|  |
| --- |
| Vysoké učení technické v Brně  Fakulta informačních technologií |
| Sniffer packetů |
| Varianta ZETA |

|  |
| --- |
| Michal Halabica (xhalab00)  IPK 2020 |

Obsah

[1. Úvod 2](#_Toc39434817)

[2. Platforma a závislosti 2](#_Toc39434818)

[2.1. Knihovny 2](#_Toc39434819)

[3. Překlad 2](#_Toc39434820)

[4. Spuštění 3](#_Toc39434821)

[4.1. Parametry 3](#_Toc39434822)

[5. Implementace 3](#_Toc39434823)

[5.1. Výpis aktivních rozhraní 3](#_Toc39434824)

[5.2. Zachytávání packetů 3](#_Toc39434825)

[6. Testování 3](#_Toc39434826)

[6.1. Alternativní nástroje (Wireshark) 3](#_Toc39434827)

[7. Zdroje 3](#_Toc39434828)

# Úvod

Cílem aplikace je sledování packetů síťového provozu. Pro sledování síťového provozu se používá síťové rozhraní, které je specifikováno při spuštění aplikace.

Aplikace podporuje výpis TCP, UDP a ICMP packetů. Zbylé druhy packetů jsou ignorovány.

# Platforma a závislosti

Aplikace je psaná v jazyce C# a jako platforma pro tento jazyk se používá platforma .NET Core 3.1

.NET Core je open-source platforma běžící napříč platformami operačních systémů (Windows, Unix (vč. MacOS)).

## Knihovny

Veškeré knihovny jsou instalovány z balíčkovacího systému NuGet, díky tomu nemusí být knihovny distribuovány při přenosu aplikace. Při překladu se všechny potřebné knihovny stáhnou automaticky.

Pro implementaci aplikace bylo využito následujících knihoven:

* [CommandLineParser](https://github.com/commandlineparser/commandline)

Knihovna pro zpracování parametrů příkazové řádky a jejich uložení do struktury.

* [SharpPcap](https://github.com/chmorgan/sharppcap)

Knihovna zajišťující multiplatformní práci s knihovnami WinPcap (Windows) a LibPcap (Unix) v prostředí jazyků z rodiny .NET. Pro správný chod této knihovny je potřeba na cílovém zařízení mít nainstalovanou příslušnou knihovnu v závislosti na operačním systému.

# Překlad

Pro přeložení aplikace lze použít nástrojů přímo ve vývojovém prostředí jako je Microsoft Visual Studio, nebo JetBrains Rider.

Vzhledem k tomu, že je aplikace psaná pod platformou .NET Core 3.1 lze aplikaci také přeložit pomocí utility „dotnet“.

Pro jednodušší překlad je u zdrojových souborů aplikace dodán i Makefile, který obsahuje následující pravidla:

* build

Překlad aplikace. Toto pravidlo volá utilitu dotnet s následujícími parametry:

* + build – Příkaz pro utilitu, že se má provádět překlad.
  + „ipk-sniffer/“ – Cesta k projektu.
  + „-c Release“ – Překlad pro finální produkční prostředí.
  + „-o build/“ – Cesta k adresáři, kde se uloží sestavená aplikace a potřebné knihovny.
* clean

Vyčištění výstupního adresáře. Toto pravidlo volá příkaz „rm -rf build/“.

# Spuštění

## Parametry

# Implementace

## Výpis aktivních rozhraní

## Zachytávání packetů

# Testování

## Alternativní nástroje (Wireshark)

# Zdroje

What is .NET? An open-source developer platform.. .NET | Free. Cross-platform. Open Source. [online]. Dostupné z: <https://dotnet.microsoft.com/learn/dotnet/what-is-dotnet>