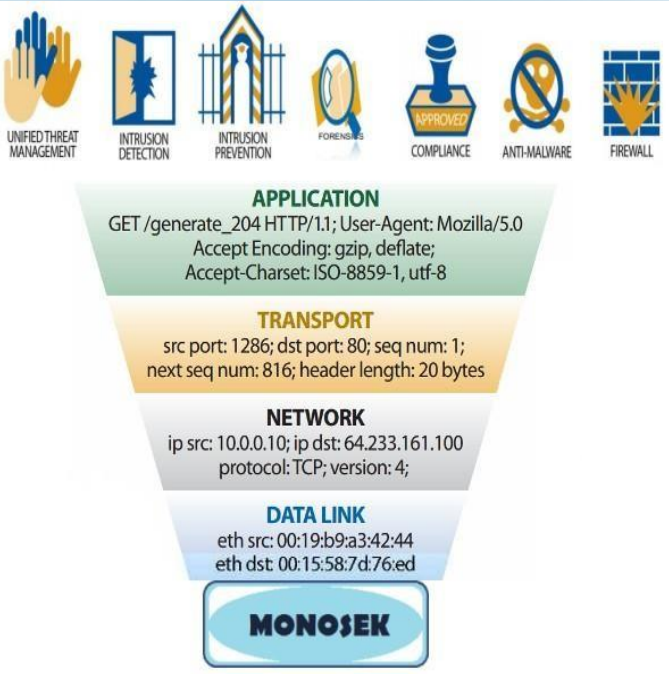
NIHON COMMUNICATION SOLUTIONS PVT. LTD

NCS
NihonCommunicationSolutions

MONOSEK

Network Security Analysis Tool



With C/C++ Programmable Interface

Network Interception - Packet Analysis & Classification

Deep Packet Inspection - IDS/IPS operations.

Deep Packet Inspection - Virus Signature Analysis & Forensics.

Website: www.ncs-in.com

Email : sales@ncs-in.com

Email : sales@ncs-in.com

ABOUT MONOSEK

Monosek is a high end Network Packet Processing and Protocol Analysis System. It offers the most complex packet and flow processing with unparalleled performance, network flow processing solution tightly couples modular I/O, L2-L4 packet processing, L4-L7 flow processing via Network Flow Engine.

This heterogeneous architecture has three layers of workload-specific packet, flow, security and application processing, each with increasing levels of granularity.
These high-performance platforms are purpose-built for network and security applications that require line-rate throughput, low latency and high availability.
Software Modules available for Packet Analysis, with Deep Packet Inspection Library Interface.

SDK library and API call support in C, C++ and Java for Research and Development.

Deployable as both Inline and Passive monitoring support.

Monosek for Students

- Monitor Live network traffic.
- Learn and Develop various protocol traffic patterns, Packet Classification and Protocol Analysis in Active/Passive Mode
- UG, PG and Research projects in Network Security/Information Security/Cyber Security.
- Intrusion Detection and Prevention for vulnerabilities using DPI techniques.
- Track Intruder's IP addresses and map to a location by Country and other Cyber Crime Related applications.
- Virus signatures - Study and Analysis.
- Network attacks - Known attacks – Identifying and Alerting, Creating statistics.
- Network attacks - Behavioral pattern matching to estimate possible new threats.

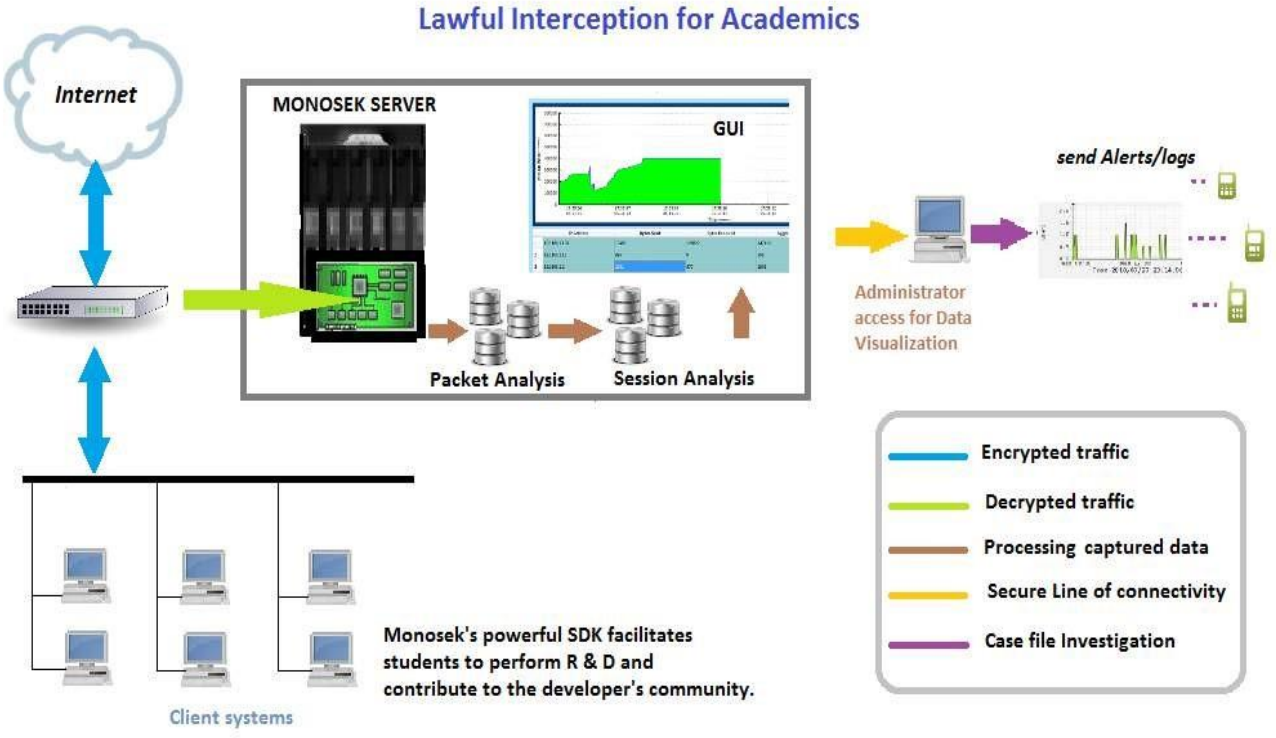
Email : sales@ncs-in.com

HARDWARE BASED MONOSEK

Dedicated network card is available in 2-port 10 Gigabit Ethernet and 6-port Gigabit Ethernet options and it provides up to 20Gbps of line-rate programmable packet and flow processing per card.

Stealth mode

In stealth mode, absolutely NO traffic can be injected or responded to or modified by Monosek, ensures that the analysis carried out on the network traffic does not reach to any wrong conclusions due to artificial additional network traffic created by the analyzer itself. It also ensures that the card itself does not fall victim to network attack



Email : sales@ncs-in.com

Undergraduate Lab Exercises:

1. Understanding of different layers in Ethernet communication, header fields and payload contents.
2. Analysis of underlying protocols used by different applications such as web browsers, chat programs, video streaming apps and mails. Usage and handling of IP UDP/TCP protocols by these applications.
3. Study of 3 way handshaking mechanism in TCP communication with respect to error handling and time taken by different hosts to establish connection.
4. Influence of various TCP parameters on TCP communication.
5. Protocol Analysis & Filtering packets.

Sl. No.	Sample Experiments for Undergraduate students (Available with SDK library and Source code)
1	Display all packets (irrespective of Transport Protocol) in a table format.
2	Display all TCP packets in a table format.
3	Display all UDP packets in a table format.
4	Display all TCP packets in a table format.
5	Display all SMTP packets in a complete packet format.
6	Display all POP3 packets in a table format.
7	Display all HTTP packets in a table format.
8	Display list of all captured IPv4 addresses being monitored.
9	Display list of all captured IPv4 addresses using HTTP services.
10	Display all packets (irrespective of Transport Protocol) in a complete packet format.
11	Display all TCP packets in a complete packet format.
12	Display all UDP packets in a complete packet format.
13	Display all packets with layer wise information display (TCP/IP model based)
14	Display a Flow Analysis of TCP Handshake mechanism.

Post Graduate/Research Lab Exercises:

1. Data mining technique to estimate Network packet characteristics.
2. Data mining technique to estimate behavior of people's internet usage.
3. Virus signatures - Study and analysis using DPI techniques.
4. Network attacks - Known attacks – Identifying and alerting, creating statistics using DPI techniques.
5. Network attacks - Behavioral pattern matching to estimate possible new threats using DPI techniques.
6. SIP/RTP – UDP VoIP mechanism and analysis.
7. H.264 Video analysis and reconstruction.

Sl. No.	Sample Experiments for Postgraduate/Research students (Available with SDK library and Source code)
1	VoIP Analysis using SIP/RTP protocols and performs VoIP session reconstruction.
2	Deep Packet Inspection techniques to detect XSS, SQLI vulnerabilities.
3	IP Trace back to map an IPv4 addresses to Geo locations.
4	Deep Packet Inspection techniques to detect Flow based Application Service protocols.
5	Pattern matching filter and Virus Signature Detection.

Monosek in Research

Monosek tools can be used to carry out research in the domain of network protocols, network security and network traffic encryption/decryption.

Why do we need Monosek?

SDK:

Practical work, extensive observations, observe network traffic with readily available GUI.

C/C++ programmable interface enables Developers to access analyzed packet information as well as raw packets in real time, Develop C programs to work on real-time packets, making use of analysis already carried out by Monosek.

Programmable Filters:

Monosek provides programmable filters, so that only packets of interest can be observed.

Filters provide deep packet inspection. So programs can be written to analyze not only headers but also contents of the packets(DPI).

Monosek provides for dynamic filters so that depending on how network traffic is behaving, the interfacing C/C++ program can add, modify or disable any/some of the filters.

Session analysis Library :

Users can develop new algorithms and recreate sessions for a protocol based on n-Tuple flow criteria.

Applications can be built by the users which can make use of Monosek powerful analyzed data such as viewing of web sites visited, viewing mail contents and contents of the files sent as attachment in the mails, listen to VoIP sessions and watch videos* that were streamed into the network under analysis by Monosek.

SPECIFICATIONS

- *Server with Intel Xeon CPU with 16GB memory, 2TB hard disk.*
- *Dedicated 2x10/6x1 Gbps Network Analysis Card.*
- *Linux Distribution*
  - *Ubuntu*
- *20/5 User License for protocol library/Session library.*
- *Protocol Analysis Tool*
  - *Libraries (Protocol, IDS/IPS , Flow for VoIP analysis/Application detection and GEOIP).*
- *Session Analysis Tool*
  - *Virus Signature Detection Library.*
- *Sample applications with source code for using above libraries*

Email : sales@ncs-in.com

University Clients

IIT-BHU, Varanasi.

NITTTR, Chandigarh.

NIT , Patna

R.V.College of Engineering, Bangalore

PSG College of Technology , Coimbatore.

GSSS, Mysore,

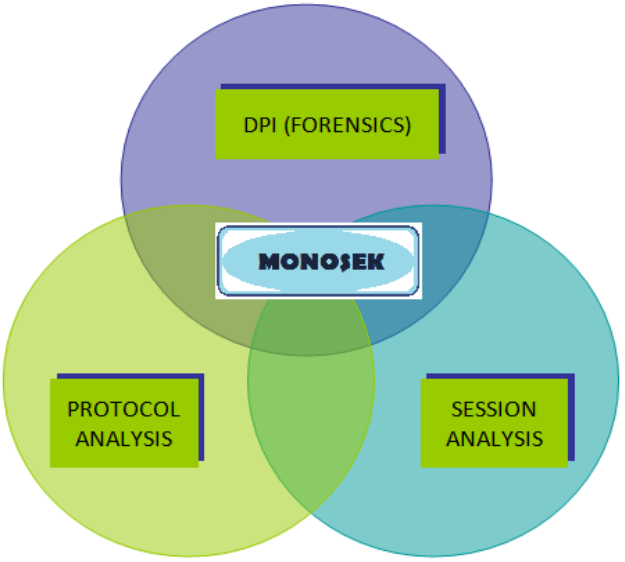
BITS Pilani,Goa.

ISM, Dhanbad.

Commercial Clients

CDAC , Hyderabad

TCS, Noida



Nihon Communication Solutions Pvt. Ltd

5/19 and 6/20, II[nd] and III[rd] floor, 2[nd] stage, 11[th] cross, Nagapura Main road,

Next to W.O.C Road, Mahalakshmipuram, Rajajinagar, Bangalore – 560086

Ph: 080-23591866 Fax: 080-23591865

www.ncs-in.com