

# Configuration Manual

MSc Research Project  
MSc in Cyber Security

Athul Antony  
Student ID: 20242239

School of Computing  
National College of Ireland

Supervisor: Rohit Verma

**National College of Ireland**  
**MSc Project Submission Sheet**  
**School of Computing**



**Student Name:** Athul Antony

**Student ID:** 20242239

**Programme:** MSc In Cyber Security

**Year:** 2021-2022

**Module:** Research Project

**Lecturer:** Rohit Verma

**Submission**

**Due Date:** 15 Aug 2022

**Project Title:** How to improve efficiency of Linux Forensics?

**Word**

**Count:** 1180..... **Page Count:** .....9.....

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

**Signature:** Athul.....

**Date:** 15/08/2022.....

**PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST**

Attach a completed copy of this sheet to each project (including multiple copies)	<input type="checkbox"/>
<b>Attach a Moodle submission receipt of the online project submission,</b> to each project (including multiple copies).	<input type="checkbox"/>
<b>You must ensure that you retain a HARD COPY of the project,</b> both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	<input type="checkbox"/>

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

<b>Office Use Only</b>	
Signature:	
Date:	
Penalty Applied (if applicable):	

# Configuration Manual

Athul Antony  
Student ID: 20242239

## 1 Forensic tool AVML

AVML tool is readily available on GitHub. The newest release of the file will be downloaded into the path `"/home/ubuntu/Downloads"`. Since the file will not have readable permission, 775 permissions will be given to the file using `chmod`. If the `avml` file is run without specifying a filename at end it will show error since a file is required to save the output obtained after running the `avml` file. Since output of AVML will be a memory dump the filename will be given as `memory.dmp`. The command `./avml memory.dmp` will be run. Depending on the RAM given to the Ubuntu system the time will vary in collecting the memory. After a short file `memory.dmp` file will be created with size equal to that of RAM allocated to the Linux machine. This is shown in Figure 1. In this case since the RAM allocated was around 4 GB the size of the file created will also be same. The memory dump that will be obtained will be in LiME format and will be a binary file. To analyze this binary file volatility can be used. Volatility is an open-source framework that will aid in memory forensics. From GitHub the https clone of the volatility can be copied. Using `"git clone"` command the volatility can be cloned into the Ubuntu system as shown in Figure 2. Once done volatility directory will be visible in the Downloads directory. There is compilation file by the name of Makefile that can be viewed under the path `"/home/ubuntu/Downloads/volatility/tools/linux"`. To compile this file `dwarfdump` is required which can be installed with the help of `apt install`. Once this is installed the command `"make"` can be given which will then executes the volatility and creates `"module.dwarf"` file in the same directory `"/home/ubuntu/Downloads/volatility/tools/linux"`. This is shown in Figure 3. The main purpose of this is to have volatility profile specific to kernel version of the ubuntu system.

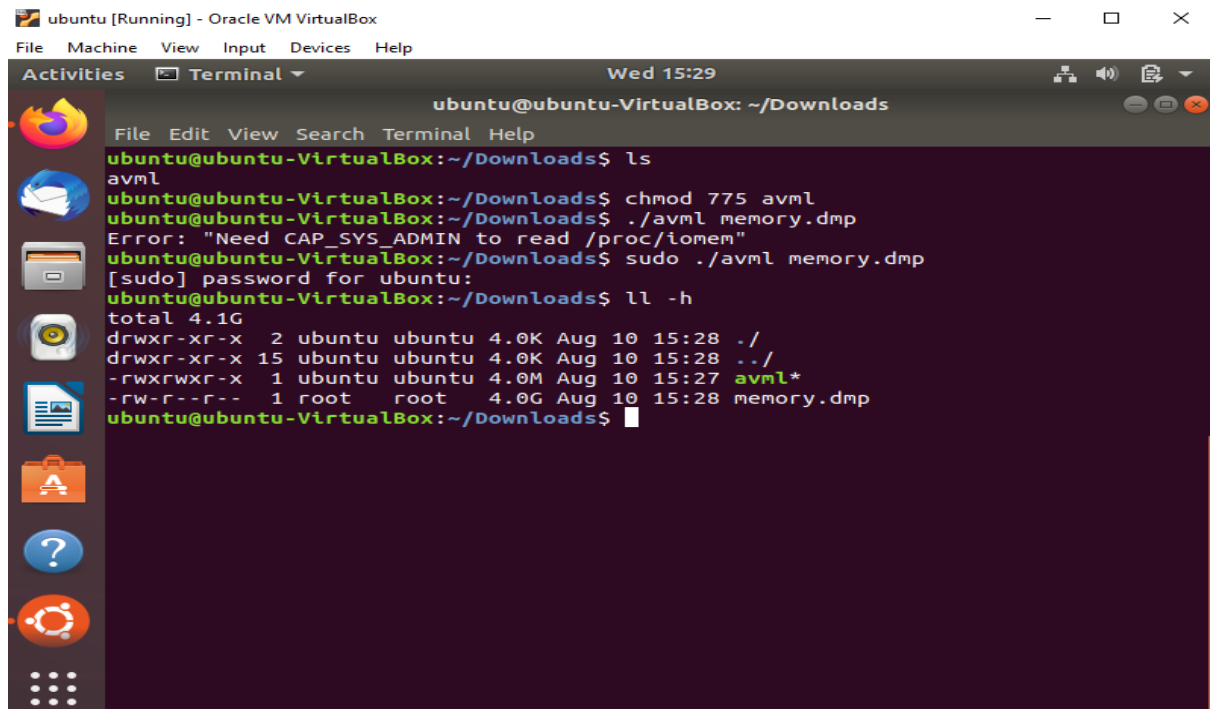


Figure 1: Initiating AVML to create memory dump

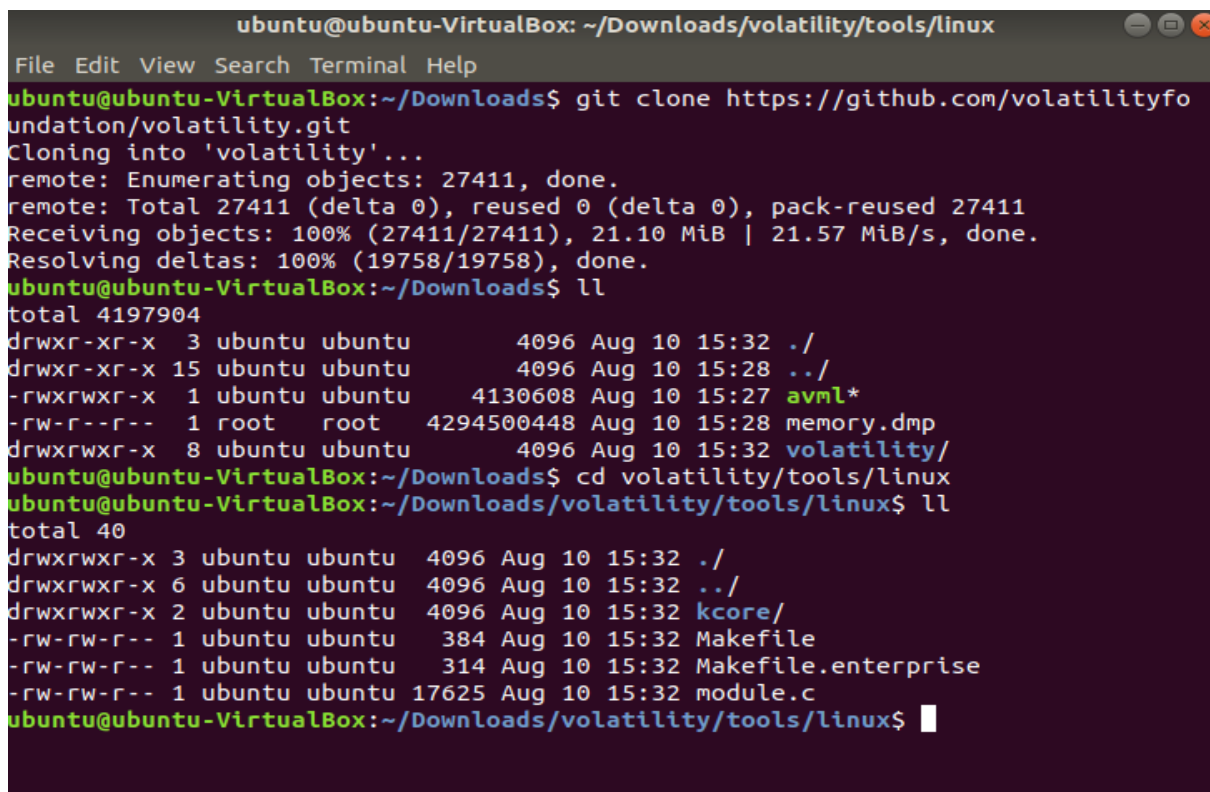


Figure 2: Cloning volatility

```

ubuntu@ubuntu-VirtualBox:~/Downloads/volatility/tools/linux$ ll
total 3328
drwxrwxr-x 3 ubuntu ubuntu 4096 Aug 10 15:40 ./
drwxrwxr-x 6 ubuntu ubuntu 4096 Aug 10 15:39 ../
drwxrwxr-x 2 ubuntu ubuntu 4096 Aug 10 15:39 kcore/
-rw-rw-r-- 1 ubuntu ubuntu 384 Aug 10 15:39 Makefile
-rw-rw-r-- 1 ubuntu ubuntu 314 Aug 10 15:39 Makefile.enterprise
-rw-rw-r-- 1 ubuntu ubuntu 17625 Aug 10 15:39 module.c
-rw-rw-r-- 1 ubuntu ubuntu 3363044 Aug 10 15:40 module.dwarf

```

**Figure 3: Compiling Makefile to create module.dwarf**

The next step is to create the zip archive of the volatility profile. The zip file should contain the newly compiled module.dwarf file and debug symbols found in the system.map file of the currently running kernel. The name of the zip file can be given same as that of the kernel version of the system but will help if there are multiple profiles within the system as shown in Figure 4. This zip file can be feed into volatility to analyze the memory image, but it needs to be placed where it can be accessed by the volatility. So the zip file will be moved to a specific location, by using “mv” command, inside the volatility directory “/volatility/volatility/plugins/overlays/linux/”.

```

ubuntu@ubuntu-VirtualBox: ~/Downloads
File Edit View Search Terminal Help
ubuntu@ubuntu-VirtualBox:~/Downloads$ ll
total 4197904
drwxr-xr-x 3 ubuntu ubuntu 4096 Aug 10 15:38 ./
drwxr-xr-x 15 ubuntu ubuntu 4096 Aug 10 15:28 ../
-rwxrwxr-x 1 ubuntu ubuntu 4130608 Aug 10 15:27 avml*
-rw-r--r-- 1 root root 4294500448 Aug 10 15:28 memory.dmp
drwxrwxr-x 8 ubuntu ubuntu 4096 Aug 10 15:39 volatility/
ubuntu@ubuntu-VirtualBox:~/Downloads$ uname -a
Linux ubuntu-VirtualBox 5.4.0-124-generic #140~18.04.1-Ubuntu SMP Fri Aug 5 11:
43:34 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
ubuntu@ubuntu-VirtualBox:~/Downloads$ sudo zip ubuntu_5.4.0-124-generic.zip ./v
olatility/tools/linux/module.dwarf /boot/System.map-5.4.0-124-generic
adding: volatility/tools/linux/module.dwarf (deflated 91%)
adding: boot/System.map-5.4.0-124-generic (deflated 79%)
ubuntu@ubuntu-VirtualBox:~/Downloads$ ll
total 4199148
drwxr-xr-x 3 ubuntu ubuntu 4096 Aug 10 15:45 ./
drwxr-xr-x 15 ubuntu ubuntu 4096 Aug 10 15:28 ../
-rwxrwxr-x 1 ubuntu ubuntu 4130608 Aug 10 15:27 avml*
-rw-r--r-- 1 root root 4294500448 Aug 10 15:28 memory.dmp
-rw-r--r-- 1 root root 1273055 Aug 10 15:45 ubuntu_5.4.0-124-generic.zi
p
drwxrwxr-x 8 ubuntu ubuntu 4096 Aug 10 15:39 volatility/
ubuntu@ubuntu-VirtualBox:~/Downloads$

```

**Figure 4: Creating zip file for volatility**

The newly installed profile can be seen with the help of the command “python vol.py –info | more”. After this using python we can point to the memory dump file created by AVML and specify the newly created profile to list all the activities that has been going on in the Ubuntu system. This is shown in Figure 5. By using grep command we can get the details for specific applications. The commands “python vol.py -f ../memory.dmp –profile=Linuxubuntu\_5\_4\_0-124-genericx64 linux\_netstat | more” will list all the network activities that has been carried out and “python vol.py -f ../memory.dmp –profile=Linuxubuntu\_5\_4\_0-124-genericx64 linux\_lsof | more” will list all the open files. These outputs obtained will help in forensic investigation depending on various needs of the forensic investigator.

```

Profiles
-----
Linuxubuntu_5_4_0-124-genericx64 - A Profile for Linux ubuntu_5.4.0-124-generic
x64
VistaSP0x64 - A Profile for Windows Vista SP0 x64
VistaSP0x86 - A Profile for Windows Vista SP0 x86
VistaSP1x64 - A Profile for Windows Vista SP1 x64
VistaSP1x86 - A Profile for Windows Vista SP1 x86
VistaSP2x64 - A Profile for Windows Vista SP2 x64
VistaSP2x86 - A Profile for Windows Vista SP2 x86
Win10x64 - A Profile for Windows 10 x64
Win10x64_10240_17770 - A Profile for Windows 10 x64 (10.0.10240.177
70 / 2018-02-10)
Win10x64_10586 - A Profile for Windows 10 x64 (10.0.10586.306
/ 2016-04-23)
Win10x64_14393 - A Profile for Windows 10 x64 (10.0.14393.0 /
2016-07-16)
Win10x64_15063 - A Profile for Windows 10 x64 (10.0.15063.0 /
2017-04-04)
Win10x64_16299 - A Profile for Windows 10 x64 (10.0.16299.0 /
2017-09-22)
Win10x64_17134 - A Profile for Windows 10 x64 (10.0.17134.1 /
2018-04-11)

```

Figure 5: Volatility profile created

## 2 Remote Acquisition GRR

Firstly MySQL will be downloaded into the Ubuntu machine if its installed. By using “sudo apt install mysql-server” we can install MySQL. A database for the grr needs to be created into the MySQL server. This is shown in Figure 6. The latest version of GRR will be downloaded from the official site with the help of “wget” and will be installed. To ensure that GRR server will be able to communicate with the datastore GRR will need to configure datastore and IP address to communicate with the server. Hence while installing GRR, it will prompt to ask for information like hostname, port, username, database and IP address. This is shown in figure 7. An admin user will be created, and password will be set up to login to the GRR server. Once these are done GRR installation will be completed.

```
ubuntu@ubuntu-VirtualBox: ~/Downloads
File Edit View Search Terminal Help
ubuntu@ubuntu-VirtualBox:~/Downloads$ sudo mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2
Server version: 5.7.39-0ubuntu0.18.04.2 (Ubuntu)

Copyright (c) 2000, 2022, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> CREATE USER 'grr'@'localhost' IDENTIFIED BY 'password';
Query OK, 0 rows affected (0.01 sec)

mysql> CREATE DATABASE grr;
Query OK, 1 row affected (0.00 sec)

mysql> GRANT ALL ON grr.* TO 'grr'@'localhost';
Query OK, 0 rows affected (0.00 sec)

mysql> exit
Bye
ubuntu@ubuntu-VirtualBox:~/Downloads$
```

**Figure 6: Setting up GRR database**

```
-GRR Datastore-
For GRR to work each GRR server has to be able to communicate with
the datastore. To do this we need to configure a datastore.

GRR will use MySQL as its database backend. Enter connection details:
MySQL Host [localhost]: localhost
MySQL Port (0 for local socket) [0]: 53
MySQL Database [grr]: grr
MySQL Username [root]: root
Please enter password for database user root:
Configure SSL connections for MySQL? [yN]: [N]: n
Successfully connected to MySQL with the provided details.

-GRR URLs-
For GRR to work each client has to be able to communicate with the
server. To do this we normally need a public dns name or IP address
to communicate with. In the standard configuration this will be used
to host both the client facing server and the admin user interface.
```

**Figure 7: Configuring datastore and communication for GRR server**

Once installation of GRR is completed we can access the GUI of GRR server in the browser by entering the IP address port details in which GRR is set up. As shown in the Figure 9 GRR server is launched by entering “10.0.2.15:8000” and giving the admin details. in the Binaries section of GRR server we can download the

required GRR client. We can unpack the GRR client with dpkg command. Once GRR client gets installed we can click on GRR server again it will show the available client details as shown in Figure 10.

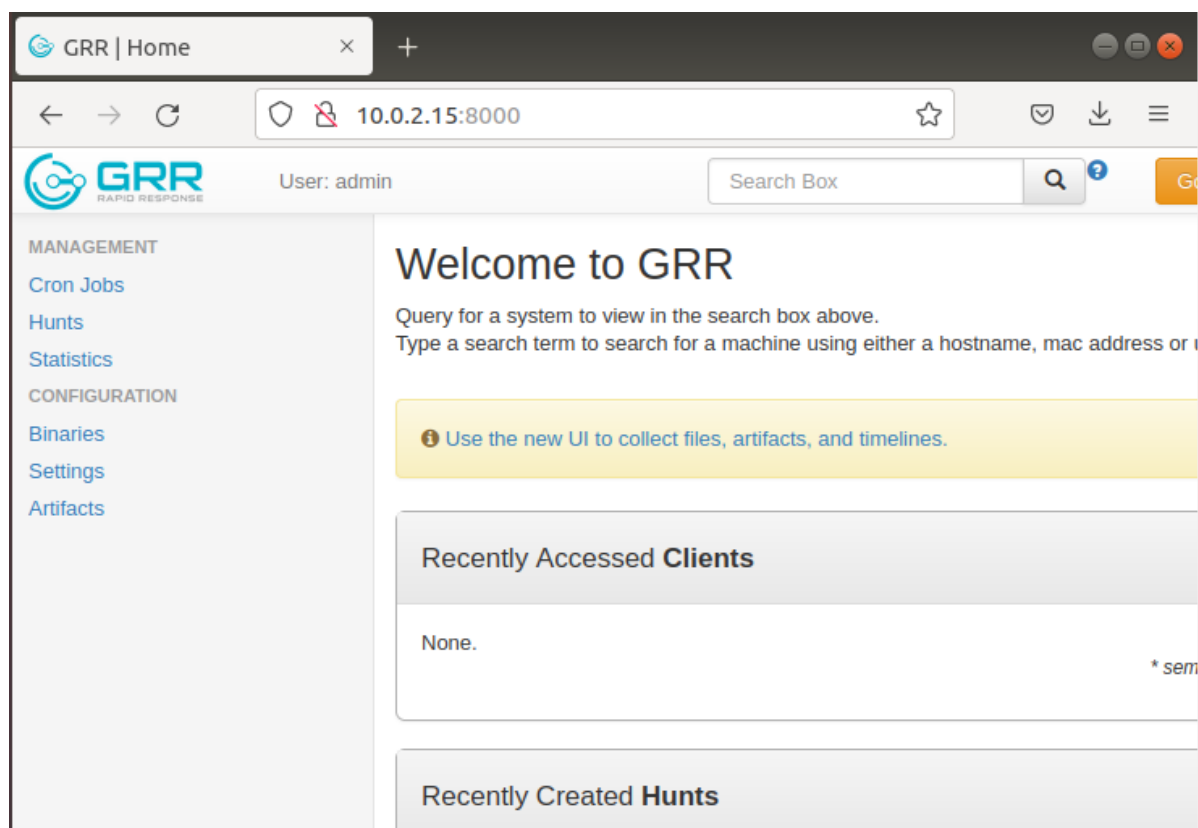
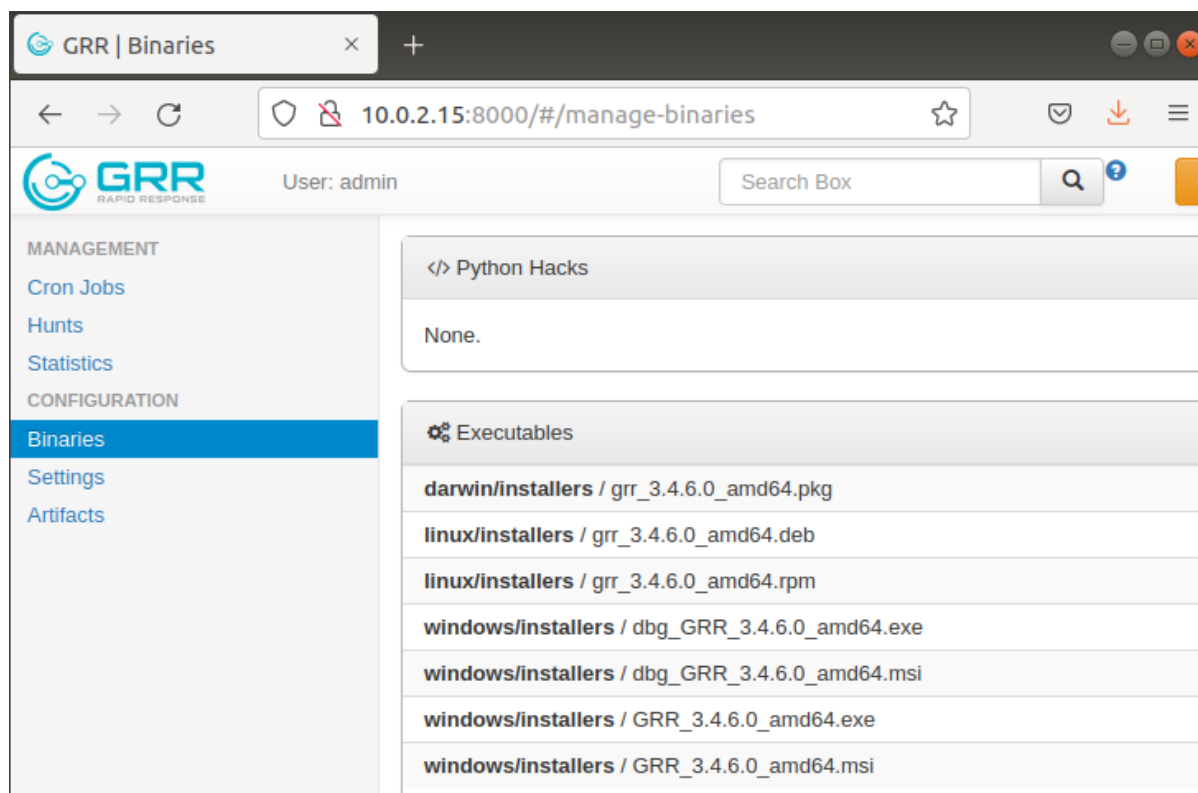
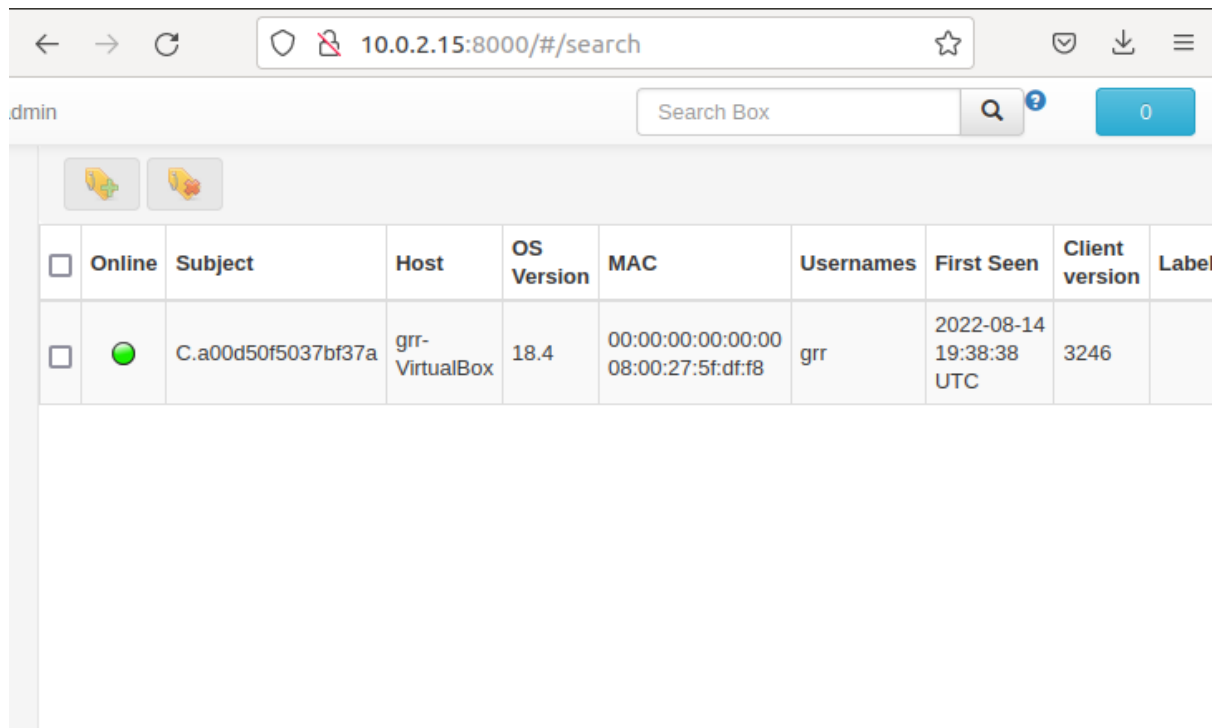



Figure 8: GRR server GUI





**Figure 9: Binaries showing list of GRR client**



<input type="checkbox"/>	Online	Subject	Host	OS Version	MAC	Usernames	First Seen	Client version	Label
<input type="checkbox"/>		C.a00d50f5037bf37a	grr-VirtualBox	18.4	00:00:00:00:00:00 08:00:27:5f:df:f8	grr	2022-08-14 19:38:38 UTC	3246	

**Figure 10: GRR client details**

## References

www.binary-zone.com. (n.d.). *Acquiring Linux Memory using AVML and Using it with Volatility / B!n@ry*. [online] Available at: <https://www.binary-zone.com/2019/06/20/acquiring-linux-memory-using-avml-and-using-it-with-volatility/> [Accessed 11 Aug. 2022].

grr-doc.readthedocs.io. (n.d.). *Installing GRR Server — GRR documentation*. [online] Available at: <https://grr-doc.readthedocs.io/en/latest/installing-grr-server/index.html> [Accessed 13 Aug 2022].