F20FO/F21FO - Digital Forensics

Lab 04: Data Hiding & Data Recovery

Lab 4: Objectives

This lab intends to introduce you to some topics of data hiding and data recovery (a core concept of forensics and security) and how a disk is partitioned. At the end of the lab you will be able:

1. Use VMware and use Virtual Machines.
2. To partition a disk
3. Examine and Repair MBR
4. To search and recover files from digital storage

Notes

There is nothing to submit at the end of this lab, however students are encouraged to log their results in a document. There are some questions coloured in blue that you can use as indication to record in your logbook (e.g. lab04_logbook). Often the lab instructions are intentionally open ended, and you will have to figure some things out for yourselves.

The lab will require you to install software and download additional resources from the Resources module for lab04 in Canvas. Before you start reading the instructions, download the files you will need for this lab. Changes to your machine should not impact on its functionality - however you are recommended to use a VM.

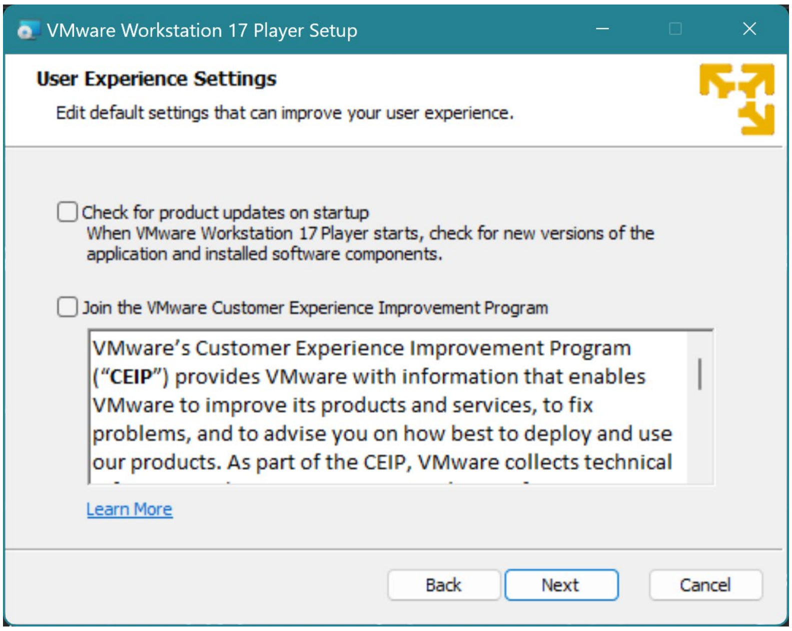
As a user it would be nice to see what a recovered file was originally called or when it was created. Even better if we would be able to put it back in its original folder on a partition. In forensics this provides context which helps when investigating data, as a name and location tells a lot about a file. Therefore, if you get a device, or raw capture of a device (a dd file), and there appears to be no data present, it would be useful if you could identify and recover any partitions. Or, if you come to a computer in your normal line of work and attempt to turn it on and it doesn't boot, you may want to repair it.

Lab 4.1: Create Partitions on Disk

Download the VM "Windows XP Pro - chrome" - you will need to unzip it.

You will use VMware for this section of the lab. You might come across different virtualisation software or toolkits in Digital Forensics workplaces. You can download WMware Player v17 from the lab04 resources folder. If you already have VMware Worksation Pro, then you do not need the Vmware Player v17. Before you install the VMware Player v17, read the notes on the next page.

It is recommended to use the VMware v17 setup files provided from Canvas for this lab. When you start installing VMware v17, you should untick the ‘Check for product updates…’ and the ‘Join the VMware…’ checkboxes.



Once you install VMware you might need to restart your machine.

Install and launch the VM using VMWare Player - you will need to unzip it. Select open in VMWare Player, as shown in Figure 1.

Figure 1: VMPlayer

Navigate to the folder where you saved “Windows XP Pro - chrome” select the .vmx file there, see Figure 2.

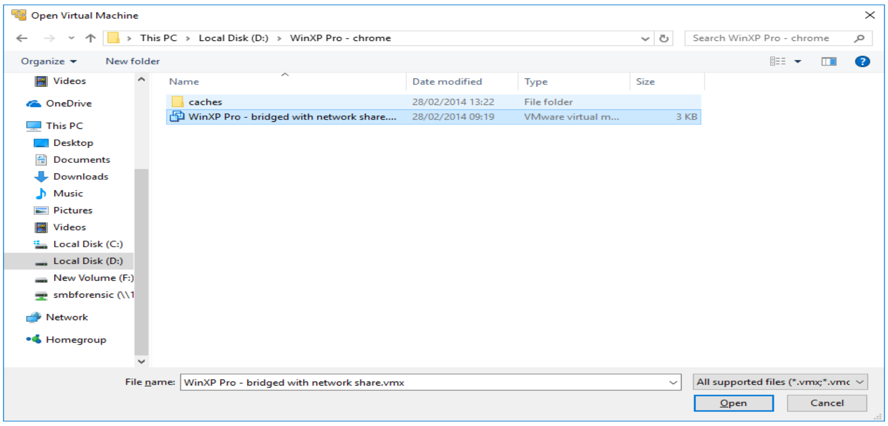


Figure 2: Open VMX file

You will see a screen as shown in Figure 3.

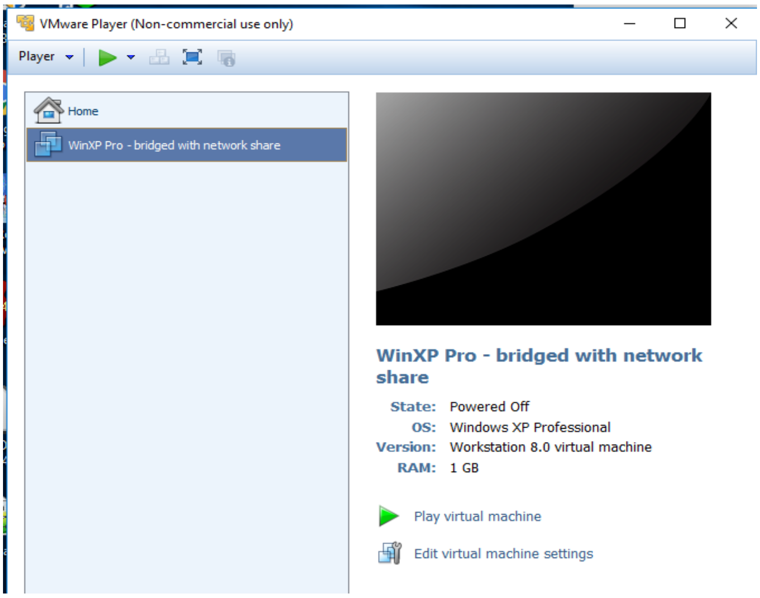


Figure 3: VMPlayer opens a VM

Next you need to add a new hard disk to the virtual machine. Click on “Edit Virtual Machine Settings”. You will see the screen shown in Figure 4:

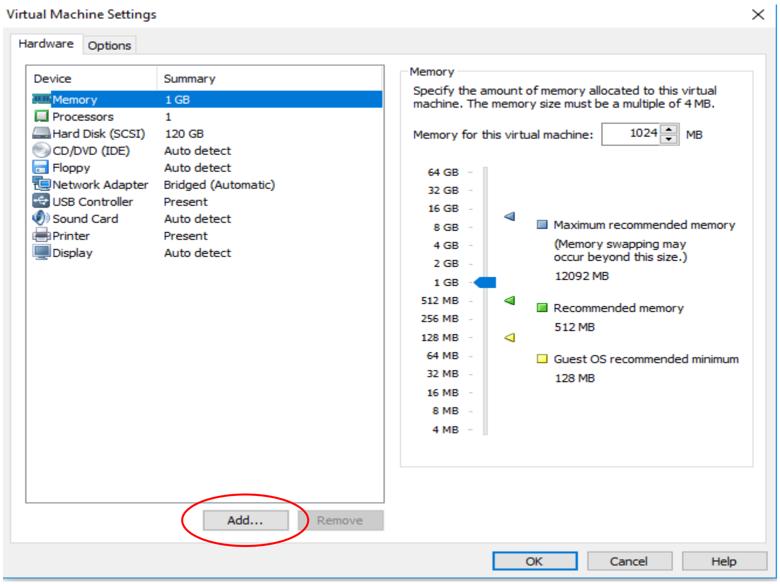


Figure 4: Edit VM settings

Select Add button. Select “Hard Disk” and click Next. Then select “SCSI” and click Next.

On the following window, select “Create a new virtual disk” as shown in Figure 5.

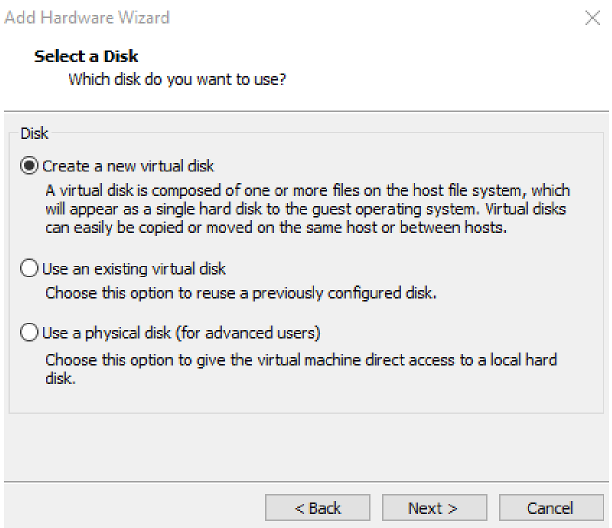


Figure 5: Create a new virtual disk

Set the hard disk to **1.01GB** and to store virtual disk as **a single file**. Click Next then Finish, then OK.

In the VMPlayer main window, click on “Play Virtual Machine”, then choose “Copied it”. Launch the VM and allow the computer to boot.

In this step you are going to create 4 Primary Partitions on your new disk.

Right click on My Computer and select Manage, as shown in Figure 6. Select manage and then click on Disk Management.

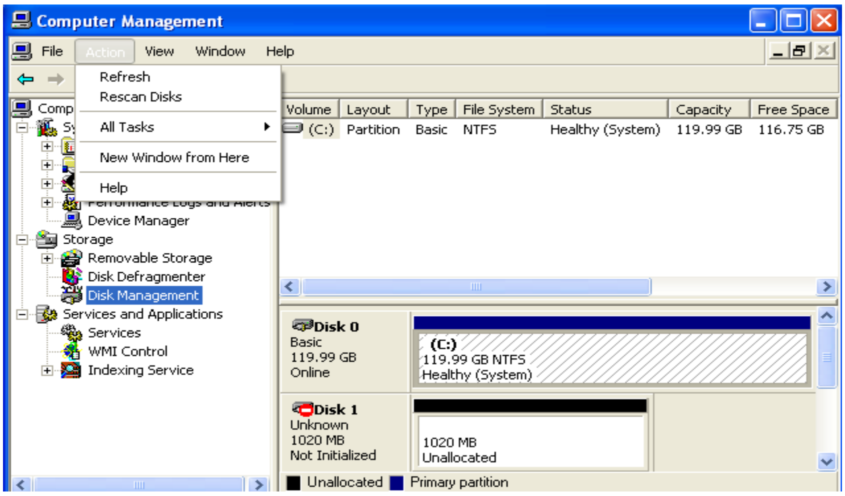


Figure 6: Disk management

Click on **Actions**, then **Rescan disks** to pick up the new disk (if Disk 1 is not picked already).

Right click on Disk1 and initialize disk. Click OK.

Create a Partition

Right click on 1020 Mb Unallocated and choose New partition. click Next.

Choose Primary Partition and click Next. Resize the partition size to 10 MB and click Next.

Assign the drive letter, or select the default drive letter if it is “E”.

Choose the following settings, call the volume label “Part1”, tick Perform Quick format and Click Next, see Figure 7.

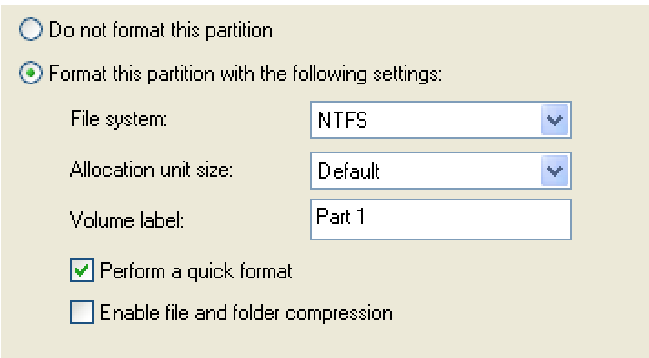


Figure 7: Format partition

Then click Finish.

Repeat the stages to create a partition for another three times to create another three partitions, but change the volume label to **Part 2, Part 3 and Part 4**.

You can replicate section 4.1 of the lab using the Windows (10 or 11) VM that you installed in lab 2. In Windows 10, you need to select MBR instead of GPT for the 1.01GB disk and partition creation is called 'New Simple Volume'.

Lab 4.2: Examine and Repair MBR

In the simplest view, partitions on hard disks are defined by their Master Boot Record (MBR). Identify the following:

- What is MBR for?
- What sector is it located at?
- How many primary partitions can it define?
- What are the last 2 bytes?

Download Hiren's Boot CD, which performs some repairs to the MBR, from the resources folder and unzip it. Create a new folder and name it 'Hiren'. Copy and paste all the files and folders from unzipped Hiren to it, so that you can access the .iso file (see figure below).

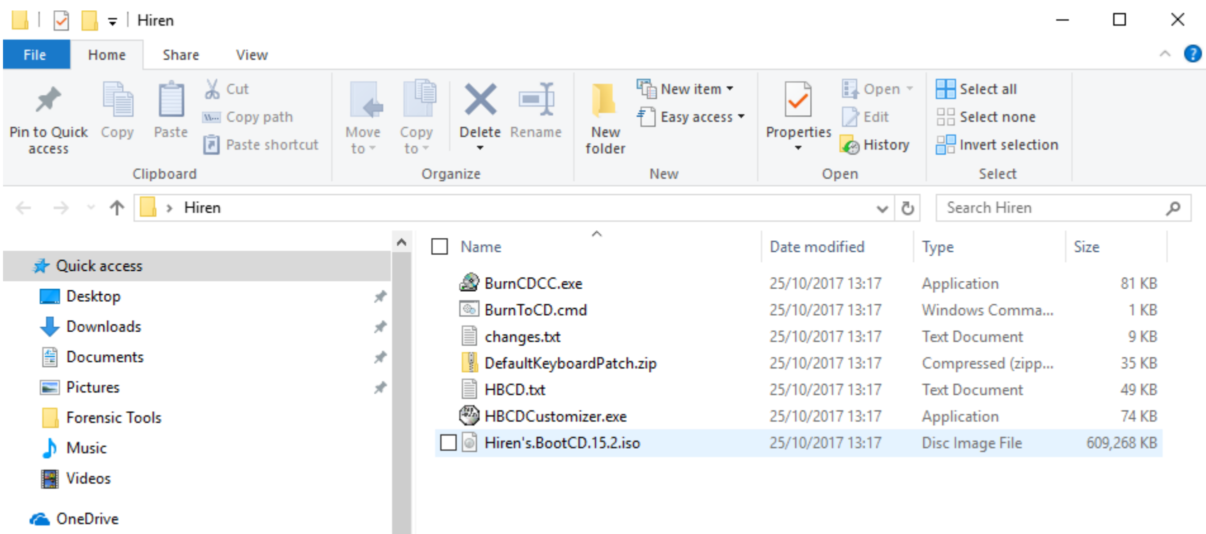


Figure 8: Unzipped Hiren

You can view the MBR of your disk using Roadkil's SectEdit, or another sector editor. On your VM:

- Use the Sectedit.zip version from the lab resources folder OR
- Download sectedit from (https://www.roadkil.net/program.php?ProgramID=24)

Extract to C:\SectEdit.

Right hand-click on the application and "run as administrator".

Launch the application and untick "Protect my computer…" and click Ok as shown in Figure 9:

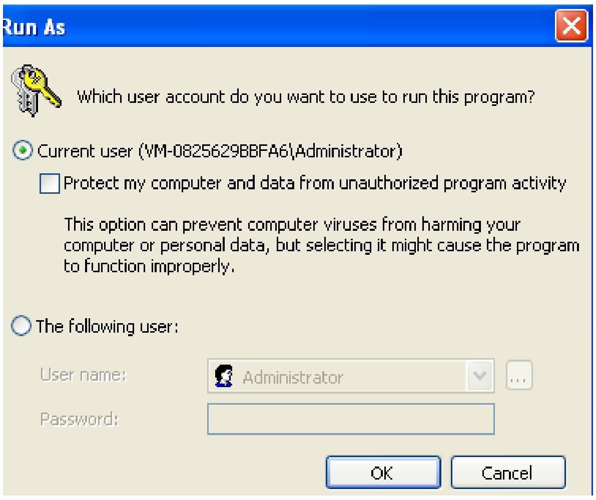


Figure 9: Sectedit launch window

You will be given an option of what it should open, either logical volumes (partitions) or a physical disc.   Select **physical 1**.

Automatically you are taken to the first sector of the drive, which is in fact the MBR.

How many times does the sequence of values 55 AA occur in the MBR?

The end of the MBR is always the HEX value "55AA" (at address $1FE_{HEX} = 510_{10}$). Immediately **prior to** the final "55 AA" there are 64 bytes which define the four primary partitions on a hard disk. Because only 64 bytes are available and each partition requires 16 bytes for its definition, there can be only four primary partitions. Other "logical volumes" (sometimes called "logical" or "extended" partitions) are possible but these are NOT primary partitions and an operating system cannot be booted from these. The logical volumes exist within pre-defined primary partitions. Both primary partitions and logical volumes are usually identified by a single letter such as C:.

You will essentially be looking at something similar to this screenshot in Figure 10. The coloured areas denote the 4 Primary Partition records (but note that you should see data in the entry for all 4 partitions):

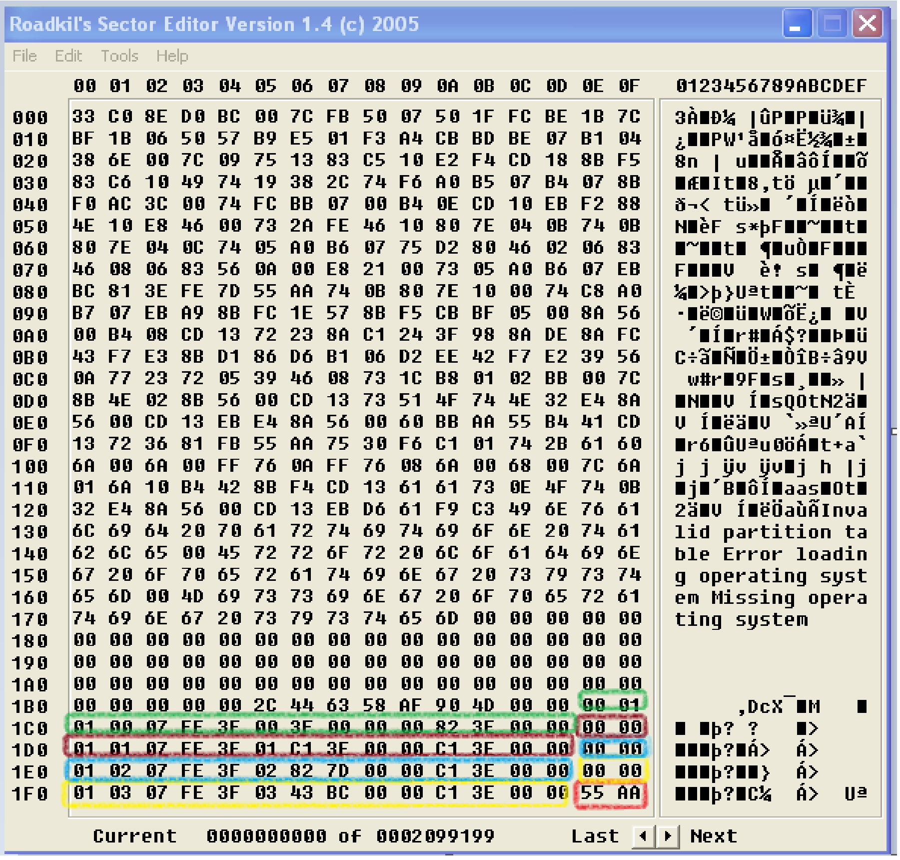


Figure 10: MBR and partitions

“55AA” is the end of MBR shown with Red. Go back 64 bytes from the 55 AA at the end of the MBR, this is the start of the partition record. Each partition (with the size of 16 bytes) is colour coded. Green is partition part 1, Brown is Partition part 2, Blue is Partition Part 3 and Yellow is Partition Part 4. Each partition (with the size of 16 bytes) which can be decoded using the following table:

Relative Offsets (within entry)- byte number for each partition	Length (bytes)	Contents
0	1	Boot Indicator (80h = active)
1 - 3	3	Starting CHS values
4	1	Partition-type Descriptor
5 - 7	3	Ending CHS values
8 - 11	4	Starting Sector read this from right to left as it is stored in little endian
12 - 15	4	Partition Size (in sectors) read this from right to left as it is stored in little endian

Let’s Look at Part2 Partition, which is in brown more closely: Here is the data, remember: the data is in hex and in little Endian format. You need to read them in reverse order (from right to left) and then you need to decode Hex to decimal (you can use a calculator for this).

00 00 01 01 07 FE 3F 01 C1 3E 00 00 C1 3E 00 00

What is the size of the partition?

Do the sizes correspond with what you can see in My Computer?

Byte number	Byte Data	
0	00	Boot Indicator, the value is 00, so it is not an active bootable partition

1-3	000101	Starting CHS values
4	07	Partition types (look at this link: https://thestarman.pcministry.com/asm/mbr/PartTypes.htm). 07 is defined as NTFS
5-7	FE3F01	Ending CHS values
8-11	C1 3E 00 00	Starting Sector: read this from right to left as it is stored in little endian: 00003EC1, then change the hex to decimal using your calculator: 16065 decimal
12-15	C1 3E 00 00	Partition Size (in sectors) read this from right to left as it is stored in little endian: 00003EC1: then change the hex to decimal using a calculator: 16065 decimal. Each sector has 512 bytes, need to multiply the number by 512. 16065x512 = 8,255,280 bytes. If you want it in KByte, it should be divided by 1024: 8,255,280 /1024 = 8,032 Kbytes. If you want the size in Mbyte, further divide the value by 1024: 8,032/1024 =7.84 ~ 8MB

Modify MBR

Within the VM, in SecEdit click on Files and choose “Select Disk”. Choose physical disc 0, Now edit the very last bytes to be read as “AA 55” instead of “55 AA” and select File->Save Sector.

Now restart the VM and you will find it no longer boots. Close the VM.

Launch VMPlayer and select “WinXP Pro - Chrome” click on “Edit Virtual Machine settings”.

Attach the Hiren’s Boot CD ISO to your VM as a CD - you will need to modify your VM settings, as shown in Figure 11:

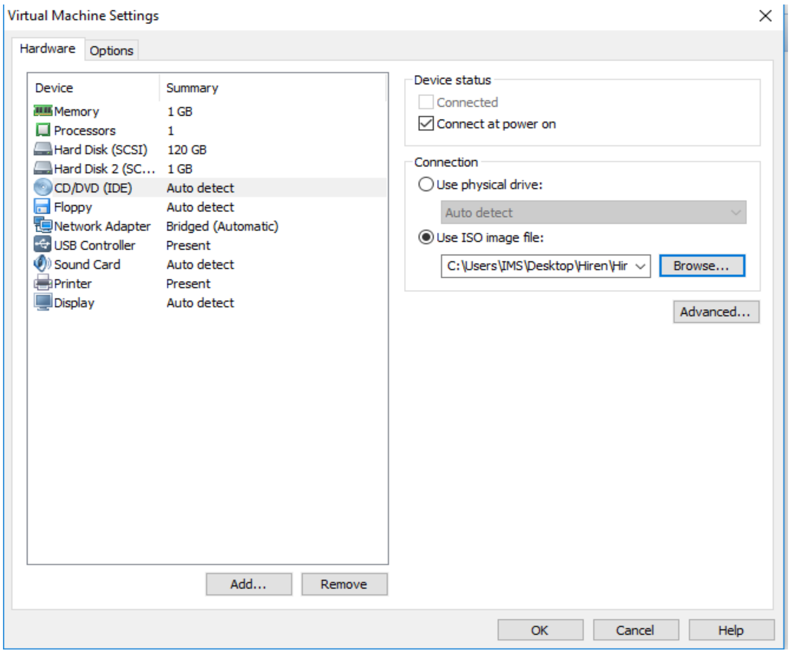


Figure 11: VM settings

Restart the VM.

You will be presented with Hiren's Boot CD menu, using arrow key on the keyboard select **Mini Windows XP.**

Once booted click on the Hiren's quick launcher in the bottom right corner and select MBRFix following the menu as shown in Figure 12.

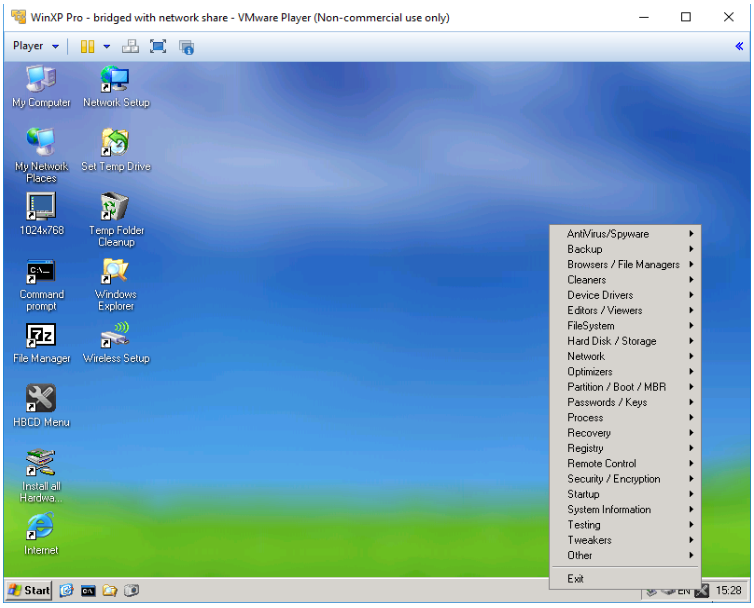


Figure 12: Hiren's quick launcher

Then choose Partition/Boot/ MBR > Command Line > MBRFix. This will launch a command prompt and a help text file. Review the text document to see what the tool does, and then launch the command:

MbrFix.exe /drive 0 driveinfo

Then type:

Mbrfix /drive

This will display the drive information about physical drive 0 - our main disk.

Type "y"

Then run:

Mbrfix /drive 0 fixmbr

And press y - you are sure

Restart the VM and you will find you can boot straight into Windows.

Still in the VM, launch sectedit and review physical disc 0 –

Is the footer (the MBR signature) fixed? Record in your logbook.

End of Lab Sheet