

**2011 DC3 DIGITAL FORENSICS
CHALLENGE RULES
v1.3**

29 Sep 2011



2011 DC3 Digital Forensics Challenge



Rules Change Summary

| Section | Change Description | Date Changed |
|-----------------------------|---|--------------|
| 5.4, 6.0, 8.0 | Added Source Code requirements for tool and script submissions for validation and testing | 3 Aug 2011 |
| 1.2, 4.3, 4.4, 5.4.1, 5.4.2 | Clarified Exercises for Challenge wording | 3 Aug 2011 |
| 4.0 | Moved Sponsors from Section 4.0 to own Appendix per Sponsor (A-2 to A-6) | 3 Aug 2011 |
| 3.0-10.0 | Renumbered Sections | 3 Aug 2011 |
| Appendix A-7 to A-13 | Added New Sponsors: AFECA, BlackBag, NIST OLEC, Paraben, US Cyber Challenge, AccessData, Dell | 3 Aug 2011 |
| Table of Contents | Updated to reflect section renumbering and added content | 3 Aug 2011 |
| 3.4 | Changed "Challenge" To "Exercise" in Bonus schedule chart | 3 Aug 2011 |
| Appendix A-6 | Updated UK Cyber Challenge Logo and Header | 3 Aug 2011 |
| 2.2 | Added "Community College" to Team Affiliations | 3 Aug 2011 |
| A-5 | Updated EC-Council's description | 3 Aug 2011 |
| A-5 | Updated EC-Council's qualification | 16 Aug 2011 |
| A-5 | Updated EC-Council's Prizes | 16 Aug 2011 |
| A-14 | Added New Sponsor: McAfee | 29 Sep 2011 |
| Table of Contents | Updated to reflect section renumbering and added content | 29 Sep 2011 |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |



Table of Contents

1.0 INTRODUCTION.....5

 1.1 BACKGROUND5

 1.2 OVERVIEW5

 1.3 OBJECTIVES.....5

2.0 ELIGIBILITY CRITERIA.....5

 2.1 REGISTRATION.....5

 2.2 REQUIREMENTS5

3.0 THE CHALLENGE.....7

 3.1 CHALLENGE OBJECTIVES.....7

 3.2 CHALLENGE RULES7

 3.3 CHALLENGE GRADING.....8

 3.4 CHALLENGE BONUS POINTS8

 3.5 CHALLENGE SCHEDULE / KEY DATES.....8

4.0 PRIZE CRITERIA.....9

 4.1 SPONSORS9

 4.2 PRIZES.....9

 4.3 ACADEMIC CRITERIA.....9

 4.3.1 Graduate 10

 4.3.2 Undergraduate 10

 4.3.3 High School..... 10

 4.4 JUDGING AND CHALLENGE RULES11

 4.4.1 Methods to Submit Solutions 11

 4.4.2 Terms of Submitting Solutions..... 11

 4.4.3 Terms of Submitting Tools Used in Solving Challenges 12

5.0 INTELLECTUAL PROPERTY.....13

6.0 LIMITATION OF LIABILITY13

7.0 TEAM DISQUALIFICATION14

8.0 CHALLENGE CANCELLATION.....14

9.0 PRIVACY POLICY14

 9.1 DOD PRIVACY ACT STATEMENT15

 9.2 CONTACT PURPOSES15

 9.3 STATISTICAL PURPOSES15

APPENDIX.....16

 A-1: CHALLENGES AND POINT STRUCTURE16

 A-2: SANS17

 A-3: IMPACT.....19

 A-5: EC-COUNCIL21

 A-6: CYBER SECURITY CHALLENGE UK24



2011 DC3 Digital Forensics Challenge



| | |
|---------------------------------|----|
| A-7: AFCEA | 25 |
| A-8: BLACKBAG | 26 |
| A-9: NIST OLEC | 27 |
| A-10: PARABEN CORPORATION..... | 28 |
| A-11: U.S. CYBER CHALLENGE..... | 29 |
| A-12: ACCESSDATA | 30 |
| A-13: DELL..... | 31 |
| A-14: MCAFEE..... | 32 |



1.0 INTRODUCTION

1.1 *Background*

The Department of Defense Cyber Crime Center (DC3) sets standards for digital evidence processing, analysis, and diagnostics for any Department of Defense (DOD) investigation that requires computer forensic support to detect, enhance, or recover digital media, including audio and video. DC3 assists in criminal, counterintelligence, counterterrorism, and fraud investigations of the Defense Criminal Investigative Organizations (DCIOs) and DOD counterintelligence activities. It also supports safety investigations, the Inspector General, and commander-directed inquiries. DC3 aids in meeting intelligence community document exploitation objectives from criminal law enforcement, digital forensic, and counterintelligence perspectives. DC3 provides computer investigation training to forensic examiners, investigators, system administrators, and any other DOD members who must ensure Defense Information Systems are secure from unauthorized use, criminal and fraudulent activities, and foreign intelligence service exploitation. DC3 remains on the leading edge of computer technologies and techniques through research, development, testing, and evaluation applied to digital evidence processing and computer forensic analysis; and by partnering with governmental, academic, and private industry computer security officials.

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. Approximately 25 different exercises ranging from basic forensics to advanced tool development are being provided to all participants. The levels (100-500) are broken down into single based exercises and are designed to be unique and separate from one another.

1.3 *Objectives*

The objectives of the Annual Digital Forensics Challenge are to establish relationships; resolve technological issues; and develop new tools, techniques, and methodologies for the digital forensic community.

2.0 ELIGIBILITY CRITERIA

2.1 *Registration*

Registration is designed to be completed online via the DC3 2011 Challenge website at <http://www.dc3.mil/challenge/2011>. 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*

DC3 Challenge entry 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:



2011 DC3 Digital Forensics Challenge



- An individual cannot participate on more than one (1) team or compete with multiple entries.
- 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 personal information (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 disqualify your team from challenge participation as per Section 8.0 – Team Disqualification.*
 - All changes to team members (add/update/remove) and their related information are the responsibility of team POC to update with the DC3 Challenge Team **in writing** to challenge@dc3.mil .
- 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 Challenge.
 - Each team member's affiliation should be relevant to when team challenges' submissions are sent to DC3 (NOT when registered):
 - **Civilian** – A person or team **NOT** an academic student, in the Military, working for the Federal Government or working in the Commercial / Private Sector.
 - **Commercial** – A person or team that is employed for a Commercial / Private Sector representing their company. This includes contractors that work for Military, Federal, State and Local Government agencies.
 - **Government** – A person or team that works 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.
 - **Undergraduate Student** – A person or team that is attending 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 attending a graduate school as a student and has **NOT** graduated before the submission of the final Challenge package.



2011 DC3 Digital Forensics Challenge



- 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 5.3 – 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 assessed as 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 5.2 - Prize Eligibility for further details.
- Any changes of team member affiliation after approval to participate 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 8.0 – Team Disqualification.
- For specific national-based prizes, all team members must be of the same citizenship category (example: U.S. or Non-U.S.) as per the prize’s rules. Mixed citizenship teams consisting of U.S. and Non-U.S citizenship players will be assigned as a mixed team affiliation
- 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 10.0 – Team Disqualification.

DC3 employees, current and former within the past year (2010), and their relatives are ineligible to participate for prizes; however they may compete for points only.

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 DC3 Challenge Website (www.dc3.mil/challenge) 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 23 single scenario based problem exercises. The chart of each specific exercise and corresponding points can be found in the Appendix under A-2 Exercises and Point Structure. There are five (5) 100 point exercises, four (4) 200 point exercises, four (4) 300 point exercises, three (3) 400 point exercises, and seven (7) 500 point exercises.

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 2010 -- 1 May 2011 | 20% |
| 2 May 2011 -- 1 July 2011 | 10% |
| 2 July 2011 -- 1 Oct 2011 | 5% |
| 2 Oct 2011 -- 1 Nov 2011 | 0% |

Example:

- Team A submits their exercise 101 submission on 1 Feb 2011.
- DC3 grades Team A's exercise 101 submission after 1 May 2011.
 - 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 2011 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

- **4 Dec 2010 – Announcement of DC3 Challenge 2011**
- **15 Dec 2010 - Registration Begins**
 - Registration and Challenge packets containing all of the challenge materials will be available for download only on or about 15 December 2010.
 - Applications received each day by close of business (COB) will be processed within 1-3 business days for approval.
- **26 Jan 2011 – Official announcement** at the 2011 DC3 Cyber Crime Conference, Atlanta, GA



2011 DC3 Digital Forensics Challenge



- **1 May 2011 – Last day for 20% Bonus points**
- **1 July 2011 – Last day for 10% Bonus points**
- **1 Oct 2011 – Last day for 5% Bonus points**
- **1 Nov 2011 - Registration Ends**
 - Registrations are no longer accepted to the Challenge 2011.
- **2 Nov 2011 – Submission Entry Deadline**
 - All DC3 Challenge 2011 solutions, including scripts and non-commercial programs created by the team, must be uploaded or postmarked to DC3 no later than November 1st, 2011 at 11:59:59 PM EST to be eligible for a prize in their assigned category.
 - Exercise solutions received after 1 November 2011 EST will not be accepted for prizes. Scoring after this date will be at the discretion of DC3.
- **1 Dec 2011 – DC3 Challenge Winners Announced**
 - 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 download of challenge level packet 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 internationally within the Cyber and Digital Forensic Communities
- Support the organization's missions and/or objectives
- Provide support of the U.S. and international Cyber Challenges for educating those up and coming in the fields for Cyber Defense and Digital Forensics

An official list of the 2011 DC3 Challenge sponsors can be found in Appendix A-2: Prize Sponsorships.

4.2 Prizes

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

Each member of the winning team will also receive a plaque as well as formal recognition at the conference by DC3.

4.3 Academic Criteria

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



2011 DC3 Digital Forensics Challenge



- Team member must be enrolled and in good standing for the academic institution attending ON the date you submit your 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 (PG)** category if they are still in a Graduate school on the date when the Challenge 2011 package **is submitted** (*not when you apply*).
- PG team (s) who submits their package **prior** to graduating will be placed in the PG category.
- PG team (s) who submits their package **after** graduating will be placed in the category of Military, Federal Government, 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 Graduation Aug 2011 changes to Dec 2011 – status will remain in the PG 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 2011 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 PG 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 Challenge 2011 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.



2011 DC3 Digital Forensics Challenge



- 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

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 with 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 exercise 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 4.5 - 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:

- For each tool (software, script, and method/technique) used in your Challenge solutions, it is documented in each individual exercise as per Section 5.4.3 – Terms of Submitting Tools Used in Solving Challenges
- 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 01st, 2011 and the same individual exercise is uploaded on Oct 10th 2011 for the same Challenge level, the first submission only will be graded.

- Teams are responsible for verifying their submissions are accurate before providing to DC3.
- 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 certify that it is free of those malicious computer programs.



2011 DC3 Digital Forensics Challenge



- 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 can disqualify a team as per Section 8.0 – Team Disqualification:

- **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 tool and script submissions
 - For level 500 tools, include additional documentation:
 - Include 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 Challenge solution(s).
 - A copy of the source code for validation and testing by DC3
 - For level 500 tools, include addition data:
 - 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 2011 DC3 Challenge.

- 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’s company



2011 DC3 Digital Forensics Challenge



- 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 Challenge participants are for the purposes of Research and Development (R&D) of digital forensics in furthering advancement for the U.S. Government and the digital forensics community.

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 U.S. 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 U.S. Government with the power to the U.S. Government to grant licenses for all governmental purposes.
- Provided at no cost to the U.S. 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. These tools, techniques, solutions, and responses may be documented and publicized in addition with 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 the DC3 Challenge participation.

It is recommended that all teams double-check their 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, 2010 and is found to be free of



2011 DC3 Digital Forensics Challenge



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 5.4.3 -- 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 and during the 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 5.0 – Prize Criteria
- Statistical reporting of the DC3 Challenge to the public and 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



2011 DC3 Digital Forensics Challenge



9.1 DOD Privacy Act Statement

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

9.2 Contact Purposes

DC3 Challenge will remain the primary contact for any request for contact information for Challenge teams during the Challenge process. These requests will be routed by DC3 Challenge to the Challenge team leader for approval for release. It is the Challenge 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, U.S. 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 | Windows Registry Analysis |
| 100 | File Hash Identification |
| 100 | File Signature Analysis |
| 100 | Creation of Affidavit for Search Seizure Warrant |
| 100 | Hot Spot Surveillance |
| 200 | File Data Examination |
| 200 | Steganography Level 2 |
| 200 | Password Cracking |
| 200 | VMWare Memory Analysis |
| 300 | Network Trap and Trace |
| 300 | Encrypted Device Image |
| 300 | Shadow Volume Win7 Registry Analysis |
| 300 | Unallocated File Recovery |
| 400 | Shadow Volumes Analysis |
| 400 | Steganography Level 4 |
| 400 | Encrypted Drive Recovery |
| 500 | Language Identifier and Translator Tool Development |
| 500 | Imaging the Android OS Tool Development |
| 500 | MFT File Reader |
| 500 | Text String Searching Tool Development |
| 500 | Data Recovery from HPA as a Universal Tool or per Manufacturer Tool Development |
| 500 | Data Recovery from Unmarried TPM Hard Disk Tool Development |
| 500 | VSC Parser Tool Development |



2011 DC3 Digital Forensics Challenge



A-2: SANS

| Logo(s) | Description |
|---|--|
|  | <p>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.</p> |
| Website URL | Qualifications |
| <p>http://www.sans.org/</p> | <p>Win 1st place in 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 U.S. citizenship. • All team members are actively attending as a U.S. student at a U.S. High School, U.S. Undergraduate or U.S. Graduate College upon submission of your 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 (U.S. 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 Challenge Rules requirements. |

Prizes:

| Category | Place | Prize |
|------------------|-----------------|---|
| US High School | 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 conference fees) |
| US Undergraduate | 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 |



2011 DC3 Digital Forensics Challenge



| | | |
|-------------|-----------------|---|
| | | conference fees) |
| US Graduate | 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 conference fees) |



2011 DC3 Digital Forensics Challenge



A-3: IMPACT

| Logo(s) | Description |
|---|---|
| | IMPACT is dedicated to bringing together governments, academia, industry leaders and cybersecurity experts to enhance the global community's capacity to prevent, defend against and respond to cyber threats. IMPACT's Global HQ is located in Cyberjaya, Malaysia. |
| Website URL | Qualifications |
| http://www.impact-alliance.org | <p>1st place International Winner</p> <ul style="list-style-type: none"> All team participants <u>DO NOT</u> hold U.S. citizenship. All team members' legal residences are located <u>outside of the U.S.</u> *AND* in an IMPACT member country (any country listed on the following website: http://www.itu.int/cgi-bin/htsh/mm/scripts/mm.list?_search=ITUstates) All team members must meet all other non-U.S. Challenge Rules and Requirements. All current DC3 or IMPACT personnel and former DC3 or IMPACT personnel who are within one calendar year (1 Jan 2010) are ineligible to participate. Any team or team member(s) under the age of 18 must provide a completed <u>DC3 Permission to Participate Form</u> to participate in the challenge. Meet all other <u>Challenge Rules</u> requirements. |

Prizes:

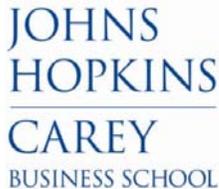
| Category | Place | Prize |
|----------------------|-----------------|---|
| International Winner | 1 st | For up to 4 team members: Trip to Malaysia for IMPACT Training |



2011 DC3 Digital Forensics Challenge



A-4: JHU/CyberWatch

| Logo(s) | Description |
|--|--|
|   | <p>With a history of educating business leaders since 1916, the Johns Hopkins Carey Business School specializes in creating innovative programs that anticipate and reflect global business trends. The School also draws upon the strengths of other Johns Hopkins schools, including the Johns Hopkins Bloomberg School of Public Health, the School of Medicine, School of Nursing, the Whiting School of Engineering, and the Zanvyl Krieger School of Arts and Sciences.</p> <p>CyberWatch (CW) is a consortium of higher education institutions, businesses, and government agencies focused on building and maintaining a stronger information assurance workforce. Consortium participants collaborate to share best practices, methodologies, curricula, and course modules and materials. It is an Advanced Technological Education (ATE) Center, headquartered at Prince George's Community College, and funded by a grant from the National Science Foundation (NSF). The CyberWatch goals are focused on information assurance (IA) education at all levels, from elementary through graduate school, but especially the community college level, and include curriculum development, faculty professional development, student development, career pathways, and public awareness.</p> |
| Website URL | Qualifications |
| <p>http://carey.jhu.edu/</p> <p>http://www.cyberwatchcenter.org/</p> | <p>Win 1st place in The US Community College Category.</p> <ul style="list-style-type: none"> • All team members must name the U.S. Community College they are attending in their team's application form • All team members must be actively attending a U.S. Community College at the time of their submission as High School Students and/or Undergraduate Students • Team members may consist of U.S. and/non-U.S. citizens • 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 Community College | 1 st | Recognition |



2011 DC3 Digital Forensics Challenge



A-5: 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 U.S. Government and U.S. Military team prizes along with Civilian and Commercial teams for all U.S. and non-U.S. 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>http://www.eccouncil.org/</p> | <ul style="list-style-type: none"> • Win 1st place in the following categories: <ul style="list-style-type: none"> ○ International Civilian ○ International Commercial ○ International High School ○ International Undergraduate ○ International Graduate ○ US Government ○ US Military • Civilian, Commercial, and Academic team prize eligibility requirements: <ul style="list-style-type: none"> ○ Team members may consists of U.S. and/or non-U.S. 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 U.S. citizenship. ○ Government: Must work in a U.S. Government position at a Federal, State, or Local Government agency. This excludes contractors. ○ Military: Must work in a U.S. 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 Challenge Rules requirements. |



2011 DC3 Digital Forensics Challenge



Prizes:

| Category | Place | Prize |
|-----------------------------|-----------------|---|
| International 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 |
| International 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 |
| International 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 |
| International 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 |



2011 DC3 Digital Forensics Challenge



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



A-6: Cyber Security Challenge UK

| Logo(s) | Description |
|--|--|
|  | <p>Cyber Security Challenge UK is a program of national challenges, designed by experts, to identify and nurture the UK's future cyber security workforce. Established by a management consortium of key figures in cyber security, it will test the nation's cyber skills, excite and inspire entrants to develop their talents, and clarify and enable pathways to the increasingly challenging and diverse range of cyber security jobs.</p> |
| Website URL | Qualifications |
| <p>https://cybersecuritychallenge.org.uk/</p> | <ul style="list-style-type: none"> • Win 1st place in the UK Cyber Challenge Category. • Team members must be UK citizens only and must have primary residency in the UK. Teams must also be registered at the UK Challenge website at https://cybersecuritychallenge.org.uk/candidates/registration.html • 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 |
|--------------------|-----------------|--|
| UK Cyber Challenge | 1 st | For up to 4 team members: Two weeks at the new UK Cyber Security Academy Invitations to take part in the Cyber Security Challenge UK's masterclass challenge |



2011 DC3 Digital Forensics Challenge



A-7: 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>http://www.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 U.S. citizenship ○ Must work in a U.S. Government position as per the Challenge rules. • US Military <ul style="list-style-type: none"> ○ Must hold a U.S. citizenship ○ Must work in a U.S. Military position as per the Challenge rules. • US Undergraduate <ul style="list-style-type: none"> ○ Must hold a U.S. citizenship. ○ Must be actively attending as a student to a U.S. 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 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-8: 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 |
| http://blackbagtech.com | <p>Win 1st place as the overall point's leader for all U.S. teams across all team categories.</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 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/Mobilyze MacQuisition SoftBlock |



2011 DC3 Digital Forensics Challenge



A-9: NIST OLEC

| Logo(s) | Description |
|---|--|
|  | <p>The Law Enforcement Standards Office (OLEC) 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>http://www.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 U.S. citizenship • Must work in a U.S. 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 (U.S. citizens abroad are eligible providing they transport themselves to the Continental United States.) • Meet all other 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> |



2011 DC3 Digital Forensics Challenge



A-10: Paraben Corporation

| Logo(s) | Description |
|---|--|
|  | Paraben specializes in comprehensive digital forensic solutions for handhelds, hard drives, and enterprise networks. Handheld innovations offer 360 degrees of solution power from seizure to analysis. The hard drive solutions move to the next level solving problems through a specialized tool approach and a single command suite. Enterprise technologies top off the repertoire with proactive and reactive solutions for a network. These solutions work through a stealth client server system that respond or prepare you for any issue in your network where forensic-grade data is key. |
| Website URL | Qualifications |
| http://paraben.com | <p>Win 1st or 2nd place in US Government or US Military categories OR win 1st place in the US Undergraduate category.</p> <p>Additional requirements per category for all team members:</p> <ul style="list-style-type: none"> • Must hold a U.S. citizenship. • US Government / US Military <ul style="list-style-type: none"> ○ Must work in a U.S. Government or Military position as per the Challenge rules • US Undergraduate <ul style="list-style-type: none"> ○ Must be actively attending as a student to a U.S. 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 Challenge Rules requirements. |

Prizes:

| Category | Place | Prize |
|------------------|-----------------|--|
| US Government | 1 st | One per team: Paraben Device Seizure Software & Toolbox |
| | 2 nd | |
| US Military | 1 st | One per team: Paraben Device Seizure Software & Toolbox |
| | 2 nd | |
| US Undergraduate | 1 st | Per team member: <ul style="list-style-type: none"> • Paraben P2 Commander Kit • Eligible for paid internship at Paraben <ul style="list-style-type: none"> ○ 1-2 members per semester ○ Travel and expenses excluded |
| | | |



2011 DC3 Digital Forensics Challenge



A-11: U.S. Cyber Challenge

| Logo(s) | Description |
|---|---|
|  | <p>The mission of the U.S. Cyber Challenge (USCC) is to significantly reduce the shortage in the cyber workforce by identifying, attracting, recruiting and placing the next generation of cyber security professionals. The Center for Internet Security's Cybersecurity Workforce Development Division (CWD) serves as the Chair and a member of the U.S. Cyber Challenge Coalition. The Center for Internet Security (CIS) is a national not-for-profit organization comprising three divisions: Security Benchmarking, Multi-State Information Sharing and Analysis Center, and Cybersecurity Workforce Development. Through its three divisions, CIS is responsible for development and distribution of benchmarks that establish standards for the secure configuration of information technology systems; provision of cyber security for state, local, tribal and territorial governments; and the identification and development of potential talent for the cyber security workforce of the future. U.S. Cyber Challenge is a division of the Center for Internet Security.</p> |
| Website URL | Qualifications |
| <p>uscyberchallenge.org</p> | <p>Win 1st place in the US Community College Category.</p> <ul style="list-style-type: none"> All team members must name the U.S. Community College they are attending in their team's application form All team members must be actively attending a U.S. Community College at the time of their submission as High School Students and/or Undergraduate Students Team members may consist of U.S. and/non-U.S. 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 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 conference fees). |



2011 DC3 Digital Forensics Challenge



A-12: 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 |
| http://www.accessdata.com | <p>Win 1st place in the US Undergraduate category</p> <p>All team members must:</p> <ul style="list-style-type: none"> • Hold a U.S. citizenship. • Actively attending as a student to a U.S. Undergraduate College upon <u>submission of their last result</u> as per the academic Challenge Rules. • Meet all other Challenge Rules requirements. |

Prizes:

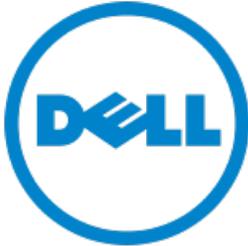
| Category | Place | Prize |
|------------------|-----------------|---|
| US Undergraduate | 1 st | <p>For each team member:</p> <ul style="list-style-type: none"> • Copy of Access Data FTK current version • Two free training classes (online or in classroom) • Optional 60 Day internship • Paid travel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



2011 DC3 Digital Forensics Challenge



A-13: Dell

| Logo(s) | Description |
|---|---|
|  | <p>Michael Dell founded the company in 1984 in Austin, TX with \$1000 and a vision of how technology should be designed, manufactured & sold. Today, Dell connects with more than 5.4 million customers every day by the phone, in person, on dell.com and, increasingly, through social networking sites. Dell makes technology more accessible to people and organizations around the world and ships more than 10,000 systems every day to customers in 180 countries — more than one every second.</p> |
| Website URL | Qualifications |
| | <ul style="list-style-type: none"> • Win 1st place in the Overall U.S. Winner and U.S. High School Student Categories • Team members may consist of U.S. and/non-U.S. 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 Challenge Rules requirements. |

Prizes:

| Category | Place | Prize |
|---------------------|-----------------|--|
| U.S. Overall Winner | 1 st | For up to 4 team members: <ul style="list-style-type: none"> • Dell Streak 7 tablet |
| U.S. High School | 1 st | For up to 4 team members: <ul style="list-style-type: none"> • Dell Streak 7 tablet |



2011 DC3 Digital Forensics Challenge



A-14: McAfee

| Logo(s) | Description |
|---|--|
|  | McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee's "Safe Never Sleeps" brand defines them as a company, and as a global team of professionals who are dedicated to tackling the world's toughest security challenges. |
| Website URL | Qualifications |
| www.mcafee.com | <ul style="list-style-type: none"> Win 1st place in The US Community College Category. All team members must provide their U.S. Community College they are attending in their team's application form All team members must be actively attending a U.S. Community College at the time of their submission as High School Students and/or Undergraduate Students Team members may consist of U.S. and/non-U.S. citizens Meet all other and 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 Challenge Rules requirements. <p style="text-align: center;">OR</p> <ul style="list-style-type: none"> Win 1st place in the UK Cyber Challenge Category. Team members must be UK citizens only and must have primary residency in the UK. Teams must also be registered at the UK Challenge website at https://cybersecuritychallenge.org.uk/candidates/registration.html 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 Community College | 1 st | Four up to four (4) team members: <ul style="list-style-type: none"> Skullcandy headphones Hacking Exposed book McAfee Total Protection software Lunch box/sack |



2011 DC3 Digital Forensics Challenge



| | | |
|---------------------|-----------------|---|
| | | <ul style="list-style-type: none">• Flashlight• Lock• McAfee Encrypted USB drive |
| UK Challenge Winner | 1 st | Four up to four (4) team members: <ul style="list-style-type: none">• Skullcandy headphones• Hacking Exposed book• McAfee Total Protection software• Lunch box/sack• Flashlight• Lock• McAfee Encrypted USB drive |