Agenda at a Glance

Organization Abbreviations

DC3: DoD Cyber Crime Center
DCFL: Defense Computer Forensics Laboratory
DCITA: Defense Cyber Investigations Training Academy
JTF-GNO: Joint Task Force Global Network Operations

	Thursday, January 21	
All Day	Travel Day	
1600–2000	Conference Registration	Landmark Foyer
	Friday, January 22	
0700–1700	Conference Registration	Landmark Foyer
0730–0830	Morning Reception	Landmark Foyer
0830–1630	PRE-CONFERENCE TRAINING ▶ See Pre-Conference Training Agenda on page 10	
	Saturday, January 23	
0700–1700	Conference Registration	Landmark Foyer
0730–0830	Morning Reception	Landmark Foyer
0830–1630	PRE-CONFERENCE TRAINING ▶ See Pre-Conference Training Agenda on page 10	
	Sunday, January 24	
0700–2000	Conference Registration	Landmark Foyer
1000–1900	Cyber Café Sponsored By: Guidance Software, Inc.	Majestic Foyer
0730–0830	Morning Reception	Landmark Foyer
0830–1630	PRE-CONFERENCE TRAINING ▶ See Pre-Conference Training Agenda on page 10	
	Monday, January 25	
0615–1700	Conference Registration	Landmark Foyer
1000–1900	Cyber Café Sponsored By: **Guidance Software, Inc.**	Majestic Foyer
0730–0830	Morning Reception	Landmark Foyer
0800–1600	Classified Session All attendees must be downstairs on the Washington Blvd. side of the Landmark Foyer by 0615. Buses will depart NLT 0645. You must already have your conference badge and have checked into registration by 0615. ALL ATTENDEES MUST POSSESS THE APPROPRIATE SECRET U.S. CLEARANCE	Scott AFB
0830–1630	PRE-CONFERENCE TRAINING ▶ See Pre-Conference Training Agenda on page 10	
1600–1800	Opening Night Reception—It's Five O'Clock Somewhere (Media/Press invited) See page 69 for details. Network with Attendees and Visit Exhibits **SILENT AUCTION BEGINS** Sponsored By: **CSC**	Exhibit Areas (Majestic A-D, Majestic Foyer and Landmark Foyer)

Agenda at a Glance

Tuesday, January 26

0700–1700	Conference Registration	Landmark Foyer
0645–2100	Cyber Café Sponsored By: Guidance Software, Inc.	Majestic Foyer
0700–0745	Morning Reception	Exhibit Areas (Majestic A-D and Majestic Foyer)
0700–1900	Exposition Open (Please note: Exhibit Areas are closed during sessions) Tuesday Only Special Raffle Visit all exhibitors on the Landmark Level and put into a special raffle to win a Kindle and a $25 Amazon.com Gift Card, a Wii or a Blu-Ray DVD Player! See page 71 for details.	Exhibit Areas (Majestic A-D, Majestic Foyer and Landmark Foyer)
PLENARY SESSION (Majestic E-H)		
0745–0815	Opening Presentation Master of Ceremonies: William M. Jimenez, Director of Staff and Business Operations, Department of Defense Cyber Crime Center (DC3) National Anthem: Chief Master Sergeant Robert "Bob" Ellison, USAF (Ret)	
0815–0845	Welcome from the Director of DC3 SA Steven D. Shirley, Executive Director, Department of Defense Cyber Crime Center (DC3)	
0845–0930	Investigating and Prosecuting Cybercrime: A Cornerstone of Cybersecurity Jason M. Weinstein, Deputy Assistant Attorney General, Department of Justice's Criminal Division	
0930–1015	Morning Coffee Break Sponsored By: **Sky Catcher Solutions**	Exhibit Areas (Majestic A-D and Majestic Foyer)
1015–1055	DC3 Digital Forensic Challenge Award SA Steven D. Shirley, Executive Director, Department of Defense Cyber Crime Center (DC3) Randy Georgieff, Section Lead Digital Forensics Challenge, Futures Exploration (FX), Defense Cyber Crime Center (DC3)	
1055–1130	Surprisingly Effective Leverage Points for Large Scale Cyber Security Improvements Alan Paller, Director of Research, SANS Institute	
1130–1300	Exposition Luncheon See page 68 for menu	Exhibit Areas (Majestic A-D and Majestic Foyer)
1300–1305	"America the Beautiful" Chief Master Sergeant Robert "Bob" Ellison, USAF (Ret)	
1305–1320	Announcements Master of Ceremonies: William M. Jimenez, Director of Staff and Business Operations, Department of Defense Cyber Crime Center (DC3)	
1320–1420	The Cybersecurity Imperative Melissa E. Hathaway, President, Hathaway Global Strategies, LLC and Senior Advisor at Harvard Kennedy School's Belfer Center	
1420–1500	Dessert Social Sponsored by: **Sky Catcher**	Exhibit Areas (Majestic A-D and Majestic Foyer)
1500–1600	Who Moved My Cheese? Why the Security Industry Has Been Turned Upside Down John N. Stewart, Vice President and Chief Security Officer, Cisco Systems, Inc	
1600–1700	Keynote Presentation: The Cyber Crime Comedy Hour Don McMillian, Chief Comedy Officer, Technically Funny, Inc.	
1700–1900	Tuesday Night Reception: Cyber Crime Investigation (Media/Press invited) See page 70 for details. Sponsors: **Bit9** | **Wiebe Tech, a brand of CRU-DataPort** | **CSC** | **EADS NA Defense Security and Systems Solutions, Inc.** | **General Dynamics** | **Intelligent Computer Solutions, Inc.** | **Lockheed Martin Corporation**	Exhibit Areas (Majestic A-D, Majestic Foyer and Landmark Foyer)
1800	Tuesday Special Raffle See page 71 for details.	Exhibit Area on the Landmark Level
1900–2100	Cyber Olympics 2010— Floppy Disk Throw and CD Toss **Proceeds Go To the National Center for Missing and Exploited Children (NCMEC)** Sponsors: **CSC** | **High Tech Crime Institute, Inc** | **Sky Catcher Solutions**	Majestic E-H

Agenda at a Glance

Organization Abbreviations

DC3: DoD Cyber Crime Center
DCFL: Defense Computer Forensics Laboratory
DCITA: Defense Cyber Investigations Training Academy
JTF-GNO: Joint Task Force Global Network Operations

Wednesday, January 27

0730–1700	Conference Registration	Landmark Foyer
0730–2100	Cyber Café Sponsored By: Guidance Software, Inc.	Majestic Foyer
0730–0830	Morning Reception	Exhibit Areas (Majestic A-D and Majestic Foyer)
0730–1240	Exposition Open	Exhibit Areas (Majestic A-D, Majestic Foyer and Landmark Foyer)
0830–1020	MORNING BREAKOUT SESSIONS ▶ See Breakout Session Agenda on page 12	
1020–1050	Morning Coffee Break Sponsored By: **Sky Catcher Solutions**	Exhibit Areas (Majestic A-D and Majestic Foyer)
1050–1140	MORNING BREAKOUT SESSIONS (Continued) ▶ See Breakout Session Agenda on page 12	
1140–1240	$5 Lunch, Raffle Drawing, Silent Auction and Exposition Closing Win Fabulous Prizes in the Raffle and Raise Money for Charity! Please purchase lunch tickets in advance $5 at Registration Desk; Raffle Winners Announced 1220 and Silent Auction Closes 1200	Exhibit Areas (Majestic A-D, Majestic Foyer and Landmark Foyer)
1240–1620	AFTERNOON BREAKOUT SESSIONS ▶ See Breakout Session Agenda on pages 13–14	
1400–1500	Beverages & Snacks Available	Landmark Foyer
1630–1830	Birds of a Feather Sessions ▶ See Birds of a Feather Agenda page 21	

Thursday, January 28

0730–1700	Conference Registration	Landmark Foyer
0700–2100	Cyber Café Sponsored By: Guidance Software, Inc.	Majestic Foyer
0730–0830	Morning Reception	Landmark Foyer
0830–1130	MORNING BREAKOUT SESSIONS ▶ See Breakout Session Agenda on pages 14–15	
1000–1100	Beverages Available	Landmark Foyer
1130–1230	Lunch On Your Own	
1230–1630	AFTERNOON BREAKOUT SESSIONS ▶ See Breakout Session Agenda on pages 15–16	
1400–1500	Beverages & Snacks Available	Landmark Foyer
1630–1830	Birds of a Feather Sessions ▶ See Birds of a Feather Agenda page 22	

Friday, January 29

0730–1200	Information Desk	Landmark Foyer
0700–1300	Cyber Café Sponsored By: Guidance Software, Inc.	Majestic Foyer
0700–0800	Morning Reception	Majestic Foyer

PLENARY SESSION (Majestic E-H)

0730–0855	Closing Remarks & Cyber Crime Survivor Game (Top 3 Olympic Participants) (Olympic Results/Awards and Closing Video will start at 0800)	Majestic E-H
0900–1200	MORNING BREAKOUT SESSIONS ▶ See Breakout Session Agenda on page 17	
1200–1300	Lunch On Your Own	

Pre-Conference Training Agenda

PRE-CONFERENCE TRAINING				
LOCATION	FRIDAY	SATURDAY	SUNDAY	MONDAY
Landmark Foyer	0930–1015: Beverage Break (Sponsored By: **Sky Catcher Solutions)**			
	1130–1230: Lunch On Your Own			
	1400–1445: Coffee/Refreshments Break (Sponsored By: **Sky Catcher Solutions)**			
0830–1630				
Landmark 1	Intro to EnCase for Prosecutors & Case Agents *Bryan Spano & Malcolm Smith* REPEATS MONDAY	Intro to Metasploit *Jesse Varsalone & Steven Bolt* REPEATS SUNDAY	Intro to Metasploit *Jesse Varsalone & Steven Bolt*	Intro to EnCase for Prosecutors & Case Agents *Bryan Spano & Malcolm Smith*
Landmark 2	Intro to Malware Analysis *Matt McFadden & Mike Cowan* REPEATS MONDAY	SNORT for Network Analysis *Joe Fichera & Ernie Krutzsh* REPEATS SUNDAY	SNORT for Network Analysis *Joe Fichera & Ernie Krutzsh*	Intro to Malware Analysis *Matt McFadden & Mike Cowan*
Landmark 3	Live System Data Capture *Dave Gilbert & Dan Raygoza* REPEATS SUNDAY-MONDAY		Live System Data Capture *Dave Gilbert & Dan Raygoza*	
Landmark 4	JTF-GNO Computer Network Threat Course *Vernon Howell & Daniel Lohin* REPEATS SUNDAY-MONDAY		JTF-GNO Computer Network Threat Course *Vernon Howell & Daniel Lohin* REPEATS SUNDAY-MONDAY	
Landmark 5	Windows Incident Response *Mike Moore & Dave DeMaio* REPEATS SUNDAY-MONDAY		Windows Incident Response *Mike Moore & Dave DeMaio*	
Landmark 6	Wireless Technology Workshop *Martin Easton & Joshua Elwell* REPEATS SUNDAY-MONDAY		Wireless Technology Workshop *Martin Easton & Joshua Elwell*	
Shaw	Intro to Network Monitoring *Ron de Leos & Andrew Ingraham* REPEATS SUNDAY-MONDAY		Intro to Network Monitoring *Ron de Leos & Andrew Ingraham*	
Westmoreland	Mac Forensics *Lucus Nelson & Casey Szyper* REPEATS SUNDAY-MONDAY		Mac Forensics *Lucus Nelson & Casey Szyper*	
Parkview/Aubert	Introduction to Wireshark *Kelly Brown & Frank Wood* REPEATS SUNDAY-MONDAY		Introduction to Wireshark *Kelly Brown & Frank Wood*	
Hawthorne	Command Line Log Analysis & Graphical Reporting *Don Ranta & Brian Baskin* REPEATS SUNDAY-MONDAY		Command Line Log Analysis & Graphical Reporting *Don Ranta & Brian Baskin*	
Landmark 7		Windows 7: A First Look *Mark Neno & Alissa Torres* REPEATS SUNDAY	Windows 7: A First Look *Mark Neno & Alissa Torres*	
Portland/ Benton (Hotel Side)	Open Source Forensic Tools *Jesse Varsalone & Steven Bolt* REPEATS MONDAY	Insider Threat Workshop: Management, Human Resources, and Information Technology—Working Together to Prevent or Detect Insider Threats *Dawn Cappelli & Randall Trzeciak*		Open Source Forensic Tools *Jesse Varsalone & Steven Bolt*
Scott AFB				Classified Session

Breakout Session Agenda—Wednesday

WEDNESDAY MORNING

0700–1700 Conference Registration (Landmark Foyer)
0700–0800 Morning Reception (Majestic A-D and Foyer)
0700–2100 Cyber Cafe (Majectic Foyer) *Sponsored by Guidance Software, Inc.*

Location	0830–0920	0930–1020	1020–1050	1050–1140
LAW ENFORCEMENT				
Landmark 1	Intentional Radio Interference Investigation and Prosecution—US vs. Rajib Mitra Case Study *Detective Cindy Murphy, Madison PD*		MORNING COFFEE BREAK Sponsored by: **Sky Catcher Solutions**	BotNets: A Case Study & Lessons Learned *Ryan Pittman, U.S. Army Criminal Investigation Command* LAW ENFORCEMENT ONLY
Landmark 2	A Beginner's Guide to Mobile Phone Forensics & Investigations *Detective Jeff Shackelford, SEMO Cyber Crimes Task Force*	Beyond Google Hacking *Jesse Varsalone, DCITA* FOUO		Cyber Investigation Search Kit *Joseph Fichera, DCITA* FOUO
RESEARCH & DEVELOPMENT				
Landmark 3	Recycle Bin Forensics within a Windows 7 and Windows Vista Shadow Volume *Timothy Leschke, DCCI* REPEATS FRIDAY	Shadow Miner: A Tool for Vista Shadow Volume Forensics *Timothy Leschke, DCCI*	MORNING COFFEE BREAK Sponsored by: **Sky Catcher Solutions**	Automating Recycle Bin Forensics within a Windows 7 and Windows Vista Shadow Volume with C# *Timothy Leschke, DCCI*
INFORMATION ASSURANCE				
Landmark 4	Cloud Computing Taxonomies: Associated Risks and Implications for IT *Dennis Hurst, Hewlett-Packard Software*	Who's Watching the Net: The Risk of Victimization with Public Access WiFi *Irv Schlanger, Drexel University and Dr. Robert D'Ovidio, Drexel University*	MORNING COFFEE BREAK Sponsored by: **Sky Catcher Solutions**	Learning by Breaking: A New Project for Insecure Web Applications *Chuck Willis, MANDIANT*
FORENSICS				
Landmark 5	An Overview of Cryptography *Gary Kessler, Gary Kessler Associates/VT ICAC*		MORNING COFFEE BREAK Sponsored by: **Sky Catcher Solutions**	Backup Tape Forensics *Dr. Gavin Manes, Avansic & Michael Harvey, Avansic*
Landmark 6	DC3 Cyber Crime Center's Digital Forensics Challenge *Randy Georgieff, DC3/FX*			Grand Challenge Annoucement/ Discussion *Shannon Sherlock, DC3/FX*
Landmark 7	How Cell Phone Forensics Tools Actually Work *Sam Brothers, US Customs and Border Protection*			Deconstructing exFAT Volume Artifacts *Jared Myers, DCFL*
LEGAL				
Crystal Ballroom	Mock Trial *Donald Flynn, DC3; Robert Gibson, Eighteenth Air Force Captain John Riesenberg, Trial Counsel Assistance Program; Andrew Ingraham, DCITA; Mike Moore, DCITA*		MORNING COFFEE BREAK Sponsored by: **Sky Catcher Solutions**	Mock Trial (continued) *Donald Flynn, DC3*
Portland/Benton (Hotel Side)	Facing New Legal Issues with Facebook and other Social Media *Rick Aldrich, IATAC*	Military Criminal Investigative Organizations (MCIO) and The Stored Communications Act *Thomas Dukes, U.S. Department of Justice*		The US Attorney's Office and Military Criminal Investigative Organizations (MCIO) *John Bodenhausen, United States Attorney's Office, Eastern District of Missouri*
Parkview/Aubert (Hotel Side)	Basic Intelligence Law *Maj Rich Ladue, AFOSI*	Reducing the Costs of Forensics Through Records and Information Management *Dr. Gavin Manes, Avansic & Michael Harvey, Avansic*		Crime and Punishment in Second Life *Dr. Sara M. Smyth, Simon Fraser University*

Breakout Session Agenda—Wednesday

Organization Abbreviations

DC3	DoD Cyber Crime Center
DCFL	Defense Computer Forensics Laboratory
DCITA	Defense Cyber Investigations Training Academy
JTF-GNO	Joint Task Force Global Network Operations

WEDNESDAY AFTERNOON

1140–1240	$5 Lunch, Exposition Closing, Raffle Drawing and Silent Auction Closing (Exhibit Areas: Majestic A-D and Majestic Foyer) *Please purchase lunch tickets at registration (See page 68 for details)*
1400–1500	Beverages & Snacks Available (Landmark Foyer)

Location	1240–1330	1340–1430	1440–1530	1540–1630
LAW ENFORCEMENT				
Landmark 1	The National Repository for Digital Forensic Intelligence *Shannon Sherlock, DC3/FX* *Dr. Mark Weiser, Oklahoma State University/NRDFI*	Virtual Villains: The Basics of Cybercrime Investigations *Jayne Hitchcock, WHOA*		
Landmark 2	Attacking the Problem of Child Exploitation from Every Angle *Christine Feller, National Center for Missing & Exploited Children &* *SA Eric Trest, National Center for Missing & Exploited Children* LAW ENFORCEMENT ONLY			An Examination of a Terrorist Cryptosystem *Gary Kessler, Gary Kessler Associates/VT ICAC* LAW ENFORCEMENT ONLY
Hawthorne (Hotel Side)	See Forensics Track			Life in Second Life *Josh Black, DC3*
RESEARCH & DEVELOPMENT				
Landmark 3	Hacking Critical Infrastructure *Ganesh Devarajan, TippingPoint - 3Com*	Scale-Free Self-Organization: Self-Defense Strategy for Distributed Systems *Dr. Glyn Gowing, Nova Southeastern University Graduate School of Computer and Information Sciences*	The Center for Cyber Intelligence and Threat Research *Rich Barger, Center for Cyber Intelligence Analysis and Threat Research* *& Andrew Pendergast, Center for Cyber Intelligence Analysis and Threat Research*	The Social Dynamics of Political and Religiously Motivated Hackers *Dr. Thomas Holt, School of Criminal Justice Michigan State University*
INFORMATION ASSURANCE				
Landmark 4	Fraud Techniques and Counter Measures *Andrew Showstead, VASCO*	Next Generation Network Mapping from the Core to the Edge: Travels across the Internet and the Global Implications of Network Infrastructure *Matt Hagovsky, Lumeta Corporation*	Severe Weather Warning: Data Ownership and Cloud Computing *Klint Walker, National Air & Space Intelligence Center*	Managing Risk From Advanced Persistent Threats *Stephen Windsor, Booz Allen Hamilton and* *Ronald Shaffer, FX* FOUO
FORENSICS				
Landmark 5	GPS Receiver Forensics *Timothy Leschke, DCCI*		Digital Data Practitioner Certification—Why Bother? *Gaylon Thompson, DCITA*	Forensic Examination of Android Phones *Eugene Libster, Mantech International Corporation*
Landmark 6	iPhone Forensics: An Investigative Approach *Sean Morrissey, US Department of State*	Self Encrypting Drives *Dave Anderson, Seagate Technology*	Splunk as an Enterprise Incident Response and Forensic Tool *Mathew McFadden, DCITA*	Memory Analysis and Forensics *Peter Silberman, MANDIANT*
Landmark 7	TCP/IP Protocols and Analysis *Gary Kessler, Gary Kessler Associates/VT ICAC*			Converting Disk Images into Working Virtual Machines *SA David Shaver, US Army Criminal Investigation Division, Computer Crime Investigative Unit* FOUO
Hawthorne (Hotel Side)	Android Forensics Techniques, File Systems and Analysis *Andrew Hoog, viaForensics*		From Extraction to Examination *Scott Lalliss, DCFL*	See Law Enforcement Track

Continue on Next Page >>

Breakout Session Agenda—Wednesday and Thursday

WEDNESDAY AFTERNOON (CONTINUED)

1140–1240 $5 Lunch, Exposition Closing, Raffle Drawing and Silent Auction Closing (Exhibit Areas: Majestic A-D and Majestic Foyer)
Please purchase lunch tickets at registration (See page 68 for details)
1400–1500 Beverages & Snacks Available (Landmark Foyer)

Location	1240–1330	1340–1430	1440–1530	1540–1630
LEGAL				
Portland/Benton (Hotel Side)	20+ Ways to Improve Digital Evidence and Cyber Crime Cases *Donald Flynn, DC3*		How the Internet Works: A Primer for Investigators and Prosecutors *Albert C. Rees, Computer Crime and Intellecutal Property Section, U.S. Department of Justice*	
Parkview/Aubert (Hotel Side)	Obtaining Electronic Evidence from Foreign Jurisdictions *Albert C. Rees, Computer Crime and Intellecutal Property Section, U.S. Department of Justice*	Sentencing Issues in Digital Evidence Trials *Captain John Riesenberg, Trial Counsel Assistance Program*	What the *$#! Do I Do Now? Confronting Real-World Legal Issues Faced by Cyber Investigators *William Yurek, US DOJ - Computer Crimes Section* LAW ENFORCEMENT ONLY	The Impact of Melendez-Diaz on Cyber Crime and Digital Evidence Cases *Donald Flynn, DC3*

THURSDAY MORNING

0700–0800 Morning Reception (Landmark Foyer)
0700–2100 Cyber Cafe (Majestic Foyer) *Sponsored by Guidance Software, Inc.*
1000–1100 Beverages Available (Landmark Foyer)
1130–1230 Lunch On Your Own

Location	0830–0920	0930–1020	1030–1120
LAW ENFORCEMENT			
Landmark 1	Black Bag Collection (Slurping for What you Want) *Steven Bolt, DCITA* FOUO	The Centrality of Google *Alissa Torres,DCITA*	Investigating Social Networking sites *Steven Bolt, DCITA* FOUO
Landmark 2	Technology, Friend or Foe? *Victor Watson, Federal Law Enforcement Training Center & Kevin Manson, Cybercop* LAW ENFORCEMENT ONLY		
RESEARCH & DEVELOPMENT			
Majestic A	Software Write Blocking - The Future of Forensic Triage and Imaging *Victor Fay-Wolfe, University of Rhode Island*	Metasponse Framework *Marcus Carey, Saecur LLC and Ronald Eddings, Jr., Saecur LLC*	Digital Image Forensics *Dr. Neal Krawetz, Hacker Factor Solutions*
Majestic B	Exploring Macro Level Correlates of Malicious Software Production *Dr. Thomas Holt, School of Criminal Justice Michigan State University*	Fibonacci Hashing *Chester Hosmer, WetStone* FOUO	
Majestic C	Automated Malware Similarity Analysis *Daniel Raygoza, DCFL*	Everybody's Got Something to Hide in a PDF Except for Me and My Monkey *Christopher Dearing, DCCI*	Do You See What I See? *Paul Cerkez, Nova Southeastern Univ and DCS Corporation & Dr. James Cannady, Nova Southeastern University*
Majestic Foyer	Tool Demo		
INFORMATION ASSURANCE			
Landmark 3	An 'Intelligent' Approach to Authentication *Ralph Rodriguez, Delfigo Security*	Proactive Cyber Security: Eliminate Malware & Prevent System Exploitation *Tom Murphy, Bit9*	Emerging Concepts in Effective Critical Infrastructure Protection (CIP) Sourcing *Richard Skibo, SPYRUS, Inc.*

Continue on Next Page >>

Breakout Session Agenda—Thursday

Organization Abbreviations

DC3: DoD Cyber Crime Center
DCFL: Defense Computer Forensics Laboratory
DCITA: Defense Cyber Investigations Training Academy
JTF-GNO: Joint Task Force Global Network Operations

THURSDAY MORNING (CONTINUED)

0700–0800	Morning Reception (Landmark Foyer)
0700–2100	Cyber Cafe (Majestic Foyer) *Sponsored by Guidance Software, Inc.*
1000–1100	Beverages Available (Landmark Foyer)
1130–1230	Lunch On Your Own

Location	0830–0920	0930–1020	1030–1120
Landmark 4	Flying Squirrel and Woodchuck Overview and Update *Jeff Watts, Smartronix* FOUO	Hacking Techniques: Hacking Stuff *Captain Rob Murphy, USMC*	
FORENSICS			
Landmark 5	Antiforensic Techniques: slacker.exe and timestomp.exe *James Meyer, DCITA* FOUO	Graphic Representation of System Process Relationships *Don Ranta, DCITA* FOUO	Google Earth Cache File Forensics *Jesse Kornblum, ManTech* LAW ENFORCEMENT ONLY
Landmark 6	Where Am I? - Ask my GPS *Gaylon Thompson, DCITA* FOUO	Data Spillage Got You Down? *Amber Schroader, Paraben Corporation*	Snort as a Forensics Tool? *Joseph Fichera, DCITA* FOUO
Landmark 7	Persistence Techniques Used by Windows Rootkits & How to Detect Them *Jesus Torres, Booz Allen Hamilton and Scot Lippenholz, Booz Allen Hamilton*	The CDMA Fraternal Clone Method—Recovering Data from Damaged Cell Phones *Detective Cindy Murphy, Madison PD*	
LEGAL			
Parkview/Aubert (Hotel Side)	DoJ Electrnoic Evidence Case Update *Thomas Dukes, U.S. Department of Justice*	The DoD Banner: Unfurling New Legal Issues *Rick Aldrich, IATAC*	Issues Regarding Digital Evidence and Cyber Crimes at Trial *Capt Michael Hopkins, Government Trial & Appellate Counsel, USAF*
Portland/Benton (Hotel Side)	The Nationless Cloud? *David Snead, David Snead P. C.*	Ask the Judges *Donald Flynn, DC3 and Robert Gibson, Eighteenth Air Force*	

THURSDAY AFTERNOON

1400–1500	Beverages and Snacks Available (Landmark Foyer)

Location	1230–1320	1330–1420	1430–1520	1530–1620
LAW ENFORCEMENT				
Landmark 2	You Can Run (udev), But You Can't Hide *Ernest Krutzsch, DCITA* FOUO	The Zeus Botnet: Stealing Everything from Millions of Americans *Gary Warner, The University of Alabama at Birmingham*	Pictures are Worth a Thousand Words, Report Development *Steven Bolt, DCITA* FOUO	Post-Exploitation vs. Incident Response *Christopher Daywalt, The Newberry Group* FOUO
RESEARCH & DEVELOPMENT				
Majestic A	NIJ's Electronic Crime and Digital Evidence Portfolio *Martin Novak, National Institute of Justice*	Win at Reversing: API Call Tracing and Sandboxing through Inline Hooking *Nick Harbour*	Apple TV: Size Doesn't Matter *SSgt Benjamin Solhjem, DCCI*	A Graph Theoretic Approach to Forensic Temporal Pattern Learning *Dr. Michael Hirsch, Raytheon Company*
Majestic Foyer	Tool Demo			
INFORMATION ASSURANCE				
Landmark 3	Lead, Follow, or Get Out of the Way *Jeff Watts, Smartronix*	Data Leaks and Insider Threats: Protecting the Nation's Most Confidential Information *Keith Fuentes, Mobile Armor*	BitTorrent: The Swarm of Internet Crime *Brian Baskin, DCITA*	

Continue on Next Page >>

THURSDAY AFTERNOON (CONTINUED)

1400–1500 Beverages and Snacks Available (Landmark Foyer)

Location	1230–1320	1330–1420	1430–1520	1530–1620
INFORMATION ASSURANCE (CONTINUED)				
Landmark 5	Identity-Enabled Networking: Controlling Network Access *Michael Kraus, Cisco Systems Inc.* FOUO			Operational Security: A Discussion of Techniques to Combat 'Spies in the Wires' *Marshall Heilman, Mandiant*
Portland/Benton (Hotel Side)	War Spying: Gathering Information via Unsecured Wireless Cameras *Steven Bolt, DCITA* FOUO	Windows 7: A First Look *Martin Easton, DCITA* FOUO	Windows Server 2008—Server Core Installation *Alissa Torres, DCITA* FOUO	Introduction to SQL Injection *Jesse Varsalone, DCITA* FOUO
Parkview/Aubert (Hotel Side)	Certified Trust Analyst *Jason Lord, d3 Services, Ltd.*			The Next Generation of Incident Response *Gib Sorebo, SAIC*
FORENSICS				
Landmark 4	Combating Enterprise Entrenchment Using Forensic Analysis *Dale Beauchamp, TSA* FOUO	Incident Response and the iPhone *Walter Barr, CSC & Sean Morrissey, US Department of State*		Social Networks: National Security's Greatest Threat *Ernest J. Hilbert, Online Intelligence*
Landmark 6	Detecting, Analyzing and Profiling Malicious Documents *Matthew Richard, Raytheon* FOUO		Forensic Implications and Analysis of the Apple TV - A Primer for Digital Forensic Investigators *Kevin Estis, Booz Allen Hamilton; Randy Robbins, Booz Allen Hamilton; Brian Baker ,Booz Allen Hamilton*	
Landmark 7	Network Based Forensics: Using Content Analysis and N-Grams to Track the Bad Guys *Michael J. (MJ) Staggs, AccessData*	Forensic Analysis of Cisco Routers Using Core Dumps and Crashinfo Files *Terrance Maguire, The Newberry Group*	Forensic Triage Programs, Risk Assessment Factors *J.J. Wallia, ADF Solutions, Inc.* LAW ENFORCEMENT ONLY	
Majestic B	Challenging the Law Enforcement Examiner—What a Defense Expert Sees *Larry Daniel,Guardian Digital Forensics, Inc.*	Digital Triage Forensics (Battlefield Lessons for Public Policing) *Stephen Pearson, High Tech Crime Institute*	Harnessing the Registry to Identify Malware *Elizabeth Schweinsberg, DoD*	BitLocker To Go Forensics *Jesse Kornblum, ManTech*
Majestic C	2010 The Mobile Forensic Odyssey *Amber Schroader, Paraben Corporation*	Advanced Reverse Code Engineering Toolkit *Adam Meyers, Department of State/ SRA Int'l* FOUO	Application Execution Redirection in Windows Volatile *Don Ranta, DCITA* FOUO	Image, Video, and Face Matching in Support of Child Exploitation Prosecution *Jeff Nash, BlueBear Law Enforcement Services*
DEFENSE INDUSTRIAL BASE				
Landmark 1	Developing Advanced Persistent Threat Malicious Code Countermeasures *Stephen Windsor, Booz Allen Hamilton and Ron Shaffer, FX* FOUO	Intelligence-driven Response for Computer Network Defense *Michael Cloppert, Lockheed Martin CIRT*		MythBusters: Advanced Persistent Threats Debunk Today's Best Practices *Stephen Windsor, Booz Allen Hamilton and Jesus Torres, Booz Allen Hamilton*

Breakout Session Agenda—Friday

Organization Abbreviations
DC3: DoD Cyber Crime Center
DCFL: Defense Computer Forensics Laboratory
DCITA: Defense Cyber Investigations Training Academy
JTF-GNO: Joint Task Force Global Network Operations

FRIDAY

0700–1200	Information Desk (Landmark Foyer)
0700–0800	Morning Reception (Majestic Foyer)
0700–1300	Cyber Cafe (Majestic Foyer) *Sponsored by Guidance Software, Inc.*
0800–0855	Plenary Session (Majestic E-H)

Location	0900–0950	1000-1050	1100-1150
LAW ENFORCEMENT			
Landmark 1	Internet Relay Chat (IRC) and Usenet (Newsgroups): The Dark Underbelly of the Internet *Bryan Spano, DCITA* FOUO	Online Under-Cover Agent Operations using Internet Relay Chat *Special Agent DeWayne Duff, AFOSI 3rd FIS* FOUO	See Forensics Track
Landmark 2	Fixing Broken Glass: Restoring Order and Reducing Cyber Crime *Dr. Taher Elgamal, Axway*	The Many Flavors of Helix *Steven Bolt, DCITA* FOUO	Investigating Cyber Crimes using Lawful Intercepts and Live Network Surveillance *Kevin Graves, IP Fabrics*
Landmark 3	Grabbing Volatile Data- Get it Now or Lose it Forever *Gaylon Thompson, DC3* FOUO	Imaging and Examining Volatile Memory *Casey Szyper, DCITA* FOUO	See Information Assurance Track
INFORMATION ASSURANCE			
Portland/Benton (Hotel Side)	Loose Lips Sink Networks - Is Social Networking Making Your Network Insecure? *Frank Nagle, Mandiant*	Wireshark—More Than A Pretty Interface *Mike Cowan, DCITA* FOUO	Overcoming Technical Challenges in Making Data Actionable: Establishing Situational Awareness *John Stoner, Symantec Corporation*
Landmark 3	See Law Enforcement Track		A Case Study on an Air Force Computer Incident *1 Lieutenant Jeremy Sparks, AFCERT*
FORENSICS			
Landmark 1	See Law Enforcement Track		Choosing Mobile Device Forensic Tools *Walter Bobby, DCITA* FOUO
Landmark 4	Recycle Bin Forensics within a Windows 7 and Windows Vista Shadow Volume *Timothy Leschke, DCCI*	Live Forensics—A How To Guide *John Riley, Federal Law Enforcement Training Center*	
Landmark 6	Forensics in the Raw *Dominique Kilman, Booz Allen Hamilton*	Drive Prophet Triage Tool *Mr Mark McKinnon, RedWolf Computer Forensics*	DCCI_StegCarver: Providing New Definition to Forensic Carving *Mark Hirsh, DCCI*
Landmark 7	FDE Process *SA Bill Dent, DC3*	Large Scale Data Acquisition and Analysis *Hermann Kelley, Efficient Forensics*	
Majestic A	RAID Reconstruction Revisited: New Challenges and Limitations *Michael Harvey, Avansic*		
Majestic B	Practitioners Guid to Memory Analysis *Dale Beauchamp, TSA* FOUO	Exploring PDF and SWF Malware: Tools and Techniques for Front-Line Analysis *Jonathan Woytek, CERT*	
Majestic C	Forensic Implications of Windows 7 *Mark Neno, DCITA* FOUO		Efficient command and control decoding for the lazy reverser *Matthew Richard, Raytheon* FOUO
DENFENSE INDUSTRIAL BASE			
Landmark 5	Cyber Betrayal: Lessons Learned on Defending Your Network from Trusted Insiders *Michael Theis, Raytheon*	Agile Development for Incident Response *Charles Smutz, Lockheed Martin &* *Samuel Wenck, Lockheed Martin*	Exploring Tools and Methods to Identify Patterns of Anomalous Behavior, Activities and Conversations Across Large Volumes of Unstructured Data *Dr. Josh Rosenthal, iQuest Analytics* FOUO