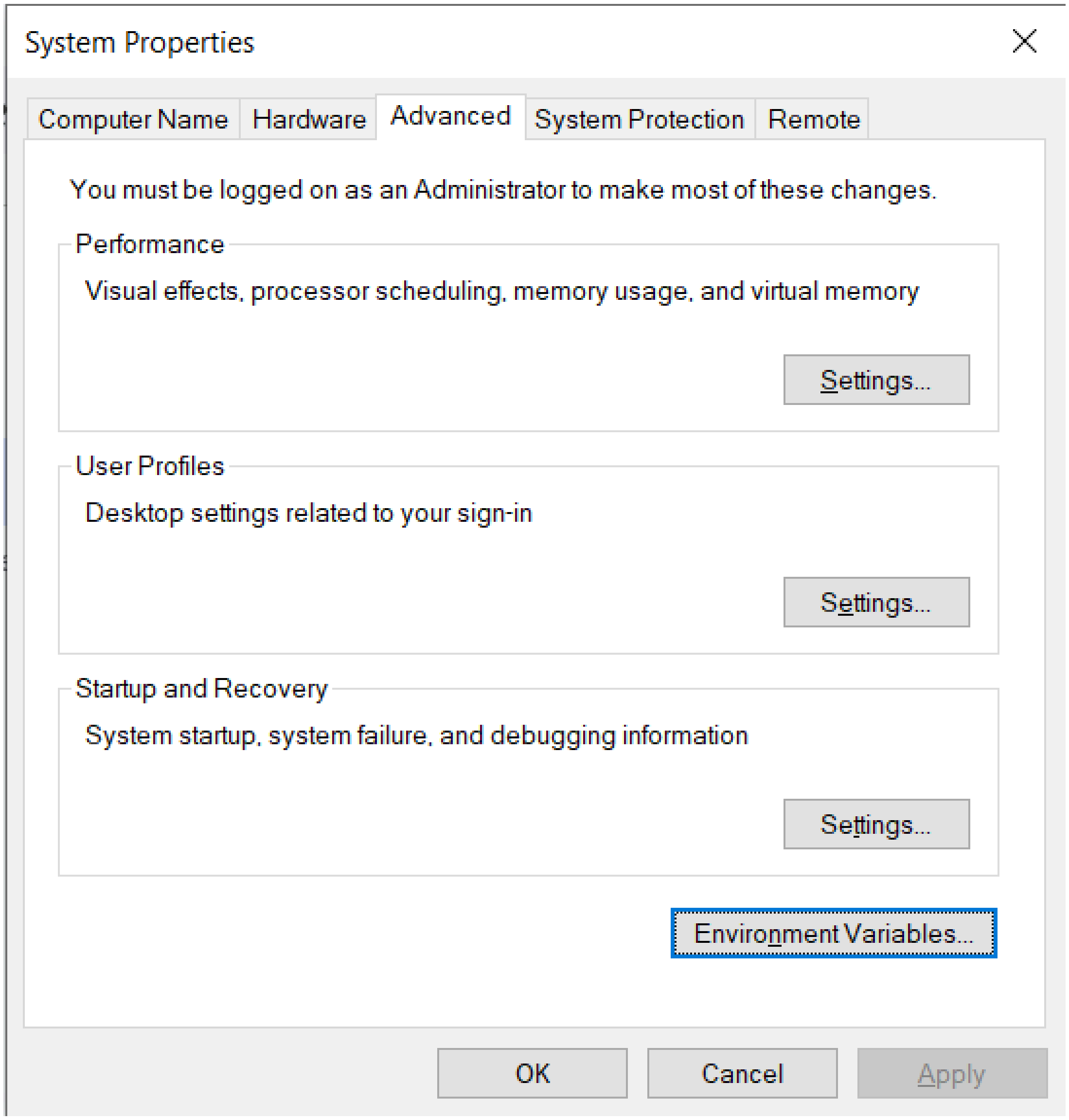
SSL/TLS setup for decrypting the data packets

Windows

1. Goto **Local Disk C -> Users -> Aditya Kulkarni** (Note: instead of Aditya Kulkarni, you will have your system name).
2. Create a folder named **SSLKeys**, and go inside this folder to create a file named **sslkeylog.log**
3. Search using **Windows key + S** and type **Environment Variables**.



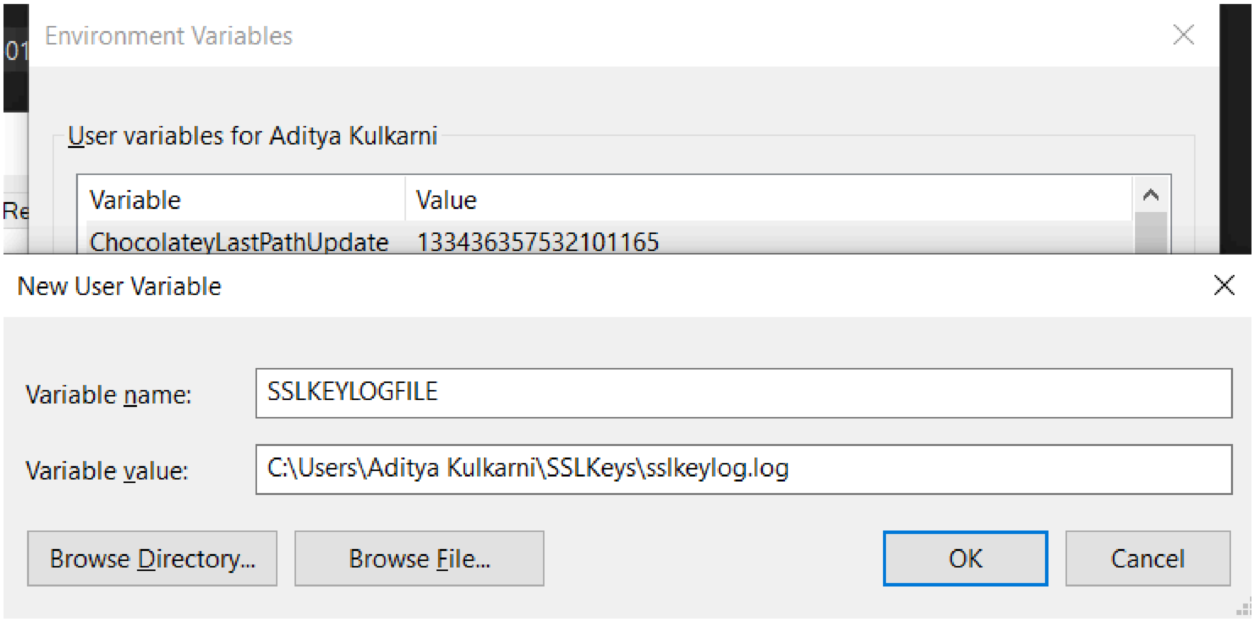
You must be logged on as an Administrator to make most of these changes.

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

Desktop settings related to your sign-in

System startup, system failure, and debugging information

4. In the **User Variables** section, click on New type the path to the created file **sslkeylog.log** and click on the **OK** button. Example:



Environment Variables

User variables for Aditya Kulkarni

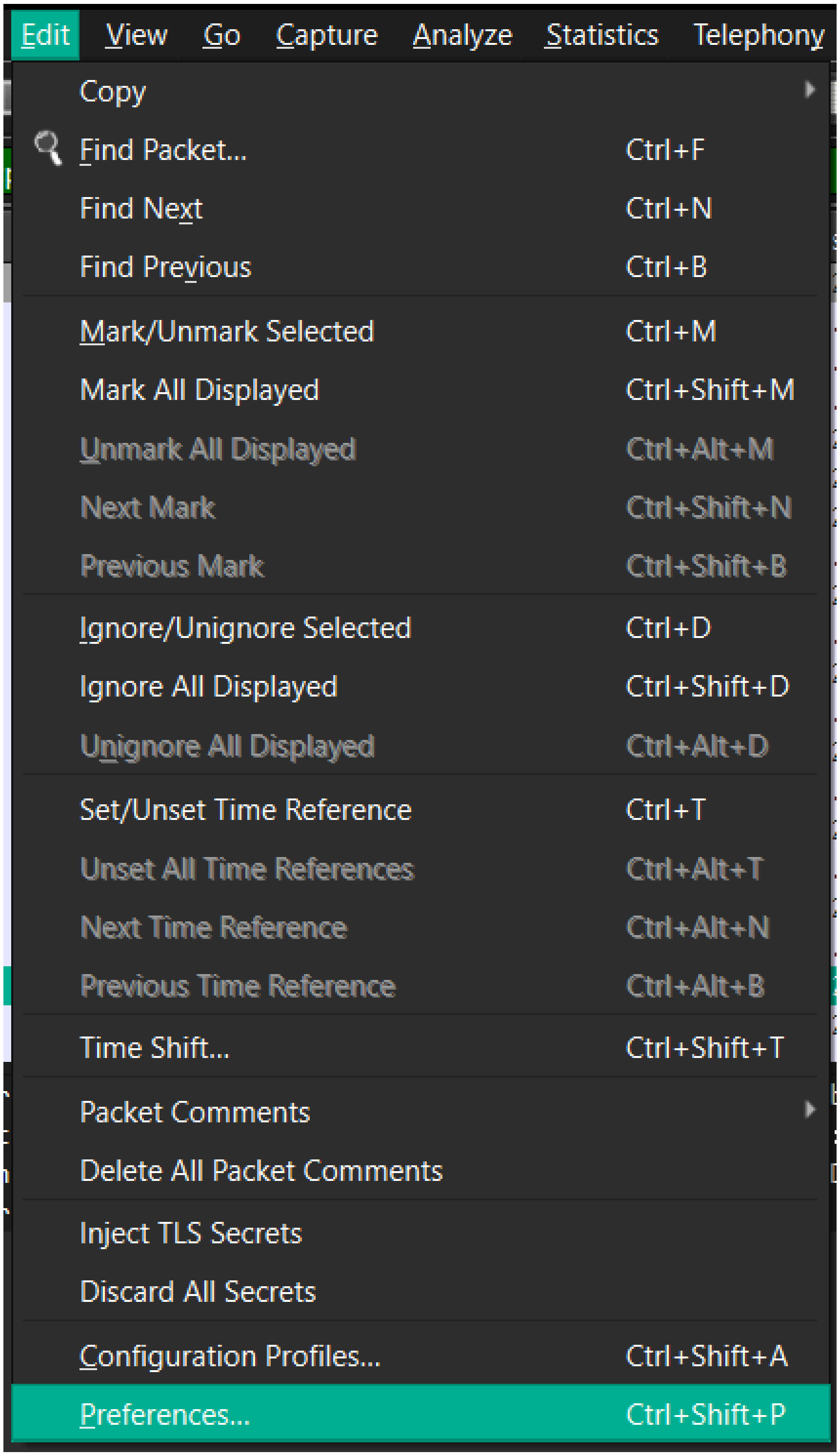
Variable	Value
ChocolateyLastPathUpdate	133436357532101165

New User Variable

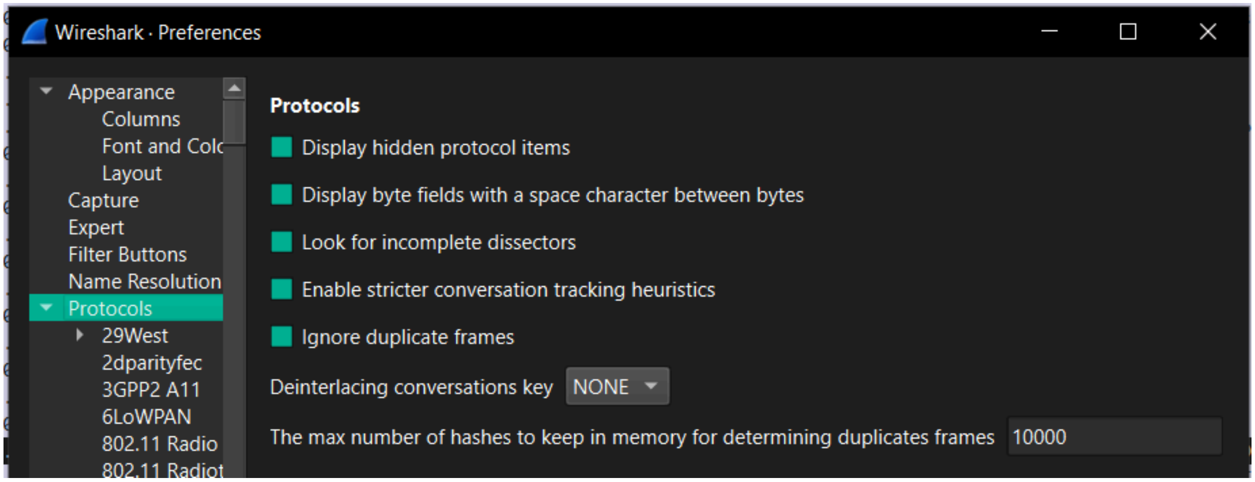
Variable name: SSLKEYLOGFILE

Variable value: C:\Users\Aditya Kulkarni\SSLKeys\sslkeylog.log

5. Restart your system
6. Open Wireshark, and in a browser type a URL (e.g., iitdh.ac.in) and capture the trace file.
7. Save the trace as a `.pcap` file, and follow the instructions
    a. Goto **Edit -> Preferences**


Edit
View
Go
Capture
Analyze
Statistics
Telephony
Copy
Find Packet... Ctrl+F
Find Next Ctrl+N
Find Previous Ctrl+B
Mark/Unmark Selected Ctrl+M
Mark All Displayed Ctrl+Shift+M
Unmark All Displayed Ctrl+Alt+M
Next Mark Ctrl+Shift+N
Previous Mark Ctrl+Shift+B
Ignore/Unignore Selected Ctrl+D
Ignore All Displayed Ctrl+Shift+D
Unignore All Displayed Ctrl+Alt+D
Set/Unset Time Reference Ctrl+T
Unset All Time References Ctrl+Alt+T
Next Time Reference Ctrl+Alt+N
Previous Time Reference Ctrl+Alt+B
Time Shift... Ctrl+Shift+T
Packet Comments
Delete All Packet Comments
Inject TLS Secrets
Discard All Secrets
Configuration Profiles... Ctrl+Shift+A
Preferences... Ctrl+Shift+P

b) Select the **Protocols** and choose **TLS**



Protocols

■ Display hidden protocol items

■ Display byte fields with a space character between bytes

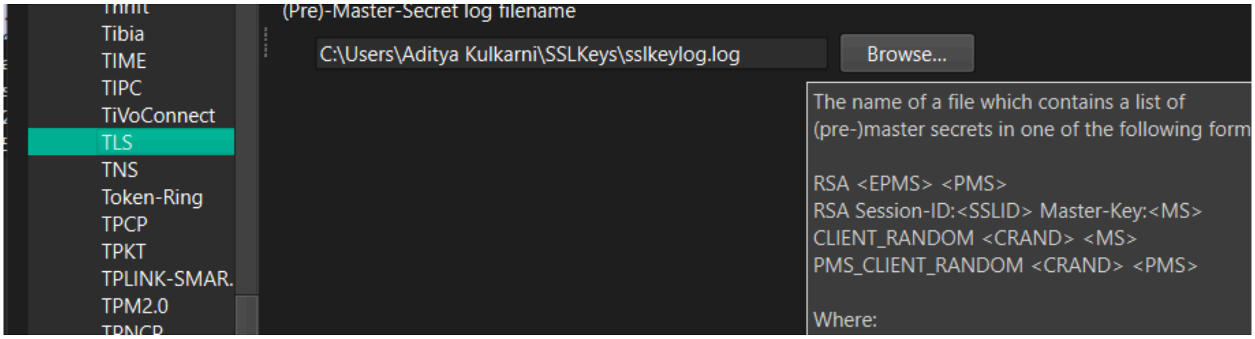
■ Look for incomplete dissectors

■ Enable stricter conversation tracking heuristics

■ Ignore duplicate frames

Deinterlacing conversations key NONE

The max number of hashes to keep in memory for determining duplicates frames 10000



(Pre)-Master-Secret log filename

C:\Users\Aditya Kulkarni\SSLKeys\sslkeylog.log

The name of a file which contains a list of
(pre-)master secrets in one of the following form

RSA <EPMS> <PMS>
RSA Session-ID:<SSLID> Master-Key:<MS>
CLIENT_RANDOM <CRAND> <MS>
PMS_CLIENT_RANDOM <CRAND> <PMS>

Where:

c) In the (Pre)-Master-Secret log filename choose the **sslkeylog.log** file, select **Apply** and **OK**.

8. Now all the packets that are encrypted are decrypted for the entire trace.

Ubuntu

1. Open the terminal enter the following commands and keep this terminal running:
   ```
   export SSLKEYLOGFILE=$HOME/sslkeylog.log
   firefox
   ```

2. Open another terminal and type the following command:
   ```
   resolvectl flush-caches
   wireshark
   ```

3. Start the Wireshark and enter a domain say, iitdh.ac.in in the browser to capture the packets

4. Stop Wireshark once the webpage loads completely, and then follow steps 7 and 8, similar to those for Windows. [**NOTE**: Load the file `sslkeylog.log` from the `/home/USER/` directory]