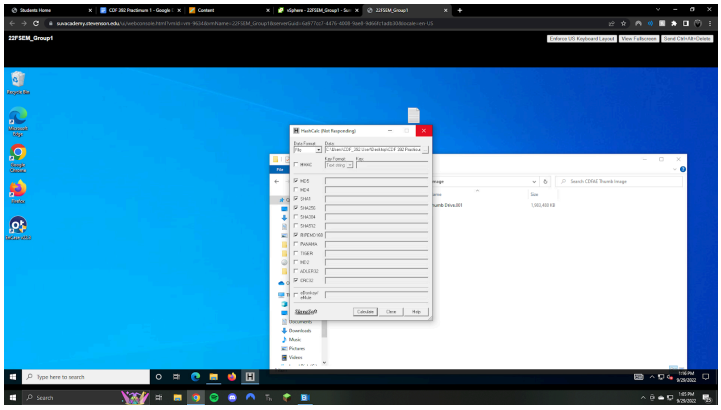
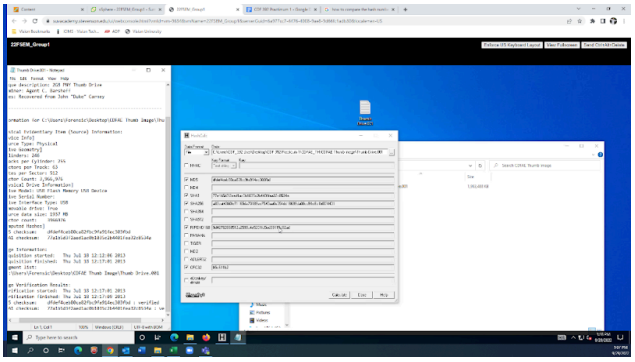
Matthew Sponaugle
Iyadunni Adegboye
Keziah Rogers

Practicum 1 Exercises

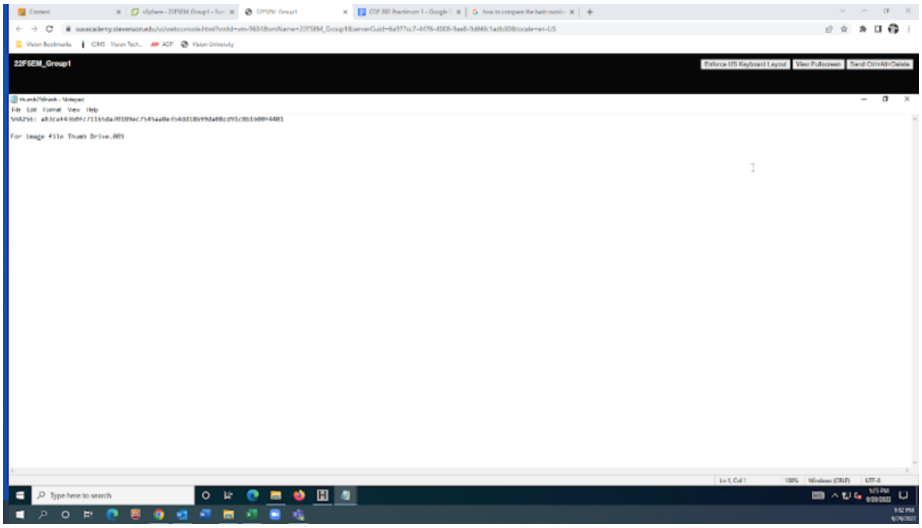
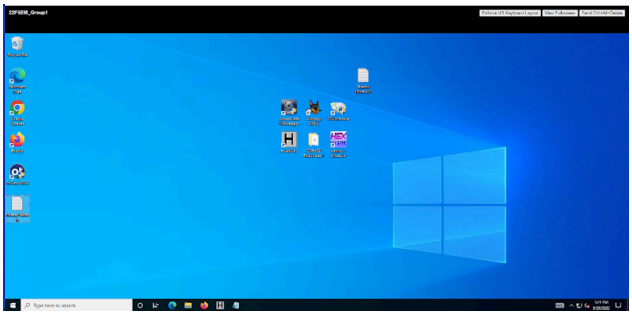
Team Tasks and Questions:

- Compare the hash number of the project hard disk image with the enclosed imaging report
    - 1) First, we opened the CDF 392 Practimum folder
    - 2) We then clicked the CDFAE Thumb Image folder
    - 3) Then we clicked the original image file (Thumb Drive.001) and opened Hash Calc
    - 4) After, we clicked the three dots by data and opened the Thumb Drive.001 drive.
    - 5) We clicked SHA-256 and calculated the hash.

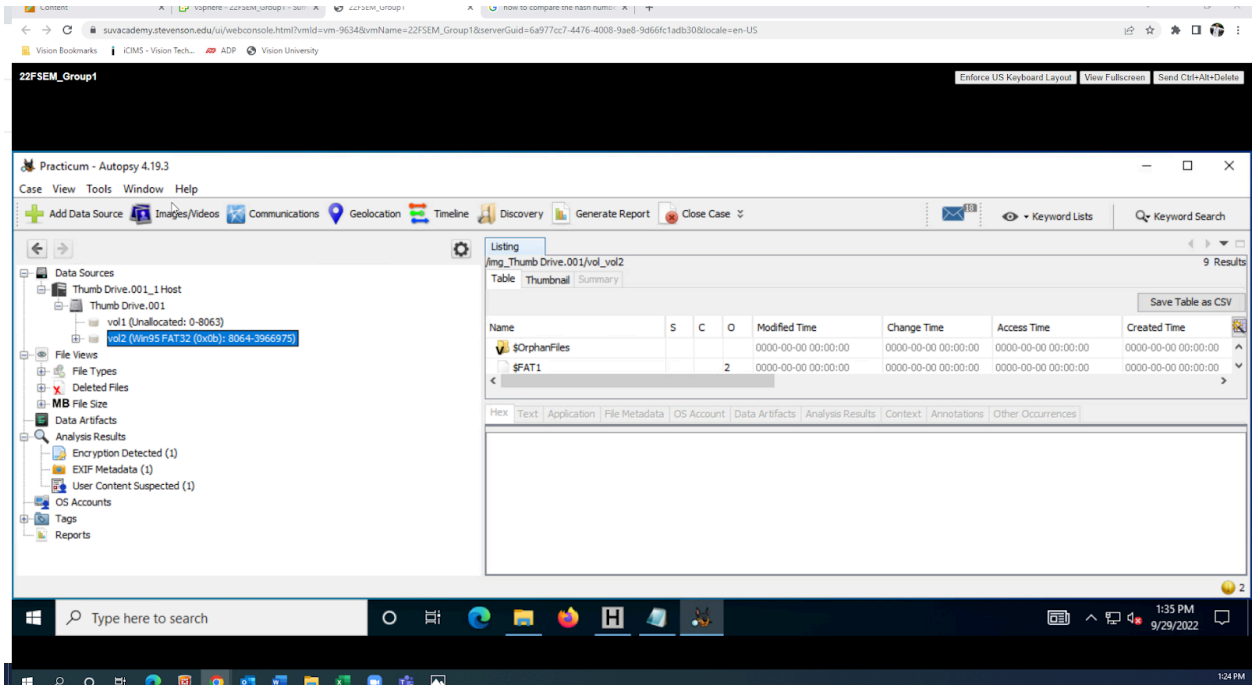


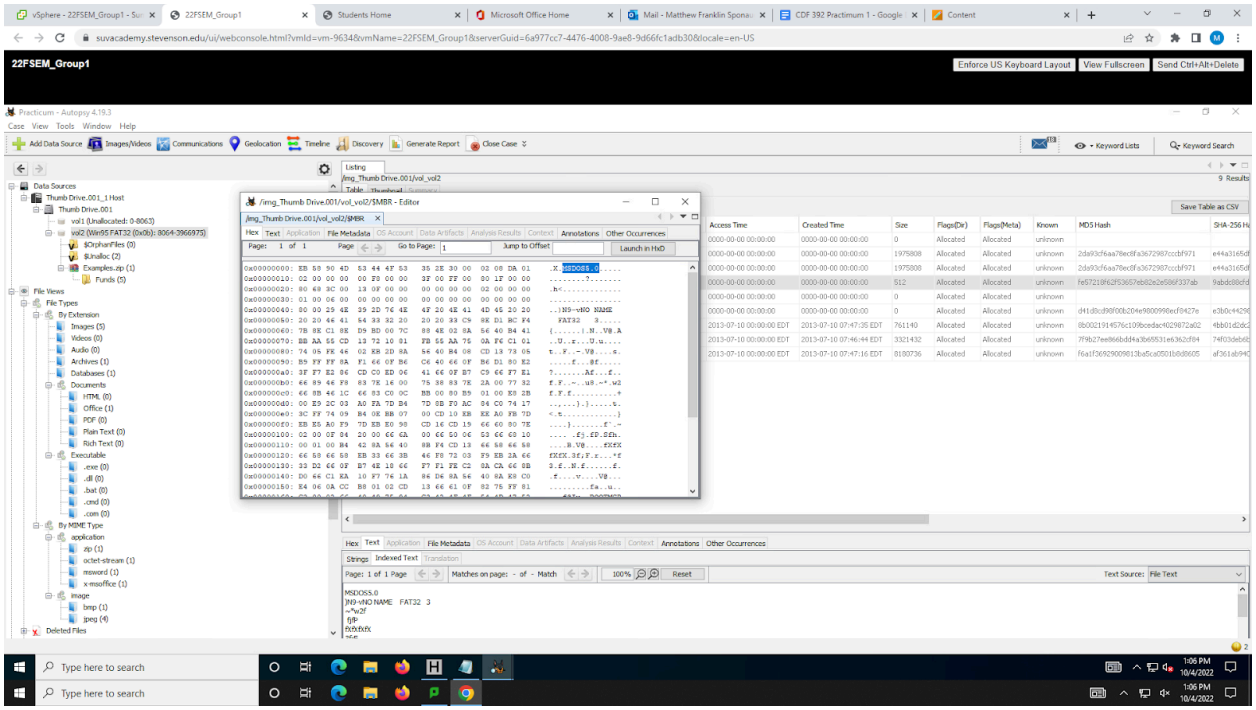


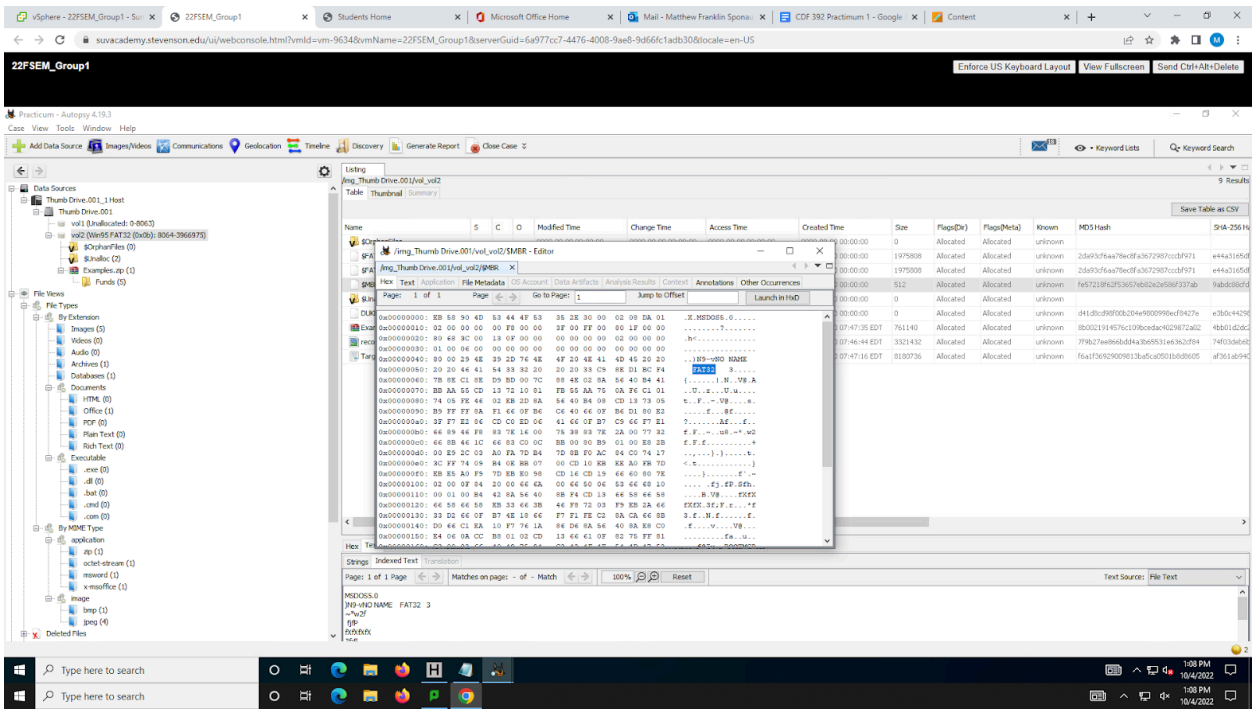
- (They are the same)
- Create a SHA 2 hash value for the image file.

- 
- Download all additional software including the additional file image file.
  - 
- Install by of each software packaging by it running on the VM.
  -
- What OS and version are on the disk? (When was it installed?)
- **Windows 95 which contains MS DOS 5.0. The file system is FAT 32. We could not find the exact date when it was installed, because there is no registry hives or Master File Table on**

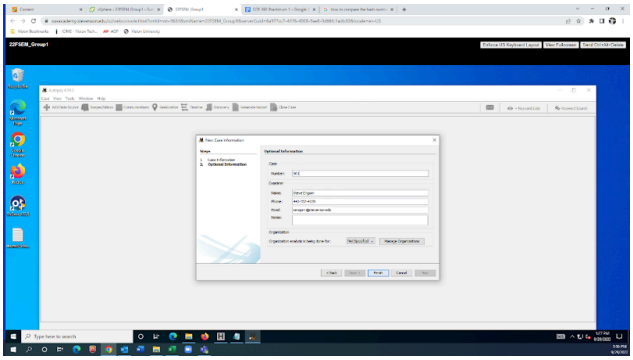
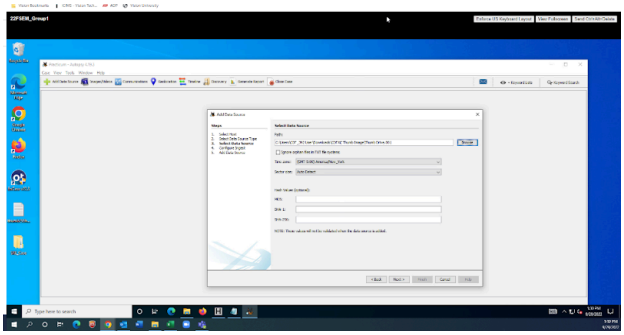
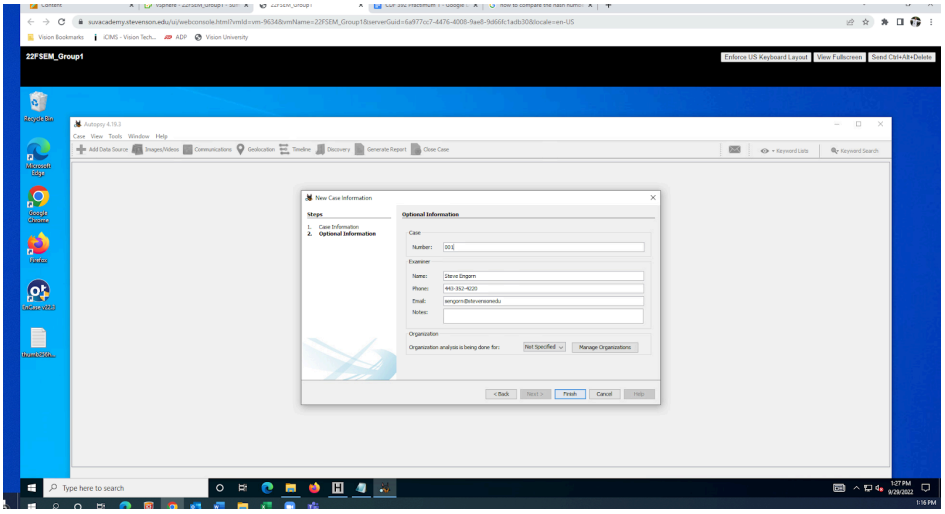
the disk.


22FSEM_Group1
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Practicum - Autopsy 4.19.3
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Data Sources
Thumb Drive.001_1 Host
Thumb Drive.001
vol1 (Unallocated: 0-8063)
vol2 (Win95 FAT32 (0x0b): 8064-3966975)
File Views
File Types
Deleted Files
MB File Size
Data Artifacts
Analysis Results
Encryption Detected (1)
EXIF Metadata (1)
User Content Suspected (1)
OS Accounts
Tags
Reports
Listing
/img_Thumb Drive.001/vol_vol2
9 Results
Table
Thumbnail
Summary
Save Table as CSV
Name
S
C
O
Modified Time
Change Time
Access Time
Created Time
$OrphanFiles
$FAT1
0000-00-00 00:00:00
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Type here to search
1:35 PM
9/29/2022
1:24 PM

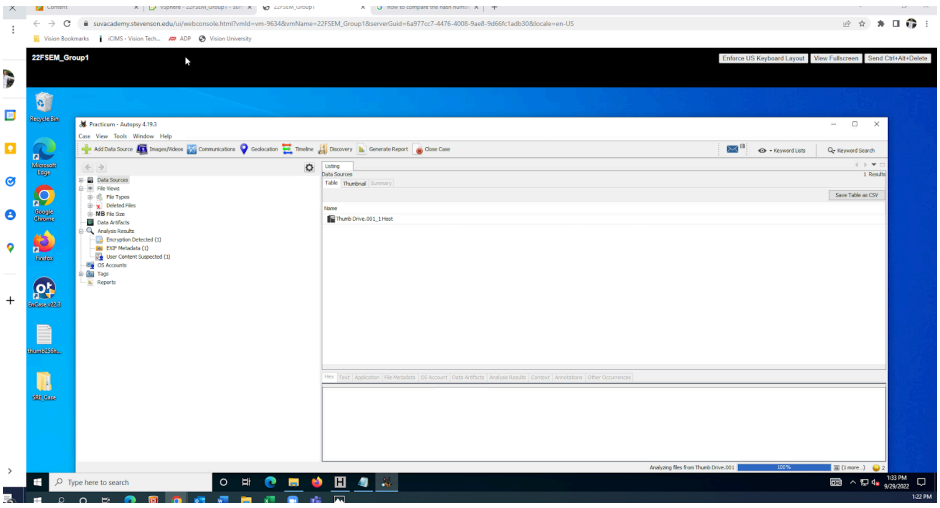




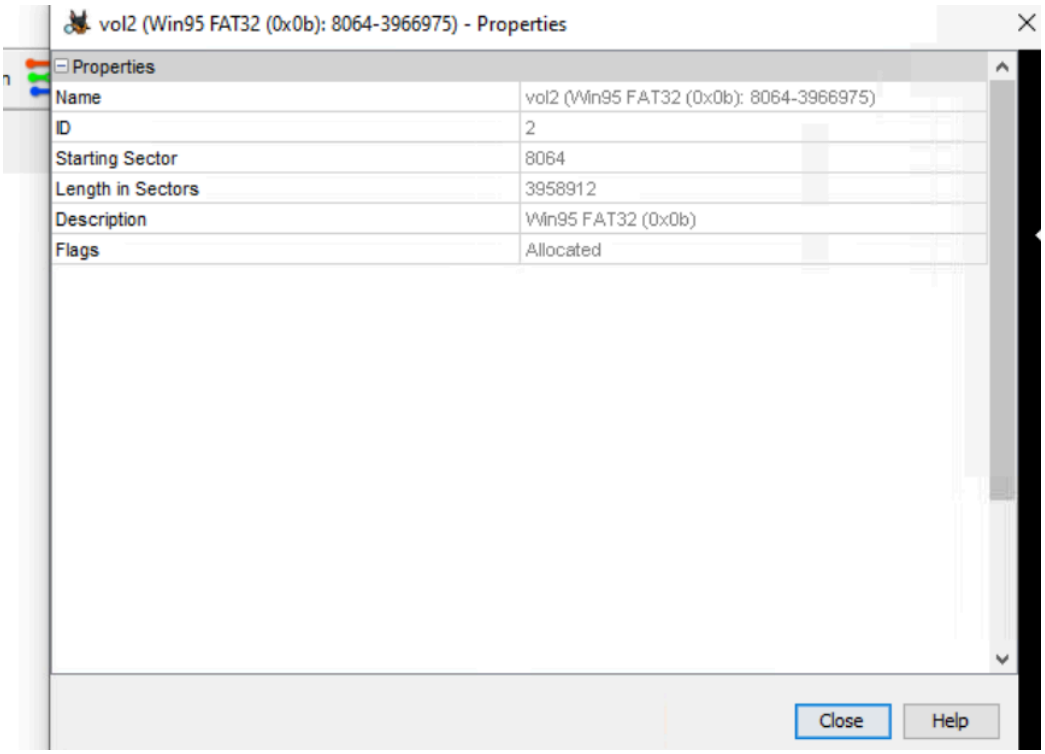
- 1) We opened Autopsy
- 2) New case information window

- 3) 
- 4) The case could not be created at first due to not saving in a valid location
- 5) We selected the host, disk image, and the data source is the thumb drive.
- 
- 

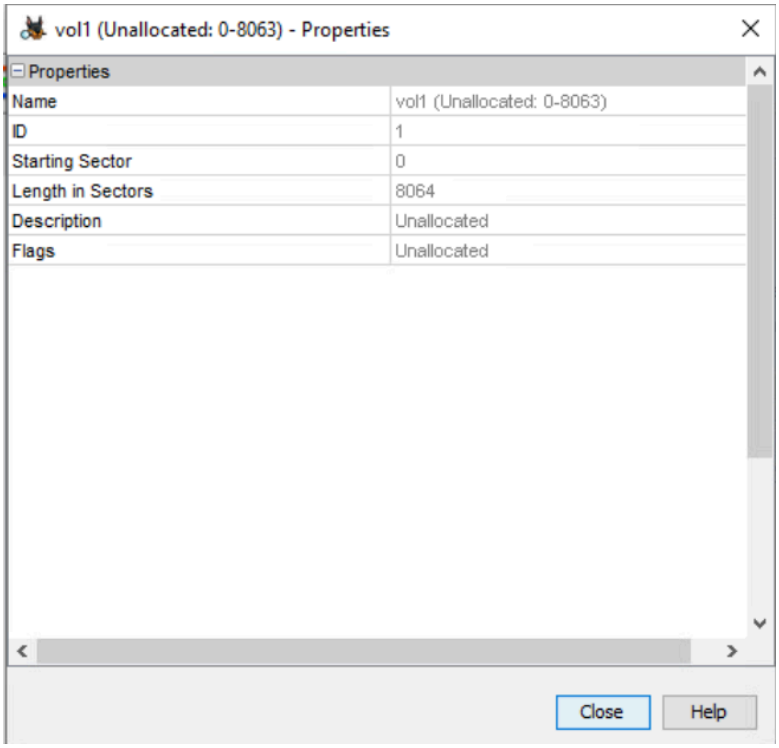
- Data source was added successfully-



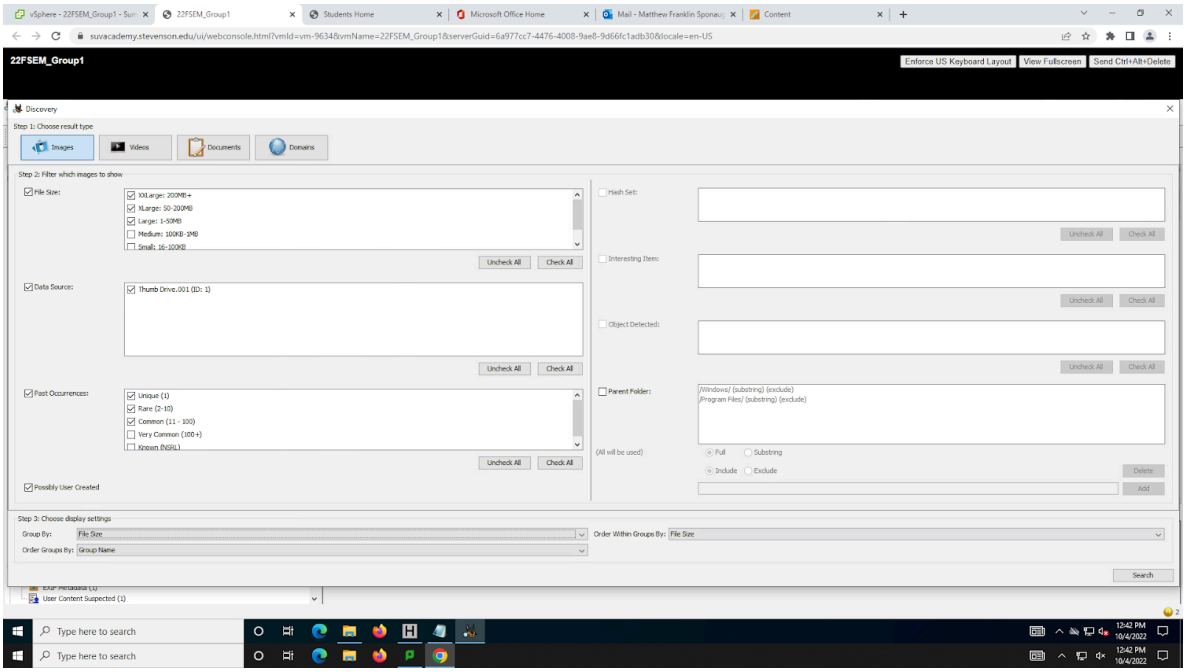
- Can you identify how many volumes are on the disk? (Include sector information)
  - **2 volumes are on the disk.**

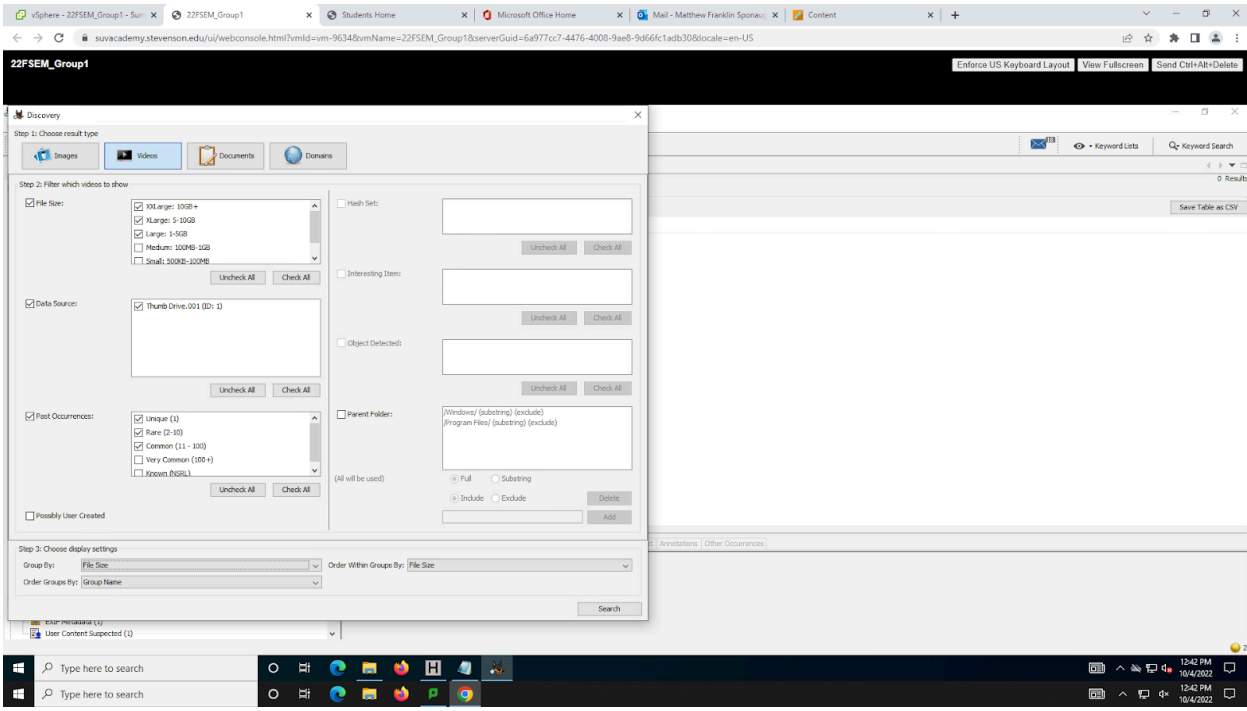


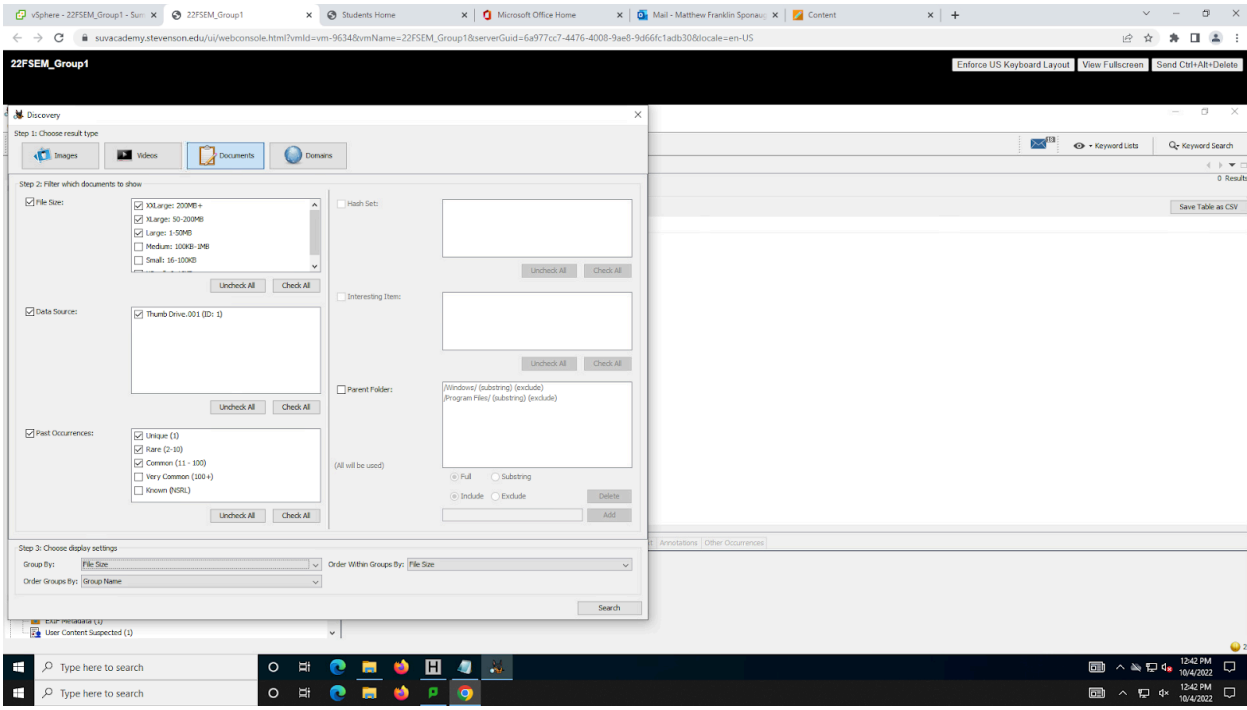
- **Unallocated-**

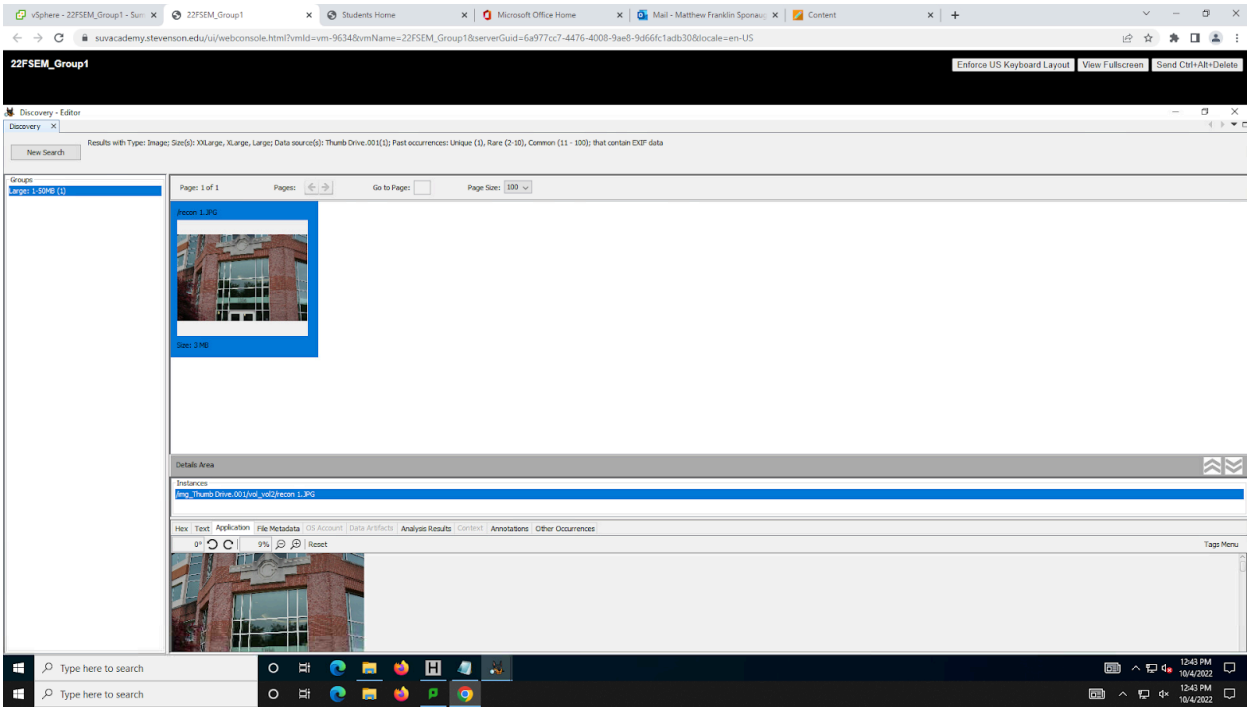


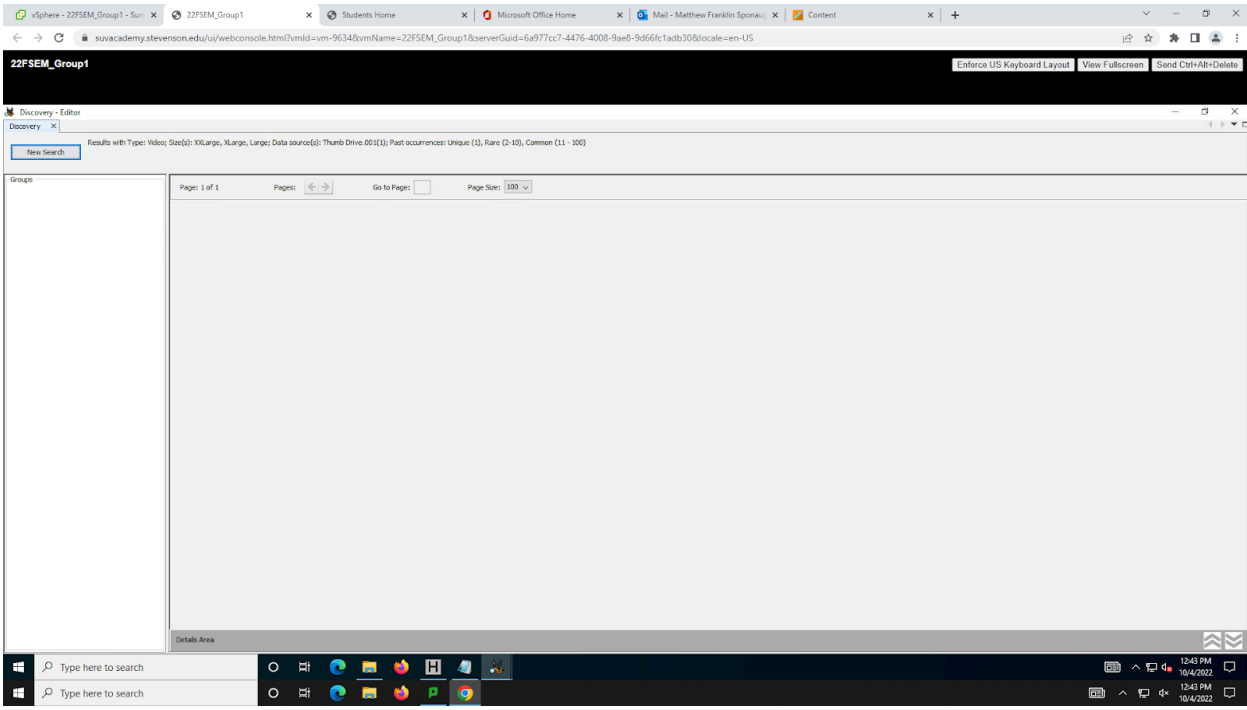
- How many files larger than one gig are there on the disk? (What are their names?)
    - None, no files appear larger than 8mb

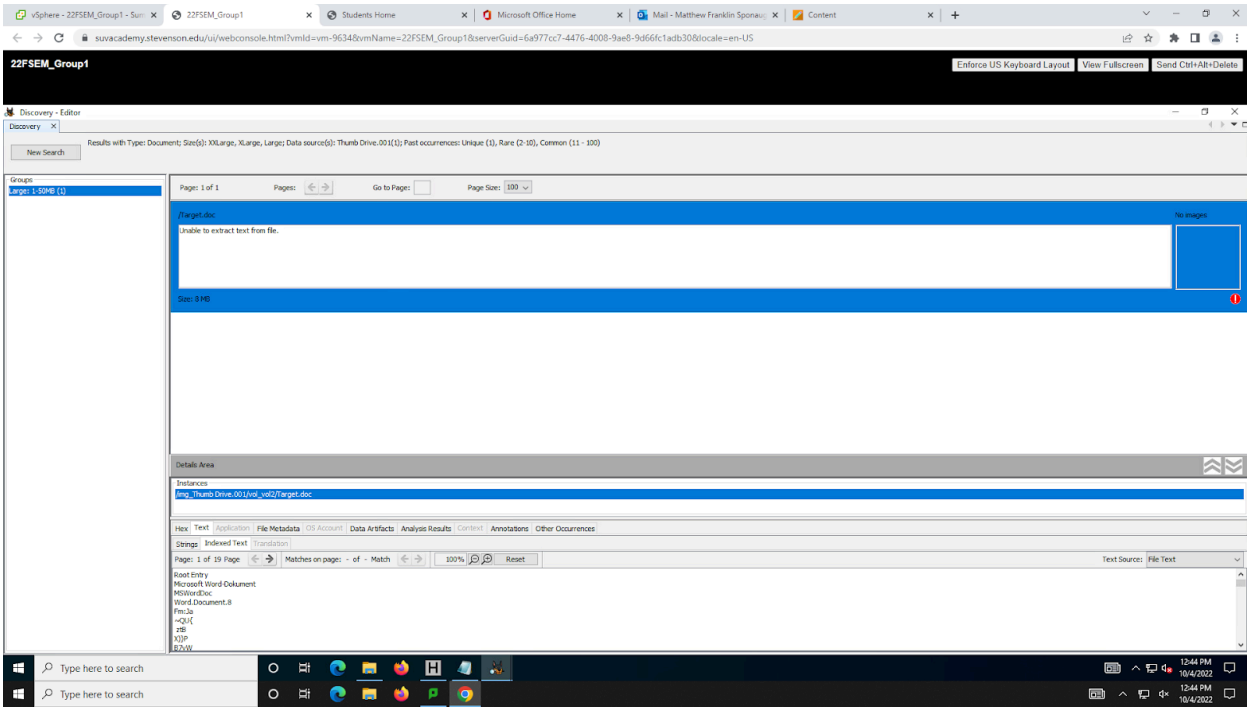

22FSEM_Group1
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Discovery
Step 1: Choose result type
Images
Videos
Documents
Domains
Step 2: Filter which images to show
File Size:
XXLarge: 200MB+
XLarge: 50-200MB
Large: 1-50MB
Medium: 100KB-1MB
Small: 16-100KB
Uncheck All
Check All
Data Source:
Thumb Drive.001 (ID: 1)
Past Occurrences:
Unique (1)
Rare (2-10)
Common (11 - 100)
Very Common (100+)
Known (NSRL)
Possibly User Created
Hash Set:
Interesting Item:
Object Detected:
Parent Folder:
/Windows/ (substring) (exclude)
/Program Files/ (substring) (exclude)
(All will be used)
Full
Substring
Include
Exclude
Delete
Add
Step 3: Choose display settings
Group By:
File Size
Order Within Groups By:
Order Groups By:
Group Name
Search
User Content Suspected (1)
Type here to search
12:42 PM
10/4/2022


22FSEM_Group1
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Discovery
Step 1: Choose result type
Images
Videos
Documents
Domains
Step 2: Filter which videos to show
File Size:
XXLarge: 10GB+
XLarge: 5-10GB
Large: 1-5GB
Medium: 100MB-1GB
Small: 500KB-100MB
Uncheck All
Check All
Data Source:
Thumb Drive.001 (ID: 1)
Past Occurrences:
Unique (1)
Rare (2-10)
Common (11 - 100)
Very Common (100+)
Known (NSRL)
Possibly User Created
Hash Set:
Interesting Item:
Object Detected:
Parent Folder:
/Windows/ (substring) (exclude)
/Program Files/ (substring) (exclude)
(All will be used)
Full
Substring
Include
Exclude
Delete
Add
Step 3: Choose display settings
Group By:
File Size
Order Within Groups By:
Order Groups By:
Group Name
Search
User Content Suspected (1)
Keyword Lists
Keyword Search
Save Table as CSV
Type here to search
12:42 PM
10/4/2022

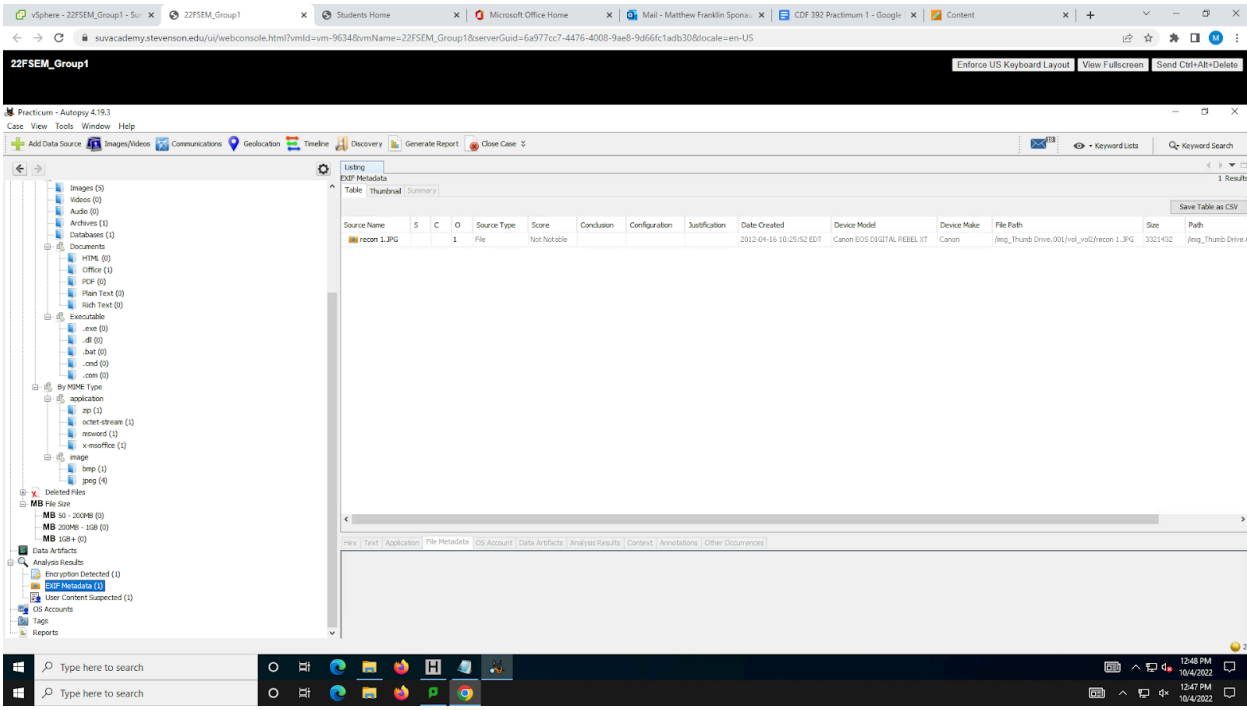

22FSEM_Group1
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Discovery
Step 1: Choose result type
Images
Videos
Documents
Domains
Step 2: Filter which documents to show
File Size:
XXLarge: 200MB+
XLarge: 50-200MB
Large: 1-50MB
Medium: 100KB-1MB
Small: 16-100KB
Uncheck All
Check All
Data Source:
Thumb Drive.001 (ID: 1)
Past Occurrences:
Unique (1)
Rare (2-10)
Common (11 - 100)
Very Common (100+)
Known (NSRL)
Hash Set:
Interesting Item:
Parent Folder:
/Windows/ (substring) (exclude)
/Program Files/ (substring) (exclude)
(All will be used)
Full
Substring
Include
Exclude
Delete
Add
Step 3: Choose display settings
Group By:
File Size
Order Groups By:
Group Name
Order Within Groups By:
Search
Keyword Lists
Keyword Search
Save Table as CSV
Annotations
Other Occurrences
User Content Suspected (1)
Type here to search
12:42 PM
10/4/2022

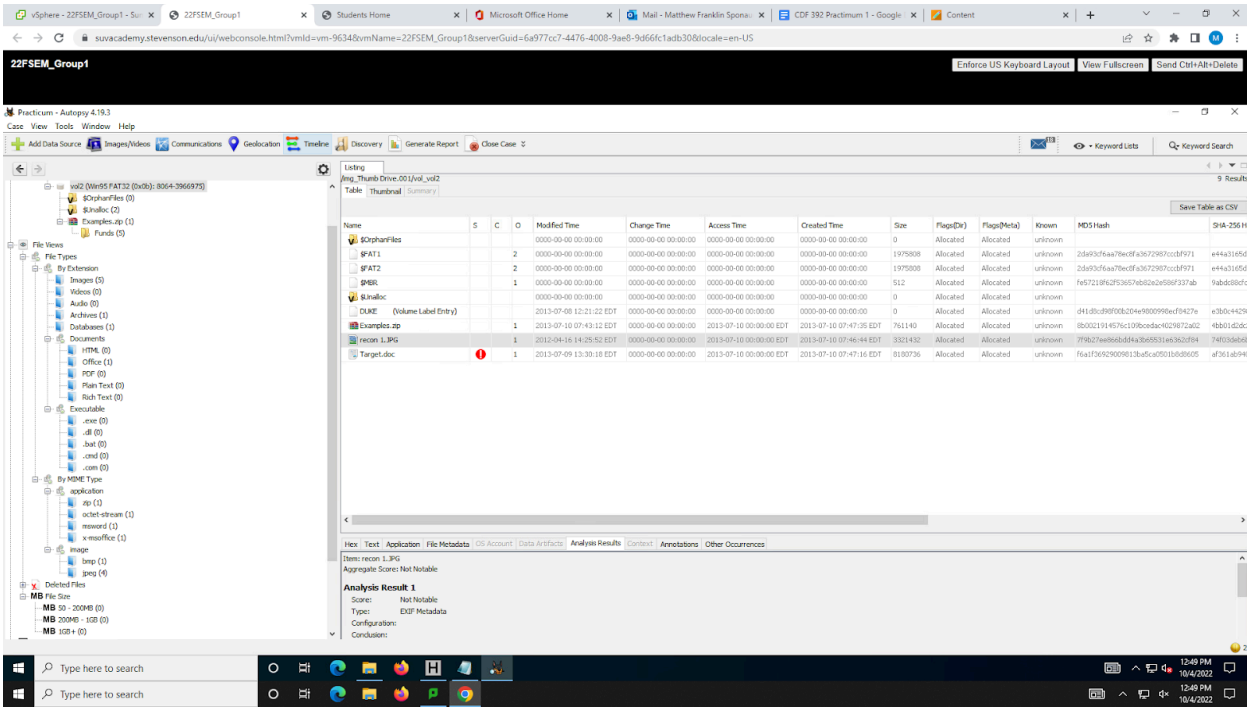

22FSEM_Group1
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Discovery - Editor
Discovery
New Search
Results with Type: Image; Size(s): XXLarge, XLarge, Large; Data source(s): Thumb Drive.001(1); Past occurrences: Unique (1), Rare (2-10), Common (11 - 100); that contain EXIF data
Groups
Large: 1-50MB (1)
Page: 1 of 1
Pages:
Go to Page:
Page Size: 100
recon-1.JPG
Size: 3 MB
Details Area
Instances
/img_Thumb Drive.001/vol_vol2/recon-1.JPG
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Reset
Tags Menu
Type here to search
12:43 PM
10/4/2022



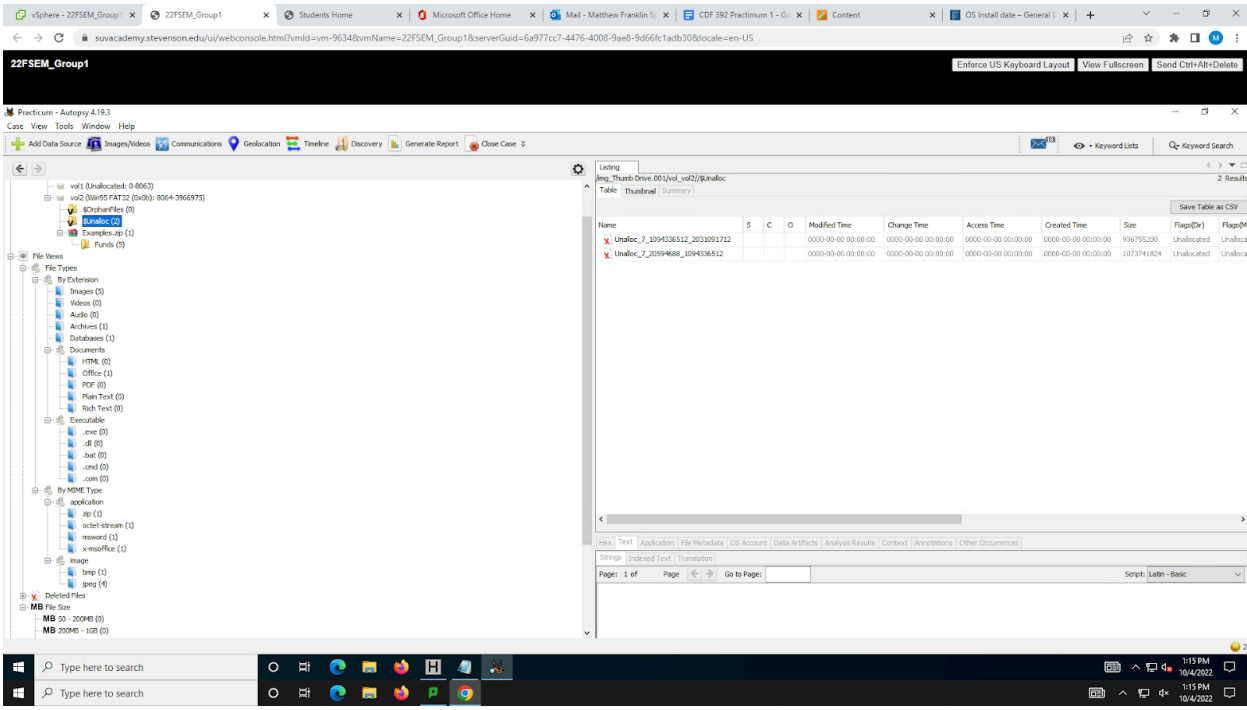


- How many files that possess EXIF data are on the disk? (please identify)
    - Only 1 file which is recon1.jpg.



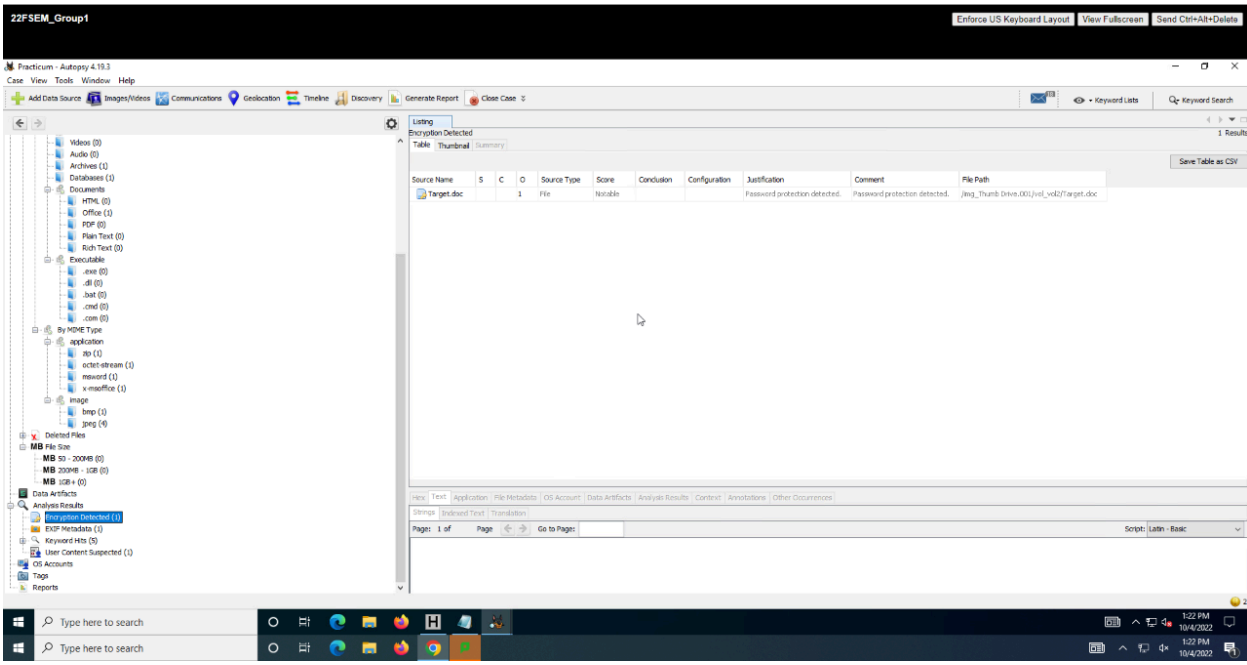


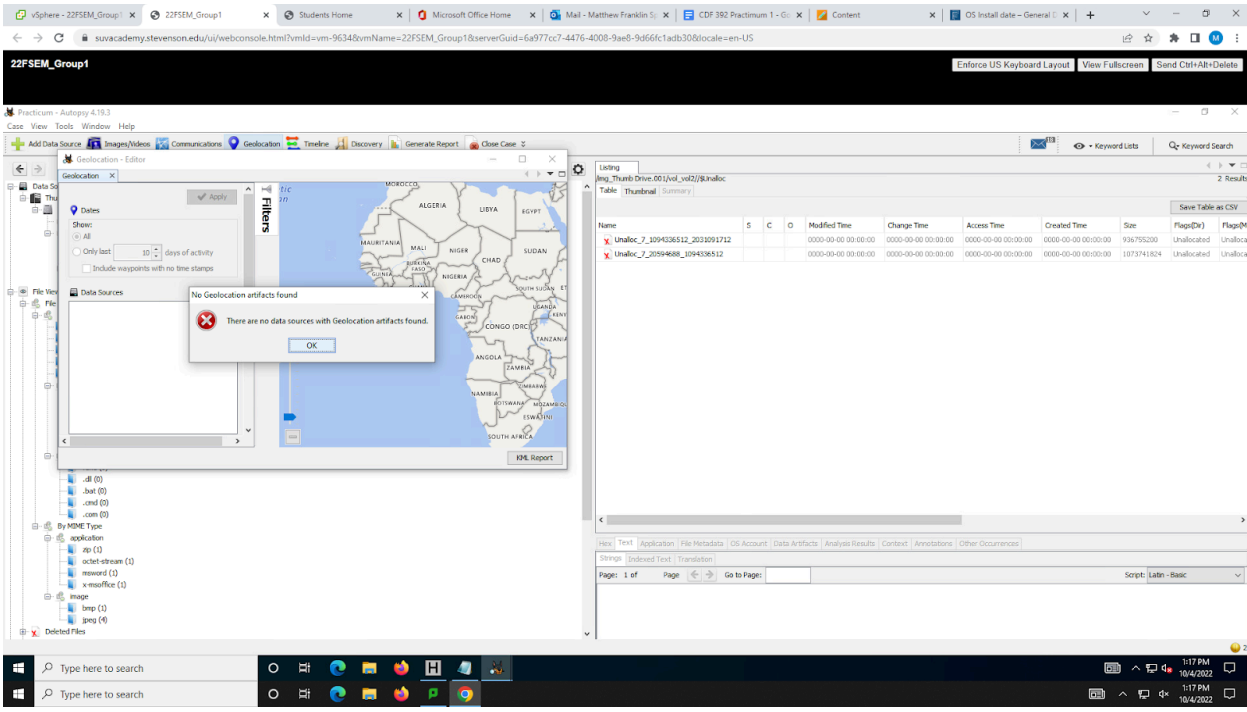
- What version of Adobe Flash Player is installed?



- There is no version of Adobe Flash Player installed. An easy way to tell is there are no executable files present on the disk, which Adobe Flash Player is.

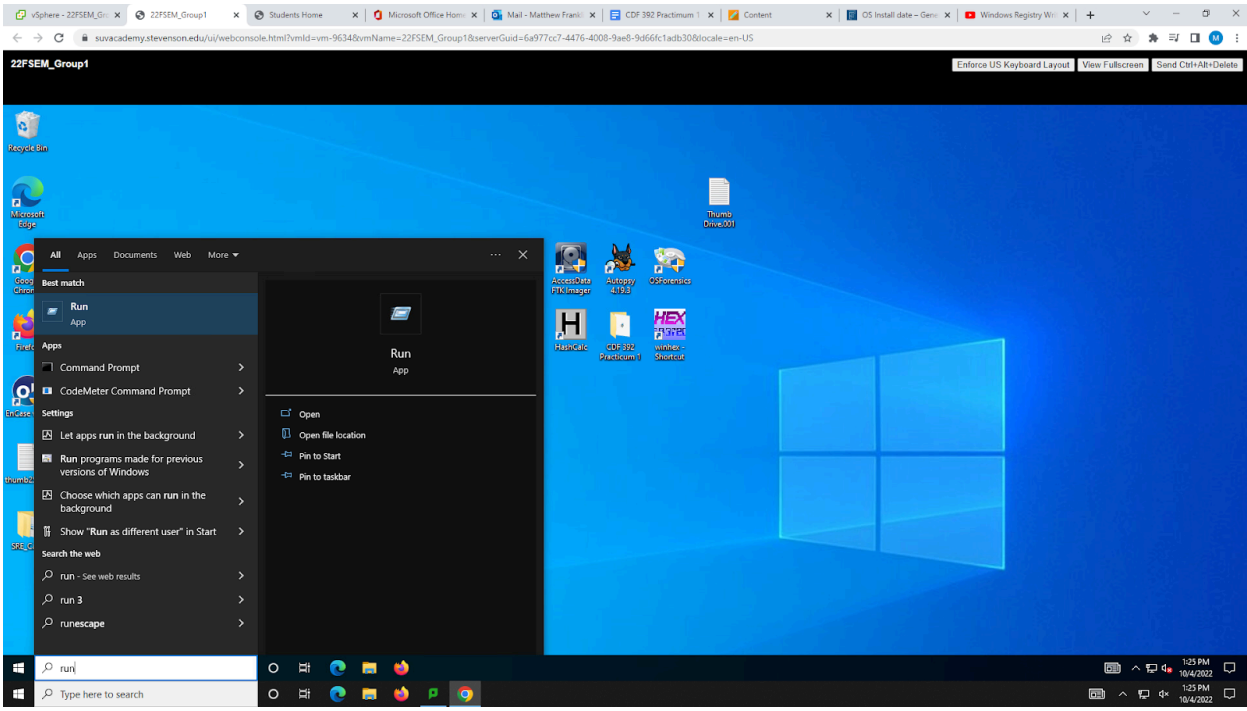
- How many video files are on the drive?
  - **There are 0 on the drive.**
- Are there any password-protected files on the hard drive?
  - **We found one password-protected file called “Target.doc” located in the “/img_Thumb Drive.001/vol_vol2/Target.doc”**

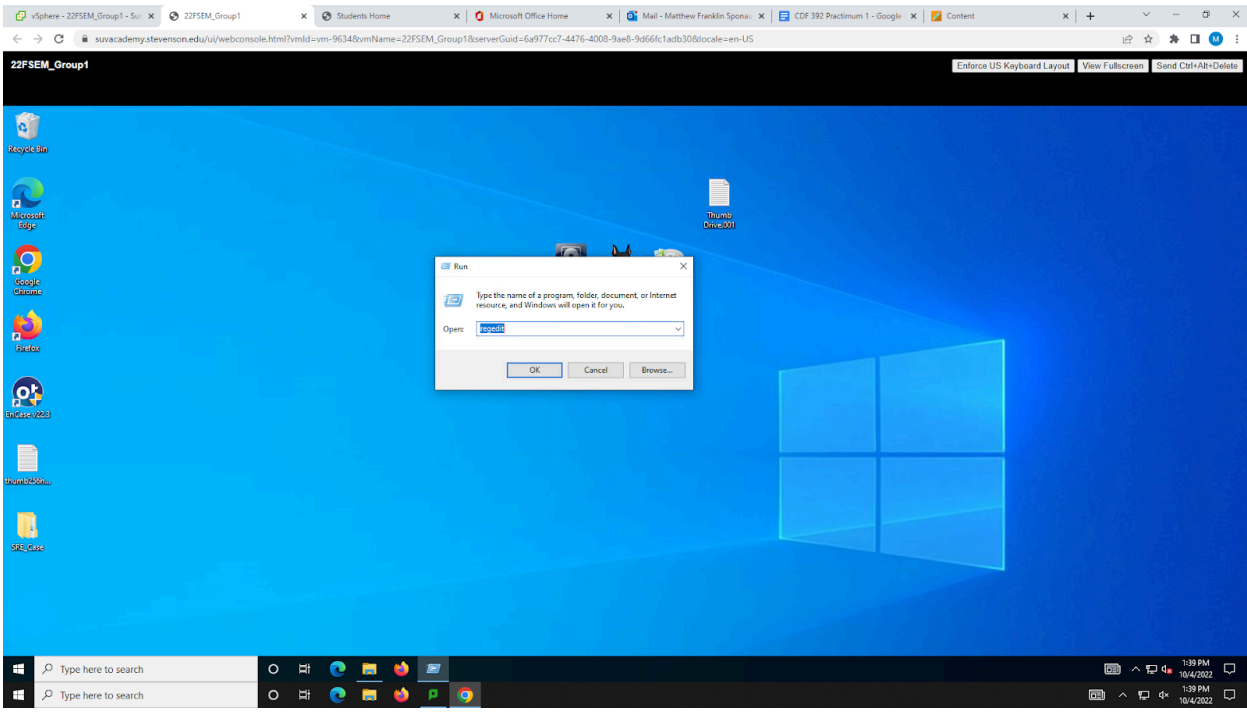


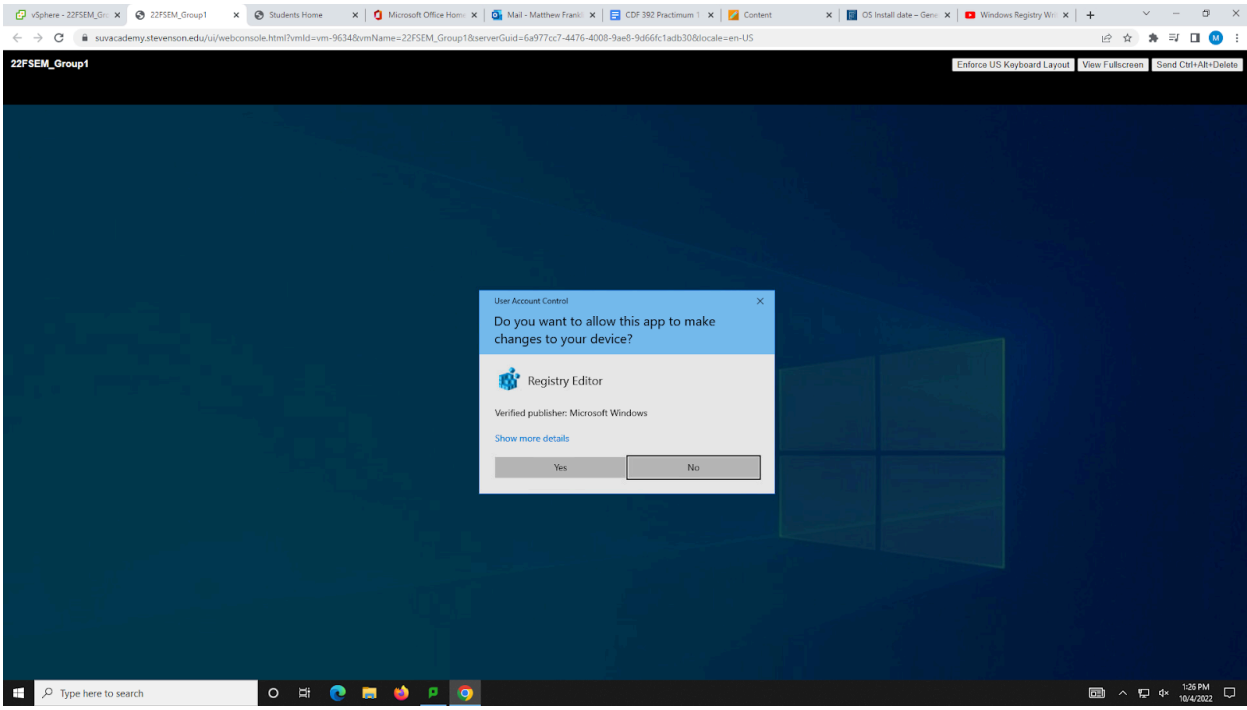
- Is there any Geolocation on the disk?
    - No files contain geolocation data.
    - 

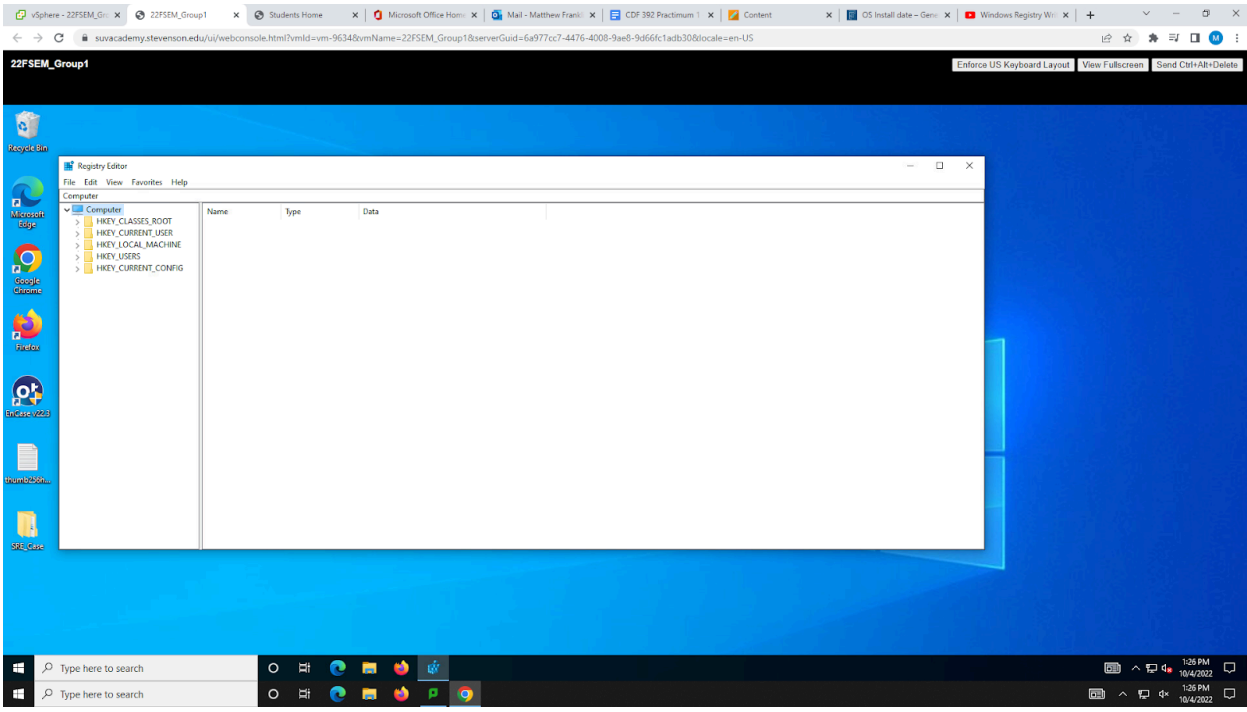
- Do this last:
    - Edit the Windows registry to enable and disable write blocking as shown in the FTK Imager video.

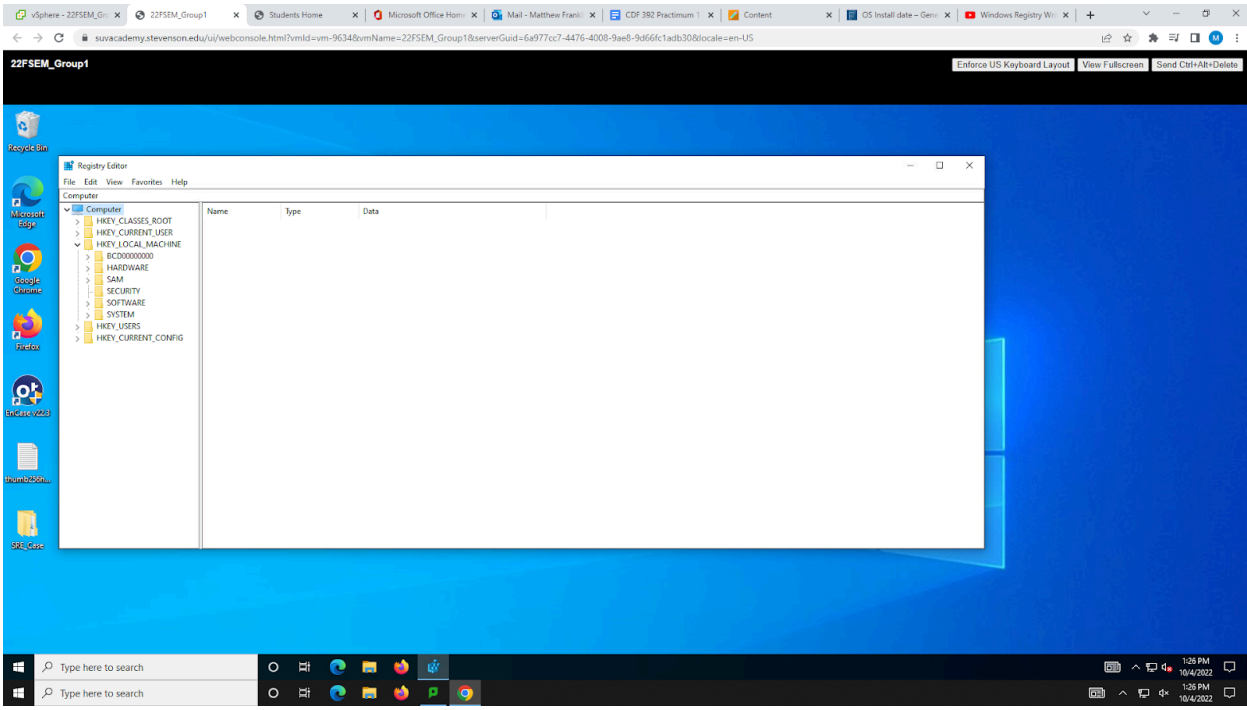
- Include screen captures demonstrating the ability to turn off and turn on write blocking.

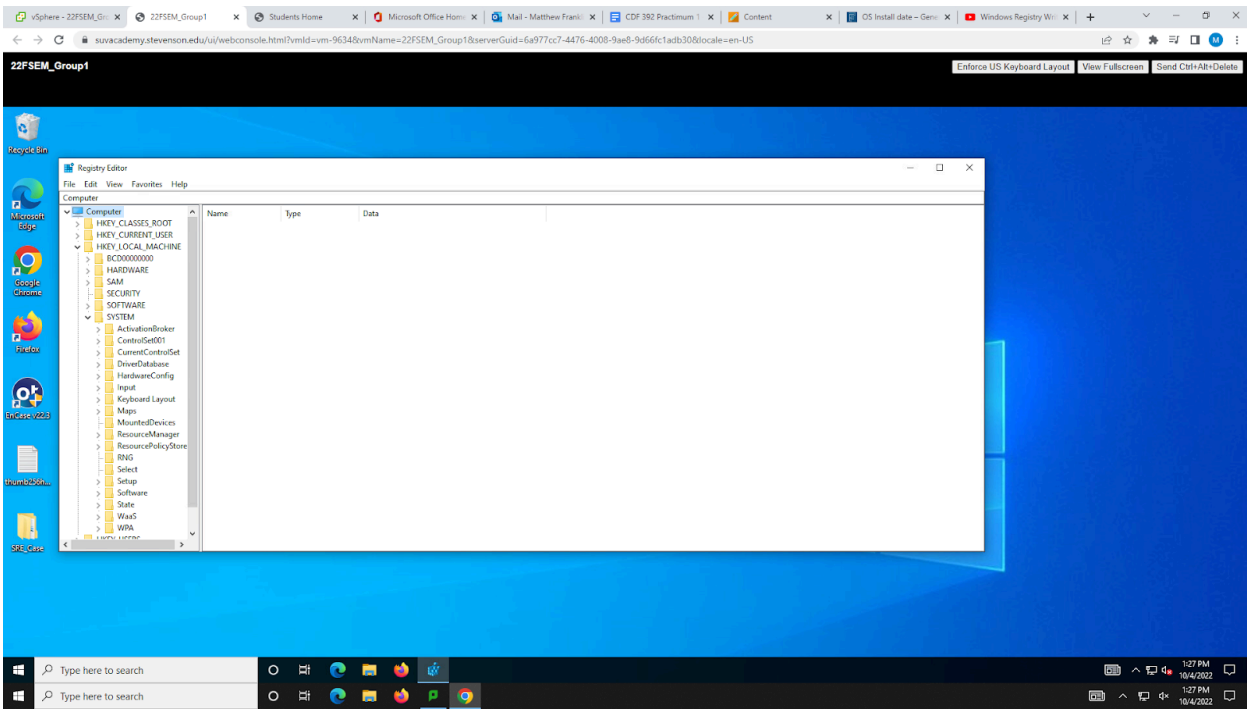


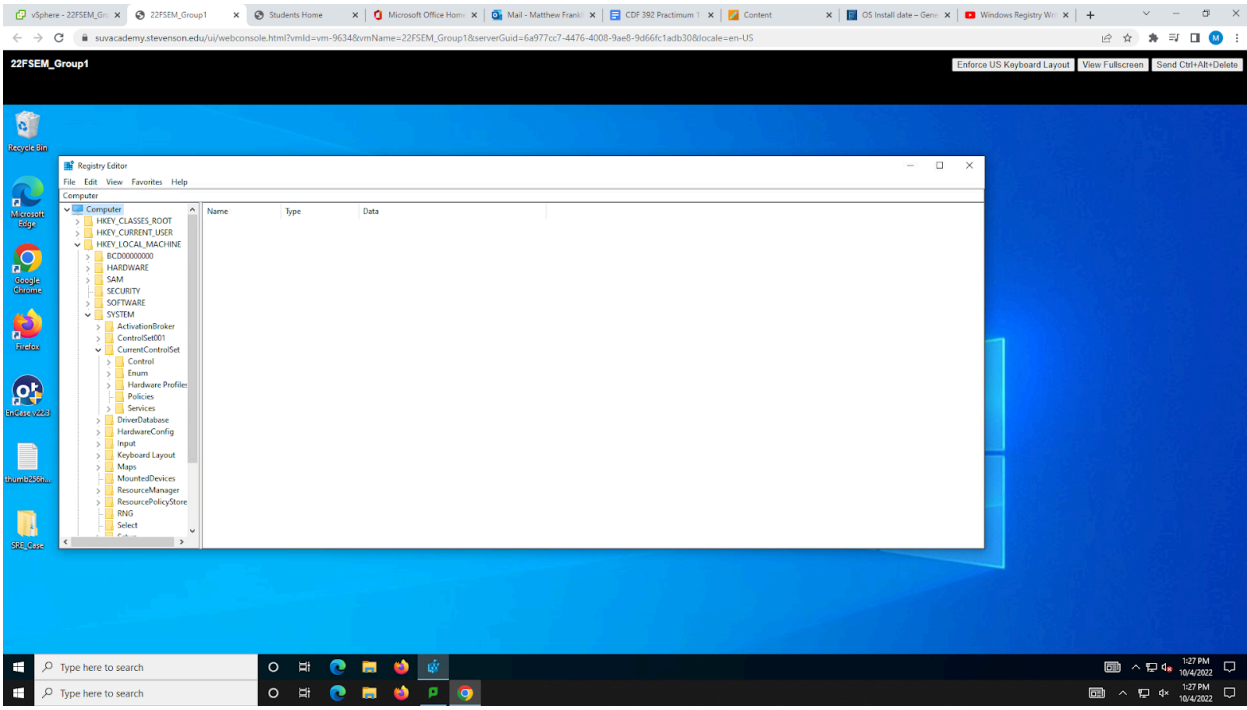


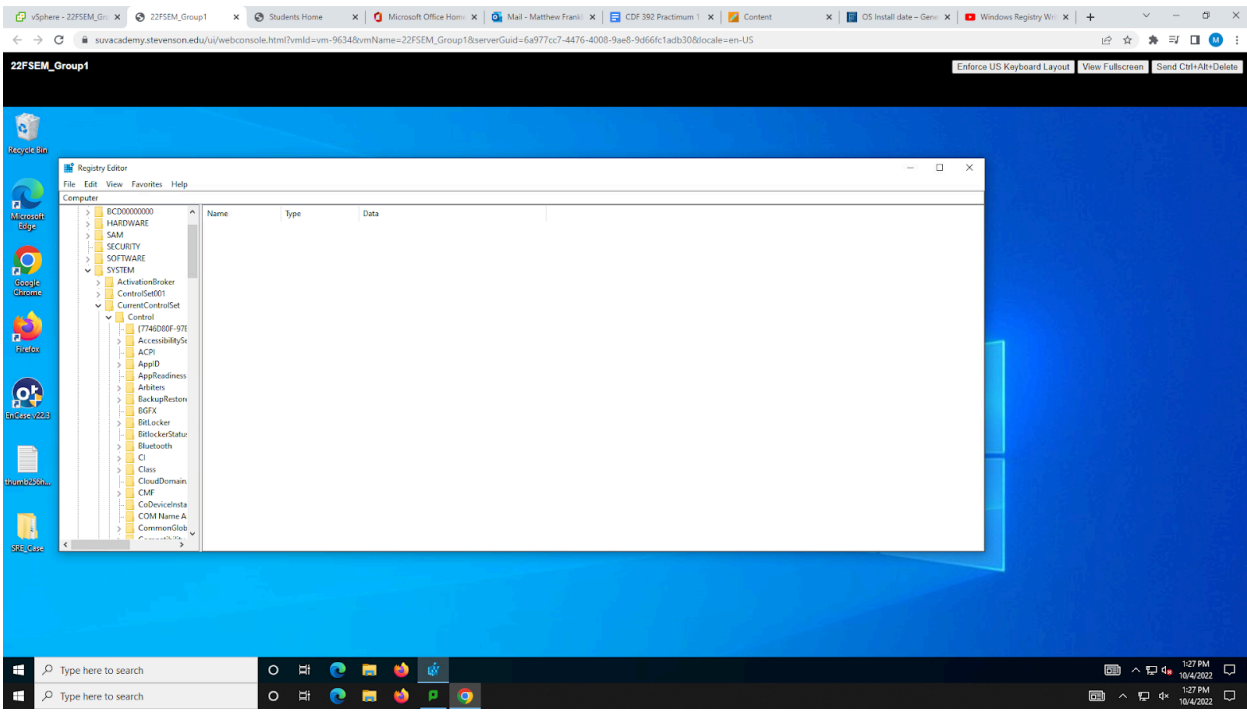

22FSEM_Group1
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
User Account Control
Do you want to allow this app to make changes to your device?
Registry Editor
Verified publisher: Microsoft Windows
Show more details
Yes
No
Type here to search
1:26 PM
10/4/2022

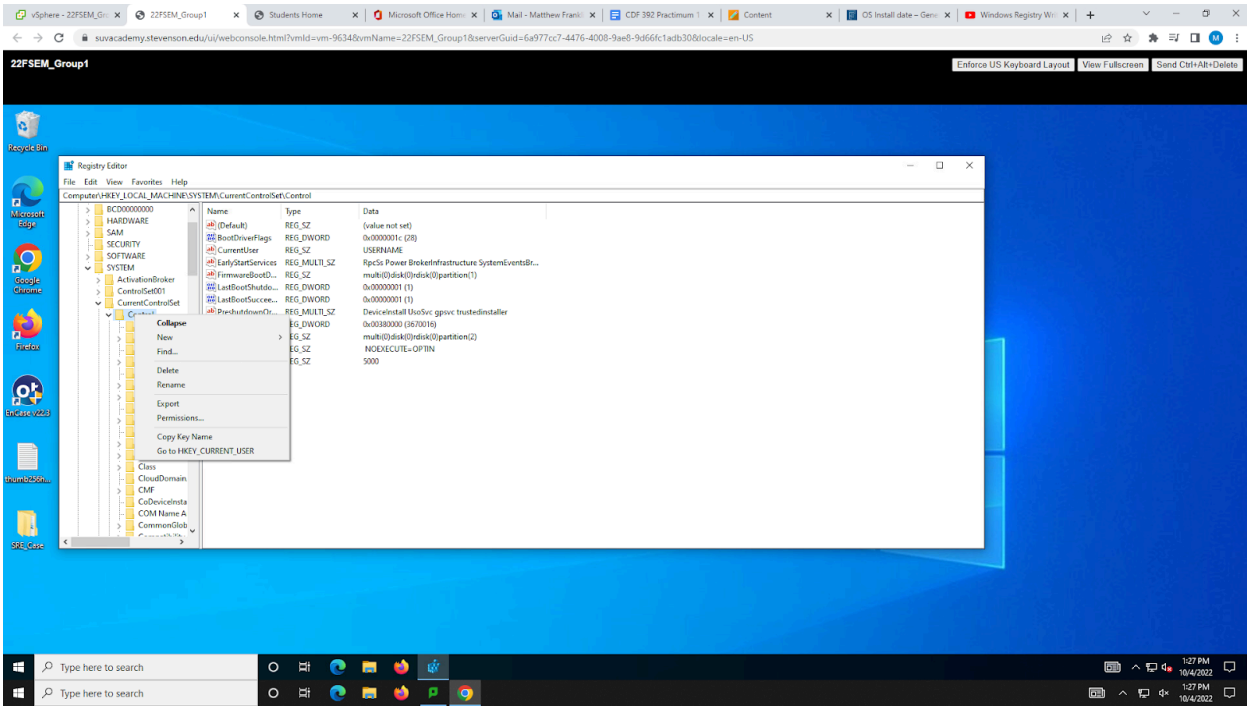

22FSEM_Group1
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Recycle Bin
Microsoft Edge
Google Chrome
Firefox
EnCase v22.3
thumbs2ohu...
SRE_Case
Registry Editor
File Edit View Favorites Help
Computer
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HKEY_USERS
HKEY_CURRENT_CONFIG
Name
Type
Data
Type here to search
1:26 PM
10/4/2022

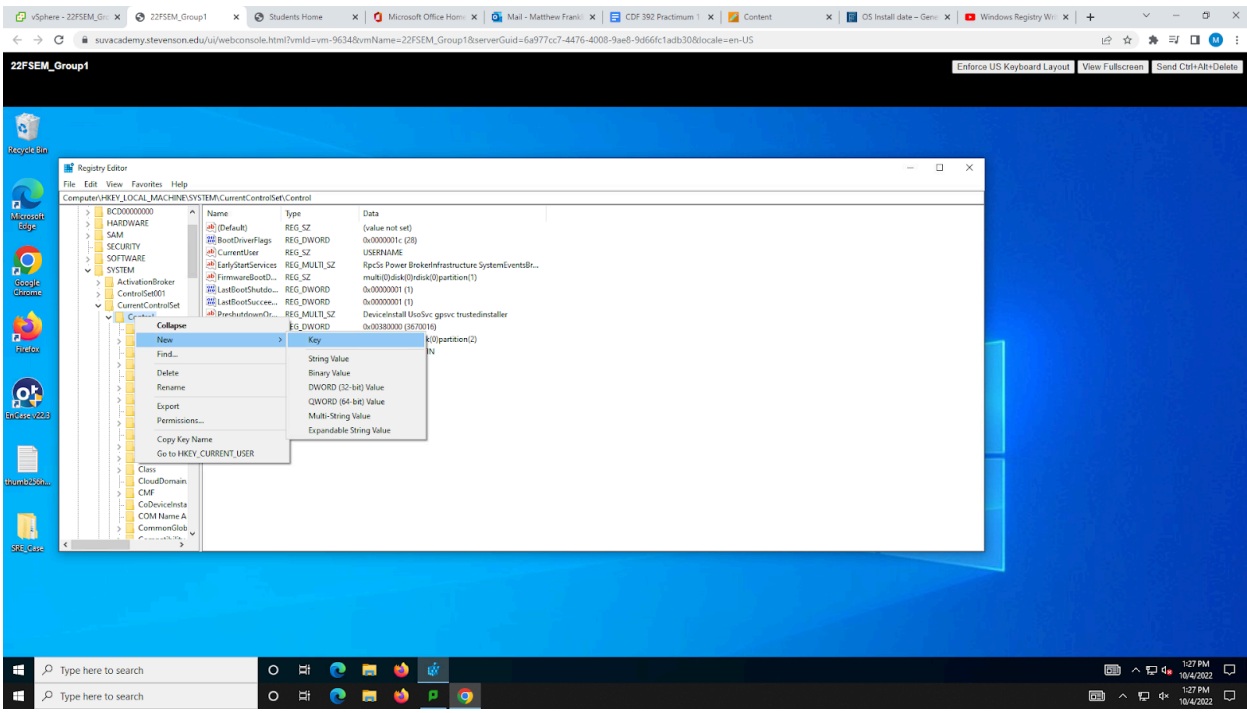

22FSEM_Group1
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Registry Editor
File Edit View Favorites Help
Computer
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
BCD00000000
HARDWARE
SAM
SECURITY
SOFTWARE
SYSTEM
HKEY_USERS
HKEY_CURRENT_CONFIG
Name
Type
Data
Type here to search
1:26 PM
10/4/2022

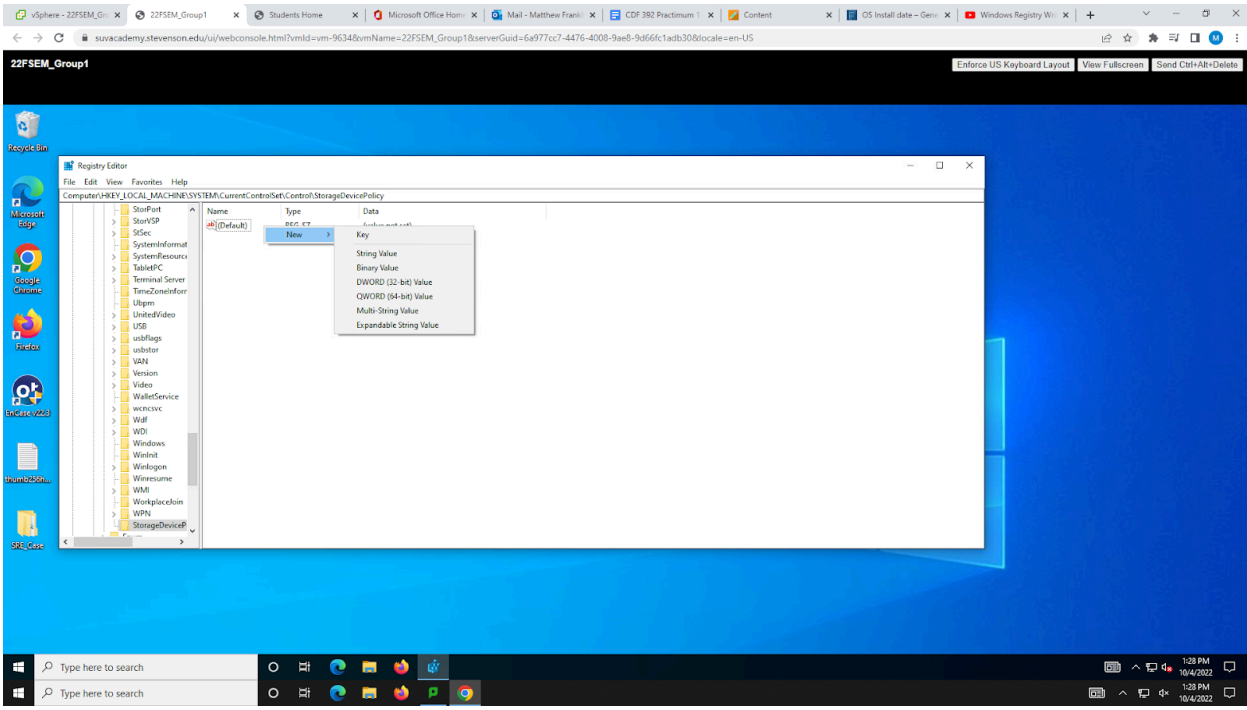

22FSEM_Group1
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Registry Editor
File Edit View Favorites Help
Computer
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
BCD00000000
HARDWARE
SAM
SECURITY
SOFTWARE
SYSTEM
ActivationBroker
ControlSet001
CurrentControlSet
DriverDatabase
HardwareConfig
Input
Keyboard Layout
Maps
MountedDevices
ResourceManager
ResourcePolicyStore
RNG
Select
Setup
Software
State
WaaS
WPA
Name
Type
Data
Type here to search
1:27 PM
10/4/2022

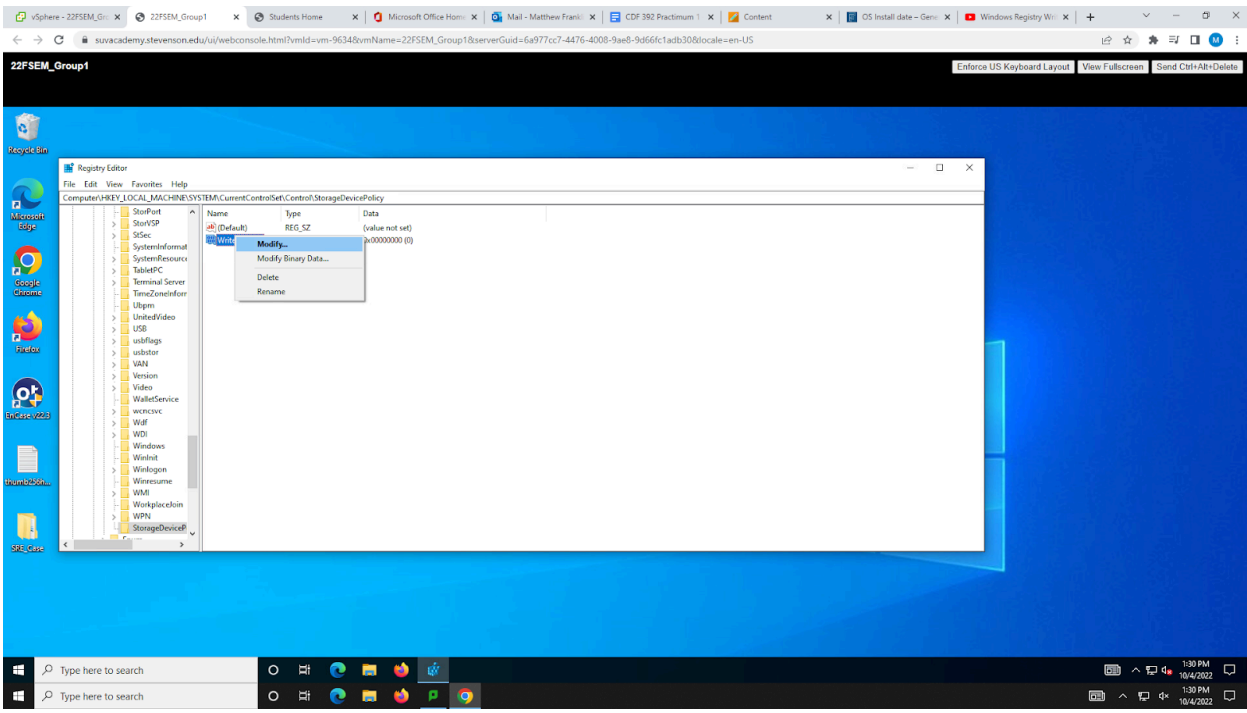

22FSEM_Group1
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Registry Editor
File Edit View Favorites Help
Computer
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
BCD00000000
HARDWARE
SAM
SECURITY
SOFTWARE
SYSTEM
ActivationBroker
ControlSet001
CurrentControlSet
Control
Enum
Hardware Profiles
Policies
Services
DriverDatabase
HardwareConfig
Input
Keyboard Layout
Maps
MountedDevices
ResourceManager
ResourcePolicyStore
RNG
Select
Name
Type
Data
Type here to search
1:27 PM
10/4/2022

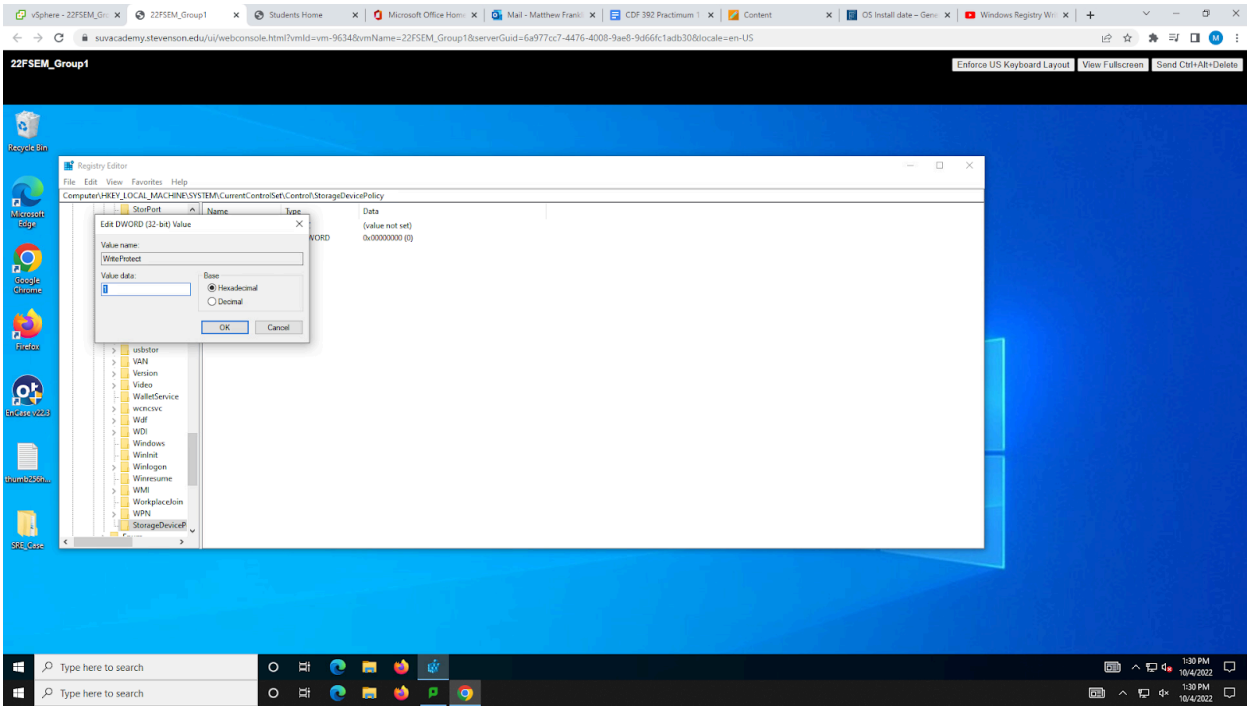

22FSEM_Group1
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Registry Editor
File Edit View Favorites Help
Computer
BCD00000000
HARDWARE
SAM
SECURITY
SOFTWARE
SYSTEM
ActivationBroker
ControlSet001
CurrentControlSet
Control
Name
Type
Data
Type here to search
1:27 PM
10/4/2022

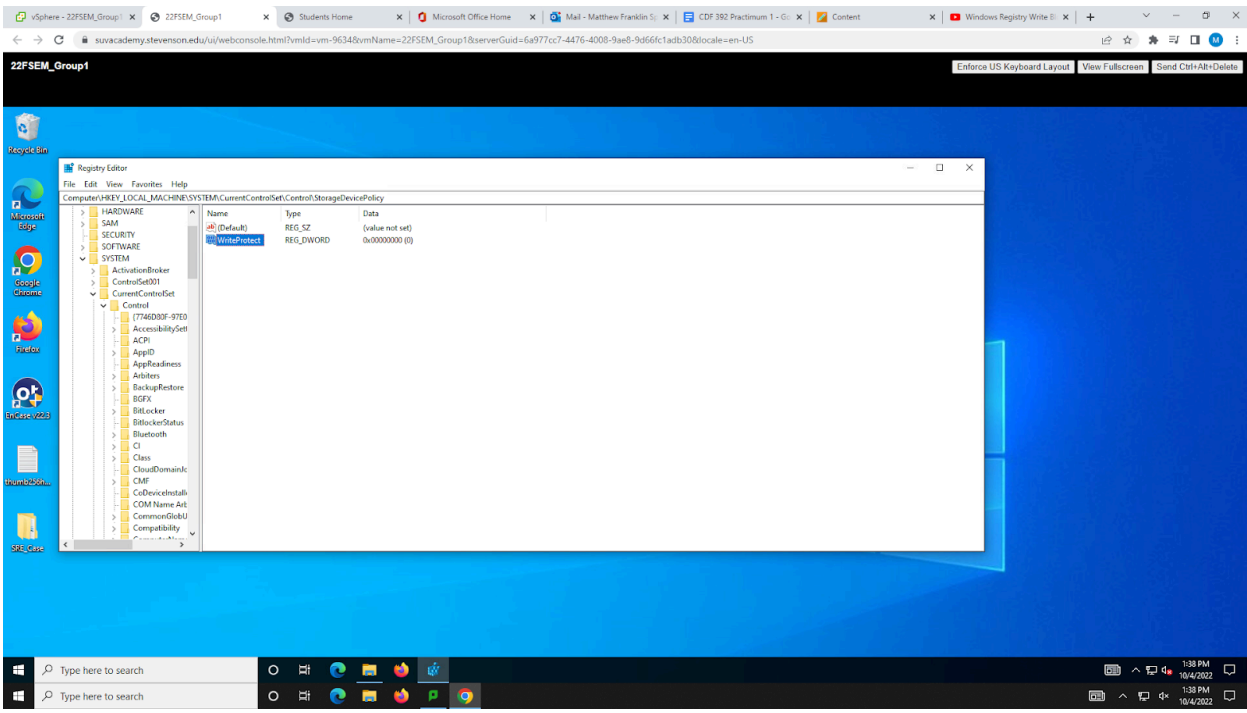

22FSEM_Group1
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Registry Editor
File Edit View Favorites Help
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control
Collapse
New
Find...
Delete
Rename
Export
Permissions...
Copy Key Name
Go to HKEY_CURRENT_USER
Type here to search


22FSEM_Group1
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Registry Editor
File Edit View Favorites Help
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control
Collapse
New
Find...
Delete
Rename
Export
Permissions...
Copy Key Name
Go to HKEY_CURRENT_USER
Key
String Value
Binary Value
DWORD (32-bit) Value
QWORD (64-bit) Value
Multi-String Value
Expandable String Value
Type here to search


22FSEM_Group1
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Registry Editor
File Edit View Favorites Help
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicy
Name
Type
Data
(Default)
New
Key
String Value
Binary Value
DWORD (32-bit) Value
QWORD (64-bit) Value
Multi-String Value
Expandable String Value
Type here to search


22FSEM_Group1
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Registry Editor
File Edit View Favorites Help
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicy
Name
Type
Data
(Default)
REG_SZ
(value not set)
Modify...
Modify Binary Data...
Delete
Rename
Type here to search





10/13 Suggestions:

- If you are stuck on a problem, go on. (Many questions can be answered out of sequence.)
- You may need to revisit previous class material or use Google
- Use the discussion board to get ideas from team members
- Document all attempts and problems that you encounter

- Include all error documentation in the PPSX file
- You may not be able to answer all of the questions
- Good documentation will enhance your grade
- Poor documentation will reduce your grade