**Handshake**

The packets that contain helpful information and help to determine the actual WPA key are the handshake packets. In each WPA packet, there is a unique temporary IV. These packets do not contain any information that can help determine the actual WPA key. Four handshake packets will be sent when a new device connects to the target network. Suppose we are at home, our device connects to the network using the password, and a process called a four-way handshake happens between the AP and the devices. In that process, four handshake packets are transferred between the two devices to authenticate the connection. We can use a wordlist using the aircrack-ng and test each password in the wordlist by using the handshake. We can capture the handshake in two ways. First, we can sit down and wait for a device to connect to the network. Once a device is connected, then we can capture the handshake. Second, we can use a de-authentication attack. In a de-authentication attack, we can disconnect any device from a network within our Wi-Fi range. If we apply this attack for a brief period, we can disconnect a device from the network for a second, the device will try to connect to the network automatically, and even the person using the device will not notice that the device is disconnected or reconnected. Then we will be able to capture the handshake packets. The handshake gets sent every time a device connects to a target network.