Secure Copying in Network Connection using Knoppix

Nisarg Trivedi
(Institute of Forensic Science,Gujarat Forensic Sciences University, India)

Abstract: *-This paper describes the steps to be taken in obtaining data using a network in virtual environment. It describes the process of secure copying of file from Windows based system to Linux system like knoppix. This procedure helps user to copy data from one system to other without the interception of other parties in same network. Knoppix system transfers data using SSH server which uses authentication protocol to manage connection between end users.*

Keywords: *-Knoppix, Virtual environment, File sharing, SSH Server, Authentication*

I. PURPOSE

The purpose of this procedure is to copy data from one hard drive/folder/file to other computer when both the hard drives are connected in network. This paper provides a procedure for copy these data on hard drives without making changes to the data on the source drives using network. Here one scenario is taken. Both the system installed in VMware Workstation. Target system (in this case it is Windows system) has a folder in it's one of the drive and user has to obtain that folder's data using network.

II. LIST OF TOOLS

i) VMware Workstation
ii) Windows Xp
iii) Knoppixsystem (ISO, CD, Bootable USB)

III. PREPARATION

Take a machine which runs Knoppix system.Knoppix is a bootable Live system on CD, DVD or USB flash drives, consisting of a representative collection of GNU/Linux software, automatic hardware detection.[1]Computers that support booting from USB devices can load Knoppix from a live USB flash drive or memory card.[2]Connect both systems (Knoppix and Target) with Ethernet Cable. Make sure that communication is ON between two systems. User can make sure that by pinging to source system. If there is no packet loss while Request\Response procedure then the target system is open for further processes.

IV .FILE SHARING ON DIFFERENT WINDOWS SYSTEMS

User must check that file sharing option is ON in the target system. Here three windows system is shown. How the sharing option could be enable is also shown. For Windows 7 and Windows 8 password protection must be turned off for sharing.

i) Windows XP

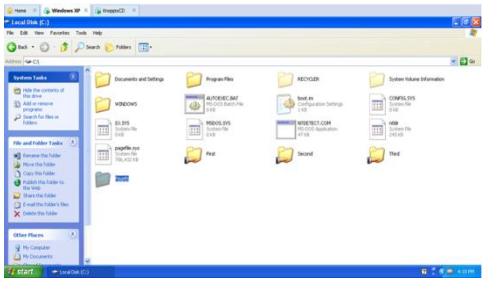

Fig. 1 List of Files and Folders

Here Windows XP is source computer. User has to take files from XP to his own system. For this practical one folder is selected named 'Fourth'.

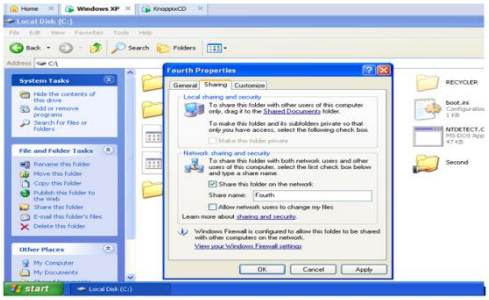

Fig.2 Sharing Folder from Windows System

To share the folder on network, go to Properties→ Sharing option. Check the 'Share this folder on the network' option. User can change the folder name.

He can also allow network users to change files. But User will not check that option, because it may alter the data. So we will leave that checkbox unmarked.

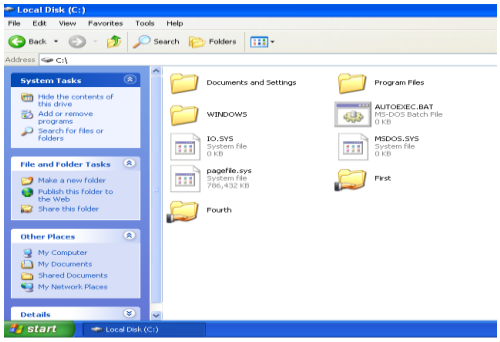

Fig.3 Sign change of Shared Folder

So we can see the change in the icon of the folder. It shows that the folder is now shared and available on network.

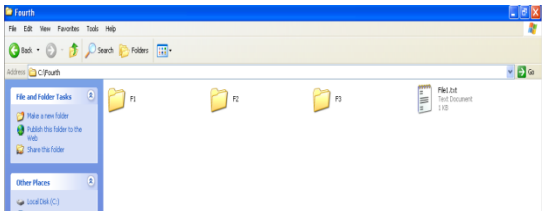

Fig.4 Content of Shared Folder

All the Files and folders of 'Fourth' folder is shown in the figure. These all are also shared as we shared the whole 'Fourth' folder. Note that if you share the parent folder than all the child folder(s)/sub folder(s) are also shared with their content.

i) Windows 7

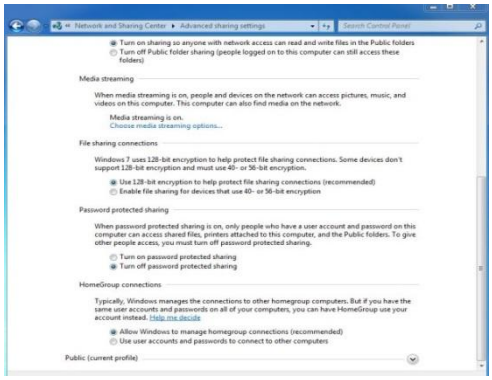

Fig.5 Change Password Protection

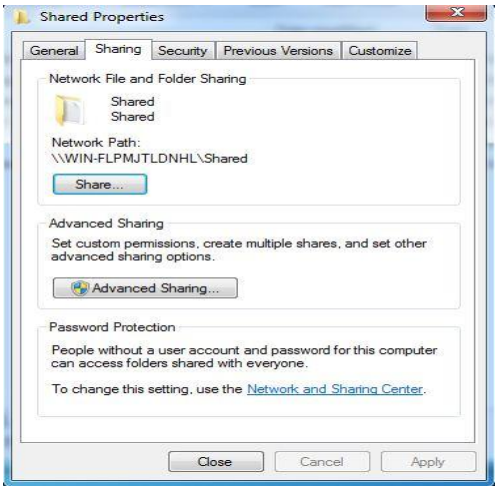

Fig.6 File sharing option

Same procedure is done on windows 7 operating system also. Here, User must sure that password protection is disabled for sharing. User can check by look into 'Advance Sharing Setting'.

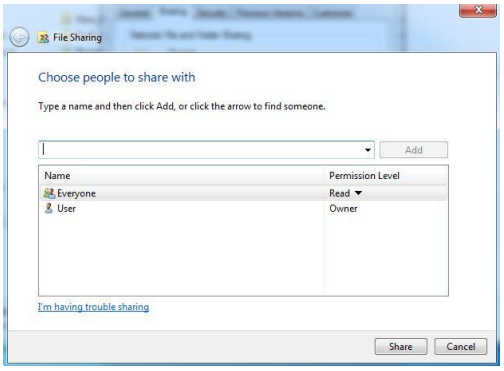

Fig.7 Authentication

Here, only READ permission is given so that there will no modification of data is happen on the device.

ii) Windows 8

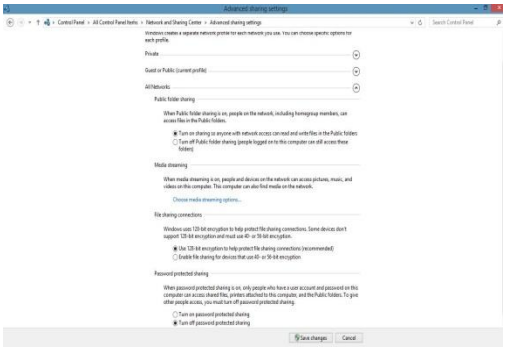

Fig.8 Advance file sharing settings in Windows 8

File sharing in windows 8 is same as Windows 7.

IV. PROCEDURE

User must have to ping between two systems to check communication between them.

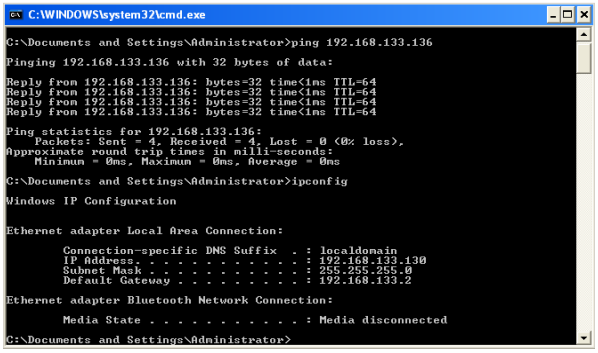

Fig.9 IP Address of Windows System

Here four packets are sent from Windows system, which all are received by Knoppix system (Reverse could also be checked). So both the systems are connected and exchange of information can be done. User must note down the IP address of source system because it will be used in upcoming steps. In

windows system IP address is shown in command prompt by writing 'ipconfig' command.

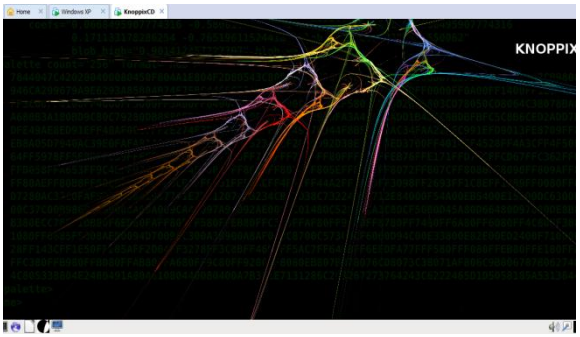

Fig.10 Home Screen of Knoppix OS Live CD

You can also ping from Knoppix system to check the communication between two systems. Here the home screen of Knoppix system is shown.

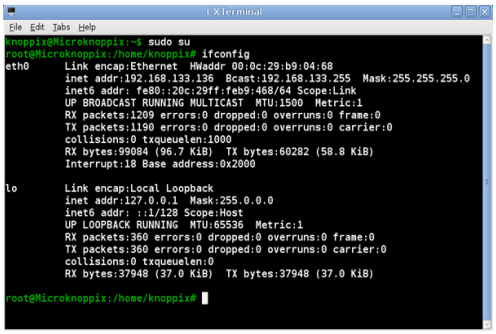

Fig.11 IP address of Knoppix System

First of all we change Knoppix system to Super User to give the Admin privileges. Now the ip address of Knoppix system displays with the help of 'ifconfig' command.

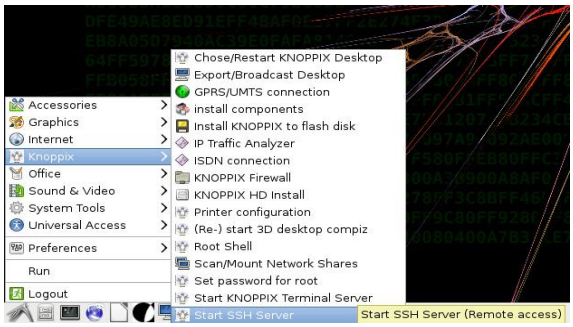

Fig.12 Starting SSH server

First step is to start SSH server from Knoppix.

Fig.13 Password Window to start SSH server

You have to enter same password twice to start the SSH services.[3]

Why SSH server?

- It provides remote login service. It is likely to replace the less-secure Telnet and rlogin programs used in the early days.
- SSH is most often used to provide strong client/server authentication/message integrity—where the SSH client runs on the user's desktop machine and the SSH server runs on some remote machine that the user wants to log into—but it also supports confidentiality. Telnet and rlogin provide none of these capabilities.
- SSH provides a way to encrypt the data sent over these connections and to improve the strength of the authentication mechanism they use to log in. SSH Communicate via port 22.

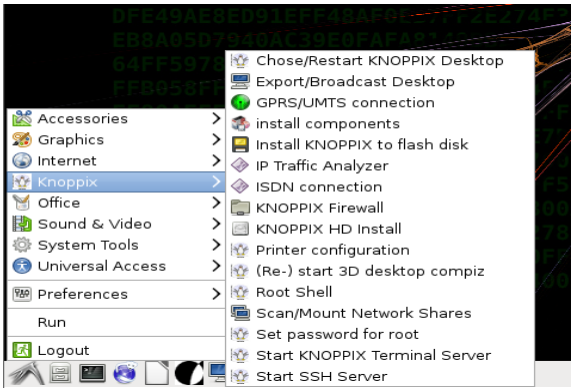

Fig.14 Knoppix Menu

Now next step is to click on Knoppix→'Scan/Mount Network Shares'. It will search for available devices/system connected in the network.

Fig.15 Searching

You can see that search for devices on network are going. Search process will take few seconds to find devices on Network.

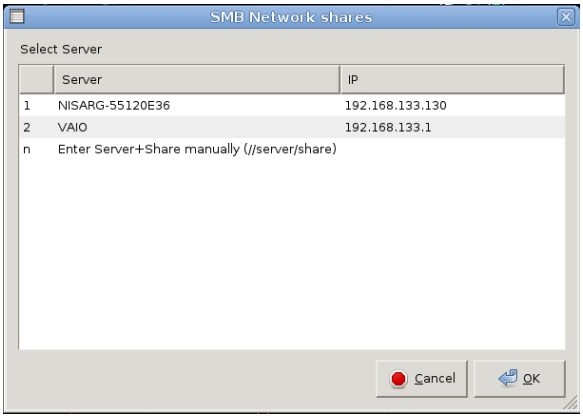

Fig.16 List of available devices on Network

Here two devices are found on network connection. If the target device not found then you can also enter Server and Share name manually. Our suspect is the first one in the list. You can see the list of device name and IP address of the systems.

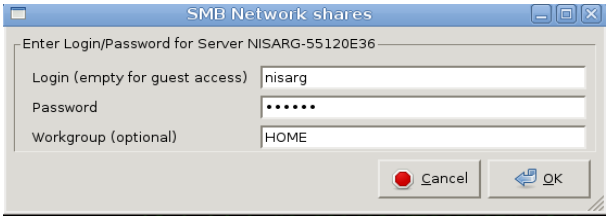

Fig.17 Login Credentials

Here, Login and Password has to be given for create secure transmission of data as discussed above. User must note down Username and Password because same username and password will be used in further steps too.

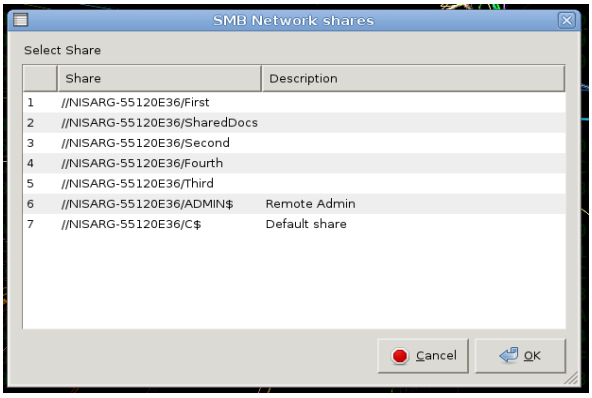

Fig.18 Shared Folders

By clicking on OK it displays the list of shared files and folders of that system. Here we can see the list of all files and folders which are shared from Suspect's system. You can also share whole drive partition.

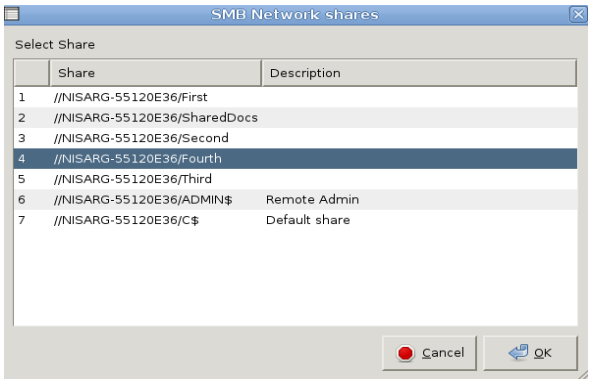

Fig.19 Selection of A folder

This will list out all the files and folders shared from source system. If there are multiple PCs connected in LAN than this box will display the entire PC name with shared folder. Here, we select the 'Fourth' named folder which was previously shared from windows system. After selecting 'Fourth' click OK.

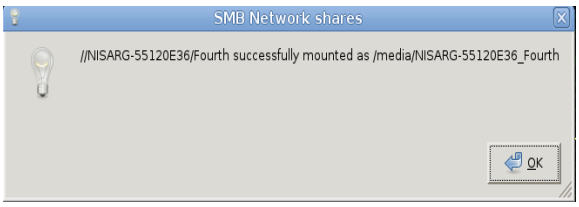

Fig.20 Mounted Successfully

Clicking on OK will take few seconds and one message will appear. It shows that folder is successfully mounted to Knoppix. So, shared folders could be seen from Knoppix system.[4]

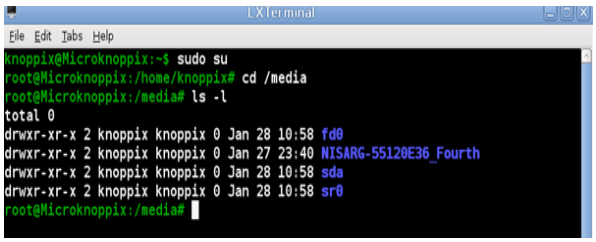

Fig.21 From Knoppix System

The location of the shared folder is in media directory of Knoppix system.So mounted folder can be seen from command prompt by listing the media folder.[5]

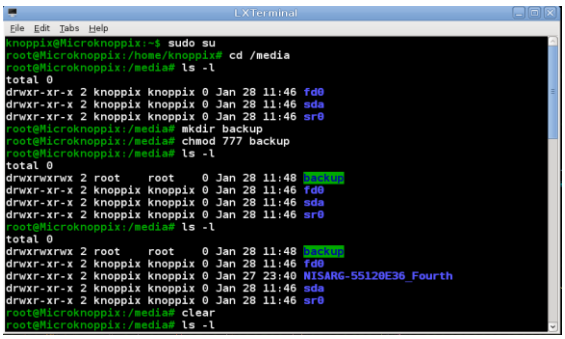

Fig.22 Creation of New Directory to Store data

Another new directory should make by user for storing files from network. Here one directory called 'backup' is created at same location in Knoppix running system. All the privileges are given to that directory. Here in below screenshot backup directory is highlighted. One folder named 'backup' is created in '/media' directory. [5]

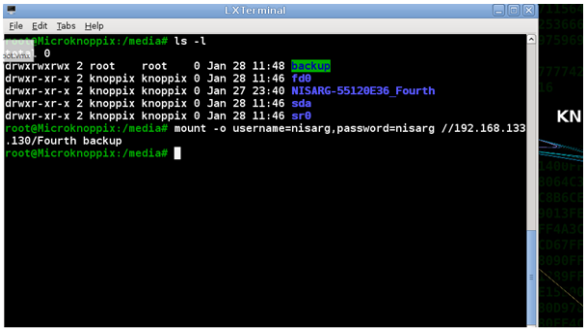

Fig.23 Copying data from Windows System Securely

Now the mount command is used to attach the data from the mapped drive/folder. Here, –o command is stands for options. User has to give username and password which was given at connection time. Ip address of the device should be mentioned and name of the folder is mentioned. At the end storage location of the data is given. Here 'Fourth' folder from ip address of windows Xp system is copied to 'backup' folder of Knoppix system.

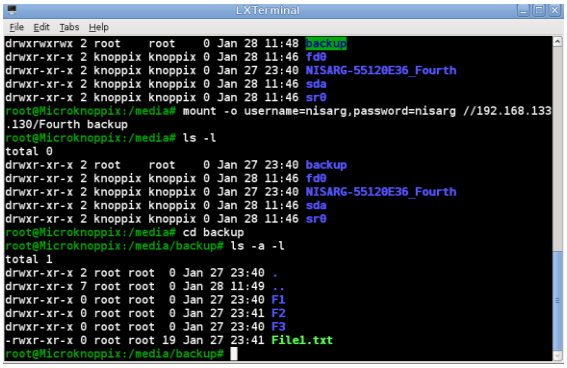

Fig.24 Folders from Windows System

Using ls -l command we can list all the files stored in the directory. [5] Path of backup folder is given. Below figure shows the list of folders and files located in backup folder. User can see the exact names of files and folders which are generated and stored on windows system in 'Fourth' folder.

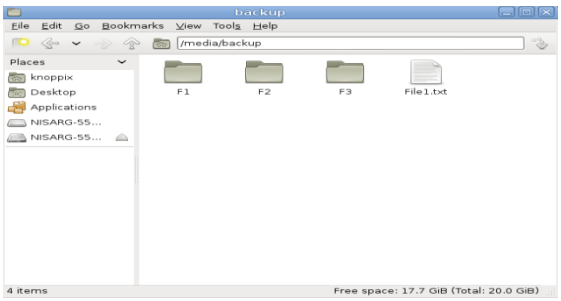

Fig.25 Mounted folder from Windows System

Here the backup folder is shown in the figure. It shows the same files and folders which are shared from Windows system. After that we can image that folder and create the dd file for investigation. It is noted that only those files are copied that are seen to user. No deleted files, slack space or unallocated files are recovered.

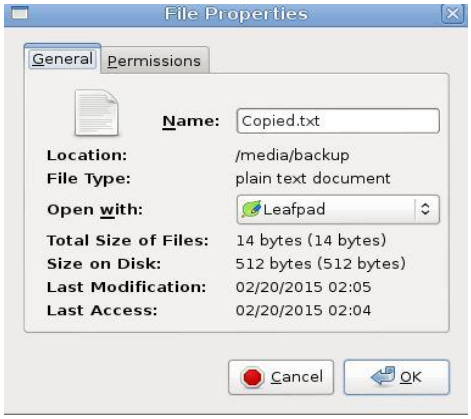

Fig.26 File Property

File property can be seen by selecting property option from pop-up menu. Here File Type, Size, Timestamp is shown.

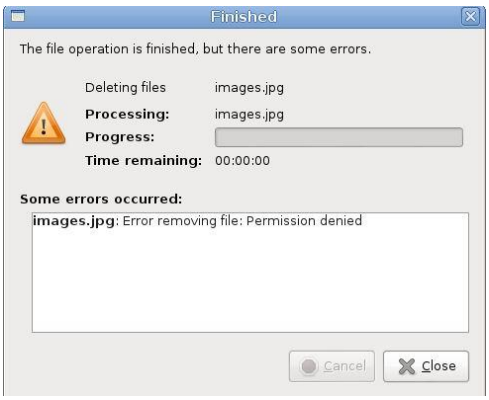

Fig.27 Deletion Failed

User could not delete the files which are copied from windows system to backup folder. So no alteration in data could be done.

V. ADVANTAGES

Data can be copied from multiple locations.
Data will start copying after entering correct username and password.
Data will pass from SSH tunnel it means copy of data is secure.
Data cannot be altered when transportation took place.
Breaching of data could not be done.
Data cannot be modified in destination folder it means that integrity of data is maintained.
User can copy the data from multiple sources in same network.
At forensic investigation time investigator can boot the system using Knoppix with LinEn (Linux EnCase) to copy suspect's system data. [6]

VI. LIMITATIONS

Both the systems should be in same network.
Both the systems should alive for communication.
User should have knowledge about Knoppix system and Knoppix commands.
In windows system like Windows 7 and above password protection should be turned off.

VII. CONCLUSION

This process is mainly used to copy data securely. It prevents the interruption of any third party in data transmission. This process helps user to copy data from multiple system which are in same network and in a system like where hard drive is impossible to remove.

REFERENCES

[1] http://www.knopper.net/
[2] http://en.wikipedia.org/wiki/Knoppix
[3] Hard Drive Cloning in Linux using dd, gzip and growisofs.pdf
[4] Linux and UNIX dd command help and examples.pdf
[5] Windows Disk Drive Image Backup to Samba Server With DD - How To - Joe's Cat Website.pdf
[6] The Official CHFI Study Guide for Computer Hacking Forensics Investigators [Exam 312-49].pdf
[7] Incident Response & Computer Forensics, 2nd Ed.,.pdf
[8] Understanding Forensic Digital Imaging.pdf
[9] http://www.pendrivelinux.com/install-knoppix-6-to-a-usb-flash-drive-in-windows/