# Steganography Detection Plugin for Autopsy

## Abstract

A steganography detection plugin for Autopsy that utilizes scripting and machine learning to analyze and detect hidden data within images. This tool streamlines the investigative process by allowing real-time, automated steganographic analysis. It plays a critical role in modern digital forensics, reflecting the increasing need for sophisticated detection methods to combat advanced concealment techniques.

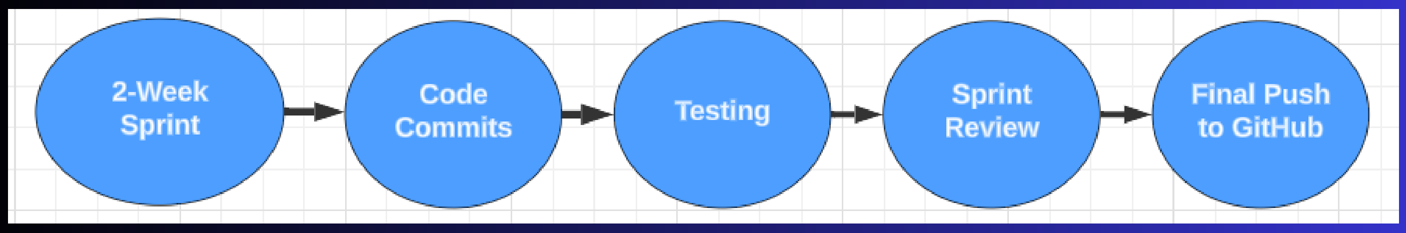
## Motivation

Autopsy, being one of the most widely used platforms in the field, lacks a dedicated steganography plugin for investigators.

## Platform

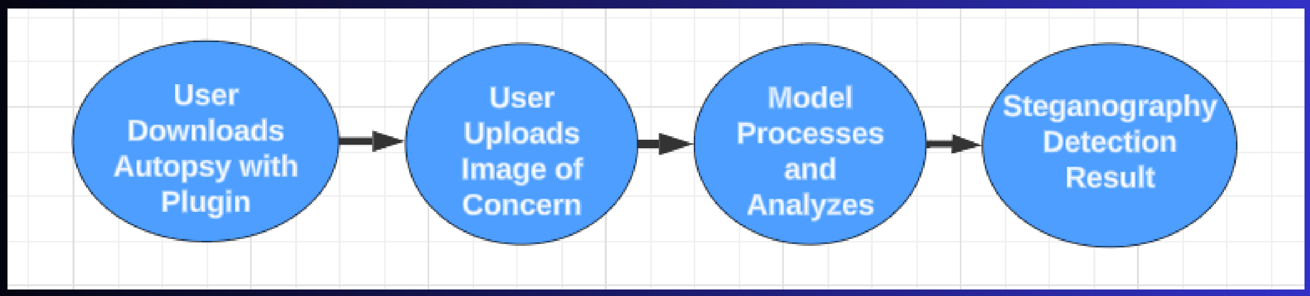
The Autopsy plugin was built from scratch using NetBeans, which enables the ability to run the Autopsy environment within NetBeans for testing purposes.

## Core Work and Methodology


2-Week Sprint → Code Commits → Testing → Sprint Review → Final Push to GitHub

- Developed Autopsy plugin functionality that has 2 core classes:
  - Factory class
  - Ingest Module
- Created two steganography detection methods:
  - LSB analysis script.
  - ML model.
- Trained model with IEEE dataset steganalysis for still images with LSB steganography
  - 70K data entries, 8 features.
  - Leveraged Kaggle & Colab for model training.
- Integrated Python scripts / models with Java for Autopsy.
- Released tool to forensics community.

## Flow Chart


User Downloads Autopsy with Plugin → User Uploads Image of Concern → Model Processes and Analyzes → Steganography Detection Result

Java python AUTOPSY DIGITAL FORENSICS CO MACHINE LEARNING GitHub kaggle

SETU Ollscoil Teicneolaíochta an Oirdheiscirt South East Technological University

## Andrew Baxter

BSc Computer Forensics & Security
Department of Computing & Maths
South East Technological University