

## [별첨2] 이 사건 태블릿PC의 무결성 훼손 현황

### 사례①

노승권 서울중앙지검 1차장과 JTBC 기자가 주고받은 문자메시지 캡처.

이 사건 태블릿을 2016. 10. 24. 오후 7시 20분경 넘겨받은 노승권 차장은 JTBC 기자와 문자를 주고받으며, 태블릿을 임의로 접속·구동하여 태블릿에 저장된 연설문, 일정 등을 열람하고 있음.



### 사례②

국과수가 2017. 11. 15. 태블릿을 재차 감정하면서 포착한 무결성 훼손 현황들. 태블릿이 검찰에 임의제출된 2016. 10. 24. 저녁부터, 포렌식을 하기 직전인 10. 25. 17시 14분까지, 태블릿이 계속 켜진 채 무단으로 구동된 기록임.

- 2016. 10. 25. 오전 11시 20분경과 오후 5시 10분경(포렌식 실시 5분 전), 태블릿의 앱이 구동된 기록들

검찰이 입수한 다음날인  
2016. 10. 25. 낮 시간대  
지속적인 태블릿 사용 흔적

번호	상태	패키지명	시작시간	종료시간
53	정상	com.android.vending	2016-10-22 AM 10:24:04	2016-10-25 AM 11:21:04
57	정상	com.sec.android.app.screencapture	2016-10-22 PM 02:30:33	2016-10-25 AM 11:21:04
58	삭제	com.android.calendar	2016-10-22 PM 08:25:45	2016-10-24 PM 04:22:56
59	삭제	com.sec.android.app.samsungapps.una2	2016-10-22 PM 11:55:54	2016-10-22 PM 11:56:45
60	정상	com.android.contacts	2016-10-23 PM 06:37:32	2016-10-25 AM 11:21:04
61	삭제	com.skt.skaf.l001mtm091	2016-10-24 AM 04:23:49	2016-10-24 PM 04:22:56
62	삭제	com.sec.android.app.videoplayer	2016-10-24 PM 03:16:30	2016-10-24 PM 04:22:56
63	삭제	com.kakao.talk	2016-10-24 PM 04:13:15	2016-10-24 PM 04:22:56
64	삭제	com.google.android.gms	2016-10-24 PM 04:22:49	2016-10-24 PM 04:22:57
65	삭제	com.sec.minimode.taskcloser	2016-10-24 PM 04:22:50	2016-10-24 PM 04:22:56
66	정상	com.sec.minimode.music	2016-10-24 PM 04:28:09	2016-10-25 AM 11:21:04
67	정상	com.sec.android.app.music	2016-10-24 PM 04:28:13	2016-10-25 AM 11:21:04
68	정상	com.android.calendar	2016-10-24 PM 07:19:26	2016-10-25 AM 11:21:04
69	정상	com.sec.android.app.samsungapps.una2	2016-10-25 AM 09:36:21	2016-10-25 AM 09:39:27
70	정상	com.google.android.apps.maps	2016-10-25 AM 10:33:16	2016-10-25 AM 11:21:04
71	정상	com.android.MtpApplication	2016-10-25 AM 11:00:55	2016-10-25 AM 11:21:04
72	정상	com.sec.android.app.videoplayer	2016-10-25 PM 04:13:19	2016-10-25 PM 05:11:51
73	정상	com.kakao.talk	2016-10-25 PM 05:10:41	2016-10-25 PM 05:11:50

2016. 10. 25. 오후 5시 14분  
포렌식 실시 5분 전까지도  
태블릿PC 사용

- 2016. 10. 25. 오전 시간대와 오후 5시경(포렌식 실시 10분 전), 연락처와 이메일, 카카오톡 등과 관련된 태블릿의 내부 파일이 변경되거나 구동된 기록들

번호	상태	파일명	유형	만든 날짜	수정된 날짜	액세스한 날짜
523	정상	traces.txt	TXT	2013-09-19 PM 11:03:20	2016-10-25 AM 12:09:57	2013-09-19 PM 11:03:20
- 파일 경로 : /Media/anr - 크기 : 128.1KB (131,194 Bytes) - 시작Offset : 0x00000000 - 해시값 (SHA1) : EBEBBECAD6653E68E1876C481DEA67DE85D49E68 (traces.txt)						
524	정상	CheckinService_00001.xml	XML	2016-10-25 AM 09:39:27	2016-10-25 AM 09:39:27	2016-10-25 AM 09:39:27
- 파일 경로 : /Media/data/com.google.android.gsf/shared_prefs - 크기 : 1.8KB (1,878 Bytes) - 시작Offset : 0x00000000 - 해시값 (SHA1) : 6EEC177FC5FCBE9D58E3828D8A45CFC84E7BF27D (CheckinService_00001.xml)						
525	정상	packages-more-backup.xml	XML	2016-10-25 AM 11:23:18	2016-10-25 AM 11:23:18	2016-10-25 AM 11:23:18
- 파일 경로 : /Media/system - 크기 : 161.7KB (165,625 Bytes) - 시작Offset : 0x00000000 - 해시값 (SHA1) : 54E8C0B5724070A94BB6C6749EE32333A6113750 (packages-more-backup.xml)						
526	정상	com.android.contacts_preferences.xml	XML	2016-10-25 PM 02:30:02	2016-10-25 PM 02:30:02	2016-10-25 PM 02:30:02
- 파일 경로 : /Media/data/com.android.contacts/shared_prefs - 크기 : 1.4KB (1,389 Bytes) - 시작Offset : 0x00000000 - 해시값 (SHA1) : 91148EEAB68FE67F1F48AD02562AF649579DD4D2 (com.android.contacts_preferences.xml)						
527	정상	appwidgets.xml	XML	2016-10-25 PM 02:33:45	2016-10-25 PM 02:33:45	2016-10-25 PM 02:33:45
- 파일 경로 : /Media/system - 크기 : 674 Bytes (674 Bytes) - 시작Offset : 0x00000000 - 해시값 (SHA1) : 429866B271F9F7BB36D58CE56394E04DD1A7B0F5 (appwidgets.xml)						
528	정상	P1SharedPreferences.xml	XML	2016-10-25 PM 04:13:24	2016-10-25 PM 04:13:24	2016-10-25 PM 04:13:24
- 파일 경로 : /Media/data/com.sec.android.app.videoplayer/shared_prefs - 크기 : 400 Bytes (400 Bytes) - 시작Offset : 0x00000000 - 해시값 (SHA1) : 92C6629D58B8BCDF21915E68AB9FCCBF02F8D57D (P1SharedPreferences.xml)						
529	정상	AndroidMail.Main.xml	XML	2016-10-25 PM 05:02:15	2016-10-25 PM 05:02:15	2016-10-25 PM 05:02:15
- 파일 경로 : /Media/data/com.android.email/shared_prefs - 크기 : 5.2KB (5,305 Bytes) - 시작Offset : 0x00000000 - 해시값 (SHA1) : DBB6B0B2632A4159DBBA0D7EF4D439770263FC2B (AndroidMail.Main.xml)						
530	정상	KakaoTalk.preferences.xml	XML	2016-10-25 PM 05:02:28	2016-10-25 PM 05:02:28	2016-10-25 PM 05:02:28
- 파일 경로 : /Media/data/com.kakao.talk/shared_prefs - 크기 : 2.6KB (2,625 Bytes) - 시작Offset : 0x00000000 - 해시값 (SHA1) : 9CB22545791A7D57527AF3E4512343B924D11A78 (KakaoTalk.preferences.xml)						

포렌식 실시 10분 전까지도  
태블릿PC 사용

### 사례③

2016. 10. 24. 저녁 7시 30분부터, 다음날인 2016. 10. 25. 포렌식 실시 30분 전까지, 검사가 한글뷰어 앱으로 태블릿의 문서파일 30여 건을 열람한 기록들

번호	상태	파일명	날짜
45	정상	/mnt/sdcard/Download/전국 축산인 한마음 전진대회 축사-2.hwp	2016-10-24 PM 07:32:55
46	정상	/mnt/sdcard/Android/data/com.android.email/cache/11.30-12.1.hwp	2016-10-24 PM 07:47:15
47	정상	/mnt/sdcard/Android/data/com.android.email/cache/5.18 33주년 기념사.hwp	2016-10-24 PM 07:58:38
48	정상	/mnt/sdcard/Download/_-1.hwp	2016-10-24 PM 08:05:12
49	정상	/mnt/sdcard/Android/data/com.android.email/cache/식사,티타임 대상자.hwp	2016-10-25 AM 08:58:30
50	정상	/mnt/sdcard/Android/data/com.android.email/cache/호주총리 통화 참고자료.hwp	2016-10-25 AM 11:04:44
51	정상	/mnt/sdcard/Android/data/com.android.email/cache/육명수여사 제38주기 추도식 인사말씀.hwp	2016-10-25 AM 11:07:05
52	정상	/mnt/sdcard/Android/data/com.android.email/cache/아베 신조 총리 특사단 접견자료.hwp	2016-10-25 AM 11:20:24
53	정상	/mnt/sdcard/Android/data/com.android.email/cache/다보스포럼.hwp	2016-10-25 AM 11:20:34

검찰이 입수한 이후  
2016 10 24 저녁 7시 30분  
~ 10 25 낮 시간대

지속적인  
태블릿PC사용 흔적

54	정상	/mnt/sdcard/Android/data/com.android.email/cache/한국시민단체협의회 축사.hwp	2016-10-25 AM 11:20:52
55	정상	/mnt/sdcard/Android/data/com.android.email/cache/청와대회동(1228).hwp	2016-10-25 AM 11:24:52
56	정상	/mnt/sdcard/Android/data/com.android.email/cache/11.29.hwp	2016-10-25 PM 01:15:30
57	정상	/mnt/sdcard/Android/data/com.android.email/cache/121228청와대회동_수정.hwp	2016-10-25 PM 01:15:56
58	정상	/mnt/sdcard/Android/data/com.android.email/cache/130109MB특별사면.hwp	2016-10-25 PM 01:16:19
59	정상	/mnt/sdcard/Android/data/com.android.email/cache/130128고용복지_업무보고_참고자료.hwp	2016-10-25 PM 01:16:34
60	정상	/mnt/sdcard/Android/data/com.android.email/cache/16일차 서울 삼성역코엑스 유세.hwp	2016-10-25 PM 01:17:09
61	정상	/mnt/sdcard/Android/data/com.android.email/cache/나는.hwp	2016-10-25 PM 01:17:34

검찰이 입수한 이후  
10 25 낮 시간대

지속적인  
태블릿PC사용 흔적

62	정상	/mnt/sdcard/Android/data/com.android.email/cache/강원도업무보고.hwp	2016-10-25 PM 04:02:33
63	정상	/mnt/sdcard/Android/data/com.android.email/cache/국무회의 말씀자료.hwp	2016-10-25 PM 04:02:45
64	정상	/mnt/sdcard/Android/data/com.android.email/cache/다보스포럼 특사 파견.hwp	2016-10-25 PM 04:03:05
65	정상	/mnt/sdcard/Android/data/com.android.email/cache/당선소감.hwp	2016-10-25 PM 04:03:12
66	정상	/mnt/sdcard/Android/data/com.android.email/cache/대통령당선인 대변인 선임관련.hwp	2016-10-25 PM 04:04:12
67	정상	/mnt/sdcard/Android/data/com.android.email/cache/양승태 대법원장 면담 말씀자료.hwp	2016-10-25 PM 04:05:22
68	정상	/mnt/sdcard/Android/data/com.android.email/cache/역대경호처 장현형.hwp	2016-10-25 PM 04:05:32
69	정상	/mnt/sdcard/Android/data/com.android.email/cache/인사.hwp	2016-10-25 PM 04:05:46
70	정상	/mnt/sdcard/Android/data/com.android.email/cache/자료.hwp	2016-10-25 PM 04:05:59
71	정상	/mnt/sdcard/Android/data/com.android.email/cache/정부조직개편안 관련 평가.hwp	2016-10-25 PM 04:06:17
72	정상	/mnt/sdcard/Android/data/com.android.email/cache/제32회 국도회의 말씀자료.hwp	2016-10-25 PM 04:07:19
73	정상	/mnt/sdcard/Android/data/com.android.email/cache/중국 특사단 추천 의원.hwp	2016-10-25 PM 04:08:45
74	정상	/mnt/sdcard/Android/data/com.android.email/cache/11일차서울유세문.hwp	2016-10-25 PM 04:40:37
75	정상	/mnt/sdcard/Download/_-5.hwp	2016-10-25 PM 04:41:19

10.25. 오후 5시 14분  
포렌식 실시  
30분 ~ 1시간 전까지  
태블릿PC 사용

#### 사례④

국과수는 이 사건 태블릿의 무결성에 대해 “태블릿 전체에 대한 무결성이 유지되지 않음”이라고 판정함(국과수 디지털분석감정서 p36).

1) 2016.10.18.자 이후 태블릿PC의 무결성 여부에 대한 질의로 판단되며, 이를 위해 태블릿PC 사본화 파일을 파일시스템 기반으로 분석한 결과, 표 14와 같이 2016.10.18.자부터 2016.10.31.자까지 생성, 수정된 파일들이 다수 발견되어 2016.10.18.자 이후 태블릿PC의 전체에 대한 무결성이 유지되지 않음,

사례⑤

검찰이 2016. 10. 25. 태블릿을 사본화할 때의 해시값과, 재봉인을 한 뒤 1년이 지난 2017. 11. 15. 국과수가 사본화할 때의 해시값 비교

**파티션 27을 제외하고, 파티션 24, 25, 26, 28 해시값이 전부 바뀜**

**검찰 포렌식 해시값 2016. 10. 25.**

(MD5 해시값)

238DF6E2E13A39DAE6111E4E90073D2E

76A8677B38DFE585A9177F461EEFA7E3

68D7FE1D9D581341A0DFDA98716AF4D6

A4AA0AF1EFED423536ACE5AF853339F3

5D8883725394C1C199520B00858F9089

**국과수 포렌식 해시값 2017. 11. 13.**

파티션24	
사본화파일명	2017-M-31653-20171115_SHV-E140S_mmcb1k0p24.bin
용량(Bytes)	1,155,530,752
해시값(MD5)	9CEF3AB5F25F2E0B5A14D61190F21328
파티션25	
사본화파일명	2017-M-31653-20171115_SHV-E140S_mmcb1k0p25.bin
용량(Bytes)	439,353,344
해시값(MD5)	21B360276B2CD2FCAF56DF1745B37B77
파티션26	
사본화파일명	2017-M-31653-20171115_SHV-E140S_mmcb1k0p26.bin
용량(Bytes)	135,266,304
해시값(MD5)	86D9D044F70546391DFA8F0A70789540
파티션27	
사본화파일명	2017-M-31653-20171115_SHV-E140S_mmcb1k0p27.bin
용량(Bytes)	904,921,088
해시값(MD5)	A4AA0AF1EFED423536ACE5AF853339F3
파티션28	
사본화파일명	2017-M-31653-20171115_SHV-E140S_mmcb1k0p28.bin
용량(Bytes)	28,935,454,720
해시값(MD5)	1E63EABDD844CBFE38070F45B421BA53

[출처] 검찰 포렌식 보고서(증거번호 135번)p5

[출처] 국과수 감정서(증거번호 133번)p7-8

## 사례⑥

검찰이 2016. 10. 25. 포렌식을 종료하고 6일 뒤인 2016. 10. 31. 오후 2시 47분경 재봉인된 태블릿을 다시 꺼내 무단으로 구동한 기록들

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 14:4	2016-10-31 14:47
inode_00620200	Deleted	파일	/deleted.files/inode_00620200	3145768	2011-01-01 9:01	2011-01-01 9:0	2016-10-31 14:47	2016-10-31 14:4	2016-10-31 14:47
inode_00620200	Deleted	파일	/deleted.files/inode_00620200	3145768	2011-01-01 9:01	2011-01-01 9:0	2016-10-31 14:47	2016-10-31 14:4	2016-10-31 14:47
/	Active	폴더	/	4096	1970-01-01 9:00	1970-01-01 9:0	2016-10-31 14:47	2016-10-31 14:4	2016-10-31 14:47
.pcsync_stream	Active	기타	/pcsync_stream	0	2016-10-31 14:47	2016-10-31 14:4	2016-10-31 14:47	2016-10-31 14:4	2016-10-31 14:47
persist.radio.adb_log_on	Active	파일	/property/persist.radio.adb_log_on	1	2016-10-31 14:47	2016-10-31 14:4	2016-10-31 14:47	2016-10-31 14:4	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 14:4	2016-10-31 14:47	2016-10-31 14:4	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 14:4	2016-10-31 14:47	2016-10-31 14:4	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 14:4	2016-10-31 14:47	2016-10-31 14:4	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 14:4	2016-10-31 14:47	2016-10-31 14:4	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 14:4	2016-10-31 14:47	2016-10-31 14:4	2016-10-31 14:47
inode_0062C700	Deleted	파일	/deleted.files/inode_0062C700	32768	2016-10-25 11:22	2016-10-25 11:2	2016-10-31 14:47	2016-10-25 11:2	2016-10-31 14:47
efs1.bin	Active	파일	/qcks/efs1.bin	3145768	2011-01-01 9:01	2011-01-01 9:0	2016-10-31 14:47	2011-01-01 9:0	2016-10-31 14:47
efs2.bin	Active	파일	/qcks/efs2.bin	3145768	2011-01-01 9:01	2011-01-01 9:0	2016-10-31 14:47	2011-01-01 9:0	2016-10-31 14:47
temp.dump	Active	파일	/qcks/temp.dump	3145728	2011-01-01 9:01	2011-01-01 9:0	2016-10-31 14:47	2011-01-01 9:0	2016-10-31 14:47
efs3.bin	Active	파일	/qcks/efs3.bin	3145768	2011-01-01 9:01	2011-01-01 9:0	2016-10-31 14:47	2011-01-01 9:0	2016-10-31 14:47
entropy.dat	Active	파일	/system/entropy.dat	4096	2011-01-01 9:01	2011-01-01 9:0	2016-10-31 14:47	2011-01-01 9:0	2016-10-31 14:47
inode_008C6F00	Deleted	파일	/deleted.files/inode_008C6F00	102128	2016-10-31 14:47	2016-10-31 14:4	2016-10-31 14:47	2016-10-31 14:4	2016-10-31 14:47
stats.bin.bak	Deleted	파일	/deleted.files/stats.bin.bak	900	2016-10-31 14:47	2016-10-31 14:4	2016-10-31 14:47	2016-10-31 14:4	2016-10-31 14:47
status.bin.bak	Deleted	파일	/deleted.files/status.bin.bak	1432	2016-10-31 14:47	2016-10-31 14:4	2016-10-31 14:47	2016-10-31 14:4	2016-10-31 14:47
packages.xml	Active	파일	/system/packages.xml	165625	2016-10-31 14:47	2016-10-31 14:4	2016-10-31 14:47	2016-10-31 14:4	2016-10-31 14:47
packages.list	Active	파일	/system/packages.list	10759	2016-10-31 14:47	2016-10-31 14:4	2016-10-31 14:47	2016-10-31 14:4	2016-10-31 14:47
packages-stopped.xml	Active	파일	/system/packages-stopped.xml	226	2016-10-31 14:47	2016-10-31 14:4	2016-10-31 14:47	2016-10-31 14:4	2016-10-31 14:47
accounts.xml	Active	파일	/system/sync/accounts.xml	3513	2016-10-31 14:47	2016-10-31 14:4	2016-10-31 14:47	2016-10-31 14:4	2016-10-31 14:47
databases	Active	폴더	/data/com.android.providers.settings/databases	4096	2011-01-01 9:02	2011-01-01 9:0	2016-10-31 14:47	2011-01-01 9:0	2016-10-31 14:47
settings.db	Active	파일	/data/com.android.providers.settings/databases/1	57344	2011-01-01 9:02	2011-01-01 9:0	2016-10-31 14:47	2011-01-01 9:0	2016-10-31 14:47
settings.db-wal	Active	파일	/data/com.android.providers.settings/databases/1	0	2016-10-31 14:47	2016-10-31 14:4	2016-10-31 14:47	2016-10-31 14:4	2016-10-31 14:47
settings.db-shm	Active	파일	/data/com.android.providers.settings/databases/1	32768	2016-10-31 14:47	2016-10-31 14:4	2016-10-31 14:47	2016-10-31 14:4	2016-10-31 14:47
property	Active	폴더	/property	4096	2011-01-01 9:00	2011-01-01 9:0	2016-10-31 14:47	2011-01-01 9:0	2016-10-31 14:47
backup	Active	폴더	/backup	4096	2011-01-01 9:02	2011-01-01 9:0	2016-10-31 14:47	2011-01-01 9:0	2016-10-31 14:47
pending	Active	폴더	/backup/pending	4096	2011-01-01 9:02	2011-01-01 9:0	2016-10-31 14:47	2011-01-01 9:0	2016-10-31 14:47
processed	Active	파일	/backup/processed	204	2016-10-31 14:47	2016-10-31 14:4	2016-10-31 14:47	2016-10-31 14:4	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 14:4	2016-10-31 14:47	2016-10-31 14:4	2016-10-31 14:47

①

① / = root 폴더

2016. 10. 31. 14:47 루트 폴더 권한 획득

② 2016. 10. 31. 14:47 계정 정보 등 대거 수정

.pcsync\_stream

root 폴더에 접근, PC를 통한 동기화 작업 수행

②

이름	상태	종류	경로	크기	생성 일시	업데이트 일시	수정 일시
journal-1995247881.tmp	Active	파일	/backup/pending/journal-1995247881.tmp	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_0078BC00	Deleted	파일	/deleted.files/inode_0078BC00	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	폴더	/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/	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/	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_fref.xml.bak	Deleted	파일	/deleted.files/MT_shared_fref.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 14:47
mmsms.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
nvmac.info	Active	파일	/nvmac.info	17	2011-01-01 9:00	2011-01-01 9:00	2016-10-31 14:47
inode_00767E00	Deleted	파일	/deleted.files/inode_00767E00	21032	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:47
inode_0075FE00	Deleted	파일	/deleted.files/inode_0075FE00	21032	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:47
inode_00755E00	Deleted	파일	/deleted.files/inode_00755E00	21032	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:47
inode_0074AE00	Deleted	파일	/deleted.files/inode_0074AE00	21032	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:47
inode_00742E00	Deleted	파일	/deleted.files/inode_00742E00	21032	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:47
inode_00738E00	Deleted	파일	/deleted.files/inode_00738E00	21032	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:47
inode_0072EE00	Deleted	파일	/deleted.files/inode_0072EE00	21032	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:47
pending.bin	Active	파일	/system/sync/pending.bin	492	2016-10-31 14:47	2016-10-31 14:47	2016-10-31 14:47
databases	Active	폴더	/data/com.android.providers.contacts/databases	4096	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:47
mac.info	Active	파일	/mac.info	18	2012-07-07 11:37	2012-07-07 11:37	2016-10-31 14:47
wpa_supplicant.conf	Active	파일	/misc/wifi/wpa_supplicant.conf	423	2012-07-13 19:18	2012-07-13 19:18	2016-10-31 14:47
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	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/EmailProvide	32768	2011-01-01 9:02	2011-01-01 9:02	2016-10-31 14:48

## 위치정보 기록, 연락처 DB, MAC 정보, 이메일 기록 등 변경

이름	상태	종류	경로	크기	생성 일시	업데이트 일시	수정 일시
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/EmailProvide	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	98304	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_008E0B00	Deleted	파일	/deleted.files/inode_008E0B00	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/databases	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@14778928857D8	Active	파일	/system/dropbox/SYSTEM_BOOT@14778928857D8	254	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48
RR_NPON.p	Active	파일	/log/RR_NPON.p	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.readershub/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.readershub/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
mmsms.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_00861E00	Deleted	파일	/deleted.files/inode_00861E00	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.db	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

## 다운로드 기록, 미디어 기록, 문자메시지 기록, 시스템 dropbox 수정

이름	상태	종류	경로	크기	생성 일시	업데이트 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
rlz_data.db	Active	파일	/data/com.google.android.partnersetup/databases	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_prefs	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/Event	242	2016-10-31 14:48	2016-10-31 14:48	2016-10-31 14:48
RLZ.xml	Active	파일	/data/com.google.android.partnersetup/shared_prefs	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_prefs	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_008A2800	Deleted	파일	/deleted.files/inode_008A2800	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.ziv9876@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.ziv9876@gmail.com.db	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.ziv9876@gmail.com.db	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.gm/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.gm/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_00888100	Deleted	파일	/deleted.files/inode_00888100	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_prefs.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/ex	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_00911800	Deleted	파일	/deleted.files/inode_00911800	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 02:23	2012-06-24 02:23	2016-10-31 14:48
inode_0093E100	Deleted	파일	/deleted.files/inode_0093E100	1090	2012-06-24 02:23	2012-06-24 02:23	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

## 구글 프레임워크, 이벤트 기록, 메일 DB, 외부장치 기록, 동기화 기록 등 변경

이름	상태	종류	경로	크기	생성 일시	업데이트 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 9:00	2011-01-01 9:00	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
usagelogs	Active	폴더	/system/usagelogs	4096	2011-01-01 9:01	2011-01-01 9:01	2016-10-31 14:48
dmappmgr.db	Active	파일	/system/dmappmgr.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.socialhub/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/usagelogs/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-mj04EE78F0	Deleted	파일	/deleted.files/talk.db-mj04EE78F0	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-mj3E643B73	Deleted	파일	/deleted.files/talk.db-mj3E643B73	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-mj35127FB4	Deleted	파일	/deleted.files/talk.db-mj35127FB4	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-mj6AF4A83E	Deleted	파일	/deleted.files/talk.db-mj6AF4A83E	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	81929	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 02:23	2012-06-24 02:23	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

## 안드로이드 시스템, 구글 프레임워크 등 수정된 흔적

번호	상태	패키지명	시작시간	종료시간
74	정상	com.android.systemui	2016-10-31 PM 02:47:54	2016-10-31 PM 02:48:26
75	정상	com.google.android.location	2016-10-31 PM 02:47:57	2016-10-31 PM 02:48:26
76	정상	com.smlm	2016-10-31 PM 02:48:00	2016-10-31 PM 02:48:26
77	정상	com.sec.phone	2016-10-31 PM 02:48:05	2016-10-31 PM 02:48:26
78	정상	com.sec.android.app.factorytest	2016-10-31 PM 02:48:05	2016-10-31 PM 02:48:26
79	정상	com.qualcomm.wiper	2016-10-31 PM 02:48:05	2016-10-31 PM 02:48:26
80	정상	com.wssyncmldm	2016-10-31 PM 02:48:05	2016-10-31 PM 02:48:26
81	정상	com.smls	2016-10-31 PM 02:48:05	2016-10-31 PM 02:48:26
82	정상	com.sec.android.app.sns	2016-10-31 PM 02:48:06	2016-10-31 PM 02:48:26
83	정상	com.sec.android.socialhub	2016-10-31 PM 02:48:06	2016-10-31 PM 02:48:26
84	정상	com.sec.android.fotaclient.components	2016-10-31 PM 02:48:06	2016-10-31 PM 02:48:26
88	정상	com.osp.app.signin	2016-10-31 PM 02:48:07	2016-10-31 PM 02:48:26
89	정상	com.google.android.gsf	2016-10-31 PM 02:48:10	2016-10-31 PM 02:48:26
90	정상	com.google.android.partnersetup	2016-10-31 PM 02:48:11	2016-10-31 PM 02:48:26
91	정상	com.google.android.syncadapters.contacts	2016-10-31 PM 02:48:11	2016-10-31 PM 02:48:26
92	정상	com.android.ahnmobilesecurity	2016-10-31 PM 02:48:12	2016-10-31 PM 02:48:26
93	정상	com.android.exchange	2016-10-31 PM 02:48:13	2016-10-31 PM 02:48:26
94	정상	com.android.email	2016-10-31 PM 02:48:13	2016-10-31 PM 02:48:26
95	정상	com.skt.skaf.Z0000SLOAD	2016-10-31 PM 02:48:14	2016-10-31 PM 02:48:26
96	정상	com.nhn.android.search	2016-10-31 PM 02:48:14	2016-10-31 PM 02:48:26
97	정상	com.android.providers.media	2016-10-31 PM 02:48:15	2016-10-31 PM 02:48:26
98	정상	com.android.providers.downloads	2016-10-31 PM 02:48:15	2016-10-31 PM 02:48:26
99	정상	com.sec.android.widgetapp.weathernewslock	2016-10-31 PM 02:48:15	2016-10-31 PM 02:48:26
100	정상	com.android.mms	2016-10-31 PM 02:48:17	2016-10-31 PM 02:48:26
101	정상	com.sec.readershub	2016-10-31 PM 02:48:18	2016-10-31 PM 02:48:26
102	정상	com.android.providers.calendar	2016-10-31 PM 02:48:19	2016-10-31 PM 02:48:26
103	정상	com.sec.android.widgetapp.digitalclock	2016-10-31 PM 02:48:19	2016-10-31 PM 02:48:26
104	정상	com.google.android.gms	2016-10-31 PM 02:48:19	2016-10-31 PM 02:48:26
105	정상	com.google.android.gm	2016-10-31 PM 02:48:20	2016-10-31 PM 02:48:26
106	정상	com.sec.minimode.taskcloser	2016-10-31 PM 02:48:26	2016-10-31 PM 02:48:26
107	정상	com.sec.app.RilErrorNotifier	2016-10-31 PM 02:48:26	2016-10-31 PM 02:48:26

포렌식 종료 6일 뒤  
2016. 10. 31. 오후 2시 이후  
태블릿PC 앱 사용 흔적