IP Fragmentation Attack is a network-layer evasion technique that exploits how fragmented IP packets are reassembled by a receiving host or intermediate security device. Fragmentation is normally a benign mechanism triggered when a datagram exceeds the Maximum Transmission Unit (MTU) along its path. However, 5G and next-generation mobile networks introduce architectural and performance constraints that make fragmentation-based attacks even more impactful.

In 5G ecosystems, especially within the user plane (UPF → gNodeB → core), encapsulated traffic often traverses GTP-U tunnels. While outer IP packets may remain intact, the **inner IP payloads carried within GTP-U** may be fragmented due to dynamic MTU negotiation, transport slice parameters, or rapid handovers. Many traditional firewalls, DPI systems, or legacy IPS devices inspect only the **outer IP headers**, failing to perform full **deep reassembly** of the encapsulated inner fragments. This creates a security blind spot that adversaries can exploit.

In the proof-of-concept demonstration, the attacker constructs fragmented UDP packets where no single fragment contains recognizable malicious content. The payload is distributed across fragments such that detection systems observing outer packets or shallow fragment inspection cannot detect the remote command. Once the fragments reach the reassembly point—often past multiple trust boundaries in a 5G architecture—the harmful command becomes visible as the final assembled packet and is executed.

These behaviors align with real-world fragmentation attacks observed in telecom environments:

- **Bypassing GTP-aware firewalls** that do not inspect inner fragments
- **Evasion of IDS/IPS systems** lacking cross-layer or cross-fragment correlation
- **Exploiting ultra-low-latency constraints**, where full reassembly may be skipped
- **Protocol smuggling inside GTP-U**, embedding malicious instructions across fragment boundaries

The attack is effective because 5G data-plane components assume correct fragmentation behavior to maintain throughput and latency guarantees. As networks evolve toward 6G with higher bandwidth, distributed edge processing, and extreme mobility, fragmentation-based evasions will continue to challenge traditional perimeter defenses unless deep reassembly, slice-aware inspection, and telecom-specific security controls are deployed.