**BÁO CÁO TIẾN TRÌNH LÀM BÀI TRÊN CyberDefenders**

**Tuần đầu :**

**Các nội dung đã thực hiện**

**luyện tập về Windows Memory Image Forensics**

**Link đề :**

[**https://cyberdefenders.org/blueteam-ctf-challenges/43**](https://cyberdefenders.org/blueteam-ctf-challenges/43)

**Đề bài :**

**Company X has contacted you to perform forensics work on a recent incident that occurred. One of their employees had received an e-mail from a co-worker that pointed to a PDF file. Upon opening, the employee did not notice anything; however, they recently had unusual activity in their bank account.**

**The initial theory is that a user received an e-mail, containing an URL leading to a forged PDF document. Opening that document in Acrobat Reader triggers a malicious Javascript that initiates a sequence of actions to take over the victim's system.**

**Company X was able to obtain a memory image of the employee's virtual machine upon suspected infection and asked you to analyze the virtual memory and provide answers to the questions.**

**CÁC CÔNG CỤ TOOLS ĐƯỢC SP TRONG BÀI :**

* [**PDF-Tools**](https://blog.didierstevens.com/programs/pdf-tools/)
* [**Malfind**](https://github.com/volatilityfoundation/volatility/wiki/Command-Reference-Mal)
* [**libemu**](http://libemu.carnivore.it/)
* [**Volatility**](https://github.com/volatilityfoundation/volatility)
* [**Strings**](https://linux.die.net/man/1/strings)
* [**Foremost**](https://linux.die.net/man/1/foremost)
* [**Hexdump**](https://linux.die.net/man/1/hexdump)
* [**Firebug**](https://blog.getfirebug.com/)
* [**Objdump**](https://linux.die.net/man/1/objdump)

**github link BankingTrouble :** [**https://github.com/Panagiotis-INS/Cyber-Defenders/tree/main/BankingTroubles**](https://github.com/Panagiotis-INS/Cyber-Defenders/tree/main/BankingTroubles)

**Q1 :** What was the local IP address of the victim's machine?

**ở phần Hint người ta đã gợi ý rằng :**

**Hint #1:**

**Try to analyze the image with volatility**

**Hint #2:**

**Use "volatility" with the "imageinfo" plugin to get the profile.**

**Hint #3:**

**Check available volatility plugins**

**Hint #4:**

**Use "volatility" with the "connections" plugin to print open connections**

**→ em sẽ dùng tool volatility để scan image của file Bob.vmem**

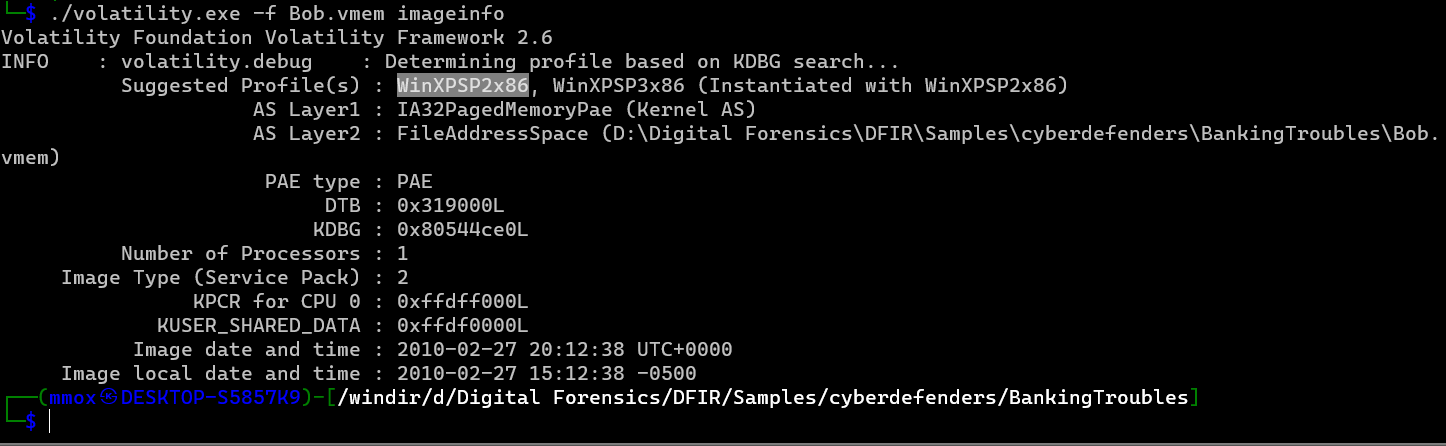
**Requirement : tools volatility là chỉ được dùng python2 nên em sẽ phải cài đặt python2**

**Sau đó em sẽ bắt đầu làm**

**B1 : em sẽ get profile của file Bob.vmem ấy**

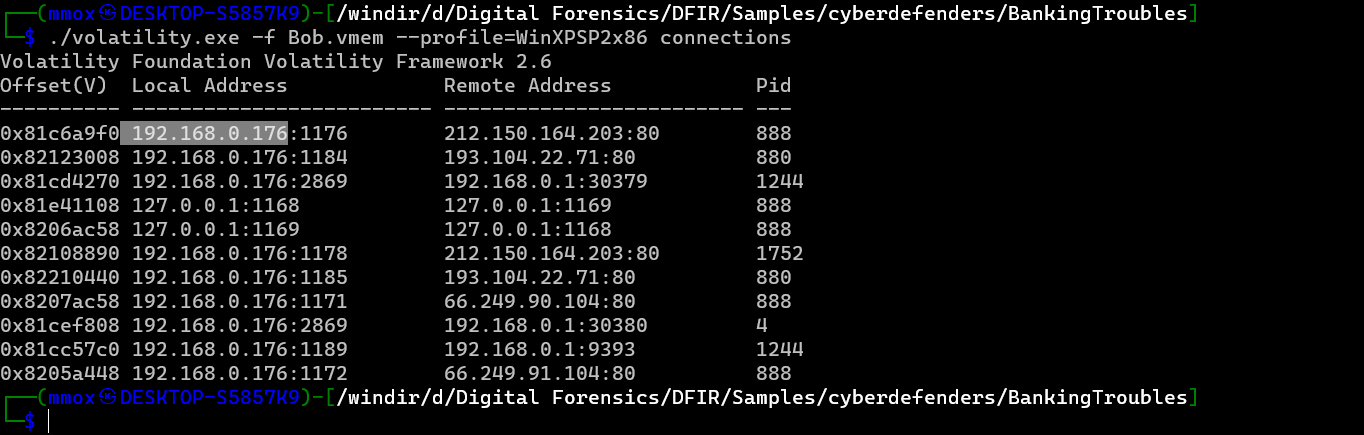
**python2 vol.py -f Bob.vmem imageinfo**

**và nó ra là “WinXPSP2x86”**

****

**B2 : ở phần gợi ý 3 người ta có nói Kiểm tra các plugin biến động có sẵn và câu hỏi đầu tiên người ta hỏi về ip của victim’s -> dùng lệnh connections để tìm ra địa python2 vol.py -f Bob.vmem --profile=WinXPSP2x86 connections**

**và nó in ra**

****

**→ đáp án 192.168.0.176**

**Q2 :** What was the OS environment variable's value?

ở câu này người ta hỏi đến environment variable's value của OS

Gợi ý :

Hint **#Try to analyze the image with volatility.**:

Try to analyze the image with volatility.

Hint **#Use "volatility" with the "imageinfo" plugin to get the profile.**:

Use "volatility" with the "imageinfo" plugin to get the profile.

Hint **#Check available volatility plugins**:

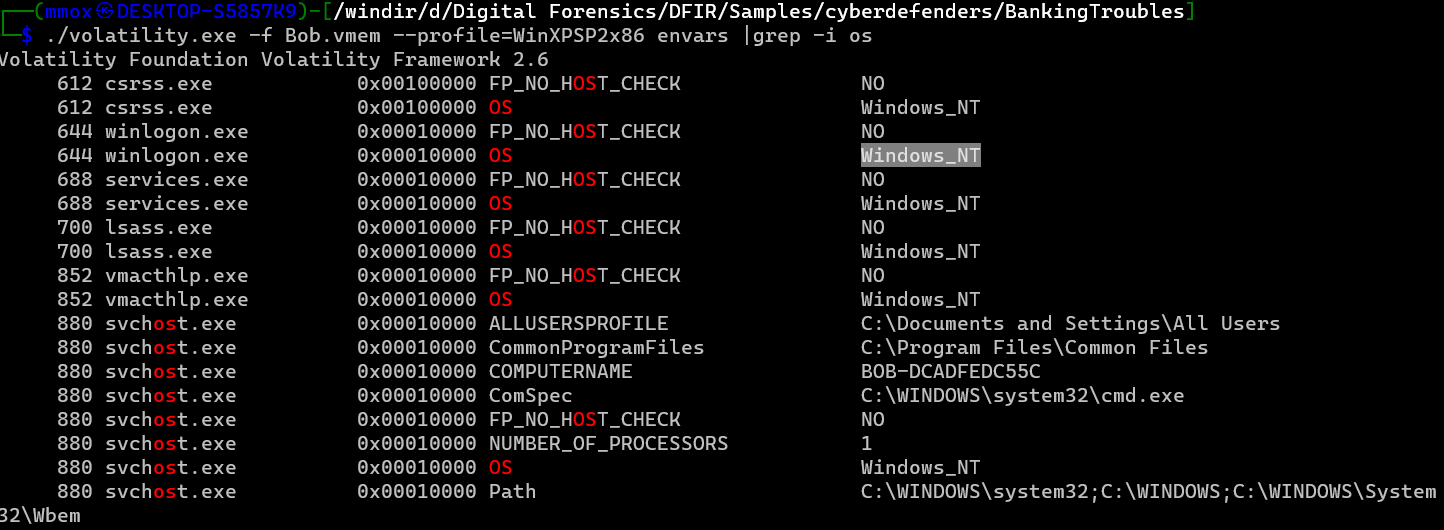
Check available volatility plugins

Hint **#Use "volatility" with the "envars" plugin to print environment variables**:

Use "volatility" with the "envars" plugin to print environment variables

-> em sẽ dùng lệnh envars |grep -i os để nó xem được cái biến môi trường

—> **python2 vol.py -f Bob.vmem** --profile=WinXPSP2x86 envars |grep -i os



**→ đáp án : Windows\_NT**

**Q3 :** What was the Administrator's password?

Gợi Ý:

Hint **#Use "volatility" with the "envars" plugin to print environment variables**:

Use "volatility" with the "envars" plugin to print environment variables

Hint **#Check available volatility plugins**:

Check available volatility plugins

Hint **#Use "volatility" with "hashdump" plugin to extract users' hashes**:

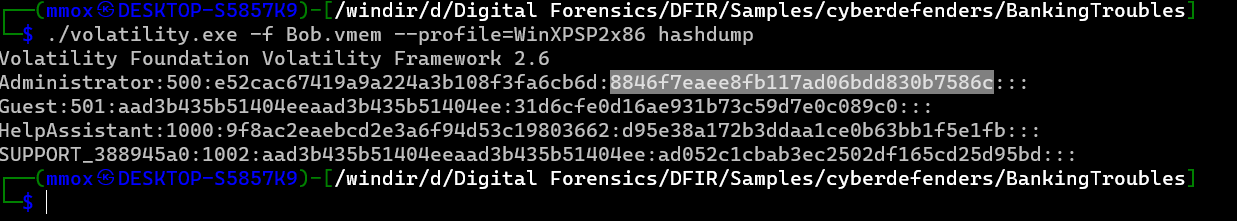
Use "volatility" with "hashdump" plugin to extract users' hashes

Hint **#Crack the administrator hash using john the ripper**:

Crack the administrator hash using john the ripper

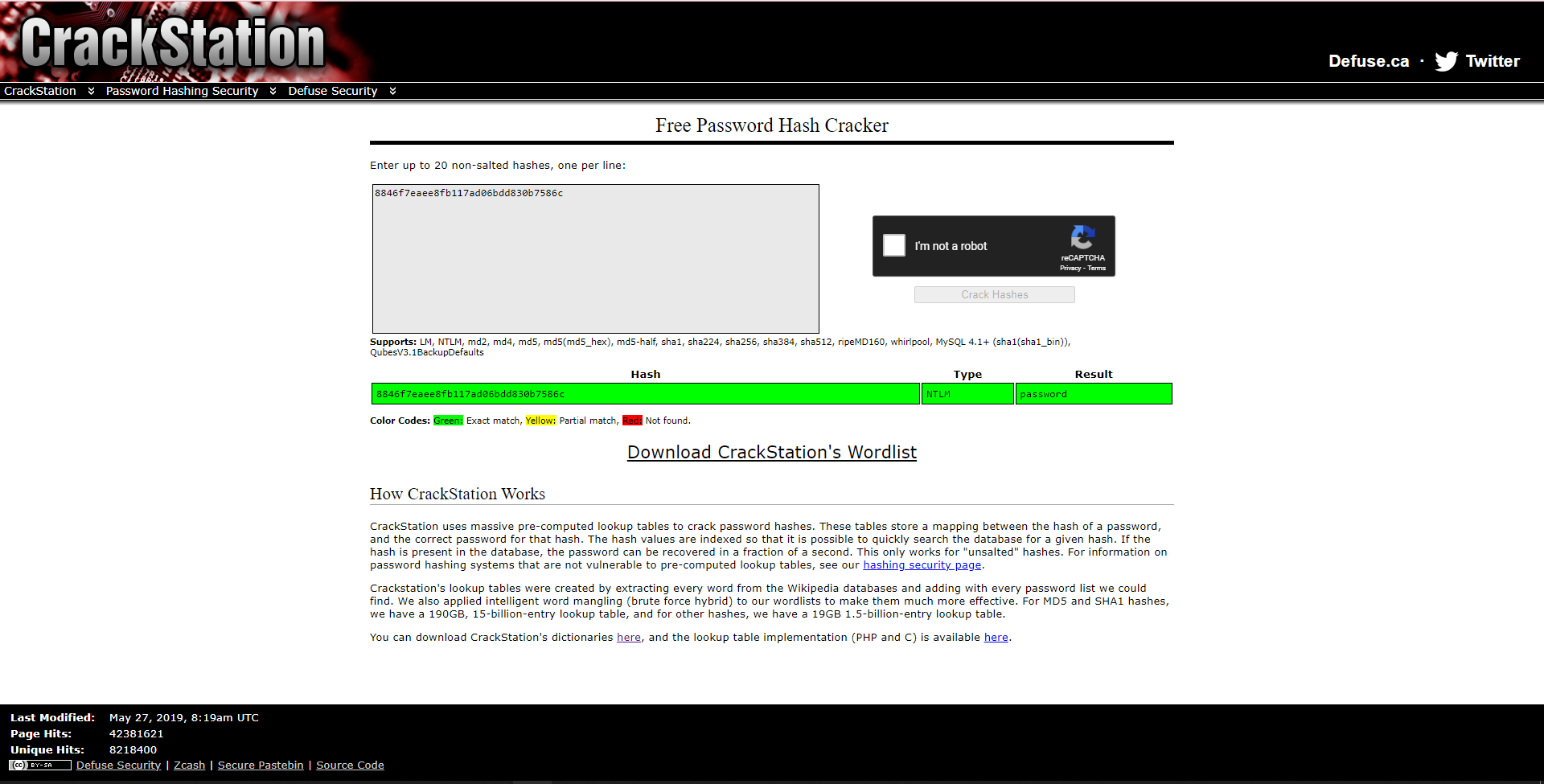
→ anh ấy muốn là mật khẩu Quản trị viên nên hashdump, sau đó sẽ xem nó có thể bẻ khóa được không

.**python2 vol.py -f Bob.vmem** --profile=WinXPSP2x86 hashdump



nó sẽ cho ra : 8846f7eaee8fb117ad06bdd830b7586c

**và sau đó em sẽ dùng tools crackstation như đã được đề cập từ đầu bài các tools được sp như vậy ta có thể bẻ khóa được nó ra là**

**:**

**→ đáp án : password**

**Q4: Which process was most likely responsible for the initial exploit?**

**Gợi ý :**

**Hint #Try to collect multiple data and link them together:**

**Try to collect multiple data and link them together**

**Hint #Use "volatility" with "pstree" to list the process.:**

**Use "volatility" with "pstree" to list the process.**

**Hint #Use "volatility" with "malfind" with "-p" argument and check the suspicious process:**

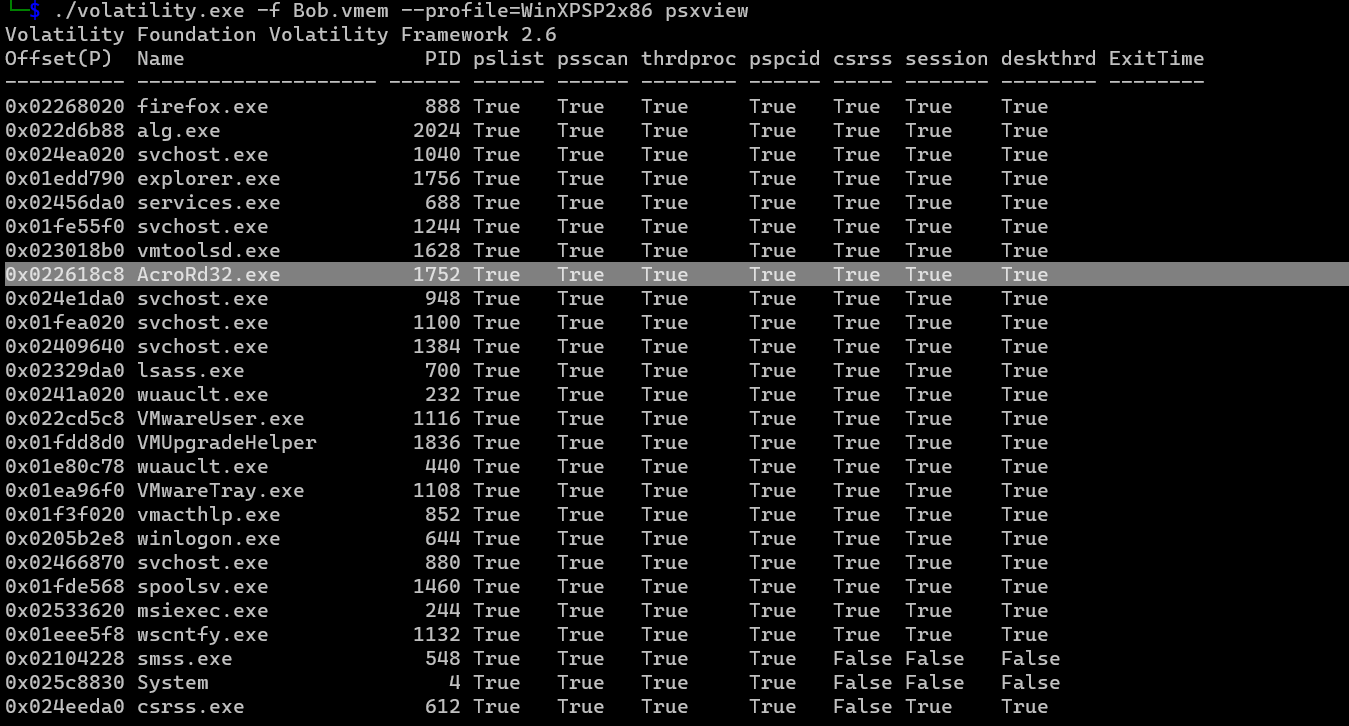
**Use "volatility" with "malfind" with "-p" argument and check the suspicious process**

**Hint #Use "volatility" with "connscan" plugin to list open connections and process responsible for it. You will find a suspicious connection from the Acrobat process with 1752 PID:**

**Use "volatility" with "connscan" plugin to list open connections and process responsible for it. You will find a suspicious connection from the Acrobat process with 1752 PID**

**→ ở hint này nhắc đến khá nhiều đến thằng 1752 PID → mình phải biết được quá trình hoạt động của từng process thằng một → dùng plugin psxview để xác định quy trình ẩn với sự biến động của thằng 1752 PID**

**→ python2 vol.py -f Bob.vmem** --profile=WinXPSP2x86 psxview



và khi ra được tất cả quá trình thì ta tìm đến thằng PID đó chính là thằng AcroRd32.exe và em nghĩ đó chính là thằng mình cần tìm

→ đáp án : AcroRd32.exe

Q5 : What is the extension of the malicious file retrieved from the process responsible for the initial exploit?

Gợi ý :

Hint **#Check the suspicious process documentation.**:

Check the suspicious process documentation.

Hint **#The extension is "pdf" according to the suspicious process.**:

The extension is "pdf" according to the suspicious process.

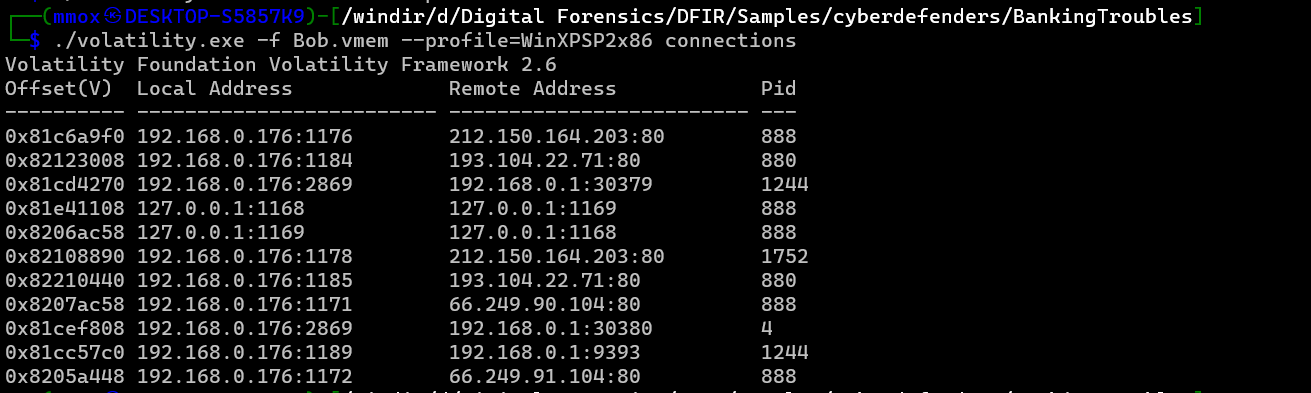
→ nó là pdf luôn (trong hint đã ghi Phần mở rộng là "pdf" theo quy trình đáng ngờ:)

→ đáp án : pdf

Q6 :Suspicious processes opened network connections to external IPs. Provide the two external IP addresses. (comma-separated without spaces)

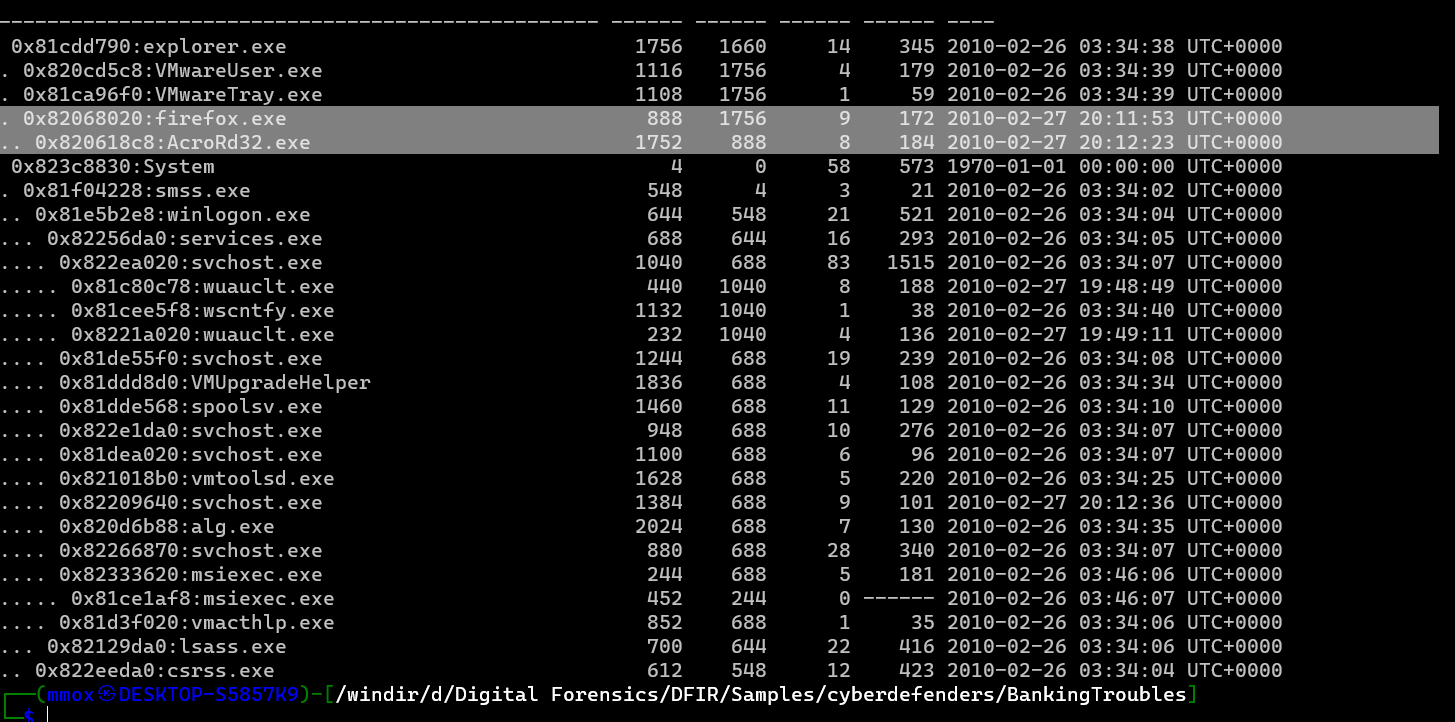
đầu tiên thì tra connections để tìm những kết nối mạng với các IP bên ngoài

**python2 vol.py -f Bob.vmem --profile=WinXPSP2x86 connections**

****

ta thấy được bên pid có 3 luồng ngoài đó chính là 1752 pid, 880 pid và cuối cùng là 4 nhưng chúng ta phải xác định các app sử dụng → chúng ta dùng lệnh pstree để tìm kiếm nó đã hoạt động những gì trong hệ thống → dùng lệnh

**python2 vol.py -f Bob.vmem --profile=WinXPSP2x86 pstree**

****

**→ svchost và System là của thg hệ thống máy chủ hoạt động**

**→ chỉ còn mỗi 1 thằng AcroRD32.exe là quy trình đáng ngờ đã mở kết nối mạng đến IP bên ngoài.**

**→ Đáp án là 193.104.22.71,212.150.164.203**

**Q8: Extract files from the initial process. One file has an MD5 hash ending with "528afe08e437765cc".**

**When was this file first submitted for analysis on VirusTotal?**

**Gợi ý :**

**Hint #Use "volatility" to analyze the memory:**

**Use "volatility" to analyze the memory**

**Hint #Use the "memdump" plugin to dump process memory.:**

**Use the "memdump" plugin to dump process memory.**

**Hint #Use binwalk of foremost to dump files from the process:**

**Use binwalk of foremost to dump files from the process**

**Hint #1. Get the md5 hash of the pdf file 2. Search using hash on virus total 3. Check the details tab you will find the first submission date under history:**

**1. Get the md5 hash of the pdf file 2. Search using hash on virus total 3. Check the details tab you will find the first submission date under history**

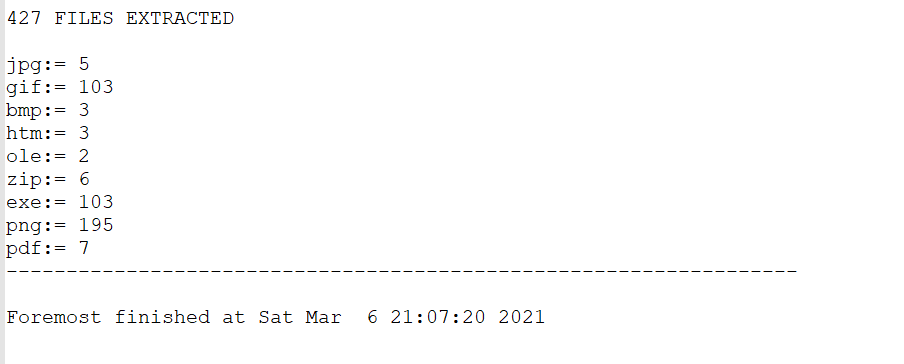
→ dùng file AcroRd32.exe để dump nó (dùng tool memdump)

python2 vol.py -f Bob.vmem --profile=WinXPSP2x86 memdump -p 1752 -D

sau đó sẽ dùng foremost để extract ra

foremost 1752.dmp

và nó sẽ ra rất nhiều dữ liệu



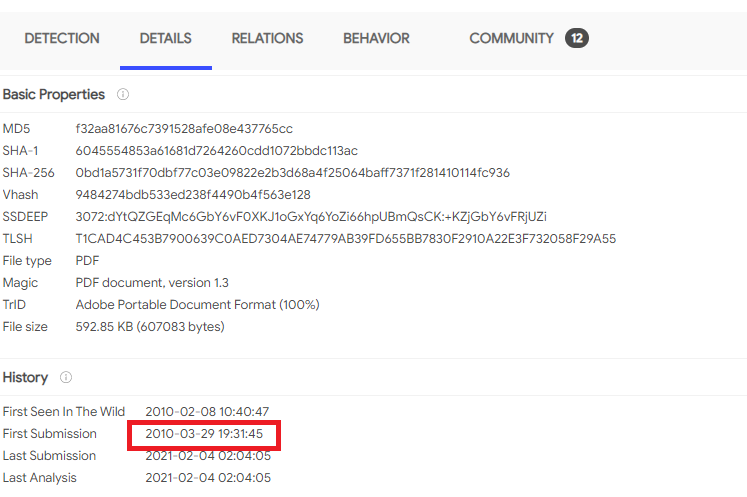
Nhưng vì quá trình này là dành cho PDF, vì vậy em sẽ kiểm tra các bản trích xuất PDF

**md5sum \* |grep 528afe08e437765cc**

vì vậy ta có hash

f32aa81676c7391528afe08e437765cc

sử dụng virustotal và tìm kiếm bằng hash ta có :



→ đáp án : **2010-03-29 19:31:45**

**Q9 : What was the PID of the process that loaded the file PDF.php?**

**→ đáp án : 1752**

**Q10 : The JS includes a function meant to hide the call to function eval(). Provide the name of that function.**

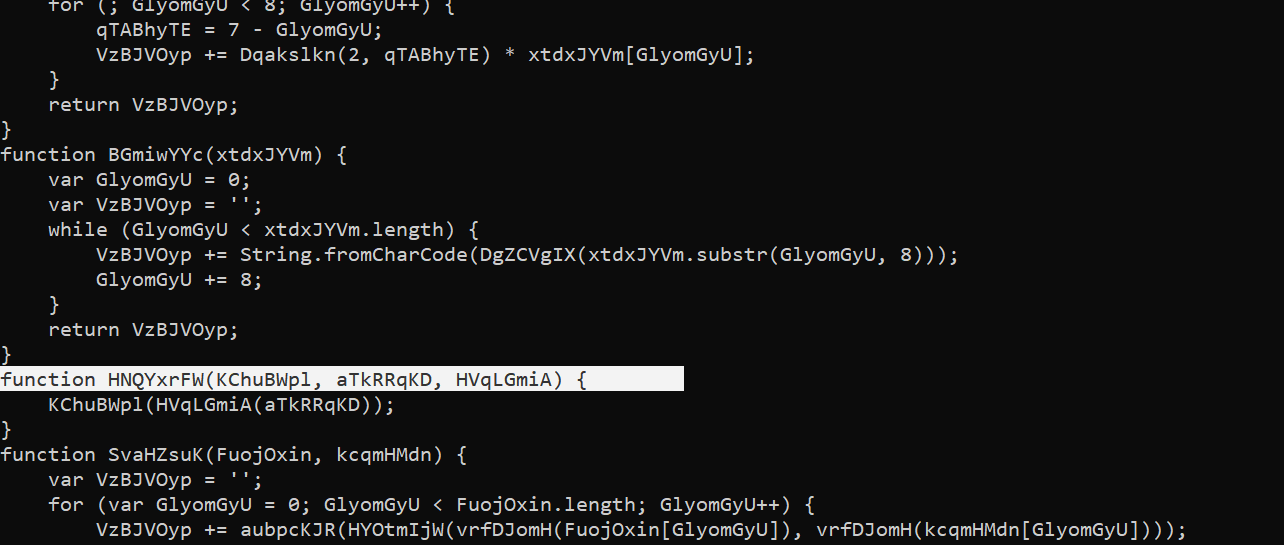
**như chúng ta đã biết SUS PDF vì vậy em sẽ sử dụng công cụ PeepDF**

**python peepdf.py 00601560.pdf**

**echo 'extract js > all-javascripts-from-my.pdf' > xtract.txt**

**python peepdf.py -l -f -s xtract.txt 00601560.pdf**

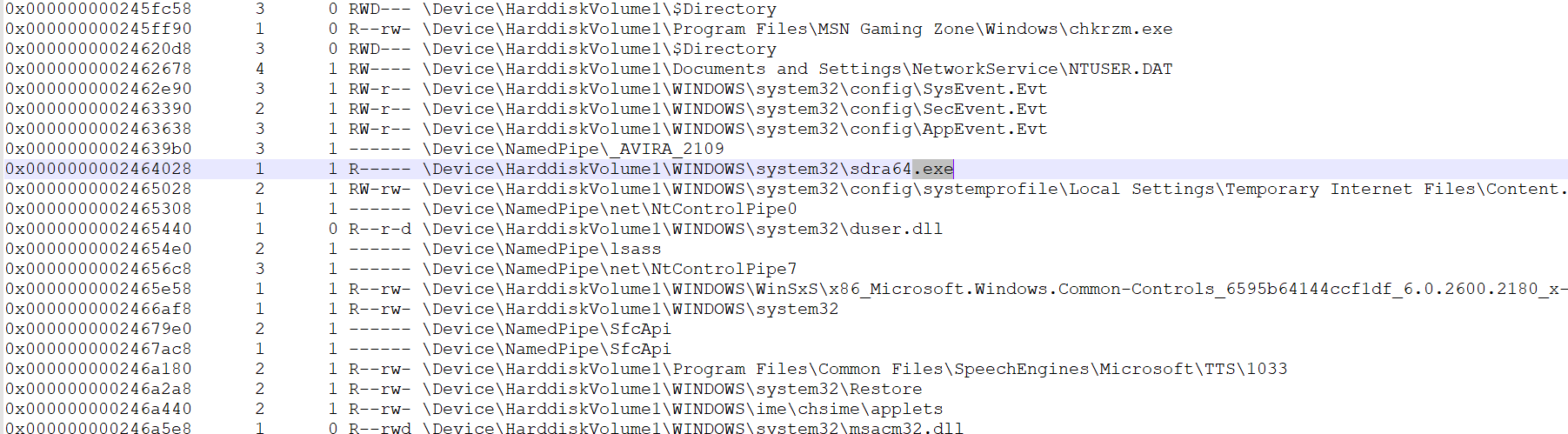
**cat all-javascripts-from-my.pdf**

****

**và em đã tìm được function name : HNQYxrFW**

| **#13** | **What is the name of the malicious executable referenced in registry hive '\WINDOWS\system32\config\software', and is variant of ZeuS trojan?** |
| --- | --- |

**python2 vol.py -f Bob.vmem --profile=WinXPSP2x86 filescan >f.txt**

****

**→ đáp án : sdra64.exe**