DIGITAL FORENSICS INVESTIGATIONS + SJU ACM CLUE

SJU ACM STUDENT CHAPTER

SJU ACM
Student Chapter

SIGN IN FORM:

INTRO TO DIGITAL FORENSICS

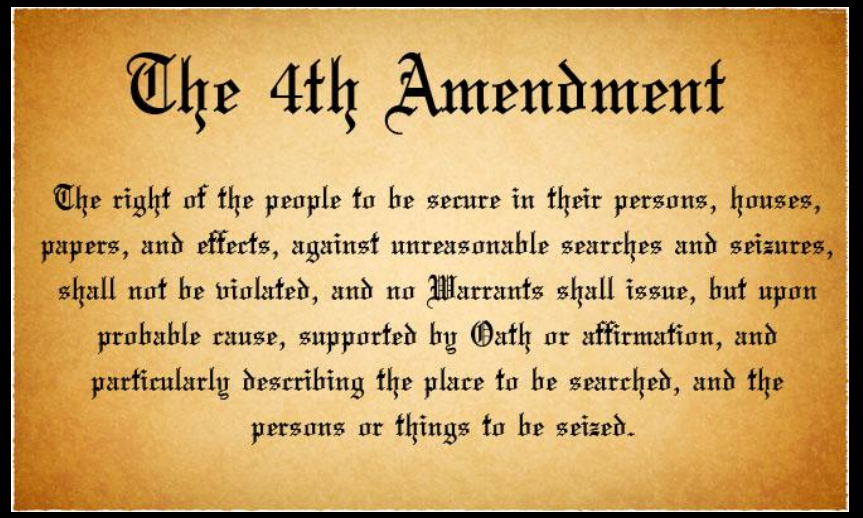
WHAT IS DIGITAL FORENSICS?

- A BRANCH OF FORENSICS SCIENCE THAT FOCUSES ON ELECTRONIC DATA
- ELECTRONIC DATA IS A HUGE COMPONENT OF CRIMINAL INVESTIGATIONS
- CAN ALSO BE USED DURING INCIDENT RESPONSE AS A PART OF CYBER ATTACK INVESTIGATIONS
- BOTH PUBLIC AND PRIVATE SECTOR
- REQUIRES A DEEP UNDERSTANDING OF HOW COMPUTERS AND FILE SYSTEMS WORK

5 STAGES OF A DIGITAL FORENSICS INVESTIGATION

1. IDENTIFICATION

- THERE ARE LEGAL CONSTRAINTS TO WHAT DATA CAN BE COLLECTED AND EXAMINED IN PUBLIC SECTOR INVESTIGATIONS
  - DETERMINE WHAT DATA IS RELEVANT TO THE CASE
  - DETERMINE THE SCOPE OF THE INVESTIGATION
  - NEED TO ACQUIRE A SEARCH WARRANT
  - FOURTH AMENDMENT RIGHTS ARE IN PLAY
- EVEN IN THE PRIVATE SECTOR, IT IS IMPORTANT TO IDENTIFY DATA PRIOR TO INVESTIGATING TO ENSURE A SMOOTH PROCESS



2. ACQUISITION

- PRESERVING EVIDENCE IS PARAMOUNT DURING ANY FORENSICS INVESTIGATION
  - ALWAYS USE A WRITE BLOCKER
- AS SUCH, ACQUISITION IS A DELICATE STAGE
- MOST COMMON ACQUISITION FORMAT: IMAGE FILE
  - A BIT-BY-BIT DIRECT COPY OF A STORAGE DRIVE
  - COMPATIBLE WITH FORENSICS TOOLKITS FOR FURTHER ANALYSIS OF THE CONTENTS OF THE DRIVE

3. ANALYSIS

- THE FUN PART
- EXAMINE DATA FOR ANY EVIDENCE THAT CONTRIBUTES TO THE GOAL OF YOUR INVESTIGATION
- CORRELATE ANY FACTS PREVIOUSLY KNOWN OR OPEN SOURCE INTELLIGENCE TO THE DATA AT HAND
- MANY TECHNIQUES TO PERFORM DEEPER ANALYSIS (MORE ON THIS LATER)

4. DOCUMENTATION

- THE NOT SO FUN PART
- VERY IMPORTANT TO KEEP TRACK OF ANY FINDINGS DURING THE INVESTIGATION
  - INCLUDE EXPLANATIONS ON HOW THE EVIDENCE WAS FOUND (TOOLS/TECHNIQUES USED)
  - FINDINGS SHOULD ALWAYS BE REPRODUCIBLE

5. PRESENTATION

- FINALLY, COMPILE ALL YOUR NOTES AND FINDINGS INTO A REPORT TO BE PRESENTED TO THE PROPER AUTHORITY

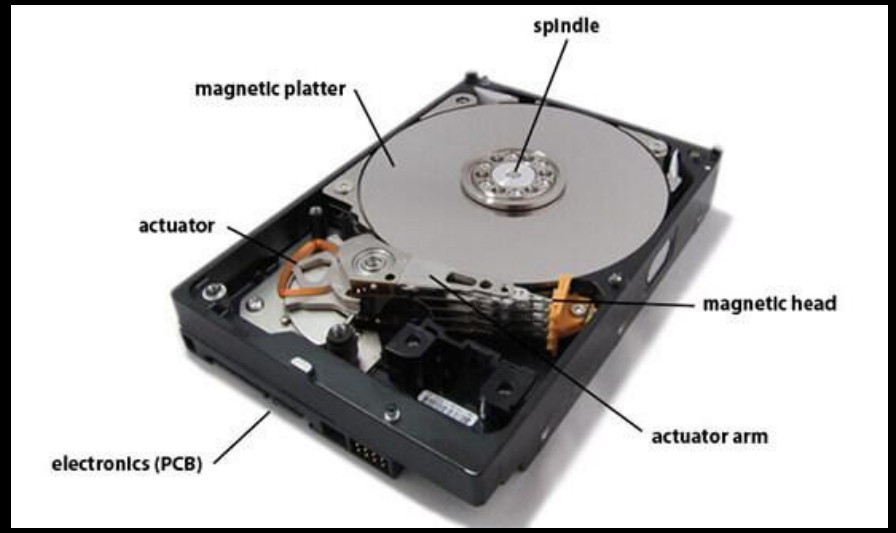
- PUBLIC SECTOR:
  - FORENSICS EXPERTS CAN PROVIDE TESTIMONY IN COURT
  - EVIDENCE COLLECTED CAN BE USED IN CRIMINAL AND CIVIL CASES
- PRIVATE SECTOR:
  - FINDINGS ARE TO BE PRESENTED TO WHOEVER HIRED YOU TO CONDUCT THE INVESTIGATION

HOW DATA IS STORED

PHYSICAL DATA STORAGE TYPES

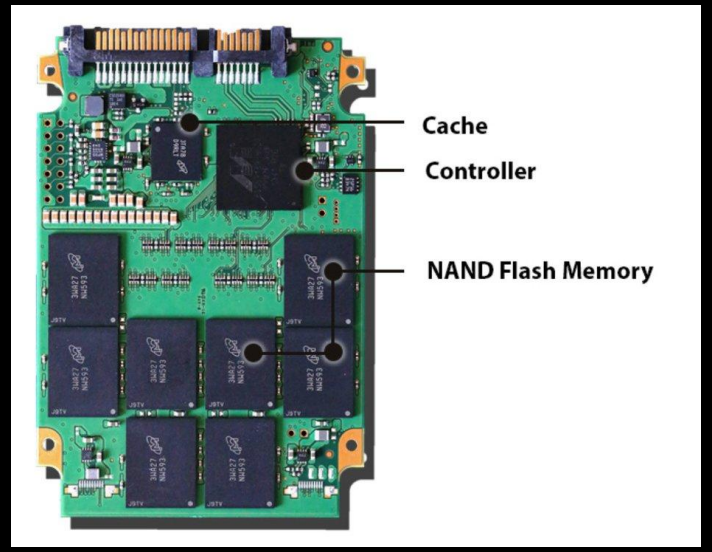
HARD DRIVE

- DATA IS MAGNETICALLY STORED ON PLATTERS
- DATA IS READ BASED ON MAGNETIC FORCE WHICH EQUATES TO ZEROS AND ONES



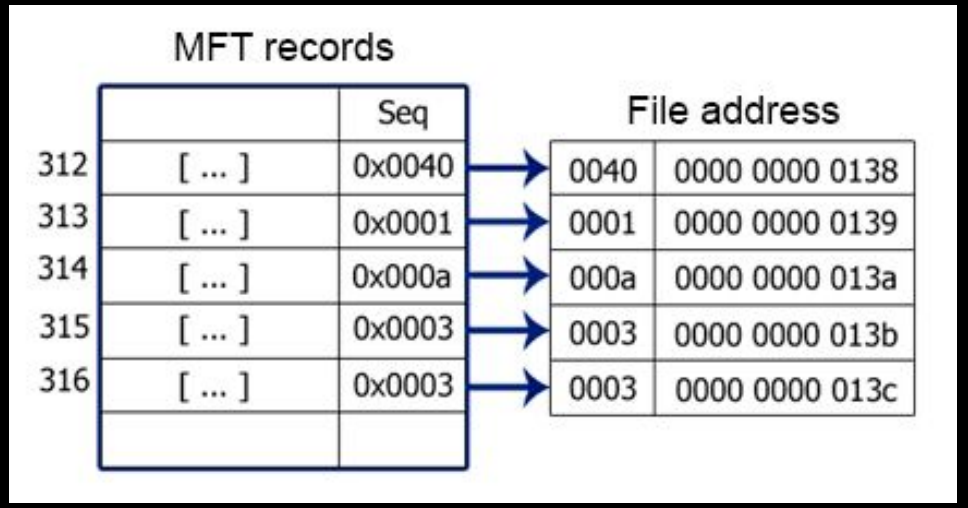
SOLID STATE DRIVE (SSD)

- DATA IS ELECTRICALLY STORED IN CIRCUITS
- DATA IS READ BASED ON ELECTRICAL CHARGES WHICH EQUATE TO ZEROS AND ONES



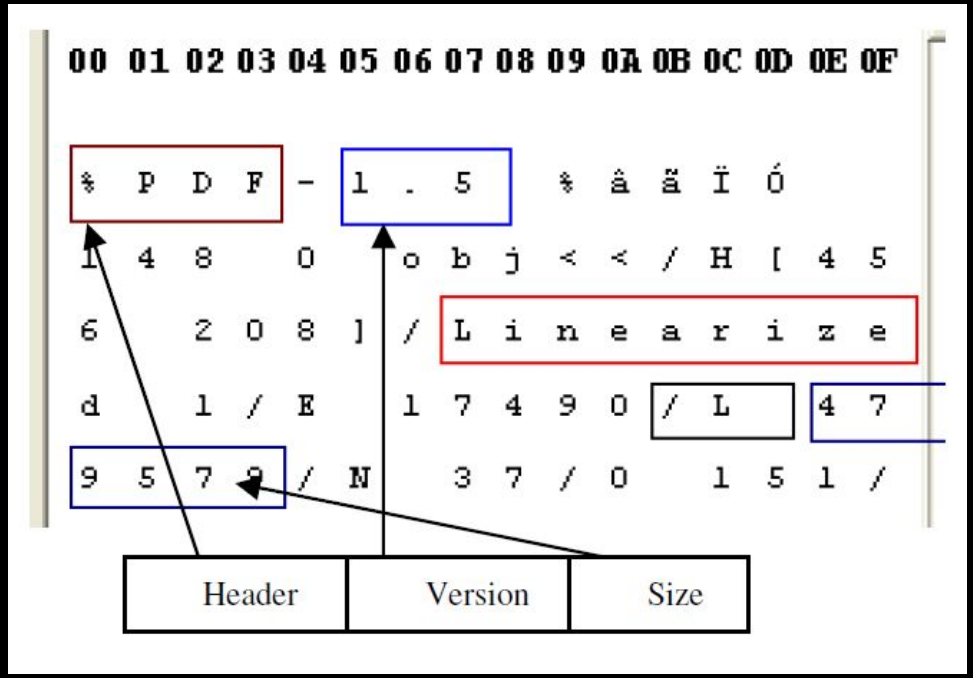
FILE SYSTEM BASICS

- MANY DIFFERENT TYPES OF FILE SYSTEMS
- GENERAL STRUCTURE:
  - FILES ARE STORED AS CLUSTERS ON THE DRIVE
  - MASTER FILE TABLE - CONTAINS THE PHYSICAL LOCATION (CLUSTER) WHERE EACH FILE IS STORED. ALSO CONTAINS METADATA ON EACH FILE
  - ANY UNUSED AREA ON THE DRIVE IS CONSIDERED UNALLOCATED SPACE AND DOES NOT HAVE AN ENTRY ON THE MASTER FILE TABLE



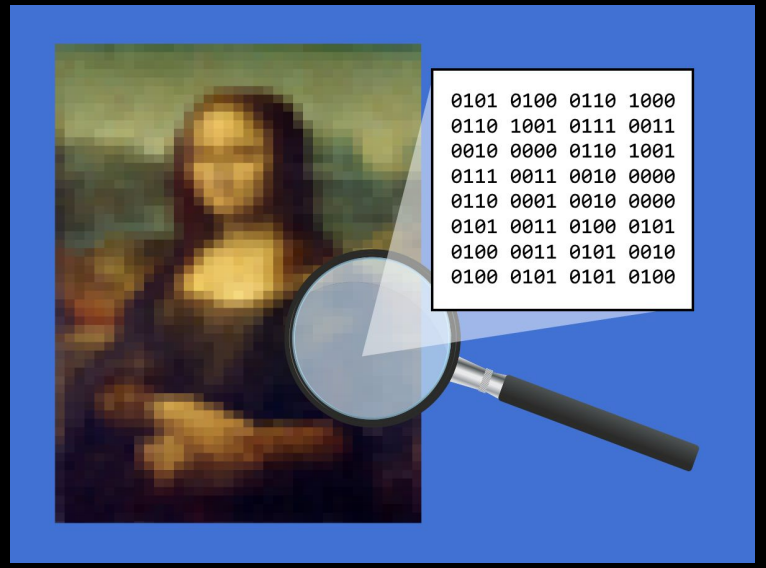
DATA CARVING

- WHEN FILES ARE DELETED FROM A FILE SYSTEM, THE MASTER FILE TABLE ENTRY FOR THAT FILE IS REMOVED, BUT THE FILE ITSELF IS NOT ACTUALLY DELETED
  - THE BITS REMAIN INTACT UNTIL OVERWRITTEN
  - THE FILE SYSTEM JUST NO LONGER KNOWS THAT THE FILE EXISTS
- THESE FILES CAN BE RECOVERED USING DATA CARVING
  - SEARCHES THROUGH UNALLOCATED SPACE FOR RECOGNIZED FILE HEADERS TO REBUILD A LOST FILE



STEGANOGRAPHY

- A METHOD OF HIDING DATA WITHIN OTHER FILES
  - MOST COMMONLY HIDDEN IN MEDIA FILE FORMATS
- DATA IS EMBEDDED INTO THE FILE'S BITS SO THAT THE MEDIA LOOKS THE EXACT SAME AT FACE VALUE
- OFTEN TIMES THE DATA IS ENCODED USING A KEY OR PASSPHRASE TO PROVIDE AN ADDED LEVEL OF SECRECY/SECURITY



LAB PREP

TOOLS YOU WILL BE USING

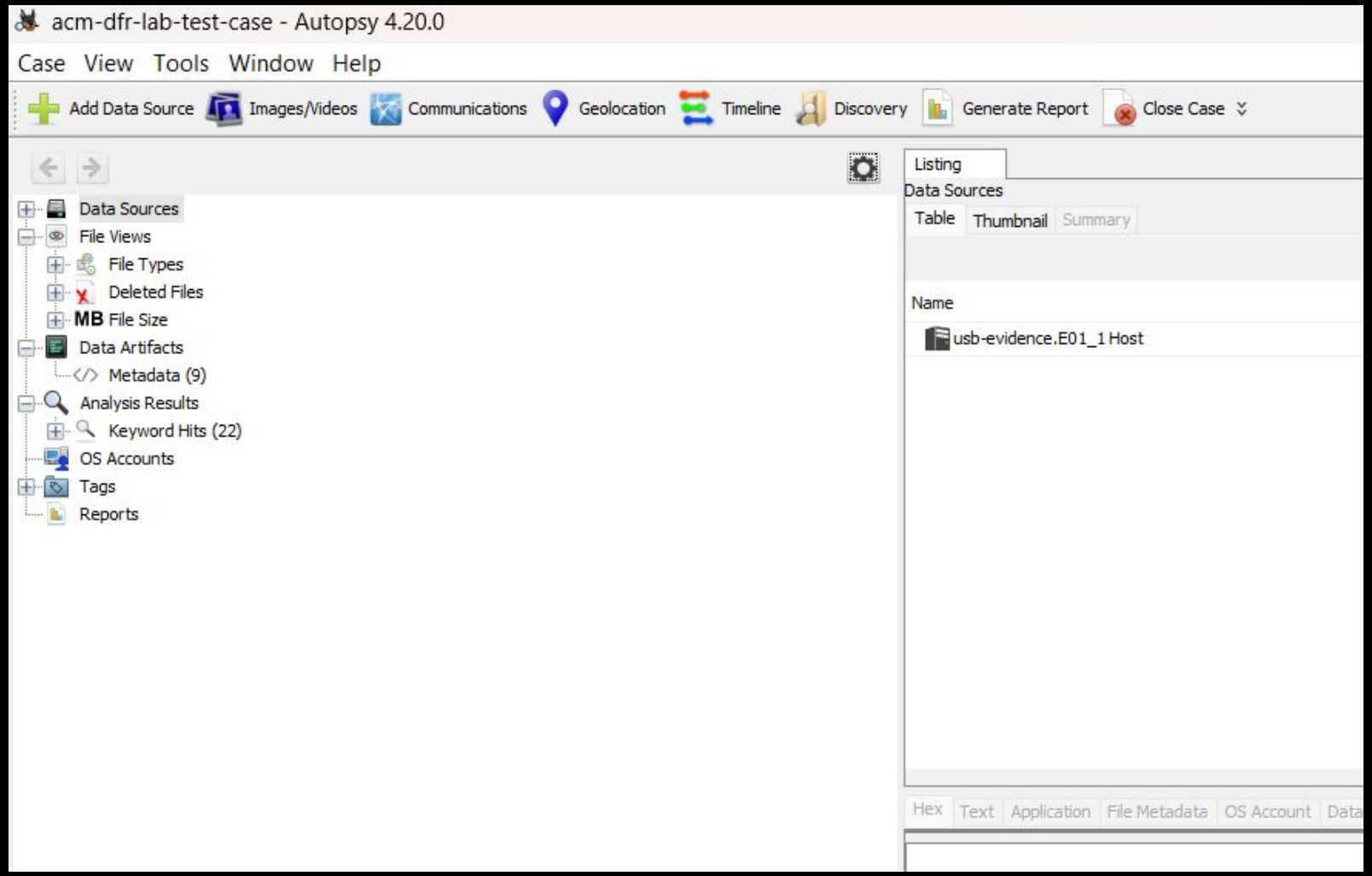
FTK IMAGER

- TOOL USED TO IMAGE A DRIVE INTO VARIOUS DIFFERENT FILE FORMATS
- WE WILL BE IMAGING A USB DRIVE AS AN “E01” FILE

AUTOPSY

- DIGITAL FORENSICS TOOLKIT
- AUTOMATICALLY PERFORMS DATA CARVING
- WE WILL USE THIS FOR THE INVESTIGATION PORTION OF THE LAB

AUTOPSY DASHBOARD



QUICK NOTE ON USB SAFETY

- NEVER PLUG IN A USB DRIVE FROM AN UNTRUSTED SOURCE
- BAD USB DRIVES CAN AUTOMATICALLY DOWNLOAD MALWARE TO YOUR COMPUTER

LAB BRIEFING

SJU ACM

CLUE

A Hack at St. John's

THE HACK

The day is Thursday, October 5. The St. John's ACM Student Chapter club is meeting for its second meeting of the Fall 2023 semester. Upon entering the cyber lab, the club is met with a terrifying discovery: St. John's University has been HACKED! The only piece of evidence left behind by the attacker is a USB drive. St. John's IT was able to estimate that the hack occurred at approximately 12 pm on Thursday, October 5, however, they suspect that a member of the SJU ACM e-board was behind it all. To assist in the investigation, the members of SJU ACM have agreed to examine the contents of the USB drive in hopes of uncovering the true identity of the culprit. It's up to you to figure out who did it, where they did it, and what malware they used.

THE SUSPECTS

RAYMOND RAMDAT

JAKE ENEA

DAVID ROSOFF

TOMAS SANTOS YCIANO

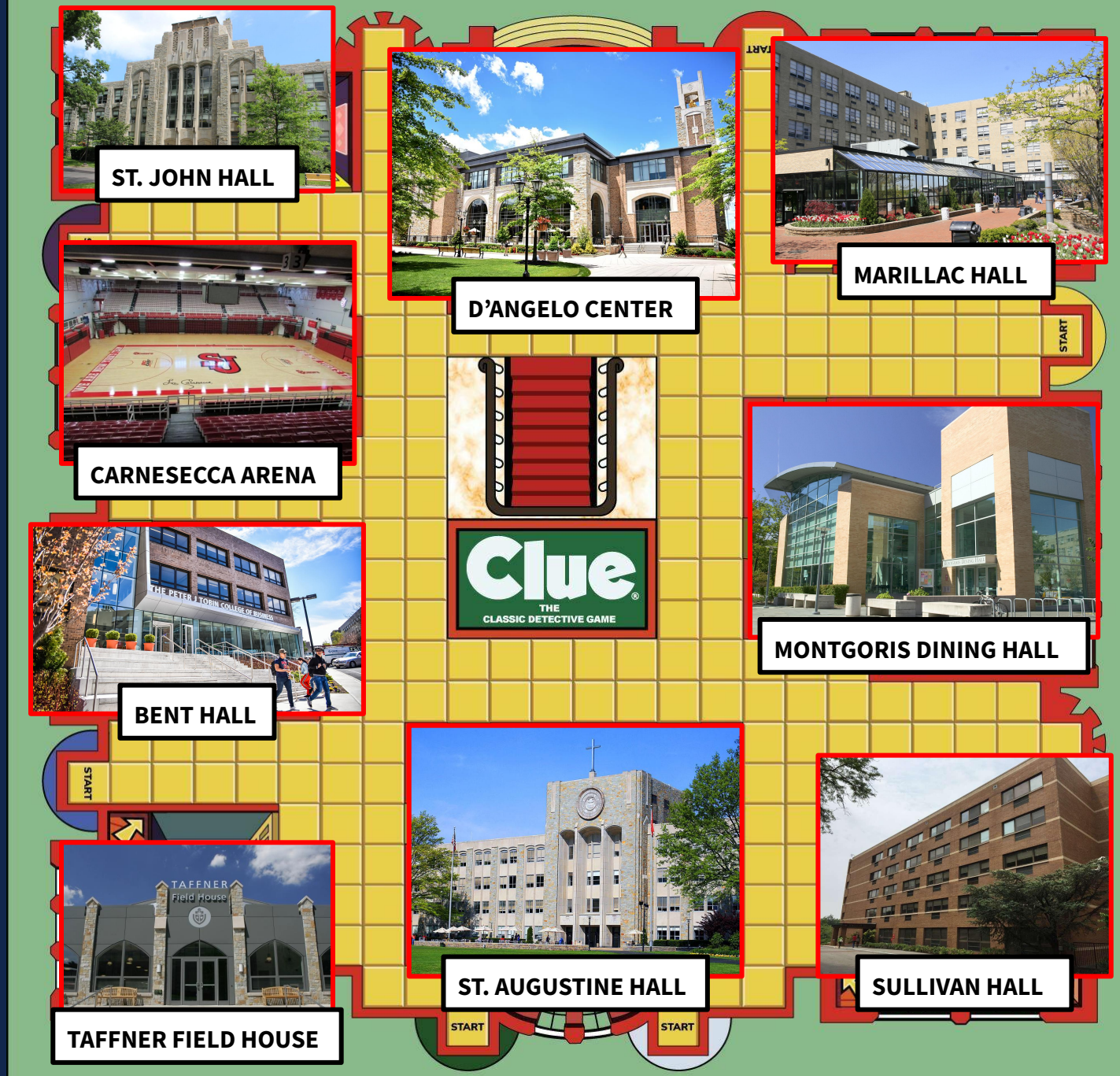
IGNACIO ANTEQUERA SANCHEZ

BEN HANIM

FAIROOZ EHSAN

AQUEENA ALEXANDER

THE BUILDINGS



THE MALWARE

THANK YOU!