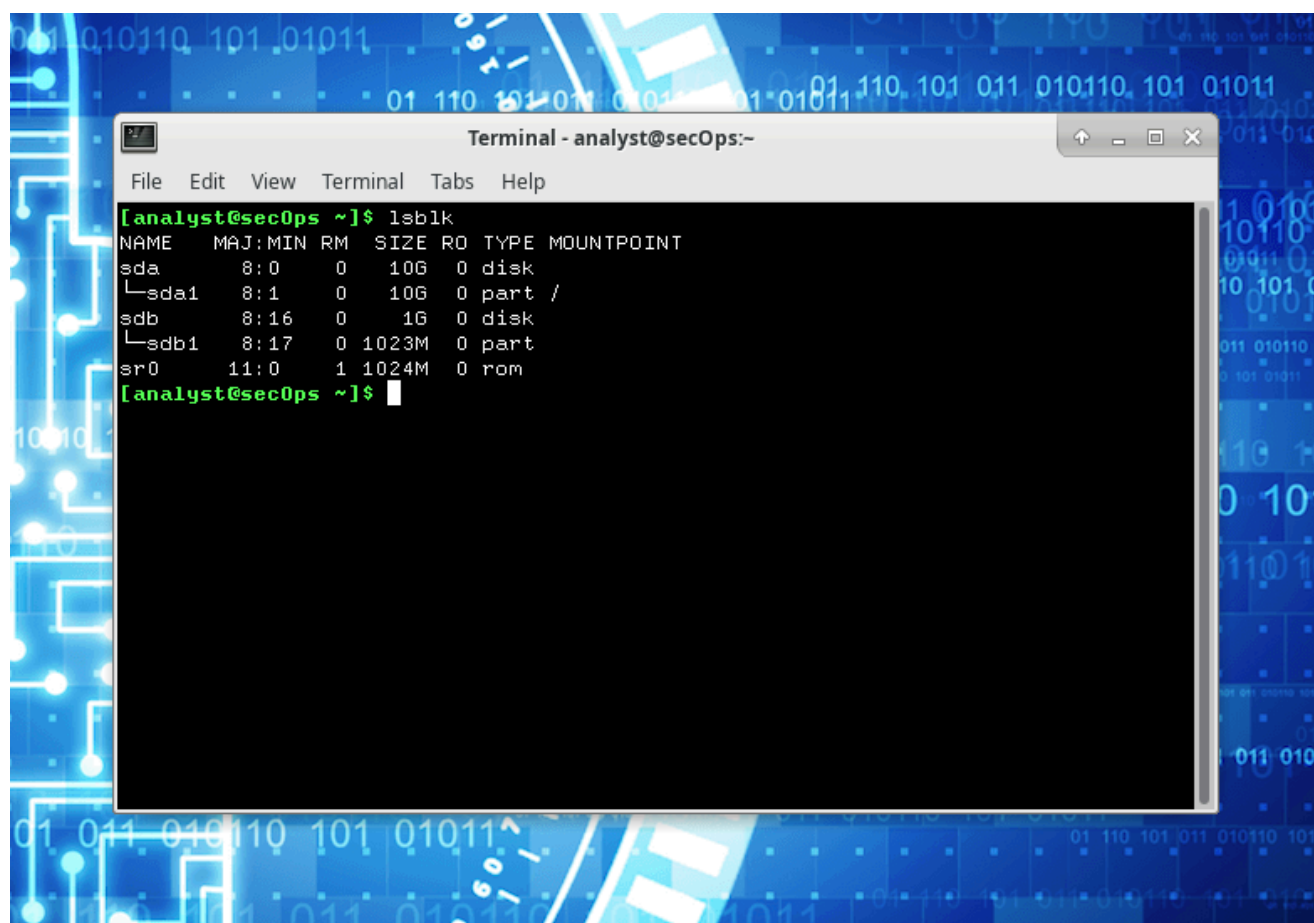


# BW3 es.3 Navigazione del File System di Linux

## Introduzione al Comando lsblk - Introduction to the lsblk Command

🌟 Tag: [#lsblk](#) [#filesystem](#) [#linux](#)

Il comando `lsblk`, abbreviazione di "list block devices", è usato per mostrare i dispositivi di blocco, come dischi rigidi, SSD e unità USB, visualizzando una tabella di informazioni su ciascun dispositivo.



The screenshot shows a terminal window titled "Terminal - analyst@secOps:~". The user has entered the command `lsblk`. The output is a table of block devices:

NAME	MAJ:MIN	RM	SIZE	RO	TYPE	MOUNTPOINT
sda	8:0	0	10G	0	disk	
└─sda1	8:1	0	10G	0	part	/
sdb	8:16	0	1G	0	disk	
└─sdb1	8:17	0	1023M	0	part	
sr0	11:0	1	1024M	0	rom	

The prompt `[analyst@secOps ~]$` is visible at the bottom of the terminal window.

---

## Dettagli del Comando lsblk - lsblk Command Details



Tag:

#comando\_lsblk

#dispositivi\_blocco

#informazioni\_dispositivo

### 1. Definizione:

- `lsblk` significa "list block devices" e mostra una lista di dispositivi di blocco presenti nel sistema.

### 2. Funzione:

- Il comando visualizza una tabella dettagliata, che include **nome, dimensione, tipo e punto di montaggio** di ogni dispositivo.

---

## Informazioni sul Filesystem - Filesystem Information



Tag:

#filesystem

#punti\_montaggio

#tipi\_filesystem

1. **Filesystem Montati:** Ogni riga rappresenta un filesystem montato, indicando l'origine e il punto di accesso nel sistema.

### 2. Tipi di Filesystem:

- **proc:** Fornisce informazioni sui processi di sistema.
- **tmpfs:** Memoria temporanea in RAM.
- **ext4:** Usato comunemente per dischi fisici.

### 3. Obiettivo:

- Familiarizzare con i filesystem e comprendere dove vengono "montati" per l'uso nel sistema.

```
[2]+  Exit 127                  Wireshark: ninda.download.pcap
[analyst@sec0ps pcaps]$ cd /home/analyst
[analyst@sec0ps ~]$ ls -l
total 368
drwxr-xr-x 2 analyst analyst 4096 Mar 22  2018 Desktop
drwxr-xr-x 3 analyst analyst 4096 Mar 22  2018 Downloads
-rw-r--r-- 1 analyst analyst  9 Oct 28 06:46 file1new.txt
lrwxrwxrwx 1 analyst analyst  9 Oct 28 06:47 file1symbolic -> file1.txt
-rw-r--r-- 2 analyst analyst  5 Oct 28 06:46 file2hard
-rw-r--r-- 2 analyst analyst  5 Oct 28 06:46 file2new.txt
drwxr-xr-x 9 analyst analyst 4096 Jul 19  2018 lab.support.files
drwxr-xr-x 3 root    root    4096 Mar 26  2018 second_drive
-rw-r--r-- 1 analyst analyst 345088 Oct 28 07:29 W32.Nimda.Amm.exe
[analyst@sec0ps ~]$ file W32.Nimda.Amm.exe
W32.Nimda.Amm.exe: PE32+ executable (console) x86-64, for MS Windows
```

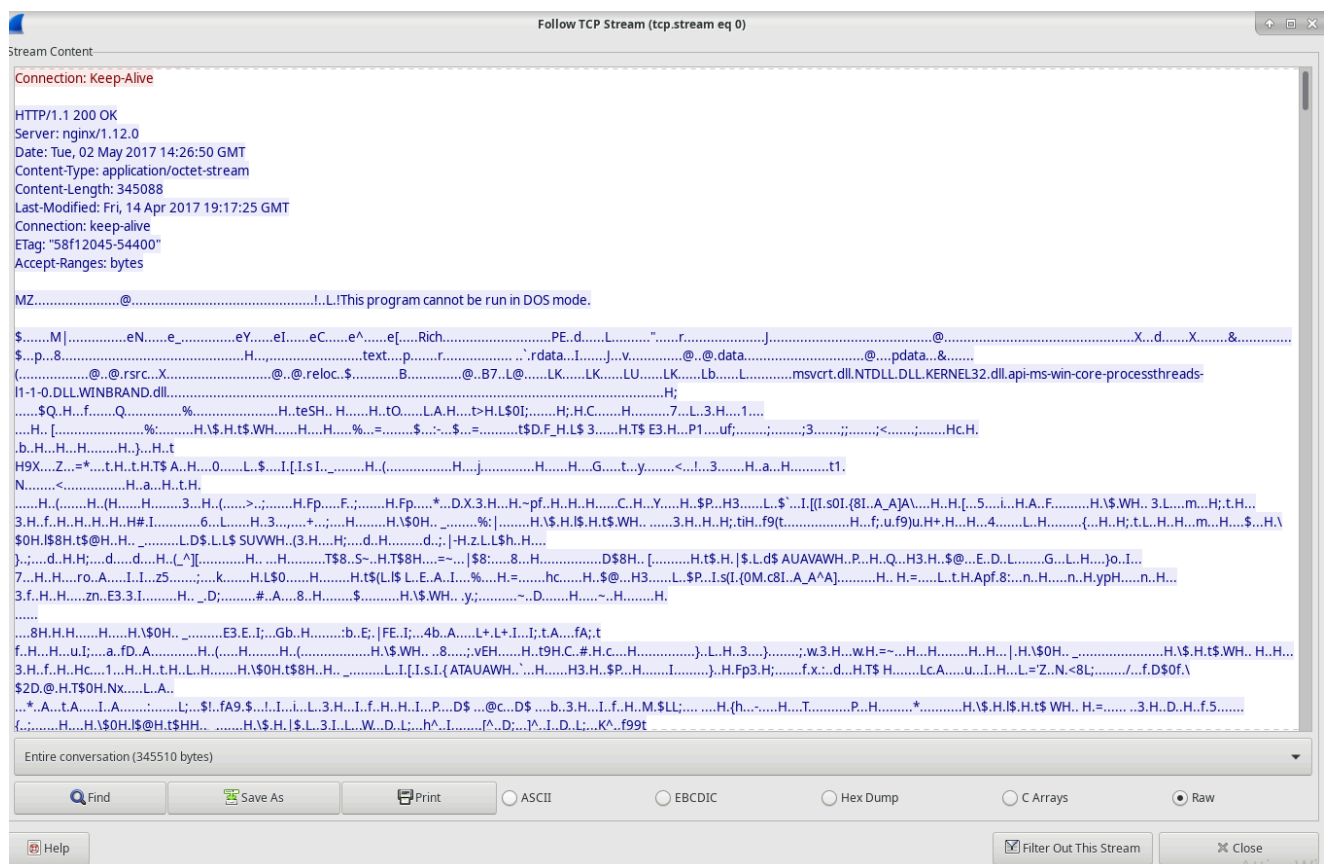
# Filtrare l'Output di Mount - Filtering Mount Output

🌟 Tag: #mount #output\_mount #filtraggio

- **Comando:** `mount | grep sda1`
- **Obiettivo:** Mostrare solo i dettagli di `sda1`.
- **Risultato:** `sda1` è montato su `/` (la radice del filesystem) con tipo `ext4`.

## Opzioni:

- `rw`: Permette lettura e scrittura.
- `relatime`: Riduce gli aggiornamenti del timestamp di accesso.
- `data=ordered`: Mantiene l'ordine sicuro di scrittura dei dati.



# Comandi di Navigazione nelle Directory - Directory Navigation Commands

🌟 Tag: #navigazione\_directory #comandi\_linux

1. **cd /**: Accede alla root, la directory principale del filesystem.
2. **ls -l**: Elenca i contenuti della directory in formato dettagliato, mostrando permessi, proprietà, dimensioni e date.
3. **cd ~**: Accede alla home dell'utente, che rappresenta lo spazio personale.
4. **ls -l**: Mostra i dettagli della home directory.

The screenshot displays the SGUIL-0.9.0 interface, which is connected to localhost. The main window is titled "seconion-import-1\_1" and shows a terminal session with the following commands and output:

```
DST: msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
DST: bind:x:105:113::/var/cache/bind:/bin/false
DST: postfix:x:106:115::/var/spool/postfix:/bin/false
DST: ftp:x:107:65534::/home/ftp:/bin/false
DST: postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
DST: mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
DST: tomcat55:x:110:65534::usr/share/tomcat5.5:/bin/false
DST: distccd:x:111:65534::/bin/false
DST: user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
DST: service:x:1002:1002:::/home/service:/bin/bash
DST: te
DST: inetd:x:112:120::/nonexistent:/bin/false
DST: proftpd:x:113:65534::/var/run/proftpd:/bin/false
DST: statd:x:114:65534::/var/lib/nfs:/bin/false
DST: analyst:x:1003:1003:Security Analyst,,,:/home/analyst:/bin/bash
DST:
SRC: cat /etc/passwd | grep root
SRC:
DST: root:x:0:0:root:/root:/bin/bash
DST:
SRC: echo "myroot:x:0:0:root:/root:/bin/bash" >> /etc/passwd
SRC:
SRC: grep root /etc/passwd
SRC:
DST: root:x:0:0:root:/root:/bin/bash
DST: myroot:x:0:0:root:/root:/bin/bash
DST:
SRC: exit
SRC:
```

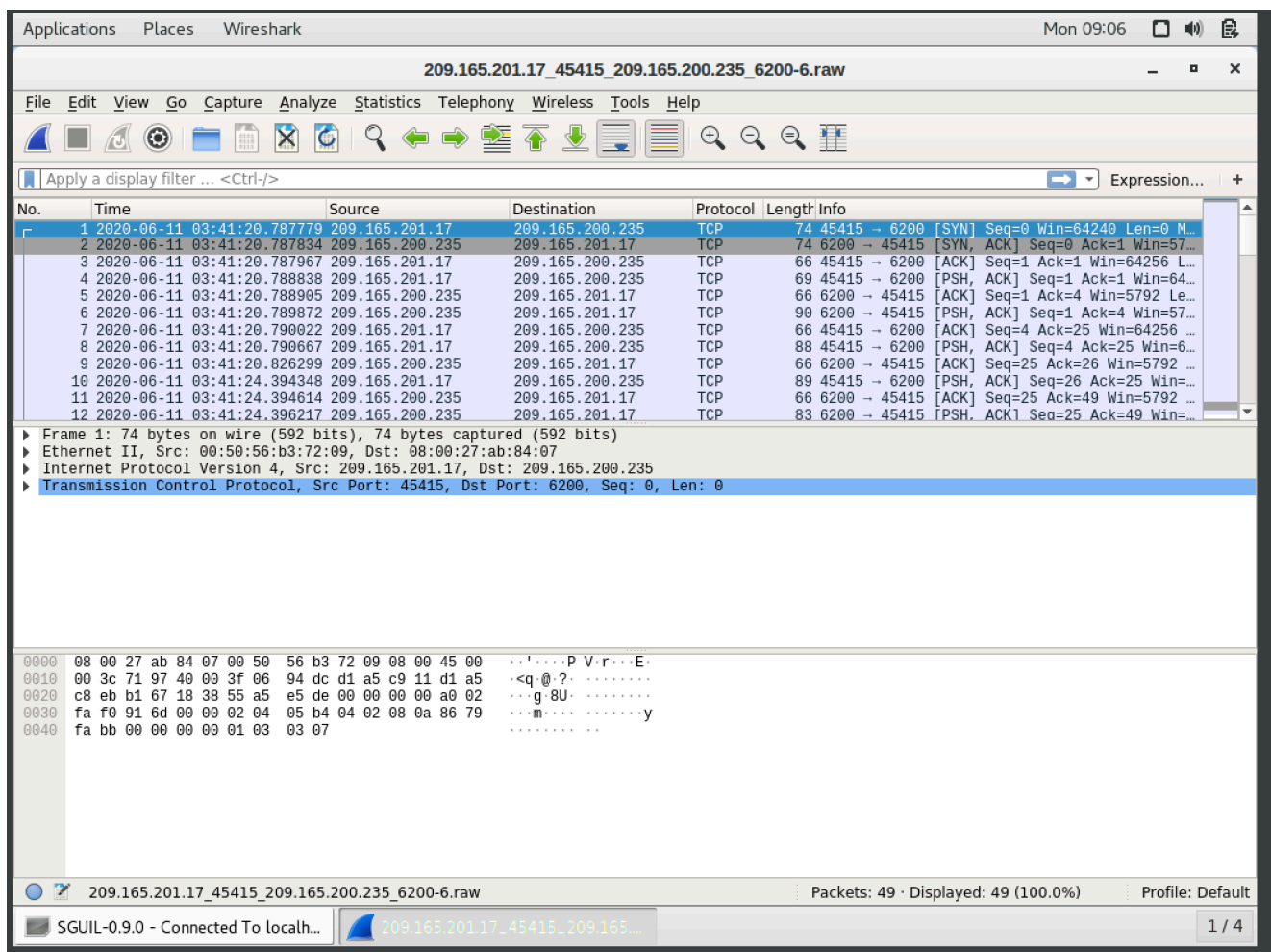
Below the terminal window, there is a "Debug Messages" section showing the following text:

```
209.165.201.17 and port 6200 and port 45415 and proto 6) or (vlan and host 209.165.200.235 and host 209.165.201.17 and port 6200 and port 45415 and proto 6)
Receiving raw file from sensor.
Finished.
```

On the right side of the interface, there is a packet capture window showing a list of events. The table below represents the data shown in this window:

DPort	Pr	Event Message
15.84	80	6 ET POLICY Data POST to a...
14	443	6 ET POLICY HTTP traffic on ...
8	53	17 ET POLICY DNS Update Fro...
174	49731	6 ET CURRENT_EVENTS Lik...
174	49731	6 ET CURRENT_EVENTS Win...
174	49731	6 ET POLICY PE EXE or DLL ...
174	49760	6 ET TROJAN ABUSE.CH SS...
201.17	45415	6 GPL ATTACK_RESPONSE i...
	0	[OSSEC] File added to the s...
	0	[OSSEC] Integrity checksum...
	0	[OSSEC] New group added t...
	0	[OSSEC] New user added to ...
	0	[OSSEC] Listened ports stat...

At the bottom of the interface, there is a "Search Packet Payload" section with radio buttons for "Hex", "Text", and "NoCase". The "Text" option is selected.



# Montaggio e Smontaggio di Partizioni - Mounting and Unmounting Partitions

🌸 Tag: [#mount](#) [#umount](#) [#gestione\\_filesystem](#)

## 1. Montaggio:

- `sudo mount /dev/sdb1 ~/second_drive/`: Monta la partizione `/dev/sdb1` nella cartella `second_drive` della home dell'utente.
- Contenuti:
  - `lost+found`: Per recuperare file persi.
  - `myFile.txt`: Un file di testo generico.

Applications Places Wireshark Mon 09:08

Wireshark · Follow TCP Stream (tcp.stream eq 0) · 209.165.201.17\_45415\_209.165....

File Edit View Go

tcp.stream eq 0

No.	Time	Source	Destination	Protocol	Length	Info
1	2020-06-11 03:00:00.000000	209.165.201.17	209.165.201.17	Ethernet II	66	Source: 209.165.201.17, Destination: 209.165.201.17
2	2020-06-11 03:00:00.000000	209.165.201.17	209.165.201.17	Internet Protocol Version 4	60	Source: 209.165.201.17, Destination: 209.165.201.17
3	2020-06-11 03:00:00.000000	209.165.201.17	209.165.201.17	Transmission Control Protocol	60	Source: 209.165.201.17, Destination: 209.165.201.17
4	2020-06-11 03:00:00.000000	209.165.201.17	209.165.201.17	TCP	60	Source: 209.165.201.17, Destination: 209.165.201.17
5	2020-06-11 03:00:00.000000	209.165.201.17	209.165.201.17	HTTP	60	Source: 209.165.201.17, Destination: 209.165.201.17
6	2020-06-11 03:00:00.000000	209.165.201.17	209.165.201.17	HTTP	60	Source: 209.165.201.17, Destination: 209.165.201.17
7	2020-06-11 03:00:00.000000	209.165.201.17	209.165.201.17	HTTP	60	Source: 209.165.201.17, Destination: 209.165.201.17
8	2020-06-11 03:00:00.000000	209.165.201.17	209.165.201.17	HTTP	60	Source: 209.165.201.17, Destination: 209.165.201.17
9	2020-06-11 03:00:00.000000	209.165.201.17	209.165.201.17	HTTP	60	Source: 209.165.201.17, Destination: 209.165.201.17
10	2020-06-11 03:00:00.000000	209.165.201.17	209.165.201.17	HTTP	60	Source: 209.165.201.17, Destination: 209.165.201.17
11	2020-06-11 03:00:00.000000	209.165.201.17	209.165.201.17	HTTP	60	Source: 209.165.201.17, Destination: 209.165.201.17
12	2020-06-11 03:00:00.000000	209.165.201.17	209.165.201.17	HTTP	60	Source: 209.165.201.17, Destination: 209.165.201.17

Frame 3: 66 bytes on wire (528 bits) captured on interface eth0

Ethernet II, Src: 08:00:27:ab:84:07, Dst: 08:00:27:ab:84:07

Internet Protocol Version 4, Src: 209.165.201.17, Destination: 209.165.201.17

Transmission Control Protocol, Src Port: 45415, Dst Port: 80, Seq: 14747, Win: 0, Len: 0

TCP, Seq: 14747, Win: 0, Len: 0

HTTP, GET /etc/shadow HTTP/1.1

root:\$1\$avpfBJ1\$X0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::daemon\*:14684:0:99999:7:::bin\*:14684:0:99999:7:::sys:\$1\$FUX6BP0t\$MiyC3Up0zQJqz4s5wFD910:14742:0:99999:7:::sync\*:14684:0:99999:7:::games\*:14684:0:99999:7:::man\*:14684:0:99999:7:::lp\*:14684:0:99999:7:::mail\*:14684:0:99999:7:::www-data\*:14684:0:99999:7:::backup\*:14684:0:99999:7:::list\*:14684:0:99999:7:::irc\*:14684:0:99999:7:::gnats\*:14684:0:99999:7:::nobody\*:14684:0:99999:7:::libuuid\*:14684:0:99999:7:::dhcpcd\*:14684:0:99999:7:::syslog\*:14684:0:99999:7:::klog\*:14684:0:99999:7:::sshd\*:14684:0:99999:7:::msfadmin\*:14684:0:99999:7:::bind\*:14684:0:99999:7:::postfix\*:14684:0:99999:7:::ftp\*:14684:0:99999:7:::postgres\*:14684:0:99999:7:::mysql\*:14684:0:99999:7:::tomcat55\*:14684:0:99999:7:::distccd\*:14684:0:99999:7:::user\*:14684:0:99999:7:::service\*:14684:0:99999:7:::

14 client pkts, 11 server pkts, 20 turns.

Entire conversation (4,388 bytes) Show and save data as ASCII Stream 0

Find: Find Next

Filter Out This Stream Print Save as... Back Close Help

209.165.201.17 SGUIL-0.9.0 - Connected To localh... 209.165.201.17\_45415\_209.165... Wireshark · Follow TCP Stream (tc... 1 / 4

Applications Places Wireshark Mon 09:09

Wireshark · Follow TCP Stream (tcp.stream eq 0) · 209.165.201.17\_45415\_209.165....

File Edit View Go

tcp.stream eq 0

No.	Time	Source	Destination	Protocol	Length	Info
1	2020-06-11 03:00:00.000000	209.165.201.17	209.165.201.17	Ethernet II	66	Source: 209.165.201.17, Destination: 209.165.201.17
2	2020-06-11 03:00:00.000000	209.165.201.17	209.165.201.17	Internet Protocol Version 4	60	Source: 209.165.201.17, Destination: 209.165.201.17
3	2020-06-11 03:00:00.000000	209.165.201.17	209.165.201.17	Transmission Control Protocol	60	Source: 209.165.201.17, Destination: 209.165.201.17
4	2020-06-11 03:00:00.000000	209.165.201.17	209.165.201.17	TCP	60	Source: 209.165.201.17, Destination: 209.165.201.17
5	2020-06-11 03:00:00.000000	209.165.201.17	209.165.201.17	HTTP	60	Source: 209.165.201.17, Destination: 209.165.201.17
6	2020-06-11 03:00:00.000000	209.165.201.17	209.165.201.17	HTTP	60	Source: 209.165.201.17, Destination: 209.165.201.17
7	2020-06-11 03:00:00.000000	209.165.201.17	209.165.201.17	HTTP	60	Source: 209.165.201.17, Destination: 209.165.201.17
8	2020-06-11 03:00:00.000000	209.165.201.17	209.165.201.17	HTTP	60	Source: 209.165.201.17, Destination: 209.165.201.17
9	2020-06-11 03:00:00.000000	209.165.201.17	209.165.201.17	HTTP	60	Source: 209.165.201.17, Destination: 209.165.201.17
10	2020-06-11 03:00:00.000000	209.165.201.17	209.165.201.17	HTTP	60	Source: 209.165.201.17, Destination: 209.165.201.17
11	2020-06-11 03:00:00.000000	209.165.201.17	209.165.201.17	HTTP	60	Source: 209.165.201.17, Destination: 209.165.201.17
12	2020-06-11 03:00:00.000000	209.165.201.17	209.165.201.17	HTTP	60	Source: 209.165.201.17, Destination: 209.165.201.17

Frame 3: 66 bytes on wire (528 bits) captured on interface eth0

Ethernet II, Src: 08:00:27:ab:84:07, Dst: 08:00:27:ab:84:07

Internet Protocol Version 4, Src: 209.165.201.17, Destination: 209.165.201.17

Transmission Control Protocol, Src Port: 45415, Dst Port: 80, Seq: 14747, Win: 0, Len: 0

TCP, Seq: 14747, Win: 0, Len: 0

HTTP, GET /etc/passwd HTTP/1.1

root:x:0:0:root:/root:/bin/bash  
daemon:x:1:1:daemon:/usr/sbin:/bin/sh  
bin:x:2:2:bin:/bin:/bin/sh  
sys:x:3:3:sys:/dev:/bin/sh  
sync:x:4:65534:sync:/bin:/bin/sync  
games:x:5:60:games:/usr/games:/bin/sh  
man:x:6:12:man:/var/cache/man:/bin/sh  
lp:x:7:7:lp:/var/spool/lpd:/bin/sh  
mail:x:8:8:mail:/var/mail:/bin/sh  
news:x:9:9:news:/var/spool/news:/bin/sh  
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh  
proxy:x:13:13:proxy:/bin:/bin/sh  
www-data:x:33:33:www-data:/var/www:/bin/sh  
backup:x:34:34:backup:/var/backups:/bin/sh  
list:x:38:38:Mailng List Managers:/var/list:/bin/sh  
irc:x:39:39:ircd:/var/run/ircd:/bin/sh  
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh  
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh  
libuuid:x:100:101:/var/lib/libuuid:/bin/sh  
dhcpcd:x:101:102:/nonexistent:/bin/false  
syslog:x:102:103:/home/syslog:/bin/false  
klog:x:103:104:/home/klog:/bin/false  
sshd:x:104:65534:/var/run/sshd:/usr/sbin/nologin  
msfadmin:x:1000:1000:msfadmin,,/home/msfadmin:/bin/bash  
bind:x:105:113:/var/cache/bind:/bin/false  
postfix:x:106:115:/var/spool/postfix:/bin/false  
ftp:x:107:65534:/home/ftp:/bin/false  
postgres:x:108:117:PostgreSQL administrator,,/var/lib/postgresql:/bin/bash  
mysql:x:109:118:MySQL Server,,/var/lib/mysql:/bin/false  
tomcat55:x:110:65534:/usr/share/tomcat5.5:/bin/false  
distccd:x:111:65534:/bin/false  
user:x:1001:1001:just a user,111,,/home/user:/bin/bash  
service:x:1002:1002:/home/service:/bin/bash

14 client pkts, 11 server pkts, 20 turns.

Entire conversation (4,388 bytes) Show and save data as ASCII Stream 0

Find: Find Next

Filter Out This Stream Print Save as... Back Close Help

209.165.201.17 SGUIL-0.9.0 - Connected To localh... 209.165.201.17\_45415\_209.165... Wireshark · Follow TCP Stream (tc... 1 / 4



Applications Places Dialog Mon 09:12

SGUIL-0.9.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost Username: analyst UserID: 2 2024-10-28 09:12:41 GMT

RealTime Events Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message	
RT	114	seconion-...	5.251	2019-07-19 18:57:23	172.16.4.205	49255	31.7.62.214	443	6	ET POLICY HTTP traffic on ...	
RT	2	seconion-...	5.365	2020-02-21 00:53:55	172.17.8.174	62362	172.17.8.8	53	17	ET POLICY DNS Update Fro...	
RT	13	seconion-...	5.366	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET CURRENT_EVENTS Lik...	
RT	13	seconion-...	5.379	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET CURRENT_EVENTS Win...	
RT	13	seconion-...	5.392	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET POLICY PE EXE or DLL ...	
RT	4	seconion-...	5.406	2020-02-21 01:11:48	91.211.88.122	443	172.17.8.174	49760	6	ET TROJAN ABUSE.CH SS...	
RT	1	seconion-...	5.1	2020-06-11 03:41:20	209.165.200.235	6200	209.165.201.17	45415	6	GPL ATTACK_RESPONSE i...	
RT	351	seconion-...	1.1	2020-06-19 18:09:28	Quick Query					0	[OSSEC] File added to the s...
RT	23	seconion-...	1.2	2020-06-19 18:09:29	Advanced Query					0	[OSSEC] Integrity checksum...
RT	7	seconion-...	1.4	2020-06-19 18:10:04	Dshield IP Lookup					0	[OSSEC] New group added t...
RT	7	seconion-...	1.5	2020-06-19 18:10:04	Copy IP Address					0	[OSSEC] New user added to ...
RT	2	seconion-...	1.18	2020-06-19 18:14:41	Alexa IP Lookup					0	[OSSEC] Listened ports stat...
RT	1	seconion-...	1.19	2020-06-19 18:18:41	Bing IP Lookup					0	[OSSEC] Received 0 packet...

IP Resolution Agent Status Snort Statistics System Msg

☐ Reverse DNS ☒ Enable External DNS

Src IP:

Src Name:

Dst IP:

Dst Name:

Whois Query: ☐ None ☐ Src IP ☐ Dst IP

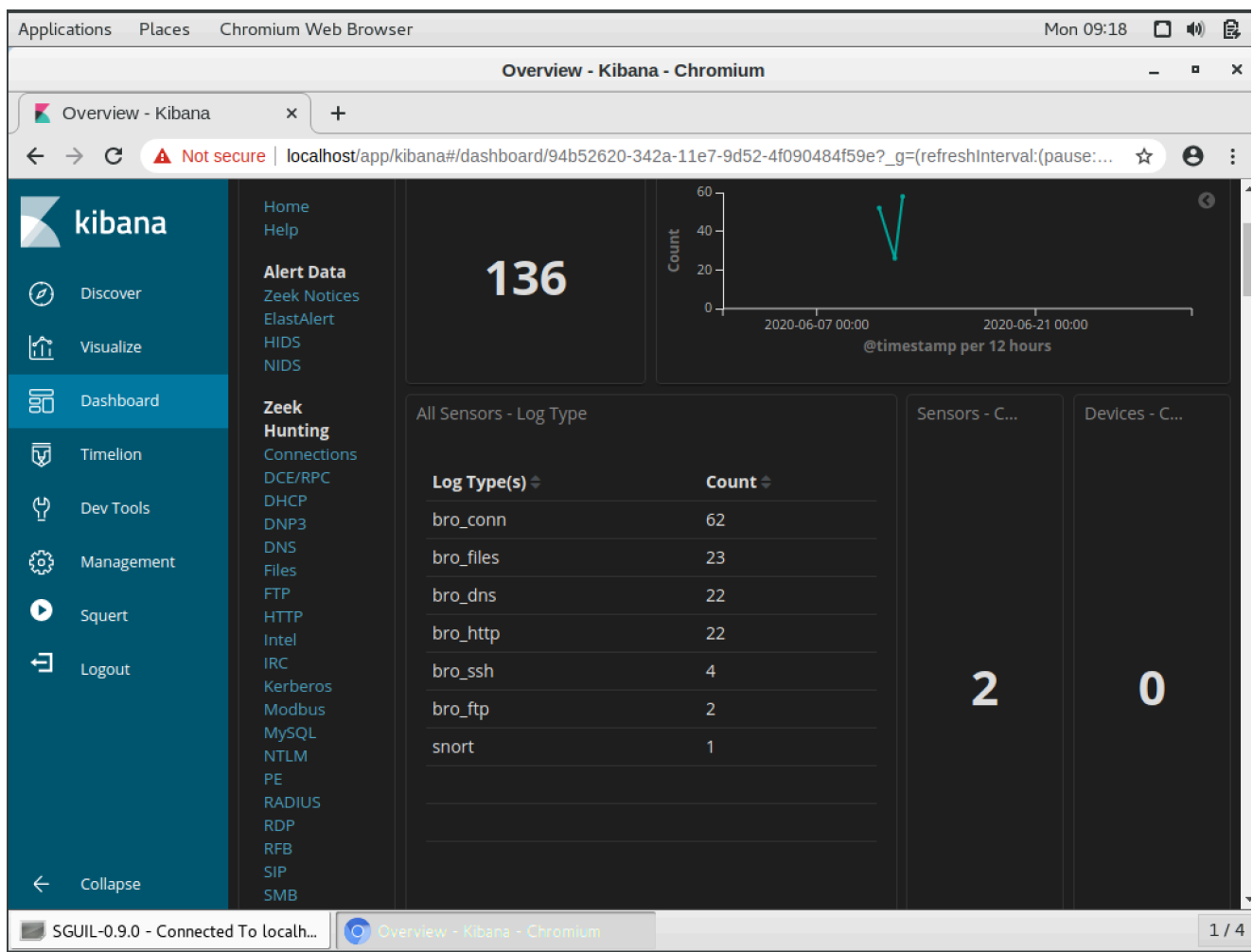
DATA

Search Packet Payload ☐ Hex ☒ Text ☐ NoCase

SGUIL-0.9.0 - Connected To localhost 1 / 4

## 2. Smontaggio:

- `sudo umount /dev/sdb1`: Smonta `/dev/sdb1` dalla cartella `second_drive`.
- **Risultato:** `second_drive` risulta vuota.



## Gestione dei Permessi e Proprietà - Permissions and Ownership Management

🌸 Tag: [#chmod](#) [#chown](#) [#permessi\\_file](#)

### 1. Visualizzazione dei permessi dei file:

- `ls -l` : visualizza i permessi dei file.

```
[analyst@sec0ps ~]$ cd lab.support.files/pcaps
[analyst@sec0ps pcaps]$ ls -l
total 4028
-rw-r--r-- 1 analyst analyst 371462 Mar 21 2018 nimda.download.pcap
-rw-r--r-- 1 analyst analyst 3750153 Mar 21 2018 wannacry_download_pcap.pcap
[analyst@sec0ps pcaps]$ wireshark nimda.download.pcap &
[1] 1093
```

### 2. Creazione di un file:



- `touch` : Con il comando `touch` proviamo a testare la possibilità di creare un file nella directory `/mnt` . Con l'aggiunta dell'opzione `-d` , elenca i permessi della parent directory.

```
[analyst@sec0ps scripts]$ touch /mnt/myNewFile.txt
touch: cannot touch '/mnt/myNewFile.txt': Permission denied
[analyst@sec0ps scripts]$ ls -ld /mnt
drwxr-xr-x 2 root root 4096 Jan  5  2018 /mnt
[analyst@sec0ps scripts]$
```

### 3. Modifica dei Permessi:

- `chmod 665 myFile.txt` : Consente lettura e scrittura a utente e gruppo.

### 4. Modifica Proprietario:

- `chown analyst myFile.txt` : Imposta il proprietario del file come `analyst`.

### 5. Verifica:

- `echo "test" >> myFile.txt` : Aggiunge testo al file.
- `cat myFile.txt` : Visualizza il contenuto del file.

```
[analyst@sec0ps scripts]$ cd ~/second_drive
[analyst@sec0ps second_drive]$ ls -l
total 20
drwx----- 2 root    root    16384 Mar 26  2018 lost+found
-rw-r--r--  1 analyst analyst  183 Mar 26  2018 myFile.txt
[analyst@sec0ps second_drive]$ sudo chmod 665 myFile.txt
[analyst@sec0ps second_drive]$ ls -l
total 20
drwx----- 2 root    root    16384 Mar 26  2018 lost+found
-rw-rw-r-x  1 analyst analyst  183 Mar 26  2018 myFile.txt
[analyst@sec0ps second_drive]$ sudo chown analyst myFile.txt
[analyst@sec0ps second_drive]$ ls -l
total 20
drwx----- 2 root    root    16384 Mar 26  2018 lost+found
-rw-rw-r-x  1 analyst analyst  183 Mar 26  2018 myFile.txt
[analyst@sec0ps second_drive]$ echo test >> myFile.txt
[analyst@sec0ps second_drive]$ cat myFile.txt
This is a file stored in the /dev/sdb1 disk.
Notice that even though this file has been sitting in this disk for a while, it couldn't be accessed until the disk was properly mounted.
test
```

## Visualizzazione dei File e Tipi di Collegamenti - Viewing Files and Link Types

🌸 Tag: [#visualizzazione\\_file](#) [#collegamenti](#) [#tipi\\_file](#)

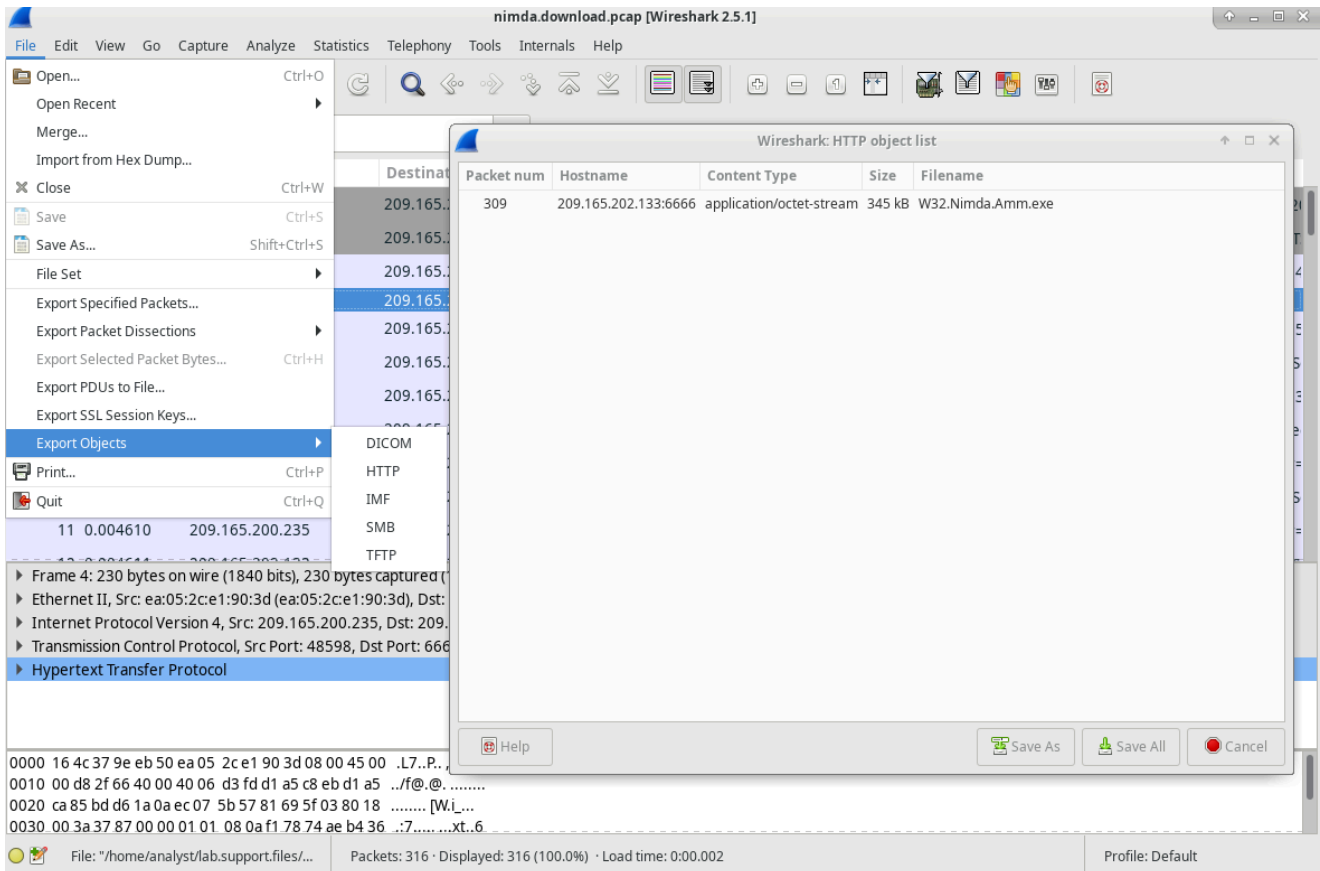
### 1. Comando Utilizzato: `ls -l /home/analyst`

- **Descrizione:** Il comando `ls -l` mostra i file nella directory `/home/analyst` , indicando con i primi caratteri il tipo di file:

- - : Indica un file.
- d : Indica una directory.

2. **Esempio:** Visualizzando la directory `/dev` , si osserva:

- b : File di blocco.
- c : Dispositivo a caratteri.
- l : Collegamento simbolico.



## Creazione di Collegamenti Simbolici e Hard - Creating Symbolic and Hard Links

🌸 Tag: [#creazione\\_link](#) [#link\\_simbolici](#) [#hard\\_link](#)

1. **Creazione File:**

- **Comandi:**

```
echo "testo" > file1.txt
```

```
echo "testo" > file2.txt
```

## 2. Collegamento Simbolico:

- **Comando:** `ln -s file1.txt file1symbolic`
- **Descrizione:** Un collegamento simbolico a `file1.txt` simile a una scorciatoia in Windows.

## 3. Collegamento Hard:

- **Comando:** `ln file2.txt file2hard`
- **Descrizione:** Un hard link a `file2.txt` punta allo stesso inode, condividendo dati e attributi con il file originale.

```
crw-rw-rw- 1 root root 1, 3 Oct 28 09:44 28
[analyst@sec0ps ~]$ echo "symbolic" > file1.txt
[analyst@sec0ps ~]$ cat file1.txt
symbolic
[analyst@sec0ps ~]$ echo "hard" > file2.txt
[analyst@sec0ps ~]$ cat file2.txt
hard
[analyst@sec0ps ~]$ ln -s file1.txt file1symbolic
[analyst@sec0ps ~]$ ln file2.txt file2hard
[analyst@sec0ps ~]$
```

---

# Differenze tra Collegamenti Simbolici e Hard - Differences between Symbolic and Hard Links

🌸 Tag: [#differenze\\_link](#) [#inode](#) [#filesystem](#)

## 1. Link Simbolico:

- Viene visualizzato come "l" nell'output `ls -l` e include un puntatore `->` al file originale.
- Modificare o spostare il file originale rende il link simbolico non funzionante.

## 2. Link Hard:

- Appare come un file normale e punta direttamente all'inode del file originale, condividendo le stesse proprietà.
- Il numero `2` nella quinta colonna dell'output `ls -l` indica due hard link che puntano allo stesso inode.

---

# Rinomina e Effetti sui Collegamenti - Renaming and Effects on Links

🌸 Tag: [#rinomina\\_file](#) [#effetti\\_link](#) [#gestione\\_file](#)

## 1. Rinomina File Originali:

- **Comando:** `mv file1.txt file1new.txt` e `mv file2.txt file2new.txt`

## 2. Osservazione:

- **Link Simbolico:** Dopo la rinomina, il collegamento simbolico a `file1.txt` non funziona più.
- **Link Hard:** Il collegamento hard a `file2.txt` continua a funzionare poiché punta all'inode, non al nome del file.

```
[analyst@sec0ps ~]$ ls -l
total 28
drwxr-xr-x 2 analyst analyst 4096 Mar 22  2018 Desktop
drwxr-xr-x 3 analyst analyst 4096 Mar 22  2018 Downloads
lrwxrwxrwx 1 analyst analyst   9 Oct 28 06:47 file1symbolic -> file1.txt
-rw-r--r-- 1 analyst analyst   9 Oct 28 06:46 file1.txt
-rw-r--r-- 2 analyst analyst   5 Oct 28 06:46 file2hard
-rw-r--r-- 2 analyst analyst   5 Oct 28 06:46 file2.txt
drwxr-xr-x 9 analyst analyst 4096 Jul 19  2018 lab.support.files
drwxr-xr-x 3 root      root    4096 Mar 26  2018 second_drive
[analyst@sec0ps ~]$ mv file1.txt file1new.txt
[analyst@sec0ps ~]$ mv file2.txt file2new.txt
[analyst@sec0ps ~]$ cat file1symbolic
cat: file1symbolic: No such file or directory
[analyst@sec0ps ~]$ cat file2hard
hard
```

---

## 🔑 Chiavi:

[collegamenti simbolici, hard link, filesystem, inode, ls -l, rinomina file]

---