THE JOURNAL OF
DIGITAL FORENSICS,
SECURITY AND LAW

Journal of Digital Forensics,
Security and Law

Volume 10 | Number 1 Article 1

2015

From the Editor-in-Chief

Ibrahim Baggili
JDFSL

Recommended Citation

Baggili, Ibrahim (2015) "From the Editor-in-Chief," *Journal of Digital Forensics, Security and Law*: Vol. 10 : No. 1 , Article 1.
DOI: https://doi.org/10.15394/jdfsl.2015.1194
Available at: https://commons.erau.edu/jdfsl/vol10/iss1/1

FROM THE EDITOR-IN-CHIEF

Welcome to JDFSL's first issue for 2015! First, I would like to thank our editorial board, reviewers, and the JDFSL team for bringing this issue to life.

It has been a big year for JDFSL as the journal continues to progress. We are continuing our indexing efforts for the journal and we are getting closer with some of the major databases.

In this issue, we continue our multidisciplinary tradition. The first paper *A survey of botnet detection techniques by command and control infrastructure*, the authors reviewed the history of botnets and botnet detection techniques illustrating that traditional techniques are passive, relying on honeypots, which are not effective at detecting peer-to-peer and decentralized botnets even though recent work has illustrated that hierarchical clustering of data flow and the use of machine learning are effective in detecting botnet peer-to-peer traffic.

In the second paper *Data loss prevention and control: Inside activity incident monitoring, identification, and tracking in healthcare enterprise environments*, the authors discuss the timely issue of healthcare data security in enterprise environments. The authors provide a novel approach to model internal threats, especially insider activities. They then investigated threat vectors and potential data loss paths in healthcare enterprise environments where vectors are enumerated and data loss statistics for some threat vectors were collected. They then disclosed a method to provide guidance for inside activity identification, tracking and reconstruction using evidence trees.

In the third paper *To license or not to license reexamined: An updated report on state statues regarding private investigators and digital examiners*, the authors provided an update to their work in 2012 where they examined statues that regulate, license, and enforce investigative functions in each U.S. state. Their results indicated that few state statues explicitly differentiate between Private Investigators (PI) and Digital Examiners (DE). There seems to also be a growing trend in which some states are changing definitions or moving to exempt DEs from PI licensing requirements.

The fourth paper *Litigation holds: Past, a present and future direction* discusses litigation hold challenges with electronically stored information. The author points out that litigation holds best practices were created to prevent routine destruction of documents and to preserve documents relevant to a litigation hold. The author further explains that for the first seven years of the new e-discovery rules, litigants who failed to preserve data received severe sanctions for spoliation of evidence and that recent cases and proposed new rules have reversed the trend of stringent standards requiring litigation holds. The author argues that this has challenged the state of the law in spite of the fact that accepted best practices do recommend high standards for litigation holds.

Finally, we are extremely proud of the multidisciplinary nature of this issue once more, spanning Digital Forensics, Security and Law. We will continue on this path as we move forward because it is our core belief at JDFSL that our domain is multidisciplinary and that impactful research should tackle cyber issues from different perspectives.

Sincerely,

Dr. Ibrahim Baggili PhD Editor-in-Chief