

Assignment 3

NADIM UDDIN 14100462

**INTERROGATE A NETWORK TO IDENTIFY THE NETWORK
ASSETS AND THEIR CONFIGURATION (P5)**

UNDERTAKE ROUTINE NETWORK MANAGEMENT TASKS (P6)

**KEEP ACCURATE RECORDS OF NETWORK MANAGEMENT
TASKS (M3)**

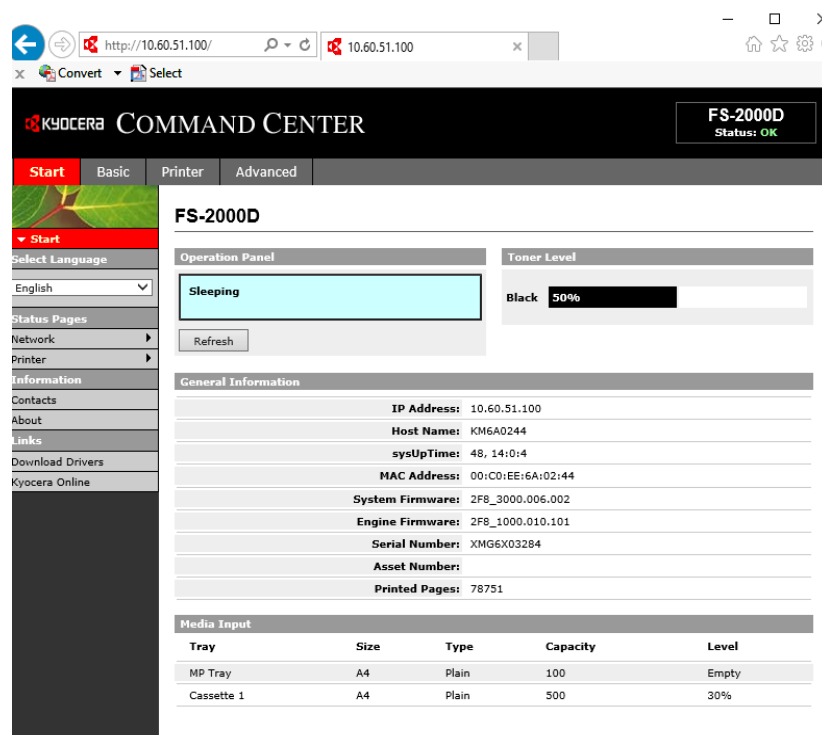
**DESIGN A NETWORK SECURITY POLICY FOR A SMALL
ORGANISATION (D2)**

Interrogate a network to identify the network assets and their configuration (P5)

Introduction: In this area of the document I will be interrogating the network to find information about network assets and configuration. I will be recording the domain name of network as well as the logical and physical topology of the network. I will also be talking about the IP address scheme which is used in the network and the services provides on the network server on the network.

Network assets and their configuration

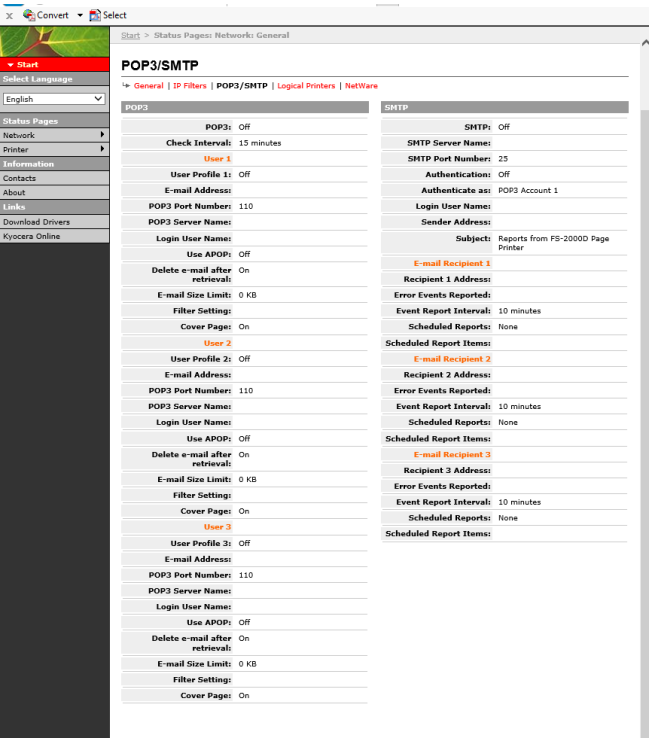
SNMP



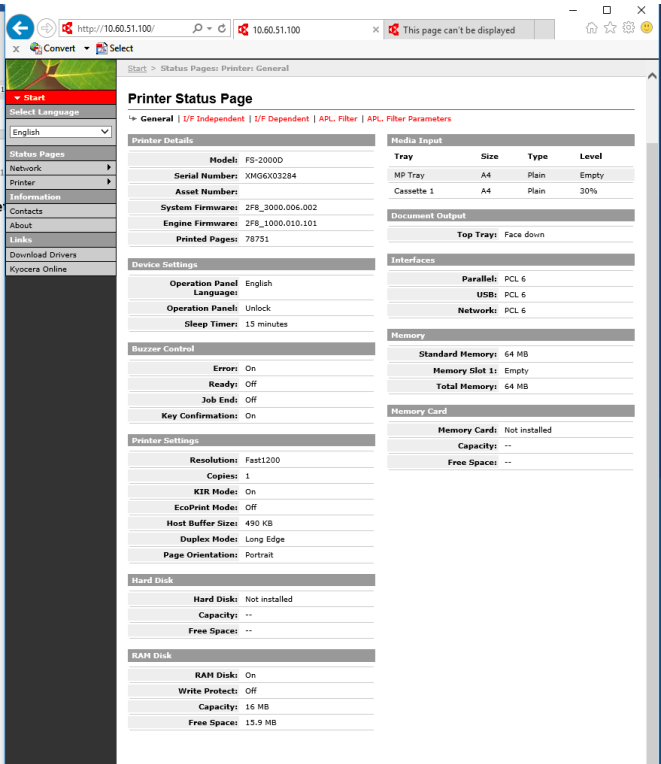
The screenshot shows the Kyocera Command Center web interface for an FS-2000D printer. The interface is accessed via a web browser at the URL <http://10.60.51.100/>. The printer's status is shown as 'Sleeping'. The 'General Information' section provides details about the printer's configuration, including its IP address, host name, and various firmware versions. The 'Media Input' section displays a table with details for the MP Tray and Cassette 1.

Tray	Size	Type	Capacity	Level
MP Tray	A4	Plain	100	Empty
Cassette 1	A4	Plain	500	30%

Here I'm using SNMP to gain access to a printer with the IP address 10.16.27.100. Using the SNMP I can gain information about the printer.

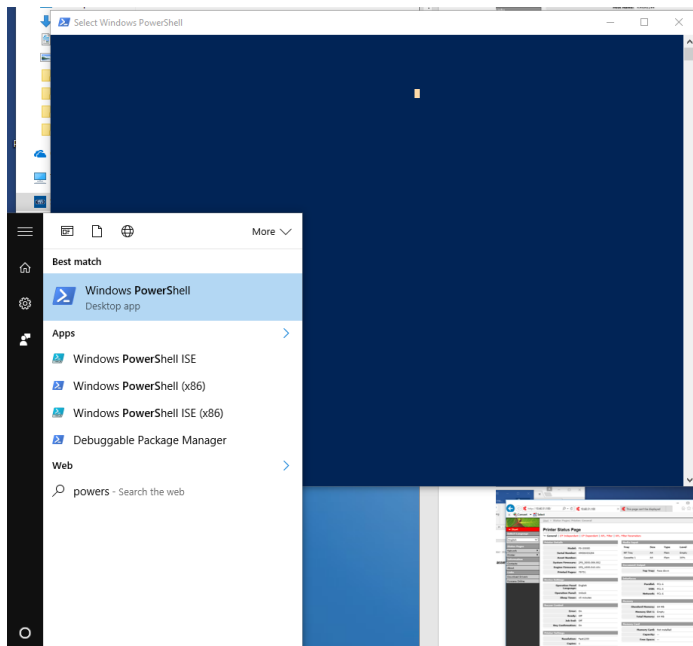


Here displays the POP 3 protocol which is a client server protocol which is used for receiving emails from an internet server.

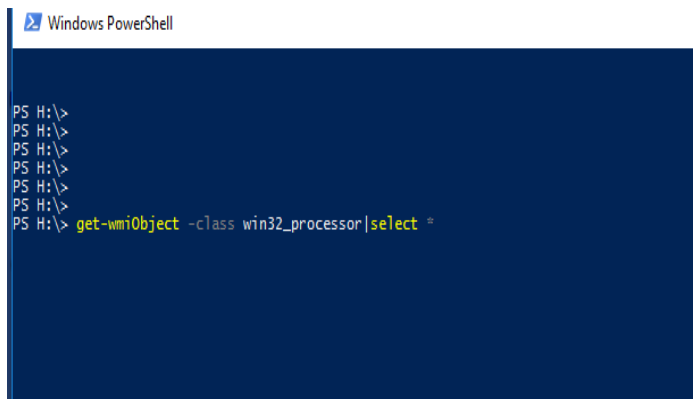


Here displays the printer status page which gives you the description of the printer for example the serial number and printer model.

Powershell



Here I'm going to use PowerShell to find information about the computer system I am working on. I will be specifically looking at the CPU as well as the information about folder and drive space.



To find the information about the CPU I put in this command shown on the left. This command allowed me to find information about the CPU on the computer system I am working on.

```

Windows PowerShell
PS H:\>
PS H:\>
PS H:\>
PS H:\> get-wmiObject -class win32_processor | select *

PSComputerName      : E2708-021222
Availability         : 3
CpuStatus           : 1
CurrentVoltage       : 12
DeviceID            : CPU0
ErrorDescription     :
LastErrorCode        :
LoadPercentage       : 1
Status              : OK
StatusInfo           : 3
AddressWidth         : 64
DataWidth           : 64
ExtClock             : 266
L2CacheSize         : 3072
L2CacheSpeed         : 2926
MaxClockSpeed        : 2926
PowerManagementSupported : False
ProcessorType        : 3
Revision            : 5898
SocketDesignation    : LGA775
Version              : 1
VoltageCaps          : 2
__GENUS              : 2
__CLASS              : Win32_Processor
__SUPERCLASS          : CIM_Processor
__DYNASTY             : CIM_ManagedSystemElement
__RELPATH             : Win32_Processor.DeviceID="CPU0"
__PROPERTY_COUNT      : 57
__DEIVATION           : [CIM_Processor, CIM_LogicalDevice, CIM_LogicalElement, CIM_ManagedSystemElement]
__SERVER              : E2708-021222
__NAMESPACE          : root\cimv2
__PATH               : \\E2708-021222\root\cimv2\Win32_Processor.DeviceID="CPU0"
Architecture         : 9
AssetTag             : To Be Filled By O.E.M.
Caption              : Intel64 Family 6 Model 23 Stepping 10
Characteristics       :
ConfigManagerErrorCodes :
ConfigManagerUserConfig :
CreationClassName     : Win32_Processor
CurrentClockSpeed     : 2926
Description           : Intel64 Family 6 Model 23 Stepping 10
Family               : L31
InstallDate          : 0
L2CacheSize          : 0
L2CacheSpeed         : 0
Level                : 0
Manufacturer         : GenuineIntel
Name                 : Intel(R) Core(TM)2 Duo CPU   E7500  @ 2.93Ghz
NumberOfCores         : 2
NumberOfEnabledCores : 2
NumberLogicalProcessors :
OtherFamilyDescription : To Be Filled By O.E.M.
PartNumber            :
PNPDeviceID           :
PowerManagementCapabilities :
ProcessorID           : BFE8BF0001067A
Role                  : CPU
SecondLevelAddressTranslationExtensions :
SerialNumber          : To Be Filled By O.E.M.
Stepping              :
SystemCreationClassName : Win32_ComputerSystem
SystemName            : E2708-021222
ThreadCount           : 21
UniqueID              :
UpgradeMethod         : False
VirtualizationFirmwareEnabled :
WmiMonitorModeExtensions :
Scope                 : System.Management.ManagementScope
Options               :
ClassPath              : \\E2708-021222\root\cimv2\Win32_Processor.DeviceID="CPU0"
Properties             : [AddressWidth, Architecture, AssetTag, Availability...]
Qualifiers             : {__GENUS, __CLASS, __SUPERCLASS, __DYNASTY...}
Site                  :
Container              :

```

After inputting the command needed, I manage to gather information about the CPU. As you can see, it includes information about the manufacturer, the name of the CPU and the Max clock speed.

```

Windows PowerShell
PS H:\> Get-Childitem -Path H:\
Get-Childitem: The term 'get-childitem' is not recognized as the name of a cmdlet, function, script file,
program, or executable file. Check the spelling of the name, or if a path was included, verify that the path is correct and
exists.
At line:1 char:1
+ Get-Childitem -Path H:\
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (Get-Childitem:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS H:\> get-childitem -path H:\
Get-Childitem: The term 'get-childitem' is not recognized as the name of a cmdlet, function, script file,
program, or executable file. Check the spelling of the name, or if a path was included, verify that the path is correct and
exists.
At line:1 char:1
+ get-childitem -path H:\
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (get-childitem:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS H:\> Get-Childitem -Path H:\
Get-Childitem: The term 'get-childitem' is not recognized as the name of a cmdlet, function, script file,
program, or executable file. Check the spelling of the name, or if a path was included, verify that the path is correct and
exists.
At line:1 char:1
+ Get-Childitem -Path H:\
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (Get-Childitem:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

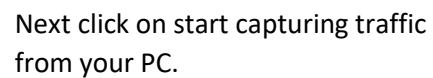
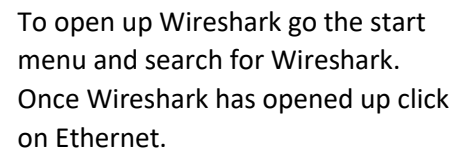
PS H:\> Get-Childitem -Path H:\
Directory: H:\

Mode                LastWriteTime         Length Name
----                -
d-----          17/09/2015         11:03
d-----          24/02/2016         14:39      Custom Office Templates
d-----          27/06/2016         12:14      Favorites
d-----          04/11/2016         10:48      Game
d-----          05/12/2016         14:04      Level 3
d-----          27/06/2016         12:14      Music
d-----          17/12/2013         10:23      My Data Sources
d-----          09/06/2016         13:35      My Shapes
d-----          27/06/2016         12:14      Pictures
d-----          27/06/2016         10:24      Red or blue
d-----          27/06/2016         12:14      Videos
d-----          10/03/2016         15:55      Web Test
-a-----          14/01/2016         14:13      465021 Logo creation copy.psd
-a-----          09/03/2016         14:41      13120 Malware.docx
-a-----          03/12/2015         11:41      683546 P2.docx
-a-----          08/06/2016         14:41      385374 Sales Data for PlayNGameV2.xlsx
-a-----          16/09/2016         11:41      1450502 Terrains.pptx
-a-----          20/11/2015          08:47      98304 Up-skilling Project - Computing Level 3 Year 1 - Games R

```

To see folder and files in PowerShell, you have to use the get-childitem command. The screenshot shown on the left displays all the folders and files which are stored at the root level of the H:/ drive of the computer system I'm using.

Wireshark



Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl>F

No.	Time	Source	Destination	Protocol	Length	Info
747	9.616767	CiscoInc_bci0bica		CGMP	60	Cisco Group Management Protocol
748	9.663836	IntelCor_BcId4:d0	Broadcast	ARP	60	kho has 10.60.2.5? Tell 10.60.27.13
749	9.675784	CiscoInc_bci0bica		CGMP	60	Cisco Group Management Protocol
750	9.688294	CiscoInc_bci0bica		CGMP	60	Cisco Group Management Protocol
751	9.698895	CiscoInc_bci0bica		CGMP	60	Cisco Group Management Protocol
752	9.705086	fe80::40f1:f14b:cee...	ff02::1:3	LLMNR	92	Standard query 0xb1b1 A N4405-026185
753	9.705223	10.60.96.139	224.0.0.252	LLMNR	72	Standard query 0xb1b1 A N4405-026185
754	9.709317	10.60.96.158	255.255.255.255	GVSP	102	LEADER [Block ID: 0 Packet ID: 0] Unknown Payload Type (0x0)
755	9.732426	CiscoInc_bci0bica		CGMP	60	Cisco Group Management Protocol
756	9.733688	CiscoInc_bci0bica		CGMP	60	Cisco Group Management Protocol
757	9.734981	CiscoInc_bci0bica		CGMP	60	Cisco Group Management Protocol
758	9.755574	CiscoInc_bci0bica		CGMP	60	Cisco Group Management Protocol
759	9.769204	10.60.96.173	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
760	9.774382	CiscoInc_bci0bica		CGMP	60	Cisco Group Management Protocol
761	9.775598	CiscoInc_bci0bica		CGMP	60	Cisco Group Management Protocol
762	9.777998	CiscoInc_bci0bica		CGMP	60	Cisco Group Management Protocol
763	9.782760	CiscoInc_bci0bica		CGMP	60	Cisco Group Management Protocol
764	9.785970	CiscoInc_b0i87:0d		CDP/VTP/DTP/PAgP/UDL	60	Dynamic Trunk Protocol
765	9.786821	CiscoInc_b0i87:0d		CDP/VTP/DTP/PAgP/UDL	60	Dynamic Trunk Protocol
766	9.812175	CiscoInc_bci0bica		CGMP	60	Cisco Group Management Protocol
767	9.816223	Clevo_Ifb18:31	Broadcast	ARP	60	kho has 10.60.96.130? Tell 10.60.96.45
768	9.821591	CiscoInc_bci0bica		CGMP	60	Cisco Group Management Protocol
769	9.857817	CiscoInc_bci0bica		CGMP	60	Cisco Group Management Protocol
770	9.866912	CiscoInc_bci0bica		CGMP	60	Cisco Group Management Protocol

> Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
 > Ethernet II, Src: Pegatron 39:94:fc (38:60:77:39:94:fc), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 > Internet Protocol Version 4, Src: 10.60.50.2, Dst: 255.255.255.255
 > User Datagram Protocol, Src Port: 55639 (55639), Dst Port: 51515 (51515)
 > GigE Vision Streaming Protocol

0000 ff ff ff ff ff ff 38 60 77 39 94 fc 08 00 45 008' w0....E.
 0010 00 58 50 56 00 00 11 ae 01 0a 3c 32 02 ff ff .XPV....<2...
 0020 ff ff d9 57 c9 3b 00 44 64 f4 01 00 00 01 00 ...M.;D d.....
 0030 00 01 00 00 00 00 00 00 00 15 00 00 01 00
 0040 00 00 0a 00 00 00 8a 02 00 00 00 00 0f 00
 0050 ae 01 11 76 00 00 45 35 30 30 35 2d 30 32 37 31 ...v..E5 005-0271
 0060 35 31 00 00 00 00 51....

Once you have started the process information will then appear about protocols that are used in the network.

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.0.6002.18005]
(c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig /all

Error: unrecognized or incomplete command line.

USAGE:
    ipconfig [/allcompartments] [/? | /all |
        /renew [adapter] | /release [adapter] |
        /renew6 [adapter] | /release6 [adapter] |
        /flushdns | /displaydns | /registerdns |
        /showclassid adapter |
        /setclassid adapter [classid] |
        /showclassid6 adapter |
        /setclassid6 adapter [classid] ]

where
    adapter          Connection name
                     (wildcard characters * and ? allowed, see examples)

Options:
    /?              Display this help message
    /all            Display full configuration information.
    /release        Release the IPv4 address for the specified adapter.
    /release6       Release the IPv6 address for the specified adapter.
    /renew          Renew the IPv4 address for the specified adapter.
    /renew6         Renew the IPv6 address for the specified adapter.
    /flushdns       Purges the DNS Resolver cache.
    /registerdns     Refreshes all DHCP leases and re-registers DNS names
    /displaydns     Display the contents of the DNS Resolver Cache.
    /showclassid    Displays all the dhcp class IDs allowed for adapter.
    /setclassid     Modifies the dhcp class id.
    /showclassid6   Displays all the IPv6 DHCP class IDs allowed for adapter.
    /setclassid6    Modifies the IPv6 DHCP class id.

The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.

For Setclassid and Setclassid6, if no ClassId is specified, then the ClassId is removed.

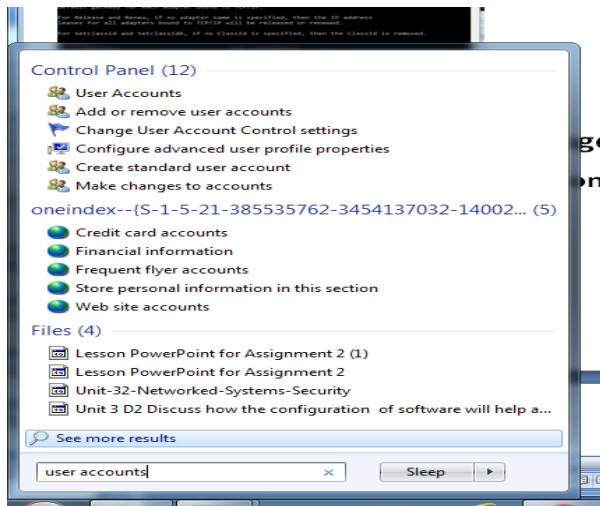
Examples:
    > ipconfig                ... Show information
    > ipconfig /all           ... Show detailed information
    > ipconfig /renew         ... renew all adapters
    > ipconfig /renew EL*     ... renew any connection that has its
                           name starting with EL
    > ipconfig /release *Con* ... release all matching connections,
                           eg. "Wired Ethernet Connection 1" or
                           "Wired Ethernet Connection 2"
    > ipconfig /allcompartments ... Show information about all
                           compartments
    > ipconfig /allcompartments /all ... Show detailed information about all
                           compartments

```

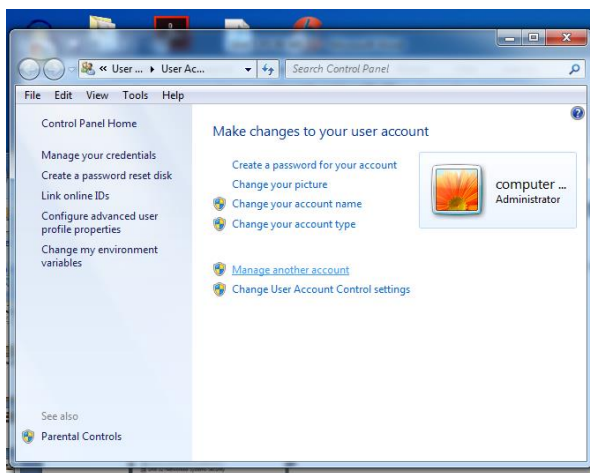
To configure an IP address, you open up the command prompt and input the command Ipconfig.

Undertake routine network management tasks (P6)

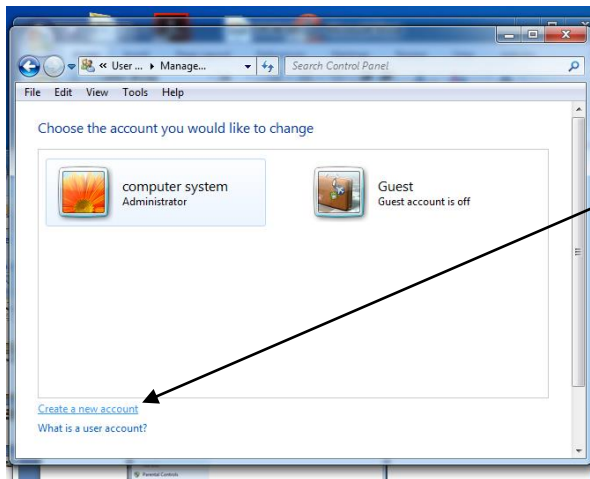
Creating user accounts/groups creation and deletion (Create user accounts on a network)



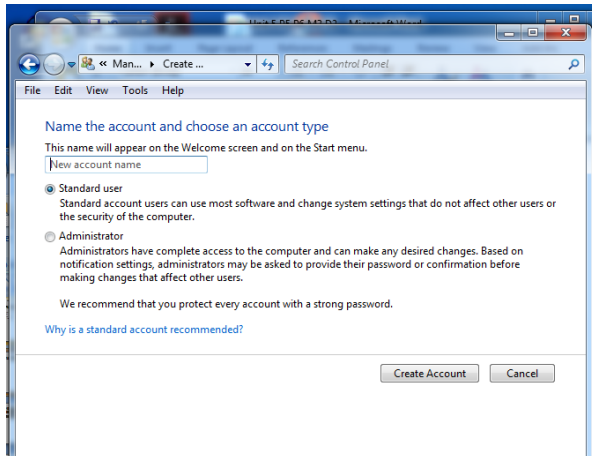
First go to the start menu on the bottom left and search up user accounts.



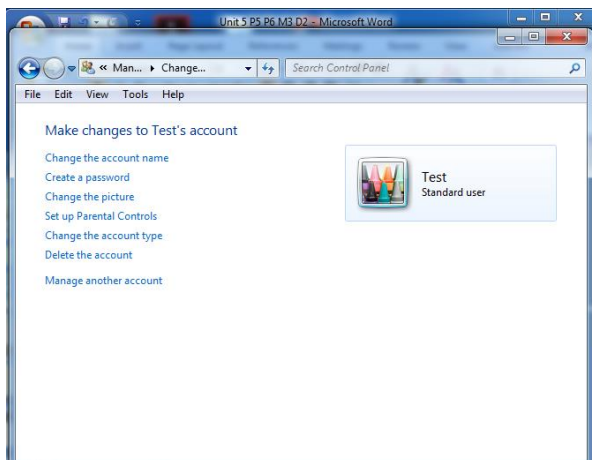
Once you have clicked on user accounts, click on manage another account.



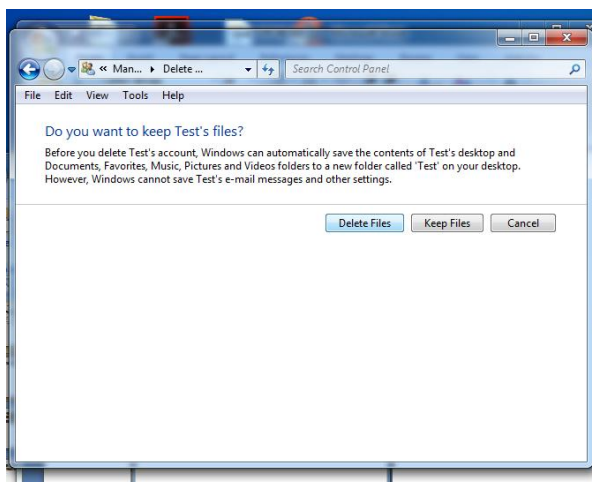
Next click on create a new account.



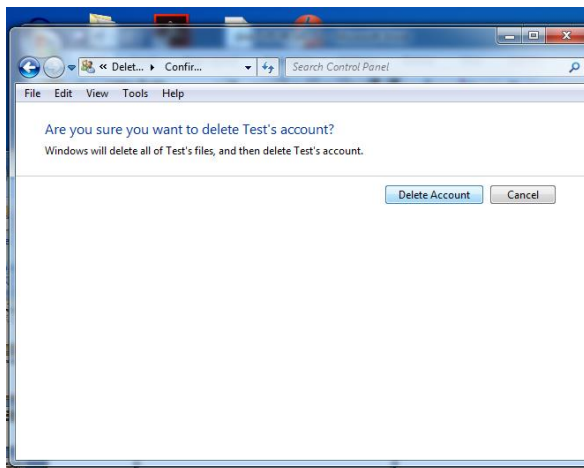
After you click on create a new account, choose what type of account you want to create. Here I'm creating a standard user account.



Now you have completed the creation of your account, you can then configure it for example adding a picture, parental controls, changing account name and creating a password. Next I will be explaining how to delete an account which is done by click delete the account.

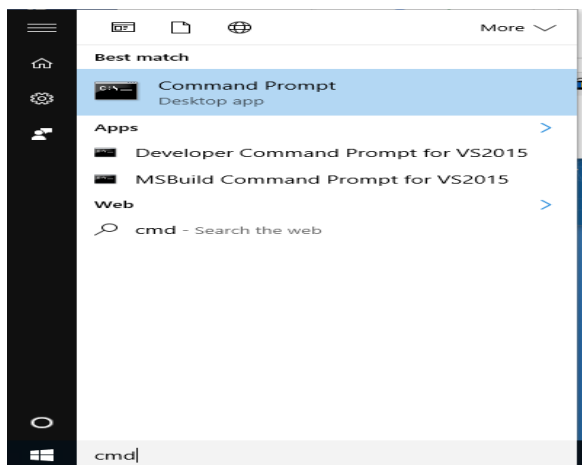


Once you clicked on delete the account, it will then ask you if you want to keep the files which were saved on the account. Here I'm clicking delete files due to there not being any important files on the account.

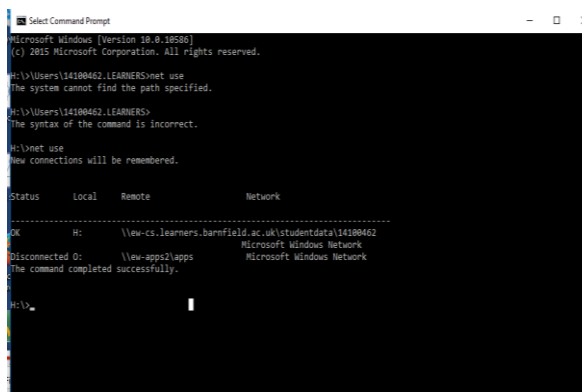


Here it will ask you if you are definitely sure that you want to delete your account. Once you clicked delete account, it will then be removed from your PC.

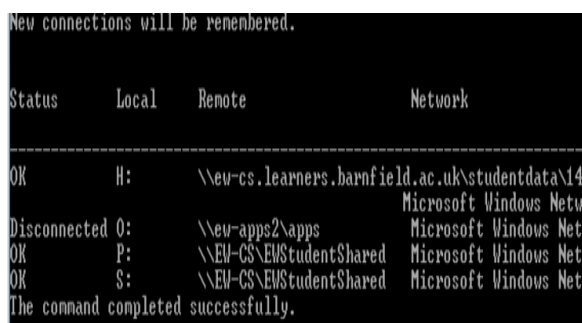
Login scripts



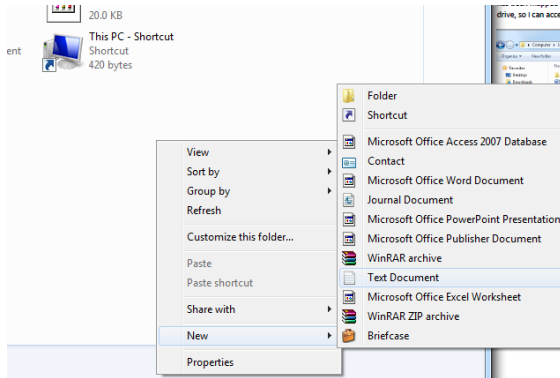
Next open up command prompt by searching up command prompt on the search bar on the start menu.



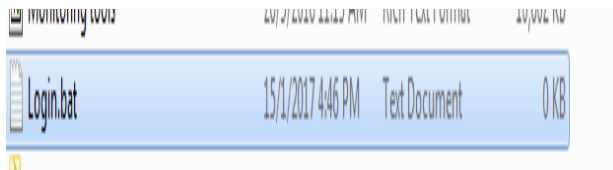
Next I will be using the command net use to see what network drives and location are already mapped out on this computer system or user account.



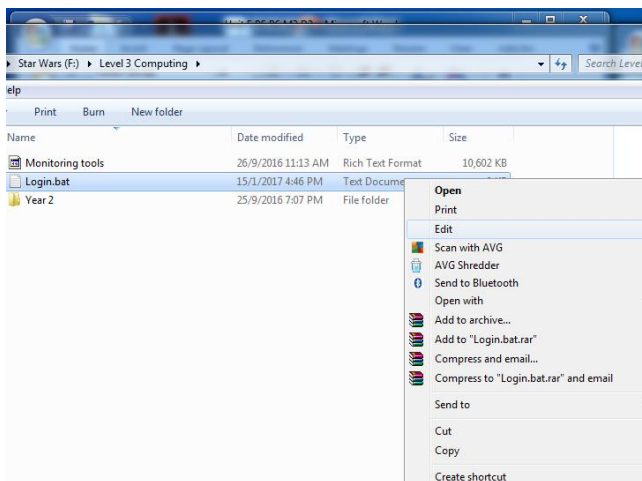
When I use the net use command you can then clearly see the network drive which has the letter P, has been mapped to my computer system and also the network location which is Student shared. Student shared is mapped to the P drive which allows me to access this location using this drive.



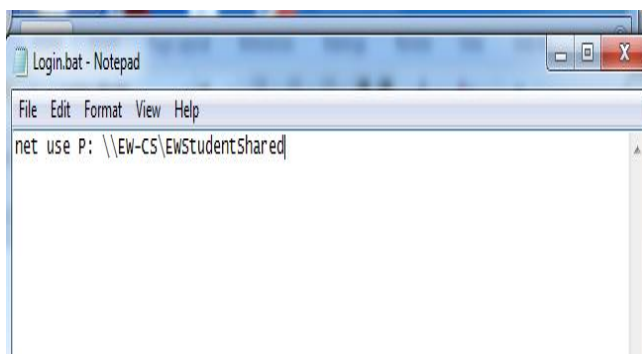
Next create a text file by right clicking your file explorer and go to new then click on text document.



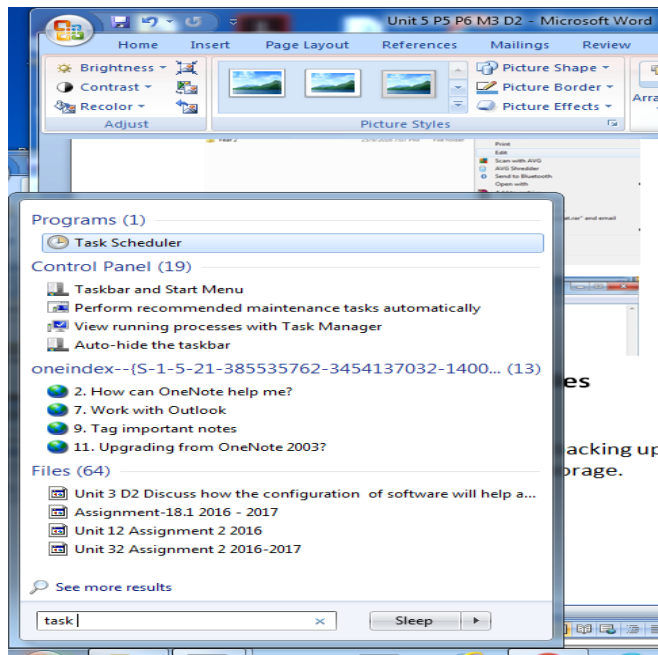
Next rename the file and call it login.bat



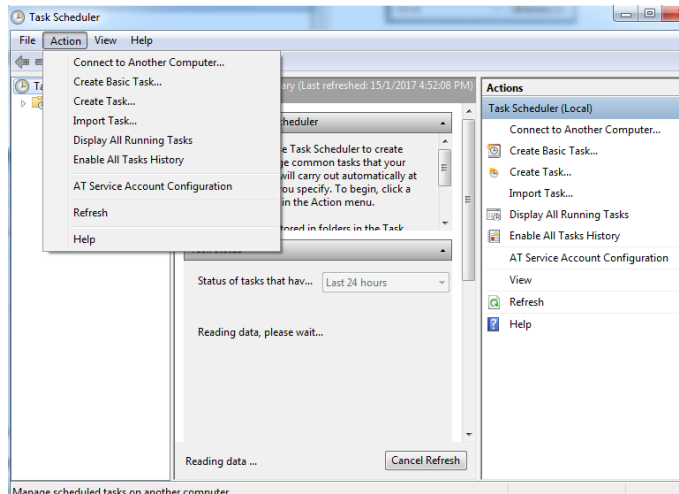
Next edit the text document by right clicking the file and clicking edit.



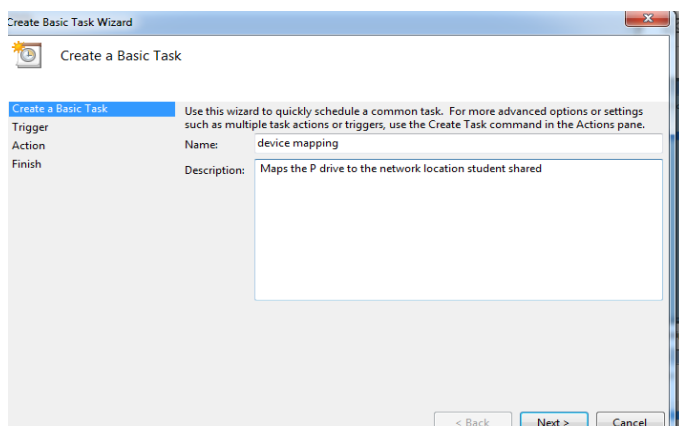
Next we'll be creating a script which performs what we just did but have it occur automatically every time the user logs on. To make this happen we have to input the following command shown on the left and save the file. Every time this script will run now, it will locate the student shared folder and be mapped to the drive with letter P.



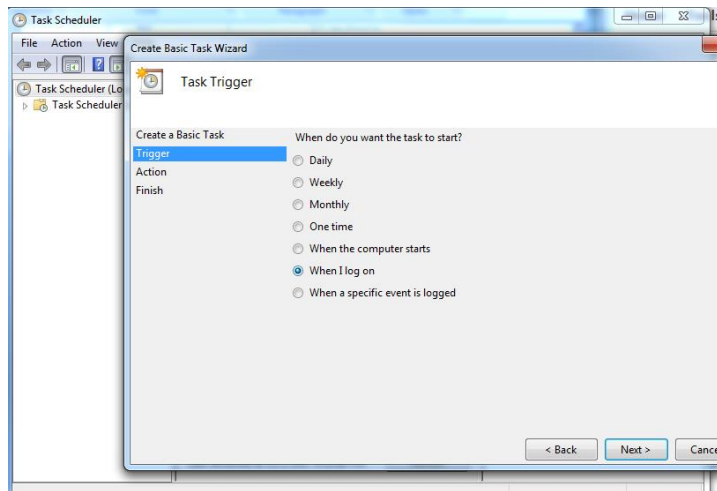
Next go to the start menu and search up task scheduler and click on it.



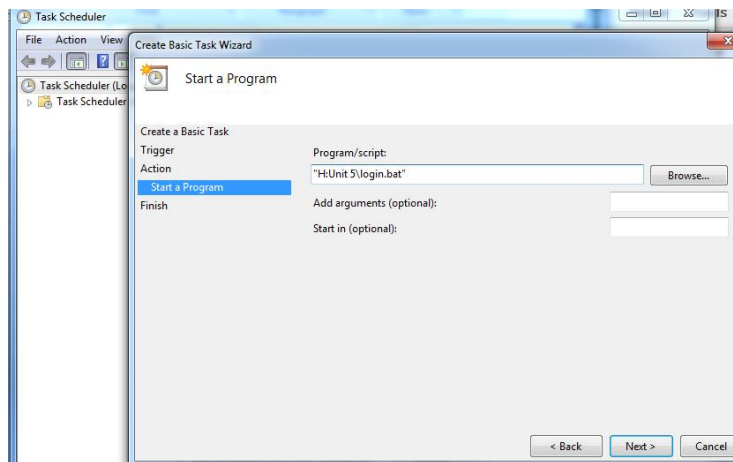
Once the application has opened, click on action on the top left and click on create new task.



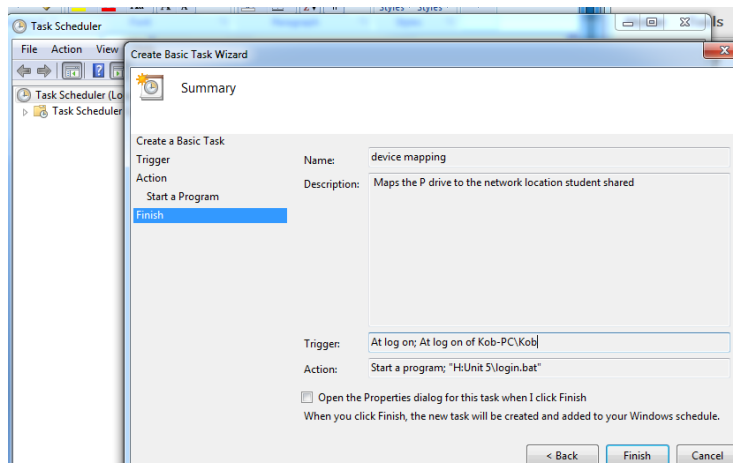
Next enter the name and description for this task and click next.



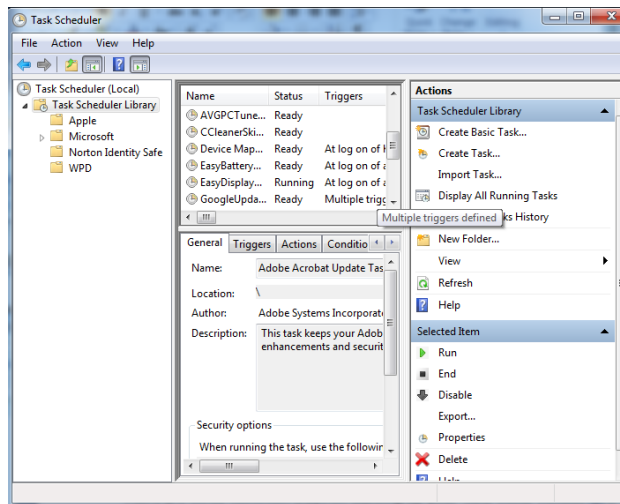
Next choose when you want the task to start. Here I chose when I log on and clicked next.



Next input the login.bat script which you have saved and click next.



Once you have fully configured everything the way you wanted to, click on finish.



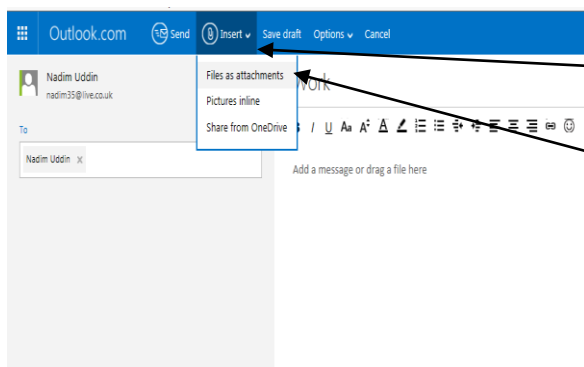
You will now be able to see the task that you created in the task scheduler home screen.

Backup and restore user files

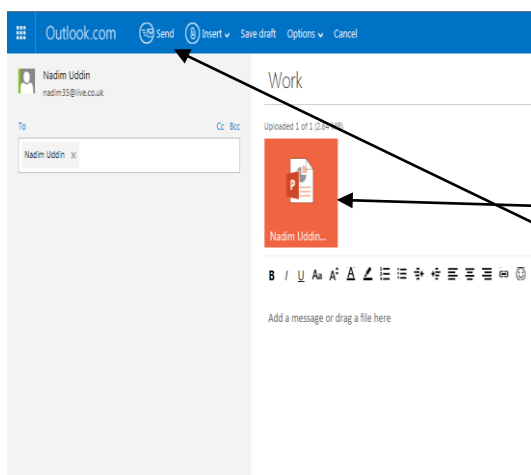
Backing up files

There are three common ways on backing up your files; these include using your email, flash drive and cloud storage.

Backing up files on your email



First create a new email message first and make yourself the recipient receiving the message. Next click on insert then click files as attachments.

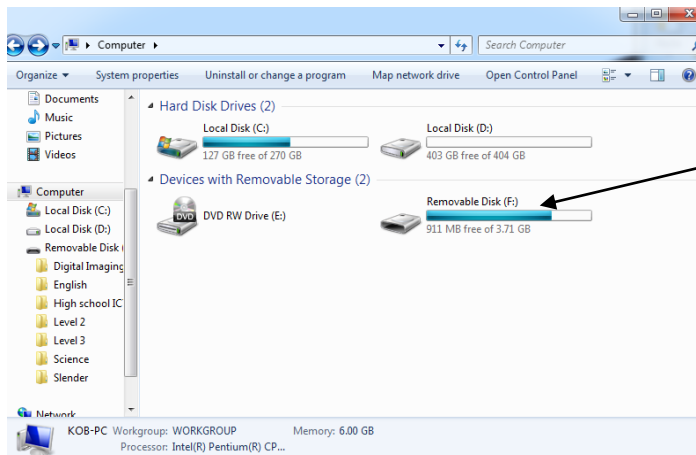


After your file has been attached you can now send the file to yourself and this will be saved onto your inbox. You can also archive it to separate it from the rest of the inbox.

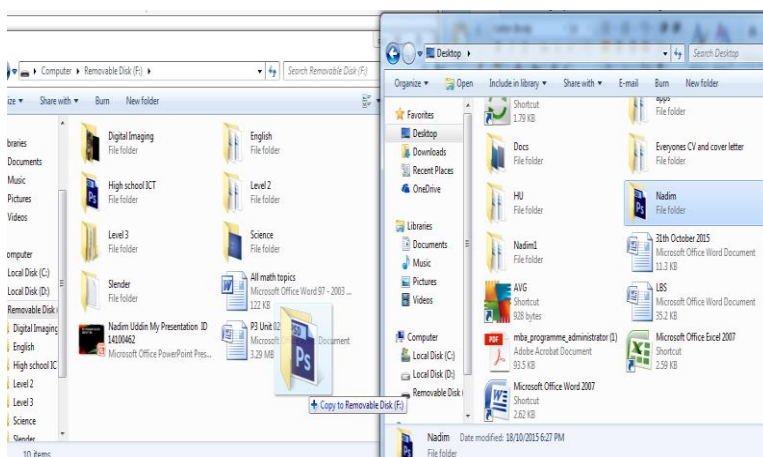
Flash drive



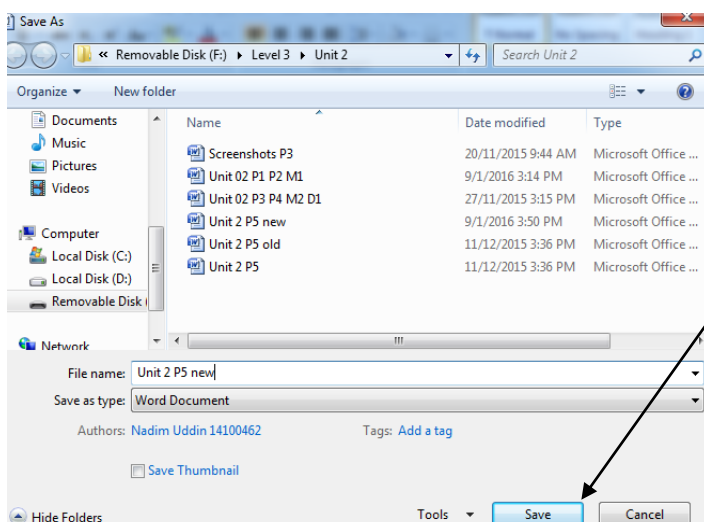
To back up with a flash drive, all you need to do is plug it into a computer systems USB port.



It should then appear on your computer system

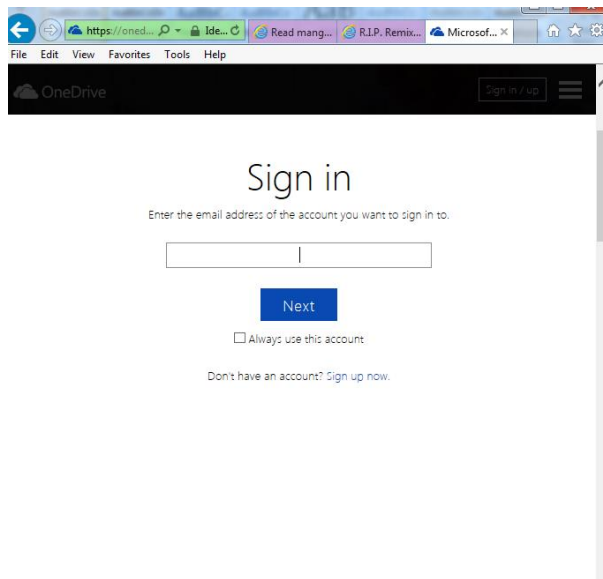


You can then can drag files into flash drive.

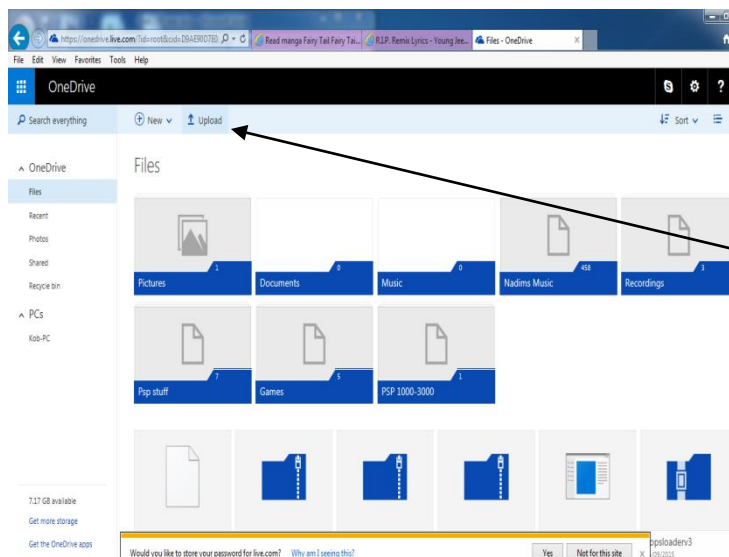


You can also save the files on the flash drive when you're doing "save as" on a software program.

Backing up on a cloud storage

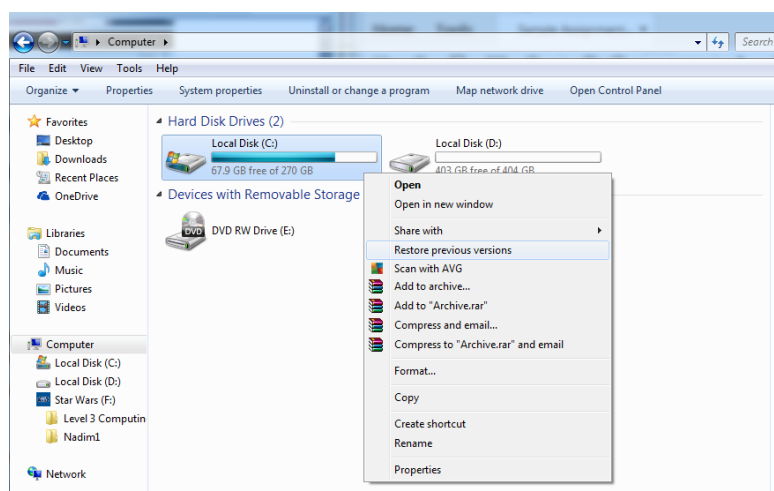


To save files on your cloud drive sign in to your email in the drive section which should be displayed on the email webpage.

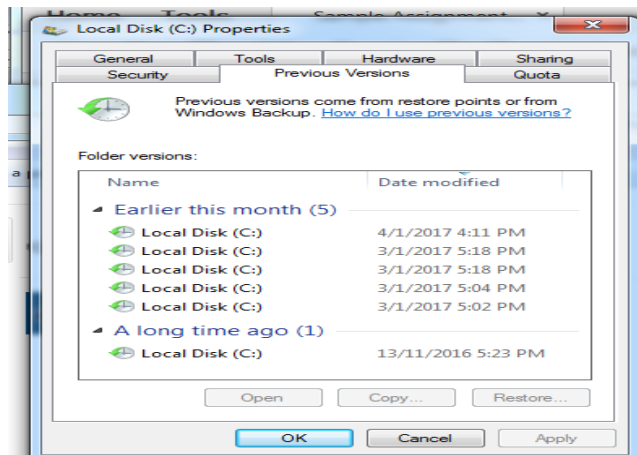


Once you have signed into your drive you can now add files to your drive but clicking on upload.

Restoring files



To restore files on your drive, you can go to the computer section on file explorer and right click on your desired computer drive. Once you have right clicked, click on restore preview versions.



Here you can revert back to a time where the file/folder was still on your drive. The options are displayed based on when the disk data was modified.

Design and develop login scripts to map a home and department directory networked shared drive

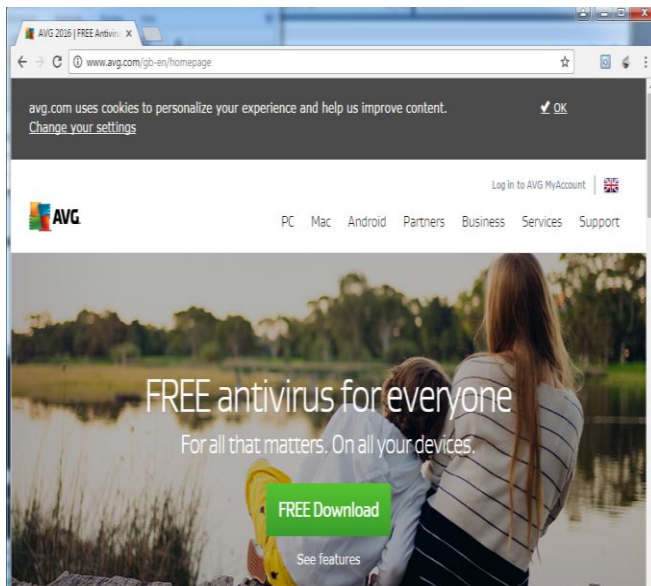
Automate system wide virus scans

Anti-Virus

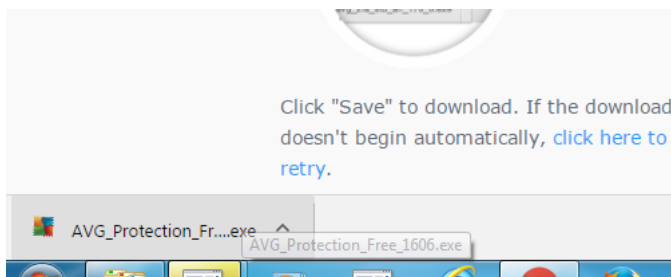
What is the purpose for your anti-Virus why should you update it?

The purpose of anti-virus software is two things that includes, blocking any viruses which are trying to allow themselves onto your computer when downloading something from the internet. When your antivirus detects the malware it will remove it. Depending on the settings you put on your anti-virus software that you have download or anti-virus software you may already have installed on your operating system, you can set it so it does basic scans which you can schedule to take place at certain times on your computer system. The benefit of anti-virus software is to protect your computer system from threats. Without anti-virus software you can become a victim to loss of data, scams or identity stealing. The reason why you should keep your anti-virus updated is because there are new viruses that are created every day and your anti-software needs to be aware of all of them and block out any vulnerabilities.

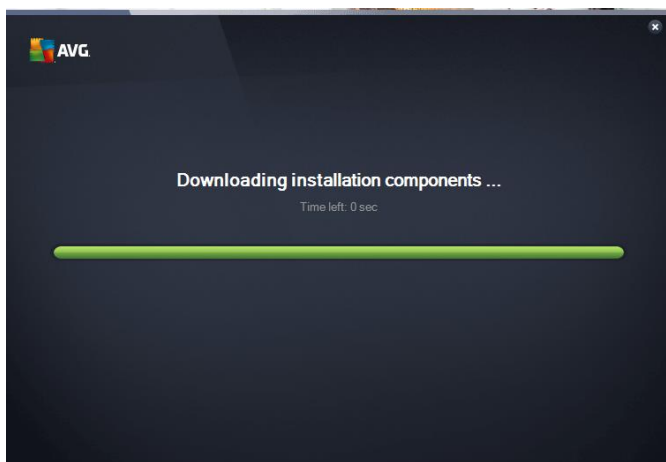
How to install and update your anti-virus software (Input how you installed the program)



To get a anti-virus software, find a good trusted website which provides an anti virus and click download.



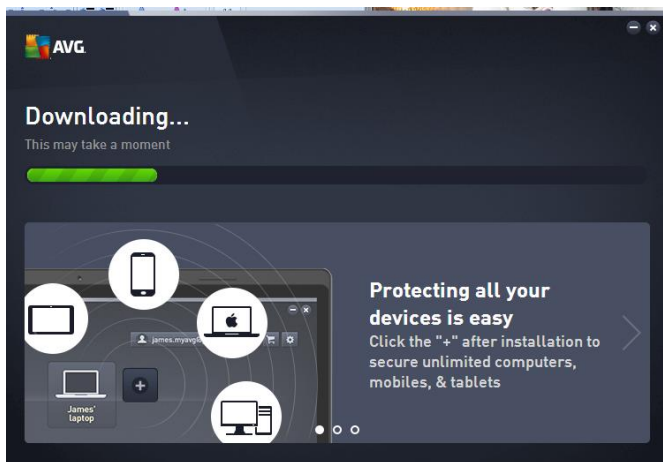
Here shows I got the installation ready. Click on it and either choose run or save to install the anti-virus software on your computer system.



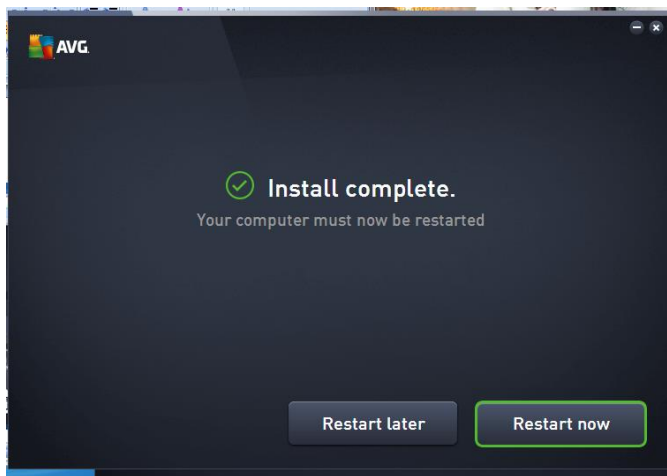
After you run the antivirus software it will then begin to install the components needed.



Here on this antivirus software you can choose whether or not you want the full protection which includes a fee or if you want an antivirus software for free with less features. Here I'm clicking full protection because there is a 30 day trial.



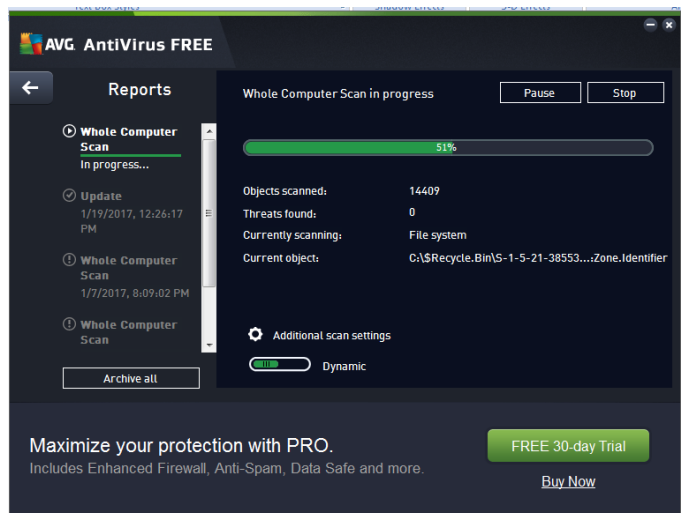
The antivirus software is now fully downloading.



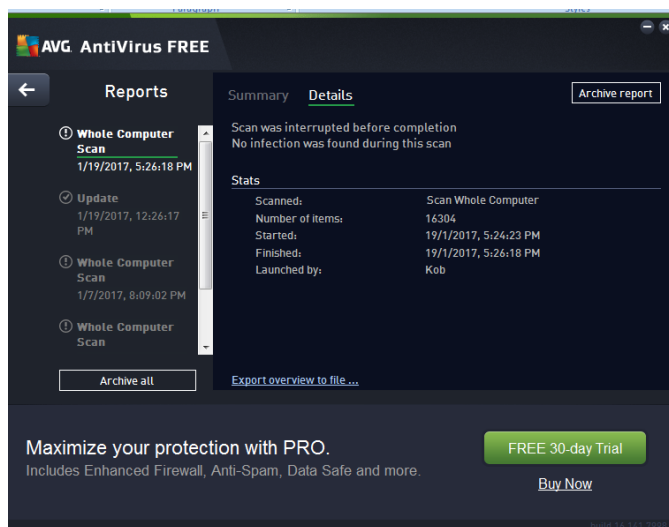
Now the antivirus software is now fully downloaded.



To scan your computer system click on scan now which should be in the antivirus section in your software.

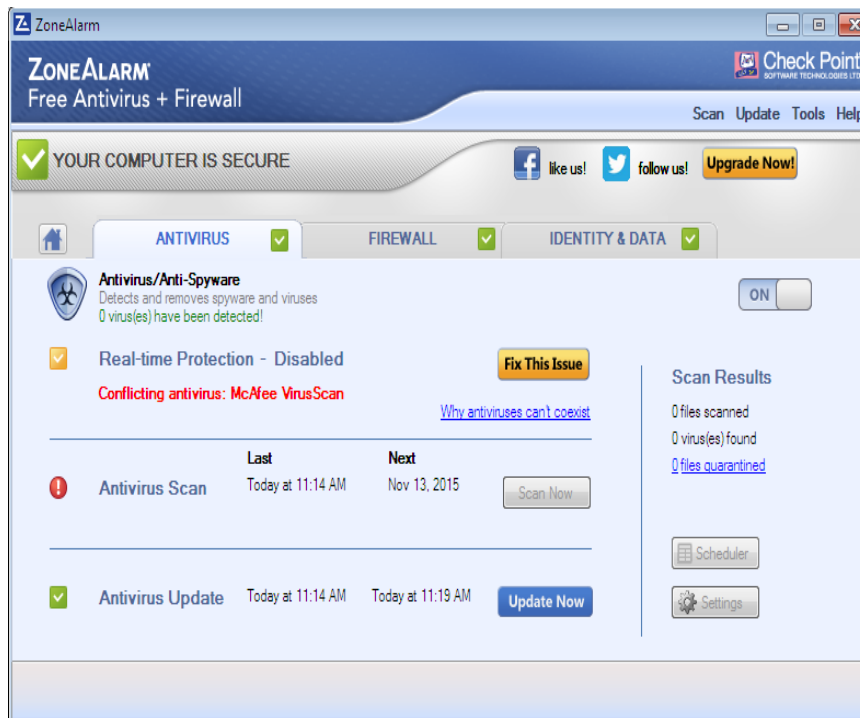


Here shows the antivirus software scanning your computer system.

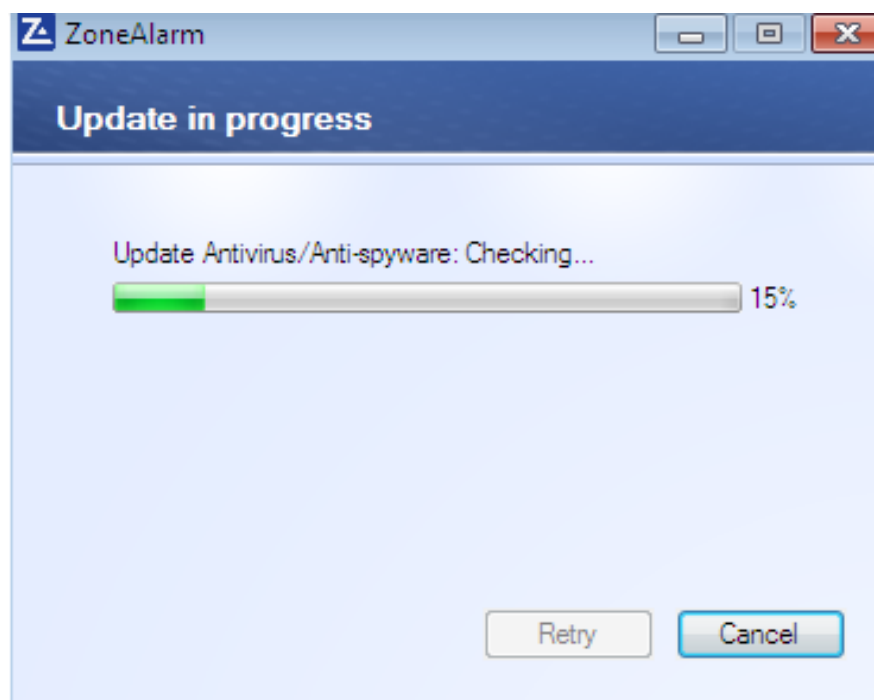


This is the end result after the scan.

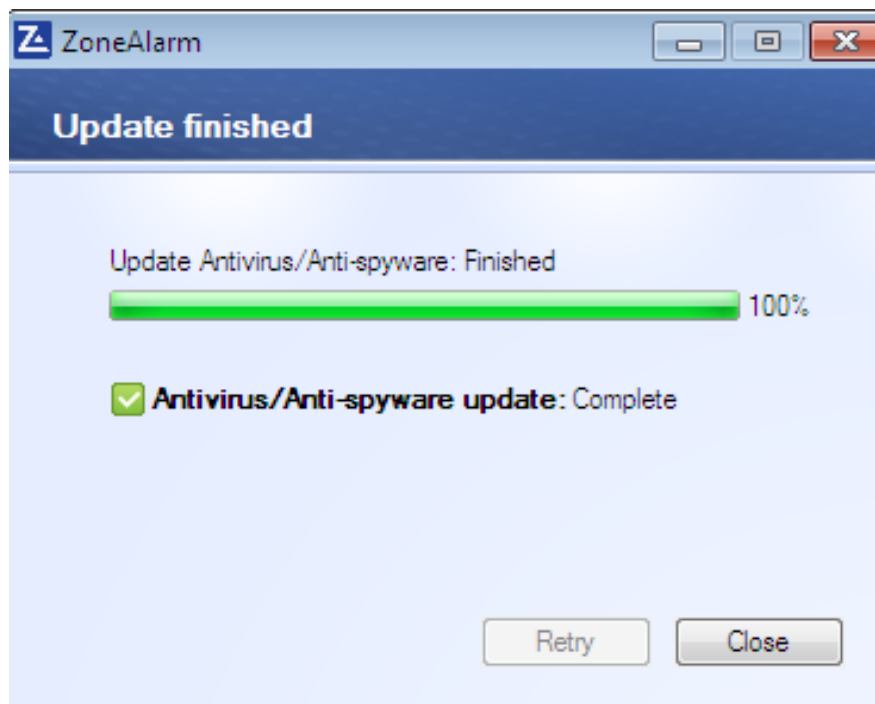
How to update an antivirus software



Once you have installed your anti-virus software click on “update now” so you have the latest version of anti-virus.



It should then be updating.



Once it has updated you should now have the latest version of the anti-virus.

Automate file clean ups (Set up an automatic clean up procedure)

Disk cleanup

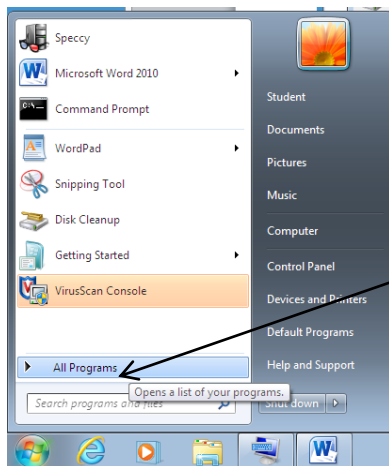
What is the purpose disk cleanup?

Disk cleanup is a utility software for the windows operating system. Disk cleanup allows users to remove files that are no longer needed on your system safely. Disk cleanup comes with many options which you can tick and untick, the recommended ones to delete would be automatically ticked for you, for exaple your recycle bin and old downloaded program files. There's also a new version of disk clean up which can delete additional data such as offline webpages, web/client published tempory files, catlog files for the content indexer and compress old files.

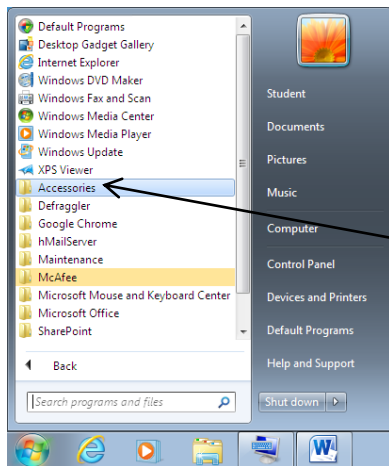
The disk cleanup process includes it analysing and searching the hard drive for files that are not needed. When it has finished searching, it will remove them and free up space on your hard drive, this can help make your computer system run a little bit more faster especially if your short on disk space.

The benefits of Disk cleanup is that it is designed to free up space on your hard drive and remove unneccsary files. Other then wanted to free up space on your hard drive you might want to speed up the bootup process by removing the unnessary files. Disk cleanup can also help with issues such as the infamous blue screen error or deleting virus infected file which take up a large space on your hard drive.

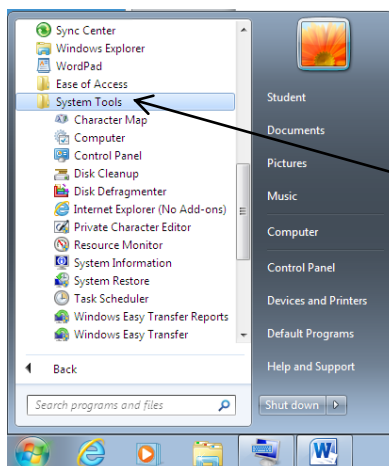
How to do a disk clean up



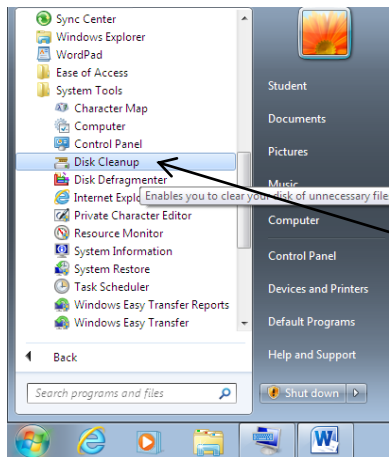
First of all go to the start menu and click on "all programs".



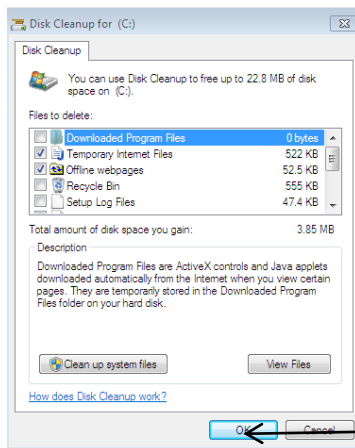
After you have clicked on all programs you then need to click on "accessories".



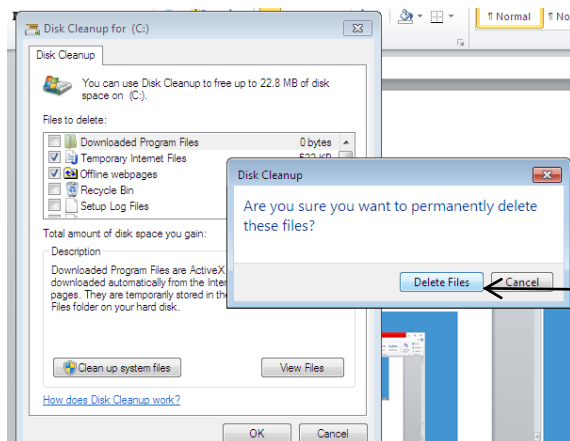
After you have click on the accessories folder you then click on "system tools".



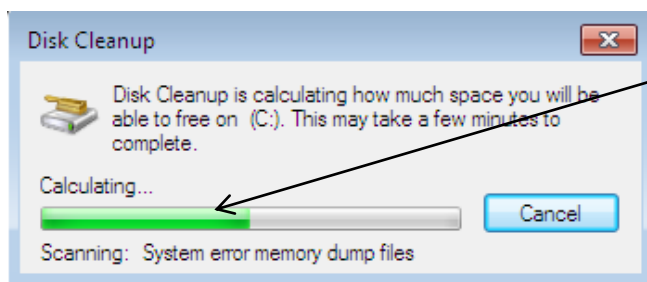
Once you have clicked on system tools you then have to click on disk clean up.



Once you have clicked on disk clean-up it should then appear with this screen. Some may be ticked already for you on files they recommend you deleting due to them be unnecessary files but you can also tick some yourself. Once you decided your ticked boxes then click on "OK"



It will then come up with this message if you are sure of your decision, click on delete files if you are fine with what you have decided.



Once you have clicked on delete files it should then be doing a disk clean up.

Keep accurate records of network management tasks (M3)

Task	Date	Comments
User account creation and deletion	05/02/16	I have created a user accounts ready for the new users to work on.
Backup and restore user files	05/03/16	I have backed all user accounts files to an external storage to make sure work productivity isn't affected and I have regained files users complained about by restoring the hardware to a previous version.
Design and develop login scripts to map a home & dept directory networked shared drive	10/03/16	I have designed and developed scripts to map a home and department directory networked shared drive. This allows users to have their own storage place for their personal files on the server and also have access to a shared drive.
Automate system wide virus scans	21/03/16	I have set up an automated antivirus which helps keep computer systems secure and it has been arranged during a time where users are not on computers so it doesn't affect work productivity.
Automate file clean up procedures.	25/04/16	I have set up an automated file clean up procedure to remove any unnecessary files that build up and keep processing on the computer system fast and efficient.

Design a network security policy for a small organisation (D2)

Security features

Device hardening

Device hardening is the term used to find various ways to protect a computer system. A protective security will protect in all layers meaning the host level, user level, application level, operating system level and all the other sublevels in between. The purpose of hardening is to make as less risks and threat possible. The main hardening activities you have on your computer system include

1. Hardening security policies, for example having a local policy which relates to how often you should change your password and what are the specifications for a good secure password.
2. Having a firewall will stop unauthorised access.
3. Disabling cookies so websites don't store information about you.
4. Never trusting unknown senders meaning not opening any emails or attachments which can potentially be a threat.
5. Having hot fixes and security patches updated.
6. Closing certain ports which include the server ports
7. Removing programs that may be unnecessary to have on your computer system.
8. When securing data, use encryption.
9. Having an anti-virus software and an anti-spyware software installed which can also have an anti-adware tool which stops any malicious software.
10. Disallowing any file sharing within programs

VPN access

VPN stands for Virtual private network. It is a technology that creates an encryption connection over a network which is less secure. The benefit on having a secure **VPN** is to make sure the right level of security to the connect systems because the network infrastructure alone can't keep it secure. The purpose of using a **VPN** access instead of just a private network is mainly because of the cost and feasibility. **VPN** access for remote access uses a public infrastructure for example the internet which provides remote users secure access to their organisations network.

Security policies and procedures

Security is important for any user who is looking to keep their data safe and this is especially for IT users. The **policy** and **procedure** for passwords is that users should regularly change their password and keep it complex with it consisting of special characters and numbers. The backup **policy** and **procedure** is that users should regularly back up their data on a separate device such as a computer system at home or a portable USB drive. In some company they may have more than one servers for the purpose of backing up. In most companies it is essential to have an anti-virus software and regularly scan the computer using it. A firewall is also necessary in a company because it stops any breaches in a network.

Security audits

Security audit is when you do an evaluation on the system of the security of an information system. It can be defined as a formal review of all the parts of the network. This is done by measuring how well it works by establishing a criteria. An audit that is thorough would normally assess the security of the systems software, information handling process, environment and user practices.

Your security audits should be able to:

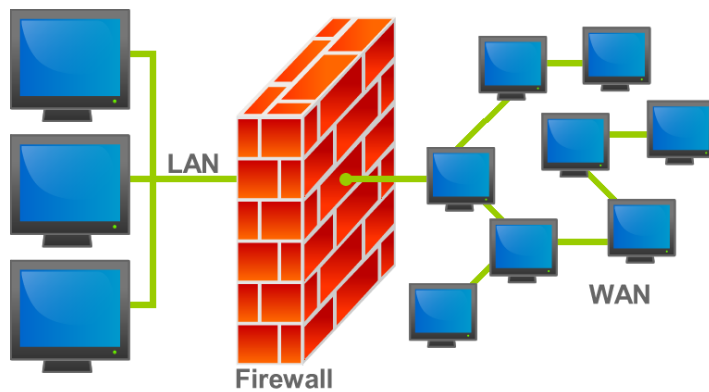
1. Be able to list all the risks that could damage the security on the network.
2. Be able to apply a security system that uses a clearance level to control the access to document and confidential files about the clients
3. Be able to apply an intrusion prevent system which is used as a safeguard for the network and the data within it plus stop authorised access from the firewall.
4. Explain what assets will be evaluated during the security audit.
5. Be able to regularly backup data and restore system to help minimise downtime and protect the client information in case of a security threat
6. Review threats that have occurred to see if there are any trends which can pinpoint a security weakness.
7. Analyse and order assets depending on the amount of vulnerabilities include and having a security response plan.
8. Ensure that information stored outside of the network is encrypted and protected.
9. Ensure the buildings security system is working and will be able to prevent penetrated from people who are not employees.

Review firewall

A **firewall** network security system which can be hardware and software based which can control incoming and outgoing traffic on a network based on a set of rules. A **firewall** can be seen as a barrier between a network. A **firewall** can control and restrict the access to resources on a network. To enforce a strong security companies separating their data from the internet using their **firewall**. When traffic tries to enter the firewall will only accept the data if the packets meet the specifications needed.

Your firewall must be able to identify attacks that hit it and these attacks are:

1. Attacks by intruders where they identify the exact position of the systems services and discovering vulnerabilities on the network
2. Denial of service attacks which is when an attack damages a network which results in computer systems become corrupt and deny users from access the network.
3. Access attacks which is when intruders attack the network for the purposing of obtaining data or attempts to change access rights.



Access control list policies

Access control list is a table that tells a computer operating system which access rights each user should have on a computer system such as an individual file or file directory. Each area has a security attribute which is identified on the **access control list**. The list has entries for each system user with access privileges. The common privileges include the ability to read only, edit only and read and write file. Examples of access control lists include Microsoft windows, NT/2000, OpenVMS and Netware.

Access control lists should be restricting users from accessing files that are not necessary to them and allowing resources that are necessary to them. The access control list should be recording what resources such as files or folders are being accessed by each of the users and it being logged in a database for the network manager to have access to. This log should be showing what users are able to access and what they are not authorised to access. Rights included for users is what they are and not allowed to do for example if the file is read or write or just read only this should be placed correctly by the **access control list**. Someone who has more authority should be able to see the access control list but cannot be changed unless it is done by the manager.

Unit 5 references

Information

<http://searchcio.techtarget.com/definition/security-audit> 12/13/16 2:01PM

<http://searchsecurity.techtarget.com/definition/firewall> 10/10/16 14:01PM

<https://www.techopedia.com/definition/24833/hardening> 13/10/16 11:06AM

<http://searchsoftwarequality.techtarget.com/definition/access-control-list> 13/01/17
11:40AM

<http://searchenterpriseWAN.techtarget.com/definition/virtual-private-network> 13/01/17
11:56AM

Images

<https://upload.wikimedia.org/wikipedia/commons/5/5b/Firewall.png> 19/10/16 15:27PM

<http://rebecca-w-h-btecit-unit5.blogspot.com/2015/10/d2-design-network-security-policy-for.html>