This essay explores the prevalence of prefix hijacking online. This gives the hijacker the option to either stop all hijacked traffic or to intercept it and send it back to the owner. This article explains prefix hijacking in detail, makes an estimate of the quantity of traffic that can be hijacked and intercepted, intercepts real-time traffic, and studies it in depth. Simply by promoting the appropriate prefix, the attacker may divert traffic. Because the traffic is transmitted back to the original recipient, which is unaware of the interception, interception is riskier. The majority of the traffic will be hijacked by the hijacking router because it will identify itself as the owner of the prefix. It may also display a longer path for the same prefix, but since we want the shortest path, this malicious path won't be taken into account very frequently. As a result, very little traffic will be hijacked by it. The other method a hijacker could employ is to increase the /xx bits in the address x.x.x.x/xx if it does so, it will draw in the majority of traffic; alternatively, it could decrease the./xx bits to capture less traffic. However, in both of these scenarios, traffic cannot be redirected back to the owner so neither method is useful for intercepting it. According to the research from the previous study, AS favours customer routes over peer routes and provider routes. The chart enables us to examine the several scenarios —peer, customer, and provider—where hijackers may be present. Where your attacker sets its router is crucial since all traffic will travel via it if your attacker is a peer router, even if it claims that it is the source prefix because it has a higher local preference. To send the data once the attack is complete, the hijacker has to have a connection to the owner of the traffic to intercept it. If the hijacker is a customer in two instances where both of them are peers, the communication won't be able to be sent since it may become tangled up in a triangle loop. Since tier-1 is at the top, lacks provider routes, and has peer connections with every other AS, the rate of prefix hijacking with an invalid route will be significantly greater there because of the downhill path that the invalid route might take. Tier-1 aircraft have an almost 70% risk of being hijacked, according to actual testing. These are only prefixed hijacking statistics, but the authors were interested in the actual traffic that was intercepted; the findings indicate that this quantity was between 60 and 70%, which is close to the entire estimate. Prefix hijacking ranges from 38 to 63% for all tiers, whereas interception ranges from 29 to 48%. There are additional numbers for independent tiers. In a simulated setting, the authors intercepted traffic on real-time ASes and discovered that while 66%–97% of it was hijacked, only 23.4–78% of it was really intercepted. The majority of the errors were due to IS-AS mapping, according to the authors, who used traceroute to identify anomalies. Based on the BGP routing table, this can be caused by sibling ASes sharing an address space, IXPs using the same address space, or customers using the provider's address space to peer with other users. Some of the anomalies were caused by traffic engineering, in which a bigger portion of the prefix was broadcast because traffic was redirected to a significant portion of the matching prefix address. Some results were inexplicable since it was unclear if they were the consequence of traffic engineering or interceptions. This study demonstrates that it is possible to intercept and record internet data. Although it may appear impossible, interception is possible, thus we must consider ways to confirm announcements or implement security measures to prevent frequent occurrences of such situations.