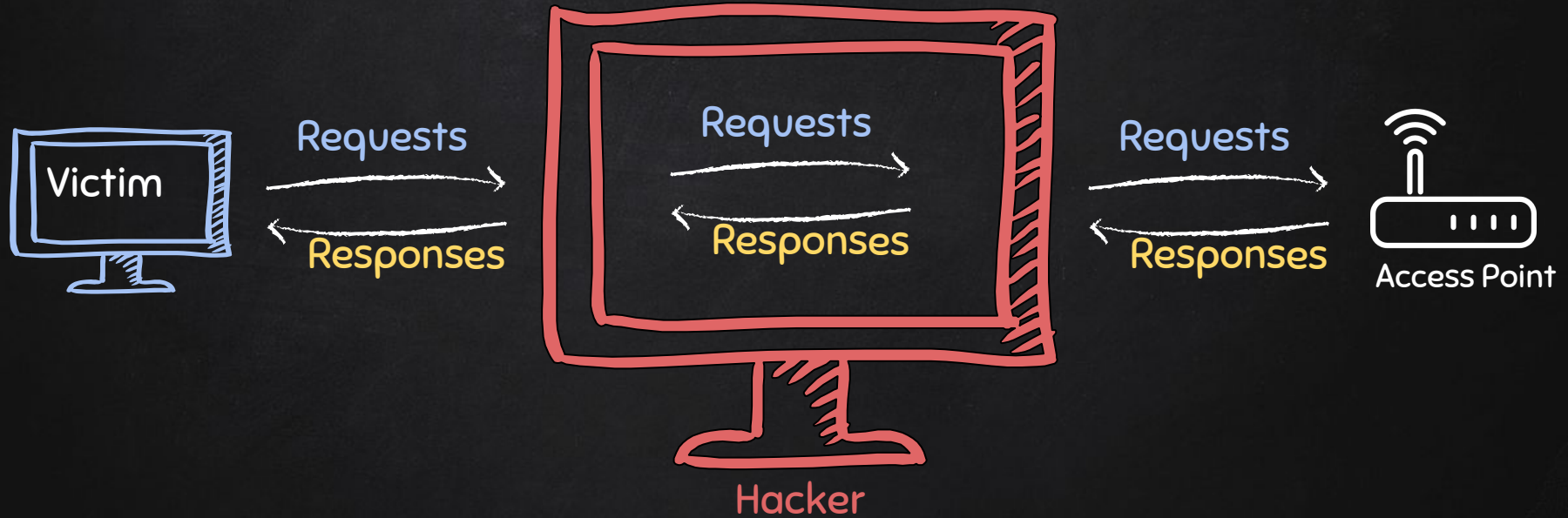


INTERCEPTING & MODIFYING PACKETS

- Scapy can be used to:
 - Create packets.
 - Analyse packets.
 - Send/receive packets.
- But it can't be used to **intercept** packets/flows.



CLASSIC MITM SCENARIO



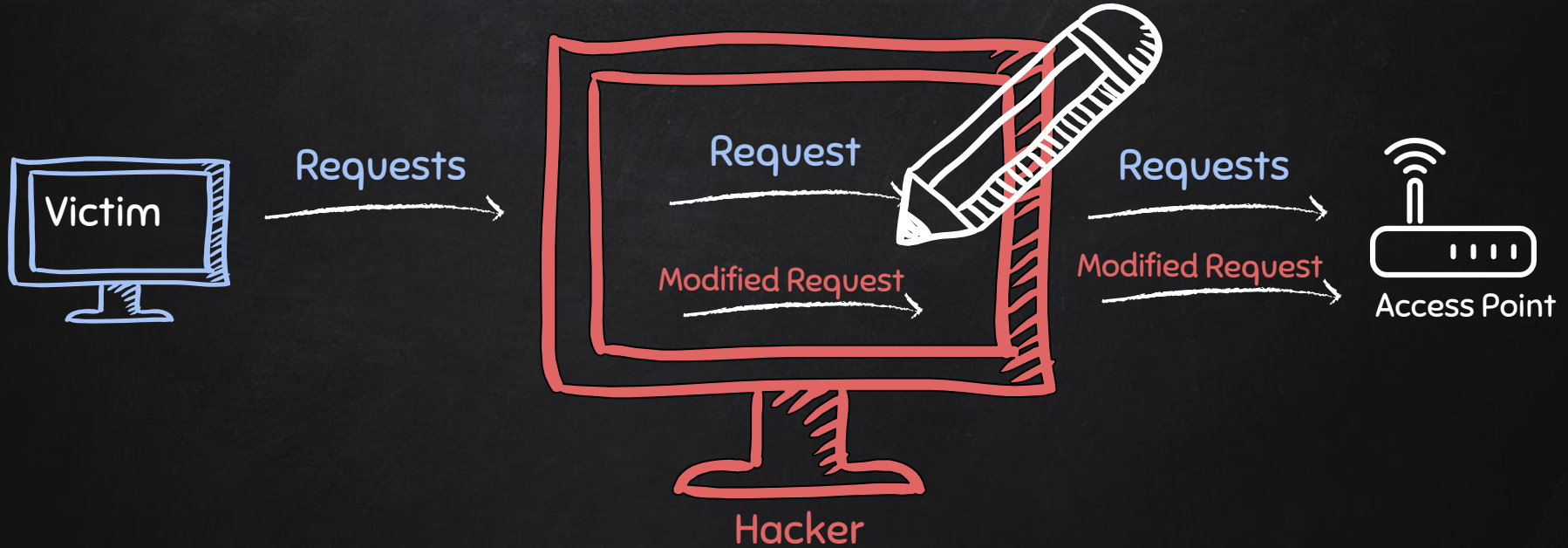
MITM - SNIFFING DATA

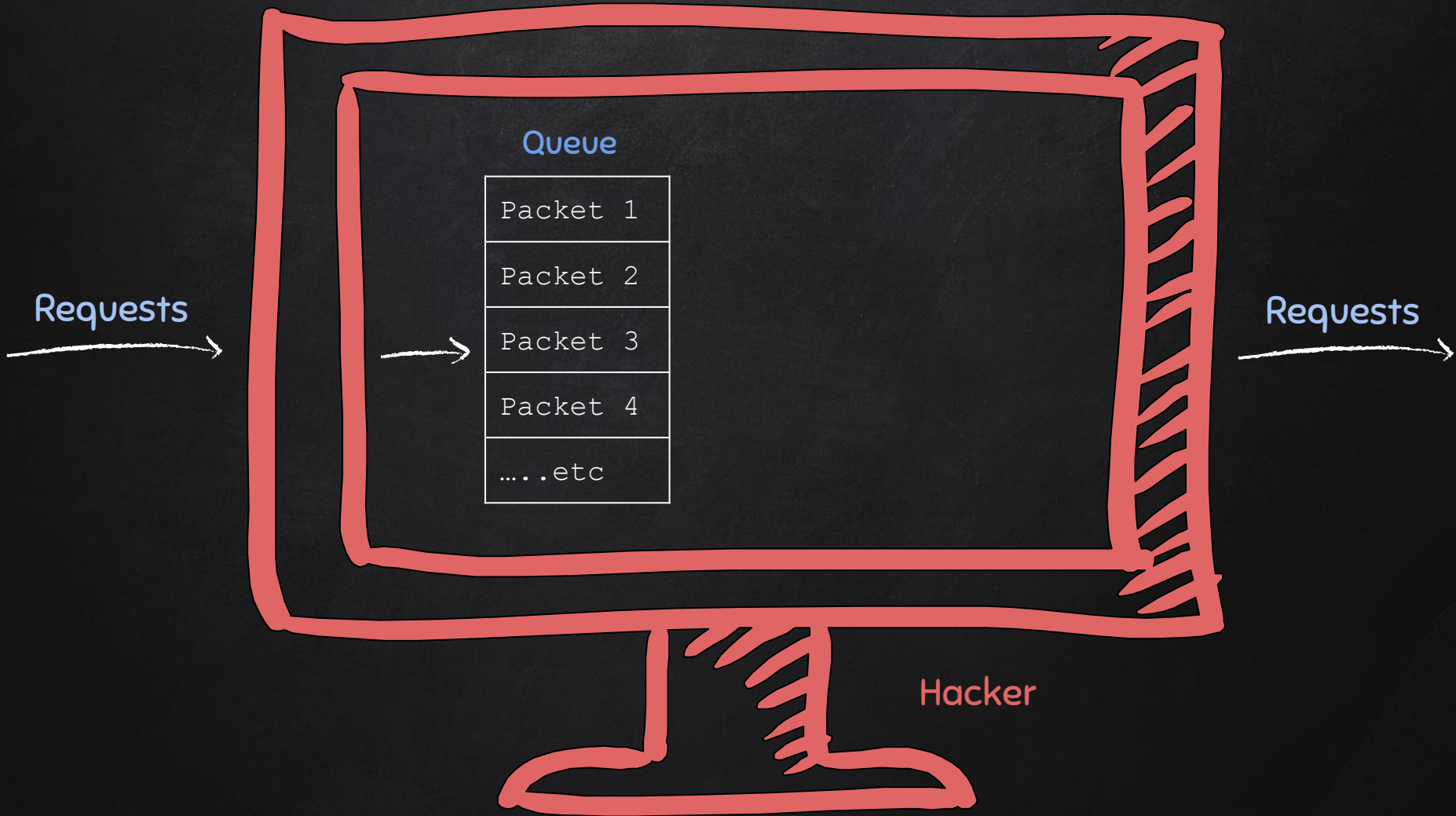


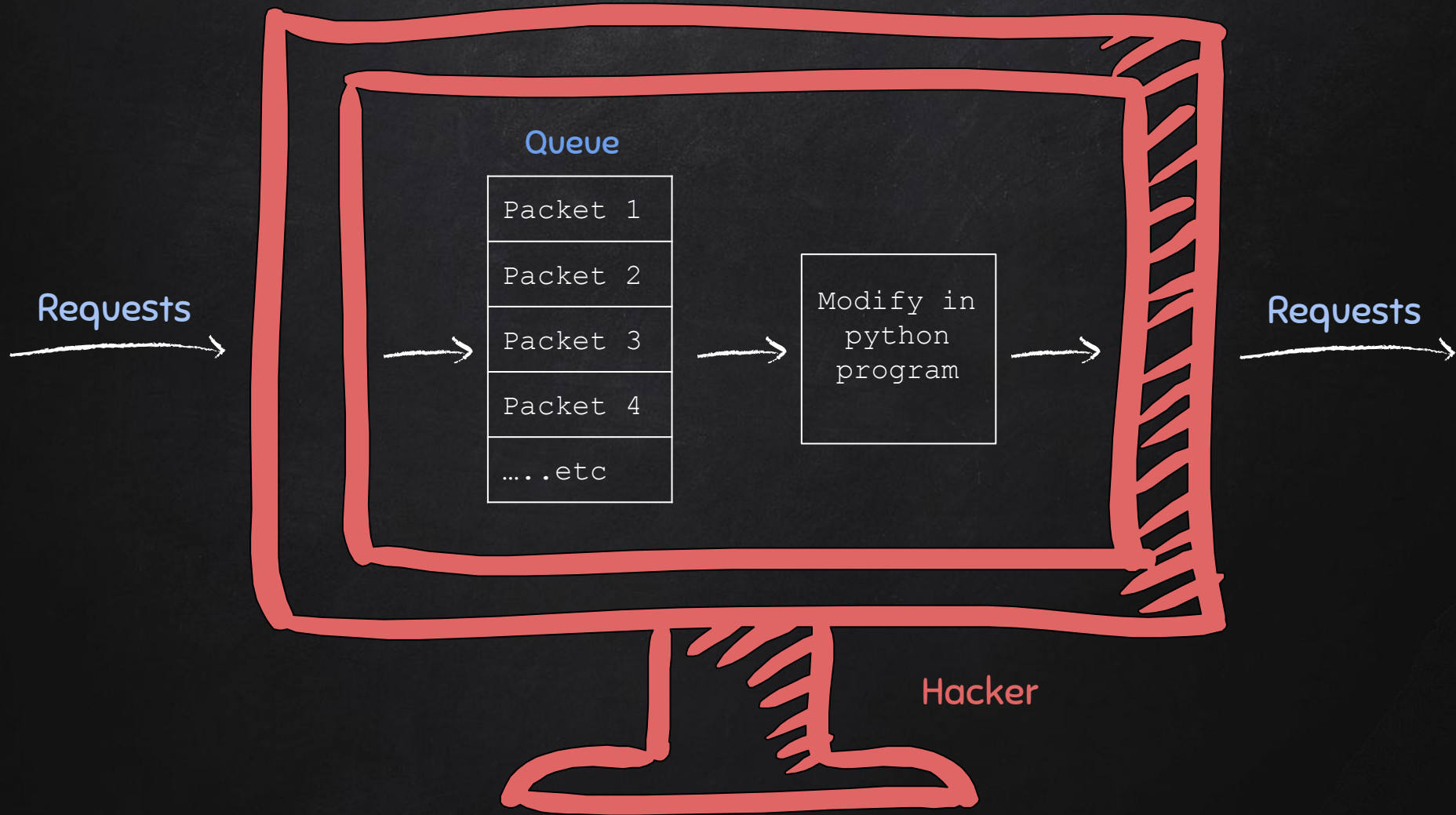
MITM - MODIFYING DATA

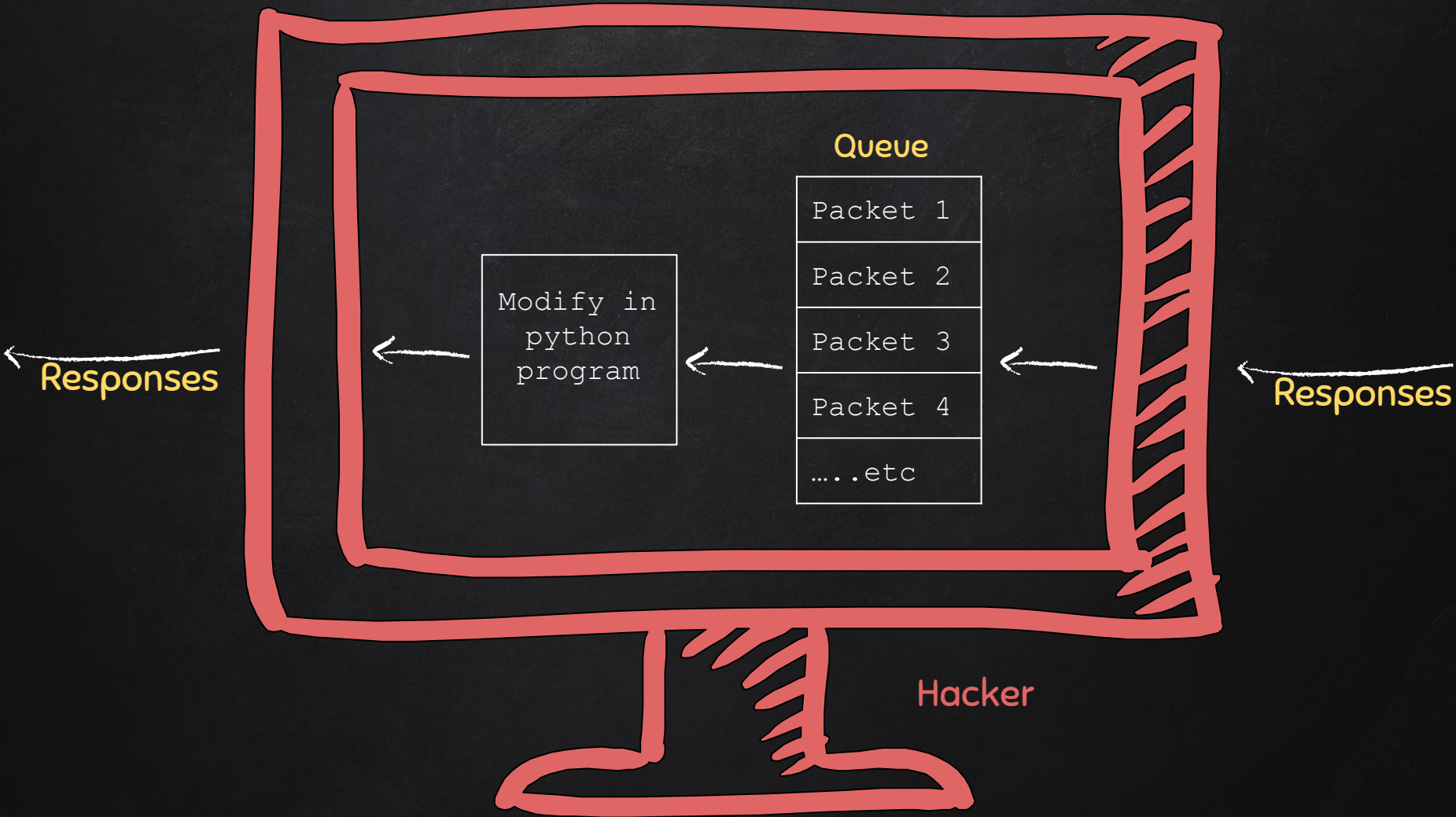


MITM - MODIFYING DATA











FACEBOOK.COM WEB SERVER
195.44.2.1



BING.COM WEB SERVER
204.79.197.200



DNS SERVER





FACEBOOK.COM WEB SERVER
195.44.2.1



BING.COM WEB SERVER
204.79.197.200

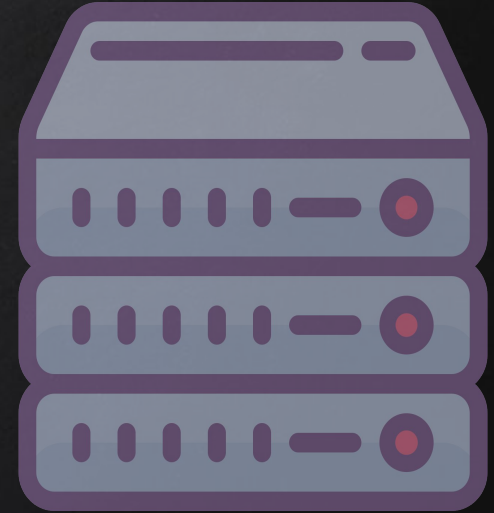


DNS SERVER



DNS RECORDS

bing.com	A	204.79.197.200
facebook.com	A	195.44.2.1
zsecurity.org	A	104.27.153.174
.....etc		





FACEBOOK.COM WEB SERVER
195.44.2.1



BING.COM WEB SERVER
204.79.197.200



DNS SERVER





FACEBOOK.COM WEB SERVER
195.44.2.1



BING.COM WEB SERVER
204.79.197.200



DNS SERVER



FACEBOOK.COM WEB SERVER
195.44.2.1



BING.COM WEB SERVER
204.79.197.200



DNS SERVER





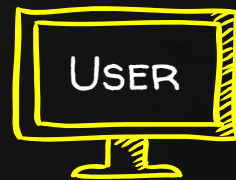
FACEBOOK.COM WEB SERVER
195.44.2.1



BING.COM WEB SERVER
204.79.197.200



DNS SERVER





FACEBOOK.COM WEB SERVER
195.44.2.1



BING.COM WEB SERVER
204.79.197.200



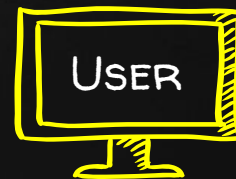
HACKER WEB SERVER
10.0.2.16



DNS SERVER



bing.com
←





FACEBOOK.COM WEB SERVER
195.44.2.1



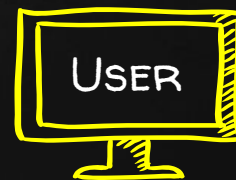
BING.COM WEB SERVER
204.79.197.200



HACKER WEB SERVER
10.0.2.16



DNS SERVER





FACEBOOK.COM WEB SERVER
195.44.2.1



BING.COM WEB SERVER
204.79.197.200

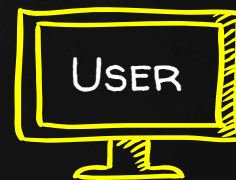


HACKER WEB SERVER
10.0.2.16



DNS SERVER

204.89.197.200





FACEBOOK.COM WEB SERVER
195.44.2.1



BING.COM WEB SERVER
204.79.197.200



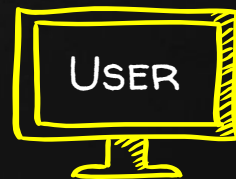
HACKER WEB SERVER
10.0.2.16



DNS SERVER



10.0.2.16





FACEBOOK.COM WEB SERVER
195.44.2.1



BING.COM WEB SERVER
204.79.197.200



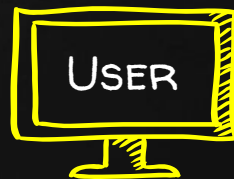
HACKER WEB SERVER
10.0.2.16



DNS SERVER



winzip.exe





FACEBOOK.COM WEB SERVER
195.44.2.1



BING.COM WEB SERVER
204.79.197.200



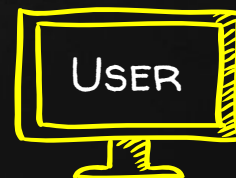
HACKER WEB SERVER
10.0.2.16



DNS SERVER



backdoor.exe



HTTPS



Problem:

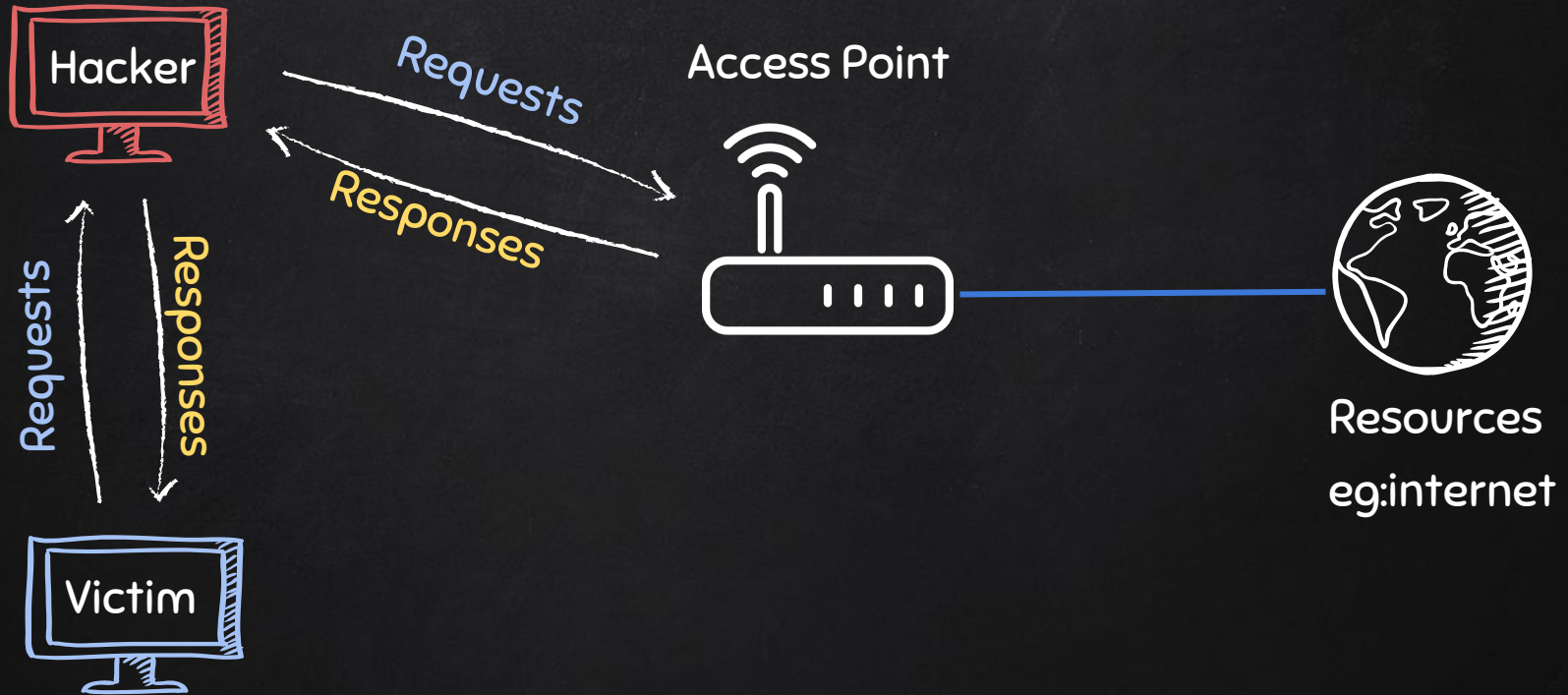
- Data in HTTP is sent as **plain text**.
- A MITM can read and edit requests and responses.

→ not secure

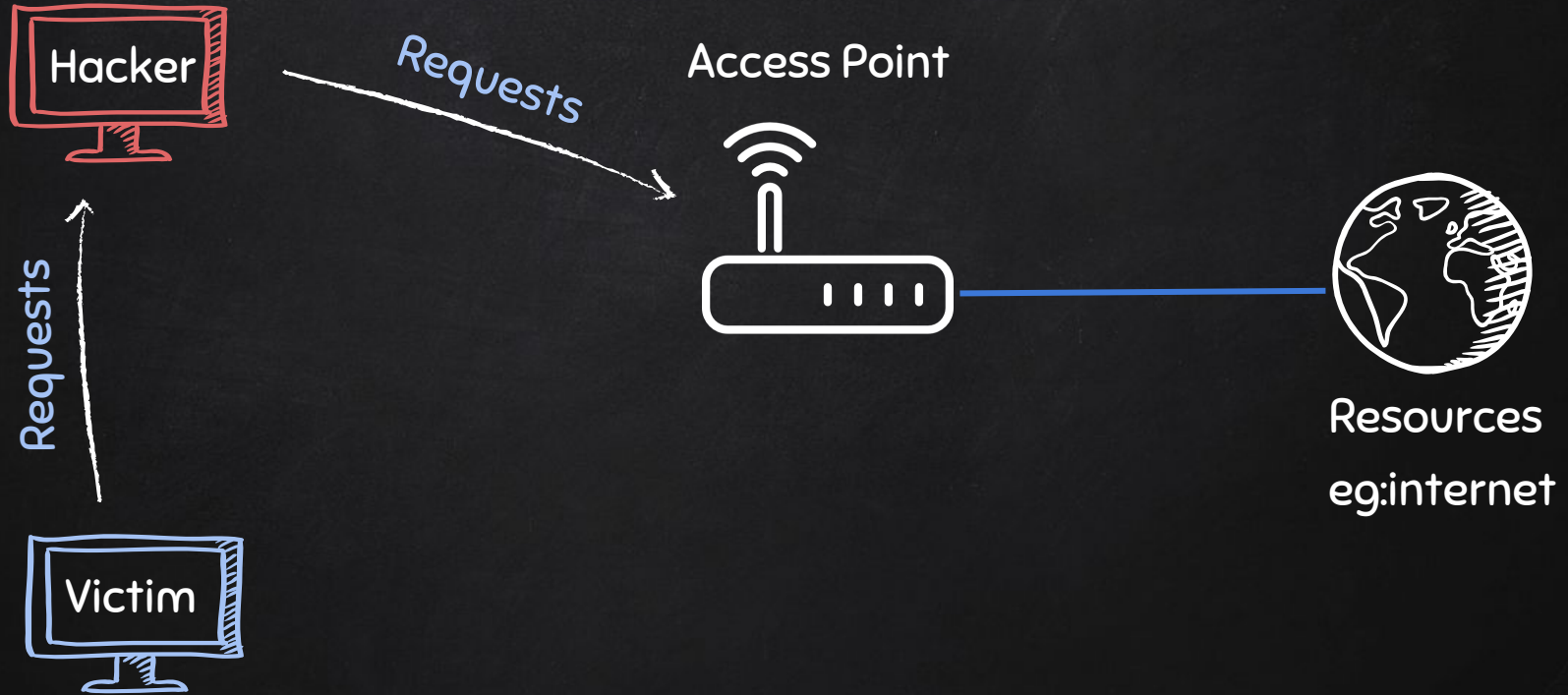
Solution:

- Use HTTPS.
- HTTPS is an adaptation of HTTP.
- **Encrypt** HTTP using TLS (Transport Layer Security) or SSL (Secure Sockets Layer).

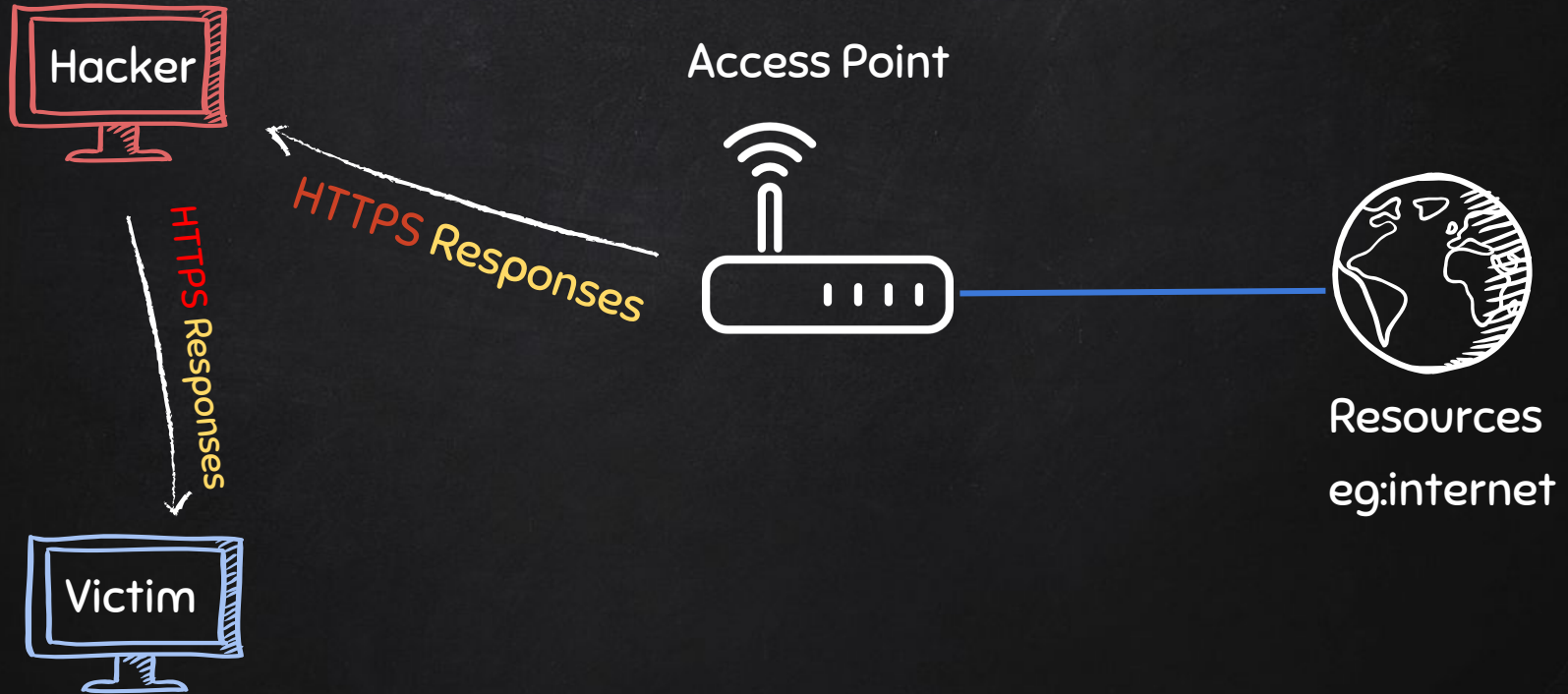
ARP SPOOFING



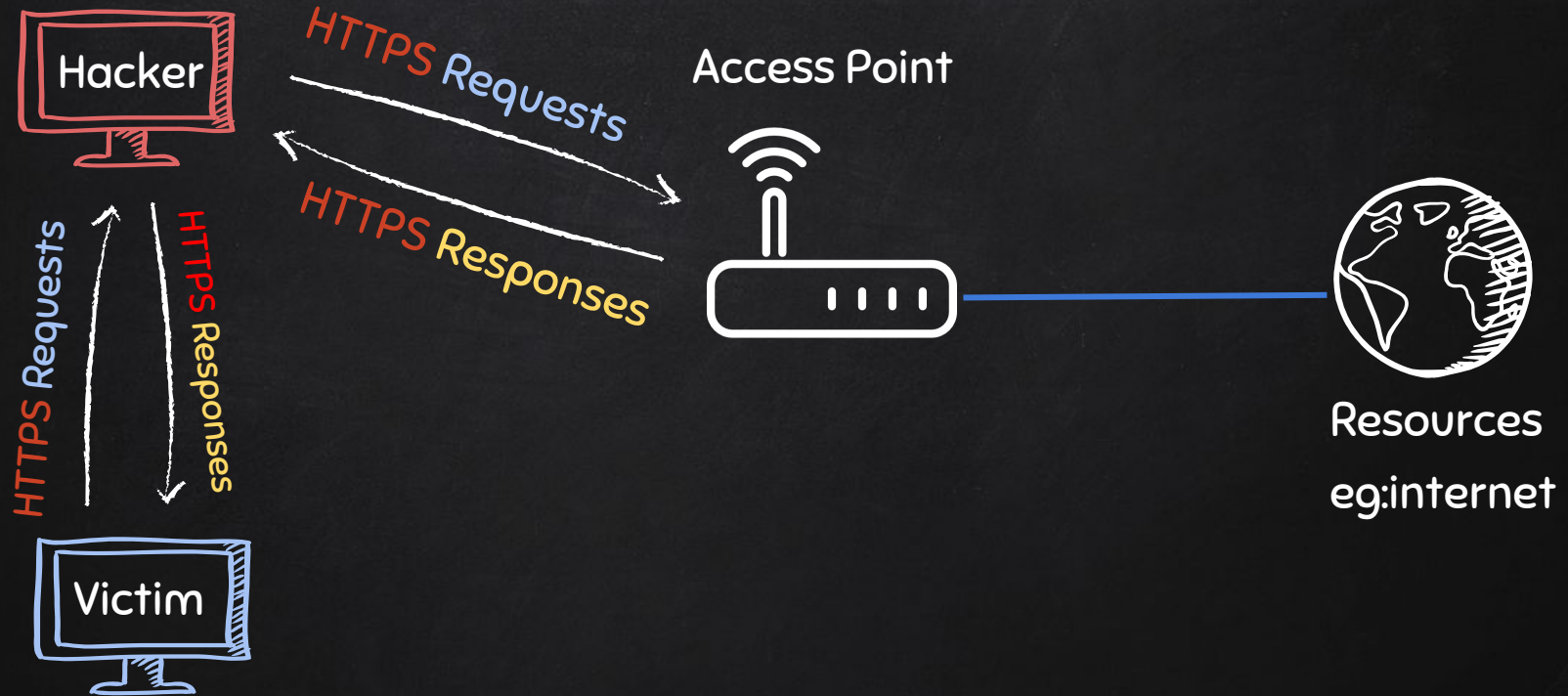
ARP SPOOFING



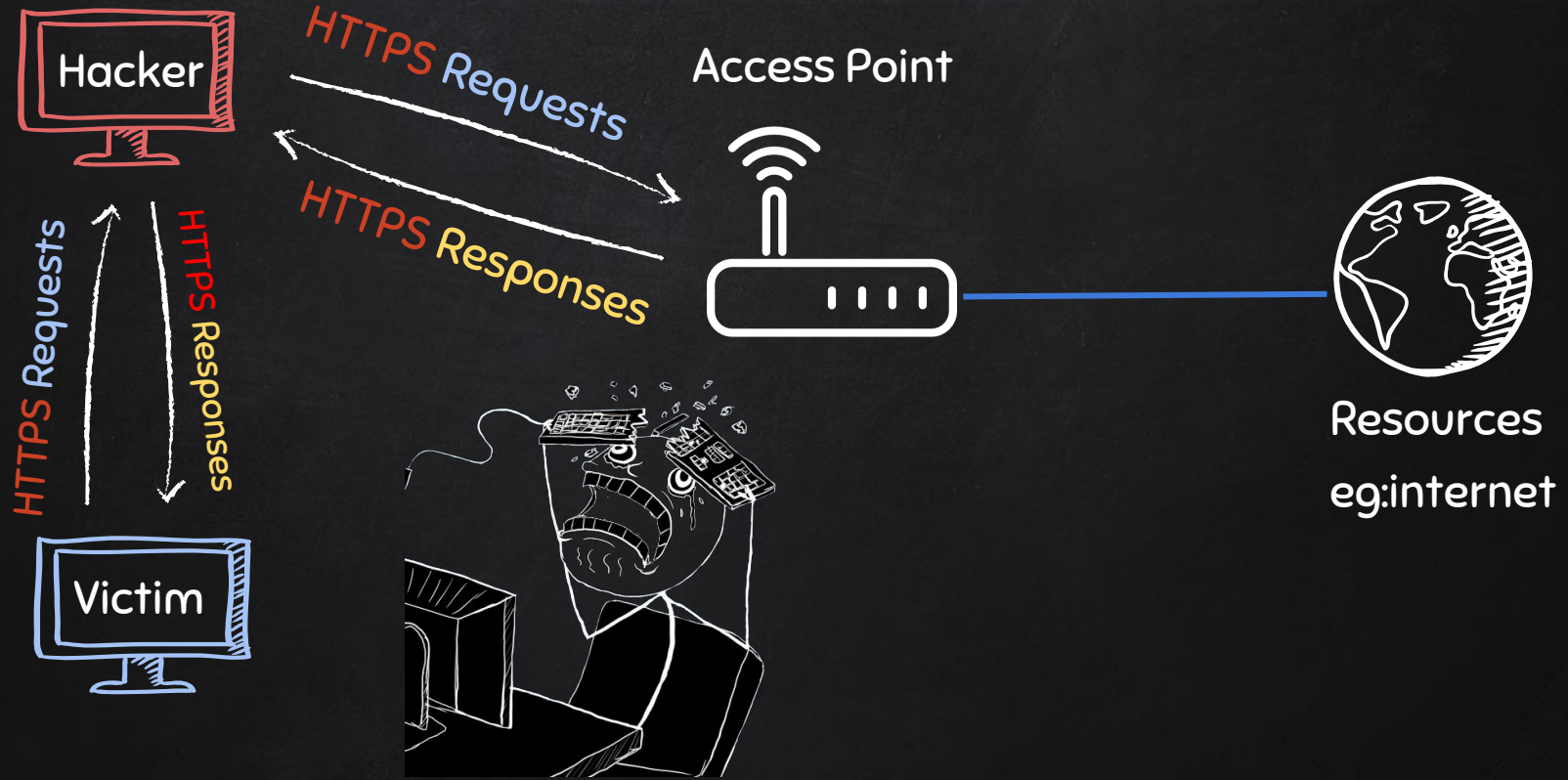
ARP SPOOFING



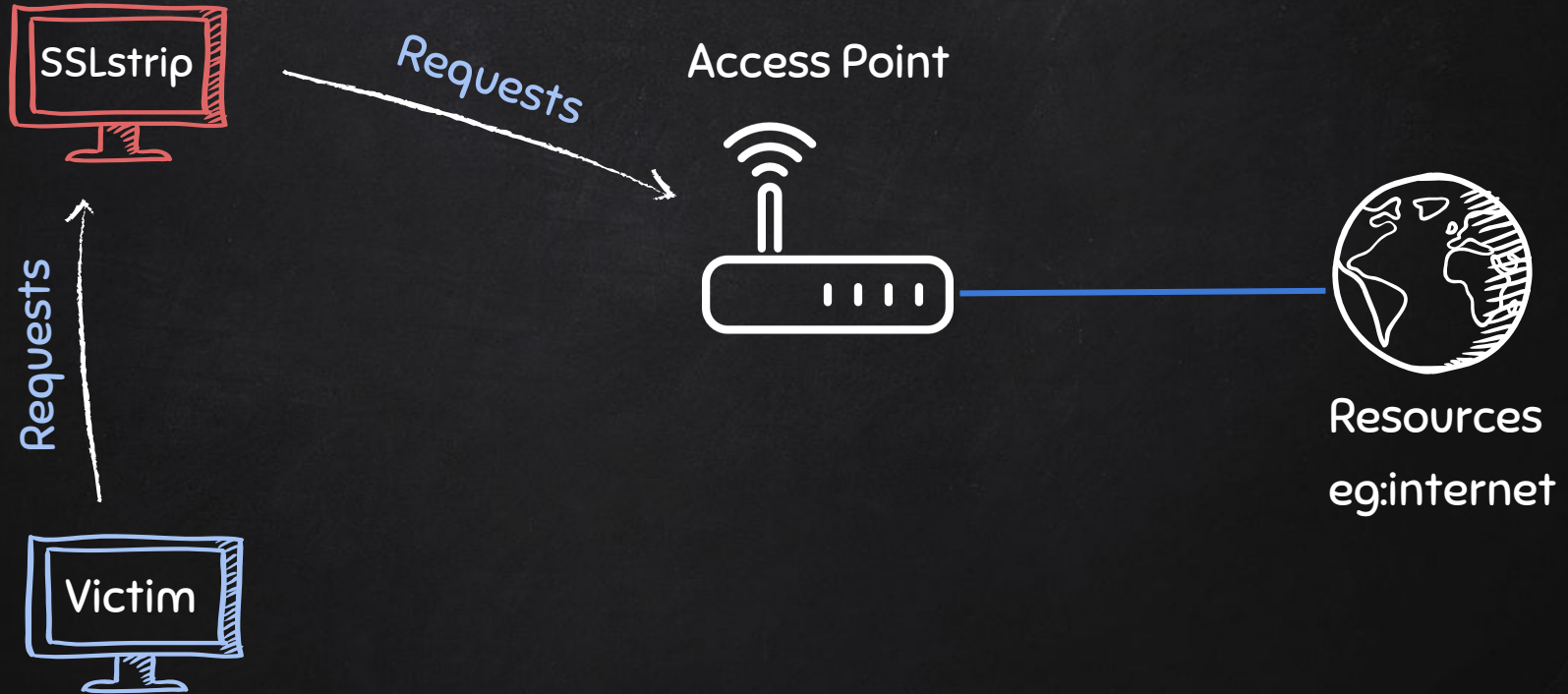
ARP SPOOFING



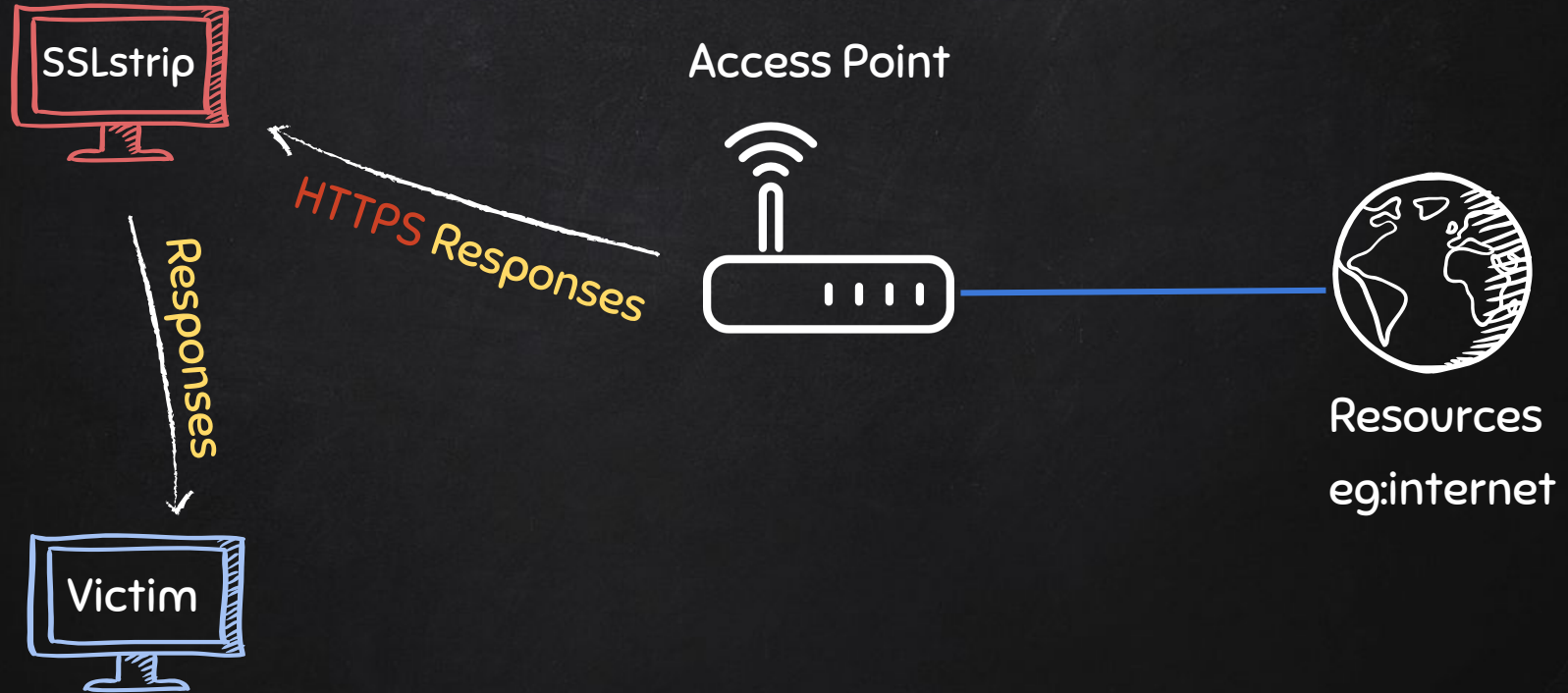
ARP SPOOFING



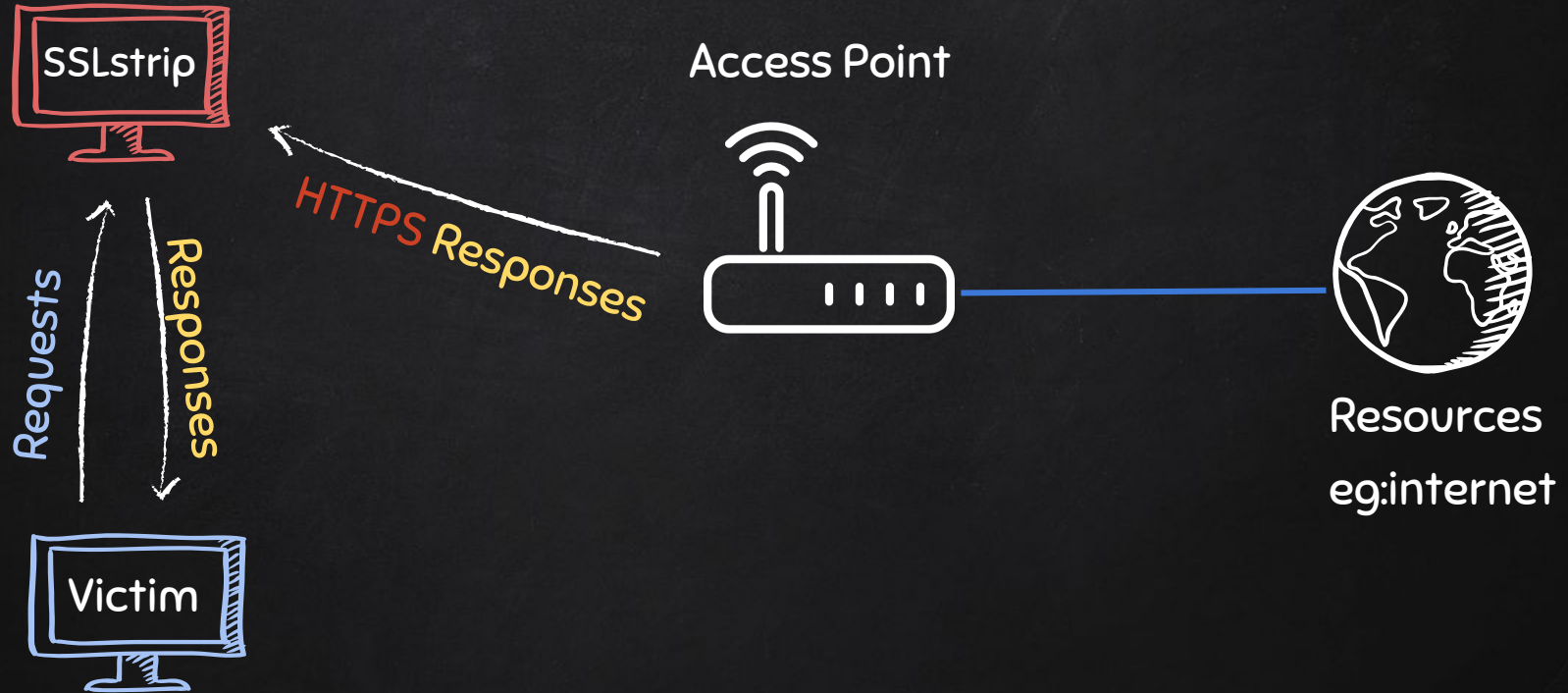
ARP SPOOFING WITH SSLSTRIP



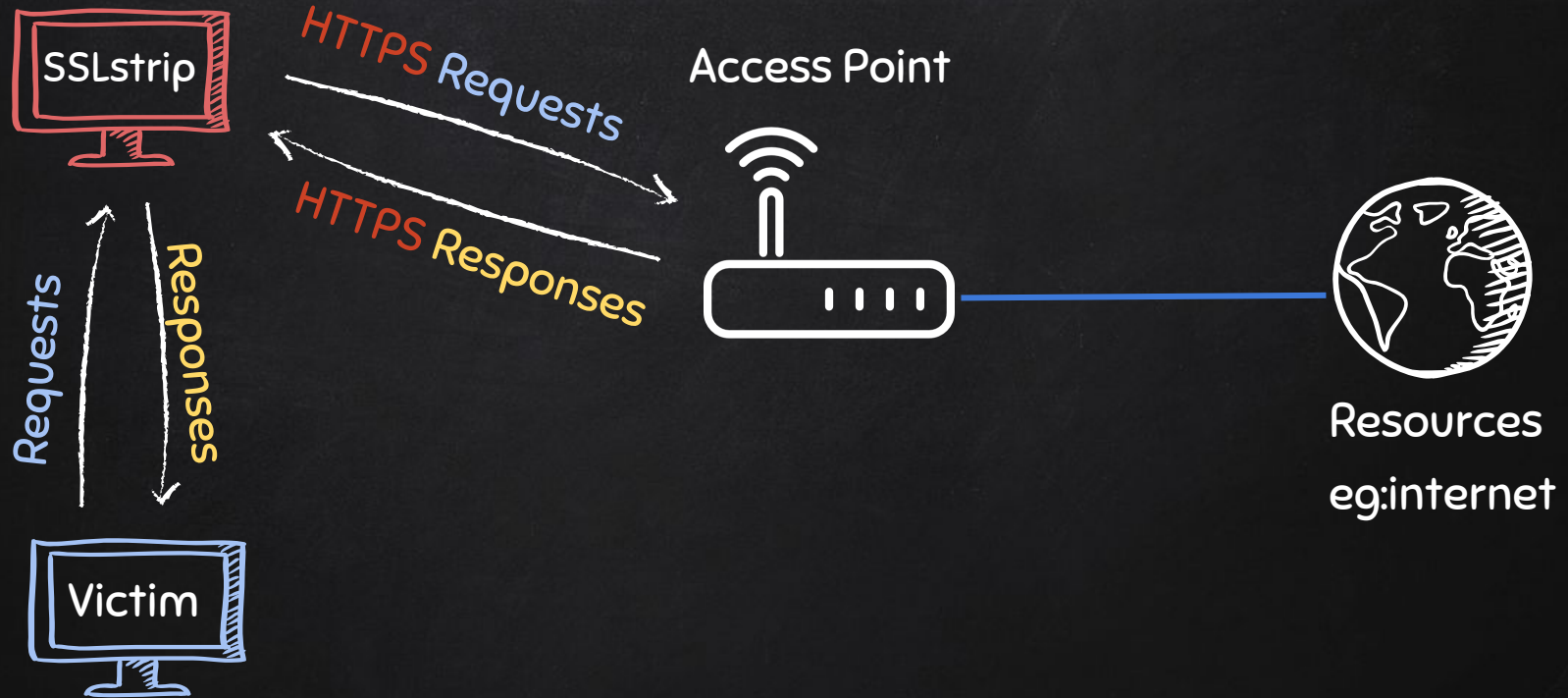
ARP SPOOFING WITH SSLSTRIP



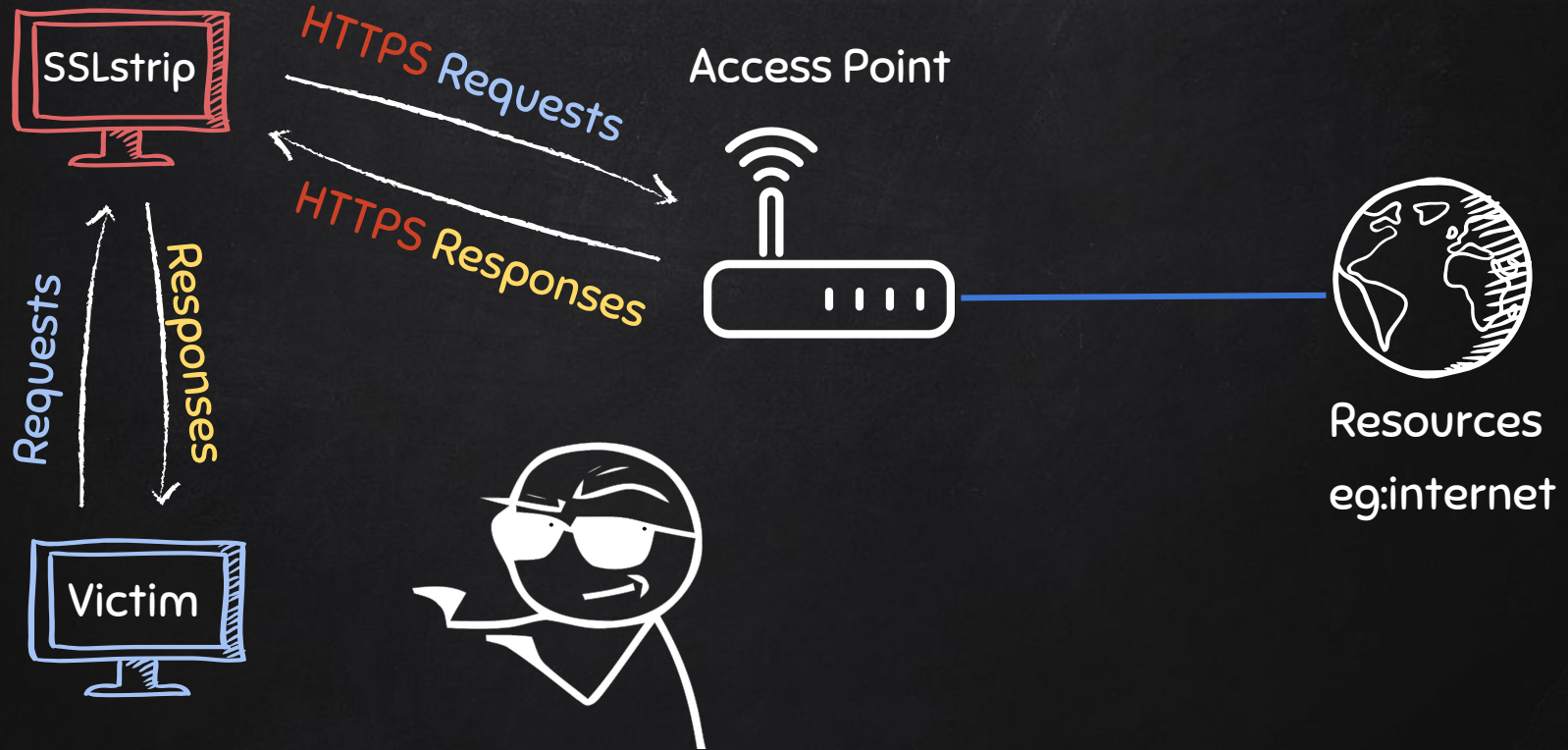
ARP SPOOFING WITH SSLSTRIP



ARP SPOOFING WITH SSLSTRIP



ARP SPOOFING WITH SSLSTRIP



PYTHON ON WINDOWS

- Python programs needs an **interpreter** to run.
- Most Linux distros come with a built-in python interpreter.
- Python can be manually installed on Windows.
- Allows Windows to run python programs.

*Note: this is a **python interpreter not a linux emulator**, if your program relies on Linux commands or operations only available in Linux then the program will not run properly.*

ARPSPOOF_DETECTOR

- Watch value for gateway mac in the arp table
 - Nice and simple, but will **not** detect an attack if the tool is executed after the attack.
- Analyse 'is-at' ARP responses:
 - Check if IP is gateway ip.
 - Check if source mac is actually the gateway's mac.
 - This method will detect attacks even if the attack was launched before the execution of the tool.

