2nd International Workshop on Cyber Forensics and Threat Investigations Challenges

October 10-11, 2022, Taking Place Virtually from the UK
https://easychair.org/cfp/CFTIC2022

Cyber forensics and threat investigations has rapidly emerged as a new field of research to provide the key elements for maintaining security, reliability, and trustworthiness of the next generation of emerging technologies such as the internet of things, cyber-physical systems, cloud/edge/fog computing, software-defined network, and network function virtualization. Complicated efforts are required in suitable and timely manners against any threats detected within these systems. Moreover, new frameworks are required to collect and preserve potential evidential data in suitable and timely manners as well. To guarantee proper cyber-defenses and strategies against the expanding landscape of criminal activities as well as rapidly advancing emerging technologies.

The main motivation for this Workshop is to bring together researchers and practitioners working on cyber forensics and threat investigations for emerging infrastructures to disseminate current research issues and advances. Original technical papers describing new, state-of-the-art research, will be considered. The Workshop welcomes submissions that evaluate existing research results by reproducing experiments. The aim of this workshop is to provide insight for the discussion of the major research challenges and achievements on various topics of interest.

Important Dates

Technical Paper Submission Deadline: 15 September 2022

Poster and Demo Track Submission Deadline: 20 September 2022

Authors Notifications: 30 September 2022

Camera Ready due: 05 October 2022

The registration is free-off-charge for All members of the Association
(Thanks to our financial supporters who made this possible)

Scope of The Workshop

Technical Paper Track

Papers on practical as well as theoretical topics and problems in various topics related to cyber forensics and threat investigations are invited, with special emphasis on novel techniques and tools to collect data from networked systems and services in emerging technologies (such as the ones can be found in cyber-physical systems and Internet of things, cloud/edge/fog computing, software-defined network, and network function virtualization). Topics include (but are not limited to):

- Forensics and threat investigations in IoT
- Forensics and threat investigations in peer-to-peer, and social networks
- Forensics and threat investigations in SDN/NFV
- Forensics and threat investigations in Cloud Computing

- Forensics and threat investigations in Smart Technologies Systems (Smart Cars, Smart Homes, Smart Cities)
- Dark Web Investigations, Forensics, and Monitoring
- Forensics and threat investigations in Virtual private networks
- Security and Privacy in Clouds, Fog Computing, and 5G, and 6G
- Security and Privacy in IoT, SDN/NFV, and Edge Computing
- Security and Privacy in Smart Technologies Systems (Smart Cars, Smart Homes, Smart Cities)
- Forensics and visualization of Big Data
- Trusted Computing in Smart Technologies Systems (Smart Cars, Smart Homes, Smart Cities)
- Tools and services for cyber forensics and threat investigations
- OSINT (Open Source Intelligence)
- Cooperative and distributed forensics and threat investigations
- Advanced threat investigations, forensic and anti-forensic techniques
- Attack detection, traceback and attribution in Emerging Technologies
- Malware Analysis and Attribution
- Digital Evidence Extraction/Analysis using Artificial intelligence, Machine Learning and Data Mining
- Data exfiltration techniques from networked devices and services (e.g. cyber-physical systems, and Internet-of-Things)
- Methods for reconstruction of Digital Evidence in Emerging Technologies
- Forensics and threat investigations in E-health/M-health
- Vulnerability & threat detection and mitigation techniques for networked services
- Novel large-scale investigations and Machine Learning techniques to analyze intelligence data sets and logs

We also encourage contributions describing innovative work in the realm of cybersecurity, cyber defense, and digital crimes.

Poster and Demo Track

CFTIC 2022 solicits the submission of posters and demos on specific aspects of cyber forensics and threat investigations, particularly related to the subject areas indicated by the CFTIC 2022 topics of interest. Posters provide a forum for authors to present their work in an informal and interactive setting. They allow authors and interested participants to engage in discussions about their work. In particular, a poster submission should motivate its relevance to the communities of cyber forensics and threat investigations, and summarize the main challenges, experiences, and novel ideas. A demonstration should present an existing tool or research prototype. Authors are expected to provide a demonstration during the poster and demonstration session. A demonstration submission should clearly describe the motivation, the novelty of the contribution, and the applicability of the tool or prototype to specific use cases. Posters or demonstrations can be submitted for evaluation in the form of an extended abstract. Submissions are limited to 1 page including references. All submissions must present only original and unpublished work that is not currently under review at any other venue. Demonstrations must include in the abstract of the paper a link to a video of up to 5 minutes hosted in a permanent location. The video must show the existing tool or research prototype in action. Moreover, demonstrations are encouraged to include a link to a website where the source code of the produced software is available when it is possible.

Submission

Paper submissions must present original research or experiences. Late-breaking advances and work-in-progress reports from ongoing research are also encouraged. Only original papers that have not been published or submitted for publication elsewhere can be submitted. Also, extended versions of conference or workshop papers that are already published may be considered as long as the additional contribution is at least 30% new content from the original. Each submission must be written in English, accompanied by a 75 to 200-word abstract, and a list of up to 5 keywords. There is a length limitation of 4 pages (at least 10pt font, one-column format) for extended abstracts including (title, abstract, figures, tables, and references). Submissions must be in ECEASST-CFTIC 2022 template. Authors should submit their papers electronically via the EasyChair online submission system.

- ECEASST-CFTIC-Latex-Template
- ECEASST-CFTIC-Word-Template

The submission processes will be managed by easychair If you have used this system before, you can use the same username and password. If this is your first time using EasyChair, you will need to register for an account by clicking the "I have no EasyChair account" button. Upon completion of registration, you will get a notification email from the system and you are ready for submitting your paper. You can upload and re-upload the paper to the system.

Publication

CFTIC 2022 proceedings are to be published open access via the Electronic Communications of the EASST Journal (ECEASST) indexed in **Scopus**, **DBLP,** and listed in the **Directory of Open Access Journals (DOAJ)**. Selected papers presented at the workshop, after further revision, will have the opportunity to be published in special issues in indexed and/or high-impact factor journals (details on the website).

Main Contact

If you have any further questions please contact the workshop organizers via https://www.acfti.org/contact

This Workshop is Technically Supported by

Association of Cyber Forensics and Threat Investigators (www.acfti.org)

Industrial Cybersecurity Center (www.cci-es.org)

Send by Andrew Zayin on Behalf of CFTIC2022 PC Chairs.

Andrew Zayin Ph.D, CISSP, CISM, CRISC, CDPSE, PMP

Association of Cyber Forensics and Threat Investigators
https://www.acfti.org
Twitter: @acfti