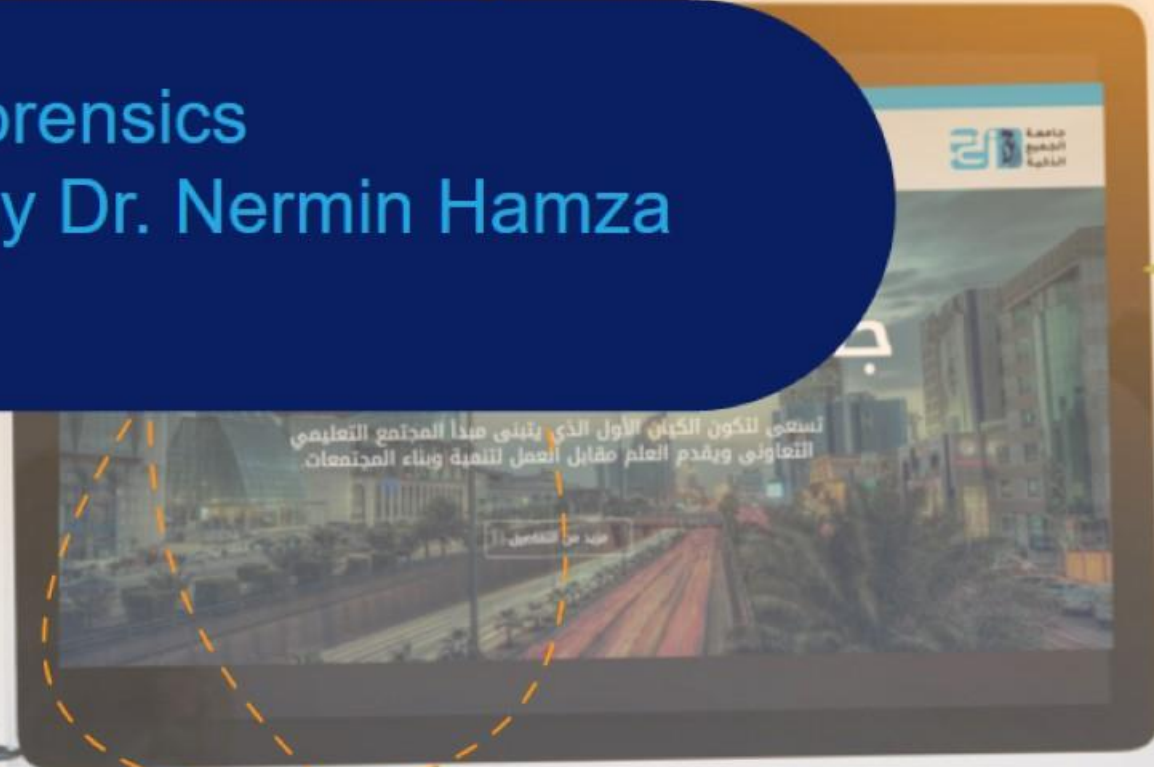


Network Forensics

Prepared by Dr. Nermin Hamza

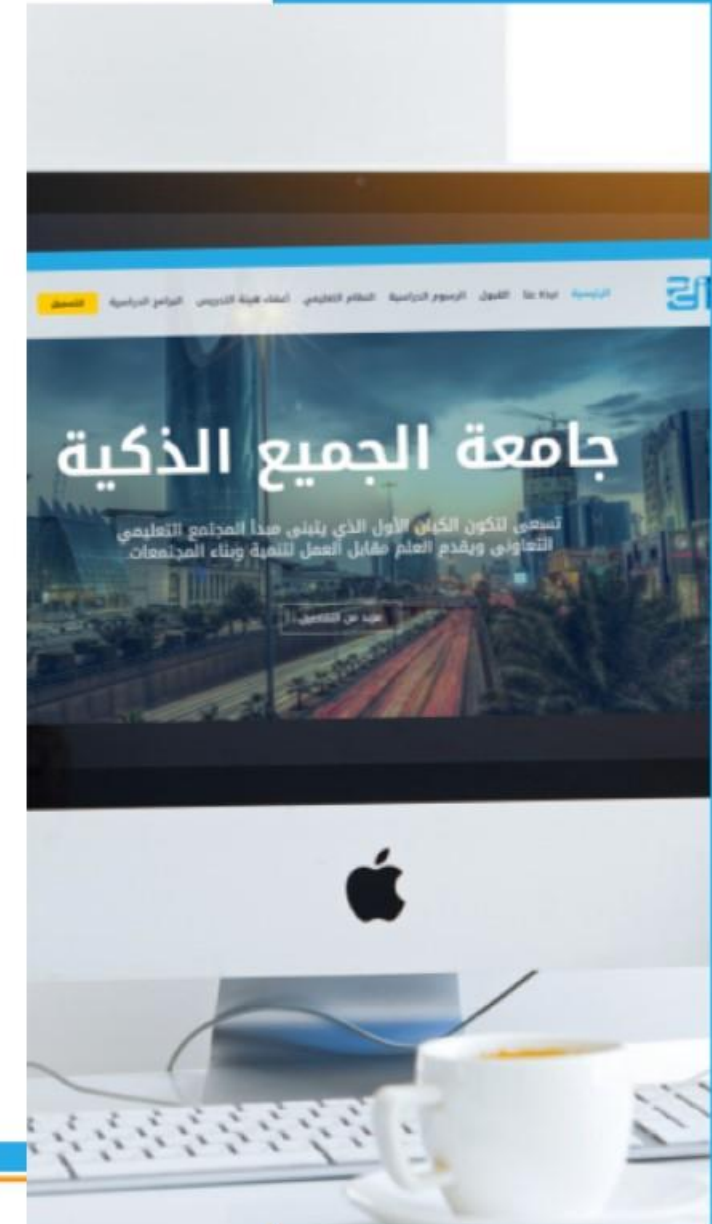
Lecture 6



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

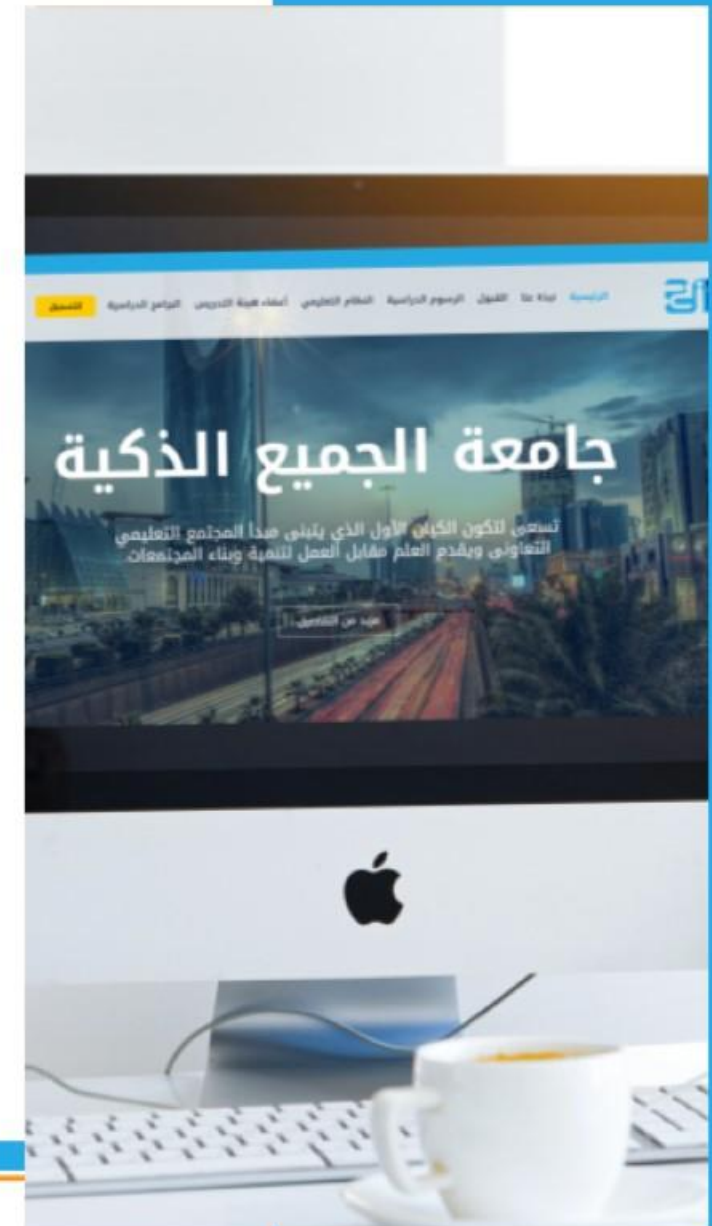
CYB 770
IT Forensics

- Overview of the OSI Model
- Network Addresses
- Log
- Gathering Evidence From ARP Table
- DHCP logging
- Sniffing
- Firewall
- IDS



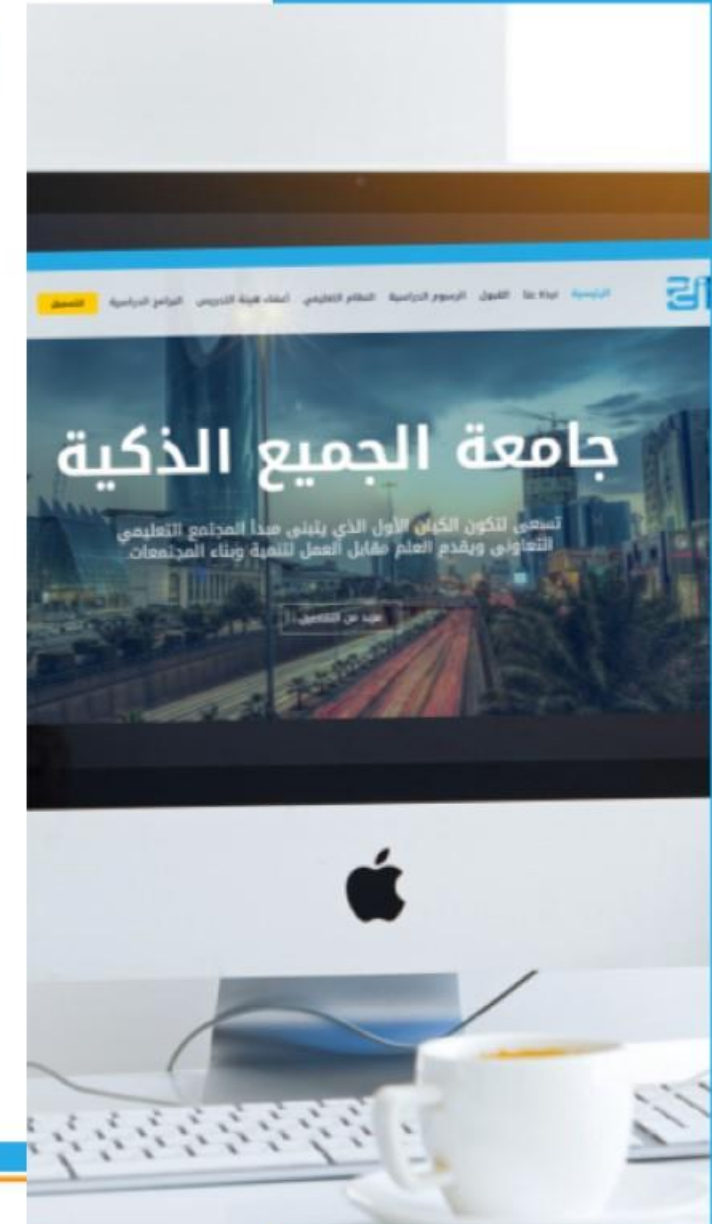
Lecture 6

Overview of the OSI Model



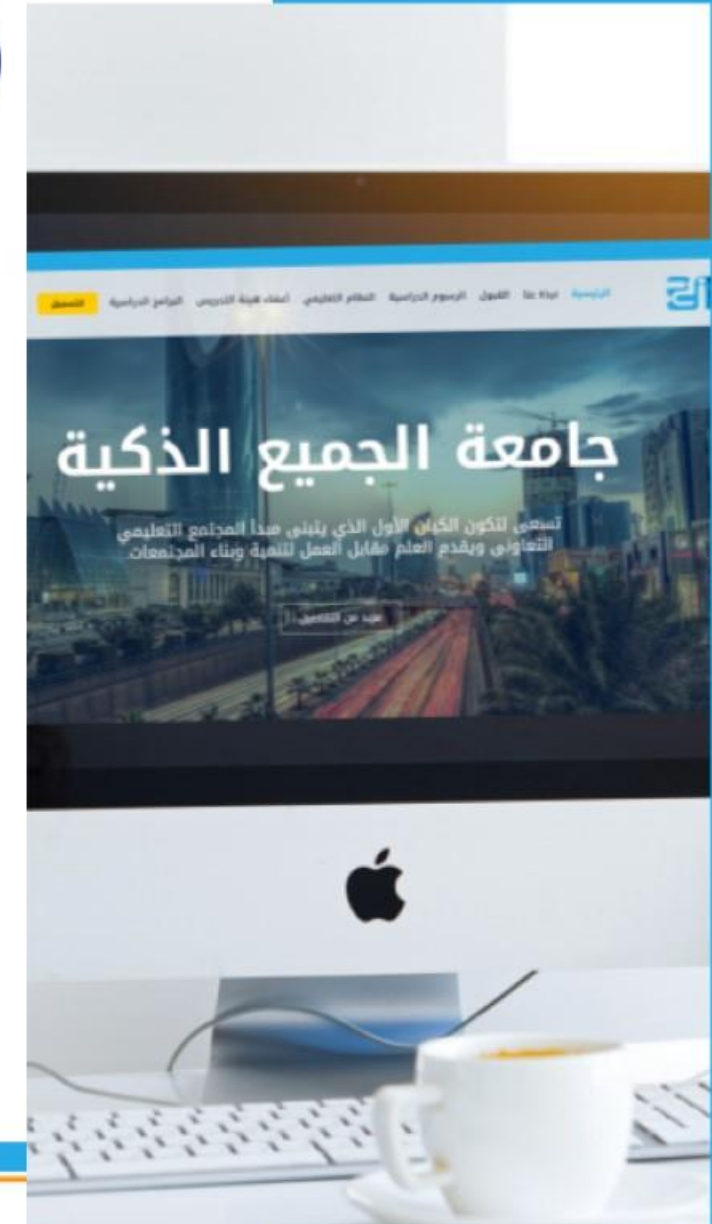
Overview of the OSI Model

- In 1984 the International Standards Organization developed the Open Systems Interconnect (OSI) model.
- The model is designed to provide order by specifying a specific hierarchy in which each layer builds upon the output of each adjacent layer.
- The model is still used today as a guide in describing the operation of a networking environment.



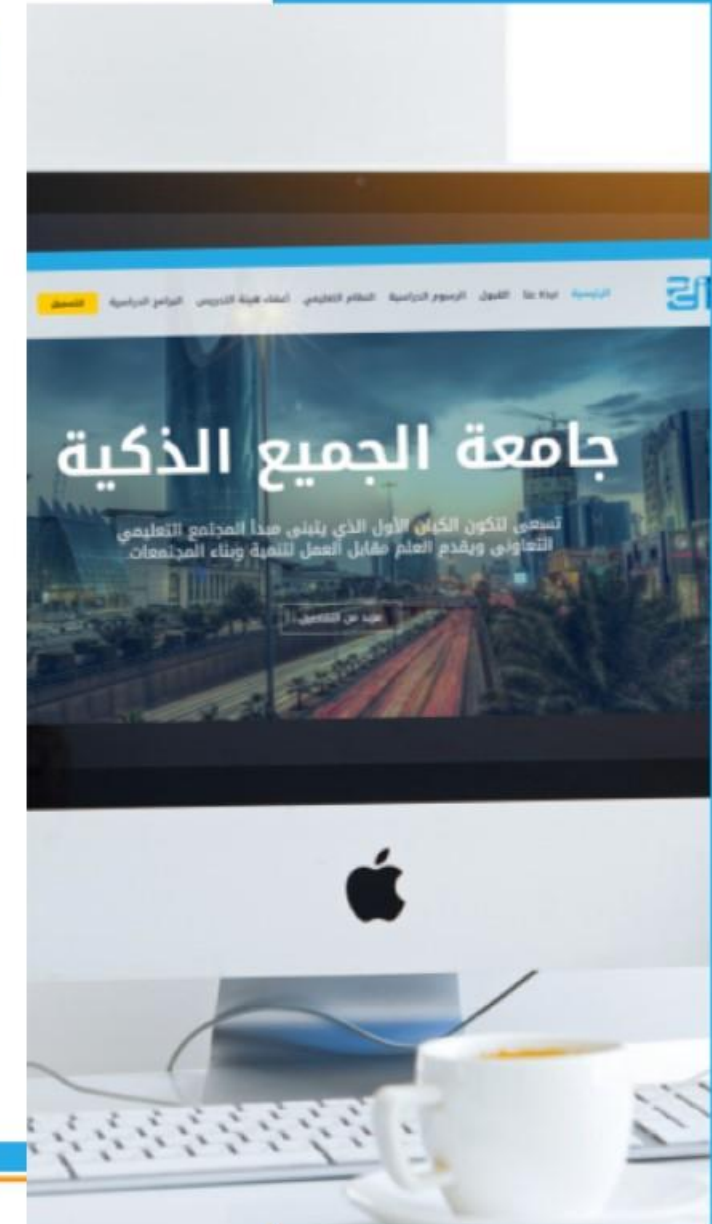
7 Layers of the OSI Model

Application	• End User layer • HTTP, FTP, IRC, SSH, DNS
Presentation	• Syntax layer • SSL, SSH, IMAP, FTP, MPEG, JPEG
Session	• Synch & send to port • API's, Sockets, WinSock
Transport	• End-to-end connections • TCP, UDP
Network	• Packets • IP, ICMP, IPSec, IGMP
Data Link	• Frames • Ethernet, PPP, Switch, Bridge
Physical	• Physical structure • Coax, Fiber, Wireless, Hubs, Repeaters



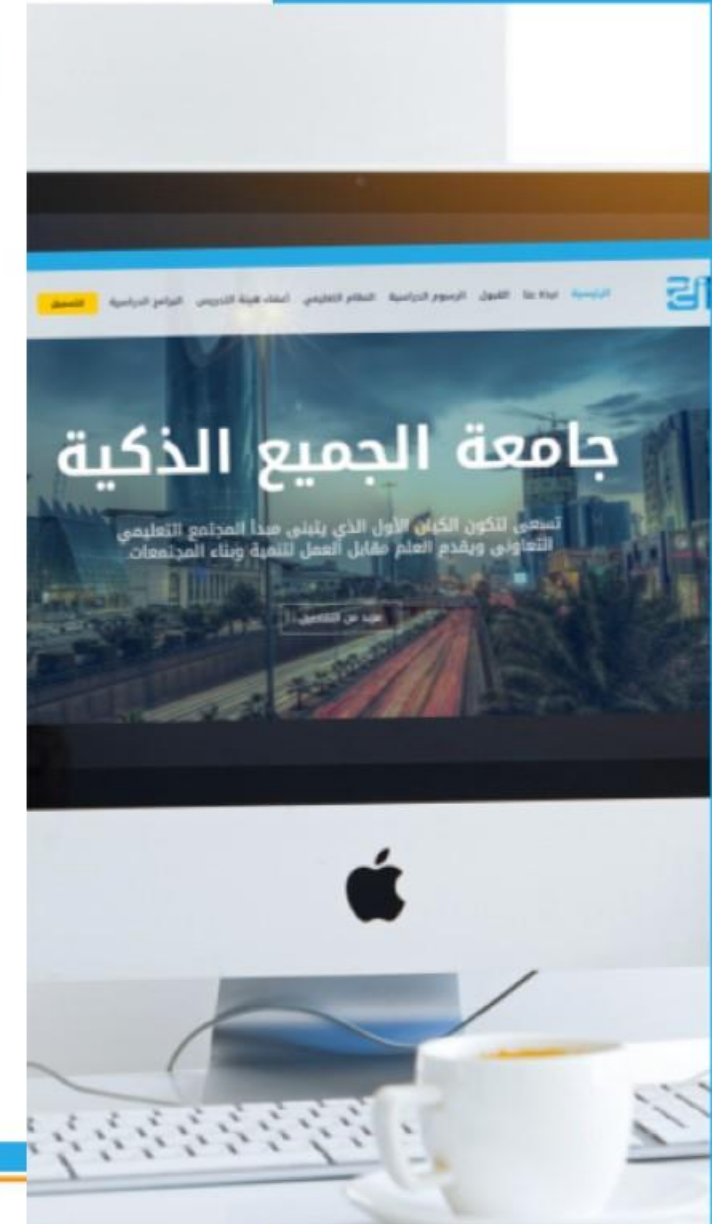
The Physical Layer

- Layer 1 is known as the physical Layer. At Layer 1, bit-level communication takes place.
- The bits have no defined meaning on the wire, but the physical layer defines how long each bit lasts and how it is transmitted and received.



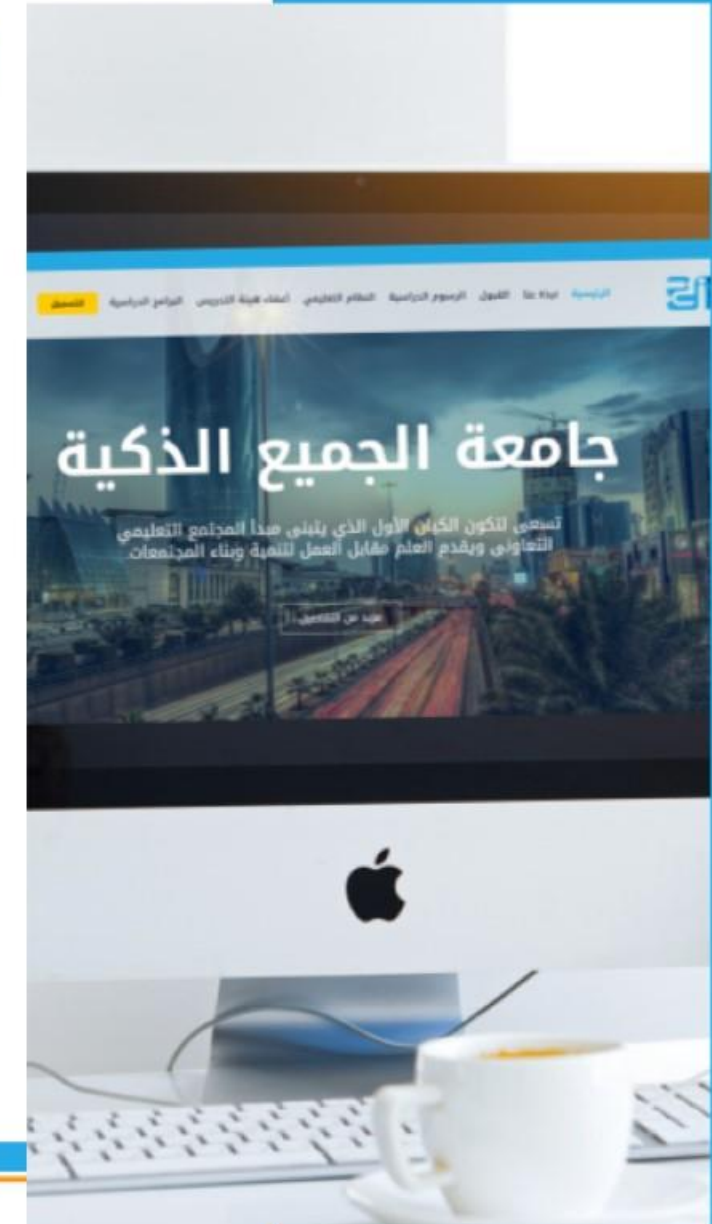
The Data Link Layer

- Layer 2 is known as the data link layer.
- The data link layer is responsible for formatting and organizing the data before sending it to the physical layer.
- The data link layer organizes the data into frames. A frame is a logical structure in which data can be placed.
- When a frame reaches the target device, the data link layer is responsible for stripping off the data frame and passing the data packet up to the network layer.
- The main address is the media access control layer (MAC).



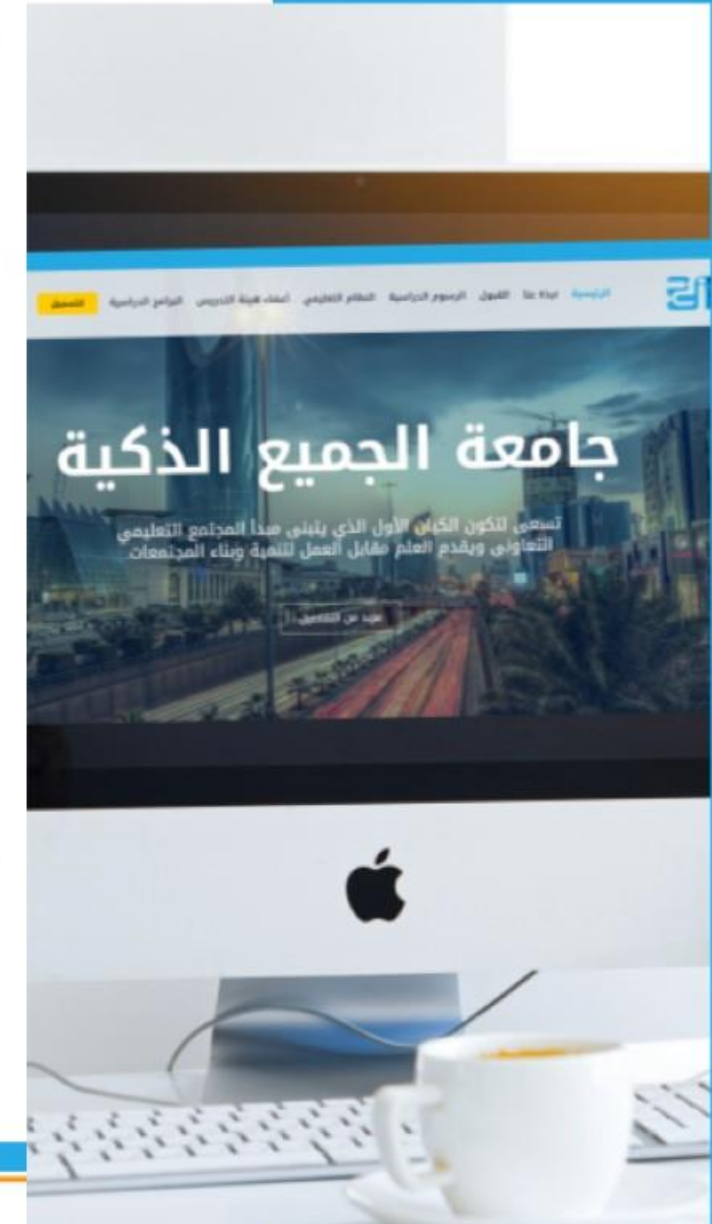
The Network Layer

- Layer 3, the network layer, is concerned with logical addressing and routing.
- The network layer is the home of the Internet Protocol (IP), which makes a best effort at delivery of datagrams from their source to their destination.
- (IP4 and IP6)



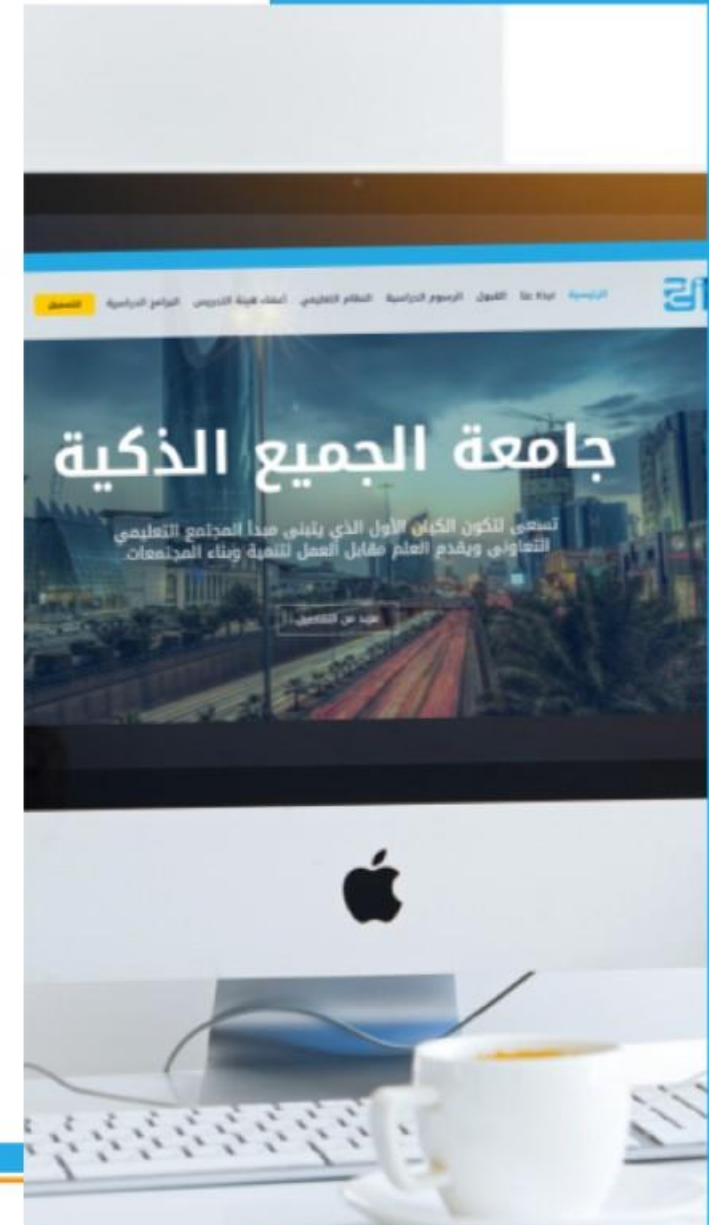
The Transport Layer

- Layer 4 is known as the transport layer, and ensures completeness by handling end-to-end error recovery and flow control.
- Transport-layer protocols include TCP, a connection-oriented protocol.
- It provides reliable communication through the use of handshaking, acknowledgments, error detection, and session teardown and User Datagram Protocol (UDP), a connectionless protocol.
- It offers speed and low overhead as its primary advantage



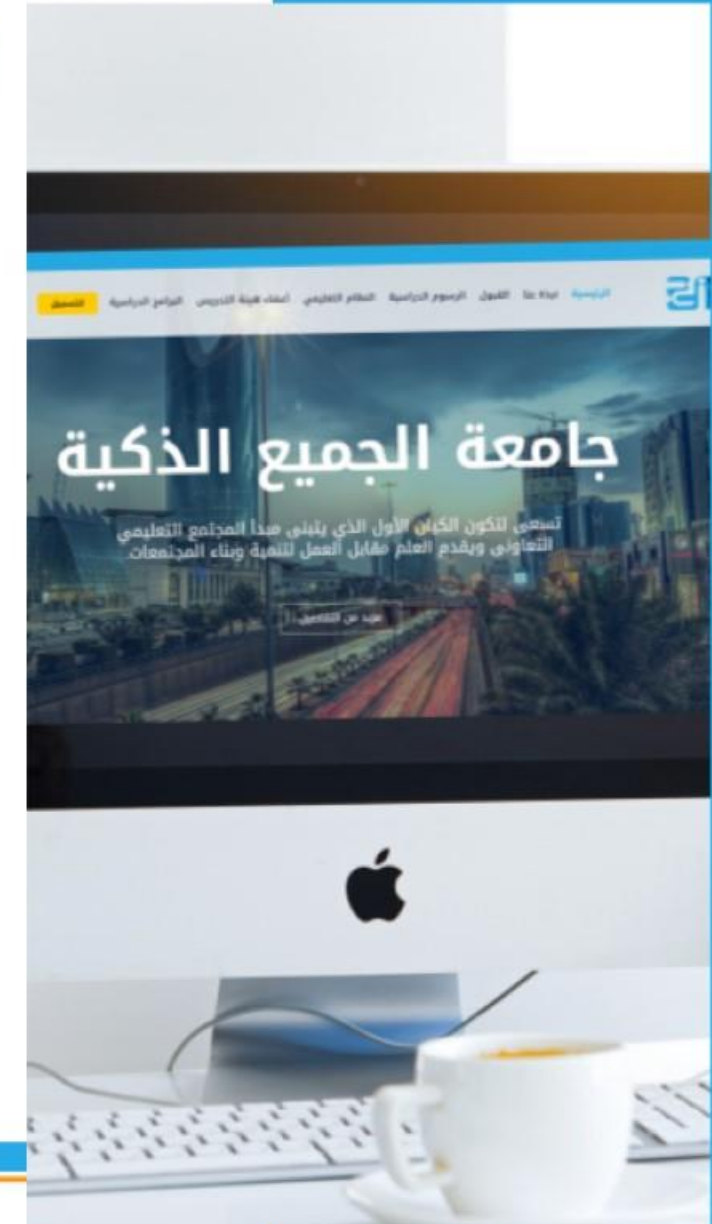
The Session Layer

- Layer 5 is known as the session layer. Its functionality is put to use when creating, controlling, or shutting down a TCP session.
- Session-layer protocols include items such as Remote Procedure Call and Structured Query Language.



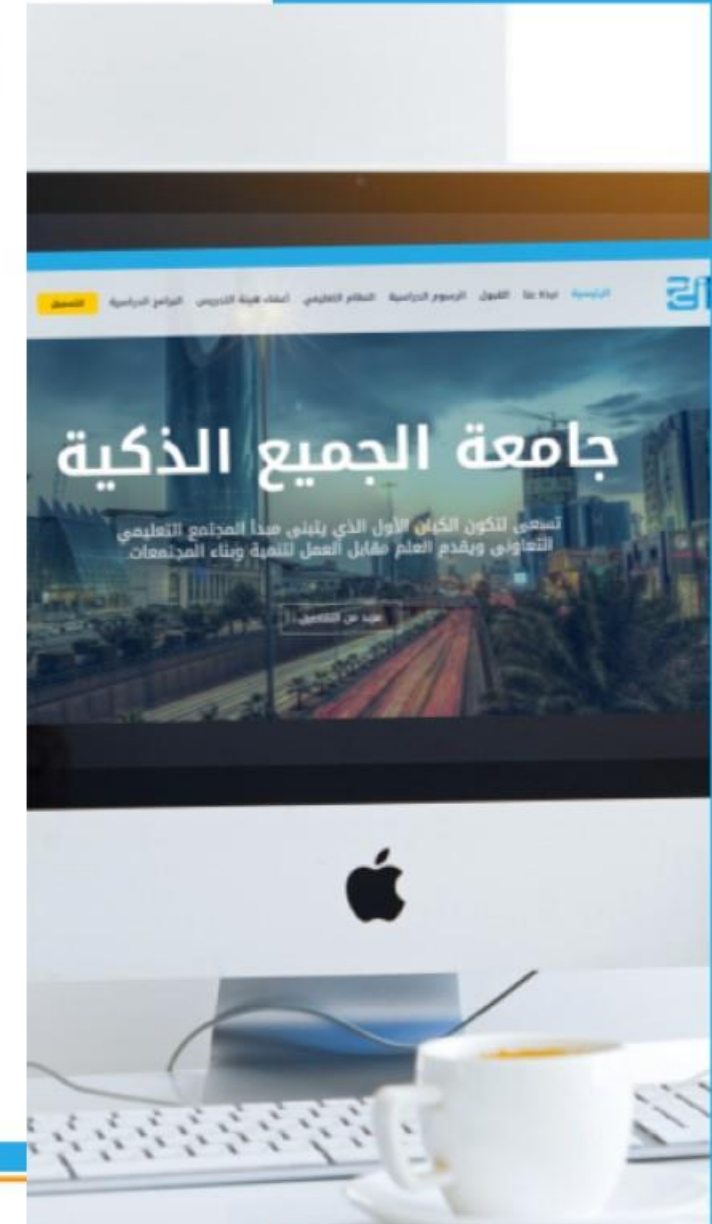
The Presentation Layer

- Layer 6, the presentation layer, is responsible for taking data that has been passed up from lower levels and put it into a format that application layer programs can understand.
- These common formats include ASCII, EBCDIC, and ANSI.



The Application Layer

- Layer 7 is known as the application layer.
- Recognized as the top layer of the OSI model, this layer serves as the window for application services.
- The application layer is one that most users are familiar with as it is the home of e-mail programs, FTP, Telnet, web browsers, office productivity suites, and many other applications.



Overview of the OSI Model

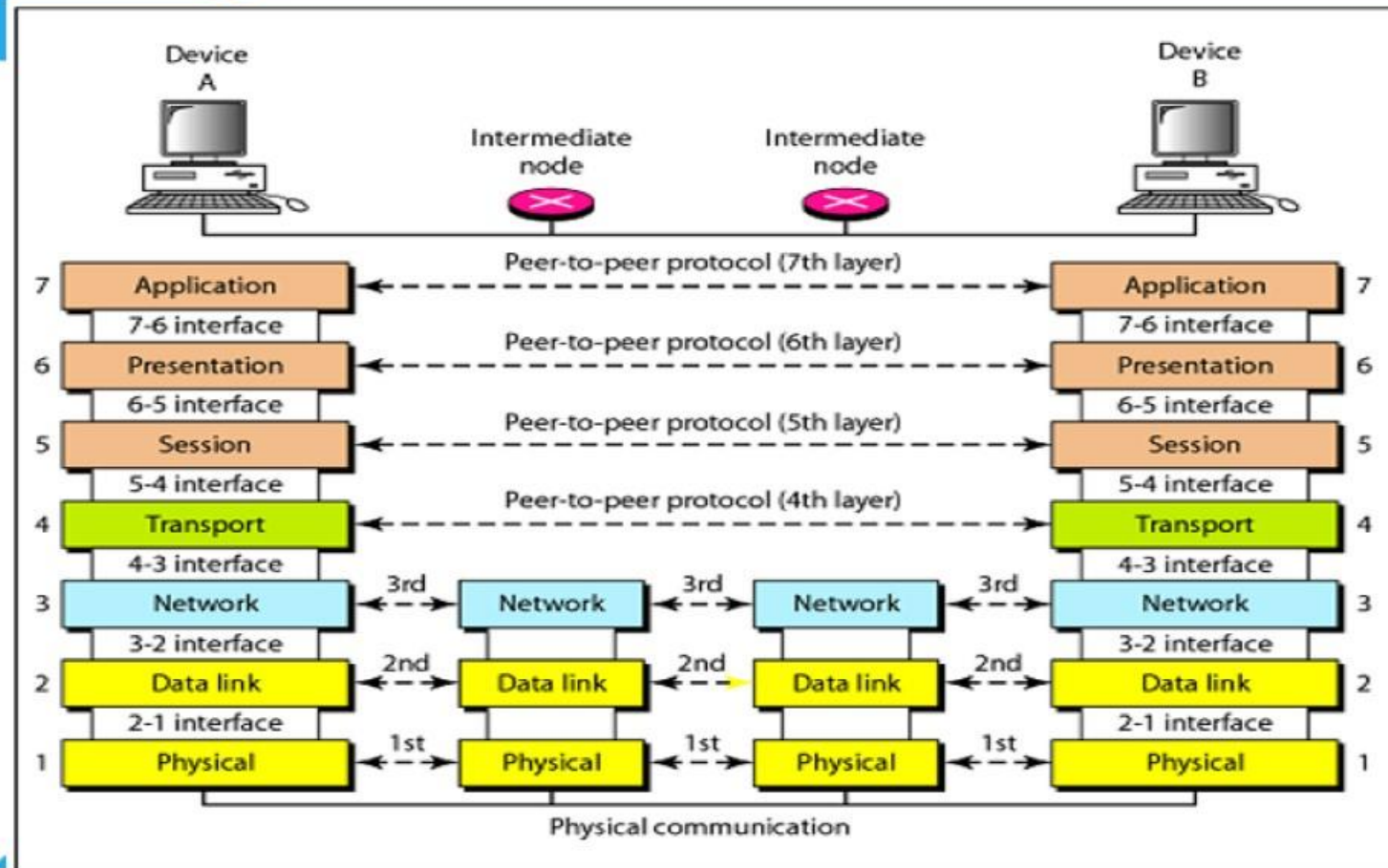
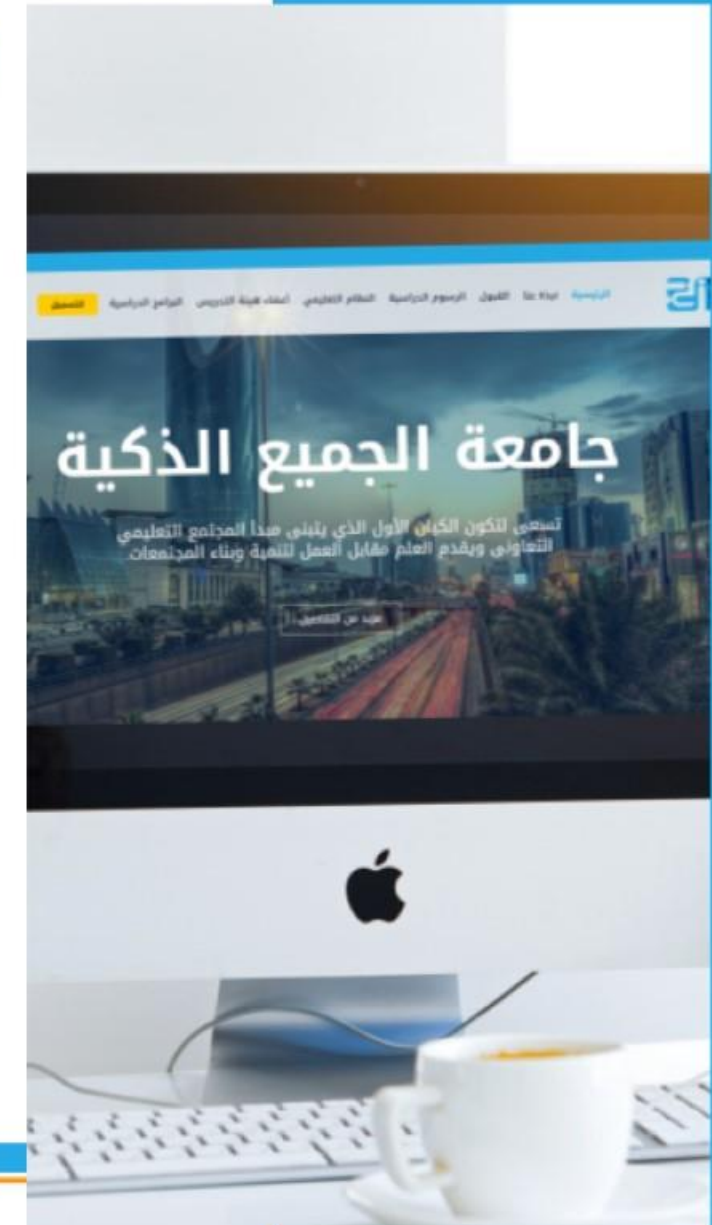
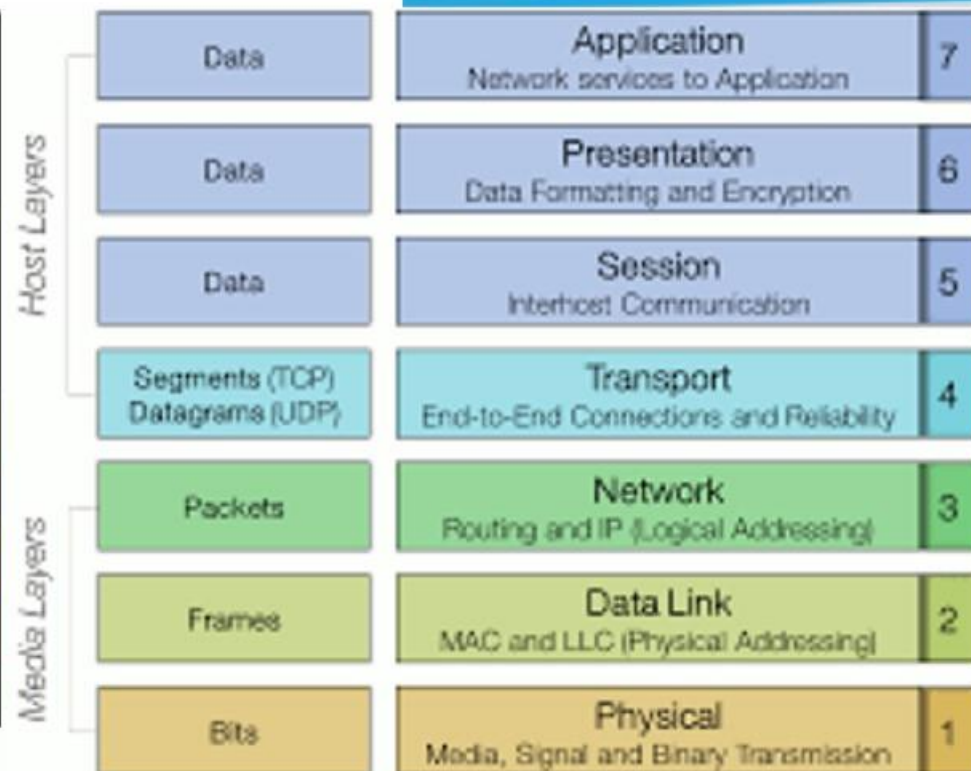


Fig: Communication & Interfaces in the OSI model



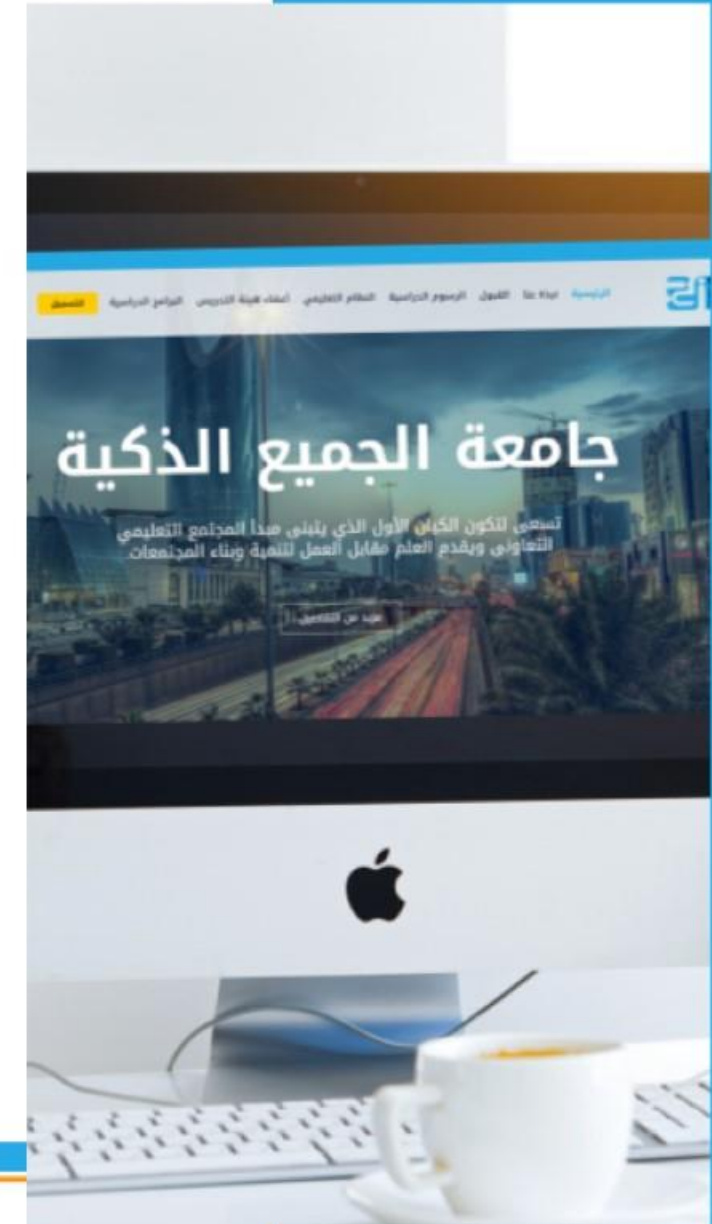
OSI model

Layer	Name	Example protocols
7	Application Layer	HTTP, FTP, DNS, SNMP, Telnet
6	Presentation Layer	SSL, TLS
5	Session Layer	NetBIOS, PPTP
4	Transport Layer	TCP, UDP
3	Network Layer	IP, ARP, ICMP, IPSec
2	Data Link Layer	PPP, ATM, Ethernet
1	Physical Layer	Ethernet, USB, Bluetooth, IEEE802.11



IP Address :

- An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.
- An IP address is a string of numbers separated by periods. IP addresses are expressed as a set of four numbers — an example address might be 192.158.1.38. Each number in the set can range from 0 to 255. So, the full IP addressing range goes from 0.0.0.0 to 255.255.255.255.

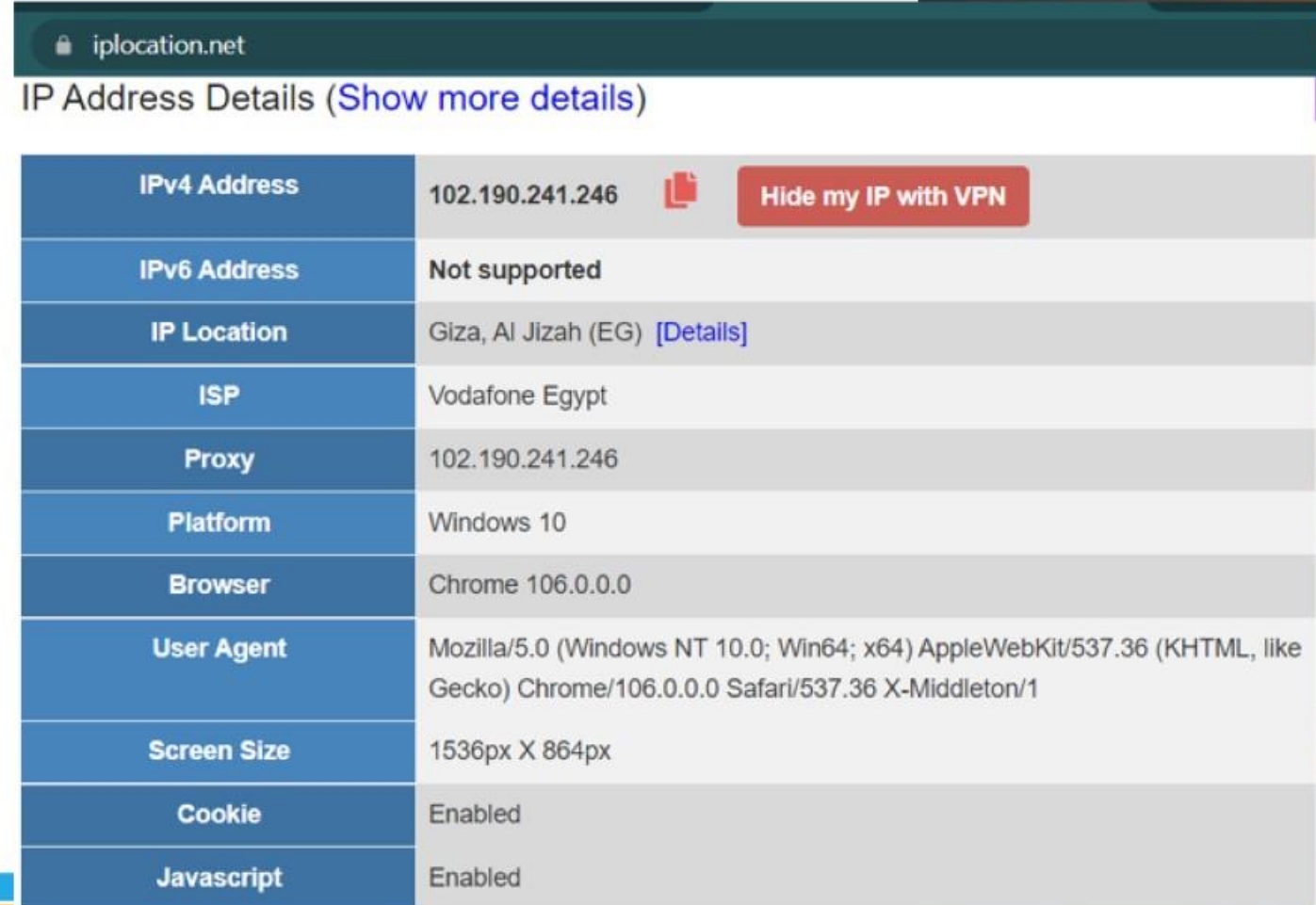


Lecture 6

Network Addresses

Open : <https://www.iplocation.net/>

What is your IP address?

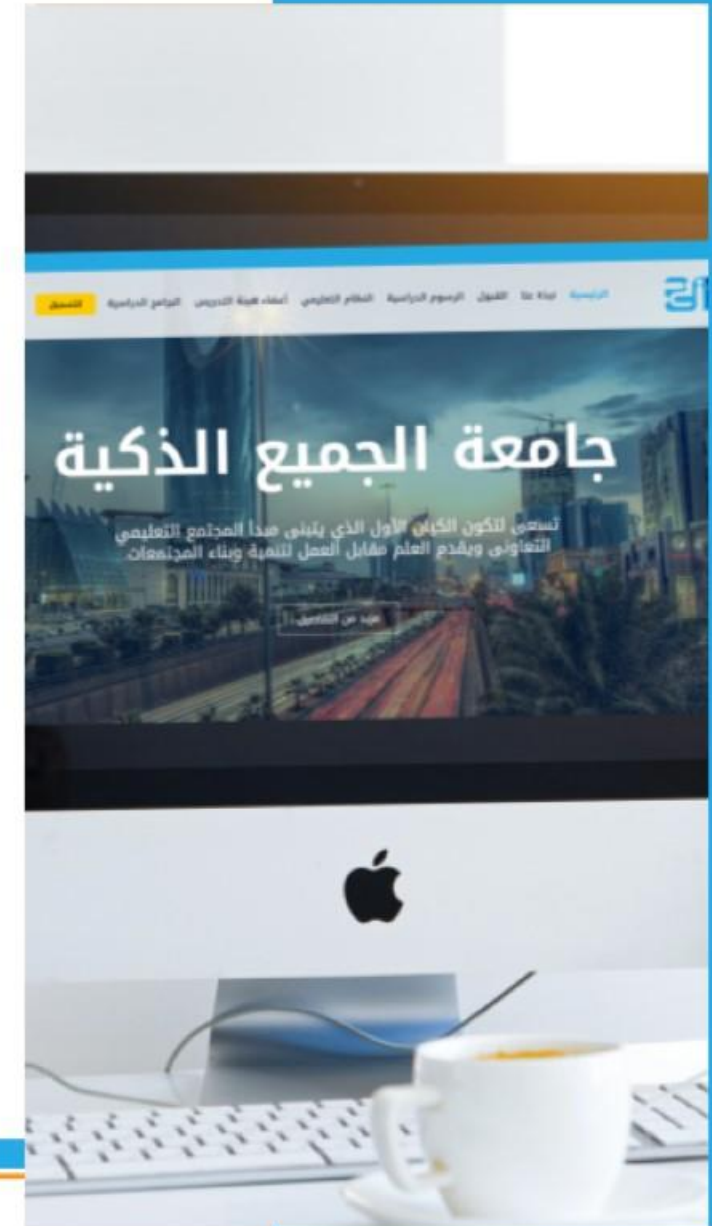


The screenshot shows the iplocation.net website. The browser's address bar displays 'iplocation.net'. Below the address bar, the text 'IP Address Details (Show more details)' is visible. A table lists various system and network details. The first row shows the IPv4 Address as 102.190.241.246, with a red button labeled 'Hide my IP with VPN' next to it. The IPv6 Address is listed as 'Not supported'. The IP Location is 'Giza, Al Jizah (EG)' with a link to '[Details]'. The ISP is 'Vodafone Egypt'. The Proxy is '102.190.241.246'. The Platform is 'Windows 10'. The Browser is 'Chrome 106.0.0.0'. The User Agent is 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36 X-Middleton/1'. The Screen Size is '1536px X 864px'. The Cookie is 'Enabled'. The Javascript is 'Enabled'.

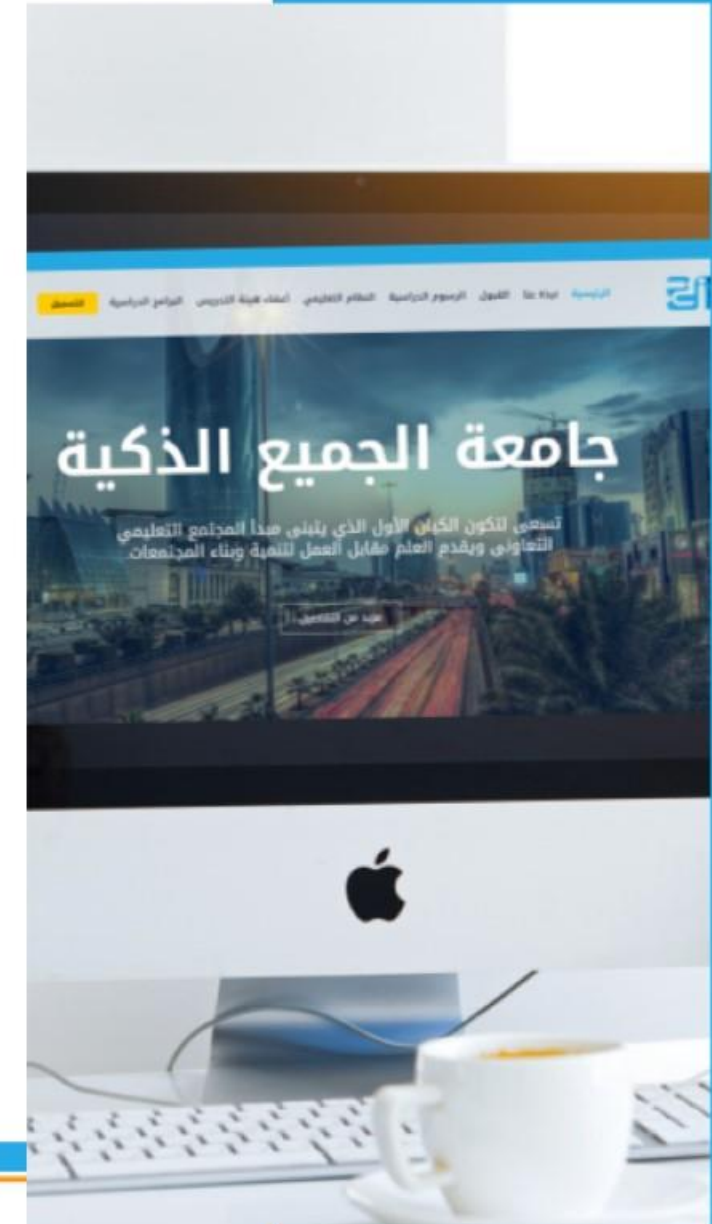
IPv4 Address	102.190.241.246	Hide my IP with VPN
IPv6 Address	Not supported	
IP Location	Giza, Al Jizah (EG)	[Details]
ISP	Vodafone Egypt	
Proxy	102.190.241.246	
Platform	Windows 10	
Browser	Chrome 106.0.0.0	
User Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36 X-Middleton/1	
Screen Size	1536px X 864px	
Cookie	Enabled	
Javascript	Enabled	

Lecture 6

Log

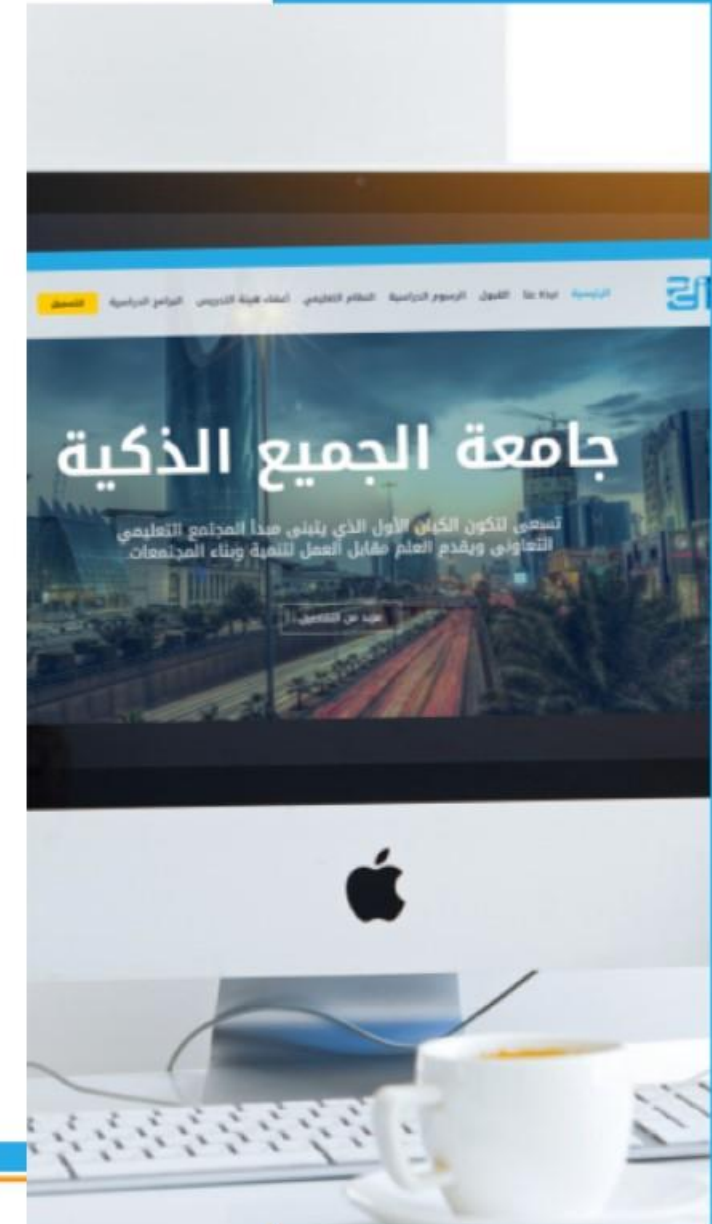


- Network Forensic is the implementation of sniffing , recording , acquisition ,and analysis of network traffic and event log to investigate a network security incident.
- Recording network traffic involving a lot of resources.
- The analysis of recorded data is the most critical and time-consuming task.



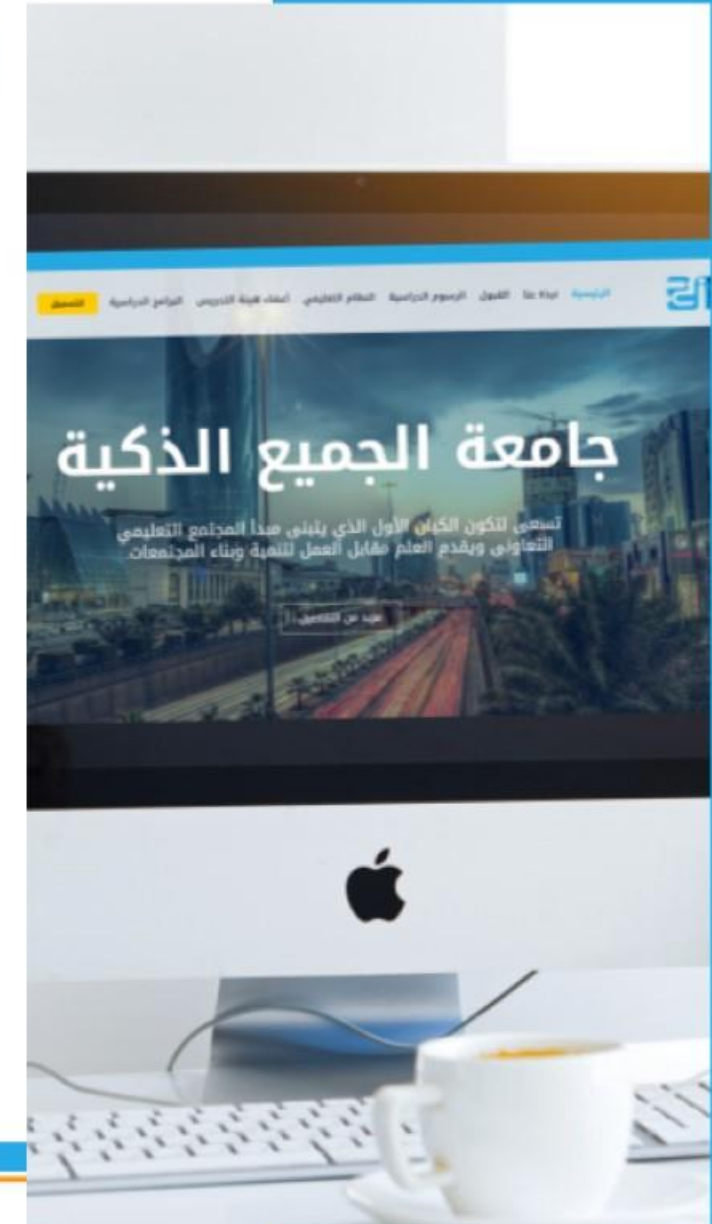
Postmortem and Real time analysis

- postmortem : is some event already happened. Investigator perform analysis on logs to detect something has already occurred in network/device.
- real time analysis: analysis on an ongoing process.



Log File : A log, in a computing context, is the automatically produced and time-stamped documentation of events relevant

- Log files are detailed, text-based records of events within an organization's IT systems.
- They are generated by a wide variety of devices and applications, among them antimalware, system utilities, firewalls, intrusion detection and prevention systems (IDSes/IPSes), servers, workstations and networking equipment.

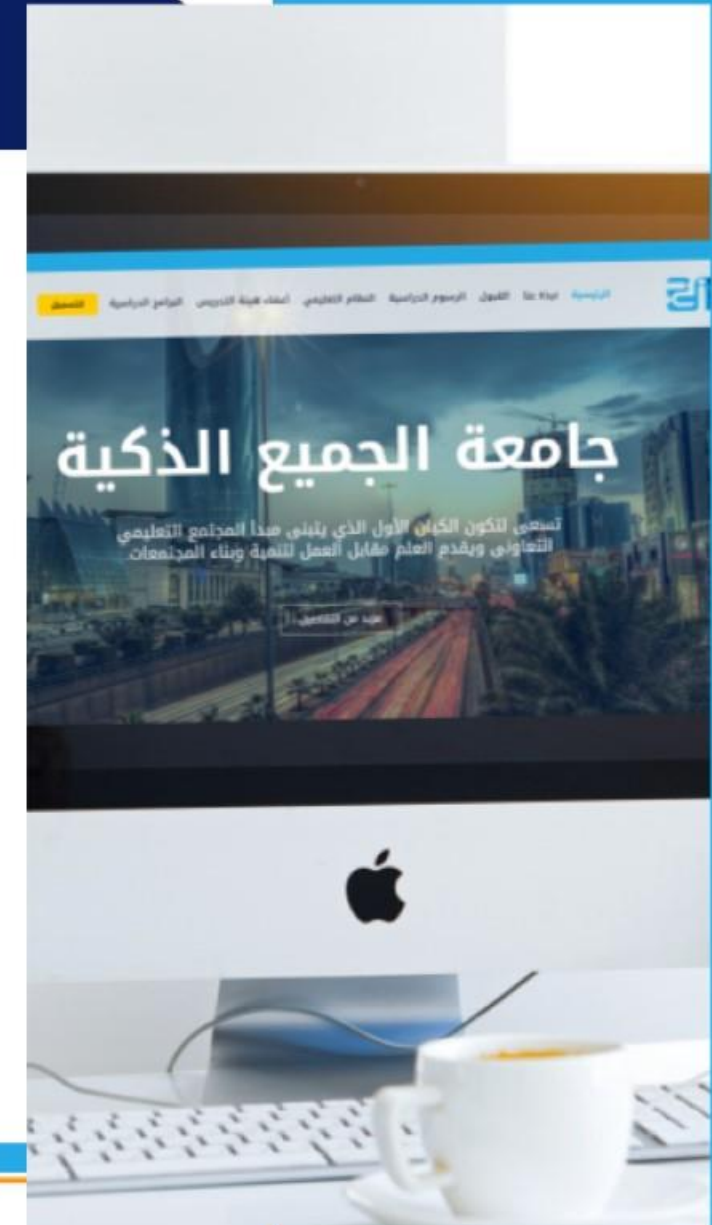


Lecture 6

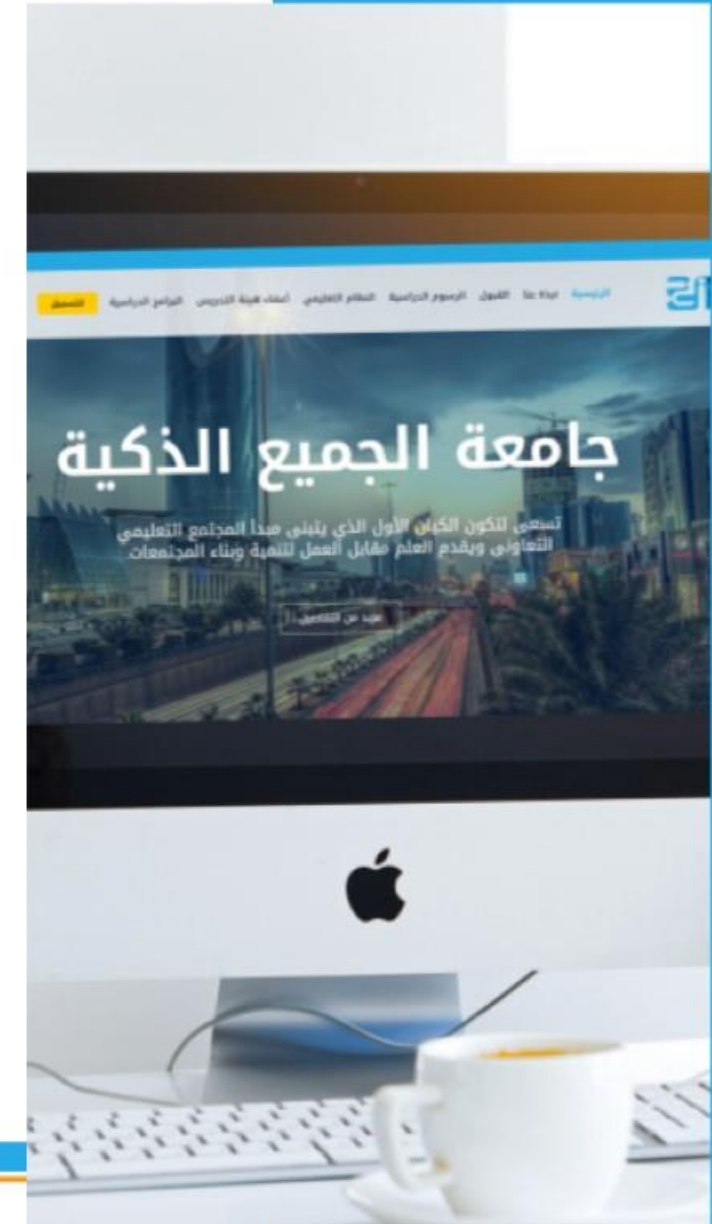
Forensic Network analysis

```
user@host> show log user
```

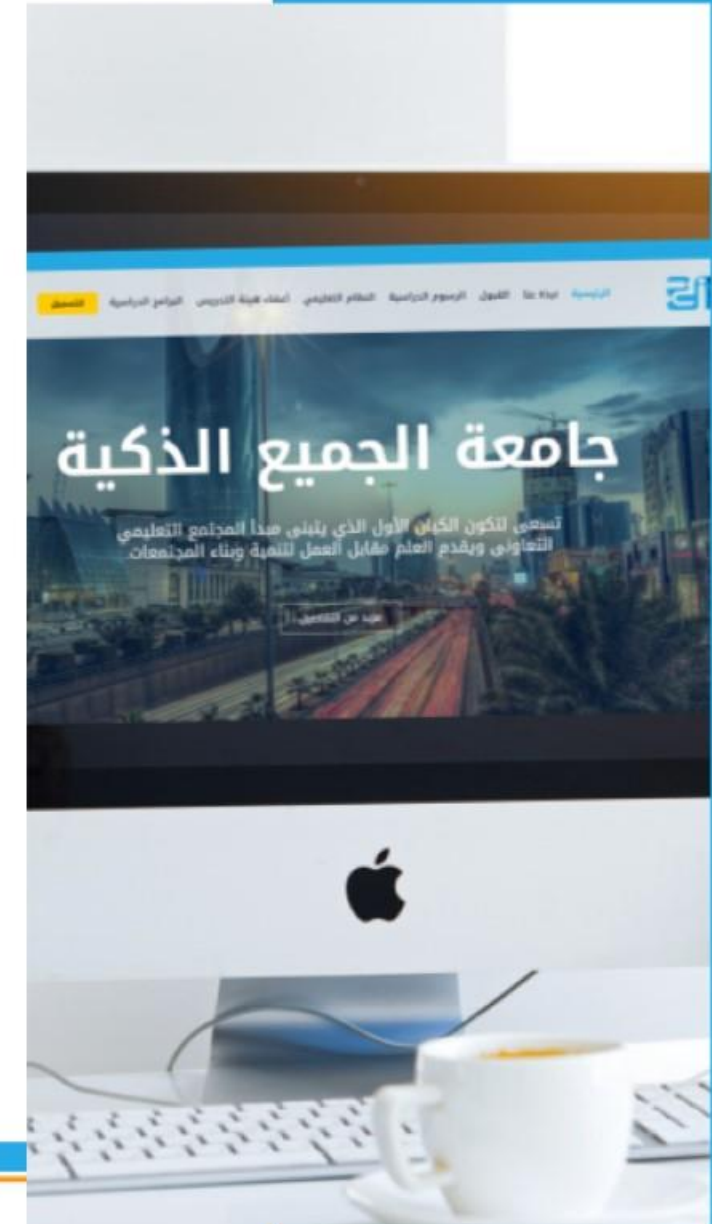
usera	mg2546		Thu Oct 1 19:37	still logged in
usera	mg2529		Thu Oct 1 19:08 - 19:36	(00:28)
usera	mg2518		Thu Oct 1 18:53 - 18:58	(00:04)
root	mg1575		Wed Sep 30 18:39 - 18:41	(00:02)
root	ttyp2	aaa.bbbb.com	Wed Sep 30 18:39 - 18:41	(00:02)
userb	ttyp1	192.0.2.0	Wed Sep 30 01:03 - 01:22	(00:19)



- **Log management** is a continuous process of centrally collecting, parsing, storing, analyzing, and disposing of data to provide actionable insights for supporting troubleshooting, performance enhancement, or security monitoring.
- **Security log management** comprises the generation, transmission, storage, analysis and disposal of security log data, ensuring its confidentiality, integrity and availability.

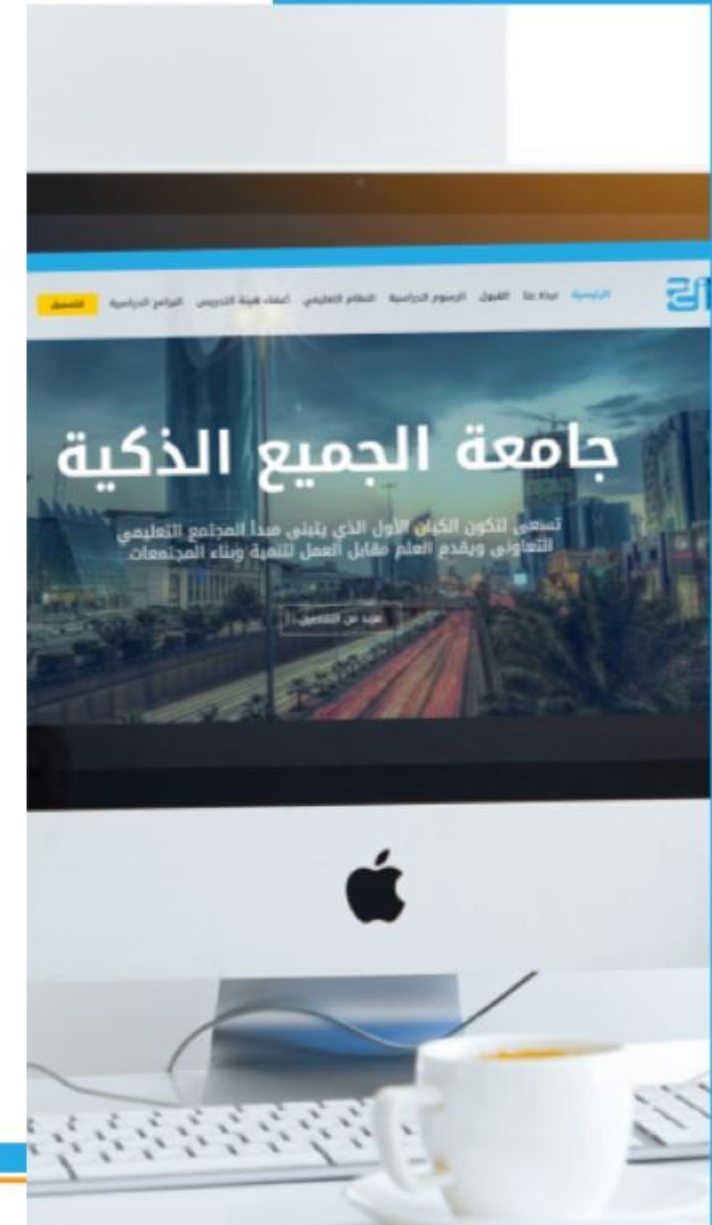


- Because logs come from multiple endpoints and different sources and formats, they require **normalizing**.
- **Normalizing:** Transforming the information into a uniform format for easy searching, comparison and readability is key. The systems and media used to share and store logs must be highly secure with tightly controlled access.

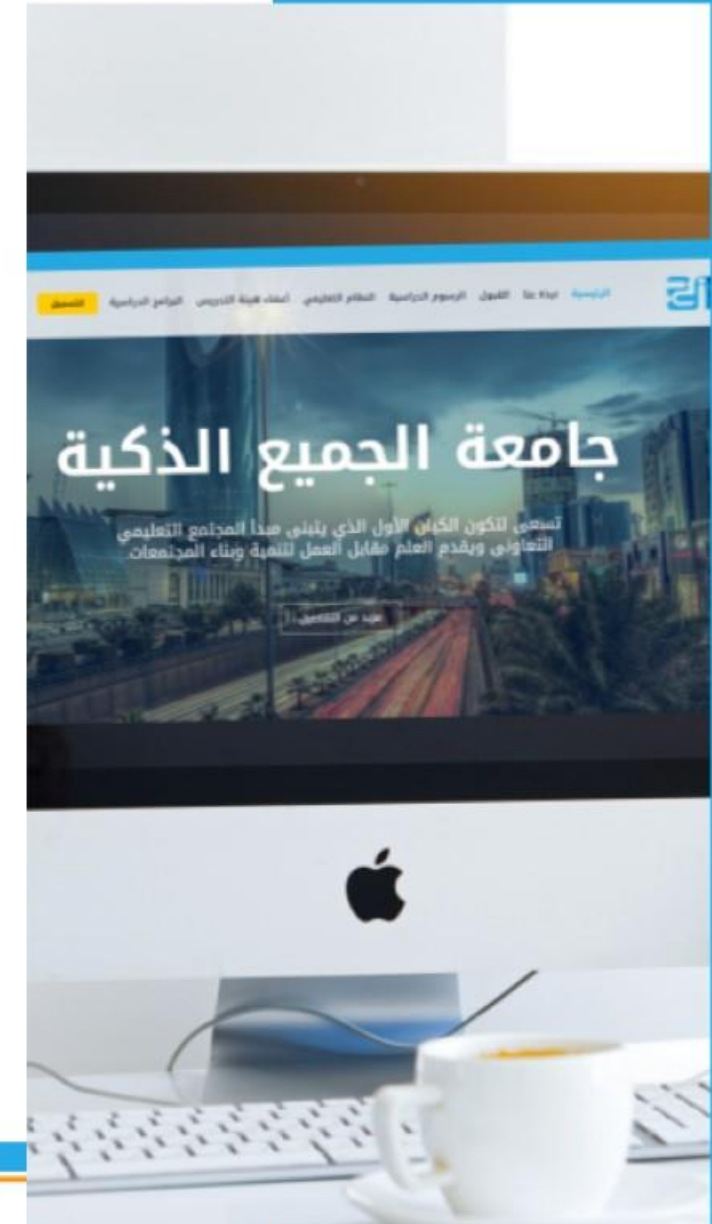


Which events should be logged?

- authentication successes and failures;
- access control successes and failures;
- session activity, such as files and applications used, particularly system utilities;
- changes in user privileges;
- processes starting or stopping;
- changes to configuration settings;
- software installed or deleted;
- devices attached or detached;
- system or application errors and alerts; and
- alerts from security controls, such as firewalls, IDSes and antimalware.

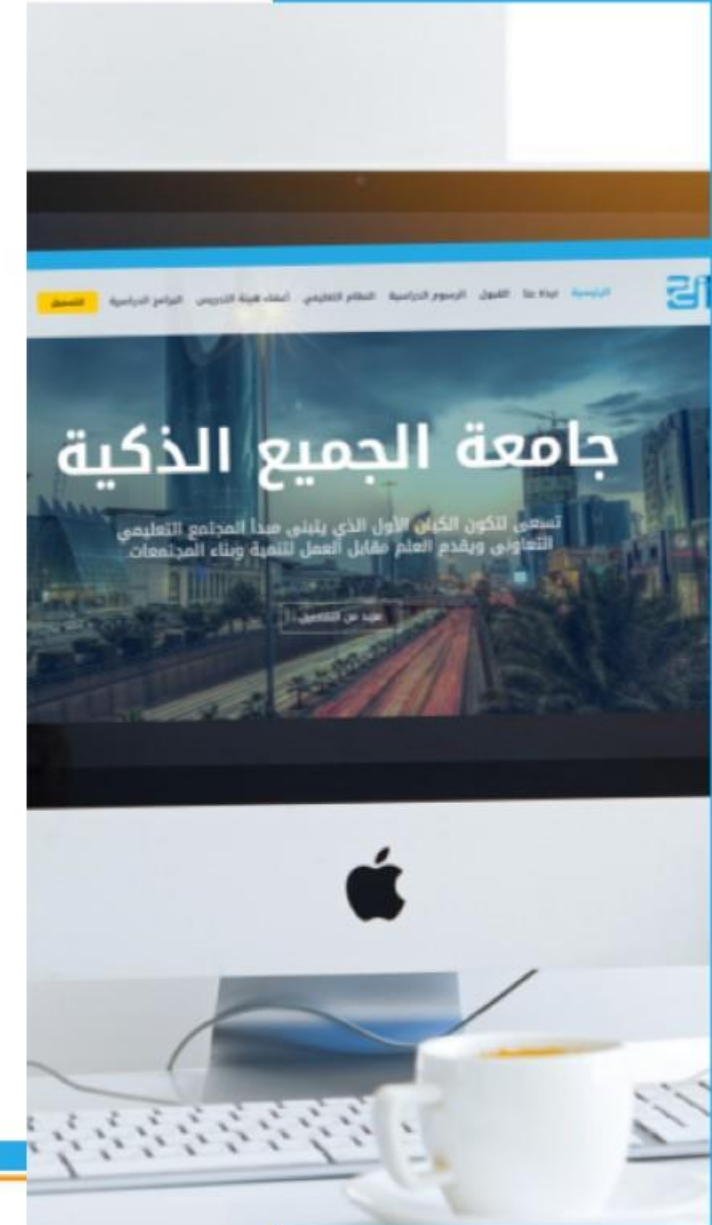
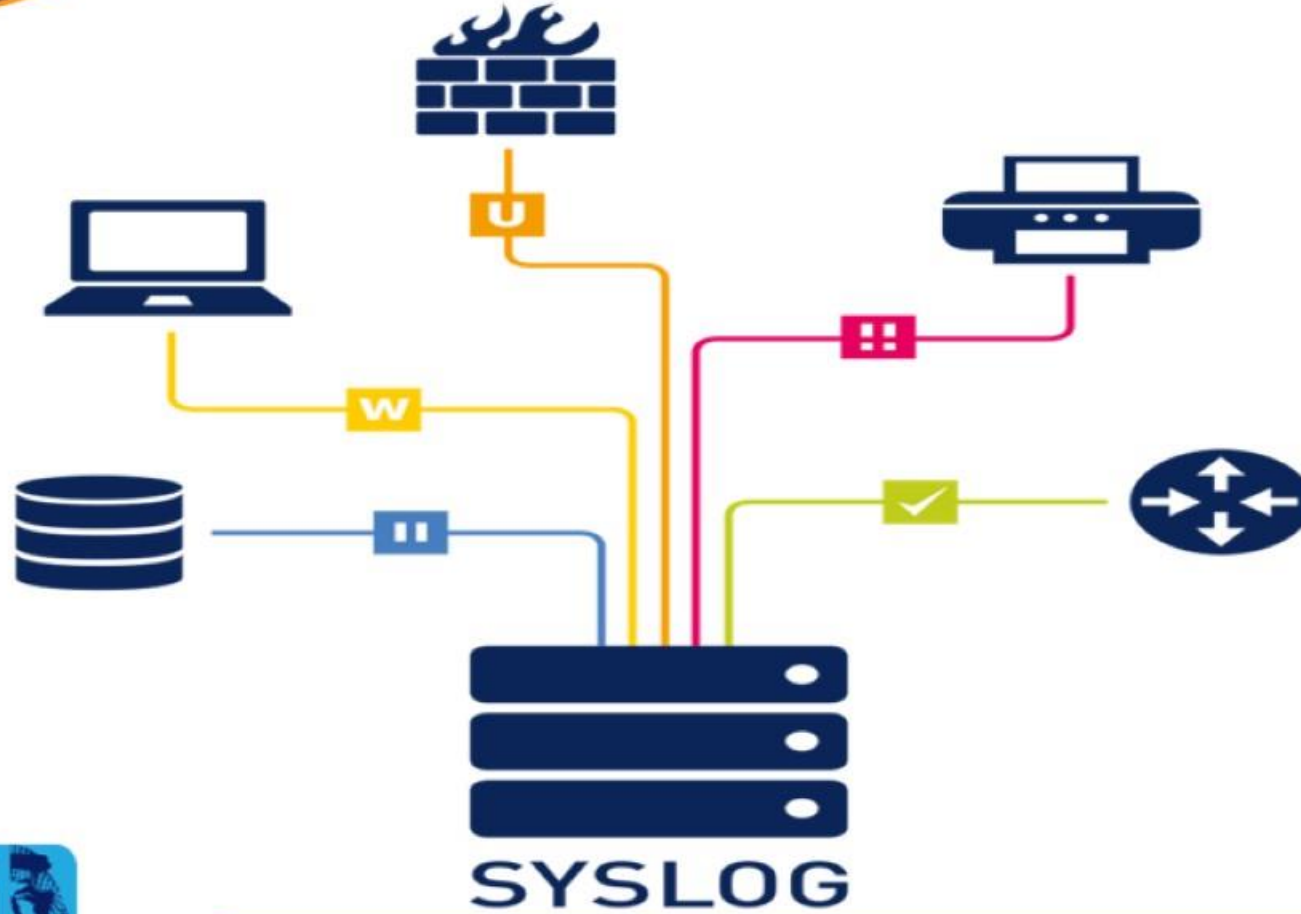


- Syslog : is a standard for message logging system event.
- syslog protocol and application or library sending syslog message.
- Each log generator uses the same high-level format.
- Syslog provides a simple framework for log entry generation, storage, and transfer, that any OS, security software, or application could use if designed to do so.



Lecture 6

Syslog

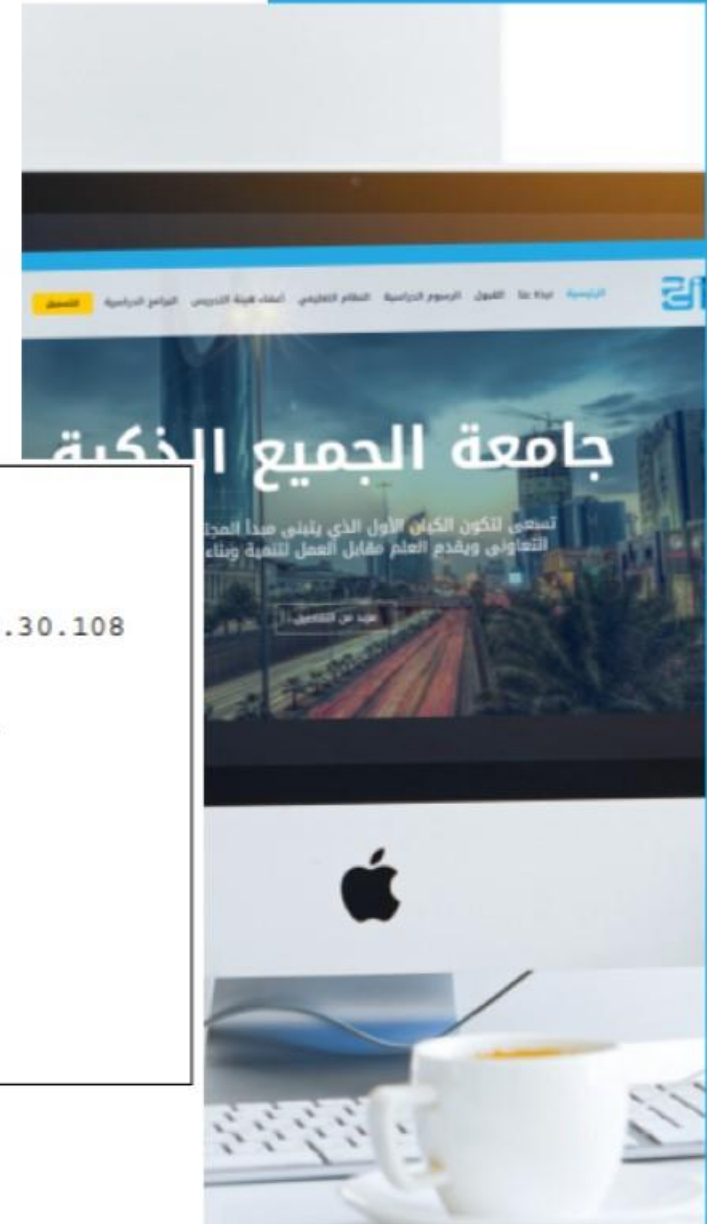


- Syslog Format

Message type, known as a facility

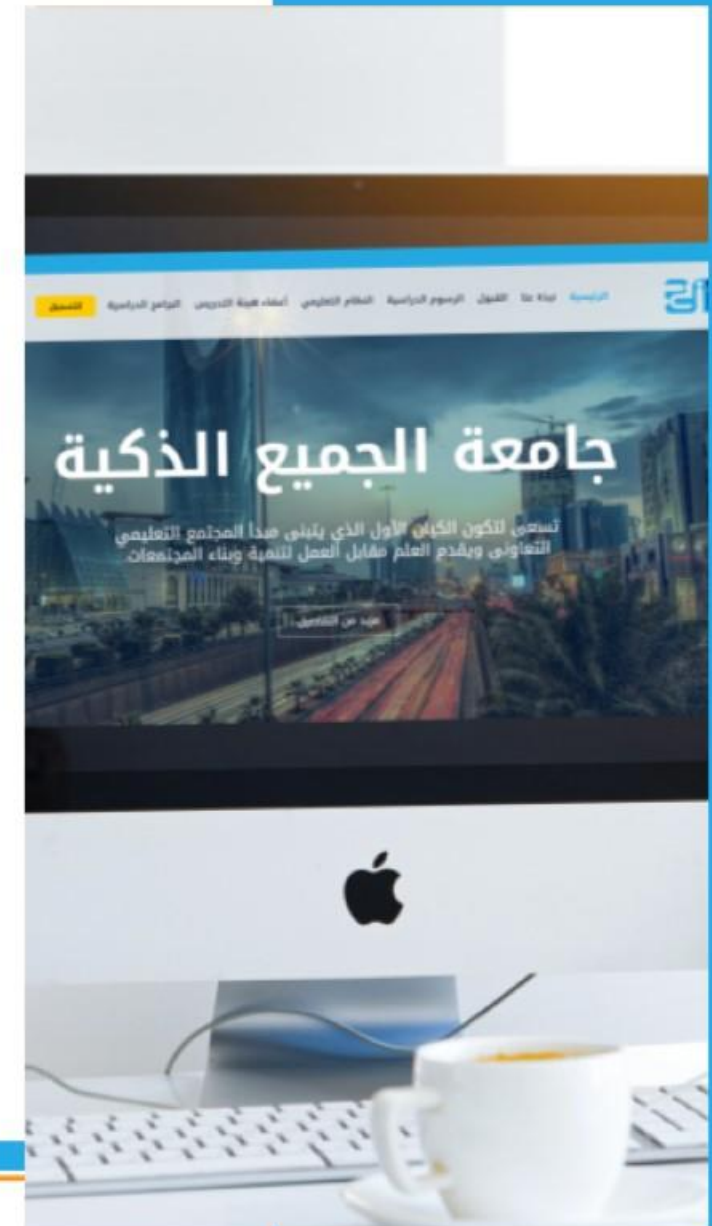
```
Mar  1 06:25:43 server1 sshd[23170]: Accepted publickey for server2 from  
172.30.128.115 port 21011 ssh2  
  
Mar  1 07:16:42 server1 sshd[9326]: Accepted password for murugiah from 10.20.30.108  
port 1070 ssh2  
  
Mar  1 07:16:53 server1 sshd[22938]: reverse mapping checking getaddrinfo for  
ip10.165.nist.gov failed - POSSIBLE BREAKIN ATTEMPT!  
  
Mar  1 07:26:28 server1 sshd[22572]: Accepted publickey for server2 from  
172.30.128.115 port 30606 ssh2  
  
Mar  1 07:28:33 server1 su: BAD SU kkent to root on /dev/ttyp2  
  
Mar  1 07:28:41 server1 su: kkent to root on /dev/ttyp2
```

Examples of Syslog Messages



Lecture 6

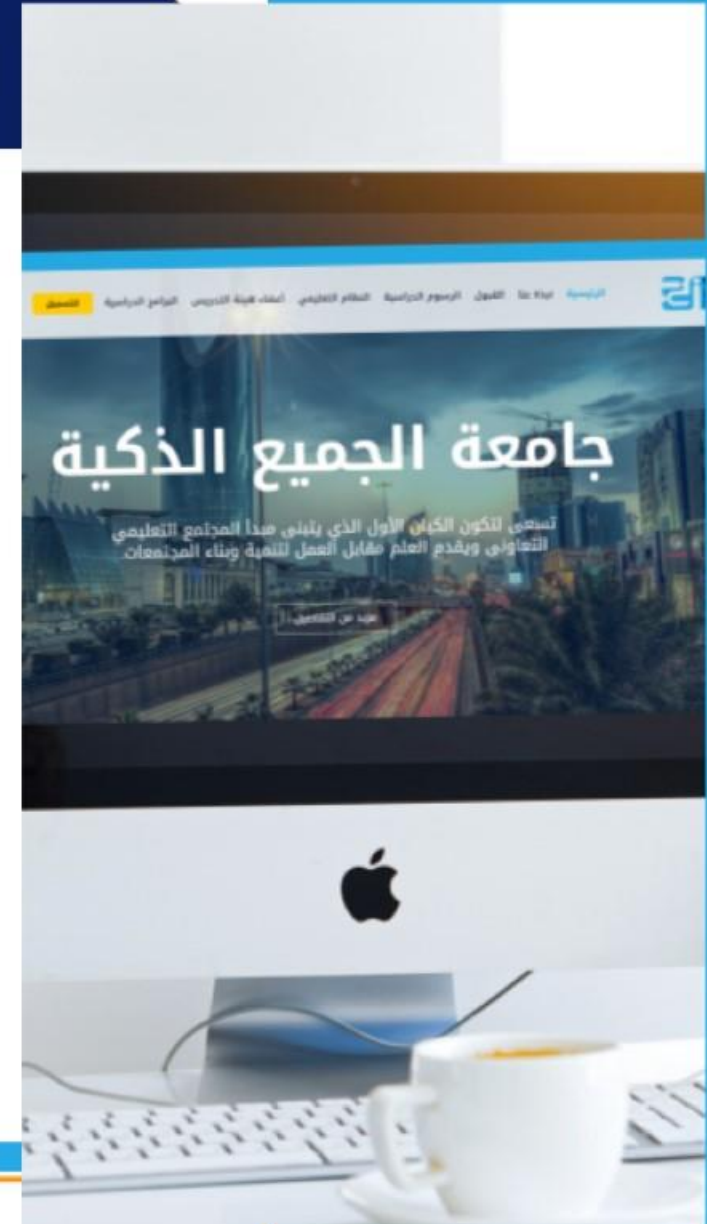
Gathering Evidence From ARP Table



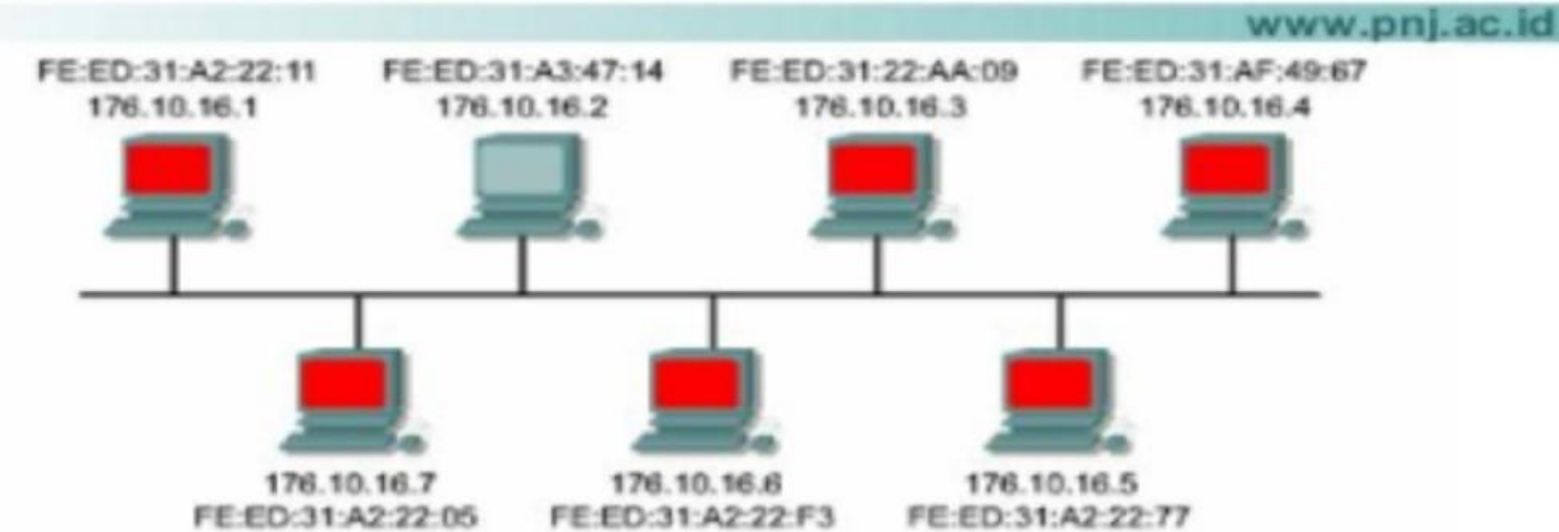
ARP table

ARP : Address Resolution Protocol (ARP)

ARP Table is used to keep the record of the IP address and MAC address of the devices (source and destination device). For the communication between two devices, it is necessary that the IP address and the MAC address of the source and the destination device should be stored in an ARP table.



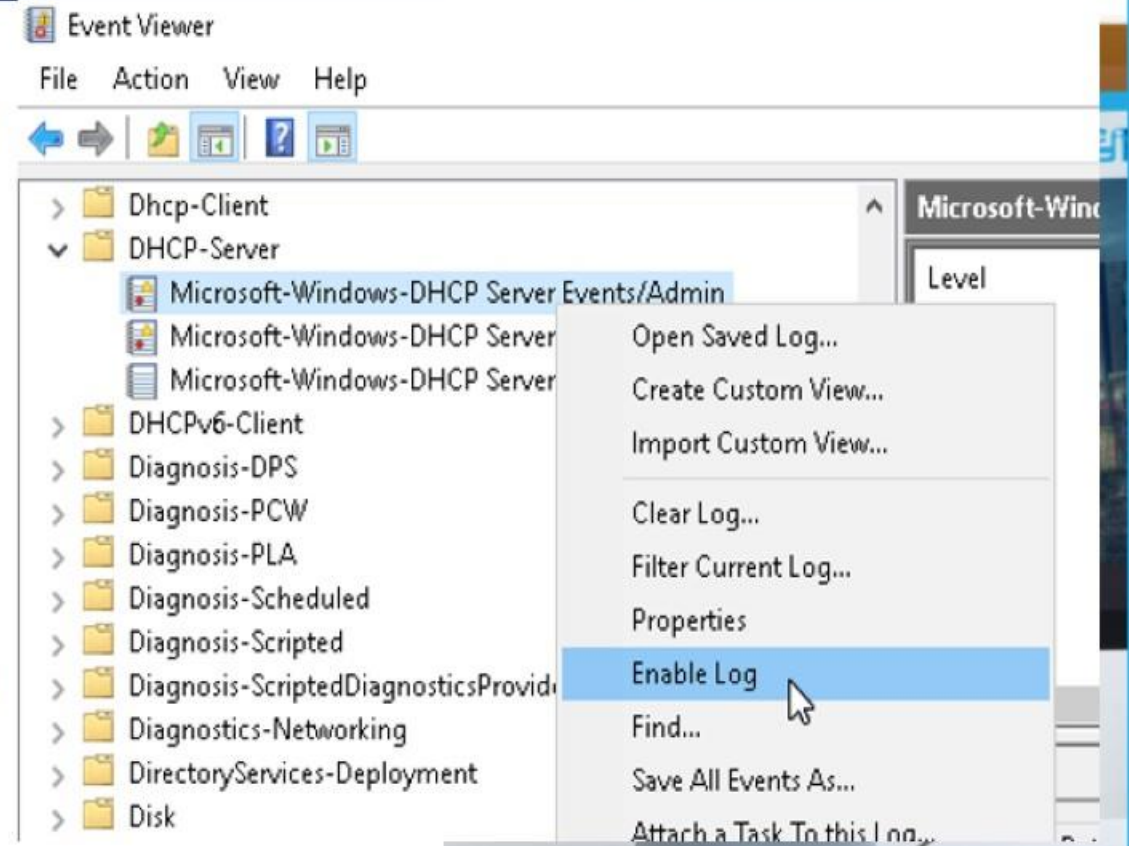
ARP Table Functions



ARP Table	
IP Address	MAC Address
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14

© 2004, Cisco Systems, Inc. All rights reserved.

- Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway
- To enable enhanced DHCP logging, perform the following steps:
 - ☐ Start the DHCP administration tool (go to Start, Programs, Administrative Tools, and click DHCP).
- C:\windows\system32\dhcp



Lecture 6

DHCP logging

```
DhcpSrvLog-Sat - Notepad
File Edit Format View Help
Microsoft DHCP Service Activity Log

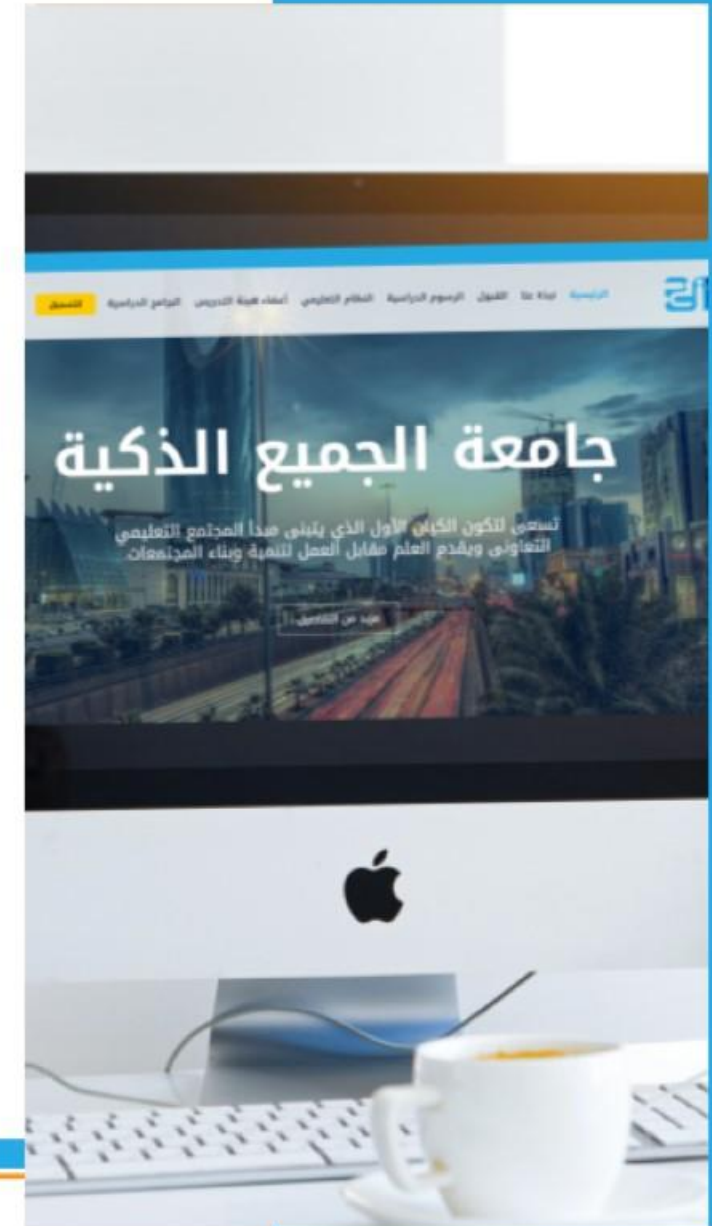
Event ID Meaning
00 The log was started.
01 The log was stopped.
02 The log was temporarily paused due to low disk space.
10 A new IP address was leased to a client.
11 A lease was renewed by a client.
12 A lease was released by a client.
13 An IP address was found to be in use on the network.
14 A lease request could not be satisfied because the scope's address pool was exhausted.
15 A lease was denied.
16 A lease was deleted.
17 A lease was expired and DNS records for an expired leases have not been deleted.
18 A lease was expired and DNS records were deleted.
20 A BOOTP address was leased to a client.
21 A dynamic BOOTP address was leased to a client.
22 A BOOTP request could not be satisfied because the scope's address pool for BOOTP was exhausted.
23 A BOOTP IP address was deleted after checking to see it was not in use.
24 IP address cleanup operation has begun.
25 IP address cleanup statistics.
30 DNS update request to the named DNS server.
31 DNS update failed.
32 DNS update successful.
33 Packet dropped due to NAP policy.
34 DNS update request failed, as the DNS update request queue limit exceeded.
35 DNS update request failed.
50+ Codes above 50 are used for Rogue Server Detection information.

QResult: 0: NoQuarantine, 1:Quarantine, 2:Drop Packet, 3:Probation, 6:No Quarantine Information

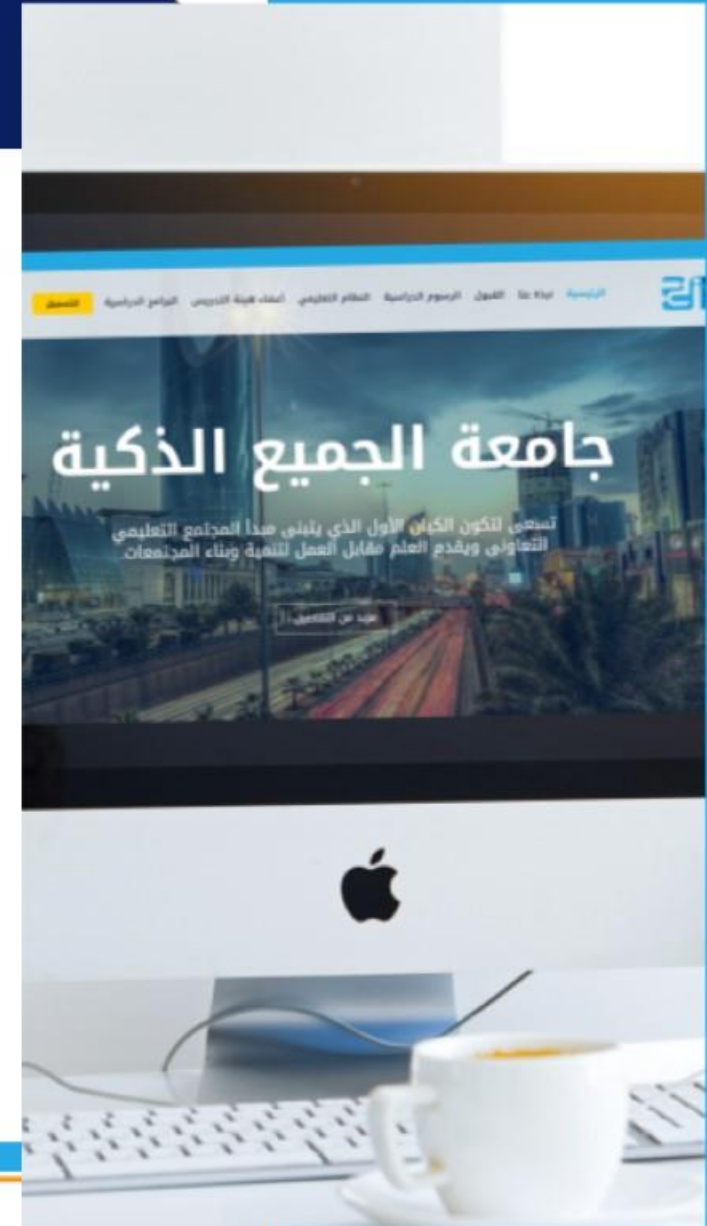
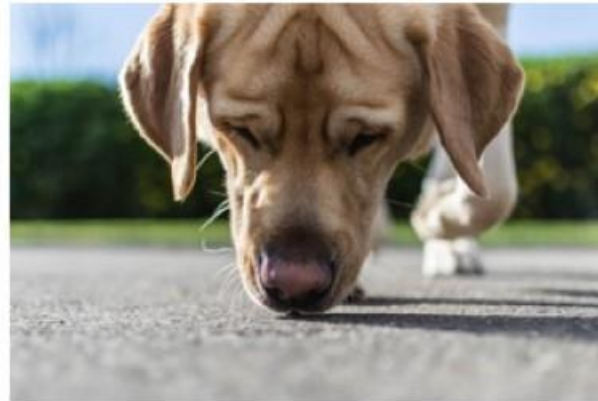
ID, Date, Time, Description, IP Address, Host Name, MAC Address, User Name, TransactionID, QResult,
24.01/14/12.00:00:40, Database Cleanup Begin, ..., 0.6...
18.01/14/12.00:00:40, Expired, 192.168.1.150, ..., 0.6...
25.01/14/12.00:00:40, 0 leases expired and 0 leases deleted, ..., 0.6...
25.01/14/12.00:00:40, 0 leases expired and 0 leases deleted, ..., 0.6...
24.01/14/12.00:01:46, Database Cleanup Begin, ..., 0.6...
25.01/14/12.00:01:46, 0 leases expired and 0 leases deleted, ..., 0.6...
25.01/14/12.00:01:46, 0 leases expired and 0 leases deleted, ..., 0.6...
24.01/14/12.01:01:46, Database Cleanup Begin, ..., 0.6...
25.01/14/12.01:01:46, 0 leases expired and 0 leases deleted, ..., 0.6...
25.01/14/12.01:01:46, 0 leases expired and 0 leases deleted, ..., 0.6...
```

Lecture 6

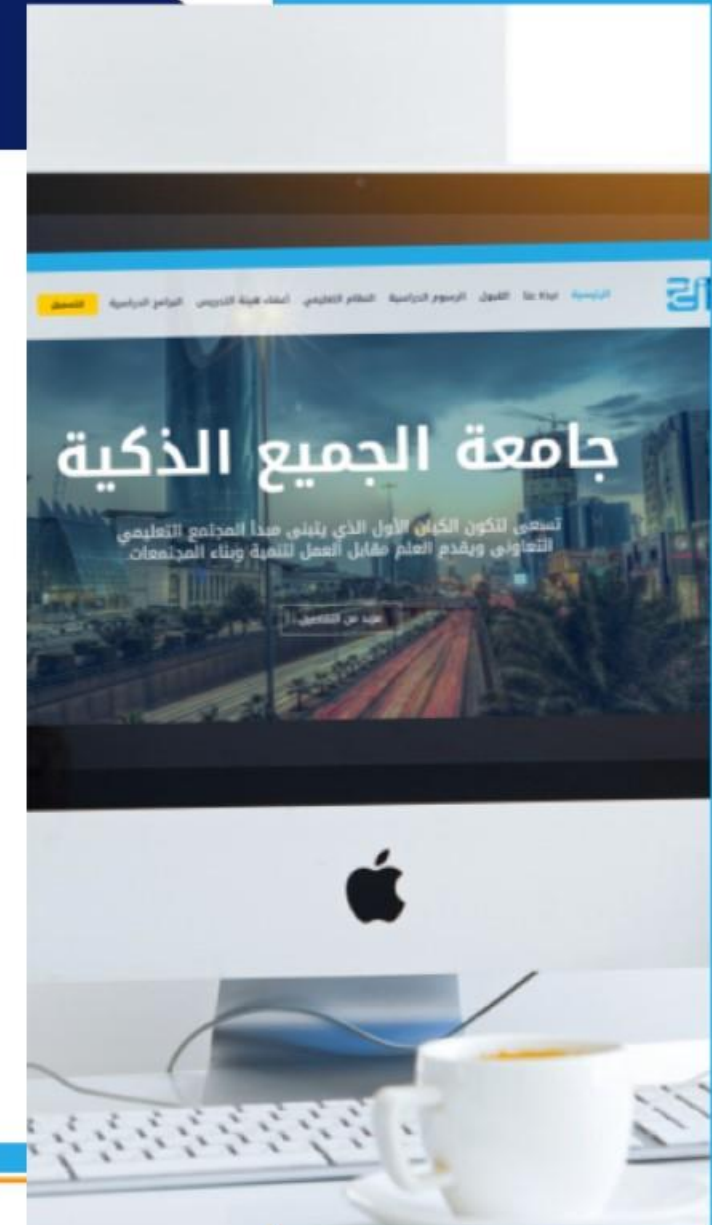
Sniffing



- Sniffers operate at the data link layer of the OSI model.
- This means they do not have to play by the same rules as applications and services that reside further up the stack.
- Sniffers can capture everything on the wire and record it for later review.

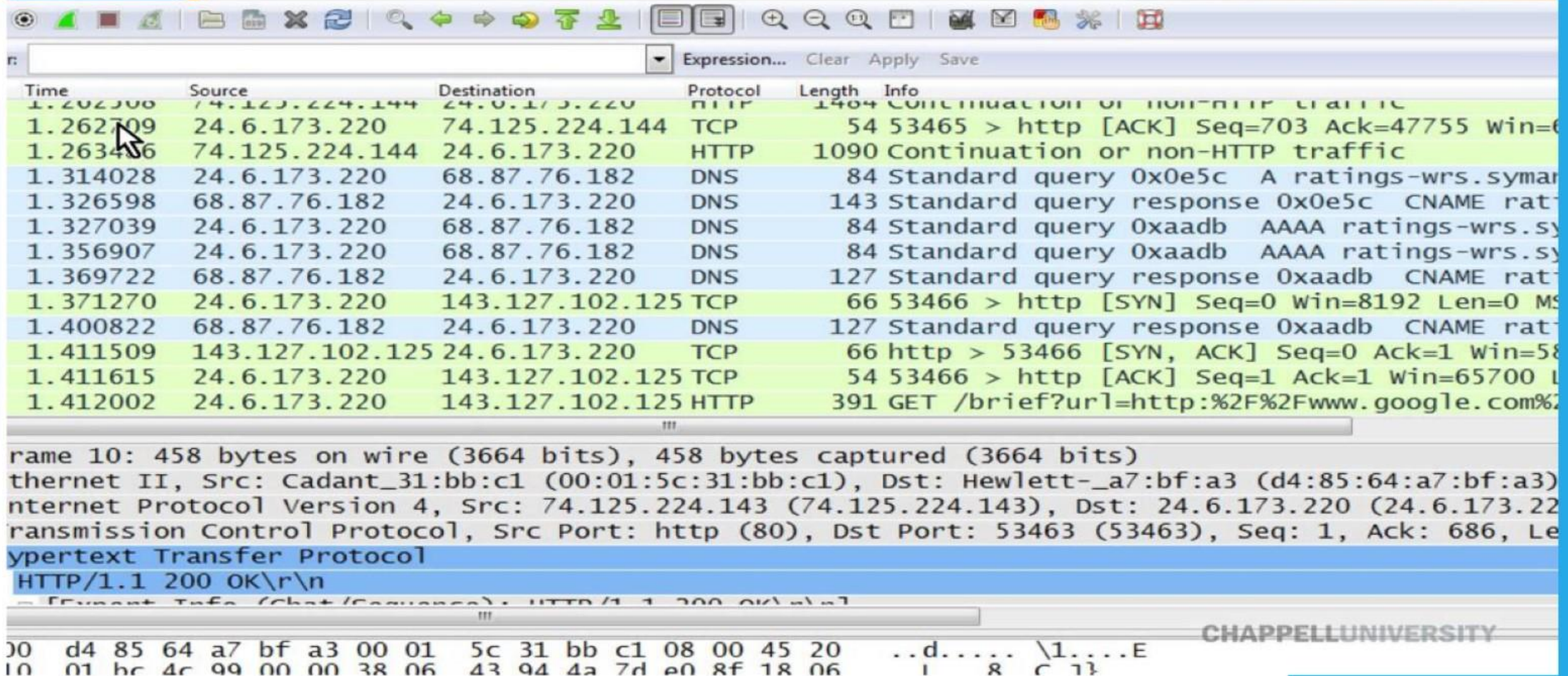


- They allow the user to analyze all the data that is contained in the packet. A good sniffer product is **Wireshark**.
- Not only is it free to use but it works well in both a Windows and Linux environment.
- You can find more details about the program at the official site, www.wireshark.com.



Lecture 6

Sniffing: Wireshark



The image shows a Wireshark network traffic capture. The top toolbar contains various icons for file operations, navigation, and analysis. Below the toolbar is a filter bar with an 'Expression...' field and buttons for 'Clear', 'Apply', and 'Save'. The main packet list table displays the following data:

Time	Source	Destination	Protocol	Length	Info
1.202308	74.125.224.144	24.6.173.220	HTTP	1404	Continuation of non-HTTP traffic
1.262709	24.6.173.220	74.125.224.144	TCP	54	53465 > http [ACK] Seq=703 Ack=47755 win=6
1.263436	74.125.224.144	24.6.173.220	HTTP	1090	Continuation of non-HTTP traffic
1.314028	24.6.173.220	68.87.76.182	DNS	84	Standard query 0x0e5c A ratings-wrs.syman
1.326598	68.87.76.182	24.6.173.220	DNS	143	Standard query response 0x0e5c CNAME rat
1.327039	24.6.173.220	68.87.76.182	DNS	84	Standard query 0xaadb AAAA ratings-wrs.sy
1.356907	24.6.173.220	68.87.76.182	DNS	84	Standard query 0xaadb AAAA ratings-wrs.sy
1.369722	68.87.76.182	24.6.173.220	DNS	127	Standard query response 0xaadb CNAME rat
1.371270	24.6.173.220	143.127.102.125	TCP	66	53466 > http [SYN] Seq=0 win=8192 Len=0 MS
1.400822	68.87.76.182	24.6.173.220	DNS	127	Standard query response 0xaadb CNAME rat
1.411509	143.127.102.125	24.6.173.220	TCP	66	http > 53466 [SYN, ACK] Seq=0 Ack=1 win=58
1.411615	24.6.173.220	143.127.102.125	TCP	54	53466 > http [ACK] Seq=1 Ack=1 win=65700
1.412002	24.6.173.220	143.127.102.125	HTTP	391	GET /brief?url=http:%2F%2Fwww.google.com%

Below the packet list, the details pane shows the selected packet (10) with the following information:

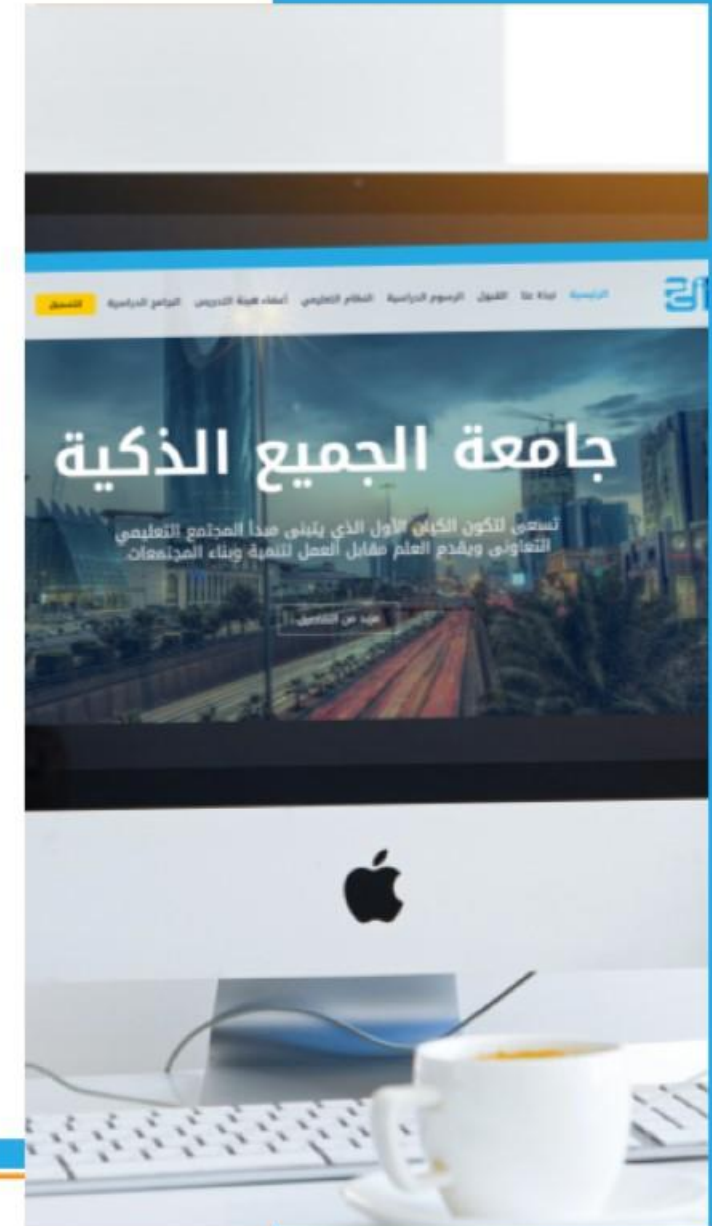
- Frame 10: 458 bytes on wire (3664 bits), 458 bytes captured (3664 bits)
- Ethernet II, Src: Cadant_31:bb:c1 (00:01:5c:31:bb:c1), Dst: Hewlett-_a7:bf:a3 (d4:85:64:a7:bf:a3)
- Internet Protocol Version 4, Src: 74.125.224.143 (74.125.224.143), Dst: 24.6.173.220 (24.6.173.220)
- Transmission Control Protocol, Src Port: http (80), Dst Port: 53463 (53463), Seq: 1, Ack: 686, Len
- Hypertext Transfer Protocol
- HTTP/1.1 200 OK\r\n

The bottom pane shows the raw packet data in hexadecimal and ASCII format:

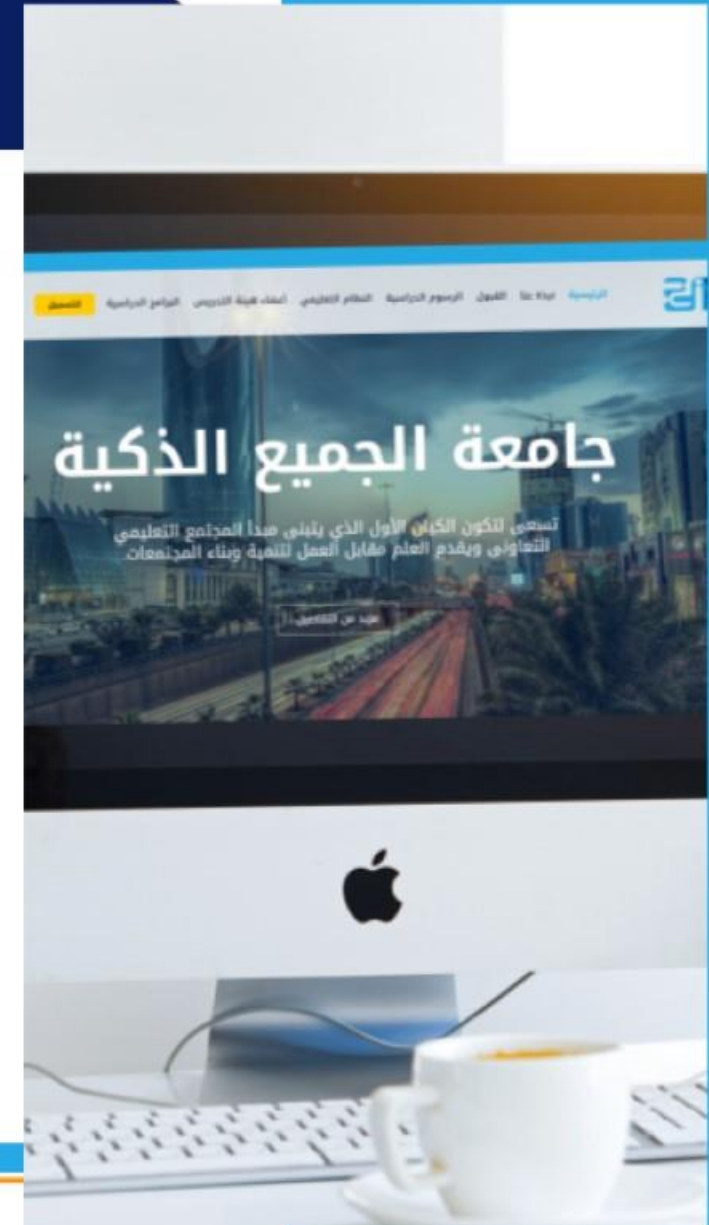
```
00  d4 85 64 a7 bf a3 00 01 5c 31 bb c1 08 00 45 20  ..d.....\1....E
10  01 bc 4c 99 00 00 38 06 43 94 4a 7d e0 8f 18 06  i 8 c 13
```

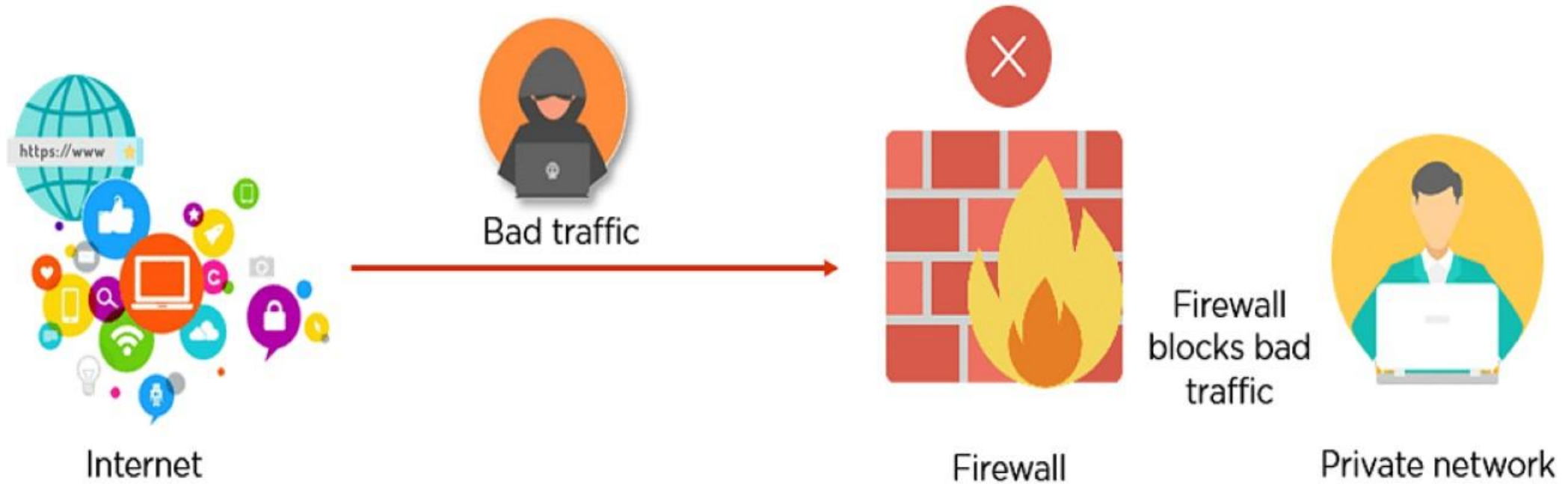
Lecture 6

Firewall



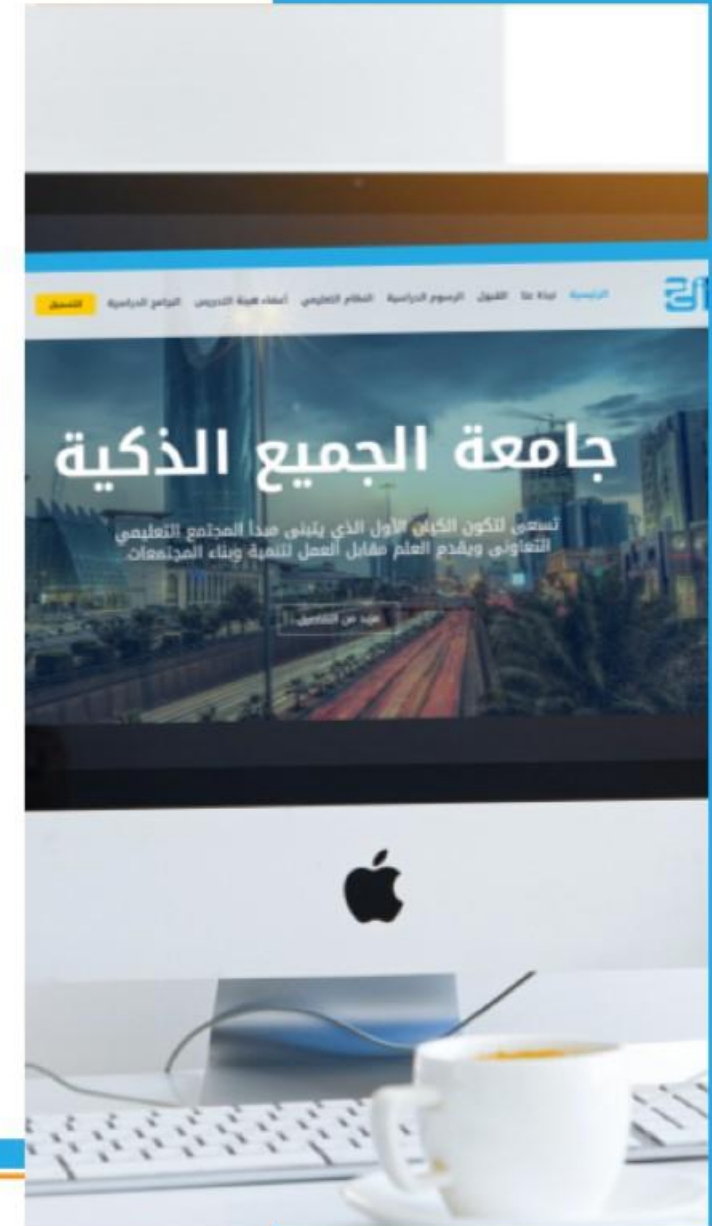
- Is a software or hardware prevent hacking or few kind of malware from getting to any PC through network or internet.
- It monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies.
- Cisco and Fortinet FortiGate.



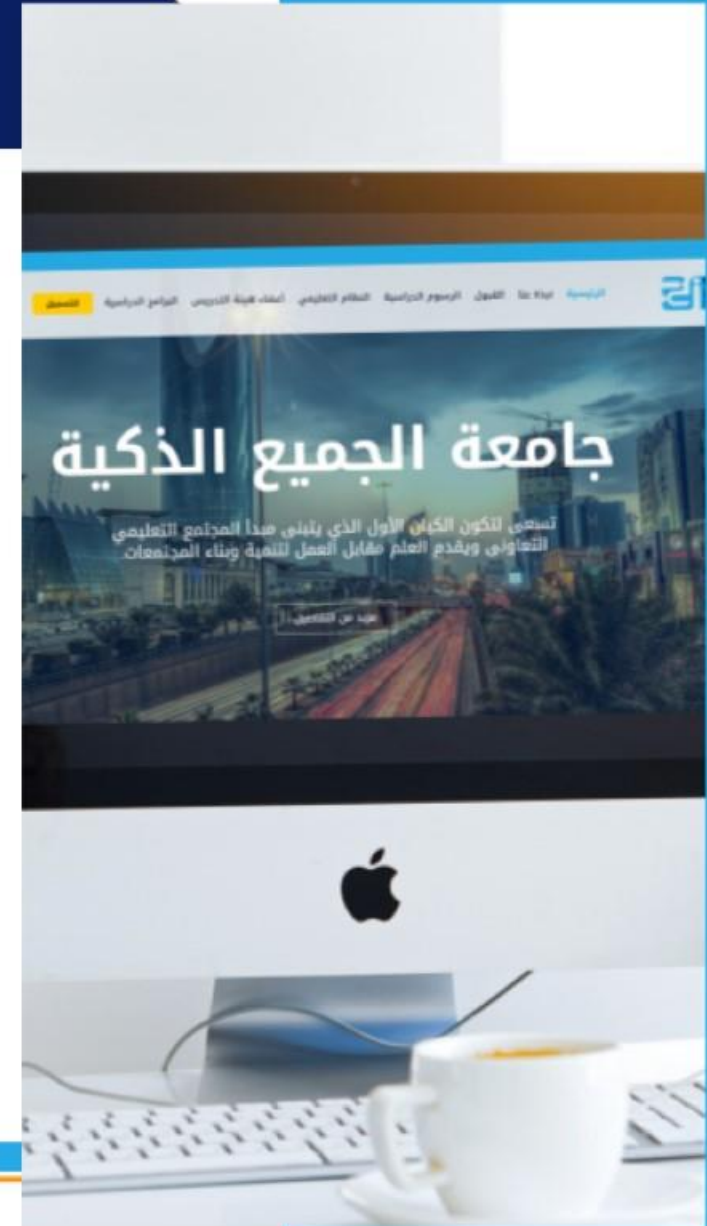


Lecture 6

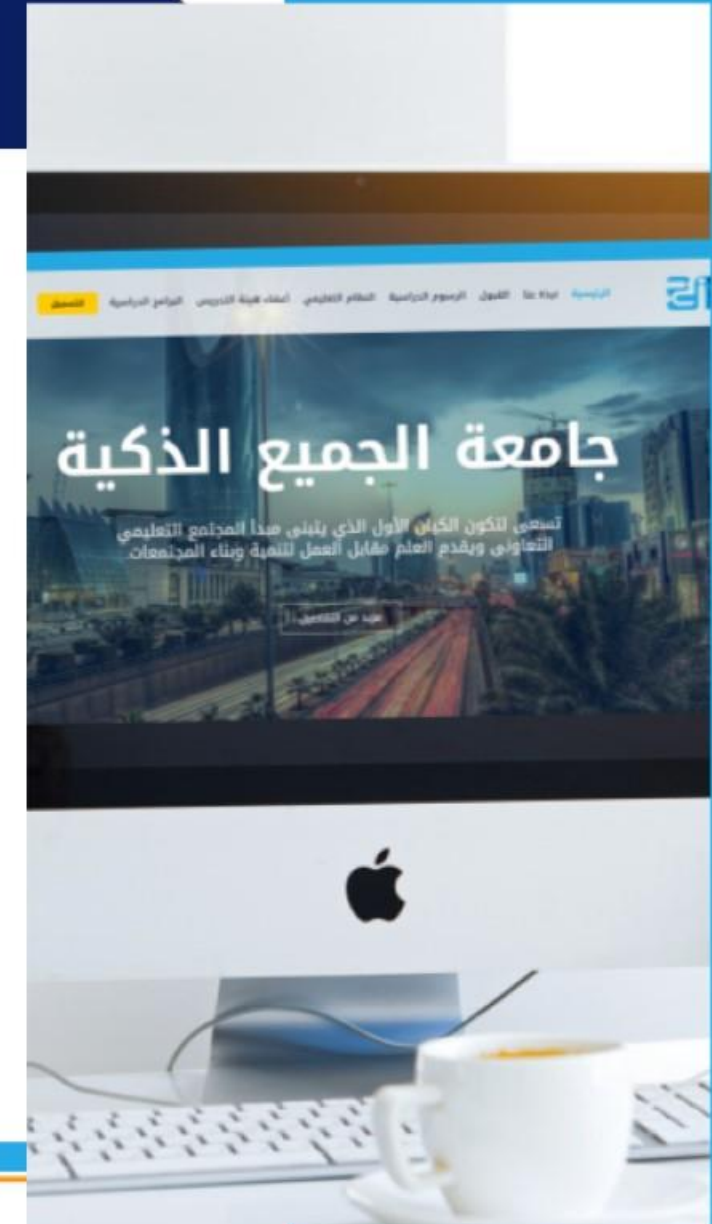
IDS

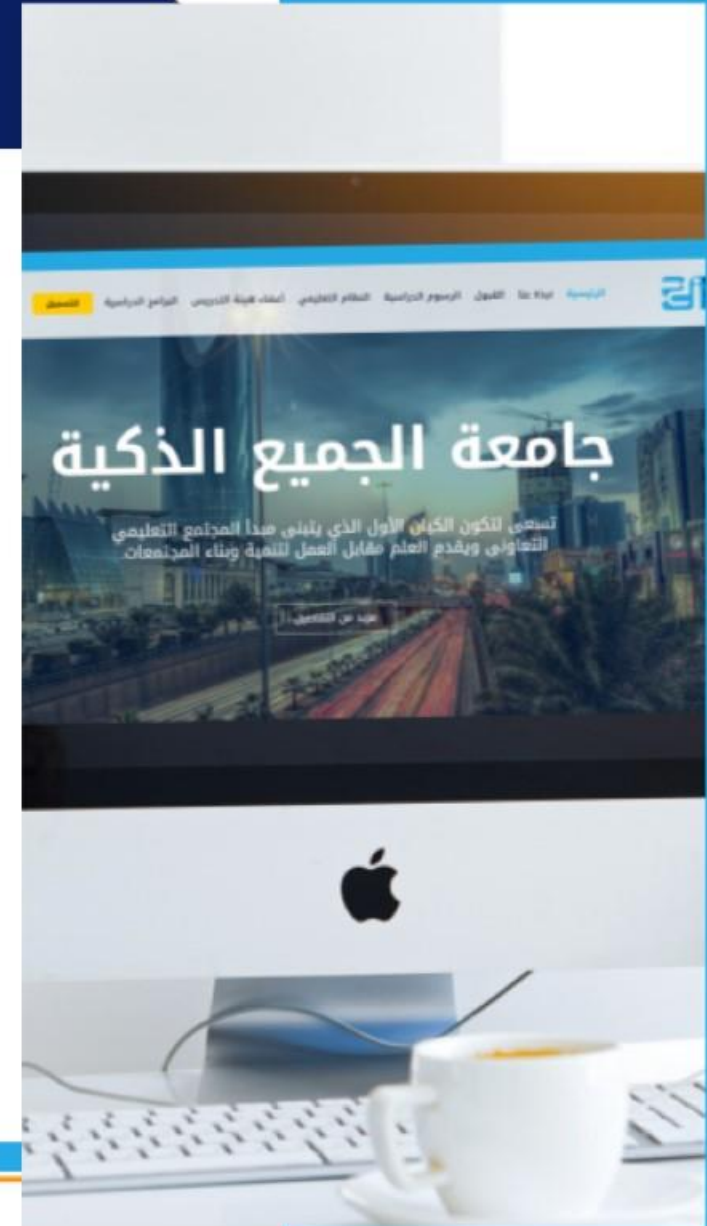
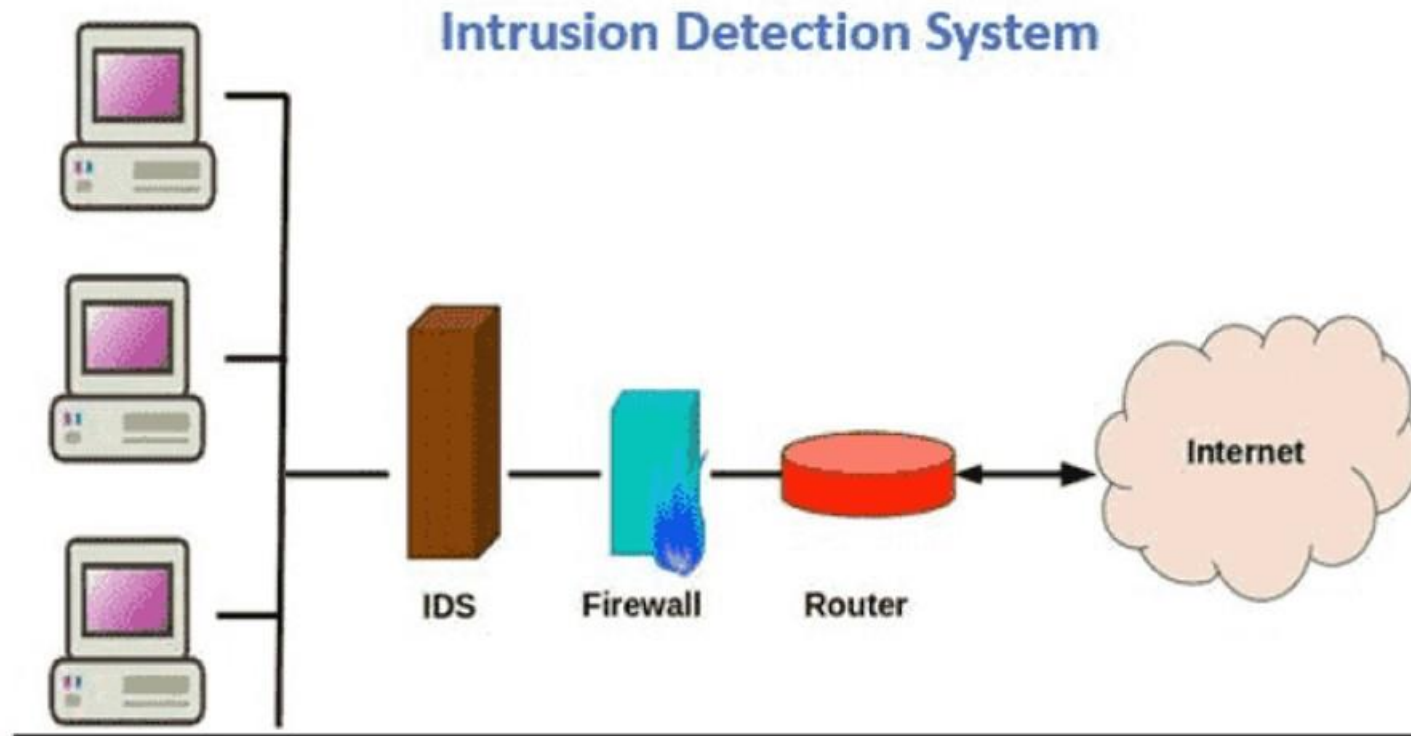


- An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for the harmful activity or policy breaching.

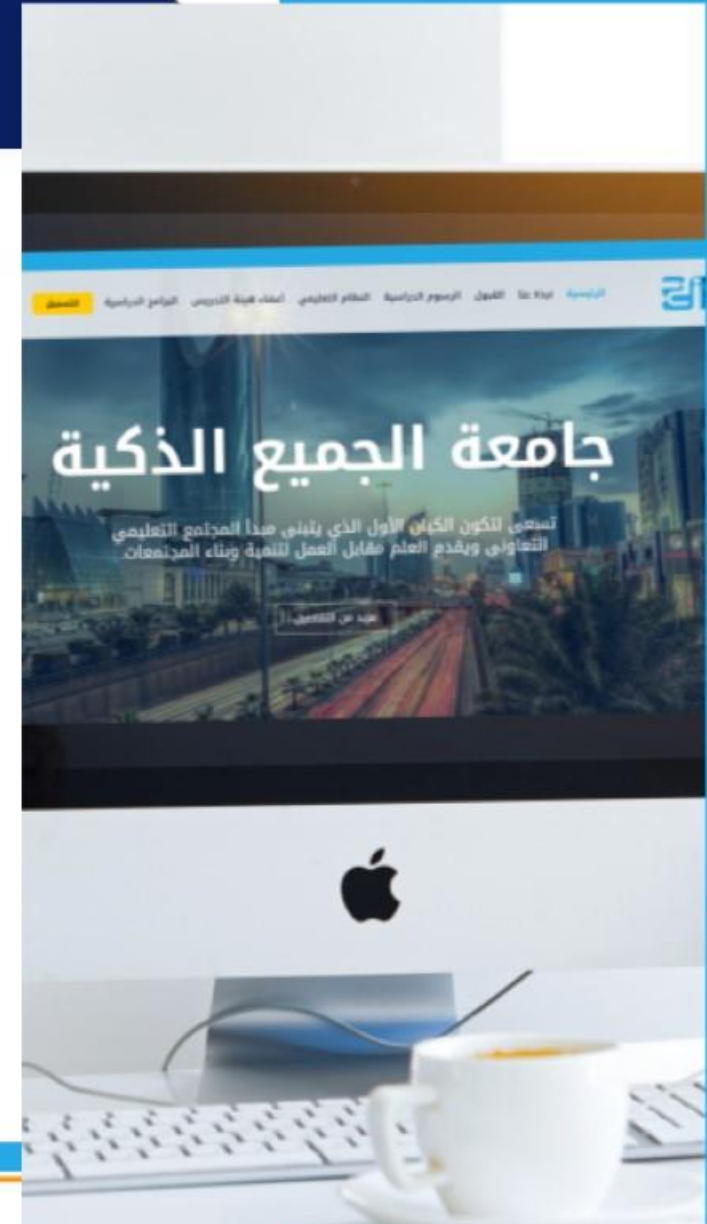


- Intrusion detection involves monitoring network traffic, detecting attempts to gain unauthorized access to a system or resource, and notifying the appropriate individuals so that counteractions can be taken.

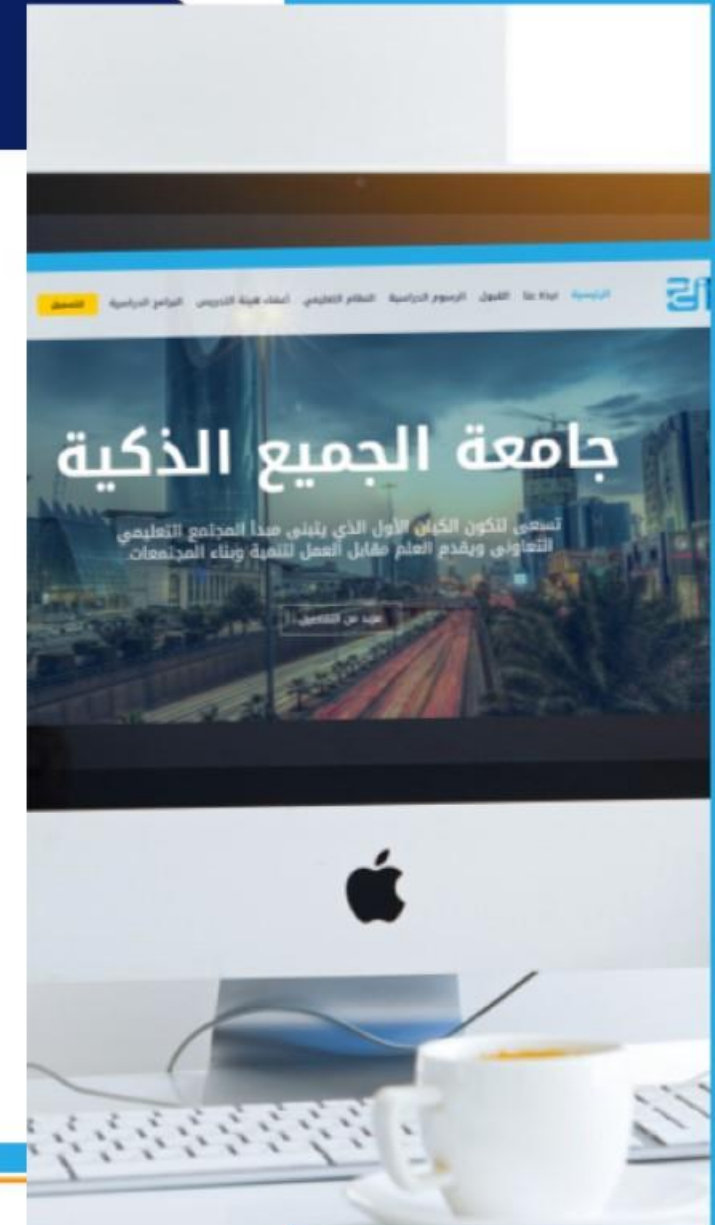




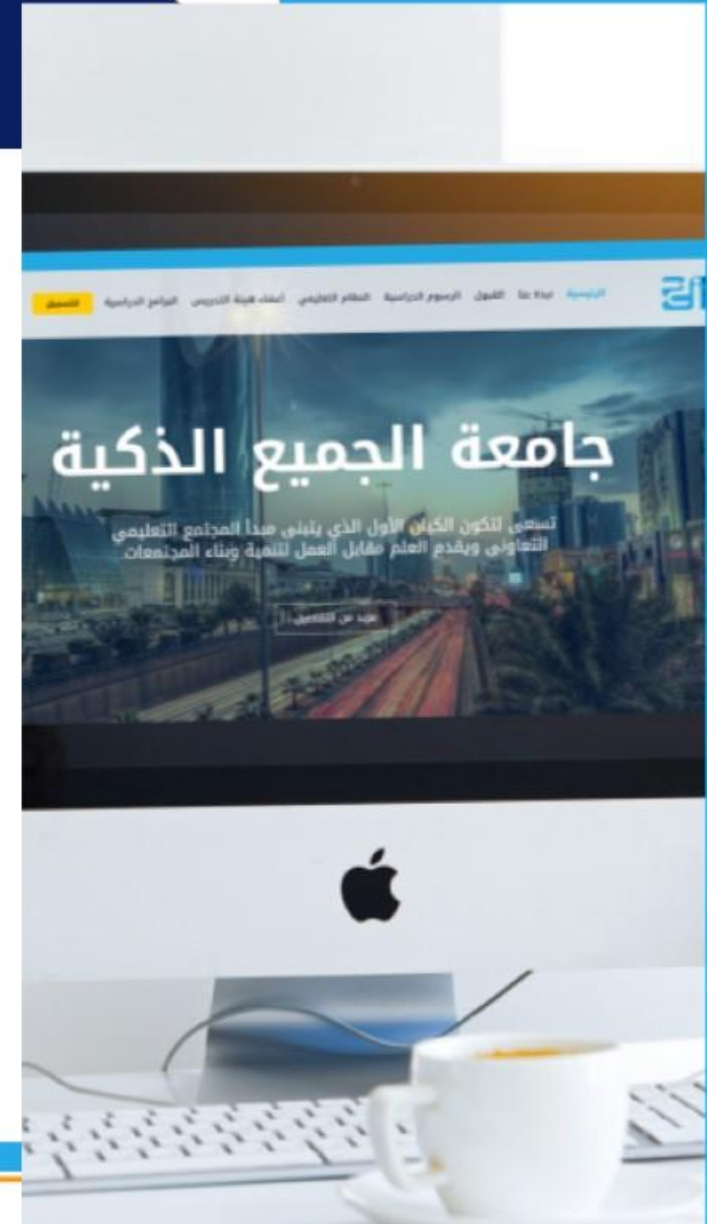
- Having the ability to analyze intrusions and attacks is a powerful tool.
- There are four types of logs that would be of interest during a forensic investigation—authentication, application, operating system, and network—but the IDS will be of use primarily with network logs.



- There are many good IDS systems available. Snort is one example of an IDS with wide industry support.



- Documentation the logs of the network are easy if the network are small
- If the evidence are in remote location documentation are more complex because the unavailability of data and timestamp.
- If remote location it is important to document the detailed information about the collection and location.



Lecture 6

Any quention

