

Investigating the Windows Subsystem for Linux (WSL)

CompTIA.

OOWJ
March 28, 2019

WHO WE ARE

CompTIA is a global, not-for-profit IT trade association and the voice of the industry

OUR MISSION

Advance the IT industry

Technology is infrastructure, just like roads and bridges. Our economic growth, national security and quality of life depend on it. When we help tech businesses grow and help build a skilled tech workforce, we make that infrastructure stronger.

WHO WE SERVE

Tech businesses, tech professionals, tech educators, and anyone interested in a tech career or a vibrant tech industry.

HOW WE DO IT



NETWORKING

Member-led communities, councils, and events that help thousands of tech executives and professionals learn and collaborate with peers.



EDUCATION

Vendor-neutral education, business standards, technical content and career advice to help drive business revenue and professional growth.



THOUGHT LEADERSHIP

Highly regarded research and subject-matter expertise on topics including technology trends, cybersecurity and workforce issues.



CERTIFICATION

Vendor-neutral certifications that help millions of IT pros around the world validate their skills and advance in their careers.



ADVOCACY

Advocacy at state, federal, and international levels for policies that build a skilled tech workforce and advance the digital economy.



PHILANTHROPY

Help for those who are under-represented in IT and those who lack economic opportunity to prepare for, secure and succeed in IT careers.

Your Presenter . . .



James Stanger, PhD

Chief Technology Evangelist - CompTIA

A+, Network+, Security+, MCSE, LPI LPIC 1, Symantec STA

Works with IT pros, managers and executives worldwide

- *Security analytics*
- *Penetration testing*
- *Risk assessment*
- *Intrusion detection*
- *Linux and open source*
- *Network administration*
- *Virtualization*
- *Web technologies*
- *Certification development*
- *Award-winning author and instructor*

Twitter: @jamesstanger

CompTIA hub: <https://tinyurl.com/y94u3v7j>

Agenda

- What is the WSL?
- What it isn't
- Who uses it, and why?
- Installing it
- Tech support and the WSL
- WSL and security



Join Dr. James Stanger for his March Office Hours with James as he investigates ways that Windows and Linux do more than simply co-exist in today's cloud and IoT-aware IT environment. He'll show you how to install, use, and support the Windows Subsystem for Linux. By the end of the Webinar, you'll not only know how to use it, but also why it's so important from an IT support and security perspective.

Introducing the Windows Subsystem for Linux (WSL)

What is it?

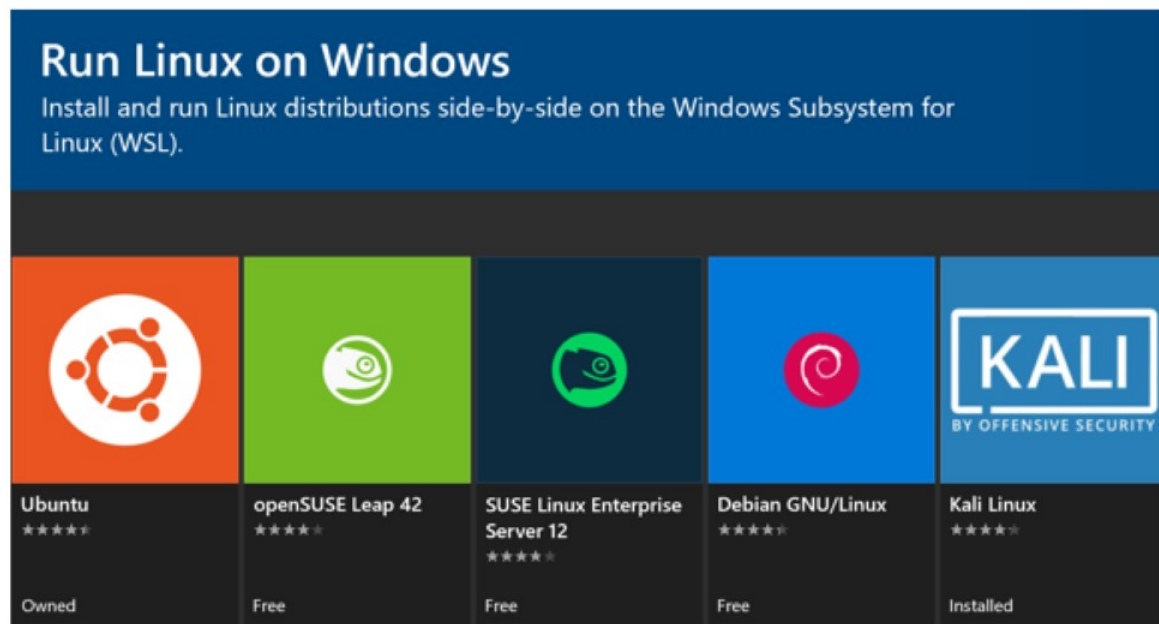
- A compatibility layer in Windows
 - A set of libraries and apps
 - Translates a Linux system call into something the Windows kernel understands
 - Runs a Linux environment from within Windows
 - Sessions are recognized by Windows
- Allows you to open a Windows console running the Bash shell

```
PS C:\Users\propeople> get-childitem HKCU:\Software\Microsoft\Windows\CurrentVersion\ShellData | ForEach-Object {
    (Get-ItemProperty $_.PSPath).BasePath
}
C:\Users\propeople\AppData\Local\State
C:\Users\propeople\AppData\Local\Packages\CanonicalGroupLimited.UbuntuonWindows_PerhapsIndigo\LocalState
C:\Users\propeople\AppData\Local\Packages\46932506_9e965d1eap42_2_82rs5jcyhac\LocalState
C:\Users\propeople\AppData\Local\Packages\46932506_9e965d1eap42_2_82rs5jcyhac\LocalState
PS C:\Users\propeople>
```

```
# using to determine current instance.
> if ! $? { echo "Error: No instance found." } else { echo "Instance found: $BASE_PATH" }
> fi
> done
# You can create and simultaneously run multiple WSL instances, comment
# out the "break", run this script within each one
# single value.
> break
> fi
done
# Run the script within each one and it'll return only
# single value.
> break
> fi
done
# You can create and simultaneously run multiple WSL instances, comment
# out the "break", run this script within each one and it'll return only
# single value.
> break
> fi
done
# Run the script within each one and it'll return only
# single value.
> break
> fi
done
```

What the WSL Isn't

- A graphical interface
- Virtualization
- Dual booting
- A cloud solution
- CygWin
- A full development environment



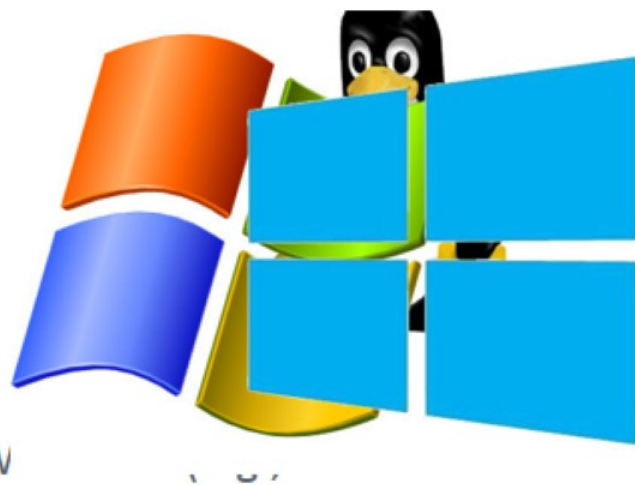
Run Linux on Windows
Install and run Linux distributions side-by-side on the Windows Subsystem for Linux (WSL).

Ubuntu	openSUSE Leap 42	SUSE Linux Enterprise Server 12	Debian GNU/Linux	Kali Linux
★★★★★	★★★★☆	★★★★☆	★★★★☆	★★★★☆
Owned	Free	Free	Free	Installed

Who Uses the WSL, and Why?

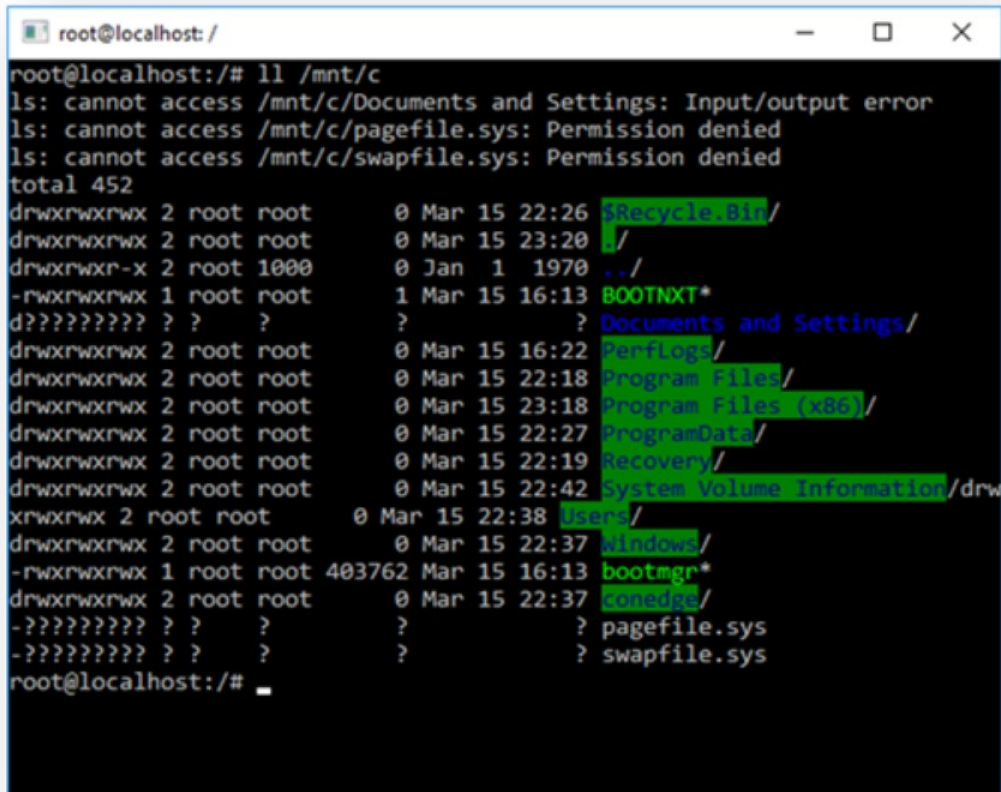
Who Uses it?

- Often used by developers / coders
 - For convenience
 - Can support multiple development environments
 - Use all Linux system resources, right from within V (Ruby, Python, Java, etc.)
 - Gives developers more coding and working options
 - Native development
 - Uploading and code processing options
- A few other uses, outside of development



Why is it Useful?

- Development efficiency
 - You have to develop to a platform
 - Why not the same one as your desktop?
- Software Development Lifecycle (SDLC) efficiency



```
root@localhost: /
root@localhost:/# ll /mnt/c
ls: cannot access /mnt/c/Documents and Settings: Input/output error
ls: cannot access /mnt/c/pagefile.sys: Permission denied
ls: cannot access /mnt/c/swapfile.sys: Permission denied
total 452
drwxrwxrwx 2 root root      0 Mar 15 22:26 $Recycle.Bin/
drwxrwxrwx 2 root root      0 Mar 15 23:20 /
drwxrwxr-x 2 root 1000      0 Jan  1  1970 ../
-rwxrwxrwx 1 root root      1 Mar 15 16:13 BOOTNXT*
d???????? ? ?      ?      ?      ? Documents and Settings/
drwxrwxrwx 2 root root      0 Mar 15 16:22 PerfLogs/
drwxrwxrwx 2 root root      0 Mar 15 22:18 Program Files/
drwxrwxrwx 2 root root      0 Mar 15 23:18 Program Files (x86)/
drwxrwxrwx 2 root root      0 Mar 15 22:27 ProgramData/
drwxrwxrwx 2 root root      0 Mar 15 22:19 Recovery/
drwxrwxrwx 2 root root      0 Mar 15 22:42 System Volume Information/
xrwxrwx 2 root root      0 Mar 15 22:38 Users/
drwxrwxrwx 2 root root      0 Mar 15 22:37 windows/
-rwxrwxrwx 1 root root 403762 Mar 15 16:13 bootmgr*
drwxrwxrwx 2 root root      0 Mar 15 22:37 conedge/
-???????? ? ?      ?      ?      ? pagefile.sys
-???????? ? ?      ?      ?      ? swapfile.sys
root@localhost:/#
```

Installing the WSL

Installation

- Is your system is a candidate?
 - Fall Creator update or later
 - Check your version
- Enable the "Windows Subsystem for Linux" optional feature using PowerShell:

```
PS C:\ Enable-WindowsOptionalFeature -Online  
-FeatureName Microsoft-Windows-Subsystem-  
Linux
```

Settings > System > About

Then, look for the OS Build and System Type fields

Home	Edition	Windows 10 Home
Find a setting	Version	1607
System	OS Build	14393.0
Power & sleep	Product ID	00326-10000-00000-AA728
Storage	Processor	Intel(R) Xeon(R) CPU W3520 @ 2.67GHz 2.67 GHz
Offline maps	Installed RAM	1.00 GB
Tablet mode	System type	64-bit operating system, x64-based processor
Multitasking	Pen and touch	No pen or touch input is available for this display

[Change product key or upgrade your edition of Windows](#)

[Read the Privacy Statement for Windows and Microsoft services](#)

**Or, must be above
version 14393.0**

Installation Details

- Control Panel
- Programs and Features
- Turn features on or off
- Reboot
- Command prompt:
bash
- Go through steps

Consider: Start menu | optionalfeatures

The screenshot shows the Windows Control Panel window titled "Windows Features". The navigation pane on the left includes "Programs" which is selected. The main content area shows "Programs and Features" with a red circle around the link "Turn Windows features on or off". Below this are "Default Programs" and "Java". A separate window in the foreground shows a list of Windows features with checkboxes:

- Windows Process Activation Service
- Windows Projected File System (Beta)
- Windows Subsystem for Linux
- Windows TIFF IFilter
- Work Folders Client

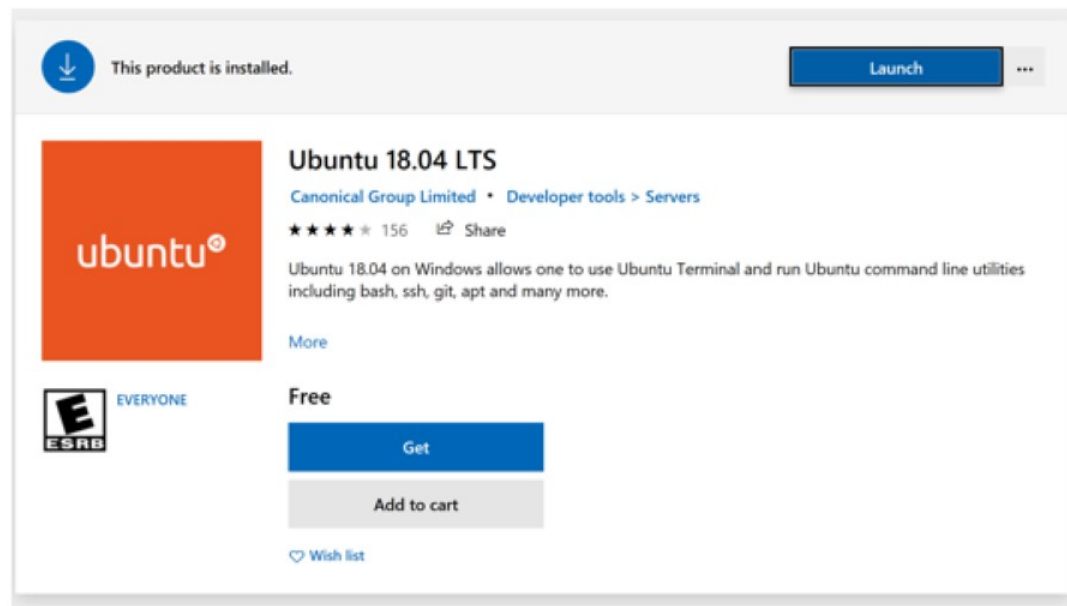
Buttons for "OK" and "Cancel" are visible at the bottom of the foreground window.

Installation (cont'd)

- Install your Linux Distribution
 - Windows store
 - Command line
 - Manually unpack and install (Windows server)
- One-time Initialization
 - Click the “Launch” button in the Windows store app
 - Linux setup begins
 - Create a user in Linux
 - Update the Linux distro’s packages
 - Pin distro to Start menu or taskbar

Ubuntu:

<https://www.microsoft.com/en-us/p/ubuntu-1804-lts/9n9tngvndl3q?activetab=pivot:overviewtab>



This product is installed. Launch

ubuntu

Ubuntu 18.04 LTS
Canonical Group Limited • Developer tools > Servers

★★★★★ 156 [Share](#)

Ubuntu 18.04 on Windows allows one to use Ubuntu Terminal and run Ubuntu command line utilities including bash, ssh, git, apt and many more.

[More](#)

Free

[Get](#)

[Add to cart](#)

[Wish list](#)

E EVERYONE **ESRB**

Installation (cont'd)

- Follow the prompts
- Linux user name doesn't need to match Windows user

```
Select james@4896RESB17: ~
Installing, this may take a few minutes...
Please create a default UNIX user account. The username does not need to match your Windows username.
For more information visit: https://aka.ms/wslusers
Enter new UNIX username: james
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Installation successful!
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

james@4896RESB17:~$
```

Installation (cont'd)

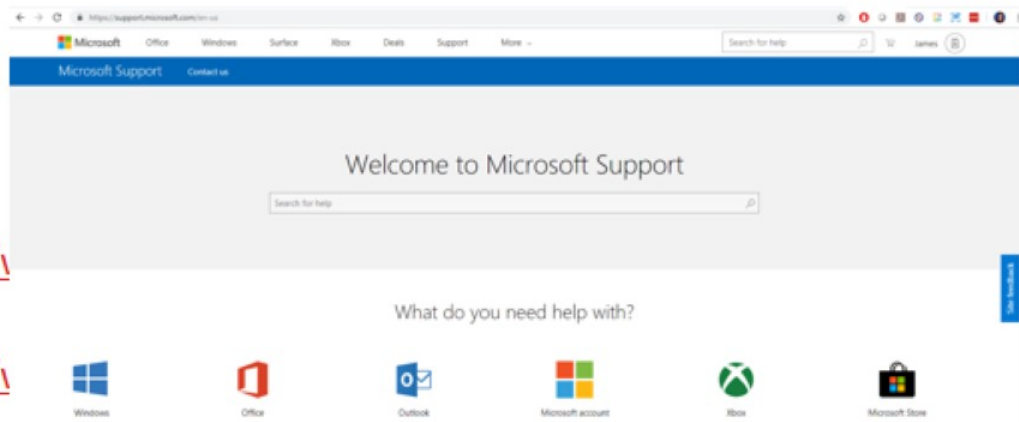
- Resources

- Installation:

- <https://docs.microsoft.com/en-us/windows/win10>
- <https://docs.microsoft.com/en-us/windows/distro>

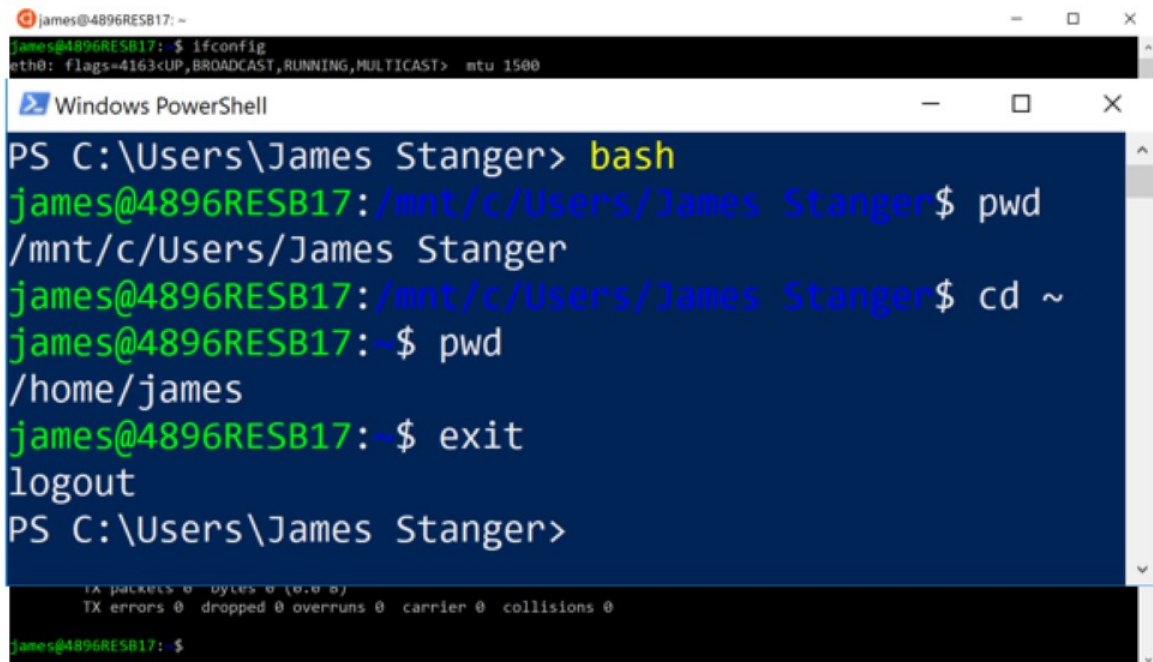
- Troubleshooting: <https://docs.microsoft.com/en-us/windows/wsl/troubleshooting#check-your-build-number>

- FAQ: <https://docs.microsoft.com/en-us/windows/wsl/faq>



Testing the Installation

- Get out of the installation prompt
- Re-open a bash shell
- Go to Start, then open either:
 - PowerShell
 - Command prompt
- Conduct your session
- Type “exit” to get out of the WSL



```
james@4896RESB17: ~  
james@4896RESB17: ~$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
james@4896RESB17: ~$  
Windows PowerShell  
PS C:\Users\James Stanger> bash  
james@4896RESB17: /mnt/c/Users/James Stanger$ pwd  
/mnt/c/Users/James Stanger  
james@4896RESB17: /mnt/c/Users/James Stanger$ cd ~  
james@4896RESB17: ~$ pwd  
/home/james  
james@4896RESB17: ~$ exit  
logout  
PS C:\Users\James Stanger>  
TX packets 0 bytes 0 (0.0 B)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
james@4896RESB17: ~$
```

Install / Manage Applications Using Apt-Get

- Remove unneeded packages
- Services
 - Web server
 - Secure Shell (SSH)
- Dev environments / compilers
 - Python
 - GCC+

```
james@4896RESB17: /mnt/c/Users/James Stanger
james@4896RESB17:/mnt/c/Users/James Stanger$ sudo apt-get install gcc+
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libfreetype6
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu cpp cpp-7 gcc-7 gcc-7-base libasan4
  libatomic1 libbinutils libc-dev-bin libc6-dev libcc1-0 libcilkrts5 libgcc-7-dev libgomp1
  libisl19 libitm1 liblsan0 libmpc3 libmpx2 libquadmath0 libtsan0 libubsan0 linux-libc-dev
  manpages-dev
Suggested packages:
  binutils-doc cpp-doc gcc-7-locales gcc-multilib make autoconf automake libtool flex
  bison gdb gcc-doc gcc-7-multilib gcc-7-doc libgcc1-dbg libgomp1-dbg libitm1-dbg
  libatomic1-dbg libasan4-dbg liblsan0-dbg libtsan0-dbg libubsan0-dbg libcilkrts5-dbg
  libmpx2-dbg libquadmath0-dbg glibc-doc
The following NEW packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu cpp cpp-7 gcc gcc-7 gcc-7-base
```

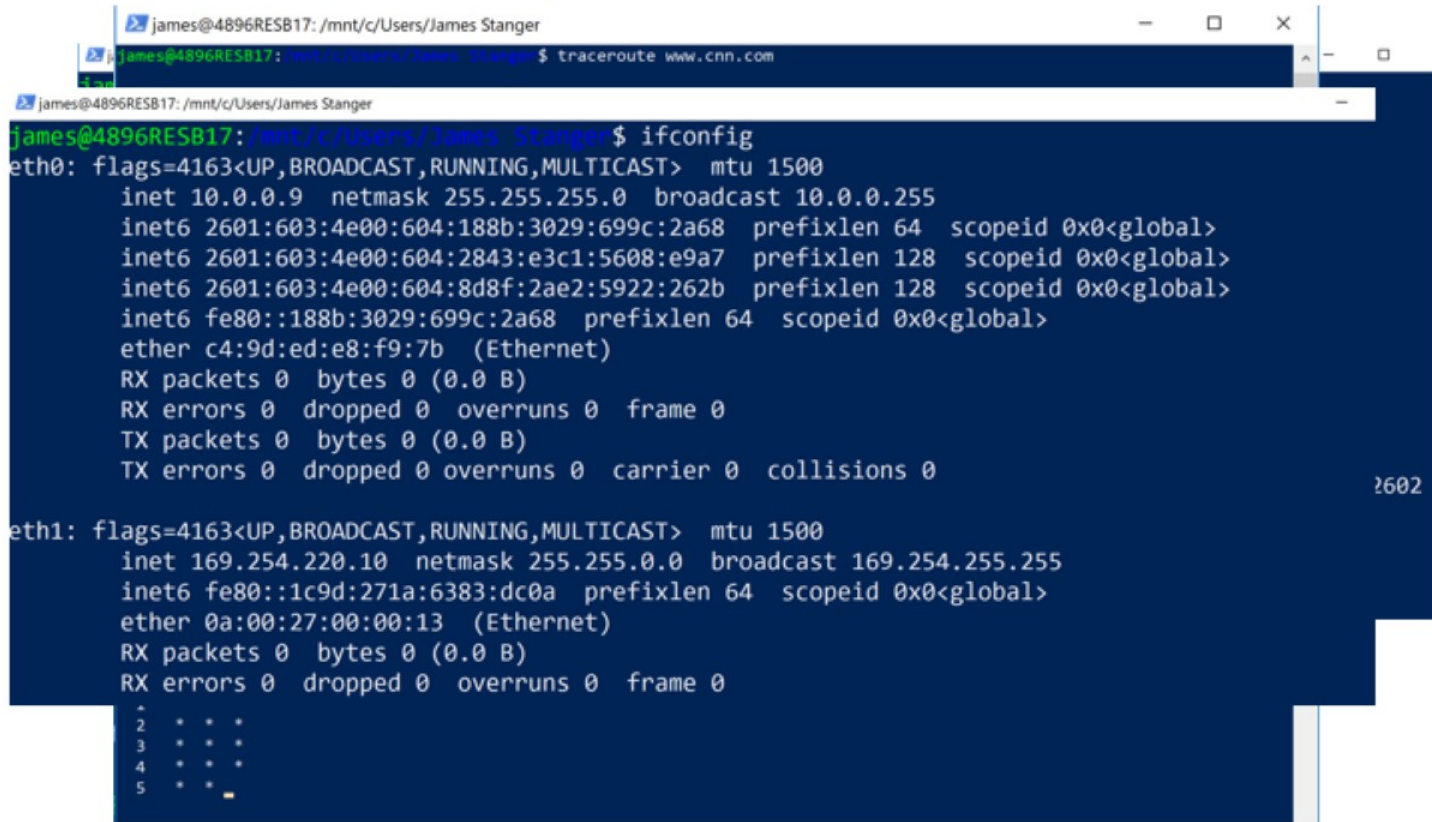
sudo apt-get update

sudo apt-get install gcc+

sudo apt-get install python

Checking Network Connectivity

- ifconfig
- ping
- netstat
- route
- traceroute
- nslookup
- dig
- Configure SSH



The screenshot shows a terminal window with the following content:

```
james@4896RESB17: /mnt/c/Users/James Stanger
james@4896RESB17: /mnt/c/Users/James Stanger$ traceroute www.cnn.com
james@4896RESB17: /mnt/c/Users/James Stanger$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.0.9 netmask 255.255.255.0 broadcast 10.0.0.255
    inet6 2601:603:4e00:604:188b:3029:699c:2a68 prefixlen 64 scopeid 0x0<global>
    inet6 2601:603:4e00:604:2843:e3c1:5608:e9a7 prefixlen 128 scopeid 0x0<global>
    inet6 2601:603:4e00:604:8d8f:2ae2:5922:262b prefixlen 128 scopeid 0x0<global>
    inet6 fe80::188b:3029:699c:2a68 prefixlen 64 scopeid 0x0<global>
    ether c4:9d:ed:e8:f9:7b (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 169.254.220.10 netmask 255.255.0.0 broadcast 169.254.255.255
    inet6 fe80::1c9d:271a:6383:dc0a prefixlen 64 scopeid 0x0<global>
    ether 0a:00:27:00:00:13 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    ^
    2 * * *
    3 * * *
    4 * * *
    5 * * *
```

Looking for System Issues

- top
- ps
- lsof
- free
- du -h
- df -h

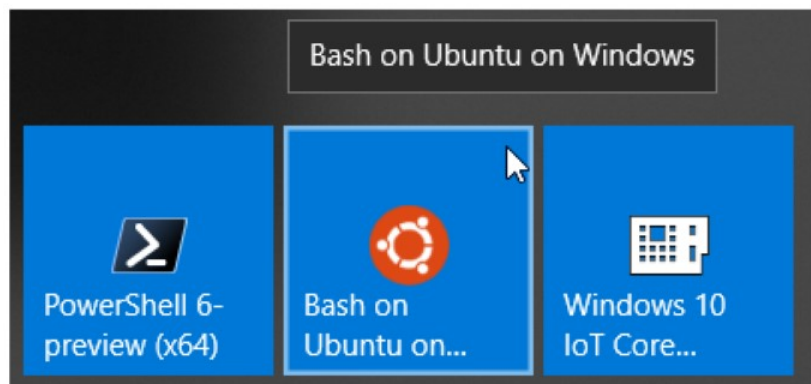
```
james@4896RESB17: /mnt/c/Users/James Stanger
james@4896RESB17: /mnt/c/Users/James Stanger$ free
              total        used        free      shared  buff/cache   available
Mem:      16700708     7579960     8891396        17720     229352     8987016
Swap:      50331648           0     50331648
james@4896RESB17: /mnt/c/Users/James Stanger$ df -h
Filesystem      Size  Used Avail Use% Mounted on
rootfs          476G  404G   73G   85% /
none            476G  404G   73G   85% /dev
none            476G  404G   73G   85% /run
none            476G  404G   73G   85% /run/lock
none            476G  404G   73G   85% /run/shm
none            476G  404G   73G   85% /run/user
C:              476G  404G   73G   85% /mnt/c
D:              1.9T  967G  897G  52% /mnt/d
james@4896RESB17: /mnt/c/Users/James Stanger$ ps
  PID TTY          TIME CMD
   530 tty3      00:00:01 bash
  1350 tty3      00:00:00 ps
james@4896RESB17: /mnt/c/Users/James Stanger$ ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.0   8304   132 ?        Ss   16:28   0:00 /init ro
root         3  0.0  0.0   8304    92 tty1     Ss   16:28   0:00 /init ro
james       4  0.0  0.0  17012  3736 tty1     S    16:28   0:01 -bash
root       190  0.0  0.0   8304    92 tty2     Ss   16:41   0:00 /init ro
james     191  0.0  0.0  17052  3804 tty2     S    16:41   0:00 -bash
root     529  0.0  0.0   8304    92 tty3     Ss   16:53   0:00 /init ro
james     530  0.1  0.0  17052  3732 tty3     S    16:53   0:01 -bash
james    1351  0.0  0.0  17380  1916 tty3     R    17:11   0:00 ps aux
james@4896RESB17: /mnt/c/Users/James Stanger$
```

\$ sudo apt-get install sysstat

Tech Support and the WSL

Considerations

- Windows Issues
 - Permissions
 - Libraries
 - Available resources
 - Memory
 - CPU
- Linux Issues
 - Permissions
 - Applications and users



```
C:\WINDOWS\system32\bash.exe
wsl@MSI-GS70:~ $ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 18.04 LTS
Release:        18.04
Codename:       bionic
wsl@MSI-GS70:~ $
```

Issues with Apt-Get

- Sometimes, apt-get will not run properly in WSL
- Consider permissions changes, as described in this screen shot

1. Write the following to `/usr/sbin/policy-rc.d` and save your changes.

```
bash

#!/bin/sh
exit 101
```

2. Add execute permissions to `/usr/sbin/policy-rc.d`

```
bash

chmod +x /usr/sbin/policy-rc.d
```

3. Run the following commands

```
bash

dpkg-divert --local --rename --add /sbin/initctl
ln -s /bin/true /sbin/initctl
```

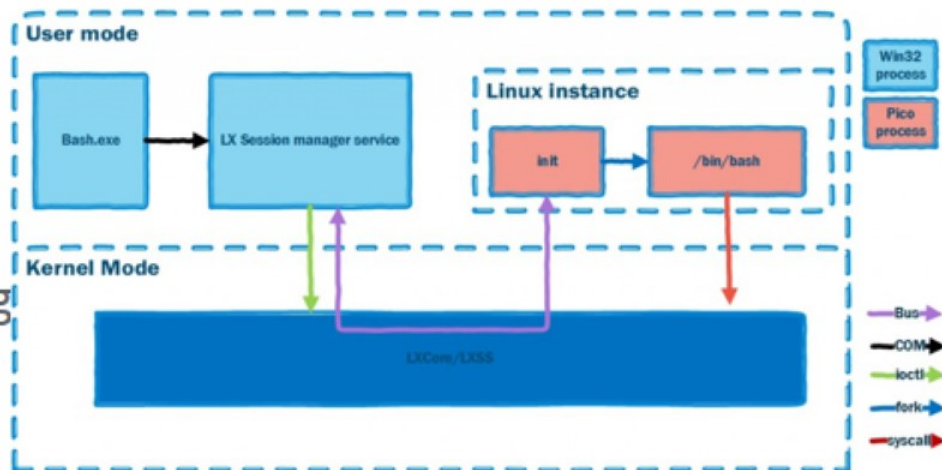
Connectivity and WSL Sessions

- Inspect Windows firewall settings
- Third parties
 - AVG
 - Avast
 - Kaspersky
- Running a Secure Shell (SSH) server
 - You need Administrator privileges
 - Run Bash on Ubuntu as admin
 - Configure SSH server and client in the Linux session



Tips, Tricks and Traps

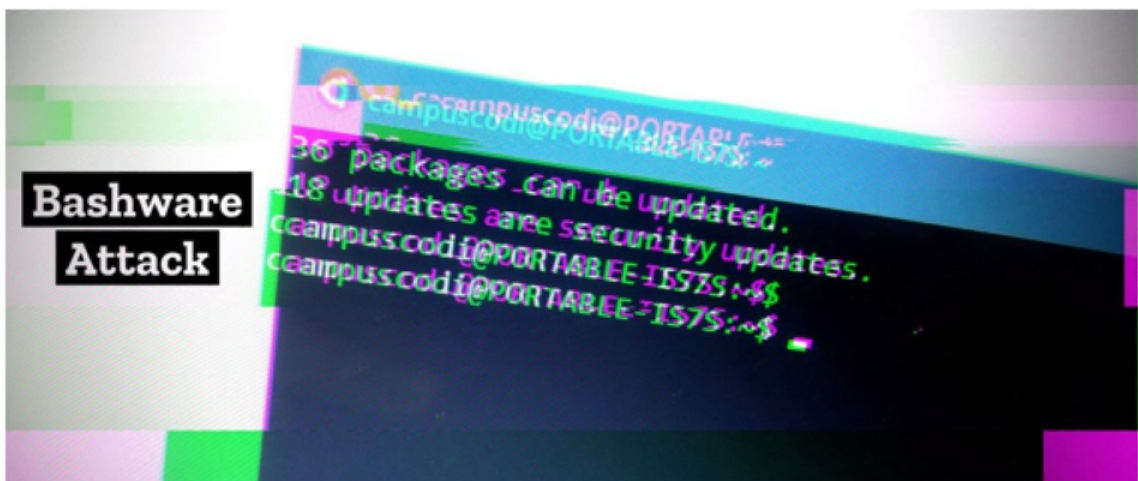
- Windows update
 - Will upgrades “break” it?
 - Consider rollback options
- Disk space
- Editing wsl.conf and using wslconfig to change settings
- Don't forget permissions



WSL and Security

WSL and Security

- Will it increase your attack surface?
 - The Windows system
 - WSL itself
 - The underlying Linux distro and how its configured



WSL and Security (cont'd)

- Permissions considerations
 - The Windows system environment
 - Code that is being created
- Useful not only for developers, but also cybersecurity workers
 - Additional resource
 - Need to create custom pen testing code
 - Python code
 - Bash scripts



Summary

- What is the WSL?
 - What it isn't
 - Who uses it, and why?
- Installing it
- Tech support and the WSL
- WSL and security



Uninstalling WSL

- Open a Windows command prompt
- Type the following:

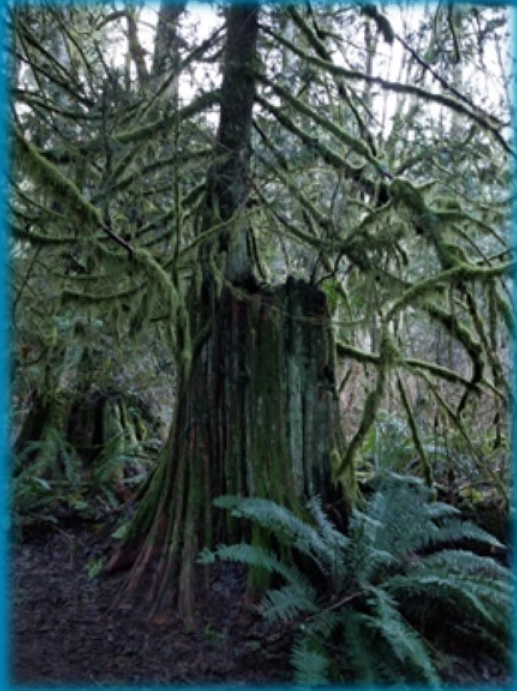
```
lxrun /uninstall /full
```

Note: If you want to keep the user's home directories and other files, omit the /full option

- UWP Ubuntu via start-menu and it worked
- Go back to Windows Features, and uncheck / untick the WSL option

WSL distributions installed from the Windows store can be uninstalled like any other Windows app, by right-clicking on the app tile and clicking Uninstall, or via PowerShell using the Remove-AppxPackage cmdlet

Questions?



Office Hours with James
Wednesday, April 11th
11:00 AM CST

CEUs
TBD

Topic
Investigating the Deep Web and VPN
Technologies

To register:

<https://event.on24.com/wcc/r/1967391/C32B6568414DB31D8207FAE66769DBB>

HDI 2019
Presenting in Person
Orlando, April 9 & 10

CEUs

*Approved for A+, Network+, Security+,
PenTest+, CASP+, Cloud+ and
CySA+ recertification*

Presentations

April 9: Security Fundamentals
for the Support Center

April 10: The Emerging Tech
Hat Trick

More info

<https://tinyurl.com/y4z2g7zx>

Service Desk Show 2019
(London)
Wednesday, 2 May
08:30 – 9:30

CEUs

*Approved for A+, Network+, Security+,
PenTest+, CASP+, Cloud+ and
CySA+ recertification*

Topics Include

Arriving at a narrative: Emerging
tech and the value of the IT
support professional

More info

<https://tinyurl.com/y4qqoat>

Thank You!



James Stanger, PhD

jstanger@comptia.org

+1 (360) 970-5357

Twitter: @jamesstanger

Skype: stangernet

Latest articles and blog entries:

[The Skills needed to combat today's cybersecurity threats \(RSA\)](#)

[Automated Pen Testing](#)
(Admin Magazine)

[Two sides of the same coin: Pen testing and security analytics](#)

[What's hot in network certifications](#)
(NetworkWorld)

[Escaping the Cybersecurity Metrics Matrix](#)
(CompTIA)

[Private Eye: Open source tools for automated pen testing](#) Admin Magazine

[Thoughts about the help desk](#)
(YouTube)

[The Hunt for the Meaning of the Red team](#)
(CompTIA)

[The IT security disconnect](#) (HP Enterprise)

[A blockchain manifesto? A report from the RSA 2018 Blockchain Focus Group](#)
[Cloud Orchestration with Chef](#)
Admin Magazine

[No more close shaves: Talking end user security](#)

[How CIOs can optimize ITSM software](#)
(SearchCIO)

[Vulnerability management: How to target bug bounty programs](#)
(TechTarget)

[My career change journey: The importance of networking](#)

[The role of the service desk in the cybersecurity kill chain \(HDI\)](#)

[How to prevent insiders from breaching your data](#) (Forbes)

[Threat Hunting with Yara](#)
Admin Magazine

[10 critical security skills every IT team needs](#)
(interview, CIO Magazine)

[How AI can help you stay ahead of cybersecurity threats](#) (CSO Magazine)

[Don't hack me, bro!](#) (Admin Magazine)

[At the hop: Security testing with hping3](#)
(Linux Magazine)

My CompTIA hub:

<https://certification.comptia.org/it-career-news/hub/James-Stanger>