Lab 2:

Overview:

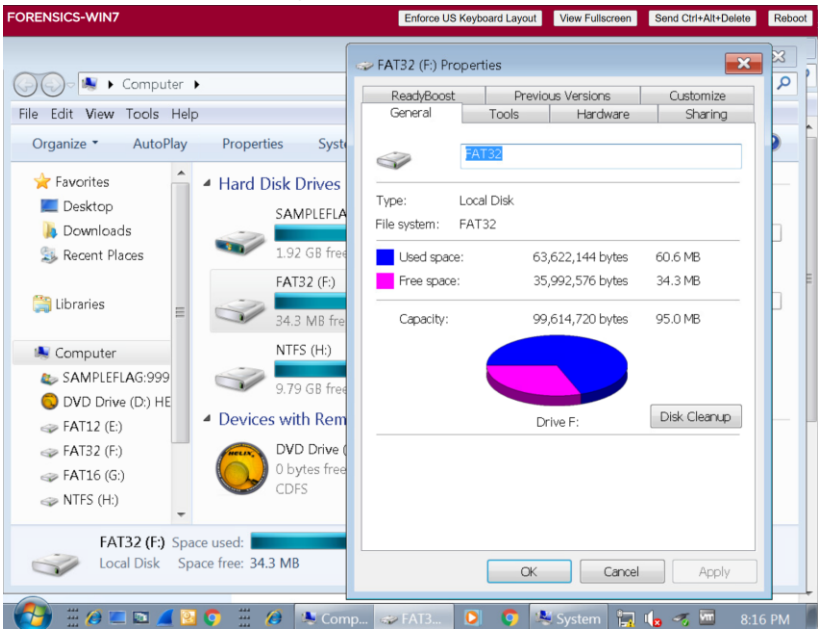
Digital devices store information in RAM, HDDs, or SSDs. This lab investigates different file systems from Windows. These processes are done behind the scenes but it is important for digital forensics to understand these processes. Microsoft operating systems include FAT and NTFS (New Technology File System). There are various versions of FAT with different descriptions. As for NTFS, this offers security whereas FAT is known for compatibility.

Outcomes:

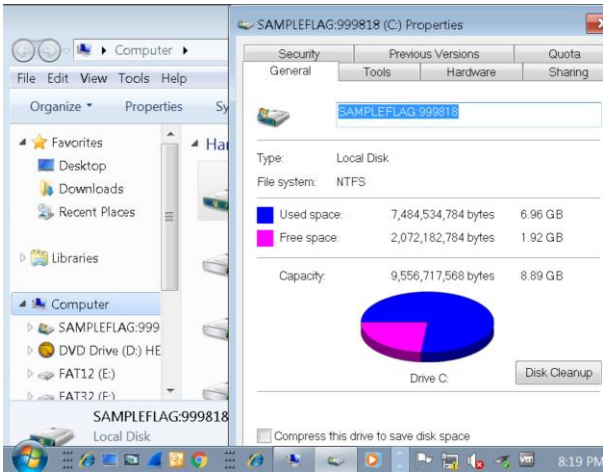
1. Examine FAT and NTFS File Systems
2. Use HEX Editor to explore a FAT partition
3. Verify and view image details
4. Analyze a FAT Partition using Autopsy.

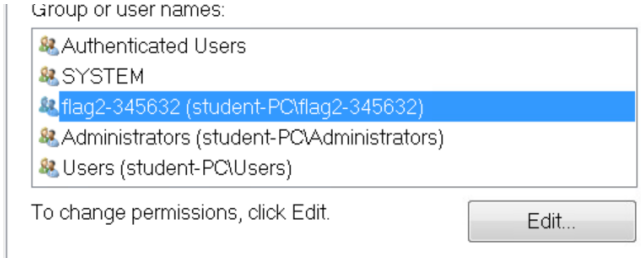
Challenge 1:

- View FAT32 drive's properties
- Does not have a security tab



- Asked to view SAMPLEFLAG Drive
    - File system of NTFS

- 

  - Mentions that security permissions and quotas can be configured to restrict access. Quotas restrict amount of storage for each user to prevent a disk from running out of space.
- 

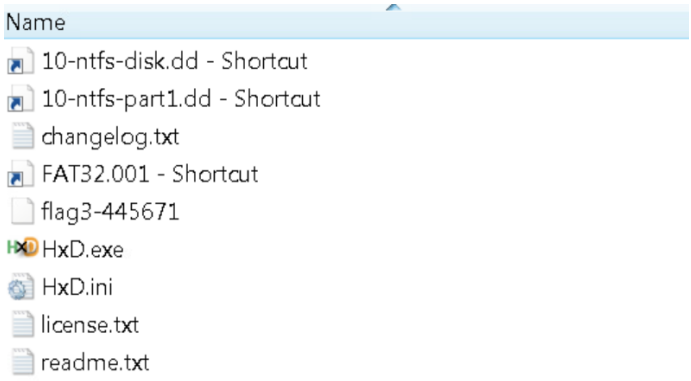
  - Viewing a user with a flag challenge.
- 

  - Converting drive F: to NTFS.
    - Allows for security and quotas
  - Required to change the name of F: from “FAT32” to “NTFS”

Using a HEX Editor to explore FAT Partitions:

- Notes
  - FAT is a legacy file system designed in the late 70s for use with floppy disks. It was adapted on hard disks and used greatly during heyday of DOS and Windows 9X OS. FAT is still used today.

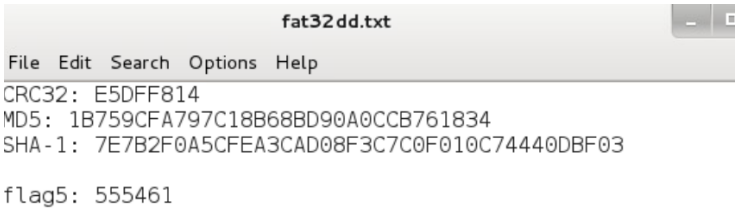
- Steps
    - Opened the available hex editor and am opening a disk image.
        - Displays a challenge flag.



        -
    - Open FAT32001 shortcut
        - Examine HEX and the first 446 bytes which is the Boot Code
        - Change offset to dev
        - First fyte is the bootable flag of 80 (boot partition)
        - Four bytes after is a FAT32 partititon set to LBA mode addressing
        - Find MBR

Verifying and Viewing Image Details:

- Kali Linux Box
    - Switch to forensics directory
    - Cat flag4.txt
    - View fat32dd.txt for hash info



        -
        - Now cat it and pipe MD5 using grep.
        - Use md5sum command on .dd file to match hashes
            - Repeated with sha1sum
- Conclusion
    - Incident responders will generate text files with image hash values with other info such as CRC.

Analyzing FAT Partitions using Autopsy.

- Overview

- Forensic analysis requires loading image files into tools. Autopsy is Open Source.
- Honestly, it just took me through a series of steps to use Autopsy. Allowed for me to use file analysis and analyze the image as a whole.