



DIGITAL FORENSICS FOR NATIONAL SECURITY

MAY 14-15 | NATIONAL HARBOR, MARYLAND

OFFICIAL AGENDA

ADVANCING INVESTIGATIONS WITH CUTTING-EDGE DIGITAL FORENSIC CAPABILITIES

SUMMIT OVERVIEW

Program Design and Goal:

DSI's 6th Annual Digital Forensics Symposium for National Security brings together leaders from the Department of Defense, federal government, intelligence agencies, industry, and academia to explore how digital forensics tools and technologies are combating sophisticated criminal activities. These leaders will share how digital forensics impacts their organizations and the crucial role it plays in investigations.

With the understanding that almost all modern crimes have a digital element, the symposium will address the increasing complexity of digital crimes and the need for continuous adaptation of tools and techniques. Attendees will gain firsthand insights into the challenges faced by national security and law enforcement officials in combating cybercrime and collecting vital digital evidence. Discussions will cover critical topics such as interagency cooperation in digital forensics through training, the evolving landscape of digital forensic tools, and the significant role of eDiscovery tools. This symposium provides a unique platform for leaders to share best practices, explore emerging technologies, and collaborate to address the evolving challenges of digital forensics in national security.

DSI's team specializes in the extensive research and development of our Summits' content and focus areas, and we will assemble the most respected minds in digital forensics as well as key policymakers across 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.

Agenda current as of 4/21/25

Operating Guidelines:

DSI's Summit directly supports IC and Federal Government 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 Summit 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 Summit is open and complimentary to all DoD and Federal employees and is considered an educational training forum, a widely attended gathering.

(Industry and academia members are charged a fee for admission)

Summit is CLOSED TO PRESS / NO RECORDINGS

SUMMIT OVERVIEW

General Target Audience

Federal Government Agencies, DoD, US Military Services, Industry, Academia, and nonprofit stakeholders involved in the research, development, capabilities planning, and acquisition of digital forensics tools to advance National Security efforts.

Specific Topics to be Discussed

- Preserving Warfighter Readiness through Digital Forensics and Cybersecurity
- Promoting Digital Forensic Techniques in the Protection of US Assets and Leaders
- Advancing Digital Forensics: FBI Challenges and Innovations in Digital Investigations
- Understanding eDiscovery Technologies Role in Digital Forensics
- Driving Innovation of Digital Forensic Devices for Criminal Investigations
- Empowering Federal, State, Local, and Tribal Law Enforcement by Training the Next
- Generation Digital Investigator

VENUE:

151 St George Blvd, Oxon Hill, MD 20745



SUMMIT OVERVIEW

2025 Confirmed Speakers Include:



Lesley H. Bernys, SES

Executive Director, DoD Cyber Crime Center (DCISE)



Michael R. Centrella, SES

Assistant Director, Office of Field Operations
US Secret Service



Clifford T. Minor

Associate Director, Cyber Operations Division OSI Center, Office of Special Investigations, Department of the Air Force



Col. Gerald Mazur

Commander, 91st Cyber Brigade, Virginia National Guard



Barbara Guttman

Group Leader, Software Quality Group, NIST



Jeffrey L. Coburn

Section Chief, Digital Forensics & Analytics Section, Operational Technology Division, FBI



David Ortiz

Division Chief, Digital Forensics and Research Brand, Army Criminal Investigation Division



Lucas Zarwell

Director, Office of Investigative and Forensic Sciences, NIJ



Zurich Shanahan

Supervisory Special Agent DoD OIG



Sundararaja Sitharama Iyengar PhD

Distinguished Professor, Florida International University, and Director, Forensic Investigations Network in Digital Sciences (FINDS) Center of Excellence



Jill Crisman, PhD

Vice President & Executive Director, Digital Safety Research Institute



Jude R. Sunderbruch

Former Executive Director, DC3

MODERATOR

SUMMIT SCHEDULE

DAY 1: WEDNESDAY, MAY 14TH

8:00—8:45 AM

Registration and Light Breakfast Reception Open

8:45—9:00 AM

Opening Remarks- Event Moderator

Jude Sunderbruch (Confirmed)

Managing Director at Cyber Defense Labs

Former Executive Director DoD Cyber Crime Center (DC3)

9:00—9:40 AM

Delivering Cutting Edge Digital Investigative Tools and Policy to Support DC3's National Security Partners

- Enabling and informing law enforcement and national security partners through innovative capabilities and high-quality cyber training.
- Protecting industry partners through the DoD–Defense Industrial Base Collaborative Information Sharing Environment (DCIS) to provide safeguards for unclassified DoD information like malware analysis and no cost-forensics
- Conducting Digital and Multimedia (D/MM) forensic examinations, extracting otherwise inaccessible data, and providing expert testimony in legal proceedings for DC3 customers.

Lesley H. Bernys, SES (Confirmed)

Executive Director

DoD Cyber Crime Center (DCISE)

9:40—10:20 AM

Preserving Warfighter Readiness through Digital Forensics and Cybersecurity

- Protecting the Army's most important asset, our soldiers.
- Using digital forensics to proactively locate sources of narcotics that resulted in fatal overdoses.

David Ortiz (Confirmed)

Division Chief, Digital Forensics and Research Brand

Army Criminal Investigation Division

10:20—11:00 AM

Networking Break & Exhibits

SUMMIT SCHEDULE

DAY 1: WEDNESDAY, MAY 14TH

11:00—11:40 AM

Supporting Airforce Operational Goals and Security with Digital Forensics

- Understanding the role of Digital Forensics at the Airforce Office of Special Investigations (OSI)
- Cooperating with partners such as DC3 to counter cybercrime and insider threats to USAF and USSF assets and personnel.
- Empowering Airforce operators through digital forensic training to combat the everchanging cyber landscape and methods of bad actors.

Clifford T. Minor (Confirmed)

Associate Director for Cyber Operations, OSI Center
Air Force Office of Special Investigations

11:40 AM—12:20 PM

Advancing Digital Forensics: FBI Challenges and Innovations in Digital Investigations

- Working with advanced technologies, forensic concepts, software, and tools to solve the FBI's most critical cases
- Collecting, preserving, and analyzing vital and hard to acquire evidence found on devices ranging from mobile devices, vehicles, and Internet of Things (IoT) devices.
- Providing support to law enforcement and other investigative agencies across the nation in digital forensics and combating crimes with digital footprints
- Analyzing the challenges of acquiring digital evidence and computer investigations.

Jeffrey L. Coburn (Confirmed)

Section Chief, Digital Forensics & Analytics Section, Operational Technology Division
FBI

12:20—12:30 PM

Tech in Ten

12:30—1:20 PM

Networking Lunch

SUMMIT SCHEDULE

DAY 1: WEDNESDAY, MAY 14TH

1:20—2:10 PM

Panel: Bridging the Gap Between eDiscovery and Digital Forensics

In the modern era, digital evidence remains an ever-constant factor in investigations into criminal justice and national security. Almost all crimes investigated have a digital component associated with it and discovering that evidence is crucial in enforcing justice. One of the most prominent types of tools to emerge to help uncover this evidence is eDiscovery technology. This fireside chat will bring together experts in eDiscovery to discuss the importance of this technology and its benefits to digital forensics. Speakers will bring their unique perspectives as implementors of eDiscovery, and the benefits they have seen with their organization.

Moderator: Robert Fried (Confirmed)- Fellow, Henry C. Lee Institute of Forensic Science

Participants:

- **Dana Willis (Invited)**- eDiscovery Unit Chief, DEA
- **Nick Wittenberg (Confirmed)** - Former White House Office of Science and Technology Policy Counsel
- **Jerry Bui (Tentatively Confirmed)** - Membership Director, Association of Certified E-Discovery Specialists, CEO, Right Forensics
- **Aron Ahmadi (Confirmed)** - Senior Director of Applied Science, Relativity

2:10—2:20 PM

Tech in Ten

2:20—2:50 PM

Moving Fast and Not Breaking Things in Digital Forensics

- How DCIS has grown and developed through the years
- Challenges with digital forensics and cyber investigations
- Successes with People, Policy, Tools
- Challenges on the Horizon

Zurich Shanahan (Confirmed)

Supervisory Special Agent
DoD OIG

2:50—3:20 PM

Networking Break & Exhibits

SUMMIT SCHEDULE

DAY 1: WEDNESDAY, MAY 14TH

3:20—4:10 PM

Joint Session: Advancing Forensic Science for a More Effective Criminal Justice System

- Understanding NIJ's role in supporting high-quality forensic science research
- Research and development on cutting edge technology to improve the accuracy, reliability, and cost-effectiveness, methods for the identification, analysis, and interpretation of forensic evidence.
- Overview of NIJ's digital and multimedia evidence portfolio

Lucas Zarwell (Confirmed)

Director

Office of Investigative and Forensic Sciences, National Institute of Justice

Danielle Crimmins, PhD (Confirmed)

Social Science Research Analyst

Office of Criminal Justice Systems, National Institute of Justice

4:10—4:50 PM

Utilizing Semantic Forensics to Enhance Protections Against Manipulated Media

- Ensuring the digital ecosystem is safer for users
- Exploiting automated media generation and manipulation algorithms that are prone to making semantic errors
- Developing models to distinguish genuine images (including those with traditional edits) from entirely AI-generated ones

Dr. Jill Crisman (Confirmed)

Vice President and Executive Director of Digital Safety Research Institute

UL Research Institutes

4:50 PM

End of Day 1

FOLLOW US

TO STAY UP TO DATE ON THE LATEST NEWS, EVENTS, AND NETWORKING OPPORTUNITIES



x.com/dsi_group



linkedin.com/company/



vimeo.com/dsigroup

SUMMIT SCHEDULE

DAY 2: THURSDAY, MAY 15TH

8:15—8:45 AM

Registration and Light Breakfast Reception Open

8:45—9:00 AM

Opening Remarks- Event Moderator

Jude Sunderbruch (Confirmed)

Managing Director at Cyber Defense Labs

Former Executive Director DoD Cyber Crime Center (DC3)

9:00—9:40 AM

Promoting Digital Forensic Techniques in the Protection of US Assets and Leaders

- Understanding the role of digital forensics at the Secret Service in the protection of major US Assets and leaders
- Fostering strong partnerships with law enforcement, prosecutors, industry, and academia to effectively combat cybercrime.
- Supporting strategic domestic and international investigations to address counterfeit, computer network breaches, ransomware, and other cyber-enabled financial crimes.

Michael R. Centrella, SES (Confirmed)

Assistant Director, Office of Field Operations
US Secret Service

9:40—10:20 AM

Researching the Evolving Landscape of Digital Forensics: Addressing Emerging Challenges and Best Practices

- Changing the paradigm for digital forensics lab quality: a very bold approach
- Developing community resources for greater efficiency: sharing datasets and artifacts

Barbara Guttman (Confirmed)

Group Leader, Software Quality Group
NIST

10:20—10:50 AM

Industry Perspective

10:50—11:30 AM

Networking Break & Exhibits

SUMMIT SCHEDULE

DAY 2: THURSDAY, MAY 15TH

11:30 AM—12:30 PM **The Digital Beat: Equipping Local Law Enforcement with Digital Forensics Skills and Tools**

The digital revolution has transformed crime, leaving a trail of electronic evidence in its wake. This panel will explore the critical role of digital forensics in modern policing, with practical insights and techniques to investigate and prosecute digital crimes effectively. This panel will bring together leaders from across local law enforcement to bring their unique perspective on how they have seen digital forensics affect their roles.

Moderator: Stephynie Velez (Confirmed) - Deputy Director - Cyber Innovation and Research Center, Noblis

Panelists:

Jesse Lindmar (Invited) Forensic Scientist Section Supervisor, Digital & Multimedia Evidence Section, Virginia Department of Forensic Science, Central Laboratory

12:30—1:30 PM **Networking Lunch**

1:30—2:10 PM **Zero Trust Forensics: AI-Driven Intrusion Detection and Network Behavior Analysis**

- Introducing a Zero Trust framework for digital forensics, emphasizing AI-powered network forensic sniffing and behavior analysis for intrusion detection.
- Understanding autonomous forensic agents, next-generation forensic architectures, and adaptive security models, highlighting innovations in AI-based forensic intrusion detection systems.
- Gaining insights into the challenges of modern forensic analysis, the integration of Zero Trust with AI, and the future of cybersecurity in an era of persistent cyber threats.

Sundararaja Sitharama Iyengar PhD (Confirmed) - Distinguished University Professor, Florida International University, and Director, Forensic Investigations Network in Digital Sciences (FINDS) Center of Excellence

Nrupul Rao (Confirmed)- Digital Forensics Expert

SUMMIT SCHEDULE

DAY 2: THURSDAY, MAY 15TH

2:10—2:40 PM

Exercising Critical Infrastructure Cyber Incident Response to Build Resiliency and Preparedness

- Cooperating with over 40 states, federal, local, academic, foreign, and private partners to promote greater cyber security
- Enabling stakeholders to understand how multiple levels of industry and government respond and work together to mitigate a cyber-attack against commercial critical infrastructure
- Understanding the role of digital forensics in Cyber Incident Exercises and in overall cyber security

Col. Gerald Mazur (Confirmed)

Commander
91st Cyber Brigade, Virginia National Guard

2:40 PM

End of Symposium