C27 A Holistic Framework for Investigating Geospatial Data in Cyber Forensics

Mohammad M. Mirza, MS, Purdue University, Knoy Hall, Lafayette, IN 47907; Umit Karabiyik, PhD, Purdue University, Knoy Hall, Lafayette, IN 47907*

Learning Overview: After attending this presentation, attendees will be able to identify several implicit types of geospatial data/metadata formats that can be stored and recovered on different digital devices; determine the best forensics and analytics practices when it comes to dealing with geospatial data; and distinguish major geospatial concepts and qualities that can be considered beneficial and critical when conducting any digital/cyber forensics investigations.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by providing extended capabilities when investigating geospatial data considering new metadata and increasing the awareness on the importance of geospatial data analysis for investigators and first responders.

Geospatial forensics is still a relatively new trend that deals with the examination of geodata that is integrated into many digital devices (e.g., Internet of things (IoT), smart phones, wearable devices, drones, autonomous vehicles, and robotics). Geospatial data has proven to be of high importance to digital forensics investigations.[1] Recently, the National Institute of Standards and Technology (NIST) pointed out challenges related to the identification phase of digital cloud forensics, where geospatial data have been considered an important component that can assist in finding evidence.[2] However, geospatial data are not always identified directly with the latest digital forensic tools. These tools depend heavily on the use of Global Positioning System (GPS) coordinates preserved in Exchangeable Image File Format (EXIF) tags or artifacts. This poses many challenges to investigators when examining geospatial data/geolocation information, represented in different data formats/schema that are not considered necessarily explicit geospatial format (e.g., Internet Protocol (IP) addresses).

Although digital forensics tools have attempted to cope with the mentioned challenges to recover geospatial data for many years, not all geospatial data formats have been taken into consideration. Moreover, there continues to be a lack of research that combines the identification and investigation of all geospatial-related types of data into one holistic investigative framework that uses multiple geospatial data analytics techniques, including geospatial Open-Source Intelligence (OSINT) and geospatial analysis. Furthermore, it is important to demystify different methods that investigations can use to fully identify information related to geolocation from a device to aid in drawing more accurate conclusions.

This presentation will illustrate the importance of the proposed geospatial holistic investigative framework to identify various geospatial data types and suggest possible geospatial examination techniques. Moreover, as many investigations happen to have devices that store geospatial data, the proposed framework will aim to look at the issue from different perspectives (e.g., geographically, forensically, and technologically). Furthermore, the proposed work will highlight the importance of spatial thinking and spatial awareness to enhance digital forensic investigators' current capabilities. Finally, the technical experiment conducted in this work will serve as a proof of concept, which will help demonstrate the newly proposed holistic approach that defines and sets the ground of all related geospatial data into the different forensics fields.

Reference(s):

1. Goodison, Sean E., Robert C. Davis, and Brian A. Jackson. Digital Evidence and the U.S. Criminal Justice System. *RAND Corporation*, April 20, 2015. https://www.rand.org/pubs/research_reports/RR890.html.
2. Herman, Martin, Michaela Iorga, Ahsen Michael Salim, Robert Jackson, Mark Hurst, Ross Leo, Richard Lee, et al. NIST Cloud Computing Forensic Science Challenges. *CSRC*, August 25, 2020. https://csrc.nist.gov/publications/detail/nistir/8006/final.

Cyber Forensics, Geospatial Data, Geospatial Forensics

*Presenting Author