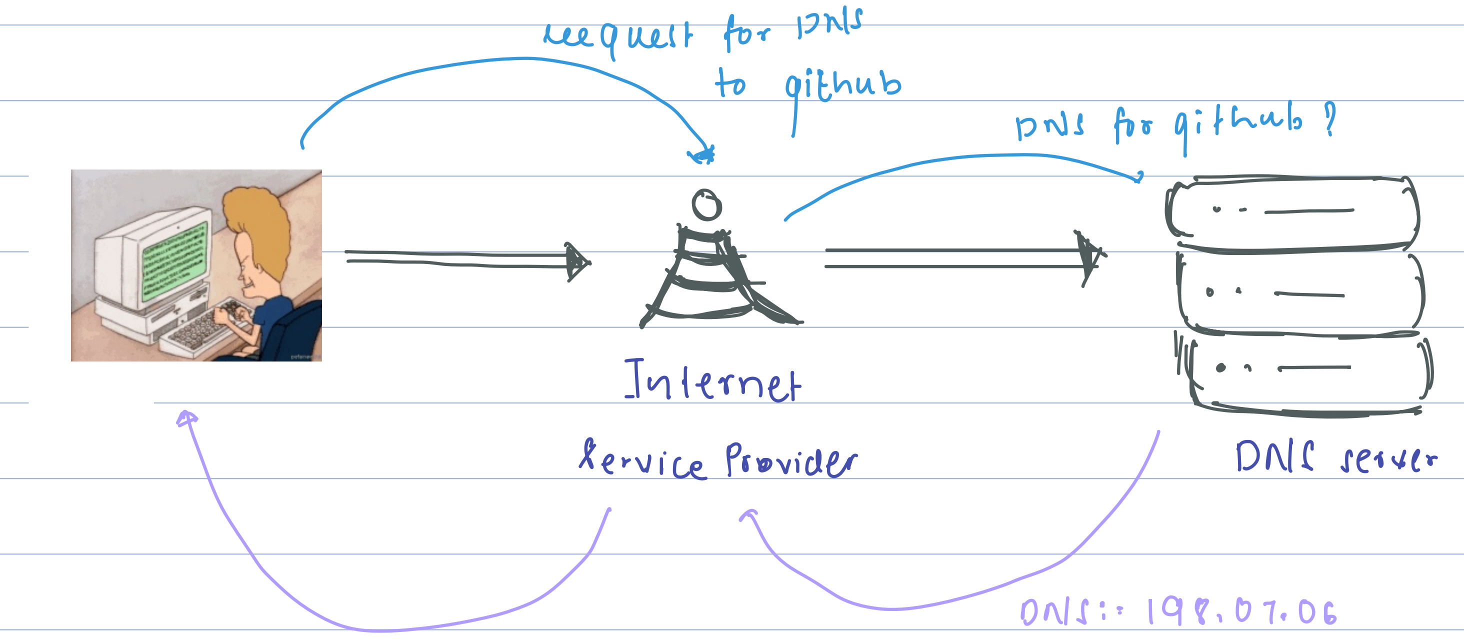
*The problem with HTTPS is that : While HTTPS encrypts the content of the communication, certain metadata, such as destination IP address, and DNS request, remains visible to the intermediaries like router, ISPs and network operators.

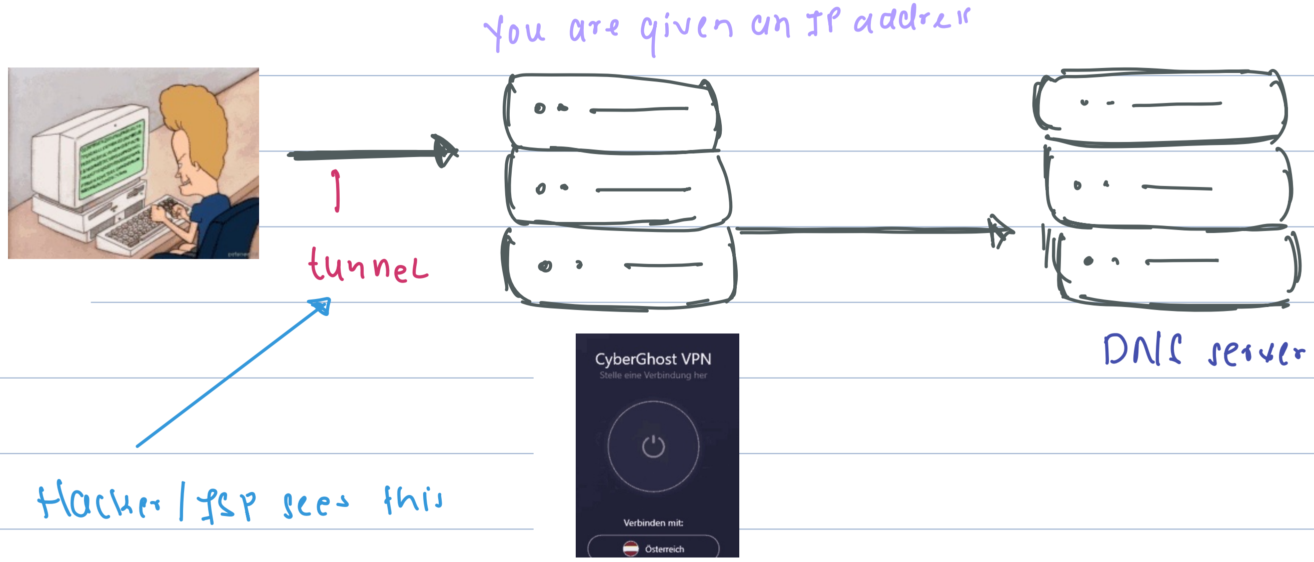
This meta data leakage can expose the identity of the website being accessed, even though the content is encrypted.

Solution : VPN (Virtual Private network)



- In this process, ISP know what website you are accessing.

- VPN creates a tunnel from client's computer to VPN servers (masking your IP address). Then the VPN server request the DNS and does everything without any intemediaries. involved / spying.



Tunnelling :-

Tunnelling involves two major steps:-

1. Encapsulation :- The original data packet is placed inside another packet format

2. Encryption:- The encapsulated packet is then encrypted for secure transmission.

source port / dest. port

IP Header	TCP Header	Data Payload

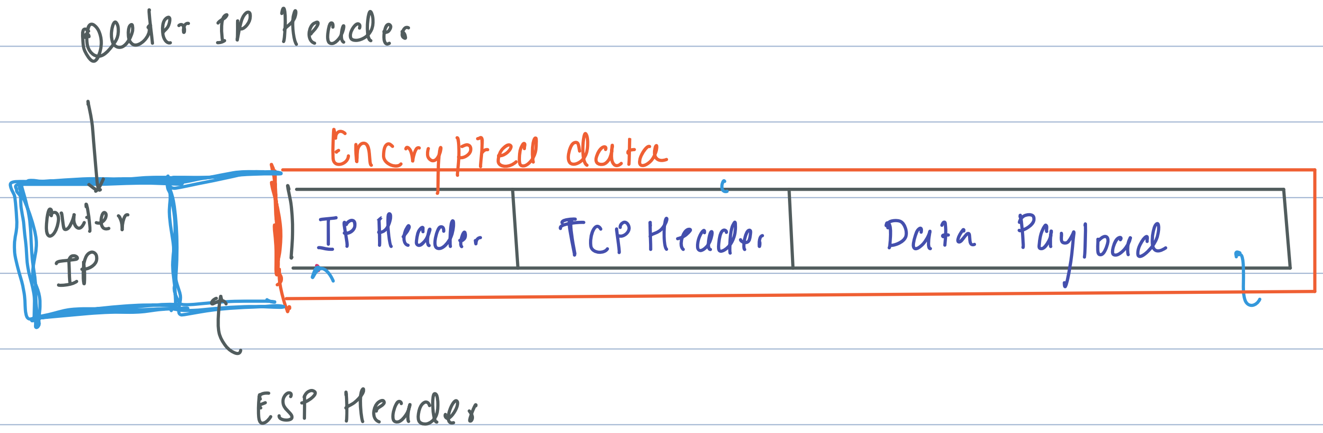
IP packet without VPN

IP Header contains source IP and destination IP

data being transmitted.

↳ ! When you send a request without a VPN, the packet header will show you original IP address as source address, which allows servers and intermediaries to identify your location.

With VPN:-



- Outer IP Header :- Contains the source IP address of the VPN client and the dest. IP address of the VPN server.

- VPN then decrypts the Encrypted, replace's the source IP with vpn's server's IP and then sends the packet

Site to site VPN protocol:

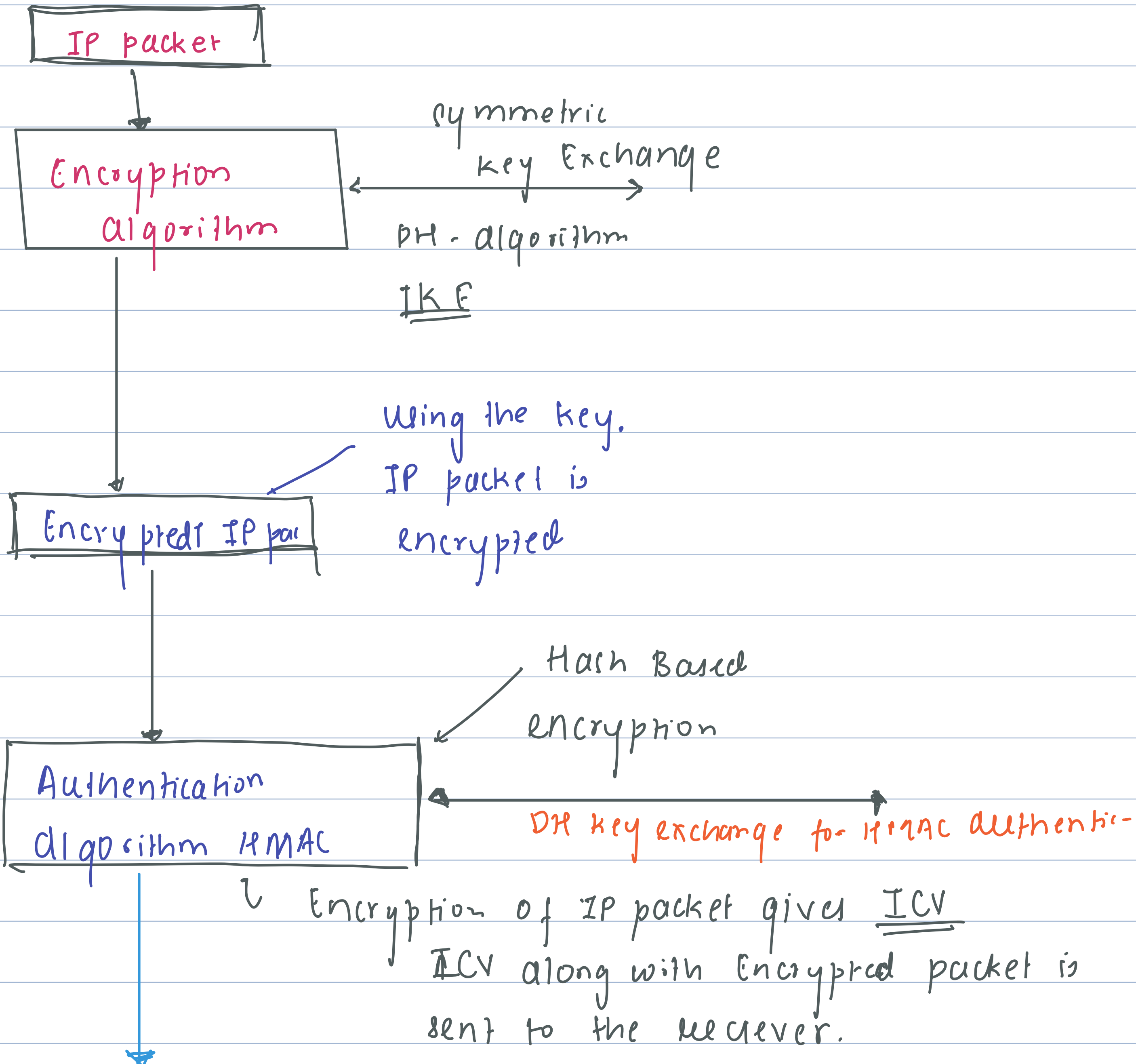
- Router A and RouteB negotiate an IKE phase one session

  - DH key exchange algorithm

  → refer sir's slide

- IPSec tunnelling

IPSec sender



symmetric key Exchange

DH - algorithm

IKE

Using the key. IP packet is encrypted

Hash Based encryption

DH key exchange for HMAC authentic-

→ Encryption of IP packet gives ICV

ICV along with Encrypted packet is sent to the reciever.

Encrypted packet +
ICV

IPsec Reciever

When IP sec reciever gets the Encrypted packet and ICV

- Reciever calculates ICV using HMAC function and key.

$$HMAC(Encrypted\ packet) = \underline{H(E)}$$

- If $H(E) == ICV$

  Authentication successful

- Else

  Unauthorized.

Using the key recieved in IKE step, reciever decrypts the Encrypted IP packet.