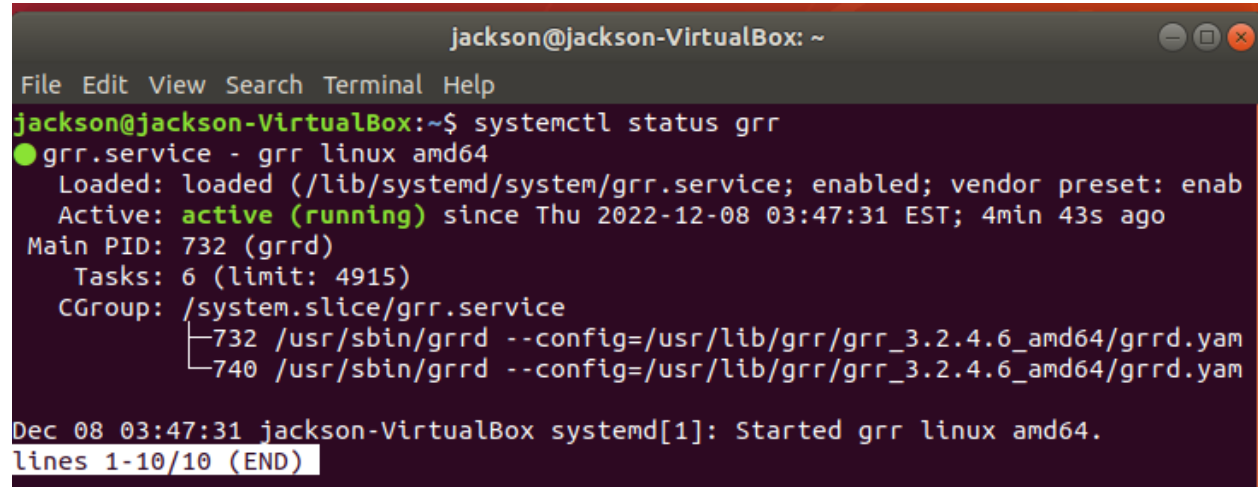


Assignment #4

Installing GRR Server + Client

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

A terminal window titled 'jackson@jackson-VirtualBox: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the command 'systemctl status grr' and its output. The output indicates that 'grr.service' is loaded and active (running) since Thursday, December 8, 2022, at 03:47:31 EST. It lists the main PID as 732 (grrd) and shows two tasks: PID 732 and PID 740, both running '/usr/sbin/grrd' with specific configuration files. At the bottom, a system log entry shows 'Started grr linux amd64.' and the prompt 'lines 1-10/10 (END)' is visible.

```
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)
```

Name: Jackson Yuan
Student #: 991302821

The image shows a desktop environment with a terminal window and a web browser. The terminal window, titled 'jackson@jackson-VirtualBox: ~', displays the command 'systemctl status grr-server' and its output. The output indicates that the 'grr-server.service' is loaded and enabled, but its active status is 'active (exited)' since Thursday, December 8, 2022, at 03:47:31 EST, 5 minutes ago. It also shows the process ID as 734 and the main PID as 734, with a status of 'SUCCESS'. Below the terminal output, there are system logs for 'systemd[1]' showing the starting and starting of the GRR Service. The web browser, titled 'GRR | Home', shows the GRR interface. The browser's address bar displays 'localhost:8000/#'. The interface includes a search box, a 'User: admin' indicator, and a timestamp '2022-12-08 08:54:10 UTC'. The main content area is titled 'Welcome to GRR' and contains instructions on how to query for a system. Below this, there are two sections: 'Recently Accessed Clients' and 'Recently Created Hunts', both of which currently show 'None.'.

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


Activities Firefox Web Browser Thu 03:54
GRR | Home
localhost:8000/#
User: admin 2022-12-08 08:54:10 UTC Search Box 0
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.
API Help Report a problem GRR Version

Name: Jackson Yuan
Student #: 991302821

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:



User: admin2022-12-08 08:55:11 UTC

Search Box

0

ackson-VirtualBox
Status: 🟡 1 hours ago
localhost

Host Information
Start new flows
Browse Virtual Filesystem

<input type="checkbox"/>	Online	Subject	Host	OS Version	MAC	Username	First Seen	Client version	Labels
<input type="checkbox"/>	🟡	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	

Name: Jackson Yuan
Student #: 991302821

Running investigating network aspect:

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

User: admin 2022-12-08 09:10:28 UTC

Search Box

0

jackson-VirtualBox
Status: 2 minutes ago
localhost

Host Information

Start new flows

Browse Virtual Filesystem

Manage launched flows

Advanced

MANAGEMENT

Cron Job Viewer

Hunt Manager

Show Statistics

Advanced

CONFIGURATION

Manage Binaries

Settings

Artifact Manager

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

Listening only ☐

Notify at Completion ☒

Advanced

Output Plugins +

Launch

Checking stored finished results:

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

User: admin 2022-12-08 09:11:24 UTC

Search Box

0

jackson-VirtualBox
Status: 3 minutes ago
localhost

Host Information

Start new flows

Browse Virtual Filesystem

Manage launched flows

Advanced

MANAGEMENT

Cron Job Viewer

Hunt Manager

Show Statistics

Advanced

CONFIGURATION

Manage Binaries

Settings

Artifact Manager

✓	F:85207E29	Netstat	2022-12-08 01:43:21 UTC	2022-12-08 01:43:23 UTC	admin
⚠		Flow finished normally.			
⚠		efoxHistory	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

Please select a flow to see its details here.

Name: Jackson Yuan
Student #: 991302821

Downloaded as a .csv file:

Flow Information Requests **Results** Log API

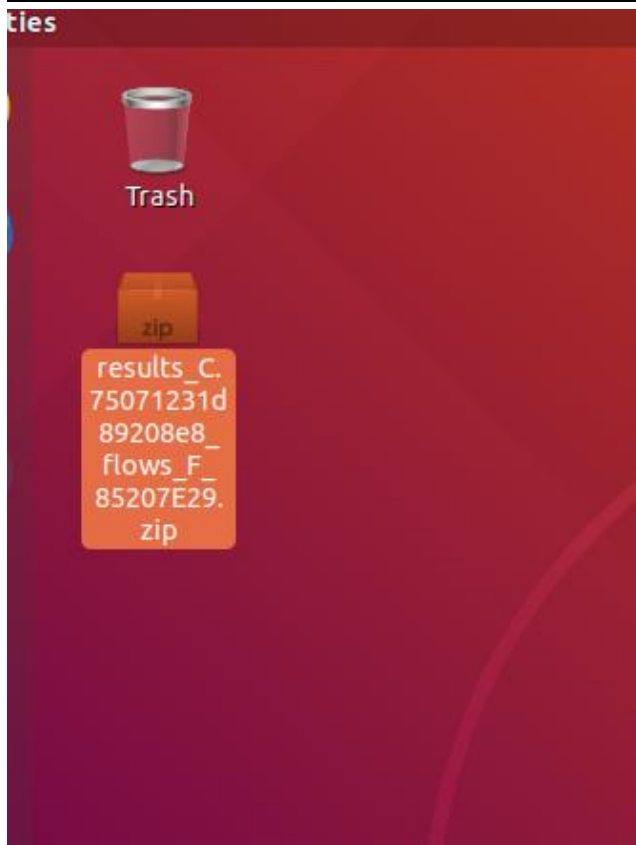
Download As: CSV (zipped)

15 entries

Value

Family	INET
Type	SOCK_STREAM
Ip	127.0.0.53

API Help Report a problem GRR Version



Name: Jackson Yuan
Student #: 991302821

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

The screenshot shows the Splunk 'Add Data' workflow. At the top, there's a navigation bar with 'splunk>enterprise' and 'Apps'. Below it, a progress bar indicates the current step is 'Select Source', with other steps being 'Input Settings', 'Review', and 'Done'. A '< Back' button and a 'Next >' button are visible. The main content area is titled 'Select Source' and contains instructions: '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](#)'. A warning icon and text state: 'Preview is not supported for this archive file, but it can still be indexed.' Below this, it says 'Selected File: results_C.75071231d89208e8_flows_F_85207E29.zip' and provides a 'Select File' button. A large rectangular box is intended for dropping the file, with the text 'Drop your data file here' and 'The maximum file upload size is 500 Mb' below it.

Splunk search query:

The screenshot shows the Splunk search interface. At the top, there's a navigation bar with 'splunk>enterprise' and 'Apps'. Below it, a dark bar contains navigation links: 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The main content area is titled 'New Search'. A search bar contains the query: 'source="results_C.75071231d89208e8_flows_F_85207E29.zip:*" host="GRR"'. Below the search bar, it shows '✓ 227 events (before 12/8/22 5:15:47.000 AM)' and a 'No Event Sampling' dropdown. At the bottom, there are tabs for 'Events (227)', 'Patterns', 'Statistics', and 'Visualization', with 'Events (227)' being the active tab.

Name: Jackson Yuan
Student #: 991302821

Results:

New Search

Save As>Create Table ViewClose

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

All time

✓ 227 events (before 12/8/22 5:15:47:000 AM) No Event Sampling

Job▶▶▶▶▶▶Smart Mode▶

Events (227)PatternsStatisticsVisualization

Format TimelineZoom OutZoom to SelectionDeselect1 hour per column

ListFormat20 Per Page▶< Prev12345678...Next>

< Hide FieldsAll Fields

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
a date_zone 1

i	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

Name: Jackson Yuan
Student #: 991302821

Analysis of one of the options:

Type	<input checked="" type="checkbox"/> Field	Value	Actions
Selected	<input checked="" type="checkbox"/> host ▾	GRR	▾
	<input checked="" type="checkbox"/> source ▾	results_C.75071231d89208e8_flows_F_85207E29.zip:\results_C.75071231d89208e8_flows_F_85207E29/ExportedNetworkConnection/from_NetworkConnection.csv	▾
	<input checked="" type="checkbox"/> sourcetype ▾	csv	▾
Event	<input type="checkbox"/> ctime ▾	0	▾
	<input type="checkbox"/> family ▾	INET	▾
	<input type="checkbox"/> local_address_ip ▾	127.0.0.1	▾
	<input type="checkbox"/> local_address_port ▾	631	▾
	<input type="checkbox"/> metadata_client_age ▾	1970-01-01 00:00:00	▾
	<input type="checkbox"/> metadata_client_urn ▾	aff4:/C.75071231d89208e8	▾
	<input type="checkbox"/> metadata_deprecated_session_id ▾	None	▾
	<input type="checkbox"/> metadata_hardware_info_bios_release_date ▾	12/01/2006	▾
	<input type="checkbox"/> metadata_hardware_info_bios_rom_size ▾	128 kB	▾
	<input type="checkbox"/> metadata_hardware_info_bios_vendor ▾	innotek GmbH	▾
	<input type="checkbox"/> metadata_hardware_info_bios_version ▾	VirtualBox	▾
	<input type="checkbox"/> metadata_hardware_info_serial_number ▾	0	▾
	<input type="checkbox"/> metadata_hardware_info_system_family ▾	Virtual Machine	▾
	<input type="checkbox"/> metadata_hardware_info_system_manufacturer ▾	innotek GmbH	▾
	<input type="checkbox"/> metadata_hardware_info_system_product_name ▾	VirtualBox	▾
	<input type="checkbox"/> metadata_hardware_info_system_sku_number ▾	Not Specified	▾
	<input type="checkbox"/> metadata_hardware_info_system_uuid ▾	832C2B91-0DBF-4444-9024-4B61BEE36DAD	▾
	<input type="checkbox"/> metadata_hostname ▾	jackson-VirtualBox	▾
	<input type="checkbox"/> metadata_kernel_version ▾	5.4.0-135-generic	▾
	<input type="checkbox"/> metadata_mac_address ▾	080027c7d6da	▾
	<input type="checkbox"/> metadata_original_timestamp ▾	None	▾
	<input type="checkbox"/> metadata_os ▾	Linux	▾
	<input type="checkbox"/> metadata_os_release ▾	Ubuntu	▾
	<input type="checkbox"/> metadata_os_version ▾	18.4	▾
	<input type="checkbox"/> metadata_source_urn ▾	aff4:/C.75071231d89208e8/flows/F:85207E29	▾
	<input type="checkbox"/> metadata_timestamp ▾	2022-12-08 07:51:11	▾
	<input type="checkbox"/> metadata_uname ▾	Linux-debian-buster/sid	▾
	<input type="checkbox"/> metadata_usernames ▾	[u'jackson']	▾
	<input type="checkbox"/> pid ▾	659	▾
	<input type="checkbox"/> remote_address_port ▾	0	▾
	<input type="checkbox"/> state ▾	LISTEN	▾
	<input type="checkbox"/> type ▾	SOCK_STREAM	▾
Time ⚙	<input type="checkbox"/> _time ▾	2022-12-08T00:00:00.000-05:00	
Default	<input type="checkbox"/> index ▾	main	▾