Analyzing and Visualizing of Metadata from Cloud Providers

Degree programme: Master of Science in Engineering | Vertiefung: Informations- und Kommunikationstechnologien
Thesis advisor: Prof. Dr. Emmanuel Benoist
Expert: Dr. Bruce Nikkel (UBS)

The main topic of our thesis is IT forensic related to cloud environments. In particular, we focused our attention to a variety of cloud platform providers, as we developed a software, which automatically pulls various metadata from different online profiles of a user. The aim of this software is to highlight connections and interactions between persons in the online life. This could be used in police investigations for finding new evidence and relationships between suspects.

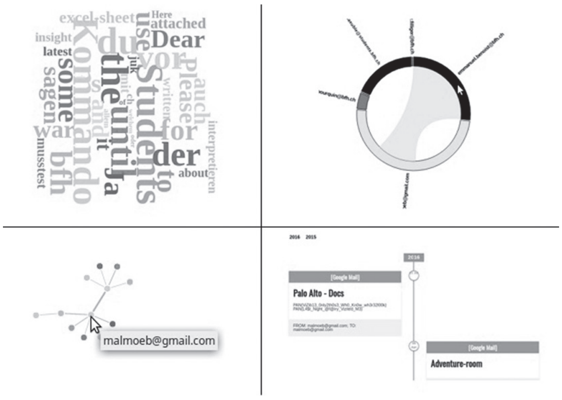
Stephan Berger

Google, Dropbox and Facebook

Cloud computing is a term which by now is not only known to a small group of computer enthusiasts, cloud computing is all around us, from storing documents on a remote server to let your friends know about your current activity. Because cloud services are ubiquitous, documents, posts and conversations stored on cloud platforms will be used more and more as evidence by police investigators in crimes that are committed in the physical world, but have been (partly) planed online. With our thesis, we developed a web-based application which can be used to help investigators during forensic analysis of metadata and files fetched from a couple of the biggest cloud service providers and social networks (Google, Dropbox and Facebook), in order to search evidence for the committed crime by the suspect.

Digital evidence that could withstand in court

IT forensic refers to the science of finding legal evidence on a digital level. According to Wikipedia: «The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.» The types of evidence involved in digital forensic covers a lot of ground, beginning by simple evidence like the browser history to more advanced types of evidence like parsing the registry to find out which software was executed on a computer. Ideally, the gathered evidence should be made «tamperproof» with a digital signature to detect forgery. Nowadays, it is not uncommon to edit office documents shared with co-workers and friends inside the browser, send e-mails, keep track of appointments and backup critical files all on the same platform (i.e. Google with its range of services). In this so-called software-as-a-service model, all the data is stored on the server-side, unlike the traditional model, which the data is stored on the client-side. This brings new challenges, but also new possibilities to an IT forensic examiner.



A selection of supported visualizations created by our software with metadata from cloud providers.

A picture is worth a thousand words

As cloud computing is not physically limited to a device or a workstation of a suspect, an investigator can pull the metadata from various online identities detached from a specific location. We implemented miscellaneous helper scripts, which connects to every cloud provider supported by our software, pulls various information about the profile in question via the API interface most cloud provider provides and store those data securely in a database. We developed also a web-based service that will make a graphical representation of the downloaded metadata. We were able to successfully download relevant metadata from well-known cloud provider like Google, Facebook and Dropbox (as a plus, files from Dropbox are saved too), and put those metadata in relationship with each other in different types of visualizations. This graphical representation can give an analyst new hints about relationships between suspects, or it can help him to strength the evidence against a suspect (because he can prove that the suspect know another suspect, according to the interconnections in a chord-diagram for example).