Traffic Sanitization Guide

December 26, 2010

1 Introduction

This document includes description of each tools that we used in TrafficSanitization project. There are two kinds of tools: kernel level and application level. You can find all of them in our VirtualMachine(TrafficSanitization.vdi).

2 Kernel Level Code

This project is built on top of CompareView project. Hence, we recommend you to use CompareView guide for code description. All the code specially related to this project are following comments *TrafficSanitization 12/20/2010* in the same files as code of CompareView.

3 Application Level Code

All the tools that we used for application part of this project are MFC application. We put them under the folder *MyCode* on the desktop of the virtual machine *WinXP_P2PTraffic*. Three main applications are used: *TCPHash*, *FakeTraffic*, and *RandomStrGen*, which are described as follows.

3.1 TCPHash

TCPHash is the peer-to-peer simulator we used to send packets for searching certain key words or downloading specific files. You can follow the steps shown in figure 1 to fulfill these function. When pressing *send* button, we search in local directory other than a real peer-to-peer network. The local directory is `c:/`. We use *kwhv:* as the beginning and hash value followed as the content of each packet.

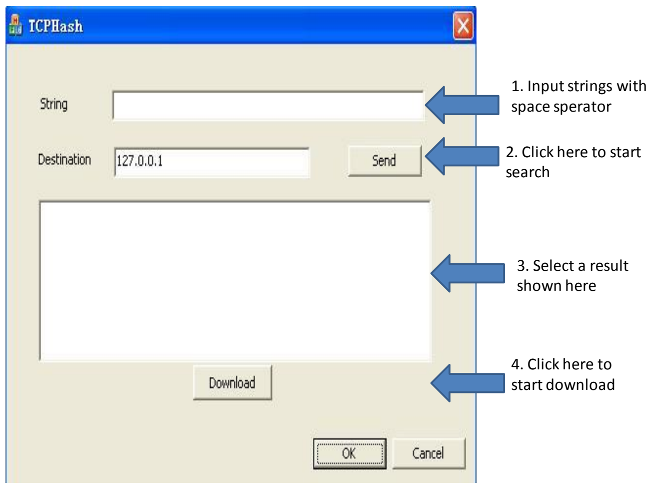

TCPHash
String
Destination
127.0.0.1
Send
Download
OK
Cancel
1. Input strings with space sperator
2. Click here to start search
3. Select a result shown here
4. Click here to start download

Figure 1: P2P simulator

3.2 FakeTraffic

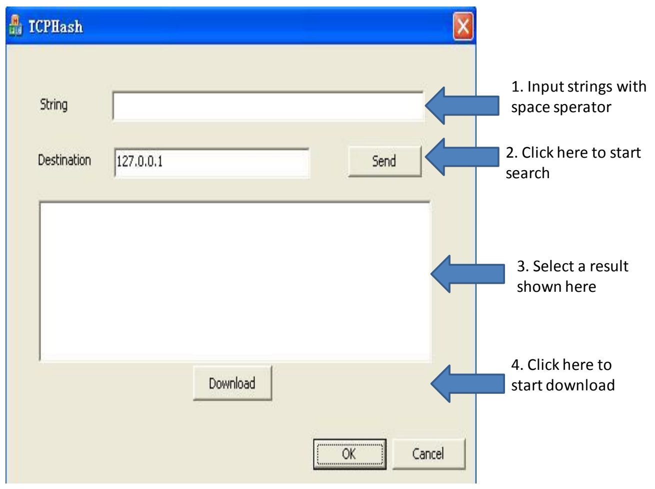
FakeTraffic sends out packets with the same format of *TCPHash* based on hashes stored in the files generated by *RandomStrGen* application. We automatically log all fake traffic in the file `C:\faketraffic.log`You can specify number and size for each sending as shown in figure 2.

3.3 RandomStrGen

RandomStrGen generate certain pairs of word and hash value stored in `C:\WINDOWS\keyhash.log`. We use space as a sperator and length of each word is random. Screenshot is shown in figure 3.

4 Others

You can find related documents or tutorials about eDonkey protocol under *Doc* directory with the source code.



String:

Destination: 127.0.0.1

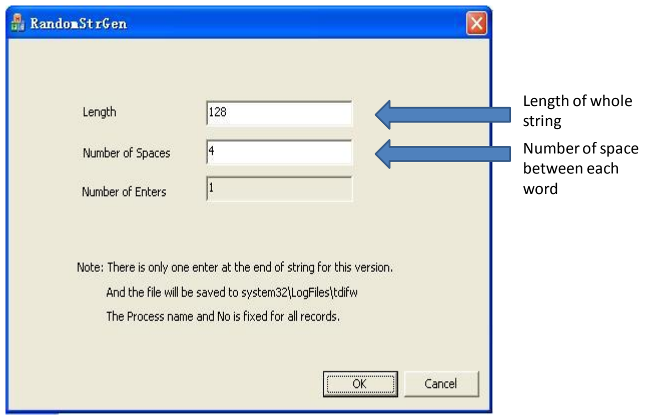
1. Input strings with space sperator

2. Click here to start search

3. Select a result shown here

4. Click here to start download

Figure 2: P2P Traffic Generator



Length: 128

Number of Spaces: 4

Number of Enters: 1

Note: There is only one enter at the end of string for this version.
And the file will be saved to system32\LogFiles\tdifw
The Process name and No is fixed for all records.

Length of whole string

Number of space between each word

Figure 3: Hash Generator