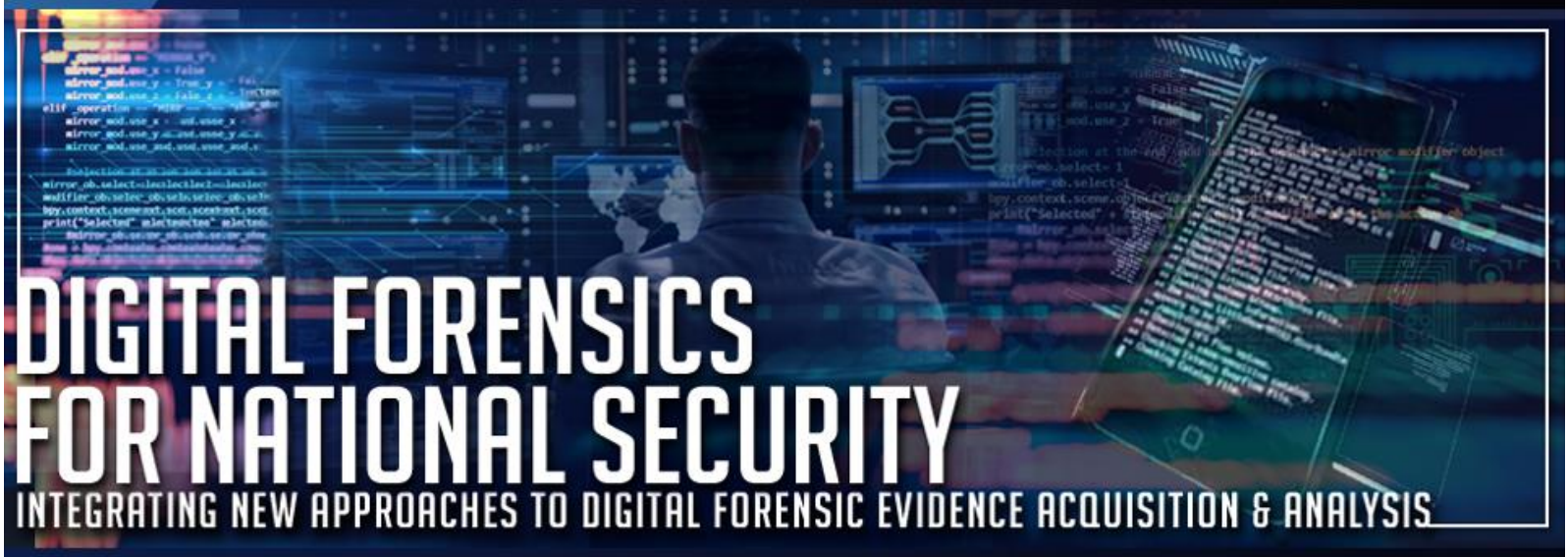

DIGITAL FORENSICS FOR NATIONAL SECURITY

INTEGRATING NEW APPROACHES TO DIGITAL FORENSIC EVIDENCE ACQUISITION & ANALYSIS

DECEMBER 10-11, 2019 | MARY M. GATES LEARNING CENTER, ALEXANDRIA, VA

2019 Speakers Include:

Dr. David B. Muhlhausen, Director, National Institute of Justice, DOJ

COL Zane Jones, USA, Deputy Director, Defense Forensics & Biometric Agency

Jude Sunderbruch, SES, Executive Director, AFOSI

SA Daniel D'Ambrosio, Executive Assistant Director, Cyber Directorate, NCIS

SYMPOSIUM AGENDA DIGITALFORENSICS.DSIGROUP.ORG

Program Design & Goal:	DSI's Digital Forensics for National Security Symposium will bring together members of the Federal Government Agencies, DoD, US Military Services, Academia, & Industry in a 'town-hall' type forum to discuss how Digital Forensics, sometimes called 'Computer Forensics', is advancing the application of scientific investigation into digital crimes, attacks, and intrusions at the national, state, and local levels. This effort can be described as the identifying, maintaining, and analyzing of digital evidence in an effort to identify the source of a cyber breach and other actionable intelligence. This Symposium will also detail how current innovations in mobile and network forensic toolkits, such as 'FileTSAR', have led to increased success in defending the cyber space, as well as enhanced the ability to recover & preserve data. The sophisticated methods that cyber criminals/terrorists have used to commit digital crimes continue to evolve, due to the advent of modern computing & the ever-changing technological landscape. This Symposium will further explain how the advancements and innovations made in the field of digital forensics in the '90s &'00s have resulted in increased capabilities of network forensic tools today. Attendees at this event will have the chance to hear briefs from senior level delegates that provide a deep dive into current/future collaborative efforts to develop & field new ways to combat digital attacks and ultimately, improve the defensive cyber capabilities of federal law enforcement & our nation's Warfighters. DSI's team specializes in the extensive research and development of our Symposiums' content and focus areas; we will assemble the most respected minds in human and technical analysis from key military and civilian offices. Our non-partisan approach allows us to reach across all services and organizations to bring together a truly holistic group of decision makers and solution providers.
Operating Guidelines:	DSI's Symposium directly supports DoD priorities by providing a conduit for officials to efficiently reach audiences outside of their respective offices that directly impact their department's mission success, at no charge to the government, and in an efficient expenditure of time. DSI's Symposium will provide a forum to address and improve internal and external initiatives, meet with and hear from partner organizations, disseminate vital capability requirements to industry, increase visibility within the larger community, and generally support their mission. The Symposium is open and complimentary to all DoD & Federal employees and is considered an educational training forum, a widely attended gathering. (Industry and academia members are charged a fee for admission) Symposium is CLOSED TO PRESS / NO RECORDINGS
General Target Audience:	Federal Government Agencies, DoD, US Military Services, Industry, Academia, and nonprofit stakeholders involved in the research, development, future capabilities planning, and acquisition of digital forensics toolkits to advance National Security efforts.
Specific topics to be discussed include:	-Using digital forensics partnerships between the military and federal govt. to improve cyber defense -Ensuring the reliability of computer forensic tools -Implementing digital forensics for large-scale networks - Utilizing Digital Forensics to Ensure the Integrity of Investigative Data -Improving Forensic tool capabilities to ensure the integrity and retrieval of data - Fielding the most advanced digital forensics tools to help Soldiers see the cyber battlefield & the weapons being deployed there -Designing ways to accelerate digital forensics analysis that significantly reduces the time necessary to process digital evidence -Guiding the efficient and effective use of computer technology to investigate crimes at all levels of government - Devising an all-in-one toolkit to combat cyber crimes -Supporting national investigations into Internet criminal activities with state-of-the-art cyber investigative methods and forensic data processing techniques - Enhancing digital forensic techniques to enhance SOF ability to recover key evidence from terrorist electronic devices - Delivering superior digital forensics and multimedia (D/MM) lab services, cyber technical training to the Defense Industrial Base

Topics & Speaker Times Subject to Edits

December 10th, 2019	
8:00 – 8:45	***Registration and Light Breakfast Reception Open***
8:45 – 9:00	**Moderator Opening Remarks** **Jim Christy, Special Agent (Retired) (Confirmed)** President & CEO of The Christy Group, LLC; Cyber Investigations & Digital Forensics Consultant
9:00 – 9:45	**NIJ Initiatives Towards Facilitating Digital Forensics R&D to Enhance Digital Evidence Acquisition and Analysis** - Accelerating the use of innovative, open source digital forensics tools to assist federal law enforcement & other government agencies - Update on current collaborative NIJ projects underway to improve the analysis and processing of digital media - Near term goals to maintain the Technology Working Group to aid in decision- making & strengthen relations between the DOJ & forensic practitioners **Dr. David B. Muhlhausen (Confirmed)** Director, National Institute of Justice DOJ
9:45 -10:30	**USAF Efforts to Apply Digital Forensics to Assist with Cyber Investigations Across the Full Spectrum of Conflict** - Using digital forensic methods to more efficiently and effectively investigate serious offenses such as computer hacking & cyber terrorism - Ensuring USAF wartime capability from counterintelligence support to force protection to find, fix, track, and neutralize enemy threats in contested & hostile environments - Conducting specialized investigative activities with the aid of digital forensic tools to help provide timely and accurate threat information to the Warfighter **Jude Sunderbruch, SES (Confirmed)** Executive Director AFOSI
10:30 – 11:00	**Networking Break & Exhibits**
11:00 – 11:45	**Utilizing Digital Forensics & Evidence for Virtually All Types of Crime to Help Defend the FBI Network from Cyber Breaches** - Advancing the data analysis of digital evidence from mobile devices to help assist with criminal investigations - Delivering technology-oriented solutions for all FBI activities including counterterrorism, counterintelligence, & cyber operations - Future S&T goals toward leveraging resources to increase the use of digital forensics to address emerging cyber threats **John Pettus (Confirmed)** Acting Section Chief, Digital Forensics & Analytics Section Director, Collections Infrastructure Section Operational Technology Division (OTD), FBI
11:45 – 12:30	**Establishment of Scientific Understandings in Cyber Deception to Increase a Warfighter's Cyber Agility** - Using advanced computer frameworks to help the Warfighter outmaneuver cyber attacks - Facilitating Army's efforts to secure the cyber domain by establishing new foundations in cyber deception - Leveraging the honeypot/decoy/signaling to manipulate, mislead, and defeat adversaries **Dr. Cliff Wang (Confirmed)** Director of Computer Science Division Army Research Office, Army Futures Command
12:30 – 1:30	**Networking Lunch**

1:30 – 2:15	**DoD Strategy: Delivering Superior Digital Forensics & Cyber Technical Training in Support of Law Enforcement, Counterintelligence, & Counterterrorism Efforts** - Providing technical solutions such as intrusion & analysis to help examine digital and multi-media - Testing & validating digital forensic tools for reliability, performance, & reproducibility - Current & future efforts to proactively identify new digital forensic workflow tools in support of the DoD Intelligence and Law Enforcement communities **Lam Nguyen (Confirmed)** Director, Cyber Forensics Lab DoD Cyber Crime Center (DC3)
2:15 – 3:00	**NCFTA Efforts to Work With All Levels of Law Enforcement to Improve Information Sharing About Criminal Activity** - Current efforts to utilize cyber forensic technology & shared information to identify, mitigate, disrupt, & neutralize cyber threats - Delivering actionable intelligence to law enforcement partners in support of national security priorities - Providing members of NCFTA real-time updates on emerging threats & allowing law enforcement to collaborate with SMEs to further uphold the integrity of their investigations **Matt LaVigna (Confirmed)** President & CEO National Cyber Forensics & Training Alliance
3:00 – 3:30	**Networking Break & Exhibits**
3:30 – 4:15	**Mobile App Forensic Evidence Project for Law Enforcement Practitioners** **Dr. Yong Guan (Confirmed)** Professor, Department of Electrical and Computer Engineering, Iowa State University Associate Director for Research, Information Assurance Center Cyber Forensics Coordinator, NIST Center of Excellence in Forensic Sciences - CSAFE
4:15-5:00	**Digital Forensic Toolkits for Network Forensics and ICAC Investigations** - FileTSAR is a network forensics toolkit for investigating cases involving large-scale computer networks - CATT analyzes chats to identify high-priority contact child sex offenders - Currently, enhancing and augmenting CATT to include demographic characteristics of chatters and biometric identification of offenders **Dr. Kathryn Seigfried-Spellar (Confirmed)** Assistant Professor, Computer & Information Technology Purdue University

End of Day 1

December 11th, 2019	
8:15 – 8:45	***Registration and Light Breakfast Reception Open***
8:45 – 9:00	**Moderator Opening Remarks** **Jim Christy, Special Agent (Retired) (Confirmed)** President & CEO of The Christy Group, LLC; Cyber Investigations & Digital Forensics Consultant
9:00 – 9:45	**Utilizing NCIS Cyber & Digital Forensic Capabilities to Disrupt, Deter, and Mitigate Criminal, Terrorist, and Foreign Intelligence Threats Against the DON** - Coordinating with law enforcement and intelligence agencies in the U.S. and abroad to identify threats in the Naval cyber domain - Conducting electronic media forensics to more efficiently & effectively track the adversary - Using Navy's digital forensic tools to monitor developments and trends in malware, phishing, and other computer intrusions **SA Daniel D'Ambrosio (Confirmed)** Executive Assistant Director, Cyber Directorate NCIS
9:45 – 10:30	**Army CID's Efforts to Field the Most Advanced Digital Forensics Tools to Help Soldiers See the Cyber Battlefield & the Weapons Being Deployed There** - Current & future CID initiatives toward investigating & analyzing digital devices using various forensic toolkits - Leading collaborations with industry to acquire the best digital forensic tools possible to help build a digital timeline to track the adversary - Near term goals toward facilitating the effective training of Soldiers & analysts to take advantage of vital cyber forensic tools **COL Zane Jones, USA (Confirmed)** Deputy Director Defense Forensics & Biometric Agency
10:30-10:40	**Overview of Macquisition and Blacklight** **Kevin Long (Confirmed)** Director, Federal Sales BlackBag Technologies
10:40 – 11:10	**Networking Break & Exhibits**

11:10 – 12:30	**Panel:** **Facilitating the Analysis & Preservation of Digital Evidence in Support of Digital Forensic Investigations** *The **Regional Computer Forensic Laboratories (RCFL**) were established to provide forensic services and guidance to support law enforcement agencies at all levels of government in collecting and examining digital evidence for a wide range of investigations, including child pornography, terrorism, violent crime, & other national security efforts. This panel will gather directors from the various RCFL's for their respective states to discuss how they are using innovative digital forensics tools and techniques to preserve the integrity of investigative data. This panel will also examine what each of these states RCFL Director's strategies are toward utilizing these tools in order to more efficiently determine what evidence is legally permissible from electronic devices.* **Panel Moderator-** **Linda Grody (Confirmed)** Unit Chief, RCFL National Program Office Operational Technology Division (OTD), FBI **Panelists-** **SSA Sarah Lucas (Confirmed)** Director, Heart of America RCFL FBI **SSA Sherman Kwok (Confirmed)** Director, Silicon Valley Regional Computer Forensic Laboratory FBI **SSA Bruce Hartung (Confirmed)** Director, New England Regional Computer Forensic Laboratory FBI **John Dziedzic (Confirmed)** Director, Chicago Regional Computer Forensic Laboratory FBI
12:30 – 1:30	**Networking Lunch**
1:30-2:15	**Promoting the Efficient and Effective Use of Computer Technology to Investigate Crimes** - Ensuring the reliability of computer forensic tools - Developing tools for testing computer forensic software, including test criteria and test sets - Update on the *CFReDS* Project **Barbara Guttman (Confirmed)** Group Leader, Software Quality Group NIST
2:15-3:00	**Advances in Cloud Based Digital Forensics** - Devising open-source digital forensics processing applications to reduce the time required to conduct investigations on desktop computers - Current updates on DFORC2 & how it will reduce the time required to ingest and process digital evidence - Using the AWS computing cloud platform to increase the efficiency of the DFORC2 prototype to better support criminal investigations **Dr. Daniel Gonzales (Confirmed)** Senior Scientist RAND Corp
3:00	**End of Summit**