LAB REPORT

Submitted by

Anirudh Sunil Ambady [RA2011030010029]

Under the Guidance of

Dr. P. Gouthaman

Assistant Professor, Networking and Communication

Department *In partial satisfaction of the requirements for*

the degree of

BACHELOR OF TECHNOLOGY
in
COMPUTER SCIENCE ENGINEERING

with specialization in Cyber Security

SCHOOL OF COMPUTING

COLLEGE OF ENGINEERING AND TECHNOLOGY

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

KATTANKULATHUR - 603203

JUNE 2022

SRM INSTITUTION OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR-603203

BONAFIDE CERTIFICATE

Certified that this lab report titled **"Network Traffic Analyser"** is the bonafide work done by Anirudh Sunil Ambady (RA2011030010029) who carried out the lab exercises under my supervision. Certified further, that to the best of my knowledge the work reported herein does not form part of any other work.

SIGNATURE

Dr. P. Gouthaman

SEPM – Course Faculty

Assistant Professor

Department of Networking and Communications

TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO
	ABSTRACT	
	LIST OF FIGURES	
	LIST OF ABBREVIATIONS	
1	PROBLEM STATEMENT	7-10
2	STAKEHOLDERS & PROCESS MODELS	11-14
3	IDENTIFYING REQUIREMENTS	15 -17
4	PROJECT PLAN & EFFORT	18-22
5	WORK BREAKDOWN STRUCTURE & RISK ANALYSIS	23-27
6	SYSTEM ARCHITECTURE USE CASE DIAGRAM & CLASS DIAGRAM	28-31
7	ENTITY-RELATIONSHIP DIAGRAM	32-37
8	DATA FLOW DIAGRAM	38-40
9	SEQUENCE & COLLABORATION DIAGRAM	41-43
10	DEVELOPMENT OF TESTING FRAMEWORK/USER INTERFACE	44-46
11	TEST CASES & REPORTING	27-52
12	ARCHITECURAL DESIGN	53-54
	CONCLUSION	55
	REFERENCES	56
	APPENDIX	

ABSTRACT

In the growing world of digitalization and networking, ensuring Secure and reliable connections across many networks is a critical necessity in IT operations. To guarantee that the flow of data in a network fulfills various security and Quality of Service criteria, IT administrators must rely on a variety of protocols, networking practices, and network monitoring technologies. Packet sniffing is a frequent approach that helps IT administrators keep track of packets (small structured units of data) and guarantee that they are transferred smoothly. While packet sniffing is frequently linked with cyber attacks, it is widely employed for network surveillance by internet service providers, government agencies, advertisers, and even major corporations. Our project aims to capture the data transmitted in a network and analyze it to prevent cyber attacks.

LIST OF FIGURES

FIGURE NO	TITLE	PAGE NO
1	Selection Of Methodology	6
2	Work Breakdown Structure	18
3	Gantt Chart	19
4	SWOT Analysis	20
5	Use Case Diagram	21
6	Class Diagram	21
7	System Architecture	23
8	ER Diagram	29
9	DFD Level 0	34
10	DFD Level 1	34
11	Sequence Diagram	36
12	Collaboration Diagram	37
13	Sample Code of Project	48

LIST OF ABBREVIATIONS

NTA	Network Traffic Analyzer
MVP	Minimum Viable Product
IT	Information Technology
ERAT	Effort Requirement Activity Task
IR	Infrastructure Requirement
XP	Extreme Programming
GANTT	Generalized Activity Normalization Time Table
API	Application Programming Interface
UI	User Interface
SWOT	Strength, Weakness, Opportunity, Threats
RMMM	Remote Monitoring and Management
DFD	Data Flow Diagram
ER	Entity Relationship

Department of Networking and Communications

SRM IST, Kattankulathur – 603 203

Course Code: 18CSC206J

Course Name: Software Engineering and Project Management

Experiment No	1
Title of Experiment	To identify the Software Project, Create Business Case, Arrive at a Problem Statement
Name of the candidate	Anirudh Sunil Ambady
Team Members	Raghul S.A,Seshapriyan T
Register Number	RA2011030010029
Date of Experiment	10/03/2022

Mark Split Up

S.No	Description	Maximum Mark	Mark Obtained
1	Exercise	5	
2	Viva	5	
	Total	**10**	

Staff Signature with date

Aim

To Frame a project team, analyze and identify a Software project. To create a business case and Arrive at a Problem Statement for the Network Traffic Analysis.

Team Members:

S. No	Register No	Name	Role
1	RA2011030010013	SESHAPRIYAN T	**Lead/Rep**
2	RA2011030010029	ANIRUDH SUNIL AMBADY	**Member**
3	RA2011030010011	RAGHUL SA	**Member**

Project Title:

NETWORK TRAFFIC ANALYSIS

Project Description

DATE	10/03/2022
SUBMITTED BY	Team Rifters
TITLE / ROLE	Network Traffic Analysis

TEAM RIFTERS

THE PROJECT

* The practice of capturing, collecting, and logging network packets that transit through a network is known as packet sniffing.
* A packet analyzer is a computer application that can intercept and log network communication as it travels through it.
* As packets travel across the network,it helps to collect, identify, and analyse them.

THE HISTORY

Ensuring Secure and reliable connections across many networks is a critical necessity in IT operations. To guarantee that the flow of data in a network fulfills various security and Quality of Service criteria, IT administrators must rely on a variety of protocols, networking practices, and network monitoring technologies. Packet sniffing is a frequent approach that helps IT administrators keep track of packets (small structured units of data) and guarantee that they are transferred smoothly. While packet sniffing is frequently linked with cyberattacks, it is widely employed for network surveillance by internet service providers, government agencies, advertisers, and even major corporations.

LIMITATIONS

* The packet sniffer's fundamental flaw is that it can't decrypt SSL traffic without first getting the server certificate.
* Another method of intercepting the network traffic is installing a system driver on the computer where the protocol analyzer is working on.

APPROACH

* Required Network Analysing Tool (Wireshark, WINDump).
* Knowledge to do Python Programming.
* Basic Knowledge about Networking.

BENEFITS

* Detecting the Root Cause of a Network Issue
* Troubleshooting Network Issues
* Traffic Analysis
* Bandwidth Management
* Network Security and Compliance

Result

Thus, the project team formed, the project is described, the business case was prepared and the problem statement was arrived.

Department of Networking and Communications

SRM IST, Kattankulathur – 603 203

Course Code: 18CSC206J

Course Name: Software Engineering and Project Management

Experiment No	2
Title of Experiment	Identification of Process Methodology and Stakeholder Description
Name of the candidate	Anirudh Sunil Ambady
Team Members	Seshapriyan T, Raghul S.A
Register Number	RA2011030010029
Date of Experiment	24/03/2022

Mark Split Up

S.No	Description	Maximum Mark	Mark Obtained
1	Exercise	5	
2	Viva	5	
	Total	**10**	

Staff Signature with date

Aim

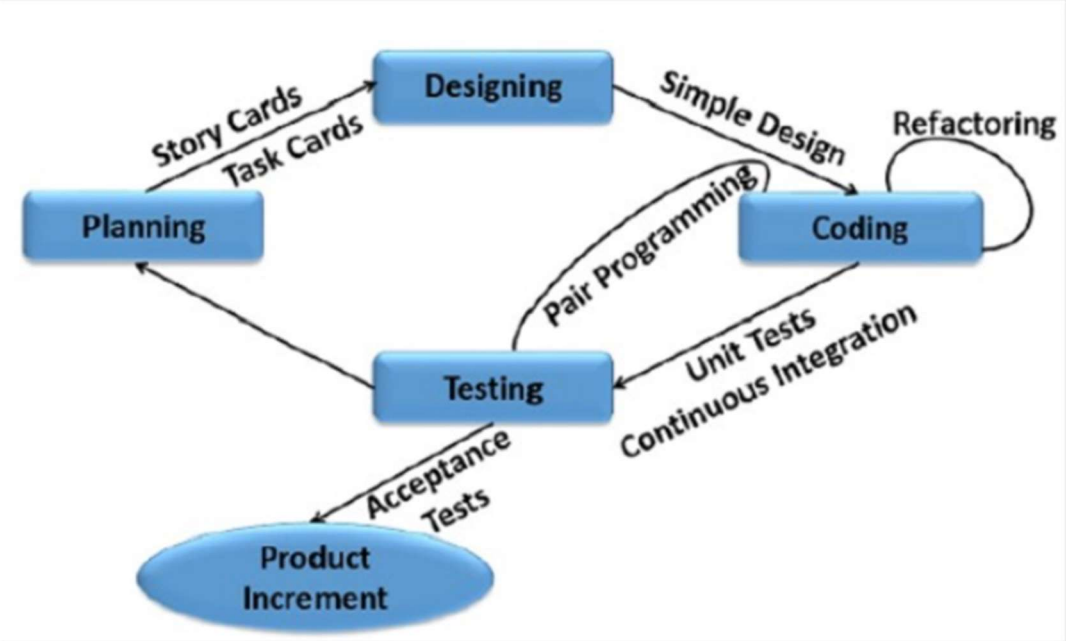
To identify the appropriate Process Model for the project and prepare Stakeholder and User Description.

Team Members:

Sl No	Register No	Name	Role
1	RA2011030010013	SESHAPRIYAN T	**Rep/Member**
2	RA2011030010011	RAGHUL SA	**Member**
3	RA2011030010029	ANIRUDH SUNIL AMBADY	**Member**

Project Title: Network Traffic Analysis

Methodology: Agile Extreme Programming (XP)



Planning:

Rather than a lengthy documents. The customer writes user stories, which define the functionality the customer would like to see, along with the business value and priority of each of those features. Some of the features are listed below,

- Identification of stakeholders and sponsors
- Infrastructure Requirements
- Security related information and gathering
- Service Level Agreements and its conditions

Design:

Simple Design is a methodology where the rule is to keep things, as the name suggests, simple. Some programmers can suggest ideas irrespective of cost and simplicity. By understanding and implementing Simple Design, and remembering the acronym, each programmer should be able to avoid costly detours and mistakes

The practice of Simple Design requires a high level of teamwork on a local basis. It does not work well remotely as it is difficult to implement in these cases. If you are wanting to adopt Simple Design, try and put the following practices into place:

- Be aware of design flaws and remedy quickly.
- Keep simple code remembering it will be easier to refactor.
- Put off some design decisions to a later date.
- Keep a backlog of design decisions and issues that can look into when the time arises.

Coding:

The concept of coding which is used in XP model is slightly different from traditional coding. Here, coding activity includes drawing diagrams (modeling) that will be transformed into code, scripting a web-based system and choosing among several alternative solutions.

In XP method the developer uses Pair Programming in which two developers' team together on one computer. The two people work together to design, code and test user stories.

Testing:

Testing is the core of extreme programming. It is the regular activity that involves both units.

Acceptance tests:

In XP the tests are written before the code creation begins. It allows the developers to write the code in accordance with the test requirements. As a result – the process of bug detection and elimination in Extreme Programming projects is very effective.

If the product is not up to the client's expectation or there are some bug in the product then the reverted back to coding phrase where the developers uses pair programming to rectify the errors and bugs.

Product Increment:

Once the product is in a ready state, the product is released the public views. Once the product is launched the maintenance department starts to maintain the product while the developers work on the updates and patch fixes for the product.

Incorporate information to below table regarding stakeholders of the project

Stakeholder Name	Activity/ Area /Phase	Interest	Influence	Priority (High/ Medium/ Low)
Owner	Obtaining objectives.	High	High	High
Programmer	Programming	High	High	Medium
Pen Tester	Testing the project	Med	Medium	Low
Project Manager	Managing	High	Medium	Medium
End User	User	Medium	Medium	Low

Result:

Thus, the Project Methodology was identified and the stakeholders were described.

Department Of Networking and Communications

SRM IST, Kattankulathur – 603 203

Course Code: 18CSC206J

Course Name: Software Engineering and Project Management

Experiment No	3
Title of Experiment	System, Functional and Non-Functional Requirements of the Project
Name of the candidate	Anirudh Sunil Ambady
Team Members	Raghul.S.A, Seshapriyan T
Register Number	RA2011030010029
Date of Experiment	29/03/2022

Mark Split Up

S.No	Description	Maximum Mark	Mark Obtained
1	Exercise	5	
2	Viva	5	
	Total	**10**	

Staff Signature with date

Aim

To identify the system, functional and non-functional requirements for the project.

Team Members:

S No	Register No	Name	Role
1	RA2011030010013	SESHAPRIYAN T	**Rep/Member**
2	RA2011030010029	ANIRUDH SUNIL AMBADY	**Member**
3	RA2011030010011	RAGHUL SA	**Member**

Project Title: Network Traffic Analysis

System Requirements

Hardware Specifications:

- Processor : 2.4 GHz Quad Core Processor
- Hard Disk : 40 GB
- RAM USAGE : 2 GB
- Network Interface Card : 64 bit PCI/ISA Ethernet or Modem

Software Specifications:

- Operating System : WINDOWS(or)LINUX
- Languages/Packages : Javascript(Front-end) / Python(Back-End)
- JavaScript version : ECMAScript 2018
- Communication Protocol : HTTP Protocol

Functional Requirements

- App Development
- System Administration
- Data Maintenance in Servers
- Ingestion of User Data

Non-Functional Requirements

- Frequent Updation of the service
- UI should be easy to use
- App Availability
- 24/7 Support

Result

Thus the requirements were identified and accordingly described.

Department of Networking and Communications

SRM IST, Kattankulathur – 603 203

Course Code: 18CSC206J

Course Name: Software Engineering and Project Management

Experiment No	4
Title of Experiment	Prepare Project Plan based on scope, Calculate Project effort based on resources and Job roles and responsibilities
Name of the candidate	Anirudh Sunil Ambady
Team Members	Seshapriyan T, Raghul.S.A
Register Number	RA2011030010029
Date of Experiment	05/04/2022

Mark Split Up

S.No	Description	Maximum Mark	Mark Obtained
1	Exercise	5	
2	Viva	5	
	Total	**10**	

Staff Signature with date

Aim:

To Prepare Project Plan based on scope, Calculate Project effort based on resources, Find Job roles and responsibilities

Team Members:

Sl No	Register No	Name	Role
1	RA2011030010013	SESHAPRIYAN T	**Lead**
2	RA2011030010011	RAGHUL SA	**Member**
3	RA2011030010029	ANIRUDH SUNIL AMBADY	**Member**

Requirements:

1. Project Management Plan

<table>
<tr><th>Focus Area</th><th>Details</th></tr>
<tr><td>Integration Management</td><td>
<table>
<tr><th>Name</th><th>Role</th></tr>
<tr><td>Seshapriyan T</td><td>Key Business User (Product Owner)</td></tr>
<tr><td>Anirudh Ambady</td><td>Project Manager</td></tr>
<tr><td>Anirudh Ambady</td><td>Business Analyst</td></tr>
<tr><td>Raghul SA</td><td>Technical Lead</td></tr>
<tr><td>Raghul SA</td><td>UX Designer</td></tr>
<tr><td>Seshapriyan T</td><td>Frontend Developer</td></tr>
<tr><td>Raghul SA & Anirudh Ambady</td><td>Backend Developer</td></tr>
<tr><td>Seshapriyan T</td><td>Tester</td></tr>
</table>
</td></tr>
<tr><td>Stakeholder</td><td>
<table>
<tr><td>Owner</td></tr>
<tr><td>Programmer</td></tr>
<tr><td>Pen Tester</td></tr>
<tr><td>Project Manager</td></tr>
<tr><td>End User</td></tr>
</table>
</td></tr>
</table>

Cost Management

Activity Description	Sub-Task	Sub-Task Description	Effort (in hours)	Cost in INR
Design the user screen	E1R1A1T1 (Effort-Requirement-Activity-Task)	Confirm the user requirements (acceptance criteria)	8	4000
	E1R1A1T2	UI Designing	45	30000
Identify Data Source for displaying units of Energy Consumption	E1R1A1T1	Go through Interface contract (Application Data Exchange) documents	20	15000
	E1R1A1T2	Strategy	2	5000

Category	Details	Qty	Cost per qty per annum	Cost per item
People	Network, System, Middleware and DB admin Developer , Support Consultant	3	2,000,000	6,000,000
License	Operating System Database Middleware IDE	10	10000	100,000
Infrastructures	Server, Storage and Network	20	20000	400,000

2. Estimation

2.1 Effort and Cost Estimation

Activity Description	Sub-Task	Sub-Task Description	Effort (in hours)	Cost in INR
Design the user screen	E1R1A1T1 (Effort-Requirement-Activity-Task)	Confirm the user requirements (acceptance criteria)	8	4000
	E1R1A1T2	UI Designing	45	30000
Identify Data Source for displaying units of Energy Consumption	E1R1A1T1	Go through Interface contract (Application Data Exchange) documents	20	15000
	E1R1A1T2	Strategy	2	5000

Effort (hr)	Cost (INR)
1	500

2.2 Infrastructure/Resource Cost [CapEx]

Infrastructure Requirement	Qty	Cost per qty	Cost per item
IR1 (PC)	n	50000	50000*n
IR2 (Server)	n	95000	95000*n
IR3 (Storage)	n	6000	6000*n

2.3 Maintenance and Support Cost [OpEx]

Category	Details	Qty	Cost per qty per annum	Cost per item
People	Network, System, Middleware and DB admin Developer , Support Consultant	3	2,000,000	6,000,000
License	Operating System Database Middleware IDE	10	10000	100,000
Infrastructures	Server, Storage and Network	20	20000	400,000

3. Project Team Formation

3.1. Identification Team members

Name	Role	Responsibilities
Seshapriyan T	Key Business User (Product Owner)	Provide clear business and user requirements
Anirudh Ambady	Project Manager	Manage the project
Anirudh Ambady	Business Analyst	Discuss and Document Requirements
Raghul SA	Technical Lead	Design the end-to-end architecture
Raghul SA	UX Designer	Design the user experience
Seshapriyan T	Frontend Developer	Develop user interface
Raghul SA & Anirudh Ambady	Backend Developer	Design, Develop and Unit Test Services/API/DB
Seshapriyan T	Tester	Define Test Cases and Perform Testing

3.2. Responsibility Assignment Matrix

RACI Matrix	Team Members			
Activity	**Name (BA)**	**Name (Developer)**	**Name (Project Manager)**	**Key Business User**
User Requirement Documentation	A	C/I	I	R
1	Seshapriyan T	All the members	Anirudh Ambady	Raghul SA

A	Accountable
R	Responsible
C	Consult
I	Inform

Result:

Thus, the Project Plan was documented successfully.

Department of Networking and Communications

SRM IST, Kattankulathur – 603 203

Course Code: 18CSC206J

Course Name: Software Engineering and Project Management

Experiment No	5
Title of Experiment	Prepare Work breakdown structure, Timeline chart, Risk identification table
Name of the candidate	Anirudh Sunil Ambady
Team Members	Seshapriyan T, Raghul.S.A
Register Number	RA2011030010029
Date of Experiment	12/04/2022

Mark Split Up

S.No	Description	Maximum Mark	Mark Obtained
1	Exercise	5	
2	Viva	5	
	Total	**10**	

Staff Signature with date

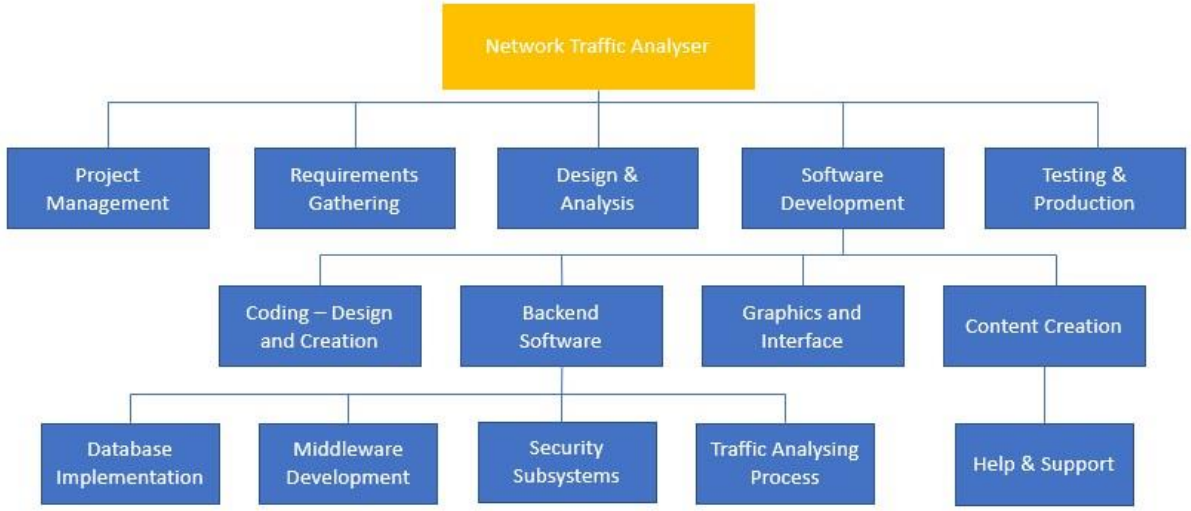
Aim

To Prepare Work breakdown structure, Timeline chart and Risk identification table

Team Members:

Sl No	Register No	Name	Role
1	RA2011030010013	Seshapriyan T	**Rep**
2	RA2011030010011	Raghul SA	**Member**
3	RA2011030010029	Anirudh Ambady	**Member**

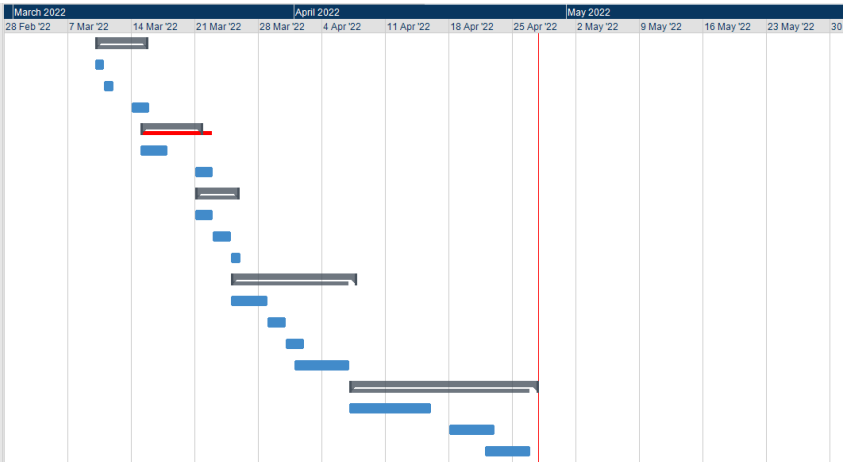
WBS



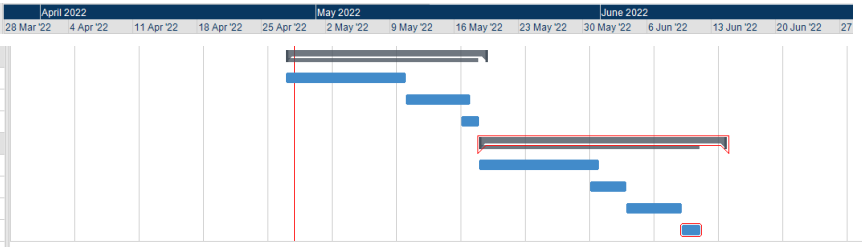
- 1.0 Project Management
- 2.0 Requirements Gathering
- 3.0 Analysis & Design
- 4.0 Software Development
    - 4.1 Coding Design and Creation
    - 4.2 Backend Software
        - 4.2.1 Database Implementation
        - 4.2.2 Middleware Development
        - 4.2.3 Security Subsystems
        - 4.2.4 Traffic Analyzing Process
    - 4.3 Graphics and Interface
    - 4.4 Content Creation
        - 4.4.1 Help & Support
- 5.0 Testing and Production

TIMELINE – GANTT CHART

	Tas...	Task Name	Duration	Start	End
1		**Initial Stage**	**4 days**	**10-03-2022**	**15-03-2022**
2		Recognizing the objectives	1 day	10-03-2022	10-03-2022
3		Identification of the approach	1 day	11-03-2022	11-03-2022
4		Project Approach	2 days	14-03-2022	15-03-2022
5		**Methods**	**5 days**	**15-03-2022**	**21-03-2022**
6		Choosing method	3 days	15-03-2022	17-03-2022
7		Identification of stakeholders	2 days	21-03-2022	22-03-2022
8		**Requirements**	**5 days**	**21-03-2022**	**25-03-2022**
9		System Requirements	2 days	21-03-2022	22-03-2022
10		Functional Requirements	2 days	23-03-2022	24-03-2022
11		Non-Functional Requirements	1 day	25-03-2022	25-03-2022
12		**Project Management**	**10 days**	**25-03-2022**	**07-04-2022**
13		Planning	2 days	25-03-2022	28-03-2022
14		Estimation of Cost	2 days	29-03-2022	30-03-2022
15		Risk Analysis	2 days	31-03-2022	01-04-2022
16		Project Timeline Review	4 days	01-04-2022	06-04-2022
17		**Designing**	**15 days**	**07-04-2022**	**27-04-2022**
18		Designing the UI	7 days	07-04-2022	15-04-2022
19		Designing the Network Information Page	5 days	18-04-2022	22-04-2022
20		Designing the other basic stuffs	3 days	22-04-2022	26-04-2022

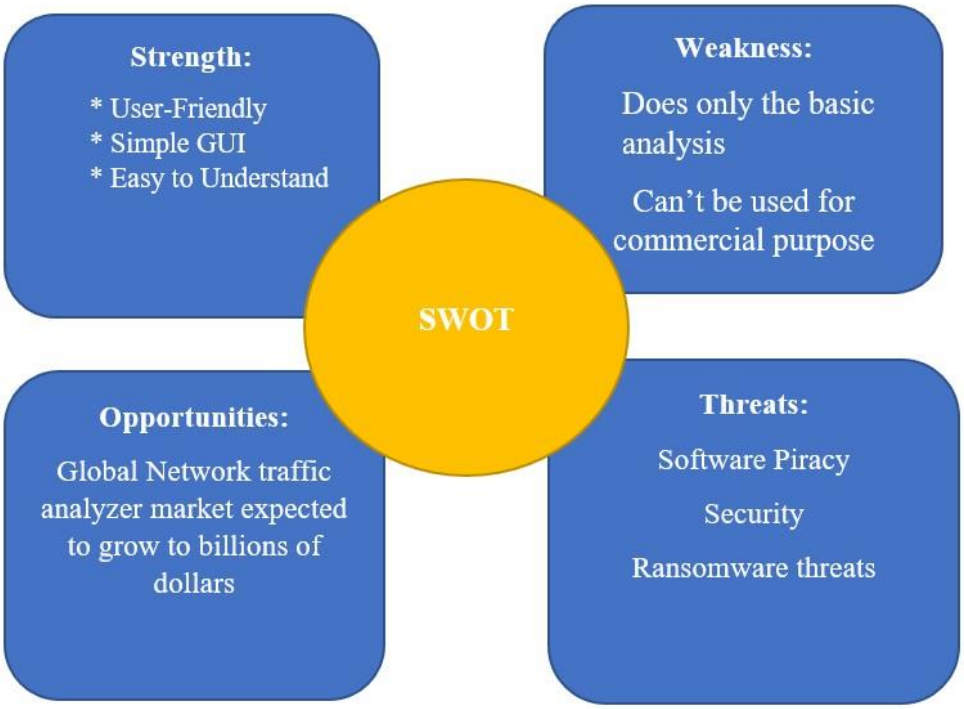


	Tas...	Task Name	Duration	Start	End
21		**Coding and Implementation**	**16 days**	**27-04-2022**	**18-05-2022**
22		Developing the base code	9 days	27-04-2022	09-05-2022
23		Developing the user interface	5 days	10-05-2022	16-05-2022
24		Reviewing and finalizing	2 days	16-05-2022	17-05-2022
25		**Back End**	**19 days**	**18-05-2022**	**13-06-2022**
26		Developing basic functions	9 days	18-05-2022	30-05-2022
27		Developing tools for users (Making as Easy to use Tool)	4 days	30-05-2022	02-06-2022
28		Model Implementation	4 days	03-06-2022	08-06-2022
29		Reviewing and ready for the next phase (Testing)	2 days	09-06-2022	10-06-2022



RISK ANALYSIS – SWOT & RMMM

SWOT:



RMMM:

RESPONSE	STRATEGY	EXAMPLES
AVOID	Risk avoidance is a strategy where the project team takes action to remove the risk or protect from the impact	• Extending the schedule • Reducing/removing scope • Change the execution strategy
TRANSFER	Risk transference involves shifting or transferring the risk threat and impact the third party, Rather transfers the responsibility and ownership	● Purchasing insurance ● Performance bonds ● Warranties ● Contact issuance
MITIGATE	Risk migration is a strategy where the project team takes action to reduce the probability of the risk occurring. This does not risk or potential impact, but rather reduces the likelihood of it becoming real.	● Increasing testing ● Changning suppliers to a more stable one ● Reducing process complexity
ACCEPT	Risk acceptance means the team acknowledges the risk and its potential impact but decides not to take any preemptive action to prevent it. It is dealt with only if it occur	● Contingency reserve budgets ● Management schedule float ● Event contingency

Result:

Thus, the work breakdown structure with timeline chart and risk table were formulated successfully.

School of Computing

SRM IST, Kattankulathur – 603 203

Course Code: 18CSC206J

Course Name: Software Engineering and Project Management

Experiment No	6
Title of Experiment	Design a System Architecture, Use Case and Class Diagram
Name of the candidate	Anirudh Sunil Ambady
Team Members	Seshapriyan T, Raghul.S.A
Register Number	RA2011030010029
Date of Experiment	21/04/2022

Mark Split Up

S.No	Description	Maximum Mark	Mark Obtained
1	Exercise	5	
2	Viva	5	
	Total	**10**	

Staff Signature with date

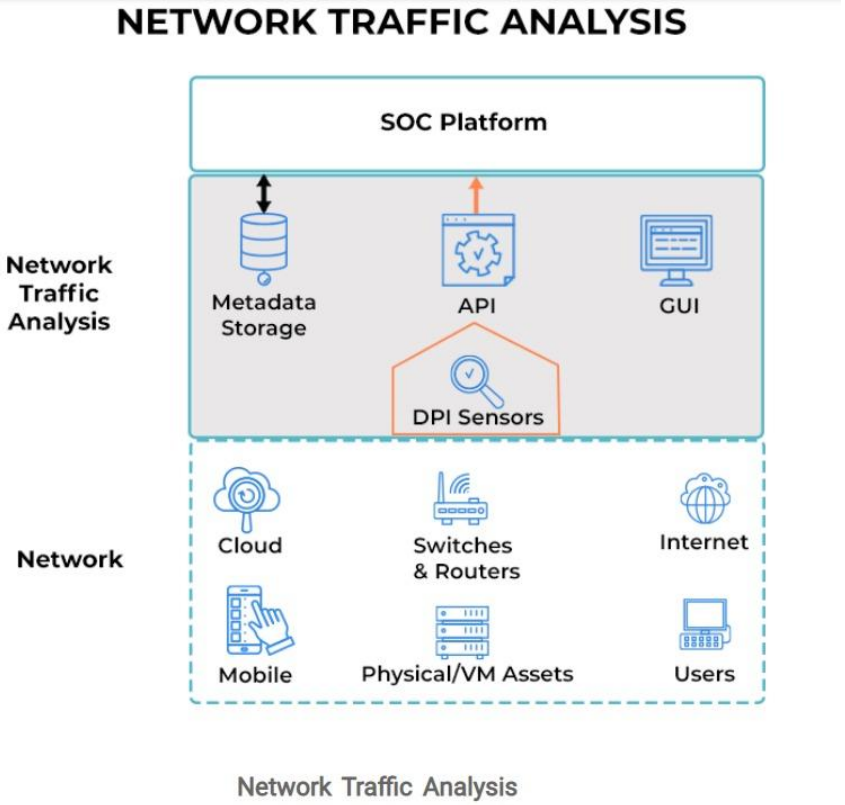
Aim

To Design a System Architecture, Use case and Class Diagram

Team Members:

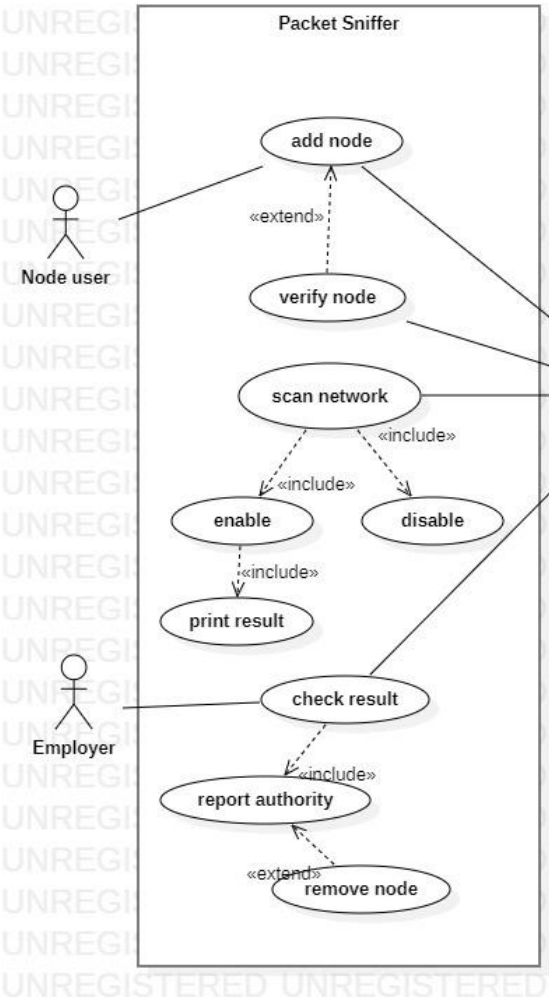
Sl No	Register No	Name	Role
1	RA2011030010013	SESHAPRIYAN T	**Rep**
2	RA2011030010011	RAGHUL SA	**Member**
3	RA2011030010029	ANIRUDH SUNIL AMBADY	**Member**

SYSTEM ARCHITECTURE

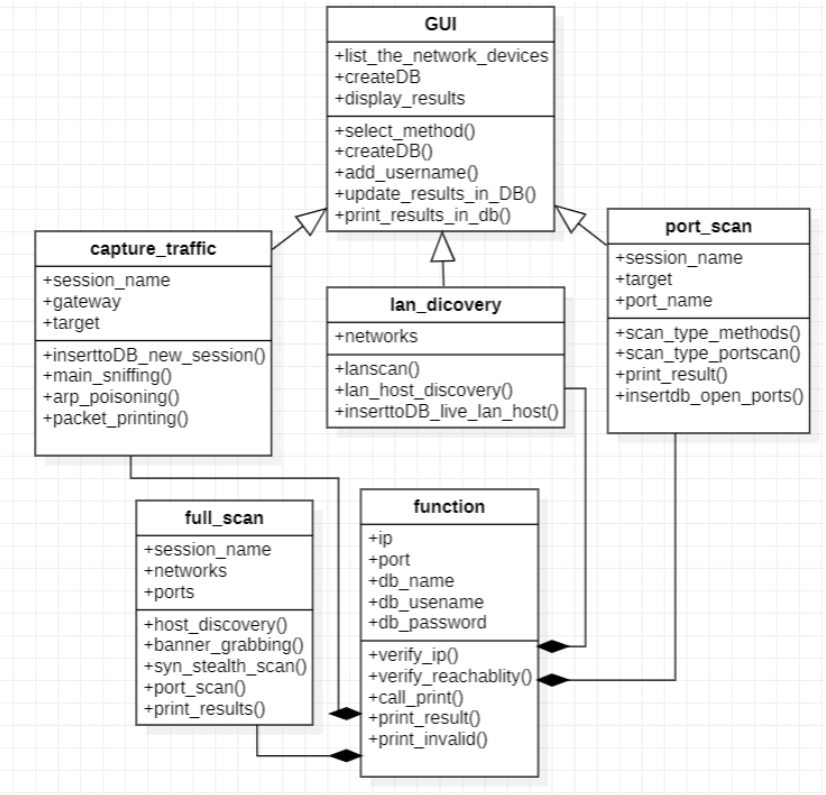


Network Traffic Analysis

USE CASE DIAGRAM



CLASS DIAGRAM



Result:

Thus, the system architecture, use case and class diagram created successfully.

School of Computing

SRM IST, Kattankulathur – 603 203

Course Code: 18CSC206J

Course Name: Software Engineering and Project Management

Experiment No	7
Title of Experiment	Design a Entity relationship diagram
Name of the candidate	Anirudh Sunil Ambady
Team Members	Seshapriyan T, Raghul.S.A
Register Number	RA2011030010029
Date of Experiment	28/04/2022

Mark Split Up

S. No	Description	Maximum Mark	Mark Obtained
1	Exercise	5	
2	Viva	5	
	Total	**10**	

Staff Signature with date

Aim

To create the Entity Relationship Diagram

Team Members:

S No	Register No	Name	Role
1	SESHAPRIYAN T	RA2011030010013	Rep
2	ANIRUDH SUNIL AMBADY	RA2011030010029	Member
3	RAGHUL SA	RA2011030010011	Member

ER Diagram, Notation and Example

What is ER Diagram?

- ER Diagram stands for Entity Relationship Diagram, also known as ERD is a diagram that displays the relationship of entity sets stored in a database. In other words, ER diagrams help to explain the logical structure of databases. ER diagrams are created based on three basic concepts: entities, attributes and relationships.
- ER Diagrams contain different symbols that use rectangles to represent entities, ovals to define attributes and diamond shapes to represent relationships.
- At first look, an ER diagram looks very similar to the flowchart. However, ER Diagram includes many specialized symbols, and its meanings make this model unique. The purpose of ER Diagram is to represent the entity framework infrastructure.

What is ER Model?

- ER Model stands for Entity Relationship Model is a high-level conceptual data model diagram. ER model helps to systematically analyze data requirements to produce a well-designed database.
- ER Model represents real-world entities and the relationships between them. Creating an ER Model in DBMS is considered as a best practice before implementing your database.
- ER Modeling helps you to analyze data requirements systematically to produce a well-designed database. So, it is considered a best practice to complete ER modeling before implementing your database.

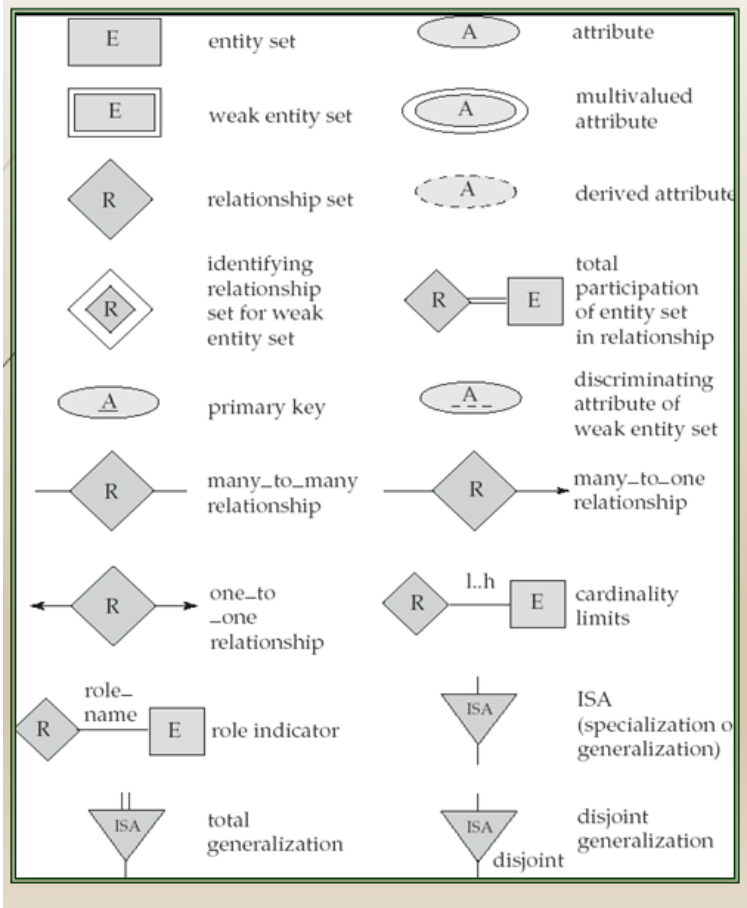
Why use ER Diagrams?

Here, are prime reasons for using the ER Diagram

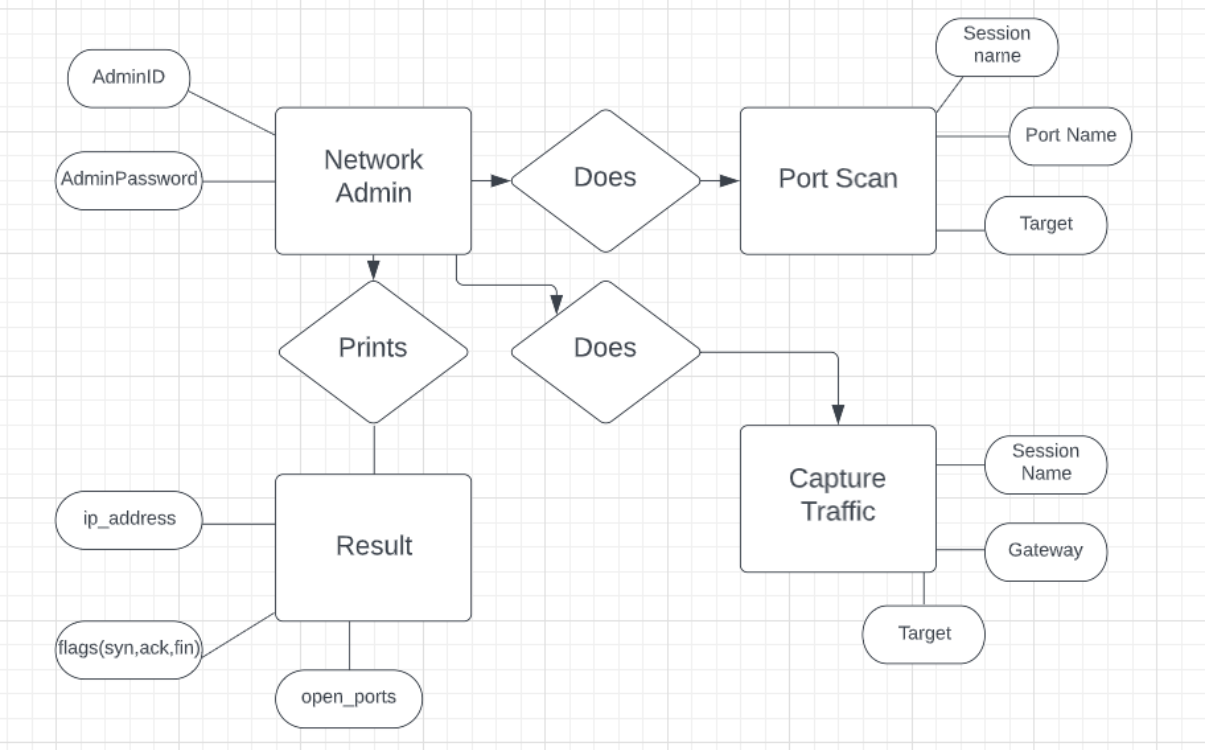
- Helps you to define terms related to entity relationship modeling
- Provide a preview of how all your tables should connect, what fields are going to be on each table
- Helps to describe entities, attributes, relationships
- ER diagrams are translatable into relational tables which allows you to build databases quickly
- ER diagrams can be used by database designers as a blueprint for implementing data in specific software applications
- The database designer gains a better understanding of the information to be contained in the database with the help of ERP diagram
- ERD Diagram allows you to communicate with the logical structure of the database to users

Components of the ER Diagram
This model is based on three basic concepts: Entities, Attributes, Relationships

ER Diagram – Notations
- Rectangles represent entity sets.
- Diamonds represent relationship sets.
- Lines link attributes to entity sets and entity sets to relationship sets.
- Ellipses represent attributes
- Double ellipses represent multivalued attributes.
- Dashed ellipses denote derived attributes.
- Underline indicates primary key attributes



ER Diagram of Packet Sniffing



ADDITIONAL NOTES

- A database can be modeled as a collection of entities, relationship among entities.
- An entity is an object that exists and is distinguishable from other objects.
Example: specific person, company, event, plant
- Entities have attributes.
Example: people have names and addresses
- An entity set is a set of entities of the same type that share the same properties.
Example: set of all persons, companies, trees, holidays

- Express the number of entities to which another entity can be associated via a relationship set.
- Most useful in describing binary relationship sets.
- We express cardinality constraints by drawing either a directed line (->), signifying "one," or an undirected line (—), signifying "many," between the relationship set and the entity set.

- An entity is represented by a set of attributes, that is descriptive properties possessed by all members of an entity set.
Example: customer = (customer-id, customer-name, customer-street, customer-city)
loan = (loan-number, amount)
- Domain – the set of permitted values for each attribute
- Attribute types:
1. Simple and composite attributes.

2. Single-valued and multi-valued attributes
E.g., multivalued attribute: phone-numbers
3. Derived Attributes-Can be computed from other attributes
E.g. age, given date of birth

Cardinality
- For a binary relationship set the mapping cardinality must be one of the following types:
1. One to one
A customer is associated with at most one loan via the relationship borrower. A loan is associated with at most one customer via borrower
2. One to many
A loan is associated with at most one customer via borrower, a customer is associated with several (including 0) loans via borrower
3. Many to one
A loan is associated with several (including 0) customers via borrower, a customer is associated with at most one loan via borrower
4. Many to many
A loan is associated with several (including 0) customers via borrower, a customer is associated with several loans (including 0) via borrower

Weak Entity Set
- An entity set that does not have a primary key is referred to as a weak entity set and represented by double outlined box in E-R diagram.
Example: Consider the entity set payment which got three attributes: payment number, payment date and payment amount. Payment numbers are sequential starting from 1 generally separately for each loan. Although each payment entity is distinct, payments for different loans may share the same payment number. Thus, this entity set does not have a primary key.

Discriminator
- The discriminator (or partial key) of a weak entity set is the set of attributes that distinguishes among all the entities of a weak entity set
Example: discriminator of weak entity set payment is the attribute payment number since for each loan a payment number uniquely identifies one single payment for that loan.

Specialization-Generalization-ISA
- E-R model provides means of representing these distinctive entity groupings
- Process of designating subgroupings within an entity set is called specialization depicted by triangle component labelled ISA ("is a")
- Bottom-up design process in which multiple entity sets are synthesized into higher level entity set - Generalization
- ISA relationship may also be referred to as superclass-subclass relationship
- Higher and lower-level entity sets are designated by the term's superclass and subclass.
- Specialization and generalization are simple inversions of each other; they are represented in an E-R diagram in the same way.

Total & Partial Participation
- Total participation (indicated by double line): every entity in the entity set participates in at least one relationship in the relationship set

E.g., participation of loan in borrower is total, every loan must have a customer associated to it via borrower
- Partial participation: some entities may not participate in any relationship in the relationship set
Example: participation of customer in borrower is partial

Cardinality limits
- Cardinality limits can also express participation constraints
- Minimum and maximum cardinality is expressed as lb. where l is the minimum and h is the maximum cardinality
- Minimum value of 1 indicates total participation of entity set in relationship set
- Maximum value of 1 indicates entity participates in almost one relationship set.
- Maximum value of * indicates no limit

Role indicator
- Entity sets of a relationship need not be distinct
- The labels “manager” and “worker” are called roles; they specify how employee entities interact via the works-for relationship set.
- Roles are indicated in E-R diagrams by labeling the lines that connect diamonds to rectangles.
- Role labels are optional, and are used to clarify semantics of the relationship

Disjoint Generalization
- Disjoint Ness constraint requires that an entity belong to more than one lower-level entity set.
Example: account entity can satisfy only one condition for account type attribute; entity can either be savings or chairing account but not both.

Result:

Thus, the entity relationship diagram was created successfully.

School of Computing

SRM IST, Kattankulathur – 603 203

Course Code: 18CSC206J

Course Name: Software Engineering and Project Management

Experiment No	8
Title of Experiment	Develop a Data Flow Diagram (Process-Up to Level 1)
Name of the candidate	Anirudh Sunil Ambady
Team Members	Seshapriyan T, Raghul.S.A
Register Number	RA2011030010029
Date of Experiment	13/05/2022

Mark Split Up

S. No	Description	Maximum Mark	Mark Obtained
1	Exercise	5	
2	Viva	5	
	Total	**10**	

Staff Signature with date

Aim

To develop the data flow diagram up to level 1 for the network traffic analyser

Team Members:

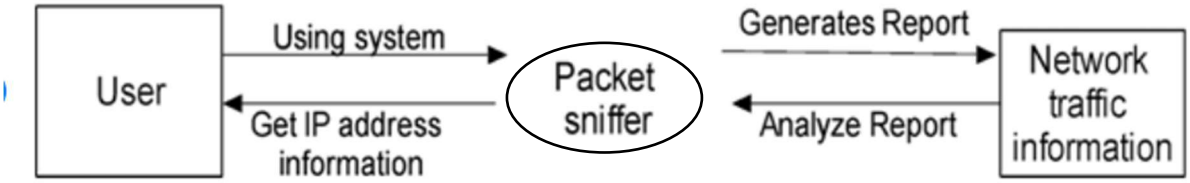
S No	Register No	Name	Role
1	RA2011030010013	Seshapriyan.T	Rep
2	RA2011030010029	Anirudh Sunil Ambady	Member
3	RA2011030010011	Raghul.S.A	Member

Data Flow Diagram

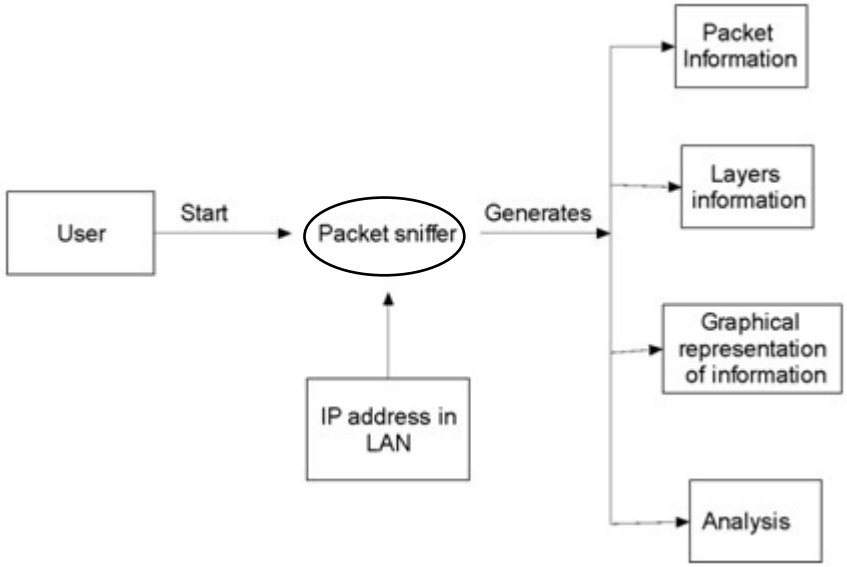
The DFD takes an input-process-output view of a system. That is, data objects flow into the software, are transformed by processing elements, and resultant data objects flow out of the software. Data objects are represented by labeled arrows, and transformations are represented by circles (also called bubbles). The DFD is presented in a hierarchical fashion. That is, the first data flow model (sometimes called a level 0 DFD or context diagram) represents the system as a whole. Subsequent data flow diagrams refine the context diagram, providing increasing detail with each subsequent level.

The data flow diagram enables you to develop models of the information domain and functional domain. As the DFD is refined into greater levels of detail, you perform an implicit functional decomposition of the system. At the same time, the DFD refinement results in a corresponding refinement of data as it moves through the processes that embody the application.
A few simple guidelines can aid immeasurably during the derivation of a data flow diagram:
(1) Level 0 data flow diagram should depict the software/system as a
single bubble;
(2) Primary input and output should be carefully noted;
(3) Refinement should begin by isolating candidate processes, data objects, and data stores to be represented at the next level;
(4) All arrows and bubbles should be labeled with meaningful names;
(5) Information flow continuity must be maintained from level to level and
(6) One bubble at a time should be refined. There is a natural tendency to overcomplicate the data flow diagram. This occurs when you attempt to show too much detail too early or represent procedural aspects of the software in lieu of information flow.

DFD Level 0



DFD Level 1



Result:

Thus, the data flow diagrams have been created for the network traffic analyzer.

School of Computing

SRM IST, Kattankulathur – 603 203

Course Code: 18CSC206J

Course Name: Software Engineering and Project Management

Experiment No	9
Title of Experiment	Design a Sequence and Collaboration Diagram
Name of the candidate	Anirudh Sunil Ambady
Team Members	Raghul.S.A ,Seshapriyan T
Register Number	RA2011030010029
Date of Experiment	24/05/2022

Mark Split Up

S. No	Description	Maximum Mark	Mark Obtained
1	Exercise	5	
2	Viva	5	
	Total	**10**	

Staff Signature with date

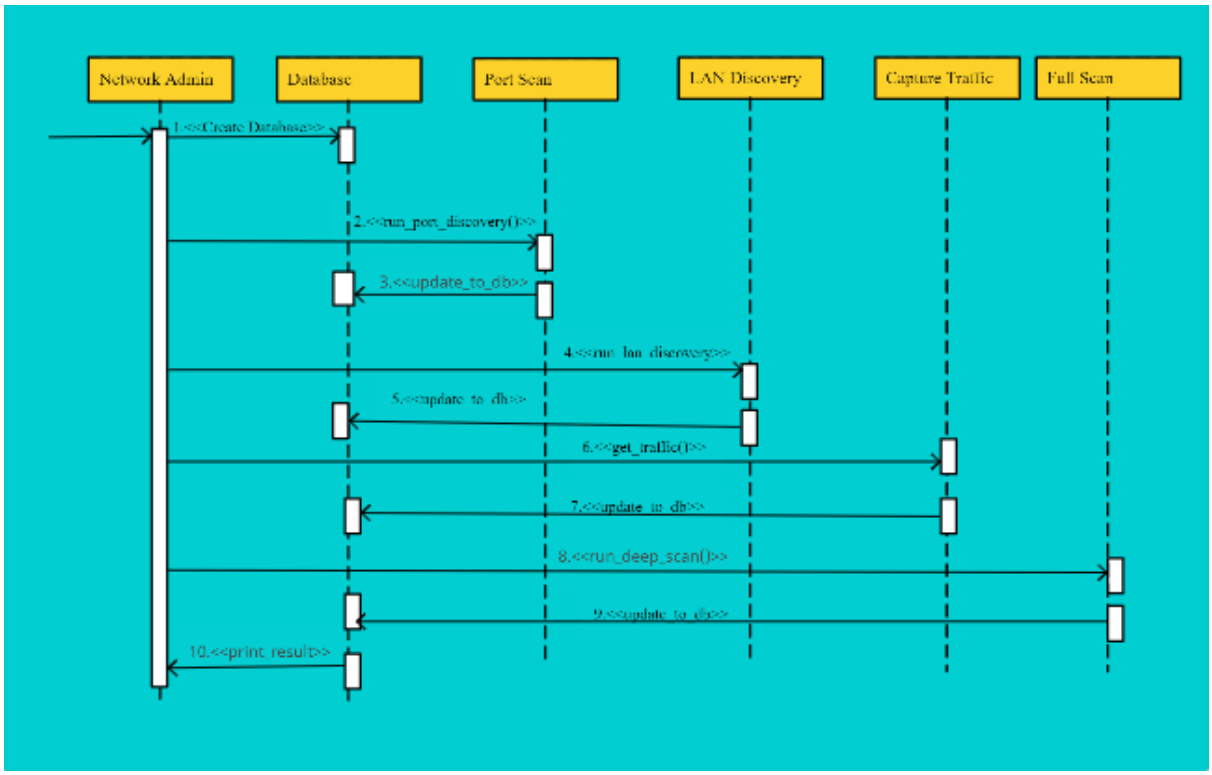
Aim

To create the sequence and collaboration diagram for the Network Traffic Analyzer

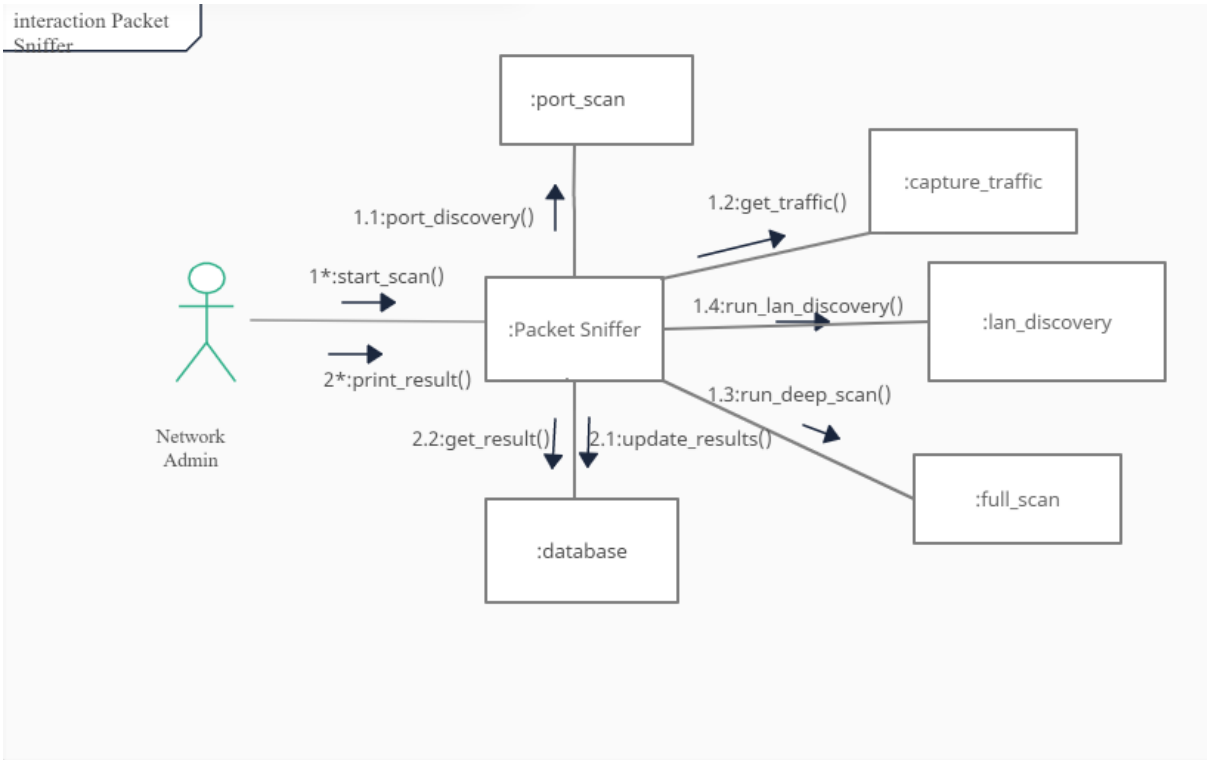
Team Members:

S No	Register No	Name	Role
1	RA2011030010013	SESHAPRIYAN T	Rep/Member
2	RA2011030010029	ANIRUDH SUNIL AMBADY	Member
3	RA2011030010011	RAGHUL.S.A	Member

Sequence Diagram



Collaboration Diagram:



Result:

Thus, the sequence and collaboration diagrams were created for the Network traffic analyzer.

School of Computing

SRM IST, Kattankulathur – 603 203

Course Code: 18CSC206J

Course Name: Software Engineering and Project Management

Experiment No	10
Title of Experiment	Develop a Testing Framework/User Interface
Name of the candidate	Anirudh Sunil Ambady
Team Members	Seshapriyan T, Raghul.S.A
Register Number	RA2011030010029
Date of Experiment	03/06/2022

Mark Split Up

S. No	Description	Maximum Mark	Mark Obtained
1	Exercise	5	
2	Viva	5	
	Total	**10**	

Staff Signature with date

Aim

To develop the testing framework and/or user interface framework for the Network Traffic Analyzer.

Team Members:

S No	Register No	Name	Role
1	**RA2011030010013**	**SESHAPRIYAN T**	**Rep/Member**
2	**RA2011030010029**	**ANIRUDH SUNIL AMBADY**	**Member**
3	**RA2011030010011**	**RAGHUL SA**	**Member**

Executive Summary

Testing Framework:

- Accuracy
- Efficiency

Test Plan

Accuracy: Does the NTA fail to detect any malware passed across the network?

Efficiency: Does the NTA fail to note down any packets transmitted between nodes on the network?

Scope of Testing

Accuracy: Ensure that the NTA analyzes and recognizes all malware that can get passed through the network to prevent being transmitted across the network and responsible nodes affected be isolated.

Efficiency: No packets transmitted across the network are missed out on and all information is gathered.

Functional:

TEST AREA	INPUT	TESTING METHOD	TOOLS
Login Module (Net Admin)	Login Username and Password	Manual	Security Infrastructure (SIN)
Port Scan	-	Automated Tools	Nmap
LAN Discovery	-	Automated Tools	Nmap
Full Scan	-	Automated Tools	Nmap
Capture Traffic	-	Automated Tools	Wireshark

Non-Functional:

TEST AREA	TESTING METHOD	TOOLS
Security	Automated Tools	ZAP, Wfuss
Performance	Automated or Manual	LoadUI Pro, WebLoad
Compatibility	Automated Tools	Lambda Test, Experitest
Accessibility	Automated Tools	AChecker, AATT

Types of Testing, Methodology, Tools

CATEGORY	METHODOLOGY	TOOLS REQUIRED
Functional Requirements	Manual	Word Template
UAT	Operational Acceptance Testing	Rally Software
Security	Agile Security Testing	ZAP

Result:

Thus, the testing framework/user interface framework has been created for the Network Traffic Analyzer.

SRM INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

School of Computing

SRM IST, Kattankulathur – 603 203

Course Code: 18CSC206J

Course Name: Software Engineering and Project Management

Experiment No	11
Title of Experiment	Test Cases & Manual Test Case Reporting
Name of the candidate	Anirudh Sunil Ambady
Team Members	Seshapriyan T, Raghul.S.A
Register Number	RA2011030010029
Date of Experiment	06/06/2022

Mark Split Up

S. No	Description	Maximum Mark	Mark Obtained
1	Exercise	5	
2	Viva	5	
	Total	**10**	

Staff Signature with date

Aim

To develop the test cases manual and to prepare the manual test case report for the Network Traffic Analyzer.

Team Members:

S No	Register No	Name	Role
1	**RA201130010013**	SESHAPRIYAN T	**Rep**
2	**RA201130010011**	RAGHUL SA	**Member**
3	**RA201130010029**	ANIRUDH SUNIL AMBADY	**Member**

Test Case

Functional Test Cases

Test ID (#)	Test Scenario	Test Case	Execution Steps	Expected Outcome	Actual Outcome	Status	Remarks
	Verify Admin Registration	Register user for software access.	1. Enter Registration details into the text box. 2. Click on Submit.	User details must be registered into software database for login verification		In-Progress	
	Verify Admin Login	Approval of software access to registered admin	1. Enter the login details in the text box 2. Click Login button	User should be taken to the next page for accessing software		In-Progress	
	Verify Admin Login	Don't Accept Non Admin Logins	1. Enter random login details in the text box.	User should be denied access to software		In-Progress	

	Verify LAN Discovery(	Software must be abl to recognize the LANs present in the connected network.	1. Enable LAN Discov ry option	Presence of LANs must be displayed and addec to database		In-Progress	
	Verify Port Scan	Software must detect number of ports in a network	1. Enable Port Scan	The number of ports present in a network active one must be displayed and registered to the database.		In-Progress	
	Verify Capture Traffic	Software must start t capture packets distributed across the network.	1. Choose Capture Traffic option 2. Click on “Start”	The packets distributed in the network must be displayed along with source and destination IP Address, time duration of transmissio n,		In-Progress	
	Verify Full Scan	Software must be able to check packets distributed along the network for malwares and other viruses.	1. Enable Deep Scan.	Software must scan packets transmitte d across the network for malware, stop transmissio n and isolate sender		In-Progress	

Non-Functional Test Cases

Test ID (#)	Test Scenario	Test Case	Execution Steps	Expected Outcome	Actual Outcome	Status	Remarks
	Compatibility Testing	Software must be installable on all versions of Windows, Mac and Linux	1. Click on Download option of software 2. Run setup file	Setup file runs and the OS supports the type of file.		In-Progress	
	Performance Testing	Response time on all functions must be significantly low	1. Choose the available options in the software	The response time for function to begin and load in the data must be very fast		In-Progress	
	Stress Testing	All data must be captured when the scan functions are enabled	1. Large amounts of data is to be transmitted from all nodes in network but within limits	The scan functions must not miss out any packets that were transmitted		In-Progress	

Category	Progress Against Plan	Status
Functional Testing	Amber	In-Progress
Non-Functional Testing	Amber	In-Progress

Functional	Test Case Coverage (%)	Status
Admin login	9%	Completed
User ID	9%	Completed
Lan discovery	6%	In-Progress
Port scan	7%	In-Progress
Capture traffic	8%	In-Progress
Full scan	6%	In-Progress
Display result	4%	In-Progress

Result:

Thus, the test case manual and test case report has been created for the Network Traffic Analyzer.

SRM INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

School of Computing

SRM IST, Kattankulathur – 603 203

Course Code: 18CSC206J

Course Name: Software Engineering and Project Management

Experiment No	12
Title of Experiment	Provide the details of Architecture Design/Framework/Implementation
Name of the candidate	Anirudh Sunil Ambady
Team Members	Seshapriyan T, Raghul.S.A
Register Numbers	RA2011030010029
Date of Experiment	13/06/2022

Mark Split Up

S. No	Description	Maximum Mark	Mark Obtained
1	Exercise	5	
2	Viva	5	
	Total	**10**	

Staff Signature with date

Aim

To provide the details of architectural design/framework/implementation

Team Members:

S No	Register No	Name	Role
1	RA2011030010013	SESHAPRIYAN T	Rep/Member
2	RA2011030010011	RAGHUL SA	Member
3	RA2011030010029	ANIRUDH SUNIL AMBADY	Member

Sample Source Code:

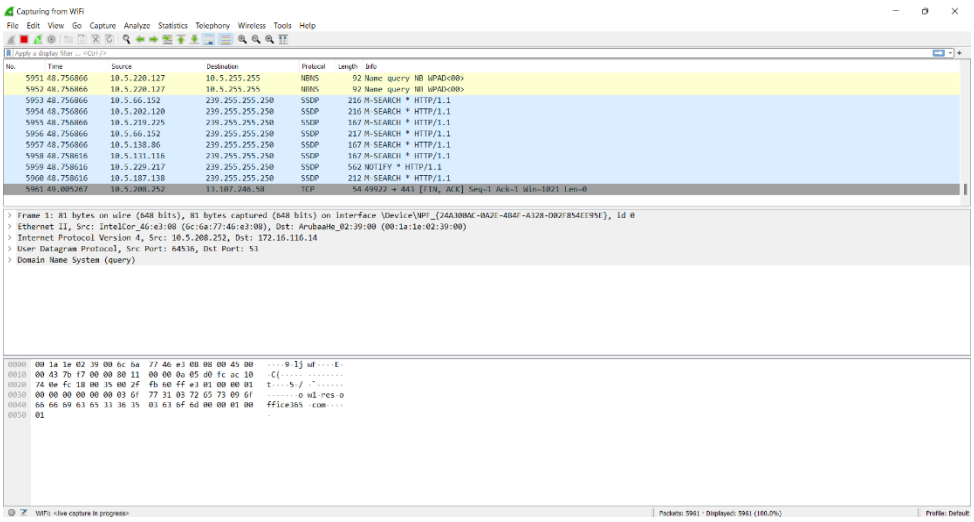
```
import dpkt
import socket

def printPcap(pcap):
    for (ts,buf) in pcap:
        try:
            eth = dpkt.ethernet.Ethernet(buf)
            ip = eth.data
            # read the source IP in src
            src = socket.inet_ntoa(ip.src)
            # read the destination IP in dst
            dst = socket.inet_ntoa(ip.dst)

            # Print the source and destination IP
            print 'Source: ' +src+ ' Destination: '  +dst

        except:
            pass
```

Screenshots:



Implementation:

- Wireshark is used to capture packets at first, while Ettercap is used to capture live packets.
- Dpkt - a python package for parsing packets that can be used as an analyzing tool. It examines each packet individually as well as the protocol layer. It displays the IP address of the user who downloaded the software from an unlawful or blacklisted website.
- The database stores all of the packet's information, including the source and destination IP addresses, timestamps, URLs.

Result:

Thus, the details of architectural design/framework/implementation along with the screenshots were provided.

CONCLUSION

With the aim of detecting malicious attacks on a network, we have created a Network Traffic Analyzer. It is capable of detecting the number of networks present and the number of active ports in each. It logs the transmission of data sent from one IP Address to another, while also scanning the data for viruses and other malicious data in them and ending the transmission. While providing tools that help monitor the network traffic.

REFERENCES

1. **GITHUB** - provider of Internet hosting for software development. https://github.com/VaideheeBarde/Network-Traffic-Analyzer

2. **Wireshark -** used for network troubleshooting, analysis, software and communications protocol development, and education. https://www.javatpoint.com/wireshark

3. **Nmap -** an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications. https://www.networkworld.com/article/3296740/what-is-nmap why-you-need-this-network-mapper.html

4. **Cisco -** Information gathered from CISCO. https://www.cisco.com/c/en/us/products/security/what-is-network-traffic-analysis.html