

Dosya Sistem Analizi

Linux İmaj İnceleme Çalışması

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

Linux Nedir ?

Linux, serbestçe dağıtılabilen, çok görevli, çok kullanıcıli 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 kullanıcıli 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, İerik ve Yöntem

- Dosya Sistem Dersi Proje ödevi için hazırlanan bu sunumda Linux işletim sistemine sahip olan bir bilgisayarın imajı manuel olarak «dd» alınmıştır. Daha sonra alınan bu imaj üzerinde hazır araçlar kullanılarak arařtırmalar 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 doğruluęu 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	<u>hbn_pc_imaj</u>
MD 5	008ace8b3902eb576c4defa49b5dd3f1
SHA-1	129da75a5daa7e4220228d23456f1271f5560fef
Yazılım Bilgisi	<u>Autopsy 4.9.0</u>
İmaj Formatı	E01 (<u>Expert Witness Compression Format</u>) <u>Vmdk</u> dosyasından dönüştürülmüş
Sıkıştırma	Orta (<u>Compression = 6</u>)
Sektör / <u>Byte</u>	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 kořan işletim sistemi ve root kullanıcı Bilgilerini ařağıdaki gibi görmekteyiz.

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

- **Bilgisayardaki İşletim Sistemi Bilgileri**

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

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

İmaji 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
<u>hbn</u>	<u>Id=0</u>	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.

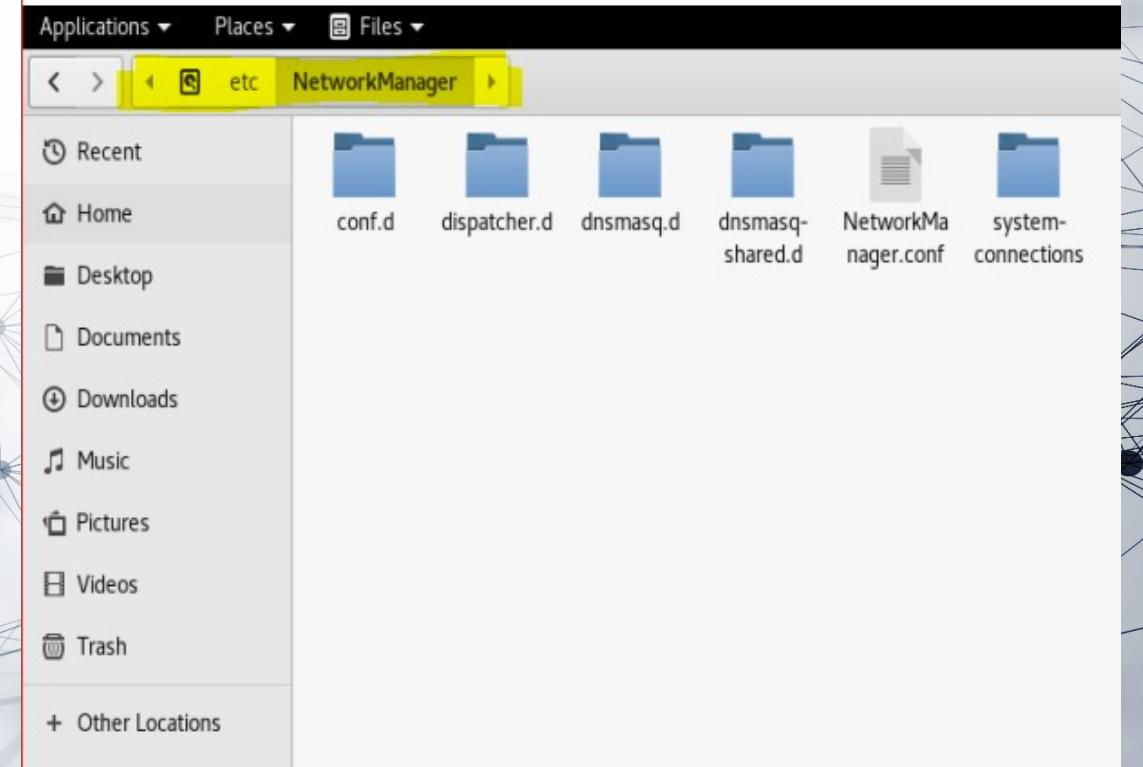
```
Applications ▾ Places ▾ Text Editor ▾ Sat 07:57
Open ▾ auth.log
/var/log
Jan 21 15:05:01 hbn CRON[1902]: pam_unix(cron:session): session opened for user root by (uid=0)
Jan 21 15:05:01 hbn CRON[1902]: pam_unix(cron:session): session closed for user root
Jan 21 15:09:01 hbn CRON[1907]: pam_unix(cron:session): session opened for user root by (uid=0)
Jan 21 15:09:01 hbn CRON[1907]: pam_unix(cron:session): session closed for user root
Jan 21 15:15:01 hbn CRON[1923]: pam_unix(cron:session): session opened for user root by (uid=0)
Jan 21 15:15:01 hbn CRON[1923]: pam_unix(cron:session): session closed for user root
Jan 21 15:17:01 hbn CRON[1926]: pam_unix(cron:session): session opened for user root by (uid=0)
Jan 21 15:17:01 hbn CRON[1926]: pam_unix(cron:session): session closed for user root
Jan 21 15:25:01 hbn CRON[1946]: pam_unix(cron:session): session opened for user root by (uid=0)
Jan 21 15:25:01 hbn CRON[1946]: pam_unix(cron:session): session closed for user root
Jan 21 15:35:01 hbn CRON[1965]: pam_unix(cron:session): session opened for user root by (uid=0)
Jan 21 15:35:01 hbn CRON[1965]: pam_unix(cron:session): session closed for user root
Jan 21 15:39:01 hbn CRON[1980]: pam_unix(cron:session): session opened for user root by (uid=0)
Jan 21 15:39:01 hbn CRON[1980]: pam_unix(cron:session): session closed for user root
Jan 21 15:45:01 hbn CRON[1984]: pam_unix(cron:session): session opened for user root by (uid=0)
Jan 21 15:45:01 hbn CRON[1984]: pam_unix(cron:session): session closed for user root
Jan 21 15:55:01 hbn CRON[2001]: pam_unix(cron:session): session opened for user root by (uid=0)
Jan 21 15:55:01 hbn CRON[2001]: pam_unix(cron:session): session closed for user root
Jan 21 16:05:01 hbn CRON[2073]: pam_unix(cron:session): session opened for user root by (uid=0)
Jan 21 16:05:01 hbn CRON[2073]: pam_unix(cron:session): session closed for user root
Jan 21 16:08:47 hbn systemd-logind[447]: System is powering down.
Jan 21 16:11:35 hbn systemd-logind[462]: New seat seat0.
Jan 21 16:11:35 hbn systemd-logind[462]: Watching system buttons on /dev/input/event4 (Power Button)
Jan 21 16:11:35 hbn systemd-logind[462]: Watching system buttons on /dev/input/event5 (Sleep Button)
```

Ağ Bağlantı Bilgileri

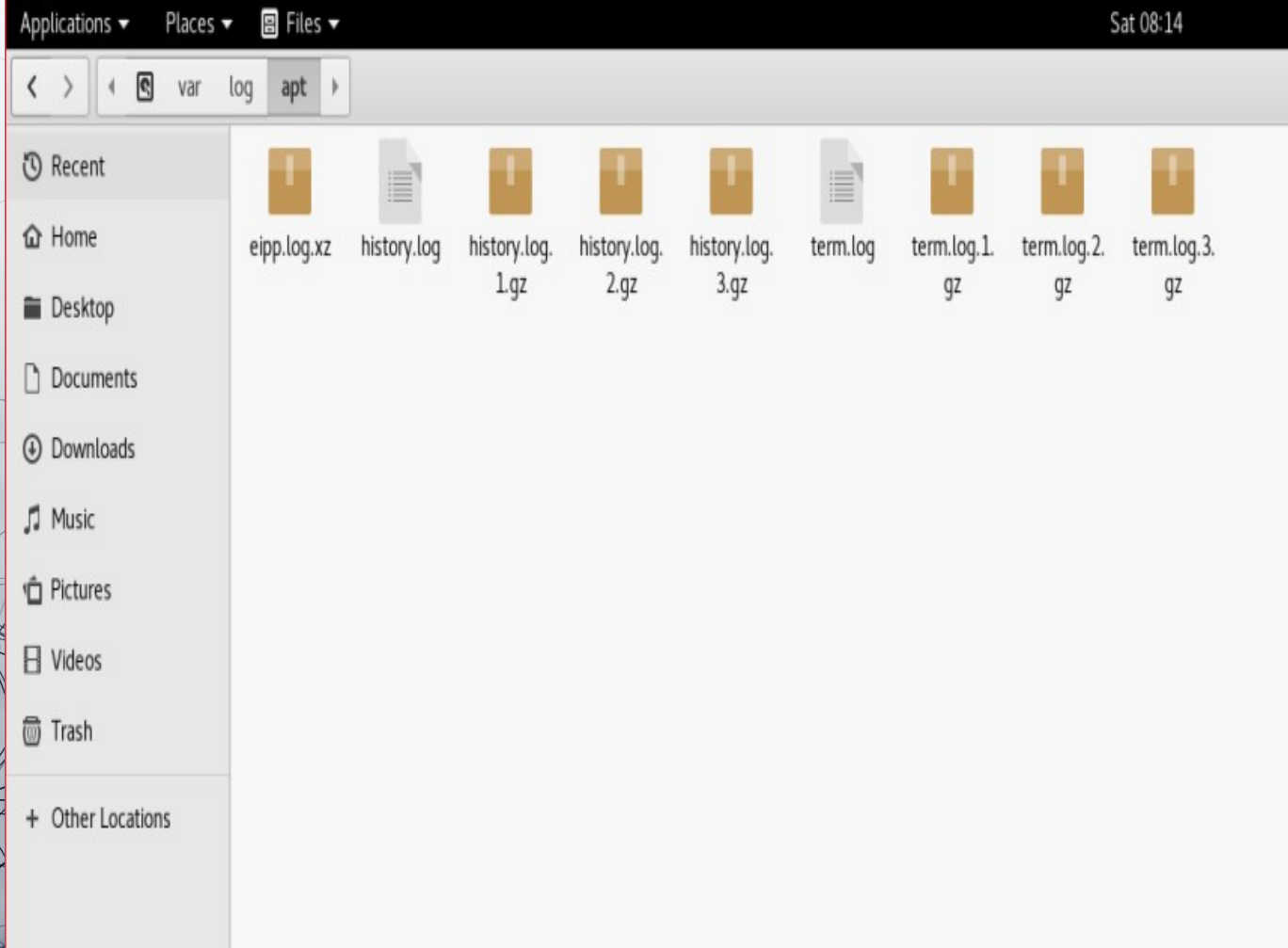
Windows işletim sistemi Registry Kayıtlarından elde ettiğimiz, ilgili bilgisayarın **geçmiş ağ bağlantı kayıtlarını** Linux işletim sisteminde aşağıda belirtilen dosya yolunda bulabilmekteyiz.

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

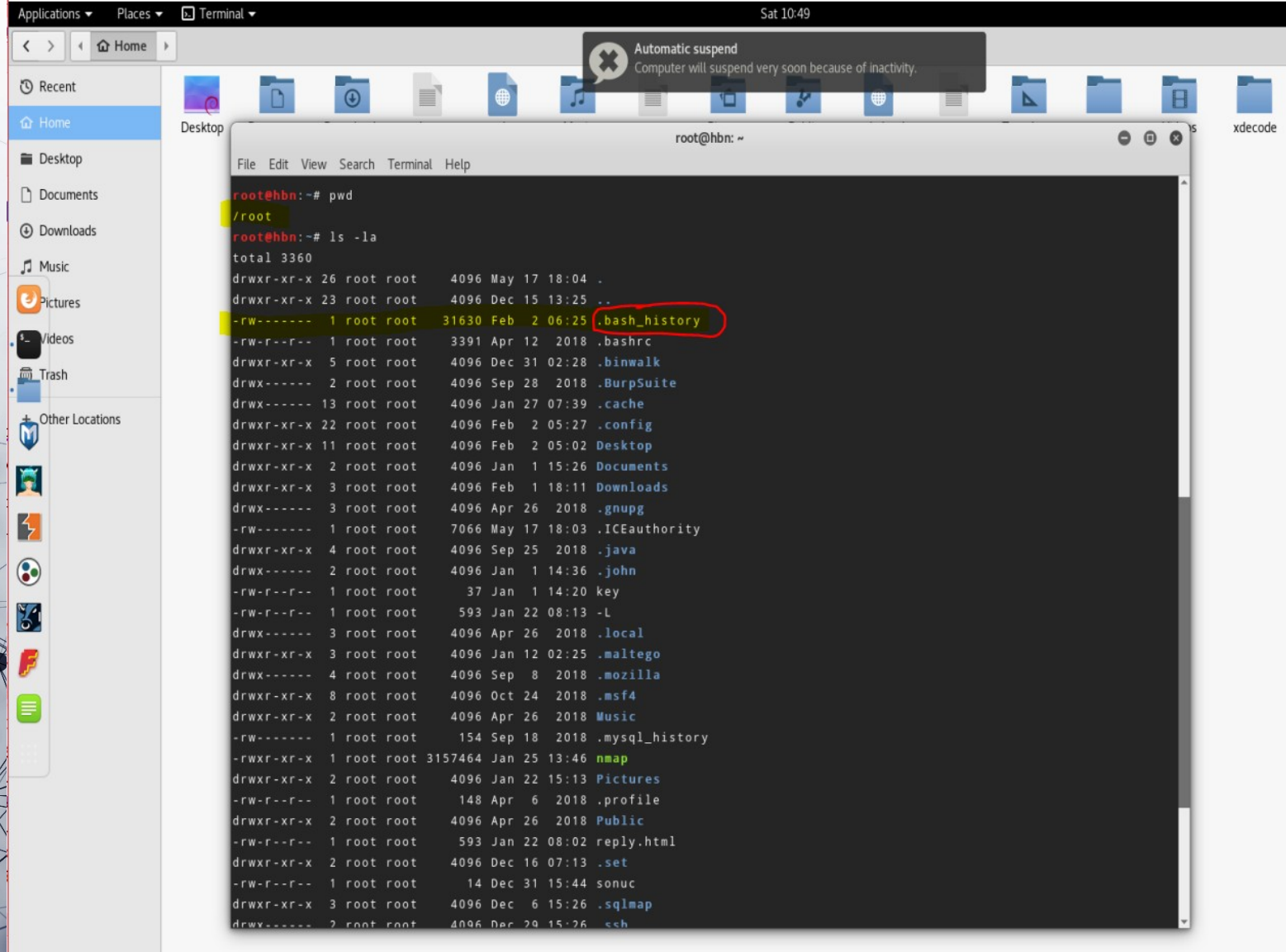
History.log dosyasının içeriği aşağıdaki gibi görülmektedir. Burada yazılımın yüklenme tarihi, saati gereksinimlerimizi ve sürümü bulunmaktadır. Ayrıca ek olarak hangi komut kullanılarak indirildiği bilgiside bize gösterilmektedir.

```
Applications ▾ Places ▾ Text Editor ▾ Sat 08:15
history.log
/var/log/apt
Save

Start-Date: 2019-02-01 17:18:22
Commandline: apt-get install xplico
Install: libsox3:amd64 (14.4.2-3, automatic), libndpi4:amd64 (1.8-1, automatic), php-sqlite3:amd64 (2:7.3+69, automatic), libsox-fmt-alsa:amd64 (14.4.2-3, automatic), php7.3-sqlite3:amd64 (7.3.1-1, automatic), librecode0:amd64 (3.6-23, automatic), php7.3-common:amd64 (7.3.1-1, automatic), sox:amd64 (14.4.2-3, automatic), recode:amd64 (3.6-23, automatic), xplico:amd64 (1.2.1-0kali3), libsox-fmt-base:amd64 (14.4.2-3, automatic), lame:amd64 (3.100-2+b1, automatic)
End-Date: 2019-02-01 17:19:03

Start-Date: 2019-02-01 17:26:06
Commandline: apt-get install mimikatz
Upgrade: mimikatz:amd64 (2.1.1-20180325-0kali1, 2.1.1-20181209-0kali1)
End-Date: 2019-02-01 17:26:07
```

Terminal Geçmişinin Analizi



```
root@hbn:~# pwd
/root
root@hbn:~# ls -la
total 3360
drwxr-xr-x 26 root root 4096 May 17 18:04 .
drwxr-xr-x 23 root root 4096 Dec 15 13:25 ..
-rw-r--r-- 1 root root 31630 Feb 2 06:25 .bash_history
-rw-r--r-- 1 root root 3391 Apr 12 2018 .bashrc
drwxr-xr-x 5 root root 4096 Dec 31 02:28 .binwalk
drwxr-xr-x 2 root root 4096 Sep 28 2018 .BurpSuite
drwxr-xr-x 13 root root 4096 Jan 27 07:39 .cache
drwxr-xr-x 22 root root 4096 Feb 2 05:27 .config
drwxr-xr-x 11 root root 4096 Feb 2 05:02 Desktop
drwxr-xr-x 2 root root 4096 Jan 1 15:26 Documents
drwxr-xr-x 3 root root 4096 Feb 1 18:11 Downloads
drwxr-xr-x 3 root root 4096 Apr 26 2018 .gnupg
-rw-r--r-- 1 root root 7066 May 17 18:03 .ICEauthority
drwxr-xr-x 4 root root 4096 Sep 25 2018 .java
drwxr-xr-x 2 root root 4096 Jan 1 14:36 .john
-rw-r--r-- 1 root root 37 Jan 1 14:20 key
-rw-r--r-- 1 root root 593 Jan 22 08:13 -L
drwxr-xr-x 3 root root 4096 Apr 26 2018 .local
drwxr-xr-x 3 root root 4096 Jan 12 02:25 .maltego
drwxr-xr-x 4 root root 4096 Sep 8 2018 .mozilla
drwxr-xr-x 8 root root 4096 Oct 24 2018 .msf4
drwxr-xr-x 2 root root 4096 Apr 26 2018 Music
-rw-r--r-- 1 root root 154 Sep 18 2018 .mysql_history
-rw-r-xr-x 1 root root 3157464 Jan 25 13:46 nmap
drwxr-xr-x 2 root root 4096 Jan 22 15:13 Pictures
-rw-r--r-- 1 root root 148 Apr 6 2018 .profile
drwxr-xr-x 2 root root 4096 Apr 26 2018 Public
-rw-r--r-- 1 root root 593 Jan 22 08:02 reply.html
drwxr-xr-x 2 root root 4096 Dec 16 07:13 .set
-rw-r--r-- 1 root root 14 Dec 31 15:44 sonuc
drwxr-xr-x 3 root root 4096 Dec 6 15:26 .sqlmap
drwxr-xr-x 2 root root 4096 Dec 29 15:26 ssh
```

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 terminalde yazılan komutların geçmiş kayıtlarının tutulduğu dosyadır.

Kişinin terminalde yazdığı tüm komutları burada görebiliriz.

Bash_history Dosyasının İçeriği

```
.bash_history
File Edit Search Options Help
mv Nessus-7.2.1-debian6_amd64.deb /Masaüstü
mv Nessus-7.2.1-debian6_amd64.deb /Desktop
e
clear
ls
cd Masaüstü
mv Nessus-7.2.1-debian6_amd64.deb /root/Downloads/
cd /Masaüstü
clear
reboot
setxkbmap tr
ping google.com
exit
ls
pwd
cd Desktop
ls -l
dpkg -i Nessus-7.2.1-debian6_amd64.deb
mkdir Nessus
mv nessus_key Nessus
cd Nessus
sl
ks
ls
ls -l
touch kullanim
leafpad kullanim
/etc/init.d/nessusd start
/etc/init.d/nessusd stop
/etc/init.d/nessusd start
ls
cat nessus_key
ifconfig
exit
root:~# nano .bash_history
```

Bilgiye Erişim
Yolu

/
/
root/.bash_histor
y

Uygulama Çalışma Kayıtları

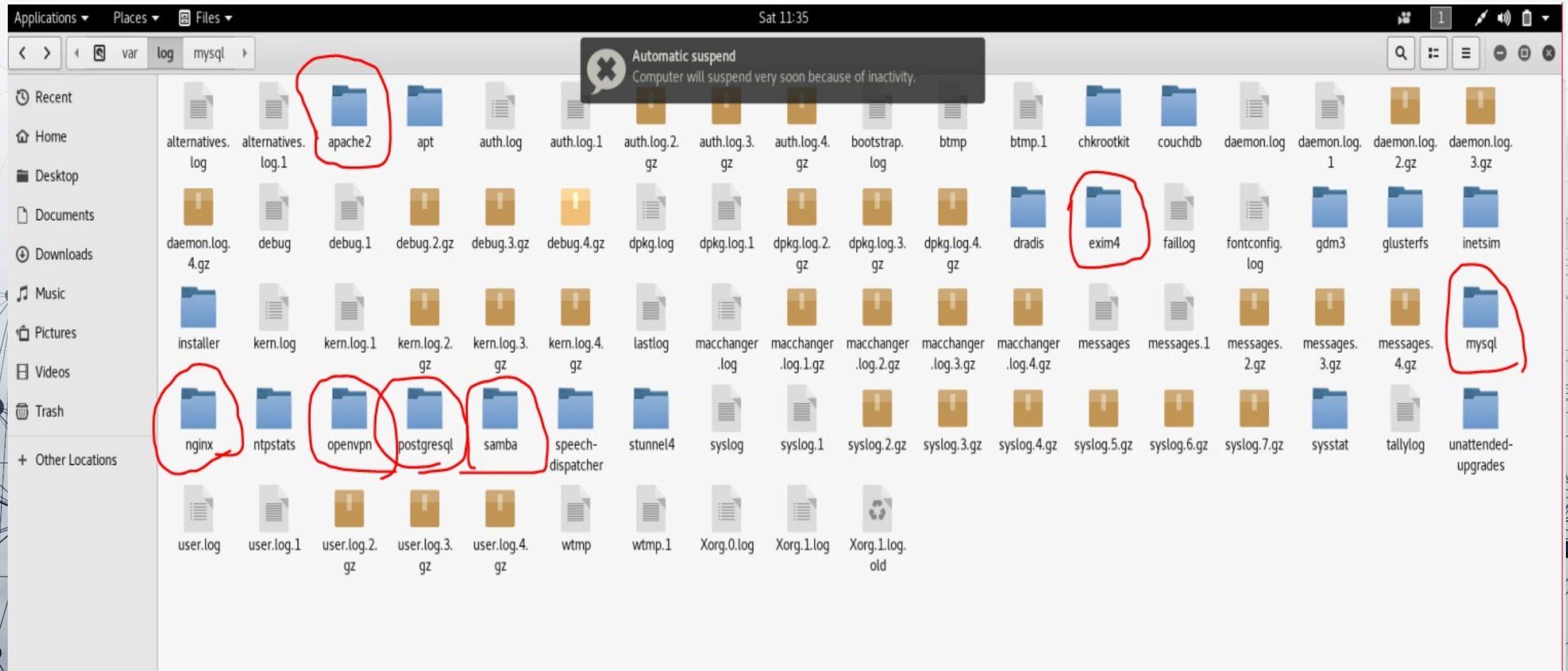
Linux sistemler gerekli uygulamaların yüklenmesiyle sunucu vb. yapılar olarak kullanılması sebebiyle kullanım alanlar ve yetkinlikleri daha fazladır. Bu bir avantajken bazı durumlarda kullanıcılar bunu dezavantaja dönüştürebilmektedir.

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`

```
root@hbn: ~/.mozilla/firefox
File Edit View Search Terminal Help
root@hbn:~/.mozilla/firefox# pwd
/root/.mozilla/firefox
root@hbn:~/.mozilla/firefox# ls
61144phq.default 'Crash Reports' profiles.ini
root@hbn:~/.mozilla/firefox# cat profiles.ini
[General]
StartWithLastProfile=1

[Profile0]
Name=default
IsRelative=1
Path=61144phq.default
Default=1
root@hbn:~/.mozilla/firefox#
```


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 loglarına düşer yani kern.log dosyasına kayıt edilir.

```
Open kern.log Save
Jan 21 16:46:49 non kernel: [ 4.478540] scsi nost2: anci
Jan 21 16:46:49 hbn kernel: [ 4.478715] ata3: SATA max UDMA/133 abar m8192@0xe8820000 port 0xe8820100 irq 24
Jan 21 16:46:49 hbn kernel: [ 4.483146] xhci_hcd 0000:00:0c.0: xHCI Host Controller
Jan 21 16:46:49 hbn kernel: [ 4.483154] xhci_hcd 0000:00:0c.0: new USB bus registered, assigned bus number 1
Jan 21 16:46:49 hbn kernel: [ 4.490888] xhci_hcd 0000:00:0c.0: hcc params 0x04000000 hci version 0x100 quirks 0x0000b930
Jan 21 16:46:49 hbn kernel: [ 4.502420] usb usb1: New USB device found, idVendor=1d6b, idProduct=0002
Jan 21 16:46:49 hbn kernel: [ 4.502422] usb usb1: New USB device strings: Mfr=3, Product=2, SerialNumber=1
Jan 21 16:46:49 hbn kernel: [ 4.502423] usb usb1: Product: xHCI Host Controller
Jan 21 16:46:49 hbn kernel: [ 4.502425] usb usb1: Manufacturer: Linux 4.15.0-kali2-amd64 xhci-hcd
Jan 21 16:46:49 hbn kernel: [ 4.502426] usb usb1: SerialNumber: 0000:00:0c.0
Jan 21 16:46:49 hbn kernel: [ 4.502573] hub 1-0:1.0: USB hub found
Jan 21 16:46:49 hbn kernel: [ 4.503052] hub 1-0:1.0: 8 ports detected
Jan 21 16:46:49 hbn kernel: [ 4.506001] xhci_hcd 0000:00:0c.0: xHCI Host Controller
Jan 21 16:46:49 hbn kernel: [ 4.506005] xhci_hcd 0000:00:0c.0: new USB bus registered, assigned bus number 2
Jan 21 16:46:49 hbn kernel: [ 4.507262] usb usb2: New USB device found, idVendor=1d6b, idProduct=0003
Jan 21 16:46:49 hbn kernel: [ 4.507264] usb usb2: New USB device strings: Mfr=3, Product=2, SerialNumber=1
Jan 21 16:46:49 hbn kernel: [ 4.507265] usb usb2: Product: xHCI Host Controller
Jan 21 16:46:49 hbn kernel: [ 4.507267] usb usb2: Manufacturer: Linux 4.15.0-kali2-amd64 xhci-hcd
Jan 21 16:46:49 hbn kernel: [ 4.507268] usb usb2: SerialNumber: 0000:00:0c.0
Jan 21 16:46:49 hbn kernel: [ 4.507358] hub 2-0:1.0: USB hub found
Jan 21 16:46:49 hbn kernel: [ 4.507857] hub 2-0:1.0: 6 ports detected
Jan 21 16:46:49 hbn kernel: [ 4.632990] ata2.00: ATAPI: VBOX CD-ROM, 1.0, max UDMA/133
Jan 21 16:46:49 hbn kernel: [ 4.641432] ata2.00: configured for UDMA/33
Jan 21 16:46:49 hbn kernel: [ 4.646747] scsi 1:0:0:0: CD-ROM VBOX CD-ROM 1.0 PQ: 0 ANSI: 5
Jan 21 16:46:49 hbn kernel: [ 4.798391] ata3: SATA link up 3.0 Gbps (SStatus 123 SControl 300)
Jan 21 16:46:49 hbn kernel: [ 4.799358] ata3.00: ATA-6: VBOX HARDDISK, 1.0, max UDMA/133
Jan 21 16:46:49 hbn kernel: [ 4.799360] ata3.00: 167772160 sectors, multi 128: LBA48 NCQ (depth 31/32)
Jan 21 16:46:49 hbn kernel: [ 4.800976] ata3.00: configured for UDMA/133
Jan 21 16:46:49 hbn kernel: [ 4.801413] scsi 2:0:0:0: Direct-Access ATA VBOX HARDDISK 1.0 PQ: 0 ANSI: 5
Jan 21 16:46:49 hbn kernel: [ 4.812129] sd 2:0:0:0: [sda] 167772160 512-byte logical blocks: (85.9 GB/80.0 GiB)
Jan 21 16:46:49 hbn kernel: [ 4.812136] sd 2:0:0:0: [sda] Write Protect is off
Jan 21 16:46:49 hbn kernel: [ 4.812137] sd 2:0:0:0: [sda] Mode Sense: 00 3a 00 00
Jan 21 16:46:49 hbn kernel: [ 4.812146] sd 2:0:0:0: [sda] Write cache: enabled, read cache: enabled, doesn't support DPO
Plain Text Tab Width: 8 Ln 858, Col 73 INS
```

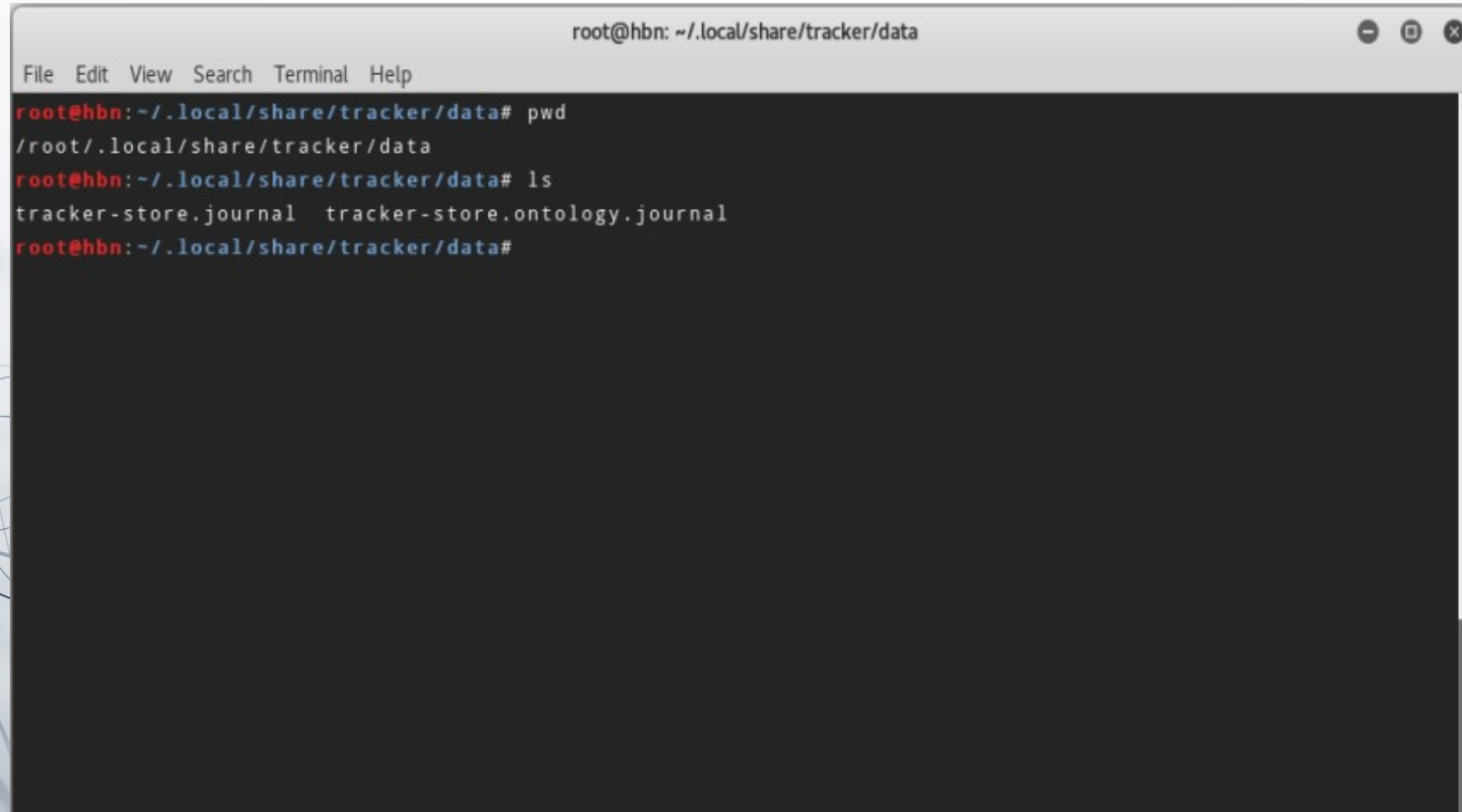
Bilgiye Erişim Yolu

/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



```
root@hbn: ~/.local/share/tracer/data
File Edit View Search Terminal Help
root@hbn:~/.local/share/tracer/data# pwd
/root/.local/share/tracer/data
root@hbn:~/.local/share/tracer/data# ls
tracker-store.journal  tracker-store.ontology.journal
root@hbn:~/.local/share/tracer/data#
```

TEŞEKKÜRLER

Fırat Üniversitesi
Adli Bilişim Mühendisliği

Hazırlayan : Hasan BASKIN