

# Learn Forensics Mode in Kali Linux

Kali Linux 'Live' provides users with 'forensic mode', a feature introduced for the first time in BackTrack Linux.

Kali Linux 'Live' provides users with ' **forensic mode** ', a feature introduced for the first time in BackTrack Linux.

## The cause of the "Forensic mode live boot" option becomes popular

The " **Forensic mode live boot** " option has become very popular for many reasons:

1. Kali Linux is a wide and easy to use application, many potential users have installed Potassium ISO or bootable USB drives.
2. When a need for analysis occurs, Kali Linux 'Live' helps quickly and easily bring Kali Linux into operation.
3. Kali Linux comes preinstalled with the most popular open source analysis software, a handy set of tools when you need to do analytics.

*Download Kali Linux*



# Changes of Forensic mode with the system

When booted into Forensic mode boot mode, there are a few important changes to the regular operation of the system:

1. First, the internal hard drive will never be touched. If there is a swap partition, it will not be used and no internal drive is automatically mounted. We have verified this by taking a standard system and removing the hard drive. A 'hash' has been added to the drive using a commercial legal package. We then re-attached the drive to the computer and started Kali Linux 'Live' in Forensic mode. After using Kali for a period of time, we turn off the system, remove the hard drive and retrieve 'hash'. These suitable 'hash' shows that nothing changes on the drive in any way.
2. Another important change is that the auto-attaching of mobile devices will be disabled. USB drives, CDs and similar devices will not be automatically attached to Kali Linux when they are inserted into the computer. The idea behind this is simple: In Forensic mode, nothing happens to any media without direct user action. Whatever you do as a user depends on you.

If you plan to use Potassium in Forensic mode, we recommend you to research it carefully. All analytical tools need to be validated to make sure you know what specific effects they have in each case.

Finally, when Kali continues to focus on providing the best collection of open source penetration testing tools available, we may not have mentioned your favorite tool. If yes, let us know in the comment section below!

See more:

1. Kali Linux commands from AZ and commonly used commands
2. Instructions for installing Kali Linux on Windows 10 are easier than ever
3. How to install and use Kali Linux on VmWare virtual machine

You finished reading the article "**Learn Forensics Mode in Kali Linux**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.