C25 A Comparative Analysis of Mobile Forensic Tools: Reliability and Accuracy Related to iOS® 13 Notes App Forensic Evidence Recognition and Classification

Tanvi Gandhi, BS, Purdue University, West Lafayette, IN 47906; Marcus Rogers, PhD, Purdue University, West Lafayette, IN 47907*

Learning Overview: After attending this presentation, attendees will be able to describe the limitations of current mobile forensics tools and understand the impact that changing data structures have on digital forensics.

Impact on the Forensic Science Community: Mobile forensics needs the ability to independently validate forensic tools. Most vendors do not publish error rates, accuracy, or reliability measures for their tools. As underlying data structures change when updates to Operating Systems (OSs) occur, it is vital that we be aware of errors this may introduce. This presentation will impact the forensic science community by providing a simple framework for testing certain aspects of mobile forensics tools.

Evidence in digital forensic investigations is largely acquired through tools that are responsible for the acquisition, interpretation, and presentation of data from digital devices. Thus, it is crucial that the data produced by these tools be accurate, valid, and reliable; the failure of this could lead to a false conviction or set an offender free. The *Daubert* considerations put further pressure on the necessity to measure or have the potential to measure reliability, accuracy, and error rates.[1] Moreover, it can risk the credibility and reputation of the investigator. Currently, the most commonly used tool testing platform is the National Institute of Standard's and Technology's Computer Forensics Tool Testing Program (NIST - CFTT), but according to some literature this program is limited and has proven insufficient in properly validating the required tools.[2] This lack of a standardized tool validation system was the motivation for performing a comparative study to analyze the accuracy and reliability of three popular forensic tools in their ability to adapt to the SQLite database changes in iOS® 13 devices. The overall organization of file backups in iOS® is in the form of directories which contain SQLite databases, plist files, Extensible Markup Language (XML) files, text files, and media files. In every major update of the iOS®, the way in which data (potential evidence) is stored in these files seems to change (i.e., location and structure), which poses a challenge for forensic tools that need to keep up with the changes.[3]

The focus of this presentation is to provide the results of a comparative analysis of the following tools: (1) MSAB XRY®, (2) UFED Cellebrite®, and (3) Magnet AXIOM® in their ability to read and categorize Notes stored in the Notes app in iPhones® running iOS® 13 (locally stored, not cloud based). The Notes app has three categories of notes: (1) Active Notes—These are the notes that are created and currently stored in the app; (2) Recently Deleted (Marked for Deletion)—These are notes that the user has deleted, which are moved to a separate folder called "Recently Deleted," which permanently deletes the notes in it after 30 days; and (3) Deleted Notes—These are permanently deleted notes, which do not exist in the "Recently Deleted" folder anymore.

The tools will be measured using two criteria: Reliability (the tool's ability to read the SQLite database and identify all three categories of notes) and Accuracy (the tool's ability to correctly place each note in the respective category). The results of the testing as well as suggestions for improving the tools will be discussed. The tool vendors will be provided with the results prior to the presentation.

Reference(s):

1. Grudzinskas, A.J., Jr, and Appelbaum, K.L. (1998). *General Electric Co. v. Joiner*: Lighting up the post-*Daubert* landscape? *The Journal of the American Academy of Psychiatry and the Law*, *26*(3), 497–503. https://www.ncbi.nlm.nih.gov/pubmed/9785292.
2. Hughes, N., and Varol, C. (2020, March). The Critical Need for Tool Validation before Using Malware Scanners in Digital Forensics. In *ICCWS 2020 15th International Conference on Cyber Warfare and Security* (p. 228). Academic Conferences and publishing limited.
3. Shimmi, S.S., Dorai, G., Karabiyik, U., and Aggarwal, S. (2020, June). Analysis of iOS SQLite Schema Evolution for Updating Forensic Data Extraction Tools. In *2020 8th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-7). IEEE.

iOS®, Tools, SQLite