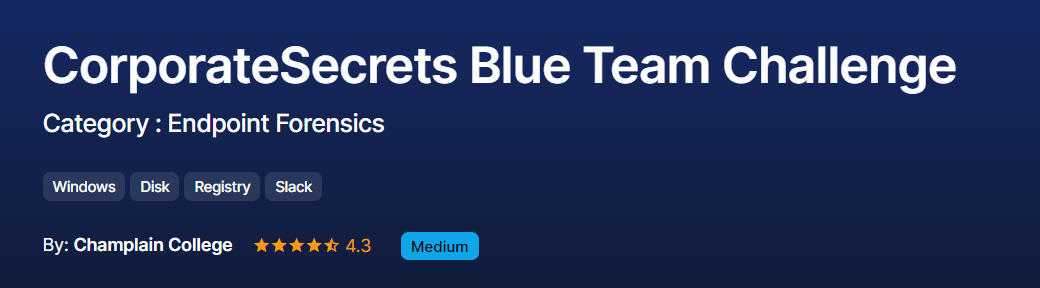
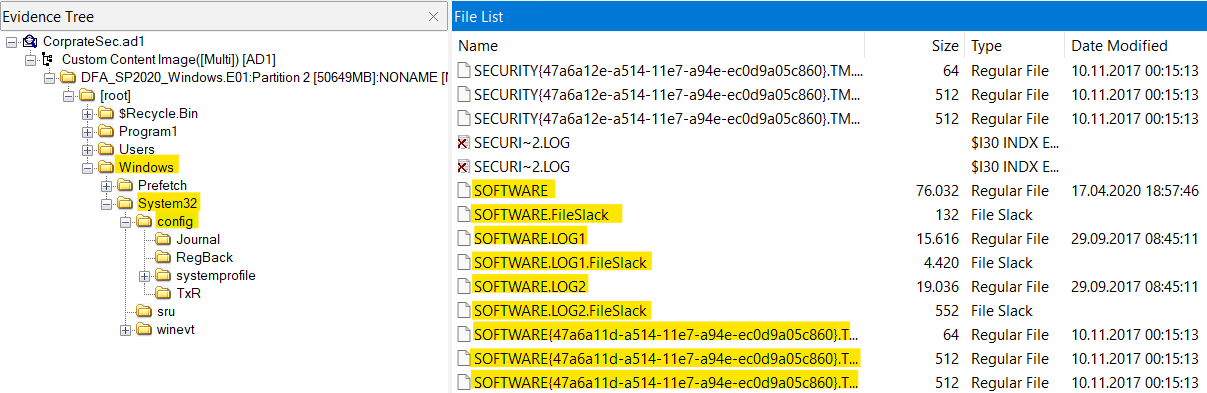
**CorporateSecrets Blue Team Challenge**



**SORU 1**

“What is the current build number on the system?”

Sistemdeki mevcut yapı numarası soruluyor. Bunu \SOFTWARE\Microsoft\Windows\CurrentVersion altında bulacağımı biliyorum.

İlk olarak software hive’ını export ediyorum.

Daha sonra Registry explorer’da incelememe devam ediyorum.

Software hive’ını ekledikten sonra *\Microsoft\Windows\CurrentVersion* dizinine gidiyorum ve aradığım sonuca ulaşıyorum.

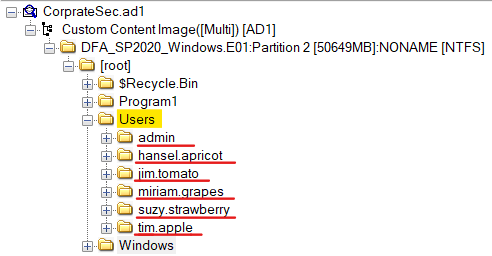


**CEVAP = 16299**

**SORU 2**

“How many users are there?”

Burada kaç kullanıcı olduğu soruluyor.



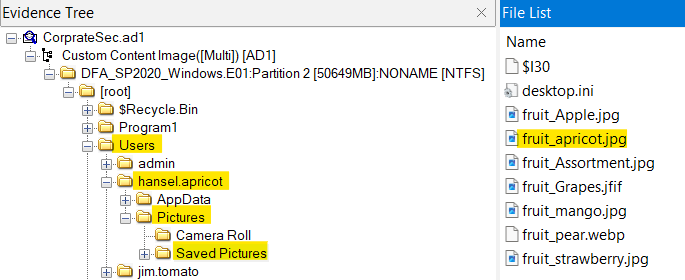
Users altında 6 adet kullanıcı olduğunu görüyorum.

**CEVAP = 6**

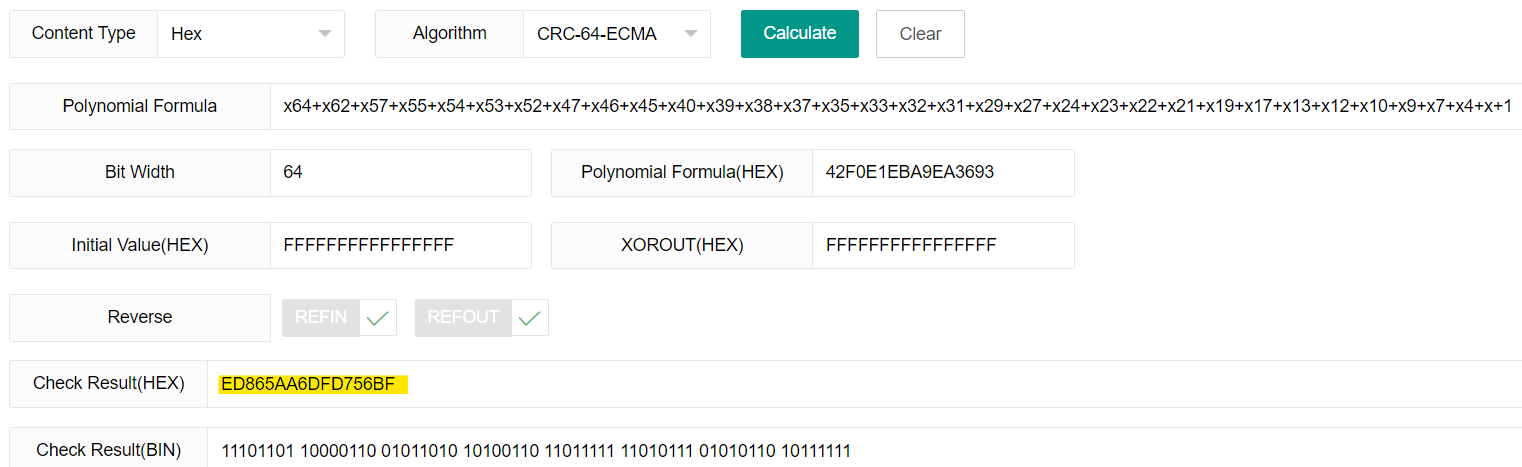
**SORU 3**

“What is the CRC64 hash of the file "fruit\_apricot.jpg"?”

Yukarıda verilen jpg dosyasının CRC64 hash’i isteniyor. Bunun için öncelikle bu jpg dosyasını buluyorum.



Jpg dosyasını export ediyorum ve online bir CRC64 hash hesaplayan websitesi buluyorum. Daha sonra jpg dosyamı upload ediyorum ve bizden istenilen değere ulaşıyorum.

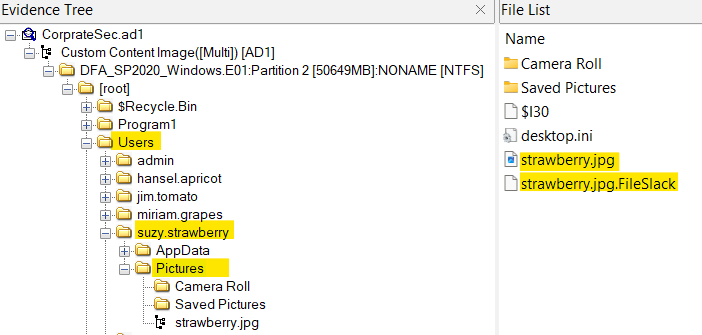


**CEVAP = ED865AA6DFD756BF**

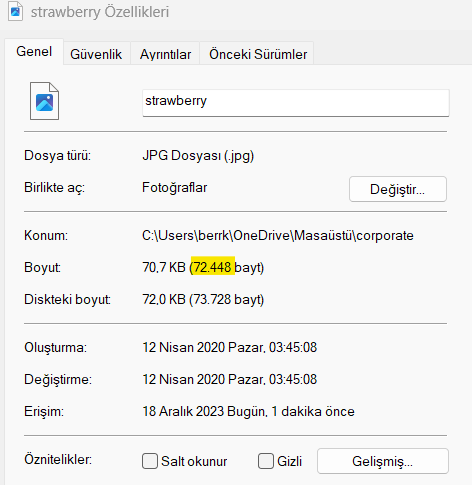
**SORU 4**

“What is the logical size of the file "strawberry.jpg" in bytes?”

Verilen jpg dosyasının mantıksal boyutu isteniyor. Yine ilk olarak jpg dosyasını buluyorum.



Export ediyorum ve jpg dosyasınız özelliklerini kontrol ediyorum. Ve aradığım sonuca ulaşıyorum.



**CEVAP = 72448**

**SORU 5**

“What is the processor architecture of the system? (one word)”

Sistemin işlemci mimarisi soruluyor. Bunu SYSTEM hive’ı içinde aracağımı biliyorum. Ufak bir araştırma ile [*system/ControlSet001/Control/Session Manager/Environment/*](http://system/ControlSet001/Control/Session%20Manager/Environment/) altında tutulduğunu öğreniyorum.

FTK’da *windows/system32/config* altında bulunan SYSTEM hive’ını export ediyorum ve Registry Explorer’da açıyorum. Bulduğum dizini kontrol ediyorum.

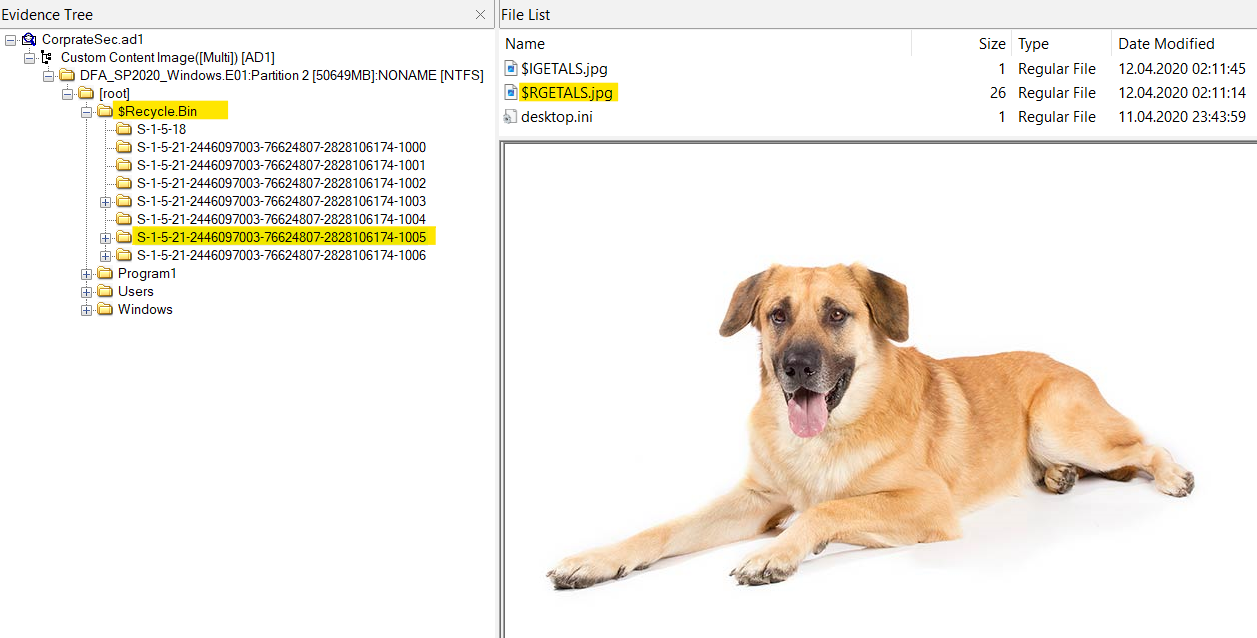


**CEVAP = AMD64**

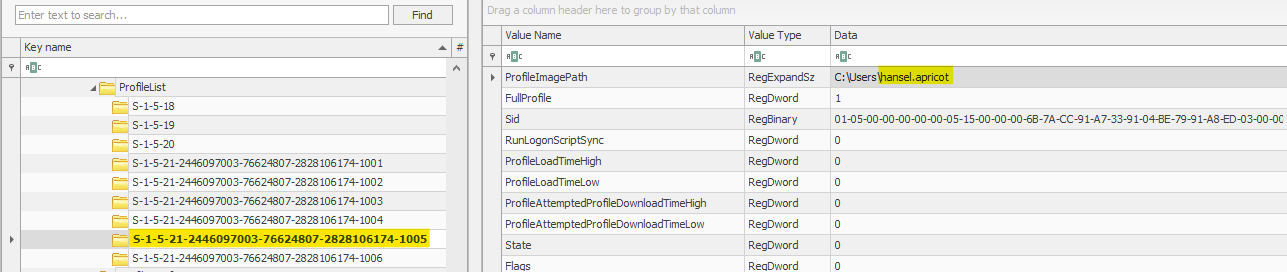
**SORU 6**

“Which user has a photo of a dog in their recycling bin?”

Hangi kullanıcının geri dönüşüm kutusunda köpek fotoğrafı olduğunu bulmamız isteniyor. Recycle.Bin’i kurcalıyorum ve köpek resmini ve hangi SID’nin sildiğini görüyorum.

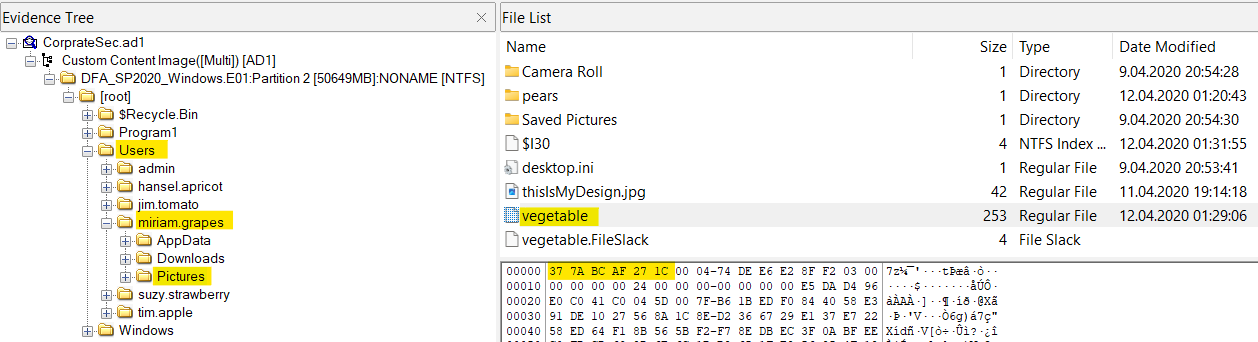


Sırada bu SID’nin hangi kullanıcıya ait olduğunu bulmak kalıyor. Bunu software hive’ı içerisinde bulacağımı biliyorum. *\Microsoft\Windows NT\CurrentVersion\ProfileList*

**CEVAP = hansel.apricot**

**SORU 7**

“What type of file is "vegetable"? Provide the extension without a dot.”

"vegetable" ın ne tür bir dosya olduğunu istiyor. İlk olarak dosyanın nerede olduğunu buluyorum.

*Users\miriam.grapes\Pictures*

Dosya imzasını alıyoruz ve hangi tür olduğunu bulmaya çalışıyoruz. hex siganature 37 7A BC AF 27 1C arıyorum ve sonucu buluyorum.



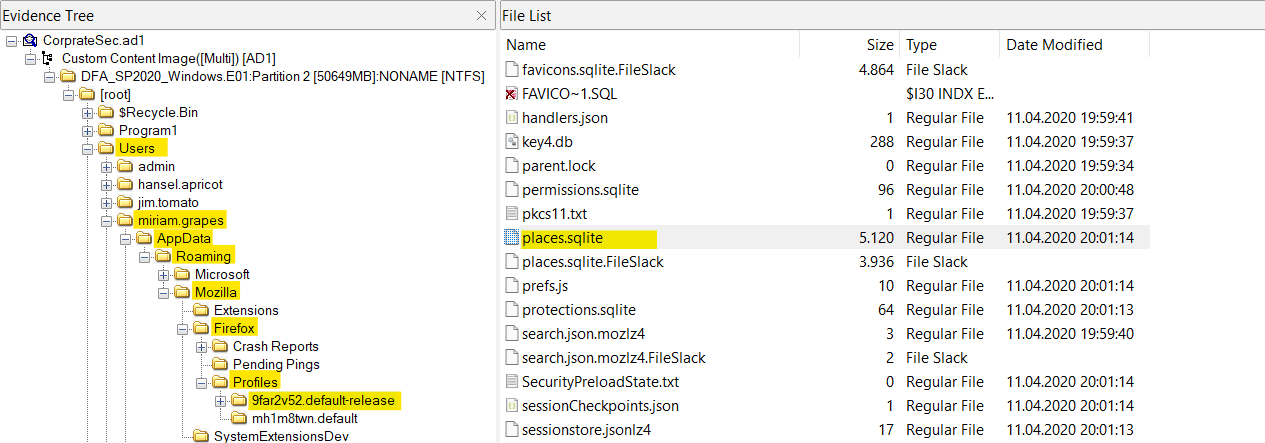
**CEVAP = 7z**

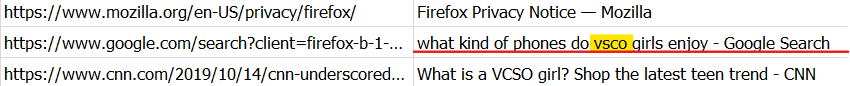
**SORU 8**

“What type of girls does Miriam Grapes design phones for (Target audience)?”

Miriam Grapes’ın ne tür kızlar için telefon tasarladığını bulmamızı istiyor. Bu soruda biraz takılıyorum ve ipuçlarından faydalanıyorum.

İpucunda verilen dizine gidiyorum ve sqlite dosyasını export ediyorum.



Daha sonra export ettiğim dosyayı sqlite ile açıp inceliyorum.

Vsco kızları ne tür telefonlardan hoşlanır diye bir arama yaptığını görüyorum ve böylelikle cevabımızı buluyorum.

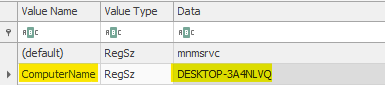
**CEVAP = VSCO**

**SORU 9**

“What is the name of the device?”

Cihazın adını bulamamız isteniyor. Bunu SYSTEM hive’ı içerisinde controlset içerisinde bulacağımı biliyorum.

*ControlSet001/Control/ComputerName/ComputerName*



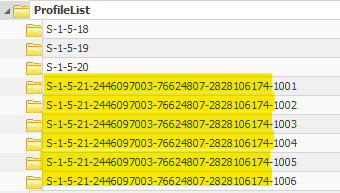
**CEVAP = DESKTOP-3A4NLVQ**

**SORU 10**

“What is the SID of the machine?”

Makinenin SID’si isteniyor. Bunu software hive’ı içerisinde bulacağımı biliyorum. *\Microsoft\Windows NT\CurrentVersion\ProfileList*

SID’lerin Son 4 hanesi hariç diğer kısım makinenin SID’sini temsil eder. Son 4 işin içine giirnce kullanıcı SID’leri olur.

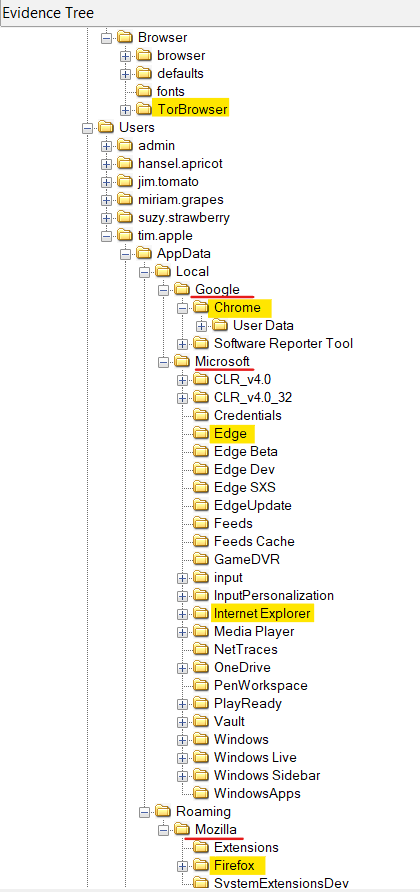


**CEVAP = S-1-5-21-2446097003-76624807-2828106174**

**SORU 11**

“How many web browsers are present?”

Kaç tane web tarayıcısının olduğunu bulmamızı istiyor.



Mozilla Firefox, Internet Explorer, Edge , Chrome Ve TorBrowser

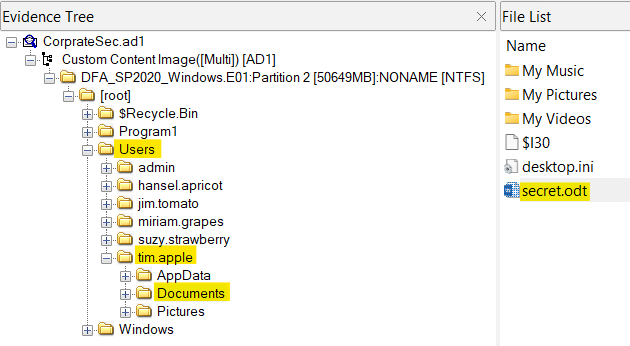
5 adet Web tarayıcısı bulunuyor.

**CEVAP = 5**

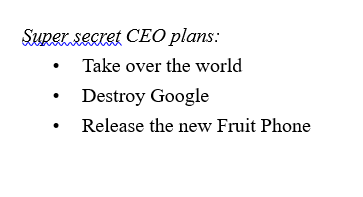
**SORU 12**

“How many super secret CEO plans does Tim have? (Dr. Doofenshmirtz Type Beat)”

Tim’in kaç tane süper gizli CEO planı olduğunu soruyor. İlk olarak Tim kullanıcısı altındaki dosyaları inceliyorum ve Documents altında secret.odt adında bir dosya buluyorum.



Bulduğum bu dosyayı export ediyorum ve açıyorum.



İçerisinde super secret CEO plan altında 3 madde olduğunu görüyorum. Fakat cevabı 3 olarak kabul etmiyor. Dosyayı daha detaylı inceliyorum ve yazı rengini değiştiriyorum.



Gizli bir madde daha olduğunu görüyorum. Böylelikle süper gizli 4 plan olduğunu görüyorum.

**CEVAP = 4**

**SORU 13**

“Which employee does Tim plan to fire? (He's Dead, Tim. Enter the full name - two words - space separated)”

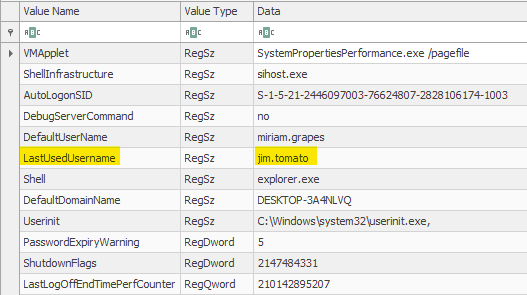
Tim’in hangi çalışanı kovmak istediğini bulmamız isteniyor. Tim’in gizli CEO planları arasında Jim Tomato’yu kovmak bulunuyor.

**CEVAP = Jim Tomato**

**SORU 14**

“What was the last used username? (I didn't start this conversation, but I'm ending it!)”

En son kullanılan kullanıcı adı isteniyor. Bunun için *SOFTWARE/Microsoft/Windows NT/CurrentVersion/Winlogon* dizinine bakıyorum ve default kullanıcı ve en son giriş yapan kullanıcı yer alıyor.



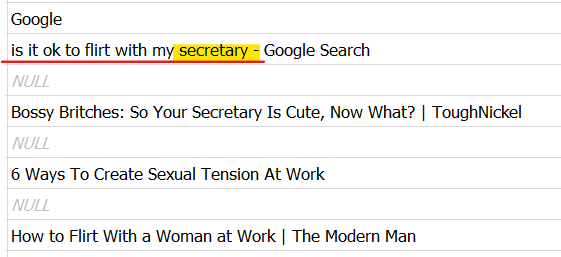
Böylelikle cevaba ulaşmış oluyoruz.

**CEVAP = jim.tomato**

**SORU 15**

“What was the role of the employee Tim was flirting with?”

Tim’in flört ettiği çalışanın rolü isteniyor. Yine export ettiğimiz sqlite dosyası içerisinde ara geçmişine baktığımızda Tim’in Sekreteriyle flört etmek için google’dan yardım aldığını görüyoruz.



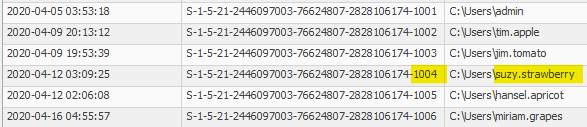
**CEVAP = Secretary**

**SORU 16**

“What is the SID of the user "suzy.strawberry"?”

suzy.strawberry kullanıcısının SID’si isteniyor. Nerde bulacağımızı artık biliyoruz.

*SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList*



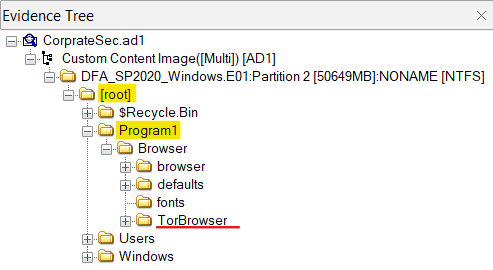
SID formatında son 4 hanenin kullanıcıya özel olduğunu biliyoruz.

**CEVAP = 1004**

**SORU 17**

List the file path for the install location of the Tor Browser.

Tor tarayıcısının kurulum dosyalarının path’i soruluyor.



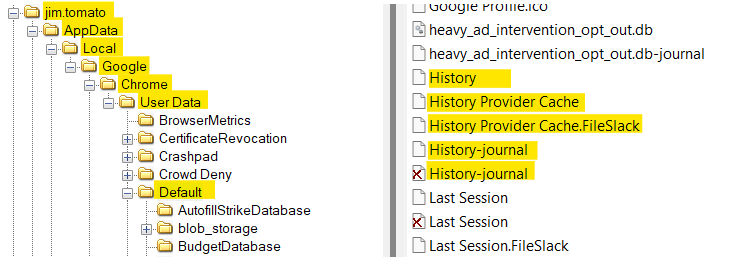
FTK imager üzerinde yaptığım incelemede TorBrowser dosyasını buluyorum.

**CEVAP = c:\Program1**

**SORU 18**

“What was the URL for the Youtube video watched by Jim?”

Burada bizden Jim’in izlediği youtube videosunun URL’si isteniyor. Bunun için Jim’in Browser geçmişini export edip inceliyoruz. Ben tüm history dosyalarını export ediyorum.



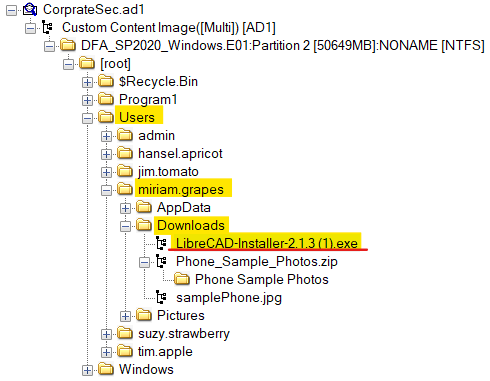
Daha sonra sqlite ile açıp url tablosunu inceliyorum ve aradığım sonuca ulaşıyorum.

**CEVAP = https://www.youtube.com/watch?v=Y-CsIqTFEyY**

**SORU 19**

“Which user installed LibreCAD on the system?”

LibreCAD’ın hangi kullanıcı tarafından yüklendiğini bulamamız isteniyor. Bunun için kullanıcıların Download klasörlerini kontrol ediyorum.



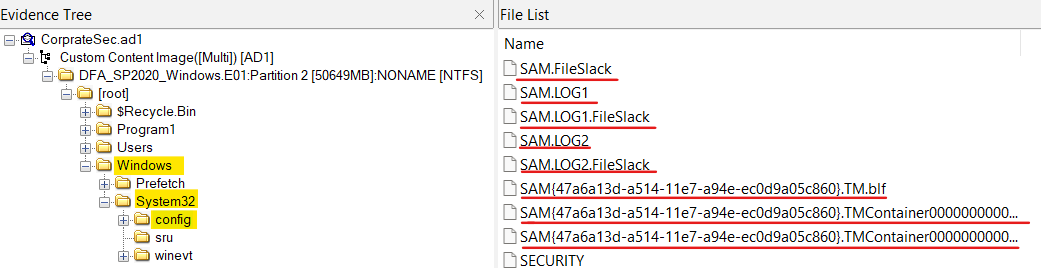
Ve aradığım uygulamaya miriam.grapes kullanıcısı altındaki Download klasöründe buluyorum.

**CEVAP = miriam.grapes**

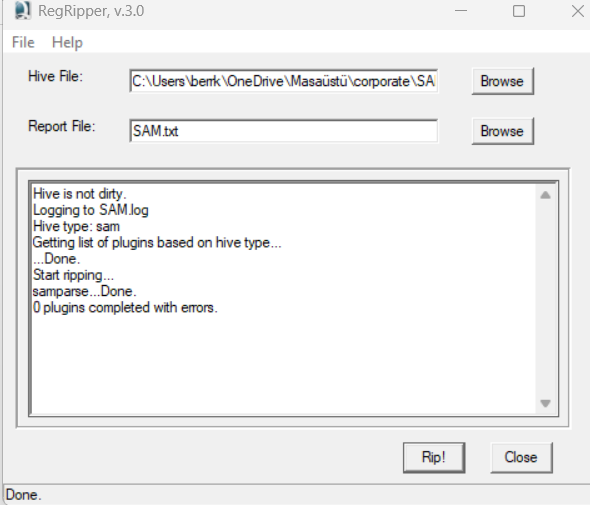
**SORU 20**

“How many times "admin" logged into the system?”

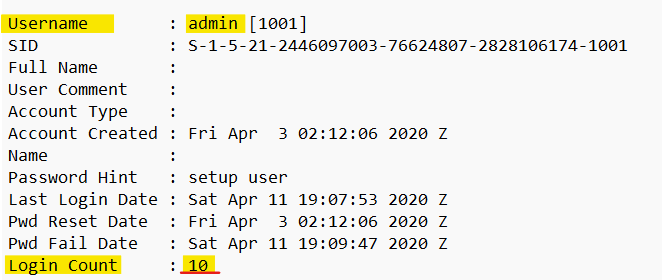
Sisteme kaç kez admin olarak giriş yapıldığı soruluyor. Bununiçin SAM dosyalarını FTK’dan export ediyorum.



Daha sonra export ettiğim SAM dosyasını RegRipper aracına veriyorum ve bana bir txt çıktısı veriyor.



Aracın bana verdiği çıktıyı incelediğim zaman admin kullanıcısının sisteme kaç kere giriş yaptığını, en son ne zaman giriş yaptığını, SID bilgisini ve buna benzer birçok bilgiye erişiyorum.

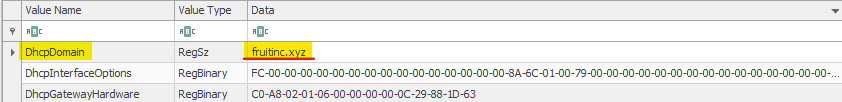


**CEVAP = 10**

**SORU 21**

“What is the name of the DHCP domain the device was connected to?”

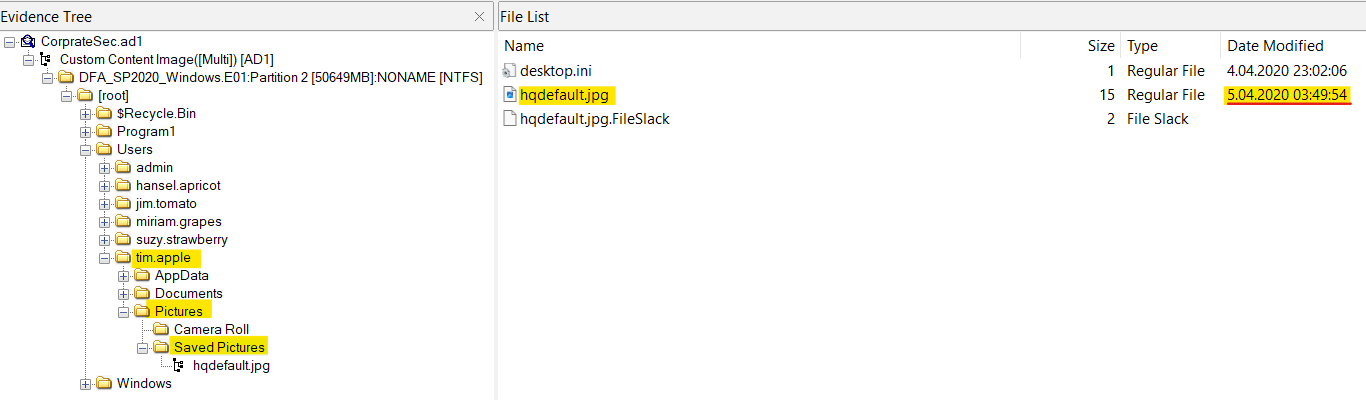
Cihazın bağlı olduğu DHCP domain’in adı soruluyor. Bunun için *system/ControlSet001 /Services/Tcpip/Parameters/Interfaces/* kontrol ediyoruz. Çünkü burası ağ ile ilgili bilgileri içerir.



**CEVAP = fruitinc.xyz**

**SORU 22**

“What time did Tim download his background image?”

Tim’in arka plan resmini saat kaçta indirdiğini bulmamız isteniyor. İlk olarak Tim’in arka plan resmini bularak başlıyoruz. Tim’in dosyalarını kontrol ettiğimde saved pictures altında bir jpg dosyası buluyorum.

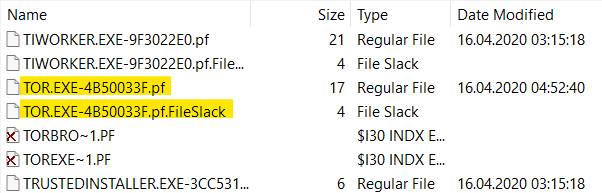
Tim’in dosyalarına baktığımda başka resm dosyasına denk gelmiyorum ve aradığım şeyin bu olduğunu düşünerek modify tarihini cevap olarak deniyorum. Soruda verilen formata dikkat ediyorum. Cevap doğru çıkıyor.

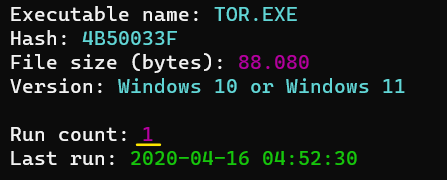
**CEVAP = 04/05/2020 03:49**

**SORU 23**

“How many times did Jim launch the Tor Browser?”

Tim kullanıcısının Tor tarayıcısını kaç kez başlattığını bulamamız isteniyor. Uygulamaların kaç kez başlatıldığı, en son ne zaman başlatıldığı gibi bilgilere .pf dosyalarından erişebiliyorduk. Pf dosyaları içerisinde Tor tarayıcı ile ilgili dosyaları export ediyorum.





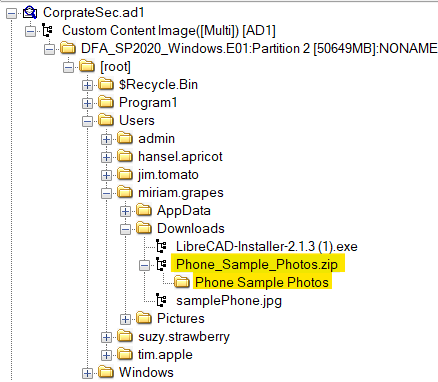
PECmd ile analiz ettiğimde borwser’ın bir kez çalıştığını görüyorum. Fakat cevap kabul edilmiyor. Kabul edilen cevap 2’dir.

**CEVAP = 2**

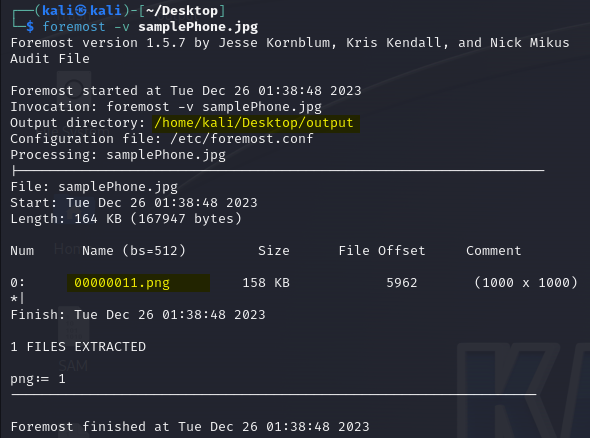
**SORU 24**

“There is a png photo of an iPhone in Grapes's files. Find it and provide the SHA-1 hash.”

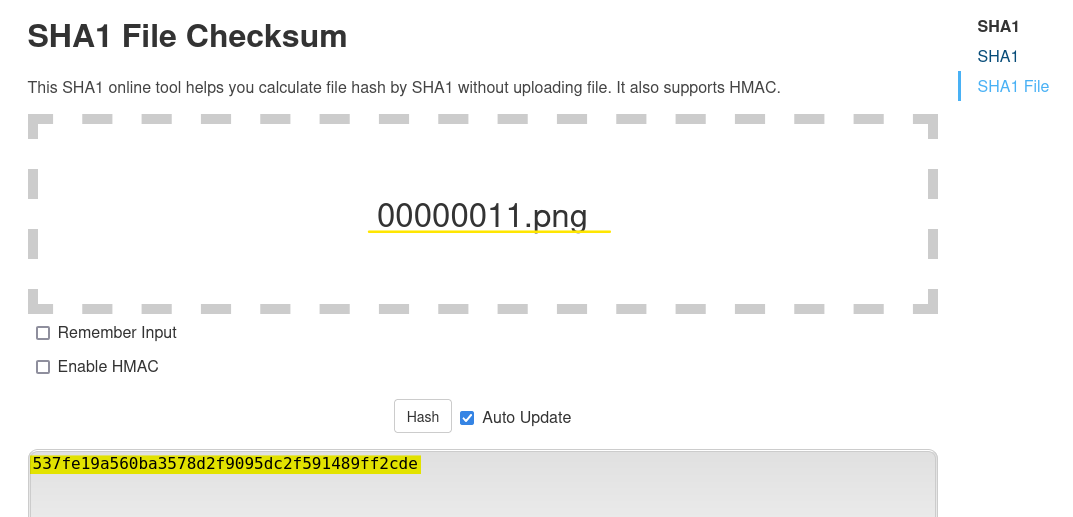
Grapes’ın dosyalırnda bir iphone png dosyası olduğunu söylüyor ve bu dosyanın SHA-1 karması isteniyor. Grapes’in dosyalarını kontrol ettiğimde herhangi bir png dosyası ile karşılaşmıyorum. Daha sonra ipuçlarından yardım alarak ilerliyorum. İpucunda bir dosyanın içeisinebirşeylerin saklanabileceğinden bahsediliyor. Ve downloads altındaki sample phone işaret ediliyor. Dosyayı export ediyorum ve içerisinde herhangi bir gizli dosya olup olmadığını inceliyorum.



Bu dosyanın içerisinden de bir jpg dosyası bulunuyor. Bu jpg ddosyasının içerisinde gizlenen bir şeyler olup olmadığını kontrol ediyorum. İlk olarak binwalk aracını deniyorum fakat bir sonuç alamıyorum. Daha sonra foremost aracı ile içerisinden bir png dosyası çıkarıyorum.



Daha sonra online dosya hash’i alan bir web sitesinde bulduğumuz png dosyasının hash’ini alarak bizden istenilen sonuca ulaşıyoruz.



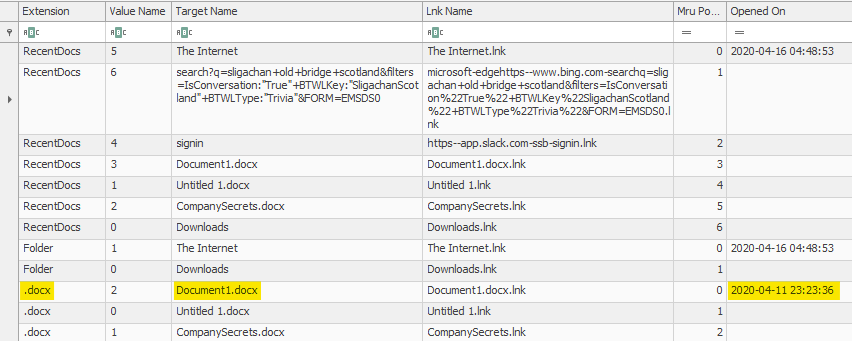
**CEVAP = 537fe19a560ba3578d2f9095dc2f591489ff2cde**

**SORU 25**

“When was the last time a docx file was opened on the device?”

Cihazda en son ne zaman docx dosyası açıldığını bulmamız isteniyor. Bu bilgiye genellikle NTUSER.DAT, USERCLASS.DAT ve AMCACHE hive’ları içerisinden erişebileceğimi biliyorum. NTUSER.DAT hive’ını daha önceden export etmiştik tekrar bu bilginin olabileceği dizini kontrol ediyorum ve bizden istenilen bilgiye ulaşıyorum.

*Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs*

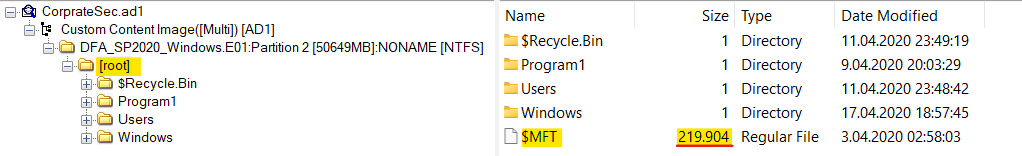


**CEVAP = 2020-04-11 23:23:36**

**SORU 26**

“How many entries does the MFT of the filesystem have?”

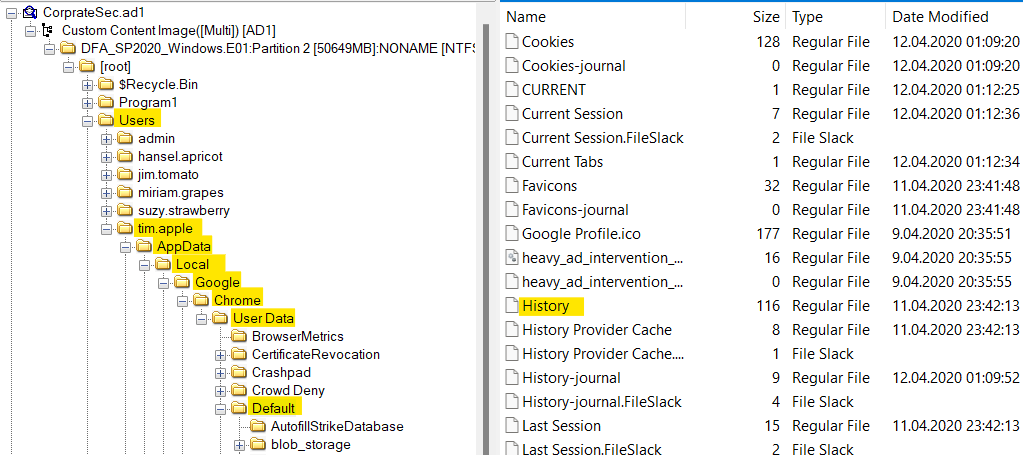
Dosya sisteminin MFT’sinde kaç giriş olduğu soruluyor.



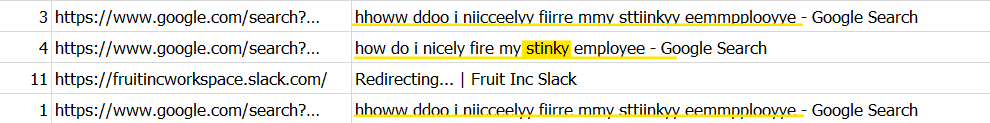
**CEVAP = 219.904**

**SORU 27**

“Tim wanted to fire an employee because they were ......?(Be careful what you wish for)”

Tim bir çalışanı kovamak istemiş bunun nedenini bulmamız isteniyor. Bunu Tim’in browser geçmişinden bulabileceğimi düşünüyorum ve ilk olarak history database dosyası arıyorum.

Buluyorum ve export edip sqlite ile açıyorum. Urls tablosunda aradığım sonuca ulaşıyorum.



**CEVAP = stinky**

**SORU 28**

“What cloud service was a Startup item for the user admin?”

Kullanıcı yöneticisi için başlangıç öğesinnin hangi bulut hizmeti olduğu soruluyor. Bunun için NTUSER.DAT hive’ı içerisinde otomatik başlatma kayıtlarını kontrol ediyoum.

*Software\Microsoft\Windows\CurrentVersion\Run*



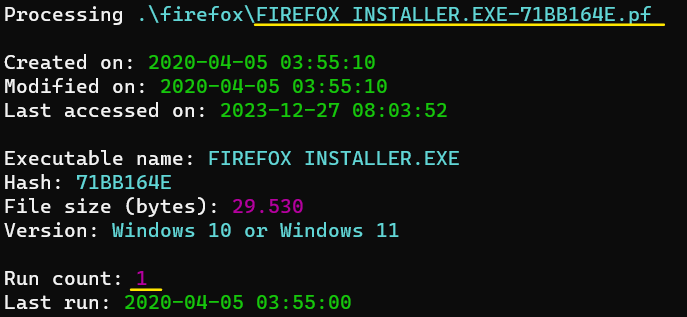
**CEVAP = OneDrive**

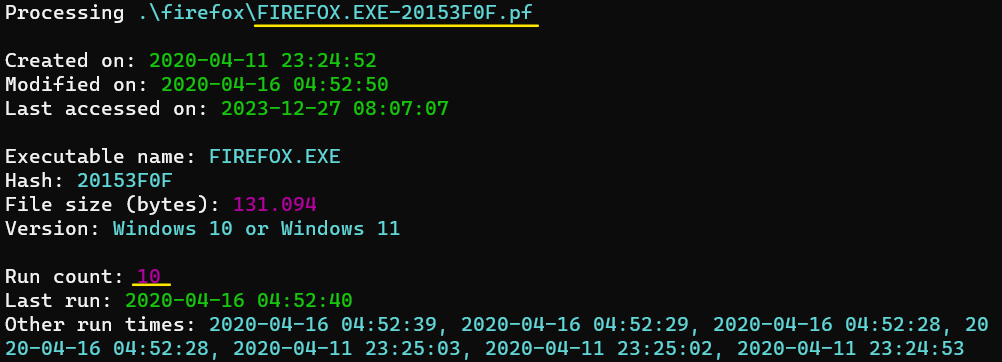
**SORU 29**

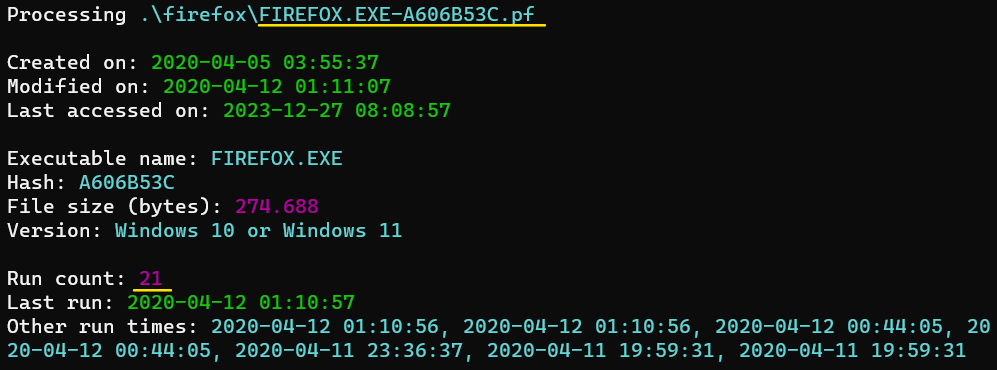
“Which Firefox prefetch file has the most runtimes?”

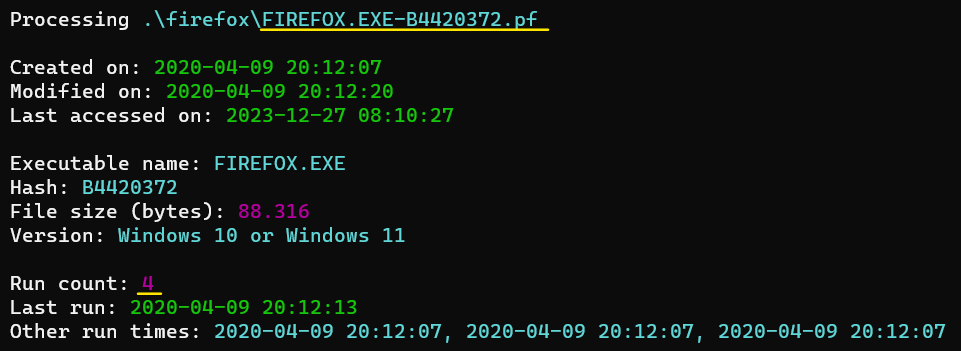
Hangi firefox prefetch dosyasının çalışma süresinin daha fazla olduğunu bulamamız isteniyor. İlk olarak firefox ile ilgili pretetch dosyalarını buluyorum ve export ediyorum. Daha sonra bu dosyaları PECmd ile analiz ediyorum.

Yaptığım analiz sonucunda bulduğum 4 tane firefox pf dosyasından en çok çalışanı ve kaç kez çalıştığını buluyorum ve istenilen sonuca ulaşıyorum.









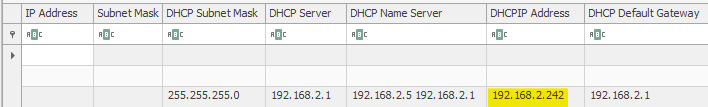
**CEVAP = FIREFOX.EXE-A606B53C.pf/21**

**SORU 30**

“What was the last IP address the machine was connected to?”

Makinenin bağlandığı son ip adresini bulamamız isteniyor. Bunu bulamak için SYSTEM hive’nın içerisinde tcpip altında interface’i kontrol edeceğimi biliyorum.

*ControlSet001\Services\Tcpip\Parameters\Interfaces*



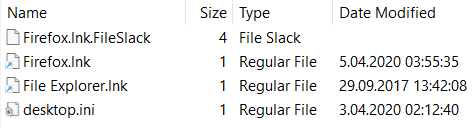
**CEVAP = 192.168.2.242**

**SORU 31**

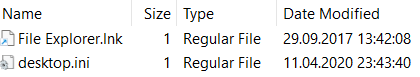
“Which user had the most items pinned to their taskbar?”

Hangi kullanıcının görev çubuğuna en fazla öğe sabitlediğini bulmamız isteniyor. *C:\Users\USERNAME\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar* dizininde sabitlenen öğeleri bulabileceğimi öğreniyorum ve her kullanıcı için kaç öğe olduğunu tek tek kontrol ediyorum.

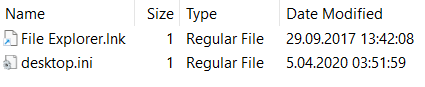
**Admin** ;



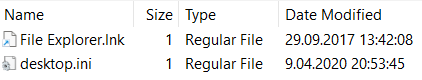
**Hansel.apricot;**



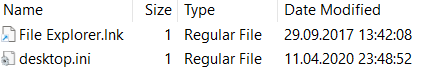
**Jim.tomato;**



**Miriam.grapes;**



**Suzy.strawberry;**



**Tim.apple;**

Tim için bu dosyayı bulamıyorum.

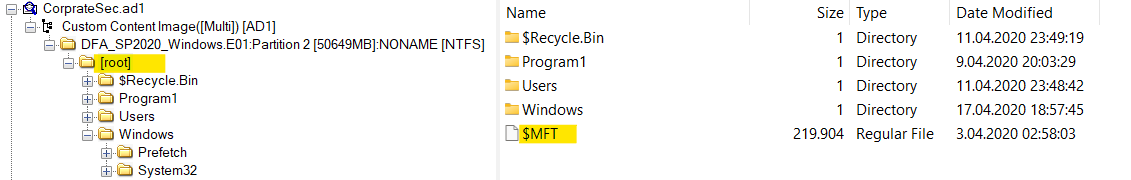
Bulduğum veriler içerisinde en çok öğeye sahip olan kullanıcı admin.

**CEVAP = admin**

**SORU 32**

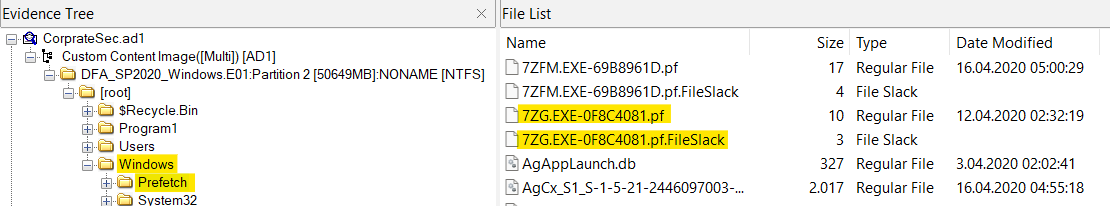
“What was the last run date of the executable with an MFT record number of 164885?”

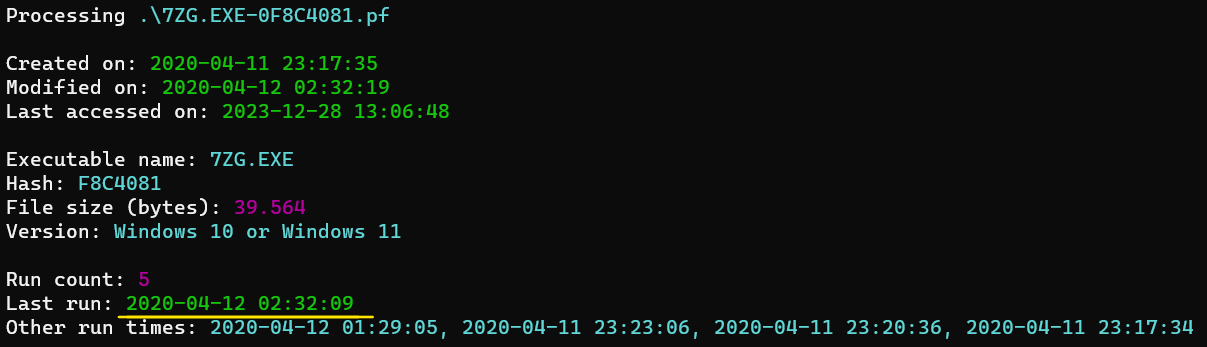
MFT kayıt numarası 164885 olan exe son çalıştırılma tarihini bulmamız isteniyor. İlk olarak bu dosyanın ne olduğunu bulmaya çalışıyorum. İlk olarak FTK’dan MFT’yi export ediyorum.



Daha sonra bunu MFTEcmd ile excel dosyasına çevirerek içerisindeki verileri okuyorum. Ve aradığım kayıt numarasına ulaşıyorum.

Bulduğum bu exe dosyasının prefetch dosyasını buluyorum ve PECmd ile analiz ederek son çalıştırılma tarihine erişiyorum ve istediğim sonucu elde ediyorum.





**CEVAP = 04/12/2020 02:32:09**

**SORU 33**

“What is the log file sequence number for the file "fruit\_Assortment.jpg"?”

"fruit\_Assortment.jpg" dosyasının log dosyası sıra numarası isteniyor. Bunu da bir önceki soruda aradığım gibi MFT tablosu içerinde arıyorum ve sonuca ulaşıyorum.

**CEVAP = 1276820064**

**SORU 34**

“Jim has some dirt on the company stored in a docx file. Find it, the flag is the fourth secret, in the format of <"The flag is a sentence you put in quotes">.”

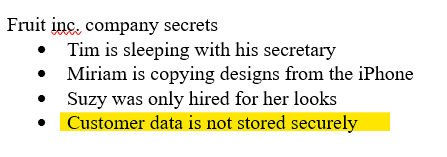
Jim’in docx dosyasında şirketle ilgili bazı kirli şeyler olduğunu söylüyor. Ve o dosyanın içerisndeki dördücü sır bizim cevabımızmış. Bu dosyayı bulmaya çalışıyoruz.

Jim’in dosyalarını karıştırdığımda bir tane docx dosyasına denk geliyorum fakat içerisinden böyle bir not çıkıyor ve aradığımız şeyin bu olmadığını anlıyoruz.



Daha sonra Recycle.Bin dosyasında Jim’in (1003 id) dosyalarına bakıyorum. Orda da docx dosyalarına denk geliyorum export edip kontrol ediyorum fakat dosyalar açılmıyor. Daha sonra ipuçlarından faydalanmaya karar veriyorum.

İpucuna göre Jim’in masaüstündeki Document1.docx dosyasını winrar ile açmamız söylenmiş. Uzantıyı zip olarak değiştirerek açıyorum. İçerisini kurcaladığımda file.xml dosyasını word ile açınca aradığım cevaba ulaşıyorum.



**CEVAP = Customer data is not stored securely**

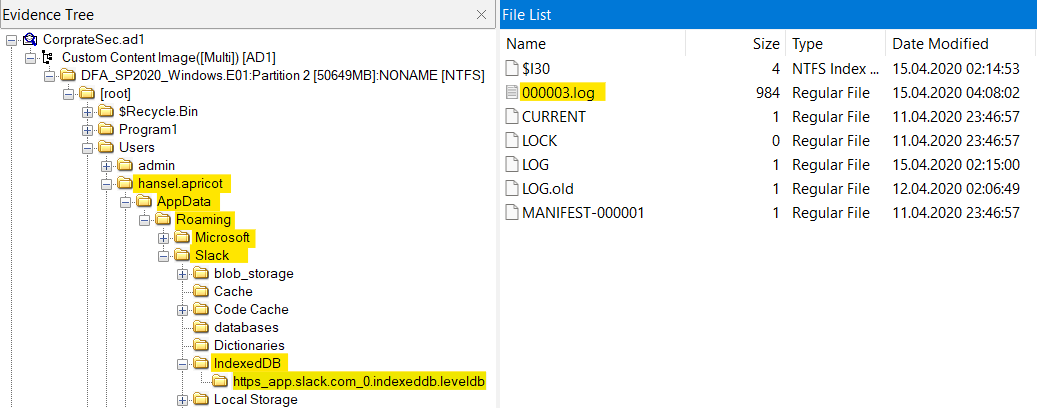
**SORU 35**

“In the company Slack, what is threatened to be deactivated if the user gets their email deactivated?”

Slack şirketinde, kullanıcının e-posta devre dışı bırakılırsa devre dışı bırakılma tehdidinde bulunan şey nedir?

Bu dosyaların nerede tutulacağı hakkında bir araştırma yapıyorum ve *C:/Users/USERNAME/AppData/Roaming/Slack* altında bulabileceğimi öğreniyorum. Kullanıcıları tek tek kontrol ediyorum ve sadece hansel.apricot kullanıcı altında slack dosyası buluyorum.

Burdan sonrasında ipucundan yararlanıyorum ve 000003.log dosyası içerinde inceleme yapıyorum.





**CEVAP = kneecaps**