

SAT1: 005: Customizing the Wireshark Interface

Overview

Wireshark is a great tool for analyzing network traffic. However, the out of the box configuration may not be optimal for an analyst. In this lab, we will look at how to better configure the interface for optimal performance.

Time: 15 Minutes

Learning Objectives

Upon completion of this lab, you should be able to:

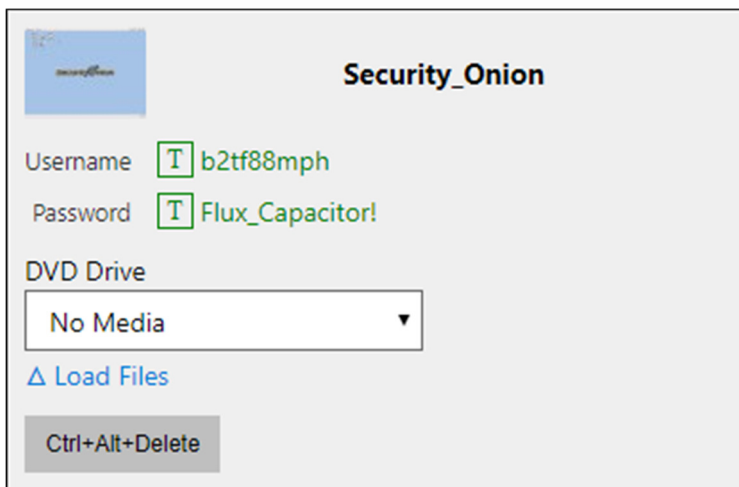
Resources

The following documents have been provided to assist you in this lab.

[Wireshark Cheat Sheet](#)

Log in to the Lab Machine

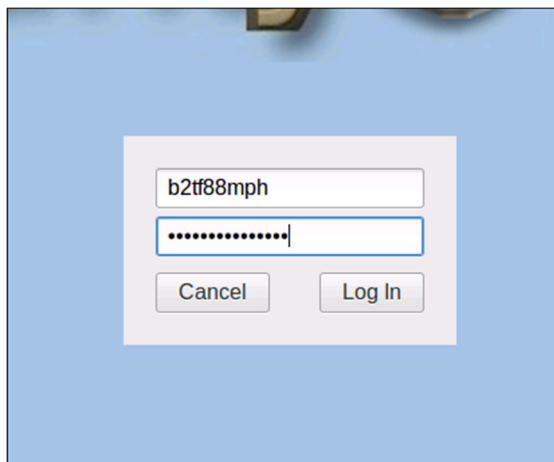
Select the **Security_Onion** machine on the Machines Tab.



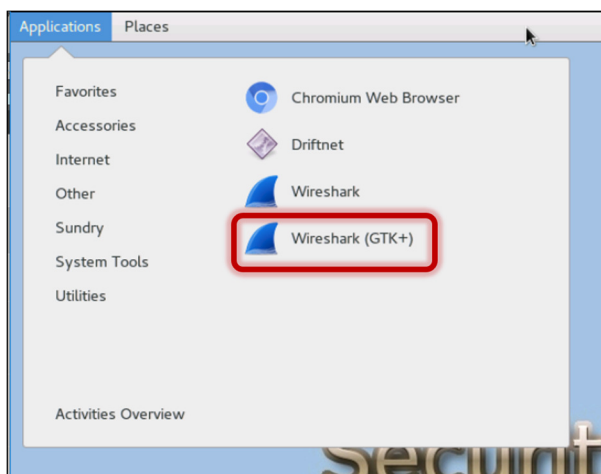
The screenshot shows a login interface for a machine named "Security_Onion". It includes a Microsoft logo, a Username field with the value "b2tf88mph", a Password field with the value "Flux_Capacitor!", a DVD Drive dropdown menu currently set to "No Media", a "Load Files" link, and a "Ctrl+Alt+Delete" button.



Enter the Username and Password on the **Security_Onion** machine, and click Log In.



First you will need to open the Wireshark application. In **Security_Onion**, Wireshark can be found by clicking on **Applications**, then move your mouse over **Internet**, then click on **Wireshark (GTK+)**.



NOTE: While the suggestions in this lab are intended to use Wireshark efficiently and effectively, they are by no means required. You will learn to adapt and use the interface the way that is best for you.

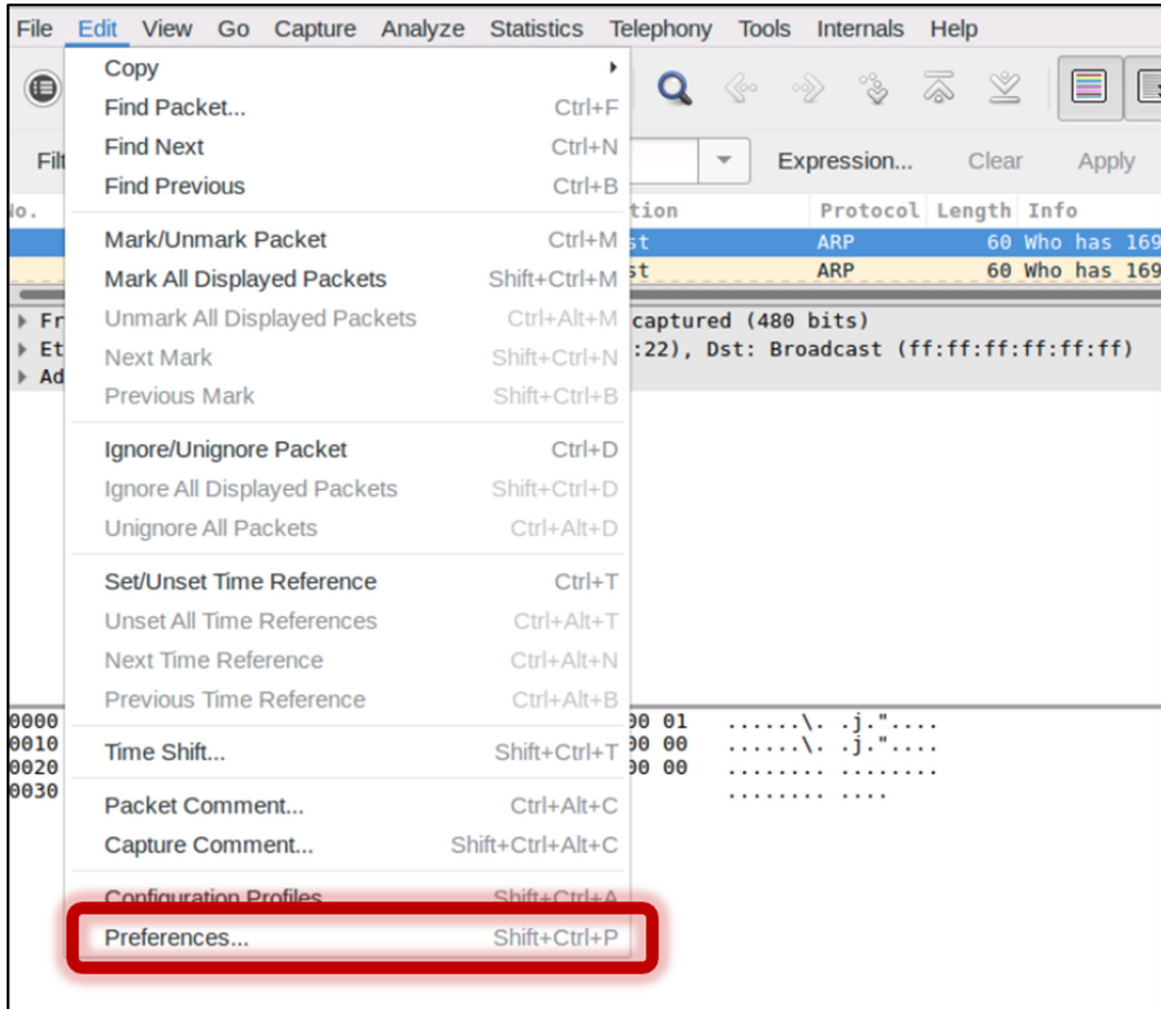
1.0 Configuring Wireshark Columns

Below is the default configuration for the Wireshark columns

30	10.15.102.1	105.108.131.81	105.108.131.522	IBV12	05 name dnelY IB 12A1Vb<00>
32	10.218088	105.108.131.81	554.0.0.525	17W1B	00 2fauqalq dnelY 0x2qdt A 129fab
34	10.11.1180	105.108.131.81	105.108.131.522	IBV12	110 BedJ2f1a1t10N IB BAK10-PC<00>
No.	Time	Source	Destination	Protocol	Length Info

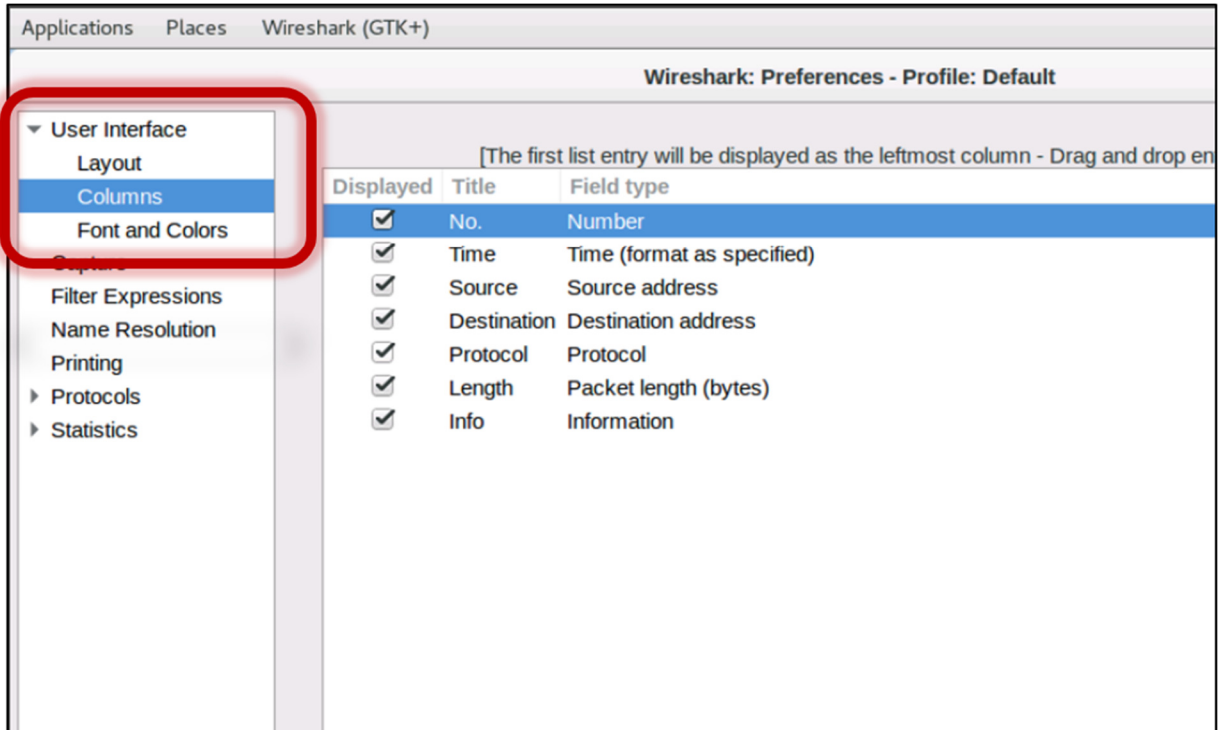


1.1 To change the column settings, click on **Edit** and click on **Preferences**.

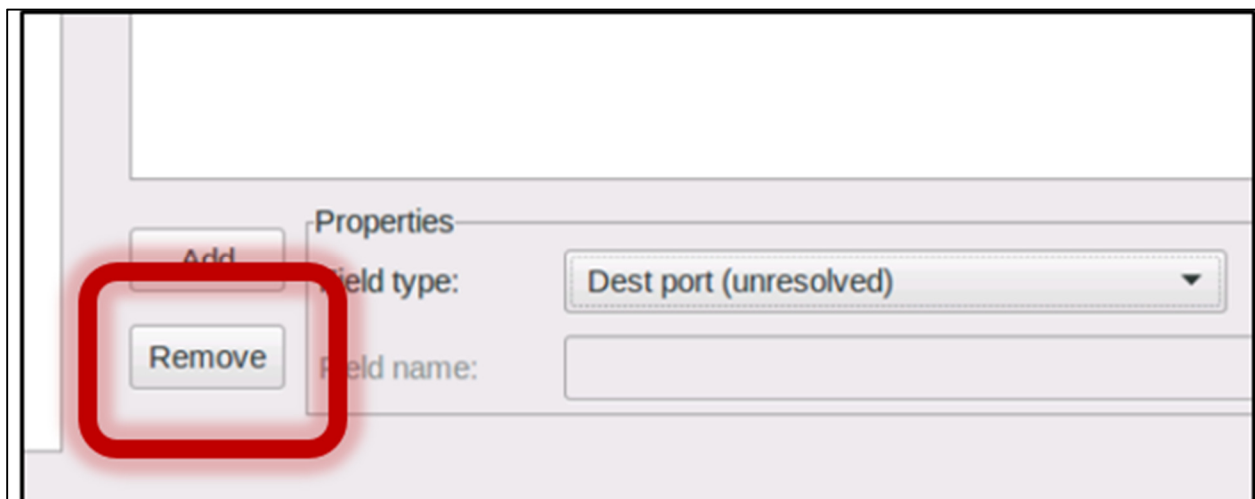




1.2 From the Preferences menu, select **Columns**.

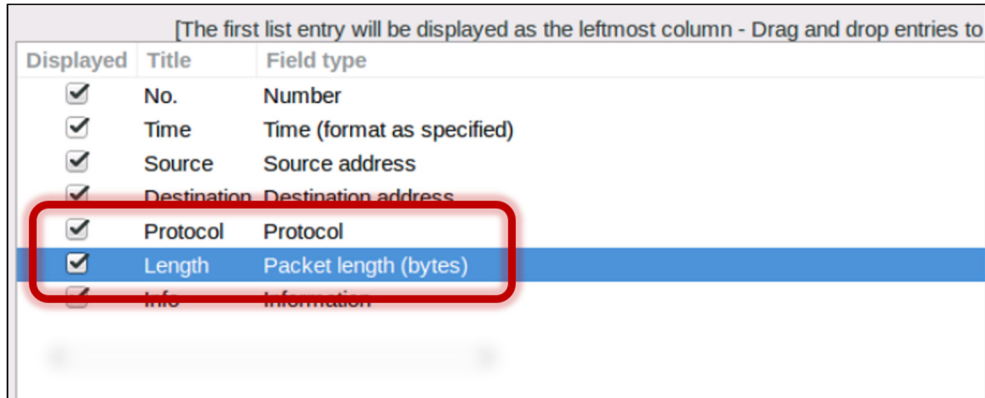


1.3 In order to remove a column, select the column you wish to remove, and select **Remove**.

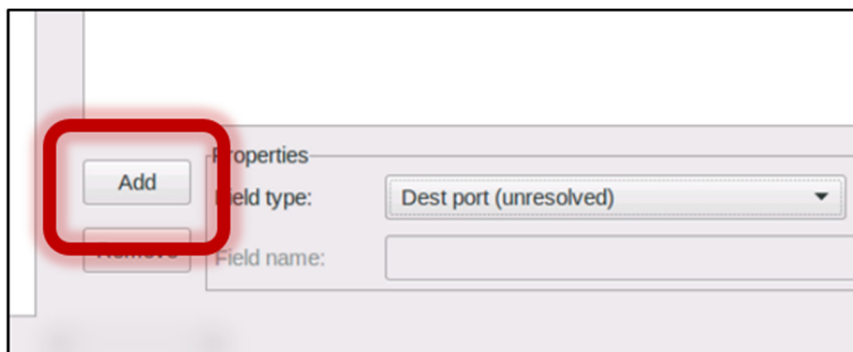




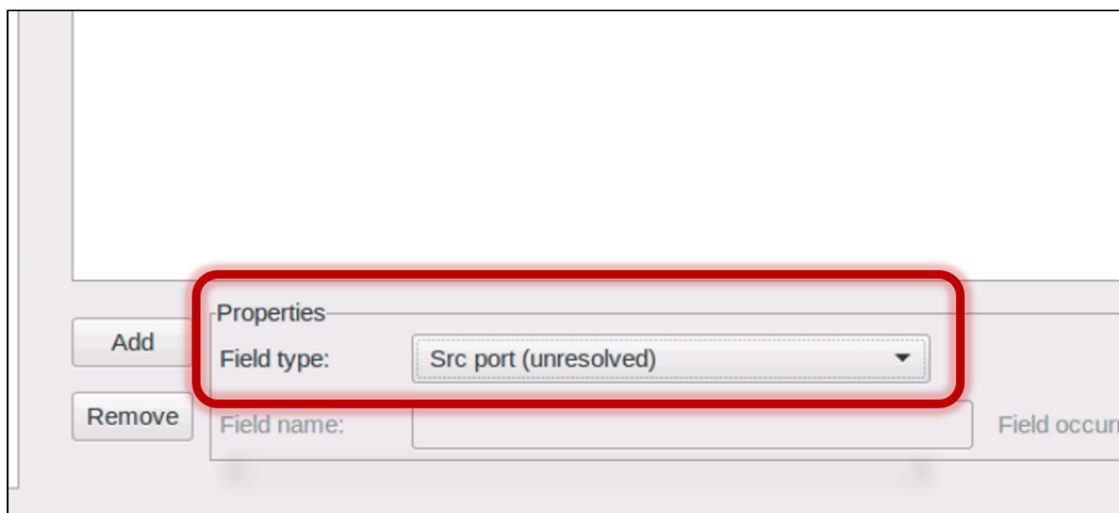
1.4 Remove the **Protocol** and **Length** columns.



1.5 In order to add a new column, select **Add**.



1.6 Double-click the **field type** and from the drop down menu select **Src port (unresolved)** so you can see the port number. Double-click the **"New Column"** title field and replace the name with Src Port.





1.7 Left click and drag the column under **Source Address**.

[The first list entry will be displayed as the leftmost column]

Displayed	Title	Field type
<input checked="" type="checkbox"/>	No.	Number
<input checked="" type="checkbox"/>	Time	Time (format as specified)
<input checked="" type="checkbox"/>	Source	Source address
<input checked="" type="checkbox"/>	Src Port	Src port (unresolved)
<input checked="" type="checkbox"/>	Destination	Destination address
<input checked="" type="checkbox"/>	Info	Information

1.8 Repeat this process and create a new columns for **Dest port (unresolved)**, and label it **Dst Port**.

Properties

Add

Remove

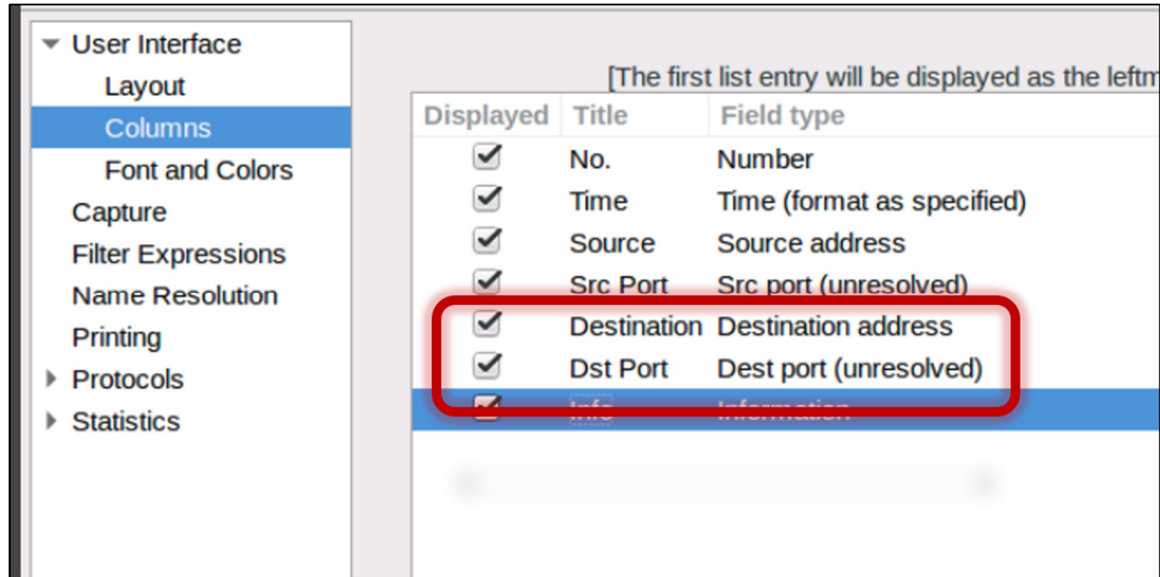
Field type: Dest port (unresolved) ▼

Field name:

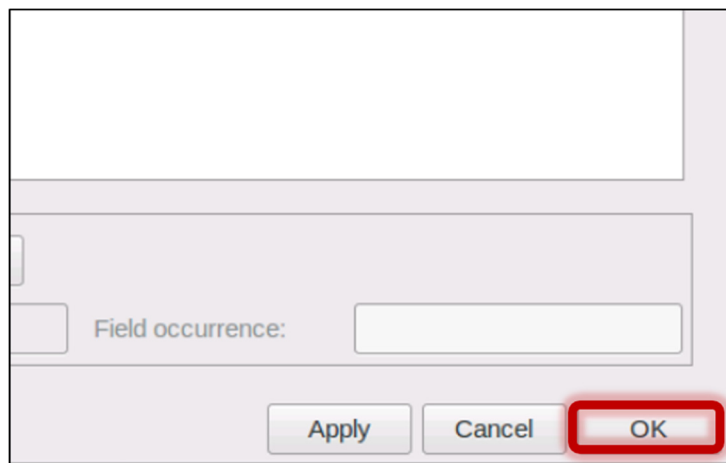
Field c



1.9 Move that column under the column labeled **Destination**.



1.10 Click **OK**.



2.0 Changing the Time Settings

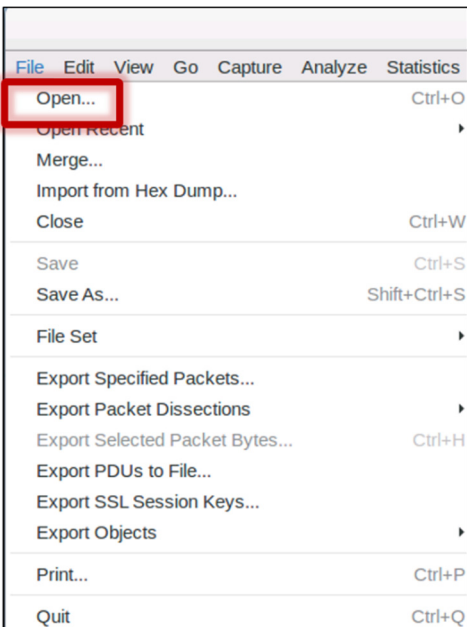
2.1 To change the Time Settings, go to **View > Time Display Format > Date and Time of Day**.

2.2 To change the precision of the displayed time, go to **View > Time Display Format** and select **Seconds**.



3.0 Web Traffic Analysis

3.1 On the Main Menu, click on **File** and click on **Open**.

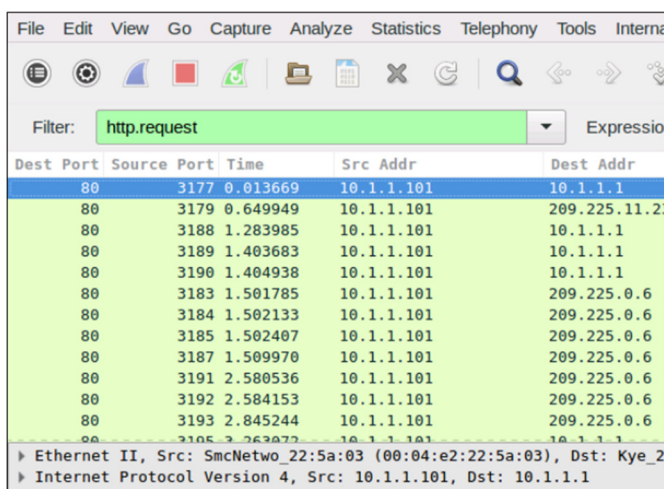


3.2 Click on **b2tf88mph**, then navigate to the **Desktop** folder followed by the **Captures** folder.

3.3 Open `2015-02-15-traffic-analysis-exercise.pcap`.

We are going to filter using the `http.request` filter.

3.4 Type `http.request` in the filter.





3.5 In the packet frame, expand the **Hypertext Transfer Protocol**.

3.6 Right-click the line that say **Host:** then click **Apply as Column**.

4.0 General Formatting

4.1 To change the column alignment, right click the column and select the proper alignment.

4.2 The src port and dst port should be aligned to the left for optimal viewing.

Great job, you have completed LAB005!

Thank You, you may now close this module.