

	Page
How to Use this Module	ii
Introduction	iii
Technical Terms	iv
Learning Outcome # 1.....	1
Information Sheet # 7.1.1	2
Operation Sheet # 7.1.1	8
Learning Outcome # 2.....	9
Information Sheet # 7.2.1	11
Self Check # 7.2.1	14
Information Sheet # 7.2.2	15
Operation Sheet # 7.2.2	20
Self check # 7.2.2	22
Information Sheet # 7.2.3	23
Operation Sheet # 7.2.3	30
Learning Outcome # 3.....	31
Job Sheet # 7.3.1.....	33
Answer keys	37



Welcome to the Module **“Maintaining of Computer System and Networks”**. This module contains training materials and activities for you to complete.

The unit of competency **“Maintain Computer System and Networks”** contains knowledge, skills and attitudes required for a *Computer Hardware Servicing NC II* course.

You are required to go through a series of learning activities in order to complete each of the learning outcomes of the module. In each learning outcome there are **Information Sheets, Job Sheets, Operation Sheets, and Activity Sheets**. Follow these activities on your own and answer the Self-Check at the end of each learning activity.

If you have questions, don’t hesitate to ask your facilitator for assistance.

Recognition of Prior Learning (RPL)

You may already have some of the knowledge and skills covered in this module because you have:

- been working for some time
- already have completed training in this area.

If you can demonstrate to your teacher that you are competent in a particular skill or skills, talk to him/her about having them formally recognized so you don’t have to do the same training again. If you have a qualification or Certificate of Competency from previous trainings show it to your teacher. If the skills you acquired are still current and relevant to this module, they may become part of the evidence you can present for RPL. If you are not sure about the currency of your skills, discuss it with your teacher.

After completing this module ask your teacher to assess your competency. Result of your assessment will be recorded in your competency profile. All the learning activities are designed for you to complete at your own pace.

Inside this module you will find the activities for you to complete followed by relevant information sheets for each learning outcome. Each learning outcome may have more than one learning activity.



Course : **Computer Hardware Servicing NC II**
Unit of Competency : **Maintain Computer System and Networks**
Module : **Maintaining Computer Systems and Networks**

INTRODUCTION

This module contains information and suggested learning activities on Computer Hardware Servicing NC II. It includes the following competencies: plan and prepare maintenance procedures; maintain computer system and networks; and inspect and test computer system and networks.

It consists of **3** learning outcomes. Each learning outcome contains learning activities supported by each instructional sheet. Upon completion of this module, report to your teacher for assessment of what you achieved in terms of knowledge and skills requirement in this module. If you pass the assessment, you will be given a certificate of completion.

SUMMARY OF LEARNING OUTCOMES:

Upon completion of the module you should be able to:

- LO1. Plan and prepare maintenance procedures
- LO2. Maintain computer system and networks
- LO3. Inspect and test computer system and networks

PRE-REQUISITES:

You must have completed module 5 “Diagnose and Troubleshoot Computer System” and module 6 “Configure Computer Systems and Networks” before studying this module.



- **OHS** – Occupational Health and Safety
- **Port hub /Port** – is a connector on the back of a computer or other device. A port is either a serial port or a parallel port.
- **Modem** - (**Modulator-Demodulator**) The modem is a device that allows a given computer to share data or otherwise a device which let computers exchange information
- **USB** – (Universal Serial Port)
- **Scanner**- is an input device that read text or illustration printed on paper, translates the information into a form that a computer can use.
- **Printer** - is a piece of hardware that produces a paper copy (also known as ‘hardcopy’) of the information generated by the computer.
- **Flash drive** –_a portable storage device which is plug directly to the USB port.

- **Network** – a group of computers and associated devices that are connected by communications facilities.
- **OS (Operating system)** software that controls the allocation and use of programs and data that a computer uses.
- **Software** – programs and data that a computer uses.
- **Maintenance** - is the testing and cleaning of equipment.
- **Planning** – is both the organizational process of creating and maintaining a plan; and the psychological process of [thinking](#) about the activities required to create a desired [future](#) on some scale
- **Computer System** - The complete computer made up of the CPU, memory and related electronics (main cabinet), all the peripheral devices connected to it and its operating system. Computer systems fall into two broad divisions: clients and servers. Client machines fall into three categories from low to high end: laptop, desktop and workstation. Servers range from small to large: low-end servers, midrange servers and mainframes.
- **Defragmentation** – the process of reorganizing and rewriting files so that they occupy one large continuous area on your hard disk.
- **CRT** – (Cathode Ray Tube) A display device used in computer monitors and television sets.
- **Boot sector** – The part of the formatted disk containing the operating system loading a program.
- **Virus** – A program intended to damage your computer system without your knowledge and permission.



Course : **Computer Hardware Servicing NC II**
Unit of Competency : **Maintain Computer System and Networks**
Module : **Maintaining Computer System and Networks**

Learning Outcome 1: Plan and Prepare Maintenance Procedures

Assessment Criteria:

1. Planning and preparing for maintenance task is organized as a prerequisite.
2. OHS policies are carried out along with the task.
3. Computer system is regularly checked in compliance with maintenance procedures.
4. Appropriate materials are used for ensuring work delivery that conforms with task specifications.
5. Proper tools, equipment and testing devices for maintenance purposes are obtained and checked against correct operation and safety.
6. Computer system and network are maintained based on the manual instructions

References:

1. Bigelow, Stephen J., *PC Technician's Troubleshooting*, McGraw Hill
2. Kelly, Dianne Rose, *Computer Maintenance and Troubleshooting Handbook* **Rose Nelson** WEB: <http://home.comcast.net/~>
3. Sandler, Corey, *Fix Your Own PC*, MIS Press
4. Kuhlman, Dave, dkuhlman@rexx.com
<http://www.rexx.com/~dkuhlman> Dave Kuhlman. This documentation is covered by The MIT License: <http://www.opensource.org/licenses/mit-license>
5. Meyers, Mike, *Introduction to PC Hardware and Troubleshooting*, McGrawHill
6. www.eserviceinfo.com
7. <http://csd/2.computer.org>
8. <http://sevier.com/wps>
9. www.yahoo.com



Plan and Prepare Maintenance Procedures

Introduction:

Planning and preparing systematic maintenance procedure save time, money and frustration. It is a good idea and opportunity to learn the proper care and maintenance of your computer.

PC maintenance is an important topic for anyone who owns a PC. Looking after your PC properly ensures you of trouble-free use. Regular PC maintenance also keeps the machine's performance optimal.

A. Plan Maintenance Procedures for Computer System and Networking.

1. Design a systematic maintenance plan for hardware.

- Design a monitoring, evaluating and updating plan.
- Place your computer in a well-ventilated area.
- Schedule use of computer for its longer life.
- Move the computer only when it is turned off and unplugged.
- Treat your computer properly.
- Maintain your hard disk

2. Design a systematic maintenance plan for your software.

- Backup your files
- Install or secure passwords
- Delete temporary files
- Update anti-virus and spy ware



MONTHLY COMPUTER MAINTENANCE PLAN

	JUNE	JULY	AUG	SEPT	OCT	NOV	DEC
Anti virus software checkups							
Disk space utilization							
Defragmentation of hard drives							
Troubleshoot hardware and software issues							

TYPES OF MAINTENANCE PROCEDURE:

- (1) Hardware maintenance is the testing and cleaning of equipment.

- (2) Information system maintenance is the routine updating of master files, such as adding and deleting employees and customers and changing credit limits and product prices.

- (3) Software or program maintenance is the updating of application programs in order to meet changing information requirements, such as adding new functions and changing data formats. It also includes fixing bugs and adapting the software to new hardware devices.

- (4) Disk or file maintenance is the periodic reorganizing of disk files that have become fragmented due to continuous updating.

PC HARDWARE SERVICING

The Strengthened Technical-Vocational Education Program



Work place procedures

- Identify hazards and assess risk.
- Execution of OHS policies are carried out along with the task.

Following certain procedure is very important to perform a given operation or evolution or in reaction to a given event. The table below shows different elements and their corresponding performance criteria to be able to identify occupational health and safety hazards, and assess risk, as well as follow instructions and procedure in the workplace with minimal supervision. The students will also be capable of participating and contributing to OHS management issues.

ELEMENT	PERFORMANCE CRITERIA
1. Identify hazards and assess risk.	1.1 Identify hazards in the work area and during the performance of workplace duties. 1.2 Assess level of risk
2. Follow procedures and strategies for risk control.	2.1 Report hazards in the work area to designated personnel according to workplace procedures 2.2 Follow workplace procedures and work instructions for assessing and controlling risks with minimal supervision. 2.3 Whenever necessary, within the scope of responsibilities and competencies, follow workplace procedures for dealing with hazards and incidents, fire and/or other emergencies.



ELEMENT**PERFORMANCE CRITERIA**

<p>3. Contribute to OHS in the workplace.</p>	<p>3.1 Describe employee’s rights regarding consultation on OH&S matters</p> <p>3.2 Raise task and/or job specific OH&S issues with appropriate people in accordance with workplace procedures and relevant OH&S legislative requirements</p> <p>3.3 Contribute to participative arrangement for OH&S management in the workplace within organisational procedures and the scope of responsibilities and competencies</p> <p>3.4 Provide feedback to supervisor on hazards in work area in line with organisational OH&S policies and procedures</p> <p>3.5 Provide support in implementing procedures to control risks in accordance with organisational procedures</p>
<p>Examples of OHS issues which may need to be raised by workers with designated personnel may include:</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Identified Hazards <input type="checkbox"/> Problems encountered in managing risks associated with hazards <input type="checkbox"/> Clarification on understanding of OHS policies and procedures <input type="checkbox"/> Communication and consultation processes <input type="checkbox"/> Follow up on reports and feedback. <input type="checkbox"/> Effectiveness of risk controls in place <input type="checkbox"/> Training needs



Materials, Tools, Equipment and Testing Devices.

Programming Tools

- (1) Programming tools are used for software development or system maintenance. Virtually, any program or utility that helps programmers or users develop applications or maintain their computers can be called a tool. Examples of programming tools are compilers, interpreters, assemblers, 4GLs, editors, debuggers and application generators.
- (2) Programming tools help the user analyze or search for data. For example, query and report programs are often called query tools and report tools.
- (3) An on-screen function in a graphics program; for example, line draw, circle draw or brush tool.
- (4) A software control panel for setting user preferences.
- (5) Sometimes people will call any software a "tool." For example, the phrase, "there aren't any tools to do that job" means that no application is available to perform the required processing.



Equipment/Facilities	Tools & Instruments	Supplies & Materials
<p>Server</p> <p>Computer peripherals</p> <p>Desktop computers</p> <p>OHS guidelines</p> <p>Phil. Environmental protection standards</p> <p>Monitors</p> <p>Motherboard</p> <p>Power supply</p> <p>Network device and cabling</p> <p>Hubs</p> <p>Switches</p> <p>LAN Cards</p> <p>Printers and</p> <p>Scanners</p> <p>Routers</p> <p>USB Flash Drives</p>	<p>Protective eye wear</p> <p>Wire stripper with cutter</p> <p>Pliers(Assorted)</p> <p>Screw drivers (Assorted)</p> <p>Soldering iron/gun</p> <p>De-soldering tool</p> <p>Flashlight</p> <p>Tweezers</p> <p>Mirrors</p> <p>Antistatic wrist wrap</p> <p>LAN Tester</p> <p>Crimping tool</p> <p>Software installer</p> <p>Work bench</p> <p>Magnifying glass</p>	<p>Floppy disk</p> <p>Compact Disk</p>



Plan and Prepare Maintenance Procedure

1. Prepare/Design a daily maintenance plan for your hardware, (time allotment: 1 week)

MAINTENANCE TASK	MON	TUE	WED	THUR	FRI
Recalibrate the battery					
Clean computer case					
Clean the keyboard					
Clean the mouse					
Clean the screen					
Clean up hard drives					

2. Design a systematic daily plan for your software, (time allotment: 1 week)

MAINTENANCE TASK	MON	TUE	WED	THUR	FRIDAY
Create an emergency diskette					
Check for viruses					
Back up files					
Defragment hard drive					
Scan hard drive for errors					



Program course : **Computer Hardware Servicing NCII**

Unit of Competency : **Maintain Computer System and Networks**

Module : **Maintaining Computer System and Networks**

LO.2 : **Maintain Computer System and Networks**

Assessment Criteria:

1. Appropriate personal protective equipment are used in conformity with the standard procedures.
2. Periodic maintenance of the equipment is performed following manufacturer’s requirements.
3. Established procedures are followed in case of repair and parts replacements.
4. Accidental events or conditions are responded to in accordance with the established standards.

Resources:

Equipment/Facilities	Tools & Instruments	Supplies & Materials
Server	Protective eye wear	Floppy disk
Computer peripherals	Wire stripper with cutter	Compact Disk
Desktop computers	Pliers(Assorted)	
OHS guidelines	Screw drivers (Assorted)	
Phil. Environmental protection standards	Soldering iron/gun	
Monitors	De-soldering tool	
Motherboard	Flashlight	
Power supply	Tweezers	
Network device and cablings	Mirrors	
Hubs	Antistatic wrist wrap	
Switches	LAN Tester	
LAN Cards	Crimping tool	
Printers and Scanners	Software installer	
Routers	Work bench	
	Magnifying glass	



USB Flash Drives		
------------------	--	--

Reference:

1. McLaughlin,Robert, Sasser,Susan, Ralston,Mary.Fix Your Own PC.Philippine Graphic Arts, Inc Tandang Sora St.Caloocan City
2. Meralco Faoundation. Microcomputer Servicing Plus. Pasig City, Philippines.
3. Legaspi,Carlos, Caiña, Mark Anthony. Operate A Personal Computer. Dasmariñas Computer Learning Center.Dasmariñas,Cavite, Philippines
4. Bigelow,Stephen J. PC Technician’s Troubleshooting ,McGaw Hill
5. www.helpwithpcs.com
6. <http://en.wikipedia.org>
7. www.techsoup.org
8. www.howstuffworks.com
9. www.microsoft.com/technet/network



Tools and equipment used to protect the user and the computer system.

Types of personal protective devices

1. Anti-static devices
2. Power surge protectors
3. Personal equipments



ESD (Electro Static Discharge)

-A small amount of static electricity that can destroy small parts of your computer.

Anti-static devices

Devices designed to protect the computer from static electricity.

Examples:

1. Anti-static wrist strap
2. Anti-static mat
3. Anti-static bag
4. Anti-static spray

Power surge protectors

Devices designed to protect the computer from sudden power surges from intermittent power sources.

Examples:

1. AVR (Automatic Voltage Regulators)
2. UPS (Uninterrupted Power Supply)

Personal Equipment

1. Small paint brush
2. Screw drivers
3. Pliers and tweezers
4. Compressed air
5. Handheld vacuum



Periodic Maintenance Scheme

Regular scheduled upkeep of your computer will keep you and your computer in working smoothly.

Daily Schedule

- Update virus and spyware definitions
- Do incremental backup – back up updated files for each date.
- Reboot upon crash- Reboot the computer to fix your pc upon crash.

Weekly

- Full virus and spyware scan
- Complete backup of files
- Patch up –Get latest software update for your operating system.

Monthly

- Clean your PC inside and out.
- Defrag your hard drive to speed up its operation.

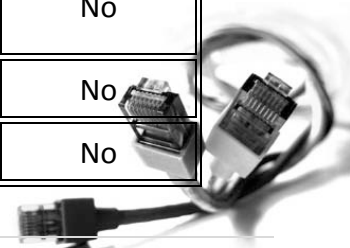
Yearly

- Check your programs – clean up unused programs
- Reformat your hard drive and reinstall the operating system
- Make a full diagnostic check on hardware and software



Sample Maintenance scheme

Preventive Maintenance Activity	Recommended Frequency	Auto?
Scan hard disk file systems for errors	Daily	Yes
Scan for viruses	Daily	Yes
Back up data	Daily	No
Clean CRT screen	Weekly	No
Defragment hard disks	Monthly	Yes
Scan for hard disk read errors	Weekly	Yes
Clean mouse	Monthly	No
Check for full hard disk volumes and remove unnecessary files	Monthly	No
Update virus definition files	Monthly	Sometimes
Check power protection devices to ensure they are still protecting the system	Quarterly	No
Check power supply fan for ventilation and dirt buildup and clean if necessary	Quarterly	No
Back up CMOS information	Quarterly	No
Update emergency boot floppies	Quarterly	No
Clean floppy disk drive internals and read/write heads	Quarterly (depending on use)	No
Check processor temperature, inspect heat sink and fan to ensure they are working	Annually (or whenever case is opened)	No
Check hard disk for temperature and vibration	Annually (or whenever case is opened)	No
Clean exterior of case	Annually	No
Clean exterior of monitor	Annually	No
Check and clean interior, motherboard and expansion cards if necessary	Annually	No
Check internal connections and cables	Annually	No
Clean keyboard	Annually	No



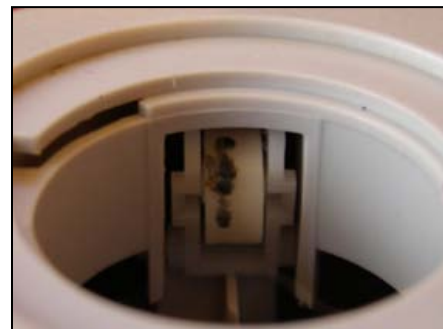
Answer the following questions

1. For somebody who always works with computers, what personal protective devices do you usually use? How often do you use them?
2. Computers should be protected from static electricity to prevent component malfunction. What anti-static devices can you utilize to avoid such malfunction?



Cleaning the Mouse

1. Shut down the PC before cleaning the mouse.
2. Roll the mouse over onto its back and remove the ball access slide cover.
3. Wash the mouse ball with water.
4. Inspect the mouse ball's chamber, for lint, dirt and threads and carefully remove any you find with tweezers.
5. Blow out the mouse ball chamber with compressed air.
6. If needed, you can use isopropyl alcohol to clean the exterior of the mouse.
7. Reconnect the mouse and restart the computer to give it a complete test



Cleaning the Monitor

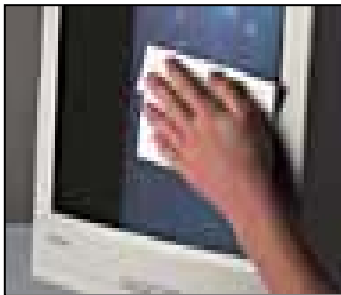
1. Turn off the monitor and unplug it from the power source.
2. Using compressed air, clean away any dust on the top of the monitor's case.
3. Use a soft cloth and isopropyl alcohol to clean the outside of the monitor.
4. Use an antistatic cleaner to clean the glass of the monitor.
5. Reconnect the monitor and test the performance.



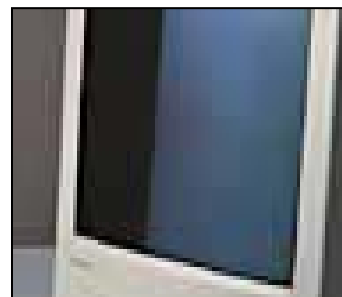
1



2



3



4



Procedure in cleaning the keyboard

1. Shut down the computer and turn off the computer.
2. Disconnect the keyboard from the computer and lay it upside-down on a flat, clean work surface.
3. Remove the screws that hold together the keyboard case.
4. Holding the case together, turn the keyboard over, and then remove the top cover. Use the compressed gas and/or brush and vacuum to clean out the keys.
5. Taking care not to dislodge any keys, remove the key assembly from the case.
6. If the keyboard has a circuit card attached to the key assembly, remove it and set it aside.
7. Remove the screws that hold the back metal plate to the key assembly. Put the screws in a cup or another container so you won't lose them.
8. Carefully lift off the metal plate. What you find underneath depends on the design of the keyboard. Carefully lift and clean the contacts on the card with the alcohol and cloth.
9. Probably, there will be some type of rubber pad between the printed circuit and the back of the keys. Carefully lift this up and clean any spill residue from the pad as well as the backs of the keys.
10. Reassemble the pads, printed circuit, circuit card and metal plate, and then turn the assembly right-side up again.
11. It would be a good idea to remove the keys and clean them, as well. They should pop off. Just don't remove more than a few at a time, because you'll have a real nightmare to figure out which key go where. Clean under them with the alcohol and cloth.



Printer Cleaning

Inkjet Printer

1. Clean the print nozzle regularly. Most inkjet printers have a built-in utility to clean or unclog the print head nozzles. You should do this regularly, especially if the printer sits idle for a couple of weeks.
2. Never turn a printer off by pulling the plug from the power source. Always use the printer's power switch to turn it off. The printer has some built-in functions, such as parking the print head that are tied to the power-off function of the printer's on/off switch.
3. Use inkjet quality paper.
4. Dust and paper scraps and bits can collect in the bottom of the paper path in an inkjet printer. Remove the paper scraps and blow out any dust or paper bits that have accumulated with compressed air.

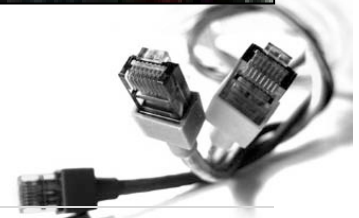


Cleaning your system unit

Cleaning the system unit and its parts is not really difficult to do; you just need the proper tools to clean it properly. Using compressed air antistatic strap and a Phillips screw driver you can effectively clean your unit

The parts that need cleaning are the ff:

1. Motherboard
2. Memory
3. Interface cards
4. Hard drives
5. Optical Drives
6. System Case



Computer Hardware Maintenance and Cleaning

Equipment and Materials:

Equipment

System unit

Monitor

Keyboard and Mouse

Printer

Materials

Screw driver

Air Compressor

Anti-static Strap

Computer Hardware Maintenance and Cleaning

The student is provided with the necessary equipment and materials to clean the different hardware components of a computer unit.



You will be assessed using the following criteria

Evaluation: CRITERIA	Passed	Failed
1. Periodic maintenance is observed		
2. Observance of safety precautions.		
3. Appropriate materials are used in cleaning the hardware components.		
4. Confirmation of computers normal function.		



Write your answers on your answer sheet:

1. Enumerate the basic tools needed in cleaning your system unit.
2. Can we use anti-static glass cleaner when cleaning the monitor? Yes or No.
Why?
3. Is it safe to clean your printer when it is still on? Explain.
4. Why do we need to shutdown our computer unit before we clean and disassemble?



Computer Virus

- A virus is a destructive executable program that infects the other programs in the [system](#) and spreads by replicating itself.
- Such a program is designed to damage the victim's [computer](#) files.
- Viruses are coded by malicious programmers in a way that they can spread in the system without one's permission and knowledge.



Virus Origins and History

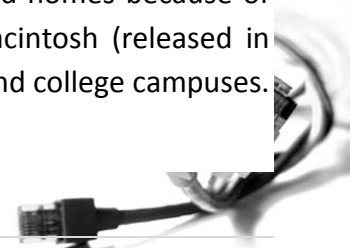
People create viruses. A person has to write the code, test it to make sure it spreads properly and then release the virus. A person also designs the virus's attack phase, whether it's a silly message or destruction of a hard disk. So why do people do it?

There are at least three reasons. The first is the same psychology that drives vandals and arsonists. Why would someone want to bust the window on someone else's car, or spray-paint signs on buildings or burn down a beautiful forest? For some people, that seems to be a thrill. If that sort of person happens to know computer programming, then he or she may funnel energy into the creation of destructive viruses.

The second reason has to do with the thrill of watching things blow up. Many people have a fascination with things like explosions and car wrecks. When you were growing up, there was probably a kid in your neighborhood who learned how to make gunpowder and then built bigger and bigger bombs until he either got bored or did some serious damage to himself. Creating a virus that spreads quickly is a little like that -- it creates a bomb inside a computer, and the more computers that get infected the more "fun" the explosion.

The third reason probably involves bragging rights, or the thrill of doing it. Sort of like Mount Everest. The mountain is there, so someone is compelled to climb it. If you are a certain type of programmer and you see a security hole that could be exploited, you might simply be compelled to exploit the hole yourself before someone else beats you to it.

Traditional computer viruses were first widely seen in the late 1980s, and they came about because of several factors. The first factor was the spread of personal computers (PCs). Prior to the 1980s, home computers were nearly non-existent or they were toys. Real computers were rare, and they were locked away for use by "experts." During the 1980s, real computers started to spread to businesses and homes because of the popularity of the IBM PC (released in 1982) and the Apple Macintosh (released in 1984). By the late 1980s, PCs were widespread in businesses, homes and college campuses.



The second factor is the use of computer bulletin boards. People could dial up a bulletin board with a modem and download programs of all types. Games are extremely popular, and so are simple word processors, spreadsheets, etc. Bulletin boards lead to the precursor of the virus known as the Trojan horse. A Trojan horse is a program that sounds really cool when you read about it. So you download it. When you run the program, however, it does something uncool like erasing your disk. So you think you are getting a neat game, but it wipes out your system. Trojan horses only hit a small number of people because they are discovered quickly. Either the bulletin board owner would erase the file from the system or people would send out messages to warn one another.

Different Aspects of Computer Virus

Finder- searches for the new uninfected files and the

Replicator- actually targets these files and infects it by multiplying itself.

Types of virus

Resident Viruses

This type of virus is a permanent which dwells in the RAM memory. From there it can overcome and interrupt all of the operations executed by the system: corrupting files and programs that are opened, closed, copied, renamed etc.

Examples include: Randex, CMJ, Meve, and MrKlunky.

Direct Action Viruses

The main purpose of this virus is to replicate and take action when it is executed. When a specific condition is met, the virus will go into action and infect files in the directory or folder that it is in and in directories that are specified in the AUTOEXEC.BAT file PATH. This batch file is always located in the root directory of the hard disk and carries out certain operations when the computer is booted.

Overwrite Viruses

Virus of this kind is characterized by the fact that it deletes the information contained in the files that it infects, rendering them partially or totally useless once they have been infected.

The only way to clean a file infected by an overwrite virus is to delete the file completely, thus losing the original content.



Examples of this virus include: Way, Trj.Reboot, Trivial.88.D.

Boot Virus

This type of virus affects the boot sector of a floppy or hard disk. This is a crucial part of a disk, in which information on the disk itself is stored together with a program that makes it possible to boot (start) the computer from the disk.

The best way of avoiding boot viruses is to ensure that floppy disks are write-protected and never start your computer with an unknown floppy disk in the disk drive.

Examples of boot viruses include: Polyboot.B, AntiEXE.

Macro Virus

Macro viruses infect files that are created using certain applications or programs that contain macros. These mini-programs make it possible to automate series of operations so that they are performed as a single action, thereby saving the user from having to carry them out one by one.

Examples of macro viruses: Relax, Melissa.A, Bablas, O97M/Y2K.

Directory Virus

Directory viruses change the paths that indicate the location of a file. By executing a program (file with the extension .EXE or .COM) which has been infected by a virus, you are unknowingly running the virus program, while the original file and program have been previously moved by the virus.

Once infected it becomes impossible to locate the original files.

Polymorphic Virus

Polymorphic viruses encrypt or encode themselves in a different way (using different algorithms and encryption keys) every time they infect a system.

This makes it impossible for anti-viruses to find them using string or signature searches (because they are different in each encryption) and also enables them to create a large number of copies of themselves.

Examples include: Elkern, Marburg, Satan Bug, and Tuareg.



File Infectors

This type of virus infects programs or executable files (files with an .EXE or .COM extension). When one of these programs is run, directly or indirectly, the virus is activated, producing the damaging effects it is programmed to carry out. The majority of existing viruses belong to this category, and can be classified depending on the actions that they carry out.

Companion Viruses

Companion viruses can be considered file infector viruses like resident or direct action types. They are known as companion viruses because once they get into the system they "accompany" the other files that already exist. In other words, in order to carry out their infection routines, companion viruses can wait in memory until a program is run (resident viruses) or act immediately by making copies of themselves (direct action viruses).

Some examples include: Stator, Asimov.1539, and Terrax.1069

FAT Virus

The file allocation table or FAT is the part of a disk used to connect information and is a vital part of the normal functioning of the computer.

This type of virus attack can be especially dangerous, by preventing access to certain sections of the disk where important files are stored. Damage caused can result in information losses from individual files or even entire directories.

Worms

A worm is a program very similar to a virus; it has the ability to self-replicate, and can lead to negative effects on your system and most importantly they are detected and eliminated by anti-viruses.

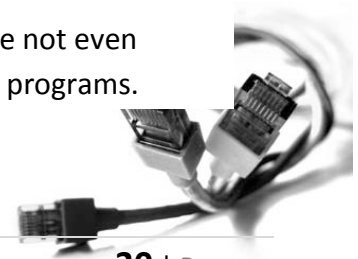
Examples of worms include: PSWBugbear.B, Lovgate.F, Trile.C, Sobig.D, Mapson.

Trojans or Trojan Horses

Another unsavory breed of malicious code are Trojans or Trojan horses, which unlike viruses do not reproduce by infecting other files, nor do they self-replicate like worms.

Logic Bombs

They are not considered viruses because they do not replicate. They are not even programs in their own right but rather camouflaged segments of other programs.



How do Virus Affect a System?

- It corrupts files
- It slows down the speed of the computer system
- It causes the system to hang frequently
- It deletes various files

Sources of Virus Infection

A virus can enter the system and infect it through various sources. Some of the sources are

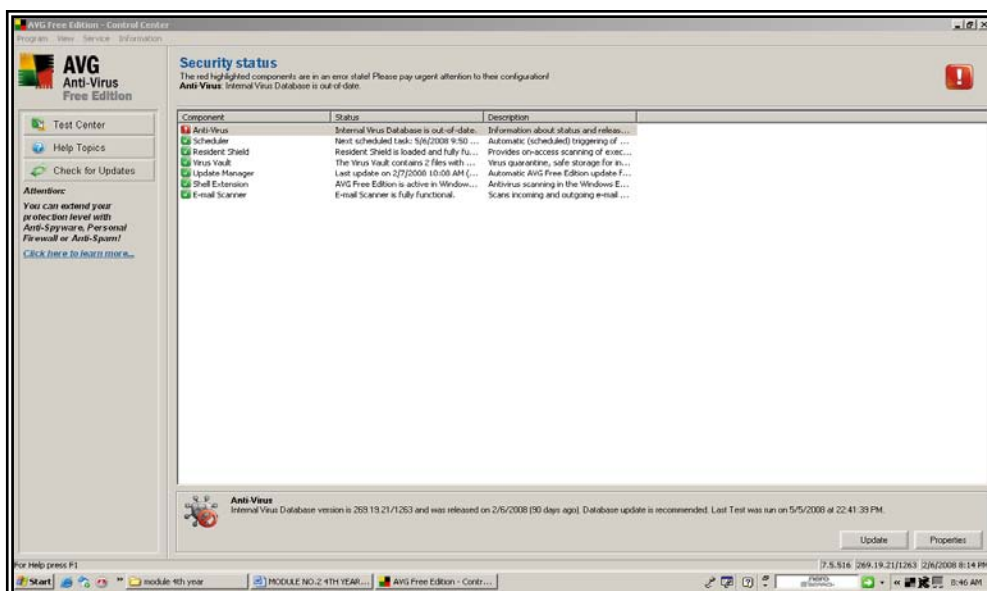
- Infected CDs, DVDs, pen drives, etc
- E-mail
- Browsing infected sites
- Downloading files from the internet

Steps to Remove Viruses

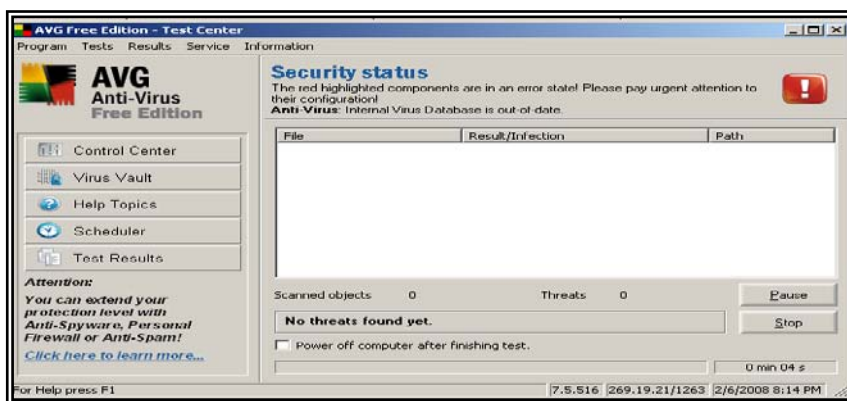
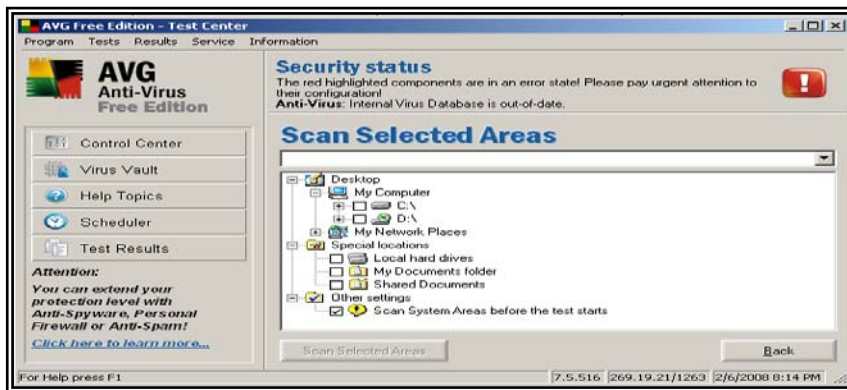
Removing viruses, though technical, is yet a very simple process if all the required steps are properly followed.

The basic steps are:

- Buy or download an antivirus software(AVG Anti-virus)
- Install the antivirus software



- Update antivirus software with the latest virus definitions
- Do a complete system scan



Methods of Eliminating Viruses

Removing the virus – When the virus can be easily identified and can be removed without affecting other files, then the antivirus removes it from the host place.

Quarantine – This is done when the virus cannot be easily identified removed from the file and the removal of virus means the removal of the complete file. In this method, although the virus is not eliminated, it is rendered inactive by moving the file into "quarantine" and renaming it.

Anti-virus Software

Software is designed to cure virus infected machines. An anti-virus is a program that searches for, identifies and removes potential viruses existing in the computer system



Examples of Anti-virus software

- Symantec Norton antivirus
- AVG antivirus
- McAfee Scan
- Microsoft Antivirus
- Kaspersky
- Avast



Virus removal

Equipment and Materials:

Equipment

System unit

Monitor

Keyboard and Mouse

Materials

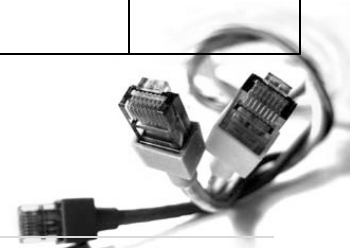
Anti-virus Software (Any Anti-virus software)

Virus removal

Provided with the necessary equipment and materials troubleshoot the virus infected area.

You will be assessed using the following criteria

Evaluation:	Passed	Failed
CRITERIA		
1.Periodic maintenance is observed		
2. Safety precautions are observed.		
3. Appropriate materials are used in virus removal.		
4. Computers Normal function is confirmed.		



Program Course : **Computer Hardware Servicing NCII**

Unit of Competency : **Maintain Computer System and Networks**

Module : **Maintaining Computer System and Networks**

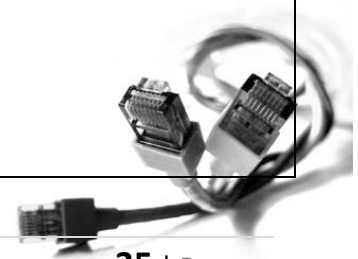
LO.3 Title : **Inspecting and testing computer system and networks**

Assessment Criteria:

1. Final inspection of the device is instituted to ensure task perfection.
2. Laboratory management and maintenance are observed to conform to company standard.
3. Accomplishment report is delivered to concerned teacher after finishing the task.

Resources:

Equipment/Facilities	Tools & Instruments	Supplies & Materials
Server	Protective eye wear	Floppy disk
Computer peripherals	Wire stripper with cutter	Compact Disk
Desktop computers	Pliers(Assorted)	
OHS guidelines	Screw drivers (Assorted)	
Phil. Environmental protection standards	Soldering iron/gun	
Monitors	De-soldering tool	
Motherboard	Flashlight	
Power supply	Tweezers	
Network device and cablings	Mirrors	
Hubs	Antistatic wrist wrap	
Switches	LAN Tester	
	Crimping tool	
	Software installer	



LAN Cards	Work bench	
Printers and Scanners	Magnifying glass	
Routers	Allen key .05-.25	
USB Flash Drives	IC insertion/extraction tool	
	RS-232 pin insertion/extraction tool	

Reference:

1. McLaughlin,Robert, Sasser,Susan, Ralston,Mary.Fix Your Own PC.Philippine Graphic Arts, Inc Tandang Sora St.Caloocan City
2. Meralco Faoundation. Microcomputer Servicing Plus. Pasig City, Philippines.
3. Legaspi,Carlos, Caiña, Mark Anthony. Operate A Personal Computer. Dasmariñas Computer Learning Center.Dasmariñas,Cavite, Philippines
4. Bigelow,Stephen J. PC Technician’s Troubleshooting ,McGaw Hill
5. www.helpwithpcs.com
6. <http://en.wikipedia.org>
7. www.techsoup.org
8. www.howstuffworks.com
9. www.microsoft.com/technet/network



Computer System and Network Inspection

Materials, Tools and Equipment

Equipment:

2 Computer units

Printer

HUB Switch

MODEM/Router

Network Cable

LAN Tester

Multi-tester

Materials:

Windows XP CD installer

Windows 98 CD installer

Anti-virus Software

Computer Maintenance Software

Hardware Inspection

Given the following tools and equipment, perform hardware inspection. Check the computers connection and configuration and check for the voltage output of the power supply.



Software Inspection

Given the following materials, perform software inspection.

Check for the ff:

1. Viruses
2. Unnecessary software
3. Drivers are installed

Network Inspection

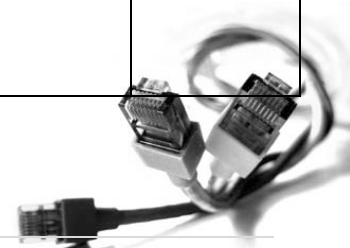
Given the following tools, perform network inspection.

Check the ff:

1. File and printer sharing
2. Internet connection
3. Proper cable connection

You will be assessed using the following criteria

Evaluation:			
	CRITERIA	Passed	Failed
	1. Sequence of steps.		
	2. Observance safety precautions.		
	3. Proper inspection of hardware components.		
	4. Proper inspection of the power supply.		



Network and Internet Inspection

You will be assessed using the following criteria

Evaluation:			
	CRITERIA	Passed	Failed
	1. Sequence of steps.		
	2. Observance of safety precautions.		
	3. Proper inspection of network components.		
	4. Proper inspection of network connection.		

Software Inspection

You will be assessed using the following criteria

Evaluation:			
	CRITERIA	Passed	Failed
	1. Sequence of steps.		
	2. Observance of safety precautions.		
	3. Proper inspection of operating system.		
	4. Proper virus removal.		



After the inspection, the student will create an accomplishment report to be submitted to the teacher.

Accomplishment report

Area to be Inspected	Good running condition	Bad running condition	Remarks
HARDWARE			
SOFTWARE			
NETWORK			



Answer key# 7.2.1

1. Personal protective devices are the tools and equipment used to protect the user and the computer system
2. Anti-static devices
 - Anti-static wrist strap
 - Anti-static mat
 - Anti-static bag
 - Anti-static spray

Answer Key #7.2.2

1. Compress Air, Phillip Screw driver, Anti-static strap
2. Yes
3. No
4. To avoid the risk of electrical shock.

