In this short lab I will be investigating logs to perform digital forensic on a system. To start I will run the SSH and Telnet honeypot Cowire which is designed to log brute force attacks and shell interaction by using the following command:

docker run -p 2222:2222/tcp cowrie/cowrie > honeypotLogs.txt

This command will run a new docker container based on the cowire/cowire image mapped to the tcp port 2222 allowing external communication. The standard output will then be directed to honeypotLogs.txt on our local machine.

Now I will open a second terminal and ssh through the open tcp port using the command:

ssh -p 2222 root@localhost

```
theia@theiadocker-bradleyrroff:/home/project$ ssh -p 2222 root@localhost
The authenticity of host '[localhost]:2222 ([::1]:2222)' can't be established.
ED25519 key fingerprint is SHA256:gDmtkw1h1nPckvn50QMxDX2xPBJnVymEymhtZIA03pA.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '[localhost]:2222' (ED25519) to the list of known hosts.
root@localhost's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
```

Now that I am connected to Cowrite I will create and delete a sample text file.

```
Problems   theia@theiadocker-bradleyrroff: /home/project   theia@theiadocker-bradleyrroff: /home/project ×
root@svr04:~# ls
root@svr04:~# echo "The is a file created through ssh">newfilefromRemote.txt
root@svr04:~# cat newfilefromRemote.txt
The is a file created through ssh
root@svr04:~# rm -f newfilefromRemote.txt
root@svr04:~# ls
root@svr04:~#
```

Opining a new terminal I will now examine the contents of the honeypotsLogs.txt file. Using the grep “login attempt’ command I can see the times I SSH into this honeypot.

```
theia@theiadocker-bradleyrroff:/home/project$ cat honeypotLogs.txt | grep "login attempt"
2025-02-27T15:47:59+0000 [HoneyPotSSHTransport,0,172.17.0.1] login attempt [b'root'/b'admin'] succeeded
2025-02-27T15:52:19+0000 [HoneyPotSSHTransport,1,172.17.0.1] login attempt [b'root'/b'admin'] succeeded
```

I can also use Grep “CMD” to see the commands I used to create and delete files.

```
theia@theiadocker-bradleyrroff:/home/project$ cat honeypotLogs.txt | grep "CMD"
2025-02-27T15:47:59+0000 [HoneyPotSSHTransport,0,172.17.0.1] CMD:
2025-02-27T15:49:57+0000 [HoneyPotSSHTransport,0,172.17.0.1] CMD: clear
2025-02-27T15:49:58+0000 [HoneyPotSSHTransport,0,172.17.0.1] CMD: lls
2025-02-27T15:50:00+0000 [HoneyPotSSHTransport,0,172.17.0.1] CMD: ls
2025-02-27T15:50:22+0000 [HoneyPotSSHTransport,0,172.17.0.1] CMD: echo "The is a file created through ssh">newfilefromRem
ote.txt

2025-02-27T15:52:39+0000 [HoneyPotSSHTransport,1,172.17.0.1] CMD: cat newfilefromRemote.txt
2025-02-27T15:52:46+0000 [HoneyPotSSHTransport,1,172.17.0.1] CMD: rm -f newfilefromRemote.txt
2025-02-27T15:52:49+0000 [HoneyPotSSHTransport,1,172.17.0.1] CMD: ls
```

Using grep “Connection lost after” I can see how the host closed the connection automatically.

```
theia@theiadocker-bradleyrroff:/home/project$ cat honeypotLogs.txt | grep "Connection lost after"
2025-02-27T15:50:59+0000 [HoneyPotSSHTransport,0,172.17.0.1] Connection lost after 192 seconds
2025-02-27T15:55:19+0000 [HoneyPotSSHTransport,1,172.17.0.1] Connection lost after 182 seconds
```