DbgView + Network Dump Files = LoVsPcapTracer Tool

Status: 2021-04-27

Author: Enno Herr

Index

Introduction

Usage case

The intention is to combine the well known tools

- DbgView (https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx)
- Wireshark (https://www.wireshark.org/)

DbgView displays the debug output of various programs, while Wireshark's purpose is to analyze network traffic.

The following tool tries to solve the correlation problem with the information coming from a specific program and what is happening the same time on the network. This should make it easier in the follow-up analysis of the data gathered. Furthermore it reduces the output to the minimum since unnecessary data is deleted – the PCAP files can take up quite huge space when gathering data over a longer period of time.
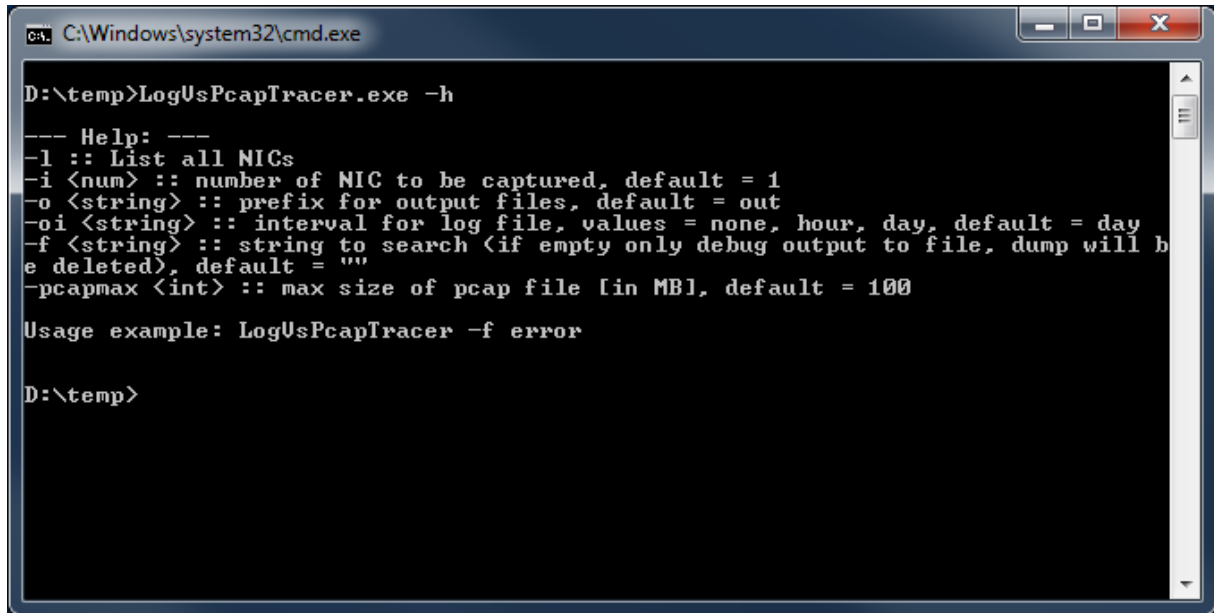
Installation requirements

If no Wireshark has been previously installed on the system, then it is necessary to install either Wireshark or Npcap (https://nmap.org/npcap/). This is a requirement in order to gather and safe network data from directly from the network card.

Help and Usage

Get Help

Use "LogVsPcapTracer -h" in order to list all the options and how to use them (see Figure 1).

One of the purposes of this program is to filter out specific data gathered by the debug output. Therefore the only Parameter that might be required is "-f <string>". Replace <string> with the data that should be searched for.
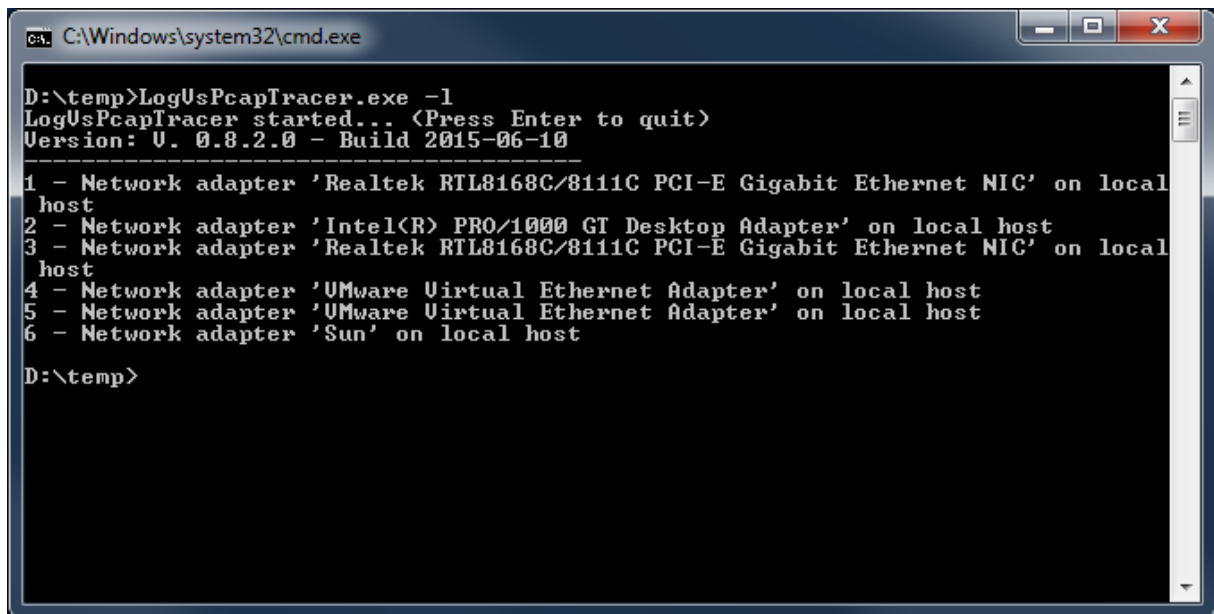

Figure 1 - Command line options

Select Network Interface

If a system with multiple network cards is in use, then it might be necessary to select the adapter which should be observed. Note that by default always the adapter with index "1" is taken. Use "LogVsPcapTracer -l" to list all the available network adapters (see Figure 2).

In the next step start the program with the adapter number, e.g. if adapter number 3 should be used then use "LogVsPcapTracer -i 3".
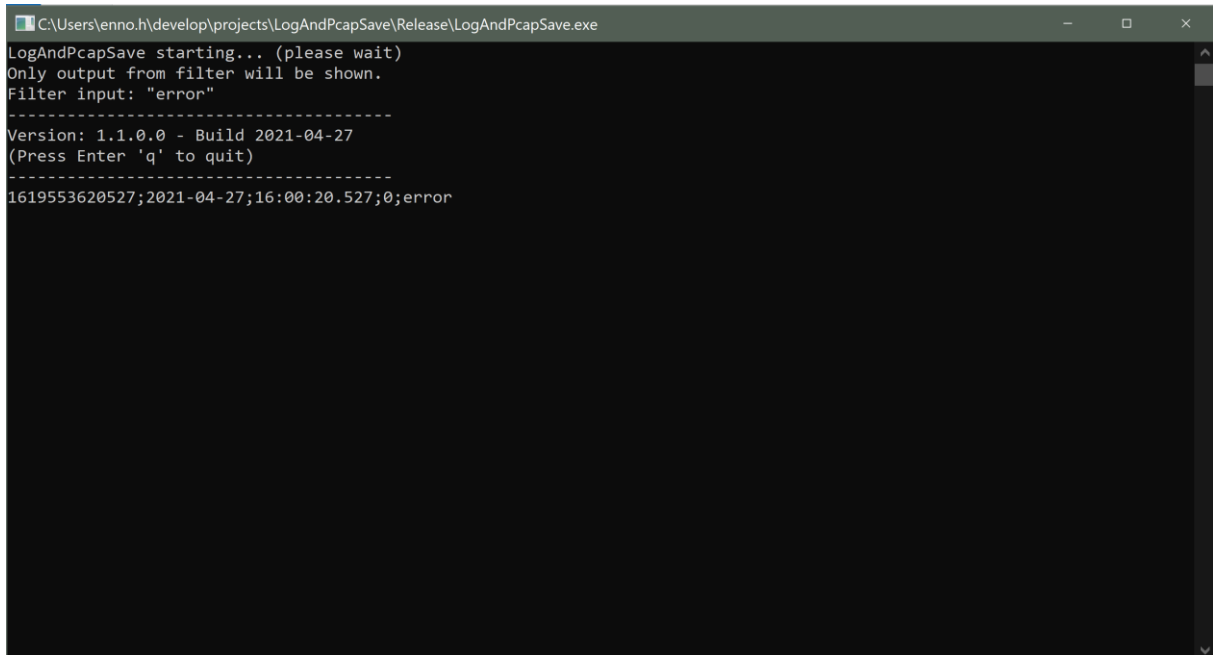
Figure 2 - Show all available network adapters

Output and Analysis

Console output

In Figure 3 LogVsPcapTracer has been started to filter the word "frames". Only this output will be shown in the console window. All other data will be gathered in log files, which will be discussed in the following chapter.

Figure 3 - Program output of the filtered results

File output

By default all debug data will be safed in the file "out_all_<year>-<month>-<day>_<hour>-<min>-<sec>-<msec>.txt" ("out" is replaced if the "-o" option is used).

If a filter is given then a log file with the name "out_filter_<…>.txt" will be created.

The third file is the network dump in the naming format "out_<…>.pcap". This file will be deleted if no filter value applies. Since the dump file size can grow very fast, those files will be deleted once after a specified size is reached (see "-pcapmax" option).

Figure 4 shows the saved files. The two PCAP files contain the captured data, while the data was filtered out of the log files.
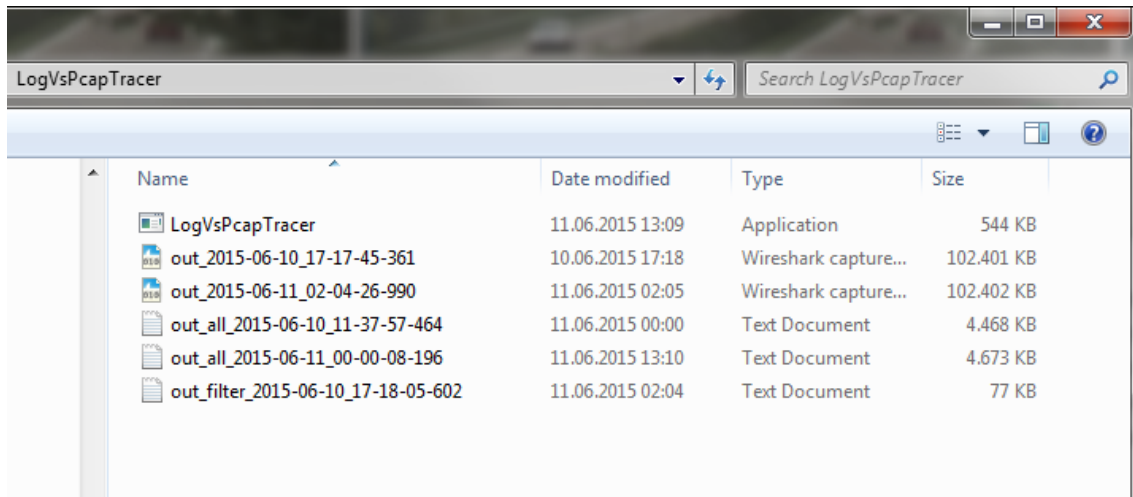
Figure 4 - Files generated by the program

Log Files

The log files (see Figure 5) are written in CSV (Comma Seperated Value) style and can be imported into e.g. Excel for further sorting and analysis.

The file contains the following columns:

- Unix Timestamp in MSec: https://en.wikipedia.org/wiki/Unix_time
- Date: <year>-<month>-<day>
- Time: <hour>:<min>:<sec>.<msec>
- Debug output: Text that was created by the program
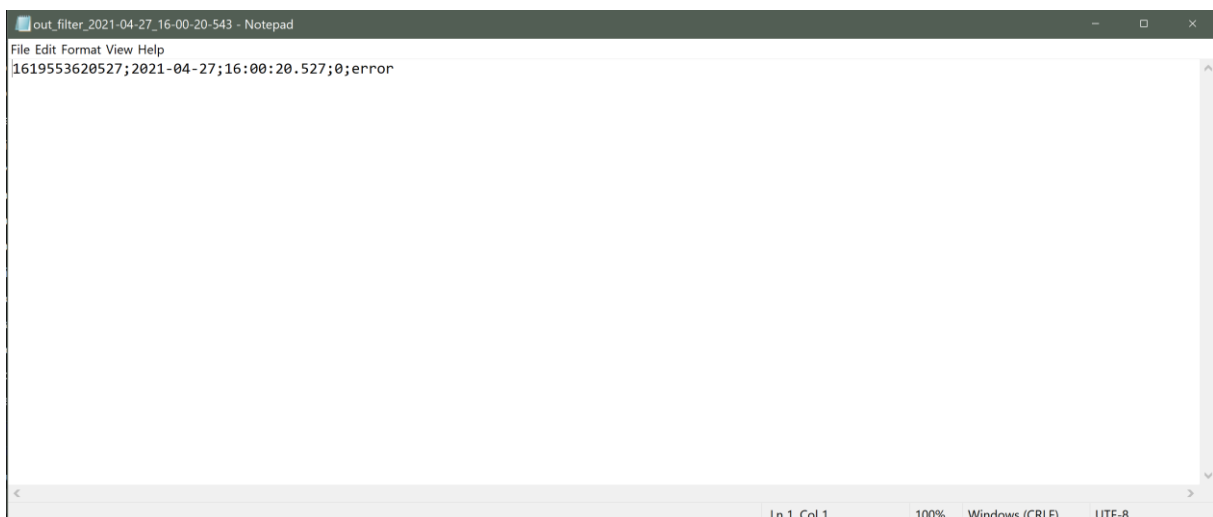

Figure 5 - Example log file data

Network Dump Files (PCAP)

The PCAP file can be opened and analyzed in Wireshark. It might be convenient to add the column "Time Readable" to find the exact date and time when the event filtered out occurred (see Figure 6).
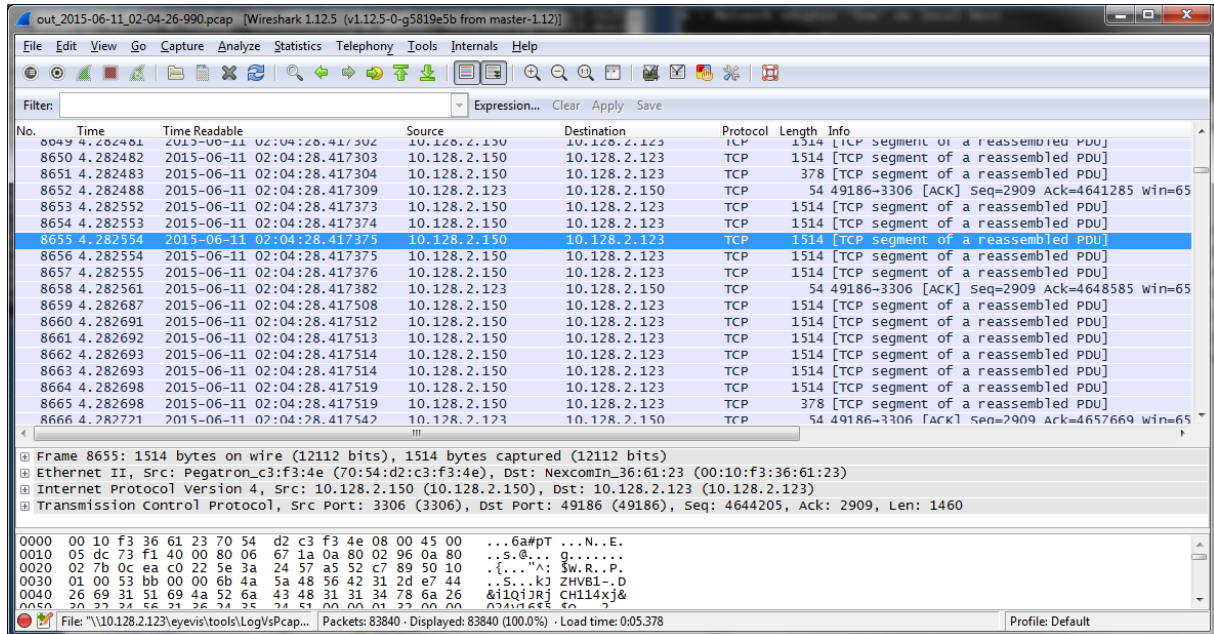

Figure 6 - Wireshark: The column Time Readable was added.