

AfricanFalls Blue Team Lab

Q1. What is the MD5 hash value of the suspect disk?

Em sẽ kiểm tra với 2 file tải về. Ở đây em thấy file **DiskDrigger.ad1.txt** đây là file mô tả quá trình thu thập và xác minh một ảnh đĩa pháp y từ một phân vùng trong tệp 001Win10.e01. Các thư mục và tệp đã được sao chép và liệt kê chi tiết trong báo cáo, kèm theo các kiểm tra hash để đảm bảo tính toàn vẹn của ảnh đĩa. Điều này giúp đảm bảo rằng dữ liệu được thu thập không bị thay đổi trong suốt quá trình và có thể được sử dụng cho các mục đích pháp lý hoặc điều tra.

```
*DiskDrigger.ad1.txt - Notepad
File Edit Format View Help
001Win10.e01:Partition 2 [50647MB]:NONAME [NTFS][root]Users\John Doe\Desktop\Start Tor Browser.lnk.FileSlack(Exact)
001Win10.e01:Partition 2 [50647MB]:NONAME [NTFS][root]Users\John Doe\Desktop\I30(Exact)
001Win10.e01:Partition 2 [50647MB]:NONAME [NTFS][root]Users\John Doe\Cookies\*(wildcard,Consider Case,Include Subdirectories)
001Win10.e01:Partition 2 [50647MB]:NONAME [NTFS][root]Users\John Doe\Contacts\*(wildcard,Consider Case,Include Subdirectories)
001Win10.e01:Partition 2 [50647MB]:NONAME [NTFS][root]Users\John Doe\Application Data\*(wildcard,Consider Case,Include Subdirectories)
001Win10.e01:Partition 2 [50647MB]:NONAME [NTFS][root]Users\John Doe\3D Objects\*(wildcard,Consider Case,Include Subdirectories)
001Win10.e01:Partition 2 [50647MB]:NONAME [NTFS][root]Users\John Doe\AppData\Local\Application Data\*(wildcard,Consider Case,Include Subdirectories)
001Win10.e01:Partition 2 [50647MB]:NONAME [NTFS][root]Users\John Doe\AppData\Local\FileZilla\*(wildcard,Consider Case,Include Subdirectories)
001Win10.e01:Partition 2 [50647MB]:NONAME [NTFS][root]Users\John Doe\AppData\Local\Google\*(wildcard,Consider Case,Include Subdirectories)
001Win10.e01:Partition 2 [50647MB]:NONAME [NTFS][root]Users\John Doe\AppData\Local\Microsoft\Windows\*(wildcard,Consider Case,Include Subdirectories)
001Win10.e01:Partition 2 [50647MB]:NONAME [NTFS][root]Users\John Doe\AppData\Roaming\FileZilla\*(wildcard,Consider Case,Include Subdirectories)
001Win10.e01:Partition 2 [50647MB]:NONAME [NTFS][root]Users\John Doe\AppData\Roaming\Microsoft\Windows\*(wildcard,Consider Case,Include Subdirectories)
001Win10.e01:Partition 2 [50647MB]:NONAME [NTFS][root]Users\John Doe\AppData\Local\BraveSoftware\Brave-Browser\*(wildcard,Consider Case,Include Subdirectories)

[Computed Hashes]
MD5 checksum: 9471e69c95d8909ae60ddff30d50ffa1
SHA1 checksum: 167aa08db25dfceb876b0176ddc329a3d9f2803a

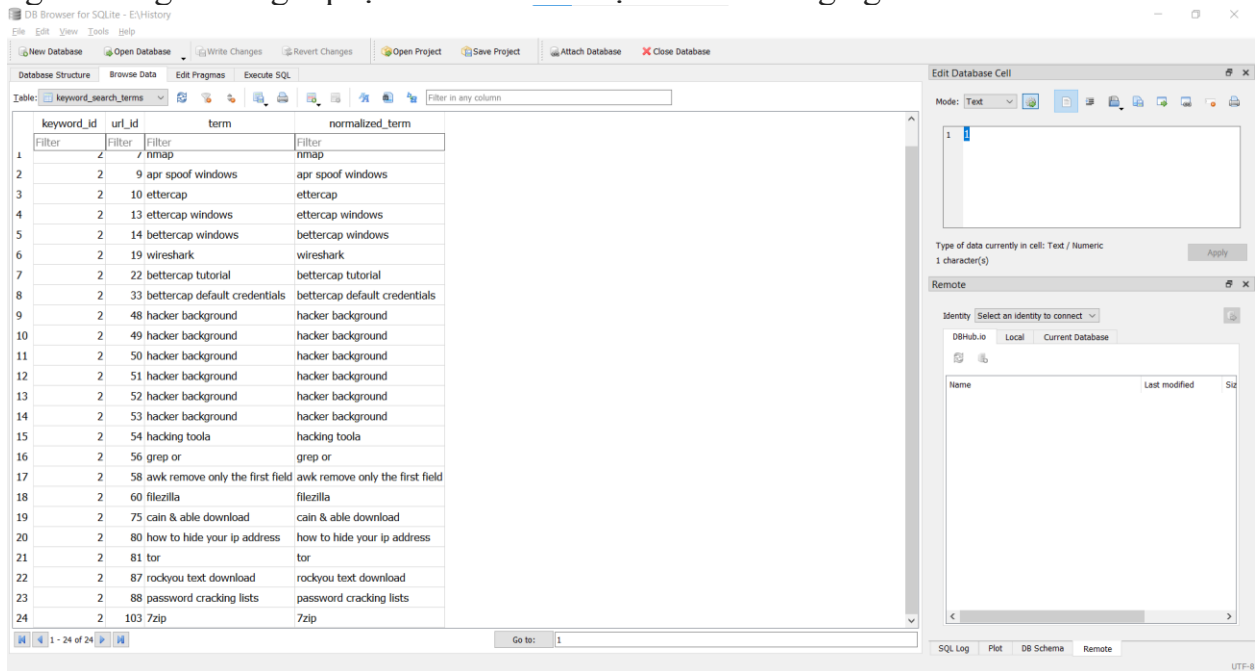
Image information:
Acquisition started: Tue Jun 15 12:28:20 2021
Acquisition finished: Tue Jun 15 12:33:10 2021
Segment list:
D:\Users\Mawso3a\Desktop\DiskDrigger.ad1

Image Verification Results:
Verification started: Tue Jun 15 12:33:18 2021
Verification finished: Tue Jun 15 12:33:51 2021
MD5 checksum: 9471e69c95d8909ae60ddff30d50ffa1 : verified
SHA1 checksum: 167aa08db25dfceb876b0176ddc329a3d9f2803a : verified
```

Vậy đáp án của câu này là **9471e69c95d8909ae60ddff30d50ffa1**

Q2. What phrase did the suspect search for on 2021-04-29 18:17:38 UTC? (three words, two spaces in between)

Ở đây câu hỏi là nghi phạm đã tìm kiếm cụm từ nào. Vậy em sẽ đọc file lịch sử của người dung xem nghi phạm đã tìm kiếm cụm từ nào đáng nghi.



The screenshot shows the DB Browser for SQLite interface. The main window displays a table named 'keyword_search_terms' with the following data:

keyword_id	url_id	term	normalized_term
1	2	9 apr spoof windows	apr spoof windows
2	2	10 ettercap	ettercap
3	2	13 ettercap windows	ettercap windows
4	2	14 ettercap windows	ettercap windows
5	2	19 wireshark	wireshark
6	2	22 ettercap tutorial	ettercap tutorial
7	2	33 ettercap default credentials	ettercap default credentials
8	2	48 hacker background	hacker background
9	2	49 hacker background	hacker background
10	2	50 hacker background	hacker background
11	2	51 hacker background	hacker background
12	2	52 hacker background	hacker background
13	2	53 hacker background	hacker background
14	2	54 hacking toola	hacking toola
15	2	56 grep or	grep or
16	2	58 awk remove only the first field	awk remove only the first field
17	2	60 filezilla	filezilla
18	2	75 cain & able download	cain & able download
19	2	80 how to hide your ip address	how to hide your ip address
20	2	81 tor	tor
21	2	87 rockyou text download	rockyou text download
22	2	88 password cracking lists	password cracking lists
23	2	103 7zip	7zip

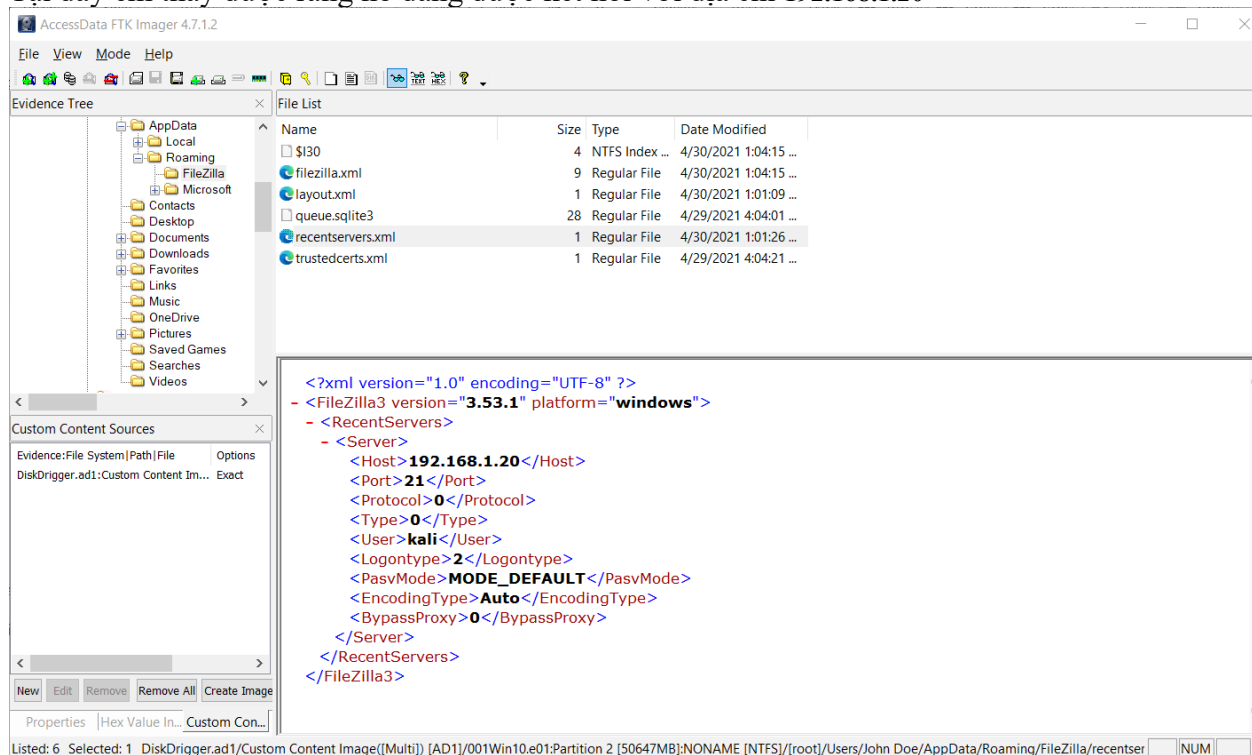
The table is displayed in a grid view. The right sidebar shows the 'Edit Database Cell' window, which is currently empty. The bottom status bar indicates the file is 'UTF-8'.

Ở đây ta thấy 1 điểm đáng nghi là có lịch sử tìm kiếm là **password cracking lists**. Vậy đây chính là đáp án của câu này.

Q3. What is the IPv4 address of the FTP server the suspect connected to?

Ở đây em sẽ kiểm tra các tập tin cấu hình và lịch sử kết nối của các ứng dụng FTP client như FileZilla. Đây là lý do vì sao kiểm tra FileZilla FTP Client có thể cung cấp thông tin về địa chỉ IPv4 của máy chủ FTP mà nghi phạm đã kết nối.

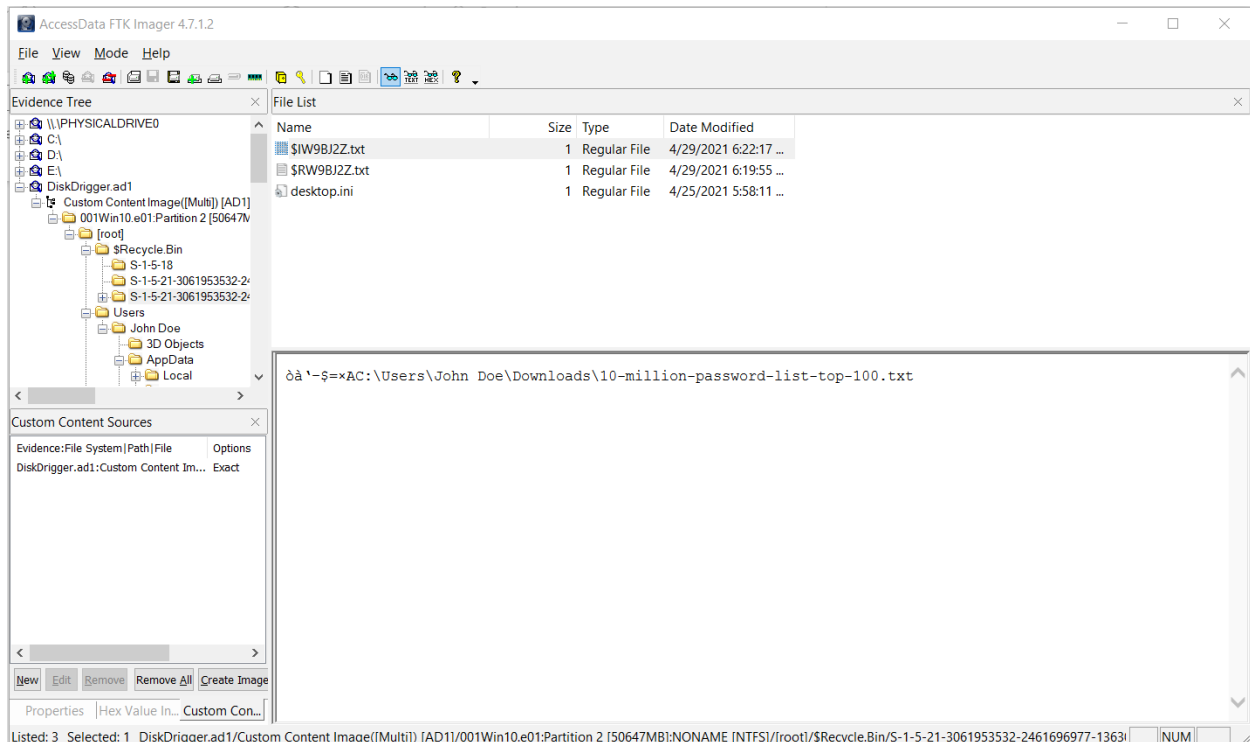
Tại đây em thấy được rằng nó đang được kết nối với địa chỉ **192.168.1.20**



Vậy đáp án của câu này **192.168.1.20**

Q4. What date and time was a password list deleted in UTC? (YYYY-MM-DD HH:MM:SS UTC)

Ở đây em thấy được rằng nếu xóa thì chắc chắn nó sẽ lưu lại dấu vết ở tệp tin Recycle Bin. Vào file này em thấy rằng nó đã xóa file 10-million-password-list-top-100.txt. Tra mạng thì ta thấy file này lưu 10 triệu mật khẩu nó kẻ tấn công đang bruce force mật khẩu.



Vậy đáp án của câu này là: **2021-04-29 18:22:17 UTC**

Q5. How many times was Tor Browser ran on the suspect's computer? (number only)

Ở bài này thấy TOR chỉ được cài đặt chứ chưa hề được chạy.

AccessData FTK Imager 4.7.1.2

File View Mode Help

Evidence Tree

- \\PHYSICALDRIVE0
 - C:\
 - D:\
 - E:\
 - DiskDrigger.ad1
 - Custom Content Image([Multi]) [AD1]
 - 001Win10.e01:Partition 2 [50647MB]
 - [root]
 - \$Recycle.Bin
 - Users
 - John Doe
 - Windows
 - Prefetch
 - ReadyBoot
 - System32

File List

Name	Size	Type	Date Modified
TORBROWSER-INSTALL-WIN64-...	26	Regular File	4/29/2021 6:22:32 ...
TORBROWSER-INSTALL-WIN64-...	3	File Slack	
TRUSTEDINSTALLER.EXE-3CC531...	5	Regular File	4/30/2021 1:15:27 ...
TRUSTEDINSTALLER.EXE-3CC531...	4	File Slack	
UNINSTALL.EXE-21BE24FA.pf	9	Regular File	4/28/2021 5:28:14 ...
UNINSTALL.EXE-21BE24FA.pf.File...	4	File Slack	
USEROEBEBROKER.EXE-D2992F...	8	Regular File	4/30/2021 1:07:31 ...
USEROEBEBROKER.EXE-D2992F...	1	File Slack	
VBOXDRVINST.EXE-7DCD6070.pf	17	Regular File	4/30/2021 12:59:54...
VBOXTRAY.EXE-1D286C83.pf	9	Regular File	4/30/2021 1:00:49 ...

Custom Content Sources

Evidence:File System Path File	Options
DiskDrigger.ad1:Custom Content Im...	Exact

Properties Hex Value In... Custom Con...

Cursor pos = 0

Vậy số lần chạy ở đây sẽ là 0

Q6. What is the suspect's email address?

Ở đây họ hỏi về Địa chỉ email của nghi phạm là gì. Em đã check file History và thấy được rằng mail của kẻ xâm nhập là

DB Browser for SQLite - C:\Users\DangLong\Desktop\66-Africanfalls\History

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Open Project Save Project Attach Database Close Database

Database Structure Browse Data Edit Pragma Execute SQL

Table: urls

	id	url	title	visit_count	typed_count	last_visit_time
91	91	https://github.com/danielmiessler/...	SecLists/Passwords at master · danielmiessler/SecLists · GitHub	2	0	13264193914183229
92	92	https://github.com/danielmiessler/...	SecLists/Passwords/Common-Credentials at master · danielmiessler/SecList...	4	0	13264193998054173
93	93	https://github.com/danielmiessler/...	SecLists/10-million-password-list-top-100.txt at master · danielmiessler/...	6	0	13264193985394190
94	94	https://github.com/danielmiessler/...		1	0	13264193929817248
95	95	https://raw.githubusercontent.com/...		1	0	13264193929817248
96	96	https://github.com/danielmiessler/...	File Finder · GitHub	2	0	13264193957137808
97	97	https://github.com/danielmiessler/...	SecLists/10-million-password-list-top-1000000.txt at master · danielmiessler...	3	0	13264194013047881
98	98	https://github.com/danielmiessler/...		1	0	13264194009326378
99	99	https://raw.githubusercontent.com/...		1	0	13264194009326378
100	100	http://youtube.com/	YouTube	1	0	13264198947390342
101	101	https://youtube.com/	YouTube	1	1	13264198947390342
102	102	https://www.youtube.com/	YouTube	1	0	13264198947390342
103	103	https://www.google.com/search?...	7zip - Google Search	2	0	13264218178171258
104	104	https://www.7-zip.org/download.html	Download	1	0	13264218178968584
105	105	http://protonmail.com/	Secure email: ProtonMail is free encrypted email.	1	0	13264218272450916
106	106	https://protonmail.com/	Secure email: ProtonMail is free encrypted email.	1	1	13264218272450916
107	107	https://mail.protonmail.com/login	Login ProtonMail	1	0	13264218277482120
108	108	https://mail.protonmail.com/inbox	Inbox dreammaker82@protonmail.com ProtonMail	1	0	13264218311766873
109	109	https://mail.protonmail.com/inbox/...	Inbox dreammaker82@protonmail.com ProtonMail	1	0	13264218318593571
110	110	file:///C:/Users/John%20Doe/...	almanac-start-a-garden.pdf	1	0	13264218357192098
111	111	http://dfir.science/	Digital Forensic Science	1	0	13264218400247448
112	112	https://dfir.science/	Digital Forensic Science	1	1	13264218400247448
113	113	https://dfir.science/2020/12/Magnet-...	Magnet CTF Week 8 - Persistence in plain sight - Digital Forensic Science	1	0	13264218406522742

91 - 112 of 113

Go to: 1

Edit Database Cell

Mode: Text

1 inbox | dreammaker82@protonmail.com | ProtonMail

Type of data currently in cell: Text / Numeric
48 character(s)

Remote

Identity Select an identity to connect

DBHub.io Local Current Database

Name Last modified

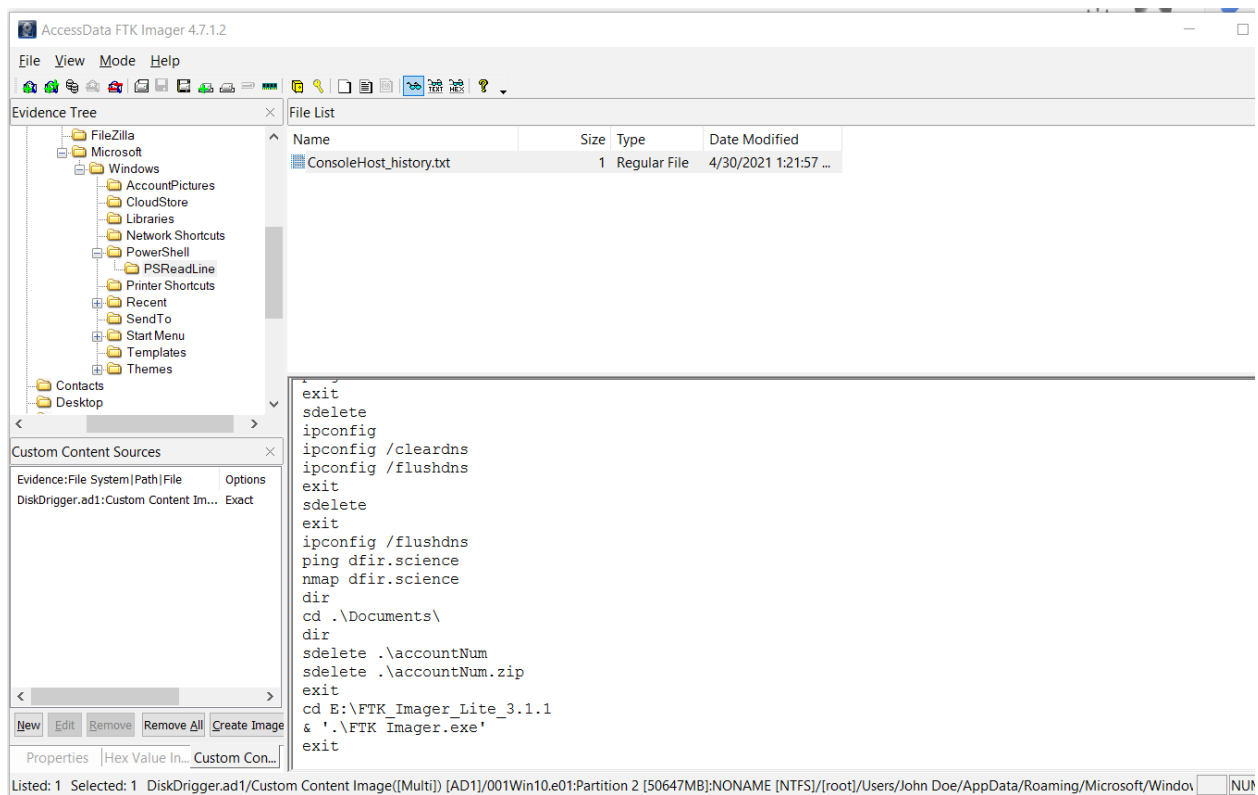
SQL Log Plot DB Schema Remote

UTF-8

Vậy đáp án của câu này là: dreammaker82@protonmail.com

Q7. What is the FQDN did the suspect port scan?

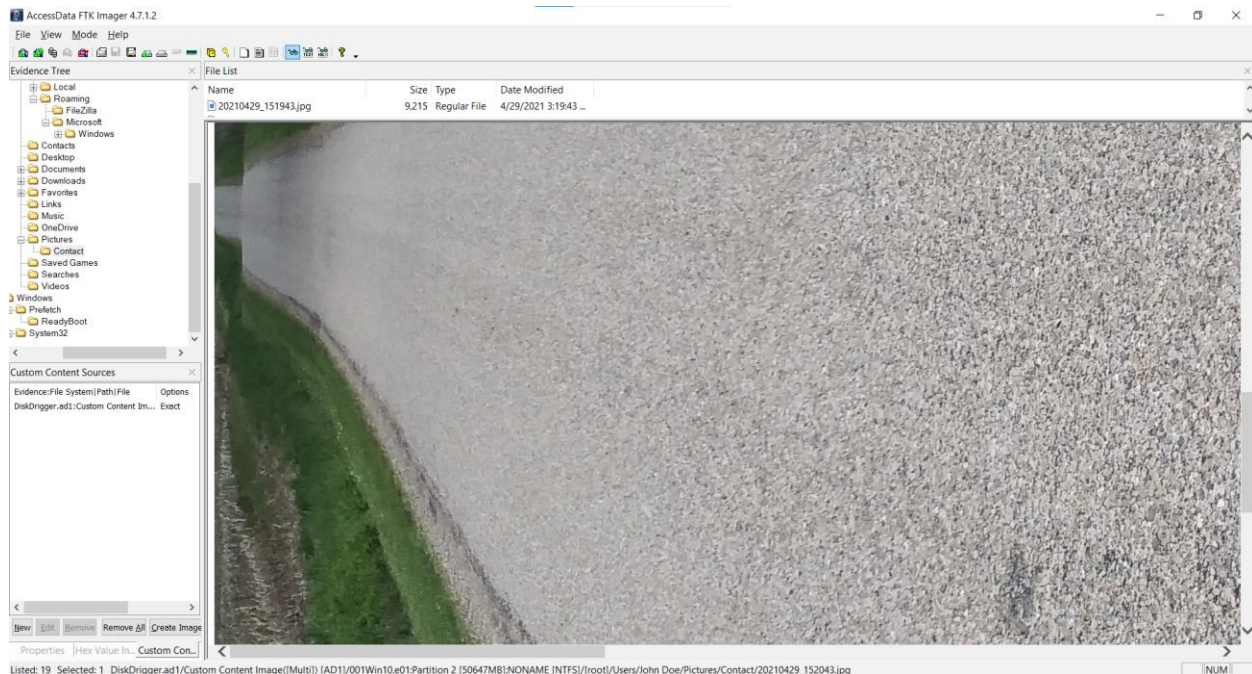
Đề quét mat công, nghi phạm phải sử dụng Công cụ dòng lệnh. Vì nghi phạm đang sử dụng Máy Windows nên rất có thể anh ta/cô ta đã sử dụng PowerShell. Có tệp ConsoleHost_history.txt trong thư mục Chuyển vùng của PowerShell.



Vậy đáp án của câu này là: dfir.science

Q8. What country was picture "20210429_152043.jpg" allegedly taken in?

Em sẽ tìm tới cái ảnh 20210429_152043.jpg tron thư mục Pictue



Ở đây em đã tìm kiếm được bức ảnh này ở **Zambia**.

Q9. What is the parent folder name picture "20210429_151535.jpg" was in before the suspect copy it to "contact" folder on his desktop?

Sau khi đọc 1 số thông tin của file thì em thấy bức ảnh này đã được. Chụp bằng LG Electronics.

Cái này rất đơn giản là ảnh sẽ được nằm ở Camera rồi.

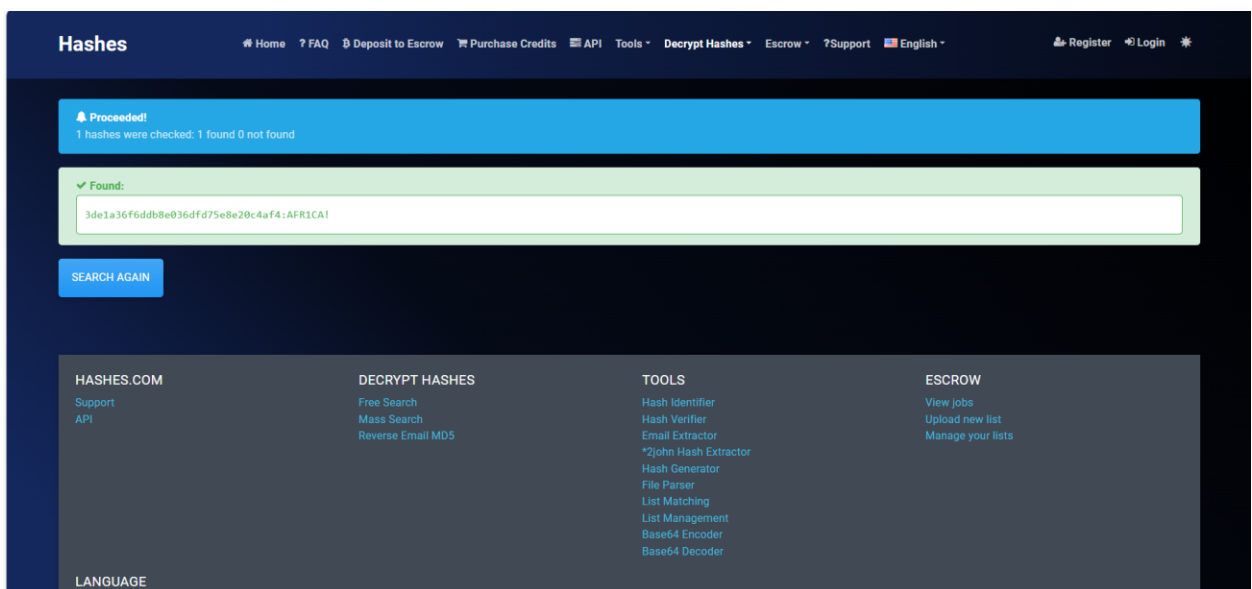
Q10. A Windows password hashes for an account are below. What is the user's password?

Anon:1001:aad3b435b51404eeaad3b435b51404ee:3DE1A36F6DDB8E036DFD75E8E20C4AF4:::

Ở đây em sẽ phân tích 1 chút

- **Anon:** Đây là tên người dùng.

- **1001**: Đây là RID (Relative Identifier) của người dùng. RID 1001 thường là của tài khoản người dùng đầu tiên được tạo sau khi tài khoản quản trị viên mặc định (500).
- **aad3b435b51404eeaad3b435b51404ee**: Đây là hash LM của mật khẩu. Nếu giá trị này là aad3b435b51404eeaad3b435b51404ee, điều đó có nghĩa là mật khẩu không được lưu dưới dạng hash LM (LM hash được tắt).
- **3DE1A36F6DDB8E036DFD75E8E20C4AF4**: Đây là hash NTLM của mật khẩu.
- **::::** Các trường bổ sung thường không có giá trị và được để trống.



Vậy đáp án của câu này là **AFR1CA!**

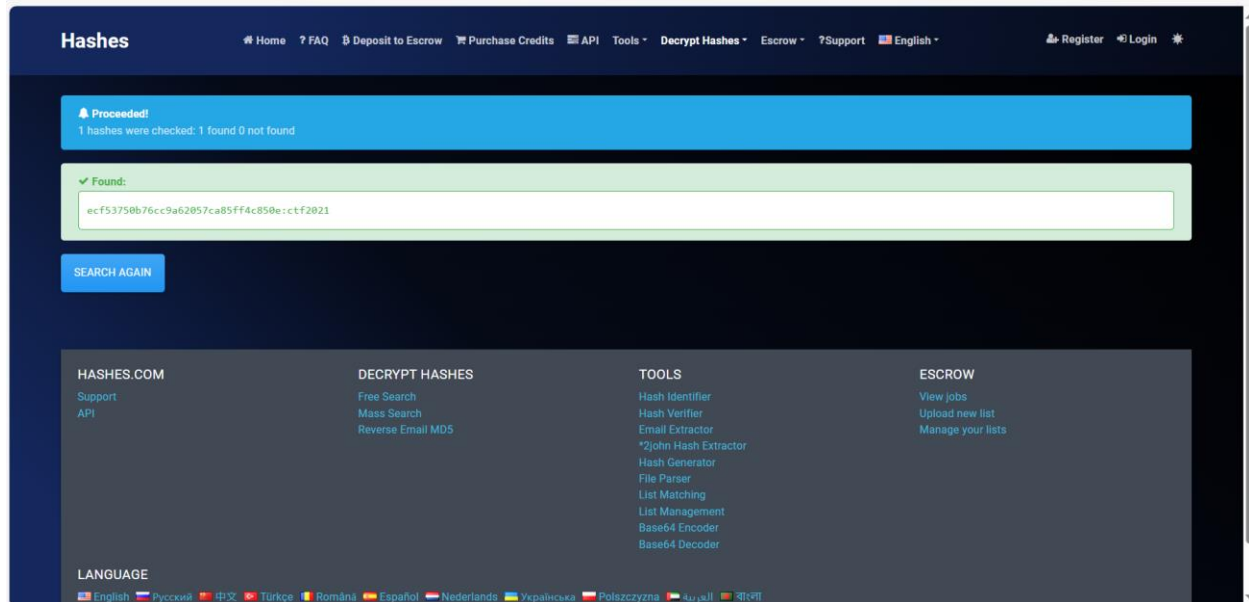
Q11. What is the user "John Doe's" Windows login password?

Sau đó kết xuất các giá trị băm bằng cách sử dụng impacket. Em sẽ dump 4 file ra
SYSTEM SOFTWARE SAM SECURITY

Sau đó em sẽ dump ra được 1 file như này

```
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:69dbee1a98d4f53fbccb1fe5ce37c851:::  
John Doe:1001:aad3b435b51404eeaad3b435b51404ee:ecf53750b76cc9a62057ca85ff4c850e:::' > ntlm.txt
```

Lúc này em sẽ ném nó vào một công cụ trực tuyến, bắt đầu với Hashes.com và xem rằng em có gặp may mắn nữa không, điều mà em đã làm được ở câu trước hay không. Và



Vậy đáp án của câu này là ctf2021