C14 Fortnite Forensics: A Study of How to Extract Artifacts From Android™ Memory

Justin Grover, MS, The MITRE Corporation, Mclean, VA 22102; Chris Meffert, MS*, The MITRE Corporation, McLean, VA 22102*

Learning Overview: After attending this presentation, attendees will better understand the current state of performing memory forensics on Android™ devices.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by providing techniques for researchers to more effectively perform forensic explorations of mobile applications.

The popular Fortnite application will be used as an example to explain the procedures involved with dealing with Android™ memory and the current challenges facing the community. Fortnite, due to its design and scope as a gaming application, may not result in many artifacts of forensic interest; however, the focus of this presentation is not on results but on the involved process used to derive any results. The forensic community will benefit by realizing the state of the field, how Android™ memory forensics can be applied to investigations, and how this process can be used to leverage information from other, more forensically valuable, applications of interest.

Memory forensics in recent years has become more commonplace in forensic and incident response investigations involving traditional laptops and desktops running Windows®, Mac OSX®, or Linux®. Procedures and tools are widely available on these platforms, and many investigators realize that "pulling the plug" will result in potential data losses. However, memory forensics on mobile devices is not a regular practice in current investigations. Given the widespread nature and usage of mobile devices across the world and their enormous impact on investigations, this presentation seeks to explore why memory forensics is not a common aspect of mobile device forensics.

The state of the mobile memory forensics field will be conveyed to attendees by summarizing recent research efforts, explaining hands-on experimentations with various memory extraction methods, and providing an assessment on current memory examination and analysis options within the popular analytical Volatility and Rekall frameworks.[1,2]

This presentation will also introduce attendees to Frida, a dynamic process injection (also known as "hooking") toolkit that can assist researchers and reverse engineers with performing memory analysis on mobile operating systems and their running applications.[3] This tool can be used to study artifacts that are stored in application memory or on a device's flash storage.

Finally, some brief thoughts will be offered on the state of memory forensics on the iOS® platform and why it is such a challenge for security researchers and investigators.

Reference(s):

1. https://www.volatilityfoundation.org/.
2. http://www.rekall-forensic.com/.
3. https://www.frida.re/.

Memory Forensics, Android™, Forensics