BoB 6기

디지털 포렌식

2017.08.8

정경주

동영상_사진 위변조 분석 보고서

1. 파일 원본, 파일 위변조

원본

20170818_142413.mp4 (147,886,921 bytes)

M5: 30eb8de42d3644d9577d4c92a282c217

SHA256: e601fe79a0ec87229f594cdc890325006bb0d920b90b6e4d04e9861e4b937a5c

20170808_193501.jpg (808,748 bytes)

M5: fbe9d4b25f2259744e17c7a71a731469

SHA256: e325db0245427f9a6f629767ae813efb34f031c02bbe9ab74ab0c3cd6edd1a90

위변조

20170818_142413_2E2770384.mp4 (37,255,813 bytes)

M5: 9286272af21323c8acd9663e3f719b08

SHA256: 12d03bd83d5257b1fe4888dd12c6e7d34d84977e8fca84addce035c3657af9b1

20170808_193501~2.jpg (808,748 bytes)

M5: 5a74bfa3a6e6e232946ad8a156457ab5

SHA256: 1c17d4c0ea85d4d580c25c5edf6a0d6370891da9e4fc3723911425335de98f74

2. 원본 파일들의 촬영 기기 명시

20170818_142413.mp4

LG-F600K

20170808_193501.jpg

LG-F600K

```
Filename: [D:\My room\Steve's work\BOB\과제\포렌식\심규선 멘토님\20170808_193501.jpg]
Filesize: [3999974] Bytes

;art Offset: 0x00000000
'* Marker: SOI (xFFD8) ***
OFFSET: 0x00000000

'* Marker: APP1 (xFFE1) ***
OFFSET: 0x00000002
Length          = 16102
Identifier      = [Exif]
Identifier TIFF = 0x[4D4D002A 00000008]
Endian          = Motorola (big)
TAG Mark x002A  = 0x002A

EXIF IFD0 @ Absolute 0x00000014
  Dir Length = 0x000A
  [DateTime                          ] = "2017:08:08 19:35:01"
  [GPSOffset                         ] = @ 0x0C9C
  [Model                             ] = "LG-F600K"
```

3. 조작 또는 편집 방법

Dae_mmf라는 도구는 동영상에 사용하였고 JPEGSnoop라는 도구는 사진에 사용하였다. 동영상 위변조는 핸드폰으로 PowerDirector라는 어플을 사용하여 화질만 다운그레이드 시켰다. 사진은 핸드폰 내장되어 있는 필터를 이용해서 위변조를 하였다.

*카카오톡으로 전송되면 여러모로 바뀌는 것이 많아 핸드폰을 컴퓨터와 연결하여 사진을 모두 직접 가져왔다.

4. 분석 내용(동일하게 확인되는 내용 + 위변조라고 판단되는 내용)

사진부터 분석하겠습니다.

사진은 일단 제일 먼저 비교가 가능한게 필터를 조금 사용하였기 때문에 어떤게 진짜인지 모릅니다.

20170808_193501.jpg

```
EXIF IFD0 @ Absolute 0x00000014
  Dir Length = 0x000A
  [DateTime                          ] = "2017:08:08 19:35:01"
  [GPSOffset                         ] = @ 0x0C9C
  [Model                             ] = "LG-F600K"
  [YCbCrPositioning                  ] = Centered
  [ResolutionUnit                    ] = Inch
  [YResolution                       ] = 72/1
  [Orientation                       ] = 1 = Row 0: top, Col 0: left
  [ExifOffset                        ] = @ 0x00C2
  [XResolution                       ] = 72/1
  [Make                              ] = "LG Electronics"
  Offset to Next IFD = 0x00000D65
```

20170808_193501~2.jpg

```
EXIF IFD0 @ Absolute 0x00000014
  Dir Length = 0x000B
  [DateTime                          ] = "2017:08:18 22:43:12"
  [GPSOffset                         ] = @ 0x0CA8
  [Model                             ] = "LG-F600K"
  [ResolutionUnit                    ] = Inch
  [YCbCrPositioning                  ] = Centered
  [YResolution                       ] = 72/1
  [ExifOffset                        ] = @ 0x00CE
  [XResolution                       ] = 72/1
  [Make                              ] = "LG Electronics"
  Offset to Next IFD = 0x00000D71
```

위 사진들을 봤을 때 모델명, 화질 단위, 제조 회사 등 똑 같은 사실을 확인할 수 있었지만 만들어진 날짜가 일단 다른걸 보아 늦은 시간이 찍힌 것이 위변조 됐다는 사실을 확인할 수 있습니다.

20170808_193501.jpg

```
*** Marker: DQT (xFFDB) ***
  Define a Quantization Table.
  OFFSET: 0x00003F10
  Table length = 132
  ----
  Precision=8 bits
  Destination ID=0 (Luminance)
    DQT, Row #0:   1   1   1   1   1   2   3   4
    DQT, Row #1:   1   1   1   1   2   3   4   3
    DQT, Row #2:   1   1   1   1   2   3   4   3
    DQT, Row #3:   1   1   1   2   3   5   5   4
    DQT, Row #4:   1   1   2   3   4   7   6   5
    DQT, Row #5:   1   2   3   4   5   6   7   6
    DQT, Row #6:   3   4   5   5   6   7   7   6
    DQT, Row #7:   4   6   6   6   7   6   6   6
    Approx quality factor = 96.95 (scaling=6.11 variance=1.09)
  ----
```

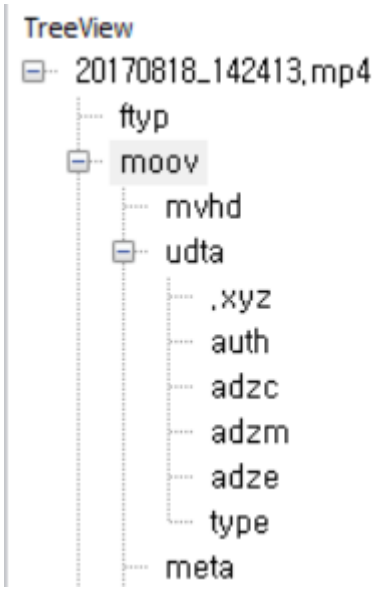
20170808_193501~2.jpg

```
*** Marker: DQT (xFFDB) ***
  Define a Quantization Table.
  OFFSET: 0x00000DD5
  Table length = 67
  ----
  Precision=8 bits
  Destination ID=0 (Luminance)
    DQT, Row #0:   3   2   2   3   5   8  10  12
    DQT, Row #1:   2   2   3   4   5  12  12  11
    DQT, Row #2:   3   3   3   5   8  11  14  11
    DQT, Row #3:   3   3   4   6  10  17  16  12
    DQT, Row #4:   4   4   7  11  14  22  21  15
    DQT, Row #5:   5   7  11  13  16  21  23  18
    DQT, Row #6:  10  13  16  17  21  24  24  20
    DQT, Row #7:  14  18  19  20  22  20  21  20
    Approx quality factor = 90.06 (scaling=19.88 variance=1.14)
```

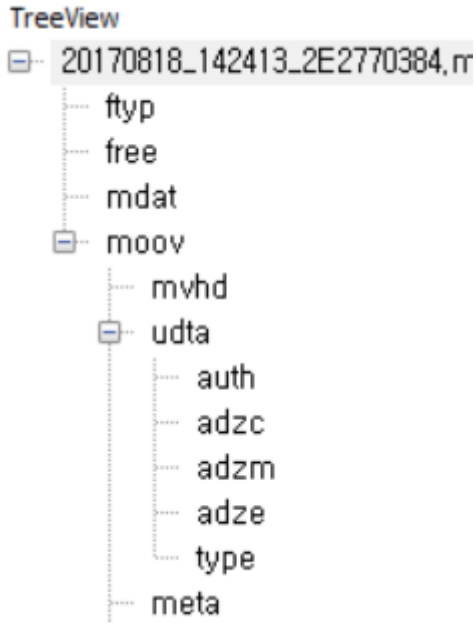
여기에서도 숫자가 다른점을 보아 위변조가 됐다는 점을 확인할 수 있습니다.

다음은 동영상 변조 분석입니다.

20170818_142413.mp4



20170818_142413_2E2770384.mp4



이처럼 트리구조로 보기만 해도 다르다는 것을 확인할 수 있습니다.

20170818_142413.mp4

```
[VIDEO Info]
File Name : D:₩My room₩Steve's work₩BOB₩과제₩포
Video Format : H264 video
Resolution : 3840 * 2160
   Sync Sample Count(I-Frames): 24
   Sample Count(I/P-Frames) : 736
   Total Sample Size(Byte)  : 146,996,266
   Header Size(Byte)        : 0
---------------------------------------
[Audio Info]
   Audio Format     : MPEG-4 audio
   Channel Count    : 2
   Sample Rate      : 48000
   Time Scale       : 48000
   Frame per Sample : 1
```

20170818_142413_2E2770384.mp4

```
[VIDEO Info]
File Name : D:₩My room₩Steve's work₩BOB₩과제₩포렌식₩심
Video Format : H264 video
Resolution : 1920 * 1080
   Sync Sample Count(I-Frames): 24
   Sample Count(I/P-Frames) : 736
   Total Sample Size(Byte)  : 36,842,055
   Header Size(Byte)        : 0
---------------------------------------
[Audio Info]
   Audio Format     : MPEG-4 audio
   Channel Count    : 2
   Sample Rate      : 48000
   Time Scale       : 48000
   Frame per Sample : 1
```

화질이 다르다는 점을 확인할 수 있습니다.

20170818_142413.mp4

```
          00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F ; 0123456789ABCDEF
-------------------------------------------------------- ; ----------------
00062EB0:                       08 CA 64 92 6D 64 61 74 21 ;         ..d.mdat!
00062EC0: 10 05 20 A4 1B FF C0 00 00 00 00 00 00 00 00 00 ; .. ..............
00062ED0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00062EE0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00062EF0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00062F00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00062F10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00062F20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00062F30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00062F40: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00062F50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00062F60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00062F70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00062F80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00062F90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00062FA0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00062FB0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00062FC0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00062FD0: 00 00 00 37 BD 80 00 00 00 00 00 00 00 00 00 00 ; ...7............
00062FE0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00062FF0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00063000: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00063010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00063020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00063030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00063040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00063050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 21 ; ..............p!
00063060: 10 05 20 A4 1B FF C0 00 00 00 00 00 00 00 00 00 ; .. ..............
00063070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00063080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00063090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000630A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000630B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000630C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000630D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000630E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
```

20170818_142413_2E2770384.mp4

```
          00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F ; 0123456789ABCDEF
-------------------------------------------------------- ; ----------------
00000C90:    02 38 40 C0 6D 64 61 74 21 11 45 00 14 50 01 ;  .8@.mdat!.E..P.
00000CA0: 46 FF F1 0A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A ; F...ZZZZZZZZZZZZ
00000CB0: 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A ; ZZZZZZZZZZZZZZZZ
00000CC0: 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A ; ZZZZZZZZZZZZZZZZ
00000CD0: 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A ; ZZZZZZZZZZZZZZZZ
00000CE0: 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A ; ZZZZZZZZZZZZZZZZ
00000CF0: 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A ; ZZZZZZZZZZZZZZZZ
00000D00: 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A ; ZZZZZZZZZZZZZZZZ
00000D10: 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A ; ZZZZZZZZZZZZZZZZ
00000D20: 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A ; ZZZZZZZZZZZZZZZZ
00000D30: 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A ; ZZZZZZZZZZZZZZZZ
00000D40: 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A ; ZZZZZZZZZZZZZZZZ
00000D50: 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A ; ZZZZZZZZZZZZZZZZ
00000D60: 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A ; ZZZZZZZZZZZZZZZZ
00000D70: 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A ; ZZZZZZZZZZZZZZZZ
00000D80: 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A ; ZZZZZZZZZZZZZZZZ
00000D90: 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A ; ZZZZZZZZZZZZZZZZ
00000DA0: 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5D ; ZZZZZZZZZZZZZZZ]
00000DB0: E5 C2 14 B4 B4 B4 B4 B4 B4 B4 B4 B4 B4 B4 B4 B4 ; ................
00000DC0: B4 B4 B4 B4 B4 B4 B4 B4 B4 B4 B4 B4 B4 B4 B4 B4 ; ................
00000DD0: B4 B4 B4 B4 B4 B4 B4 B4 B4 B4 B4 B4 B4 B4 B4 B4 ; ................
00000DE0: B4 B4 B4 B4 B4 B4 B4 B4 B4 B4 B4 B4 BC 21 11 ; ..............!.
00000DF0: 45 00 14 50 01 46 FF F1 0A 5A 5A 5A 5A 5A 5A 5A ; E..P.F...ZZZZZZZ
00000E00: 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A ; ZZZZZZZZZZZZZZZZ
00000E10: 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A ; ZZZZZZZZZZZZZZZZ
00000E20: 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A ; ZZZZZZZZZZZZZZZZ
00000E30: 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A ; ZZZZZZZZZZZZZZZZ
00000E40: 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A ; ZZZZZZZZZZZZZZZZ
00000E50: 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A ; ZZZZZZZZZZZZZZZZ
00000E60: 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A ; ZZZZZZZZZZZZZZZZ
00000E70: 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A ; ZZZZZZZZZZZZZZZZ
00000E80: 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A ; ZZZZZZZZZZZZZZZZ
00000E90: 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A ; ZZZZZZZZZZZZZZZZ
00000EA0: 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A 5A ; ZZZZZZZZZZZZZZZZ
```

mdat값을 보면 원본은 0으로 되어있는데 변조가 된 파일은 다 5A값이 들어가있는 것을 보면 위 변조가 됐음을 또 한번 확인할 수 있습니다.

20170818_142413.mp4

```
Start offset : 32 (0X00000020)
Box Size : 108 (0X0000006C)
Box Type : mvhd (0X6D766864)
---------------------------------------
version  : 0 (0000)
flags    : 0 (00000000)
Creation Time :
   8/18/2017 5:24:39 AM
   3,585,878,679 (0XD5BC2A97)
Modification Time:
   8/18/2017 5:24:39 AM
   3,585,878,679 (0XD5BC2A97)
```

20170818_142413_2E2770384.mp4

```
Start offset : 37,244,249 (0X02384D59)
Box Size : 108 (0X0000006C)
Box Type : mvhd (0X6D766864)
---------------------------------------
version  : 0 (0000)
flags    : 0 (00000000)
Creation Time :
   8/18/2017 5:45:07 AM
   3,585,879,907 (0XD5BC2F63)
Modification Time:
   8/18/2017 5:45:07 AM
   3,585,879,907 (0XD5BC2F63)
```

두 동영상의 생성 시간을 확인해보면 변조 영상이 더 늦게 만들어졌음을 확인할 수 있습니다. 생성시간도 역시 변조를 할 수 있습니다만 여기서는 안했다는 가정하에 하겠습니다. 그러므로 두번째 영상이 더 늦게 만들어진 점을 보아 변조를 확인할 수 있습니다.

멘토님의 강의시간에 강의 들을때는 금방 찾을 수 있을거라 생각을 했는데 생각보다 찾는방법 혹은 분석능력이 제가 모자라서 하기가 힘들었습니다. 제가 핸드폰 어플을 이용하여 화질을 죽였는데 어플 흔적을 남겼을거라 생각했는데 그 부분도 찾지 못하였습니다. 그래도 이렇게 영상에 대해서도 배울 수 있는 기회가 되고 관심이 있었던 분야여서 좋은 경험이었던 것 같습니다.