RET Site: Research Experience in Cybersecurity for Nevada Teachers (RECNT)

Josh Barham
Carl Antiado and Eric Valdez
PI: Shamik Sengupta, Co-PI: David Feil-Seifer

Introduction

Digital Forensics is a field that requires a deep understanding of the digital environment. Before one can dig in on an investigation you must understand what it is you need to be looking for and where you can find it.

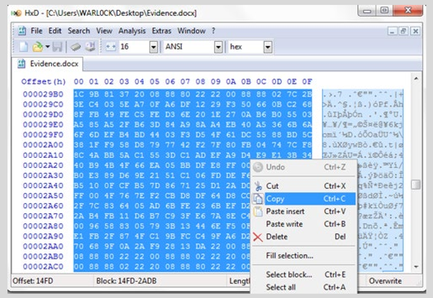
Mock-Investigation

NIST (Nation Instituite of Standards and Technology) Provides anyone with pre-created images to perform a mock investigation. These comprehensive images give one an idea of what a real investigation looks like.

NIST
National Institute of Standards and Technology

Key topics

- File Systems
- File Types
- Imaging
- Checksums
- Chain of Custody
- Deleted files
- Registry
- Documentation
- Validation
- File Carving



Evidence creation

NIST's free images are great but there are only so many available. What if we want a new one or a custom scenario. Our research explored the viability of creating an application to customize a memory space to facilitate mock digital investigations

Software

Building foundational knowledge is important. A digital investigation could be performed 100% by hand. One could spend perhaps a lifetime manually evaluating a memory space. Luckily, there are applications that can aid in an investigation. Open-source software makes exploration like this more accessible in a classroom environment.

- Autopsy
- HXD Hex Editor
- OST Kernel Viewer
- DB Browser
- Exif Tools

Oceans 5: UNR

Our research was showed the easiest method currently available was to manually create your own evidence packages. As a cohort we created a fake heist occurring at UNR for our students to investigate. As our cohort consists of five individuals, we dubbed it Oceans 5.

This research is supported by NSF Award #1855159: RET Site: Research Experiences in Cybersecurity for Nevada Teachers (RECNT).