SEOULTECH

SeoulTech UCS Lab

Ubiquitous Computing & Security Laboratory

Digital forensics
Technical Fundamentals

Saurabh Singh

159744151

saurabhgcet1989@gmail.com

Topics

- Source of network based evidence
- Principles of internetworking
- Internet protocol Suite
- conclusion

Source of network based evidence

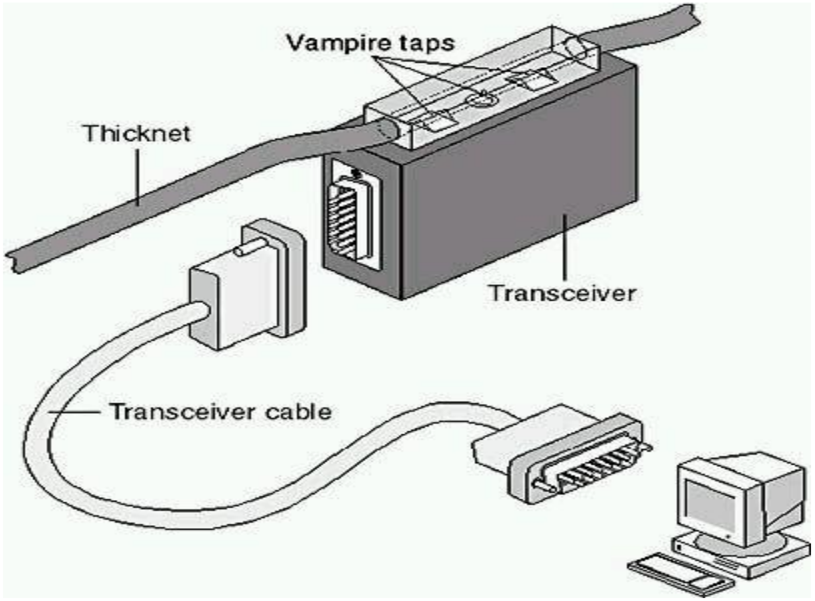
- On wire
- In air
- Switches
- Routers
- DHCP Servers
- Name servers
- Authentication servers
- NID/PS
- Firewalls
- Web proxies
- Application servers
- Central log servers

On the wire

- used to provide the connectivity between stations on LAN and the Local switches.
- Between switches and routers
- It consist of copper and in the form of twisted pair(TP) OR Coaxial cable.
- It also consists of fiber optics line made of thin strands of glass.
- Stations connected via fiber signal data through the presence or absence of photons.

Forensics value

- investigators can tap into physical cabling to copy and preserve network traffic as it is transmitted across the line.
- puncture the insulation and make contact with copper wires, to surreptitious fiber taps, which bend the cable and cut the sheathing to reveal the light signals as they traverse the glass.



Ex. "Vampire Tap"

In The Air

- Data transmits station-to-station signals is via “wireless” networking,
- It consists of radio frequency (RF) and (less commonly) infrared (IR) waves.
- Wireless networks can easily be deployed even without “line-of-sight”.
- RF waves can and do travel through air, wood, and brick, no se of cables.

Forensics value

wireless access points act as hubs, broadcasting all signals so that any station within range can receive them. As a result, it is often trivial for investigators to gain access to traffic traversing a wireless network.

Switches

- Used to hold our LAN together and connect multiple stations.
- Switches connected to other switches and connect to other switches and form a complex switched network environment.

- Two types of switches
  - **CORE** aggregate traffic from many different segments.
  - **EDGE** aggregate stations on individual segments**.**

Forensics value

- Switches contain a "content addressable memory" (CAM) table, which stores mappings between physical ports and each network card's MAC address.

- using mac address investigator determine switches and corresponding port.

- It also provide VLAN to capture traffic from the mirroring port with a packet sniffer.

Core switch

Edge switch

Routers

- It connect different subnets or networks together and facilitate transmission of packets between different network segments.
- It allows LAN, MAN, WAN and GAN connections.

Forensics value

- Switches have CAM tables, routers have routing tables.
- tables map ports on the router to the networks that they connect.
- This allows a forensic investigator to trace the path that network traffic takes to traverse multiple networks.

DHCP Servers

- Dynamic Host Configuration Protocol (DHCP) is widely used as the mechanism for assigning IP addresses to LAN stations which could change dynamically as needed.

  - **Forensic Value**

- When DHCP servers assign (or “lease”) IP addresses, they typically create a log of the event, which includes the assigned IP address, the MAC address of the device receiving the IP address, and the time the lease was provided or renewed.
- Other details, such as the requesting system’s hostname, may be logged as well.

Name Servers

- Mechanism to map MAC addresses to IP addresses.
- Enterprises typically use the Domain Name System (DNS), in which individual hosts query central DNS servers when they need to map an IP address to a hostname, or vice versa.

Forensic Value

- DNS servers can be configured to log queries for IP address and hostname resolutions.
- DNS servers can log not only queries, but also the corresponding times. Therefore, forensic investigators can leverage DNS logs to build a timeline of a suspect’s activities

Authentication Servers

- Theses servers are designed to provide centralized authentication services to users throughout an organization so that user accounts can be managed in one place, rather than on hundreds or thousands of individual computers. This allows enterprises to streamline account provisioning and audit tasks.

Forensic Value

- Authentication servers typically log successful and/or failed login attempts and other related events.
- Investigators can analyze authentication logs to identify brute-force password-guessing attacks, account logins at suspicious hours or unusual locations, or unexpected privileged logins, which may indicate questionable activities.

Network Intrusion Detection/Prevention Systems

- NIDS/NIPS specifically designed to provide security analysts and forensic investigators with information about network

  security–related events.
- It monitors network traffic in real time for indication of any adverse events.
- When indications are detected they alert the security personals.

Forensic Value

- Designed to provide for timely data pertaining to adverse event on the network.
- Forensic investigators can request that network staff tune the NIDS

  to gather more granular data (source and destination IP addresses, the TCP/UDP ports, and the time the event occurred) for specific events

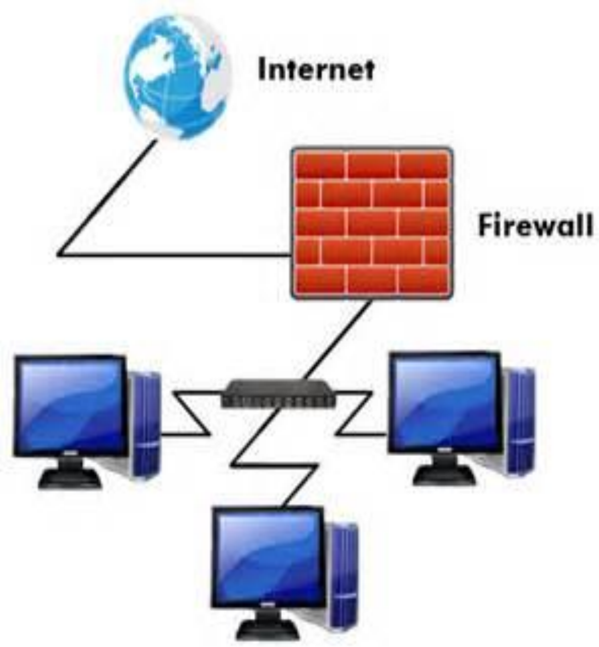
  of interest or specific sources and destinations.

Firewalls

- Firewalls are specialized routers designed to perform deeper inspection of network traffic in order to make more intelligent decisions as to what traffic should be forwarded and what traffic should be logged or dropped.

  - **Forensic Value**

- They were most definitely designed to implement security policies to prevent violations.
- Firewalls can be configured to produce alerts and log allowed or denied traffic, system configuration changes, errors, and a variety of other events.



Web Proxies

- Web proxies are commonly used within enterprises for two purposes:
- first, to improve performance by locally caching web pages

  and second, to log, inspect, and filter web surfing traffic.
- End clients send their traffic through an anonymous web proxy so that the remote web server only sees the proxy's IP address rather than the end-user's IP address.

Forensic Value

- Web proxies are configured to retain granular logs for an extended period of time.
- Investigator can produce the web surfing history for users of a single device.
- It finds user's inappropriate web surfing habits, or identify the source of web-based malware.

Central Log Servers

- Central log servers aggregate event logs from a wide variety of sources, such as authentication servers, web proxies, firewalls, and more.

- Individuals servers send logs to central log servers, where they time stamped analyze and correlated.

Forensic Value

Devices such as routers, which typically have very limited storage space, may retain logs for very short periods of time, but the same logs may be sent in real time to a central log server and preserved for months or years.

Principles of Internetworking

- What are protocols
- OSI Model
- Working of OSI Model

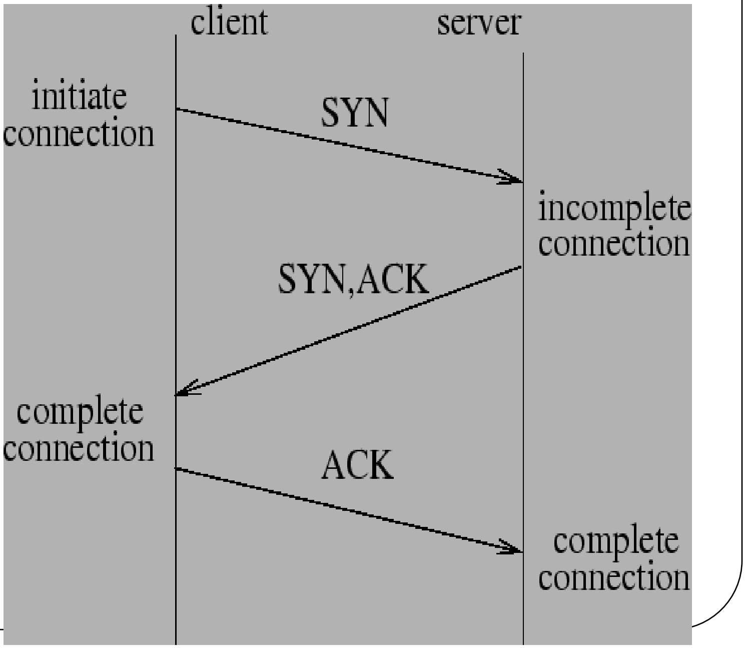
Principles of Internetworking

- Communication on the Internet involves coordinating hundreds of millions of computers around the world.
- To connect these computers we have to follow some standards and protocols.

Protocols

- A protocol is the special set of rules that end points in a telecommunication connection use when they communicate.
- It takes new meaning when viewed in the context of forensics investigation.

– three easy step to establish the communication



What are protocols

- Rules for successful communication between different systems
- Prearranged specifications for actions
- Designed to avoid implementation dependence
- Designed to avoid ambiguity
- Designed to recover gracefully from errors
- A perpetual attack target

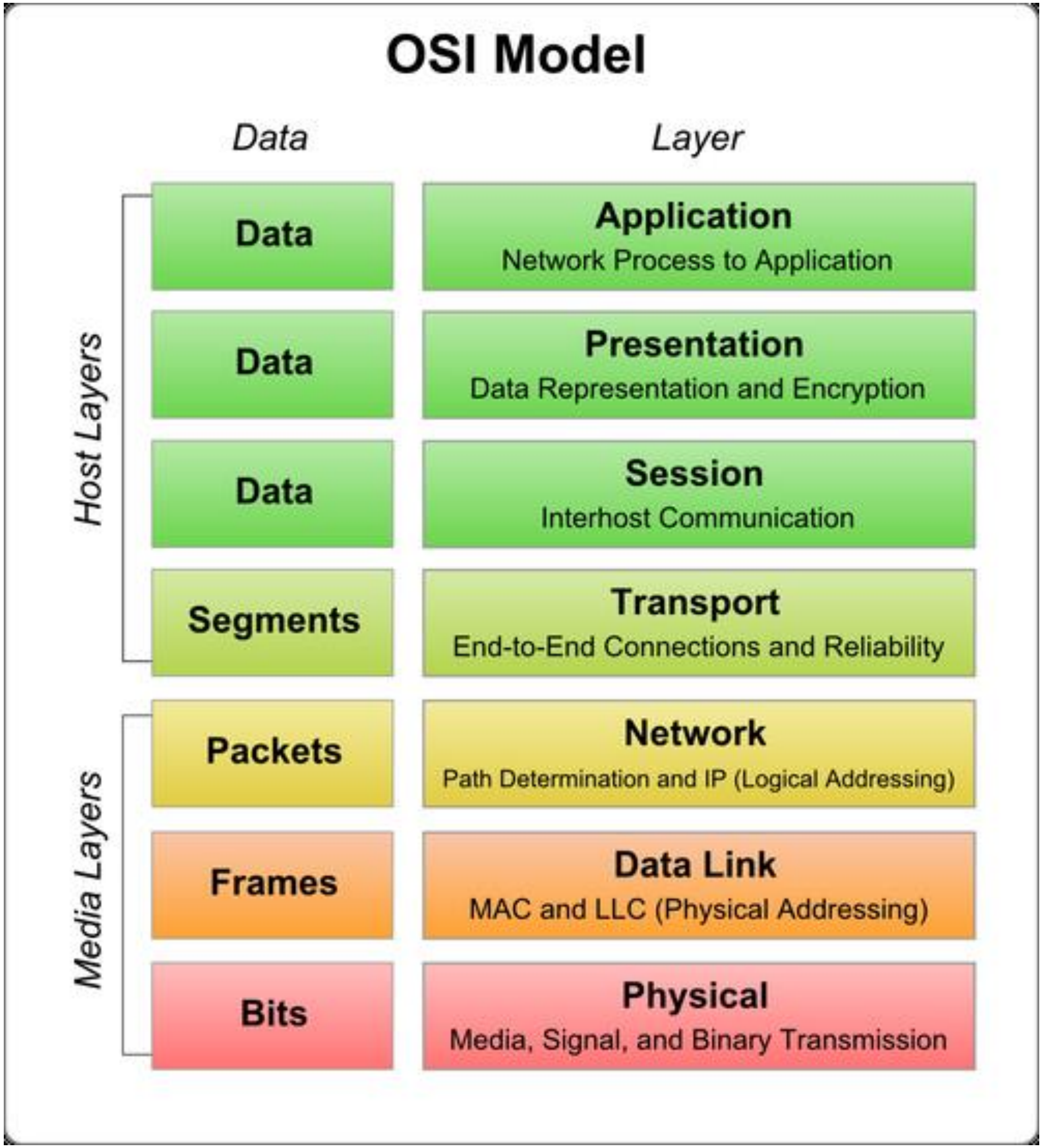
OSI Model

- It is Open System Interconnection Model designed by ISO to provide

  - **Modularity** Breaks down a complex communication problem into more manageable parts.

  - **Flexibility** Supports interchangeable parts within a layer.

  - **Abstraction** Describes the functionality of each layer, so that developers don’t need to know the specific details of protocol implementations in order to design interoperable processes.



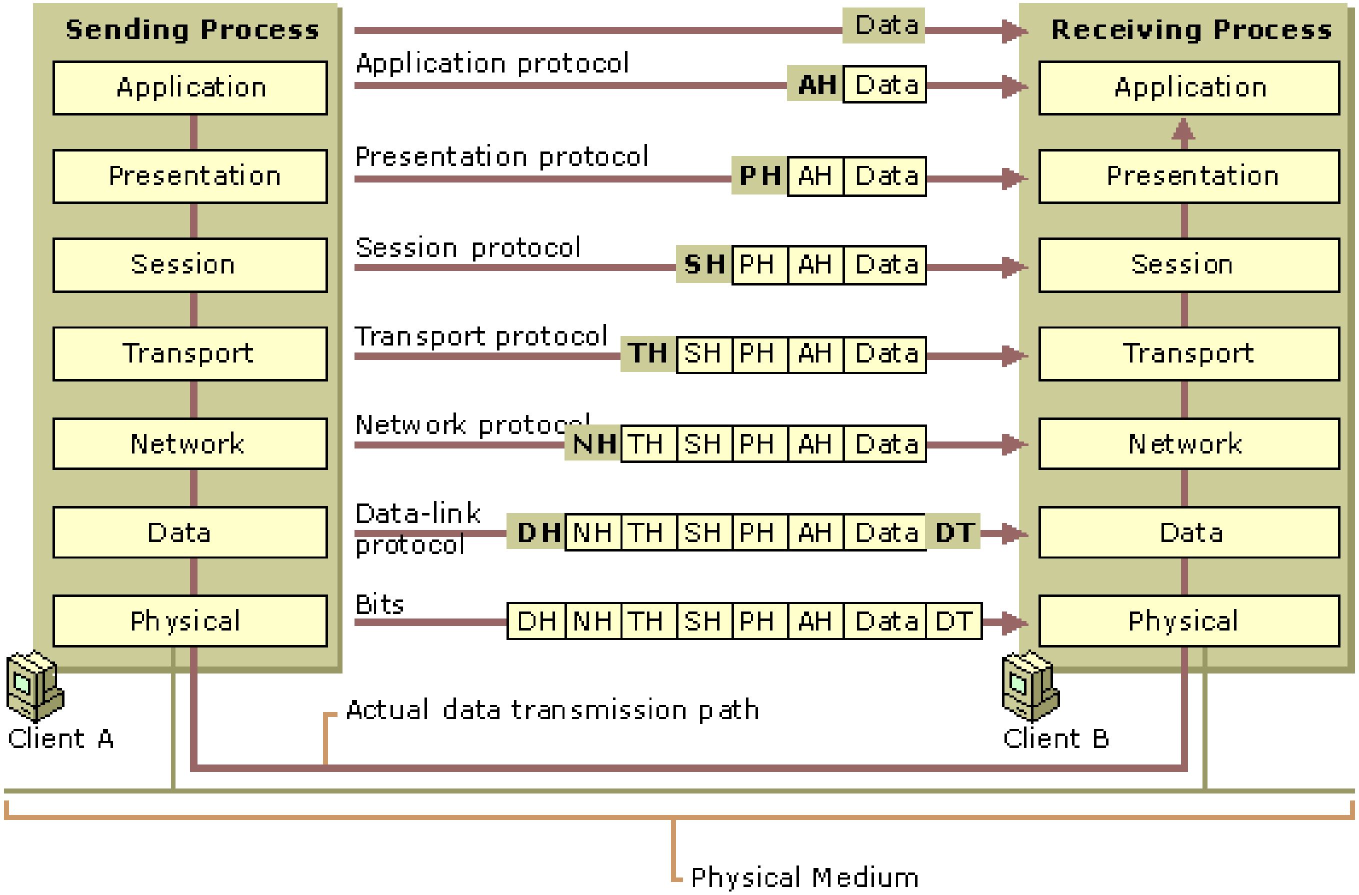
OSI Model

	Data	*Layer*
Host Layers	**Data**	**Application** Network Process to Application
	Data	**Presentation** Data Representation and Encryption
	Data	**Session** Interhost Communication
	Segments	**Transport** End-to-End Connections and Reliability
Media Layers	**Packets**	**Network** Path Determination and IP (Logical Addressing)
	Frames	**Data Link** MAC and LLC (Physical Addressing)
	Bits	**Physical** Media, Signal, and Binary Transmission

Working of OSI Model

Encapsulation

Demultiplexing



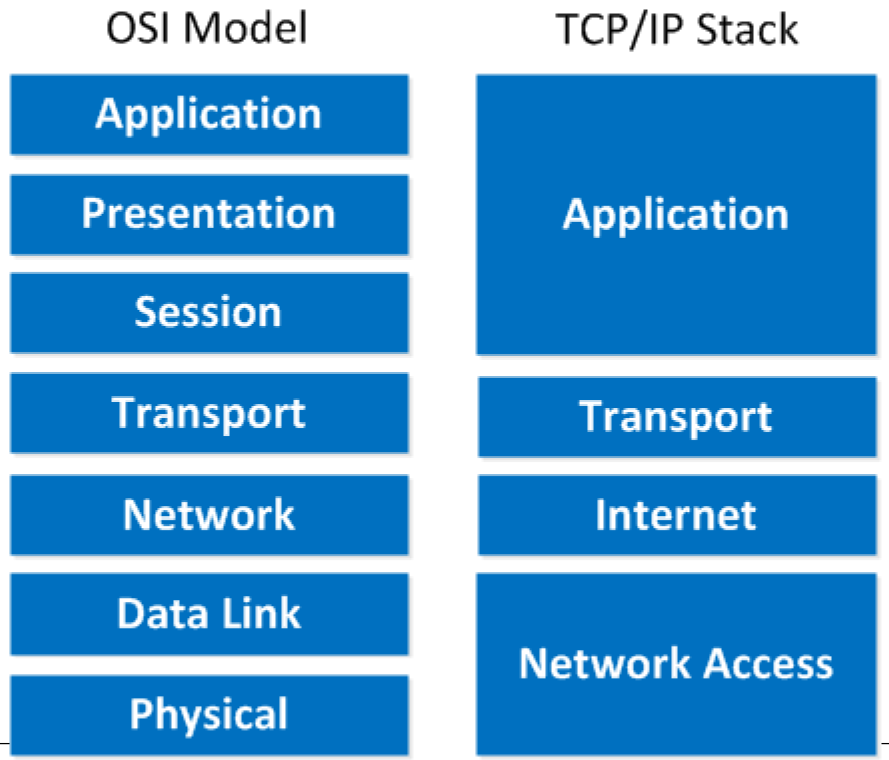
Client A sends data to client B

Internet Protocol Suite

- Internet Protocol
- Ipv4 packet header
- Ipv6 packet header
- Transmission Control Protocol (TCP)
- User Datagram Protocol

Internet Protocol Suite

- Also knows as TCP/IP protocol suite
- Set of protocol used to implement important functions on the Internet and in many other packet-switched networks.
- For forensics investigator the effectiveness is depend upon familiarity with which key protocol and header files.



Internet Protocol

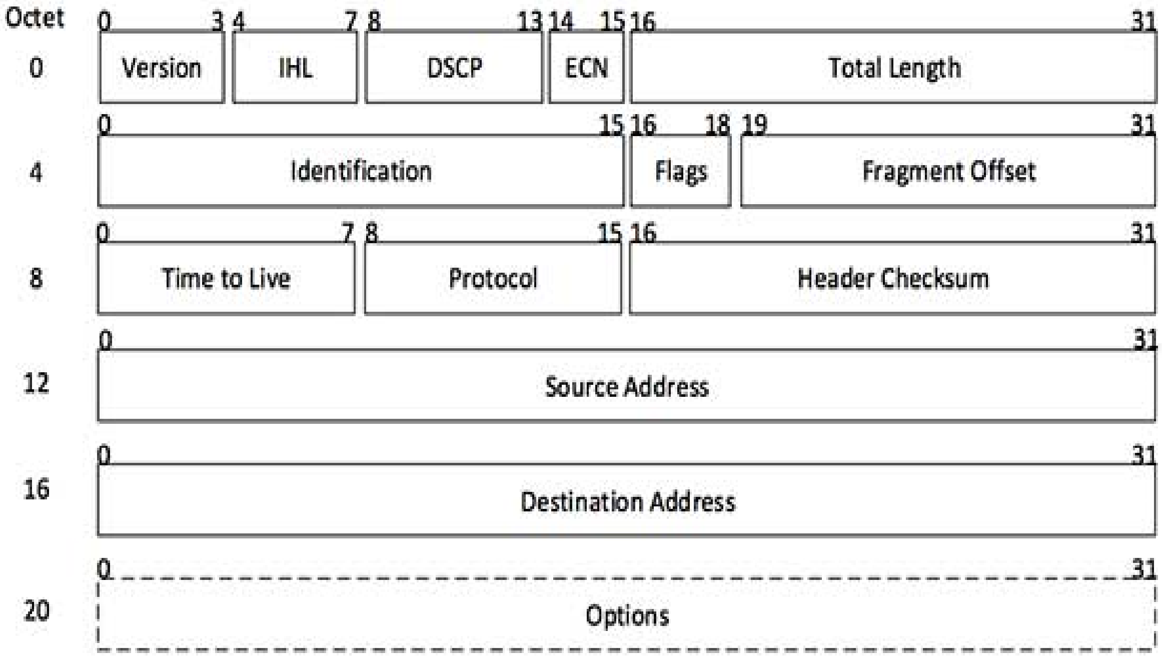
- Internet protocol is a set if technique used by many host for trans mitting data over the internet.
- uniquely identifying source and destination systems on a network IP address.
- Ip address are stored as binary numbers they are usually displayed in human readable notations for example

  192.169.190.43(ipv4)

  2001:db8:3:3456:0:465:1:10 (ipv6)

Ipv4 packet header

- Support for addressing and routing
- Connection less
- Unreliable
- Include header no footer
- Header+ payload = IP Packet



header

[Image: IP Header]

Ipv6 packet header

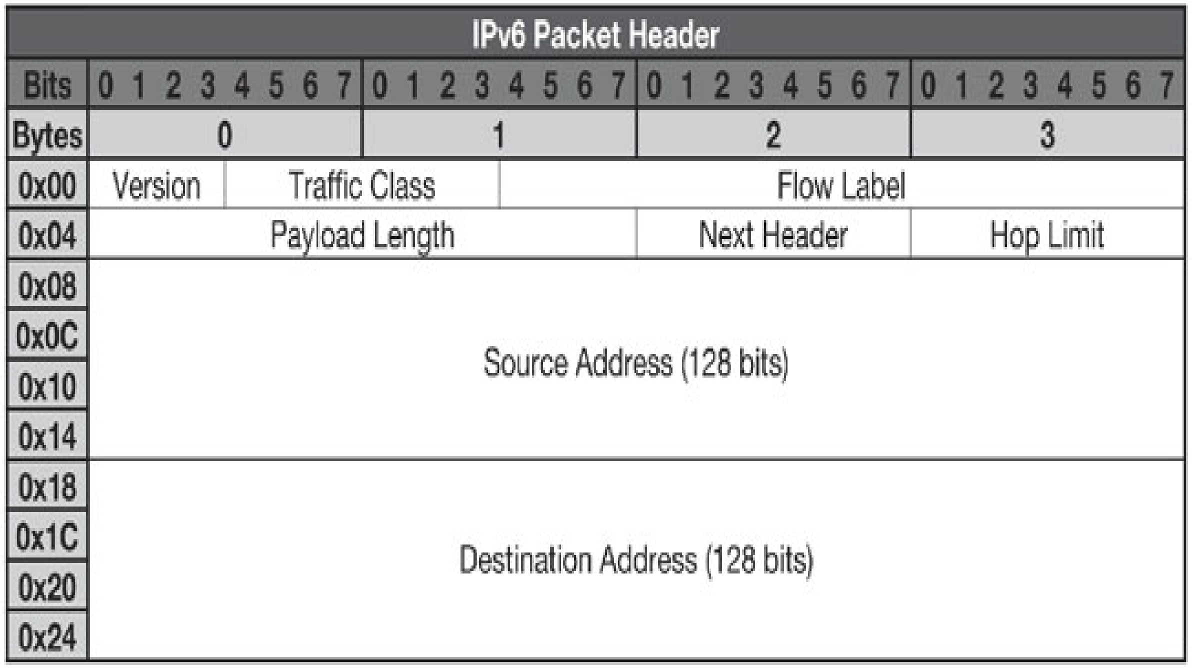
- 8 groups of 16-bit hexadecimal numbers separated by ":"
- Size is **40Byte+payload = packet size**

3FFE:085B:1F1F:0000:0000:0000:00A9:1234

↓

3FFE:85B:1F1F::A9:1234

40 bytes

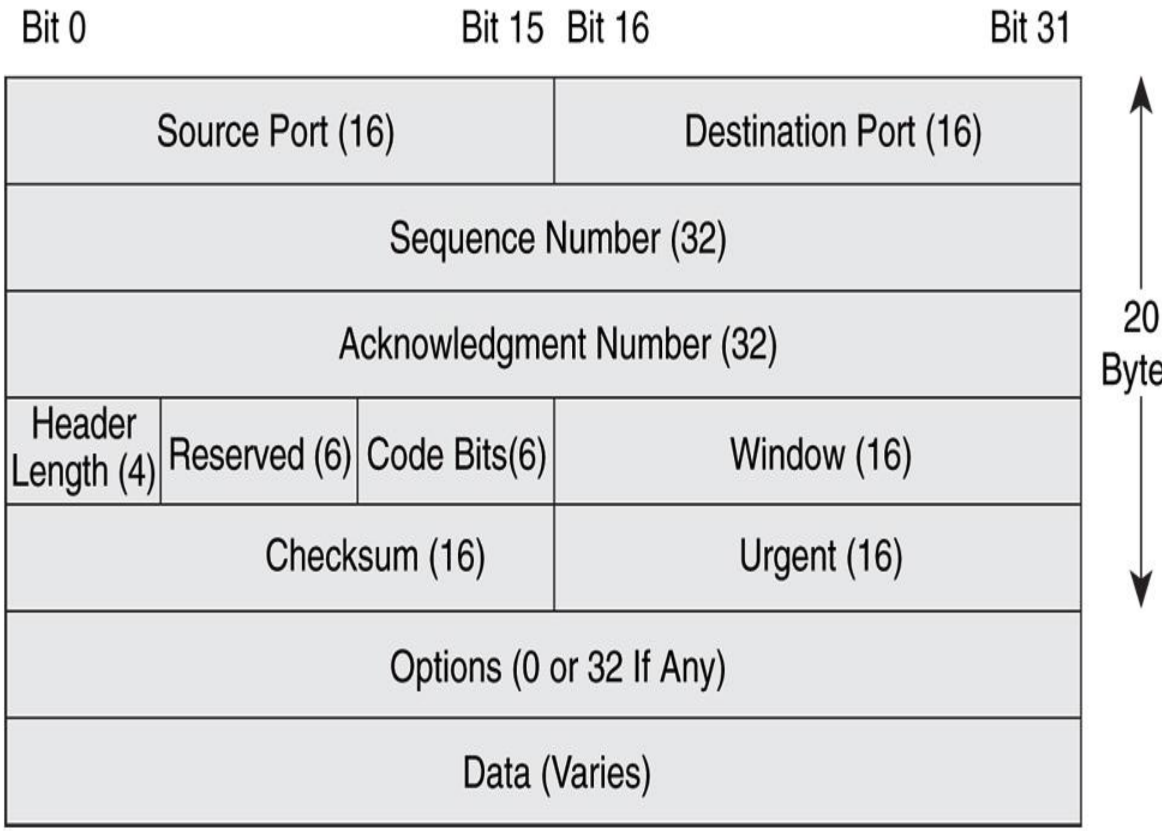


IPv6 Packet Header

Bits	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Bytes	0	1	2	3
0x00	Version Traffic Class	Traffic Class	Flow Label	
0x04	Payload Length		Next Header	Hop Limit
0x08	Source Address (128 bits)			
0x0C				
0x10				
0x14				
0x18	Destination Address (128 bits)			
0x1C				
0x20				
0x24				

Transmission Control Protocol (TCP)

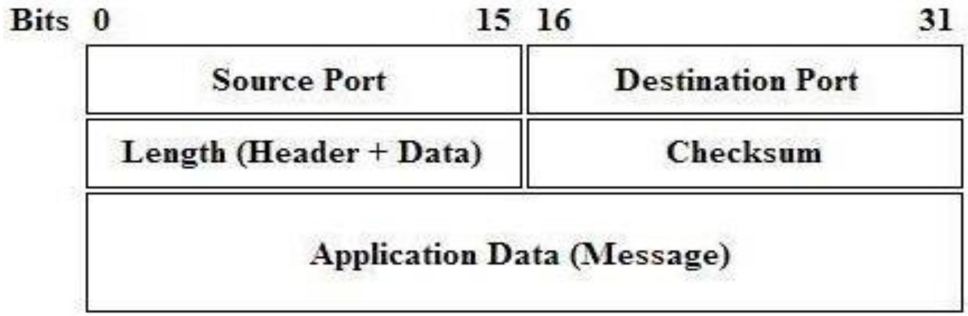
- It designed to handle multiplexing of process communications on the host, as well as reliability and sequencing.
- Includes a header (no footer)
- Header + Payload = TCP Segment
- Connection-oriented
- Handles sequencing
- Reliable



Bit 0		Bit 15	Bit 16 Bit 31
Source Port (16)			Destination Port (16)
Sequence Number (32)			
Acknowledgment Number (32)			
Header Length (4)	Reserved (6)	Code Bits(6)	Window (16)
Checksum (16)			Urgent (16)
Options (0 or 32 If Any)			
Data (Varies)			

User Datagram Protocol

- Unreliable
- Connectionless
- Port numbers range from 0 to 65535
- Includes a header (no footer)
- Header plus payload is called a UDP datagram



Bits	0 15	16 31
	Source Port	Destination Port
	Length (Header + Data)	Checksum
	Application Data (Message)	

CONCLUSION

- Here we discussed from wires to routers to web proxies to DNS servers, there are innumerable potential sources of network-based evidence.

- In this chapter, we reviewed common classes of network devices and discussed the types of evidence typically found on each, and the value for forensic investigators.

- We discussed the Internet Protocol Suite and highlighted key features of IPv4, IPv6, TCP, and UDP

- We followed OSI models

- Your mileage will vary based on the specific devices and communications protocols involved in each investigation

Thank you

Q/A