

Display WireShark Using Cygwin

Goal: We will display the WireShark application on Windows using Cygwin when we press Sniff Packets which actually runs WireShark on the Linux LANforge machine.

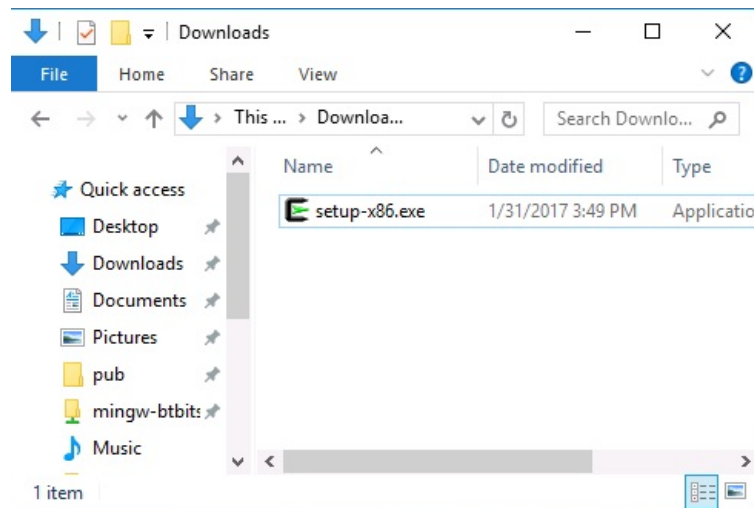
The native display protocol for Linux (and Unix) is the X Display Protocol. The Cygwin.org project provides Linux software that runs natively on Windows. You can run an X display server on Windows that accepts connection from LANforge. We will walk through setting up Cygwin and configuring an X display.



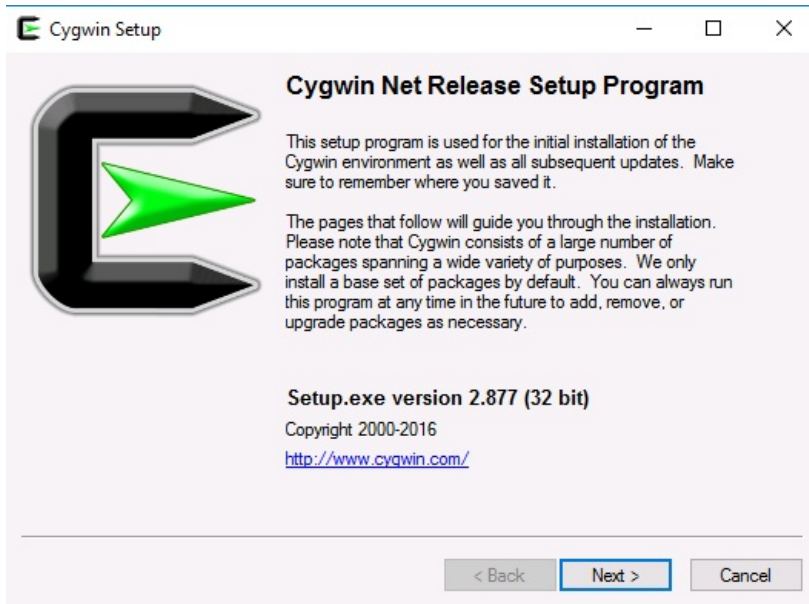
-
1. Installing Cygwin and the X display components
 2. We will start at Cygwin.org and download the Cygwin installer.



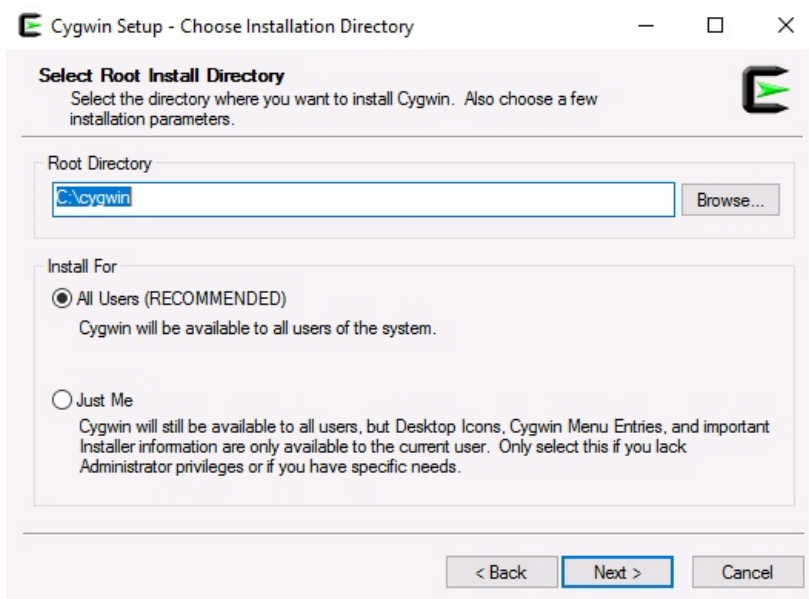
- Download `setup-x86.exe` or `setup-x86_64.exe` as appropriate. Go to your Downloads folder and double start the program.



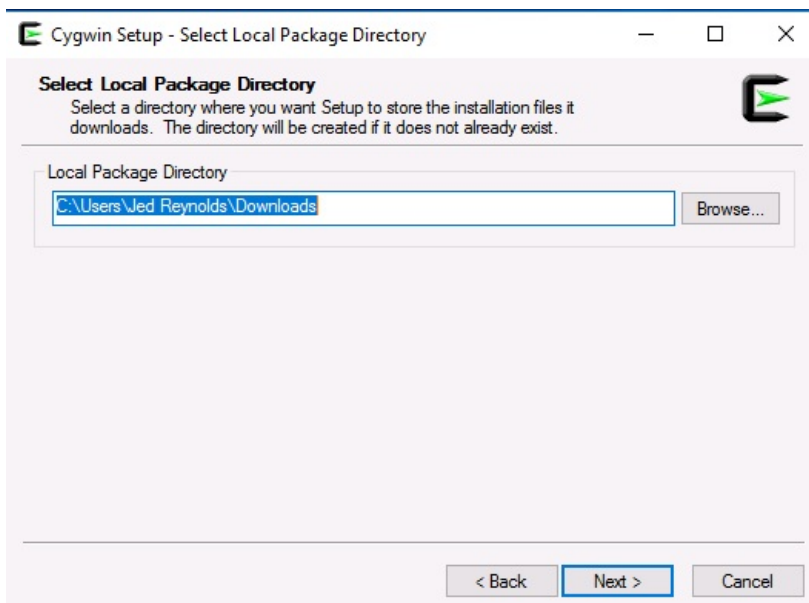
- Next



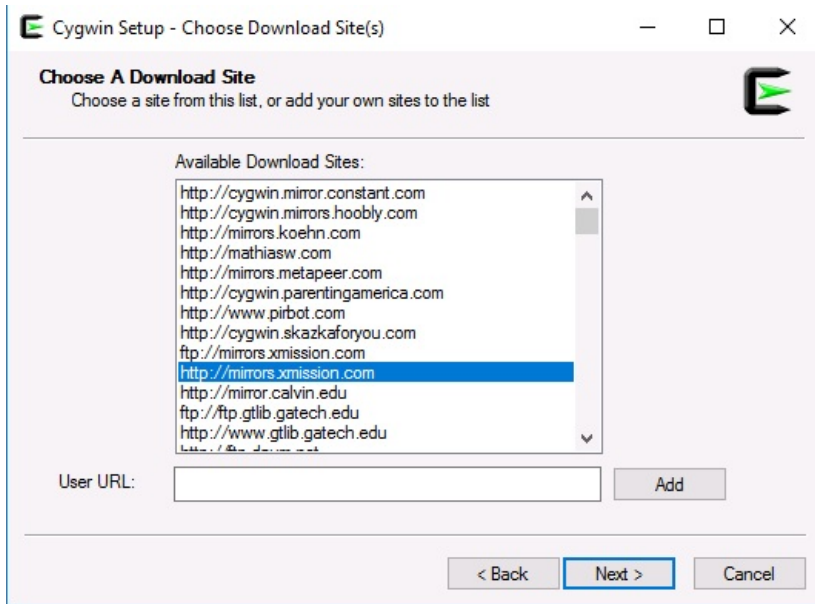
5. Next



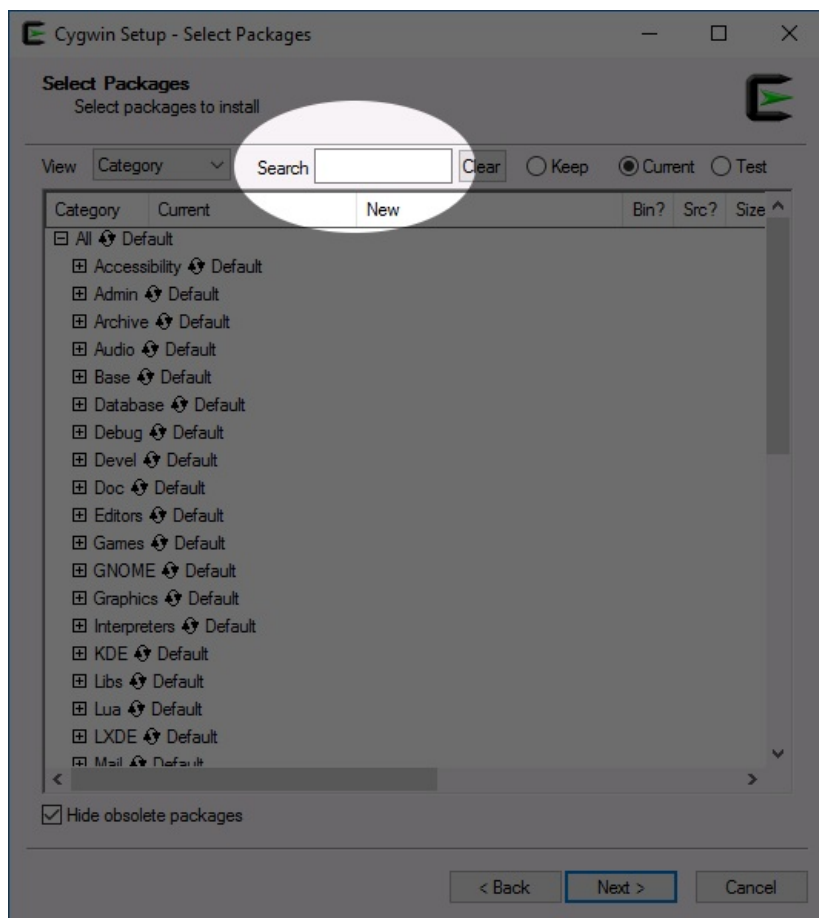
6. Next



7. Choose a mirror that might be close to you, click Next

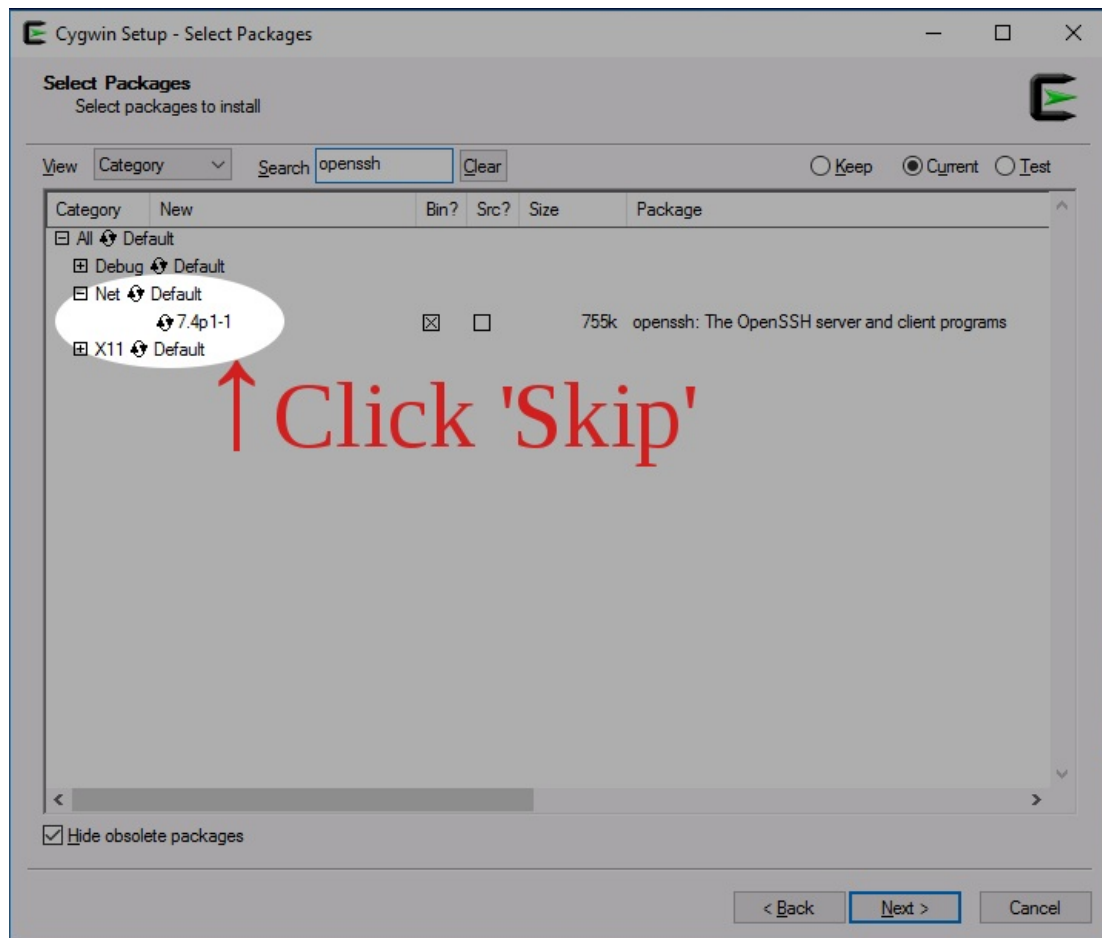


8. Now you see a the software selection screen, sorted by category. Some of these entries appear two or more times, because they belong to multiple categories. Try using the search box in upper middle above the software list to search for the packages listed below.

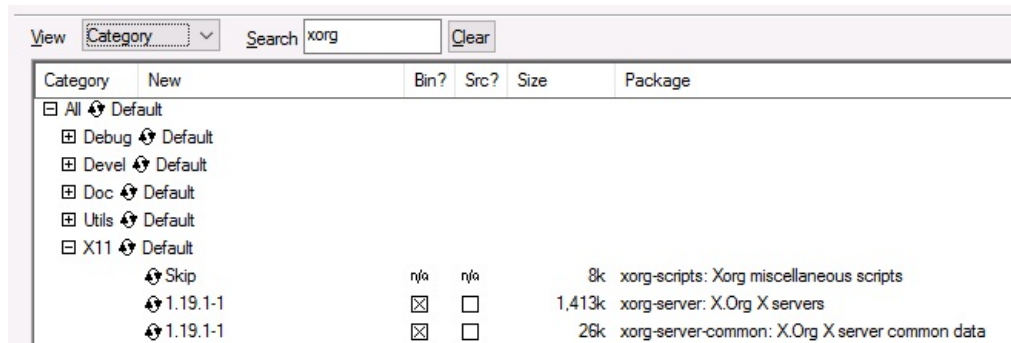


9. The items you want to search for are
- o openssl
 - o xorg-server
 - o xinit
 - o rxvt
 - o xlaunch

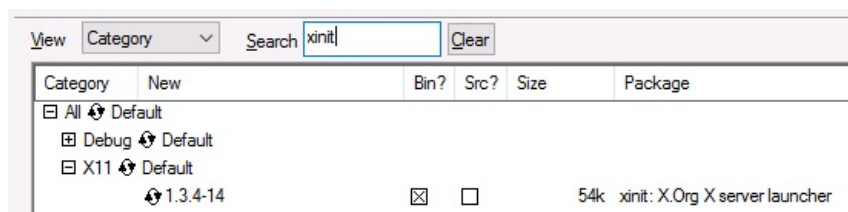
A. Search for `openssh` and click the Skip property once to change it to the most recent version to set it to install.



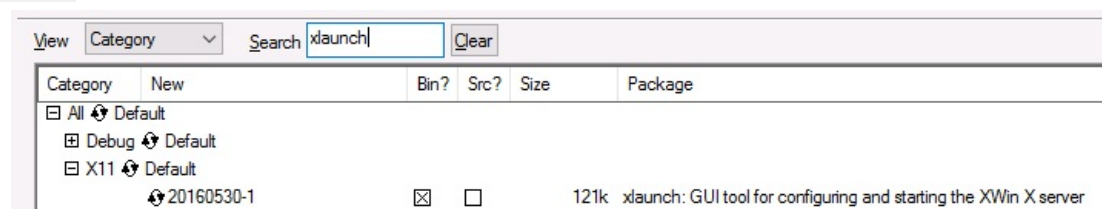
B. `xorg-server` provides the X display system



C. `xinit` helps the X system launch



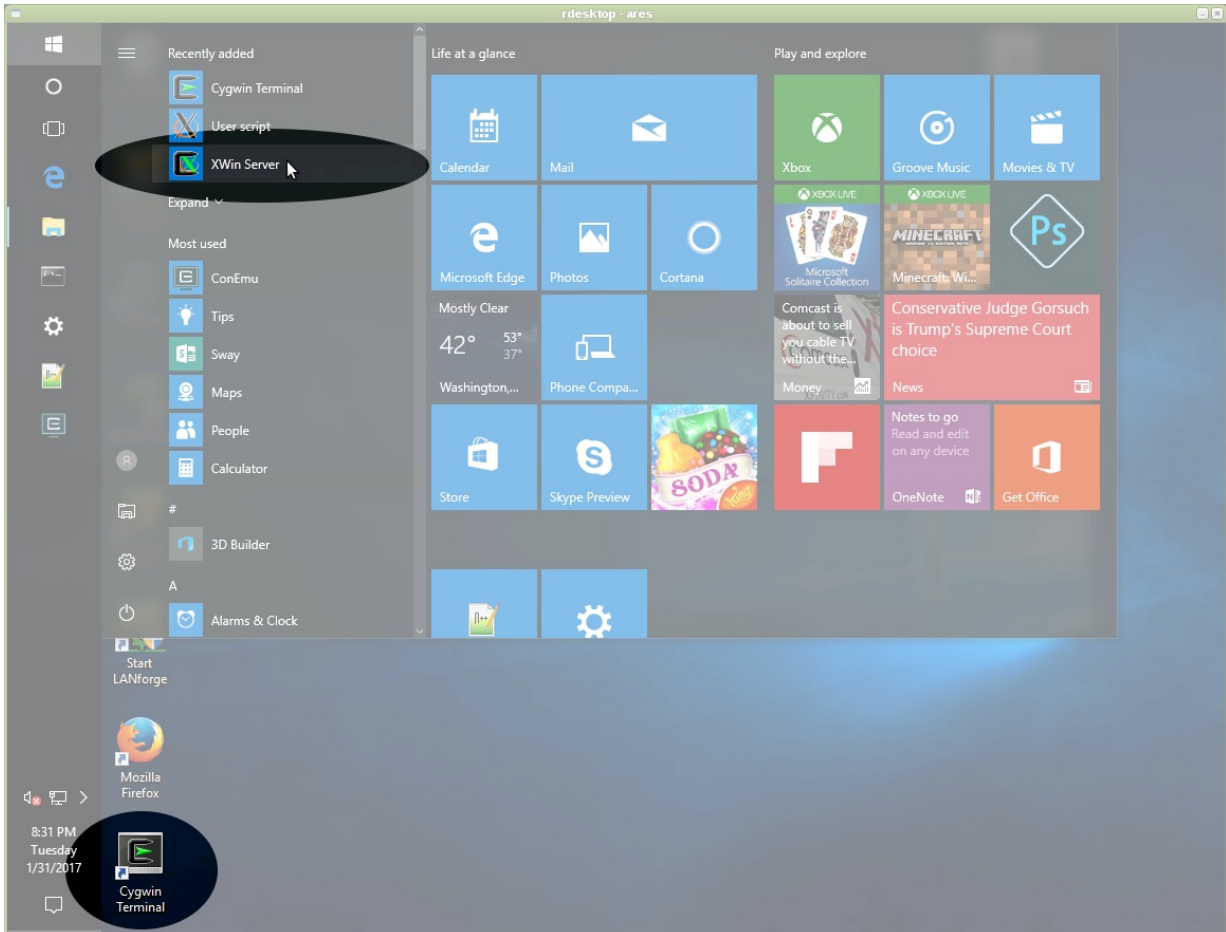
D. `xTlaunch` is what you will drag to your task bar to launch your Cygwin X server



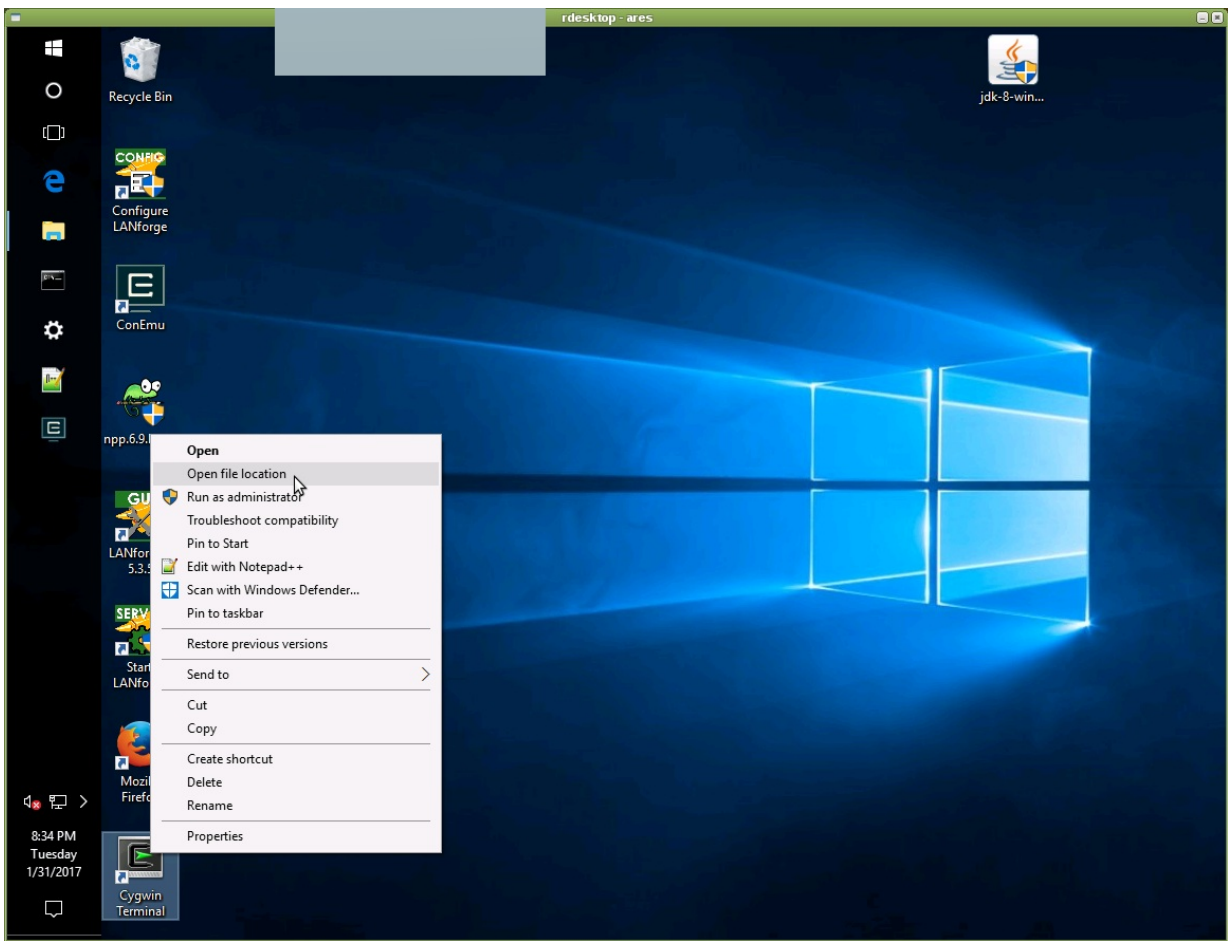
E. `rxvt` and `rxvt-unicode` are more useful terminals than the `minterm` program that Cygwin provides by default.

View	Category	Search	Bin?	Src?	Size	Package
	All	rxvt				
	Default					
	Debug					
	Shells					
		2.7.10-1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	125k	rxvt: Lightweight VT102 terminal emulator
		9.22-1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	690k	rxvt-unicode: An improved version of rxvt with Unicode support

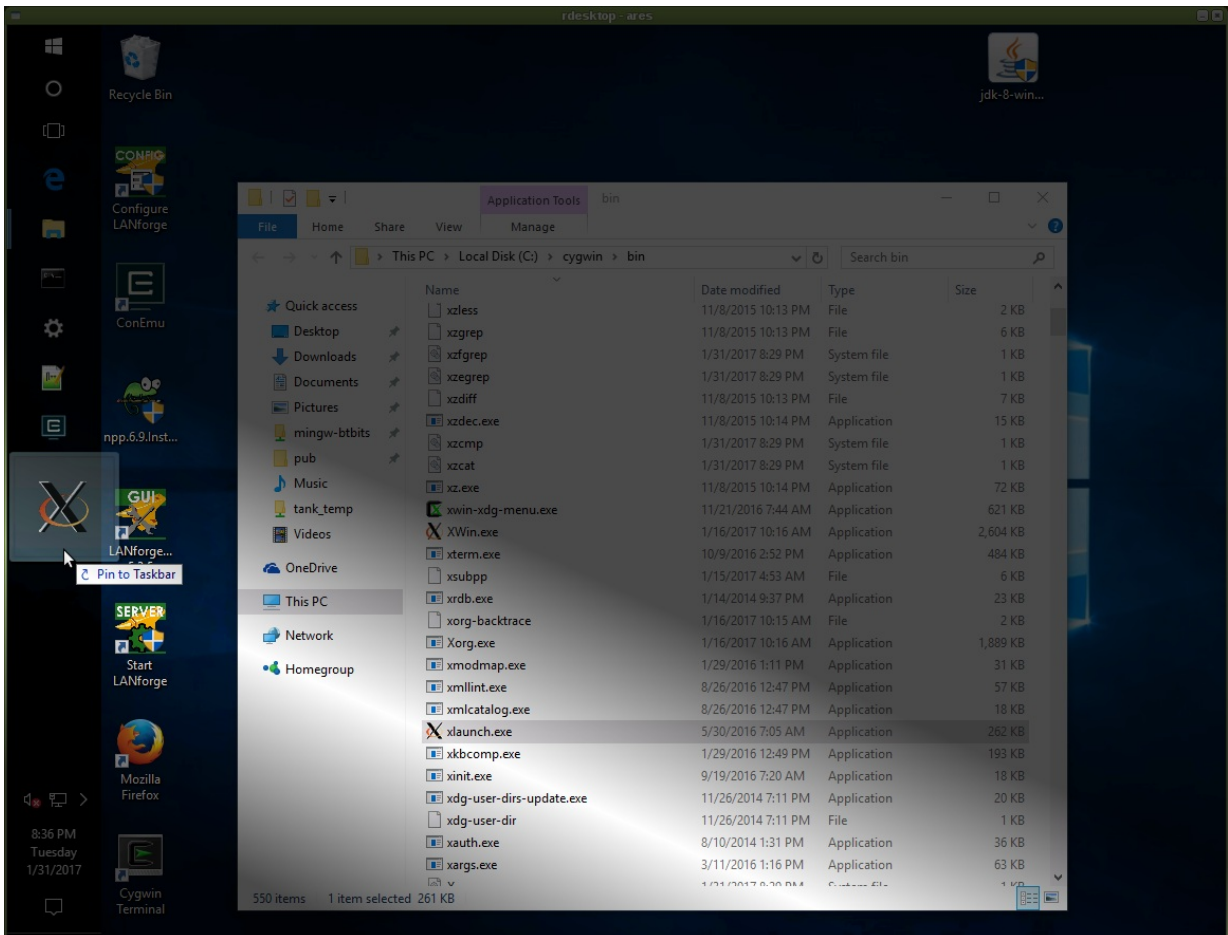
10. Click Next and let the installer finish the installation of the Cygwin packages. You will see a Cygwin Terminal icon appear on your desktop and new Cygwin icons in your Start menu.



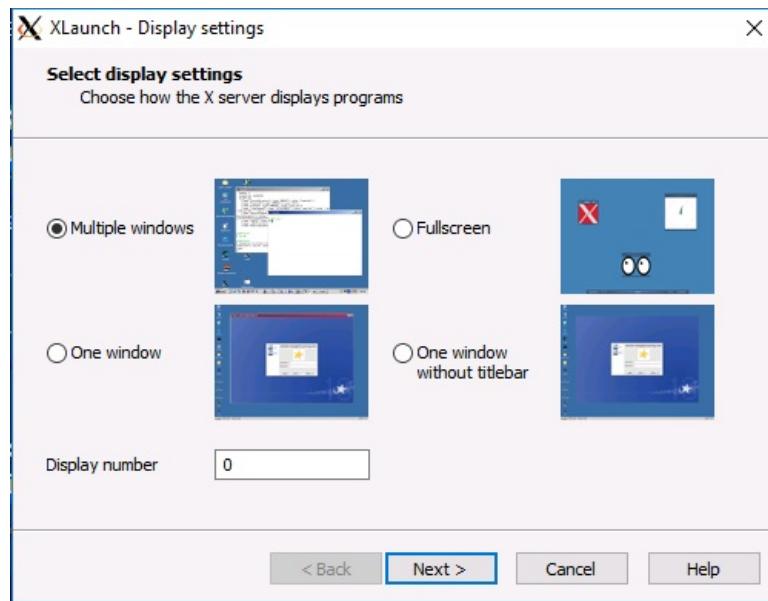
11. Next we will **right-click** on the Cygwin Terminal icon and select Open File Location



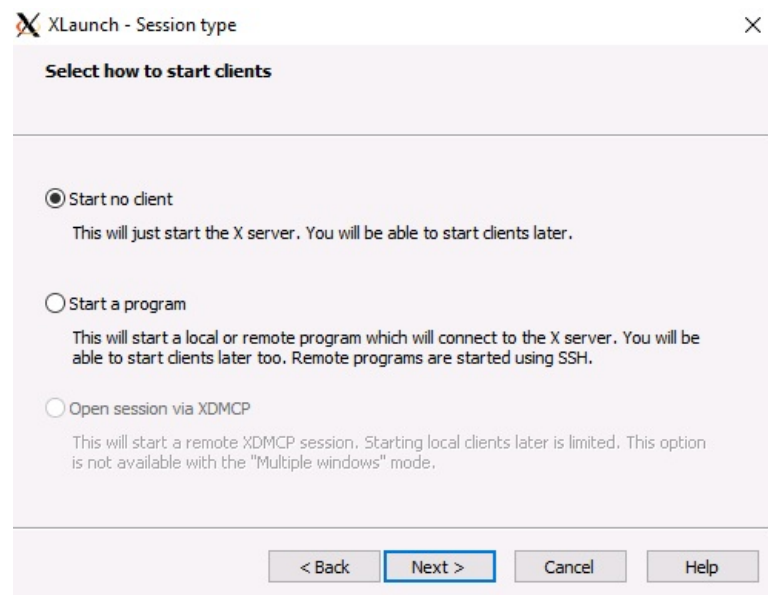
12. In the Explorer window, scroll to find `x1launch.exe`, and drag it to the Task Bar



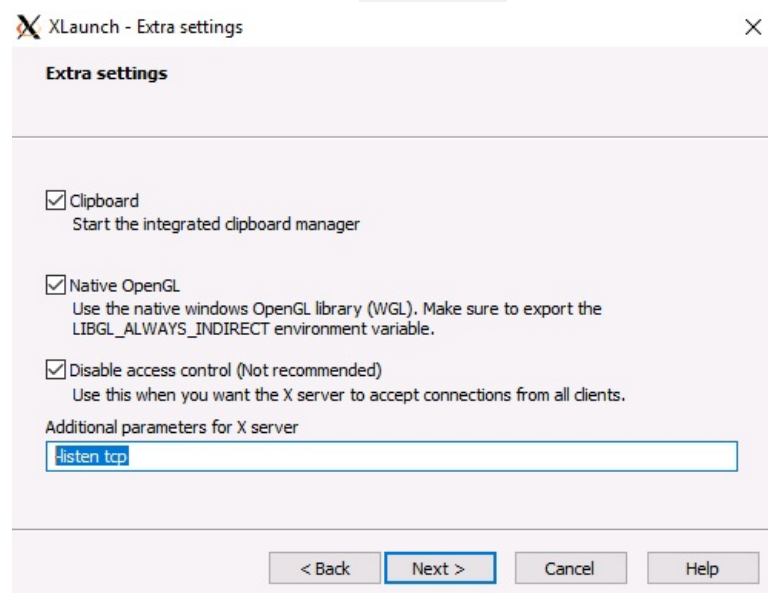
13. Click the `x1launch` icon on the task bar, and click Next



14. Next



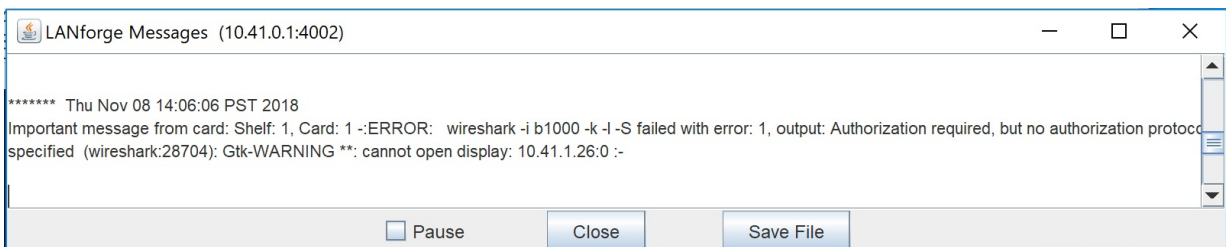
15. Check Disable Access Control and add the option: `-listen tcp`. Click Next



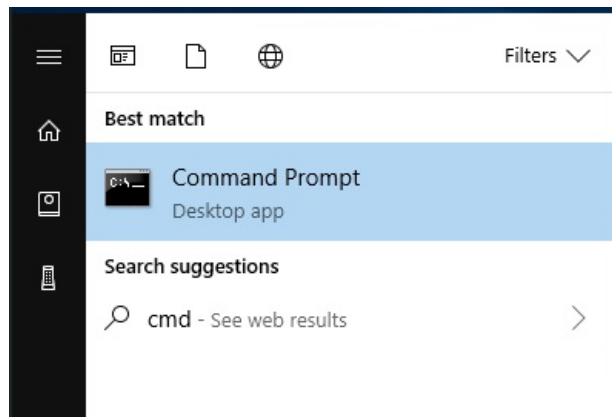
16. Firewall, Click Allow Access



17. If the LANforge Messages window reports 'No Access', you might need to use `xhost.exe` to grant X11 access.



A. Open a CMD window

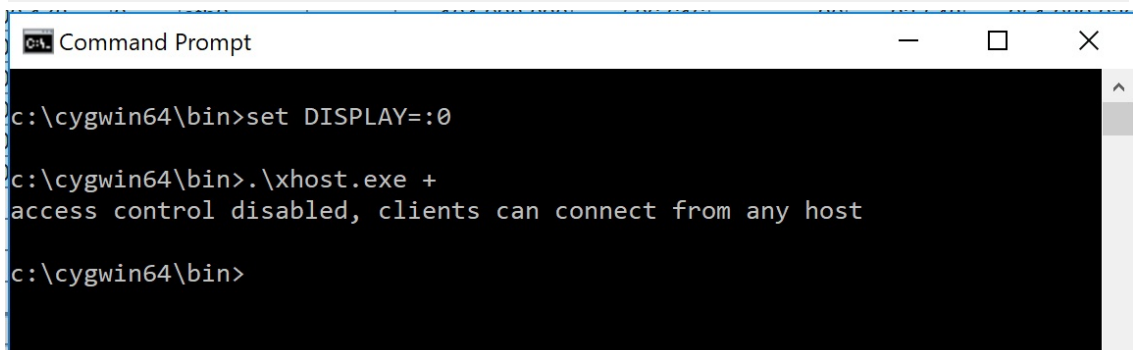


B. Go to the `cygwin\bin` folder:

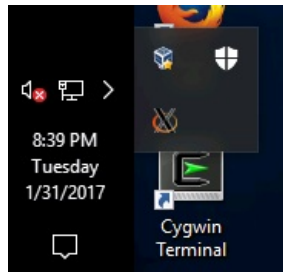
```
C:\> cd \cygwin\bin
```

C. Use `xhost.exe` to open permissions:

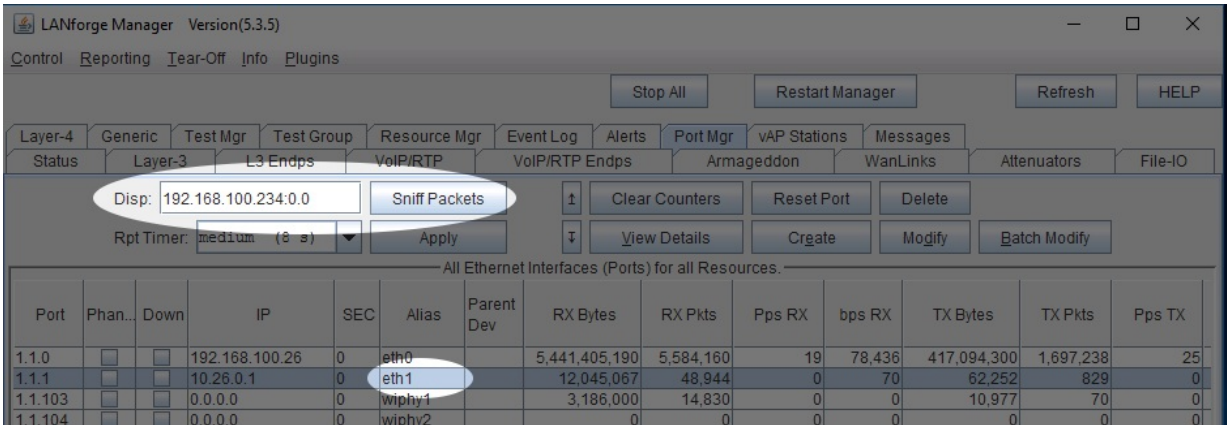
```
C:\> .\xhost.exe +
```



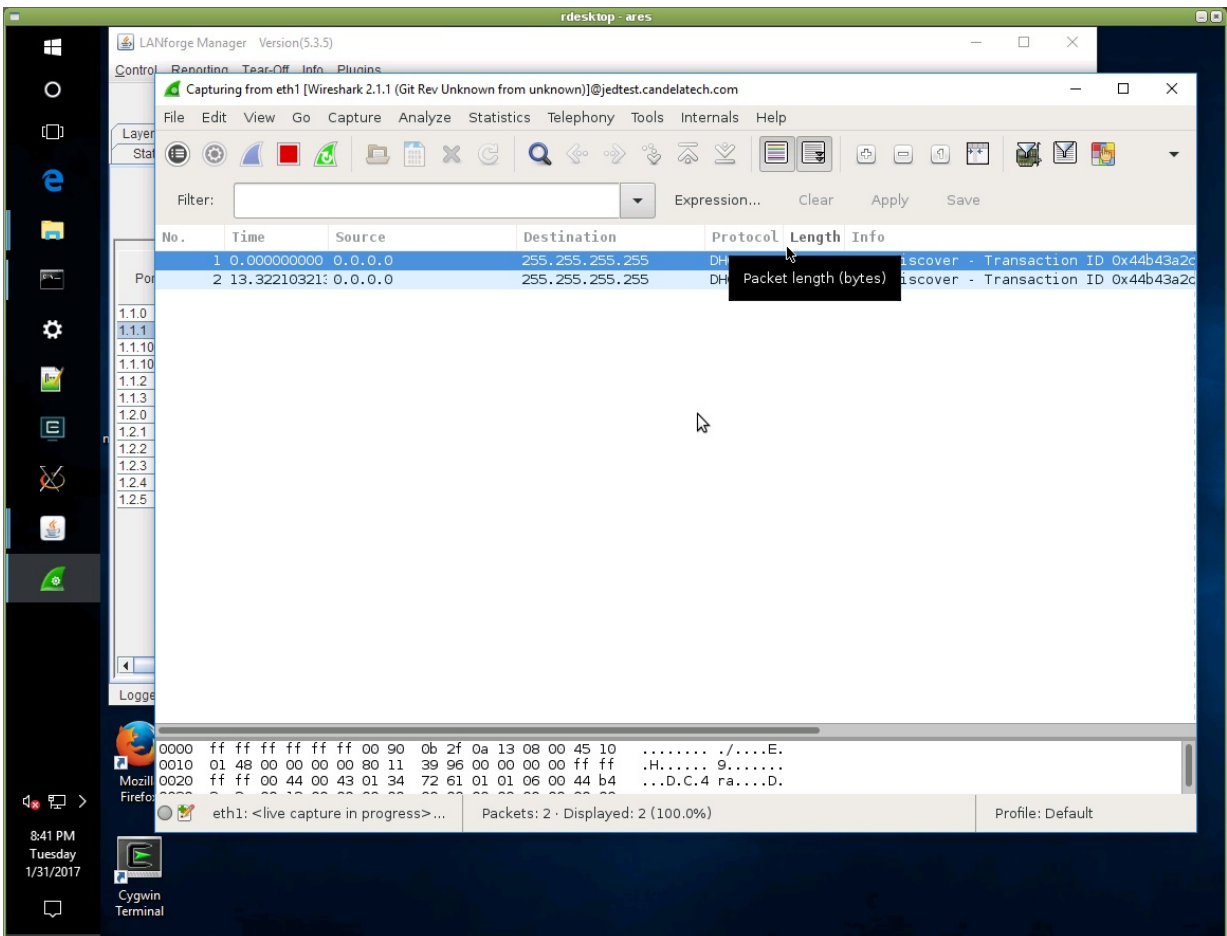
18. Now your X display service is running. You can check that it's running by clicking into the System Tray and seeing if the icon is there.



19. Launch the LANforge GUI from your desktop. Select a port from the Port Mgr tab. Notice how the **Disp** field has your laptop's LAN address. This is the display address the remote machine will display the Wireshark window to.



20. You will see WireShark



21. Resources and other Documentation:

- A. <http://unix.stackexchange.com/questions/227889/cygwin-on-windows-cant-open-display>
- B. https://www.cs.virginia.edu/~csadmin/wiki/index.php/Using_Cygwin_for_X11_Forwarding

C. <http://www.arisc.edu/arisc/knowledge-base/ssh-and-x11-forwarding-us/index.xml>

Candela Technologies, Inc., 2417 Main Street, Suite 201, Ferndale, WA 98248, USA
www.candelatech.com | sales@candelatech.com | +1.360.380.1618