ABSTRACT

Recently, the integration of geographical coordinates into a picture has become more and more popular. Indeed almost all smartphones and many cameras today have a built-in GPS receiver that stores the location information in the Exif header when a picture is taken. Although the automatic embedding of geotags in pictures is often ignored by smartphone users as it can lead to endless discussions about privacy implications, these geotags could be really useful for investigators in analysing criminal activity. Currently, there are many free tools as well as commercial tools available in the market that can help computer forensics investigators to cover a wide range of geographic information related to criminal scenes or activities. However, there are not specific forensic tools available to deal with the geolocation of pictures taken by smartphones or cameras. In this paper, an image scanning and mapping tool for investigators is proposed and developed. This tool scans all the files in a given directory and then displays particular photos based on optional filters (date/time/device/localisation…) on Google Map. The file scanning process is not based on the file extension but its header. This tool can also show efficiently to users if there is more than one image on the map with the same GPS coordinates, or even if there are images with no GPS coordinates taken by the same device in the same timeline. Moreover, this new tool is portable; investigators can run it on any operating system without any installation. Another useful feature is to be able to work in a read-only environment, so that forensic results will not be modified. This tool’s real-world application is also presented and evaluated in this paper.

MapExif: An Image Scanning and Mapping Tool for Investigators

Lionel Prat, French Gendarmerie Forensics Research Institute (IRCGN), Rosny-sous-Bois, France
Cheryl Baker, University College Dublin, Dublin, Ireland
Nhien An Le-Khac, University College Dublin, Dublin, Ireland

1. INTRODUCTION

Since the start of the digital information age to the rise of the Internet, the amount of digital data has dramatically increased. Some data is structured and stored in a traditional relational database, while other data, including pictures and videos, is unstructured. Organizations also have to consider new sources of data generated by new devices such as smartphones and cameras. The availability and adoption of newer, more powerful mobile devices, coupled with ubiquitous access to global networks will drive the creation of more new sources for data. As a consequence, we have had a deluge of data from not only science and industry fields but

DOI: 10.4018/IJDCF.2015040104
also digital forensics fields. Obviously, handling and analysing large and complex data has always offered the greatest challenges as well as benefits for organisations of all sizes. Although the amount of data available to us is constantly increasing, our ability to process it becomes more and more difficult. This is especially true for the criminal investigation today.

One of the big challenges for the IT forensics department of the French Gendarmerie Forensic Sciences Institute is the number of pictures investigators have to analyse. Sometimes it is not urgent as for instance, the suspect is already in prison, and a traditional image forensics approach can be applied. However, most of the time, especially for field investigators, the images retrieved need to be analysed in a very short time. The following example shows the requirement for a geolocation-based tool. A floating body is discovered in a river and a “friend” of the victim is suspected. During searching, the investigators found a number of smart phones, hard disks, memory cards… The suspect claims to have not been at the crime scene. To verify his story, investigators have to analyse thousands of photos by manually checking the geolocation data embedded into the picture. During the analysis they discovered a picture of him in an area, near the crime scene. Unfortunately it was 48 hours before the picture was found, and due to lack of proof, the suspect had already been released. This example demonstrates the need for a tool that helps the mapping and analysing of photos based on exif data, especially geotagging.

In fact, there are software available nowadays, such as GeoSetter (GeoSetter, 2014) and Google Picasa (Google Picasa, 2014), that can display the position of pictures on a map. However, they just spot all images regardless of the device used, and with no filter function. The only way to have a custom view for the user is to select which images to display before they are shown on the map. Moreover, GeoSetter and Google Picasa are not forensics tools; investigators do not know if these tools make changes to the data, which would be unacceptable if they were to be used as evidence. These current tools moreover cannot handle images without GPS information; neither to generate user reports.

Therefore, in this paper, we present a new geolocation-based forensics tool, MapExif, that scans all pictures retrieved from smart phones, cameras, etc. and extracts the exif data (date/time, device, geolocation) to display them efficiently on a map. MapExif is developed in PHP/MySQL, thereby making it compatible with different operating systems. It can run on both a single computer and on a server. It scans recursively all files in a given directory and identifies and indexes all the images in the databases. MapExif also offers important functionalities such as zone filter, device filter, and date filter. Indeed, this tool can handle and display images without GPS information.

It makes the connection between a geotagged non-geotagged images taken by the same device in the same time line. As pictures do not always have geotagged information, for example in the case of a photograph taken inside a building, this functionality is very useful. By using MapExif, investigators can also generate reports and easily manipulate the results without fear that the results could be altered. We describe in this paper the architecture and the development of this tool. We also discuss experiments using MapExif tool in scanning and mapping forensics images during real work application.

The rest of the paper is organised as follows: Section 2 describes the background research in the area. Section 3 details the architecture of the MapExif tool. We present and analyse its functionalities in Section 4. Next, we discuss the test results of the tool in different forensics scenarios in Section 5. Finally, we conclude in Section 6.

2. BACKGROUND

In this section, we present firstly the background concepts related to photographic metadata, exif format and geotagging. We then look at related work in this context.
Related Content

Efficient Forensic Analysis for Anonymous Attack in Secure Content Distribution
[www.igi-global.com/article/efficient-forensic-analysis-anonymous-attack/1592?camid=4v1a](www.igi-global.com/article/efficient-forensic-analysis-anonymous-attack/1592?camid=4v1a)

Efficient Image Matching using Local Invariant Features for Copy Detection
[www.igi-global.com/chapter/efficient-image-matching-using-local/52858?camid=4v1a](www.igi-global.com/chapter/efficient-image-matching-using-local/52858?camid=4v1a)

A High Capacity Reversible Data Hiding Scheme Based on Multi-Level Integer DWT and Histogram Modification