Two approaches to build an IDS

Signature-based IDS

Have pre-defined malicious message pattern

➡ Relies on a signature database

Heuristic-based

Builds a model of acceptable message exchange patterns

➡ Relies on machine learning

(Network) Intrusion Detection Systems

IDS - Intrusion detection systems performs deep packet inspection

- Looks at the headers
- Look at packet contents (payload)
- Looks at the packet fragmentation