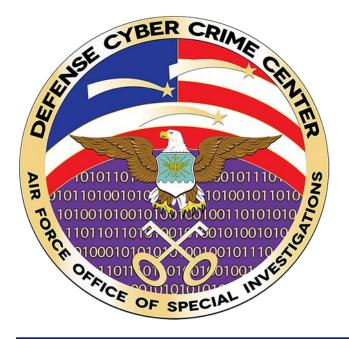


Defense Cyber Crime Center

A National Cyber Center

Defense Cyber Crime Center Digital Crime Scene Challenge



Jim Christy, Special Agent (Ret), HQE
Director, Future Explorations
Defense Cyber Crime Center
Version 1



Challenge Overview

- Designed to be fun
- Experience a crime scene scenario
- Search for evidence that may be relevant to your investigation







Background

- Volume contained in digital devices continues to increase
- Law Enforcement & Security professionals need to be aware of the changing crime scenes
- Speed counts
 - How to triage the enormous amounts of data to find the relevant evidence quickly is key
- This Challenge was designed for players to have fun and to experience the new issues faced



Digital Proliferation



MP3 Players

Mables.com



PDAs & Cell Phones





Alarm Systems



Programmable Appliances



Cole

Cameras





Thumb Drives





Watches



Storage Capacity

	Characters	Digital Size
1 Line of Text80 characters per line	80	80 B
1 Page of Text60 lines per page	4,800	≈ 4.6 KB
1 Ream of Paper500 pages per ream	2,400,000	≈ 2.2 MB
1 Safe Drawer10 reams per drawer	24,000,000	≈ 22.8 MB
1 Paper Safe5 drawers per safe	120,000,000	≈114.4 MB



WikiLeaks = 1 DVD = 4.7 GB

■ 4.7 GB = 350,000 classified documents and cables



How to Play

- Teams (1-5 members)
- Participants don't need any equipment
- Read 1 page scenario
- Read 1 page interrogation
- Enter crime scene with 15 minutes to:
 - Identify all digital devices
 - Triage digital devices based on scenario & Interrogation to select the one device that has the evidence you need
 - Discover the information of evidentiary value
 - Points for each device, and evidence
 - Tie-Breaker is shortest time to complete



Scoring

- You score points:
 - For each Device you uncover
 - Identifying the correct device in triage process that has the evidence
 - Displaying the evidence from the seized device
 - Points available: 1-100
- Clock starts as you enter crime scene
 - Stops when you say you have found everything
- Tie Breaker is Least Time to complete
 - Maximum of 15 minutes in crime scene



Some Hints

- Assign roles/functions:
 - Lead Investigator (directs team)
 - Responding Investigators (2) perform the search
 - <u>Evidence Custodian</u> places seized devices in proper position and informing referee of discovered devices
 - <u>Digital Forensics Examiner</u> person to put selected device into the provided forensics workstation and uncover the evidence



Rules to Remember

- Be on time!
- Crime Scene is Off Limits!
 - Do Not Enter Crime Scene until directed to
- Be respectful to suspect & property
- Do Not touch forensic workstation until you're given permission to do so
- Do have FUN!



Summary

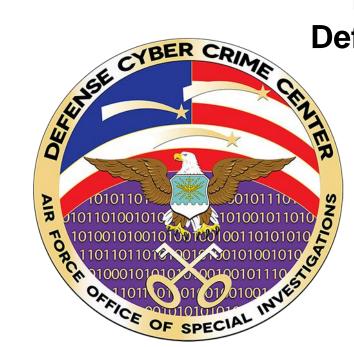
- You have 15 minutes to find digital devices based on a scenario and the scene
 - Read the scenario and the interrogation thoroughly
- The teams search the 'scene' for all items, separating digital items and non-digital items
 - Digital devices are triaged until the correct one is identified (the one with the evidence)
- Teams are scored based on:
 - Which digital devices they find
 - Selecting the correct device that has the evidence
 - Points deducted for selecting wrong device
 - Successfully uncovering the evidence
 - Tie-breaker is the shortest time to complete



Defense Cyber Crime Center

A National Cyber Center

James Christy, Special Agent (Ret), HQE
Director, Future Explorations
Defense Cyber Crime Center (DC3)



James.Christy@dc3.mil Office 410-981-6699 Cell 410-925-0573 Web www.dc3.mil