TechFest v2.017 Competitive Event Playbook

Competition Title: Forensics in the Digital Age

Competition Sponsor: Ivy Tech Community College of Northeast Indiana

Competition Summary: Teams of four students will work collaboratively to find and identify digital evidence from a simulated crime scenario and solve a collection of forensics problems within the allotted time limit.

Competition Details: This will be an exercise in Digital Forensics documentation using the Chain of Custody and searching evidence gathered from the crime scene for a warrant on an alleged crime that was committed. You will be presented a bit-to-bit copy of digital evidence from a crime scene where you will use provided digital tools to answer a series of questions.

Pre-defined Team Roles: 2 students partnered as the First Responder Team and document the crime scene, 2 students partnered using FTK to research image file(s) already gathered from the crime scene.

School Points Awarded for Gold, Silver, Bronze: 5,000, 3,000, 1,000, respectively

Scoring Rubric:
Teams will be given five or more challenges which will be scored individually. Points will be awarded for: crime Scene protection, documentation, and evidence gathering, obtaining Search Warrants, evidence evaluation, and reporting the Evidence for the case. The teams who scores the most points wins.

Event Software That Will Be Provided:
FTK Imager: Download from AccessData http://accessdata.com/product-download
HexWorkshop: Download from Breakpoint Software http://www.bpsoft.com/downloads/
IrfanView: Download from www.irfanview.com
PsTools: Download from http://technet.microsoft.com/en-us/sysinternals/bb896649.aspx
Wireshark: Download from www.wireshark.org
Checklist: https://www.policeone.com/investigations/articles/2142763-Investigating-property-crimes-A-checklist-for-success/

Pre-Work Required: None

Pre-Work Possible (not required): Look into the software above and become familiar with it to go in with a better understanding of how to utilize each different program. Understand the scope of a search warrant and what you are looking for at the crime scene. Also securing the scene with pictures, labeling etc. Collecting and securing the evidence with the Chain of Custody. Using FTK to search through the data collected to document evidence for the case.