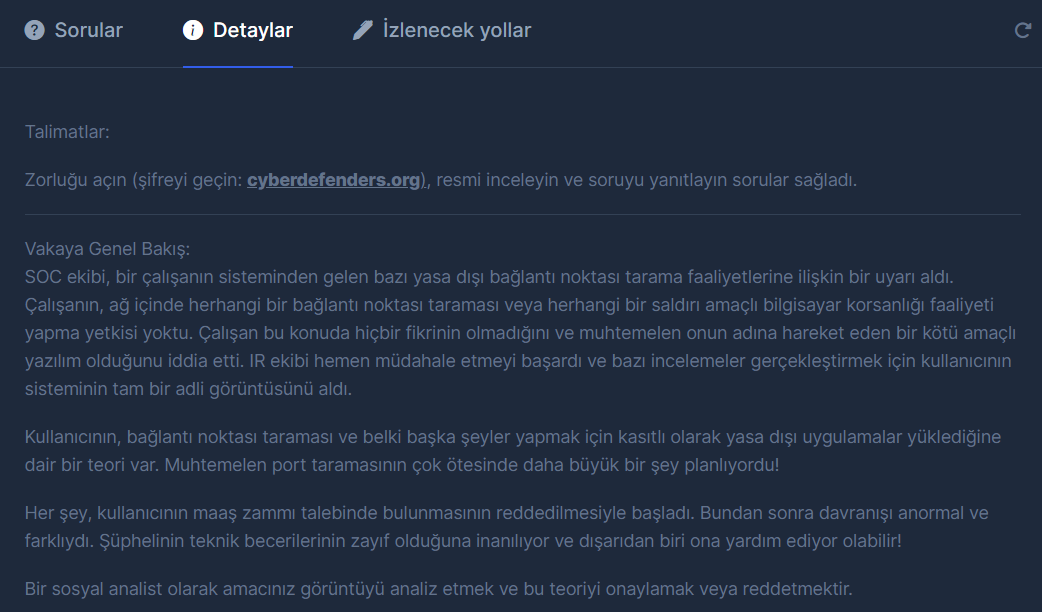
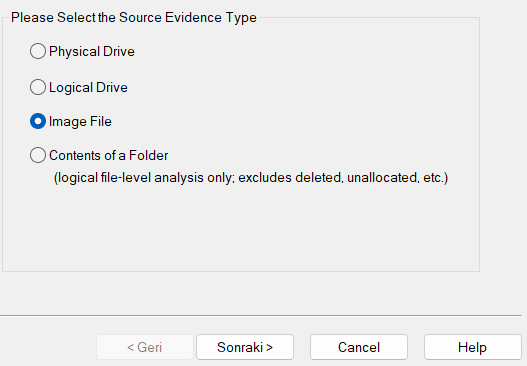
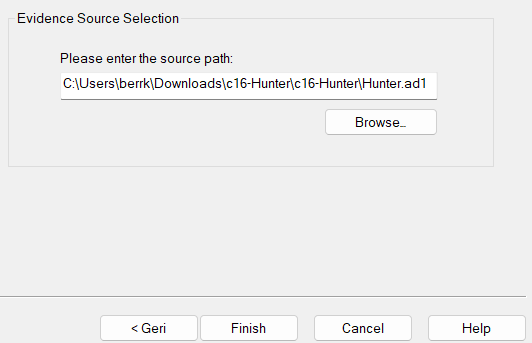
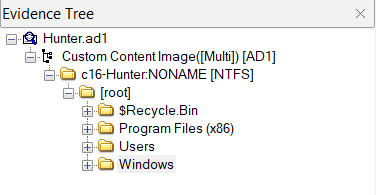
**Hunter Blue Team Challenge**

**Senaryo**

Bize verilen dosyaları zipten çıkararak başlıyoruz. Daha sonra FTK ile bize verilen .ad1 formatındaki imajı açıyoruz.



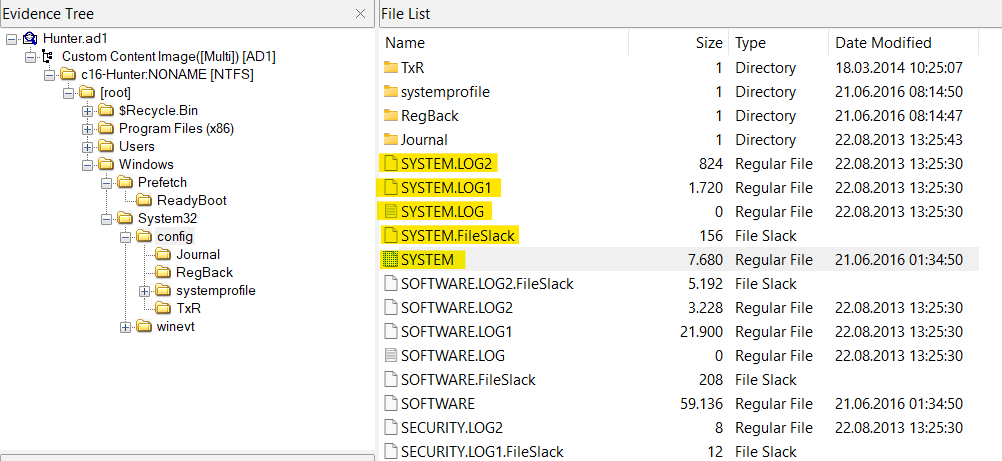


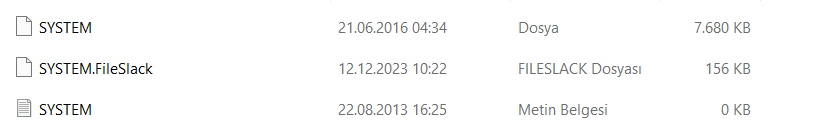


**SORU 1**

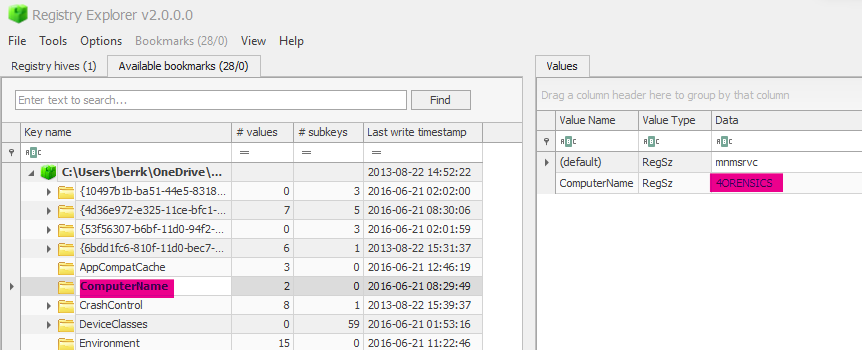
“What is the computer name of the suspect machine?”

Şüpheli makinenin adı isteniyor. İlk olarak *windows/system32/config* alındaki system hive’larını export edip bir dosyaya alıyoruz.





Export ettiğim bu dosyaları *registry explorer’da* açarak inceleme yapacağım.



Bizden istenilen computer name’e erişmiş oluyoruz.

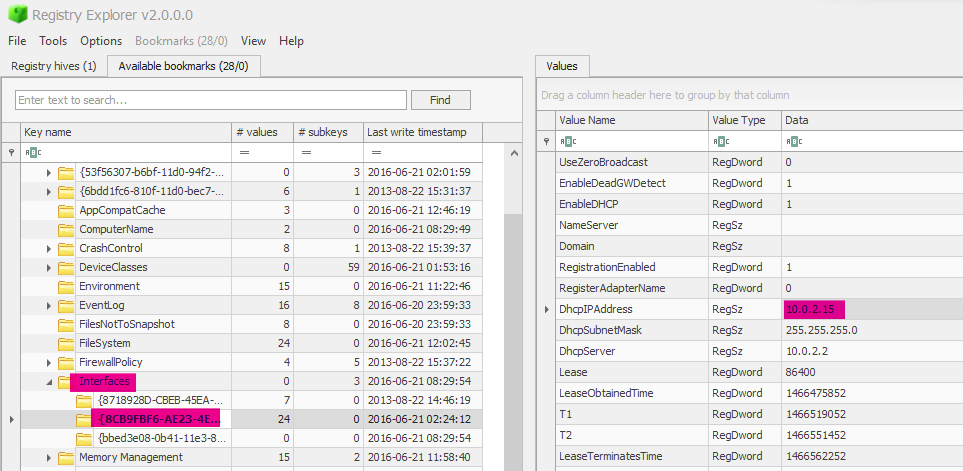
*\ControlSet001\Control\ComputerName\ComputerName*

**CEVAP = 4ORENSICS**

**SORU 2**

“What is the computer IP?”

Bu soruda bizden bilgisayar ip isteniyor. Yine açtığım system hive’ı içerisinden interfaces kısmından ip adresini çıkarıyorum.

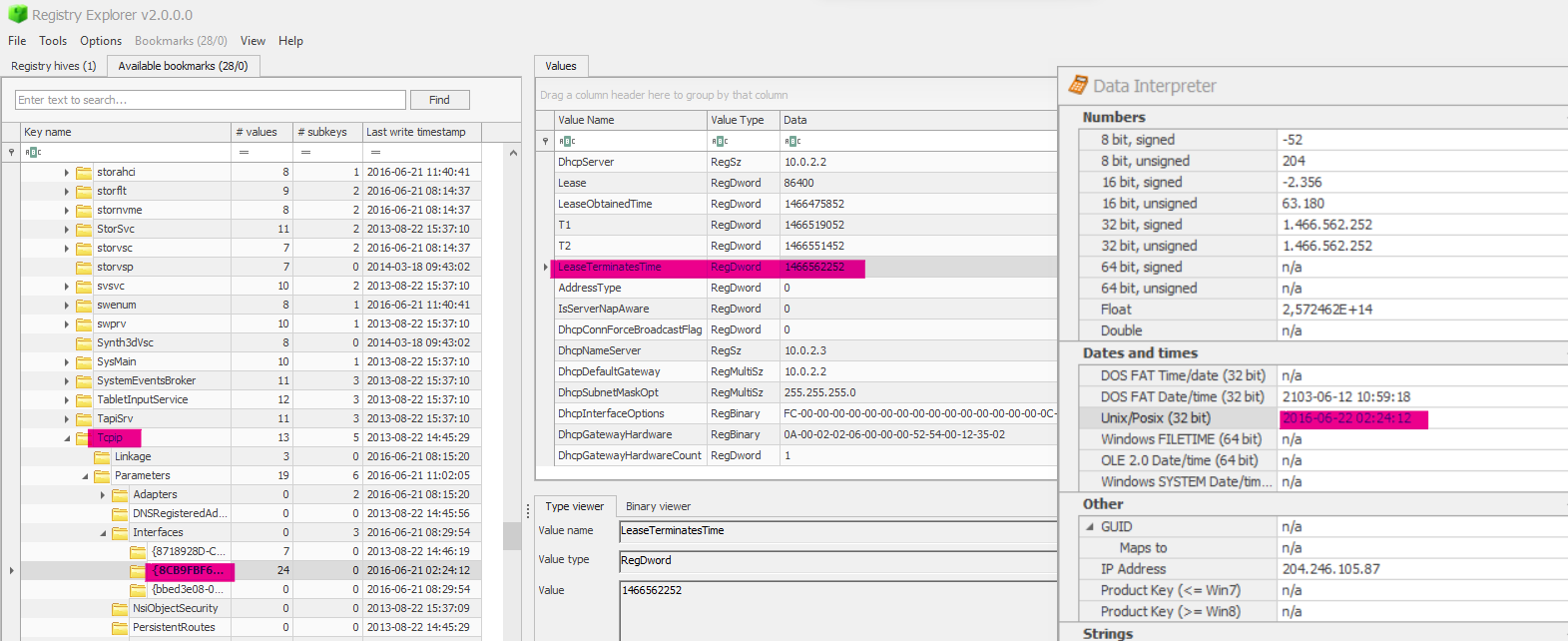


*\ControlSet001\Services\Tcpip\Parameters\Interfaces*

**CEVAP = 10.0.2.15**

**SORU 3**

“What was the DHCP LeaseObtainedTime?”

Bizden DHCP LeaseObtainedTime isteniyor. Bu sunucudan ip’yi kiraladığı zamanını ifade eder.

*\ControlSet001\Services\Tcpip\Parameters\Interfaces*

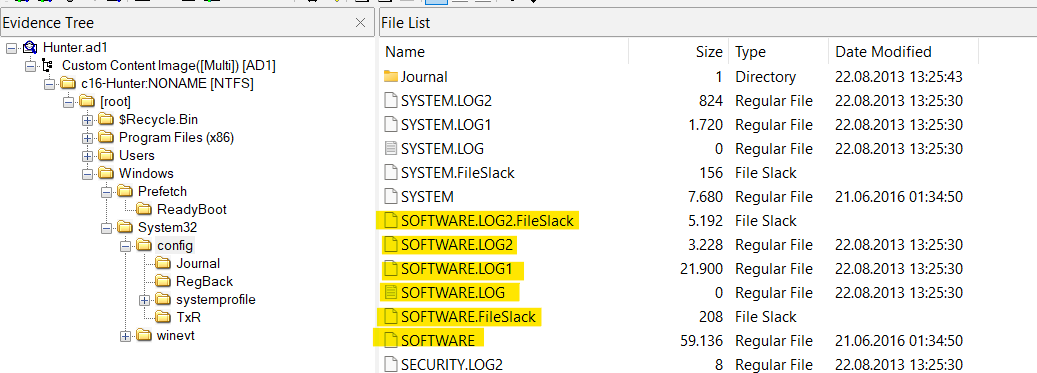
Değere sağ tıklayıp yorumlamasını istiyorum ve istenilen zaman bilgisine erişiyorum.

**CEVAP = 21/06/2016 02:24:12 UTC**

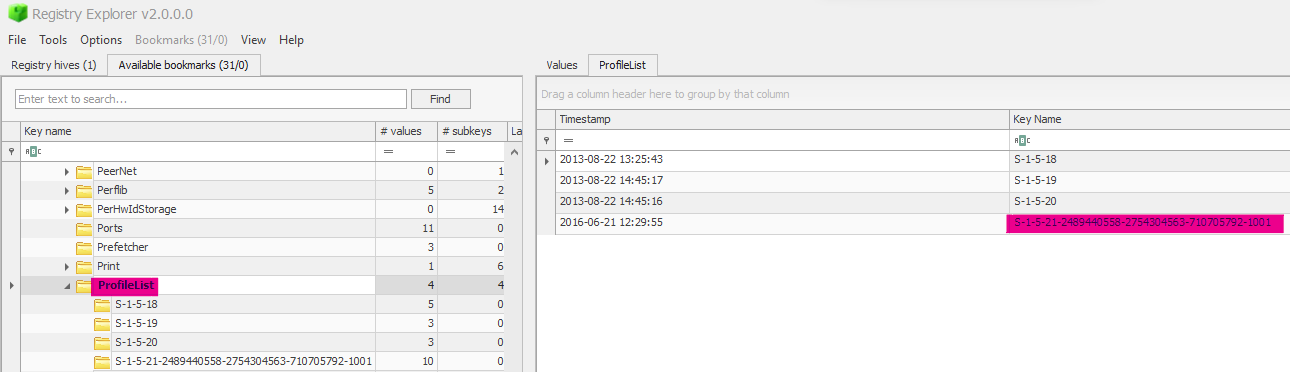
**SORU 4**

“What is the computer SID?”

Burada bilgisayarın SID bilgisi isteniyor. *\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList* burada SID bilgilerini bulacağımı biliyorum bu yüzden FTK dan Software kovanını export ederek registry explorer da inceleyeceğim.



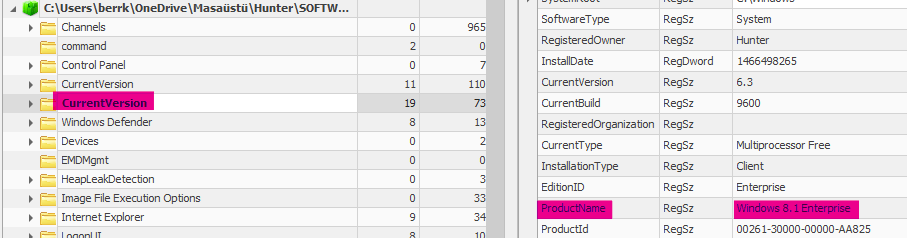
SID yapısında son 4 hane kullanıcı id’si olarak tututlur.son 4 haneyi almadan pc SID’ni buluyoruz.

**CEVAP =** **S-1-5-21-2489440558-2754304563-710705792**

**SORU 5**

“What is the Operating System(OS) version?”

Bizden işletim sistemi versiyonu isteniyor. */software/Microsoft/Windows NT/CurrentVersion/* altındabulunduğunu biliyorum.



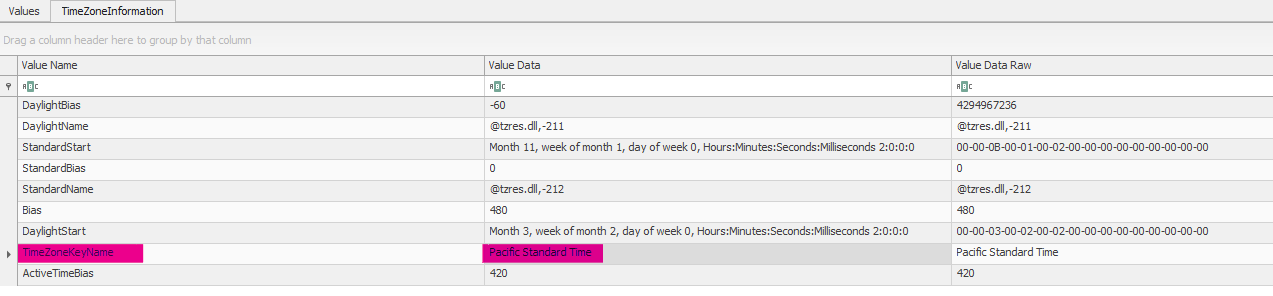
Böylelikle versiyon bilgisine ulaşıyorum.

**CEVAP = 8.1**

**SORU 6**

“What was the computer timezone?”

*/system/CurrentControlSet/Control/TimeZoneInformation/* altında bulabileceğimi biliyorum o yüzden system hive’ı içerisinde arıyorum.

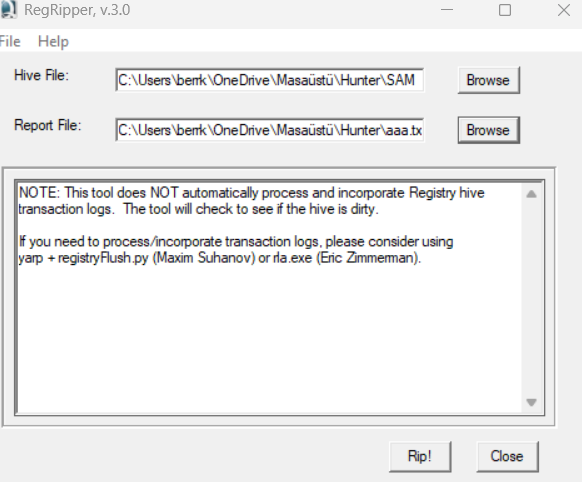
Biraz araştırma ile Pacific Standard Time = UTC-07:00 olduğunu öğreniyorum.

**CEVAP = UTC-07:00**

**SORU 7**

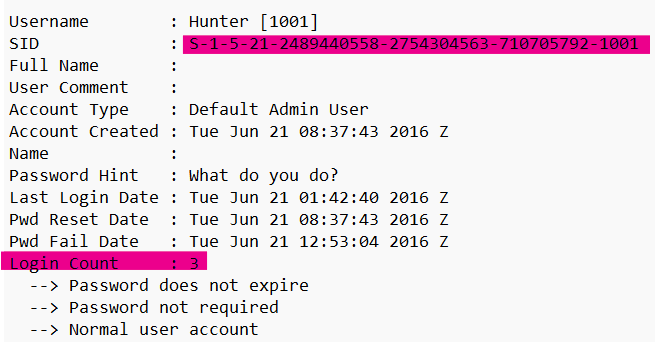
“How many times did this user log on to the computer?”

Bu kullanıcın kaç kere oturum açtığı soruluyor. Kullanıcı hesapları ve kimlik doğrulama bilgileri SAM’da tutuluyor. FTK’ dan SAM dosyalarını export ederek Regripper ile inceleyeceğim.



Sam hive’nı export etmiştim hive file kısmına veriyorum. Çıktıyı bir .txt dosyasına yazdırıyor.

Birçok kullanıcı için bilgiler bulunuyor fakat bizden *S-1-5-21-2489440558-2754304563-710705792* SID’li kullanıcının ne kadar giriş yaptığı isteniyor.

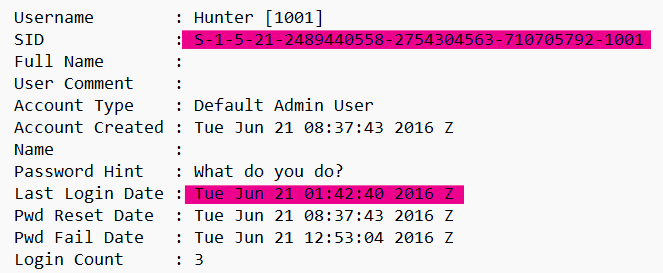


**CEVAP = 3**

**SORU 8**

“When was the last login time for the discovered account? Format: one-space between date and time”

Keşfedilen hesaba en son ne zaman giriş yapıldığını bulamaız isteniyor. Bir önceki soruda bunun cevabınıda bulmuştuk.

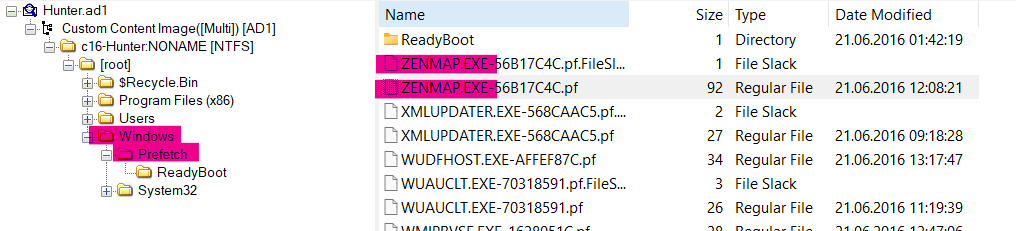


**CEVAP = 2016-06-21 01:42:40**

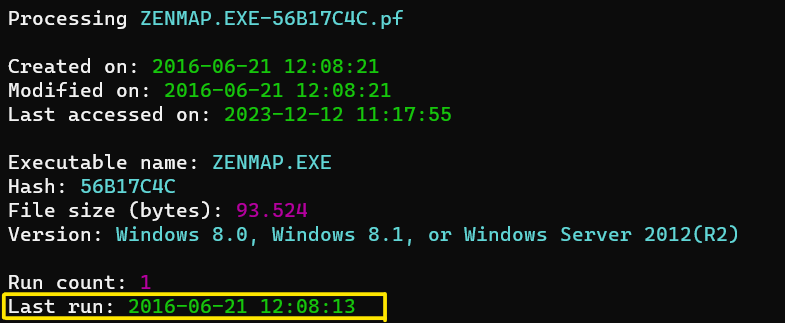
**SORU 9**

“There was a “Network Scanner” running on this computer, what was it? And when was the last time the suspect used it? Format: program.exe,YYYY-MM-DD HH:MM:SS UTC”

Bilgisayarda bir ağ tarama aracı çalışmış bizden bu aracın adını ve en son ne zaman çalıştığını bulmamız isteniyor. Prefetch, bilgisayarda hangi programın çalıştırıldığını gösterir.



.pf dosyasını export ediyorum ve pecmd aracı ile inceleme yapıyorum.



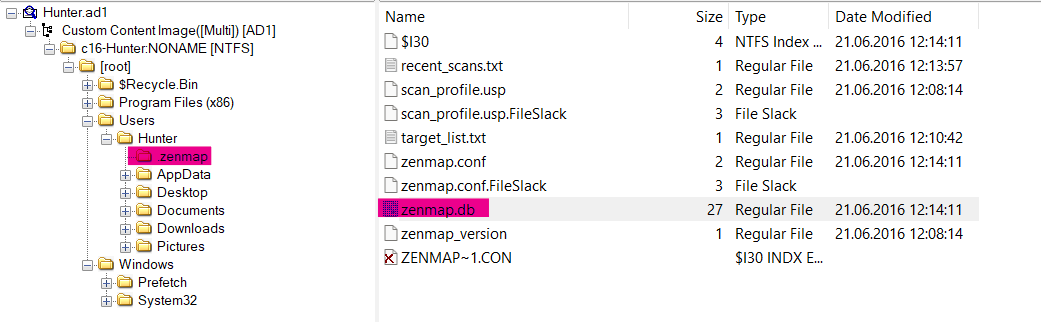
Ve en son ne zaman çalıştığı bilgisinede bu inceleme sonucunda ulaşıyorum.

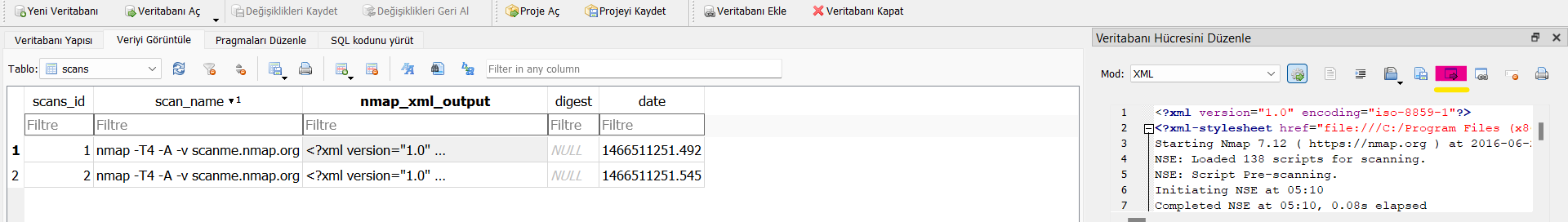
**CEVAP = zenmap.exe,2016-06-21 12:08:13 UTC**

**SORU 10**

“When did the port scan end? (Example: Sat Jan 23 hh:mm:ss 2016)”

Yapılan ağ taramasının ne zaman sona erdiği bilgisi isteniyor.



Yukarıda gördüğüm .db dosyasını sql lite kullanarak açıyorum

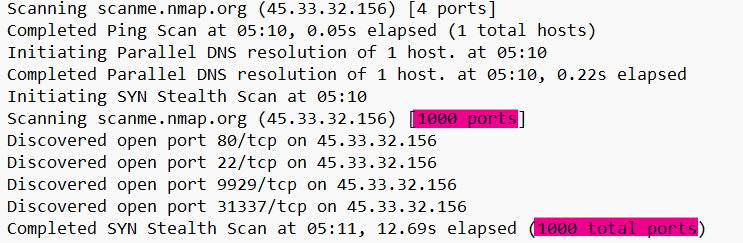
****İşaretlediğim yerden notepad’i seçererk verilere erişiyorum. Finished için filtreleme yaparak en son ne zaman çalıştığını buluyorum.

**CEVAP = Tue Jun 21 05:12:09 2016**

**SORU 11**

“How many ports were scanned?

Bu soruda kaç portun tarandığı soruluyor. Bunu yine .db içerisinden çıkardığım dosyaları kontrol ederek buluyorum.



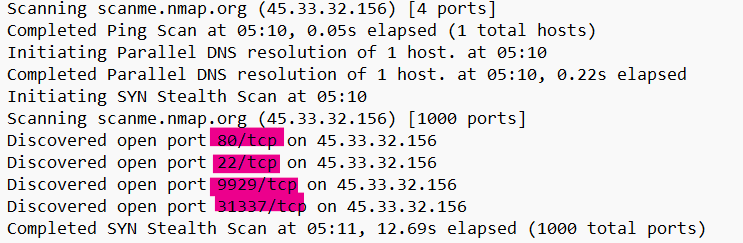
Kaç port tarandığı ve açık olan portların hangileri olduğunu görüyorum.

**CEVAP = 1000**

**SORU 12**

“What ports were found "open"?(comma-separated, ascending)”

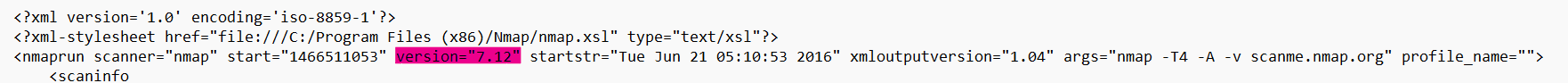
Hangi portların açık olduğu soruluyor bunu az önceki soruda bulmuştum.

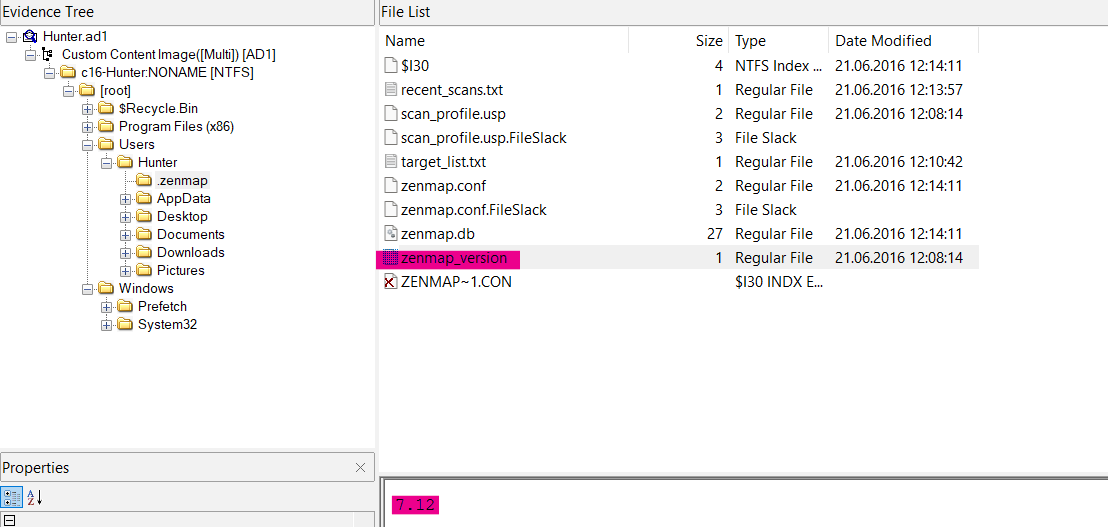


**CEVAP = 22,80,9929,31337**

**SORU 13**

“What was the version of the network scanner running on this computer?”

Bilgisayarda çalışan ağ tarayıcısının sürümü isteniyor. Database’den çıkardığım xml dosyası içerisinde versiyon bilgisine de ulaşabiliyorum.

****

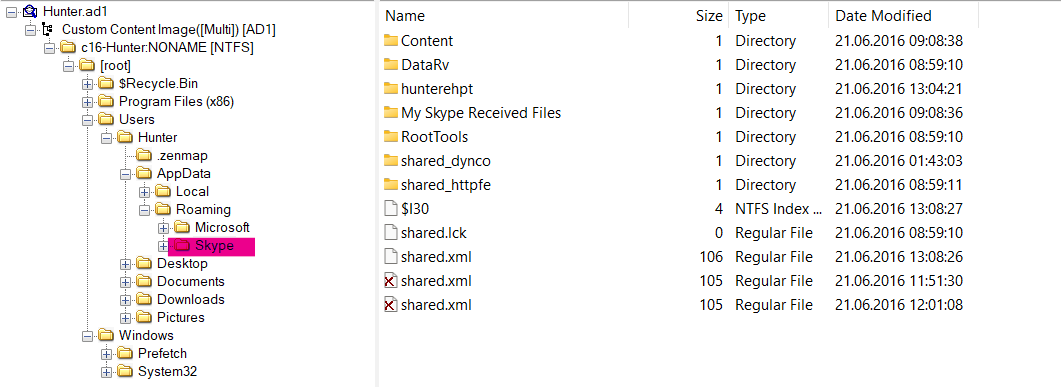
FTK’da Zenmap dosyaları içerisinde de versiyon bilgisine erişiyorum.

**CEVAP = 7.12**

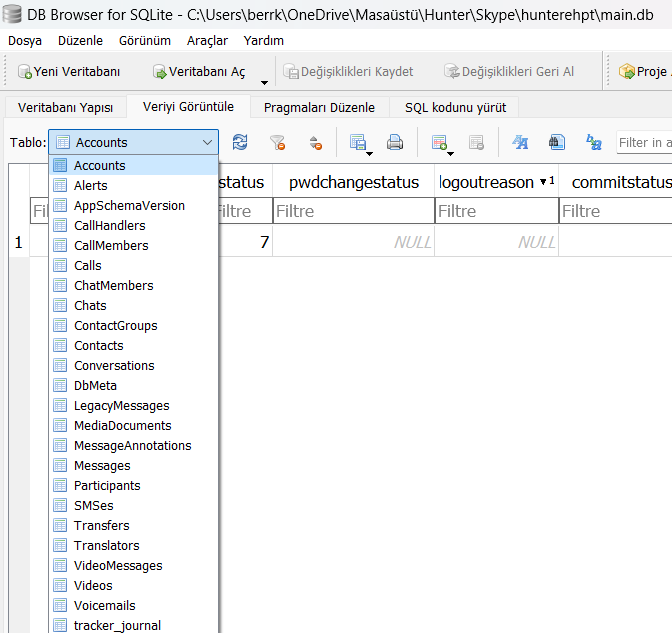
**SORU 14**

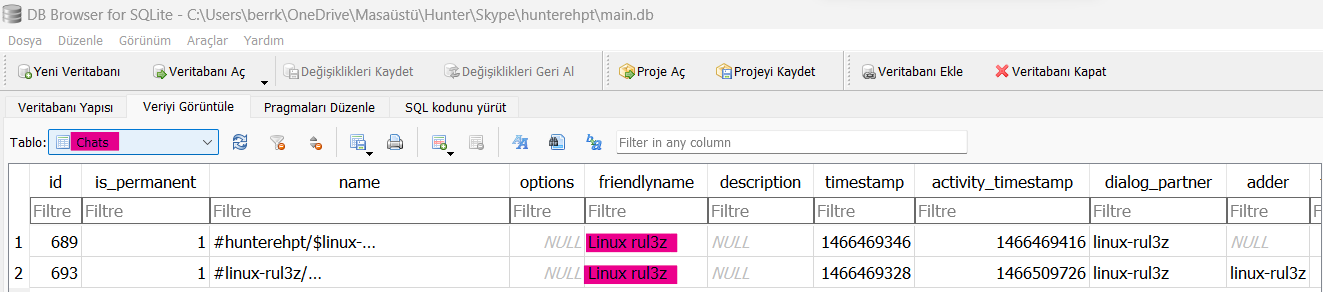
“The employee engaged in a Skype conversation with someone. What is the skype username of the other party?”

Biriyle skype görüşmesi yapılmış ve bizden karşı tarafın kullanıcı adı isteniyor.



Skype dosyasını export ediyorum. Dosyaları biraz kurcaladığımda .db dosyaları olduğunu görüyorum. Hunterehpt içerisinde main.db’yi sqllite ile açıyorum. Karşıma birçok tablo çıkıyor.



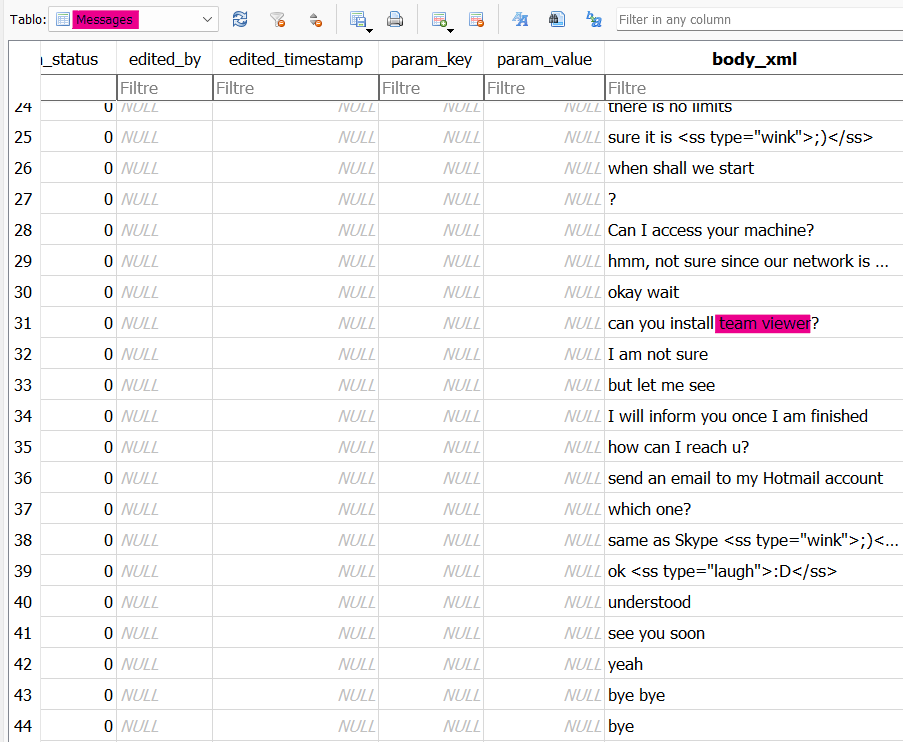
Bu tabloları biraz kurcaladığımda kiminle görüşme yaptığına erişebiliyorum.

**CEVAP = linux-rul3z**

**SORU 15**

“What is the name of the application both parties agreed to use to exfiltrate data and provide remote access for the external attacker in their Skype conversation?”

Her iki kullanıcınında veri sızdırmak ve uzaktan erişim sağlamak için kullanmayı anlaştıkları bir uygulama olduğundan bahsediliyor. Bizden bu uygulamanın adını bulamamız isteniyor. Bu bilgiye erişmek için konuşmalara erişmem gerekiyor. Konuşmaları tekrar main.db içereisinden çıkarıp çıkaramayacağımı kontrol ediyorum.

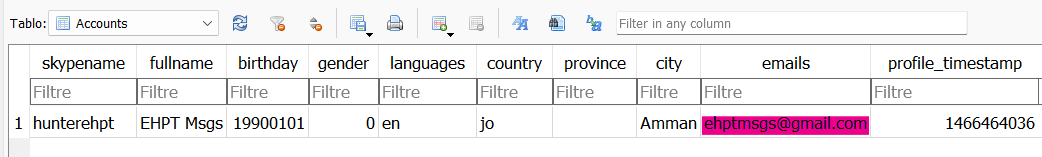


Messages tablosundan konuşmalara eriştim ve hangi uygulama için anlaştıklarını buldum.

**CEVAP = teamviewer**

**SORU 16**

“What is the Gmail email address of the suspect employee?”

Burada bizden süpheli çalışanımızın e-mail adresi isteniyor. Yine bu bilgiyi accounts tablosundan erişiyorum. Zaten tek kayıt var.

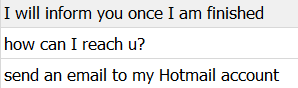
**CEVAP = ehptmsgs@gmail.com**

**SORU 17**

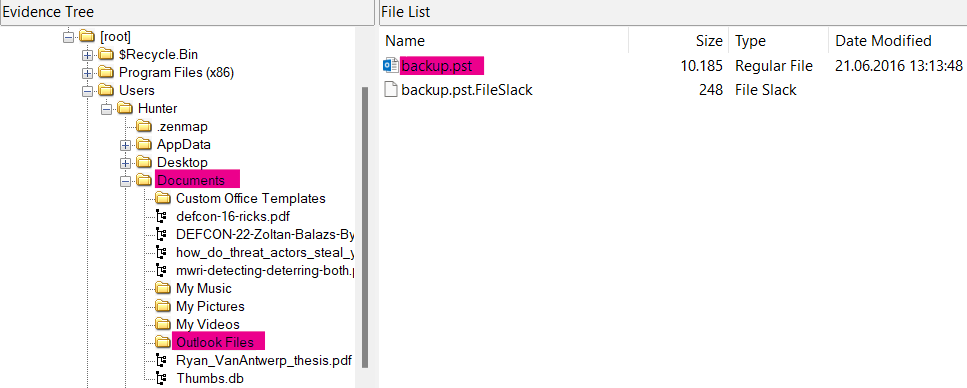
“It looks like the suspect user deleted an important diagram after his conversation with the external attacker. What is the file name of the deleted diagram?”

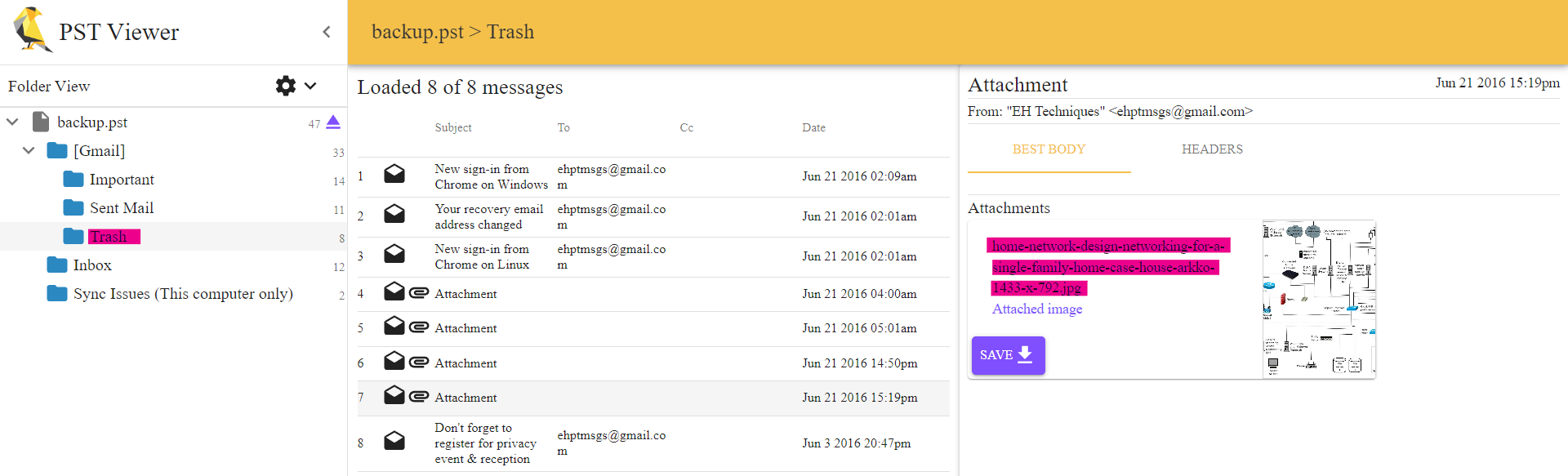
Şüpheli kullanıcının saldırganla yaptığı görüşmeden sonra önemli dosya silmiş. Bizden bu silinen dosyanın adını bulamamız isteniyor.

Konuşmaları okurken hotmail hesabı üzerinden aktarıldığı sonucuna varıyorum.



FTK üzerinde inceleme yaparken Outlook dosyası olduğunu ve içerisinde backup.pst olduğunu görüyorum . backup.pst export ediyorum.



Online bir pst viewer kullanarak içerisindeki bilgilere erişiyorum.

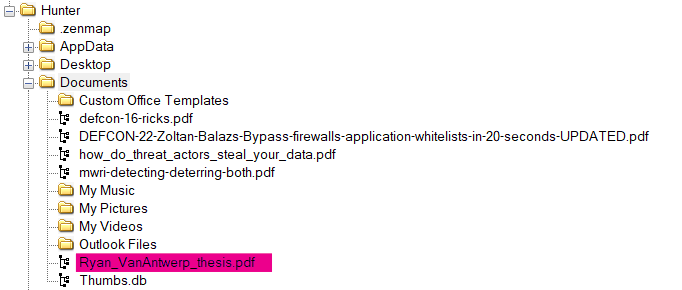
**CEVAP = home-network-design-networking-for-a-single-family-home-case-house-arkko-1433-x-792.jpg**

**SORU 18**

“The user Documents' directory contained a PDF file discussing data exfiltration techniques. What is the name of the file?”

Kullanıcı belgeleri dizininin, veri sızdırma tekniklerini içeren bir pdf içerdiğini söylüyor. Bizden de bu pdf dosyasının tam adını istiyor.

Belgeler klasörünü kontrol ettiğimde birkaç tane .pdf dosyası olduğunu görüyorum. Cevap formatına en uygun beelgeyi buluyorum. Pdfleri kontrol ettiğimde birden fazlası sızma tekniği hakkında bilgiler içeriyordu. Bu yüzden cevap formatından yola çıkarak yanıtladım.



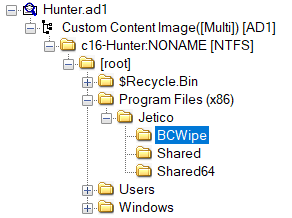
**CEVAP = Ryan\_VanAntwerp\_thesis.pdf**

**SORU 19**

“What was the name of the Disk Encryption application Installed on the victim system? (two words space separated)”

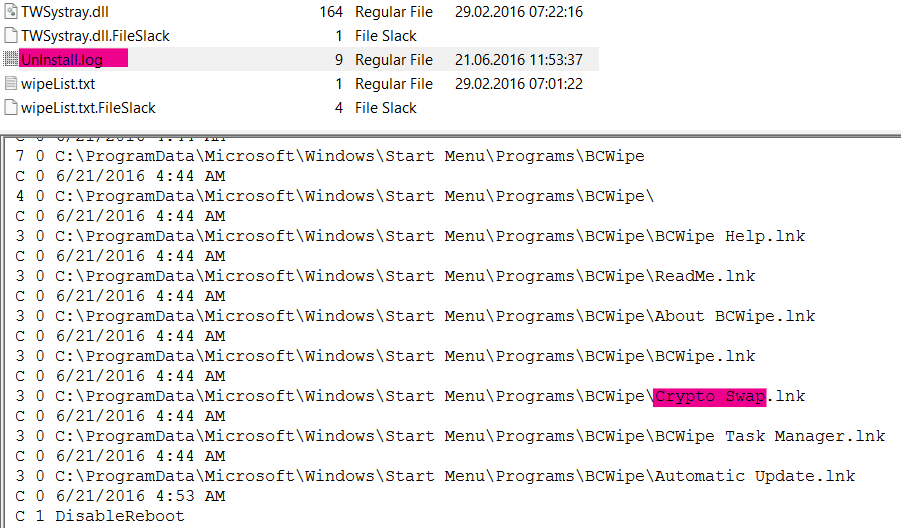
Kurban sisteme yüklenen disk şifreleme uygulamasının adı isteniyor.

Bunun için program dosyalarını kontrol ediyorum ve BCWipe adlı bi program dosyasıyla karşılaşyorum.



Daha önce wipe kelimesine ne demek olduğuna aşina olduğum için işime yarayacak bir şey çıkarabileceğimi düşünüyorum ve uygulamayı biraz araştırıyorum. Diske zarar vermede verileri kalıcı olarak silmeye yarayan bir program olduğunu ve birçok farklı işlemler yapabilen bir paket olduğu, içerisinde birçok alt uygulama olduğu bilgisine ulaştım. Bu alt uygulamalarından birinin bizim aradığımız şey olduğunu düşündüm.

BCWipe içerisinde bir log dosyası olduğunu görüyorum ve inceliyorum. Ve şifreleme yapan ve silinen uygulamayı buluyorum.



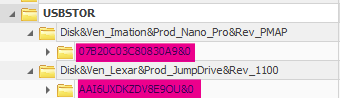
**CEVAP = Crypto Swap**

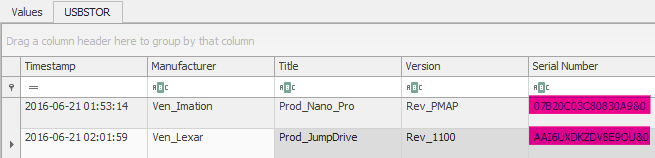
**SORU 20**

“What are the serial numbers of the two identified USB storage?”

Cihaza takılan iki adet USB’nin seri numarası isteniyor. Bunun için nereye bakacağımı biliyorum.

*SYSTEM\CurrentControlSet\Enum\USBSTOR*



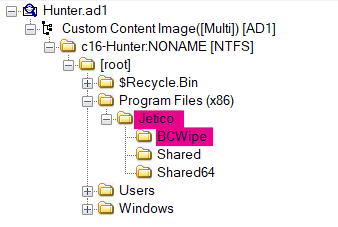


**CEVAP = 07B20C03C80830A9,AAI6UXDKZDV8E9OU**

**SORU 21**

“One of the installed applications is a file shredder. What is the name of the application? (two words space separated)”

Uygulamalardan birinin dosya parçalayıcı olduğunu söylüyor ve bu uygulamanın adını istiyor. Kurulu olan uygulamalara bakınca BCWipe’ın dosya parçalamak için kullanıldığını görüyorum.

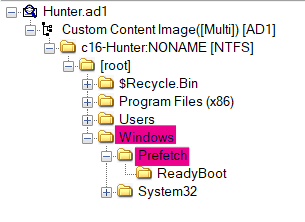


**CEVAP = Jetico BCWipe**

**SORU 22**

“How many prefetch files were discovered on the system?”

Sistemde kaç tane prefetch dosyası Olduğunu soruyor*. C:\Windows\prefetch* ‘ta olan dosyaları export eediyorum.

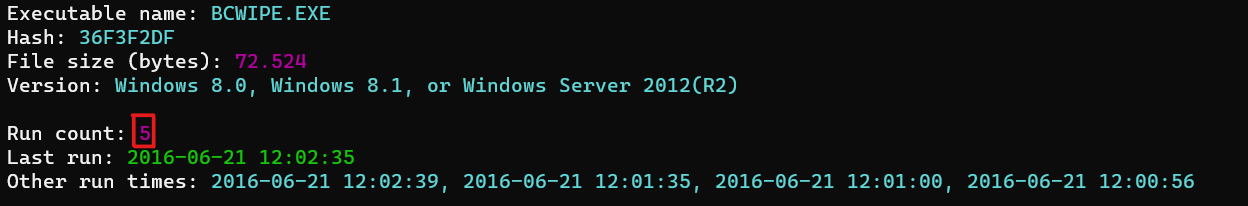


.pf uzantılı ve boyutu sıfırdan büyük dosyaları powershell komutu ile saydırıyorum.

**CEVAP = 174**

**SORU 23**

“How many times was the file shredder application executed?”

Dosya parçalayıcı uygulamanın kaç kez çalıştığını bulmamıız isteniyor. Bu uygulamanın hangisi olduğunu biliyoruz. Prefetch dosyaları içerisinde BCWipe ait .pf dosyasını bularak PECmd ile analiz ediyorum.

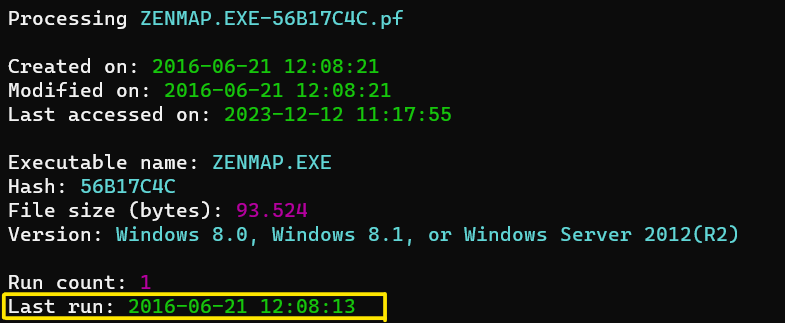
Ve uygulamanın kaç kez çalıştığını tespit ediyorum.

**CEVAP = 5**

**SORU 24**

“Using prefetch, determine when was the last time ZENMAP.EXE-56B17C4C.pf was executed?”

Prefetch dosyalarını kullanarak ZENMAP.EXE-56B17C4C.pf’nin en son ne zaman çalıştığını bulmamız isteniyor. Bunu 9. Soruda da bulmuştuk.



**CEVAP = 06/21/2016 12:08:13 PM**

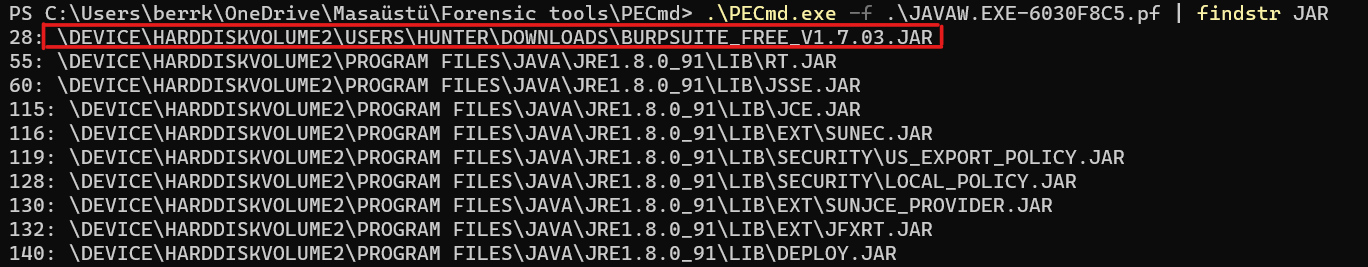
**SORU 25**

**“**A JAR file for an offensive traffic manipulation tool was executed. What is the absolute path of the file?”

Saldırgan bir trafik manipülasyon aracına yönelik JAR dosyası yürütmüş. Bu dosyanın tam yolu isteniyor.

JAR (Java Archive) dosyası, Java programları, uygulamaları ve kütüphanelerini depolamak ve dağıtmak için kullanılan bir arşiv dosya formatıdır.

Prefetch dosyaları içerisinden java ile ilgili dosyalara baktım ve JAVAW.EXE-6030F8C5.pf dosyasına ulaştım. Bu dosyayı PECmd ile inceleyeceğim.

*.\PECmd.exe -f .\JAVAW.EXE-6030F8C5.pf | findstr JAR*

Burpsuit görünce hemen aradığım şey olduğunu anlıyorum.

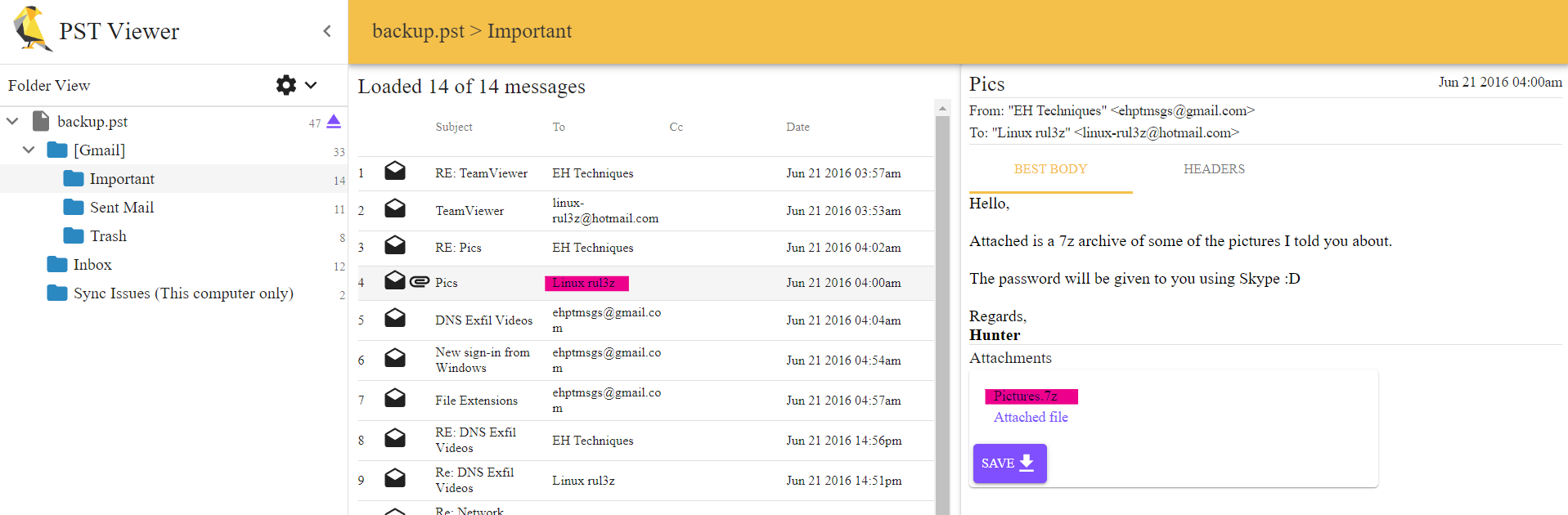
**CEVAP = C:\Users\Hunter\Downloads\burpsuite\_free\_v1.7.03.jar**

**SORU 26**

“The suspect employee tried to exfiltrate data by sending it as an email attachment. What is the name of the suspected attachment?”

Şüpheli çalışanın, e-posta eki olarak veri sızdırmaya çalıştığını söylüyor. Şüphelenilen ekin adı isteniyor.

Şüphelinin e-posta yazışmalarına 17. Soruda erişmiştik. Şüpheli ile yaptığı konuşmaya erişiyorum ve ekteki dosyanın ne olduğunu buluyorum.

**CEVAP = Pictures.7z**

**SORU 27**

“Shellbags shows that the employee created a folder to include all the data he will exfiltrate. What is the full path of that folder?”

Shellbags, çalışanın sızdıracağı verilerin tümünü bir klasörde topladığını söylemiş. Bizden bu klasörün tam yolu isteniyor.

ShellBags, Microsoft Windows işletim sisteminde kullanılan bir özelliktir ve kullanıcıların dosya gezginini kullanarak geçmişteki klasörleri ve dosyaları takip etmelerine yardımcı olan bir mekanizmadır. Bu dosyalar normalde aşağıda verilen konumlarda bulunur: *HKEY\_CURRENT\_USER\Software\Microsoft\Windows\Shell\Bags*

*HKEY\_CURRENT\_USER\Software\Microsoft\Windows\Shell\bagMRu*

Shellbag dosyaları şuralarda da bulunabilir :

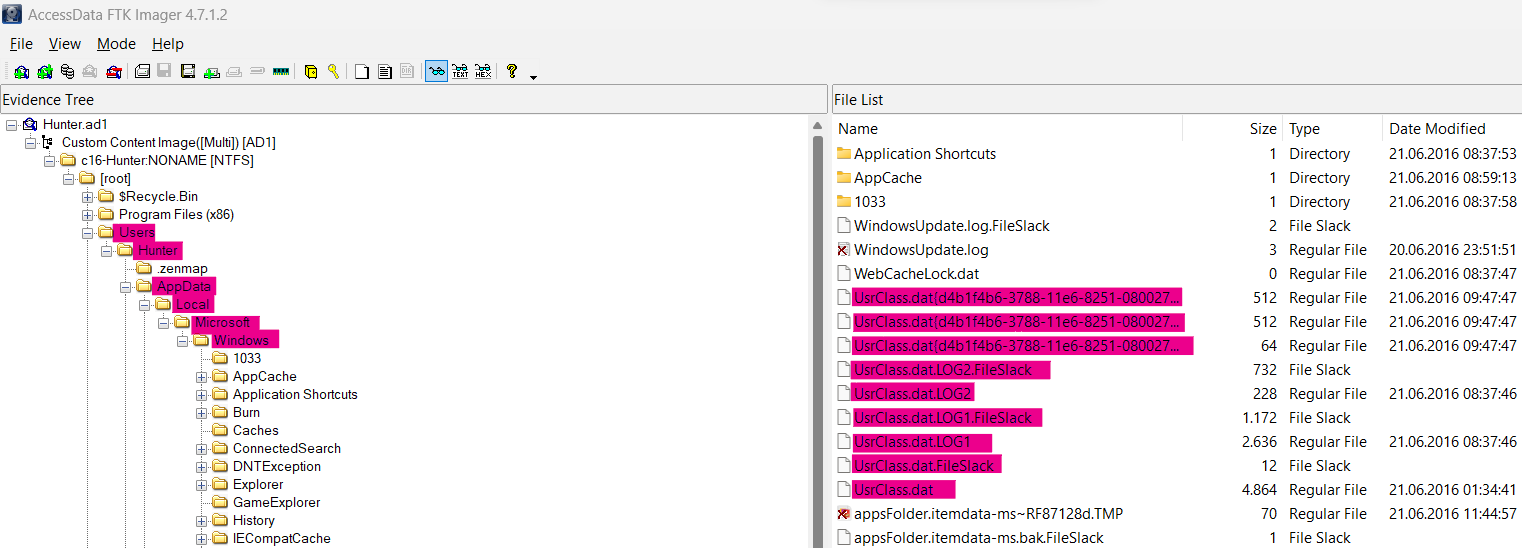
*USRCLASS.DAT\LocalSettings\Software\Microsoft\Windows\Shell\BagMRU*

*USRCLASS.DAT\LocalSettings\Software\Microsoft\Windows\Shell\Bags*

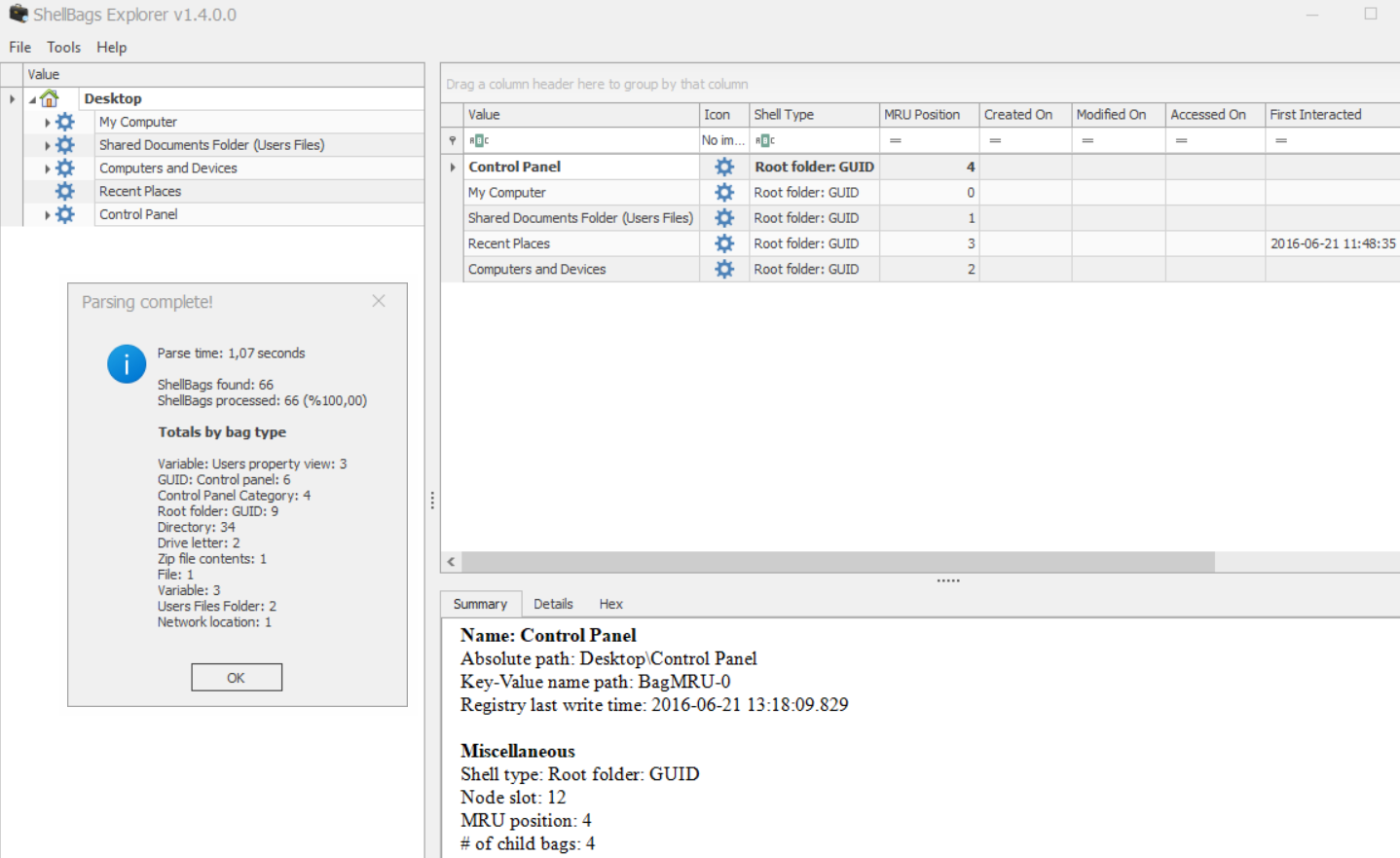
*NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU*

*NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags*

FTK’dan tüm USERCLASS.DAT dosyalarını export ediyorum.

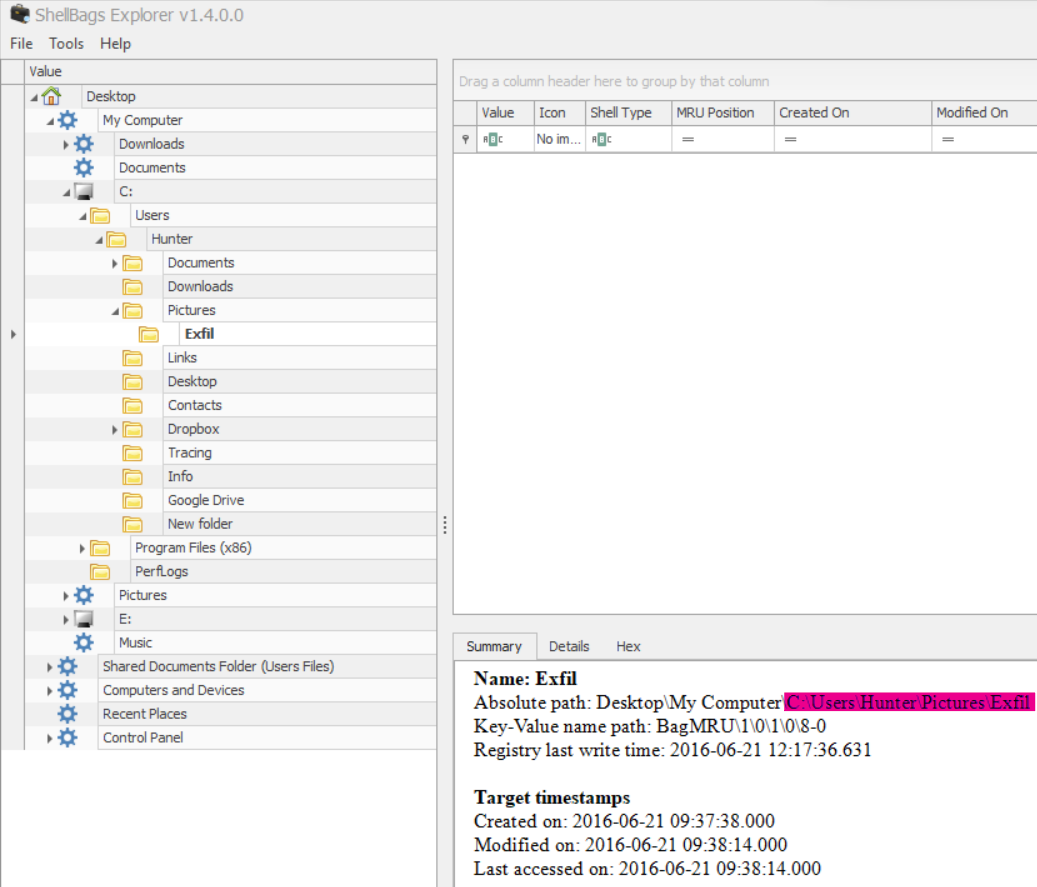


Daha sonra USERCLASS.DAT’ı Shellbags Explorer aracı ile inceliyorum.



Burada 66 adet shellbag’in bulunduğunu söylüyor.

İncelediğimde kalsörler arasında “Exfil “ adında bir klasöre denk geliyorum.

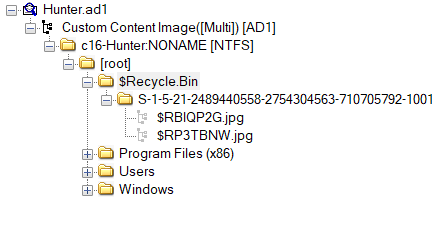


**CEVAP = C:\Users\Hunter\Pictures\Exfil**

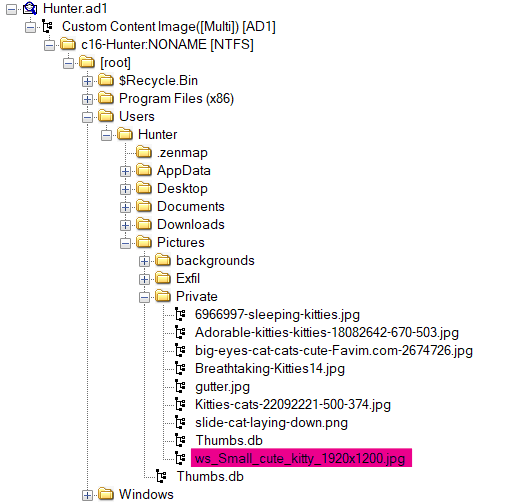
**SORU 28**

“The user deleted two JPG files from the system and moved them to $Recycle-Bin. What is the file name that has the resolution of 1920x1200?”

Kullanıcı iki JPG dosyasını sistemden sildiğini ve bunları $Recycle-Bin'e taşıdığını söylüyor. 1920x1200 çözünürlüğündeki dosyanın adı isteniyor bizden.



Burada 2 adet JPG dosyası var fakat dosya isimleri cevap için uygun değil.



Pictures adlı klasörü görünce kurcalıyorum. 1920x1200 görünce aradığım şey olduğunu düşünüyorum ve Recycle.Bin içerisindeki JPGler ile karşılaştırıyorum. Aynı resmin orada da olduğunu görüyorum ve aradığım şeyin bu olduğunu anlıyorum.

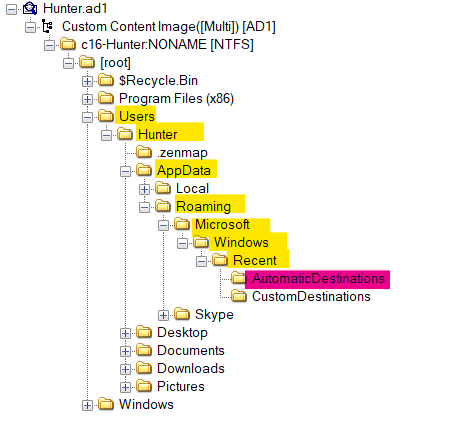
**CEVAP = ws\_Small\_cute\_kitty\_1920x1200.jpg**

**SORU 29**

“Provide the name of the directory where information about jump lists items (created automatically by the system) is stored?”

Jump lists hakkında bilgilerin saklandığı otomatik olarak oluşturulan dizini istemiş.

*Users/User/AppData/Roaming/Microsoft/Windows/Recent* dizininde oluşturulur.

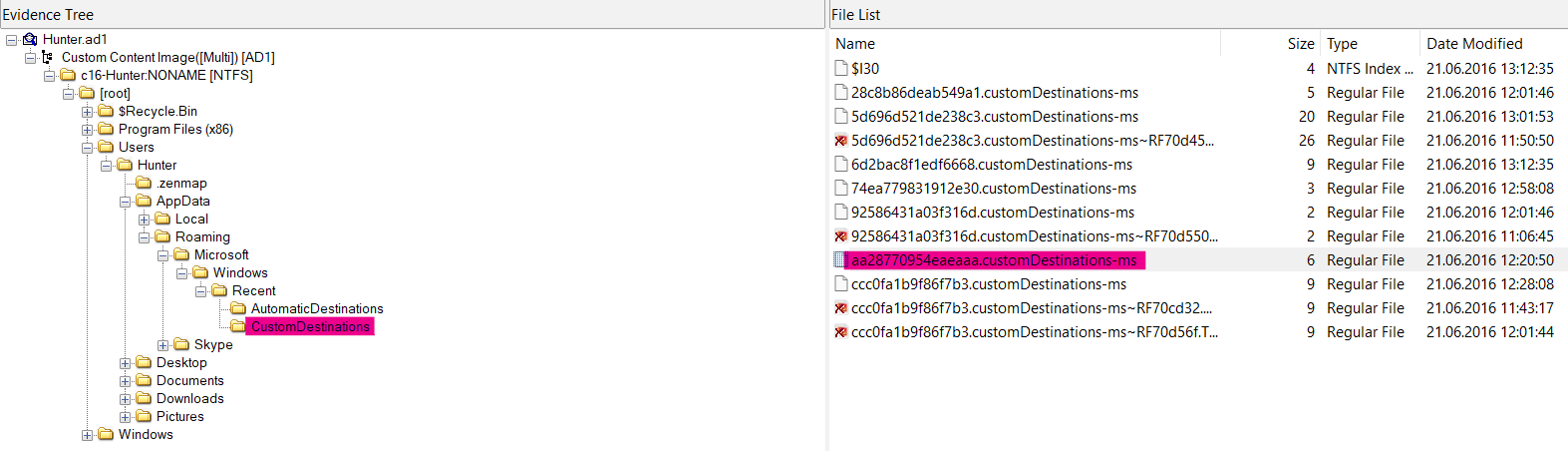


**CEVAP = AutomaticDestinations**

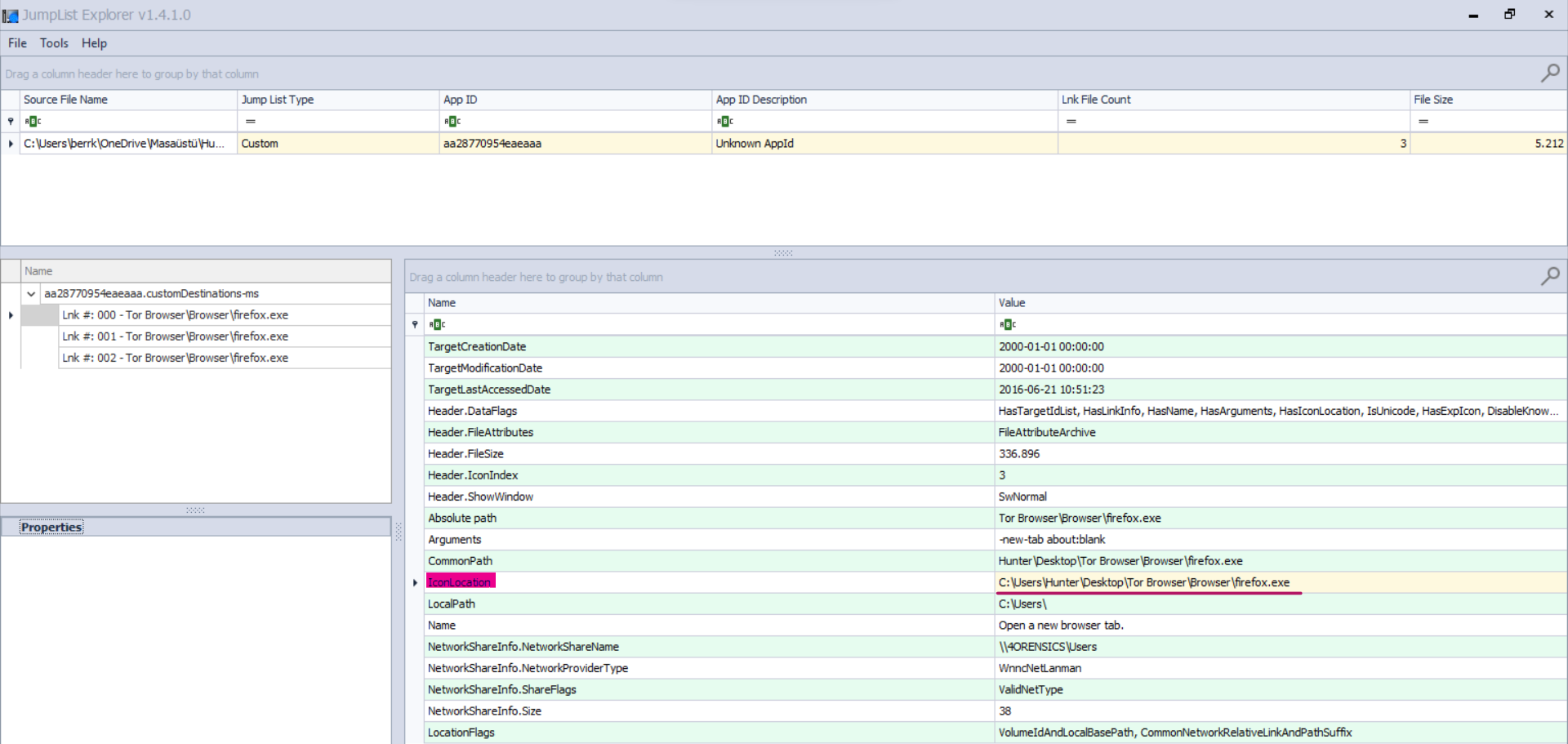
**SORU 30**

“Using JUMP LIST analysis, provide the full path of the application with the AppID of "aa28770954eaeaaa" used to bypass network security monitoring controls.”

 "aa28770954eaeaaa" AppID'sini kullanan uygulamanın tam yolunu jump list analizini kullanarak bulmamız isteniyor. Ağ güvenliği izleme kontrollerini atlamak için kullanılıyormuş.



Bize verilen Id’ye ait jumplist’i incelemek için export ediyorum. Bu dosyayı jumplist explorer ile inceliyorum ve uygulamanın tam yolunu buluyorum.



**CEVAP = C:\Users\Hunter\Desktop\Tor Browser\Browser\firefox.exe**