Prerequisites

• Set up XMing X Server: <u>http://sourceforge.net/projects/xming</u>

Step 1:

Log in to your AWS instance. Using nano or vi, edit /etc/ssh/ssh_config. Uncomment ForwardX11 and save the file.

```
wbuntu@ip-172-31-13-42:~ - - ×
This is the set offer system-wide configuration file. See
set configuration data is parsed as follows:
i users, and the values can be changed in per-user configuration files
f or on the command line.
i Configuration data is parsed as follows:
i . command line options
i . user-specific file
i . system-wide file
i . system-wide file
i . any configuration value is only changed the first time it is set.
i Thus, hest-specific defaults for some commonly used options. For a comprehensive
i list of available options, their meanings and defaults, pleate see the
set configuration no
ForwardX11 no
i . ForwardExAuthentioning
i . BarterBibMuthentioning
i . BarterBi
```

Step 2:

Reboot your instance (sudo reboot now)

Step 3:

Make sure XMing is running. Open PuTTY and set it up as before (using your IP and key file.). This time, also enable X11 Forwarding in Connection > SSH > X11.

PuTTY Configuratio	on	?	×	
ategory:				
Bell	^	Options controlling SSH X11 forwarding		
Features		X11 forwarding		
Appearance		Enable X11 forwarding		
Behaviour		X display location		
Translation Selection Colours		Remote X11 authentication protocol MIT-Magic-Cookie-1 XDM-Authorization-1 X authority file for local display		
Connection		Brows	e	
Data				
Proxy				
Blogin				
SSH				
Kex				
Cipher				
🕂 ·· Auth				
TTY				
-X11				
Tunnels				
Bugs				
- More bugs	¥			
About	Help	Open Cano	cel	

To make this easier to do later, you should save a profile. Go back to the first tab, type a name, and select Save. You can click this when you need to use it in the future and select Load to restore the configuration.

ategory:				
Session Logging Logging Terminal Keyboard Bel Features Window Appearance Behaviour Translation	^	Basic options for your PuTTY session		
		Specify the destination you want to conn Host Name (or IP address)	ect to Port	
		Connection type: Raw Telnet Rlogin SS	H O Serial	
		Load, save or delete a stored session Saved Sessions		
Selection	Selection Colours Connection Data	mininet		
Colours		Default Settings mininet	Load	
Data			Save	
Proxy Telnet Rlogin ⊡- SSH Kex Cipher Auth TTY V			Delete	
	~	Close window on exit: Always Never Only on clean exit		
About	Help	Open	Cancel	

Step 4:

Install wireshark

sudo apt-get update sudo apt-get install wireshark

Step 5:

Set up OpenFlow plugin

Run commands:

sudo apt-get install libgtk2.0-dev cd ~/openflow/utilities/wireshark_dissectors

Edit file: packet-openflow.c

Change line 769 from:

dissector_add(TCP_PORT_FILTER, global_openflow_proto, openflow_handle);

to

dissector_add_uint(TCP_PORT_FILTER, global_openflow_proto, openflow_handle);

Run command:

make

sudo cp packet-openflow.so /usr/lib/wireshark/libwireshark1/plugins/

Conclusion:

At this point, you should be all set. To do labs, open up two SSH sessions. In one, you can run Wireshark (sudo wireshark), and in the other you can do the modifications/run Mininet.