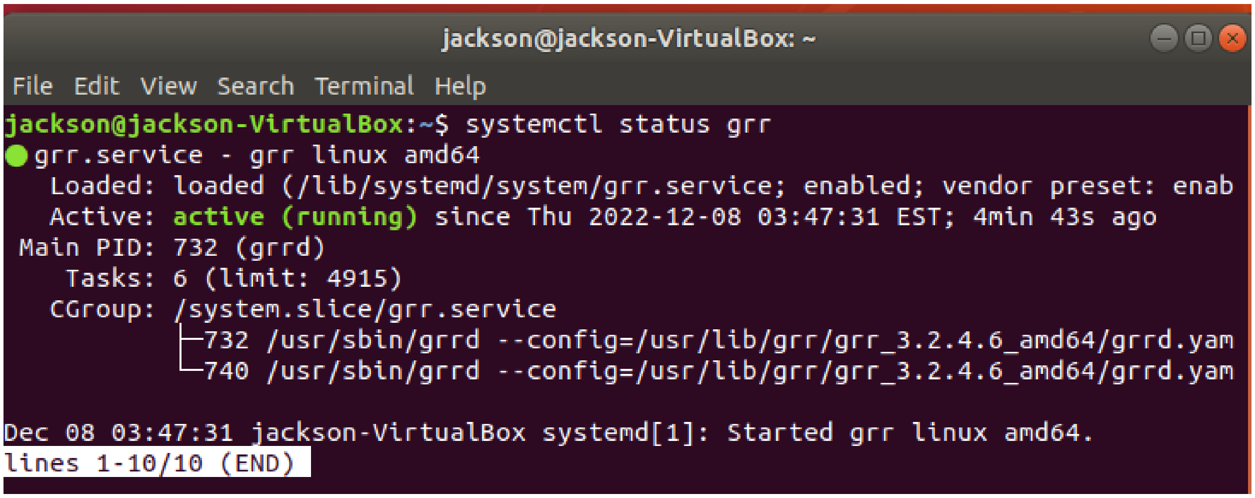
Installing GRR Server + Client

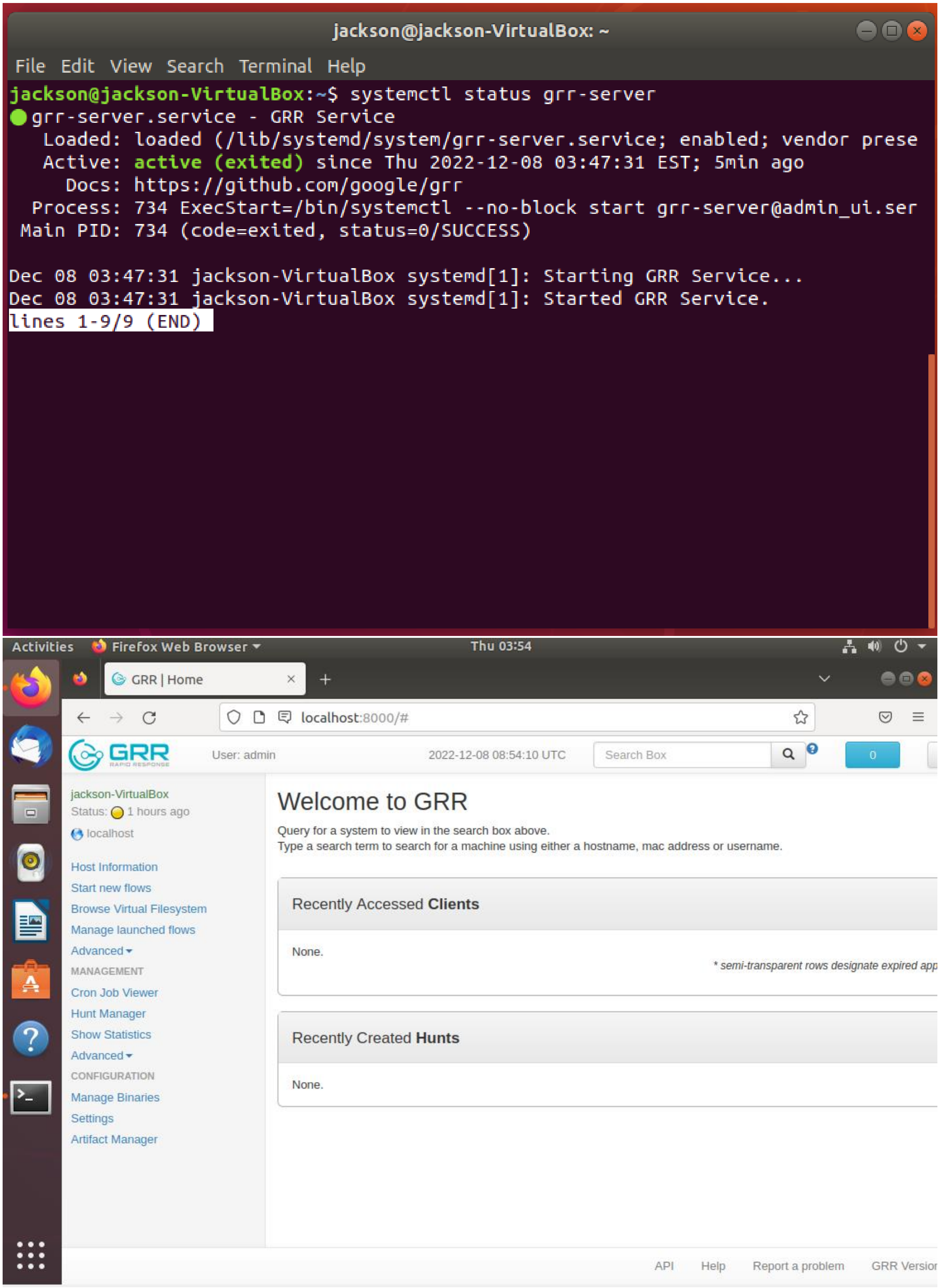
Followed the instructions on link provided in class and installed both client and server



jackson@jackson-VirtualBox: ~
File Edit View Search Terminal Help

```
jackson@jackson-VirtualBox:~$ systemctl status grr
● grr.service - grr linux amd64
   Loaded: loaded (/lib/systemd/system/grr.service; enabled; vendor preset: enab
   Active: active (running) since Thu 2022-12-08 03:47:31 EST; 4min 43s ago
 Main PID: 732 (grrd)
    Tasks: 6 (limit: 4915)
   CGroup: /system.slice/grr.service
           ├─732 /usr/sbin/grrd --config=/usr/lib/grr/grr_3.2.4.6_amd64/grrd.yam
           └─740 /usr/sbin/grrd --config=/usr/lib/grr/grr_3.2.4.6_amd64/grrd.yam

Dec 08 03:47:31 jackson-VirtualBox systemd[1]: Started grr linux amd64.
lines 1-10/10 (END)
```



```
jackson@jackson-VirtualBox:~$ systemctl status grr-server
● grr-server.service - GRR Service
   Loaded: loaded (/lib/systemd/system/grr-server.service; enabled; vendor prese
   Active: active (exited) since Thu 2022-12-08 03:47:31 EST; 5min ago
     Docs: https://github.com/google/grr
  Process: 734 ExecStart=/bin/systemctl --no-block start grr-server@admin_ui.ser
 Main PID: 734 (code=exited, status=0/SUCCESS)

Dec 08 03:47:31 jackson-VirtualBox systemd[1]: Starting GRR Service...
Dec 08 03:47:31 jackson-VirtualBox systemd[1]: Started GRR Service.
lines 1-9/9 (END)
```

Welcome to GRR

Query for a system to view in the search box above.
Type a search term to search for a machine using either a hostname, mac address or username.

Recently Accessed **Clients**

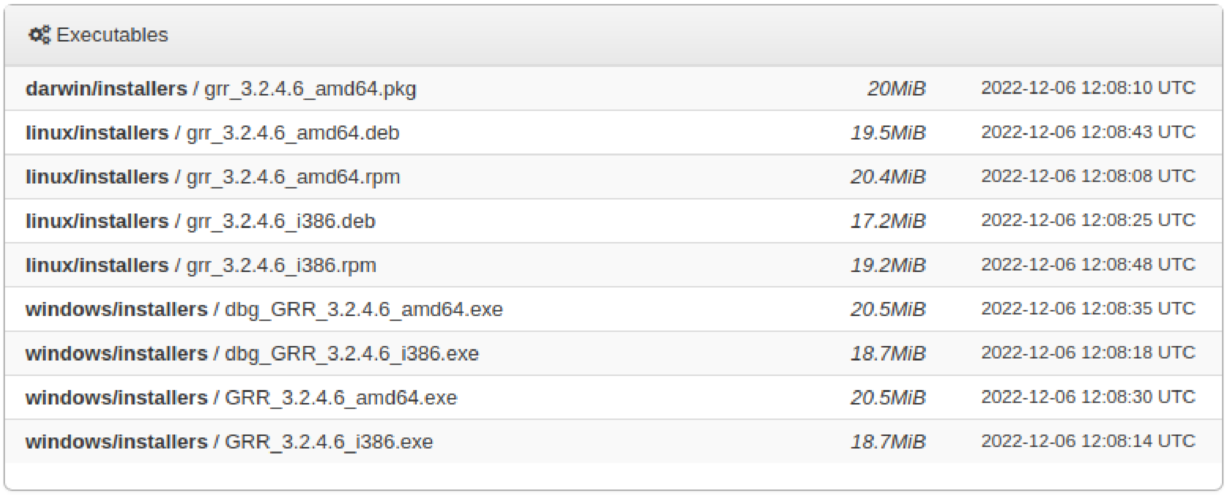
None.

** semi-transparent rows designate expired app*

Recently Created **Hunts**

None.

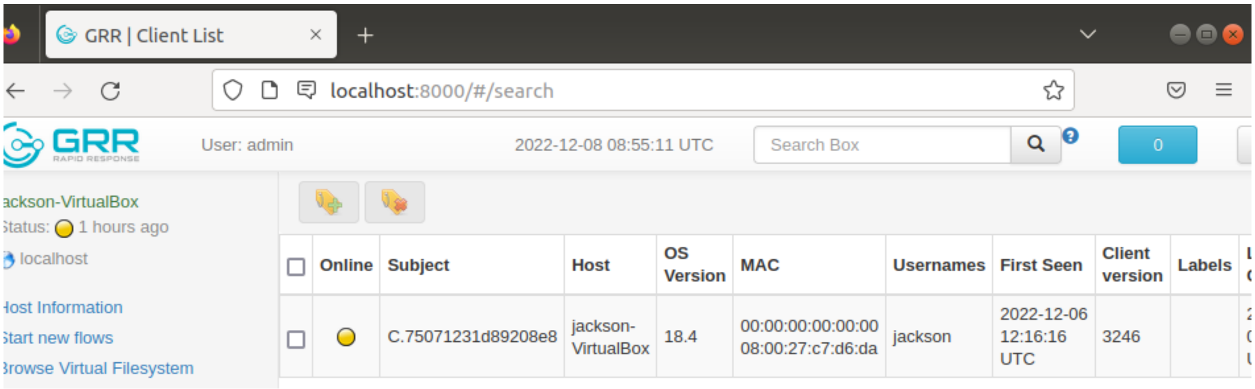
List of clients:



Executables

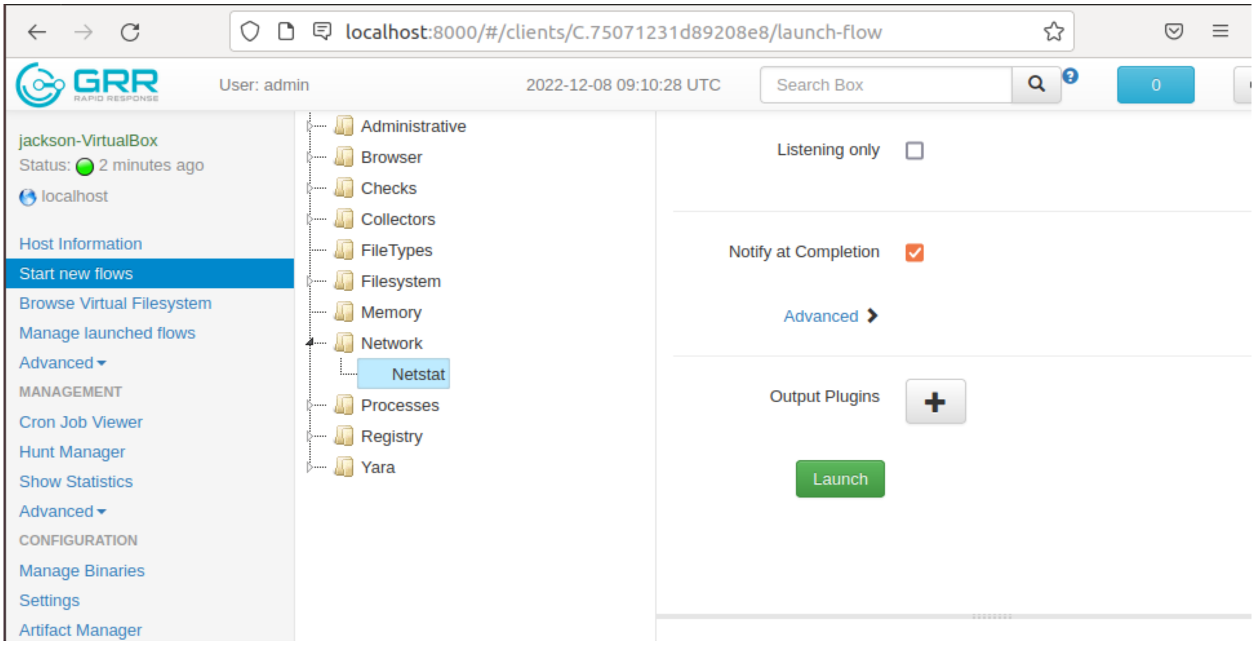
darwin/installers / grr_3.2.4.6_amd64.pkg	*20MiB*	2022-12-06 12:08:10 UTC
linux/installers / grr_3.2.4.6_amd64.deb	*19.5MiB*	2022-12-06 12:08:43 UTC
linux/installers / grr_3.2.4.6_amd64.rpm	*20.4MiB*	2022-12-06 12:08:08 UTC
linux/installers / grr_3.2.4.6_i386.deb	*17.2MiB*	2022-12-06 12:08:25 UTC
linux/installers / grr_3.2.4.6_i386.rpm	*19.2MiB*	2022-12-06 12:08:48 UTC
windows/installers / dbg_GRR_3.2.4.6_amd64.exe	*20.5MiB*	2022-12-06 12:08:35 UTC
windows/installers / dbg_GRR_3.2.4.6_i386.exe	*18.7MiB*	2022-12-06 12:08:18 UTC
windows/installers / GRR_3.2.4.6_amd64.exe	*20.5MiB*	2022-12-06 12:08:30 UTC
windows/installers / GRR_3.2.4.6_i386.exe	*18.7MiB*	2022-12-06 12:08:14 UTC

Client:



□	Online	Subject	Host	OS Version	MAC	Usernames	First Seen	Client version	Labels
□	●	C.75071231d89208e8	jackson-VirtualBox	18.4	00:00:00:00:00:00 08:00:27:c7:d6:da	jackson	2022-12-06 12:16:16 UTC	3246	

<u>Running investigating network aspect:</u>



localhost:8000/#/clients/C.75071231d89208e8/launch-flow

User: admin

2022-12-08 09:10:28 UTC

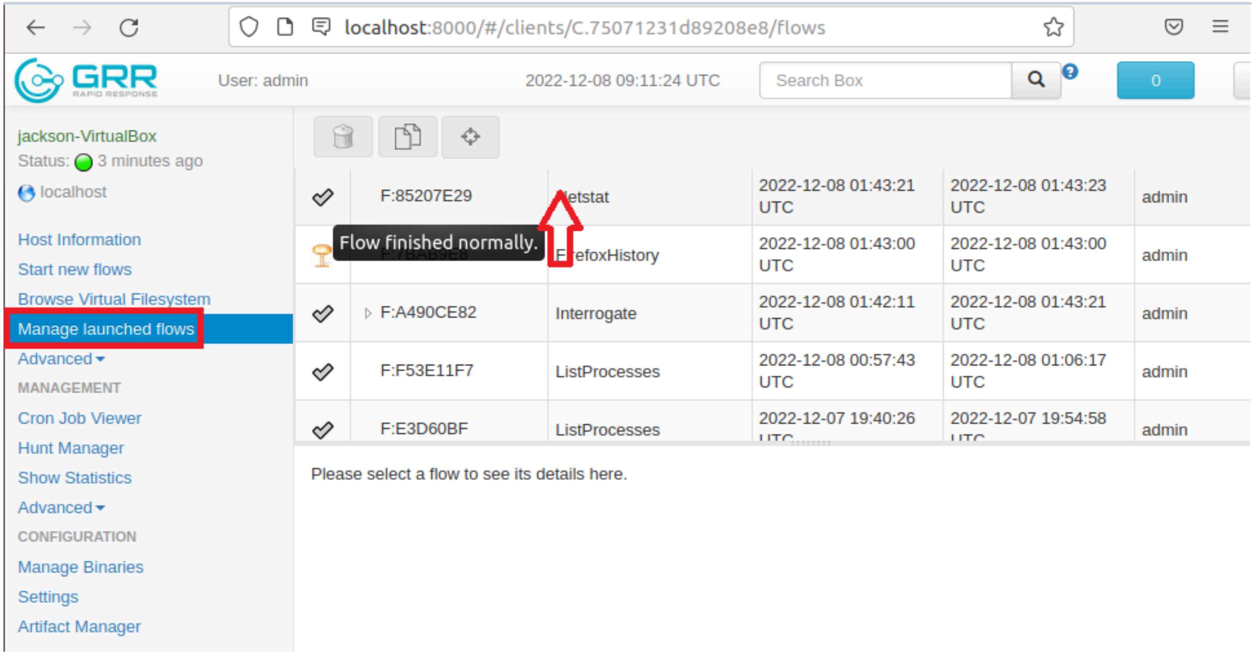
jackson-VirtualBox
Status: 2 minutes ago
localhost

- Administrative
- Browser
- Checks
- Collectors
- FileTypes
- Filesystem
- Memory
- Network
  - Netstat
- Processes
- Registry
- Yara

Listening only ☐

Notify at Completion ☑

<u>Checking stored finished results:</u>



localhost:8000/#/clients/C.75071231d89208e8/flows

User: admin

2022-12-08 09:11:24 UTC

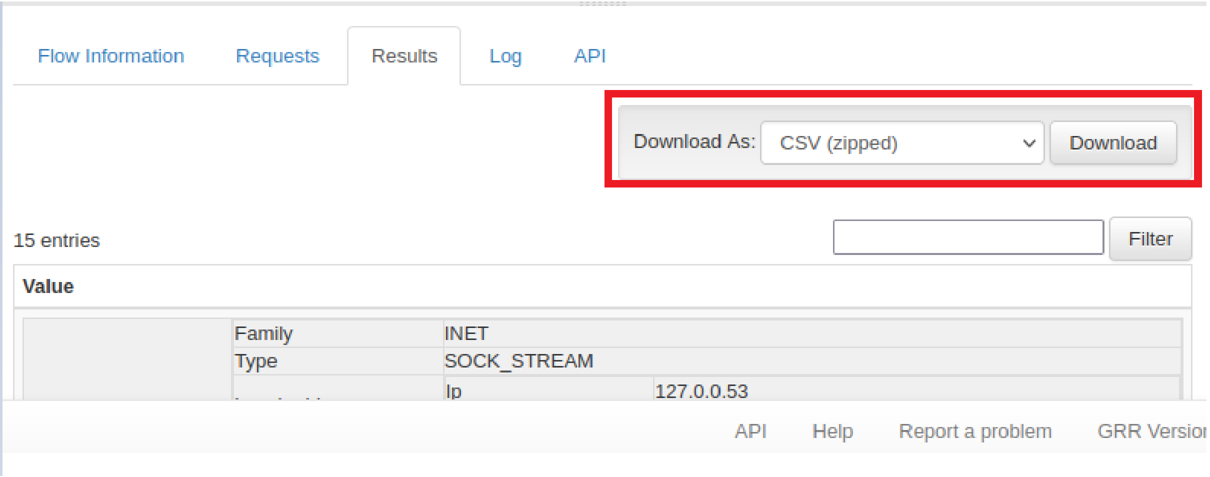
jackson-VirtualBox
Status: 3 minutes ago
localhost

✓	F:85207E29	Netstat	2022-12-08 01:43:21 UTC	2022-12-08 01:43:23 UTC	admin
	F:7BAB9E8	FirefoxHistory	2022-12-08 01:43:00 UTC	2022-12-08 01:43:00 UTC	admin
✓	F:A490CE82	Interrogate	2022-12-08 01:42:11 UTC	2022-12-08 01:43:21 UTC	admin
✓	F:F53E11F7	ListProcesses	2022-12-08 00:57:43 UTC	2022-12-08 01:06:17 UTC	admin
✓	F:E3D60BF	ListProcesses	2022-12-07 19:40:26 UTC	2022-12-07 19:54:58 UTC	admin

Flow finished normally.

Please select a flow to see its details here.

<u>Downloaded as a .csv file:</u>

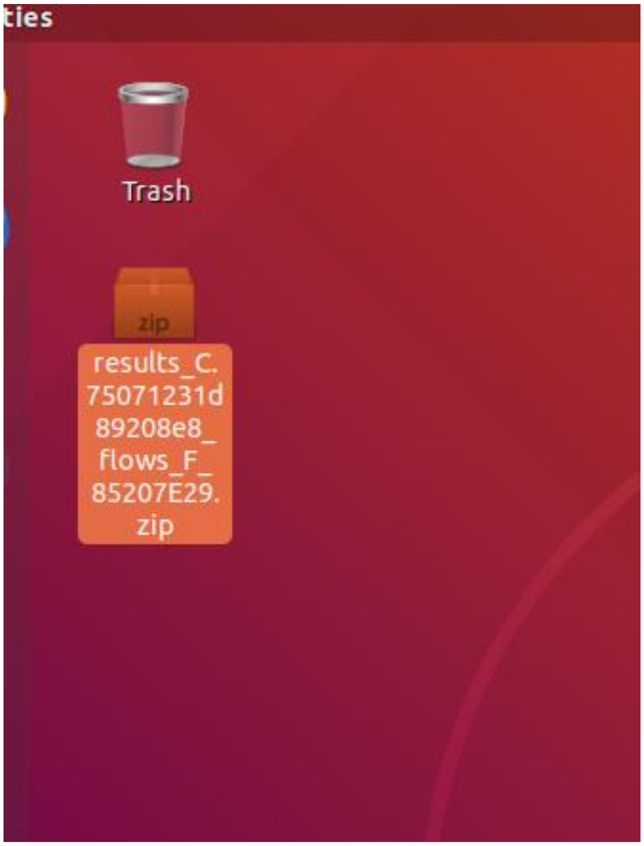


Download As: CSV (zipped)

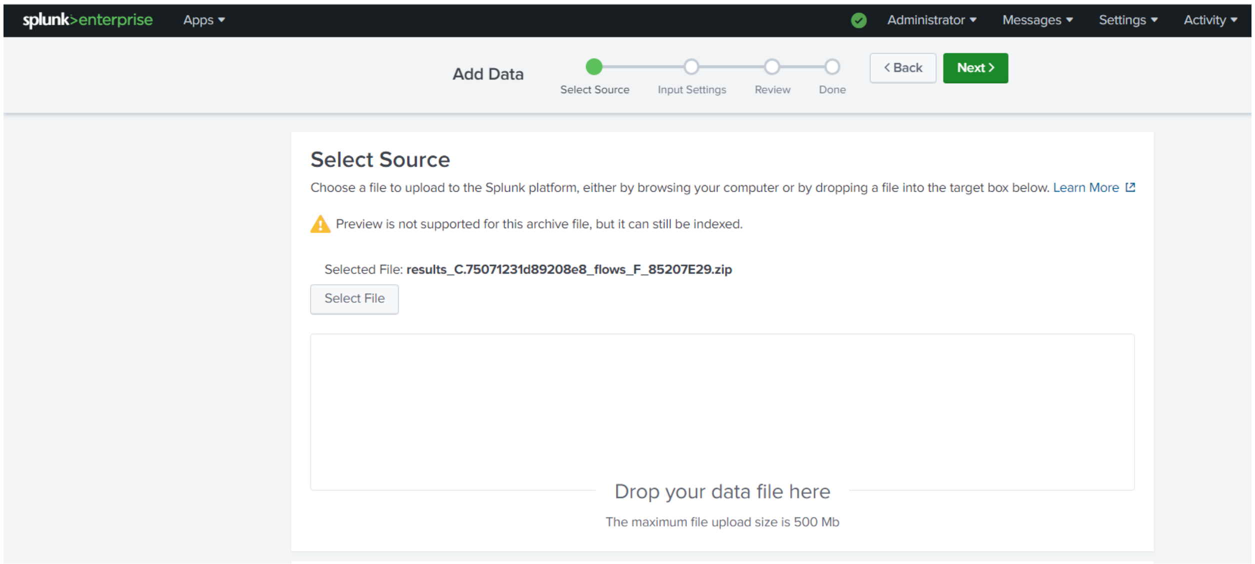
15 entries

Value

Family	INET	
Type	SOCK_STREAM	
	Ip	127.0.0.53



Emailed to self on the window's VM with Splunk:



Select Source

Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. Learn More

⚠ Preview is not supported for this archive file, but it can still be indexed.

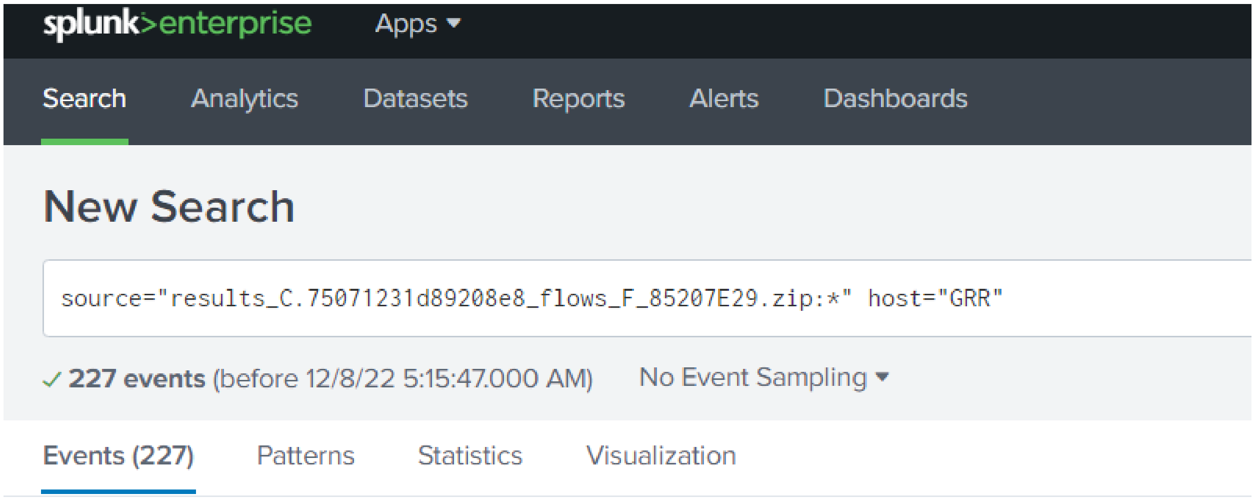
Selected File: **results_C.75071231d89208e8_flows_F_85207E29.zip**

Select File

Drop your data file here

The maximum file upload size is 500 Mb

Splunk search query:

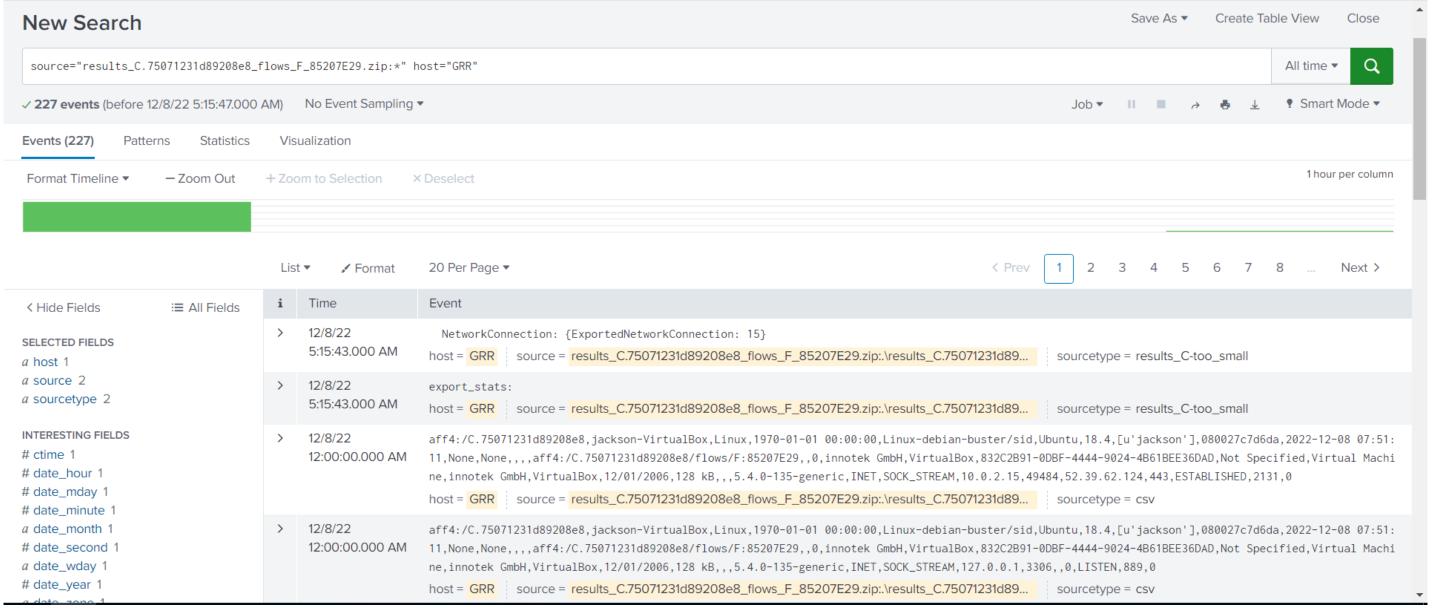


New Search

```
source="results_C.75071231d89208e8_flows_F_85207E29.zip:*" host="GRR"
```

✓ **227 events** (before 12/8/22 5:15:47.000 AM) No Event Sampling ▾

Results:



```
source="results_C.75071231d89208e8_flows_F_85207E29.zip:*" host="GRR"
```

✓ 227 events (before 12/8/22 5:15:47.000 AM) No Event Sampling ▾

SELECTED FIELDS
- a host 1
- a source 2
- a sourcetype 2

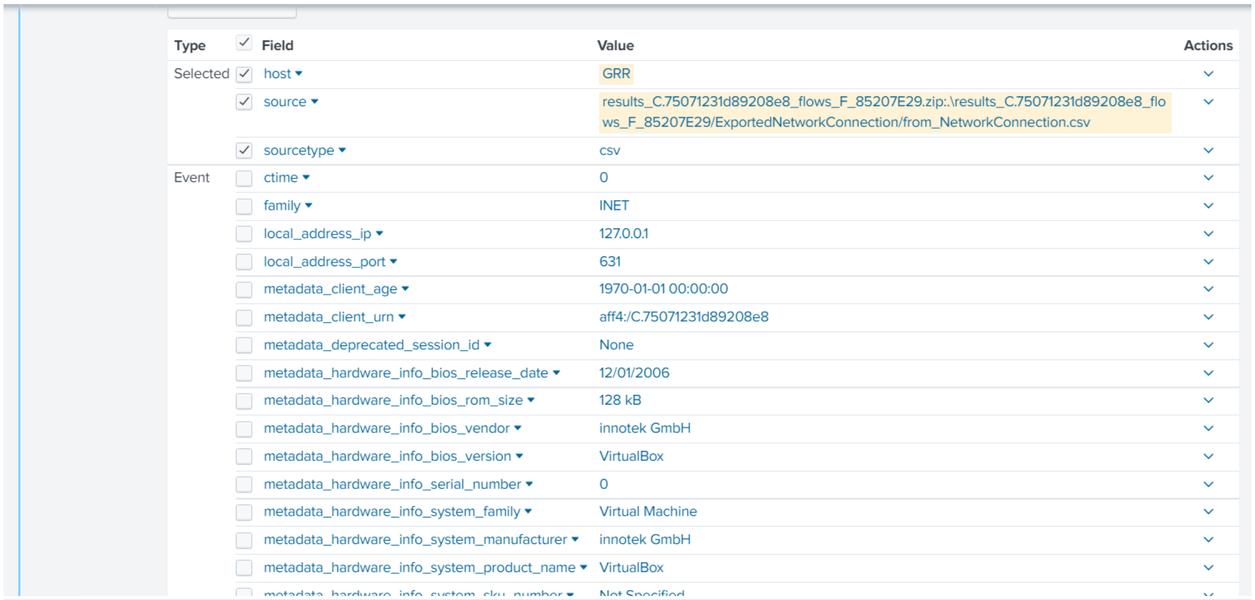
INTERESTING FIELDS
- # ctime 1
- # date_hour 1
- # date_mday 1
- # date_minute 1
- a date_month 1
- # date_second 1
- a date_wday 1
- # date_year 1

Time	Event

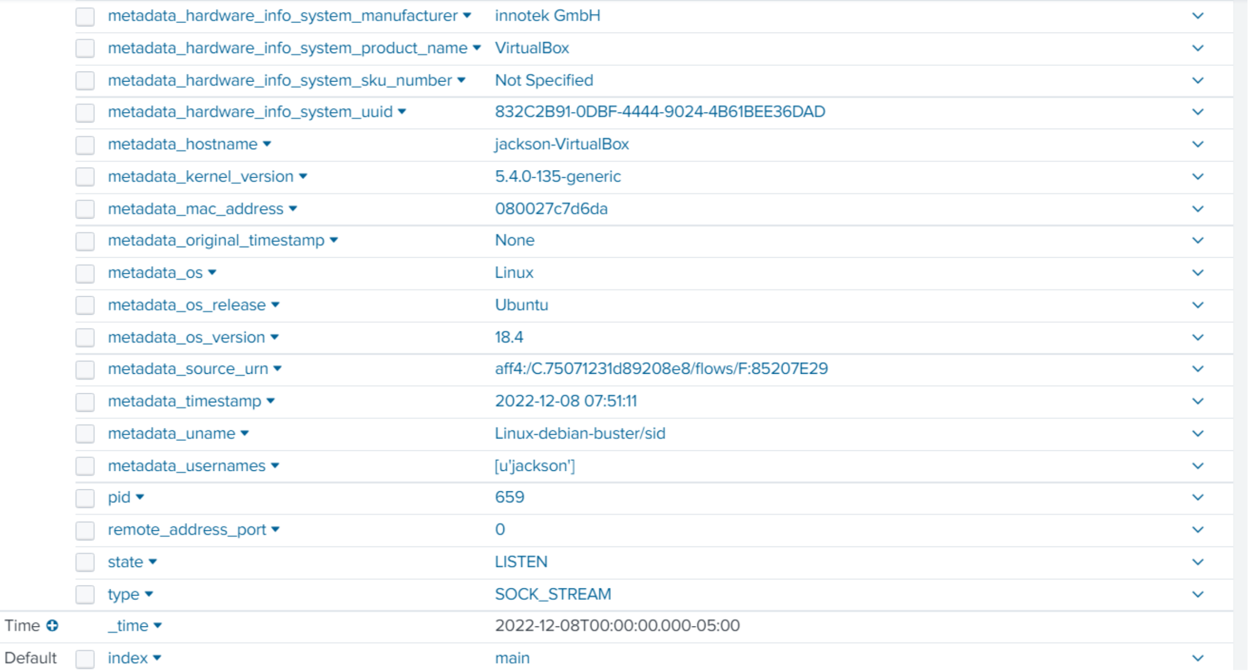
12/8/22 5:15:43.000 AM	NetworkConnection: {ExportedNetworkConnection: 15}
	host = GRR source = results_C.75071231d89208e8_flows_F_85207E29.zip:.\results_C.75071231d89... sourcetype = results_C-too_small

12/8/22 5:15:43.000 AM	export_stats: host = GRR source = results_C.75071231d89208e8_flows_F_85207E29.zip:.\results_C.75071231d89... sourcetype = results_C-too_small
12/8/22 12:00:00.000 AM	aff4:/C.75071231d89208e8,jackson-VirtualBox,Linux,1970-01-01 00:00:00,Linux-debian-buster/sid,Ubuntu,18.4,[u'jackson'],080027c7d6da,2022-12-08 07:51:11,None,None,,,,aff4:/C.75071231d89208e8/flows/F:85207E29,,0,innotek GmbH,VirtualBox,832C2B91-0DBF-4444-9024-4B61BEE36DAD,Not Specified,Virtual Machine,innotek GmbH,VirtualBox,12/01/2006,128 kB,,,5.4.0-135-generic,INET,SOCK_STREAM,10.0.2.15,49484,52.39.62.124,443,ESTABLISHED,2131,0 host = GRR source = results_C.75071231d89208e8_flows_F_85207E29.zip:.\results_C.75071231d89... sourcetype = csv
12/8/22 12:00:00.000 AM	aff4:/C.75071231d89208e8,jackson-VirtualBox,Linux,1970-01-01 00:00:00,Linux-debian-buster/sid,Ubuntu,18.4,[u'jackson'],080027c7d6da,2022-12-08 07:51:11,None,None,,,,aff4:/C.75071231d89208e8/flows/F:85207E29,,0,innotek GmbH,VirtualBox,832C2B91-0DBF-4444-9024-4B61BEE36DAD,Not Specified,Virtual Machine,innotek GmbH,VirtualBox,12/01/2006,128 kB,,,5.4.0-135-generic,INET,SOCK_STREAM,127.0.0.1,3306,,0,LISTEN,889,0 host = GRR source = results_C.75071231d89208e8_flows_F_85207E29.zip:.\results_C.75071231d89... sourcetype = csv

Analysis of one of the options:



Type	☑	Field	Value	Actions
Selected	☑	host ▾	GRR	⌄
	☑	source ▾	results_C.75071231d89208e8_flows_F_85207E29.zip:.\results_C.75071231d89208e8_flows_F_85207E29/ExportedNetworkConnection/from_NetworkConnection.csv	⌄
	☑	sourcetype ▾	csv	⌄
Event	□	ctime ▾	0	⌄
	□	family ▾	INET	⌄
	□	local_address_ip ▾	127.0.0.1	⌄
	□	local_address_port ▾	631	⌄
	□	metadata_client_age ▾	1970-01-01 00:00:00	⌄
	□	metadata_client_urn ▾	aff4:/C.75071231d89208e8	⌄
	□	metadata_deprecated_session_id ▾	None	⌄
	□	metadata_hardware_info_bios_release_date ▾	12/01/2006	⌄
	□	metadata_hardware_info_bios_rom_size ▾	128 kB	⌄
	□	metadata_hardware_info_bios_vendor ▾	innotek GmbH	⌄
	□	metadata_hardware_info_bios_version ▾	VirtualBox	⌄
	□	metadata_hardware_info_serial_number ▾	0	⌄
	□	metadata_hardware_info_system_family ▾	Virtual Machine	⌄
	□	metadata_hardware_info_system_manufacturer ▾	innotek GmbH	⌄
	□	metadata_hardware_info_system_product_name ▾	VirtualBox	⌄
	□	metadata_hardware_info_system_sku_number ▾	Not Specified	⌄



	□	metadata_hardware_info_system_manufacturer ▾	innotek GmbH	⌄
	□	metadata_hardware_info_system_product_name ▾	VirtualBox	⌄
	□	metadata_hardware_info_system_sku_number ▾	Not Specified	⌄
	□	metadata_hardware_info_system_uuid ▾	832C2B91-0DBF-4444-9024-4B61BEE36DAD	⌄
	□	metadata_hostname ▾	jackson-VirtualBox	⌄
	□	metadata_kernel_version ▾	5.4.0-135-generic	⌄
	□	metadata_mac_address ▾	080027c7d6da	⌄
	□	metadata_original_timestamp ▾	None	⌄
	□	metadata_os ▾	Linux	⌄
	□	metadata_os_release ▾	Ubuntu	⌄
	□	metadata_os_version ▾	18.4	⌄
	□	metadata_source_urn ▾	aff4:/C.75071231d89208e8/flows/F:85207E29	⌄
	□	metadata_timestamp ▾	2022-12-08 07:51:11	⌄
	□	metadata_uname ▾	Linux-debian-buster/sid	⌄
	□	metadata_usernames ▾	[u'jackson']	⌄
	□	pid ▾	659	⌄
	□	remote_address_port ▾	0	⌄
	□	state ▾	LISTEN	⌄
	□	type ▾	SOCK_STREAM	⌄
Time ⊕		_time ▾	2022-12-08T00:00:00.000-05:00	
Default	□	index ▾	main	⌄