Social Network/Media Forensics

Social Network/Media Sites

- Social networks have become the largest and fastest growing websites on the Internet. They provide services to individuals to connect and communicate with each other based on different nature and nomenclature.
- Users can connect and communicate to each other for various purposes by creating a public or semi-public profile within the social media site.
- Users can articulate a list of other users with whom they share a connection.
- And users can view and traverse their list of connections and those made by others within the social media site.
- Therefore, sites such as Facebook or LinkedIn contain sensitive and personal data of hundreds of millions of people.

Generic Data Sources of Social Networks

- The social footprint: What is the social graph of the user? With whom is he/she connected as a “friend"?
- Communications pattern: How is the network used for communicating, what method is used, and with whom is the user communicating?
- Pictures and videos: What pictures and videos were uploaded by the user? On which other peoples pictures is he/she tagged?
- Times of activity: When is a specific user connected to the social network? When exactly did a specific activity of interest take place?
- Apps: What apps is the user using, what is their purpose, and what information can be inferred in the social context?

Challenges in Social Network Forensics

- Most or all the aforementioned information cannot be found on a suspect's hard drive, as it is solely stored at the social network operator.
- Acquiring the information stored on the social network site is not feasible, and accessing the data directly requires the cooperation of the social network operator.
- As described in the Facebook Law Enforcement Guidelines published by the Electronic Frontier Foundation, an investigator who files a data request with an operator may or may not receive all the relevant data. (Electronic Frontier Foundation, 2010)
- Another option is to use network forensic systems such as PyFlag or Xplico to capture data, however, due to their passive nature they cannot retrieve all the information.
- Therefore, social network forensics has to rely on a limited set of data sources in many cases.

Reference: Electronic Frontier Foundation. (2010). Facebook 2010 Law Enforcement Guidelines. Retrieved from: https://www.eff.org/document/facebook-2010-law-enforcement-guide

Information Retrieval From Social Media Sites

- It is possible to retrieve information about the users who visit someone's profile on Social Network Sites.
- Therefore, unlike traditional digital forensics methods which are based on the analysis of file systems, captured network traffic or log files, new approaches for extracting data from social networks or cloud services are needed.
- The data extraction methods for social networks based on custom web crawlers do not seem to be very efficient either due to several factors such as high network traffic, additional or hidden data which can be missed by crawlers, and maintainability.

Information Retrieval From Social Media Sites

- Some social media sites provide built-in applications to the site members that enables them to get information about the people who visit the member's profile.
- Other sites store log transcripts, which capture chat session information such as username and date.
- Facebook encourages its users to use Facebook Timeline as a historical archive. This feature will greatly benefit digital forensic investigations of Facebook accounts.
- The function of user data retrieval can be accomplished within a website with user incorporation of scripting languages such as Java Script or PHP.

Using Graphs to Visualize Social Network Activities for Social Network Forensics: Basic Graphs

- Social Interconnection Graph groups users into groups and visualizes the user connection to different groups/users.
- Social Interaction Graph reveals who communicated with whom on social networks.
- Complete Timeline, not only shows the activity of the member, but also the activity of all his/her friends with possible times of activity.
- Location Visualization extracts the geolocation information stored in social networks. Such information known as geotags provide the locations to forensics investigators.

Using Graphs to Visualize Social Network Activities for Social Network Forensics: Advanced Graphs

- Event tracking tracks viral scammers and other malicious applications.
- Timeline matching matches timelines of different profiles, and eventually creates an exact timeline for a complete cluster of friends or even bigger.
- Differential Snapshots allows the forensic framework to provide the functionality to not only visualize the social network data of a user, but also the functionality to visualize differences with previous images of the same user.

Investigation of Social Network Artifacts on Computers and Mobile Devices

- The investigation of artifacts left by social networking sites on computer systems is easier to analyze due to available tools and methods that assist in the extraction of such artifacts.
- The increased use of social networking applications on smartphones makes these devices a goldmine for forensic investigators.
- Surveys show that over 90% of smartphone users use social networks on their phones.
- Potential evidence can be held on these devices and recovered with the right tools and examination methods. However, forensics analysis of mobile devices is a more challenging task.

Challenges in Smartphone Investigation

- Smartphones are always active and are constantly updating data, which can cause faster loss of evidentiary data.
- Second, forensics examination tools are available for Linux-based smartphones. However, for the smart phones with closed-source operating systems, the examiners are required to use custom tools to retrieve evidence. This could be a difficult task for forensic examiners.
- In addition, smartphone vendors tend to release OS updates very often, making it hard for forensic examiners to keep up with the examination methods and tools required to forensically examine each release. The variety of proprietary hardware of smartphones is another issue faced by forensic examiners.

Is it Possible to Retrieve Social Network Artifacts from Smartphones?

- The question is whether activities performed through smartphone social networking applications are stored on the internal memory of these devices and whether these data can be recovered.
- The results of studies show that no traces of social networking activities could be recovered from BlackBerry devices.
- However, iPhones and Android phones stored a significant amount of valuable data that could be recovered and used by the forensic investigator.
- The social networking data that could be recovered from these devices are in the backup files.

Examples of Social Media Artifacts on Smartphones That Can Be Recovered

- Android Facebook user and friend data inkling contact details and profile photo uploads, created albums, pictures viewed with app, mailbox/chat messages
- Android Twitter for user and people followed: user names, posted tweets and photos, etc.
- iPhone Facebook user and friend data inkling contact details and profile, picture URLs, photo uploads, comments posted, timestamps, all previously logged in users, friends with active chat sessions
- iPhone Twitter for user and people followed: user names, profile picture, URLs, tweets posted, timestamps

References

Alastair, I., & Harjinder Singh, L. (2014). Digital Forensics to Intelligent Forensics. Retrieved from the UMGC digital library: https://doaj.org/article/77741ce91be44f9b94623b123f0d552f#?

Brian, C., & Jung, S. (2013). EVIDENCE EXAMINATION TOOLS FOR SOCIAL NETWORKS. Retrieved from the UMGC digital library: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.302.8874#?

Electronic Frontier Foundation. (2010). Facebook 2010 Law Enforcement Guidelines. Retrieved from: https://www.eff.org/document/facebook-2010-law-enforcement-guide

Markus, H., Martin, M., Manuel, L., Sebastian, S., & Gilbert, W. (2013). Social Snapshots: Digital Forensics for Online Social Networks. Retrieved from the UMGC digital library: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.368.3462#?