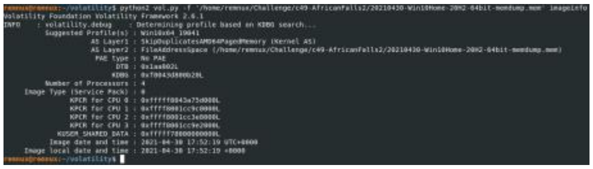
Brave Challenge

A memory image was taken from a seized Windows machine. As a security blue team analyst, analyze the image and answer the provided questions.

Task 1:
What time was the RAM image acquired according to the suspect system? (YYYY -MM-DD HH:MM:SS)

I used the imageinfo

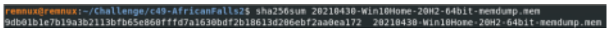


```
remnux@remnux:~/volatility$ python2 vol.py -f '/home/remnux/Challenge/c49-AfricanFalls2/20210430-Win10Home-20H2-64bit-memdump.mem' imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win10x64_19041
                     AS Layer1 : SkipDuplicatesAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/remnux/Challenge/c49-AfricanFalls2/20210430-Win10Home-20H2-64bit-memdump.mem)
                      PAE type : No PAE
                           DTB : 0x1aa002L
                          KDBG : 0xf8043d800b20L
          Number of Processors : 4
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0xfffff8043a75d000L
                KPCR for CPU 1 : 0xffff8001cc9c0000L
                KPCR for CPU 2 : 0xffff8001cc3e0000L
                KPCR for CPU 3 : 0xffff8001cc9e2000L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2021-04-30 17:52:19 UTC+0000
     Image local date and time : 2021-04-30 17:52:19 +0000
remnux@remnux:~/volatility$ 
```

Answer: 2021-04-30 17:52:19

Task 2:
What is the SHA256 hash value of the RAM image?

I used the sha256sum command

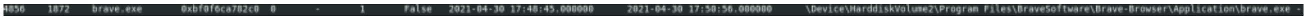


```
remnux@remnux:~/Challenge/c49-AfricanFalls2$ sha256sum 20210430-Win10Home-20H2-64bit-memdump.mem
9db01b1e7b19a3b2113bfb65e860fffd7a1630bdf2b18613d206ebf2aa0ea172  20210430-Win10Home-20H2-64bit-memdump.mem
```

Answer: 9db01b1e7b19a3b2113bfb65e860fffd7a1630bdf2b18613d206ebf2aa0ea172

Task 3:
What is the process ID of "brave.exe"?

I used the pstree plugin

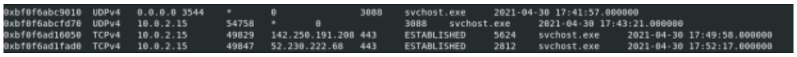


```
4856    1872    brave.exe       0xbf0f6ca782c0  0       -       1       False   2021-04-30 17:48:45.000000      2021-04-30 17:50:56.000000      \Device\HarddiskVolume2\Program Files\BraveSoftware\Brave-Browser\Application\brave.exe -
```

Answer: 4856

Task 4:
How many established network connections were there at the time of acquisition? (number)

I used the netscan plugin and counted the "ESTABLISHED"

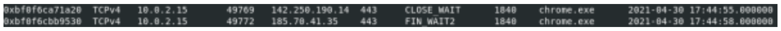


```
0xbf0f6abc9010  UDPv4   0.0.0.0 3544    *       0               3088    svchost.exe     2021-04-30 17:41:57.000000
0xbf0f6abcfd70  UDPv4   10.0.2.15       54758   *       0               3088    svchost.exe     2021-04-30 17:43:21.000000
0xbf0f6ad16050  TCPv4   10.0.2.15       49829   142.250.191.208 443     ESTABLISHED     5624    svchost.exe     2021-04-30 17:49:58.000000
0xbf0f6ad1fad0  TCPv4   10.0.2.15       49847   52.230.222.68   443     ESTABLISHED     2812    svchost.exe     2021-04-30 17:52:17.000000
```

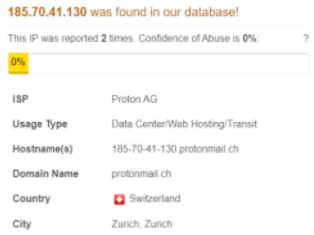
Answer: 10

Task 5:
What FQDN does Chrome have an established network connection with?

I checked the IP 185.70.41.130 on AbuseIPDB to find the domain name



```
0xbf0f6ca71a20  TCPv4   10.0.2.15       49769   142.250.190.14  443     CLOSE_WAIT      1840    chrome.exe      2021-04-30 17:44:55.000000
0xbf0f6cbb9530  TCPv4   10.0.2.15       49772   185.70.41.35    443     FIN_WAIT2       1840    chrome.exe      2021-04-30 17:44:58.000000
```



185.70.41.130 was found in our database!

This IP was reported **2** times. Confidence of Abuse is **0%**: ?

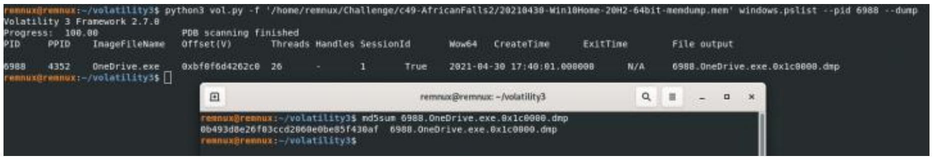
0%

ISP	Proton AG
Usage Type	Data Center/Web Hosting/Transit
Hostname(s)	185-70-41-130.protonmail.ch
Domain Name	protonmail.ch
Country	🇨🇭 Switzerland
City	Zurich, Zurich

Answer: protonmail.ch

Task 6:
What is the MD5 hash value of process executable for PID 6988?

I dumped the process with pslist and checked the MD5



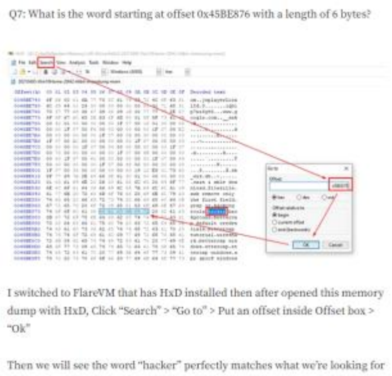
```
remnux@remnux:~/volatility3$ python3 vol.py -f '/home/remnux/Challenge/c49-AfricanFalls2/20210430-Win10Home-20H2-64bit-memdump.mem' windows.pslist --pid 6988 --dump
Volatility 3 Framework 2.7.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

6988    4352    OneDrive.exe    0xbf0f6d4262c0  26      -       1       True    2021-04-30 17:40:01.000000      N/A     6988.OneDrive.exe.0x1c0000.dmp
remnux@remnux:~/volatility3$ 
```

```
remnux@remnux:~/volatility3$ md5sum 6988.OneDrive.exe.0x1c0000.dmp
0b493d8e26f03ccd2060e0be85f430af  6988.OneDrive.exe.0x1c0000.dmp
remnux@remnux:~/volatility3$
```

Answer: 0b493d8e26f03ccd2060e0be85f430af

Task 7:
What is the word starting at offset 0x45BE876 with a length of 6 bytes?

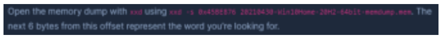
First I dumped the process and opened it with HxD and I tried to find the hex but it didnt and I already know this is the way to find it.
I also watched the walkthrough which says this is the way to find the answer


Q7: What is the word starting at offset 0x45BE876 with a length of 6 bytes?

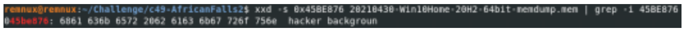
I switched to FlareVM that has HxD installed then after opened this memory dump with HxD, Click "Search" > "Go to" > Put an offset inside Offset box > "Ok"

Then we will see the word "hacker" perfectly matches what we're looking for

So I used the hint to see their way to find it


Open the memory dump with xxd using xxd -s 0x45BE876 20210430-Win10Home-20H2-64bit-memdump.mem. The next 6 bytes from this offset represent the word you're looking for.

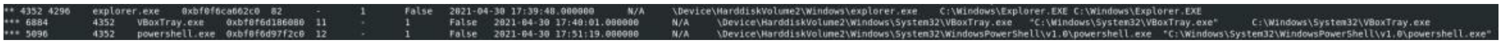
I used the command "xxd -s 0x45BE876 20210430-Win10Home-20H2-64bit-memdump.mem | grep -i
45BE876"
and also grepped for "45BE876"


```
remnux@remnux:~/Challenge/c49-AfricanFalls2$ xxd -s 0x45BE876 20210430-Win10Home-20H2-64bit-memdump.mem | grep -i 45BE876
045be876: 6861 636b 6572 2062 6163 6b67 726f 756e  hacker backgroun
```

Answer: hacker

Task 8:
What is the creation date and time of the parent process of "powershell.exe"? (YYYY -MM-DD
HH:MM:SS)

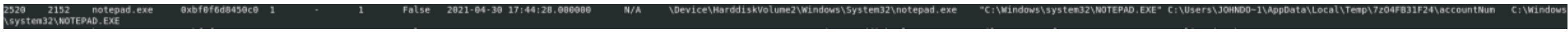
I used the pstree plugin and found the parent process of the powershell.exe


```
** 4352 4296    explorer.exe    0xbf0f6ca662c0  82      -       1       False   2021-04-30 17:39:48.000000      N/A     \Device\HarddiskVolume2\Windows\explorer.exe    C:\Windows\Explorer.EXE C:\Windows\Explorer.EXE
*** 6884        4352    VBoxTray.exe    0xbf0f6d186080  11      -       1       False   2021-04-30 17:40:01.000000      N/A     \Device\HarddiskVolume2\Windows\System32\VBoxTray.exe   "C:\Windows\System32\VBoxTray.exe"      C:\Windows\System32\VBoxTray.exe
*** 5096        4352    powershell.exe  0xbf0f6d97f2c0  12      -       1       False   2021-04-30 17:51:19.000000      N/A     \Device\HarddiskVolume2\Windows\System32\WindowsPowerShell\v1.0\powershell.exe  "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
```

Answer: 2021-04-30 17:39:48

Task 9:
What is the full path and name of the last file opened in notepad?

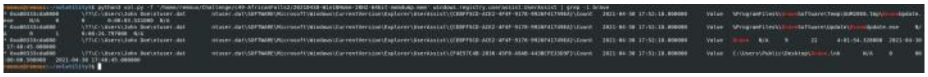
I used the pstree plugin and found the Notepad process with the path


```
2520    2152    notepad.exe     0xbf0f6d8450c0  1       -       1       False   2021-04-30 17:44:28.000000      N/A     \Device\HarddiskVolume2\Windows\System32\notepad.exe    "C:\Windows\system32\NOTEPAD.EXE" C:\Users\JOHNDO~1\AppData\Local\Temp\7zO4FB31F24\accountNum   C:\Windows
\system32\NOTEPAD.EXE
```

Answer: C:\Users\JOHNDO~1\AppData\Local\Temp\7zO4FB31F24\accountNum

Task 10:
How long did the suspect use Brave browser? (hh:mm:ss)

I used the windows.registry.userassist.UserAssist plugin and grepped for brave


```
remnux@remnux:~/volatility3$ python3 vol.py -f '/home/remnux/Challenge/c49-AfricanFalls2/20210430-Win10Home-20H2-64bit-memdump.mem' windows.registry.userassist.UserAssist | grep -i brave
* 0xad0333cda000        \??\C:\Users\John Doe\ntuser.dat        ntuser.dat\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count   2021-04-30 17:52:18.000000      Value   %ProgramFiles%\BraveSoftware\Temp\GUM2888.tmp\BraveUpdate.
exe     N/A     0       0       0:00:03.331000  N/A
* 0xad0333cda000        \??\C:\Users\John Doe\ntuser.dat        ntuser.dat\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count   2021-04-30 17:52:18.000000      Value   %ProgramFiles%\BraveSoftware\Update\BraveUpdate.exe     N/
A       0       1       0:00:24.797000  N/A
* 0xad0333cda000        \??\C:\Users\John Doe\ntuser.dat        ntuser.dat\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count   2021-04-30 17:52:18.000000      Value   Brave   N/A     9       22      4:01:54.328000  2021-04-30
 17:48:45.000000
* 0xad0333cda000        \??\C:\Users\John Doe\ntuser.dat        ntuser.dat\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}\Count   2021-04-30 17:51:18.000000      Value   C:\Users\Public\Desktop\Brave.lnk       N/A     0       00
:00:09.500000   2021-04-30 17:48:45.000000
remnux@remnux:~/volatility3$
```

Answer: 04:01:54