1. Payload and Data Inside the Datalink Layer of the LoRa Device: The payload of a LoRaWAN packet is contained within the PHY Payload (PHYPayload) which consists of three groups of fields: a MAC Header (MHDR) defining information about the type of message and its format version, a MAC Payload (MACPayload) containing the information being transmitted12. The maximum payload size varies by Data Rate (DR) and is region-specific2.
2. Data Transmission from Device to Gateway to Server: In a LoRaWAN network, end devices send data to gateways (uplinks), and the gateways pass it on to the network server, which, in turn, passes it on to the application server as necessary34. All LoRa gateways within range of an end node receive data from the device. Then, the gateways forward this data to the LoRaWAN network server5.
3. Breaching the Data Link Layer and the Stage of Breach: The security of the LoRaWAN protocol has been a subject of research, and vulnerabilities have been identified in the past6789. These vulnerabilities could potentially allow an attacker to access sensitive information, modify data, or disrupt the operation of the network. However, exploiting these vulnerabilities would require a deep understanding of the LoRaWAN protocol and sophisticated attack techniques.
4. Data Retrieval Program: Retrieving data from the data link layer of the LoRaWAN protocol would require a program that can interact with the LoRaWAN hardware and software. One approach could be to use a software-defined radio (SDR) to capture the radio signals transmitted by the LoRaWAN devices and then decode these signals to extract the data. However, this would require a deep understanding of the LoRaWAN protocol and the specific radio frequencies used by the devices. There are also legal and ethical considerations to keep in mind when capturing and decoding radio signals.

Please note that breaching the data link layer of a LoRaWAN network is a complex task

that requires a deep understanding of the LoRaWAN protocol and sophisticated attack techniques. It's also important to note that unauthorized access to a network is illegal and unethical. If you're interested in studying the security of LoRaWAN networks, I would recommend doing so in a controlled environment and with the proper permissions.

As for the program to retrieve data from the data link layer of the LoRaWAN protocol, there are existing research works like DaRe101112 that focus on data recovery through application layer coding for LoRaWAN. However, creating a program to breach the data link layer for malicious purposes is not only unethical but also illegal.

I hope this information helps you with your research. If you have any more questions, feel free to ask!