EECS 388: Lab 11

- Project 4 Review
- Forensics Project
- Autopsy Tutorial

Current Assignments

- Project 4 - AppSec
  - Done!
- Project 5 - Forensics
  - Available now!
  - Lab assignment 5 due Thursday, November 30th @ 6pm
  - Project 5 due **Thursday, December 7th @ 6pm**
    You MUST work with a partner for Project 5
    Register your group in the Autograder by November 23rd @ 11:59 pm

Project 4 Review

Buffer overflow techniques

- Targets 1-2
  - `LEA` command + 8 (RBP)
- Target 3
  - `strncpy` w/ additional 16 bytes for ***a*** and ***p***
  - Set p to return address
- Target 4
  - Integer overflow
- Target 5
  - Set registers so a call to execve runs `/bin/sh`
- Target 6
  - Insert `nop` sled
- Target 7
  - Find ways to clear a register
- Target 8
  - Use analysis and process of elimination to understand functionality

~~Project 5~~

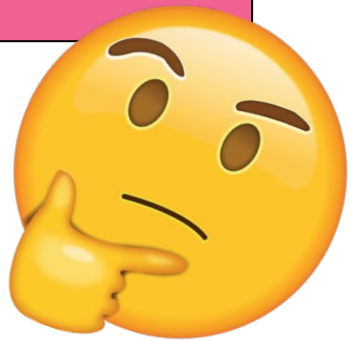
Welcome to **SUPER DUPER SKETCHY CORP**!

You Work for SDSC Now

- https://superdupersketchycorp.biz/
- SDSC seems to have an issue.
- An employee, **Leslie Nielson**, set to be let go, suddenly disappeared and their drive has been encrypted.
- We have obtained a (decrypted) copy of their hard drive. It's up to you to figure out:
    - Are they guilty of a crime?
    - If so, what crime?
    - What evidence supports this claim?

Project 5 Tips

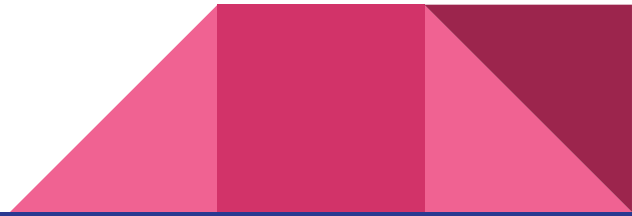
Read the spec very carefully! Additional questions ***might*** be uncovered throughout the course of your investigation that are not listed in the spec.



- Completely open-ended.
  - We do not expect anyone to find *all* of the secrets
- But how do I know when I'm done?
  - Full credit if you get at least 40 tokens! (Proportional credit for fewer.)
  - This project is full of secrets that get increasingly difficult to find.
  - Your goal is gather enough evidence to form a coherent case for or against Leslie.
- Take notes of EVERYTHING you do.
  - You will write a report in the end, detailing whether Leslie is innocent or guilty of a particular crime.

Project 5 Tips

- Start early!
  - The open endedness of project 5 can make progress slow at times, and you don't want to run out of time on a promising lead.
- Start early!
  - Sometimes it takes some sleep to put the clues together.
- Start early!
  - Hint emails will take significantly longer close to the deadline due to volume.
- Start early!
  - Courses always tell you to start early, but it really matters this time.
  - This is not a project you can put off!



Project 5: Getting Help

- **Ask HQ for permission** before visiting any external sites, resources, or places.
  - https://superdupersketchycorp.biz/admin/permissions/
- Email HQ for mission-specific help.
  - Hints: Each group can get help on 3 *specific* questions. **(There are no generic hints.)**
  - To: eecs388-proj5@umich.edu
  - Subject: **388 P5 Question**
- Use Office Hours / Piazza for tool-based questions.
  - **We can help with tools in general, but we cannot give hints or permissions!**
  - Only HQ knows about the investigation.

Good vs. Bad Questions

Good (Specific question)

eecs388-proj5@umich.edu

388 P5 Question

Hi HQ,

I've managed to get into the Bungle! site and located the next major vulnerability which I believe to be related to this search bar. I understand that an XSS attack could inject a script to the site, and I know we should steal the previous search, but I can't find what port to send this info to. What port should this be? Or any guidance on where to look to find the port?

Any help regarding this attack would be greatly appreciated!

Verdana

Bad ("What's next?")

eecs388-proj5@umich.edu

388 P5 Question

Hi HQ,

I'm at the Bungle! site. To get here, I found a file that contained this url, so I visited it on my TOR browser. Where should I go from here? Is this site helpful or is it a dead end?

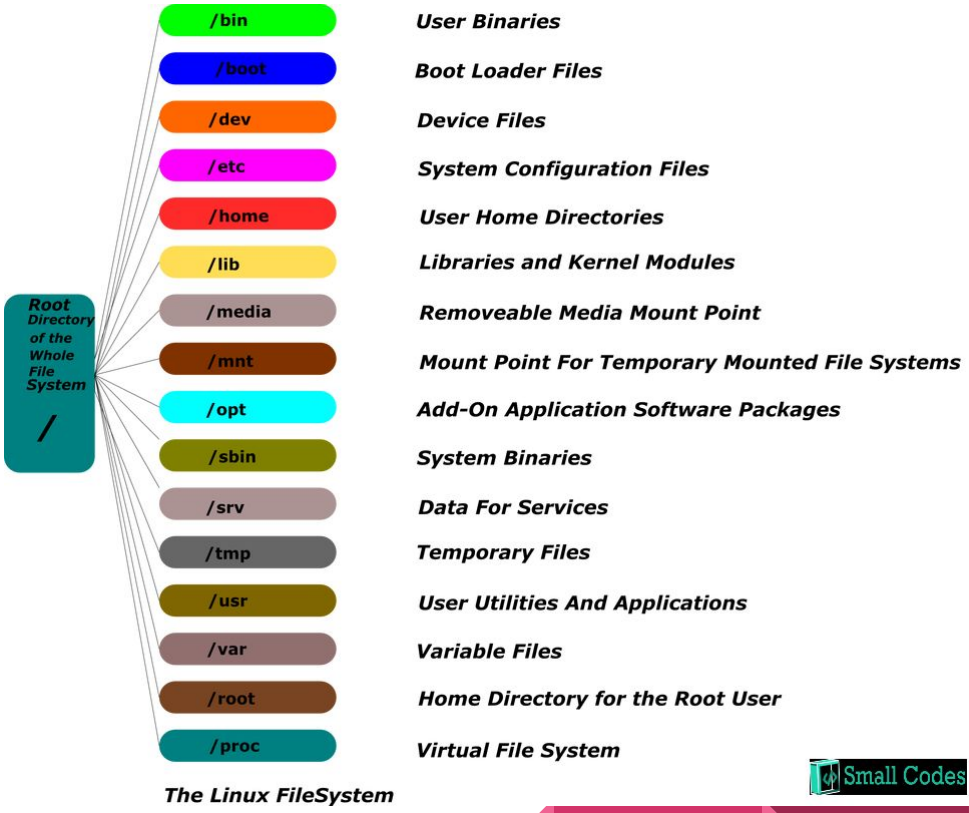
Thanks.

Verdana

*Assuming the student first requested permission to access "Bungle!"

Helpful Linux directories

- /bin
  - Binary executables
- /etc
  - Configuration files
  - Startup and shutdown scripts
- /var
  - Variable files (files expected to grow)
  - Think logs, mail, temp files…
- /home/user
  - For users to store personal files



more directories

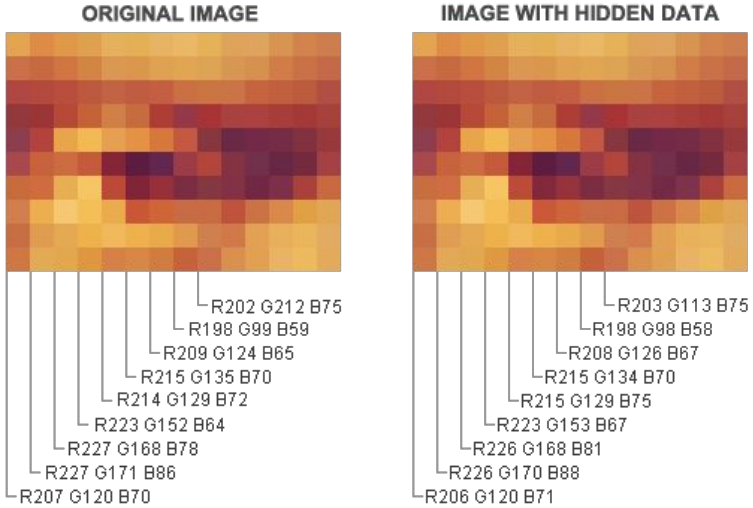
Project 5 Tools

- Autopsy
  - Useful for examining a system without running it
  - Spec has instructions on how to set it up

- Password cracking
  - John the Ripper
    - Brute forces password-protected files
    - Hash generators for different file formats + wordlists available online

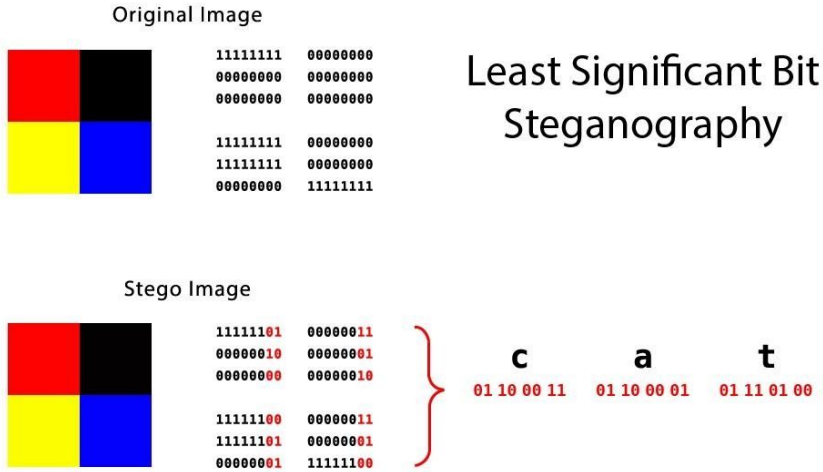
Steganography & Steganalysis

- Steganography
  - Covertly hide content
  - Modern stego involves digital documents
    - Audio and images (MP3, AAC, PNG, JPEG, …)
  - Exploits limits in human sensory systems
- Steganalysis
  - Detecting hidden content



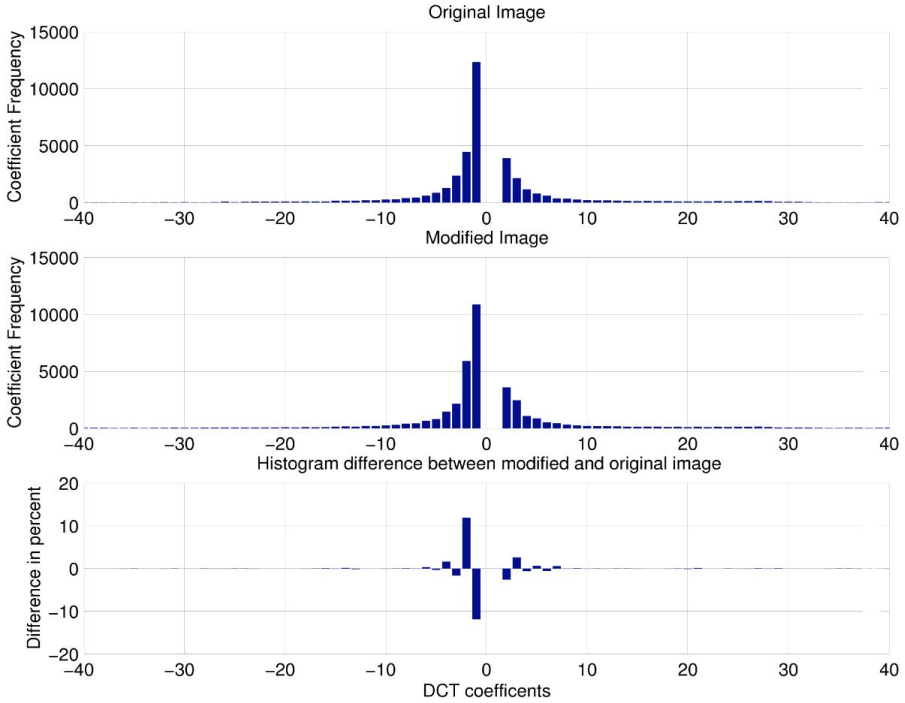
Techniques

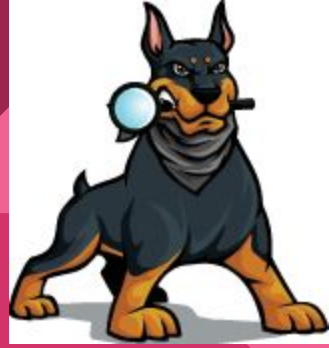
- Simple approach
  - “Hiding” message in the metadata (in the JPEG EXIF or MP3 tag)
- Perceptual coding
  - LSB encoding
    - Modifying the least significant bit of the pixels of the original image
  - Hide the message in the redundant bits
- Used by ISIS to send secret messages
  - https://www.wired.com/story/muslimcrypt-steganography/



Statistical Analysis of JPEG

- Stegdetect
  - Computes a chi-squared test on adjacent pixels
  - Classifies image as likely, possible, or unlikely to contain stego content
  - Looks for stego embedded with 3 popular programs: Jsteg, JPHide, OutGuess

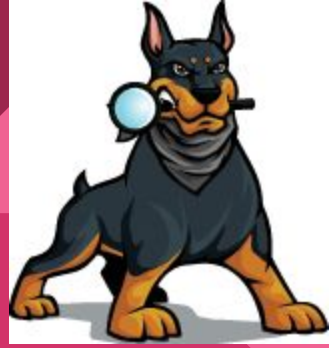




Autopsy

What is Autopsy?

- A tool for the parsing, search of viewing of computer disks.
  - In our case it will be an .vhd file.
- Key Features:
  - **Ease of use** → Intuitive and easy to navigate GUI.
  - **Searchability** → Allows for keyword search over the entire disk file.
  - **Breadth of Files** → Includes variety of known file types, including web artifacts (cookies, search history, etc.).
  - **Data Carving** → Recovers any deleted files from space that hasn't been overwritten.



Autopsy Functionality

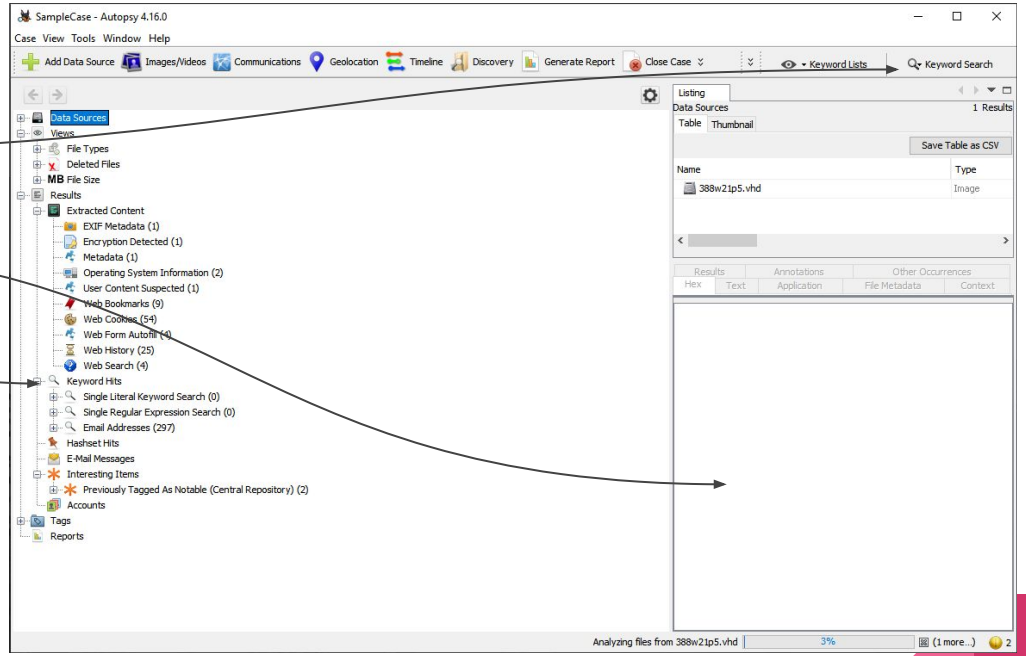
Overview

Toolbar

Search

File Data

File Tree



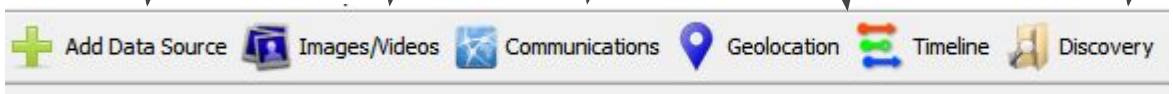
Toolbar

Unnecessary
have already
.vhd

Shows you i
videos found

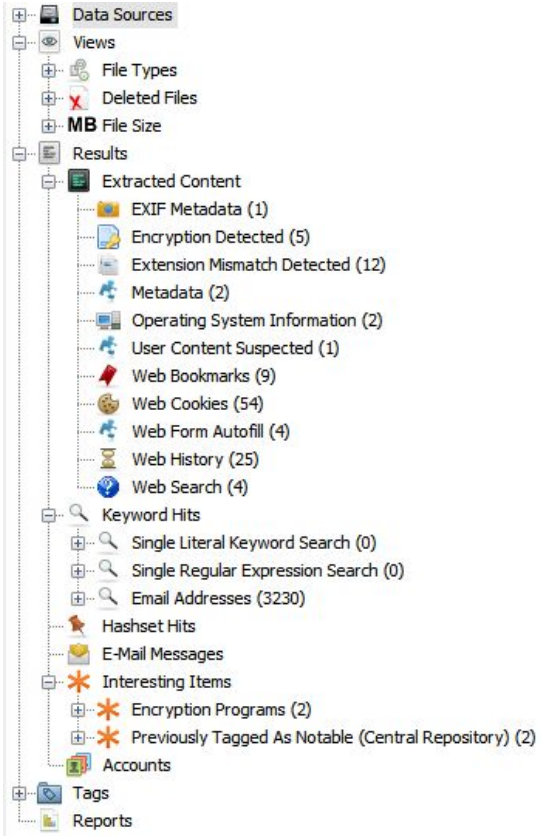
Would show you communications from this device, logged locations, and a timeline of files. Not necessary for this project.

Allows you to search for files using certain limitations (e.g. type, size)



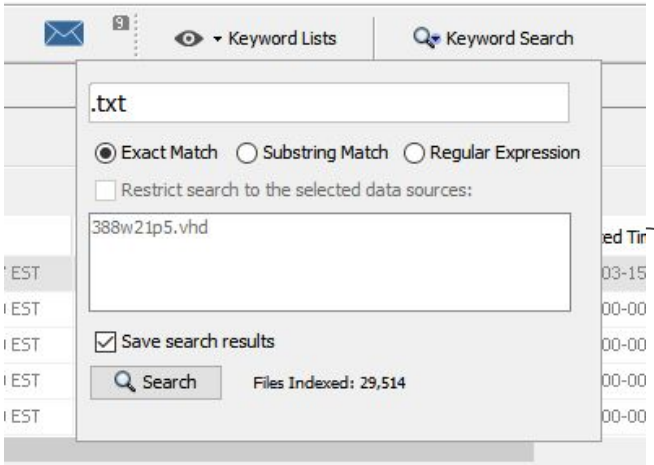
File Tree

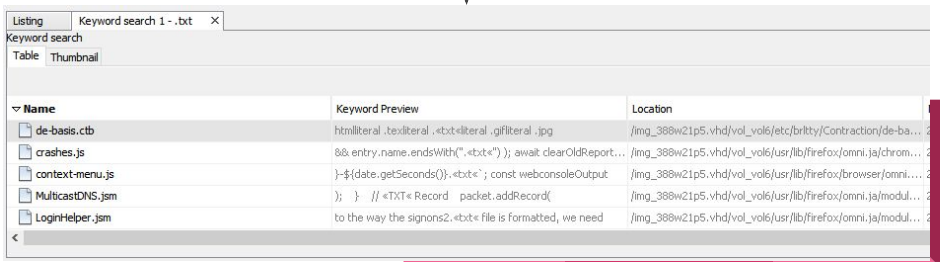
- Shows you the types of files discovered.
- Click on each individual section to see those types.



Search and Search Results

- Can Query Autopsy to search for strings, substrings, or regular expressions.





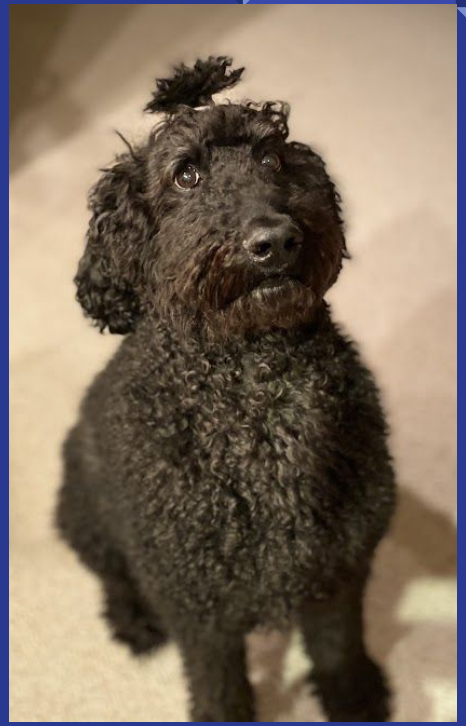
Resources

- Functionality Page (contains tutorials)
- User Guide and Documentation

Start Early Start Early Start Early Start Early Start Early Start Early Start Early
Start Early Start Early Start Early Start Early Start Early Start Early Start Early
Start Early Start Early Start Early Start Early Start Early Start Early Start Early
Start Early Start Early Start Early Start Early Start Early Start Early Start Early
Start Early Start Early Start Early Start Early Start Early Start Early Start Early
Start Early Start Early Start Early Start Early Start Early Start Early Start Early
Start Early Start Early Start Early Start Early Start Early Start Early Start Early
Start Early Start Early Start Early Start Early Start Early Start Early Start Early
Start Early Start Early Start Early Start Early Start Early Start Early Start Early
Start Early Start Early Start Early Start Early Start Early Start Early Start Early
Start Early Start Early Start Early Start Early Start Early Start Early Start Early
Start Early Start Early Start Early Start Early Start Early Start Early Start Early
Start Early Start Early Start Early Start Early Start Early Start Early Start Early

See ya!

(No lab next week)



this is champ