C35 iOS® Photo Vault Forensics

Siddharth S. Chowdhury, MS, Purdue University, West Lafayette, IN 47907; Kayla Rux, Mishawaka, IN 46545; Kathryn C. Seigfried-Spellar, PhD*, Purdue University, West Lafayette, IN 47907*

Learning Overview: After attending this presentation, attendees will be aware of what artifacts may be forensically recovered from photo vault applications using iOS®.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by providing relevant information for digital forensic investigators who may need to identify and recover relevant artifacts from a vault application on the iOS®.

Modern digital devices, such as laptops, personal computers, mobile phones, and tablets, have vault apps—applications that hide photos, videos, and texts in a secure "vault."[1] These vault applications allow the user to securely store their personal data, which makes it difficult for anyone except the device's owner to view the files, even if they have access to the device.[2] These mobile vault applications often disguise themselves by pretending to look like other applications, such as a calculator, or only display information when the user enters a valid password.

From a law enforcement investigation perspective, offenders may use vault apps to hide illegal images, such as child sexual exploitation materials or illicit text messages with minors. In cases such as these, vault applications may serve as a hindrance to law enforcement. While traditional digital forensic tools may be able to recover photos directly stored on the phone, they may not be able to find those secured by photo vaults.[3]

While studies have examined vault applications on Android® operating systems, limited research exists using the iPhone® or iOS® ecosystem. The current study had four aims: determine what information can be forensically recovered from vault applications, examine implications for user privacy, document the methods for forensically extracting information from vault apps, and compare the results from different digital forensic tools. The five most popular vault applications in 2019 on the iOS® store were analyzed. Various types of photos were uploaded to the vault applications using the following techniques: creating a photo by taking a screenshot, saving a photo from a text message, saving a photo from a browser, and using the phone's camera to create the photo. This study also compared the results of various digital forensic tools (e.g., Cellebrite®, Axiom®). The results will be fully discussed and recommendations for the digital forensic examination of photo vault apps on the iOS® ecosystem will be provided.

Reference(s):

1. Newton, C. (2017, October 17). *Nude is a next-generation photo vault that uses AI to hide your sensitive photos*. Retrieved March 10, 2018, from https://www.theverge.com/.
2. Zhang, X., Baggili, I., and Breitinger, F. (2017). Breaking into the vault: Privacy, security and forensic analysis of Android vault applications. *Computers & Security*, *70*, 516-531.
3. Alghafli, K.A., Jones, A., and Martin, T.A. (2012, December). Forensics data acquisition methods for mobile phones. In *Proceedings of International Conference for Internet Technology and Secured Transactions* (pp. 265-269). IEEE. London, UK.

Photo Vault, Digital Forensics, Mobile Forensics