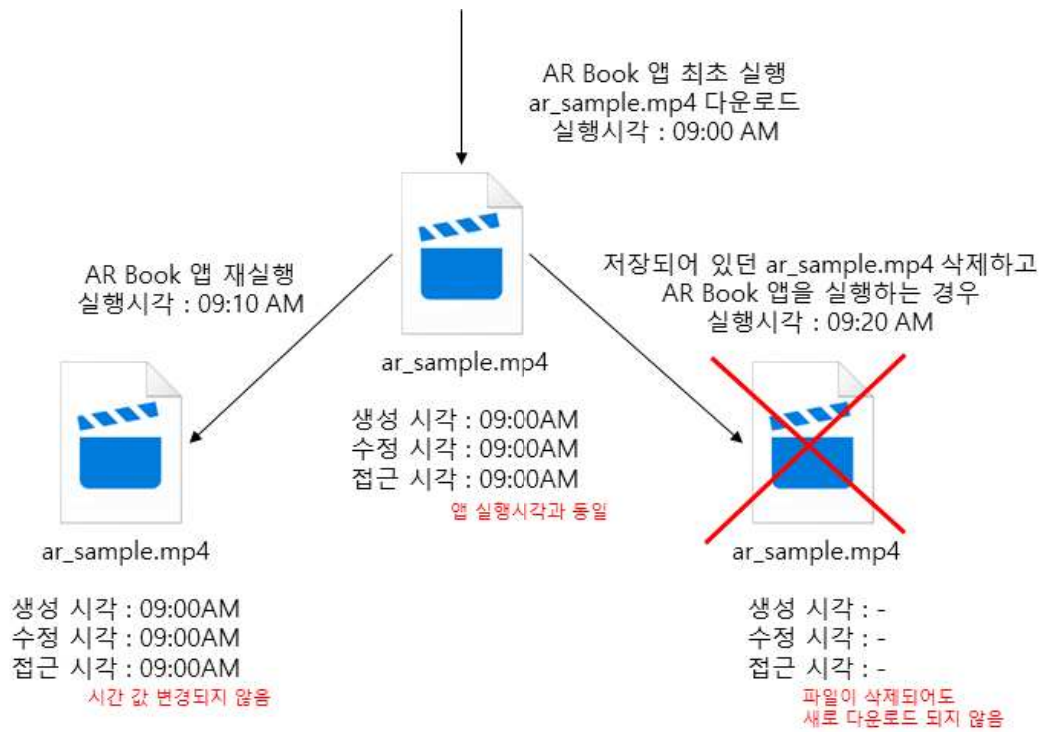
ARBook 앱의 설치파일(ARBook.apk 파일)에는 ar_sample.mp4 이름의 동영상 파일이 포함되어 있다. 이 동영상 파일은 apk파일 내 /res/raw 경로의 base_data.zip 압축파일에 압축되어 있으며, 압축파일 내 /sample 경로에 저장되어 있다. [그림 20]은 apk파일 내에 있는 ar_sample.mp4 파일의 저장 위치를 나타낸 것이다.



[그림 20] apk파일 내 ar_sample.mp4 파일의 저장 위치

ARBook 앱이 기기에서 최초로 실행되면, apk파일 내 ar_sample.mp4 파일이 추출되어 해당 기기의 /data/com.samsung.arbook.ARBook/sample/ 경로에 저장된다. 쟁점 태블릿PC와 동일한 모델의 기기에 설치되어 있는 ARBook 1.06 앱을 최초로 실행하면, 동영상 파일이 새로 생성됨을 실험을 통해 확인하였으며, 상위 업데이트 버전인 1.31버전에서도 동일한 방식으로 동작하는 것을 확인하였다.

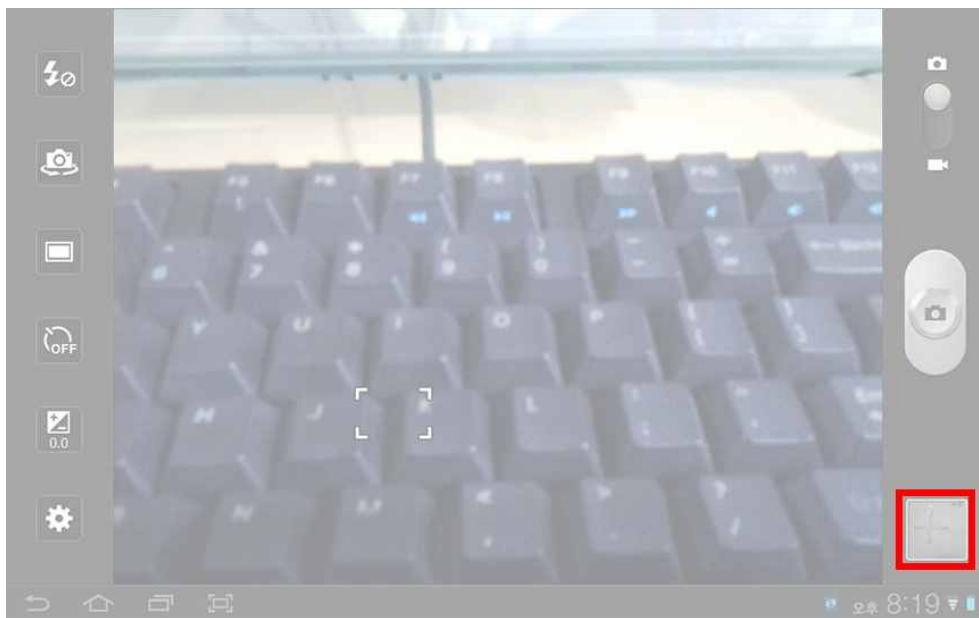
앱이 재실행(최초 실행이 아닌 경우)될 경우에는 동영상 파일이 새로 생성되지 않으며 최초 실행으로 저장된 동영상 파일을 삭제한 후에 앱을 재실행하더라도 새로 생성되지 않는 것을 실험으로 확인하였다. [그림 21]은 본 연구팀이 진행한 실험에서 ARBook 앱 실행에 따른 ar_sample.mp4 파일의 시간 값을 확인한 내용을 표현한 것으로, ar_sample.mp4 파일의 생성시간을 통해 ARBook 앱이 최초로 실행된 시간을 알 수 있다.



[그림 21] ar_sample.mp4 파일 생성 및 시간 값 변경 원리

12. 검찰 보고서의 970, 1805, 1871 사진 파일에 대한 설명

.tec 파일은 카메라 앱 상에서 촬영한 사진을 바로 확인할 때, 사용하는 퀵뷰 앱(QuickView.apk)에서 생성하는 캐시 파일이다. [그림 22]는 카메라 앱을 실행시킨 상태이며, 여기서 우측 하단의 사진을 클릭하면 퀵뷰 앱이 실행된다. 사진을 촬영한 후 갤러리 앱에서 사진을 확인하면, .tec파일이 생성되지 않고, 퀵뷰 앱을 통해 사진을 확인할 경우에만 .tec 파일이 생성된다.



[그림 22] 퀵뷰 앱(QuickView.apk)

본 연구팀에서 생점 태블릿PC와 동일한 기종의 태블릿PC로 실험한 결과, 저장되어 있는 사진 파일을 갤러리 앱에서 회전시키면 대상 사진 파일의 생성시간은 회전시킨 시간으로 변경된다. 하지만 회전된 내용이 자동으로 .tec 파일로 생성되는 것은 아니며 퀵뷰 앱에서 회전된 사진을 열람해야만 .tec 파일이 추가 생성된다. 즉, 특정 사진 파일을 갤러리 앱에서 회전시킨 사진 파일은 회전시킨 시간으로 생성시간이 변경되며, .tec 파일은 퀵뷰 앱에서 열람한 시간으로 추가 생성된다. 참고로 퀵뷰 앱에서는 사진을 편집하는 기능이 없다.



[그림 23] 킥뷰 앱에서 사진을 열람하는 화면(편집 기능이 없음)

테블릿PC에서 촬영하면, 촬영된 사진의 파일명은 촬영한 ‘시각.jpg’ (예:20171128_121335.jpg, YYYYMMDD_hhmmss.jpg 형태)으로 명명된다. 그리고 킥뷰 앱을 사용한 경우에는 .tec 파일이 생성되기 때문에 이 때의 생성시간으로 해당 사진 파일을 킥뷰 앱에서 열람한 시간을 알 수 있다. 또한 사진을 회전시키면, 해당 사진 파일의 생성시간이 회전시킨 시간으로 변경된다.

위의 세 가지 사실을 종합하여 .tec 파일의 쟁점사항에 대해 해석이 가능하다. 파일명으로부터 사진의 촬영시간, .tec 파일의 생성시간으로부터 킥뷰 앱을 통한 최초 열람시간, .jpg 파일의 생성시간으로부터 사진의 최종 회전시간을 알 수 있다.

[표 8] 사진파일의 부가정보를 이용한 행위 분석

대 상	항 목	행 위	조건
JPG 파일	파일명	사진을 촬영한 시각	—
TEC 파일	파일 생성시간	킥뷰 앱을 통한 최초 열람시간	—
JPG 파일	파일 생성시간	사진이 최종 회전(편집)된 시각	(파일명 시간) < (파일 생성시간)

[표 9] 검찰 포렌식 분석결과에 포함된 사진파일

번호	사진	파일명	찍은 날짜	생성시간 / 접근시간	수정시간
970		001038810 3883.tec		2012.06.25 19:20:34	2012.06.25 19:20:34
1805		20120625_1 91956.jpg	2012.06.25 19:19:56	2016.10.18 17:43:07	2016.10.18 17:43:08
1871		001038810 3885.tec		2016.10.21. 22:51:36	2016.10.21. 22:51:37

[표 9]는 검찰 포렌식 분석결과 중 .tec 파일에 대한 설명을 위해 일부 발췌한 내용이다. 1805번 사진 파일은 2012년 6월 25일 19시19분56초에 촬영되었고, 해당 사진 파일을 대상으로 하는 사용자 행위에 대한 시나리오를 [표 10]으로 나타내었다.

[표 10] .jpg 파일과 .tec 파일 대상 사용자 행위 시나리오

시 각	사용자 행위	태블릿PC 동작
2012.06.25 19:19:56	사진 촬영	20120625_191956.jpg 파일(1805번 사진) 생성
2012.06.25 19:20:34	뷰 앱 실행	0010388103883.tec 파일(970번 사진) 생성
2016.10.18 19:43:07	사진 회전	20120625_191956.jpg 파일(1805번 사진) 생성시간 변경
2016.10.21 22:51:36	뷰 앱 실행	0010388103885.tec 파일(1871번 사진) 생성


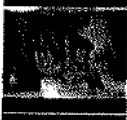

추가적으로 본 연구팀은 쟁점 태블릿PC와 동일한 기종의 태블릿PC로 사진을 촬영할 때 가로(landscape) 모드와 세로(portrait) 모드로 촬영한 사진 파일에 대한 재현실험을 하였다. 쟁점 태블릿PC는 자동회전 기능과 전·

후방 카메라를 가지고 있으므로 가능한 모든 경우를 설정하여 촬영된 사진 파일의 원본 JPG 파일, 회전시킨 JPG 파일, .tec 파일에 대해서 생성시간과 저장되어 있는 사진 내용을 확인하였다. 쟁점 태블릿PC는 사진의 높이와 너비가 자동회전 기능과 무관하게 고정되어 촬영되며, JPG 파일의 EXIF는 해상도(height, width)와 방향(orientation) 정보를 포함한다. .tec 파일은 사용자 화면과 동일하게 저장된다는 점을 확인하였다.

가. 국과수 감정 보고서 의견 관련

국과수 보고서 <그림 29. 장승호 사진 3장 정보>의 의견 ‘한편, 그림 28의 20120625_191956.jpg 사진 파일은 붉은 색 네모 박스로 표기한 바와 같이 파일명, 생성 일시, 수정 일시가 차이가 있으며, EXIF 정보도 다른 파일들과 다르게 구성되어 있어 본 카메라 촬영된 파일의 원본으로 볼 수 없음.’에 대해 설명하고자 한다.

4) 한편, 그림 28의 20120625_191956.jpg 사진 파일은 붉은 색 네모 박스로 표기한 바와 같이 파일명, 생성 일시, 수정 일시가 차이가 있으며, EXIF 정보도 다른 파일들과 다르게 구성되어 있어 본 카메라 촬영된 파일의 원본으로 볼 수 없음.

파일 이름	미리 보기	크기정보	EXIF	날 짜
20120625_192129.jpg		오프셋 : 0 너 비 : 2,048 높 이 : 1,536	카메라 제조사 : SAMSUNG 카메라 모델 : SHV-E140S 소프트웨어 : FB23 촬영 일시 : 2012-06-25 19:21:28 저장 일시 : 2012-06-25 19:21:28	생성 일시 : 2012-06-25 19:21:29 수정 일시 : 2012-06-25 19:21:29 접근 일시 : 2012-06-25 19:21:29
20120625_192134.jpg		오프셋 : 0 너 비 : 2,048 높 이 : 1,536	카메라 제조사 : SAMSUNG 카메라 모델 : SHV-E140S 소프트웨어 : FB23 촬영 일시 : 2012-06-25 19:21:33 저장 일시 : 2012-06-25 19:21:33	생성 일시 : 2012-06-25 19:21:34 수정 일시 : 2012-06-25 19:21:34 접근 일시 : 2012-06-25 19:21:34
20120625_191956.jpg		오프셋 : 0 너 비 : 2,048 높 이 : 1,536	카메라 제조사 : SAMSUNG 카메라 모델 : SHV-E140S	생성 일시 : 2016-10-18 17:43:07 수정 일시 : 2016-10-18 17:43:08 접근 일시 : 2016-10-18 17:43:07

이 정보가 없음

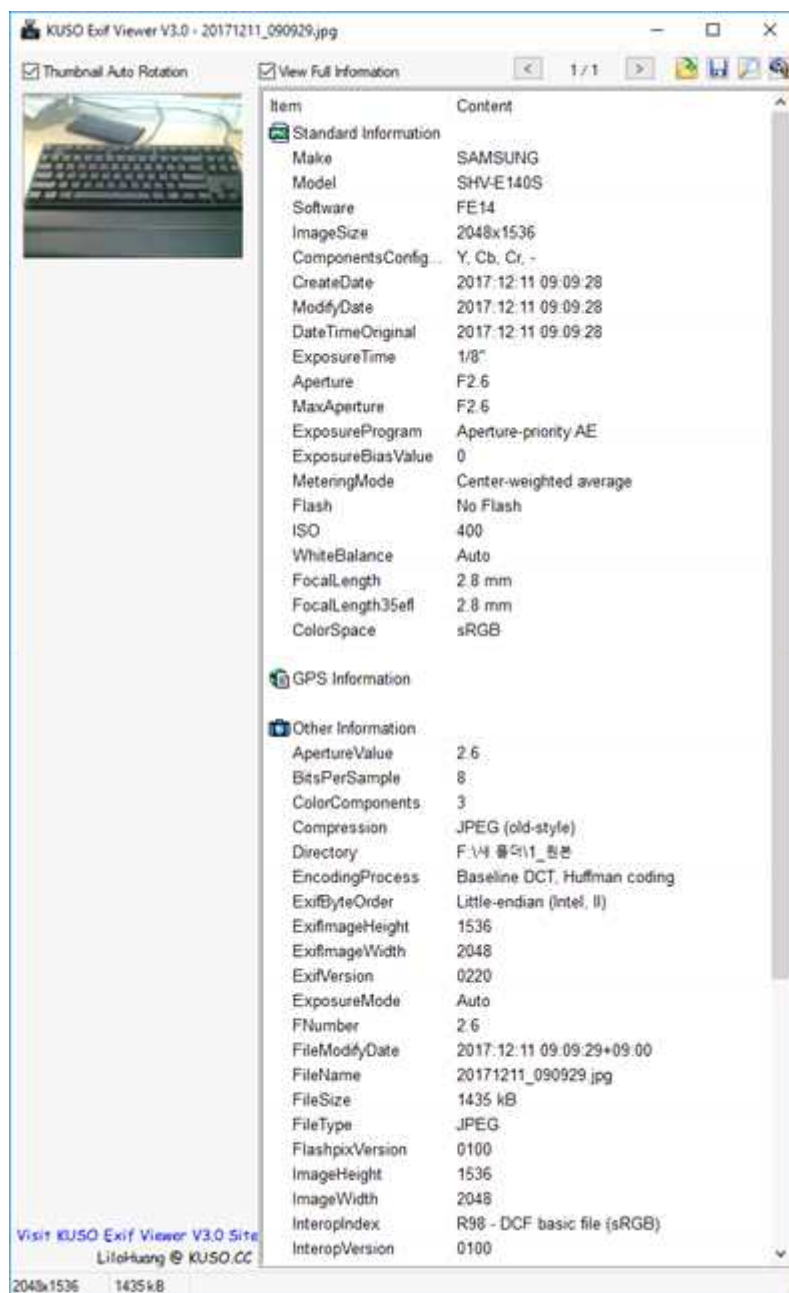
<그림 28. 장승호 사진 3장 정보>

[그림 24] 국과수 보고서 일부

쟁점 태블릿PC는 갤러리 앱에서 사진 회전 기능이 있으며, 동일한 기종의 태블릿PC를 이용한 실험을 통해 사진을 회전할 경우 EXIF 정보 일부가 삭

제되는 것을 확인하였다.

[그림 25]는 촬영된 사진의 원본파일에 있는 EXIF 정보를 나타낸다. [그림 26]은 갤러리 앱에서 원본 파일을 시계방향으로 1번 회전 후, 다시 반시계 방향으로 1번 회전하여 원 사진과 동일한 각도로 변경한 파일의 EXIF 정보이다. [그림 25]와 [그림 26]을 통해 상당히 많은 EXIF 정보가 삭제되는 것을 알 수 있으며, 국과수 보고서에 있는 소프트웨어와 촬영 일시, 저장 일시에 해당하는 항목들도 삭제되어 있음을 확인할 수 있다.



[그림 25] 사진 원본



[그림 26] 갤러리 앱에서 사진을 회전한 경우

나. 쟁점 사진파일들의 원본 식별

일부 사진들에 대해 사진이 조작되었으며, 제3자가 사진을 삽입하였다고 주장되는 의견이 있으나, 실험을 통해 .tec파일과 사진파일에 대한 쟁점 사항이 충분히 발생할 수 있음을 설명하였다. 추가적으로 이미지 조작과 관련된 사항의 경우 해당 기기에서 촬영된 사진임을 증명하기 위해서는 사진 파

일이 생성될 때 사용되는 DQT 테이블 정보를 활용하는 것이 좋다.

DQT¹⁸⁾란 JPEG 이미지 안에 포함된 양자화 테이블로써 이미지의 압축률을 결정하는데 사용된다. 이미지의 저장 방식이나 이미지의 화질에 따라 형태가 달라지며, 이는 사진을 촬영하거나 편집했을 때 촬영 기기나 편집 도구에 따라 서로 다른 DQT 형태를 가지게 되는 경우가 많으며, 이를 통해 동일한 기종에서 촬영되었는지 확인하는 정보로 활용할 수 있다.

쟁점 태블릿의 경우 원본 사진과 회전된 사진의 DQT 테이블이 동일한 것을 확인하였다. 이러한 실험결과를 통해 해당 쟁점 파일들을 분석한다면 DQT 테이블을 통해 다른 기종에서 촬영되었을 가능성을 판별할 수 있을 것이다.

현재까지 DQT 테이블 정보를 표현해주는 도구는 별도로 없으며, 본 연구 센터에서 개발한 JPEGViewer¹⁹⁾를 통해 확인할 수 있다. [그림 27]은 쟁점 태블릿에서 촬영한 사진의 DQT 테이블 정보를 나타낸 화면이다.

The screenshot shows the JPEG Viewer application. On the left is a file explorer showing a directory structure. The central pane displays a photograph of a computer keyboard. On the right, the 'Jpeg-Info' pane lists various metadata tags like ComponentsConfiguration, ShutterSpeedValue, ApertureValue, etc. Below this, the 'DQT' section is highlighted with a red box, showing a table of DQT IDs and their values.

DQT ID	Value
0	132
DQT, Row #0	1 1 1 1 1 2 2 2
DQT, Row #1	1 1 1 1 1 2 2 2
DQT, Row #2	1 1 1 1 2 2 3 2
DQT, Row #3	1 1 1 1 2 3 3 2
DQT, Row #4	1 1 1 2 3 4 4 3
DQT, Row #5	1 1 2 3 3 4 5 4
DQT, Row #6	2 3 3 3 4 5 5 4
DQT, Row #7	3 4 4 4 4 4 4 4
DQT ID	1
DQT, Row #0	1 1 1 2 4 4 4 4
DQT, Row #1	1 1 1 3 4 4 4 4
DQT, Row #2	1 1 2 4 4 4 4 4
DQT, Row #3	2 3 4 4 4 4 4 4
DQT, Row #4	4 4 4 4 4 4 4 4
DQT, Row #5	4 4 4 4 4 4 4 4
DQT, Row #6	4 4 4 4 4 4 4 4
DQT, Row #7	4 4 4 4 4 4 4 4

[그림 27] DQT 테이블 정보

18) 김민식, 정두원, 이상진. (2016). 스마트폰 JPEG 파일의 출처 식별을 위한 DQT 정보 데이터베이스 구축. 정보보호학회논문지, 26(2), 359-367.

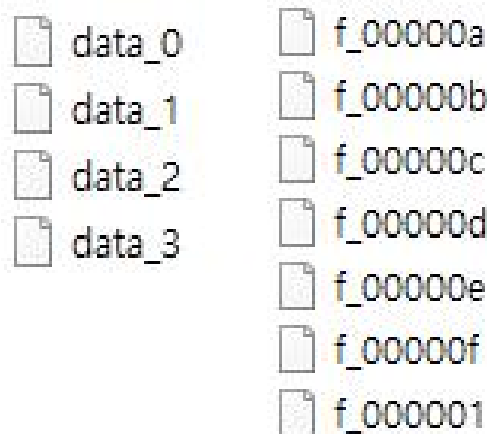
19) JPEGViewer : <http://forensic.korea.ac.kr/tools/jpegviewer.html>

13. 웹 캐시 파일에 대한 설명

캐시는 컴퓨터 과학에서 데이터나 값을 미리 복사해 놓는 임시 장소를 가리킨다. 캐시는 캐시의 접근 시간에 비해 원래 데이터에 접근하는 시간이 오래 걸리는 경우나 값을 다시 계산하는 시간을 절약하고 싶은 경우에 사용한다. 캐시에 미리 복사해 놓으면 계산이나 접근 시간 없이 더 빠른 속도로 데이터에 접근할 수 있다.²⁰⁾

웹 브라우저도 특정 사이트를 처음 방문하면 해당 사이트에 있는 html이나 image, js, css 등을 내려 받아 특정 위치에 복사본을 저장하는 캐시 기능이 있는데, 이 때 저장하는 파일을 웹 캐시라 말한다. 이후 동일한 사이트의 Resource를 요청하면 다시 내려 받지 않고 내부에 저장한 파일을 보여줌으로써 빠르게 서비스를 제공한다.

안드로이드 기본 웹 브라우저 앱의 패키지명은 “com.android.browser”이다. “/data/data/com.android.browser/cache”는 기본 브라우저 앱의 캐시 파일 저장 경로이다. 네이버 브라우저 앱의 패키지명은 “com.nhn.android.search”이다. “/data/data/com.nhn.android.search/cache”는 네이버 브라우저 앱의 캐시 파일 저장 경로이다.



[그림 28] 캐시 파일

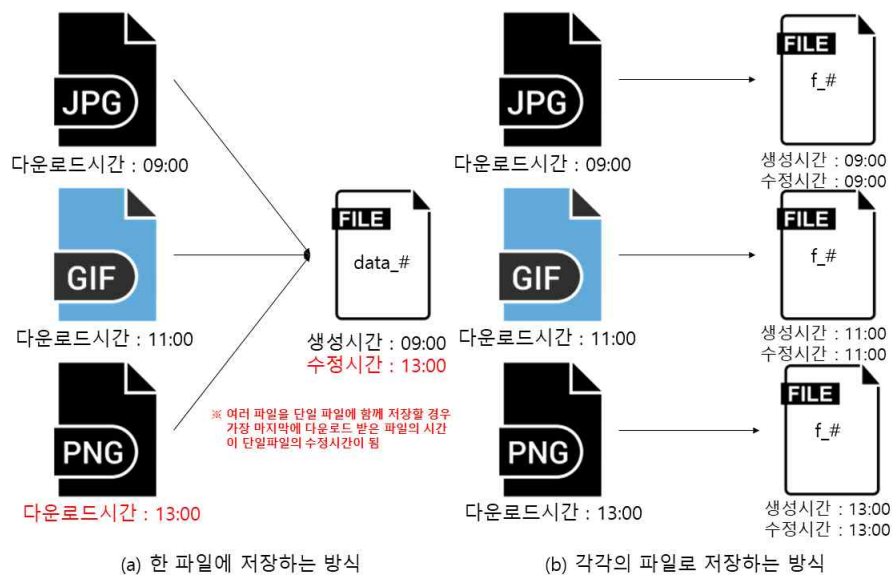
두 앱의 캐시 파일 저장 방식은 내려 받은 파일들을 하나의 캐시 파일에 저장하는 방식과 내려 받은 파일을 각각의 캐시 파일 형태로 저장하는 방식이 있으며, [그림 28]은 두 앱의 캐시 파일들이 저장되는 형태를 보여준다.

20) 캐시 (<https://ko.wikipedia.org/wiki/캐시>)

캐시 파일이 저장되는 폴더에는 index 파일과 4개의 데이터 파일이 저장되어 있다.

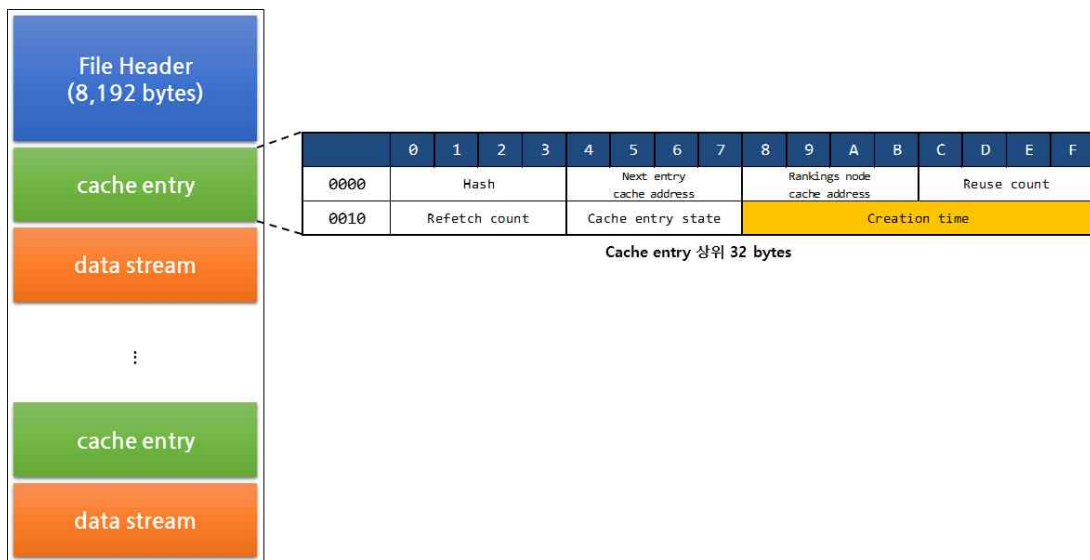
- index 파일 : 해시 정보 포함
- data_0 : 얼마나 자주 업데이트되는지에 대한 정보
- data_1 : 1Kbyte 이하의 데이터를 256byte 블록으로 나누어 저장
- data_2 : 4Kbyte 이하의 데이터를 1Kbyte 블록으로 나누어 저장
- data_3 : 16Kbyte 이하의 데이터를 4Kbyte 블록으로 나누어 저장
- 16Kbyte 이상의 데이터는 f_xxx로 시작하는 이름을 가지는 별도의 파일로 저장

data_1 ~ data_3에는 웹 캐시 데이터가 추가되는 방식이며, f_xxx로 시작하는 이름을 가지는 파일은 매번 생성되는 웹 캐시 데이터이기 때문에 해당 파일의 생성시간 및 수정시간은 [그림 29]와 같은 방식으로 정해진다.



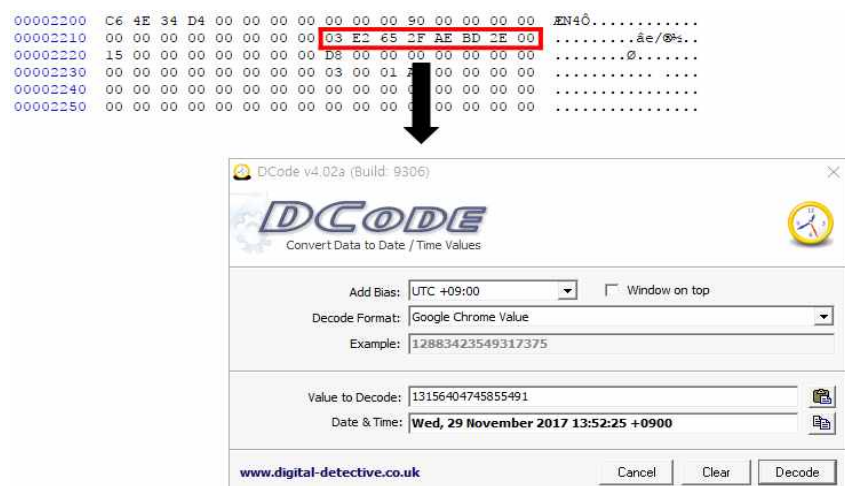
[그림 29] 웹 브라우저 캐시 생성시간 및 수정시간

따라서 한 파일로 저장하는 방식은 가장 처음에 캐시 파일이 저장된 시점에서 생성되어 생성시간은 변경되지 않고, 캐시 파일이 추가될 때 수정시간이 변경된다. 단, 한 파일로 저장하는 방식의 경우 data_# 파일의 내부 구조에서 각 캐시 파일의 생성시간을 알 수 있다. 각각의 파일로 저장하는 방식은 캐시 파일을 저장한 시간에 생성시간과 수정시간이 기록된다.



[그림 30] data_# 파일 내부 구조

[그림 30]은 한 파일로 저장하는 방식인 data_# 파일의 내부 구조²¹⁾이다. data_# 파일은 데이터 블록 파일이라고 하는데 파일 헤더와 캐시 엔트리 및 데이터 스트림으로 구성되어 있다. 파일 헤더에는 데이터 블록 파일의 메타데이터가 저장되어 있으며, 캐시 엔트리가 실제 캐시 파일의 메타 데이터, 데이터 스트림에는 실제 캐시 파일의 데이터를 포함하고 있다. 캐시 데이터의 메타 데이터를 포함하고 있는 캐시 엔트리의 구조를 살펴보면 캐시 데이터의 생성시간을 알 수 있다.



[그림 31] 캐시 엔트리 예시

21) 크롬 캐시 파일 구조, http://www.forensicswiki.org/wiki/Chrome_Disk_Cache_Format

[그림 31]은 캐시 엔트리 예시이다. 예시에서 알 수 있듯이 오프셋 0x18에서 8바이트가 캐시 파일의 생성시간이며, 시간 값 표현 형식은 구글 크롬에서 사용하는 방식이다.

본 연구팀에서는 쟁점 태블릿PC와 같은 기종의 태블릿PC에서 기본 웹 브라우저 앱과 네이버 브라우저 앱이 생성하는 웹 캐시의 개수에 대해서 실험하였다. 기본 웹 브라우저 앱과 네이버 브라우저 앱에서 네이버 포털 사이트 메인 페이지에 접속하였을 때 생성되는 캐시파일의 개수를 조사하였다. 그리고 이를 검찰 보고서에 있는 캐시 파일의 개수와 비교하였다. data 파일의 경우 각각의 이미지 파일에 대한 생성시간 및 수정 시간을 알 수 없기 때문에 [표 11]에서는 객관적인 평가를 위해서 단일 이미지 파일인 f_xxx 파일의 개수만 비교하였다. 또한 검찰 보고서의 이미지 파일 중에 수정 시간이 2016년도 이후인 파일만 개수에 포함하였다.

[표 11] f_xxx 형태의 웹 캐시 파일 개수 비교

구 분	실험 데이터	검찰 보고서
기본 웹 브라우저 앱	45개	26개 (2016년 10월 18일 생성) 50개 (2016년 10월 20일 생성)
네이버 브라우저 앱	66개	0개

실험 결과 네이버 포털 사이트 메인 페이지만 들어갔음에도 수십 개의 웹 캐시 파일이 생성되었다. 이를 검찰 보고서의 개수와 비교해 보았을 때, 검찰 보고서에 포함되어 있는 웹 캐시 파일은 일반적으로 생성될 수 있는 개수로 보인다.

웹 캐시의 개수는 방문하는 사이트의 구성 형태에 따라 천차만별이다. 광고가 많은 네이버는 상대적으로 웹 캐시가 많으며, 텍스트만 있는 사이트는 웹 캐시가 없을 수 있다. 따라서 웹 캐시가 2016년 10월 18일 이후 많이 생성되었다고 해서 이상한 일은 아니다.

14. 이메일 수신/발신 시간의 역전현상에 대한 설명

쟁점 태블릿 PC의 이메일 앱은 연동한 계정의 이메일 수신 및 발신 내역을 확인할 수 있다. 이메일 앱은 /data/com.android.email/databases/emailprovider.db 데이터베이스 파일에 [표 12]와 같이 메일의 수신 혹은 발신 기록을 저장한다.

[표 12] emailprovider.db 파일의 데이터 중 일부

구분(컬럼명)	저장된 데이터 의미
subject	수신 혹은 발신된 메일의 제목
fromList	발신자 계정
toList	수신자 계정
timeStamp	메일을 수신 혹은 발신한 시각
syncServerTimeStamp	메일이 기기에 동기화된 시각

이메일 앱은 위에서 언급한 것처럼 하나의 이메일에 대해 두 가지 시간 값을 기록하는데, 두 시간 값은 네트워크 상태에 따라 약간의 차이가 있을 수 있다. 수신한 이메일에 대한 기록은 연동한 계정이 이메일을 수신한 즉시 태블릿PC로 동기화하기 때문에 수신시간과 동기화된 시각이 동일하거나 근사한 값이 저장된다. 하지만 발신한 이메일에 대한 기록은 태블릿 PC에 즉시 동기화되는 것이 아니라, 태블릿PC의 동기화 주기 설정에 따라 자동으로 동기화 되거나, 사용자에 의해 수동으로 동기화되며 그 시각이 발신한 메일의 동기화 시각으로 저장된다.

수신 및 발신한 이메일의 동기화 시각이 이메일 앱 데이터베이스에 저장되는 방식을 확인하기 위한 실험을 진행하였다. 실험은 쟁점 태블릿PC와 동일한 기종의 태블릿PC 내 이메일 앱에 메일 계정(forensicmon@gmail.com)을 연동시키고, 앱 내부에서 연동한 메일 계정에게 2개의 메일을 전송하였다. 1번 메일은 2017년 11월 28일 22시 18분 49초에 전송한 “18분”이라는 제목의 메일이고 같은 날 22시 19분 22초에 수동으로 동기화하였다.

2번 메일은 2017년 11월 28일 22시 21분 46초에 전송한 “21” 이라는 제목의 메일이며 같은 날 22시 23분 04초에 수동으로 동기화하였다. 태블릿 PC에 연동되어있는 메일 계정으로부터 동일한 계정에 메일을 보낸 것이므로, 이메일 앱에서는 하나의 메일에 대하여 수신정보와 발신정보가 각각 기록된다. 본 실험에서는 2개의 메일을 전송하였으므로 총 4개의 메일 정보가 데이터베이스 파일에 저장되며 데이터베이스에 저장된 데이터와 데이터의 해석을 [그림 32]에서 확인할 수 있다.



[그림 32] 이메일 데이터베이스에 저장되는 데이터 및 데이터 해석

결과적으로, 메일을 수신한 시각과 수신한 메일이 동기화된 시각은 동일하지만, 메일을 발신한 시각과 발신한 메일이 동기화된 시각은 다르며 동기화된 시각이 더 늦은 시각으로 기록된다. 이 경우 동일한 메일을 수신한 이후에 발신한 것으로 보이게 된다.

따라서 태블릿 PC에서 발신 및 수신한 동일 메일에 대하여 시간 역전현상이 발견된 항목은 검찰이 사용한 FINALMobile Forensics5 도구에서 이메일 앱 분석할 때 메일의 수신 및 발신 시각을 태블릿 PC에 동기화된 시각(syncServerTimeStamp)을 사용한 것으로 추측되며, 쟁점 태블릿PC의 데이터를 확인하여야 정확히 판단할 수 있다.

※ 해설서 이력관리 ※

버 전	작성일	내 용
1.0	2017.11.02.	초안
1.1	2017.11.22.	항목 11 추가, 항목 3 내용 보완
1.2	2017.11.29.	항목 12, 13, 14 추가
1.3	2017.12.02.	항목 13, 14 내용 보완
1.4	2017.12.13.	항목 12 내용 보완