**Template for the PIVOT Open Lab/Challenge Project:**

**Version 0.9**

Lab / Challenge Developers,

We have an eager audience of participants ready to try out your new lab/challenge - they just need a little info to get started. Please provide some basic details of your work by filling out this brief template.

Keep in mind that we encourage creativity and new ideas, so if your lab or challenge does not fit some of the questions below, that’s OK! Just let us know as much as possible about the special thing you’ve built. If you have any questions, please contact ????.

|  |
| --- |
| Title of Lab / Challenge: Digital Forensics Challenge - Save the Animals  Location on Web: [**https://drive.google.com/folderview?id=0B5wo\_1rRmpqVZ3Myc2xtNFBkT0k&usp=sharing**](https://drive.google.com/folderview?id=0B5wo_1rRmpqVZ3Myc2xtNFBkT0k&usp=sharing)  **The Basic Facts**  *Who?* Author’s Name: Mandy Galante  Author’s Organization: Red Bank Regional High School  *What?* Short description of the Lab/Challenge  Analyze evidence to help the Toy Story Police Department (TSPD) investigation of a series of kidnappings. Baby stuffed animals are being kidnapped from their homes and sold on the international stuffed slave market. The TSPD has found 4 pieces of digital evidence and your job is to analyze the acquired data and find enough evidence so that Sheriff Woody can bust this evil stuffed slave market.  *Why?* Skills that can be learned from this Lab/Challenge  Digital Forensics techniques = (1) Analyze file metadata (2) Extract info and files from a packet capture (3) Retrieving deleted files (4) File carving fragmented files (5) Retrieving info from Browser files (6) Extract info about a Windows computer from a Registry File  *Pre-Req?* Skills that are needed going into this Lab/Challenge  Some familiarity with some or all of these tools: Wireshark, Exiftool, FTK Imager or Autopsy, RegRipper, Scalpel or Foremost.  *Difficulty Level ? (circle one)* Introductory - Moderate - Advanced  *How long?* to Complete Instruction: no teaching materials included  to Complete Lab / Challenge: 60 to 90 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:** Exercise is targeted at providing practice for those who have previous experience with the tools suggested for each task BUT also possible to figure out how to use the tools through online research. |
| **Checklist**  *What you get:*  - Assets provided in this Lab / Challenge. (Please list all, such as pcap files, VM images, evidence files, etc.):  **j3uv3vk.default folder FlashEvidencce.001 SAM Evidence\_Pcap.pcapng**  *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 and an internet connection**  *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.):  Access to a virtual machine that has preloaded forensic software tools - examples are Kali Linux or SANS SIFT Workstation 3.0 [https://digital-forensics.sans.org/blog/2014/03/23/sans-sift-3-0-virtual-machine-released#](https://digital-forensics.sans.org/blog/2014/03/23/sans-sift-3-0-virtual-machine-released%23) |

|  |
| --- |
| **Wrapping it up**  Can you give us a longer narrative that tells us what makes the Lab / Challenge fun, interesting, and targets the development of useful information security skills?  This challenge offers the chance to apply knowledge of several tools to solve a puzzle. The challenge does not have a "right or wrong" way to find the answers so the competitor is pushed past the typical following of instructional steps to figure out their own methods. But the good news is that there is enough support info so that the competitor will not end up flailing or getting lost. Recommend this exercise be done with an instructor present who has the answer sheet so that the competitor can be assisted with hints.  If you have had a chance to look at the existing challenges, can you suggest where your Lab/Challenge fits into that Roadmap or Sequence? |