Put Student Name(s) ↓	Put Student IDs ↓	Due Date	Grade Weight
Ishan Aakash Patel	146151238	As Posted	6%

Name	Lab 8 – Tails OS, Qubes OS, WHOIX
Instructions	• It is an Individual assignment. Put your name + Student ID in the empty spaces above. • Submit via the BB relevant link ONLY. NO submission via email please. Be sure to submit the final version file ONLY. • Show your genuine signs of your work is done on your machine. This includes: ○ Screenshots that show your desktop background with Date/Time. ○ Show a pop-up bx that shows "your name + IP". ○ Show your logged account w8en applicable. Optional: Your photo. Submit your report name: CYT215-Lab8-Student Name & ID
Prior Knowledge	• **Virtualization Software**: Install VirtualBox or VMware on your system. • **Tails ISO**: Download the latest Tails ISO from the official Tails website. https://tails.net/install/
Steps	**Steps for VirtualBox** 1. **Open VirtualBox**: Launch VirtualBox on your system. 2. **Create a New VM**: ○ Click on "New". ○ Name your VM (e.g., "Tails VM"). ○ Set the type to "Linux". ○ Set the version to "Other Linux (64-bit)". ○ Click "Next". 3. **Allocate Memory**: ○ Allocate at least 2048 MB (2 GB) of RAM. ○ Click "Next". 4. **Create a Virtual Hard Disk**: ○ Select "Do not add a virtual hard disk". ○ Click "Create". 5. **Configure the VM**: ○ Select the newly created VM and click "Settings".

- Under "System" -> "Motherboard", ensure that "Enable EFI (special OSes only)" is unchecked.
- Under "System" -> "Processor", allocate 2 or more CPUs (if available).
- Under "Display" -> "Screen", allocate the maximum Video Memory (128 MB).
- Under "Storage", click on the empty disk under "Controller: IDE" and then click on the disk icon to choose a virtual optical disk file.
- Select the Tails ISO you downloaded.
- Under "Network", ensure the adapter is attached to "NAT" for internet access.

6. **Start the VM**:
   - Click "Start".
   - Follow the prompts to boot into Tails.

Steps for VMware

1. **Open VMware**: Launch VMware Workstation or VMware Player on your system.
2. **Create a New Virtual Machine**:
   - Select "Create a New Virtual Machine".
   - Choose "Installer disc image file (iso)" and browse to the Tails ISO.
   - Click "Next".
3. **Select Guest Operating System**:
   - Select "Linux" as the operating system.
   - Select "Other Linux 5.x and later kernel 64-bit".
   - Click "Next".
4. **Name the VM**:
   - Name your VM (e.g., "Tails VM").
   - Click "Next".
5. **Specify Disk Capacity**:
   - Select "Store virtual disk as a single file".
   - Click "Next".
6. **Customize Hardware**:
   - Allocate at least 2048 MB (2 GB) of RAM.
   - Allocate 2 or more CPUs (if available).
   - Click "Close".
7. **Finish and Start the VM**:
   - Click "Finish".

  - Start the VM and follow the prompts to boot into Tails.

Using Tails

Once Tails boots up, follow the on-screen instructions to configure and use Tails. Tails is designed to be amnesic, meaning it doesn't retain any information between sessions unless you explicitly save it to persistent storage.

Important Notes

- **Persistence**: Tails can be used with persistent storage if needed, but setting up persistence on a VM can be tricky. It's generally recommended to use Tails on a USB drive for persistent storage.
- **Security**: Tails is designed for privacy and anonymity. Running it in a VM might expose it to some risks that would not be present when running it on bare metal (e.g., USB drive).

By following these steps, you should have a functional Tails VM for secure and anonymous browsing.

Provide a screenshot of Tails being setup on in your environment.

Answer the following questions in a report format:

Introduction to Tails OS

1. **What is Tails OS?**
    - Describe the main purpose and features of Tails OS.
2. **Why is Tails OS considered secure and anonymous?**
    - Explain the security and anonymity features of Tails OS.
3. **How does Tails OS handle data persistence?**
    - Describe the options available for data persistence in Tails OS.
4. **How can you verify the integrity of the Tails OS ISO file before installation?**

- Explain the process of verifying the Tails OS ISO file.

Network Configuration and Security

7. **How does Tails OS ensure secure internet browsing?**
    - Discuss the use of Tor in Tails OS for secure browsing.
8. **What are the potential risks of using Tails OS on public networks, and how can they be mitigated?**
    - Identify risks and mitigation strategies when using public networks.

Working with Tails OS

10. **How do you install additional software on Tails OS?**
    - Explain the process of installing additional software packages.
11. **What tools does Tails OS provide for secure communication?**
    - List and describe tools available for secure communication.
12. **How can you securely transfer files using Tails OS?**

- Explain methods for secure file transfer in Tails OS.

Malware Analysis

13. **Why is Tails OS a suitable environment for malware analysis?**
    - Discuss the features that make Tails OS suitable for malware analysis.
14. **What are the steps to set up a secure malware analysis environment in Tails OS?**
    - Provide a step-by-step guide for setting up a secure environment for malware analysis.
15. **How can you capture network traffic in Tails OS for analysis?**
    - Describe tools and methods for capturing and analyzing network traffic.
16. **What precautions should be taken when analyzing malware on Tails OS?**

- List and explain safety precautions to take during malware analysis.

17. Research about CalmAV and explain how it can be used on Tails for Malware Analysis.

Practical Application

18. **Create a scenario where you use Tails OS to analyze a suspicious file. What steps would you follow?**
    - Outline a practical scenario and the steps taken to analyze the file.
19. **How can you use Tails OS to report findings securely to a third party?**
    - Explain methods for securely reporting findings.
20. **Discuss the limitations of using Tails OS for malware analysis.**
    - Identify and explain the limitations.

21. Warch the following videos - https://www.youtube.com/watch?v=VtzwfX0NgKA, https://www.youtube.com/watch?v=u5Lv_HXICpo&t=0s and provide feedback on Tails OS. This is free writing highlighting your thoughts on Tails OS.

	OPTIONAL -- Look into Qubes OS , Whonix https://www.qubes-os.org/ https://www.youtube.com/watch?v=DmKMi_XjIqA https://www.youtube.com/watch?v=-dWEcBQZBXw https://www.whonix.org/
Grading Alerts	• If you do NOT use this template or delete any part of it or use any other template, you will be degraded. • If you do NOT follow the fie naming convention, you will be degraded. • If you do NOT submit your file in PDF; you will be degraded. • If you do NOT show your account real name (when applicable); you will be degraded. If you do NOT write (in your own words) your learning experience for the activity practices, you will be degraded. NOTE – THIS IS AN INDVIDUAL REPORT AND MUST BE IN YOUR OWN WORDS. ALL THOUGH COLLABORATION IS ENCOURAGED, YOUR REPORT SHOULD BE YOUR OWN. Feel free to reference google when answering the above questions. Please follow and abide by the Seneca Academic Integrity policy –

Academic Integrity at Seneca

What is Academic Integrity?

The International Center for Academic Integrity defines academic integrity as a commitment, even in the face of adversity, to six Fundamental Values of Academic Integrity: honesty, trust, fairness, respect, responsibility, and courage. From these values flow principles of behavior that enable academic communities to translate ideals into action.

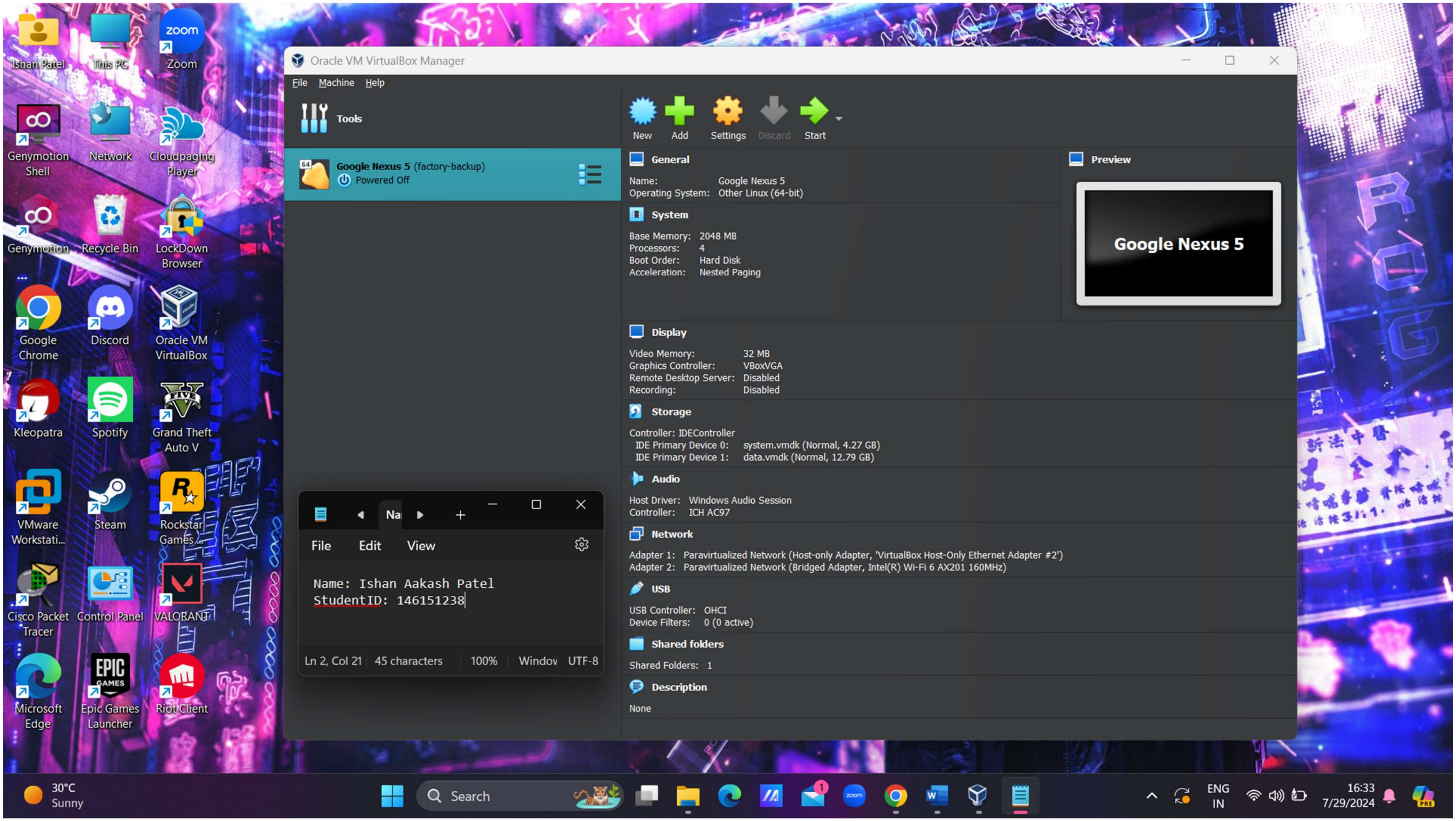
Why does Academic Integrity Matter?

When each member of the Seneca Community embraces and incorporates these values into our teaching, learning and working environments, then we are able to maintain the college's reputation as a leading educational institution and to graduate high quality students who are poised to succeed in their careers and contribute meaningfully to society.

Academic Integrity - Student Resources

-------------------------------------Report goes below here --

Installing Tails OS in Virtual Box



Google Nexus 5 (factory-backup)
Powered Off

General

Name: Google Nexus 5
Operating System: Other Linux (64-bit)

System

Base Memory: 2048 MB
Processors: 4
Boot Order: Hard Disk
Acceleration: Nested Paging

Display

Video Memory: 32 MB
Graphics Controller: VBoxVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDEController
IDE Primary Device 0: system.vmdk (Normal, 4.27 GB)
IDE Primary Device 1: data.vmdk (Normal, 12.79 GB)

Audio

Host Driver: Windows Audio Session
Controller: ICH AC97

Network

Adapter 1: Paravirtualized Network (Host-only Adapter, 'VirtualBox Host-Only Ethernet Adapter #2')
Adapter 2: Paravirtualized Network (Bridged Adapter, Intel(R) Wi-Fi 6 AX201 160MHz)

USB

USB Controller: OHCI
Device Filters: 0 (0 active)

Shared folders

Shared Folders: 1

Description

None

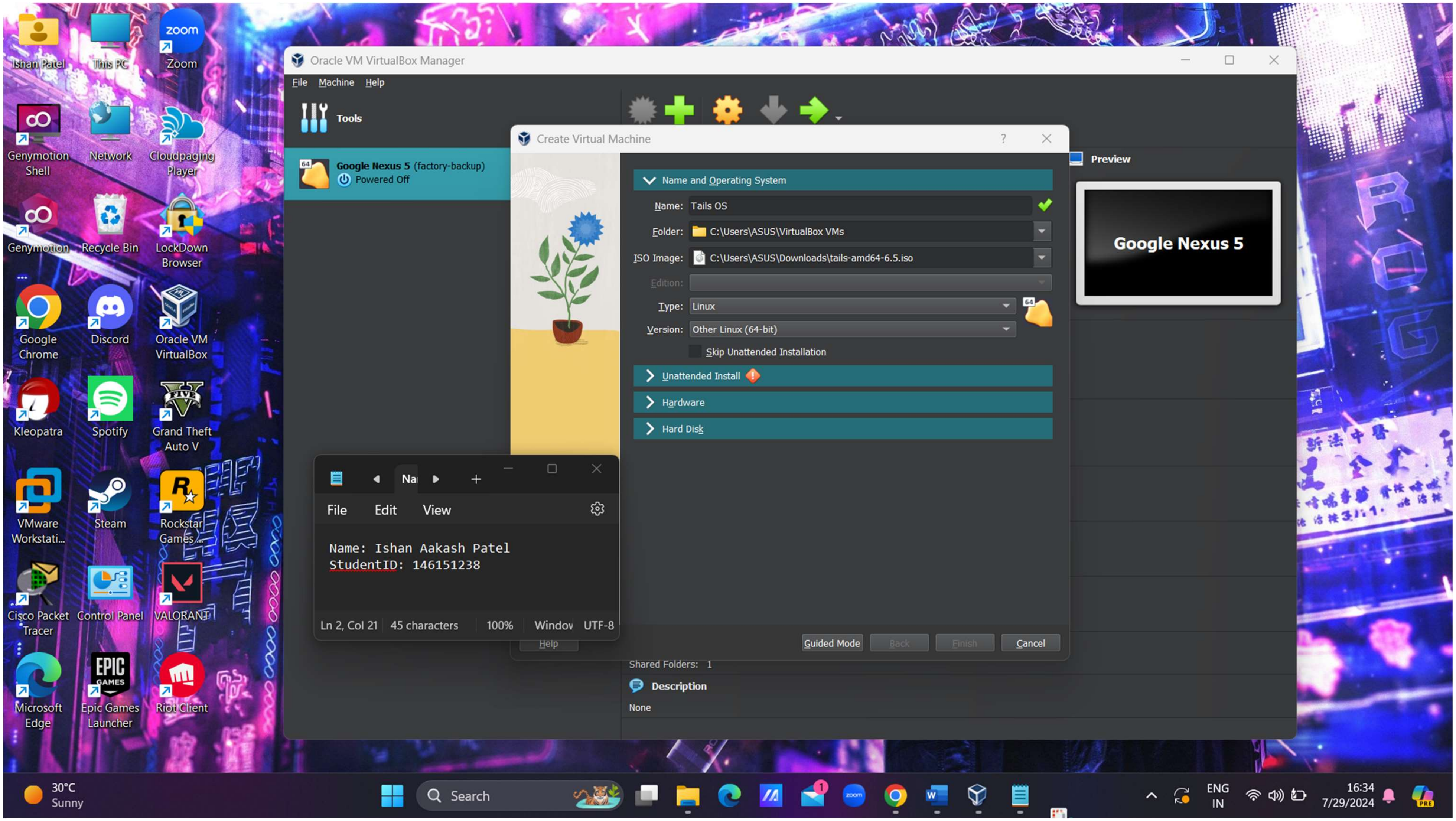
Na

File Edit View

```
Name: Ishan Aakash Patel
StudentID: 146151238
```

Ln 2, Col 21 | 45 characters | 100% | Windov | UTF-8

Figure 1 : Virtual Box



Name: Tails OS

Folder: C:\Users\ASUS\VirtualBox VMs

ISO Image: C:\Users\ASUS\Downloads\tails-amd64-6.5.iso

Edition:

Type: Linux

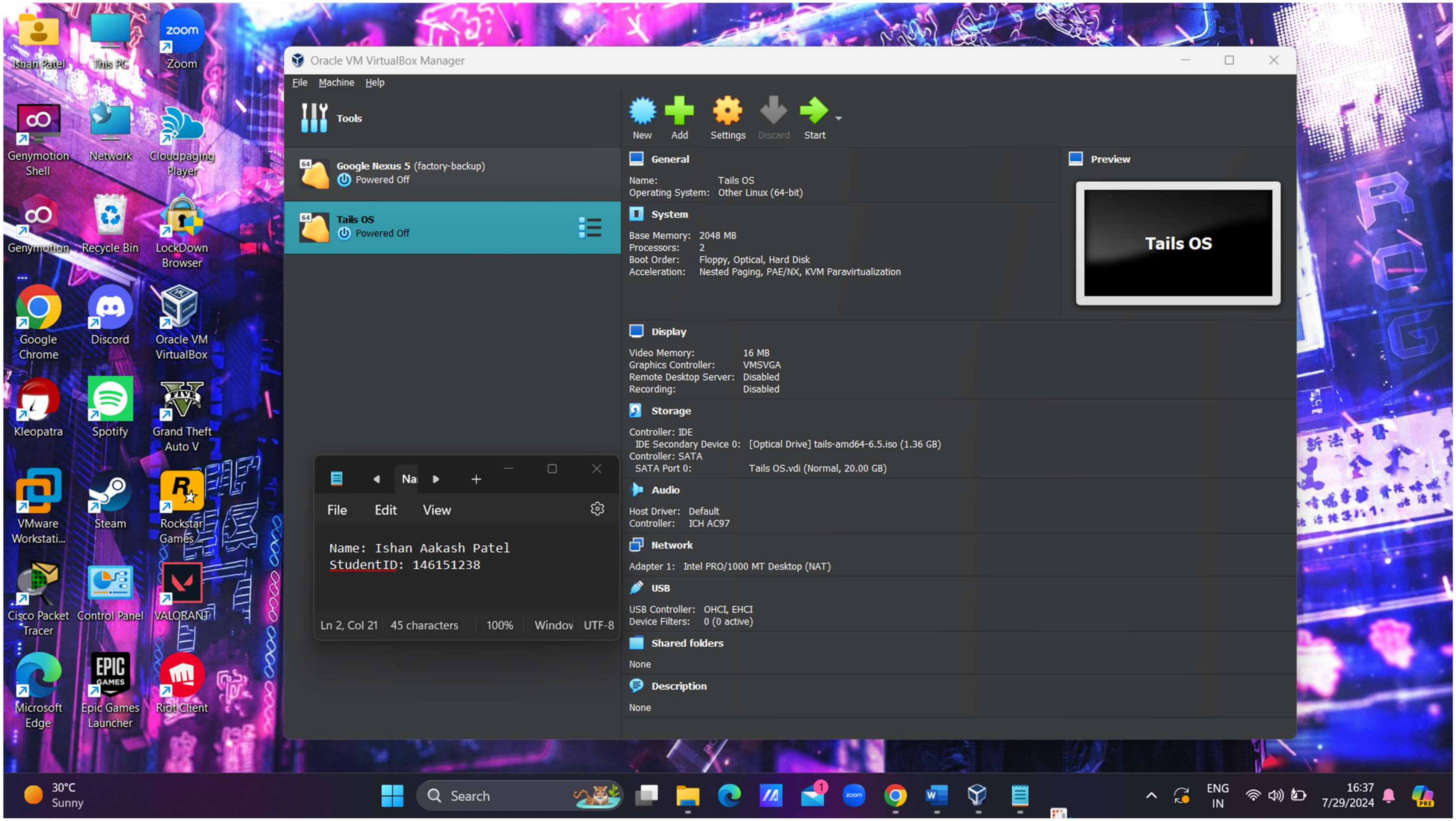
Version: Other Linux (64-bit)

□ Skip Unattended Installation

```
Name: Ishan Aakash Patel
StudentID: 146151238
```

Ln 2, Col 21 45 characters 100% Windov UTF-8

Figure 2 : Installing and Configuring tails OS



Google Nexus 5 (factory-backup)
Powered Off

Tails OS
Powered Off

General

Name: Tails OS
Operating System: Other Linux (64-bit)

System

Base Memory: 2048 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, PAE/NX, KVM Paravirtualization

Display

Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] tails-amd64-6.5.iso (1.36 GB)
Controller: SATA
SATA Port 0: Tails OS.vdi (Normal, 20.00 GB)

Audio

Host Driver: Default
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB

USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

Shared folders

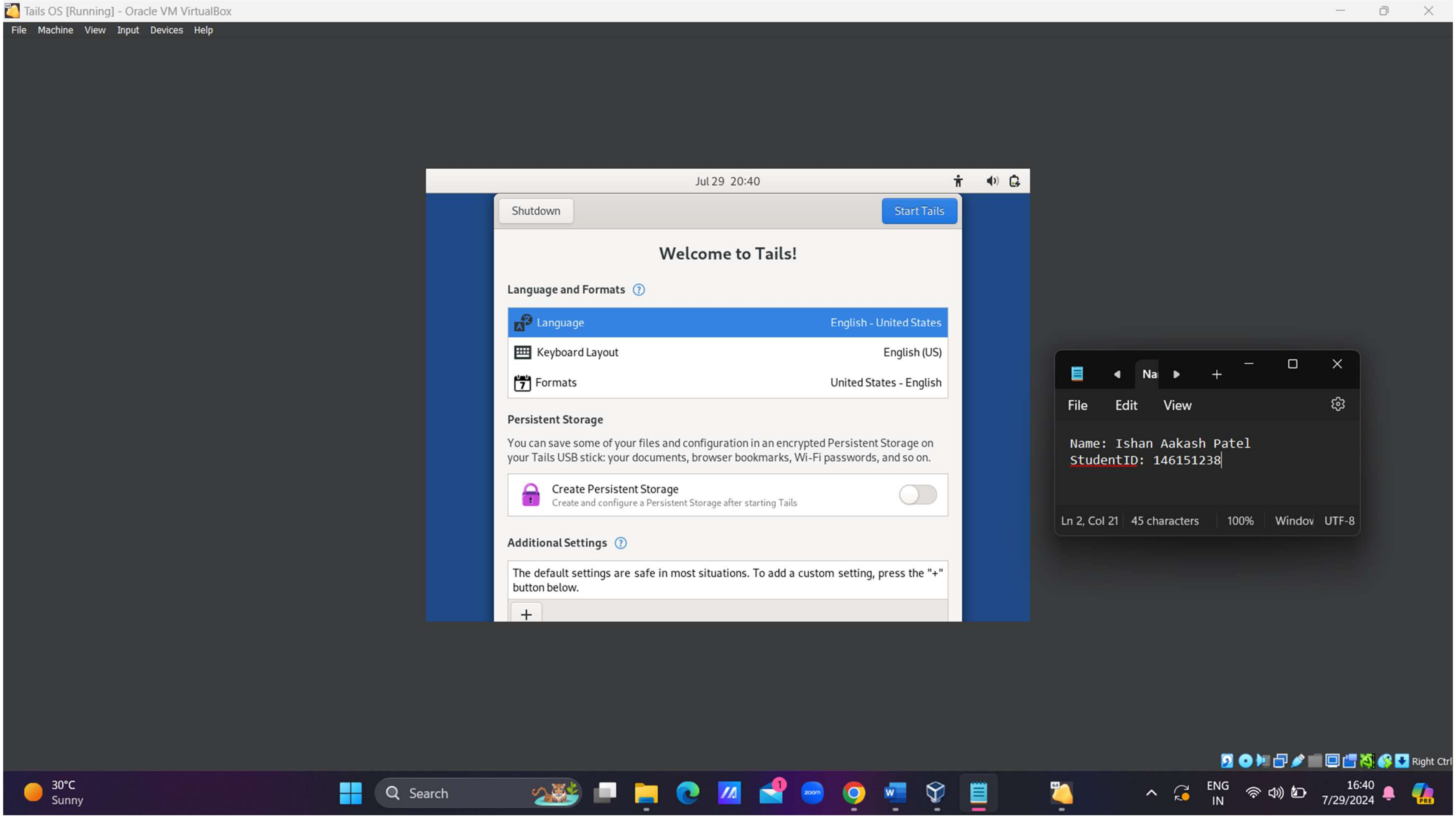
None

Description

None

```
Name: Ishan Aakash Patel
StudentID: 146151238
```

Ln 2, Col 21 | 45 characters | 100% | Window | UTF-8


Tails OS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Jul 29 20:40
Shutdown
Start Tails

Welcome to Tails!

Language and Formats

Language	English - United States
Keyboard Layout	English (US)
Formats	United States - English

Persistent Storage

You can save some of your files and configuration in an encrypted Persistent Storage on your Tails USB stick: your documents, browser bookmarks, Wi-Fi passwords, and so on.

Create Persistent Storage
Create and configure a Persistent Storage after starting Tails

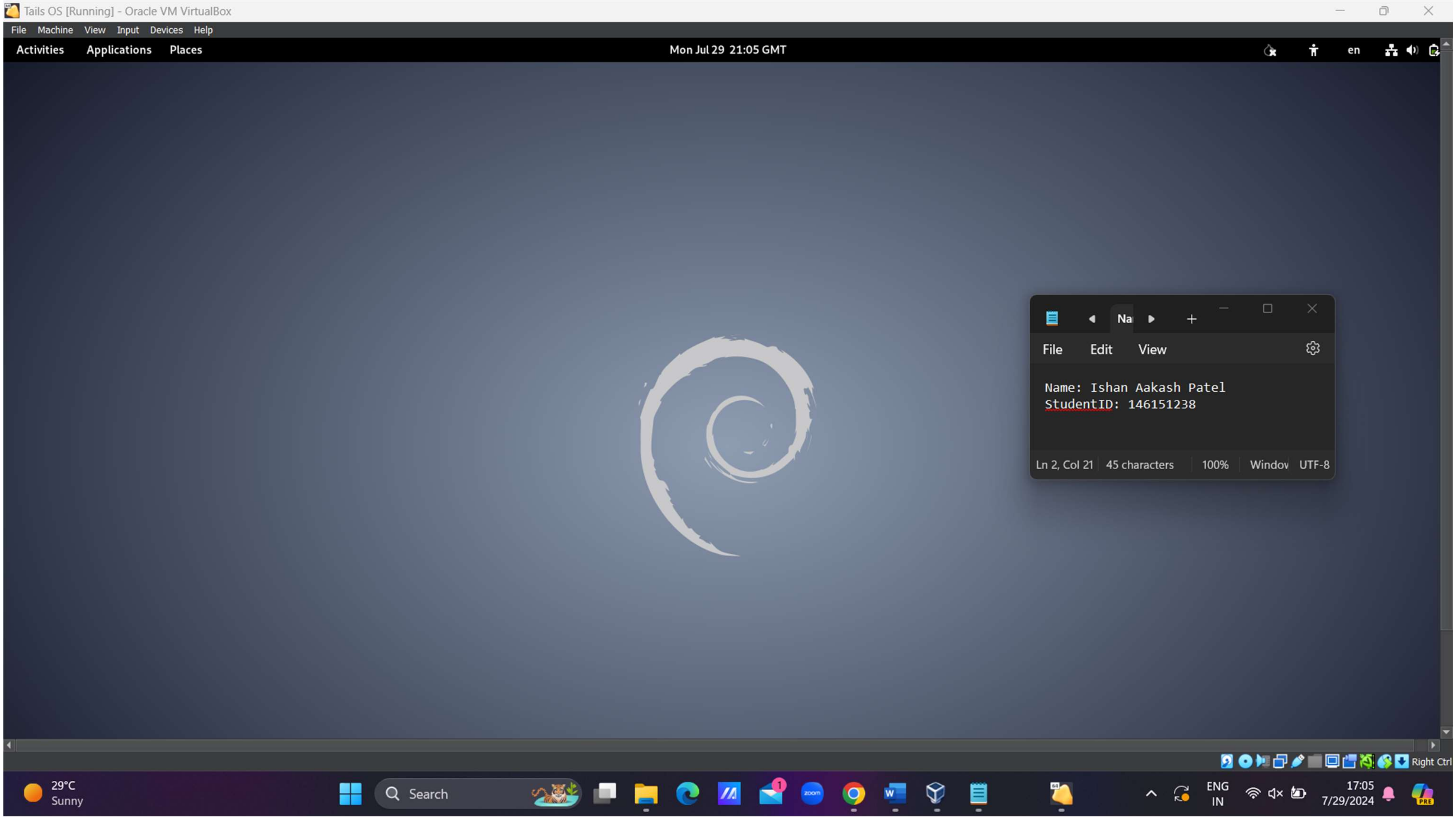
Additional Settings

The default settings are safe in most situations. To add a custom setting, press the "+" button below.

```
Name: Ishan Aakash Patel
StudentID: 146151238
```

Ln 2, Col 21 | 45 characters | 100% | Windov | UTF-8

Figure 3 : Tails OS Installed



```
Name: Ishan Aakash Patel
StudentID: 146151238
```

Questions and Answers

1. **What is Tails OS?**

Tails OS (The Amnesic Incognito Live System) is a security-focused Linux distribution designed to preserve privacy and anonymity. Its main purpose is to provide a secure, anonymous computing environment that leaves no trace on the computer you're using.

Main features of Tails OS:

- Runs from a USB stick or DVD
- Routes all internet traffic through the Tor network
- Includes pre-installed privacy and encryption tools
- Leaves no trace on the host computer after shutdown

2. **Why is Tails OS considered secure and anonymous?**

Tails OS is considered secure and anonymous due to several key features:

- Tor integration: All internet connections are routed through the Tor network, masking the user's IP address and location.
- Amnesia: It doesn't write to the computer's hard drive, leaving no trace after shutdown.
- Encryption: Built-in tools for encrypting files, emails, and instant messages.
- Open-source: The code is publicly available for scrutiny.
- Regular updates: Frequent security patches and updates.

3. **How does Tails OS handle data persistence?**

Tails OS primarily operates as a live system, meaning it doesn't save data by default. However, it offers options for data persistence:

- Persistent Storage: Users can create an encrypted partition on the Tails USB drive to store files, settings, and additional software.
- Persistence options: Users can choose which types of data to make persistent (e.g., personal files, network connections, browser bookmarks).

4. **How can you verify the integrity of the Tails OS ISO file before installation?**

To verify the Tails OS ISO file:

1. Download the ISO file and the corresponding signature file.
2. Import the Tails signing key.
3. Use a tool like GnuPG to verify the signature against the ISO file.
4. Check that the signature is valid and matches the official Tails signing key.
5. How does Tails OS ensure secure internet browsing?

7. Tails OS ensures secure browsing primarily through:

- Tor Browser: A modified version of Firefox that routes all traffic through the Tor network.
- NoScript: Blocks potentially dangerous JavaScript and other executable content.
- HTTPS Everywhere: Enforces secure connections to websites when available.
- Regular updates to address security vulnerabilities.

8. **What are the potential risks of using Tails OS on public networks, and how can they be mitigated?**

Risks:

- End-node monitoring: The exit node of the Tor network could potentially monitor unencrypted traffic.
- Physical surveillance: Someone could observe your screen or keystrokes.
- Malicious hotspots: Fake Wi-Fi networks could attempt to intercept data.

Mitigation strategies:

- Use HTTPS whenever possible.
- Avoid accessing sensitive information on public networks.
- Use a privacy screen to prevent visual eavesdropping.
- Verify the legitimacy of public Wi-Fi networks before connecting.

10. How do you install additional software on Tails OS?

Installing additional software on Tails OS:

1. Enable the Additional Software feature in the Persistent Storage.
2. Use the Synaptic Package Manager to search for and install software.
3. Alternatively, use the command line with 'sudo apt-get install [package-name]'.
4. Remember that additional software will only persist if you've enabled the appropriate persistence option.
5. What tools does Tails OS provide for secure communication?

11. Tails OS includes several tools for secure communication:

- Thunderbird with Enigmail for encrypted email
- Pidgin with OTR for encrypted instant messaging
- OnionShare for secure file sharing
- MAT (Metadata Anonymization Toolkit) for removing metadata from files

12. How can you securely transfer files using Tails OS?

Methods for secure file transfer in Tails OS:

- OnionShare: Creates a temporary onion service for secure file sharing.
- Encrypted email attachments using Thunderbird and Enigmail.
- Use of encrypted storage devices.
- Secure file transfer protocols like SFTP through Tor.

13. Why is Tails OS a suitable environment for malware analysis?

Tails OS is suitable for malware analysis because:

- It's isolated from the host system, preventing accidental infection.
- It leaves no trace on the host computer.

- It includes tools useful for analysis (e.g., network monitoring tools).
- Its amnesic nature allows for a clean environment for each analysis session.

14. Setting Up a Secure Malware Analysis Environment in Tails OS

1. Boot Tails OS:
   - Start your computer with Tails OS from a USB stick. This ensures your work is not saved and remains anonymous.
2. Configure Tor and Networking:
   - Tails OS uses the Tor network to anonymize your internet connection. Make sure Tor is running properly and your internet connection is secure.
3. Update Tails OS and Tools:
   - Keep Tails OS and all installed tools up to date to protect against known vulnerabilities.
4. Install Necessary Analysis Tools:
   - While Tails comes with some tools, you may need additional software. Install tools like ClamAV (for scanning), Wireshark (for network analysis), and volatility (for memory analysis) from trusted sources.
5. Create a Virtual Machine (Optional):
   - Use a virtual machine (VM) within Tails to isolate the malware and prevent it from affecting your main system. VirtualBox can be used for this purpose.
6. Isolate the Analysis Environment:
   - Use Tails' built-in "Unsafe Browser" or "Amnesic Incognito Live System" features to keep your analysis isolated from your primary activities.
7. Disable Network if Necessary:
   - Disconnect from the internet during analysis to prevent malware from communicating with external servers.
8. Use Read-Only Media:
   - Analyze files from read-only media (e.g., CD/DVD or write-protected USB) to prevent malware from spreading.

9. Set Up Safe Data Storage:
   - Use encrypted storage devices if you need to save data. Tails OS supports encryption for this purpose.

15. Capturing Network Traffic in Tails OS

1. Install Wireshark:
   - Wireshark is a popular tool for capturing and analyzing network traffic. It can be installed from the Tails package manager.
2. Start Wireshark:
   - Open Wireshark and select the network interface you want to monitor (usually "eth0" for wired connections or "wlan0" for wireless).
3. Begin Capture:
   - Click the "Start" button to begin capturing network traffic. Wireshark will display the captured packets in real time.
4. Analyze Traffic:
   - Use Wireshark's filtering and analysis tools to inspect the captured traffic. Look for suspicious connections, unusual protocols, or unexpected data transfers.
5. Save Capture:
   - Save the capture file for later analysis or reporting. Use encrypted storage if necessary.

16. Precautions When Analyzing Malware on Tails OS

1. Isolate the Malware:
   - Always use a VM or a sandbox environment to isolate the malware from your main system.
2. Disable Networking:
   - Disconnect from the internet to prevent the malware from communicating with external servers.
3. Use Read-Only Media:
   - Analyze malware from read-only media to prevent it from spreading.

4. Use Strong Encryption:
    - Encrypt any data or files saved during analysis to protect sensitive information.
5. Be Aware of Legal Implications:
    - Ensure that you have the legal right to analyze the malware, especially if it belongs to someone else.
6. Avoid Personal Data Exposure:
    - Do not expose personal or sensitive data during analysis, as the malware may attempt to exfiltrate it.
7. Dispose of the Environment Safely:
    - After analysis, securely wipe the VM or environment to prevent any residual malware from persisting.

17. ClamAV for Malware Analysis on Tails

ClamAV is an open-source antivirus engine that can be used to scan files for malware. Here's how to use it in Tails:

1. Install ClamAV:
    - Use the Tails package manager to install ClamAV.
2. Update Virus Definitions:
    - Run freshclam to update ClamAV's virus definitions. This ensures you have the latest information on malware signatures.
3. Scan Files:
    - Use the command clamscan -r /path/to/directory to scan files or directories for malware. The -r flag allows recursive scanning.
4. Review Scan Results:
    - Check the output for any detected threats. ClamAV will list files that are infected and provide details.
5. Take Action:
    - Quarantine or delete infected files based on your findings and organizational policies.

18. Practical Application: Analyzing a Suspicious File in Tails OS

Scenario: You receive a suspicious email attachment and want to analyze it safely using Tails OS.

Steps:

1. Boot Tails OS:
   - Start your system with Tails OS from a USB stick.
2. Set Up a VM:
   - Create a virtual machine to contain the suspicious file.
3. Disable Networking:
   - Disconnect the VM from the internet to prevent potential communication from the malware.
4. Transfer the File:
   - Use a read-only USB stick to transfer the file to the VM.
5. Initial Scan:
   - Use ClamAV to scan the file for known malware.
6. Behavioral Analysis:
   - Run the file in the VM and monitor its behavior using tools like Wireshark (for network activity) and Process Explorer (for process activity).
7. Document Findings:
   - Record any suspicious activity, file modifications, or network connections.
8. Secure the VM:
   - After analysis, securely wipe the VM to remove any traces of the malware.

19. Securely Reporting Findings Using Tails OS

1. Encrypt Reports:
   - Use tools like GnuPG to encrypt your findings before sending them. This protects the information from being intercepted.

2. Use Secure Communication Channels:
    - Send the report through secure channels like encrypted email or secure file-sharing services.
3. Anonymize Data:
    - Remove any personally identifiable information from your report to protect your identity and privacy.
4. Use Tor for Anonymity:
    - Use the Tor network to send your report, ensuring your connection is anonymous and secure.
5. Confirm Receipt:
    - If possible, confirm that the recipient has securely received and decrypted the report.

20. Limitations of Using Tails OS for Malware Analysis

1. Limited Persistent Storage:
    - Tails OS is designed to leave no trace, which can make it challenging to store large datasets or logs persistently.
2. Software Limitations:
    - The range of available software might be limited compared to other Linux distributions, potentially missing specialized analysis tools.
3. Resource Constraints:
    - Running analysis in a live environment can be resource-intensive, and Tails OS may not provide the same performance as a dedicated analysis machine.
4. Lack of Persistent Environment:
    - Since Tails OS resets after each session, setting up tools and environments repeatedly can be time-consuming.
5. Network Anonymity Restrictions:
    - The Tor network, while providing anonymity, can slow down internet speeds, affecting tasks like downloading large malware samples or updates.

22. **Watch the following videos - https://www.youtube.com/watch?v=VtzwfX0NgKA, https://www.youtube.com/watch?v=u5Lv_HXICpo&t=0s and provide feedback on Tails OS. This is free writing highlighting your thoughts on Tails OS.**

    Tails OS, short for The Amnesic Incognito Live System, is an operating system designed with a strong emphasis on privacy and anonymity. After watching the videos, I found Tails to be an impressive tool for individuals needing to protect their online activities from surveillance. The system routes all internet traffic through the Tor network, which anonymizes users by masking their IP addresses and encrypting their internet traffic. This feature makes Tails particularly useful for journalists, activists, and anyone who needs to maintain a high level of privacy online.

    Another key feature of Tails is its "amnesic" nature, which means it does not leave any trace of the user's activities on the computer. This is achieved by running the operating system entirely from a USB stick or DVD, without installing anything on the hard drive. Once the session ends, all data and activities are wiped out, providing an additional layer of security. Moreover, Tails includes various tools for secure communication, such as encrypted email and messaging, making it a comprehensive solution for anyone concerned about privacy. The user-friendly interface and built-in privacy tools make it accessible even to those who may not be technically savvy.

Learning Experience

Working on this assignment has provided me with a deep understanding of Tails OS and its applications in cybersecurity. Setting up a secure malware analysis environment in Tails OS allowed me to grasp the importance of privacy and anonymity in digital forensics. The process of booting Tails OS, setting up virtual machines, and using tools like ClamAV for malware detection highlighted the critical steps in creating a safe environment for analyzing potentially dangerous files. This hands-on experience reinforced the concepts of isolating the malware, ensuring the environment's integrity, and maintaining secure communication channels.

Additionally, learning about network traffic analysis and the precautions necessary when handling malware underscored the complexity and risks involved in cybersecurity. The importance of using secure methods for reporting findings and understanding the limitations of using Tails OS in a virtualized environment also became clear. This assignment not only enhanced my technical skills but also emphasized the ethical considerations and the need for rigorous security measures in cybersecurity practices.