BRNO UNIVERSITY OF TECHNOLOGY — FACULTY OF INFORMATION TECHNOLOGY

#52 Excel@FIT 2017

Network Traffic Capture with Application Tags

Jozef Zuzelka
Faculty of Information Technology, Brno University of Technology
xzuzel00@stud.fit.vutbr.cz

Abstract Network traffic capture and analysis are useful in case we are looking for problems in our network, or when we want to know more about applications and their network communication. This research aims on the process of network applications identification that runs on the local host and their association with captured packets. Every identified application is stored in an application cache with information about its socket to save time and not to search for already known applications. Operations that can be done independently are parallelized to speed up packet processing and reduce packet loss.

Problem solution

- Network traffic capture using *libpcap*/*npcap*.
- Uses PF_RING to speed up capture process.
- Captured traffic is continuously saved to the output file.
- Recognized applications are appended to the end of the output file as a separate pcap-ng block.

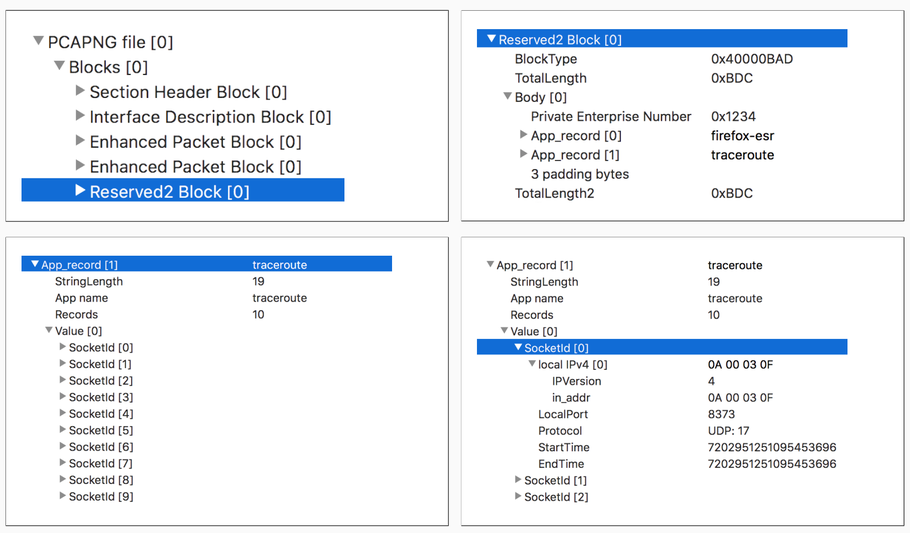

Fig. 1: Structure of extended pcap-ng file

Experiments

Tests were made on *Ubuntu 16.04 LTS* with *Broadcom 5701* ethernet card. Fig. 4 shows an amount of data which can be processed in dependence on packet size. It is important to note that it shows identification of just one communicating application.

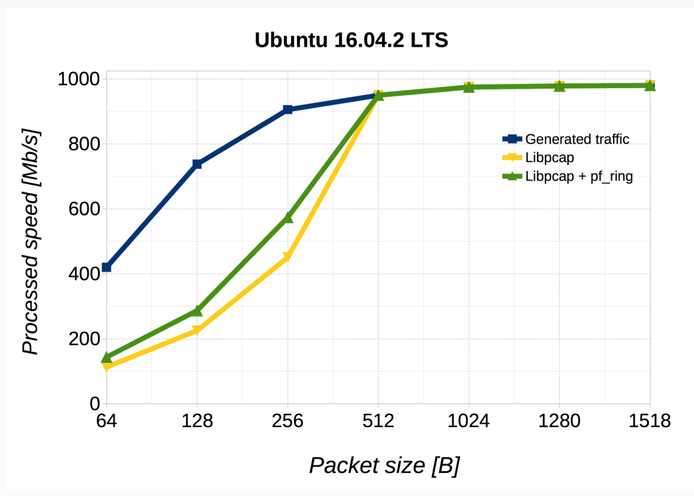

Fig. 4: Determining applications on Linux

Design

- The application works in three threads.
- It also uses ring buffers between threads to handle sudden peaks in network traffic.

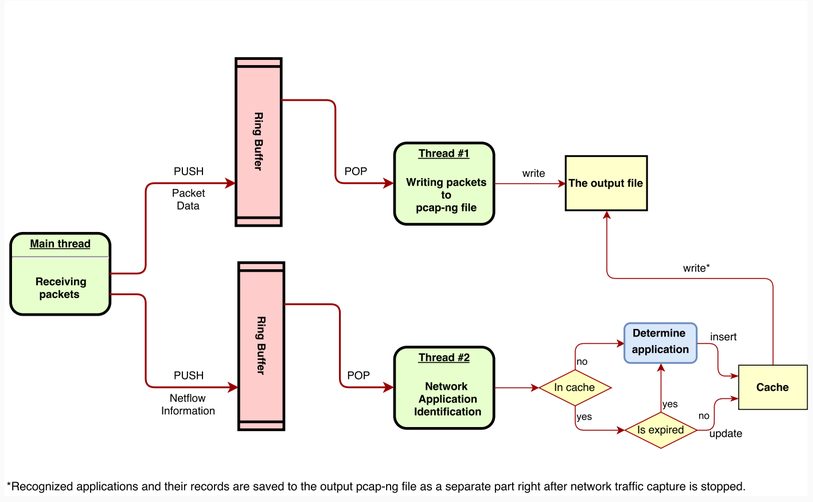

Fig. 2: Threads and their roles

- An application cache is used to speed up network application identification.
- The cache consists of three levels – local port level, local IP address level and transport protocol level.

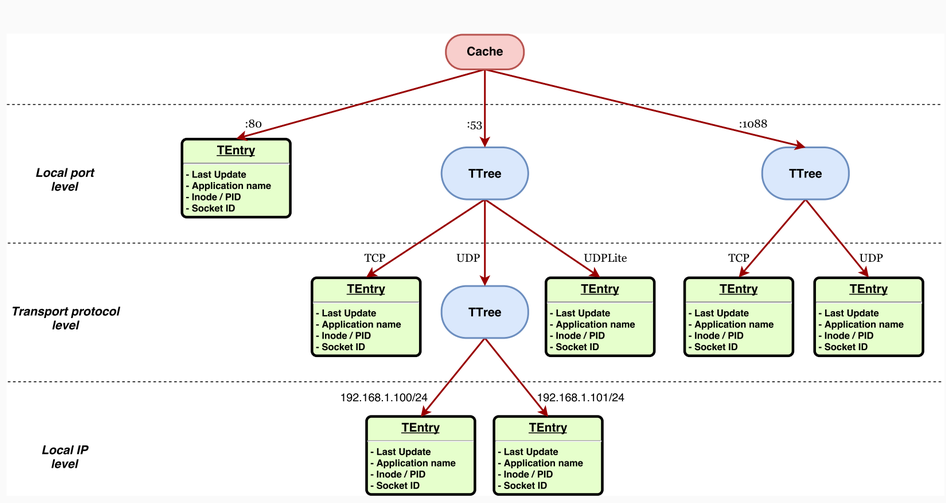

Fig. 3: Example cache structure

Future work

- Support for other platforms (FreeBSD, MacOS)
- Exploring faster methods of determining applications in Linux