

IEEE International Workshop on Cyber Forensics, Security, and E-discover (CFSE 2021)

In conjunction with the 21st IEEE International Conference on Software Quality, Reliability, and Security

Hainan Island, China, Dec. 6 - 10, 2021

<https://qrs21.techconf.org/track/workshops/cfse>

Description

To battle with cybercrimes, investigate online financial frauds, and mediate personal digital property disputes, cyber forensics, security, and e-discovery professionals and researchers are always working hand in hand. Due to the nature of the cyberspace, these three fields are built on the same digital foundation that provides numerous similarities in law practice, legal procedures, investigation strategies, evidence handling, research methodologies, implementation platforms, and application tools.

The theme of this workshop is to advance the research in the conjunction of Cyber Forensics, Security, and E-discovery with a data-intelligent-driven, legal-proceedings-enforced, and innovative-interdisciplinary-promoted approach. While a digital forensic professional needs to work on security or join a team for mediating a digital property from time to time, a researcher in digital forensics should also think about the impact of their work on security and e-discovery. This is also true to the professionals and researchers who are working on the fields of security and e-discovery. Therefore, we are intended to establish a forum where all the researchers and practitioners in these three fields can share their latest findings and experience while have a chance to learn what is happening in these sister-fields. Not only do they ask questions and discuss their concerns to others presentations, they also have the opportunities to hear what are the concerns and impact of their research on these sister fields. As the technology keeps its unthinkable pace of advance, everything seems to become closer and similar to each other. We believe that the effort made by this workshop will promote the collaboration among these three fields and enrich as well as expand their research and practice.

Topics

The list of topics includes, but is not limited to:

- Augmented and Virtual Reality Forensics and Security
- Blockchain Technology in Cyber Forensics, Cybersecurity, and E-discovery
- Cloud Forensics / Fog Forensics, Security, and E-discovery
- Cyber Defense/Offense/Operation
- Cyber Physical Systems (CPS) Forensics and Security
- Curriculum Development in Digital Forensics, Cybersecurity, and E-discovery
- Data-Driven Cybersecurity, Incident Response, and E-discovery
- Electronic Discovery and Fraud Detection/Investigation
- Forensic Testing / Cyber Crime Simulation
- Game / Virtual World Forensics

Image Forensics / Information Hiding Technology
IoT (Internet of Things) Forensics, Security, and E-discovery
Legal, Ethical, and Privacy Issues in Computing
Malware and Intrusion Detection and Penetration Testing
Quantum Computing Forensics/Next Generation Forensics
Risk Analysis in Security, Safety, Privacy, and Forensics Applications
SCADA / Critical Infrastructures Forensics
Social Networking Forensics, Security, and E-discovery
Software Application Forensics/E-discovery (Medical, Financial, and Governmental)
Software Forensics and Profiling
System Software Forensics and Security
Ubiquitous/Mobile/iPhone Forensic Computing and Cybersecurity
Visualization of Computer/Digital Forensics, Security, and E-discovery

Paper submission:

Authors are invited to submit original unpublished *research papers* as well as *industrial practice papers*. Simultaneous submissions to other conferences are not permitted. Detailed instructions for electronic paper submission, panel proposals, and review process can be found at <https://qrs21.techconf.org/submission>.

The length of a camera ready paper will be limited to eight pages. Each paper should include a title, the name and affiliation of each author, a 150-word abstract, and up to 6 keywords. Shorter version papers (up to four pages) are also allowed.

All papers must conform to the [QRS Conference Proceedings Format](#) and Submission Guideline set in advance by QRS 2021 co-located workshops. At least one of the authors of each accepted paper is required to pay full registration fee and present the paper at the workshop. Arrangements are being made to publish selected accepted papers in reputable journals. Submissions must be in PDF format and uploaded to the conference submission site.

Program Chairs

Ryoichi Sasaki
Tokyo Denki University, Tokyo, Japan
r.sasaki@mail.dendai.ac.jp

Tetsutaro Uehara
Ritsumeikan University, Kyoto, Japan
uehara@cs.ritsumeai.ac.jp

Jigang Liu
Metropolitan State University, St. Paul, MN, USA
jigang.liu@metrostate.edu

Program Committee:

Yuki Ashino, NEC, Japan
Francis Avorgbedor, Metropolitan State University, USA
Vinod Bhattathiripad, G J Software Forensics, India
Farris Hassan, Minnesota IT Services, USA
Satoshi Kai, Hitachi Ltd., Japan
Anyi, Liu, Oakland University, USA
Dan Lo, Kennesaw State University, USA
Masakatsu Nishigaki, Shizuoka University, Japan
Mathew Nyamagwa, Metropolitan State University, USA
Sean Thorpe, University of Technology, Jamaica
Michael Tu, Purdue University Calumet, USA
Ben Turnbull, Defense Science and Technology, Australia
Shiuh-Jeng Wang, Central Police University, Taiwan
S. M. Yiu, the University of Hong Kong, China
Hiroshi Yoshiura, The University of Electro-Comm., Japan
Yanjun Zuo, University of North Dakota, USA