Contribution ID: **124**   Type: **Talk**

MQFIP: Towards a Digital Forensic Investigation Process of a Compromised MySQL Database

Thursday, 1 December 2022 10:55 (20 minutes)

Database forensics, is a branch of digital forensic science that allows forensic examination of databases to be conducted by following normal digital investigation, processes. Regardless, while conducting investigation processes on databases, the aim is always directed towards the extraction of Potential Digital Evidence (PDE) in a forensically sound manner. More often than not, forensic investigations on databases targets data in a database, the metadata and this data may at different instances contain important facts that can be used to prove or disprove facts in a court of law during criminal or civil proceedings. Normally, the metadata forensically presents a technique that determines how the digital data that is extracted from the databases can be interpreted. The main problem that is being addressed in this paper is how a digital forensic investigation process can be applied to a compromised MySQL database. The research has achieved this by simulating attack scenarios, reconstructing MySQL database and conducting MySQL Forensic Investigation Process (MqFIP) and the findings have been extrapolated well.

Key words: Database forensics, Database management system, Forensic configuration, Database, MySQL, MySQL forensic investigation process

Primary author: HUNGWE, Taurai (Sefako Makgatho Health Sciences University)

Presenter: HUNGWE, Taurai (Sefako Makgatho Health Sciences University)

Session Classification: DIRISA

Track Classification: DIRISA