

?:OSSLab thx

??EPS ?? ?Windows 2000 ,2003 Sever , XP ,7 ,Vista ??? (????? ,2008??)

Windows ?????????????? SAM HKEY_LOCAL_MACHINE\SAM ??????????
????Ntfs ?????os ??,?? Offline nt ??windows sam????
?????AD? ,????.

????????????????SAM ???????????????.

?????? ????? VHD image file +??? ??????????

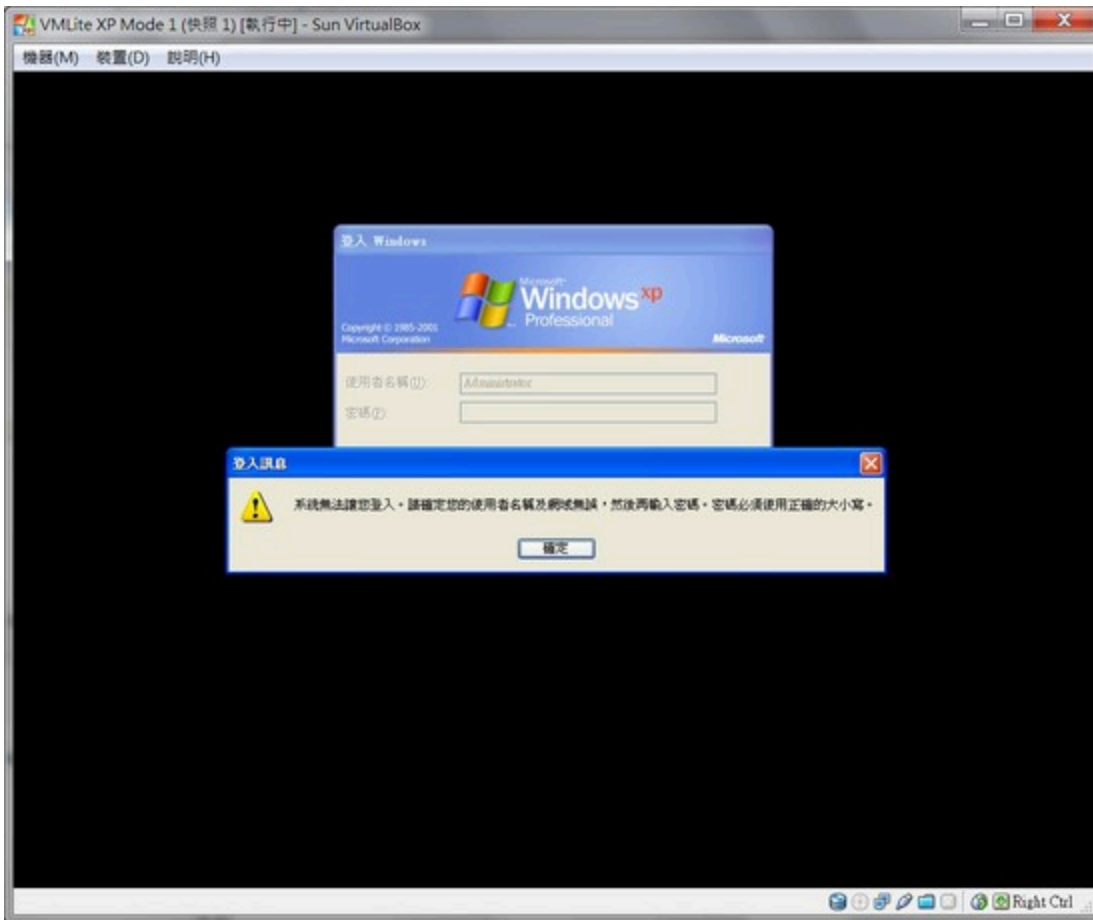
????.

- 1.<http://ophcrack.sourceforge.net/>
- 2.<http://jay-fva.blogspot.com/2009/12/...nistrator.html>

?:
??? [ultimate CD ISO 5.0rc 1](#) ?

?????? ?? XP mode ??,??? VHD file ,

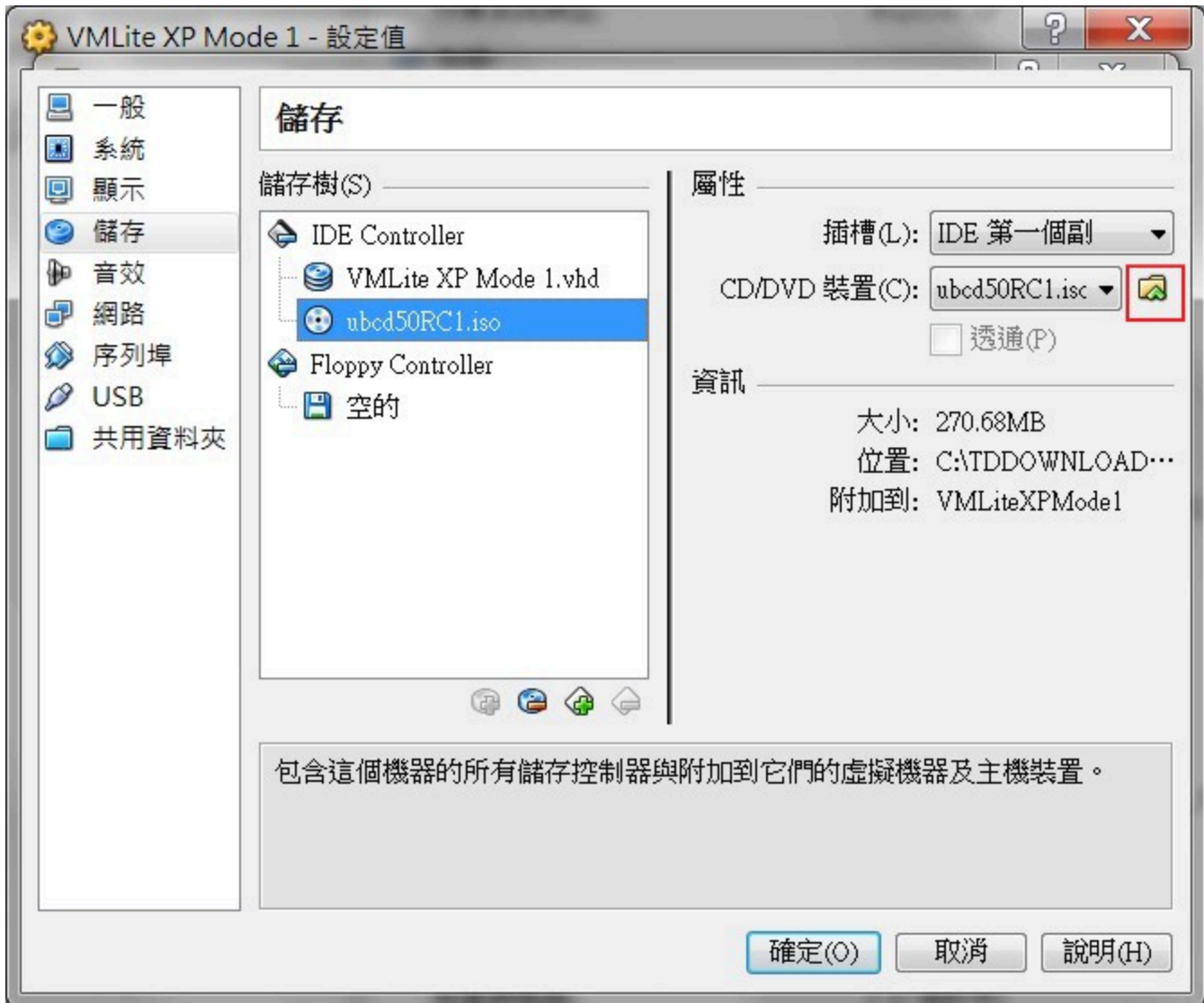
??? XP VM VHD in Virtualbox
??XP mode ?VM ??administrator ????????



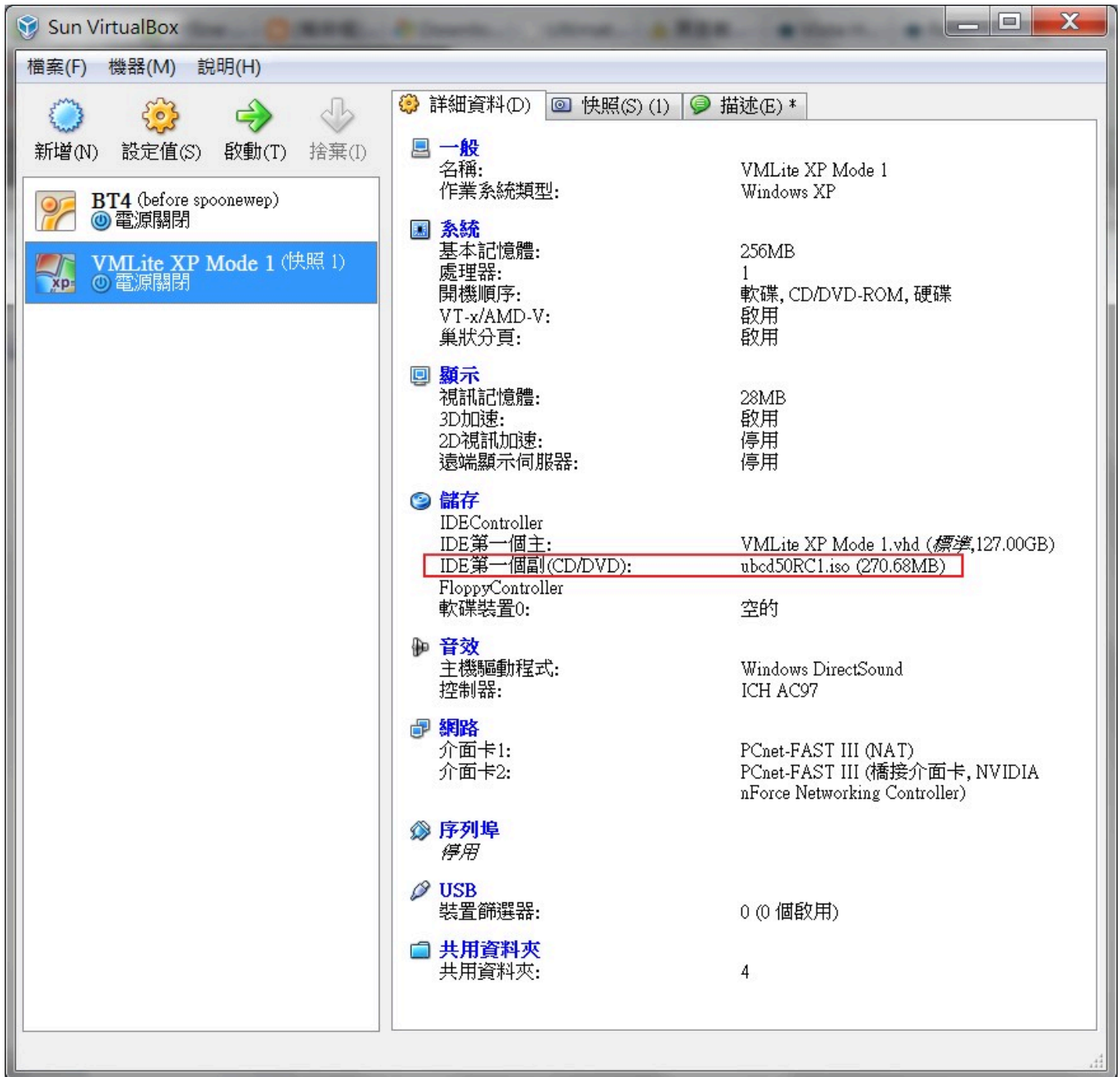
????????

?virtualbox?????? ?????

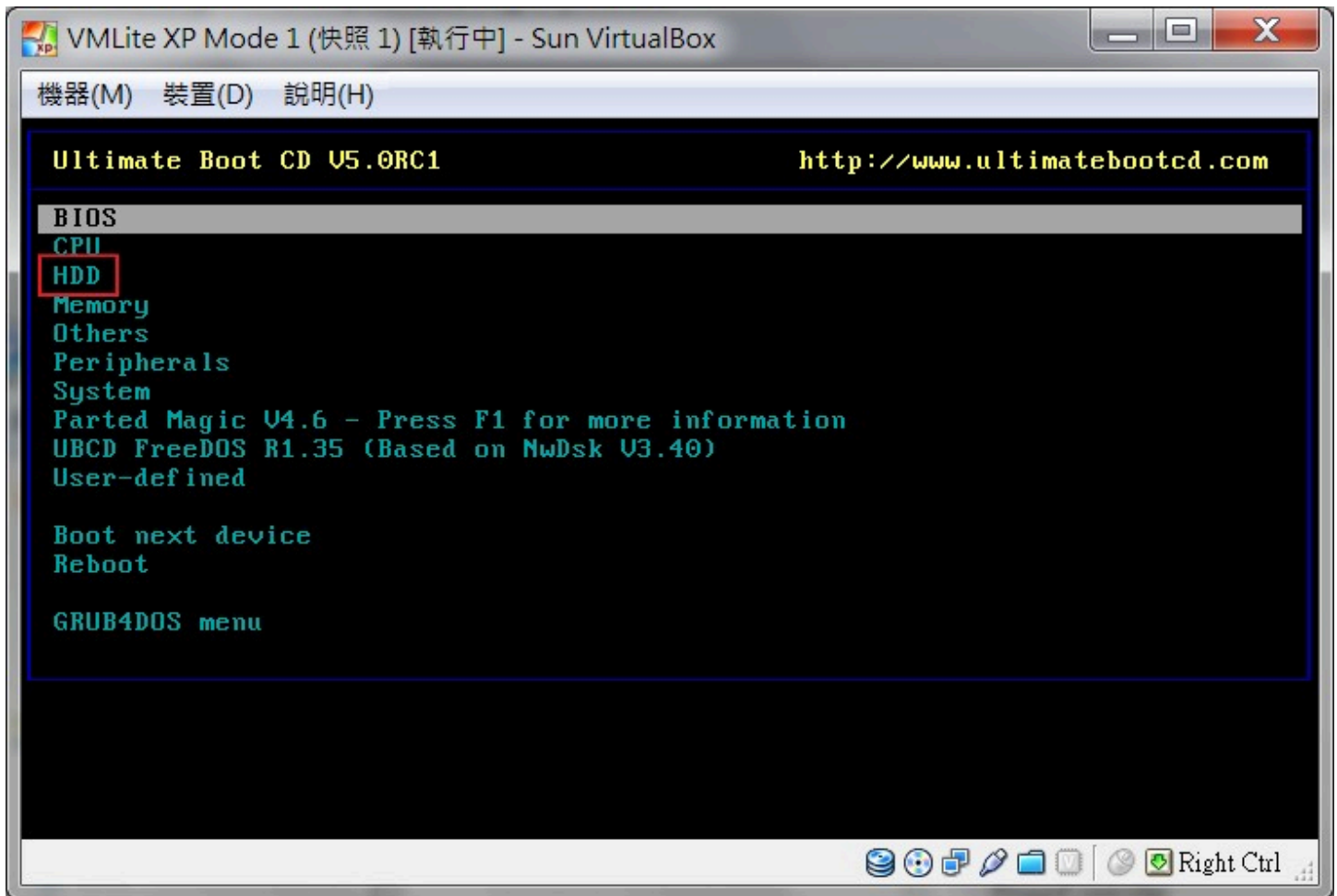
1.???????? ubcd5rc1?iso?.



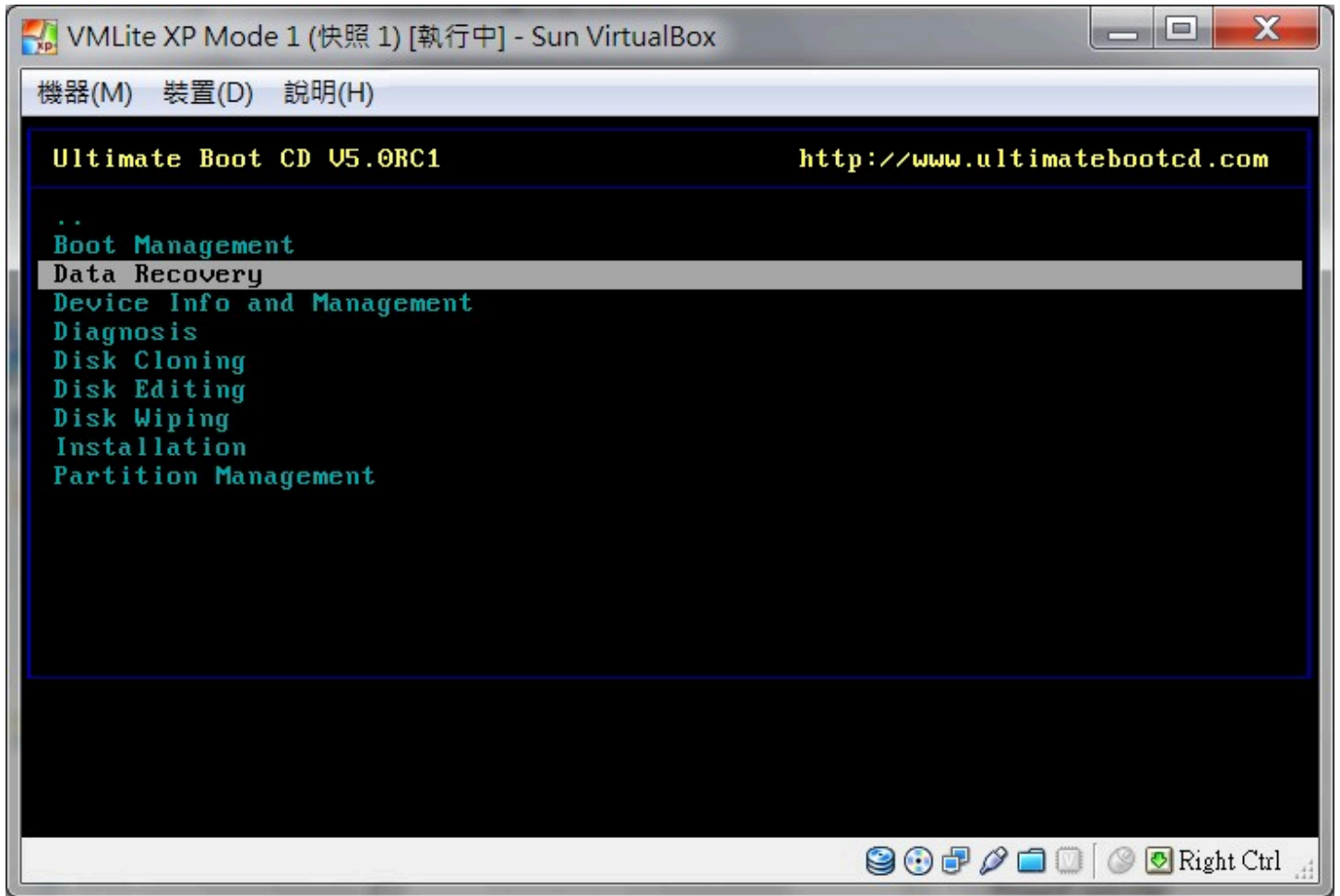
????????iso????



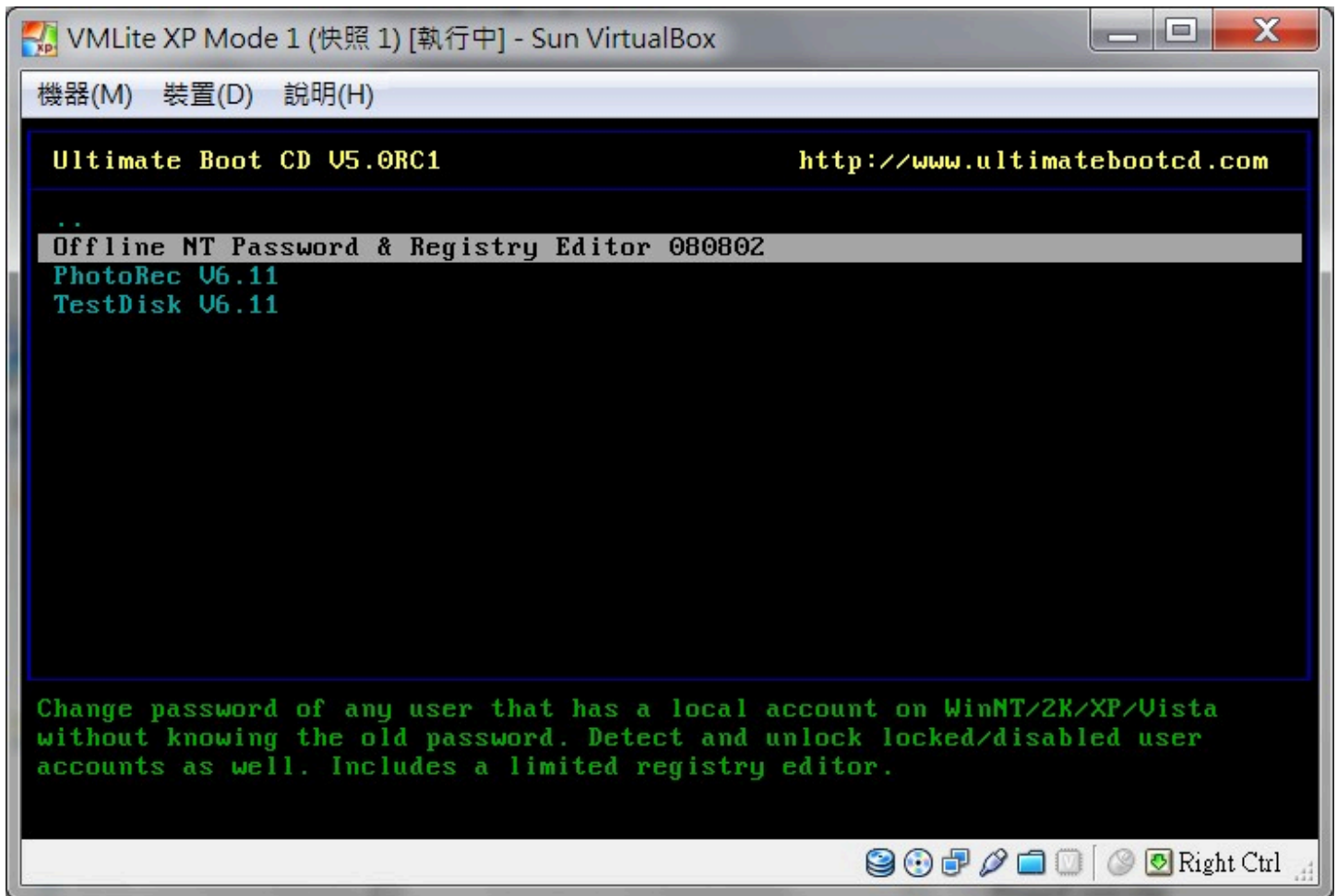
????ISO????????????????iso????????????????F12???



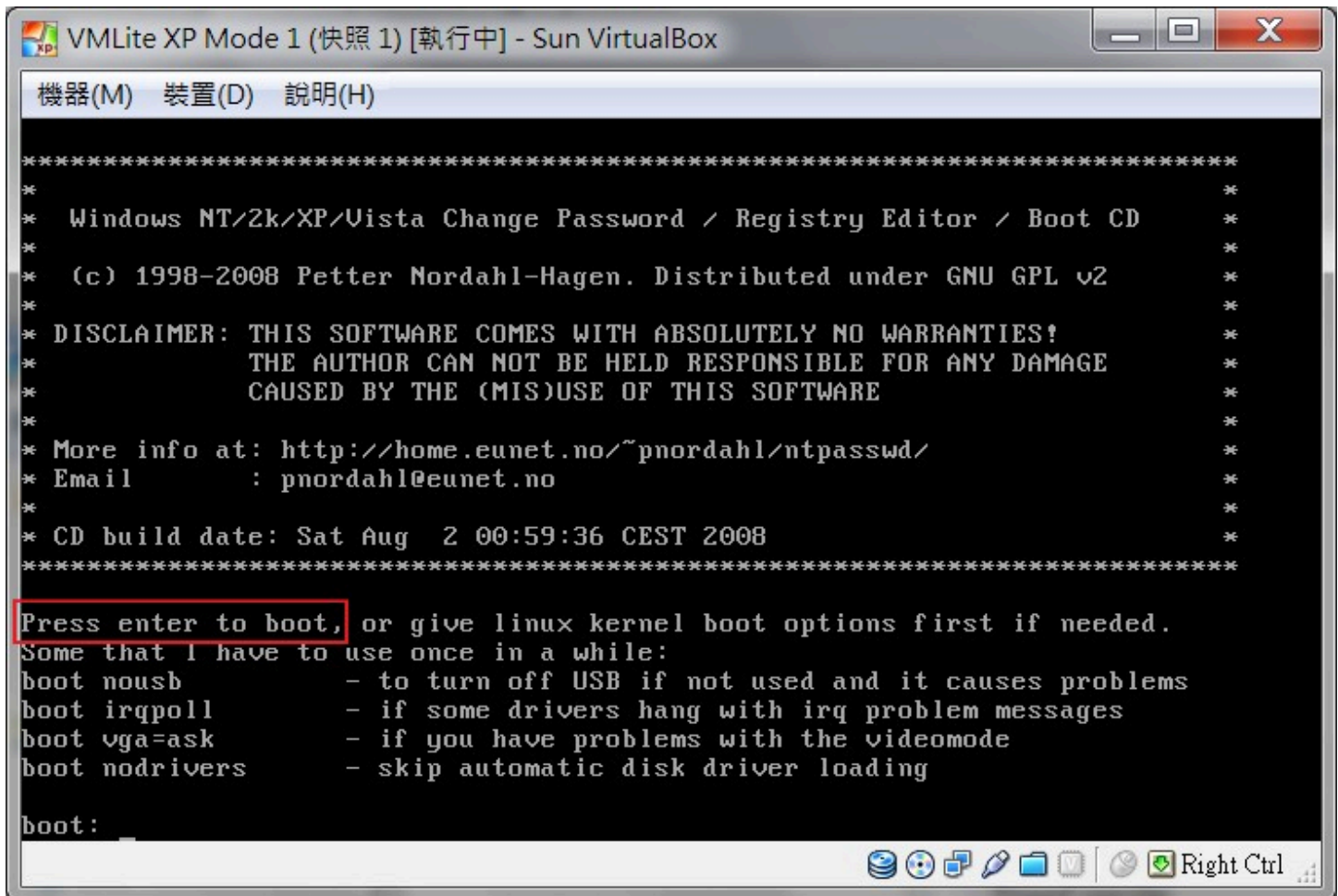
?????????ubcd?????HDD?



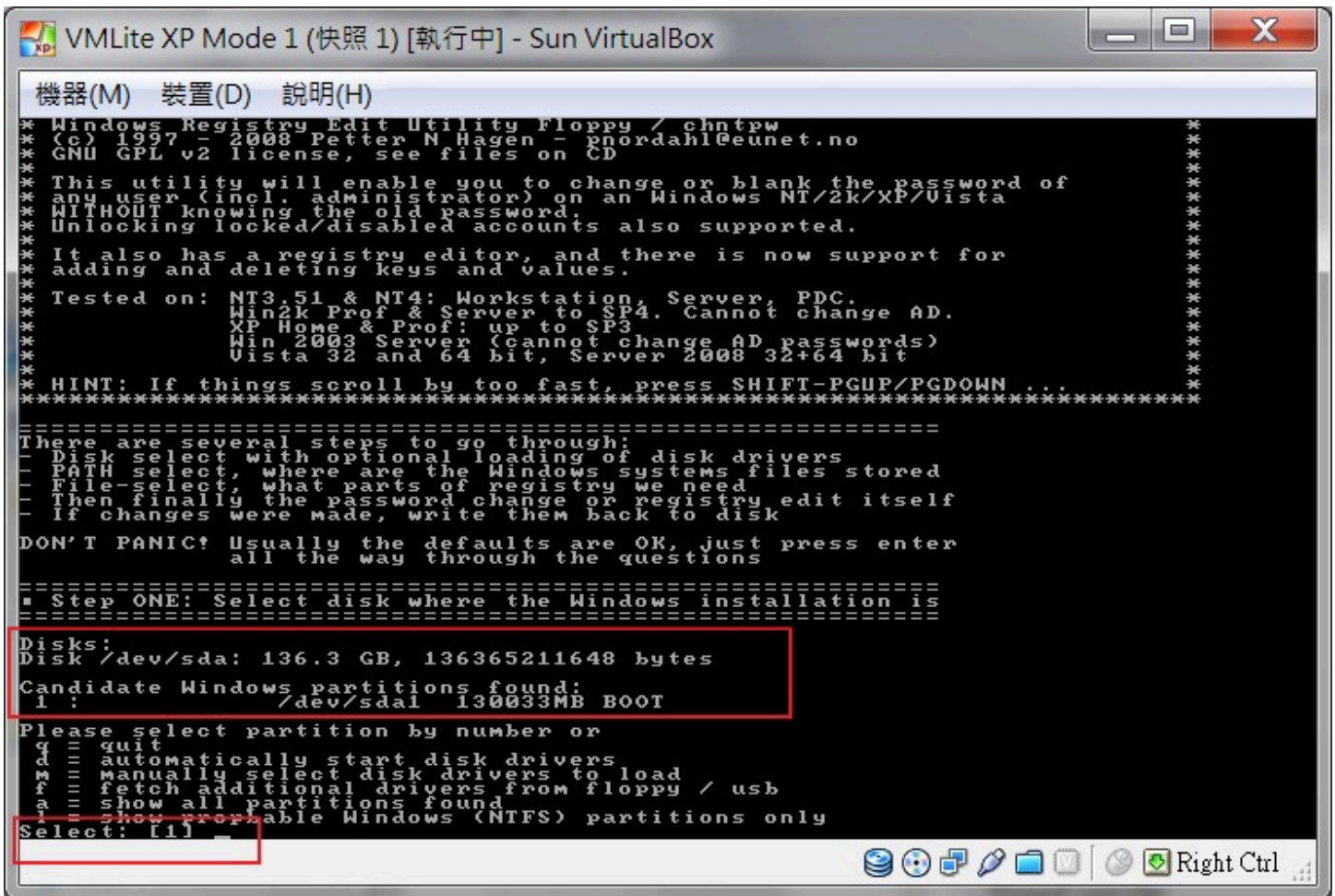
??data recovery?



??Offline NT Password & Registry Editor?

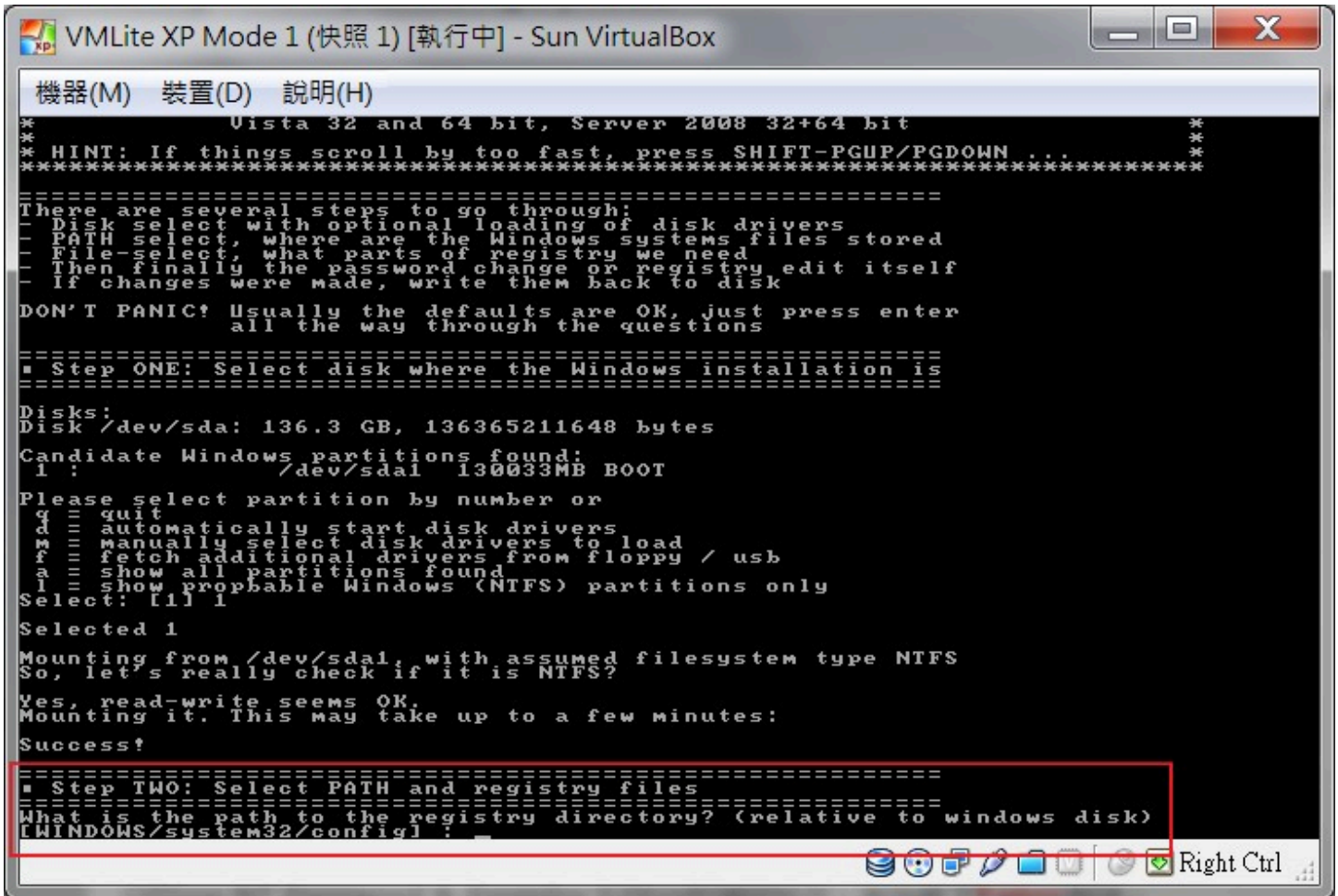


??Offline NT Password & Registry Editor???enter to boot ??????



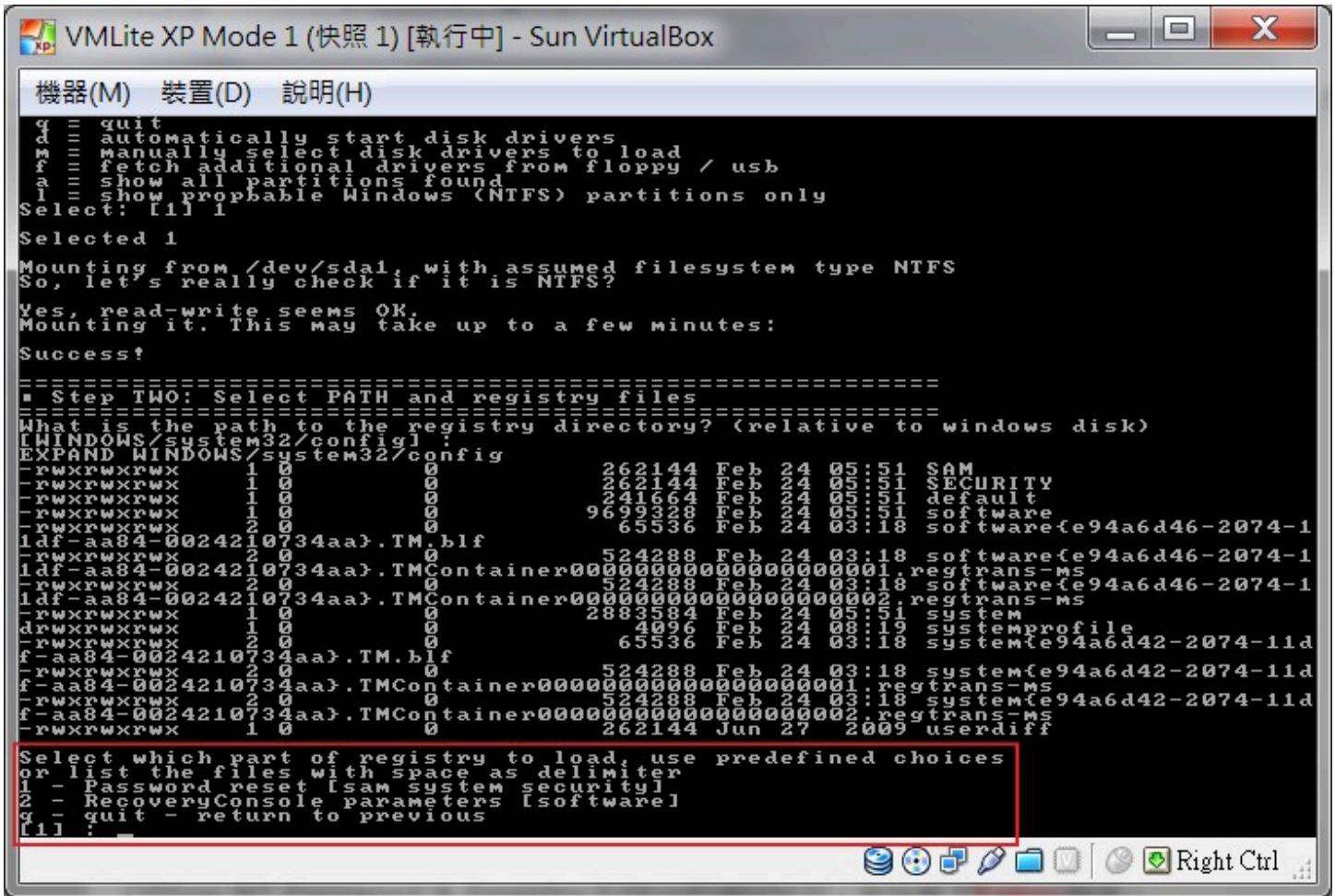
??XP?????:

????1?????????"1"?? "??1"



??XP?????:

??registry????????????\windows\system32\config???enter?????



????????1?????

```

VMLite XP Mode 1 (快照 1) [執行中] - Sun VirtualBox
=====
or list the files with space as delimiter
1 - Password reset [sam system security]
2 - RecoveryConsole parameters [software]
q - quit - return to previous
[1] : 1
Selected files: sam system security
Copying sam system security to /tmp
=====
Step THREE: Password or registry edit
=====
chntpw version 0.99.6 080526 (sixtyfour), (c) Petter N Hagen
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
Page at 0x6000 is not 'hbin', assuming file contains garbage at end
File size 262144 [40000] bytes, containing 5 pages (+ 1 headerpage)
Used for data: 230/16568 blocks/bytes, unused: 9/3752 blocks/bytes.

Hive <system> name (from header): <SYSTEM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
Page at 0x2a2000 is not 'hbin', assuming file contains garbage at end
File size 2883584 [2c0000] bytes, containing 648 pages (+ 1 headerpage)
Used for data: 50667/2715328 blocks/bytes, unused: 1120/20544 blocks/bytes.

Hive <SECURITY> name (from header): <emRoot\System32\Config\SECURITY>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
Page at 0xa000 is not 'hbin', assuming file contains garbage at end
File size 262144 [40000] bytes, containing 9 pages (+ 1 headerpage)
Used for data: 795/35104 blocks/bytes, unused: 5/1472 blocks/bytes.

* SAM policy limits:
Failed logins before lockout is: 0
Minimum password length      : 0
Password history count       : 0

<>=====<> chntpw Main Interactive Menu <>=====<>
Loaded hives: <SAM> <system> <SECURITY>

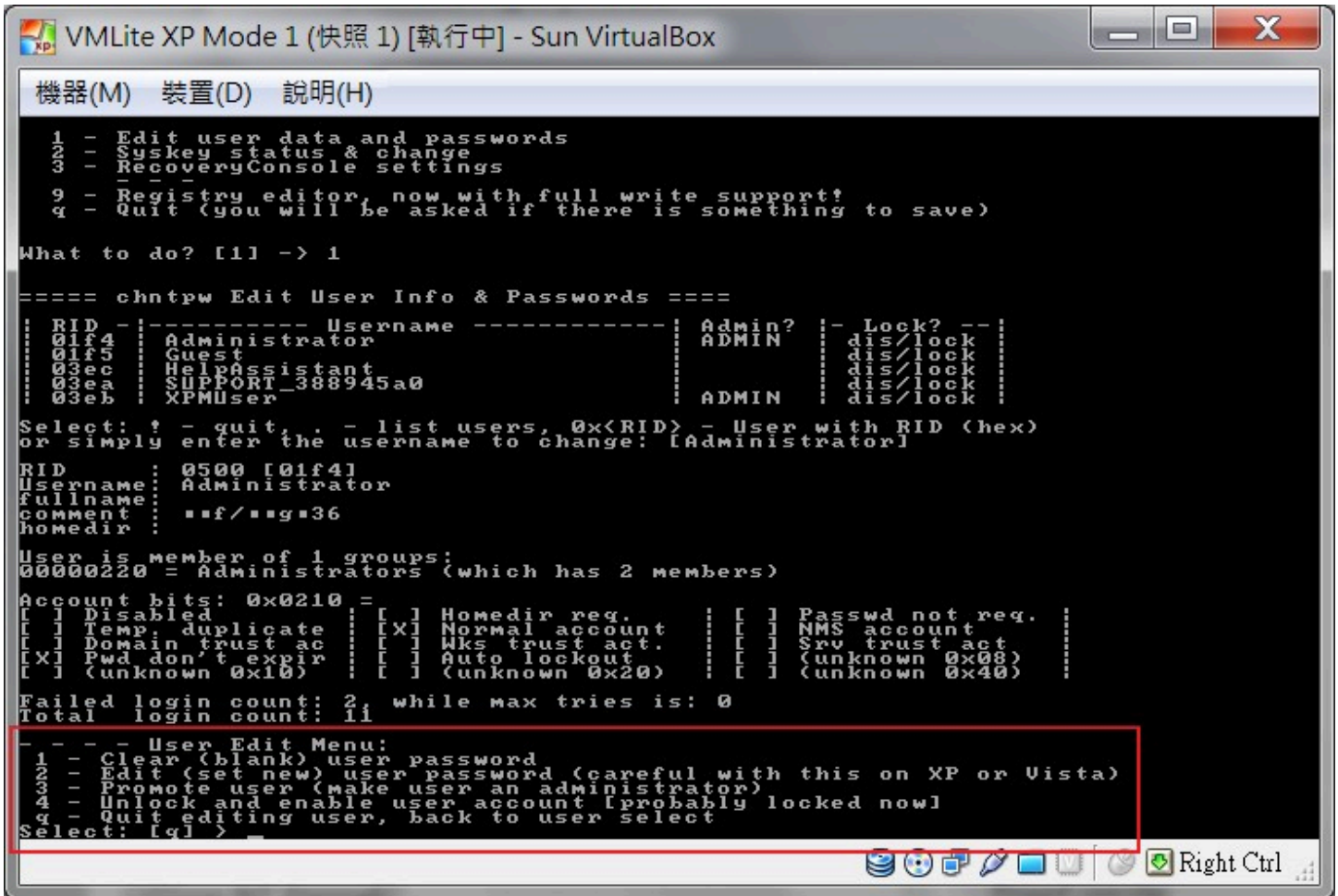
1 - Edit user data and passwords
2 - Syskey status & change
3 - RecoveryConsole settings
_ _ _
9 - Registry editor, now with full write support!
q - Quit (you will be asked if there is something to save)

What to do? [1] ->

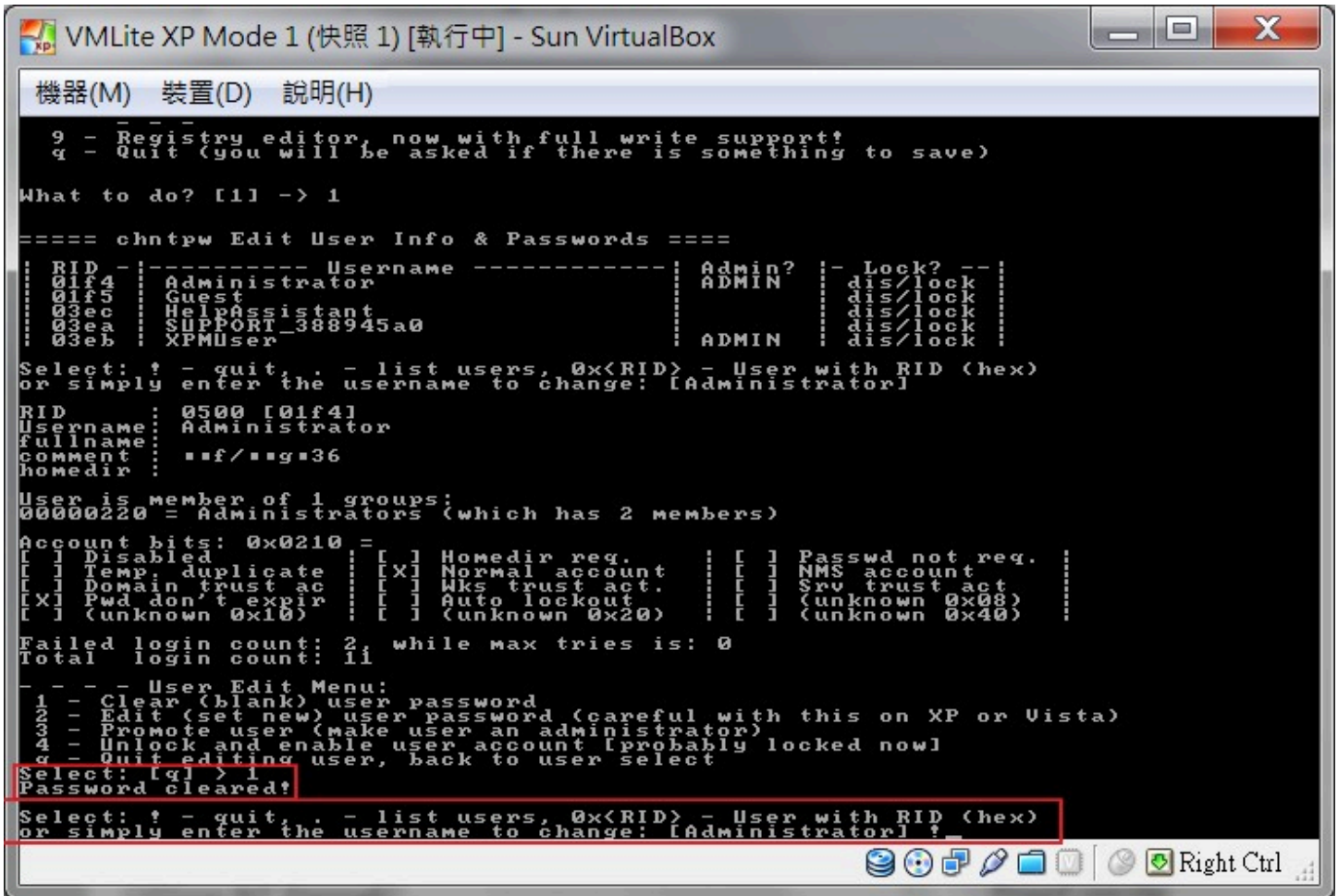
```

??XP?????:

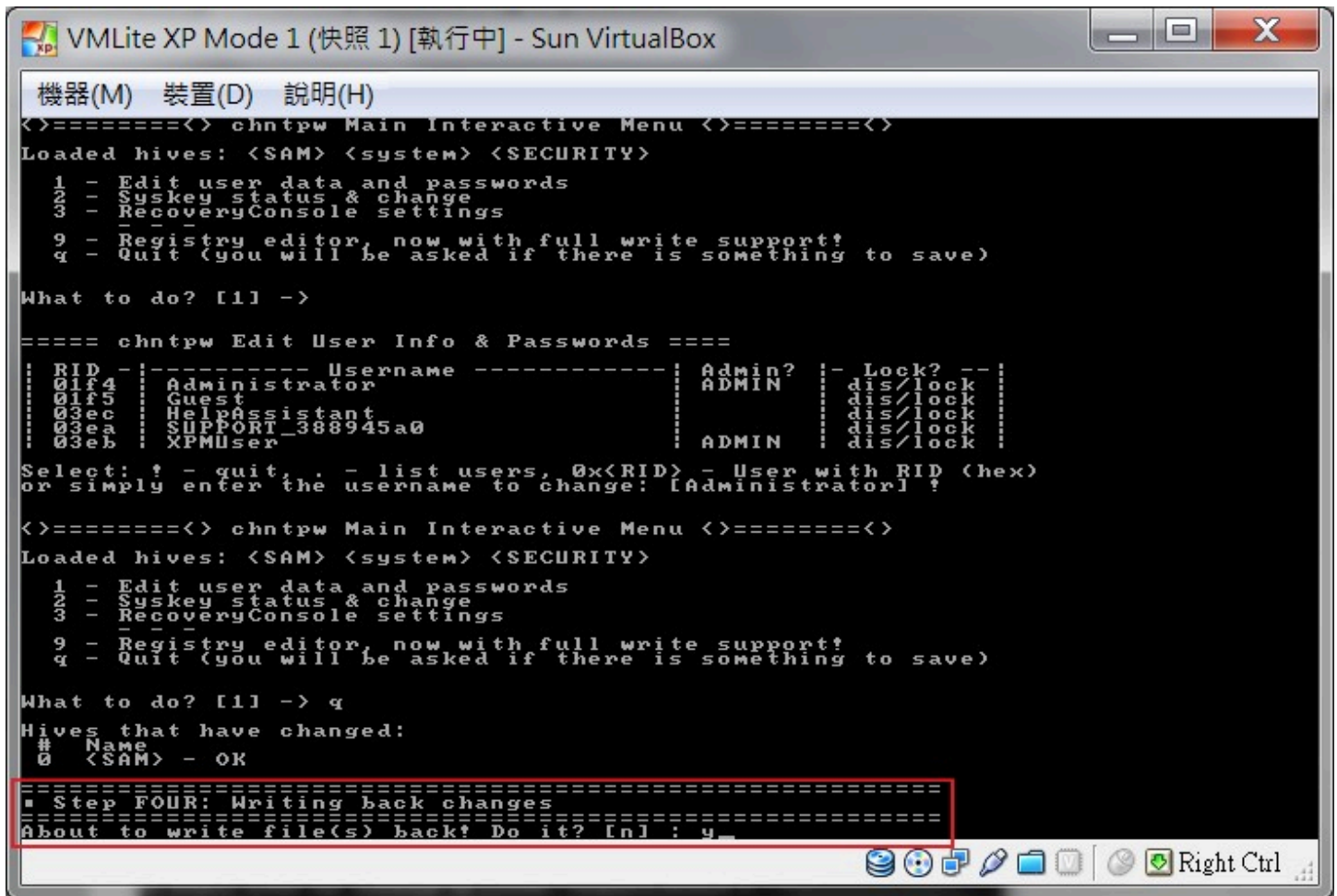
????????1?????



????1????(????????)?

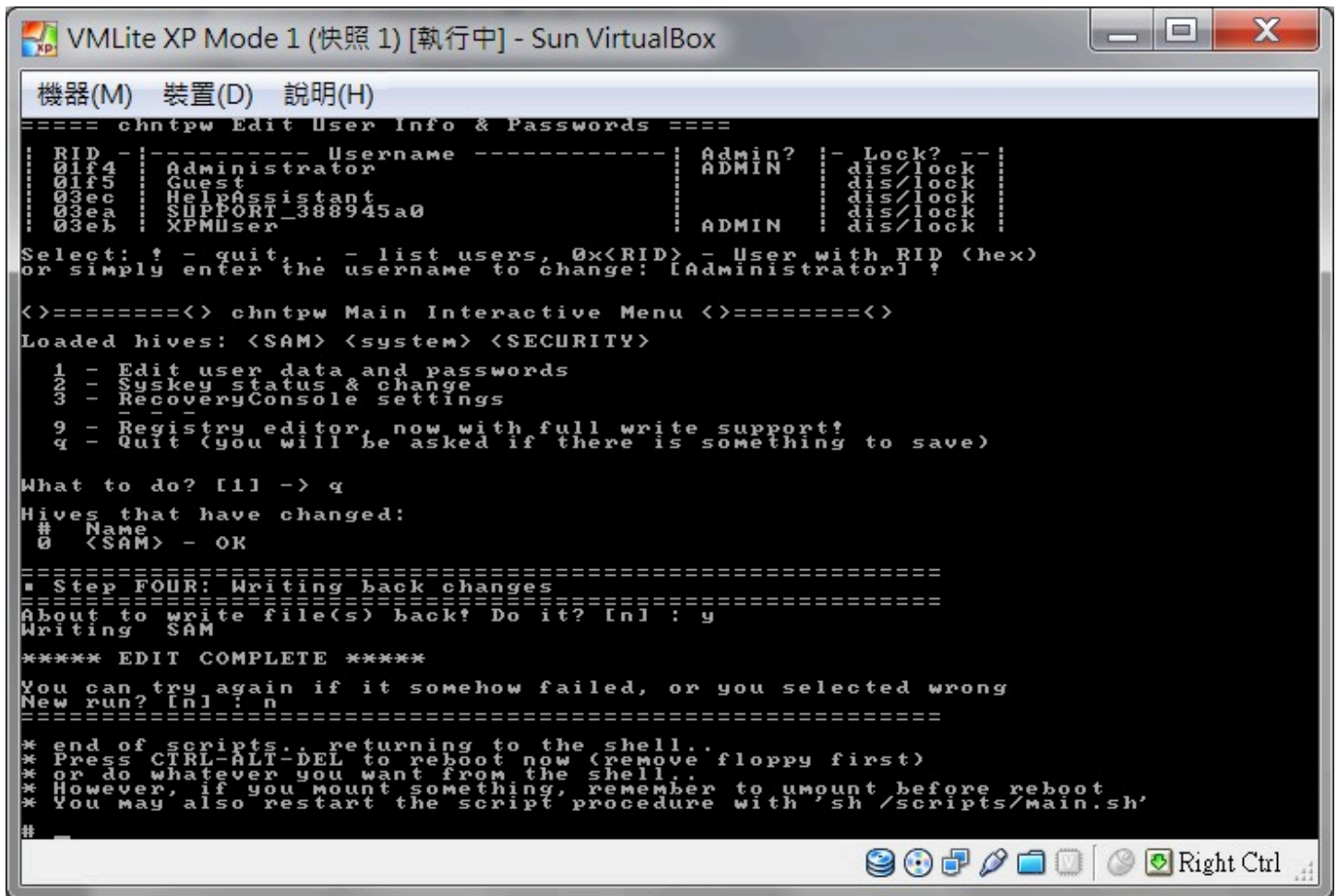


????????????Offline NT Password & Registry Editor?????username????administrator????enter?????????



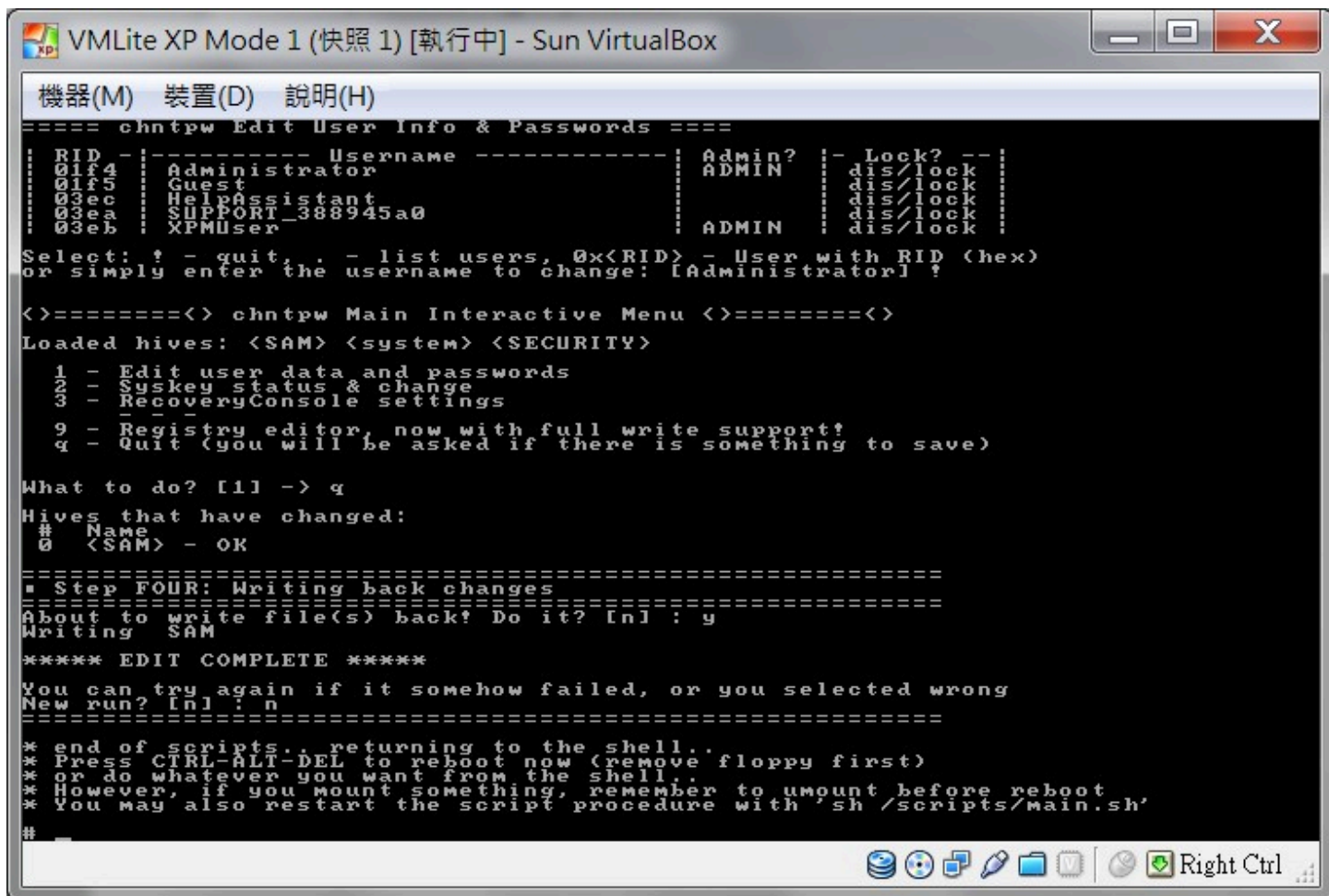
??XP?????:

offline?????????????"Y"???



EDIT COMPLETE!

??n???Enter???Offline NT Password & Registry Editor?



???????virtual machine??????

??? ??F12 ? IDE Primary ??

Administrator????,??????

???Raid card ?????Driver.????Win PE CD

??NT offline ??SAM password?? ???????