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

PI:Shamik Sengupta, Co-PI: David Feil-Seifer and
Muhammed S Bilgin

Introduction

It is a great opportunity to explore unique ways to engage myself in summer research experiences that emphasize Digital forensics. The purpose of this project is to explain the key aspects of digital forensics. Digital Forensics uses scientific principles to provide the method of evidence acquisition. It is common to have a standard digital forensic process to deal with the acquisition, analysis, and reporting of data in any organization – not just law enforcement.

Chain Of Custody

According to NIST The process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose of the transfer

Chain of Custody Steps

- Record each item as evidence
- Record who collected it and when
- Write the description of the item
- Record the evidence in a container and properly labeled with who collected it and when
- Record all message digest (hash) values
- Securely transport the item to storage
- Obtain a signature from a person at the storage facility
- Prevent access to/ability to compromise item
- Securely transport item to court as evidence

Chain Of Custody Terms

Timeline of Sequence of Events
- ❖ -List of where the data has gone and who has touched it

Time Stamp
- ❖ -A record of when an artifact was collected

Time Offset
- ❖ -Aligning with a coordinated time zone

Admissible
- ❖ -Acceptable as evidence in court

Video Evidence
- ❖ Video of collecting/altering artifacts

Evidence Integrity

Non-Repudiation
- Without a doubt the evidence was not tampered with

Hashing
- Putting digital evidence through a hashing algorithm to get a checksum
- Will be different if evidence has been tampered with

Checksum
- The output of the hashing algorithm

Provenance
- Earliest known state of the evidence

Preservation
- Protect the data

Legal Host

- Also known as Litigation Hold

-Legal action to properly preserve evidence for a case

- A legal document provided as a hold notification informing the organization on what should be preserved
- Once notice is received, no data may be altered, otherwise, the court may view it as obstructing, tampering with, or destroying evidence

Digital Evidence Terms

- **On-premise gathering**
  -Collecting evidence that is on-site
- **Cloud gathering**
  -Collecting evidence from remote systems/servers
- **Jurisdiction**
  -Law enforcement's legal authority to gather evidence
- **Data Breach Notification Laws**
  -Laws in areas that regulate when they are required to publicly notify data breaches
- **Right-to-Audit Clause**
  -When someone has the authority to audit or investigate a system

Tags→Used for numbering evidence
Event logs→logs of what has occurred during the evidence collection
-Who collected what evidence?
-What evidence has been collected?
Reports→detailed Reports are taken to document what has occurred
Interviews→First-hand experiences from all those involved

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