Organized criminal groups increasingly rely on anonymous and encrypted communication applications and privacy-centric financial platforms to coordinate activities, exchange instructions, and move illicit funds. These applications typically employ End-to-End Encryption (E2EE – End-to-End Encryption), obfuscation techniques, and anonymity layers such as Virtual Private Networks (VPN – Virtual Private Network) and The Onion Router (Tor – The Onion Router).

As a result, even when Party A (the accused) is in lawful custody and their device is available for examination, law-enforcement agencies face serious limitations in identifying Party B (the remote communicator) due to:

1. Inaccessibility of message content due to encryption
2. Lack of visible identifiers (phone number, username, IP address)
3. Use of intermediary servers, relays, or anonymization networks
4. Rapid deletion and self-destructing communication features

Traditional device forensics alone is often insufficient to establish communication linkage, timing correlation, or network attribution between the accused and the remote party.

Therefore, there is a critical operational requirement for a lawful, non-intrusive, and technically reliable packet capture–based solution that can be deployed on a suspect's device to extract network-level metadata and assist in identifying or narrowing down the B party involved in encrypted communications.