**PACKETEYE 1.0**

A project report submitted for pre final year of

**Bachelor of Technology**

in

**Computer Science and Engineering**

By

P.AYYAPPA SWAMY(N120170)

P.RAMA KRISHNA(N120382)

D.VARA LAKSHMI(N120155)

K.MANI(N120642)

*Under the Supervision of*

**KUMAR ANURUPAM**



**Department of Computer Science and Engineering**

**Rajiv Gandhi University of Knowledge Technologies – Nuzvid**

**Nuzvid, Krishna – 521202**

April, 2017

**--------------------------------------------------------------------------------------------------------------------------------------**

**R rajiv Gandhi University of Knowledge Technologies**

**(A.P. Government Act 18 of 2008)**

**RGUKT-NUZVID, Krishna Dist - 521202**

Tele Fax : 08656 – 235557/235150

## CERTIFICATE OF COMPLETION

This is to certify that the work entitled, “PACKETEYE A PACKET SNIFFER**”** is the bonafied work of P. ***Ayyappa Swamy, ID No: N120170, P. Rama Krishna ,ID No: N120382, D. Vara Lakshmi, ID No: N120155, K. Mani, ID No: N120642*** carried out under my guidance and supervision for pre final year project of **Bachelor of Technology** in the department of Computer Science and Engineering under RGUKT IIIT Nuzvid. This work is done during the academic session December 2016 – April 2017, under our guidance.

­­

---------------------------- ---------------------------

**Mr. Kumar Anurupam**

Project Supervisor Head of Department

Lecturer Dept. of CSE Assistant Professor Dept. of CSE

RGUKT IIIT Nuzvid, RGUKT IIIT Nuzvid,

Nuzvid. Nuzvid.

**--------------------------------------------------------------------------------------------------------------------------------------**

**R rajiv Gandhi University of Knowledge Technologies**

**(A.P. Government Act 18 of 2008)**

**RGUKT-NUZVID, Krishna Dist - 521202**

Tele Fax : 08656 – 235557/235150

## CERTIFICATE OF EXAMINATION

This is to certify that the work entitled, “**PacketEye a packet sniffer”** is the bonafide work of ***P. Ayyappa Swamy, ID No: N120170, P. Rama Krishna, ID No: N120382, D. Vara Lakshmi, ID No: N120155, K. Mani, ID No: N120642*** *and* here by accord our approval of it as a study carried out and presented in a manner required for its acceptance in pre final year of **Bachelor of Technology** for which it has been submitted. This approval does not necessarily endorse or accept every statement made, opinion expressed or conclusion drawn, as a recorded in this thesis. It only signifies the acceptance of this thesis for the purpose for which it has been submitted.

­­

---------------------------- ---------------------------

**Mr.Kumar Anurupam Examiner**

Project SupervisorProject Examiner

Lecturer Dept. of CSE Lecturer Dept. of CSE

RGUKT IIIT Nuzvid, RGUKT IIIT Nuzvid,

Nuzvid. Nuzvid.

**--------------------------------------------------------------------------------------------------------------------------------------**

**Rrajiv Gandhi University of Knowledge Technologies**

**(A.P. Government Act 18 of 2008)**

**RGUKT-NUZVID, Krishna Dist - 521202**

Tele Fax : 08656 – 235557/235150

## DECLARATION

We, ***P.Ayyappa Swamy, ID No: N120170, P.Rama Krishna, ID No: N120382, D. Vara Lakshmi, ID No: N120155, K. Mani, ID No: N120642*** hereby declare that the project report entitle “**PacketEye a packet sniffer”** done by us under the guidance of **Mr. Kumar Anurupam M.Tech** is submitted for pre final year of **Bachelor of Technology** in **Computer Science and Engineering** the academic session December 2016 – April 2017 at RGUKT – Nuzvid.

We also declare that this project is a result of our own effort and has not been copied or imitated from any source. Citations from any websites are mentioned in the references.

The results embodied in this project report have not been submitted to any other university or institute for the award of any degree or diploma.

­­

**Date : \_\_\_\_\_\_\_\_\_\_\_\_ P. Ayyappa Swamy [N120170]**

**Place :\_\_\_\_\_\_\_\_\_ P. Rama Krishna[N120382]**

**D. Vara Lakshmi[N120155]**

**K. Mani[N120642]**

**ACKNOWLEDGEMENT**

We would like to express our profound gratitude and deep regards to my guide ***Mr. Kumar Anurupam***  for his exemplary guidance, monitoring and constant encouragement throughout the course of this thesis.

We are extremely grateful for the confidence bestowed in us and entrusting our project entitled “PacketEye a packet sniffer”.

At this juncture we feel deeply honored in expressing our sincere thanks to him for making the resources available at right time and providing valuable insights leading to the successful completion of our project.

We would like to thank RGUKT Nuzvid Director, faculty and staff for their valuable suggestions and discussions.

Last but not least I thank almighty, and I place a deep sense of gratitude to my family members and my friends who have been constant source of information during the preparation of this project work.

P. Ayyappa Swamy

P. Rama Krishna

D.Vara Lakshmi

K. Mani

**ABSTRACT**

A crucial part of the Networking course is the examination of and experimentation with network traffic data. The information running through networks is a valuable source of evidence for network administrators to fish out intruders or anomalous connections. The need to capture this information has lead to the development of packet sniffers.

This project’s intention is to develop a tool called (PacketEye) Packet Sniffer. A Packet Sniffer is a program that can monitor every packet that crosses the network. The packet sniffers which are available in the market are quite expensive and those freely available packet sniffers will consume large amount of memory. The PacketEye application is going to write in Java unlike the other sniffers that are written in C language. So it is platform-independent and consumes less memory.

It captures the packet, size of the packet, source IP address, destination IP address, source MAC address, destination MAC address, protocols (TCP,UDP,ICMP,ARP)and ports then displays it to the user. We can also store that captured information for future references.

Table of Contents

Table of Contents 7

1. Introduction 8

1.1 Purpose 8

1.2 Project Scope and Product Features 8

1.3 References 9

2. Overall Description 9

2.1 Product Perspective 9

2.2 User Classes and Characteristics 9

2.3 Operating Environment 10

2.4 Design and Implementation Constraints 10

2.5 User Documentation 12

2.6 Assumptions and Dependencies 12

3. System Features 13

3.1 Network monitoring for wired networks(Ether Net) 13

3.2 Network monitoring for wire less networks(Wifi) 13

3.3 Packet Store/Retrieve 13

3.3 Packet Filtering 13

3.4 Graphical User Interface (GUI) 13

4. External Interface Requirements 14

4.1 User Interfaces 14

4.2 Hardware Interfaces 14

4.3 Software Interfaces 14

4.4 Communications Interfaces 14

5. Other Nonfunctional Requirements 15

5.1 Performance Requirements 15

5.2 Safety Requirements 15

5.3 Security Requirements 15

5.4 Software Quality Attributes 15

Appendix A: Data Dictionary 16

# Introduction

## Purpose

Purpose of PacketEye project is to analyze ongoing traffic in a network. It will help the administrator to examine network system for any security breaches by observing the IP addresses.

## Project Scope and Product Features

PacketEye software is extensively used for protocol analysis and security. More precisely, this application can capture, decode, and display the required information that is passing through the network to the user. The information that the user can capture includes protocol, time of capture, source and destination IP, source and destination MAC, port numbers and the data. Features of this software include:

a) Network monitor for different networks (Ethernet, wifi etc)

b) Packet store/retrieve

c) Packet Filtering

d) Platform independent GUI

## References

1. Sonoo Jaiswal

http://www.javatpoint.com/java-swing

1. Keita Fujii (kfujii@uci.edu)

http://jpcap.gitspot.com/tutorial/index.html

1. ProgrammingKnowledge(Java Eclipse GUI Tutorial for beginners)

https://www.youtube.com/playlist?list=PLS1QulWo1RlbYMA5ljb72QHaHbCrPKfS2

1. Stackoverflow.com
2. O Oluwabukola, Psniffer

iisit.org/Vol10/IISITv10p389-400Oluwabukola0037.pdf

1. Goutam aurora, A simple packet sniffer by using java

gforgeek.blogspot.com/2005/04/simple-packet-sniffer-using-java.html

# Overall Description

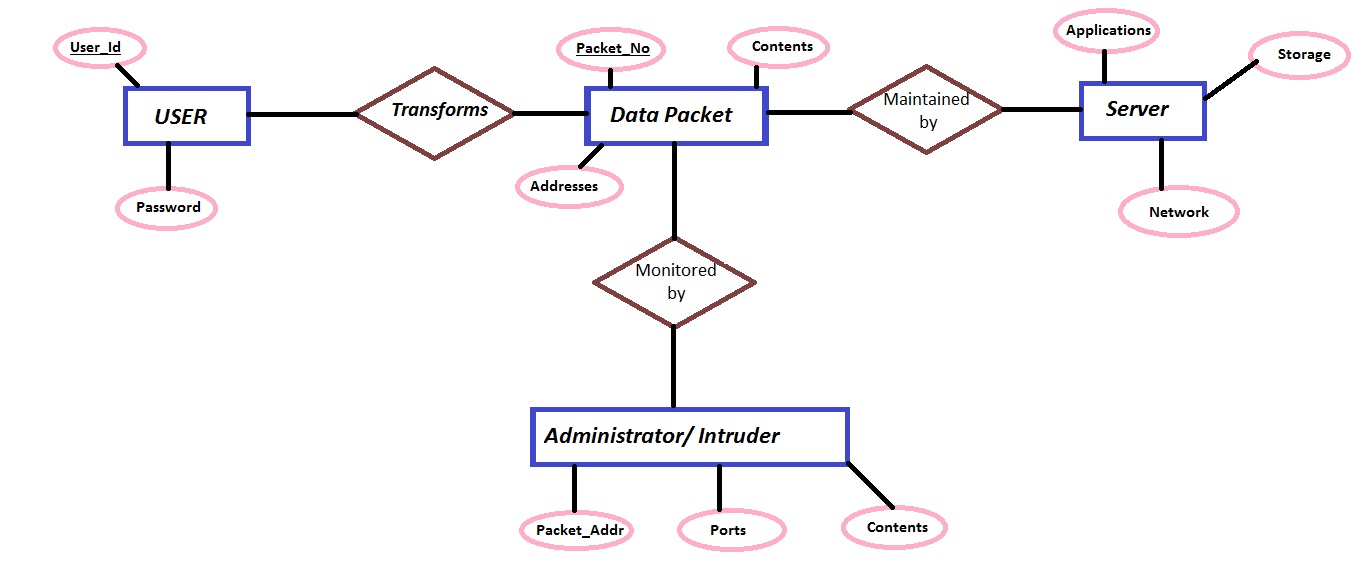
## Product Perspective

From a technical perspective, packet sniffers are the most sophisticated tools for data collection. It collects every possible bit of data that can be recorded, which creates security risks. These types of tools are very helpful to the network administrators.

## User Classes and Characteristics

|  |  |
| --- | --- |
| Sender :: | A sender is any device that sends any request or data to the receiver through the network. Whenever the data is transmitting, the data is encrypted for the security purpose. |
| Receiver :: | A sender is also a device that gives response to the devices which sent the request to that device. |
| Intruder :: | Any device or person that uses the captured information for his own evil purposes like stealing the usernames and passwords. |
| Administrator :: | Any device or person that uses the captured information to enhance the security of the network. |

## ER diagram



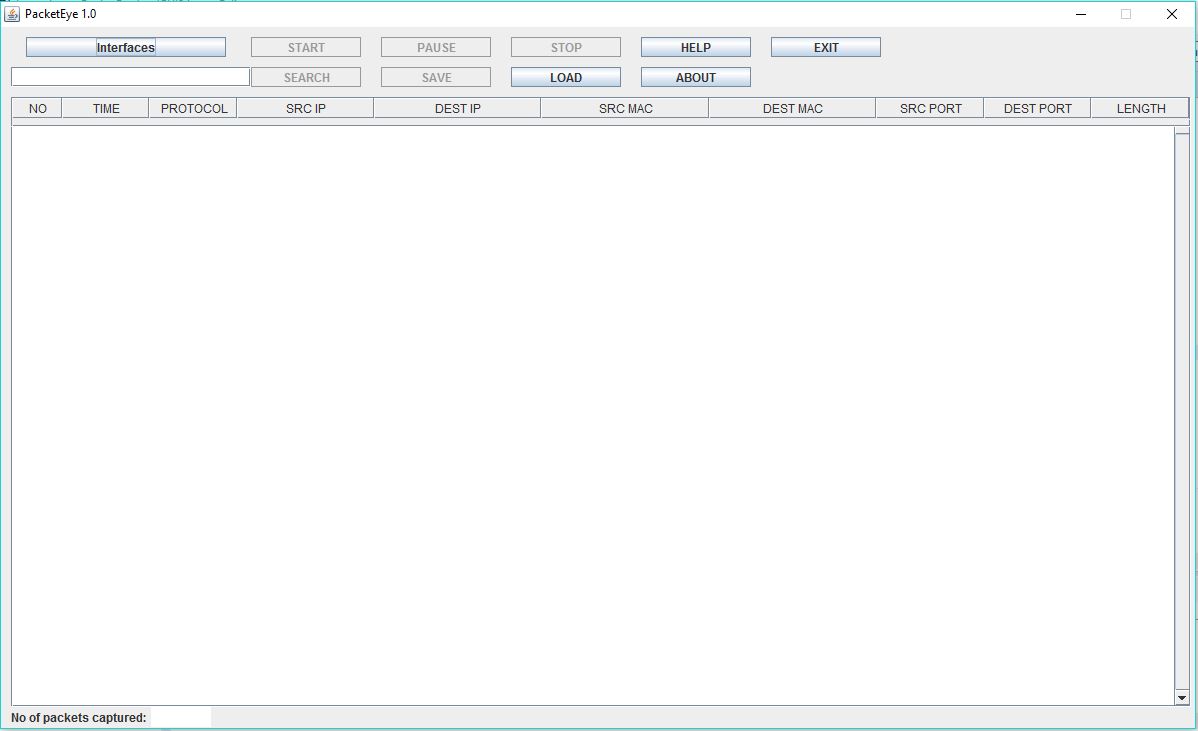
## Operating Environment

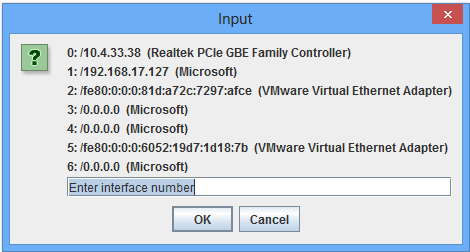
OE-1: The PacketEye application can work in any Windows operating system (Windows 7, Windows 8, etc.) in which JDK (Java Development Kit) is installed.

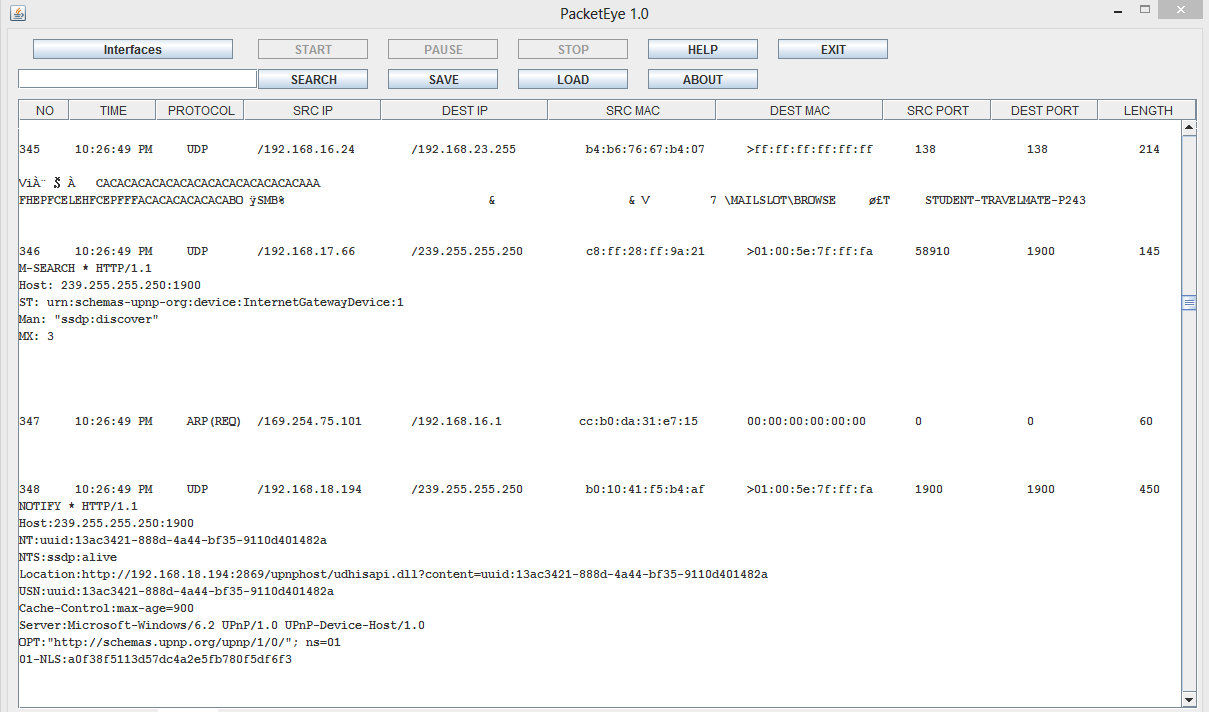
## Design and Implementation Constraints

PacketEye software captures network data as well as provides sufficient means for the decision making process of an administrator. This application designed in a new model and defined its benefits over existing packet sniffers; the model was developed in Java totally. The aim of this model is to rewrite C language sniffer models into Java, and also develop a model that consumes little memory on the hard disk. In this model we are placed packet sniffer on a network in promiscuous mode to capture and analyze all of the network traffic.

**GUI of PacketEye**







CO-1: The system comprises of some independent modules that handles different tasks efficiently using JPCAP for sniffing.

CO-2: The system will work in promiscuous mode to capture and analyze all of the network traffic.

CO-3: All the GUI components designed in Java awt and swings.

CO-4: All the back-end written by using an API called Jpcap.

CO-5: All the captured data will save in .txt format.

## User Documentation

UD: GUI will provide a ‘HELP’ button to instruct the user about PacketEye.

And also provide ‘ABOUT’ button that describes the version of PacketEye and also designers.

## Assumptions and Dependencies

AS-1: The PacketEye captures all the ongoing traffic in the network.

DP-1: In our software START button is depending on the INTERFACES (Ethernet, wifi etc).

DP-2: PAUSE, STOP, SEARCH buttons are depending on START button.

DP-3: SAVE, EXIT buttons are depending on the STOP button.

DP-4: PAUSE & RESUME are interdependent on one another.

# System Features

PacketEye is a customized application that has number of features. These features enable:

## Network Monitoring for wired networks [Ethernet]

This feature will provide the facility to capture network packets in Ethernet interface.

## Network monitoring for wireless networks [802.11]

This feature will provide the facility to capture network packets in wireless (Wi-Fi) interface.

## Packet Store/Retrieve

Packets can be stored in a TXT file and later retrieved for viewing or analysis.

We will use SAVE and LOAD buttons for this feature.

## Packet Filtering

The packets can be filtered by Protocols and Port numbers in GUI.

We use SEARCH button for this feature.

## Graphical User Interface (GUI)

Java based GUI for better user experience will be provided. It can run on any windows platforms.

# External Interface Requirements

## User Interfaces

1. Help is available for easy understanding

2. Graphical user interface is available for ease and convenience of the application

3. Most functions require mouse click thus simplifying operations

## Hardware Interfaces

1. Mouse is required for use of application.

2. Keyboard is required for use of application.

3. Monitor is required for use of application.

4. Network interface card is required to capture packets.

5. 27.3KB of hard disk space required.

## Software Interfaces

1. Jpcap V0.7
2. JDK V8 OR above
3. WinPcap V4.0 or above
4. Jpcap.dll

## Communication Interfaces

# PacketEye works on all the available interfaces of a system.

# Other non functional requirements

## Performance Requirements

1. RAM minimum 250MB required
2. CPU minimum 0.8GHz required

## Security Requirements

PacketEye software needs administrative privileges to interact with NIC.

## Software System Attributes:

### Availability

Since this system has been tested for defects and fixed, the downtime is low and therefore is available.

### Security

Security features are also provided by java.

### Maintainability

Ease of maintenance is one of the advantages of java.

### Portability

Our application is developing with java. As we all know java is portable so that out application also portable.

### Performance

Performance of this application is good on a small network. It has yet to be tested on a larger network.

### Reliability

This software has been tested and found to be reliable.

**Appendix A: Data Dictionary**

UDP = User Datagram Protocol

TCP = Transmission Control Protocol

ARP = Address Resolution Protocol

ICMP = Internet Control Message Protocol

Promiscuous mode = Promiscuous mode is a type of computer networking

Operational mode in which all network data packets can be accessed and viewed by all network adapters operating in this mode.

Protocols = Protocols are formal standards and policies comprised of

rules, procedures and formats that define communication between two or more devices over a network.

Packet = A packet is the unit of data that is routed between an origin

and a destination on the Internet or other network.

AWT = Abstract Windowing Toolkit

Network Interface = A network interface is the point of interconnection

between a computer and a private or public network.

Sniffer = Computer software or hardware that can intercept and log

traffic passing over a digital network.

Sender = a sender is a device that originates, or generates, an

information transfer to one or more receivers.

Receiver = A Receiver is a device that receives the message.

Intruder = an intruder is something that invades your computer.

Administrator = person who is monitoring all the traffic in network.

Communication = The transmission of data from one computer to another, or

from one device to another.

Port = A port is an endpoint of communication in an operating

System.

NIC = Network Interface Card.

Data = It is a form of text.

MAC Address = Physical address of a computer.

IP address = Logical address of a computer.

Ethernet = Ethernet is a physical and data link layer technology for

local area networks (LANs)