



**2012 DC3 DIGITAL FORENSICS
CHALLENGE RULES
v1.5**

12 September 2012



Table of Contents

1.0 INTRODUCTION.....5

 1.1 BACKGROUND.....5

 1.2 OVERVIEW.....5

 1.3 OBJECTIVES.....5

2.0 ELIGIBILITY CRITERIA.....5

 2.1 REGISTRATION.....5

 2.2 REQUIREMENTS6

3.0 THE CHALLENGE.....9

 3.1 CHALLENGE OBJECTIVES.....9

 3.2 CHALLENGE RULES9

 3.3 CHALLENGE GRADING.....9

 3.4 CHALLENGE BONUS POINTS.....9

 3.5 CHALLENGE SCHEDULE / KEY DATES.....10

4.0 PRIZE CRITERIA.....11

 4.1 SPONSORS.....11

 4.2 PRIZES.....11

 4.3 ACADEMIC CRITERIA.....11

 4.3.1 Graduate11

 4.3.2 Undergraduate.....12

 4.3.3 High School.....12

 4.4 JUDGING AND CHALLENGE RULES12

 4.4.1 Methods to Submit Solutions12

 4.4.2 Terms of Submitting Solutions.....13

 4.4.3 Terms of Submitting Tools Used in Solving Challenges13

5.0 INTELLECTUAL PROPERTY.....15

6.0 LIMITATION OF LIABILITY.....15

7.0 TEAM DISQUALIFICATION.....16

8.0 CHALLENGE CANCELLATION.....16

9.0 PRIVACY POLICY.....16

 9.1 DOD PRIVACY ACT STATEMENT16

 9.2 CONTACT PURPOSES17

 9.3 STATISTICAL PURPOSES.....17

APPENDIX.....18

 A-1: CHALLENGES AND POINT STRUCTURE18

 A-2: SANS19

 A-3: EC-COUNCIL.....20

 A-4: AFCEA23

 A-5: BLACKBAG.....24

 A-6: NIST OLES.....25



2012 DC3 Digital Forensics Challenge



A-7: NATIONAL BOARD OF INFORMATION SECURITY EXAMINERS (NBISE)	26
A-8: ACCESSDATA.....	27
A 9: BEST BUY.....	28



1.0 INTRODUCTION

1.1 Background

Operating since 1998, the Department of Defense Cyber Crime Center (DC3) provides digital and multimedia (D/MM) forensics, cyber investigative training; research, development, test and evaluation (RDT&E); and cyber analytics to DoD computer network defense (CND), law enforcement (LE), intelligence community (IC), counterintelligence (CI) and counterterrorism (CT) agencies. Established as an entity within the Air Force, DC3 operates under Secretary of the Air Force (SECAF) Executive Agency with program oversight via the Air Force Office of Special Investigations (AFOSI), and the DoD CIO is the principal staff assistant per DoDD 5505.13E, DoD Executive Agent (EA) for the DoD Cyber Crime Center (DC3). DC3 was recognized as a national cyber center in NSPD 54/HSPD 23 and serves as the operational focal point for the Defense Industrial Base (DIB) Cybersecurity and Information Assurance DIB CS/IA Program.

DC3 is located in Linthicum, MD with an authorized staff of ~400 (currently), roughly one-third of whom are DoD civilians and US military personnel, and two-thirds of whom are contractors. DC3 also hosts 13 liaisons from other agencies to include DHS, USD/DAMO, DSS, NSA, and USCYBERCOM.

1.2 Overview

The DC3 Challenge encourages innovation from a broad range of individuals, teams, and institutions to provide technical solutions for computer forensic examiners in the lab as well as in the field. The DC3 Challenge is comprised of approximately 25 different exercises ranging from basic forensics to advanced tool development. The levels (100-500) are broken down into single exercises and are designed to be unique and separate from one another.

1.3 Objectives

The objectives of the annual DC3 Digital Forensics Challenge are to address the shortage of cyber professionals; establish relationships; resolve technological issues; and develop new tools, techniques, and methodologies for the digital forensics community.

2.0 ELIGIBILITY CRITERIA

2.1 Registration

Registration is designed to be completed online via the 2012 DC3 Digital Forensics Challenge (DC3 Challenge) website at <http://www.dc3.mil/challenge/2012>. Registration must be for all team participants in its entirety. If any 'anonymous' information is supplied with application submittal, the application will be denied. In the unlikely event that the website is not functioning, a team member can provide the necessary information in an email to challenge@dc3.mil or call the DC3 challenge line at 410-981-6610.



2.2 Requirements

The DC3 Challenge is open to both individuals and teams. Teams may include corporate or academic entities but are not limited to these. Each entry must meet the following eligibility requirements:

- An individual cannot participate on more than one (1) team.
- Teams will consist of one (1) to four (4) member(s).
- The team's first team member will be assigned as the team leader and considered the sole Point of Contact (POC).
- All members are required to provide their personally identifiable information (PII) (Full Name, Address, Telephone Number, Email Address, Etc) for team approval.
 - *Failure to provide accurate personal information **OR** falsifying registration information will cause denial of your application and may disqualify your team from challenge participation as per Section 7.0 – Team Disqualification.*
 - The team POC is responsible for coordinating any and all changes to team members (add/update/remove) with the DC3 Challenge Team **in writing** at challenge@dc3.mil.
 - See Section 9.0 - Privacy Policy on the use of PII information within the DC3 Challenge.
- Team and Team Member Affiliations
 - Team member affiliations are required at time of registration by the DC3 Challenge for determining team affiliation and team's potential prizes to be awarded as part of the team's approval to play in the DC3 Challenge.
 - Each team member's affiliation should be relevant to when team's FINAL exercise submissions are sent to DC3 (NOT when registered):
 - **Civilian** – A person or team who chooses not to be otherwise affiliated with any other specified affiliation category.
 - **Commercial** – A person or team that is employed for a Commercial / Private Sector entity and is representing their company. This includes contractors that work for Military, Federal, State and Local Government agencies.
 - **Government** – A person or team that works directly for their nation's Federal, State, or Local Government agency. This excludes contractors.
 - **Military** – A person or team that is military member or civil servant to their nation's Military. This excludes contractors.
 - **High School Student** – A person or team that is attending a high school as a student and has **NOT** graduated before the submission of the final Challenge package.
 - **Community College Student** – A person or team that is attending a 2-year Institute as a student and has **NOT** graduated before the submission of the final DC3 Challenge.



2012 DC3 Digital Forensics Challenge



- **Undergraduate Student** – A person or team that is attending a 4-year continuing education program at a College/University/Technical School as a student and has **NOT** graduated before the submission of the final Challenge package.
- **Graduate Student** – A person or team that is enrolled in a graduate or post-graduate program at a College/University/Technical School as a student and has **NOT** graduated before the submission of the final Challenge package.
- The overall team affiliation is calculated by the DC3 Challenge team based on the provided team member(s) affiliation(s).
 - If a team consists of all members of the same team having the same affiliation (i.e. 4 Government members), the team will be assessed by its common member affiliation (i.e. Government).
 - If a team consists of all academic students, the highest category level will be assessed as the team affiliation. See Section 4.3 – Academic Criteria for additional details.
 - If a team consists of a mix of 2 or more team member affiliations that are not all academic (i.e. 2 Civilian and 1 High School Student), the team will be assigned the team affiliation of Civilian.
- Once team affiliation is determined by the DC3 Challenge team, the team is listed under the available prize(s) based on the team's registration entry information. See Section 4.2 - Prizes for further details.
- Any changes of team member affiliation after approval to participate has been granted should be submitted to the DC3 Challenge team at challenge@dc3.mil by the POC at time of change. Be aware that changes in team members, and their affiliation, could affect the entire team affiliation as per the rules noted previously. Failure to report team member affiliation changes will be cause for disqualification as per Section 7.0 – Team Disqualification.
- If any participant is under the age of 18 at the time of registration, the team is required to provide written authorization from a parent / legal guardian via the DC3 Permission to Participate form for **each** under-aged team member. Failure to provide this written permission will be cause for disqualification as per Section 7.0 – Team Disqualification.
- DC3 employees, current and former within the past year (2011), and their immediate relatives are ineligible to participate for prizes; however they may compete for points only.
- For specific national-based prizes:
 - All team members must be of the same citizenship category (example: US or Non-US) as per the prize's rules.
 - Mixed citizenship teams consisting of US and Non-U.S citizenship players will be assigned as a global team affiliation and will not qualify for any US or Non-US specific prizes as per the prize's rules.



2012 DC3 Digital Forensics Challenge



- For specific US State-based prizes:
 - All team members must have a current US residential address in corresponding US state awarding the prize.
 - Proof that the individual resides in their residential state will be required by winners to receive recognition and any prizes.
 - Residence will be validated by providing DC3 with all of the following depending on their team affiliation:

Team Affiliation	Proof of Identification and Residency Requirements
High School Student	<ul style="list-style-type: none"> • High school transcript showing attendance in a school located in the corresponding state during the time of the challenge (copy or formal document) <p style="text-align: center;">AND</p> <ul style="list-style-type: none"> • A copy of a valid corresponding state driver's license or identification card with individual's name, indicating a physical address in the corresponding state. <p style="text-align: center;">AND</p> <ul style="list-style-type: none"> • The Permission to Participate form completed by a legal guardian if under the age of 18. The form can be found at http://dc3.mil/challenge/2012/play/rules.php
Undergrad and graduate students	<ul style="list-style-type: none"> • College transcript showing attendance in a college located in the corresponding state during the time of the challenge (copy or formal document). <p style="text-align: center;">AND</p> <ul style="list-style-type: none"> • A copy of a valid US state-issued driver's license or identification card with the participant's name.
Active Duty US Military	<ul style="list-style-type: none"> • US Military orders with a duty station located in corresponding state during the time of the challenge <p style="text-align: center;">AND</p> <ul style="list-style-type: none"> • A copy of a valid US Military ID with individual's name
All others	<ul style="list-style-type: none"> • A copy of a utility bill with the individual's name and a valid in state street address showing residence in the corresponding state during the time of the challenge. <p style="text-align: center;">AND</p> <ul style="list-style-type: none"> • A copy of a valid corresponding state driver's license or identification card with individual's name, indicating a physical address in the corresponding state.



3.0 THE CHALLENGE

3.1 Challenge Objectives

The Objectives of the Annual Digital Forensics Challenge are to:

- Establish relationships within the Digital Forensics Community;
- Resolve issues facing the Digital Forensics Community;
- Develop new tools, techniques, and methodologies for the Digital Forensic Community

3.2 Challenge Rules

The Challenge Rules are published on the 2012 DC3 Challenge Website

(<http://www.dc3.mil/challenge/2012/play/rules.php>) and are subject to change. All changes will be documented as they occur. Please review and refer back on a regular basis to ensure that compliance in all areas is maintained.

3.3 Challenge Grading

There are 27 single scenario-based problem exercises. The chart of each specific exercise and corresponding points can be found in the Appendix under A-1 Exercises and Point Structure. There are twelve* (12) 100 point exercises, six (6) 200 point exercises, six (6) 300 point exercises, five (5) 400 point exercises, and six (5) 500 point exercises.

*There were five original challenges with five (5) additional 100 point Bonus Challenges were added 03/30/2012 and three (3) more added 07/02/2012.

3.4 Challenge Bonus Points

A team may acquire additional bonus points for early exercise submissions to the DC3 Challenge. The solution submitted for each exercise scenario is eligible for the bonus award based on the time it is submitted to DC3 Challenge. Only the team's initial submission is eligible for a bonus award points.

Bonus points are calculated based on the team's grade for that exercise submission and the submission date. The team's initial submission is the **FINAL** submission for that specific exercise.

Bonus points will be awarded based on the following schedule:

Date Range	Bonus Awarded to Exercise Score
15 Dec 2011 -- 1 Apr 2012	20%
2 Apr 2012 -- 1 Jul 2012	10%
2 Jul 2012 -- 1 Oct 2012	5%
2 Oct 2012 -- 1 Nov 2012	0%

Example:

- Team A submits their exercise 101 submission on 1 Feb 2012.
- DC3 grades Team A's exercise 101 submission after 1 Apr 2012.
 - Their submission is graded by DC3 at 90 out of 100 points.
 - Their submission is marked at 20% bonus points due to their 1 Feb 2012 submission date.
- Team A is awarded the following points for exercise 101:
 $90 \text{ points graded} + (90 \text{ pts} * 20\%) \text{ bonus} = 108 \text{ points total}$



3.5 Challenge Schedule / Key Dates

Key Date	Schedule
1 Dec 2011	Announcement of DC3 Challenge 2012
15 Dec 2011	Registration Begins <ul style="list-style-type: none">Registration and Challenge packets containing all of the challenge materials will be available for download only on or about 15 December 2011.Applications received each day by close of business (COB) will be processed within 1-3 business days for approval.
24 Jan 2012	Official announcement at the 2012 DoD Cyber Crime Conference, Atlanta, GA
1 Apr 2012	Last day for 20% Bonus points
1 Jul 2012	Last day for 10% Bonus points
1 Oct 2012	Last day for 5% Bonus points
15 Oct 2012	Last Day for Registration <ul style="list-style-type: none">Registrations are no longer accepted for the 2012 DC3 Challenge.
1 Nov 2012	Last Day for Submissions <ul style="list-style-type: none">All 2012 DC3 Challenge solutions, including scripts and non-commercial programs created by the team, must be uploaded or postmarked to DC3 no later than November 1st, 2012 at 11:59:59 PM EST to be eligible for a prize in their assigned category.Exercise solutions received after 1 November 2012 EST will not be accepted for prizes. Scoring after this date will be at the discretion of DC3.
3 Dec 2012	DC3 Challenge Winners Announced <ul style="list-style-type: none">All participants will be notified via email of the posting of scoring results to the DC3 Challenge Website.Final results will be posted on the DC3 Challenge Website.In the event of a tie score for the top exercise solution package, the tie will be broken by the time difference between INITIAL registration approval email and LAST individual exercise submittal (by electronic upload or postmarked date) of the team's solution packets.



4.0 PRIZE CRITERIA

4.1 Sponsors

In support of the DC3 Challenge objectives, DC3 offers sponsorship with select organizations to:

- Grow locally, nationally, or globally within the Cyber and Digital Forensic Communities
- Support the organization's missions and/or objectives
- Provide support of the US and global Cyber Challenges for educating those up and coming in the fields for Cyber Defense and Digital Forensics

An official list of the DC3 Challenge 2012 sponsors can be found in Appendix A-2: Prize Sponsorships.

4.2 Prizes

Based upon their team affiliation criteria provided by the DC3 Challenge sponsor's requirements, several prizes are available to DC3 Challenge teams.

Each member of the winning teams will also receive a plaque as well as formal recognition at the DoD Cyber Crime Conference by DC3.

4.3 Academic Criteria

Should an academic category be selected as a team category, the following applies:

- Team member(s) must be enrolled and in good standing with the academic institution attending ON the date of submitted solutions package to be eligible for placement in the Academic category.
 - Proof of enrollment and student status by the Academic Institution ("Full-time", "Part-time") must be provided
 - A letter or fax on the institution letterhead, signed by team member and institution administrative office will suffice
 - Age of the player on the date of the Challenge solution is submitted does not matter
 - Failure to provide proof of enrollment with appropriate signatures will disqualify the team from the Academic category and will be placed in the Civilian / Private Sector category.
- If the team consists of students from different academic categories (e.g. 2 high school students, 1 undergraduate student, and 1 graduate student), the highest academic category level will be used to assess the category status for the team. In the example above, the team's category would be designated as Graduate students.

4.3.1 Graduate

- Individuals / Team status **will be** placed in the **Graduate** category if they are still in a Graduate program on the date when the Challenge 2012 package is **submitted** (*not when you apply*).
- Graduate team(s) who submits their package **prior** to graduating will be placed in the Graduate category.
- Graduate team(s) who submits their package **after** graduating will be placed in the category of Military, Federal Government, Civilian, or Commercial/Private Sector and are ineligible for Academic recognition.
- Should the Individual / Team member have a change in their expected graduation date, they **must** inform the DC3 Challenge staff (i.e. anticipated



2012 DC3 Digital Forensics Challenge



Graduation May 2012 changes to Dec 2012 – status will remain in the Graduate category). Proof of this change will have to be provided.

4.3.2 Undergraduate

- Individuals /Team status **will be** placed in the **Undergraduate (UG)** category if they are still in an Undergraduate program on the date when the Challenge 2012 package **is submitted** (*not when you apply*).
- UG team (s) who submits their package **prior** to graduating will be placed in the UG category.
- UG team (s) who submits their package **after** graduating but while attending a graduate program will be placed in the Graduate category.
- UG person(s) who submits their package **after** graduating but **not** attending a graduate program will be placed in the category of Military, Federal Government, Commercial/Private, or Civilian and will be ineligible for Academic recognition.

4.3.3 High School

- Individuals / Teams **will be** placed in the **High School (HS)** category on the date when the DC3 Challenge 2012 package **is submitted** (*not when you apply*).
- HS senior(s) or Team with a HS senior member who submits their package **prior** to graduating will be placed in the HS category.
- HS senior(s) or Team with a HS senior member who submits their package **after** graduating, but while attending college/university/technical program will be placed in the Undergraduate (UG) category.
- HS senior(s) or Team with a HS senior member who submits their package **after** graduating, but **not** attending college/university/technical program will be placed in the category of Military, Federal Government, Commercial/Private, or Civilian and will be ineligible for Academic recognition.

4.4 Judging and Challenge Rules

DC3 Challenge Judges will adjudicate and resolve any discrepancies throughout the grading process. In the event of a tie for equal points, the team providing the exercise submissions within the shortest amount of time (based on the difference of the time between the INITIAL registration approval email and the LAST team submission to the DC3) will be declared as the winner. **All decisions of the DC3 Challenge Judges are final.**

4.4.1 Methods to Submit Solutions

Team submission packages can be submitted to DC3 via two ways:

- *By single packages for each individual exercise submitted over time* (**RECOMMENDED**). Uploading individual exercise submissions via electronic submission only, including tools and scripts. This allows teams to submit individual exercises as they are completed to DC3 before the Submission deadline.
- *By a complete package of all Challenge level solutions (e.g. all 100 level exercises) at one time* via electronic submission or mailed to DC3 before the deadlines stated in Section 3.5 - Challenge Schedule / Key Dates in the DC3 Challenge rules.



4.4.2 Terms of Submitting Solutions

By submitting a proposed solution to the DC3 Challenge, you agree to the following terms:

- Solutions are submitted and presented in English to be graded.
- For each tool (software, script, and method/technique) used in your Challenge solutions,
 - It is documented in each individual exercise as per Section 4.4.3 – Terms of Submitting Tools Used in Solving Challenges
 - Copyrighted tools can only be submitted as part of a solution if the tool's creator allows distribution to and by the US Government.
- Teams are responsible for verifying that their submissions are accurate before providing them to DC3.
- All submissions (individual exercises and packages) to DC3 are considered final and no revisions are allowed unless authorized by DC3.

Example: If one individual exercise is uploaded on Oct 1, 2012 and the same individual exercise is uploaded on Oct 10, 2012 for the same challenge level, the first submission only will be graded.

- If a team has provided their submission in error, they must contact the DC3 Challenge team at challenge@dc3.mil within 2 business days of their submission to remove it from DC3 Challenge grading.
- Solutions and answers must be checked for viruses, trojans, and malicious code using commercially available antivirus software and teams must certify that the submission package is free of those malicious computer programs.
- DC3 is the final arbiter of any dispute concerning interpretation of the rules for the DC3 Challenge. **ALL DECISIONS ARE FINAL.**

4.4.3 Terms of Submitting Tools Used in Solving Challenges

For each tool (program, script, and method/technique) used toward exercise solutions, the following information must be provided with each Challenge solution - failure to provide this information can disqualify a team as per Section 7.0 – Team Disqualification.

NOTE: All tools and documentation MUST be submitted and presented in English. Tools must be capable of running on a standalone system with no internet connectivity.

- **Custom Developed tools (including Level 500 tools)**
This includes all non-commercial tools OR modified open-source tools used in all exercises. All Level 500 tools are considered this type of tool – NO EXCEPTIONS.
 - Documentation
 - Step by step instructions, to include “screen shots” as appropriate on how to use the tool
 - Source code for all tools and scripts need to be included as part of the submission.
 - Dependencies need to be referenced for submissions.
 - For Level 500 tools, include additional documentation:



2012 DC3 Digital Forensics Challenge



- Documentation and screenshots of your results of your validation of the Challenge against your test bed
- A completed test plan outlining the steps necessary for a functional test (template is provide within the Level 500 Challenges)
- A completed [Tool Evaluation Worksheet](#) form that includes your tool's information, dependencies, and test bed information.
- Tool
 - A copy of each non-commercial tool and/or script OR modified open-source tools and/or scripts used to accomplish the exercise solution(s).
 - A copy of the source code for validation and testing by DC3
 - For level 500 tools - additional data required:
 - Data test case used to validate your tool.
 - Listing of execution dependencies in the [Tool Evaluation Worksheet](#)
- **Resubmission of Custom Developed tools**

This includes all tools developed for past DC3 Challenge solutions re-used or improved for the DC3 Challenge 2012.

 - Include all requirements listed in "Custom Developed tools"
 - Additional requirements:
 - A list of changes of the tool that documents improvements, increased functionality, etc. to be awarded full points.
 - Submission of tools if submitted "as-is" from the prior year's Challenge without any form of improvement, will receive zero points.
- **Commercial tools**

This includes all commercial tools AND closed-source tools for all Challenge solutions except Level 500 tools.

 - Name of the tool and version
 - Tool creator's company
 - A URL to the company's website
- **Open Source tools**

This includes all tools with source code shared to the public Internet not used in Level 500 Challenge solutions.

 - Name of the tool
 - A URL to the site from the open source sharing site must be provided. Examples of the open source sharing sites include Source Forge, Google Code, Code Plex, etc.



5.0 INTELLECTUAL PROPERTY

All submissions provided to the DC3 Challenge by the participants are for the purpose of Research and Development (R&D) of digital forensics in furthering advancement for the US Government and the digital forensics community.

DC3 may seek to establish Cooperative Research and Development Agreements (CRADAs) for selected tools developed as part of the DC3 Digital Forensics Challenge for further research and development.

All tools and methods created by the DC3 Challenge participants will remain the intellectual property of their creator(s). Submissions provided to the DC3 Challenge by Challenge participants will be provided to the US Government with the following conditions as per Air Force Instruction (AFI) 51-303: "Intellectual Property – Patents, Patent Related Matters, Trademarks, and Copyrights" at the submitted version:

- Granted as a nonexclusive, irrevocable, royalty-free license to the US Government with the power to the US Government to grant licenses for all governmental purposes.
- Provided at no cost to the US Government without expectation of reimbursement.
- Challenge participants must provide a copy of the source code to DC3 Challenge team at the time of submission:
 - All source code will be used for the purposes of testing and validation of submissions for malicious content within DC3 only.
 - Source code of compiled code, unless already made public by the team or under an open-source license, will not be shared or redistributed outside of DC3 to protect the intellectual property rights of their creator(s).
- All team submissions with team-created tools, techniques, solutions, and responses, in their entirety, unless stated above, may be shared, in their entirety, with the Challenge participants, DOD partners, and the digital forensics community. In addition, these tools, techniques, solutions, and responses may be documented and publicized to the general public at DC3's discretion.

Failure to provide the required tools, scripts, source code, and methods / techniques upon submission will disqualify the team from receiving points for the submitted exercise.

It is recommended that all teams double-check their DC3 Challenge submissions to remove any possible personal identifiable data you are not willing to release to the public. It is not the responsibility of DC3 to remove this data.

6.0 LIMITATION OF LIABILITY

The computer data and media supplied for the DC3 Challenge has been checked for computer viruses, trojans, and other malicious code using commercial antivirus software configured with current signatures as of December 15th, 2011 and is found to be free of such programs. If the materials received appear tampered with discontinue use immediately and return the materials to DC3.

In consideration of participating in the DC3 Challenge, contestants acknowledge that DC3 is not responsible for any damage caused to any computer or network due to the loading of, or operation of the storage media holding the DC3 Challenge materials.



7.0 TEAM DISQUALIFICATION

Registered individuals/teams will be disqualified for any of the following reasons:

- Failure to provide accurate personal information and/or falsifying registration information
- Failure to provide scripts, programs, and/or methods as referenced in Section 4.4.3 -- Terms of Submitting Tools Used in Solving Challenges in the DC3 Challenge Rules
- Failure to submit source code for all tool and script submissions
- If at the time of submission grading and verification, it is determined that a team or member of a team has not met the eligibility requirements, the entire team shall be disqualified without regard to DC3 Challenge performance in meeting prize objectives
- Failure to submit documents by the required solution due date
- Fraudulent acts, statements, or misrepresentations involving any DC3 or other federal government documentation or systems used for the DC3 Challenge.
- Violation of any federal, state, or local law or regulation determined to be inconsistent with the DC3 Challenge.
- Any team member under the age of 18 must submit a DC3 Permission to Participate form, signed by a parent / legal guardian to participate in the Challenge. If it is discovered that a team member is under the age of 18 and has not submitted this form, the team will be immediately disqualified.

8.0 CHALLENGE CANCELLATION

The DC3 reserves the right to cancel this challenge at any time leading up to or during the DC3 Challenge time frame.

9.0 PRIVACY POLICY

All team information provided during team registration for the DC3 Challenge is collected for the following purposes:

- Vetting and approval of teams to play in the DC3 Challenge
- Determining the team's available prizes from DC3 Challenge sponsors as stated in Section 4.0 – Prize Criteria
- Statistical reporting of the DC3 Challenge to the public and DC3 Challenge sponsors/partners
- Contacting teams to provide:
 - News and updates about the DC3 Challenge
 - Opportunities related to the DC3 Challenge and other government/academic Cyber Challenges
 - Verification of winners and award prizes with DC3 Challenge sponsors

9.1 DOD Privacy Act Statement

The DC3 Challenge will only share the information disclosed during registration with another government agency if your inquiry relates to that agency, or as otherwise required by law.



2012 DC3 Digital Forensics Challenge



9.2 Contact Purposes

The DC3 Challenge team will remain the primary contact for any request for the participating team's contact information during the Challenge process. These requests will be routed by the DC3 Challenge team to the participating team's leader for approval for release. It is the participating team's discretion to be contacted by the interested party outside of DC3 thereafter.

For DC3 Challenge news and updates, teams may elect to "opt-out" by contacting the DC3 Challenge team at challenge@dc3.mil

9.3 Statistical Purposes

For DC3 Challenge and other government/academic Cyber Challenge promotional purposes, specific anonymous information may be shared with 3rd parties. This information will be unassociated from Team Names and their Team Member's personal and contact information. This information includes the following:

- Member affiliations, states, and countries from Team Members as part of the statistical reporting of the DC3 Challenge's progress with the public and press.
- Member affiliations, US citizenship, schools, states, zip codes, and countries from Team Members may be shared with the DC3 Challenge sponsors/partners and other partners as part of government/academic Cyber Challenges.



APPENDIX

A-1: Challenges and Point Structure

Points	Challenge Title
100	Internet Explorer Internet History Analysis
100	Linux Password and Shadow File
100	Google Chrome Internet History Analysis
100	Mozilla Firefox Internet History Analysis
100	Safari Internet History Analysis
100	File Metadata Analysis *
100	File Signature and Reconstruction *
100	Password Recovery *
100	Hidden Data Analysis *
100	Hash Analysis and Comparison *
100	Detect Suspicious Software**
100	Image Analysis**
100	Manipulated Images**
200	Steganography Extraction Challenge
200	Cracking Linux Logins
200	Linux Intrusion - Network Capture
200	Windows Intrusion - Network Capture
200	Evidence of USB Usage between MAC and Windows
200	E-mail Header Analysis
300	Encrypted Archives Challenge
300	Linux Encrypted Volume Challenge
300	Data Recover [RAID Reconstruction]
300	Linux Intrusion - Dead Box Exam
300	iOS Mail Conversion
300	Basic Level Malware Analysis
400	Camera Shy Steganography Challenge
400	Linux LUKS Volume Decryption
400	Cryptomathic File2File Decryption
400	Deleted Drive Recovery
400	Advanced Malware Analysis
500	Linux Executable Packer
500	Windows Executable Packer
500	File Activity Timeline
500	Volume Shadow Copy Analyzer
500	Windows File Tag Analysis

*Bonus Challenge Added 03/30/2012

**Bonus Challenge Added 07/02/2012



2012 DC3 Digital Forensics Challenge



A-2: SANS

Logo(s)	Description
	The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals around the world. A range of individuals from auditors and network administrators, to chief information security officers are sharing the lessons they learn and are jointly finding solutions to the challenges they face. At the heart of SANS are the many security practitioners in varied global organizations from corporations to universities working together to help the entire information security community.
Website URL	Qualifications
sans.org	<p>Win 1st place in one of the following categories:</p> <ul style="list-style-type: none"> • US High School • US Undergraduate • US Graduate <p>Additional requirements for all team members:</p> <ul style="list-style-type: none"> • All team members must hold US citizenship. • Must be actively attending as a student at a High School, Undergraduate or Graduate College upon submission of results as per the Academic Criteria in Section 5.3. • Be able to travel from within the Continental United States in order to claim the trip to the Conference (US citizens abroad are eligible providing they transport themselves to the Continental United States). • Any team or team member(s) under the age of 18 must provide a completed DC3 Permission to Participate Form to participate in the challenge. • Meet all other DC3 Challenge Rules requirements.

Prizes:

Category	Place	Prize
US High School	1 st	For up to 4 team members: Airfare and lodging to the 2012 DoD Cyber Crime Conference (airfare, lodging, and paid conference fees)
US Undergraduate	1 st	For up to 4 team members: Airfare and lodging to the 2012 DoD Cyber Crime Conference (airfare, lodging, and paid conference fees)
US Graduate	1 st	For up to 4 team members: Airfare and lodging to the 2012 DoD Cyber Crime Conference (airfare, lodging, and paid conference fees)



2012 DC3 Digital Forensics Challenge



A-3: EC-Council

Logo(s)	Description
	<p>With over 450 training locations of its information security courses in over 60 countries, the International Council of Electronic Commerce Consultants (EC-Council) provides technical training and certification for the Information Security community. It is the most trusted source for vendor neutral Information Security training solution. EC-Council and DC3 have partnered to provide a Digital Forensic Challenge opportunity for both US Government and US Military team prizes along with Civilian and Commercial teams for all US and non-US entries. This opportunity will provide additional prizes for winners in these categories for continuing education in the information security field.</p>
Website URL	Qualifications
<p>eccouncil.org</p>	<p>Win 1st place in the one of the following categories:</p> <ul style="list-style-type: none"> • Global Civilian • Global Commercial • Global High School • Global Undergraduate • Global Graduate • US Government • US Military <p>Additional requirements for all team members:</p> <ul style="list-style-type: none"> • Civilian, Commercial, and Academic team prize eligibility requirements: <ul style="list-style-type: none"> ○ Team members may consists of US and/or non-US citizens ○ Must be actively attending as a student at a High School, Undergraduate or Graduate College upon submission of results as per the Academic Criteria in Section 5.3. • Government and Military team prize eligibility requirements <ul style="list-style-type: none"> ○ Team members <u>must</u> hold US citizenship. ○ Government: Must work in a US Government position at a Federal, State, or Local Government agency. This excludes contractors. ○ Military: Must work in a US Military position that is a military member or civil servant. This excludes contractors. • Additional prize eligibility requirements are as follows: <ul style="list-style-type: none"> ○ All team members are responsible for travel arrangements and costs • Any team or team member(s) under the age of 18 must provide a completed DC3 Permission to Participate Form to participate in the challenge. • Meet all other DC3 Challenge Rules requirements.



2012 DC3 Digital Forensics Challenge



Prizes:

Category	Place	Prize
Global Civilian	1 st	For up to 4 team members: <ul style="list-style-type: none">• A Plaque• A Pass to the Hacker Halted Conference worth \$1799• Any free EC-Council electronic courseware of choice for the winners on Ethical Hacking, Computer Forensic, Security Analysis or Disaster Recovery worth \$650 each
Global Commercial	1 st	For up to 4 team members: <ul style="list-style-type: none">• A Plaque• A Pass to the Hacker Halted Conference worth \$1799• Any free EC-Council electronic courseware of choice for the winners on Ethical Hacking, Computer Forensic, Security Analysis or Disaster Recovery worth \$650 each
US Government	1 st	For up to 4 team members: <ul style="list-style-type: none">• A Plaque• A Pass to the Hacker Halted Conference worth \$1799• Any free EC-Council electronic courseware of choice for the winners on Ethical Hacking, Computer Forensic, Security Analysis or Disaster Recovery worth \$650 each
US Military	1 st	For up to 4 team members: <ul style="list-style-type: none">• A Plaque• A Pass to the Hacker Halted Conference worth \$1799• Any free EC-Council electronic courseware of choice for the winners on Ethical Hacking, Computer Forensic, Security Analysis or Disaster Recovery worth \$650 each
Global High School	1 st	For up to 4 team members: <ul style="list-style-type: none">• A Plaque• A Pass to the Hacker Halted Conference worth \$1799• Any free EC-Council electronic courseware of choice for the winners on Ethical Hacking, Computer Forensic, Security Analysis or Disaster Recovery worth \$650 each
Global Undergraduate	1 st	For up to 4 team members: <ul style="list-style-type: none">• A Plaque• A Pass to the Hacker Halted Conference worth \$1799• Any free EC-Council electronic courseware of choice for the winners on Ethical Hacking,



2012 DC3 Digital Forensics Challenge



		Computer Forensic , Security Analysis or Disaster Recovery worth \$650 each
Global Graduate	1 st	For up to 4 team members: <ul style="list-style-type: none">• A Plaque• A Pass to the Hacker Halted Conference worth \$1799• Any free EC-Council electronic courseware of choice for the winners on Ethical Hacking, Computer Forensic, Security Analysis or Disaster Recovery worth \$650 each



2012 DC3 Digital Forensics Challenge



A-4: AFCEA

Logo(s)	Description
	<p>AFCEA International, established in 1946, is a non-profit membership association serving the military, government, industry, and academia as an ethical forum for advancing professional knowledge and relationships in the fields of communications, IT, intelligence, and global security.</p>
Website URL	Qualifications
<p>afcea.com</p>	<p>Win 1st place in the US Government, US Military, or the US Undergraduate category.</p> <p>Additional requirements per category for all team members:</p> <ul style="list-style-type: none"> • US Government <ul style="list-style-type: none"> ○ Must hold a US citizenship ○ Must work in a US Government position as per the Challenge rules. • US Military <ul style="list-style-type: none"> ○ Must hold a US citizenship ○ Must work in a US Military position as per the Challenge rules. • US Undergraduate <ul style="list-style-type: none"> ○ Must hold a US citizenship. ○ Must be actively attending as a student to a US Undergraduate College upon <u>submission of their last result</u> as per the academic Challenge Rules. • Any team or team member(s) under the age of 18 must provide a completed DC3 Permission to Participate Form to participate in the challenge. • Meet all other DC3 Challenge Rules requirements.

Prizes:

Category	Place	Prize
US Government	1 st	One year membership
US Military	1 st	One year membership
US Undergraduate	1 st	One year membership



A-5: BlackBag

Logo(s)	Description
	BlackBag Technologies, Inc. provides Mac-based forensic and eDiscovery data solutions to law enforcement and private sector clients. Based in Silicon Valley, our company offers clients a comprehensive suite of services, software and training solutions. BlackBag acknowledges the growing challenges faced by forensic examiners and legal professionals in the field and is dedicated to creating flexible, open environment solutions. We serve a wide range of clients including federal, state and local law enforcement agencies as well as leading private sector security, legal and human resource professionals.
Website URL	Qualifications
blackbagtech.com	<p>Win 1st place as the overall point's leader for all US teams across all team categories.</p> <p>Additional requirements for all team members:</p> <ul style="list-style-type: none"> Any team or team member(s) under the age of 18 must provide a completed DC3 Permission to Participate Form to participate in the challenge. Meet all other DC3 Challenge Rules requirements.

Prizes:

Category	Place	Prize
US Overall	1 st	<p>One per team:</p> <ul style="list-style-type: none"> BBT Forensic Kit: OGIO Lap Top Bag w/BBT Logo, BBT Mug BBT Notepad BBT Pens BBT Voucher good for all software BlackLight MacQuisition SoftBlock



2012 DC3 Digital Forensics Challenge



A-6: NIST OLES

Logo(s)	Description
	<p>The Law Enforcement Standards Office (OLES) helps criminal justice, public safety, emergency responder, and homeland security agencies make informed procurement, deployment, applications, operating, and training decisions, primarily by developing performance standards, measurement tools, operating procedures and equipment guidelines. This ensures that the equipment law enforcement, corrections, criminal justice, and public safety agencies purchase and the technologies they use are safe, dependable, and effective. OLES is located on the National Institute of Standards and Technology (NIST) campus in Gaithersburg, Maryland.</p>
Website URL	Qualifications
<p>nist.gov/oles</p>	<p>Win 1st place in US Government category.</p> <p>Additional requirements per category for all team members:</p> <ul style="list-style-type: none"> • Must hold a US citizenship • Must work in a US Government position at a Federal, State, or Local Government agency. This excludes contractors. • All team members must be able to travel from within the Continental United States in order to claim the trip to the Conference (US citizens abroad are eligible providing they transport themselves to the Continental United States.) • Meet all other DC3 Challenge Rules requirements.

Prizes:

Category	Place	Prize
US Government	1 st	<p>For up to 4 team members: Trip to the 2012 DoD Cyber Crime Conference based on government per Diem (airfare, lodging, meals, and paid conference fees) for up to 4 team members.</p>



2012 DC3 Digital Forensics Challenge



A-7: National Board of Information Security Examiners (NBISE)

Logo(s)	Description
	<p>National Board of Information Security Examiners (NBISE) mission is to increase the security of information networks, computing systems, and industrial and military technology by improving the potential and performance of the cyber security workforce.</p> <p>NBISE was formed to leverage the latest advances in assessment and learning science towards the solution of one of the United States' most critical workforce shortages: cyber security professionals. Through its Advanced Defender Aptitude and Performance Testing and Simulation (ADAPTS) program, NBISE coordinates the work of teams of practitioners, researchers, and educators which develop and validate or enhance existing performance-based learning and assessment vehicles to materially accelerate the acquisition of hands-on skill and tacit knowledge by students and practitioners in collegiate and continuing education programs. NBISE's work and research seeks to develop assessment instruments to reliably predict future performance and aptitude for cyber security jobs, allowing for a better understanding of the efficacy of performance-based learning platforms.</p>
Website URL	Qualifications
<p>https://www.nbise.org/</p>	<p>Win 1st place in the US Community College category.</p> <p>All team members must:</p> <ul style="list-style-type: none"> • Provide the name of the US Community College they are attending in their team's application form • Actively attending a US Community College at the time of their submission as High School Students and/or Undergraduate Students • Team members may consist of US and/non-US citizens • Meet all other academic Challenge Rules requirements. • Any team or team member(s) under the age of 18 must provide a completed DC3 Permission to Participate Form to participate in the challenge. • Meet all other DC3 Challenge Rules requirements.

Prizes:

Category	Place	Prize
US Community College	1 st	For up to 4 team members: Trip to the 2012 DoD Cyber Crime Conference based on government per Diem (airfare, lodging, meals, and paid



2012 DC3 Digital Forensics Challenge



	conference fees).
--	-------------------

A-8: AccessData

Logo(s)	Description
	<p>AccessData has pioneered digital investigations for 20+ years, serving government agencies, law enforcement and corporations worldwide. AccessData delivers computer forensics, cyber defense, decryption, information assurance and eDiscovery solutions and training.</p> <p>Access data provides training in Forensics, Network Forensics, Network Defense, Password cracking, eDiscovery, Attorney Review products and Mobile Forensics from our training centers and on line.</p>
Website URL	Qualifications
<p>accessdata.com</p>	<p>Win 1st place in the US Undergraduate category.</p> <p>All team members must:</p> <ul style="list-style-type: none"> • Hold a US citizenship. • Actively attending as a student to a US Undergraduate College upon <u>submission of their last result</u> as per the academic Challenge Rules. • Meet all other DC3 Challenge Rules requirements.

Prizes:

Category	Place	Prize
US Undergraduate	1 st	<p>For each team member:</p> <ul style="list-style-type: none"> • Copy of Access Data FTK current version • Two free training classes (online or in classroom) • Optional 60 Day internship • Paid travel expenses and hotel room • Possible remuneration will be based on ability to contribute



2012 DC3 Digital Forensics Challenge



A 9: Best Buy

Logo(s)	Description
	Since its inception in 1966, Best Buy Co, Inc. has grown steadily and enhanced its business through inspired innovations. Community partnership is central to the way Best Buy does business. It believes in the power of our youth and shows its support by sponsoring the DC3 Challenge educational winners.
Website URL	Qualifications
www.bestbuy.com	<ul style="list-style-type: none"> • Win 1st place as the overall points leader for all U.S. teams across all team categories. • Any team or team member(s) under the age of 18 must provide a completed DC3 Permission to Participate Form to participate in the challenge. • Meet all other Challenge Rules requirements.

Prizes:

Category	Place	Prize
US High School	1 st	One per team Member: <ul style="list-style-type: none"> • \$250 Best Buy Gift Card (up to 4 per team)
US Community College	1 st	One per team Member: <ul style="list-style-type: none"> • \$250 Best Buy Gift Card (up to 4 per team)
US Undergraduate teams	1 st	One per team Member: <ul style="list-style-type: none"> • \$250 Best Buy Gift Card (up to 4 per team)