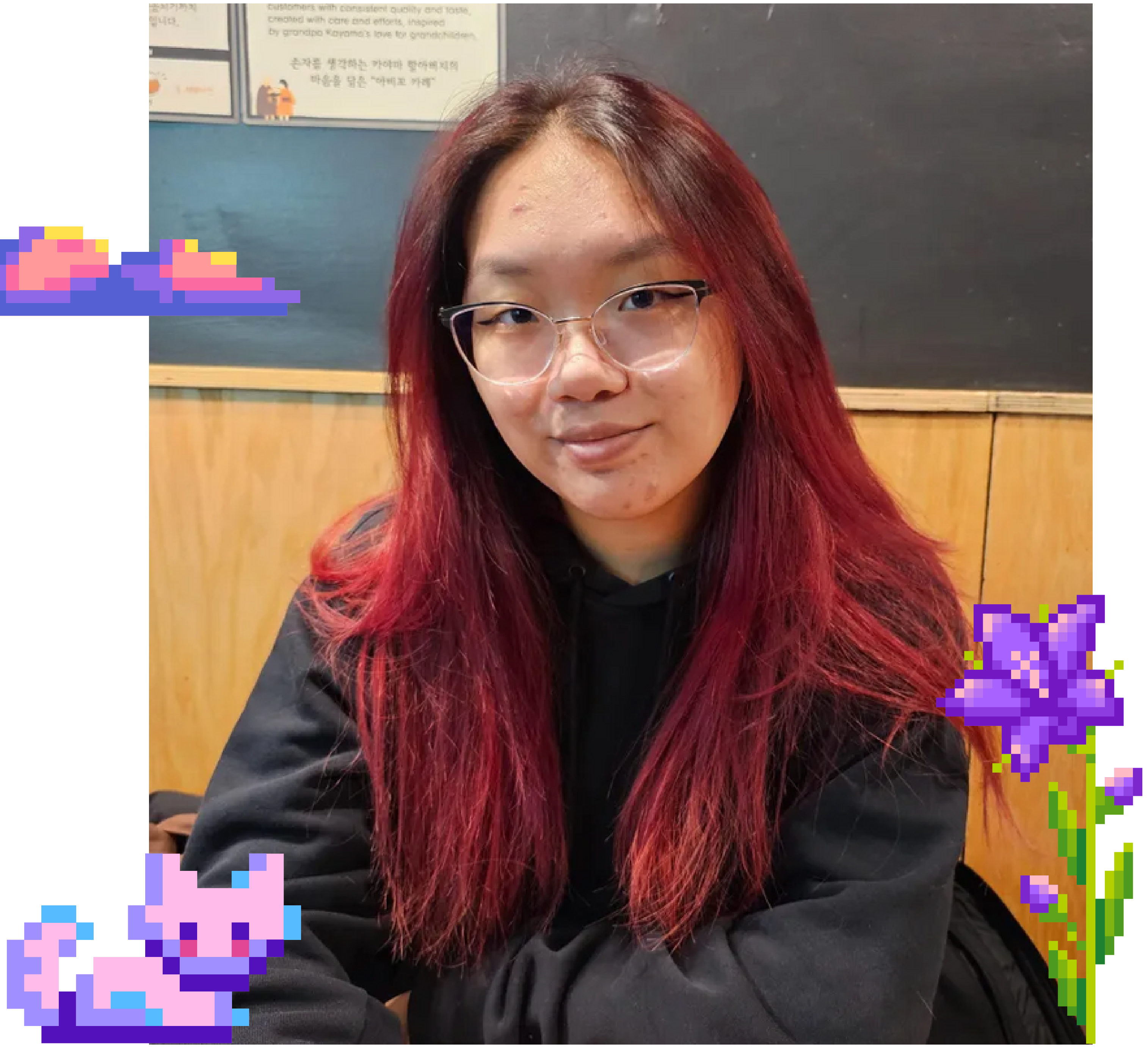
Digital Forensics and Incident Response

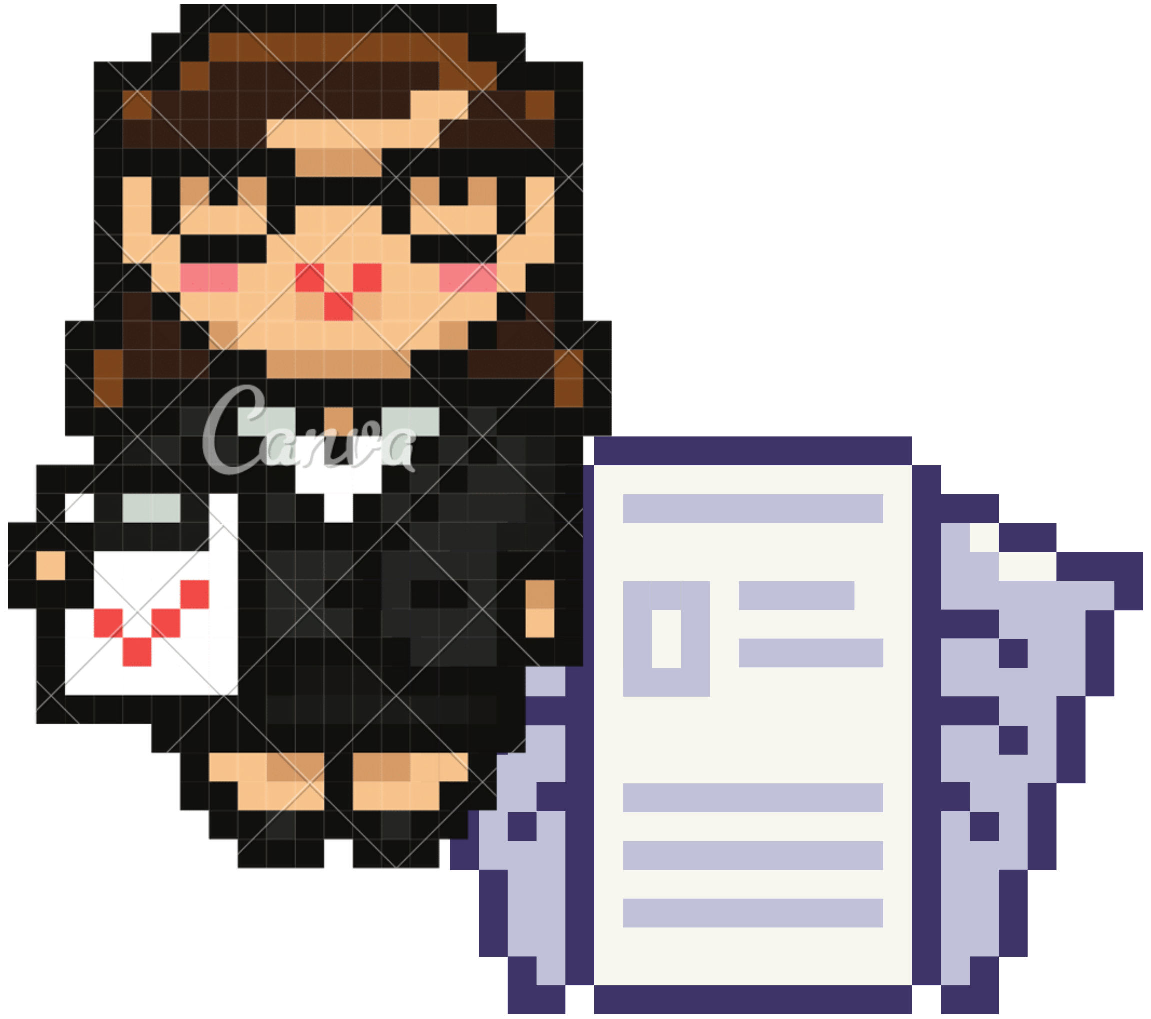
By Kat Nayan

$whoami

🐈 Kat Nayan
👩🏻‍💻 4th year CSEC
💻 DFIR LOVER <3
😎 cat mom to dumpy and uni
👟 i paint on shoes sometimes
❤️Sigma Psi Zeta Sorority, Inc.,
(ex) WiCyS Secretary,
(ex) WiC Outreach Co-Head
💌 @meekzen on disc



Agenda



✓ **Incident Response**

- Introduction
- Lifecycle

✓ **Digital Forensics**

- Introduction
- Process
- Significance
- Challenges

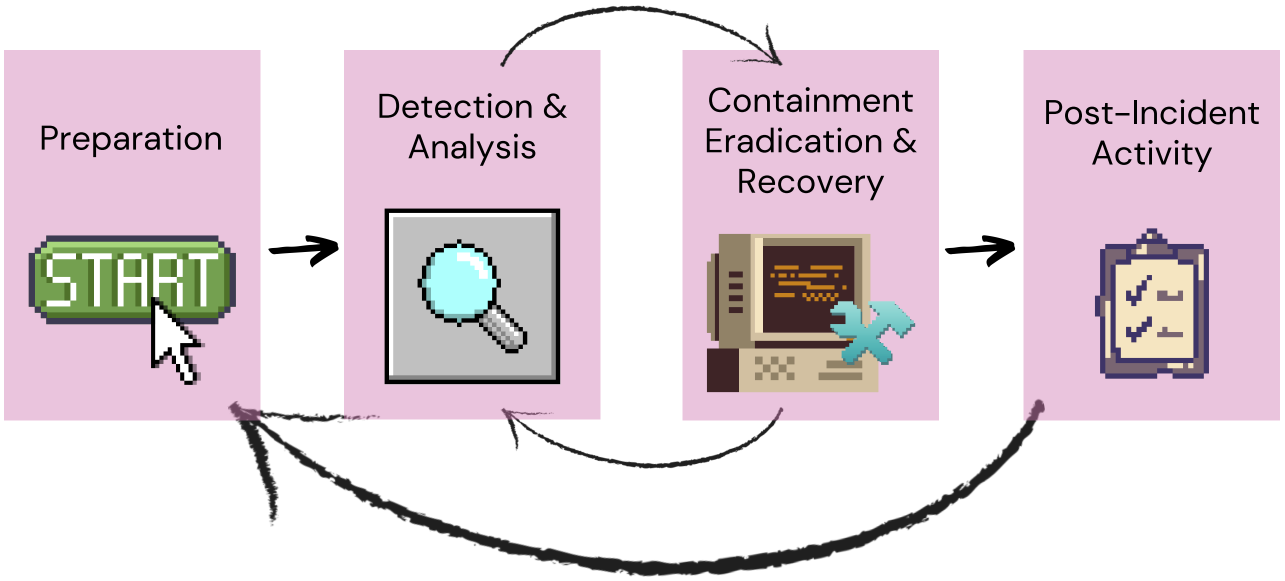
Incident Response

Introduction

Introduction

Incident Response

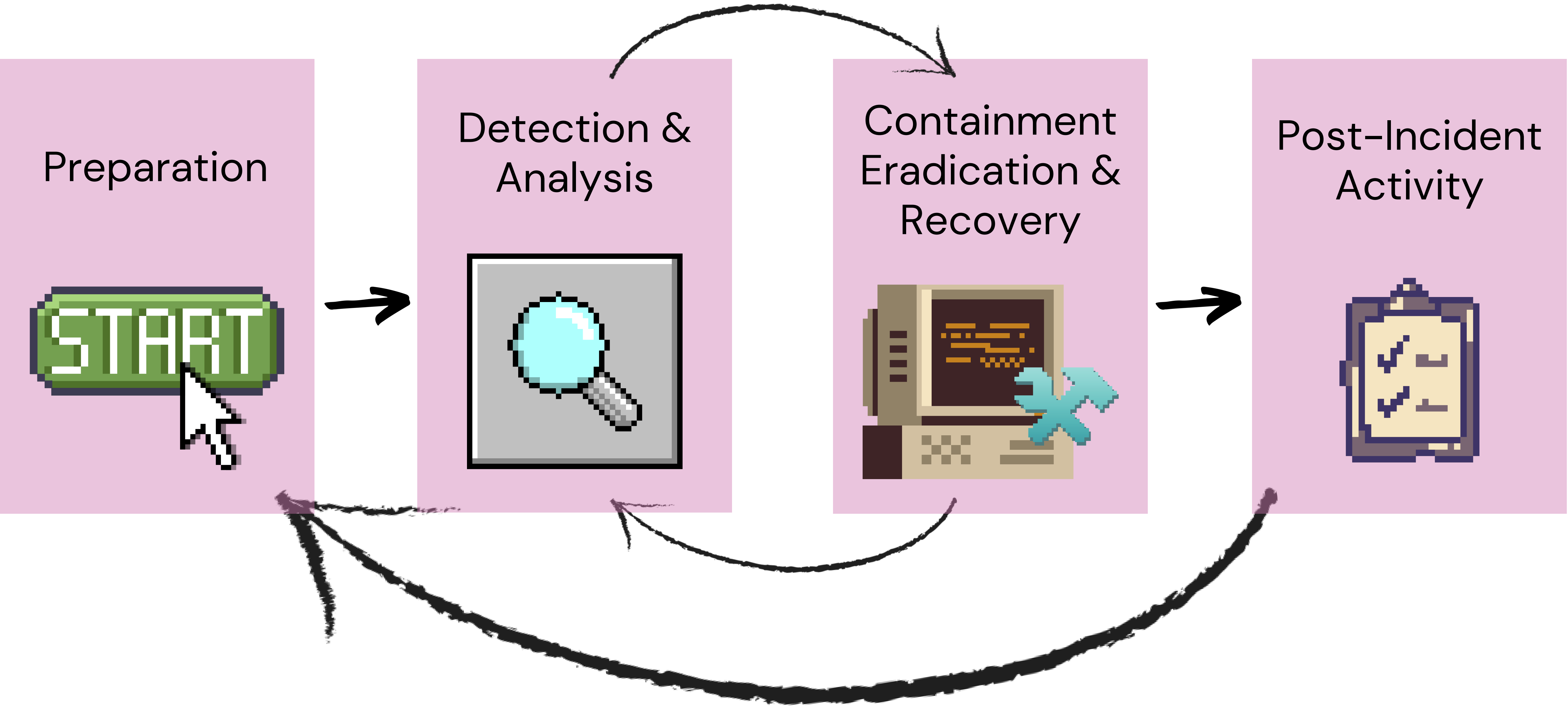
- The steps used to **prepare for, detect, contain, and recover** from a data breach
- Effectively manage the incident so that damage is limited
- Want recovery time, costs, and collateral damage kept to a minimum



Incident Response Lifecycle

Introduction

Lifecycle



Preparation

Detection & Analysis

Containment Eradication & Recovery

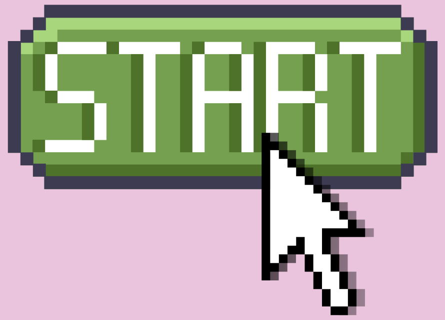
Post-Incident Activity

Lifecycle

Preparation

- Develop incident response policies and procedures
- Identify incident response team roles and responsibilities
- Establish communication protocols
- Identify necessary resources (e.g. tools, personnel, training)
- Conduct regular testing and training

Preparation



Lifecycle

Detection & Analysis

- Monitor for unusual activity (e.g. network traffic, system logs)
- Review logs for potential indicators of compromise (IoCs)
- Conduct forensic analysis to determine the nature and scope of the incident
- Classify the incident based on severity
- Notify appropriate incident response team members

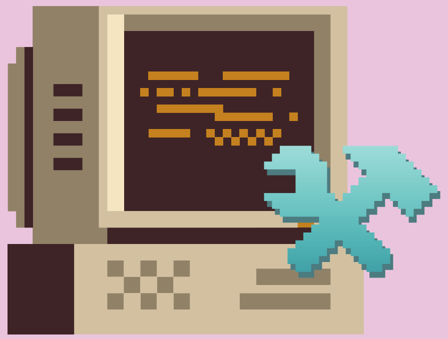
Detection & Analysis

Lifecycle

Containment & Eradication

- Identify and isolate affected systems or network segments
- Limit the spread of the incident
- Prevent additional damage or data loss
- Preserve evidence for analysis and investigation
- Notify appropriate incident response team members

Containment
Eradication &
Recovery

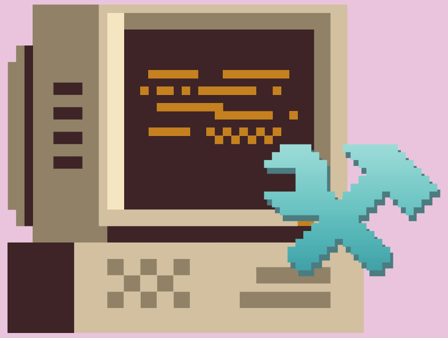


Lifecycle

Recovery

- Restore systems or data from backups
- Verify that data integrity has been maintained
- Test restored systems and applications for functionality
- Reconnect systems or networks to the production environment
- Notify appropriate incident response team members

Containment Eradication & Recovery



Lifecycle

Post-Incident Activity

- Assess the effectiveness of the incident response process
- Identify areas for improvement
- Document lessons learned and share with appropriate stakeholders
- Communicate the incident response process and outcomes to relevant parties
- Monitor for potential residual effects or follow-up incidents

Post-Incident Activity

Digital Forensics

Introduction

Introduction

Digital Forensics

- A subfield of forensic science concerned with the **identification, acquisition, analysis, and reporting** of data stored electronically, which is referred to as **evidence**
- Must be careful when handling as it will/may be presented in a court of law

Introduction

Artifacts

- Ways to tell something was executed
- **Things you can collect from a dead system:**
  - *Passwords, Logs, Hidden Data, SUID/SGID Files*
- **Prove execution:**
  - *Amcache, Shimcache, Prefetch, MUICache, UserAssist, Jumplists, NTUSER.DAT, etc.*
- **Imply Potential Execution:**
  - *shellbags, .LNK files*

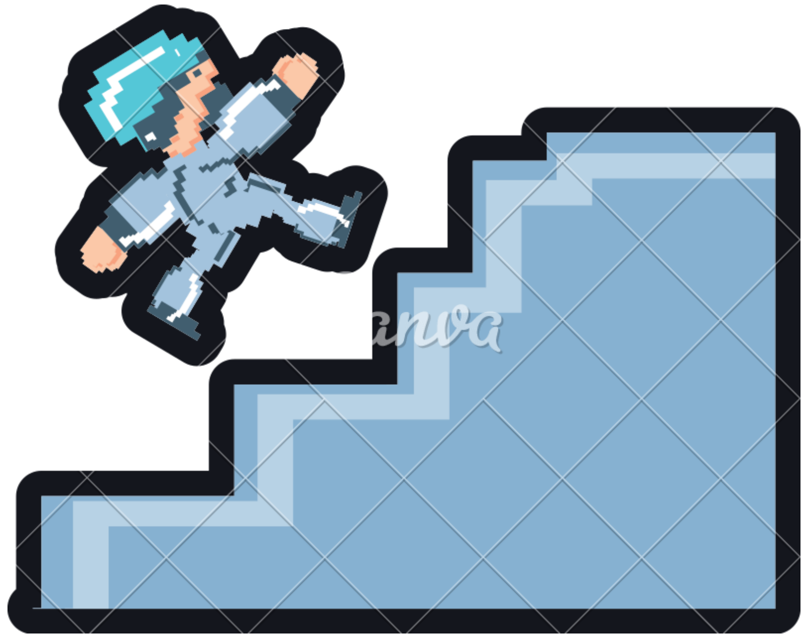
Digital Forensics
Process

Process

Procedure

There are **four** main steps to a digital forensics investigation process:

- Collection and Acquisition
- Preservation of Evidence
- Analysis
- Reporting and Presenting



Process - Procedure

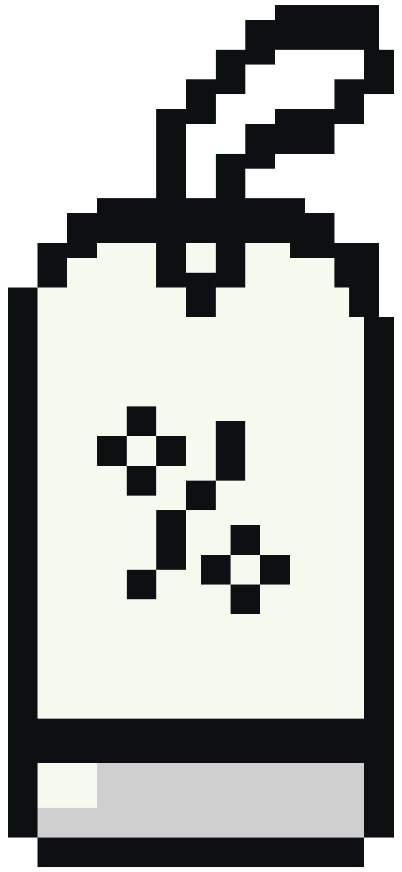
Collection

- If the system you are collecting data from is still alive, unplug the network and plug in somewhere else that isn’t connected to anything else
- Acquire volatile data
  - Volatile Data
  - Non Volatile Data
- Used to gather information about users, determine what happened, create a timeline, discover tools and exploits

Process – Procedure

Preservation

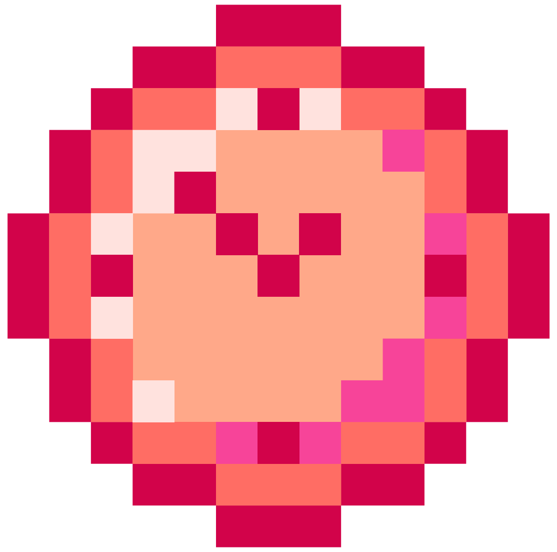
- Establish a chain-of-custody
  - Maintain a detailed record of how evidence has been handled from the moment it was collected to the moment it was presented in court
  - **Includes:**
    - Date and time of evidence collection
    - Information of people processing evidence
    - Locations and descriptions of evidence
- Verify the evidence is intact and has not been altered
- Evidence is stored in a tamper-proof manner
- MD5 and SHA1 are commonly used (integrity verification and prevents collisions)
- Timestamps and timelines



Process - Procedure

Analysis

- Important to analyze content that may have been deleted or data that is typically inaccessible
  - Analyze files and file systems
  - Construct a timeline - examine MAC times
    - Modified
    - Accessed
    - Created
  - Look for artifacts
  - Search for keywords and perform hash analysis



(this is supposed to be a clock.....)

Process – Procedure

Reporting

- Purpose is to report legally admissible evidence to a court of law
- Make sure all steps are included:
  - Equipment used
  - Methodologies
- Facts and data to support or reject the statement
- Included analysis details during your report
- Statements and conclusions should be accurate

Digital Forensics
Tools

Tools

Tools/Frameworks

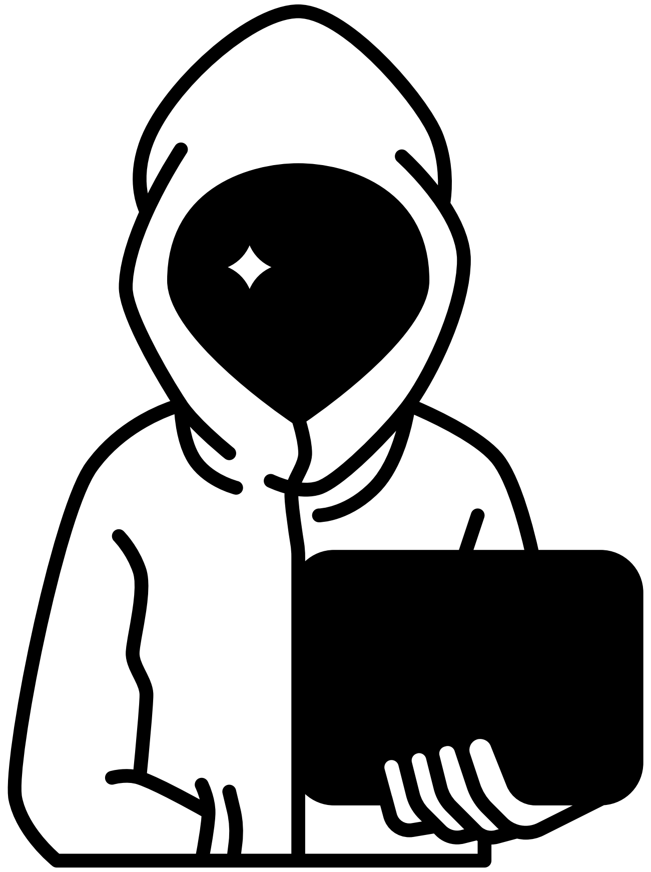
- Autopsy (Free)
- FTK ($ $ $)
- FTK Imager (Free)
- EnCase ($ $ $)
- Volatility (Free)
- SIFT (Free?ish?)
- Axiom ($ $ $)
- etc.

Digital Forensics
Challenges

Challenges

Anti-Digital Forensics

- What is ADF?
  - Acts aimed to make the discovery of illegal activities by a user harder to discover
- To manipulate, erase, or obfuscate digital data
- Make examination difficult, time consuming, or virtually impossible
- **Methods include:**
  - Overwriting or wiping data
  - Hiding/obfuscating data
  - Steganography or cryptography



Thank you!

Any Questions?

kyn3603@rit.edu or
@meekzen on discord