CSCN4021
Cyber Crime
Investigations

Presearch consideration & Acquisition

Course Co-Ordinator

Dr. Jayakumar

Assistant Professor

Department of Computer Science and Engineering
Galgotias University

2020/10/2

Outline

- Digital Evidence and Recovery
  - Digital Evidence on Computer Systems
  - Digital Evidence on Networks
- Challenges

Computer (or Cyber) Forensics

(Warren. G. Kruse ii and Jay G. Heiser, 2002, *Computer Forensics – Incident Response Essentials*, Addison Wesley)

- Methodology:
  - Acquire the evidence without altering or damaging the original.
  - Authenticate that the recovered evidence is the same as the original seized.
  - Analyze the data without modifying it.

Category of Digital Evidence

- Hardware
- Software
  - Data
  - Programs

Digital Evidence

- Definition
  - Digital data that can establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its perpetrator.(source: Casey, Eoghan, *Digital Evidence and Computer Crime: Forensic Science, Computer and the Internet*,Academic Press, 2000.)
  - Categories
    - Text
    - Audio
    - Image
    - Video

Where Evidence Resides

- Computer systems
  - Logical file system
    - File system
      - Files, directories and folders, FAT, Clusters, Partitions, Sectors
    - Random Access memory
    - Physical storage media
      - magnetic force microscopy can be used to recover data from overwritten area.
  - Slack space
    - space allocated to file but not actually used due to internal fragmentation.
  - Unallocated space

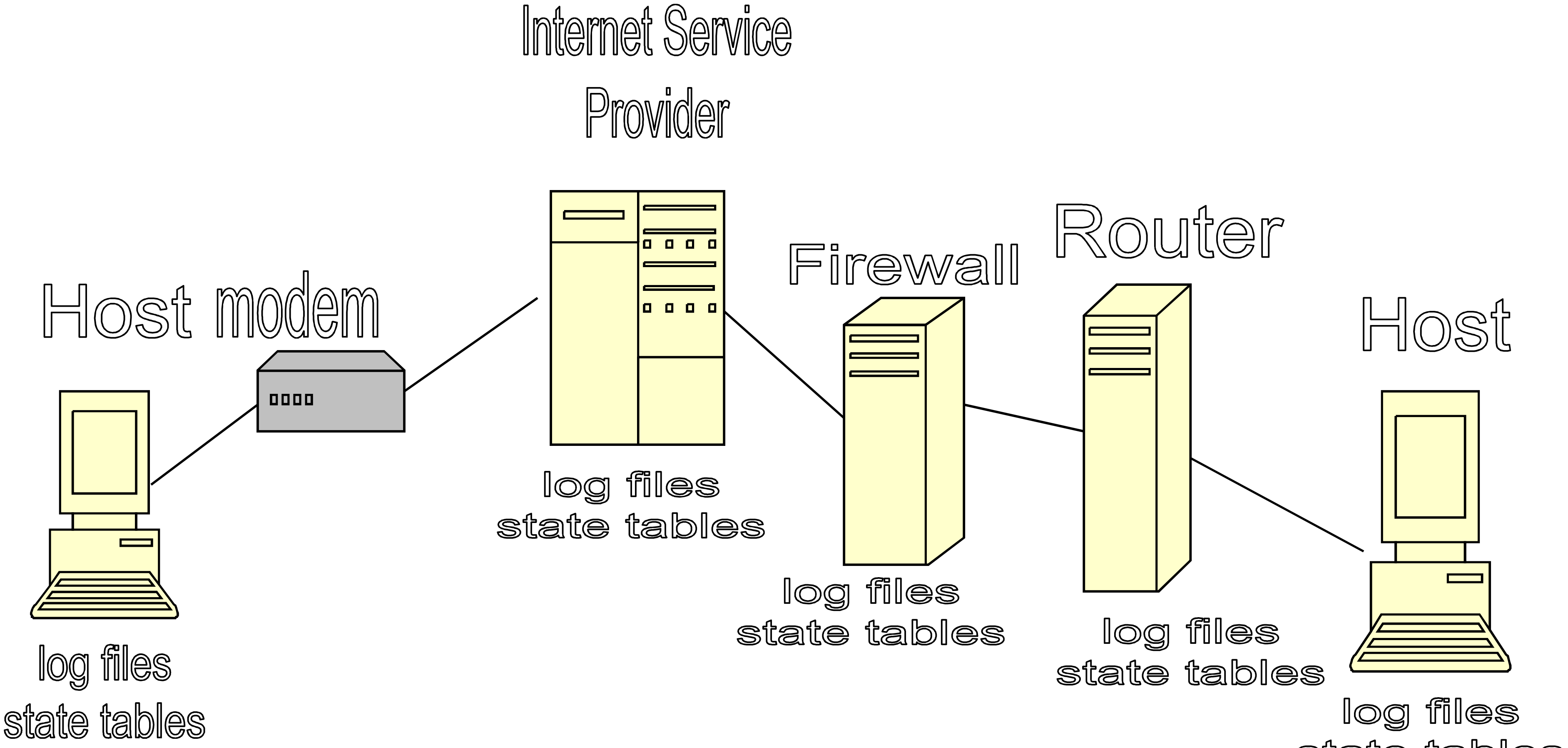
Where Evidence Resides (continued)

- Computer networks.
  - Application Layer
  - Transportation Layer
  - Network Layer
  - Data Link Layer

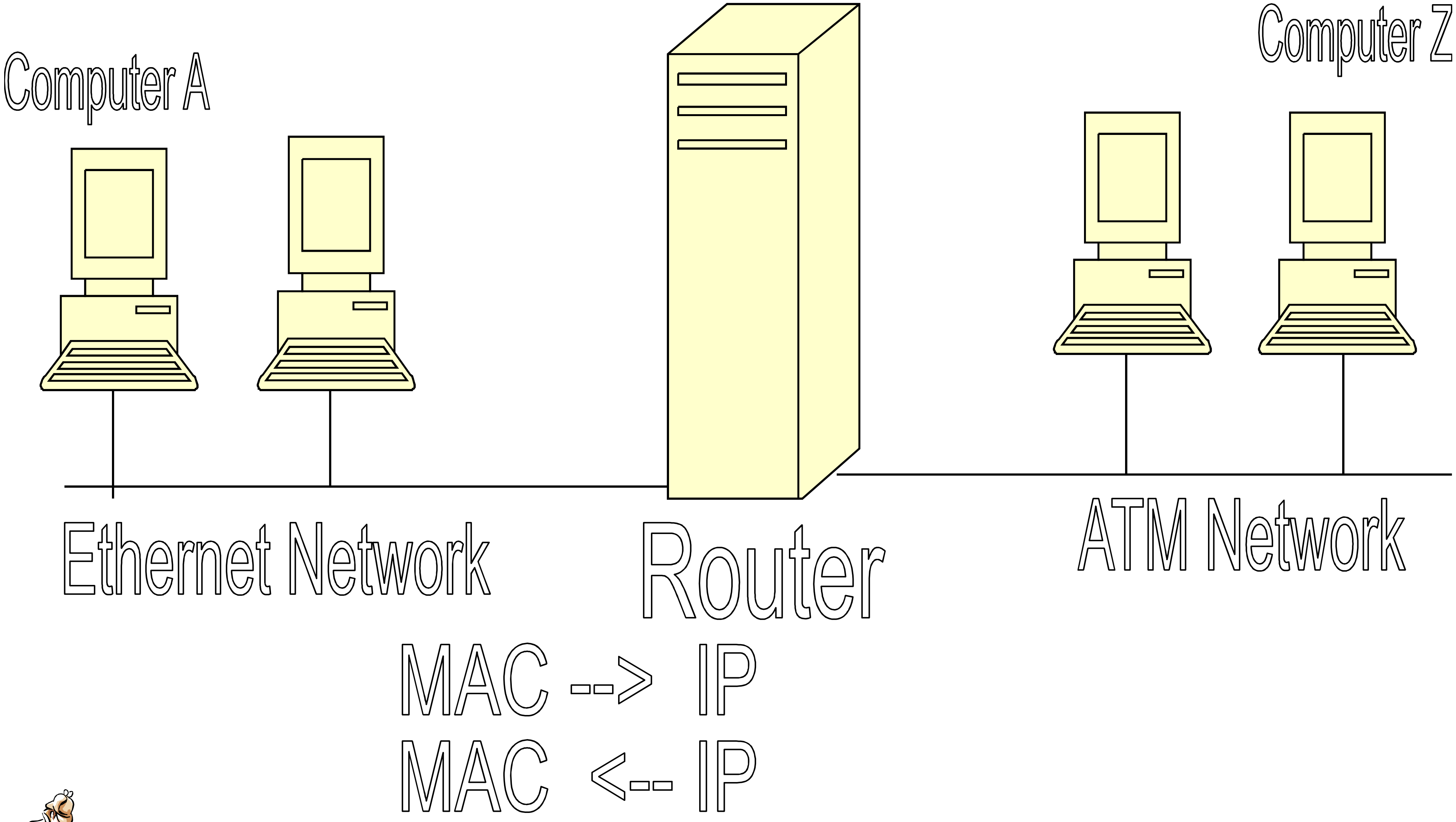
Evidence on Application Layer

- Web pages, Online documents.
- E-Mail messages.
- News group archives.
- Archive files.
- Chat room archives.
- …

Evidence on Transport and Network Layers



Evidence on the Data-link and Physical Layers



Challenges of Computer Forensics (continued)

- How to collect the specific, probative, and case-related information from very large groups of files?
  - Link analysis
  - Visualization
- Enabling techniques for lead discovery from very large groups of files:
  - Text mining
  - Data mining
  - Intelligent information retrieval

Challenges of Computer Forensics (continued)

- Computer forensics must also adapt quickly to new products and innovations with valid and reliable examination and analysis techniques.