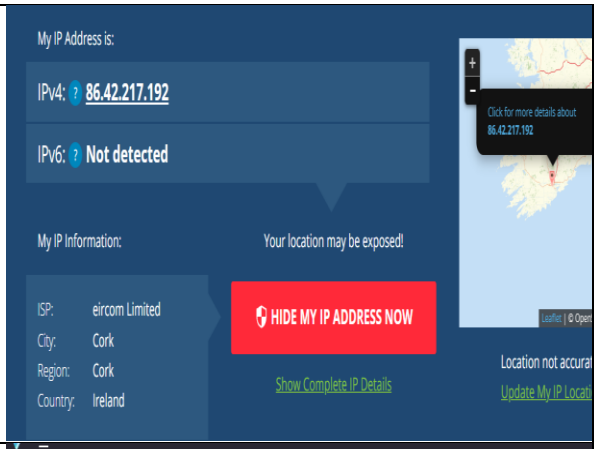
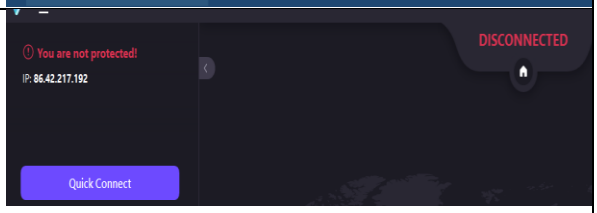
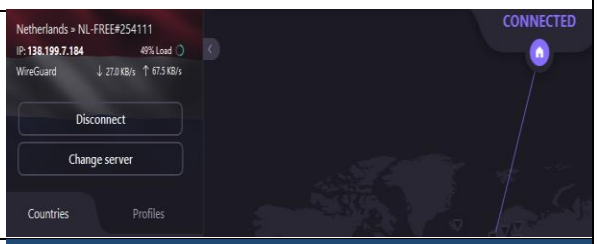
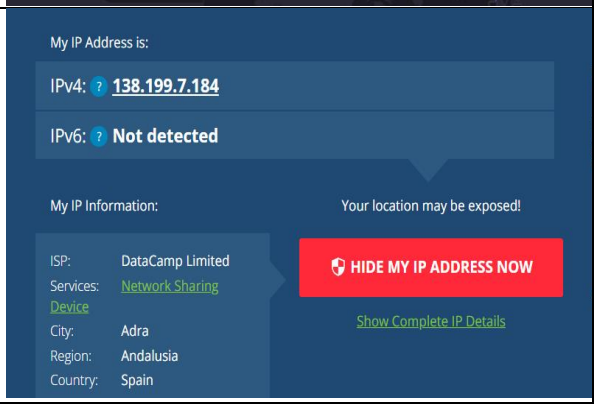
The Importance of Encryption

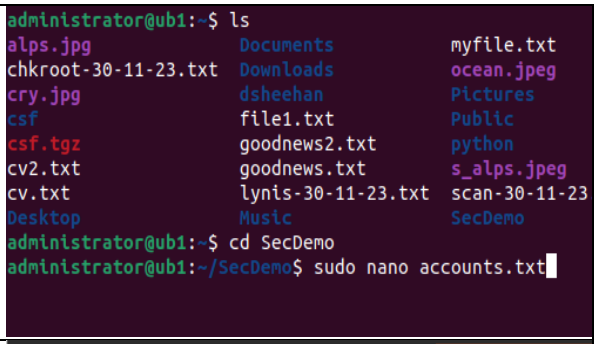
Daniel Sheehan

Introduction:

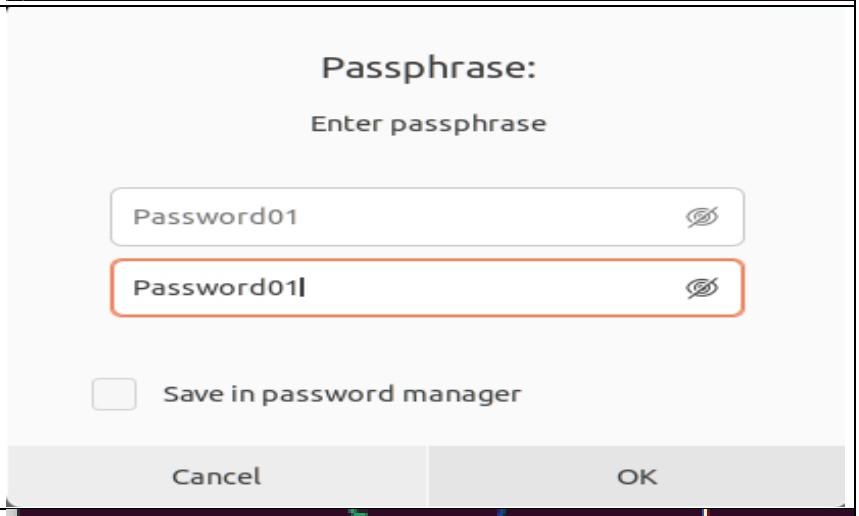
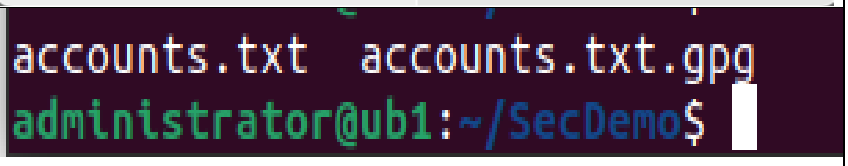
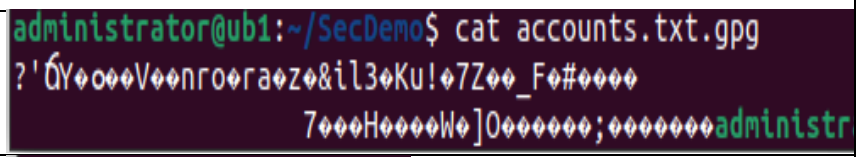
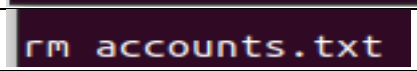
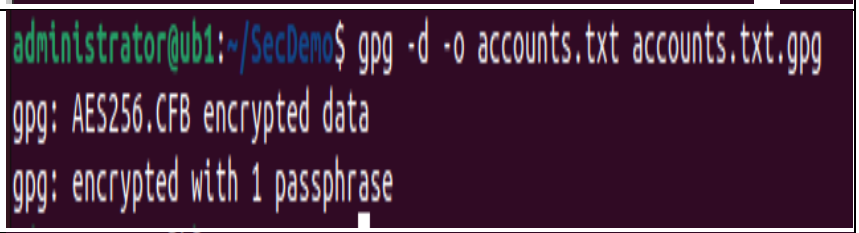
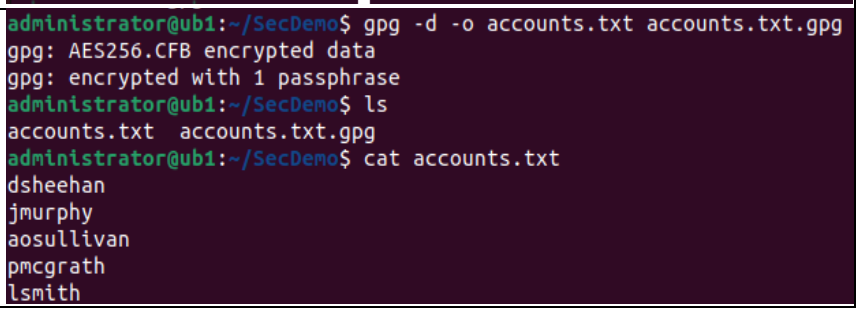
In this skills demo I will be exploring the importance of secure digital communication as well as a variety of encryption methods such as using a VPN to safely browse the web, Encryption methods such as GPG and Steghide, setting up and configuring secure wireless communication through encryption methods such as WPA2 and MAC address filtering. Another key aspect of secure communication I will be covering is the ability to use SSH to connect to a remote server and using SFTP to securely transfer files onto my local machine.

Virtual Private Networks (ProtonVPN)

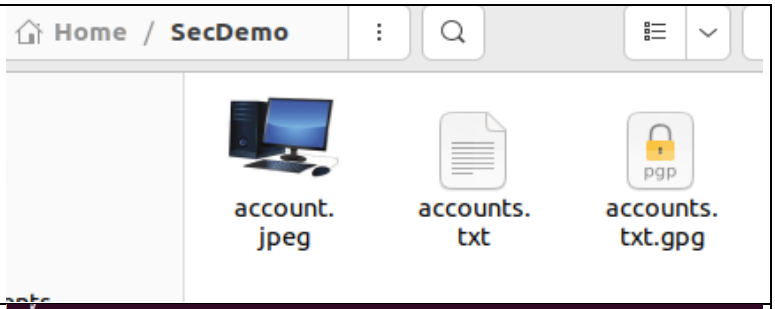
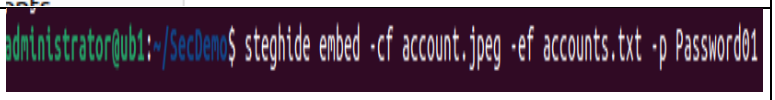
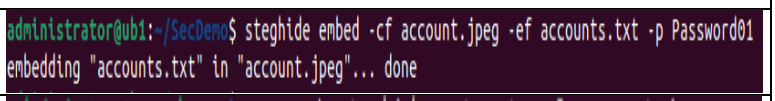
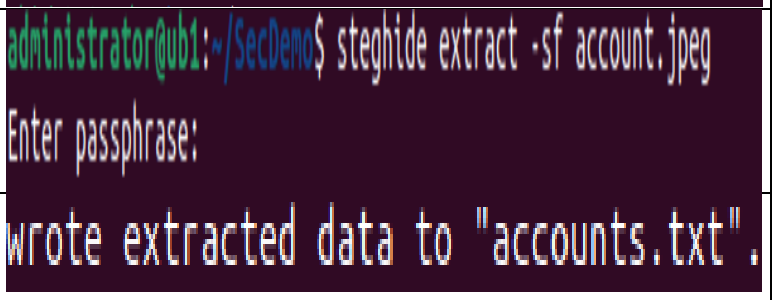
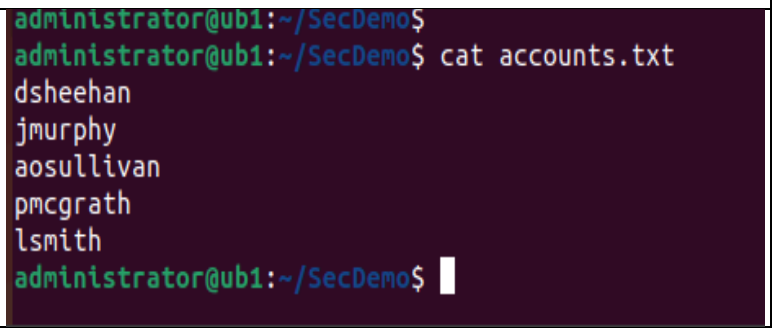
The first thing I will do for this opening segment of the skills demo is check my IP address using https://whatismyipaddress.com. As I can see my IPV4 address is 86.42.217.192 and is coming out of Cork, Ireland	
I will be using the free edition ProtonVPN in order to obtain a new IP address that will be assigned to us from another country. Once the software is installed press quick connect on the map screen.	
I should now see that the indicator in the top right has changed to purple from red and now says “Connected” meaning I have successfully been assigned a new IP address.	
Upon navigating back to https://whatismyipaddress.com and refreshing the page I can now see that I have been assigned a new IP address (138.199.7.184) coming from Andalusia, Spain This shows us that my VPN is working and I am now ready to browse the internet more securely.	

I will create a text file in my SecDemo directory known as accounts.txt Sudo nano accounts.txt	
In this NANO file I will enter a few sample account names for the contents	
I will then cat my accounts.txt file to verify the contents	

Encrypt (GPG)

I will now encrypt my accounts.txt file: gpg –symmetric accounts.txt	
I will now set the password as: Password01 This will ensure my file stays protected.	
I now have 2 files the original and the encrypted (accounts.txt.gpg)	
I can now see from the cat output the file contents are encrypted.	
Remove the original file	
keep the encrypted version so I can revert it back to accounts.txt	
I have now decrypted the contents of my encrypted file and outputted them to a new file called accounts.txt	
As I can see from the output I have successfully decrypted the text content and put it into my accounts.txt file	

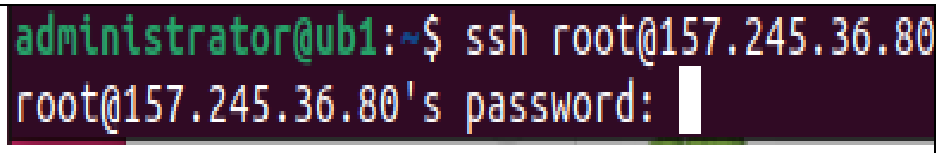
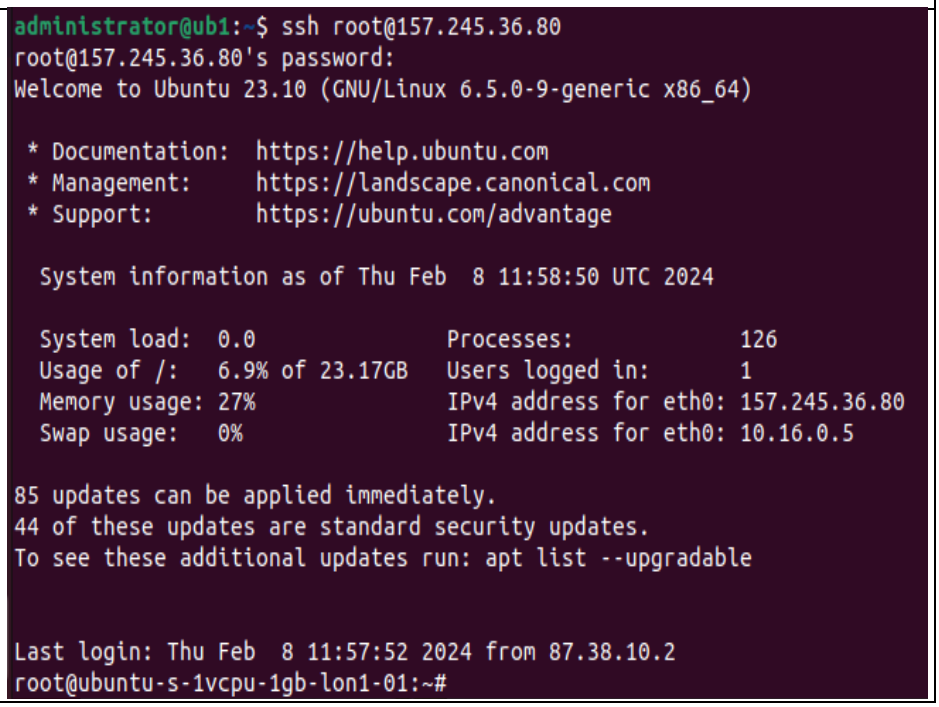
Steghide (embed text into image)

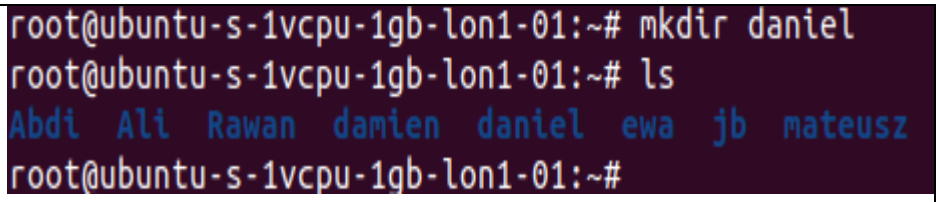
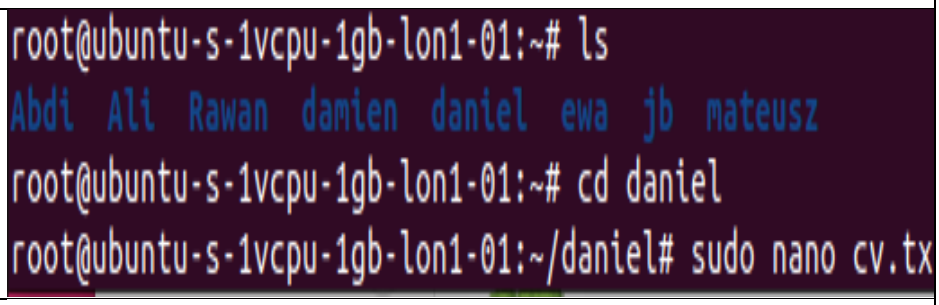
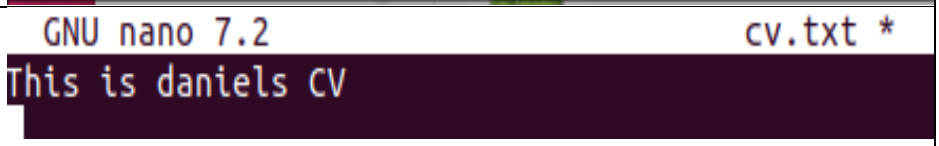
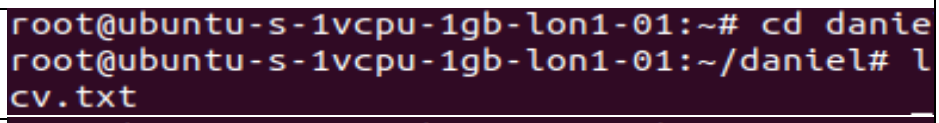
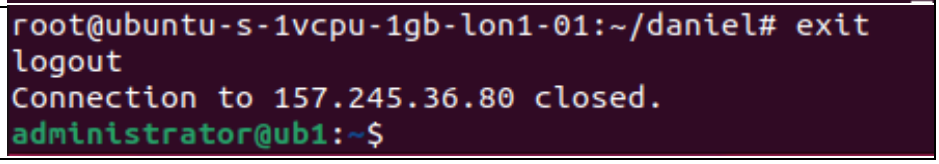
I will now download a jpg image to hide my plain text file (accounts.txt) this means I am embedding my text in the image.	
To do this I will be using steghide Steghide embed -cf account.jpg -ef accounts.txt -p Password01	
My text is now embedded in my jpeg file.	
Let's decrypt this. Using Password01 I will extract my txt file from my jpeg.	
As shown here I have successfully made a new accounts.txt file that should contain my decrypted text content	
I will now cat this to verify the output. As shown by the output I can see the text has been decrypted telling us I have successfully completed these steps.	

Connecting to a remote server

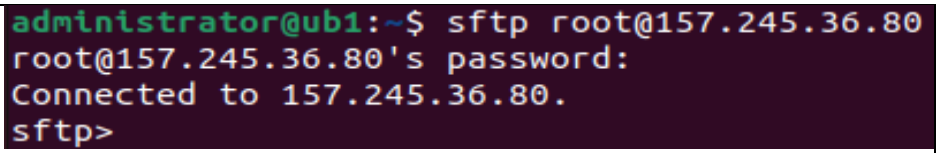
In this next segment I will be connecting to a remote digitalocean server in a data centre in London through SSH, once I have connected, I will be creating a folder that will contain a txt file once I have created both files, I will be using the list (ls) command to show the contents of the directory. Once this has been completed, I will be using SFTP to transfer the file from the virtual server machine to my local machine and deleting the folder on the server.

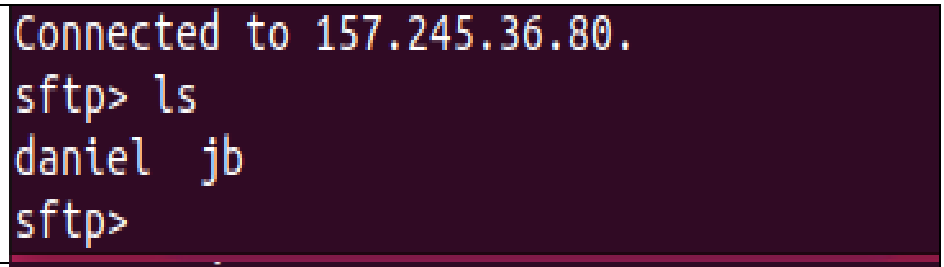
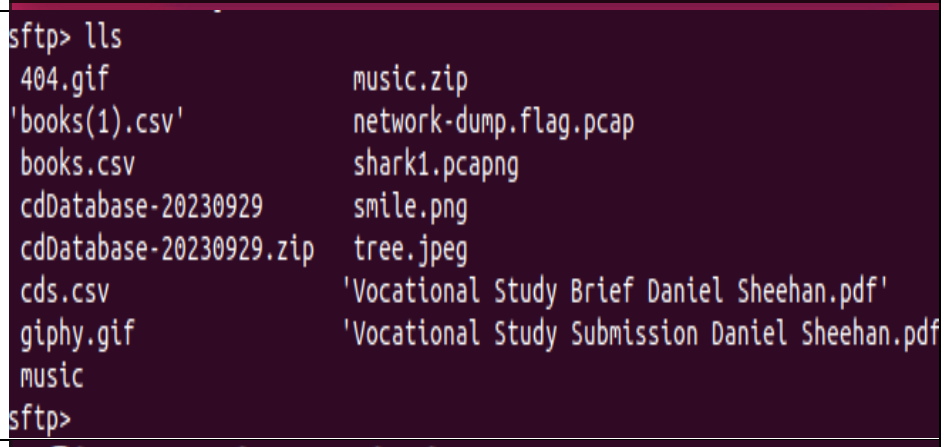
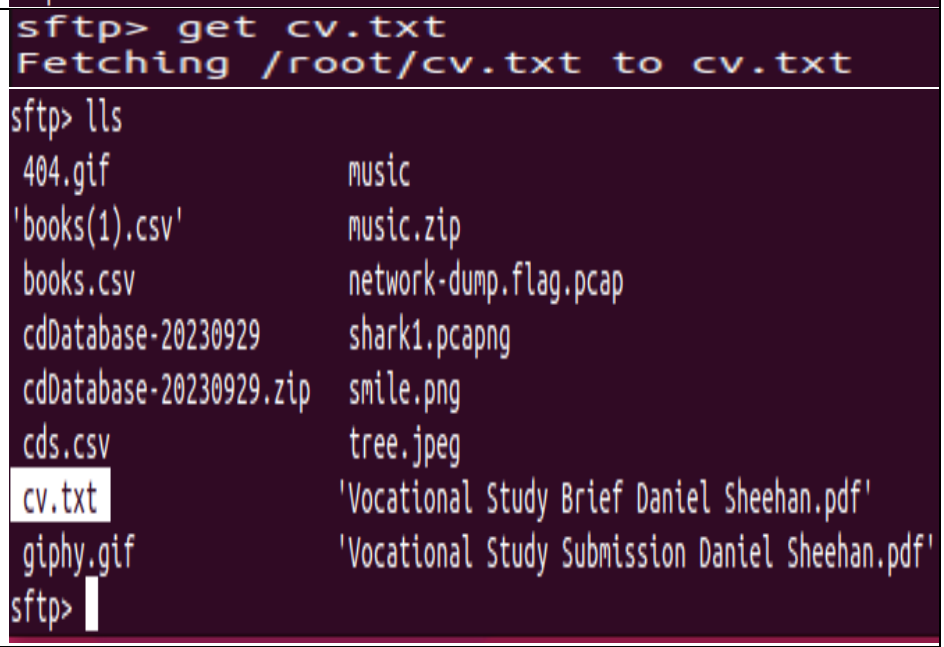
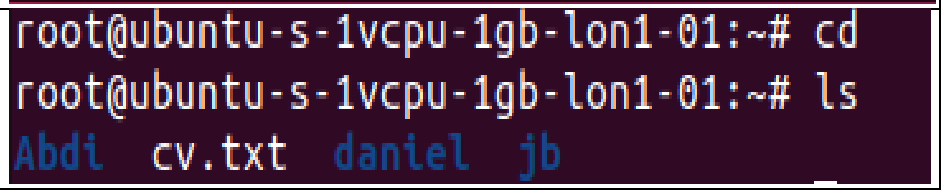
SSH:

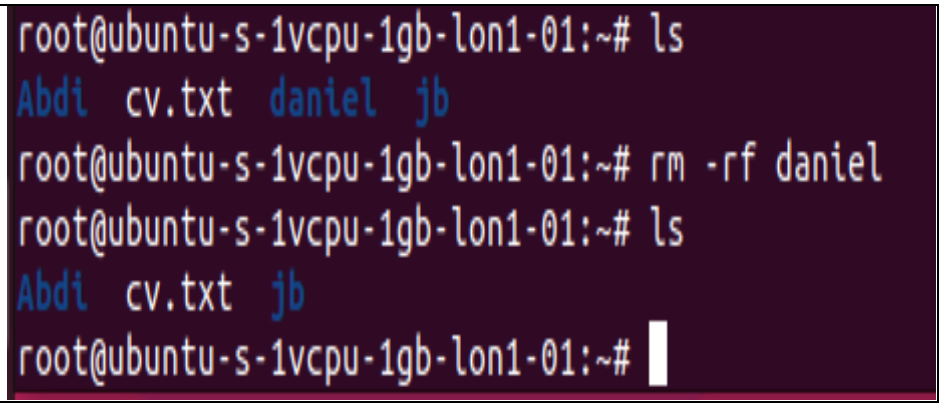
To begin I will navigate to the cli terminal on my Ubuntu machine and type the following commands in order to connect to this remote server being hosted on a data centre in London. Ssh root@157.245.36.80 Once I type this command I will then enter the password 4BlindMice and attempt to connect	
As I can see I have successfully connected to the remote server as the root user meaning I have permissions to create new directories and files. I will type cd to ensure I am in the home directory	

Now that I know where I am I will make a new directory called “daniel” by using the mkdir command. After I create the directory I will type ls again and I should see the daniel directory has been created.	
Next I will cd into the daniel directory and create a file called cv.txt using the command sudo nano cv.txt	
I will write contents to verify the integrity of my file and then press ctrl s ctrl x to save and exit	
Once I type ls again I can see my cv.txt file	
I will now press exit to close my connection to the server.	

SFTP(Secure File Transfer Protocol):

I will now log back into the server using SFTP and the same login as previously: root@157.245.36.80 pass: 4BlindMice	

Once I have connected I will us the ls command to view my servers home directory containing the daniel directory.	
Using the ls command I can see the contents of my local machine away from the server. I will use sftp to retrieve my cv.txt file from my server and put it on my local machine.	
To achieve this I must use the following command: Get cv.txt After this I will run another ls and as I can see my file has been re-tried and is now present on my local machine meaning I have used sftp successfully.	
I will now clean up after myself in order to securely remove any traces of my activity.	
Exit sftp	
I will login again using ssh and type ls where I can see my daniel directory.	

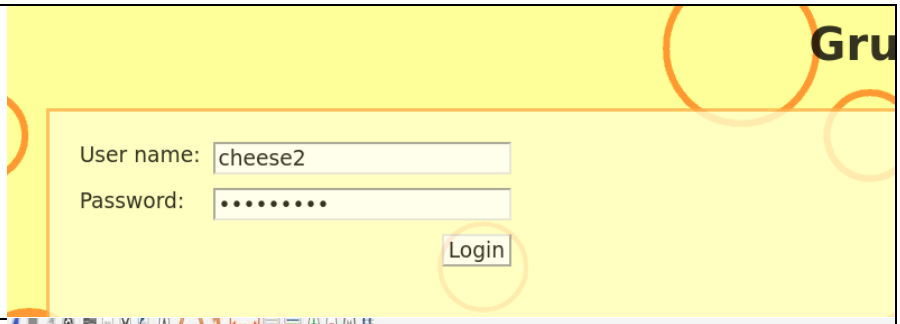
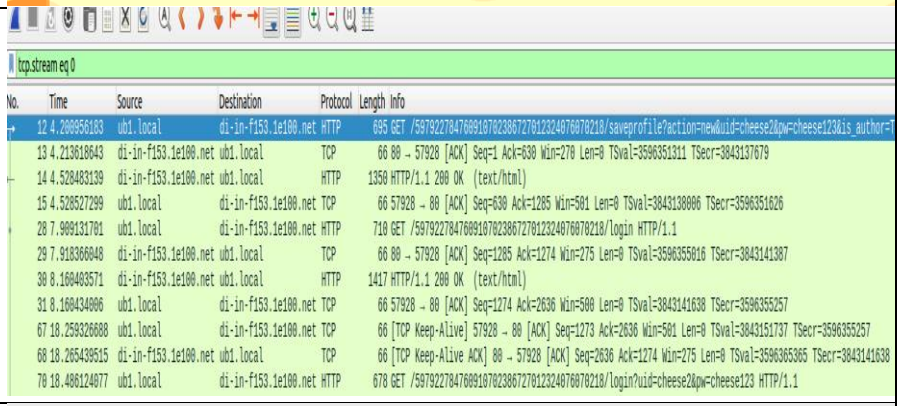
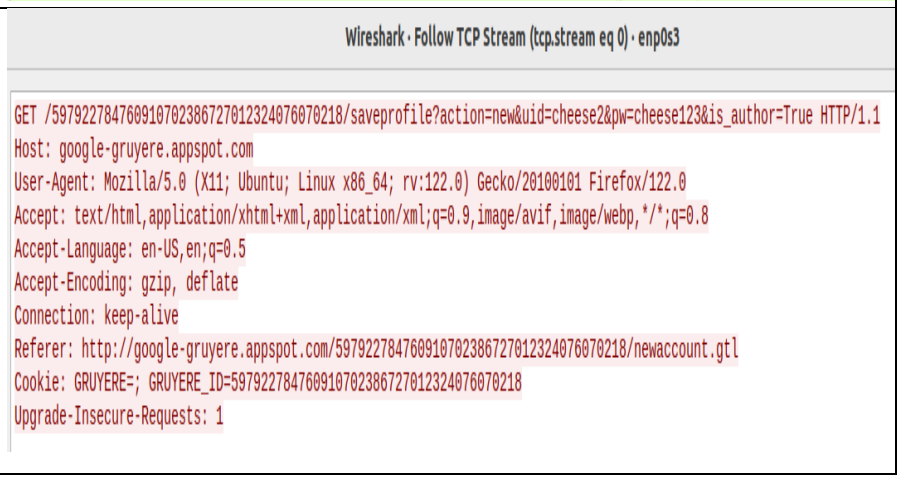
Finally I will type rm -rf daniel I will then type ls and see I have successfully removed the daniel directory meaning I have cleared any trace of my activity.	

HTTP vs HTTPS

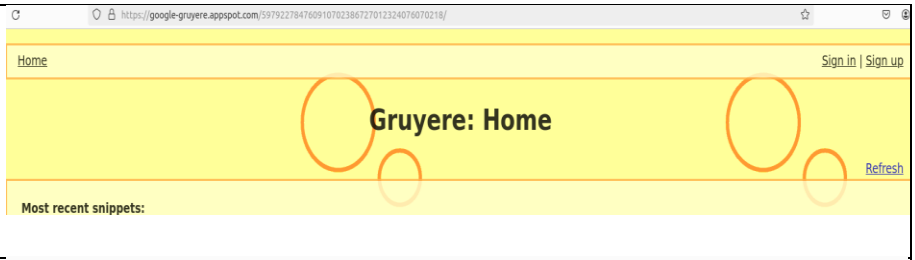
In this segment of my skills demo I will be demonstrating the difference of a HTTP vs a HTTPS website. HTTP messages are written in plaintext which allows anyone on the internet to access and read them, HTTPS however transmits all data encrypted, this means that when users fill out forms and submit sensitive information, they can be confident that it is secure.

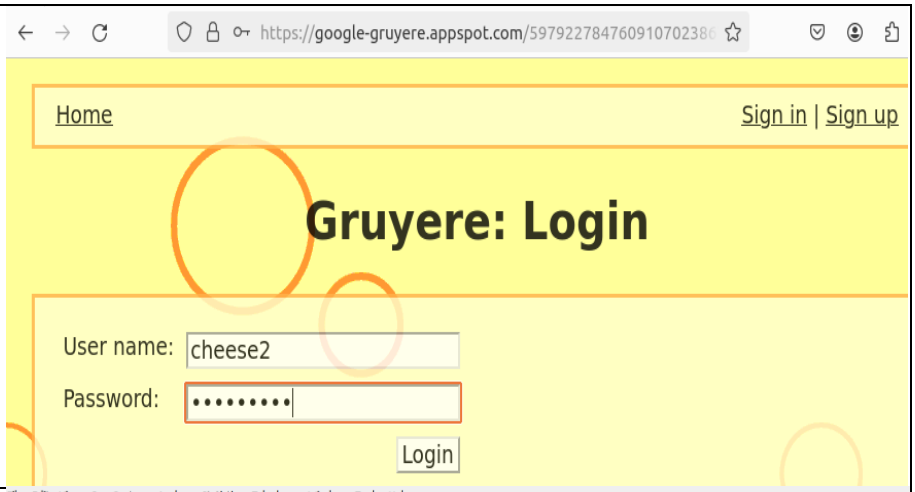
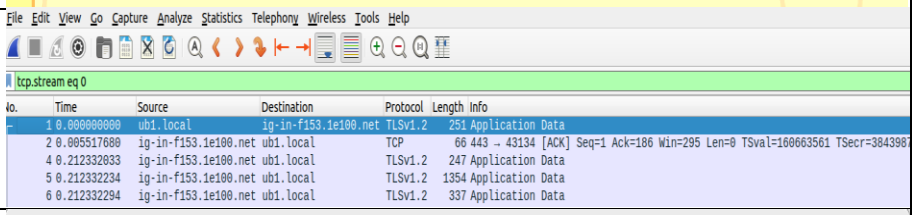
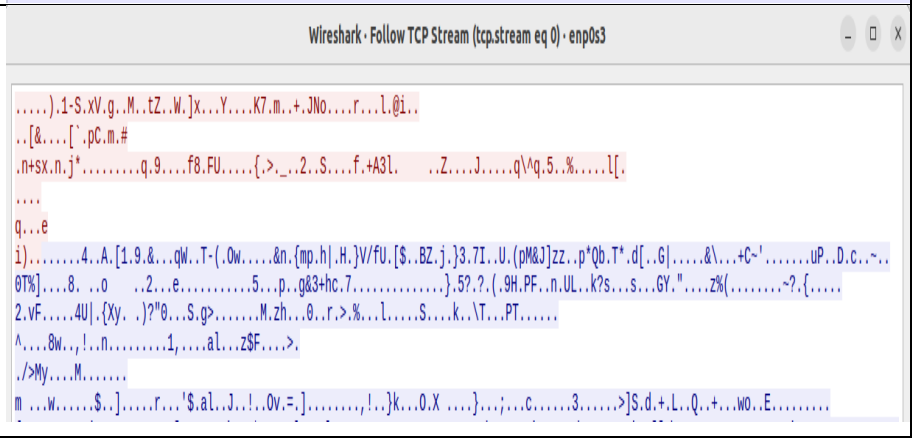
HTTP:

I began by logging onto Google-Gruyere.appspot.com, I will use this site to look at the difference between http and https.	
On the HTTP site I can see that there is a red mark going through the padlock this is warning users that the site may be unsecure and to be mindful when entering any data and filling forms	

I will test this by creating and logging onto an account as follows: User – cheese2 Password – cheese123	
Using Wireshark, I will monitor any packets going through the site and locating the one containing my username and password. Once I find it I will follow the TCP stream on the HTTP service and view the results	
Once I follow the stream, I can clearly see my username (cheese2) and password (cheese123) can be viewed as plain text by anyone monitoring the page. This shows us that no encryption method has been used as previously stated.	

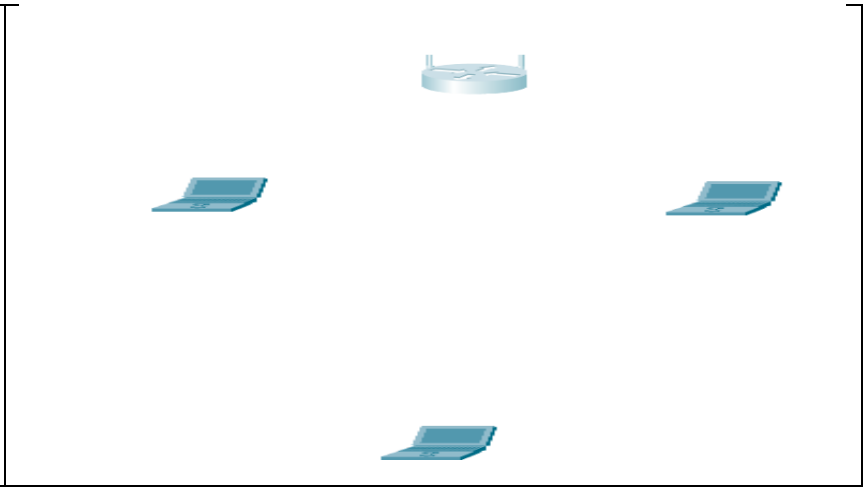
HTTPS:

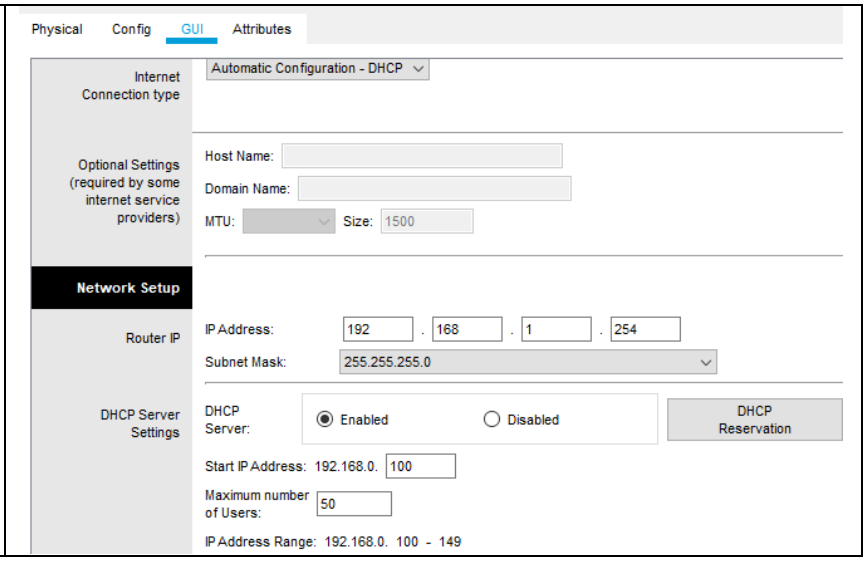
Next, I will be testing the HTTPS version of the Gruyere site in order to see if my user inputted data is encrypted.	
As I can see the padlock has no red line across it indicating that this version of the site is secure and encrypted.	

I will repeat my previous steps and log in to the site using the following details: User – cheese2 Password-cheese123	
Once I have entered my data, I will follow the TCP stream in order to see if my data is encrypted.	
Here I can now see that my username and password are no longer displayed as plain text, this is because HTTPS has been used and my data is encrypted and more secure instead of being stored as plain text.	

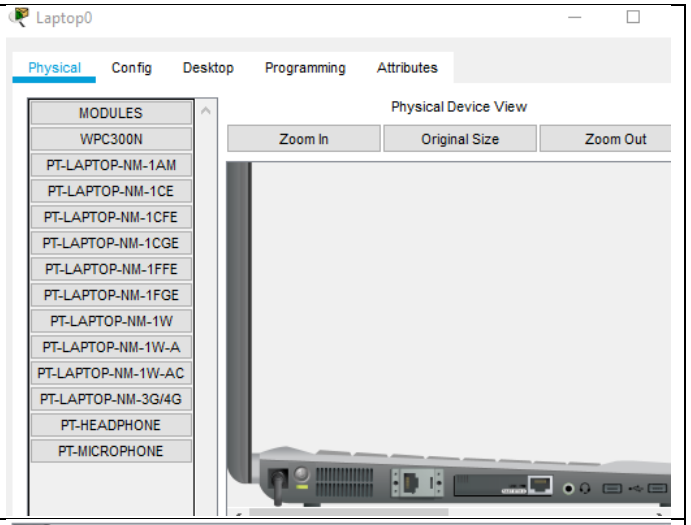
Filtering MAC Address + WPA2 integration

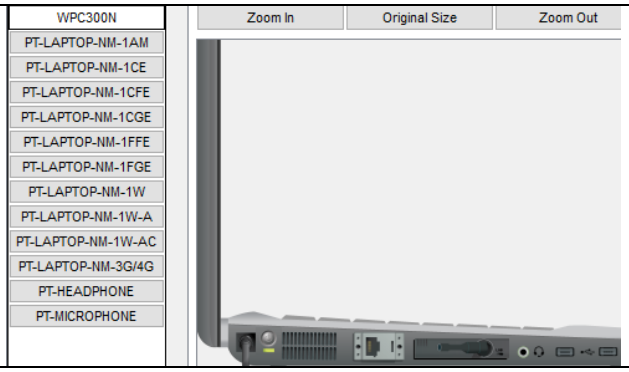
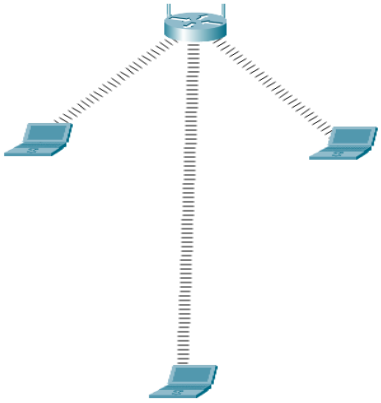
Topology & Wireless Router Setup:

For this segment of the skills demo I will be implementing WPA2 on a wireless access point and utilizing MAC address filtering. I will be setting up a topology in Packet Tracer using 3 laptops and Wireless Router	

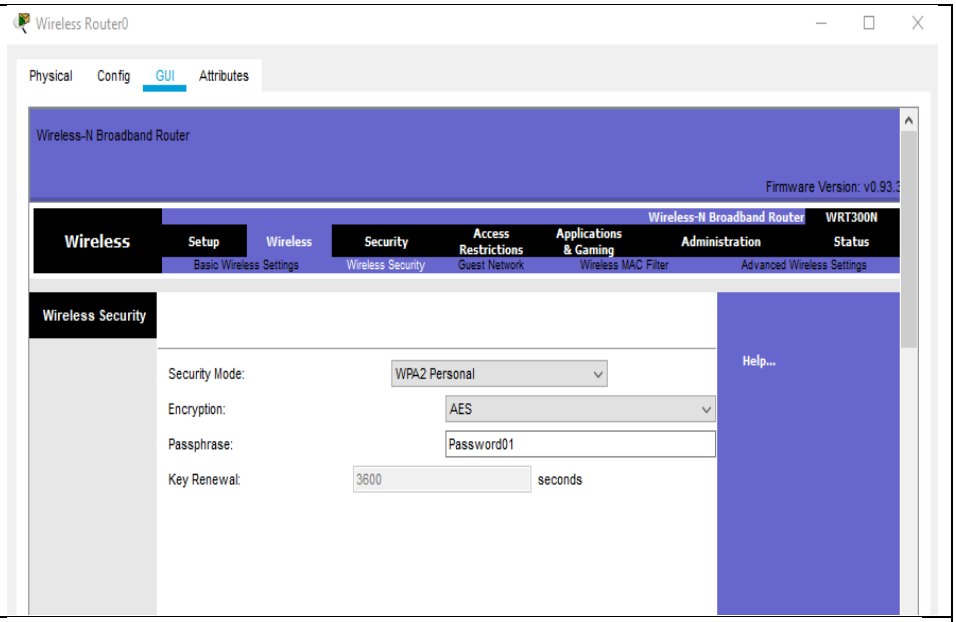
I will begin by navigating to the Router's GUI and setting its IP address to 192.168.1.254 and ensuring that DHCP is enabled. My starting IP Address will also be set to 100 and I will have a maximum of 50 users. Once this is completed, I am ready to move onto the next step.	

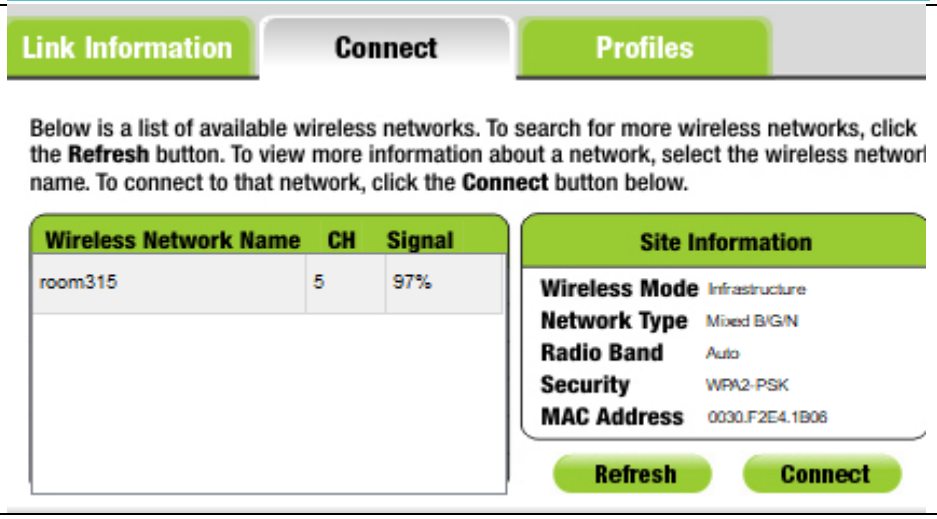
Laptops setup:

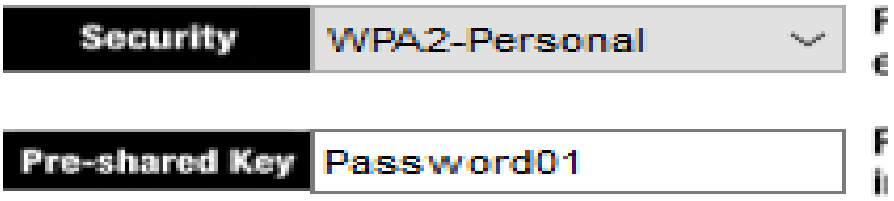
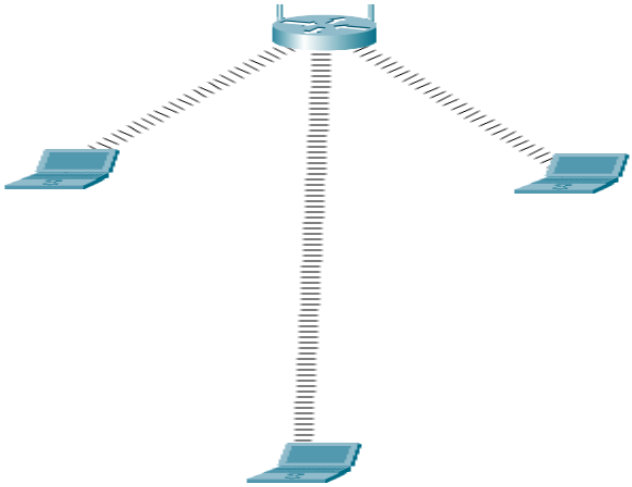
Next, I will navigate to my 1st laptop and access the physical tab, here I will be met with a list containing a few different Wi-Fi card models.	
Before selecting the card that I require I will have to click the button on the left of the laptop in order to power off the device. I will then remove the current card before I progress.	

Next, I will insert the WPC300N card from the list and power the laptop back on, and repeat these exact steps for all laptops/devices	
I now have a successful connection for each device to the wireless router as indicated by the line which forms connecting each device to the wireless router. Now that I can see my devices have connected successfully, I will need to set up a basic layer of encryption so that only authorized devices can connect to the network.	

Basic Encryption for Network (WPA2):

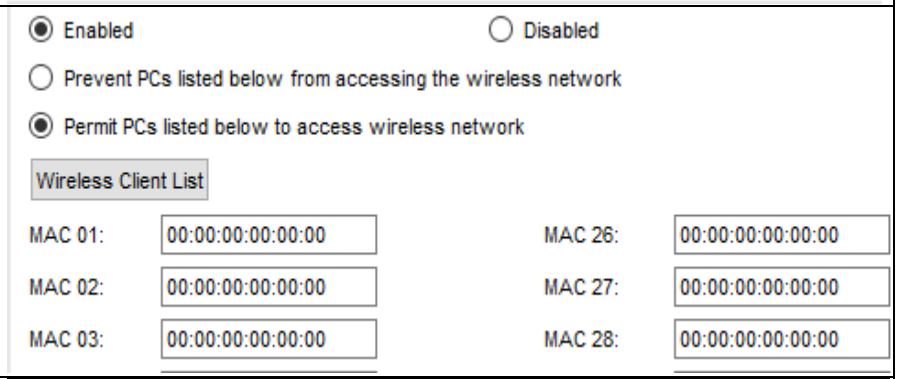
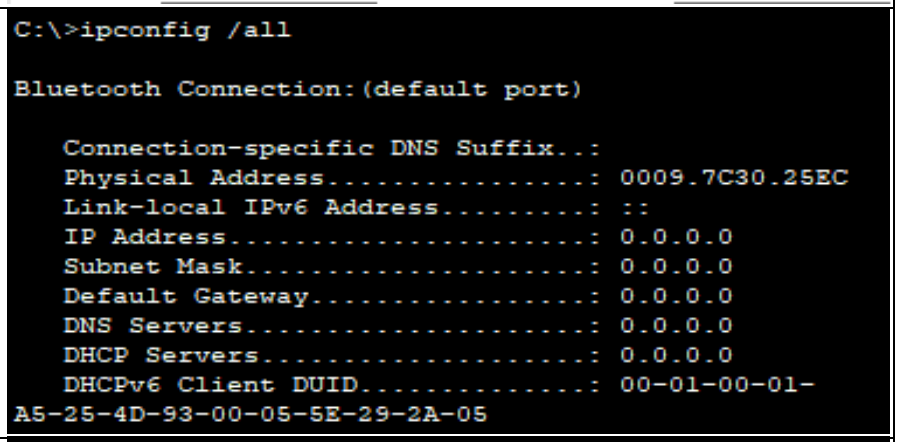
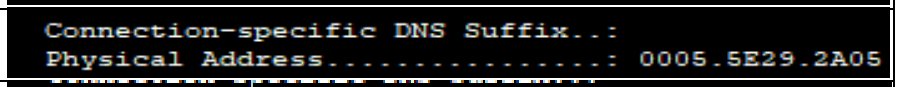
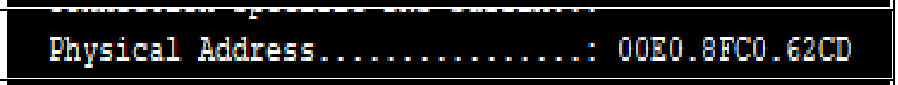
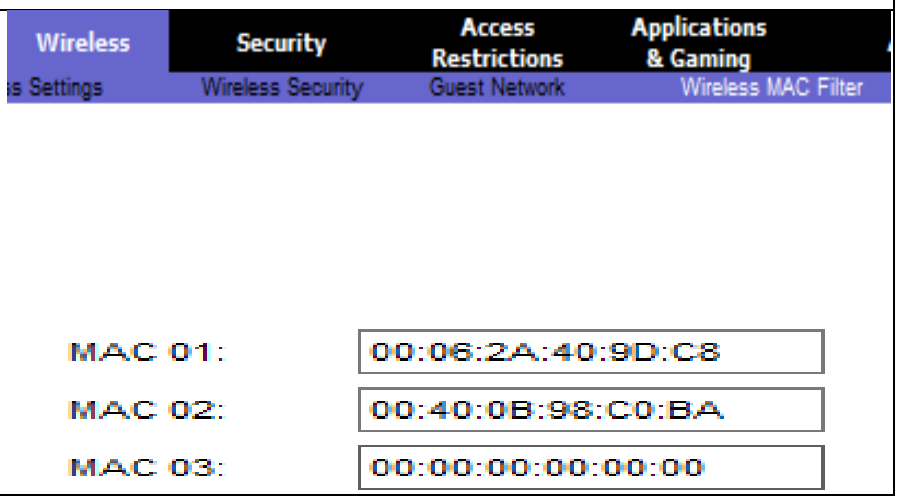
I will now use Wi-Fi protected access (WPA2) in order to protect my network. To do this I will navigate back to the GUI of my router and enable WPA2 Personal as my Security Mode. The password I will set is Password01.	
I will have to scroll down and click save settings before exiting in order to save my changes.	

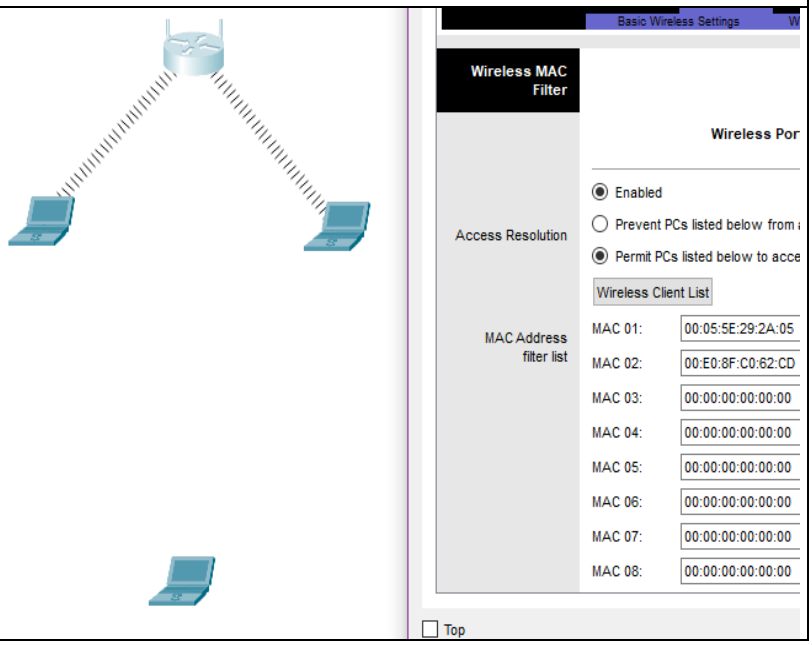
My connection is gone so I must log in using the laptop GUI to access the router again otherwise I am not permitted to access the network. This has shown us I have successfully enabled WPA2	
Going back to my Router GUI I will navigate to the basic wireless settings tab and configure the network as follows:	
Next on the laptops I will navigate to the PC wireless tab using the GUI and get ready to join my Network that should now be set up.	
Navigate to the second tab (Connect) and click refresh, Here I should see the name of my Wireless Network “room315” appear, Select it and say connect	

Here I will need to enter the password I set up earlier: Password01	
Repeat for all devices and I have a connection again with a layer of security. This shows that WPA2 has been utilized successfully.	

Filtering MAC addresses:

My next and final layer of security for my network that I will be setting up for this Skills Demo is MAC address filtering. This makes it so that only devices that have authorized MAC addresses from my Router have permission to connect to the network.

In router GUI I will navigate to Wireless tab and select wireless MAC filter	
Here I have a list of mac addresses permitted to connect to the router, this offers an extra layer of security	
If I navigate to one of my laptops and enter CLI I can type ipconfig /all This provides us with the devices MAC Address	
My MAC address: PC1	
PC2 MAC Address:	
PC 3 (Unpermitted MAC Address)	
For my next step I will navigate to the Router and under the wireless Tab I will click the "Wireless MAC Filtering" option this will provide us with a list that I can add the Physical MAC Addresses I have obtained from running the ipconfig command in CLI so that they are	

permitted to join my network, I will purposely leave the address of the 3rd laptop out of the list in order to test if it has worked effectively	
As I can see I now have a list of MAC addresses that I have allowed to access the router, PC 1 and PC2 have access but PC3 can't connect as it's MAC address isn't listed among the permitted addresses	

This shows us that my list is working, and I have successfully filtered MAC addresses to allow and deny access to my Network depending on the devices MAC address and whether or not it is permitted to connect to my network.

Conclusion:

In conclusion in this skills demo I showcased a variety of different uses for secure communication such as setting up and using VPNs to browse the internet securely and setting up different encryption methods such as GPG and Steghide in order to keep data secure and hidden. I also managed to successfully set up secure wireless connections on 3 different devices using WPA2 and MAC address filtering to keep unauthorized devices off of my wireless network. I also learned the importance of remote server access through methods such as using SSH to access files and SFTP to securely transfer them from a network onto my physical way in an encrypted way. I also demonstrated the importance of HTTPS over HTTP and how users should be cautious when inputting data on unsecure sites in order to avoid theft and their data falling into the wrong hands.