Title of Lab / Challenge: Forensic Image Extraction

Location on Web:

The Basic Facts

Who? Author's Name: Mandy Galante
Author's Organization: Red Bank Regional High School
Based on a CyFor Module from NYU Polytechnic School of Engineering

What? Short description of the Lab/Challenge
Part 1: focus is on using *AccessData FTK Imager* to create a forensic image of a drive. Part 2: use *AccessData FTK Imager* to investigate and extract the files from a forensic image.

Why? Skills that can be learned from this Lab/Challenge
Familiarize with free tool to easily create a forensically sound image of a drive and use the same tool examine all data on the drive including deleted files and hexadecimal representation of data.

Pre-Req? Skills that are needed going into this Lab/Challenge
None

Difficulty Level ? (circle one) [✓ Introductory] - Moderate - Advanced

How long? to Complete Instruction: no teaching materials included

to Complete Lab / Challenge: 60 minutes

A little more detail

How does it work?

- Type of Hands-on Lab / Challenge
  - **Step-by-Step Lab**
  - Capture the Flag
  - **Solve the Puzzle**
  - Other. Please describe: ______________________________

- Scoring mechanism:
  - **No scoring (lab only)**
  - Shortest time wins
  - Point-based system
  - **Other. Please describe: Success/Failure at finding all the evidence**

How many?

- Is the Challenge / Lab for individuals or teams? **individual or work in pairs**

- If groups, what is the ideal team size? ______ people per team

- How much is "too much" - is there a maximum scale of number of participants for the challenge, given performance or other characteristics? Yes/**No**

Maximum number ________ people

How will I learn? - Instructional Method (check one or more)

- □ Video
- □ Article / Presentation
- □ **None – the challenge explains itself**
- □ Other. Please describe:

Checklist

What you get:

- Assets provided in this Lab / Challenge. (Please list all, such as pcap files, VM images, evidence files, etc.):

PIVOT_Instructions_ForensicImageExtraction.pdf
FlashOne.001
FlashTwo.001
ForensicImageExtraction_Answers.pdf

What you need #1:

- Infrastructure Requirements needed to run the Lab / Challenge (Please list all, including required devices such as PCs, tablets, local networking configuration, Internet connectivity, bypass of firewall or proxy restrictions, etc.)

Computer, usb drive (size <or= 128 MB)

What you need #2:

- Assets needed in Advance for the Lab / Challenge (Please list all, such as virtual machines, operating system installs, application installations, etc.):

Installation of AccessData FTK Imager - http://accessdata.com/product-download