Journal of Cyber Forensics and Advanced Threat Investigations

CFATI OPEN ACCESS

Volume 1(1-3), 1-2. https://doi.org/10.46386/ijcfati.v1i1-3.26

Editorial: Inaugural Issue of the *IJ*CFATI

John William Walker[1]

Abstract

This article introduces the inaugural issue for the *International Journal of Cyber Forensics and Advanced Threat Investigations*. The article outlines the journal's aims and scope and summarizes the articles published in the issue.

Keywords

cybersecurity, digital forensics, incident response, threat investigations.

Submitted: 15/02/2021— **Accepted: 15**/02/2021 — **Published: 15**/02/2021

Corresponding author [1] Address: School of Science & Technology,Nottingham Trent University, 50 Shakespeare St, Nottingham NG1 4FQ

Editorial

Well, here we are in the midst of a pandemic as a backdrop for the inaugural launch of this brand new publication, the ***'International Journal of Cyber Forensics and Advanced Threat Investigations'*** or *IJ*CFATI for short, a publication crafted out by the leadership of visionaries at the association of cyber forensics and threat investigators, the industrial cybersecurity center, and the University of South Wales. On a personal note I must add that I am deeply honoured to have been offered the position of Editor in Chief of this exciting future focused publication. The *IJ*CFATI is the outcome of the dedication of various professionals and academics who are selflessly willing to invest in long hours of work with the goal of giving back to the DFIR and cybersecurity communities. We highly appreciated those who have completed the initial editorial and reviewing works and those who will follow after.

I am guessing that one initial thought of potential subscribers may be, is there room for yet another publication covering the diverse subject of cyber and investigations in an already crowded marketplace? - the answer is a resounding yes. To ensure that *IJ*CFATI fills an open gap in the cyber publication's arena, it is aiming high to be recognised as a fresh and leading resource in its field. To this end, the team have set some very clear and forward thinking objectives, and so *IJ*CFATI will aim to provide its readers with a balance of insightful information from the world of research and academia, which will be complimented by recognised international disciplined expertise, examples of which are:

CSIRT (Computer Security Incident Response Teams)
Digital Forensics
OSINT (Open Source Intelligence)
Data Analytics
Cyber Crimes
Advanced Threat Analysis
Artificial intelligence
Cyber Defence
Cyber Security Operations

The aforementioned representing but a sample of topics from which we will produce value add, pragmatic articles to provision our readership with the most up-to-data accurate, quality information and resources of the time within this specialised field of cyber-sciences.

We, like most professionals also recognise that the area of implied urgent need for a robust Incident Response capability (IRc) to be established within the organisation is now possibly one of the most demanding and important capabilities the internal security team should possess - an observation which is further driven home by the current 30% rise, above the norm of cyber-attacks during this time of the coronavirus pandemic in which a robust IRc should be recognised as a must have dimension to be added to the companies security posture.

The *IJ*CFATI has an impressive opening in the first issue. The published articles depict various studies that can advance our understanding of cyber forensics and threat investigations when considered in a forum. The issue consists of five papers briefly introduced in the following paragraphs.

In the first article, a comparative and objective analysis has been carried out, showing the impact of executing some memory capture tools on the system. This comparative study provides details of both the private and shared workspaces, for each of the processes executed by each of the tools used. The objective of this article is to provide insights related to choosing the right tool, and the impact this tool has on the RAM of the system. The article also contains key information for the resolution of such a case and the kind of information that will be lost if the right tool is not used properly.

In the second article, comprehensive security and forensic analysis were conducted to contribute to the security enhancement of selected IoT devices and the assisting the current IoT forensics approaches. The presented approach follows several techniques such as forensic analysis of identifiable information, including connected devices and sensor data. Furthermore, a security assessment was performed to explore insecure communication protocols, plain text credentials, and sensitive information. This includes reverse engineering some binary files and manual analysis techniques. The presented analysis includes a data-set of home automation devices provided by the VTO labs: (1) the eufy floodlight camera, and (2) the Kasa smart light bulb. The main goal of the technical experiment in this research is to support the proposed model, that can be applied to other IoT devices. Moreover, The presented model concentrates on non-traditional techniques, and all phases of the model were supported by the conducted technical experiment.

In the third article, the technical background related to "how deleted content can be made visible again in an SQLite-database" was examined by presenting some techniques for carving and acquisition of deleted data in SQLite databases. Besides an algorithm for the recovery of deleted data pages, a novel heuristic for detecting deleted records on a binary level within the database's slack areas was introduced. As proof of concept, an open-source application named FQLite was presented, which implements all proposed techniques. The search quality, as well as the performance of the program, is tested using the standard forensic corpus. The results of a performance study are discussed, as well. The benchmark scope has proved that the program can handle almost all pitfalls of the SQLite data format. In particular, FQLite performs better in this field than many other forensic solutions currently on the market. It could achieve the highest recovery rate within our test.

In the fourth article, a Hot Spot Note introduces the importance of process during the investigation and the acquisition phases of logical/physical artifacts which may be required during the course of such professional engagement. The article then focuses on the necessity to have a robust supportive framework in a state of preparedness to facilitate the First Responders and CSIRT (Computer Security Incident Response Team) with the necessary underpin to support such investigative engagements – considering effective and pragmatic Policies, Case Management, operational Security Protocols (Run-Books) and all other necessary attributes to underpin a professional, prepared posture from which a team may effectively, and robustly engage an investigation/incident.

In the fifth article, a Hot Spot Note looks to outline the threats of the current age of 2020 posed by Ransomware attacks and focuses on how the overlooked SME and Individuals may secure their most precious data object, and their business with affordable, simplistic tools and practices.

In this, and future issues of *IJ*CFATI we will be covering the emergence of investigative techniques and methodologies, the latest tool-sets and applications, and where we are able the team at *IJ*CFATI intend to provision our readership with real-time, pragmatic offers and takeaways to assist them in creation, maintenance and enhancement of their IRc.

So welcome to this new *IJ*CFATI publication which we hope will become a **must-have** publication for every Cyber Professional and Incident Responder to get their hands on. So, without further commentary from me, please turn the page and enjoy the ride in the world of Threats, Investigations and every discipline in between.

Declaration of Conflicting Interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) declared no financial support for the research, authorship, and/or publication of this article.

Acknowledgments

To the DFIR and cybersecurity communities.