ISSN: 2278 – 1323
*International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*
*Volume 1, Issue 7, September 2012*

# AN OVERVIEW & ANALYSIS COMPARISION OF INTERNET PROTOCAL TCP\IP V/S OSI REFRENCE MODAL

**Nitin Tiwari[1] ,Rajdeep Singh solanki, Gajaraj Singh pandya**

***Abstract*** **:-Basically network is a set number of interconnected lines presenting a net, and a network's roads |an interlinked system, a network of alliances. Today, computer networks are the core of modern communication. All modern aspects of the Public Switched Telephone Network (PSTN) are computer-controlled, and telephony increasingly runs over the Internet Protocol, although not necessarily the public Internet. The scope of communication has increased enough in the past decade, and this boom in communications would not have been feasible without the progressively advancing computer network. Computer networks and the technologies needed to connect and communicate through and between them, continue to drive computer hardware, software, and peripherals industries. This expansion is mirrored by growth in the numbers and types of users of networks from the researcher to the home user. We Discussed to internet protocol TCP/IP and The concept of internet working (inter connection of network) Developed together A internet under TCP\IP operates like a single network connecting many computer of any size and type. but compare to OSI Reference modal concept of the international standard organization (ISO) is a multinational body dedicated to world wide agreement on international standard, An ISO Cover all aspects of network communication is the open system interconnection (OSI) model .an open system is a set of protocol that allow two different system to communicate regardless of their underline architecture. it is a modal for understanding the design of a network architecture.**

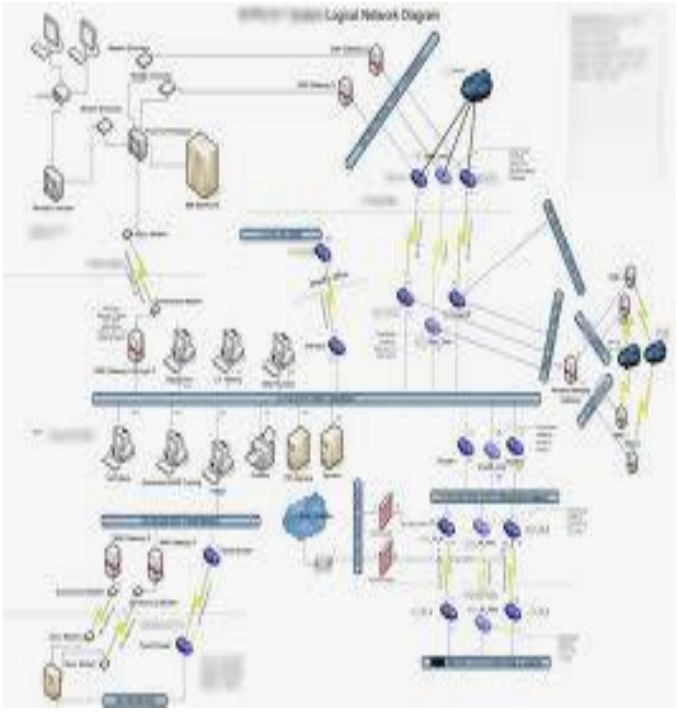
***keywords*—TCP/IP, OSI REFRENCE MODAL,IP HEADER,ICMP.**

## Introduction

**A LAN (local area network) is a network that linked computers and devices in a limited geographical area such as home, school, computer laboratory, office building, or closely positioned group of buildings. Each computer or device on the network is a node. Current wired LANs are most likely to be based on Ethernet technology, although new standards like ITU-T GHz also provide a way to create wired LAN using existing home wires (coaxial unfailing, phone lines and power lines). A (Metropolitan area network) MAN is a large computer network that usually spans a city or a large campus. The HUB network is an example of a MAN. A (wide area network) WAN is a computer network that covers a large geographic area such as a city, country, or spans even intercontinental distances, using a communications channel that combines many types of media such as telephone lines, unfailing, and air waves. A WAN often uses transmission utilities provided by common carriers, such as telephone companies. WAN technologies generally function at the lower three layers of the OSI reference model: the physical layer, the data link layer, and the network layer. The Internet is a global system of interconnected governmental, academic, corporate, public, and private computer networks. In other words, the Internet is a worldwide interconnection of computers and networks which are either owned privately or**

*Manuscript received June, 2012.*
***Nitin Tiwari[1], research scholar Network Security,,mphil, m.sc (comp.sc) Institute of Computer Science Vikram University, Ujjain india***
**Rajdeep Solanki[2] research scholar ,Network Security,mphil, m.sc (comp.sc) ,Institute of Computer Science Vikram University ,Ujjain India.**
**Gajaraj Pandya- research scholar, Network Security,mphil, m.sc (comp.sc) Institute of Computer Science Vikram University, Ujjain**

**publicly. It is based on the networking technologies of the Internet Protocol Suite. It is the successor of the Advanced Research Projects Agency network (ARPANET) developed by DARPA of the United States Department of Defence. The Internet is also the communications backbone underlying the World Wide Web (WWW).**



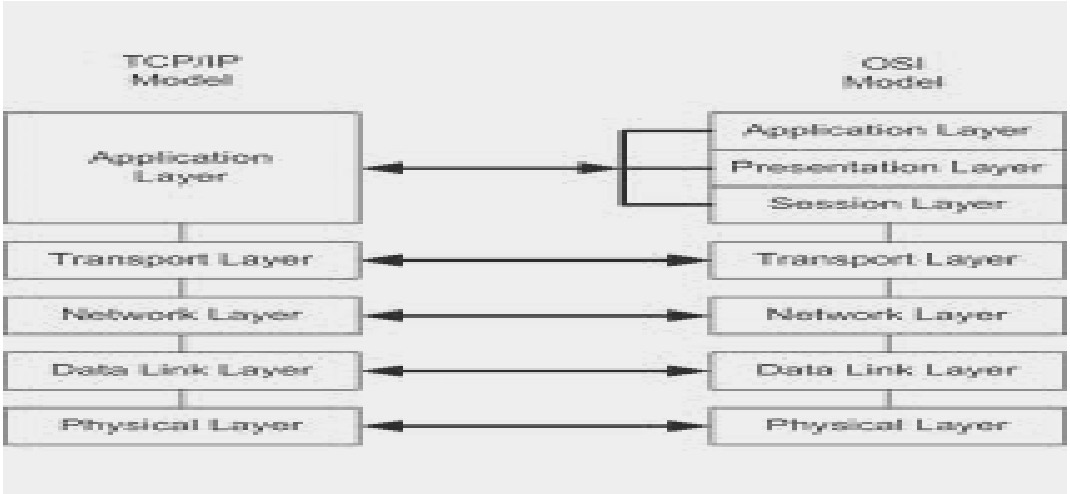
**Understanding ISO in OSI model to know the function for every layer is instrumental tools for understanding data link to each other within LAN, MAN or WAN. Created a layered model by ISO (International Standards Company) is called the OSI (Open Systems Interconnect) model, to explain known layers in a network operating system. To give clearly known functions by layers is that can increase improvement in Internet work connectivity among "computer" making companies. There is standard defined input and a standard defined output for every layer.**

## TCP/IP vs. OSI

**There using four layers by TCP/IP model, the top six layers of the OSI reference model is logically span equivalent to TCP/IP four layers; But the TCP/IP model not covered 4 physical layer because the data link layer is assumed the point at which the interface occurs among the TCP/IP stack and the underlying networking hardware. The main differences among the OSI architecture and that of TCP/IP relate to the layers above the transport layer (layer 4) and those at the network layer (layer 3). OSI has both, the session layer and the presentation layer, whereas TCP/IP combines both into an Application layer. The requirement for a connectionless protocol also required TCP/IP to combine OSI's physical layer and data link layer into a network level. Given below are the TCP/IP model layers, beginning from the bottom. The TCP/IP structure model has four layers that about match six of the seven layers in the OSI Reference Model. The TCP/IP model does not has address the physical layer, there is hardware devices reside and next 3 layers network interface, internet and point to point transport relate to layers 2, 3 and 4 of the OSI model. The TCP/IP application layer conceptually "blurs" the top three OSI layers. It's also worth noting that some people consider certain aspects of the OSI session layer to be arguably part of the TCP/IP host-to-host transport layer. The adoption of TCP/IP does not conflict with the OSI standards because the two protocol stacks were developed concurrently. In some ways, TCP/IP contributed to OSI, and vice-versa. Several significant differences do exist, though, which arise from the basic requirements of TCP/IP which are:**

1. **A common set of applications**
2. **Dynamic routing**
3. **Connectionless protocols at the networking level**
4. **Universal connectivity**
5. **Packet-switching**

**OSI Reference Model and TCP/IP Model Layers**



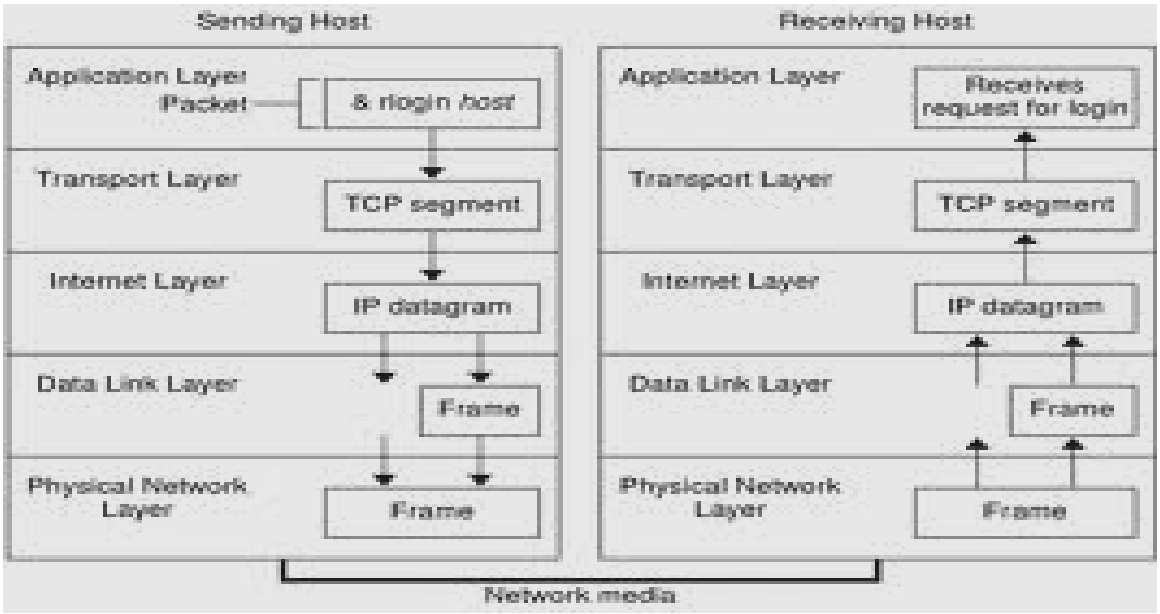

## TCP/IP Protocols

**Transmission Control Protocol/Internet Protocol (TCP/IP) to interlink various defence department computer networks. The TCP/IP suite includes the following protocols; TCP is a standard protocol with STD number 7. The Transmission Control Protocol (TCP), documented in RFC 793, makes up for IP's deficiencies by providing trusted, stream-oriented connections that hide most of IP's shortcomings. The protocol suite gets its name because most TCP/IP protocols are based on TCP, which is in turn based on IP. TCP and IP are the twin pillars of TCP/IP.**

**The Internet, an international Wide Area Network, uses TCP/IP to connect government and educational institutions across the world. TCP/IP is also in wide spread use on commercial and private networks.**

**Figure: Encapsulation of data in TCP/IP stack**

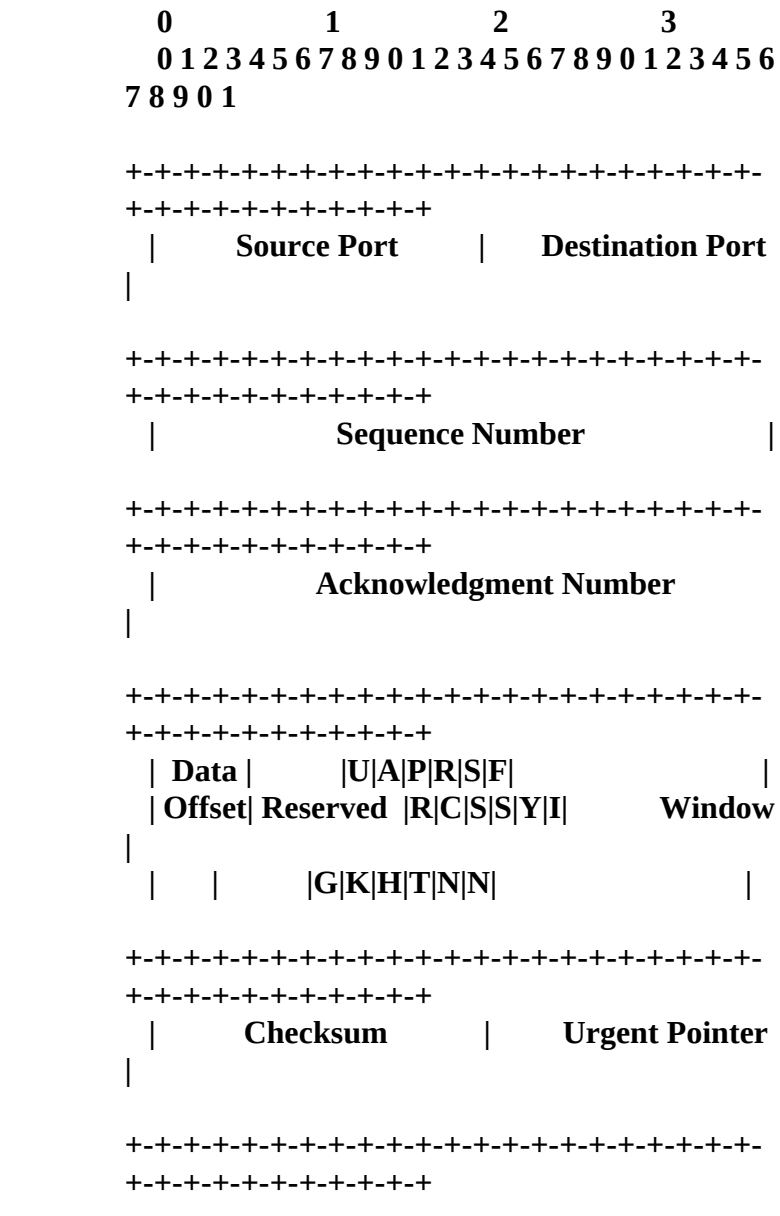
**Among two computers sending any data TCP first breaks the data into small parts called a packet. TCP sends again until the data not reach to destination if packet fails to reach its destination.**



**TCP Header:-**

**TCP segments are sent as internet data-grams each unit of data transmitted by TCP has a TCP header. The Internet Protocol header carries several information fields, including the source and destination host addresses [2]. TCP header contains all the details which help to keep TCP connections in order, to again the packet at other end, and to detect any transmission errors. Here is TCP header format. A TCP header follows the internet header, supplying information specific to the TCP protocol. This division permits for the existence of host level protocols other than TCP.**
**Figure TCP Header**

**TCP Header Format**




**TCP Header Format**

**The TCP header padding is used to ensure that the TCP header ends and data Begins on a 32 bit boundary A TCP segment consists of a TCP header optionally followed by data. A TCP header includes six flag bits. One or more of them can be turned on at the same time:**

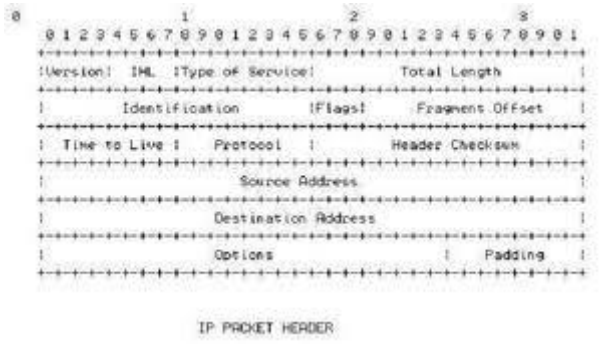
- **SYN Synchronize sequence numbers to beginning a connection.**
- **FIN the sender is finished sending data.**
- **RST reset the connection.**
- **URG the urgent pointer is valid.**
- **ACK the acknowledgment number is valid**
- **PSH the receiver should pass this data to the application as soon as feasible.**

**IP Header**

**The first field in the IP header is the version field. This is used to opinion which version of IP was used to create the header. IP header is responsible for telling the TCP/IP that where in coming packets suppose to go. Header Checksum field makes sure that IP header does not get damaged and the information is not corrupted. This is significant in internets because not every network is running the same version of a protocol. If the IP header was created in a network using the latest version of IP, it may contain information not identity effectual by an older version of IP. Protocol field talks to IP on receiving computer and makes sure about receiving protocol is TCP or UDP. Time to live field is used to 7 controls the life lifetime of a packet. Every time the packet passes by a system, the field's value is decrease. The packet is destroyed when it reaches zero,. There are two fields are for IP addresses of the source input and the task machines. Network to network packet jumps from, IP address to**

**decide where the packet should be sent by IP header.**

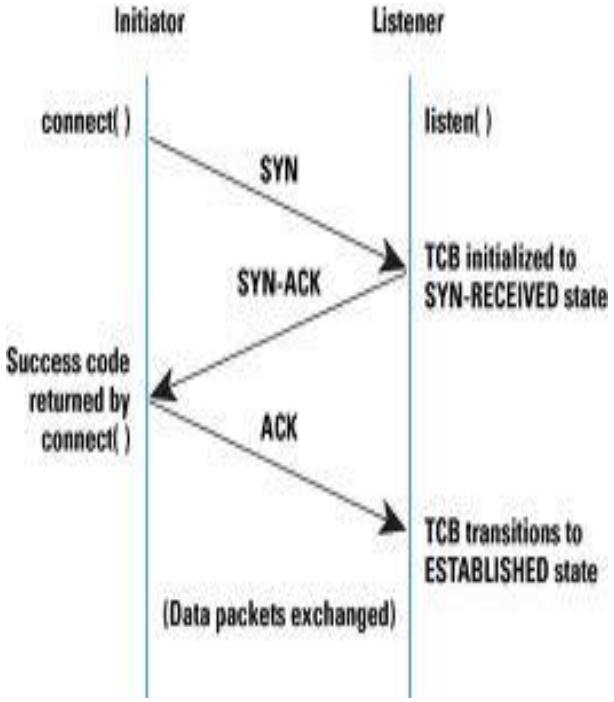
**Figure : IP Header**




**By opening connections the TCP functions become remote host to connection oriented. Maintaining status information related the links by TCP to makes and is therefore a trusted protocol. The TCP links is opinion by the IP addresses and virtual port numbers used by both ends. At the time of linking additional numbers are used to keep track of the order or series of number which identity what order the part of data should be again. Finally, a maximum transfer size is unique negotiated by a fallback mechanism called windowing. The grouping of port numbers, series numbers and window sizes construction a link, or pipe. TCP uses the three-way handshake for establish a connection. In one direction this three way handshake will only be completed even if in same time both sides initialize connections avail unfailing.**

**BUILDING CONNECTIONS: Three Way Handshake Detail the TCP 3-way handshake process is given below. The parameter "T" is using to change a order of points going towards in time.**
**Time Event DIAGRAM T Host A sends a TCP Synchronize packet to Host B**

**T+1 Host B receives A's Synchronize**
**T+2 Host B sends it's own Synchronize**
**T+3 Host A receives B's Synchronize**
**T+4 Host A sends Acknowledge**
**T+5 Host B receives Acknowledge.**
**TCP connection is established.**



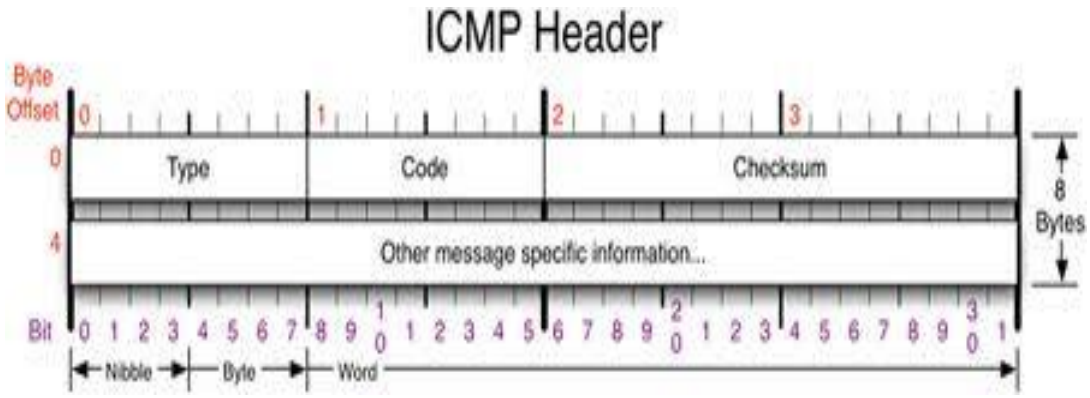

**Tunfailing: Three-way TCP/IP handshake TCP can divided up a message, to the pieces and again if they are find out of order. Once linked TCP hands off to the program for data transfer and linked.**

**ICMP :-**

**The headers differ a little bit from ICMP type to ICMP type. Most of the ICMP types are feasible to group by their headers. The Internet Protocol (IP) defined by RFC 792 through control Message Protocol. Supporting packets by ICMP having error, control, and informational messages; The PING command, i.e., uses ICMP to examine an Internet connection. ICMP messages, transfer in IP packets, are used for out-of-band messages linked to network operation or miss-operation. But ICMP uses IP, ICMP packet delivery is un-trusted, hence hosts can't count on getting ICMP packets for any network problem.**

**Figure: ICMP Header**

ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 1, Issue 7, September 2012




**Providing simple error reporting, diagnostics and limited configuration for IP hosts by ICMP is logically on the IP layer but ICMP packets are encapsulated by IP as shown. It is link less like as IP, and un-trusted the error reporting messages copy the offending packets**
**IP header and the first 8 bytes of its TCP or UDP header Or, the entire packet so that the ICMP message is < 576 bytes (RFC1812)**

**Figure: ICMP Format**

| 8-bit ICMP Type | 8-bit ICMP Code | 16-bit ICMP Checksum |
|---|---|---|
| ICMP Contents (dependent on type and code) | | |

**Format and Fields ICMP has a fixed "header" portion of 4 bytes:**
**Type:**

- **Type of message Code**
- **Subtype of message Checksum**

**Unless for the checksum field itself, which is set to 0 the 1's compliment calculated over entire ICMP message, To a different purpose can be normal or complex by rest of the ICMP data depends on the type and code.**

**Conclusion:- In chapter one has a phrase to the networking, its active design, the network –transport protocols, the present landscape of safety and virus, the concept of Network TCP/IP protocol and OSI Reference modal The substructure of computer networking is described, and then move on to a contemplation of few popular networks. Following that, more in-depth see at OSI model and used to run the Internet and many intranets by TCP/IP. The network protocol suite most TCP/IP protocols are based on TCP, which is in turn based on IP. TCP and IP are the twin pillars of TCP/IP. TCP/IP is also in wide spread use on commercial and private networks. The adoption of TCP/IP does not conflict with the OSI standards because the two protocol stacks were developed concurrently. In some ways, TCP/IP contributed to OSI, and vice-versa. Once disguised this, few of the virus that managers and admin of computer networks require encountering, visible by different header expand during network analysis techniques. the most basic of traffic reveals so much about the devices on the network, IP Header Format and edge router OSI should be maintained to allow only that traffic which is absolutely essential to production even ICMP should be carefully restricted. This paper is providing an overview of these strategies**

**.**

**Reference:-**

**[1] Arkin, Ofir. "ICMP Usage in Scanning – The Complete Know How." June 2001. ICMP_Scanning_v3.0.pdf , May 2, 2003.**

**[2] CERT coordination center, A Taxonomy of Computer and Network Attacks**

**[3] Dethy, "Examining port scan methods – Analysing Audible Techniques."**

**[4] Gael Roualland and Jean-Marc Saffroy, "IP Personality", URL:**

**[5] Introduction to Network Safety, URL: Techniques."**

**[6] Ethereal: A Network Protocol Analyzer.**

**[7] Net filter and IP infallibles. Avail infallible.**

**[7] McGraw-Hill. Let's Talk: Computer Networks Tech CONNECTS Online**:

**[8] RFC 793 "Transmission Control Protocol", USC, University of Southern**

**[9] Chi-Keung Luk, Robert Cohn, Robert Muth, Harish Patil, Artur Klauser, Geoff Lowney, Steven Wallace, Vijay Janapa Reddi, and Kim Hazelwood. Pin: Building Customized Program Analysis Tools**

**[10] Matthew Smart G. Robert Malan Farnam Jahanian, "Defeating TCP/IP Stack**

**32] Richard Stevens, TCP/IP Illustrated, Volume 1, Addison-Wesley.**

**[11] Seong Soo Kim, A. L. Narasimha Reddy and Marina Vannucci, "Detecting traffic anomalies through aggregate analysis of packet header data", in Proceedings of Networking 2004, Lecture Notes in Computer Science (LNCS)vol. 3042, pp. 1047-1059, Athens, Greece, May 2004.**

**[12] Honeynet Project, "Know Your Enemy: Passive Finger stamping, Opinioning remote hosts, without them knowing**

**[13 ] Zalewski, Michal; Strange Attractors and TCP/IP Sequence Number Analysis**

*Nitin Tiwari[1], research scholar Network Security,,mphil, m.sc (comp.sc) Institute of Computer Science Vikram University,Ujjain India*

Rajdeep Solanki[2] research scholar, Network Security,mphil, m.sc (comp.sc) ,Institute of Computer Science Vikram University,Ujjain

Gajaraj Pandya research scholar, Network Security,mphil, m.sc (comp.sc),Institute of Computer Science Vikram University,Ujjain