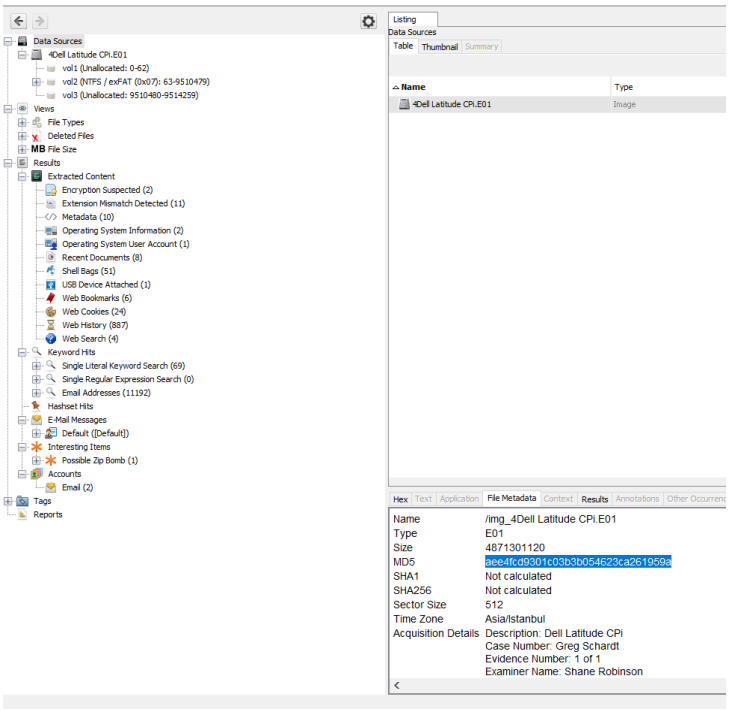
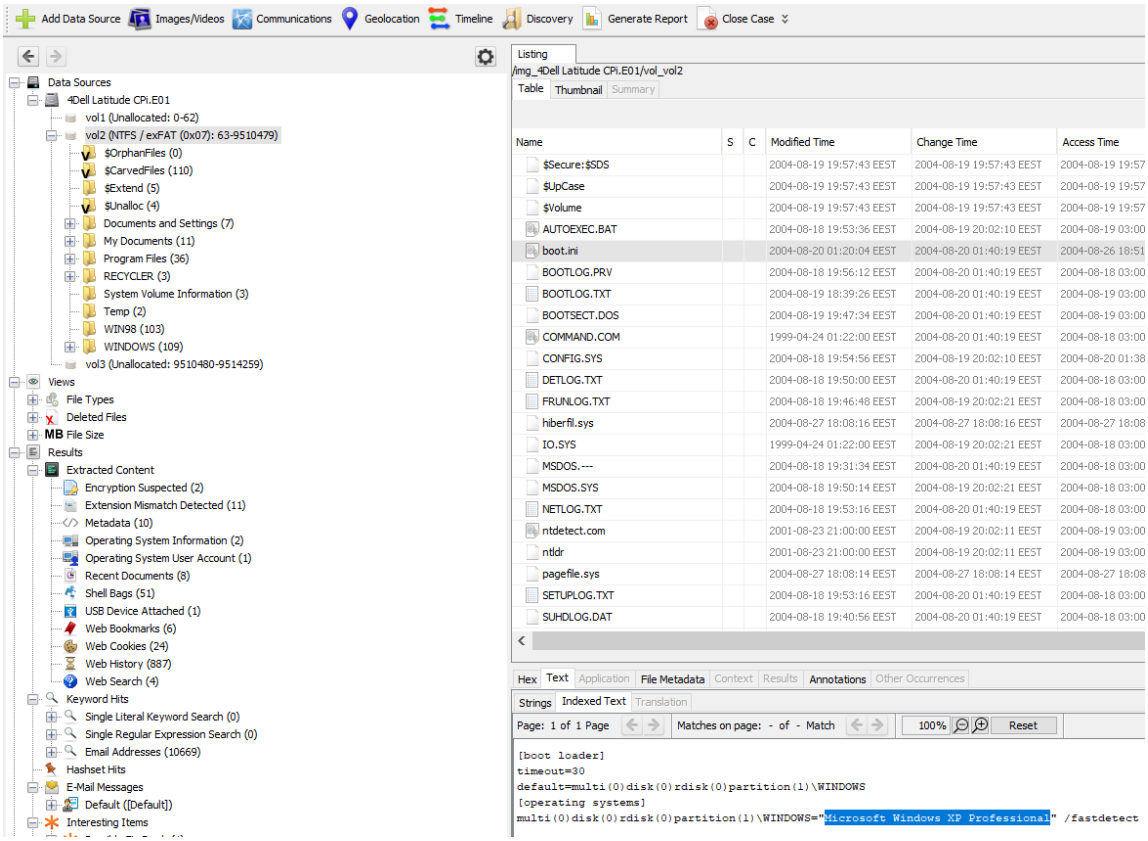
4DELL VAKA ANALİZ RAPORU

- Hash değeri



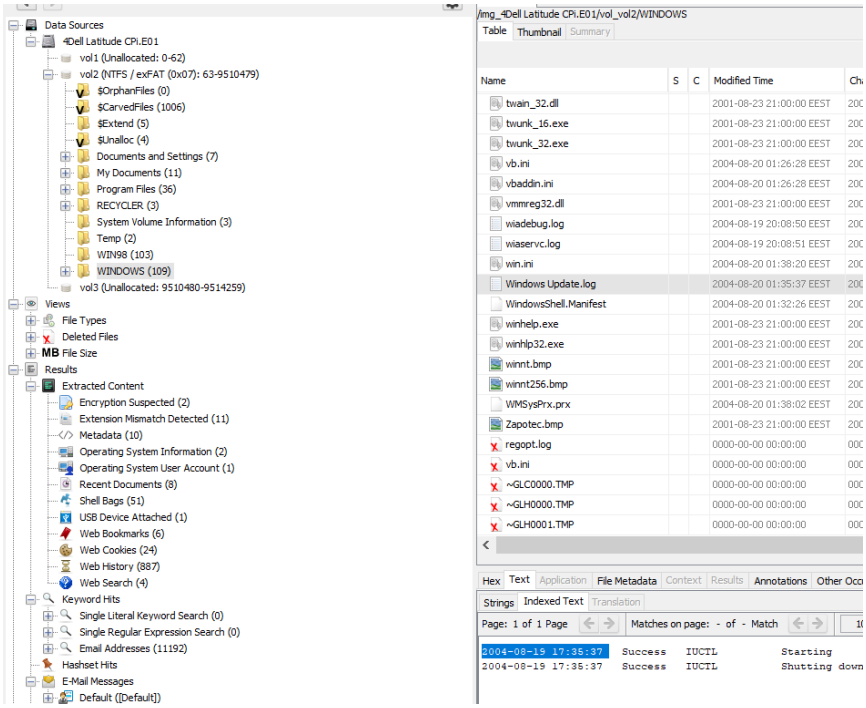
Hash değerini bulmak için imaj dosyasının dosya meta verilerine bakıyoruz. Burada hash değerinin md5 formatında “aee4fcd9301c03b3b054623ca261959a” olduğunu görüyoruz.

- İşletim sistemi



NTFS dosya sisteminde boot.ini dosyasına baktığımızda Microsoft Windows XP işletim sistemini ve Professional sürümünün kullanıldığı buluyoruz.

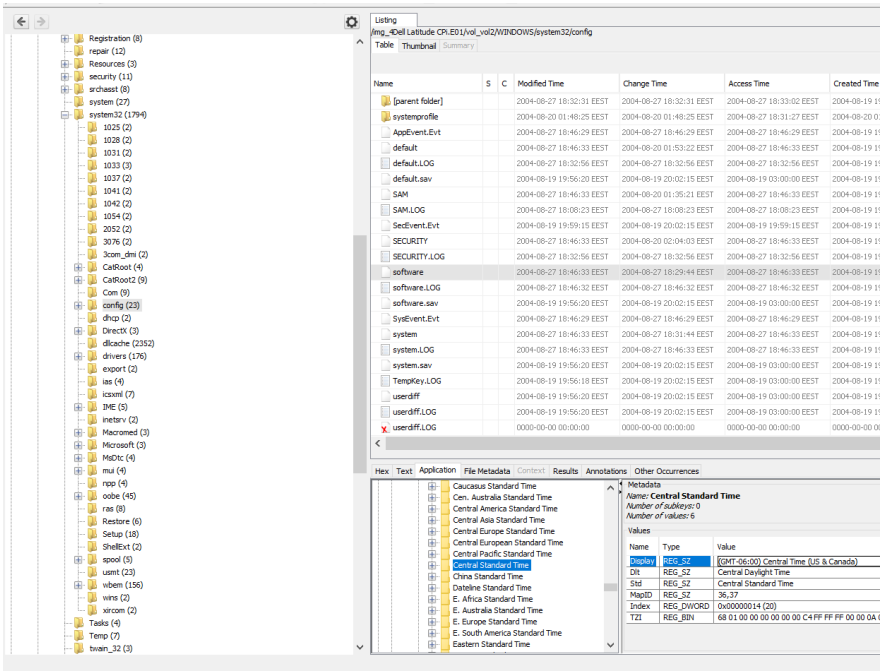
- Kurulum tarihi



Kurulum tarihini öğrenmek için Windows klasöründeki Windows update.log kayıtlarına bakıyoruz.

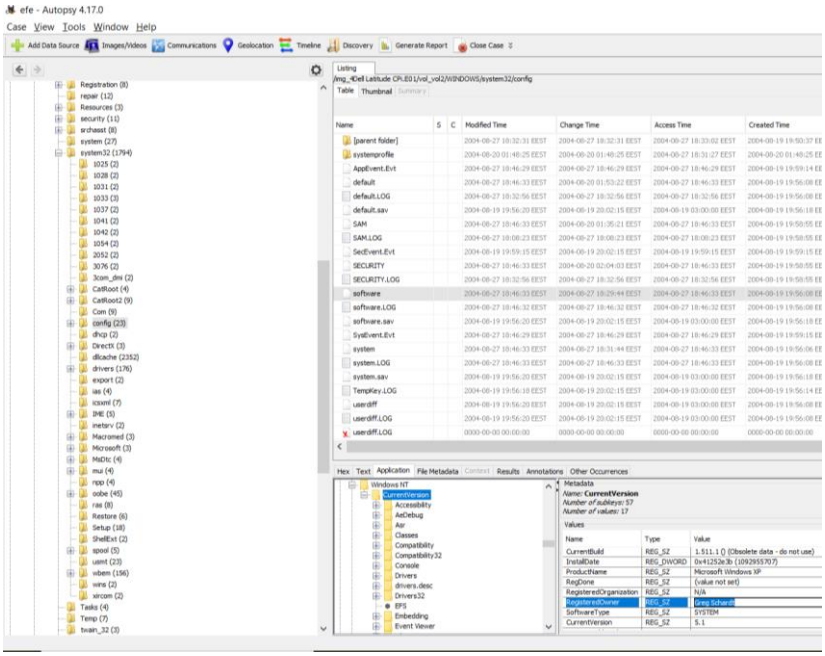
Buradan 2004-08-19 17:35:37 gibi bir sonuçla karşılaşıyoruz. Önceki sürümden Windows XP'ye 19 ağustos 2004 tarihinde saat17:35 de güncellendiğini görüyoruz.

- Saat dilimi



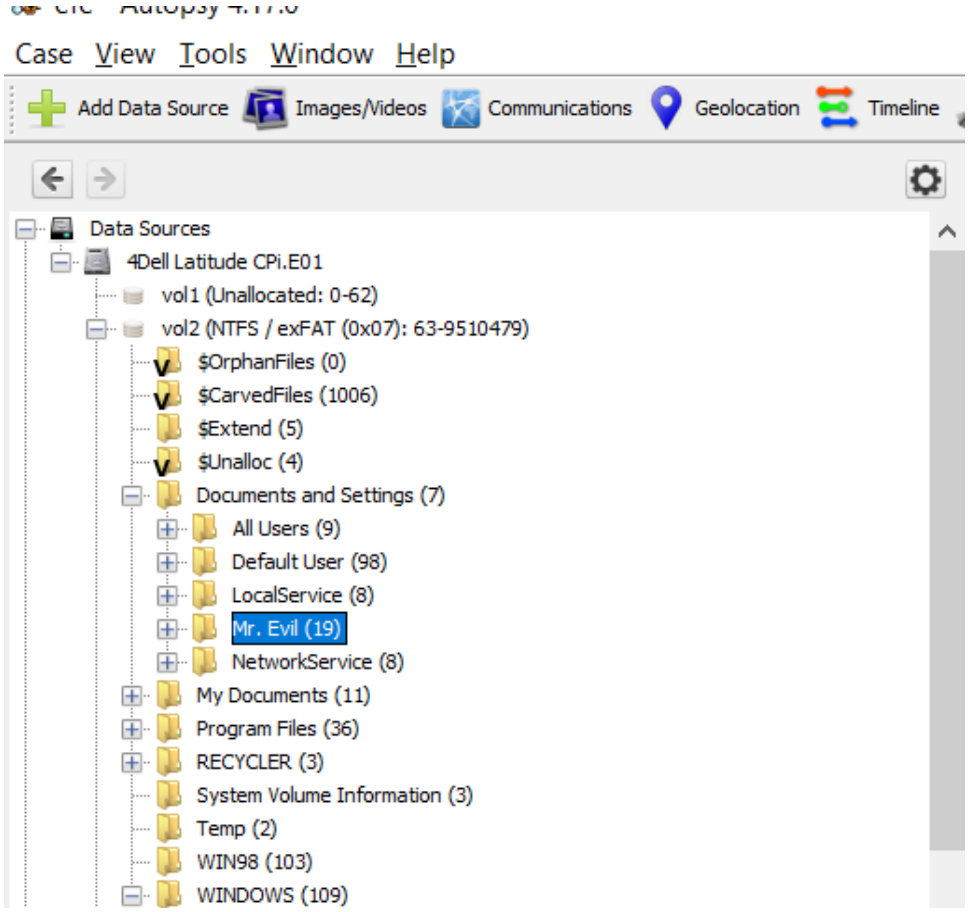
Saat dilimini öğrenmek için Windows/system32 dosyasında bulunan software'ye giriyoruz. Ardından Microsoft\Windows NT\CurrentVersion\Time Zones'un içerisinde GMT-06:00 saat dilimi kullanıldığını buluyoruz.

- Cihaz sahibi



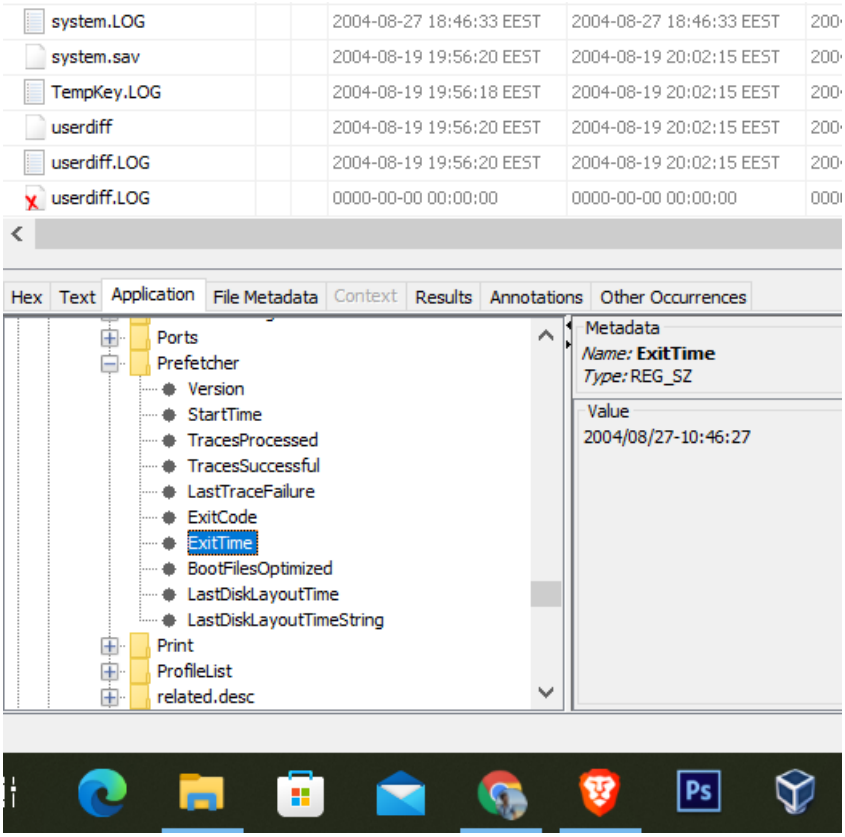
Saat dilimini öğrenirken girdiğimiz dosya konumunda bu kez CurrentVersion'un içerisinde Greg Schardt isimli kişinin kayıtlı kişi olduğunu öğreniyoruz.

- Hesap ismi



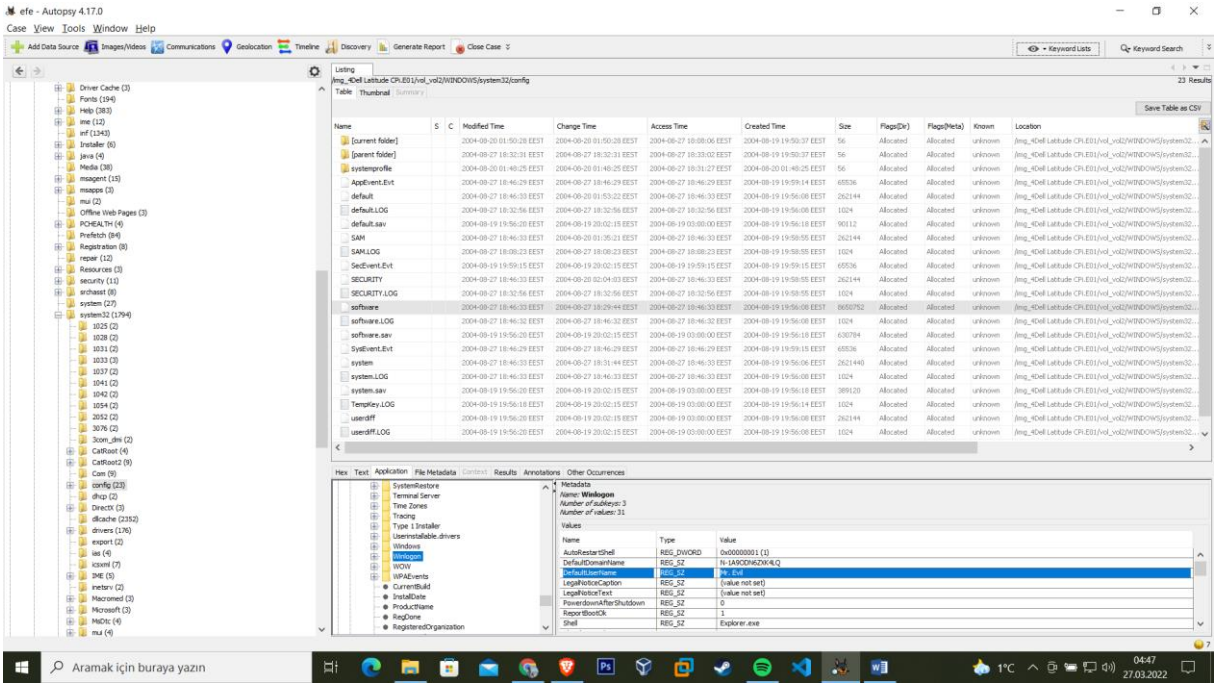
Hesap isminin ise Documents and Setting bölümünden “Mr. Evil” yani bay kötü olduğunu öğreniyoruz.

- Cihazın son kapanma zamanı



Cihaz sahibini öğrenmek için girdiğimiz CurrentVersion dosyasında bu sefer Prefetcher dosyasına giriyoruz buradaki ExitTime bölümünden son kapanma zamanını şu şekilde buluyoruz: 27/08/2004–10:46:27

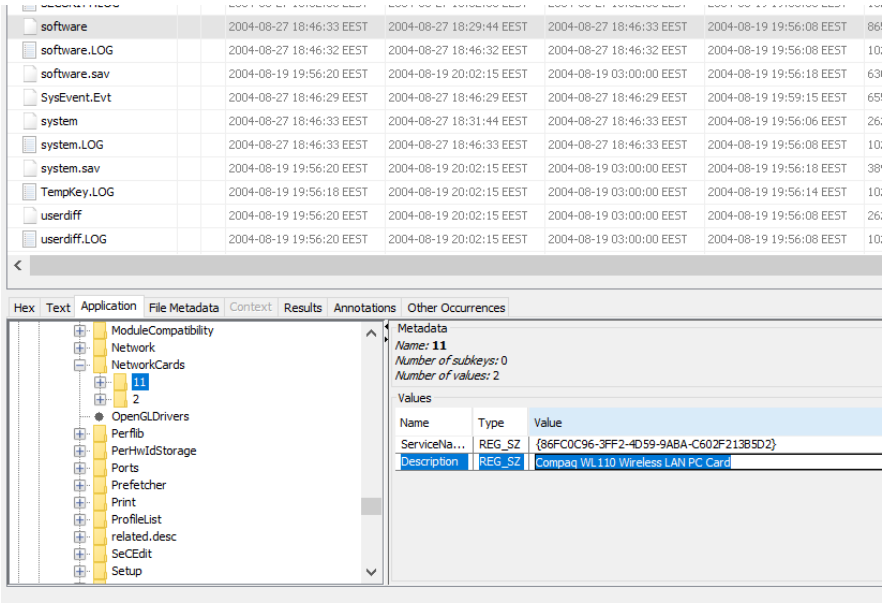
- Kullanıcı sayısı



Cihazda bulunan kullanıcı sayısını bulmak için system32 dosyasında bulunan config dosyasındaki SAM

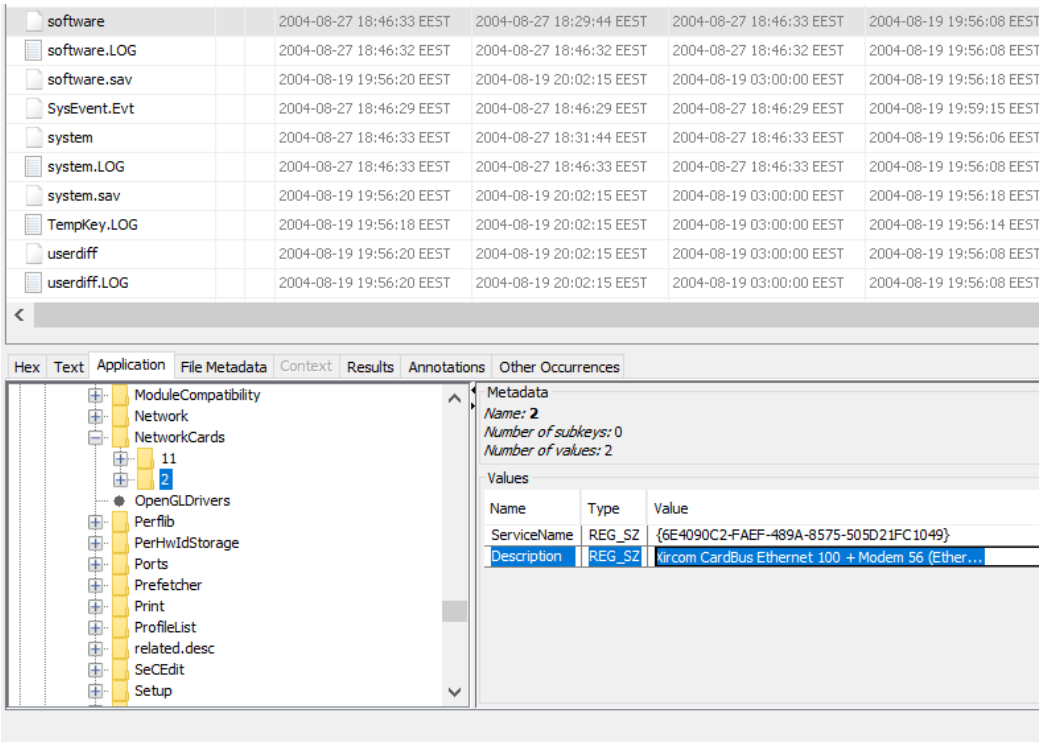
dosyasına giriyoruz.SAM/SAM/Domains/Account/Users/Names bölümünde 5adet kullanıcı yer aldığını görebiliyoruz.

- Oturum açan son kullanıcı



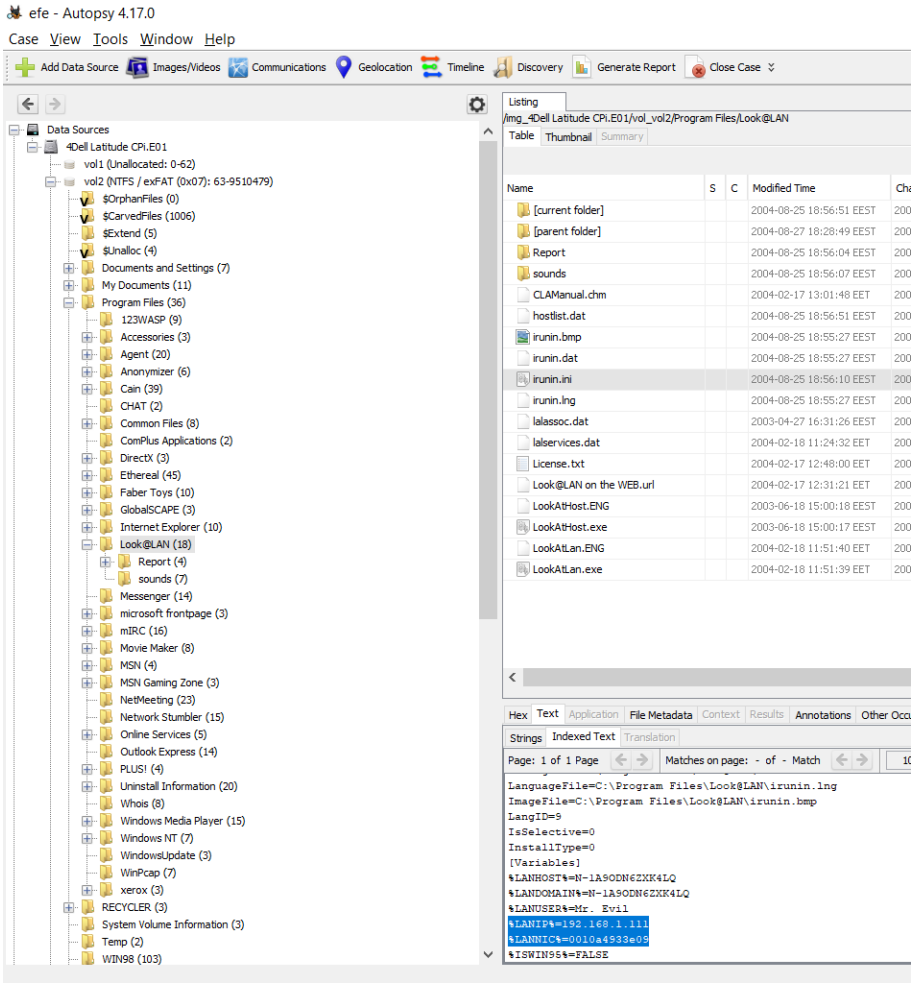
Cihazda oturum açan son kullanıcıyı bulmak için CurrentVersion'daki Winlogon dosyasına bakıyoruz ve son giriş yapan kullanıcının Mr. Evil olduğunu görüyoruz.

- Kullanılan ağ kartları



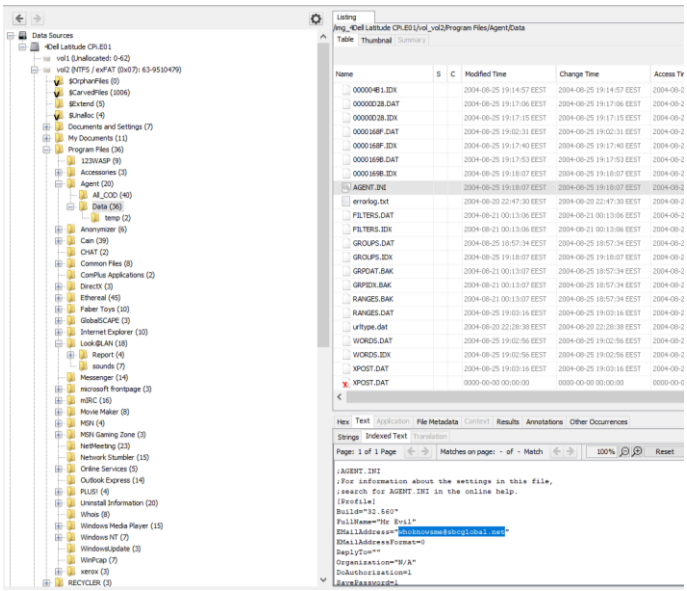
Bu cihazdaki kullanılan ağ kartlarını öğrenmek için CurrentVersion içerisinde yer alan NetworkCards dosyasını inceliyoruz ve Compaq WL110 Wireless LAN PC Card Xircom ve CardBus Ethernet 100 + Modem 56 (Ether... ağ kartlarını görüyoruz.

- IP adresi ve MAC adresi



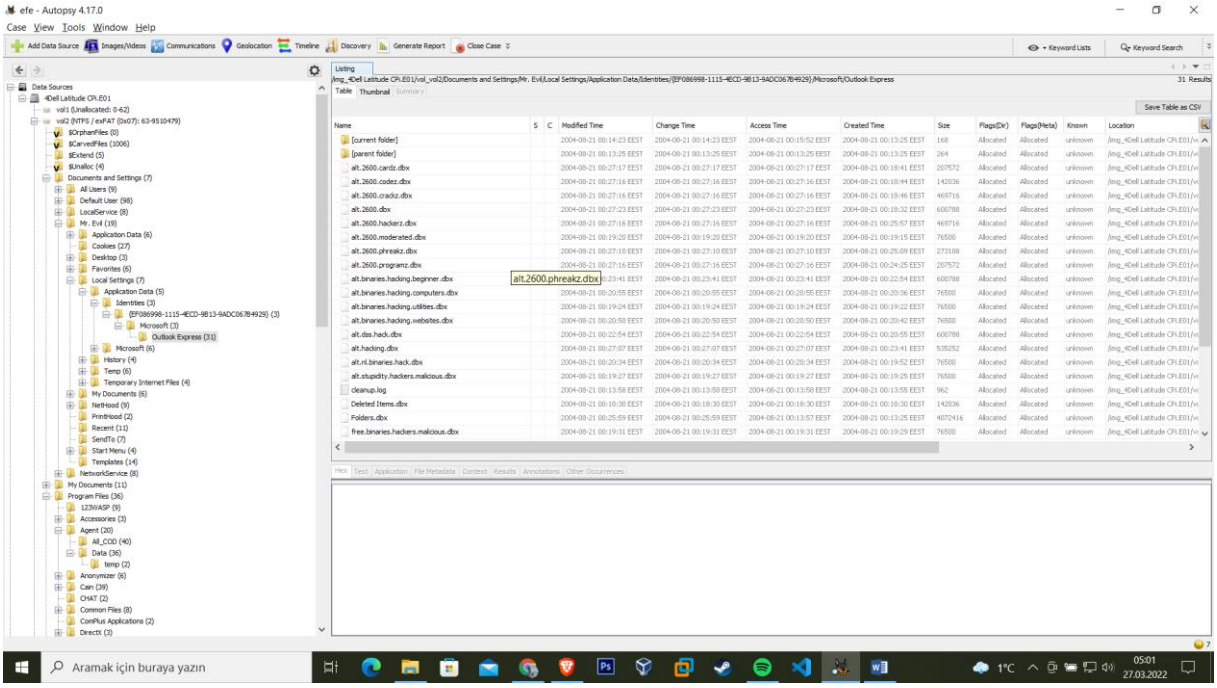
Program Files dosyasından Look@LAN dosyasındaki irunun.ini'yi incelediğimiz zaman İp adresini 192.168.1.111 olduğunu ve MAC adresinin 0010a4933e09 olduğunu görüyoruz.

- E-posta adresi



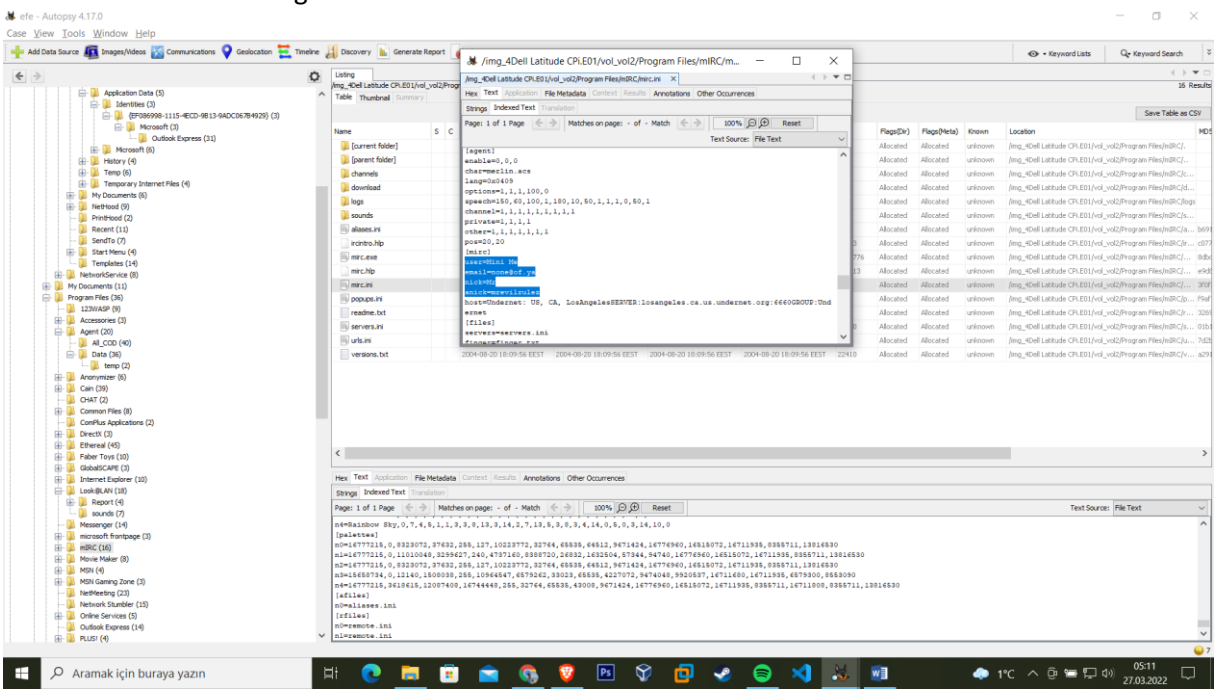
Program Files/Agent/Data/AGENT.İNİ'yi incelediğimiz zaman Mr. Evil'ın e-posta adresinin whoknowsme@sbcglobal.net olduğunu görüyoruz.

- Abonelikler



Mr. Evil'ın abone olduğu grupları görmek için Documents and Settings\Mr. Evil/Local Settings\Application Data\Identities\Microsoft\Outlook Express konumunu inceliyoruz. Burada bir çok hack grubuna abone olduğunu öğreniyoruz.

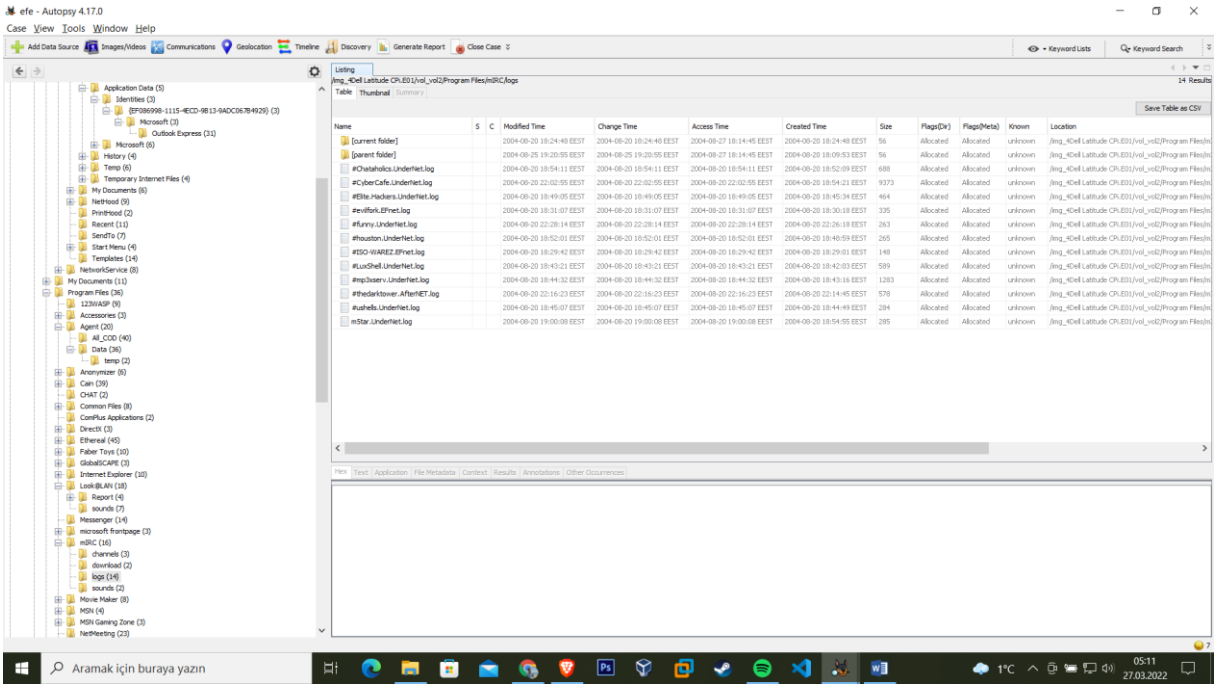
- Mirc kullanıcı bilgileri



Bu bilgiler erişmek için mIRC dosyasındaki mirc.ini'yi incelememiz yeterli olacaktır ve aşağıdaki bilgilere erişeceğiz.

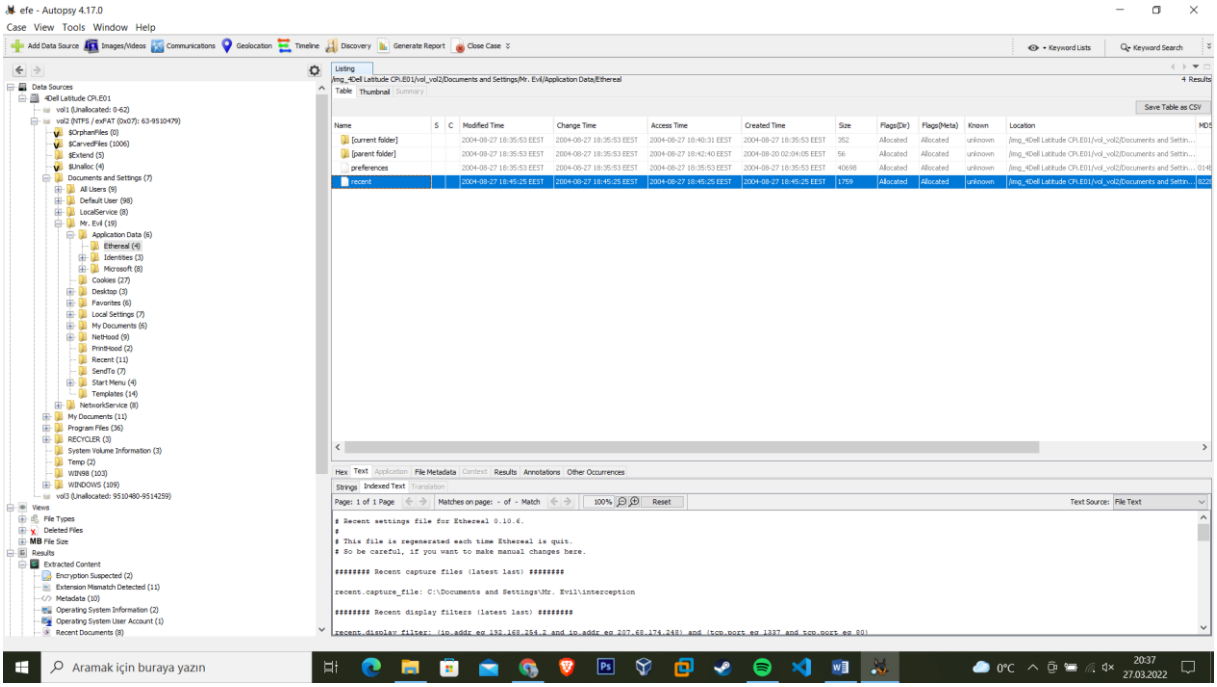
user=Mini Me
email=none@of.ya
nick=Mr
anick=mrevilrulez

- Mirc kanalları



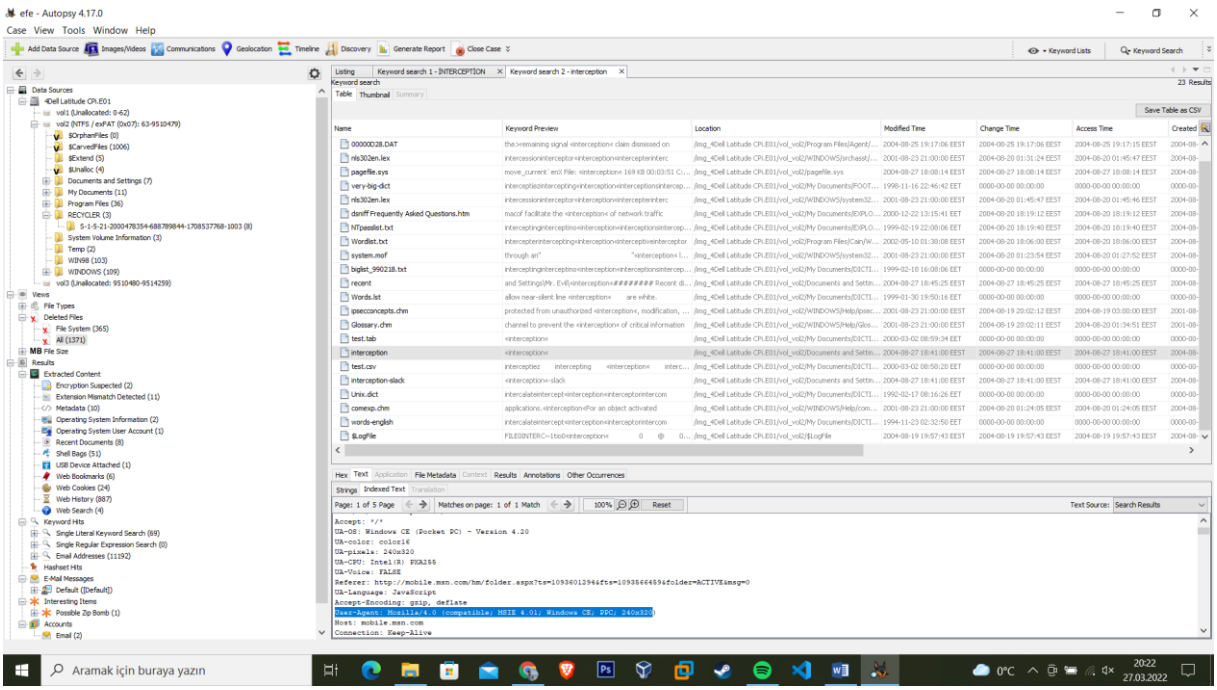
Bu kanallara erişmek için mIRC içerisinde yer alan logs dosyasına bakıyoruz ve bir çok kanalın yer aldığını görüyoruz.

- Şüpheli uygulama



Mr. Evil dosyası içerisindeki Application Data klasöründe Ethereal programının yer aldığını görüyoruz. Bu program internet paketlerini kesmek için kullanılır. Recentte ise programın kullanıldığını ve işlemlerin başarılı olduğunu görüyoruz.

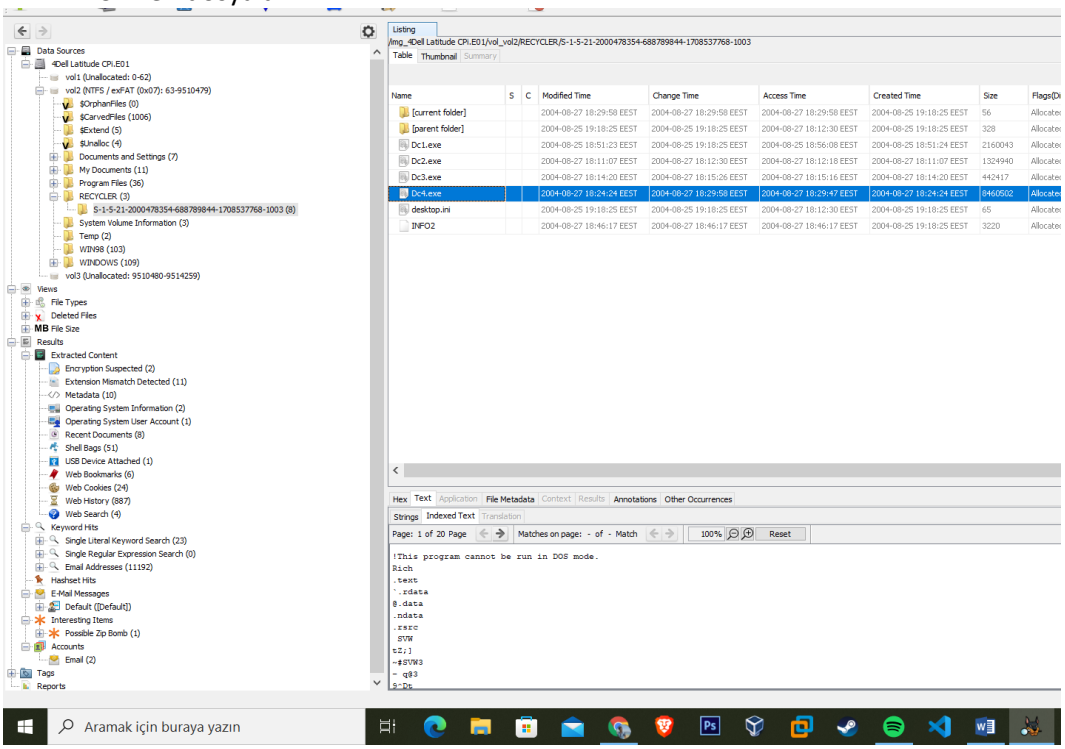
- Mağdurun bilgileri



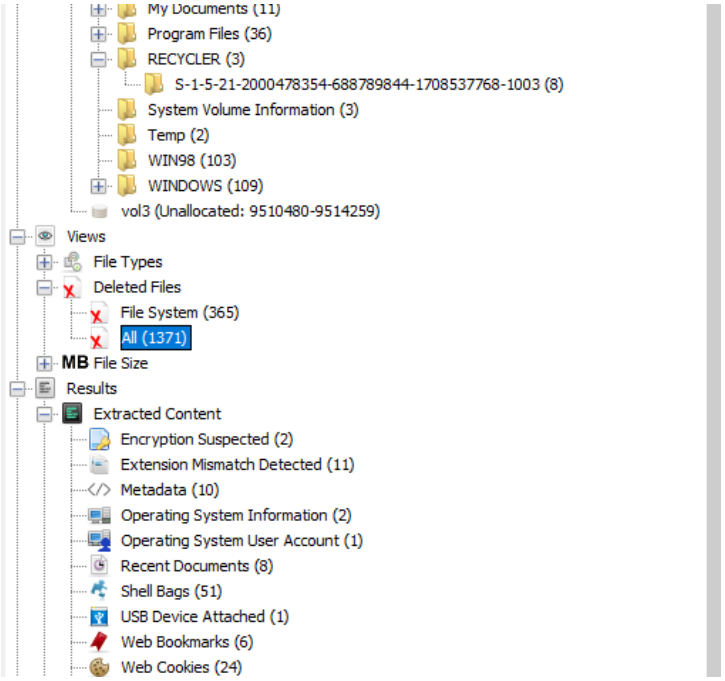
Kelime araması kısmında “interception”u aratıyoruz ve çıkan interception dosyasını inceliyoruz buradan mağdur kişinin Windows ce isimli bir cihazdan Mozilla 4.0 tarayıcısından giriş yaptığı görülüyor.

Ayrıca mağdur kişi mobile.msn.com a erişiyormuş.

- Silinen dosyalar

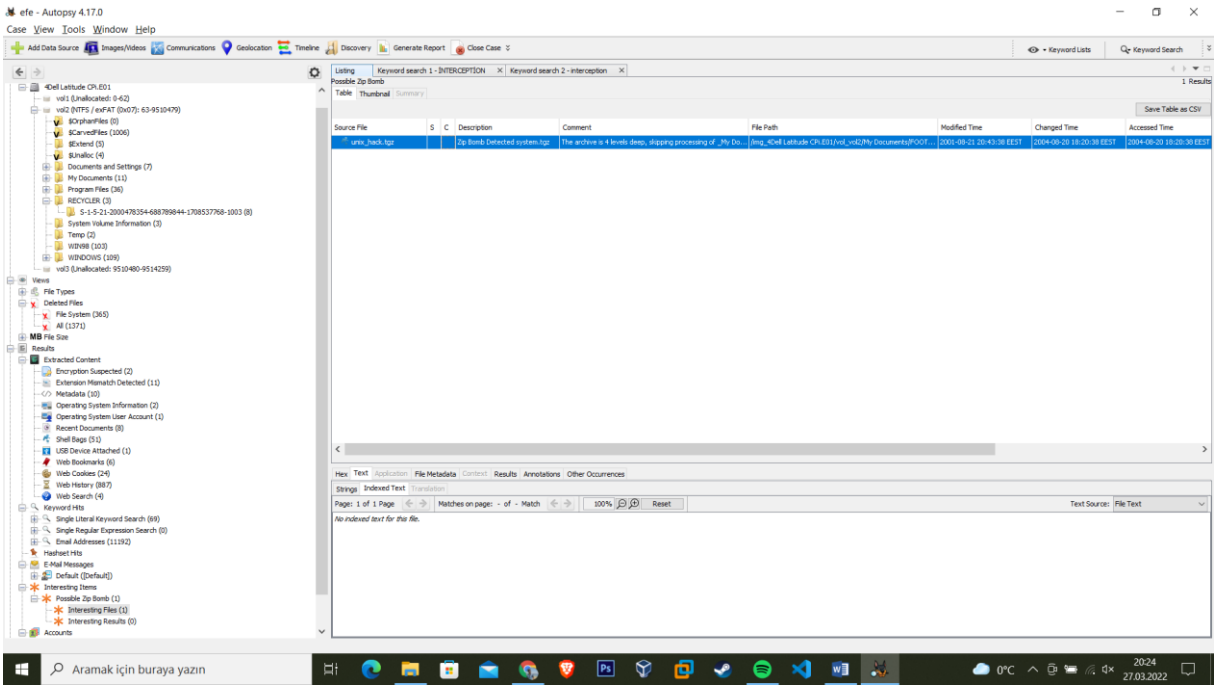


Geri dönüşüm kutusuna gönderilen 4 adet exe dosyası mevcut.



Gerçekten silinen ise 1371 adet dosya vardır.

- Cihazda Virüs var mı?



İlginç dosyalara baktığımız zaman bir adet zip bombası olduğunu görüyoruz.