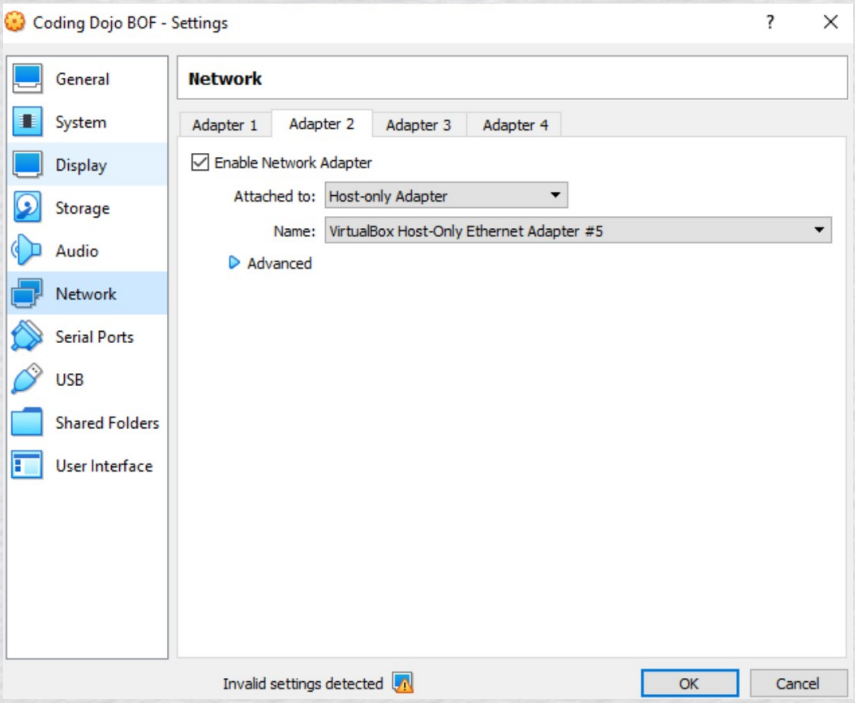
Name : Ahmed Alzahrani **|| Email** : You-187@hotmail.com

Malware Analysis

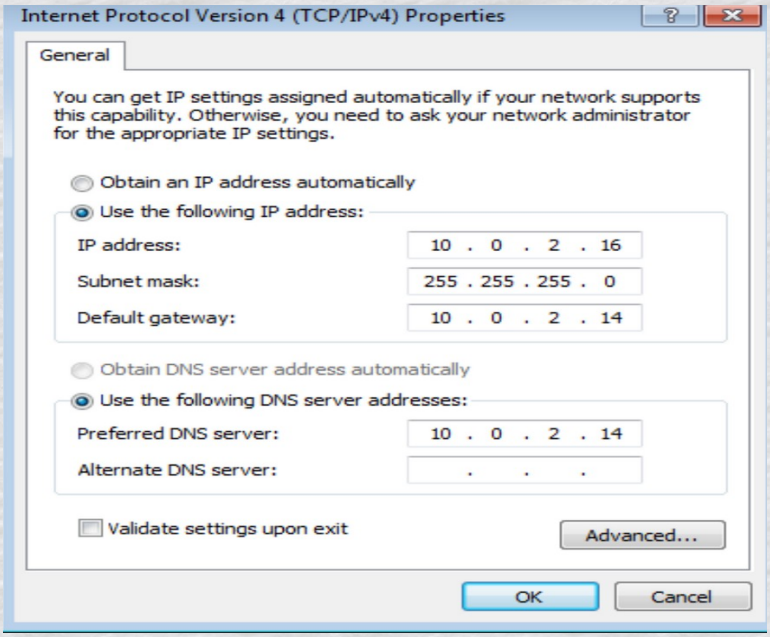
1. Put Windows VM in Host Only mode



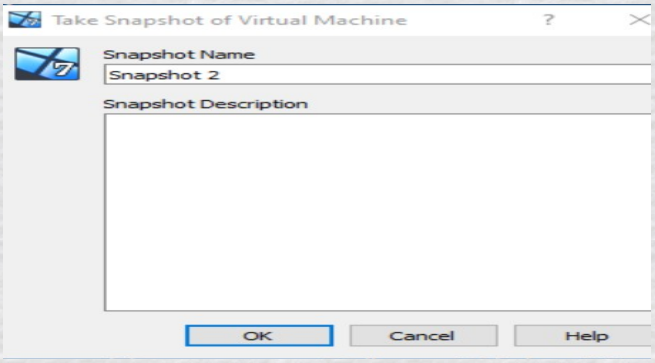
2. Start up your REMNUX VM and take note of the IP address

```
remnux@remnux:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.14  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe7c:a70b  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:7c:a7:0b  txqueuelen 1000  (Ethernet)
        RX packets 4  bytes 1300 (1.3 KB)
```

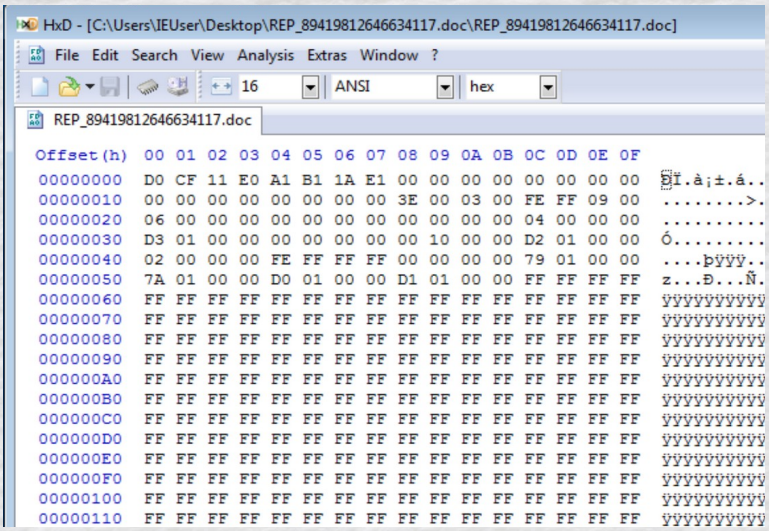
3. Go back to your Windows VM and manually configure the default gateway to be the IP of REMNUX



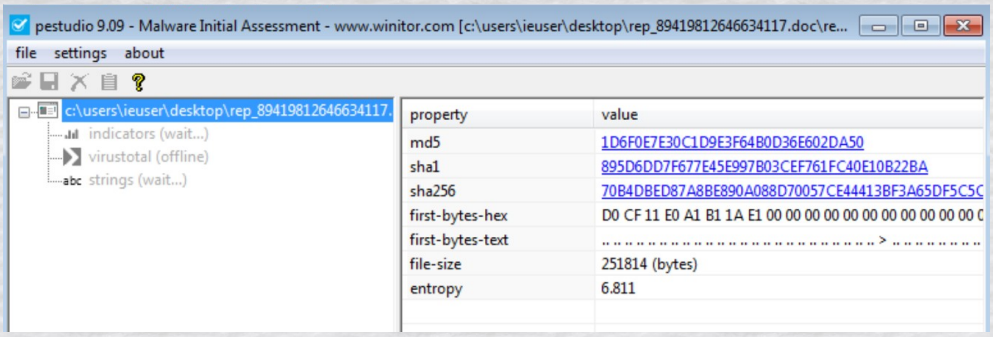
4. Take a snapshot of your Windows VM now



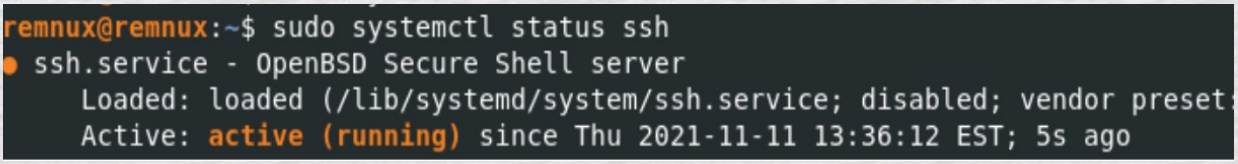
5. Drag and drop the malware file to the hxd icon on the desktop and take a quick look at the first 4 bytes. It should look like it spells something, sort of...



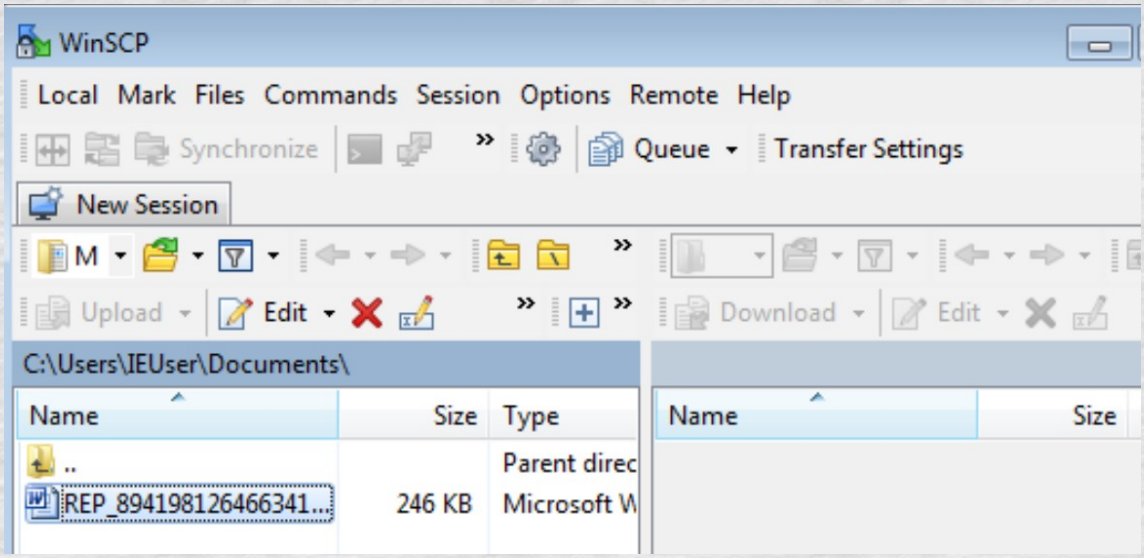
6. Open the malware in pestudio and get the hash, indicators adn strings.



Open REMNUX now. Make sure ssh is running on remnux.



On Windows open WinSCP and choose SCP. Choose IP of REMNUX for host name, username
remnux, password is malware. Select word doc on desktop and drag across and close WinSCP.



```
FILE: REP_89419812646634117.doc
Type: OLE
-------------------------------------------------------------------------------
VBA MACRO Frjpossu.cls
in file: REP_89419812646634117.doc - OLE stream: 'Macros/VBA/Frjpossu'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Private Sub Document_open()
Lvpcgwokshh
End Sub
-------------------------------------------------------------------------------
VBA MACRO Xhrcwkmbidam.frm
in file: REP_89419812646634117.doc - OLE stream: 'Macros/VBA/Xhrcwkmbidam'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(empty macro)
-------------------------------------------------------------------------------
VBA MACRO Yokxdhzeadumj.bas
in file: REP_89419812646634117.doc - OLE stream: 'Macros/VBA/Yokxdhzeadumj'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Function Teupaekd()
   Do While Fgqqpushblnf = 900
            Do While Kdrfvbettmaj = 3 + 2
            Miibxfajx = Chr(4)
```

Now it's time to start running the macro!

502	HTTP	www.microsoft.com	/pkiops/crl/MicCodSigPCA...	512	no-cac...
502	HTTP	amelano.net	/wp-includes/css/dist/2ew/	512	no-cac...
502	HTTP	911concept.com	/images/i6ngX5/	512	no-cac...
502	HTTP	ayonschools.com	/U8kogn/	512	no-cac...
502	HTTP	beech.org	/wayne/lido/	512	no-cac...
502	HTTP	firelabo.com	/wp-includes/mf6f4/	512	no-cac...

Explorer.EXE	2368	RegOpenKey	HKLM\Software\Microsoft\Windows\S...	NAME NOT FOUND
Explorer.EXE	2368	RegOpenKey	HKCU\Software\Microsoft\Windows\S...	NAME NOT FOUND
Explorer.EXE	2368	RegQueryKey	HKCU\Software\Classes	SUCCESS
Explorer.EXE	2368	RegOpenKey	HKCU\Software\Classes\Directory	SUCCESS
Explorer.EXE	2368	RegQueryKey	HKCU\Software\Classes\Directory	SUCCESS
Explorer.EXE	2368	RegOpenKey	HKCU\Software\Classes\Directory\Cur...	NAME NOT FOUND
Explorer.EXE	2368	RegOpenKey	HKCR\Directory\CurVer	NAME NOT FOUND
Explorer.EXE	2368	RegQueryKey	HKCU\Software\Classes\Directory	SUCCESS
Explorer.EXE	2368	RegQueryKey	HKCU\Software\Classes\Directory	SUCCESS
Explorer.EXE	2368	RegCloseKey	HKCU\Software\Classes\Directory	SUCCESS
Explorer.EXE	2368	RegQueryKey	HKCU\Software\Classes\Directory	SUCCESS
Explorer.EXE	2368	RegOpenKey	HKCU\Software\Classes\Directory	SUCCESS
Explorer.EXE	2368	RegCloseKey	HKCU\Software\Classes\Directory	SUCCESS
Explorer.EXE	2368	RegQueryKey	HKCU\Software\Classes\Directory	SUCCESS
Explorer.EXE	2368	RegOpenKey	HKCU\Software\Classes\Directory\Shel...	NAME NOT FOUND
Explorer.EXE	2368	RegOpenKey	HKCR\Directory\ShellEx\IconHandler	NAME NOT FOUND
Explorer.EXE	2368	RegQueryKey	HKCU\Software\Classes	SUCCESS
Explorer.EXE	2368	RegOpenKey	HKCU\Software\Classes\Folder	NAME NOT FOUND
Explorer.EXE	2368	RegOpenKey	HKCR\Folder	SUCCESS
Explorer.EXE	2368	RegQueryKey	HKCR\Folder	SUCCESS
Explorer.EXE	2368	RegOpenKey	HKCU\Software\Classes\Folder\ShellE...	NAME NOT FOUND
Explorer.EXE	2368	RegOpenKey	HKCR\Folder\ShellEx\IconHandler	NAME NOT FOUND
Explorer.EXE	2368	RegQueryKey	HKCU\Software\Classes	SUCCESS
Explorer.EXE	2368	RegOpenKey	HKCU\Software\Classes\AllFilesystemO...	NAME NOT FOUND
Explorer.EXE	2368	RegOpenKey	HKCR\AllFilesystemObjects	SUCCESS
Explorer.EXE	2368	RegQueryKey	HKCR\AllFilesystemObjects	SUCCESS
Explorer.EXE	2368	RegOpenKey	HKCU\Software\Classes\AllFilesystemO...	NAME NOT FOUND
Explorer.EXE	2368	RegOpenKey	HKCR\AllFilesystemObjects\ShellEx\Ico...	NAME NOT FOUND
Explorer.EXE	2368	RegQueryKey	HKCU\Software\Classes\Directory	SUCCESS
Explorer.EXE	2368	RegOpenKey	HKCR\Directory	SUCCESS
Explorer.EXE	2368	RegQueryValue	HKCU\Software\Classes\Directory\Doc...	NAME NOT FOUND
Explorer.EXE	2368	RegQueryValue	HKCR\Directory\DocObject	NAME NOT FOUND
Explorer.EXE	2368	RegCloseKey	HKCR\Directory	SUCCESS
Explorer.EXE	2368	RegQueryKey	HKCU\Software\Classes\Directory	SUCCESS
Explorer.EXE	2368	RegOpenKey	HKCU\Software\Classes\Directory\Doc...	NAME NOT FOUND
Explorer.EXE	2368	RegOpenKey	HKCR\Directory\DocObject	NAME NOT FOUND
Explorer.EXE	2368	RegQueryKey	HKCR\Folder	SUCCESS
Explorer.EXE	2368	RegOpenKey	HKCU\Software\Classes\Folder	NAME NOT FOUND
Explorer.EXE	2368	RegQueryValue	HKCR\Folder\DocObject	NAME NOT FOUND
Explorer.EXE	2368	RegQueryKey	HKCR\Folder	SUCCESS
Explorer.EXE	2368	RegOpenKey	HKCU\Software\Classes\Folder\DocOb...	NAME NOT FOUND
Explorer.EXE	2368	RegOpenKey	HKCR\Folder\DocObject	NAME NOT FOUND
Explorer.EXE	2368	RegQueryKey	HKCR\AllFilesystemObjects	SUCCESS
Explorer.EXE	2368	RegOpenKey	HKCU\Software\Classes\AllFilesystemO...	NAME NOT FOUND