Yazma Koruması

Efekan Acar

Adli Bilişim Mühendisliği, Fırat Üniversitesi

200509047@firat.edu.tr

Özet

Bu makalede ilk olarak yazma korumasından bahsettim. Daha sonra fiziksel ve yazılımsal yazma korumalı belekleri açıkladım. Yazılımsal yazma koruma özelliği farklı işletim sistemlerinde farklı şekillerde USB belleğe eklenebilir, bunun 4 türünü gösterdim: Windows komut satırı, Windows registry, 3.parti yazılımlar, Linux komut satırı. Yazma koruması ve adli bilişimden bahsettim bununla birlikte: write blocker cihazları, Safe Block, Guymager yazılım ve donanımlarından da bahsettim.

Giriş

Bu makalede yazma korumasının tanımından, özelliklerinden, nerelerde yer aldığından, ne şekilde aktif/deaktif edildiğinden bahsettim. Ana makinem Windows 10 Pro, Linux makinem Kali Linux 2023.1-VMware Workstation Pro.

Anahtar kelimeler: yazma koruması , adli bilişim , disk, imaj

Yazma Koruması

Yazma koruması, kullanıcıların verilerinin korunması için kullanılan bir özelliktir. Bu özellik, USB bellekler, harici sabit diskler ve SD kartlar gibi taşınabilir bellek aygıtlarında yer alabilir. Bellekteki verinin silinmesini veya değiştirilmesi engellenir ancak okunulabilir durumdadır.

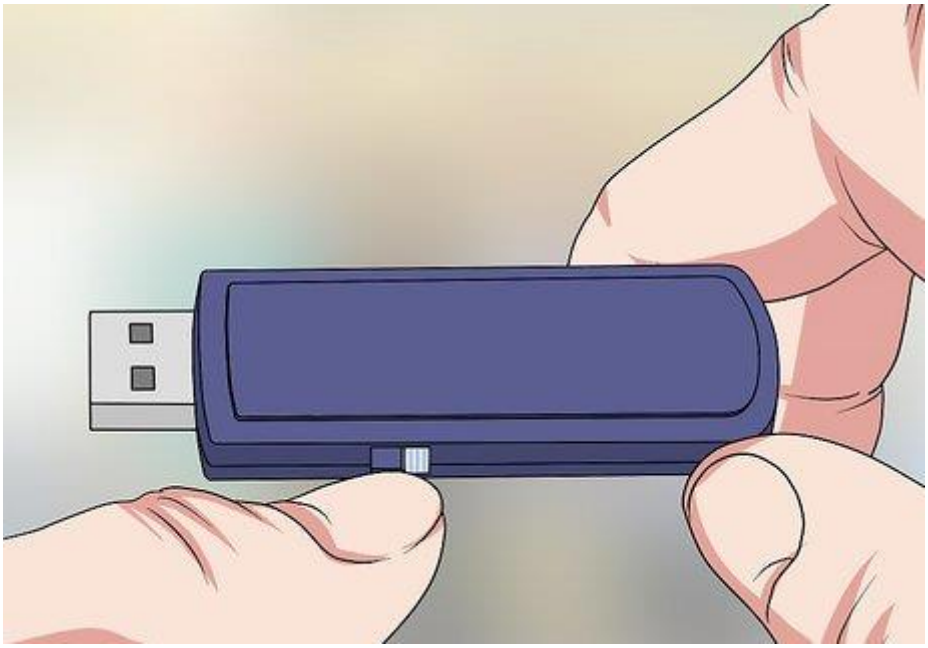
Yazma korumalı bellekler, fiziksel bir anahtar ile veya yazılım sayesinde kullanıcıların veri yazma ve silme işlemlerini engeller. Yalnızca yazma ve silme işlemlerini engellemekle kalmaz, verileri şifreleyebilir. Bu sayede kötü amaçlı bir saldırı sonucu verilerin güvenliği en üst düzeyde tutulmuş olur. Genellikle kamu kurumlar, askeri birimler, bankalar, özel kurumlar gibi verinin güvenliğinin önemli olduğu yerlerde kullanılmaktadır. Bireysel kullanıcılarda verilerini korumak için yazma korumalı bellekleri kullanabilir.

Yazma Koruması, dijital delil incelemesi, veri kurtarma veya diğer güvenlik işlemlerinde kullanılır. Adli Bilişim işlemlerinde verilerin bütünlüğü ve doğruluğu büyük önem taşıdığı için yazma koruması olmadan bu iş yapılamaz. Yazma koruması verinin doğruluğunu bozmadan inceleme yapılmasını sağlar.

Yazma korumalı belleklerde yalnızca belirli alan sadece okunabilir formattadır, yeni bir veri eklemek veya silmek mümkün değildir. Sonuç olarak; yazma koruması, verilerin güvenliğini sağlamak için tasarlanmış son derece önemli bir özelliktir.

Fiziksel Yazma Korumalı Bellekler

Fiziksel Yazma Korumalı USB belleklerde veya bazı diğer taşınabilir belleklerde bir adet tuş veya anahtar yer alır. Bu anahtar ile yazma korumasını açıp kapatabiliriz. Yazma koruması açık iken veri yazılamaz veya silinemez. Bu sayede kötü amaçlı yazılımlardan korunmuş oluruz, tekrar veri yazmak istediğimiz zaman ise yazma korumasını kapatmamız yeterlidir.



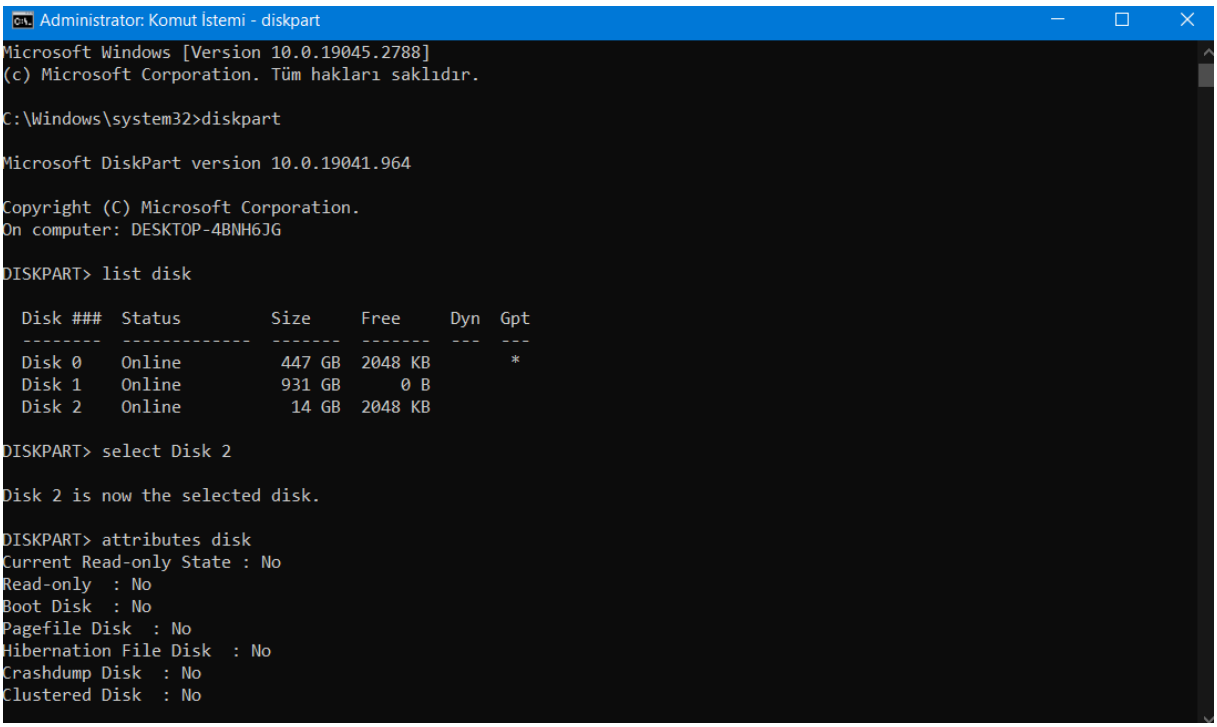
Yazılımsal Yazma Korumalı Bellekler

Yazılımsal Yazma Korumalı Bellekler yani normal bellekler ekonomik olarak daha uygundur ancak kötü amaçlı yazılımlardan etkilenebilir. Yazma koruma özellikleri farklı işletim sistemlerinde farklı şekillerde belleklere eklenebilir.

1.Windows Komut Satırı

Windows Komut İstemcisini yani ‘cmd’yi yönetici olarak çalıştırıyoruz. Ardından sırası ile ‘diskpart’ ve ‘list disk’ komutlarını yazıyoruz. Burada bilgisayarımıza bağlı olan bütün diskleri görebiliyoruz. Usb belleğinizi yani yazma koruması özelliğini aktif etmek istediğiniz belleğinizi seçmemiz lazım.

Yanlış diski seçmemeye dikkat edin. Benim yazma korumasını aktif etmek istediğim USB belleğim Disk 2, bu yüzden ‘select Disk 2’ komutunu yazıyoruz. Diskin özelliklerini görmek için ‘attributes disk’ komutu yazıyoruz. Burada da görüldüğü üzere diskimizin yazma koruması kapalı.



Yazma korumasını açmak için ‘attributes disk set readonly’ komutunu yazıyoruz. İşlemimiz başarılı oldu.

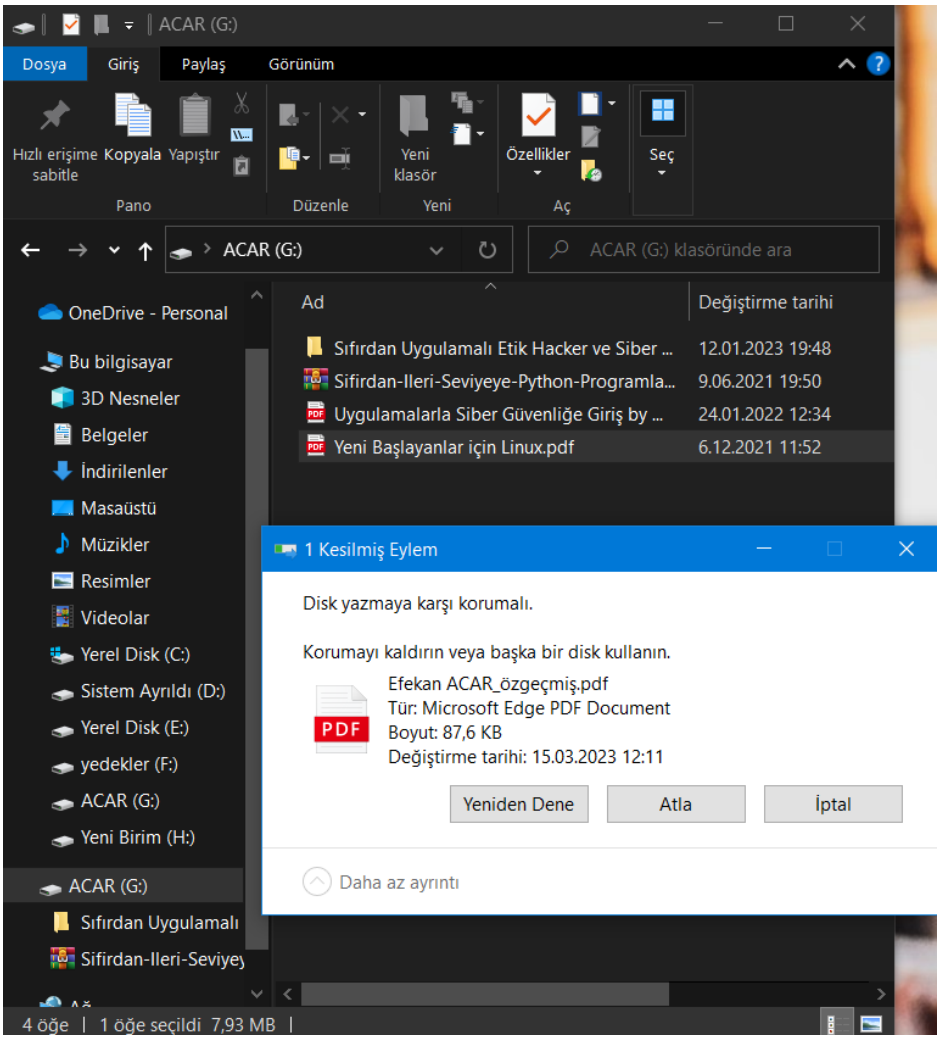
```
DISKPART> attributes disk set readonly

Disk attributes set successfully.

DISKPART> attributes disk
Current Read-only State : Yes
Read-only  : Yes
Boot Disk  : No
Pagefile Disk  : No
Hibernation File Disk  : No
Crashdump Disk  : No
Clustered Disk  : No

DISKPART>
```

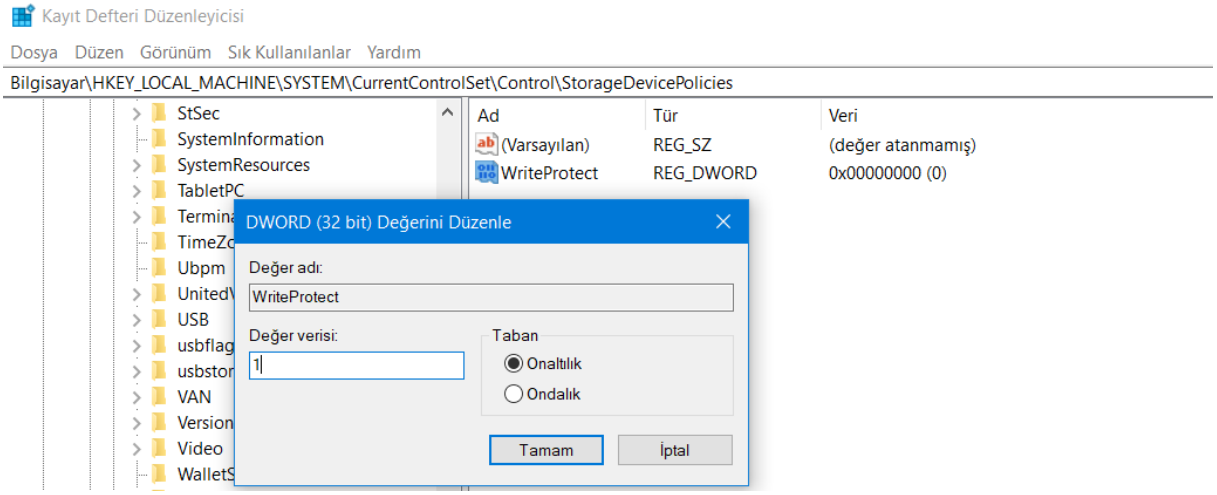
Bu sayede diskin içerindeki veriler silinemez ve değiştirilemez hale geldiler. Yalnızca okuma işlemini gerçekleştirebiliyoruz. Eski haline çevirmek için ise ‘attributes disk clear readonly’ komutunu yazmak yeterlidir.



2.Windows Registry

Windows Registry'i açmak için Windows ve R tuşlarına aynı anda basarak çalıştır menüsünü açıyoruz. Daha sonra regedit yazarak Kayıt Defteri Düzenleyicisini yani Registry Editörü açıyoruz.

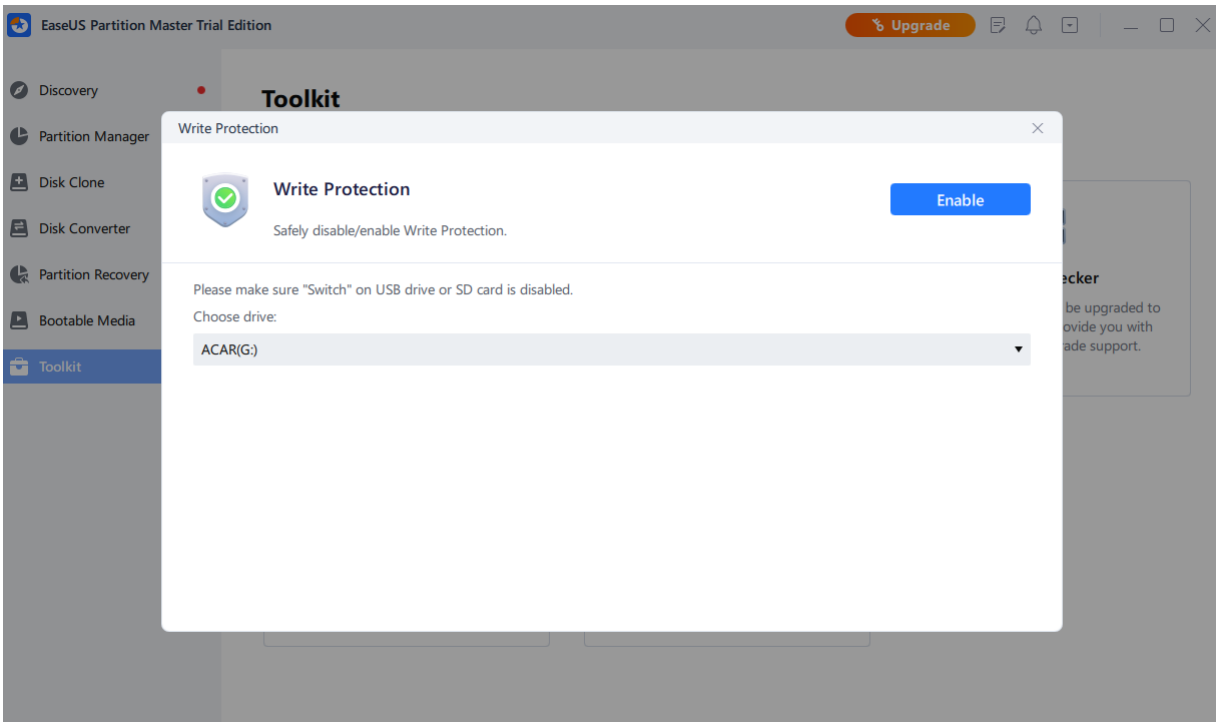
Buradan "Bilgisayar\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies" konumuna gidiyorum. Eğer bu anahtar mevcut değilse yeni anahtar olarak oluşturuyorum. İçerisine ismi "WriteProtect" yeni DWORD (32bit) değeri oluşturuyoruz.



Bu değeri düzenlemek istediğimiz zaman Değer verisini 1 yaparsak yazma koruması aktif olur,0 yazarsak deaktif olur. Bu yöntem tüm sürücülere yazma koruması verebilir.

3.3.Parti Yazılımlar

EaseUS Partition Master Programını açıyoruz. Toolkit sekmesinde yer alan Write Protection kısmından diskimizi seçerek Enable konumuna alırsak yazma koruması aktif olur. Disable diyerek de deaktif konuma alabiliriz.

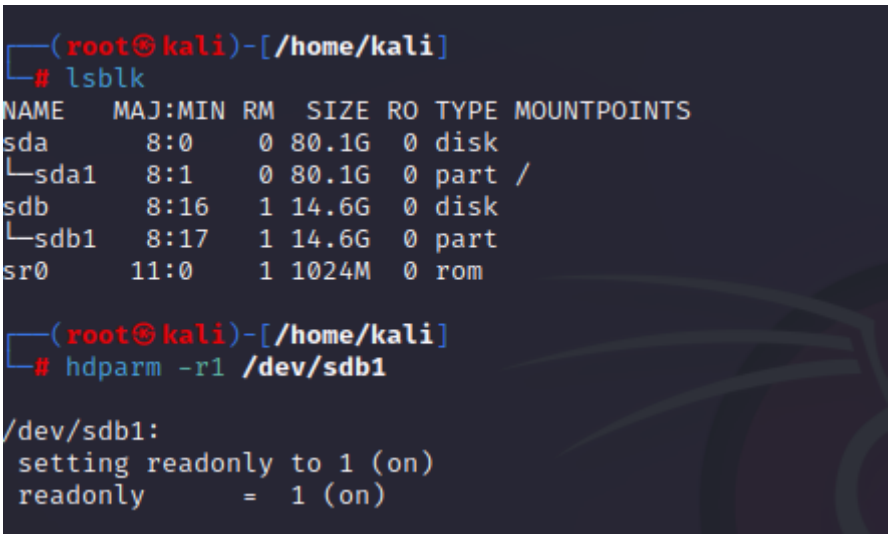


Buna benzer başka yazılımlarda kullanabiliriz, ancak dikkatli olmak lazım orijinal yazılım olduğundan emin olduktan sonra indirmek daha güvenli olur.

4.Linux Komut Satırı

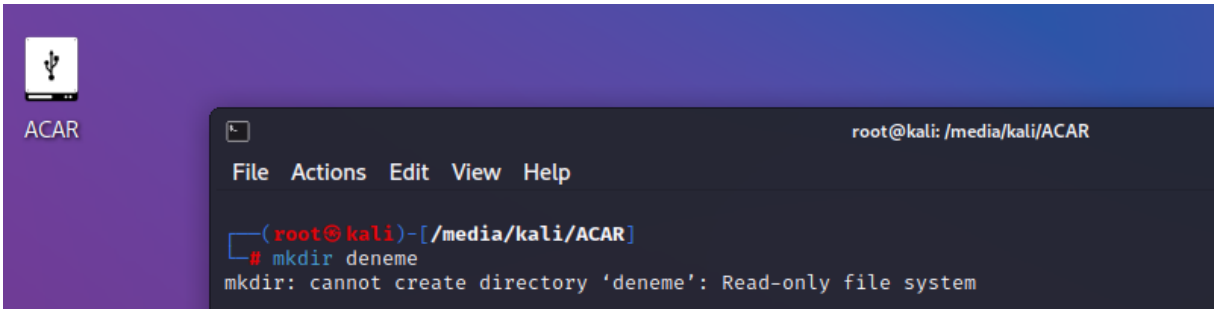
Linux işletim sistemleri açık kaynaklı sistemlerdir. Diğer işletim sistemlerinde olduğu gibi herhangi bir diski bağlamak mümkündür. Bu diskleri görmek için "df –h", "sudo fdisk –l", "lsblk" komutlarından birisi kullanılabilir. Öncelikle bağlı disklerimizi görelim.

Yazma korumasını aktif etmek istediğimiz diske karar verdikten sonra işleme başlıyoruz, bunun için de farklı komutlar kullanılabilir ancak ben daha sade olduğu için "hdparm" komutunu kullanacağım. Genellikle Linux sistemlerde hdparm yüklü geliyor ancak değil ise "sudo apt-get install hdparm" komutu ile indirebiliriz.



"-r1" r readonly yani yazma korumasını ifade ediyor, 1 ise aktif etmek istediğimizi ifade ediyor. Yazma korumasını deaktif etmek için 1 yazan yere 0 yazarak aynı kodu kullanabiliriz.

"dev/sdb1" diskimizin konumunu belirtiyor.



Yeni bir dosya yüklemeyi veya içerisindeki dosyada değişiklik yapmayı denediğim zaman izin vermiyor ve diskin yazma korumalı olduğunu belirtiyor.

Yazma Koruması ve Adli Bilişim

Yazma koruması, adli bilişim açısından önemli bir konudur. Adli bilişim, dijital delillerin toplanması, incelenmesi ve yasal delil olarak kullanılmasını kapsar. Orijinal veriye ulaşmak için yazma koruması şarttır. Ancak bazı durumlarda yazma koruması veri toplama işlemini yavaşlatabilir veya verilerin toplanmasını engelleyebilir.

Write Blocker Cihazları

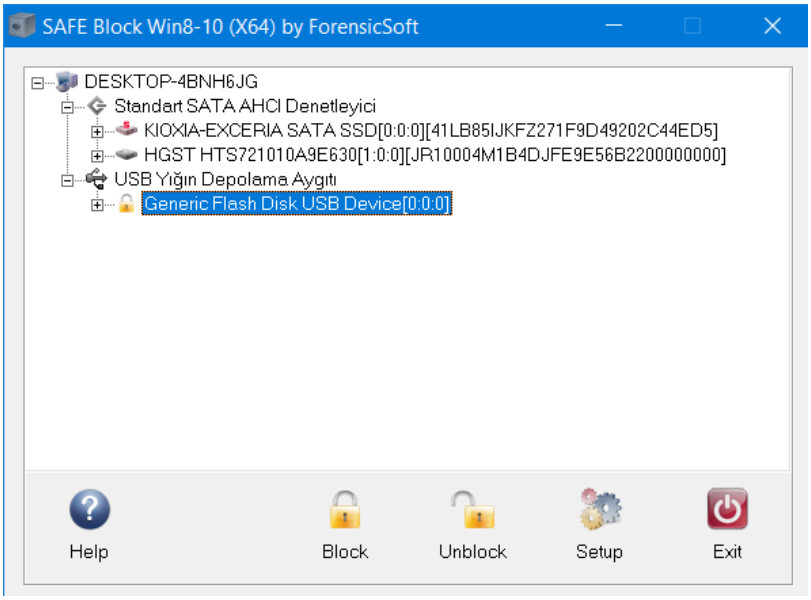
Şüpheli disk içindeki verileri korumak için write blocker cihazları kullanılarak yazmaya karşı korumak gerekir. Write blocker, bir donanım cihazı veya yazılım uygulamasıdır. Yazma korumalarını engeller ve disk ortamına salt okunur erişmemizi sağlar.

Donanımsal usb bellek, sd kart, kamera ve diğer dijital cihazlardaki verilerin orjinalliğini korur. Ayrıca adli bilişim donanımlarının giriş portları da yazma korumalıdır veya yazma koruması sağlayan bridgeler mevcuttur(Ditto, Tableu). Örneğin CRU® WiebeTech® USB WriteBlocker™, Tableau Forensic USB Bridge, vb.

Yazılımsal write blocker fiziksel bir donanıma ihtiyaç duymaz, ekonomik olarak daha ulaşılabilirdir. Yazılımın güvenilirliği ve kaliteside önemlidir. Adli bilişim işlemlerinde sıkça kullanılır. Deneyimli ve bilgili kişilerin kullanması önerilir çünkü yanlış kullanımda istenmeyen sonuçlara neden olabilir. Örneğin SAFE Block, MacForensicsLab Write Controller, vb.

Safe Block

Safe Block, bilgisayar ve diğer dijital cihazlarda veri toplama işlemlerinde kullanılan bir donanımsal write blocker cihazıdır. SafeBlock, kapsamlı yazma koruması sağlayan ve dijital verilerin orijinalliğini koruyan bir cihazdır. Ücretli bir yazılımdır ancak test etmek için 7 günlük deneme sürümünü alabilirsiniz.

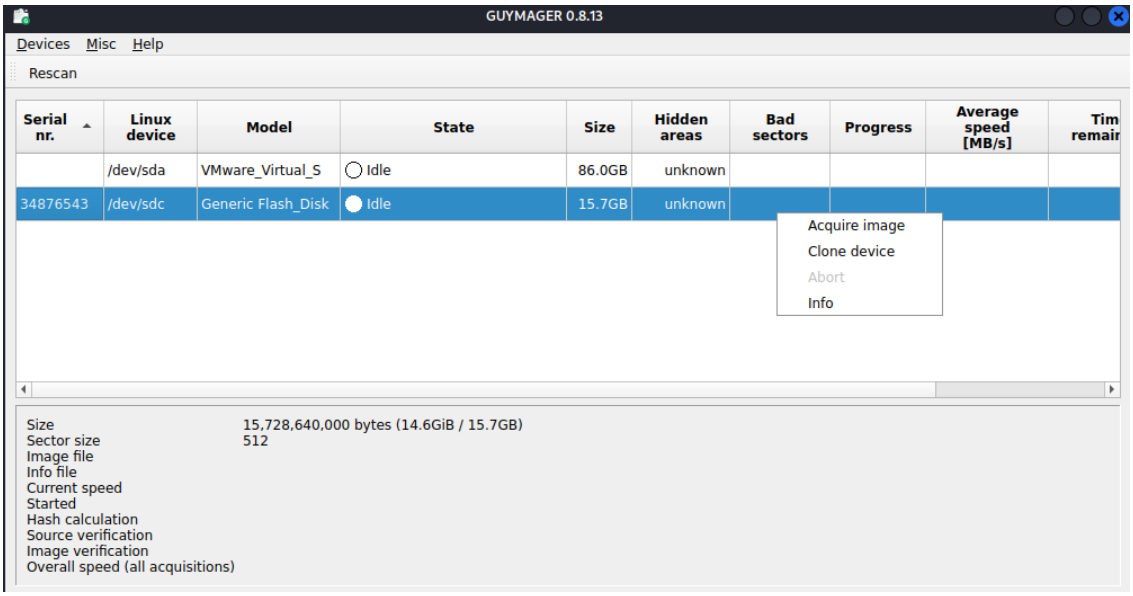


Basit bir arayüzü var, bağlı bütün diskleri görebiliyoruz. Yazma koruması ayarlamak istediğimiz diski seçiyoruz ve 'block' veya 'unblock' diyerek yazma korumasını aktif veya deaktif hale getirebiliyoruz.

Guymager

Guymager, adli bilişim işlemlerini yapmaya yarayan Linux ve diğer Unix tabanlı işletim sistemlerinde kulanılan açık kaynak kodlu bir araçtır. Dijital verilerden veri toplamaya yaran bir write blocker'dır. Hem GUI hem komut satırı ile kullanılabilir. İmaj oluşturmak ve analiz etmek için kullanılabilir. Araç, çeşitli yazma koruması modlarına sahiptir. Verinin değiştirilmesini ve silinmesini engelleyerek orjinalliğini ve bütünlüğünü korur.

Komut satırına 'guymager' yazarak açabilirsiniz, yüklü değil ise 'apt-get install guymager' yazarak indirebilirsiniz.



Burada bütün bağlı diskleri görebilirsiniz. 'acquire image' ile imaj alabilir, 'clone device' ile klonunu alabilir, 'info' ile disk hakkında bilgi edinebilirsiniz.

Kaynaklar

https://www.easeus.com/partition-master/kingston-write-protected-removal-tool.html

https://www.computerhope.com/issues/ch001617.htm#:~:text=Protecting%20individual%20files.-,Write%2Dprotection%20hardware%20switch,to%20the%20%22Lock%22%20position.

https://www.wikihow.com/Format-a-Write%E2%80%93Protected-Pen-Drive

https://www.alphr.com/how-to-remove-write-protection-from-a-usb/

https://www.forensicsoft.com/products/safe-block