INJECT 03

-------------------------------------------------------------------------------------------------------------------------

**Question 1**

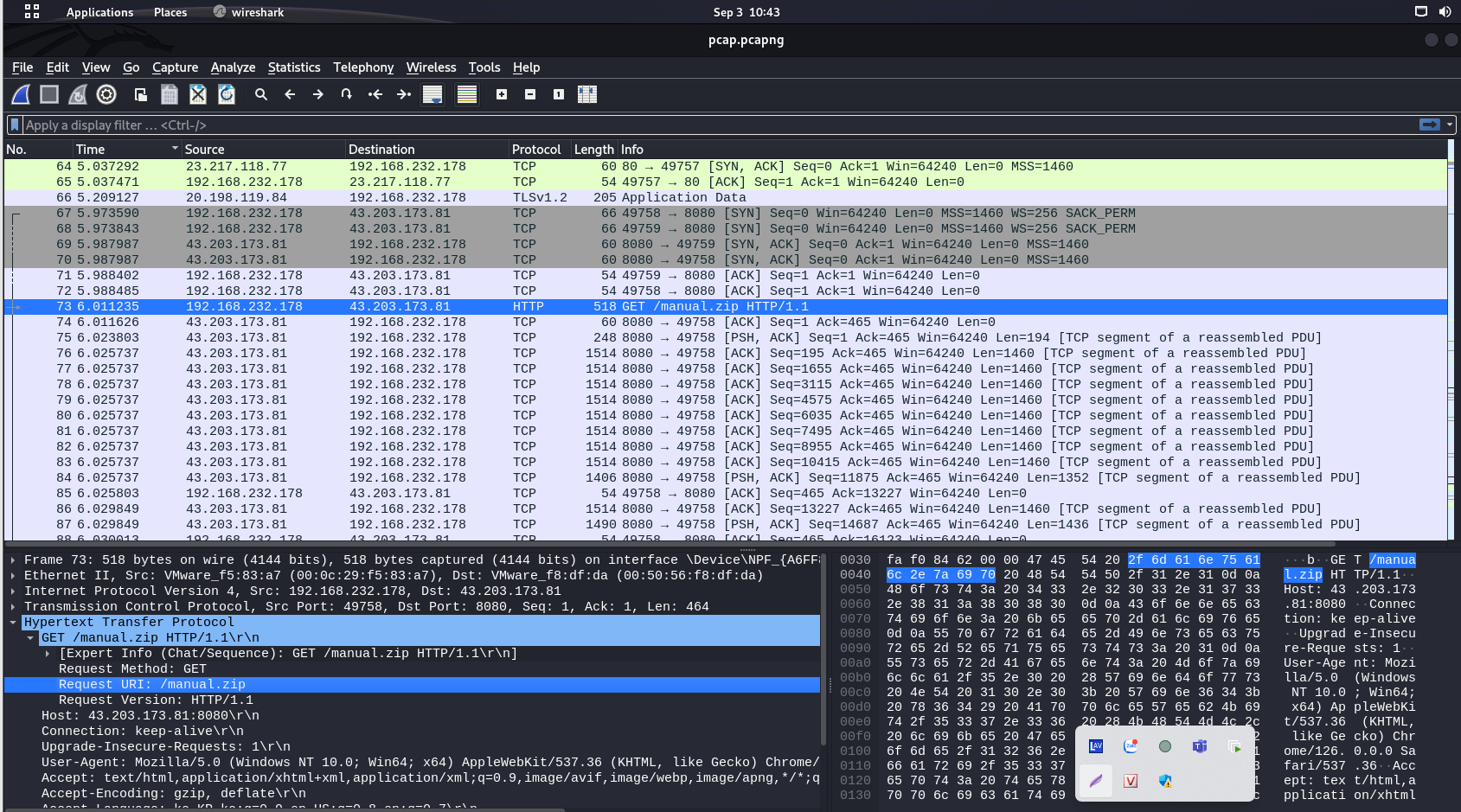
Mã hash của tệp mã độc (100)

Vui lòng thu thập tệp mã độc (không phải tệp nén). Tính mã hash md5 và trả lời.

## Answer 1

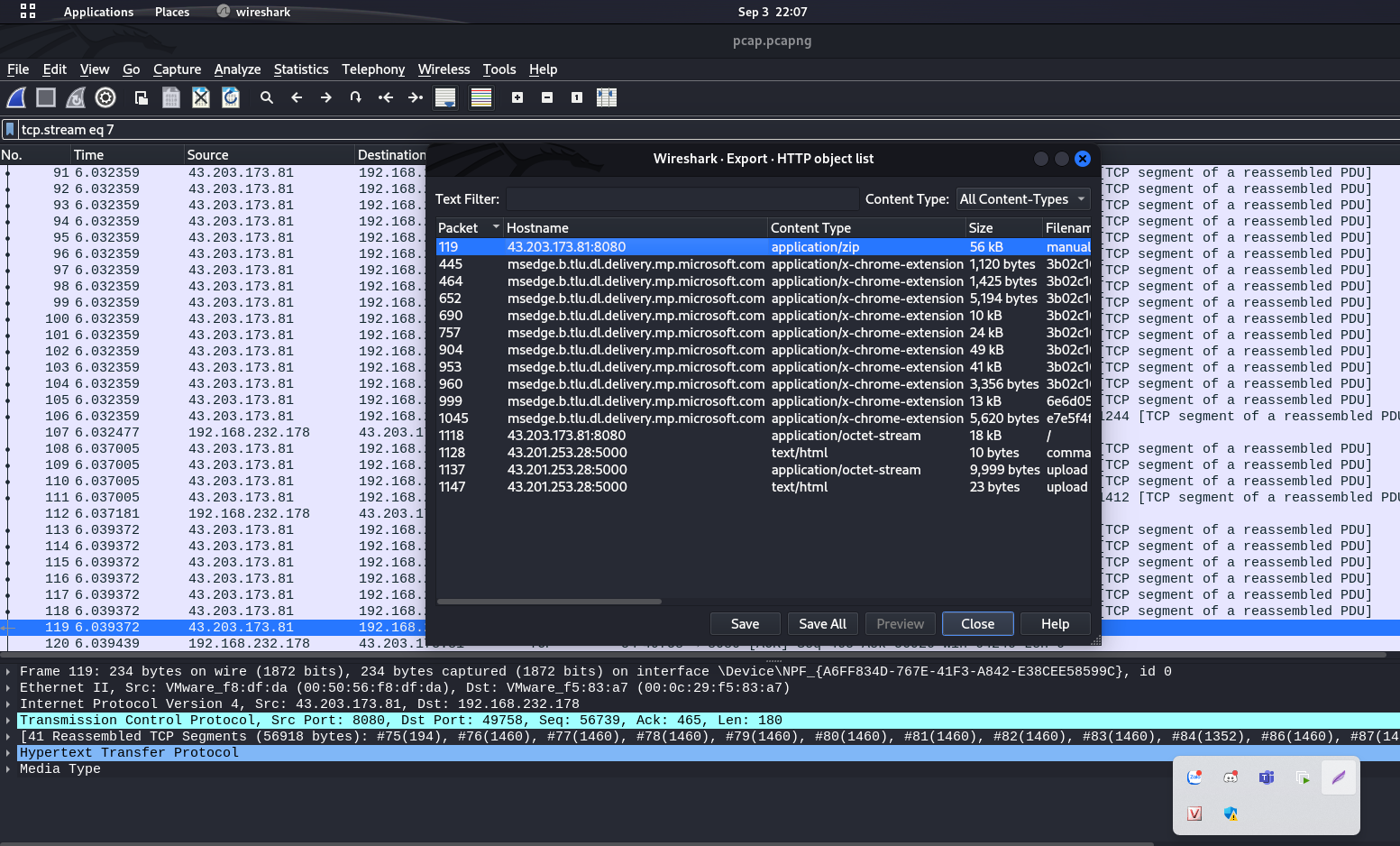
Ta biết được file chứa mã độc được tải về là manual.zip.  
Mở file pcap.pcapng bằng wireshark để đọc lưu lượng mạng.

Ta tìm gói tin dùng để tải về file mã độc.

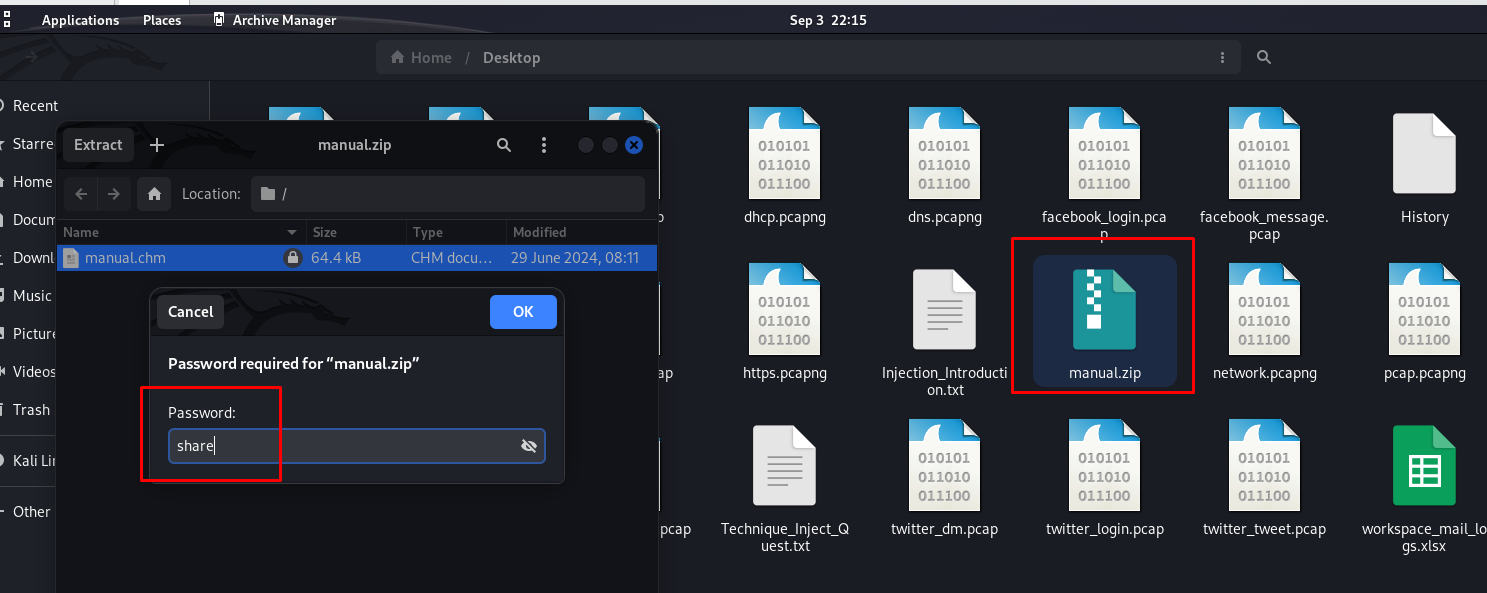


Trích xuất file manual.zip:

>>> manual.zip > Follow HTTP stream > File > Export objects > HTTP



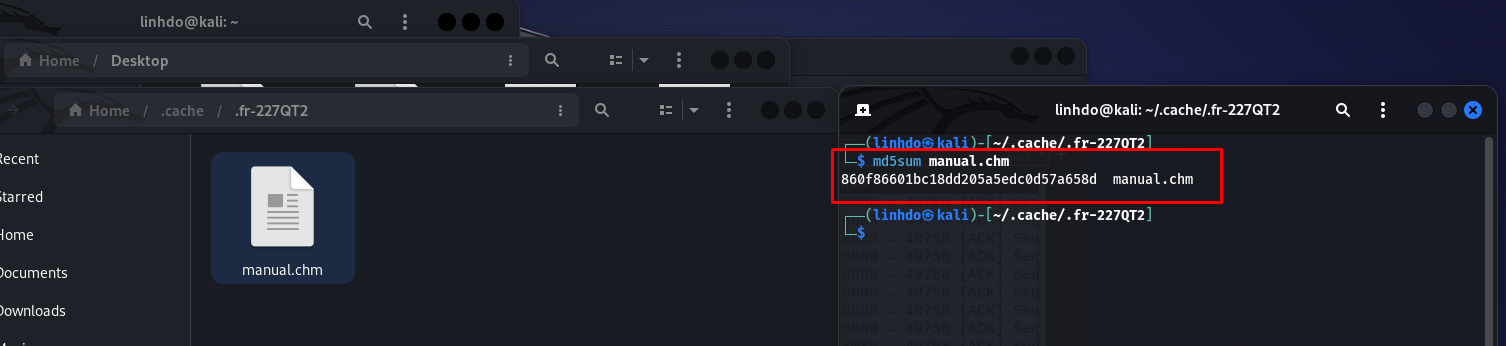
Sau khi lưu file, sử dụng mật khẩu **share** giải nén



Sau khi giải nén ta có file manual.chm

Dùng lệnh md5sum manual.chm

Mã hash của tệp mã độc: 860f86601bc18dd205a5edc0d57a658d



-------------------------------------------------------------------------------------------------------------------------

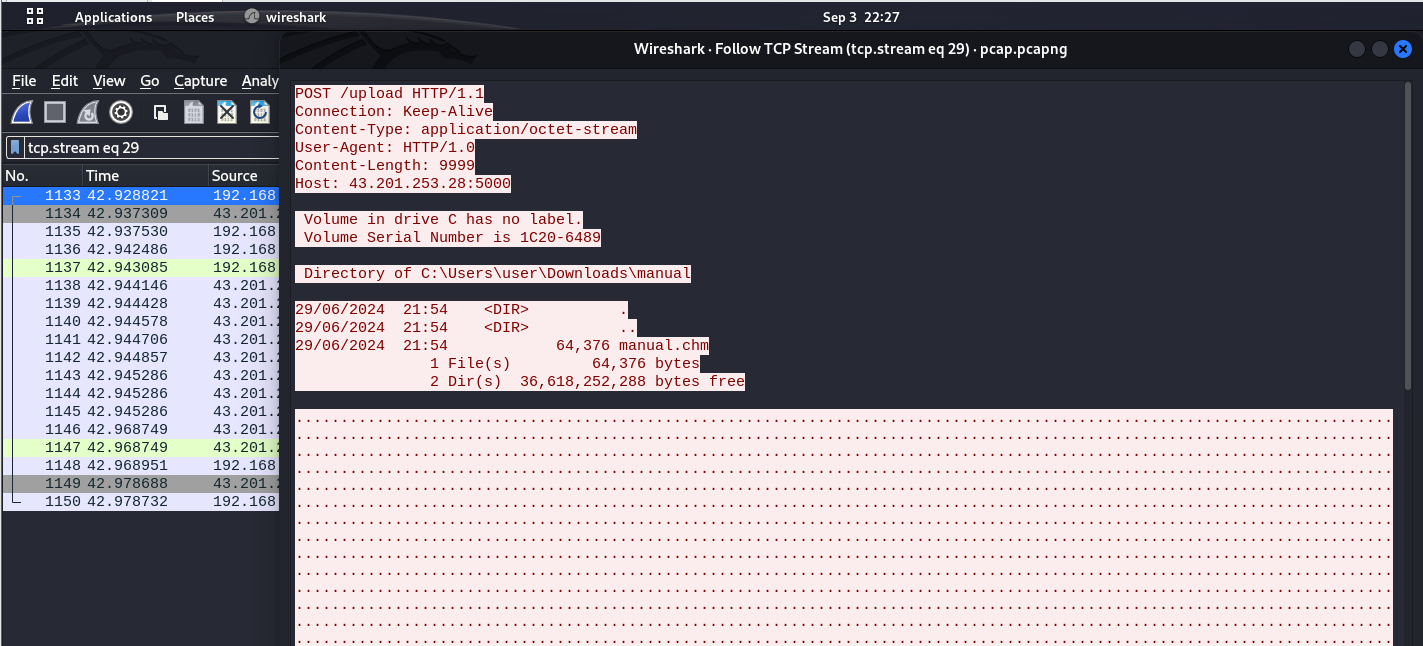
**Question 2**

Địa chỉ của C2 Server được sử dụng để nhận thông tin (100)

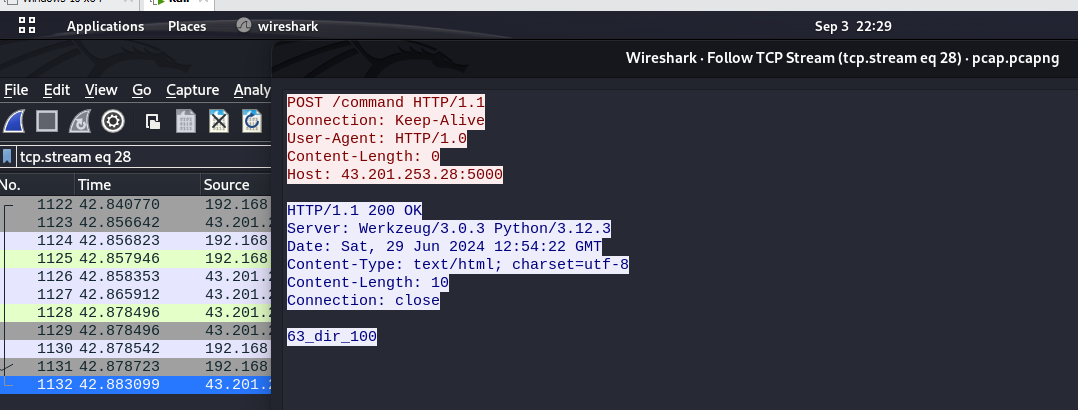
Trả lời địa chỉ của C2 server theo dạng: IP:PORT

## Answer 2

Ta thấy stream 29 máy bị tấn công gửi đi một lưu lượng dữ liệu



ở stream 28 câu lệnh dir gửi đi máy chủ C&C



>>> Wireshark or analyze malware

>>> follow stream packet "command/post" > dir command > next stream have C&C server

**43.201.253.28:5000**

-------------------------------------------------------------------------------------------------------------------------

**Question 3**

Câu lệnh C2 (100)

Mã độc đã nhận được lệnh gì từ C2 Server?

Chọn 1 trong các đáp án

1. dir

2. whoami

3. ipconfig

4. ifconfig

5. ls

## Answer 3

1

Như đã tìm thấy ở trên câu lệnh C&C gửi tới là dir

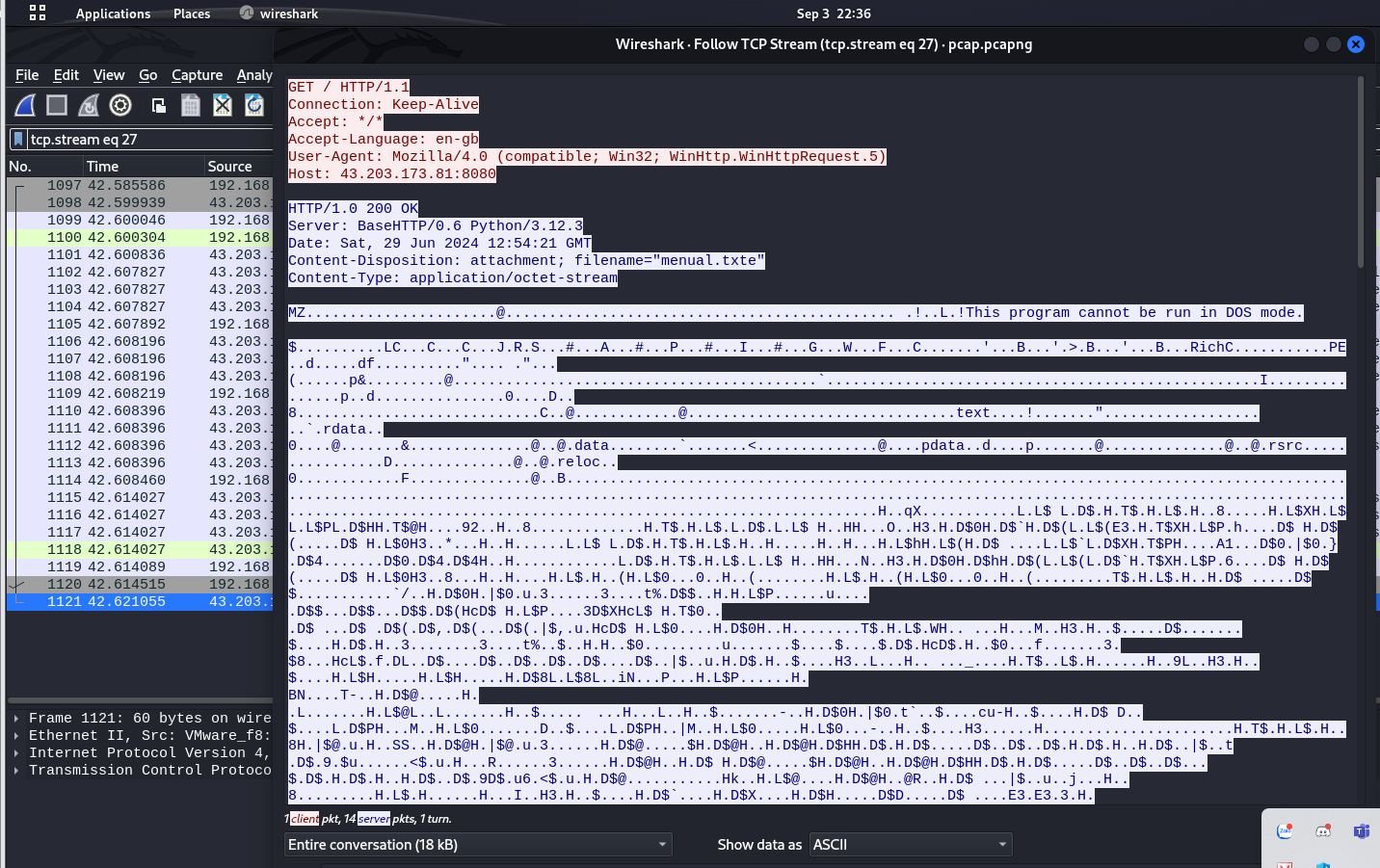
-------------------------------------------------------------------------------------------------------------------------

**Question 4**

Downloader (100)

Sau khi được thực thi, mã độc đã tải về một tệp mã độc khác, hãy trả lời url được sử dụng để tải về.

Answer 4: http://43.203.173.81:8080



-------------------------------------------------------------------------------------------------------------------------

**Question 5**

Mã hash của độc menual (100)

Vui lòng trả lời mã hash md5 của mã độc menual đã được tải về.

## Answer 5

md5sum menual.exe

0de9be1aba2e6dc3ce016fb24faad9e