QuinStreet ●●● 10400 Linn Station Road, Suite 100 ●●● Louisville, KY 40223

Using Attack Graphs in Forensic Examinations

Abstract-attack graphs are used to compute potential attack paths from a system configuration and known vulnerabilities of a system. Attack graphs can be used to determine known vulnerability sequences that were exploited to launch the attacks and help forensic examiners in identifying many potential attack paths. After an attack happens, forensic analysis, including linking evidence with attacks, helps further understand and refine the attack scenario that was launched. Given that there are anti-forensic tools that can obfuscate, minimize or eliminate attack footprints, forensic analysis becomes harder. As a solution, the authors propose to apply attack graph to forensic analysis. They do so by including anti-forensic capabilities into attack graphs, so that the missing evidence can be explained by using longer attack paths that erase potential evidence. The authors show this capability in an explicit case study involving a Database attack.

The attached zip file includes:

- Intro Page.pdf
- Terms and Conditions.pdf
- UsingAttackGraphs.pdf