8-10-2020

Measuring Computer Forensics Skill

Mike Watson
BYU, mike_watson@byu.edu

Quincy Taylor
BYU, quincy.taylor8@gmail.com

Justin Giboney
BYU, justin_giboney@byu.edu

Measuring Computer Forensics Skill

TREO Talk Paper

Mike Watson
Brigham Young University
mike_watson@byu.edu

Quincy Taylor
Brigham Young University
quincytaylor@byu.net

Justin Giboney
Brigham Young University
justin_giboney@byu.edu

Abstract

Computer forensic analysts combine their technical skills with their forensic aptitude to recover information from computers and storage devices. Most technology professionals demonstrate expertise through the acquisition of different professional certifications. Certifications, however, are not always a valid judge of skill, because certifications are formatted as written and applicable tests.

It is common for people to forget knowledge and skills when they are not routinely practiced. The same applies with technology certifications. One must practice the skills learned for the certification test consistently in order to convert them to long-term memory. "Cognitive processes play a prominent role in the acquisition and retention of new behavior patterns" (Bandura 1977, p. 192). As a skill is practiced, it is better retained.

Due to the current inability to accurately measure an individual's skills and understanding of computer forensics principles, this research will investigate how to measure proficiency amongst professionals and novices. Recent research utilized conceptual expertise within the context of computer security (Giboney et al. 2016). This study utilized a technique to quickly measure the difference between novices and experts. Following their guidelines, we propose to do the same for computer forensics expertise with the following research question:

What knowledge, skills and abilities are needed to be demonstrated in a measure to assess computer forensics expertise?

Conceptual expertise is the understanding about the theoretical concepts and their relationship in a topic area. The SEAM process (Giboney et al. 2016) aims to gauge the practical application of situations to the goal wherein experts can show their conceptual expertise. The conceptual expertise task is based on the idea that those who have surface level knowledge will group scenarios by surface features while experts will be able to group the same scenarios by deep features (Giboney et al. 2016).

The assessment has been designed to measure the understanding of basic computer forensics processes. It consists of twenty-five situations created to highlight different stages of the digital forensic process. These situations focus on a gender-neutral individual, Jordan and the tasks they perform given certain parameters. Survey takers will group the situations by stage of forensics or by what crime the task is involved with. We will show that the assessment can accurately determine an individual's understanding of computer forensics. When this is shown, this assessment could be used in a variety of ways including initial assessments of job candidates and pre- and post- tests for computer forensic classes.

References

Bandura, A. 1977. "Self-Efficacy: Toward a Unifying Theory of Behavioral Change," *Psychological Review* (84:2), pp. 191–215. (https://doi.org/10.1037//0033-295X.84.2.191).

Giboney, J. S., Proudfoot, J. G., Goel, S., and Valacich, J. S. 2016. "The Security Expertise Assessment Measure (SEAM): Developing a Scale for Hacker Expertise," *Computers & Security* (60), Elsevier Ltd, pp. 37–51. (https://doi.org/10.1016/j.cose.2016.04.001).