

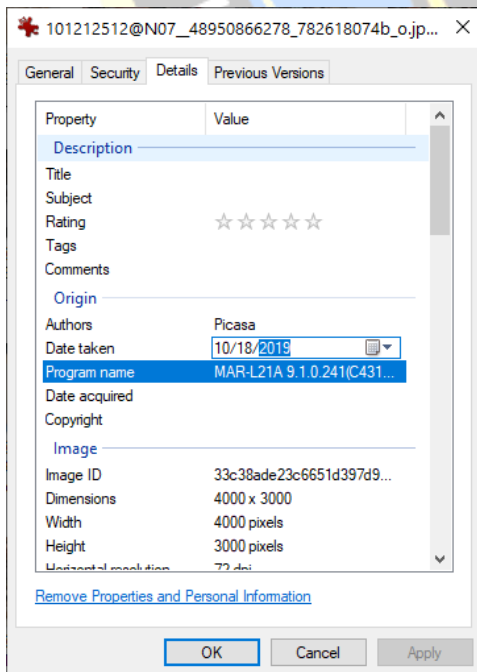
METADATA VERİLERİ NE KADAR GÜVENİLİR

Mehmet ŞEN, Emniyet Müdürü (E), Olay yeri inceleme ve adli görüntüleme uzmanı

Dosya Sistemi Meta Verileri dosyanın bir parçası değildir. İşletim sistemi tarafından ev sahibi cihaz üzerinde başka bir yerde oluşturulur ve muhafaza edilirler. Windows söz konusu olduğunda, diğerlerinin yanı sıra, her dosya için bir *Oluşturma tarihi (Create date)*, bir *Değiştirme tarihi (Modify date)* ve bir *Erişim tarihi (Access date)* tutulur. Bir program dosyaya her eriştiğinde (sadece bir kısmını okumak için bile olsa), *Erişim tarihi* güncellenir (güncellenmelidir). Ne zaman bir program dosyaya bir şey yazsa, *Değiştirme tarihi* değişir (dosya aslında değişmemiş olsa bile). *Oluşturma tarihi*, adından da anlaşılacağı gibi, bu dosyanın dosya sisteminde ne zaman oluşturulduğunu gösterir.

Şimdi, iş arkadaşınız dosyayı size getirdiğinde, USB sürücüden kopyaladınız ve iş istasyonunuza yapıştırdınız. Yeni bir kopya oluşturduğunuz için, dosya sistemi kopya tarihini *Oluşturma tarihi* olarak ayarlarken, elbette kaynak dosyanın Oluşturma tarihi değişmeden kalır. Ancak, dosya sadece kopyalandığı için, dosya sistemi Değiştirme tarihini güncellemez - ve bu, Değiştirme tarihinden daha sonraki bir Oluşturma tarihine nasıl kolayca sahip olabileceğinizi açıklar!

Gömülü Meta Veriler farklı bir hikayedir: dosyanın içine yazılırlar ve onunla birlikte hareket ederler. Normalde görüntü/video oluşturulduğunda yazılırlar ve muhtemelen dosya herhangi bir şekilde manipüle edildiğinde işleme yazılımı tarafından güncellenirler. Dosya yükünün bir parçası oldukları için kopyala-yapıştır işlemlerinden etkilenmezler. Ancak ne yazık ki, bir saldırgan için bunları silmek veya değiştirmek çok kolaydır! Windows'ta, bazı gömülü meta veriler Dosya Özellikleri panelinden değiştirilebilir veya silinebilir!



Kaynak: Amped 5, <https://blog.ampedsoftware.com/2021/05/04/metadata-so-useful-but-not-so-reliable>

