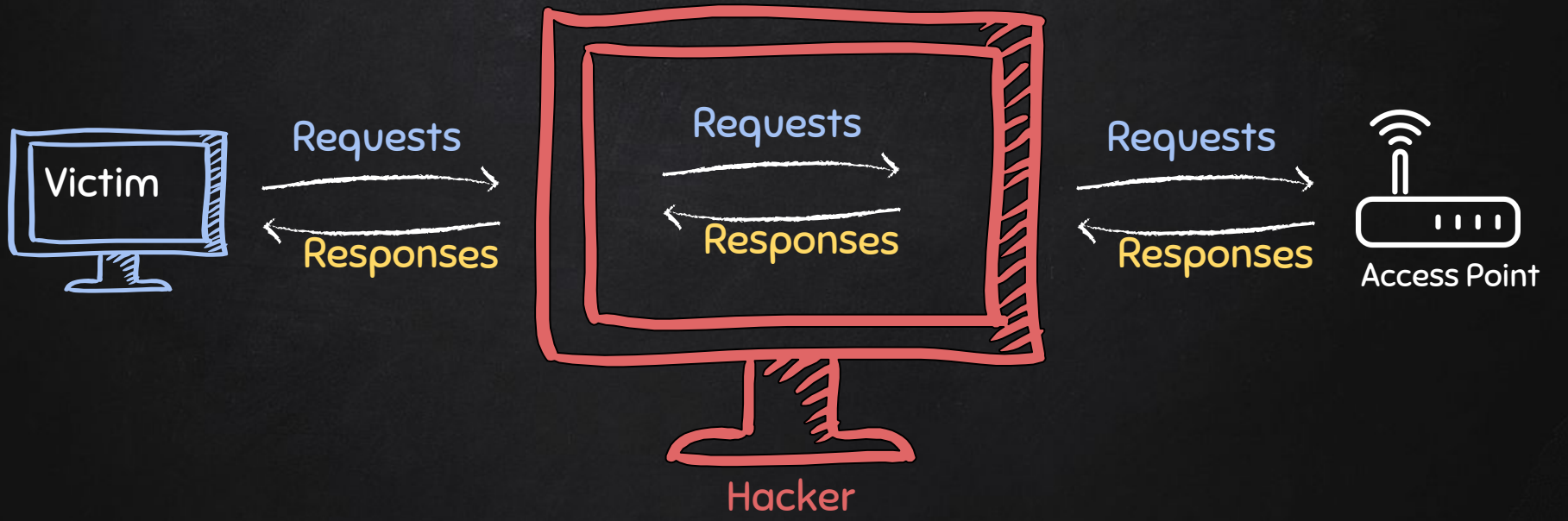
Intercepting & Modifying Packets

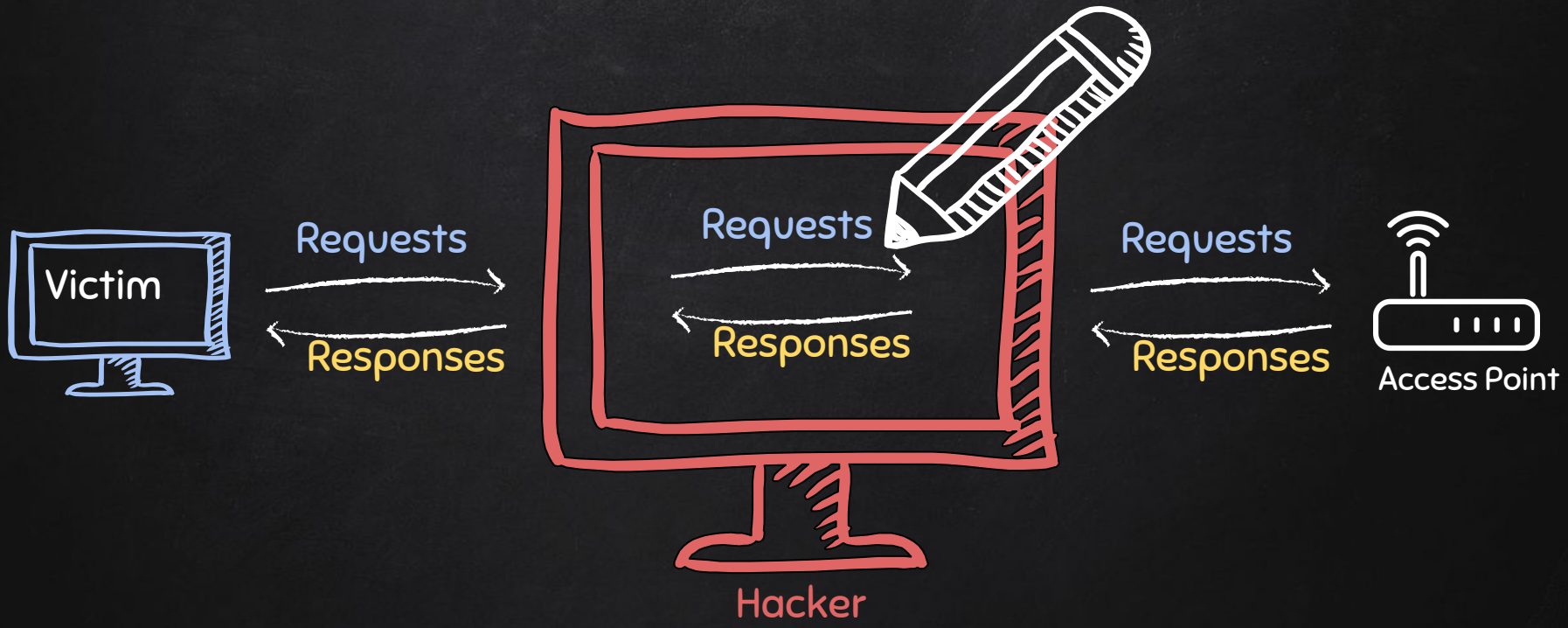
- Scapy can be used to:
  - Create packets.
  - Analyse packets.
  - Send/receive packets.
- But it can't be used to intercept packets/flows.

Classic MITM Scenario

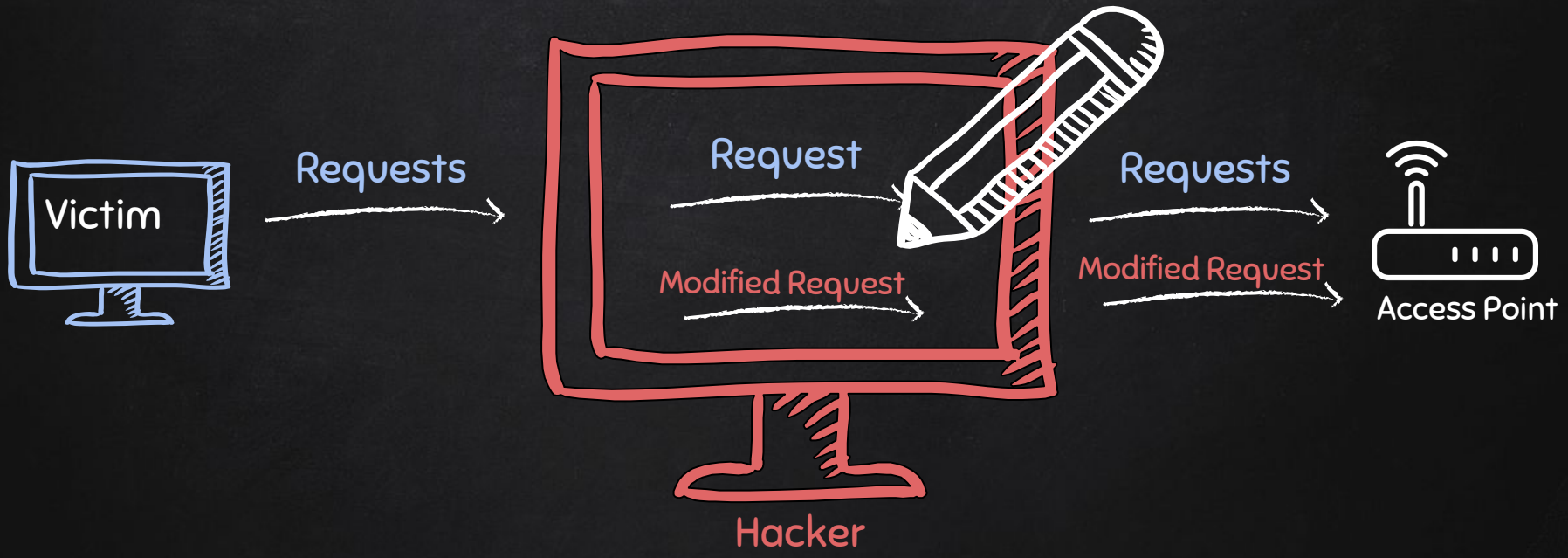


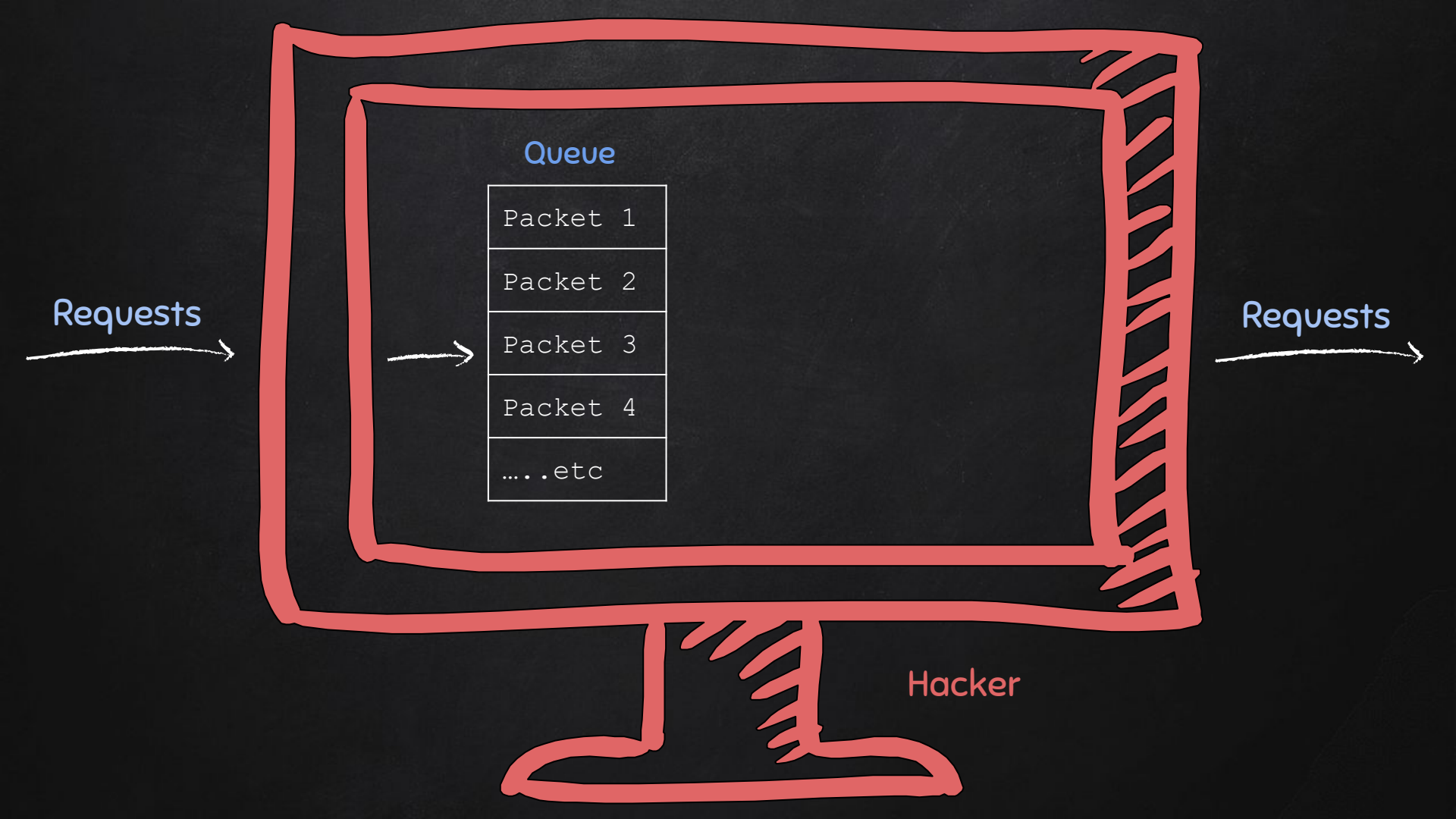
MITM - Sniffing Data

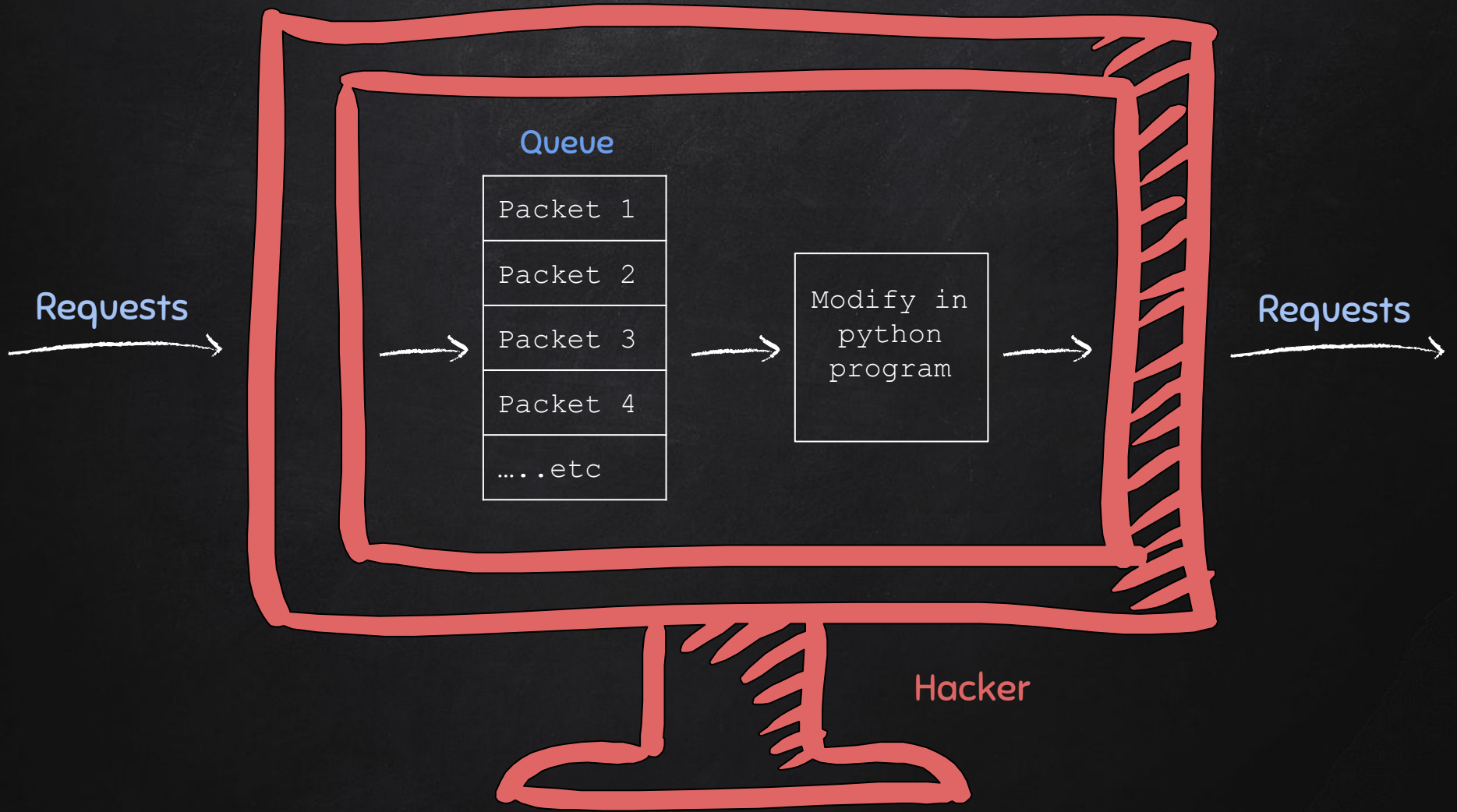
MITM – Modifying Data

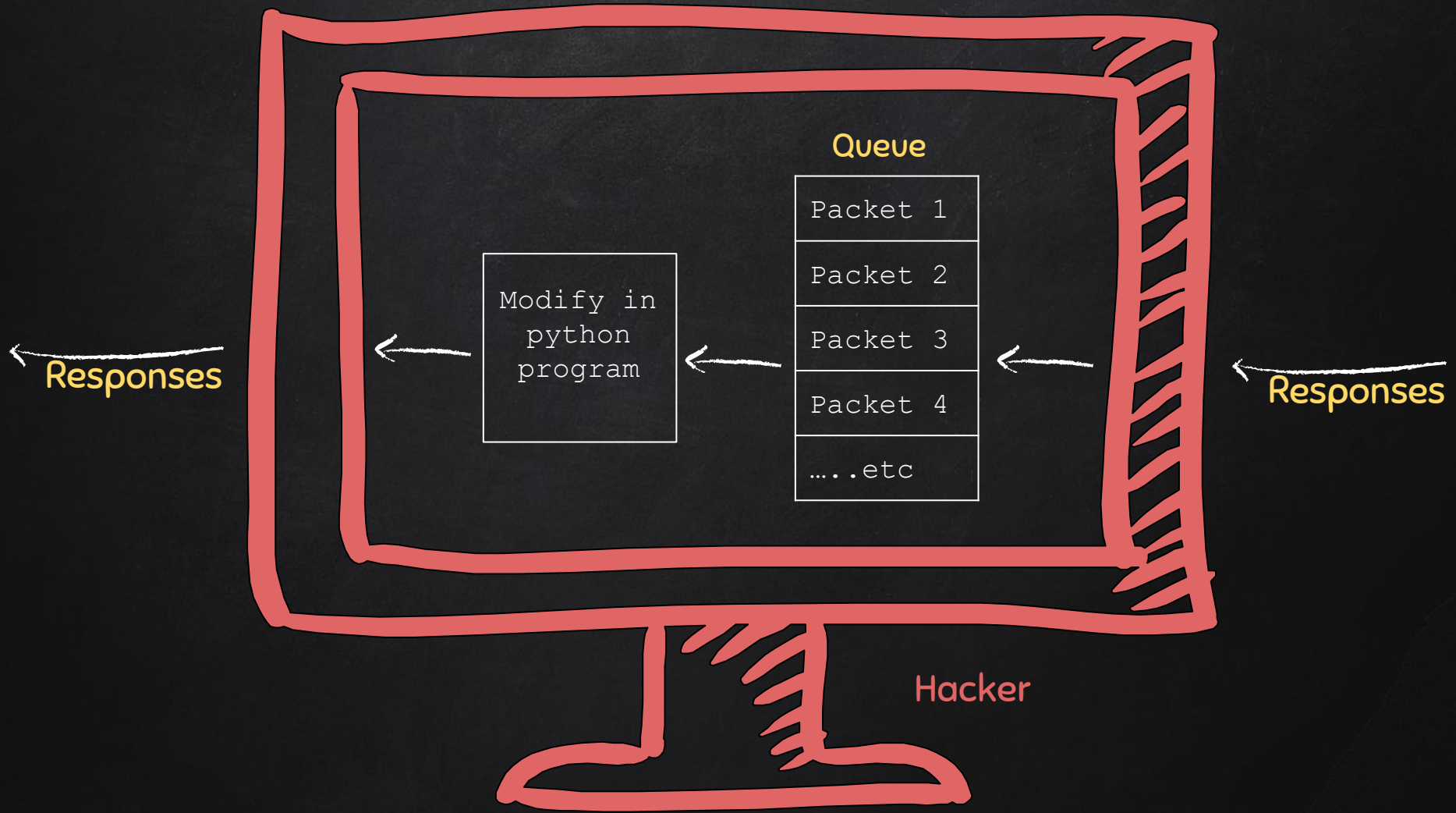


MITM - Modifying Data



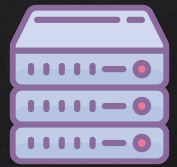

Requests
Queue
Packet 1
Packet 2
Packet 3
Packet 4
…..etc
Requests
Hacker


Requests
Queue
Packet 1
Packet 2
Packet 3
Packet 4
…..etc
Modify in python program
Requests
Hacker


Queue
Packet 1
Packet 2
Packet 3
Packet 4
…..etc
Modify in python program
Responses
Responses
Hacker

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

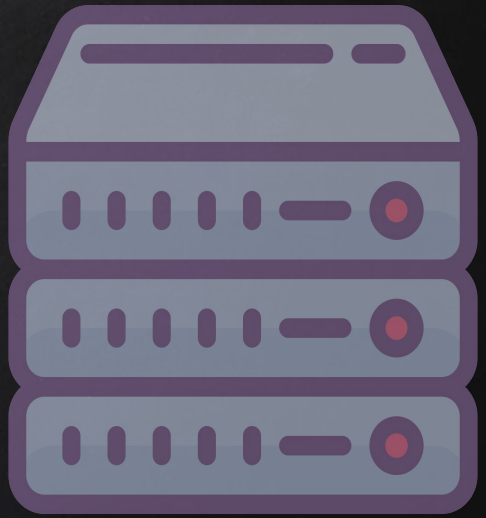
BING.COM WEB SERVER
204.79.197.200

BING.COM

DNS SERVER

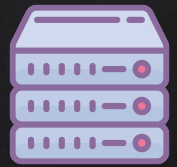
DNS Records

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

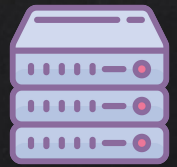
Bing.com web server
204.79.197.200



DNS server

Bing.com web server
204.79.197.200

facebook.com web server
195.44.2.1



DNS server

FACEBOOK.COM WEB SERVER
195.44.2.1

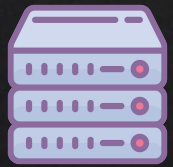
BING.COM WEB SERVER
204.79.197.200

BING.COM

DNS SERVER

Bing.com web server
204.79.197.200

facebook.com web server
195.44.2.1



DNS server

Requests

Responses

Requests

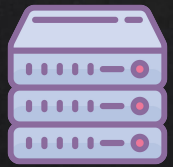
Responses

FACEBOOK.COM WEB SERVER
195.44.2.1

BING.COM WEB SERVER
204.79.197.200

bing.com

HACKER WEB SERVER
10.0.2.16



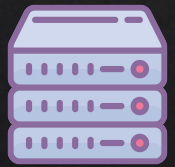
DNS SERVER

facebook.com web server
195.44.2.1

Bing.com web server
204.79.197.200

bing.com

Hacker web server
10.0.2.16

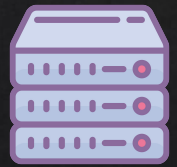


DNS server

FACEBOOK.COM WEB SERVER
195.44.2.1

BING.COM WEB SERVER
204.79.197.200

HACKER WEB SERVER
10.0.2.16



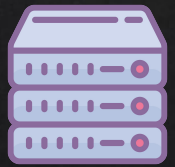
DNS SERVER

FACEBOOK.COM WEB SERVER
195.44.2.1

BING.COM WEB SERVER
204.79.197.200

10.0.2.16

HACKER WEB SERVER
10.0.2.16



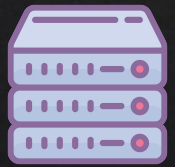
DNS SERVER

FACEBOOK.COM WEB SERVER
195.44.2.1

BING.COM WEB SERVER
204.79.197.200

winzip.exe

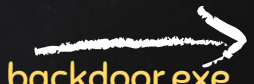
HACKER WEB SERVER
10.0.2.16



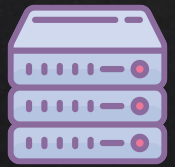
DNS SERVER

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

HTTPS

Problem:

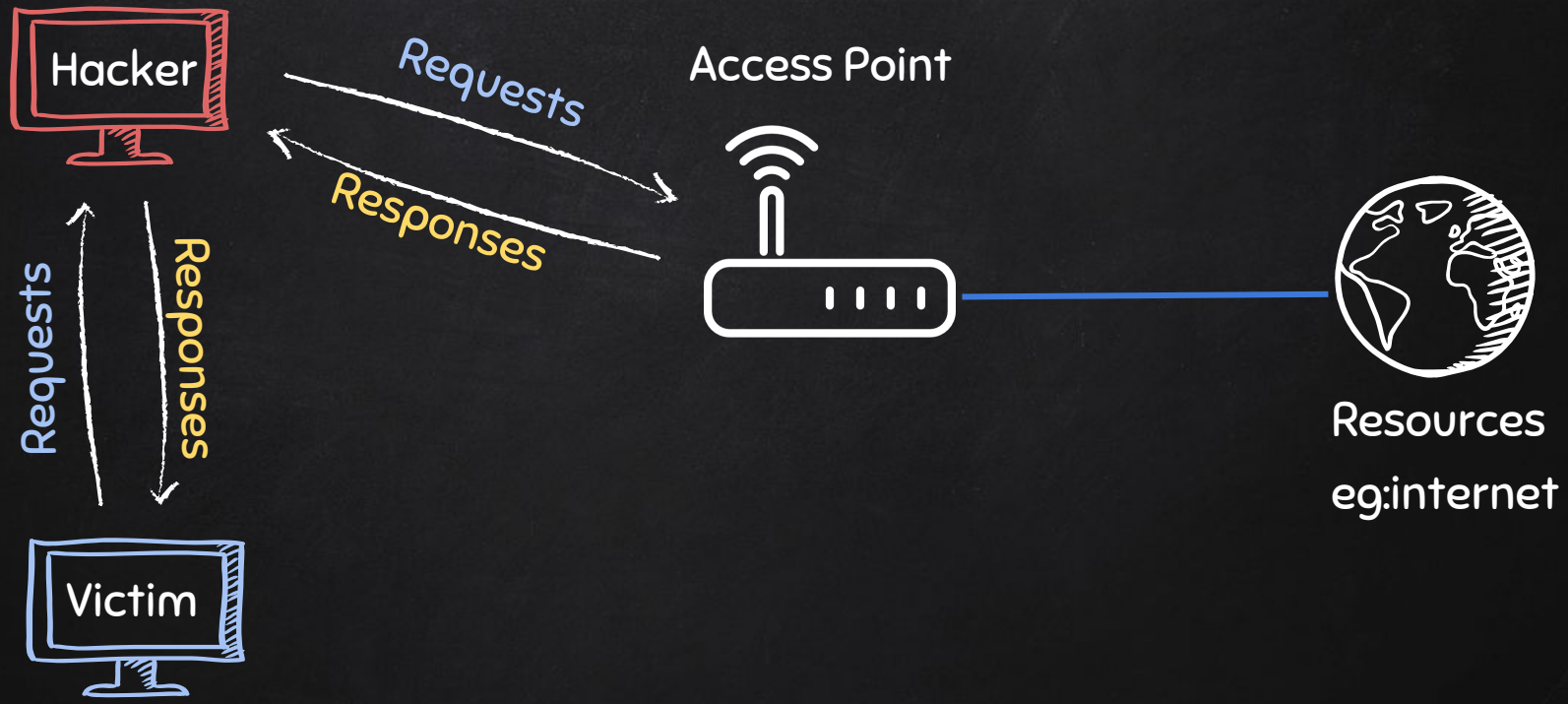
- Data in HTTP is sent as plain text.
- A MITM can read and edit requests and responses.

→ not secure

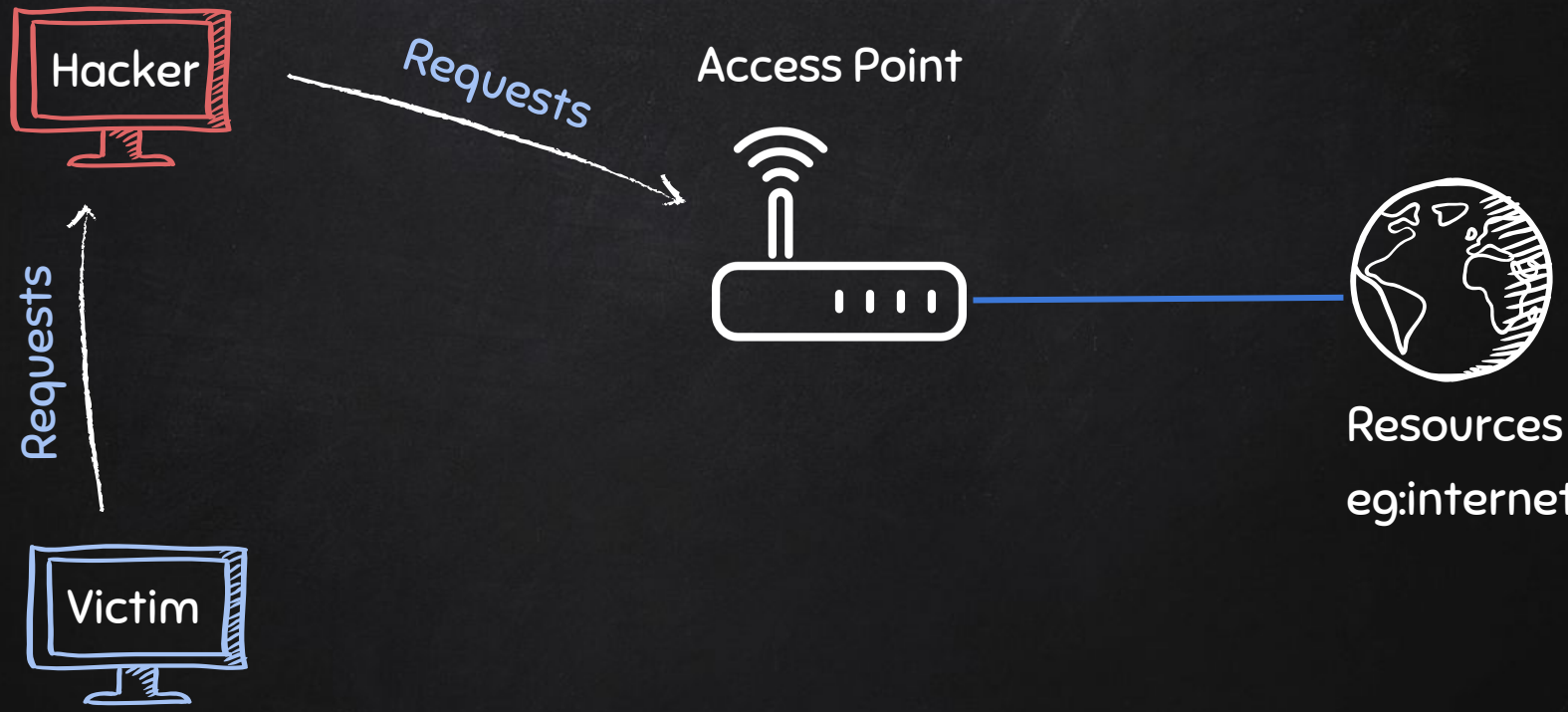
Solution:

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

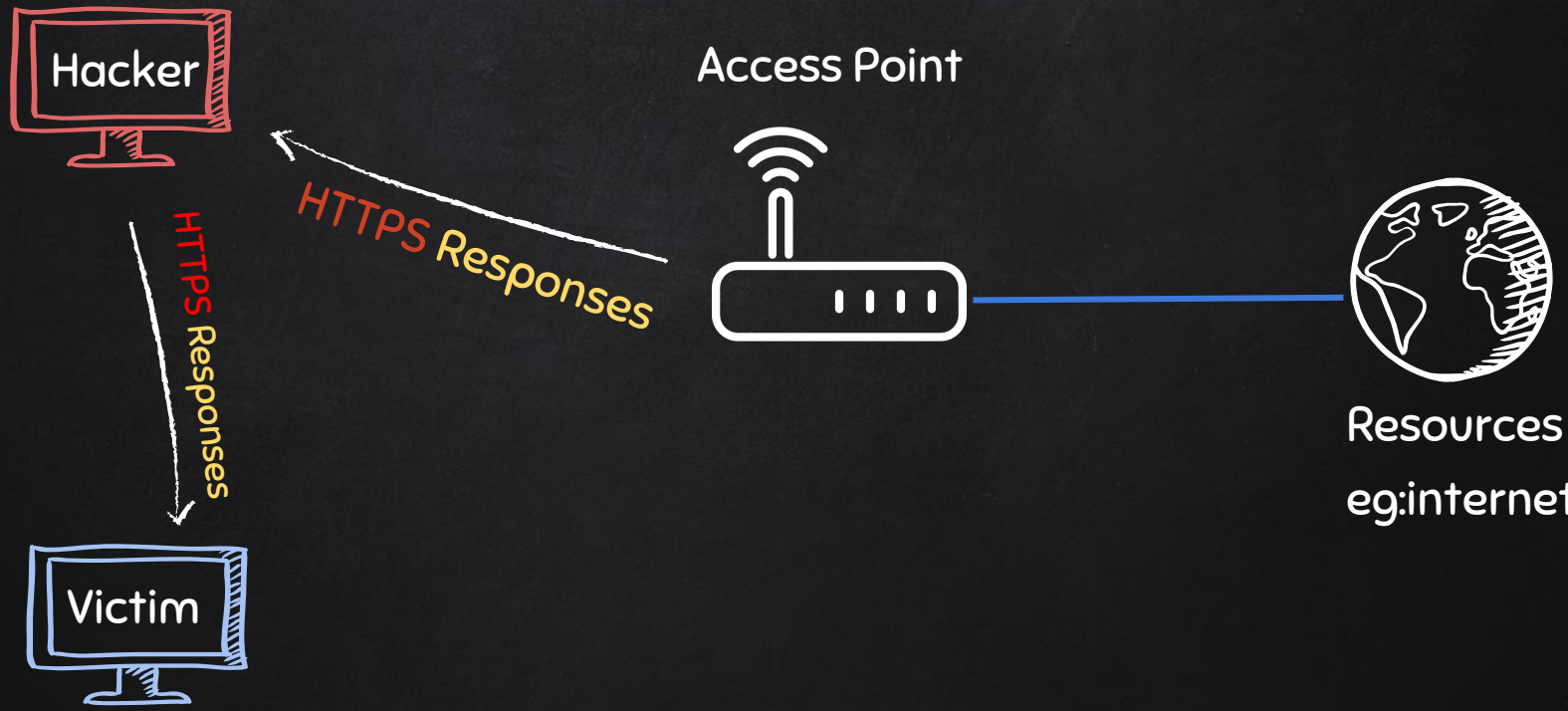
ARP Spoofing



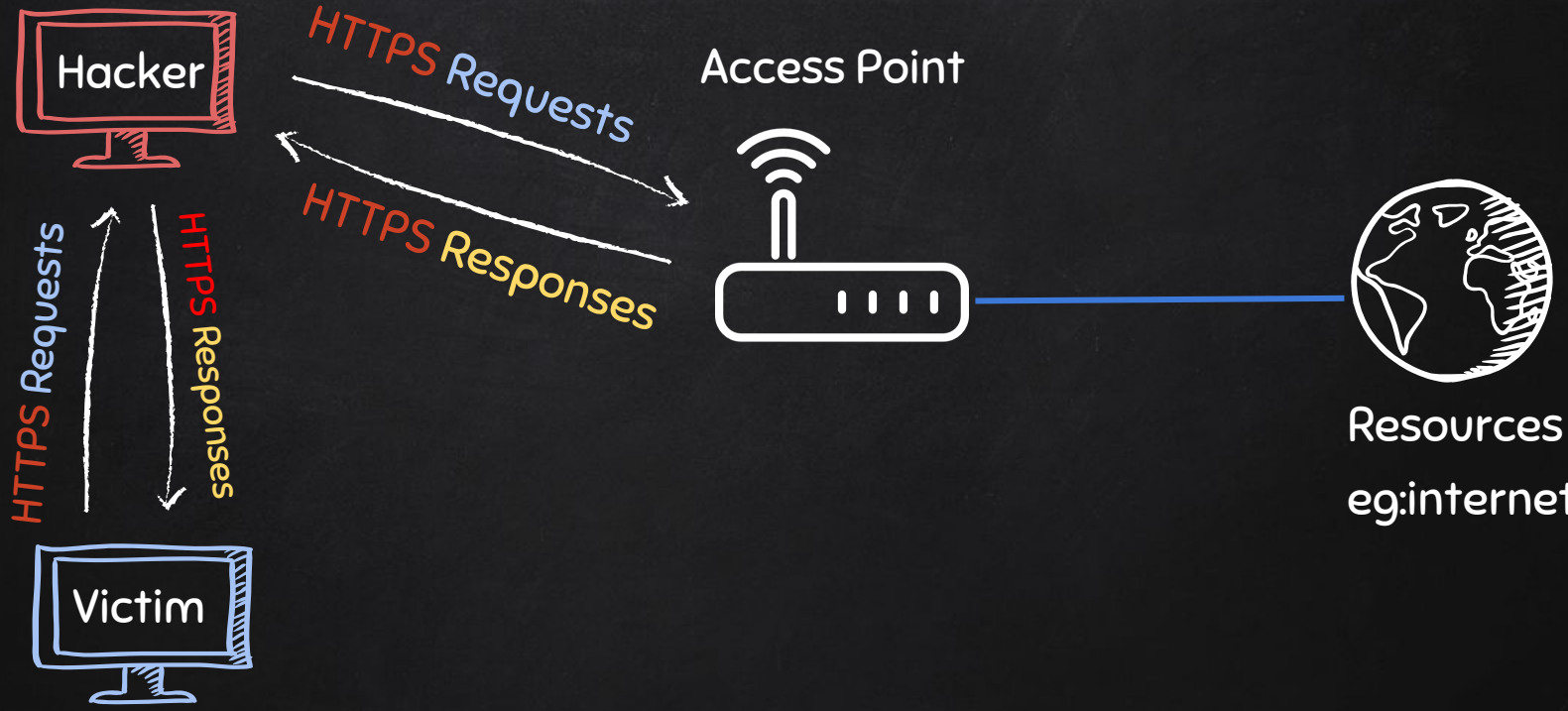
ARP Spoofing



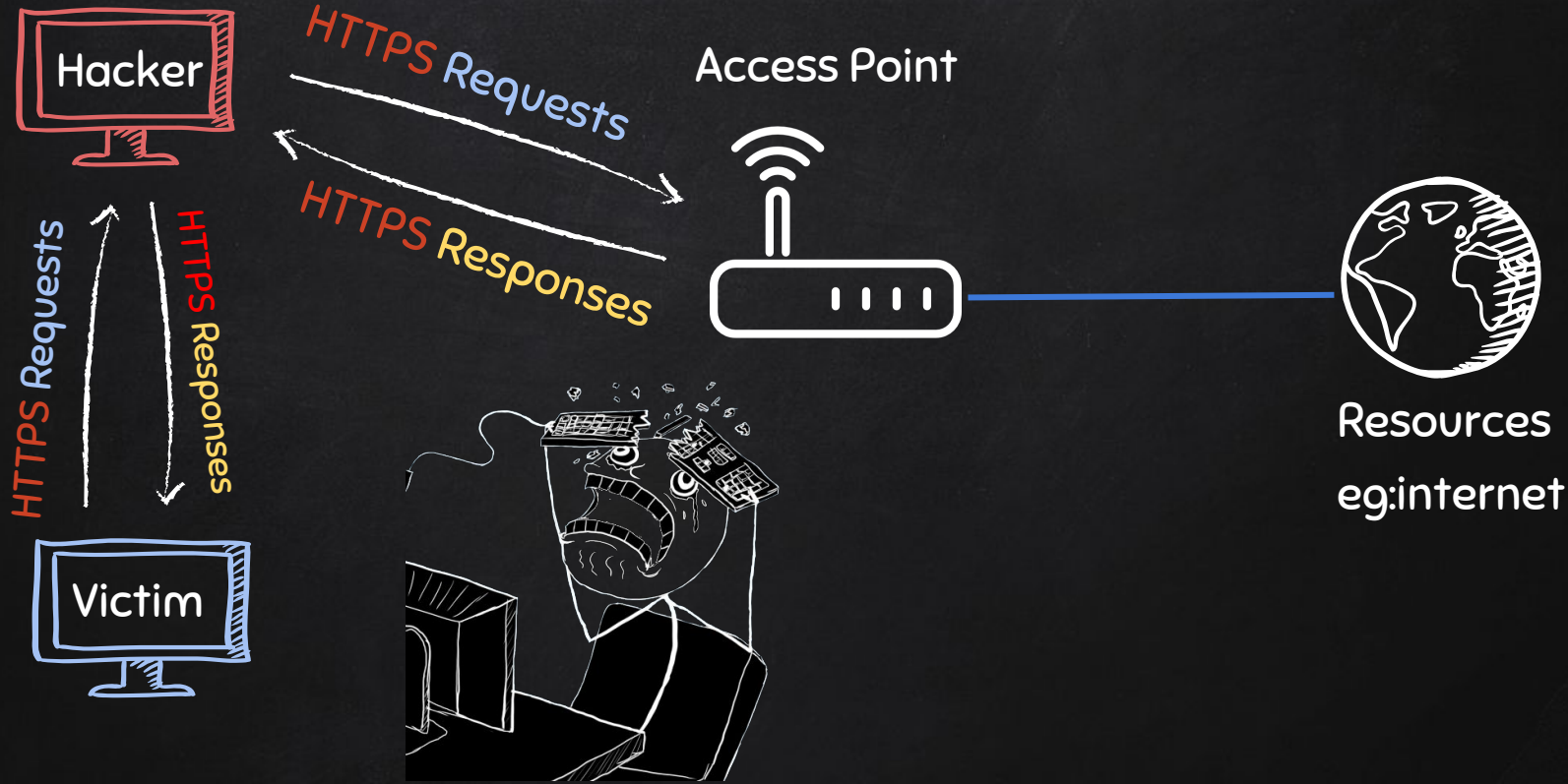
ARP Spoofing



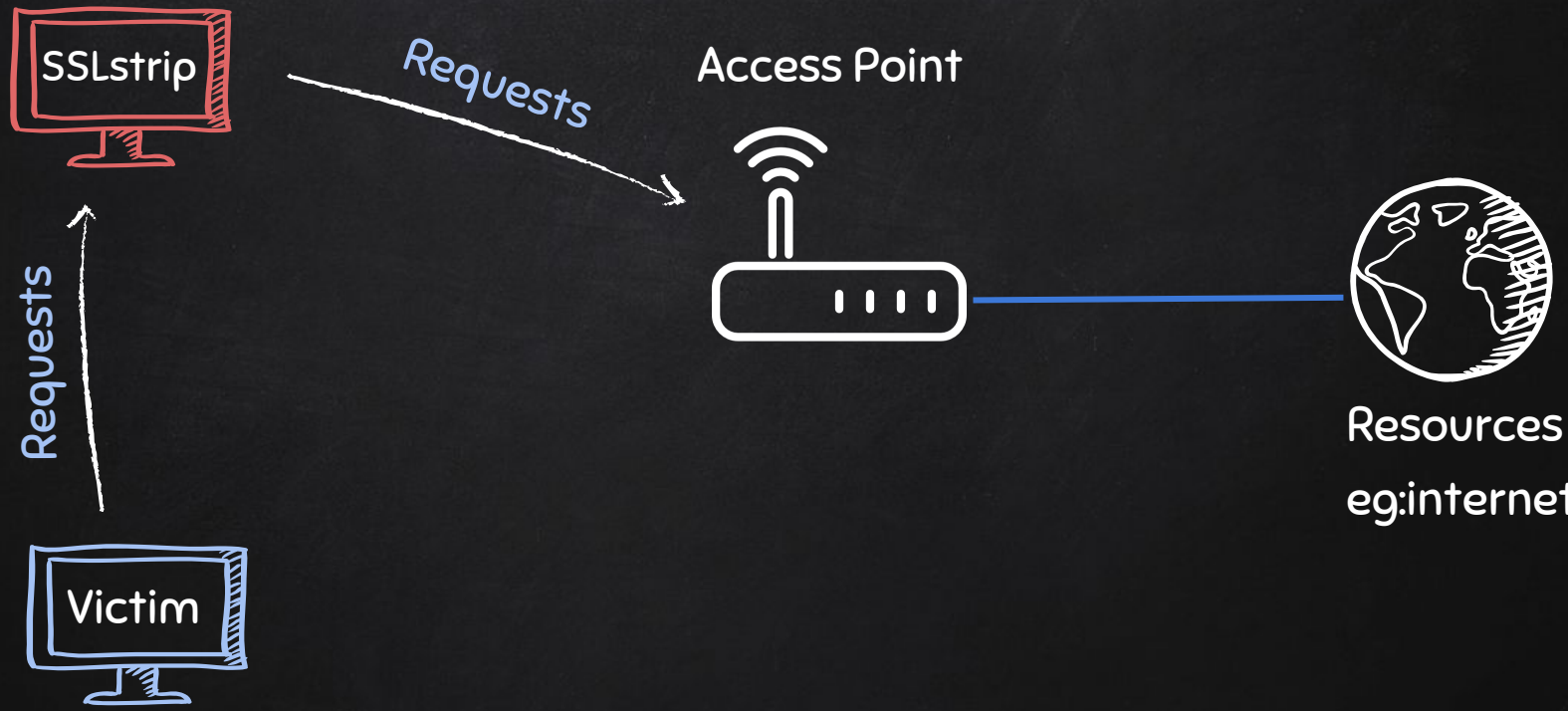
ARP Spoofing



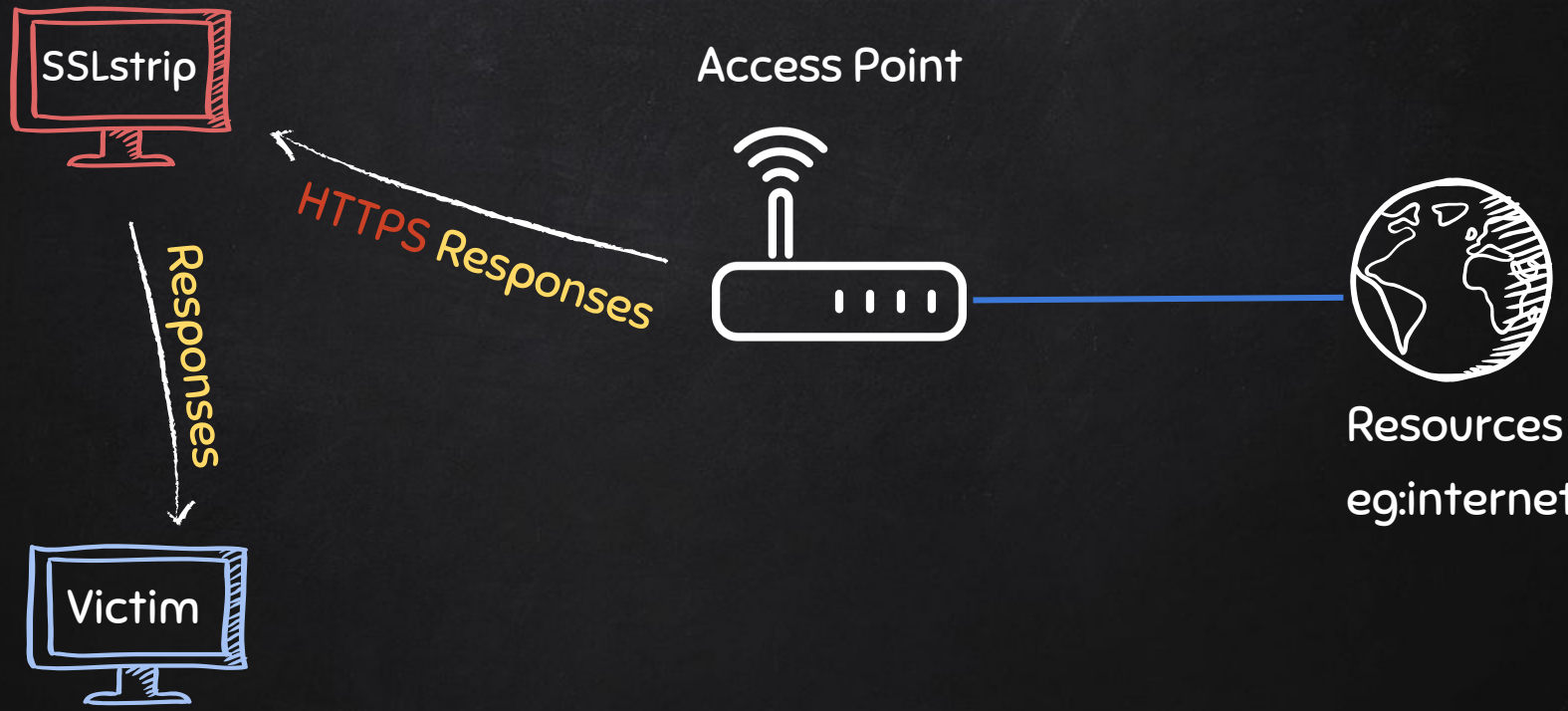
ARP Spoofing



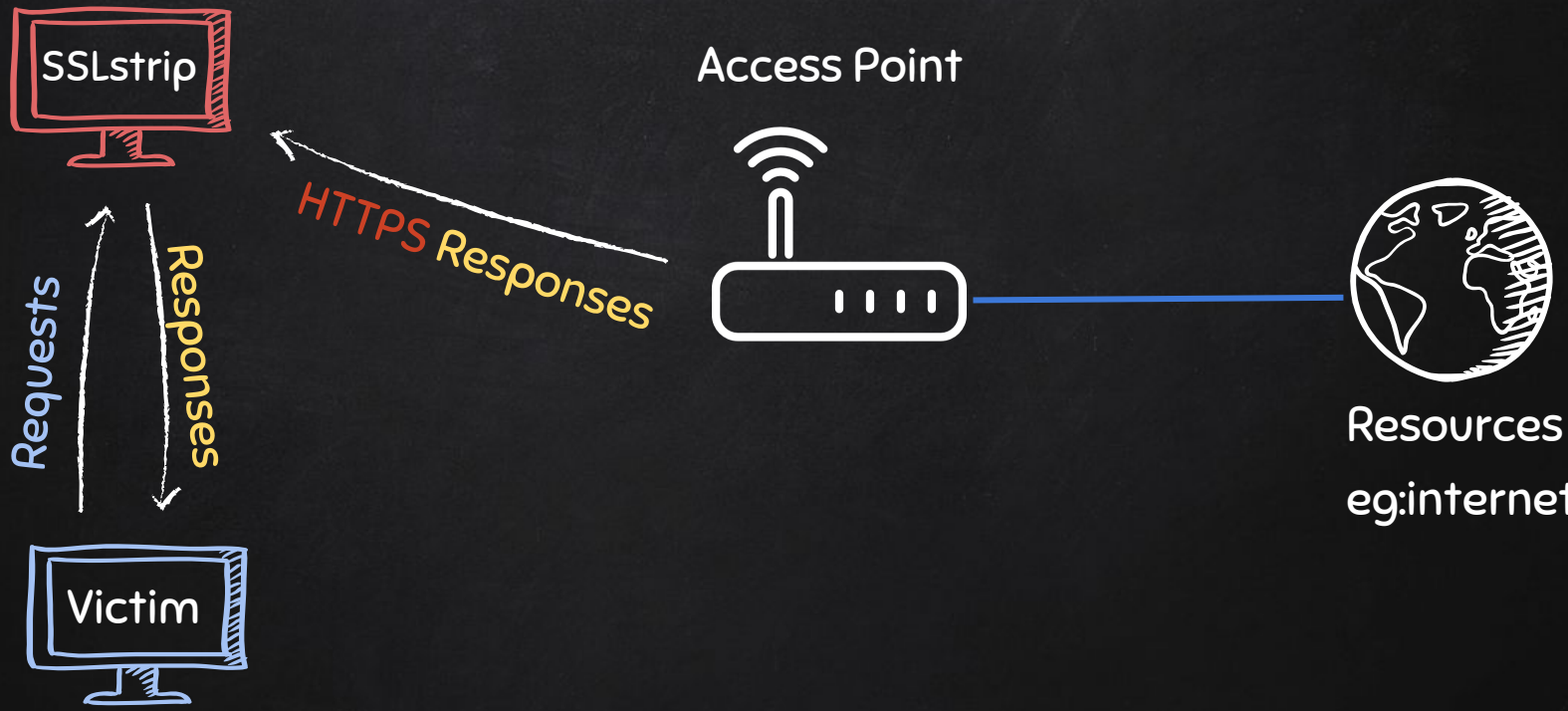
ARP Spoofing With SSLstrip



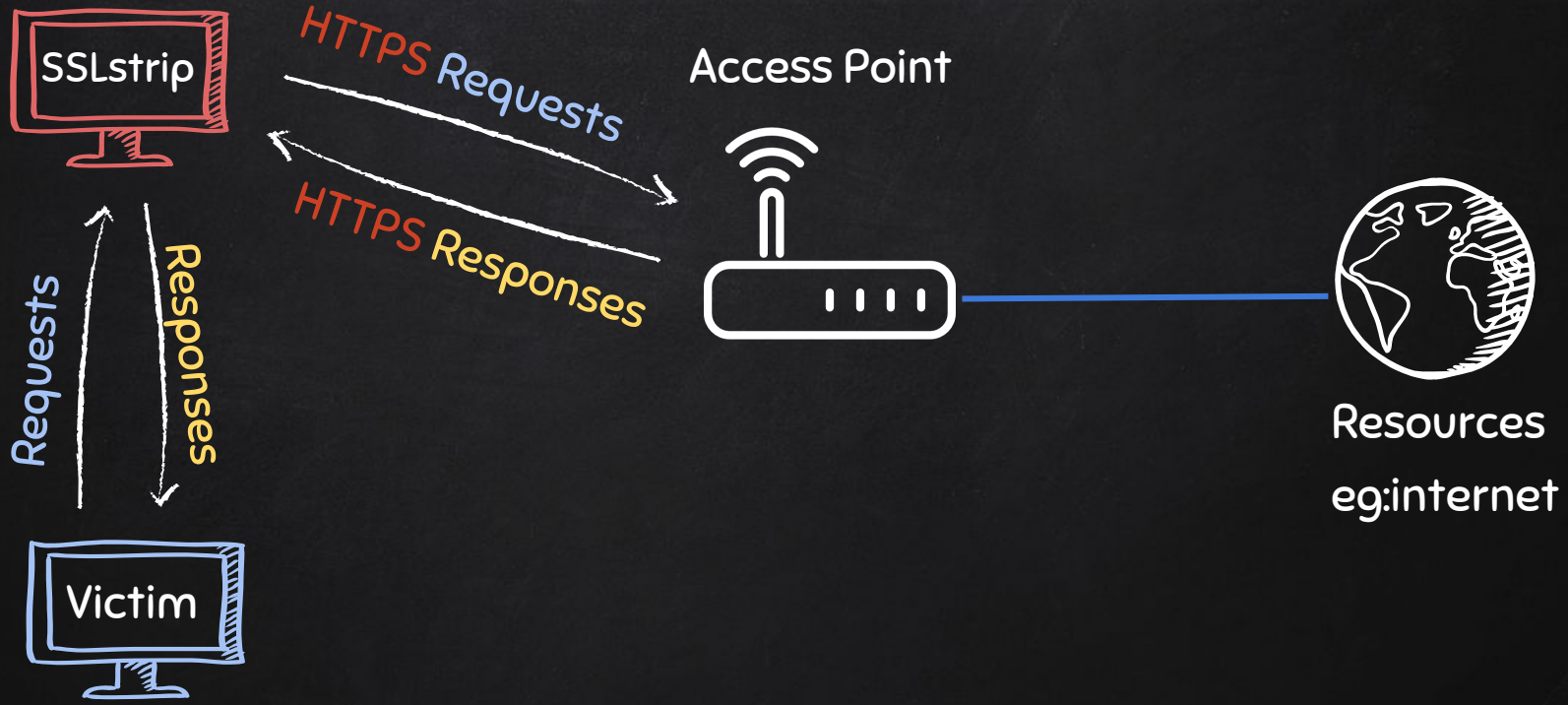
ARP Spoofing With SSLstrip



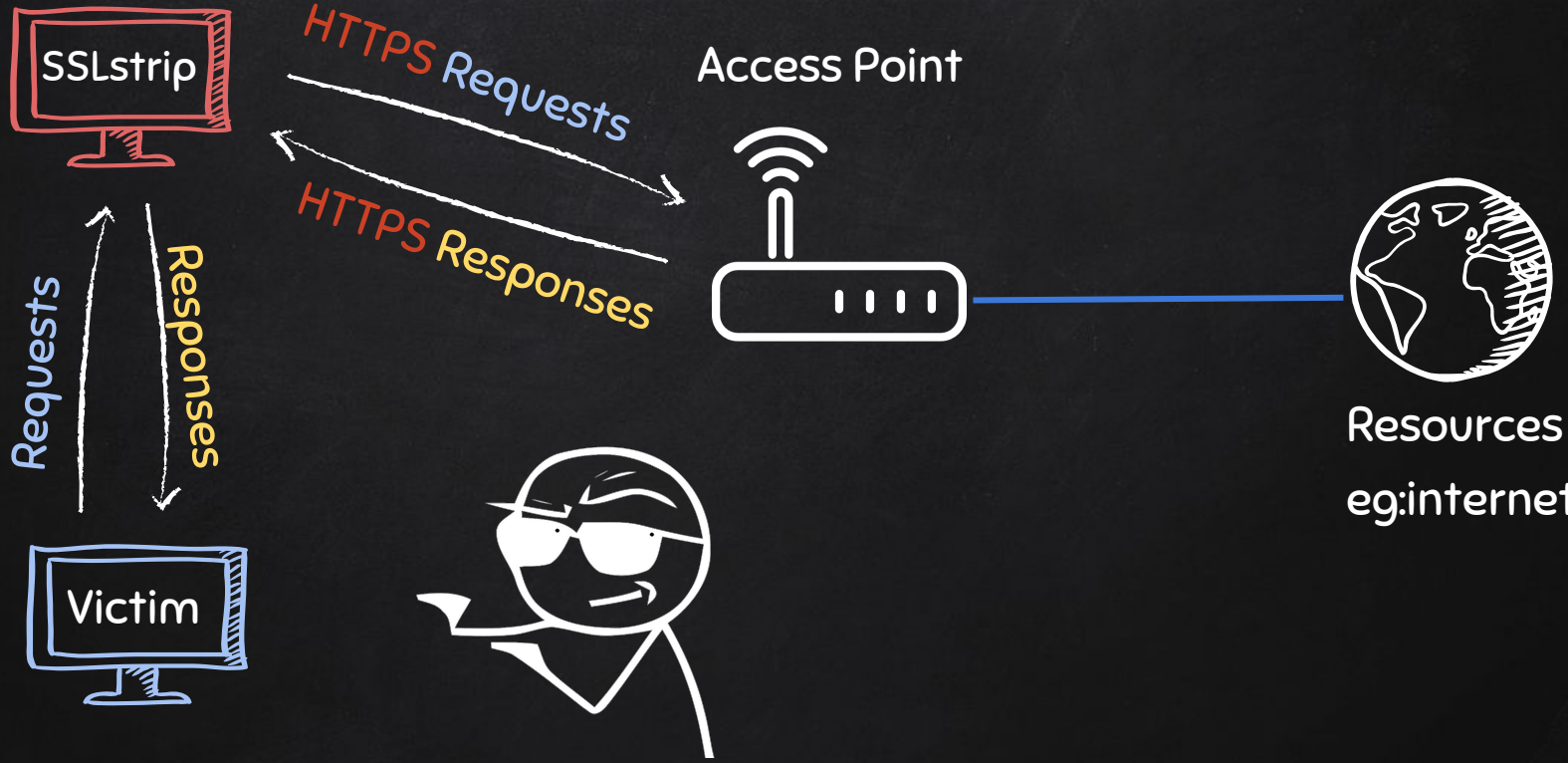
ARP Spoofing With SSLstrip



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.