

**TASK 1**  **Volatility forensics**

**1.Soru**

Victim.zip adlı dosyayı indirmemiz ve zipten çıkarmamız isteniyor.

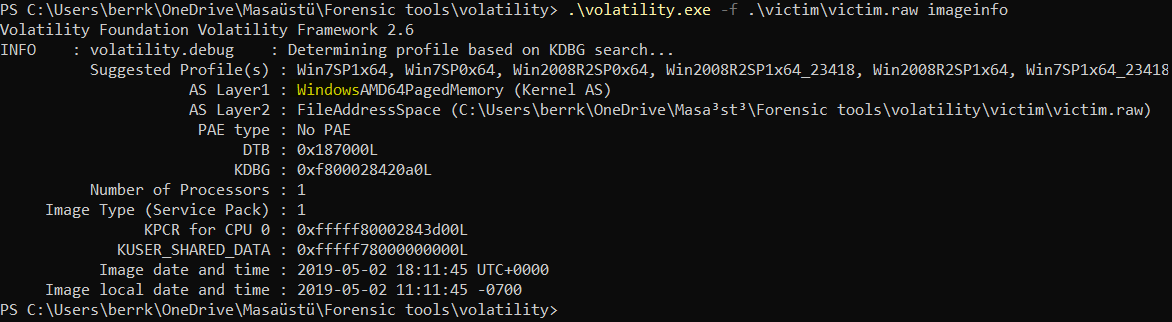
Bu odada volatility aracını kullanacağız. Bu araç, Python ile yazılmış açık kaynak kodlu bir memory forensics aracıdır. Volatility, bir bilgisayarın bellek görüntülerini inceleyerek, sistemin o anki durumu hakkında bilgi sağlar. Bu analiz, bir sistemde meydana gelen saldırıların tespiti, kötü amaçlı yazılımların belirlenmesi veya olay müdahale süreçlerinde kullanılabilir.

**2.Soru**

“What is the Operating System of this Dump file? (OS name) “

Bu soruda bize işletim sistemi soruluyor. Volatility kullanarak image hakkında bilgi toplayacağız.

*“.\volatility.exe -f .\victim\victim.raw imageinfo”* komutu ile işletim sistemini öğreniyoruz.



**CEVAP = Windows**

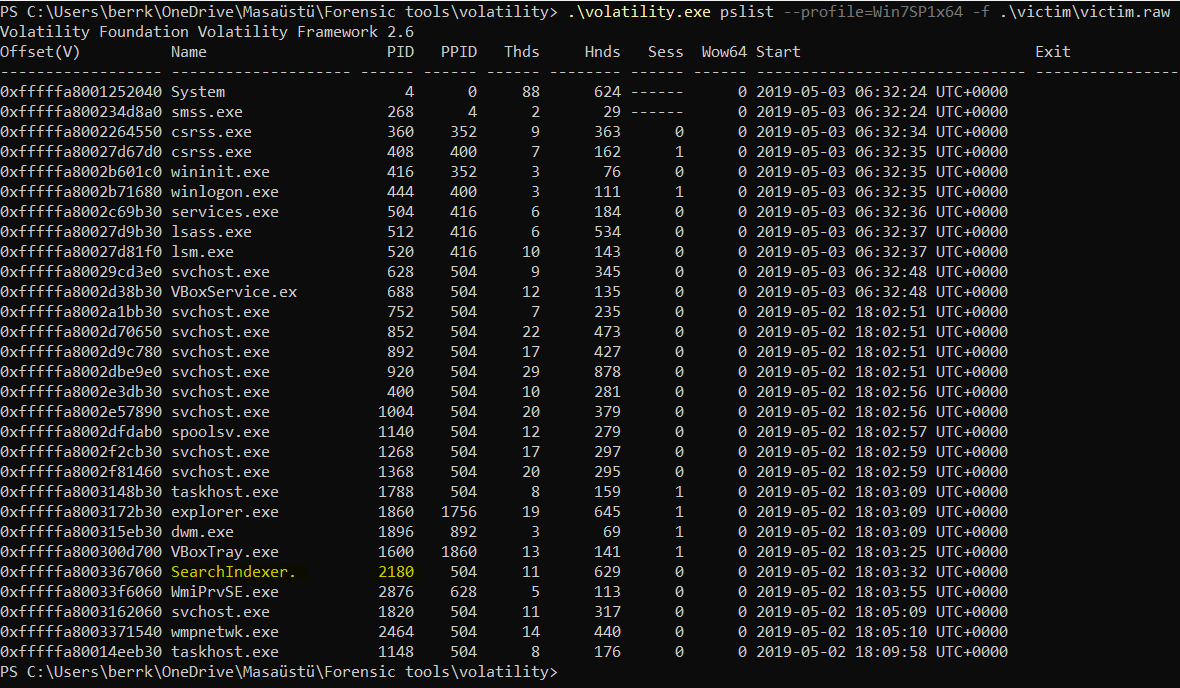
**3.Soru**

“What is the PID of SearchIndexer?”

SearchIndexer’in PID’si soruluyor.

*“.\volatility.exe pslist --profile=Win7SP1x64 -f .\victim\victim.raw”*

pslist komutu, Çalışan tüm prosesleri, PID değerlerini, başlatılma zamanlarını gibi değerleri getirir.



**CEVAP = 2180**

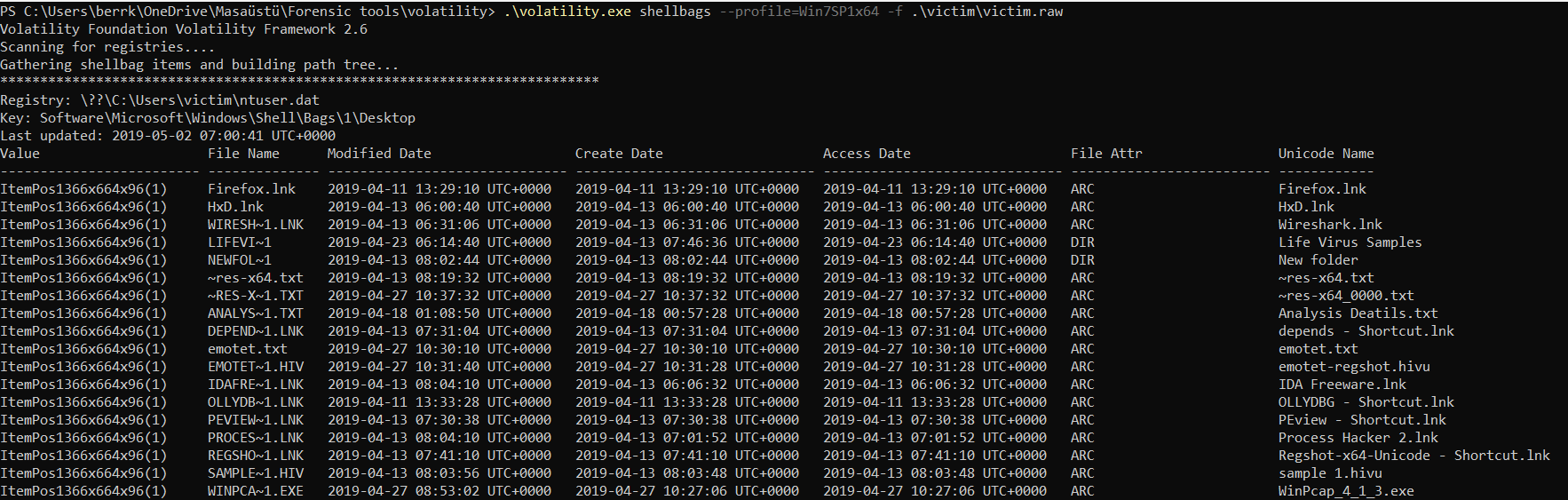
**4.Soru**

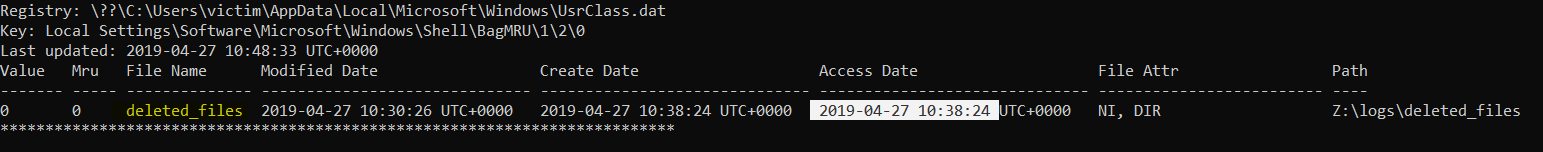
“What is the last directory accessed by the user? “

Kullanıcının eriştiği son dizin soruluyor.

Windows işletim sisteminde dosya ve dizinlerin görünümü hakkında bilgiyi shellBag tutar. Shellbag analizi, bir bilgisayarın kullanım geçmişini, dosya gezgini davranışları ve kullanıcı etkileşimleri hakkında bilgiler elde etmemizi sağlar. Erişim tarihi ve saatini kontrol ederek istenilen bilgiye erişiyoruz.

*“.\volatility.exe shellbags --profile=Win7SP1x64 -f .\victim\victim.raw”*





**CEVAP = deleted\_files**

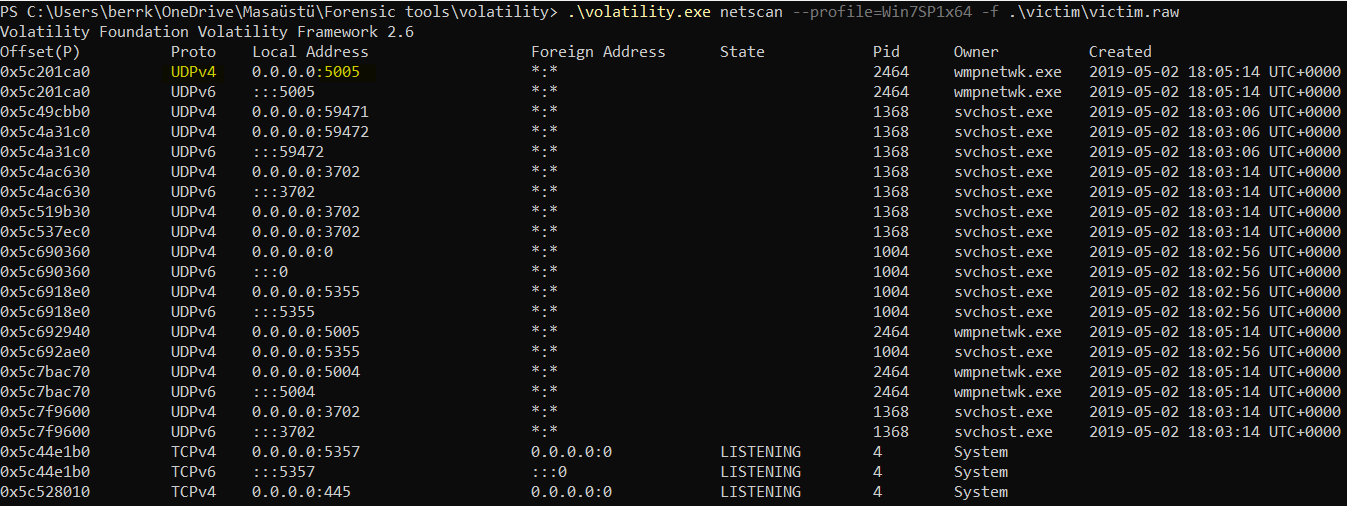
**TASK 2**

**1.Soru**

“There are many suspicious open ports; which one is it?”

Açık birçok bağlantı noktası olduğunu ve bu noklatardan süpheli olanı istiyor bizden…

Volatility aracının netscan komutunu kullanarak açık bağlantı noktalarını tespit edebiliriz.



Birçok port açık ancak hintte ilk olanı istemiş.

**CEVAP = UDP:5005**

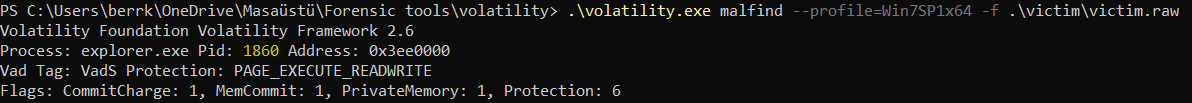
**2.Soru**

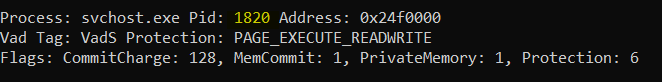
“Vads tag and execute protection are strong indicators of malicious processes; can you find which they are?”

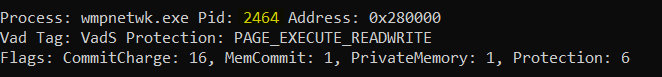
Vads etiketi ve yürütme koruması, kötü amaçlı işlemlerin güçlü göstergesidir, hangileri olduklarını bulabilir misin? (PID’ler)

Kötü amaçlı işlemleri tespit eden volatility komutu olan “malfind” kullanarak bunları tespit edeceğim.

*“.\volatility.exe malfind --profile=Win7SP1x64 -f .\victim\victim.raw”*







Çıktı sonucunda üç farklı PID buluyorum. Üçündede vads etiketi mevcut

**CEVAP = 1820;1860;2464**

**TASK 3 IOC SAGA**

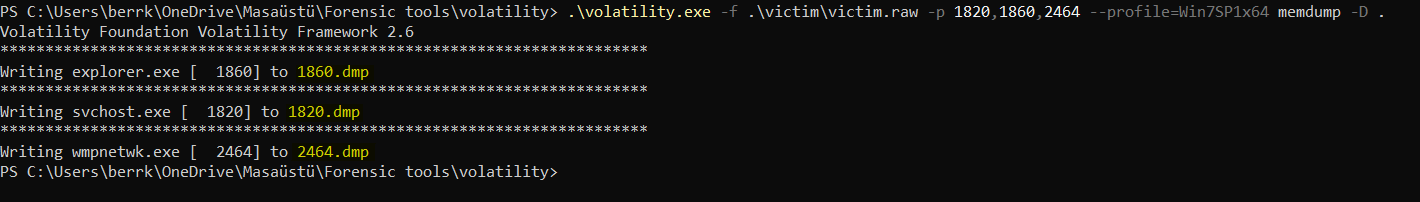
IOC, "Indicator of Compromise" (Tehdit Belirteci) kısaltmasıdır. Bir bilgisayar sisteminde veya ağda mevcut olan bir güvenlik tehdidini belirlemek için kullanılan belirli bir işareti veya belirteciyi ifade eder.

Genellikle güvenlik olaylarını tespit etmek ve ele almak için kullanılan güvenlik sistemleri ve araçları tarafından kullanılır. Bu belirteçler, kötü amaçlı yazılımlar, saldırılar veya diğer güvenlik tehditleri ile ilişkilendirilmiş olabilir. İşte IOC'lerin örnekleri;

* Dosya adlrı ve yolları
* Ip adresleri
* Domain adları
* Hash değerleri
* URL’ler

Elde ettiğimiz zararlı olabilecek 1820,1860,2426 PID’li şüpheli dosyalarla ilgili daha fazla analiz yapabilmek için volatility aracımızın *memdump* komutunu kullanarak bu zararlıları tek tek inceleyeceğiz.

*“.\volatility.exe -f .\victim\victim.raw -p 1820,1860,2464 --profile=Win7SP1x64 memdump -D .”* komutu ile zararlı exe’leri elde ediyoruz.



**1.Soru**

“ 'www.go\*\*\*\*.ru' (write full url without any quotation marks)”

Bu sorularda strings ve grep komutlarını kullanarak bizden istenilen bilgilere ulaşmaya çalışacağız. Strings komutu .dump dosyası içindeki her şeyi bize getirecek, grep komutu ise bu çıktı içerisinde filtreleme yapmamızı sağlaycak. Yani grep sayesinde spesifik olarak arama yapabileceğiz.



**CEVAP =** [**www.goporn.ru**](http://www.goporn.ru)

**2.Soru**

'www.i\*\*\*\*.com'

****

**CEVAP =** [**www.ikaka.com**](http://www.ikaka.com)

**3.Soru**

'www.ic\*\*\*\*\*\*.com'



**CEVAP = www.icsalabs.com**

**4.Soru**  
“202.\*\*\*.233.\*\*\* (Write full IP)”

****

**CEVAP = 202.107.233.211**

**5.Soru**

“\*\*\*.200.\*\*.164 (Write full IP)”

****

**CEVAP = 209.200.12.164**

**6.Soru**

“ 209.190.\*\*\*.\*\*\* ”

****

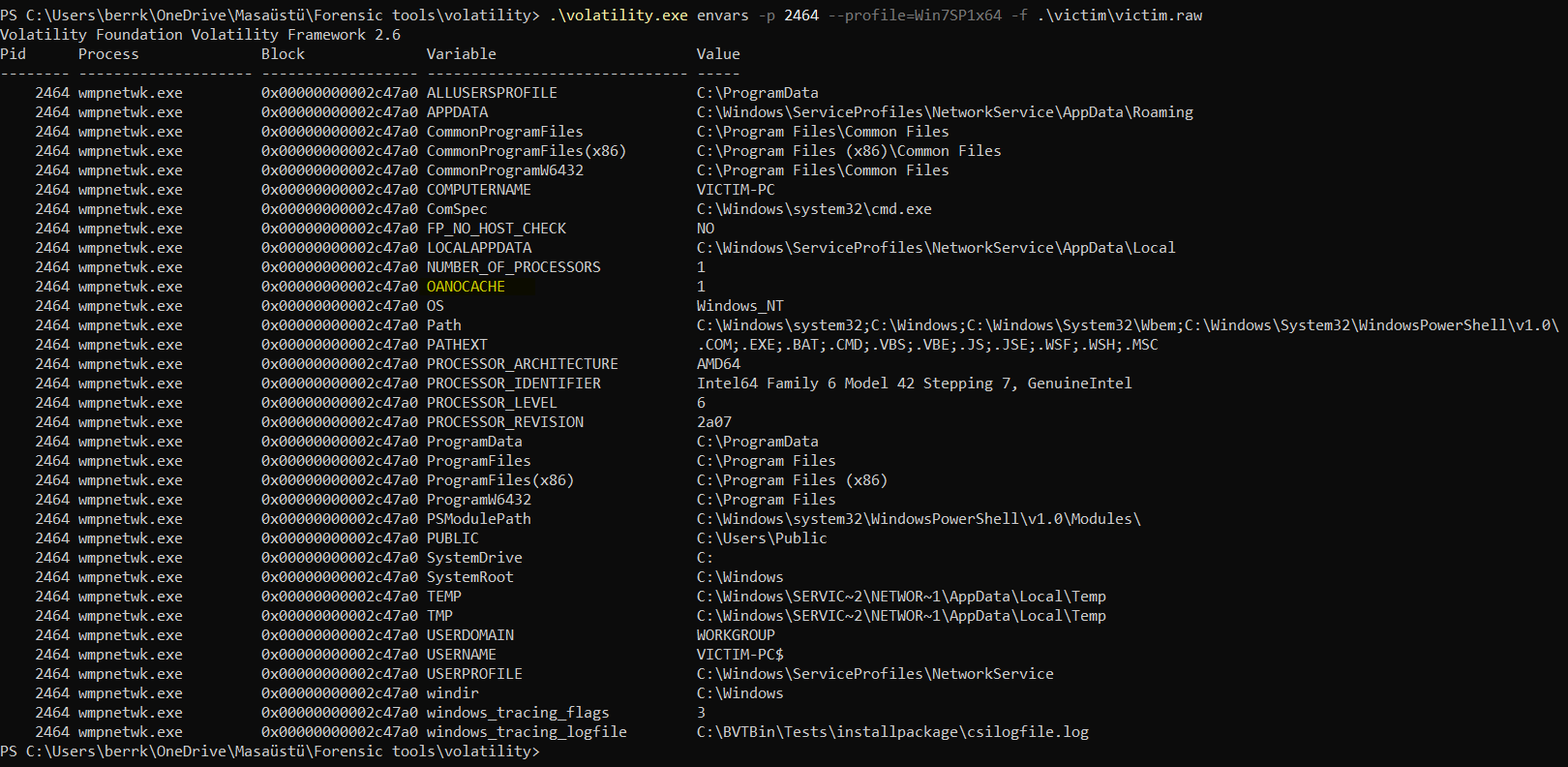
**CEVAP = 209.190.122.186**

**7.Soru**

“ What is the unique environmental variable of PID 2464? ”

"Environmental variable" (çevresel değişken), bir bilgisayar işletim sistemi tarafından belirli bir işlemin veya uygulamanın çalışma ortamını belirlemek ve yapılandırmak için kullanılan bir değişkendir. Bu değişkenler, işletim sisteminin genel ayarlarını, sistem yapılandırmalarını ve kullanıcı tercihlerini depolar. Volatility aracında *envars* komutu ile bu değişkenleri çekebiliriz.

*“ .\volatility.exe envars -p 2464 --profile=Win7SP1x64 -f .\victim\victim.raw “*



PID’si 2464 olan process’in değişkenleri listelenmiş.

**CEVAP = OANOCACHE**