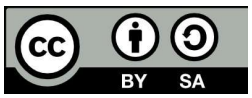
DOI: 10.21120/LE/10/3-4/3 **Landscape & Environment 10 (3-4) 2016. 117-122**

GUIDELINES FOR COST-EFFECTIVE GEOVISUALIZATION IN DIGITAL FORENSICS

MARIANNA ZICHAR

University of Debrecen, Faculty of Informatics, Department of Computer Graphics and Image Processing, H-4002, Debrecen, Kassai út 26. P.Box 400.
e-mail: zichar.marianna@inf.unideb.hu

Received 9 August 2016, accepted in revised form 29 August 2016



Abstract
Every field of our life is influenced by the appearance of new technologies. This means that new challenges keep being met and finding solutions, developing methods to deal with them belong to our tasks. Law enforcement has to be always ready to adopt the achievements of any disciplines. Experts and professionals in any field should be aware of applicability of the knowledge they have that is why it is important to highlight as much fields where our knowledge can be used as we can. Digital forensics differs from traditional forensics in many aspects that is why a general GIS professional can be involved into an investigation easily. This paper aims to provide methods to geovisualize information containing or referring to location data. Cost effective solutions are preferred throughout the paper.

Keywords: digital forensics, GIS tools, geovisualization, Google Earth, Fusion tables

1. Introduction

Our life immersed in digital technologies has changed considerably. Everything became, becomes or is going to become simpler by using the several innovative features of informatics. You can keep in touch with people living far away for free (by email, Skype, social media, etc.), store, share and look for any kind of information (web portals, digital archives, browsers, search engines, cloud applications), facilitate administration (booking, banking, purchasing, etc.), acquire new skills (by taking online courses, (video) tutorials), control your household appliances (with innovations of internet of things) and the listing could be continued. The volume of influencing our life by digital technologies differs from generation to generation. Generation Z (with birth years starting from the late 1990s) is often called also digital natives, because they are all "native speakers" of the digital language of computers, video games and the internet. They are surrounded by digital appliances since their birth, so their usage is natural for them. Following the track of a plane in internet is as obvious for this generation as picking up a book for their parents. People who were not born into the digital world, but during their life have become committed in adopting new achievements of digital technology are referred as digital immigrants. The nature of the two groups is summarized in the work of Prensky (Prensky 2001). It can be claimed without any doubt that life in the 21st century is strongly influenced by IT. Unfortunately, dark sides of this phenomena have also to be mentioned, because like the physical world, the digital one is also threatened by criminals.

Digital technologies can appear in two different contexts in forensics. Firstly, digital world itself can be the object or a tool of a crime. Rather common form of this is

hacking a website (and altering its content), or online interfaces of different applications (online banking, stores) accessed via web browsers. Computer viruses (independently whether they do damage or not) belong to this category as well.

Second context is when the digital world provides us evidences about crimes. In the field of law enforcement GIS is often used for visualization purposes as well as for data analysis (Pődör 2014) or for data acquisition (Pődör 2016). Crime mapping and analysis do not substitute for, but complete to other forms of crime analysis. Our task is to understand characteristics of available information in order to be able to recognize where tools of GIS can support the investigation. While mapping means that hidden information is captured mainly by the investigator based on the visual experience, analysis produces new in-formation that can confirm or deny our hypothesis. In other words, mapping indicates who, what, when, and where, but analysis helps determine why and what it all means (Bruce 2001).

Digital forensics differs from traditional forensics in many aspects. A criminal investigation is conducted by members of law enforcement, but digital forensics may be used to explore data by organizations or individuals as well. Digital forensics is the application of scientific principles to the process of discovering information from a digital device (Gogolin 2013). The complex process is supported by software products, methods, regulations and requires a particular detailed, sometimes exhaustive work. Basically, any digital device can provide data for investigation not only computers (in any form), but printers, cell phones, mobile devices, GPS devices, storage media or other programmable devices. Geographic Information Systems (GIS) can enhance the process of cognitive interpretation of the hidden spatial information by recognizing the geospatial relationship between objects, people, scenes, events, etc. (Zichar 2013).

The basic steps of a digital forensic investigation (Harrington – Cross 2015):

- Seizure

Obtaining and preserving computers, additional digital devices and/or media.

- Acquisition

Data retrieval from devices resulted by the previous step.

- Analysis

Examinations of data retrieved in the previous step to answer questions.

- Reporting

Creating documentations about the evidentiary findings.

It is mainly the last two stages where a GIS expert can be involved into the investigation, but sometimes acquiring GPS data from a device can provide additional information about a case too.

2. Simple geovisualization tools for digital forensics

Without professional investigating software it is our task to look for data that can provide us additional information about the activity of the device owner. This section overviews the types of digital information containing geospatial data component and also highlights the methods how to geovisualize them. The order of the listing is determined by the mapping types. The mapping can be classified into two groups with significant differences (Table 1).

Direct mapping means that the data to be visualized are available in a format that can be interpreted (opened) by an appropriate GIS application immediately. In the case of indirect mapping (often time consuming) preprocessing has to be done in order to start the visualization (Zichar 2016).

GPS data

Nowadays, more and more digital devices (such as mobile phones, navigation systems, tablets, etc.) have built-in GPS units which make it possible to determine the current

Table 1. Comparing types of mapping

	Direct	*Indirect*
Availability of geospatial component of the information	Available	Not available
Time for preprocessing	Minimal	Can be significant
Special skills of the user	Not required	Required

physical location of the device and also to record it. This means that data about the motion of the device holder are available if we can retrieve them through some tool. One of the simplest solution is to use Google Earth (GE) to import data from GPS devices through a direct connection or by importing the files themselves acquired from a device. GE is ready immediately to show the data on the virtual globe.

Geotagged photos

Digital cameras, smart phones and also computers can contain photos with information about the geographical location where they were taken. In practice this means, that at least latitude and longitude are assigned to the image, while additional information such as altitude, track, or compass bearing are only optional. It has to be mentioned that these metadata can be assigned to a picture later as well either automatically or manually. Panorado Flyer is for example a small, but powerful tool for linking geolocation to JPEG image files. If a photo is geotagged, then the details tab in the Properties window of the image contains also a GPS section (Fig. 1). Theoretically, each part of a picture could have information about its geographic location, but usually only the position of the camera is associated with the image, which makes the process of geovisualization simpler. Not only the visual content of the photos but also the geospatial information can reveal new evidences, so it is worth mapping the information.

Google has launched recently a brand new application called PlaNet that is capable of identifying the place a photo was taken even the photo is not geotagged. This very hard task can use only visual features and available textual tags, so a clear, not blurred photo is a requirement. It uses a special neural network based on a grid of approximately 26000 boxes, the team divided the world into. The test results seem convincing although the service is not yet perfect, but can be a powerful tool providing for the investigator.

Geocoding with fusion tables

Digital devices can contain several files referring to geographical locations in different forms. Information can be found in the content of documents, notes, presentations, spreadsheets, etc. and the information itself can be settlements names, names of countries, regions, buildings, organizations, geographical locations, etc. Visualization of them can also highlight important spatial relationship which otherwise remain hidden. Although in case of only a few items the visualization can be performed manually (for example with Google Maps, or Google Earth) usually the number of items is high. The geocoding of large amount of items can be performed with the help of Fusion Tables from Google. Fusion Tables is an experimental data visualization web application to gather, visualize, and share data tables coming from different sources (Zichar 2012a). Making a map takes only a minute if the data are imported into a table, and Figure 2 shows a small table with only one column Location and four rows, while Figure 3 shows the visualized point features in a map. There are many tools to make customization (icons, contents of associated bubble, creating legends, etc.), but their discussion is out of the scope of this paper. The result can be downloaded in file format csv or kml, which ensures further editing options. This free online service is definitely one of the simplest way to visualize large amount of data.

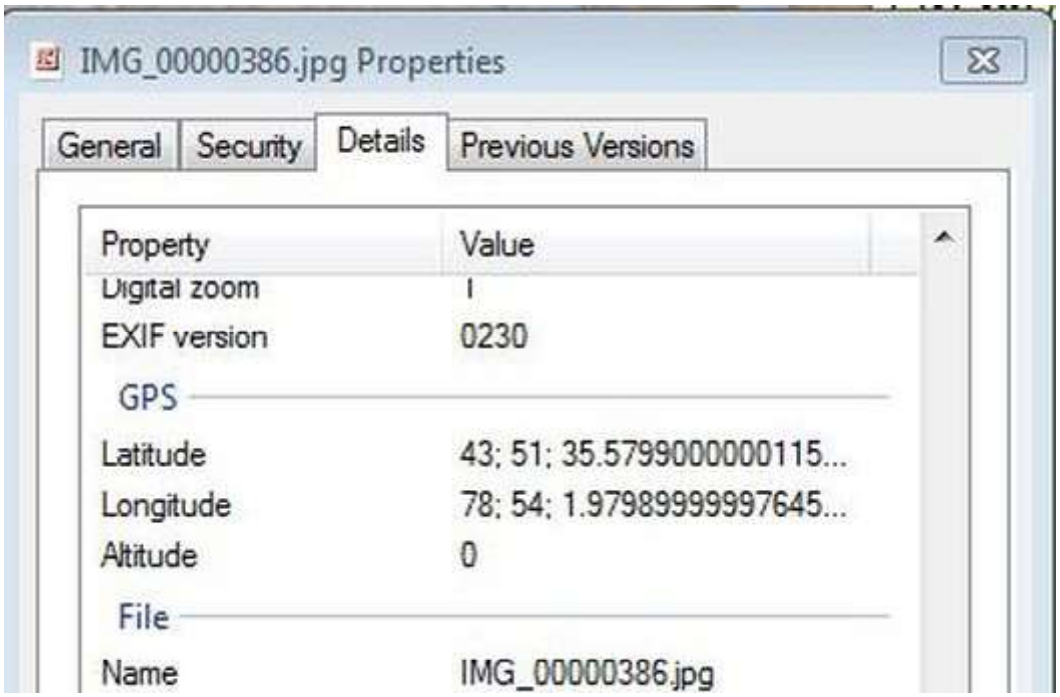


Fig. 1. Metadata of a geotagged photo in the GPS section

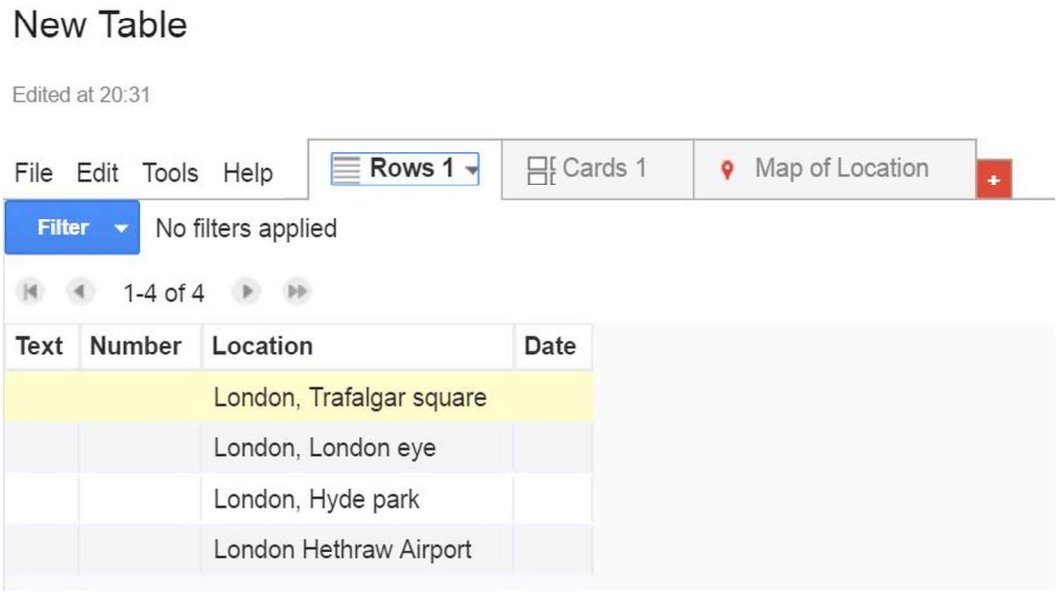


Fig. 2. Fusion table containing only location data

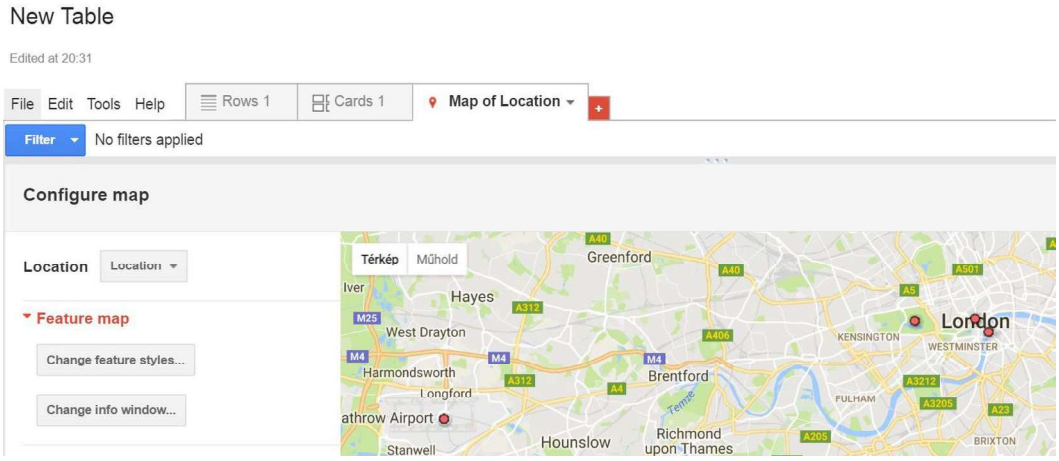


Fig. 3. Geocoded data represented in a map in Fusion Tables

Keyhole Markup Language

In case of a few item the user interface of GE can be used directly to map the information by using the Search panel. This manual method is slow, but provides opportunity to make several customization, especially if you are familiar with the KML language. KML (Keyhole Markup Language) is an XML based language that does not require strong programming skills from the user. The final map can be downloaded as a kml or kmz file and edited as well. (The last, compressed version has to be uncompressed before editing, of course.)

3. Conclusions

When studying new things we also have to know where and how this knowledge can be used later. Beyond the trivial usage, usually there are many other fields where our knowledge is welcome. Most people would not think, that their GIS skills can be applied in digital forensics. This paper gave an overview about how different forms of geovisualization can support an investigation. Nowadays, GIS courses are held for students majored in wide range of programs all over the world (e.g. Business Information Security at Ferris State University, USA; Forensics Anthropology, University of Toronto, Canada), so not only the students but also the educators can be motivated to acquire novel approaches.

4. References

Bruce, C.W. (2001): A thousand words for a picture. Is the overvaluation of GIS disrupting a critical balance in crime analysis? Massachusetts Association of Crime Analysts, Crime Analysts' Round Table

Crandall, D. – Backstrom, L. – Huttenlocher, D. – Kleinberg, J. (2009): Mapping the World's Photos. In: 18th International World Wide Web Conference, April 20.24, Madrid, 2009. pp. 761-770.

Gogolin, G. (2013): Digital Forensics Explained, Taylor & Fransics Group

Harrington, M. – Cross, M. (2015): Google Earth Forensics, Using Google Earth Geo-Location in Digital Forensic Investigations, Elsevier.

Pődör, A. (2014): Bűnügyi statisztikai adatok és a bűnözéstől való félelem összehasonlítása Kalocsa példáján, In: Térinformatikai konferencia és szakkiállítás konferencia kiadványa, Debrecen. pp. 281-287. (in Hungarian)

Pődör, A. (2016): A bűnözéstől való félelem mérése egy webalkalmazás segítségével, In: Térinformatikai konferencia és szakkiállítás konferencia kiadványa, Debrecen. pp. 395-403. (in Hungarian)

Prensky, M. (2001): "Digital Natives, Digital Immigrants Part 1". On the Horizon. 9(5):1-6.

Tompson, L. – Townsley, M. (2010): (Looking) back to the future: using space-time patterns to better predict the location of street crime. International Journal of Police Science & Management. 12(1): 23-40.

Zichar, M. (2012a): Fúziós táblák a számítási felhőben, In: Térinformatikai konferencia és szakkiállítás konferencia kiadványa, Debrecen. pp. 451-457.

Zichar, M. (2012b): Cognitive aspects of a web-based geovisualization application, In: IEEE 3rd International Conference on Cognitive Infocommunications (CogInfoCom) proceedings, 291-294.

Zichar, M. (2013): Geovizualizáció interdiszciolináris megközelítésben, In: Térinformatikai konferencia és szakkiállítás konferencia kiadványa, Debrecen, pp. 497-504.

Zichar, M. (2016): GIS support of digital forensics, In: Térinformatikai konferencia és szakkiállítás konferencia kiadványa, Debrecen, pp. 533-538.