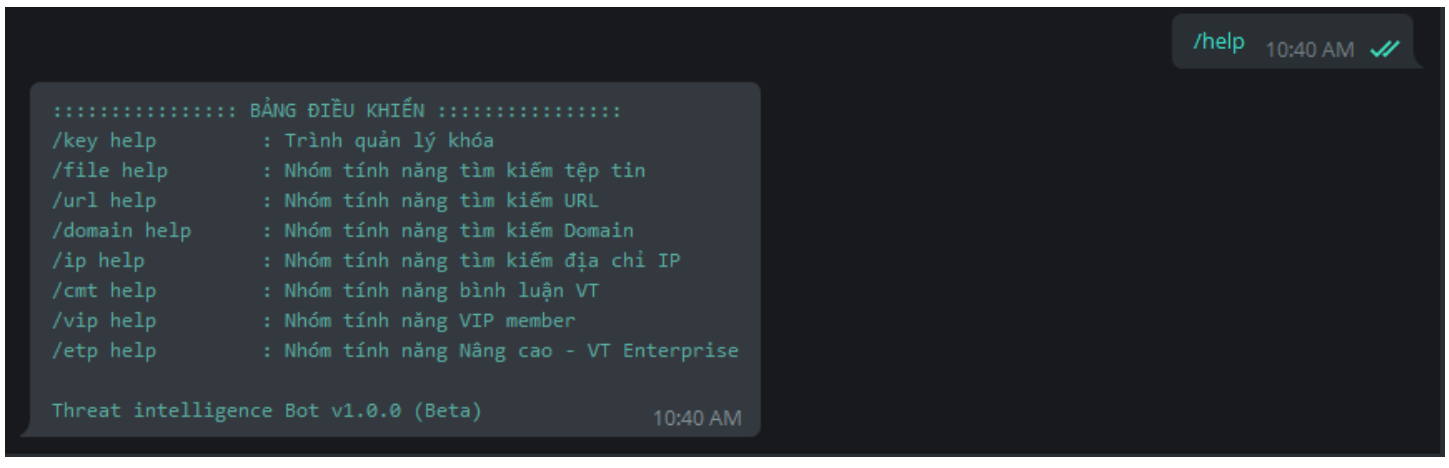
# Docs - Threat Intelligence Bot



## 1. Bảng điều khiển

Bảng điều khiển của **Threat Intelligence Bot** là một menu giới thiệu tất cả tính năng hiện sẵn có của Bot. Để show bảng điều khiển chúng ta gửi lệnh:

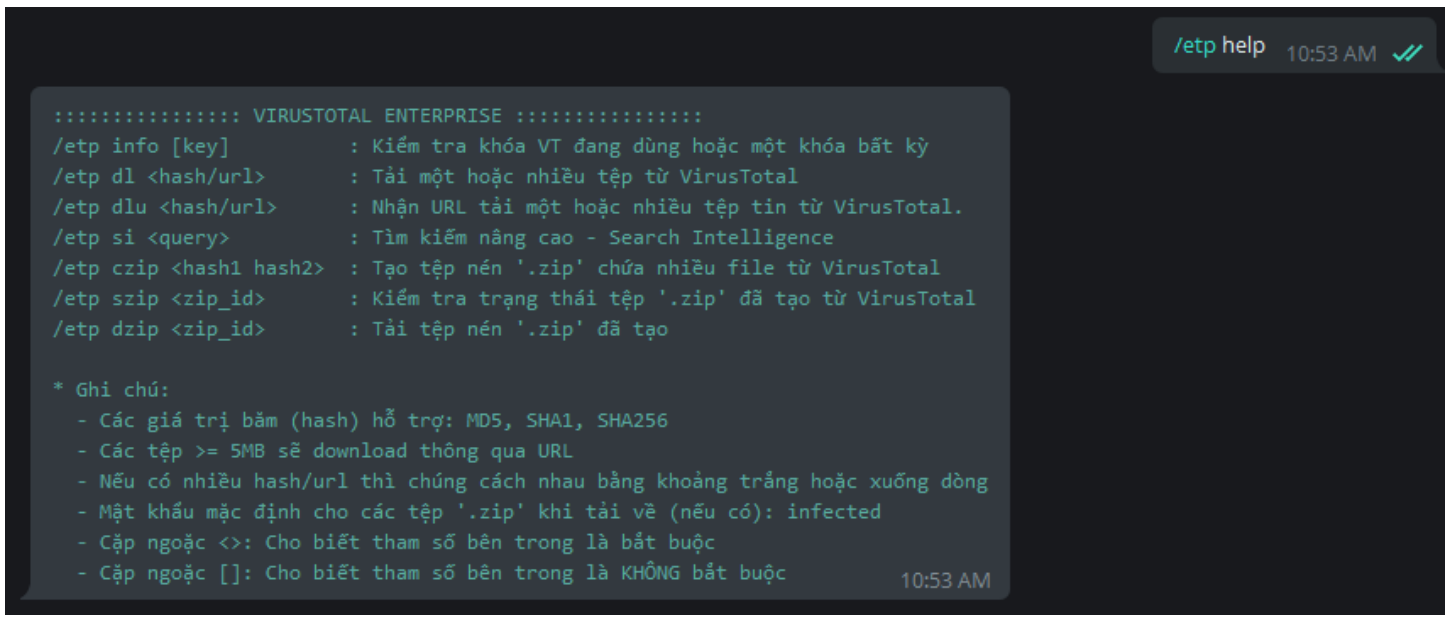
```
/help
```




Tại đây chúng ta có các nhóm tính năng được phân loại theo các `command` riêng biệt. Ví dụ nhóm tính năng nâng cao dành cho người dùng có **Premium/Private VirusTotal API Key** có command là: `/etp`

Để hiển thị trợ giúp cho một nhóm tính năng bất kỳ. Chúng ta gửi lệnh theo cú pháp: `</command>` hoặc `</command> help`. Ví dụ:

```
/etp
# Hoặc
/etp help
```

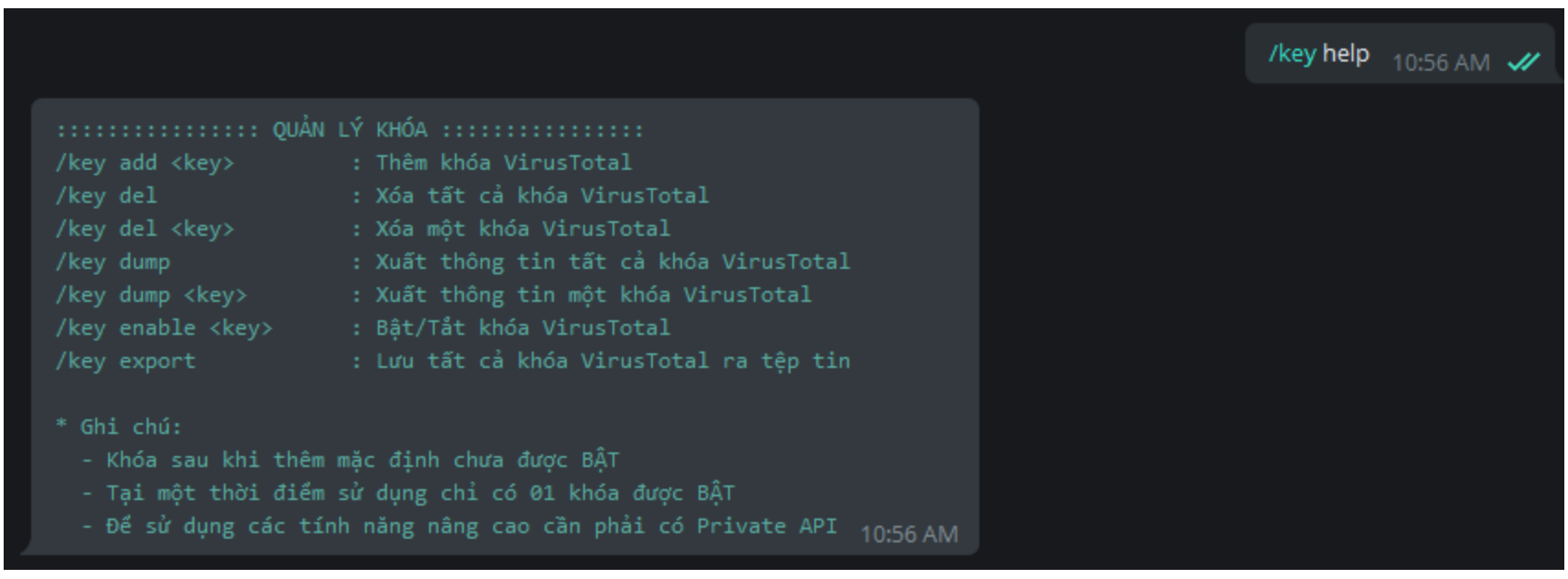



> 💡 MẸO khi sử dụng Bot: Chỉ cần gõ `/` và **một vài ký tự đầu** tiên của `command` sau đó nhấn phím `TAB` trên bàn phím. Khi đó Bot sẽ tự động hoàn thành `command` mà bạn không nhất thiết phải gõ toàn bộ command.

# 2. Trình Quản lý khóa

Để có thể sử dụng Bot, việc đầu tiên cần phải làm đó là **thiết lập khóa cá nhân** với Bot. Hiện tại Bot đã hỗ trợ đa người dùng, mỗi khóa cá nhân sẽ được định danh kèm với Telegram UserID. Như vậy với mỗi tài khoản người dùng Telegram **có thể thiết lập nhiều khóa** VirusTotal nhưng các khóa này **không được trùng nhau**. Bắt đầu thiết lập khóa với Bot, bạn nhập lệnh sau để nhận trợ giúp:

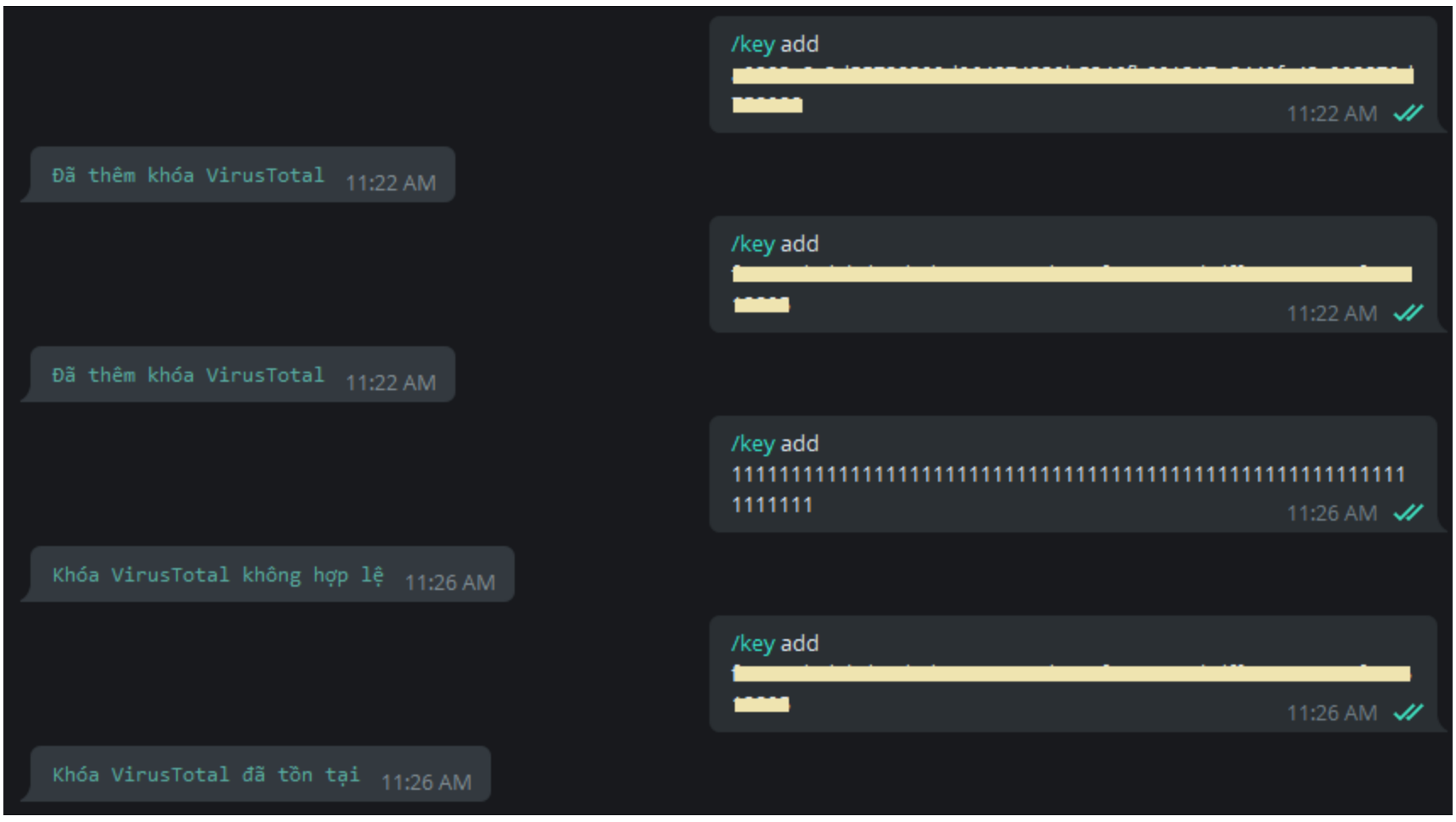
```
/key help
```




## 2.1. Thêm mới khóa VirusTotal

Để thêm mới một khóa VirusTotal. Bạn sử dụng lệnh: `/key add <key>`. Trong đó: Tham số `add` là hành động thực hiện và `<key>` là chuỗi giá trị khóa VirusTotal của bạn. Ví dụ:

```
/key add <your-api-key>
```



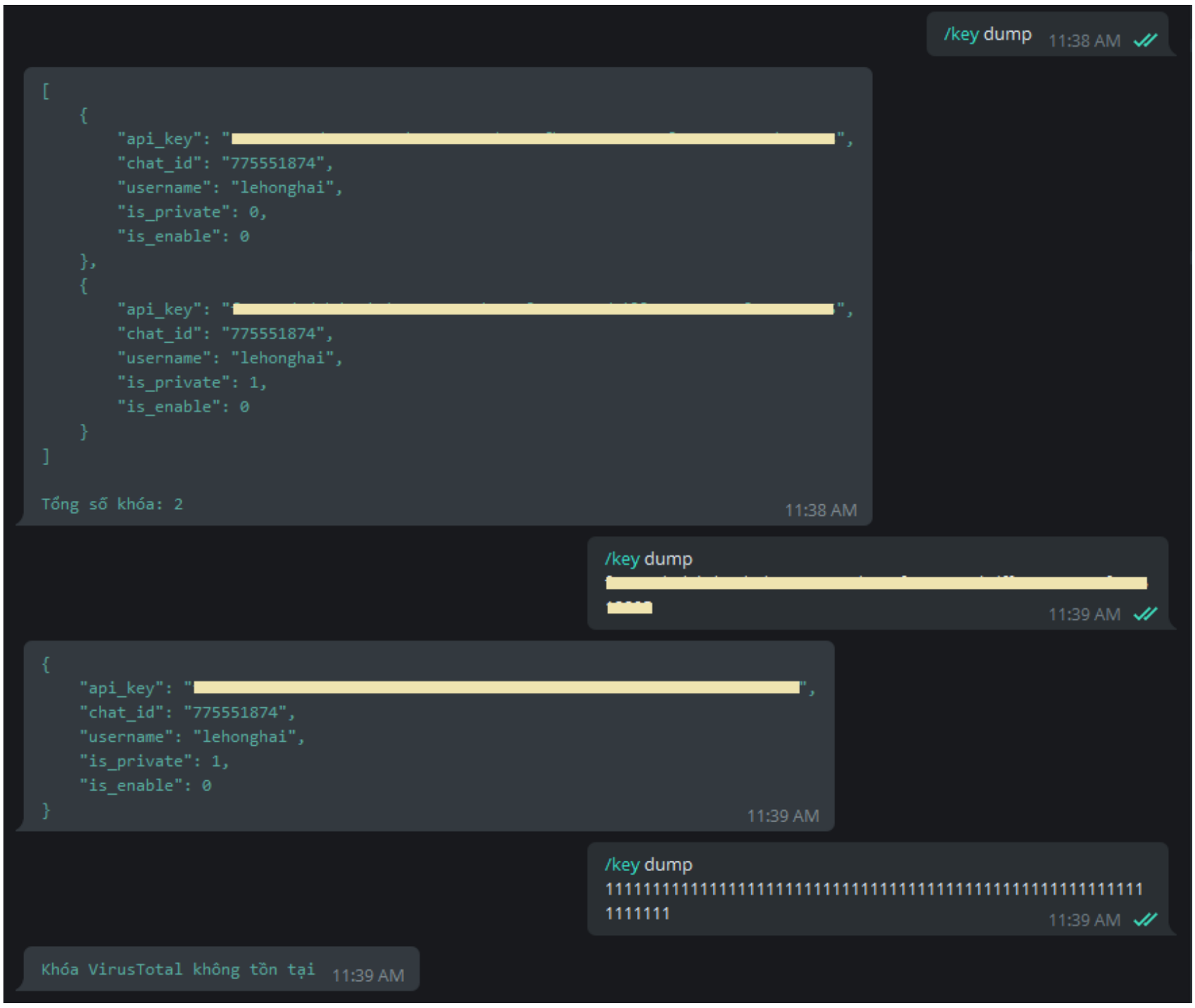

Trường hợp bạn cung cấp khóa VT không hợp lệ hoặc khóa đã được thêm trước đó, Bot sẽ thông báo như hình trên.

## 2.2. Xuất thông tin khóa VirusTotal

Để kiểm tra thông tin về các khóa VT mà bạn đã thêm. Gửi lệnh sau cho Bot:

```
# Xuất thông tin tất cả khóa VirusTotal đã thiết lập:
/key dump

# Xuất thông tin cụ thể một khóa VirusTotal đã thiết lập:
/key dump <your-api-key>
```




Giá trị `is_private` cho biết khóa đó thuộc loại nào:

- `"is_private": 1` ⇒ Cho biết đây là **Private VT Key**
- `"is_private": 0` ⇒ Cho biết đây là **Public VT Key**

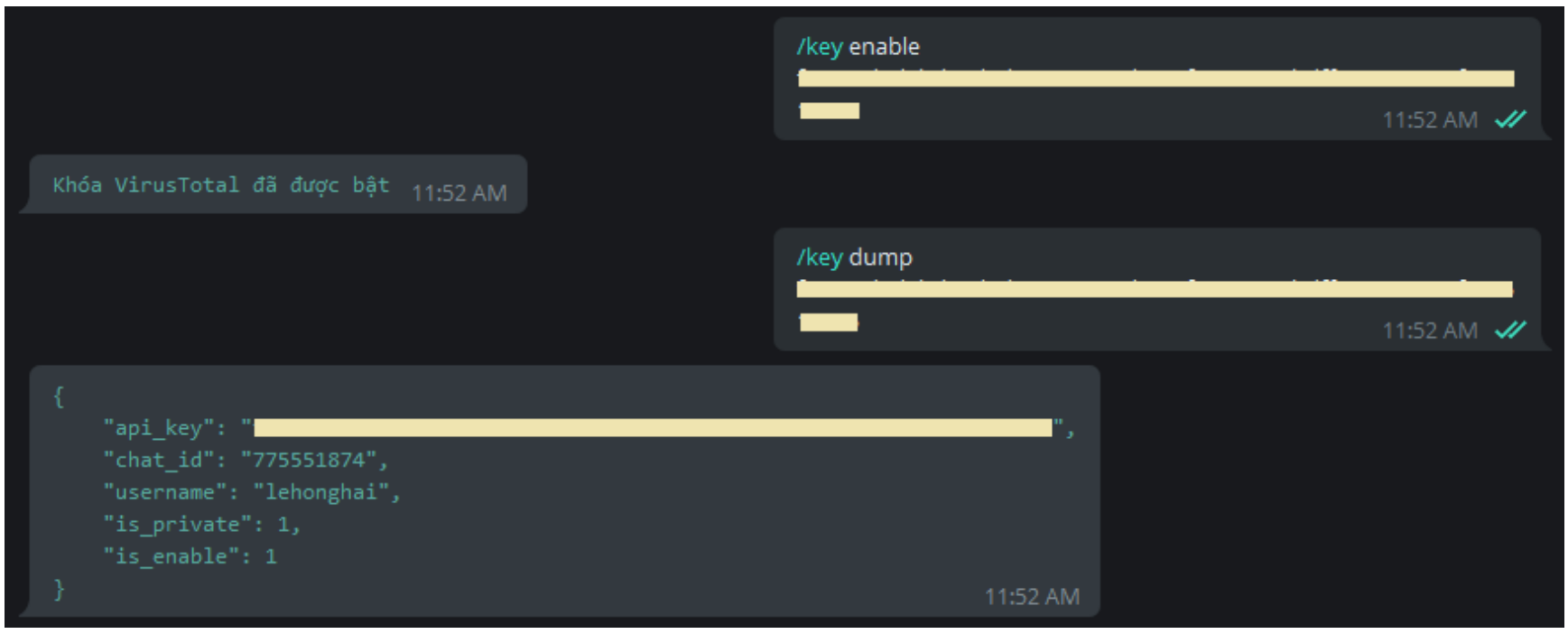
Giá trị `is_enable` cho biết trạng thái của khóa đó:

- `"is_enable": 1` ⇒ Cho biết khóa đang được **BẬT**
- `"is_enable": 0` ⇒ Cho biết khóa đang bị **TẮT**

## 2.3. Bật khóa VirusTotal

Theo mặc định, sau khi thiết lập khóa VT với Bot thì khóa đó ở trạng thái bị **TẮT** (tức là: `"is_enable": 0`). Để bắt đầu sử dụng các tính năng của Bot, cần phải **BẬT** một khóa lên. Gửi lệnh sau cho Bot:

```
/key enable <your-api-key>
```




Giá trị `is_enable` chuyển sang `1` báo hiệu khóa VT đã được bật.

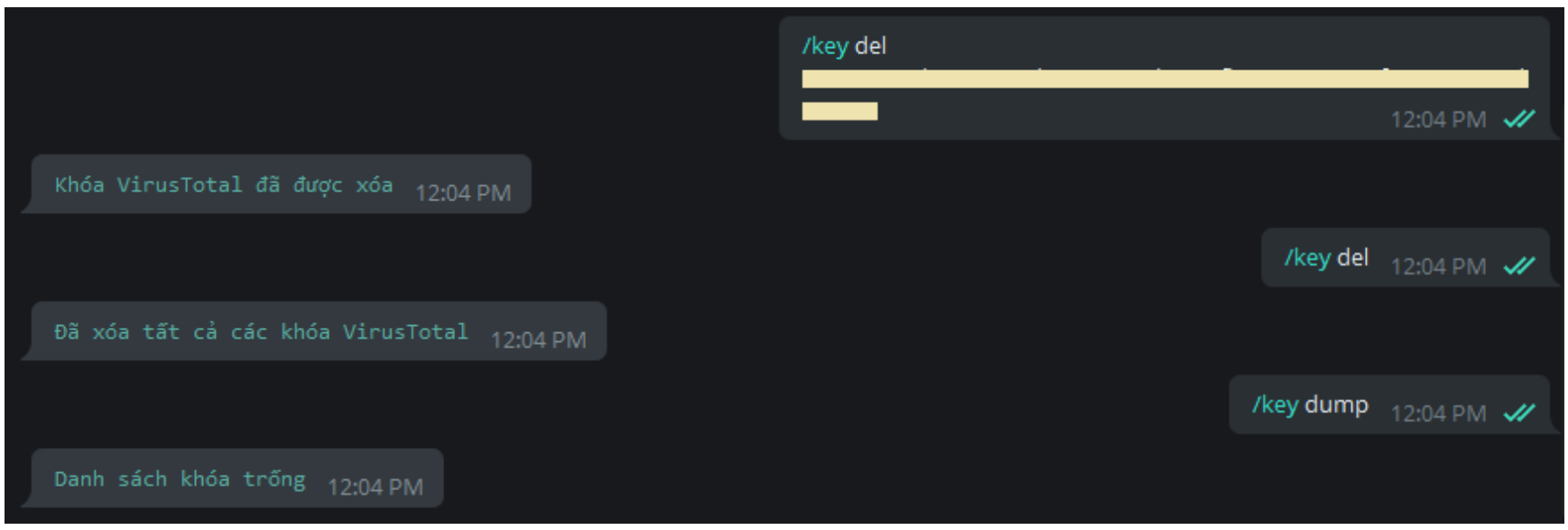
> 💡 **Lưu ý:** Tại một thời điểm chỉ có **duy nhất** một khóa VT được BẬT. Khi bạn cố gắng BẬT một khóa khác lên thì khóa đc bật trước đó sẽ chuyển sang trạng thái TẮT.

## 2.4. Xóa khóa VirusTotal

Để xóa khóa VT đã thiết lập với Bot trước đó. Bạn gửi lệnh sau cho Bot:

```
# Xóa một khóa VT đã thêm trước đó:
/key del <your-api-key>

# Xóa tất cả các khóa có trong danh sách:
/key del
```




## 2.5. Tải về khóa VirusTotal

Để tiện lợi cho việc lưu trữ các khóa đã thiết lập với Bot. Bạn có thể tải về tệp tin chứa cấu hình các khóa. Gửi lệnh sau cho Bot:

```
/key export
```

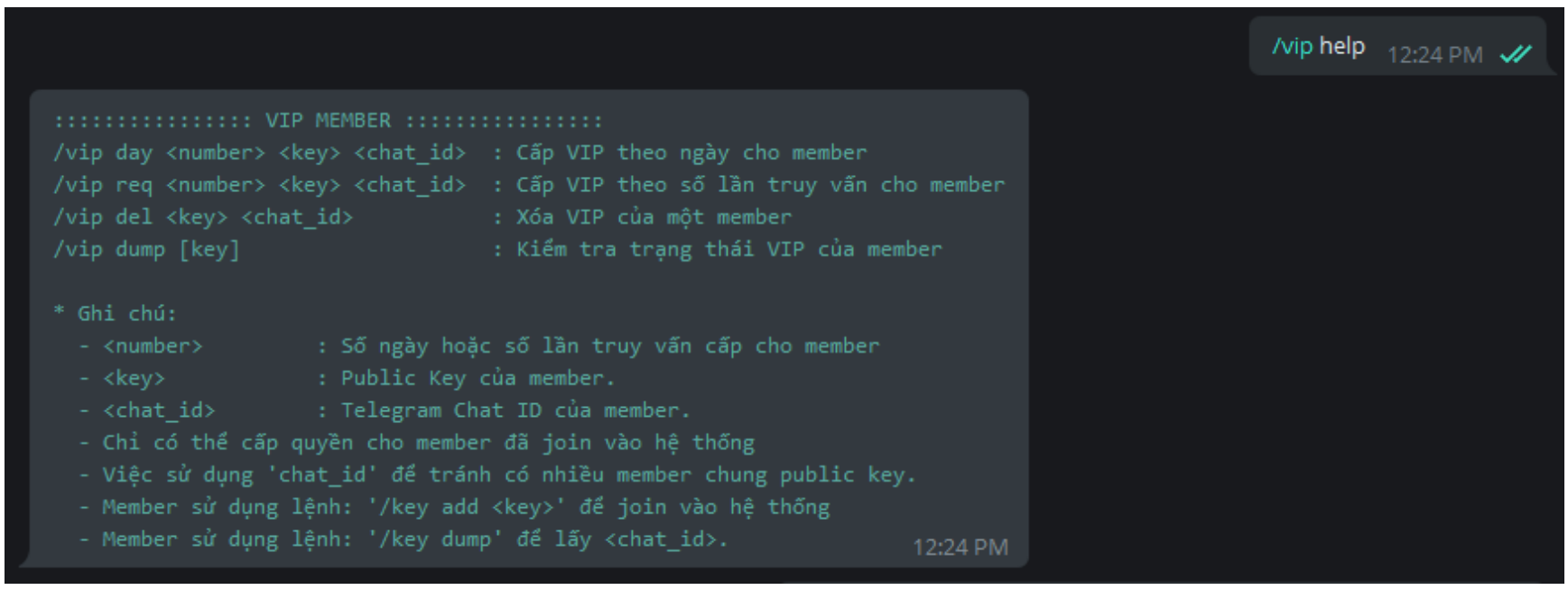

Bây giờ bạn đã có thể tải về file cấu hình các khóa VT và lưu nó ở một nơi an toàn trên máy tính của bạn.

# 3. Quản lý Member

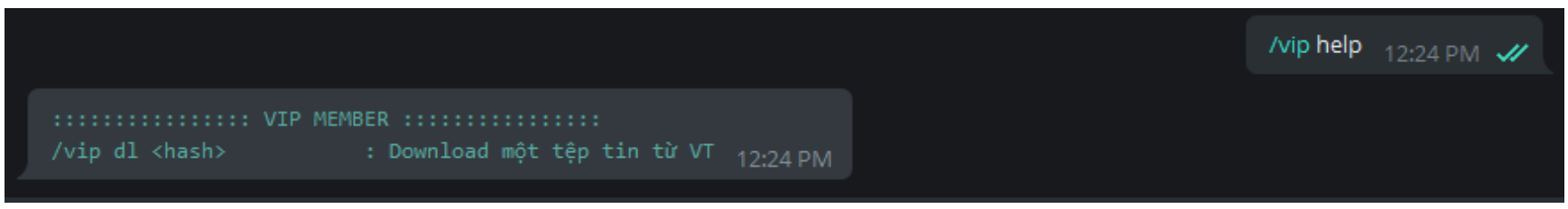
Để linh động trong quá trình sử dụng Bot. Người dùng sở hữu khóa **VT Private** (sau đây gọi là **Admin**) có thể cấp một số quyền mà chỉ có Private Key mới có cho người dùng chỉ sở hữu khóa **VT Public** (sau đây gọi là **Member**). Hiện tại Bot hỗ trợ cấp quyền `download` một tệp tin từ VT cho Member theo `02` hình thức sau, gọi chung là cấp `VIP` 🤣:

1. **Cấp VIP theo ngày**: Member trong thời hạn sử dụng của mình tính theo ngày có thể download không giới hạn số lần từ VT.
2. **Cấp VIP theo số lần request**: Member sử dụng số lần download trong phạm vi đc cấp, nếu download bị lỗi Member vẫn được bảo toàn lượt download đó mà không bị trừ. Nếu hết số lượt download, Member liên hệ Admin để cấp tiếp.

Giao diện chức năng VIP của **Admin**:




Giao diện chức năng VIP của **Member**:




## 3.1. Admin cấp VIP cho Member

Member muốn được cấp VIP cần liên hệ và gửi cho **Admin** thông tin về khóa VT Public của mình kèm Telegram UserID. Member thực hiện các bước sau:

1. Thêm mới khóa VT
2. Xuất thông tin khóa VT
3. Gửi thông tin khóa Public VT đã thêm cho Admin. Ví dụ:

```
[
    {
        "api_key": "1111111111111111111111111111111111111111111111111111111111111111",
        "chat_id": "775551874",
        "username": "lehonghai",
        "is_private": 0,
        "is_enable": 1
    }
]
```

Admin sau khi có được thông tin gồm: `api_key` và `chat_id` của Member. Có thể lựa chọn các phương thức cấp `VIP` sau:

### 3.1.1. Cấp VIP theo số ngày cho một Member:

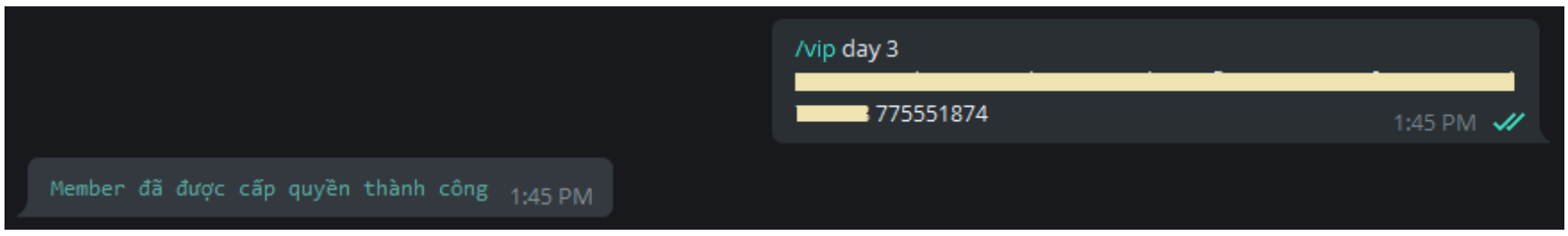
```
/vip day <number> <api_key> <chat_id>
```

**Trong đó:**

- `<number>`: Số ngày muốn cấp cho Member

- `<api_key>`: Khóa VT Public của Member
- `<chat_id>`: Telegram UserID của Member

Demo: **Cấp VIP 03 ngày** cho Member



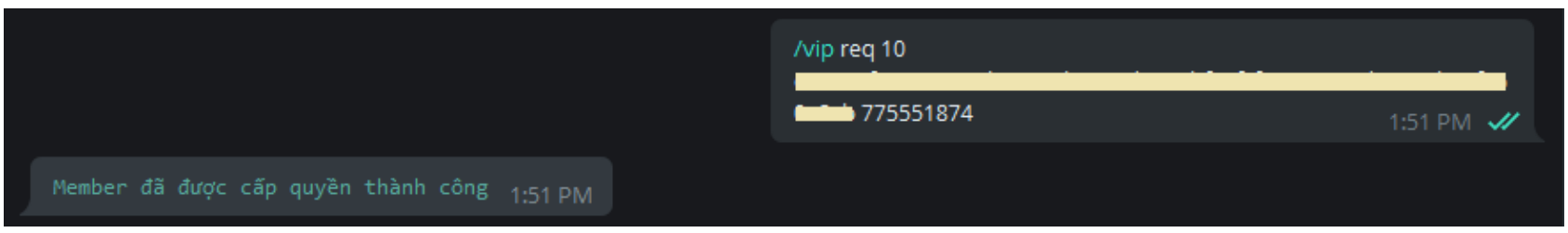

### 3.1.2. Cấp VIP theo số lượt truy vấn cho Member

```
/vip req <number> <api_key> <chat_id>
```

**Trong đó:**

- `<number>`: Số lượt truy vấn muốn cấp cho Member
- `<api_key>`: Khóa VT Public của Member
- `<chat_id>`: Telegram UserID của Member

Demo: **Cấp VIP 10 lượt** truy vấn (download) cho Member

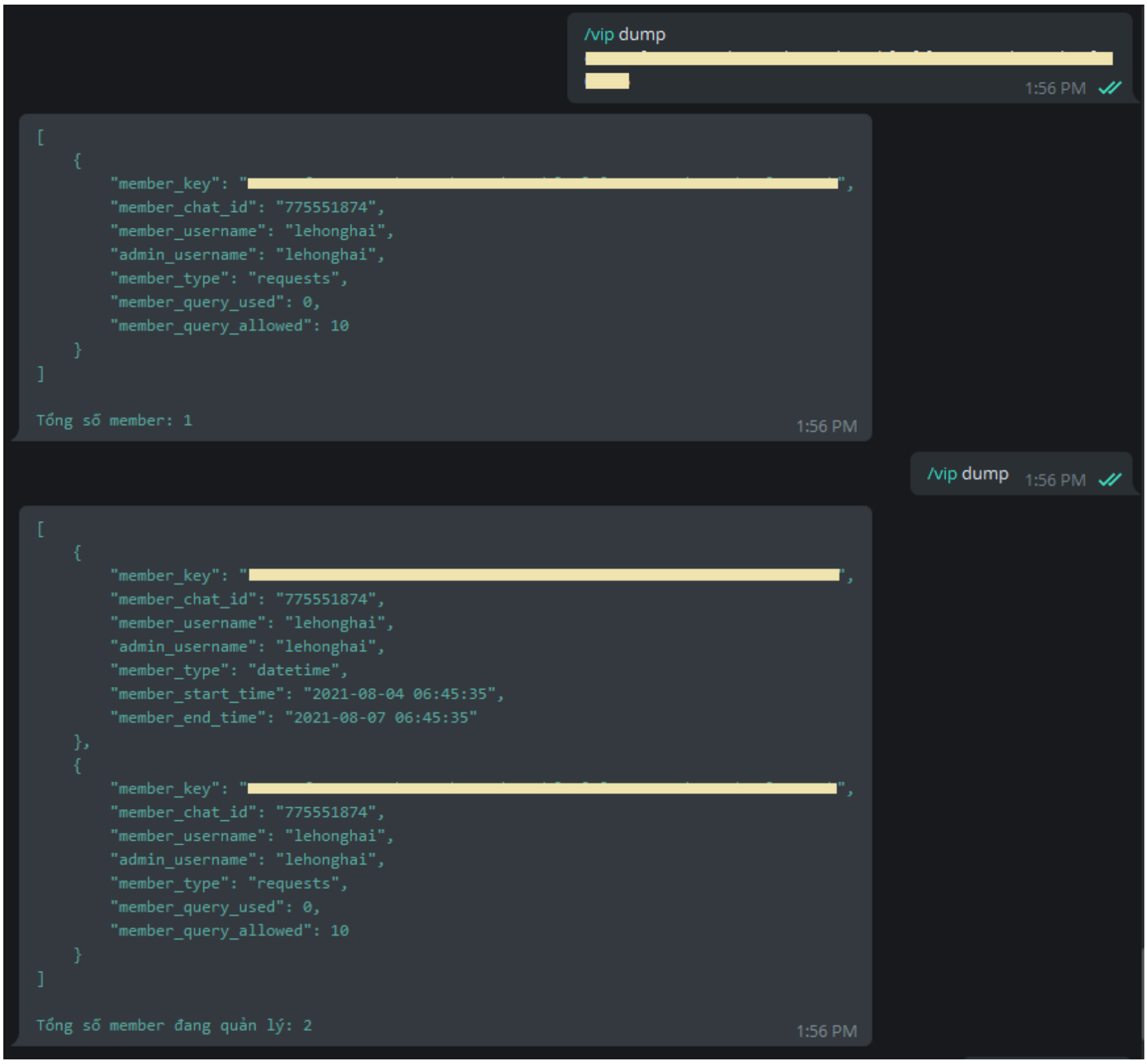



## 3.2. Admin kiểm tra trạng thái VIP của Member

Tại giao diện chức năng VIP của Admin. Để kiểm tra trạng thái VIP của các Member cũng như mức độ đã sử dụng của Member. Gửi lệnh sau cho Bot:

```
# Kiểm tra trạng thái của một Member
/vip dump <api_key>

# Hoặc: Kiểm tra trạng thái của tất cả Member
/vip dump
```



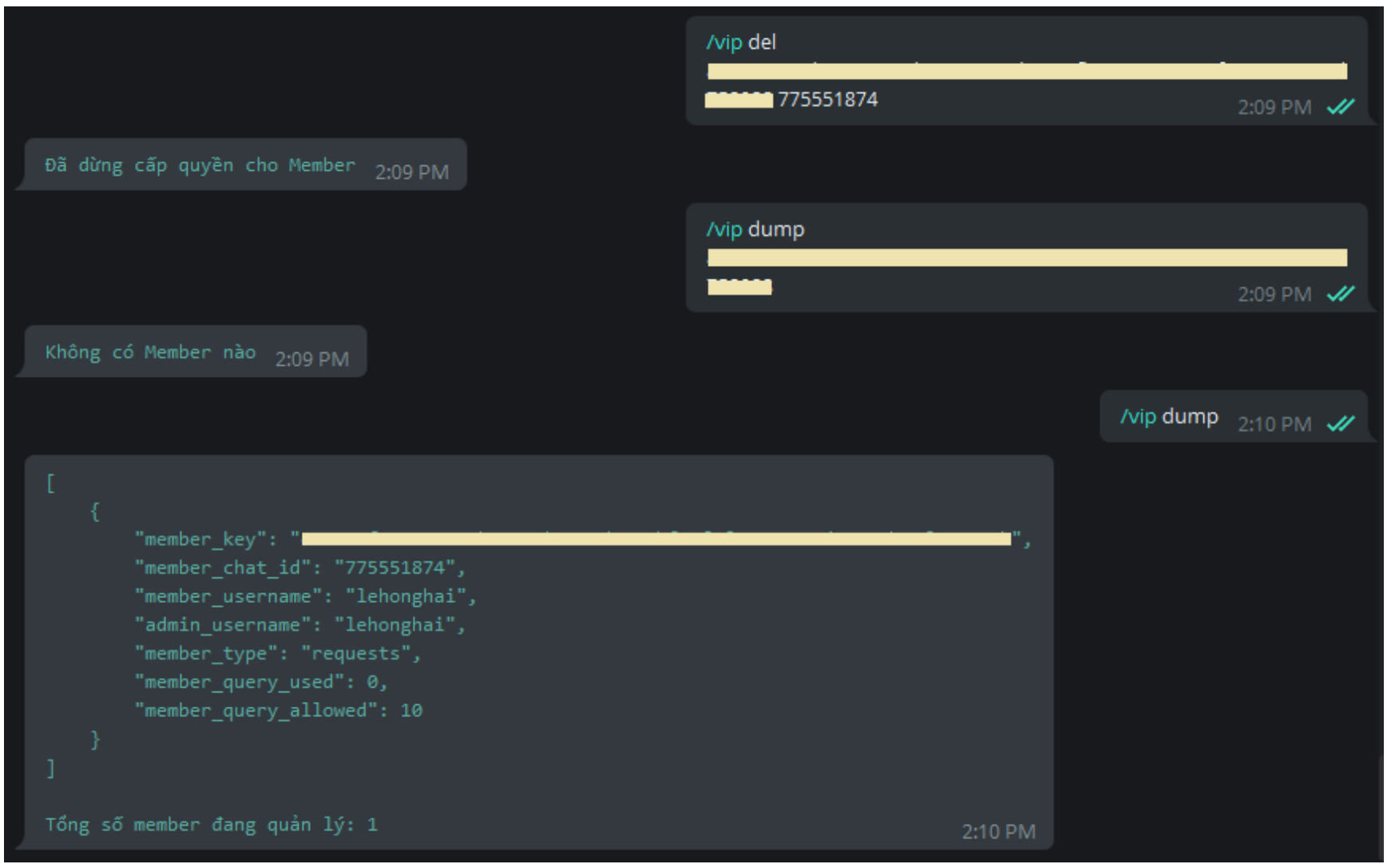

Trong đó:

- `member_key`: Khóa VT của Member
- `member_chat_id`: Telegram UserID của Member
- `member_username`: Telegram Username của Member
- `admin_username`: Telegram Username của Admin
- `member_type`: Loại VIP Member (`datetime`: VIP theo ngày, `requests`: VIP theo lượt download)
- `member_start_time`, `member_end_time`: Thời gian bắt đầu và kết thúc VIP của Member
- `member_query_used`, `member_query_allowed`: Số lượt download đã dùng và tổng số lượt download của Member

## 3.3. Admin Thu hồi VIP của Member

Để ngừng cấp VIP cho một Member. Admin tiến hành gửi lệnh sau:

```
/vip del <api_key> <chat_id>
```

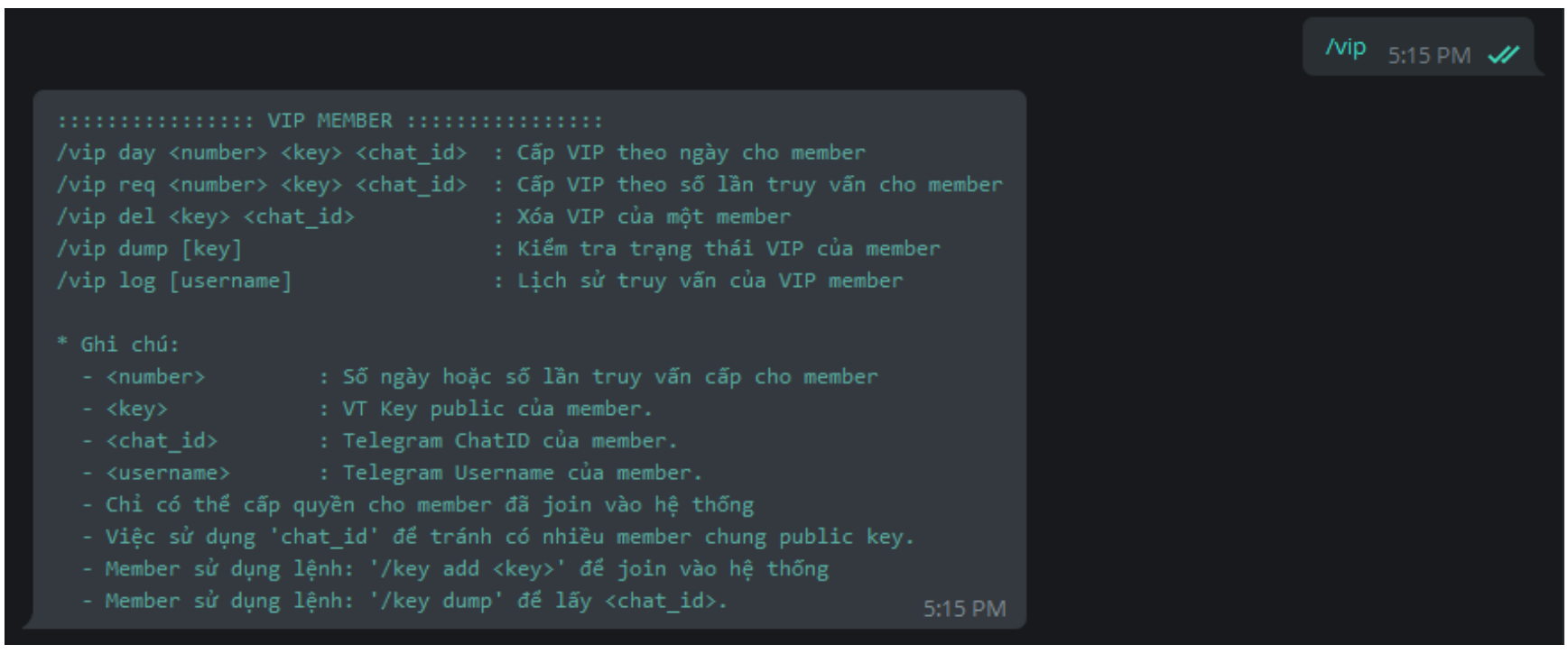



## 3.4. Lịch sử truy vấn của VIP Member

Bot hiện đã có tính năng theo dõi hoạt động của VIP Member. Admin có thể sử dụng tính năng này để theo dõi số lần truy vấn thành công, thất bại của Member. Biết được Member đã search những gì và download những tệp nào.

Gửi lệnh sau để nhận Menu trợ giúp từ Bot

```
/vip
# Hoặc
/vip help
```




Có 02 hình thức xem lại lịch sử truy vấn của Member như sau:

- Xem logs của tất cả Member mà mình đang quản lý. Cú pháp: `/vip log`
- Xem logs của một Member cụ thể theo Telegram Username. Cú pháp: `/vip log <username>`

Và theo mặc định thì Bot sẽ gửi về kết quả của 20 bản ghi logs gần nhất theo thứ tự thời gian từ cũ nhất ⇒ mới nhất.

### 3.4.1. Xem logs của tất cả Member:

```
/vip log
```

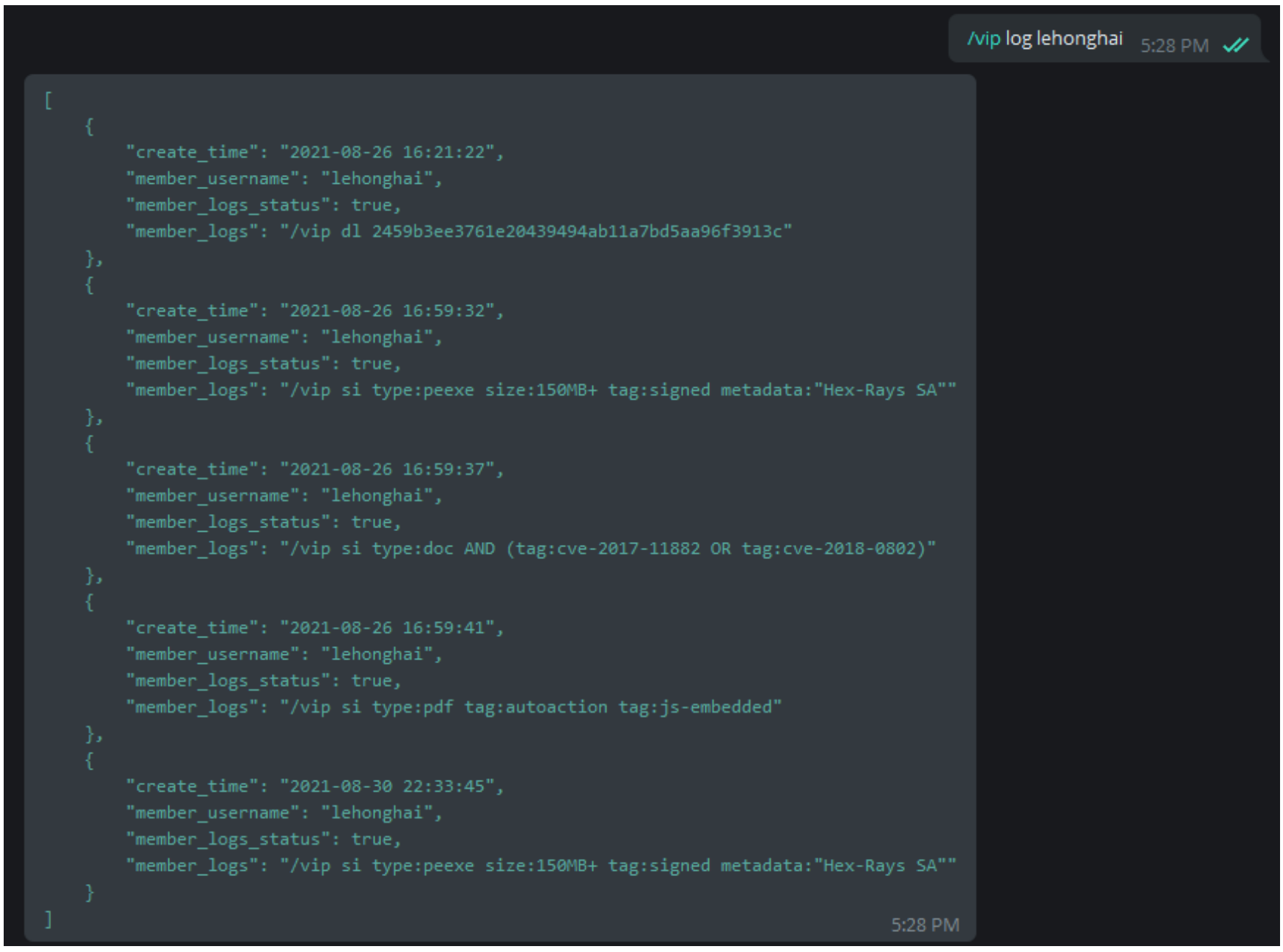
/vip log 5:20 PM


```
[
    {
        "create_time": "2021-08-26 10:17:16",
        "member_username": "lehonghai",
        "member_logs_status": true,
        "member_logs": "/vip dl 8ccd9591e9438a313a21958c7f8edce4b238bbb147e8284ec4a2b7b488b920ca"
    },
    {
        "create_time": "2021-08-26 16:21:22",
        "member_username": "lehonghai",
        "member_logs_status": true,
        "member_logs": "/vip dl 2459b3ee3761e20439494ab11a7bd5aa96f3913c"
    },
    {
        "create_time": "2021-08-26 16:59:26",
        "member_username": "lehonghai",
        "member_logs_status": true,
        "member_logs": "/vip si type:zip size:50MB+ name:"Assessor""
    },
    {
        "create_time": "2021-08-26 16:59:32",
        "member_username": "lehonghai",
        "member_logs_status": true,
        "member_logs": "/vip si type:peexe size:150MB+ tag:signed metadata:"Hex-Rays SA""
    },
    {
        "create_time": "2021-08-26 16:59:37",
        "member_username": "lehonghai",
        "member_logs_status": true,
        "member_logs": "/vip si type:doc AND (tag:cve-2017-11882 OR tag:cve-2018-0802)"
    }
]
```


5:20 PM

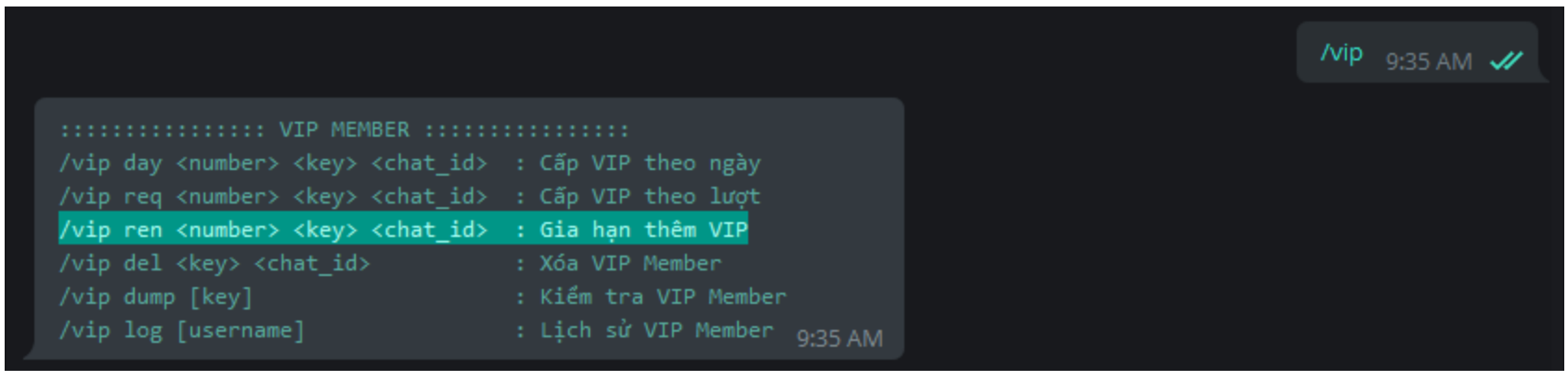
### 3.4.2. Xem logs của một Member:

```
/vip log lehonghai
```




## 3.5. Gia hạn VIP Member

Trường hợp Member hết hạn sử dụng VIP, để không phải xóa Member đi xong tạo lại có thể sử dụng chức năng Gia hạn VIP, áp dụng cho cả 2 loại VIP Member là theo số ngày được cấp phép và theo Số lượt truy vấn được cấp.




Cú pháp như sau:

```
/vip ren <number> <key> <chat_id>
```

**Trong đó:**

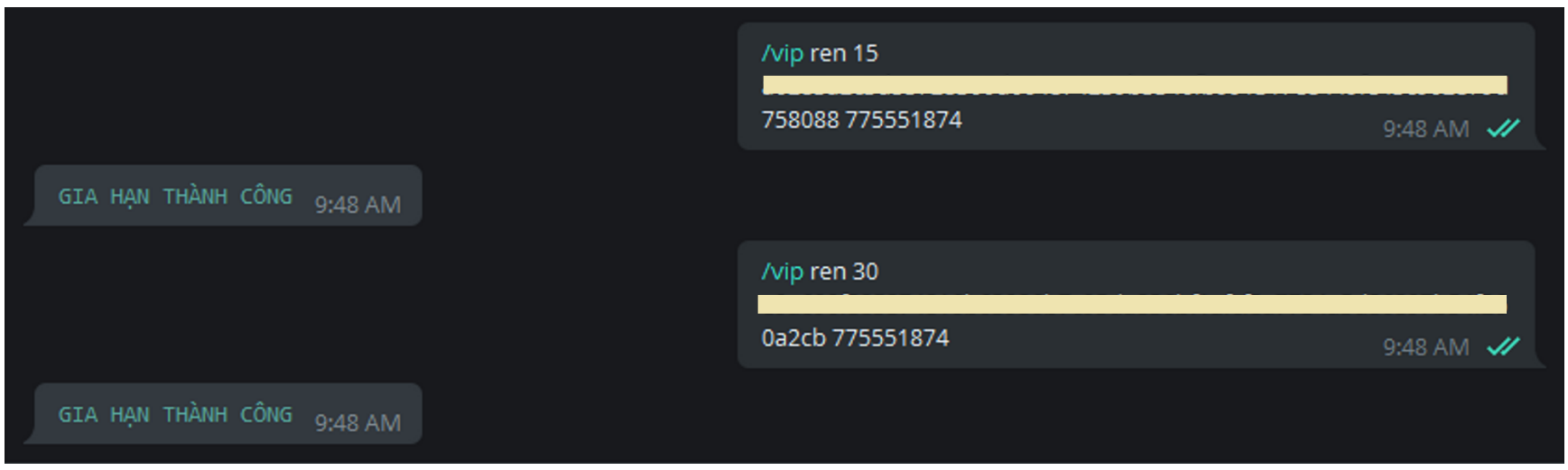
- `number`: Số lượt truy vấn hoặc số ngày muốn tăng thêm cho Member
- `key`: Khóa VT của Member. Sử dụng `/vip dump` để xem thông tin các Member mình đã cấp VIP.
- `chat_id`: Telegram ID của Member. Cũng sử dụng `/vip dump` để xem thông tin này.

**Demo:**

Giả sử hiện tại đang cấp VIP cho 2 Member:

- member 1: Có ngày hết hạn VIP là: `2021-11-11 21:04:19`
- member 2: Có tổng số lượt truy vấn là: `20`


Thực hiện gia hạn `thêm 15 ngày` cho Member 1 và `thêm 30 lượt` truy vấn cho Member 2:

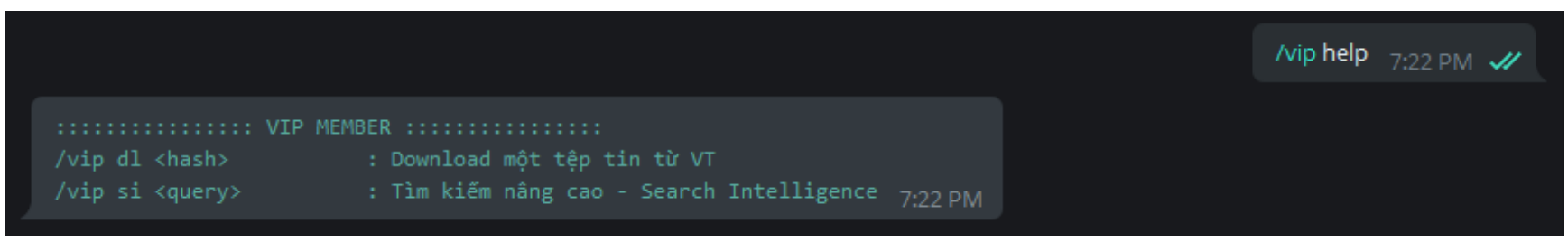



Kiểm tra kết quả: Member 1 được gia hạn thêm từ `2021-11-11 21:04:19` lên thành `2021-11-26 21:04:19`. Còn Member 2 gia hạn thêm từ `20` lên `50`:


# 4. Nhóm chức năng cho VIP Member

Để biết VIP Member hiện tại được sử dụng những chức năng gì. Bạn gửi một trong các lệnh sau cho Bot:

```
/vip
/vip help
```

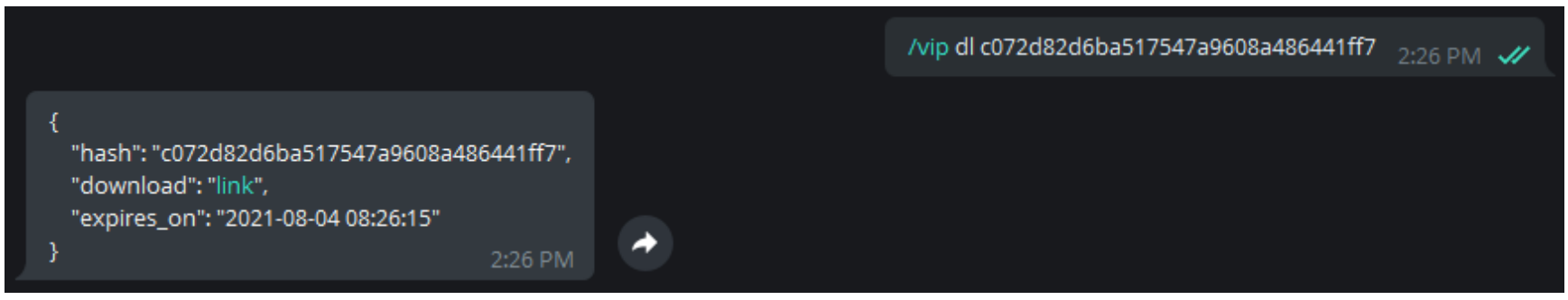



## 4.1. Download tệp tin từ VT

Sau khi Member được cấp quyền download tệp tin từ VT. Member thực hiện gửi lệnh sau để nhận URL download từ Bot:

```
/vip dl <hash>
```

Trong đó: `<hash>` là giá trị băm của tệp muốn download. Hiện tại Bot hỗ trợ 3 loại băm là: `MD5`, `SHA1`, `SHA256`




> 💡 Bot sẽ gửi link download cho Member, link download có hiệu lực trong vòng 60 phút và không giới hạn số lần click download trong 60 phút này. Quá thời gian 60 phút sẽ không thể download tệp được nữa.

## 4.2. VirusTotal Intelligence Search

VT Search Intelligence là tính năng mới dành cho VIP Member. Member được cấp quyền thực hiện tính năng này có thể Search nâng cao như tính năng dành cho Admin. Để thực hiện Search Intelligence, bạn gửi lệnh theo cú pháp sau cho Bot:

```
/vip si <query>
```

Cách thực hiện và Demo xem phần 5.3. VirusTotal Intelligence Search. **Lưu ý sử dụng đúng cú pháp là:** `/vip si <query>`. **KHÔNG** sử dụng cú pháp `/etp si <query>` vì cú pháp đó dành cho Admin.

# 5. Sử dụng nhóm tính năng VT Enterprise

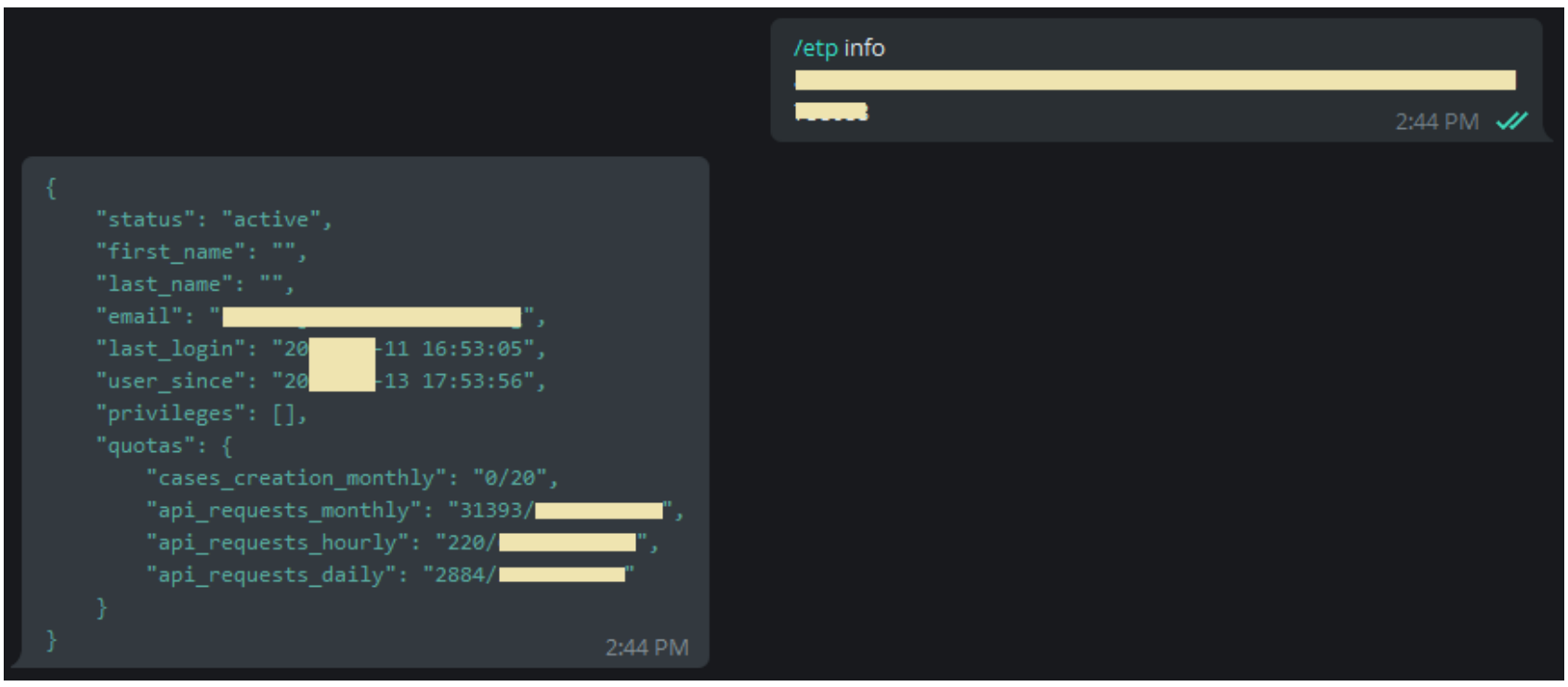
## 5.1. Kiểm tra khóa đang dùng hay khóa bất kỳ

Kiểm tra thông tin khóa VT đang sử dụng

```
/etp info
```


Kiểm tra thông tin một khóa VT bất kỳ

```
/etp info <api_key>
```



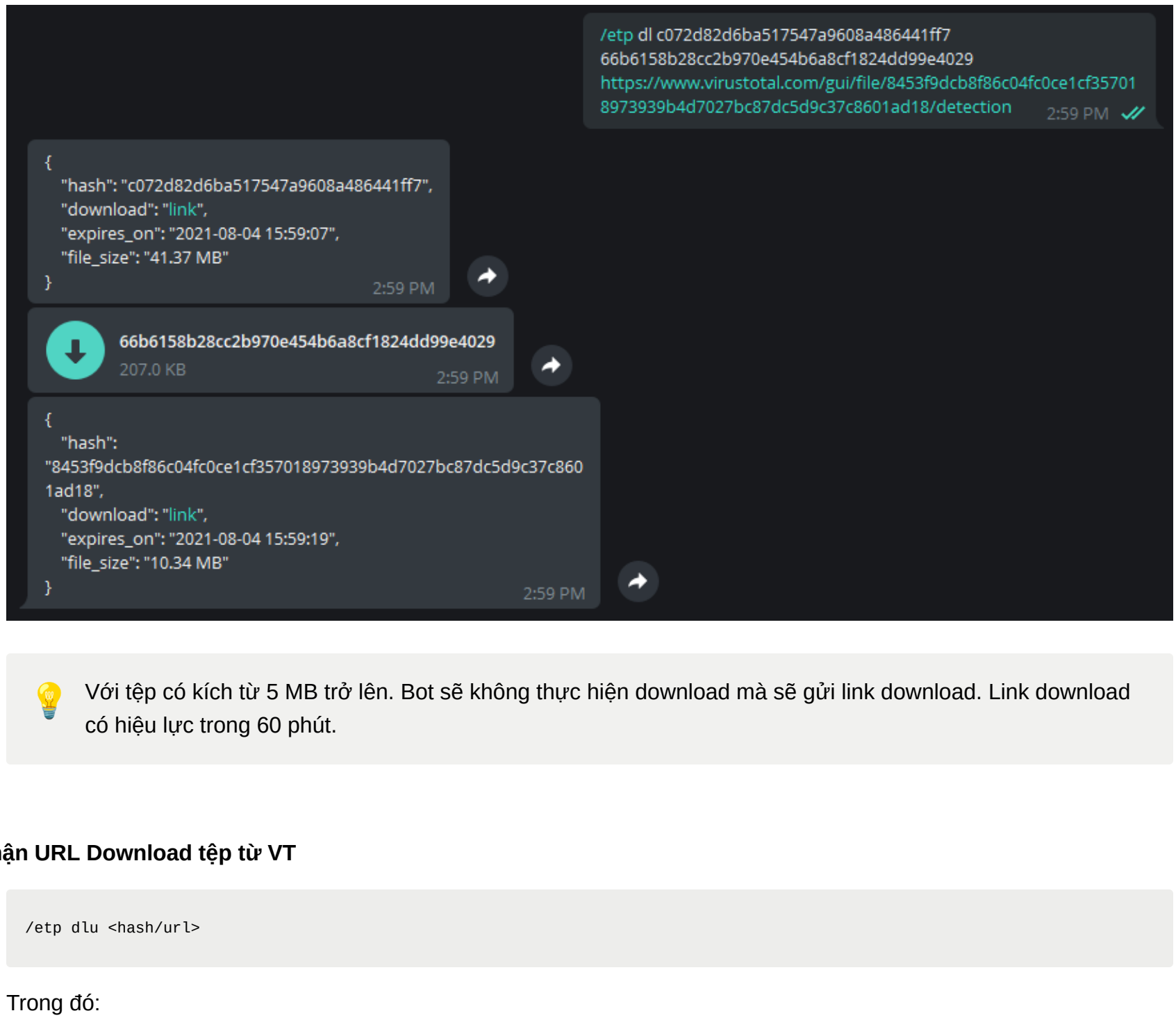

## 5.2. Download tệp tin từ VT

### Download tệp từ VT

```
/etp dl <hash/url>
```

**Trong đó:**

- `<hash/url>`: Giá trị băm (`MD5`, `SHA1`, `SHA256`) hoặc địa chỉ `URL` đến VirusTotal Sample. Chức năng này hỗ trợ gửi nhiều hash hoặc URL. tuy nhiên không được vượt quá 10.



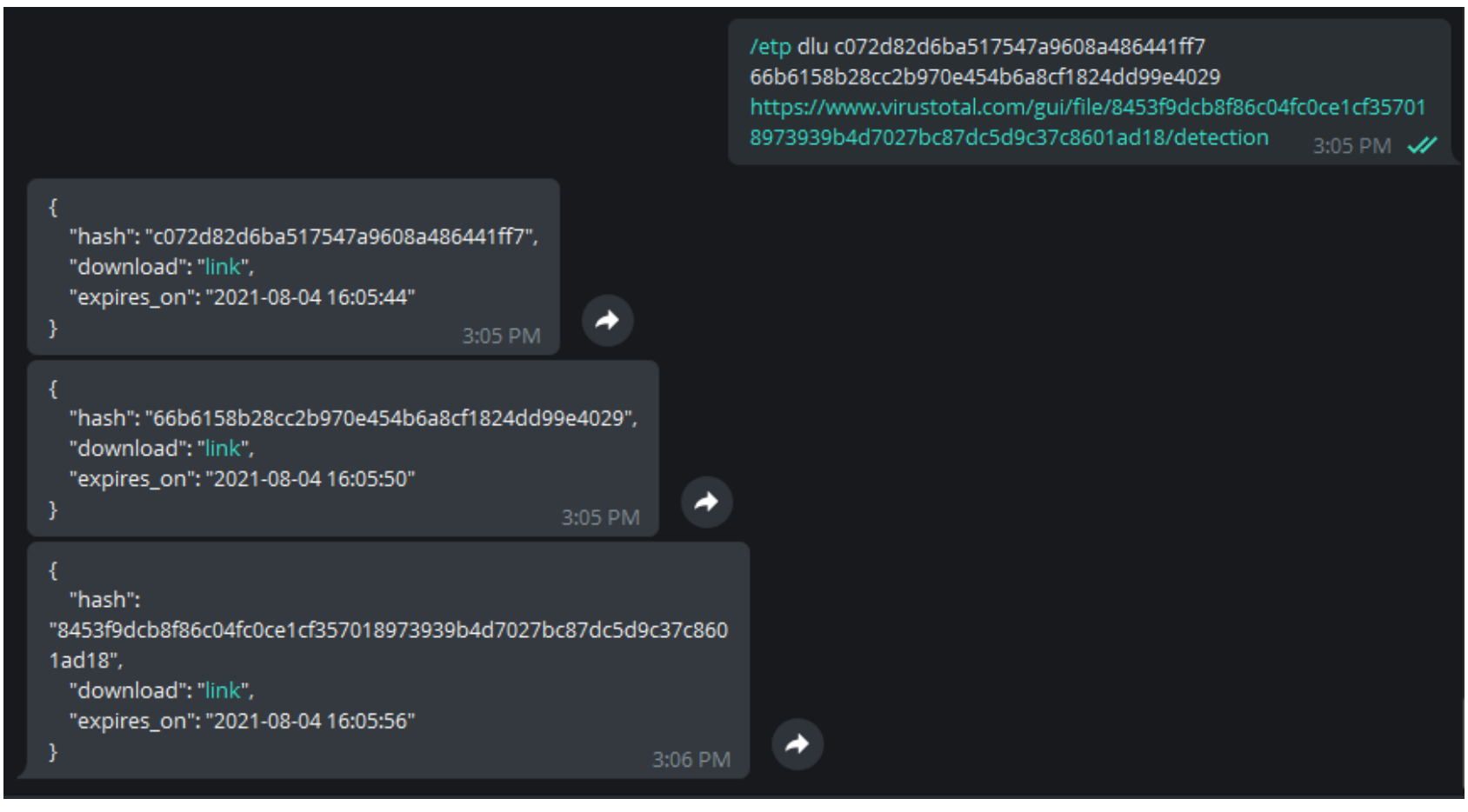

> 💡 Với tệp có kích từ 5 MB trở lên. Bot sẽ không thực hiện download mà sẽ gửi link download. Link download có hiệu lực trong 60 phút.

### Nhận URL Download tệp từ VT

```
/etp dlu <hash/url>
```

Trong đó:

- `<hash/url>`: Giá trị băm (`MD5`, `SHA1`, `SHA256`) hoặc địa chỉ `URL` đến VirusTotal Sample. Chức năng này hỗ trợ gửi nhiều hash hoặc URL. tuy nhiên không được vượt quá 10.




## 5.3. VirusTotal Intelligence Search

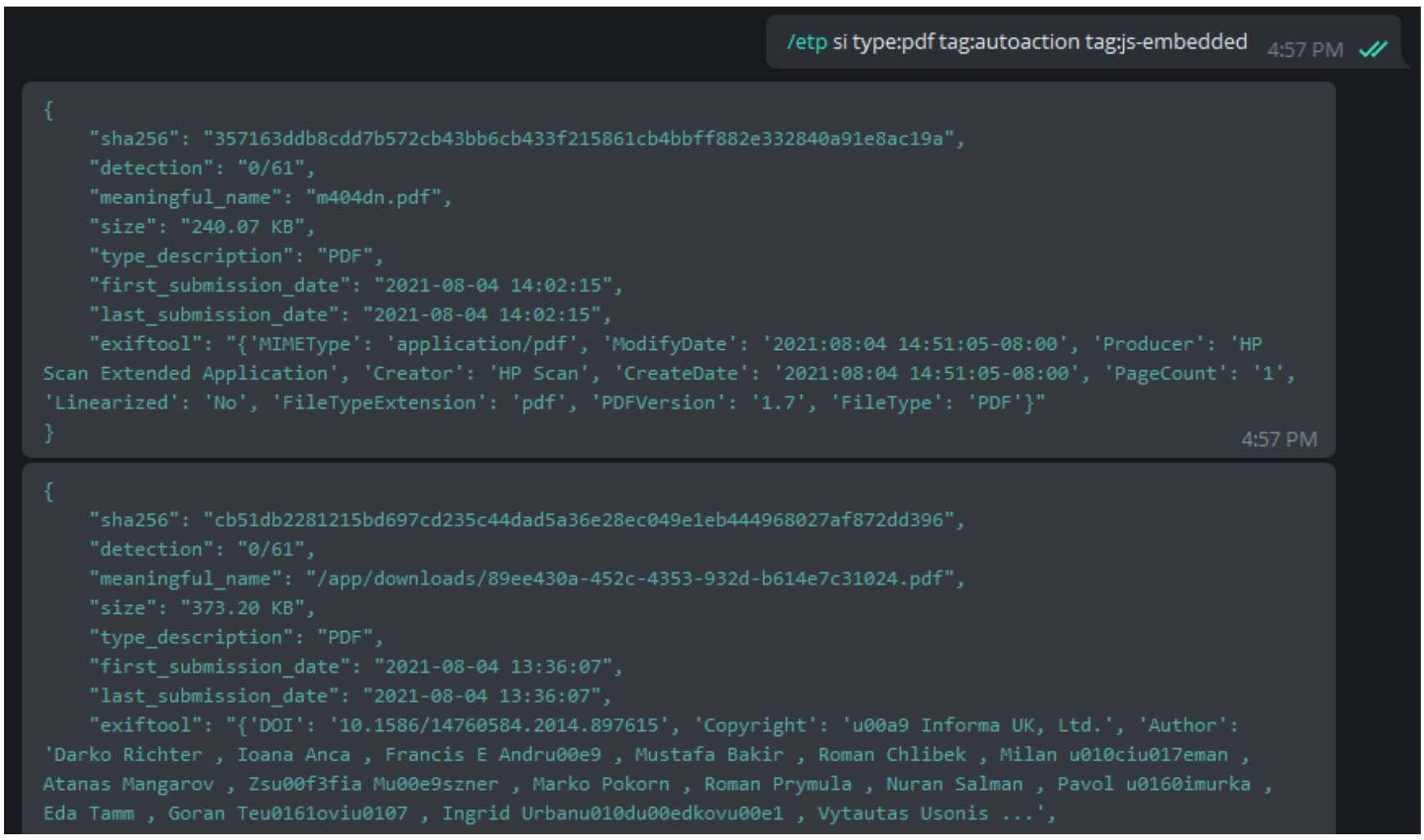
**VirusTotal Intelligence Search** không chỉ áp dụng cho đối tượng `Tệp tin` mà còn cho cả `Domain`, `IP Adress` và `URL`. Hiện tại **Bot đã hỗ trợ Intelligence Search với** `Tệp tin`.

Tham khảo cú pháp cũng như cách thức tạo câu truy vấn cho **Intelligence Search:**

- **VirusTotal Intelligence Introduction**: https://support.virustotal.com/hc/en-us/articles/360001387057-VirusTotal-Intelligence-Introduction
- **File search modifiers**: https://support.virustotal.com/hc/en-us/articles/360001385897-VT-Intelligence-search-modifiers

**Demo 1:** Search các tệp **PDF** có khả năng là **Malicious documents.** Các tệp này có nhúng **JavaScript** bên trong:

```
/etp si type:pdf tag:autoaction tag:js-embedded
```




**Demo 2:** Search các tệp **Office Documents** được VT phát hiện là có mã khai thác **Microsoft Word** . Lỗ hổng có định danh là: `CVE-2017-11882` hoặc `CVE-2018-0802`

```
/etp si type:doc AND (tag:cve-2017-11882 OR tag:cve-2018-0802)
```

/etp si type:doc AND (tag:cve-2017-11882 OR tag:cve-2018-0802)
5:03 PM


```
{
    "sha256": "1ae2cbaf4fca2de9703c1948084959265117c1ebe3f6fbcff2ffdec26cb22040",
    "detection": "3/60",
    "meaningful_name": "oleObject0.bin",
    "size": "71.53 KB",
    "type_description": "MS Word Document",
    "first_submission_date": "2021-08-04 14:24:46",
    "last_submission_date": "2021-08-04 14:24:46",
    "exiftool": "{'MIMEType': 'image/vnd.fpx', 'FileType': 'FPX', 'FileTypeExtension': 'fpx'}"
}
```

5:03 PM


```
{
    "sha256": "459c51c1a5eaec318bd21a79361a9c31491d286bcd8e10c77310ef4940d15b54",
    "detection": "20/59",
    "meaningful_name": "oleObject0.bin",
    "size": "73.31 KB",
    "type_description": "MS Word Document",
    "first_submission_date": "2021-08-04 14:23:38",
    "last_submission_date": "2021-08-04 14:23:38",
    "exiftool": "{'MIMEType': 'image/vnd.fpx', 'FileType': 'FPX', 'FileTypeExtension': 'fpx'}"
}
```

5:03 PM


```
{
    "sha256": "d186a5412947f0085778b0ec03d8b1c20853dc960bbd515fe11aa192b97fea93",
    "detection": "17/59",
    "meaningful_name": "oleObject0.bin",
    "size": "73.31 KB",
    "type_description": "MS Word Document",
    "first_submission_date": "2021-08-04 14:14:33",
    "last_submission_date": "2021-08-04 14:14:33",
    "exiftool": "{'MIMEType': 'image/vnd.fpx', 'FileType': 'FPX', 'FileTypeExtension': 'fpx'}"
}
```

5:03 PM

💡 Theo mặc định số lượng kết quả trả về khi Intelligence Search là: `05`

# 6. Sử dụng Shodan Search Engine

Hiện tại Threat Intelligence Bot đã tích hợp **Shodan Search Engine**. Sử dụng lệnh `/shodan` hoặc `/shodan help` để nhận trợ giúp cho nhóm tính năng này:

```
/shodan
/shodan help
```

/shodan help 4:36 PM

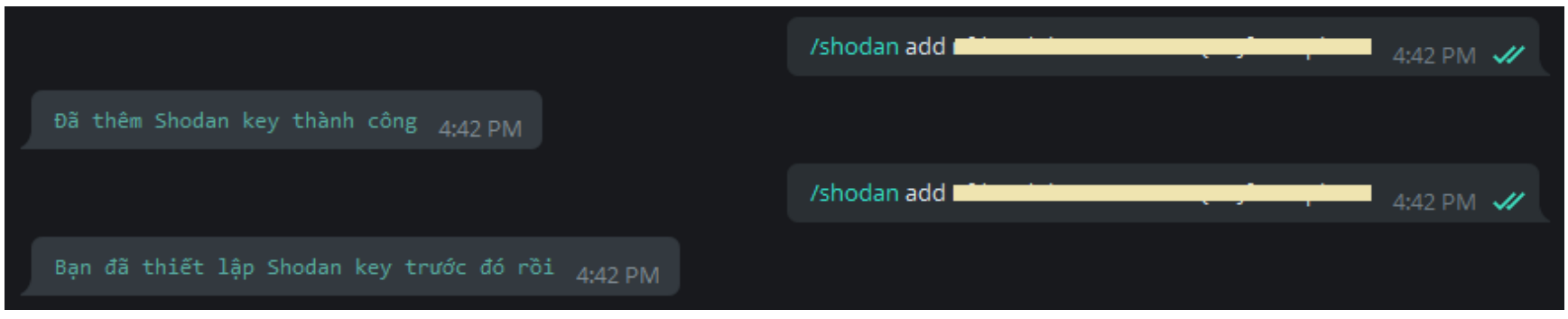
```
:::::::::::::::: SHODAN SEARCH ENGINE ::::::::::::::::
/shodan add <key>               : Thêm Shodan key
/shodan del                     : Xóa Shodan key
/shodan info <key>              : Thông tin Shodan key
/shodan ip <ip>                 : Tìm kiếm một IP trên Shodan
/shodan search <string>         : Tìm kiếm nâng cao trên Shodan với các bộ lọc
/shodan sub <domain>            : Tìm kiếm subdomain trên Shodan
/shodan dti <domain1,domain2>   : Domains to IP
/shodan itd <ip1,ip2>           : IP to Domains

* Ghi chú:
  - Shodan search có thể chậm do phải đợi máy chủ của Shodan phản hồi
```
4:36 PM

## 6.1. Thêm hoặc Xóa Shodan API Key

Để có thể thao tác được với các chức năng của Shodan, bạn cần phải thêm Shodan API Key. Sử dụng lệnh sau để thêm khóa mới cho Shodan:

```
/shodan add <key>
```




Hiện tại tính năng quản lý khóa của Shodan chỉ hỗ trợ một API Key cho một người dùng ở một thời điểm. Chưa hỗ trợ một người dùng với nhiều Shodan API Key.

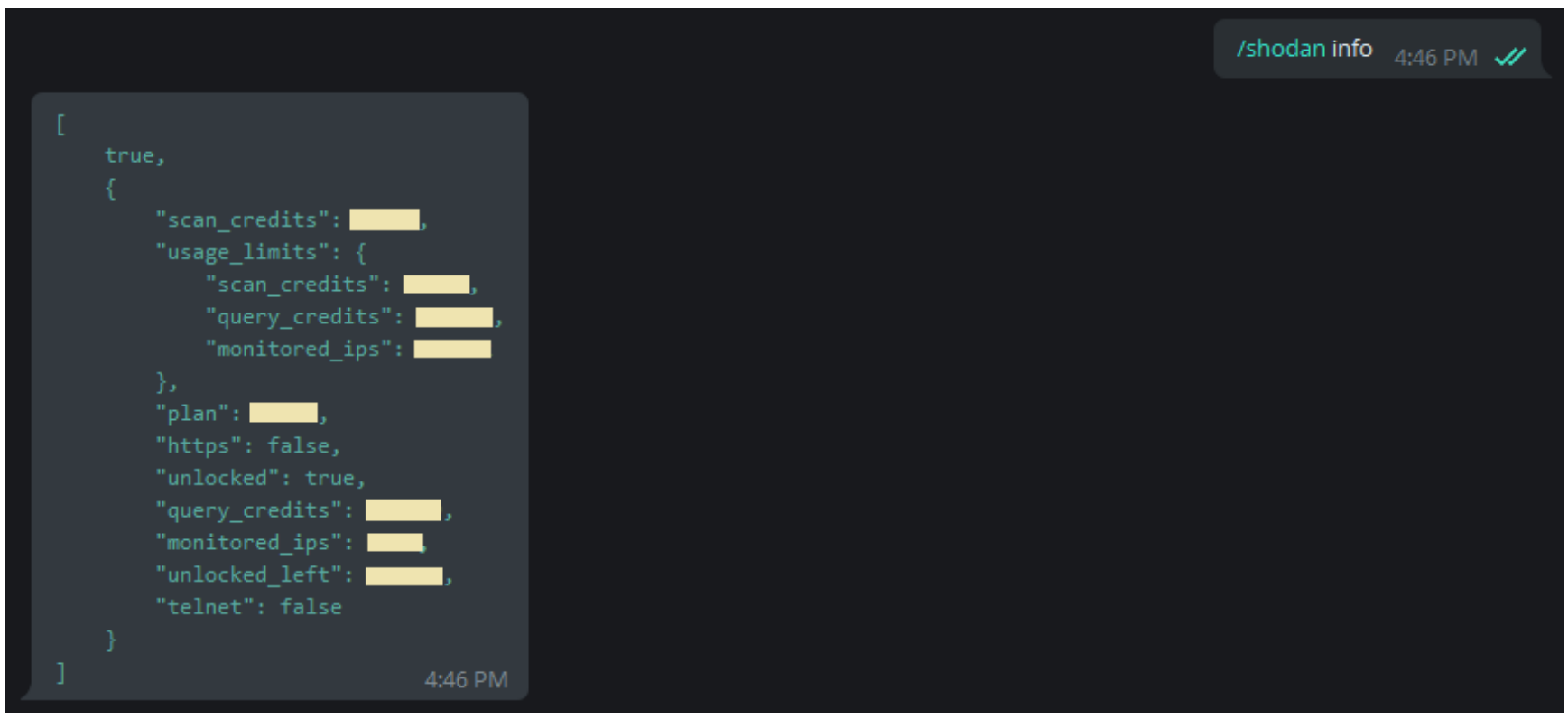
Để xóa Shodan Key đã thêm trước đó, sử dụng lệnh sau:

```
/shodan del
```


## 6.2. Kiểm tra thông tin Shodan API Key

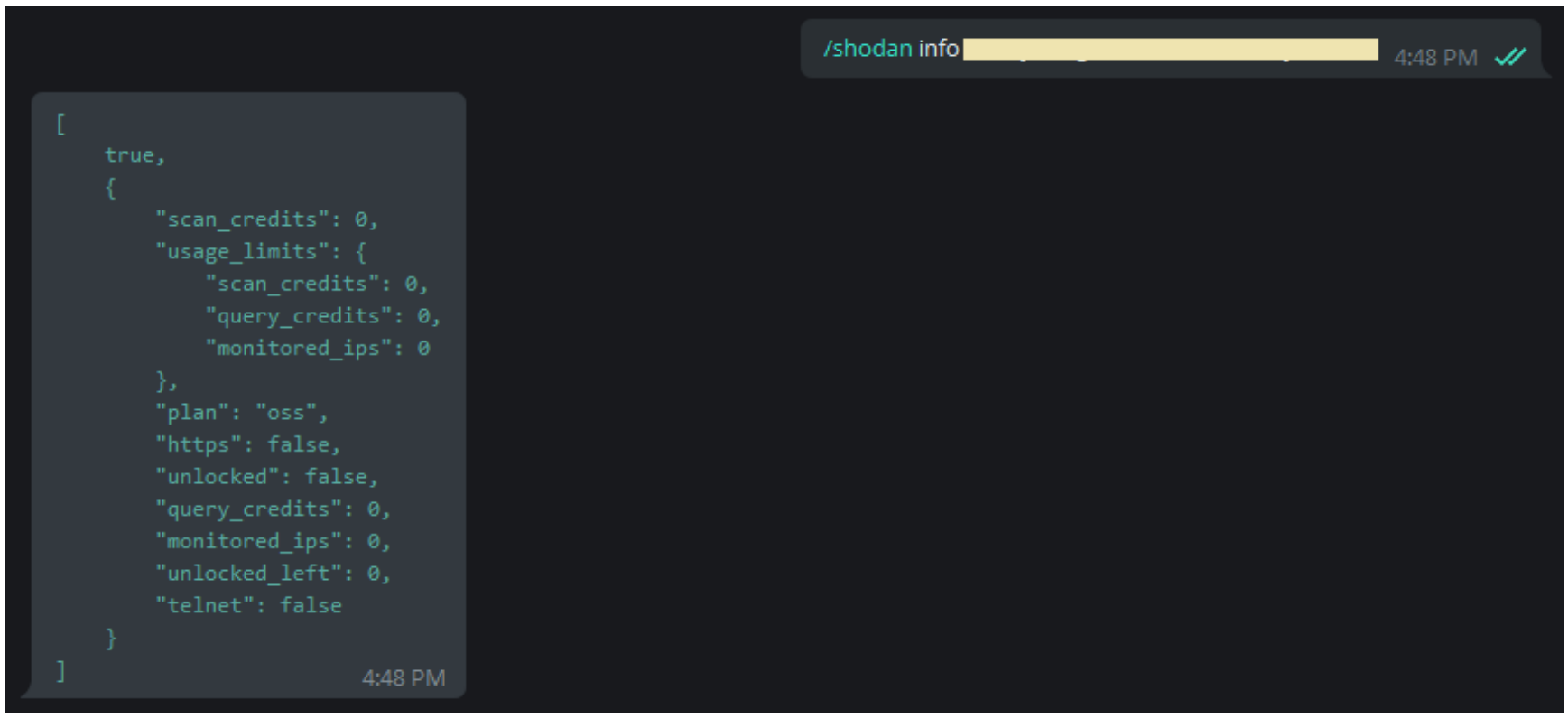
Để kiểm tra thông tin Shodan API Key đang sử dụng. Bạn gửi lệnh sau cho Bot:

```
/shodan info
```




Để kiểm tra thông tin một Shodan API Key bất kỳ. Bạn gửi lệnh sau cho Bot:

```
/shodan info <key>
```

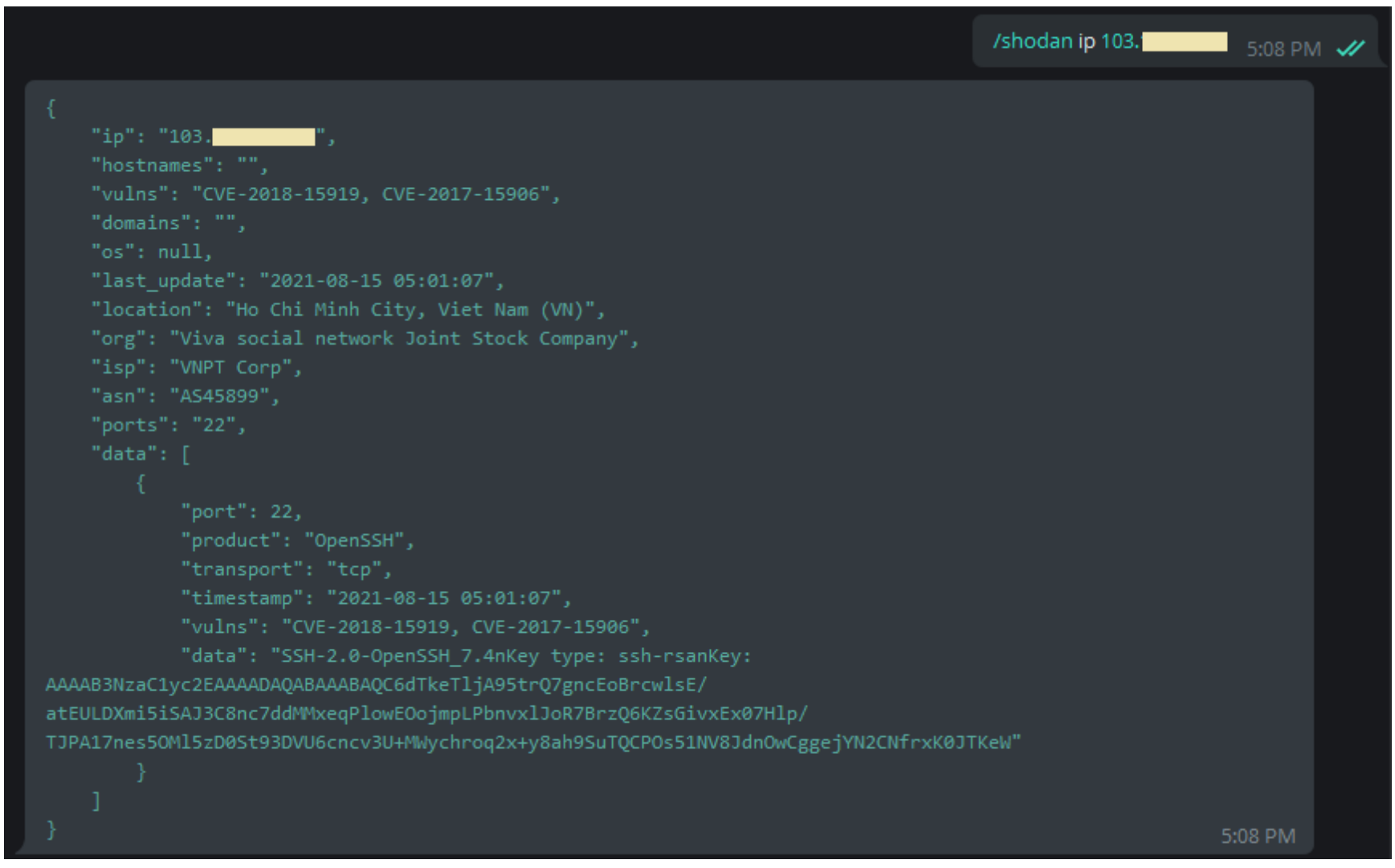


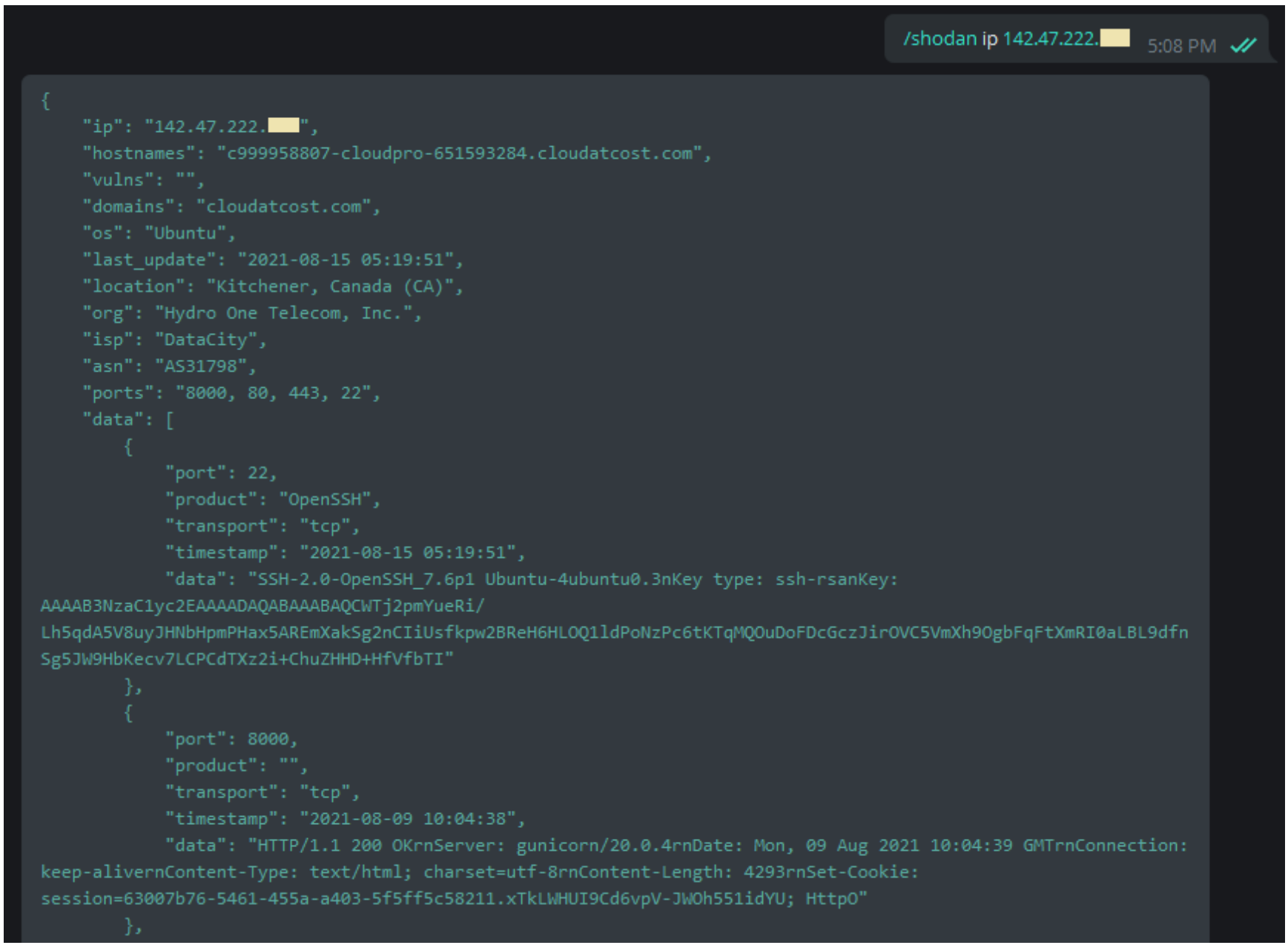

Tính năng này sẽ không yêu cầu người dùng Bot phải thiết lập Shodan Key trước đó.

## 6.3. Tìm kiếm một IP hay một Host trên Shodan

Trong nhiều tình huống cần kiểm tra nhanh một địa chỉ IP, có thể sử dụng các **Threat Intelligence Platform** như **Shodan** hoặc **VirusTotal**. Thông tin thu được từ các platform này có thể hữu ích trong nhiều bài toán, một số thông tin có được như: Nhà cung cấp, Quốc gia, các hostnames, domains liên quan, các cổng đang mở, thậm chí là lỗ hổng bảo mật của dịch vụ đang chạy,.v.v.. Để tìm kiếm một địa chỉ IP, bạn gửi lệnh sau cho Bot:

```
/shodan ip <ip-address>
```

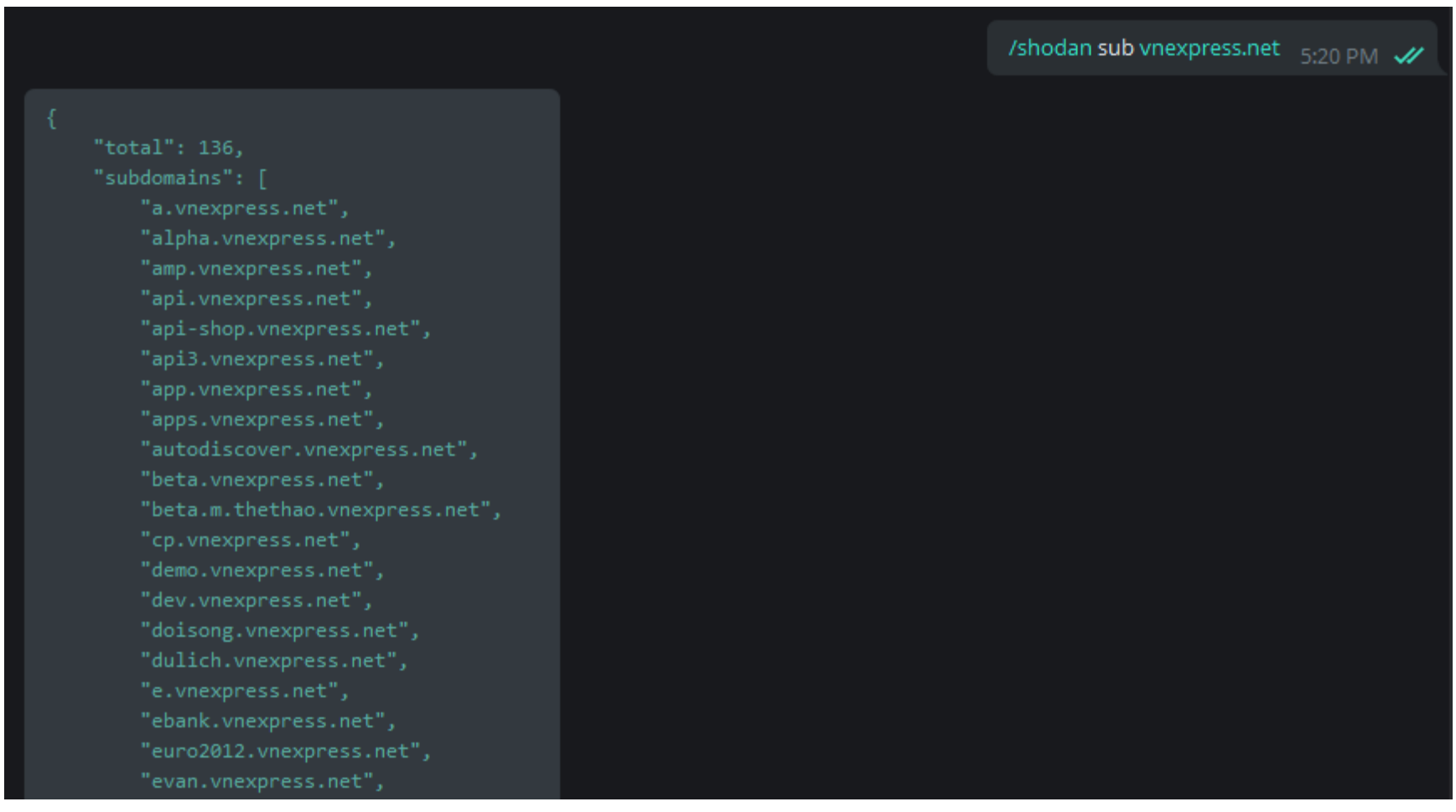





## 6.4. Tìm kiếm các SubDomain trên Shodan

Để tìm kiếm các SubDomain của một Domain. Bạn gửi lệnh sau cho Bot:

```
/shodan sub <domain>
```



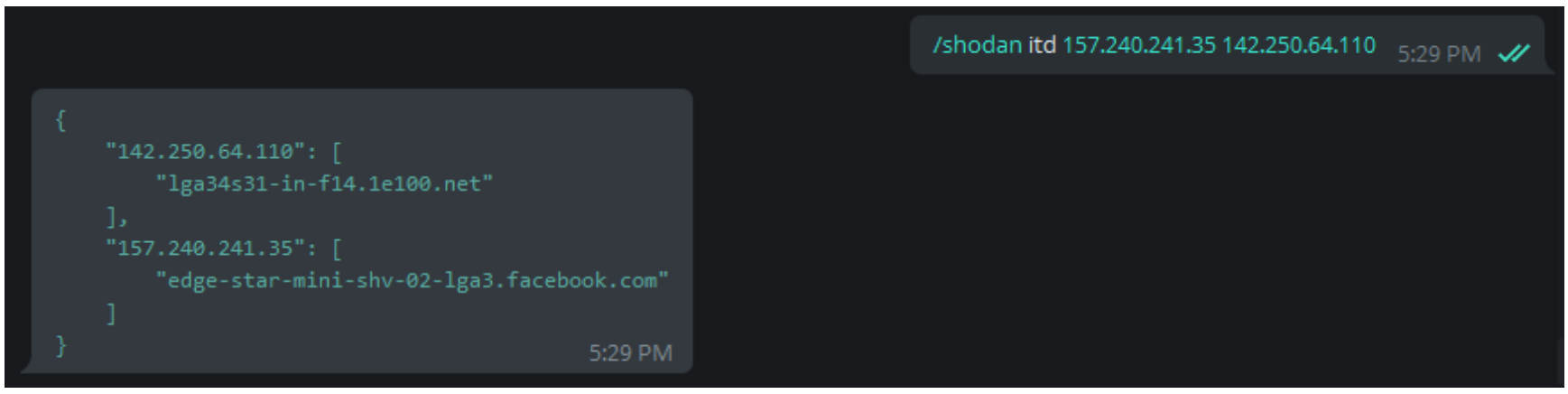

## 6.5. Domain to IP và IP to Domain

Để tìm kiếm địa chỉ IP của một hay nhiều Domain, bạn gửi lệnh sau cho Bot:

```
/shodan dti <domain1,domain2>
```


Để tìm kiếm xem có domain nào đang sử dụng địa chỉ IP đã biết, bạn gửi lệnh sau cho Bot:

```
/shodan itd <ip1,ip2>
```




## 6.6. Tìm kiếm nâng cao với các bộ lọc trên Shodan

Đây là tính năng rất mạnh của Shodan Search Engine. Bot hiện tại đã hỗ trợ bạn gửi các truy vấn (query) kèm các bộ lọc để tìm kiếm trên Shodan. Một số lưu ý như sau khi gửi truy vấn cho Bot:

- Càng sử dụng nhiều bộ lọc (Filter) thì càng cho nhiều kết quả chính xác. Nên sử dụng
- Tính năng này sẽ mất nhiều thời gian do phải đợi máy chủ của Shodan phản hồi. Trong lúc đợi, không nên thao tác gì tránh Bot quá tải
- **KHÔNG** nên chỉ sử dụng **MỘT** bộ lọc chung chung. Ví dụ: `product:Apache`, `port:22`,.. vì khi đó Shodan sẽ tìm kiếm rất lâu, mất thời gian đợi phản hồi và dữ liệu trả về sẽ cực lớn (Tất nhiên đã có limit theo mặc định nhưng sẽ phải đợi rất lâu). Có thể dẫn đến Time Out.
- NÊN kết hợp nhiều bộ lọc để giảm tải cũng như giảm thời gian chờ đợi. Ví dụ: `product:Apache port:80 country:VN`
- Các kết quả trả về từ Shodan rất dài dòng và nhiều, kết quả Bot hiển thị là đã được lược bỏ và chỉ lấy những thông tin tổng quát.

Một số tài liệu tham khảo khi sử dụng tính năng Search nâng cao:

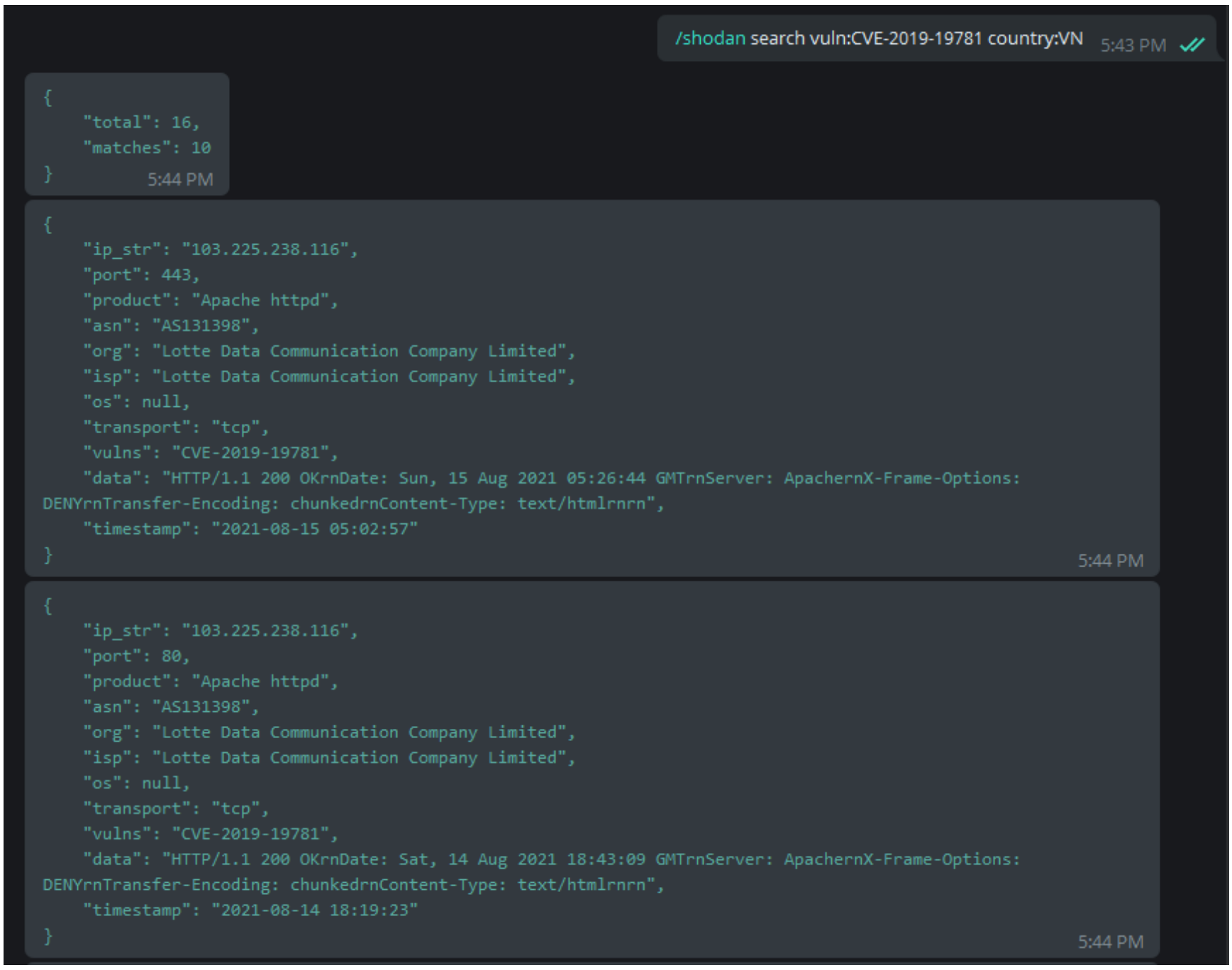
1. Filter Reference: https://www.shodan.io/search/filters
2. Search Query Examples: https://www.shodan.io/search/examples
3. Facet Analysis: https://beta.shodan.io/search/facet

Để sử dụng tính năng tìm kiếm nâng cao với Shodan. Bạn gửi lệnh sau cho Bot:

```
/shodan search <query>
```

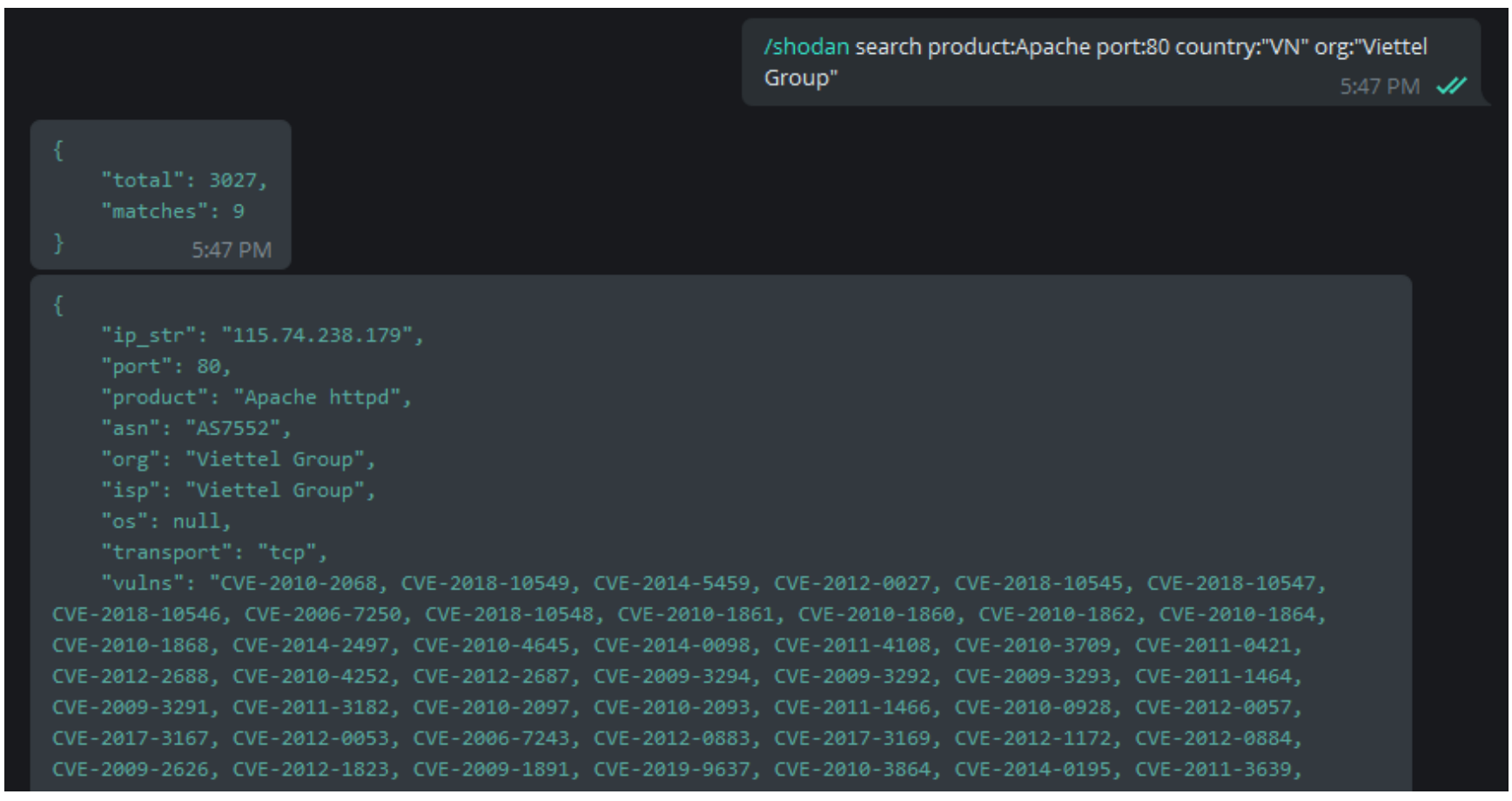
**Demo 1:** Tìm kiếm các máy chủ tồn tại lỗ hổng bảo mật có định danh: CVE-2019-19781 tại Việt Nam.

```
/shodan search vuln:CVE-2019-19781 country:VN
```




**Demo 2:** Tìm kiếm các máy chủ chạy Apache trên cổng 80, của nhà mạng Viettel

```
/shodan search product:Apache port:80 country:"VN" org:"Viettel Group"
```



```
{
    "ip_str": "125.212.221.202",
    "port": 80,
    "product": "Apache httpd",
    "asn": "AS7552",
    "org": "Viettel Group",
    "isp": "Viettel Group",
    "os": null,
    "transport": "tcp",
    "data": "HTTP/1.1 200 OKrnAccept-Ranges: bytesrnContent-Type: text/htmlrnDate: Sun, 15 Aug 2021 10:25:40
GMTrnEtag: "2c-5af0ba0bef338"rnLast-Modified: Fri, 11 Sep 2020 15:49:19 GMTrnServer: Apache/2rnVary: User-
AgentrnContent-Length: 273rnrn",
    "timestamp": "2021-08-15 10:28:27"
}
```
5:47 PM

```
{
    "ip_str": "171.249.40.197",
    "port": 80,
    "product": "Apache httpd",
    "asn": "AS7552",
    "org": "Viettel Group",
    "isp": "Viettel Group",
    "os": null,
    "transport": "tcp",
    "vulns": "CVE-2017-7679, CVE-2016-2182, CVE-2016-2178, CVE-2016-2179, CVE-2018-1312, CVE-2016-2177,
CVE-2016-8612, CVE-2016-0798, CVE-2016-6303, CVE-2016-6302, CVE-2017-7668, CVE-2016-6306, CVE-2016-6304,
CVE-2017-3167, CVE-2016-0702, CVE-2016-2181, CVE-2016-2180, CVE-2016-2183, CVE-2015-3197, CVE-2017-3169,
CVE-2016-0800, CVE-2016-2105, CVE-2016-4975, CVE-2016-2842, CVE-2016-0799, CVE-2016-0705, CVE-2015-3194,
CVE-2016-0797, CVE-2015-3195",
    "domains": "viettel.vn",
    "data": "HTTP/1.1 200 OKrnDate: Sun, 15 Aug 2021 10:27:24 GMTrnServer: Apache/2.2.31 (Win32) mod_ssl/2.2.31
OpenSSL/1.0.1prnX-Powered-By: ZendServer 8.5.1rnSet-Cookie: PHPSESSID=agv45vofu4218qfvqe6kh1vse3; expires=Sun,
15-Aug-2021 14:27:24 GMT; Max-Age=14400; path=",
    "timestamp": "2021-08-15 10:27:24",
    "hostnames": "dynamic-ip-adsl.viettel.vn"
}
```
5:47 PM

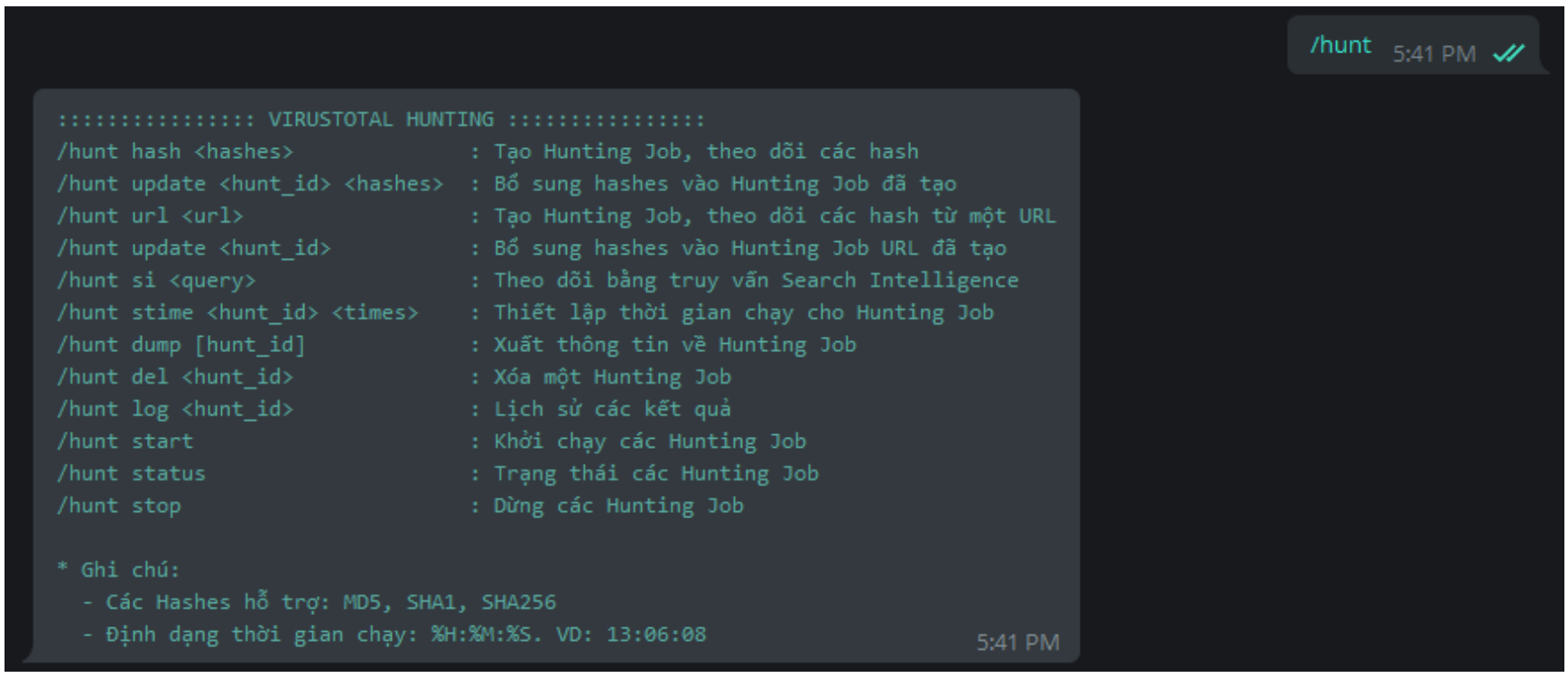

# 7. VT Hunting

Threat Intelligence Bot đã có tính năng mới cho phép người dùng thực hiện: Lập lịch, theo dõi các hash, search intelligence,.v.v.. theo định kỳ. Và nhận thông báo khi có kết quả từ Bot. Đây là một tính năng mới thay thế cho tính năng VT HUNTING (Retrohunt, Livehunt) có sẵn của VirusTotal, nó khắc phục được các nhược điểm sau:

- Cảnh báo trực tiếp đến người dùng qua Telegram thay vì qua Email vì dễ bị đánh vào Spam.
- Không bị lộ lọt các Hunting Job với người khác. Vì một Private API key có thể đang được sử dụng bởi nhiều người, những người này có thể biết đc API Key này đang thiết lập các Hunting Job nào, dẫn đến việc có thể sẽ bị khóa API Key.
- Linh động và tùy biến cao: Nhiều cách thức Monitor (Hash, Query), Lập lịch theo thời gian tùy ý,.v.v...

Để nhận Menu trợ giúp từ Bot cho tính năng VT Hunting. Bạn gửi lệnh sau cho Bot:

```
/hunt
# Hoặc
/hunt help
```



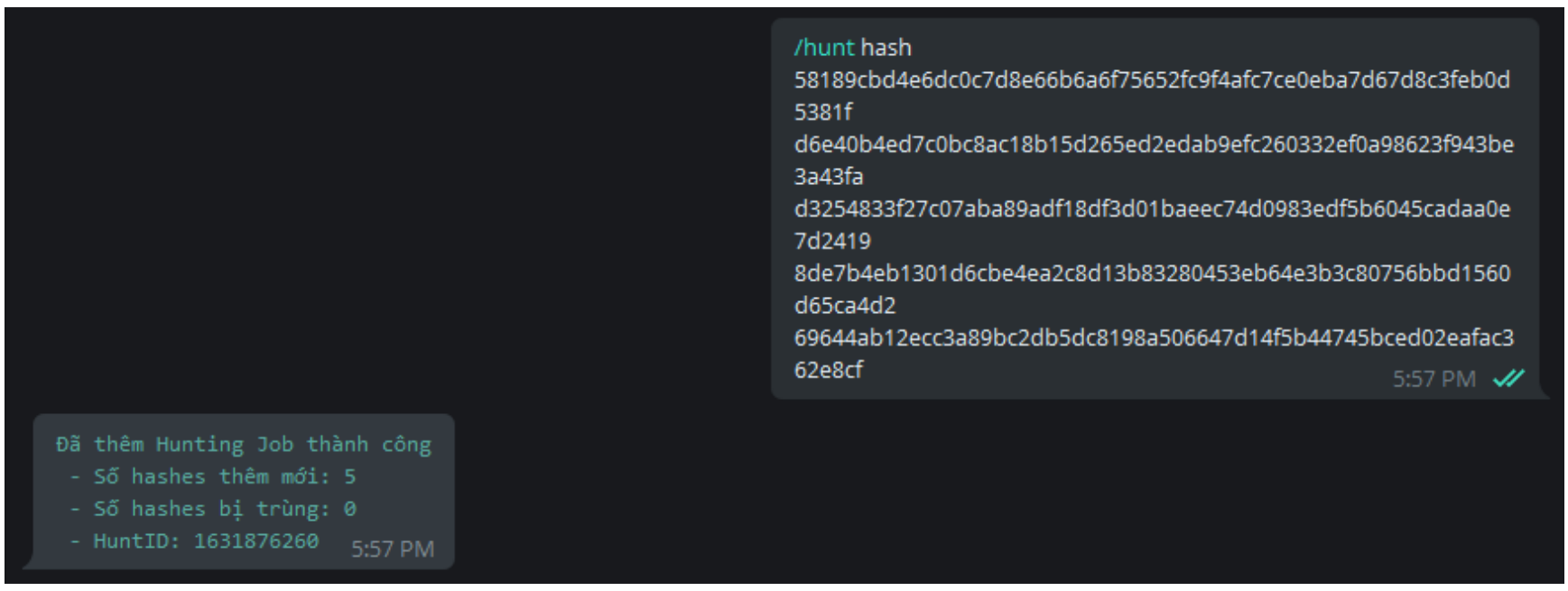

## 7.1. Khởi tạo các Hunting Job

Hiện tại chức năng VT Hunting hỗ trợ tạo **03** loại Hunting Job sau:

1. **Hashes Hunting Job:** Tạo Job với các Hashes cần theo dõi một cách thủ công. Các Hashes ngăn cách nhau bằng dấu `khoảng trắng` hoặc `xuống dòng`
2. **URL Hunting Job:** Tạo Job theo dõi một URL. URL này chứa các Hashes và số lượng các Hashes có thể thay đổi theo thời gian
3. **Search Query Hunting Job:** Tạo Job thực hiện truy vấn nâng cao (Search Intelligence). Tính hiệu quả phụ thuộc vào độ sáng tạo của người viết câu truy vấn lên VirusTotal.

### 👷 Tạo Hash Hunting Job

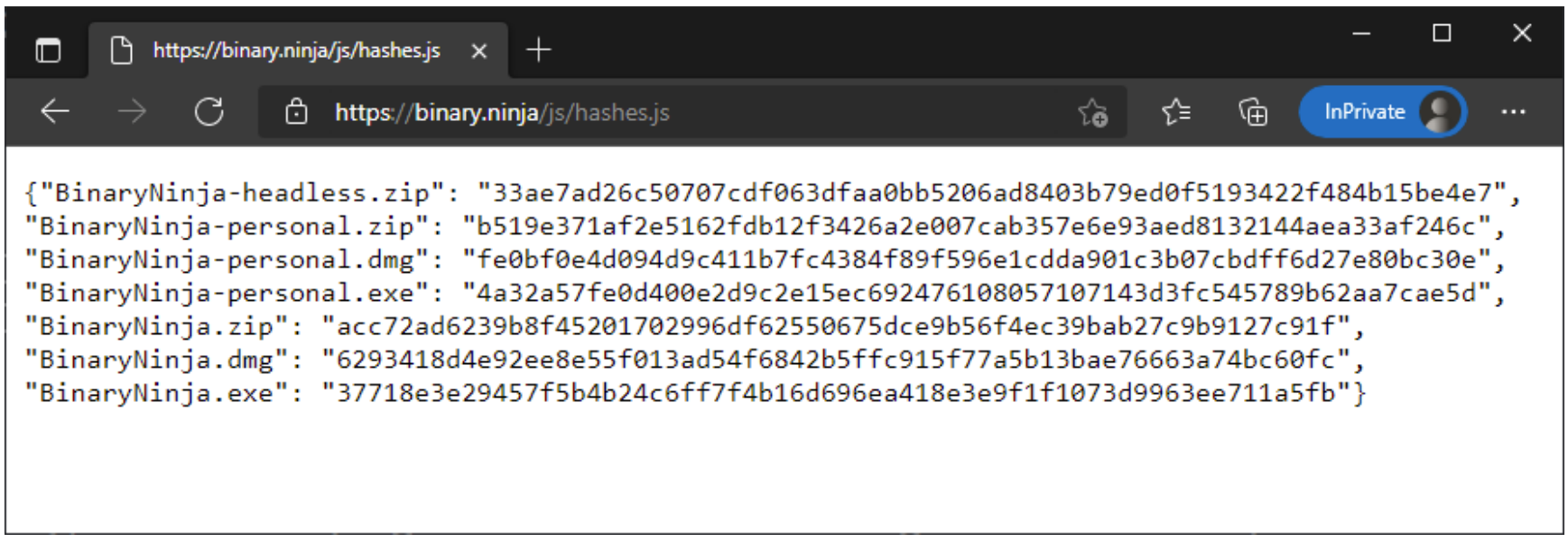
```
/hunt hash <hash1 hash2 hash3>
```

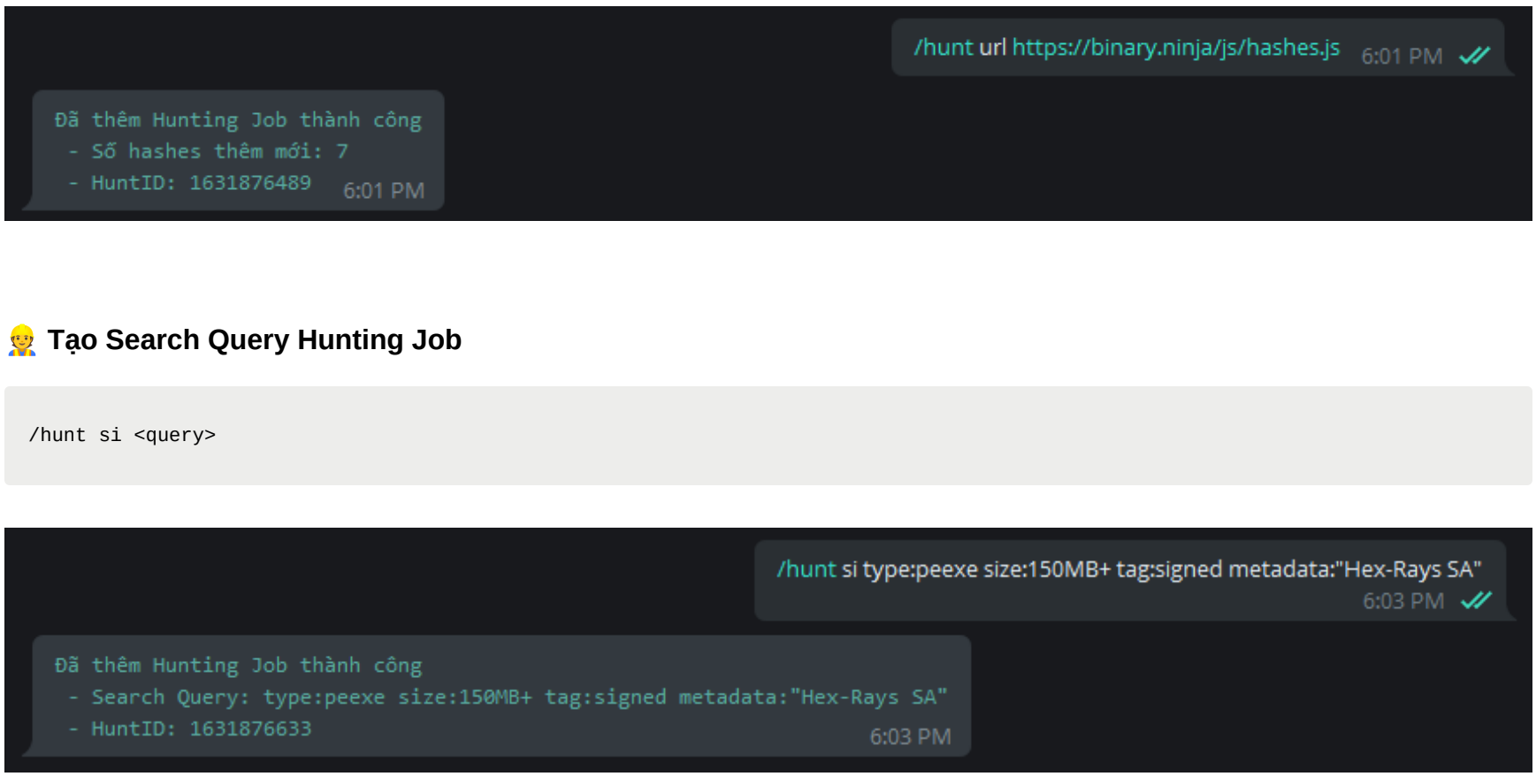



### 👷 Tạo URL Hunting Job

```
/hunt url <url>
```

Giả sử ta cần Monitor một URL chứa các hash như sau: https://binary.ninja/js/hashes.js




### 👷 Tạo Search Query Hunting Job

```
/hunt si <query>
```

### 🔍 Bây giờ để xem lại các Hunting Job bạn đã tạo trước đó. Gửi lệnh sau cho Bot:

```
/hunt dump
# Hoặc
/hunt dump <hunt_id>
```

/hunt dump 6:08 PM


```
[
    {
        "id": 1631876260,
        "type": "hash",
        "create_time": "2021-09-17 17:57:40",
        "status": "OFF",
        "run_at": "",
        "num_of_hashes": 5,
        "content": "['...']",
        "source": "manual",
        "last_run": "1970-01-01 07:00:00"
    },
    {
        "id": 1631876489,
        "type": "url",
        "create_time": "2021-09-17 18:01:29",
        "status": "OFF",
        "run_at": "",
        "num_of_hashes": 7,
        "content": "['...']",
        "source": "https://binary.ninja/js/hashes.js",
        "last_run": "1970-01-01 07:00:00"
    },
    {
        "id": 1631876633,
        "type": "query",
        "create_time": "2021-09-17 18:03:53",
        "status": "OFF",
        "run_at": "",
        "num_of_hashes": 0,
        "content": "type:peexe size:150MB+ tag:signed metadata:"Hex-Rays SA"",
        "source": "manual",
        "last_run": "1970-01-01 07:00:00"
    }
]
```


6:08 PM

Với lệnh `/hunt dump` chúng ta chỉ có thể xem cấu hình ngắn gọn của các Hunting Job đã tạo. Để xem cấu hình chi tiết hơn. Sử dụng lệnh: `/hunt dump <hunt_id>`

/hunt dump 1631876489 6:13 PM


```
{
    "id": 1631876489,
    "type": "url",
    "create_time": "2021-09-17 18:01:29",
    "status": "OFF",
    "run_at": "",
    "num_of_hashes": 7,
    "content": [
        "4a32a57fe0d400e2d9c2e15ec692476108057107143d3fc545789b62aa7cae5d",
        "33ae7ad26c50707cdf063dfaa0bb5206ad8403b79ed0f5193422f484b15be4e7",
        "37718e3e29457f5b4b24c6ff7f4b16d696ea418e3e9f1f1073d9963ee711a5fb",
        "fe0bf0e4d094d9c411b7fc4384f89f596e1cdda901c3b07cbdff6d27e80bc30e",
        "6293418d4e92ee8e55f013ad54f6842b5ffc915f77a5b13bae76663a74bc60fc",
        "acc72ad6239b8f45201702996df62550675dce9b56f4ec39bab27c9b9127c91f",
        "b519e371af2e5162fdb12f3426a2e007cab357e6e93aed8132144aea33af246c"
    ],
    "source": "https://binary.ninja/js/hashes.js",
    "last_run": "1970-01-01 07:00:00"
}
```


6:13 PM

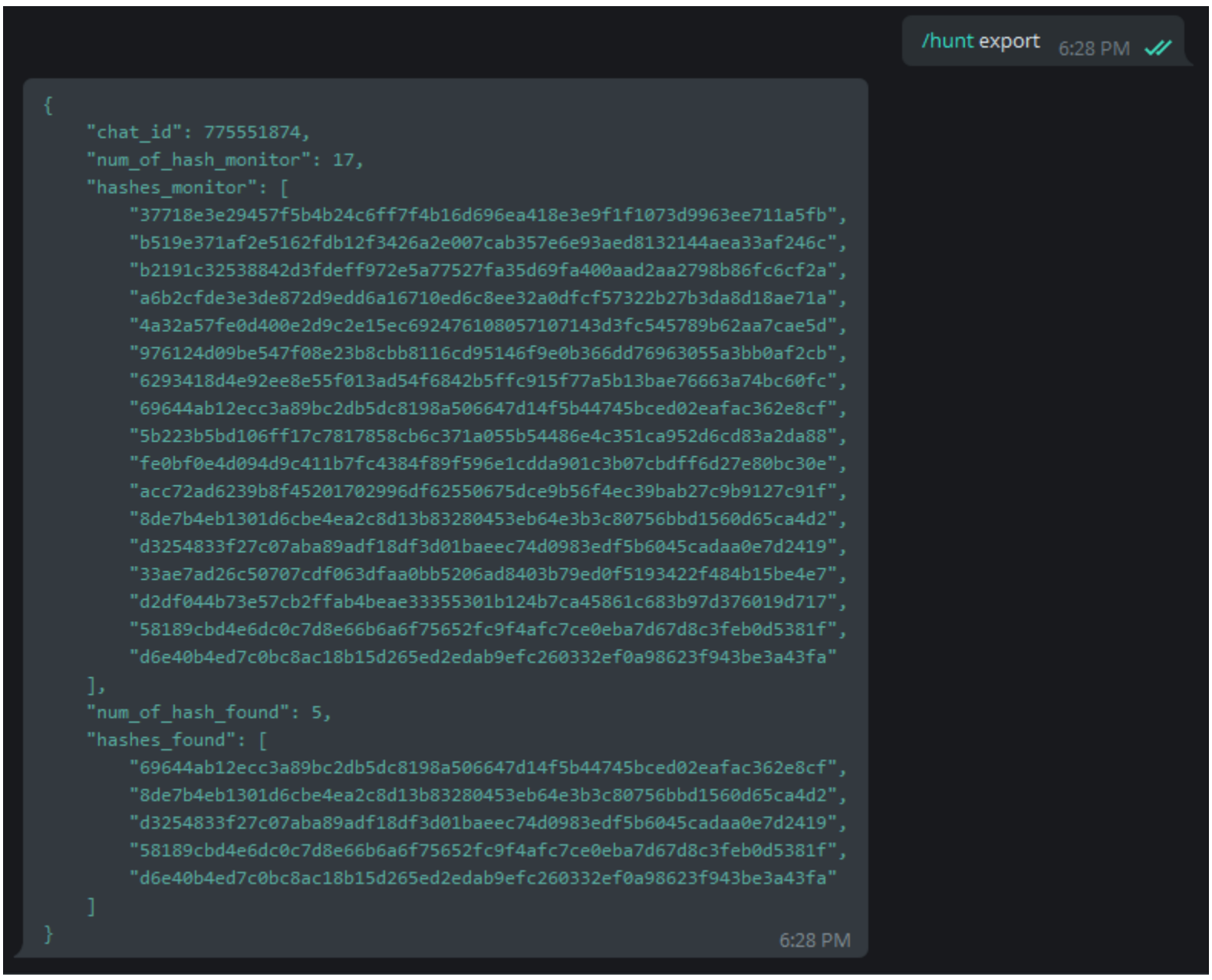
**Giải thích một vài thông số:**

- `id`: HuntID của một Hunting Job, con số này là duy nhất. Sinh tự động và trả về cho người dùng sau khi Hunting Job được tạo
- `type`: Hunting Job Type: hash, url hoặc query
- `create_time`: Thời gian Hunting Job được tạo
- `status`: Mặc định trạng thái của Hunting Job là `OFF` sau khi được tạo. Khi thiết lập thời gian chạy thì nó sẽ chuyển thành `ON`.

- `run_at`: Thời gian chạy trong ngày của Hunting Job. Khi chưa thiết lập thì giá trị này sẽ là trống.
- `num_of_hashes` và `content`: Số lượng các hash và nội dung cụ thể các hashes đã thêm.
- `source`: Cho biết Hunting Job này được tạo thủ công (manual) hay được lấy từ một URL
- `last_run`: Thời điểm lần cuối cùng Hunting Job này chạy. Mặc định giá trị `1970-01-01 07:00:00` cho biết Job này chưa được chạy lần nào.

Trường hợp muốn xem lại tất cả các hashes đang theo dõi và các hashes đã tìm thấy mà không cần nhập vào **HuntID**. Bạn gửi lệnh sau cho Bot:

```
/hunt export
```




**Trong đó:**

- `hashes_monitor`: Số hashes đang theo dõi trên VT
- `hashes_found`: Số hashes đã tìm thấy trên VT

Nếu số lượng hashes quá nhiều. Bot sẽ export sang dạng tệp tin `*.json` và gửi cho bạn.

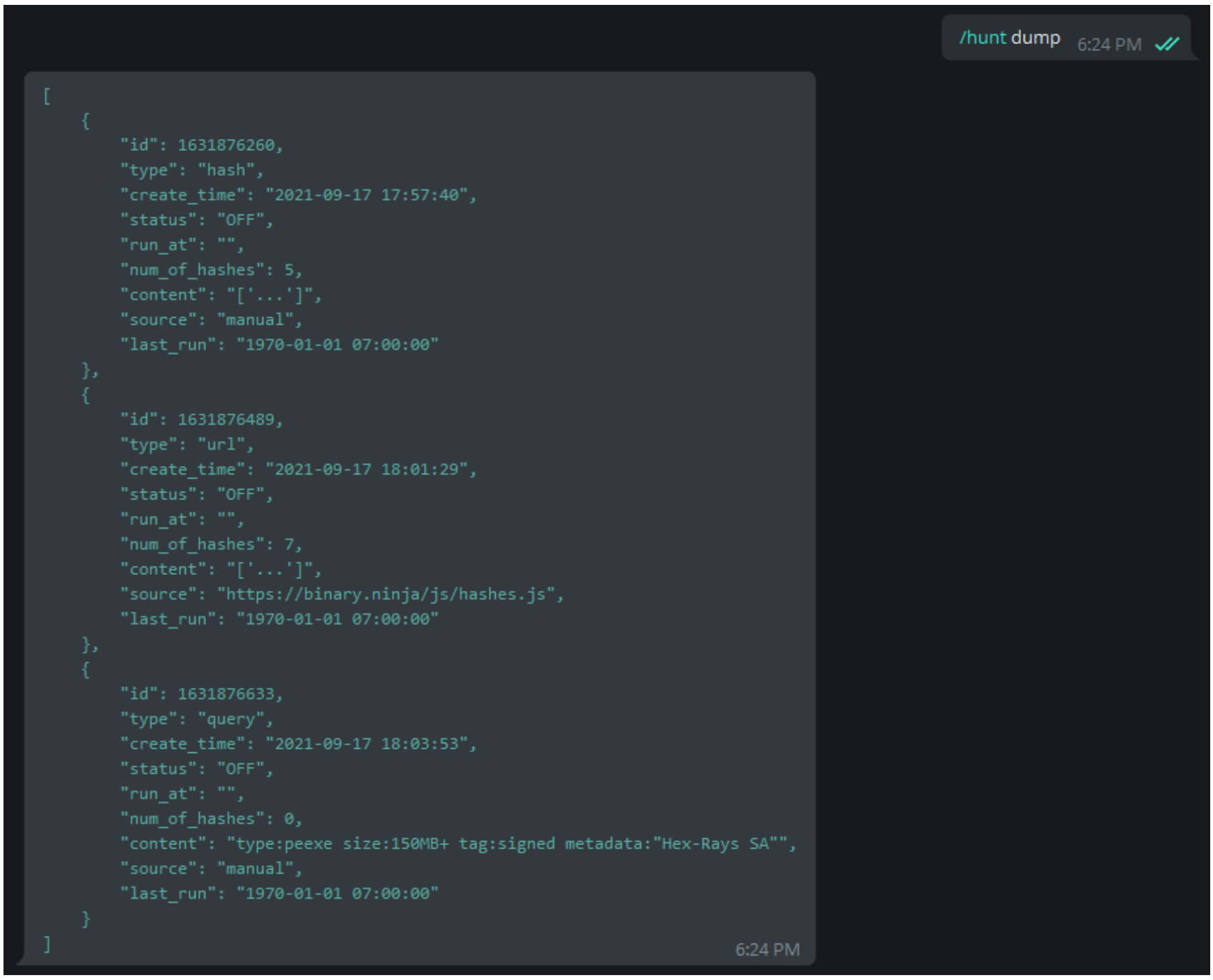
Và cuối cùng để xóa một Hunting Job. Bạn gửi lệnh sau cho Bot:

```
/hunt del <hunt_id>
```


## 7.2. Cấu hình và khởi chạy các Hunting Job

### 7.2.1 Cấu hình (Lập lịch) thời gian chạy cho các Hunting Job

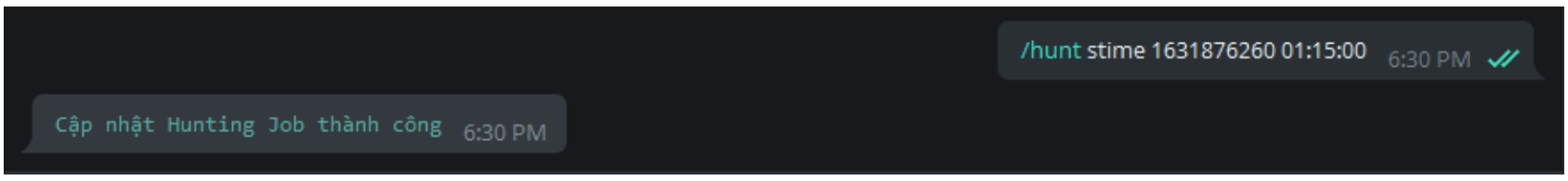
Trước tiên, ta xuất thông tin các Hunting Job đã tạo, xem cấu hình hiện tại và cũng để lấy HuntID của các Job.




#### ⏲️ Lập lịch chạy 01 lần mỗi ngày

```
/hunt stime <hunt_id> <time>
```

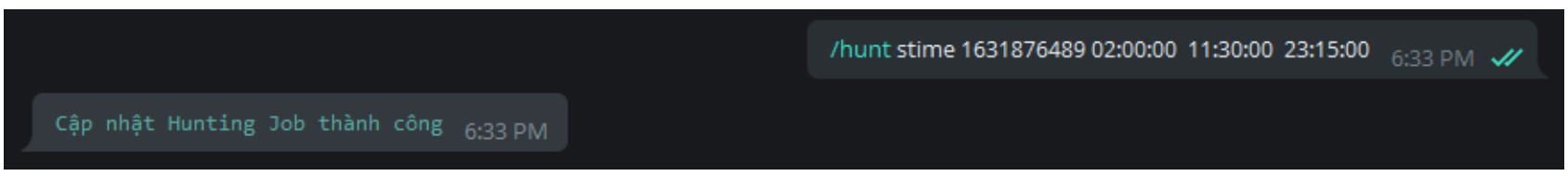
Demo: Đặt lịch chạy Hunting Job vào `01 giờ 15 phút` sáng sớm mỗi ngày.




#### ⏲️ Lập lịch chạy nhiều lần mỗi ngày

```
/hunt stime <hunt_id> <time1 time2 time3>
```

Demo: Đặt lịch chạy Hungting Job vào lúc: `02 giờ` sáng, `11 giờ 30 phút` trưa và `23 giờ 15` phút tối của mỗi ngày.



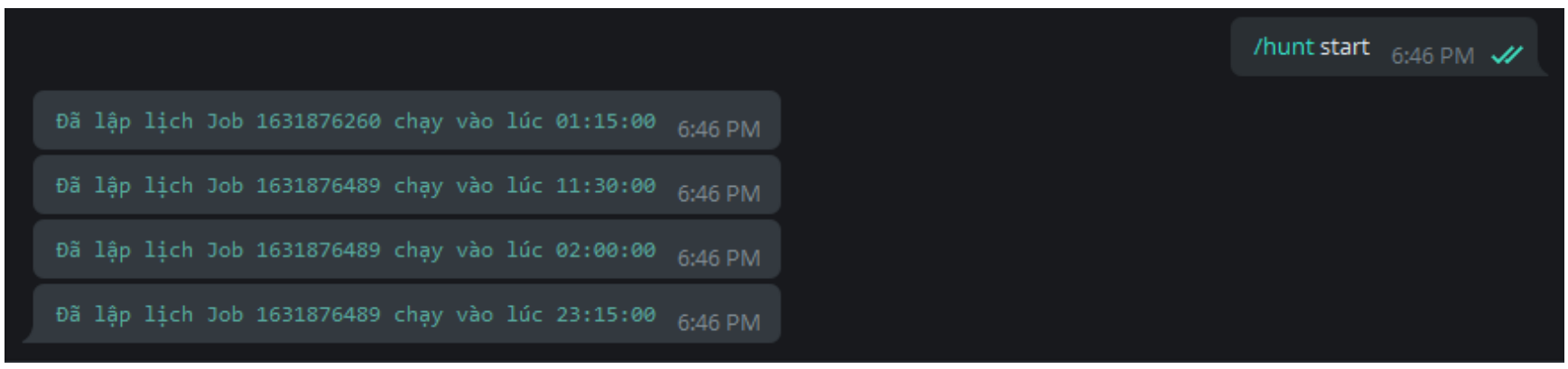
Cùng xem lại các mốc thời gian đã cấu hình cho Hunting Job: Để ý thông số cấu hình: `run_at` đã được thay đổi.


### 7.2.2. Khởi chạy các Hungtin Job

Khi đã hoàn tất việc cấu hình các Hunting Job theo ý muốn. Bạn có thể bắt đầu cho chạy các Hungtin Job này. Ngoài ra, Bot cũng hỗ trợ người dùng kiểm tra, theo dõi các Hunting Job đang chạy, đồng thời có thể buộc dừng các Hunting Job này theo yêu cầu của người dùng.

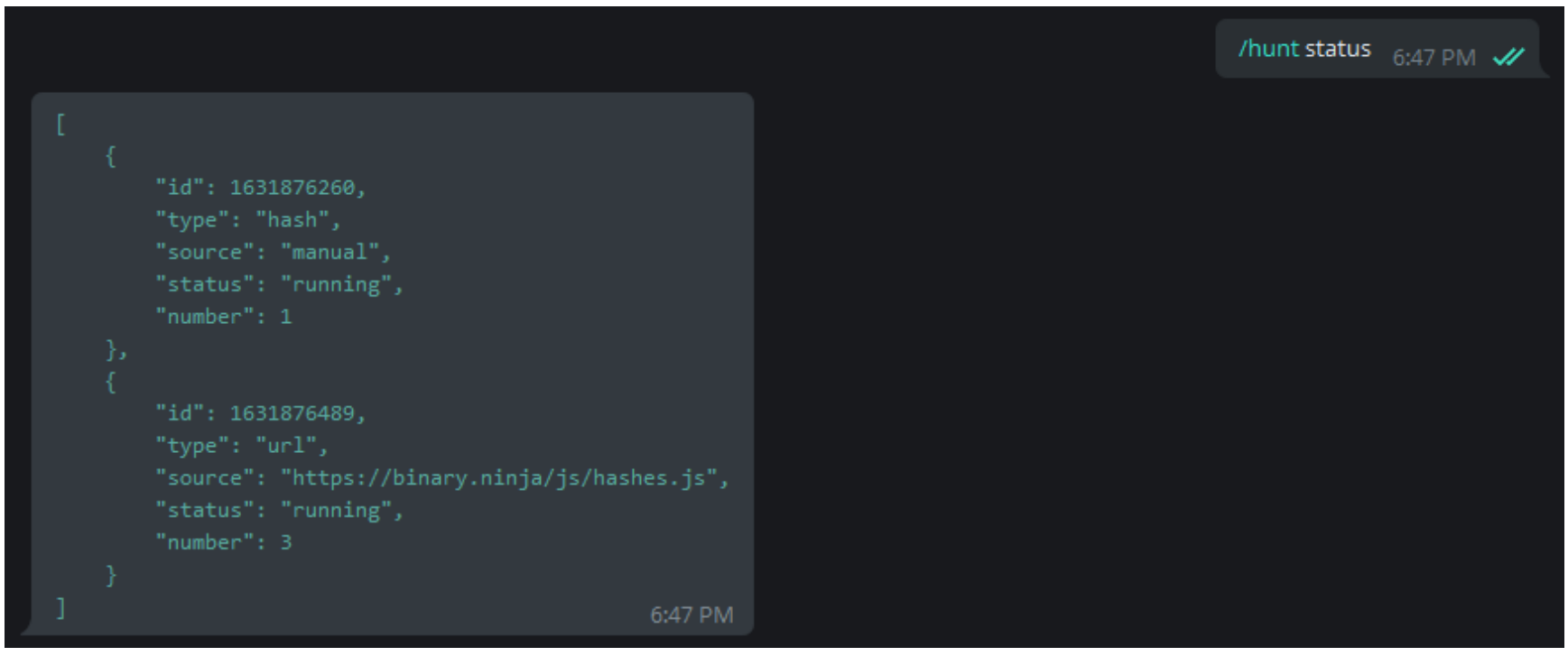
#### 🎛 Khởi chạy các Hunting Job - START

```
/hunt start
```




#### 🎛 Kiểm tra trạng thái các Hunting Job - STATUS

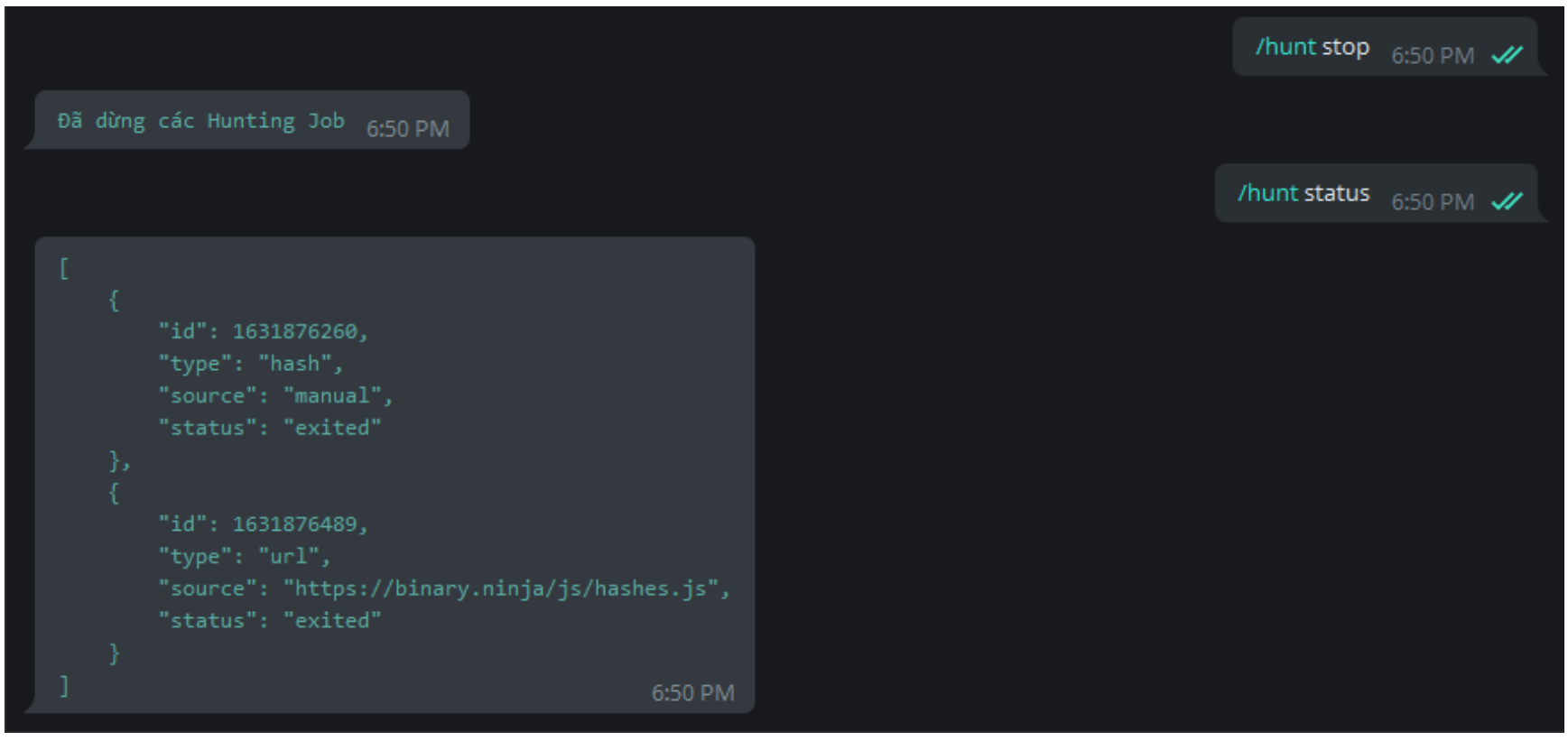
```
/hunt status
```




Với Hunting Job có ID `1631876489`. Do chúng ta trước đó đã lập lịch chạy ở các khoảng thời gian `11:30:00`, `02:00:00` và `23:15:00`. Nên khi kiểm tra với `/hunt status` sẽ thấy xuất hiện thông số `number` trả về `3`.

### 🎛️ Buộc dừng các Hunting Job - STOP

```
/hunt stop
```



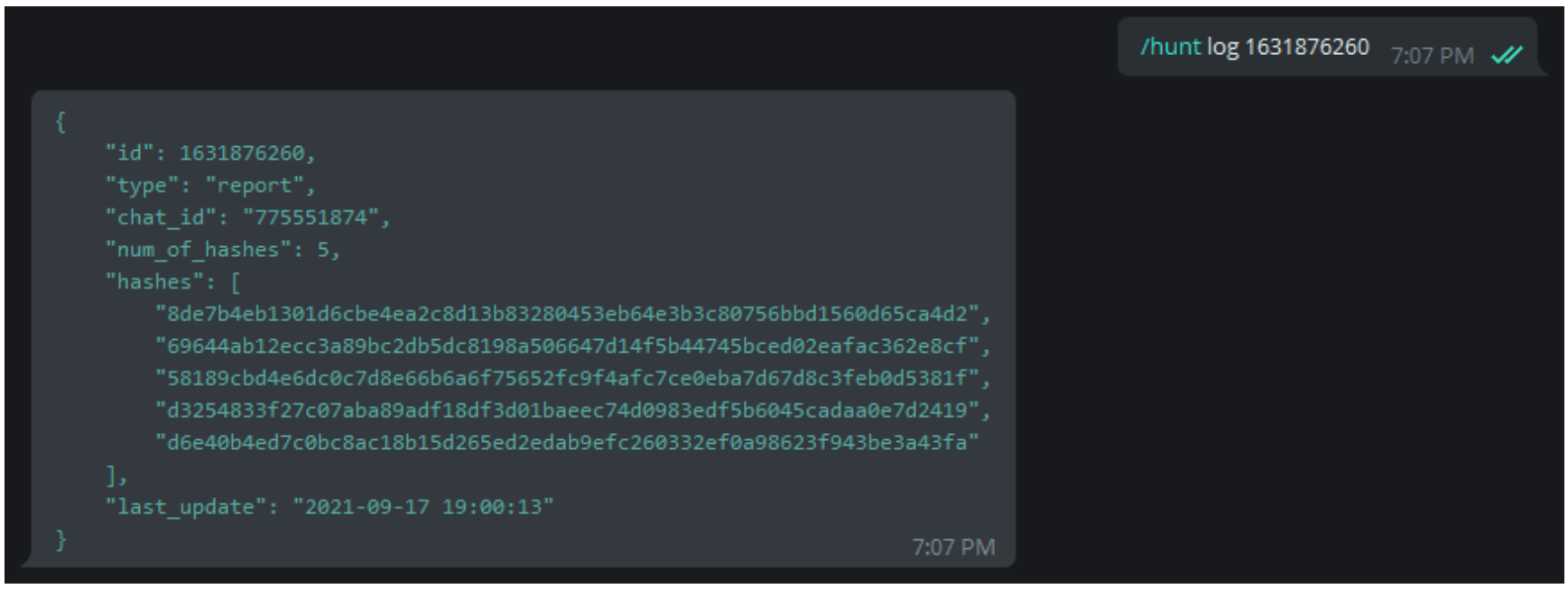

### 🍰 Nhận kết quả sau khi chạy của Hunting Job

Sau khi đã lập lịch các Hunting Job chạy vào các khoảng thời gian theo ý muốn của bạn. Công việc còn lại lúc này chỉ là chờ đợi. Giả sử bạn đặt lịch cho Job chạy vào lúc đêm, khi đó bạn đã đi ngủ. Khi đến thời điểm đã lập lịch, Bot chạy lấy kết quả các hash nó tìm thấy và nếu có nó sẽ gửi tin nhắn cho bạn.

Lưu ý rằng, các hashes sẽ được lưu vào Cơ sở dữ liệu để thuận tiện cho việc tra cứu sau này và các hash mà Bot đã tìm thấy nó sẽ không cảnh báo lại đến bạn ở các lần chạy vào hôm sau.


### 🍰 Kiểm tra lại kết quả của các lần chạy Hunting Job

```
/hunt log <hunt_id>
```

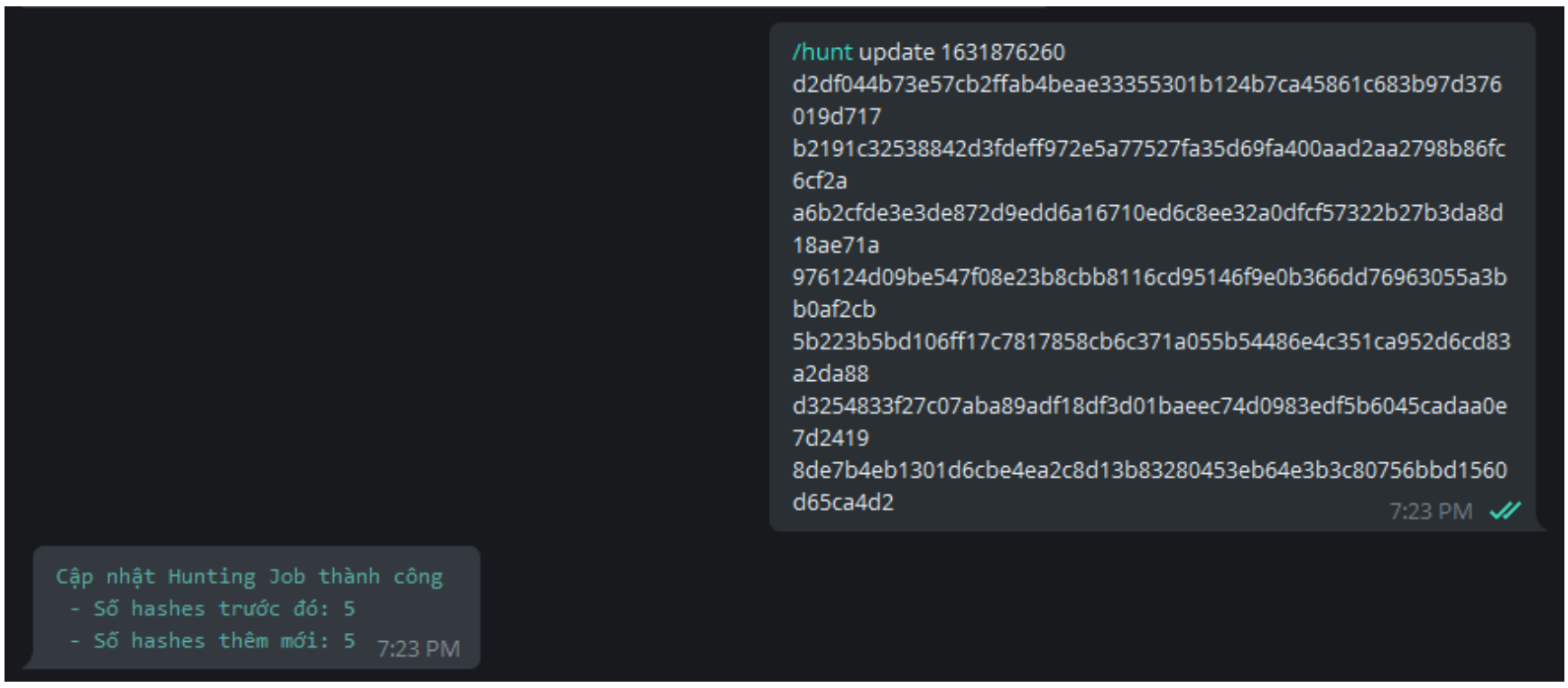



## 7.3. Cập nhật các thay đổi của Hunting Job

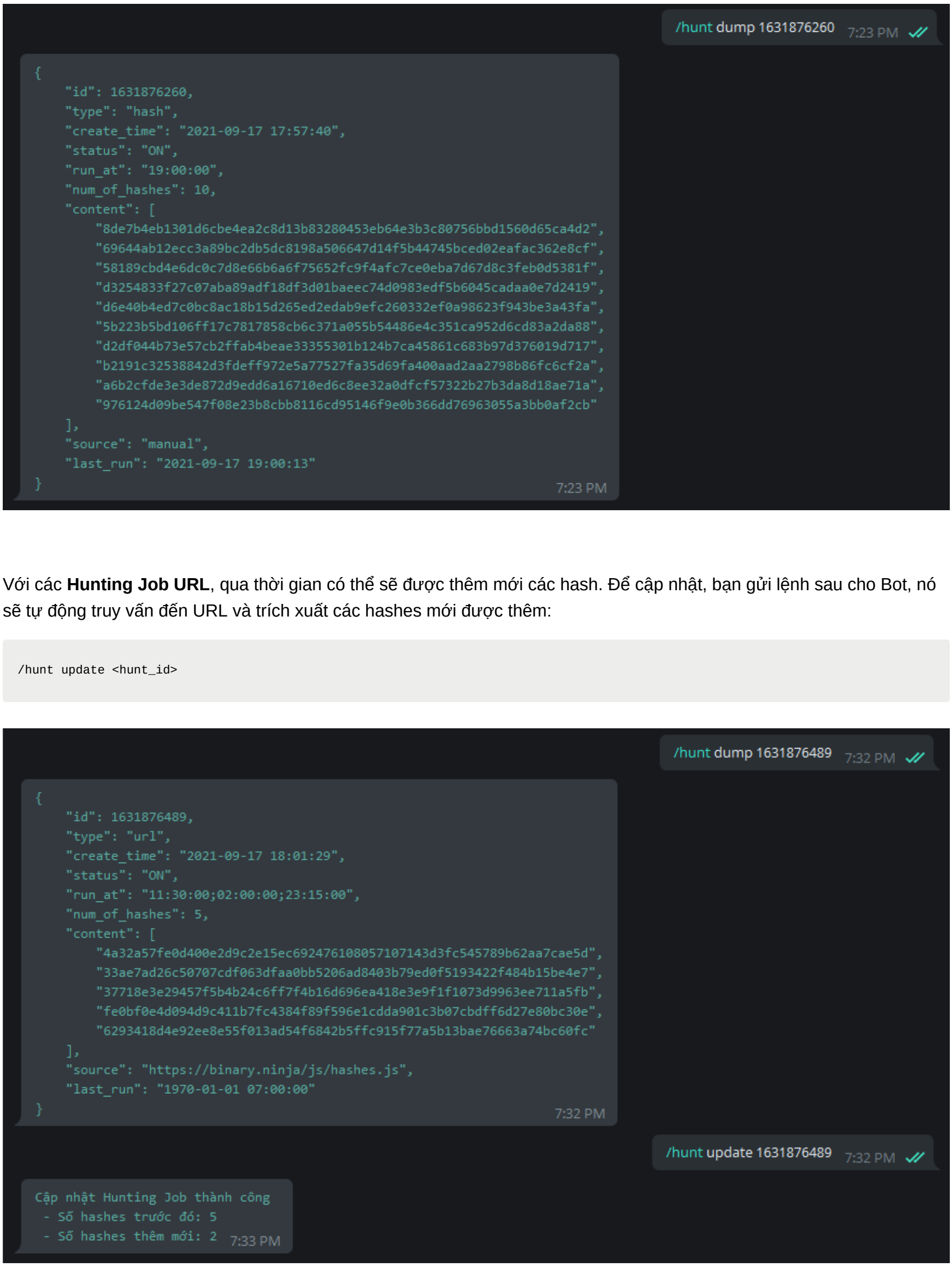
### 🔨 Cập nhật thêm các Hashes

Để cập nhật thêm các Hashes của một **Hunting Job Hash**. Bạn gửi lệnh sau cho Bot:

```
/hunt update <hunt_id> <hashes>
```




Hình trên cho thấy, tôi muốn cập nhật thêm `7 hash` mới vào một Hunting Job đã tạo trước đó, và trong số đó có `2 hash` đã tồn tại trước đó rồi. Vậy sẽ chỉ có `5 hash` mới được thêm.




Với các **Hunting Job URL**, qua thời gian có thể sẽ được thêm mới các hash. Để cập nhật, bạn gửi lệnh sau cho Bot, nó sẽ tự động truy vấn đến URL và trích xuất các hashes mới được thêm:

```
/hunt update <hunt_id>
```

/hunt dump 1631876489 7:33 PM


```
{
    "id": 1631876489,
    "type": "url",
    "create_time": "2021-09-17 18:01:29",
    "status": "ON",
    "run_at": "11:30:00;02:00:00;23:15:00",
    "num_of_hashes": 7,
    "content": [
        "6293418d4e92ee8e55f013ad54f6842b5ffc915f77a5b13bae76663a74bc60fc",
        "37718e3e29457f5b4b24c6ff7f4b16d696ea418e3e9f1f1073d9963ee711a5fb",
        "33ae7ad26c50707cdf063dfaa0bb5206ad8403b79ed0f5193422f484b15be4e7",
        "4a32a57fe0d400e2d9c2e15ec692476108057107143d3fc545789b62aa7cae5d",
        "fe0bf0e4d094d9c411b7fc4384f89f596e1cdda901c3b07cbdff6d27e80bc30e",
        "acc72ad6239b8f45201702996df62550675dce9b56f4ec39bab27c9b9127c91f",
        "b519e371af2e5162fdb12f3426a2e007cab357e6e93aed8132144aea33af246c"
    ],
    "source": "https://binary.ninja/js/hashes.js",
    "last_run": "1970-01-01 07:00:00"
}
```


7:33 PM

### 🔨 Cập nhật thời gian chạy của các Hunting Job

Để thay đổi thời gian chạy (lập lịch) của các Hunting Job. Bạn thực hiện tương tự như lúc thiết lập thời gian. Lúc này mốc thời gian mới bạn thiết lập sẽ ghi đè lên các mốc thời gian cũ. Cú pháp:

```
/hunt stime <hunt_id> <times>
```

Và cuối cùng để áp dụng các thay đổi. Bạn cần dừng các Hunting Job đang chạy sau đó khởi động lại chúng.

```
/hunt stop
/hunt start
```