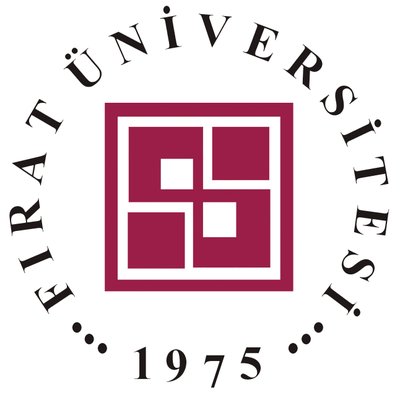
**T.C.**

**FIRAT ÜNİVERSİTESİ**

**TEKNOLOJİ FAKÜLTESİ**

**ADLİ BİLİŞİM MÜHENDİSLİĞİ BÖLÜMÜ**



**ABM317 – Bilişim Suçu İnceleme Donanımları  
Ödev Ön Raporu**

**TABLEAU TD3 İLE PRATİK ÇALIŞMA**

**175509027**

**MERVE NUR KARADAŞ**

**Danışman :** [**Dr. Öğr. Üyesi Mustafa KAYA**](https://abs.firat.edu.tr/mkaya)

Bu pratik çalışma raporu Tableau TD 3 Adli imaj ve kopya alma cihazı kullanılarak aşağıdaki adımların sırasıyla gerçekleştirilmesi neticesinde bilgisayar suçları inceleme donanımları dersi için oluşturulmuştur.

Pratik çalışma esnasında gerçekleştirilen adımlar:

1- USB Belleğin biçimlendirilerek içerisine ses, görüntü, doküman, video vs. ortamların yüklenmesi

2- İçerisinde veri bulunan USB Belleğin Tableau TD3 kullanılarak ilk olarak hash değerinin hesaplanması ve ardından fiziksel imajının alınıp hedef diske kayıt edilmesi

3- Aynı cihazın bu sefer de yine hash değerlerinin hesaplatılıp ardından logical (mantıksal) imajının alınması

4- USB Belleğin içerisindeki verilerin Windows işletim sistemi üzerinde basit yöntem doğrudan silinmesi

5-İçerisi boş olarak görünen USB Belleğin hash değerleri hesaplatılıp ardından imaj alınması

6- USB Belleğin Tableau TD3 cihazı kullanılarak WIPE edilmesi

7- Wipe edilen USB Belleğin tekrar hash değerlerinin hesaplatılıp ardından imajı alınması

8- Alınan imajlar üzerinden veri kurtarma işlemlerinin yapılması

9- Elde edilen sonuçların kıyaslanması ve çalışma raporunun oluşturulması

TABLEAU TD3 Adli imaj alma ve kopyalama cihazının görüntüsü:



TABLEAU TD3 cihazı ile farklı durumlarda imaj alıp bu imajlar üzerinden veri kurtarma ve inceleme işlemlerini yapmak üzerek tableau cihazımız kullanıma hazır hale getirildi.

-İlk olarak imaj almak istediğimiz ve imajımızı yükleyeceğimiz depolama cihazlarını source ve destination kısımlarına taktık.

-Ardından imaj yükleyeceğimiz cihazın boş olup olmadığını ‘blank check’ seçeneğinden kontrol ettik (Resim 1.1)..



**Resim 1.1**

İmajı alacağımız cihaz

(Destination)

İmajı alınacak cihaz

(Source)

-İmaj alacağımızın cihazımın ilk olarak hash değerini hesapladık, ayarlar kısmından araştırmacı bilgilerini, case id değiştirildikten sonra MD5 ve SHA1 hash değerleri hesaplandı(Resim 1.2).



**Resim 1.2**

-Hash değerleri hakkında daha ayrıntılı bilgi edinmek için view log yazısına tıklayarak hash işleminin ayrıntılarına bakıldı (Resim 1.3).

**Resim 1.3**

- View log seçeneği ayrıntıları (Resim 1.4.1-4). Bize kaynak, hedef disk hakkında ve hash değerleri hakkında bilgiler vermiştir.



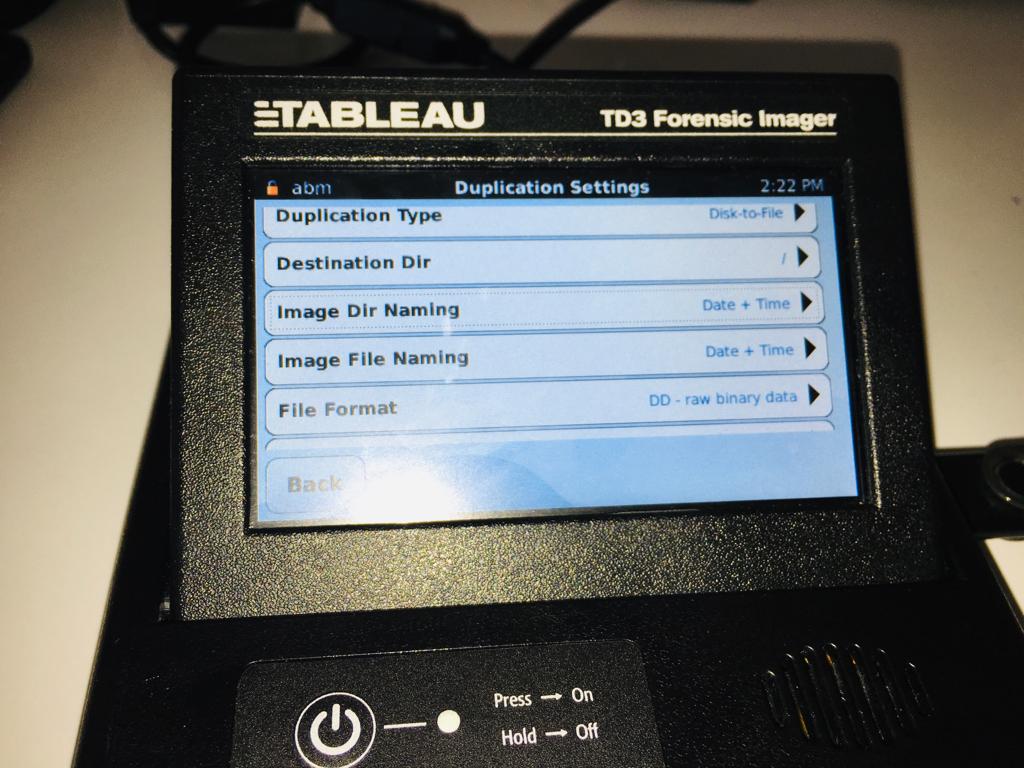
**Resim 1.4.1**

**Resim 1.4.2**

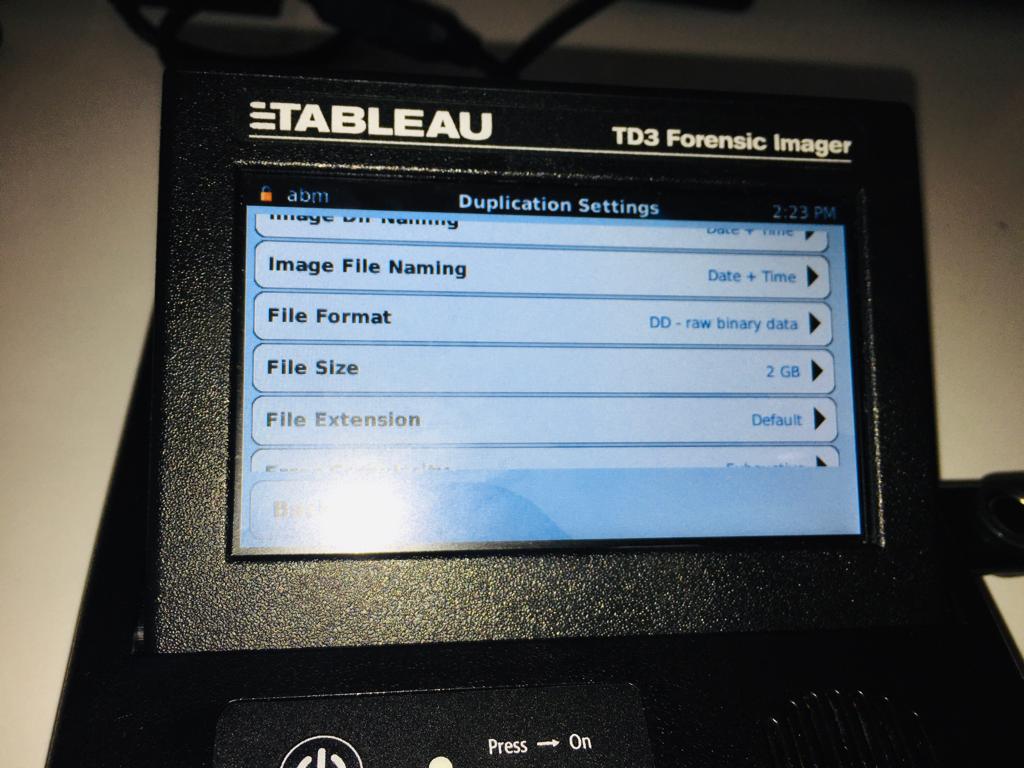
**Resim 1.4.3**

**Resim 1.4.4**

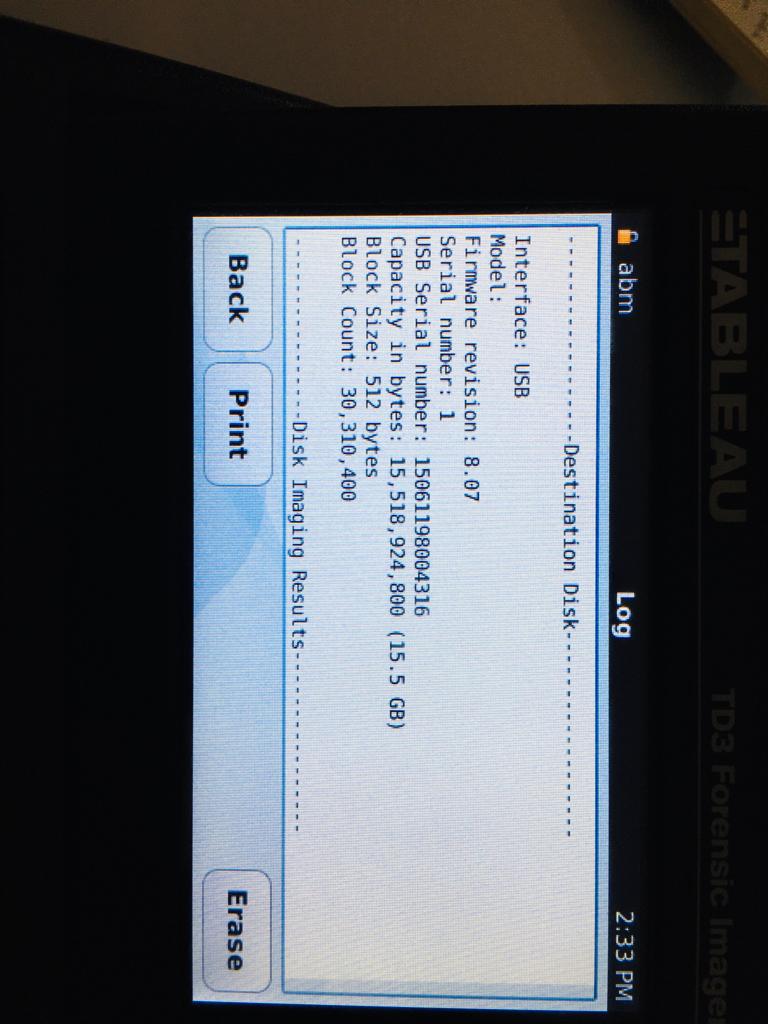
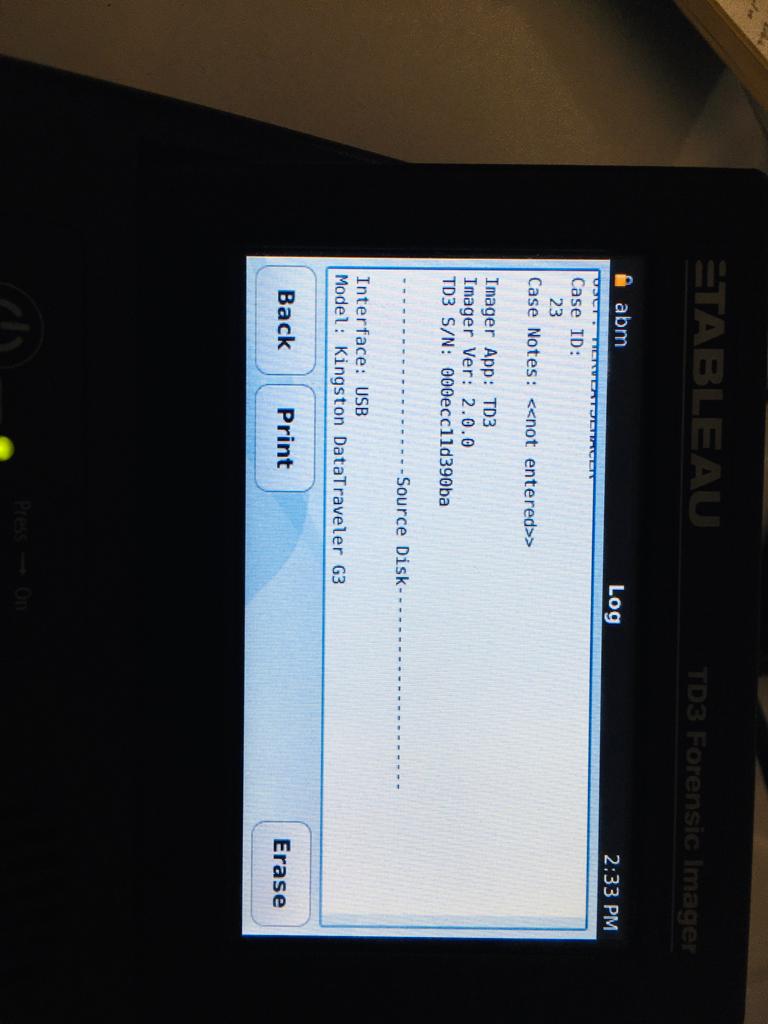
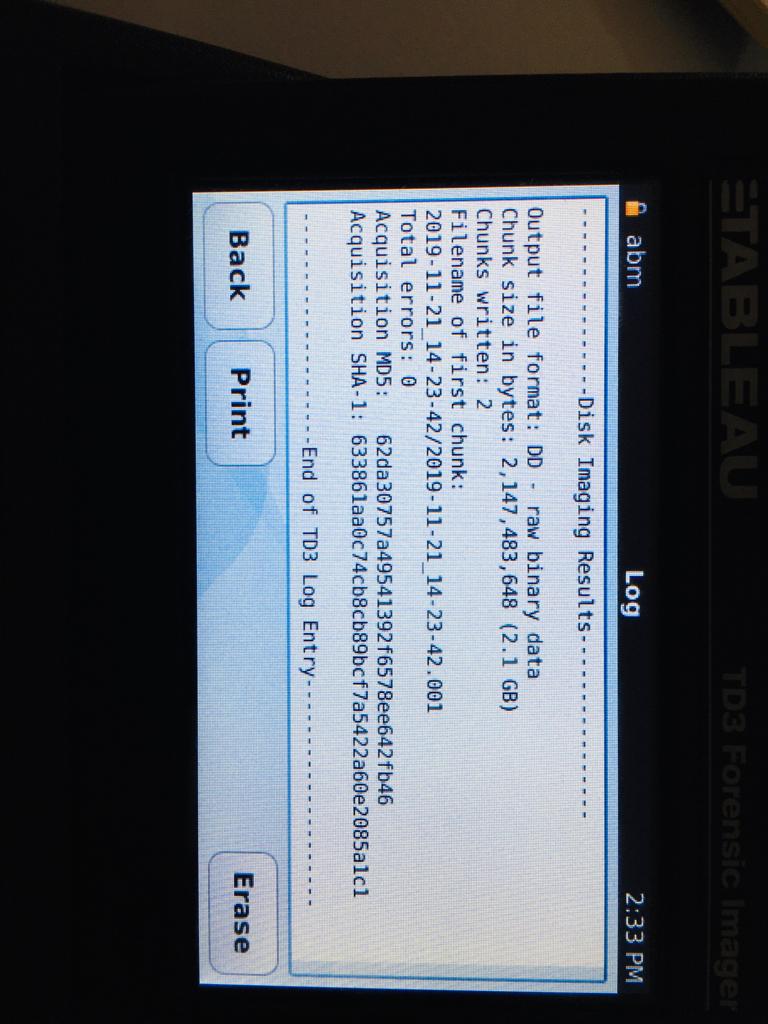
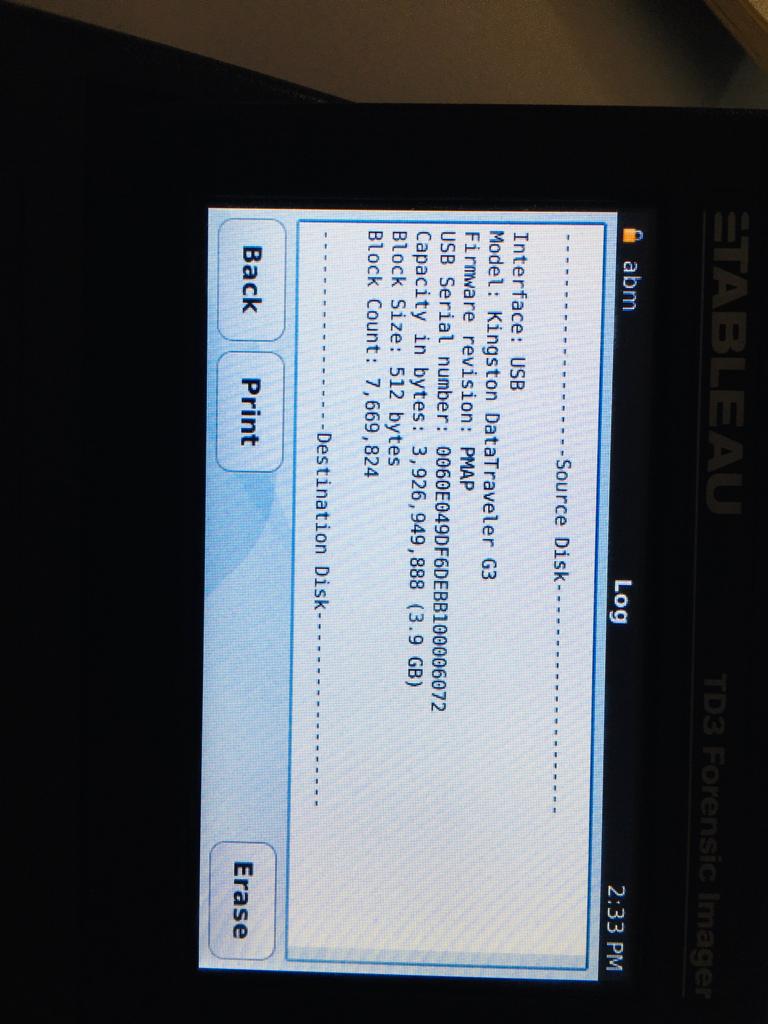
-Hash değeri hesaplanmasından sonra imaj işlemimizi başlattık. İmaj işleminde ilk olarak fiziksel imaj (dd) aldık. Bunun için File Format: dd , Duplication Type: Disk-to-File, Imagine Dir Naming: Date+Time olarak değiştirildi.(Resim 1.5).



**Resim 1.5**

-File Size kısmında ne kadar boyutlu bir dosya ayrılmasının istendiğini soruyor. Bu kısım 2 GB olarak değiştirildi(Resim 1.6)

**Resim 1.6**

-İmaj işlemi tamamlandıktan sonra yine view log yapılarak detaylı bilgilere ulaşıldı(Resim 1.7.1-5).

**Resim 1.7.3**

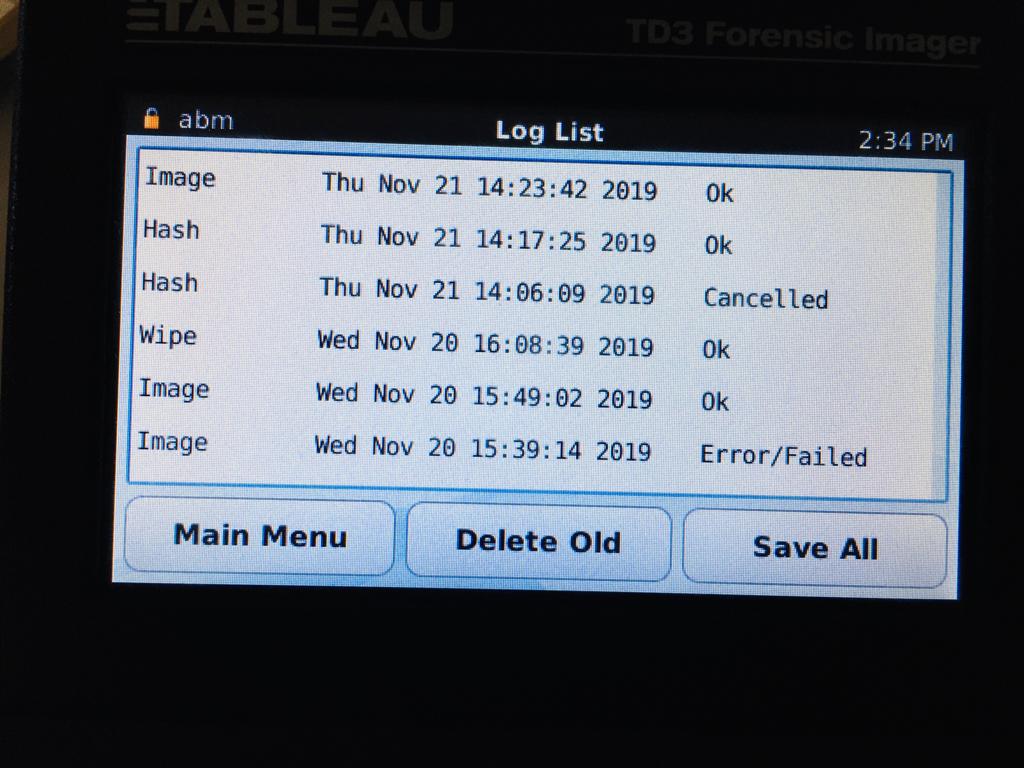
**Resim 1.7.5**

**Resim 1.7.1**

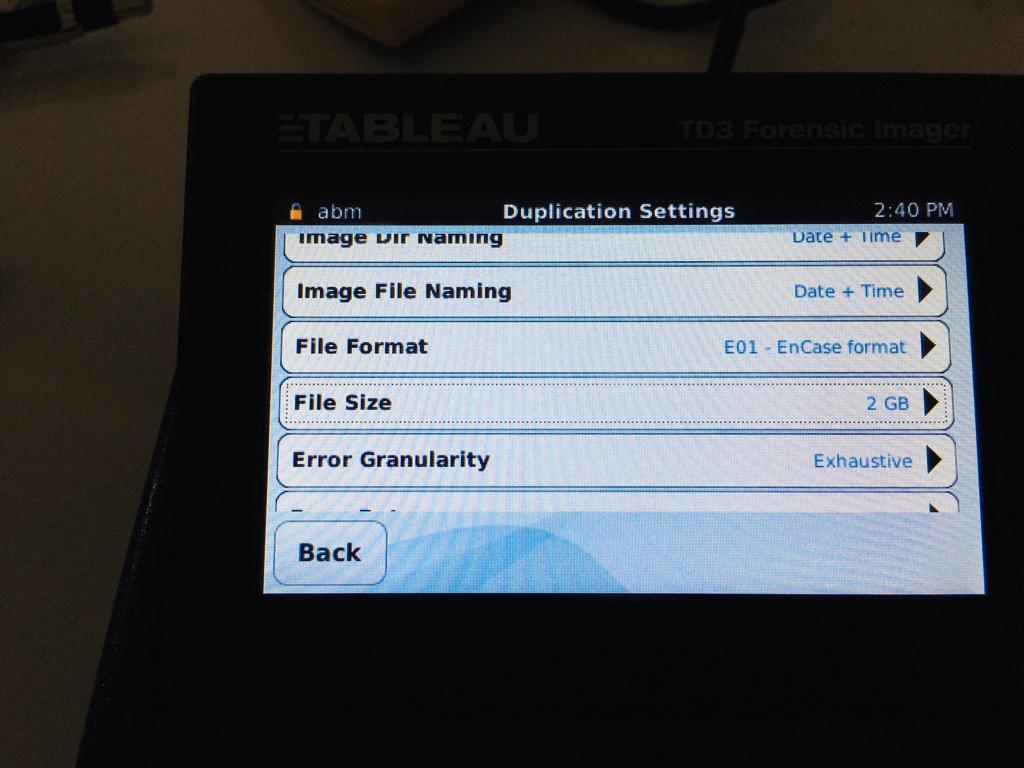
**Resim 1.7.2**

**Resim 1.7.4**

-Ana ekrana gelip logs dediğimizde yaptığımız işlemleri görebiliyoruz(Resim 1.8). İlk 3 satır yaptığımız işlemlerdir.

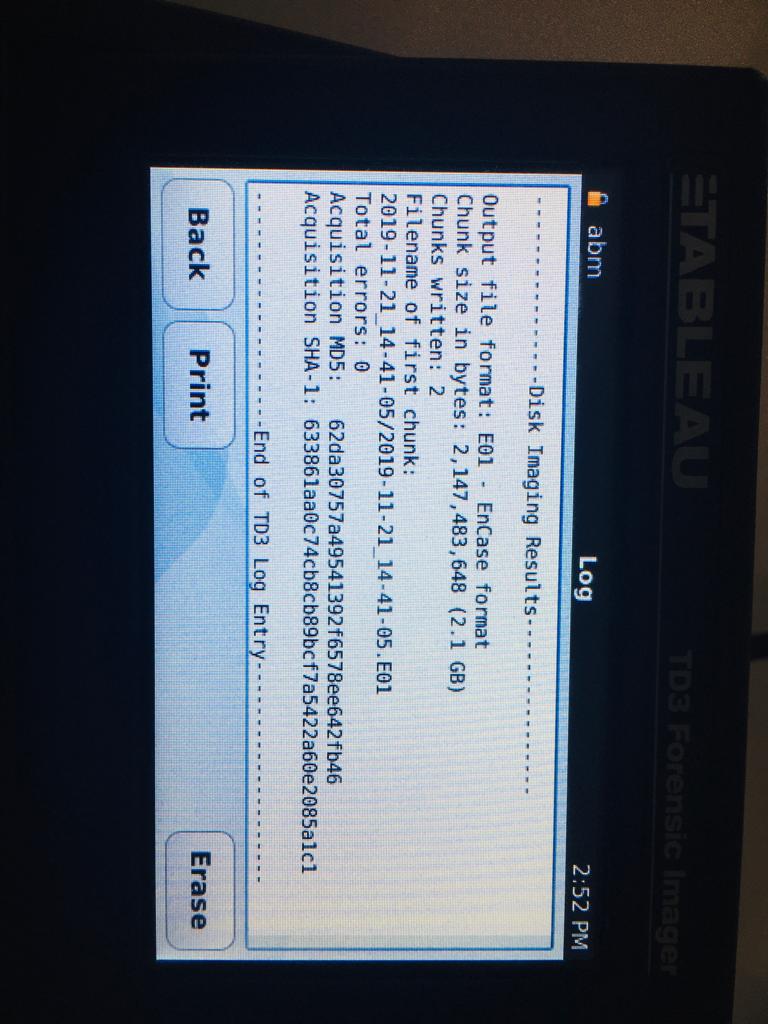
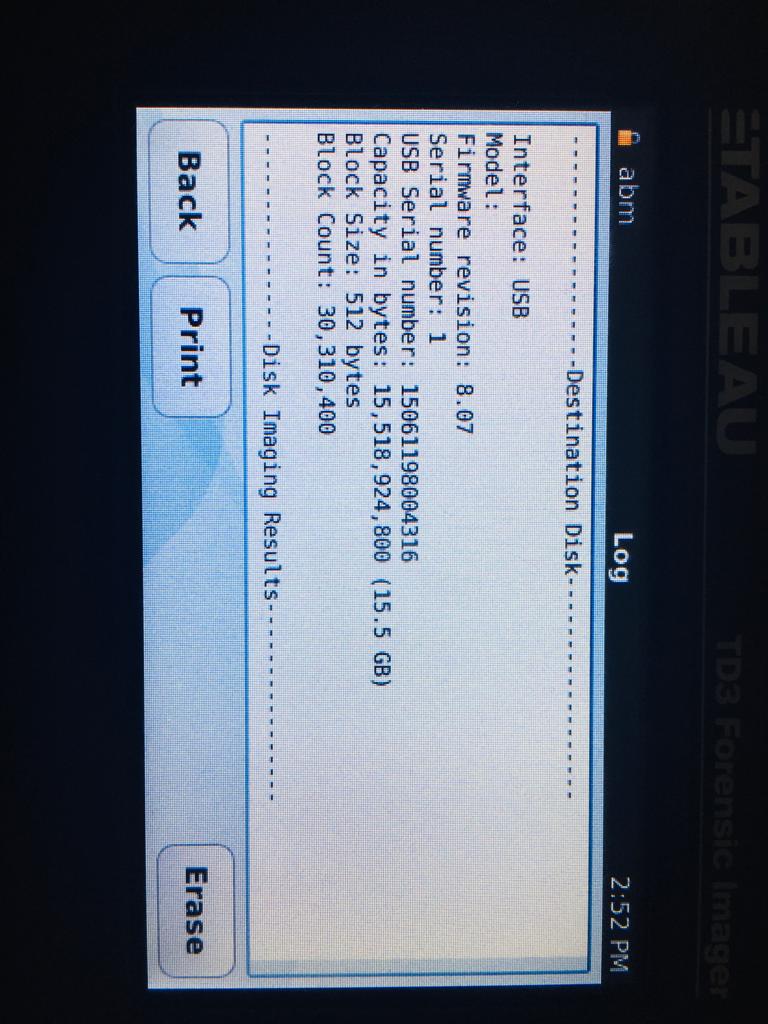
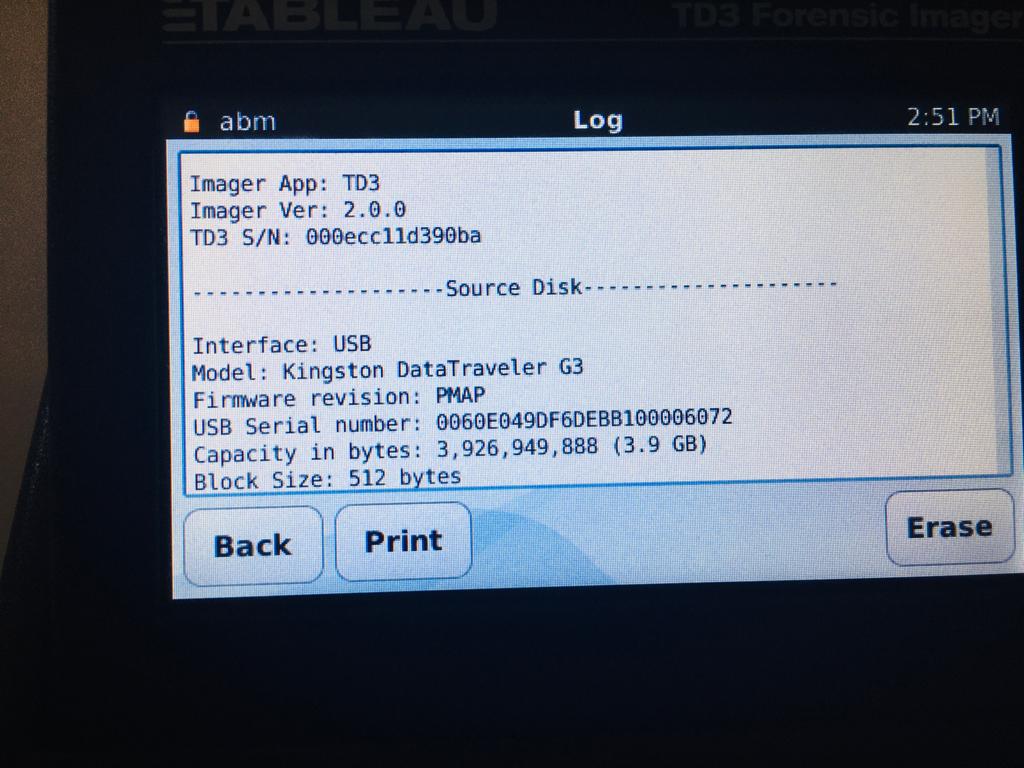


**Resim 1.8**

-İlk imaj işlemi tamamlandı şimdi sırada logical(mantıksal) imaj alma işlemi yapacağız. Fiziksel imajda aldığımız bilgiler aynı kalacak şekilde sadece File Size kısmını mantıksal olacak şekilde E01 Encase format şeklinde yapıldı(Resim 1.9).

**Resim 1.9**

-Gerekli işlemler yapıldıktan sonra logical imaj için imaj alma başlatıldı. İmaj işlemi bittikten sonra view log yaparak ayrıntılı bir şekilde imaj sonucu görüntülendi(Resim 1.10.1-1.10.4)

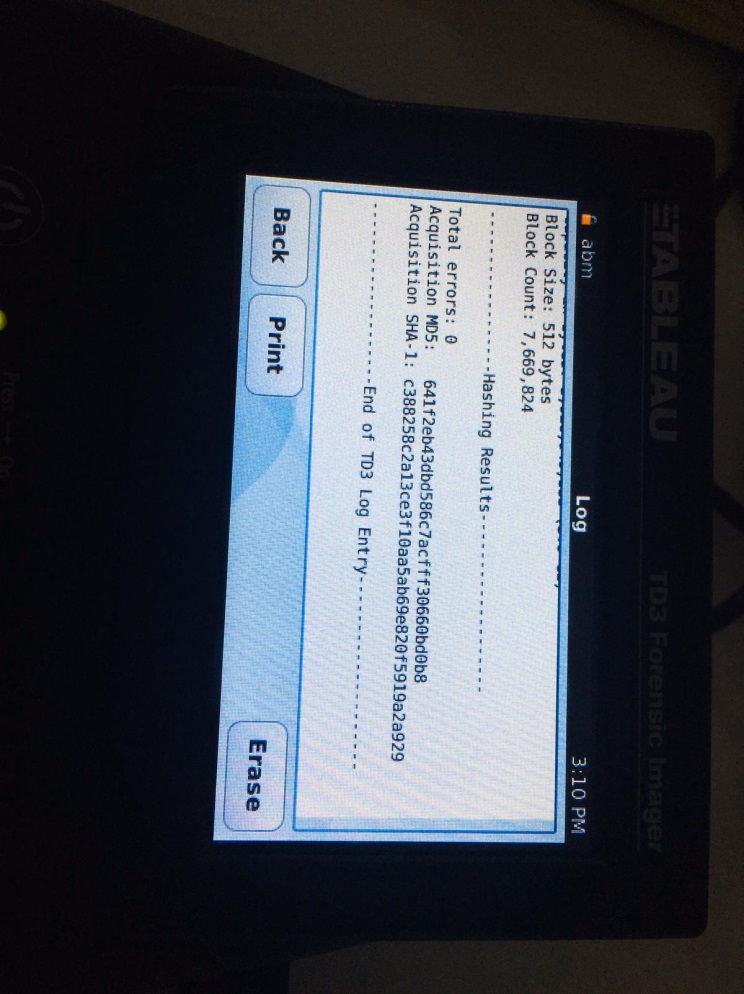


**Resim 1.10.4**

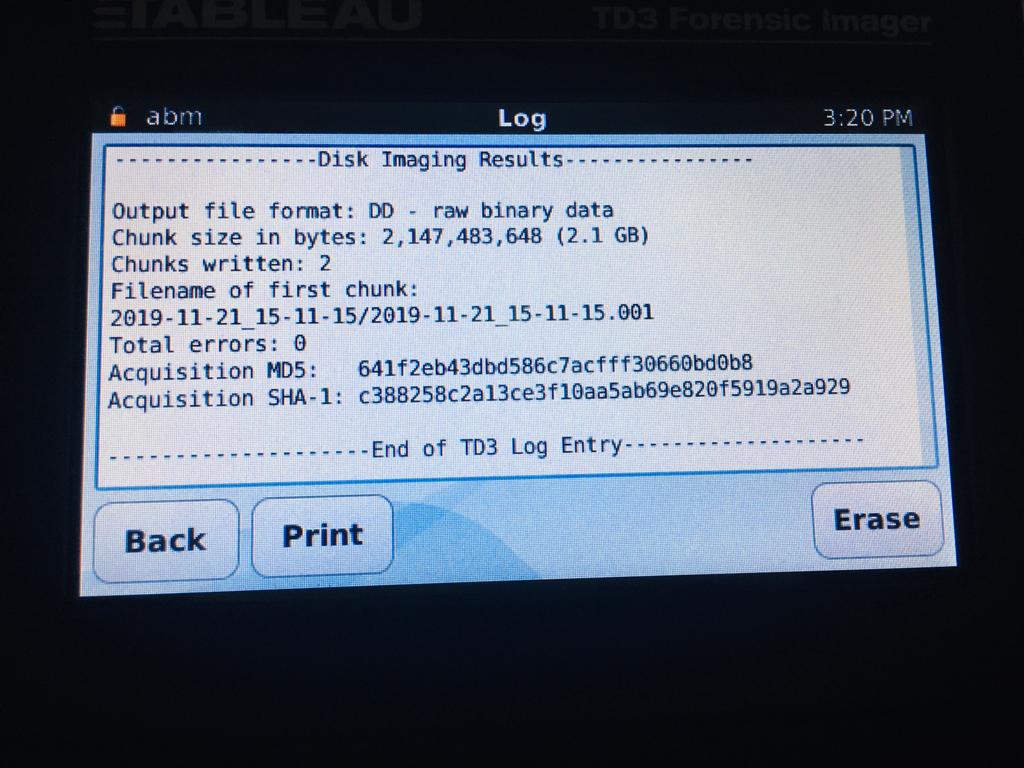
**Resim 1.10.3**

**Resim 1.10.2**

**Resim 1.10.1**

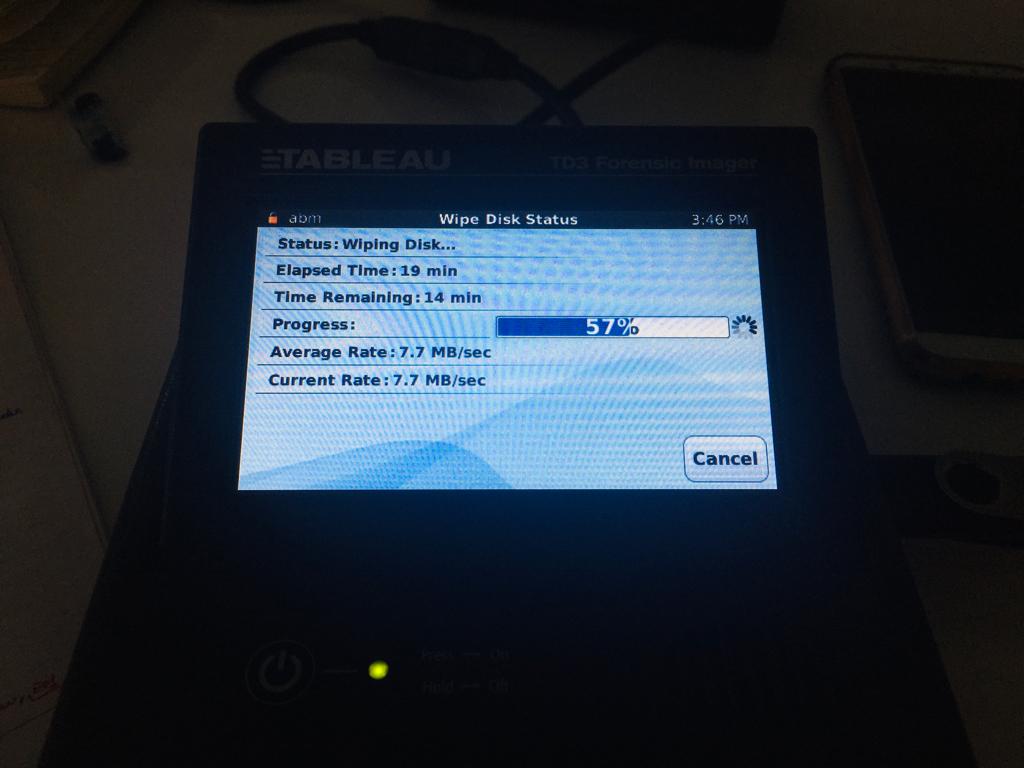
-Fiziksel ve mantıksal imajlar alındıktan sonra içerisinde veri bulunan usb’mizi windows’ta basit bir şekilde silerek tekrar cihazın ilk olarak hash değerini hesaplanıldı(Resim 2.1)

**Resim 2.1**

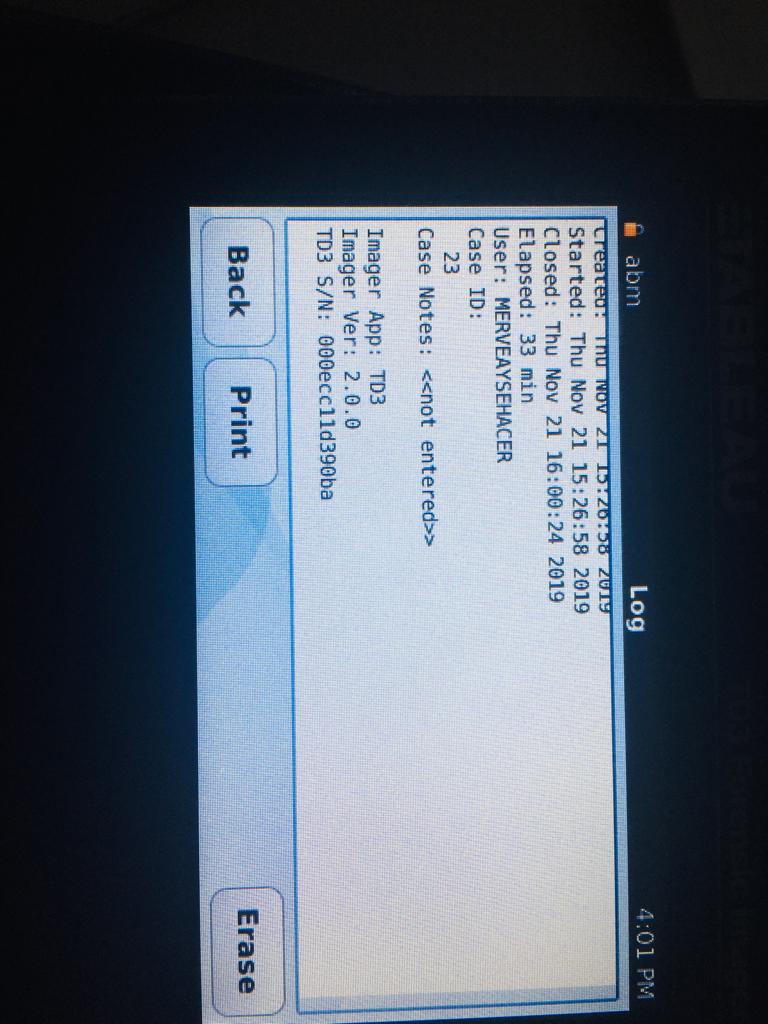
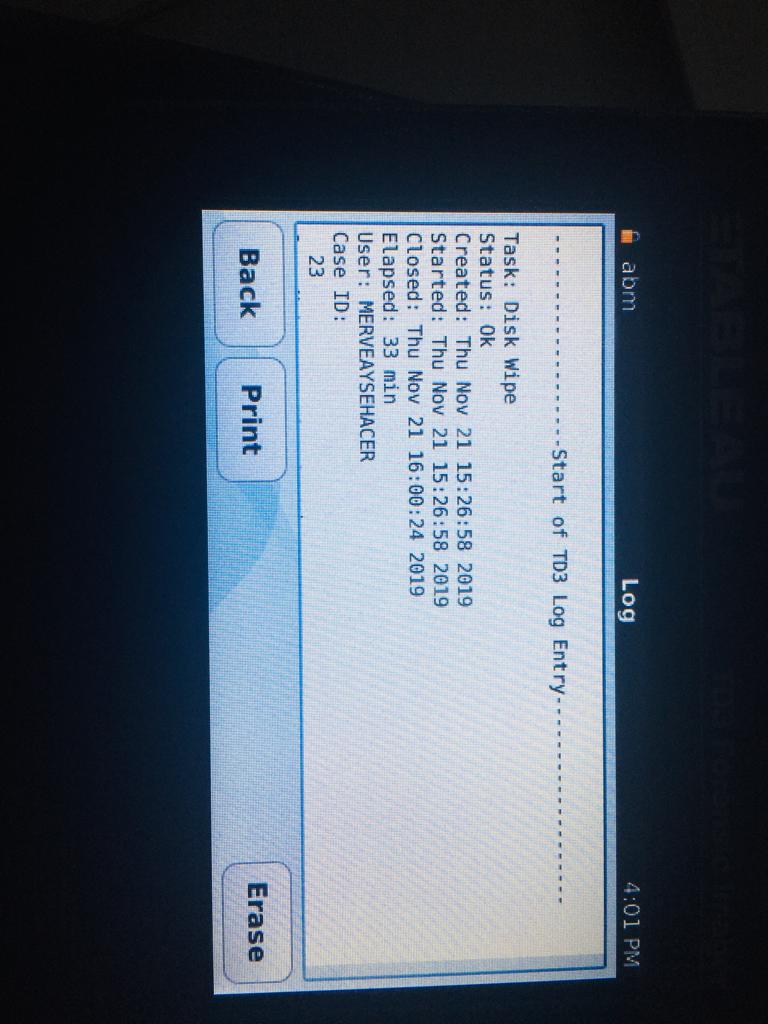
-Ardından imaj alındı. View log’da detaylı bilgiler mevcuttur(Resim 2.2).

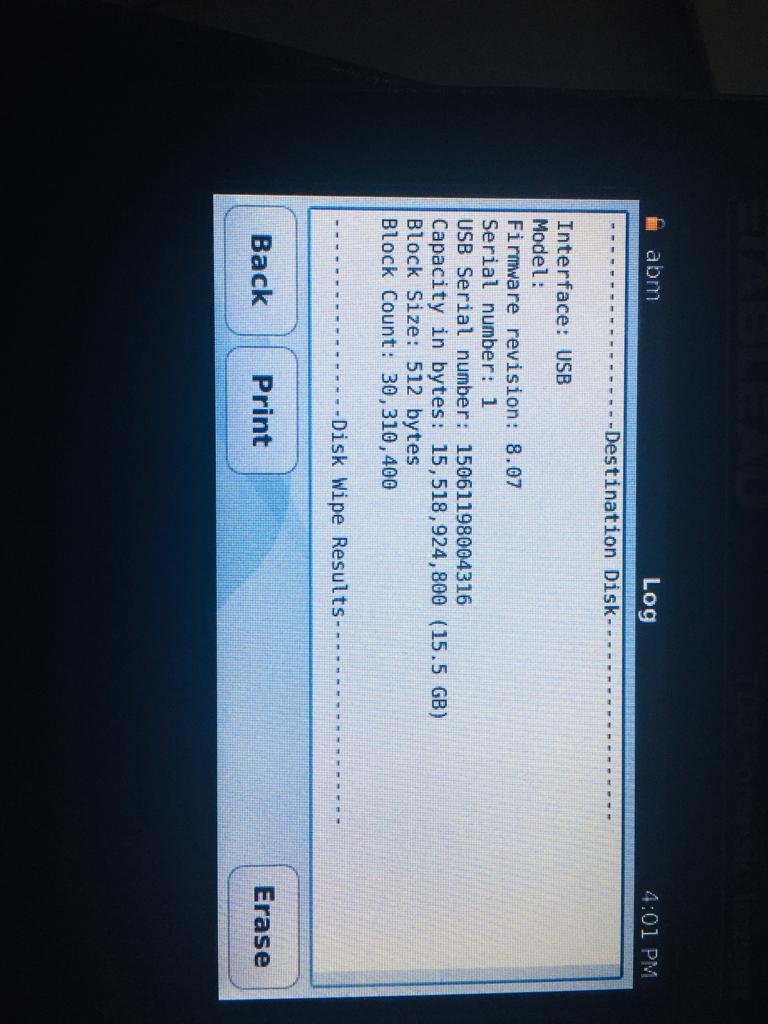
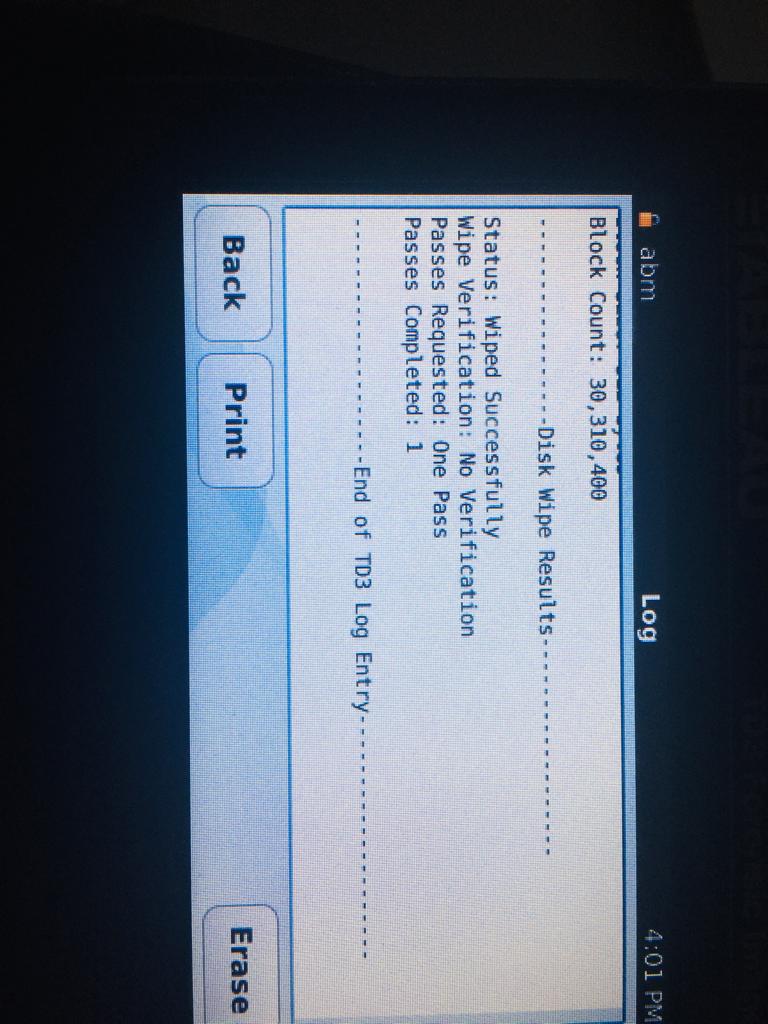
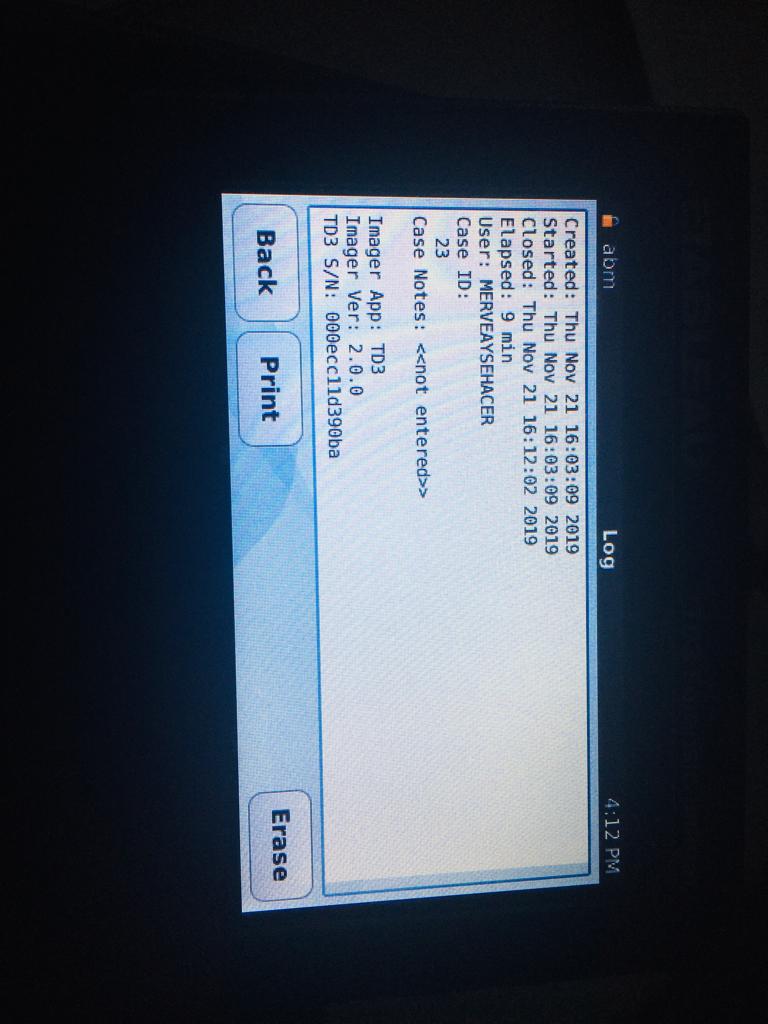
**Resim 2.2**

-Şimdi de basit yöntemle silinen USB belleği wipe ettik(Resim 2.3). Wipe işlemi yaklaşık 33 dakika sürdü.



**Resim 2.3**



-Wipe işlemi sonrasında tekrardan wipe edilen USB bellek üzerinde imaj alındı(Resim 2.4.1-9). View log seçeneğinden detaylı bilgileri görüyoruz.

**Resim 2.4.6**

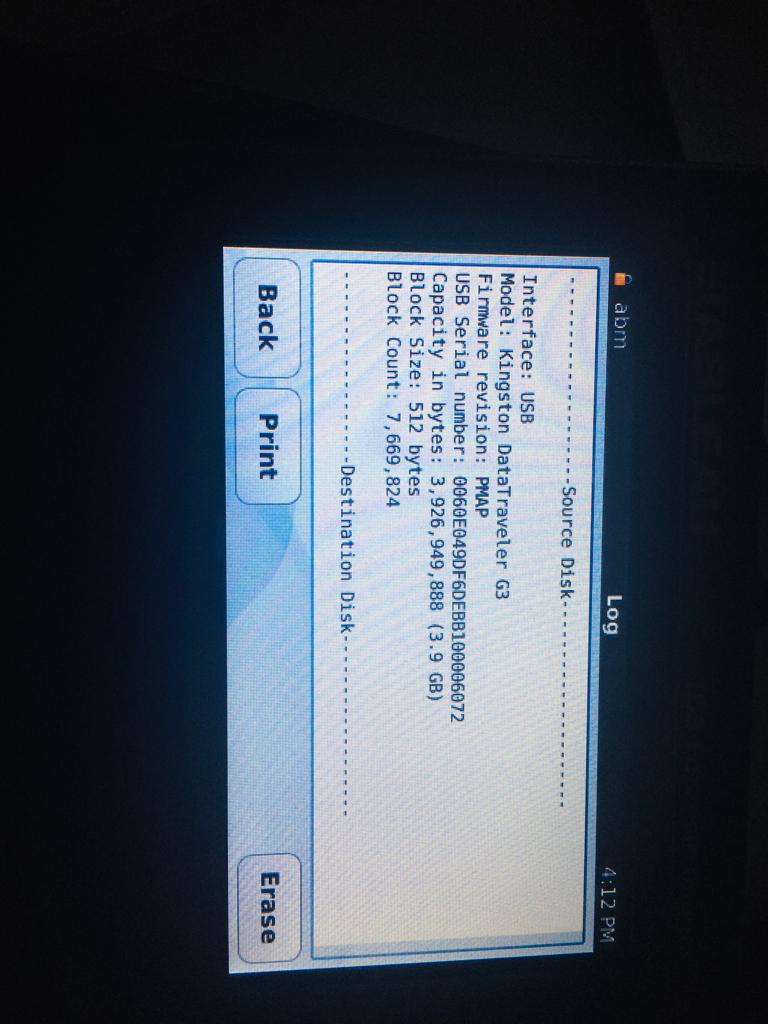
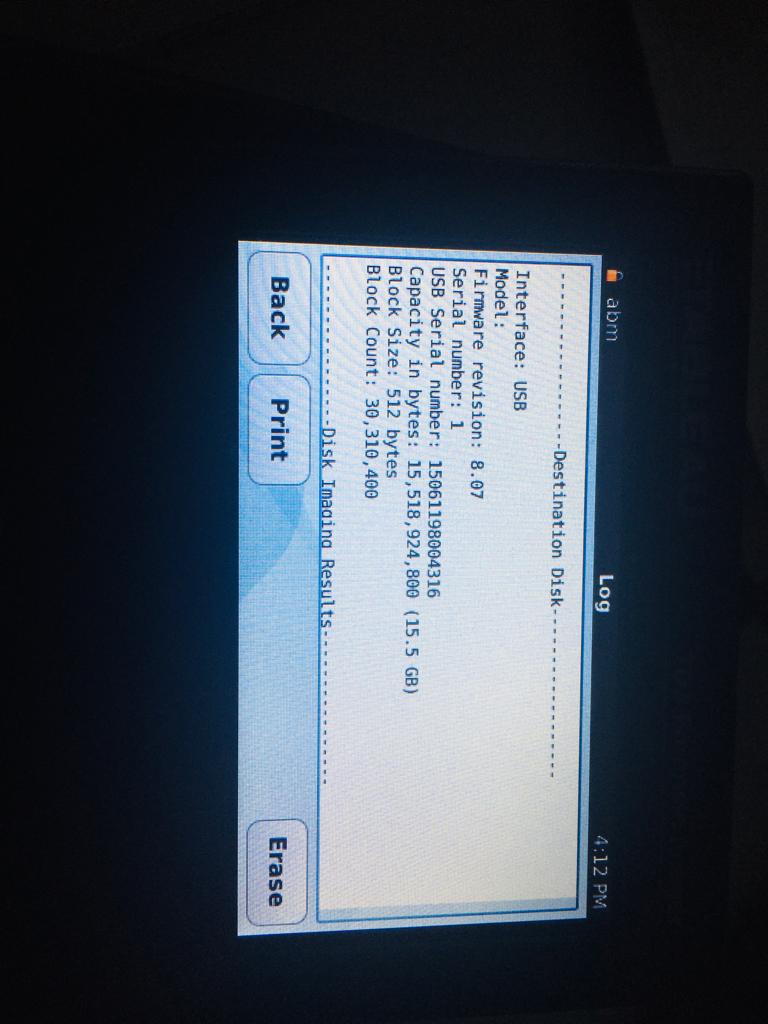
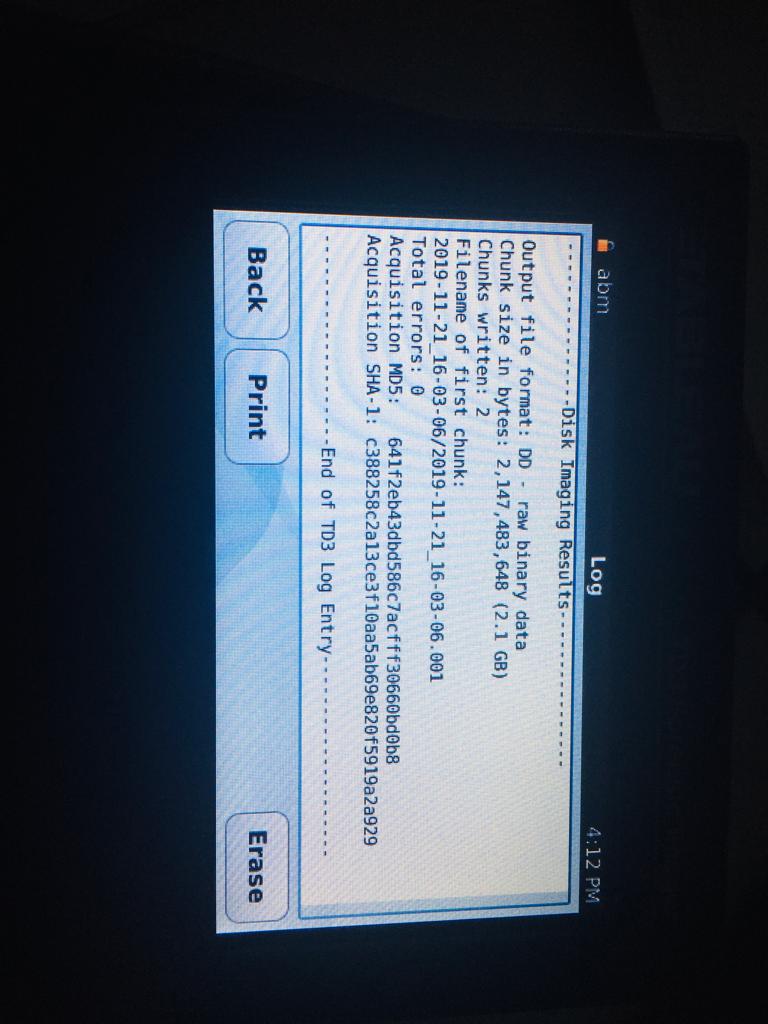
**Resim 2.4.5**

**Resim 2.4.4**

**Resim 2.4.3**

**Resim 2.4.2**

**Resim 2.4.1**



**Resim 2.4.9**

**Resim 2.4.8**

**Resim 2.4.7**

-USB Belleğin wipe edilmesi işleminin tamamlanmasıyla imaj alma işlemlerimiz tamamlanmıştır. Böylelikle elimizde 3 adet imaj dosyası mevcut hale gelmiştir.

**Elde edilen imajlar**

1-İçerisinde veri bulunan diskin imajı

2- İçerisindeki verilerin silindiği diskin imajı

3- Wipe işleminden geçirilen diskin imajı

Yukarıda belirtilen imajlardan 2. ve 3. imaj üzerinde veri kurtarma işlemleri gerçekleştirilmiştir.

(1.imaj dosyası içerisinde zaten veriler mevcuttur silme işlemi yapılmamıştır.)

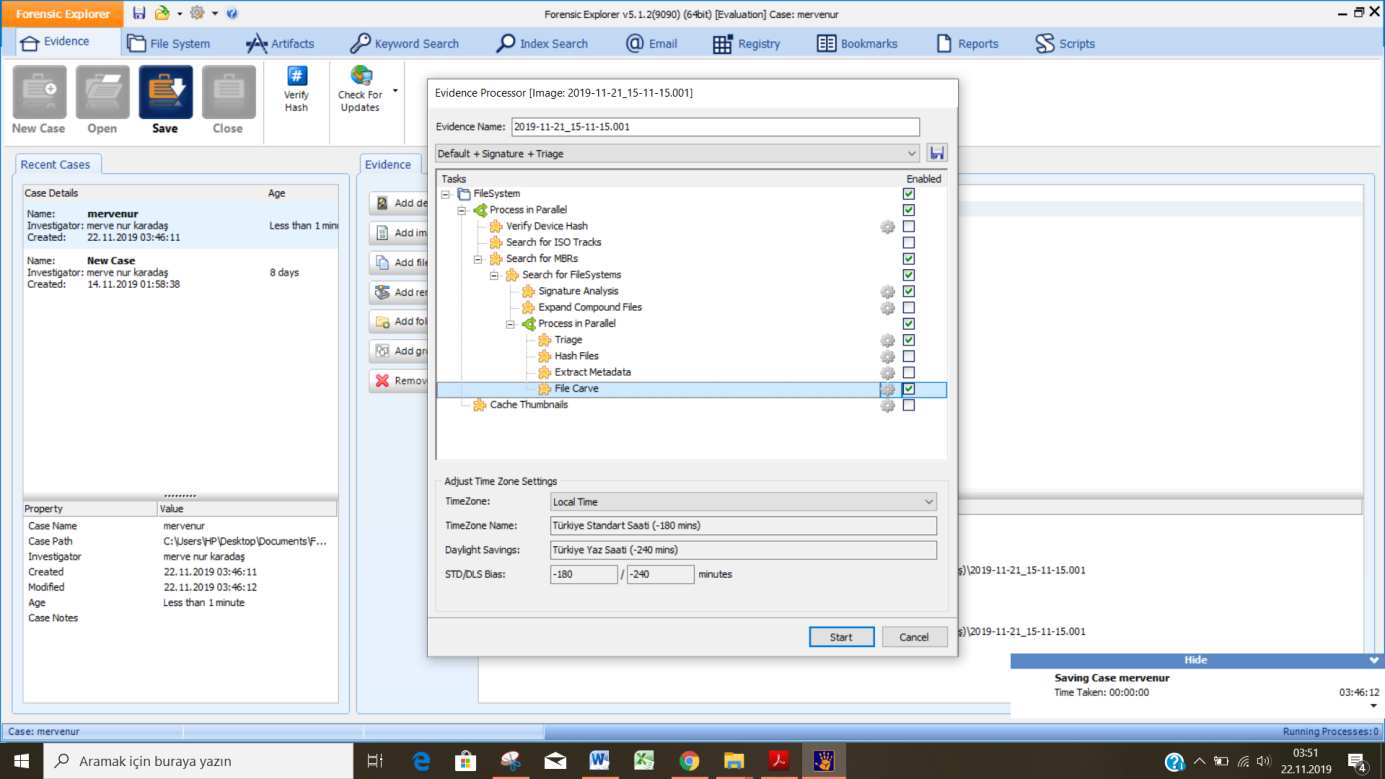
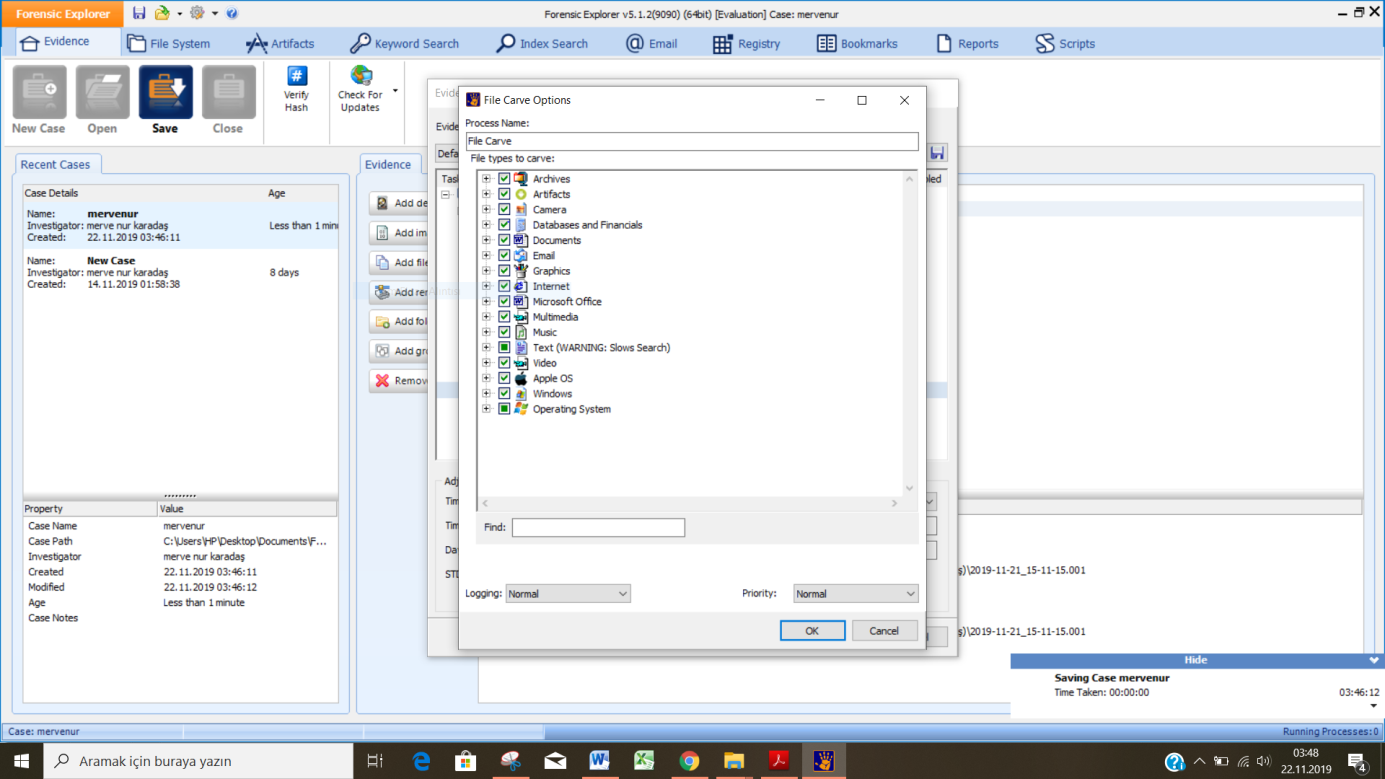
Veri Kurtarma İşlemleri Aşamasında Kullanılan Yazılımlar:

Veri kurtarma aşamasında sadece 1 yazılım kullandım. Forensic explorer, burada File Carve (veri kazıma) yaparak veri kurtarma işlemi yaptım.

Bu aşamada öncelikle FORENSIC EXPLORER Adli imaj alma ve inceleme yazılımı kullanılarak TABLEAU TD3 cihazıyla alınan 2.imaj mount edilmiştir.

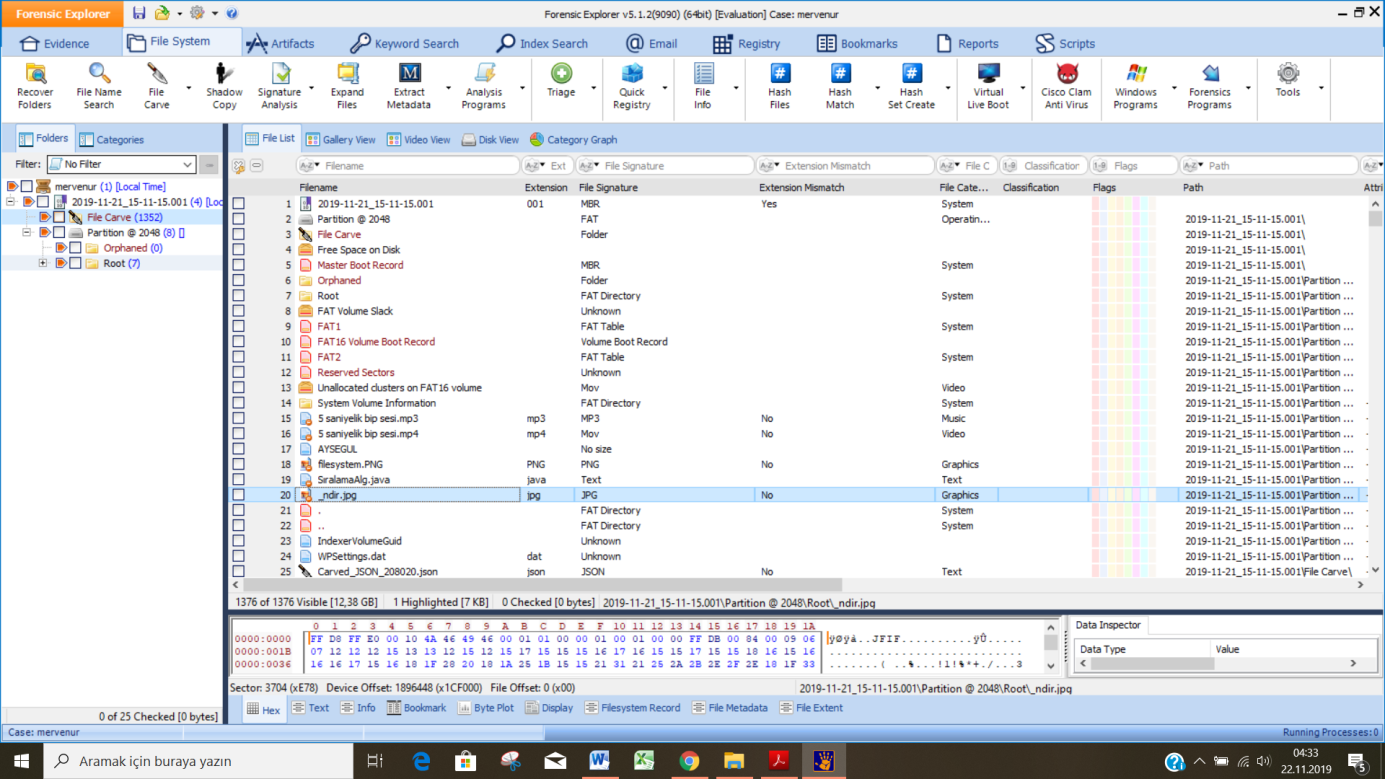
Forensic explorer programını açtığımızda New case ile yeni bir dosya açtım.

Ardından add image diyerek imaj dosyasını açtım. İmaj açıldığından imaj için hangi processeslerin gerçekleştirilmesi gerekiyorsa onu seçtim. Bu seçenekleri File Carve kısmını aktif ederek yaptım(Resim 2.5.1-2).

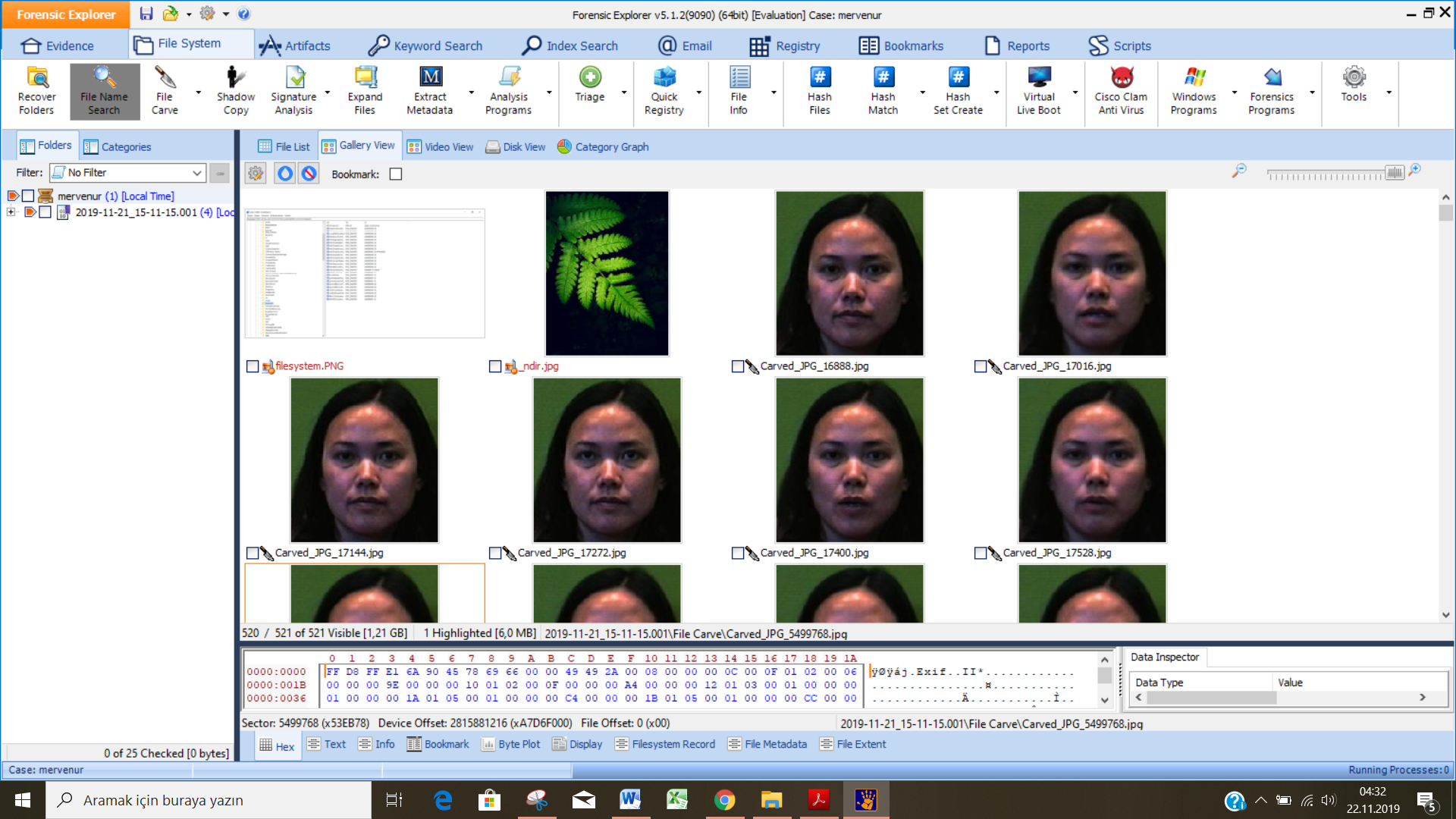


**Resim 2.5.2**

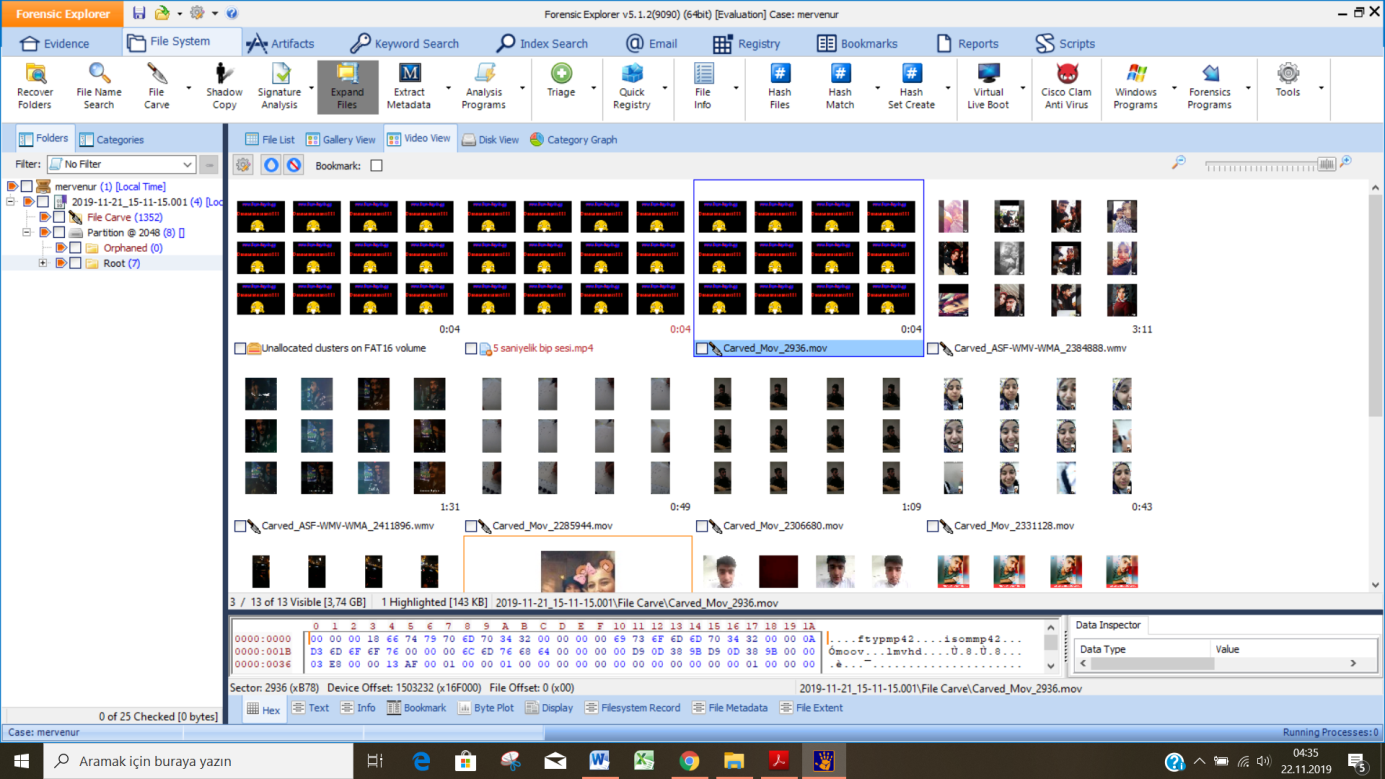
**Resim 2.5.1**

-File Carve işlemi sonrasında aşağıdaki gibi resim, galeri,video gibi dokümanlar geri geldi(Resim 2.6.1-)

**Resim 2.6.1**



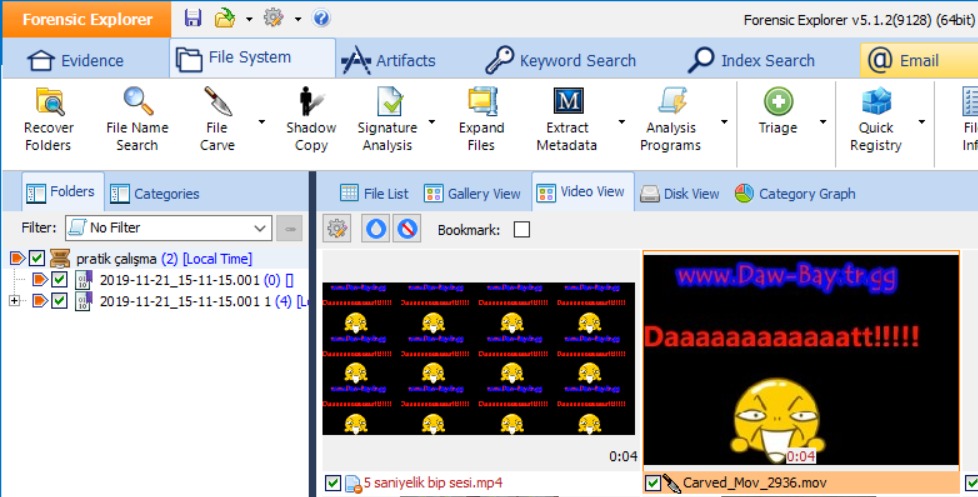
**Resim 2.6.2**



**Resim 2.6.3**

-Windows’ta basit silme işleminden sonra şimdi de wipe işlemi yapılan imaj dosyası üzerinde File Carve yaptım. Prosess seçimini ilk başta yaptığım gibi yaptım. Ardından File Carve işlemini başlattım(Resim 2.7)

- Diski wipe ettikten sonra tekrar file carve işlemini yaptığımda ise tekrar dosyaların geldiğini gözlemledim. Lakin wipe ettikten sonra gelen verilerle, ilk kurtarma işlemi arasında ufak bir fark olduğunu gözlemledim. Wipe ettikten sonra da veriler gelmiştir. Lakin ilk kurtarmada kurtarmada gelen verilerin hepsi gelmemiştir ufak bir kısmı gelmiştir(Resim 2.7)



**Resim 2.7**

-Bu işlemlerden sonra tekrardan secure modda wipe işlemi yaptığımda hiçbir verinin geri gelmediğini gördüm.

SONUÇ

* Aldığım fiziksel, mantıksal, silinmiş ve wipe edilmiş imajlar başarıyla alınmıştır. Hepsinin hash değerleri hesaplatılmıştır.
* Silinmiş flash bellekten aldığımız imaj dosyası üzerinden veri kurtarma işlemimizi başarıyla sonuçlandırdım. Veriler hasarsız bir şekilde kurtarılmıştır.
* İçindeki verileri silmiş olduğum imaj dosyasını wipe ettiğimde verilerin yine bir kısmını geri getirdim. Ama tekrar secure modda wipe ettiğimde ise verilerin geri dönüşümsüz olarak silindiğini ve geri getirilemeyeceğini fark ettim.
* Wipe edilen bir sürücüden herhangi bir veriyi burada geri getiremedik.
* İçerisindeki verilerinin silindiği bir usb flash bellekten veri kurtarma işlemini başarıyla tamamlarken wipe edilen bir diskten veri kurtarmayı başaramadık