How to fix: 'WARNING:REMOTE HOST INDENTIFICATION HAS CHANGED' or the authenticity of host 'blabla' can't be established

When you connect to a server via SSH, it gets a fingerprint for the ECDSA key, which it then saves to you home directory under ~/.ssh/known_hosts. This is done after first connecting to the server, and will prompt you with a message like:

```
$ ssh ec2-user@ec2-192-168-1-1-.compute-1.whatever
The authenticity of host 'ec2-192-168-1-1-.compute-1.whatever' can't be
established.
ECDSA key fingerprint is 'SHA256:hotsbx/lkjdfs/fdlgkjrtilfgdk+lkjz+lkjsdf.
Are you sure you want to continue connecting (yes/no)?
```

if you enter 'yes', then the fingerprint is saved to the know_hosts file, which SSH then consults every time you connect to that server.

But what happens if a server's ECDSA key has changed since you last connected to it? This is alarming because it could actually mean that you're connecting to a different server without knowing it. If this new server is malicious then it would be able to view all data sent to and from your connection.

Of course, this isn't always the case, and there are many reasons for the ECDSA key fingerprint to change fo a server.

Fixing it:

In the warning message find the line that tells you where the offending ECDSA key is located in the known_hosts file:

```
Offendiing ECDSA key in /Users/your_name/.ssh/known_hosts:12
```

refers to line 12

Open the known_hosts file and delete the line specified in the warning message.

save and exit known_host file and thats it.