Thursday, January 19			
ALL DAY	**Travel Day**		
1600-2000	**Conference Registration/ Information Desk** *Grand Hall Foyer*		

Friday, January 20			
0730-1630	**Conference Registration/Information Desk** *Grand Hall Foyer*		
0730-1630	**Cyber Café** *Grand Hall Foyer* **Sponsored By: Guidance Software**		
0730-1630	**DC3 Digital Crime Scene Challenge—See page 96 for more information** *Grand Hall Foyer* **Sponsored By: Booz Allen Hamilton and Forward Discovery**		
0730-0830	**Morning Reception** *Conference Level Foyer*		
0830-1630	**PRE-CONFERENCE TRAINING: DAY 1**		
TRAINING ROOM	**Auburn**	**Baker**	**Courtland**	**Dunwoody**

TRAINING ROOM	**Auburn**	**Baker**	**Courtland**	**Dunwoody**
	EnCase for Examiners **REPEATS MONDAY**	Windows Incident Response Fundamentals **REPEATS MONDAY**	Introduction to Malware Analysis **REPEATS SUNDAY/MONDAY**	Introduction to Server 2008 **REPEATS MONDAY**
TRAINING ROOM	**Edgewood**	**Fairlie**	**Hanover C**	**Hanover D**
	Essential Trade Craft for Digital Sleuths **REPEATS MONDAY**	Mac Forensics **REPEATS MONDAY**	Introduction to Cyber Analysis **REPEATS SUNDAY/MONDAY**	Linux Incident Response Scripting **REPEATS MONDAY**
TRAINING ROOM	**Hanover E**	**Hanover F**	**International North**	**International South**
	Analyzing Malicious Carrier Files and Common Exploits **REPEATS SUNDAY/MONDAY**	Wireless Technology Workshop **REPEATS SUNDAY/MONDAY**	Digital Forensics with DCITA LIVE **REPEATS MONDAY**	SANS - Lethal Digital Forensic Techniques and Memory Analysis **LAPTOP REQUIRED** **REPEATS SUNDAY/MONDAY**

0930-1015	**Morning Coffee Break** *Conference Level Foyer*		
1400-1445	**Afternoon Break** *Conference Level Foyer*		

Saturday, January 21			
0730-1700	**Conference Registration/Information Desk** *Grand Hall Foyer*		
0730-1700	**Cyber Café** *Grand Hall Foyer* Sponsored By: Guidance Software		
0730-1730	**DC3 Digital Crime Scene Challenge—See page 96 for more information** *Grand Hall Foyer* Sponsored By: Booz Allen Hamilton and Forward Discovery **NEW**		
0730-0830	**Morning Reception** *Conference Level Foyer*		
0830-1630	**PRE-CONFERENCE TRAINING: DAY 2**		
TRAINING ROOM	**Auburn**	**Baker**	**Courtland**	**Dunwoody**
	Advanced Wireless Lab **REPEATS SUNDAY**	Linux Incident Response Fundamentals **REPEATS SUNDAY**	Introduction to Malware Analysis (Cont.) **REPEATS SUNDAY/MONDAY**	Introduction to Windows 7 **REPEATS SUNDAY**
TRAINING ROOM	**Edgewood**	**Fairlie**	**Hanover C**	**Hanover D**
	Introduction to EnCase for Prosecutors and Case Agents **REPEATS SUNDAY**	Mac Response **REPEATS SUNDAY**	Introduction to Cyber Analysis (Cont.) **REPEATS SUNDAY/MONDAY**	Windows Incident Response Scripting **REPEATS SUNDAY**
TRAINING ROOM	**Hanover E**	**Hanover F**	**International North**	**International South**
	Analyzing Malicious Carrier Files and Common Exploits (Cont.) **REPEATS SUNDAY/MONDAY**	Wireless Technology Workshop (Cont.) **REPEATS SUNDAY/MONDAY**	Pen Testing 101 **REPEATS SUNDAY**	SANS - Lethal Digital Forensic Techniques and Memory Analysis (Cont.) **LAPTOP REQUIRED** **REPEATS SUNDAY/MONDAY**
0930-1015	**Morning Coffee Break** *Conference Level Foyer*		
1400-1445	**Afternoon Break** *Conference Level Foyer*		
1630-1800	**Saturday Night Get Together Reception** *Grand Hall Foyer* See page 90 for details.		

Sunday, January 22

Time	Event
0730-1800	**Conference Registration/Information Desk** *Grand Hall Foyer*
0730-1800	**Cyber Café** *Grand Hall Foyer* **Sponsored By: Guidance Software**
0730-1800	**DC3 Digital Crime Scene Challenge—See page 96 for more information** *Grand Hall Foyer* **Sponsored By: Booz Allen Hamilton and Forward Discovery** *NEW*
0730-0830	**Morning Reception** *Conference Level Foyer*

PRE-CONFERENCE TRAINING: DAY 3 (0830-1630)

TRAINING ROOM	Auburn	Baker	Courtland	Dunwoody
	Advanced Wireless Lab	Linux Incident Response Fundamentals	Introduction to Malware Analysis	Introduction to Windows 7

TRAINING ROOM	Edgewood	Fairlie	Hanover C	Hanover D
	Introduction to EnCase for Prosecutors and Case Agents	Mac Response	Introduction to Cyber Analysis	Windows Incident Response Scripting

TRAINING ROOM	Hanover E	Hanover F	International North	International South
	Analyzing Malicious Carrier Files and Common Exploits	Wireless Technology Workshop	Pen Testing 101	SANS - Lethal Digital Forensic Techniques and Memory Analysis **LAPTOP REQUIRED**

Time	Event
0830-1630	**AFOSI Meeting (Closed Session)** *Learning Center*
0930-1015	**Morning Coffee Break** *Conference Level Foyer*
1400-1445	**Afternoon Break** *Conference Level Foyer*

NEW

DC3 Digital Crime Scene Challenge

Think like Anthony "Tony" DiNozzo from CBS's NCIS

Visit the DC3 Digital Crime Scene Challenge Area in the Grand Hall Foyer to test your investigative skills and win great prizes!

The Crime Scene Area is open during the following times:

Friday	0730-1630		Tuesday	0700-1900
Saturday	0730-1730		Wednesday	0730-1700
Sunday	0730-1800		Thursday	0730-1200
Monday	0730-1900			

See page 96 for more information about this NEW event!

Sponsored By:

Booz | Allen | Hamilton

FORWARD DISCOVERY

Monday, January 23			
0600-1830	**Conference Registration/Information Desk** *Grand Hall Foyer*		
0730-1900	**Cyber Café** *Grand Hall Foyer* **Sponsored By: Guidance Software**		
0730-1900	**DC3 Digital Crime Scene Challenge—See page 96 for more information** *Grand Hall Foyer* **Sponsored By: Booz Allen Hamilton and Forward Discovery**		
0730-0830	**Morning Reception** *Conference Level Foyer*		
0800-1600	**Classified Session: Cyber Counterintelligence (CI) Briefing—See below for more information** All attendees must possess the appropriate Secret U.S. Clearance. Please note that buses will depart promptly at 0715.		
0830-1630	**PRE-CONFERENCE TRAINING: DAY 4**		
TRAINING ROOM	**Auburn**	**Baker**	**Courtland**	**Dunwoody**
	EnCase for Examiners	Windows Incident Response Fundamentals	Introduction to Malware Analysis (Cont.)	Introduction to Server 2008
TRAINING ROOM	**Edgewood**	**Fairlie**	**Hanover C**	**Hanover D**
	Essential Trade Craft for Digital Sleuths	Mac Forensics	Introduction to Cyber Analysis (Cont.)	Linux Incident Response Scripting
TRAINING ROOM	**Hanover E**	**Hanover F**	**International North**	**International South**
	Analyzing Malicious Carrier Files and Common Exploits (Cont.)	Wireless Technology Workshop (Cont.)	Digital Forensics with DCITA LIVE	SANS - Lethal Digital Forensic Techniques and Memory Analysis (Cont.) **LAPTOP REQUIRED**
0830-1630	**AFOSI Meeting (Closed Session)** *Learning Center*		
0930-1015	**Morning Coffee Break** *Conference Level Foyer*		
1400-1445	**Afternoon Break** *Conference Level Foyer*		
1615-1900	**Exhibit Hall Grand Opening Night Reception & NCMEC Silent Auction (Media/Press are welcome to attend)** *Exhibit Hall (Grand Hall)* **Sponsored By: CSC** All attendees are invited to a special reception inside the Exhibit Hall. Don't miss this opportunity to connect with colleagues and learn about the IT products and service solutions that our exhibitors have to offer. Hors d'oeuvres and drinks will be served. See page 90 for details.		
1615-1900	**Visit DC3 Booth 817—Recruiter Available** A DC3 recruiter will be available to discuss employment opportunities at their booth.		

CLASSIFIED SESSION: Cyber Counterintelligence (CI) Briefings

Clearance Check: 0630 | Buses Depart Hotel: NLT 0715 | Pickup for Return Trip: 1600

You must have preregistered and prequalified to attend. Due to the sensitive nature of its content, the session is classified as Secret//NOFORN. This session will have two panel groups and five individuals discussing a range of topics that will include the following:

- Current DoD and DIB APT intrusion events
- Tool Development
- Malware
- Future APT trends
- Cyber CI Policy
- Media exploitation

* These topics are subject to change based on speaker participation.

Important Information

Classified Session attendees must register and pick up a conference badge at the Conference Registration Desk at the Exhibition Level prior to arriving at the clearance checkpoint on Monday morning. Conference Registration is open Sunday until 1800 and opens Monday morning at 0600. On Monday morning, meet at the clearance checkpoint in the hotel (Grand Hall East) at 0630. Please arrive early due to the large number of people attending this session. DC3 staff will verify your conference registration, your clearance, and your government-issued picture ID prior to allowing you to board the bus.

NOTE: Please DO NOT carry cell phones or other PDA devices to the classified session. Cyber CI Briefing registration is limited and restricted to U.S. citizens who possess a SECRET clearance with the United States.

Tuesday, January 24

0700-1700	**Conference Registration/Information Desk** | *Grand Hall Foyer*
0700-1900	**Cyber Café** | *Grand Hall Foyer* **Sponsored By: Guidance Software**
0700-1900	**DC3 Digital Crime Scene Challenge—See page 96 for more information** | *Grand Hall Foyer* **Sponsored By: Booz Allen Hamilton and Forward Discovery**
0700-0745	**Morning Reception** | *Centennial Foyer* **Sponsored By: CompTia and Syngress**
0900-1900	**Exhibit Hall Open** | *Exhibit Hall (Grand Hall)*
0900-1600	**Visit DC3 Booth 817 in the Exhibit Hall—Recruiter Available** A DC3 recruiter will be available to discuss employment opportunities at their booth.
0745-1700	**PLENARY SESSION | Centennial Ballroom I-IV** *(Media/Press are welcome to attend Tuesday's Plenary Session)*
0745-0815	**Opening Presentation: Presentation of the Colors, National Anthem and Opening Remarks** Master of Ceremonies: **Jeff Stutzman**, Director, Department of Defense - Defense Industrial Base Collaborative Information Sharing Environment, Department of Defense Cyber Crime Center | National Anthem Singer: **Lauren-Ashley Blake**, Civilian, Georgia National Guard | Presentation of Colors: **Air Force Honor Guard**, Dobbins Air Force Base, Marietta, Georgia
0815-0845	**Welcome from the Director of DC3** **SA Steven D. Shirley**, Executive Director, Department of Defense Cyber Crime Center
0845-0930	**Six People Who Are Changing the World of Security** **Alan Paller**, Director of Research, SANS Institute
0930-1015	**Morning Coffee Break in the Exhibit Hall** | *Exhibit Hall (Grand Hall)* **Sponsored By: Raytheon**
1015-1025	**U.S. Cyber Challenge** **Renee McLaughlin**, Executive Director, Cybersecurity Workforce Division, Center for Internet Security, and Chair, U.S. Cyber Challenge
1025-1035	**Air Force Association's CyberPatriot National High School Cyber Defense Competition** **Brigadier General (USAF, Ret) Bernie Skoch,** Commissioner, CyberPatriot
1035-1045	**National Collegiate Cyber Defense Competition** **Dr. Gregory White**, Director, Center for Infrastructure Assurance and Security, The University of Texas at San Antonio
1045-1055	**DC3 Digital Forensics Challenge** **Brian C. Andrzejewski**, Outreach Team Lead, Futures Exploration, Department of Defense Cyber Crime Center
1055-1130	**2011 DC3 Digital Forensics Challenge Awards Presentation** **Brian C. Andrzejewski**, Outreach Team Lead, Futures Exploration, Department of Defense Cyber Crime Center **SA Steven D. Shirley**, Executive Director, Department of Defense Cyber Crime Center
1130-1300	**Fiesta-Style Lunch in the Exhibit Hall** | *Exhibit Hall (Grand Hall)* **Sponsored By: Raytheon**
1300-1315	**Announcements** Master of Ceremonies: **Jeffery Stutzman**, Director, Department of Defense - Defense Industrial Base Collaborative Information Sharing Environment, Department of Defense Cyber Crime Center
1315-1400	**Forensics** **Ovie Carroll**, Director, Cybercrime Lab at the Computer Crime and Intellectual Property Section, U.S. Department of Justice
1400-1445	**The Future of Crime** **Marc Goodman**, Global Security Advisor, Singularity University and Founder, Future Crimes Institute
1445-1530	**Dessert Social in the Exhibit Hall** | *Exhibit Hall (Grand Hall)* **Sponsored By: Raytheon**
1530-1615	**Legal Issues in Addressing the Insider Threat** **John Lynch**, Principal Deputy Chief, Computer Crime and Intellectual Property Section, U.S. Department of Justice
1615-1700	**Kingpin: How One Hacker Took Over the Billion-Dollar Cyber Crime Underground** **Kevin Poulsen**, News Editor, Wired.com and Author of Kingpin - How One Hacker Took Over the Billion Dollar Cyber Crime Underground (Crown, 2010) *Kingpin* is available for purchase at the Conference Registration Desk (while supplies last)
1700-1900	**Cyber Crime Stadium Reception—Play sports-related games and win prizes** | *Exhibit Hall (Grand Hall)* **Sponsored By: BAE Systems** See page 90 for details.

Wednesday, January 25

Time		
0730-1700	**Conference Registration/Information Desk** | *Grand Hall Foyer*	
0730-1700	**Cyber Café** | *Grand Hall Foyer* | **Sponsored By: Guidance Software**	
0730-1700	**DC3 Digital Crime Scene Challenge** | *Grand Hall Foyer* | **Sponsored By: Booz Allen Hamilton and Forward Discovery** *(NEW)*	
0715-0830	**Morning Reception (Grab breakfast and take it to Plenary Session)** | *Centennial Foyer* | **Sponsored By: CompTia and Syngress**	
0730-0830	**PLENARY SESSION** | *Centennial Ballroom II-III* **DoD Private Sector Teaming for Dominance** **Eric Hutchins**, Chief Intelligence Analyst, Computer Incident Response Team, Lockheed Martin	
0830-1630	**NCMEC ID Lab** | *Hanover A* (See page 97 for details.) This is not a session and is restricted to Law Enforcement attendees only. Please wear your conference badge and bring proof of identity to gain entry. *(NEW)*	

TRACK	Defense Industrial Base Track			Forensic Track				
LOCATION	**Kennesaw**	**Inman**	**International Ballroom South**	**Centennial Ballroom 1**	**Centennial Ballroom 2-3**	**Centennial Ballroom 4**	**Learning Center**	**Grand Hall A**
0830-0920	How to Give a Winning Security Presentation	Coordination Processes Between Law Enforcement, Counter-Intelligence and Computer Network Defense Organizations	DIB 101	U.S. Cyber Challenge - Cyber Workforce Development Panel	Terrorist Use of Technology: Dissecting the 2008 Mumbai Incident	Cyber Analytics - Network Integrity Testing	Dropbox Forensics	Retrieving Internet Chat History with the Same Ease as a Squirrel Cracks Nuts
0930-1020	Open Meeting Room *See page 26 for details.*	Open Meeting Room *See page 26 for details.*		Identifying and Mitigating Advanced Persistent Threat: A Case Study		Browser Forensics	Decoding Data Exfiltration - Techniques to Understand What Was Taken	Gaining Insight Into Network Skulduggery
1000-1515	**Exhibit Hall Open** | *Exhibit Hall (Grand Hall)*							
1000-1515	**Visit DC3 Booth 817 in the Exhibit Hall—Recruiter Available** | *Exhibit Hall (Grand Hall)* *(NEW)* A DC3 recruiter will be available to discuss employment opportunities at their booth.							
1030-1100	**Morning Coffee Break** | *Exhibit Hall (Grand Hall)* | **Sponsored By: Raytheon**							
1100-1150	Open Meeting Room *See page 26 for details.*	Proactive Threat Identification, What's Working for Us?	Open Meeting Room *See page 26 for details.*	National Centers of Digital Forensic Academic Excellence (CDFAE) *Session Repeats*	Public-Private Partnerships in Cybersecurity Information Sharing	Audits, Triage and the Future of Hashing	Forensic Clusters: Advanced Processing with Open Source Software	Insider Data Theft: Forensics & Investigation
1200-1330	**Italian-Style Lunch and NCMEC Silent Auction Closing (Bidding Ends at 1230)** | *Exhibit Hall (Grand Hall)*							
1330-1700	**DC3 Academic Curriculum Alliance (DACCA) Working Group Session/Closed Session** | *Edgewood* This working group is comprised of DACCA board members and select Subject Matter Experts in the digital forensics education field. The learning objectives and assessment process for the CDFAE program will be the primary objective of the working group.							
1330-1420	Open Meeting Room *See page 26 for details.*	How to Break Web Browsing in Order to Save Your Data	DCISE GoldRush: Automated Analytics Application	DC3 Digital Forensics Challenge: Making Ideas Into Reality	Identifying Malware via Code Reuse	Vulnerabilities In Forensic Software and How to Mitigate Them	So You want to Image RAM	Dropping the Noise Floor in Enterprise Incident Investigations
1430-1500	**Afternoon Break, Raffle Drawing, NCMEC Silent Auction Winners Posted, and Exhibit Hall Closing** | *Exhibit Hall (Grand Hall)* | **Break Sponsored By: Raytheon**							
1500-1550	Today's Social Networking Hack, Tomorrow's Infrastructure Threat (Panel Discussion)	Room being utilized by Forensics Track	Open Meeting Room *See page 26 for details.*	2011 DC3 Digital Forensics Challenge: Winner Presentations	Room being utilized by conference staff	Timeline Analysis Using Log2Timeline with DCITA LIVE	An Overview to Cryptography	Building a Forensic Imaging (Linux) Boot Disk Using SUSE Studio
1600-1650			Cyber Security Front Line: Leveraging Policy Standards to Protect Against Advanced Persistent Threats					Introduction to DCITA LIVE
1700-1900	**Cyber Crime Olympics 2012: Floppy Disk Throw, CD Toss and Pizza Social** | *Centennial Ballroom* | **Sponsored By: CSC and Syngress** *(NEW)* **New This Year:** $5 pizza and salad dinner. Purchase your ticket for the Pizza Social at Conference Registration/Information Desk (while supplies last).							

Wednesday, January 25

Time	Event
0730-1700	**Conference Registration/Information Desk** | *Grand Hall Foyer*
0730-1700	**Cyber Café** | *Grand Hall Foyer* | **Sponsored By: Guidance Software**
0730-1700	**DC3 Digital Crime Scene Challenge** | *Grand Hall Foyer* | Sponsored By: Booz Allen Hamilton and Forward Discovery **NEW**
0715-0830	**Morning Reception (Grab breakfast and take it to Plenary Session)** | *Centennial Foyer* | Sponsored By: CompTia and Syngress
0730-0830	**PLENARY SESSION** | *Centennial Ballroom II-III* **DoD Private Sector Teaming for Dominance** **Eric Hutchins**, Chief Intelligence Analyst, Computer Incident Response Team, Lockheed Martin
0830-1630	**NCMEC ID Lab** | *Hanover A* (See page 97 for details.) **NEW** This is not a session and is restricted to Law Enforcement attendees only. Please wear your conference badge and bring proof of identity to gain entry.

TRACK	Forensic Track			Information Assurance Track			Law Enforcement/ Criminal Investigators (LE/CI) Track			Legal Track		Research & Development Track (R&D)	
LOCATION	Grand Hall B	Hanover E	Inman	Grand Hall C	Grand Hall D	International Ballroom North	Hanover C-D	Hanover F-G	Fairlie	Auburn	Baker	Courtland	Dunwoody
0830-0920	Timeline Analysis	Is Your Tool Bag Too Big?	Room being utilized by Defense Industrial Base Track	Own the Network, Own the Data (LEO Only)	Open Meeting Room *See page 26 for details.*	Database Security in the Cloud *Session Repeats*	Smile for the Grenade! Camera go Bang!	Operational and Investigative Information Sharing and Coordination	Open Meeting Room *See page 26 for details.*	Effective Expert Witness Testimony	Getting Electronic Evidence from Foreign Countries	Malicious Code Automated Run-Time Analysis	LBS: Building Location Profiles from a Mobile Device
0930-1020				Metasploit on the iPad			The Wild, Wild Web: Knowing the Basics for Online Investigations *Session Repeats*	Open Meeting Room *See page 26 for details.*		Next Generation Forensically Sound Collection	The Top Ten Most Important Cases Affecting Digital Forensics and Digital Evidence in 2011	An Introduction to More Advanced Steganography *Session Continues thru 1200*	Cake and Grief Counseling Available: Artificial Intel for Forensics Without Jeopardizing Humanity *Session Repeats*
1000-1515	**Exhibit Hall Open** | *Exhibit Hall (Grand Hall)*												
1000-1515	**Visit DC3 Booth 817 in the Exhibit Hall—Recruiter Available** | *Exhibit Hall (Grand Hall)* **NEW** A DC3 recruiter will be available to discuss employment opportunities at their booth.												
1030-1100	**Morning Coffee Break** | *Exhibit Hall (Grand Hall)* | Sponsored By: Raytheon												
1100-1150	Detection of Insider Turning Behaviors With Forensic Methods	How Private is Your Browsing?	Room being utilized by Defense Industrial Base Track	Network Intrusion and Malware Visualization	Critical Line of Cyber Defense - Employees	Let me Hijack Your Workstation - You're an Active Directory Administrator, Right?	If a Picture is Worth a Thousand Words, What are a Thousand Pictures Worth?	Estimation of Victim Age in Child Pornography and Child Sexual Exploitation Investigations	Open Meeting Room *See page 26 for details.*	First Thing We Do, Let's Kill all the Lawyers	Dissecting the Triage—A Lawyers' and Agents' Guide to The DCFL Forensic Extraction Program	An Introduction to More Advanced Steganography *Continued Session*	Reverse Engineering Made Easy with Hydra
1200-1330	**Italian-Style Lunch and NCMEC Silent Auction Closing (Bidding Ends at 1230)** | *Exhibit Hall (Grand Hall)*												
1330-1700	**DC3 Academic Curriculum Alliance (DACCA) Working Group Session/Closed Session** | *Edgewood* This working group is comprised of DACCA board members and select Subject Matter Experts in the digital forensics education field. The learning objectives and assessment process for the CDFAE program will be the primary objective of the working group.												
1330-1420	Android Rootkit Detection and Volatile Memory Forensics	Mac Forensics (A Look at Lion)	Room being utilized by Defense Industrial Base Track	Introduction to Cellular Networking	Registry Analysis for Network Intrusions	Stopping the Leak: Insider Threat Detection Through Effective Cyber Auditing	Investigating the Cloud is a Piece of Cake	Emerging Mobile Security Threats: The Past, The Present and The Future	Open Meeting Room *See page 26 for details.*	Hacking Back in Self-Defense: Is it Legal; Should it Be?	Using Demonstrative Evidence in Digital Evidence Cases	Malware Analysis on Windows: Tools and Techniques	Exploring the Social Dynamics of Stolen Data Markets
1430-1500	**Afternoon Break, Raffle Drawing, NCMEC Silent Auction Winners Posted, and Exhibit Hall Closing** | *Exhibit Hall (Grand Hall)* | Break Sponsored By: Raytheon												
1500-1550	Vehicle Embedded System Imaging & Extraction and Examination	Virtualization and Forensics	Harbinger of Evil: The Forensic Art of Finding Malware	Changing APT Tactics: Anatomy of an Attack by Today's Adaptive Adversaries	Database Security in the Cloud *Repeat Session*	Countering Government-Sponsored Cyber Attacks	Decloaking the Enemy	The Wild, Wild Web: Knowing the Basics for Online Investigations *Repeat Session*	Open Meeting Room *See page 26 for details.*	A Day in the life of an AFOSI Cyber Investigator	Going Mobile	Foreign Language Detection in Malware Data-analysis for Forensic Engineers	Software Requirements Specification for Digital Forensics Software Tools
1600-1650	Open Meeting Room *See page 26 for details.*		Using Emerging Threat Snort Rules to Better Detect Network Threats		Professional Network Security Monitoring on a Shoestring Budget	Automated Log File Analysis as Triage for eCrime First Responders	Geo-Tagging with the Eye-Fi Card			Dueling Banners: What's New with the DoD and IC Banners?	Cyber Vigilantes: How Security Researchers Are Hurting the Business of Hacking	Automating Repetitive Tasks Using Memory Introspection
1700-1900	**Cyber Crime Olympics 2012: Floppy Disk Throw, CD Toss and Pizza Social** | *Centennial Ballroom* | Sponsored By: CSC and Syngress **NEW** New This Year: $5 pizza and salad dinner. Purchase your ticket for the Pizza Social at Conference Registration/Information Desk (while supplies last).												

	Thursday, January 26
0730-1700	**Conference Registration/Information Desk**	*Grand Hall Foyer*
0730-1700	**Cyber Café**	*Grand Hall Foyer*	Sponsored By: Guidance Software
0730-1200	**DC3 Digital Crime Scene Challenge**	*Grand Hall Foyer*	Sponsored By: Booz Allen Hamilton and Forward Discovery **NEW**
0730-0830	**Morning Reception**	*Centennial Foyer*	Sponsored By: CompTia and Syngress
0830-1630	**NCMEC ID Lab**	*Hanover A* — This is not a session and is restricted to Law Enforcement attendees only. Please wear your conference badge and bring proof of identity to gain entry. See page 97 for details. **NEW**
0730-1700	**Defense Crime Center Tool Expo**	*Centennial Foyer* — Unique opportunity to demo DC3 developed free tools, speak directly to the developers, and provide feedback. See page 94 for details.
0830-1700	**DC3 Academic Curriculum Alliance (DACCA) Working Group Session/Closed Session**	*Edgewood*	This working group is comprised of DACCA board members and select Subject Matter Experts in the digital forensics education field. The learning objectives and assessment process for the CDFAE program will be the primary objective of the working group.

TRACK	Defense Industrial Base Track			Forensic Track									Information Assurance Track		
LOCATION	Kennesaw	Inman	International Ballroom South	Centennial Ballroom 1	Centennial Ballroom 2-3	Centennial Ballroom 4	Learning Center	Grand Hall A	Grand Hall B	Hanover E	Hanover F-G	Hanover C-D	Grand Hall C	Grand Hall D	Inman
0830-0920	Key Ingredients for Building a More Resilient Security Program *Session Continues through 1150*	Open Meeting Room *See page 26 for details.*	Open Meeting Room *See page 26 for details.*	Next-Generation Decryption	Advanced Persistent Threats: War Stories from the Front Lines	Building America's Cyber Warriors Panel Discussion	DCCI Segfrensic Tools	Live Acquisition and Triage - Catch 'Em In The Act	The Digital Forensics Cyber Exchange Principle	iOS Device: Seizure and Analysis *Session Continues through 1200*	Accessing OS X File Vault *Session Repeats*	Room utilized by the LE/CI Track during this session	Practical Application White-Listing in Windows, Mac, and Linux	New Technology for the Improved Handling of Advanced Exploits	Room utilized by the DIB Track during this session
0930-1020		Room utilized by the IA Track during this session	Sophisticated Techniques, Tactics and Procedures (TTPs) Employed by Wekby* and Methods for Mitigation	Analyzing the Knockoffs: MediaTek-Based Phones				Mac, Beyond the GUI: Understanding Where to Look to Uncover System Artifacts	Car Forensics		Hacking Stuff Round II		Data Breach - How the Bad Guys are Eating Our Lunch *Session Repeats*		Adding Network Flow analysis to Your Security Architecture *Session Repeats*
1030-1100	**Morning Coffee Break**	*Centennial Foyer*	Sponsored By: Raytheon												
1100-1150	Key Ingredients for Building a More Resilient Security Program *Continued Session*	Room utilized by the IA Track during this session	Restoring Credential Integrity after an APT Intrusion	Building Trusted Tool Kit 🖧	How the Cookie Crumbles	The Color of a Forensicator's Parachute: Professional Development and Retainment Panel	Skype Forensics	Password Cracking	APT Attacks and Proactive Inside-Out Security Approaches For Protecting Internal Data and Information	iOS Device: Seizure and Analysis *Continued Session*	Room utilized by the LE/CI Track during this session	Room utilized by the LE/CI Track during this session	Introduction to Metasploit Wireless Tools	Open Meeting Room *See page 26 for details.*	You're About to Fire John. Don't Let Him Walk off with Your Data
1200-1330	**Lunch On Your Own**														
1330-1420	Moving from Crime Scene Investigators to Pre-Crime Oracles	Living In a Constant State of Cyber Insecurity	Open Meeting Room *See page 26 for details.*	Solid State Drives: Past, Present and Future	Advanced Acquisition Techniques	iDevices: An Overview of Forensics Techniques 🖧	Obfuscating Data in Docx Files	Forensic Imaging Workshop *Session Continues through 1700*	Countering the Anti-Forensics of Timestomping	Drive Prophet Triage Tool	Room utilized by the LE/CI Track during this session	Room utilized by the LE/CI Track during this session	A Net Defender's Guide to the PRC's State-Developed Linux Distribution	Red & Blue Security Readiness Testing —Beyond Compliance	Room utilized by the DIB Track during this session
1430-1500	**Afternoon Break**	*Centennial Foyer*	Sponsored By: Raytheon												
1500-1550	Defense Industrial Base - Supply Chain Cyber Path *Session Repeats*	Room utilized by the IA Track during this session	Rapid Engineering for Incident Response	Malware Analysis and Final Report Generation	Reverse Engineering Mobile Malware	Demystifying GREP Expressions 2012	Data Hiding and Steganography, 21st Century Innovations	Forensic Imaging Workshop *Continued Session*	High School Digital Forensic Clubs Program	Device Tracking with Geolocation Artifacts	Room utilized by the LE/CI Track during this session	Room utilized by the LE/CI Track during this session	Security and Identity Management for IP-Based Systems	Developing Standardized Processes for Incident Response: Challenges and Opportunities	The Realities of Investigating Social Media
1600-1650	Room utilized by the IA Track during this session	Open Meeting Room *See page 26 for details.*	Open Meeting Room *See page 26 for details.*	Open Meeting Room *See page 26 for details.*	Acquisition and Forensic Examination of a Nook Color *Session Repeats*	Tag You're IT 🖧			Creating the "Perfect" Live CD For Forensics/ Incident Response (Or How to Roll Your Own Live CD)	An Application Footprint Reference Set: Tracking the Lifetime of Software	Hacking 2011: Lessons for 2012		White-Listing to Protect Your Network *Session Repeats*		Open Meeting Room *See page 26 for details.*
1700-1830	**Birds of a Feather Sessions** (See pages 25-26 for the complete list of sessions and locations)														

Thursday, January 26

Time	Event
0730-1700	**Conference Registration/Information Desk** | *Grand Hall Foyer*
0730-1700	**Cyber Café** | *Grand Hall Foyer* | **Sponsored By: Guidance Software**
0730-1200	**DC3 Digital Crime Scene Challenge** | *Grand Hall Foyer* | **Sponsored By: Booz Allen Hamilton and Forward Discovery** [NEW]
0730-0830	**Morning Reception** | *Centennial Foyer* | **Sponsored By: CompTia and Syngress**
0830-1630	**NCMEC ID Lab** | *Hanover A* [NEW] This is not a session and is restricted to Law Enforcement attendees only. Please wear your conference badge and bring proof of identity to gain entry.
0730-1700	**Defense Crime Center Tool Expo** | *Centennial Foyer* Unique opportunity to demo DC3 developed free tools, speak directly to the developers, and provide feedback. See page 94 for details.
0830-1700	**DC3 Academic Curriculum Alliance (DACCA) Working Group Session/Closed Session** | *Edgewood* This working group is comprised of DACCA board members and select Subject Matter Experts in the digital forensics education field. The learning objectives and assessment process for the CDFAE program will be the primary objective of the working group.

TRACK	Information Assurance Track		Law Enforcement/Criminal Investigators (LE/CI)			Legal Track		Research & Development Track (R&D)	
LOCATION	International Ballroom North	Kennesaw	Hanover C-D	Hanover F-G	Fairlie	Auburn	Baker	Courtland	Dunwoody
0830-0920	Open Meeting Room See page 26 for details.	Room utilized by the DIB Track during this session	National Repository for Digital Forensic Intelligence (NRDFI)	Room utilized by the Forensics Track during this session	Open Meeting Room See page 26 for details.	20+ Ways to Improve Digital Evidence and Cyber Crime Trials	Obtaining Electronic Evidence from Service Providers: An ECPA Primer	NetHunter: On-the-Fly, High-Speed, Enterprise Network Forensic Analyzer	Protocol Reverse-Engineering with REcat
0930-1020	All sides of Android, il buono, il brutto, il cattivo		DCFL Operations: "What Happens To My Case When It Goes to DCFL?"				Confronting Forensic Digital Evidence in Light of Recent Sixth Amendment Jurisprudence	Cake and Grief Counseling Available: Artificial Intel for Forensics Without Jeopardizing Humanity *Repeat Session*	Registry Decoder: Automated Acquisition and Investigation of the Windows Registry
1030-1100	**Morning Coffee Break** | *Centennial Foyer* | **Sponsored By: Raytheon**								
1100-1150	The Zero-Trust Approach to IT Access: Eliminating Trust to Achieve Security	Room utilized by the DIB Track during this session	Facebook/Twitter Investigations	Leveraging Data Retention Technologies for Cyber Forensic Investigations on Large-Scale Networks	Open Meeting Room See page 26 for details.	Cloudy with a Chance of Pain: The Trials and Tribulations of a Cloud Environment	What is 68b of Article 134?	Empirical Intelligence Valuation Through Indicator Volatility Analysis	Forensic Acquisition Techniques for Cloud Computing
1200-1330	**Lunch On Your Own**								
1330-1420	A Token Defense: Effects of the RSA SecurID Breach on Network Security, and How Devise Identity Can Help	Room utilized by the DIB Track during this session	Introduction to Honeypots	Maltego as an Open Source Information Gathering Platform	Open Meeting Room See page 26 for details.	A Guide to Department of Defense Cyber Crime Institute Test and Validation Process and Reports	In the Path of Heracles: Admissibility of Digital and Multimedia Evidence	Mac OS X and Linux Physical Memory Acquisition and Analysis	Modeling Civilian Participation in Political Conflicts On- and Off-Line
1430-1500	**Afternoon Break** | *Centennial Foyer* | **Sponsored By: Raytheon**								
1500-1550	Case Study: The Advance Persistent Threat *Session Repeats*	Room utilized by the DIB Track during this session	Digital Character Assessment as an Investigation Accelerator	Using Data Analytics in Missing & Exploited Children Cases	Open Meeting Room See page 26 for details.	Digital Evidence Trial Preparation Part II	Encryption: A Primer for Prosecutors	On the Random Hawtness Theatre and an Ethics For Porn	Patterns in Social Networks and Advancements in Analytical Research Methods
1600-1650	Increasing Security and Compliance with a 360-Degree View of User Activity	Social Media and the Department of Defense Insecurities, Technological Cultural Challenges and Potential Solutions	Room utilized by the Forensics Track during this session	Room utilized by the Forensics Track during this session		Encryption: How it Impacts Privacy and Investigations	Search Incident to Arrest in the Digital Age	IPv6: The Future Is Now. Routing, LANS, and Wireshark	Open Meeting Room See page 26 for details.
1700-1830	**Birds of a Feather Sessions** (See pages 25-26 for the complete list of sessions and locations)								

Friday, January 27

0730-1200	**Conference Registration/Information Desk** | *Grand Hall Foyer*
0700-1200	**Cyber Café** | *Grand Hall Foyer* | **Sponsored By: Guidance Software**
0700-0800	**Morning Reception** | *Centennial Foyer* | **Sponsored By: CompTia and Syngress** Grab breakfast and take it to Plenary Session
0730-0850	**PLENARY SESSION** | *Centennial Ballroom II-III* **Cyber Crime Survivor Game, Olympic Awards, Closing Remarks, and Closing Video**
0800-1000	**NCMEC ID Lab** | *Hanover A* NEW This is not a session and is restricted to Law Enforcement attendees only. Please wear your conference badge and bring proof of identity to gain entry. See page 97 for details.
0900-1200	**Digital Evidence Mock Trial Demonstration** | *Learning Center* See page 97 for details.

TRACK	Defense Industrial Base Track		Forensic Track						
LOCATION	**Kennesaw**	**Inman**	**Baker**	**Centennial Ballroom 1**	**Centennial Ballroom 2-3**	**Centennial Ballroom 4**	**Grand Hall A**	**Grand Hall B**	**Hanover E**
0900-0950	Defense Industrial Base—Supply Chain Cyber Path *Repeat Session*	How DHS, Commercial and Private Coders Created the Next Generation IDS/IPS Engine and Released it as Open Source	Exploiting Facebook Artifacts	Forensic Acquisition of Virtual Servers	APT Hangover: How to Find Out What Happened	Considerations for Forensic Acquisition of Solid-State Drives	Entropy Near-Match Analysis for Improved Detection in Malware Across and Enterprise	Hands-on Registry Analysis and Data Point Correlation	Backup File Forensics
1000-1050	Transforming the Security Operations Center to a Security Intelligence Center	Cyberwar Threats and Defenses	Shadow Warriors —A Tour of Vista/Windows7 Volume Shadow Copy	Full System State Extraction Using Hypervisors	Data Mining	Interactive Game Training for Digital Forensics and Cyber Investigation	Acquisition and Forensic Examination of a Nook Color *Repeat Session*	Accessing OS X File Vault *Repeat Session*	
1100-1150	Strategy Execution for Cyber Defense—For the 10% That Will Succeed	Room utilized by Forensics Track during this session	Room utilized by Information Assurance Track during this session	Memory Forensics in Linux Incident Response	Advanced Persistent Threats: Leading the Wave of Cybercrime	Lion, Snow Leopard, and Leopard, Oh My!	Reverse Engineering Cryptographic Routines in Steganography Programs	Demystifying the Host Protected Area	Bitcoins and Distributed Banking. What About the Money Trail?
1200	**Conference Concludes—Thanks For Attending!**								

DC3 Is Hiring!

We're looking for hard-charging intelligence analysts, computer scientists, computer engineers, forensic examiners, IT specialists, cyber analysts, and cyber instructors who thrive on challenging and meaningful work in a dynamic environment. Candidates must be U.S. citizens.

DC3 offers generous family-friendly benefits, access to courses offered by our in-house training academy, use of cutting-edge technology, and much more. **Stop by the DC3 booth 817 in the Exhibit Hall** on Tuesday 0900-1600 and Wednesday 1000-1515 to learn more about our employment opportunities.

Friday, January 27

0730-1200	**Conference Registration/Information Desk**	*Grand Hall Foyer*
0700-1200	**Cyber Café**	*Grand Hall Foyer*	**Sponsored By: Guidance Software**
0700-0800	**Morning Reception**	*Centennial Foyer*	**Sponsored By: CompTia and Syngress** Grab breakfast and take it to Plenary Session
0730-0850	**PLENARY SESSION**	*Centennial Ballroom II-III* **Cyber Crime Survivor Game, Olympic Awards, Closing Remarks, and Closing Video**
0800-1000	**NCMEC ID Lab**	*Hanover A* **NEW** This is not a session and is restricted to Law Enforcement attendees only. Please wear your conference badge and bring proof of identity to gain entry. See page 97 for details.
0900-1200	**Digital Evidence Mock Trial Demonstration**	*Learning Center* See page 97 for details.

TRACK	Forensic Track			Information Assurance Track			Law Enforcement/ Criminal Investigators (LE/CI)		Legal Track	Research & Development Track (R&D)
LOCATION	Hanover C-D	Hanover F-G	Inman	Baker	Grand Hall C	Grand Hall D	Hanover C-D	Hanover F-G	Learning Center	Dunwoody
0900-0950	Room utilized by LE/CI Track during this session	Room utilized by LE/CI Track during this session	Room utilized by DIB Track during this session	Room utilized by Forensics Track during this session	Network Forensics for Cyber Security	Adding Network Flow Analysis to Your Security Architecture *Repeat Session*	The Expert in the Room: Feed-Forward Situational Awareness	Understanding Network Data Access Technologies for Forensically Sound Collection	Digital Evidence Mock Trial Demonstration *See page 97 for details.*	PCAPFAST: Coping with Large Network Traffic Captures
1000-1050	Room utilized by LE/CI Track during this session	Room utilized by LE/CI Track during this session	Room utilized by DIB Track during this session	Room utilized by Forensics Track during this session	Case Study: The Advance Persistent Threat *Repeat Session*	Data Breach - How the Bad Guys are Eating Our Lunch - *Repeat Session*	Role of Counter-intelligence in the Digital Environment	Intelligence Gathering Over Twitter		Carving 3GP Videos
1100-1150	National Centers of Forensic Academic Excellence (CDFAE) Update *Repeat Session*	SQLite Database Forensics	Advances in the Sleuth Kit and Autopsy 3 Open Source Forensic Tools	Top 5 Reasons Your Incident Response Program Fails	White-Listing to Protect Your Network *Repeat Session*	Splunk as an Enterprise Incident Response and Forensic Tool	Room utilized by Forensics Track during this session	Room utilized by Forensics Track during this session		Visualizing Change-Over-Time to Support Digital Forensics
1200	**Conference Concludes—Thanks For Attending!**									