6th International Conference on

DIGITAL FORENSICS & CYBER CRIME

ICDF2C
Digital Forensics & Cyber Crime

CO-HOSTED WITH THE

Systematic Approaches to Digital Forensic Engineering (SADFE)

TECHNICAL PROGRAMME

OMNI Hotel @ Yale

NEW HAVEN, Connecticut, United States

18-20 September 2014

ORGANIZED BY:

University of New Haven
TAGLIATELA COLLEGE OF ENGINEERING

TAKE A BYTE OUT OF CRIME
www.UNHcFREG.com

EAI European Alliance for Innovation

SPONSORS:

MICRO SYSTEMATION

Gold Sponsor

cellebrite
delivering mobile expertise

Silver Sponsor

JONES & BARTLETT LEARNING
An Ascend Learning Company

Reception Sponsor

HTCIA
HIGH TECHNOLOGY CRIME INVESTIGATION ASSOCIATION
CONNECTICUT CHAPTER

Exhibition Sponsor

JDFSL
The Journal of Digital Forensics, Security and Law

DIGITAL FORENSICS ADFSL SECURITY LAW

Media Partners

CREATE-NET

Technical Sponsors

WELCOME TO ICDF2C 2014!

Dear Delegates,

It is an honor to co-chair two of the most world-renowned conferences in cyber forensics on the same day. We are very excited to host the 2014 conference in New Haven, CT, and we are especially excited about the quality of this year's proceedings.

First, we had a very competitive conference acceptance rate this year. Overall, fifty-three papers were submitted and only seventeen were accepted. This makes this year's acceptance rate 32%. Second, we are excited that this year's proceedings will be published in the peer-reviewed, open access Journal of Digital Forensics, Security and Law (JDFSL). We are also proud of the truly international nature of this year's conference. We have people joining us from fourteen countries and eight US states.

It is important to thank everyone that helped support this year's conference. Firstly, I would like to thank our sponsors MicroSystemation, Cellebrite, Jones & Bartlett Learning and the Connecticut Chapter of HTCIA.

I would also like to thank the European Alliance for Innovation (EAI) and especially its president Imrich Chlamtac and Petra Jansen for working very hard to make sure the event is in order.

I want to also thank a number of colleagues at the University of New Haven for their support: Ron Harichandran – Dean of the college of Engineering, Ali Golbazi – Chair of the ECECS department, the ever famous Dr. Henry Lee for his support and Keynote address, President Steve Kaplan and Provost Dan May for their support, Karen Grava and Dean Golembeski for their media support, and Paula Hackenjos and Gail Berardesca for their administrative support. Without their support, this event would not have been possible.

I would also like to thank Douglas White – a prominent computer scientist and leader of the National Software Reference Library Project (NSRL) at the National Institute for Standards and Technology (NIST).

It is also important to thank Glenn Dardick – JDFSL publisher and Linda Lau – Associate Editor-in-Chief; the team at JDFSL that ensured a quality journal special issue is reviewed, edited and published in time for the conference.

I would also like to thank the TPC chairs – Joshua James, Frank Breitinger, Andrew Marrington and Ricci Ieong. Furthermore, it is important to thank all the hard work by the TPC committee that helped us with the quality review process of the submitted papers.

We are very excited about this year's conference, and we welcome you to ICDF2C / SADFE 2014!

Have a wonderful conference!

Sincerely,

Ibrahim (Abe) Baggili Ph.D.
Conference Chair
Assistant Professor of Computer Science, Tagliatela College of Engineering
Editor-in-Chief – Journal of Digital Forensics, Security and Law
UNHcFREG Director

KEYNOTES

DR. HENRY LEE

University of New Haven

Dr. Henry C. Lee is one of the world's foremost forensic scientists. Dr. Lee's work has made him a landmark in modern-day forensic sciences. He has been a prominent player in many of the most challenging cases of the last 40 years. Dr. Lee has worked with law enforcement agencies in helping to solve more than 6000 cases. In recent years, his travels have taken him to England, Bosnia, China, Brunei, and other locations around the world.

Dr. Henry Lee's testimony figured prominently in the O. J. Simpson trial, and in convictions of the "Woodchipper" murderer as well as hundreds of other murder cases. Dr. Lee has assisted local and state police in their investigations of other famous crimes, such as the murder of JonBenét Ramsey in Boulder, Colorado, the 1993 suicide of White House Counsel Vincent Foster, and the reinvestigation of the Kennedy assassination.

Dr. Henry Lee is currently the Chief Emeritus for the Department of Public Safety, Division of Scientific Services and was the Commissioner of the Connecticut Department of Public Safety for over two years and has served as that state's Chief Criminalist from 1979 to 2000. Dr. Lee was the driving force in establishing a modern State Police Forensic Science Laboratory in Connecticut.

In 1975, Dr. Henry Lee joined the University of New Haven, where he created the school's Forensic Sciences program. He has also taught as a professor at more than a dozen universities, law schools, and medical schools. Though challenged with the demands on his time, Dr. Lee still lectures throughout the country and world to police, Universities and civic organizations. Dr. Henry Lee has authored hundreds of articles in professional journals and has co-authored more than 25 textbooks, covering the areas, such as; DNA, Fingerprints, Trace Evidence, Crime Scene Investigation and Crime scene reconstruction.

DOUGLAS WHITE

Computer Scientist — NIST (Leader of the National Software Reference Library

Douglas White leads the National Software Reference Library project for the National Institute of Standards and Technology. Doug has worked at NIST since 1987. His experience has covered distributed systems, distributed databases and telecommunication protocols, real time biomonitoring, real time video processing, system administration and network monitoring. He holds both a B.A. and M.S. in computer science from Hood College. He has given lectures for the American Academy of Forensic Sciences, the Federal Law Enforcement Training Center, the High Technology Crime Investigation Association, the Digital Forensic Research Workshop and numerous other digital forensic conferences.

PROGRAMME

DAY 1: 18th September 2014

07:45 – 08:30 **Breakfast**

08:30 – 09:00 **Registration**

09:00 – 09:15 **Welcome to ICDF2C'14**

09:15 – 10:15 **Keynote — Dr. Henry Lee (UNH)**

15 min Coffee Break

SESSION I: Network Forensics

10:30 – 12:00 **On Identities in Modern Networks:** Libor Polčák, Radek Hranický and Tomáš Martínek, (Brno University of Technology, Czech Republic)

File Detection on Network Traffic Using Approximate Matching: Frank Breitinger and Ibrahim Baggili. (University of New Haven, CT, USA)

Accurate Modeling of the Siemens S7 SCADA Protocol for Intrusion Detection and Digital Forensics: Amit Kleinman and Avishai Wool. (Tel Aviv University, Israel)

1.5 Hours Lunch Break (on your own)

SESSION II: Digital Forensic Investigation and Cases

13:30 – 15:00 **Understanding Computer Forensics Requirements in China via the "Panda Burning Incense" Virus Case:** Frank Law, K P Chow and Y H Mai. (Hong Kong Police Force, University of Hong Kong, Hong Kong)

Multi-Stakeholder Case Prioritization in Digital Investigations: Joshua I. James. (Soonchunyang University, South Korea)

Forensics of Software Copyright Infringement Crimes: Dr. P Vinod Bhattathiripad. The modern POSAR test juxtaposed with the dated AFC test (India)

15 min Coffee Break

15:15 – 17:15 **Workshop — Microsystemation**

19:00 – Whenever **Join Us for a Common Dinner *(on your own)***

DAY 2: 19th September 2014

08:00 – 08:45 **Breakfast**

08:45 – 09:00 **Registration**

09:00 – 10:00 **Keynote — Douglas White (NIST)**

15 min Coffee Break

SESSION III: Online Forensics

10:15 – 11:45 **Leveraging Decentralisation to Extend the Digital Evidence Acquisition Window: Case Study on BitTorrent Sync:** *Mark Scanlon, Jason Farina, Nhien-An Le-Khac and Tahar Kechadi. (University College Dublin, Dublin, Ireland)*

Fast RTP Detection and Codecs Classification in Internet Traffic: *Petr Matousek, Ondrej Rysavy and Martin Kmet. (Brno University of Technology, Czech Republic)*

Developing a Conceptual Framework for Modeling "Deviant Cyber Flash Mob": A Socio-Computational Approach Leveraging Hypergraph Constructs: *Samer Al-Khateeb and Nitin Agarwal. (University of Arkansas at Little Rock, USA)*

1.5 Hours Lunch Break (on your own)

13:15 – 15:15 **Workshop — Cellebrite**

Short break

15:30 – Whenever **Cocktail Party at the University of New Haven: Grand Opening of the Cyber Forensics Research and Education Laboratory:** Bus transportation is provided from the Omni to the UNH campus and back.

DAY 3: 20th September 2014

08:00 – 08:45 **Breakfast**

08:45 – 09:00 **Registration**

SESSION IV: Digital Investigations — Tools and Approaches

09:00 – 10:00 **Automated Disk Investigation Toolkit:** *Umit Karabiyik and Sudhir Aggarwal. AUDIT: (Florida State University, Florida, USA)*

Exploring Forensic Implications of the Fusion Drive: *Shruti Gupta and Marcus Rogers (Purdue University, Indiana, USA)*

15 min Coffee Break

SESSION V: Digital Forensics Analysis Techniques

10:15 – 11:15 **An Efficient Similarity Digests Database Lookup — A Logarithmic Divide and Conquer Approach:** *Frank Breitinger, Christian Rathgeb and Harald Baier. (CASED, Germany)*

"Time for Some Traffic Problems": Enhancing E-Discovery and Big Data Processing Tools with Linguistic Methods for Deception Detection: *Erin Smith Crabb. (University of Maryland, MD, USA)*

1.5 Hours Lunch Break (on your own)

SESSION VI: Laws and Standards

12:45 – 13:45 **Relating Admissibility Standards for Digital Evidence to Attack Scenario Construction:** *Changwei Liu, Anoop Singhal and Duminda Wijesekera. (George Mason University, VA, USA)*

Evidentiary Power and Propriety of Digital Identifiers and The Impact on Privacy Rights in the United States: *Michael Losavio and Deborah Keeling. (University of Louisville, KY, USA)*

15 min Coffee Break

SESSION VII: Mobile Forensics

14:00 – 15:00 **Effects of the Factory Reset on Mobile Devices:** *Riqui Schwamm and Neil Rowe. (Naval Postgraduate School, USA)*

Testing Framework for Mobile Device Forensics Tools: *Maxwell Anobah, Shahzad Saleem and Oliver Popov. (Stockholm University, Sweden)*

15:00 – 15:15 **Closing Words**

ORGANIZED BY:

TAKE A BYTE OUT OF CRIME
www.UNHcFREG.com

University of New Haven
TAGLIATELA COLLEGE OF ENGINEERING

EAI European Alliance for Innovation

SPONSORS:

MICRO SYSTEMATION

Gold Sponsor

cellebrite
delivering mobile expertise

Silver Sponsor

JONES & BARTLETT LEARNING
An Ascend Learning Company

Reception Sponsor

HTCIA
HIGH TECHNOLOGY CRIME INVESTIGATION ASSOCIATION
CONNECTICUT CHAPTER

Exhibition Sponsor

JDFSL
The Journal of Digital Forensics, Security and Law

DIGITAL FORENSICS SECURITY LAW ADFSL

Media Partners

CREATE-NET

Technical Sponsors