A NATIONAL CYBER CENTER

DC3

Defense Cyber Crime Center
Air Force Office of Special Investigations

DC3 DIGITAL CRIME SCENE CHALLENGE

ADMINISTRATIVE PACKET

Table of Contents

Welcome

Thank you for your interest in the Defense Cyber Crime Center (DC3) Digital Crime Scene Challenge! This package contains all materials needed to run your own instance of this Challenge at your own event or as a training tool:

- Four scenarios that include a full set of interrogation questions
- The source code for the web application, along with tutorials on how to use it
- The basic rules for the Challenge participants along with our recommended presentation
- A recommended inventory list of all the items hidden at the crime scene
- An evidence map of the placement of all digital and non-digital items for event execution
- Backup grading forms should you prefer paper grading and not use the web application

We hope that this Challenge serves the greater community in continuing its purpose: educate participants on the issues Investigators currently face in the field with potential sources of digital evidence, while keeping their attention through a fun and interactive competition.

Sincerely,

Defense Cyber Crime Center (DC3)
Website: http://www.dc3.mil
Email: info@dc3.mil

Legal

License

The DC3 Digital Crime Scene Challenge (hereafter “Software”) constitutes as a work of the United States Government and is not subject to domestic copyright protection under 17 USC § 105.

This Software utilizes code licensed under the terms of the GNU General Public License (GPL) and therefore is licensed under GPL v2 or later:

- Date Format 1.2.3 by Scott Trenda and Kris Kowal (MIT License)
- Countdown for jQuery v1.5.9 by Keith Wood (GPL v2 or MIT Licenses)
- jQuery JavaScript Library v1.5.1 by The Dojo Foundation (GPL v2 or MIT or BSD Licenses)
- jQuery UI 1.8.13 by the jQuery Project (GPL v2 or MIT Licenses)
- jQuery Mobile v1.0b3 by the jQuery Project (GPL v2 or MIT Licenses)
- jQuery UI Widget by the jQuery Project (GPL v2 or MIT Licenses)
- jquery.dataTables v1.7.5 by Allan Jardine (GPL v2 or BSD 3 point style)

This Software is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License (GPL) as published by the Free Software Foundation, either version 2 of the License, or (at your option) any later version.

This Software is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this Software. If not, see <http://www.gnu.org/licenses/>.

Disclaimer of Use

An individual or organization (hereafter "User") that downloads or uses the DC3 Digital Crime Scene Challenge (hereafter “Software”) agrees to indemnify and hold harmless DC3, the U.S. Air Force, and the Department of Defense and their respective directors, officers, employees, agents, and assigns, as applicable, against any and all claims, damages, losses and expenses (including reasonable attorneys' fees), as incurred, arising from or in connection with or otherwise with respect to any claim, demand or legal action by a client, potential client, employee, consultant, independent contractor or agent of the User, the User themselves, any of the User's affiliates, or by a third party, related directly or indirectly to the User's use of or inability or failure to use the Software for any purpose.

In no event shall DC3 be liable for any damages, direct or indirect (including, without limitation, consequential, special, incidental or punitive damages, lost profits, business interruption, or lost information), arising out of the User's use of or inability (or failure) to use the Software, and whether in an action based on contract, warranty, strict liability, tort (including, without limitation, negligence) or otherwise.

Disclaimer of Endorsement

Reference to, or identification of, any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, for the DC3 Digital Crime Scene Challenge does not constitute or imply its endorsement, recommendation, or favoring by the United States Government. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government, and shall not be used for advertising or product endorsement purposes. Neither the United States Government nor any of its employees, makes any warranty, expressed or implied, including merchantability, fitness for a particular purpose, or assumes any liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights.

Competition Overview

The object of the Digital Crime Scene Challenge is for participants to use their forensic and investigative skills to focus on potential digital evidence and conduct triage/analysis of such evidence. Teams of 1-5 participants are given a scenario and an interrogation script of a suspect. The scenario and script outline that there is vital information to be found – without it, the suspect must be let go! It is the team's job to review the case information and analyze the scene quickly.

Participants need to find all the evidence items and the key device with the vital information stored on it in less than 15 minutes. Points are awarded for:

- Each evidence item found and secured
- Identifying the key device
- Finding the vital information on the device

If there is a tie with points, the team with the fastest time will win. The goal of this challenge is to educate participants on the issues Investigators currently face, while keeping their attention through a fun and interactive competition.

Competition Overview

- The participant(s) will be given a scenario in which a cybercrime has been committed. They are allowed to read the scenario as many times as they wish and may take the scenario into the scene with them, if they so choose.

- Along with the scenarios will be an interrogation script from a previous interrogation of the suspect.

- Once the scenario and interrogation script have been reviewed, the participant will be given gloves to put on and then lead into the crime scene.

- It will be the participant's job to identify and secure all digital devices and analyze one device for evidence within a 15 minute time frame.

- To secure a digital device, place it on the table side marked "DIGITAL DEVICES" and describe the item to the Score Keeper for recording.

- Other items, considered non-digital, should be placed on the table side marked "NON-DIGITAL DEVICE."

- The one device the participants analyze must be correctly attached to the forensic laptop and be approved by the Score Keeper.

- Choose the correct evidence device on the first try to gain more points.

- If an incorrect device is chosen, the Score Keeper will state "Improper device" and the participant will have to search for another. Points will be deducted for this.

- When the evidence is found on the device, show it to the 'Evidence Custodian' and tell them the search is complete to stop the timer.

- Participants can choose to continue to look for other devices after the evidence is found, if they so choose. However, they must inform the Score Keeper.

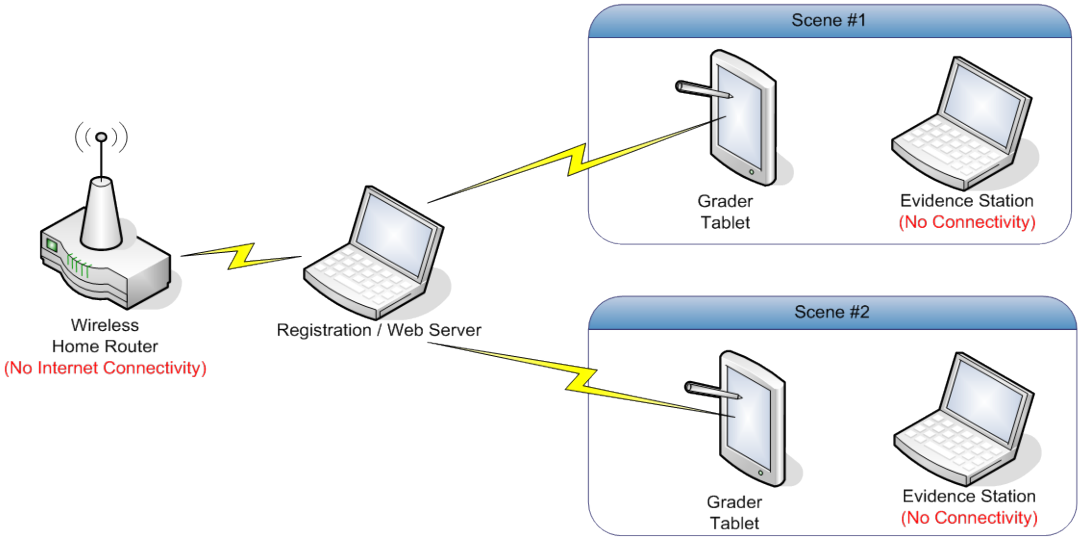
- Once time is up, the score is submitted and participants must leave the area without touching anything.

NOTE:
Some devices are worth more than others. The team with the most points wins. If there is a tie with points, time will be used as the tie-breaker.

Network and Computer Configurations

Network Diagram

This is an example setup executed for past events by the DC3 team:



Necessary Equipment

Router/Switch to provide a private local area network:

- DHCP preferred – can use static IPs per device
- Wireless (optional) with security abilities (WPA2, lock down to MAC addresses)
- No Internet Connectivity

A computer with ability to run as a web server and registration:

- Network connectivity to the Router to communicate to Grader Tablets (wired preferred)
- Ability to run a Web Server with PHP5 and MySQL 5.1
- Modern Desktop Web Browser that supports JQuery Mobile 1.0b

A tablet or computer for grading scene:

- Network connectivity to the Router (wireless preferred)
- Modern Mobile Web Browser that supports JQuery Mobile 1.0b

A computer for scene evidence station:

- Base installation of an Operating System using a guest profile (preferred)
- No Network Connectivity

Web Application Setup

The following instructions detail the full process required to get the Digital Crime Scene Challenge grading application installed and running properly. If you already have a web server and database engine running on your machine, you can skip most of the initial steps.

Items needed:

- Copy of the Digital Crime Scene Challenge code (provided in this packet)
- Administrative access to a local machine
- Web Server software with the following modules to install on the local machine:
    - Apache 2.x
    - PHP 5.3 or above
    - MySQL 5.1 or above
    - phpMyAdmin

NOTE: These instructions assume you are using XAMPP, an Open Source pre-built web server package from ApacheFriends.org This particular distribution includes the above modules pre-configured for Windows, Mac, and Linux. If you are using a different web server setup, please skip XAMPP's setup and check for configuration settings noted.

Step 1 - Setting Up Your Web Server

1. Install XAMPP on your registration machine.
2. Note the location of its installation folder on your harddrive – this will be referred to **<XAMPP folder>** for these steps.
3. Make the following configuration changes to the web server as administrator:
    a. Increase the default memory limit for PHP to execute:
        i. Locate the php.ini file under the **<XAMPP folder>/etc** folder.
        ii. Edit the **memory_limit** parameter in the php.ini file to **64M**
        Note: If you cannot find the parameter, add it to the end of the file. Not

editing this parameter may cause the application to not fully load interfaces and prevent saves from interfaces.

b. Increase the default memory limit for MySQL to execute:
    i. Locate the **my.cnf** file under the ***<XAMPP folder>/etc*** folder.
    ii. Edit the **thread_stack** parameter in **my.cnf** file to **4M** and save.
    Note: If you cannot find the parameter, add it to the end of the file. Not editing this parameter will cause the application to lock up during MySQL updates and inserts.

4. Now that you've finished the basic configuration of your web server, you are ready to start it up for the first time.
    a. In the ***<XAMPP folder>***, launch the **XAMPP Control** application.
    b. On the dialog box that appears, you want to click the **Start** buttons next to **Apache** and **MySQL**. This will launch your web server and database engine, respectively.
    c. When you click the first button, you will be prompted for an administrator password.
5. Once the two services are enabled, you can test your web server by opening a web browser and entering **localhost** in the address bar. If a screen with the XAMPP logo comes up, your server has been installed successfully.

Step 2 - Unpack and Configure Web Code

6. Unpack the file named "Cyber Crime Scene.zip" from the distribution. This file contains the complete web code used for running the grading application. You should now have a folder named **cyber_crime_scene**.
7. Copy the **cyber_crime_scene** folder into your web server's web root as local administrator at ***<XAMPP folder>/htdocs***
8. Edit the web application’s configuration files.
    a. Update the **$basePath** variable in the **global.php** located the **inc** folder if you have not placed it directly in the **<XAMPP folder>htdocs/cyber_crime_scene**

  b. Update the database connection information in the **db.php** located in the **inc/fx_lib** folder if you are not using XAMPP's default database settings.

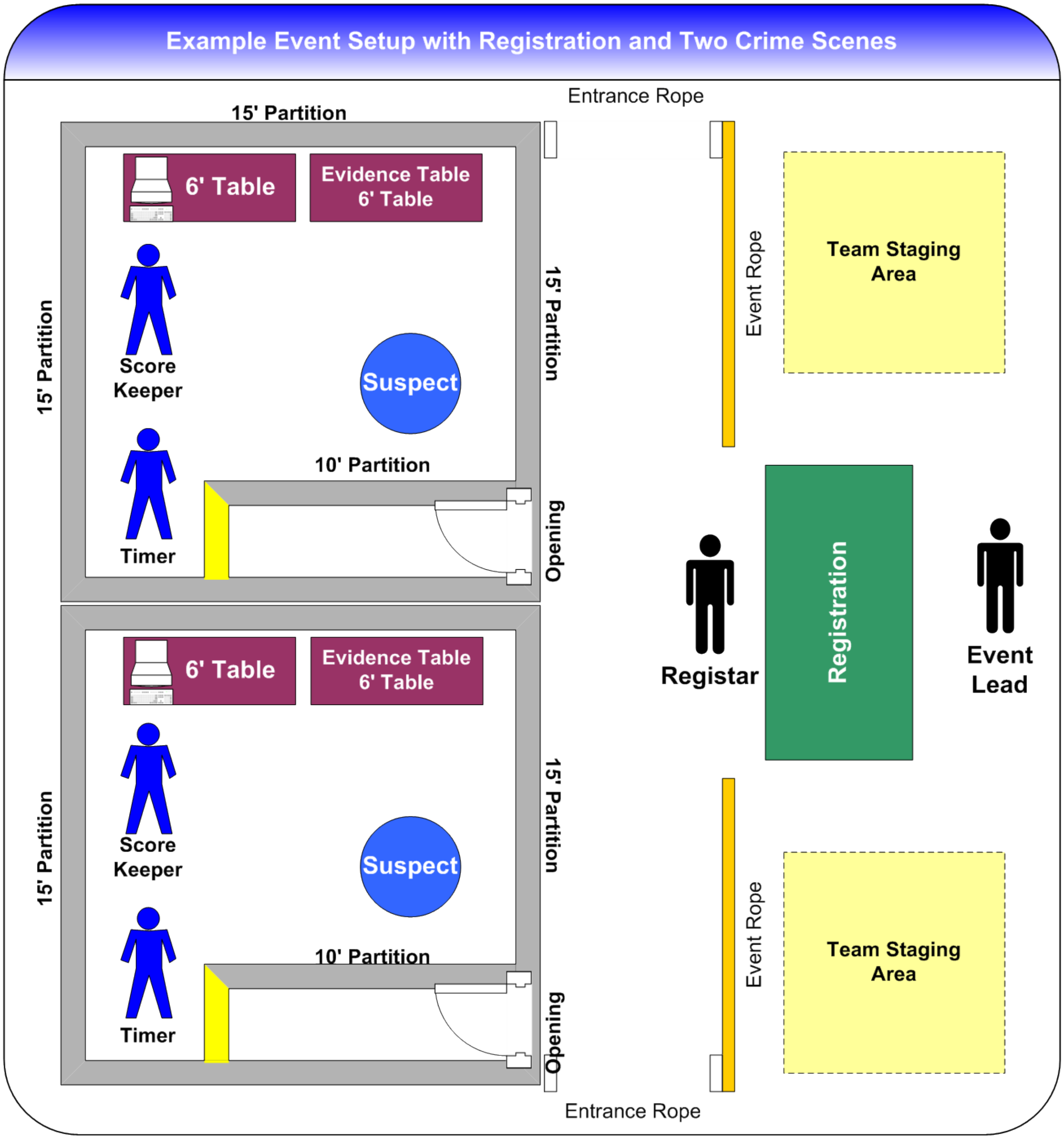
9. At this point, the web code should be configured properly. We'll now move on to the final step: the database side.

Step 3 - Set Up and Populate Database

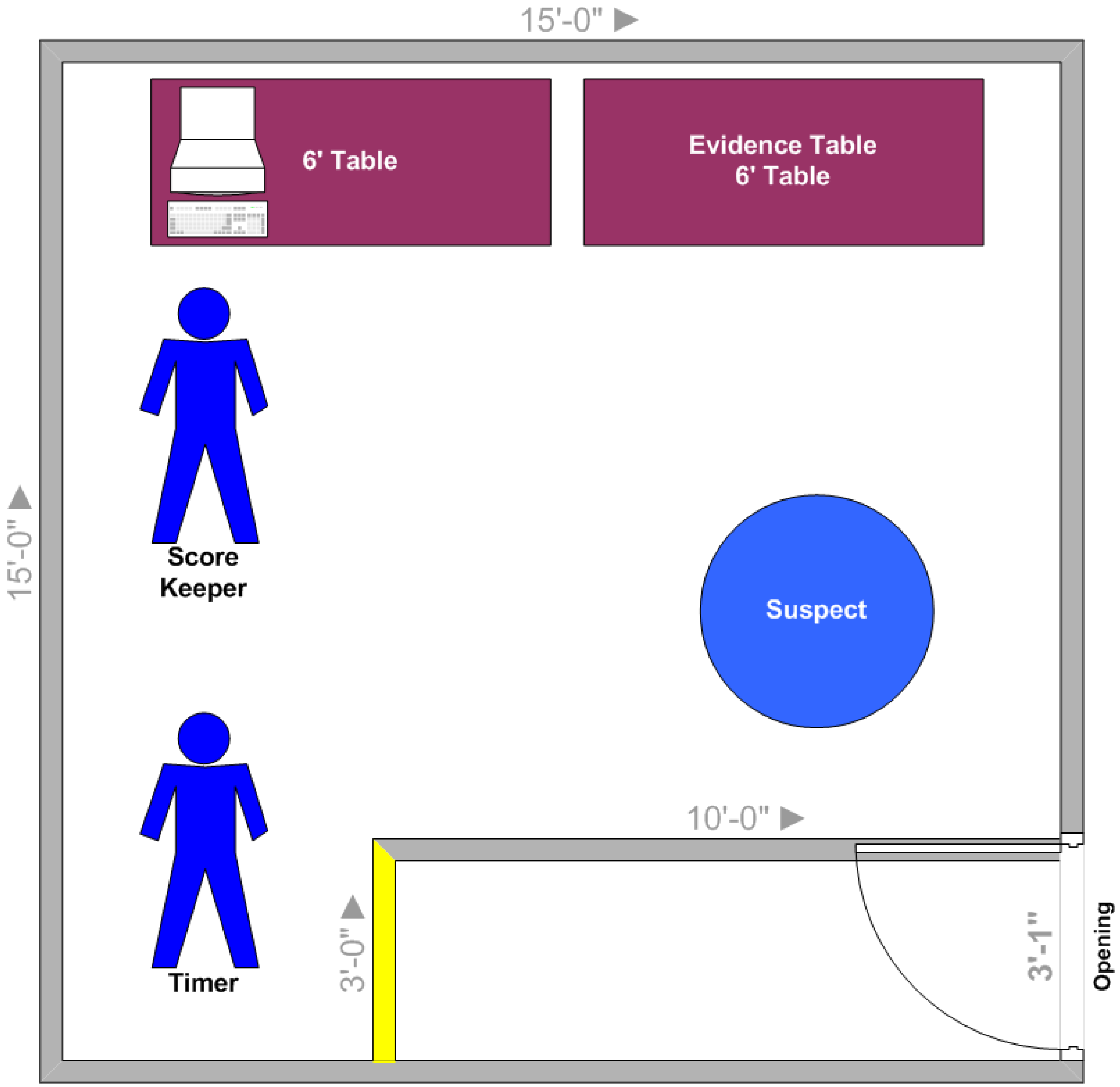
10. In the **cyber_crime_center** folder, open the **sql** folder. This folder contains all of the code necessary to construct and populate the database. You can close this folder - just make sure you remember where it is, as you'll need the contents soon.
11. Open your web browser, and enter "localhost/phpmyadmin" into the address bar. This will take you to the homepage of the phpMyAdmin database management tool, which you can use to set up, maintain, and modify your database.
12. Import the default Crime Scene Challenge database in phpMyAdmin
    a. By default, the web code is looking for a database with the name "crime_scene_challenge" (which can be changed in the db.php file you viewed earlier).
    b. Near the top of your browser window, you should see a series of tabs. Click the 'Import' tab, and click the 'Browse' button on the subsequent page.
    c. Navigate to the location of the sql/ folder you viewed earlier, select the 'cyber_crime_scene.sql' file, and click 'Go' in the phpMyAdmin window.
    d. A small green box should appear near the top of your screen letting you know that the database has been created and the import is successful.
13. Enter the following into your address bar to verify you correctly loaded the database: **http://localhost/cyber_crime_scene**
    a. If the home screen of the grading application comes up, congratulations! You've successfully installed the Digital Crime Scene Challenge grading application.
    b. If not, double check that you had no errors when you imported. You may have to delete the database and start over.

Scene Setup and Layout Information

Floor Plan – Event Setup Example



Floor Plan – Crime Scene Example



Inventory List

Digital Devices

Disclaimer:

The following is the previous list of items used by DC3 for execution of this event – your mileage may vary on which digital are available to use for your event. If you choose to use different devices, you will need to update via the web application and the paper grading sheet.

	Qty	Name	Description	Type
[ ]	3	Hard Drive	500GB	Digital Device
[ ]	7	Wristband	Blue 256 MB	Digital Device
[ ]	3	Memory watch	Mega Memory Watch 2GB	Digital Device
[ ]	3	USB on lanyard	2GB	Digital Device
[ ]	3	USB Keychain	2GB	Digital Device
[ ]	3	CD in green case	CD in green case	Digital Device
[ ]	3	DVD in blue case	DVD in blue case	Digital Device
[ ]	3	Mini CD in clear case	Mini CD in clear case	Digital Device
[ ]	3	Game Console	16GB	Digital Device
[ ]	3	Smartphone/PDA		Digital Device
[ ]	3	USB pen	Example: Disk Go 4GB silver	Digital Device
[ ]	3	Spy coin	Hollow half dollar	Digital Device
[ ]	3	Floppy disk	3.5" black	Digital Device

	Qty	Name	Description	Type
[ ]	3	Camcorder	Digital	Digital Device
[ ]	3	Video Recording Sunglasses		Digital Device
[ ]	3	MP3 player		Digital Device
[ ]	4	SD card	4GB	Digital Device
[ ]	7	Micro SD card	2GB	Digital Device
[ ]	4	Pico USB	16GB	Digital Device
[ ]	3	CF card	2 128MB, 1 64MB	Digital Device

Scene Setup

	Qty	Name	Description	Type
[ ]	3	Mannequin		Scene Hardware
[ ]	3	Mannequin stand		Scene Hardware
[ ]	3	Camping shirt		Scene Hardware
[ ]	3	Investigator vest		Scene Hardware
[ ]	3	Cargo pants		Scene Hardware
[ ]	3	Cord belts		Scene Hardware
[ ]	3	Lanyard		Scene Hardware
[ ]	3	Baseball cap		Scene Hardware

	Qty	Name	Description	Type
[ ]	3	Stop watch		Scene Hardware
[ ]	3	Forensic laptop		Scene Hardware
[ ]	3	PC power adapter		Scene Hardware
[ ]	3	USB extension		Scene Hardware
[ ]	3	Portable gaming device power cord		Scene Hardware
[ ]	3	Firewire to USB cord		Scene Hardware
[ ]	3	Card reader	Forensic Card Reader	Scene Hardware
[ ]	8	Micro SD HC adapters		Scene Hardware
[ ]	2	VGA cable		Registration
[ ]	1	Laptop		Registration
[ ]	3	Mouse - USB		Scene Hardware
[ ]	1	Mouse - USB		Registration
[ ]	1	USB keyboard		Registration
[ ]	3	Tablet PCs		Scene Hardware
[ ]	3	Storage Case		Registration
[ ]	2	Pelican Case		Registration
[ ]	4	Laptop case		Registration
[ ]	3	Power extension cords	50"	Registration

	Qty	Name	Description	Type
[ ]	2	Roll of duct tape		Registration
[ ]	2	Roll of Crime Scene tape		Registration
[ ]	8	Boxes of gloves (non-latex)	2S, 2M, 2L, 2XL	Registration
[ ]	4	Raid jackets		Registration
[ ]	1	Folder for documents		Registration
[ ]		Table cloth	Possibly	Registration
[ ]	3	Master locks with keys		Registration
[ ]	3	PC cord locks		Registration
[ ]	1	Wireless Home Router		Registration
[ ]	1	Power Adapter for router		Registration
[ ]	1	Ethernet Cable		Registration
[ ]	3	Tablet PC Power Adapter		Registration
[ ]	8	Scenario	Laminated	Documentation
[ ]	8	Foam board Signs		Documentation
[ ]	150	Slick Sheets		Documentation
[ ]	2	Digital/Non-digital Evidence Signs	Laminated	Documentation
[ ]	3	Evidence Custodian Scripts	Laminated	Documentation
[ ]	4	Evidence Maps	Laminated	Documentation

Team Documentation

Team Guide

1) Before Competing

   a) This guide contains a scenario in which a cybercrime has been committed. Along with the scenario will be an interrogation script from a previous interrogation of the suspect. Participants are asked to read the scenario and interrogation scripts, analyze the situation, and develop leads. Teams are allowed to read these as many times as they wish and take them into the scene with them, if they so choose.

   b) Teams are required to read the rules of the challenge before they enter the scene. If the teams have any questions before they enter the scene, they may ask an event staff member at the 'Registration' desk. Once teams enter to compete, they are assumed to have read the rules and fully understand proper and improper behavior as well as possible consequences.

   c) We advise that teams with more than 2 members divide up into 'roles'. Members can take on more than 1 role. Both members on 2-member teams will assume all roles. Teams with 3 and 4 members do not need to have a 'Lead Investigator'. Typical personnel involved in Cyber Investigations include, but are not limited to:

      i) <u>Digital Forensic Examiner:</u> an individual who is responsible for imaging, analyzing, and reporting on digital evidence provided by an investigator. (During this competition, the Digital Forensic Examiner will not be imaging or reporting, only analyzing evidence on-site. This practice is called "Triaging" evidence.)

      ii) <u>Evidence Custodian:</u> When the evidence custodian is called on-site, they are typically in charge of telling the investigators how to seize certain items, where the items need to go, and records the items on a 'Chain of Custody'. (During this competition, the Evidence Custodian would stand next to the table marked for digital and non-digital items and determine which items should be placed on which side.)

      iii) <u>Lead Investigator:</u> an individual who is responsible for a case. This person would delegate responsibilities to other agents and determine which items are pertinent to the case and should be seized. (During this competition, the Lead Investigator would not search the scene, but manage team members. Team captains would fit this position, but are not required to do so.)

      iv) <u>Responding Agent(s):</u> The first person on scene who is responsible for securing the area, ensuring evidence is not tampered with or destroyed, and collecting the evidence. (During this competition, the Responding Agent(s) will be actively searching and seizing items from the scene. They will also be handing over evidence to the Evidence Custodian. We recommend only 2 team members for this scenario)

2) During the Competition

a) Once the team arrives to compete, members will be given latex gloves to put on and then lead into the crime scene as a team. (If anyone is allergic to latex, please let us know for an alternative solution).

b) When all team members are inside the scene, it will be their responsibility to identify and secure all evidence items and analyze only 1 seized device for digital evidence within a 15 minute time frame.

c) In the crime scene, there will be two tables. One table will have a black, Dell laptop. The other table will be divided into two sections – one section marked "DIGITAL DEVICES", and the other marked "NON-DIGITAL DEVICES". These tables are NOT part of the crime scene and do not need to be searched. They are part of the investigative work area where you will store, secure, and analyze evidence.

d) To secure a digital device, place it on the table side marked "DIGITAL DEVICES" and describe the item to the score keeper for points.

e) Other items, considered non-digital, should be placed on the table side marked "NON-DIGITAL DEVICE" and describe the item to the score keeper for points.

f) The 1 digital device that the participants choose to analyze must be correctly attached to the forensic laptop after being approved by the score keeper.

g) Choose the correct evidence device on the first try to gain fifteen points.

h) If an incorrect device is chosen, the event staff member will state "Improper device" and the participant will have to search for another. Five Points will be deducted each time this occurs.

i) Once the team is approved by an event staff member for analyzing the digital device on the 'forensic laptop', they may attach it and retrieve the vital information from the device.

j) When the correct evidence from the digital device is found, show it to the event staff member and tell them the search is complete to stop the time and submit the score.

k) Once time is up, the score is submitted and participants must leave the area without touching anything.

NOTE: Some evidence items are harder to find and are worth more than others. The winners of this challenge are the team with the most points, so be sure to try and find all the evidence items before searching for the digital evidence. Should there be a tie with points; time will be used as the tie-breaker.

Crime Scene Challenge Rules

1) **Do not** remove any items from the scene. Inventory is taken after each participant completes the investigation.

2) **Do not** behave or act inappropriately with the suspect – show respect for them.

3) **Do not** remove clothing or other items from the suspect unless required to locate and collect evidence. As a general rule, the only items to be removed are those that would be required to come off at an Airport Security Check-Point.

4) **Do not** plug in a device to the forensic machine that the event staff has not approved.

5) **Do not** touch event staff members or photographers in an inappropriate manner.

6) **Do not** break any items in the crime scene.

7) **Do not** bring cell phones or other recording devices into the scene.

8) **Do not** discuss any details of the crime scene with friends – it is a competition.

9) **Do not** enter the scene without an event staff member or other crime scene administrator.

10) **Do not** take down signs or logos without prior consent from a crime scene administrator.

11) **Do not** use the equipment in any way for malicious purposes.

12) **Do not** cheat.

13) **Do have FUN!**

Scenarios

Scenario – Military

- You are a Special Agent in the U.S. Air Force on duty.

- The Base Commander received intelligence that an unidentified US Military member is aiding a terrorist group by smuggling weapons across the Iranian border.

- While performing routine checks at a security checkpoint, you discover an unusual amount of military weapons in the possession of Airman First Class (A1C) Donovan.

- You notify the Officer in Charge of the situation. After speaking with the Base Commander, He orders you to seize the suspect, advise him of his Article 31 rights[1], and conduct an interrogation.

- During the interrogation, you and your partner are notified that the terrorist group is now targeting the base.

- The suspect admits to being involved with the suspected group and that the attack should take place in an hour.
- The suspect has stopped talking and the details of the attack are unknown. It is now up to you to find the evidence.

[1] Example of advisement of Article 31 rights for military suspects:
I am __________, _________, _________ (military installation). I am investigating the alleged offense(s) of ___________, of which you are suspected. Before proceeding with this investigation, I want to advise you of your rights under Article 31 of the Uniform Code of Military Justice. You have the right to remain silent, that is, to say nothing at all. Any statement you do make, either oral or written, may be used against you in a trial by court-martial or in other judicial, nonjudicial or administrative proceedings. You have the right to consult with a lawyer prior to any questioning and to have a lawyer present during this interview. You have the right to military counsel free of charge. In addition to military counsel, you are entitled to civilian counsel of your own choosing at your own expense. You may request a lawyer at any time during this interview. Have you previously requested counsel after advisement of rights? ***(If the answer is yes, stop. Consult your JAG Office before proceeding)***. If you decide to answer questions during this interview, you may stop the questioning at any time. Do you understand your rights? Do you want a lawyer? ***(If the answer is yes, cease all questioning)***. Have you already consulted an attorney about this matter? ***(If the answer is yes, stop questioning)***. Are you willing to answer questions? Do you understand that you are free to end this interview at any time?

Interrogation - Military

Q- Airman Donovan, we have reason to believe that you are aiding and abetting a known terrorist group by smuggling weapons for them. Is this true?

A- No

Q- Then why were you carrying extra weapons?

A- A friend of mine hurt his back hauling gear, so I told him I would take his.

Q- There were five rifles and the grenades you were carrying were not secure or marked on your inventory sheet. Why didn't you mark them on the sheet?

A- I forgot! This is ridiculous, I'm leaving.

Q- SIT DOWN Airman Donovan! I have orders from Col. Jacobson to question you. Do you know anything about a terrorist group targeting this base?

A- Well…uh…..what time is it?

Q- A quarter after 3. Why are you in such a hurry?

A- I just don't like being here. I want to leave.

Q- I understand, but there are questions we need answers to. The more you cooperate, the sooner we will finish.

A- Okay, I want to get this over. I've been selling weapons to some guy. I don't know his name. He had a lot of money. I think he's part of a group that's planning an attack on the base today. I overhear him talking with people at his store. I really just want to go because I know what they have and what they're capable of. We all really need to get out of here, just in case. Please, let's just go.

Q- We're not leaving. Can you give me any names of people you've had contact with regarding the weapons?

A- Hmm…. Chad. He's the one I'd meet up with most of the time, but I couldn't tell you his real name.

Q- Was he the only person you met with? Were there any others, you said he was part of a group?

A- No. He was the only one I saw. But I would overhear him talking to other people when we would meet.

Q- At what location would you meet? Was it always the same place or were there various places?

A- Just one place. A little alley down by the main market. Chad had a shop there where he sold random things like cell phones, radios, video games, laptops, and other things like that. That's actually how we met. I bought a lot of my electronics from him.

Q- Did you ever communicate with him via any of these things?

No, just used them like normal. He never wanted to use the phone anyway, everything was always face-to-face.

Q- You said before you would overhear 'Chad' talking with other people at his shop. What made you believe they were planning an attack on the base today?

A- I saw him last week. He told me to meet him today at 3:30 with the weapons and to not be late. He said that I would pay dearly if I were late and that he is only looking out for my safety. He turned and talked to some guy in back and I understood something about 'it will blow sky high at 4'.

Q- Was there anything else that happened the last time you met with 'Chad'? Anything you might think important? Did he give you anything or touch anything on you?

A- No. Well…..he did go and get a pen from the back of his shop. He said that for my assistance, I would be greatly rewarded and the pen is my first gift – or something like that.

Q- Do you still have this pen?

A- Yea, somewhere.

Scenario – TSA

- You are a TSA Agent at the Chicago – O'hare International Airport.
- A young man is arrested for possession with intent to distribute narcotics.
- When searching the luggage, cocaine was found. A laptop was discovered stored further down in the suitcase.
- The laptop is secured and found to be protected with full-drive encryption.
- A search warrant authorized the search for information in whatever form relating to drug trafficking and controlled substances (including digital devices that can store data).
- Prior to questioning, the suspect waived his rights to self-incrimination.
- While in questioning, the suspect confessed to working for "Mr. Yev".
- You receive confirmation that "Mr. Yev" is actually a highly wanted international criminal involved in murders and human trafficking as well.
- The agent calls you in to search for possible hidden items and analyze any digital evidence pertaining to "Mr. Yev" and the narcotics.

Interrogation - TSA

Q- What's your name?

A- Jake Jarvis

Q- Jake, Why were you carrying so much cocaine in your luggage?

A- I didn't want to do it, dude. Look, I got a little girl who's got Burkitt's lymphoma. The hospital bills are outrageous and our insurance won't cover anymore. There's this guy my buddy hooked up with, payed him $10,000 just to fly with a bag. My buddy told him of my situation and he said he'd help. He sent me a bunch of cool things just to let me know he can take care of us. I knew it might have been something, but we needed the money.

Q- I'm very sorry to hear that about your daughter. Can you tell me the guy's name?

A- Mr. Yev, that's all I know.

Q- What kind of 'cool things' did Mr. Yev give you when you first started working for him?

A- A new phone, a new laptop, a portable video game, a watch, gift cards to different places, clothes, toys for my kids, jewelry for my wife, a lot of stuff.

Q- Is the laptop in the suitcase the one Mr. Yev originally gave you?

A- No. It's Mr. Yev's. I don't know what he uses it for, but it's part of the whole package.

Q- Can you tell me, in detail, all the components of a 'whole package'?

A- Um, there's the suitcase, the cocaine, the laptop, the keys, paper with details of the delivery, a nice pen, and a hat or jacket for a disguise.

Q- How would you get the package?

A- I would get a package in the mail with the details and a key. I would follow the directions on the paper and use the key somehow to get the suitcase. Once I got it, I would call the number on the paper to talk to Mr. Yev.

Q- So, I understand the suitcase, the cocaine, the laptop, keys, documents, even the disguise, but why a pen?

A- I don't know, it just was always included and had to be delivered with everything else. I guess it was like a way for Mr. Yev to say "thank you"?

Q- Did you ever use the phone he gave you to communicate with him?

A- Na, I'm not allowed to use any type of cell phone or anything like that when we talk- so, we always talk over pay phones in the airport before and after delivery.

Q- What do you and Mr. Yev talk about over the phone?

A- Normally, it's real quick – "Hey I'm here – Okay" type of stuff. Today, though, he told me that he's going away on vacation and the money would be a little late, but that I'd get it once he got back. He's supposed to be flying out in about half an hour.

Q- Can you tell me any other details about his flight?

A- No, I'm sorry.

Q- Do you know the password to the laptop?

A. No

Q- Is there anything else we should be aware of that you have not already disclosed?

A- Just that this was the last job I needed to do before we had enough money to pay for my daughter's treatment.

Scenario Description – Business Security

- You are the Chief Security Officer for a large corporation.
- The security guard of the corporation informed you that they believe an employee is stealing company information.
- The guard noticed on video surveillance tapes that the employee entered restricted areas, to which they do not have authority to enter.
- The CEO gave permission to search the employee’s desk.
- A search was discreetly conducted at his desk last night.
- Electronic devices were found that did not belong to the company and are not permitted in the building.
- Also found were letters from a business competitor addressed directly to the suspect.
- Upon exiting the building today, the employee was detained and questioned by the security guard.
- After the questioning, you were called in to search for hidden devices and analyze any digital evidence.

Interrogation Questions and Answers – Business Security

Q- Mr. Jermer, have you been entering a restricted area of this facility?

A- No

Q- Sir, we have you on tape. Let me ask you again, have you been entering the Research and Development area, to which you do not have permission to enter?

A- ….yes

Q- Why have you been visiting that area?

A- To talk to colleagues.

Q- The area is clearly marked as restricted and each employee is briefed when they are first hired here that the area is off limits to all but the R&D team. Why couldn't you wait to talk to your colleagues?

A- Because I needed some information, and they told me they would let me in.

Q- How did you get in?

A- Maggie O'Connor gave me her access card

Q- Why would Ms. O'Connor give you her own access card? Wouldn't she need it for work?

A- She was on vacation. She gave it to me so I could use it while she was gone.

Q- So you lied before when you said that you went in to talk to colleagues?

A- No! I needed to get some information from her and she said she'd let me in. She gave me her card.

Q- That sounds like lying to me. You got information from her, but there was no talking involved. Before, you said you entered to talk to colleagues. That's the second time you've lied to me.

A- Whatever

Q- Was anyone else aware that Ms. O'Connor gave you her access card?

A- No.

Q- What information were you looking for?

A- Our kids are on the same soccer team. My wife wanted to invite the other parents and their kids to a get together at my house. She had the team roster saved to her computer. She gave me her card, I went in, got the roster and left.

Q- Why would she have a kid's soccer roster on her work computer in a restricted area?

And why couldn’t you get it from someone else?

A- She’s the coach of the team. She probably just e-mailed it to herself and then saved it to her desktop.

Q- So then Ms. O’Connor had the roster at her house to be able to send it to herself at work. Why couldn’t you just get the one she had at home?

A- I don’t know, like I said before, she PROBABLY e-mailed it to herself. I don’t know how SHE put it on there. I just know that was where she told me to look after I asked for it.

Q- The company does not allow storage devices/media in the building that doesn’t belong to them. Why did you have personal electronic devices at your desk?

A- Everybody sneaks in their phones, iPods, CDs, and things like that. The work here is so monotonous that we all need something to entertain us otherwise we’d go crazy.

Q- The video surveillance shows you entering R&D twice. Why twice?

A- I left my pen. I had to go back and get it.

Q- What is so special about your pen?

A- It’s my favorite. I always keep it with me. Plus, I didn’t want anyone else to take it.

Scenario Description – Law Enforcement

- You are a Deputy Detective at a local Law Enforcement Agency trained in digital forensics.

- Based on previous interviews and evidence, the detective finds probable cause that Mr. Smith is a co-conspirator to a homicide.

- The detective is granted an arrest warrant for Mr. Smith from the magistrate and brings Smith into custody.

- The detective is also granted a search warrant for digital devices and documentation since there is reason to believe that the suspect and his accomplice communicated via digital devices.

- The agent questions the suspect and finds that the primary suspect is leaving the country in less than an hour.

- An initial search for weapons has already been conducted; however, there may be other important or hidden items.

- He calls you in to search for possible hidden items and analyze any digital evidence.

Interrogation Questions and Answers – Law Enforcement

Q- Mr. Smith, on Tuesday, December 14th, Ms Yvonna Dvorkin was found dead outside of Tulsa. One of your trucks transported her from Atlanta. What can you tell me about Ms. Dvorkin?

A- The name sounds familiar but I don't think that I know her.

Q – We know that you monitor all the loadings; and that late at night you sneak immigrants onto the trucks, so don't bother to deny it. Unfortunately, Ms. Dvorkin's body was found along the highway. Why don't you tell us what happened?

A- I didn't kill her.

Q - The rope that was used to tie her up had chemicals which were traced back to your facility. There were also traces of two different types of hair found on the rope that didn't belong to her. One of those hairs was yours. Do you want to change your answer now?

A- Ok, but I didn't kill her, it was Jake Johnson, my driver

Q- We also know that he only did so after you convinced him to. Do you know where Jake is now?

A- He's leaving. He quit the company and decided to go.

Q- Where is Jake going?

A- Far away, somewhere outside the U.S.

Q- Do you know where specifically?

B- Nope, he wouldn't have told me.

Q- Is he flying?

A- Yep, flight leaves in less than an hour, you'll never catch him.

Q- **Can you give me any more details about the flight?**

A- Yep. But I'm not going to.

Q- When was the last time you talked to him?

A- Three days ago

Q- What did you both talk about?

A- Nothing really, He just gave me a pen and told me to write him sometime

Q- So then you have his address somewhere?

A- I didn't say that. Maybe he plans on sending it to me in the future. Maybe he just wanted to be nice. I don't know.

Q- When you talked to Jake, how did you both communicate? Over the phone, the internet, face-to-face?

A- Face-to-face

Q- I see here in my report that you not only own the company, but you also manage all the network and IT work as well. Is that true?

A- Yes.

Q- So, you are pretty technical guy. I did some research and saw that you gave a speech on how to hide devices. This makes me think you may have communicated with Jake that way. Did you?

A- I am pretty sure I don’t have to answer that question.

Q- Do you have any devices on you now you would like to declare before we conduct a search?

A- I guess you’ll just have to find out.

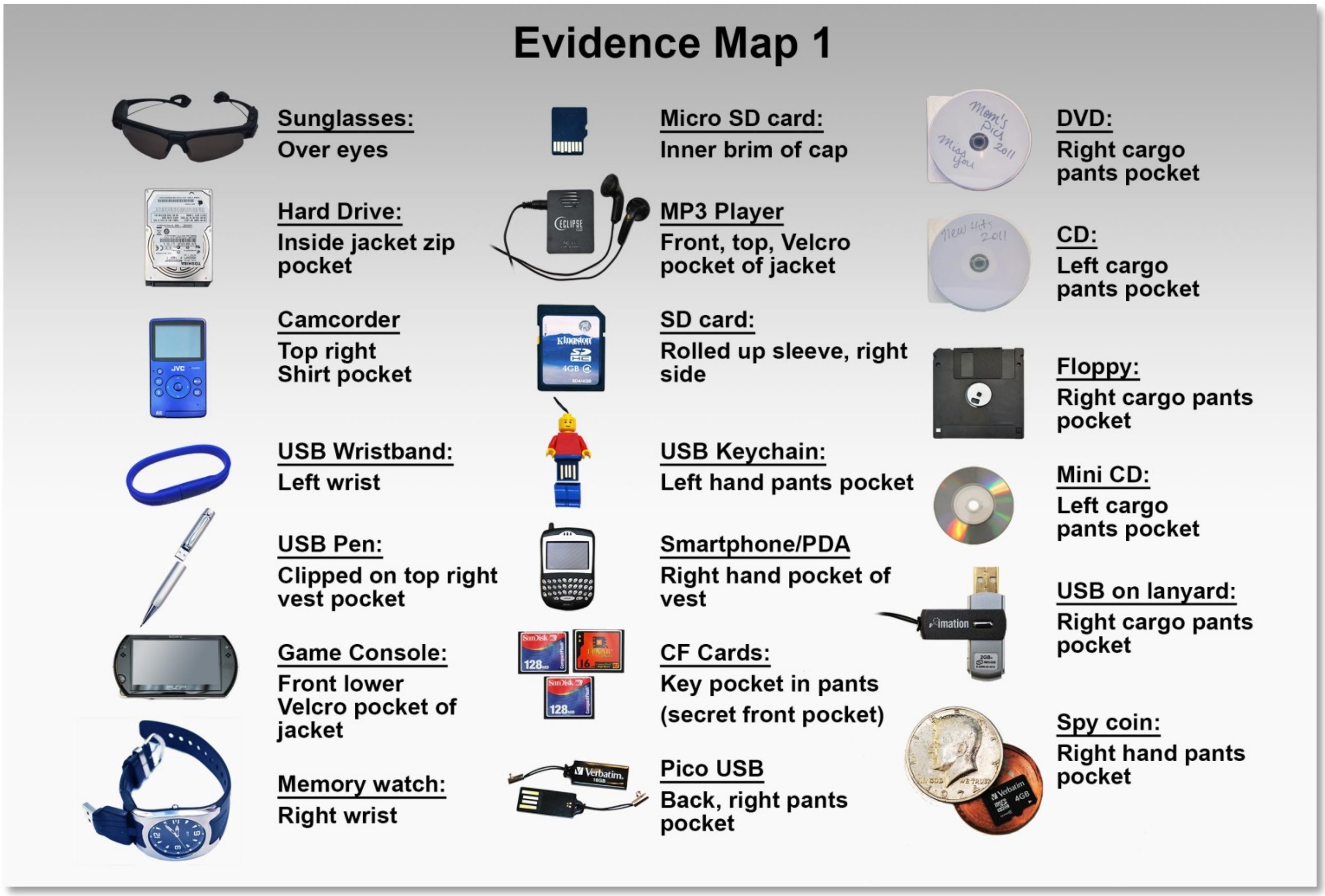
DIGITAL DEVICES

Non-Digital Devices

NON-DIGITAL DEVICES

Evidence Map

Page 1 of 2



Evidence Map 1

Sunglasses:
Over eyes

Hard Drive:
Inside jacket zip pocket

Camcorder
Top right
Shirt pocket

USB Wristband:
Left wrist

USB Pen:
Clipped on top right vest pocket

Game Console:
Front lower Velcro pocket of jacket

Memory watch:
Right wrist

Micro SD card:
Inner brim of cap

MP3 Player
Front, top, Velcro pocket of jacket

SD card:
Rolled up sleeve, right side

USB Keychain:
Left hand pants pocket

Smartphone/PDA
Right hand pocket of vest

CF Cards:
Key pocket in pants (secret front pocket)

Pico USB
Back, right pants pocket

DVD:
Right cargo pants pocket

CD:
Left cargo pants pocket

Floppy:
Right cargo pants pocket

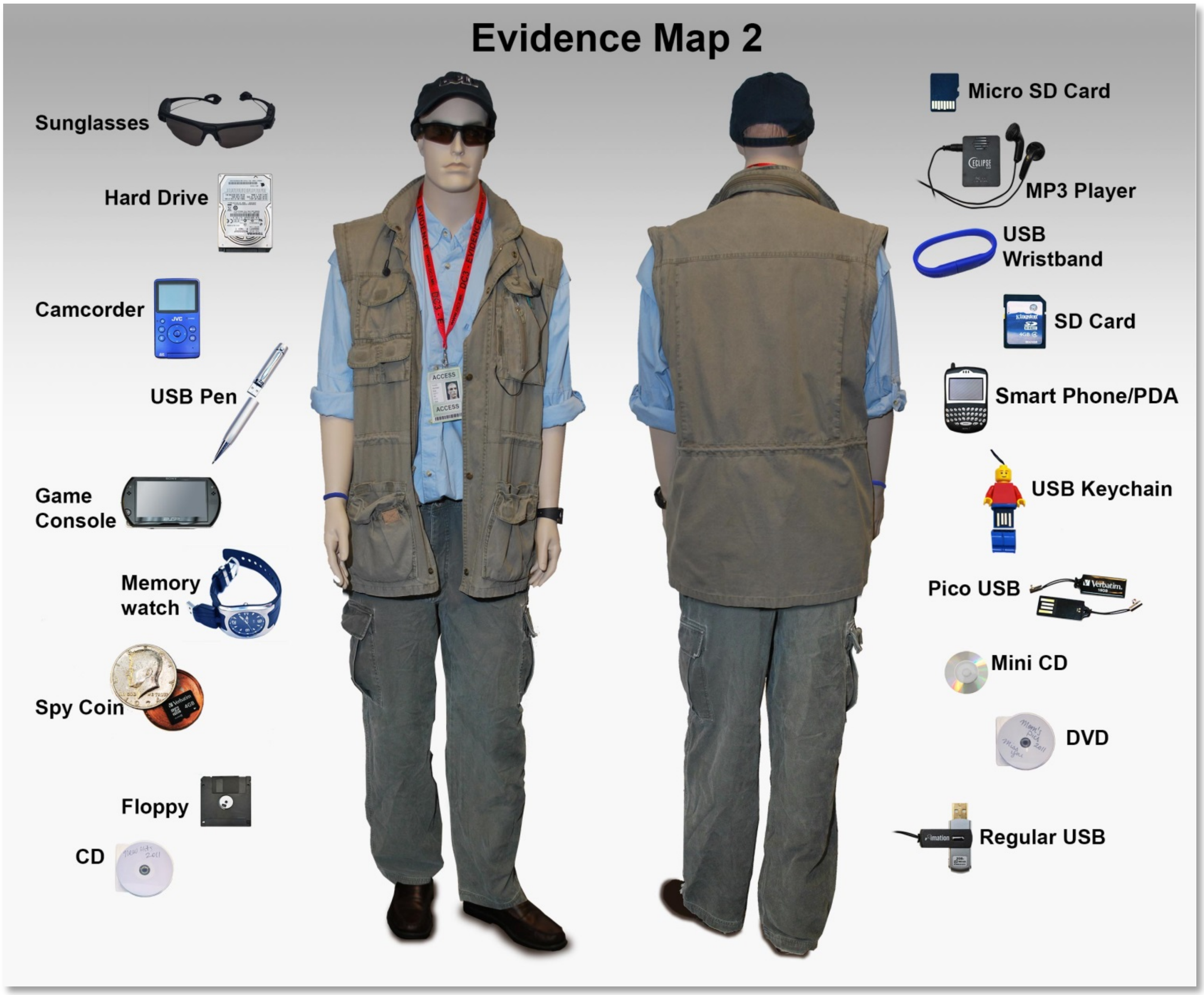
Mini CD:
Left cargo pants pocket

USB on lanyard:
Right cargo pants pocket

Spy coin:
Right hand pants pocket

Evidence Map

Page 2 of 2



Event Staff

Event Staff Requirements

At least 4 members of staff are required to run the Digital Crime Scene Challenge with 1 scene – each additional scene will add 2 additional staff members.

Staff member roles include:

- Event Management
  - Event Lead – 1 staff member to supervise the set up and execution of the event
  - Registrar – 1-2 staff members to register incoming teams and schedule scenes

- Crime Scene Management – Per Crime Scene
  - Score Keeper – 1 staff member to watch and log found evidence for points
  - Timer – 1 staff member to run a stopwatch

Please see the following pages for further details on event staff responsibilities and scripts.

Registration Responsibilities & Script

Registrars will be located at the registration table and will sign up teams, assign scene room, and obtain both team and school name. If the team would like their scores sent to them upon completion of the challenge, the registrar will also obtain the team member(s) email address(es). The registrar will read the "Registration Script" to every team that is registering for the challenge. The registrar will also confirm that teams have a "Team Package." He/she may suggest that the team read the package and complete the affidavit before starting the challenge.

"Welcome to the Digital Crime Scene Challenge! Would you (your team) like to register now and play later? Or register and play right now?"

Team is registering & will RETURN TO PLAY LATER:
"You have **15 minutes** to search the suspect, find the digital devices, and locate the digital evidence."

"Remember, **ONLY** team members are eligible to play. Team mentors are observers **ONLY**; they may **NOT** participate or help their team within the challenge at any time."

"Your team's time will start once your team crosses the crime scene tape. If you are not prepared to start at your designated time, your time will start **five minutes** after your scheduled time whether you are present or not."

"If you would like your results, please provide me with your email address now or after you have completed the challenge."

"Do you have any questions?"

"We'll see you soon!"

Team is registering & will PLAY NOW:
"You have **15 minutes** to search the suspect, find the digital devices, and locate the digital evidence."

"Remember, **ONLY** team members are eligible to play. Team mentors are observers **ONLY**; they may **NOT** participate or help their team within the challenge at any time."

"Your team's time will start once your team crosses the crime scene tape."

"If you would like your results, please provide me with your email address now or after you have completed the challenge."

"Do you have any questions?"

Score Keeper Responsibilities & Script

The Score Keeper will be stationed at the scene entrance and will be the first to greet the participant(s). Upon completion of each challenge, he/she will assist in resetting the scene by placing the evidence on the mannequin using the "Evidence Map" and ensuring the Tablet PC is reset in order to begin the next challenge. Once the mannequin and Tablet PC are reset, the Timer will notify the Registrar that a new challenge can begin.

"Hello, I am the Score Keeper for this case. May I have your team name, please?" *(Click on correct Team Name on the Tablet PC).*

"Upon crossing the crime scene tape, your **15 minutes** will commence.   Please conduct your search of the suspect; please **DO NOT** undress the suspect. There is a table that is divided with signs designating 'DIGITAL DEVICES' and 'NON-DIGITAL DEVICES.' Place all evidence in their respective areas."

"Remember, **ONLY** team members are eligible to play. Team mentors are observers **ONLY**; they may **NOT** participate or help their team within the challenge at any time."
"Do you have any questions?"

"Are you ready to begin?"

(The team must cross the crime scene tape to begin the timer)

"Thank you. Your time starts **NOW**." ***("Now"** is verbal cue to the Timer to start the time).*

Timer Responsibilities & Script

*The Timer will be stationed inside the scene. He/she will keep the time with a stopwatch, which will be in synchronization with the Score Keeper's timer on the Tablet PC. When the Score Keeper states, "*Your time starts **NOW**,*" the Timer will start the stopwatch. Upon completion of each challenge, the Timer will assist in resetting the scene.*

(While the team is completing the challenge)

"You have 15 minutes remaining."

"You have 10 minutes remaining."

"You have 5 minutes remaining."

"You have 1 minute remaining."

(You must call out each Digital Device's name that the team places in the "Digital Devices" area. **DO NOT** call out the device's name if it is incorrectly placed!)

(The team receives their score)

"Thank you playing. Please remember you are not allowed to share any answers or information regarding this challenge before the winner is announced. If you do so, you will be disqualified. Do you have any questions?"

(Escort the team out of the area and to the registration desk)

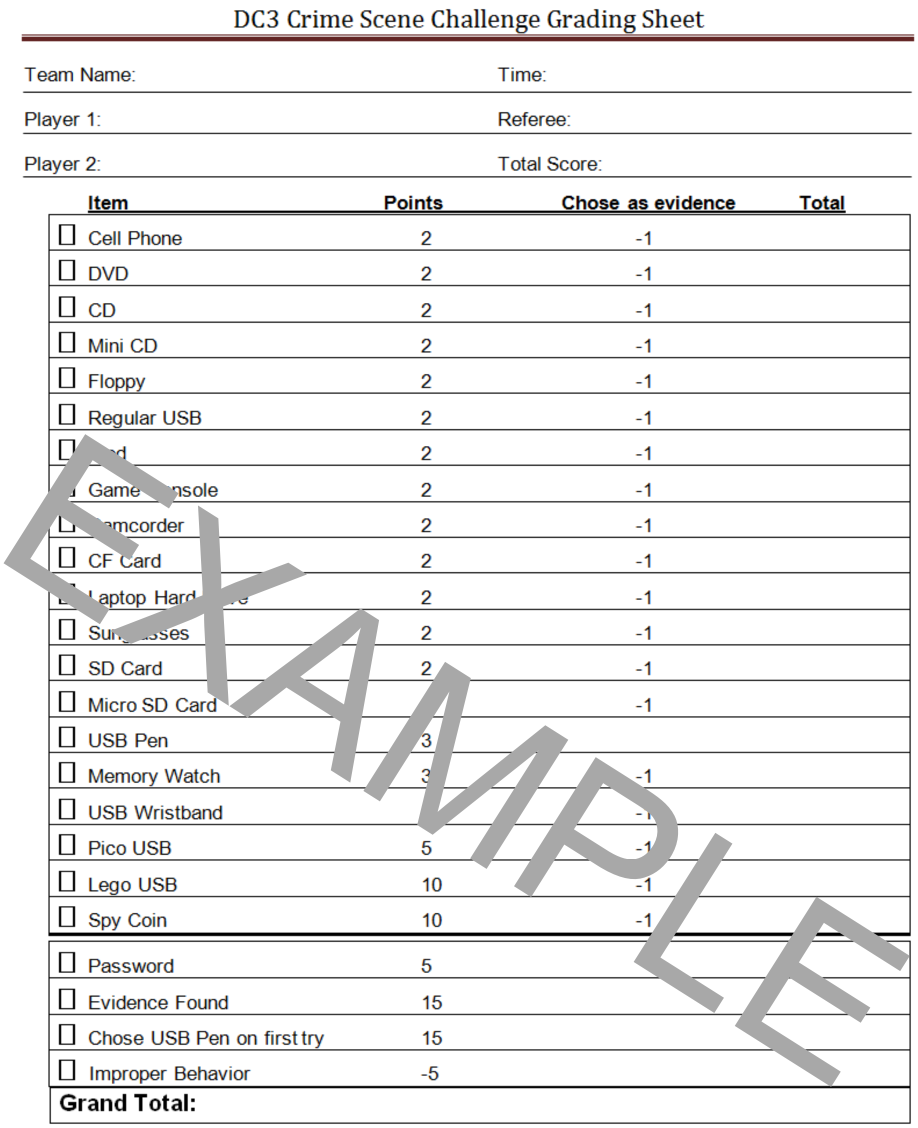
Team Email List

TEAM NAME	EMAIL ADDRESS

Documentation

Contingency Grading Documentation

Example



DC3 Crime Scene Challenge Grading Sheet

Team Name:

Time:

Player 1:

Referee:

Player 2:

Total Score:

Item	Points	Chose as evidence	Total
□ Cell Phone	2	-1	
□ DVD	2	-1	
□ CD	2	-1	
□ Mini CD	2	-1	
□ Floppy	2	-1	
□ Regular USB	2	-1	
□ Ipod	2	-1	
□ Game Console	2	-1	
□ Camcorder	2	-1	
□ CF Card	2	-1	
□ Laptop Hard Drive	2	-1	
□ Sunglasses	2	-1	
□ SD Card	2	-1	
□ Micro SD Card	[illegible]	-1	
□ USB Pen	3		
□ Memory Watch	3	-1	
□ USB Wristband	[illegible]	-1	
□ Pico USB	5	-1	
□ Lego USB	10	-1	
□ Spy Coin	10	-1	
□ Password	5		
□ Evidence Found	15		
□ Chose USB Pen on first try	15		
□ Improper Behavior	-5		
Grand Total:			

Personal Consent and Release

Example

I, ________________________________ (printed name), hereby grant the (ORGANIZATION RUNNING THE CHALLENGE) permission to use my likeness, voice, picture, name, and presentation. (ORGANIZATION RUNNING THE CHALLENGE), as sole owner of all rights in any recordings, photographs or other visual images of the event may use, reproduce, publish, modify, and distribute my likeness, voice, picture, name, and presentation, with or without personal identification, in transcript form, video, or other medium now known or hereafter developed, in whole or in part, alone or with other materials.

I hereby release and discharge (ORGANIZATION RUNNING THE CHALLENGE), its assigns, and designees from any and all claims and demands arising out of, or in connection with, the use of my likeness, voice, picture, name, or presentation, including, but not limited to, any claims for defamation, invasion of privacy, or right of publicity.
This consent and release is intended to be of perpetual duration, unless otherwise revoked in writing. I hereby attest that I have read and agree to the above statements on this ______day of ________ (month), 20____.

______________________________________ ______________________________________
(signature) (email address)

If the contestant is a minor under the age of 18, my signature, as Parent/Guardian, indicates that my child,

Full Name: ____

Team Name: ____

has my permission to participate in the Digital Crime Scene Challenge. Moreover, I agree to the information set forth in this Consent and Release form. Specifically, if the team referenced above wins a challenge prize, the minor's name may be released to the public by (ORGANIZATION RUNNING THE CHALLENGE) and/or its sponsors.

Failure to provide accurate personal information will deny the minor's participation in the Digital Crime Scene Challenge.

Parent's/Guardian's signature: ____

Parent's/Guardian's printed name: ____

Relationship to minor: ____

Parent's/Guardian's email address: ____

Please bring this completed and signed form with you to the event or send this signed form to us