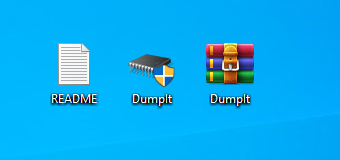
|  |
| --- |
| ***DumpIt ve FTK Imager*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| Ram geçici hafıza olarak görev yaparken,arka planda çalışan uygulamalar,web sitesi kayıtları gibi bilgiler burada depolanır.Bu veriler ise Adli bilişim açısından çok önemli verilerdir.DumpIt ve FTK Imager kullanılarak ram imajı nasıl alınır bunun hakkında bilgi vereceğim. |

**14.07.2021**

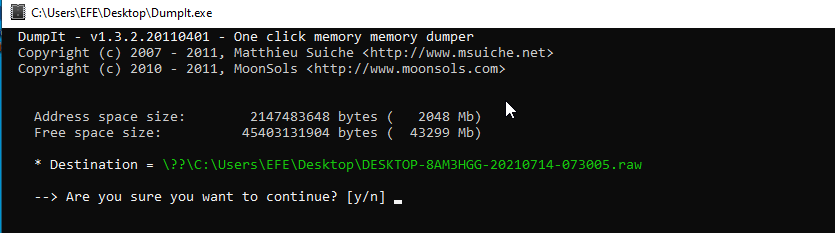
-RAM, bilgisayarların o an çalıştırdığı prosesleri, internet bağlantılarını, dokümanları, konsol ekranına yazılan komutları, sistemi kullanan kullanıcıları, kullanıcılara ait şifreleri ve tarayıcı geçmişleri gibi bir çok bilgiyi tutmaktadır.

-Bu ram imajlarını almak için kullanılan belli başlı toollar vardır.Bunlara “DumpIt ve FTK Imager örnek verilebilir.Bunlar hakkında size bilgi vereceğim.Ardından almış olduğum imajları başka bir tool yardımıyla incelemeyi göstereceğim.

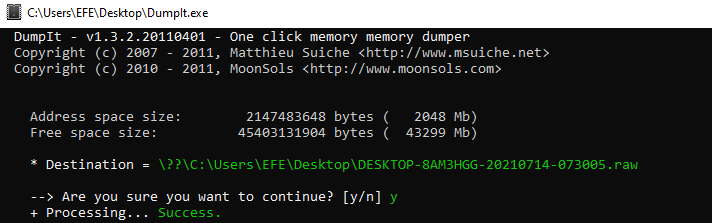
-Öncelikle DumpIt toolu ile başlamak istiyorum. “<https://down10.software/download-dumpit/>” bağlantısından indirebiliriz.



İndirdiğimiz tool’u “rar” formatından çıkarıyorum ve çalıştırıyorum.

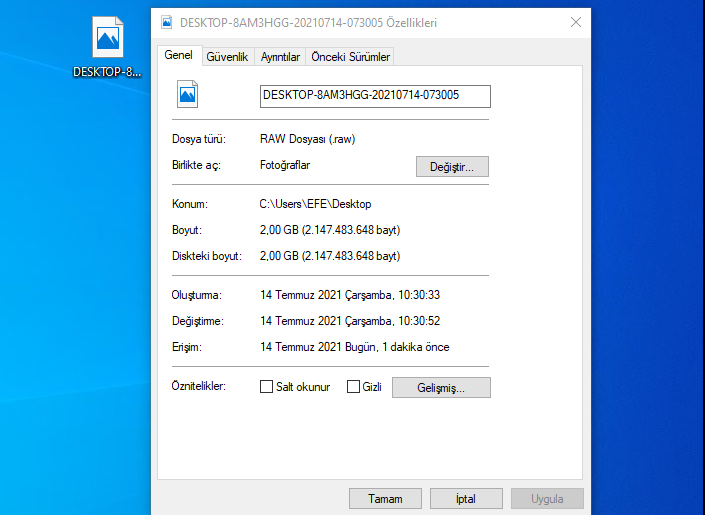


Ardından açılan pencerede alınan imajın kaydedileceği yer “Destination” kısmında belirtilmiştir.İmaj alma işlemi başlamak için “y” tuşuna basıp “enter”a basıyoruz.



İşlemin uzunluğu RAM’in boyutuna bağlı olarak değişmektedir.Processing yazısının yanına “Success” yazısı geldiğinde işlemimiz başarılı bir şekilde sonlanmıştır.

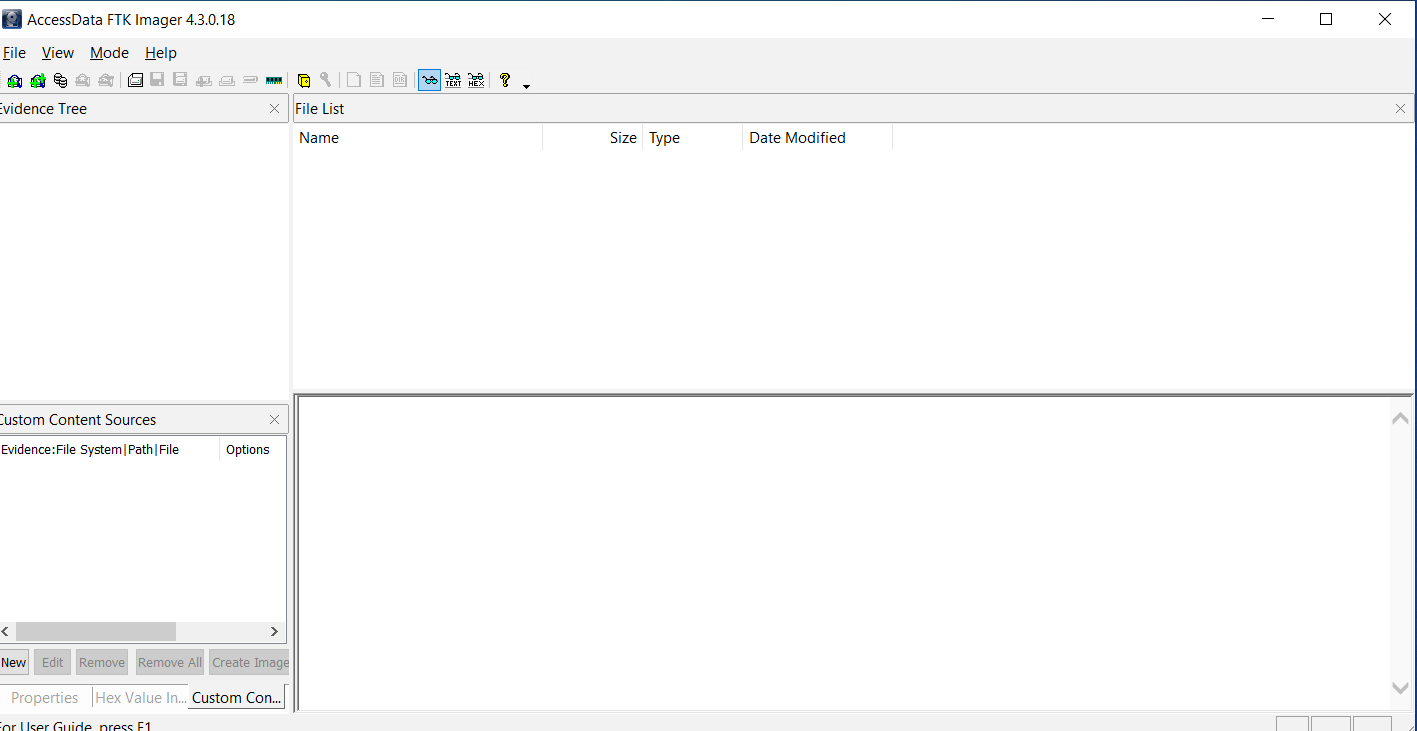
-Ram imajını “DD” formatında yani RAM boyutu ile aynı boyutta olacak şekilde bir imaj oluşturur.Oluşan imaj DumpIt’i çalıştırdığımız dizine kayıt edilecektir.



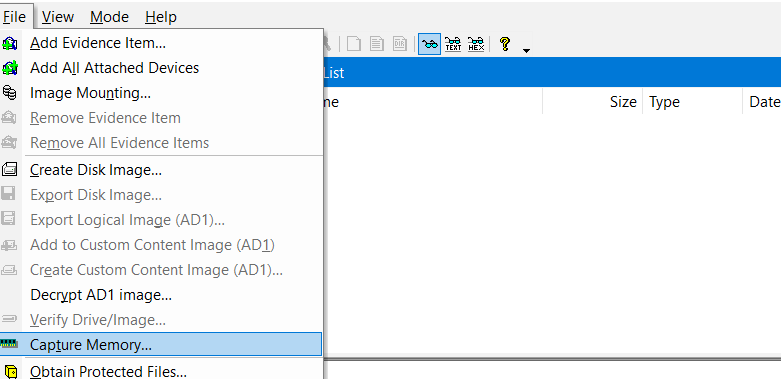
DumpIt kullanarak almış olduğum imajın boyutunu görüntüleyip işlemin başarılı bir şekilde gerçekleşip gerçekleşmediğini de teyit edebilirim.

- FTK Imager, Adli bilişim alanında çok fazla ve ücretsiz olarak kullanılan yaygın bir yazılımdır.Ram imajının haricinde “DD ve E01” formatında HDD’inde imajını alabildiğimiz bir yazılımdır.

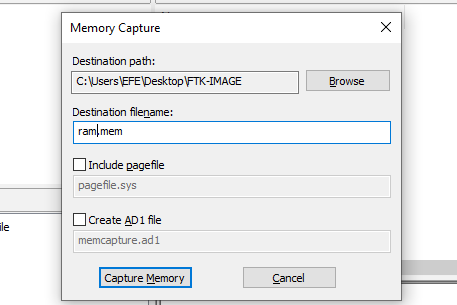
- “<https://accessdata.com/product-download/ftk-imager-version-4-5>” bağlantısından erişim sağlayabiliriz.Açılan site üzerinden,kayıt olma işlemi gerçekleştirilir ve kayıt olurken vermiş olduğumuz “e-posta” üzerinden gelen link üzerinden indirme işlemine başlanabilir.



İndirme işlemi sonrasında bizi bu ekran karşılar.



Ardından “File>Capture Memory” sekmesine geçiş yapıyoruz.



-Pagefile ya da AD1 eklemek için seçim yapılabilir.Bu kesinlikle isteğe bağlı olarak değişmektedir.

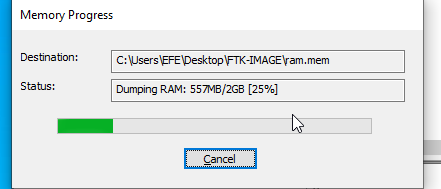
-Ad1; içerisinde ram ve pagefile imajlarınıda bulunduran bir imaj türüdür.

-Pagefile;Ram uzantısına bağlı bir dosyadır ve ram eğer yetersiz gelir ise buraya depolanır.

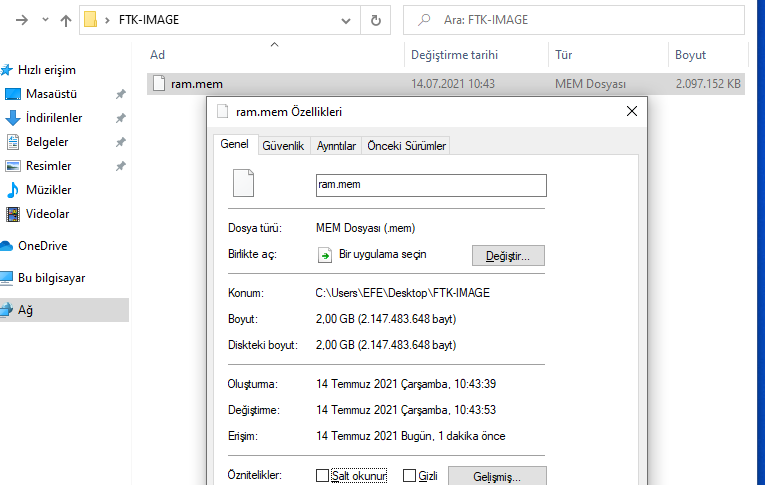
-Destination bölümünde imajımızın alınacağı yeri seçebiliyoruz.

-Destination Filename kısmında ise imajımızın ismini değiştirebiliyoruz.

-Tüm bu ayarlar bittikten sonra “Capture Memory” butonuna basıyoruz.



İmaj alma işlemimiz başarılı bir şekilde başladı ve imaj alma sürecini buradan takip edebiliriz.



İmaj alma işleminden sonra Destination bölümünde belirttiğimiz dizine imajımız kayıt edilecektir ve “DD” formatında aldığı için RAM’in belleğiyle aynı boyuttadır.