dondavinayreddy@gmail.com

Hands-On Lab: Malware Defense

To accompany Whitman and Mattord, Principles of Information Security, 7th Ed., 2022, ISBN 9780357506431; Malware Defense

Table of Contents

dondavinayreddy@gmail.com

Introduction

Malicious software (a.k.a. malware) has been an ever-present concern even before the recent explosion of networked devices known as Internet of Things. In this lab, you will explore a few options that are available to deal with the threat of viruses and other malware.

Objective

Upon completion of this activity, the student will be able to:

- Understand the basic setup and use of an open-source AV product.
- Install and use Clam AV on a Windows system.
- Using a USB storage device create a portable AV scanner.
- Understand what a YARA file is and how it is used.

These activities will help you complete future labs in this course.

Estimated Completion Time

If you are prepared, you should be able to complete:

- The Anti-virus/Malware labs in 1 to 1.5 hours, depending on the complexity of the computer being scanned.

Materials Required

Students will need their:

- laptop or desktop computer.
- USB device 8GB in size that can be formatted.
- Two downloads from Clam AV web site.

Minimum System Configuration

To complete the labs included, it is recommended that you operate them from a computer system (desktop or laptop) that is running Windows 10 and has:

- Intel i5 or better CPU
- 8 GB RAM (minimum) - 16 GB RAM (recommended)
- 1 TB Hard Drive with at least 250 GB free (minimum) - 350 GB free (recommended)
- Microsoft Windows 10 or latest version
- 8 Gb USB storage device

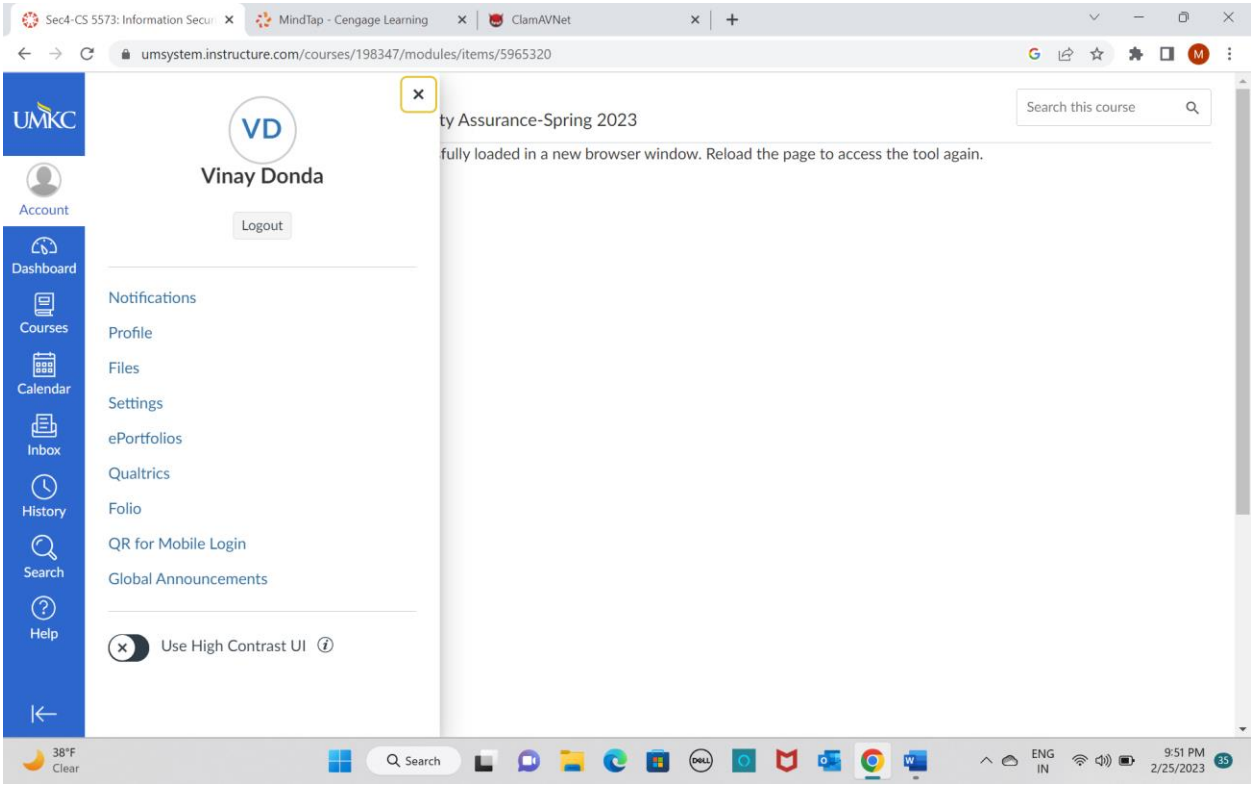
dondavinayreddy@gmail.com

Virus and Malware Prevention with Clam AV

This lab will be using Clam AV to introduce a standard open-source multiplatform signature-based antivirus engine. Clam AV runs on Windows, Linux, BSD, Solaris, and Macintosh operating systems. Clam AV also has multiple projects and tools based around the source code. Clam Av uses a virus database for managing signature and is extensible with YARA rules. We cover YARA rules further along in the lab. More information on Clam AV can be found in their documentation.

Downloading Clam AV

1. Open your preferred web browser and navigate to https://www.clamav.net/downloads#otherversions
2. This should present on the Alternate Versions of ClamAV downloads web page. I am testing on Windows 10 system 64-bit system. I will need to download the *portable.zip file and the .exe file shown in Figure L03-1. At the time of testing, clamav-0.103.2 is the latest version. Choose the latest version available.



dondavinayreddy@gmail.com

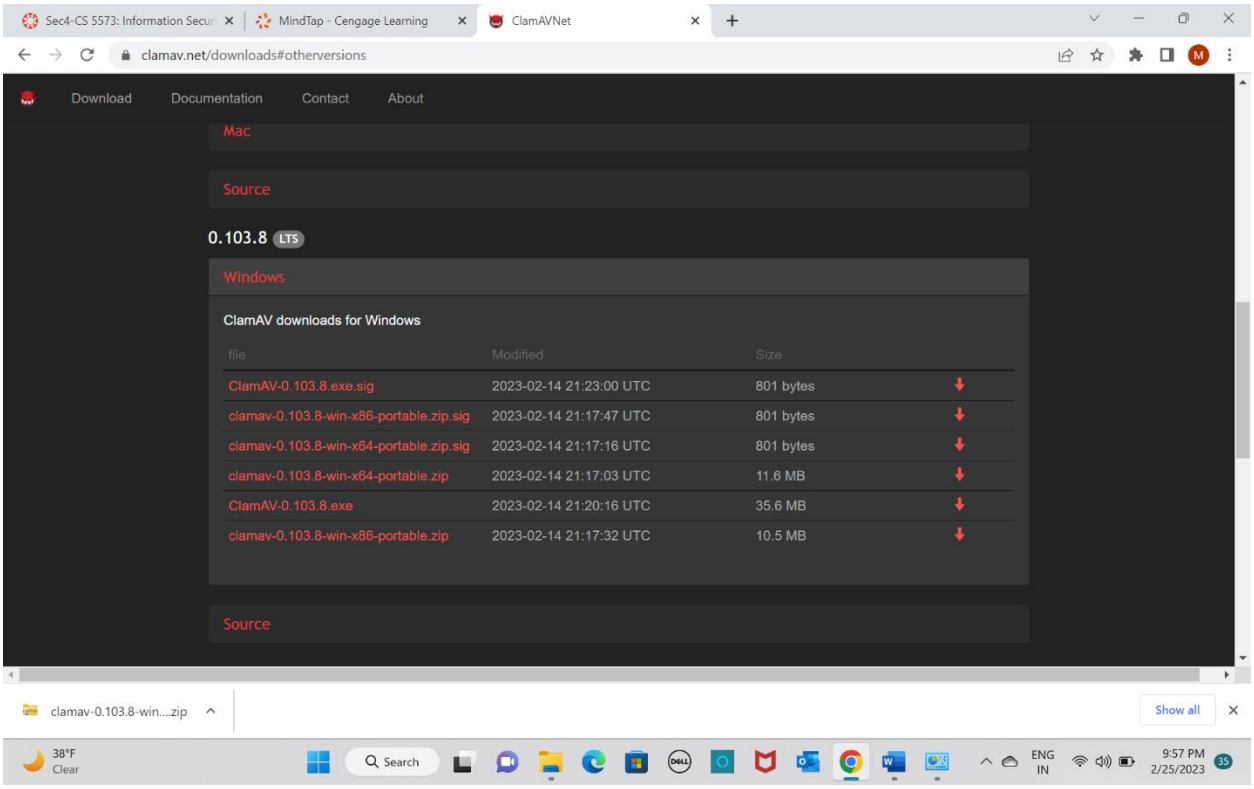
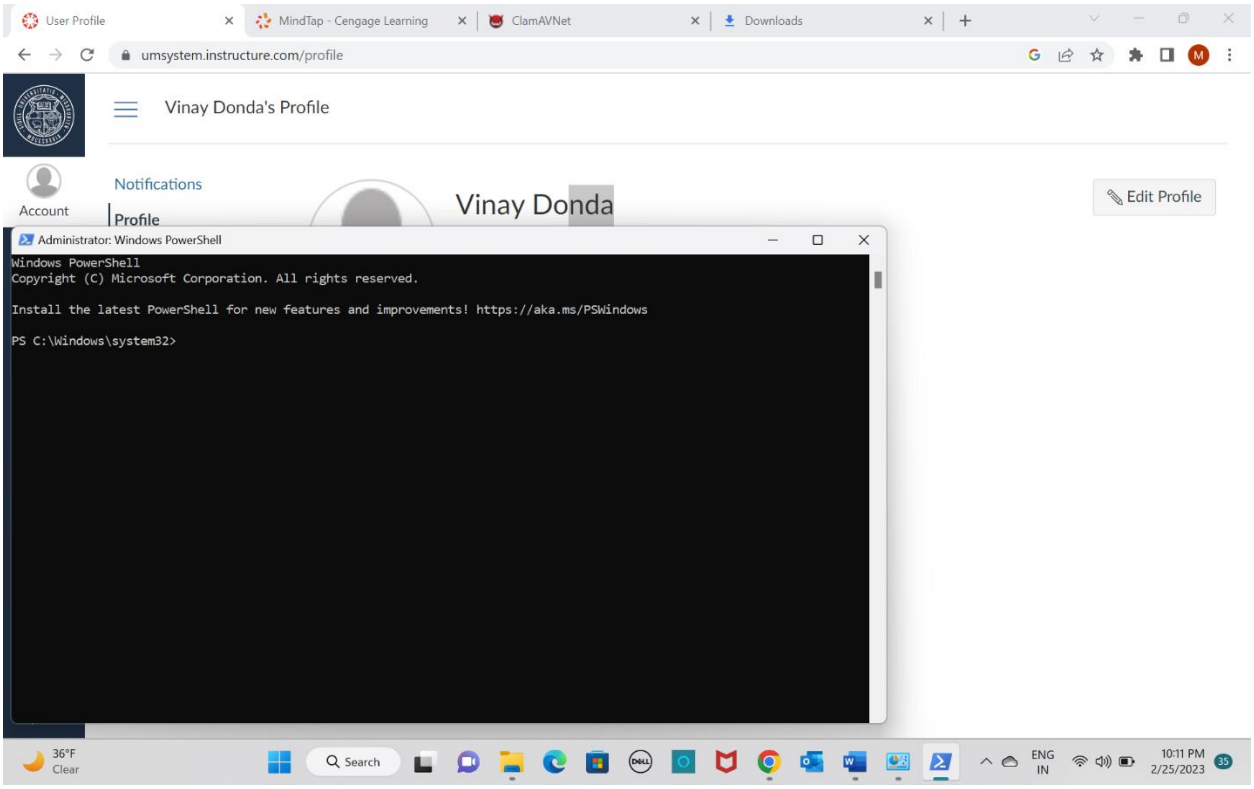


Figure L03-1 ClamAv dowload site Win64

Installing AVG

3. Using Windows Explorer, go to the location the file was downloaded and double click it or double click the downloaded file from your web browser.
4. Follow the instructions to install Clam AV. Use the defaults provided. You may need to authorize the execution of the program if you get a Windows pop-up asking for permission.
5. You will need to open a PowerShell Command Line Interface (CLI) in order to complete the installation. In the Windows Search Bar, type PowerShell, navigate your mouse over the application in the menu, right click, and select “Run as administrator”.
6. Change to the Clam AV installation directory by typing:
    a. **cd "c:\program files\clamav"**.
7. In the PowerShell window preform the following commands.
    a. **copy .\conf_examples\freshclam.conf.sample .\freshclam.conf**
    b. **copy .\conf_examples\clamd.conf.sample .\clamd.conf**

dondavinayreddy@gmail.com



dondavinayreddy@gmail.com

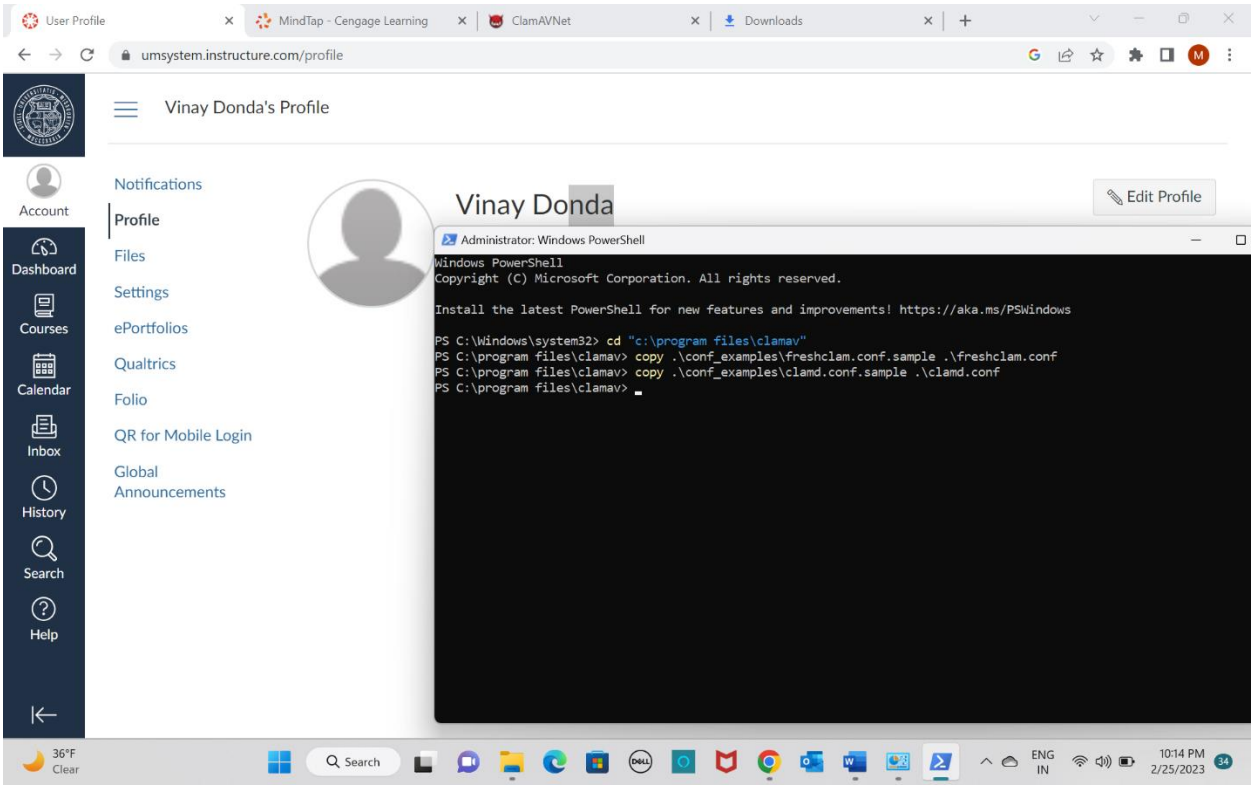
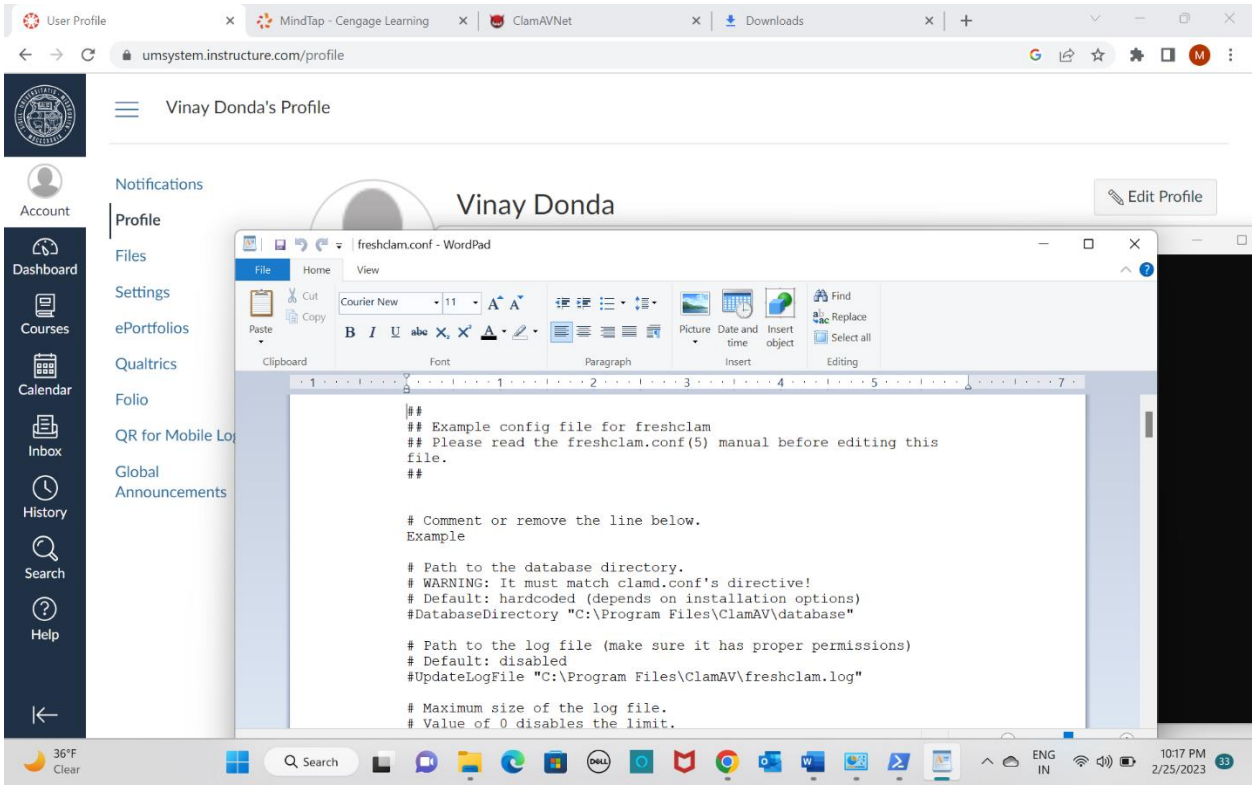
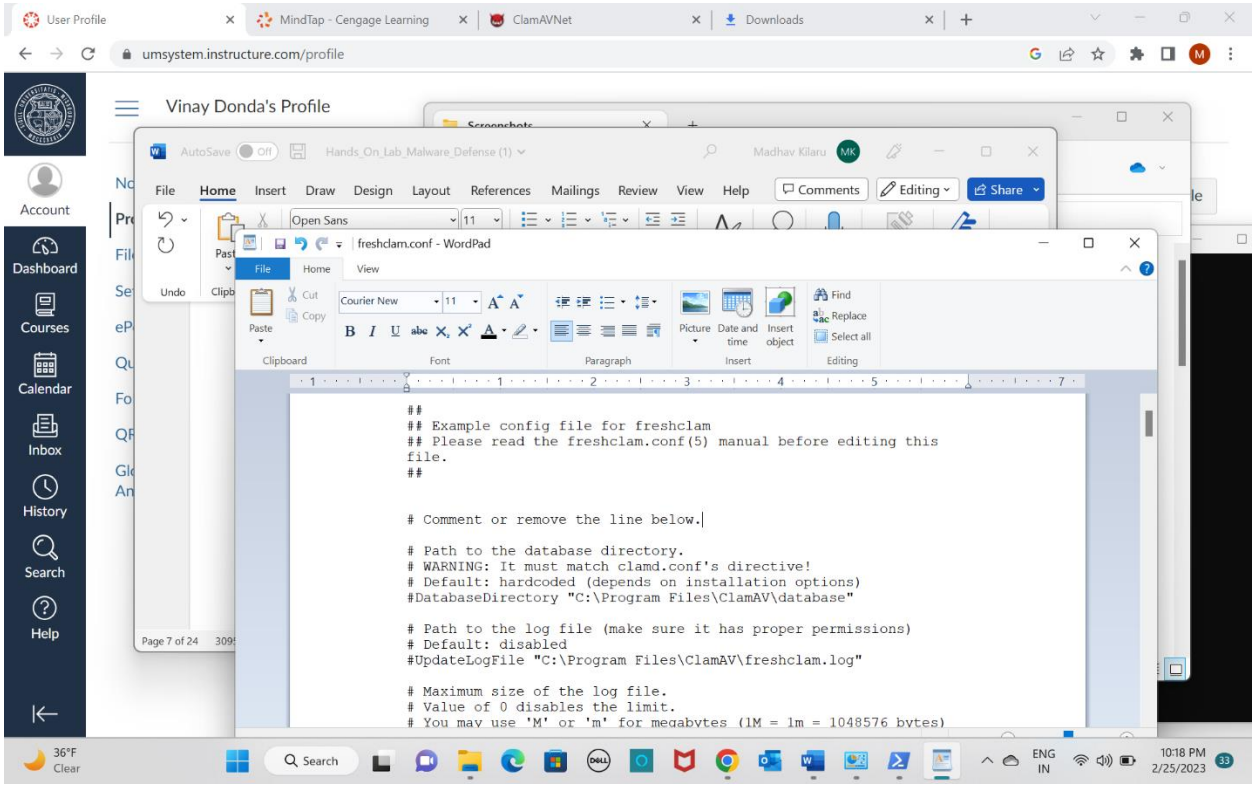


Figure L03-2 PowerShell commands for ClamAV

8. Next, we will run the write.exe command. This will open the specific conf file (short for config) in WordPad and allow us to delete the line that says “Example” as shown in Figure 3.
    a. **Write.exe .\freshclam.conf**
    b. Save the file and close WordPad

dondavinayreddy@gmail.com





dondavinayreddy@gmail.com

9. Repeat the same procedure for clamd.conf
    a. **Write.exe .\clamd.conf**
    b. Save the file and close WordPad

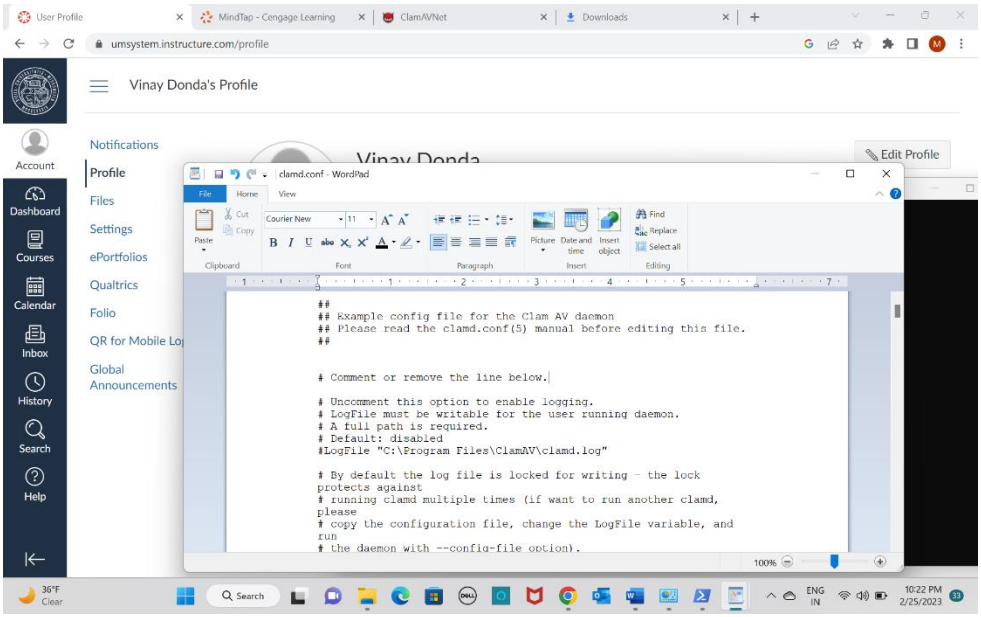
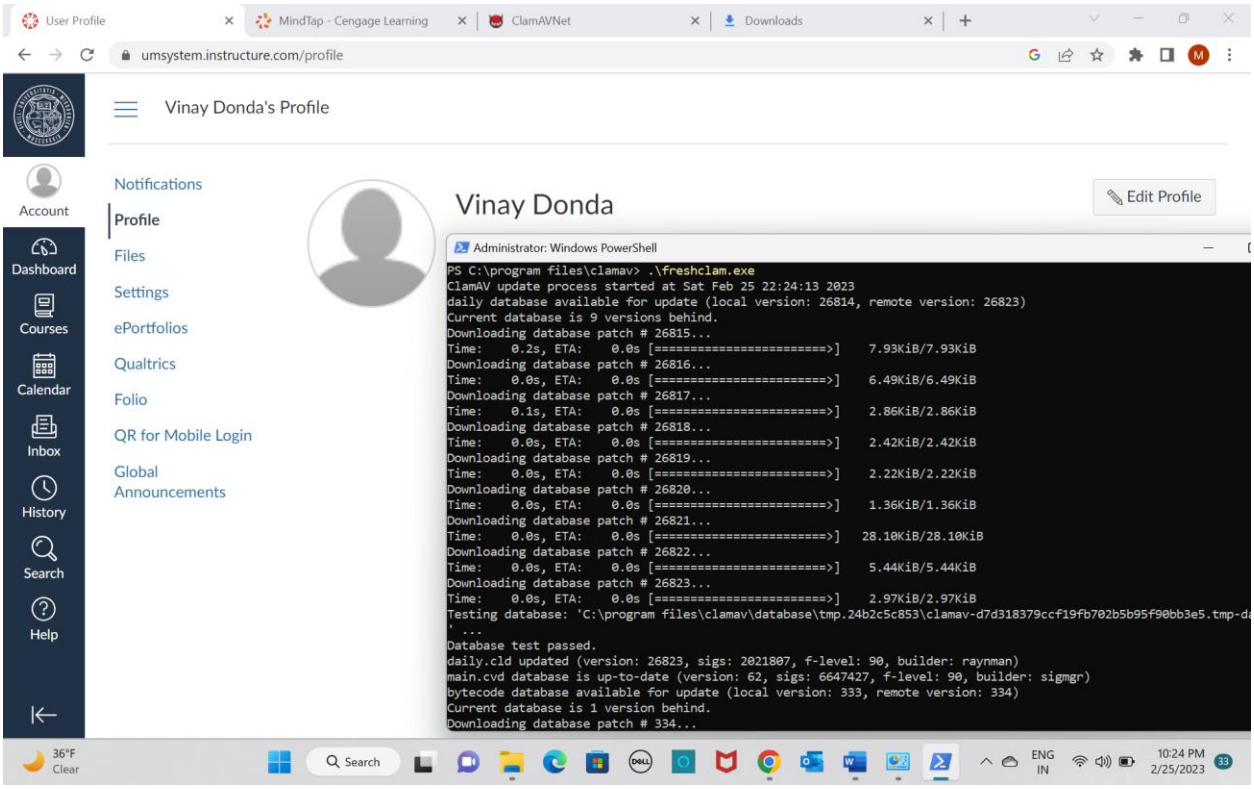


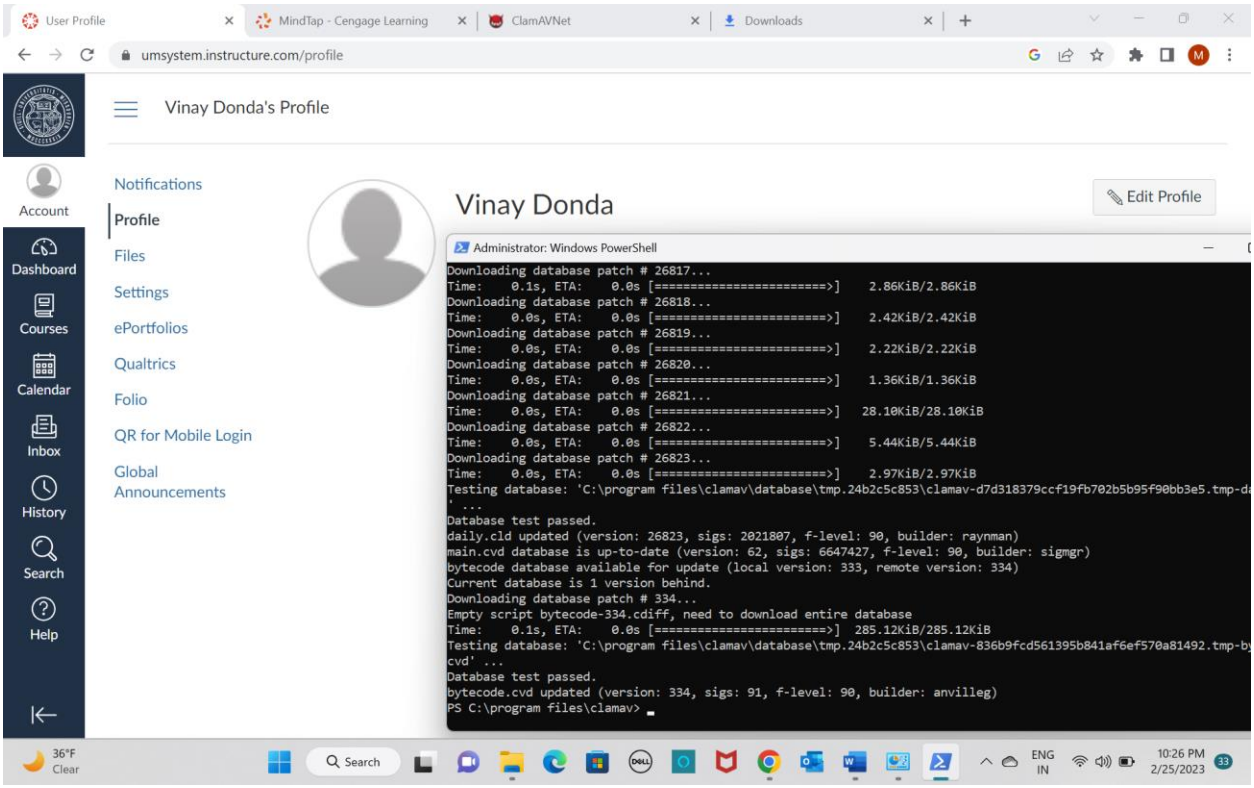
Figure L03.3 Delete "Example" from the conf file

10. Next, update the ClamAV Database. In the PowerShell window run:
    a. **.\freshclam.exe**

11. Provide a screen shot of your Power Shell window showing a successful update to Clam AV.

dondavinayreddy@gmail.com

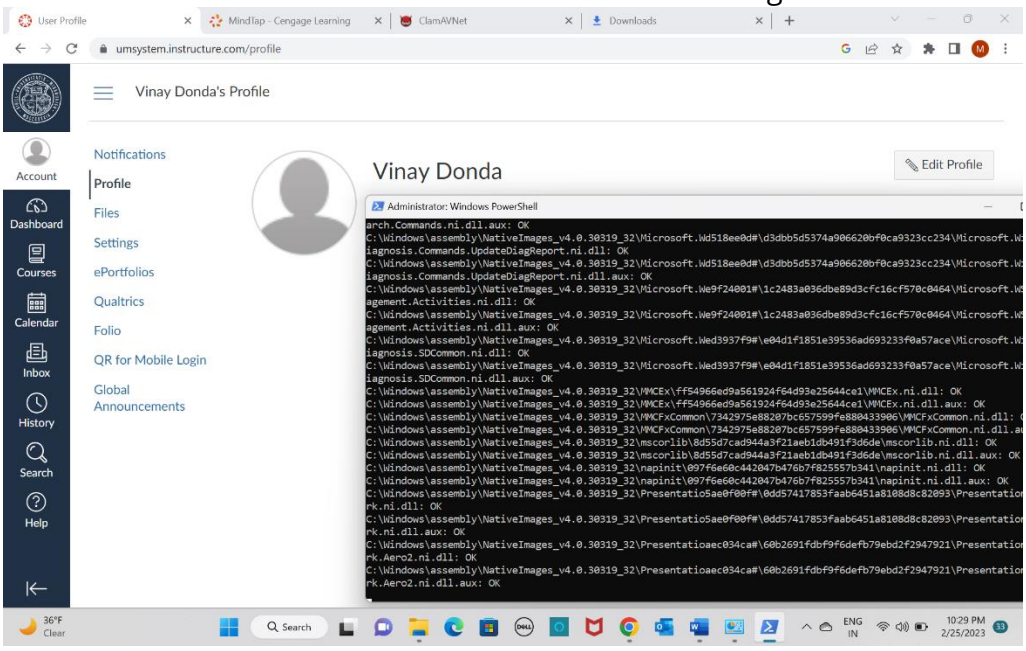


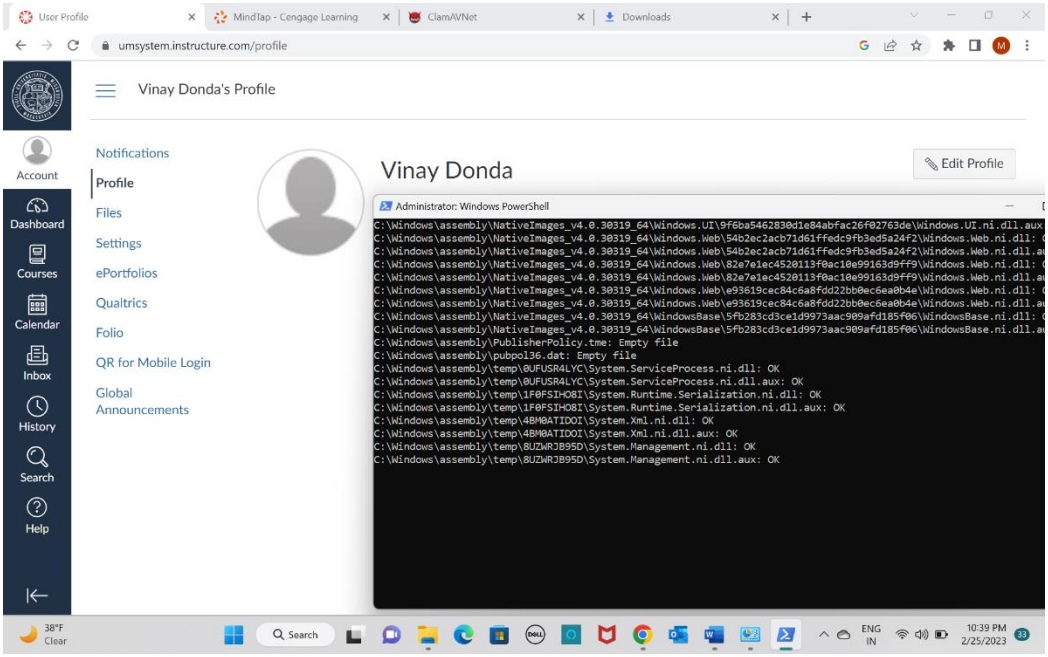


Scanning the Local System with AVG

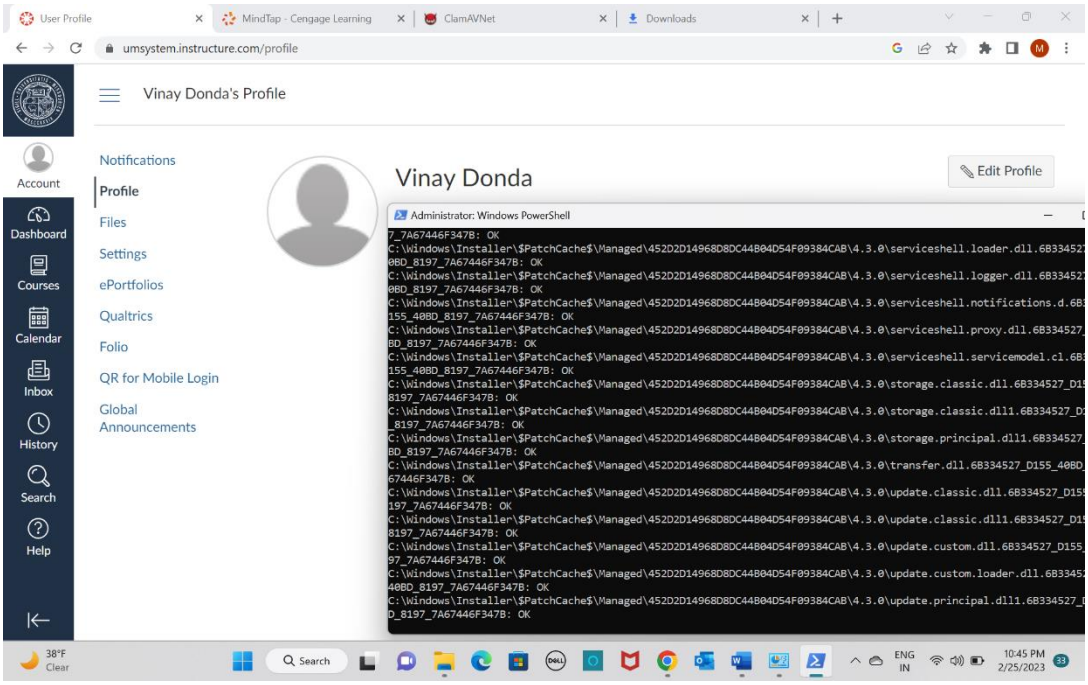
dondavinayreddy@gmail.com

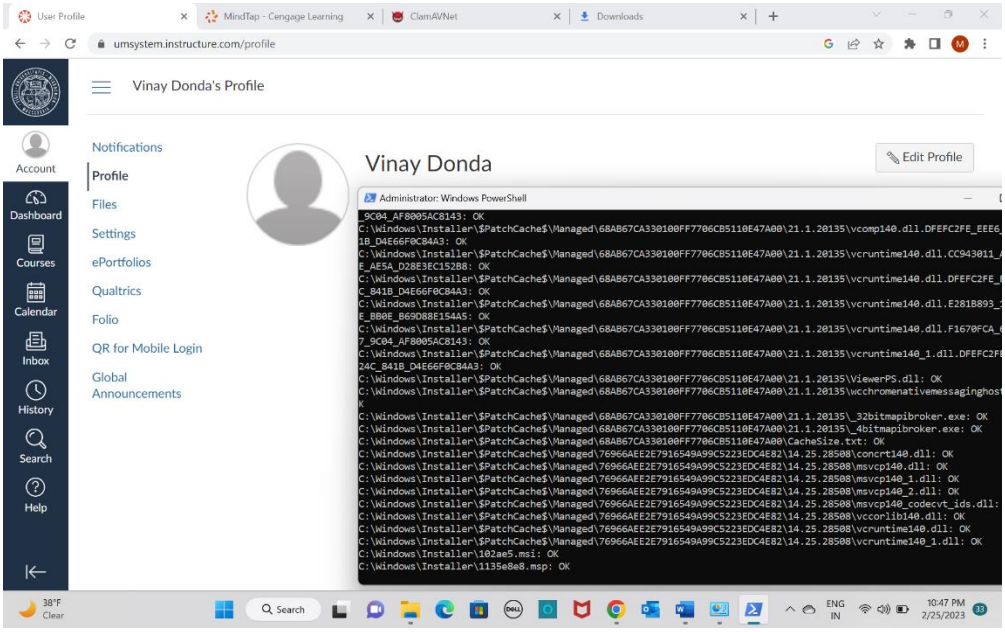
12. Now that Clam AV is installed on the system and the virus database is updated, we will perform a scan of the c: drive or [root] drive. In the PowerShell windows type:
    a. `.\clamscan.exe "C:\Windows" -r` (This will take some time to run)
    b. The PowerShell screen should start to scroll showing the files that have been scanned and if the files are OK or malicious as seen in Figure L03-5.



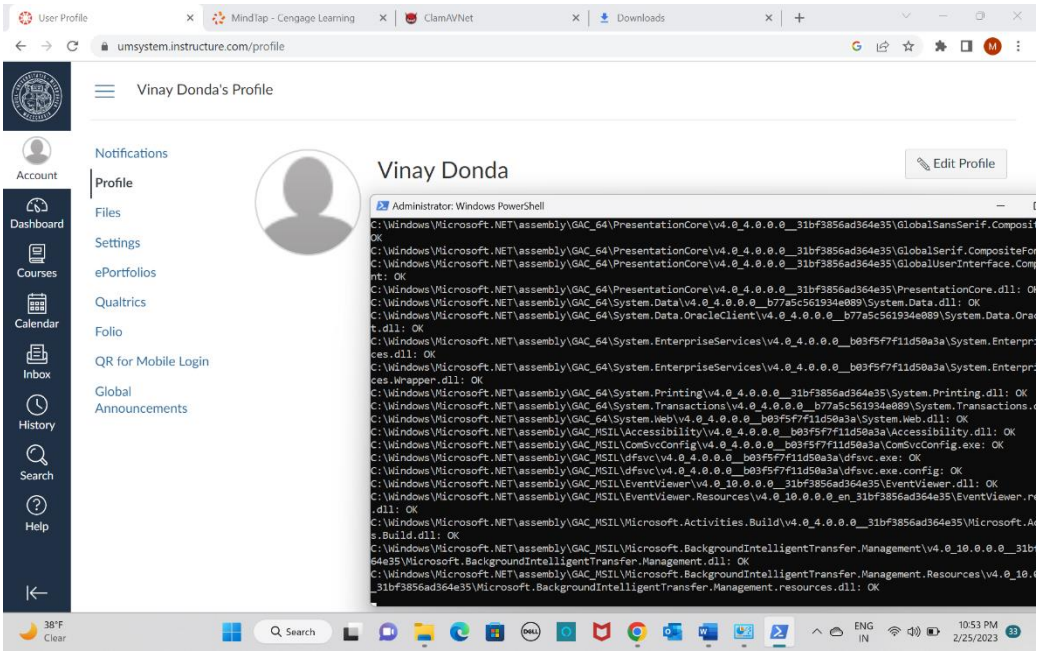


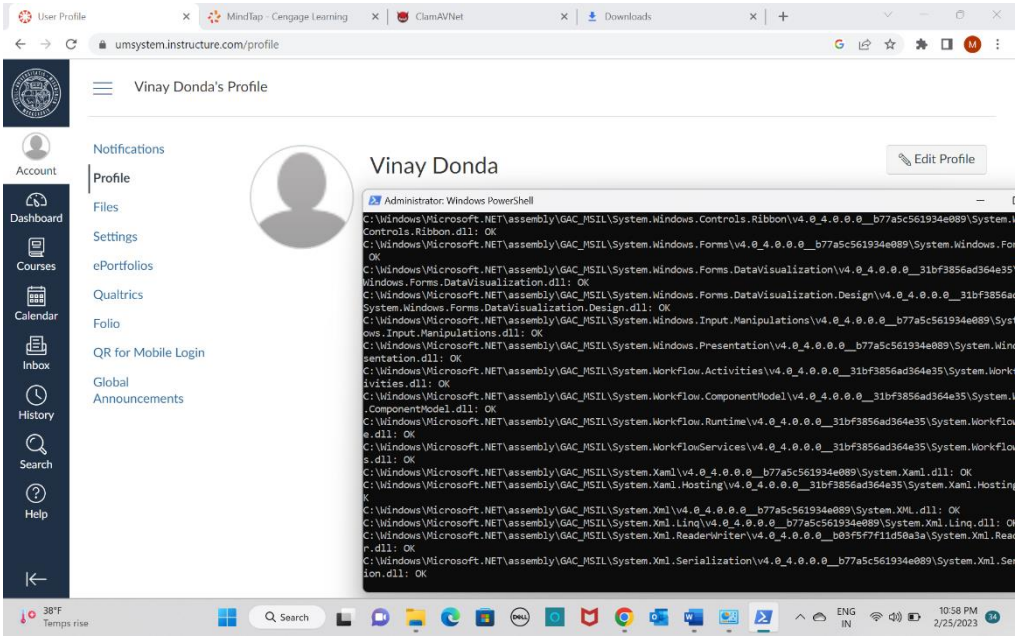
dondavinayreddy@gmail.com





dondavinayreddy@gmail.com





dondavinayreddy@gmail.com

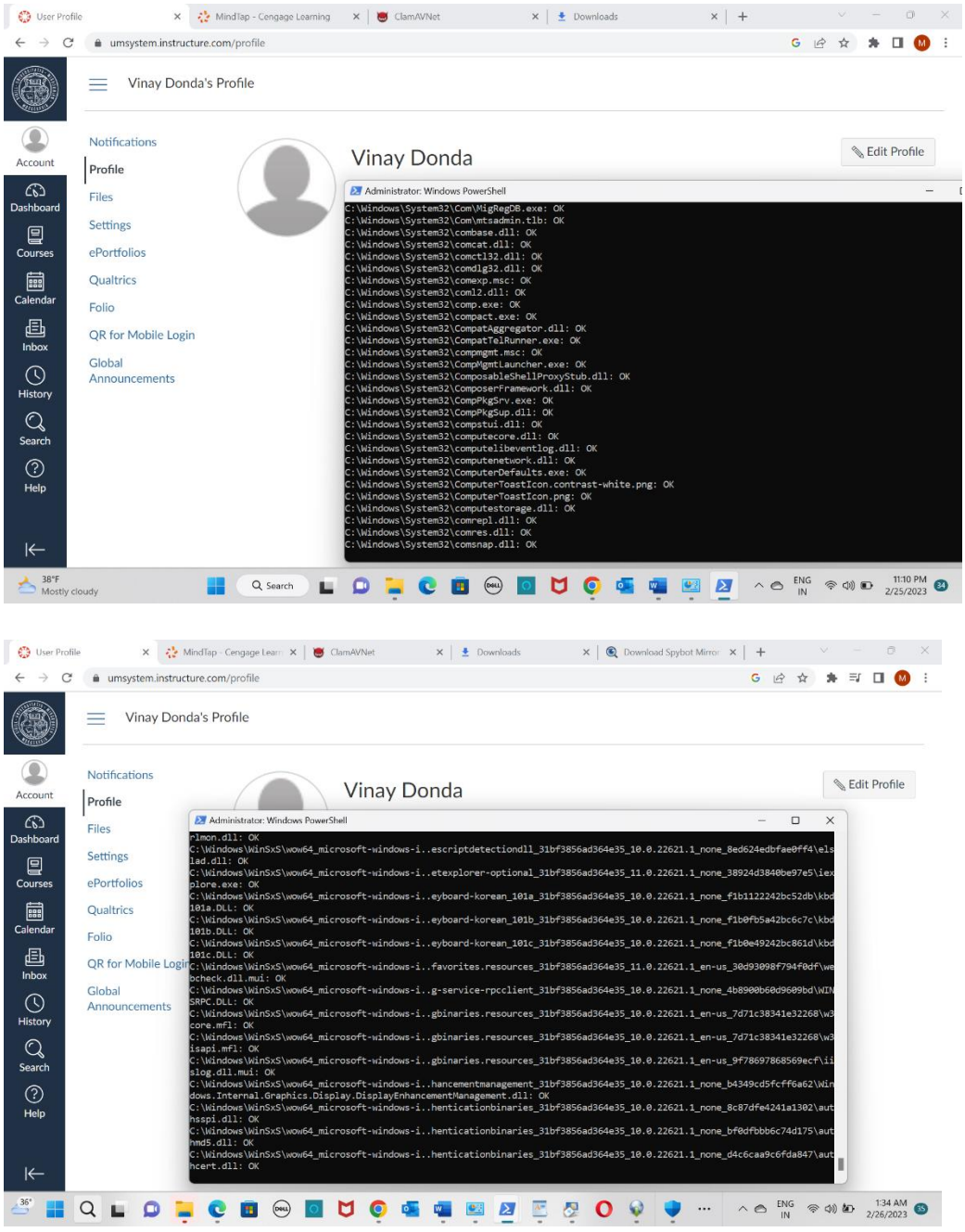
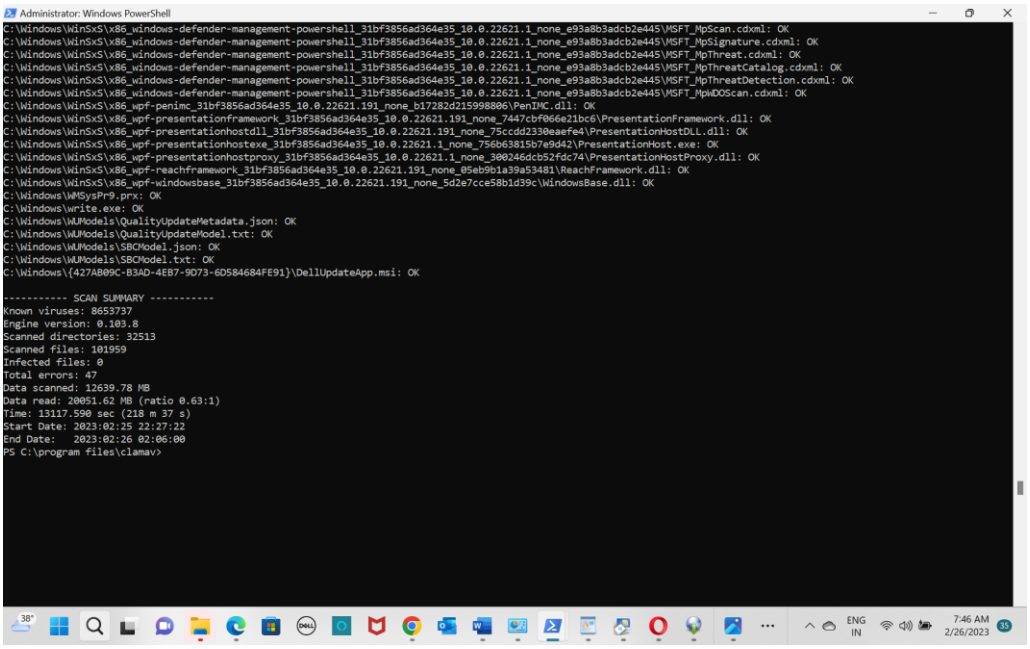


Figure L03-4 ClamAV scanning files

13. Provide a Screen shot of the PowerShell window showing a completed scan.

dondavinayreddy@gmail.com



Installing ClamAV to a USB device

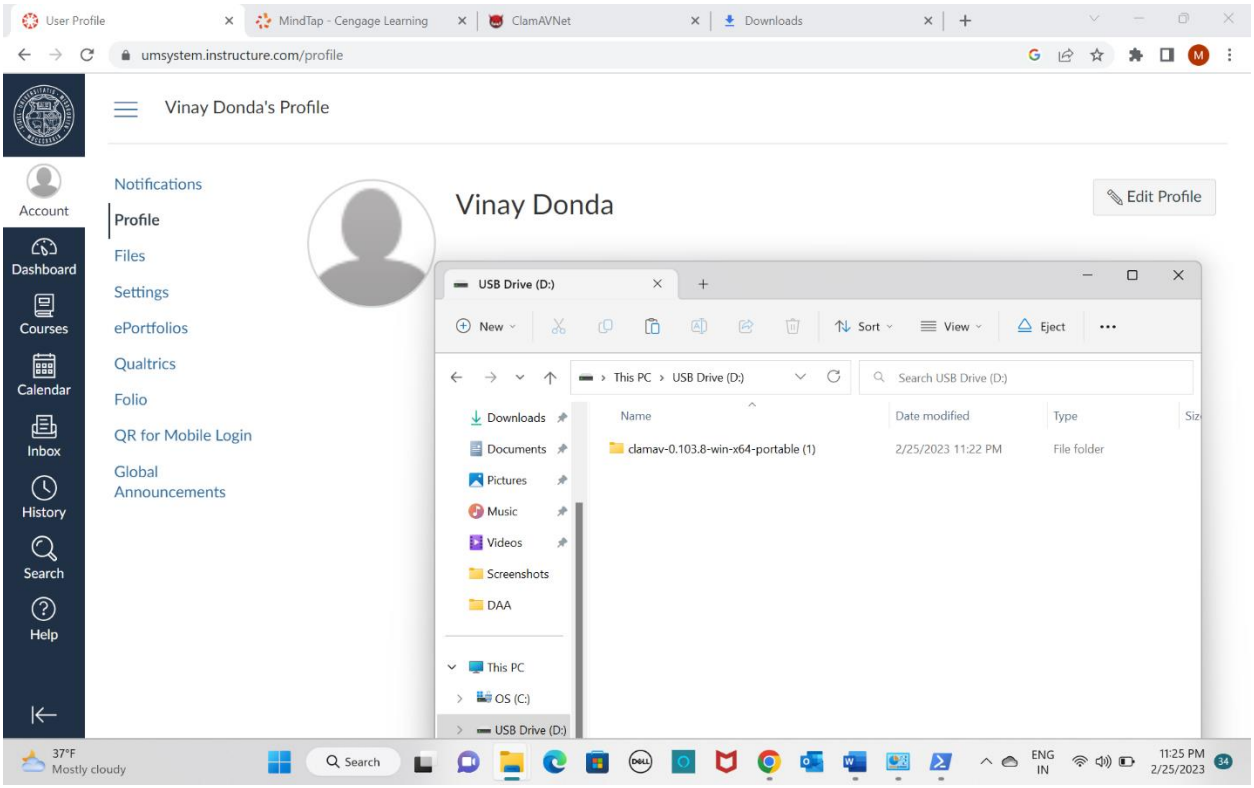
dondavinayreddy@gmail.com

The next section we will the portable version of ClamAV and install it on a USB drive. This is a useful tool to have if an analyst needs to scan systems that can't have active antivirus installed or are separated from the internet.

14. Insert your 4Gb or larger USB device. You should backup and relocate any files that you need to keep that are present om the device.

15. Using Windows Explorer, go to the location the file, "*portable.zip" was downloaded and double click it in the default Zip Application.

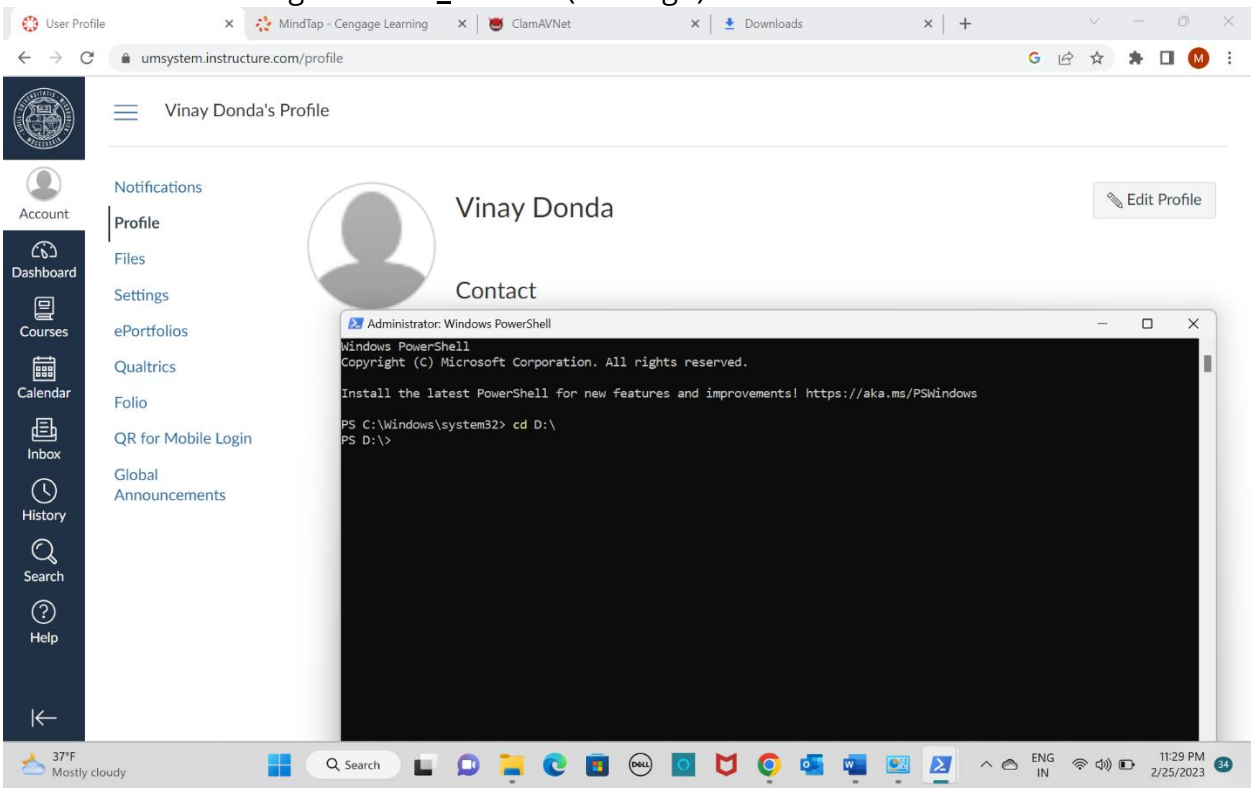
16. Extract the folder contained in the "*portable.zip" file to the USB device. We are using 7zip in the example shown in figure L03-6.



dondavinayreddy@gmail.com

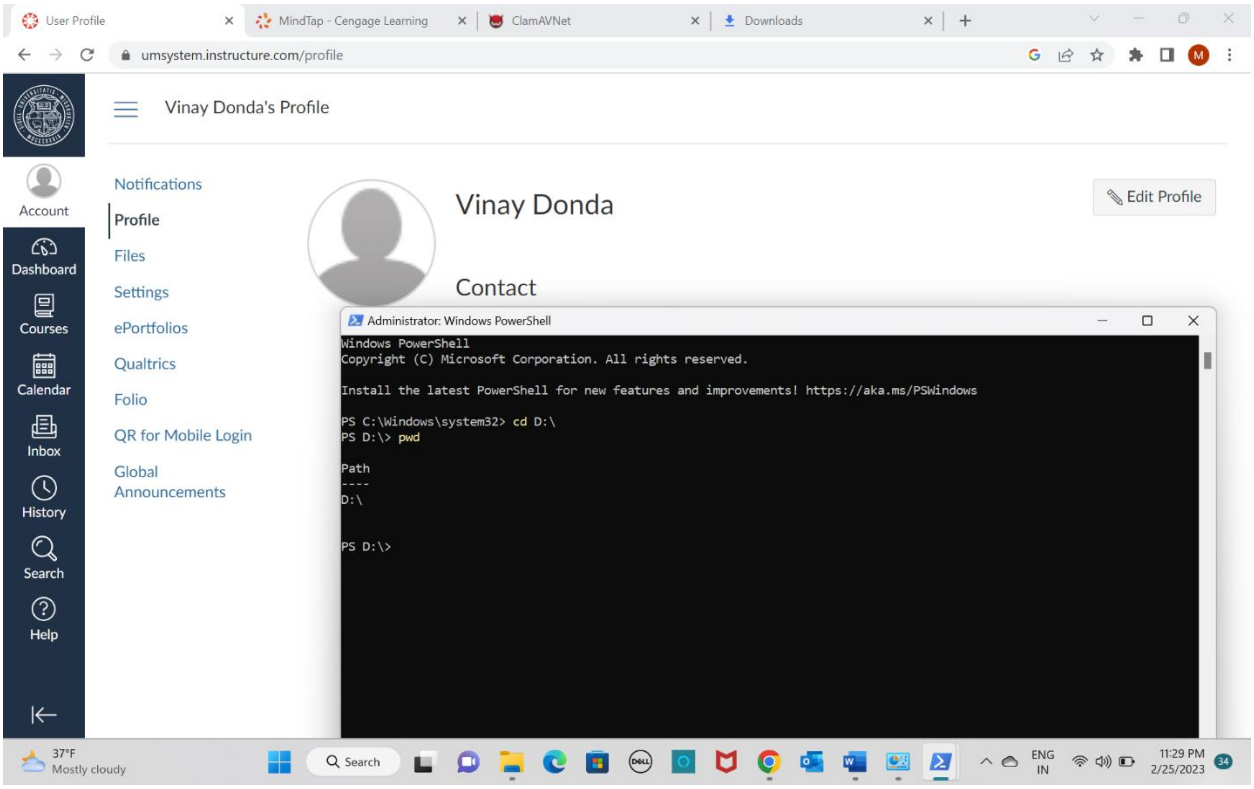
Figure L03-5 Using 7zip to extract the zip file

17. Now we perform the same procedure we did above to prepare ClamAV. Open up or return to your PowerShell window opened with administrative privileges. Navigate to the USB drive using **cd <drive_letter>:** (i.e. cd g:\)



18. Type **pwd** in the PowerShell window to verify you're on the root of your USB device.

dondavinayreddy@gmail.com



19. In the PowerShell window, perform the following commands.
    a. **copy .\conf_examples\freshclam.conf.sample .\freshclam.conf**
    b. **copy .\conf_examples\clamd.conf.sample .\clamd.conf**

dondavinayreddy@gmail.com

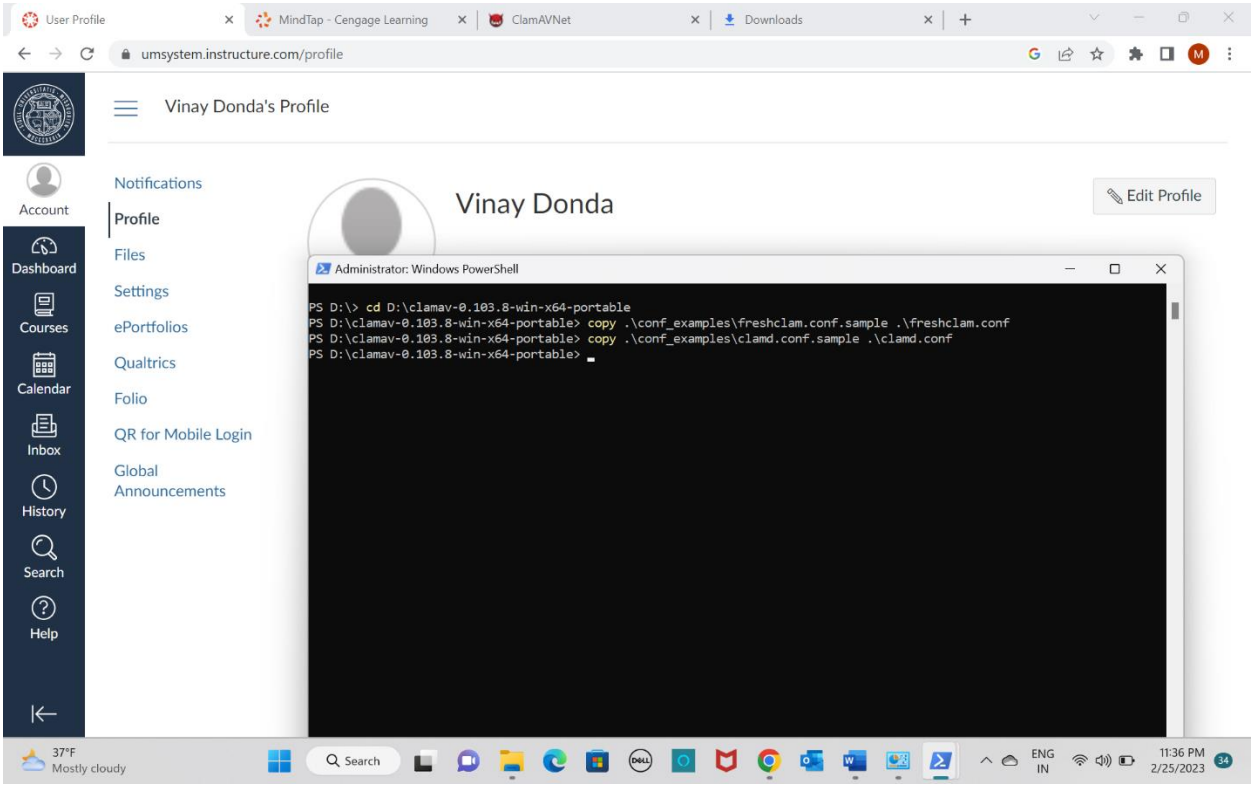
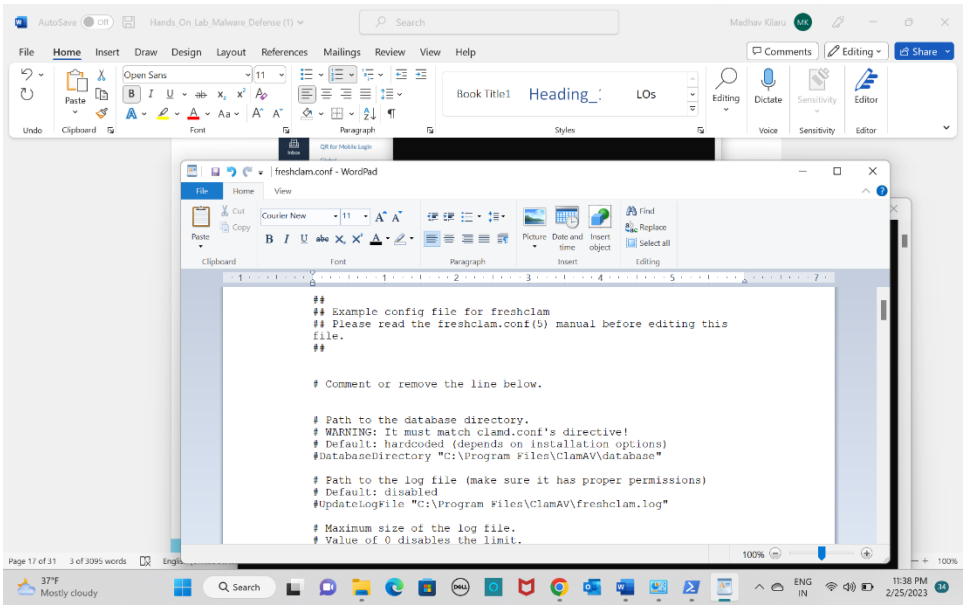


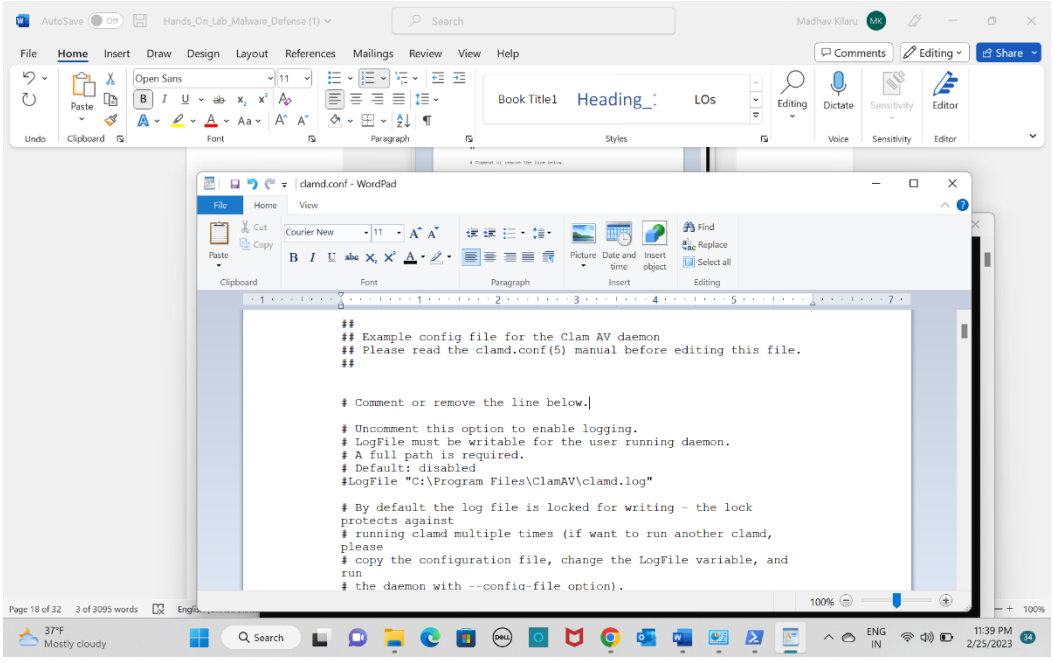
Figure L03-6 PowerShell commands on USB device

20. Next, we will run the write.exe command. This will open the specific conf file (short for config) in WordPad and allow us to delete the line that says “Example” as shown in Figure 3.
    a. **Write.exe .\freshclam.conf.**
    b. Save the file and close WordPad.

dondavinayreddy@gmail.com

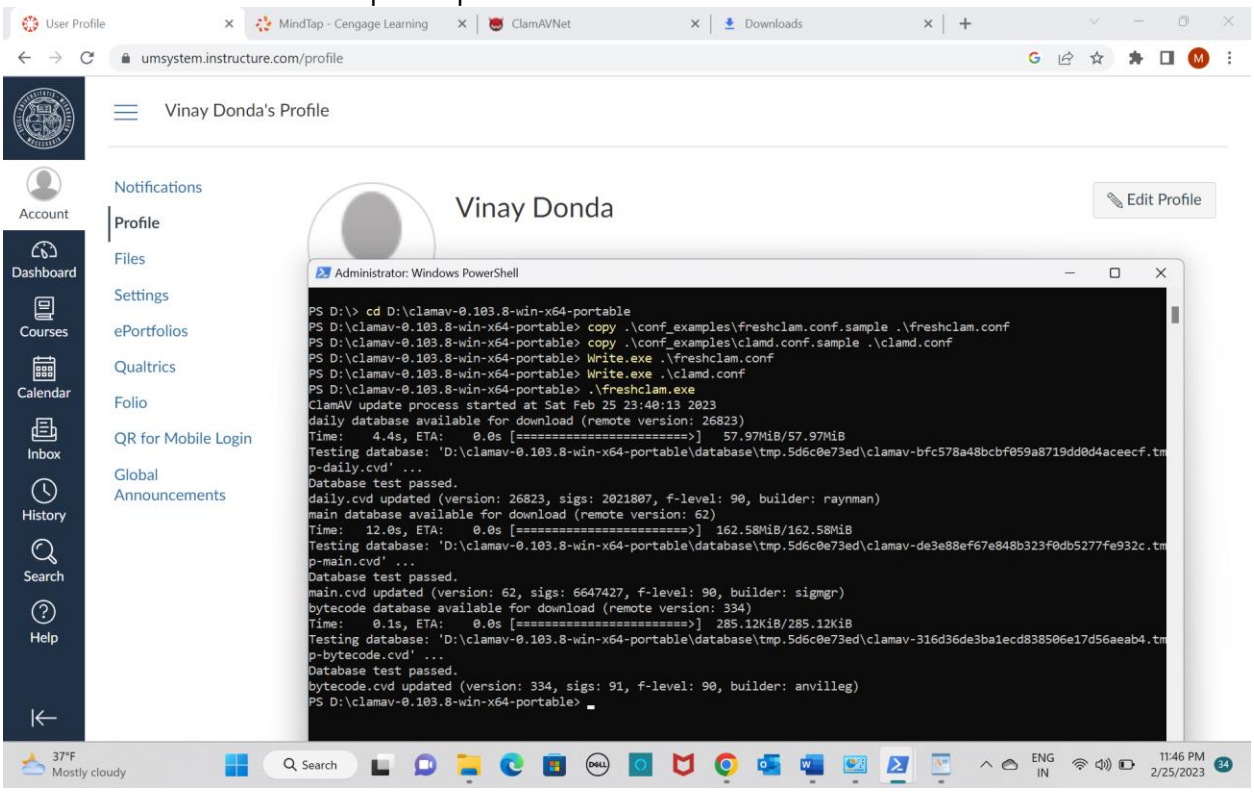


21. Repeat the same procedure for clamd.conf.
    a. **Write.exe .\clamd.conf** .
    b. Save the file and close WordPad.



dondavinayreddy@gmail.com

22. Next, update the ClamAV Database. In the PowerShell window, run:
    a. **.\freshclam.exe**
23. Save a screen shot of the update performed on the USB device.



YARA Rules in Information Security

dondavinayreddy@gmail.com

Composing a YARA Rule for use in ClamAV is beyond the scope of this lab. However, it is important to talk about how YARA rules are used in information security and more specifically malware research and detection.

YARA Rules are tools used primarily for malware research and detection. It was originally developed by Victor Alvarez of Virus Total. These are rules used to scan files, memory images, or network traffic looking for textual or binary patterns that match known malware samples. YARA rules use strings and Boolean expressions to apply different conditions as well as a modified form of PERL regular expressions.

YARA Rules basically allows analyst to react write custom rules and updates for multiple information security platforms at one time. These can be very useful when an IR analyst has discovered an indicator of compromise for a malware and wants generate a rule to alert on the presence of that malware. As an example, A YARA rule written to detect a bad string in a file can also be applied to a tool like volatility.exe and used to scan a memory image for the same malicious strings. Rules that are well written and tested can be applied for detection in IDS/IPS devices monitoring network traffic as well as next generation firewalls.

```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        threat_level = 3
        in_the_wild = true

    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"

    condition:
        $a or $b or $c
}
```

Figure L03-7 YARA Rule Example

In Figure L03 8 is an example of simple example of a YARA Rule. The rule name is “silent_banker”, it looks for three specific strings ($a,$b,$c) and it will alert if it finds any of those three strings based on the condition statement.

When finished with this lab, uninstall AVG, and reboot the computer.

dondavinayreddy@gmail.com

Malware Detection with Spybot Search & Destroy

Another leading free anti-malware tools available today is Spybot Search & Destroy. Unlike traditional antivirus/anti-malware software, Spybot S&D is on demand, meaning it doesn't run all the time, monitoring your systems. If you purchase the upgraded version of Spybot + AV, it will provide real-time anti-virus protection. The free version, however, does not provide AV support. Begin by checking to see if Spybot S&D has already been installed on your system.

1. Click the **Windows Start** button and scroll down the list of installed applications that appears on the right. Look for Spybot S&D. If it is installed, skip the installation process that follows.

Installing Spybot S&D

2. Using a Web browser, go to https://www.safer-networking.org/download/.
3. Select one of the *Safer-Networking Ltd.* Mirror sites to download the software, as shown in Figure L03-9. noting the location where the **.exe** is stored (note your version may be labeled differently). Note you may find a newer version than this.

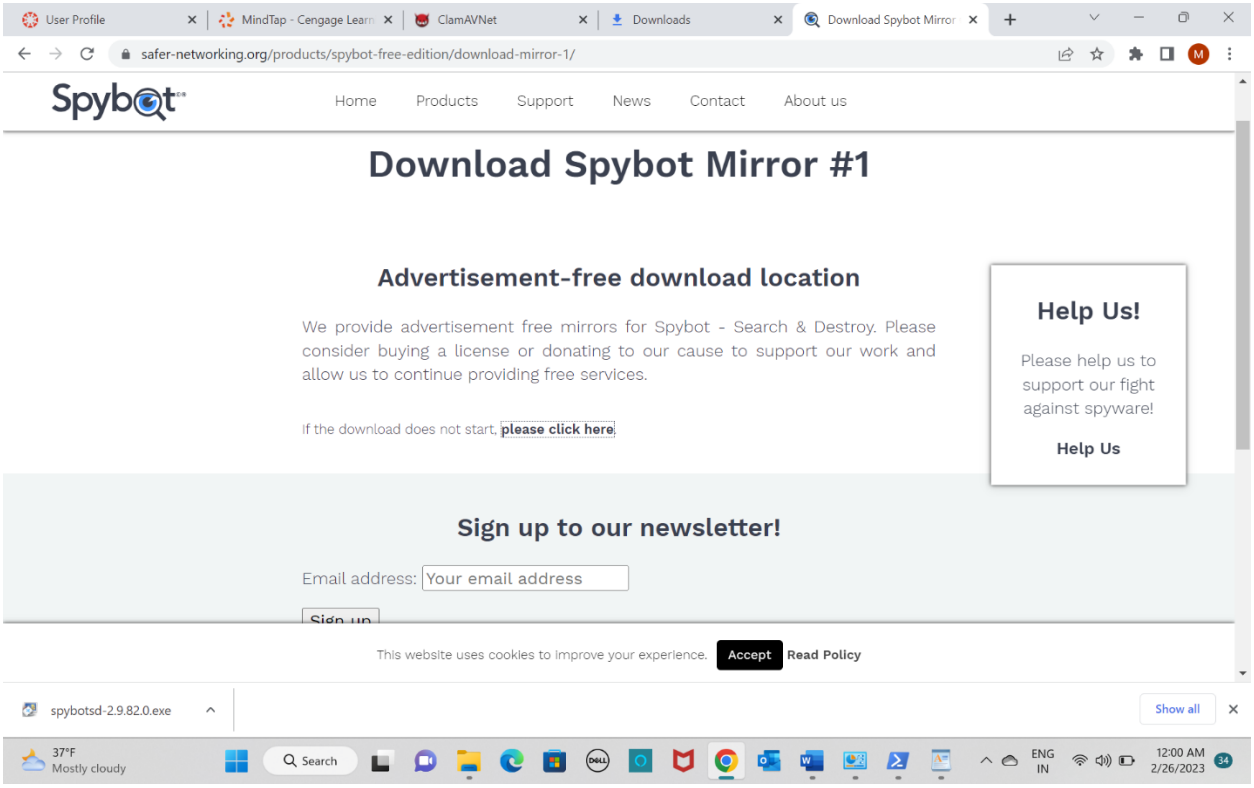


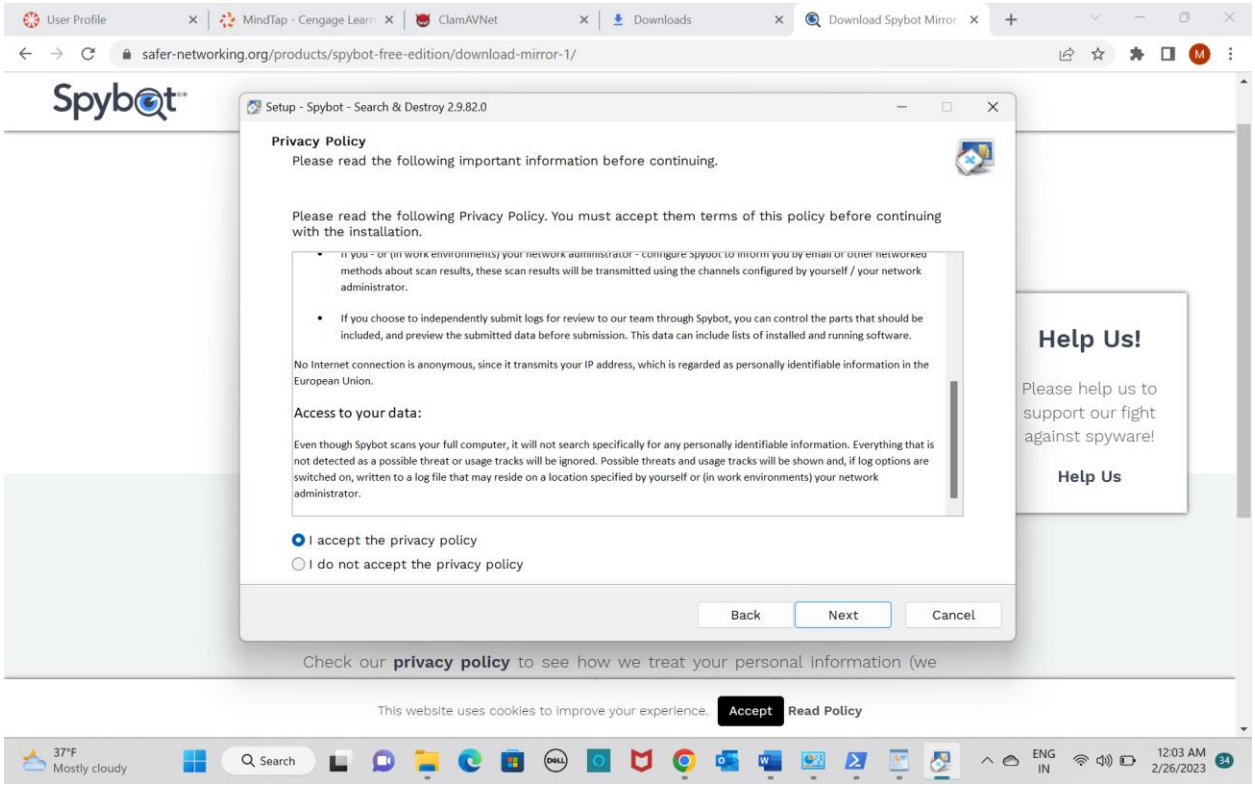
Figure L03-9 Spybot Download Locations

4. Using Windows Explorer, go to the location the file was downloaded and double click the .exe file, or click on the link at the bottom of your web browser to install Spybot S&D. Follow the instructions on the screen to complete the installation,

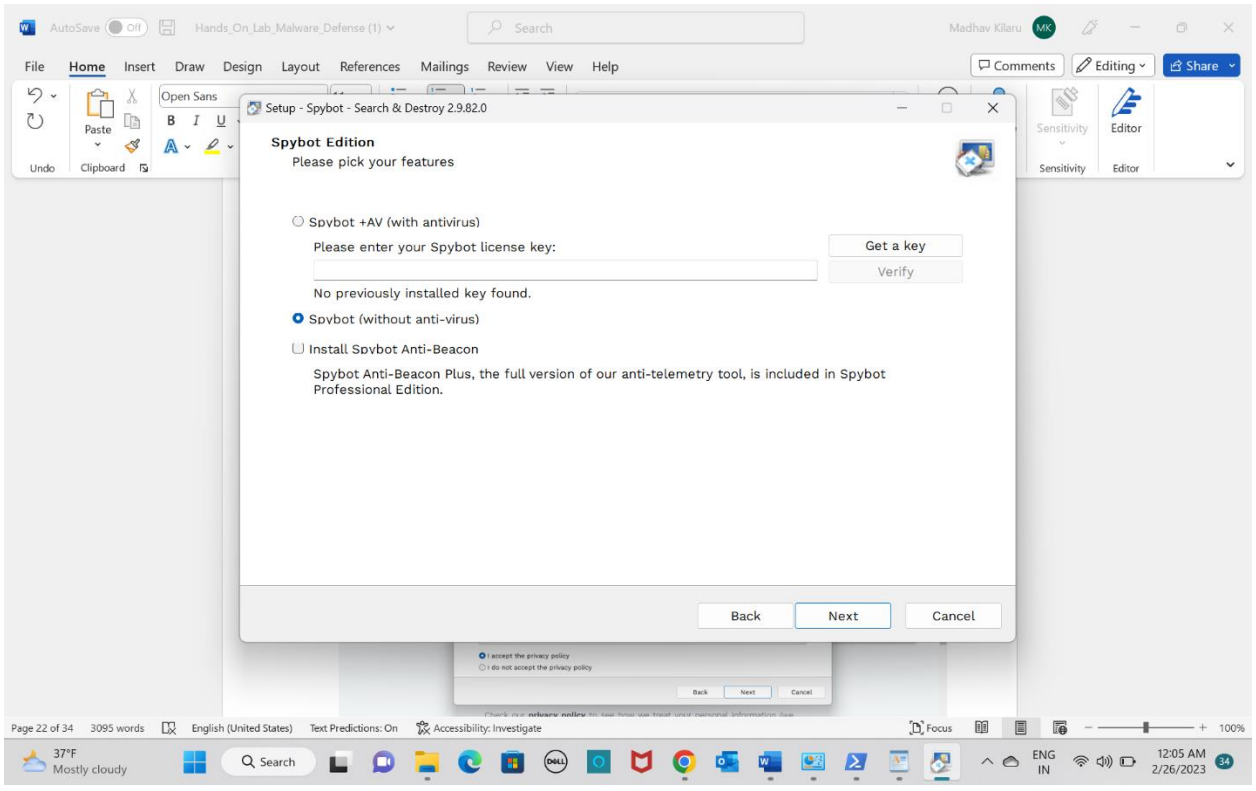
dondavinayreddy@gmail.com

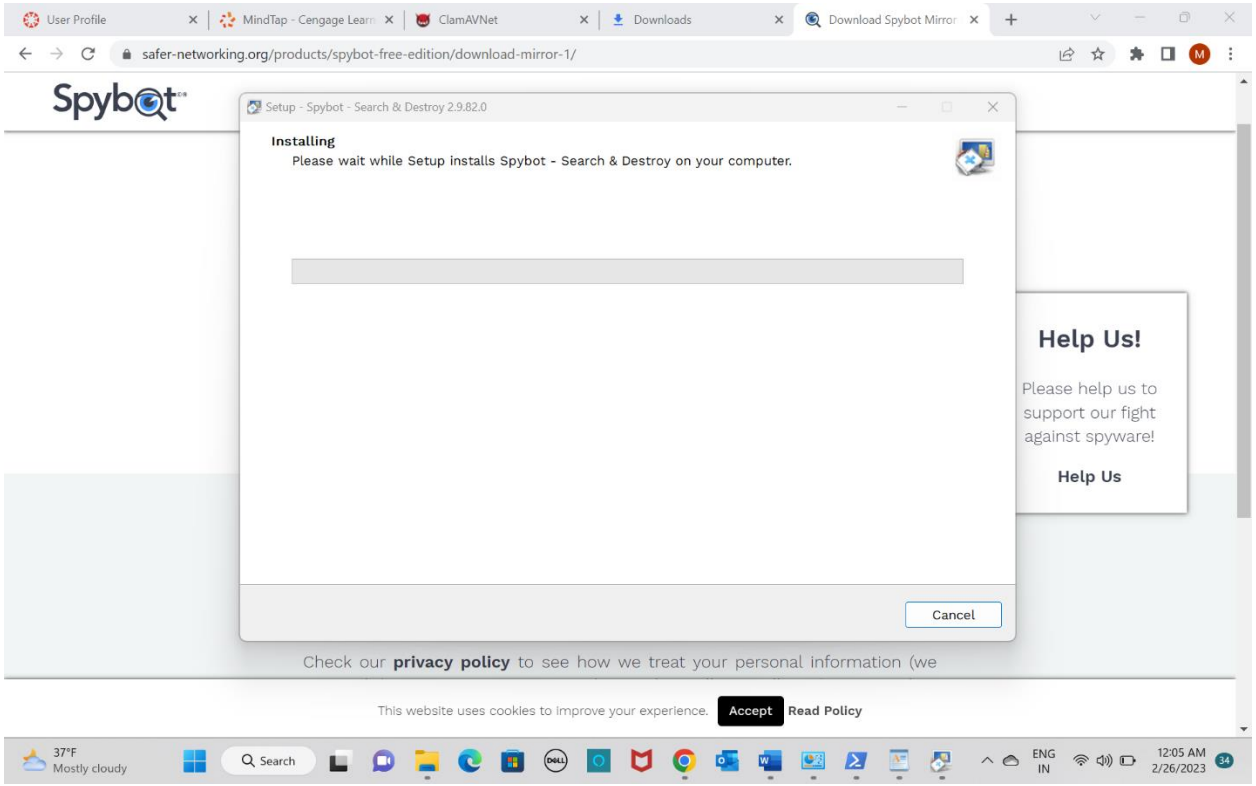
selecting the “more control” option when prompted. Accept the agreements and specify the installation location. Then specify **Spybot (without anti-virus)** as this requires a purchased subscription. Next, click through the remaining windows until Spybot installs.

5. The last step is to specify the startup options as shown in Figure L03-10.

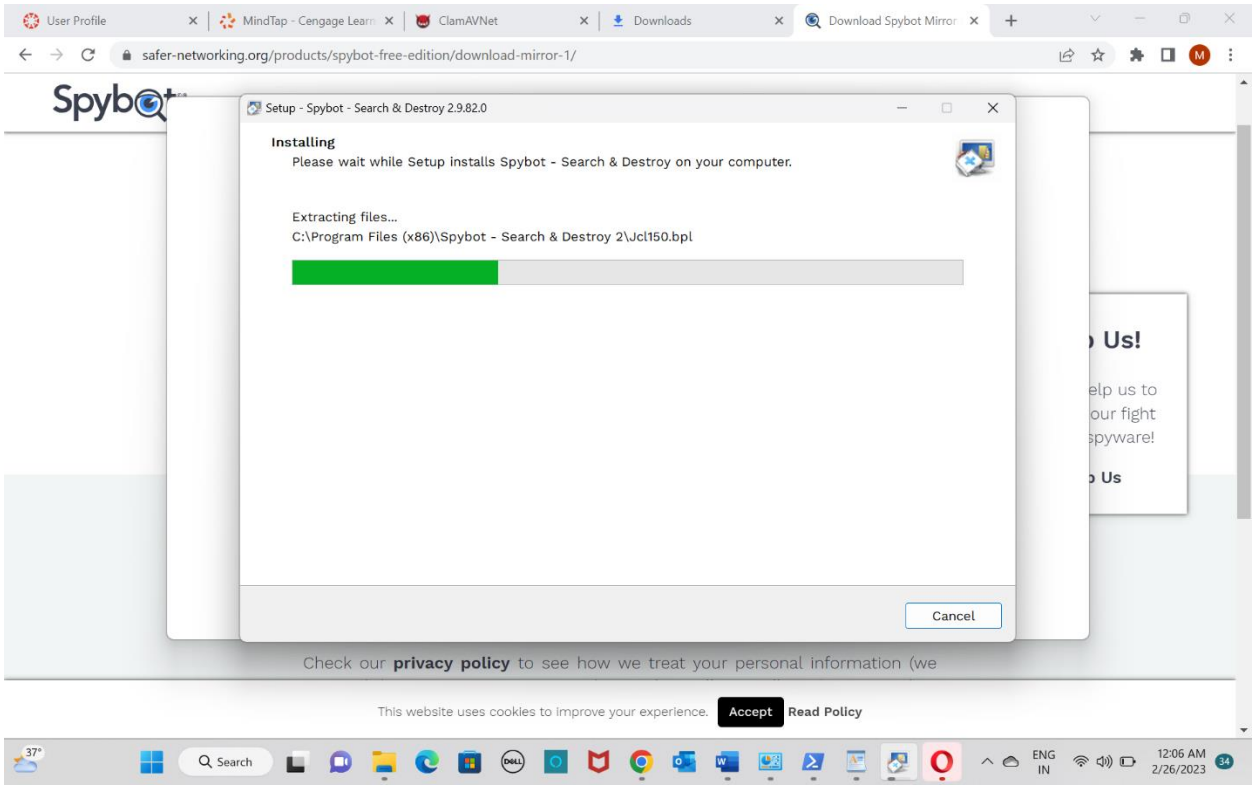


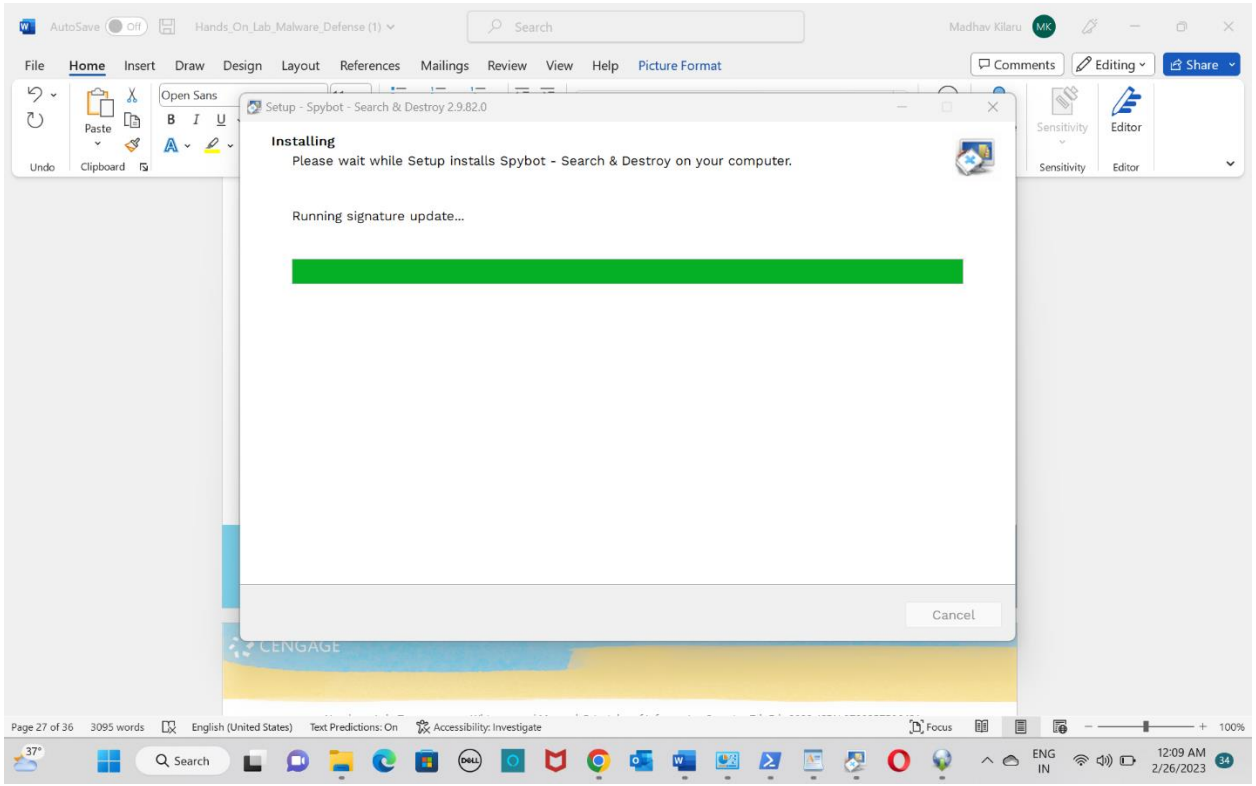
dondavinayreddy@gmail.com





dondavinayreddy@gmail.com





dondavinayreddy@gmail.com

Figure L03-10 Spybot setup Wizard options

Scanning the Local Drive with Spybot S&D

6. Once Spybot is started (See Figure L03-11), it should automatically update.

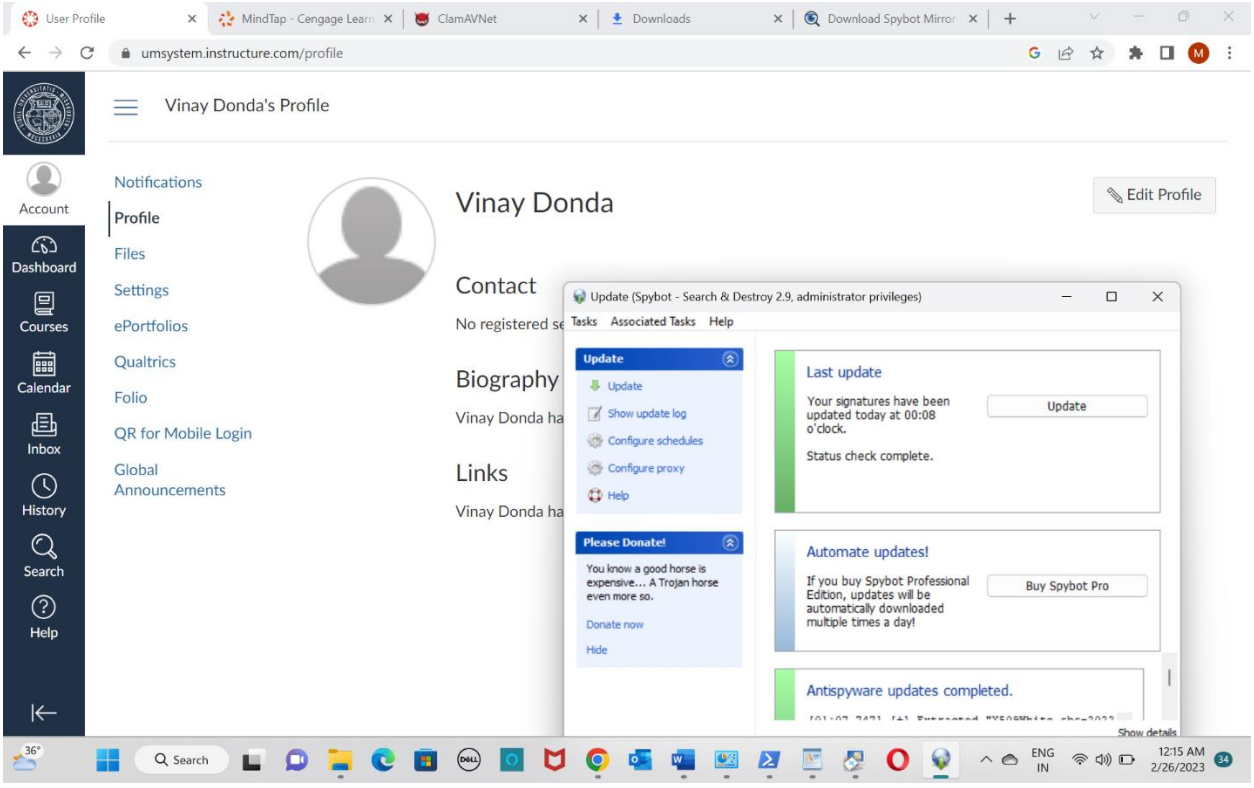


Figure L03-11 Spybot Start Center

7. Click the **Associated Tasks** menu at the top of Spybot and select **Settings**. As shown in Figure L03-12, here you can specify a number of configuration options. Spend a few minutes familiarizing yourself with these options.

dondavinayreddy@gmail.com

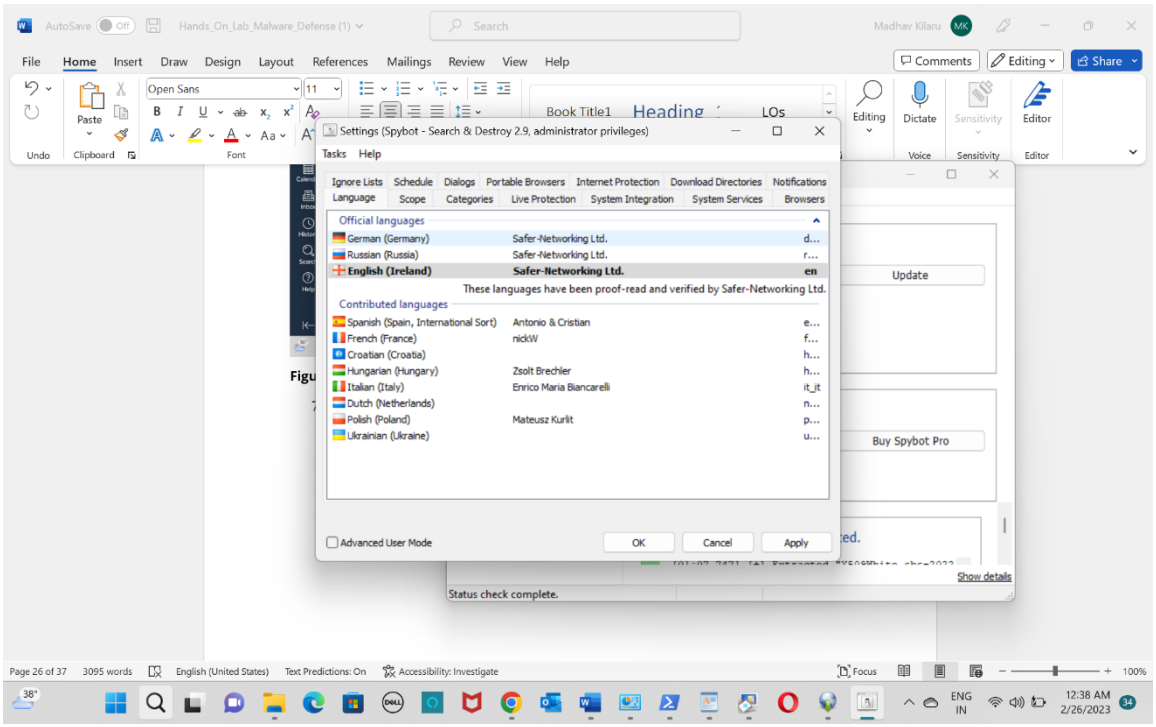


Figure L03-12 Spybot Settings Menu

8. One key feature of this menu is the ability to schedule a scan, rather than having to do it manually. On the **Schedule** tab, you would select **Add** if no scan is currently scheduled. As shown in Figure L03-13, the software has automatically set up a scan for the example system for the first of every month at 12:30 am. If you want to change this, you click the **Edit** button and make any needed changes.

dondavinayreddy@gmail.com

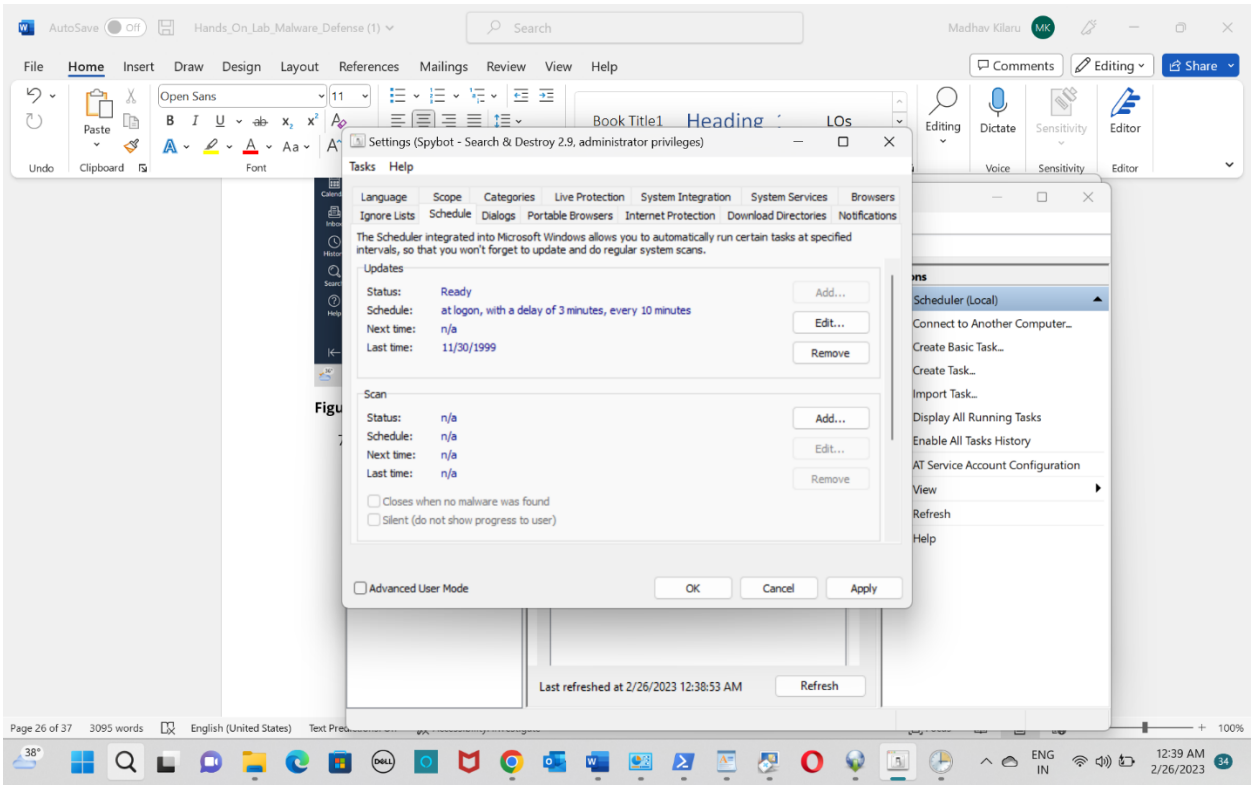
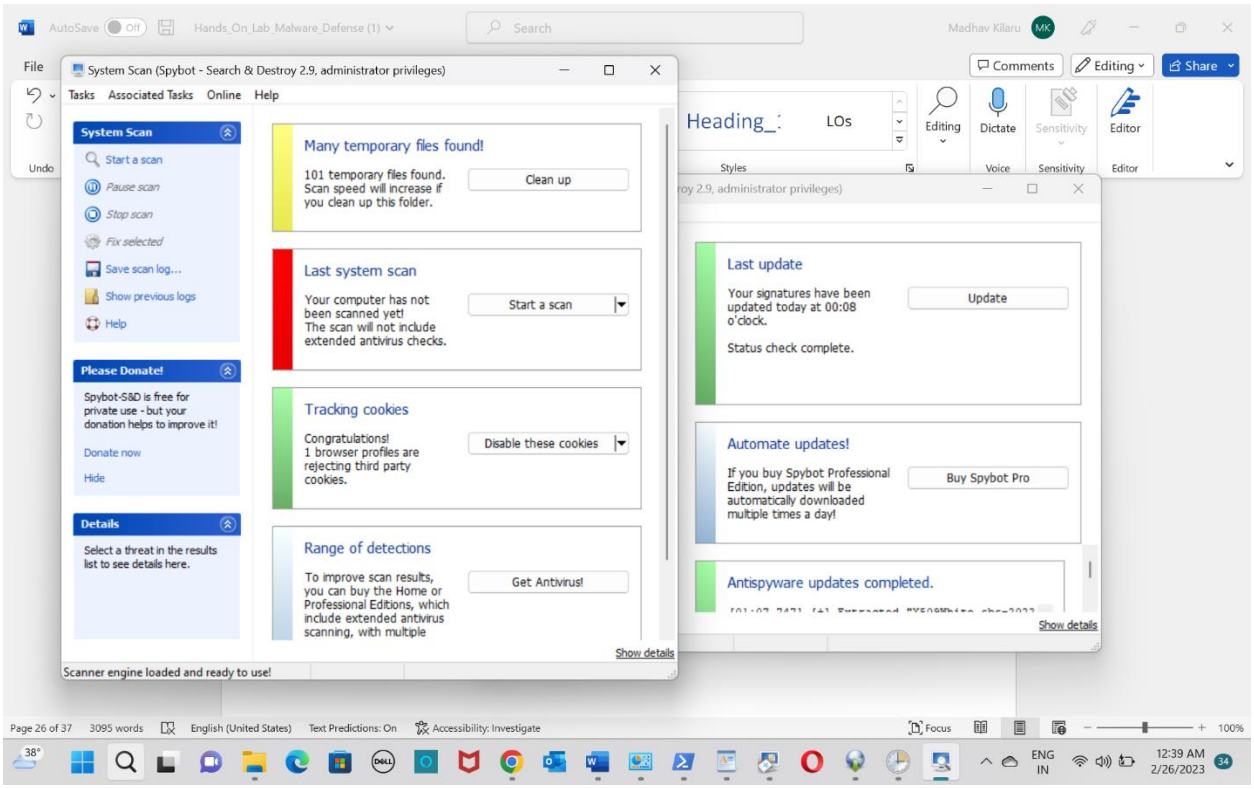
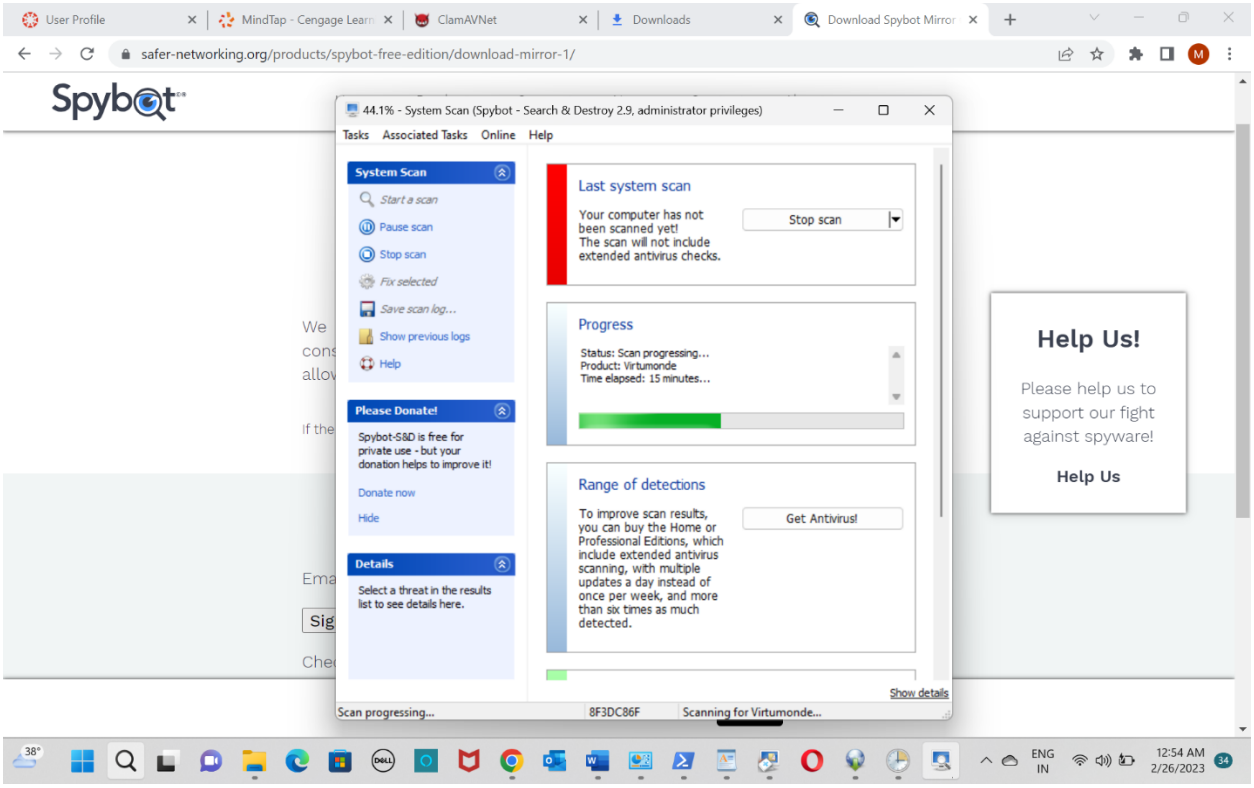


Figure L03-13 Spybot Schedule Scan example

9. Click the **Associated Tasks** menu at the top of Spybot and select **Systems Scan**. You should see a window similar to Figure L03-14 appear. Make sure your settings match those in Figure L03-14 and click **Start a Scan** in the left side menu.

dondavinayreddy@gmail.com





dondavinayreddy@gmail.com

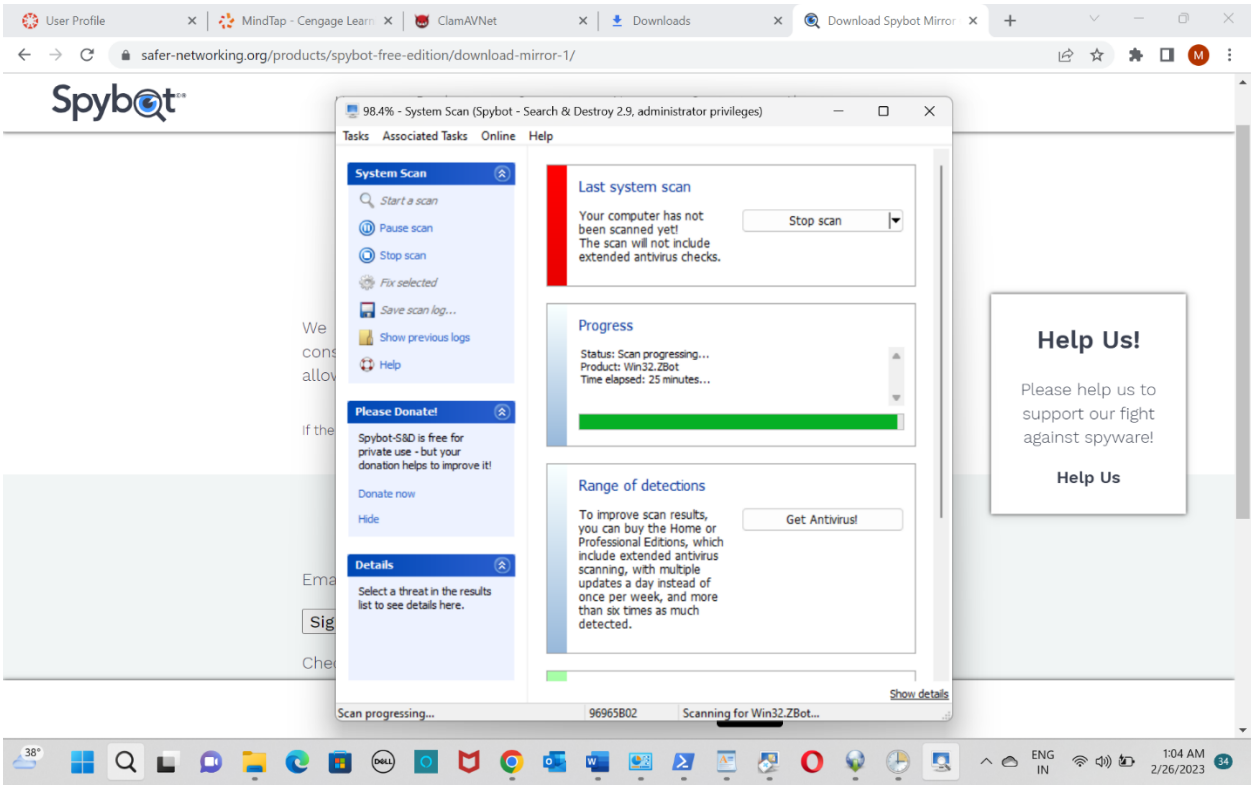


Figure L03-14 Spybot System Scan Menu

10. Let the application run. Note it may take several minutes for the scan to finish, depending on the size and number of your system's hard drives. It took approximately 17 minutes on the system used for this example, which had several multi-terabyte drives, each with hundreds of gigabytes of data.

11. Spybot will scan your system for specific malware attacks that an AV program might overlook, including spyware monitoring software, startup tools and rootkits. You can see what malware is being scanned for at the bottom of the System Scan window. Some organizations may intentionally install employee-monitoring software, so check with our supervisor if you're using this on an office computer.
    Once the scan has finished, review the results. You may see pages of tracking cookies, stored temporary files, and possibly even malware in the results, as shown in Figure L03-15.

dondavinayreddy@gmail.com

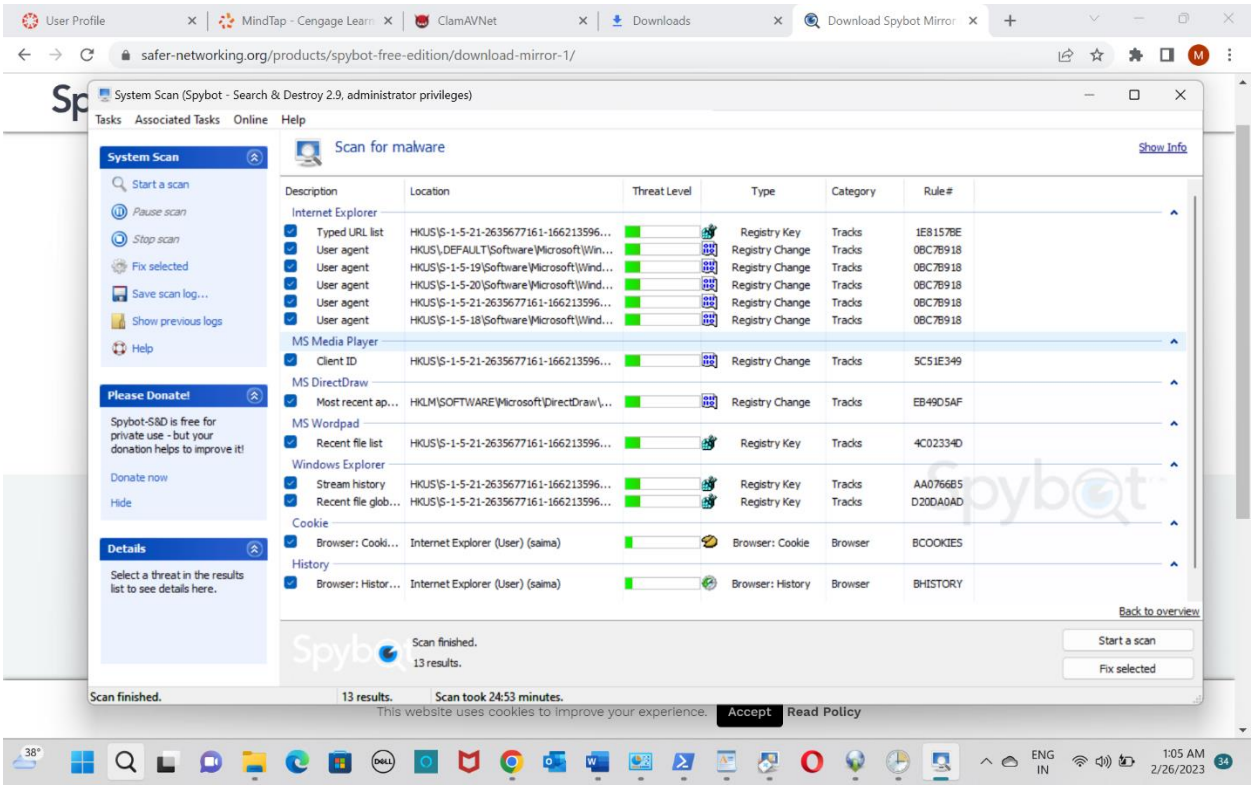
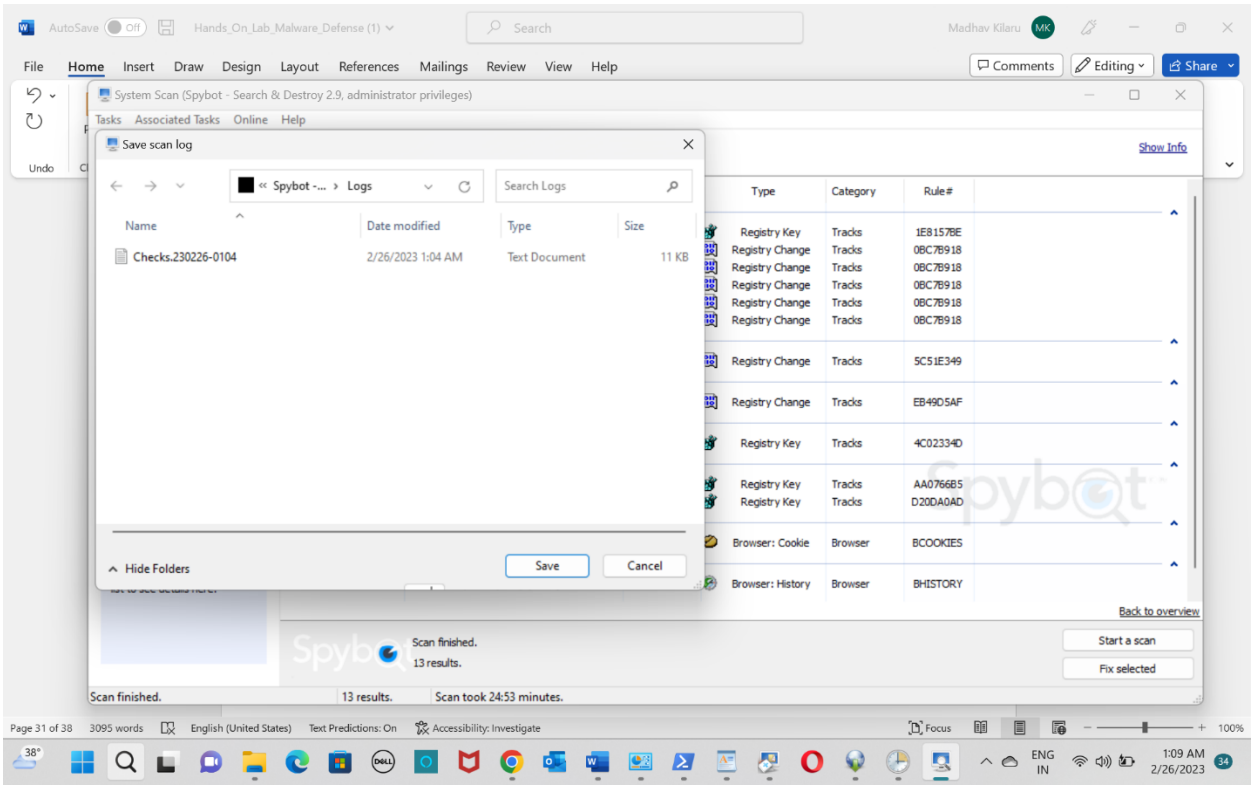


Figure L03-15 Spybot Scan Results

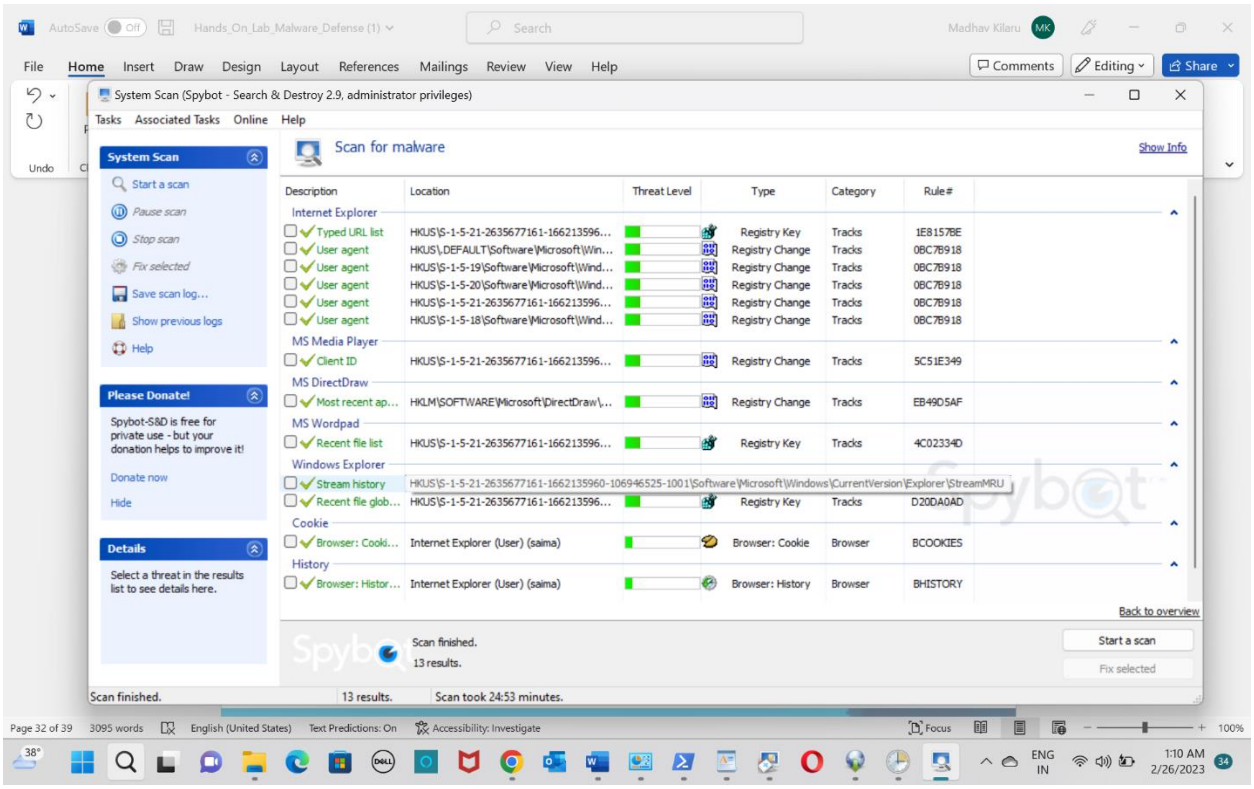
12. You can save your scan log by **Save scan log...** in the System scan menu on the left.

dondavinayreddy@gmail.com



13. If you want to fix the issues identified by Spybot, leave all the items checked in the right pane and click the **Fix selected** button at the bottom. If you only want to fix selected items, uncheck those you do not want to fix.

dondavinayreddy@gmail.com



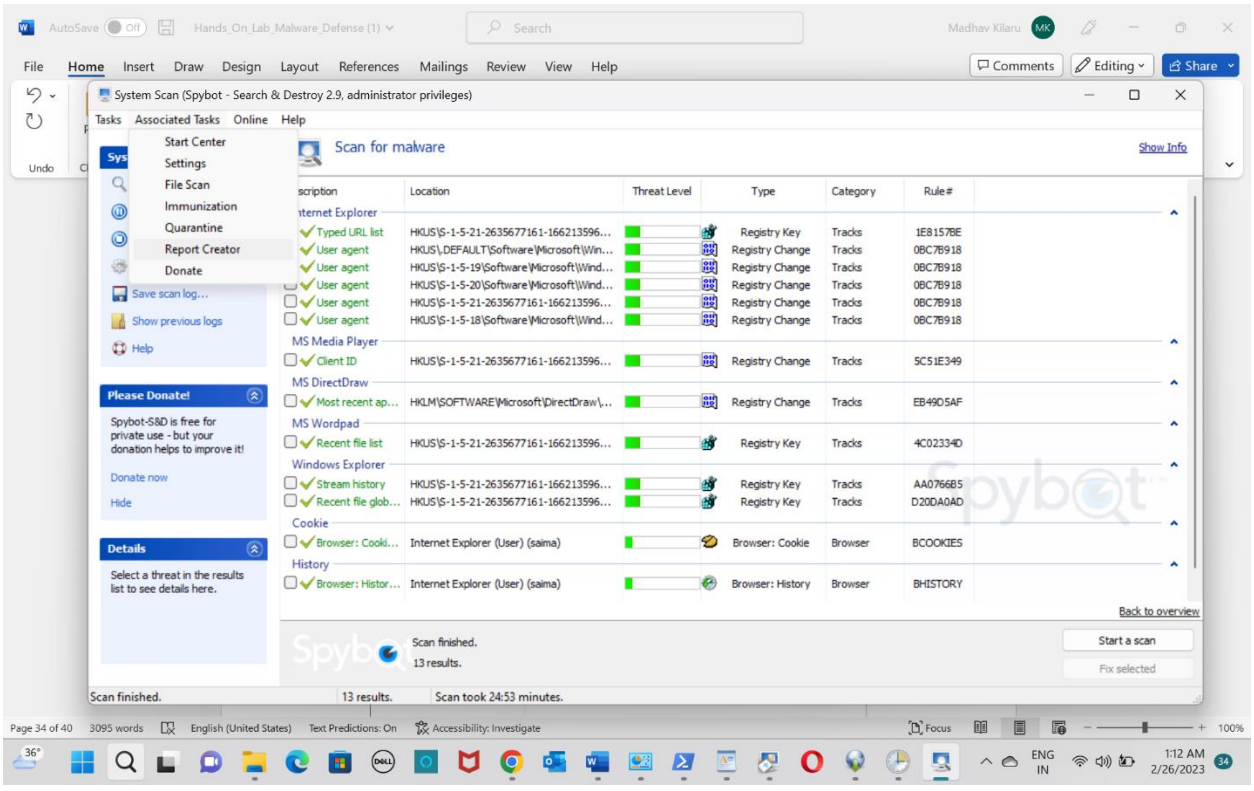
14. Some options available in Spybot include *Immunization* and *Quarantine*, under the *Associated Tasks* menu. Immunization updates a Windows host file noting web sites that contain malware. It also prevents the storage of cookies on the system and blocks the installation of spyware from known sources. Quarantine allows the user to override the software and restore a file that Spybot thinks is malware. Most Malware/AV software will automatically quarantine or delete files they think are malicious. However, sometimes a file isn't really malware, but is easily mistaken for it. (Search for the term "EICAR testfile" for an example). If you have a file that gets quarantined, you can select this menu option and restore the file.

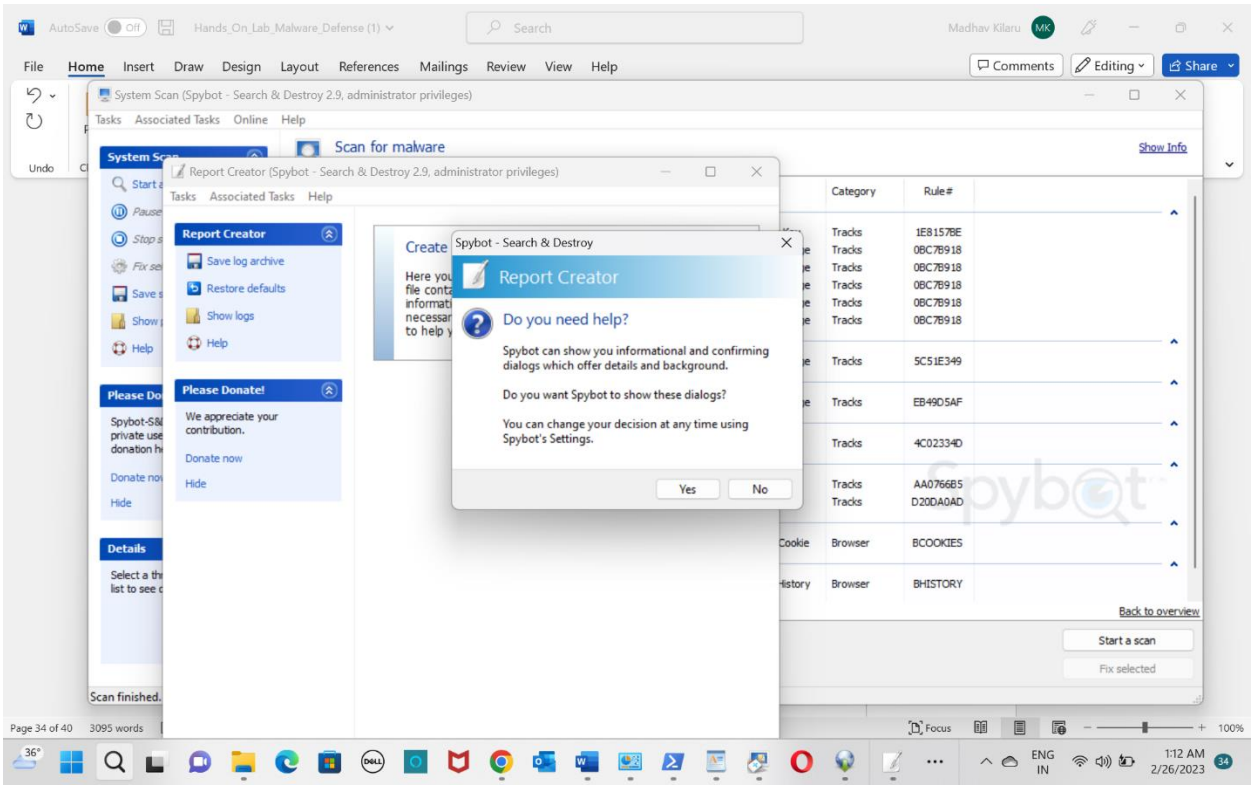
15. You can generate a report of your results by selecting Associated Tasks then Report Creator, as shown in Figure L03-16. Spybot will walk you through the process.

Figure L03-16 Spybot Report Creator

16. If you installed this on your personal system, you can leave it installed. Otherwise, ask your instructor if they want you to uninstall the software.

dondavinayreddy@gmail.com





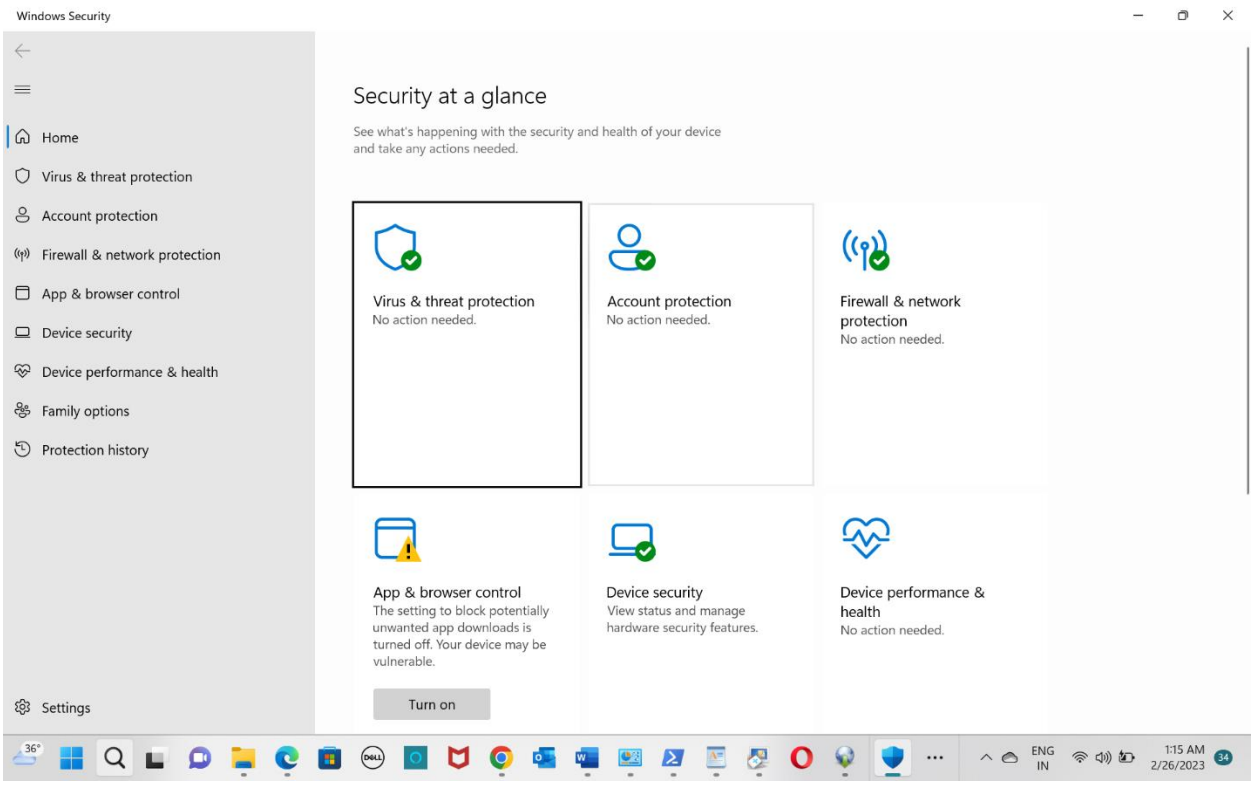
dondavinayreddy@gmail.com

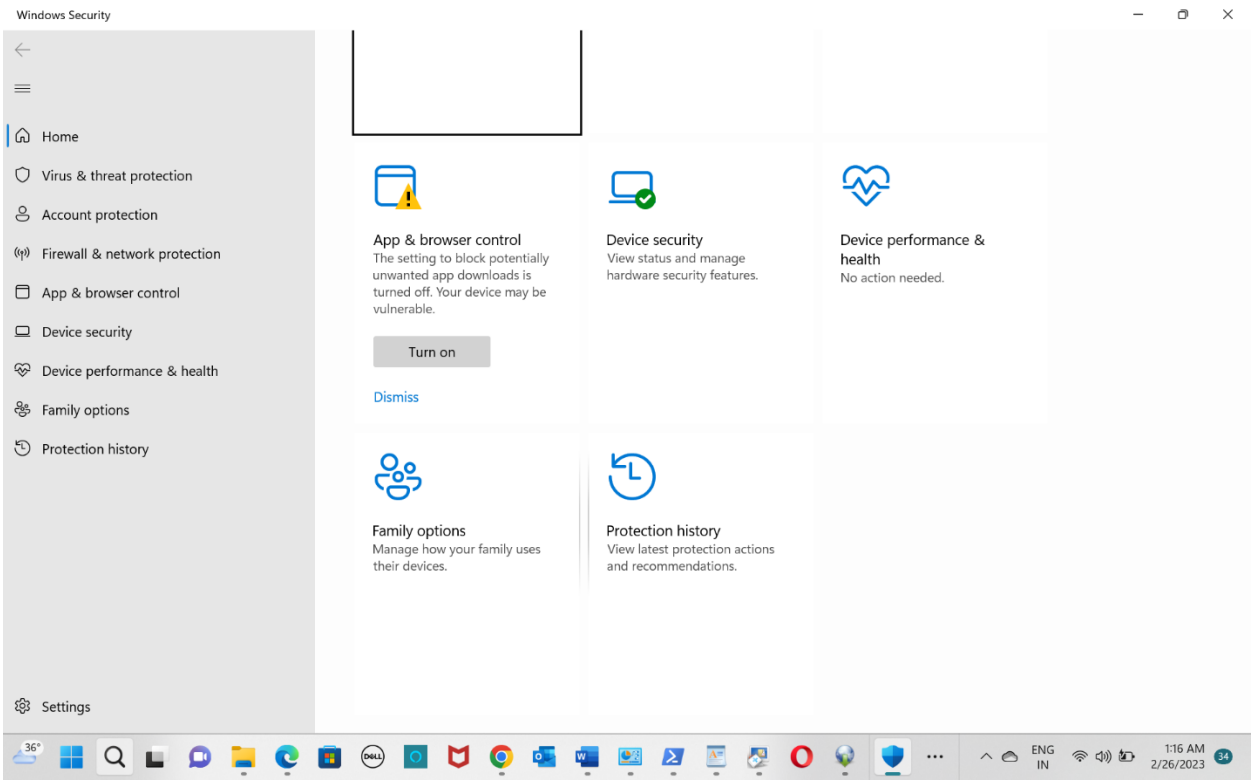
Virus and Malware Prevention with Windows Security

If you're running a current Windows OS, like Windows 10, you have a free anti-virus application installed. Windows Security (formerly known as Windows Defender Security Center) is installed by default. It will be disabled if you're running a third-party application, but in the absence of another application, it can provide protection. Begin by checking to see if Windows Security is active on your system. If you are using a computer in your university's lab or in a commercial office, you may not be able to perform all of the labs below, but can still review the settings and watch the indicate videos.

1. Click the Windows **Start** button and scroll down the list of installed applications that appears on the right. Look for *Windows Security*. Click on the link. If it is active, you will see a screen like Figure L03-17 and can skip the installation process that follows.

dondavinayreddy@gmail.com





dondavinayreddy@gmail.com

Figure L03-16 Windows Security

dondavinayreddy@gmail.com

Enabling Windows Security

2. The only way to enable Windows Security is to uninstall all other versions of anti-virus/anti-malware. If you are performing these labs on your personal computer, you may want to ensure no other AV software is installed. New computers may have trial versions of AV software installed. If you don't plan to renew those applications, uninstall them, and open Windows Security.

Windows Security Options and Operations

1. If Windows security is not already started, type Windows Security in the Taskbar search field, and click on the link that appears. The front page shown in Figure L03-16 above should have a green check mark or the words "no action needed' for the top six menu options. The good news is that the majority of this application is automated, if you have it set up properly. If you don't have a green check mark on the boxes, you will need to check that link and follow the prompts to activate that portion of the application.
2. Click the Virus & threat protection menu on the left, or the icon in the top left corner of the right side of the menu. You should see the screen shown in Figure L03-17 below.

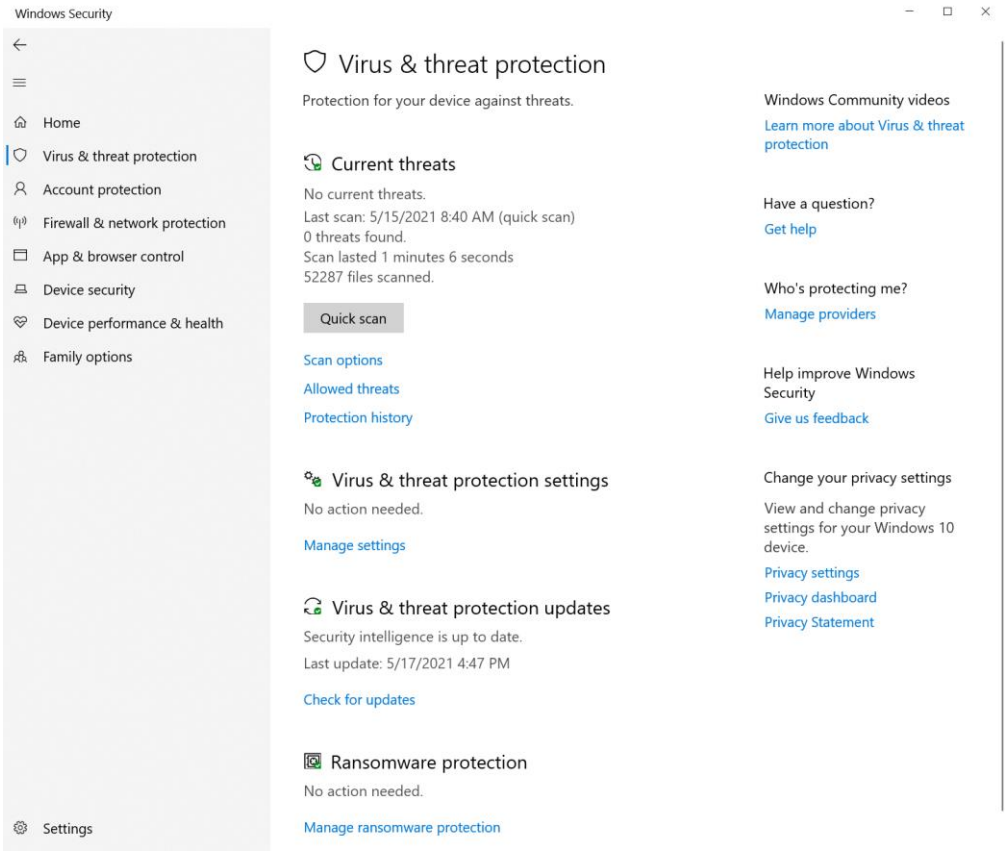
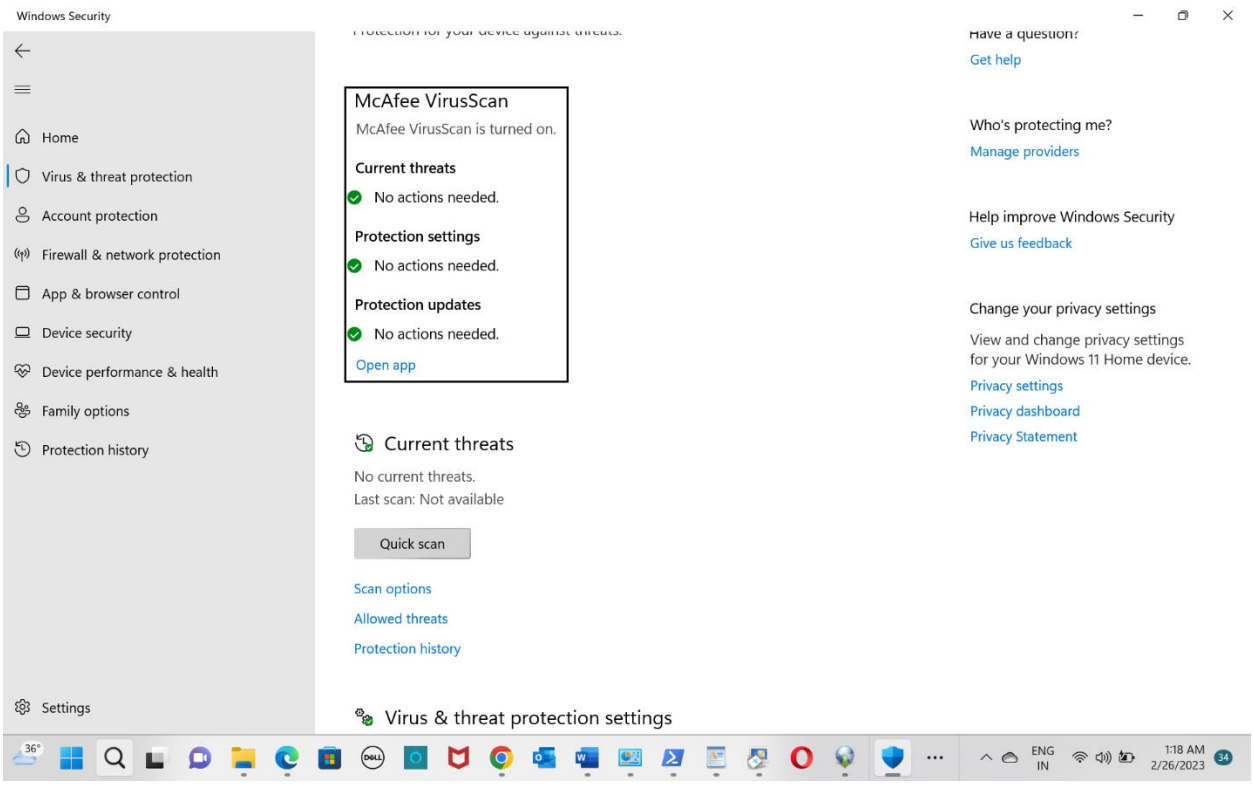


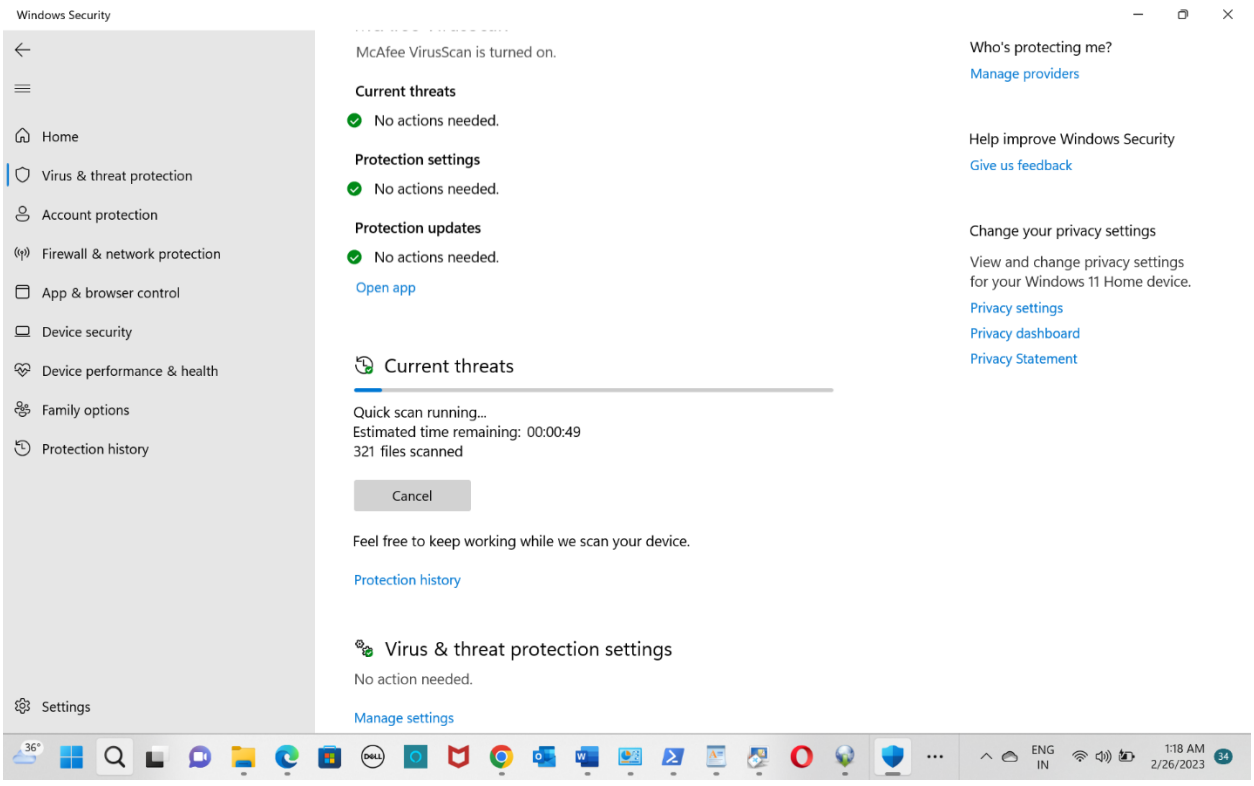
Figure L06-17 Window Security Virus & Threat Protection

dondavinayreddy@gmail.com

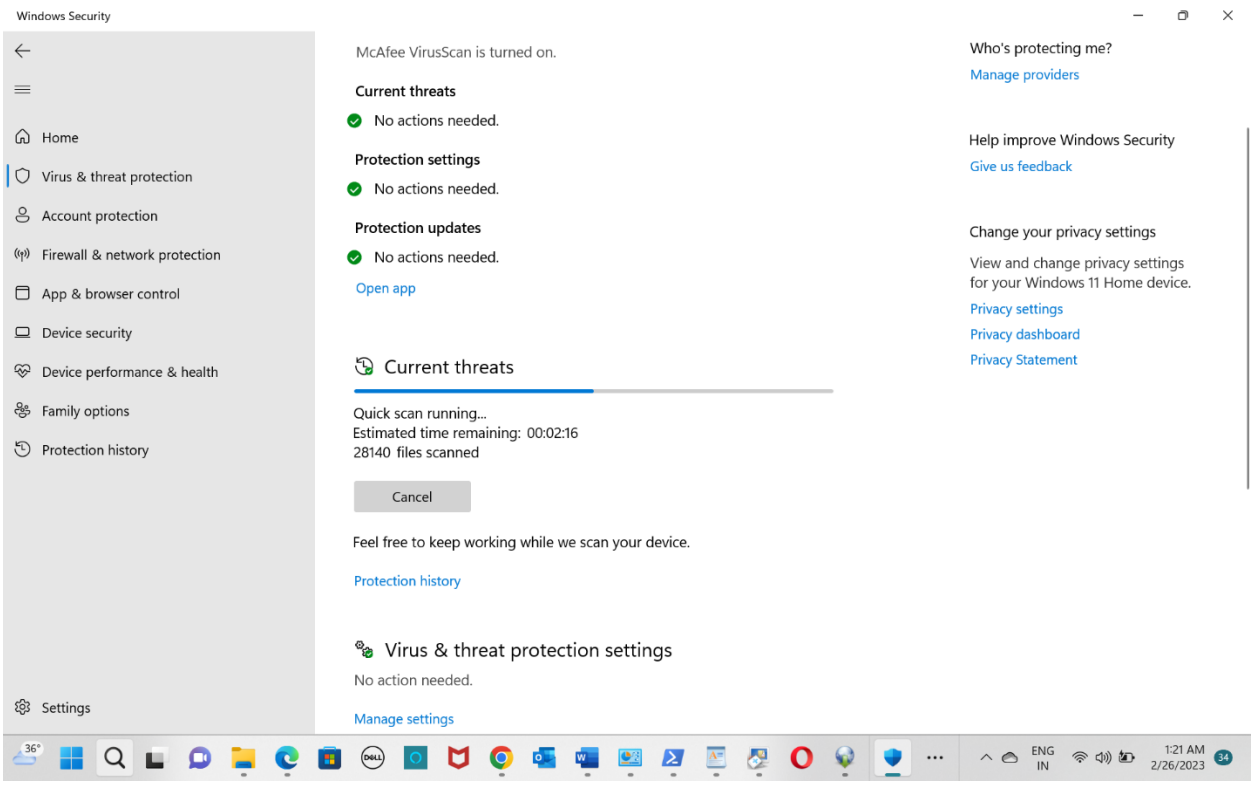
3. First learn a little more about Windows Defender Antivirus by clicking the link in the upper left corner titled "Learn more about Virus and threat protection." This will take you to a Windows community web site where there are several videos about Windows Security and Windows Defender. Watch the following videos:
    a. Windows Security: The dashboard for device protections - https://community.windows.com/en-us/videos/windows-security-the-dashboard-for-device-protections/e_Z2bk7Cp1g?from=search
    b. Virus & threat protection: Keep Defender antivirus at full strength - https://community.windows.com/en-us/videos/keep-your-pc-more-secure-with-windows-security-updates/YmIitr4eJ8E?from=search
    c. Windows Defender team: Make security easier - https://community.windows.com/en-us/videos/windows-defender-team-make-security-easier/vuduNkegxb8?from=search
4. Click the button labeled **Quick scan**. his will scan your core Windows files. It only takes a few minutes.
5. If you want a more thorough scan, click the **Scan options** menu below the *Quick scan* button. As shown in Figure L03-18, you can perform a full scan, custom scan, or offline scan.

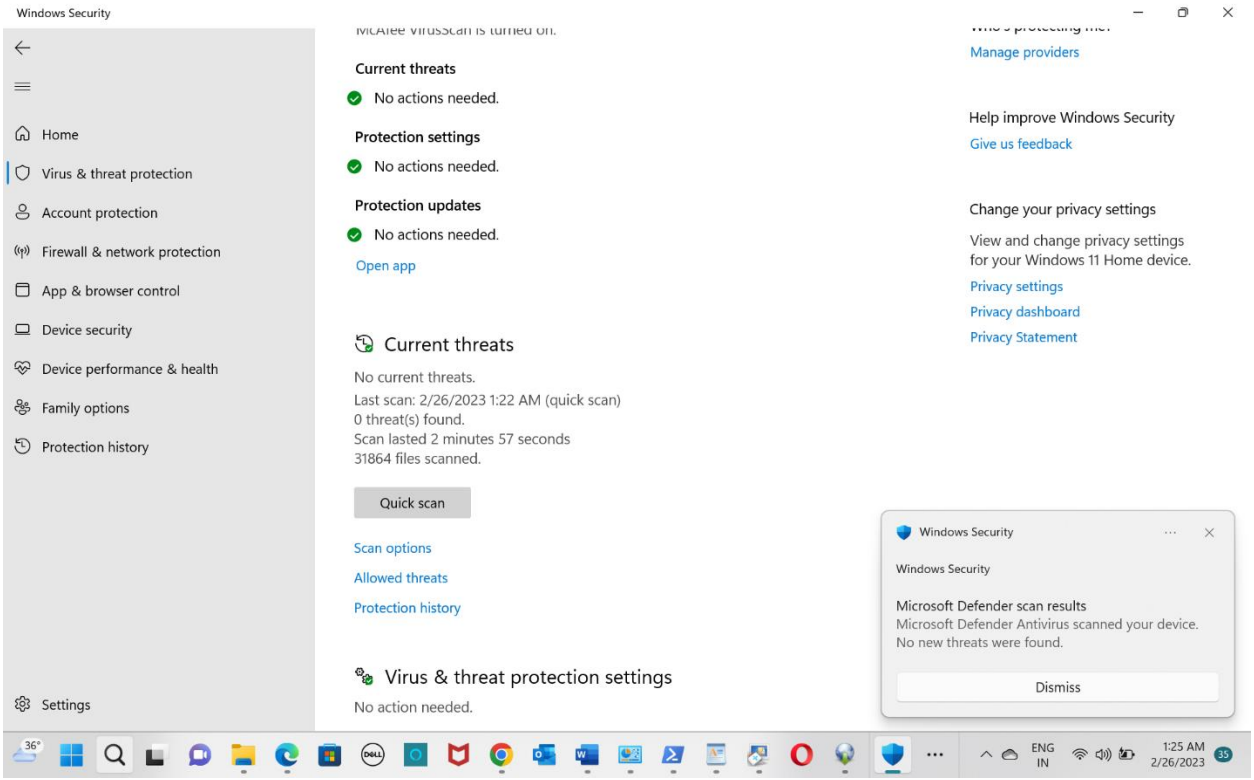
dondavinayreddy@gmail.com





dondavinayreddy@gmail.com

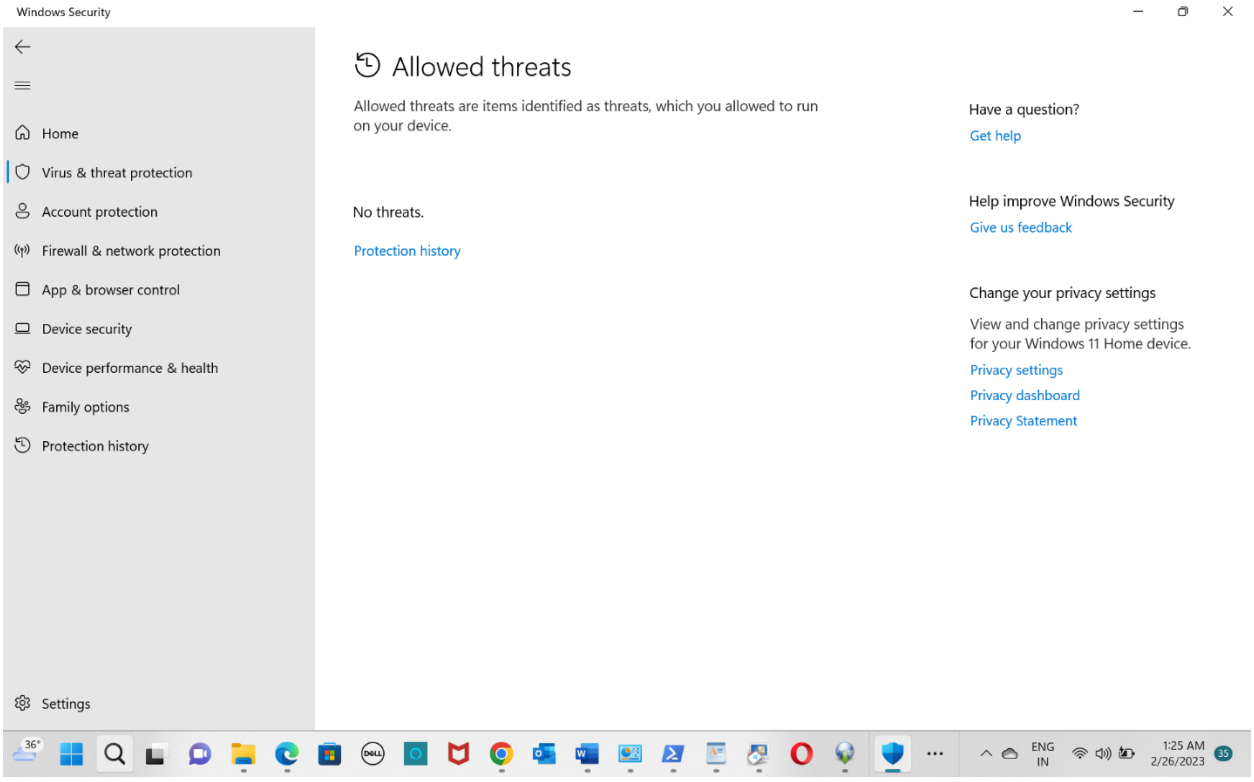




dondavinayreddy@gmail.com

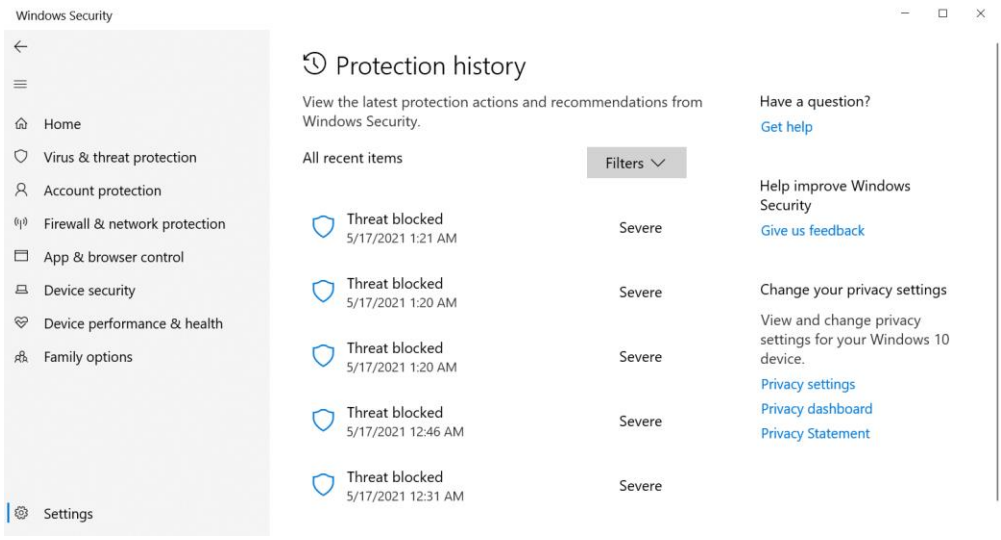
Figure L06-18 Windows Defender Scan Options

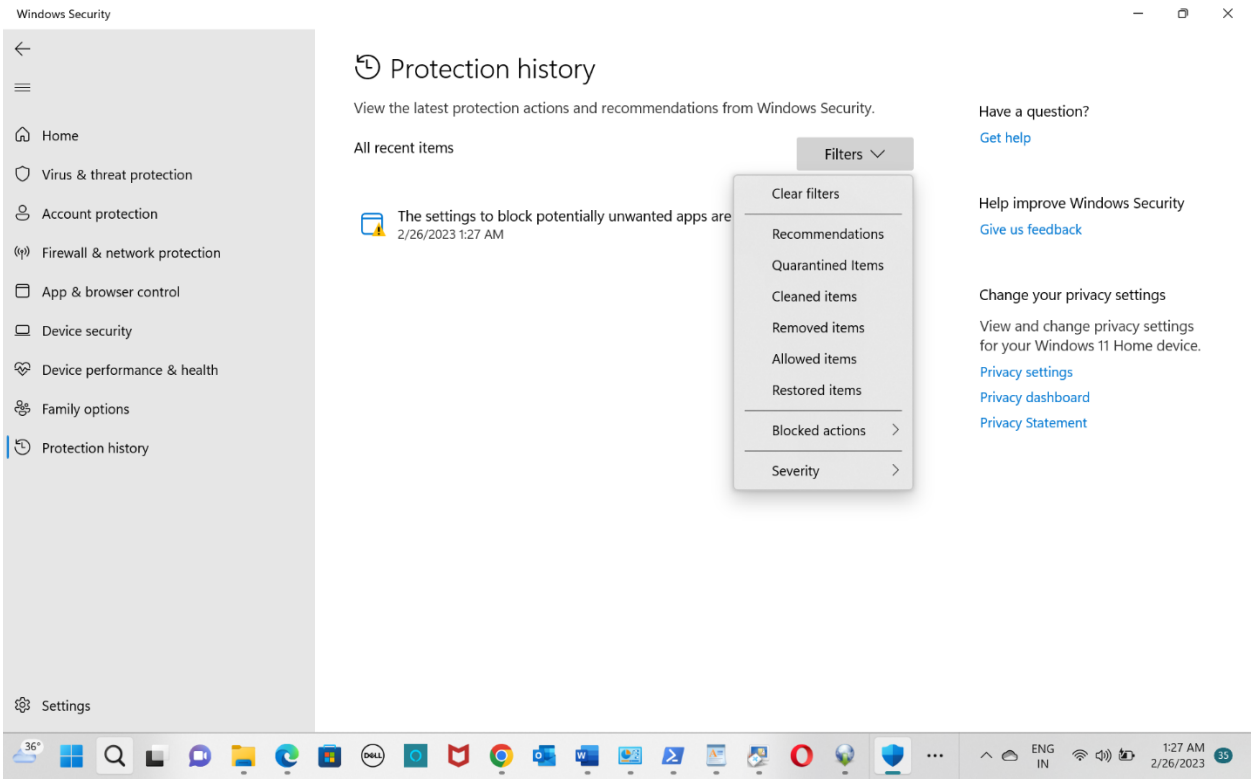
6. Click the back arrow at the top left of the Windows Security window. The **Allowed threats** option gives you the option to provide an exception for a particular file you know is safe, but Windows Defender keeps deleting.



7. Click the **Protection history** menu option. Here you can see what actions Windows Defender has taken over the past few days, as shown in Figure L03-19. If you have a long list, the Filters button allows you to sort and filter the threats shown.

dondavinayreddy@gmail.com

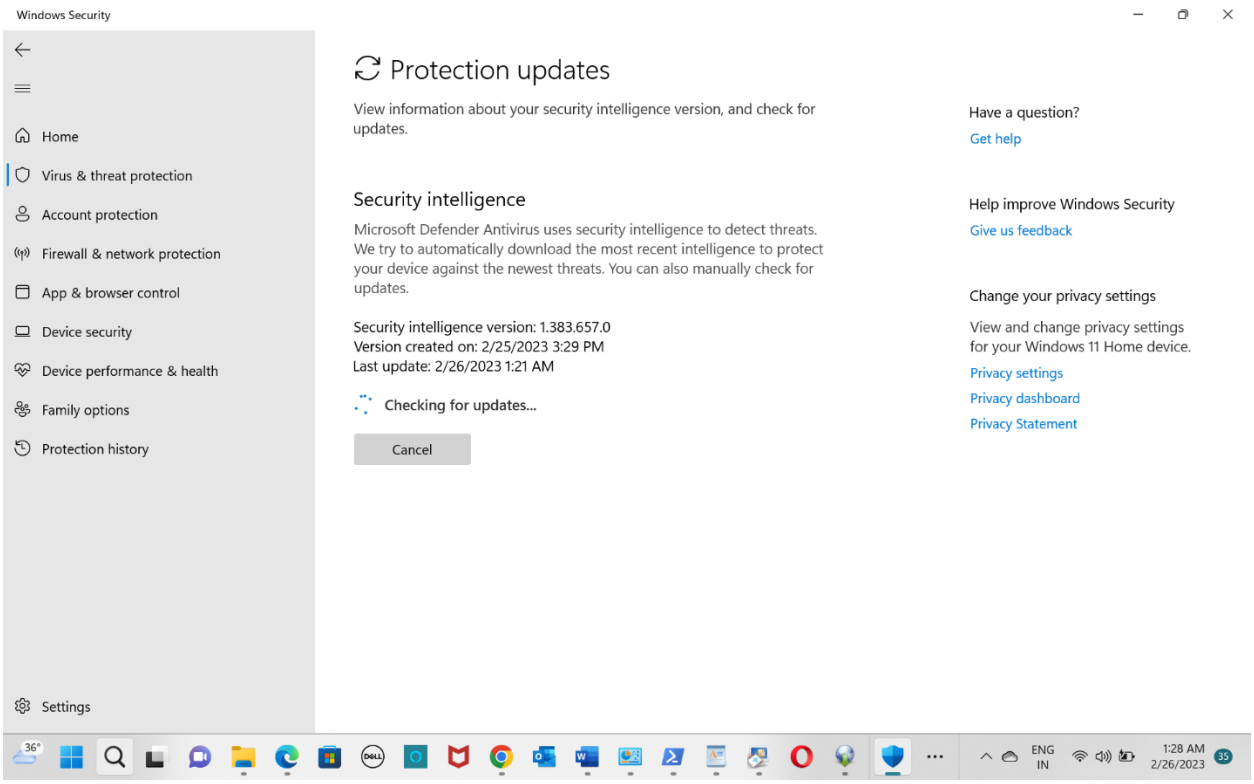




dondavinayreddy@gmail.com

Figure L06-19 Windows Defender Protection History

8. Click the back arrow to go back to the *Virus & threat protection* menu. Look at the Virus & threat protection updates. Is your version up to date? If it isn't, you can click the **Check for updates** link to access the Protection updates menu shown in Figure L03-20 below. If your system isn't up to date with a "Last update" date within the last week, click the **Check for updates** button on the Protection updates menu.



dondavinayreddy@gmail.com

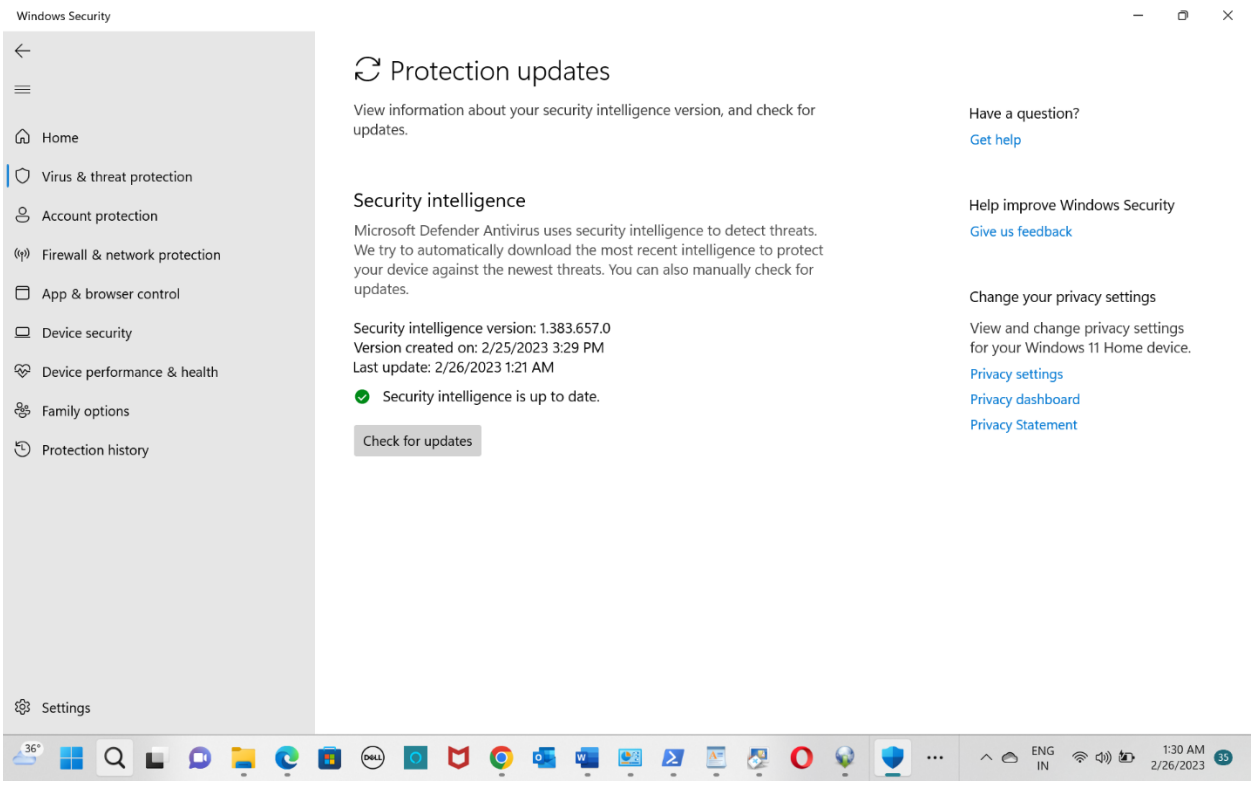


Figure L06-20 Window Security Protection updates

9. The last option we'll examine is the Ransomware Protection. If you are using a personal computer to perform these labs, and have access to Microsoft OneDrive you can set up protected space on the OneDrive to allow you to recover key files in case your computer is locked or encrypted by Ransomware. Never pay the ransom! Click the **Manage ransomware protection** link to view the options shown in Figure L06-21.

dondavinayreddy@gmail.com

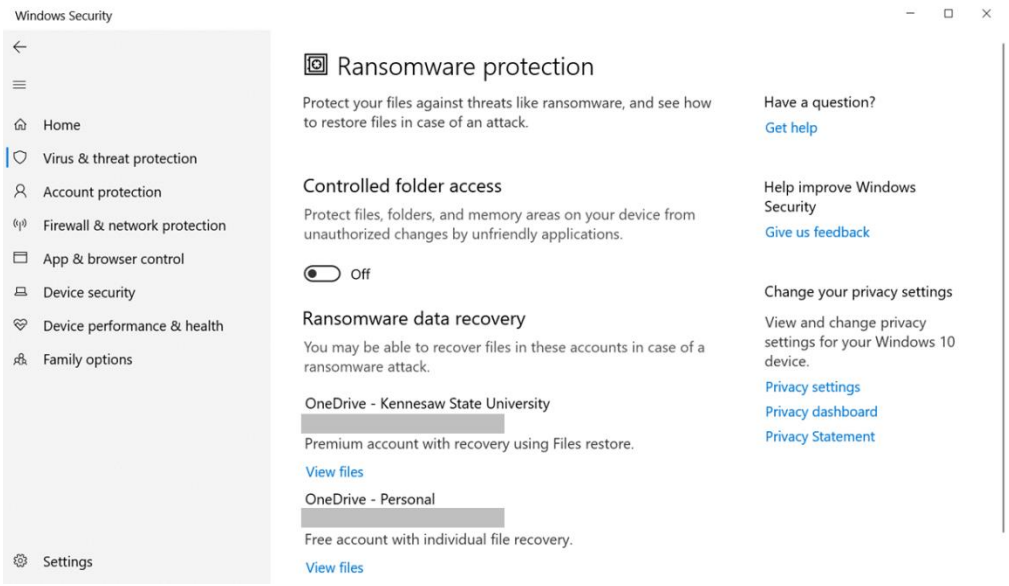
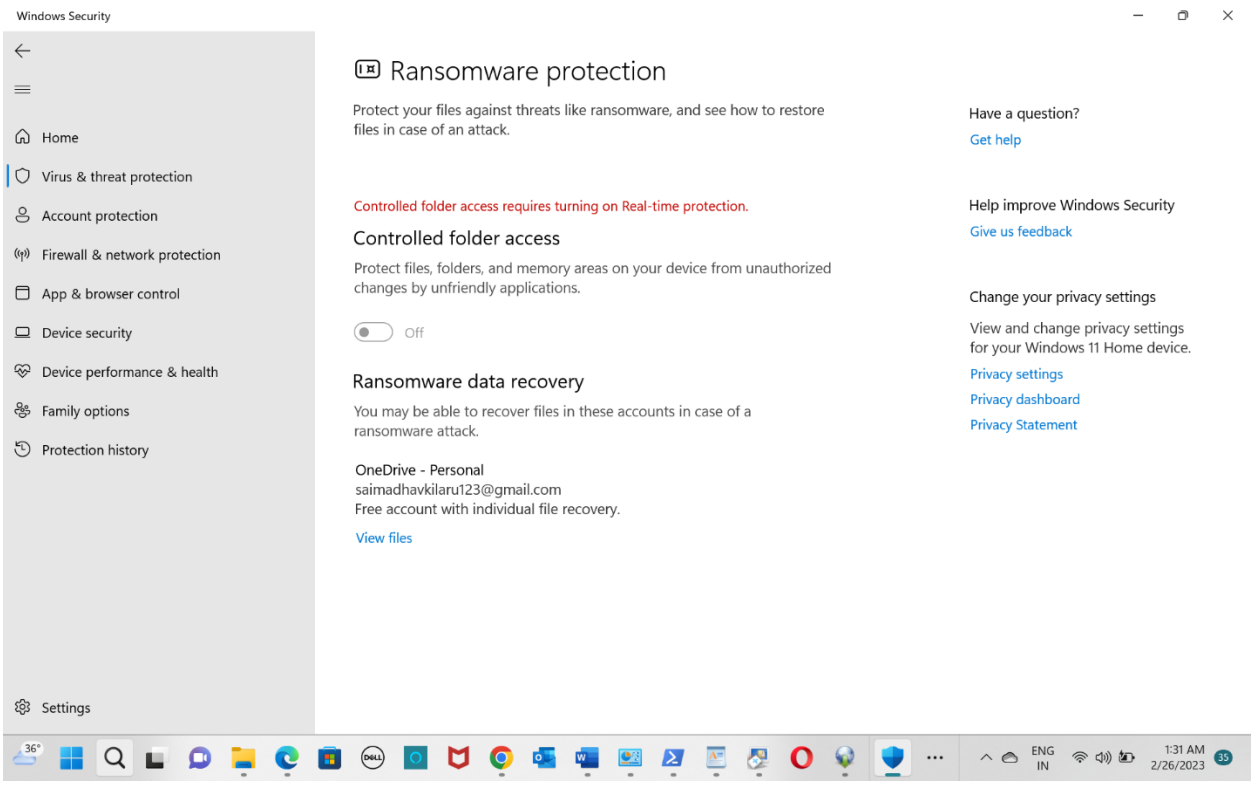
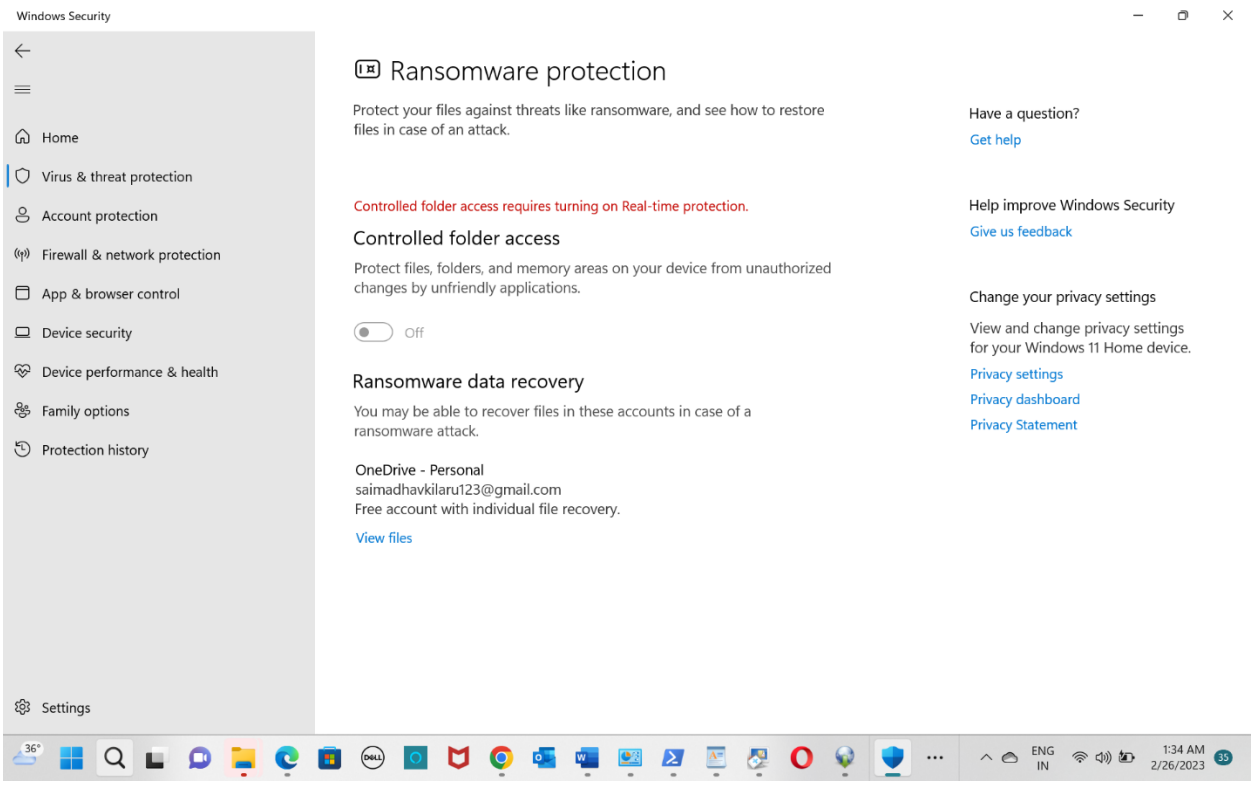


Figure L06-21 Windows Security Ransomware protection



dondavinayreddy@gmail.com



10. Close the Windows Security window.

Self-Reflection and Response

Please share your experiences in installing the antivirus software program.

It's beneficial to be aware of these antivirus software solutions so we can protect our files and data from harmful websites and apps. And I did learn more about the security features of Windows antivirus. discovered how various antivirus programs work when performing system scans.

Did your scan reveal any malware operating on your computer? If yes, please describe.

No, none of my scans turned up any virus!

Did your scan reveal any malware operating on your computer? If yes, please describe.

No, none of my scans turned up any virus!

Were you able to install and run SpyBot Search and Destroy? If yes, describe the results of your scan.

dondavinayreddy@gmail.com

Yeah, I was able to install, launch, and do a full scan using Spybot Search and Destroy on my computer. It checked my entire PC for malware of any kind. Once the scan is finished, it displays detailed descriptions, allows us to track cookies, and displays temporary files.

Please share your experiences in using the Windows AntiVirus solution. Did it find malware undiscovered by the earlier programs?

If no other antivirus software is installed on the system, it is a good idea to employ this protection function. But, you can activate this setting, which periodically scans for risks while running other software. There was no malware found on my system.

Instructor's Response

SS