Labolatorium Programowania Sieciowego

Analizator ruchu TCP/UDP/SCTP

Radosław Skałbania 07.01.2020

1. Opis działania oraz instrukcja obsługi programu PyShark.

PyShark jest to napisany w języku programowania „Python” program ściągający pakiety z sieci, posiadający interfejs graficzny. W szczególności oparty jest on na surowych gniazdach („RAW sockets”).

Część graficzna została stworzona przy pomocy modułu „Tkinter”, który umożliwił przetworzenie danych w taki sposób aby wszystkie pakiety przychodzące na urządzenie pojawiały się w czasie rzeczywistym w prosty i przejrzysty sposób na ekranie użytkownika. Część backend’owa została głównie oparta na module „sockets” oraz na manipulacji strukturami danych („lists” , „dictionaries”). Połączenie strony backednowej z frontendem umożliwiła biblioteka threading.

Uruchamiając program mamy do wyboru cztery przyciski: „Run sniffing”, „Stop”, „Clear” oraz „Quit”. Dodatkowo istnieje również kilka sposobów na odfiltrowanie pakietów – wybór protokołów warstwy trzeciej (IPV4, IPV6) oraz protokołów transportowych warstwy czwartej (ICMP, TCP, UDP, SCTP). Pierwszy z przycisków uruchamia ściąganie pakietów z sieci, drugi zatrzymuje tę procedurę, trzeci oczyszcza okno z danymi, a czwarty zamyka program. Poniżej przycisków znajduje się siedem kolumn. Każda z nich reprezentuje pewien rodzaj danych poszczególnych pakietów. Każdy z rzędów reprezentuje jedną ramkę. Interfejs został zaprojektowany w stylu “tree view”, oznacza to że klikając na daną ramkę rozwija się ona o dodatkowe informacje. W pierwszej warstwie znajdują się informacje na temat warstwy internetowej ramki, po jej rozwinięciu uzyskujemy dane związane z warstwą fizyczną oraz transportową pakietu.

Struktura projektu została podzielona na trzy części: “backend_pkg”, “frontend_pkg” oraz skrypt uruchamiający cały program “run.py”. Pierwsza z nich posiada funkcje oraz klasy odpowiadające za ściąganie pakietów z sieci, formatowanie ich oraz wstawianie ich do interfejsu graficznego. Druga część posiada klasę tworzącą GUI. Do wszystkich klas w projekcie zostały dodane opisy (“docstring”).

Do prawidłowego uruchomienia programu nie są wymagane żadne zewnętrzne moduły. Jedynym warunkiem prawidłowego działania aplikacji jest korzystanie z systemów Linux oraz uruchomienie skryptu „run.py” z przywilejem administraotra. W moim przypadku program działa prawidłowo na systemie “Ubuntu 18.04”.

- Wymagania
  ➔ „Python 3”- testowane na wersji 3.7.4
  ➔ System linuxowy – testowane na Ubuntu 18.04
- Dodatkowo
  ➔ Moduł : „pyinstaller”

- Uruchomienie programu

  Aby poprawnie urchomić program należy przez terminal wejść do katalogu w którym znajduje się skrypt „run.py”. Następnie uruchomić go za pomocą komendy „sudo python3 run.py”.

  Można również stworzyć plik binarny używając modułu „pyinstaller”, za pomocą komendy „pyinstaller run.py –onefile”. Utworzy nam się nowy folder o nazwie „dist” w katalogu docelowym. Należy do niego wejść a następnie uruchomić program za pomocą komendy „sudo ./run”

Poniżej zamieszczam link do repozytorium projektu:

https://github.com/radekska/Projects/tree/master/Python/PyShark