



저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:



저작자표시. 귀하는 원저작자를 표시하여야 합니다.



비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.



변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 [이용허락규약\(Legal Code\)](#)을 이해하기 쉽게 요약한 것입니다.

[Disclaimer](#)

공학석사 학위논문

사진파일 Exif GPS정보 조작여부
판단에 관한 연구



부 경 대 학 교 대 학 원

정보보호학 협동과정

홍 성 진

공학석사 학위논문

사진파일 Exif GPS정보 조작여부
판단에 관한 연구



부 경 대 학 교 대 학 원

정보보호학 협동과정

홍 성 진

홍성진의 공학석사 학위논문을 인준함.

2011년 8월 26일



주심 공학박사 김 창 수 (인)

위원 이학박사 박 만 곤 (인)

위원 이학박사 이 경 현 (인)

차 례

그림 차례	iii
표 차례	iv
Abstract	v
서론	1
II. 관련연구	2
2.1 스마트폰의 GPS 위치정보 저장방식	2
2.2 Exif(EXchangable Image File format)	5
2.2.1 Exif 포맷이란?	5
2.2.2 Exif 포맷구조	6
2.2.2.1 TIFF Header	6
2.2.2.2 IFD(Image File Directory)의 구조	7
2.2.3 Exif 포맷에 저장될 수 있는 정보	7
2.2.4 Exif 포맷의 GPS 위치정보	9
2.2.5 Exif 시각 정보	11
2.3 파일 유사성 검증기법	12
2.3.1 Traditional Cryptographic Hash를 이용한 검증기법	12
2.3.2 Piecewise hashing	13
2.3.3 CTPH(Context Triggered Piecewise Hash)	15
2.3.4 엔트로피 방식	15
2.4 파일의 시간정보 저장위치	15
2.4.1 FAT32 파일시스템 Directory Entry의 시간정보	16
2.4.2 NTFS 파일시스템 MFT Entry의 시간정보	17
III. 사진파일 Exif GPS정보 조작방법	20
3.1 Exif 위치정보 조작	20
3.1.1 Exif 편집 프로그램을 활용한 위치정보 조작	20
3.1.2 WinHex 프로그램을 활용한 위치정보 조작	23
IV. 사진파일 Exif GPS정보 조작여부 판단	23
4.1 파일 유사성 검증에 의한 판단	24
4.2 Exif GPS 위치정보 분석에 의한 판단	26
4.3 시간속성 정보 분석에 의한 판단	28
4.4 실제위치 주변정보 확인에 의한 판단	30

V. 결론32

참고문헌34



그림 차례

<그림 1> 스마트폰 위치 측정 방법	4
<그림 2> Exif 포맷 구조	8
<그림 3> Exif 정보 내 GPSInfo 태그 ID와 Offset 정보	8
<그림 4> GPS 위치정보	9
<그림 5> MD5 해쉬값 비교	10
<그림 6> Piecwise 해쉬	13
<그림 7> FAT32 파일시스템 Directory Entry 시간정보 분석사례	17
<그림 8> NTFS 파일시스템 MFT STANDARD_INFORMATION 속성 시간정보 분석 사례	18
<그림 9> NTFS 파일시스템 MFT FILE_NAME 속성 시간정보 분석사례	19
<그림 10> 원본 사진의 GPS 위치정보	21
<그림 11> 지도상의 실제 사진촬영 위치	21
<그림 12> Exif 편집도구를 이용하여 위치정보 수정	22
<그림 13> 위치정보가 조작된 사진촬영 위치	22
<그림 14> WinHex 프로그램을 이용한 위치정보 조작	24
<그림 15> 파일 유사성 검증 도구를 이용한 유사파일 탐지	25
<그림 16> 위·경도 정보는 조작되었으나 고도정보 일치	26
<그림 17> 파일 유사성 검증 도구를 이용해 발견한 원본파일	27
<그림 18> 고도정보를 이용하여 위치정보 조작여부 판단	28
<그림 19> Exif 시각정보	24
<그림 20> 위치정보를 수정한 파일의 시각정보	24

표 차례

<표 1> Exif 바이너리 기입방식	6
<표 2> GPSInfo 태그	12
<표 3> Exif 시각 정보	9
<표 4> FAT32 파일시스템 Directory Entry 구조	13
<표 5> NTFS 파일시스템 MFT STANDARD_INFORMATION 속성 구조 ..	18
<표 6> NTFS 파일시스템 MFT FILE_NAME 속성 구조	19



A study on manipulation detection of Exif GPS information in photographic files

Sung Jin Hong

Interdisciplinary Program of Information Security, The Graduate School,
Pukyong National University

Abstract

Recently, several manufacturers offer cameras and smartphones with a built-in GPS (Global Positioning System) receiver. GPS on smartphones is no longer an emerging trend. It' is almost a must-have feature nowadays. A picture can be tied to a geographer location, through GPS function so we can identify the position of the photographer. The location information of a picture can be important clues in solving crimes in terms of digital forensics perspective. In this thesis We introduce several types of identifying schemes which detect the similarity between two files. Moreover, we analyze the file attribute structures to obtain time and geographic information in file systems.

In the end, we propose a method to detect similar files which include the different GPS information based on LBS and manipulation of Exif GPS information in photographic files. The proposed scheme can be applied to provide some clues to solve civil and criminal cases.

I. 서론

최근에 사용되고 있는 디지털카메라나 스마트폰에는 GPS정보 수신기능이 탑재되어 있어 사진 촬영시 사진을 찍은 위치정보가 사진파일의 Exif정보에 저장된다. 사진파일의 위치정보는 디지털 포렌식 관점에서 범죄해결의 중요한 단서가 될 수 있다. 예를 들면 범행의 장소를 추적한다든지 용의자의 행적을 추적하는 경우에 활용될 수 있다. 따라서 이러한 위치정보를 고의로 조작하여 알리바이를 구성하고, 용의자의 행적을 은닉한다면 범죄수사에 큰 혼선을 일으킬 것이므로 위치정보 조작여부를 판단에 관한 연구의 필요성이 대두되고 있다.

본 논문에서는 사진파일의 GPS정보 조작여부의 판단방법에 대하여 4가지 관점의 접근방법을 소개한다.

첫 번째는 파일 유사성 비교기법을 활용해 원본 사진파일의 존재 여부를 확인하여 원본과 비교를 통해 조작여부를 판단하는 접근방법으로 용의자가 사용한 모든 디지털기기들에 저장된 수많은 파일들 중에서 위치정보가 조작된 파일과 유사한 원본파일을 찾는 방법에 대하여 소개한다.

두 번째는 Exif정보 각 태그 정보에 대한 개별비교와 특히 GPS 위·경도 정보와 고도정보를 분석하여 조작여부를 판단하는 접근방법으로 3차원의 위치정보가 완벽하게 조작되기란 쉽지 않을 것이라는 관점에서 조작여부를 판단한다.

세 번째는 파일의 시간속성 정보와 Exif정보에 저장된 시간정보를 비교분석하여 조작여부를 판단하는 접근방법을 소개한다.

마지막으로 앞에서 말한 3가지 판단방법과 함께 용의자가 주장하

는 사진촬영 장소 현장조사를 통해 사진에서 나타날 수 있는 자연현상의 영향을 분석하여 최종적으로 조작여부를 판단하는 방법에 대하여 소개한다.

앞에서 소개한 위치정보 조작여부 판단에 관한 4가지 접근방법에서 사용되는 기술에 대해서는 관련연구에서 자세히 알아보겠다.

II. 관련연구

본 절에서는 GPS의 원리와 디지털카메라나 스마트폰 등 GPS정보 수신기능이 내장된 장치에서 위치정보 저장과 관련된 기술 및 국제규격을 소개하고 위치정보 조작여부 판단과 관련하여 파일의 유사성 검증기법과 파일시스템의 시간정보 저장방식을 소개한다.

2.1 스마트폰의 GPS 위치정보 저장방식

GPS(Global Positioning System)는 미 국방성에서 개발한 것을 위성을 이용하여 위치, 속도 및 시간측정 서비스를 제공하는 시스템이다. GPS는 3차원 위치, 고도 및 시간의 정확한 측정을 할 수 있고, 24시간 연속적으로 서비스를 제공할 수 있으며, 기상조건, 간섭 및 방해에 강하고, 전 세계적인 공통 좌표계를 사용한다는 특징이 있다. 지금까지 20년 이상 오랜 세월을 걸쳐 개발하고 있는 GPS는 지구의 주

위를 선회하는 24개의 인공위성과 5개소의 감시국, 그리고 제어국으로 구성된다.

GPS의 위치결정 원리를 간단하게 설명하면 추적된 궤도에 의해서 정확한 위치를 알고 있는 위성에서 발신하는 전파를 수신하여 위성에서 관측점까지의 전파 도달시간을 측정함으로써 공간적 위치를 구하는 것이다. 따라서, 위성과의 거리를 결정하는 가장 중요한 요소는 시간이며, GPS 위성에는 지극히 안정도가 높은 원자시계를 탑재하고 있다. 위성에 탑재된 시계와 수신기의 시계가 정확히 일치한다면, 3개의 위성과의 거리만으로도 3차원적인 위치를 결정할 수 있다. 그러나, 위성에 탑재된 원자시계는 매우 고가이므로 일반인이 사용하기에는 부적합하여 수신기에는 저가의 비교적 정도가 낮은 시계를 사용하고 있다. 이러한 문제를 해결하기 위하여 4개의 위성에서 전파를 수신하여 위성 시각과 수신기 시각에서 발생하는 미지의 시간차를 제거하게 된다.

해상과 같이 고도를 알고 있거나, 2차원적인 위치 결정을 위해서 적어도 3개의 위성에서 전파를 수신할 수 있어야 하며, 3차원적인 위치를 결정하기 위해서는 적어도 4개의 위성에서 전파를 수신할 수 있어야 한다. [1]

아이폰과 같은 스마트폰 기기에서는 <그림 1>과 같이 위치측위를 위한 세 가지 방법 중 위치정보의 오차범위에 따라 GPS 위성신호, Wi-Fi AP, 3G 기지국 ID 순서로 위치정보를 제공받도록 하고 있으며 안드로이드에서도 동일하게 이루어지고 있다. 이러한 위치측위 방식은 GPS 기반 위치측위로 해결할 수 없는 도심과 실내 측위에 대해서 WLAN 기반 측위의 사용이 가능하게 하고 있다. Skyhook과 같은 사업자에 의해서 WLAN AP의 DB화가 이루어짐으로써 현재 스마트폰에서의 WLAN 기술은 3G/WLAN interworking 뿐만 아니라 위치측

위에서도 중요한 요소가 되고 있다.



<그림 1> 스마트폰 위치 측정 방법

WiFi 방식은 연결된 무선공유기의 위치 및 IP주소를 통해 자신의 대략적인 위치를 파악하는 것으로 오차범위가 큰 단점이 있으며, 3G 기지국 방식은 주변에 있는 3G 기지국과의 삼각측량을 통하여 자신의 대략적인 위치를 파악하는 방식으로 오차범위는 수십미터 이내로 WiFi 방식보다 비교적 정확하며, GPS 방식으로 GPS 위성을 통하여 위치를 파악하는 방식으로 오차범위는 3미터 이내로 가장 정확도가 높은 방식이다.

또한, 아이폰 iOS에서는 기존 위성 GPS의 취약지역에서도 위치정

보를 제공하기 위해 위성정보를 사용한 위치정보 뿐만 아니라 스카이
혹 와이어리스(<http://skyhookwireless.com>)에서 제공하는 Wi-Fi
Hotspot 정보, 구글 맵스(<http://maps.google.com/>)에서 제공하는 셀
기지국의 위치정보 API를 통한 위치정보를 이용해 사용자에게 높은
정확도의 위치정보를 제공한다. 이러한 정보를 바탕으로 구글 맵스 애
플리케이션을 통해 사용자의 위치를 지도에서 보여주는 기능을 제공하
고 있다. 또한 개발자는 별도의 라이브러리를 통해 구글 맵스 외에도
야후 지도, 네이버 맵 등의 지도정보 서비스가 가능하다. 지도 정보를
제공하는 회사의 open API 또는 URL을 이용해 위치정보와 외부 데
이터베이스를 연동한 LBS를 손쉽게 개발할 수 있다. [2]

2.2 Exif(EXchangable Image File format)

2.2.1 Exif 포맷이란?

Exif Format은 일본전자산업진흥협회(JEIDA)에서 개발한
Format으로써 1995년 Exif ver1.0을 시작으로 2003년 Exif ver
2.21 까지 개발된 상태이다. 이미지에 썸네일(thumbnail) 이미지,
GPS 정보, 시각 정보, 촬영환경 정보 등을 저장할 수 있으며 JPEG,
TIFF 6.0, RIFF, WAV 파일 Format에 적용될 수 있다. 디지털카메
라의 경우 JPEG, TIFF 6.0 방식으로 촬영할 경우 Exif 데이터를 삽
입할 수 있다. [3]

2.2.2 Exif 포맷구조

Exif Format는 APP1 마커의 데이터 영역이 삽입되어 있다. 썸네일(Thumbnail) 이미지 JPEG Format으로 구성되어 있으므로 원본 이미지와 마찬가지로 SOI마커로 시작해서 EOI마커로 끝나게 된다. Exif Format의 시작인 Exif Header는 4bytes로 '45 78 69 66' 즉, 아스키 코드로 'E x i f'이다. Exif 포맷의 구조는 <그림 2>와 같다. [4]

2.2.2.1 TIFF Header

TIFF Header는 <표 1>과 같이 Exif 데이터가 Intel 방식(Big Endian)으로 쓰여졌을 경우에는 '0x4949'로 되어있으며, Motorola 방식(Little Endian)으로 쓰여졌을 경우에는 '0x4d4d'로 되어있다.

<표 1> Exif 바이너리 기입방식

바이너리 기입방식 (2bytes)	TAG Mark (2bytes)	0th IFD 까지의 offset (4bytes)
II(0x4949)	0x002a	(일반적으로 0x00000008)
MM(0x4d4d)	0x002a	(일반적으로 0x00000008)

그 뒤를 TAG Mark와 0th IFD까지의 offset이 따르고 있다. 보통 TIFF Header 바로 뒤에 1st IFD가 따르는 구조로 되어 있으므로 0th IFD는 'II' 혹은 'MM'에서 부터 8바이트 뒤에서 시작하게 된다.

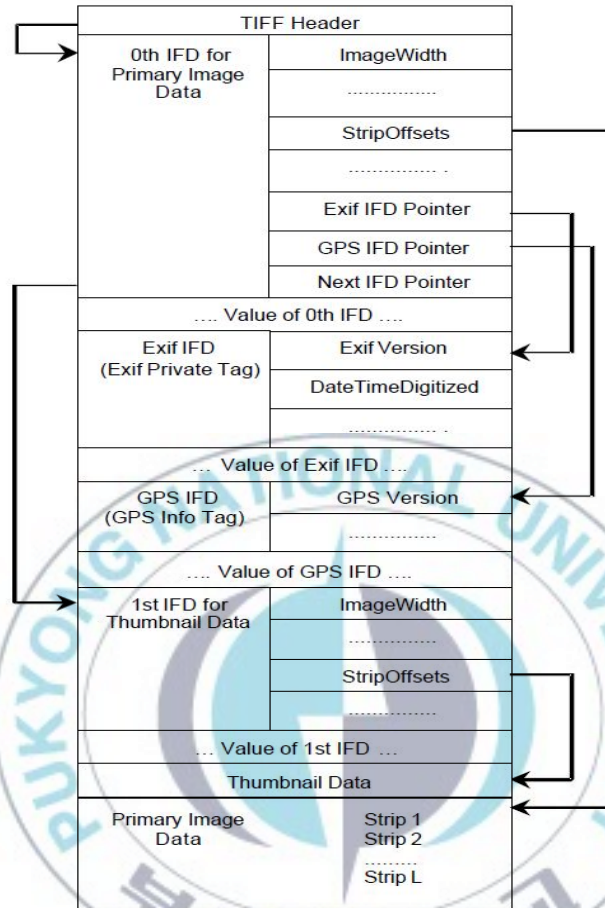
그리하여 일반적으로 offset은 0x00000008이 기입된다.

2.2.2.2 IFD(Image File Directory)의 구조

IFD란 이미지에 대한 정보를 기록하는 일종의 틀로서 일반적인 Exif Format에서 IFD영역은 0th IFD와 Exif IFD 그리고 1st IFD 가지로 구성되어 있다. 0th IFD는 원본 이미지에 대한 간단한 정보가 기재되어 있으며 Exif IFD에는 셔터스피드, 노출시간 등 원본 이미지에 대한 보다 자세한 정보를 담고 있으며 1st IFD에는 썸네일 이미지에 대한 정보를 기록하고 있다. 각각의 IFD는 디렉토리 엔트리(Directory Entry)로 구성되어 있으며 1개의 디렉토리 엔트리는 12bytes를 이용하여 데이터를 저장한다. 0th IFD와 Exif IFD, 그리고 1st IFD 또한 위와 같은 구조로 이루어져 있으며, 각 IFD에 속한 디렉토리 엔트리의 종류는 각각 다르다.

2.2.3 Exif 포맷에 저장될 수 있는 정보

Exif Format에 삽입될 수 있는 정보는 0th IFD의 경우는 32가지, EXIF IFD의 경우 57가지, 1st IFD의 경우는 32가지 등 약 120여 가지의 정보가 삽입될 수 있다. 이 중 디지털 포렌식 관점에서 중요한 GPS 정보 및 시각정보가 EXIF Format에 기록되어 있다.



<그림 2> Exif 포맷 구조

<표 2> GPSInfo 태그

태그 ID	변수명	변수타입	크기	설명
00	GPSVersionID	BYTE	4	GPS version
01	GPSLatitudeRef	ASCII	2	N(북쪽), S(남쪽)
02	GPSLatitude	RATIONAL	3	위도
03	GPSLongitudeRef	ASCII	2	E(동쪽), W(서쪽)
04	GPSLongitude	RATIONAL	3	경도
05	GPSAltitudeRef	BYTE	1	고도와 해수면과의 관계
06	GPSAltitude	RATIONAL	1	고도

07	GPSTimeStamp	RATIONAL	3	UTC(세계협정시)로 변환한 GPS촬영 시간(시,분,초)
08	GPSSatellites	ASCII	무관	측정에 사용된 위성
09	GPSStatus	ASCII	2	촬영에 사용된 GPS 수신기의 상태
0a	GPSMeasureMode	ASCII	2	GPS 측정 모드
0b	GPSDOP	RATIONAL	1	GPS 데이터의 정확도
0c	GPSSpeedRef	ASCII	2	GPS 수신기 속도에 관한 부호
0d	GPSSpeed	RATIONAL	1	GPS 수신기의 속도
0e	GPSTrackRef	ASCII	2	GPS 수신기 방향에 관한 부호
0f	GPSTrack	RATIONAL	1	GPS 수신기의 방향
10	GPSTrgDirectionRef	ASCII	2	피사체의 방향에 관한 부호
11	GPSTrgDirection	RATIONAL	1	피사체의 방향
12	GPSMapDatum	ASCII	무관	지정학적 위치에 관한 정보
13	GPSDestLatitudeRef	ASCII	2	N(북쪽), S(남쪽)
14	GPSDestLatitude	RATIONAL	3	목표 지점의 위도
15	GPSDestLongitudeRef	ASCII	2	E(동쪽), W(서쪽)
16	GPSDestLongitude	RATIONAL	3	목표 지점의 경도
17	GPSDestBearingRef	ASCII	2	목표 지점의 Bearing에 관한 부호
18	GPSDestBearing	RATIONAL	1	목표 지점의 Bearing
19	GPSDestDistanceRef	ASCII	2	목표 지점까지의 거리에 관한 부호
1a	GPSDestDistance	RATIONAL	1	목표 지점까지의 거리
1b	GPSProcessingMethod	UNDEFINED	무관	거리측정에 사용된 방법
1c	GPSAreaInformation	UNDEFINED	무관	GPS Area에 관한 정보
1d	GPSDataStamp	ASCII	11	UTC(세계협정시)로 변환한 GPS촬영 시간(년,월,일)
1e	GPSDifferential	SHORT	1	"GPS Differential Correction"기술의 적용여부

2.2.4 Exif 포맷의 GPS 위치정보

GPS란 3곳 이상의 인공위성에서 위치정보를 조합하여 특정한 위치를 전자정보로써 표현하는 것을 의미한다. 일반적으로 GPS 정보는 도(°)분(')초(")로 기록하며 우리나라의 경우 1초는 약 37미터 거리

에 해당한다.

Exif format에서는 0.001초 차이까지 기록할 수 있도록 되어 있다. 즉, GPS 장비가 오차 없이 현재의 위치를 정확히 측정할 수 있다고 가정하면 약 3.7센티미터의 미세한 위치정보의 차이를 탐지해 낼 수 있다. 따라서 GPS 정보만으로도 이미지에 찍힌 피사체가 해당 위치에 존재했음을 증명할 수 있게 된다. Exif format에서는 30가지의 필드를 통하여 GPS 정보를 나타낸다.

<표 2>와 같이 30가지의 필드를 이용하여 GPS 정보를 기록하고 있는데, Exif 정보를 보여주는 툴의 대부분은 1, 2, 3, 4, 7, 16, 17번 필드를 추출하여 GPS를 표시한다.

스마트폰으로 촬영한 사진파일 내 위치정보는 실제로 <그림 3, 4>와 같이 저장되어 있다. [5]

000000FF	D8 FF E1 27 43 45 78 69 66 00 00	y0ya'CExif..
00000124D	4D 00 2A 00 00 00 08 00 0B 01 0F	MM*.....
000002400	02 00 00 00 06 00 00 00 92 01 10
000003600	02 00 00 00 09 00 00 00 98 01 12
000004800	03 00 00 00 01 00 06 00 00 01 1A
000006000	05 00 00 00 01 00 00 00 A2 01 1B
000007200	00 00 00 00 00 00 00 00 00 00 00
000008400	00 00 00 00 00 00 00 00 00 00 00
000009600	00 00 00 00 00 00 00 00 00 00 00
000010800	00 00 00 00 00 00 00 00 00 00 00
000012000	03 00 00 00 01 00 01 00 00 87 69#i
000013200	04 00 00 00 01 00 00 00 CC 88 25I^%
000014400	04 00 00 00 01 00 00 02 3E 00 00>..
000015602	C8 41 70 70 6C 65 00 69 50 68 6F	·ÈApple ·iPho
00001686E	65 20 34 00 00 00 00 00 48 00 00	ne 4·····H··
000018000	01 00 00 00 48 00 00 00 01 34 2E	·····H·····4.
000019232	2E 31 00 32 30 31 31 3A 30 32 3A	2.1·2011:02:
000020430	38 20 31 37 3A 34 36 3A 35 31 00	08 17:46:51·
000021600	17 82 9A 00 05 00 00 00 01 00 00	··,š······

<그림 3> Exif 정보 내 GPSInfo 태그 ID와 Offset 정보

000050400					00	05	32	30	20			
000051631	GPS TagID				20	31	37	3A	11:02:08	17:			
000052834	0x0001 GPSLatitudeRef				31	31	3A	30	46:51	·2011:0			
000054032	0x0002 GPSLatitude				34	36	3A	35	2:08	17:46:5			
000055231	0x0003 GPSLongitudeRef				04	E2	00	00	1.....	·â··			
000056410	0x0004 GPSLongitude				00	4D	00	00	·i···M··			
000057600	0x0007 GPSTime Stamp				02	B8	00	05	·Ç»·,·			
000058800	01	02	00	00	00	02	4E	00	00	00	N.....	·N···	
000060000	02	05	00	00	00	03	00	00	02	80	·€···	
000061200	03	00	02	00	00	02	45	00	00	00	E.....	·E···	
000062400	04	00	05	00	00	03	00	00	02	98	·····	
000063600	07	00	05	00	00	03	00	00	02	B0	·°···	
000064800	00	00	00	00	00	02	23	00	00	00	01	·#···
000066000	04	2E	00	00	00	00	64	00	00	00	00	·d···
000067200	00	00	01	00	00	00	81	00	00	00	01	· ···
000068400	00	01	BE	00	00	00	64	00	00	00	00	·d···
000069600	00	00	01	00	00	00	08	00	00	00	01	·····
000070800	00	00	2E	00	00	01	00	00	00	14	39	·9···
000072000	00	00	64	00	00	03	00	03	00	00	00	·d···
000073200	01											·····
000074400	01											·····
000075600	01											·····
000076800	01											·····
000078000	01											·····
000079200	01	00	00	24	13	00	00	00	00	00	00	·\$···
000080400	48	00	00	00	01	00	00	00	48	00	00	·H···

<그림 4> GPS 위치정보

2.2.5 Exif 시각 정보

보통 파일의 시각정보는 파일의 내부가 아닌 메타데이터에 기록한다. 그리하여 파일시스템의 수준에서 파일의 시각정보를 조작할 수 있다. 그런데 Exif Format의 경우 <표 3>과 같이 Exif Format 내부에 시각정보를 기록하고 있어 촬영 당시부터 법정 제출시까지 파일이 조작되지 않는 이상 저장매체의 환경이나 기타 악성코드의 영향을 받지 않고 촬영시각을 특정할 수 있다. [3]

<표 3> Exif 시각 정보

태그 ID	변수명	변수타입	크기	설명
132	DateTime	ASCII	20	이미지의 생성시각
9003	DateTimeOriginal	ASCII	20	피사체가 촬영된 시각
9004	DateTimeDigitized	ASCII	20	피사체가 디지털이미지로 처리된 시각

2.3 파일 유사성 검증기법

2.3.1 Traditional Cryptographic Hash를 이용한 검증기법

디지털증거분석 대상매체에서 동일한 파일을 검색하기 위하여 통상 고전적인 암호화 해쉬값 비교 방식(MD5, SHA1 등)이 사용되는데, 이러한 해쉬값은 충돌의 회피 즉, 대상파일의 미세한 변화도 결과 해쉬값이 크게 변경되는 특징이 있어 증거물의 무결성을 증명하기 위한 방편으로 널리 사용된다. 또한 어떤 두 파일의 해쉬값이 같을 경우 그 파일들은 동일한 파일이라는 가정이 가능하므로 분석대상 매체에서 어떤 특정한 파일을 찾기 위한 방법으로 비교대상 파일들의 해쉬값을 산출하여 그 해쉬값을 비교하는 방식이 주로 사용되어져 왔다. 하지만, 비교대상의 파일이 손상 또는 변조되어 부분적으로만 일치하는 경우 <그림 5>와 같이 고전적인 해쉬값 비교방식으로는 그 유사성을 판단할 수 없다. [7] [9]



파일 1 MD5 해쉬값: d53903834a71e83b2a1af44825c5a698
 파일 2 MD5 해쉬값: 3d460618c720c850629542712547230f

<그림 5> MD5 해쉬값 비교

2.3.2 Piecewise hashing

Piecewise 해쉬 알고리즘은 한 파일 전체에 대한 해쉬값을 계산해 내지 않고 일정크기 단위로 구분하여 각 단위 블록에 대한 해쉬값을 만들어 내는 방식이다. 예를 들면, <그림 6>과 같이 어떤 파일에 대하여 처음 512바이트에 대한 해쉬값을 산출하고 그 다음 512바이트 이후부터 같은 길이로 해쉬값을 산출하는 것과 같은 방식이다. 이러한 해쉬방식은 디지털증거물에 대한 이미징시 에러를 최소화하기 위하여 개발된 것인데 만약에 에러가 발생하게 되더라도 특정 블록에 대한 무결성에만 문제가 되고 나머지 부분에 대하여는 여전히 유효한 증거로써 사용될 수 있게 하기 위한 것이었다. [8]

0-512	: 0016a7bb1e413650ff7981e06bfca0ee
512-1024	: 6d9e5e53e25f0b7b0de55ab9fad90c17
1024-1536	: 823d51512036a1c9913287a1dcccddf2

<그림 6> Piecewise 해쉬

2.3.3 CTPH(Context Triggered Piecewise Hash)

Piecewise 해쉬의 경우 파일의 어느 한 부분의 증감 또는 변형이 일어나면 그 이후 내용이 동일하다 하더라도 블록의 위치가 모두 틀어지기 때문에 모든 해쉬값이 달라져 파일의 유사성을 도출해 내기 위한 방법으로는 부적절하다. 롤링해쉬 알고리즘은 이러한 문제를 보완하기 위하여 개발 되었는데 파일내의 문구(context)를 기준으로 구분자를 만들어 각각의 구분된 영역의 마지막 몇 바이트에 대한 해쉬값을 취하여 체크섬(checksum) 데이터를 만들게 되면 유사도를 비교할 수 있다는 원리이다. 수식(1)에서 n개 만큼의 문자(character)를 가진 파일이 있다고 가정할 때 i 번째의 바이트는 b_i 로 표현될 수 있다. 그러므로 전체 내용은 (b_1, b_2, \dots, b_n) 으로 표현할 수 있다. 입력 파일에서 임의의 p 위치를 기준으로 롤링해쉬 값은 마지막 s 바이트들에 의해서 결정된다. 그러므로 롤링해쉬 r 은 다음과 같은 수식으로 표현할 수 있다. [8]

$$r_p = F(b_p, b_{p-1}, b_{p-2}, \dots, b_{p-s}) \quad (1)$$

이제 주어진 r_p 로부터 b_{p-s} 의 영향을 제거하기 위해 $X(b_{p-s})$ 와 b_{p+1} 의 요인을 더한 $Y(b_{p+1})$ 을 적용함으로써 수식(2),(3)과 같이 r_{p+1} 의 계산이 가능하다.

$$r_{p+1} = r_p - X(b_{p-s}) + Y(b_{p+1}) \quad (2)$$

$$r_{p+1} = F(b_{p+1}, b_p, b_{p-1}, \dots, b_{(p-s)+1}) \quad (3)$$

2.3.4 엔트로피 방식

엔트로피 방식은 열역학에서 출발한 개념으로써 폐쇄계에서 무질서의 정도를 측정한 값이 엔트로피라 할 수 있다. 예를 들어 얼음의 분자구조는 이것이 녹아서 물이 되었을 때보다 더 낮은 엔트로피를 가지고 있다. 또한 물이 증발하게 되면 분자는 공기를 자유롭게 움직일 수 있게 되기에 가장 높은 엔트로피를 가지게 된다. 열역학에서의 엔트로피 법칙과 정보시스템에서의 엔트로피 법칙의 가장 큰 차이점은 열역학에서는 모든 상태량을 측정하는 것이 불가능하기 때문에 통계학에 의해서 근사치를 구하는 방법이 사용되는데 정보시스템에서는 파일의 내용은 모두 알고 있는 값이기 때문에 모든 수치는 정확히 정해져 있는 수치라는 것이다. 정보시스템에서 파일의 유사성 판별 도구로 엔트로피값이 사용될 수 있다. [10]

2.4 파일의 시간정보 저장위치

본 절에서는 GPS 위치정보 수신기능이 탑재된 디지털카메라나 스마트폰에서 촬영된 사진을 사용자 컴퓨터에 옮겨 위치정보를 조작한 경우를 가정하여 우리나라에서 대부분의 일반 사용자들이 마이크로소프트 윈도우즈 운영체제에서 사용하는 파일시스템에서의 파일의 시간

정보에 대해서 알아본다.

<표 4> FAT32 파일시스템 Directory Entry 구조

Offset	Description
0 - 10	Short name (8+3) for file/folder
11	File attribute (Read only, directory, System file, and so on)
12	Reserved
13	Millisecond time for file creation
14 - 15	File creation time
16 - 17	File creation date
18 - 19	File access date
20 - 21	High 16-bit cluster number
22 - 23	File modification time
24 - 25	File modification date
26 - 27	16-bit cluster number
28 - 31	File size in bytes

2.4.1 FAT32 파일시스템 Directory Entry의 시간 정보

FAT32 파일시스템에서 파일의 시간정보는 Directory Entry에 저장되며 <표 4>와 같은 구조로 파일의 속성정보들이 저장되며 <그림 7>과 같이 파일 접근일자정보는 시각정보가 없이 날짜 정보만 저장된다. [11]

File Record						
Name	Created	Written	Accessed	Size	Cluster	
E¼%Aø~1.JPG	2010-11-10 16:59:20	2010-11-10 16:59:22	2011-04-13	55107	350299	

096	20	20	10	00	78	90	81	箭제사~1	·x	를
112	3E	77	08	00	10	00	00	p>□>··맨p>w·	·	·
128	41	4D	D6	31	8	9D	C9	85	BA	0F
144	C4	C9	2E	00	6A	00	00	00	00	00
160	C8	AB	BC	BA	C1	F8	7E	31	4A	50
176	6A	3D	8D	3E	05	00	6B	87	6A	3D
192	45	70	00	00	00	00	00	00	00	00
208	FF	FF	FF	FF	FF	FF	FF	FF	00	00
224	04	76	00	65	00	72	00	78	00	20

<그림 7> FAT32 파일시스템 Directory Entry 시간정보 분석사례

2.4.2 NTFS 파일시스템 MFT Entry의 시간정보

NTFS 파일시스템에서 파일의 시간정보는 MFT Entry에 두 가지 속성(STANDARD_INFORMATION과 FILE_NAME) 정보에 시간이 저장되는데 FILE_NAME 속성의 시간정보는 파일을 만들 때와 이름을 변경할 때 STANDARD_INFORMATION 속성의 시간정보가 복사되어 저장된다. <표 5, 6>과 같은 구조로 파일 시간속성을 포함한 정보들이 저장되어 있으며, <그림 8>과 같이 STANDARD_INFORMATION 시간정보가 분석되어 사용자들이 파일의 속성정보에서 확인 가능한 정보로 보여지며, FILE_NAME 속성의 시간정보는 <그림 9>와 같이 분석하여 볼 수 있으며 일반 사용자들이 운영체제에서 제공하는 정보로 확인할 수는 없다. [11][12]

<표 5> NTFS 파일시스템 MFT STANDARD_INFORMATION 속성 구조

Offset	Size	OS	Description
~	~		Standard Attribute Header
0x00	8		C Time - File Creation
0x08	8		A Time - File Altered
0x10	8		M Time - MFT Changed
0x18	8		R Time - File Read
0x20	4		DOS File Permissions
0x24	4		Maximum Number of Versions
0x28	4		Version Number
0x2C	4		Class Id
0x30	4	2K	Owner Id
0x34	4	2K	Security Id
0x38	8	2K	Quota Charged
0x40	8	2K	Update Sequence Number (USN)

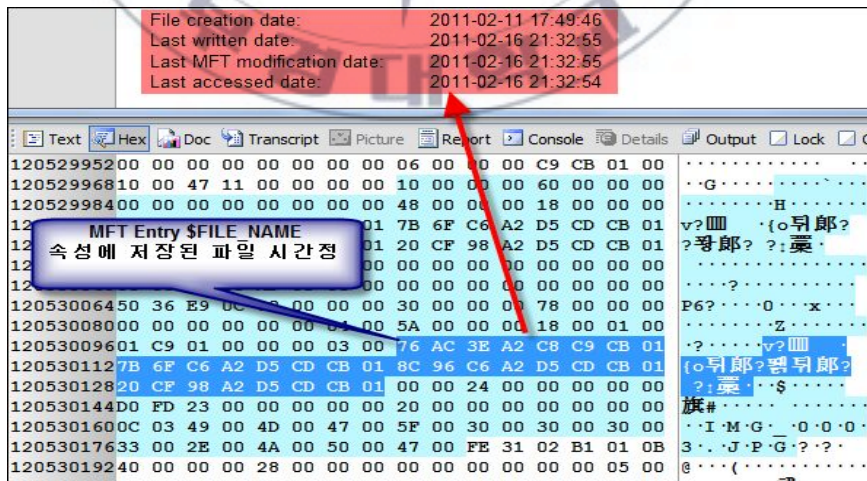
File creation date: 2011-02-11 17:49:46
 Last written date: 2011-02-16 21:32:55
 Last MFT modification date: 2011-02-16 21:32:55
 Last accessed date: 2011-02-16 21:32:54

MFT Entry \$STANDARD_INFORMATION
 속성에 저장된 파일 시간정보

<그림 8> NTFS 파일시스템 MFT STANDARD_INFORMATION 속성 시간정보 분석사례

<표 6> NTFS 파일시스템 MFT FILE_NAME 속성 구조

Offset	Size	Description
~	~	Standard Attribute Header
0x00	8	File reference to the parent directory.
0x08	8	C Time - File Creation
0x10	8	A Time - File Altered
0x18	8	M Time - MFT Changed
0x20	8	R Time - File Read
0x28	8	Allocated size of the file
0x30	8	Real size of the file
0x38	4	Flags, e.g. Directory, compressed, hidden
0x3c	4	Used by EAs and Reparse
0x40	1	Filename length in characters (L)
0x41	1	Filename namespace
0x42	2L	File name in Unicode (not null terminated)



<그림 9> NTFS 파일시스템 MFT FILE_NAME 속성 시간정보 분석사례

Ⅲ. 사진파일 Exif GPS정보 조작방법

본 절에서는 사진파일에 저장되어 있는 Exif GPS정보를 조작하는 방법에 대하여 소개한다.

3.1 Exif 위치정보 조작

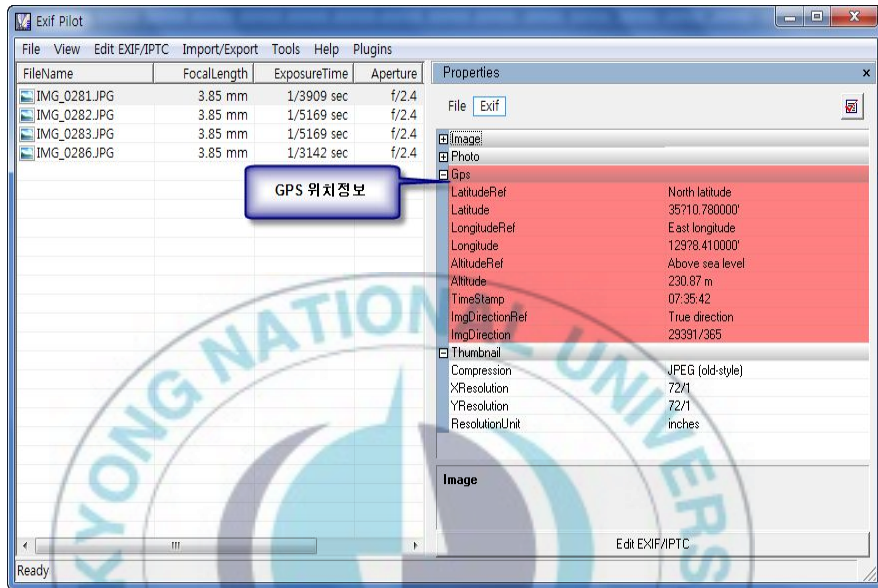
본 절에서는 iPhone4 스마트폰에서 촬영한 사진파일의 Exif 정보를 Two Pilots社에서 제작한 Exif Pilot 프로그램을 활용하여 분석하고 조작하는 방법과 X-Ways Software Technology社에서 제작한 WinHex프로그램을 활용하여 조작하는 방법을 소개한다.

3.1.1 Exif 편집 프로그램을 활용한 위치정보 조작

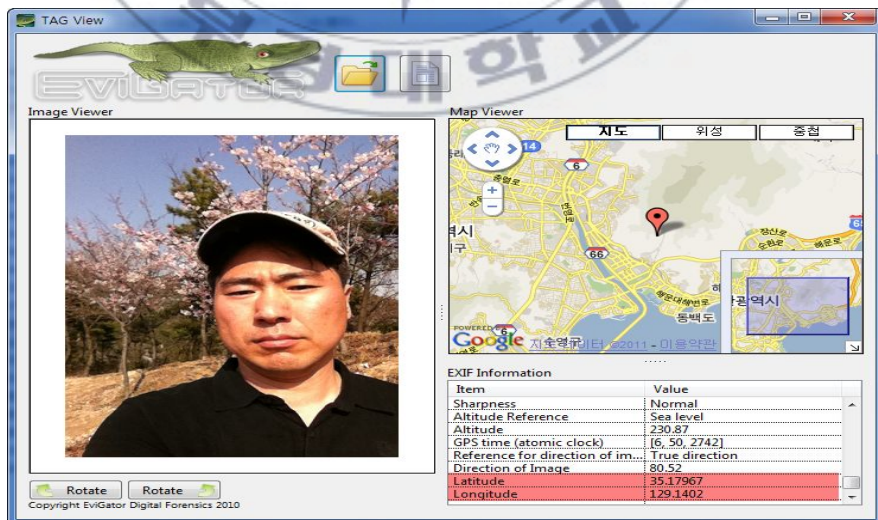
사진파일의 Exif 정보를 편집하는 도구들은 여러 가지가 나와 있어 인터넷을 통해 손쉽게 구할 수 있고 사용법 또한 간단하여 누구나 쉽게 사용할 수 있다. <그림 10, 11>은 Exif Pilot 프로그램의 Exif 정보 조회기능을 활용하여 위치정보를 확인하고 실제위치를 지도상에 표시한 것이며,

<그림 12, 13>은 Exif Pilot 프로그램의 Exif 편집기능을 활용하여 위치정보를 수정한 후 저장하고, 수정된 파일의 촬영 위치를 지도

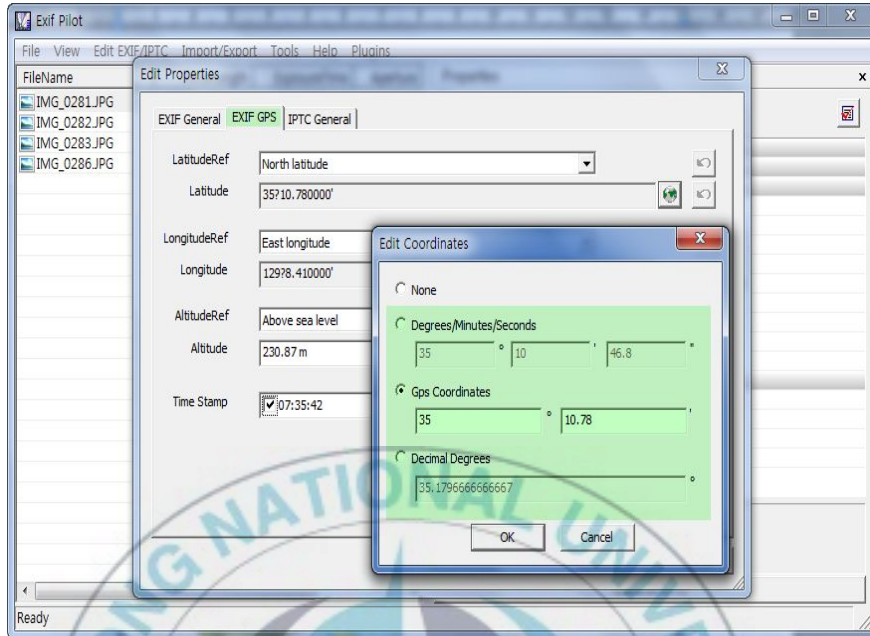
상에 표시한 것이다. 지도를 자세히 보면 위치정보가 원본은 산 중턱이며, 수정된 위치는 해수면과 가까운 강변임을 알 수 있다.



<그림 10> 원본 사진의 GPS 위치정보



<그림 11> 지도상의 실제 사진촬영 위치



<그림 12> Exif 편집도구를 이용하여 위치정보 수정



<그림 13> 위치정보가 조작된 사진촬영 위치

3.1.2 WinHex 프로그램을 활용한 위치정보 조작

사진파일의 Exif GPS 위치정보 태그의 헥사코드를 WinHex 프로그램을 이용하여 직접 수정할 수 있다. 단, Exif의 구조를 잘 알고 있어야 가능할 것이다. <그림 14>는 GPS 위·경도 정보를 WinHex 프로그램을 이용하여 수정하는 그림이다.

IV. 사진파일 Exif GPS정보 조작여부 판단

본 절에서는 사진파일 Exif GPS정보의 조작여부를 판단하는 방법에 대하여 3가지 관점의 접근방법을 소개한다. 첫 번째는 파일 유사성 비교기법을 활용해 원본 사진파일의 존재여부를 확인하여 원본과 비교를 통해 조작여부를 판단하는 접근방법이며, 두 번째는 Exif정보 각 태그 정보에 대한 개별비교와 특히 GPS 위·경도 정보와 고도 정보를 분석하여 조작여부를 판단하는 접근방법이며, 세 번째는 파일의 시간 속성 정보와 Exif정보에 저장된 시간정보를 비교분석하여 조작여부를 판단하는 접근방법을 소개한다. 마지막으로 앞에서 말한 3가지 판단방법과 함께 용의자가 주장하는 사진촬영 장소 현장조사를 통해 최종적으로 조작여부를 판단하는 방법에 대하여 연구한다.

Offset	0	1	2	3	4	5	6	7	8	9	10	11	
00000540	38	00	00	00	DF	80	00	00	12	BB	00	00	8...B!...»..
00000552	12	ED	00	00	07	7E	00	00	00	4D	00	00	.i...~...M..
00000564	00	14	00	09	00	01	00	02	00	00	00	02
00000576	4E	00	00	00	00	02	00	05	00	00	00	03	N.....
00000588	00	00	02	9C	00	00	00	00	00	00	00	00
00000600	45	00	00	00	00	00	00	00	00	00	00	00
00000612	00	00	02	B4	00	00	00	00	00	00	00	00
00000624	00	00	00	00	00	00	08	00	05	00	00	01
00000636	00	00	02	CC	00	07	00	05	00	00	00	03	...i.....
00000648	00	00	02	D4	00	10	00	02	00	00	00	02	...ô.....
00000660	54	00	00	00	00	11	00	05	00	00	00	01	T.....
00000672	00	00	02	EC	00	00	00	00	00	00	00	23	...i.....#
00000684	00	00	00	01	00	00	04	36	00	00	00	646...d
00000696	00	00	00	00	00	00	00	01	00	00	00	81
00000708	00	00	00	01	00	00	03	49	00	00	00	64I...d
00000720	00	00	00	00	00	00	00	01	00	00	88	2EI..
00000732	00	00	00	97	00	00	00	06	00	00	00	01	...!.....
00000744	00	00	00	32	00	00	00	01	00	00	0A	B6	...2.....
00000756	00	00	00	01	00	00	72	CF	00	00	01	6Drî...m
00000768	00	06	01	03	00	03	00	00	00	01	00	06
00000780	00	00	01	1A	00	05	00	00	00	01	00	00
00000792	03	42	01	1B	00	05	00	00	00	01	00	00	...B.....

<그림 14> WinHex 프로그램을 이용한 위치정보 조작

4.1 파일 유사성 검증에 의한 판단

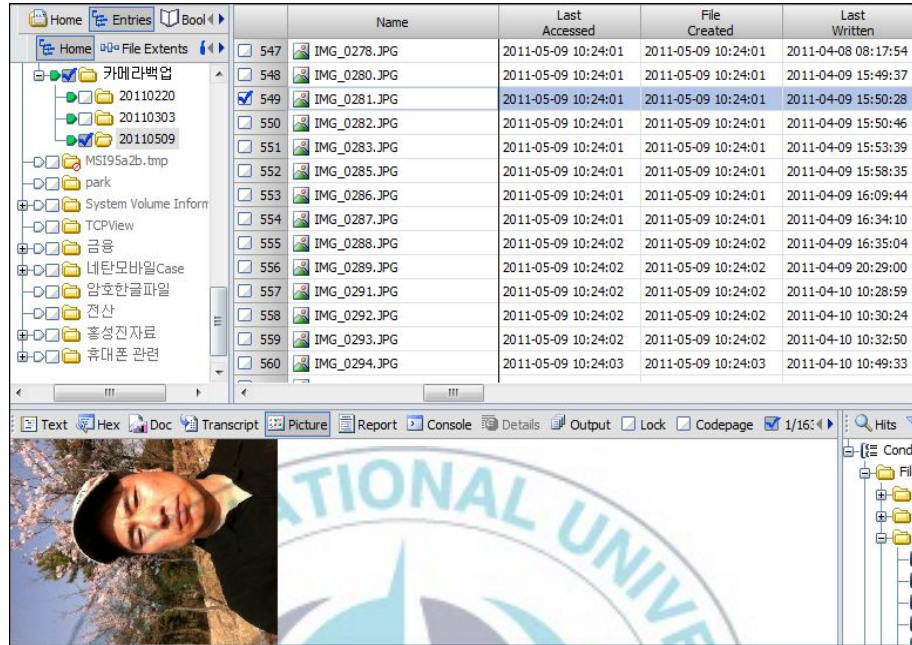
용의자가 알리바이를 증명하기 위해 제시한 사진파일의 GPS 위치 정보가 조작되었는지 조사하기 이전에 우선 원본 사진파일을 찾아서 원본파일의 위치정보와 비교한다면 가장 효율적인 판단방법이 될 것이다. 하지만, 사진을 촬영한 휴대전화를 찾을 수 없는 경우나 삭제되어 복구가 불가능한 경우에는 용의자가 사용한 컴퓨터 등 디지털저장 매체를 확보하여 원본 사진파일의 존재여부를 조사해 볼 필요가 있다.

이 경우에 기존의 암호화 해쉬(MD5, SHA1 등) 비교방식으로는 100% 동일한 파일은 검색해 내지만 1bit의 데이터 차이만 있어도 전혀 다른 파일로 인식되어 검색하지 못하는 단점이 있다. 이러한 단점을 보완하기 위해 파일의 유사성 정도를 측정하는 방식의 해쉬기법이 연구되었고, 본 연구에서는 CTPH(Context Triggered Piecewise

Hash) 기법이 구현된 도구(Ssdeep 2.6)를 활용해 용의자가 사용한 디지털저장매체에서 GPS 위치정보가 조작된 파일과 유사도가 높은 파일을 검색하여 <그림 15>와 같이 유사도가 높은 파일이 발견된다면 그 파일은 <그림 16>과 같이 원본 파일일 가능성이 있다. 즉, GPS 위치정보가 조작된 파일과 원본파일의 위치정보를 비교하여 조작여부를 판단할 수 있을 것이다. 단, 원본 파일이 남아있는 경우에 가능하다는 문제점이 있다.



<그림 15> 파일 유사성 검증 도구를 이용한 유사파일 탐지



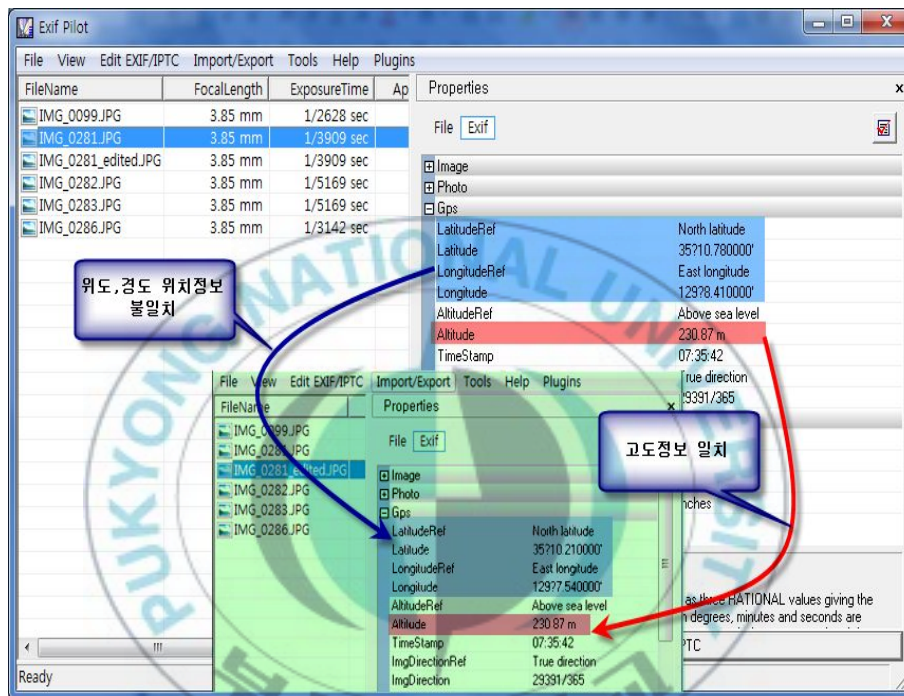
<그림 16> 파일 유사성 검증 도구를 이용해 발견한 원본파일

4.2 Exif GPS 위치정보 분석에 의한 판단

Exif GPS 위치정보에서 위도와 경도정보를 통해 2차원의 평면적인 위치가 정해진다면 실제 3차원 공간상의 위치는 고도정보가 더해지면서 확정된다. 2차원의 평면적인 위도와 경도정보가 조작되었다면 조작된 위치의 고도정보를 확인하여 실제 고도정보와 전혀 다른 정보가 확인된다면 사진파일의 위치정보가 조작되었다고 추정할 수 있을 것이다.

<그림 17>과 같이 실제 해발 250미터의 산에서 촬영된 사진의 위치정보를 조작하여 강변 공원에서 촬영한 것처럼 조작하였으나 <그림 18>과 같이 고도정보가 조작된 위치의 고도정보와 현저한 차이를

보여 위치정보의 조작사실을 확인할 수 있다.



<그림 17> 위·경도 정보는 조작되었으나 고도정보 일치

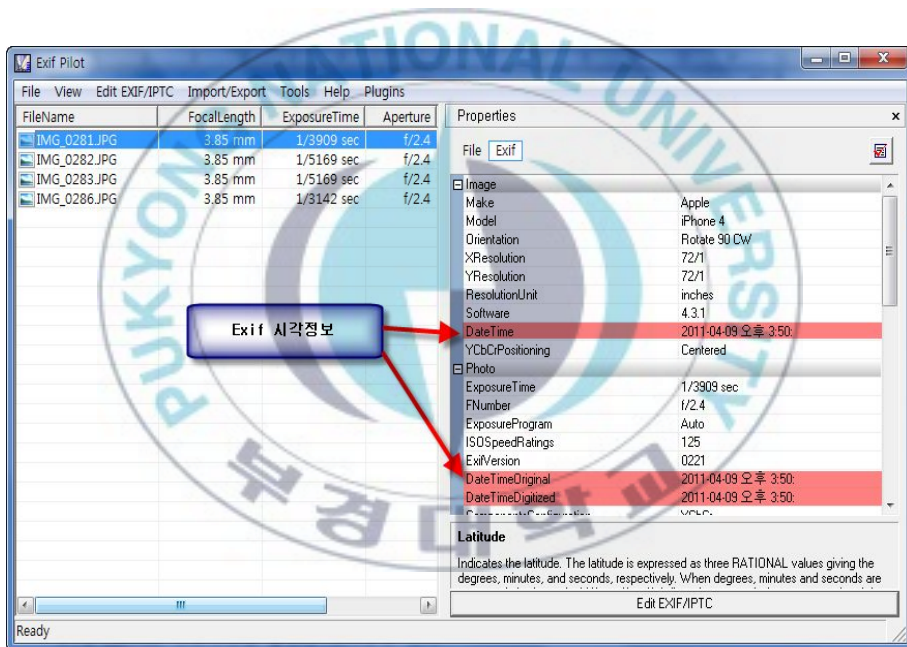


<그림 18> 고도정보를 이용하여 위치정보 조작여부 판단

4.3 시간속성 정보 분석에 의한 판단

Exif에는 <표 3>과 같이 이미지의 생성시각을 저장하는 DateTime 태그와 피사체가 촬영된 시각을 저장하는 DateTimeOriginal 태그, 피사체가 디지털이미지로 처리된 시각을 저장하는 DateTimeDigitized 태그가 있어 사진이 촬영되면 <그림 19>와 같이 각각의 시각정보를 해당 위치에 저장한다. 대부분의 사진에서 3가지의 시간정보는 동일하게 확인된다. 일반적으로 사진파일의 위치정보를 수정하려면 사진파일을 편집할 컴퓨터에 옮긴 후 편집작업을 하게 되는데 이때 파일이 옮겨져서 저장된 파일시스템에 <그림 20>과 같이 해당 파일에 대한 시각정보가 생성된다. 시각정보를 자세히 살펴보면 파일 생성시각과 접근시각은 복사된 시간으로 저장되지만 최종수

정시각정보는 사진을 찍은 시각정보가 저장되는 것을 확인할 수 있다. 최종수정시각정보는 Exif에 저장되어 있는 시각정보 태그에 저장된 시각정보와 일치한다. 만약 위치정보를 조작하면서 파일을 수정하였다면 최종수정시각정보가 Exif 시각정보와 다르게 설정되는 것을 확인할 수 있다. 이 사실을 바탕으로 위치정보의 조작을 의심해 볼 수 있는 근거가 되는 것이다.



<그림 19> Exif 시각정보

	Name	Last Accessed	File Created	Last Written
<input type="checkbox"/> 1	IMG_0282.JPG	2011-04-13 19:26:27	2011-04-13 19:26:27	2011-04-09 15:50:46
<input type="checkbox"/> 2	IMG_0283.JPG	2011-04-13 19:26:27	2011-04-13 19:26:27	2011-04-09 15:53:39
<input type="checkbox"/> 3	IMG_0286.JPG	2011-04-13 19:26:28	2011-04-13 19:26:28	2011-04-09 16:09:44
<input type="checkbox"/> 4	IMG_0099.JPG	2011-04-14 13:25:57	2011-04-14 13:25:57	2011-03-01 15:09:52
<input type="checkbox"/> 5	IMG_0281_edited.JPG	2011-04-14 13:56:46	2011-04-13 19:26:27	2011-04-14 13:56:46

위치정보가 수정된 파일은 생성시각보다 최종수정시각이 더 늦게 설정되어 있음.

<그림 20> 위치정보를 수정한 파일의 시각정보

4.4 실제위치 주변정보 확인에 의한 판단

모든 사진은 실제 촬영된 위치가 존재한다. 따라서 사진의 위치정보가 조작되었다고 의심된다면 가장먼저 확인해야 할 것은 사진파일에 설정되어 있는 위치정보를 확인하고 실제 위치주변에 가서 주변 지형지물을 확인하여야 할 것이다. 실제위치 주변에서 사진에서 발견되는 지형지물이 발견되지 않는다면 당연히 조작된 것으로 판단할 수 있을 것이며 지형지물로 판단되지 않는 사진의 경우 앞에서 소개한 방식으로 조사해 보아야 할 것이다. 그리고, 사진촬영 시각정보와 촬영장소의 당시 날씨정보, 촬영방향과 촬영장소의 태양광 각도 등 사진파일에 나타나는 빛과 바람 등 자연현상의 영향을 분석하여 사진파일을 관찰한다면 위치정보 조작여부 판단에 큰 도움이 될 것이다. 특히, 빛은 장소와 계절, 날씨 그리고 시간에 따라 각기 다른 분위기를 띤다. 봄, 여

름, 가을, 겨울이 그렇고 흐린 날과 맑은 날, 새벽과 정오 또는 저녁이
냐에 따라서 시시각각으로 다양한 느낌을 주므로 실제장소의 빛의 영
향과 조작된 위치에서의 빛의 영향을 분석한다면 조작여부를 판단할
수 있을 것이다.



V. 결론

본 논문에서는 사진파일의 GPS정보 조작여부의 판단방법에 대하여 4가지 관점의 접근방법과 을 소개하였다.

첫 번째로 파일 유사성 비교기법을 활용해 원본 사진파일의 존재 여부를 확인하여 원본과 비교를 통해 조작여부를 판단하는 접근방법으로 용의자가 위치정보가 포함된 사진파일의 위치정보를 편집하였다고 의심된다면 용의자가 사용한 모든 디지털기기들을 압수하여 조사하여야 할 것이다. 가장 먼저 사진을 촬영한 장치를 조사하여 원본 사진파일이 남아 있는지 여부를 조사하고, 용의자가 사용한 이동식저장장치(USB)나 개인용 컴퓨터 및 노트북, 혹은 직장 내 컴퓨터 등 가능한 모든 디지털 저장매체들을 조사하여야 할 것이다. 이처럼 대량의 파일들 중에서 위치정보가 조작된 파일과 유사한 원본파일을 찾는 것은 기존의 전통적인 암호화 방식의 해쉬 기법으로 조사를 한다면 엄연히 용의자의 컴퓨터 등에 남아 있는 원본 파일은 발견할 수 없을 것이다. 따라서 CTPH(Context Triggered Piecewise Hash)와 같은 파일 유사성 비교기법을 활용는 이런 경우 매우 효과적이다.

두 번째는 Exif GPS 위치정보를 분석하여 조작여부를 판단하는 접근방법으로 iPhone4와 같은 최신 스마트폰은 2차원의 위·경도 정보와 함께 3차원의 고도정보까지 저장되어 있어 위치정보를 조작할 경우 3차원의 정보를 완벽하게 조작하지 않았다면 사진파일에 포함된 2차원 위치정보에 실제 고도를 확인하여 위치정보 조작여부를 판단할 수 있을 것이다. 그러나 같은 기기를 가지고 서로 다른 위치에서 촬영한 여러 파일의 3차원 위치정보를 발췌하여 조작하고자 하는 사진파일

의 위치정보에 저장하였다면 이 방식으로는 위치정보 조작여부를 판단하는 방법으로 적합하지 않을 것이다.

세 번째는 파일의 시간속성 정보와 Exif정보에 저장된 시각정보를 비교분석하여 조작여부를 판단하는 접근방법으로 파일에는 생성시간, 접근시간, 수정시간 등의 시간정보가 있는데 파일을 실행, 복사, 이동, 편집, 삭제할 경우 시간정보는 조금씩 변화한다. 예를 들면, 파일을 열어보는 경우 마지막 접근시간이 수정되고, 수정하는 경우 마지막 수정시간이 수정하고 저장한 시간으로 변경된다. 또한, 파일을 복사하여 옮긴 경우 생성시간과 접근시간은 복사된 시간으로 변경되지만 수정시간은 변경되지 원본 파일과 동일하다. 이러한 특성을 활용하여 원본 Exif 정보 내에 포함된 시간은 실제 사진이 촬영된 시간을 의미하고 이 시간은 직접 수정하지 않는 이상 변함이 없다. 만약 사진파일을 단순히 복사하였다면 원본 파일의 Exif 정보 내 시간은 복사된 파일의 마지막 수정시간과는 동일한 시간으로 설정되어 있어야 한다. 사진파일의 위치정보가 수정되었다면 Exif 정보 내 시간정보와 파일의 마지막 수정시간은 서로 다를 것이다. 이런 사실을 기반으로 위치정보의 조작을 추정할 수 있다.

앞에서 소개한 3가지 방법들은 용의자가 완벽하게 위치정보와 파일의 시간정보를 조작하고 원본파일을 삭제하였다면 아무런 의미가 없는 방법일 수 있지만 최소한 완벽하게 조작하지 못한 용의자의 알리바이는 깰 수 있을 것이다.

마지막으로 비록 조작되었지만 사진 촬영장소인 현장은 존재하고 촬영시간이 특정되므로 당시 현장상황을 판단할 만한 기타 자료(주변 지형지물, 태양광의 방향, 바람의 방향, 날씨 등)를 수집하여 비교·분석하고 유사 장소에서 같은 시간대에 촬영된 다른 사진파일들을 수집

하여 위치정보가 조작된 사진파일에서 발견되는 자연현상과 비교하여 분석한다면 사진파일의 조작여부를 판단할 수 있을 것이다.

모든 범죄는 흔적을 남긴다” 는 말이 있다. 용의자가 아무리 완벽하게 조작하였다 하여도 흔적은 남기 마련이다.



참고문헌

- [1] Wikipedia encyclopedia, “Global Positioning System (GPS)” ,
http://en.wikipedia.org/wiki/Global_Positioning_System, 2011
- [2] 정구민, 최완식, “스마트폰 위치기반 서비스(LBS) 기술동향” ,
2010
- [3] 한국정보통신산업협회, “LBS 기술 및 시장동향 연구보고서” , 2010
- [4] 한규영, 최완식, 전주원, 안준배, “LBS 측위기술 현황 및 고도화 이슈” , 2009
- [5] Google mobile, "<http://www.google.com/mobile>"
- [6] Radio Shack, "A Guide To The Global Positioning System (GPS) – GPS Timeline", 2010
- [7] JEITA, “EXIF 2.2 Specification” , 2002.
- [8] Metadata Working group, "Guidelines for Handling Image Metadata", 2008
- [9] Andreas Huggel, "Exiv2 Image Metadata Library", 2009
- [10] Wikipedia encyclopedia, “Exchangeable image file format” ,
http://en.wikipedia.org/Exchangeable_image_file_format, 2011.
- [11] Wikipedia encyclopedia, “Geotagging standards in electronic file formats” , <http://en.wikipedia.org/wiki/Geotagging>, 2011.
- [12] Phil Harvey, “ExifTool Tag Names” , 2008.
- [13] Dustin Hurlbut-AccessData, “Fuzzy Hashing for Digital Forensic Investigators” , 2009.
- [14] Jesse Kornblum, “Identifying almost identical files using

- context triggered piecewise hashing” , 2006.
- [15] Vassil Roussev, Golden G. Richard III, Lodovico Marziale, “Multi-resolution similarity hashing” , 2007.
- [16] Tom Davis, “Utilizing Entropy to Identify Undetected Malware” , 2009.
- [17] Brian Carrier, "File System Forensic Analysis", 2005
- [18] Wikipedia encyclopedia, “File Allocation Table” ,
<http://en.wikipedia.org/wiki/Fat32#FAT32>, 2011
- [19] Andries E. Brouwer, "The FAT filesystem"., 2006
- [20] Richard Russon and Yuval Fledel, "NTFS Documentation", 2007
- [21] Microsoft Corporation, "How NTFS Works", 2008
- [22] Guidance Software, "EnCase Advanced Computer Forensics “, 2009
- [23] 이정범, 윤용인, 이상훈, 두경수, 하동환, "빛의 방향 분석을 기반으로 한 합성된 이미지 판독", 2006
- [24] 이정범, "MATLAB을 이용한 디지털 이미지의 위, 변조 분석 연구", 2006