Investigating WSL Endpoints

Asif Matadar
@d1r4c

OSDFCon 2020

#whoami

- Director of Endpoint Detection & Response (EDR) at Tanium
- Seasoned Incident Response professional with over a decade working in InfoSec and specifically leading high-profile cases around the world, such as advanced targeted attacks, nation-state attacks, and data breaches, to name a few
- Public speaker at industry recognised conferences around the world:
  - DFRWS USA 2020
  - WSLConf (U.S.) 2020
  - OSDFCon (U.S.) 2019
  - OSDFCon (U.S.) 2018
  - IMF (Germany) 2018
  - OSDFCon (U.S.) 2017
  - BSidesNOLA (U.S.) 2017
  - BSidesMCR (U.K.) 2015
- Research focus on memory analysis and automation, *nix-based forensics, cloud forensics, and triage analysis

Investigating WSL Endpoints

- Since the announcement of the Windows Subsystem for Linux (WSL) back in 2016, there has been a lot of excitement to try and leverage WSL across workstations and servers a like by organisations and those that work in the industry.

- What does that mean for someone who works as a Digital Forensics & Incident Response professional?
  - Well adversaries and malware authors have already started focussing their attention on WSL; therefore, it is important to understand the underlying architecture changes that will allow one to investigate a compromised Windows 10 or Windows Server 2019 in the not too distant future.

- This talk will highlight the nuances to be aware of from a Digital Forensics & Incident Response perspective and illustrate forensic artefacts of interest, which will consist of a forensic examination on a WSL Endpoint to provide the audience an appreciation of what that entails and share insights that will assist them when the time arises.

Agenda

- What is WSL 2?
- What does that mean for Digital Forensics & Incident Response professionals?
- Forensic examination on a WSL Endpoint
  - 11 experiments

What is WSL2?

What is WSL 2?

- Full System Call Compatibility
  - WSL 2 has its own customised kernel specifically for WSL 2
    - Docker
  - WSL 1 had a translation layer to interpret the system calls, that allows them to work on the Windows NT kernel
- Faster than WSL 1
- Raw sockets

What is WSL 2?

- New architecture for Windows Subsystem for Linux
- Developed in-house kernel from stable branch at kernel.org source from version 4.19 kernel
- Customised kernel specifically for WSL 2
- As it's developed by Microsoft, updates to the kernel will be serviced by Windows Update
- Lightweight Utility VM
  - Hyper-V hypervisor

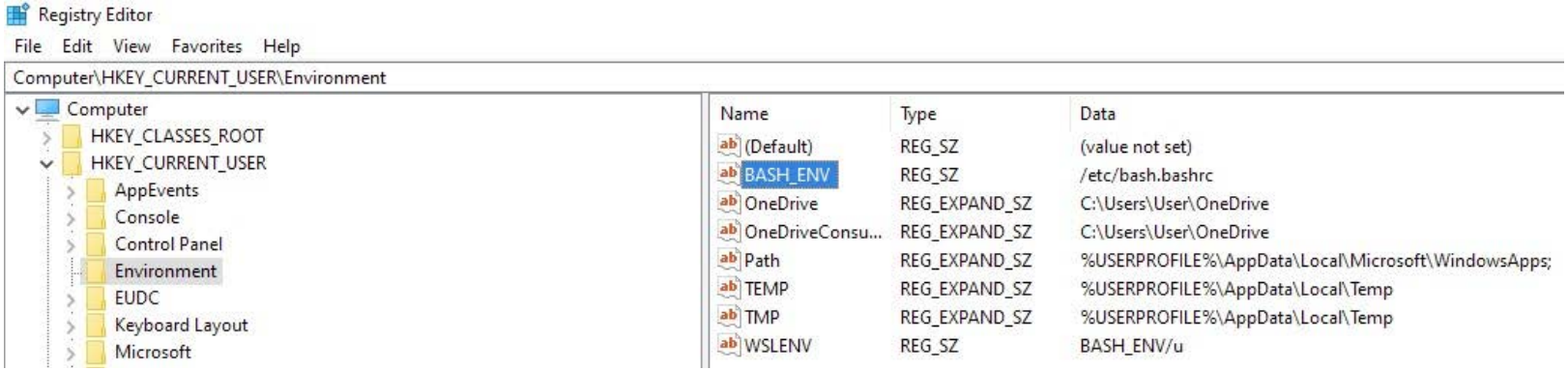
What does that mean for Digital Forensics & Incident Response professionals?

What does that mean for Digital Forensics & Incident Response professionals?

- Full System Call Compatibility
- Lightweight Utility VM
  - Hyper-V hypervisor
  - Not a traditional Virtual Machine
  - EXT4 Virtual Disk
    - `C:\Users\User\AppData\Local\Packages\CanonicalGroupLimited.UbuntuonWindows_79rhkp1fndgsc\LocalState\ext4.vhdx`
- Management of WSL
  - wsl.exe (WSL 2)
  - wslconfig (WSL 1)

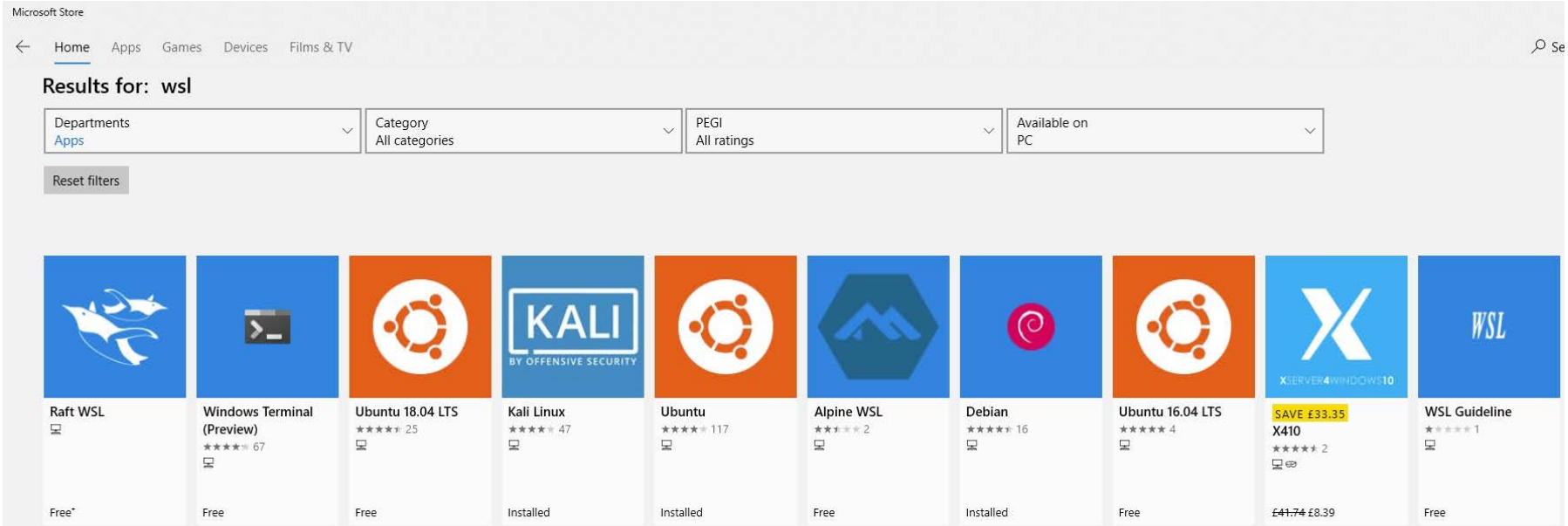
What does that mean for Digital Forensics & Incident Response professionals?

Environment Variables



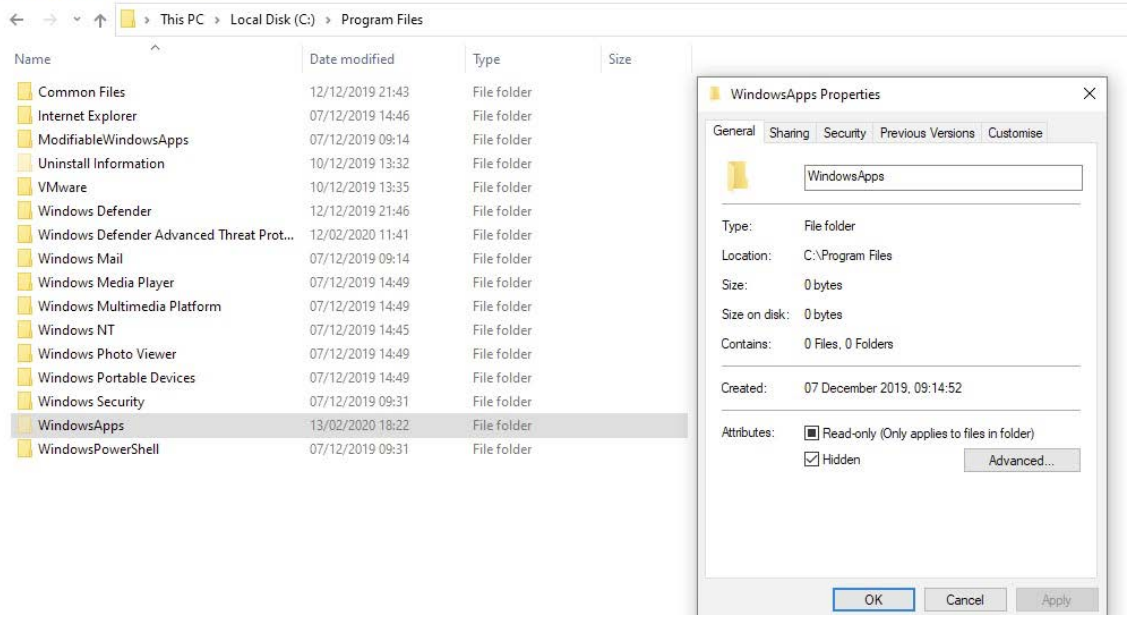
What does that mean for Digital Forensics & Incident Response professionals?

Microsoft Store



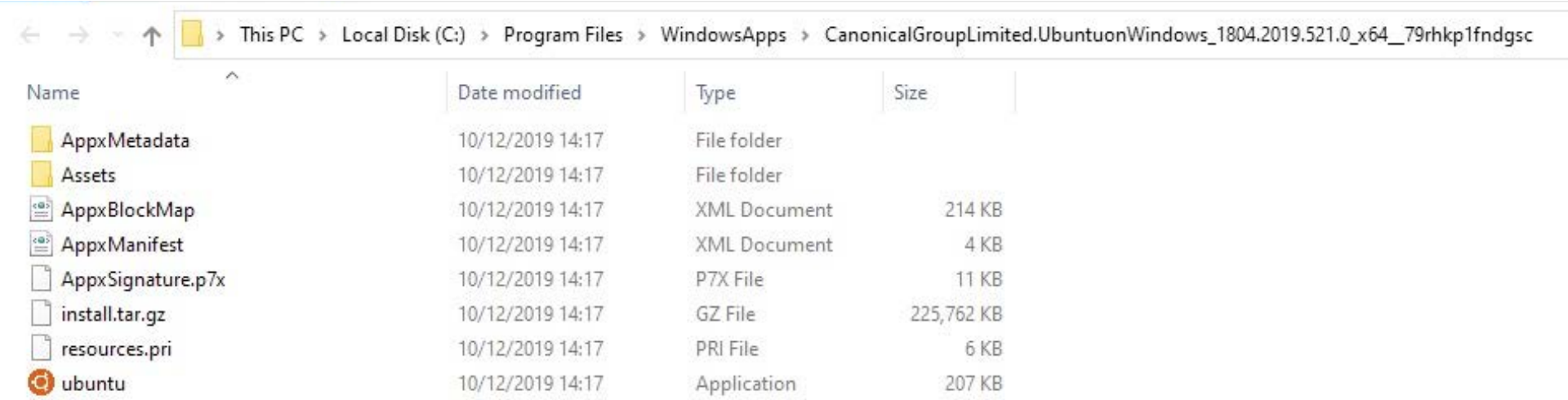
What does that mean for Digital Forensics & Incident Response professionals?

WindowsApps



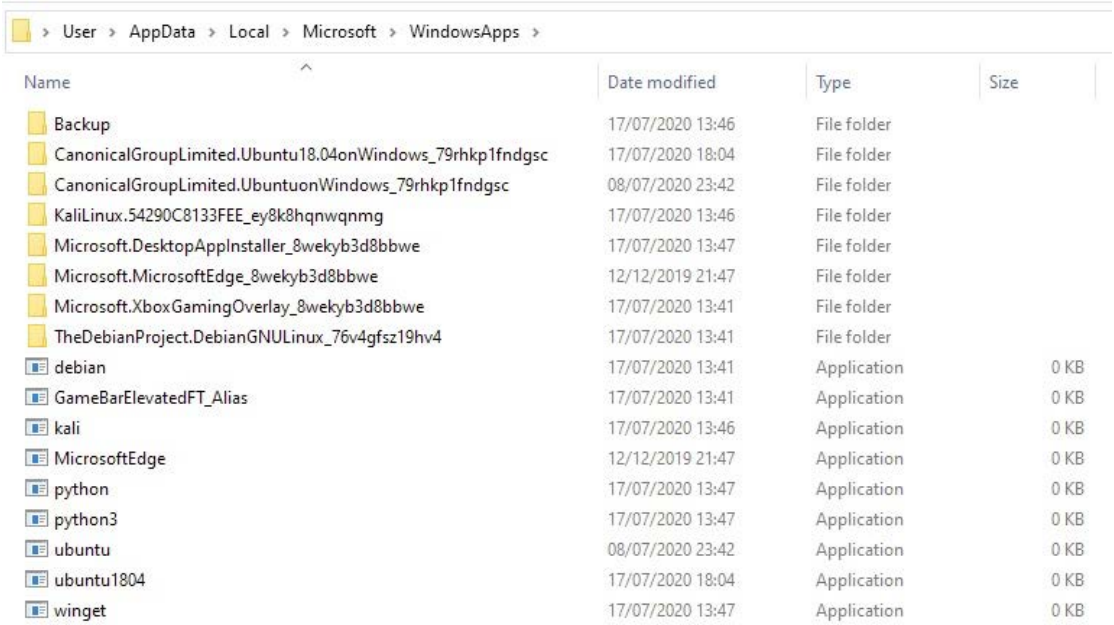
What does that mean for Digital Forensics & Incident Response professionals?

WindowsApps



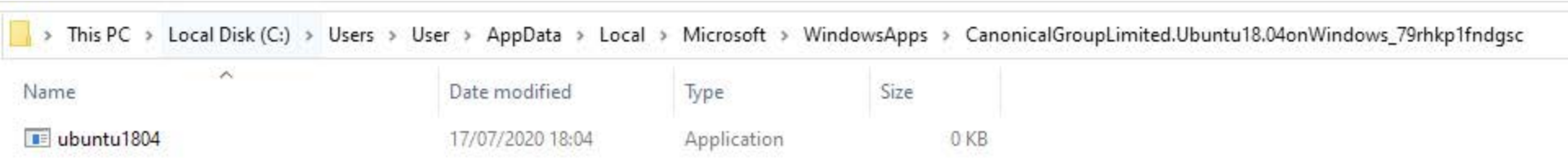
What does that mean for Digital Forensics & Incident Response professionals?

WindowsApps



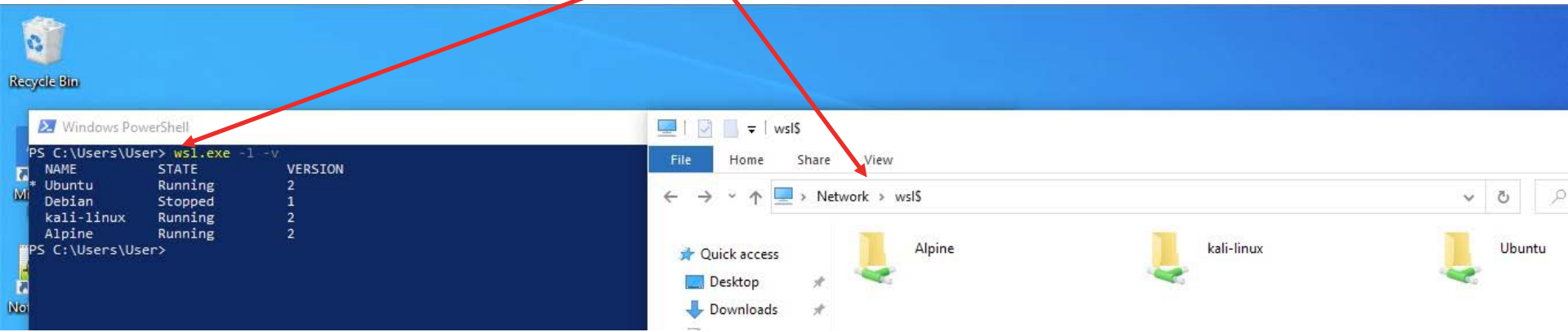
What does that mean for Digital Forensics & Incident Response professionals?

WindowsApps



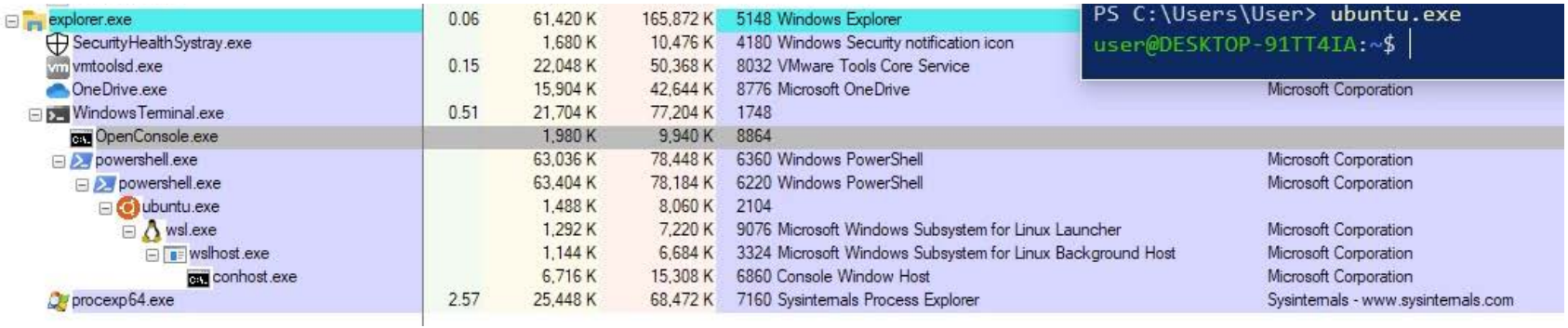
What does that mean for Digital Forensics & Incident Response professionals?

Access to Linux files



What does that mean for Digital Forensics & Incident Response professionals?

Windows Terminal

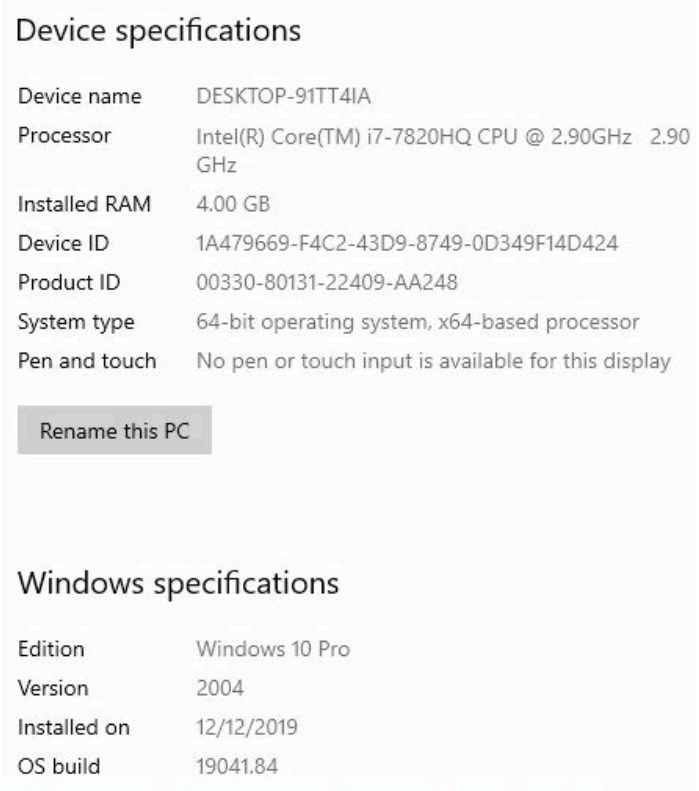


explorer.exe	0.06	61,420 K	165,872 K	5148	Windows Explorer	
SecurityHealthSystray.exe		1,680 K	10,476 K	4180	Windows Security notification icon	
vmtoolsd.exe	0.15	22,048 K	50,368 K	8032	VMware Tools Core Service	
OneDrive.exe		15,904 K	42,644 K	8776	Microsoft OneDrive	Microsoft Corporation
WindowsTerminal.exe	0.51	21,704 K	77,204 K	1748		
OpenConsole.exe		1,980 K	9,940 K	8864		
powershell.exe		63,036 K	78,448 K	6360	Windows PowerShell	Microsoft Corporation
powershell.exe		63,404 K	78,184 K	6220	Windows PowerShell	Microsoft Corporation
ubuntu.exe		1,488 K	8,060 K	2104		
wsl.exe		1,292 K	7,220 K	9076	Microsoft Windows Subsystem for Linux Launcher	Microsoft Corporation
wslhost.exe		1,144 K	6,684 K	3324	Microsoft Windows Subsystem for Linux Background Host	Microsoft Corporation
conhost.exe		6,716 K	15,308 K	6860	Console Window Host	Microsoft Corporation
procexp64.exe	2.57	25,448 K	68,472 K	7160	Sysinternals Process Explorer	Sysinternals - www.sysinternals.com

Forensic examination on a WSL Endpoint

Forensic examination on a WSL Endpoint

- Environment:
  - Windows 10 Pro
  - Version 2004
  - Installed on 12/12/2019
  - OS Build 19041.84



Forensic examination on a WSL Endpoint

- Experiments

1. Persistence: Bashrc
2. Persistence: Persistence through Inception! (Systemd)
3. Persistence: Crontab
4. Execution: Bourne Shell Reverse Shell
5. Execution: PowerShell Reverse Shell
6. Execution: Python Download File
7. Lateral Movement: Remote File Copy
8. Command and Control: Custom Command and Control Protocol
9. Execution: wsl.exe
10. Execution: bash.exe
11. Execution: curl.exe

Persistence: Bashrc

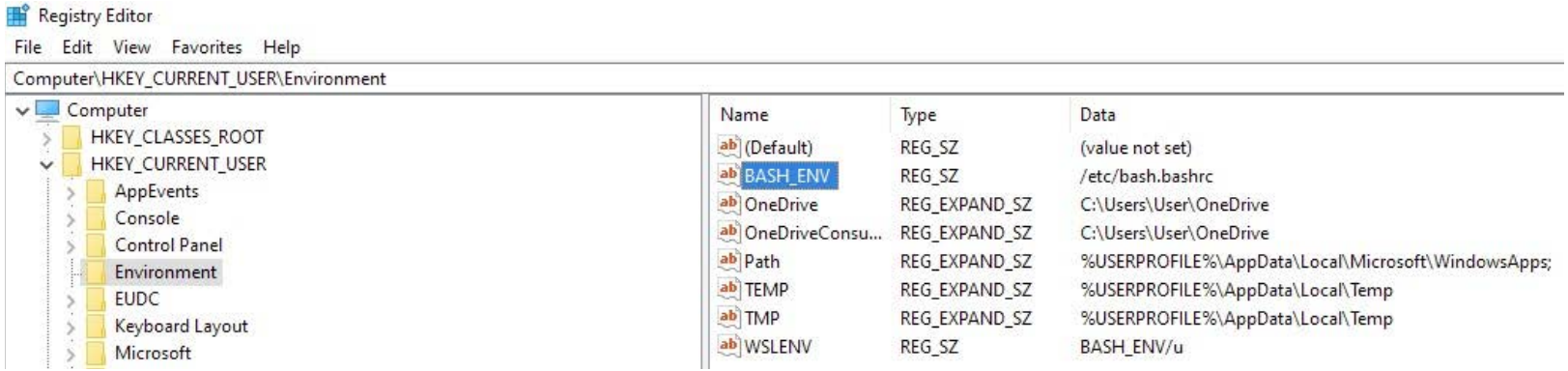
Forensic examination on a WSL Endpoint

Persistence: Bashrc

Registry Key: HKEY_CURRENT_USER\Environment

Registry Key Name: BASH_ENV

Registry Data Name: /etc/bash.bashrc

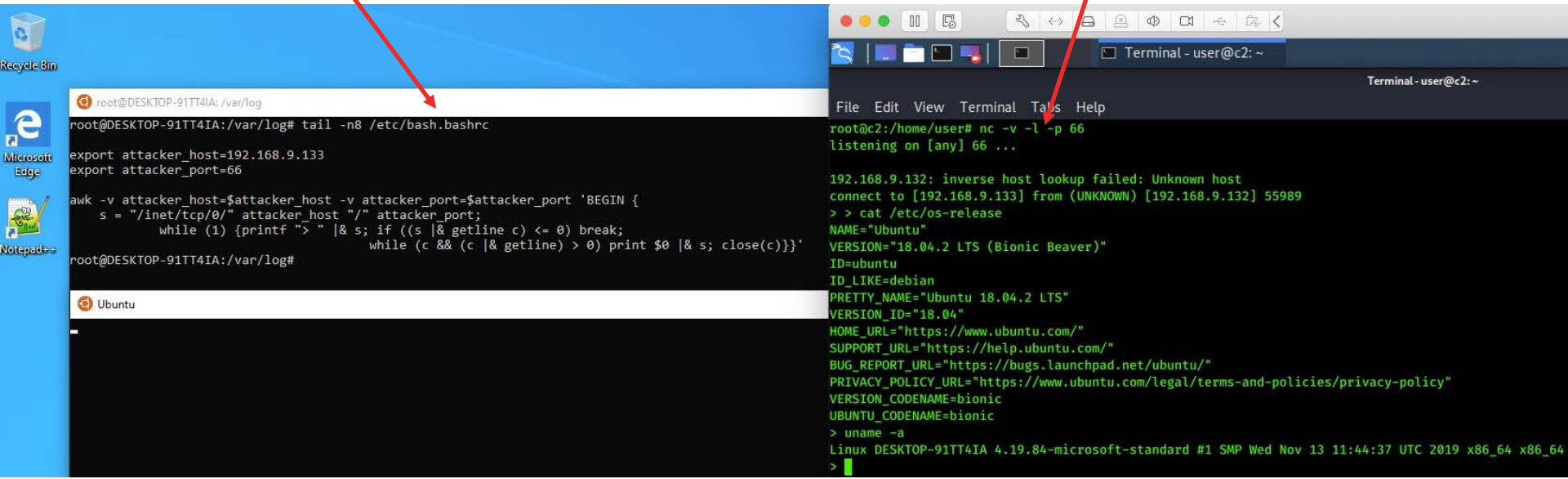


Forensic examination on a WSL Endpoint

Persistence: Bashrc

Modify /etc/bash.bashrc

Attacker Listener



Forensic examination on a WSL Endpoint

Persistence: Bashrc

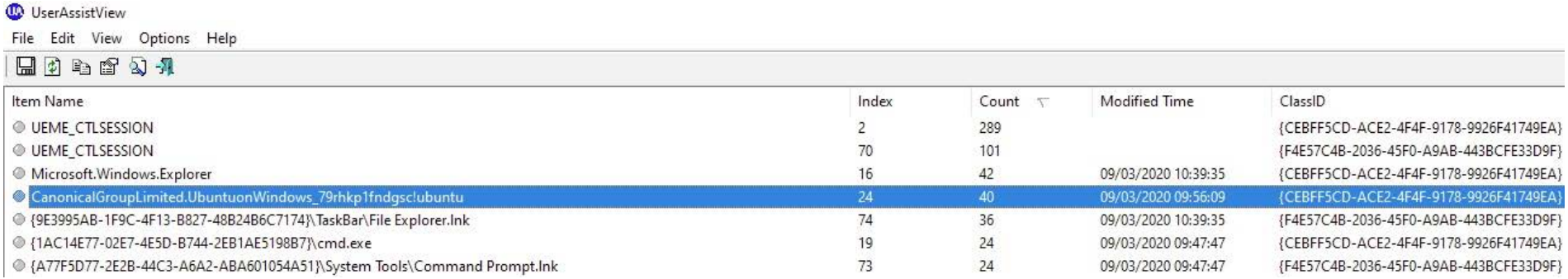
- Trace the MAC times and data contents
  - `/etc/bash.bashrc, ~/.bash_history, ~/.sh_history`
- Timeline of the inodes

- Process Execution:
  - AMCache Program Entries
    - `2020-02-26 10:21:57,CanonicalGroupLimited.UbuntuonWindows,1804.2019.521`
  - AMCache Associated File Entries
    - `CanonicalGroupLimited.UbuntuonWindows,2019-12-12 21:48:22`
  - AppCompactCache
    - `C:\Program Files\WindowsApps\CanonicalGroupLimited.UbuntuonWindows_1804.2019.521.0_x64__79rhkp1fndgsc\ubuntu.exe`
    - `CanonicalGroupLimited.UbuntuonWindows`

Forensic examination on a WSL Endpoint

Persistence: Bashrc

- UserAssist



Item Name	Index	Count	Modified Time	ClassID
UEME_CTLSESSION	2	289		{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
UEME_CTLSESSION	70	101		{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
Microsoft.Windows.Explorer	16	42	09/03/2020 10:39:35	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
CanonicalGroupLimited.UbuntuonWindows_79rhkp1fndgsc!ubuntu	24	40	09/03/2020 09:56:09	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
{9E3995AB-1F9C-4F13-B827-48B24B6C7174}\TaskBar\File Explorer.lnk	74	36	09/03/2020 10:39:35	{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\cmd.exe	19	24	09/03/2020 09:47:47	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
{A77F5D77-2E2B-44C3-A6A2-ABA601054A51}\System Tools\Command Prompt.lnk	73	24	09/03/2020 09:47:47	{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}

Forensic examination on a WSL Endpoint

Persistence: Bashrc

- Prefetch
  - `/Windows/Prefetch/UBUNTU.EXE-39E7ED6A.pf`

- MFT
  - `/Users/User/AppData/Local/Packages/CanonicalGroupLimited.UbuntuonWindows_79rhkp1fndgsc/LocalState/ext4.vhdx`
  - `/Users/User/AppData/Local/Microsoft/WindowsApps/ubuntu.exe`
  - `/Users/User/AppData/Local/Microsoft/WindowsApps/CanonicalGroupLimited.UbuntuonWindows_79rhkp1fndgsc/ubuntu.exe`

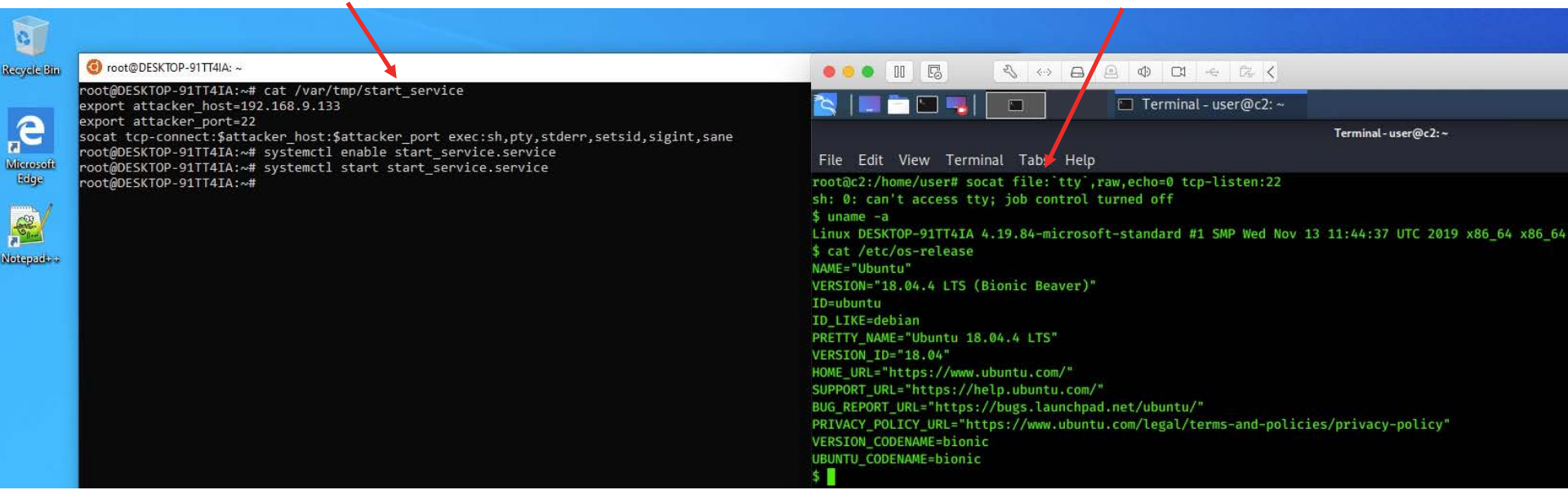
Persistence: Persistence through Inception! (Systemd)

Forensic examination on a WSL Endpoint

Persistence: Persistence through Inception! (Systemd)

Systemd Service

Attacker Listener

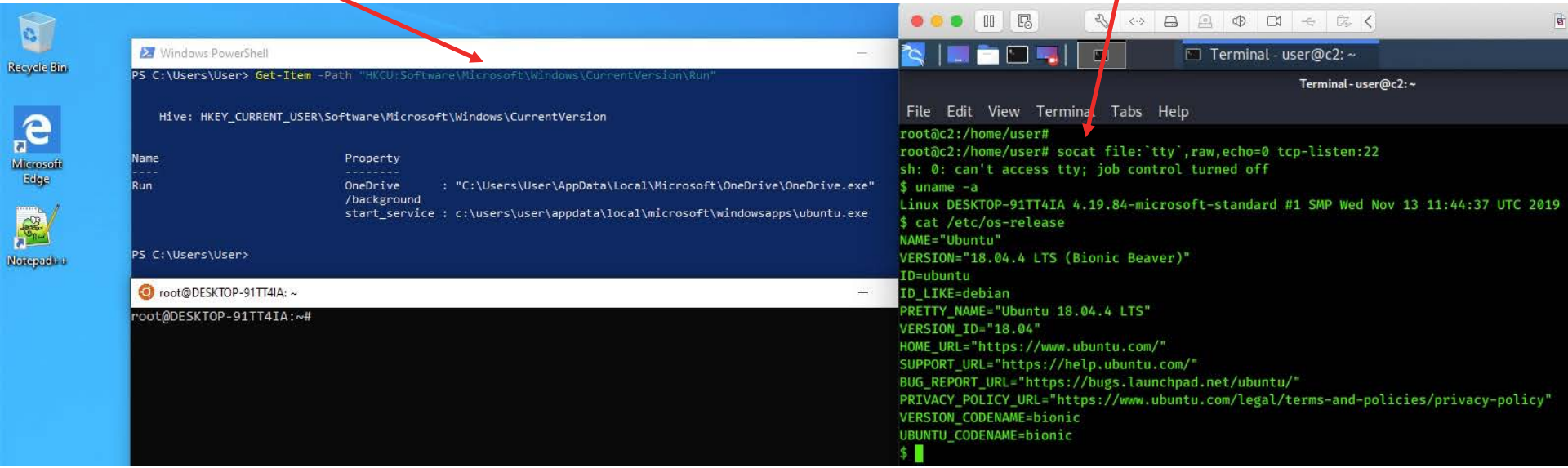


Forensic examination on a WSL Endpoint

Persistence: Persistence through Inception! (Systemd)

Run Key

Attacker Listener



Forensic examination on a WSL Endpoint

Persistence: Persistence through Inception! (Systemd)

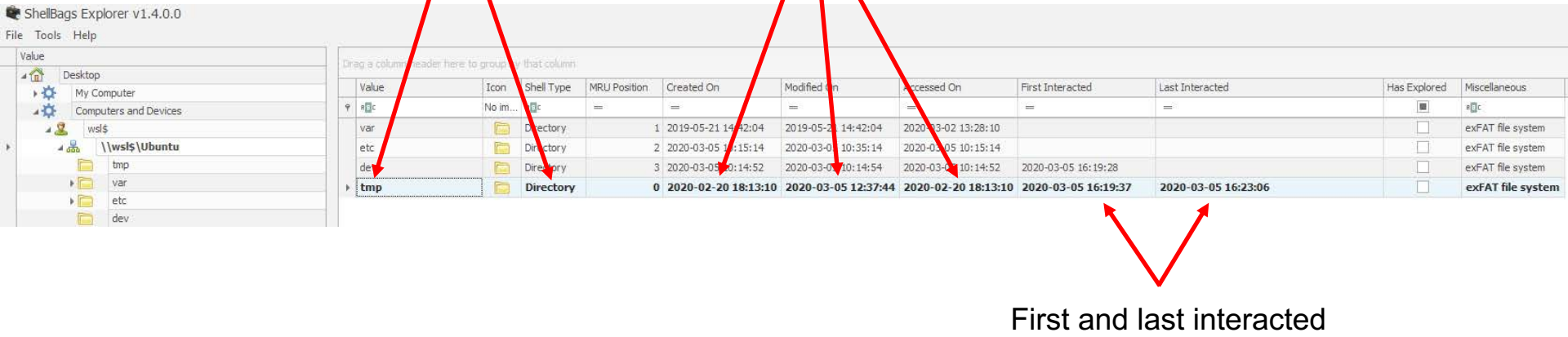
- Systemd Journals
  - `/run/log/journal/*/system.journal`
  - `/run/systemd/journal/*`
- Systemd configuration files
  - `/etc/systemd/system/*`
  - `/run/systemd/*`
  - `/var/lib/systemd/*`
  - `/usr/lib/systemd/*`
- Registry Artefacts for persistence

Forensic examination on a WSL Endpoint

Persistence: Persistence through Inception! (Systemd)

tmp Directory

MAC Times



First and last interacted

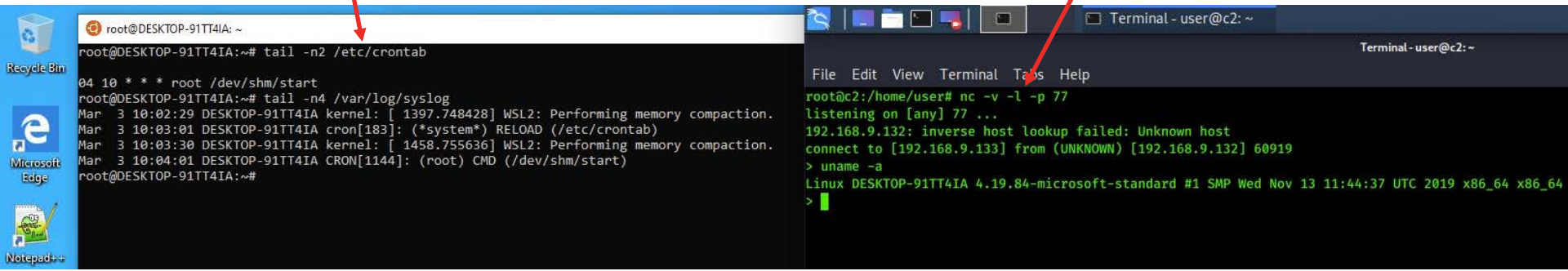
Persistence: Crontab

Forensic examination on a WSL Endpoint

Persistence: Crontab

Modify /etc/crontab

Attacker Listener



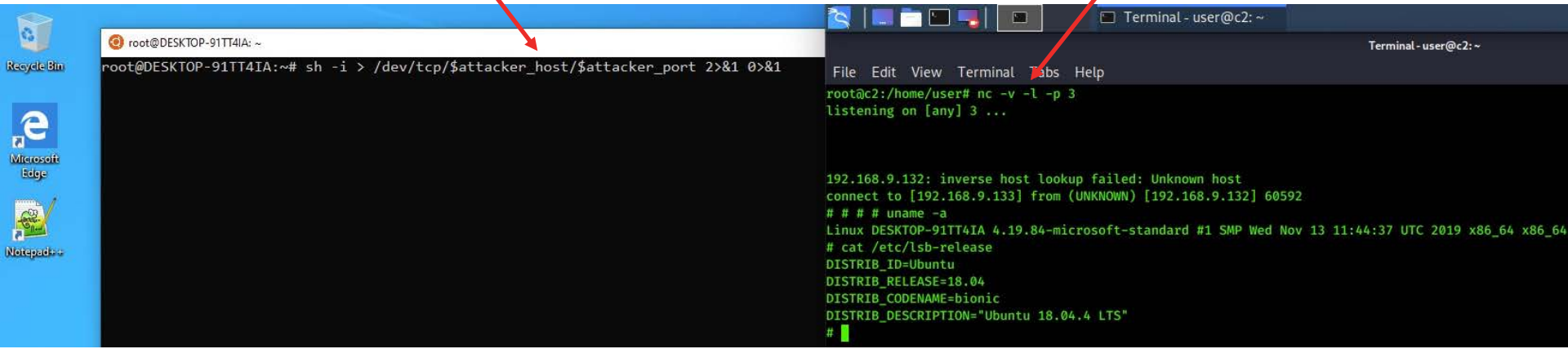
Execution: Bourne Shell Reverse Shell

Forensic examination on a WSL Endpoint

Execution: Bourne Shell Reverse Shell

Bourne Shell Reverse Shell

Attacker Listener



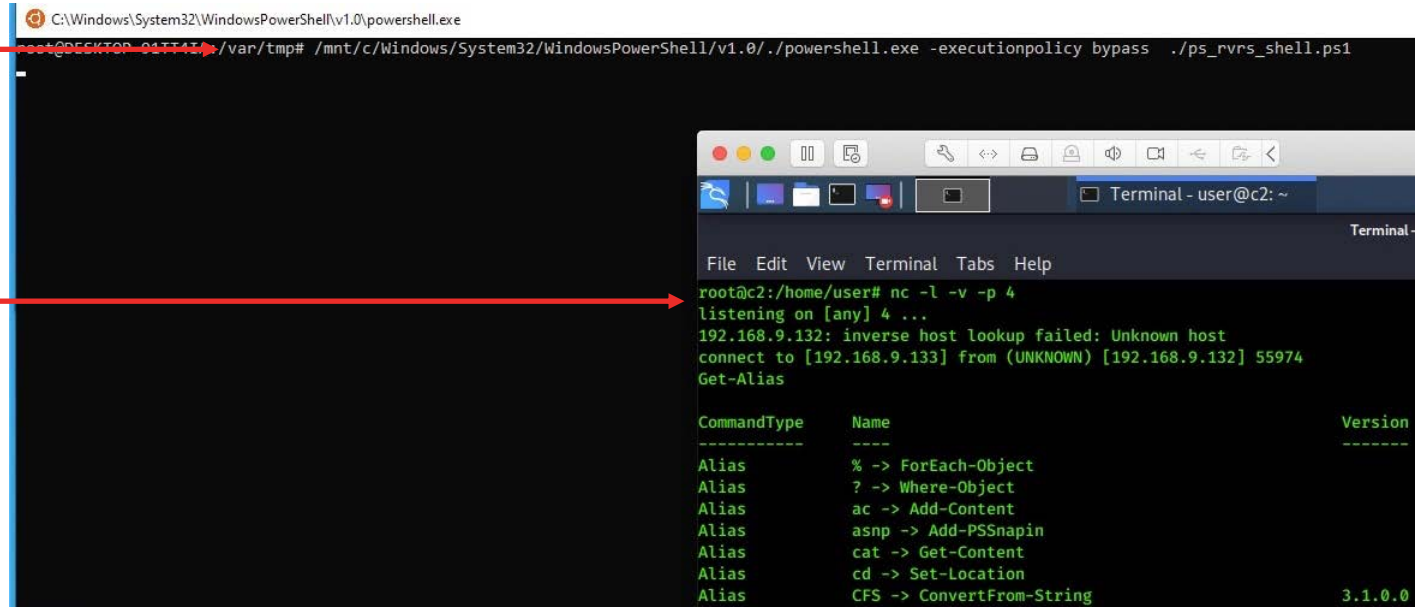
Execution: PowerShell Reverse Shell

Forensic examination on a WSL Endpoint

Execution: PowerShell Reverse Shell

PowerShell Reverse Shell

Attacker Listener

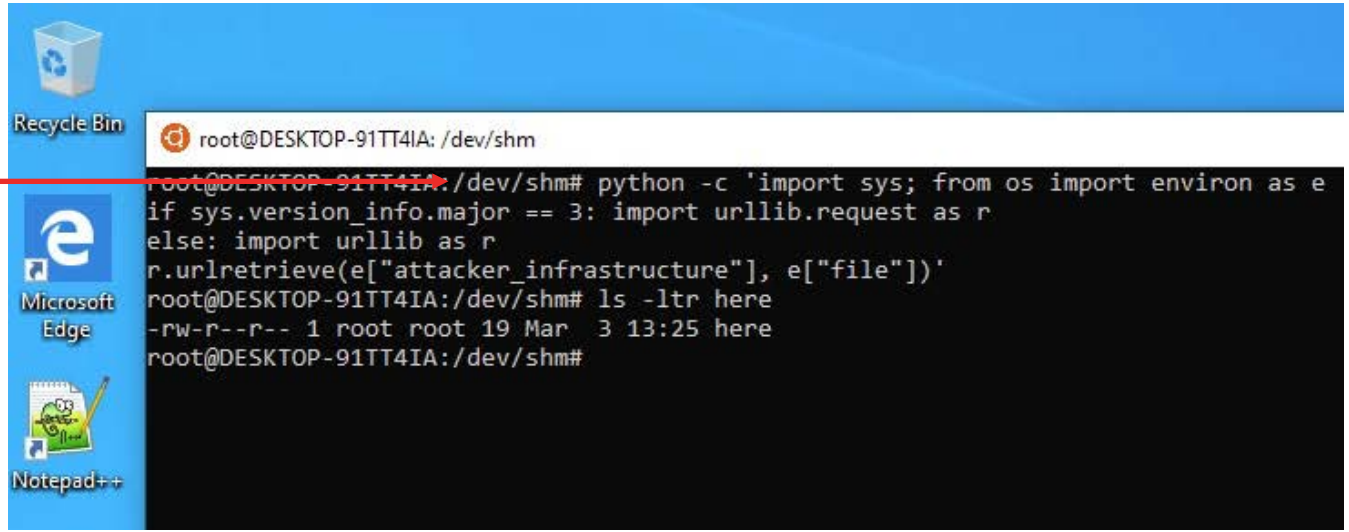


Execution: Python Download File

Forensic examination on a WSL Endpoint

Execution: Python Download File

Python Download File

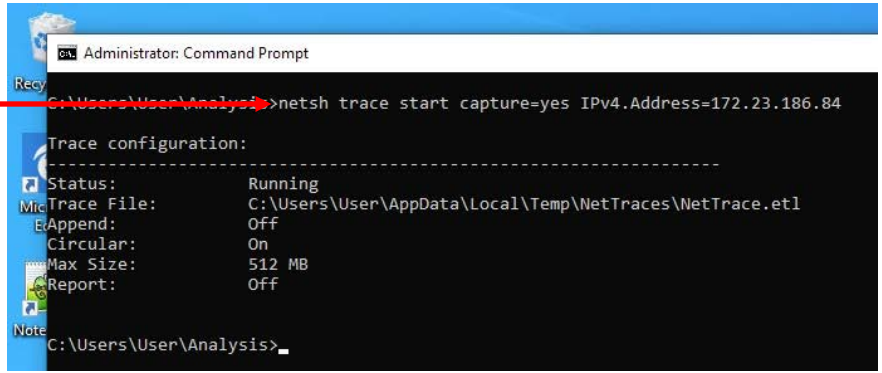


Lateral Movement: Remote File Copy

Forensic examination on a WSL Endpoint

Lateral Movement: Remote File Copy

Enable trace

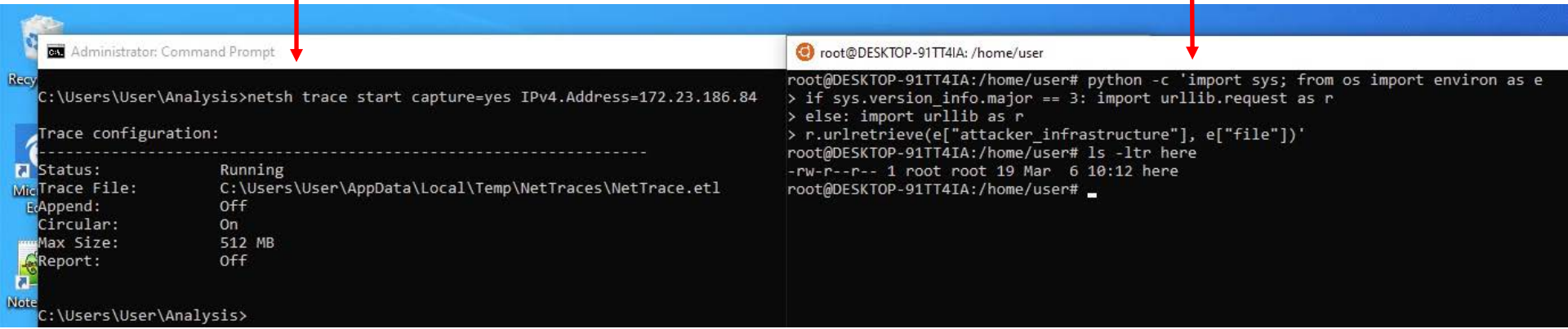


Forensic examination on a WSL Endpoint

Lateral Movement: Remote File Copy

netsh trace start

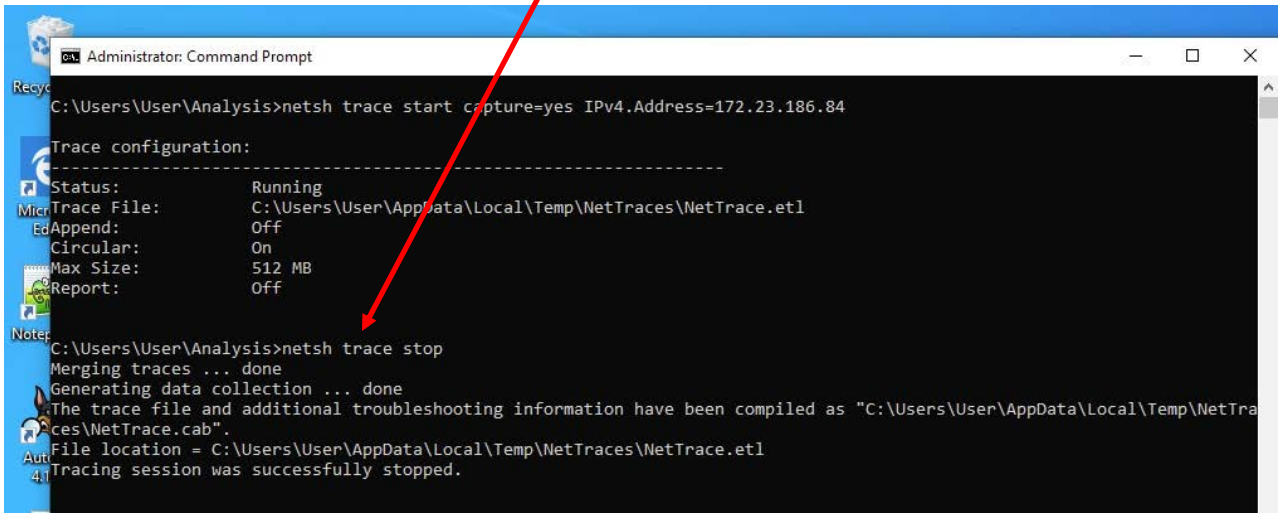
Download file with python



Forensic examination on a WSL Endpoint

Lateral Movement: Remote File Copy

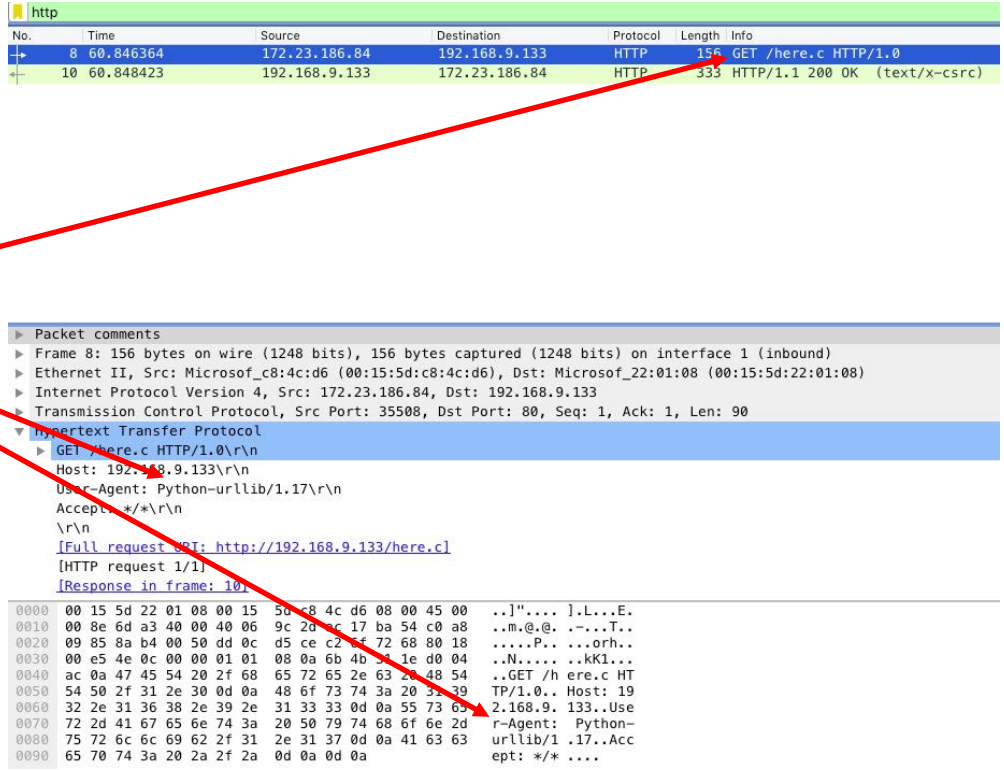
Stop trace



Forensic examination on a WSL Endpoint

Lateral Movement: Remote File Copy

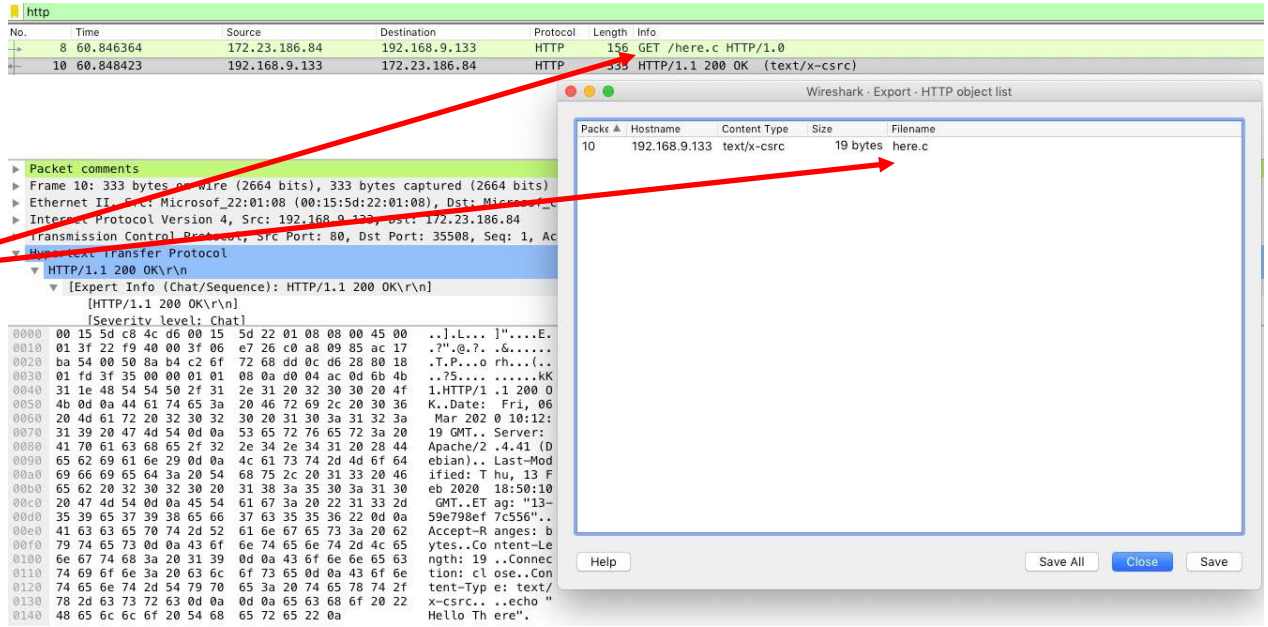
Download file with python



Forensic examination on a WSL Endpoint

Lateral Movement: Remote File Copy

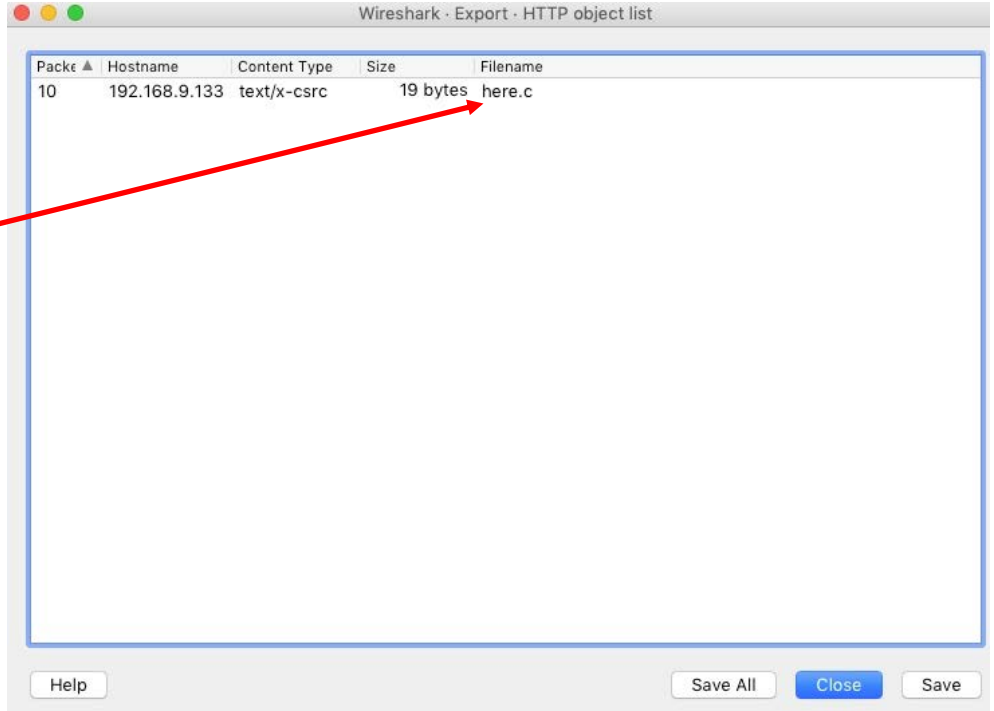
Download file with python



Forensic examination on a WSL Endpoint

Lateral Movement: Remote File Copy

Extract and download file

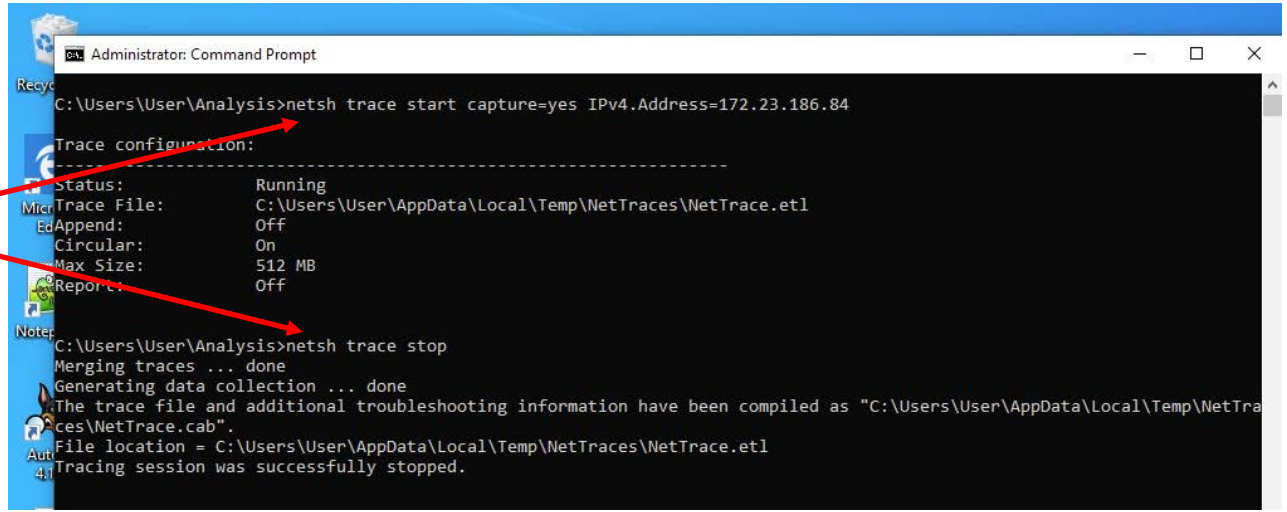


Command and Control: Custom Command and Control Protocol

Forensic examination on a WSL Endpoint

Command and Control: Custom Command and Control Protocol

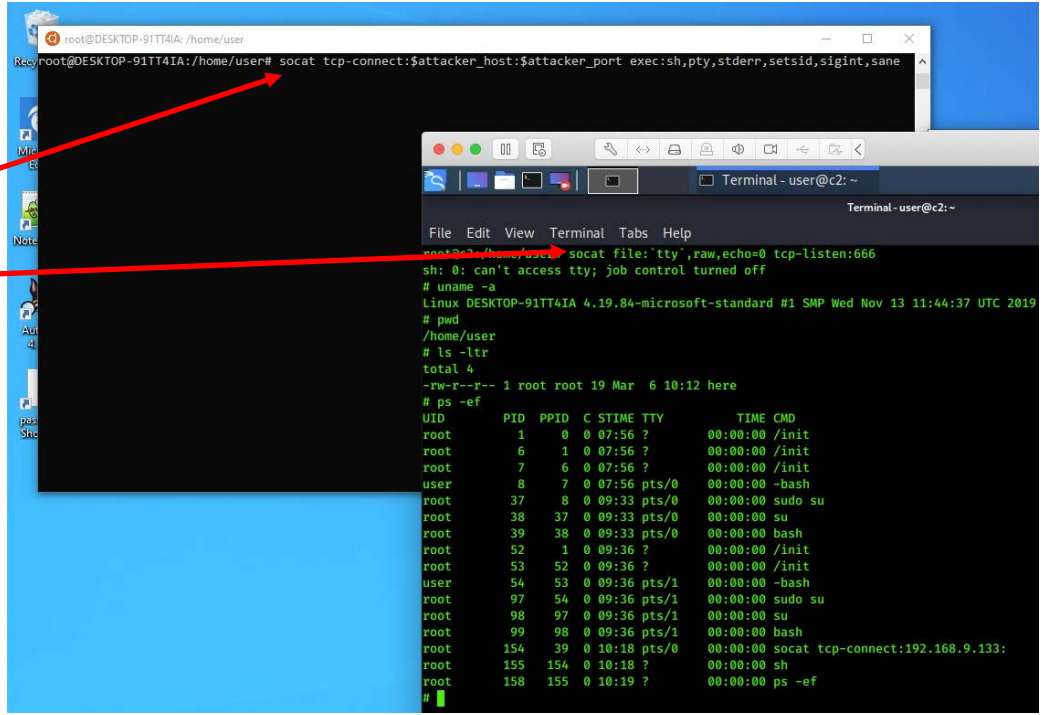
Enable and stop trace



Forensic examination on a WSL Endpoint

Command and Control: Custom Command and Control Protocol

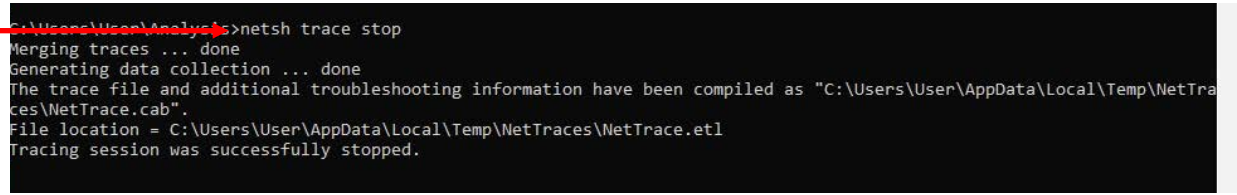
Socat Reverse Shell



Forensic examination on a WSL Endpoint

Command and Control: Custom Command and Control Protocol

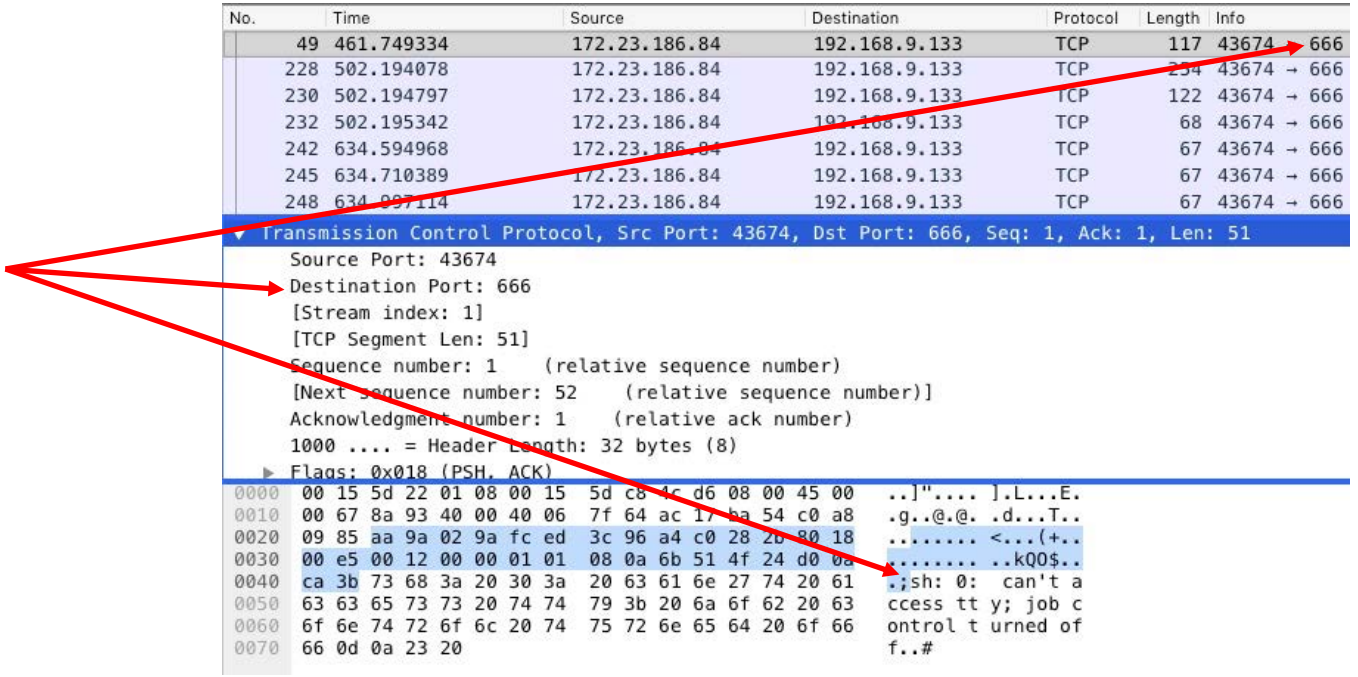
Stop trace



Forensic examination on a WSL Endpoint

Command and Control: Custom Command and Control Protocol

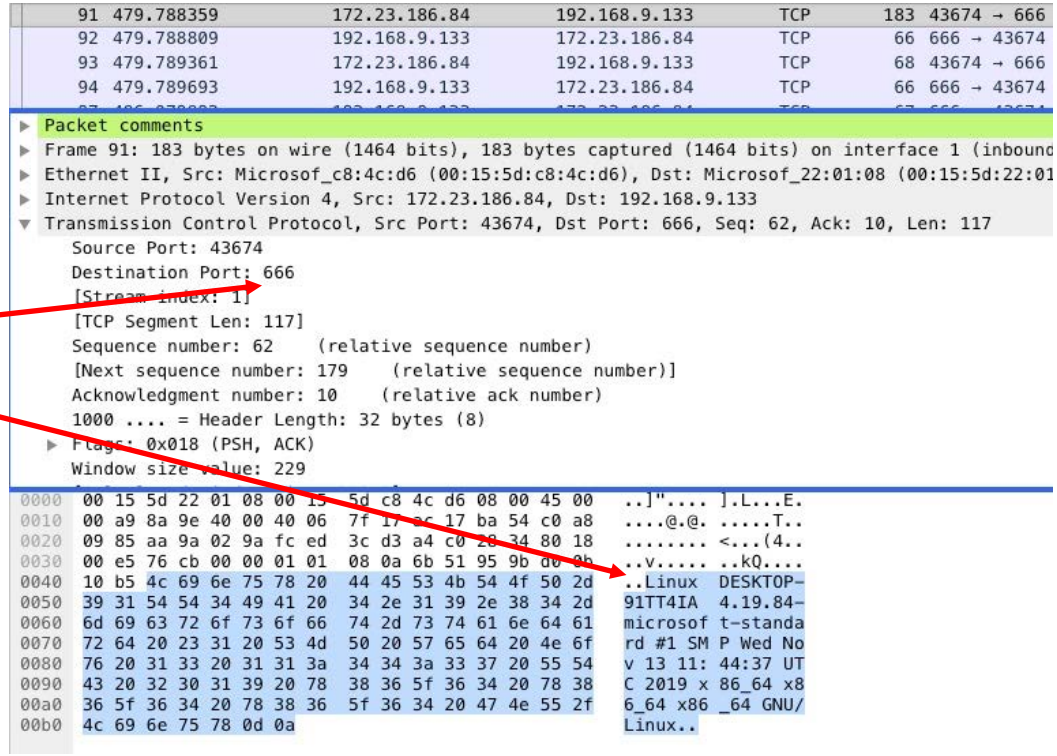
Socat Reverse Shell



Forensic examination on a WSL Endpoint

Command and Control: Custom Command and Control Protocol

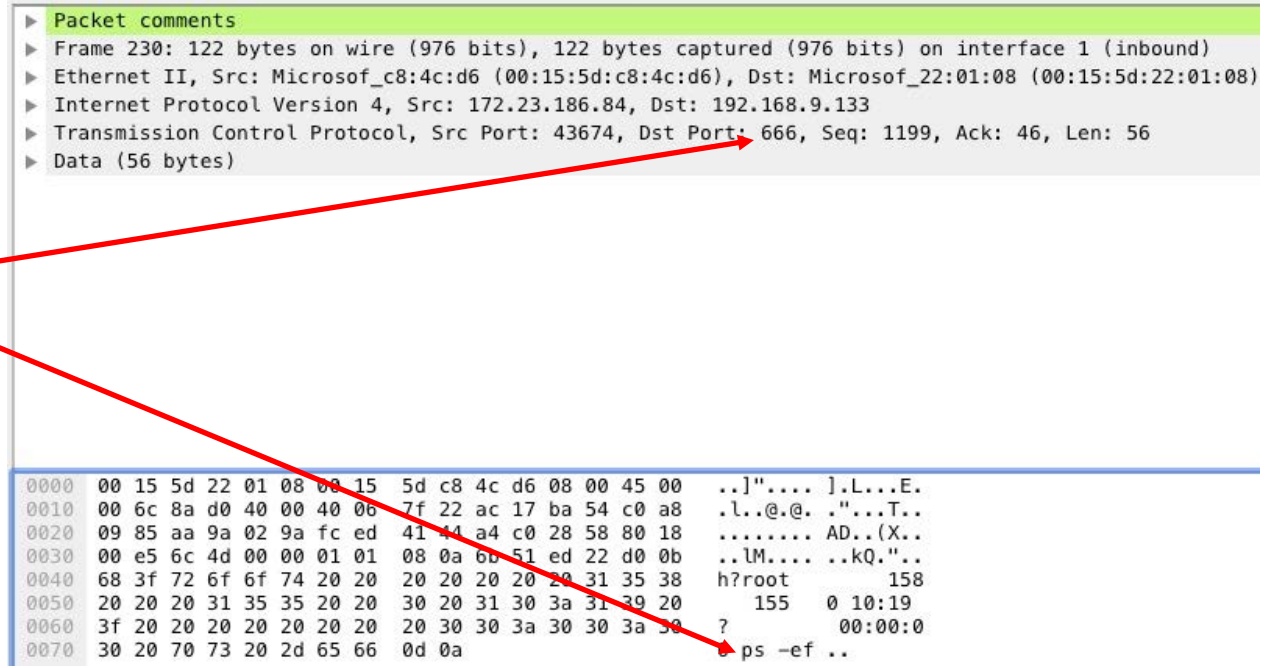
Socat Reverse Shell



Forensic examination on a WSL Endpoint

Command and Control: Custom Command and Control Protocol

Socat Reverse Shell

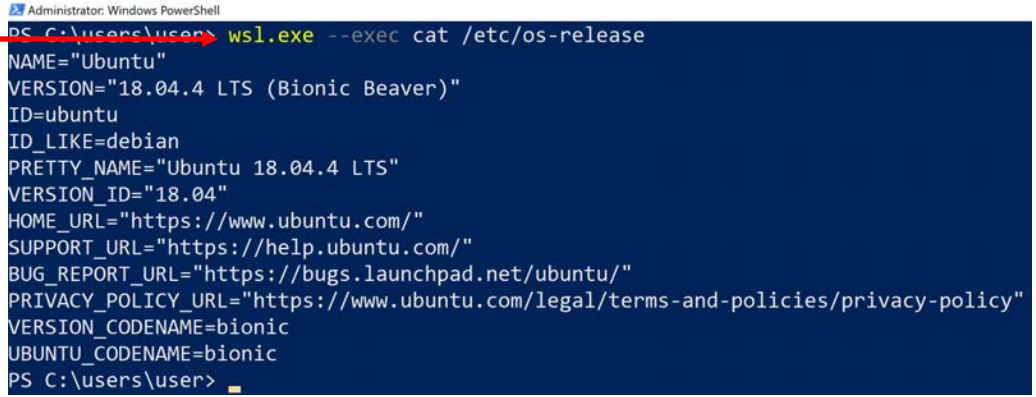


Execution: wsl.exe

Forensic examination on a WSL Endpoint

Execution: wsl.exe

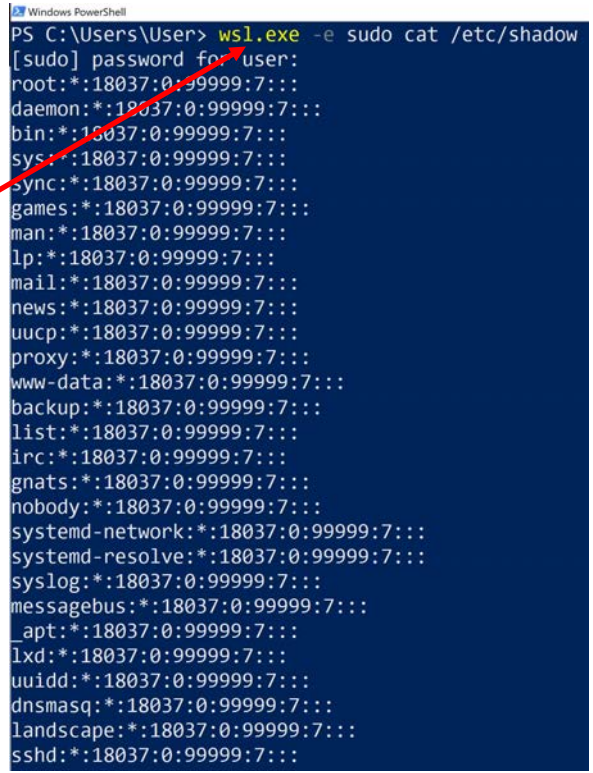
wsl.exe Execution



Forensic examination on a WSL Endpoint

Execution: wsl.exe

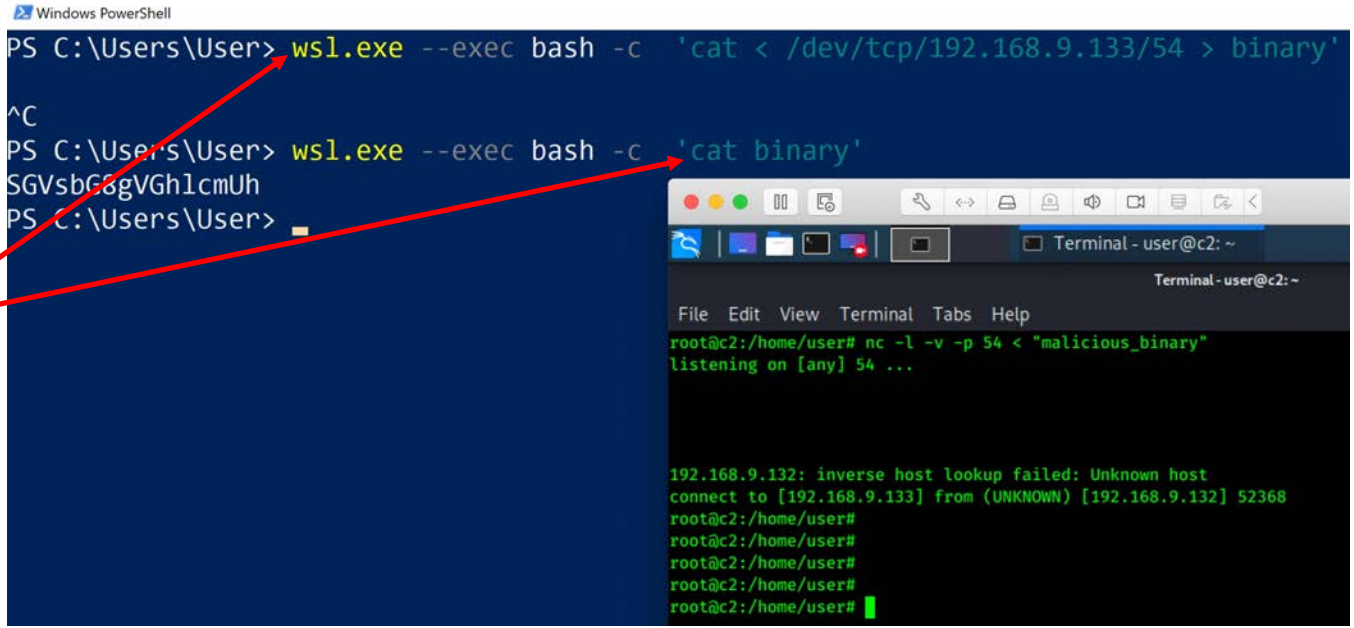
wsl.exe Execution



Forensic examination on a WSL Endpoint

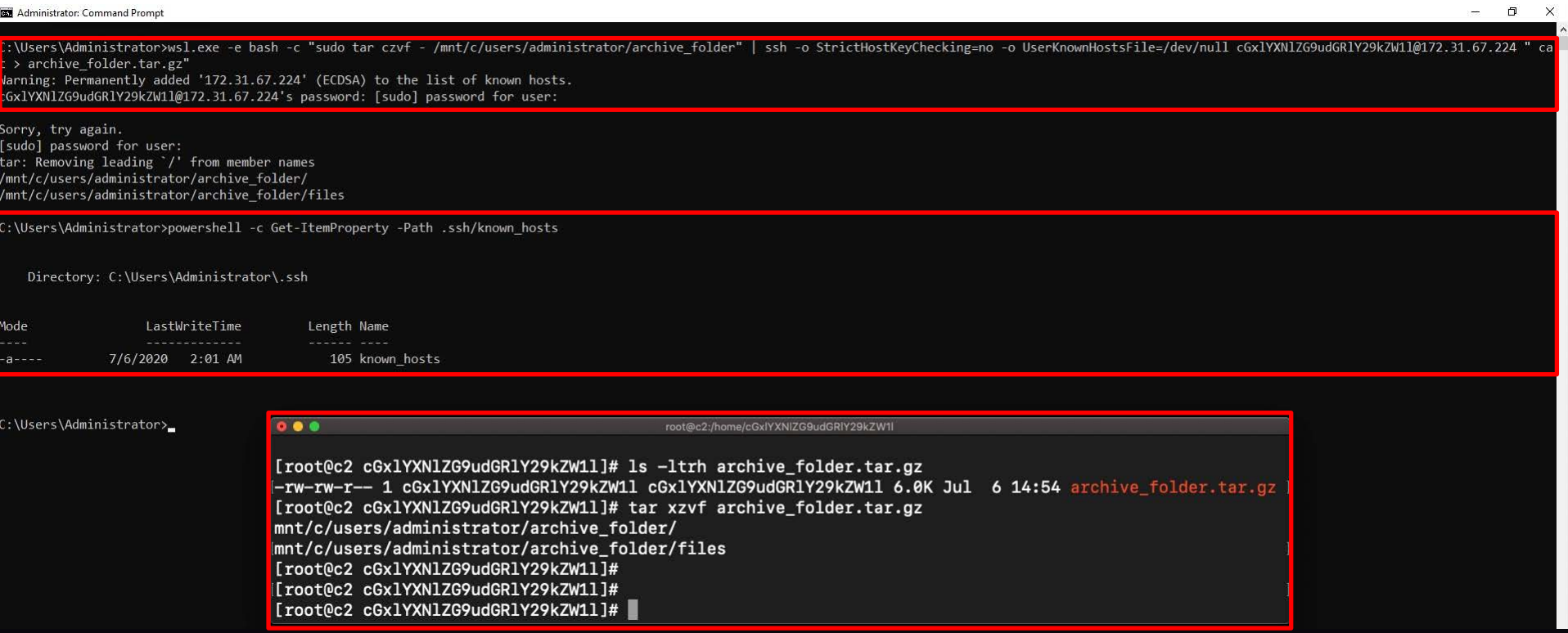
Execution: wsl.exe

wsl.exe Execution



Forensic examination on a WSL Endpoint

Execution: wsl.exe



Forensic examination on a WSL Endpoint

Execution: wsl.exe

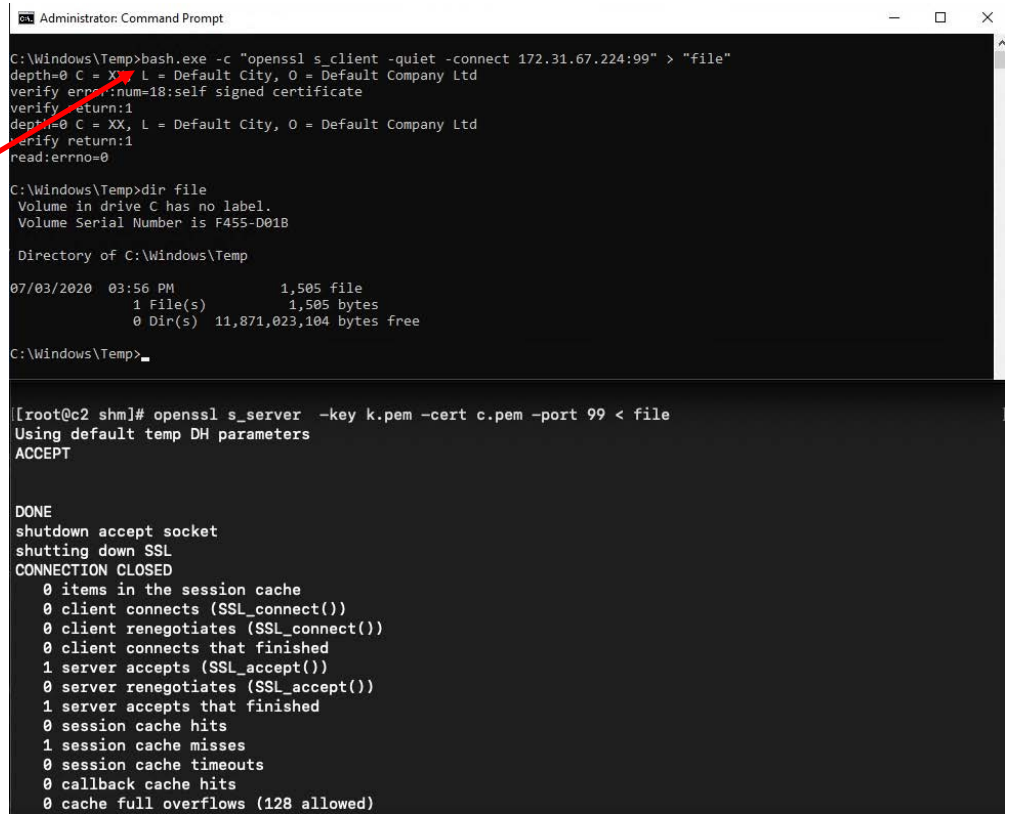
- Process command line activity
- Process lineage
- Caveat:
  - Execution of Linux commands will not be saved in ~/.bash_history, ~/.sh_history, etc,

Execution: bash.exe

Forensic examination on a WSL Endpoint

Execution: bash.exe

bash.exe Execution

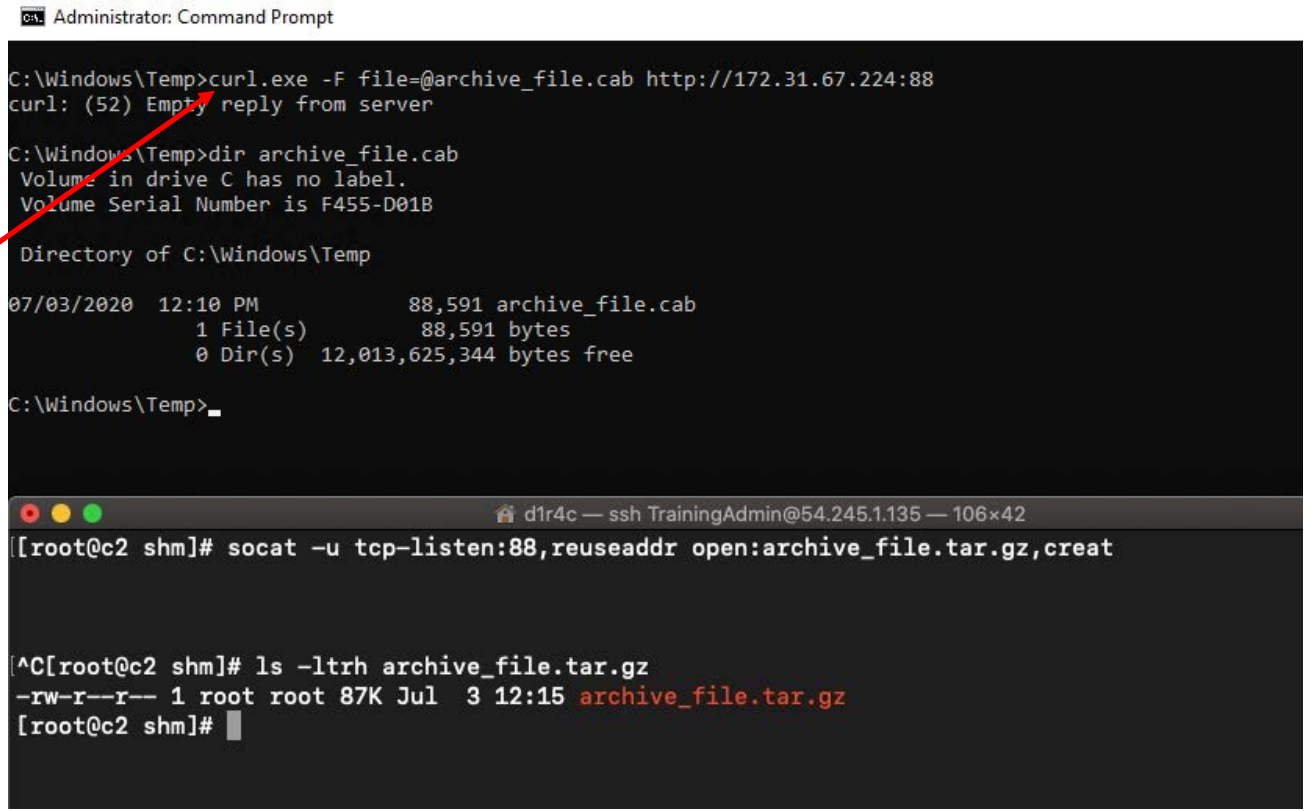


Execution: curl.exe

Forensic examination on a WSL Endpoint

Execution: curl.exe

curl.exe Execution

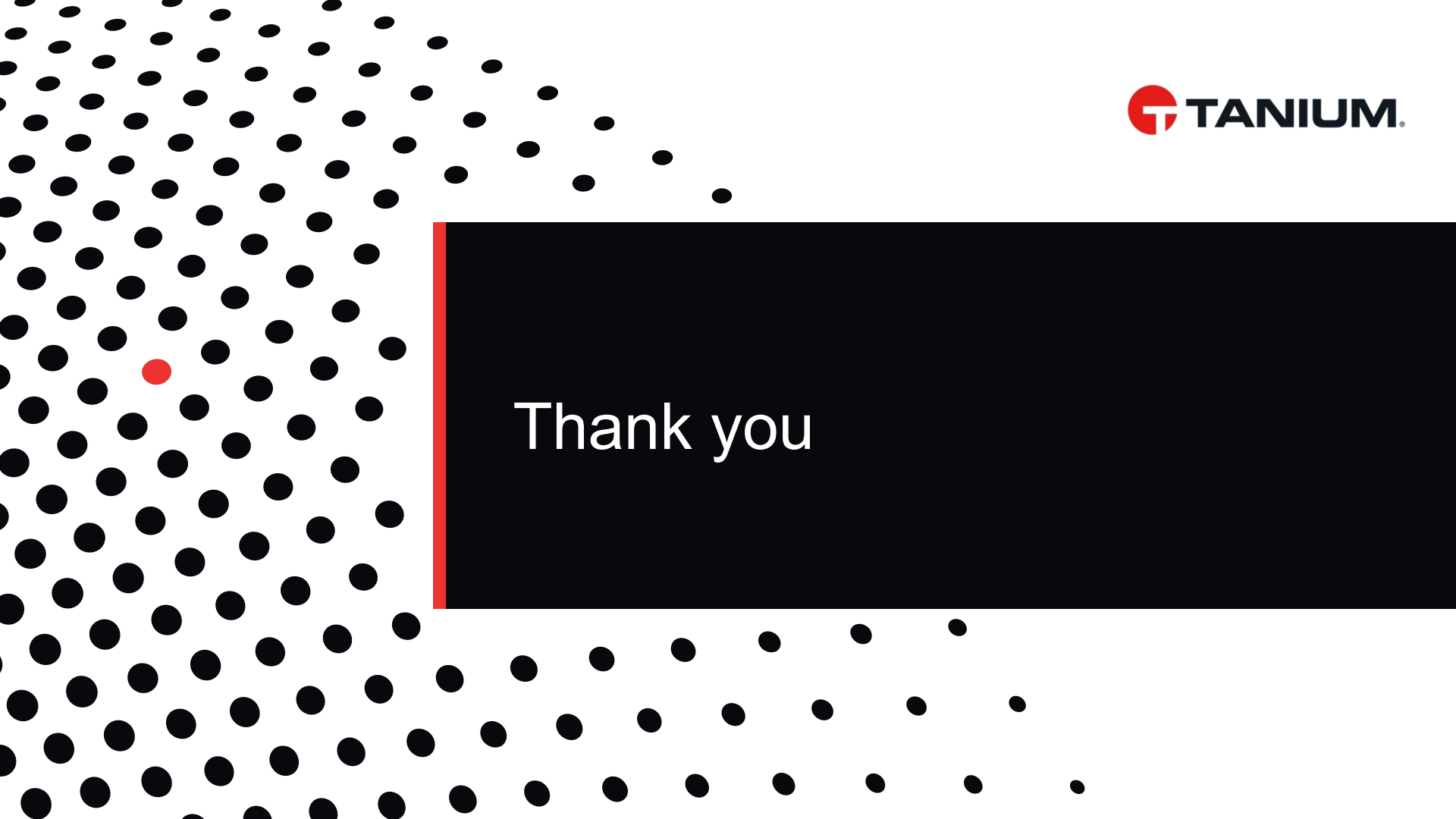


Conclusion

- Adversaries and malware authors will continue to explore attack surfaces on WSL 2, as it becomes more prevalent across enterprise environments
- WSL 2 Endpoints is going to make Digital Forensics and Incident Response professionals lives a lot more interesting
- I highlighted 11 techniques based on my initial research, but I expect there to be more attack surfaces with WSL 2

References

- OSDFCon 2019: Investigating Linux Endpoints
  - https://www.osdfcon.org/presentations/2019/Asif-Matadar_Investigating-Linux-Endpoints.pdf
- https://lolbas-project.github.io/lolbas/OtherMSBinaries/Wsl/
- https://twitter.com/d1r4c/status/1280196218308694016
- https://lolbas-project.github.io/lolbas/Binaries/Bash/
- https://twitter.com/d1r4c/status/1279085773522862082
- https://twitter.com/d1r4c/status/1279042657508081664


TANIUM
Thank you