File Carving From PCAP

Mr. Nikunj Chavda [1], Mr. Anisetti Anjaneyulu [2],Mr. Dhruv Prajapati[3]

[1]Digital Forensics Analyst e-SF Labs LTD

[3]Digital Forensics Analyst e-SF Labs LTD

Abstract: - *In today's world sharing files on the Internet is quite a simple task for any of the people even for the kids also and now a days crimes is happening through the network with viruses and Trojans and also some of the mischief documents are sending through the Internet. For all of this, network monitoring and pcap analysis are sparingly required. All the network monitoring tools create pcap files and analyst may further analyze this file and find any anonymous activity. Here in this paper there is one scenario in which pcap is analyzed in such a manner that if any file transmission occurs through then embedded files can be carved when it is deeply analyzed with proper techniques. File carving is the process of reassembling computer files from fragments in the absence of file-system meta-data. The basic analysis scenario is, we have three pcap files. Each pcap file has the packets which are captured while transferring different files and in this practical scenario we will see how can we analyze the pcap file and will carve the transferred files over it.*

Keywords: *Network traffic analysis, pcap analysis , file carving, file time-stamps*

I. INTRODUCTION

Cyber crime! Cyber crime! Cyber crime!

Now a day it's a common word for crime happening through technology because it grows worse. People use more and more technology and do the wrong things with it and it's under cyber crime. Network forensics is a most important part of the cyber forensics. Commonly people think what they see (means hard-disk , pen drive and data storage) it's the artifact for the cyber crime cases but now network artifacts which are not seen routing through network packets is the most crucial artifacts for cyber crimes.

Anti-forensic techniques leads cyber investigators to the another black hole of the cyber world. Most of the anti-forensics techniques are used on the file system or on storage devices, but network artifacts cannot be hidden from the cyber analyst eyes. There are very less number of anti-forensics techniques in network area and they are very hard to do and mostly nobody knows about the network artifacts. But network artifact is a very crucial thing because storage media can be wiped-out very easily but when network traffic has been monitoring, its fragments cannot be altered and can be stored in the pcap files. Some miscellaneous file transferred from one end to another can be proven through network traffic which is stored in pcap files therefore first thing is to monitor a network and later analyze pcap files. In corporate environment network traffic is monitored throughout its servers and this can be further analyzed through various tools which is described in this paper. File carving is the most powerful technique in the disk forensics to recover deleted files and here the same will be applied to pcap files so that embedded files transferred over the network may be carved from the pcap file and this becomes a potential artifact in the area of cyber forensics.

II. TOOLS & TECHNOLOGY USED

For the monitoring of the network traffic and for analysis of that pcap file there are lots of tools available in the market. Here goes to present some of the best tools which are used for analysis.

1. Wireshark:
Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

2. Network miner:
NetworkMiner is a Network Forensic Analysis Tool (NFAT) for Windows that can detect the OS, hostname and open ports of network hosts through packet sniffing or by parsing a PCAP file. NetworkMiner can also extract transmitted files from network traffic.

3. Foremost:
Foremost is a console program to recover files based on

their headers, footers, and internal data structures. This process is commonly referred to as data carving.

III. ACQUIRE NETWORK TRAFFIC

Network traffic acquisition is the most important task since this is live monitoring so if any mistake occurs during acquisition, one may lose important artifacts. Here Wireshark is used for monitoring the network traffic. Steps for monitoring network traffic through wireshark are described below.

1. Open Wireshark and select the network interface which is active.
2. Now start capturing packets and save the pcap file.

IV. ANALYSIS PROCESS

After capturing the network traffic main thing is to analyze pcap files so here there are three tools used to describe how to analyze it the tools & technology section. The Analysis process is little bit tough compare to normal hard disk analysis because here there are lots of network packets in one small packet file. The Analyst has to an identified need of the case and through that filter can be applied and has to identify the packet needed to prove the crime.

1. Analysis Through Wireshark:

Open the pcap file in the Wireshark and in the filter type "http". Wireshark shows the http packets now find any file format packets in the packet description. Here it is is a zip file.

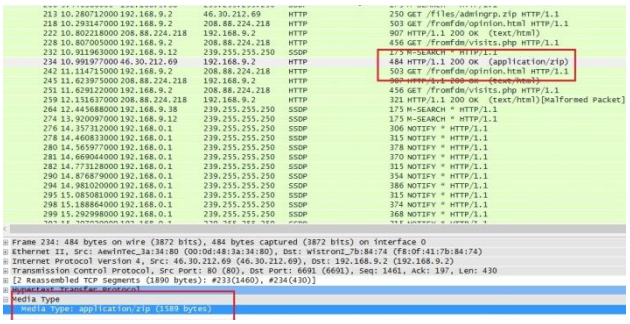

Fig.1 Packet Information In Wireshark

Now select the media type shown in the above image and go to "File menu > Export Selected Packet Bytes" and save it in the appropriate file format. Here it is a zip file so here it's saved as 1.zip with packet as a media type.

Here is the proof that the zip file is the same which is transferred through the network and the file which is stored in disk both files has same hash.

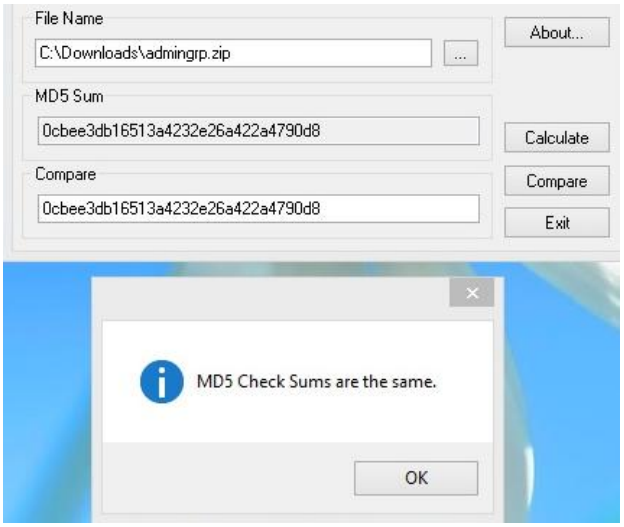

Fig.2 Integrity Checking

2. Analysis through Network Miner

In this scenario one document file is downloaded through the network and network monitor is done through the network server and captured in one pcap file. Now the analysis of this pcap would be done by Network Miner. Steps to analyze the pcap file and identification of the doc is explained in below steps.

1. First open the pcap file in Network Miner. It shows the packet information in host tab that specifies the connection of this pc to the other hosts.

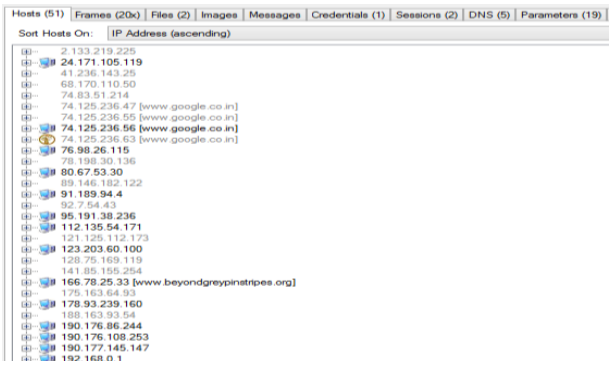

Fig.3 Pcap In Networkminer

2. Now go to the file tab (not File menu) in the Network Miner. Here it shows the file which is transferred through the network with a destination and source IP-address with specific time and also file size and protocol used to transfer that file from source to destination. Now right

click on the file packet and click on the open folder option, it will show the reconstructed file path from the network packets.

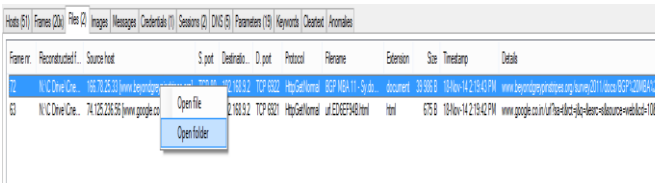

Fig.4 Carved File In Networkminer

Here is the proof that the doc file is the same which is transferred through the network and the file which is stored on disk and both these files has same hash.

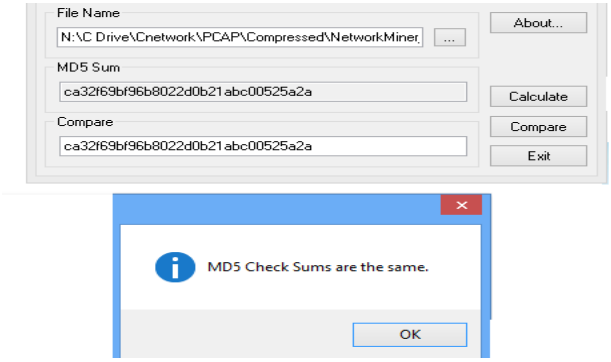

Fig.5 Integrity Checking

3. Analysis Through Foremost

Foremost is file-carving tool for various types of files supported. It is installed inbuilt in some forensic tool-kit's like DEFT , SIFT etc. Foremost is a command line tool for the Linux flavor. Below is a step For carving from the pcap file in the foremost.

1. First open the foremost and write the command.

Foremost -v -i "/root/Desktop/img.pcap" -T

Where -v denotes verbose mode

-i denotes input file

-T denotes all the type of file

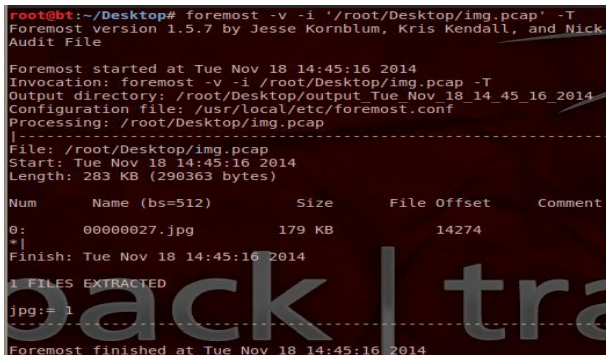

Fig.6 Pcap In Foremost

2. Now go to the path where the output is stored. It is shown in the above image.

In the output folder one audit file is there that shows the result of the carving.

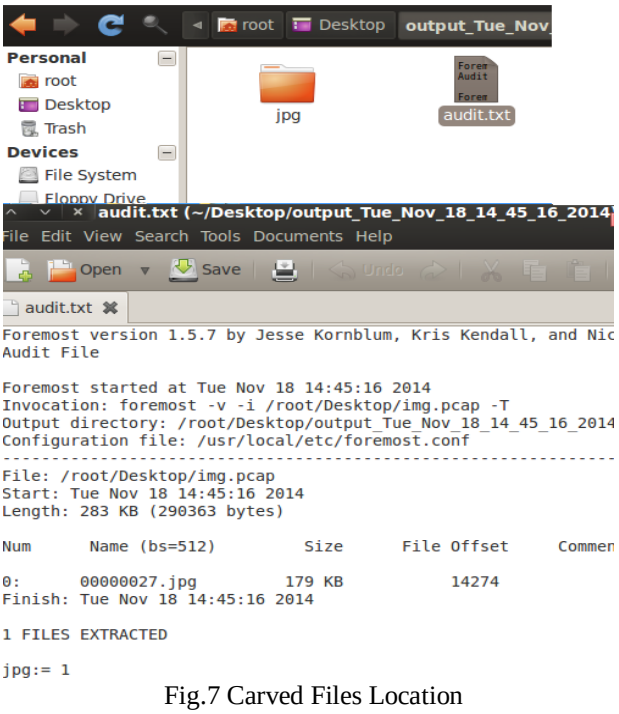

Fig.7 Carved Files Location

And the image is in the output folder display here.

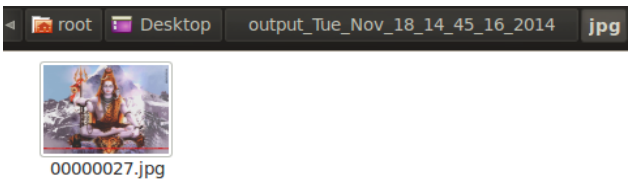

Fig.8 Carved File

Here is the proof that the image is the same that is transferred through the network and that is stored on disk and both has same hash.

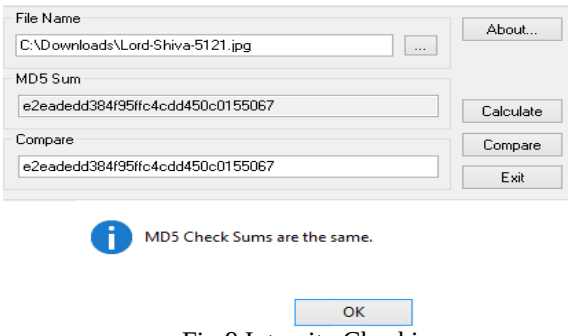

Fig.9 Integrity Checking

V. CONCLUSION

From the above experiment it is proving that network analysis is sparingly necessary for the live forensics and also the carving method from the network traffic. In future may be more efficient techniques would be invented for network analysis.

REFERENCES

[1] http://foremost.sourceforge.net
[2] http://sourceforge.net/projects/networkminer/files/networkminer
[3] http://en.wikipedia.org/wiki/Wireshark
[4] http://sourceforge.net/projects/sevenzip/?source=typ_redirect
[5] www.beyondgreypinstripes.org/survey2011/docs
[6] http://3.bp.blogspot.com/_9A-AM7dxzww/TITzUKFQRmI/AAAAAAAAADQ/-ujVYQE_pZ8/s1600/Lord-Shiva-5121.jpg
[7] www.nullriver.com
[8] http://www.ijmer.com/papers/Vol3_Issue5/DD3530963106.pdf
[9] http://www.sans.org/course/advanced-network-forensics-analysis
[10] http://www.sigcomm.org/sites/default/files/ccr/papers/2012/April/2185376-2185382.pdf
[11] http://delaat.net/rp/2013-2014/p73/report.pdf