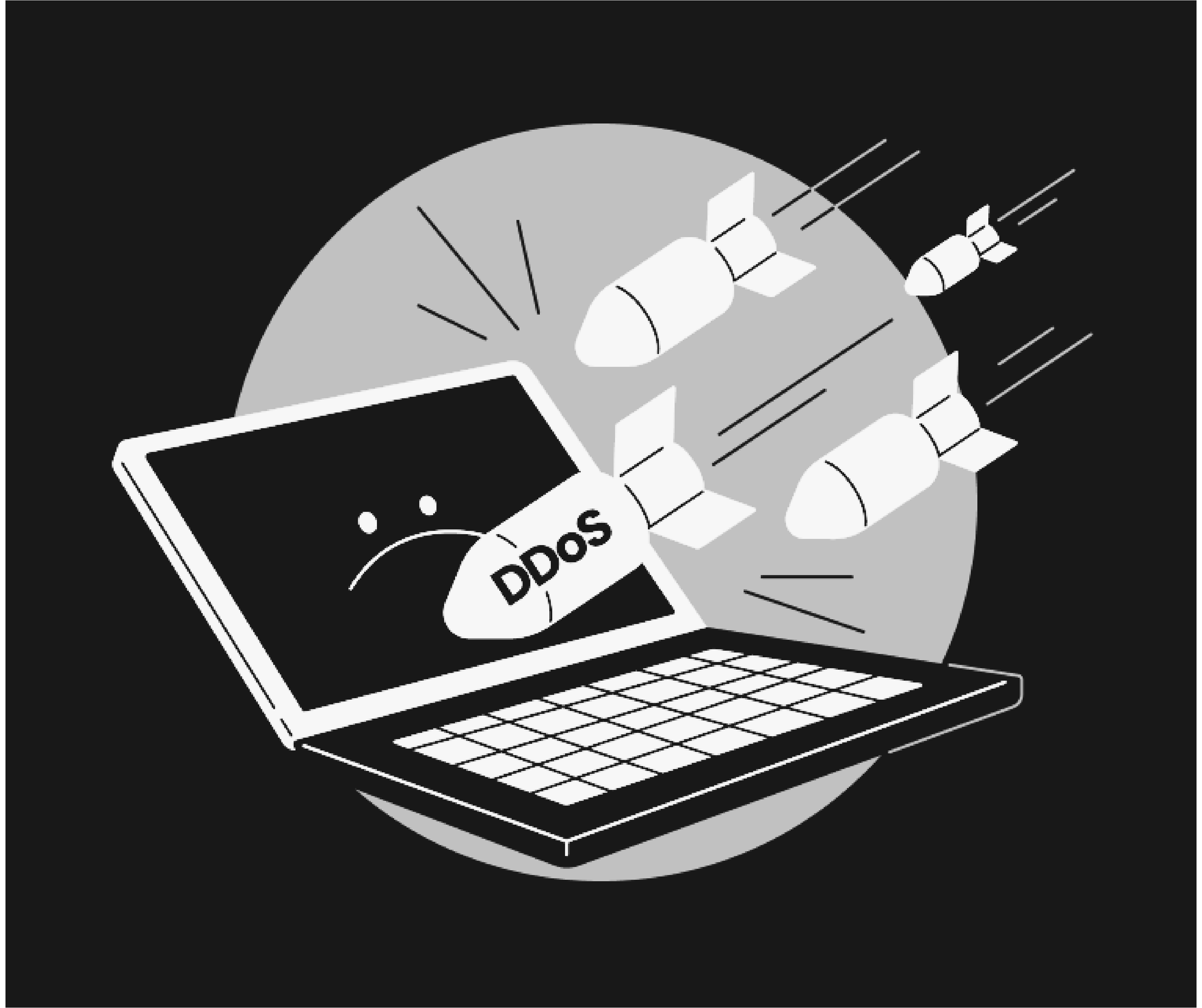
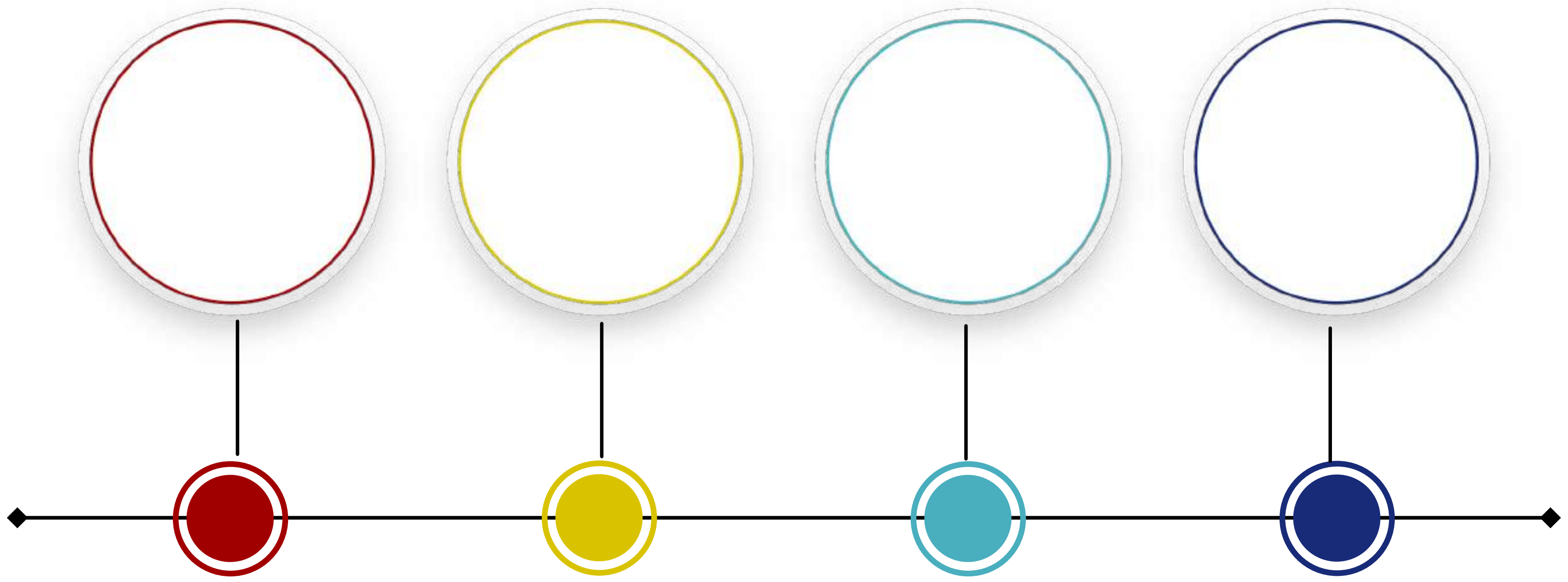
VIETNIX

WEB ATTACK & DEFEND

- DANG TUAN -



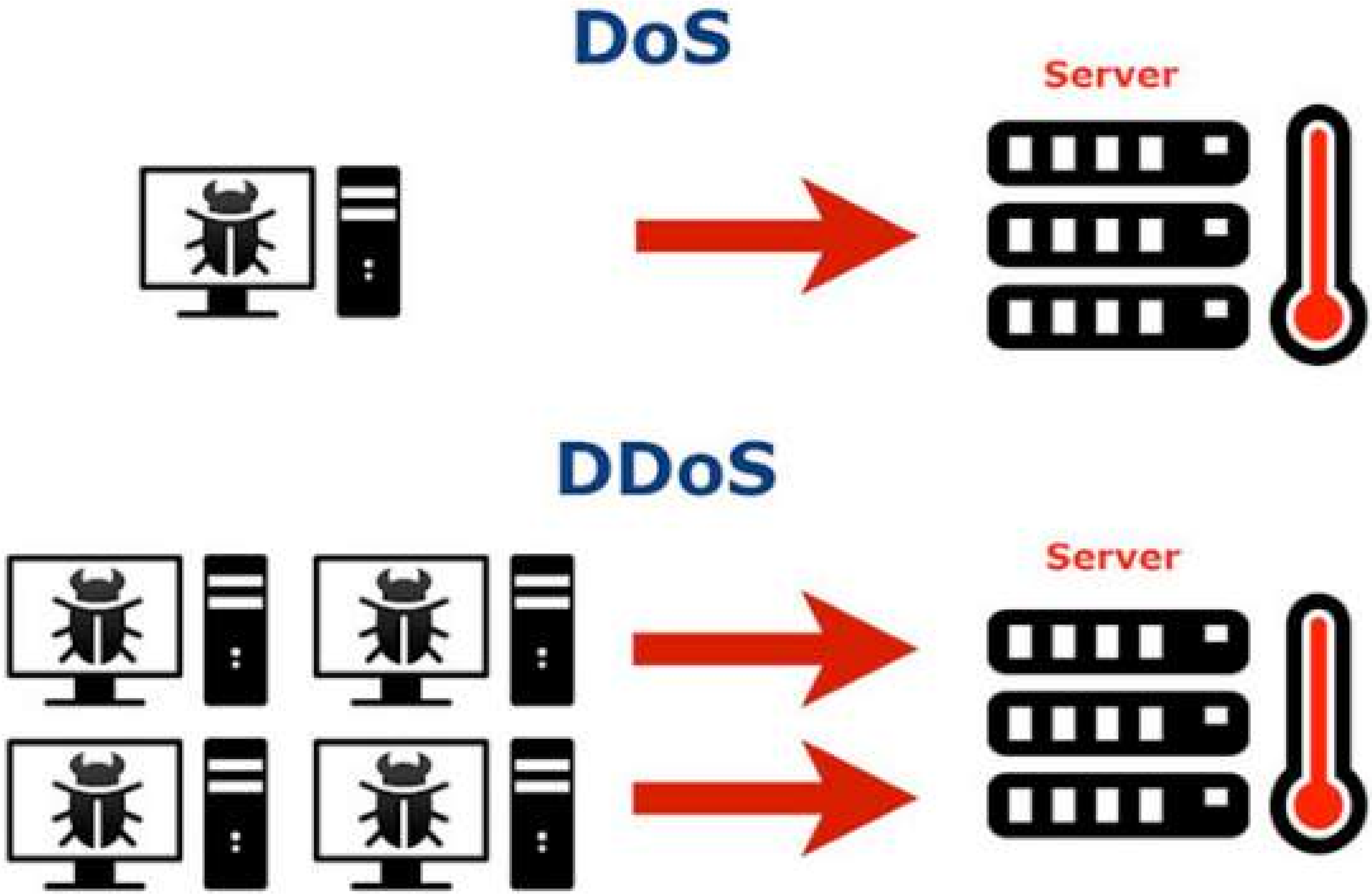
fb.com/nightbarron.dt



Nội dung chính

- Tổng quan về DDOS
- Application Attack
- Tư duy phòng thủ
- Q&A

VIETNIX



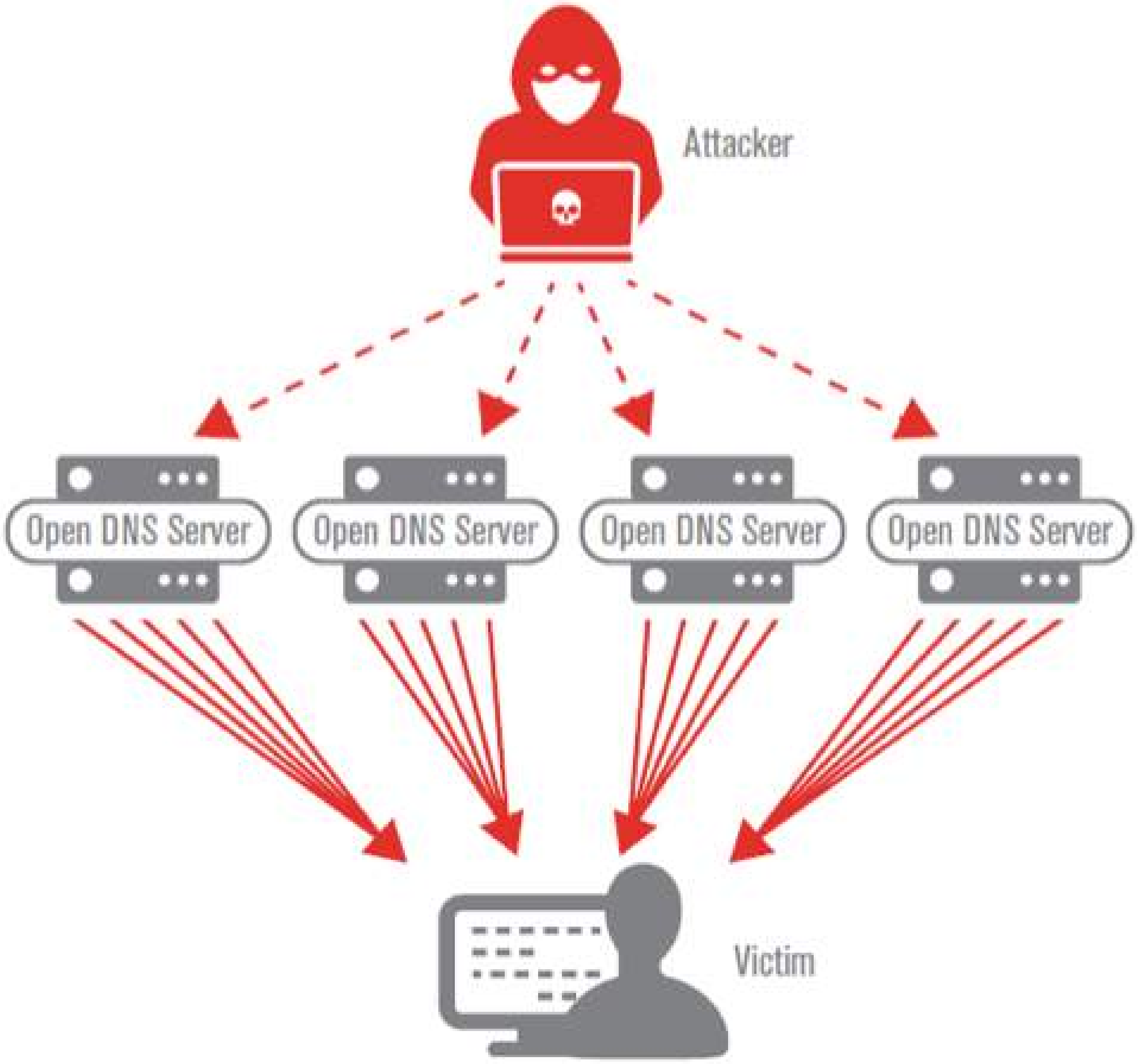
1. TẤN CÔNG DDOS

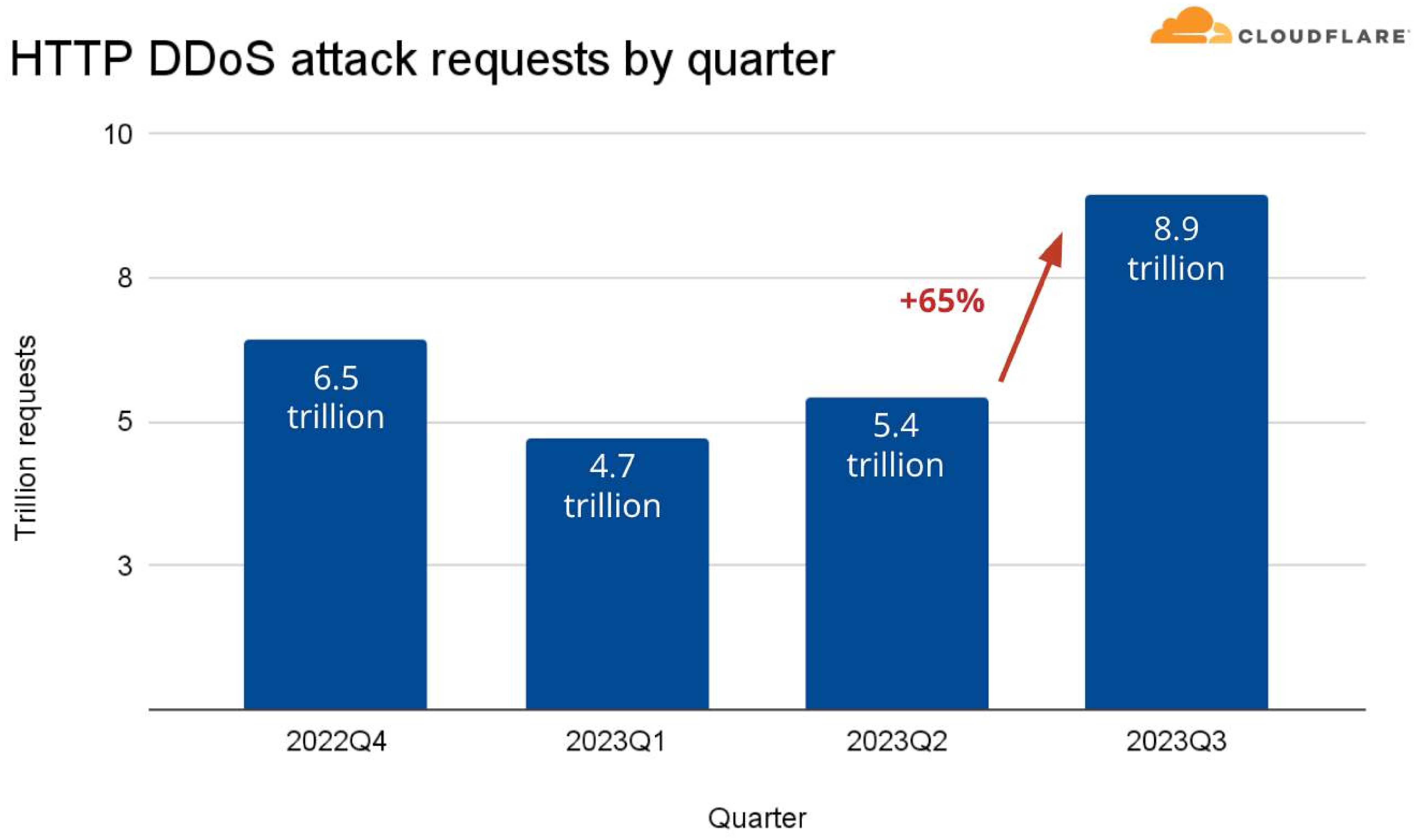
“Mượn đao giết người”

DOS có nguy hiểm không?

CÁC LOẠI TẤN CÔNG DDOS

- **Application Attack:** HTTP DDOS
- **Protocol Attack:** SYN Flood, Fragment Attack, ACK/ACK-PSH Flood, ICMP Flood,...
- **Volumetric Attack:** DNS/NTP amplification, ICMP Flood, UDP Flood,...

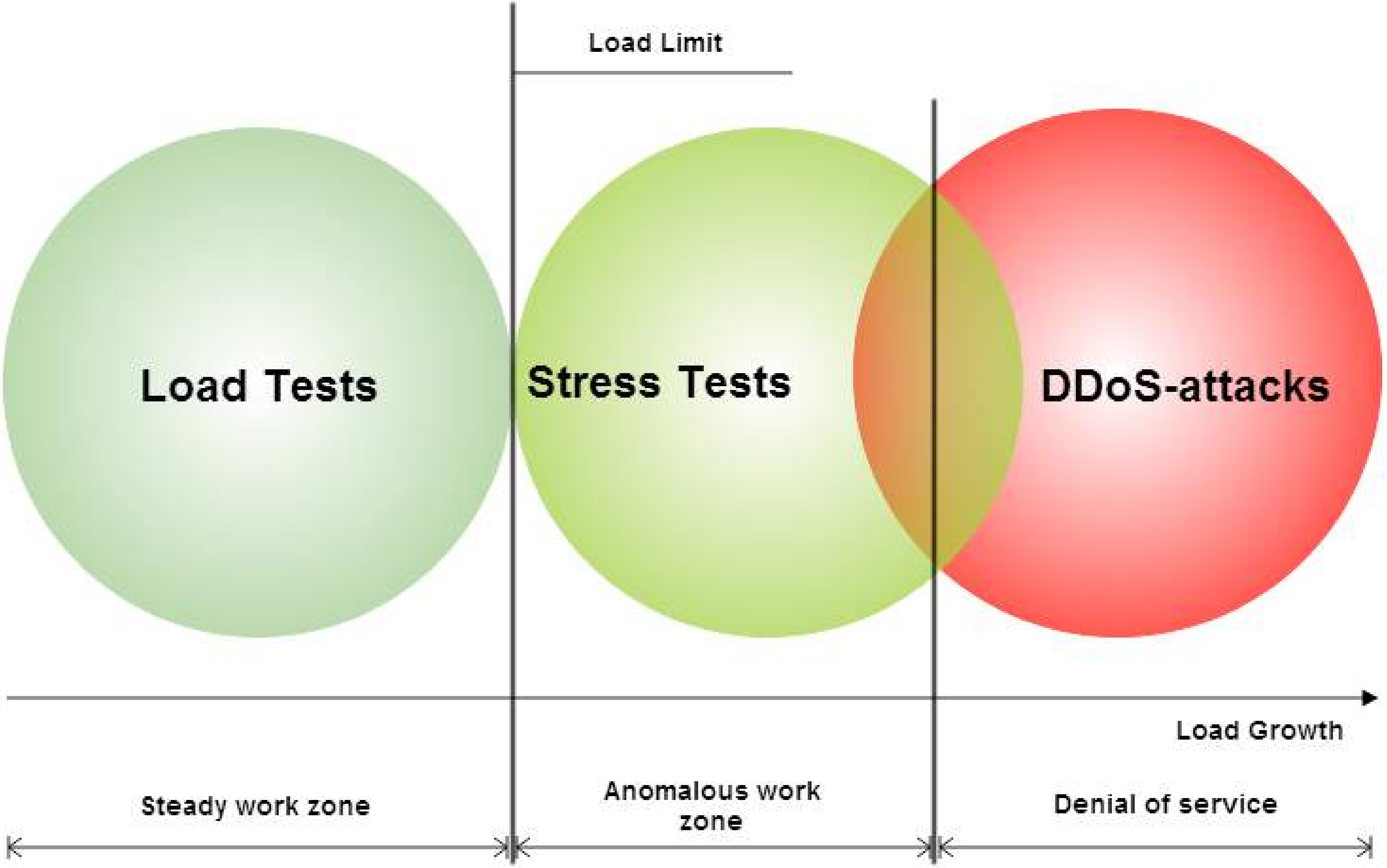


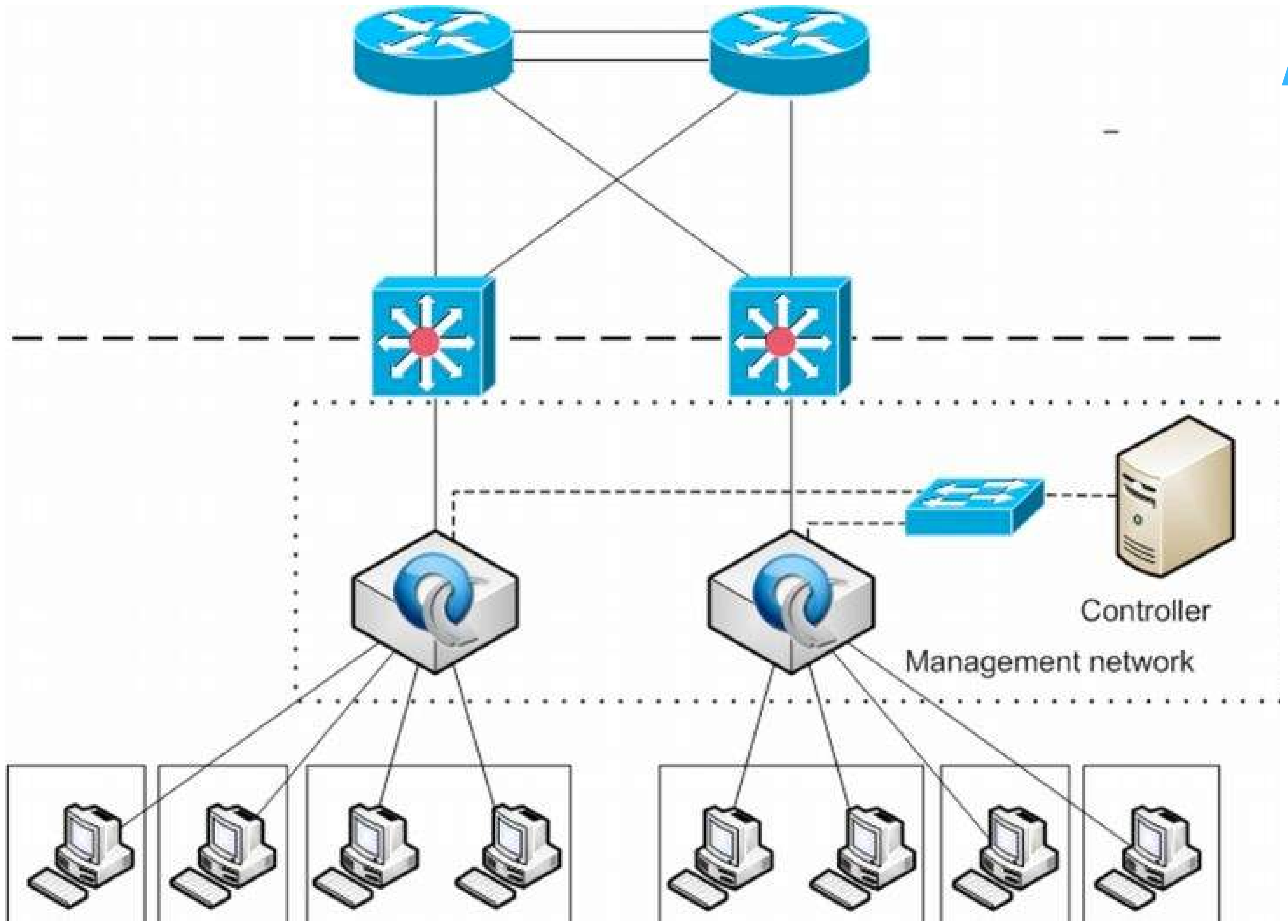


Nguồn: https://blog.cloudflare.com/ddos-threat-report-2023-q3/

Mục đích

- Stress Test
- Tấn công phá hoại



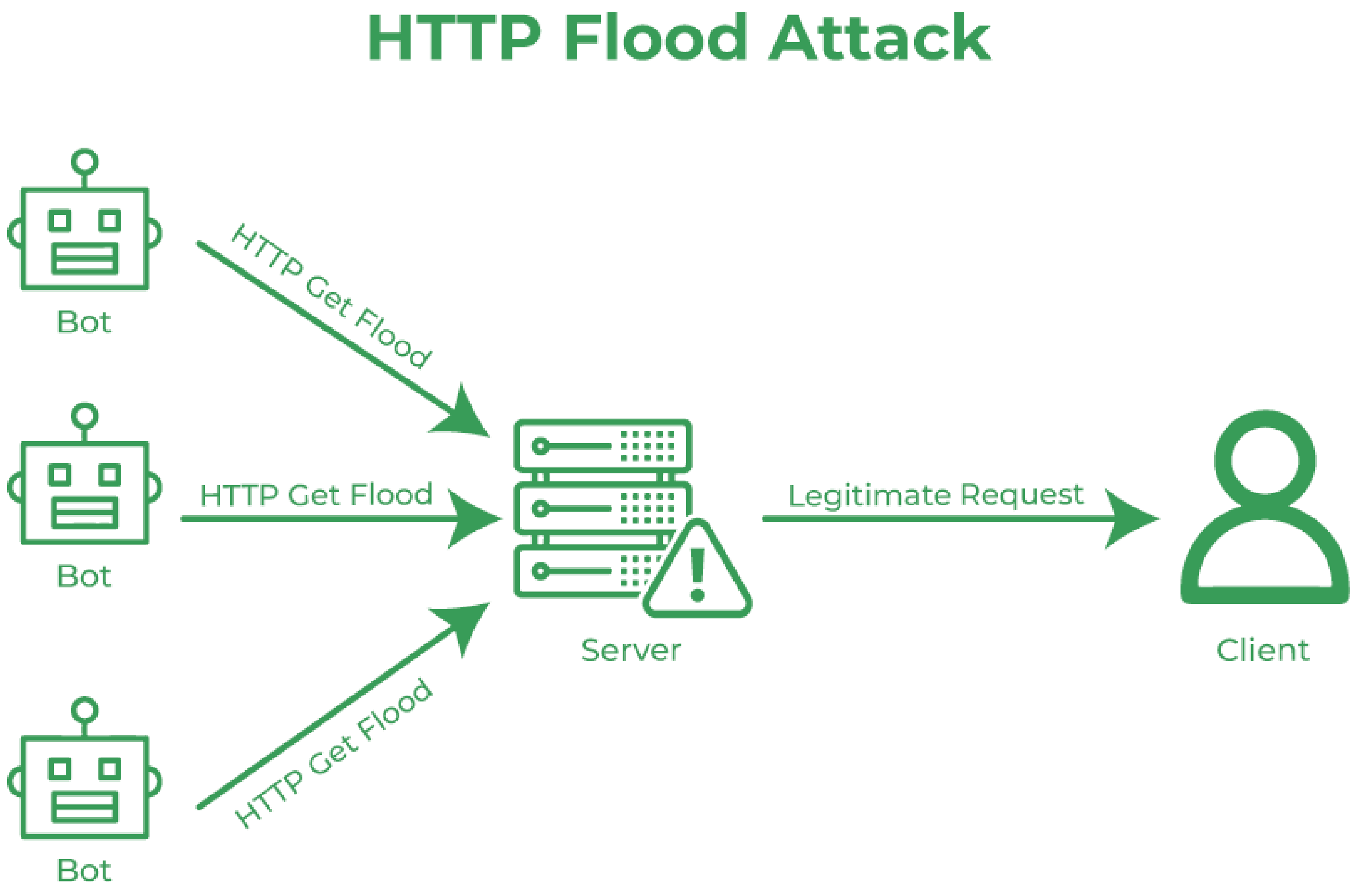


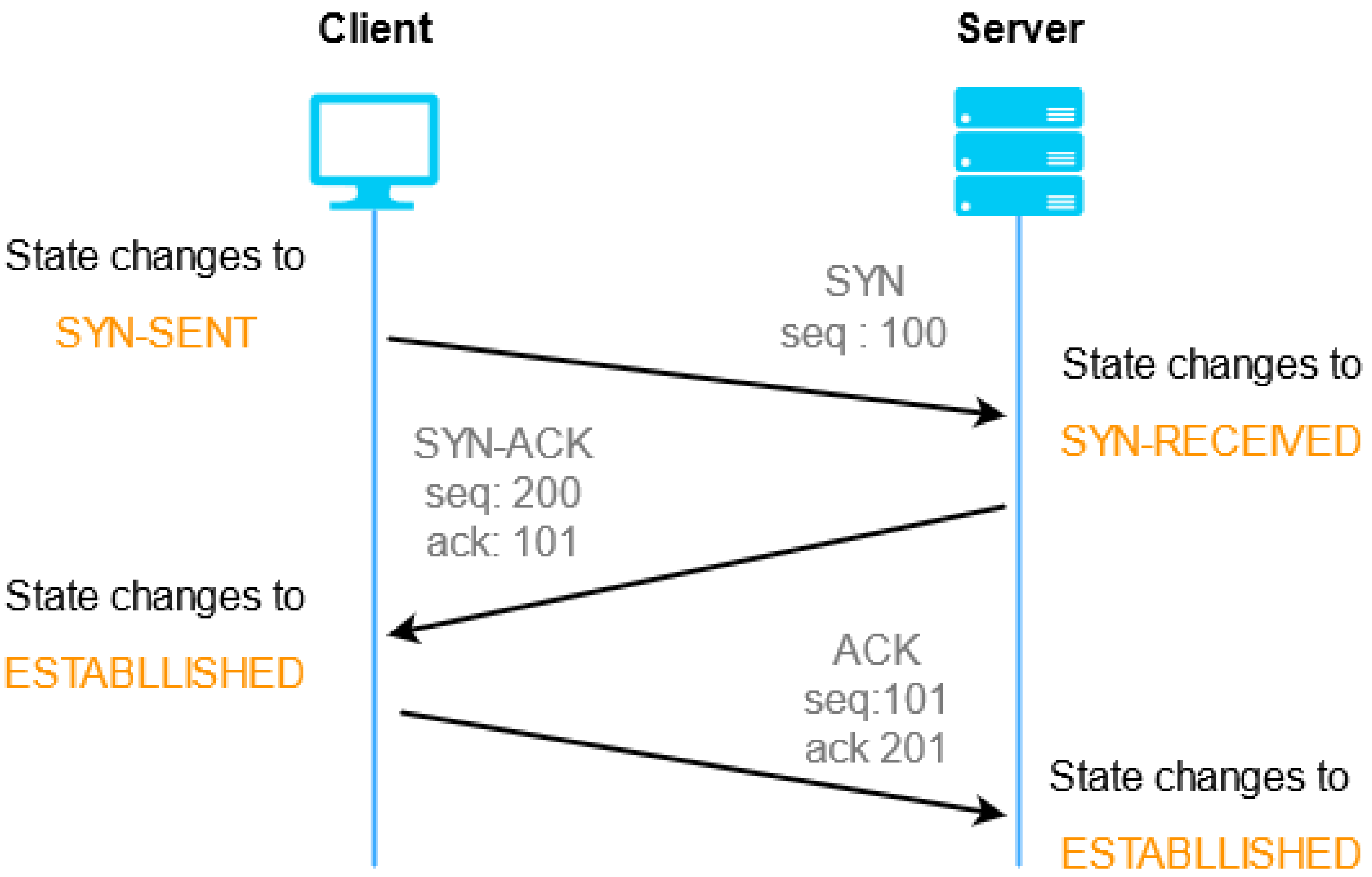
ẢNH HƯỞNG

- **Ứng dụng:** Giới hạn xử lý của ứng dụng, Giới hạn Process, Workers,...
- **Hệ điều hành:** Full Conntrack Tables, Tràn Bộ đệm, Tăng Interrupt,...
- **Tài Nguyên - Hạ tầng:** Full CPU, RAM; Nghẽn I/O; Nghẽn băng thông và thậm chí full uplink,...

VIETNIX

2. Application Attack - HTTP DDOS





HTTP DDOS có phải thiết lập kết nối TCP 3 ways Handshake?

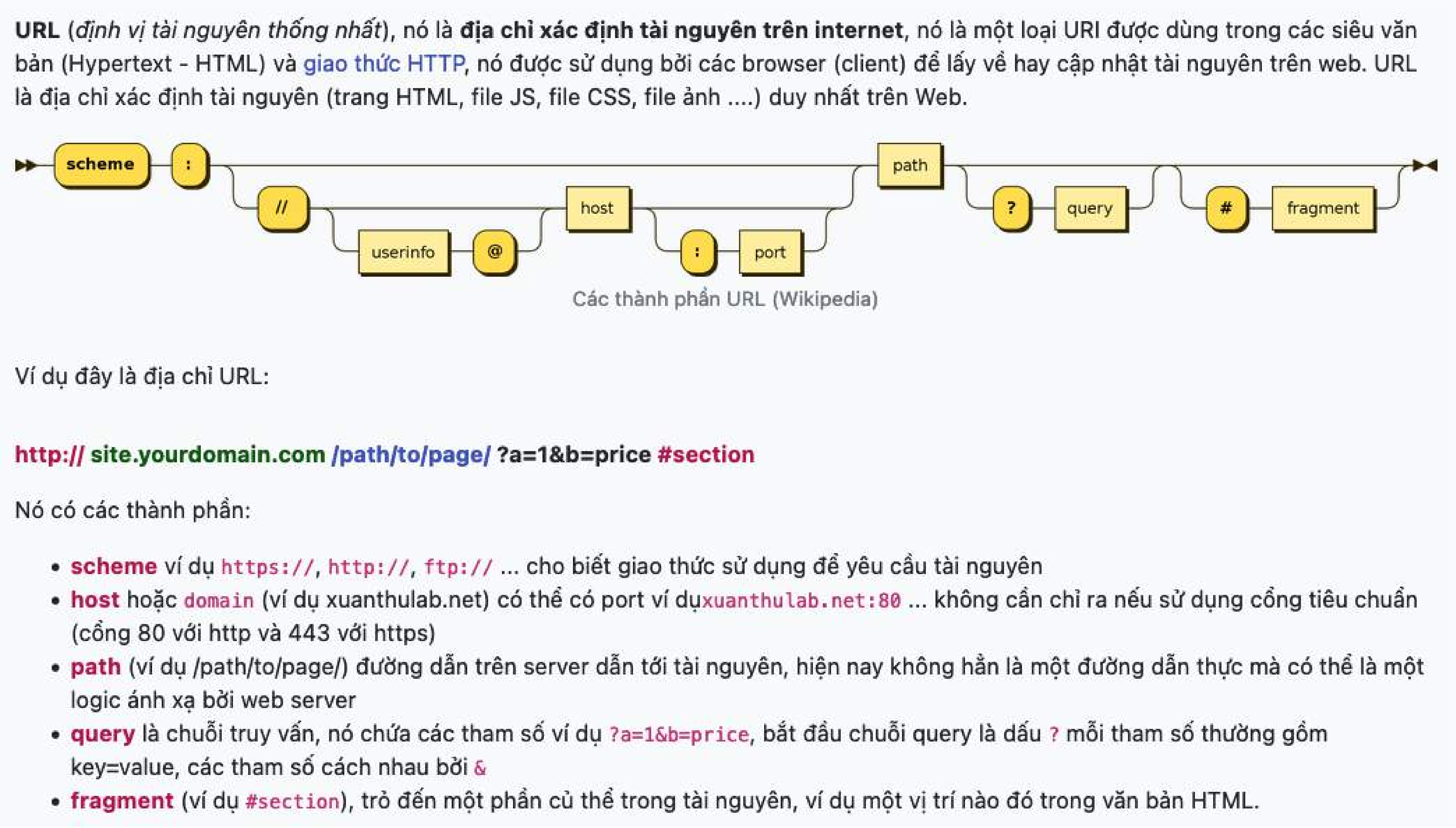
COMMON SECURITY ATTACKS IN THE OSI LAYER MODEL

LAYERS		ATTACKS
7 APPLICATION	←	EXPLOIT
6 PRESENTATION	←	PHISHING
5 SESSION	←	HIJACKING (XSS ATTACKS, SESSION SIDE JACKING, MALWARE)
4 TRANSPORT	←	RECONNAISSANCE/ DOS (TCP SESSION HIJACK, FRAGGLE, SYN FLOOD, LAND ATTACK)
3 NETWORK	←	MAN-IN-THE-MIDDLE (SMURF ATTACK, PING OF DEATH, TEARDROP)
2 DATA LINK	←	SPOOFING (MAC SPOOFING, MAC FLOODING, VLAN HOPPING)
1 PHYSICAL	←	SNIFFING

CÁC KIỂU TẤN CÔNG WEB PHỔ BIẾN

- Request Method Flood (GET/POST/HEAD)
- Random Path (/asb, /csdet, /3s$df)
- Random Query String (/?qs=ab, /?key=33,...)
- Challenge Bypass (Cookie, JS, Captcha, ...)
- Anti DDos Firewall Bypass
- ...

Cấu trúc URL



URL (*định vị tài nguyên thống nhất*), nó là **địa chỉ xác định tài nguyên trên internet**, nó là một loại URI được dùng trong các siêu văn bản (Hypertext - HTML) và giao thức HTTP, nó được sử dụng bởi các browser (client) để lấy về hay cập nhật tài nguyên trên web. URL là địa chỉ xác định tài nguyên (trang HTML, file JS, file CSS, file ảnh ....) duy nhất trên Web.

Các thành phần URL (Wikipedia)

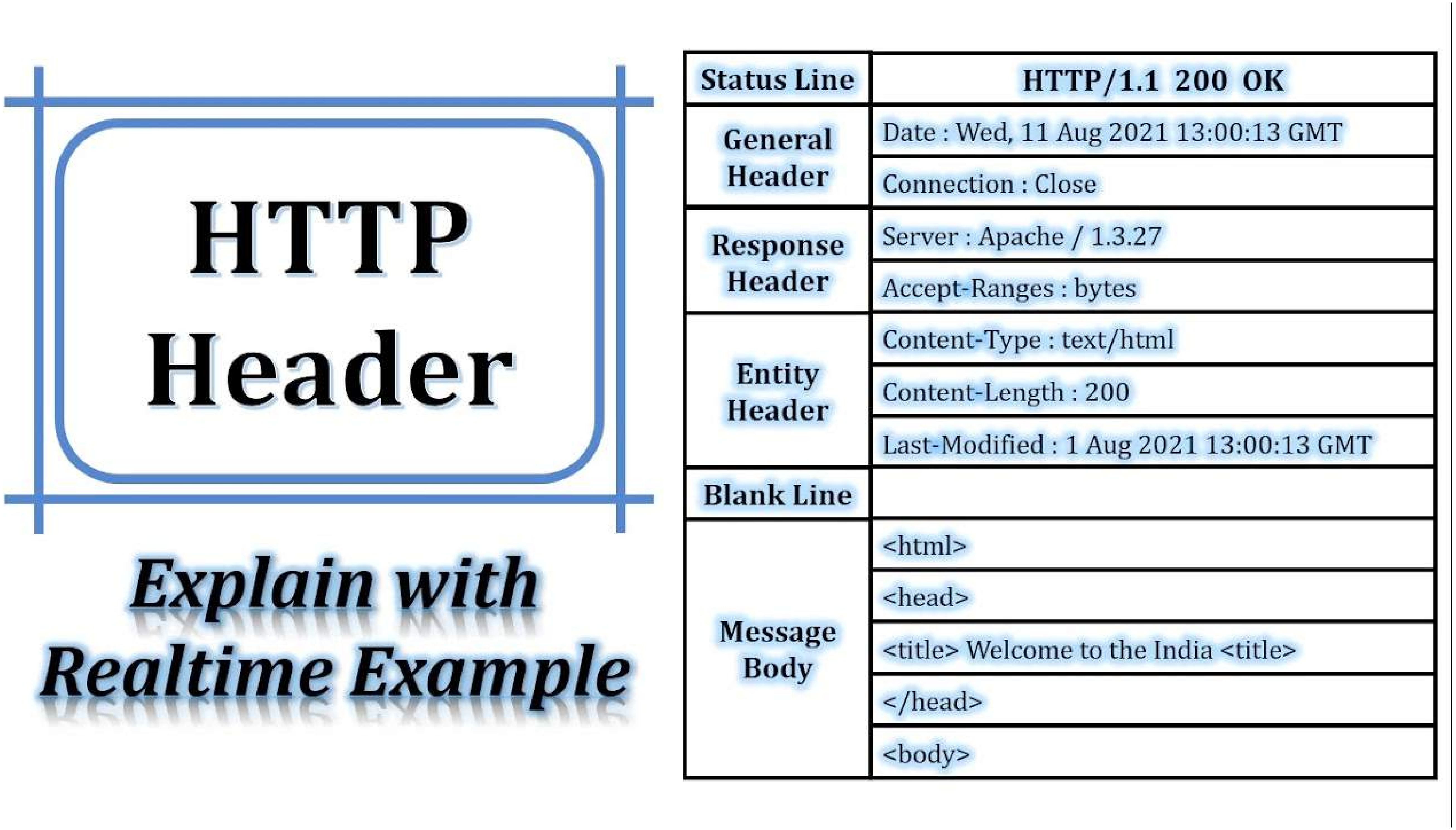
Ví dụ đây là địa chỉ URL:

http:// site.yourdomain.com /path/to/page/ ?a=1&b=price #section

Nó có các thành phần:

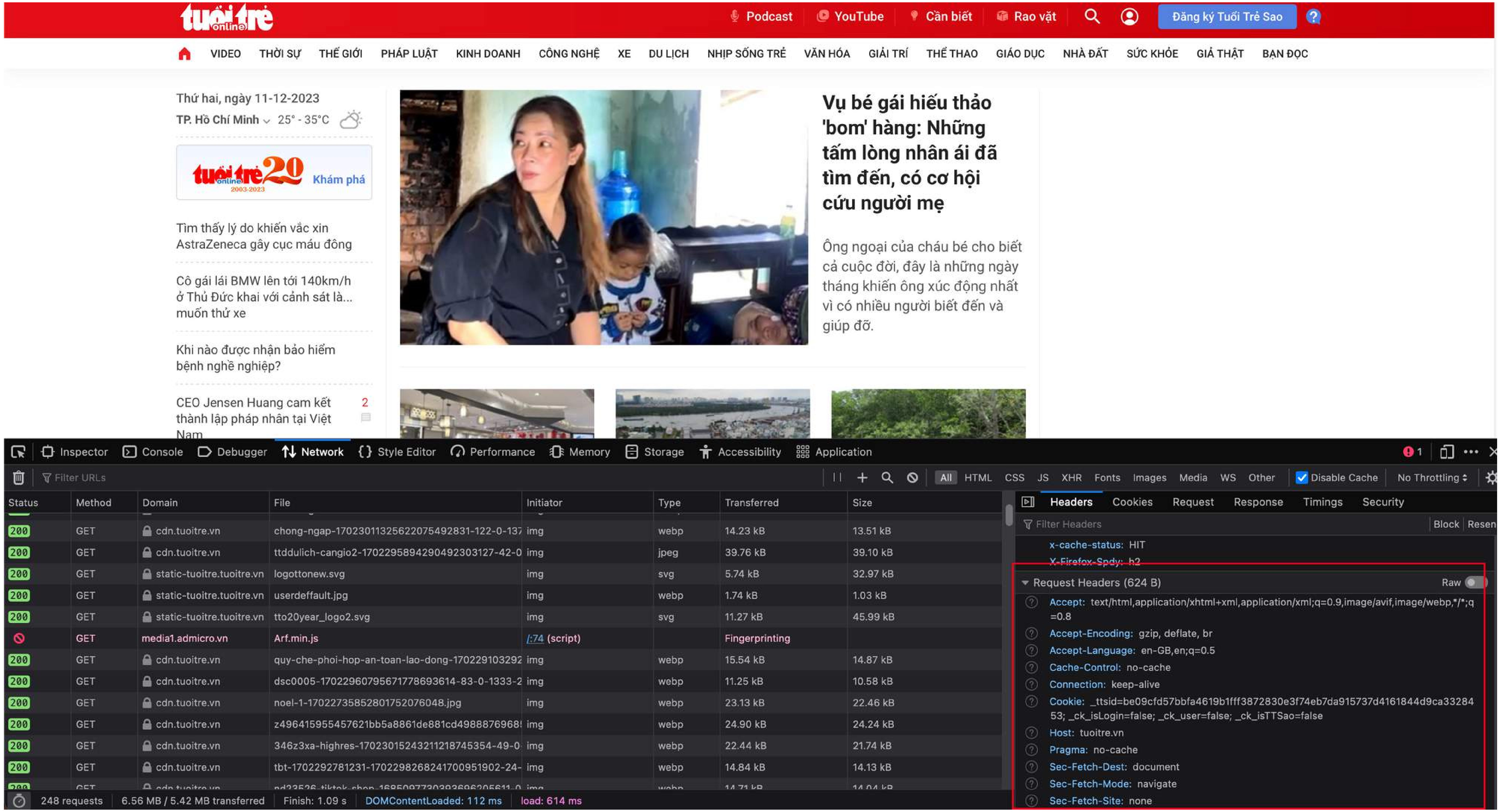
- **scheme** ví dụ `https://`, `http://`, `ftp://` ... cho biết giao thức sử dụng để yêu cầu tài nguyên
- **host** hoặc `domain` (ví dụ xuanthulab.net) có thể có port ví dụ`xuanthulab.net:80` ... không cần chỉ ra nếu sử dụng cổng tiêu chuẩn (cổng 80 với http và 443 với https)
- **path** (ví dụ /path/to/page/) đường dẫn trên server dẫn tới tài nguyên, hiện nay không hẳn là một đường dẫn thực mà có thể là một logic ánh xạ bởi web server
- **query** là chuỗi truy vấn, nó chứa các tham số ví dụ `?a=1&b=price`, bắt đầu chuỗi query là dấu `?` mỗi tham số thường gồm key=value, các tham số cách nhau bởi `&`
- **fragment** (ví dụ `#section`), trỏ đến một phần củ thể trong tài nguyên, ví dụ một vị trí nào đó trong văn bản HTML.

Thành phần của HTTP:


HTTP
Header
Explain with
Realtime Example

Status Line	HTTP/1.1 200 OK
General Header	Date : Wed, 11 Aug 2021 13:00:13 GMT
	Connection : Close
Response Header	Server : Apache / 1.3.27
	Accept-Ranges : bytes
Entity Header	Content-Type : text/html
	Content-Length : 200
	Last-Modified : 1 Aug 2021 13:00:13 GMT
Blank Line	
Message Body	<html>
	<head>
	<title> Welcome to the India <title>
	</head>
	<body>

Thành phần của HTTP



Podcast | YouTube | Cần biết | Rao vặt | Đăng ký Tuổi Trẻ Sao

VIDEO THỜI SỰ THẾ GIỚI PHÁP LUẬT KINH DOANH CÔNG NGHỆ XE DU LỊCH NHỊP SỐNG TRẺ VĂN HÓA GIẢI TRÍ THỂ THAO GIÁO DỤC NHÀ ĐẤT SỨC KHỎE GIẢ THẬT BẠN ĐỌC

Thứ hai, ngày 11-12-2023
TP. Hồ Chí Minh 25° - 35°C

Tuổi Trẻ 20 2003-2023 Khám phá

Tìm thấy lý do khiến vắc xin AstraZeneca gây cục máu đông

Cô gái lái BMW lên tới 140km/h ở Thủ Đức khai với cảnh sát là... muốn thử xe

Khi nào được nhận bảo hiểm bệnh nghề nghiệp?

CEO Jensen Huang cam kết thành lập pháp nhân tại Việt Nam 2

Vụ bé gái hiếu thảo 'bom' hàng: Những tấm lòng nhân ái đã tìm đến, có cơ hội cứu người mẹ

Ông ngoại của cháu bé cho biết cả cuộc đời, đây là những ngày tháng khiến ông xúc động nhất vì có nhiều người biết đến và giúp đỡ.

Inspector | Console | Debugger | Network | Style Editor | Performance | Memory | Storage | Accessibility | Application

Filter URLs | All HTML CSS JS XHR Fonts Images Media WS Other | ☑ Disable Cache | No Throttling

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	cdn.tuoitre.vn	chong-ngap-17023011325622075492831-122-0-137	img	webp	14.23 kB	13.51 kB
200	GET	cdn.tuoitre.vn	ttddulich-cangio2-17022958942904923031 27-42-0	img	jpeg	39.76 kB	39.10 kB
200	GET	static-tuoitre.tuoitre.vn	logottonew.svg	img	svg	5.74 kB	32.97 kB
200	GET	static-tuoitre.tuoitre.vn	userdeffault.jpg	img	webp	1.74 kB	1.03 kB
200	GET	static-tuoitre.tuoitre.vn	tto20year_logo2.svg	img	svg	11.27 kB	45.99 kB
⃠	GET	media1.admicro.vn	Arf.min.js	/:74 (script)		Fingerprinting	
200	GET	cdn.tuoitre.vn	quy-che-phoi-hop-an-toan-lao-dong-170229103292	img	webp	15.54 kB	14.87 kB
200	GET	cdn.tuoitre.vn	dsc0005-17022960795671778693614-83-0-1333-2	img	webp	11.25 kB	10.58 kB
200	GET	cdn.tuoitre.vn	noel-1-17022735852801752076048.jpg	img	webp	23.13 kB	22.46 kB
200	GET	cdn.tuoitre.vn	z496415955457621bb5a8861de881cd4988876968	img	webp	24.90 kB	24.24 kB
200	GET	cdn.tuoitre.vn	346z3xa-highres-17023015243211218745354-49-0-	img	webp	22.44 kB	21.74 kB
200	GET	cdn.tuoitre.vn	tbt-1702292781231-17022982682417009519 02-24-	img	webp	14.84 kB	14.13 kB

248 requests | 6.56 MB / 5.42 MB transferred | Finish: 1.09 s | DOMContentLoaded: 112 ms | load: 614 ms

Headers | Cookies | Request | Response | Timings | Security

Filter Headers | Block | Resen

```
x-cache-status: HIT
X-Firefox-Spdy: h2
```

Request Headers (624 B) Raw

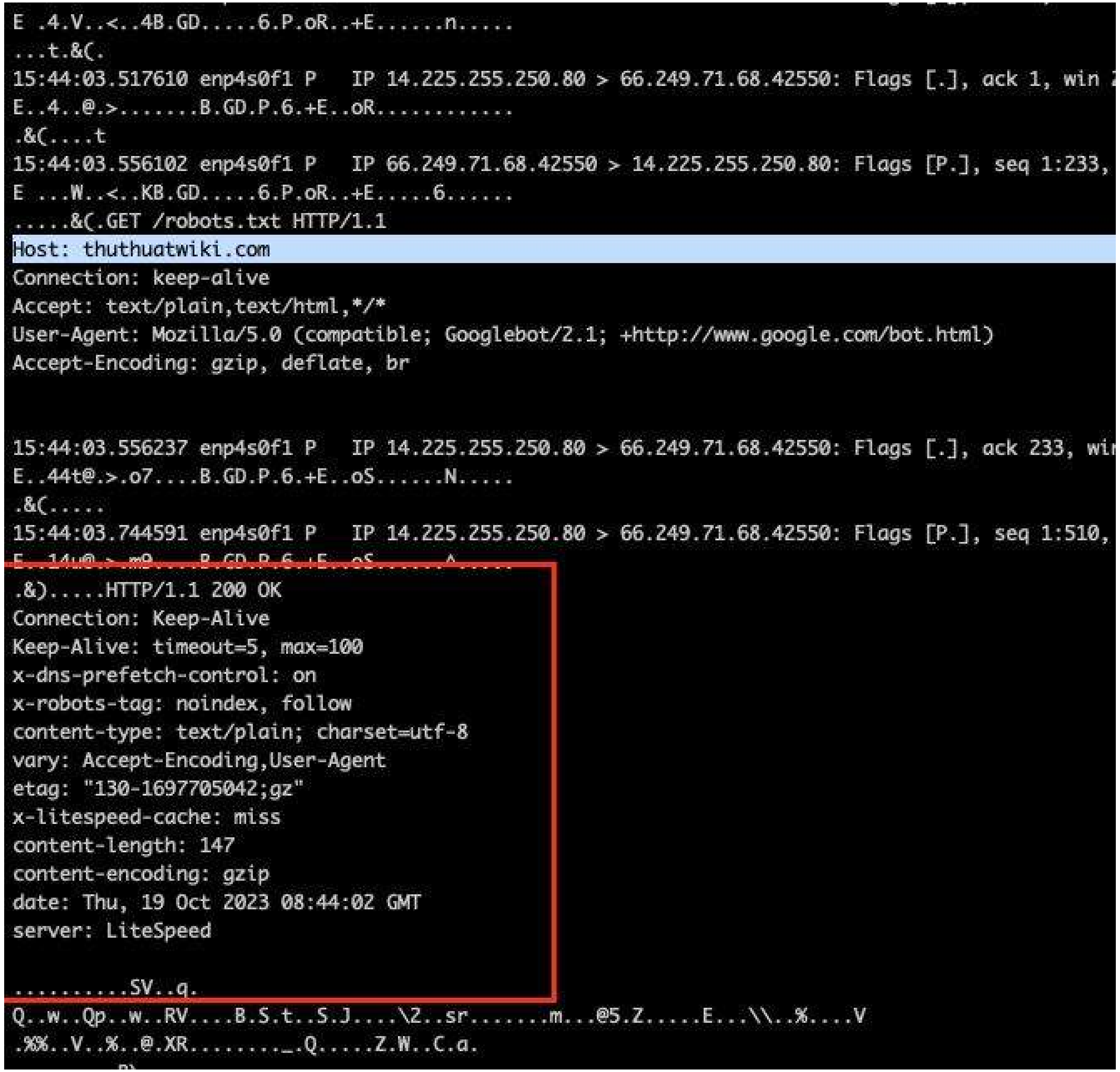
```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: en-GB,en;q=0.5
Cache-Control: no-cache
Connection: keep-alive
Cookie: _ttsid=be09cfd57bbfa4619b1fff3872830e3f74eb7da915737d4161844d9ca3328453; _ck_isLogin=false; _ck_user=false; _ck_isTTSao=false
Host: tuoitre.vn
Pragma: no-cache
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
```

Thành phần của HTTP:

Nếu sử dụng Wireshark

hoặc tcpdump thì có thể bắt được HTTP

Header (scheme: https) không?

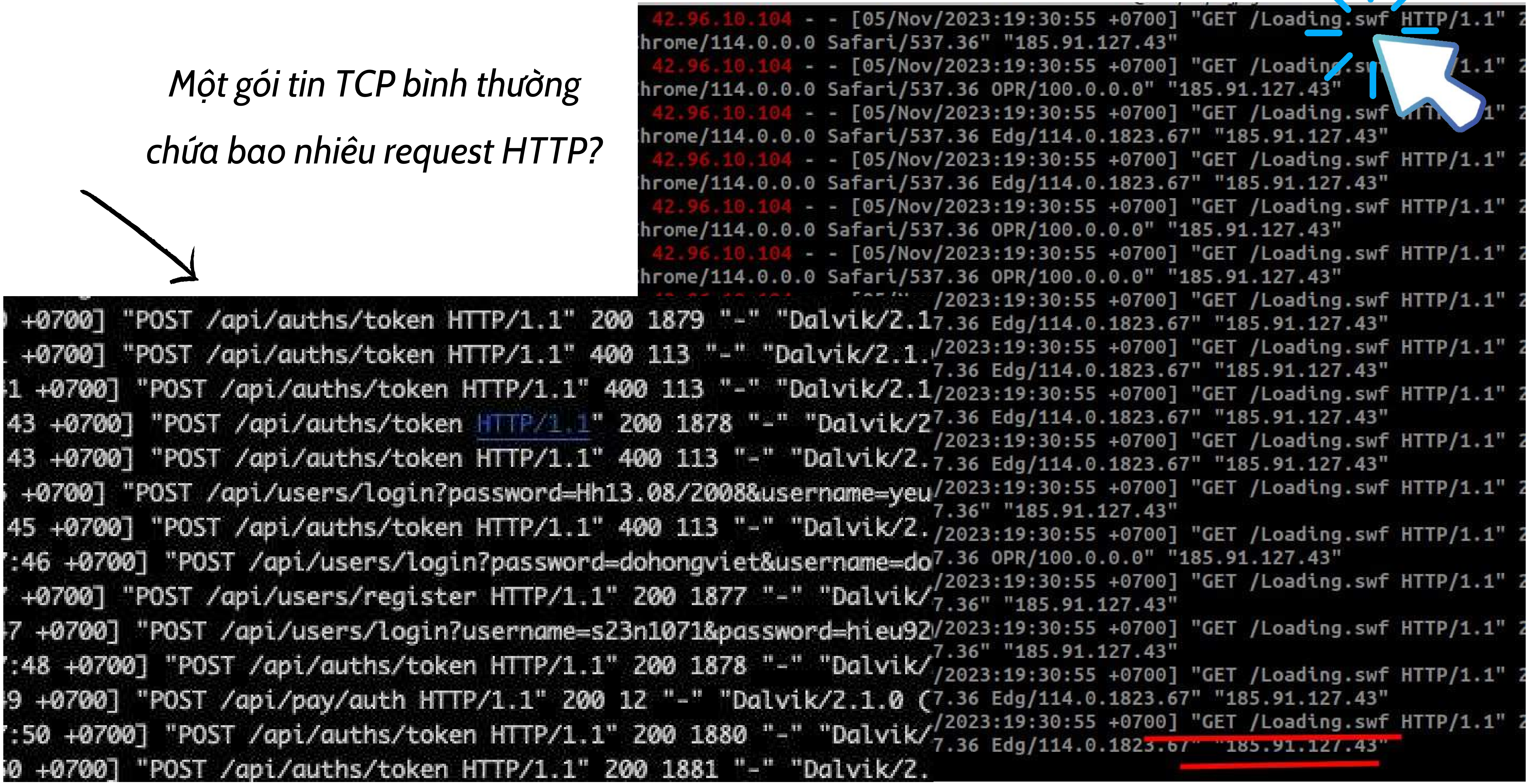


```
E .4.V..<..4B.GD.....6.P.oR..+E......n.....
...t.&(.
15:44:03.517610 enp4s0f1 P   IP 14.225.255.250.80 > 66.249.71.68.42550: Flags [.], ack 1, win
E..4..@.>.......B.GD.P.6.+E..oR...........
.&(....t
15:44:03.556102 enp4s0f1 P   IP 66.249.71.68.42550 > 14.225.255.250.80: Flags [P.], seq 1:233,
E ...W..<..KB.GD.....6.P.oR..+E.....6......
.....&(.GET /robots.txt HTTP/1.1
Host: thuthuatwiki.com
Connection: keep-alive
Accept: text/plain,text/html,*/*
User-Agent: Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Accept-Encoding: gzip, deflate, br


15:44:03.556237 enp4s0f1 P   IP 14.225.255.250.80 > 66.249.71.68.42550: Flags [.], ack 233, wi
E..44t@.>.o7....B.GD.P.6.+E..oS......N.....
.&(.....
15:44:03.744591 enp4s0f1 P   IP 14.225.255.250.80 > 66.249.71.68.42550: Flags [P.], seq 1:510,
E..14u@.>.m9....B.GD.P.6.+E..oS......A.....
.&).....HTTP/1.1 200 OK
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
x-dns-prefetch-control: on
x-robots-tag: noindex, follow
content-type: text/plain; charset=utf-8
vary: Accept-Encoding,User-Agent
etag: "130-1697705042;gz"
x-litespeed-cache: miss
content-length: 147
content-encoding: gzip
date: Thu, 19 Oct 2023 08:44:02 GMT
server: LiteSpeed

..........SV..q.
Q..w..Qp..w..RV....B.S.t..S.J....\Z..sr.......m...@5.Z.....E...\\..%....V
.%%..V..%..@.XR........_.Q.....Z.W..C.a.
```

GET/POST Flood

Một gói tin TCP bình thường

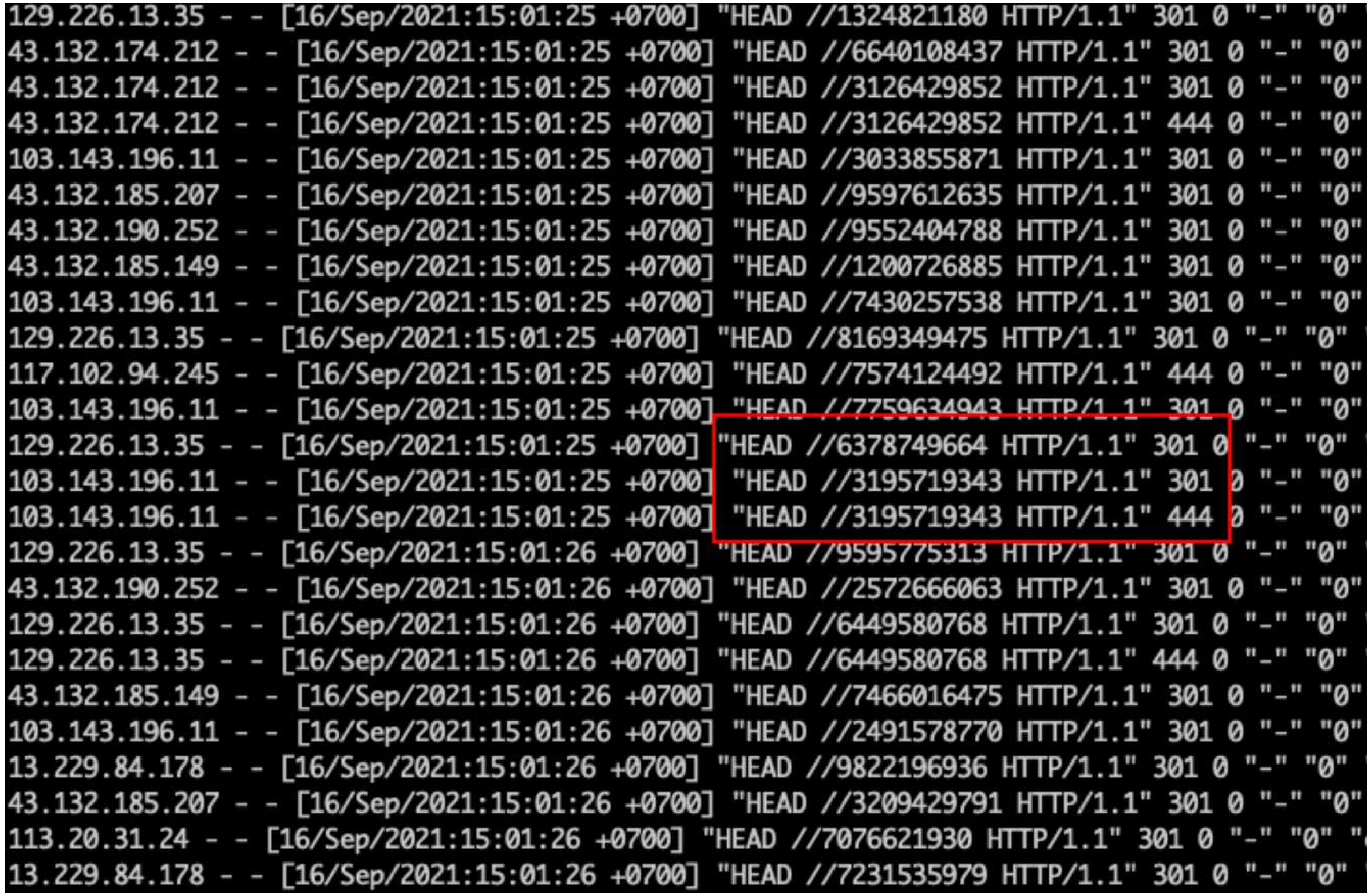
chứa bao nhiêu request HTTP?



```
 42.96.10.104 - - [05/Nov/2023:19:30:55 +0700] "GET /Loading.swf HTTP/1.1" 2
hrome/114.0.0.0 Safari/537.36" "185.91.127.43"
 42.96.10.104 - - [05/Nov/2023:19:30:55 +0700] "GET /Loading.sw     /1.1" 2
hrome/114.0.0.0 Safari/537.36 OPR/100.0.0.0" "185.91.127.43"
 42.96.10.104 - - [05/Nov/2023:19:30:55 +0700] "GET /Loading.swf HTT    1" 2
hrome/114.0.0.0 Safari/537.36 Edg/114.0.1823.67" "185.91.127.43"
 42.96.10.104 - - [05/Nov/2023:19:30:55 +0700] "GET /Loading.swf HTTP/1.1" 2
hrome/114.0.0.0 Safari/537.36 Edg/114.0.1823.67" "185.91.127.43"
 42.96.10.104 - - [05/Nov/2023:19:30:55 +0700] "GET /Loading.swf HTTP/1.1" 2
hrome/114.0.0.0 Safari/537.36 OPR/100.0.0.0" "185.91.127.43"
 42.96.10.104 - - [05/Nov/2023:19:30:55 +0700] "GET /Loading.swf HTTP/1.1" 2
hrome/114.0.0.0 Safari/537.36 OPR/100.0.0.0" "185.91.127.43"
/2023:19:30:55 +0700] "GET /Loading.swf HTTP/1.1" 2
7.36 Edg/114.0.1823.67" "185.91.127.43"
/2023:19:30:55 +0700] "GET /Loading.swf HTTP/1.1" 2
7.36 Edg/114.0.1823.67" "185.91.127.43"
/2023:19:30:55 +0700] "GET /Loading.swf HTTP/1.1" 2
7.36 Edg/114.0.1823.67" "185.91.127.43"
/2023:19:30:55 +0700] "GET /Loading.swf HTTP/1.1" 2
7.36 Edg/114.0.1823.67" "185.91.127.43"
/2023:19:30:55 +0700] "GET /Loading.swf HTTP/1.1" 2
7.36" "185.91.127.43"
/2023:19:30:55 +0700] "GET /Loading.swf HTTP/1.1" 2
7.36 OPR/100.0.0.0" "185.91.127.43"
/2023:19:30:55 +0700] "GET /Loading.swf HTTP/1.1" 2
7.36" "185.91.127.43"
/2023:19:30:55 +0700] "GET /Loading.swf HTTP/1.1" 2
7.36" "185.91.127.43"
/2023:19:30:55 +0700] "GET /Loading.swf HTTP/1.1" 2
7.36 Edg/114.0.1823.67" "185.91.127.43"
/2023:19:30:55 +0700] "GET /Loading.swf HTTP/1.1" 2
7.36 Edg/114.0.1823.67" "185.91.127.43"
```

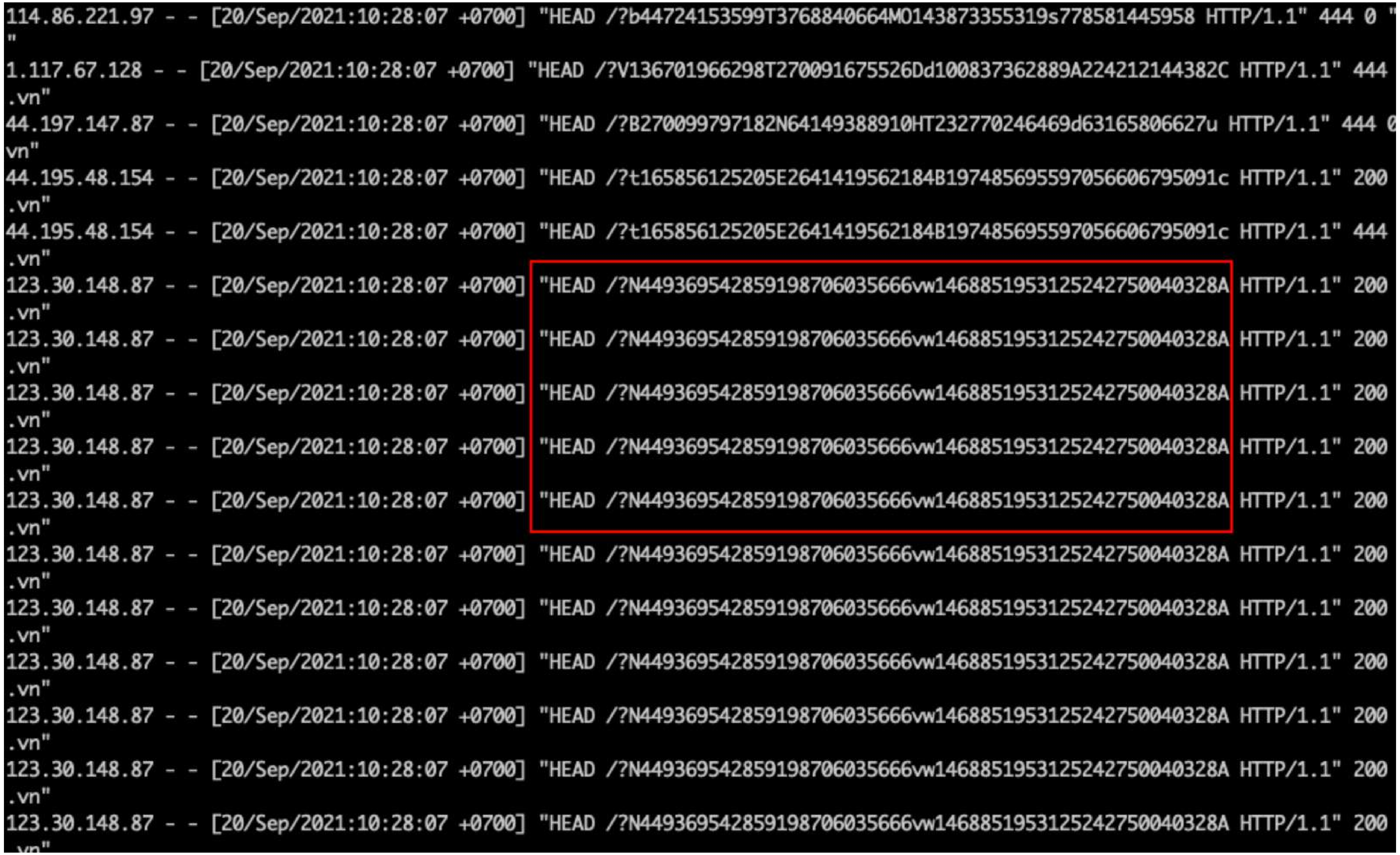
```
 +0700] "POST /api/auths/token HTTP/1.1" 200 1879 "-" "Dalvik/2.1
 +0700] "POST /api/auths/token HTTP/1.1" 400 113 "-" "Dalvik/2.1.
1 +0700] "POST /api/auths/token HTTP/1.1" 400 113 "-" "Dalvik/2.1
43 +0700] "POST /api/auths/token HTTP/1.1" 200 1878 "-" "Dalvik/2
43 +0700] "POST /api/auths/token HTTP/1.1" 400 113 "-" "Dalvik/2.
 +0700] "POST /api/users/login?password=Hh13.08/2008&username=yeu
45 +0700] "POST /api/auths/token HTTP/1.1" 400 113 "-" "Dalvik/2.
:46 +0700] "POST /api/users/login?password=dohongviet&username=do
 +0700] "POST /api/users/register HTTP/1.1" 200 1877 "-" "Dalvik/
7 +0700] "POST /api/users/login?username=s23n1071&password=hieu92
:48 +0700] "POST /api/auths/token HTTP/1.1" 200 1878 "-" "Dalvik/
9 +0700] "POST /api/pay/auth HTTP/1.1" 200 12 "-" "Dalvik/2.1.0 (
:50 +0700] "POST /api/auths/token HTTP/1.1" 200 1880 "-" "Dalvik/
0 +0700] "POST /api/auths/token HTTP/1.1" 200 1881 "-" "Dalvik/2.
```

Random Path



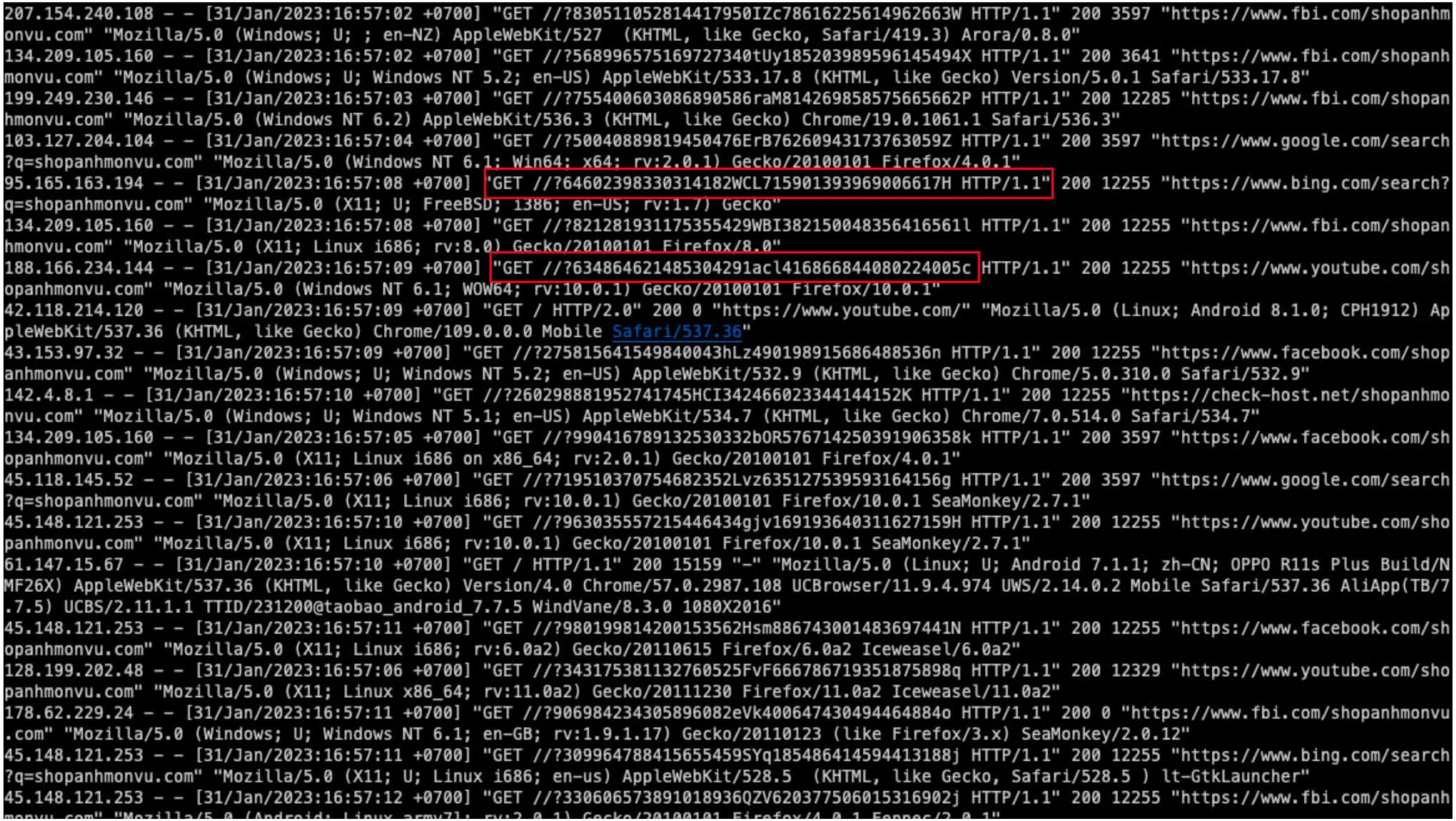
```
129.226.13.35 - - [16/Sep/2021:15:01:25 +0700] "HEAD //1324821180 HTTP/1.1" 301 0 "-" "0"
43.132.174.212 - - [16/Sep/2021:15:01:25 +0700] "HEAD //6640108437 HTTP/1.1" 301 0 "-" "0"
43.132.174.212 - - [16/Sep/2021:15:01:25 +0700] "HEAD //3126429852 HTTP/1.1" 301 0 "-" "0"
43.132.174.212 - - [16/Sep/2021:15:01:25 +0700] "HEAD //3126429852 HTTP/1.1" 444 0 "-" "0"
103.143.196.11 - - [16/Sep/2021:15:01:25 +0700] "HEAD //3033855871 HTTP/1.1" 301 0 "-" "0"
43.132.185.207 - - [16/Sep/2021:15:01:25 +0700] "HEAD //9597612635 HTTP/1.1" 301 0 "-" "0"
43.132.190.252 - - [16/Sep/2021:15:01:25 +0700] "HEAD //9552404788 HTTP/1.1" 301 0 "-" "0"
43.132.185.149 - - [16/Sep/2021:15:01:25 +0700] "HEAD //1200726885 HTTP/1.1" 301 0 "-" "0"
103.143.196.11 - - [16/Sep/2021:15:01:25 +0700] "HEAD //7430257538 HTTP/1.1" 301 0 "-" "0"
129.226.13.35 - - [16/Sep/2021:15:01:25 +0700] "HEAD //8169349475 HTTP/1.1" 301 0 "-" "0"
117.102.94.245 - - [16/Sep/2021:15:01:25 +0700] "HEAD //7574124492 HTTP/1.1" 444 0 "-" "0"
103.143.196.11 - - [16/Sep/2021:15:01:25 +0700] "HEAD //7759634943 HTTP/1.1" 301 0 "-" "0"
129.226.13.35 - - [16/Sep/2021:15:01:25 +0700] "HEAD //6378749664 HTTP/1.1" 301 0 "-" "0"
103.143.196.11 - - [16/Sep/2021:15:01:25 +0700] "HEAD //3195719343 HTTP/1.1" 301 0 "-" "0"
103.143.196.11 - - [16/Sep/2021:15:01:25 +0700] "HEAD //3195719343 HTTP/1.1" 444 0 "-" "0"
129.226.13.35 - - [16/Sep/2021:15:01:26 +0700] "HEAD //9595775313 HTTP/1.1" 301 0 "-" "0"
43.132.190.252 - - [16/Sep/2021:15:01:26 +0700] "HEAD //2572666063 HTTP/1.1" 301 0 "-" "0"
129.226.13.35 - - [16/Sep/2021:15:01:26 +0700] "HEAD //6449580768 HTTP/1.1" 301 0 "-" "0"
129.226.13.35 - - [16/Sep/2021:15:01:26 +0700] "HEAD //6449580768 HTTP/1.1" 444 0 "-" "0"
43.132.185.149 - - [16/Sep/2021:15:01:26 +0700] "HEAD //7466016475 HTTP/1.1" 301 0 "-" "0"
103.143.196.11 - - [16/Sep/2021:15:01:26 +0700] "HEAD //2491578770 HTTP/1.1" 301 0 "-" "0"
13.229.84.178 - - [16/Sep/2021:15:01:26 +0700] "HEAD //9822196936 HTTP/1.1" 301 0 "-" "0"
43.132.185.207 - - [16/Sep/2021:15:01:26 +0700] "HEAD //3209429791 HTTP/1.1" 301 0 "-" "0"
113.20.31.24 - - [16/Sep/2021:15:01:26 +0700] "HEAD //7076621930 HTTP/1.1" 301 0 "-" "0" "
13.229.84.178 - - [16/Sep/2021:15:01:26 +0700] "HEAD //7231535979 HTTP/1.1" 301 0 "-" "0"
```

Random Query String



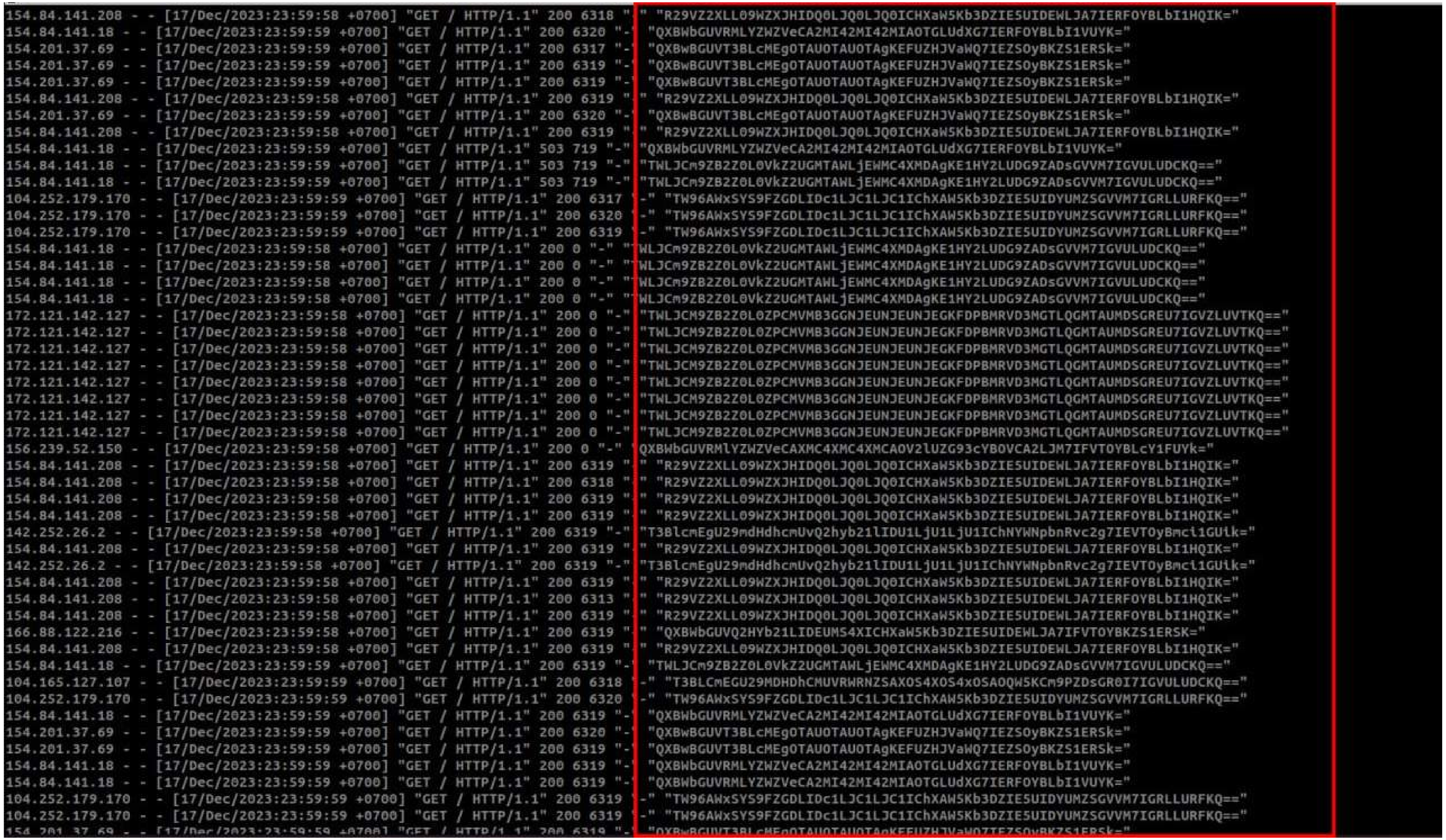
```
114.86.221.97 - - [20/Sep/2021:10:28:07 +0700] "HEAD /?b44724153599T3768840664MO143873355319s778581445958 HTTP/1.1" 444 0 "
"
1.117.67.128 - - [20/Sep/2021:10:28:07 +0700] "HEAD /?V136701966298T270091675526Dd100837362889A224212144382C HTTP/1.1" 444
.vn"
44.197.147.87 - - [20/Sep/2021:10:28:07 +0700] "HEAD /?B270099797182N64149388910HT232770246469d63165806627u HTTP/1.1" 444 0
vn"
44.195.48.154 - - [20/Sep/2021:10:28:07 +0700] "HEAD /?t165856125205E264141956218 4B197485695597056606795091c HTTP/1.1" 200
.vn"
44.195.48.154 - - [20/Sep/2021:10:28:07 +0700] "HEAD /?t165856125205E2641419562184B197485695597056606795091c HTTP/1.1" 444
.vn"
123.30.148.87 - - [20/Sep/2021:10:28:07 +0700] "HEAD /?N449369542859198706035666vw146885195312524275004032 8A HTTP/1.1" 200
.vn"
123.30.148.87 - - [20/Sep/2021:10:28:07 +0700] "HEAD /?N449369542859198706035666vw1468851953125242750040328A HTTP/1.1" 200
.vn"
123.30.148.87 - - [20/Sep/2021:10:28:07 +0700] "HEAD /?N449369542859198706035666vw1468851953125242750040328A HTTP/1.1" 200
.vn"
123.30.148.87 - - [20/Sep/2021:10:28:07 +0700] "HEAD /?N449369542859198706035666vw1468851953125242750040328A HTTP/1.1" 200
.vn"
123.30.148.87 - - [20/Sep/2021:10:28:07 +0700] "HEAD /?N449369542859198706035666vw1468851953125242750040328A HTTP/1.1" 200
.vn"
123.30.148.87 - - [20/Sep/2021:10:28:07 +0700] "HEAD /?N449369542859198706035666vw1468851953125242750040328A HTTP/1.1" 200
.vn"
123.30.148.87 - - [20/Sep/2021:10:28:07 +0700] "HEAD /?N449369542859198706035666vw1468851953125242750040328A HTTP/1.1" 200
.vn"
123.30.148.87 - - [20/Sep/2021:10:28:07 +0700] "HEAD /?N449369542859198706035666vw1468851953125242750040328A HTTP/1.1" 200
.vn"
123.30.148.87 - - [20/Sep/2021:10:28:07 +0700] "HEAD /?N449369542859198706035666vw1468851953125242750040328A HTTP/1.1" 200
.vn"
123.30.148.87 - - [20/Sep/2021:10:28:07 +0700] "HEAD /?N449369542859198706035666vw1468851953125242750040328A HTTP/1.1" 200
.vn"
123.30.148.87 - - [20/Sep/2021:10:28:07 +0700] "HEAD /?N449369542859198706035666vw1468851953125242750040328A HTTP/1.1" 200
.vn"
```

Random Query String



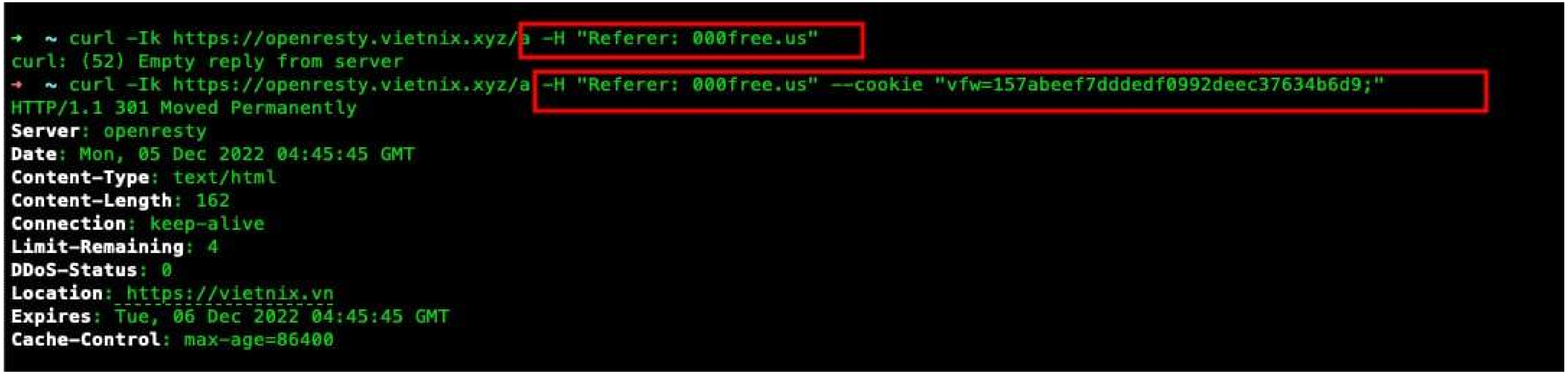
```
207.154.240.108 - - [31/Jan/2023:16:57:02 +0700] "GET //?830511052814417950IZc78616225614962663W HTTP/1.1" 200 3597 "https://www.fbi.com/shopanhm
onvu.com" "Mozilla/5.0 (Windows; U; ; en-NZ) AppleWebKit/527  (KHTML, like Gecko, Safari/419.3) Arora/0.8.0"
134.209.105.160 - - [31/Jan/2023:16:57:02 +0700] "GET //?568996575169727340tUy185203989596145494X HTTP/1.1" 200 3641 "https://www.fbi.com/shopanh
monvu.com" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US) AppleWebKit/533.17.8 (KHTML, like Gecko) Version/5.0.1 Safari/533.17.8"
199.249.230.146 - - [31/Jan/2023:16:57:03 +0700] "GET //?755400603086890586raM814269858575665662P HTTP/1.1" 200 12285 "https://www.fbi.com/shopan
hmonvu.com" "Mozilla/5.0 (Windows NT 6.2) AppleWebKit/536.3 (KHTML, like Gecko) Chrome/19.0.1061.1 Safari/536.3"
103.127.204.104 - - [31/Jan/2023:16:57:04 +0700] "GET //?50040889819450476ErB76260943173763059Z HTTP/1.1" 200 3597 "https://www.google.com/search
?q=shopanhmonvu.com" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:2.0.1) Gecko/20100101 Firefox/4.0.1"
95.165.163.194 - - [31/Jan/2023:16:57:08 +0700] "GET //?64602398330314182WCL715901393969006617H HTTP/1.1" 200 12255 "https://www.bing.com/search?
q=shopanhmonvu.com" "Mozilla/5.0 (X11; U; FreeBSD; i386; en-US; rv:1.7) Gecko"
134.209.105.160 - - [31/Jan/2023:16:57:08 +0700] "GET //?821281931175355429WBI382150048356416561l HTTP/1.1" 200 12255 "https://www.fbi.com/shopan
hmonvu.com" "Mozilla/5.0 (X11; Linux i686; rv:8.0) Gecko/20100101 Firefox/8.0"
188.166.234.144 - - [31/Jan/2023:16:57:09 +0700] "GET //?634864621485304291acl416866844080224005c HTTP/1.1" 200 12255 "https://www.youtube.com/sh
opanhmonvu.com" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:10.0.1) Gecko/20100101 Firefox/10.0.1"
42.118.214.120 - - [31/Jan/2023:16:57:09 +0700] "GET / HTTP/2.0" 200 0 "https://www.youtube.com/" "Mozilla/5.0 (Linux; Android 8.1.0; CPH1912) Ap
pleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Mobile Safari/537.36"
43.153.97.32 - - [31/Jan/2023:16:57:09 +0700] "GET //?275815641549840043hLz490198915686488536n HTTP/1.1" 200 12255 "https://www.facebook.com/shop
anhmonvu.com" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US) AppleWebKit/532.9 (KHTML, like Gecko) Chrome/5.0.310.0 Safari/532.9"
142.4.8.1 - - [31/Jan/2023:16:57:10 +0700] "GET //?260298881952741745HCI342466023344144152K HTTP/1.1" 200 12255 "https://check-host.net/shopanhmo
nvu.com" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.7 (KHTML, like Gecko) Chrome/7.0.514.0 Safari/534.7"
134.209.105.160 - - [31/Jan/2023:16:57:05 +0700] "GET //?990416789132530332bOR576714250391906358k HTTP/1.1" 200 3597 "https://www.facebook.com/sh
opanhmonvu.com" "Mozilla/5.0 (X11; Linux i686 on x86_64; rv:2.0.1) Gecko/20100101 Firefox/4.0.1"
45.118.145.52 - - [31/Jan/2023:16:57:06 +0700] "GET //?719510370754682352Lvz635127539593164156g HTTP/1.1" 200 3597 "https://www.google.com/search
?q=shopanhmonvu.com" "Mozilla/5.0 (X11; Linux i686; rv:10.0.1) Gecko/20100101 Firefox/10.0.1 SeaMonkey/2.7.1"
45.148.121.253 - - [31/Jan/2023:16:57:10 +0700] "GET //?963035557215446434gjv169193640311627159H HTTP/1.1" 200 12255 "https://www.youtube.com/sho
panhmonvu.com" "Mozilla/5.0 (X11; Linux i686; rv:10.0.1) Gecko/20100101 Firefox/10.0.1 SeaMonkey/2.7.1"
61.147.15.67 - - [31/Jan/2023:16:57:10 +0700] "GET / HTTP/1.1" 200 15159 "-" "Mozilla/5.0 (Linux; U; Android 7.1.1; zh-CN; OPPO R11s Plus Build/N
MF26X) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/57.0.2987.108 UCBrowser/11.9.4.974 UWS/2.14.0.2 Mobile Safari/537.36 AliApp(TB/7
.7.5) UCBS/2.11.1.1 TTID/231200@taobao_android_7.7.5 WindVane/8.3.0 1080X2016"
45.148.121.253 - - [31/Jan/2023:16:57:11 +0700] "GET //?980199814200153562Hsm886743001483697441N HTTP/1.1" 200 12255 "https://www.facebook.com/sh
opanhmonvu.com" "Mozilla/5.0 (X11; Linux i686; rv:6.0a2) Gecko/20110615 Firefox/6.0a2 Iceweasel/6.0a2"
128.199.202.48 - - [31/Jan/2023:16:57:06 +0700] "GET //?343175381132760525FvF666786719351875898q HTTP/1.1" 200 12329 "https://www.youtube.com/sho
panhmonvu.com" "Mozilla/5.0 (X11; Linux x86_64; rv:11.0a2) Gecko/20111230 Firefox/11.0a2 Iceweasel/11.0a2"
178.62.229.24 - - [31/Jan/2023:16:57:11 +0700] "GET //?906984234305896082eVk400647430494464884o HTTP/1.1" 200 0 "https://www.fbi.com/shopanhmonvu
.com" "Mozilla/5.0 (Windows; U; Windows NT 6.1; en-GB; rv:1.9.1.17) Gecko/20110123 (like Firefox/3.x) SeaMonkey/2.0.12"
45.148.121.253 - - [31/Jan/2023:16:57:11 +0700] "GET //?309964788415655459SYq185486414594413188j HTTP/1.1" 200 12255 "https://www.bing.com/search
?q=shopanhmonvu.com" "Mozilla/5.0 (X11; U; Linux i686; en-us) AppleWebKit/528.5  (KHTML, like Gecko, Safari/528.5 ) lt-GtkLauncher"
45.148.121.253 - - [31/Jan/2023:16:57:12 +0700] "GET //?330606573891018936QZV620377506015316902j HTTP/1.1" 200 12255 "https://www.fbi.com/shopanh
monvu.com" "Mozilla/5.0 (Android; Linux armv7l; rv:2.0.1) Gecko/20100101 Firefox/4.0.1 Fennec/2.0.1"
```

Khác: Random User Agent



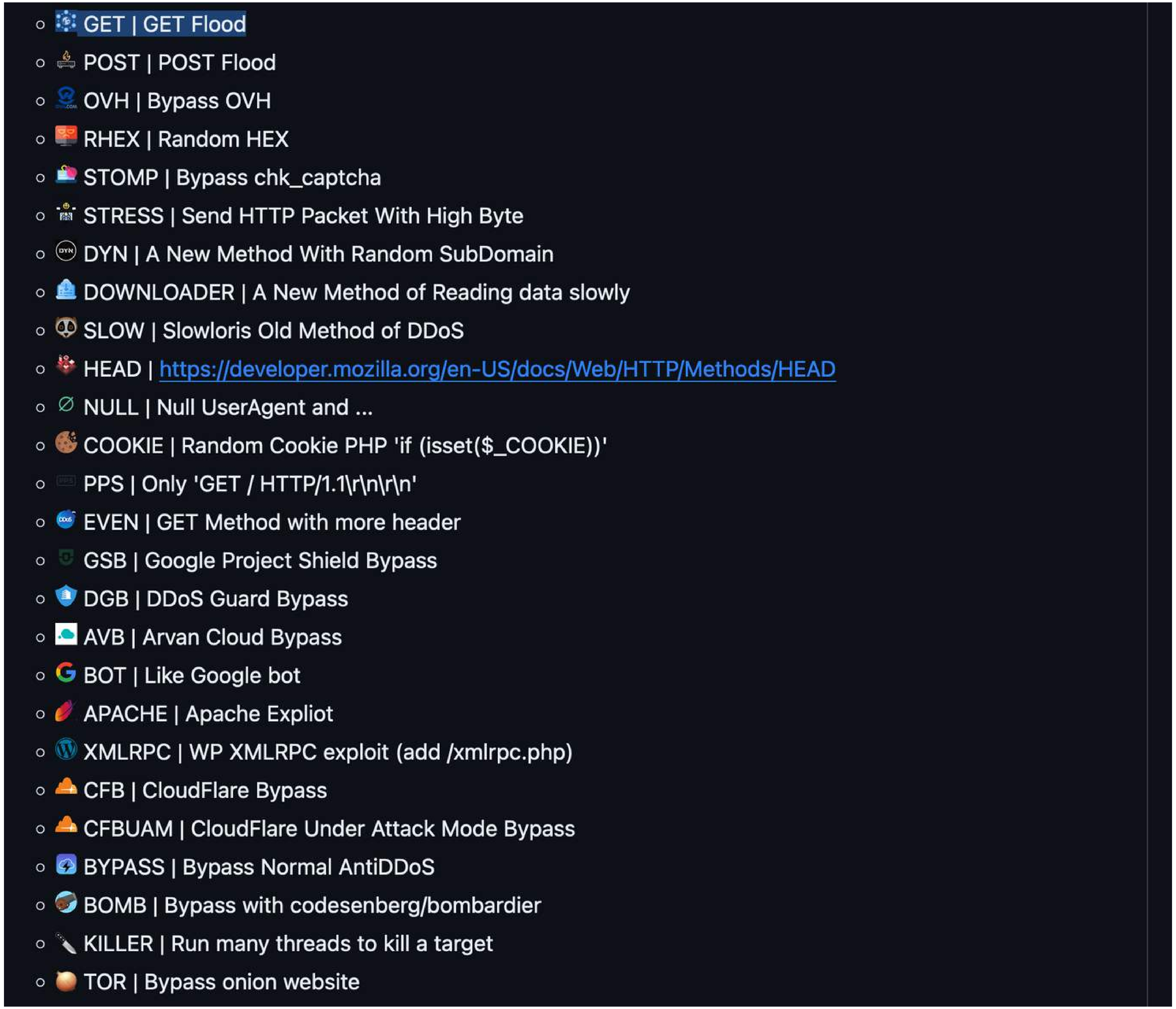
```
154.84.141.208 - - [17/Dec/2023:23:59:58 +0700] "GET / HTTP/1.1" 200 6318 "-" "R29VZ2XLL09WZXJHIDQ0LJQ0LJQ0ICHXaW5Kb3DZIE5UIDEWLJA7IERFOYBLbI1HQIK="
154.84.141.18 - - [17/Dec/2023:23:59:59 +0700] "GET / HTTP/1.1" 200 6320 "-" "QXBWbGUVRMLYZWZVeCA2MI42MI42MIAOTGLUdXG7IERFOYBLbI1VUYK="
154.201.37.69 - - [17/Dec/2023:23:59:59 +0700] "GET / HTTP/1.1" 200 6317 "-" "QXBwBGUVT3BLcMEgOTAUOTAUOTAgKEFUZHJVaWQ7IEZSOyBKZS1ERSk="
154.201.37.69 - - [17/Dec/2023:23:59:59 +0700] "GET / HTTP/1.1" 200 6319 "-" "QXBwBGUVT3BLcMEgOTAUOTAUOTAgKEFUZHJVaWQ7IEZSOyBKZS1ERSk="
154.201.37.69 - - [17/Dec/2023:23:59:59 +0700] "GET / HTTP/1.1" 200 6319 "-" "QXBwBGUVT3BLcMEgOTAUOTAUOTAgKEFUZHJVaWQ7IEZSOyBKZS1ERSk="
154.84.141.208 - - [17/Dec/2023:23:59:58 +0700] "GET / HTTP/1.1" 200 6319 "-" "R29VZ2XLL09WZXJHIDQ0LJQ0LJQ0ICHXaW5Kb3DZIE5UIDEWLJA7IERFOYBLbI1HQIK="
154.201.37.69 - - [17/Dec/2023:23:59:59 +0700] "GET / HTTP/1.1" 200 6320 "-" "QXBwBGUVT3BLcMEgOTAUOTAUOTAgKEFUZHJVaWQ7IEZSOyBKZS1ERSk="
154.84.141.208 - - [17/Dec/2023:23:59:58 +0700] "GET / HTTP/1.1" 200 6319 "-" "R29VZ2XLL09WZXJHIDQ0LJQ0LJQ0ICHXaW5Kb3DZIE5UIDEWLJA7IERFOYBLbI1HQIK="
154.84.141.18 - - [17/Dec/2023:23:59:59 +0700] "GET / HTTP/1.1" 503 719 "-" "QXBWbGUVRMLYZWZVeCA2MI42MI42MIAOTGLUdXG7IERFOYBLbI1VUYK="
154.84.141.18 - - [17/Dec/2023:23:59:59 +0700] "GET / HTTP/1.1" 503 719 "-" "TWLJCm9ZB2Z0L0VkZ2UGMTAWLjEWMC4XMDAgKE1HY2LUDG9ZADsGVVM7IGVULUDCKQ=="
154.84.141.18 - - [17/Dec/2023:23:59:59 +0700] "GET / HTTP/1.1" 503 719 "-" "TWLJCm9ZB2Z0L0VkZ2UGMTAWLjEWMC4XMDAgKE1HY2LUDG9ZADsGVVM7IGVULUDCKQ=="
104.252.179.170 - - [17/Dec/2023:23:59:59 +0700] "GET / HTTP/1.1" 200 6317 "-" "TW96AWxSYS9FZGDLIDc1LJC1LJC1IChXAW5Kb3DZIE5UIDYUMZSGVVM7IGRLLURFKQ=="
104.252.179.170 - - [17/Dec/2023:23:59:59 +0700] "GET / HTTP/1.1" 200 6320 "-" "TW96AWxSYS9FZGDLIDc1LJC1LJC1IChXAW5Kb3DZIE5UIDYUMZSGVVM7IGRLLURFKQ=="
104.252.179.170 - - [17/Dec/2023:23:59:59 +0700] "GET / HTTP/1.1" 200 6319 "-" "TW96AWxSYS9FZGDLIDc1LJC1LJC1IChXAW5Kb3DZIE5UIDYUMZSGVVM7IGRLLURFKQ=="
154.84.141.18 - - [17/Dec/2023:23:59:58 +0700] "GET / HTTP/1.1" 200 0 "-" "WLJCm9ZB2Z0L0VkZ2UGMTAWLjEWMC4XMDAgKE1HY2LUDG9ZADsGVVM7IGVULUDCKQ=="
154.84.141.18 - - [17/Dec/2023:23:59:58 +0700] "GET / HTTP/1.1" 200 0 "-" "WLJCm9ZB2Z0L0VkZ2UGMTAWLjEWMC4XMDAgKE1HY2LUDG9ZADsGVVM7IGVULUDCKQ=="
154.84.141.18 - - [17/Dec/2023:23:59:58 +0700] "GET / HTTP/1.1" 200 0 "-" "WLJCm9ZB2Z0L0VkZ2UGMTAWLjEWMC4XMDAgKE1HY2LUDG9ZADsGVVM7IGVULUDCKQ=="
154.84.141.18 - - [17/Dec/2023:23:59:58 +0700] "GET / HTTP/1.1" 200 0 "-" "WLJCm9ZB2Z0L0VkZ2UGMTAWLjEWMC4XMDAgKE1HY2LUDG9ZADsGVVM7IGVULUDCKQ=="
172.121.142.127 - - [17/Dec/2023:23:59:58 +0700] "GET / HTTP/1.1" 200 0 "-" "TWLJCM9ZB2Z0L0ZPCMVMB3GGNJEUNJEUNJEGKFDPBMRVD3MGTLQGMTAUMDSGREU7IGVZLUVTKQ=="
172.121.142.127 - - [17/Dec/2023:23:59:58 +0700] "GET / HTTP/1.1" 200 0 "-" "TWLJCM9ZB2Z0L0ZPCMVMB3GGNJEUNJEUNJEGKFDPBMRVD3MGTLQGMTAUMDSGREU7IGVZLUVTKQ=="
172.121.142.127 - - [17/Dec/2023:23:59:58 +0700] "GET / HTTP/1.1" 200 0 "-" "TWLJCM9ZB2Z0L0ZPCMVMB3GGNJEUNJEUNJEGKFDPBMRVD3MGTLQGMTAUMDSGREU7IGVZLUVTKQ=="
172.121.142.127 - - [17/Dec/2023:23:59:58 +0700] "GET / HTTP/1.1" 200 0 "-" "TWLJCM9ZB2Z0L0ZPCMVMB3GGNJEUNJEUNJEGKFDPBMRVD3MGTLQGMTAUMDSGREU7IGVZLUVTKQ=="
172.121.142.127 - - [17/Dec/2023:23:59:58 +0700] "GET / HTTP/1.1" 200 0 "-" "TWLJCM9ZB2Z0L0ZPCMVMB3GGNJEUNJEUNJEGKFDPBMRVD3MGTLQGMTAUMDSGREU7IGVZLUVTKQ=="
172.121.142.127 - - [17/Dec/2023:23:59:58 +0700] "GET / HTTP/1.1" 200 0 "-" "TWLJCM9ZB2Z0L0ZPCMVMB3GGNJEUNJEUNJEGKFDPBMRVD3MGTLQGMTAUMDSGREU7IGVZLUVTKQ=="
172.121.142.127 - - [17/Dec/2023:23:59:58 +0700] "GET / HTTP/1.1" 200 0 "-" "TWLJCM9ZB2Z0L0ZPCMVMB3GGNJEUNJEUNJEGKFDPBMRVD3MGTLQGMTAUMDSGREU7IGVZLUVTKQ=="
172.121.142.127 - - [17/Dec/2023:23:59:58 +0700] "GET / HTTP/1.1" 200 0 "-" "TWLJCM9ZB2Z0L0ZPCMVMB3GGNJEUNJEUNJEGKFDPBMRVD3MGTLQGMTAUMDSGREU7IGVZLUVTKQ=="
156.239.52.150 - - [17/Dec/2023:23:59:58 +0700] "GET / HTTP/1.1" 200 0 "-" "QXBWbGUVRMlYZWZVeCAXMC4XMC4XMCAOV2lUZG93cYBOVCA2LJM7IFVTOYBLcY1FUYk="
154.84.141.208 - - [17/Dec/2023:23:59:58 +0700] "GET / HTTP/1.1" 200 6319 "-" "R29VZ2XLL09WZXJHIDQ0LJQ0LJQ0ICHXaW5Kb3DZIE5UIDEWLJA7IERFOYBLbI1HQIK="
154.84.141.208 - - [17/Dec/2023:23:59:58 +0700] "GET / HTTP/1.1" 200 6318 "-" "R29VZ2XLL09WZXJHIDQ0LJQ0LJQ0ICHXaW5Kb3DZIE5UIDEWLJA7IERFOYBLbI1HQIK="
154.84.141.208 - - [17/Dec/2023:23:59:58 +0700] "GET / HTTP/1.1" 200 6319 "-" "R29VZ2XLL09WZXJHIDQ0LJQ0LJQ0ICHXaW5Kb3DZIE5UIDEWLJA7IERFOYBLbI1HQIK="
154.84.141.208 - - [17/Dec/2023:23:59:58 +0700] "GET / HTTP/1.1" 200 6319 "-" "R29VZ2XLL09WZXJHIDQ0LJQ0LJQ0ICHXaW5Kb3DZIE5UIDEWLJA7IERFOYBLbI1HQIK="
142.252.26.2 - - [17/Dec/2023:23:59:58 +0700] "GET / HTTP/1.1" 200 6319 "-" "T3BlcmEgU29mdHdhcmUvQ2hyb21lIDU1LjU1LjU1IChNYWNpbnRvc2g7IEVTOyBmci1GUik="
154.84.141.208 - - [17/Dec/2023:23:59:58 +0700] "GET / HTTP/1.1" 200 6319 "-" "R29VZ2XLL09WZXJHIDQ0LJQ0LJQ0ICHXaW5Kb3DZIE5UIDEWLJA7IERFOYBLbI1HQIK="
142.252.26.2 - - [17/Dec/2023:23:59:58 +0700] "GET / HTTP/1.1" 200 6319 "-" "T3BlcmEgU29mdHdhcmUvQ2hyb21lIDU1LjU1LjU1IChNYWNpbnRvc2g7IEVTOyBmci1GUik="
154.84.141.208 - - [17/Dec/2023:23:59:58 +0700] "GET / HTTP/1.1" 200 6319 "-" "R29VZ2XLL09WZXJHIDQ0LJQ0LJQ0ICHXaW5Kb3DZIE5UIDEWLJA7IERFOYBLbI1HQIK="
154.84.141.208 - - [17/Dec/2023:23:59:58 +0700] "GET / HTTP/1.1" 200 6313 "-" "R29VZ2XLL09WZXJHIDQ0LJQ0LJQ0ICHXaW5Kb3DZIE5UIDEWLJA7IERFOYBLbI1HQIK="
154.84.141.208 - - [17/Dec/2023:23:59:58 +0700] "GET / HTTP/1.1" 200 6319 "-" "R29VZ2XLL09WZXJHIDQ0LJQ0LJQ0ICHXaW5Kb3DZIE5UIDEWLJA7IERFOYBLbI1HQIK="
166.88.122.216 - - [17/Dec/2023:23:59:58 +0700] "GET / HTTP/1.1" 200 6319 "-" "QXBWbGUVQ2HYb21LIDEUMS4XICHXaW5Kb3DZIE5UIDEWLJA7IFVTOYBKZS1ERSK="
154.84.141.208 - - [17/Dec/2023:23:59:58 +0700] "GET / HTTP/1.1" 200 6319 "-" "R29VZ2XLL09WZXJHIDQ0LJQ0LJQ0ICHXaW5Kb3DZIE5UIDEWLJA7IERFOYBLbI1HQIK="
154.84.141.18 - - [17/Dec/2023:23:59:59 +0700] "GET / HTTP/1.1" 200 6319 "-" "TWLJCm9ZB2Z0L0VkZ2UGMTAWLjEWMC4XMDAgKE1HY2LUDG9ZADsGVVM7IGVULUDCKQ=="
104.165.127.107 - - [17/Dec/2023:23:59:59 +0700] "GET / HTTP/1.1" 200 6318 "-" "T3BLCmEGU29MDHDhCMUVRWRNZSAXOS4XOS4xOSAOQW5KCm9PZDsGR0I7IGVULUDCKQ=="
104.252.179.170 - - [17/Dec/2023:23:59:59 +0700] "GET / HTTP/1.1" 200 6320 "-" "TW96AWxSYS9FZGDLIDc1LJC1LJC1IChXAW5Kb3DZIE5UIDYUMZSGVVM7IGRLLURFKQ=="
154.84.141.18 - - [17/Dec/2023:23:59:59 +0700] "GET / HTTP/1.1" 200 6319 "-" "QXBWbGUVRMLYZWZVeCA2MI42MI42MIAOTGLUdXG7IERFOYBLbI1VUYK="
154.201.37.69 - - [17/Dec/2023:23:59:59 +0700] "GET / HTTP/1.1" 200 6320 "-" "QXBwBGUVT3BLcMEgOTAUOTAUOTAgKEFUZHJVaWQ7IEZSOyBKZS1ERSk="
154.201.37.69 - - [17/Dec/2023:23:59:59 +0700] "GET / HTTP/1.1" 200 6319 "-" "QXBwBGUVT3BLcMEgOTAUOTAUOTAgKEFUZHJVaWQ7IEZSOyBKZS1ERSk="
154.84.141.18 - - [17/Dec/2023:23:59:59 +0700] "GET / HTTP/1.1" 200 6319 "-" "QXBWbGUVRMLYZWZVeCA2MI42MI42MIAOTGLUdXG7IERFOYBLbI1VUYK="
154.84.141.18 - - [17/Dec/2023:23:59:59 +0700] "GET / HTTP/1.1" 200 6319 "-" "QXBWbGUVRMLYZWZVeCA2MI42MI42MIAOTGLUdXG7IERFOYBLbI1VUYK="
104.252.179.170 - - [17/Dec/2023:23:59:59 +0700] "GET / HTTP/1.1" 200 6319 "-" "TW96AWxSYS9FZGDLIDc1LJC1LJC1IChXAW5Kb3DZIE5UIDYUMZSGVVM7IGRLLURFKQ=="
104.252.179.170 - - [17/Dec/2023:23:59:59 +0700] "GET / HTTP/1.1" 200 6319 "-" "TW96AWxSYS9FZGDLIDc1LJC1LJC1IChXAW5Kb3DZIE5UIDYUMZSGVVM7IGRLLURFKQ=="
154.201.37.69 - - [17/Dec/2023:23:59:59 +0700] "GET / HTTP/1.1" 200 6319 "-" "QXBwBGUVT3BLcMEgOTAUOTAUOTAgKEFUZHJVaWQ7IEZSOyBKZS1ERSk="
```

Challenge Bypass



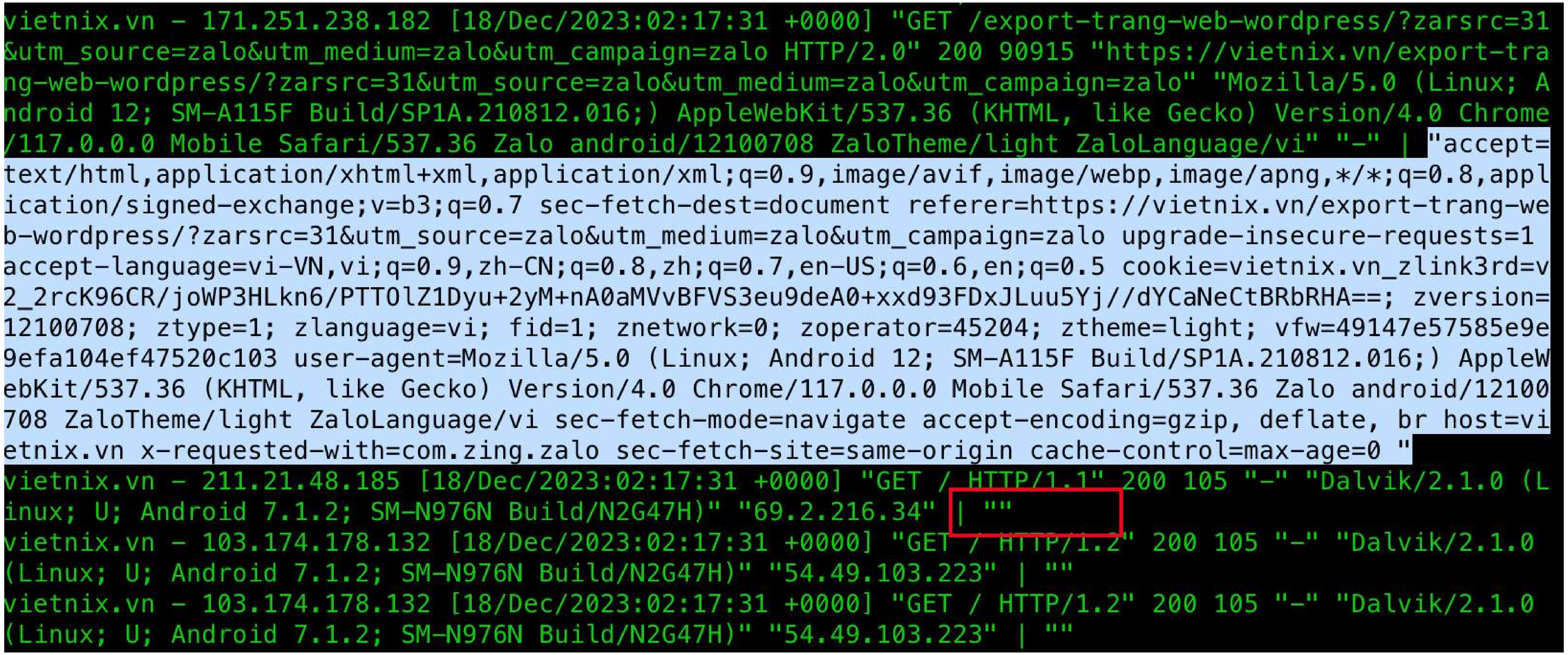
```
→  ~ curl -Ik https://openresty.vietnix.xyz/a -H "Referer: 000free.us"
curl: (52) Empty reply from server
→  ~ curl -Ik https://openresty.vietnix.xyz/a -H "Referer: 000free.us" --cookie "vfw=157abeef7dddedf0992deec37634b6d9;"
HTTP/1.1 301 Moved Permanently
Server: openresty
Date: Mon, 05 Dec 2022 04:45:45 GMT
Content-Type: text/html
Content-Length: 162
Connection: keep-alive
Limit-Remaining: 4
DDoS-Status: 0
Location: https://vietnix.vn
Expires: Tue, 06 Dec 2022 04:45:45 GMT
Cache-Control: max-age=86400
```

Các kiểu tấn công khác



- GET | GET Flood
- POST | POST Flood
- OVH | Bypass OVH
- RHEX | Random HEX
- STOMP | Bypass chk_captcha
- STRESS | Send HTTP Packet With High Byte
- DYN | A New Method With Random SubDomain
- DOWNLOADER | A New Method of Reading data slowly
- SLOW | Slowloris Old Method of DDoS
- HEAD | https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods/HEAD
- NULL | Null UserAgent and ...
- COOKIE | Random Cookie PHP 'if (isset($_COOKIE))'
- PPS | Only 'GET / HTTP/1.1\r\n\r\n'
- EVEN | GET Method with more header
- GSB | Google Project Shield Bypass
- DGB | DDoS Guard Bypass
- AVB | Arvan Cloud Bypass
- BOT | Like Google bot
- APACHE | Apache Expliot
- XMLRPC | WP XMLRPC exploit (add /xmlrpc.php)
- CFB | CloudFlare Bypass
- CFBUAM | CloudFlare Under Attack Mode Bypass
- BYPASS | Bypass Normal AntiDDoS
- BOMB | Bypass with codesenberg/bombardier
- KILLER | Run many threads to kill a target
- TOR | Bypass onion website

Request hợp lệ vs Request tấn công



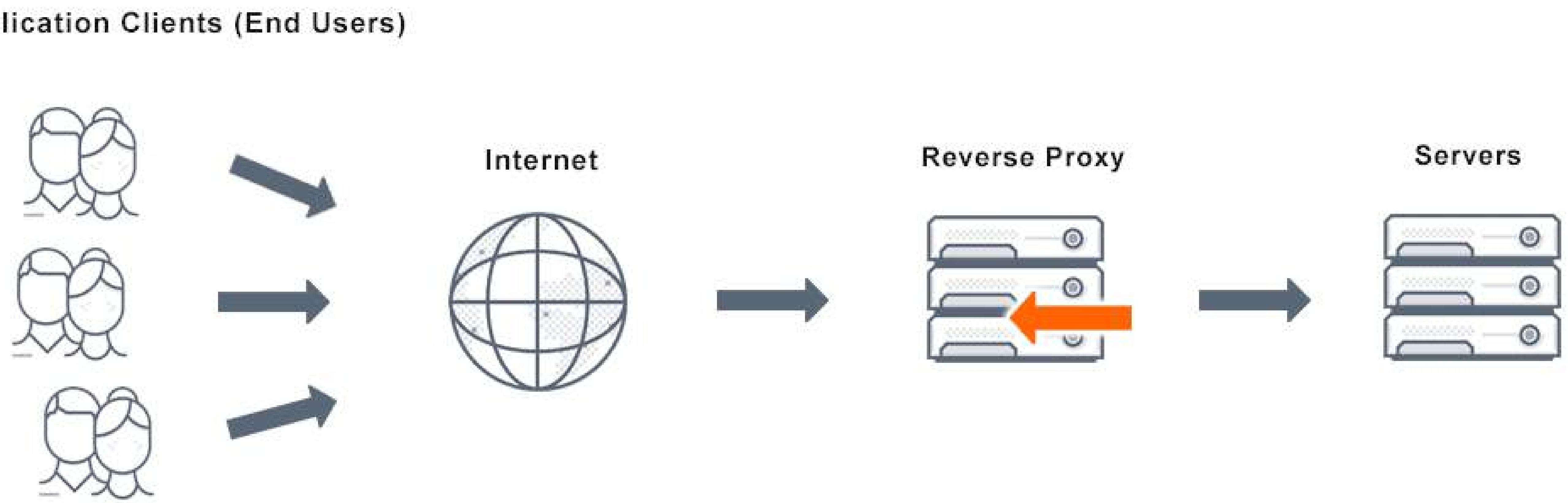
```
vietnix.vn - 171.251.238.182 [18/Dec/2023:02:17:31 +0000] "GET /export-trang-web-wordpress/?zarsrc=31
&utm_source=zalo&utm_medium=zalo&utm_campaign=zalo HTTP/2.0" 200 90915 "https://vietnix.vn/export-tra
ng-web-wordpress/?zarsrc=31&utm_source=zalo&utm_medium=zalo&utm_campaign=zalo" "Mozilla/5.0 (Linux; A
ndroid 12; SM-A115F Build/SP1A.210812.016;) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome
/117.0.0.0 Mobile Safari/537.36 Zalo android/12100708 ZaloTheme/light ZaloLanguage/vi" "-" | "accept=
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appl
ication/signed-exchange;v=b3;q=0.7 sec-fetch-dest=document referer=https://vietnix.vn/export-trang-we
b-wordpress/?zarsrc=31&utm_source=zalo&utm_medium=zalo&utm_campaign=zalo upgrade-insecure-requests=1
accept-language=vi-VN,vi;q=0.9,zh-CN;q=0.8,zh;q=0.7,en-US;q=0.6,en;q=0.5 cookie=vietnix.vn_zlink3rd=v
2_2rcK96CR/joWP3HLkn6/PTTOlZ1Dyu+2yM+nA0aMVvBFVS3eu9deA0+xxd93FDxJLuu5Yj//dYCaNeCtBRbRHA==; zversion=
12100708; ztype=1; zlanguage=vi; fid=1; znetwork=0; zoperator=45204; ztheme=light; vfw=49147e57585e9e
9efa104ef47520c103 user-agent=Mozilla/5.0 (Linux; Android 12; SM-A115F Build/SP1A.210812.016;) AppleW
ebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/117.0.0.0 Mobile Safari/537.36 Zalo android/12100
708 ZaloTheme/light ZaloLanguage/vi sec-fetch-mode=navigate accept-encoding=gzip, deflate, br host=vi
etnix.vn x-requested-with=com.zing.zalo sec-fetch-site=same-origin cache-control=max-age=0 "
vietnix.vn - 211.21.48.185 [18/Dec/2023:02:17:31 +0000] "GET / HTTP/1.1" 200 105 "-" "Dalvik/2.1.0 (L
inux; U; Android 7.1.2; SM-N976N Build/N2G47H)" "69.2.216.34" | ""
vietnix.vn - 103.174.178.132 [18/Dec/2023:02:17:31 +0000] "GET / HTTP/1.2" 200 105 "-" "Dalvik/2.1.0
(Linux; U; Android 7.1.2; SM-N976N Build/N2G47H)" "54.49.103.223" | ""
vietnix.vn - 103.174.178.132 [18/Dec/2023:02:17:31 +0000] "GET / HTTP/1.2" 200 105 "-" "Dalvik/2.1.0
(Linux; U; Android 7.1.2; SM-N976N Build/N2G47H)" "54.49.103.223" | ""
```

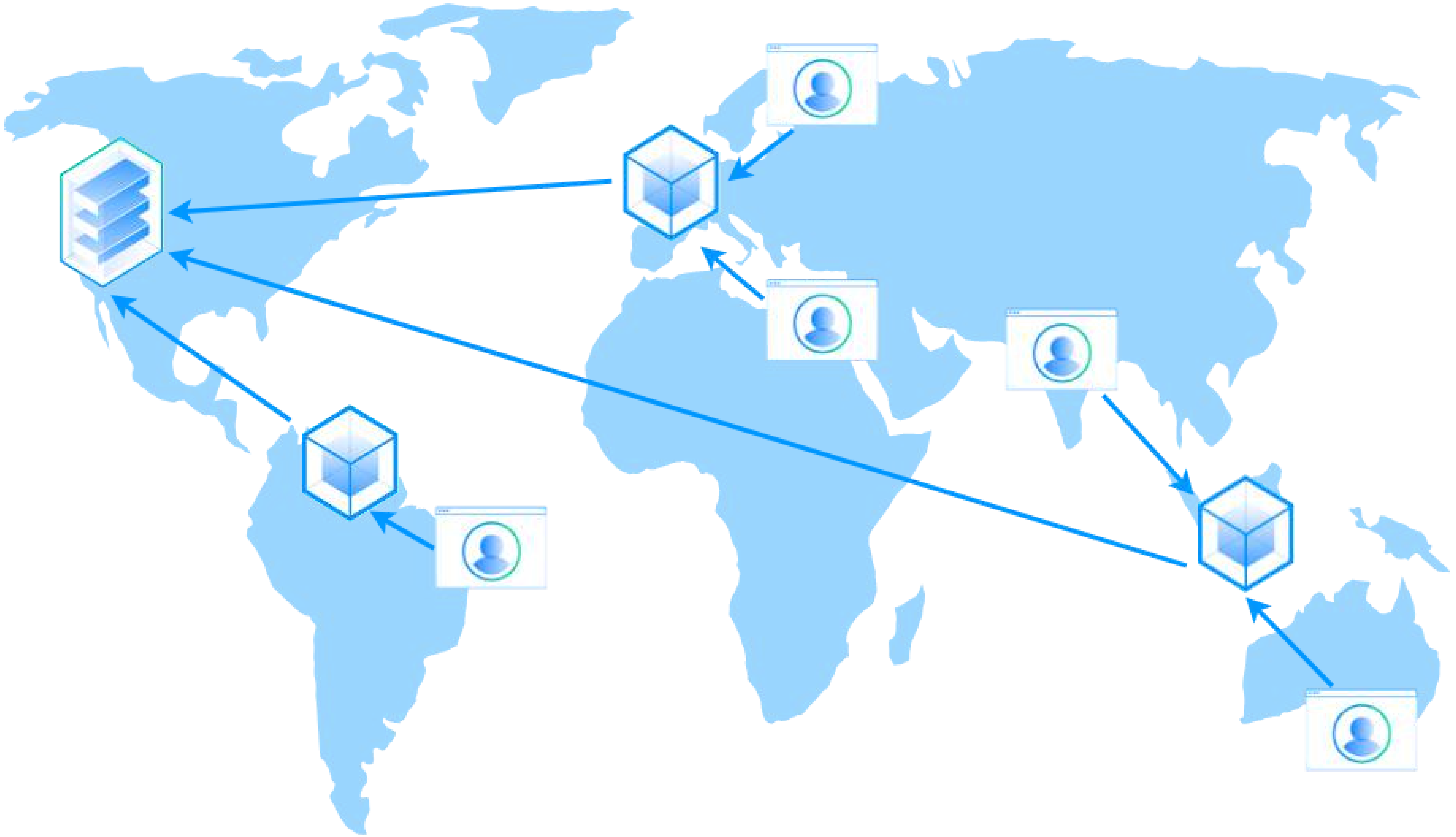
Kiểu tấn công Anti DDos Firewall Bypass (Bypass CloudFlare)

Nguyên tắc chung:

Đẩy **càng nhiều** requests về BACKEND server **càng tốt**!!

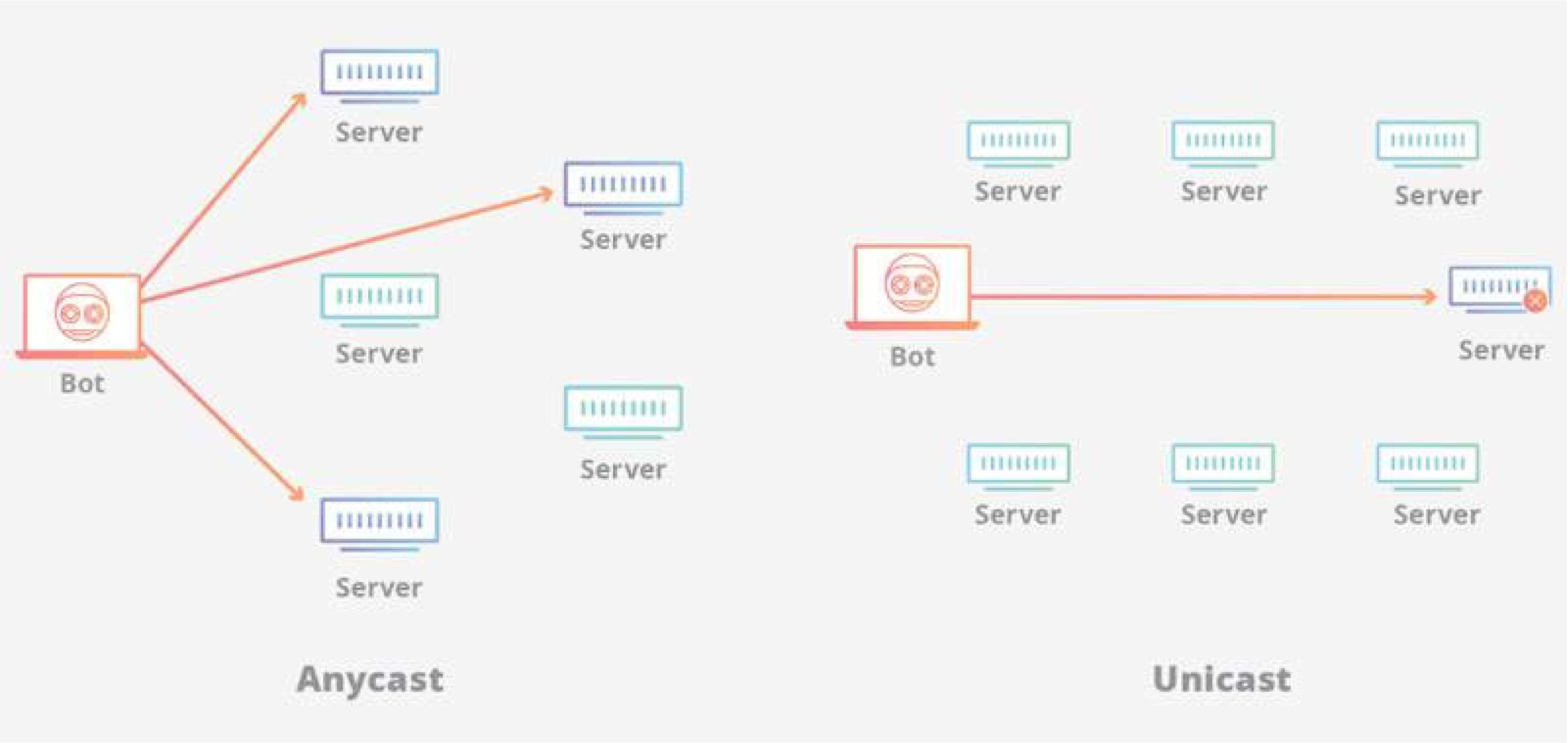
Mô hình Web Firewall đơn giản (Reverse Proxy)





Content Delivery Network (CDN)

Anycast


Server
Server
Server
Server
Server
Bot
Anycast
Server
Server
Server
Bot
Server
Server
Server
Server
Unicast

CloudFlare (CF) và cách bypass CloudFlare

- Hoạt động ở Layer 7
- Mặc định, CF không cache HTML, chỉ cache static content
- Nếu bật “Cache EveryThing”: cache key =

  md5sum(**$zone_id:$scheme://$hostname$request_uri**) =

  md5sum(123abc:https://tuoitre.vn/?asdb3f=1h8dca3hfj2) =

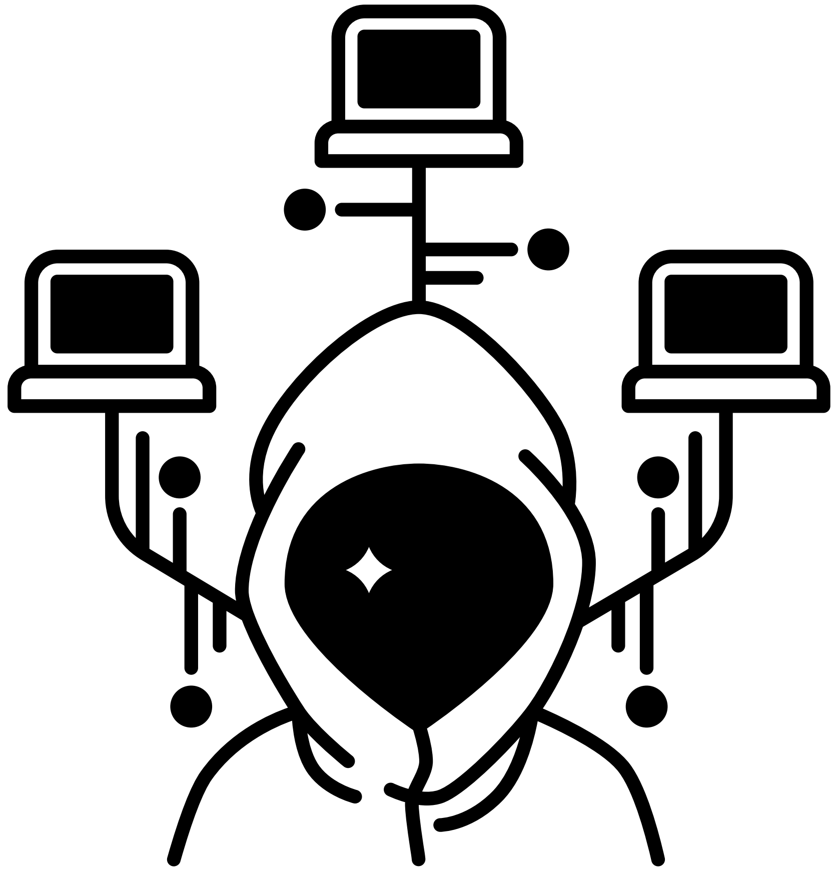
  258580a80ba7e32b9c46dad524877118
- POST sẽ không được cache

Tham khảo: https://quantrilinux.vn/chong-ddos-bypass-cloudflare-bang-csf-p1.html

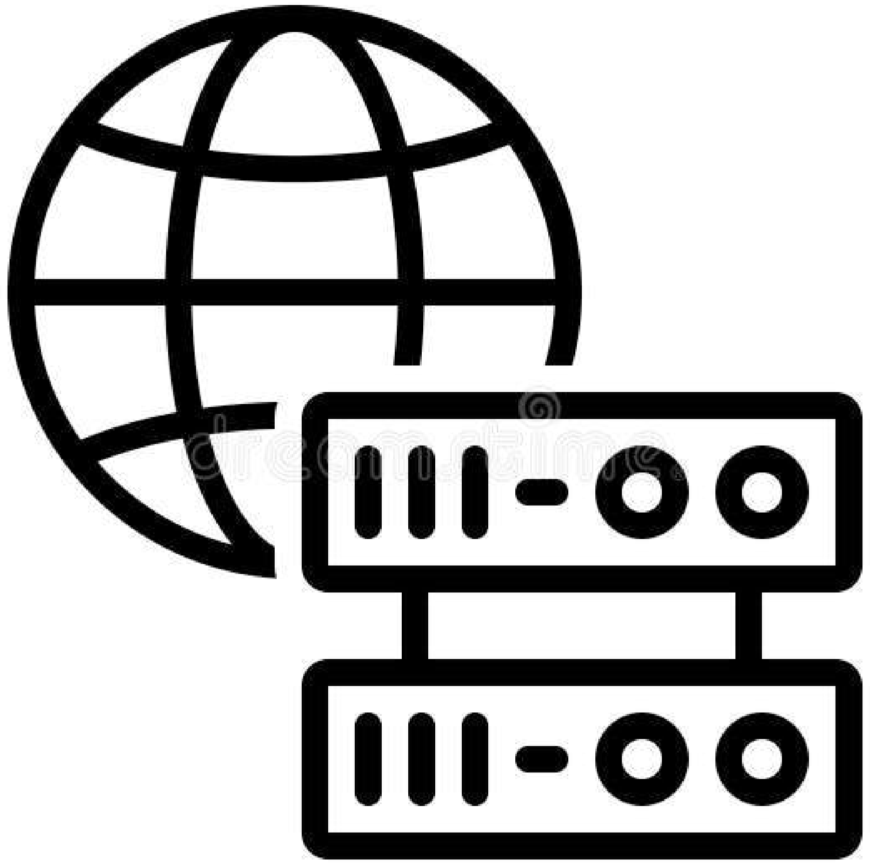
Nếu tấn công SYN Flood vào web trỏ về CF thì có ảnh hưởng backend không?

Nguồn Tấn Công Web

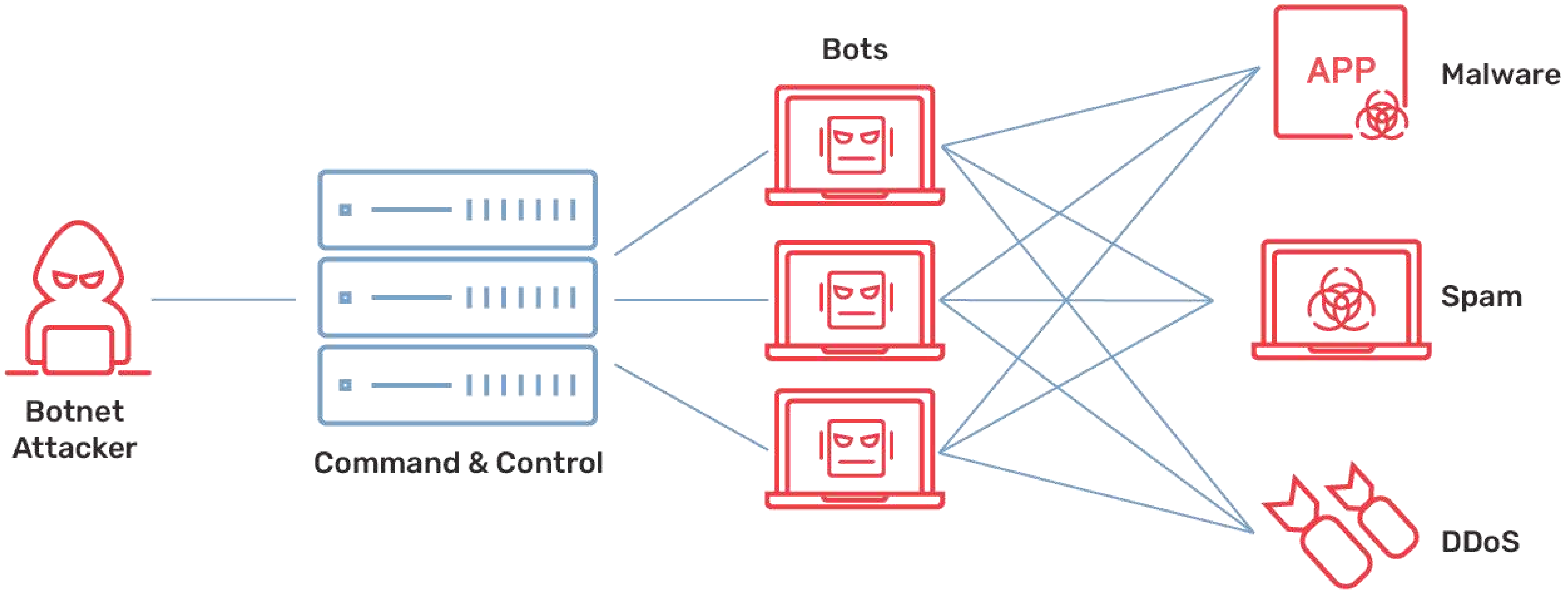
Botnets



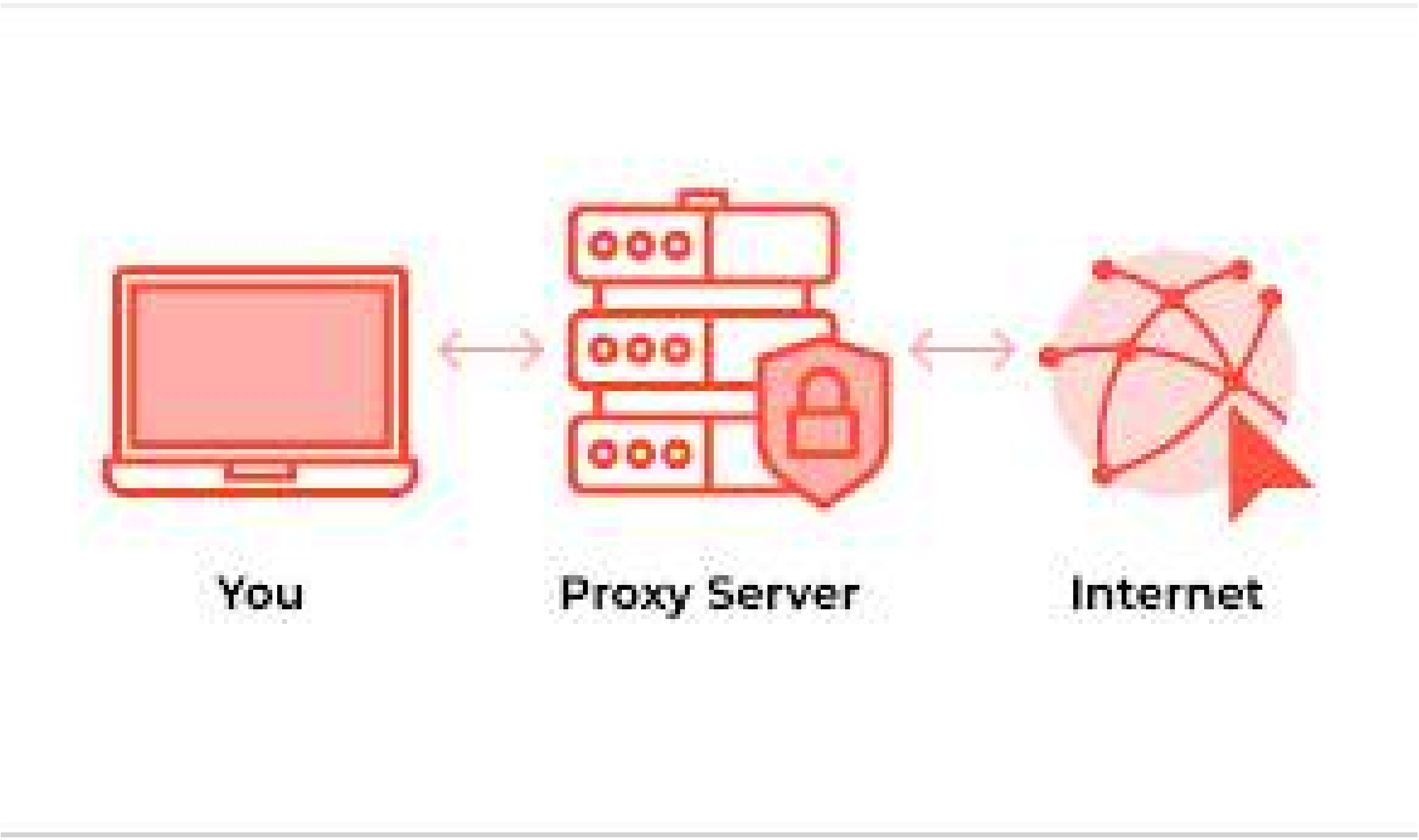
Public Proxy



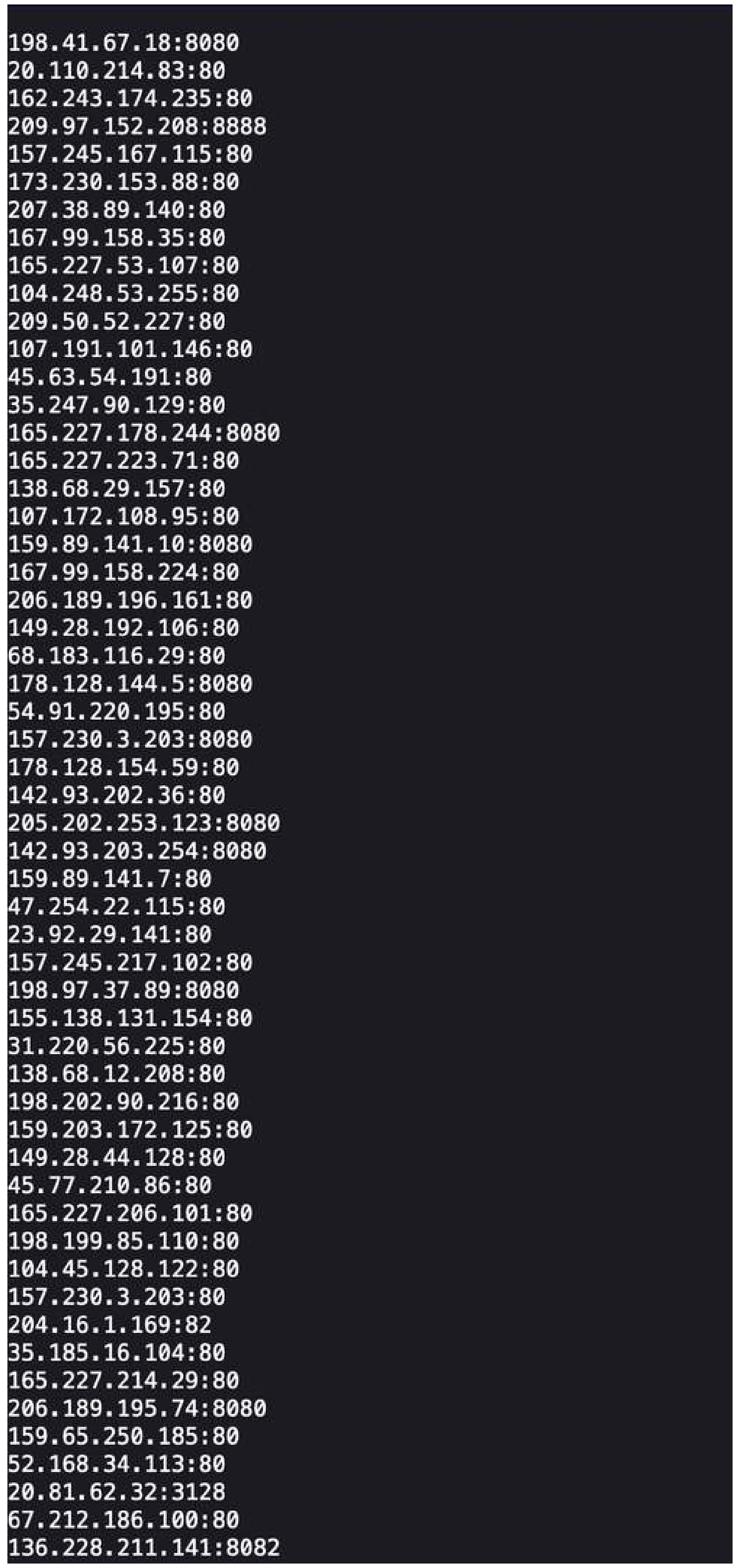
Botnets


Botnet
Attacker
Command & Control
Bots
APP
Malware
Spam
DDoS

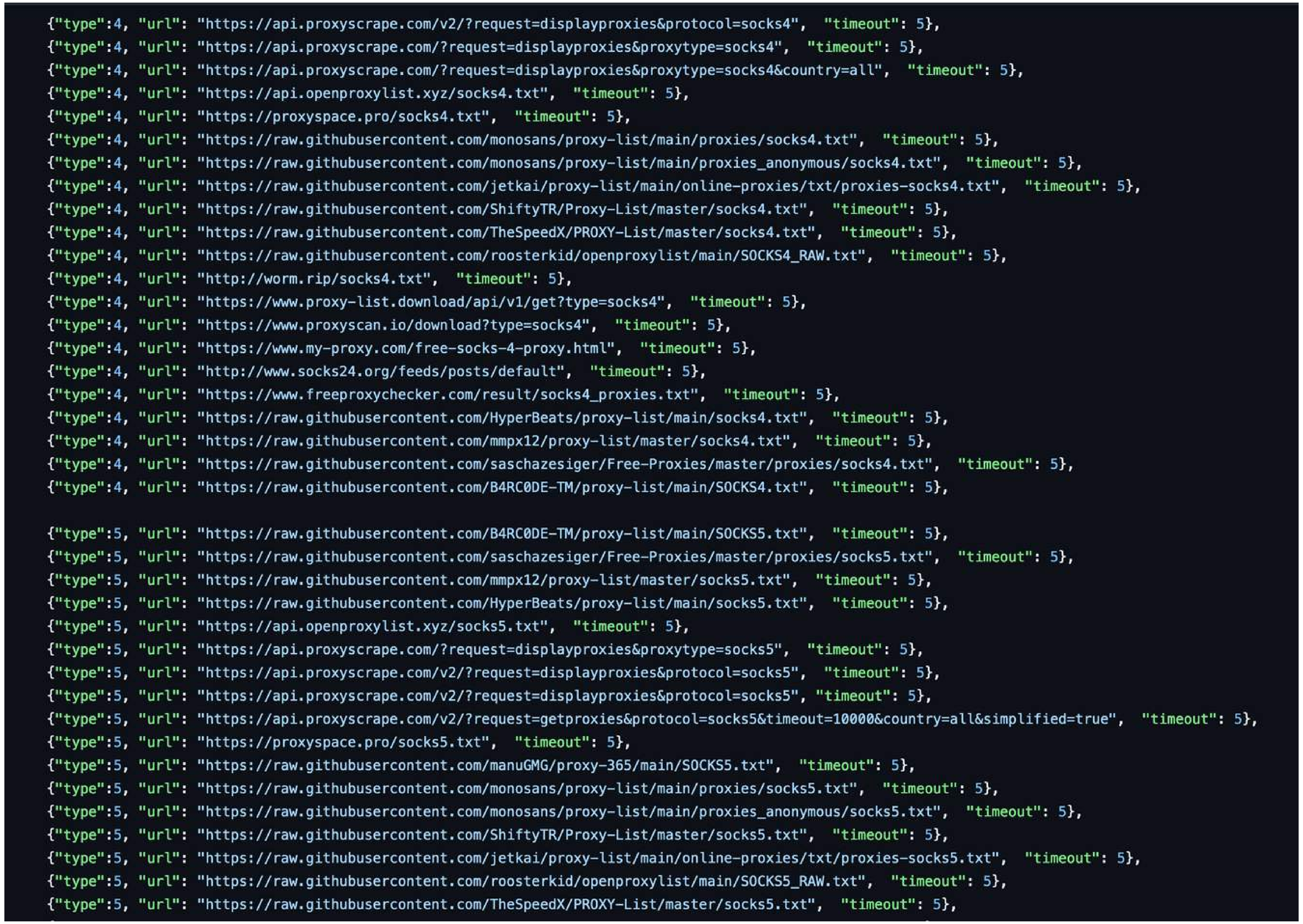
Public Proxy



Public Proxy



```
198.41.67.18:8080
20.110.214.83:80
162.243.174.235:80
209.97.152.208:8888
157.245.167.115:80
173.230.153.88:80
207.38.89.140:80
167.99.158.35:80
165.227.53.107:80
104.248.53.255:80
209.50.52.227:80
107.191.101.146:80
45.63.54.191:80
35.247.90.129:80
165.227.178.244:8080
165.227.223.71:80
138.68.29.157:80
107.172.108.95:80
159.89.141.10:8080
167.99.158.224:80
206.189.196.161:80
149.28.192.106:80
68.183.116.29:80
178.128.144.5:8080
54.91.220.195:80
157.230.3.203:8080
178.128.154.59:80
142.93.202.36:80
205.202.253.123:8080
142.93.203.254:8080
159.89.141.7:80
47.254.22.115:80
23.92.29.141:80
157.245.217.102:80
198.97.37.89:8080
155.138.131.154:80
31.220.56.225:80
138.68.12.208:80
198.202.90.216:80
159.203.172.125:80
149.28.44.128:80
45.77.210.86:80
165.227.206.101:80
198.199.85.110:80
104.45.128.122:80
157.230.3.203:80
204.16.1.169:82
35.185.16.104:80
165.227.214.29:80
206.189.195.74:8080
159.65.250.185:80
52.168.34.113:80
20.81.62.32:3128
67.212.186.100:80
136.228.211.141:8082
```



```
    {"type":4, "url": "https://api.proxyscrape.com/v2/?request=displayproxies&protocol=socks4",  "timeout": 5},
    {"type":4, "url": "https://api.proxyscrape.com/?request=displayproxies&proxytype=socks4",  "timeout": 5},
    {"type":4, "url": "https://api.proxyscrape.com/?request=displayproxies&proxytype=socks4&country=all",  "timeout": 5},
    {"type":4, "url": "https://api.openproxylist.xyz/socks4.txt",  "timeout": 5},
    {"type":4, "url": "https://proxyspace.pro/socks4.txt",  "timeout": 5},
    {"type":4, "url": "https://raw.githubusercontent.com/monosans/proxy-list/main/proxies/socks4.txt",  "timeout": 5},
    {"type":4, "url": "https://raw.githubusercontent.com/monosans/proxy-list/main/proxies_anonymous/socks4.txt",  "timeout": 5},
    {"type":4, "url": "https://raw.githubusercontent.com/jetkai/proxy-list/main/online-proxies/txt/proxies-socks4.txt",  "timeout": 5},
    {"type":4, "url": "https://raw.githubusercontent.com/ShiftyTR/Proxy-List/master/socks4.txt",  "timeout": 5},
    {"type":4, "url": "https://raw.githubusercontent.com/TheSpeedX/PROXY-List/master/socks4.txt",  "timeout": 5},
    {"type":4, "url": "https://raw.githubusercontent.com/roosterkid/openproxylist/main/SOCKS4_RAW.txt",  "timeout": 5},
    {"type":4, "url": "http://worm.rip/socks4.txt",  "timeout": 5},
    {"type":4, "url": "https://www.proxy-list.download/api/v1/get?type=socks4",  "timeout": 5},
    {"type":4, "url": "https://www.proxyscan.io/download?type=socks4",  "timeout": 5},
    {"type":4, "url": "https://www.my-proxy.com/free-socks-4-proxy.html",  "timeout": 5},
    {"type":4, "url": "http://www.socks24.org/feeds/posts/default",  "timeout": 5},
    {"type":4, "url": "https://www.freeproxychecker.com/result/socks4_proxies.txt",  "timeout": 5},
    {"type":4, "url": "https://raw.githubusercontent.com/HyperBeats/proxy-list/main/socks4.txt",  "timeout": 5},
    {"type":4, "url": "https://raw.githubusercontent.com/mmpx12/proxy-list/master/socks4.txt",  "timeout": 5},
    {"type":4, "url": "https://raw.githubusercontent.com/saschazesiger/Free-Proxies/master/proxies/socks4.txt",  "timeout": 5},
    {"type":4, "url": "https://raw.githubusercontent.com/B4RC0DE-TM/proxy-list/main/SOCKS4.txt",  "timeout": 5},

    {"type":5, "url": "https://raw.githubusercontent.com/B4RC0DE-TM/proxy-list/main/SOCKS5.txt",  "timeout": 5},
    {"type":5, "url": "https://raw.githubusercontent.com/saschazesiger/Free-Proxies/master/proxies/socks5.txt",  "timeout": 5},
    {"type":5, "url": "https://raw.githubusercontent.com/mmpx12/proxy-list/master/socks5.txt",  "timeout": 5},
    {"type":5, "url": "https://raw.githubusercontent.com/HyperBeats/proxy-list/main/socks5.txt",  "timeout": 5},
    {"type":5, "url": "https://api.openproxylist.xyz/socks5.txt",  "timeout": 5},
    {"type":5, "url": "https://api.proxyscrape.com/?request=displayproxies&proxytype=socks5",  "timeout": 5},
    {"type":5, "url": "https://api.proxyscrape.com/v2/?request=displayproxies&protocol=socks5",  "timeout": 5},
    {"type":5, "url": "https://api.proxyscrape.com/v2/?request=displayproxies&protocol=socks5", "timeout": 5},
    {"type":5, "url": "https://api.proxyscrape.com/v2/?request=getproxies&protocol=socks5&timeout=10000&country=all&simplified=true",  "timeout": 5},
    {"type":5, "url": "https://proxyspace.pro/socks5.txt",  "timeout": 5},
    {"type":5, "url": "https://raw.githubusercontent.com/manuGMG/proxy-365/main/SOCKS5.txt",  "timeout": 5},
    {"type":5, "url": "https://raw.githubusercontent.com/monosans/proxy-list/main/proxies/socks5.txt",  "timeout": 5},
    {"type":5, "url": "https://raw.githubusercontent.com/monosans/proxy-list/main/proxies_anonymous/socks5.txt",  "timeout": 5},
    {"type":5, "url": "https://raw.githubusercontent.com/ShiftyTR/Proxy-List/master/socks5.txt",  "timeout": 5},
    {"type":5, "url": "https://raw.githubusercontent.com/jetkai/proxy-list/main/online-proxies/txt/proxies-socks5.txt",  "timeout": 5},
    {"type":5, "url": "https://raw.githubusercontent.com/roosterkid/openproxylist/main/SOCKS5_RAW.txt",  "timeout": 5},
    {"type":5, "url": "https://raw.githubusercontent.com/TheSpeedX/PROXY-List/master/socks5.txt",  "timeout": 5},
```

3. Tư Duy Phòng Thủ

Nguyên tắc chung:

Phải **PHÂN BIỆT** được đâu là **NGƯỜI**, đâu là **BOT**!!!

3. Tư Duy Phòng Thủ

Rate Limit

Signatures

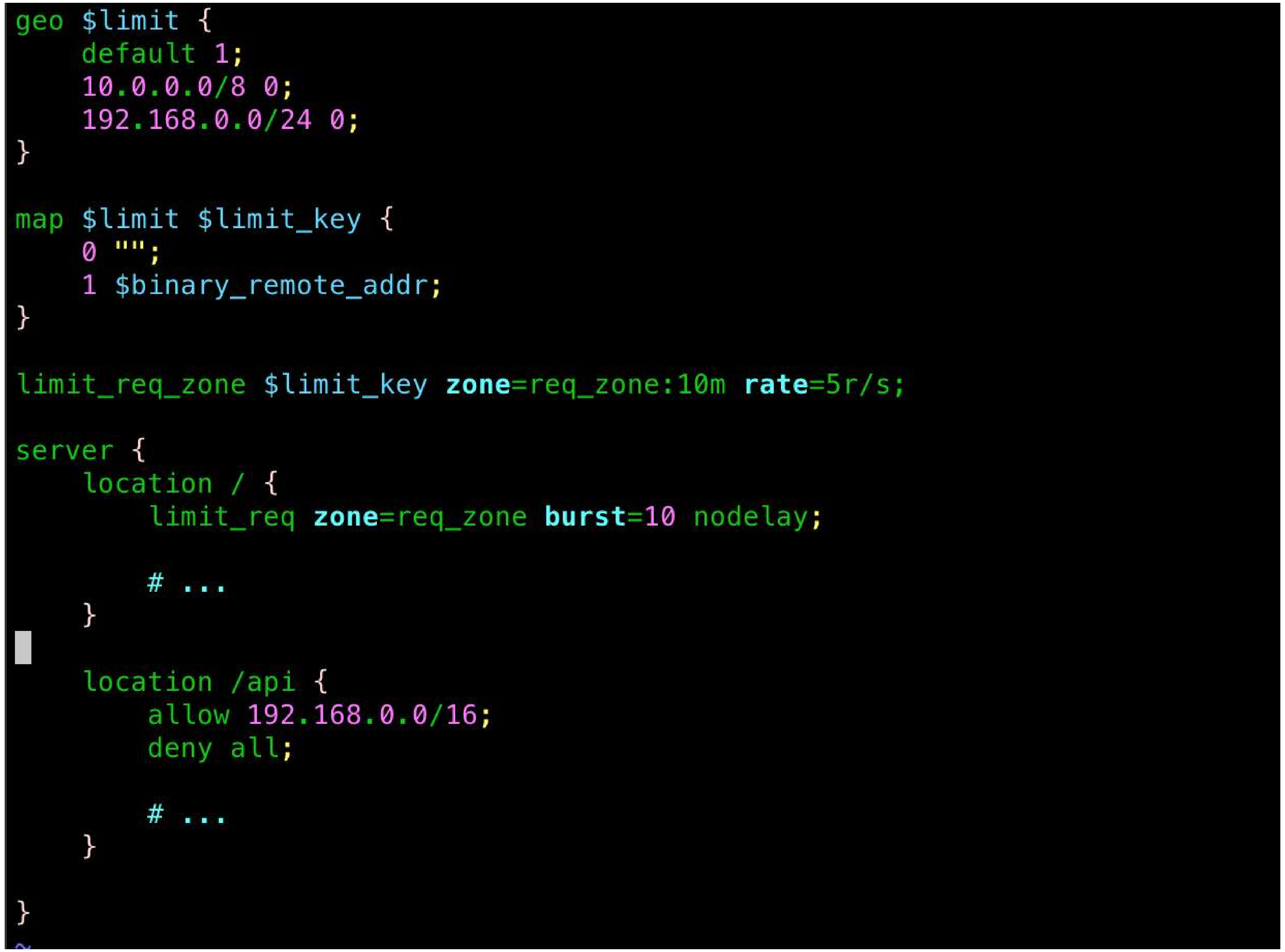
Challenges

RATE LIMIT

- Tách location để đặt giới hạn riêng: static content, = /, /, api,...
- Giới hạn truy cập với các location đặc biệt
- Giới hạn theo khu vực: ví dụ trong nước/ quốc tế hoặc request từ proxy/ không qua proxy

Tham khảo: https://quantrilinux.vn/chong-ddos-bypass-cloudflare-bang-csf-p2.html

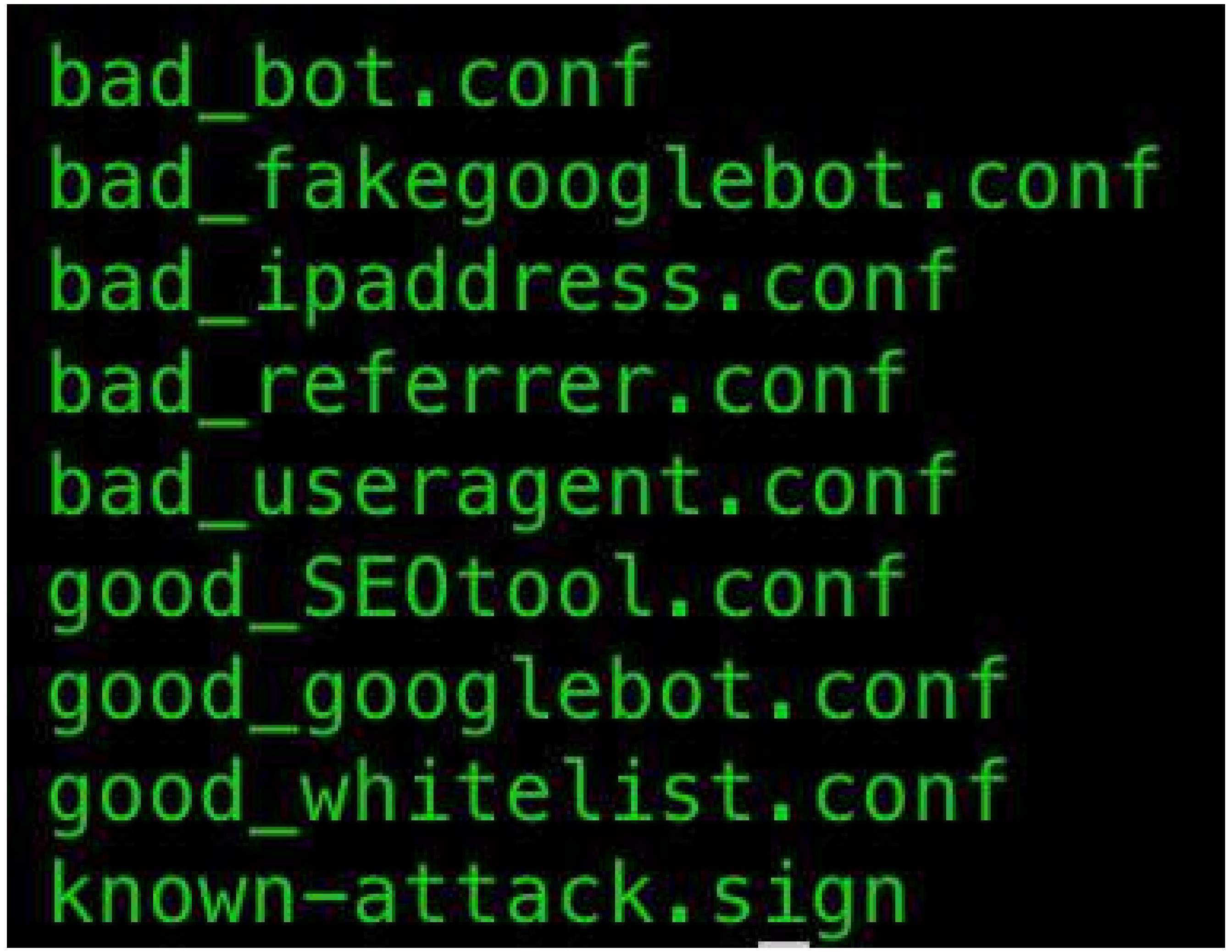
RATE LIMIT



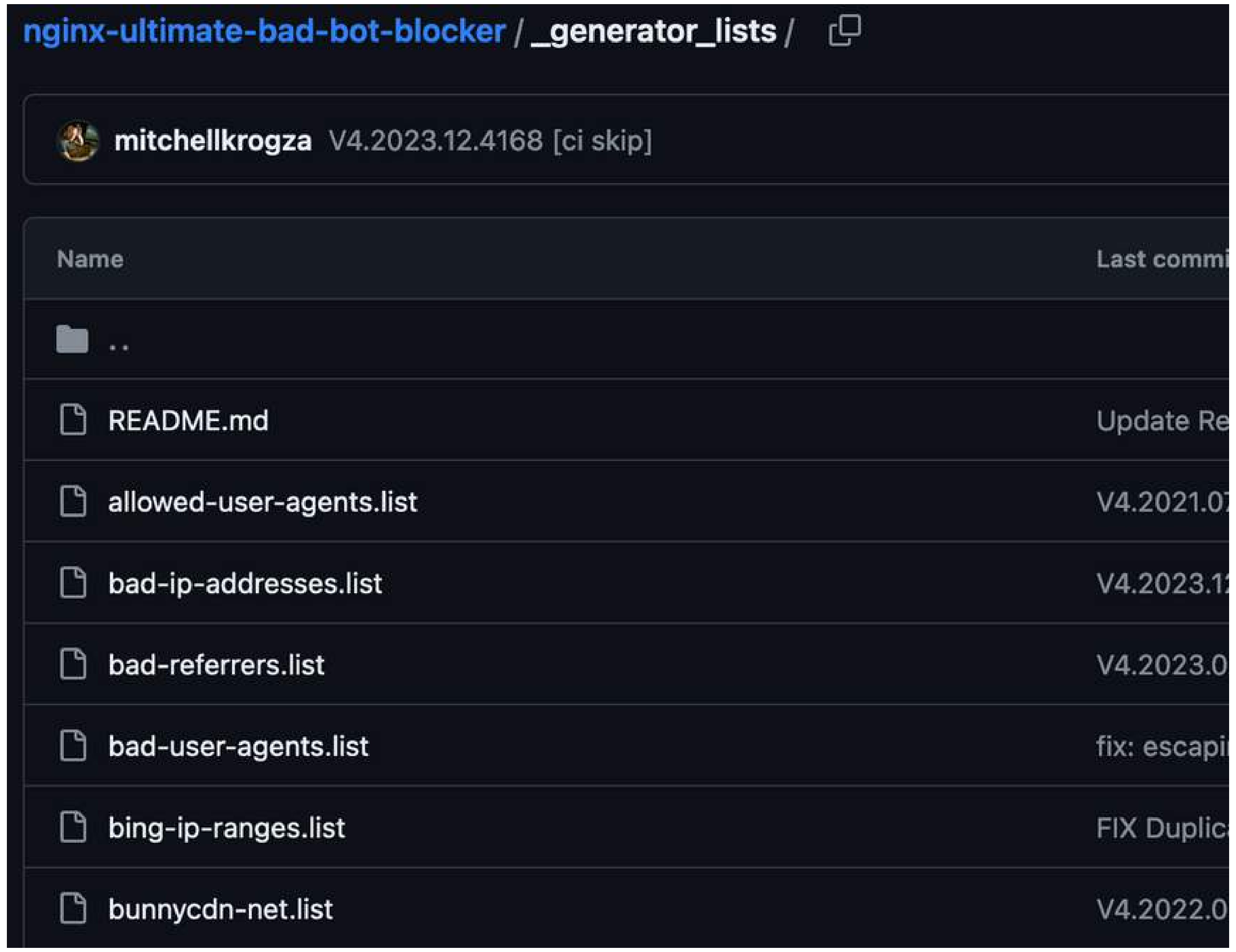
```
geo $limit {
    default 1;
    10.0.0.0/8 0;
    192.168.0.0/24 0;
}

map $limit $limit_key {
    0 "";
    1 $binary_remote_addr;
}

limit_req_zone $limit_key zone=req_zone:10m rate=5r/s;

server {
    location / {
        limit_req zone=req_zone burst=10 nodelay;

        # ...
    }

    location /api {
        allow 192.168.0.0/16;
        deny all;

        # ...
    }

}
```

SIGNATURES

- Thu thập các dấu hiệu từ cộng đồng, internet,...
- link: https://github.com/mitchellkrogza/nginx-ultimate-bad-bot-blocker/tree/master/_generator_lists



```
bad_bot.conf
bad_fakegooglebot.conf
bad_ipaddress.conf
bad_referrer.conf
bad_useragent.conf
good_SEOtool.conf
good_googlebot.conf
good_whitelist.conf
known-attack.sign
```

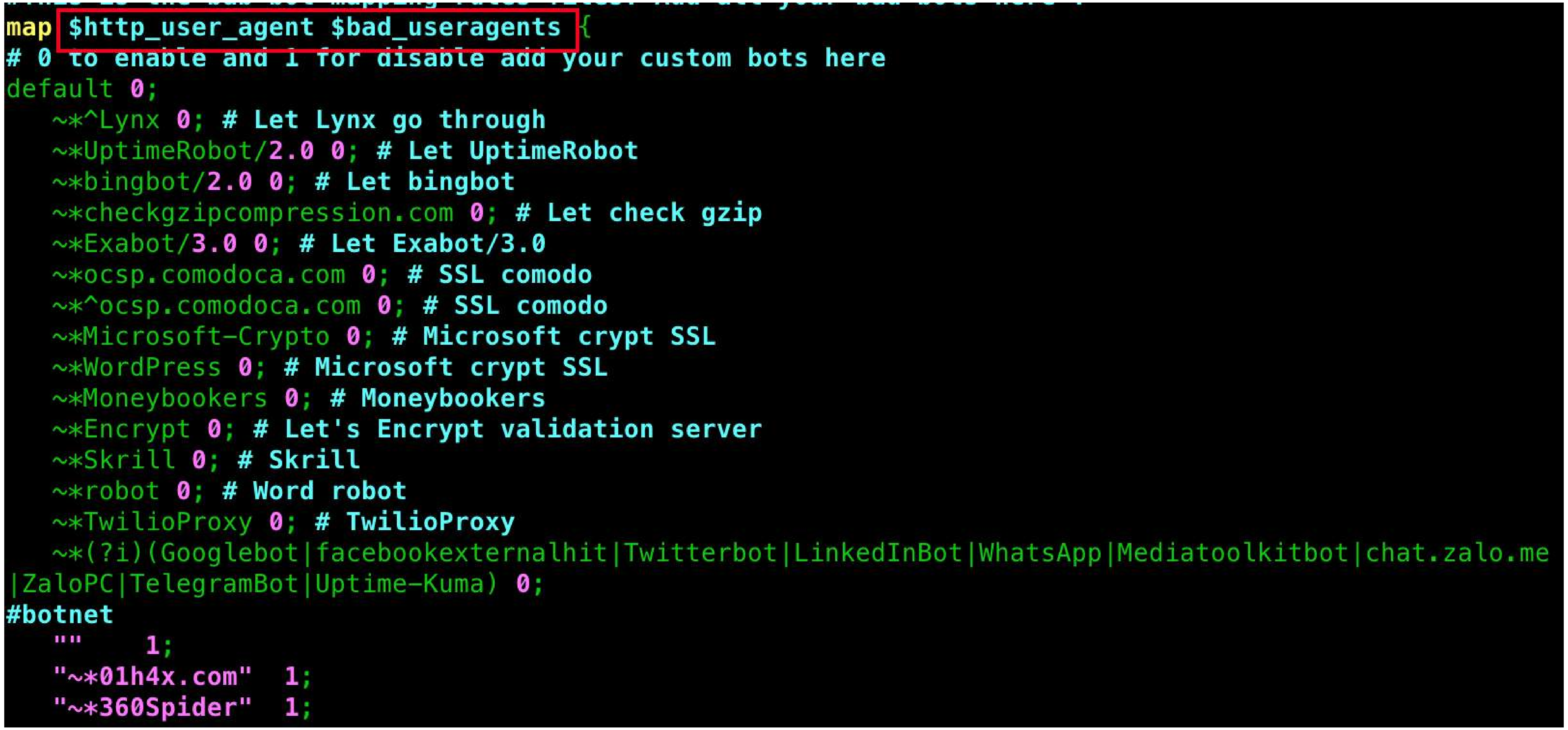


nginx-ultimate-bad-bot-blocker / _generator_lists /

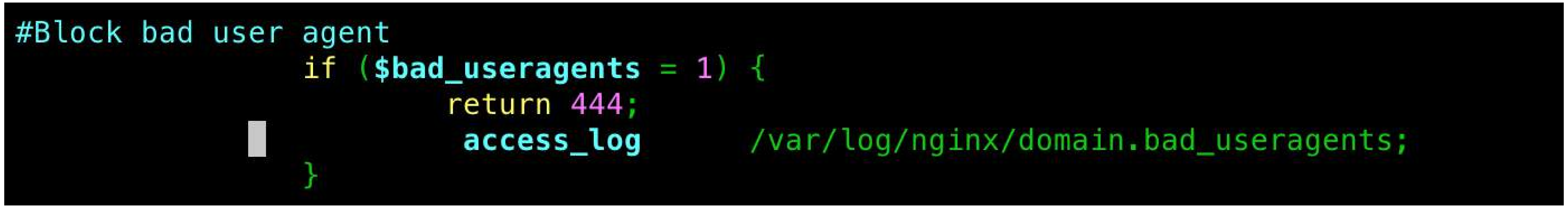
mitchellkrogza V4.2023.12.4168 [ci skip]

Name	Last commi
..	
README.md	Update Re
allowed-user-agents.list	V4.2021.0
bad-ip-addresses.list	V4.2023.1
bad-referrers.list	V4.2023.0
bad-user-agents.list	fix: escapi
bing-ip-ranges.list	FIX Duplic
bunnycdn-net.list	V4.2022.0

SIGNATURES

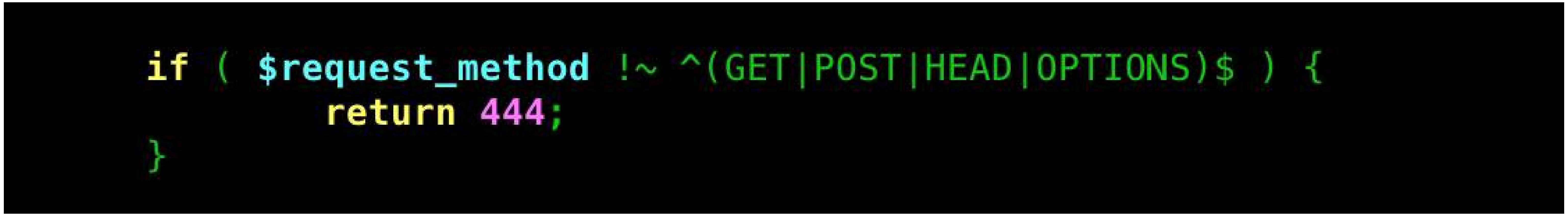


```
# This is the bad bot mapping rules filter. Add all your bad bots here !
map $http_user_agent $bad_useragents {
# 0 to enable and 1 for disable add your custom bots here
default 0;
   ~*^Lynx 0; # Let Lynx go through
   ~*UptimeRobot/2.0 0; # Let UptimeRobot
   ~*bingbot/2.0 0; # Let bingbot
   ~*checkgzipcompression.com 0; # Let check gzip
   ~*Exabot/3.0 0; # Let Exabot/3.0
   ~*ocsp.comodoca.com 0; # SSL comodo
   ~*^ocsp.comodoca.com 0; # SSL comodo
   ~*Microsoft-Crypto 0; # Microsoft crypt SSL
   ~*WordPress 0; # Microsoft crypt SSL
   ~*Moneybookers 0; # Moneybookers
   ~*Encrypt 0; # Let's Encrypt validation server
   ~*Skrill 0; # Skrill
   ~*robot 0; # Word robot
   ~*TwilioProxy 0; # TwilioProxy
   ~*(?i)(Googlebot|facebookexternalhit|Twitterbot|LinkedInBot|WhatsApp|Mediatoolkitbot|chat.zalo.me
|ZaloPC|TelegramBot|Uptime-Kuma) 0;
#botnet
   ""     1;
   "~*01h4x.com"  1;
   "~*360Spider"  1;
```



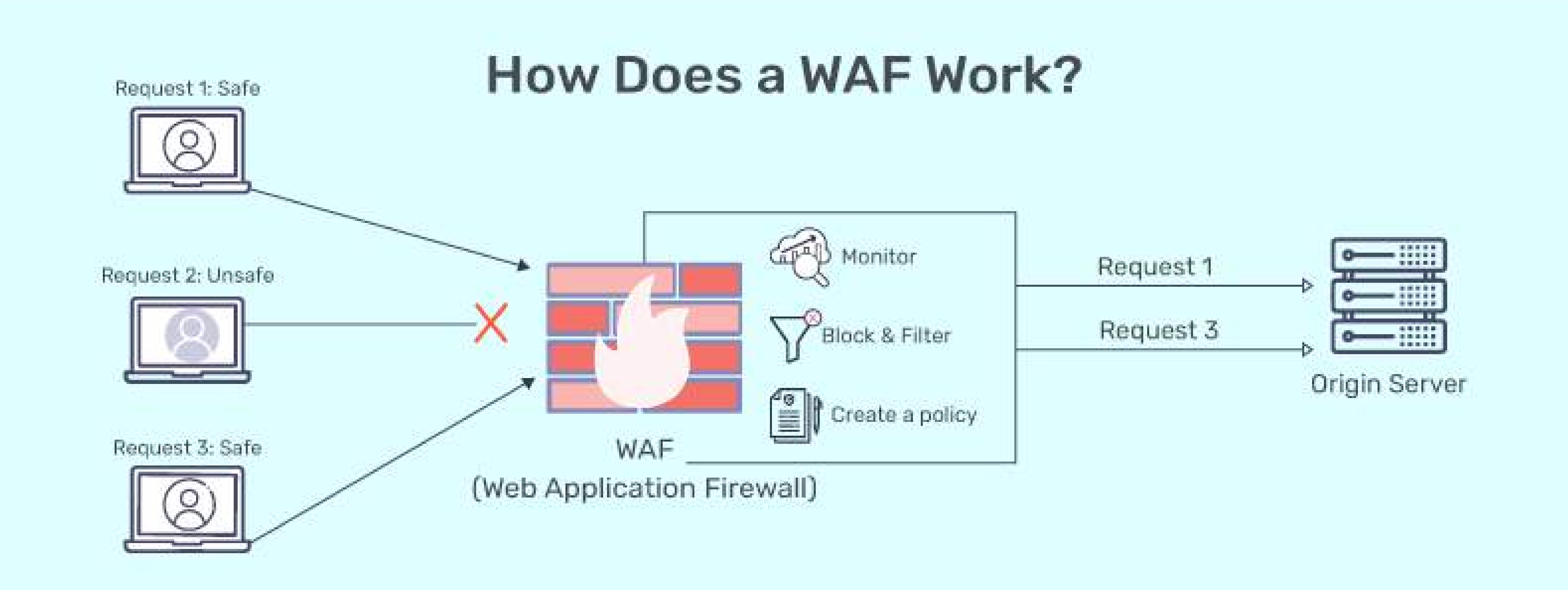
```
#Block bad user agent
                  if ($bad_useragents = 1) {
                           return 444;
                            access_log      /var/log/nginx/domain.bad_useragents;
                  }
```

SIGNATURES

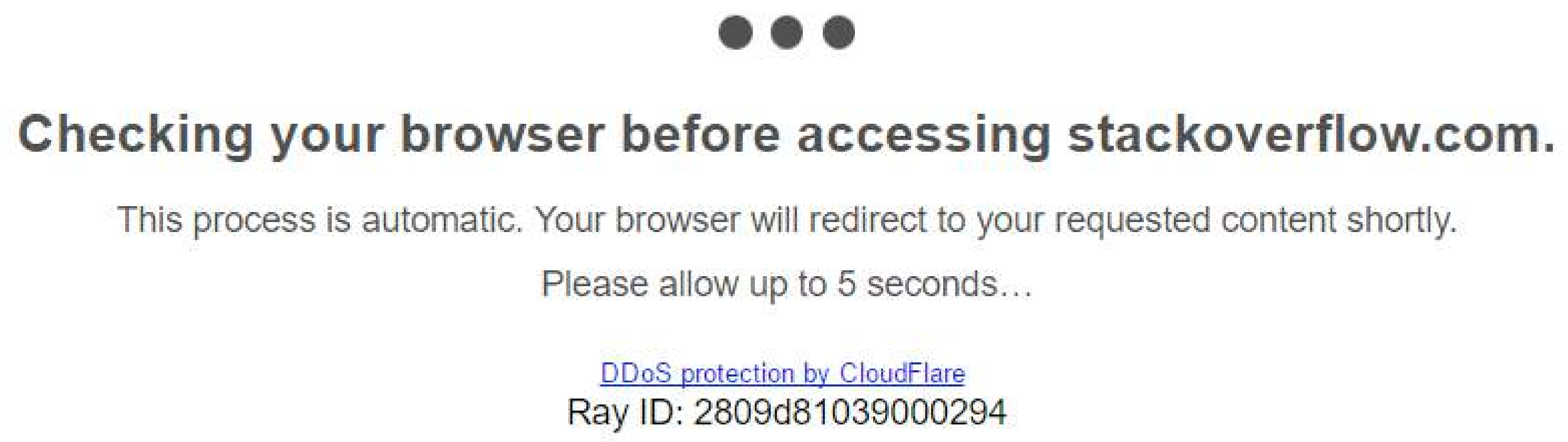


```
if ( $request_method !~ ^(GET|POST|HEAD|OPTIONS)$ ) {
        return 444;
}
```

SIGNATURES (WAF): ModSecurity



Challenges (Browser Integrity Check): cookies, JS challenge, ...

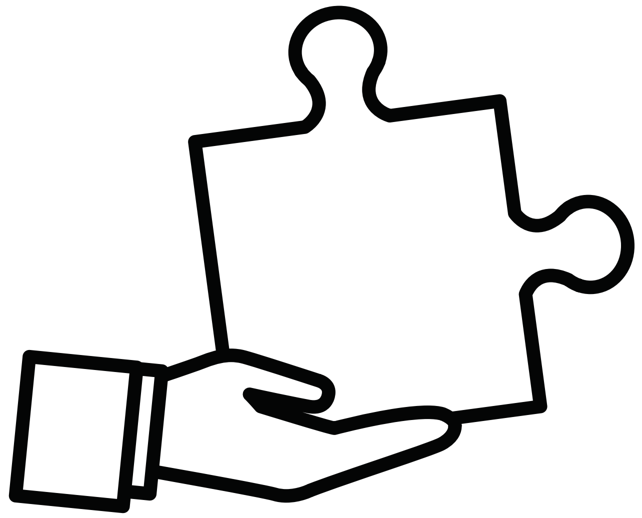


Checking your browser before accessing stackoverflow.com.

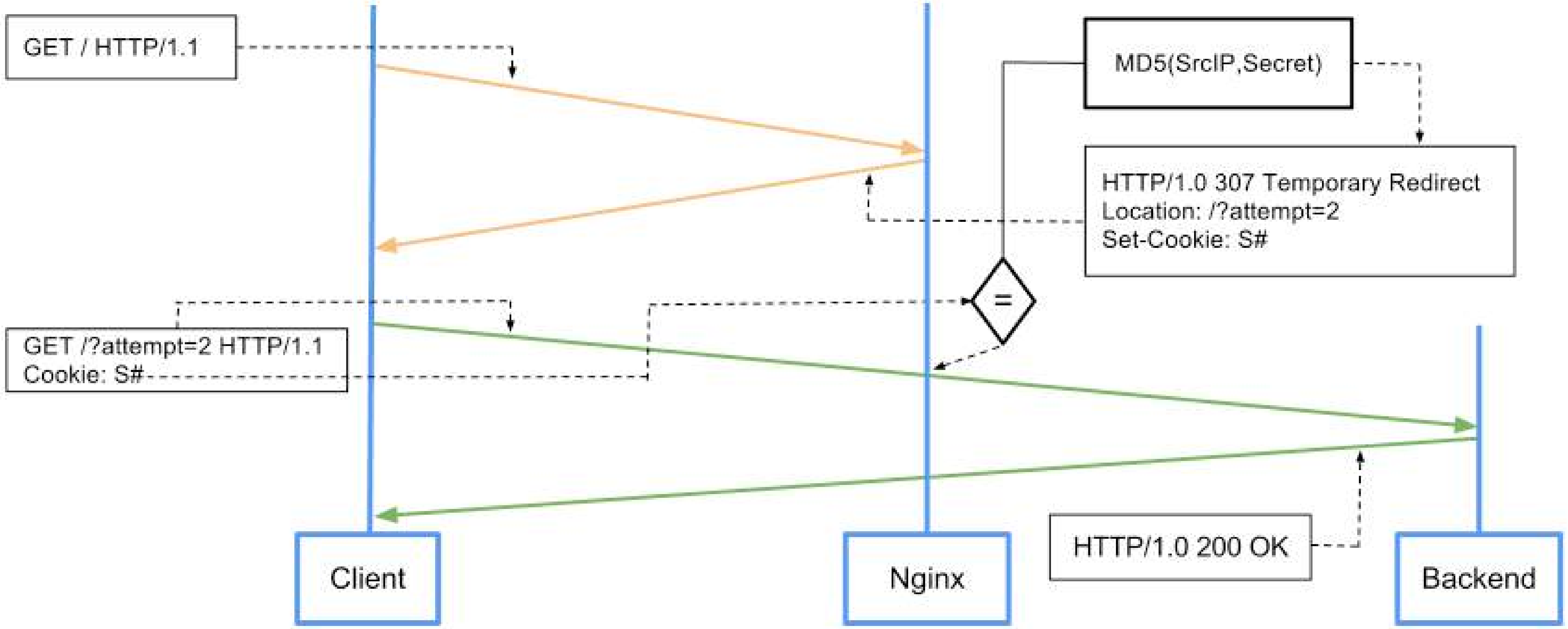
This process is automatic. Your browser will redirect to your requested content shortly.

Please allow up to 5 seconds…

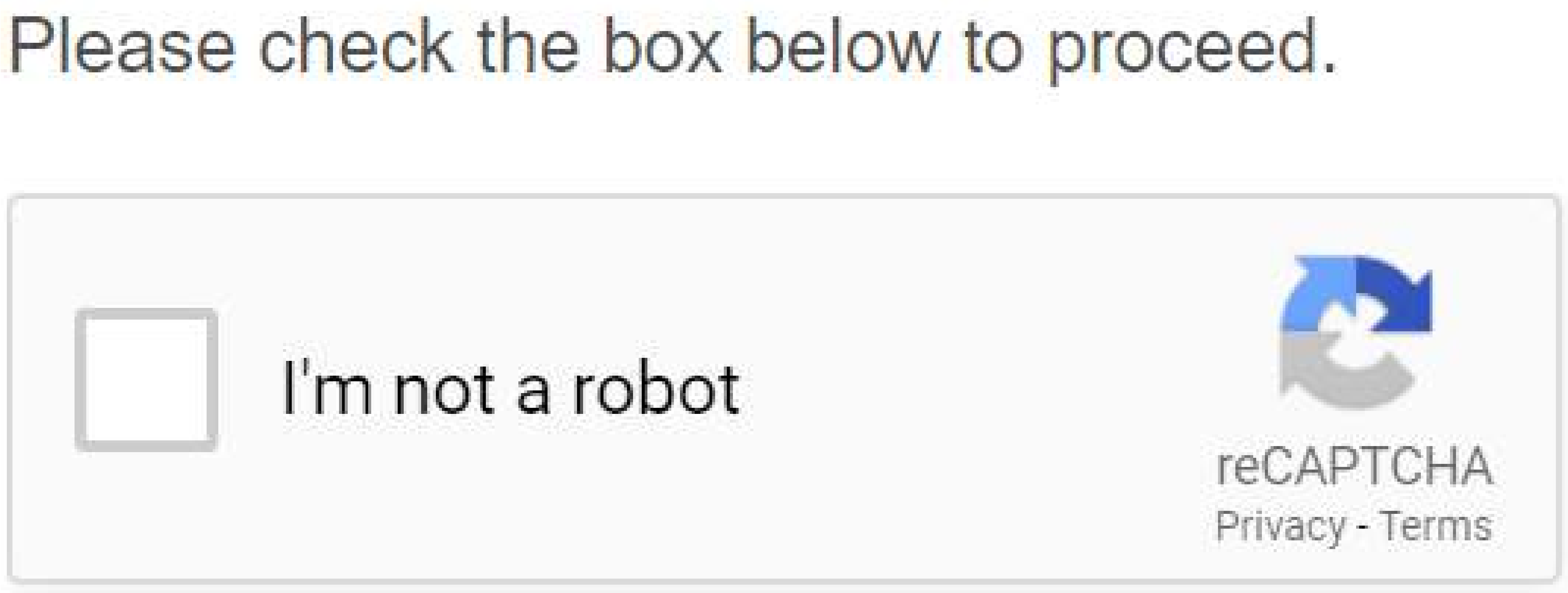
DDoS protection by CloudFlare
Ray ID: 2809d81039000294



Challenges (Browser Integrity Check): testcookie



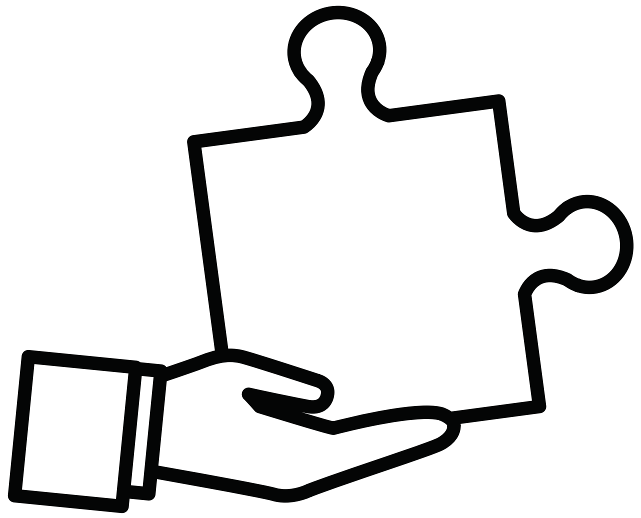
Challenges (User Check): reCaptcha - Invisible reCaptcha



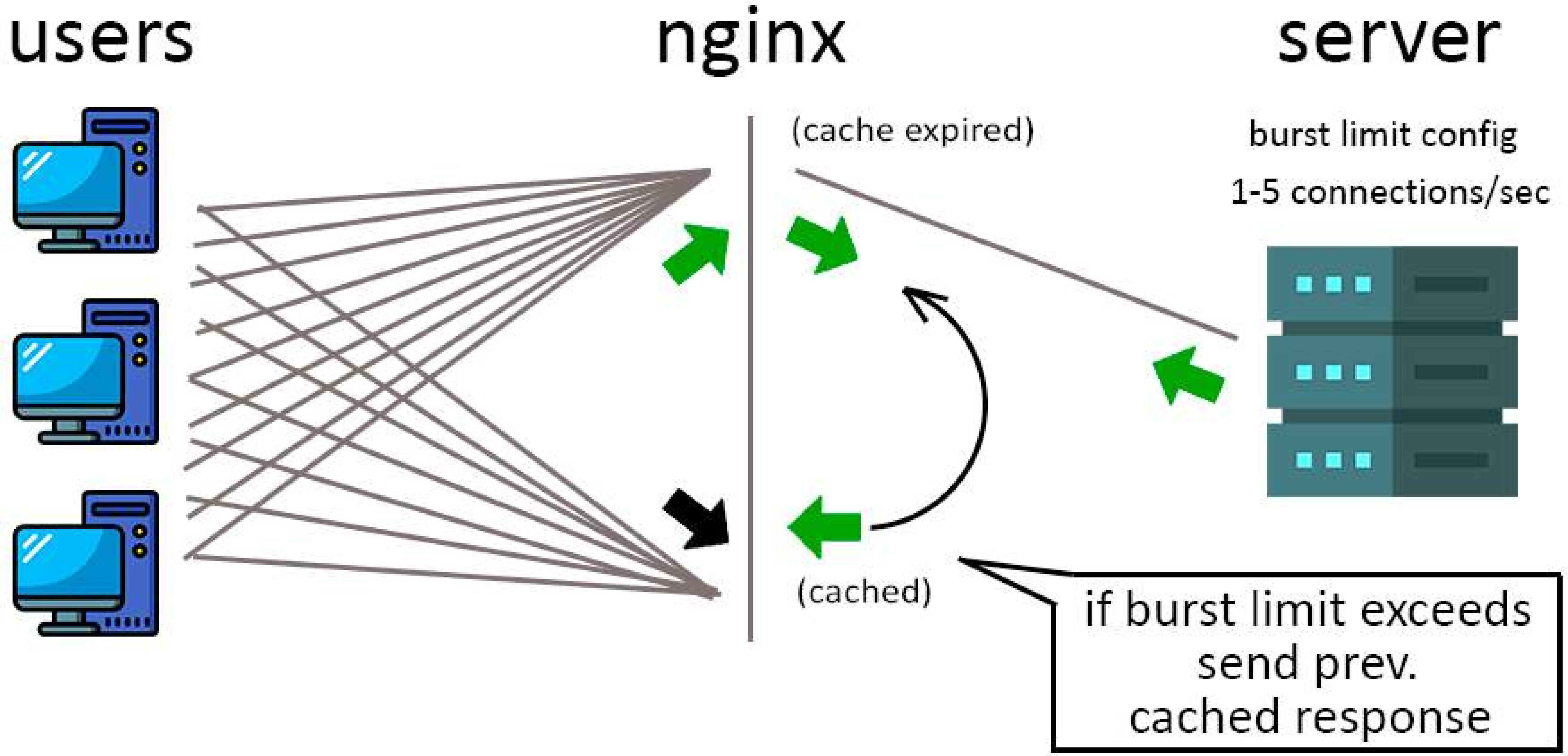
Please check the box below to proceed.

□ I'm not a robot

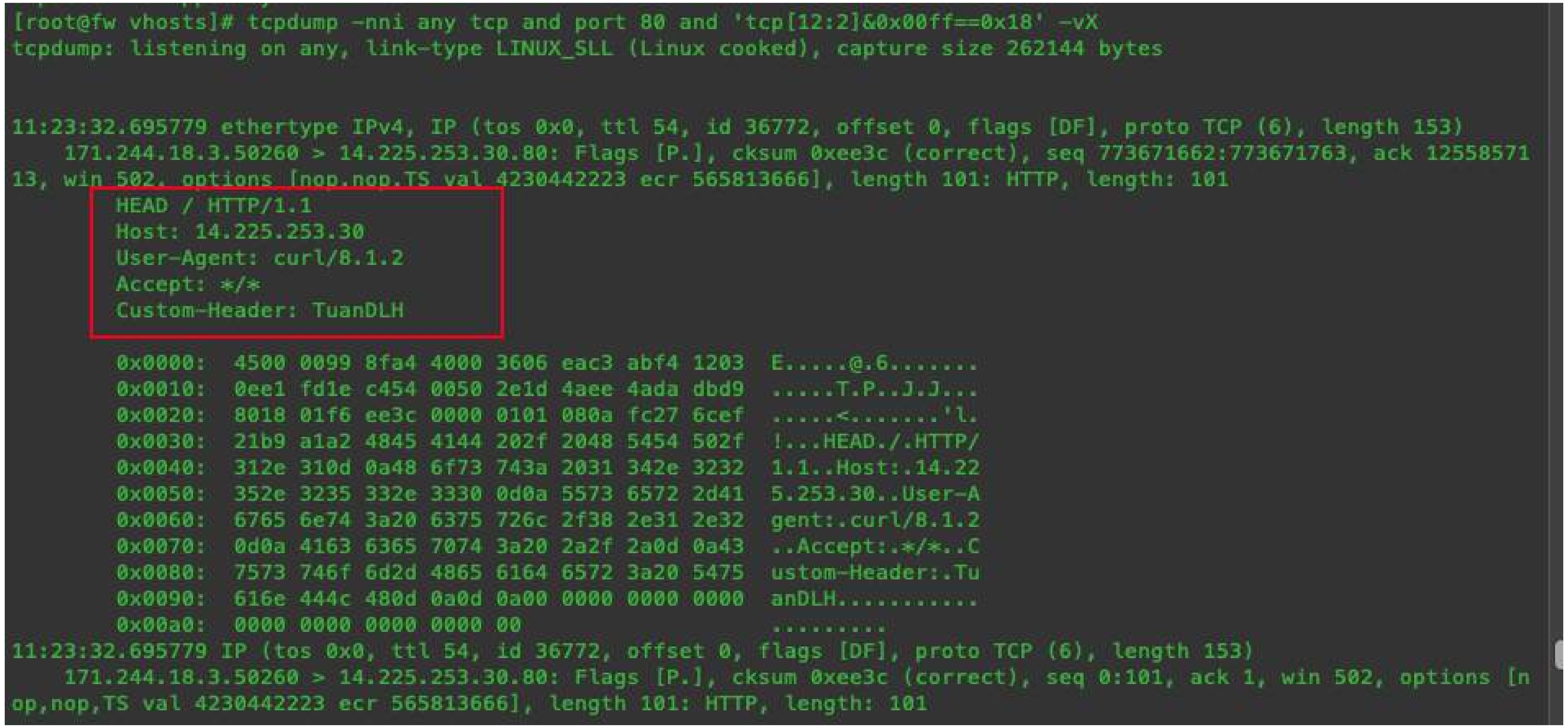
reCAPTCHA
Privacy - Terms



Kỹ thuật khác: Sử dụng cache

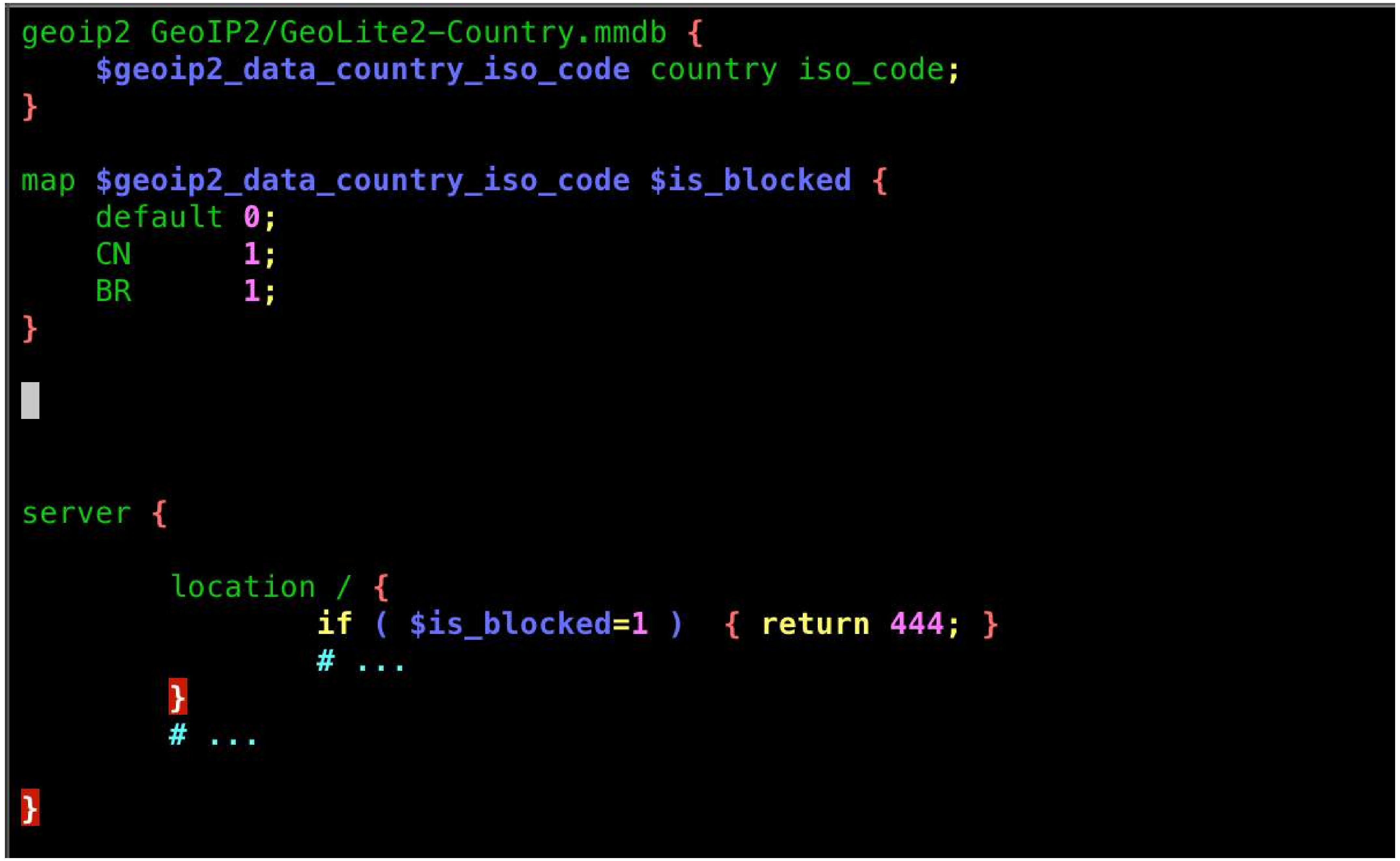


Kỹ thuật khác: Parse và Phân tích HTTP Header



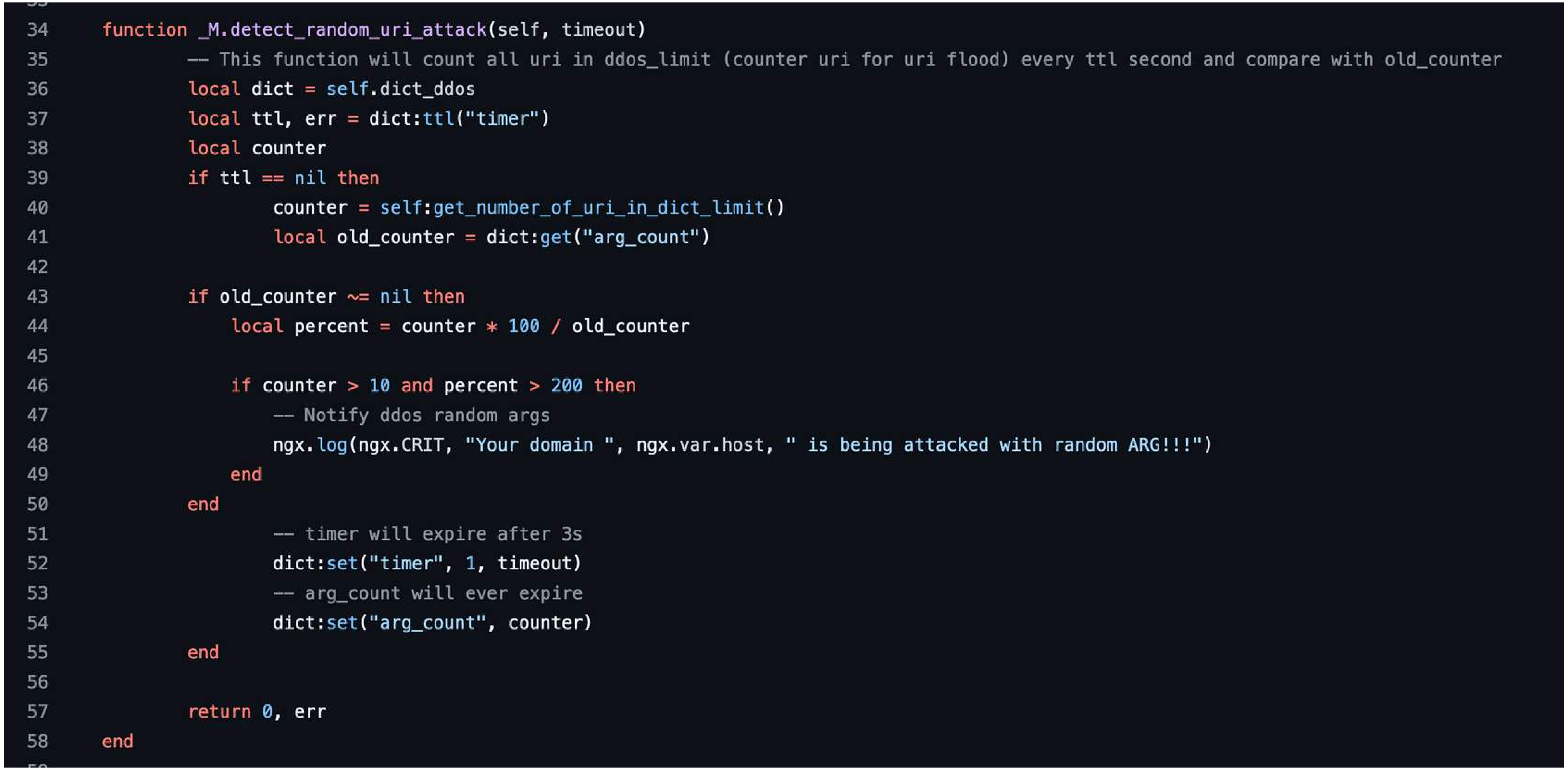
```
[root@fw vhosts]# tcpdump -nni any tcp and port 80 and 'tcp[12:2]&0x00ff==0x18' -vX
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes


11:23:32.695779 ethertype IPv4, IP (tos 0x0, ttl 54, id 36772, offset 0, flags [DF], proto TCP (6), length 153)
    171.244.18.3.50260 > 14.225.253.30.80: Flags [P.], cksum 0xee3c (correct), seq 773671662:773671763, ack 12558571
13, win 502, options [nop,nop,TS val 4230442223 ecr 565813666], length 101: HTTP, length: 101
        HEAD / HTTP/1.1
        Host: 14.225.253.30
        User-Agent: curl/8.1.2
        Accept: */*
        Custom-Header: TuanDLH

        0x0000:  4500 0099 8fa4 4000 3606 eac3 abf4 1203  E.....@.6.......
        0x0010:  0ee1 fd1e c454 0050 2e1d 4aee 4ada dbd9  ......T.P..J.J...
        0x0020:  8018 01f6 ee3c 0000 0101 080a fc27 6cef  .....<.......'l.
        0x0030:  21b9 a1a2 4845 4144 202f 2048 5454 502f  !...HEAD./.HTTP/
        0x0040:  312e 310d 0a48 6f73 743a 2031 342e 3232  1.1..Host:.14.22
        0x0050:  352e 3235 332e 3330 0d0a 5573 6572 2d41  5.253.30..User-A
        0x0060:  6765 6e74 3a20 6375 726c 2f38 2e31 2e32  gent:.curl/8.1.2
        0x0070:  0d0a 4163 6365 7074 3a20 2a2f 2a0d 0a43  ..Accept:.*/*..C
        0x0080:  7573 746f 6d2d 4865 6164 6572 3a20 5475  ustom-Header:.Tu
        0x0090:  616e 444c 480d 0a0d 0a00 0000 0000 0000  anDLH...........
        0x00a0:  0000 0000 0000 0000 00                   .........
11:23:32.695779 IP (tos 0x0, ttl 54, id 36772, offset 0, flags [DF], proto TCP (6), length 153)
    171.244.18.3.50260 > 14.225.253.30.80: Flags [P.], cksum 0xee3c (correct), seq 0:101, ack 1, win 502, options [n
op,nop,TS val 4230442223 ecr 565813666], length 101: HTTP, length: 101
```

Kỹ thuật khác: Chống tấn công theo GEOIP



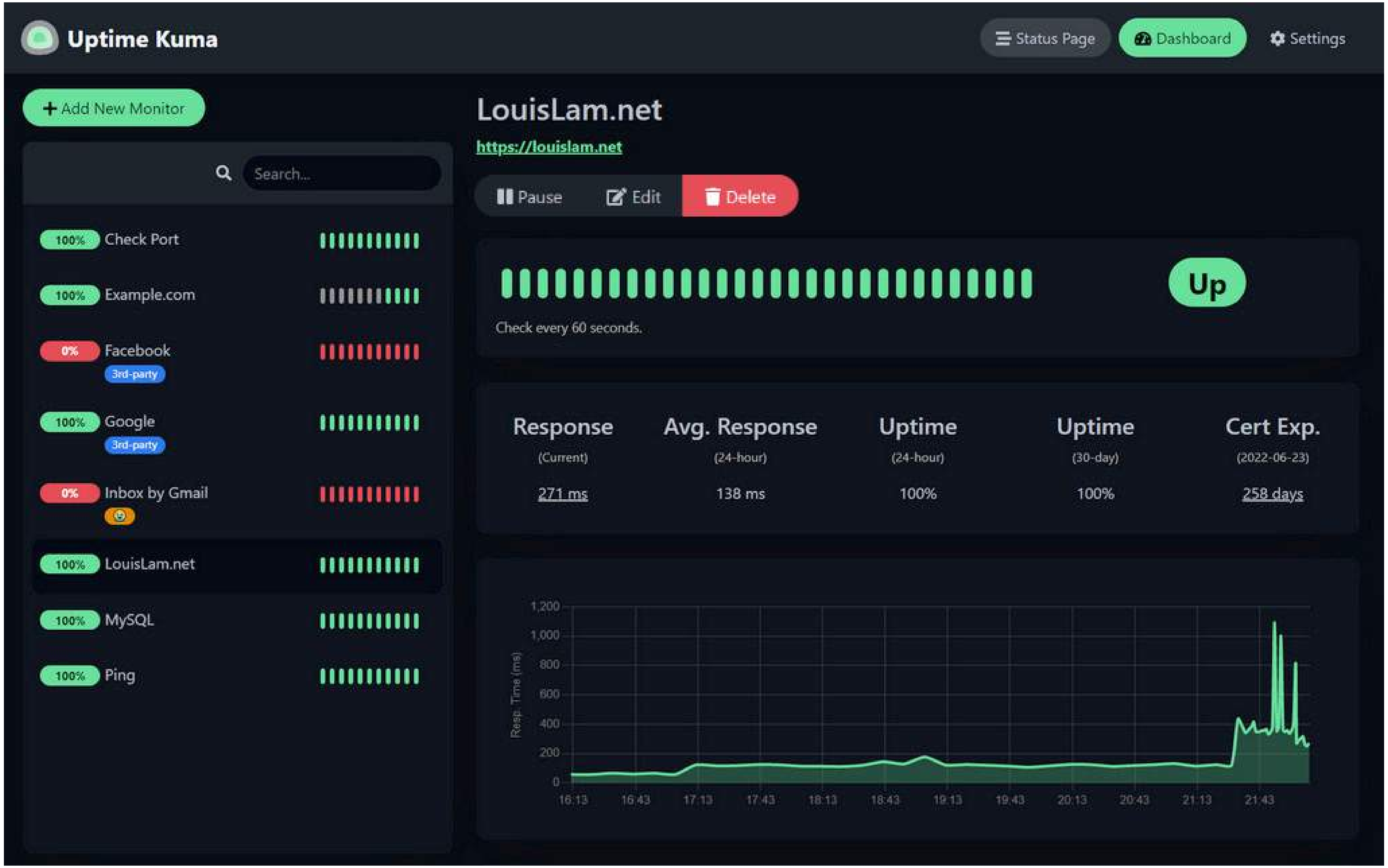
```
geoip2 GeoIP2/GeoLite2-Country.mmdb {
    $geoip2_data_country_iso_code country iso_code;
}

map $geoip2_data_country_iso_code $is_blocked {
    default 0;
    CN      1;
    BR      1;
}




server {

        location / {
                if ( $is_blocked=1 )  { return 444; }
                # ...
        }
        # ...

}
```

Kỹ thuật khác: Monitor log - chống tấn công theo url path



```lua
function _M.detect_random_uri_attack(self, timeout)
        -- This function will count all uri in ddos_limit (counter uri for uri flood) every ttl second and compare with old_counter
        local dict = self.dict_ddos
        local ttl, err = dict:ttl("timer")
        local counter
        if ttl == nil then
                counter = self:get_number_of_uri_in_dict_limit()
                local old_counter = dict:get("arg_count")

        if old_counter ~= nil then
            local percent = counter * 100 / old_counter

            if counter > 10 and percent > 200 then
                -- Notify ddos random args
                ngx.log(ngx.CRIT, "Your domain ", ngx.var.host, " is being attacked with random ARG!!!")
            end
        end
                -- timer will expire after 3s
                dict:set("timer", 1, timeout)
                -- arg_count will ever expire
                dict:set("arg_count", counter)
        end

        return 0, err
end
```

Kỹ thuật khác: Monitor and Alert



100%	Check Port
100%	Example.com
0%	Facebook 3rd-party
100%	Google 3rd-party
0%	Inbox by Gmail
100%	LouisLam.net
100%	MySQL
100%	Ping

LouisLam.net

https://louislam.net

Check every 60 seconds.

Response	Avg. Response	Uptime	Uptime	Cert Exp.
(Current)	(24-hour)	(24-hour)	(30-day)	(2022-06-23)
271 ms	138 ms	100%	100%	258 days

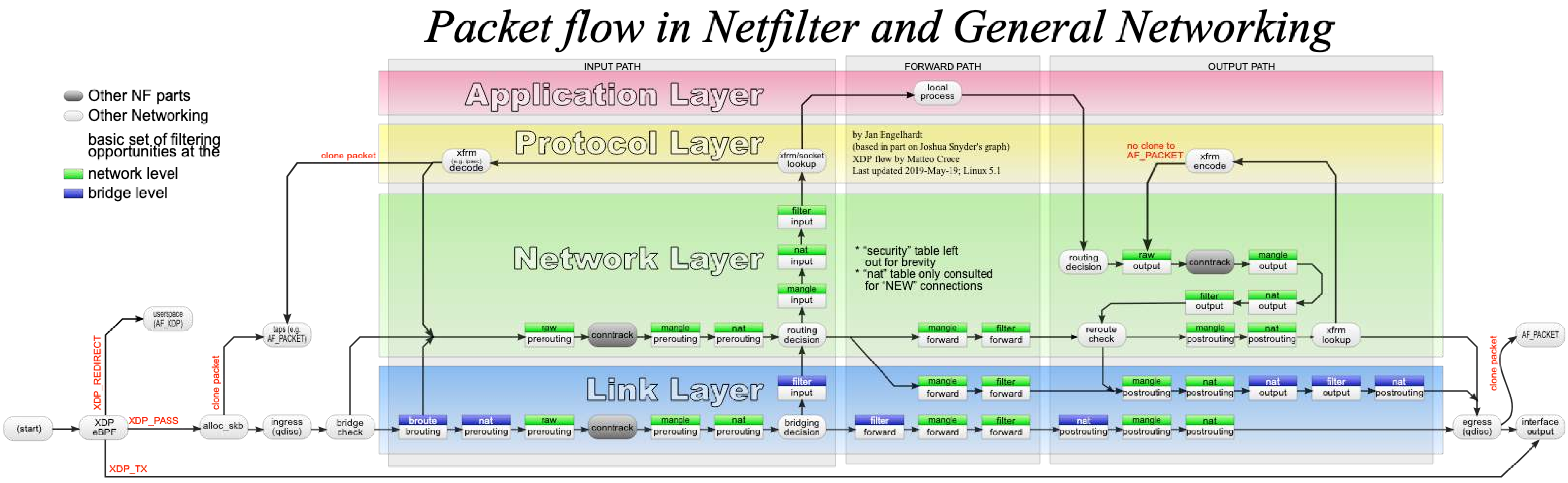
Kỹ thuật chốt hạ:

Chặn dấu hiệu tấn công DDOS **càng sớm càng tốt**!!!

Đẩy traffic xuống iptables

(video demo here)

Offload signature to networkcard using XDP/eBPF

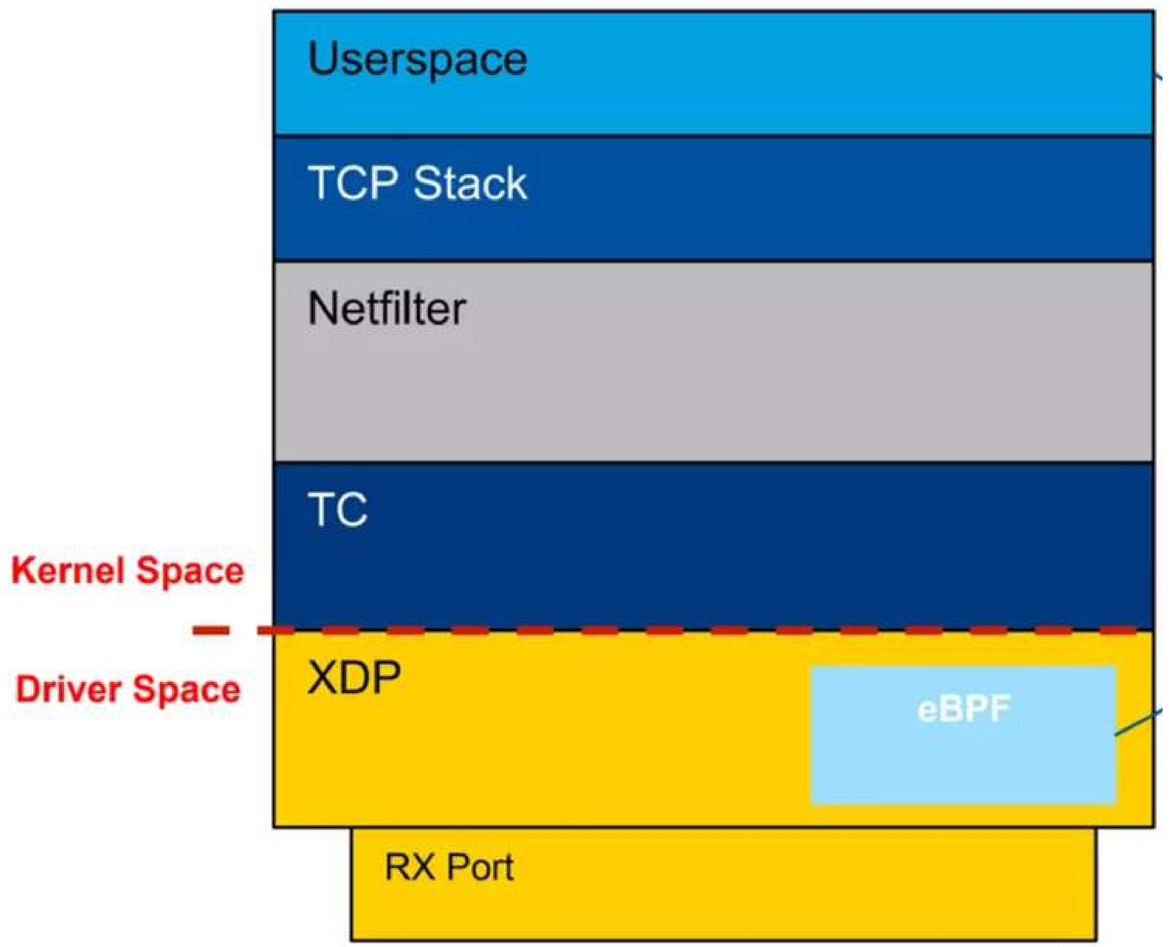


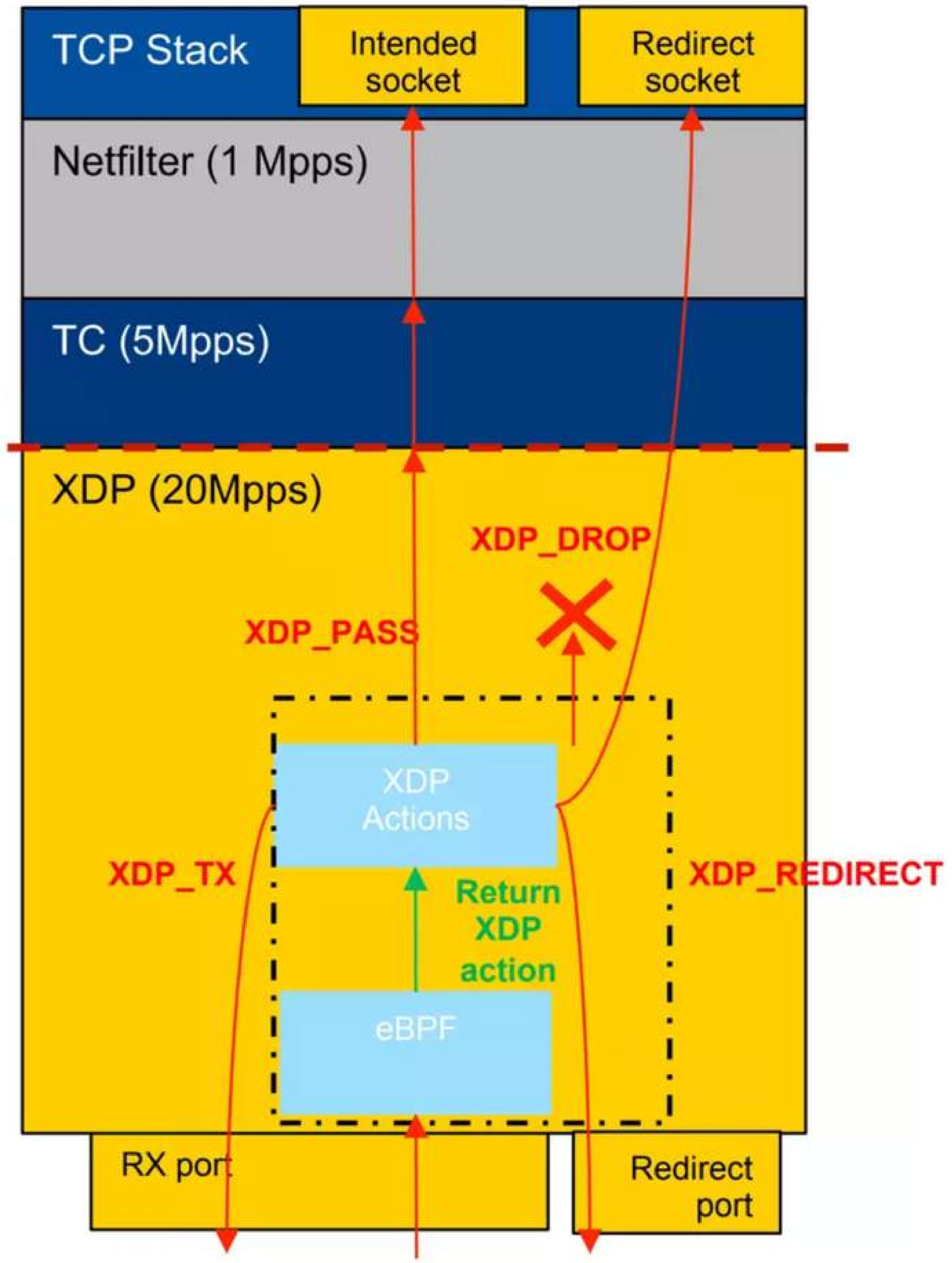
Packet flow in Netfilter and General Networking

by Jan Engelhardt
(based in part on Joshua Snyder's graph)
XDP flow by Matteo Croce
Last updated 2019-May-19; Linux 5.1

- "security" table left out for brevity
- "nat" table only consulted for "NEW" connections

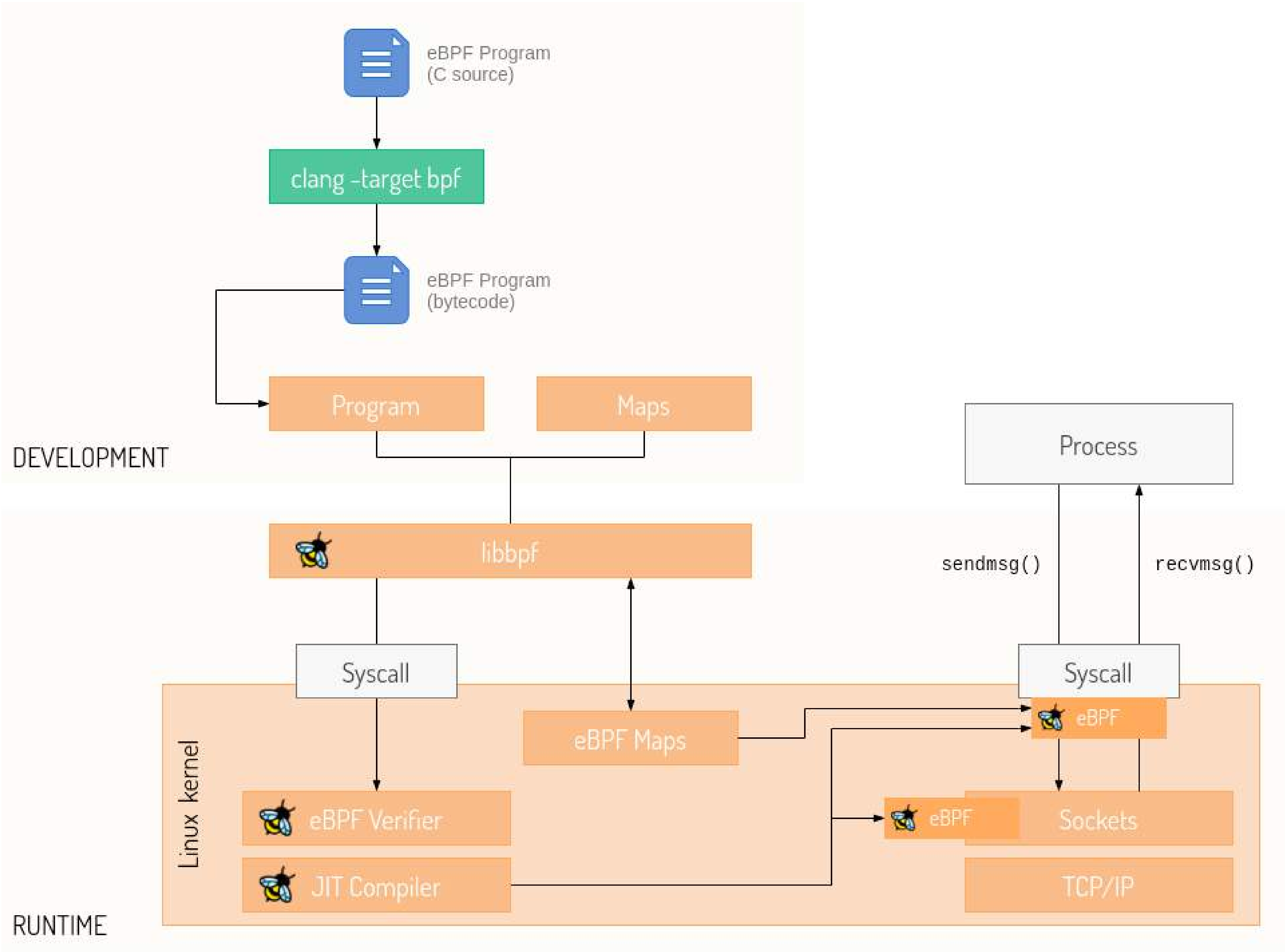
Offload signature to networkcard using XDP/eBPF



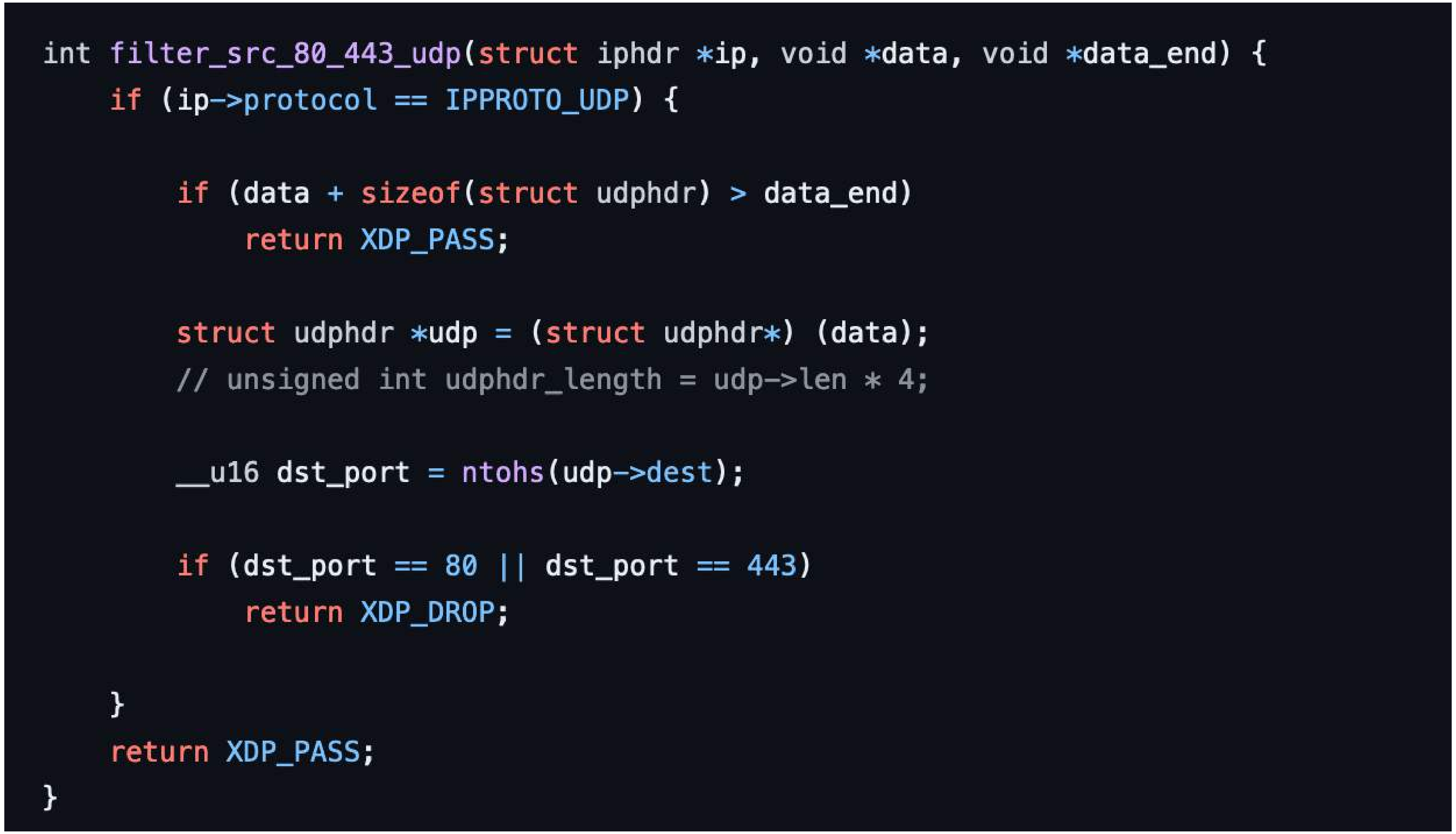


Tham khảo: https://www.slideshare.net/Netronome/ebpfxdp-sigcomm-2018

Offload signature to networkcard using XDP/eBPF



Offload signature to networkcard using XDP/eBPF



```c
int filter_src_80_443_udp(struct iphdr *ip, void *data, void *data_end) {
    if (ip->protocol == IPPROTO_UDP) {

        if (data + sizeof(struct udphdr) > data_end)
            return XDP_PASS;

        struct udphdr *udp = (struct udphdr*) (data);
        // unsigned int udphdr_length = udp->len * 4;

        __u16 dst_port = ntohs(udp->dest);

        if (dst_port == 80 || dst_port == 443)
            return XDP_DROP;

    }
    return XDP_PASS;
}
```

Q&A