Tutorial Question 1

With the help of an example, explain the fundamental difference between incremental backup and differential backup.

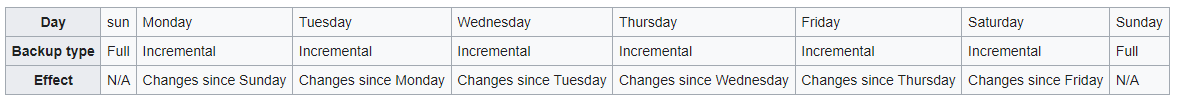
Incremental backup, backs the data up from the last time the data was backed up. Differential backup, backs data from the last time the data was fully backed up.

For example, if the data is scheduled to have a full backup on Sunday and a differential backup was made on Monday, and a following differential backup as well as an incremental backup is made on Tuesday, the differential backup will contain the changes in backup

<https://en.wikipedia.org/wiki/Differential_backup#:~:text=A%20differential%20backup%20refers%20to,since%20the%20last%20incremental%20backup>.

Difference between a differential backup and Incremental Backup

A differential backup refers to a backup made to include the differences since the **last full backup**, while an incremental backup contains only the changes since the **last incremental backup.**



The above assumes that backups are done daily. Otherwise, the “Changes since” entry must be modified to refer to the last backup (whether such last backup was full or incremental). It also assumes a weekly [rotation](https://en.wikipedia.org/wiki/Backup_rotation_scheme).  
It is important to remember the industry standard meaning of these two terms because, while the terms above are in very wide use, some writers have been known to reverse their meaning. For example, [Oracle Corporation](https://en.wikipedia.org/wiki/Oracle_Corporation) uses a backward description of differential backups in their DB product as of May 14, 2015: 

"Differential incremental backups - In a differential level 1 backup, RMAN backs up all blocks that have changed since the most recent cumulative or differential incremental backup, whether at level 1 or level 0. RMAN determines which level 1 backup occurred most recently and backs up all blocks modified after that backup. If no level 1 is available, RMAN copies all blocks changed since the level 0 backup."[[4]](https://en.wikipedia.org/wiki/Differential_backup#cite_note-4)

Tutorial Question 2

It has been suggested that an old hard drive can be securely erased by encrypting the whole drive with a sophisticated algorithm and key, and then destroy the key. Discuss whether this software approach to data erasure is sufficient.

It is sufficient, if the encryption is strong. Destroying the key is the ultimate form of sanitation. The destruction of the key will lead to no one having any means of opening the drive with the key again.

**Extra knowledge**

The best way to make sure an old-fashioned mechanical hard drive is securely erased is to overwrite it with dummy data multiple times. There's a popular freeware app called DBAN (Darik's Boot and Nuke) that writes to all the sectors using secure sanitization methods.

DBAN is its own boot environment (no OS necessary) so you can use it to securely erase the boot drive on a computer without taking that drive out and attaching it to another PC. However, if the hard drive you're wiping is not the boot drive, you must be very careful when using DBAN so that you don't accidentally wipe the wrong drive.

Tutorial Question 3

Research and find out why wiping data off an SSD drive needs more consideration than regular SATA/PATA hard drives.

PATA

PATA stands for Parallel Advanced Technology Attachment which is a bus interface used for connecting secondary storage devices like hard disks, optical drives. It was first introduced in the year 1986 by Western Digital and Compaq. It was later replaced by SATA.

PATA hard drives are made of mechanical moving parts and are based on parallel signaling technology – meaning they transmit multiple bits of data simultaneously.

SATA

SATA stands for Serial Advanced Technology Attachment is a bus interface that connects hard disks, optical drives. It was introduced in 2001 after PATA was slowly declining its demand by Serial ATA Working Group. SATA has more advantages than PATA making its demand more.

The mode of connection to a computer remains the same as PATA, but instead of parallel signaling technology for data transmission, they use serial signaling technology. This means that they transfer data one bit at a time.

SCSI

Small Computer System Interface (SCSI)

SCSI hard drives are upgrades over SATA and PATA drives for many reasons such as round-the-clock operations, speed, storage, and several others.

For connection, SCSI hard drives use a small computer system interface – which is a standard for connecting peripheral devices such as printers, scanners, and others.

Best of all, they allow the connection of peripheral devices such as printers, scanners, and other hard drives. In addition, they transmit data at 320 MB/S and you can connect them internally or externally.

Connections through SCSI on personal computers have now been replaced by the Universal Serial BUS (USB). This means that SCSI is no longer used as consumer hardware.

SSD

SSD stands for Solid State Hard Drive. The reading and writing of data are much faster because it is not a mechanical hard drive. It uses non-volatile flash memory to hold and access data. There are no moving parts available like a hard drive.

Unlike the hard drive technologies before SSD drives, they don’t consist of moving parts and they don’t use magnetism for storing data.

Instead, they use integrated circuits (ICs) just like third-generation computers. This makes them more durable, faster, and less prone to damage and corruption.

SSD hard drives have a notable advantage of transferring data at speed of 550 MB/S and allow faster boot times than the types of hard drives before them.

<https://www.makeuseof.com/tag/securely-erase-ssd-without-destroying/>

Tools like Darik’s Boot and Nuke are not always effective. They’re write intensive nature can largely reduce performance and shorten SSD drives lives. As a reminder, traditional hard drive store lives in physical locations on a magnetic matter, which is then indexed in a file system and access using a mechanical arm which is a very linear way of doing it.

**Extra knowledge**

A traditional hard drive stores files in physical locations on a magnetic platter. The operating system indexes the file locations in a file system and accesses the data using a mechanical arm. Whereas a solid-state drive is a form of flash memory, like a USB thumb drive—but with a much larger capacity.

While the SSD uses a file system to communicate data storage locations to the host system, it also re-shuffles the data to ensure even wear across all memory blocks. Changes made for wear leveling record to a separate file map.

In other words, SSDs do not use any physically indexable locations, and software cannot specifically target sectors on the disk. Basically, your computer has no way of telling "where" that information was just copied to.

How to securely erase an SSD

The difference is that instead of securely wiping all data from the drive, an SSD "resets" to a clean memory state (not factory state, which implies there is no drive wear!).

The "ATA Secure Erase" command instructs the drive to flush all stored electrons, a process that forces the drive to "forget" all stored data. The command resets all available blocks to the "erase" state (which is also the state the TRIM command uses for file deletion and block recycling purposes).

Importantly, the ATA Secure Erase command does not write anything to the SSD, unlike a traditional secure wipe tool. Instead, the command causes the SSD to apply a voltage spike to all available flash memory blocks in unison. The process resets every available block of space in a single operation, and the SSD is "clean."

Using the ATA Secure Erase command does use a whole program-erase cycle for your SSD. So yes, it does cause a small amount of wear, but it is negligible compared to a traditional secure wipe tool.

Alternatively,

1. The SSD manufacturer's management app is the first place to check for a secure erase tool. However, some manufacturers do not include the ATA Secure Erase command as an option. Furthermore, in some cases, your SSD model may not support the command. If that is the case with your SSD, move to the next section.
2. There is a third method to erase your SSD securely. The Physical Security ID (PSID) revert effectively cryptographically erases the content of your SSD, then resets it to the erase state. However, this method only works if you cannot securely erase the drive due to full disk encryption.
3. Wiping an SSD clean requires different tools than a regular hard drive. Now you know the options, you can securely erase your SSD before selling or donating it. Manufacturer secure erase options are handy, but the Parted Magic secure erase option is best.

Remember, if you're not selling or donating the drive and just want to destroy the data, you can always smash it up with a giant hammer. Of course, this will obliterate your data, as well as the drive itself. But you will securely erase your data in the process.

Tutorial Question 4

Compare the two archiving choices: tape vs disk: Discuss the pros and cons of each approach, and explain where you would consider one but not the other.

**Tape backup** is moving data from hard drive to tape cartridge for long-term archiving or data recovery in the event of computer corruption. LTO (Linear Tape-Open) is a standard for magnetic data tape. The copied data is written to tape sequentially, one file after another, and access is also sequential.

**Disk backup** (disk-based backup) refers to backing up data to hard disk storage unit for [disaster recovery](https://www.ubackup.com/enterprise-backup/disaster-recovery-levels.html) (DR) in a large enterprise.

<https://www.ubackup.com/enterprise-backup/tape-vs-disk-backup-pros-and-cons.html>

Tape pros : High capacity, lower cost, reliability of robustness, reliability and longevity

Tape cons : Slow, maintenance required and recovery is slow

Disk pros : rapid recovery, high level security and efficiency

**When to use them:**

Use tapes when archiving old data, not use short term

Use disk when want to use incremental data when quick recovery or high security recovered

Cloud long term cannot be w reliable and secured data, better w 3rd party tape vaulting services

Tutorial Question 5

Describe two (2) situations where data masking is particularly important and give three (3) reasons to explain why.

Situation:

1. Testing new software on confidential data
2. Sending Data for 4rd party analysis

Reasons:

1. Reduce risks of data breaches
2. Sends High quality data
3. Ensure data compliance and mandates regulations

Tutorial Question 6

Data involved in any data masking must remain meaningful at several levels. Explain what it means by ‘‘meaningful”.

**Meaningful : obfuscated field must be correctly validated**

eg. postcode must seem legit

Although data is masked, data has to be validated when items are purchased on e commerce websites (Shoppee, Amazon etc.)

Such websites must allow customers to do transaction such that unauthorised parties cannot read the masked data but system must be able to understand transactions between customers and merchants.

Tutorial Question 7

One important requirement of data masking is that it must prevent reverse engineering which can compromise the confidentiality of the data. Describe one example of a poor data masking practice that can be reverse engineered by a competent hacker.

The data must undergo enough changes so that it is not obvious that a masked data is not from a source of production data.

Eg. It may be common knowledge in an organisation that there are 10 snr managers all earning in an excess of $30000. If a test environment of the organisation HR system also includes 10 identities in the same earning bracket, then other information could be pieced together the reverse the engineer of a real life identity. Theoretically, if the identity is obviously masked, or obfuscated, then it will be reasonable for someone who has access to the database to assume that they could reverse engineer the identity data if they have some degree of knowledge of the identities in the production data set. **Accordingly,** data obfuscation or masking of a data set applies in such a manner to ensure that identity and sensitive data records are protected, not just the individual data elements in discrete bills and payments.

Tutorial Question 8

Explain the fundamental difference between two data masking techniques: substitution and shuffling.

Shuffling:

* a common form of data obfuscation (to hide the data),
* Similar to substitution method but it derives the substitute set from column of data that is being masked
* If used in isolation, anyone with any knowledge of the original data can and then, apply a “what if” scenario to the data set and piece back together a real identity
* Shuffling method is open to being reversed if the shuffling algorithm can be deciphered

Tutorial Question 9 (Found in lecture notes)

Explain the pros and cons of static data masking.

Advantages:

* Sensitive data is commonly removed because the data transformations are applied to the data store. If an attacker compromises a statically masked database, the sensitive data is simply not there.

Disadvantages:

* It cannot be used to protect the production database because it permanently alters the underlying data.

Tutorial Question 10

Specify at least four major security problems associated with the Cloud Infrastructure-as-a-Service.

1. Cause traffic issues
2. Network availability
3. Cloud provider accessibility
4. Security incidents
5. Damage recovery and Business Continuity

Tutorial Question 11

Explain why it is often a poor practice to follow a vendor’s approach to secure a system.

The vendor usually has a different objective from the organisation

Eg. Routers: default login pwd and emphasises a gd system connectivity rather than security so wireless connection today mostly use lowest security settings

Tutorial Question 12

SQL injection is a common type of attacks to database servers. In 2014, a university in the United States became a victim of such an SQL injection attack against one of its servers which stored personal information about students and staff. The attack exploited a vulnerability in the outdated database server software to steal personal details of about 900 students and staff. The attacker then contacted the university officials, detailing the breach and making extortion threat. As the university refused to hand over the credentials, the attacker posted the stolen information on a public website.

* Which security goal (Availability/Integrity/Confidentiality) was compromised by this SQL injection attack? Explain your reasoning.
* Suggest three (3) necessary actions that should have been taken by the affected organisation to prevent such an attack from happening and causing damage. For each action, briefly explain how it helps.

**Confidentiality -** The attack releases the stolen information from the university to a public website

\* SQL Attacks exploits the vulnerabilities of a system

Encryption at backend

1. Patch the system promptly w latest security update.

How: remove the vulnerability so that it will not be exploited

1. Perform frequent security audits or testing - Perform regular penetration testing ( to identify vul so that org will able to patch vul timely before hacker can exploit vul)
2. Harden access control when provisioning the accts used to connect to the sql database (nvr allow web application to connect to database w administrator privileges, this reduces the amount of information that could be leaked)
3. Running education training for employees. - Ensure employees, esp those managing the server, follow strong security practices to keep their credentials secure.

Tutorial Question 13 **(check qn to see how ransomware is carried out)**

Ransomware attacks are a major data security concern nowadays. In 2016, a ransomware attack known as Petya targeted at computers running certain vulnerable Windows operating systems. In this attack, the victim received an email purporting a job application. It directed the victim to a zip file containing a malicious program which appeared to the victim as a PDF document. Once the victim allowed this malicious program to be executed at the administrator privilege, the ransomware encrypted the master file table and this effectively removed all mappings to actual files on the hard disk. The ransomware then demanded payment from the victim.

* Which security goal (Availability/Integrity/Confidentiality) was compromised in this case? Explain your reasoning.
* Suggest three (3) necessary actions that should have been taken by the affected organisations to address this security threat. For each action, briefly explain how it helps.

**Integrity and Availability**

* Master file table was modified and corrupted
* Though actual data file is still on hard drive, mapping was erased and there was no way to locate or retrieve them

1. Security education and training - Staff recognise phishing emails and will not click on the emails
2. Install anti-virus or ransomware detective and preventive measures so that org can monitor and suppress the malicious attacks
3. Backup files and data frequently to external backu dev so data can be recov to latest ver
4. Do not gr admn privileg to normal non- admin users, privilege escalation will not be possible for ransomware to exploit