FORTRA

beSTORM
13.1.0

Fuzzing Wi-Fi Devices Guide

Copyright Terms and Conditions

Copyright © Fortra, LLC and its group of companies. All trademarks and registered trademarks are the property of their respective owners.

The content in this document is protected by the Copyright Laws of the United States of America and other countries worldwide. The unauthorized use and/or duplication of this material without express and written permission from Fortra is strictly prohibited. Excerpts and links may be used, provided that full and clear credit is given to Fortra with appropriate and specific direction to the original content.

202308030901

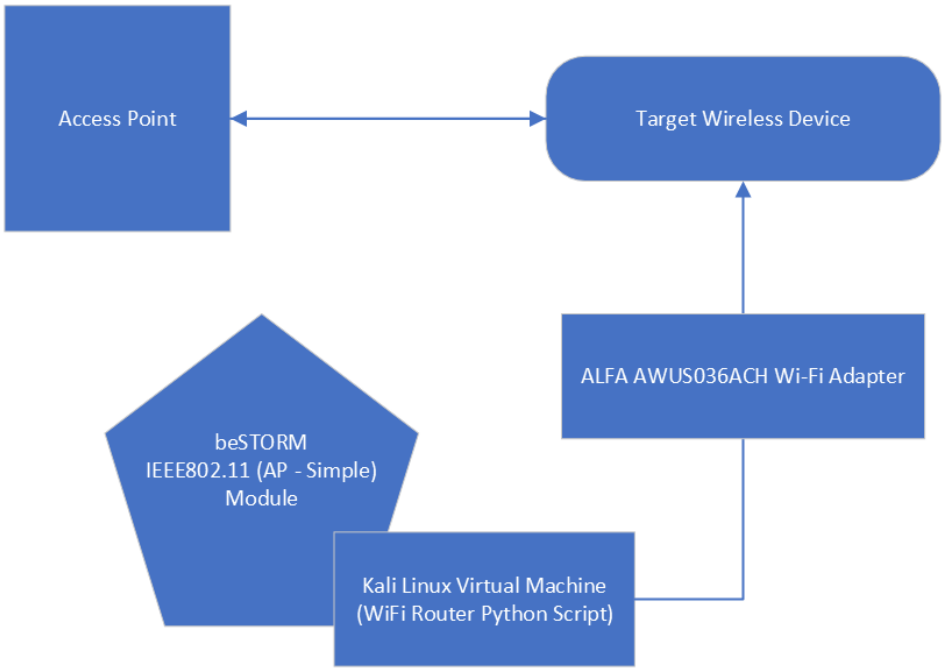
Table of Contents

Overview

To perform Wi-Fi fuzzing with beSTORM, you must install and configure a Kali Linux virtual machine on the computer running beSTORM and purchase and connect the ALFA AWUS036ACH USB Type-C dual-band AC1200 WiFi adapter.

How beSTORM fuzzes Wi-Fi devices

Fuzzing is performed by injecting malformed Wi-Fi packets into an existing communication between a live access point and the target wireless device you want to test. beSTORM uses the IEEE802.11 (AP) module to perform attacks on the target wireless device in a non-encrypted environment (WEP or WPA is not supported).



Hardware & software requirements

The following items are required to set up and perform Wi-Fi fuzzing with beSTORM:

- beSTORM 13.1.0 or later (licensed)
- Windows 10 or later
- VirtualBox 7.0 or later for Windows Hosts
- Kali Linux 2023.2 or later for VirtualBox

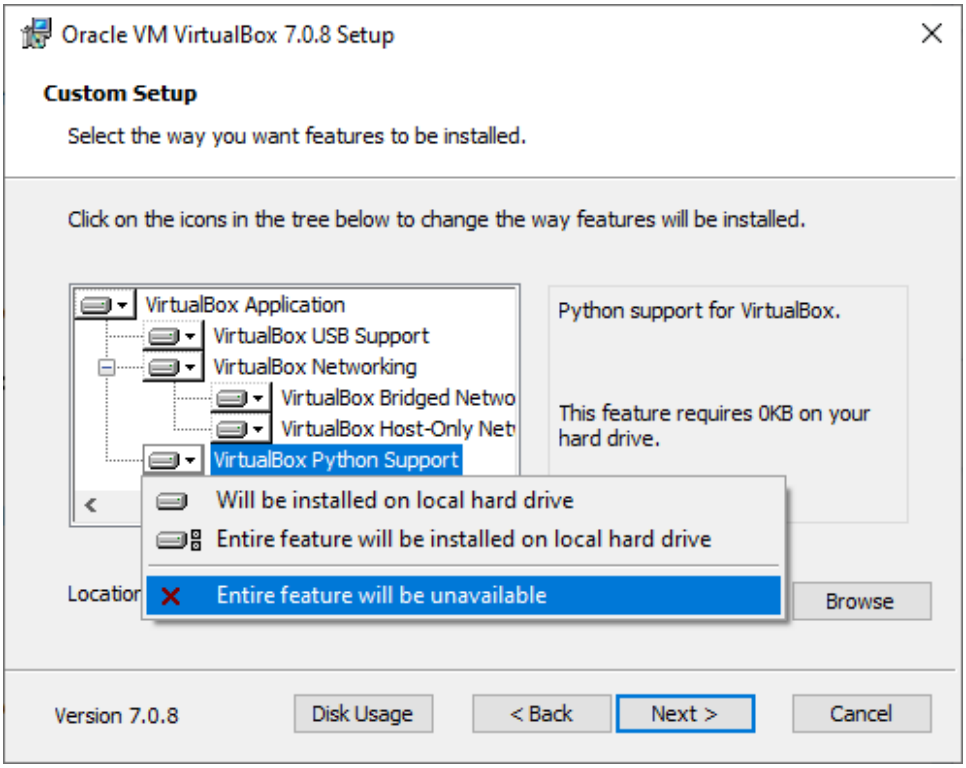
- 7-Zip
- ALFA AWUS036ACH USB Type-C dual-band AC1200 WiFi adapter

Install and Configure the Kali Linux Virtual Machine

Follow these steps to install and configure a Kali Linux virtual machine on the computer running beSTORM:

Install Oracle VM VirtualBox

1. Go to virtualbox.org/wiki/Downloads.
2. Download the **Windows hosts** version of VirtualBox.
3. Right-click the VirtualBox installer file, and then select **Run as administrator**. The VirtualBox setup wizard opens.
4. On the **Welcome** page, select **Next**.
5. On the **Custom Setup** page, select **VirtualBox Python Support**, and then select **Entire feature will be unavailable**.



6. Select **Next**, and then continue through the rest of the setup wizard to finish the installation process.

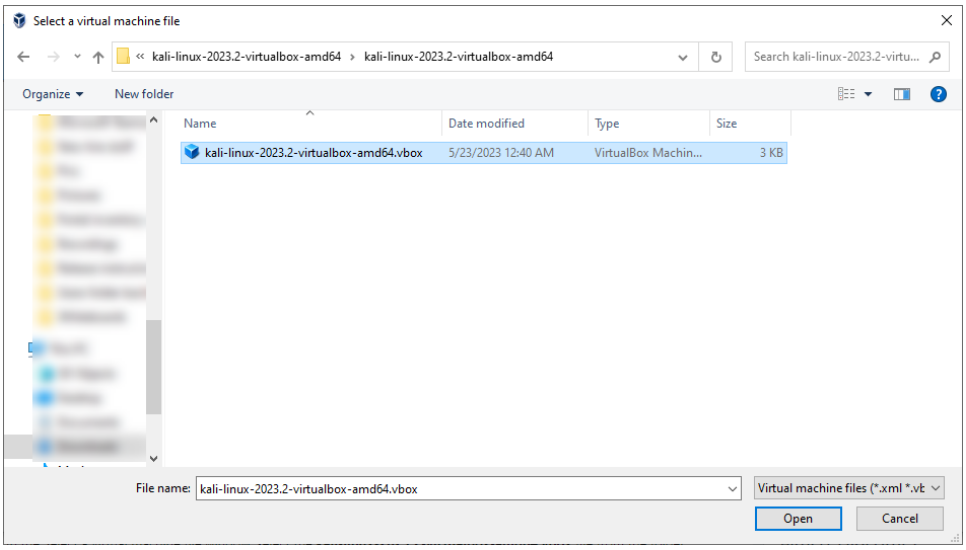
Install 7-Zip

1. Go to 7-zip.org.
2. Download and install the latest version of 7-Zip.

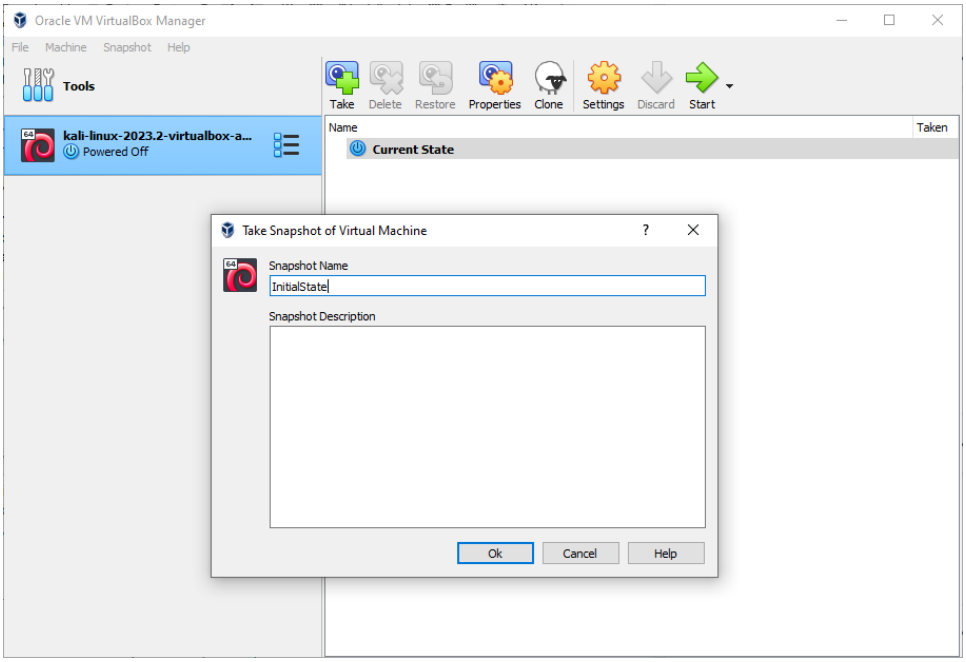
Create and configure the Kali Linux virtual machine

1. Go to kali.org/get-kali.
2. Select **Virtual Machines**.
3. Download the version of **VirtualBox** that corresponds with your version of Windows (this guide uses the 64-bit version).
4. Right-click the **kali-linux virtualbox** file, and then select **7-Zip** > **Extract files**.
5. On the Extract dialog, enter the desired file path. Leave all other options to their default setting.
6. Select **OK** to extract the files. The extracted folder should contain the following files:

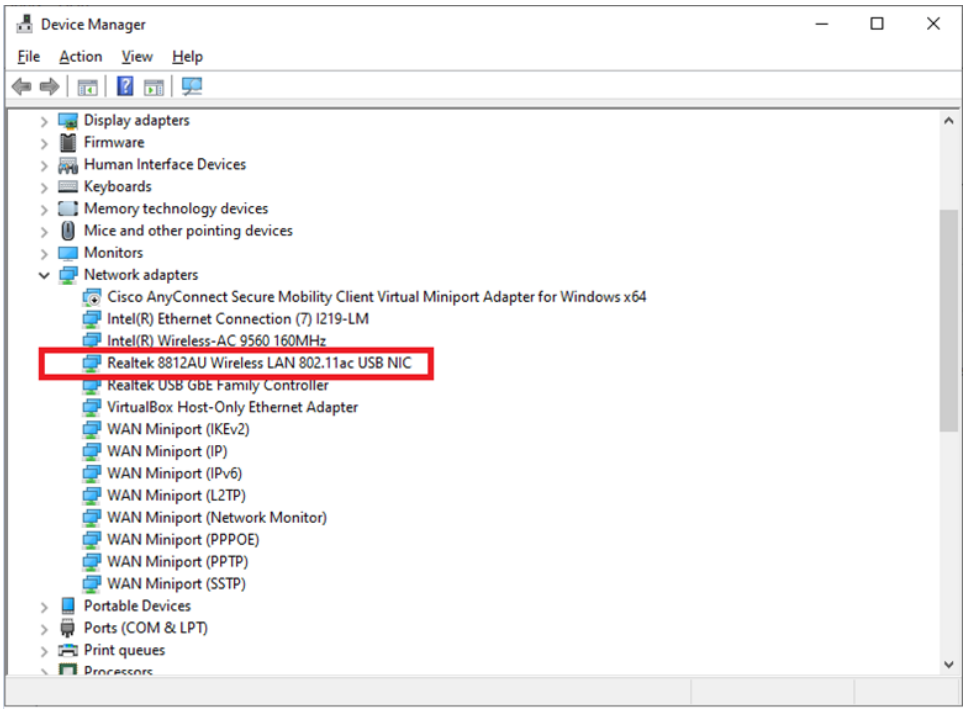
7. Open **Oracle VMVirtualBox**.
8. Select **Machine** > **Add**.
9. In the **Select a virtual machine file** window, select the **kali-linux-2023.2-virtualbox-amd64.vbox** file from the folder you extracted in step 6.



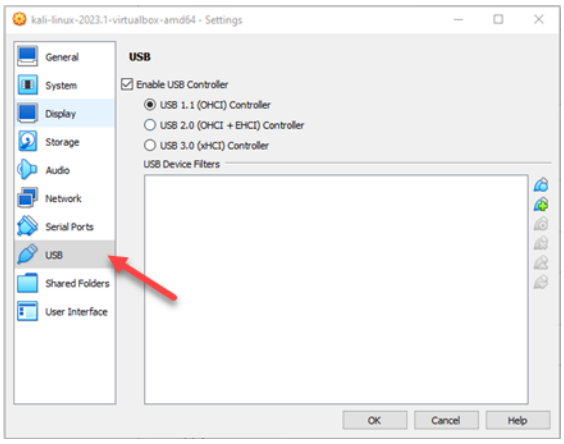
10. Select **Open**. The Kali Linux virtual machine is added to the Oracle VM VirtualBox Manager.
11. From the top of the Oracle VM VirtualBox Manager, select **Machine** > **Tools** > **Snapshots**.
12. Select **Take**, and then enter a name for the snapshot (for example, "InitialSetup"). This creates a snapshot of your Kali Linux virtual machine in the event you need to restore it to its initial state.



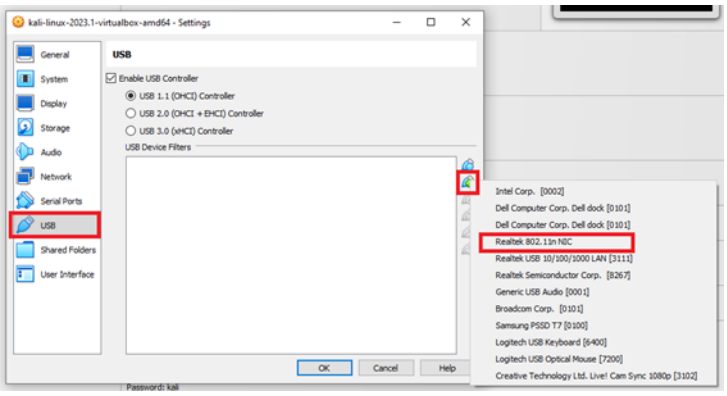
13. Select **OK**.
14. Connect the **AWUS036ACH Wi-Fi adapter** to the beSTORM computer using the provided USB cable.
15. After Windows finishes installing the adapter, confirm **Realtek 8812AU Wireless LAN 802.11ac USB NIC** appears in the Device Manager.



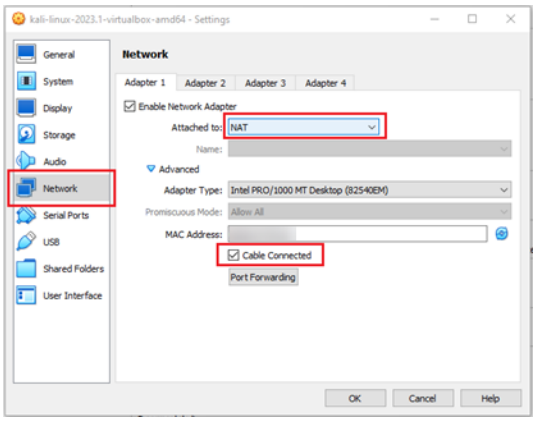
16. From the top of the Oracle VM VirtualBox Manager, select **Machine** > **Settings**.
17. From the left pane, select **USB**.



18. Select the **Adds new USB filter with all fields set to the values of the selected USB device attached to the host PC** button, and then select **Realtek 802.11n NIC**.



19. From the left pane, select **Network**.
20. On the **Adapter 1** tab, select **NAT** from the **Attached to** box.
21. Expand the **Advanced** section, and then select the **Cable Connected** checkbox.

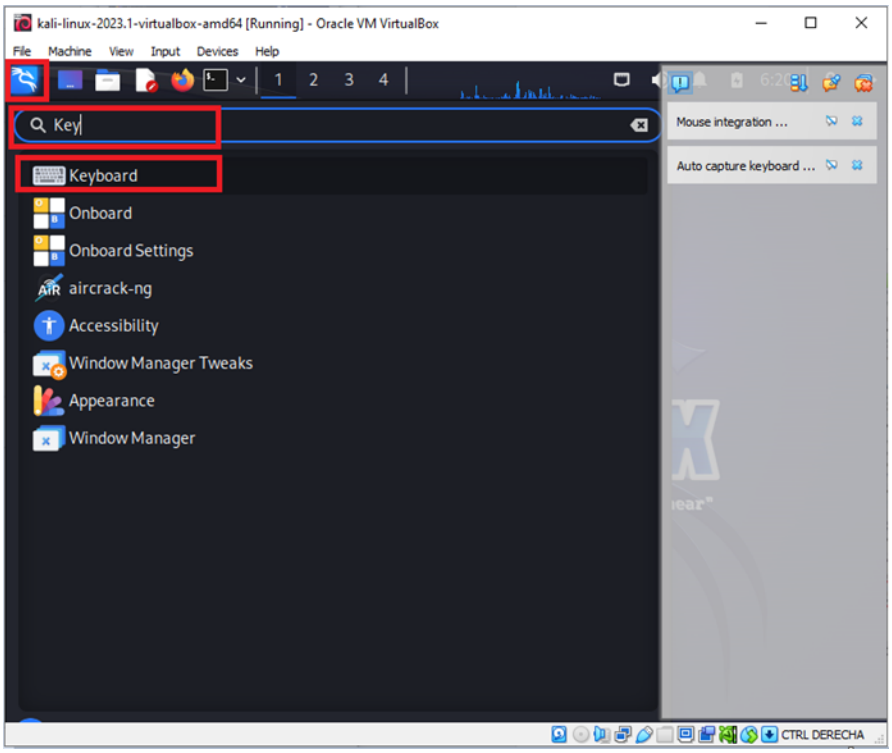


22. Select **OK**.
23. From the top of the Oracle VM VirtualBox Manager, select **Start**. The Kali Linux virtual machine will start booting up.
24. On the Kali log in screen, enter **kali** in both boxes (default username and password), and then select **Log In**.

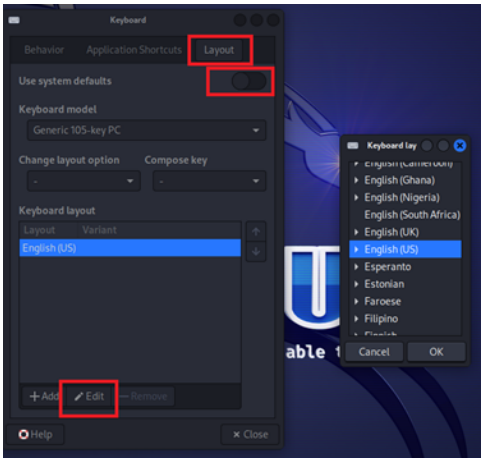
Change the keyboard layout in Kali Linux (optional)

If you need to change your keyboard layout after logging in to Kali Linux, do the following:

1. From the top of the Kali desktop, select the **Applications** icon.
2. In the search bar, enter **keyboard**.



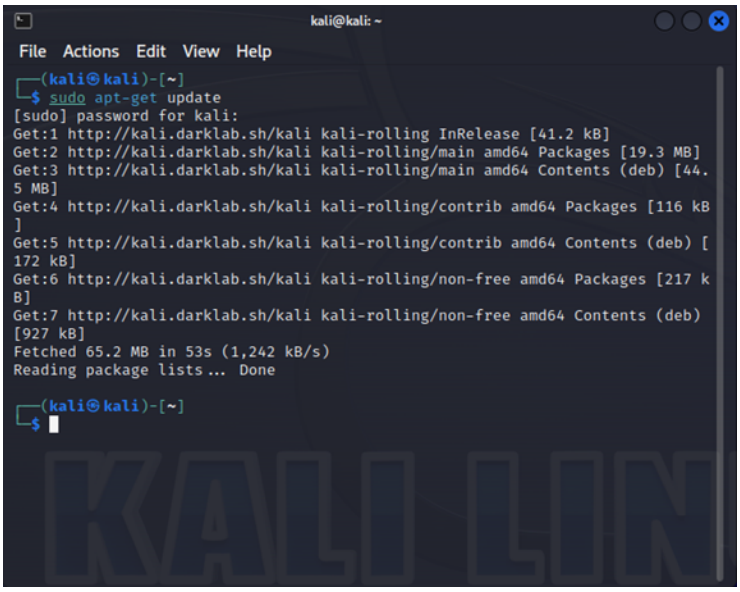
3. Select **Layout**.
4. Disable **Use system defaults**.
5. Select **Edit**, and then select the desired keyboard layout.



Install the AWUS036ACH Wi-Fi adapter drivers for Kali Linux

1. From the top of the Kali Linux desktop, select the **Applications** icon > **Terminal Emulator**.
2. In the Terminal Emulator window, run the following command to update Kali Linux:

```
sudo apt-get update
```



3. Run the following command to install the linux-headers package (prerequisite for the drivers):

```
sudo apt install -y linux-headers-$(uname -r)
```

> **NOTE:** If the "Couldn't find any package by..." error appears while installing the linux-headers package, see ***Install any missing packages* on page 10**.

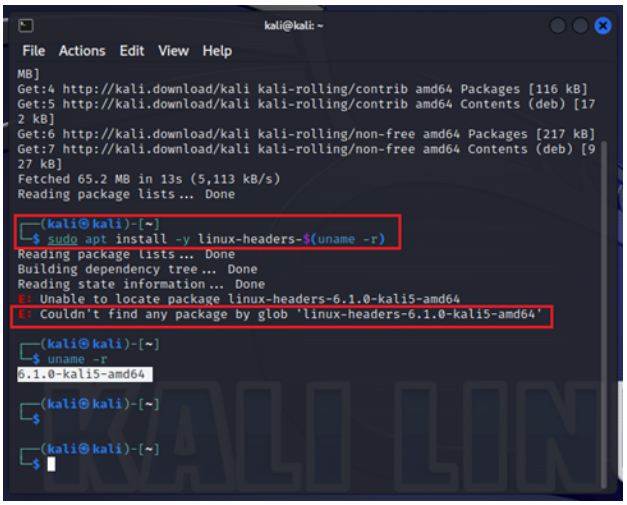
4. Run the following command to install the Linux drivers:

```
sudo apt install realtek-rtl88xxau-dkms
```

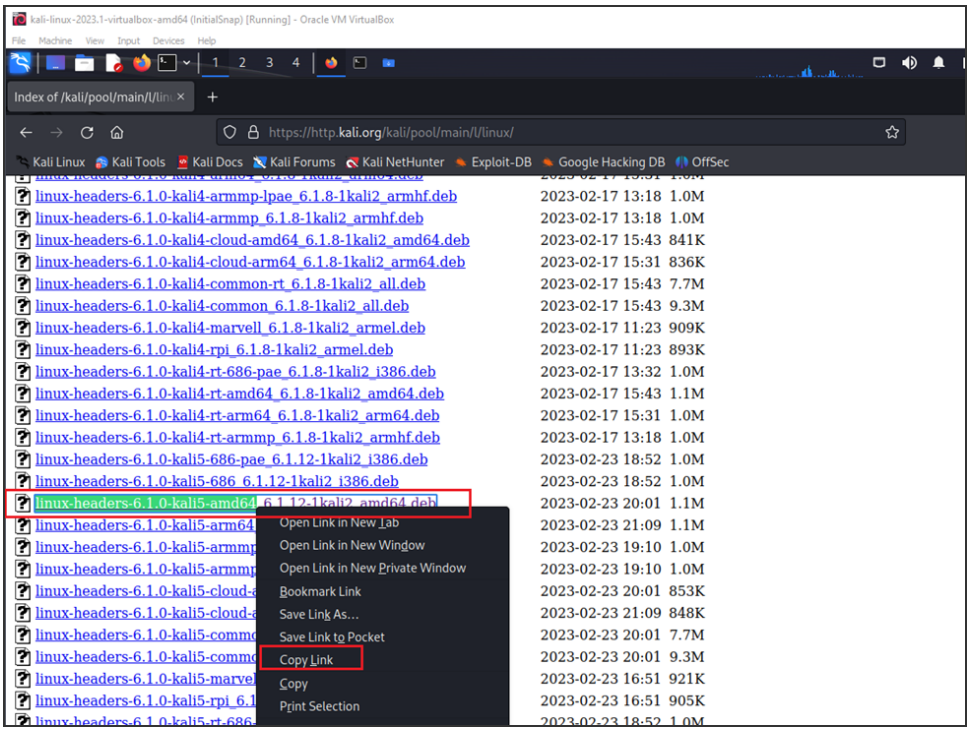
5. When prompted, enter **y** to continue.

Install any missing packages

If the "Couldn't find any package by..." error appears while installing the linux-headers package, do the following:

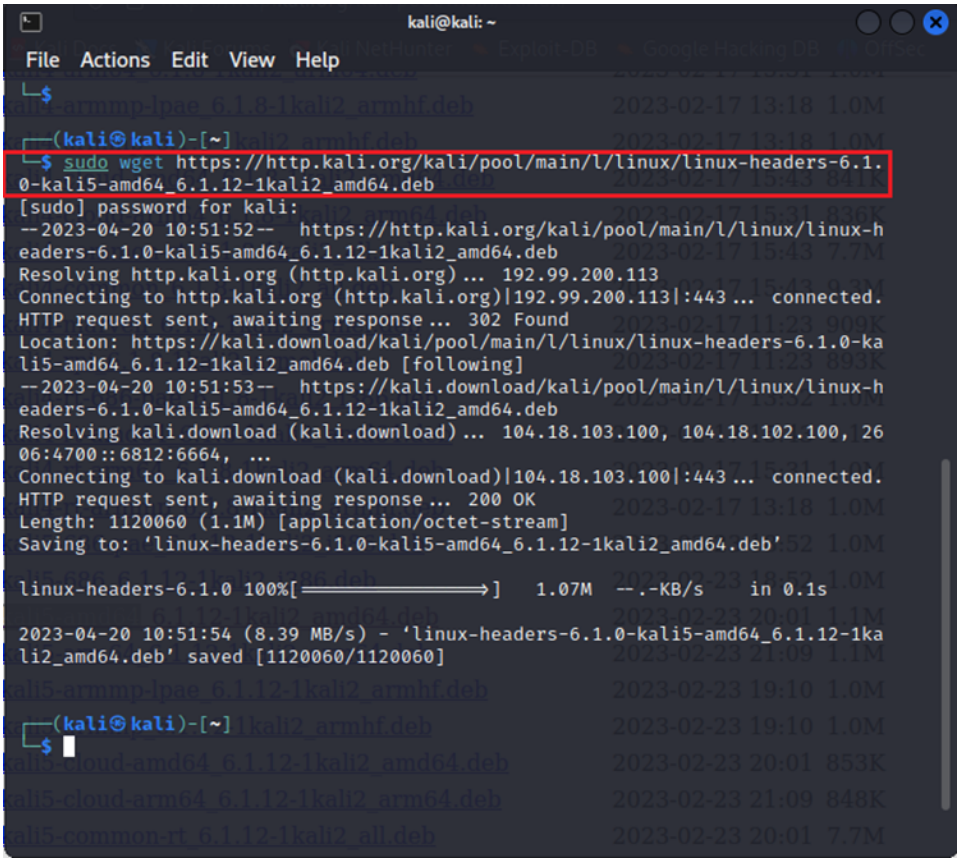


1. Make note of the missing package's name.
2. From the top of the Kali Linux desktop, select the **Applications** icon > **Web Browser**.
3. Go to **https://http.kali.org/kali/pool/main/l/linux/**, and then search for the package's name.
4. Right-click the package's link, and then select **Copy Link**.



5. Open the **Terminal Emulator**.
6. Enter `sudo wget`, and then after the command text, right-click and select **Paste Link**.

7. Run the command.



8. Enter `sudo dpkg -i`, and then after the command text, right-click and select **Paste Link**.
9. Run the command.

> **NOTE:** If you see dependency problems in the Terminal Emulator after running the `sudo dpkg -i` command, see ***Install any missing dependencies* on page 12**.

Install any missing dependencies

If you see the "dependency problems" error in the Terminal Emulator after running the `sudo dpkg -i` command, you must search for and install the missing dependencies before retrying the command. To install each missing dependency, repeat steps 3-9 from ***Install any missing packages* on page 10**.

In this example, there are three dependencies missing:

```
kali@kali: ~
File  Actions  Edit  View  Help
linux-headers-6.1.0 100%[===================>]   1.07M  --.-KB/s    in 0.1s
2023-04-20 10:51:54 (8.39 MB/s) - 'linux-headers-6.1.0-kali5-amd64_6.1.12-1ka
li2_amd64.deb' saved [1120060/1120060]

┌──(kali㉿kali)-[~]
└─$ ls
Desktop    Downloads                                                  Music   Public   Videos
Documents  linux-headers-6.1.0-kali5-amd64_6.1.12-1kali2_amd64.deb    Pictures  Templates

┌──(kali㉿kali)-[~]
└─$ sudo dpkg -i linux-headers-6.1.0-kali5-amd64_6.1.12-1kali2_amd64.deb
Selecting previously unselected package linux-headers-6.1.0-kali5-amd64.
(Reading database ... 392545 files and directories currently installed.)
Preparing to unpack linux-headers-6.1.0-kali5-amd64_6.1.12-1kali2_amd64.deb ...
Unpacking linux-headers-6.1.0-kali5-amd64 (6.1.12-1kali2) ...
dpkg: dependency problems prevent configuration of linux-headers-6.1.0-kali5-amd64:
 linux-headers-6.1.0-kali5-amd64 depends on linux-headers-6.1.0-kali5-common (= 6.1.12-1kali2); however:
  Package linux-headers-6.1.0-kali5-common is not installed.
 linux-headers-6.1.0-kali5-amd64 depends on linux-kbuild-6.1 (≥ 6.1.12-1kali2); however:
  Package linux-kbuild-6.1 is not installed.
 linux-headers-6.1.0-kali5-amd64 depends on linux-compiler-gcc-12-x86; however:
  Package linux-compiler-gcc-12-x86 is not installed.

dpkg: error processing package linux-headers-6.1.0-kali5-amd64 (--install):
 dependency problems - leaving unconfigured
Errors were encountered while processing:
 linux-headers-6.1.0-kali5-amd64

┌──(kali㉿kali)-[~]
└─$
```

When copying dependencies, note the following:

- If you are missing a linux-headers common dependency, copy the version without "-rt" in its name.

linux-headers-6.1.0-kali5-common-rt_6.1.12-1kali2_all.deb	2023-02-23 20:01	7.7M
linux-headers-6.1.0-kali5-common_6.1.12-1kali2_all.deb	2023-02-23 20:01	9.3M
linux-headers-6.1.0-kali5-marvell_6.1.12-1kali2_armel.deb	2023-02-23 16:51	921K

- If you are missing a linux-kbuild dependency, copy the version that includes the same version number in the original missing package's file name. For example, in ***Install any missing packages* on page 10**, the missing package's file name is "linux-headers-6.1.0-kali5-amd64_6.1.12-1kali2_amd64.deb." The corresponding missing dependency is "linux-kbuild-6.1_6.1.12-1kali2_amd64.deb."

linux-kbuild-6.1-dbgsym_6.1.20-2kali1_armhf.deb	2023-04-18 15:49	1.0M
linux-kbuild-6.1-dbgsym_6.1.20-2kali1_i386.deb	2023-04-18 14:51	952K
linux-kbuild-6.1_6.1.12-1kali2_amd64.deb	2023-02-23 20:01	829K
linux-kbuild-6.1_6.1.12-1kali2_arm64.deb	2023-02-23 21:09	818K
linux-kbuild-6.1_6.1.12-1kali2_armel.deb	2023-02-23 16:51	806K

Once you have copied and installed the missing dependencies, execute the following command to install the Linux drivers for the AWUS036ACH Wi-Fi adapter:

```
sudo apt install realtek-rtl88xxau-dkms
```

When prompted, enter **y** to continue.

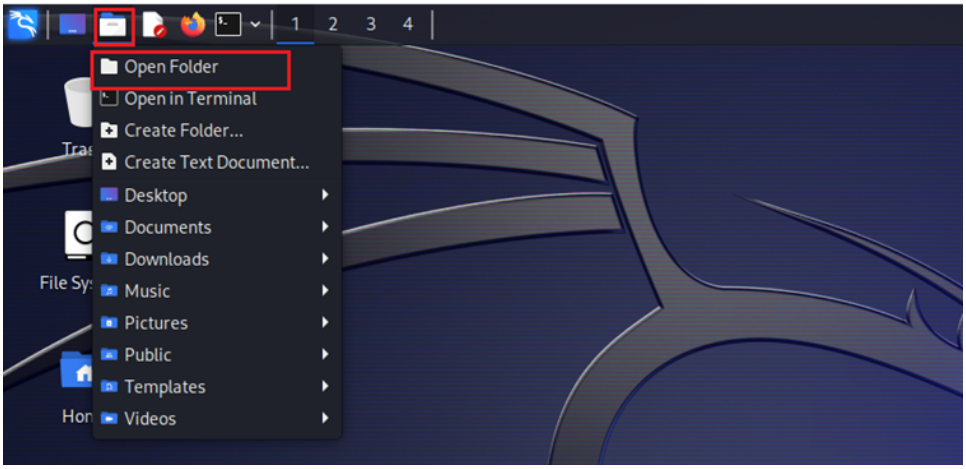
Install hexinject

In the Terminal Emulator, run the following command to install hexinject:

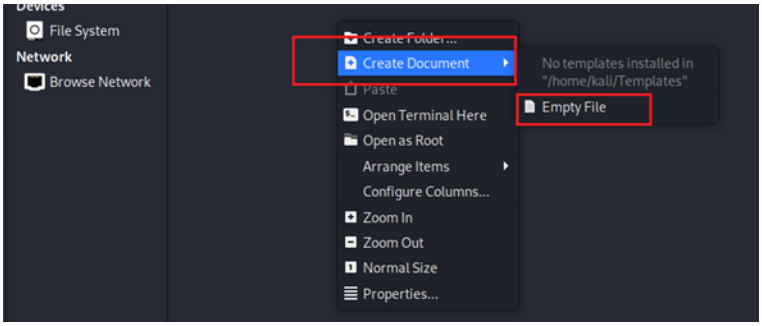
```
sudo apt install hexinject
```

Create the Wi-Fi router Python script

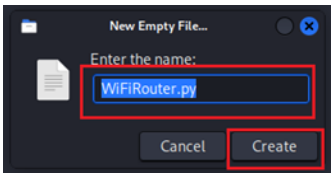
1. From the top of the Kali Linux desktop, select the folder icon > **Open Folder**.



2. Right-click within the folder, and then select **Create Document** > **Empty File**.

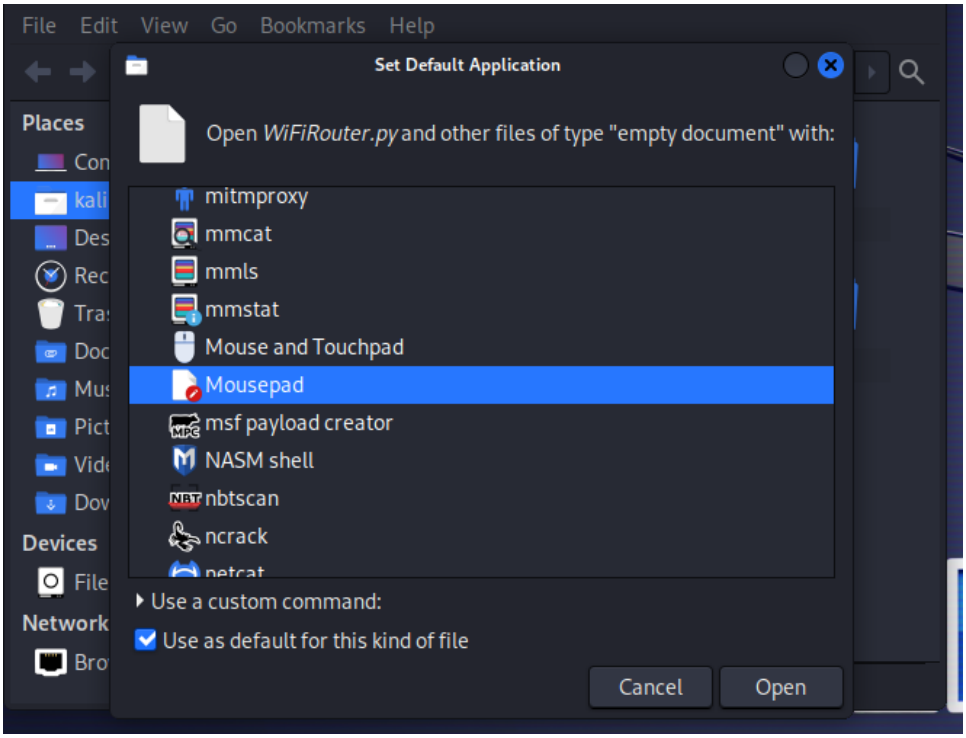


3. In the **Enter the name** box, enter **WiFiRouter.py**.

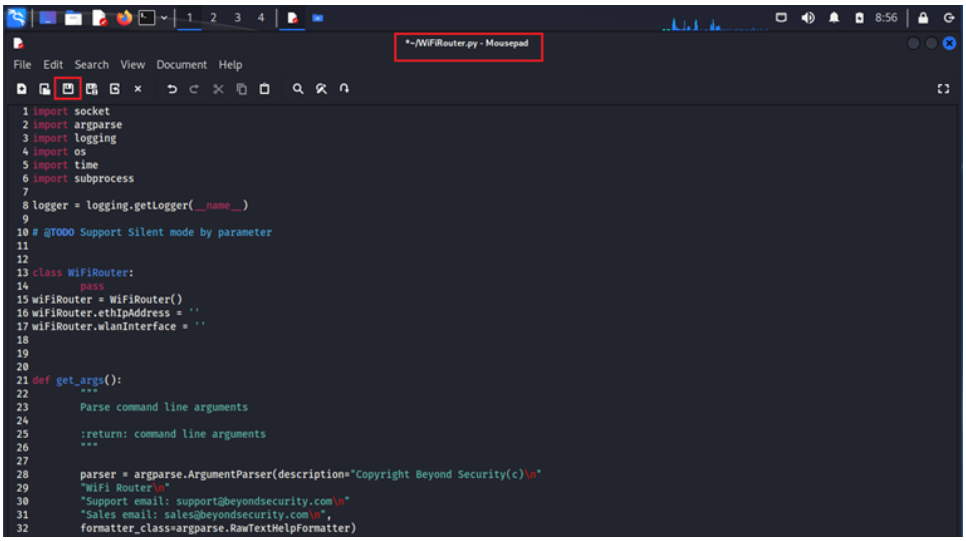


4. Select **Create**.
5. Double-click the **WiFiRouter.py**file.

> **NOTE:** If you need to set a default application, select **Mousepad**, and then select **Open**.



6. In Windows, open the **beSTORM** folder (C:\Program Files (x86)\beSTORM).
7. Using Notepad, open the **WiFiRouter.py** file.
8. Select **Edit** > **Select All**.
9. Select **Edit** > **Copy**.
10. In Kali Linux, right-click in the open WiFiRouter.py file window, and then select **Paste**.

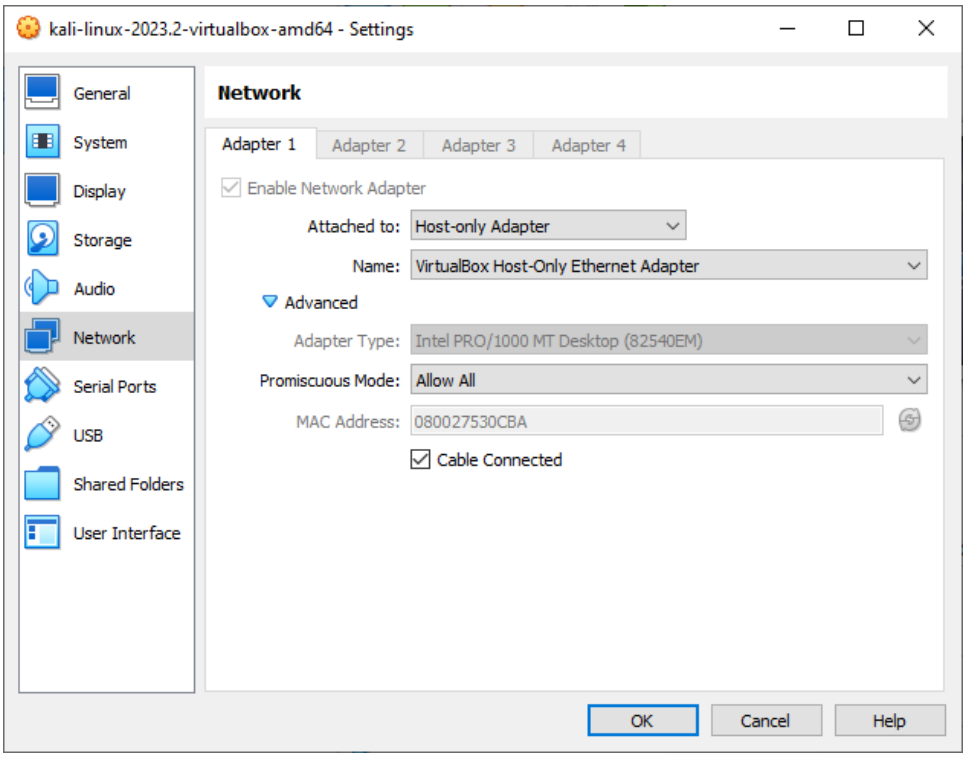


11. Select **File** > **Save**.
12. Close the Kali Linux WiFiRouter.py file.
13. In Windows, close the beSTORM WiFiRouter.py without saving (if prompted).

Update the network adapter settings

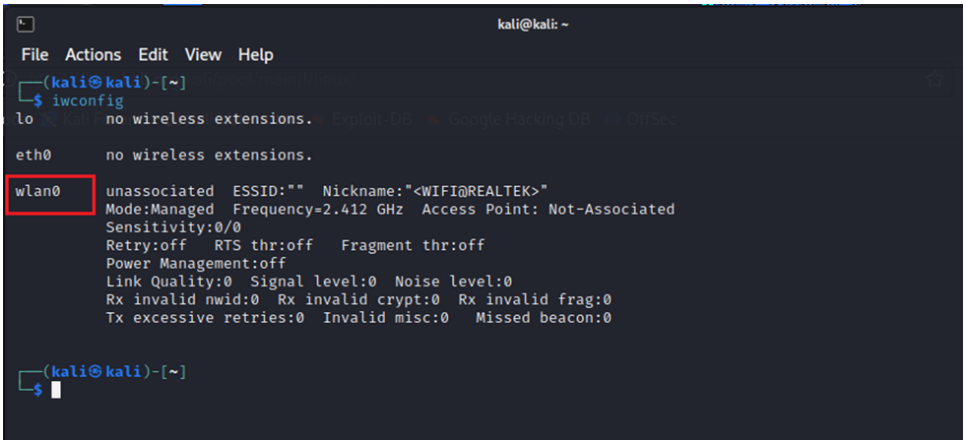
After installing the Linux drivers for the AWUS036ACH Wi-Fi adapter, do the following:

1. Close Kali Linux virtual machine window.
2. On the Close Virtual Machine dialog, select **Save machine state**.
3. From the top of the Oracle VM VirtualBox Manager, select **Machine** > **Settings**.
4. From the left pane, select **Network**.
5. On the **Adapter 1** tab, update these settings to the following:
    a. **Attached to** - Host-only Adapter
    b. **Name** - VirtualBox Host-Only Ethernet Adapter
    c. Advanced
        i. **Promiscuous Mode** - Allow All
        ii. **Cable Connected** - Selected



6. Select **OK**.
7. From the top of the Oracle VM VirtualBox Manager, select **Machine** > **Start** > **Normal Start**.
8. Log in to Kali Linux.
9. In the Terminal Emulator, enter and run the following command to verify the AWUS036ACH Wi-Fi adapter is recognized in Kali Linux:

```
iwconfig
```



10. Disconnect the **AWUS036ACH Wi-Fi adapter** from the beSTORM computer (you will reconnect the adapter in ***Start the Wi-Fi router Python script* on page 19**.

Fuzzing Your Target Wireless Device

Follow these steps to fuzz your target wireless device with beSTORM using the Kali Linux virtual machine and AWUS036ACH Wi-Fi adapter:

Set up an access point

Set up an access point on an open network (disable WEP or WPA encryption). Internet access is not required. Take note of the SSID (Name of the access point) and the channel in use by the access point.

To test the access point, connect to it from the computer running beSTORM, and then ping the IP address of the access point. To ping an IP address in Windows, do the following:

1. In the Windows search bar, enter **cmd**.
2. Select **Command Prompt** from the search results.
3. In the Command Prompt window, enter **ping**, followed by the IP address of the access point.

   EXAMPLE: `ping 192.168.0.0`

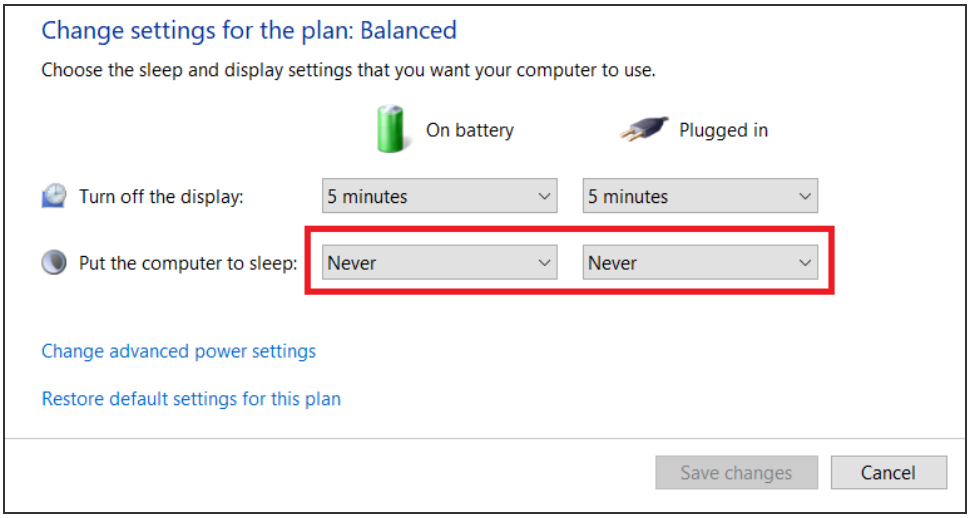
4. Press **Enter** on your keyboard.
5. Once your ping is successful, connect the target wireless device you want to fuzz to the access point.

Disable sleep mode in Windows

To prevent the computer from going to sleep during fuzzing, do the following:

1. In the Windows search bar, enter **Power & sleep settings**, and then select **Power & sleep settings** from the search results.
2. For the computer's sleep settings, set the **battery power** and **plugged in** options to

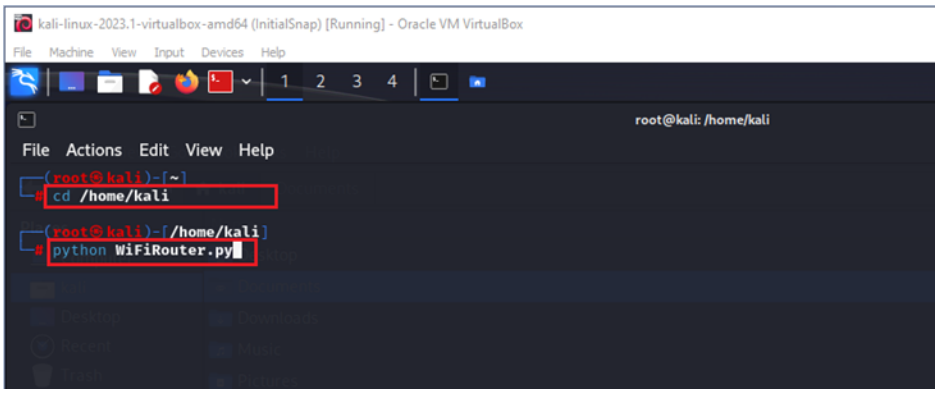
Never.



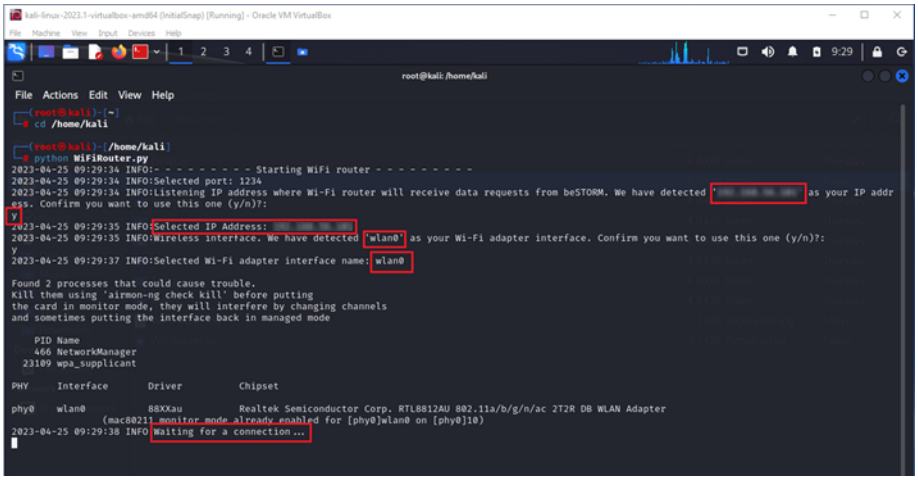
Start the Wi-Fi router Python script

1. Log in to the Kali Linux virtual machine (enter **kali** for the username and password boxes).
2. Connect the **AWUS036ACH Wi-Fi adapter** to the beSTORM computer.
3. From the top of the Kali Linux desktop, select the **Applications** icon > **Terminal Emulator**.
4. Using the folder and WiFiRouter.py file you created in steps 1-4 of ***Create the Wi-Fi router Python script* on page 14**, run the following commands in the Terminal Emulator:

```
cd /home/kali
sudo python WiFiRouter.py
```

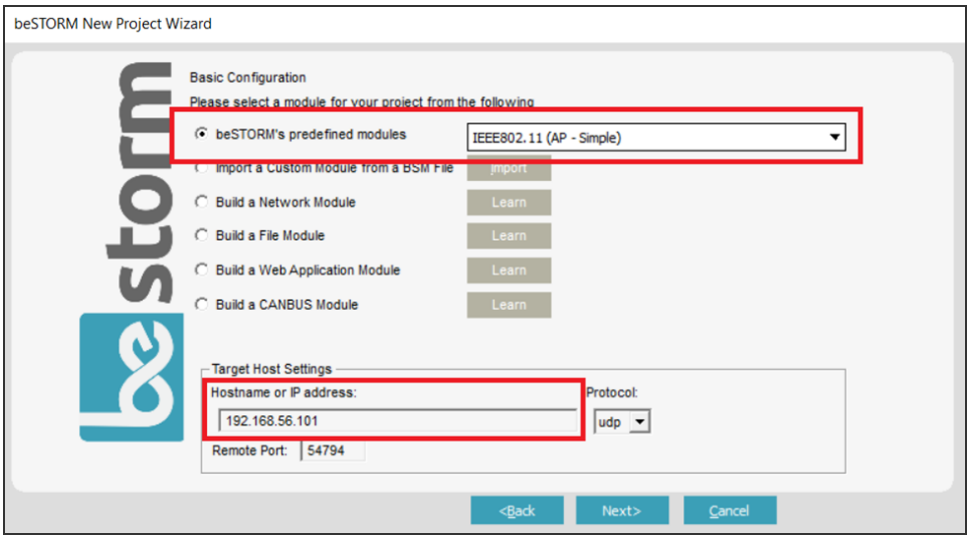


5. The Wi-Fi router Python script will start and detect the Selected IP Address of your Kali Linux virtual machine (you will need this IP address while configuring beSTORM), and the wireless adapter's interface name. Once "Waiting for connection" appears, the router is ready to use for fuzzing.

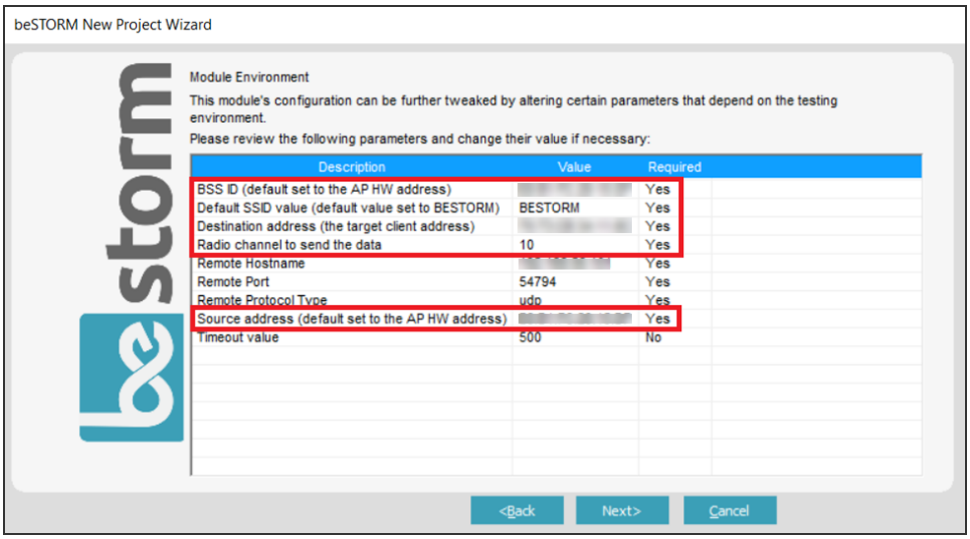


Create a Wi-Fi fuzzing project in beSTORM

1. Start **beSTORM Client**.
2. Select **New Project**. The beSTORM New Project Wizard opens.
3. On the **Welcome** page, enter a name in the **Project Name** box. Leave all other options to their default setting.
4. Select **Next**.
5. On the **Basic Configuration** page, select **IEEE802.11 (AP Simple)** from the **beSTORM's predefined modules** box.
6. In the **Hostname or IP address** box, enter the Selected IP Address from step 5 of ***Start the Wi-Fi router Python script* on page 19**. Leave the **Protocol** and **Remote Port** options to their default settings.

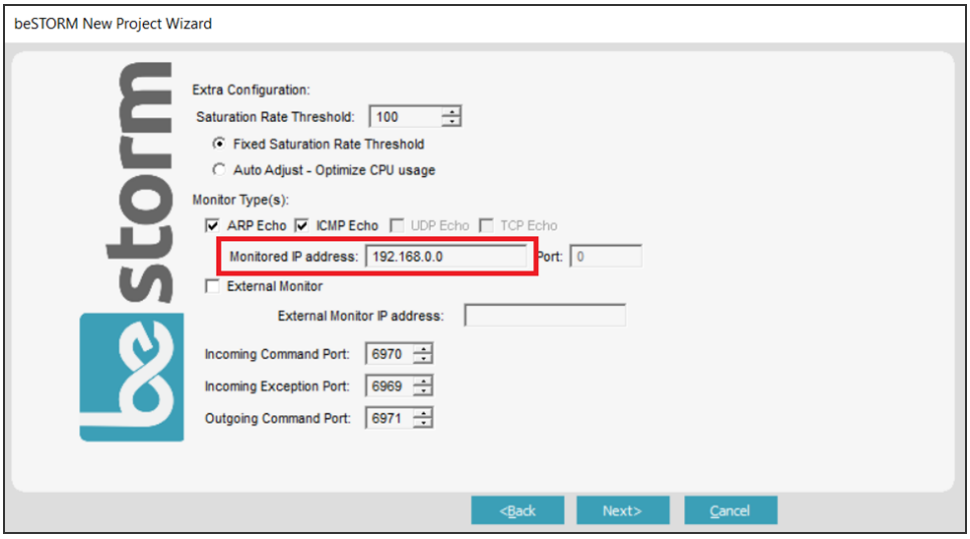


7. Select **Next**.
8. On the **Module Environment** page, confirm or set the following:
   a. **BSS ID** - The MAC address of the Access Point.
   b. **Default SSID Value** - The name of the access point you are replacing.
   c. **Destination Address** - This is the MAC address of the target wireless device. You can double-click the **Value** box to open the MAC Address Finder dialog (a useful tool for locating a device's MAC address).
   d. **Radio channel to send the data** - This is channel of the previous access point, and where the radio waves will be sent.
   e. **Remote Hostname** - The IP address of the Kali Linux virtual machine.
   f. **Remote Port** - The default port number selected on the Basic Configuration page.
   g. **Remote Protocol Type** - The default protocol type selected on the Basic Configuration page.
   h. **Source Address** - The MAC address of the access point. This test will spoof the access point's MAC address to inject packets into the communication between the access point and the target wireless device. You can double-click the Value box to open the MAC Address Finder dialog (a useful tool for locating a device's MAC address).
   i. **Timeout value** - Leave to default value.



NOTE: Use this example configuration to set up the IEEE802.11 (AP) or IEEE802.11 (AP - Simple) module. To create a project for the IEEE802.11 (Subscriber) or IEEE802.11 (Subscriber - Simple) module, switch the values for the Destination Address and Source Address (BSS ID remains the same).

9. Select **Next**.
10. On the **Extra Configuration** page, to monitor fuzzing, enter the IP address of the wireless target device in the **Monitored IP address** box.

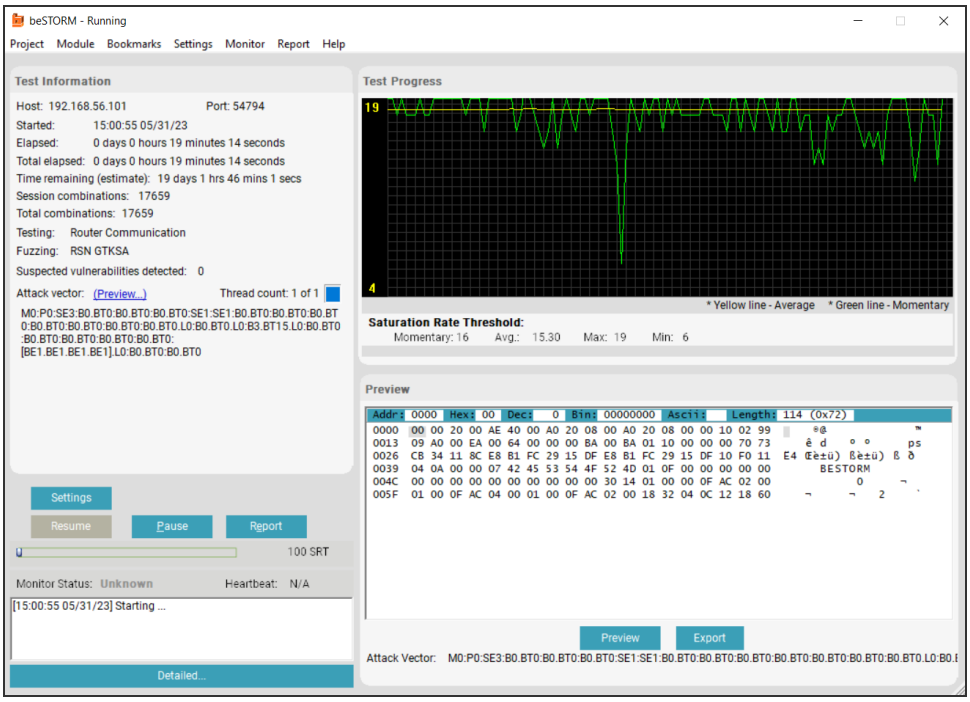


> **NOTE:** If you can run software on the target wireless device, the Windows monitor or GDB monitor are ideal methods to monitor for failure. However, the most compatible method is to ping the target wireless device. If Internet Control Message Protocol (ICMP) pinging over Wi-Fi is unsuccessful, this indicates the client's Wi-Fi stack stopped working, which shows a potential weakness.
>
> Verify monitoring works by pinging the target wireless device from the beSTORM computer using the ping command in the Windows Command Prompt. For example:
>
> ```
> ping 192.168.0.0
> ```
>
> If you receive a response, the monitoring will work with ICMP.

11. Select **Next**.
12. On the **Complete beSTORM wizard** page, clear the **Auto-start beSTORM scan now** checkbox.
13. Select **Finish**.
14. Stop the access point that the target wireless device connects to.

    > **NOTE:** Skip this step if you are using the IEEE802.11 (Subscriber) or IEEE802.11 (Subscriber - Simple) module.

15. On the **beSTORM Monitor** window, select **Start** to begin fuzzing. If there are no issues, fuzzing will begin immediately.



16. You can also view fuzzing results on your Kali Linux virtual machine.