Ebru Celikel Cankaya et al., J Forensic Res 2017, 8:4 (Suppl)
DOI: 10.4172/2157-7145-C1-023

A survey of network security tools from a forensics perspective

Ebru Celikel Cankaya and **Christopher Lopez-Araiza**
University of Texas, USA

In an effort to establish a standard for responsive networking systems, we provide a survey of available tools and their applications for network forensics, as well as discuss the accessibility of these solutions to implement. Our paper investigates four network security tools in detail: Fail2ban, Netdata, Nmap, and HoneyDrive3 to test run on experimental setup. We compare these tools with respect to 7 fundamental forensics criteria as logging, automated threat response, active monitoring, capability to prevent attack, malicious activity detection, notification of malicious activity, and security auditing. The results of these experiments are compared for further evaluation. We rank results based on the percentage of coverage for the full set of 7 forensics criteria. We also emphasize how the utilization of the relevant solutions could have aided in mitigating past threats.

Biography

Ebru Celikel Cankaya, PhD has her expertise in the general area of computer security. She has been working on ways to improve lossless compression of text, as well as implementing novel cryptographic algorithms by bringing together some known algorithms together to exploit their individual benefits. Dr. Cankaya has been teaching at University of Texas at Dallas and has been nominated/ recipient of several teaching awards.

exc067000@utdallas.edu

Notes: