****

**T.C**

**FIRAT ÜNİVERSİTESİ**

**TEKNOLOJİ FAKÜLTESİ**

**ADLİ BİLİŞİM MÜHENDİSLİĞİ BÖLÜMÜ**

**TABLEAU TD3 ve DİTTO**

**İNCELEME ÇALIŞMASI**

**DANIŞMAN HAZIRAYAN**

Dr. Öğr. Üyesi Mustafa KAYA Mazlum BAYDAR-16525006

**ELAZIĞ-2019**

Bu rapor Tableau TD 3 ve Ditto Adli imaj ve kopya alma cihazlarını kullanılarak aşağıdaki adımların sırasıyla gerçekleştirilmesi neticesinde oluşturulmuştur.

Çalışma esnasında gerçekleştirilen adımlar:

1. Farklı bir veri depolama cihazına fiziksel ve lojik imajlar alma.
2. İlk depolama cihazındaki klasör Normal silme işlemi ile silindikten sonra, dublicator ile tekrar kopyalanacak ve klasör kurtarılmaya çalışılacaktır.
3. Aynı depolama cihazı son olarak secure erase veya wipe işlemi yapıldıktan sonra, dublicator ile yine kopyalanarak kurtarılmaya çalışılacaktır.

Çalışma da kullanılan bahsi geçen TABLEAU TD3 ve DİTTO Adli imaj alma ve kopyalama cihazının görüntüsü:





1.Tableau TD3 2.Ditto DX

**1.TABLEAU TD3**

TABLEAU TD3 cihazı ile farklı durumlarda imaj alıp bu imajlar üzerinden veri kurtarma ve inceleme işlemlerini yapmak üzerek tableau cihazımız kullanıma hazır hale getirildi.Kullanım kolaylığı olması için Ethernet kablosu ise bilgisayarımızın Ethernet girişine tableau cihazı bağlandım.

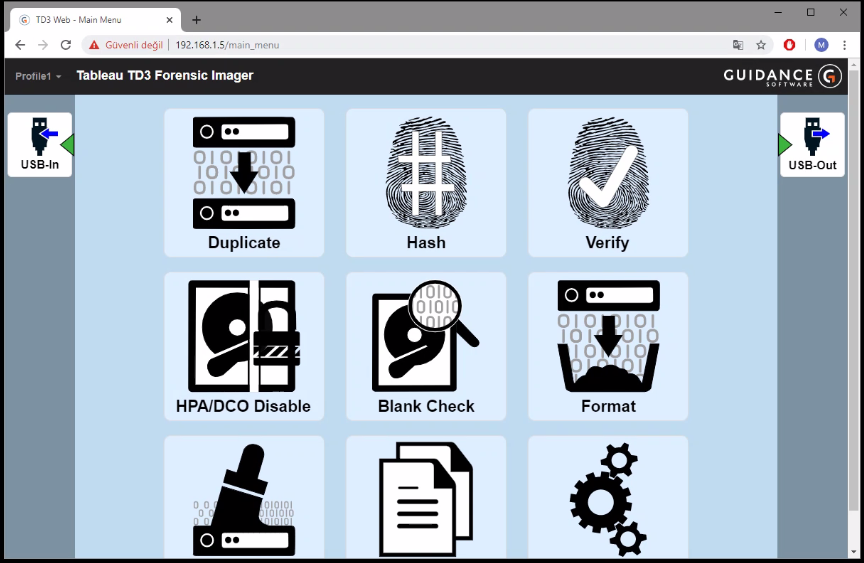
Asıl işlemlere başlamadan önce cihaz ayarları menüsüne giriş yaparak web arayüzüne bilgisayara üzerinden bağlanabilmemiz gerekli olan IP yapılanladırma ayarları yapıldı.

Tableau cihazının Ethernet portuna statik olarak bir IP adresi (kimliği) belirledikten sonra aynı IP adresi kullanılarak cihazı bağladığımız bilgisayarın Ağ ayarlarından statik olarak gerekli ayarlamalar yapıldı.

Herhangi bir tarayıcı kullanılarak (Projede İnternet Explorer kullanıldı) statik olarak belirlenen IP arama çubuğuna yazılarak Tableau cihazının web arayüzüne giriş yapıldı.

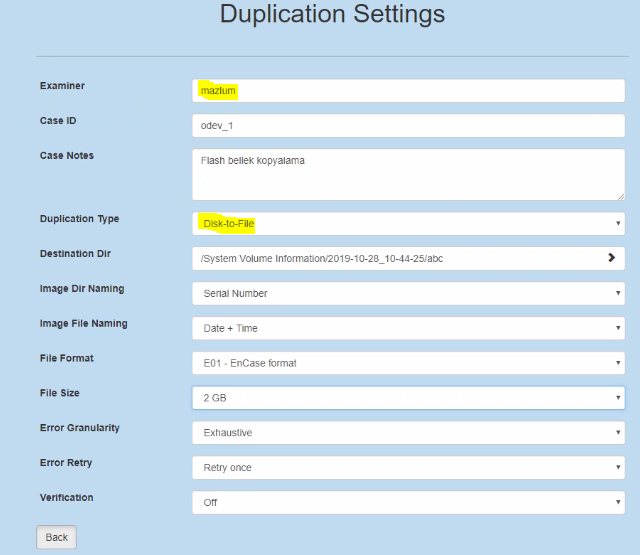
Tableau TD3 cihazının dokunmatik ekranı kullanılarak kendi arayüzünden ayarlar menüsünden seçilen profil bilgileri (kullanıcı adı ve parola bilgisi) web arayüzünde gerekli alanlara girilerek Tableau TD3 cihazının web arayüzüne giriş yaptıktan sonra işlemlere başlamış oldum.

**1.FİZİKSEL VE MANTIKSAL İMAJ ALMA İŞLEMİ**



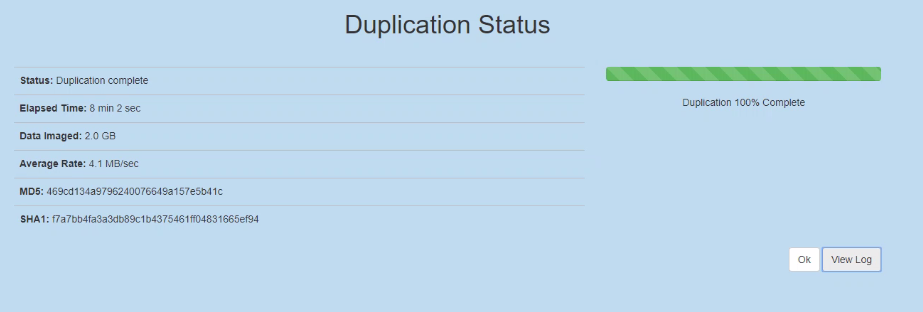
3.Tableau TD3 Web Arayüzü

Daha önceden hazırlamış olduğum USB Belleğe resim,müzik,video,doküman atıp işlemlere hazır hale getirdim.



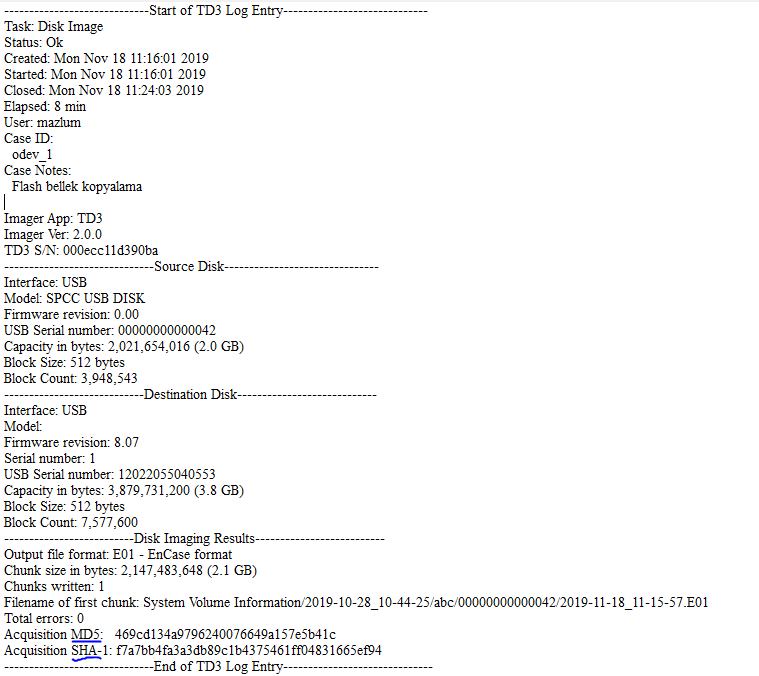
4. Duplicaton Ayarları

Lojik imaj alabilmek için öncellikle Duplicator ayarlarına girip incelemeyi yapacak kişinin ismini ve duplication tipini disk-to-file yani mantıksal imaj olarak ayarlıyıp kayıt ediyoruz.



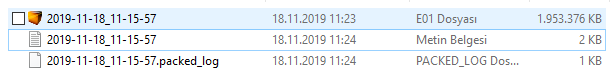
5.Duplication Lojik İmaj

Lojik(mantıksal) imajımız başarılı bir şekilde alınmıştır.Log kayıtlarını inceleyecek olursak yapılan işlem ile ilgili detaylı bilgilere erişebiliriz.



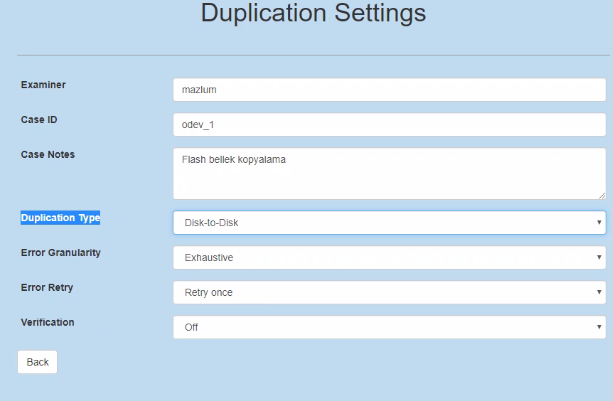
6.Lojik İmaj Log Bilgisi

Log Bilgisini incelediğimiz vakit disklerimiz ile ilgili bilgileri ,zaman,hash değerlerini bize vermektedir.



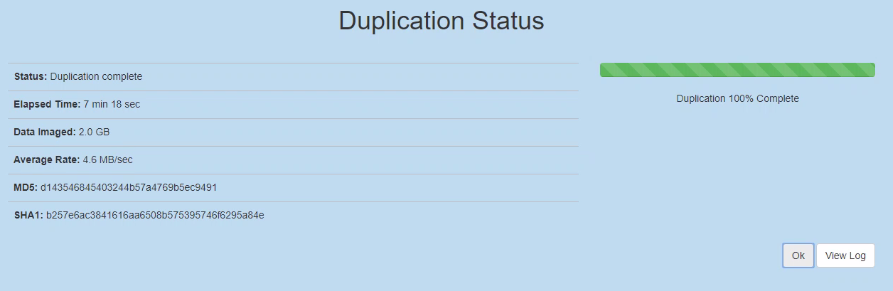
7.Alınan lojik imaj

Diskimizde alınan lojik imajı görüntüleyebiliriz.



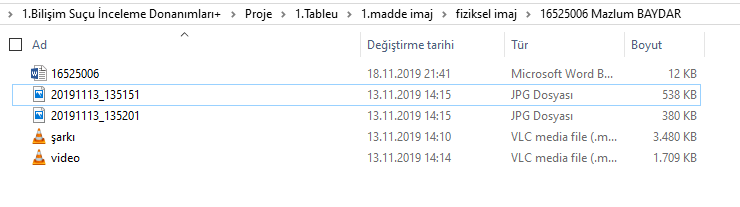
8.Dublication Fiziksel İmaj Ayarları

Bir sonraki işlemimiz ise diskimizin fiziksel imajı almak olacaktır. Bunun için dublication settings kısmından dublication type disk-to-disk yani fiziksel imaj olarak seçmek olacaktır.



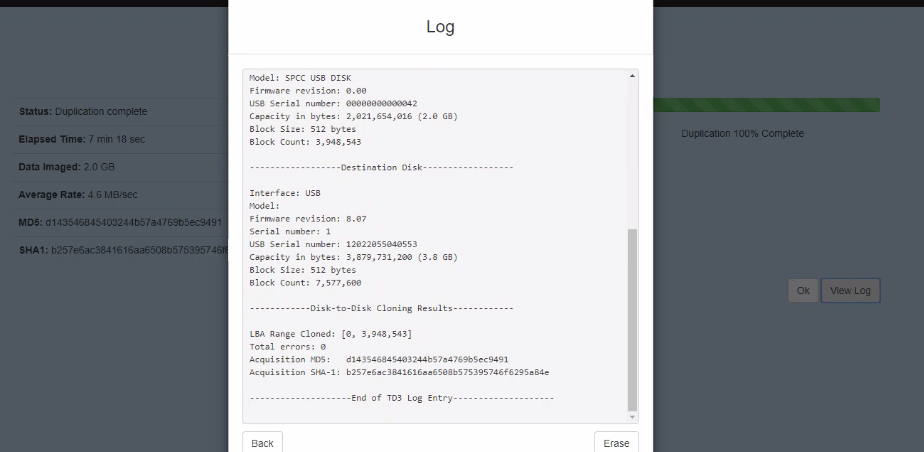
9.Fiziksel imaj alma

Gerekli ayarları yaptıktan sonra fiziksel imajımızı başlattık ve 7 dakika bekledikten sonra işlemimiz başarılı bir şekilde sonlandı.



10.Disk

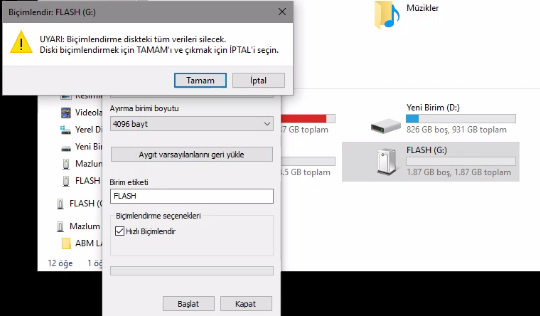
Fiziksel imajdan sonra diskimize baktığımız zaman başarılı bir şekilde alındını gözlemleyebiliyoruz.



11.Fiziksel İmajın Logu

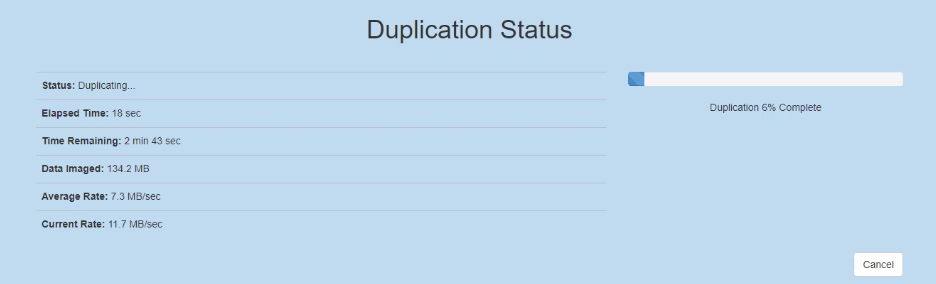
**2.NORMAL SİLME İŞLEMİ YAPILMIŞ DİSKTEN DOSYA KURTARMA İŞLEMİ**

2.İşlemimiz ,diskimizdeki dosyaları silip tekrar dublicator ile verileri kurtarmaya çalışacağız.



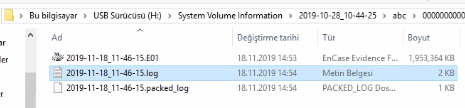
12.Diski temizleme

Diskimi boşaltıyoruz.



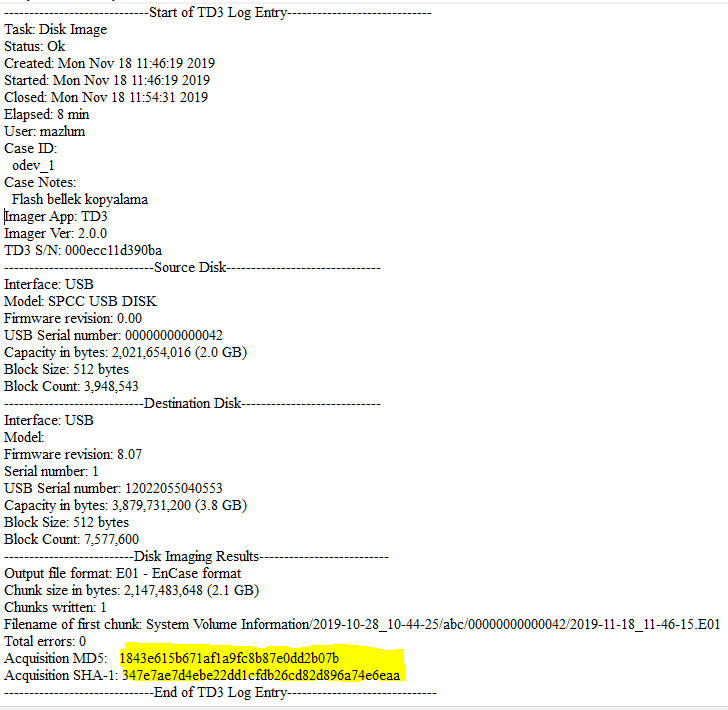
13.Tekrar Duplication Uygulama

Verileri silinen diskimizdeki verileri kurtarmak için tekrardan dublication uygulamasını yapıyoruz.



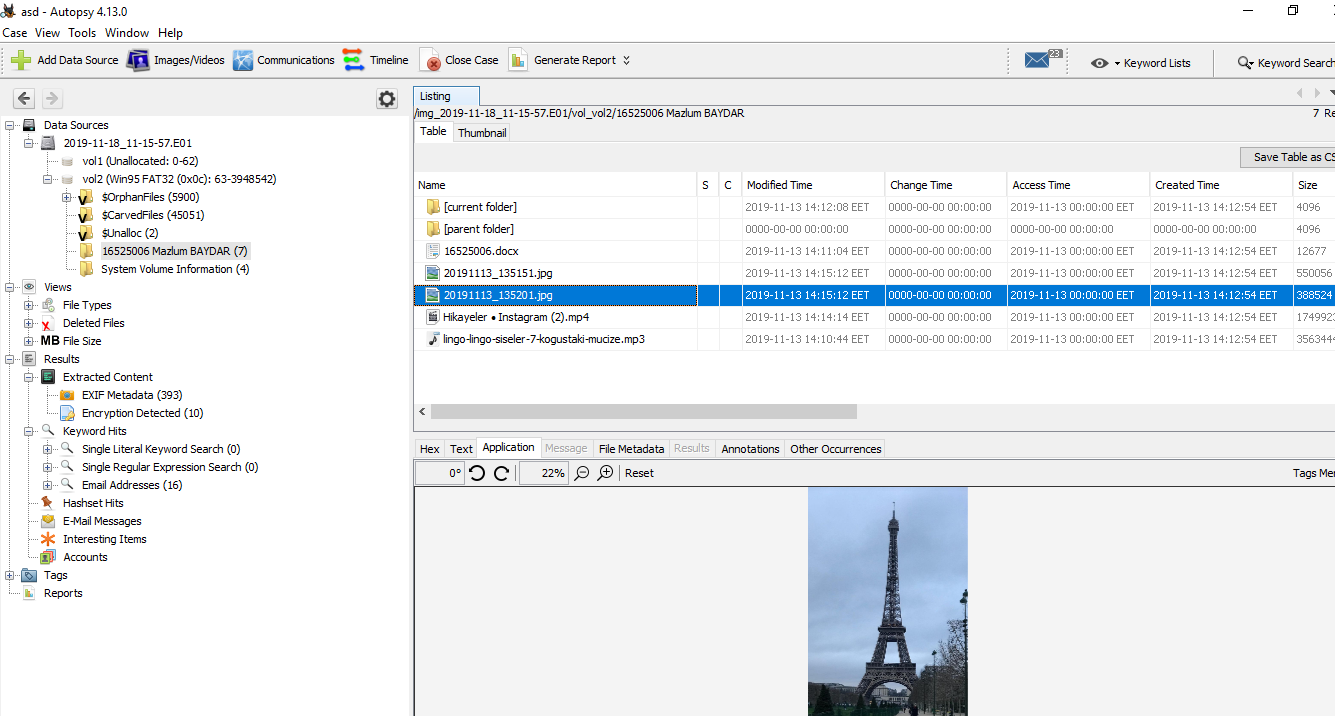
14.Diski görüntüleme

İşlem bittikten sonra diskimizi gözlemlediğimiz vakit başarılı bir şekilde imajımız alınmış bunu çeşitli imaj inceleyen yazılımlar yardımıyla açıp içeresindeki verilerimizi kurtarabiliriz.



15. Silinen Verileri Kurtarma İşlemindeki Log Kayıtları

Kurtarma işlemi yaptığımız vakit oluşan log kayıtlarını incelediğimiz zaman hash değerlerindeki değişimi gözlemleyebiliyoruz.

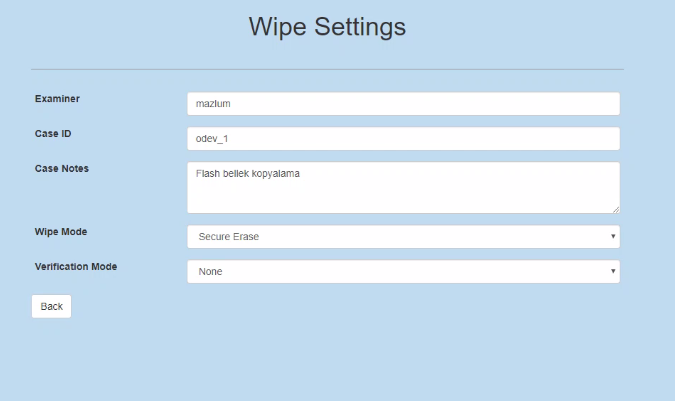


16.Autopsy inceleme

Ücretsiz yazılım olan Autopsy kullanılarak imajımızı inceleyebiliriz. Görüldüğü üzere verilerimiz başarılı bir şekilde kurtarılmış oldu.

**3.WİPE İŞLEMİ YAPILMIŞ DİSKTEN VERİLERİ KURTARMA İŞLEMİ**

3.işlemimiz ise diskimizi wipe ile sildikten sonra tekrar dublicator işlemi gerçekleştirerek verilerimizi kurtarmaya çalışacağız.

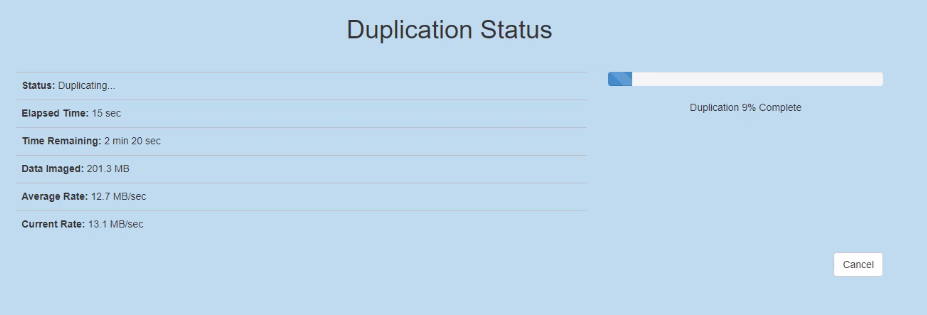


17.Wipe Setting

Tableau web arayüzünden wipe ayarları kısmından gerekli ayarlamalarımızı yapıp kayıt ediyoruz.



18.Wipe İşlemi



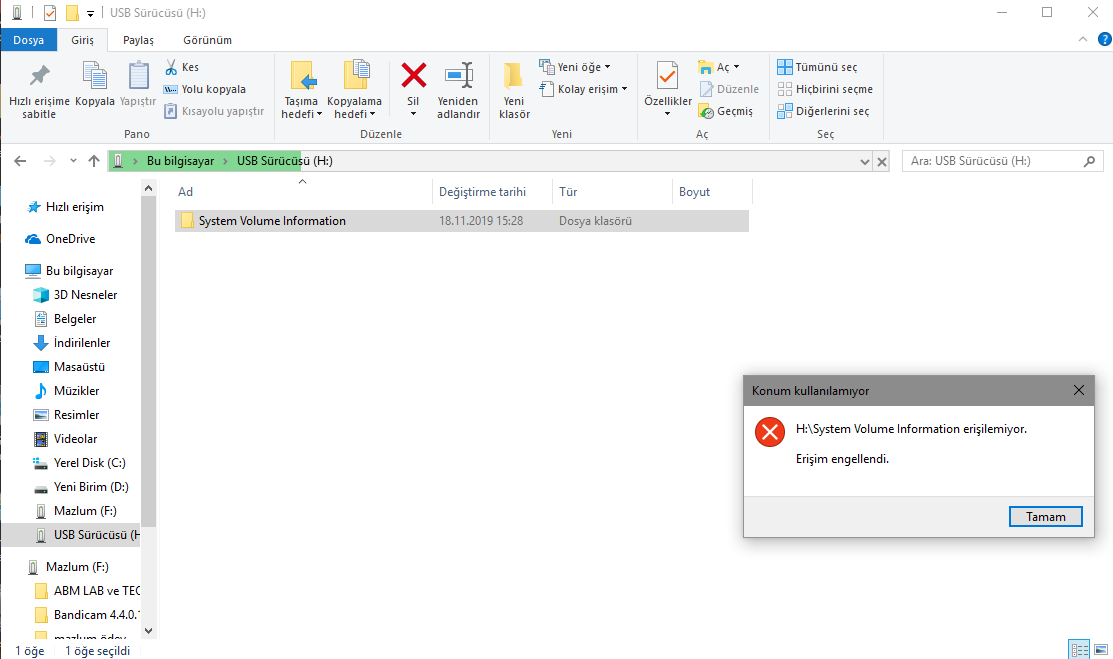
19.Duplication Status

Wipe ettiğimizi diski tekrar duplicator işlemi uygulayıp verilerimizi kurtarabilecek miyiz ona bakalım.



20. Duplicator Log

Wipe işlemi için yaptığımız duplicator işleminin log kayıtları.



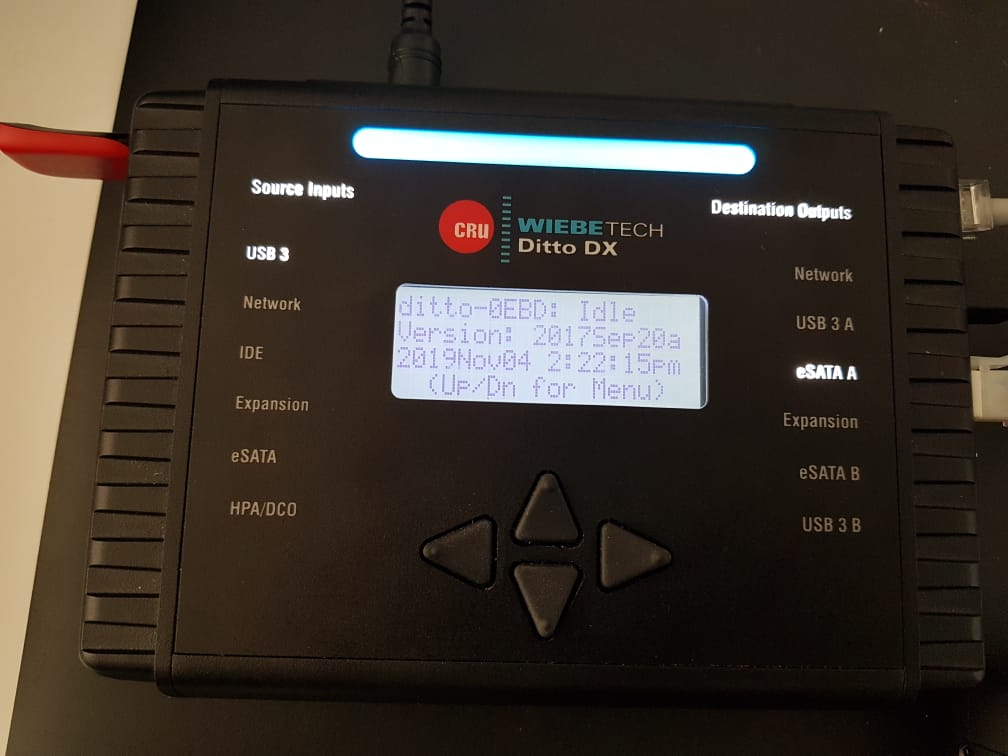
21. Wipe Edilmiş Diskten Veri Kurtarma

Wipe edilen diskimize duplicator uyguladık ve işlem bittikten sonra diskimizi bilgisayar bağladık.Görüldüğü gibi disk içerisindeki verilere hiçbir şekilde erişilememektedir.

**2.DİTTO DX**

Tableau yapılan işlemlerin aynısını ditto dx cihazından da yapalım.

**1.FİZİKSEL VE MANTIKSAL İMAJ ALMA İŞLEMİ**

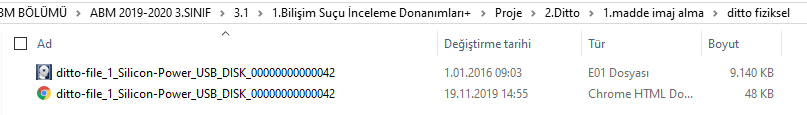
****

22.Ditto DX

Cihazımızdaki gerekli bağlantıları yaptıktan sonra fiziksel imaj alma işlemine başlıyabiliriz.

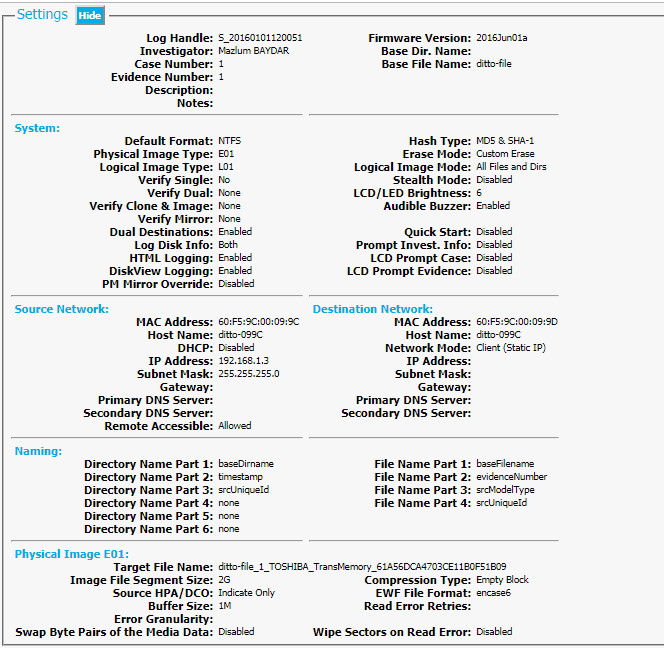


23. Diski bağlama

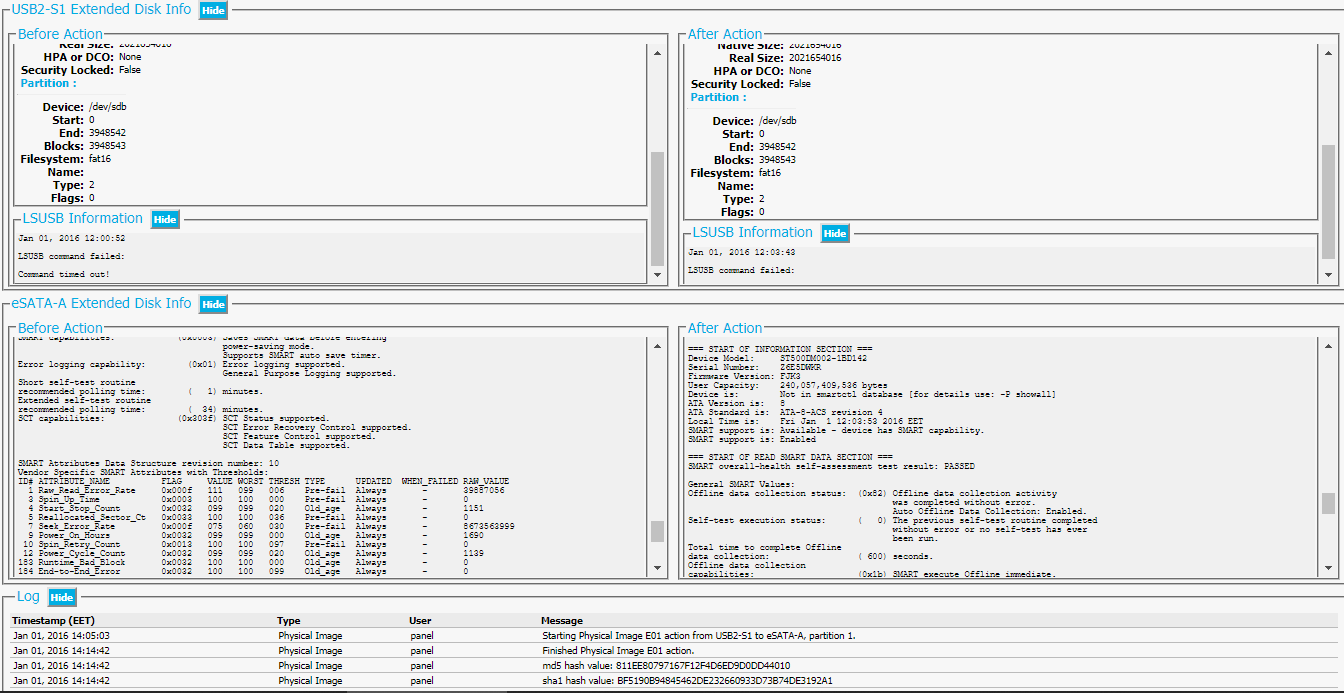


24.Fiziksel imaj alınmış hali

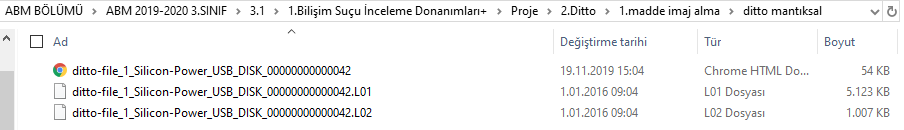
Fiziksel imaj alma işlemi başarılı bir şekilde gerçekleşti.Ekranda E01 formatında alınan fiziksel imajımız gözükmektedir.



25. Fiziksel imaj Log Kayıt-1

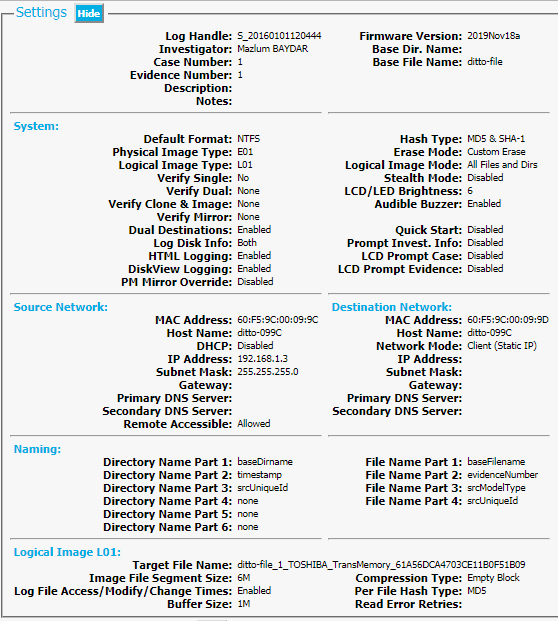
26. Fiziksel imaj Log Kayıt-2

Bir diğer işlem olan Lojik imajı yani mantıksal imajı alalım.

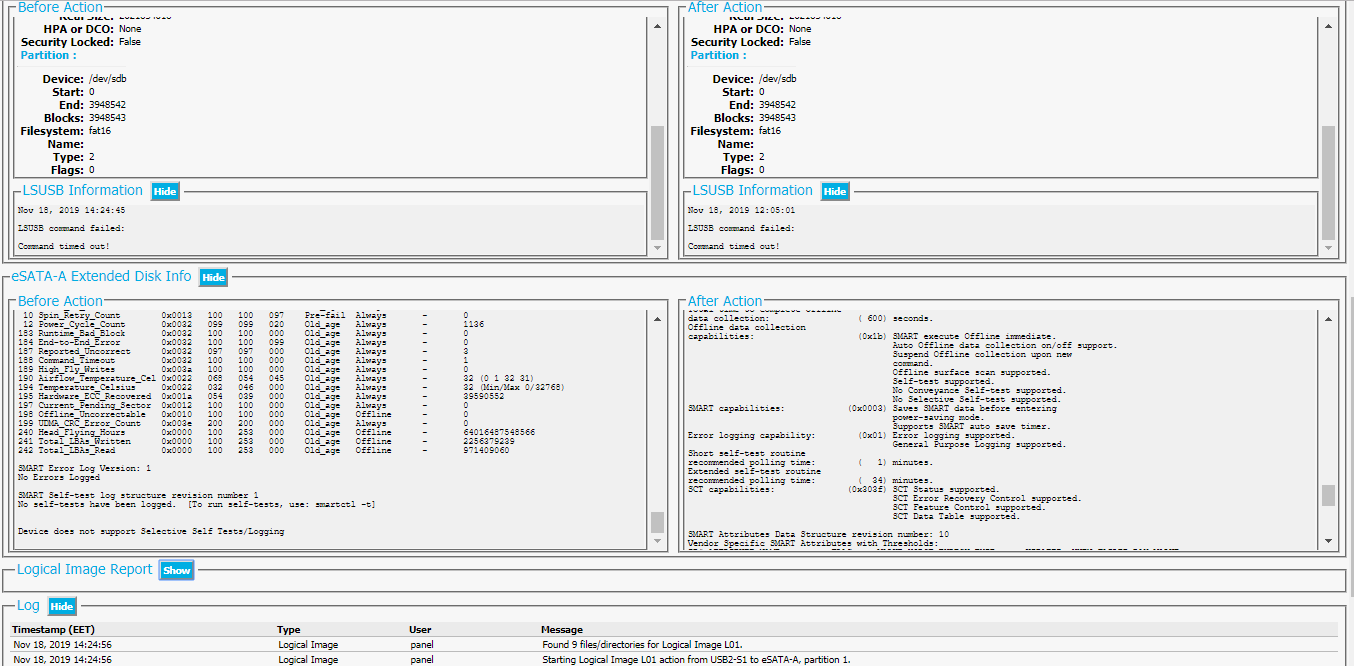


27.Lojik İmaj

Aldığım lojik fiziksel imajı gözükmektedir.



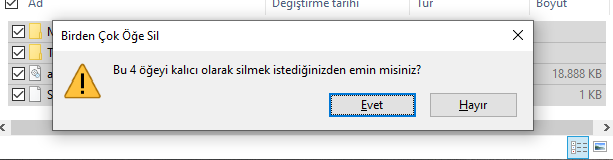
28.Lojik İmaj Log Kayıtları-1



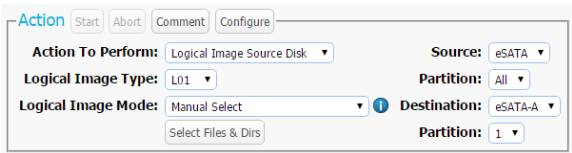
29.Lojik İmaj Log Kayıtları-2

**2.NORMAL SİLME İŞLEMİ YAPILMIŞ DİSKTEN DOSYA KURTARMA İŞLEMİ**

İkinci aşamada ise diskimizden verileri normal olarak silip tekrardan imaj alıp bu imajdan verileri kurtarmaya çalışacağız.

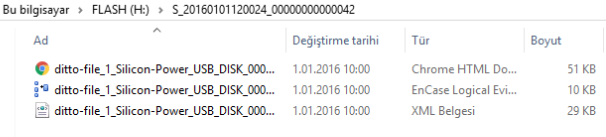


30.Normal Silme.



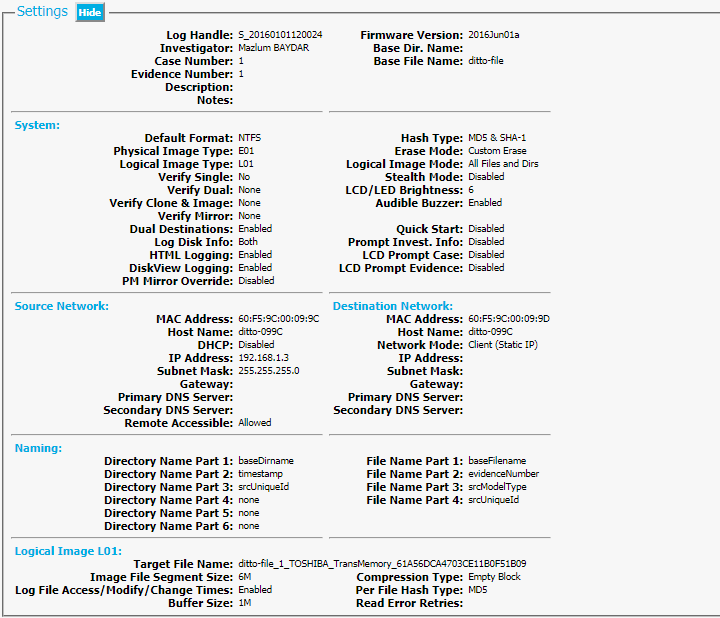
31.İmaj Alma

Tekrar silinen diske imaj alma işlemini gerçekleştiriyoruz.

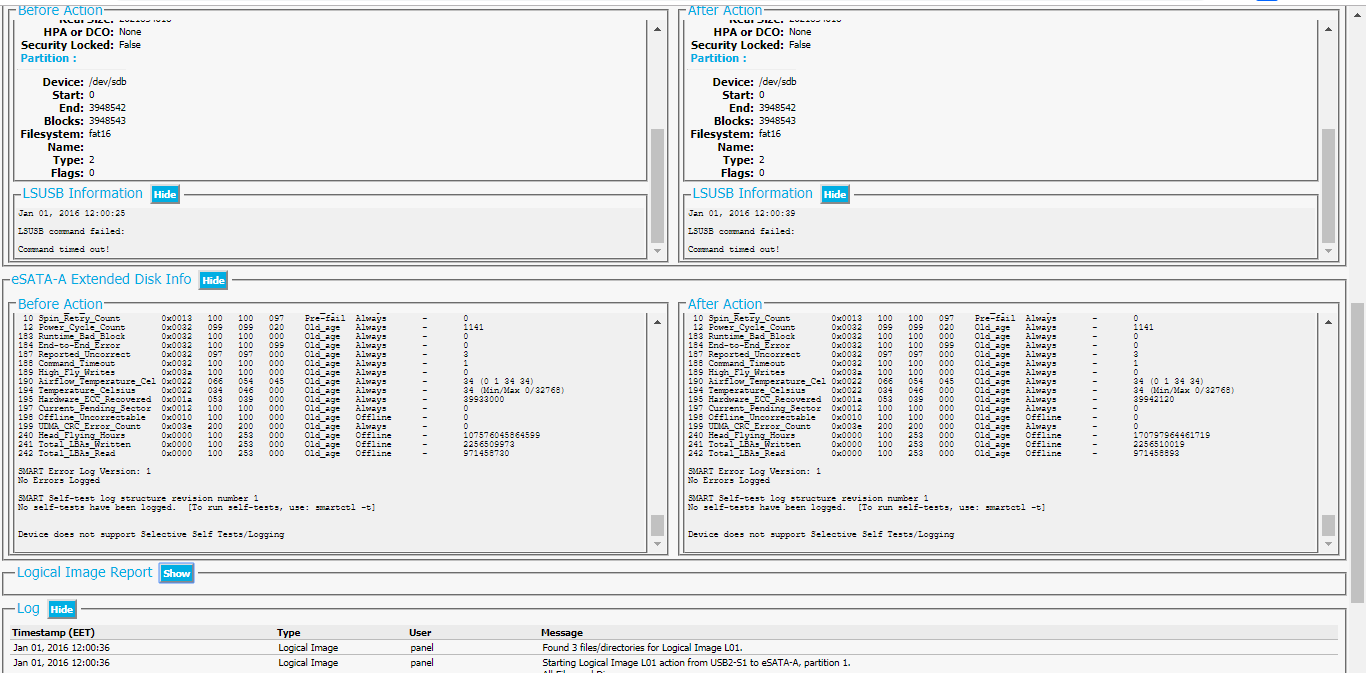


32.Kurtama

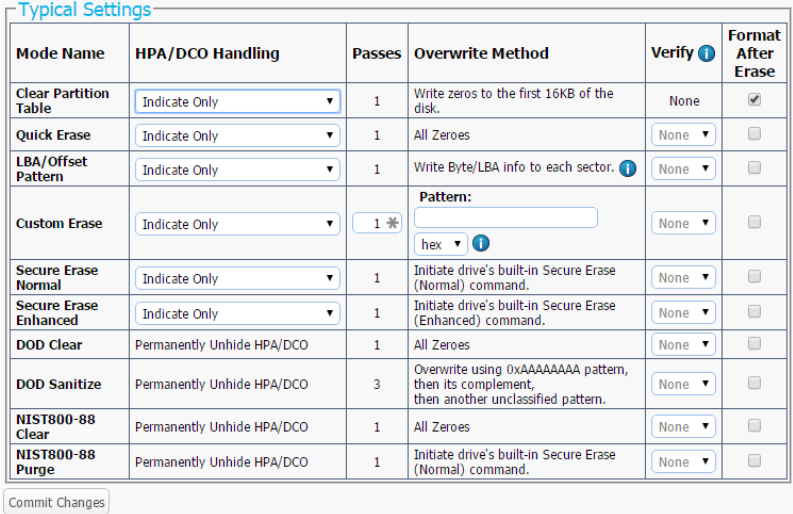
Dosyalarımız kurtarılmış şekilde gelmiş bulunmaktadır. Bunu herhangi bir yazılım ile incelediğimiz vakit verilerimize ulaşabiliriz.



33.Kurtarılan İmaj Log Kayıtları-1

34. .Kurtarılan İmaj Log Kayıtları-2

**3.WİPE İŞLEMİ YAPILMIŞ DİSKTEN VERİLERİ KURTARMA İŞLEMİ**



35.Wipe Tipini

Wipe Türünü seçip işlemimizi başlatıyoruz.Gerekli tüm işlemler bittikten sonra tekrar diskimizin imajını alıp alınan imajı incelediğimiz vakit wipe edilmiş dosyaları kurtarılmadığını görmüş olduk.