Module	CMP209 – Digital Forensics
Module Lecturer	Dr Karl van der Schyff
Lab No	10
Due Date	complete before your next lab.

LAB INSTRUCTIONS

WHERE (and what) TO SUBMIT?	• Note that this lab is formative in nature. In other words, although you are expected to complete it, I do not require you to hand it in for assessment. Having said this, I am more than happy to give feedback if you wish to receive it.
WHAT ABOUT USING AI?	• Use of Generative AI Tools such as ChatGPT, DALL-E, Bard etc. is explicitly prohibited for this module's assessment (i.e., the court report). The output gleaned or generated from the tools mentioned and others that are similar relates to sources already published/available. **Also, be aware that the information obtained can be inaccurate or incomplete. Thus, all work should be your own.** If the assessment (i.e., court report) is found to have been plagiarised or to have used unauthorised AI tools, you will be referred to the Student Disciplinary Officer within the School and this may result in an Academic Misconduct charge.

LAB REQUIREMENTS

WHAT DO I NEED TO COMPLETE IT?	• Access to the analysis workstation, which is an Ubuntu VM that can be accessed via VMware Workstation. • You can also download the analysis VM from MLS via the tile labelled "*OneDrive link to analysis VM download files*". • Access to MLS to download these documents (and the supplementary docs), but also the John Doe image file. The image file is labelled *johnDoe.dd.gz*

AIM OF THIS LAB

The aim of this lab is to:

- Decrypt some of the evidence found on John Doe's disk image.

CORE LEARNING OUTCOMES

- Increased understanding and competence using the Linux operating system to perform digital forensics.
- Familiarization with the processes required to conduct a digital forensic investigation (read the supplementary docs for this). In particular, understanding,
  i. **How to systematically analyse the evidence that has been gathered thus far.**
  ii. **How to work with encrypted and password protected evidence.**
  iii. **How to produce a custom dictionary to use for password cracking.**

Digital Forensics and Encryption – Part 1 – Recovering GPG keys

Amongst the files on John Doe's disk is one called `birdpics.gpg`. From the name, it would seem to be relevant, but it's a gpg-encrypted file. In this lab we will investigate one way of obtaining access to the file. When gpg is used to encrypt a file, it uses a strong cryptographic key without which we can't decrypt the file. The use case for gpg encryption is usually that the file is sent over an insecure Internet connection. The receiver should already have access to the key. Anyone intercepting the file can't read it because they don't have the key, and using brute force approaches will take too long. We do, however, have access to John Doe's computer (via the image we created) and the key will be on there. It's actually stored in a file (called `secring.gpg`) which is protected by a much weaker password which we can expose via a brute force attack.

1. Use the loopback mounting technique to access John Doe's files. In particular, you should be looking for the `C:/Documents and Settings/johndoe/Application Data/GnuPG` directory.

2. Once located, copy the entire `GnuPG` directory to your `jd` directory on the analysis workstation. Once you have changed to the above directory you could run the following command to perform the copy:

   ```
   cp -r GnuPG/ ~/jd/GnuPG
   ```

3. Then, locate the `birdpics.gpg` file and copy it to your copy of the `GnuPG` directory.

4. Change into your copy of the `GnuPG` directory and use `chmod` to make all the files read only. Use the following command:

   ```
   chmod 400 *
   ```

Before proceeding, note that John the Ripper (JtR) sometimes gives an error when run from certain CPU architectures. As such, if step 5 below gives you an error I would advise you to use the Kali VM that is available within VMware Workstation on the lab workstations in 4511. Once, you have started running Kali go to step 18 within Part 3.

5. Convert the stored password from `gpg's` format to something our brute force tool (i.e., `john the ripper`) can work with. Note that I am assuming you are using the Ubuntu analysis VM. If you are using your own VM or workstation, these paths will likely differ.

   ```
   ~/Downloads/john-bleeding-jumbo/run/gpg2john secring.gpg > secring.jtr
   ```

6. Once converted, you can start the brute forcing process with this command. First, change to your john the ripper directory with the first command. Then, run the second brute force command.

   ```
   cd ~/Downloads/john-bleeding-jumbo/run/
   ./john ~/jd/GnuPG/secring.jtr
   ```

7. After some time (typically a few minutes) it should locate the password. At this point you should import John Doe's secret key with the file command listed below. Note that it will ask you for a password so please go ahead and enter the password recovered from step 6 (or step 23).

   ```
   gpg --import ~/jd/GnuPG/secring.gpg
   ```

8. Decrypt the `birdpics.gpg` with the following command. However, first change to your copy of the `GnuPG` directory:

```
d ~/jd/GnuPG/
gpg -d birdpics.gpg > birdpics.dat
```

9. Note that the above file is not actually a picture file. To find out what type of file it is use the following command:

```
file birdpics.dat
```

10. You will notice that it is actually a zip file. To rename it execute the following command:

```
mv birdpics.dat birdpics.zip
```

11. Once unzipped, inspect the images.

Digital Forensics and Encryption – Part 2 – Brute force vs. dictionary

Dictionary attacks are typically quicker than brute force attacks. So, where is the best source of words that John Doe is likely to have used as his password. Could it be his own disk? Note that if you were unable to run John the Ripper in step 5, you will also be unable to run steps 13 to 17. If this is the case, please go to step 24.

12. If you have not done so already, use the `strings` command to produce a list of all the words on John Doe's disk. Note that this command will take a few minutes to run:

```
strings johnDoe.dd >> johnDoe.dd.strings
```

13. Once completed, run `john the ripper` in dictionary mode. Remember to change to the correct `john the ripper` directory before attempting to run the command:

```
./john -wordlist:~/jd/johnDoe.dd.strings ~/jd/GnuPG/secring.jtr
```

14. Many people use the same password for a variety of their other systems and online passwords. Have a look around the installation of `Thunderbird (`on John Doe's disk) to see if you can find any stored passwords there.

15. From one of the earlier labs, you may have noticed that some of the PDF files recovered via the file carving process are password protected. Find the output directory where you stored the output from your file carving process. In that directory there will be another directory called `pdf.` Copy the contents of this directory to the `~/jd/encpdf` directory. Note that you will first have to create this directory.

16. You will need to create the hash file for each password protected PDF file using the `pdf2john.pl` tool which is available in the `run` directory of `john the ripper`. To achieve the latter, execute the following command. Note that the below command is using one of the PDF files as an example and that the paths in use are specific to the Ubuntu analysis VM:

```
./pdf2john.pl ~/jd/encpdf/RdrMsgENU.pdf > ~/jd/encpdf/RdrMsgENU.hash
```

17. Once the hash file has been created, you can use `john the ripper` to execute a brute force attack to obtain the password. Execute the following from the `john the ripper` directory:

    ```
    ./john ~/jd/encpdf/RdrMsgENU.hash
    ```

    Note that it will most probably take a few minutes to locate the password.

Digital Forensics and Encryption – Part 3 – Using Kali to crack secring.gpg

18. Log in to the Kali VM with the username `kali` and password `kali`.

19. Once you have logged in, copy the `secring.gpg` file from the Ubuntu analysis VM to Kali using `WinSCP`, for example. Any location would work, but it may be easier to simply paste it onto the desktop. By now you should know how to use `WinSCP` as we have used it to copy the evidence file to the analysis VM in an earlier week. First, you will have to ensure that the ssh service is installed and running.

    ```
    sudo apt-get install ssh
    ```

20. Restart the Kali VM and open a terminal again. Then start the `ssh` service with:

    ```
    systemctl start ssh
    ```

21. You will now be able to use `WinSCP`. Just remember to make a note of the ip address of the Kali VM using the `ifconfig` command before running `WinSCP`. **Once copied please disable the ssh service again using:**

    ```
    systemctl stop ssh
    ```

22. Change to the directory where you have placed the `secring.gpg` file (e.g., Desktop). Then execute the following command:

    ```
    gpg2john secring.gpg > secring.jtr
    ```

23. The above command will convert the file into the correct format. You are now ready to crack the password by running:

    ```
    john secring.jtr
    ```

    After a few moments you should see the password highlighted in orange within the terminal output. At this point, please return to step 7, which should be executed on the Ubuntu analysis VM.

Digital Forensics and Encryption – Part 4 – Dictionary attack in Kali

24. Copy your `johnDoe.dd.strings` file from Ubuntu to Kali using `WinSCP`. Ensure that it is in the same directory as your `secring.jtr` file. In other words, the file produced after executing step 12. You would have to enable the ssh service again if you disabled it. Just please remember to disable it again once you have completed step 26.

25. Once copied, run the following from the directory containing the `secring.jtr` file.

    ```
    john -wordlist:johnDoe.dd.strings secring.jtr
    ```

26. Copy the encrypted pdf files from the Ubuntu analysis VM to Kali and crack them using `john`. You will have to first convert them using the command `pdf2john` so please adapt the command line from step 16.

27. **Disable the ssh service on the Kali VM once you have copied all the files**.

Digital Forensics and Encryption – Part 4 – Using other approaches…

There are several other approaches you could use to crack the password given that it is technically a dictionary-based password. For example, you could try to use `hashcat` or some of the online password cracking utilities.