



DC3 Permission to Participate

for the 2010 DC3 Digital Forensics Challenge



<http://www.dc3.mil/challenge>

This letter indicates that my child,

First Name: _____

Last Name: _____

Team Name: _____

School Name: _____

has my permission as Parent/Guardian to participate in the DC3 Digital Forensics Challenge (known as "DC3 Challenge") if their application is approved by the DC3 Challenge team.

I acknowledge that I have read and accepted the following as applicable to my child:

- DC3 Challenge's Rules:
http://www.dc3.mil/challenge/2010/files/2010_DC3_Digital_Forensics_Challenge_Rules.pdf
- DC3 Challenge's Privacy & Security Policy:
<http://www.dc3.mil/challenge/2010/privacy.php>

I understand that while DC3 Challenge does not release personally identifiable information collected during the Challenge, their name and school will be associated with their team name when released by DC3 and/or its sponsors to the public upon winning a contest prize. A listing of DC3's partners and sponsors can be found on our website.

Failure to provide accurate personal information and/or not returning this signed form will deny your child's participation in the DC3 Challenge.

Parent's/Guardian's printed name: _____

Relationship to minor: _____

Parent's/Guardian's phone number: _____

Parent's/Guardian's email address: _____

Parent's/Guardian's signature: _____

Send this signed form to us via any of the following methods:

- Fax to (410)-981-1092
- Scanned PDF via email to us at challenge@dc3.mil

About the DC3 Digital Forensics Challenge:

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 challenges ranging from basic forensics to advanced tool development are being provided to all participants. The challenges are single based challenges and are designed to be unique and separate from one another. This format is different than the whole forensic process scenario, with incorporated challenges, provided for the 2009 DC3 Challenge.

About DC3 (Department of Defense Cyber Crime Center):

The Department of Defense Cyber Crime Center (DC3) sets standards for digital evidence processing, analysis, and diagnostics for any 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 forensics 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.