Sydney Petrehn

Digital Forensics

Dr. Haney

Project 1: Build a Forensic Workstation

Option Chosen: CAINE

Task 1: Download and Verify

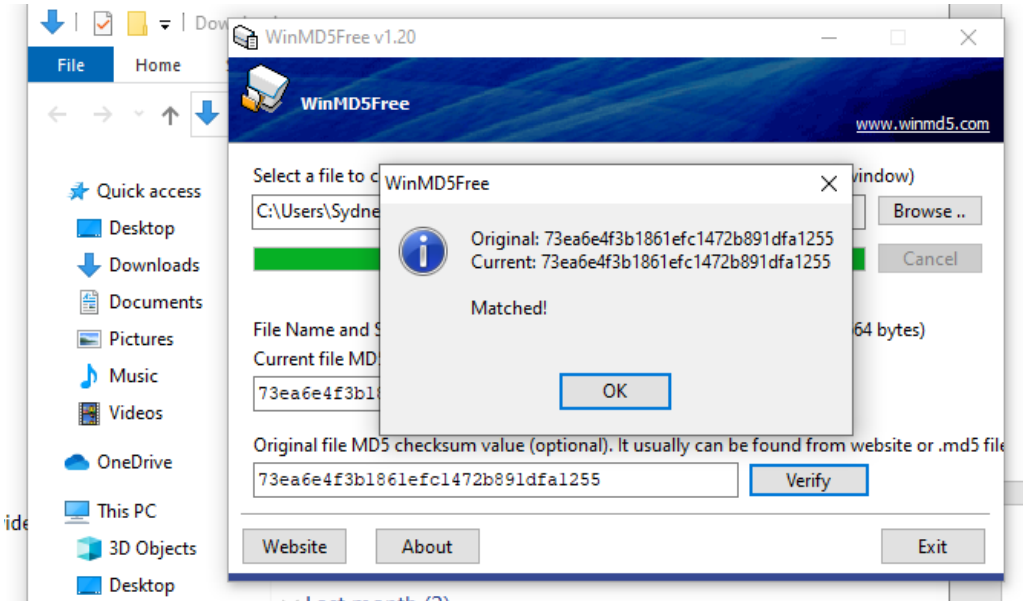
I chose to use CAINE for this first project. I followed the link provided to this website where I downloaded the ISO image for CAINE 11.0.

The website provided the following as the official hash of the file:

`MD5 - 73EA6E4F3B1861EFC1472B891DFA1255 caine11.0.iso`

`SHA1 - 74E059AF4547CB5D765080BDB8B236E4CB4550AE caine11.0.iso`

I downloaded WinMD5Free to verify the hash of the file to make sure It was correct and it was a verified match.



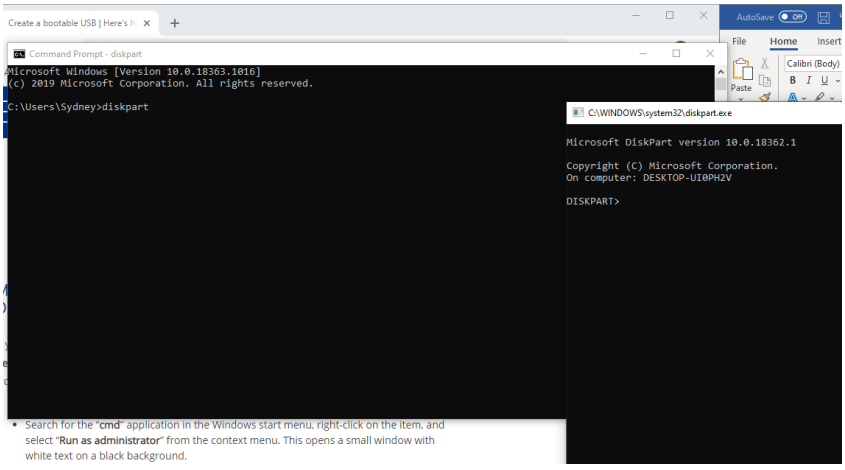
Task 2: Create a read only bootable device

I did task 1 and 3 on Sunday however I did not have the USB drives sent to me yet since they are on their way. So I did this task on Monday September 7, 2020 the day after so that I could run to Walmart and get a USB.

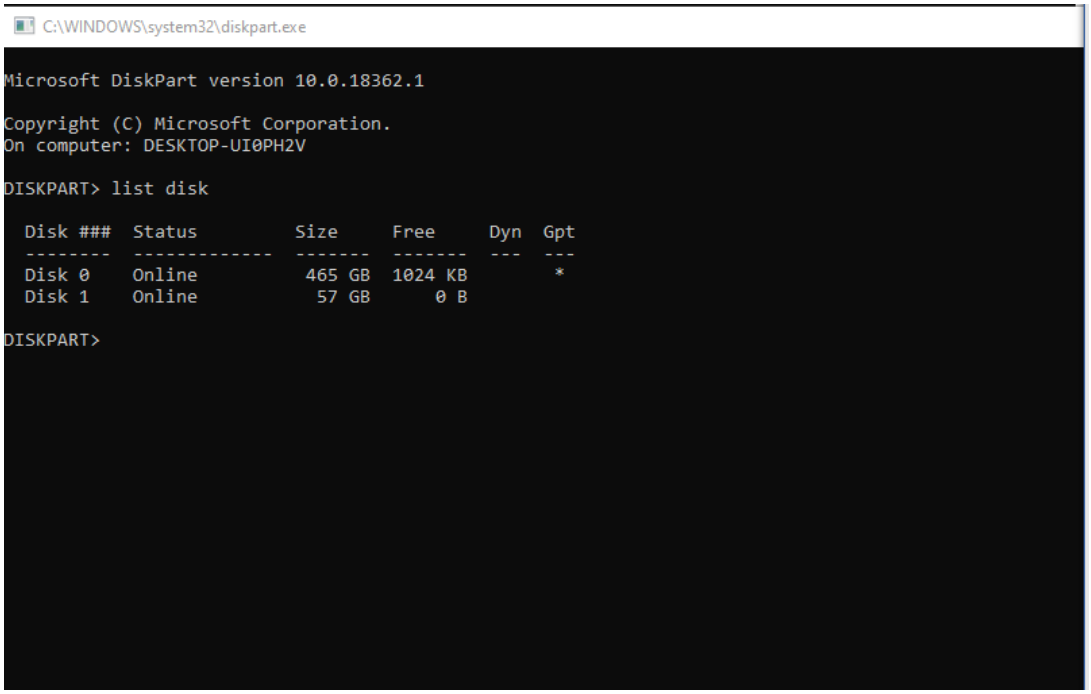
I got a 64GB flash drive from Walmart to make a bootable USB.

I found the following Guide on how to make a USB stick bootable and I followed it for this assignment. https://www.ionos.com/digitalguide/server/know-how/make-a-bootable-usb-drive/

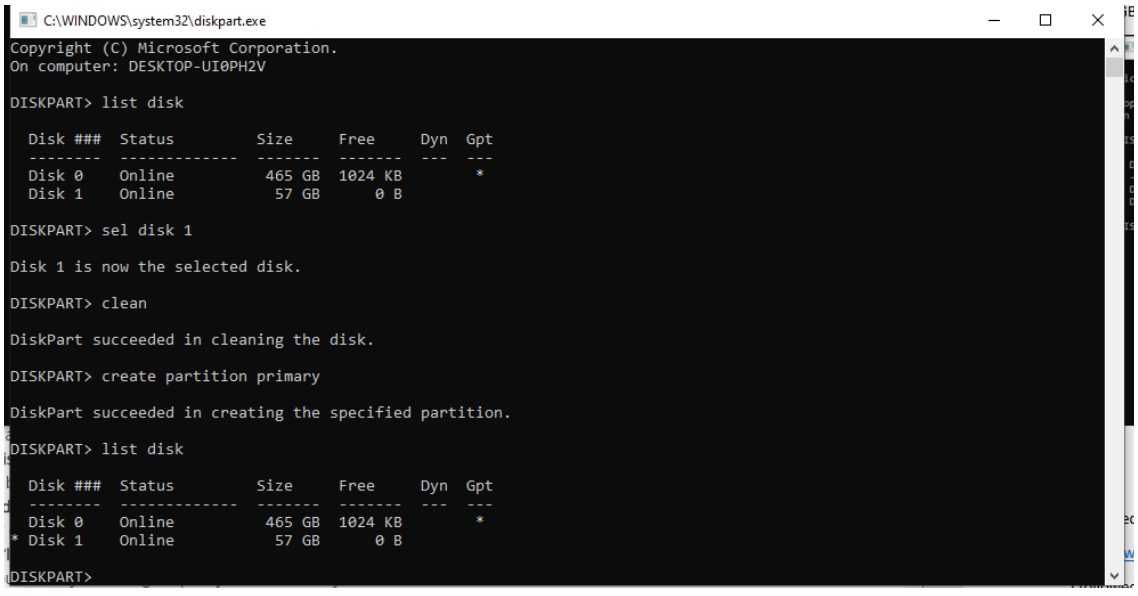
To make the USB bootable I opened the command line and typed *diskpart*. This opened a new window of the command line for the USB.



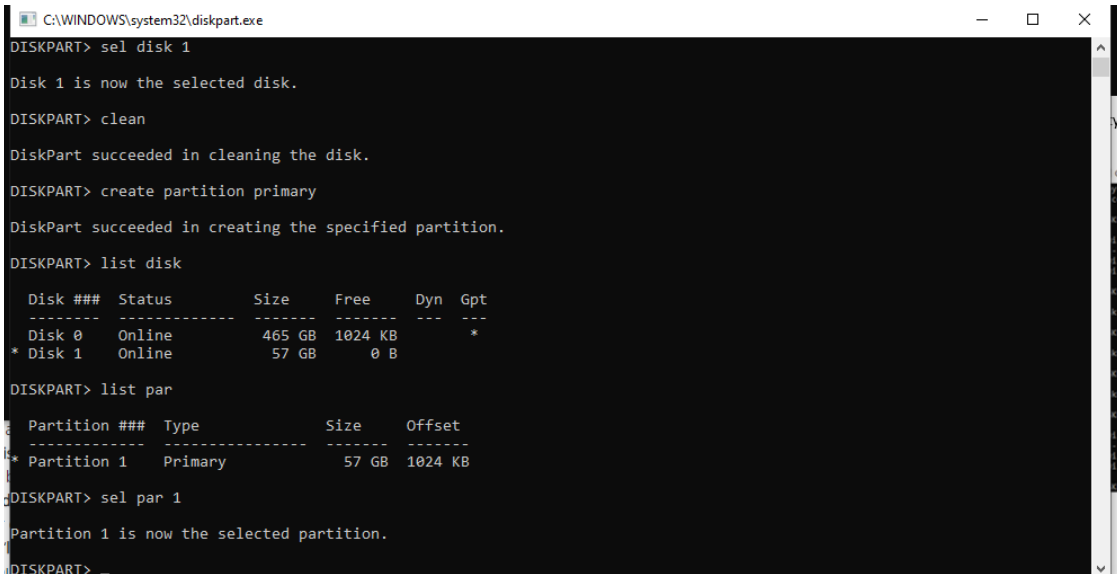
Then to identify which device was the USB I typed the command *list disk* which listed the hard drive of my computer and the USB. I was able to tell which one was the USB by the amount of storage it had available. My USB said it was 64 GB but I thought it was interesting that this screen showed that it only had 57GB available.



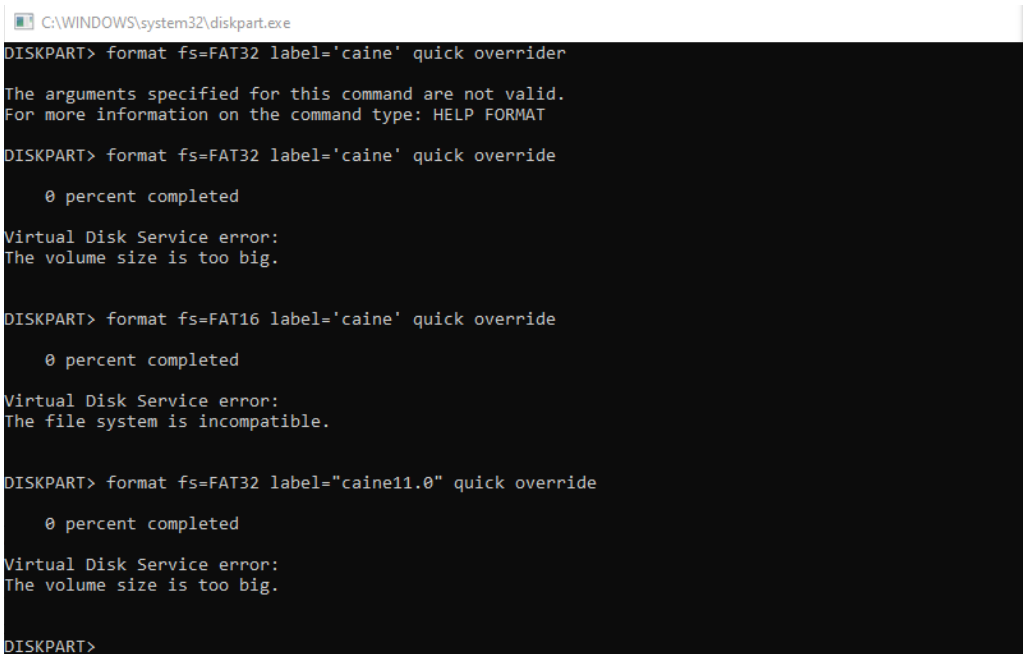
Next I typed *sel disk 1* to select the USB. Then I typed *clean* to clean the disk. Then I created a partition on the USB by typing *create partition primary*.



Then I listed the partitions on the USB by typing *list par* then I selected the first partition I just created by typing *sel par 1*.



Now the tutorial had me try to format the USB however when I typed *format fs=FAT32 label="caine11.0" quick override* it had an error that the volume size is too big. This led to me googling and trying to look for a tutorial on how to format a USB.

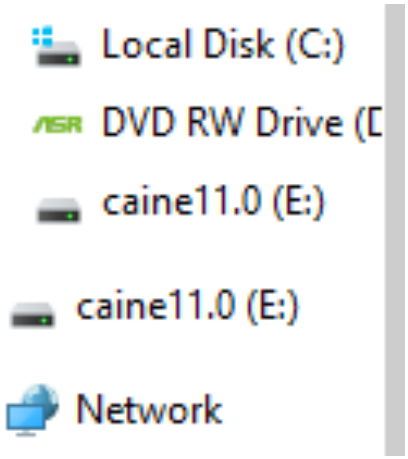


I used this tutorial that said to type *format fs=ntfs quick* and changing the FAT32 to ntfs worked. I am not sure at this point if this will affect my ability to boot from the USB but I will continue with the first tutorial as if I ran into no errors.

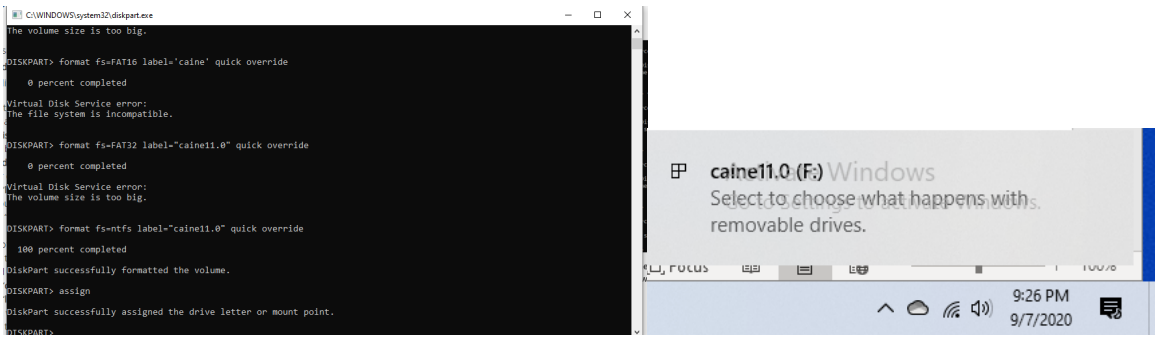
https://docs.microsoft.com/en-us/windows-server-essentials/install/create-a-bootable-usb-flash-drive

```
    0 percent completed

Virtual Disk Service error:
The volume size is too big.


DISKPART> format fs=FAT16 label='caine' quick override

    0 percent completed

Virtual Disk Service error:
The file system is incompatible.


DISKPART> format fs=FAT32 label="caine11.0" quick override

    0 percent completed

Virtual Disk Service error:
The volume size is too big.


DISKPART> format fs=ntfs label="caine11.0" quick override

  100 percent completed

DiskPart successfully formatted the volume.

DISKPART>
```

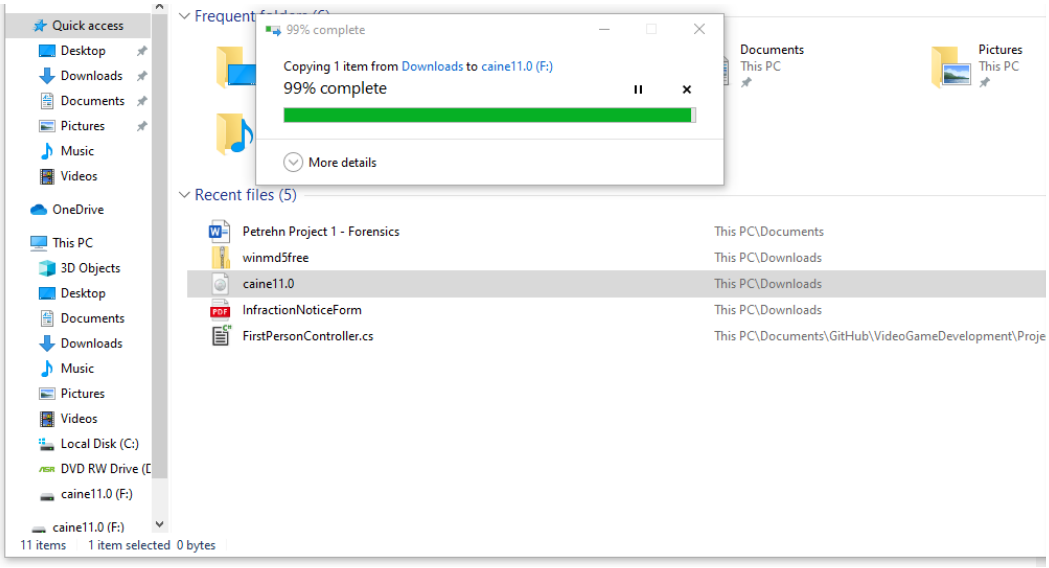
I also checked how my PC registered the USB at this point and it did read it as caine11.0 so I know the format was successful.



Next I typed *assign* which automatically assigned a drive letter to my USB. In my case it was assigned to E.



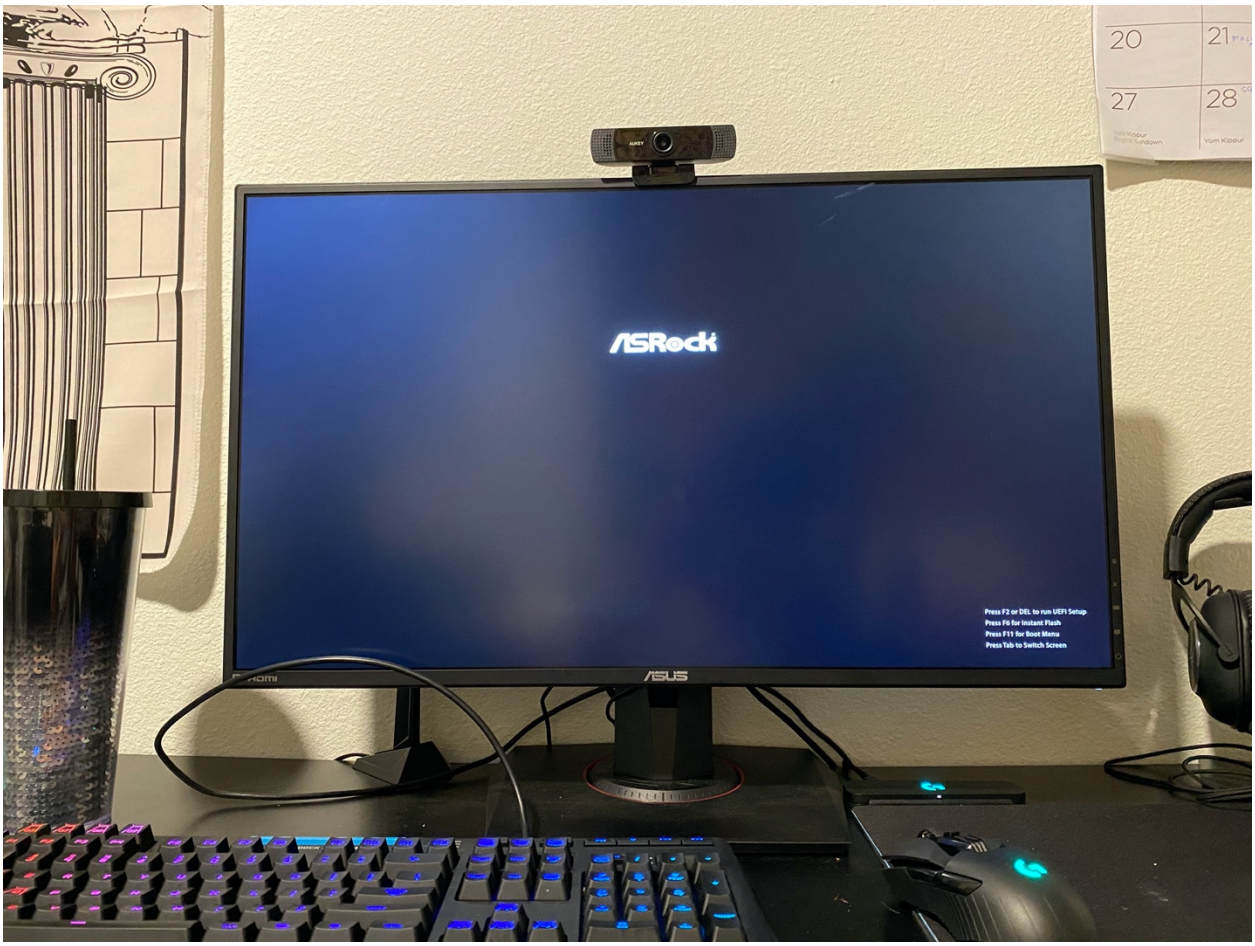
Then I exited the command line and dragged and dropped the Caine11.0 ISO into the USB.



Now I shut down my pc and entered the system's bios to boot from the USB.

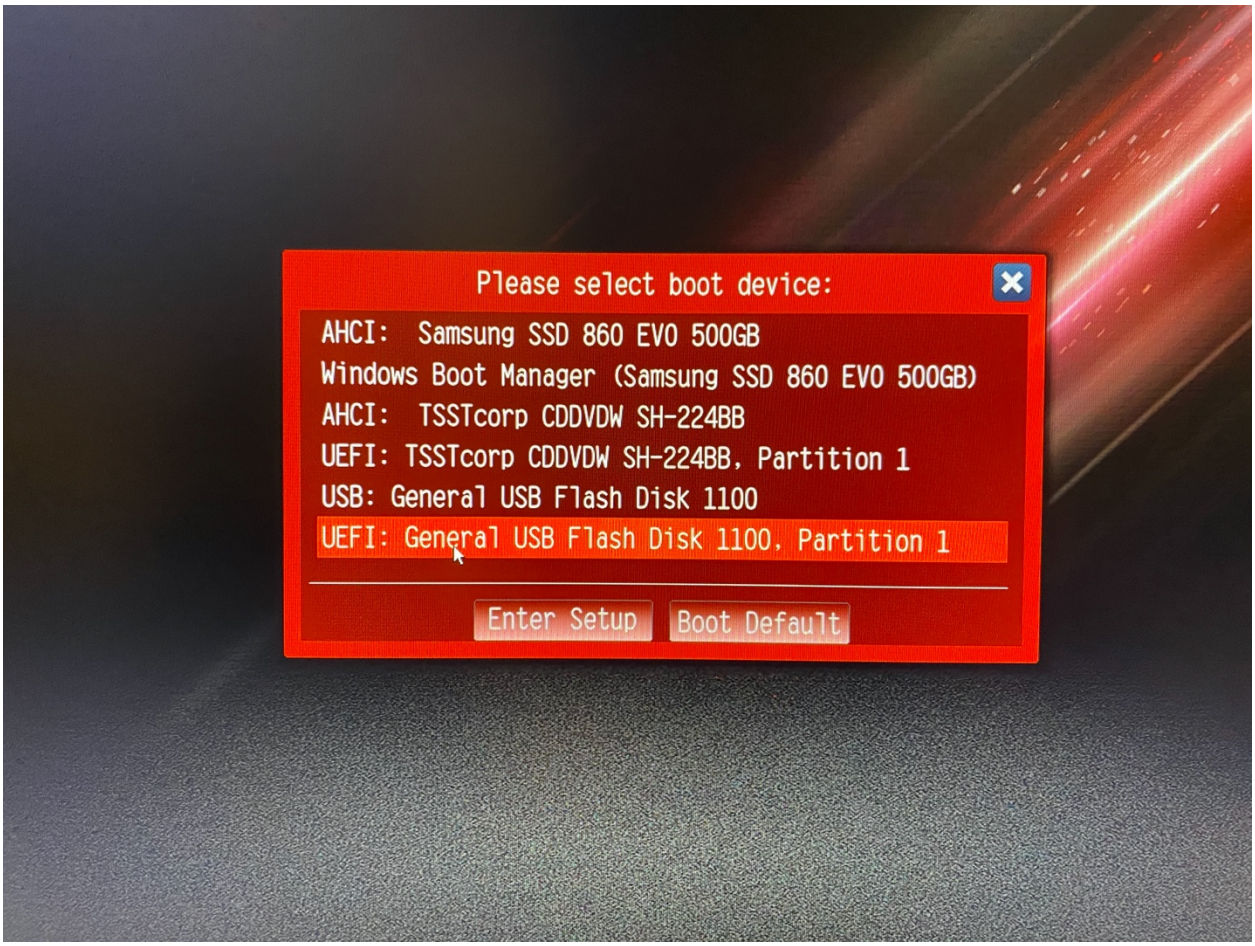
I entered the BIOS by pressing DEL

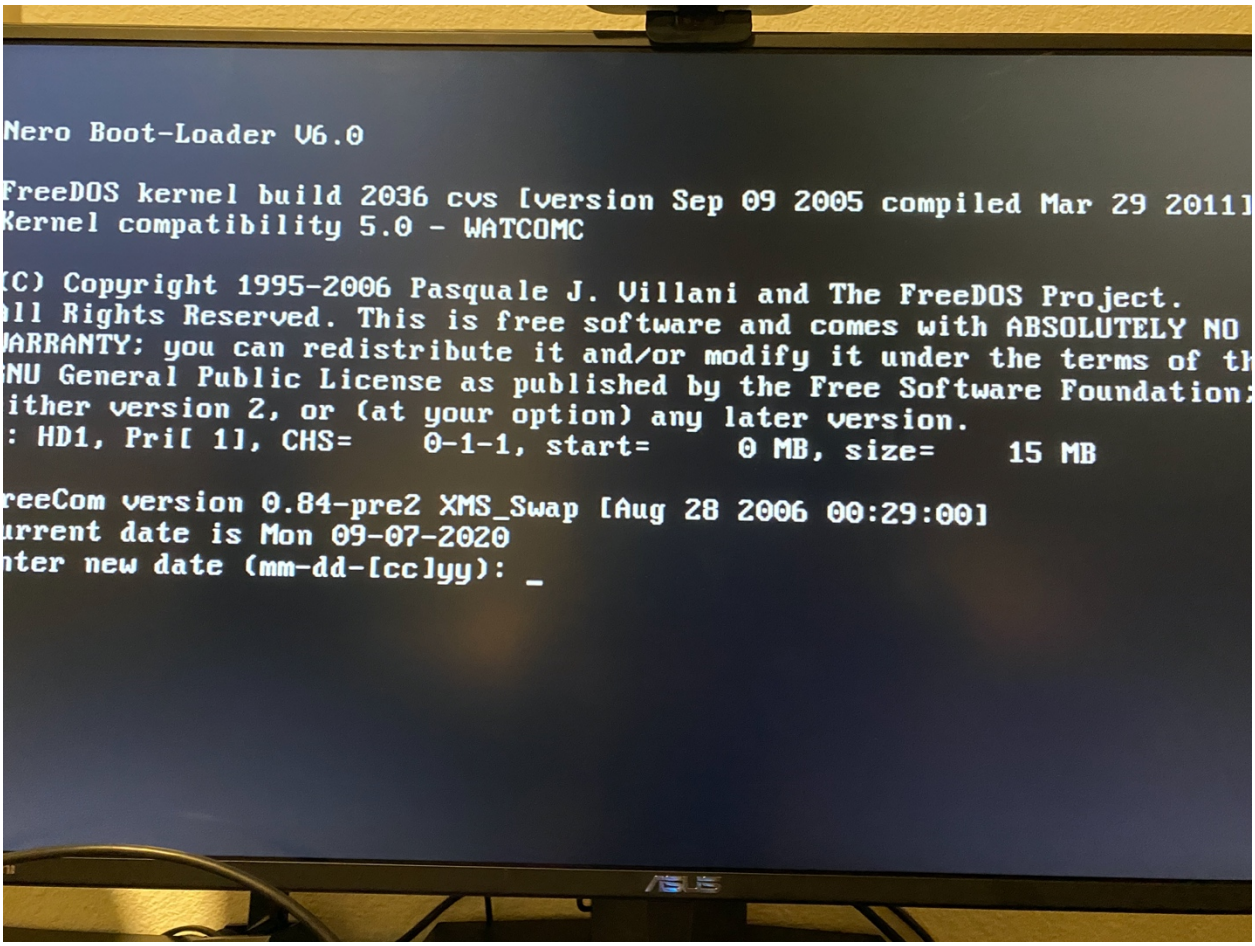
I set the boot order so that the PC would boot from the USB. However this did not work.

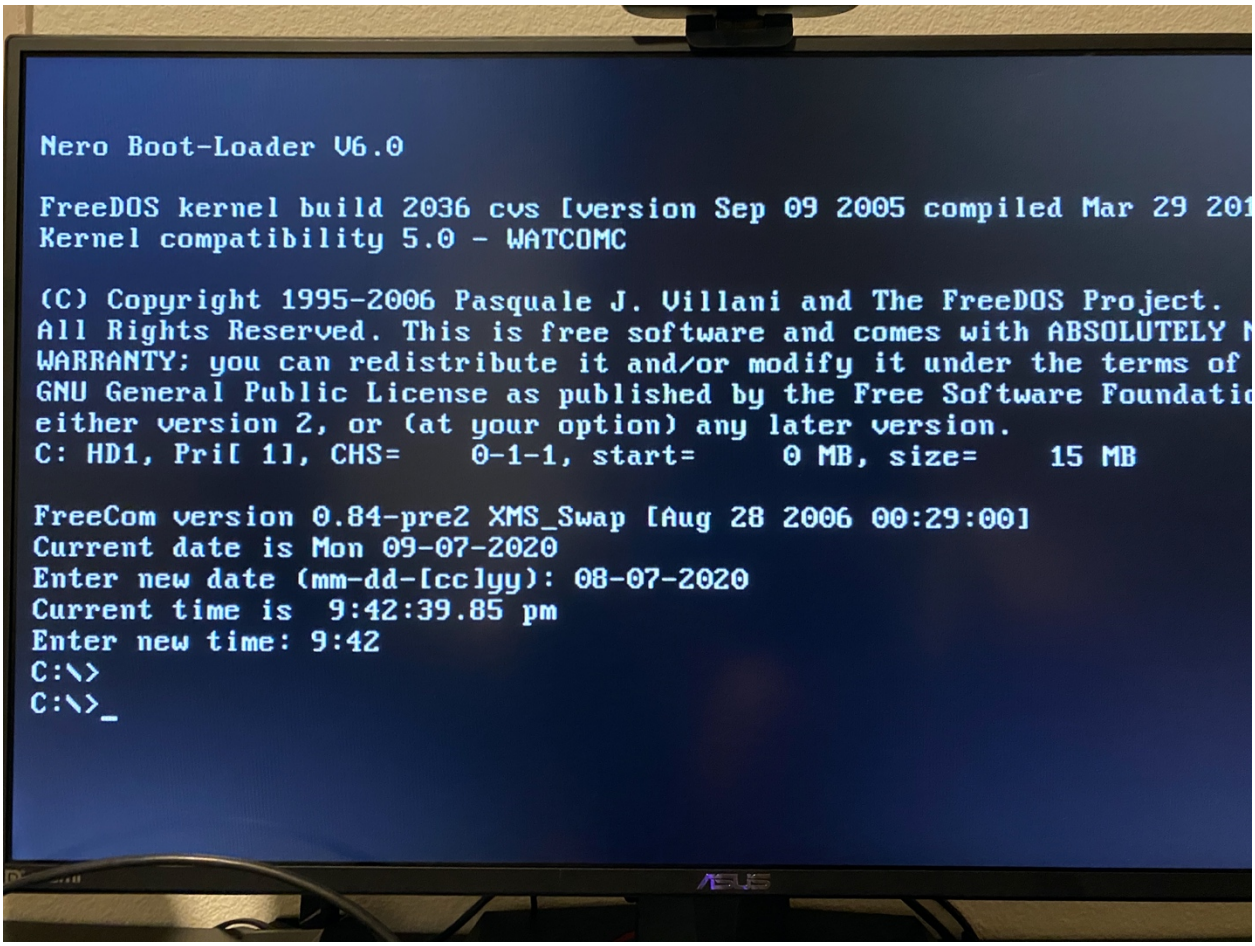


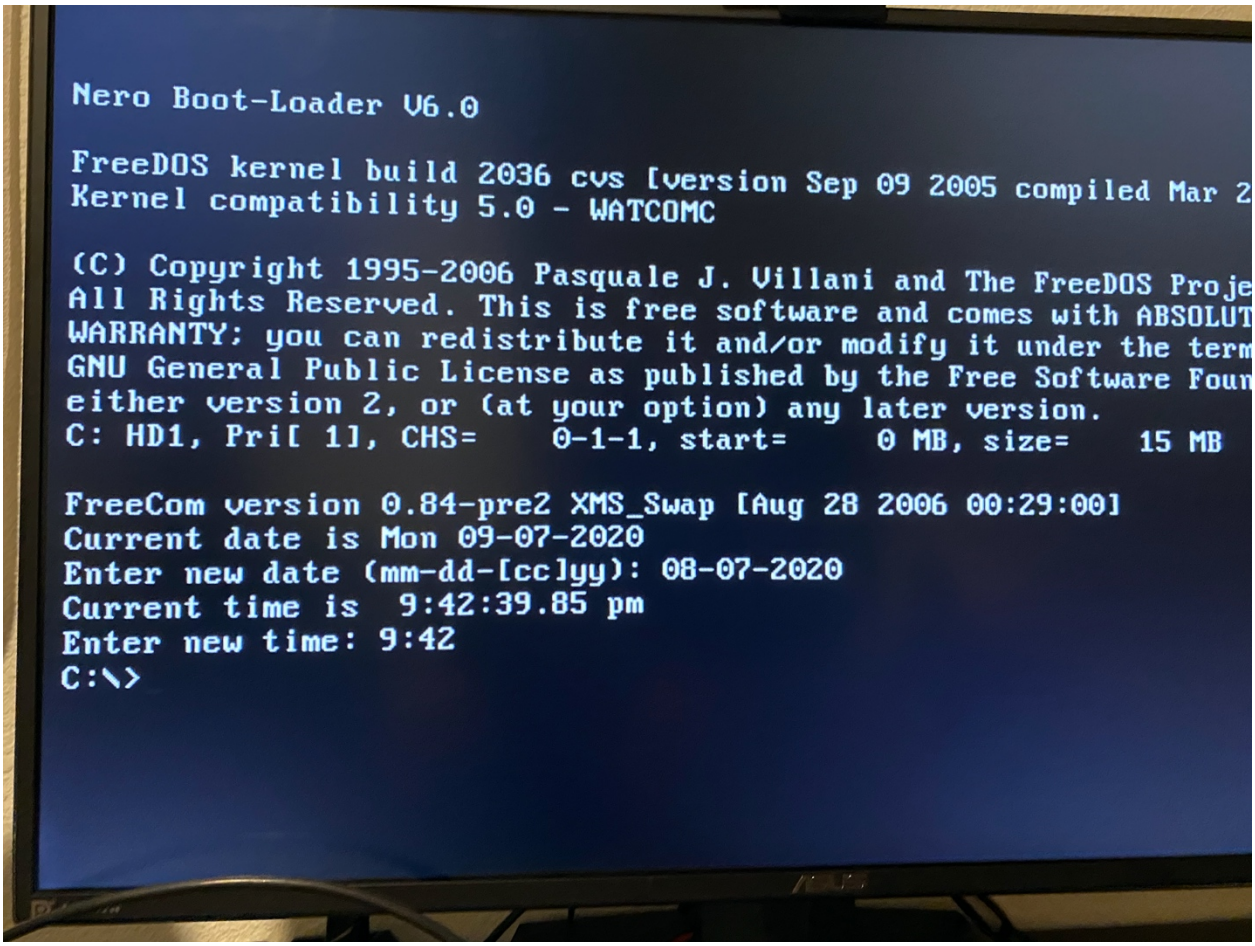

Main
OC Tweaker
Advanced
Boot Option Priorities
Boot Option #1
Boot Option #2
Boot Option #3
Boot Option #4
Boot Option #5
Boot Option #6
Hard Drive BBS Priorities
CD/DVD ROM Drive BBS Priorities
USB Device BBS Priorities
Boot From Onboard LAN
Boot Beep
Setup Prompt Timeout
Bootup Num-Lock
Full Screen Logo
AddOn ROM Display
Windows Boot Manager ...
AHCI: Samsung SSD 86...
AHCI: TSSTcorp CDDVD...
Boot Option #1
AHCI: Samsung SSD 860 EVO 500GB
Windows Boot Manager (Samsung SSD 860 EVO 500GB)
AHCI: TSSTcorp CDDVDW SH-224BB
UEFI: TSSTcorp CDDVDW SH-224BB, Partition 1
USB: General USB Flash Disk 1100
UEFI: General USB Flash Disk 1100, Partition 1
Disabled
Disabled
1
On
Enabled
Enabled
English


An operating system wasn't found. Try disconnecting any drives that don't
contain an operating system.
Press Ctrl+Alt+Del to restart
_
20
27


Please select boot device:
AHCI: Samsung SSD 860 EVO 500GB
Windows Boot Manager (Samsung SSD 860 EVO 500GB)
AHCI: TSSTcorp CDDVDW SH-224BB
UEFI: TSSTcorp CDDVDW SH-224BB, Partition 1
USB: General USB Flash Disk 1100
UEFI: General USB Flash Disk 1100, Partition 1
Enter Setup
Boot Default


Nero Boot-Loader V6.0
FreeDOS kernel build 2036 cvs [version Sep 09 2005 compiled Mar 29 2011]
Kernel compatibility 5.0 - WATCOMC
(C) Copyright 1995-2006 Pasquale J. Villani and The FreeDOS Project.
All Rights Reserved. This is free software and comes with ABSOLUTELY NO
WARRANTY; you can redistribute it and/or modify it under the terms of th
GNU General Public License as published by the Free Software Foundation;
either version 2, or (at your option) any later version.
: HD1, Pri[1], CHS= 0-1-1, start= 0 MB, size= 15 MB
reeCom version 0.84-pre2 XMS_Swap [Aug 28 2006 00:29:00]
urrent date is Mon 09-07-2020
nter new date (mm-dd-[cc]yy): _


Nero Boot-Loader V6.0
FreeDOS kernel build 2036 cvs [version Sep 09 2005 compiled Mar 29 201
Kernel compatibility 5.0 - WATCOMC
(C) Copyright 1995-2006 Pasquale J. Villani and The FreeDOS Project.
All Rights Reserved. This is free software and comes with ABSOLUTELY N
WARRANTY; you can redistribute it and/or modify it under the terms of
GNU General Public License as published by the Free Software Foundatic
either version 2, or (at your option) any later version.
C: HD1, Pri[1], CHS= 0-1-1, start= 0 MB, size= 15 MB
FreeCom version 0.84-pre2 XMS_Swap [Aug 28 2006 00:29:00]
Current date is Mon 09-07-2020
Enter new date (mm-dd-[cc]yy): 08-07-2020
Current time is 9:42:39.85 pm
Enter new time: 9:42
C:\>
C:\>_



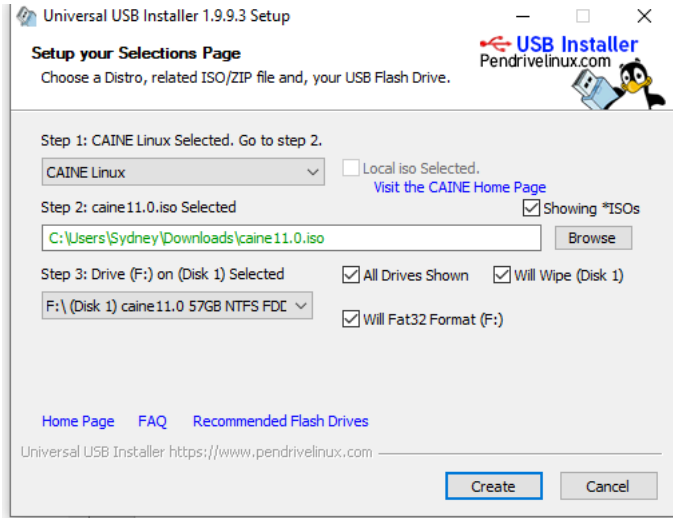
I found a new tutorial here on how to make a bootable USB specifically for CAINE which is probably what I should have looked for from the beginning…

https://ixnfo.com/en/how-to-make-a-bootable-usb-flash-drive-with-caine.html

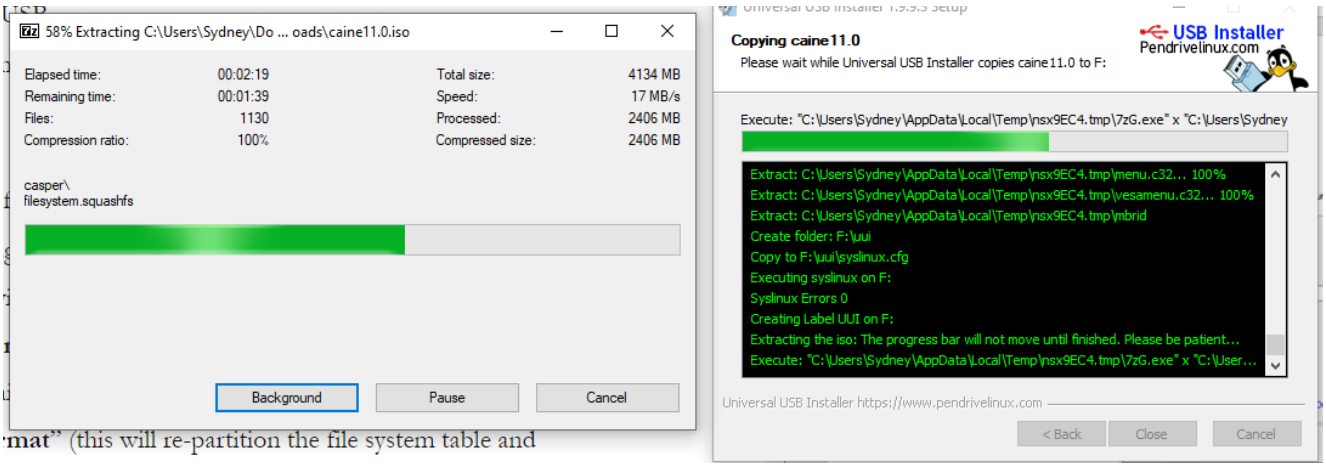
This guide had me download Universal USB to create the bootable USB. This can be found at the following website.

Installer http://www.pendrivelinux.com/universal-usb-installer-easy-as-1-2-3/

In Universal USB I selected CAINE Linux as the Distro and then selected the ISO I downloaded previously for CAINE then I formatted the USB and erased everything I previously did in this section.

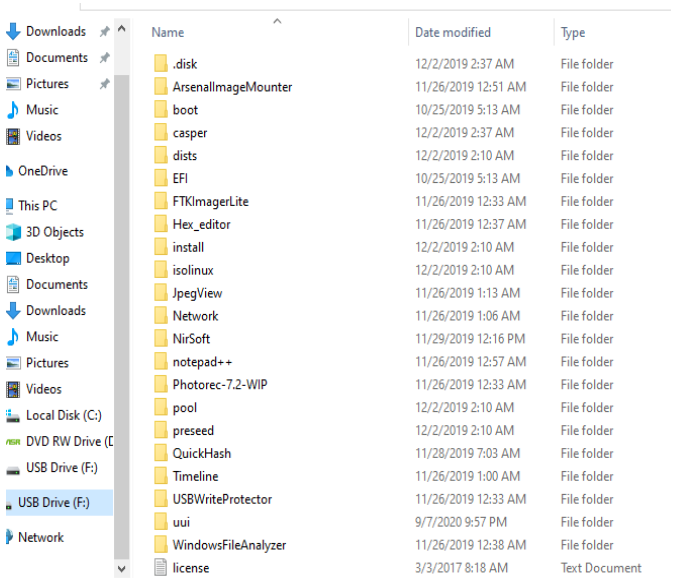


Then I hit the create button and the software did its thing. I recognized a lot of the commands it was running since I had just previously used them to attempt to format the USB myself.



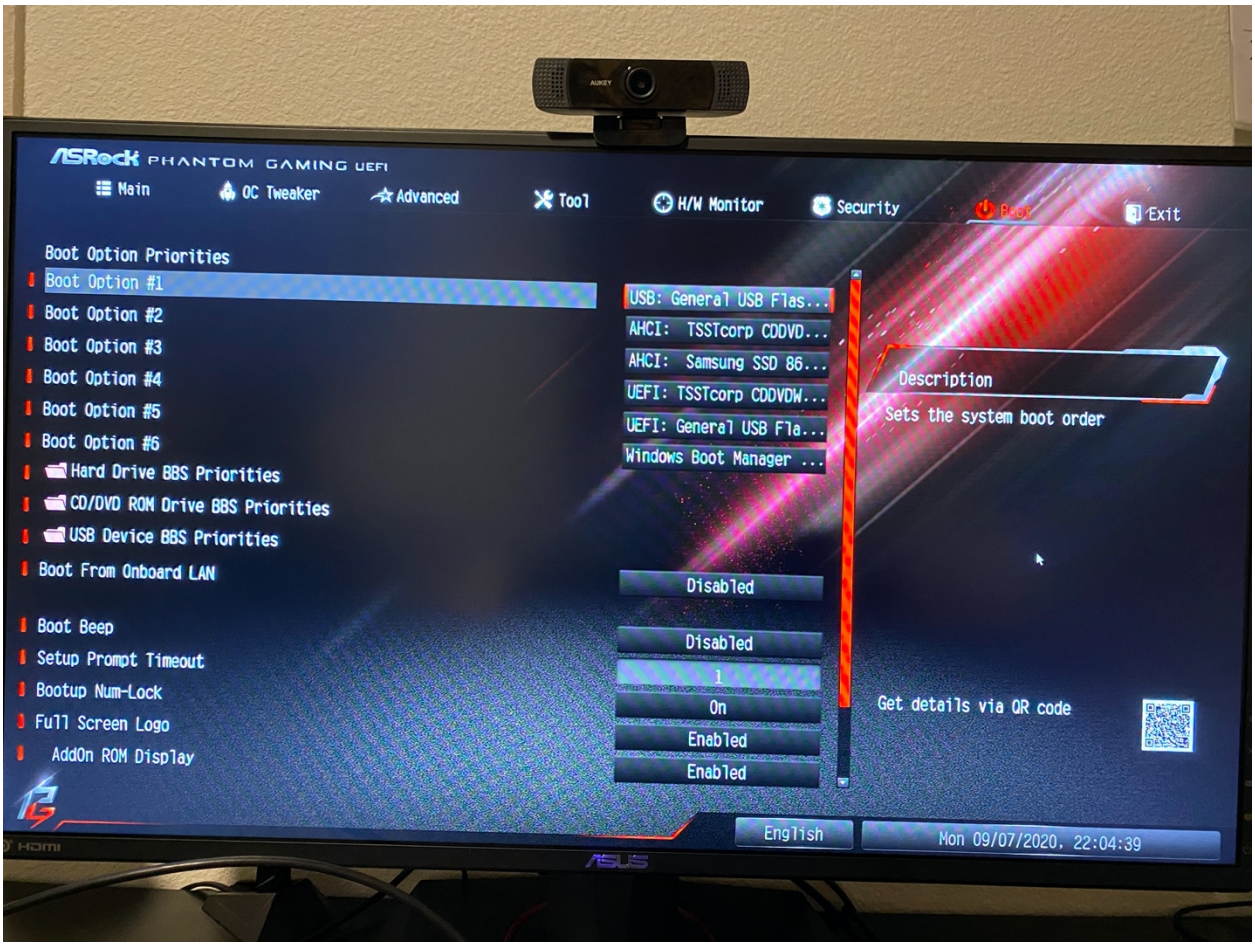
That is the end of the tutorial so I will once again attempt to boot my PC from the USB.

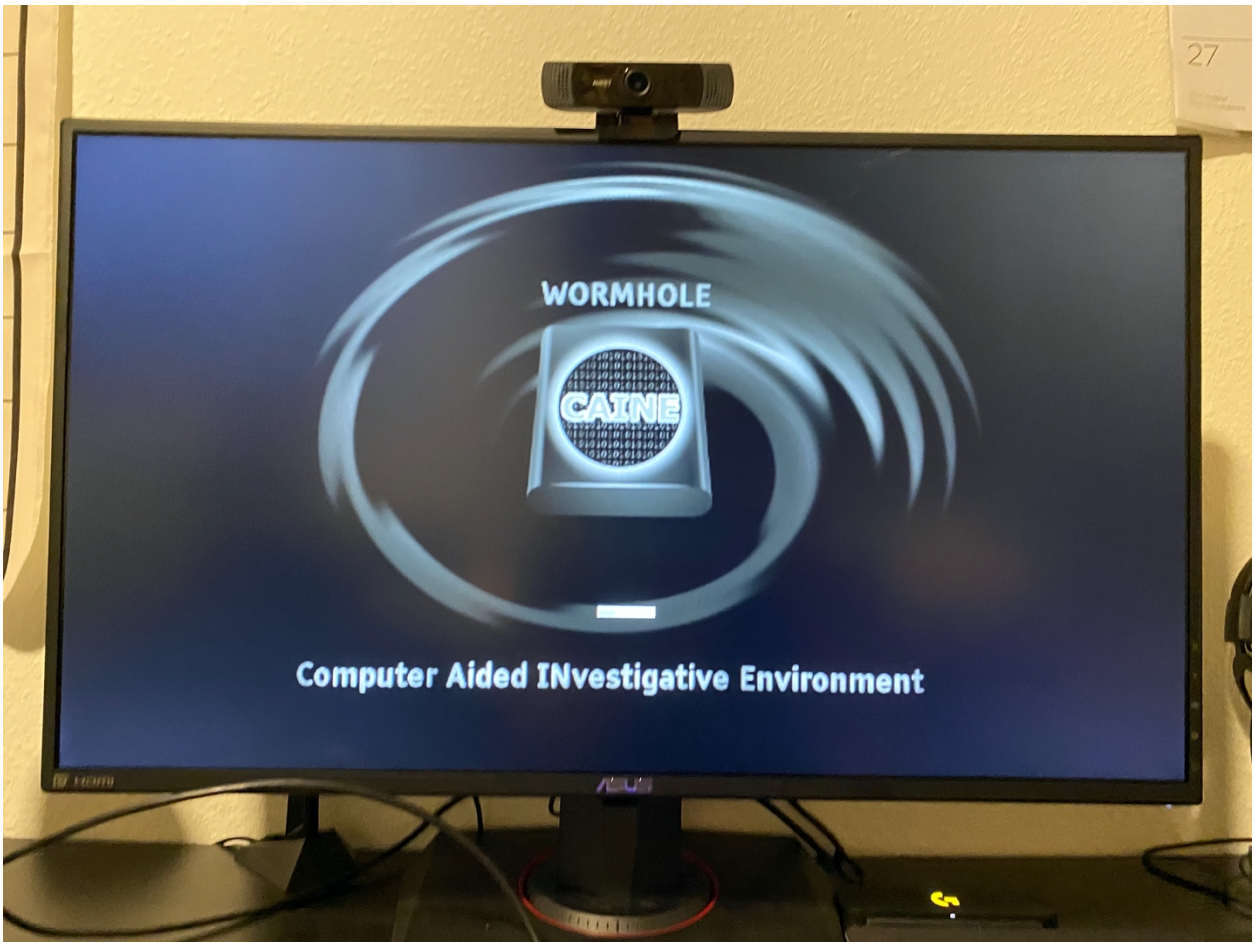
This is how my USB looks now, the name has changed since the software reformatted it.



I booted from the USB and it worked! Proof below:


WORMHOLE
CAINE
Computer Aided INvestigative Environment
caine's Home
Network
Trash
UnBlock
Autopsy
Computer
Network Servers
Caja-Root
Disk Image Mounter
Guymager
Install CAINE 10.04
keyboard
ASUS
mar set 8, 00:07


ASRock PHANTOM GAMING UEFI
Main
OC Tweaker
Advanced
Tool
H/W Monitor
Security
Boot
Exit
Boot Option Priorities
Boot Option #1
Boot Option #2
Boot Option #3
Boot Option #4
Boot Option #5
Boot Option #6
Hard Drive BBS Priorities
CD/DVD ROM Drive BBS Priorities
USB Device BBS Priorities
Boot From Onboard LAN
Boot Beep
Setup Prompt Timeout
Bootup Num-Lock
Full Screen Logo
AddOn ROM Display
USB: General USB Flas...
AHCI: TSSTcorp CDDVD...
AHCI: Samsung SSD 86...
UEFI: TSSTcorp CDDVDW...
UEFI: General USB Fla...
Windows Boot Manager ...
Disabled
Disabled
1
On
Enabled
Enabled
Description
Sets the system boot order
Get details via QR code
English
Mon 09/07/2020, 22:04:39


WORMHOLE
CAINE
Computer Aided INvestigative Environment

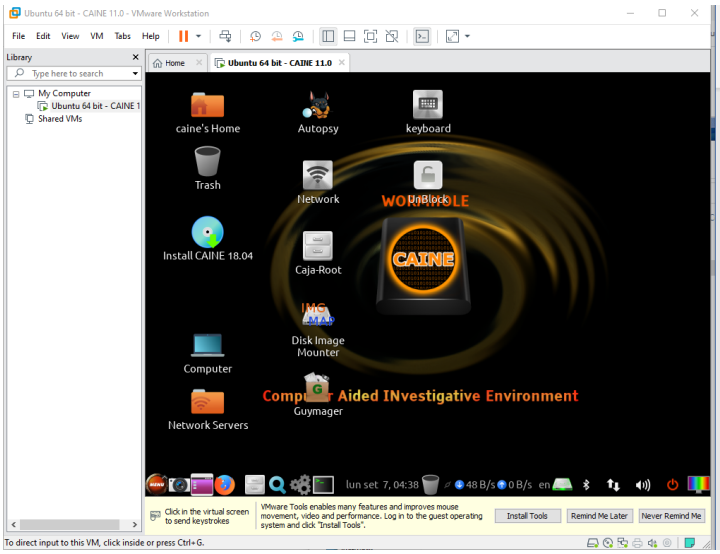

caine's Home
Network
Trash
UnBlock
Autopsy
Computer
Network Servers
Caja-Root
Disk Image Mounter
Guymager
Install CAINE 10.04
keyboard
WORMHOLE
CAINE
Computer Aided INvestigative Environment
en
mar set 8, 00:06
ASUS
HDMI

Task 3: Install a persistent (read-write) instance

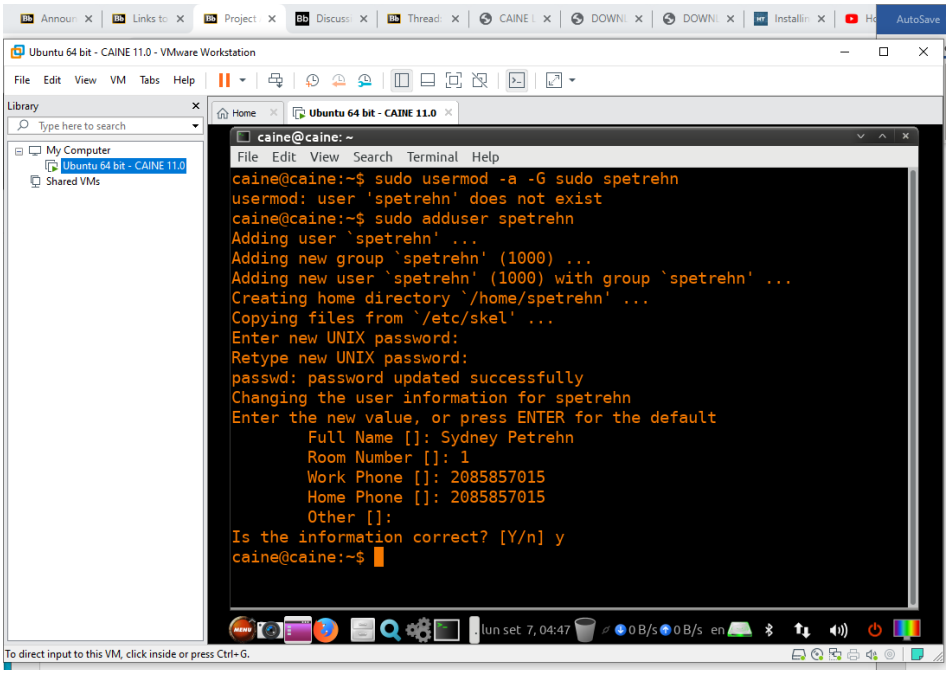
I followed the tutorial provided here to create a new VM Workstation and have CAINE as the disk image.

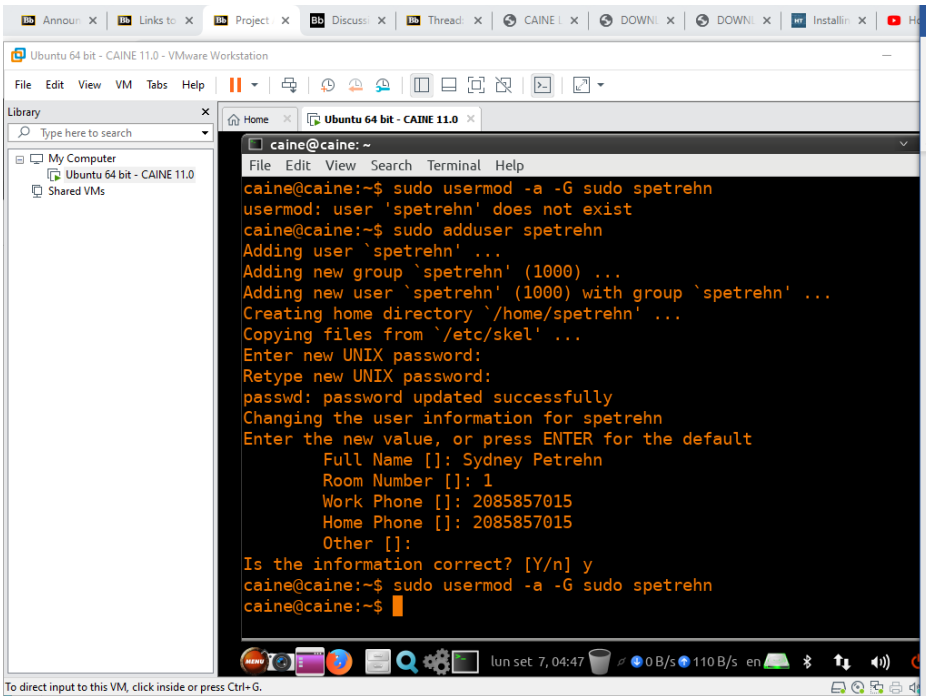
https://www.hackingtutorials.org/digital-forensics/installing-caine-8-0-on-a-virtual-machine/

I followed the tutorial step by step and had the same settings for my machine the only difference was that I am using a newer version of CAINE. In that tutorial they were using CAINE 8.0 however that did not affect my installation process. This tutorial got me to where I had CAINE installed and running on the Virtual Machine as shown below



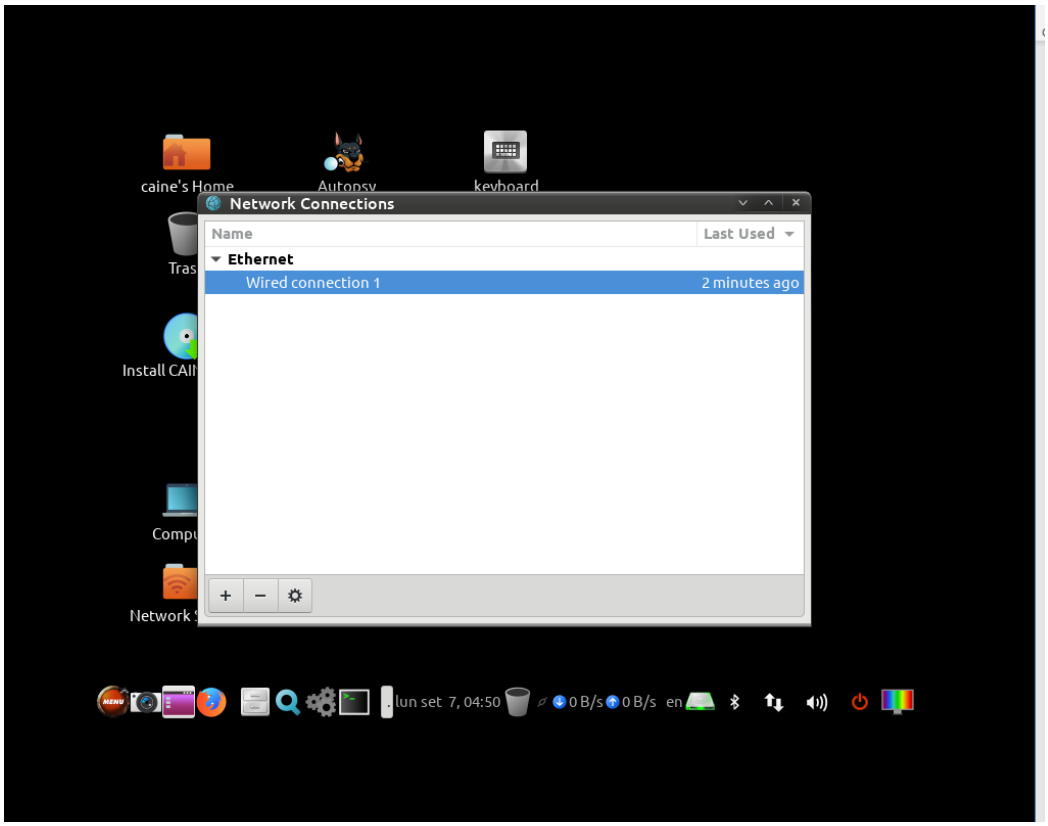
Next I created a unique username and password for my installation. I used the following command on the command line: sudo adduser spetrehn and then I set the password as CAIN!1 then I used `sudo usermod -a -G sudo spetrehn`



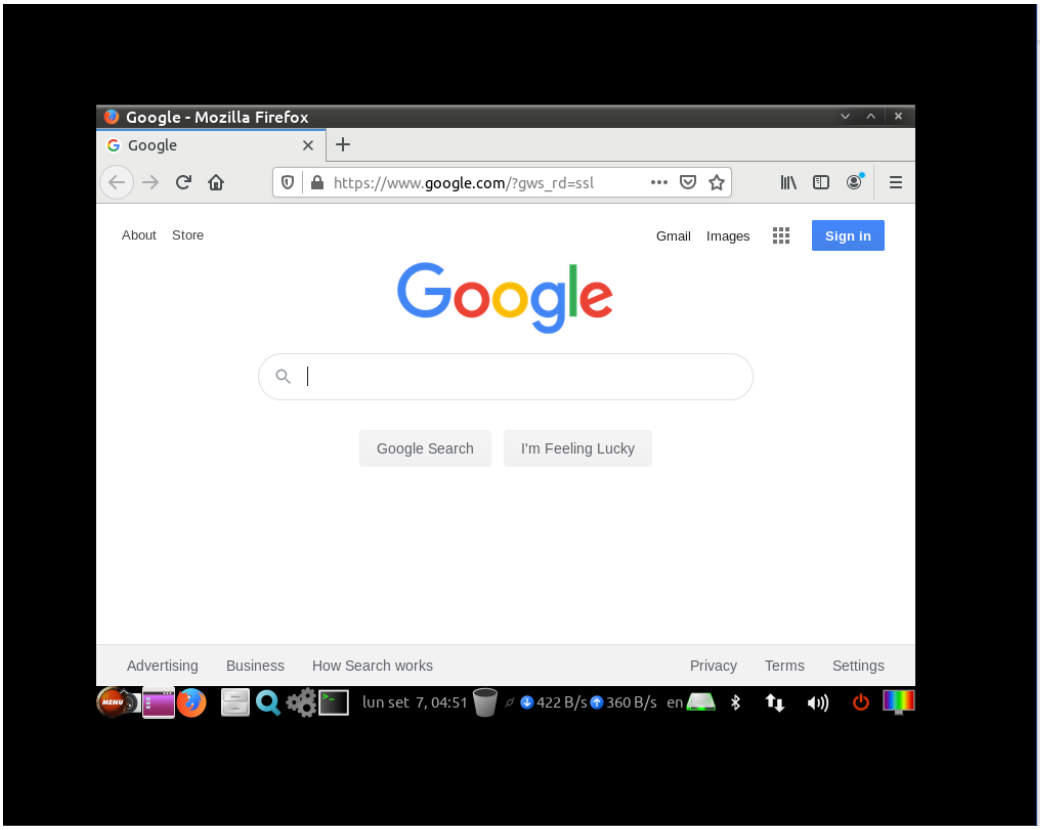


To get onto the internet I went here:

Once in the Internet screen I found there was the wired connection already established in the system and I assumed this was the WIFI my PC was running on already.

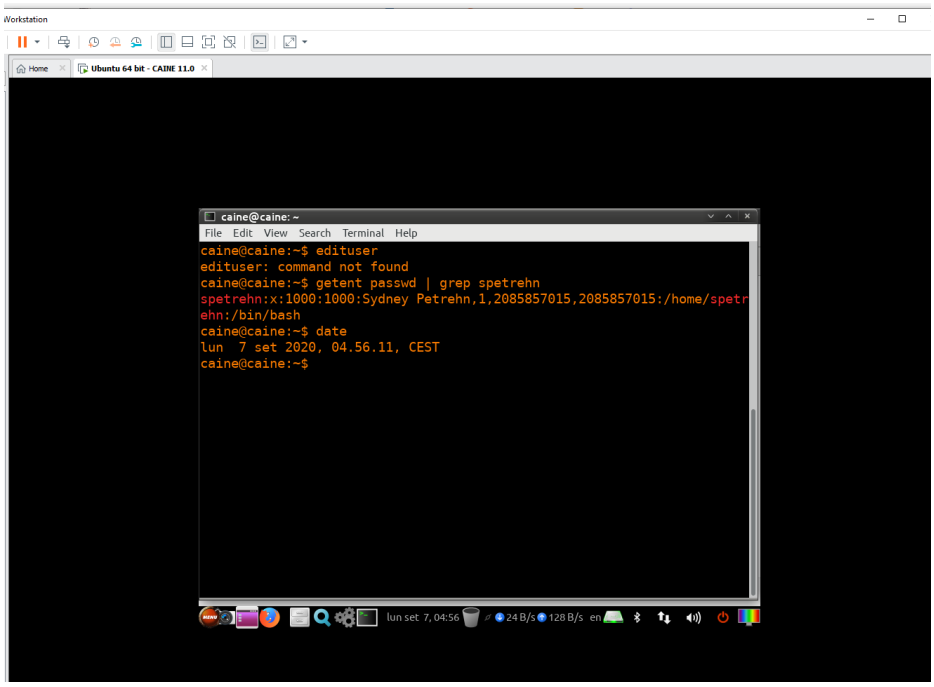


To test this theory I opened a version of Firefox and tried connecting to www.Google.com which was successful so I was already connected to the Internet.



Task 4: Report

Verification that this was successful with the date command screenshot provided below.


Workstation
Home
Ubuntu 64 bit - CAINE 11.0
caine@caine: ~
File Edit View Search Terminal Help
caine@caine:~$ edituser
edituser: command not found
caine@caine:~$ getent passwd | grep spetrehn
spetrehn:x:1000:1000:Sydney Petrehn,1,2085857015,2085857015:/home/spetrehn:/bin/bash
caine@caine:~$ date
lun 7 set 2020, 04.56.11, CEST
caine@caine:~$
lun set 7, 04:56
24 B/s 128 B/s
en