Official documentation for CyPHER

Please be advised that this is a project undertaken by second-year students of Computer Science and Engineering (CSE) and is not intended as a comprehensive application; rather, it serves as an educational endeavour. Our efforts aim to provide practical experience and application of theoretical knowledge within the scope of our academic curriculum and research done till date. It is crucial to recognize that this project is primarily an educational exercise and may not attain the standards or functionality associated with a fully developed application. Your understanding of this educational focus is greatly appreciated.

Usage:

Our software serves as a robust tool for analysing network traffic, evaluating its safety, and identifying potential threats such as DDoS, SSH, Web attacks, BotNet, Infiltration, and Heartbleed. Upon system boot, the software initiates a packet sniffing phase for 60 seconds every ten minutes. The collected data is then processed through an API hosted on a complimentary server.

Please be aware that the analysis may require some time, as our software is provided free of charge and relies on a free server for hosting.

The real-time analysis of 60 seconds every 10 minutes can be stopped by simply clicking on “Stop real-time analysis”

In addition to its primary network analysis capabilities, our software includes an advanced feature designed to detect newly connected external drives. Upon detecting a new external drive, users will receive a notification prompting them to either initiate a scan or skip the scanning process. This feature encourages users to exercise caution when interacting with files on the detected external drive, ensuring a thorough assessment of its safety status. It serves as a proactive measure to identify and address potential security concerns associated with external drives deemed "potentially" unsafe.

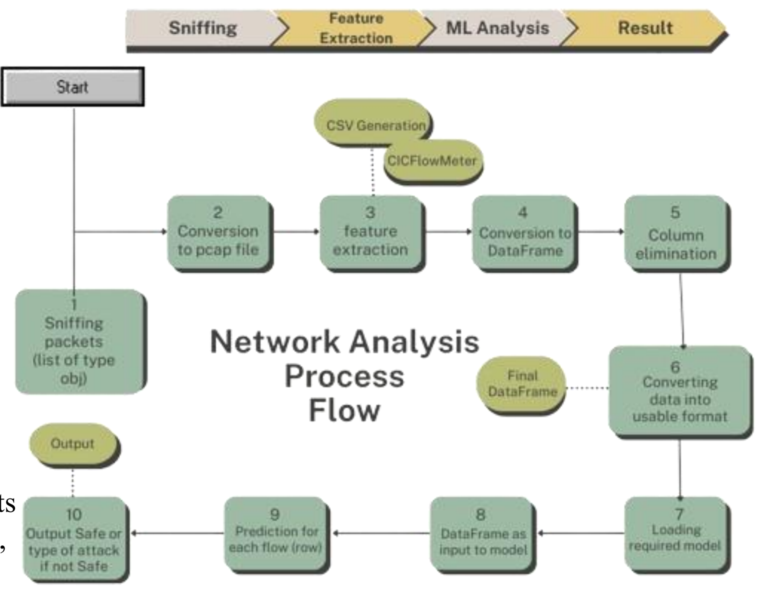
As for now this has only been developed for WINDOWS systems only.

Working:

Here we will talk about the brief understanding of how the software works and all the modules/ dependencies used to build the software.

Towards the left is a diagram, a flowchart, simplifying the Network analysis process flow into 10 steps.

Using the python module scapy, we were able to capture packets for a specified duration, here in this case 60 secs, by interacting with the OS kernel to set up packet capture. Mainly interacting with Data-Link Layer and Network Layer considering the OSI model. The captured packets are parsed and extracting necessary information,



Sniffing
Feature Extraction
ML Analysis
Result
Start
CSV Generation
CICFlowMeter
2 Conversion to pcap file
3 feature extraction
4 Conversion to DataFrame
5 Column elimination
1 Sniffing packets (list of type obj)
Network Analysis Process Flow
Final DataFrame
6 Converting data into usable format
Output
10 Output Safe or type of attack if not Safe
9 Prediction for each flow (row)
8 DataFrame as input to model
7 Loading required model

Figure 1: Flowchart of Network Analysis Process Flow

returning a list of Packet objects which are then save to a file in the libpcap format, hence converting the List of Packet Objects to a pcap file. The pcap file is then analyzed by CICFlowMeter, mainly for feature extraction. It reads pcap files containing captured network traffic; for each packet, it analyzes the source and destination addresses, creating bidirectional flows (bi-flows) representing the communication between two endpoints.

CICFlowMeter creates unique “flow-key” for each bi-directional flow using the Source IP, Dest IP, Source Port, Dest Port, and Protocol. By analysing packets that have the same “flow key” are grouped together into the same bi-flow. This creates a continuous representation of the communication between two endpoints. Hence, to put it in simpler terms CICFlowMeter provides a higher-level view of network traffic as flows instead of a long list of packets.

The CSV generated by CICFlowMeter, where each row represents a flow and each column is a different feature of the flow, is converted into a pandas DataFrame. Next, the columns which are not required are dropped and further the DataFrame is converted into a more usable format by replacing infinity values with 0, filling NaN values with 0, etc.

Finally, the DataFrame goes through a loop where each flow(row) is analysed and predicted by a pre-trained model accordingly.

We have used AdaBoost, Random Forest, K-Nearest Neighbours

Getting Started

Dependencies:

- Windows 10 or above suggested
- Internet connection required for both network analysis and USB file scanning
- WinPcap
- Java Runtime Environment

Installing:

Website: webisteLink.com

To download and install our software on a Windows system, please follow these steps:

1. **Access the Download Page:**

   Scroll down on our website until you find the "Download for Windows ↓" button. Click on the button to initiate the download of a zip file.

2. **Extract Files**:

   After downloading, extract the contents of the zip file. Locate the executable file named cypher_py.exe, which serves as the main program.

3. **Install WinPcap**:

   In the extracted files, find the "WinPcap_4_1_3.exe" file. Execute this file to launch the installation wizard for WinPcap. Follow the instructions provided by the wizard to complete the installation of WinPcap.

4. **Configure Java Runtime Environment**:

Before using the main software, ensure that the Java Runtime Environment (JRE) variable is set up on your system. Follow these instructions to ensure a smooth setup for Java development.

Set Up Java Environment Variable (Windows 11):

a. **Access Environment Variables**:
Press the Windows key and search for "**Environment variables**"

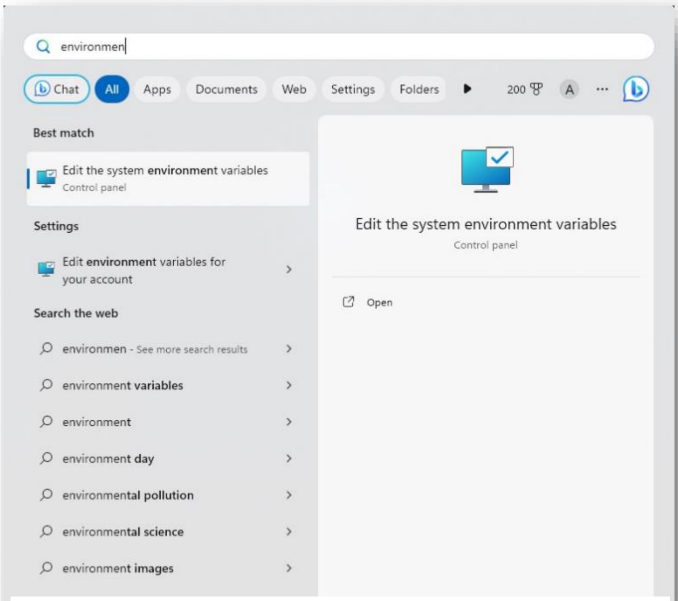
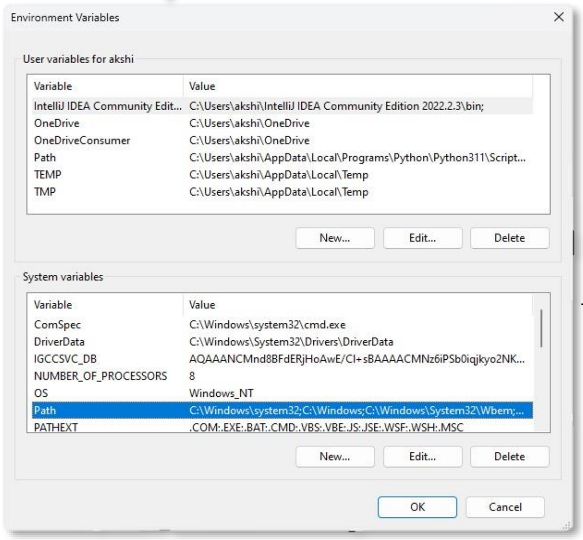


Figure 2: Access Environment Variables

b. **Verify JDK Path**
Check for the Java JDK path in your system variables.
If "<u>`C:\Program Files\Common Files\Oracle\Java\javapath`</u>" is not present in your system variables' PATH section, proceed to the next step.



Environment Variables

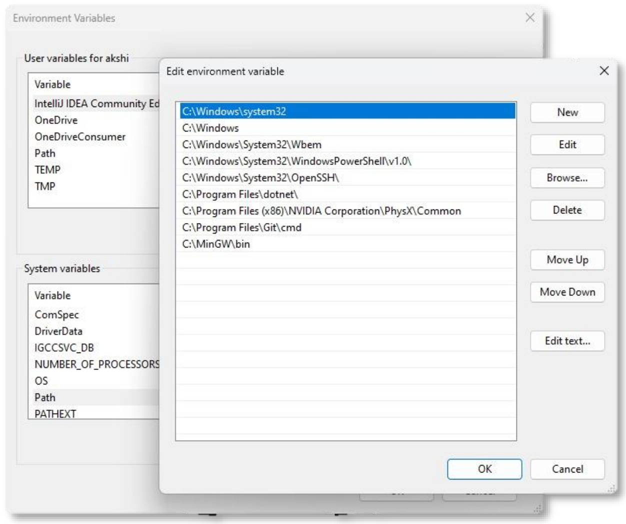
User variables for akshi

Variable	Value
IntelliJ IDEA Community Edit...	C:\Users\akshi\IntelliJ IDEA Community Edition 2022.2.3\bin;
OneDrive	C:\Users\akshi\OneDrive
OneDriveConsumer	C:\Users\akshi\OneDrive
Path	C:\Users\akshi\AppData\Local\Programs\Python\Python311\Script...
TEMP	C:\Users\akshi\AppData\Local\Temp
TMP	C:\Users\akshi\AppData\Local\Temp

System variables

Variable	Value
ComSpec	C:\Windows\system32\cmd.exe
DriverData	C:\Windows\System32\Drivers\DriverData
IGCCSVC_DB	AQAAANCMnd8BFdERjHoAwE/Cl+sBAAAACMNz6iPSb0iqjkyo2NK...
NUMBER_OF_PROCESSORS	8
OS	Windows_NT
Path	C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;...
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC

Figure 4: Navigate to the path section in the system variables



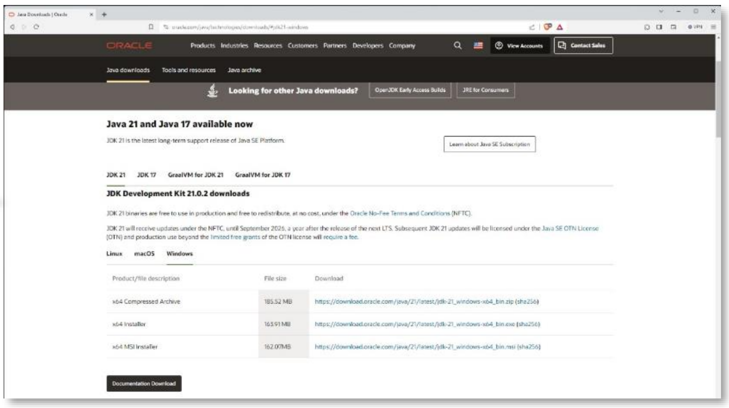
Edit environment variable

```
C:\Windows\system32
C:\Windows
C:\Windows\System32\Wbem
C:\Windows\System32\WindowsPowerShell\v1.0\
C:\Windows\System32\OpenSSH\
C:\Program Files\dotnet\
C:\Program Files (x86)\NVIDIA Corporation\PhysX\Common
C:\Program Files\Git\cmd
C:\MinGW\bin
```

Figure 3: Cross check the JAVA path

c. Download JAVA for Windows

Open your browser and download Java for Windows using the MSI installer.



Java Downloads | Oracle
ORACLE
Products Industries Resources Customers Partners Developers Company
View Accounts
Contact Sales
Java downloads Tools and resources Java archive
Looking for other Java downloads?
OpenJDK Early Access Builds
JRE for Consumers
Learn about Java SE Subscription
JDK 21 JDK 17 GraalVM for JDK 21 GraalVM for JDK 17
Linux macOS Windows
Documentation Download

Java 21 and Java 17 available now

JDK 21 is the latest long-term support release of Java SE Platform.

JDK Development Kit 21.0.2 downloads

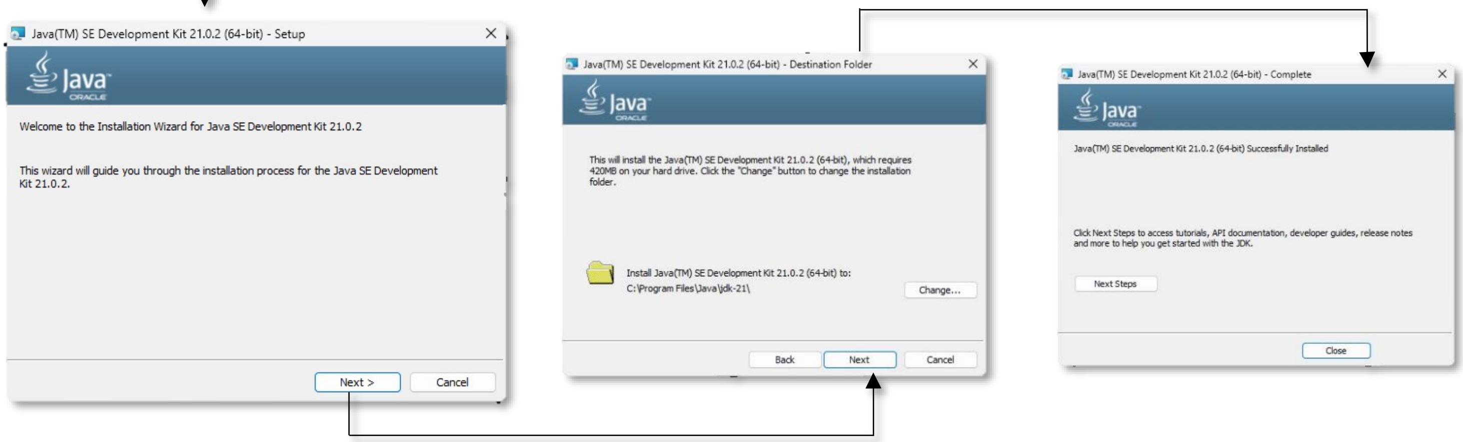
JDK 21 binaries are free to use in production and free to redistribute, at no cost, under the Oracle No-Fee Terms and Conditions (NFTC).

JDK 21 will receive updates under the NFTC, until September 2026, a year after the release of the next LTS. Subsequent JDK 21 updates will be licensed under the Java SE OTN License (OTN) and production use beyond the limited free grants of the OTN license will require a fee.

Product/file description	File size	Download
x64 Compressed Archive	185.52 MB	https://download.oracle.com/java/21/latest/jdk-21_windows-x64_bin.zip (sha256)
x64 Installer	163.91 MB	https://download.oracle.com/java/21/latest/jdk-21_windows-x64_bin.exe (sha256)
x64 MSI Installer	162.07MB	https://download.oracle.com/java/21/latest/jdk-21_windows-x64_bin.msi (sha256)

Figure 5: Download JAVA from official website

Accept all terms and conditions during the installation process.
Complete the installation of Java.



Java(TM) SE Development Kit 21.0.2 (64-bit) - Setup
Java
ORACLE
Next >
Cancel
Java(TM) SE Development Kit 21.0.2 (64-bit) - Destination Folder
Change...
Back
Next
Cancel
Java(TM) SE Development Kit 21.0.2 (64-bit) - Complete
Next Steps
Close

Welcome to the Installation Wizard for Java SE Development Kit 21.0.2

This wizard will guide you through the installation process for the Java SE Development Kit 21.0.2.

This will install the Java(TM) SE Development Kit 21.0.2 (64-bit), which requires 420MB on your hard drive. Click the "Change" button to change the installation folder.

Install Java(TM) SE Development Kit 21.0.2 (64-bit) to:
C:\Program Files\Java\jdk-21\

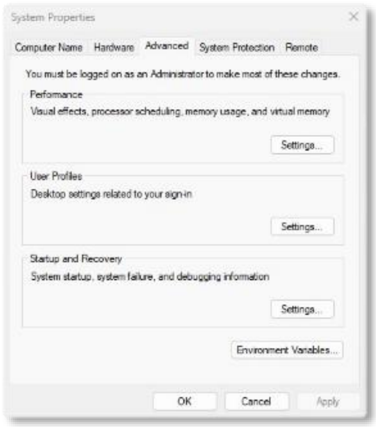
Java(TM) SE Development Kit 21.0.2 (64-bit) Successfully Installed

Click Next Steps to access tutorials, API documentation, developer guides, release notes and more to help you get started with the JDK.

Figure 6-8: Installation Steps

d. Verify System Variables

Check the system variables for the path mentioned above "`C:\Program Files\Common Files\Oracle\Java\javapath`".

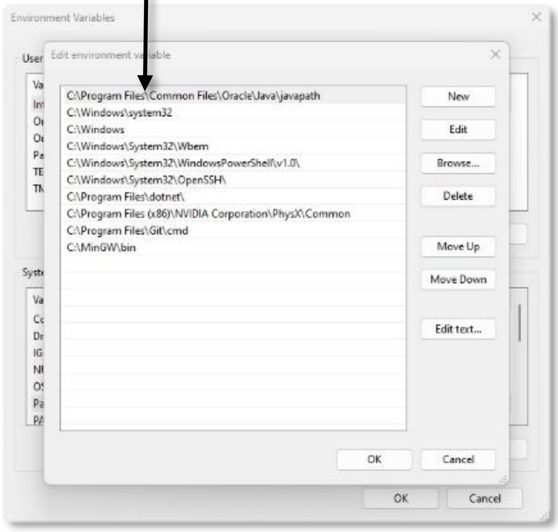


You must be logged on as an Administrator to make most of these changes.

Visual effects, processor scheduling, memory usage, and virtual memory

Desktop settings related to your sign-in

System startup, system failure, and debugging information



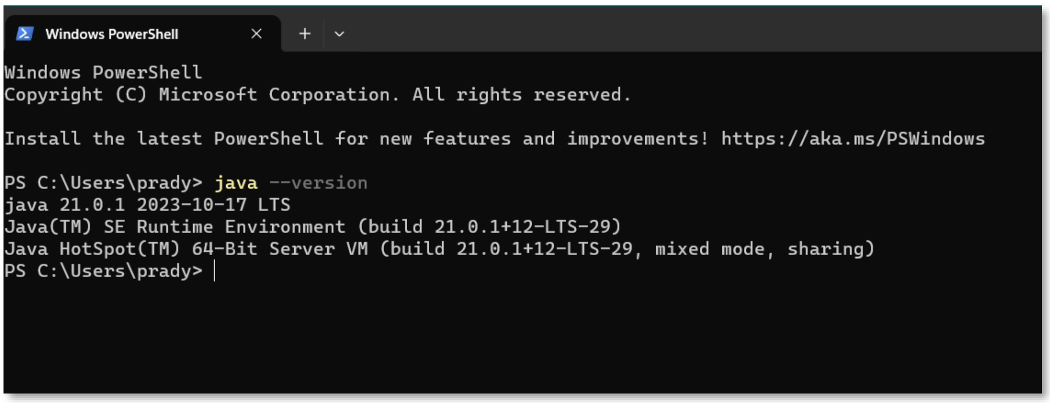
```
C:\Program Files\Common Files\Oracle\Java\javapath
C:\Windows\system32
C:\Windows
C:\Windows\System32\Wbem
C:\Windows\System32\WindowsPowerShell\v1.0\
C:\Windows\System32\OpenSSH\
C:\Program Files\dotnet\
C:\Program Files (x86)\NVIDIA Corporation\PhysX\Common
C:\Program Files\Git\cmd
C:\MinGW\bin
```

Figure 9 &10: Verifying the JDK Path

e. Check JAVA Version

Open the command prompt or Windows PowerShell.

Run the command *java --version* to check the installed Java version.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\prady> java --version
java 21.0.1 2023-10-17 LTS
Java(TM) SE Runtime Environment (build 21.0.1+12-LTS-29)
Java HotSpot(TM) 64-Bit Server VM (build 21.0.1+12-LTS-29, mixed mode, sharing)
PS C:\Users\prady>
```

Figure 11: Checking JAVA Version

You are now ready to use the main software. Execute cypher_py.exe to launch the application.

Contributors:

Pradyumna Jonnalagadda

Baba Gandhi Kandagatla

Kummari Sai Teja

Sagar Puppala

Bharadwaj Reddy

Gnana Lakshmi Priya Darshini

Version History:

- 0.1.0
    - Initial release

Acknowledgements:

- Iman Sharafaldin, Arash Habibi Lashkari, and Ali A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization”, 4th International Conference on Information Systems Security and Privacy (ICISSP), Portugal, January 2018 IDS 2017 | Datasets | Research | Canadian Institute for Cybersecurity | UNB

- Pre-Trained Models kahramankostas/Anomaly-Detection-in-Networks-Using-Machine-Learning: A thesis submitted for the degree of Master of Science in Computer Networks and Security (github.com)

- CICFlowMeter Applications | Research | Canadian Institute for Cybersecurity | UNB

  CanadianInstituteForCybersecurity/CICFlowMeter: CICFlowmeter-V4.0 (formerly known as ISCXFlowMeter) is a network traffic Bi-flow generator and analyzer for anomaly detection that has been used in many Cybersecurity datsets such as Android Adware-General Malware dataset (CICAAGM2017), IPS/IDS dataset (CICIDS2017), Android Malware dataset (CICAndMal2017) and Distributed Denial of Service (CICDDoS2019). (github.com)