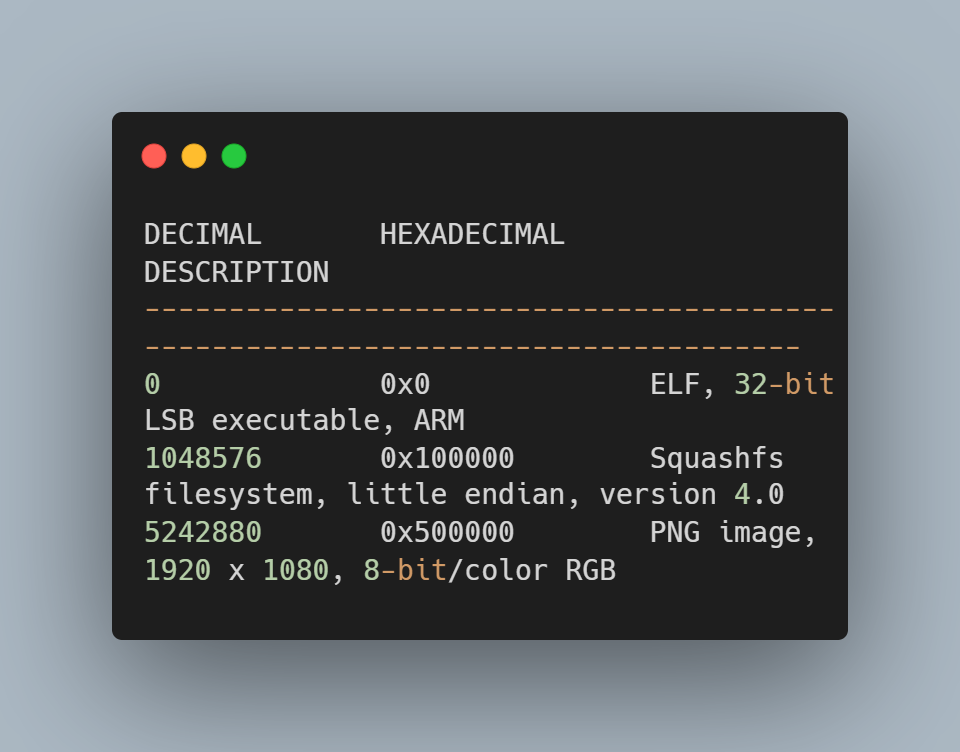
**Binwalk Nedir?**

Öncelikle "firmware" kavramını kısaca açıklayalım. Firmware, genellikle akıllı cihazların (modemler, yazıcılar, güvenlik kameraları gibi) içindeki yazılımdır. Bu yazılım, cihazın donanımını kontrol eder.

Binwalk, firmware dosyalarının içinde neler olduğunu anlamamıza yardımcı olan açık kaynaklı bir analiz aracıdır. Genellikle .bin, .img gibi uzantılara sahip olan bu dosyaların içeriğini incelemek için kullanılır.

Binwalk, "binary" dosyaları (ikili dosyalar) açmak, içindeki gizli verileri veya dosya sistemlerini ortaya çıkarmak için kullanılır.



Bu çıktı bize şunu anlatır:

* Sıfırıncı bayttan başlayan bir ARM çalıştırılabilir dosyası var
* 1 MB’dan sonra bir Squashfs (dosya sistemi) başlıyor
* 5 MB civarında bir PNG görsel dosyası yer alıyor

**Binwalk Nasıl Yüklenir?**

Binwalk, Linux sistemlerde kolayca yüklenebilir. Kali Linux gibi siber güvenlik dağıtımlarında genellikle hazır kurulu gelir.

Linux (Debian/Ubuntu) için yükleme komutu:

***sudo apt-get update***

***sudo apt-get install binwalk***

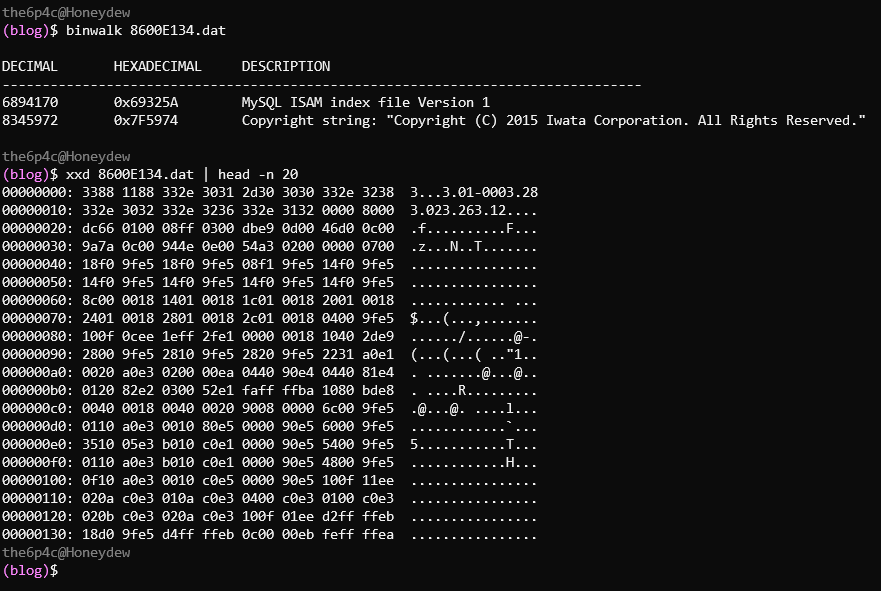
Alternatif olarak Python paket yöneticisiyle de kurulabilir:

***sudo pip install binwalk***

***Binwalk ile Neler Yapılabilir?***

Binwalk ile bir firmware dosyası ya da herhangi bir binary dosya üzerinde aşağıdaki işlemler yapılabilir:

* Dosya içindeki gömülü dosya türlerini tespit etme (örneğin PNG, ZIP, ELF dosyaları)
* Sıkıştırılmış dosyaları bulup çıkartma
* Gömülü dosya sistemlerini tanıma (örneğin squashfs, cramfs)
* Firmware parçalarını otomatik olarak ayıklama
* Steganografi ya da zararlı yazılım analizlerinde yardımcı araç olarak kullanma



Binwalk -e komutu ile otomatik çıkarma yaptığında oluşturulan klasör yapısını gösteriyor.

**Temel Kullanım Komutları**

Basit analiz: ***binwalk firmware.bin***

Bu komut, firmware dosyasının içindeki bilinen dosya türlerini ve başlangıç offset'lerini listeler.

Otomatik çıkarma (extract): ***binwalk -e firmware.bin***

-e parametresi ile Binwalk bulduğu içerikleri bir klasöre çıkartır.

Daha derin analiz için: ***binwalk -Me firmware.bin***

-M (recursive) ile bulunan her dosya da tekrar taranır. -e ile içerikler çıkarılır.

**Gerçek Hayatta Nerede Kullanılır?**

Binwalk, şu alanlarda kullanılır:

* Tersine mühendislik (Reverse Engineering)
* Güvenlik araştırmaları (özellikle IoT cihazları)
* Cihaz yazılım güncellemelerinin analizinde
* Zararlı yazılım analizlerinde (örneğin gizlenmiş dosyaları bulmak için)

Binwalk gibi analiz araçları yasal izne sahip olduğunuz firmware dosyalarında kullanılmalıdır. Başka bir cihaza ait, izinsiz alınmış firmware dosyalarını analiz etmek yasal sorunlara yol açabilir.

Binwalk, firmware dosyalarının iç yapısını anlamak isteyen herkes için oldukça güçlü ve kullanışlı bir araçtır. Özellikle siber güvenlik, IoT güvenliği ve tersine mühendislik gibi alanlarda temel araçlardan biridir.

Bu yazıyla beraber artık:

* Binwalk’ın ne işe yaradığını,
* Nasıl yüklendiğini,
* Temel komutlarını  
  öğrenmiş oldunuz.