[SecAthon2025]External Attack Investigation

During the operation of the banking enterprise's IT system, the SOC team suspected that a private server within the servers zone was targeted in a flooding attack originating from the external zone. The server zone contains both public and private servers. The path of packets originating from the external zone to the server zone is illustrated in the following diagram: [external_zone] --> incoming packets --> [basic_firewall] --> [servers_zone]
The basic firewall has been configured to block all incoming packets originating from the external zone that are intended for the private server. The private server may be configured not to respond to any external packets; however, the server's logs indicate that it has received those packets.
You, as a Tier 2 analyst, have been assigned to examine an file named *external_servers_capture.pcapng*, which contains previously recorded incoming network traffic.

Your task is to analyze the capture and answer the following questions:
1. What is the type number (X) corresponding to the header field that was exploited by the threat actors to conduct the attack?
2. What is the ordered list of IP addresses (Y=Y1,Y2,…Yn) set by the threat actors that the attacking packet must traverse on its way to the destination? Y may contain one or more values.
3. What is the IP address (Z) of the private server that was attacked?

Your answers will form the flag in the following format: FUSec2025{X-Y-Z}
For example:
X:789, Y1: 1.1.1.1, Y2: 2.2.2.2, Z: 9.9.9.9 --> FUSec2025{789-1.1.1.1,2.2.2.2-9.9.9.9}