The ADFSL Conference on Digital Forensics, Security and Law is the official annual conference of the ADFSL, the Association of Digital Forensics Security and Law. The Conference is a unique and innovative event organized and managed by the Association of Digital Forensics, Security and Law (ADFSL). The first annual conference of the ADFSL Conference on Digital Forensics, Security and Law was held in Las Vegas, Nevada, USA on April 20-21, 2006. The conference was created on the premise that digital forensics goes beyond digital evidence. The mission of the conference is to significantly expand the domain of digital forensics research to a wide and eclectic audience of academics, consultants and executives who are involved in the curriculum, research and use of digital forensics.

The next ADFSL Conference on Digital Forensics, Security and Law will be held at The University of Texas at San Antonio, San Antonio, TX from May 17 to 18, 2018 (see http://commons.erau.edu/adfsl/2018/).

The conference focuses on the current and expanding role of digital forensics within investigations and the courts as well as its important role within cyber security - both national as well as corporate. Topics not only include technology and evidence, but also are very much focused on how to prepare students for careers in digital forensics.

INFORMATION TECHNOLOGY - Digital forensics and information technology - Cyber law and information technology - Information security and information technology - Accounting digital forensics information technology	INTERNATIONAL ISSUES - International issues in digital forensics - International issues in cyber law - International issues in information security - International issues in accounting digital forensics	CURRICULUM - Digital forensics curriculum - Cyber law curriculum - Information security curriculum - Accounting digital forensics curriculum
NETWORKS AND THE INTERNET - Digital forensics and the Internet - Cyber law and the Internet - Information security and Internet - Digital forensics accounting and the Internet	THEORY - Theory development in digital forensics - Theory development in information security - Methodologies for digital forensic research - Analysis techniques for digital forensic and information security research	TEACHING METHODS - Digital forensics teaching methods - Cyber law teaching methods - Information security teaching methods - Accounting digital forensics teaching methods
ANTI-FORENSICS AND COUNTER ANTI-FORENSICS - Steganography - Stylometrics and author attribution - Anonymity and proxies - Encryption and decryption	PRIVACY ISSUES - Privacy issues in digital forensics - Privacy issues in information security - Privacy issues in cyber law	CASES - Digital forensics case studies - Cyber law case studies - Information security case studies - Accounting digital forensics case studies
SOFTWARE FORENSICS - Software piracy investigation	NATIONAL SECURITY AND CYBERCRIME	

- Software quality forensics	- Cyber culture - Cyber terrorism - Cyber war - Cybercrime	

DEADLINES

- January 15, 2018 Submission Due
- February 15, 2018 Reviews Completed
- March 1, 2018 Acceptance Decisions
- April 1, 2018 Camera Ready Submission
- May 17-18, 2018 Conference

SUBMISSION TYPES

- Research papers: A research question or an argument is posed and subsequently conducted. Empirical work (quantitative or qualitative) is necessary. Research papers will be presented by the authors in a regular conference session. These papers should be extensive. Typical length is about 5000-6000 words. All research papers will be considered for publication in the Journal of Digital Forensics, Security and Law (JDFSL).
- Short briefing papers: A technology or a management briefing on an aspect of digital forensics, information security, and/or cyber law. Such papers will be presented by the author in a round table discussion format at the conference. These papers need not be extensive. Typical length is about 1500-2000 words.
- Case Studies: Case studies are typically descriptions of a given digital forensics situation. Names of organizations/actors can be kept anonymous to maintain confidentiality. Case studies will be presented by the authors at the conference. Typical length is about 5000-6000 words. All case studies will be considered for publication in the Journal of Digital Forensics, Security and Law (JDFSL).
- Student Scholar Track: Up to six student papers will be selected for the Student Scholar Track. Of the six papers, one will be selected for the Student Scholar Award. The primary author must be present at the conference. To participate, the primary author of the paper must be a student. The primary author must email the conference chair and specify that they wish their submitted paper to be considered for the Student Scholar track.
- Panels: Panels and workshop proposals are welcome. Typical length is about 1000 words long and covers a current technology or a controversial issue.

All research papers and case studies are double blind peer reviewed.

Instructions for authors may be found at http://commons.erau.edu/adfsl/2018/ , and the Conference Submission System may be found at http://commons.erau.edu/cgi/ir_submit.cgi?context=adfsl

BEST PAPERS

Selected papers from the conference will be considered for inclusion in a special issue of Journal of Digital Forensics, Security and Law.

PARTICIPANTS

The conference is of particular interest to individuals who are interested in developing curriculum and teaching methods as well as conducting research related to the areas of digital forensics, security, and law. This conference will be of value to both academic and practitioner audiences.

Conference General Chairs	**Program Chair**
Dr. David Dampier The University of Texas at San Antonio, Texas, USA david.dampier@utsa.edu Dr. Nicole Beebe The University of Texas at San Antonio, Texas, USA nicole.beebe@utsa.edu	Dr. Kim-Kwang Raymond Choo The University of Texas at San Antonio, Texas, USA raymond.choo@fulbrightmail.org https://sites.google.com/site/raymondchooau/