Dosya Sistem Analizi

Linux İmaj İnceleme Çalışması

Adli Bil. Müh. Hasan BASKIN
info@hasanbaskin.com

Linux Nedir ?

Linux, serbestçe dağıtılabilen, çok görevli, çok kullanıcılı UNIX işletim sistemi türevidir. Linux, İnternet üzerinde ilgili ve meraklı birçok kişi tarafından ortak olarak geliştirilmekte olan ve başta IBM-PC uyumlu kişisel bilgisayarlar olmak üzere birçok platformda çalışabilen ve herhangi bir maliyeti olmayan bir işletim sistemidir.

UNIX 70'li yılların ortalarında büyük bilgisayarlar üzerinde çok kullanıcılı bir işletim sistemi olarak geliştirilmiştir. Zaman içerisinde yayılmış ve birçok türevi ortaya çıkmıştır.

En Çok Kullanılan Linux Forensic Araçları

- Sans Sift
- CrowdStrike CrowdResponse
- Volatility
- The Sleuth Kit (Autopsy)
- Ftk Imager
- Linux «dd» Komutu
- Linux Caine distrosu
- ExifTool
- Deft
- Last Activity View

Konu, İçerik ve Yöntem

- Dosya Sistem Dersi Proje ödevi için hazırlanan bu sunumda Linux İşletim sistemine sahip olan bir bilgisayarın imajı manuel olarak «dd» alınmıştır. Daha sonra alınan bu imaj üzerinde hazır araçlar kullanılarak araştırmalar yapılmıştır.

- Günümüzde birçok Forensic Tool'u Linux sistemleri inceleme noktasında fazlasıyla yetersiz kalmaktadır.Bu noktada halihazırda bilinen hazır adli inceleme araçlarıyla yaptığım Linux incelemesine ek olarak kendim tek tek ilgili dosya yollarını kontrol ederek hem programın doğruluğu test etmiş oldum hemde Yerine göre daha detaylı bilgiler ve çıkarımlar elde edebilmiş oldum.

Autopsy açık kaynak kodlu adli imaj inceleme (forensic) yazılımını kullanarak İmaj inceleme işlemlerimi gerçekleştirmeden önce üzerinde çalıştığım imaj Hakkındaki nitelikli bilgileri bu şekilde tablo olarak belirtebiliriz.

- **Linux İmaj Bilgileri**

Madde	Detaylı Bilgi
Dosya Adı	hbn_pc_imaj
MD 5	008ace8b3902eb576c4defa49b5dd3f1
SHA-1	129da75a5daa7e4220228d23456f1271f5560fef
Yazılım Bilgisi	Autopsy 4.9.0
İmaj Formatı	E01 (Expert Witness Compression Format) Vmdk dosyasından dönüştürülmüş
Sıkıştırma	Orta (Compression = 6)
Sektör / Byte	512
Top. Sektör Sayısı	172.168.215
Toplam Boyut	10 GB (9,792,0 KB)
Sıkıştırılmış Boyut	7.182,114 KB

İncelemekte olduğumuz bilgisayar üzerinde koşan işletim sistemi ve root kullanıcı Bilgilerini aşağıdaki gibi görmekteyiz.

Bilgiye Erişim Yolu : /etc/redhat-release
/var/log/auth.log
/etc/hostname

- **Bilgisayardaki İşletim Sistemi Bilgileri**

İşletim Sisteminin Adı	Kali Linux
Sürüm	4.15.0-kali2-amd64
Sistem Mimarisi	X86 64
Kurulum Tarihi	2019-05-04 22:14:20
Kayıtlı Sahibi	hbn

Bilgisayar üzerinde kullanılan saat / takvim yerel bölge bilgisine otomatize araçlar sayesinde kolaylıkla erişebilmekteyiz.
Burada kullandığımız yazılım bu bilgiyi bize getirmektedir.

Bilgiye Erişim Yolu : /usr/share/zoneinfo

- **Timezone Bilgisi**

Zaman Dilimi	Doğu Avrupa Zaman Dilimi (GMT +03:00)
Günlük Zaman Sapması	+1

İmajı alınan cihaza kurulum aşamasında verilen kullanıcı adı bilgisi

Bilgiye Erişim Yolu : /etc/hostname

- **Bilgisayarın Adı**

hbn

Oturum Açan Kullanıcı Bilgisi

İşletim sisteminde sistem sahibi olan root kullanıcıları haricinde işletim sisteminde bulunan tüm kullanıcı hesapları ve ve bu kullanıcıların adı, ID bilgisi, oturum açma sayısı, oturum açma tarihi gibi genel bilgilere ulaşabilmekteyiz.

Bilgiye Erişim Yolu : /var/log/auth.log
/var/log/faillog

Hesap	SID	Durum	Oturum açma sayısı	Hesap oluşturma tarihi	Son oturum açma zamanı	Başarısız oturum açma zamanı
hbn	Id=0	Aktif	26	2019-05-05 17:51:40	2019-15-12 02:29:01	-

Son Oturum Açan Kullanıcı

Bilgiye Erişim Yolu : /var/log/auth.log

PC'de Son oturum açan kullanıcı.

hbn

Sistemin En Son Kapatılmasına Ait Zaman Bilgisi

Bilgiye Erişim Yolu : /var/log/auth.log

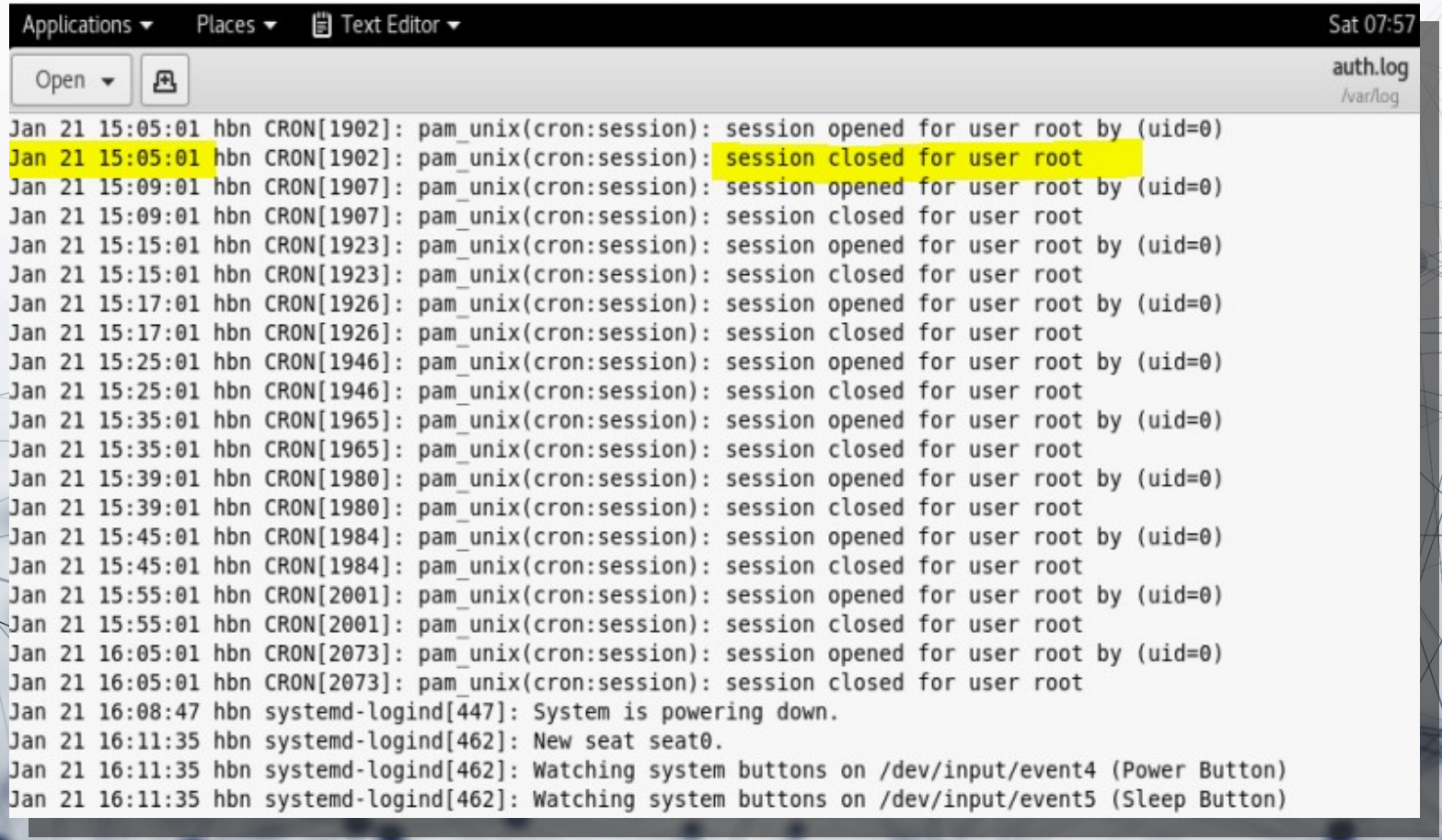
Kaydedilmiş En Son Sistem Kapanma Tarihi ve saati.

2019-05-16 02:25:01

Sisteme Giren Kullanıcıların Bilgisi

İşletim sisteminde son kapatılan oturum bilgilerini daha önce sistemde giriş yapan kullanıcıların bilgilerine ulaştığımız log dosyasından da ulaşabilmekteyiz.

Auth.log dosyasının içeriğini incelediğimiz zaman içinde bulunduğumuz vakitten epey öncesine kadar açılan ve kapanan session bilgilerine ve hangi kullanıcıların bu işlemleri gerçekleştirdiği bilgilerini elde edebiliriz.

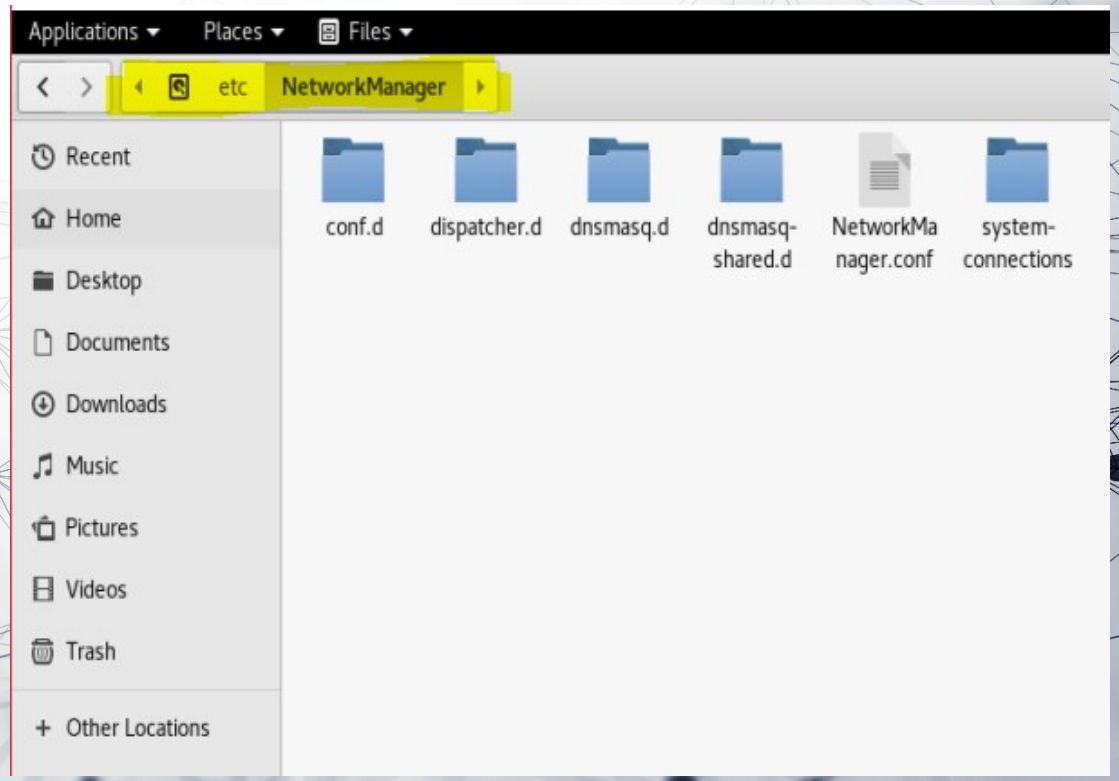


Ağ Bağlantı Bilgileri

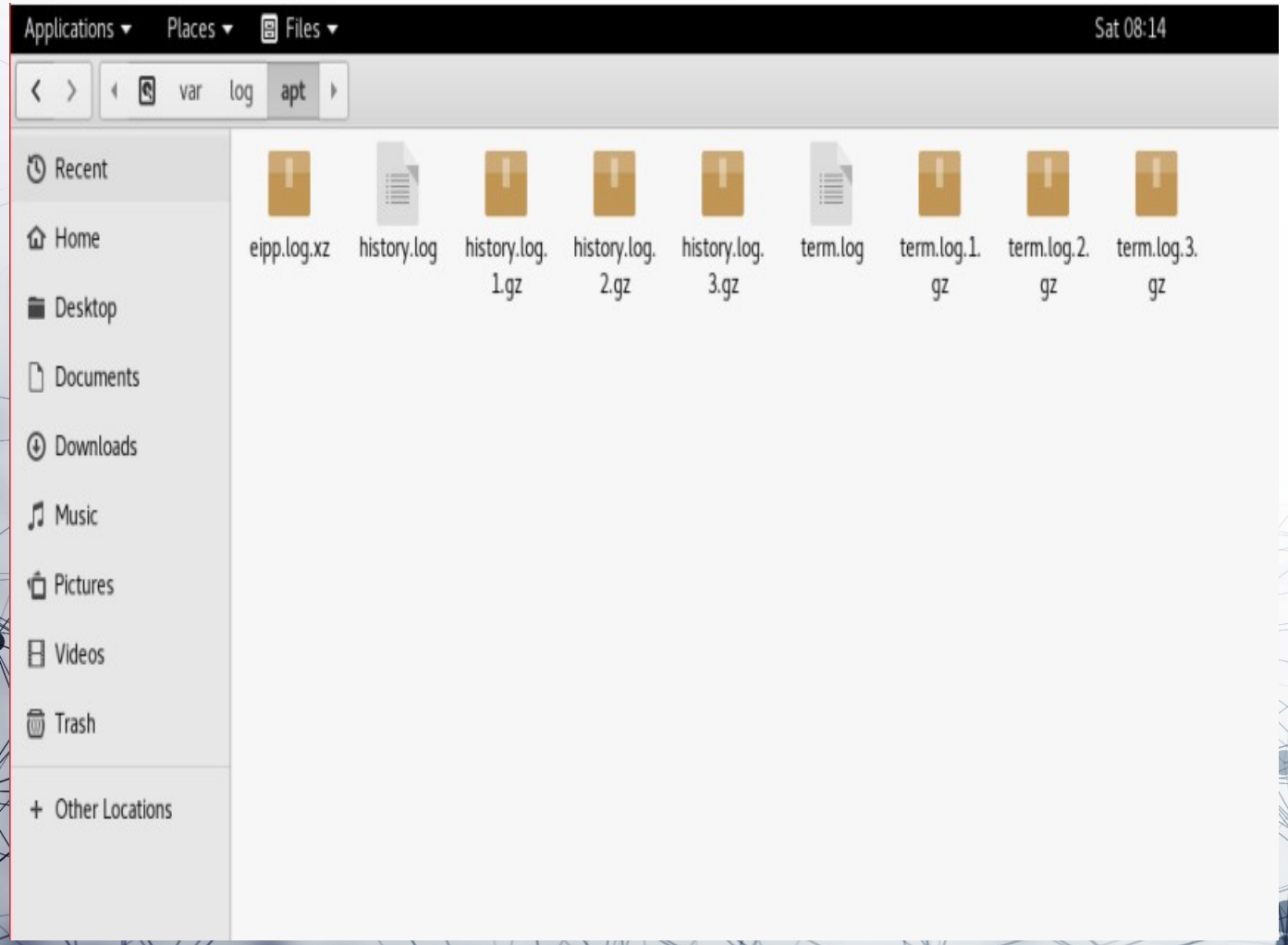
Windows işletim sistemi Registry Kayıtlarından elde ettiğimiz, ilgili bilgisayarın geçmiş ağ bağlantı kayıtlarını Linux İşletim sisteminde aşağıda belirtilen dosya yolunda bulabilmekteyiz.

Bilgiye Erişim Yolu : /etc/network
/etc/networkManager

Adı	Ev_wifi
IP adres	10.0.2.15
IPv6 Adres	fe80::a00:27ff:fe59:1b51
Alt Ağ Maskesi	255.255.255.0
Donanım Adresi	08:00:27:59:1B:51
İsim Sunucusu	10.0.2.1
Domain	Localhost domain
Varsayılan Gateway	10.0.2.1
DNS	156.154.70.25 156.154.71.25
DHCP Kullanımı	Evet
DHCP Sunucusu	10.0.2.254



Yüklenen Yazılım/Araç Bilgileri



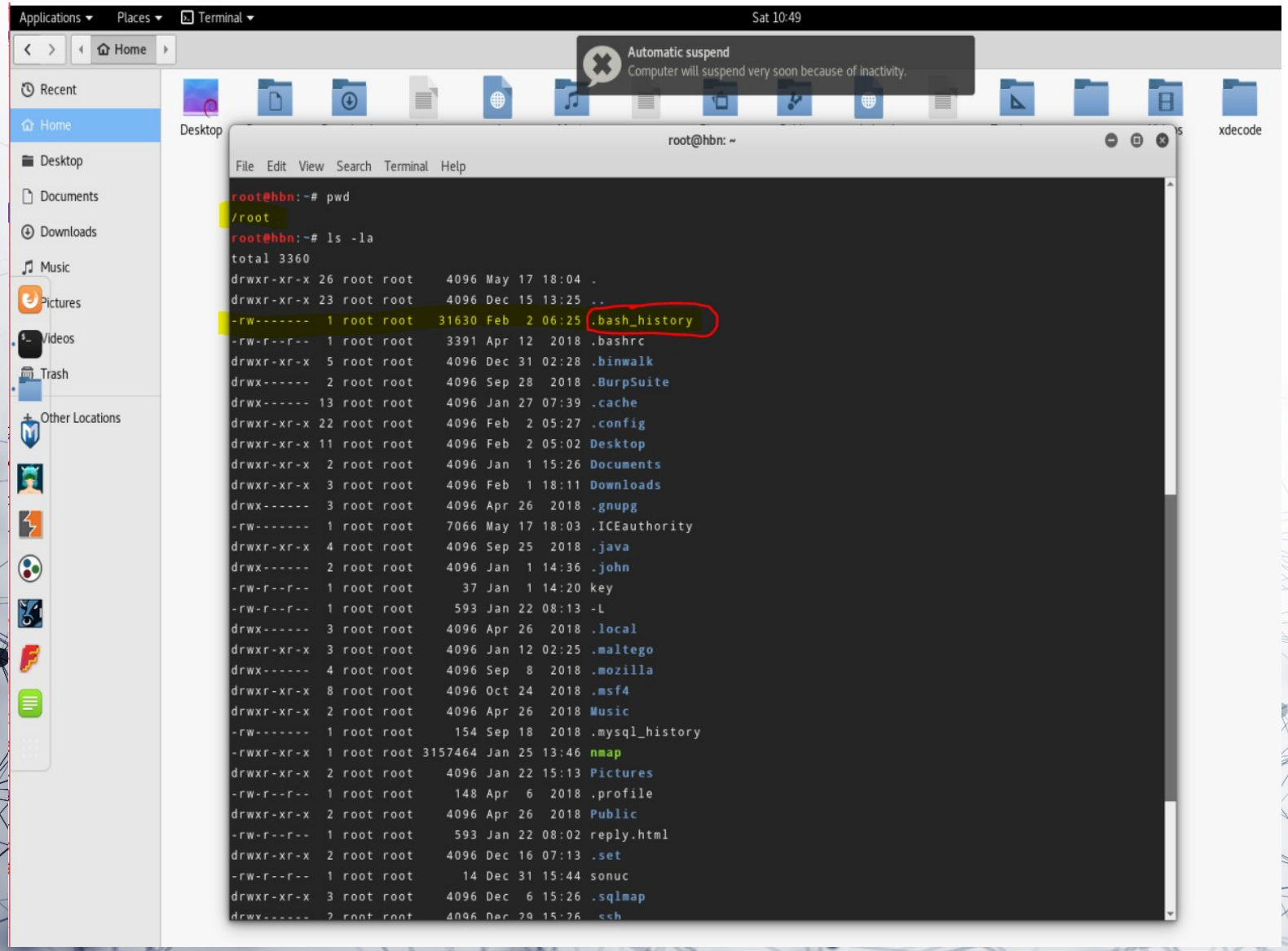
Linux işletim sistemi üzerine kullanıcı tarafından daha sonradan özel olarak yüklenen
ve kurulumları yapılan 3.parti yazılımların ve
sistem üzerine kurulan araçların neler olduğu
bilgisine aşağıdaki dosya yolunda tutulmakta
olan apt log dosyasından erişebiliriz.

Bilgiye Erişim Yolu :
/var/log/apt/history.log

Yüklenen Yazılım/Araç Bilgileri

History.log dosyasının içeriği aşağıdaki gibi görülmektedir.
Burada yazılımın yüklenme tarihi, saati gereksinimlerimizi ve sürümü bulunmaktadır.
Ayrıca ek olarak hangi komut kullanılarak indirildiği bilgiside bize gösterilmektedir.

Terminal Geçmişinin Analizi



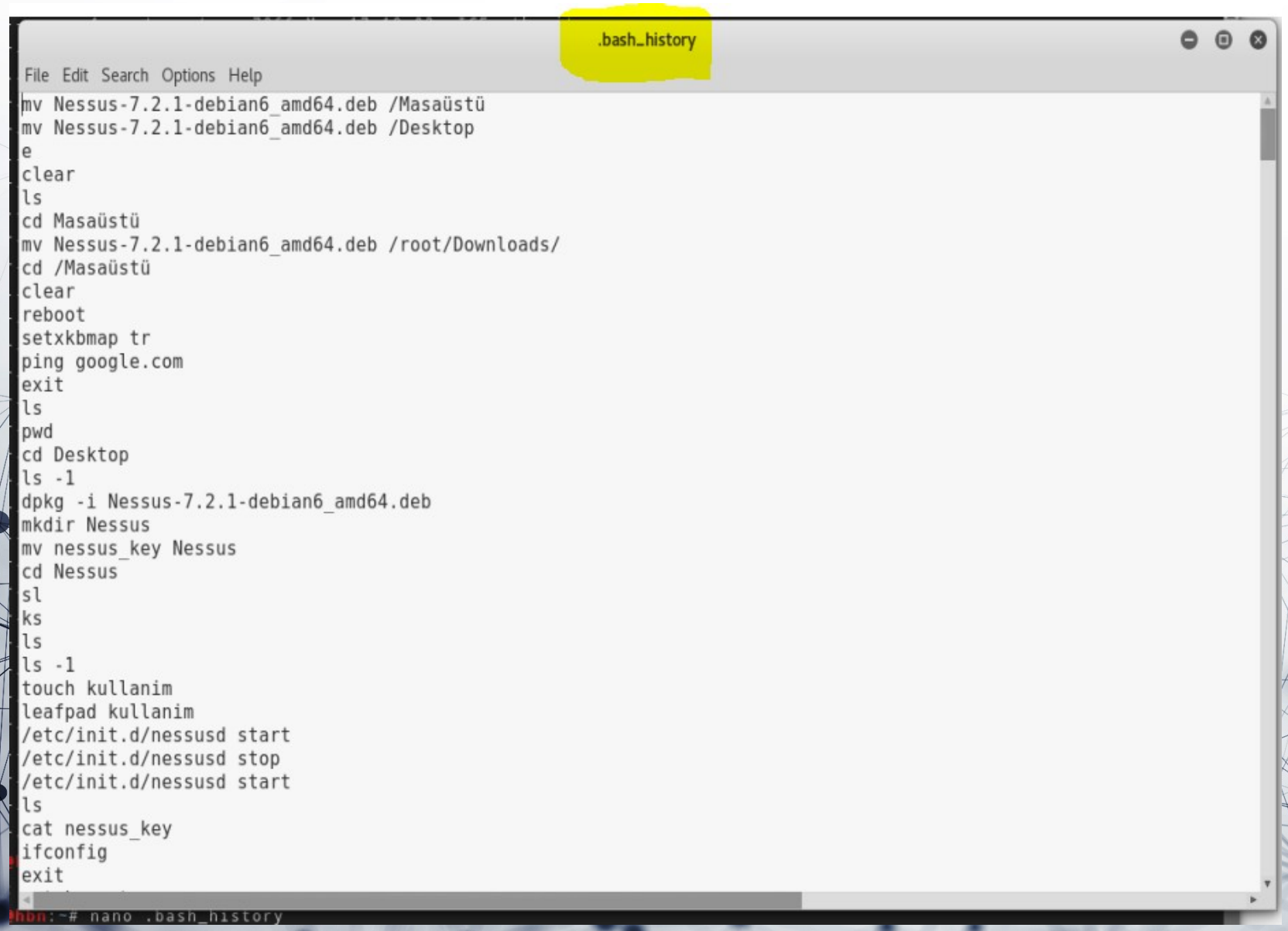
Sisteme yüklenen programların neler olduğunu öğrenebilmek için bir başka yolda bash history dosyasının analiz edilmesidir.

Bash_history dosyası Linux işletim sistemlerinde root dizini içerisinde gizli dosya olarak bulunmaktadır.

Root dizinine girdikten sonra ls –la komutunu kullanarak gizli dosyaları görebiliriz.
Bash_history dosyası Linux teminalde yazılan komutların geçmiş kayıtlarının tutulduğu dosyadır.

Kişinin terminalde yazdığı tüm komutları burada görebiliriz.

Bash_history Dosyasının İçeriği



Bilgiye Erişim Yolu

/ root/.bash_history

Uygulama Çalışma Kayıtları

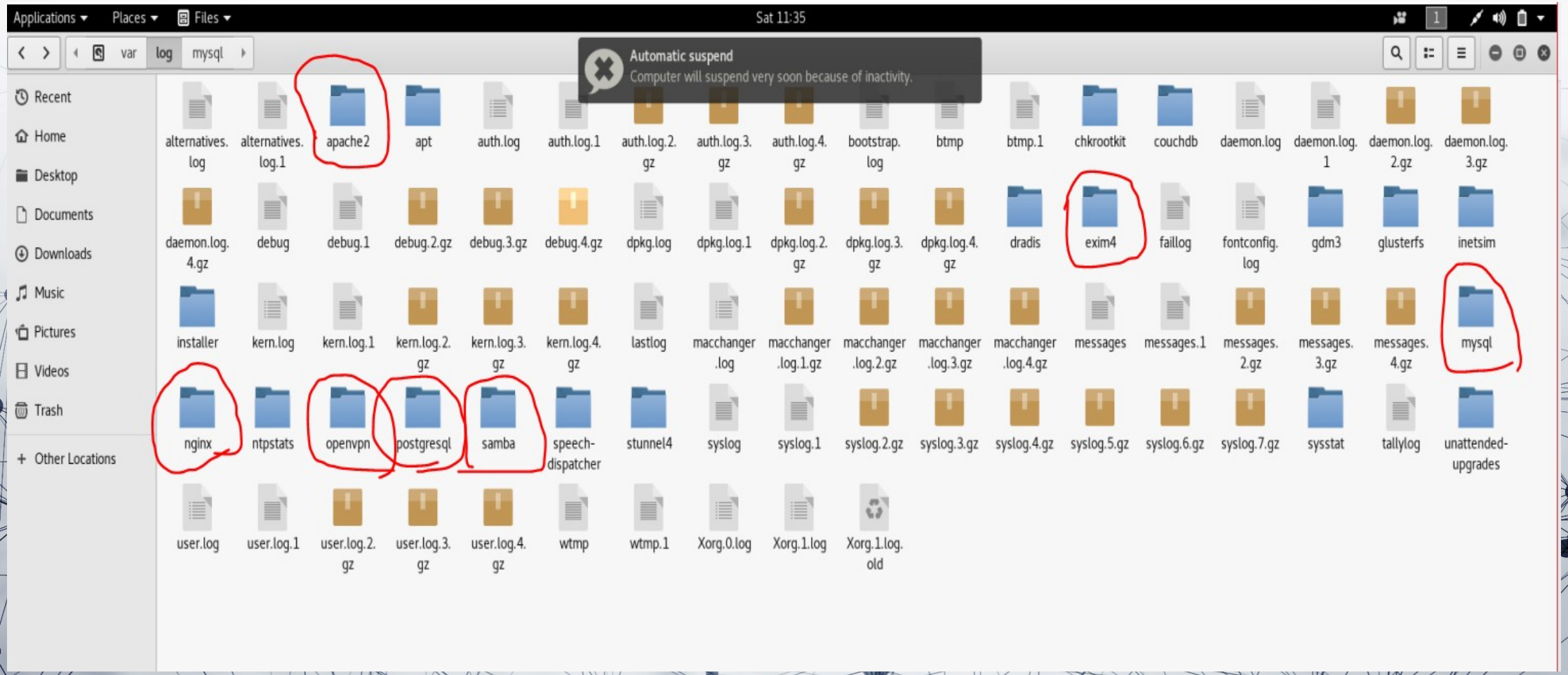
Linux sistemler gerekli uygulamaların yüklenmesiyle sunucu vb. yapılar olarak kullanılması sebebiyle kullanım alanlar ve yetkinlikleri daha fazladır.Bu bir avantajken bazı durumlarda kullanıcılar bunu dezavantaja dönüştürebilmektedir.

Böyle durumlarda sistem üzerinde kurulu olan uygulamaları tespit ettikten sonra uygulamaların çalışma zamanları, çalıştırılabilir yol bilgisi ve çalıştırılma sayılarına ulaşabiliriz.

Bilgi Edinme Yolu :

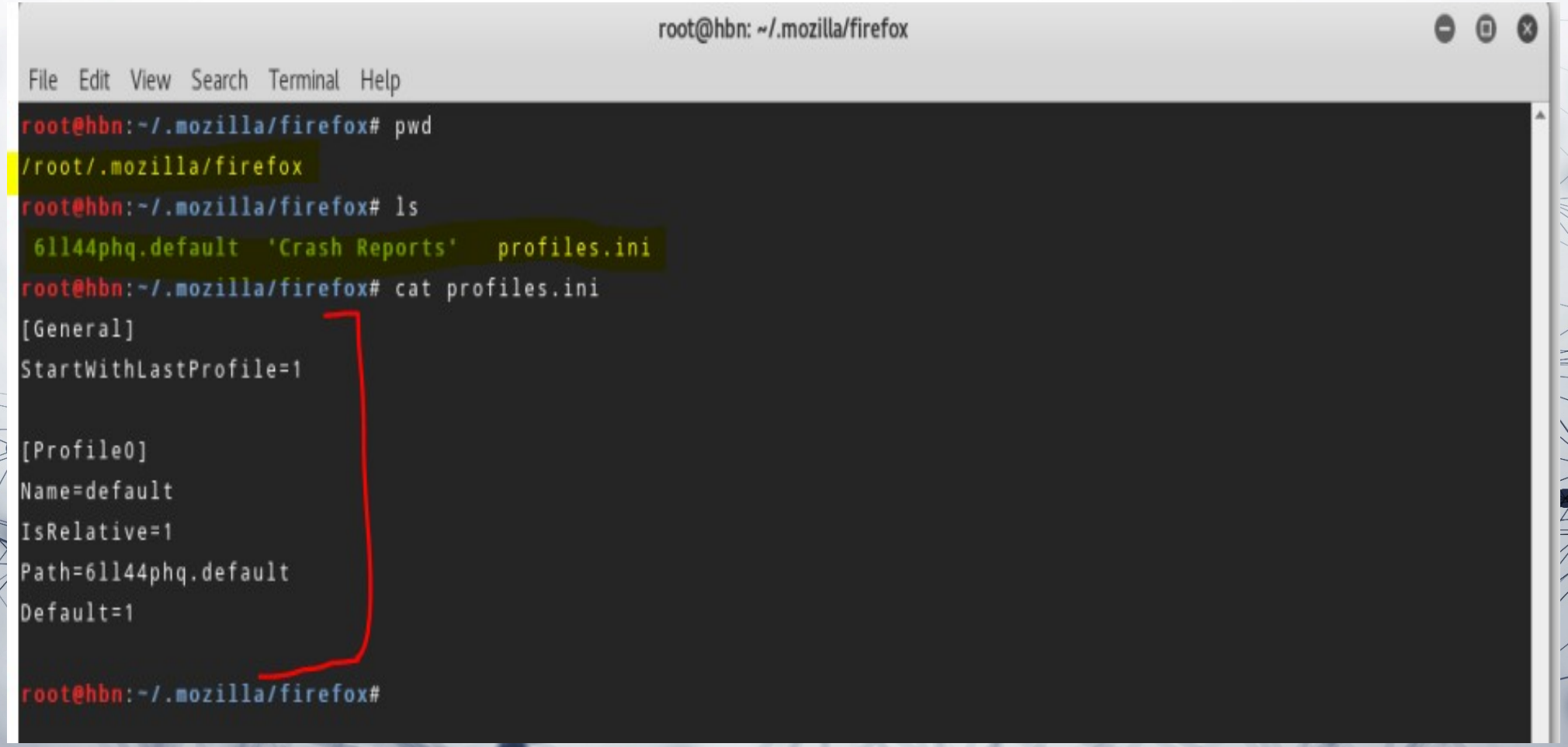
- Var/log/veil
- Var/log/mysql
- Var/log/apache2
- Var/log/exim4
- Var/log/apt
- Root/mozilla/firefox

Klasör Görünümü



Web Tarayıcı Bilgileri

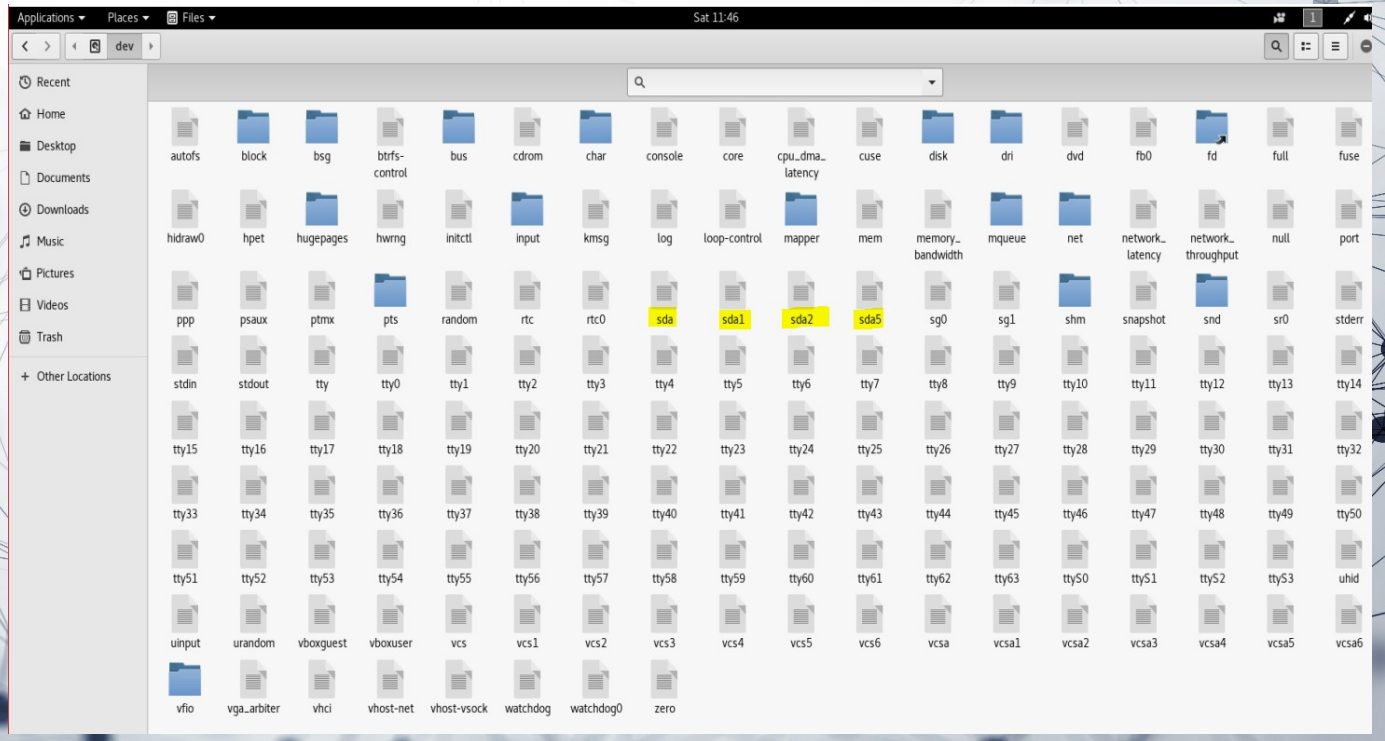
Bilgiye Erişim Yolu : /root/.mozilla/firefox/profiles.ini



Bilgisayara Bağlanan Harici Depolama Cihazları

Windows işletim sistemin de registry kayıtlarını analiz ederek ulaştığımız bu bilgiye Linux
sistem yapısının bize sunduğu kolaylık sayesinde doğrudan klasör erişimi yaparak ulaşabilmekteyiz.

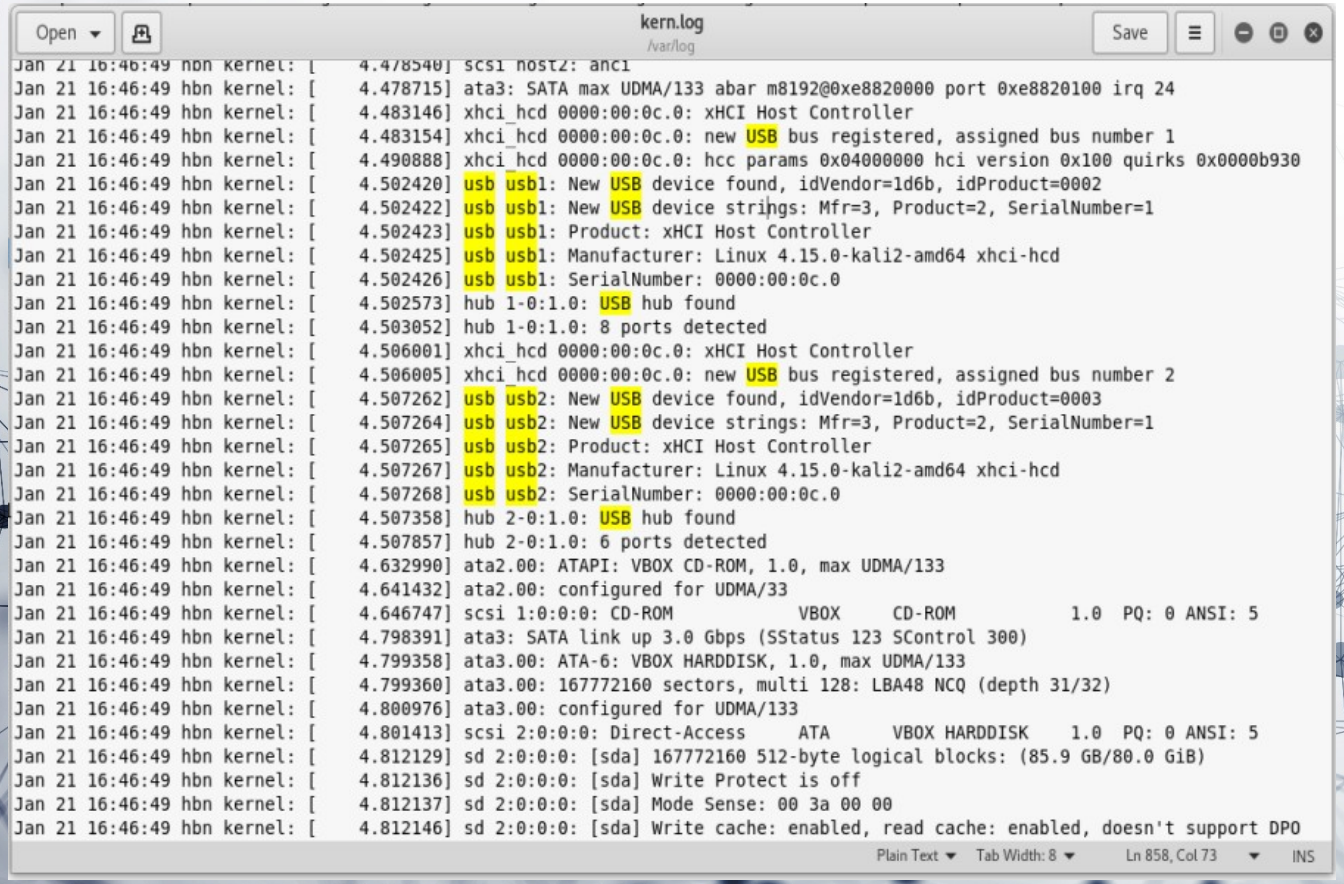
Bilgi Edinme Yolu : /dev/...



Kernel Logları

Bilgisayara takılan harici depolama aygıtlarını (usbdisk vb.) kernel log kayıtları analiz ederek tespit edebilmemiz de mümkündür.

Linux sistemlerde bilgisayara bir usb disk takıldığı zaman mutlaka
flash diskin bilgileri kernel loğlarına düşer yani kern.log dosyasına kayıt edilir.



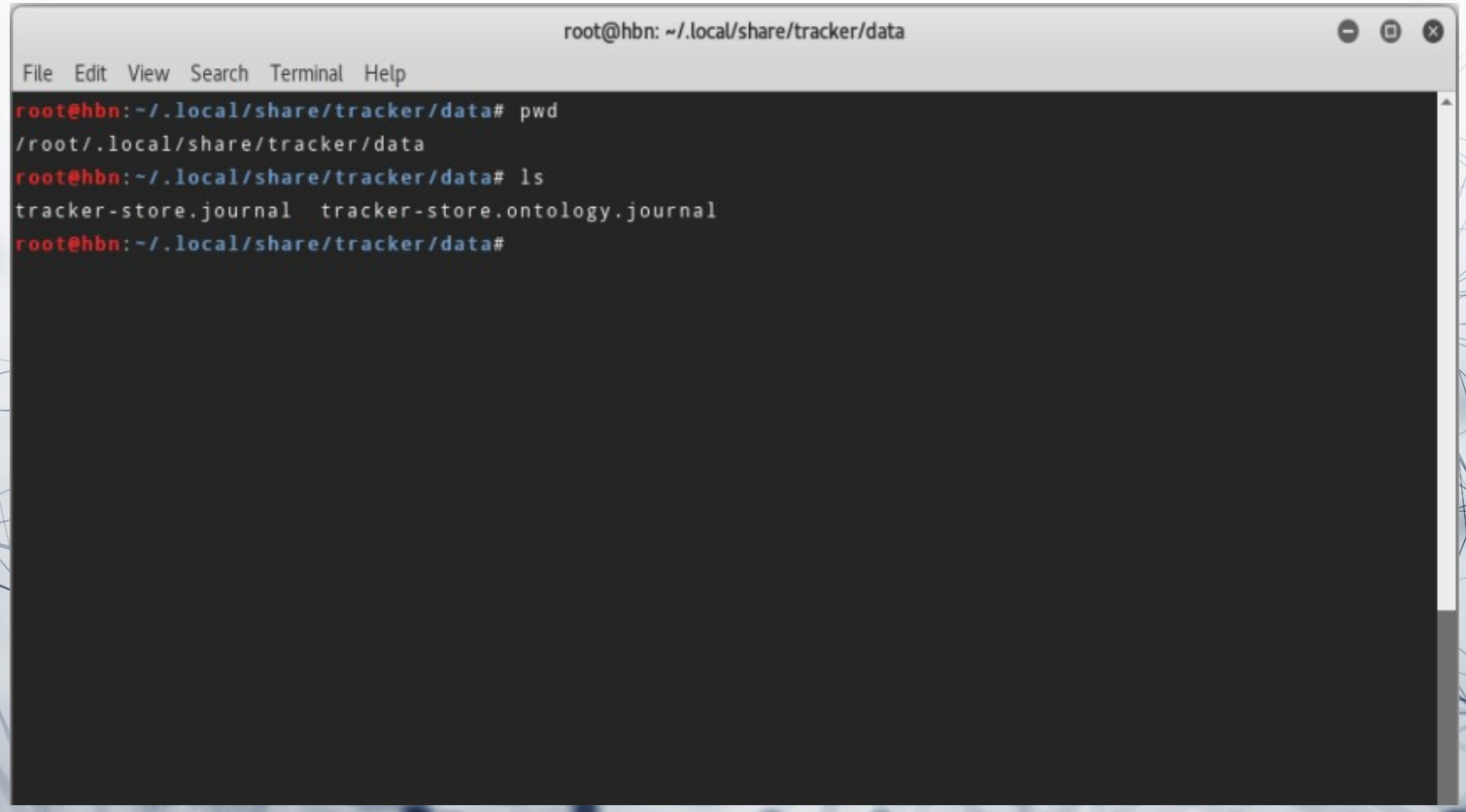
Bilgiye Erişim Yolu

/var/log/kern.log

Geridönüşüm / Çöp Dosyaları

İşletim sistemi içerisinde daha önceden bulunmakta olan sonradan kullanıcı tarafından silinen dosyalar ve klasörler hakkındaki bilgilere aşağıdaki journal dosyalarından ulaşabiliriz.

Bilgiye Erişim Yolu : /root/.local/share/tracer/data



TEŞEKKÜRLER

Fırat Üniversitesi
Adli Bilişim Mühendisliği

Hazırlayan : Hasan BASKIN