



**kali-linux-2025.4-virtualbox-amd64**
 Saved

**General**

Name: kali-linux-2025.4-virtualbox-amd64  
Operating System: Debian (64-bit)

**System**

Base Memory: 2048 MB  
Processors: 2  
Boot Order: Hard Disk, Optical  
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization

**Display**

Video Memory: 128 MB  
Graphics Controller: VMSVGA  
Remote Desktop Server: Disabled  
Recording: Disabled

**Storage**

Controller: IDE  
IDE Secondary Device 0: [Optical Drive] VBoxGuestAdditions.iso (61.08 MB)  
Controller: SATA  
SATA Port 0: kali-linux-2025.4-virtualbox-amd64.vdi (Normal, 80.09 GB)

**Audio**

Host Driver: Windows DirectSound  
Controller: ICH AC97

**Network**

Adapter 1: Intel PRO/1000 MT Desktop (NAT)  
Adapter 2: Intel PRO/1000 MT Desktop (Host-only Adapter, 'VirtualBox Host-Only Ethernet Adapter')

**USB**

USB Controller: OHCI  
Device Filters: 0 (0 active)

**Shared folders**

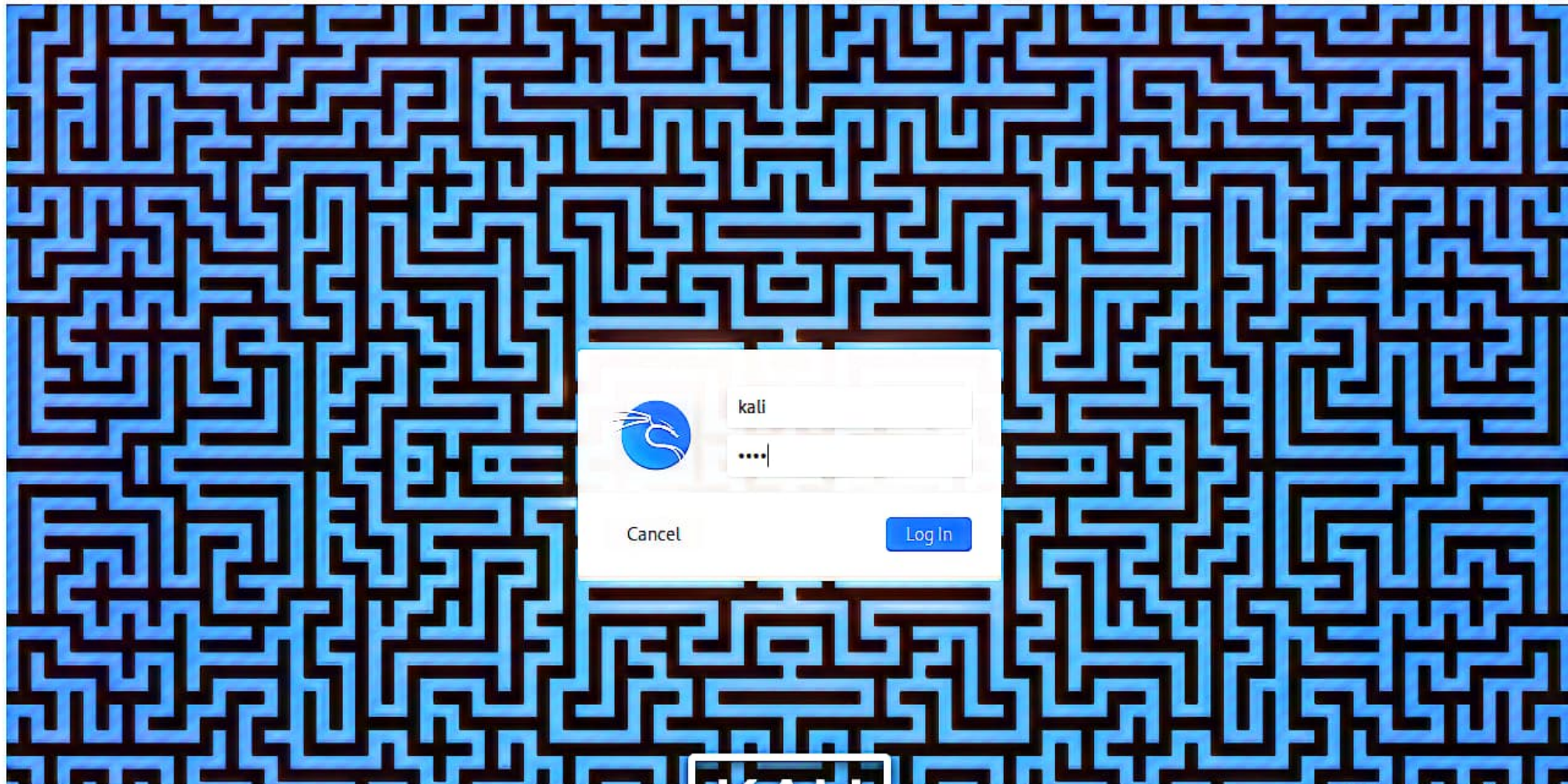
None

**Description**

Kali Rolling (2025.4) x64  
2025-12-03  
-----  
Username: kali  
Password: kali



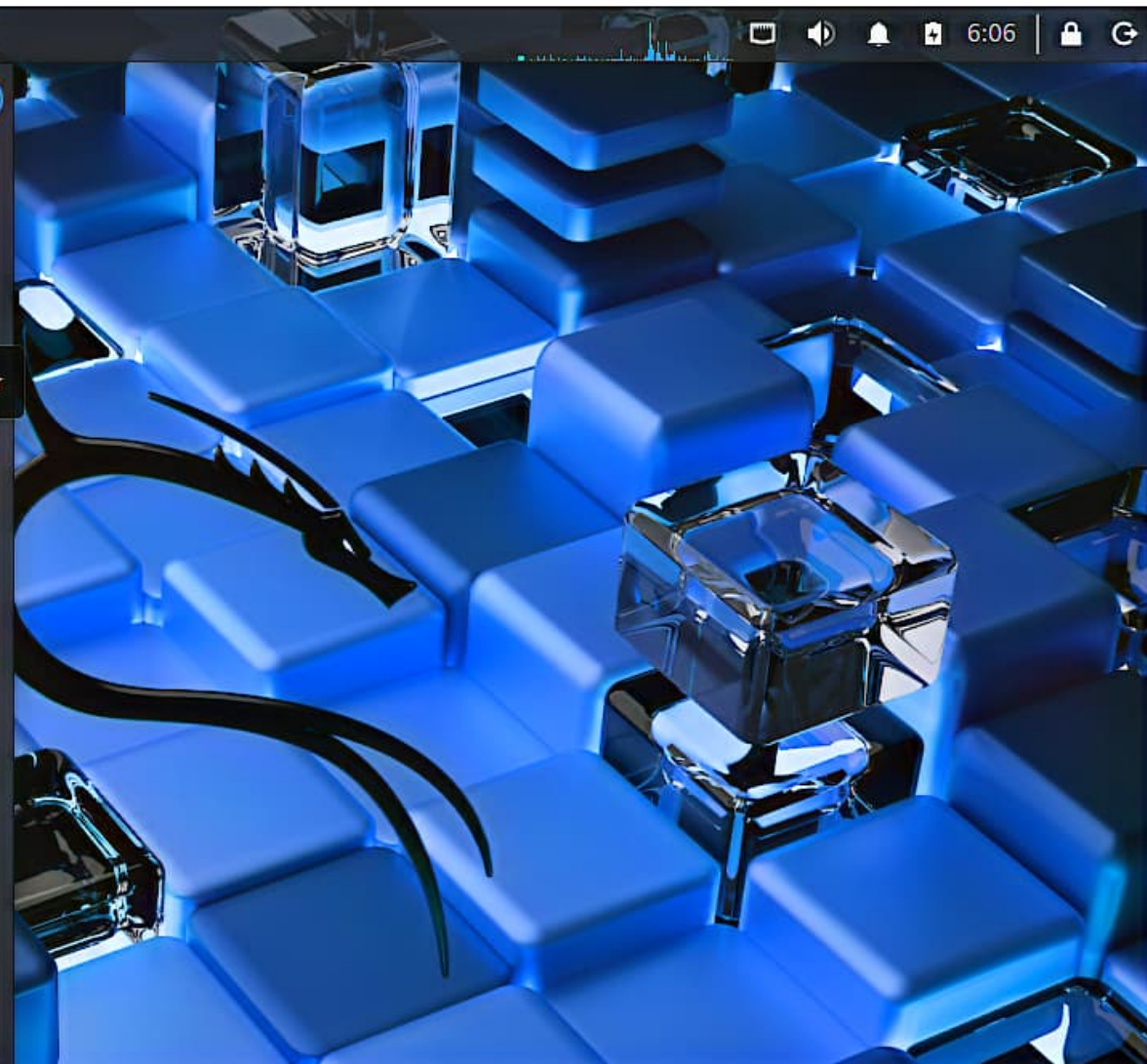
kali

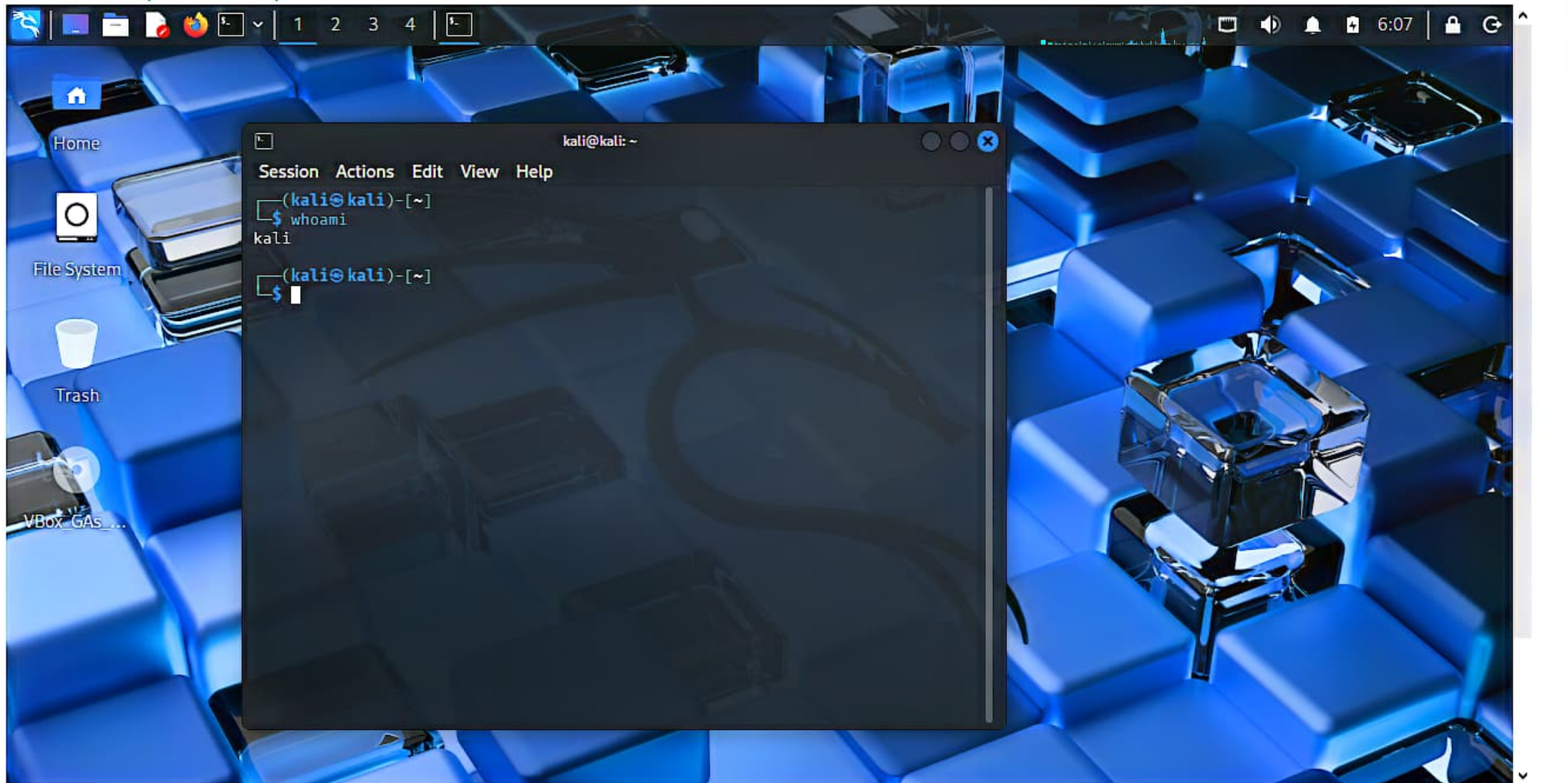




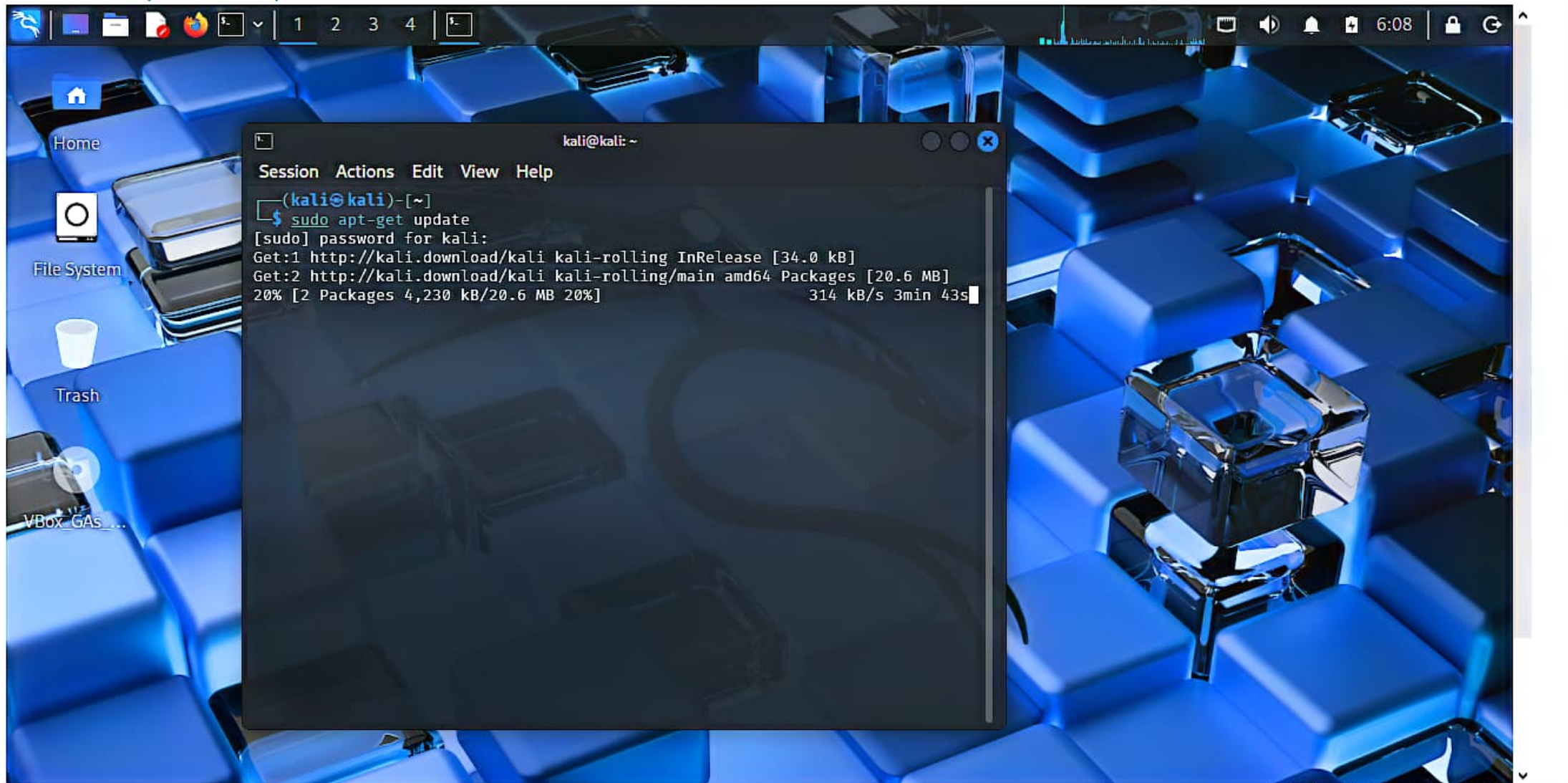


The image shows the left sidebar of the Kali Linux desktop environment. It features a search bar at the top. Below it are several sections: "Favorites" with a star icon, "Recently Used" with a clock icon, "All Applications" with a folder icon, and "Usual Applications" with a grid icon. The "Usual Applications" section contains a list of 15 numbered items: "01 - Reconnaissance", "02 - Resource Development", "03 - Initial Access", "04 - Execution", "05 - Persistence", "06 - Privilege Escalation", "07 - Defense Evasion", "08 - Credential Access", "09 - Discovery", "10 - Lateral Movement", "11 - Collection", "12 - Command and Control", "13 - Exfiltration", "14 - Impact", and "15 - Forensics". To the right of these sections is a list of application icons: "Terminal Emulator", "Root Terminal Emulator", "File Manager", "Text Editor", "Web Browser", "Kali Linux", "Kali Tools", "Kali Docs", "Kali Bugs", "OffSec Training", "Exploit Database", and "VulnHub". A tooltip labeled "Simple Text Editor" is visible over the "Text Editor" icon.









kali@kali: ~

Session Actions Edit View Help

(kali@kali)-[~]

\$ sudo apt-get upgrade

[sudo] password for kali:

Reading package lists ... Done

Building dependency tree ... Done

Reading state information ... Done

Calculating upgrade ... Done

The following packages were automatically installed and are no longer required:

d:

```
bloodhound.py curlftpfs libaudio2 libconfig-inifiles-perl libfuse2t64
libvdpau-va-gl1 mesa-vdpau-drivers python3-aiocache python3-aiomcache
python3-fs python3-wapiti-arsenic python3-yaswfp ruby-unf-ext
vdpau-driver-all
```

Use 'sudo apt autoremove' to remove them.

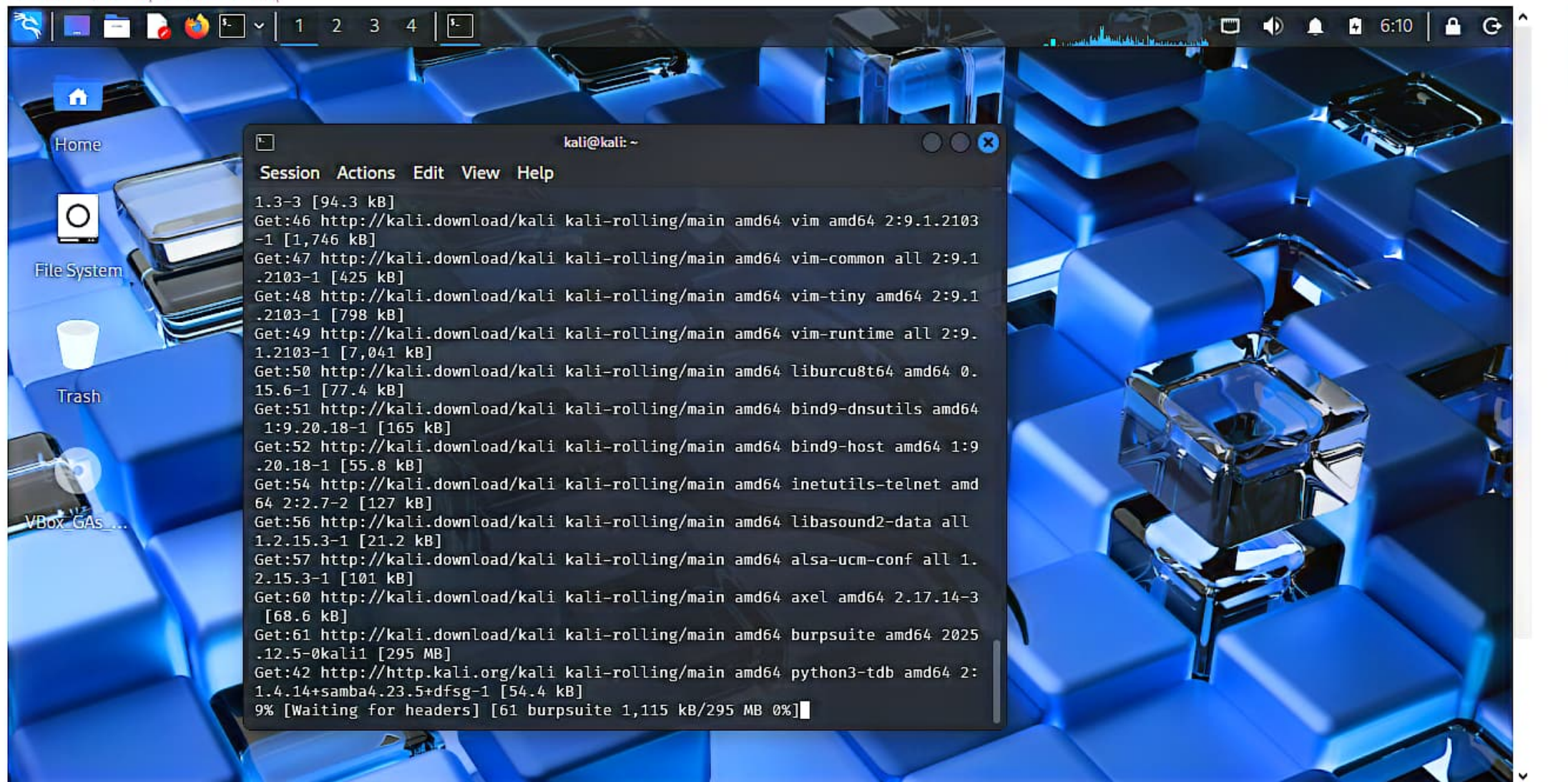
The following packages have been kept back:

```
binutils-mingw-w64-i686 binutils-mingw-w64-x86-64 clang colord
freerdp3-x11 gstreamer1.0-libav gstreamer1.0-plugins-bad
kali-desktop-xfce libavif16 libcolorhug2 libegl-mesa0
libfreerdp-client3-3 libfreerdp3-3 libgbm1 libgl1-mesa-dri libglx-mesa0
libgstreamer-plugins-bad1.0-0 libgtk-3-0t64 libgtk-3-bin libgtk-4-1
libgtk-4-bin libnss-systemd libpam-systemd libqt6multimedia6
libsystemd-shared libsystemd0 libudev1 libvte-2.91-0 libvte-2.91-common
libwinpr3-3 linux-image-amd64 mesa-libgallium mesa-vulkan-drivers
mupdf-tools nodejs patator postgresql-18 postgresql-18-jit
postgresql-client-18 powershell-empire python3-asttokens
python3-pyqtgraph python3-tables-lib sqlitebrowser systemd systemd-sysv
systemd-timesyncd udev
```

The following packages will be upgraded:

```
alsa-ucm-conf apache2 apache2-bin apache2-data apache2-utils apt
apt-utils aspell avahi-daemon avahi-utils axel bind9-dnsutils bind9-host
bind9-libs bsdxtrutils bsduutils burpsuite chromium chromium-common
chromium-sandbox cryptsetup cryptsetup-bin cryptsetup-initramfs
dracut-install eject faraday fdisk firmware-ath9k-htc gcc-mingw-w64-base
gcc-mingw-w64-i686-win32 gcc-mingw-w64-i686-win32-runtime
gcc-mingw-w64-x86-64-win32 gcc-mingw-w64-x86-64-win32-runtime
gsettings-desktop-schemas gnumd gnumd-common imagemagick
```







Shell No. 1

Session Actions Edit View Help

ting system provides version 2.42.

HINT: Rebuild all objects in this database that use the default collation and run ALTER DATABASE postgres REFRESH COLLATION VERSION, or build PostgreSQL with the right library version.

[+] Creating databases 'msf'

WARNING: database "postgres" has a collation version mismatch  
DETAIL: The database was created using collation version 2.41, but the operating system provides version 2.42.

HINT: Rebuild all objects in this database that use the default collation and run ALTER DATABASE postgres REFRESH COLLATION VERSION, or build PostgreSQL with the right library version.

WARNING: database "postgres" has a collation version mismatch  
DETAIL: The database was created using collation version 2.41, but the operating system provides version 2.42.

HINT: Rebuild all objects in this database that use the default collation and run ALTER DATABASE postgres REFRESH COLLATION VERSION, or build PostgreSQL with the right library version.

[+] Creating databases 'msf\_test'

WARNING: database "postgres" has a collation version mismatch  
DETAIL: The database was created using collation version 2.41, but the operating system provides version 2.42.

HINT: Rebuild all objects in this database that use the default collation and run ALTER DATABASE postgres REFRESH COLLATION VERSION, or build PostgreSQL with the right library version.

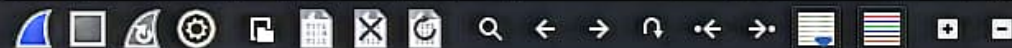
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'

[+] Creating initial database schema

□

The Wireshark Network Analyzer

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



Apply a display filter ... &lt;Ctrl-/&gt;

Welcome to Wireshark

## Capture

...using this filter:  All interfaces s

eth0  
any  
Loopback: lo  
eth1  
bluetooth-monitor  
nflog  
nfqueue  
dbus-system  
dbus-session

## Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord

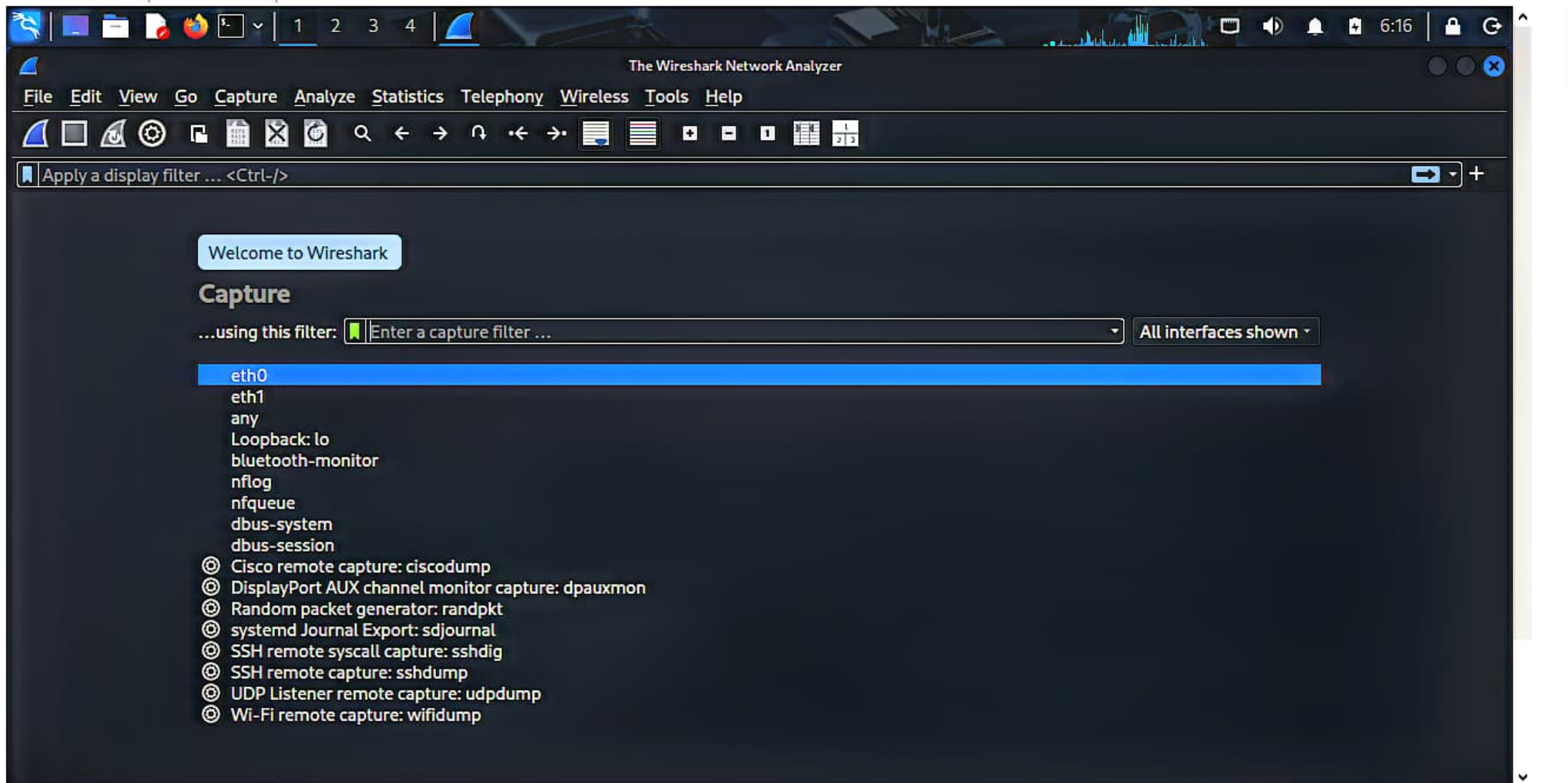
You are running Wireshark 4.6.3.

Ready to load or capture

No Packets

Profile





```
$ /usr/share/kali-menu/helper-scripts/metasploit-framework.sh
[sudo] password for kali:
[i] Database already started
[i] The database appears to be already configured, skipping initialization
Metasploit tip: Enable verbose logging with set VERBOSE true
```

```
      .;lx00K0XXK00xl:.
      ,o@wMMMMMMMMMMMMMMMMMMkd,
      'xNMMMMMMMMMMMMMMMMMMMMMMWx,
      :KMMMMMMMMMMMMMMMMMMMMMMMMMMK:
      .kMMMMMMMMMMMMMMMMMMMMMMMMMMX,
      lWMMMMMMMMMMMMMMXd:.. ..;dKMMMMMMMMMMMo
      xMMMMMMMMMMMMMMWd. .oNMMMMMMMMMMMMMk
      oMMMMMMMMMMx. dMMMMMMMMMMx
      .WMMMMMMMMM: :MMMMMMMMM,
      xMMMMMMMMMo lMMMMMMMMMo
      NMMMMMMMMW ,cccccoMMMMMMMMWlcccc;
      NMMMMMMMMX ;KMMMMMMMMMMMMMMMMMMX:
      NMMMMMMMMW ;KMMMMMMMMMMMMMMMMMMX:
      xMMMMMMMMd ,@MMMMMMMMMK;
      .WMMMMMMMMc 'OMMMMMMO,
      lMMMMMMMMMk .kMMO'
      dMMMMMMMMMMd"
      cWMMMMMMMMMMMMMMNxc".
      .@MMMMMMMMMMMMMMMMMMWc
      ;@MMMMMMMMMMMMMMMMMMo.
      .dNMMMMMMMMMMMMMMo
      'o@WMMMMMMMMMo
      ..cdk00K;

      #####
      #+# #+#
      +:+
      +#+:++#+
      +:+
      :+: :+:
      :+::+:+:
```

Metasploit

```
= [ metasploit v6.4.108-dev ]
+ -- [ 2,598 exploits - 1,322 auxiliary - 1,710 payloads ]
+ -- [ 432 post - 49 encoders - 14 nops - 9 evasion ]
```

Metasploit Documentation: <https://docs.metasploit.com/>  
The Metasploit Framework is a Rapid7 Open Source Project

msf > █