Cryptocurrency Forensics: Analysis on Bitcoin E-Wallet from Computer Source Evidence

Authors : Muhammad Nooraiman bin Noorashid, Mohd Sharizuan bin Mohd Omar, Mohd Zabri Adil bin Talib, Aswami Fadillah bin Mohd Ariffin

Abstract : Nowadays cryptocurrency has become a global phenomenon known to most people. People using this alternative digital money to do a transaction in many ways (e.g. Used for online shopping, wealth management, and fundraising). However, this digital asset also widely used in criminal activities since its use decentralized control as opposed to centralized electronic money and central banking systems and this makes a user, who used this currency invisible. The high-value exchange of these digital currencies also has been a target to criminal activities. The cryptocurrency crimes have become a challenge for the law enforcement to analyze and to proof the evidence as criminal devices. In this paper, our focus is more on bitcoin cryptocurrency and the possible artifacts that can be obtained from the different type of digital wallet, which is software and browser-based application. The process memory and physical hard disk are examined with the aims of identifying and recovering potential digital evidence. The stage of data acquisition divided by three states which are the initial creation of the wallet, transaction that consists transfer and receiving a coin and the last state is after the wallet is being deleted. Findings from this study suggest that both data from software and browser type of wallet process memory is a valuable source of evidence, and many of the artifacts found in process memory are also available from the application and wallet files on the client computer storage.

Keywords : cryptocurrency, bitcoin, digital wallet, digital forensics

Conference Title : ICLDF 2018 : International Conference on Law and Digital Forensics

Conference Location : Osaka, Japan

Conference Dates : October 11-12, 2018