Abstract – In the recent years, the rapid adoption of mobile devices has dramatically changed the access to various networking services which led to the large increase of mobile service traffic. latest studies show that mobile packets can be identified and classified to type of device and app actions that are been used by user, however with mobile traffic been encrypted it becomes more challenging to identify the mobile devices. using machine learning we can solve this encryption issue with a collected dataset that has been created from variety of devices. previous approaches are not applicable to real life settings because previous approaches analyst unencrypted data. The previous approaches are port and payload-based methods. port method assumes that the applications consistently use TCP or UDP port numbers. payload-based method is identifying applications by inspecting the packet headers or even payload. With the excellent ability of automatic feature learning, Deep Learning (DL) undoubtedly becomes a highly desirable approach for mobile services traffic classification, especially encrypted traffic. In this work, we extend the ability of these classification identifying mobile device using encrypted packets send by mobile device by using ML(Machine learning) or DL(Deep learning) method. We test the method to get real datasets collected by using Raspberry Pi to extract the mobile packets from different mobile devices maybe we also use public datasets like ISCX2012. Our approach leverages a small number of labeled instances of encrypted traffic from a source configuration, in order to construct a classifier capable of identifying a device type in a different (target) mobile cellular which is completely unlabeled.