Q1: What is normalization?

Ans: **Normalization** is a process of organizing the data in database to avoid data redundancy, insertion anomaly, update anomaly & deletion anomaly. There are two primary advantages of having a highly normalized data schema:

1. **Increased consistency**. Information is stored in one place and one place only, reducing the possibility of inconsistent data.
2. **Easier object-to-data mapping**. Highly-normalized data schemas in general are closer conceptually to object-oriented schemas because the object-oriented goals of promoting high cohesion and loose coupling between classes results in similar solutions (at least from a data point of view).

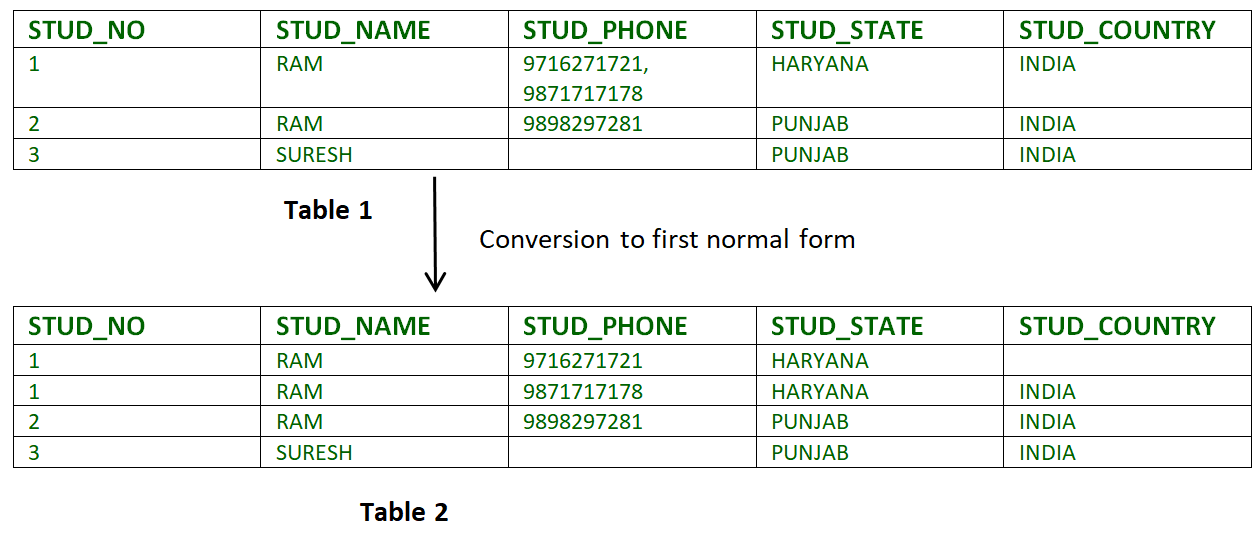
You typically want to have highly normalized operational data stores (ODSs) and data warehouses (DWs).

The primary disadvantage of normalization is slower reporting performance. You will want to have a [denormalized](http://agiledata.org/essays/dataNormalization.html" \l "Denormalization) schema to support reporting, particularly in data marts.

Q2: What is 1NF? Explain with examples.

Ans: If a relation contain composite or multi-valued attribute, it violates first normal form, or a relation is in first normal form if it does not contain any **composite** or **multi-valued attribute**. A relation is in first normal form if every attribute in that relation is singled valued attribute.

**Example-1:**  
Relation STUDENT in table 1 is not in 1NF because of multi-valued attribute STUD\_PHONE. Its decomposition into 1NF has been shown in table 2.



**Example-2:**

ID Name Courses

------------------

1 A c1, c2

2 E c3

3 M C2, c3

In the above table Course is a multi valued attribute so it is not in 1NF.

Below Table is in 1NF as there is no multi valued attribute:

ID Name Course

------------------

1 A c1

1 A c2

2 E c3

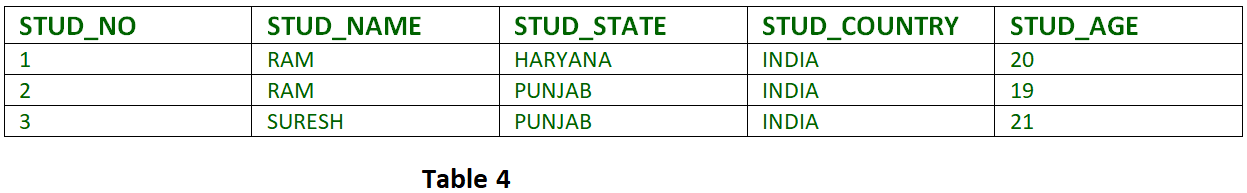
3 M c1

3 M c2

Q3: What is 3NF? Explain with examples.

Ans: A relation is in third normal form, if there is no transitive dependency for non-prime attributes as well as it is in second normal form.

A relation is in 3NF if at least one of the following condition holds in every non-trivial function dependency X –> Y:

1. X is a super key.
2. Y is a prime attribute (each element of Y is part of some candidate key).
3. In relation STUDENT given in Table 4,
4. 
5. FD set:  
   {STUD\_NO -> STUD\_NAME, STUD\_NO -> STUD\_STATE, STUD\_STATE -> STUD\_COUNTRY, STUD\_NO -> STUD\_AGE}
6. Candidate Key:  
   {STUD\_NO}
7. For this relation in table 4, STUD\_NO -> STUD\_STATE and STUD\_STATE -> STUD\_COUNTRY are true. So STUD\_COUNTRY is transitively dependent on STUD\_NO. It violates the third normal form. To convert it in third normal form, we will decompose the relation STUDENT (STUD\_NO, STUD\_NAME, STUD\_PHONE, STUD\_STATE, STUD\_COUNTRY\_STUD\_AGE) as:
8. STUDENT (STUD\_NO, STUD\_NAME, STUD\_PHONE, STUD\_STATE, STUD\_AGE)
9. STATE\_COUNTRY (STATE, COUNTRY)
10. **Example-2:**  
    Consider relation R(A, B, C, D, E)
11. A -> BC,
12. CD -> E,
13. B -> D,
14. E -> A

Q4: What is BCNF? Explain with examples.

Ans: Boyce–Codd Normal Form (BCNF) is based on [functional dependencies](https://www.geeksforgeeks.org/functional-dependency-and-attribute-closure/) that take into account all candidate keys in a relation; however, BCNF also has additional constraints compared with the general definition of 3NF.

A relation is in BCNF iff, X is superkey for every functional dependency (FD) X?Y in given relation.

**Example-1:**  
Find the highest normal form of a relation R(A, B, C, D, E) with FD set as:

{ BC->D, AC->BE, B->E }

**Explanation:**

* **Step-1:** As we can see, (AC)+ ={A, C, B, E, D} but none of its subset can determine all attribute of relation, So AC will be candidate key. A or C can’t be derived from any other attribute of the relation, so there will be only 1 candidate key {AC}.
* **Step-2:** Prime attributes are those attribute which are part of candidate key {A, C} in this example and others will be non-prime {B, D, E} in this example.
* **Step-3:** The relation R is in 1st normal form as a relational DBMS does not allow multi-valued or composite attribute.

Q5: What is Operating system? Give examples?

Ans: An operating system (OS) is a software program that serves as the [interface](https://www.webopedia.com/TERM/I/interface.html) between other applications and the hardware on a computer or mobile device. [Desktop](https://www.webopedia.com/TERM/D/desktop_computer.html) operating systems perform basic tasks, such as recognizing input from a [keyboard](https://www.webopedia.com/TERM/K/keyboard.html), sending output to a [display screen](https://www.webopedia.com/TERM/D/display_screen.html), managing [files](https://www.webopedia.com/TERM/F/file.html) and [directories](https://www.webopedia.com/TERM/D/directory.html) on a [storage](https://www.webopedia.com/TERM/D/data-storage.html) drive, and controlling [peripheral devices](https://www.webopedia.com/TERM/P/peripheral_device.html) like [printers](https://www.webopedia.com/TERM/P/printer.html). Operating systems on larger devices can also support many advanced operations, including [multitasking](https://www.webopedia.com/TERM/M/multitasking.html), [multi-user](https://www.webopedia.com/TERM/M/multi_user.html) management, [multiprocessing](https://www.webopedia.com/TERM/M/multiprocessing.html), and [multithreading](https://www.webopedia.com/TERM/M/multithreading.html).

Mobile devices, such as [tablets](https://techterms.com/definition/tablet) and [smartphones](https://techterms.com/definition/smartphone) also include operating systems that provide a GUI and can run [applications](https://techterms.com/definition/application). Common mobile OSes include Android, iOS, and Windows Phone. These OSes are developed specifically for portable devices and therefore are designed around [touchscreen](https://techterms.com/definition/touchscreen) input. While early mobile operating systems lacked many features found in desktop OSes, they now include advanced capabilities, such as the ability to run third-party apps and run multiple apps at once.

The most common operating systems are Microsoft Windows, Apple macOS, Linux, **Android** and Apple's **iOS**.

Q6: What is Linux operating system? Why it is considered as better alternative than windows?

Ans: Linux® is an [open source](https://www.redhat.com/en/topics/open-source/what-is-open-source) operating system (OS). An [operating system](https://www.redhat.com/en/technologies/linux-platforms/old-enterprise-linux) is the software that directly manages a system’s hardware and resources, like CPU, memory, and [storage](https://www.redhat.com/en/topics/data-storage/software-defined-storage). The OS sits between applications and hardware and makes the connections between all of your software and the physical resources that do the work.

[Linux](https://www.redhat.com/en/topics/linux) was designed to be similar to UNIX, but has evolved to run on a wide variety of hardware from phones to [supercomputers](https://www.redhat.com/en/blog/red-hat-enterprise-linux-builds-foundation-worlds-fastest-supercomputers). Every Linux-based OS involves the [Linux kernel](https://www.redhat.com/en/topics/linux/what-is-the-linux-kernel)—which manages hardware resources—and a set of software packages that make up the rest of the operating system.

Reasosn why it I considered better than windows:

* .It offers a **free operating system**. You do not have to shell hundreds of dollars to get the OS like Windows!
* Being open-source, anyone with programming knowledge can modify it.
* It is easy to learn Linux for beginners
* The Linux operating systems now offer **millions of programs/applications and Linux softwares to choose from**, most of them are free!
* Once you have Linux installed you no longer need an antivirus! Linux is a highly secure system. More so, there is a global development community constantly looking at ways to enhance its security. With each upgrade, the OS becomes more secure and robust
* Linux freeware is the OS of choice for Server environments due to its stability and reliability (Mega-companies like Amazon, Facebook, and Google use Linux for their Servers). A Linux based server could run non-stop without a reboot for years on end.

Q7: What is trojen horse?

Ans: A Trojan horse, or Trojan, is a type of malicious code or software that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general inflict some other harmful action on your data or network.

A Trojan acts like a bona fide application or file to trick you. It seeks to deceive you into loading and executing the malware on your device. Once installed, a Trojan can perform the action it was designed for.

A Trojan is sometimes called a Trojan virus or a Trojan horse virus, but that’s a misnomer. Viruses can execute and replicate themselves. A Trojan cannot. A user has to execute Trojans. Even so, Trojan malware and Trojan virus are often used interchangeably.

Here’s a Trojan malware example to show how it works.

You might think you’ve received an email from someone you know and click on what looks like a legitimate attachment. But you’ve been fooled. The email is from a cybercriminal, and the file you clicked on — and downloaded and opened — has gone on to install malware on your device.

When you execute the program, the malware can spread to other files and damage your computer.

Q8: What is MD5 hash and exlpain its significance using a practical example?

Ans: In cryptography, MD5 (Message-Digest algorithm 5) is a widely used cryptographic hash function with a 128-bit hash value. As an Internet standard ([RFC 1321](http://www.ietf.org/rfc/rfc1321.txt)), MD5 has been employed in a wide variety of security applications, and is also commonly used to check the integrity of files. An MD5 hash is typically expressed as a 32 digit hexadecimal number.

MD5 is a strengthened version of [MD4](http://practicalcryptography.com/hashes/Cryptographic-category/md4/). Like MD4, the MD5 hash was invented by Professor Ronald Rivest of MIT. Also, MD5 was obviously used as the model for [SHA-1](http://practicalcryptography.com/hashes/Cryptographic-category/sha-1/), since they share many common features. MD5 and SHA-1 are the two most widely used hash algorithms today, but use of MD5 will certainly decline over time, since it is now considered broken

Currently, MD5 and SHA-1 checksums are either listed on a webpage or email (see Example #1) or stored in a separate file such as (filename.ext.md5 or filename.ext.sha1) (see Example #2). There is no standard or automatic way to use them. Verifying a file after you have the hash is not complex, but it is more than the average user is used to doing (see [OpenOffice.org: Using MD5 sums](http://www.openoffice.org/dev_docs/using_md5sums.html)). MD5 checksums are 32 digit hexadecimal numbers, while SHA-1 checksums are 40, and SHA-256 checksums are 64.

Q9: What is dark web?

Ans: The dark web refers to encrypted online content that is not indexed by conventional search engines. Sometimes, the dark web is also called the [dark net](https://www.investopedia.com/insights/what-dark-net/). The dark web is a part of the [deep web](https://www.investopedia.com/terms/d/deep-web.asp), which just refers to websites that do not appear on search engines. Most deep web content consists of private files hosted on [Dropbox and its competitors](https://www.investopedia.com/articles/company-insights/090116/dropboxs-top-3-competitors-box-goog.asp) or subscriber-only databases rather than anything illegal.

Specific browsers, such as Tor Browser, are required to reach the dark web.1﻿ Using the dark web often provides considerably more privacy than just using Tor to access the web. Many dark web sites simply provide standard web services with more secrecy, which benefits political dissidents and people trying to keep medical conditions private. Unfortunately, online marketplaces for drugs, exchanges for stolen data, and other illegal activities get most of the attention.

As with the early Internet, the dark web has also gained a reputation as a haven for illegal activities. The dark web, like the web before it, is frequently blamed for horrible crimes, such as child abuse and murder for hire. However, these crimes existed long before the Internet or the dark web. The dark web makes it harder to enforce both just and unjust laws.

Q10: How can be we access dark web?

Ans: If you want to visit the dark web you need to keep in mind that this can be dangerous if you do not take the right precautions. To visit the dark web in the safest possible way we have created a guide full of tips and tricks. Below you will find a slimmed-down version of this guide, with the bare essentials. It is crucial to remember that the following steps will keep you relatively safe, but in no way completely anonymous.

* Install a VPN (we suggest [NordVPN](https://vpnoverview.com/go/nordvpn" \t "_blank)) on your device and switch it on.
* Make sure you’ve got up-to-date antivirus software on your device.
* Download and [install the anonymous Tor browser](https://vpnoverview.com/privacy/anonymous-browsing/tor/).
* Start the Tor browser.
* Make sure the running of scripts in Tor is forbidden.
* Optional: change the security settings in Tor.

Q11: What is black and white hat hackers?

### Ans: ****‘Black Hat’ Hackers****

The term “black hat” originated from Western movies, where the bad guys wore black hats and the good guys wore white hats.[1]

A black-hat hacker is an individual who attempts to gain unauthorized entry into a system or network to exploit them for malicious reasons. The black-hat hacker does not have any permission or authority to compromise their targets. They try to inflict damage by compromising security systems, altering functions of websites and networks, or shutting down systems. They often do so to steal or gain access to passwords, financial information, and other personal data.

### ‘White Hat’ Hackers

White-hat hackers, on the other hand, are deemed to be the good guys, working with organizations to strengthen the security of a system. A white hat has permission to engage the targets and to compromise them within the prescribed rules of engagement.

White-hat hackers are often referred to as ethical hackers. This individual specializes in ethical hacking tools, techniques, and methodologies to secure an organization’s information systems.

Unlike black-hat hackers, ethical hackers exploit security networks and look for backdoors when they are **legally permitted**to do so. White-hat hackers always disclose every vulnerability they find in the company’s security system so that it can be fixed before they are being exploited by malicious actors.

Some Fortune 50 companies like Facebook, Microsoft, and Google also use white-hat hackers.

Q12: Which operating systems are used for hacking and penetration testing?

* Ans: **Kali Linux**. ...
* BackBox. ...
* **Parrot Security** Operating System. ...
* DEFT **Linux**. ...
* Network Security Toolkit. ...
* BlackArch **Linux**. ...
* **Cyborg Hawk Linux**. ...
* GnackTrack.

Q13: Why windows are more prone to viruses?

Ans: Microsoft Windows undeniably powers [most of the world’s desktop computer](http://gs.statcounter.com/os-market-share/desktop/worldwide/#monthly-201707-201807-bar) and laptops today and has been the case for most of the years. This makes it the prime target for malware makers. It is therefore, the most vulnerable to viruses. With access to most people, malicious malware creators will seek to infect average PCs with mischievous agenda like stealing credit card numbers and vital financial data. As a result, Windows has a long history of succumbing to attacks from malware but the reason for this susceptibility is not only based on its popularity and wide use but also its design.

Initially, Microsoft was not keen on securing Windows when they first started out releasing the operating system. The original versions of Windows were open and never limited users from accessing personal data. Linux and Mac OS X, on the other hand, focused on limiting unauthorized access from scratch.

Although Windows 3.1, 95, and 98 seemed like advanced operating systems, they were based on the old DOS. It was a single-user design without proper user accounts. DOS did not offer security restrictions and proper file permissions to reinforce protection of data and the OS from intrusions.

There was no dire need for it anyway, so it took time before the company shifted its attention towards reinforcing security measures. The result was Windows NT, which became the base for later popular versions such as Windows 2000, XP, Vista, 7, 8, and 10. These are modern multi-user platforms that include security features to restrict unauthorized entry.

Q15: What is open source softwares?

Ans: The Open Source Initiative (OSI), a global nonprofit founded in 1998, acts as a leading authority on OSS. Its definition of open-source software includes ten criteria, relating to matters such as:

* Software redistribution
* Source code availability and integrity
* Distribution and properties of licenses
* Derived works
* Anti-discrimination

The open source software movement grew out of the related, but separate, "free software" movement. In 1983, Richard Stallman, at the time a programmer at the MIT Artificial Intelligence Laboratory, [said](https://groups.google.com/forum/#!msg/net.unix-wizards/8twfRPM79u0/1xlglzrWrU0J) he would create a free alternative to the Unix operating system, then owned by AT&T; Stallman dubbed his alternative GNU, a [recursive acronym](https://en.wikipedia.org/wiki/Recursive_acronym) for "GNU's Not Unix."

Q16: Why windows Vista was a big failure?

Ans: **1. The delay.**

**2. Unfulfilled hype.**

**3. Microsoft’s initial marketing also raised people’s expectations to bizarre heights**

**4. It depended too much on misplaced glitz**

**5. Too many features were too little, too late.**

**6. It missed too many opportunities**

**7. Initial driver and application hassles**

**8. The “Vista Capable” mess.**

**9. Too many PC manufacturers made an iffy product worse.**

**10. Vista started shaky and stayed shaky**

**11. Microsoft eventually gave up trying to market Vista.**

**12. Apple’s operating system**