Forensic Challenge

Based on
the
DFRWS RODEO CHALLENGE

Introduction:

This is your chance to take part in a computer forensics investigation, similar to what would happen in real life. We're asking you to play the part of the investigator and find what information you can about the evidence you have been given. In particular we're going to ask you to find specific bits of evidence that might help the police in their investigations.

Wave your hand if you have a question or get stuck and the lecturer will pop over and give you a tip.

Scenario:

The city of New Orleans passed a law in 2014 making possession of ten or more unique rhinoceros images a serious crime. The network administrator at the University of New Orleans recently alerted police when his instance of RHINOVORE flagged illegal rhino traffic. Evidence in the case includes a computer and USB key seized from one of the University's labs. Unfortunately, the computer had no hard drive. The USB key was imaged and a copy of the image is on your forensic workstation.

In addition to the USB key drive image, three network traces and an email are also available— these were provided by the network administrator and involve the machine with the missing hard drive. The suspect is the primary user of this machine, who has been pursuing his Ph.D. at the University and is called Mallory.

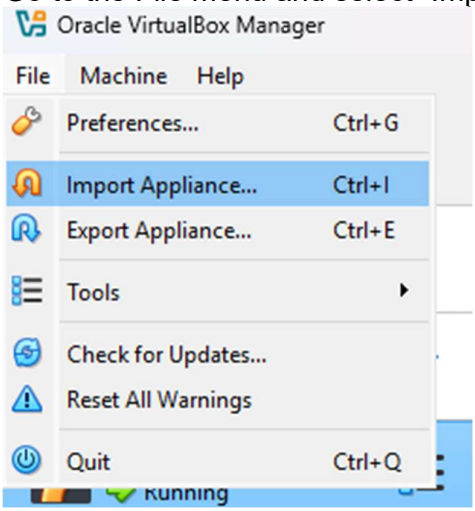
Your task:

Recording the information as if it were a real forensics challenge, recover as many rhino pictures from the available evidence as you can and find out as many usernames and passwords as you can. See if you can also answer the following questions –

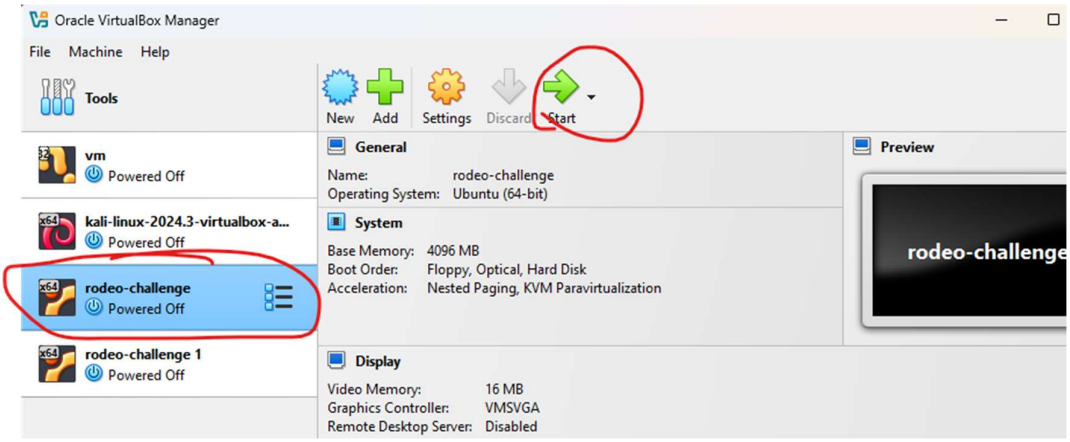
- What happened to the hard drive in the computer? Where is it now? Is it worth spending police time recovering it?
- What happened to the USB key?
- Is there any evidence that connects the USB key and the network traces? If so, what?
- What is recoverable from the dd image of the USB key?
- Who gave the accused a telnet/ftp account?
- What's the username/password for the account?
- Do you have enough evidence to prosecute?

Stage 0 - Getting Started

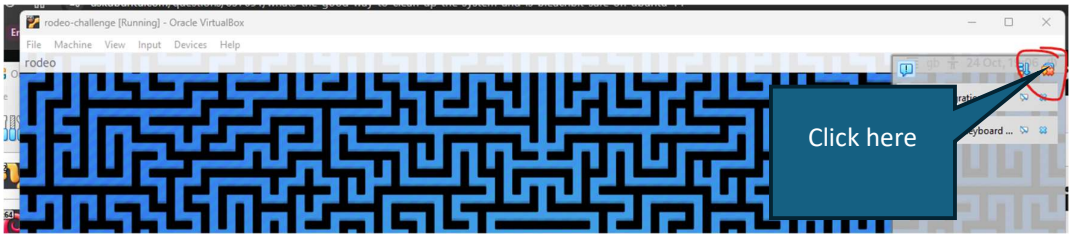
1. Download the virtual machine from Moodle (it's 5.9GB, so it may take a few minutes). You'll get a warning saying that it's too big for Google to scan for viruses, click "Download anyway"
2. Run the programme VirtualBox from the start menu
3. Go to the File menu and select "Import Appliance…"



4. Make sure the source is "Local File System" and browse to where you downloaded the VM to (normally your Downloads folder) and click "Finish" (leave the rest of the settings the same.
5. Wait (it will take a few minutes)
6. Click on the VM and then click on the start button



7. You will get messages about Auto capture of keyboard and mouse. Just click on the little “x” at the top of the notification window to get rid of them -



8. Log in with the username `student` and the password `student`
9. On the desktop you will see a folder called GBS-forensic-challenge – this contains our evidence files from the case and the path to the folder is `/home/student/Desktop/GBS-forensic-challenge/`
10. Just above the desktop, you’ll see the menu bar. On it, you'll see the start menu (), the button for the web browser () and the button for the command prompt ()
11. Press the command prompt button to open up a command prompt (you can have multiple command prompts open at the same time and it’s useful to have a few on the screen at any one time).


Start menu
1
2
3
4
Command Prompt
Home
Web browser
File System
Wastebasket
GBS-forens.
Folder with the evidence

Stage 1 - First steps, cracking the passwords:

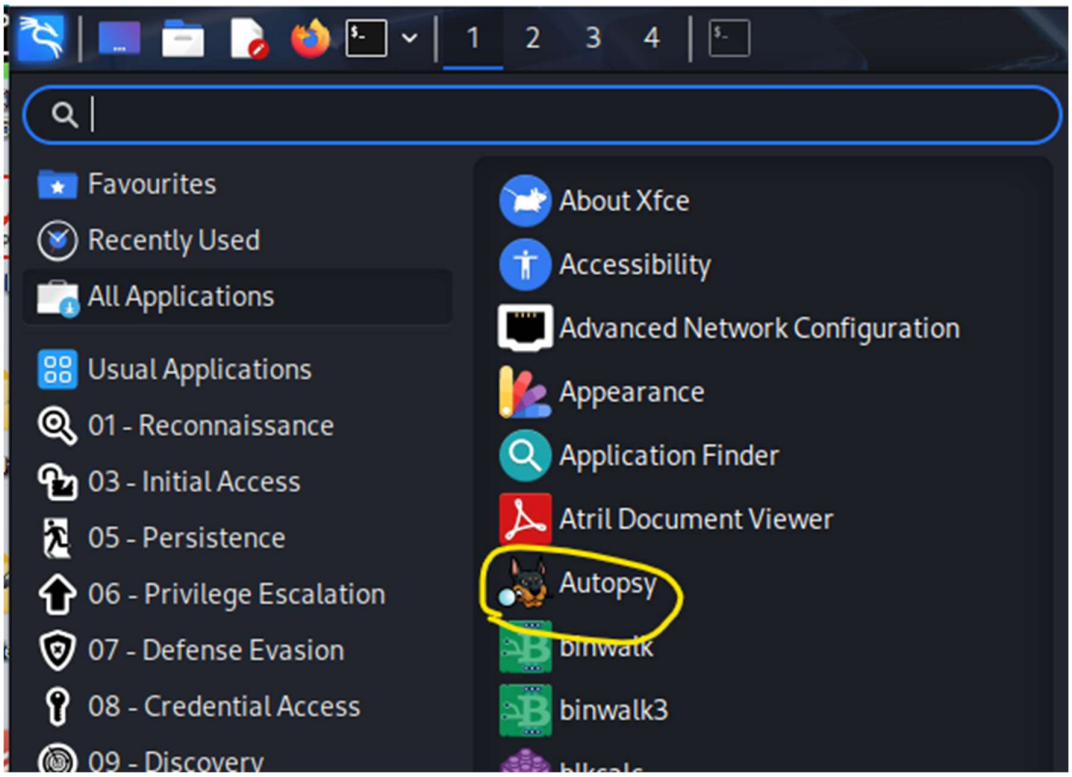
1) Finding out passwords can take a long time, so let's do that first. The file `jtr_passwd.txt` is a password file showing usernames and encrypted passwords of Mallory's associates. It would be useful if we could get the passwords used by these people as they are also suspects and people often use the same password on different accounts. Fortunately we have a program called *John the Ripper* which will help us do this. To start John, open up a command prompt window. At the command prompt that opens type

```
john /home/student/Desktop/GBS-forensic-challenge/jtr_passwd.txt
```

and see what passwords it finds. It will get some very quickly and others will take much longer. Record the one's it has retrieved quickly and leave it running. (Don't forget to look at the end to see what else it has found though)

Stage 2 - Looking at the USB stick

2) There is a tool called "autopsy" that we can use to help us manage the investigation. To start that, click on the start menu in the top right corner of the desktop (), select "all applications, and then click on the one called "autopsy"



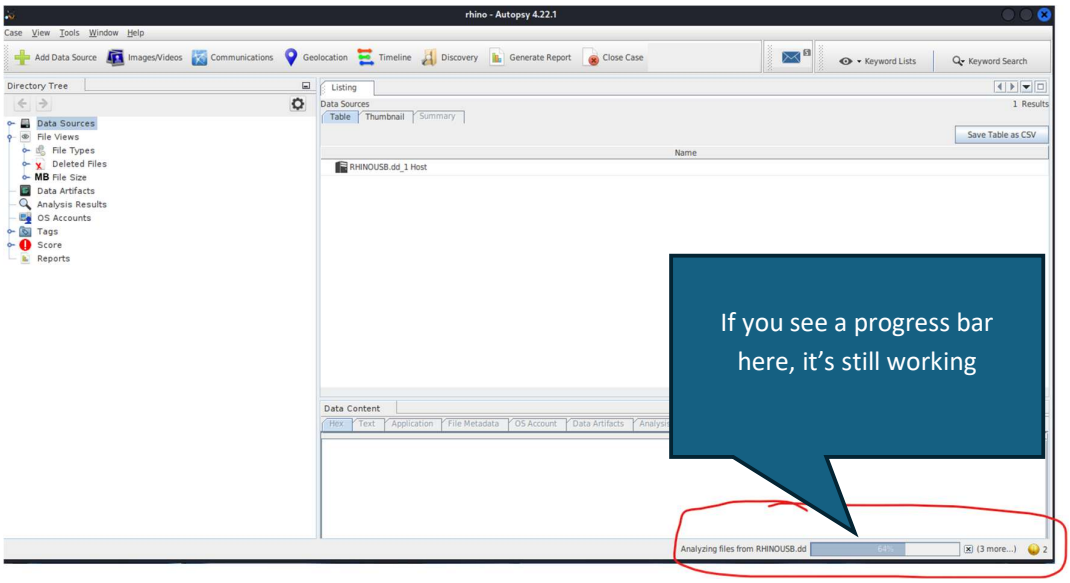
3) Click on the "New Case" button - you'll come up with a page with where you are asked for the case details, fill in the case name, call it "Rhino1", and browse to the location of the files (`/home/student/Desktop/GBS-forensic-challenge/`). Click on the "Next" button and then enter your name in the examiners part and then click on "Finish".

4) We now need to add in the data sources, starting with the USB image, so click on the "Add Data Source" button and fill in the details as follows (you

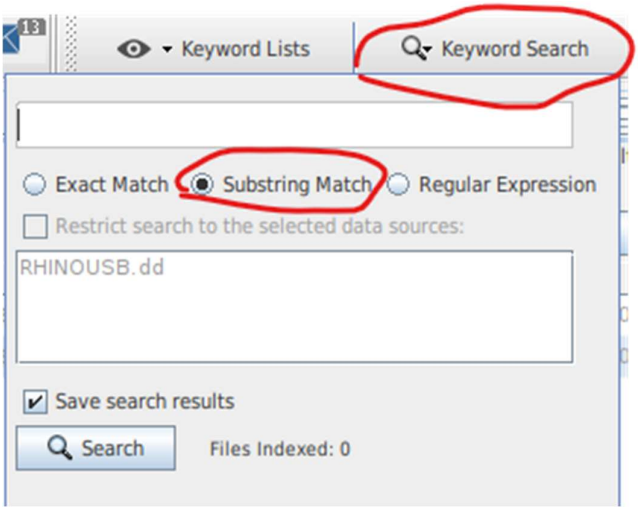
will need to click on the “Next” button add the end of each stage to go onto the next stage) –

- Select Host – select the “Generate new host name based on data source name”
- Select Data Source Type – select “Disk Image or VM File”
- Select Data Source – click browse and browse to `/home/student/Desktop/GBS-forensic-challenge/RHINOUSB.dd`
- Configure Ingest – untick the options “Android Analyzer (aLEAPP)”, “DJI Drone Analyzer”, “YARA Analyzer”, “iOS Analyzer (iLEAPP)”, and “Android Analyzer”
- Add Data Source – click the “Finish” button

4) Wait until the system has finished analysing the USB stick



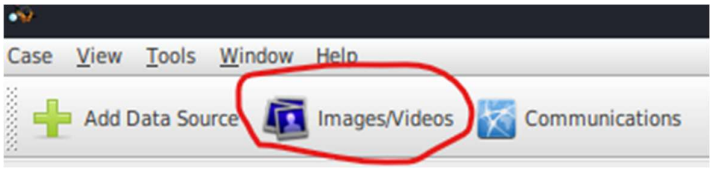
5) We’re now ready to search for some information, so let’s start by looking for keywords. Click on the “Keyword Search” button (top right), select “Substring Match” and try some potential words that you might want to look for.



6) Click on some of the results it's found. The information is organised into pages and you can scroll through and find out any other useful information. Try a few keywords and see what you find.

Stage 3 -Looking for pictures:

7) Autopsy will also extract any images you might have on the image. Click on the "Images/Videos" button and see what comes up –



8) We can use another tool called foremost which is sometimes a bit more useful and is run from the command prompt. To run foremost we use the command

```
foremost -o /home/student/Desktop/images
/home/student/Desktop/GBS-forensic-challenge/RHINOUSB.dd
```

(you'll need to type the command on the same line). This will extract any useful files on the USB image and put them in a folder called "images" on your desktop. You can click into this folder and see what images it's found.

Stage 4 - Digging in the network:

9) Click on the command prompt button (remember, it's the one on the task bar, to the right of the web browser icon and looks a bit like a DOS prompt) and in the command prompt, type

```
cd  /home/student/Desktop/GBS-forensic-challenge
```

and press the return key.

10) If we type

```
strings rhino.log | grep XXXX
```

where `XXXX` is what we want to search for, we can search all the files for keywords. Using this can you find evidence of an FTP login? (Hint – what do you need to log in to a machine? Look for those keywords)

11) If we type

```
strings rhino.log > rhino.txt
```

we can create a text file of all the strings which we can look at in a text editor by typing the command

```
mousepad rhino.txt
```

– see if you can find a username and password for your list in this.

12) We can even use foremost to look at network log files. To run foremost on the log files we use the command

```
foremost -o /home/student/Desktop/images2
/home/student/Desktop/GBS-forensic-challenge/rhino*.log
```

(again it's all on one line) – this time we're looking at the network logs to extract files! Once again click on the "*images2*" folder and have a look to see what you have found.

(Optional) Looking for pictures – the advanced way

13) The problem with using foremost on network traffic is that pictures may be in multiple packets and as such not reconstruct properly. However driftnet is a picture that will sniff network traffic for images. The problem with driftnet is it won't work with saved network traces like our log files. The program tcpreplay is a program that allows us to replay network traffic that has been stored in logs. See if you can work out how to use driftnet and tcpreplay together to see if there are any more rhino pictures in the traffic. To find out what a program does and how to use it, we can go back to our command prompt and type

```
man program_name
```

to find out what the program `program_name` does, *Hint 1*, you probably don't want to use a network interface that goes onto the network – fortunately there is a special interface called **lo** (short for loopback) that allows us to send a receive traffic on the same computer. *Hint 2,* the file rhino.log is very big so you probably want to apply a speedup factor there. *Hint 3,* you need to be a superuser to interact directly with the network. Fortunately, there is a command called `sudo` that will let you run any other command as the superuser. To use it, you type –

```
sudo <command_you_want_to_run_as_superuser>
```

Stage 5 – The email

14) The one thing we haven't looked at yet is the email file `Piccies.eml`. If you go to the command prompt and type

```
ls -lah
```

that will give you a breakdown of all the stats about the files in the directory you are currently in.

15) If you look at the email file, you can see it's rather large which suggests that there is an attachment in there. We can use the command munpack at the command line to extract the attachment –

```
munpack Piccies.eml
```

That will extract any attachments, which in this case is a large file containing a picture of some ferrets.

16) Investigate the file and the email to see if there is anything else there that's worth looking at. *Hint* – there is, but it won't be easy to find, so don't worry if you can't find it.

And finally

17) Go back and check to see how John has got on.

Useful commands

You might find these commands useful to use at the command line

Command	What it does
`apropos <WORD>`	Looks for <WORD> in the manual pages – used to find out what command does a particular task.
`cat <FILENAME>`	Displays the contents of `<FILENAME>`
`cd <DIRECTORY_NAME>`	Changes to the directory/folder named
`cd ..`	Go up to the directory above
`cd ~`	Go to the users home directory
`cp <ORIGINAL_FILE> <NEW_FILE>`	Make a copy of `<ORIGINAL_FILE>` to `<NEW_FILE>`
`cp <ORIGINAL_FILE> <DIRECTORY/NEW_FILE>`	Make a copy of `<ORIGINAL_FILE>` to `<NEW_FILE>` in the directory `<DIRECTORY>`
`less <FILENAME>`	Displays the contents of `<FILENAME>` a page at a time (press space to go to the next page)
`ls`	Lists what is in the current directory
`ls -lah`	Lists what is in the current directory and information about each file
`man <COMMAND>`	Gives the instructions (manual page) for `<COMMAND>`
`mousepad <FILENAME>`	Opens up `<FILENAME>`in a text editor
`mv <ORIGINAL_FILE> <NEW_FILE>`	Renames a file
`mv <ORIGINAL_FILE> <DIRECTORY/NEW_FILE>`	Moves `<ORIGINAL_FILE>` to a file called `<NEW_FILE>` in the directory `<DIRECTORY>`
`strings <FILENAME>`	Lists all the strings in `<FILENAME>`
`sudo <COMMAND>`	Runs the `<COMMAND>` as a superuser
`zip <FILENAME>` `unzip <FILENAME>`	Zip/Unzip `<FILENAME>`