Contribution ID: **129** Type: **Oral**

Traceroute Analysis in Mobile Forensics Using AT&T Video Optimizer

Network traffic analysis represents an important element of mobile forensics that can provide an understanding of device communication patterns, application activity, and possible threats. Traceroute analysis, in particular, can determine network routes, the nodes in transition, and endpoint states, all of which can contribute critical forensic evidence. However, utilizing any model of this information, across multiple mobile applications like iPhones, rooted or locked Android devices, can be difficult because of the imbalances in system access as well as the variances in security and evidence retrieval.

In this study, we explore the capability of AT&T Video Optimizer, an open-source diagnostic tool typically used in mobile applications to analyze mobile application performance, to capture and analyze traceroute data in various device states. Based upon running test and trial environments on such distinctly different environments like iOS and Android, while being locked and rooted, we analyze the extent to which network traceroutes can be identified and analyzed for forensic collection. Our research implementation employs data collection that is non-intrusive, maintaining forensic integrity and consideration for any real-world applicability in investigative scenarios.

Consequently, the analysis is expected to demonstrate the feasibility and limitations of using the AT&T Video Optimizer as a network collector and analysis tool in mobile forensic investigations, especially in cases when traditional models were limited. This effort helps to close the gap between forensic probing and diagnostic performance tools by showing how available utilities can be diverted for digital evidence collection.

Keywords: Mobile Forensics, Network Traceroute, AT&T Video Optimizer, iOS, Android, Locked Devices, Rooted Devices

Author: YOGA, Sanjana

Co-author: Mr VENKATESH, N Vishnu

Presenter: YOGA, Sanjana

Track Classification: Forensic Sciences