

401 - Detecting Object Removal

Team Information

Team Name: ISEGYE_IDOL

Team Member: Eungchang Lee, Sojeong Kim, Mingyu Seong, Donghyun HA

Email Address: dfc-isegyeidol@googlegroups.com

Instructions

Description With the development of AI technology, smartphone apps are being released that provide functions that allow you to manipulate photos with just a simple touch of the screen, such as erasing objects, adding objects, changing the background, and adjusting facial expressions. Through this problem, you will analyze photos that have been partially manipulated through the 'object removal' function. You must find the photos that are suspected of being manipulated and provide forensically the basis for your judgment.

Target	Hash (MD5)
PIC.zip	98bcc3458e7a9a67cce32c4453cab3b7

Questions

1. In two of the sample pictures, some objects were removed using the 'Snapseed' app. What are the two pictures? (30 points)
2. In two of the sample pictures, some objects were removed using the 'Photoshop Fix' app. What are the two pictures? (100 points)
3. In two of the sample pictures, some objects were removed using the Samsung Galaxy's 'Object Eraser'. What are the two pictures? (100 points)
4. In addition to the pictures found in questions #1~#3, four pictures

were manipulated. What are the four pictures? (50 points)

5. Find the parts where the objects were removed from the pictures found in questions #1~#4 and provide the rationale for it forensically. (120 points)

Teams must:

- Develop and document the step-by-step approach used to solve this problem to allow another examiner to replicate team actions and results.
- Specify all tools used in deriving the conclusion(s).

Tools used:

Name:	ExifTool	Publisher:	Phil Harvey
Version:	12.45		
URL:	https://exiftool.org/		

Name:	010Editor	Publisher:	sweetscape
Version:	13.0		
URL:	https://www.sweetscape.com/010editor/		

Name:	Forensically	Publisher:	Jonas Wagner
Version:	beta		
URL:	https://29a.ch/photo-forensics		

Step-by-step methodology:

1. In two of the sample pictures, some objects were removed using the 'Snapseed' app. What are the two pictures?

PIC 이미지의 메타데이터를 exiftool 프로그램을 이용하여 확인한 결과, Snapseed APP을 사용하여 이미지 조작한 경우 메타데이터에서 조작 흔적을 발견할 수 있다. 이 흔적은 Software 항목에 [Snapseed 2.0] 값으로 설정되어 있다.

Resolution Unit	:	inches
Software	:	Snapseed 2.0
Modify Date	:	2022:07:26 12:09:59

[그림 1] exiftool 실행 결과

Windows의 문자열 검색 명령어인 findstr로 [Snapseed 2.0]을 검색하여 두 개의 이미지 파일을 도출하였다.

```
C:\#Users\lexd0tpy\Documents\PIC>findstr /M /S "Snapseed" *.*  
|PIC031.jpg  
|PIC060.jpg
```

[그림 2] Snapseed로 조작한 이미지들

따라서 Snapseed로 조작한 이미지는 다음과 같다.

- PIC031.jpg
- PIC060.jpg

2. In two of the sample pictures, some objects were removed using the 'Photoshop Fix' app. What are the two pictures?

Photoshop Fix APP을 직접 설치하여 분석용으로 PIC123.jpg를 임의로 조작하여 원본 파일과 데이터

비교 분석을 진행하였다.



[그림 3] 임의로 조작한 PIC123.jpg

Hex Editor(010editor)를 이용하여 분석한 결과, jpeg quantization table 0 특정 값으로 변경되는 것을 발견하였다.

C:\Users\exd0tpy\Documents\PIC\PIC123.jpg vs. C:\Users\exd0tpy\...\PIC\PIC123_ADJ.jpeg				
Result	Address A	Size A	Address B	Size B
Match	0h	243h	0h	243h
Difference	243h	85h	243h	85h
Match	2C8h	16h	2C8h	16h
Difference	2DEh	7h	2DEh	5h
Match	2E5h	Bh	2E3h	Bh
Difference	2F0h	70h	2EEh	67h
Match	360h	Dh	355h	Dh
Difference	36Dh	4Ch	362h	36h
Match	3B9h	Eh	398h	Eh
Difference	3C7h	7F24Bh	3A6h	3D7D8h

[그림 4] 조작된 이미지와 비교 결과

PICT23_ADJ.jpeg x																
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0200h:	D3	2D	6D	6C	75	63	00	00	00	00	00	00	01	00	00	
0210h:	00	0C	65	6E	55	53	00	00	00	20	00	00	00	1C	00	
0220h:	00	6F	00	6F	00	67	00	6C	00	65	00	20	00	49	00	
0230h:	00	63	00	2E	00	20	00	32	00	30	00	31	00	36	FF	
0240h:	00	43	00	06	04	05	06	05	04	06	06	05	06	07	07	
0250h:	08	0A	10	0A	0A	09	09	0A	14	0E	0F	0C	10	17	14	
0260h:	18	17	14	16	16	1A	1D	25	1F	1A	1B	23	1C	16	16	
0270h:	2C	20	23	26	27	29	2A	29	19	1F	2D	30	2D	28	30	
0280h:	28	29	28	FF	DB	00	43	01	07	07	07	0A	08	0A	13	
0290h:	0A	13	28	1A	16	1A	28	28	28	28	28	28	28	28	28	
02A0h:	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	
02B0h:	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	
02C0h:	28	28	28	28	28	28	28	28	FF	C0	00	11	08	05	A0	
02D0h:	00	02	01	22	00	02	11	01	02	11	01	FF	C4	00	1C	

Template Results - JPG.bt				
Name	Value	Start	Size	Color
struct JPGFILE jpgfile		0h	3DB7Eh	Fg: Bg:
enum M_ID SOIMarker	M_SOI (FFD8h)	0h	2h	Fg: Bg:
> struct APP0 app0		2h	12h	Fg: Bg:
> struct APP2 app2		14h	22Ah	Fg: Bg:
> struct DQT dqt[0]		23Eh	45h	Fg: Bg:
enum M_ID marker	M_DQT (FFDBh)	23Eh	2h	Fg: Bg:
WORD szSection	67	240h	2h	Fg: Bg:
> struct QuanTable qtable		242h	41h	Fg: Bg:
> struct DOT dot[11]		283h	45h	Fg: Bg:

[그림 5] 변경된 jpeg quantization table

변경된 quantization table의 값을 가지는 PIC jpg를 검색한 결과, 두 개의 이미지를 도출하였다.

File	Address	Value
▼▼ Found 1▼ Found ▼ Four▼ Fc▼ Fc▼ ▼▼ Found 1 occurrences of '00 06 04 05 06 05 04 06 06 05 06 07 07 06 08 0A 10 0A 0A 09		
C:\Users\...\\PIC066.jpg	242h	00 06 04 05 06 05 04 06 06 05 06 07 07 06 08 0A 10 0A 0A 09
▼▼ Found 1▼ Found ▼ Four▼ Fc▼ Fc▼ ▼▼ Found 1 occurrences of '00 06 04 05 06 05 04 06 06 05 06 07 07 06 08 0A 10 0A 0A 09		
C:\Users\...\\PIC076.jpg	242h	00 06 04 05 06 05 04 06 06 05 06 07 07 06 08 0A 10 0A 0A 09

[그림 6] quantization table 검색 결과

따라서 Photoshop Fix로 조작한 이미지는 다음과 같다.

- **PIC066.jpg**
- **PIC076.jpg**

3. In two of the sample pictures, some objects were removed using the Samsung Galaxy's 'Object Eraser'. What are the two pictures?

특정 이미지에서 EOI marker 이후 데이터가 존재함을 발견하였다.

2F:0F80h:	A1 0B 18 00	00 00 50 68	6F 74 6F 45	64 69 74 6F	i.....PhotoEditor_Re_Edit_Data{"
2F:0F90h:	72 5F 52 65	5F 45 64 69	74 5F 44 61	74 61 7B 22	originalPath": "\/data\/sec\/phot
2F:0FA0h:	6F 72 69 67	69 6E 61 6C	50 61 74 68	22 3A 22 5C	oeditor\/0\/storage\/emulated\/0
2F:0FB0h:	2F 64 61 74	61 5C 2F 73	65 63 5C 2F	70 68 6F 74	\DCIM\/pictures
2F:0FC0h:	6F 65 64 69	74 6F 72 5C	2F 30 5C 2F	73 74 6F 72	\20170325_13075
2F:0FD0h:	61 67 65 5C	2F 65 6D 75	6C 61 74 65	64 5C 2F 30	9.jpg", "isBlendi
2F:0FE0h:	5C 2F 44 43	49 4D 5C 2F	70 69 63 74	75 72 65 73	"isNotReEdit": true, "se
2F:0FF0h:	5C 2F 32 30	31 37 30 33	32 35 5F 31	33 30 37 35	pVersion": "13010
2F:1000h:	39 2E 6A 70	67 22 2C 22	69 73 42 6C	65 6E 64 69	0", "reSize": 4, "ro
2F:1010h:	6E 67 22 3A	66 61 6C 73	65 2C 22 69	73 4E 6F 74	otation": 1, "isAp
2F:1020h:	52 65 45 64	69 74 22 3A	74 72 75 65	2C 22 73 65	plyShapeCorrecti
2F:1030h:	70 56 65 72	73 69 6F 6E	22 3A 22 31	33 30 31 30	on": false}....
2F:1040h:	30 22 2C 22	72 65 53 69	7A 65 22 3A	34 2C 22 72	..Original_Path_
2F:1050h:	6F 74 61 74	69 6F 6E 22	3A 31 2C 22	69 73 41 70	Hash_Keyd0346118
2F:1060h:	70 6C 79 53	68 61 70 65	43 6F 72 72	65 63 74 69	e74ef4a5bb93c250
2F:1070h:	6F 6E 22 3A	66 61 6C 73	65 7D 00 00	A1 0B 16 00	e0798b7313c3567a
2F:1080h:	00 00 4F 72	69 67 69 6E	61 6C 5F 50	61 74 68 5F	0aa6e97a2f39f005
2F:1090h:	48 61 73 68	5F 4B 65 79	64 30 33 34	36 31 31 38	f0c4f8ae/3729283
2F:10A0h:	65 37 34 65	66 34 61 35	62 62 39 33	63 32 35 30	SEFHk.....i.
2F:10B0h:	65 30 37 39	38 62 37 33	31 33 63 33	35 36 37 61	b...ü....;f...
2F:10C0h:	30 61 61 36	65 39 37 61	32 66 33 39	66 30 30 35	
2F:10D0h:	66 30 63 34	66 38 61 65	2F 33 37 32	39 32 38 33	
2F:10E0h:	53 45 46 48	6B 00 00 00	02 00 00 00	00 00 A1 0B	
2F:10F0h:	62 01 00 00	FC 00 00 00	00 00 A1 0B	66 00 00 00	

[그림 7] EOI 이후 데이터

"PhotoEditor" 문자열을 알아본 결과, 삼성 내장 이미지 조정 앱이라는 사실을 알게되었고, PhotoEditor APP을 직접 사용하여 객체를 삭제하는 Object Eraser 기능을 확인하였다.

이에 "PhotoEditor" 문자열을 지닌 이미지를 검색하였고, 이미지 두장을 발견하였다.

▼ Found 1 occurrences of 'PhotoEditor' in file 'C:\Users\exd0tpy\Documents\PICT\PIC008.jpg'.
C:\Users\...\\PIC008.jpg 2FOF86h PhotoEditor
▼ Found 1 occurrences of 'PhotoEditor' in file 'C:\Users\exd0tpy\Documents\PICT\PIC065.jpg'.
C:\Users\...\\PIC065.jpg 157303h PhotoEditor

[그림 8] PhotoEditor 검색 결과

따라서 Object Eraser로 조작한 이미지는 다음과 같다.

- PIC008.jpg
- PIC065.jpg

4. In addition to the pictures found in questions #1~#3, four pictures were manipulated. What are the four pictures?

PIC 이미지를 직접 확인하고 여러 포렌식 툴을 사용하여 네 장의 조작된 이미지를 발견하였다. 자세한 근거는 5번 문제에서 설명한다.

- **PIC086.jpg**
- **PIC088.jpg**
- **PIC089.jpg**
- **PIC109.jpg**

5. Find the parts where the objects were removed from the pictures found in questions #1~#4 and provide the rationale for it forensically.

- #1 (PIC031.jpg, PIC060.jpg)

파일명	PIC031.jpg
사진	
사유	Forensically 프로그램의 [Error Level Analysis] 기능으로 압축 수준이 다른 부분을 확인한다. 오른쪽 사진과 같이 눈에 띠는 부분이 존재한다. 바다 속에 빠진 사람과 비치볼이 조작된 것으로 추정된다. 해당 부분에 이미지 조작이 있음을 유추할 수 있다.

파일명	PIC060.jpg
사진	
사유	Forensically 프로그램의 [Error Level Analysis] 기능으로 압축 수준이 다른 부분을 확인한다. 오른쪽 사진과 같이 눈에 띠는 부분이 존재한다. 해당 부분에 이미지 조작이 있음을 유추할 수 있다.

- #2 (PIC066.jpg, PIC076.jpg)

파일명	PIC066.jpg	
사진		
사유	Forensically 프로그램의 [Noise Analysis] 기능으로 압축 수준이 다른 부분을 확인한다. 오른쪽 사진과 같이 눈에 띠는 부분이 존재한다. 강아지를 산책하는 사람을 삭제한 것으로 추정된다. 해당 부분에 이미지 조작이 있음을 유추할 수 있다.	

파일명	PIC076jpg	
사진		
사유	Forensically 프로그램의 [Error Level Anaylsis] 기능으로 압축 수준이 다른 부분을 확인한다. 오른쪽 사진과 같이 눈에 띠는 부분이 존재한다. 원본 파일에서는 투명 칸막이가 없는 벽 부분의 위치이지만, 오류 검출 기능일 때 눈에 띠는 것으로 보아 투명 칸막이를 삭제한 것으로 추정된다. 따라서 해당 부분에 이미지 조작이 있음을 유추할 수 있다.	

- #3 (PIC008.jpg, PIC065.jpg)

파일명	PIC008.jpg
사진	 
사유	Forensically 프로그램의 [Noise Analysis] 기능으로 압축 수준이 다른 부분을 확인 한다. 오른쪽 사진과 같이 눈에 띠는 부분이 존재한다. 길거리에 있던 사람을 삭제 한 것으로 추정된다. 해당 부분에 이미지 조작이 있음을 유추할 수 있다.

파일명	PIC065.jpg
사진	 
사유	Forensically 프로그램의 [Noise Analysis] 기능으로 압축 수준이 다른 부분을 확인 한다. 오른쪽 사진과 같이 눈에 띠는 부분이 존재한다. 강아지를 산책하는 사람을 삭제한 것으로 추정된다. 해당 부분에 이미지 조작이 있음을 유추할 수 있다.

- #4 (PIC086.jpg, PIC088.jpg, PIC089.jpg, PIC109.jpg)

파일명	PIC086.jpg
사진	
사유	Forensically 프로그램의 [Clone Detection] 기능으로 이미지 내의 유사한 영역을 강조 표시하여 복제 도구 사용을 의심한다. 오른쪽 사진과 같이 눈에 띄는 부분이 존재한다. 들판의 좌우를 복제하여 강아지를 산책시키던 사람을 삭제한 것으로 추정된다. 해당 부분에 이미지 조작이 있음을 유추할 수 있다.

파일명	PIC088.jpg
사진	
사유	Forensically 프로그램의 [Level Sweep] 기능으로 특정 밝기 레벨의 대비를 확대한다. 오른쪽 사진과 같이 눈에 띄는 부분이 존재한다. 부산의 3대 건물 중 하나가 삭제된 것으로 추정된다. 따라서 해당 부분에 이미지 조작이 있음을 유추할 수 있다.

파일명	PIC089.jpg
사진	
사유	Forensically 프로그램의 [Luminance Gradient] 기능으로 이미지의 x축 및 y축을 따라 밝기 변화를 분석한다. 오른쪽 사진과 같이 눈에 띄는 부분이 존재한다. 발표자를 삭제한 것으로 추정된다. 따라서 해당 부분에 이미지 조작이 있음을 유추할 수 있다.

파일명	PIC109.jpg
사진	 
사유	Forensically 프로그램의 [Principal Component Analysis] 기능으로 이미지에 대한 주성분 분석을 수행한다. 오른쪽 사진과 같이 눈에 띠는 부분이 존재한다. 배를 블러처리하여 조작한 것으로 추정된다. 따라서 해당 부분에 이미지 조작이 있음을 유추할 수 있다.