CYBER FORENSICS

CS6004

Syllabus

UNIT I	**NETWORK LAYER SECURITY & TRANSPORT LAYER SECURITY**
UNIT II	**E-MAIL SECURITY & FIREWALLS**
UNIT III	**INTRODUCTION TO COMPUTER FORENSICS**
UNIT IV	**EVIDENCE COLLECTION AND FORENSICS TOOLS**
UNIT V	**ANALYSIS AND VALIDATION**

CYBER FORENSICS

- **Cyber:** Computers, Information technology
- **Forensics :** Techniques to detect crime

- Resource Centre for Cyber Forensics (RCCF), Centre For Development Of Advanced Computing,(CDAC)

CYBER FORENSICS

- **Cyber Crimes**
  - Illegal activities committed using computer
  - Targeting
    - Computer
    - Network
    - Operations
  - Against
    - A person
    - An organization
    - A government
- **Cyber forensics**
  - Computer forensics or digital forensics
  - A process of extracting information and data from computers to serve as digital evidence to prove and legally prosecute cyber crime

CYBER FORENSICS

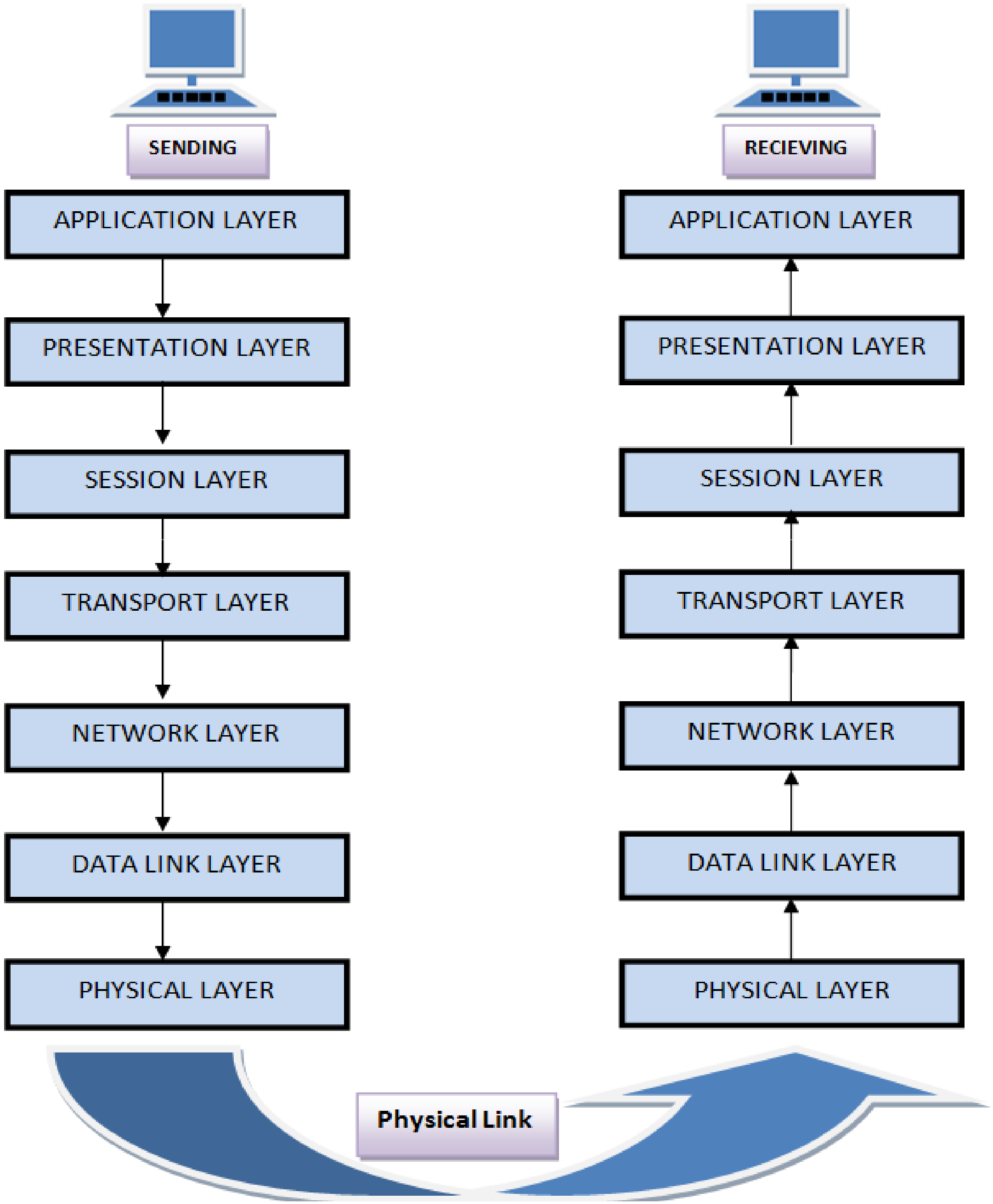
- There are several computer forensics certifications
  - ISFCE
  - DFIP
  - IACRB
  - IACIS
- Asian School of Cyber Laws
  - Offers international level certifications
  - In Digital Evidence Analysis and in Digital Forensic Investigation
  - Online as well as class room mode
- Proprietary certifications by commercial companies
  - For example, Guidance Software offering the (EnCE) certification on their tool EnCase
  - AccessData offering (ACE) certification on their tool FTK
  - PassMark Software offering (OCE) certification on their tool OSForensics
  - X-Ways Software Technology offering (X-PERT) certification for their software, X-Ways Forensics

Network Model

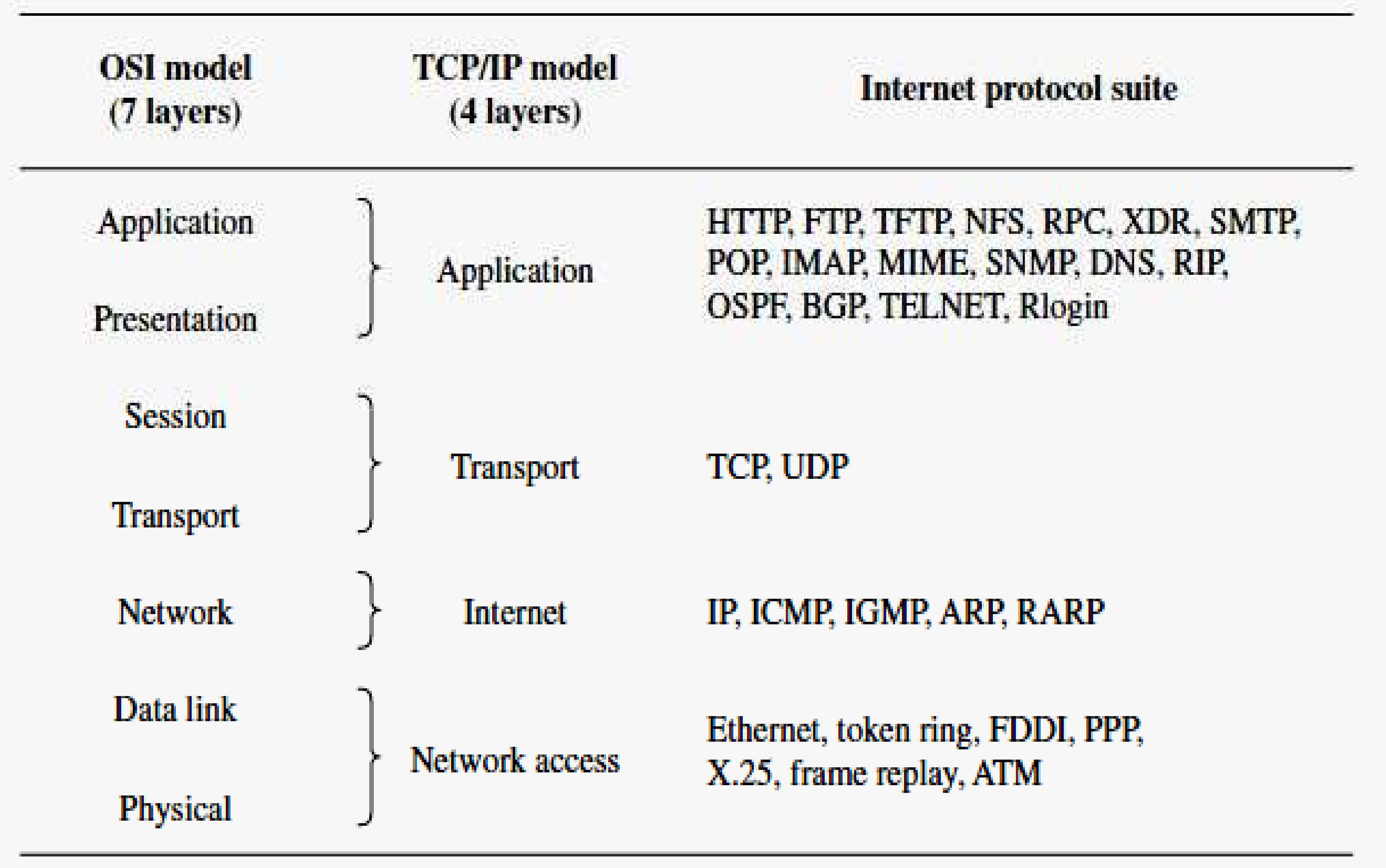
ISO/OSI Model in Communication Networks

- International Organisation for Standardisation (ISO)
- Open System Interconnect (OSI)
- Developed and published in 1982

ISO/OSI Model



TCP/IP Model

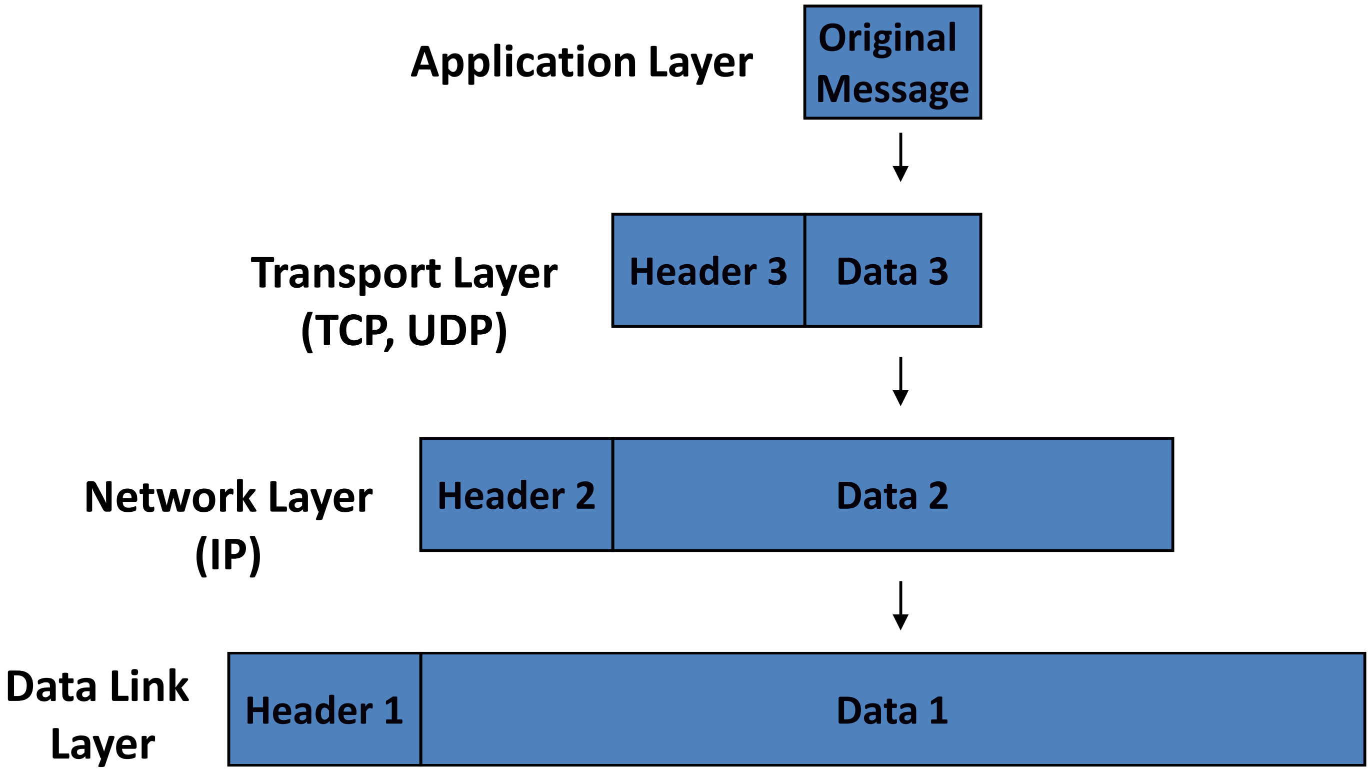


OSI model (7 layers)	TCP/IP model (4 layers)	Internet protocol suite
Application Presentation	Application	HTTP, FTP, TFTP, NFS, RPC, XDR, SMTP, POP, IMAP, MIME, SNMP, DNS, RIP, OSPF, BGP, TELNET, Rlogin
Session Transport	Transport	TCP, UDP
Network	Internet	IP, ICMP, IGMP, ARP, RARP
Data link Physical	Network access	Ethernet, token ring, FDDI, PPP, X.25, frame replay, ATM

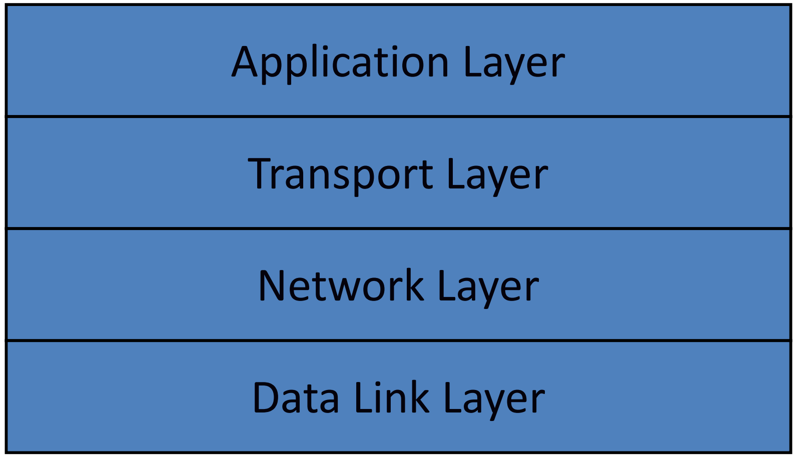
Figure 1.3 The TCP/IP model and Internet protocol suite.

TCP/IP Model

Encapsulation of Data for Network Delivery



Security at What Level?



Application Layer	PGP, Kerberos, SSH, etc.
Transport Layer	SSL
Network Layer	IP Security
Data Link Layer	Hardware encryption

Protocol

- Set of rules
- Governing the way data will be transmitted and received over data communication networks
- Must be
  - Reliable
  - Error-free communication of user data
  - Error free network management function

- Security Protocols
  - Network Layer -- IPSec
  - Transport Layer -- SSL and TSL

Cryptography

- TCP/IP communication – secured through cryptography
- Cryptographic methods and protocols main purposes are in securing communication on the Internet

  Eg:

  - IPsec for network layer security
  - SSL and TLS for HTTP Web traffic at transport layer
  - S/MIME and PGP for e-mail at application layer

Cryptographic Protocols

Network layer security:

- IPSec Protocol
- IP Authentication Header
- IP ESP
- Key Management Protocol for IPSec

Transport layer Security:

- SSL protocol (Secure Sockets Layer)
- TLS Protocol (Transport Layer Security)

Application layer Security:

- PGP
- S/MIME (Secure/Multipurpose Internet Mail Extension (S/MIME))