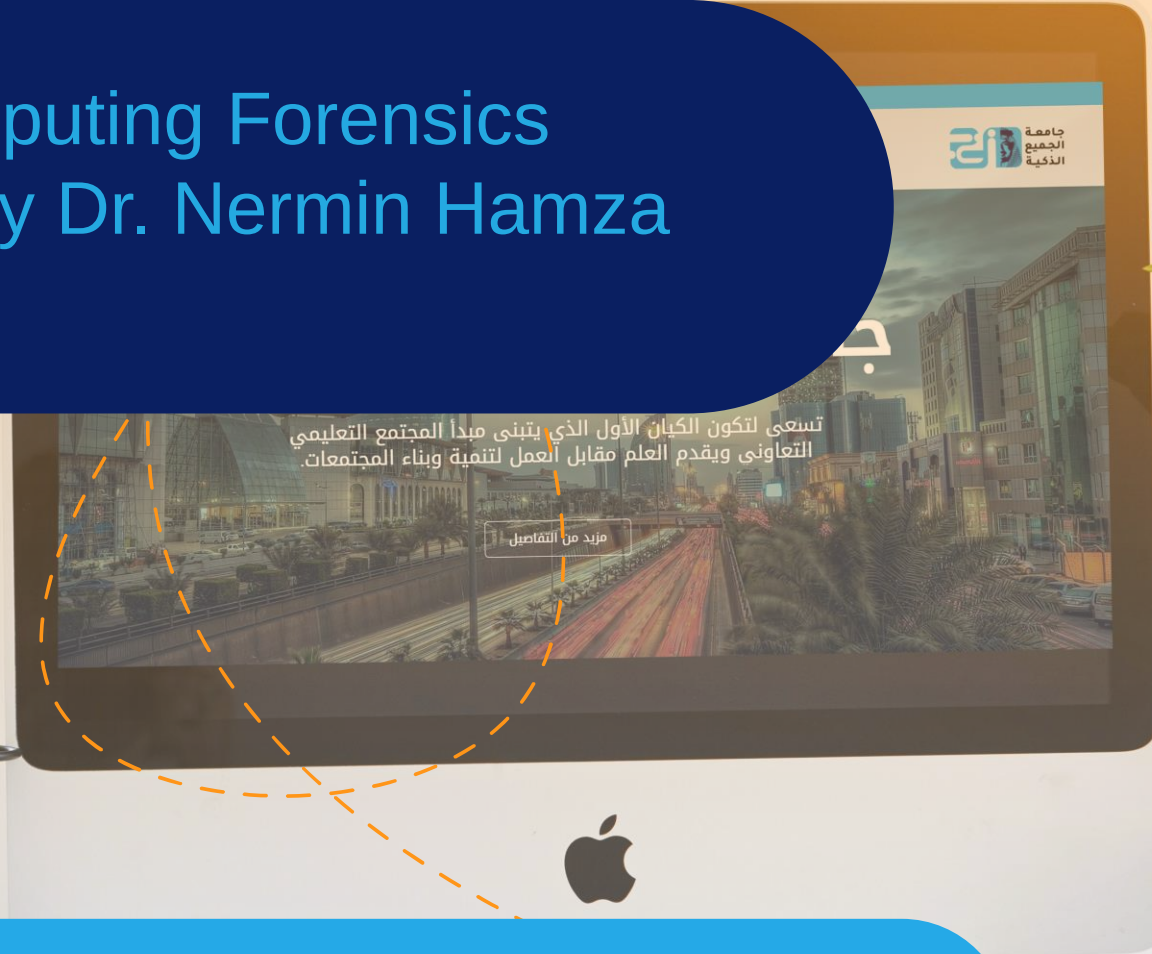


Cloud Computing Forensics

Prepared by Dr. Nermin Hamza

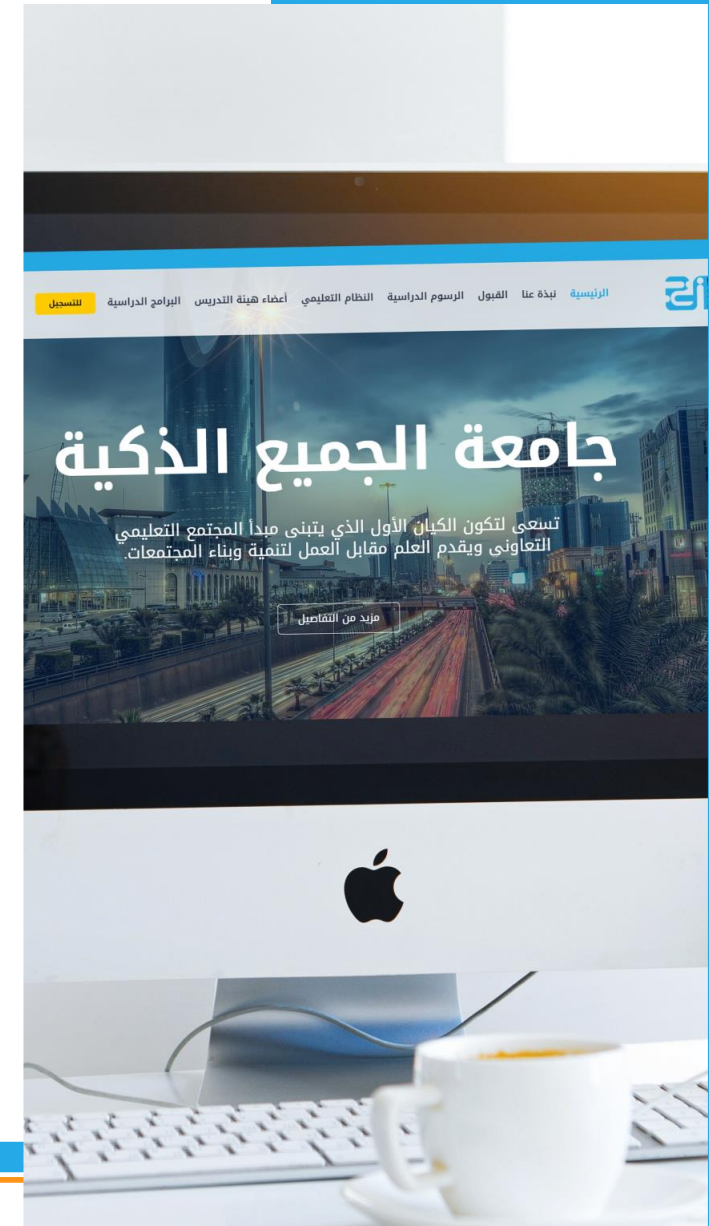
Lecture 8



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

CYB 670
IT Forensics

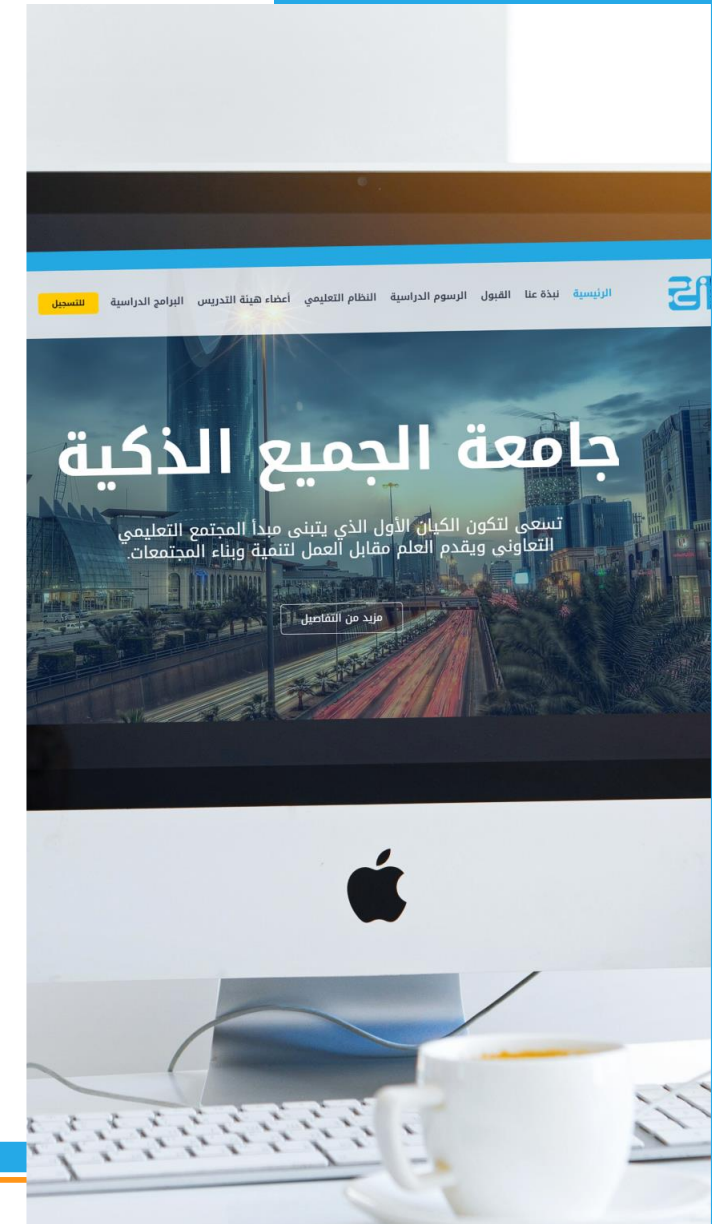
- Cloud Computing
- Cloud Computing Threats
- Cloud Computing Attacks
- Cloud forensics
- Cloud Forensic Steps
- Cloud Storage services



Lecture 8

Cloud Computing

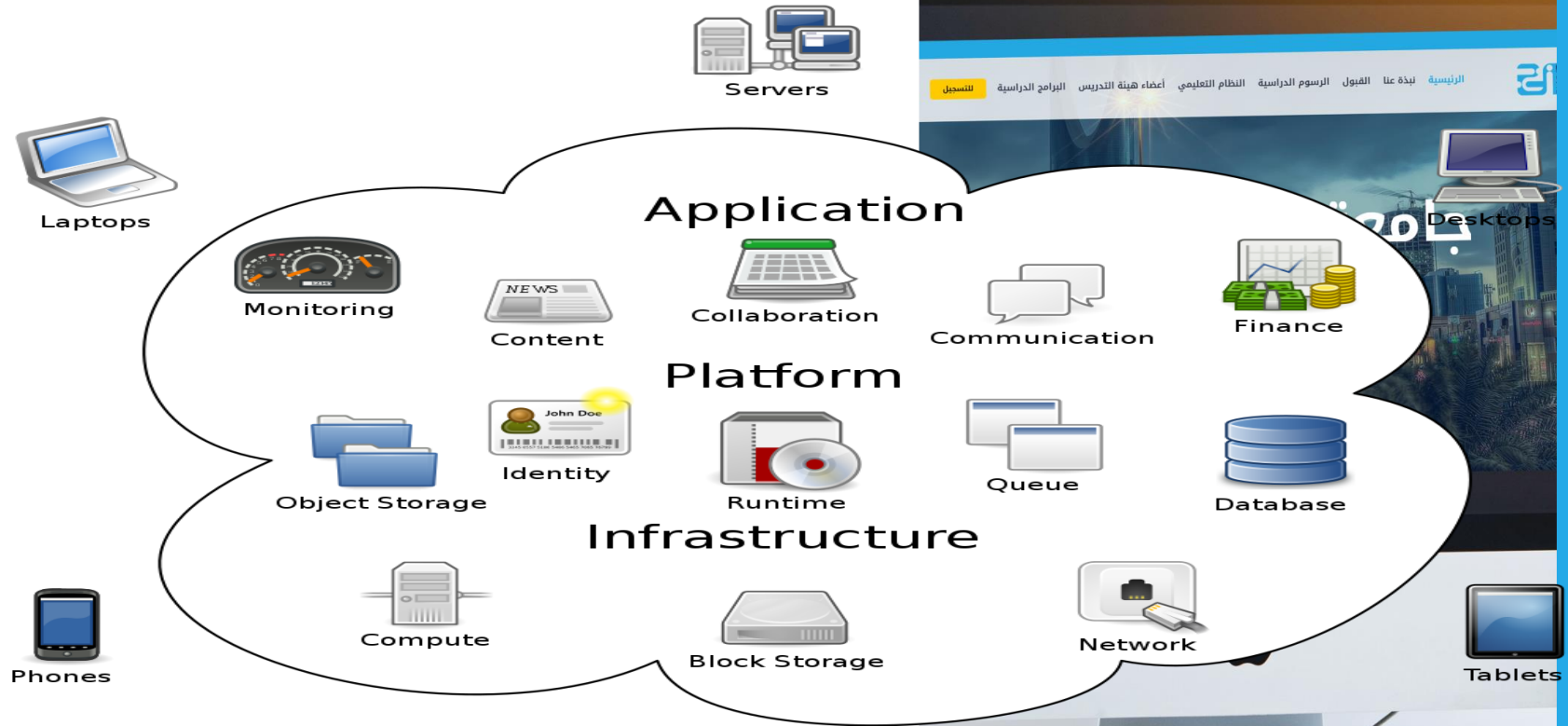
Cloud Computing: is the on-demand availability of computer system resources, especially data storage (cloud storage) and computing power, without direct active management by the user.



Lecture 8

Cloud Computing

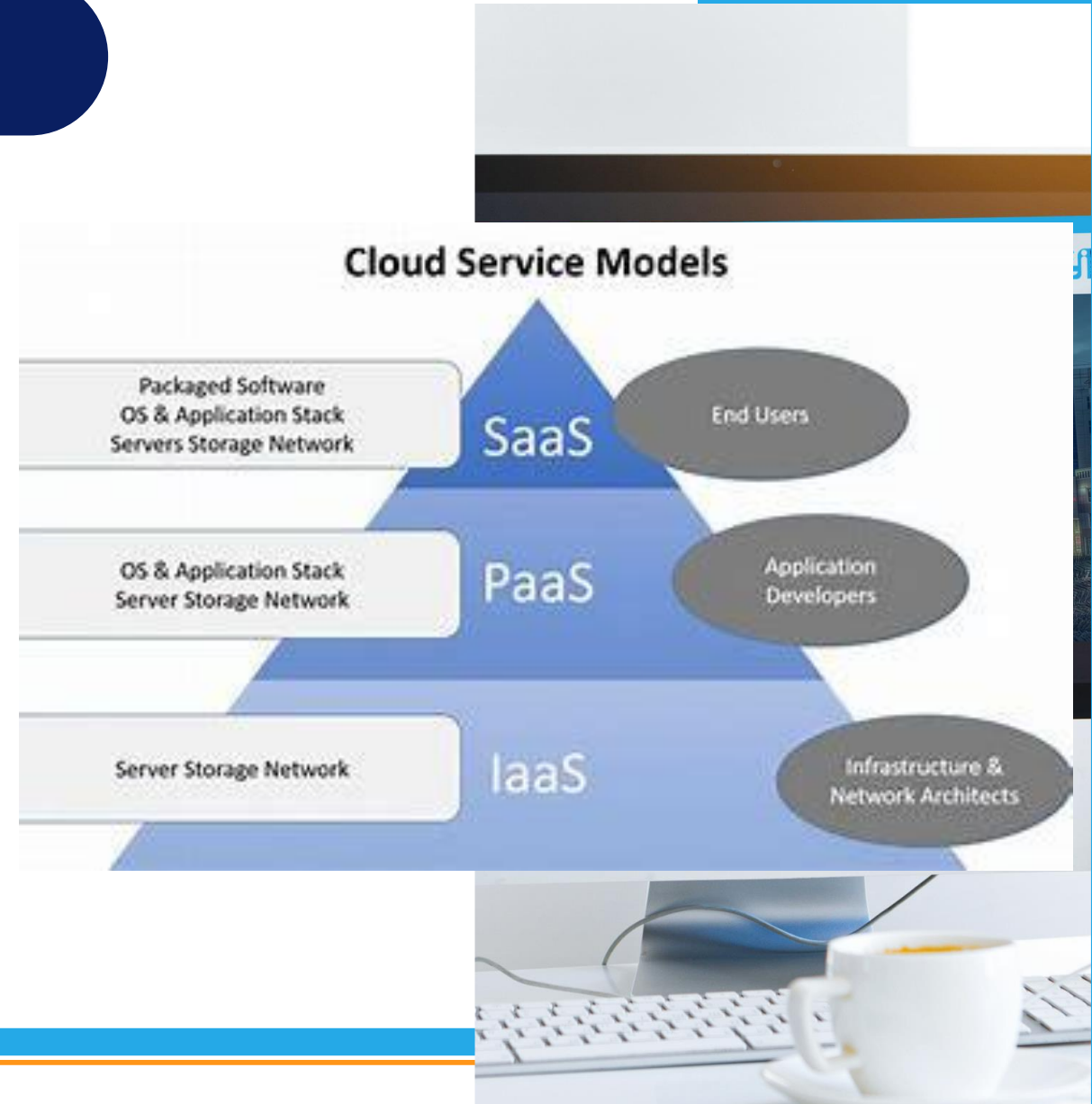
The term is generally used to describe data centers available to many users over the Internet.



Cloud service model mainly divided into three types:

- Infrastructure as a Service (IAAS),
- Platform as a Service (PAAS) and
- Software as a Service (SAAS).

Selection of right service model depends on your requirement.



-



- **Platform-as-a-Service (PaaS):** Cloud service providers deliver set of resources such as hardware, servers, storage, networking etc.

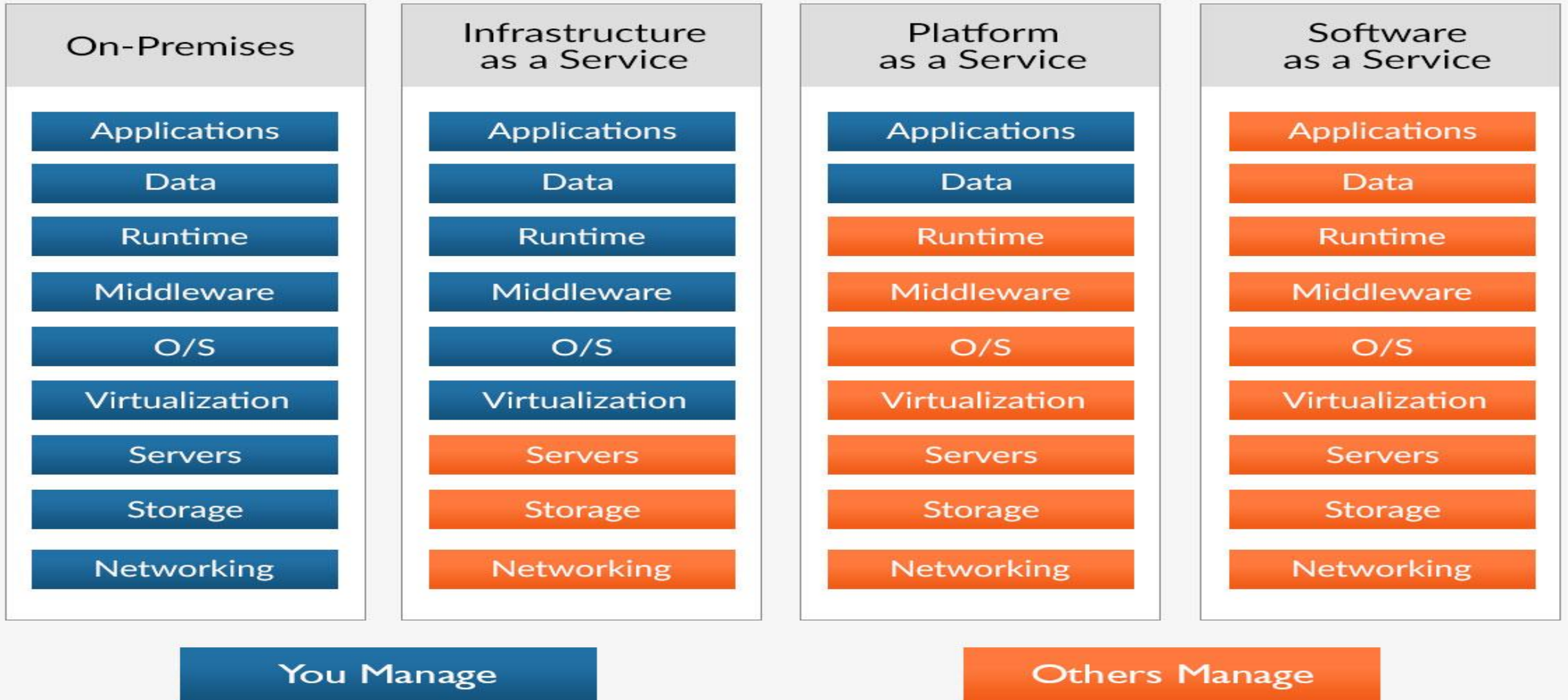


- **Software-as-a-Service (SaaS):** SAAS model allows quick access of your business using internet with zero installation, User only needs a web browser to access cloud-based web applications



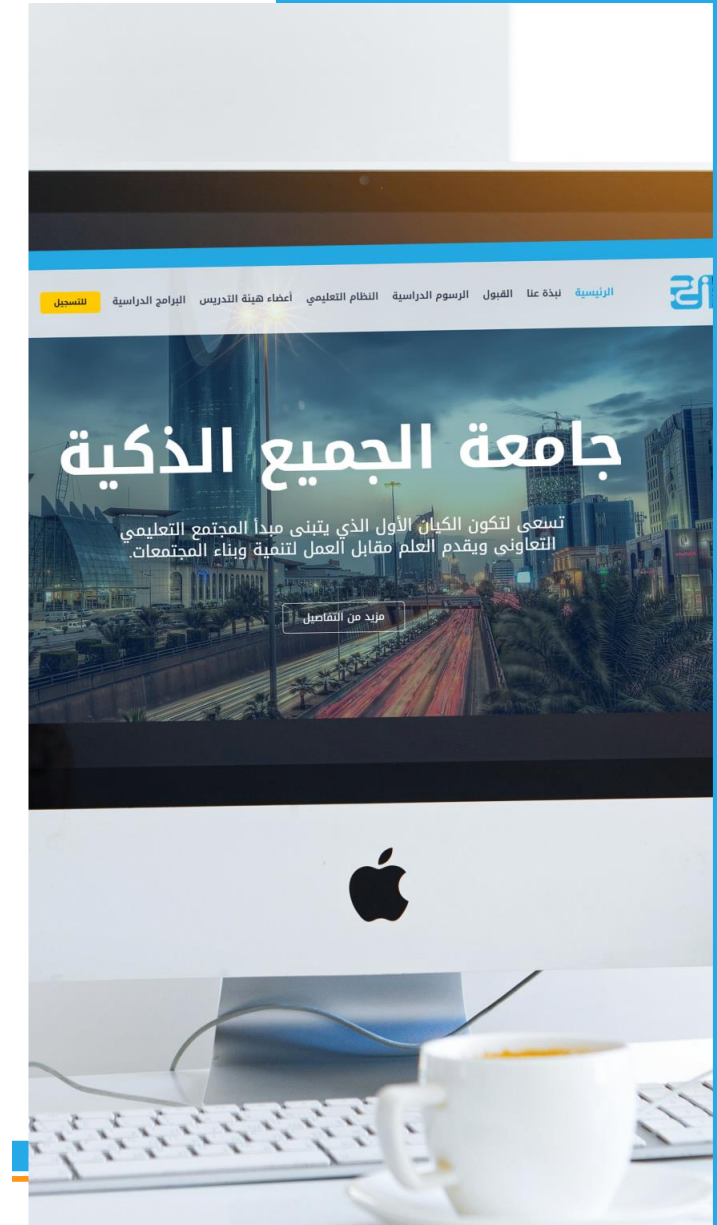
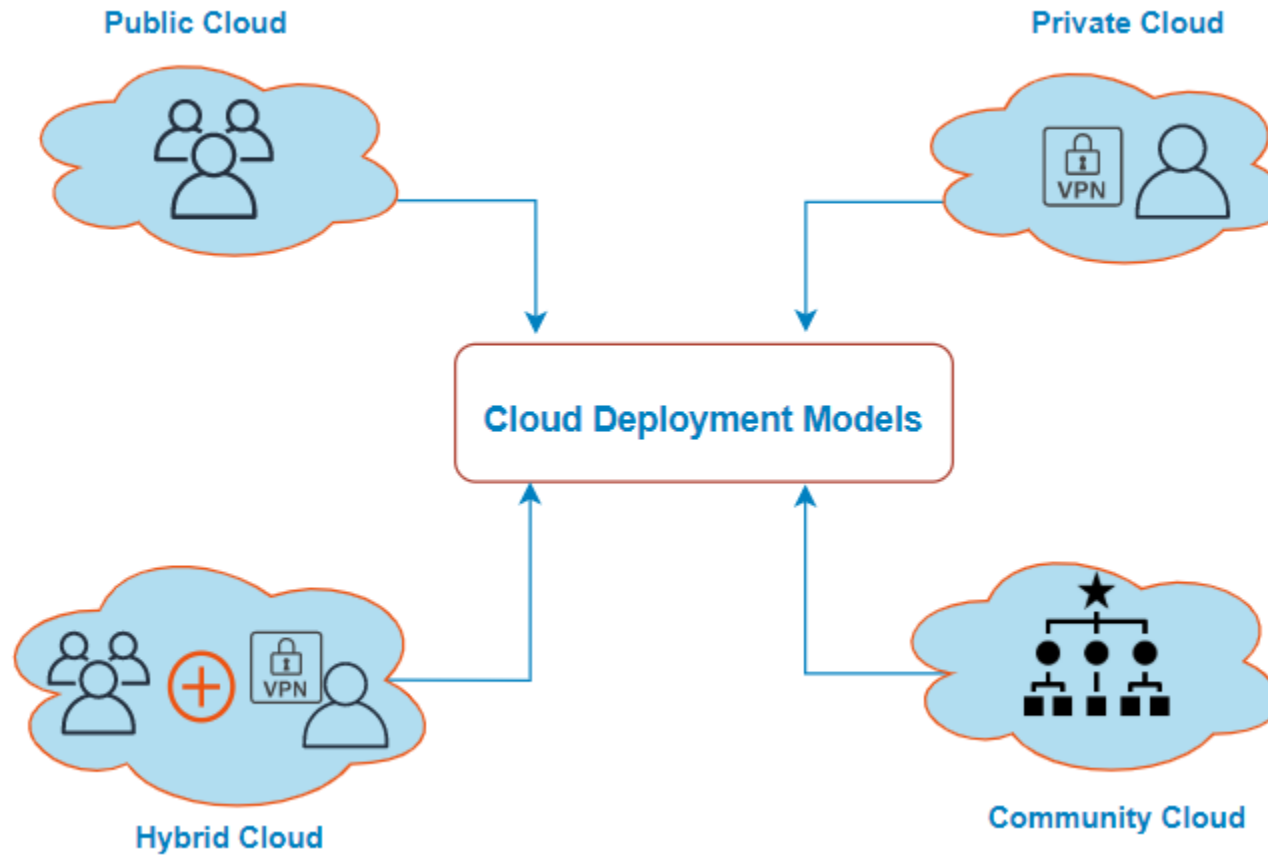
Lecture 8

Cloud Service Model

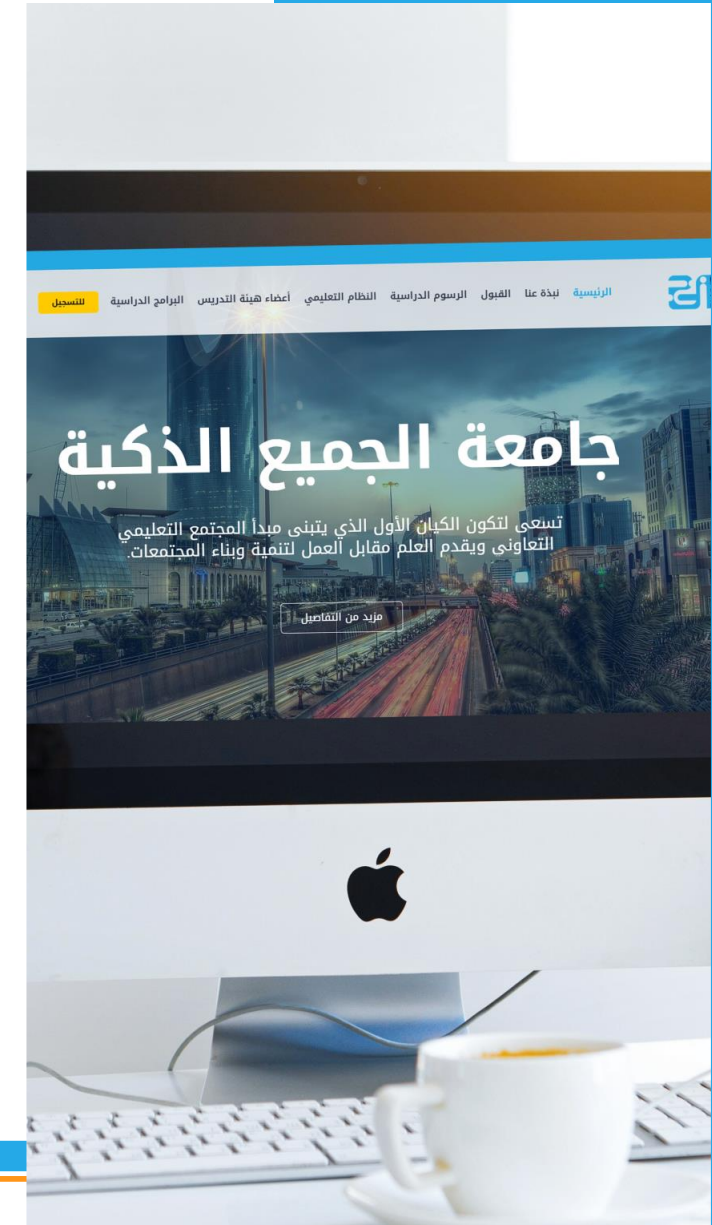


Lecture 8

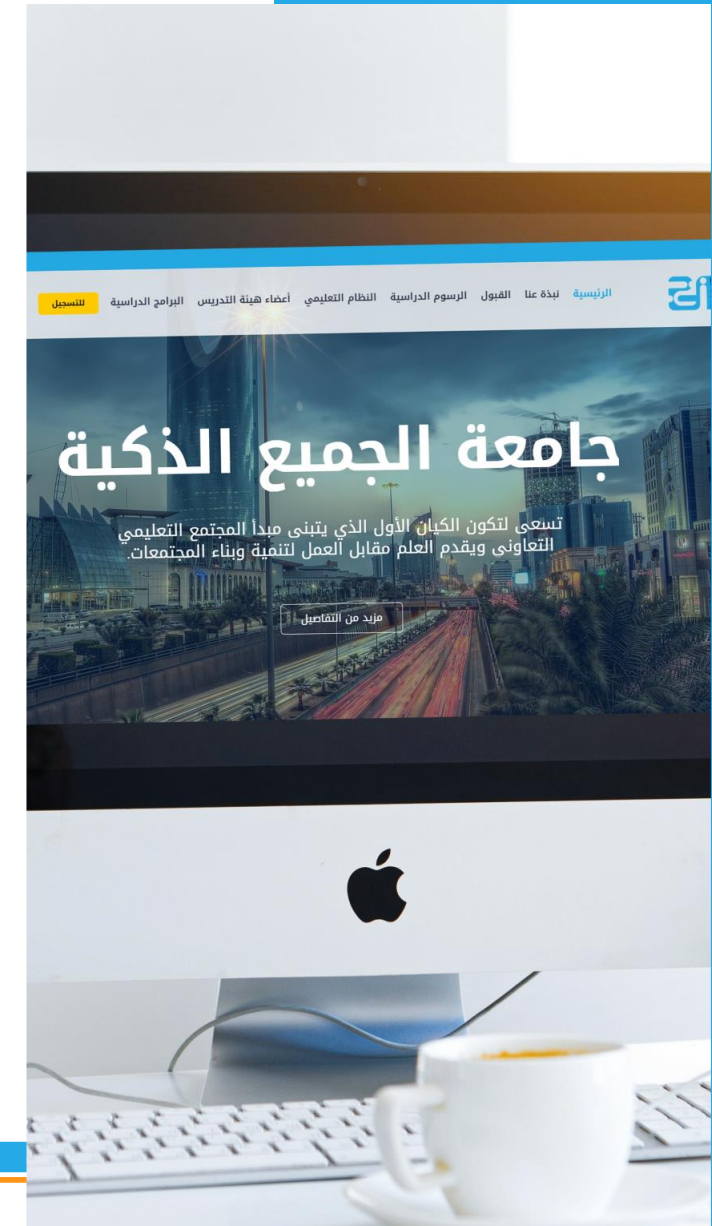
Cloud :Deployment Model



1. **Public Cloud:** Public clouds are available for all users who wants to use infrastructure such as computing resources.
2. **Private Cloud:** Private cloud is more expensive than public cloud, but it allows better control on security and privacy of organizations

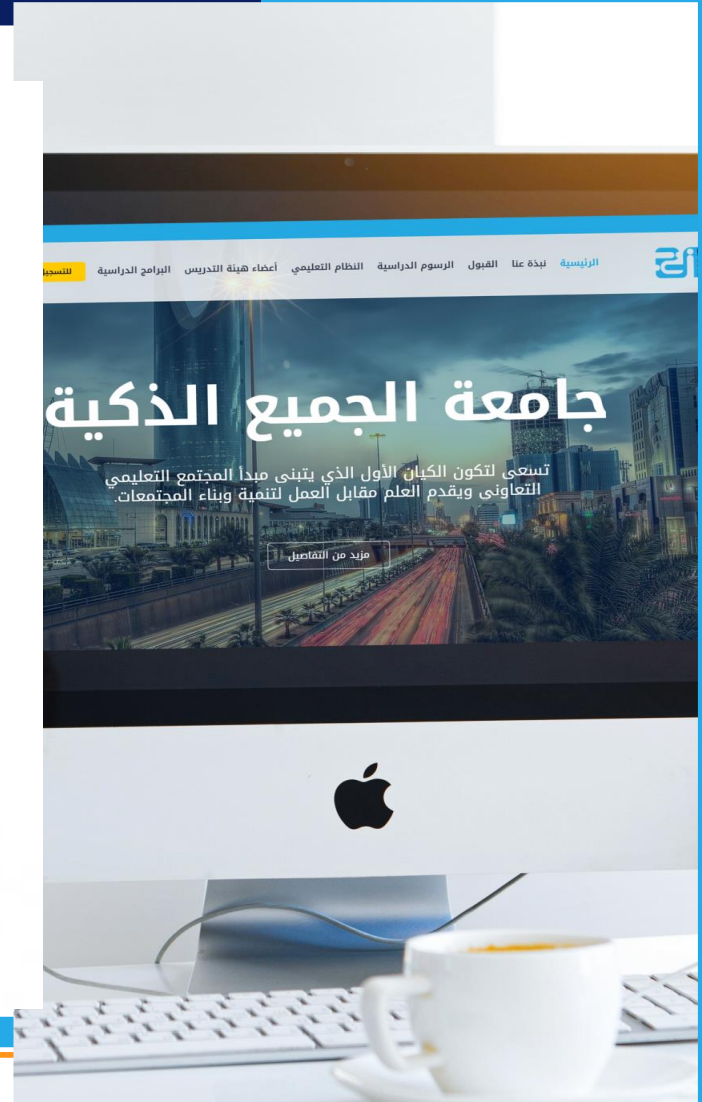
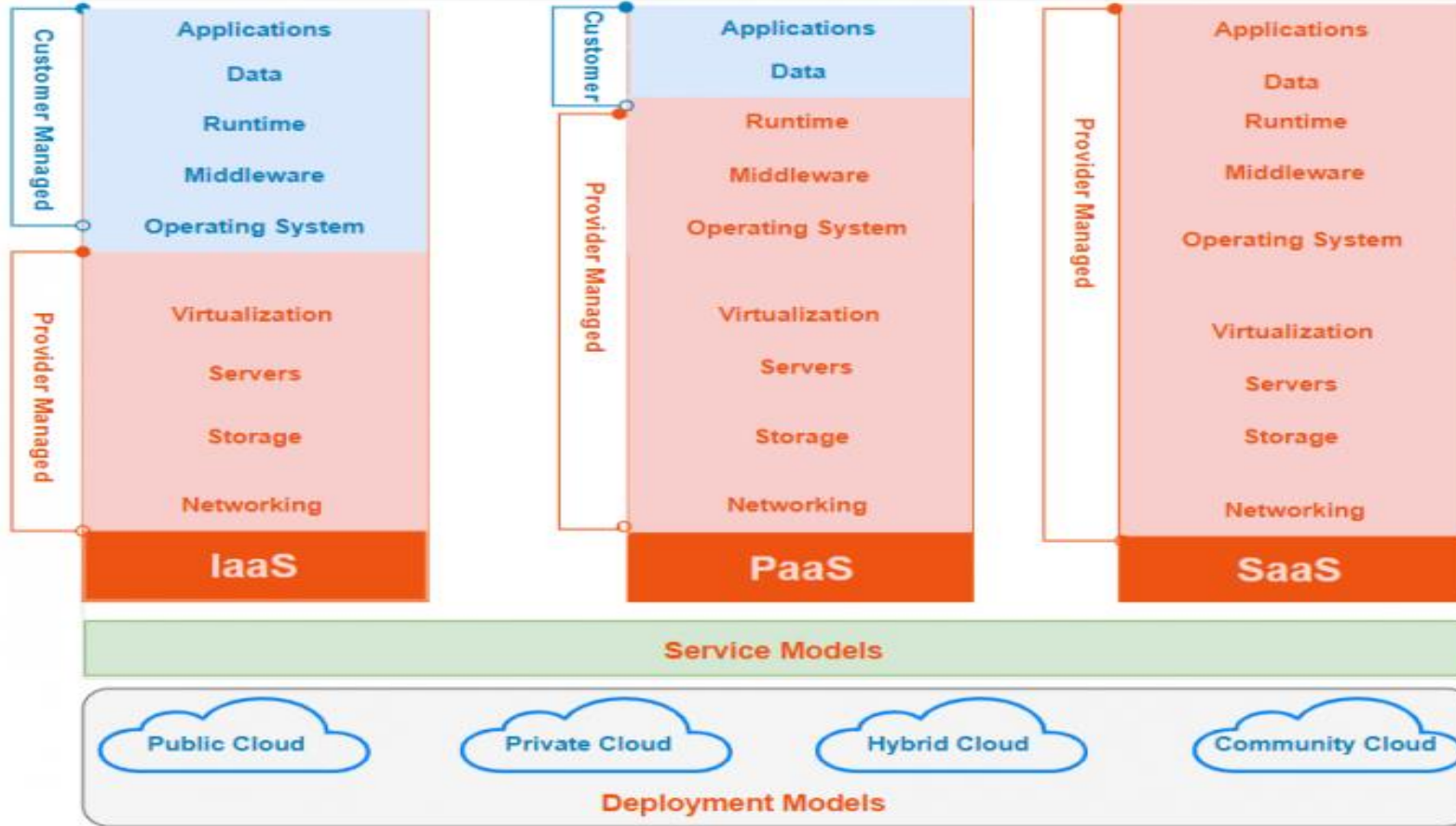


3. **Hybrid Cloud:** It is a combination of public and private cloud. For example, An organization can manage their mission-critical workloads on a secure private cloud and deploying less sensitive/secure ones to public cloud
4. **Community Cloud:** A community deployment model almost same as private cloud but the difference is sharing data between organizations.



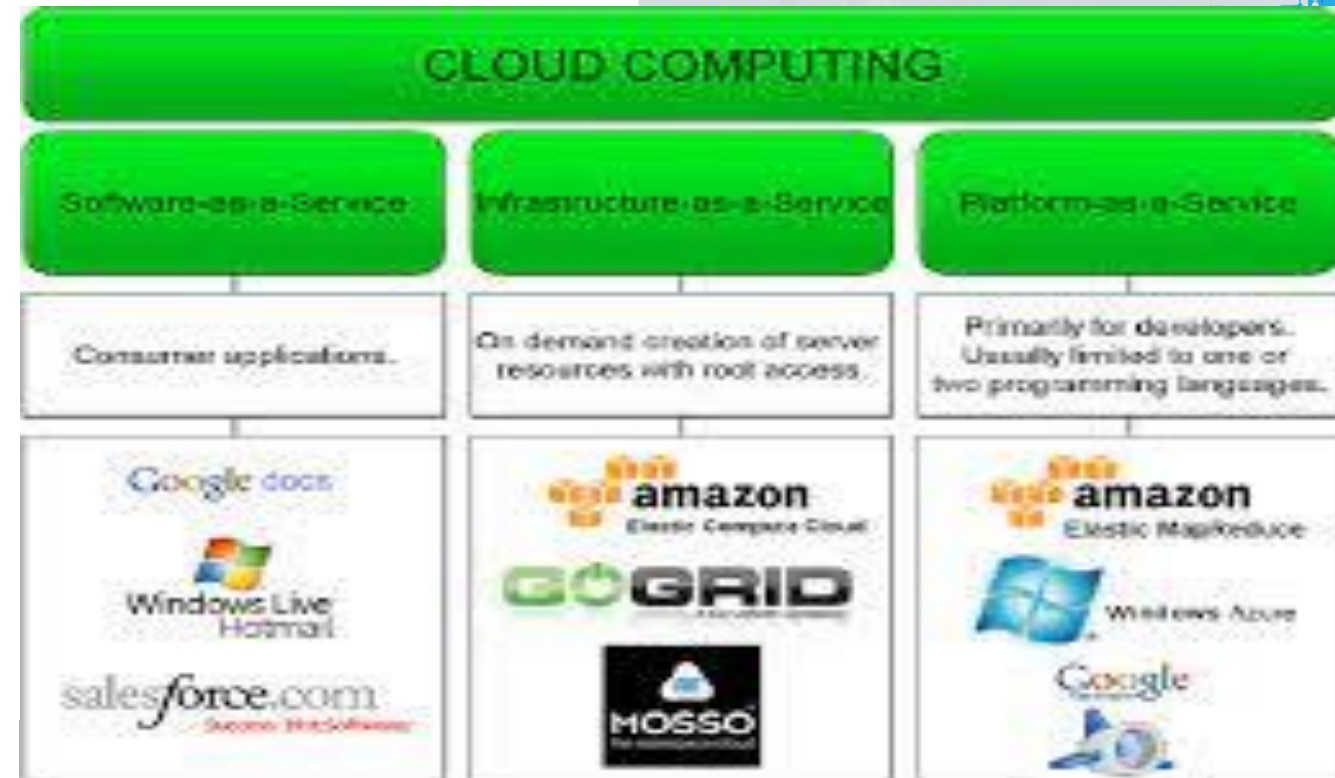
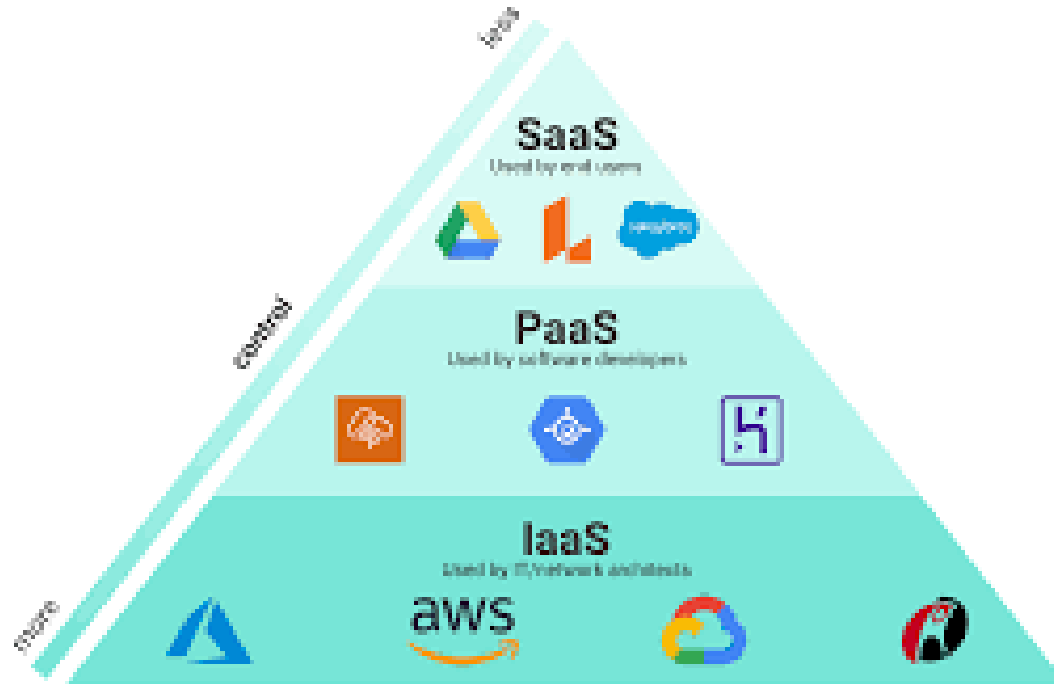
Lecture 8

Cloud Services and Deployment Model



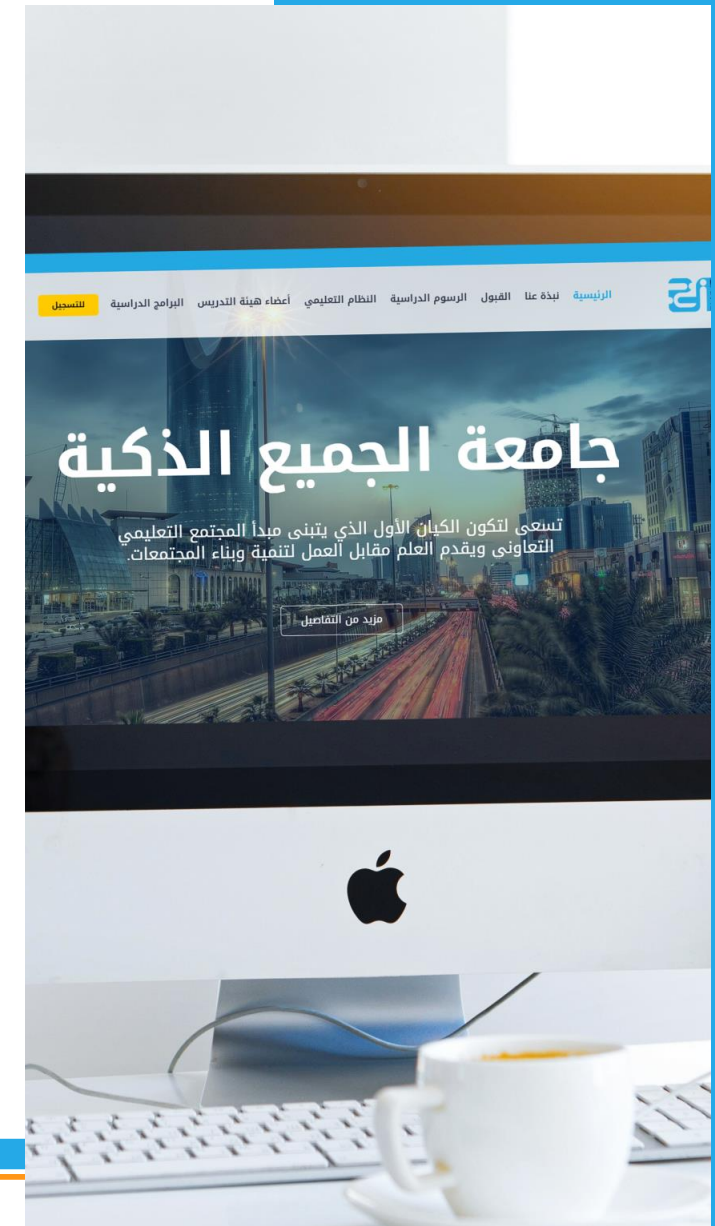
Lecture 8

Cloud Computing Examples

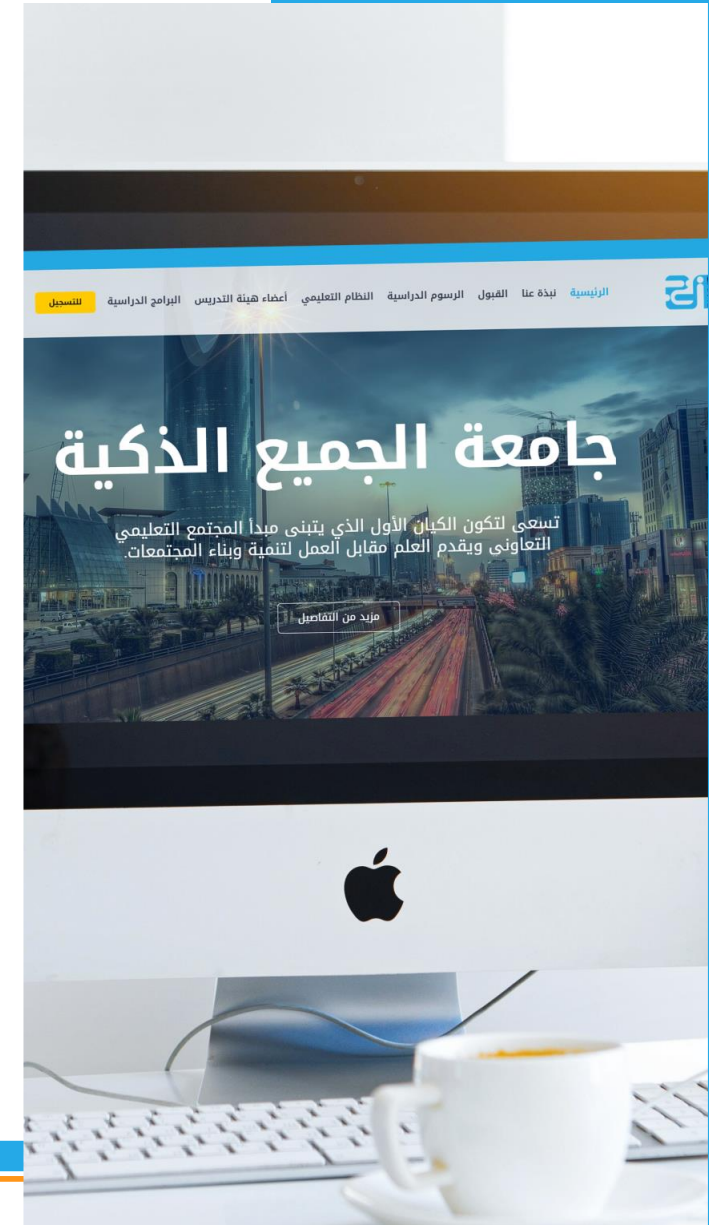


Lecture 8

Cloud Computing Threats

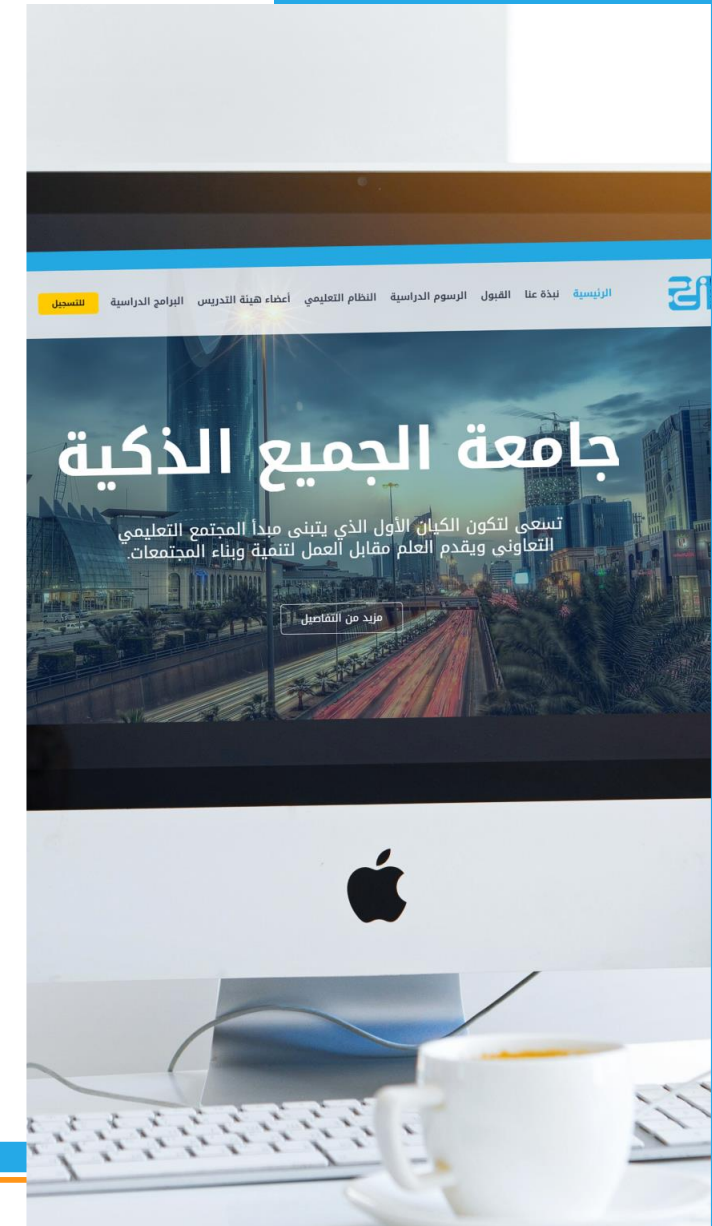


- Data breaches
- Insider threats
- Shared Technology Issues



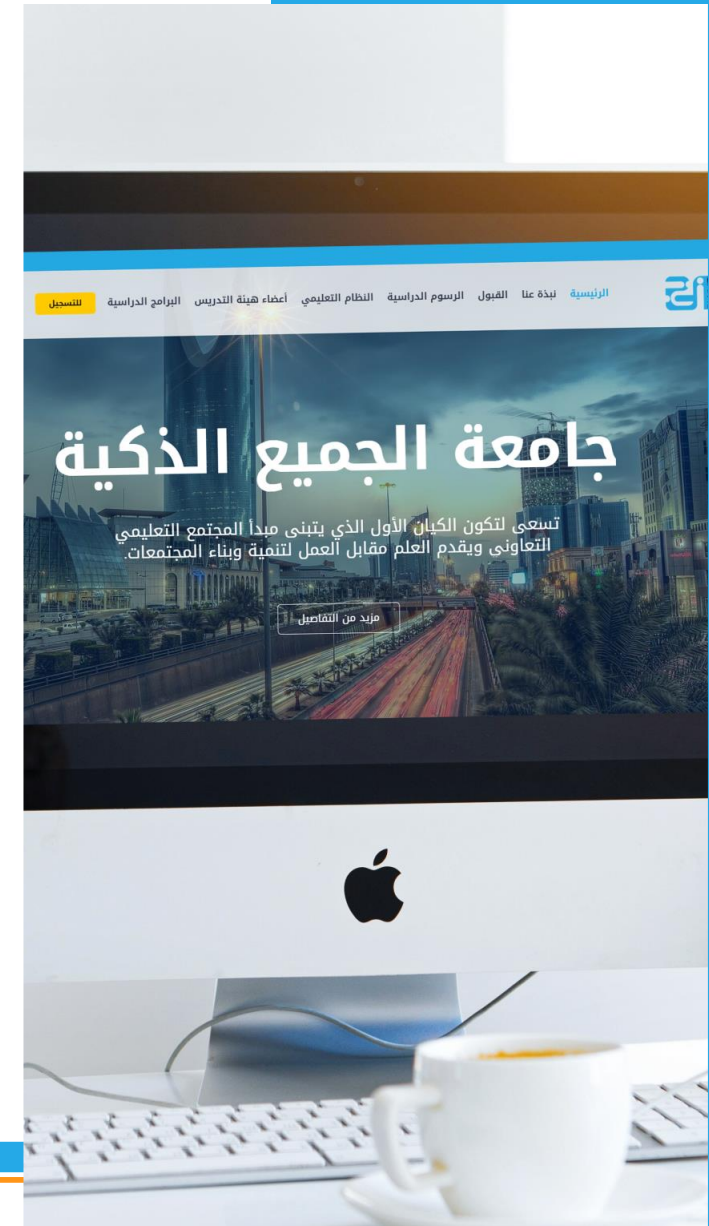
Data breaches

- Perhaps the most common threat to cloud computing is the issue of **leaks or loss of data** through data breaches.
- A data breach typically occurs when a business is attacked by cybercriminals who are able to gain unauthorized access to the cloud network or utilize programs to view, copy, and transmit data.
- Encryption Keys are lost or stolen
- Misuse of Data by Cloud Server Provider



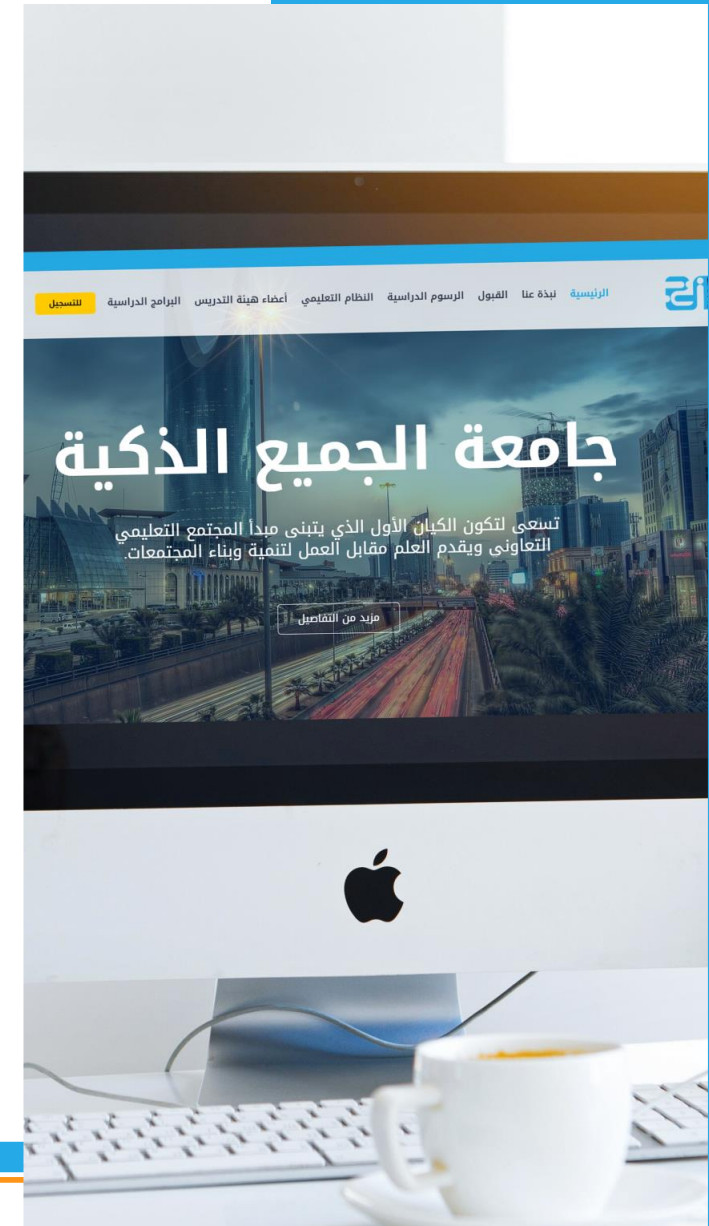
Insider threats

- sometimes the problem originates from the inside of the company.
- Insider threats can be malicious – such as members of staff going rogue – but they can also be due to negligence or simple human error.



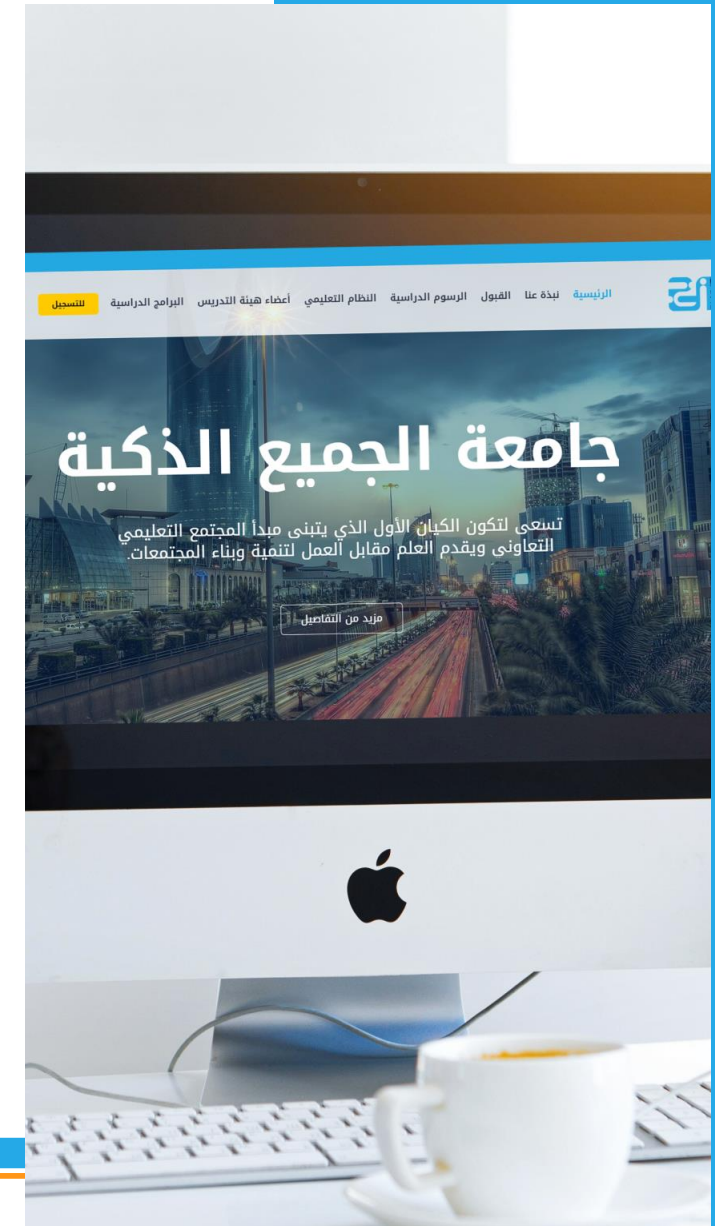
Shared Technology Issues

- Most underlying component of cloud infrastructure (ex: GPU ,CPU cash) does not offer strong isolation which enable attackers to attack other machines if they can exploit vulnerabilities in one client application

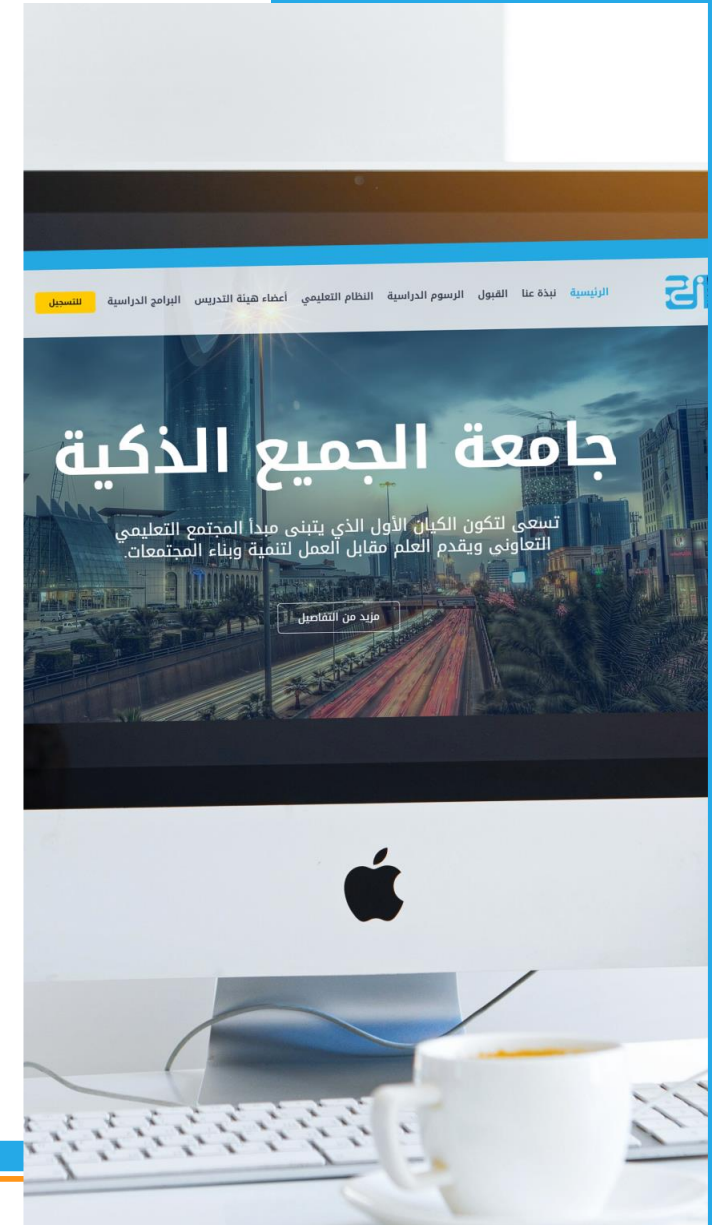


Lecture 8

Cloud Computing Attacks

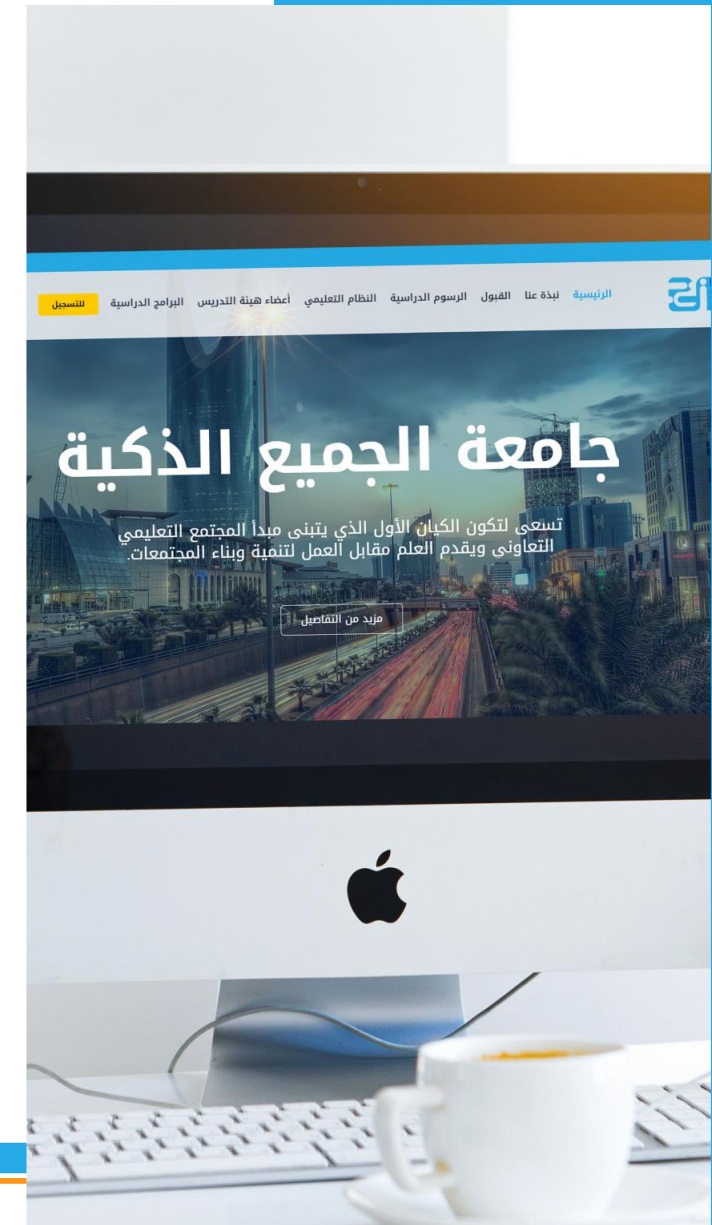


- DOS attack
- Hijacking accounts
- SQL injection attack
- DNS Attack



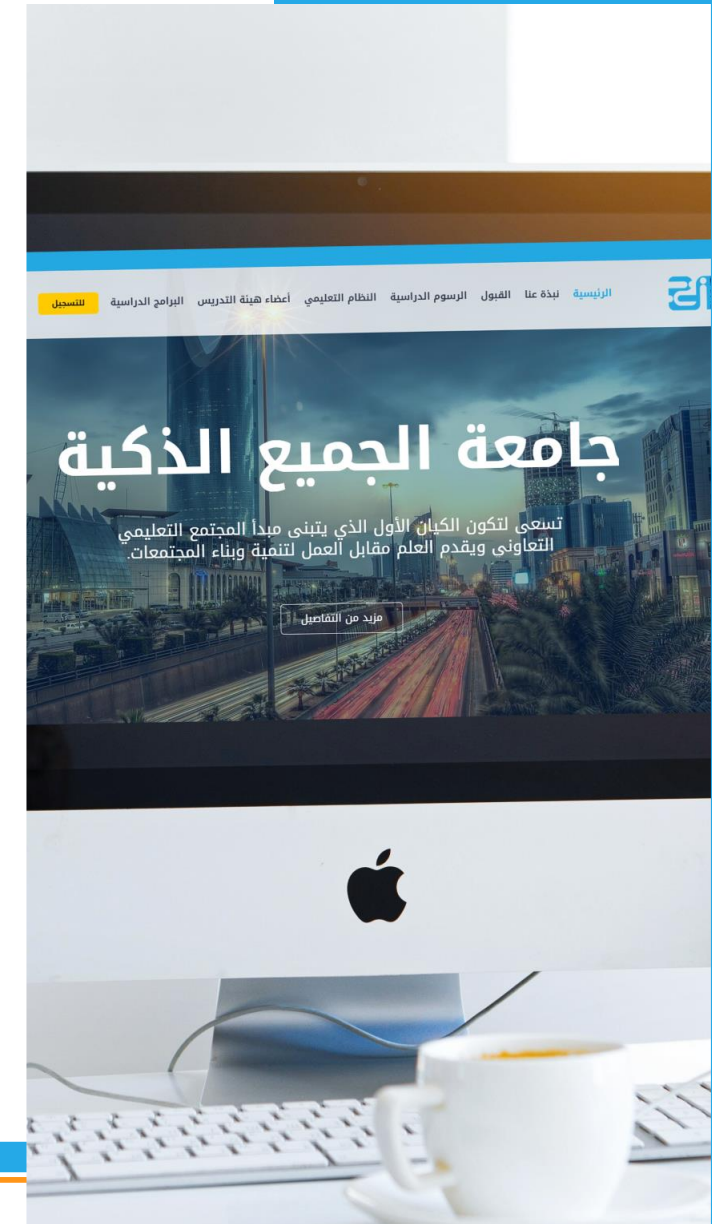
Denial of service

- One of the most damaging threats to cloud computing is a denial of service (DoS) attack.
- These can shut down your cloud services and make them unavailable both to your users and customers, but also to your staff and business as a whole.

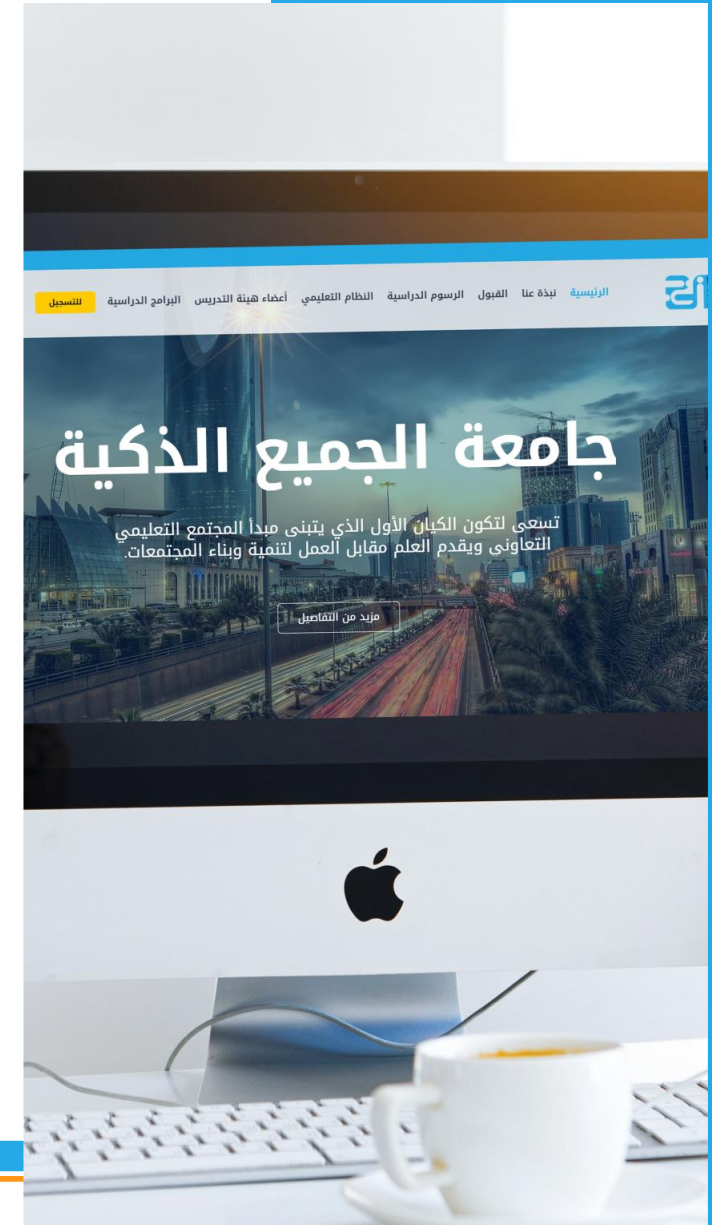


Hijacking accounts

- Perhaps the greatest threat to a business that uses cloud computing technologies is the challenge of hijacked accounts.
- If a criminal can gain access to your system through a staff account, they could potentially have full access to all of the information on your servers without you even realizing any crime has taken place.

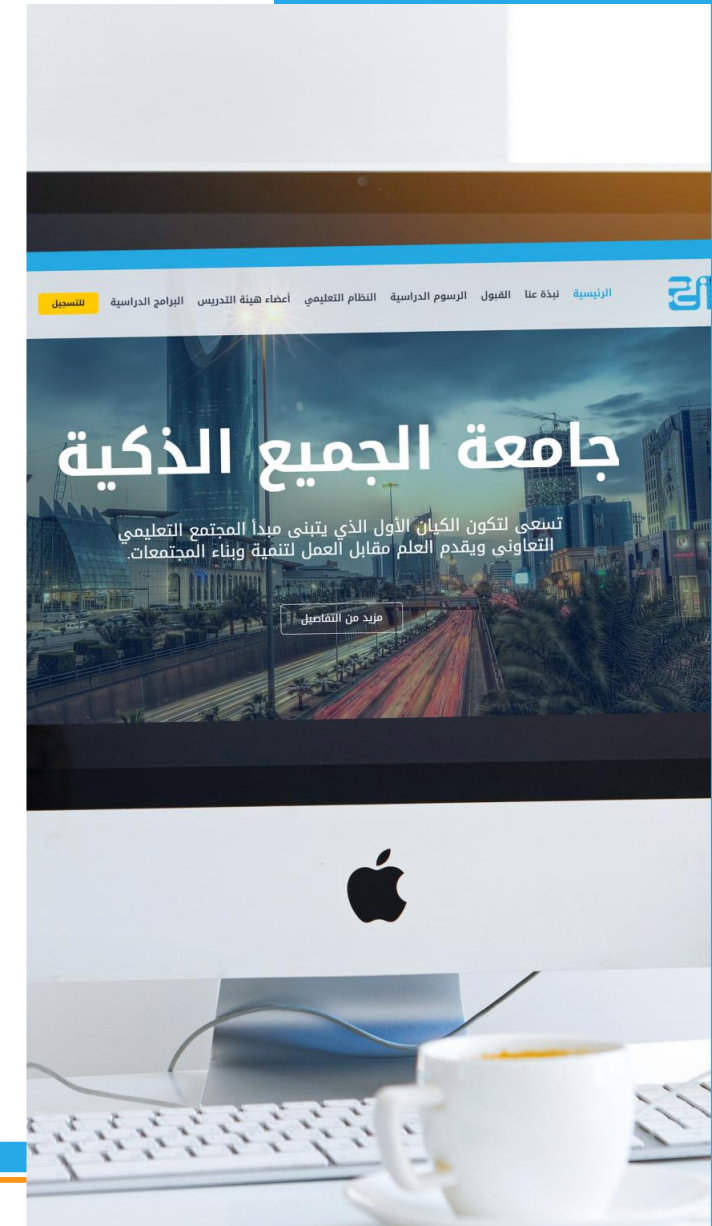


- **SQL Injection**
- In SQL Injection the attacker attacks malicious code into stander SQL code to gain unauthorized access to the database.



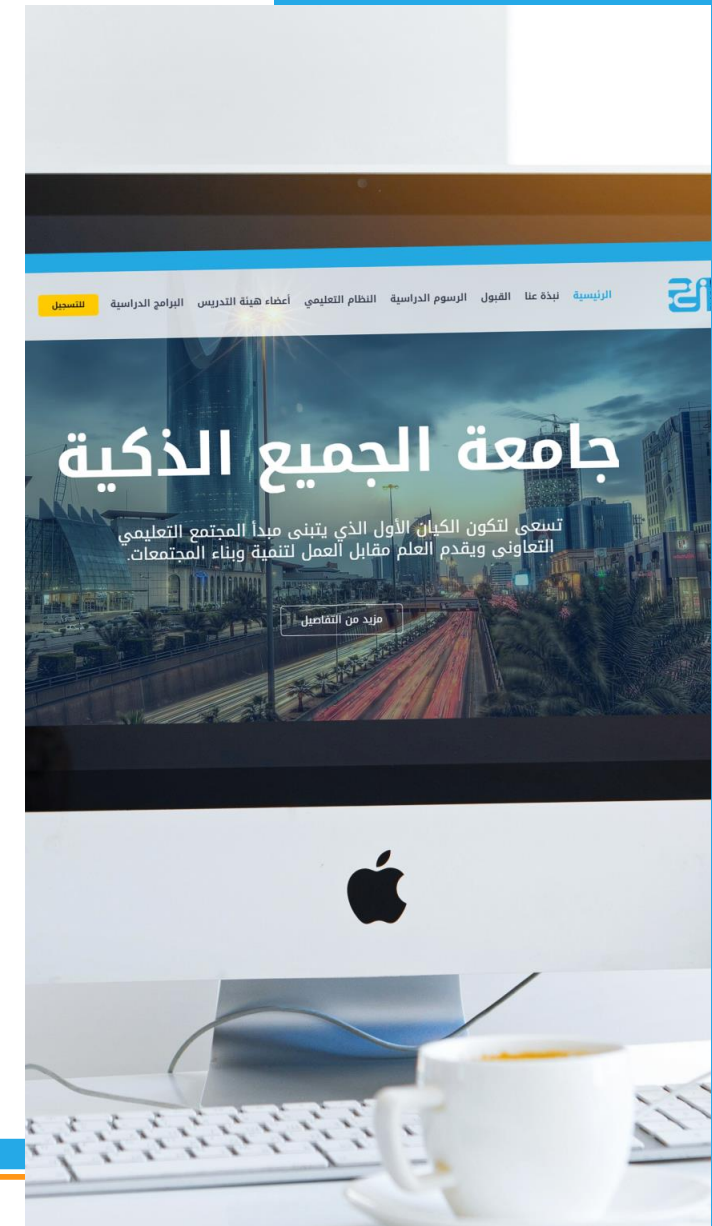
DNS Attack (Domain Name Server)

- attackers are able to compromise a registrar that manages DNS records, it has the potential to impact a broad number of organizations and individuals.
- The user query the internal DNS server to get DNS Information, DNS internal query the respective cloud server , the attacker block the DNS response and send DNS response with IP for fake website . The DNS Internal server will update his cash with the fake website.

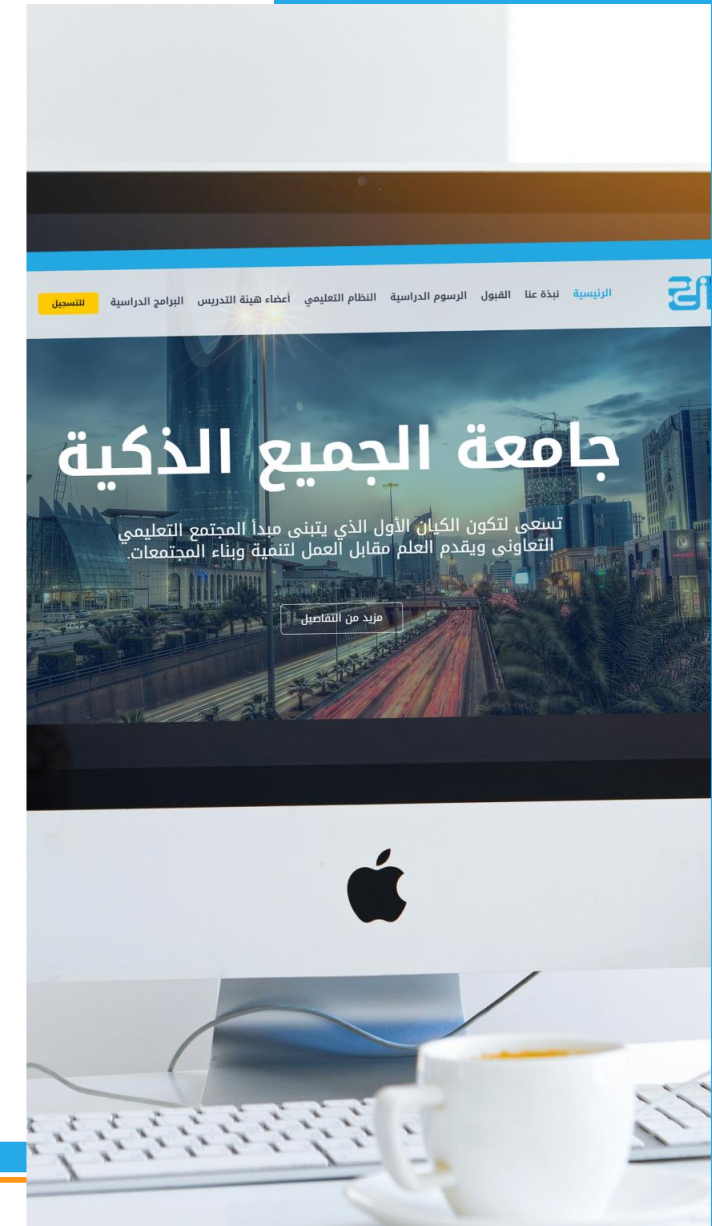


Lecture 8

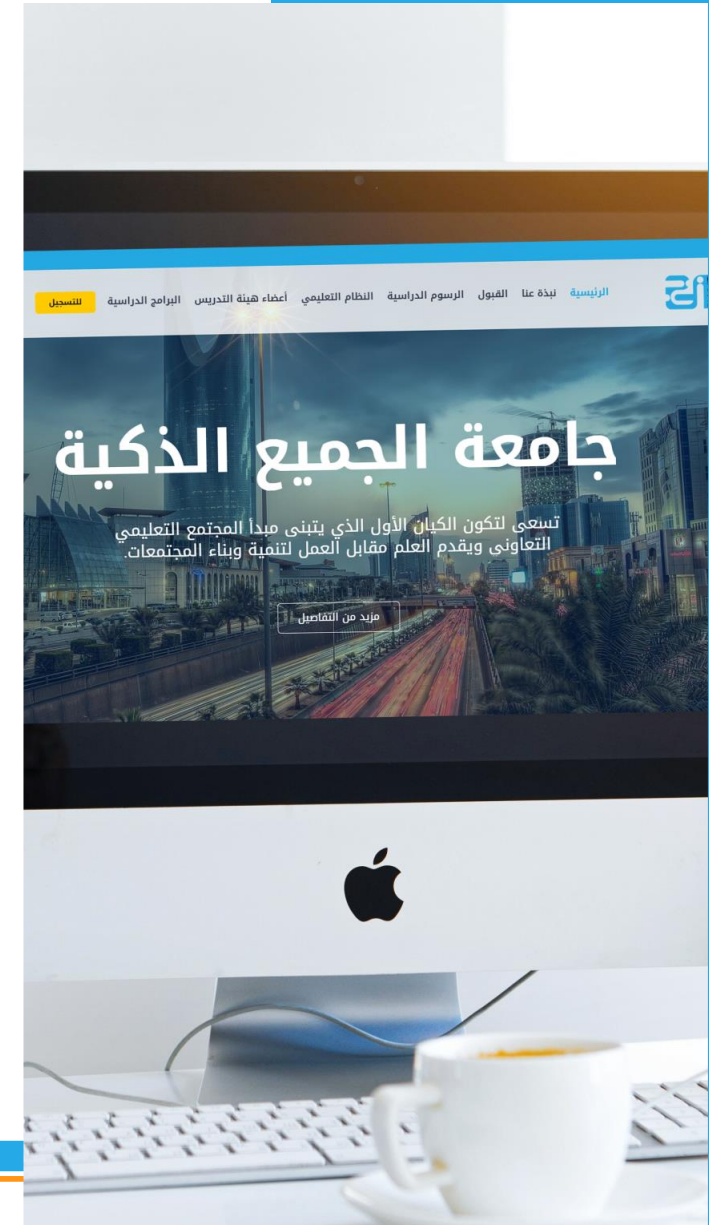
Cloud Forensics



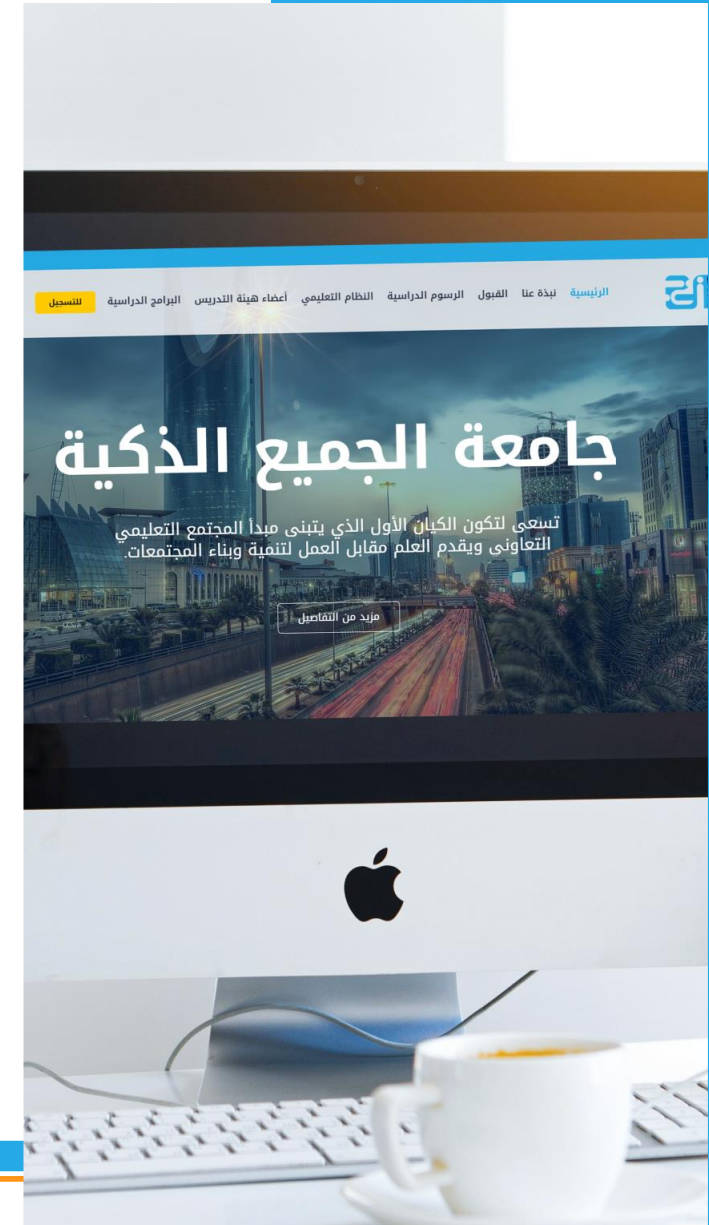
- Cloud forensics refers to the use of forensic techniques to investigate cloud environments.
- When criminal behavior has occurred using the cloud, cloud forensics experts use their skills and knowledge to detect the individuals or groups responsible.
- Cloud forensics encompasses users of the cloud, both victims and perpetrators.
- For example, a company using cloud servers might be the victim of a data breach or denial of the service incident. Criminals themselves might also use the cloud to launch an attack.



- As with other subfields of forensics, cloud forensic investigators must follow strict regulations to ensure their work is admissible in a court of law.

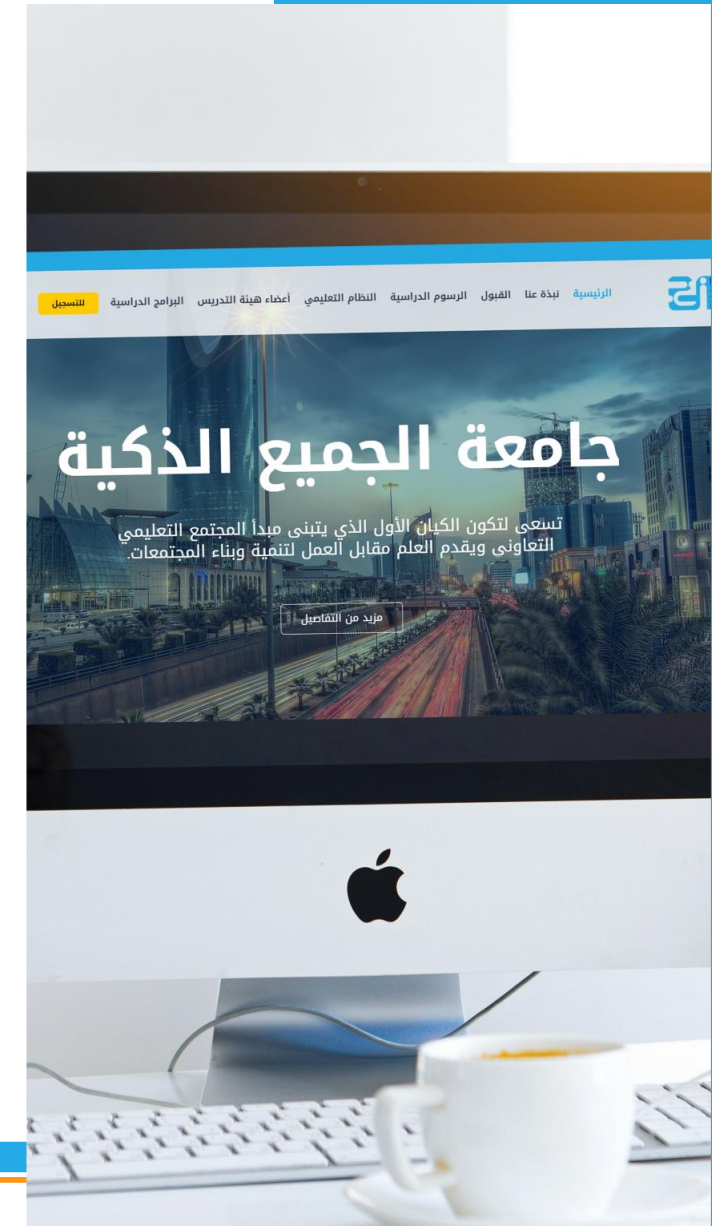


- Unlike traditional digital forensics, cloud forensics can be a bit more complicated, since data may be hosted outside of local dominions.
- The investigator have no control over the ones hired by CSP to investigate.

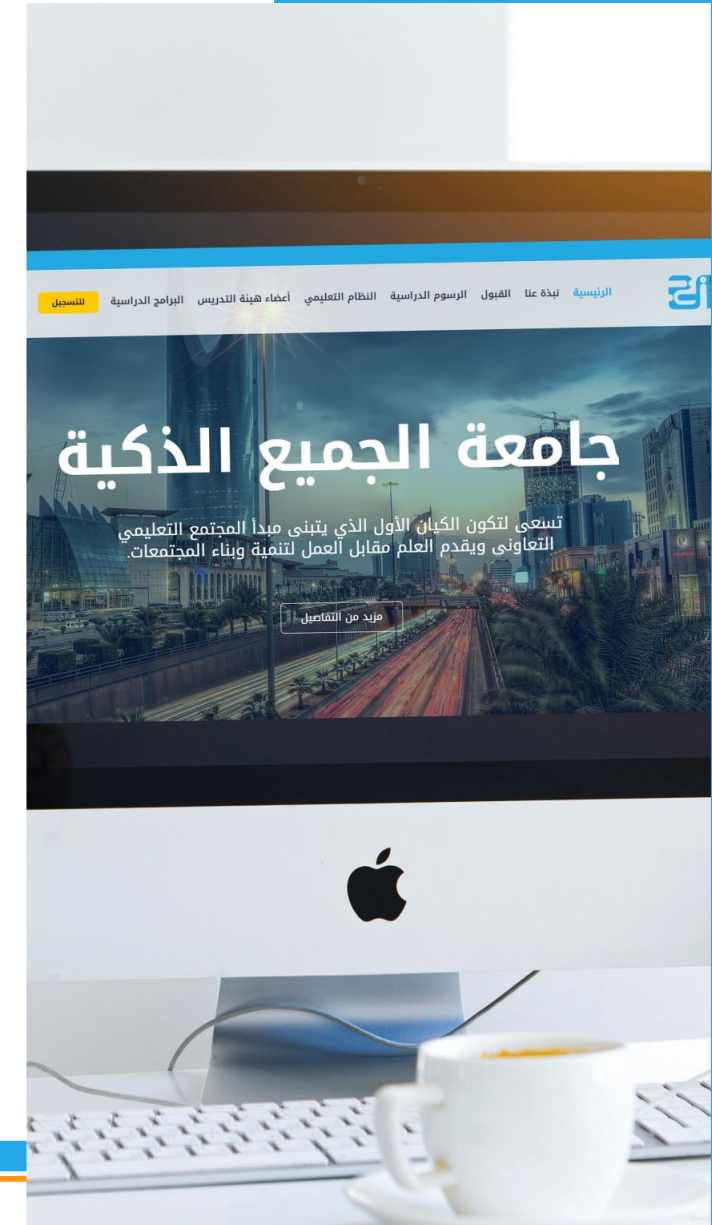


Cloud Forensics Challenge

- Cloud forensic stakeholders consist of private enterprises, government members, law enforcement, etc.
- Cloud forensic investigators are expected to know the roles and responsibilities of each stakeholder to perform an investigation effectively.
- As a cloud forensic investigator, the main challenge for you is to ensure the security of the digital evidence and make sure it is not tampered with by third parties.



- In the PaaS (Platform-as-a-Service) and SaaS (Software-as-a-Service) cloud computing service model, users are dependent on the cloud service providers (CSPs). They do not have access to their logs due to a lack of control over hardware.



Lecture 8

Cloud Crime

Cloud as subject

In this case , crime is carried out within the cloud environment.

Ex: identity theft of cloud user's account

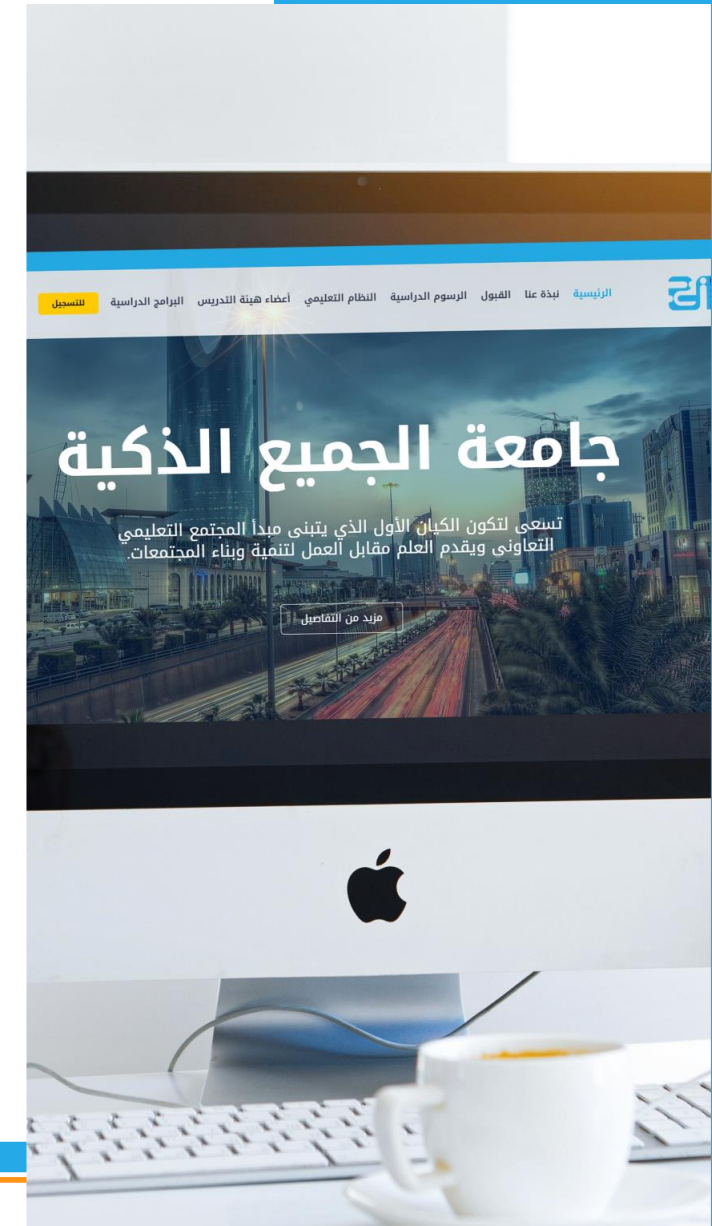
Cloud as Object

In this case, target of the crime is the CSP.

Ex: Techniques such as DDOS attacks are implemented that target few sections of the cloud or the entire cloud

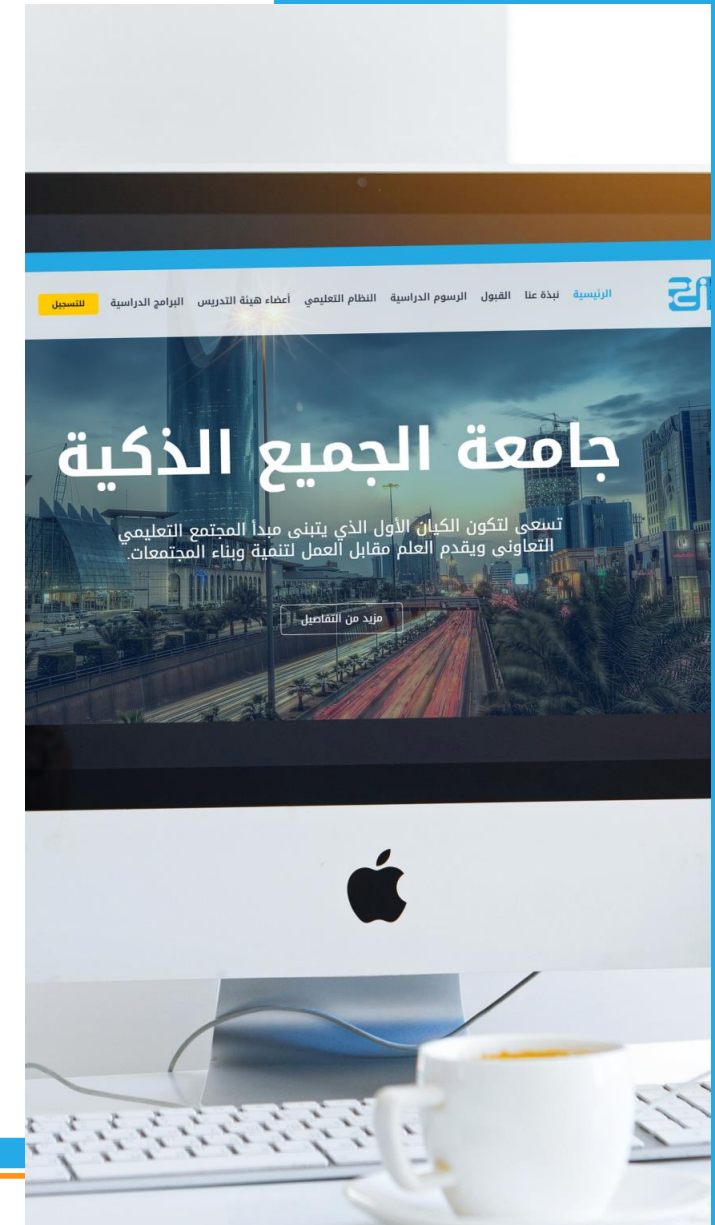
Cloud as a tool

In this case, cloud is used to plan and carry out a crime case include suing a cloud to perform an attack on other cloud or when a crime related evidence is saved and shared in the cloud



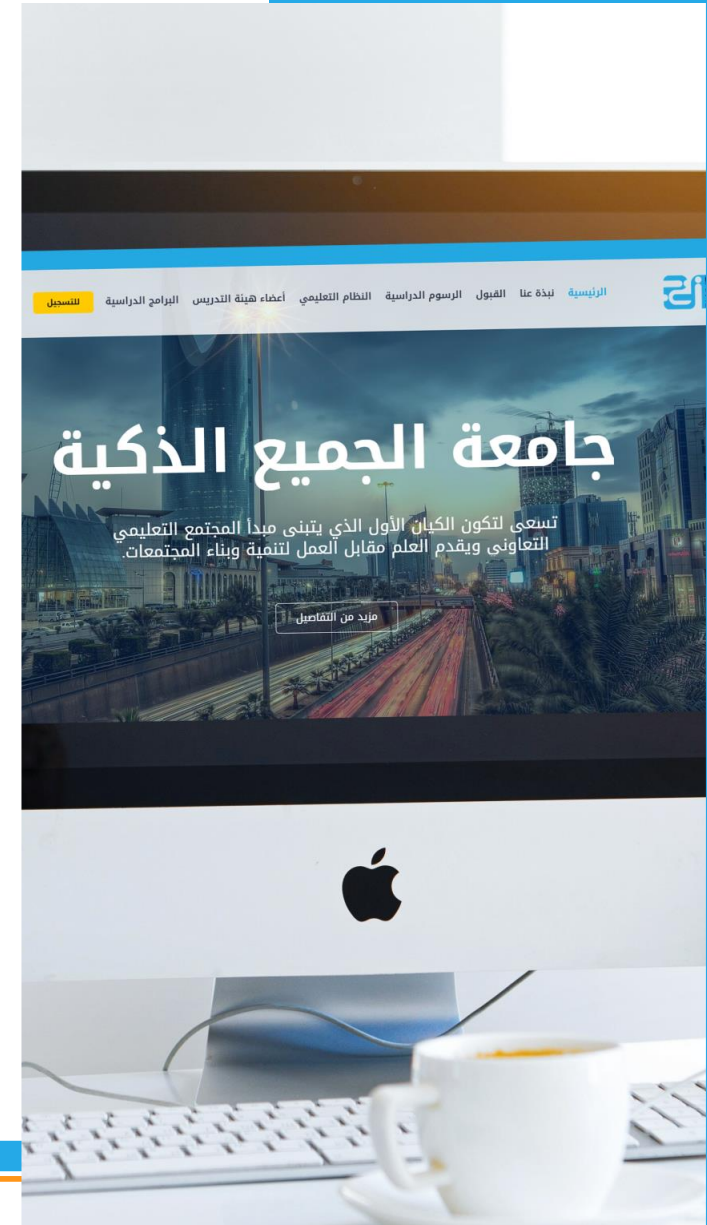
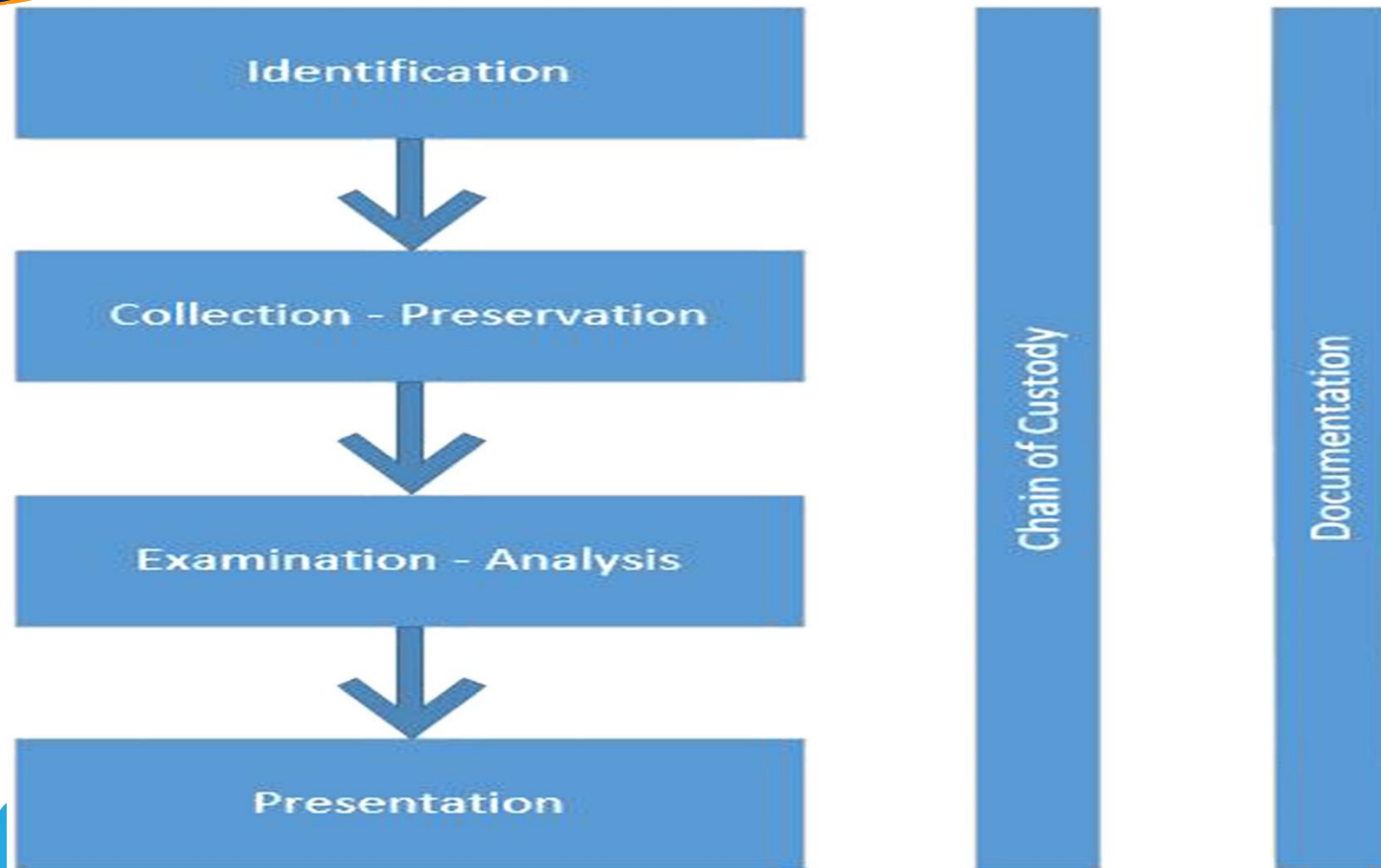
Lecture 8

Cloud Forensic Steps



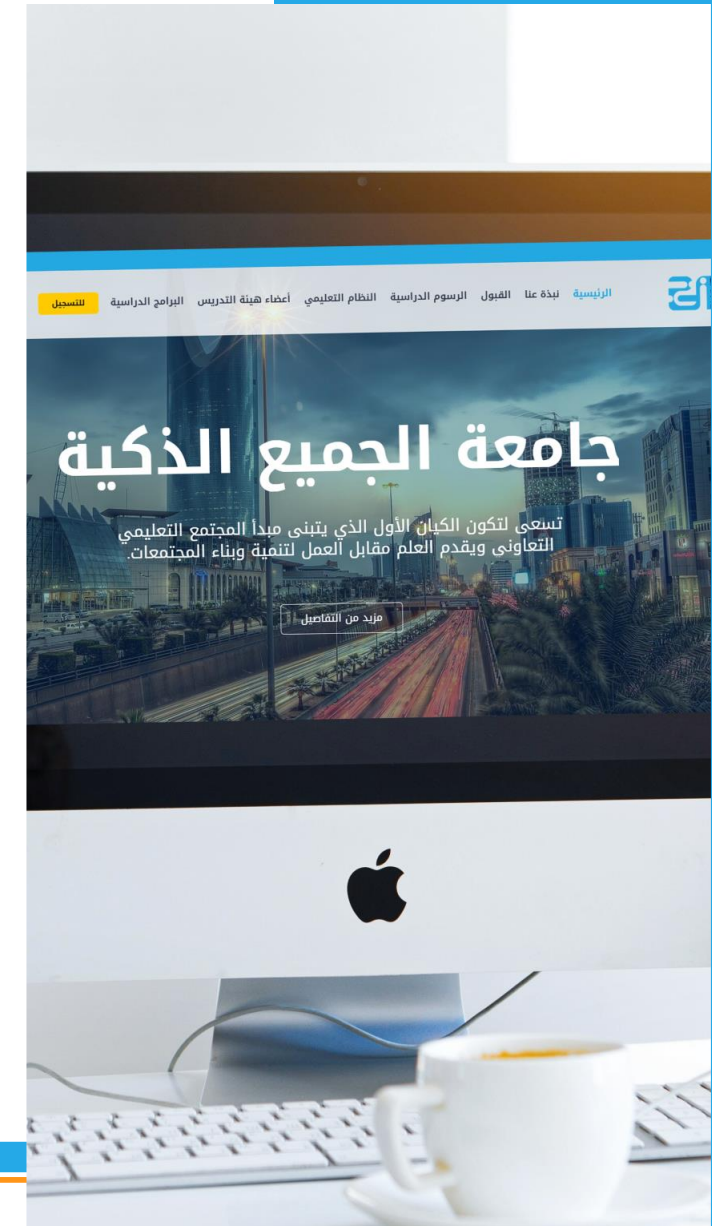
Lecture 8

Cloud Forensic Steps



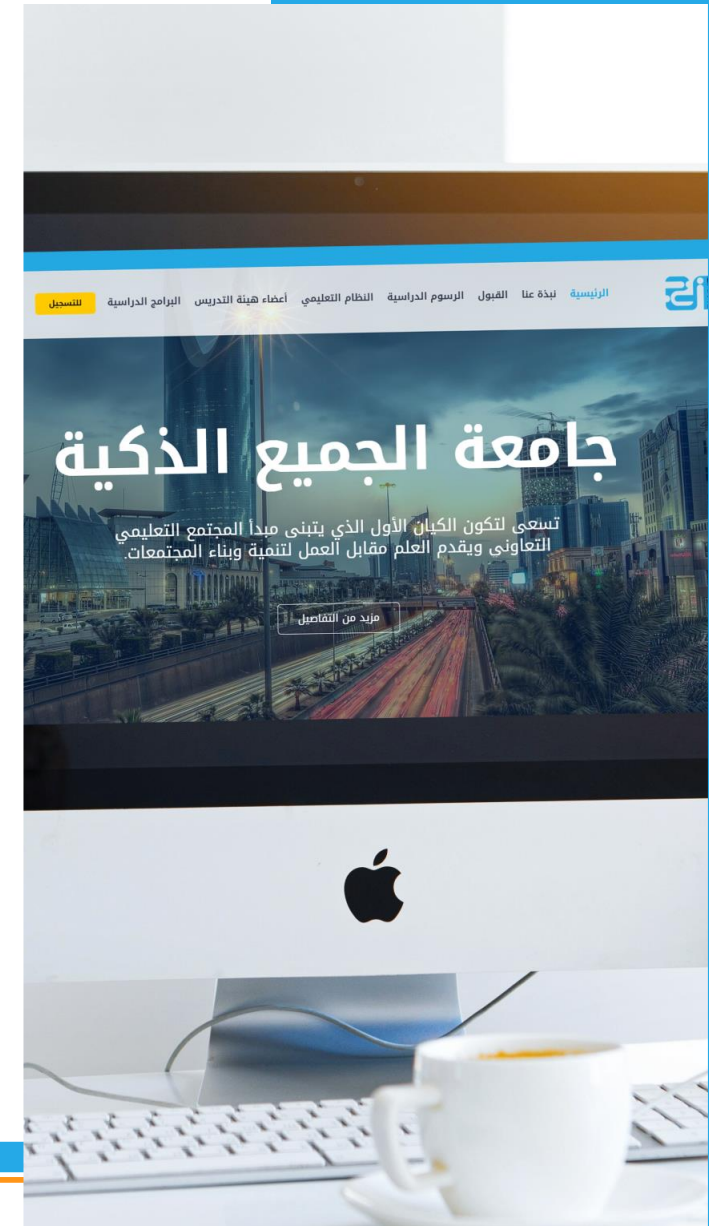
Identification:

- Is the first stage, and the main concern is to identify all possible sources that may contain potential evidence in a cloud environment, in order to prove that the incident took place.
- Investigators need to determine the type of crime and what type of assets (hardware, software, and data) has been used.



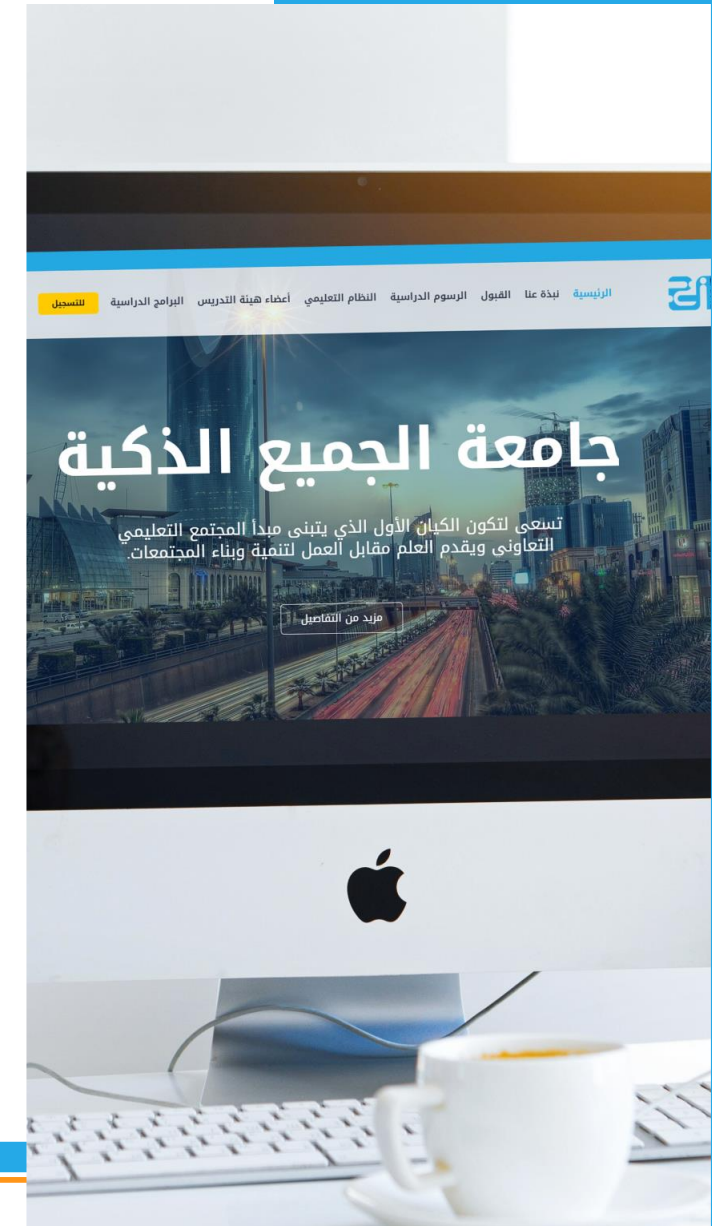
Identification:

- They also need to identify the location of the incident and the cloud provider.
- An investigation team is formed consisting of people with special skills in cloud environments, such as legal advisors, experienced technicians, and law officers. In this stage, a search warrant needs to be issued to attain access to CSP's infrastructure



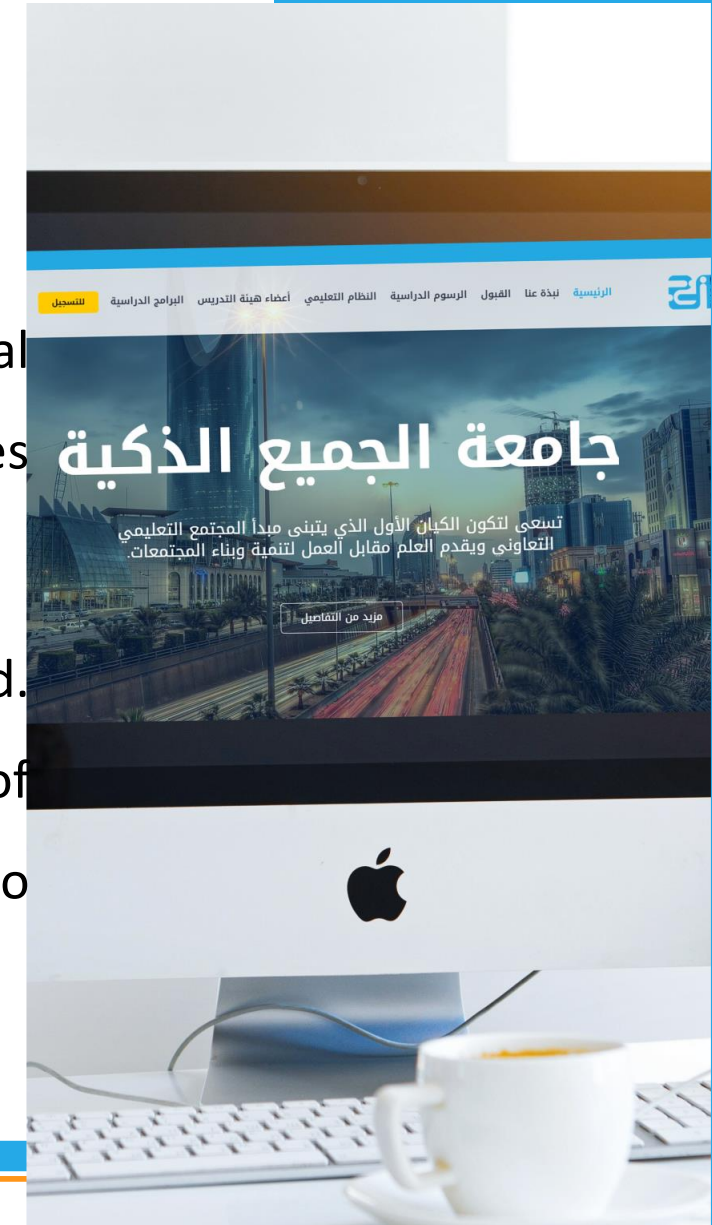
Preservation —Collection.

- After identifying the potential evidence, the collection and acquisition of the evidence from the locations they reside in clouds follows. Investigators need to isolate and preserve the evidence by preventing people from using the digital device or by duplicating digital evidence.
- During the collection-acquisition specific resources will be used.



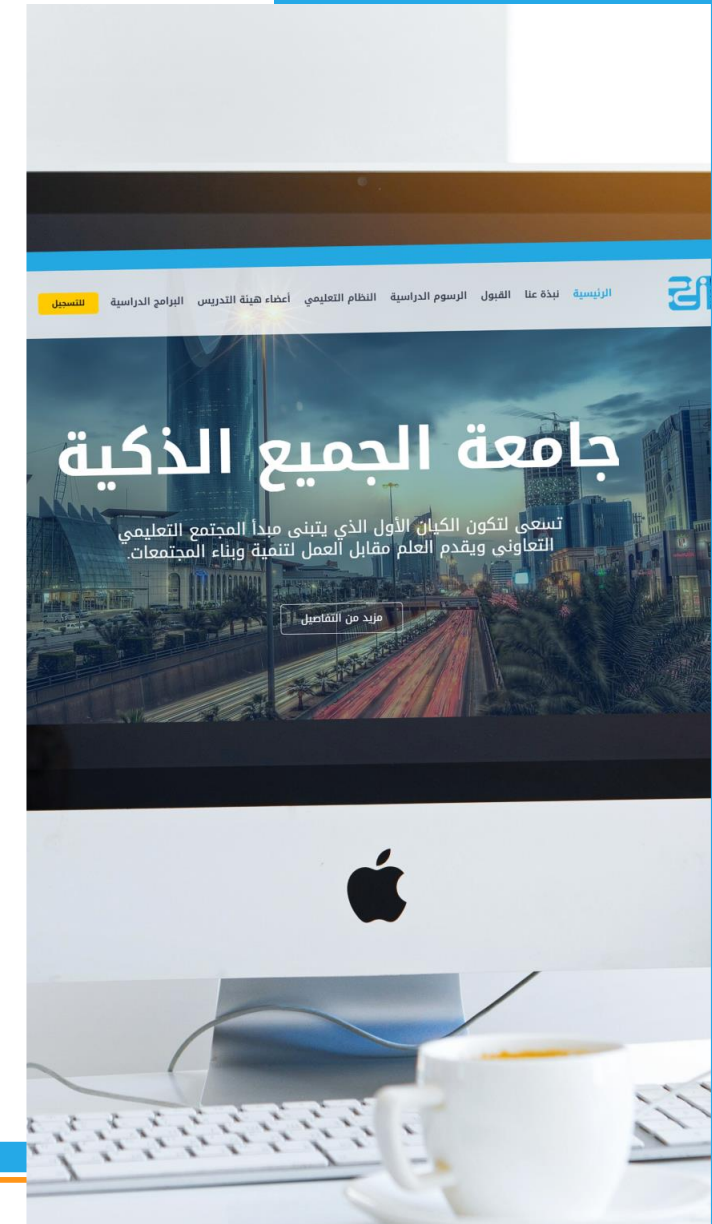
Preservation — Collection.

- This involves well trained personnel (internal or even external), special tools for cloud extraction data, and up-to-date methodologies/processes such as protection mechanisms and action plans.
- Integrity and unauthorized alterations of digital evidence must be ensured. The most important issue in this step is to maintain the chain of custody of the evidence and to ensure the validity and the integrity of them in order to be used in a court of law.



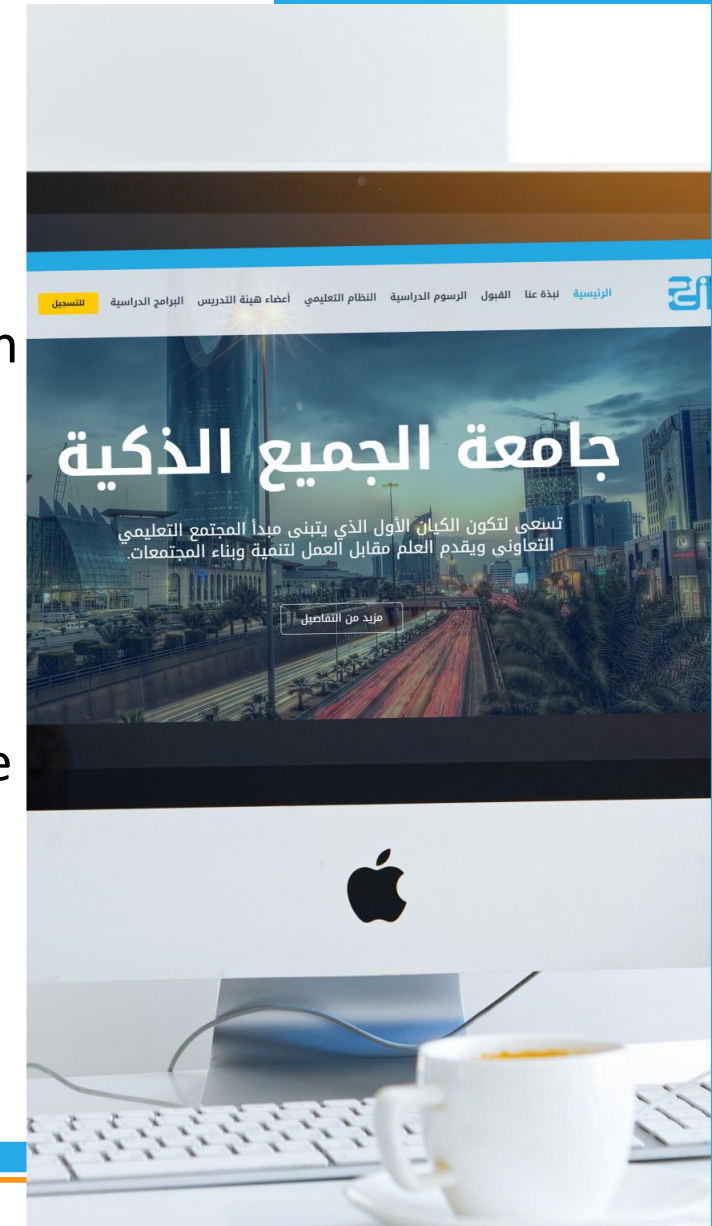
Examination — Analysis

- involves the extraction of data from the previous stage and the inspection of the huge amount of data identified. Trained personnel and technician experts should examine all the data to find evidence.
- Examiners should review previously encountered cases and training plans to find patterns that can help reduce the time of the examination and develop their action plan.

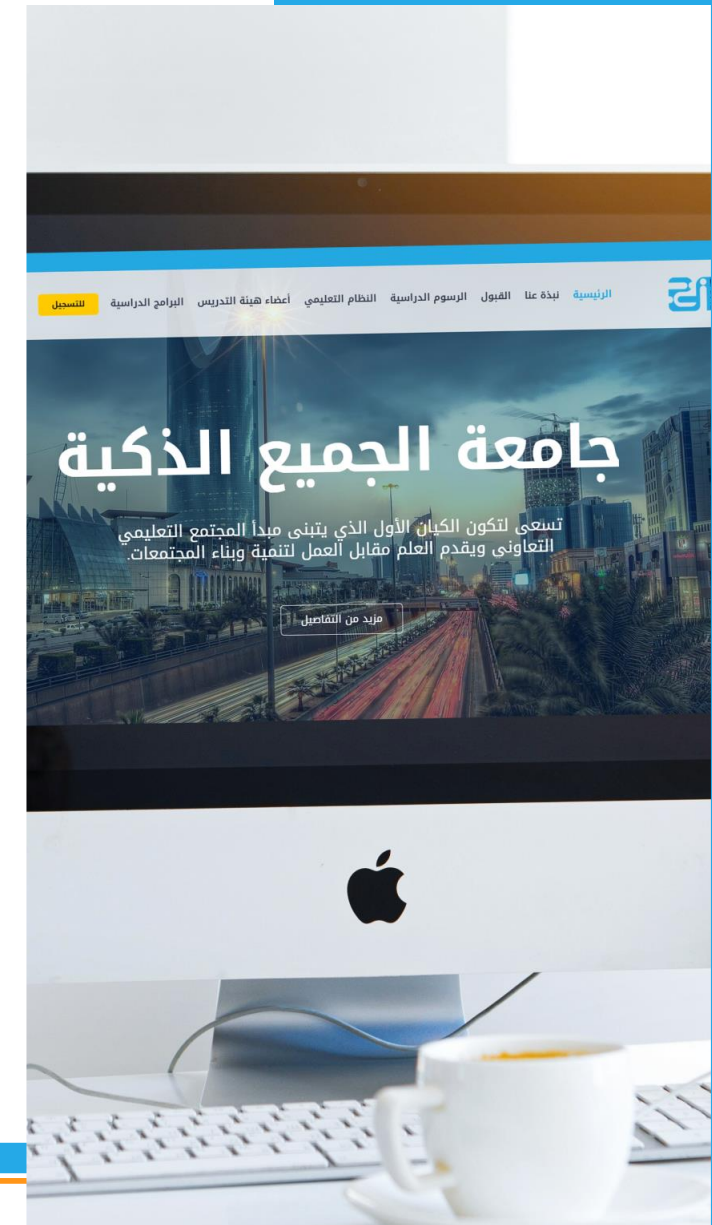


Presentation stage

- Is the final stage and deals with the presentation of the evidence in a court of law.
- A well-documented report with findings must be produced using expert testimony on the analysis of the evidence.
- Experts with personal knowledge of the procedures that generate the reports should be chosen.
- They should be prepared to confront the jury who lacks knowledge of cloud computing.
- Evidence must be presented in a way that the jury will understand all the technical details because cloud computing is a very complicated environment for ordinary Internet users to understand.



- Most commonly used cloud storage services amazon, Dropbox ,Google, Microsoft etc.
- User can use these cloud services through the web site or by installing a platform-based application on their systems.
- When the clients start using these services, they create folders and save files on the system which can be used as evidences in case of security incident.

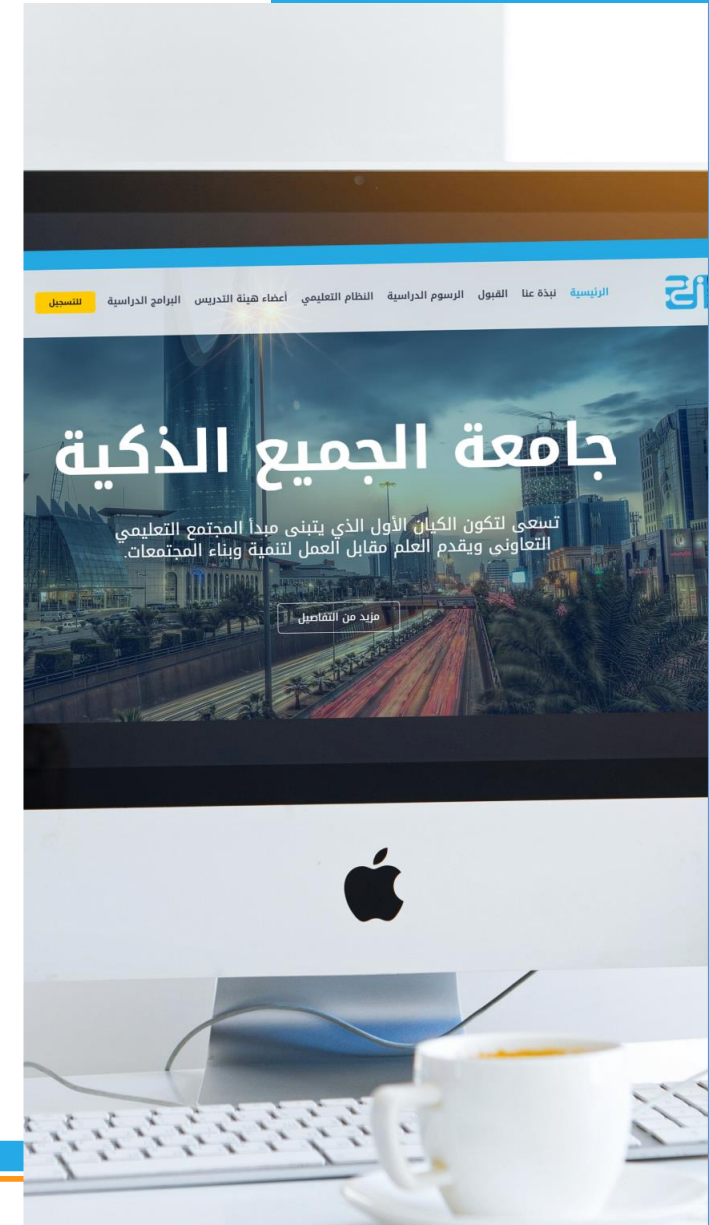


Lecture 8

Cloud Storage services

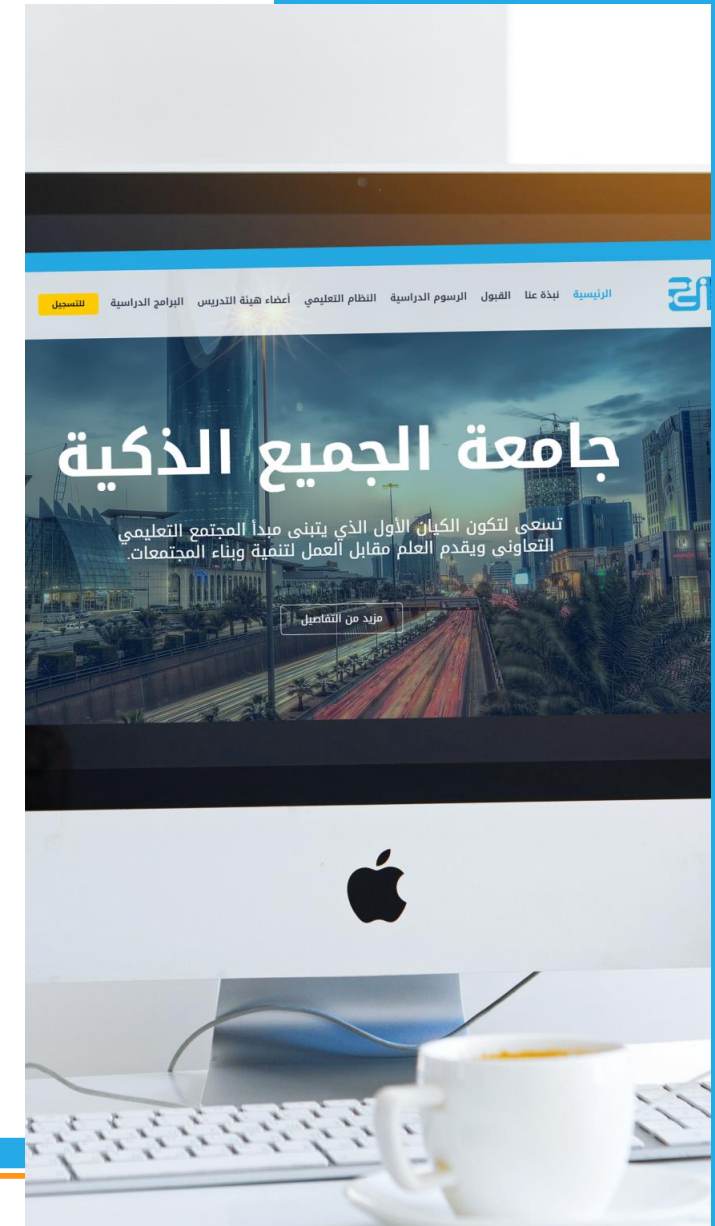
Saas

- Dropbox
- Google Drive

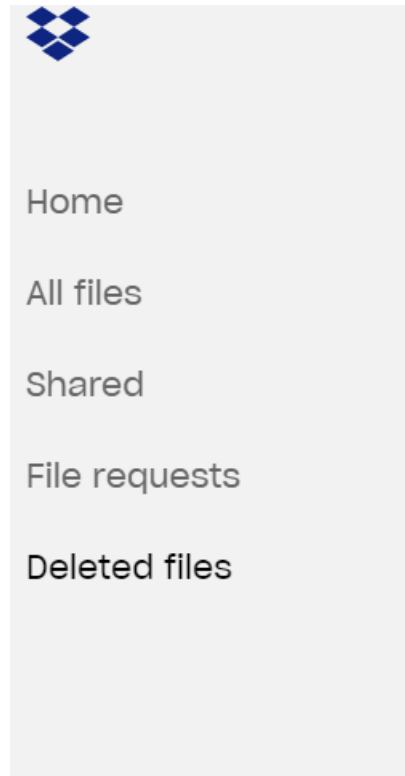


Lecture 8

Dropbox



- You can access all deleted files
- Commercial all deleted files can be recovered



Deleted files

Need help restoring deleted files? [Learn more](#)



You can get information about :

- Last browser **session**
- **Devices** linked with the dropbox

Sessions

These are the web browsers currently logged in to your Dropbox.

Browser	Location	Most recent activity
 Chrome on Windows	United States 	Current session 

Devices

You've linked these devices.

Name	Country	Most recent activity	
 Beast	United States	in the last hour 	
 DESKTOP-RSCAKAN	United States	about a day ago 	
 Cerberus	United States	about a year ago 	
 Mini-Beast	United States	about a year ago 	
 Medusa	United States	about 3 years ago 	

You can get information about :

- Apps linked with the dropbox
- Menu -> security -> setting

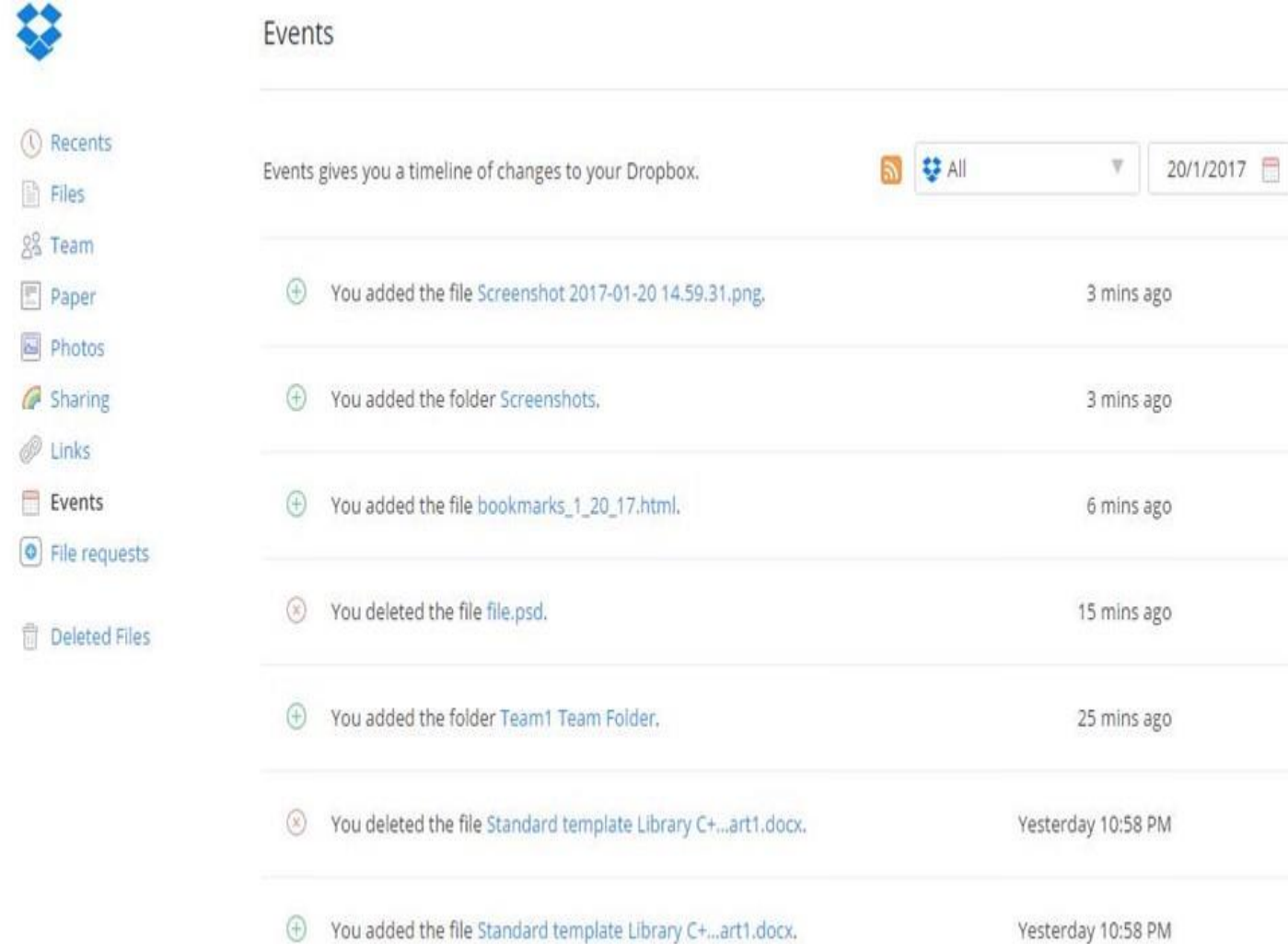
Apps linked

You've given these apps access to your personal Dropbox.

App name	Publisher	Access type	
 DataSync	Quint Stoffers	No access - App folder deleted 	
 Dropbox for Windows Store	Dropbox	Official app 	
 Titanium Backup PRO	Titanium Track	Full Dropbox 	
 Quickoffice	Quickoffice	Full Dropbox 	



- You can view **Event** section to know the timeline of changes in Dropbox

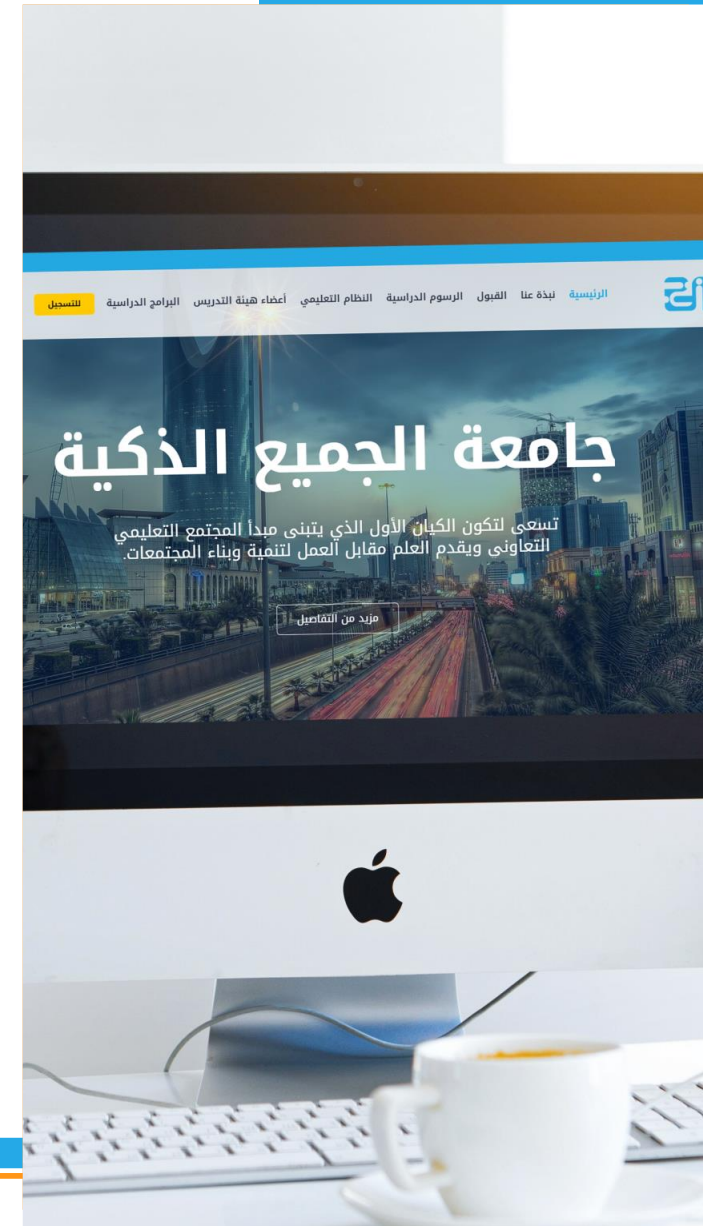


The screenshot displays the Dropbox 'Events' interface. On the left is a sidebar with navigation options: Recents, Files, Team, Paper, Photos, Sharing, Links, Events (highlighted), File requests, and Deleted Files. The main content area is titled 'Events' and includes a sub-header: 'Events gives you a timeline of changes to your Dropbox.' To the right of this header are filters for 'All' (selected) and the date '20/1/2017'. Below the header is a list of events, each with a status icon (plus for addition, minus for deletion), a description, and a timestamp.

Status	Event Description	Timestamp
+	You added the file Screenshot 2017-01-20 14.59.31.png.	3 mins ago
+	You added the folder Screenshots.	3 mins ago
+	You added the file bookmarks_1_20_17.html.	6 mins ago
-	You deleted the file file.psd.	15 mins ago
+	You added the folder Team1 Team Folder.	25 mins ago
-	You deleted the file Standard template Library C+...art1.docx.	Yesterday 10:58 PM
+	You added the file Standard template Library C+...art1.docx.	Yesterday 10:58 PM

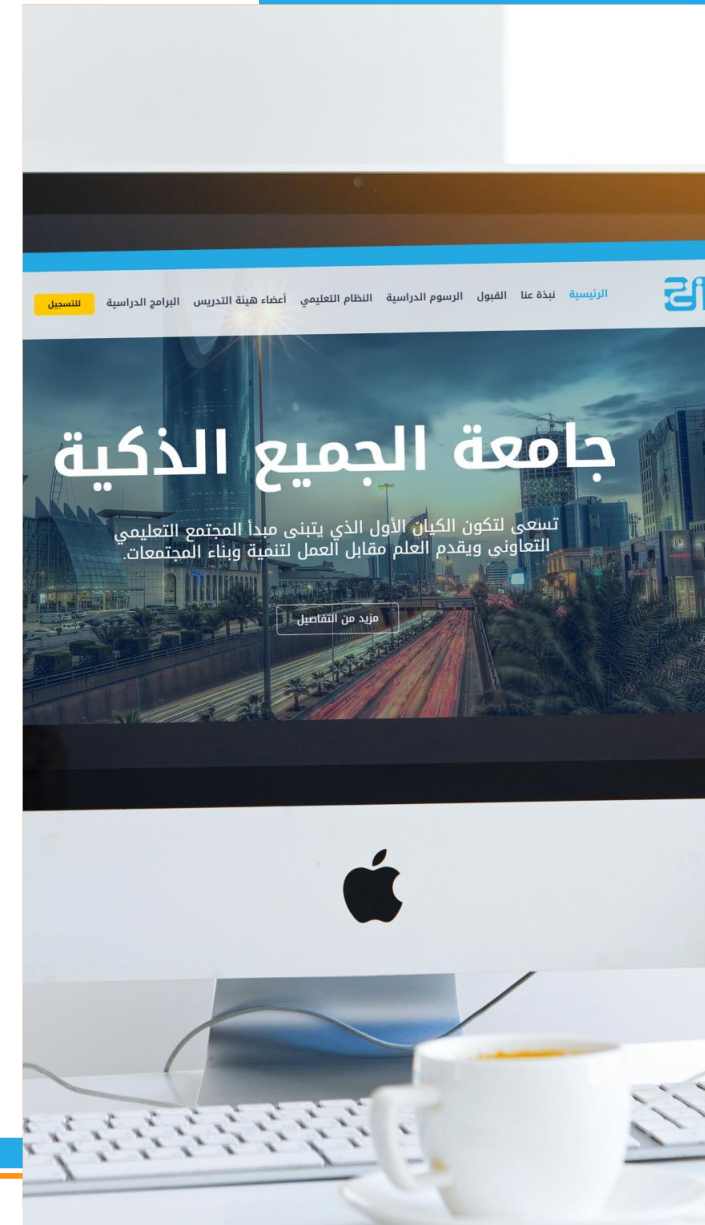
The installed directory for dropbox :

- **config.db:** contains configuration settings that the Dropbox client references in order to run in a table named config.
- **host_id:** the authentication hash used by the Dropbox client to authenticate into the Dropbox “cloud.” email: account holder’s email address.
Can be changed to any value without consequence – set at install/authentication.

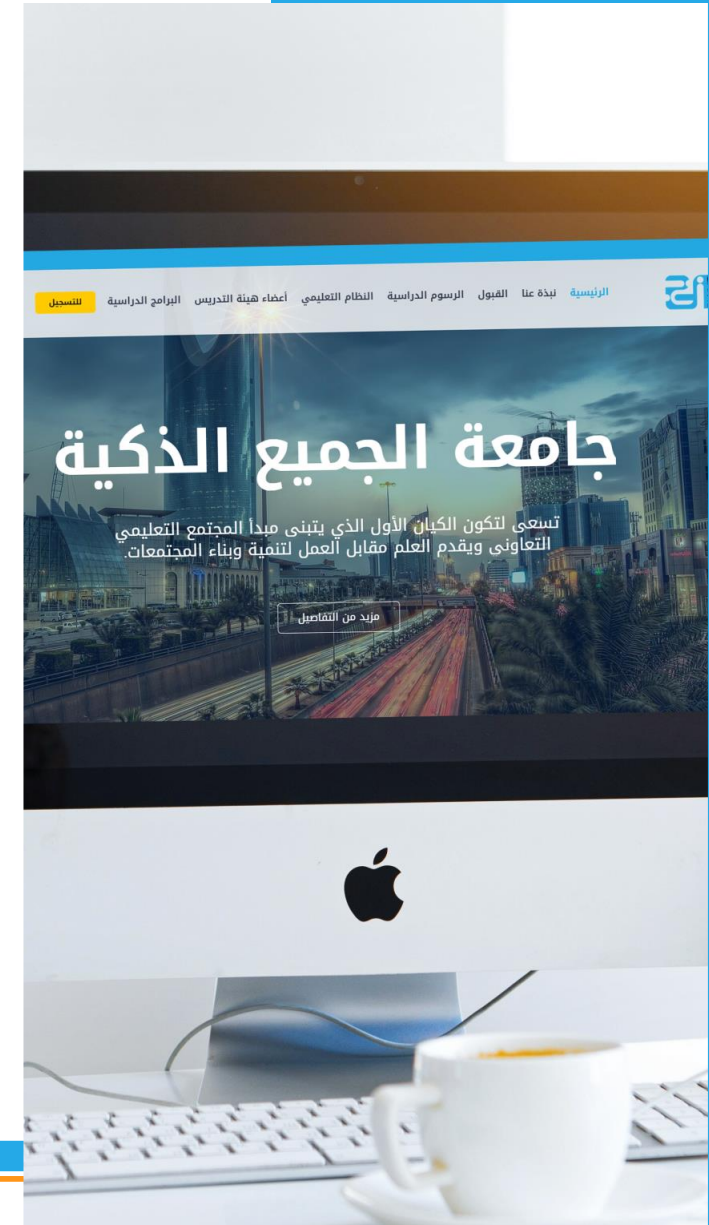


The installed directory for dropbox :

- **dropbox_path**: actual path to the user's Dropbox on the local system.
- **filecache.db**: contains a number of tables, but the primary focus is to describe all files actively in the Dropbox (deleted/removed files are removed from this table upon deletion/removal).

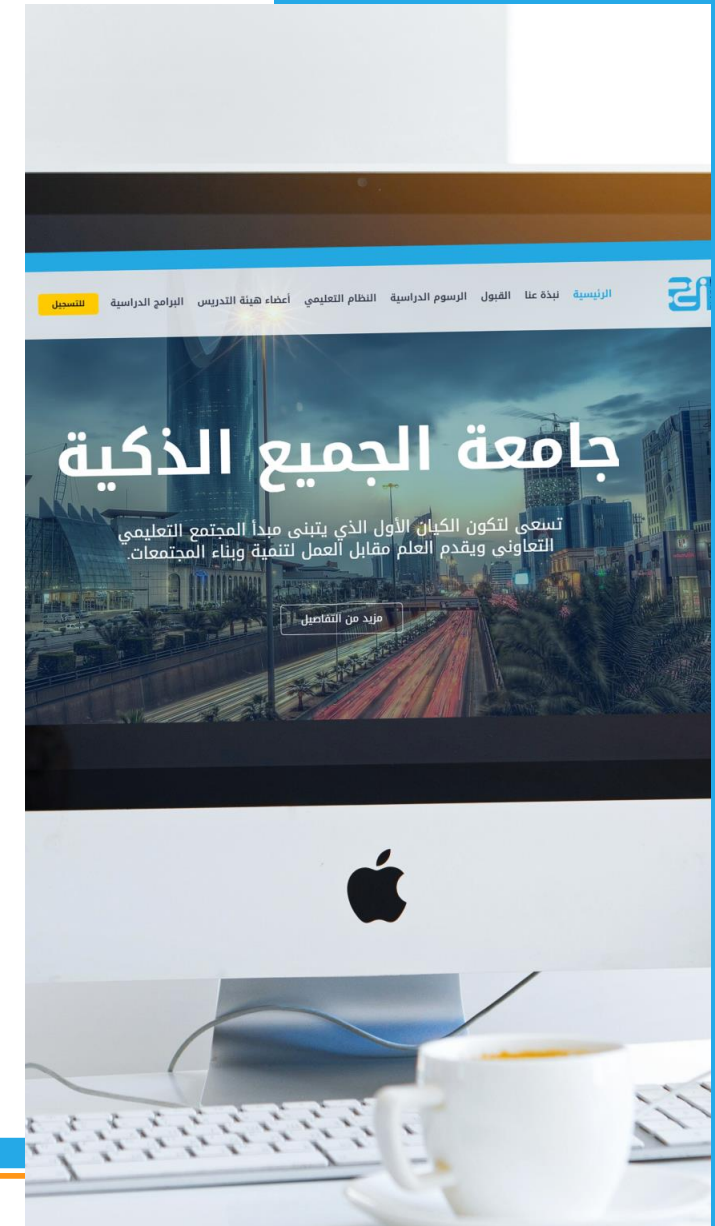


- **host.db:** contains what looks to be a hash of some sort (possibly SHA-1?) and the dropbox path (dropbox_path in config.db) encoded in base-64.
- **sigstore.db:** stores hash values which correspond to the values found in the block_cache table in filecache.db.



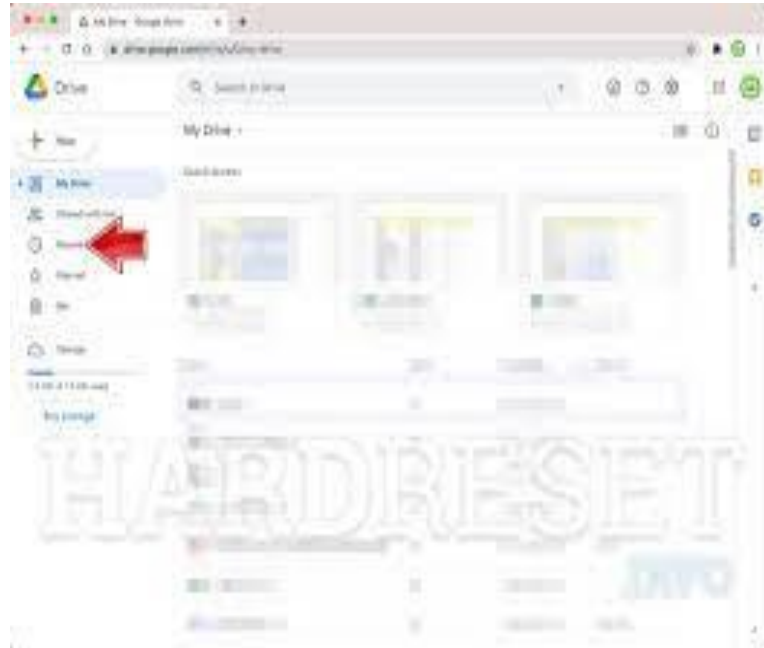
Lecture 8

Google Drive

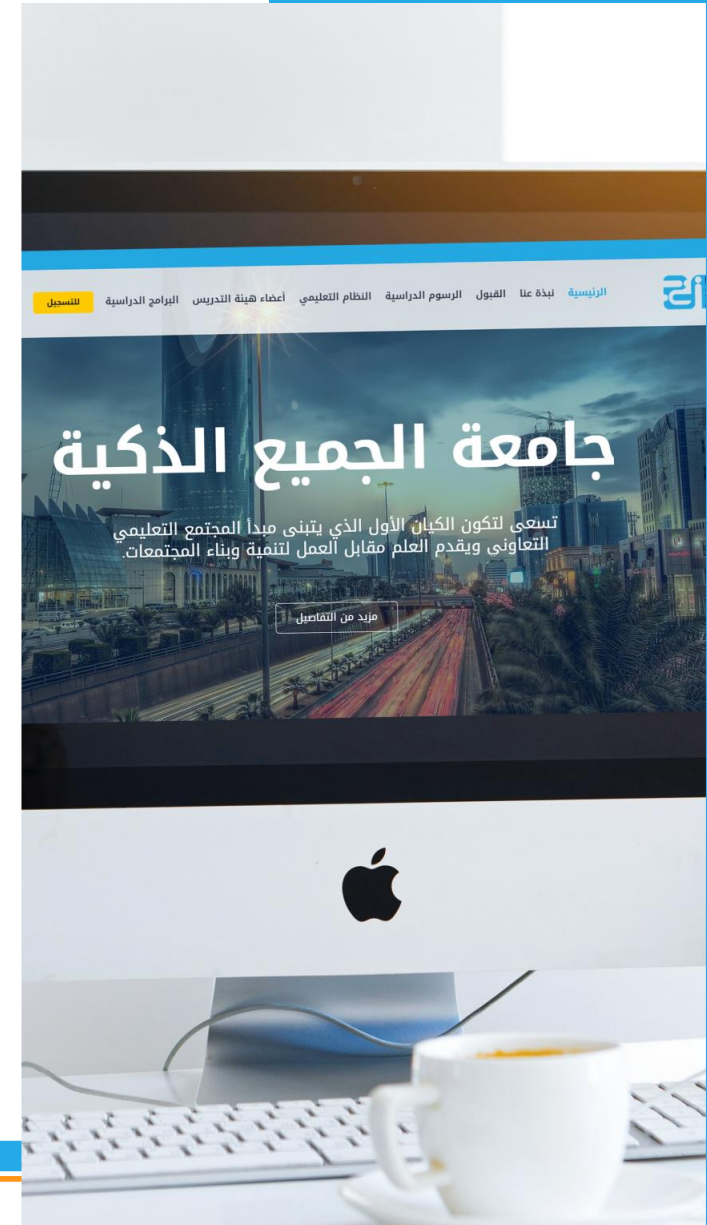


Lecture 8

Google Drive



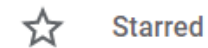
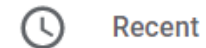
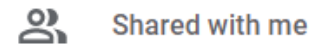
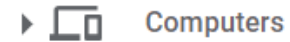
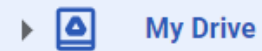
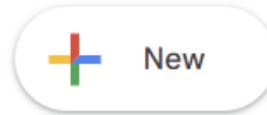
- ▶  My Drive
- ▶  Computers
-  Shared with me
-  Recent
-  Starred
-  Bin



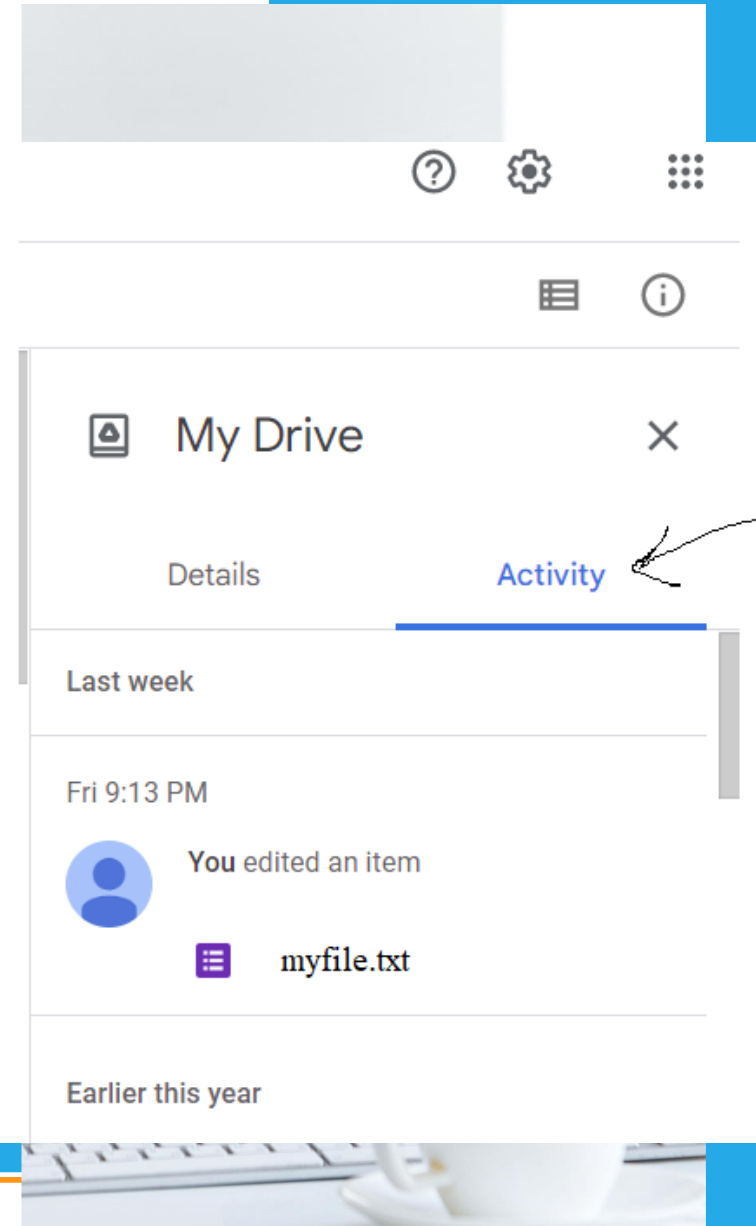
Lecture 8

Google Drive

- Activity log at Google drive



1.72 GB of 15 GB used



- Default Installation Path

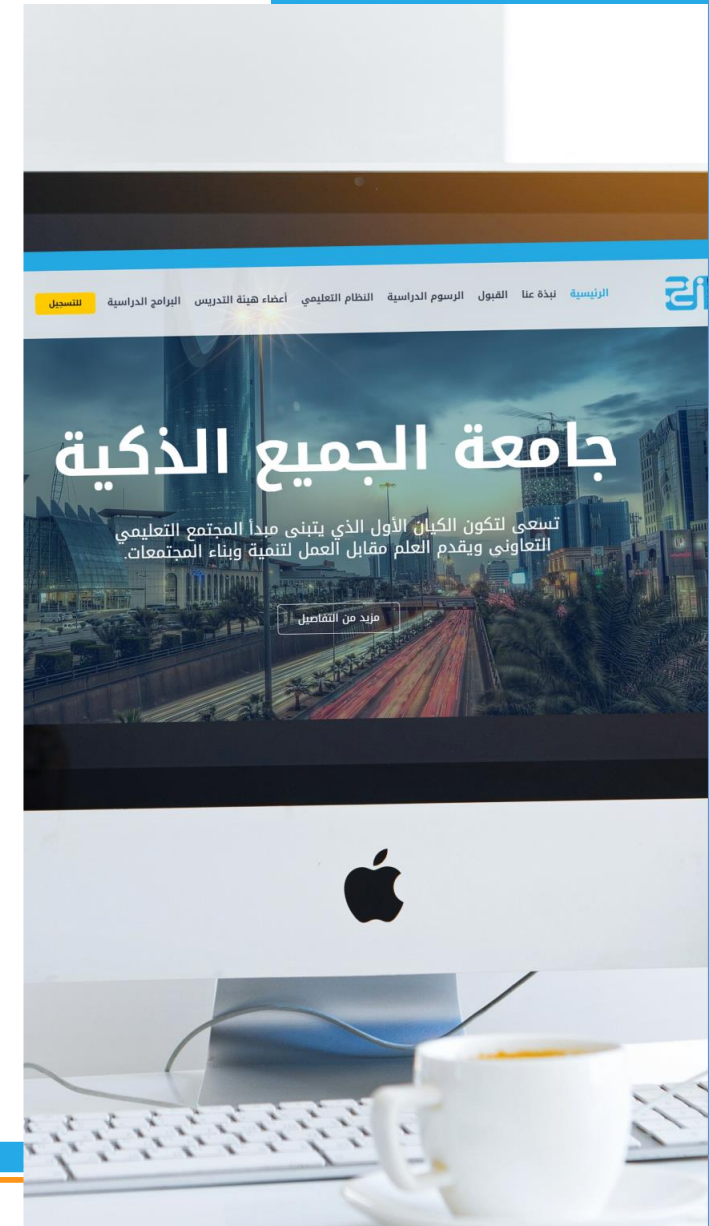
C:\Program Files\Google\Drive

- Default Sync Folder

C:\Users\<username>\Google Drive

- Default Database Path

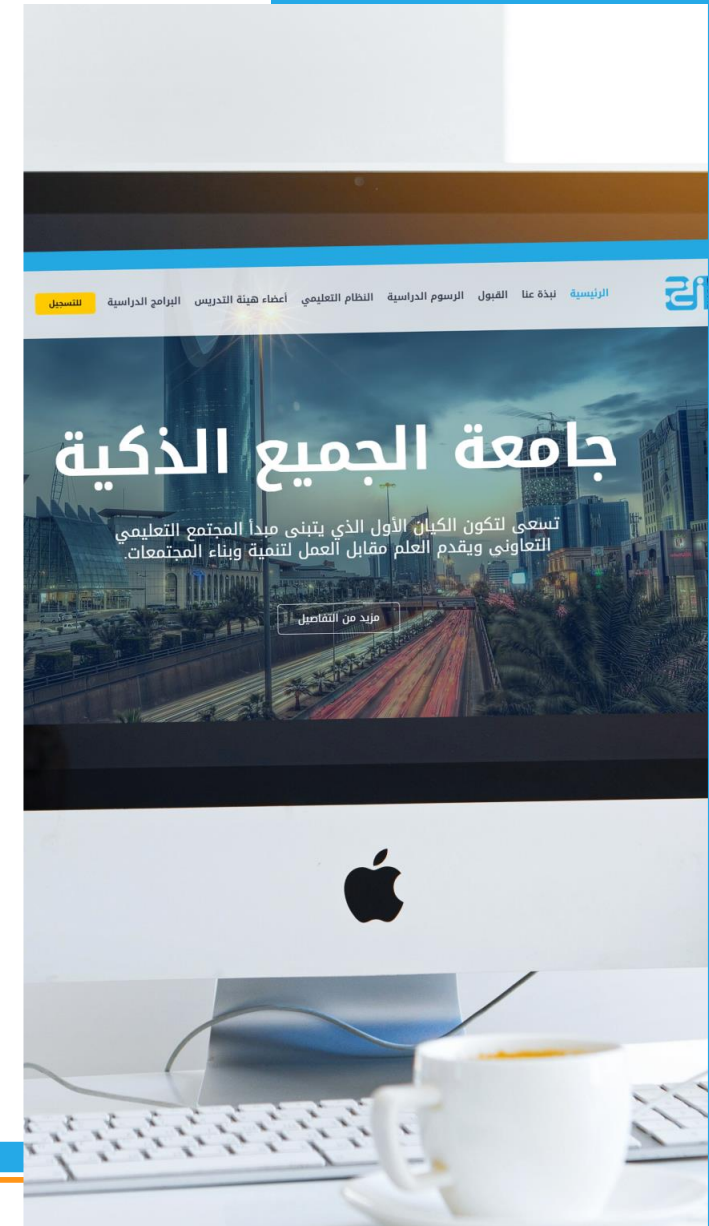
C:\Users\<username>\AppData\Local\Google\Drive



Lecture 8

Google Drive

C:\Program Files\Google\Drive	In this folder you can find the executable file of the application.
C:\Program Files (x86)\Google\Drive	In this folder, you can find information about the updates of the application.
C:\Users\<username>\GoogleDrive	This folder is being used (by default) by the app for synchronizing user's files with Google Drive cloud service. You can choose from the native app's settings, which directories you wish to be automatically synced with the cloud, but you can also drop any file to this folder and it will automatically be uploaded to the user's cloud.
C:\Users\<username>\AppData\Local\Google\Drive	In this directory you will find all the native app's files that store information about both the app and the user's data.



Lecture 8

Google Drive

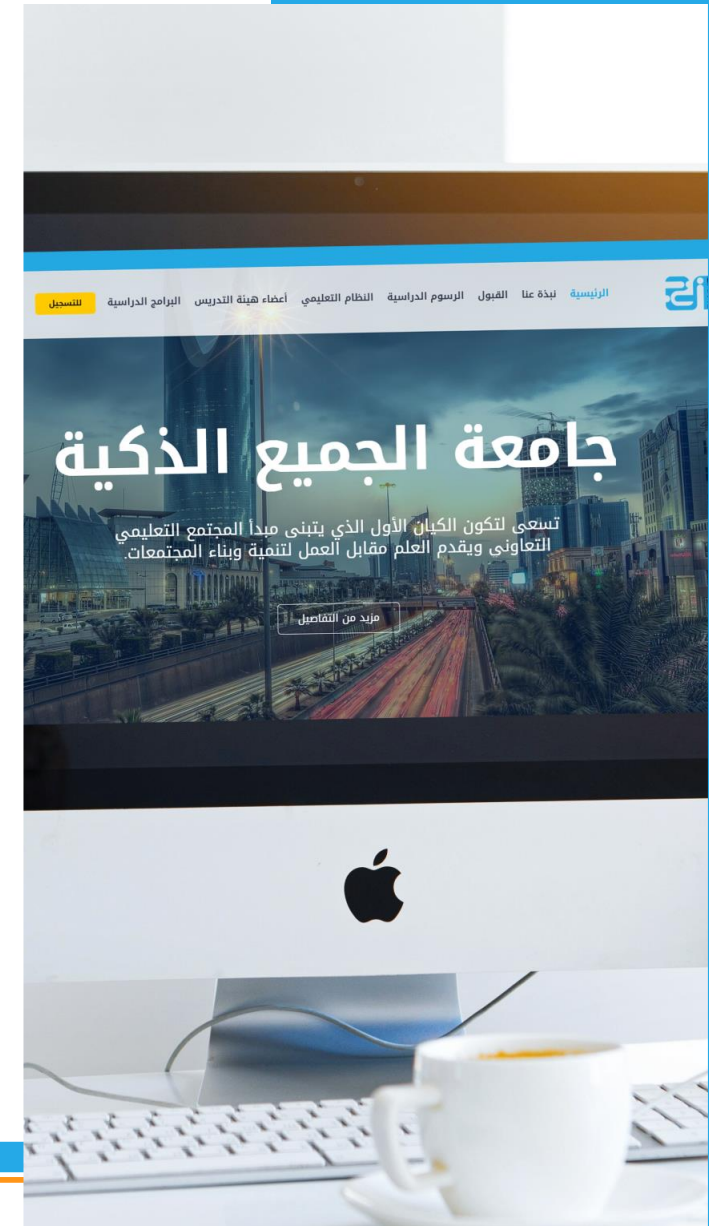
C:\Users\<username>\AppData\Local\Google\Drive\user_default\snapshot.db

This database stores information about the files that have been synced with the user's Google Drive account.

C:\Users\<username>\AppData\Local\Google\Drive\user_default\sync_config.db

This database stores information such as user's Google Drive account email.

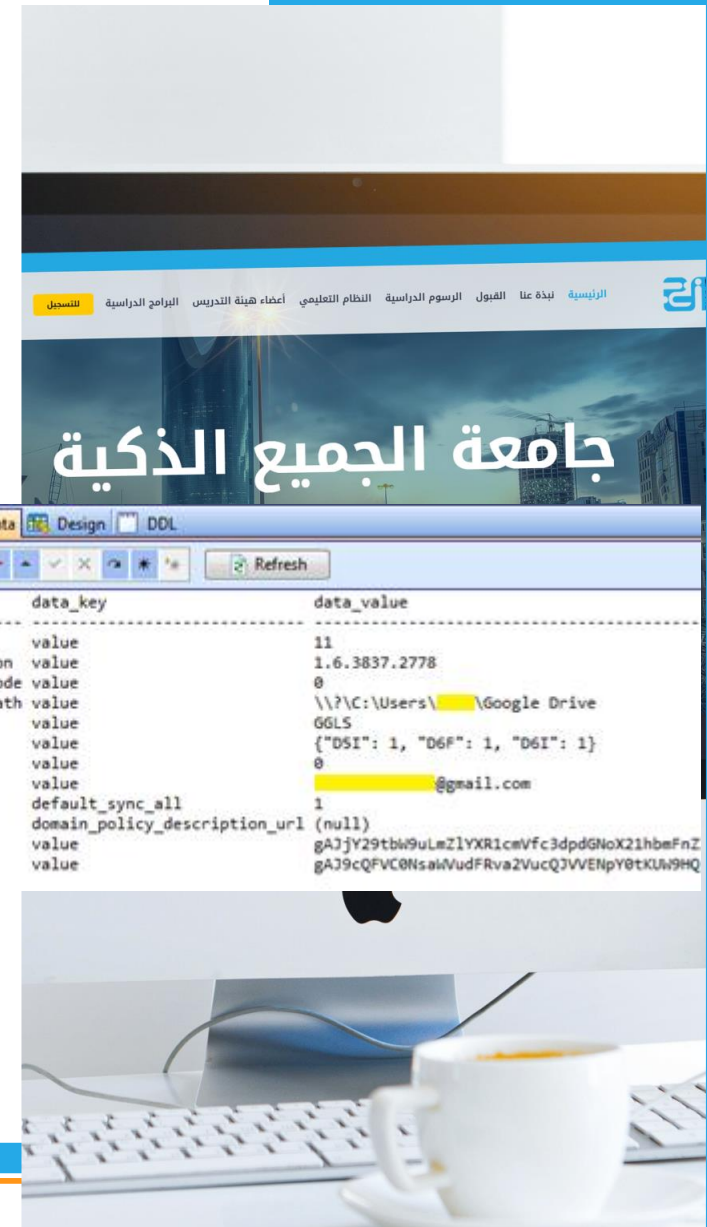
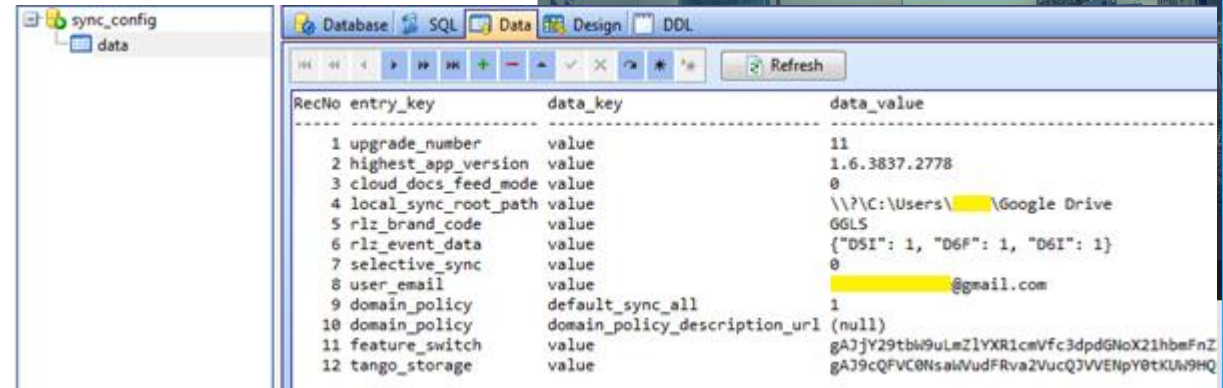
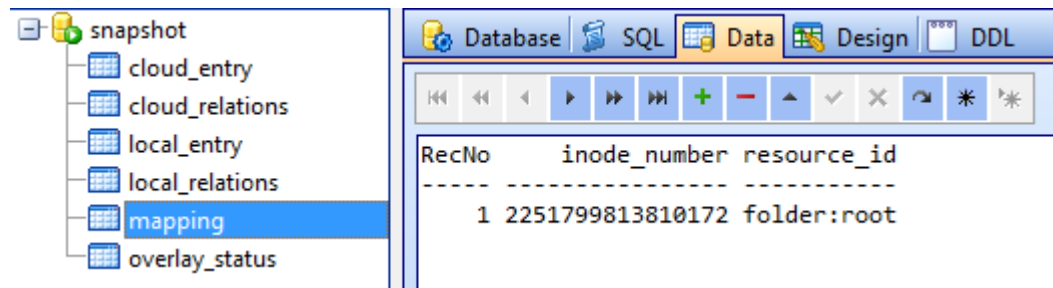
Name	Date modified	Type	Size
CrashReports	11/12/2012 3:35 PM	File folder	
cacerts	11/12/2012 3:35 PM	File	4 KB
lockfile	11/12/2012 3:35 PM	File	0 KB
pid	11/12/2012 3:35 PM	File	1 KB
snapshot.db	11/12/2012 5:38 PM	DB File	18 KB
sync_config.db	11/12/2012 6:20 PM	DB File	6 KB



Lecture 8

Google Drive

- The “snapshot.db” is a SQLite file that contains a list of files that Google Drive is aware of and is watching actions for in the synchronization folder. This log includes interesting bits of info like file hashes, names, Google IDs, and timestamps:



Lecture 8

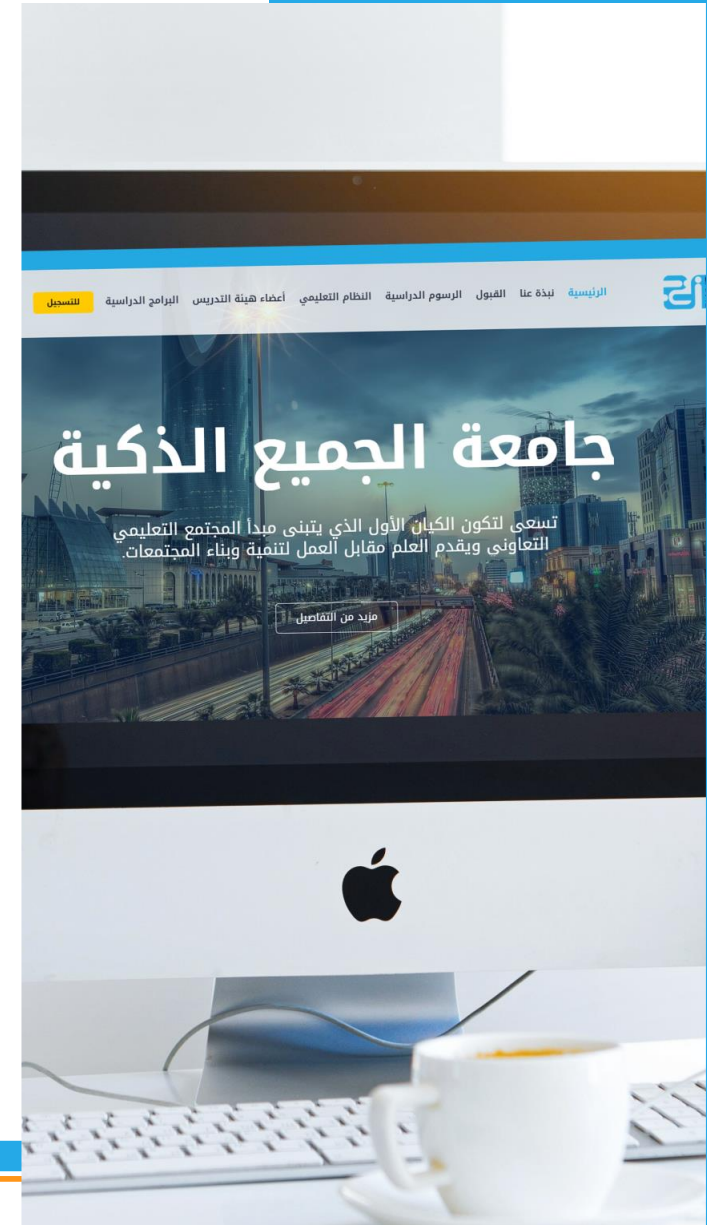
Google Drive

C:\Users\\AppData\Local\Google\Drive\global.db

This database also stores information such as user's Google Drive account email.

Table:  data 

	entry_key	data_key	
	Filter	Filter	Filter
1	storage_policy_mode	value	original
2	user_email	value	[REDACTED]@gmail.com
3	shown_setup_overlays	setup_overla...	google_drive_setup_overlay



- **DiskPulse** and **Directory Monitor** are Tools to view changes at Dropbox and Google Drive.

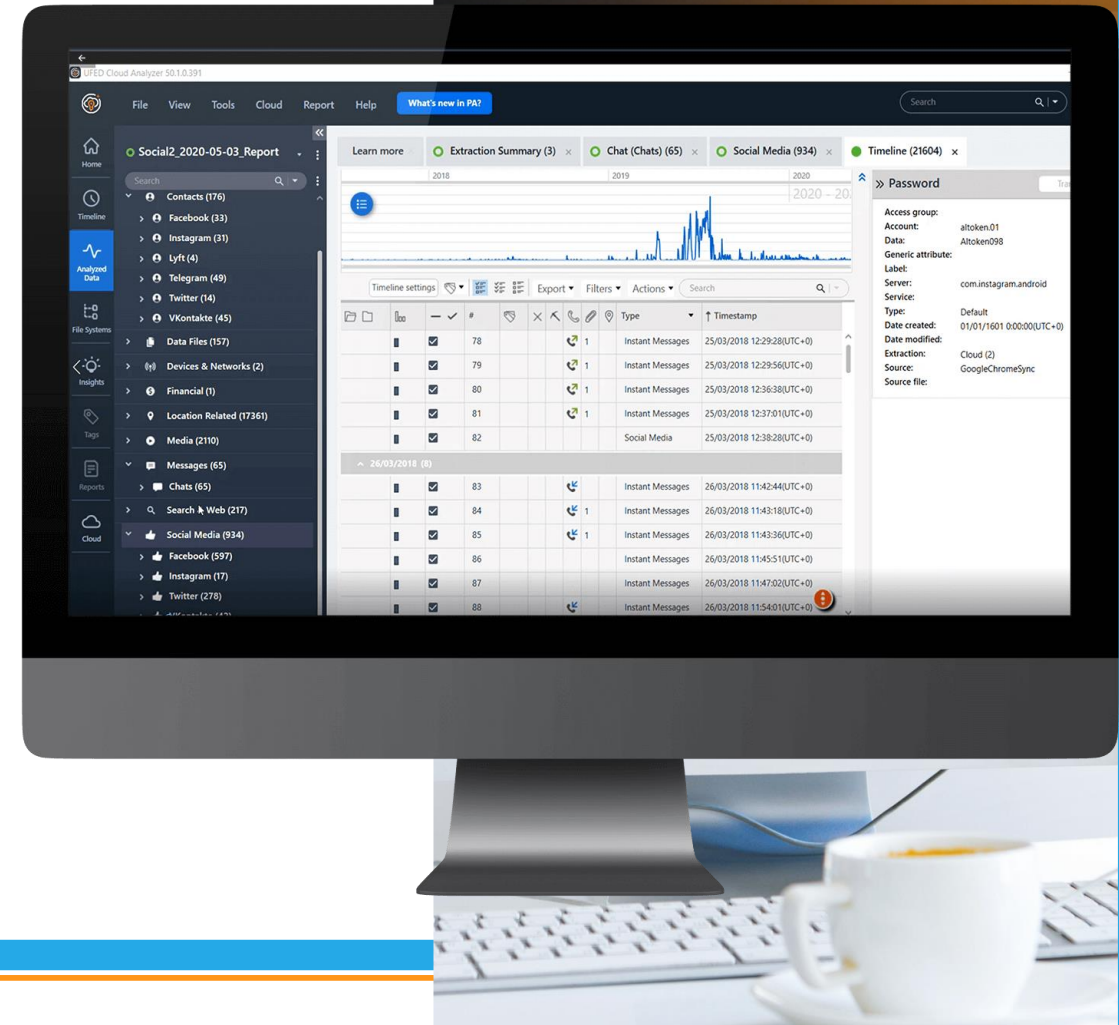
The screenshot displays the DiskPulse application window. The main pane shows a list of file operations with columns for Date, Time, Operation, Size, Owner, and Name. The operations include Deleted, Renamed, Renamed To, and Modified files, mostly in the C:\Users\wurf\AppData\Local\... directory. A summary table at the bottom left shows statistics like Total Changes (80), Changed Dirs (29), and Change Rate (47 CH/Min). A file categories table at the bottom right shows the distribution of file types, with NOEXT Files being the most common at 55.00%.

Date	Time	Operation	Size	Owner	Name
20-Aug-2021	11:30:09	Deleted	0 Bytes	---	C:\Users\wurf\AppData\Local\...
20-Aug-2021	11:30:09	Renamed	0 Bytes	---	C:\Users\wurf\AppData\Local\...
20-Aug-2021	11:30:09	Renamed To	3.04 KB	wurf	C:\Users\wurf\AppData\Local\...
20-Aug-2021	11:30:09	Modified	0 Bytes	wurf	C:\Users\wurf\AppData\Local\...
20-Aug-2021	11:30:09	Renamed	0 Bytes	---	C:\Users\wurf\AppData\Local\...
20-Aug-2021	11:30:09	Renamed To	3.04 KB	wurf	C:\Users\wurf\AppData\Local\...
20-Aug-2021	11:30:09	Modified	0 Bytes	wurf	C:\Users\wurf\AppData\Local\...
20-Aug-2021	11:30:09	Modified	3.04 KB	wurf	C:\Users\wurf\AppData\Local\...
20-Aug-2021	11:30:09	Deleted	0 Bytes	---	C:\Users\wurf\AppData\Local\...
20-Aug-2021	11:30:09	Modified	0 Bytes	wurf	C:\Users\wurf\AppData\Local\...
20-Aug-2021	11:30:16	Modified	208.62 KB	TrustedInstaller	C:\Windows\Media\Windows ...
20-Aug-2021	11:30:16	Modified	0 Bytes	TrustedInstaller	C:\Windows\Media
20-Aug-2021	11:30:29	Modified	8.52 KB	wurf	C:\Users\wurf\AppData\Local\...
20-Aug-2021	11:30:29	Modified	20.00 KB	wurf	C:\Users\wurf\AppData\Local\...
20-Aug-2021	11:30:29	Modified	0 Bytes	wurf	C:\Users\wurf\AppData\Local\...
20-Aug-2021	11:30:29	Modified	12.52 KB	wurf	C:\Users\wurf\AppData\Local\...
20-Aug-2021	11:30:29	Modified	52.00 KB	wurf	C:\Users\wurf\AppData\Local\...
20-Aug-2021	11:30:29	Modified	0 Bytes	wurf	C:\Users\wurf\AppData\Local\...
20-Aug-2021	11:30:41	Modified	120.00 KB	wurf	C:\Users\wurf\ntuser.dat.LOG1

Status	Value
Total Changes	80
Changed Dirs	29
Changed Files	51
Excluded Files	0
Monitor Actions	0
Monitor Errors	0
Change Rate	47 CH/Min
Process Time	1 Min, 42 Secs

File Categories	Count	Percentage
NOEXT Files	44	55.00 %
TMP Files	18	22.50 %
ZIP Files	6	7.50 %
LNK Files	2	2.50 %
PF Files	2	2.50 %
LOG2 Files	1	1.25 %
LOG1 Files	1	1.25 %
AUTOMATICDESTINATIONS-MS Files	1	1.25 %
SRD-SHM Files	1	1.25 %

- UFED Cloud is Lawfully Access Cloud-Based Evidence to Accelerate Investigations : Collect, preserve and analyze public and private-domain, social-media data, instant messaging, file storage, web pages, and other cloud-based content.



- Any Question

