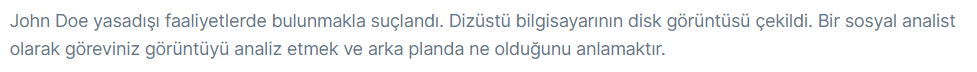
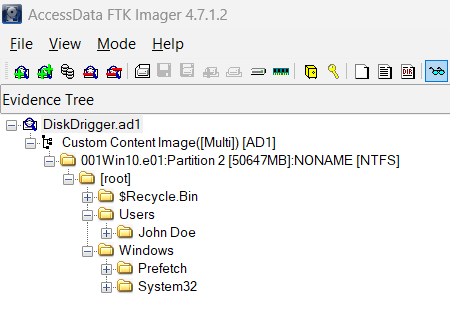
**AfricanFalls Blue Team Chellange**

**Senaryo**



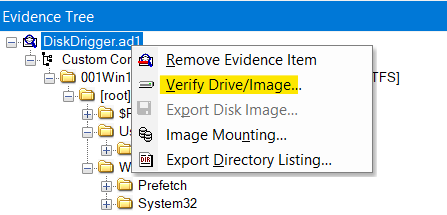
İlk olarak bize verilen imajı FTK ile görüntüleyerek başlıyorum.

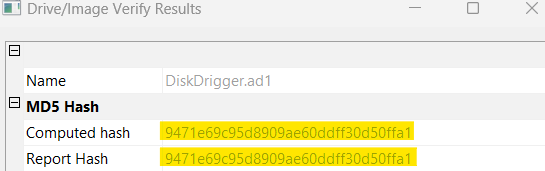


**SORU 1**

“What is the MD5 hash value of the suspect disk?”

Bize verilen şüpheli diskin MD5 hash değerini istiyor. FTK üzerinde diskin tamamına sağ tıklayarak imajı verify ederek hash değerine ulaşıyorum.



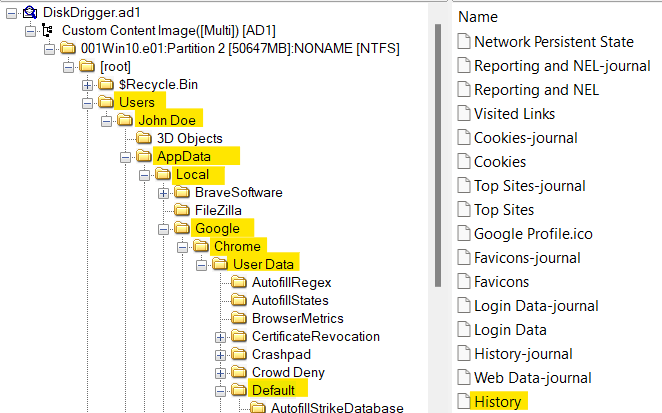


**CEVAP = 9471e69c95d8909ae60ddff30d50ffa1**

**SORU 2**

“What phrase did the suspect search for on 2021-04-29 18:17:38 UTC? (three words, two spaces in between)”

Şüphelinin 2021-04-29 18:17:38 UTC'de hangi ifadeyi aradığını soruyor. Bunu bulmak için Jhon’un browser geçmişine göz atmamız lazım. History dosyasını bulup extrackt ediyorum.



Export ettiğim bu dosyayı sqlite ile açıyorum ve aradığım veriye erişiyorum.

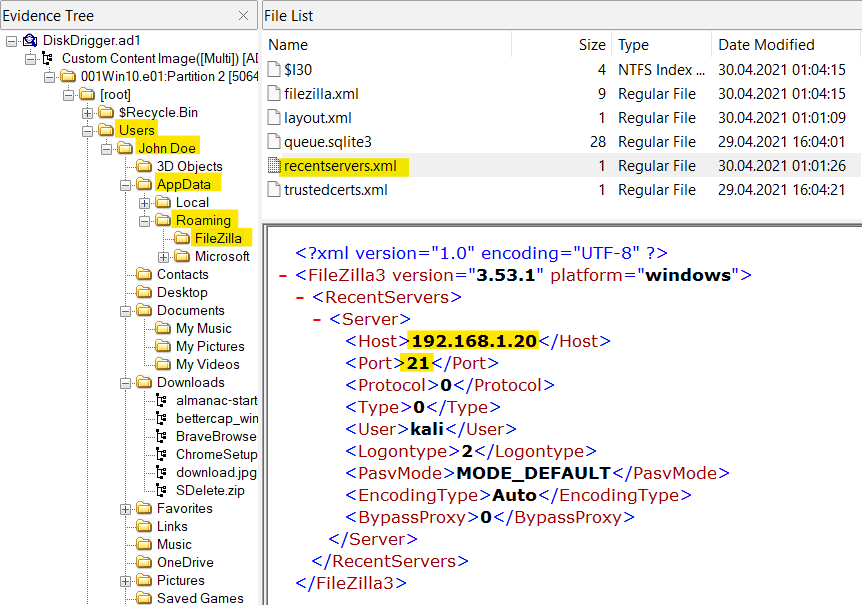


**CEVAP = password cracking lists**

**SORU 3**

“What is the IPv4 address of the FTP server the suspect connected to?”

Şüphelinin bağlı olduğu FTP sunucusunun ip adresi isteniyor. FTP sunucusunu kullanmamız için bir yapılandırma yapmamız gerekir. Bu yapılandırma dosyaları ise genellikle users/appdata/roaming dizini altında bulunur. Bu dizinleri kontrol ettiğimde 21. Port için bir yapılandırma olduğunu görüyorum. Genellikle 21. Portu FTP kullanır. Böylelikle sonuca ulaşıyorum.

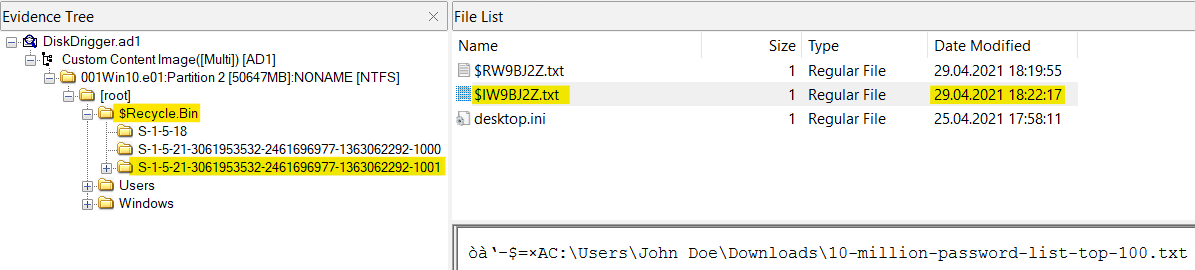


**CEVAP = 192.168.1.20**

**SORU 4**

“What date and time was a password list deleted in UTC? (YYYY-MM-DD HH:MM:SS UTC)”

Bir şifre listesi olduğunu ve silindiğini söylüyor. Bu listenin ne zaman silindiğini bulamamız isteniyor. Silinen dosyalar için Recycle.Bin klasörünü kontrol ediyorum ve silinen .txt dosyaları olduğunu ve içerisinde gerçekten şifrelerden bahsedildiğini görüyorum.

****

Modify tarihini deniyorum ve cevap doğru çıkıyor.

**CEVAP = 2021-04-29 18:22:17 UTC**

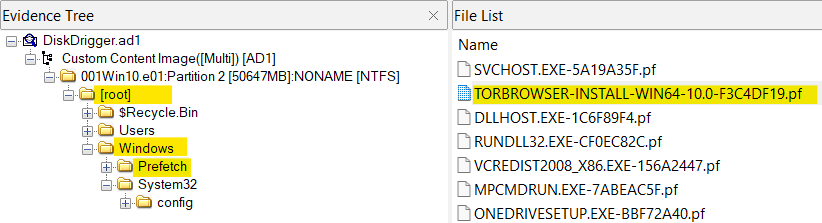
**SORU 5**

“How many times was Tor Browser ran on the suspect's computer? (number only)”

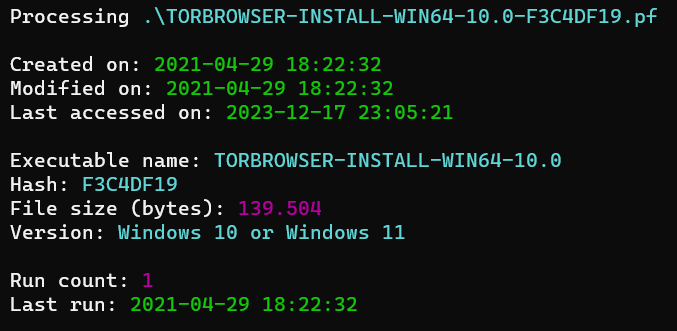
Bu soruda süpheli bilgisayarda kaç kere Tor tarayıcı çalıştığını bulmamız isteniyor.

Her ugulamanın bir prefetech dosyası oluşturulur ve bu dosya; dosya adı, dosya yolu, programın kaç kez çalıştığını, son çalıştırılma zamanı ve kullanılan DLL’ler gibi bilgileri tutar. Bizde Tor browser’ın pf dosyasını bulup analiz ederek bu bilgiye ulaşabiliriz.

Pf dosyasını bulup export ediyoruz.



Daha sonra bu pf dosyasını PECmd aracı ile analiz ediyorum.



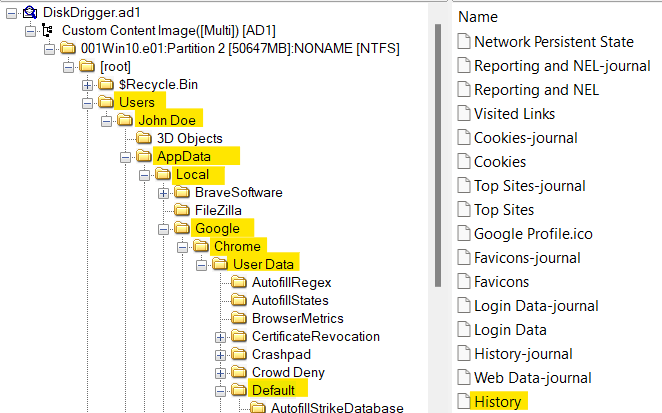
PECmd çıktısında bir olarak gözüküyor fakat cevap kabul edilmiyor.kabul edilen cevap 0’dır.

**CEVAP = 0**

**SORU 6**

“What is the suspect's email address?”

Şüphelinin e-mail adresi isteniyor. Web geçmişini görüntüleyerek sonuca ulaşmayı hedefliyorum. İlk olarak bize verilen imaj içerisinde Google crome ait History dosyasını bularak export ediyorum.



Export ettiğim bu dosyayı Sqllite ile açarak içerindeki verilere erişiyorum. url’ler arasında protonmail olduğunu ve title’ında bir mail adresi olduğunu görüyorum.



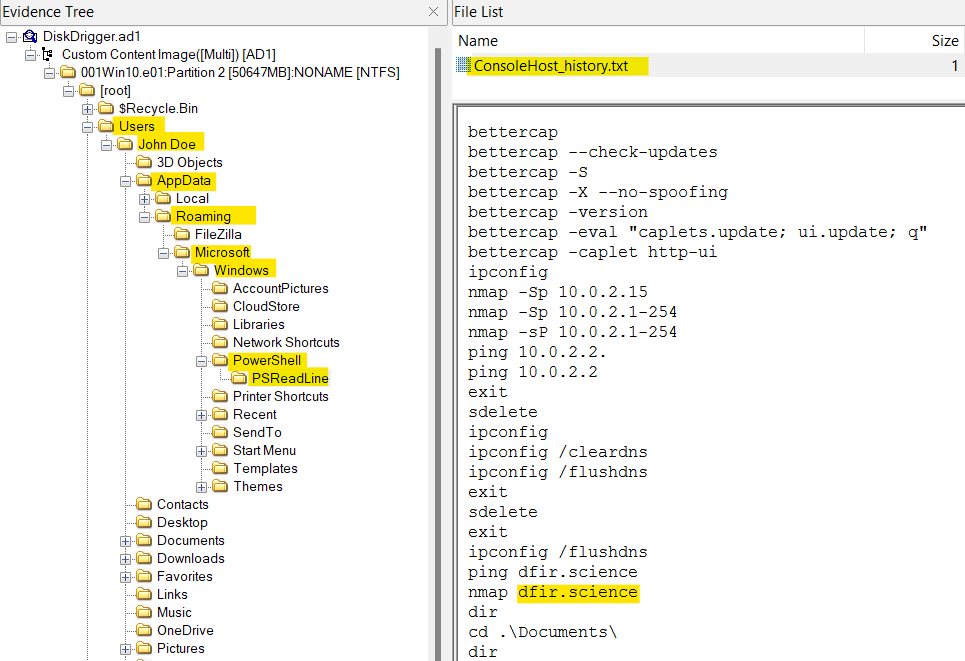
**CEVAP = dreammaker82@protonmail.com**

**SORU 7**

“What is the FQDN did the suspect port scan?”

Şüpheli bağlantı noktasının tarandığı Alan adını istiyor. Port taraması denince aklımıza ilk nmap geliyor. Ve bunu komut satırından yaptığı bariz. İlk olarak Poweshell geçmişinin tutulduğu yeri buluyorum.

*user/appdata/roaming/microsoft/windows/powershell/PSReadLine/ConsoleHost\_history.txt*

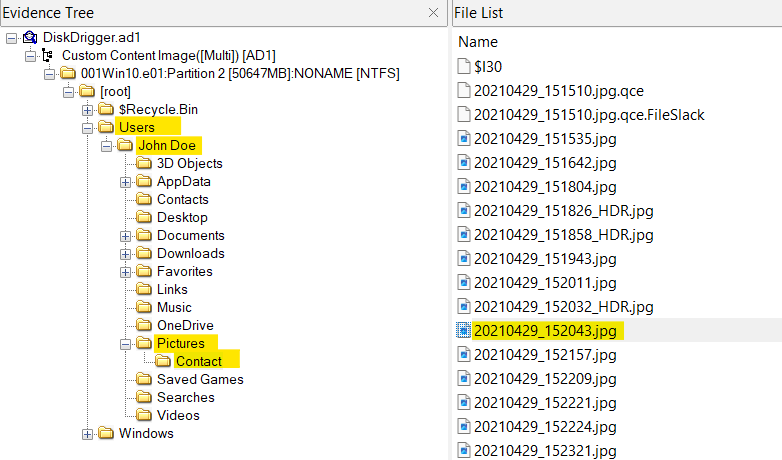


**CEVAP = dfir.science**

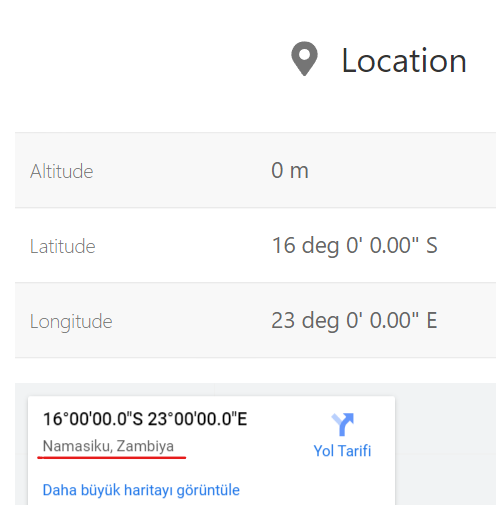
**SORU 8**

“What country was picture "20210429\_152043.jpg" allegedly taken in?”

"20210429\_152043.jpg" bu resmin hangi ülkeye ait olduğunu bulammız isteniyor. Metadata bilgilerine bakarak bunu buabiliriz.



İstenilen jpg dosyasını bularak export ediyorum. Ve online bir exiftool kullanarak sonuca ulaşıyorum.



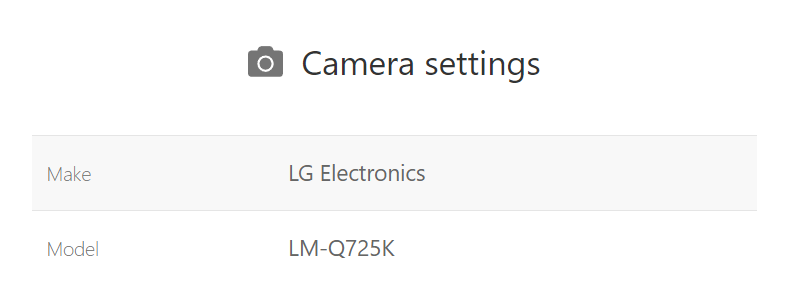
**CEVAP = zambia**

**SORU 9**

“What is the parent folder name picture "20210429\_151535.jpg" was in before the suspect copy it to "contact" folder on his desktop?”

"20210429\_151535.jpg" süpheli bu resimi contact klasörüne kopyalamadan önce resmin nerede olduğu isteniyor bizden.

Yine ilk olarak resmi bulup extract ederek exif bilgilerine bakacağız.

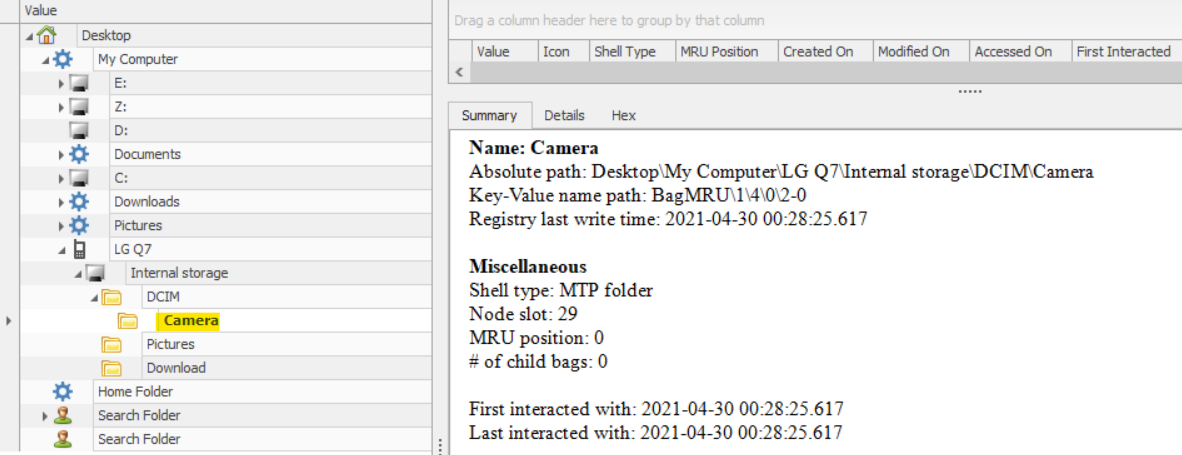


Exif bilgilerinden fotografın çekildiği cihaz ve modeline ulaşıyoruz.

Dosyalar hakkında bilgi almak için shellbagleri kullanıyorduk. Shellbag analizi yapcağım.

*C:\Users\John Doe\AppData\Local\Microsoft\Windows\UsrClass.dat* ‘ı export ediyorum ve Shellbag explorerda inceleme yapıyorum.

Bulduğumuz cihaza ait dosyların neler olduğuna erişiyoruz.

**

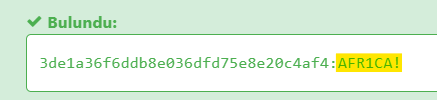
**CEVAP = camera**

**SORU 10**

“A Windows password hashes for an account are below. What is the user's password? Anon:1001:aad3b435b51404eeaad3b435b51404ee:3DE1A36F6DDB8E036DFD75E8E20C4AF4:::”

Bir kullanıcıya ait şifre hash’i verilmiş ve bizden şifrenin ne olduğu isteniyor. Bu yapıda ilk kısım kullanıcı adını, ikinci kısım genellikle kullanıcıya özgü bir numara, üçüncü kısım NTLM hashin kendisi son kısım ise şifrenin hashini tutar.

Son kısmı online bir hash kırma platformunda kırıyoruz ve sonuca ulaşıyoruz.

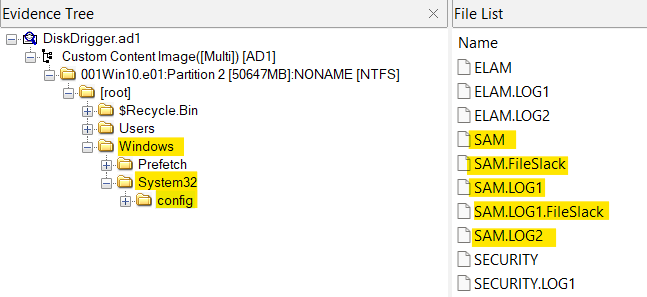


**CEVAP = AFR1CA!**

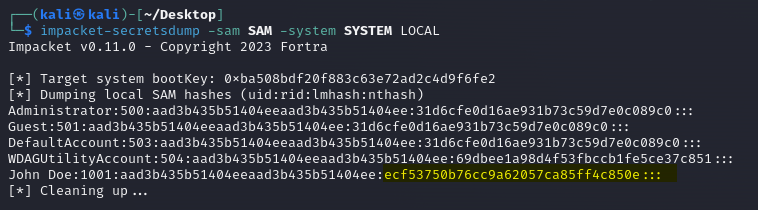
**SORU 11**

“What is the user "John Doe's" Windows login password?”

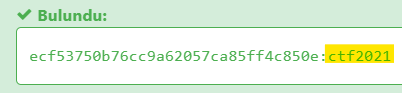
John Doe’nun oturum açma parolası isteniyor bizden. Oturum açma bilgilerini SAM hive’nın tuttuğunu biliyorum ve FTK’dan SAM’ı export ediyorum.



SAM’ın yanı sıra SYSTEM hive’larını da export ediyorum. Daha sonra kalide secretdump aracını kullanarak kullanıcı hashlerini buluyorum.



Bulduğum bu hashi online platformda kırıyorum ve istediğim sonucu elde ediyorum.



**CEVAP = ctf2021**