

Task-1

❖ Bootable pendrive without using any software.

To create a bootable pendrive, you can primarily use three methods:

1. using the built-in Windows tools like Diskpart.
2. utilizing dedicated third-party software like Rufus or Balena Etcher.
3. by manually creating partitions and copying files through the command prompt.
each offering different levels of complexity and features depending on your needs.

Key points about these methods:

- **Windows Diskpart:**

- This is a native Windows tool accessible through the command prompt, allowing you to directly manipulate disk partitions and set a bootable flag on your USB drive.

- **Third-party software (Rufus, BalenaEtcher):**

- These applications provide a user-friendly interface to create bootable USBs, often with additional features like selecting the desired operating system ISO, formatting options, and compatibility with various operating systems.

Steps (Using Rufus as an Example):

1. **Download and Install Rufus:**

- Download Rufus from its [official website](#) and run the executable file.

2. **Insert USB Drive:**

- Plug in your USB drive and launch Rufus.

3. **Select USB Drive:**

- Under "Device," select your USB drive.

4. **Choose ISO File:**

- Click on "Select" to browse and choose the operating system ISO file.

5. **Configure Settings:**

- Partition Scheme: Choose MBR or GPT based on your system's BIOS/UEFI.
- File System: Select FAT32 (for compatibility).

6. **Start the Process:**

- Click "Start" and confirm any warnings about erasing data on the USB drive.

7. Wait for Completion:

- Rufus will copy the files and make the USB bootable. Once completed, you'll see a "Ready" status.

Outcome:

Your USB is bootable with minimal effort.

• **Command Prompt manipulation:**

For advanced users, you can manually use command line commands within the command prompt to format the USB drive, create partitions, and copy necessary files to make it bootable.

Step-1

Open Command Prompt as Administrator:

Step-2

List Available Drives:

diskpart

list disk

Identify your USB drive (e.g., Disk 1) based on its size.

Step-3

Select the USB Drive:

select disk <disk_number>

Replace <disk_number> with the USB disk number.

Step-4

Clean the USB Drive:

clean

Step-5

Create a Primary Partition:

create partition primary

Step-6

Format the Partition:

format fs=fat32 quick

Step-7

Assign a Drive Letter:

assign

Step-8

Make the USB Bootable:

- Insert your bootable ISO into your system or mount it.
- Copy the contents of the ISO to the USB drive:

```
xcopy <source_path>\*.* <USB_drive_letter>\ /E /F /H
```

Replace <source_path> with the path to the ISO files and <USB_drive_letter> with the USB drive letter.

Step-9

Eject USB

Task-2

❖ How to bit locker enable & disable? How to recover bit locker if loss the recovery key.

1. Enable BitLocker

Step 1: Open the BitLocker Manager

- Press Win + S and type BitLocker, then click Manage BitLocker.

Step 2: Select the Drive to Encrypt

- Locate the drive and click Turn on BitLocker.

Step 3: Choose an Unlock Method

- **Select a method to unlock the drive during startup, such as:**
 - Password: Set a password to unlock the drive.
 - USB Drive: Use a USB drive to unlock the drive.

Step 4: Save the Recovery Key

- **Choose where to save the recovery key:**
 - Save to your Microsoft Account.
 - Save to a USB drive.
 - Save to a file (external storage recommended).
 - Print the recovery key.

Step 5: Select Encryption Options

- **Choose either:**
 - Encrypt used disk space only (faster for new PCs).
 - Encrypt the entire drive (more secure).

Step 6: Start Encryption

- Click Start Encryption and wait for the process to complete. The time will depend on the size of the drive and selected options.

2. Disable BitLocker

Step 1: Open BitLocker Manager

- Press Win + S, type BitLocker, and click Manage BitLocker.

Step 2: Locate the Encrypted Drive

- Find the drive with BitLocker enabled.

Step 3: Turn Off BitLocker

- Click Turn off BitLocker and confirm.

Step 4: Decrypt the Drive

- BitLocker will begin decrypting the drive. This process can take time depending on the drive size.

3.If you've lost the BitLocker recovery key, try the following methods to recover it:

- If you have lost the BitLocker recovery key, recovering the data without the key is generally not possible due to the following reasons:

❖ Possible Scenarios

- **Recovery Key Backup Exists:**

If you saved the recovery key to a Microsoft account, USB drive, file, or printed copy, you can recover your data.

- **Recovery Key ID:**

If you have the Recovery Key ID (displayed during recovery), provide it to your IT admin or Microsoft support for assistance.

Task-3

❖ What is SMPS?

- **SMPS stands for Switched Mode Power Supply. It is an electronic power supply device that uses a switching regulator to convert electrical power efficiently.**

❖ Find the SMPS wired voltages & all colorize.

Orange → +3.3V (for logic circuits)

Red → +5V (for logic circuits)

Yellow → +12V (for motors, fans, GPUs)

Blue → -12V (for serial ports)

Purple → +5V (power for standby state(Always On))

Black → 0V (common ground)

White → -5V

❖ How to direct check SMPS is ON or OFF?

Observe the Fan:

- If the SMPS fan is spinning, it is ON.

Check Standby Voltage:

- Use a multimeter to check the purple wire (+5VSB). If it outputs 5V, the SMPS is receiving power.

Task-4

❖ If Blue screen error than how to recover data? (Data backups of dead system)

- If you encounter a blue screen error on your computer, the best way to recover data is to access your system through an external recovery drive or a bootable USB containing recovery software

1. Access Recovery Mode:

- **Restart your computer:** Power off your computer and then restart it.
- **Access Boot Menu:** During the boot process, press the designated key (usually F12, F11, or Del) to access the boot menu.
- **Select Recovery Option:** Navigate to the recovery option on your boot menu, which may be labeled as "Advanced Startup Options" or "Recovery Mode."

2. Use Recovery Tools:

- **Choose a recovery environment:**

Select an option to boot from a recovery drive or a bootable USB if you have one created beforehand.

- **Access your hard drive:**

Once in recovery mode, navigate to your hard drive partition where your data is stored.

3. Data Recovery Software:

- **Launch Data Recovery Software:**

If you don't have a recovery drive, boot from a bootable USB containing data recovery software (like Recuva, EaseUS Data Recovery Wizard, etc.).

- **Scan your drive:**

Select the drive you want to recover data from and initiate a scan.

- **Preview and select files:**

The software will list recoverable files; preview them to ensure they are intact and select the ones you want to recover.

- **Save to a safe location:**

Choose a different drive (preferably an external hard drive) to save your recovered data.

Task-5

❖ Window file partition type and linux file partition type

Windows File Partition Types

1. **NTFS (New Technology File System):**

- Default and most widely used in Windows.
- Features: File permissions, encryption, compression, large file support (>4GB), journaling.
- Best for: Modern Windows systems.

2. **FAT32 (File Allocation Table 32):**

- Older format with wide compatibility.
- Features: Limited file size (4GB max) and partition size (32GB max in Windows tools).
- Best for: USB drives and devices requiring cross-platform compatibility.

3. **exFAT (Extended File Allocation Table):**

- Designed for flash drives and external drives.
- Features: Large file support (>4GB) without the overhead of NTFS.
- Best for: External storage devices.

4. **ReFS (Resilient File System):**

- Advanced, fault-tolerant file system.
- Features: Data integrity, resilience to corruption, large volume support.
- Best for: High-reliability storage (e.g., servers).

Linux File Partition Types

1. **ext4 (Fourth Extended Filesystem):**

- Default and most common for Linux.
- Features: Journaling, large file and volume support, backward compatibility with ext3/ext2.
- Best for: General Linux systems.

2. **ext3/ext2:**

- Older versions of ext4.
- Features: ext3 includes journaling; ext2 does not.
- Best for: Compatibility with older systems.

3. **XFS:**

- High-performance journaling file system.
- Features: Efficient handling of large files, scalability.
- Best for: Servers and high-performance systems.

4. **Btrfs (B-Tree File System):**

- Advanced file system with modern features.
- Features: Snapshots, checksums, compression, data integrity.
- Best for: Advanced storage needs, backup systems.

5. **Swap Partition:**

- Acts as virtual memory (similar to a Windows page file).
- Features: Used when RAM is full to handle overflow.
- Best for: Systems with limited RAM.

6. **VFAT (Linux-compatible FAT):**

- Compatible with FAT32/exFAT.
- Features: Useful for sharing drives with Windows systems.
- Best for: Cross-platform drives.

7. **ZFS (Zettabyte File System):**

- High-performance and robust.
- Features: Snapshots, data integrity, large storage capabilities.
- Best for: Enterprise and high-redundancy environments.

Task-6

If system disk is full than how to install/download software?

- If your system disk is full, to install or download software, you need to first free up space on your system drive by deleting unnecessary files, using the Disk Cleanup tool, or potentially moving the installation location to a different drive with more available space.

❖ how to address a full system disk before installing software?

- **Use Disk Cleanup:**
 - Access the Disk Cleanup tool through your system settings to automatically identify and delete temporary files, old system files, and other large data that is no longer needed.
- **Manually delete files:**
 - Navigate through your system drive and identify large files or folders you can delete, including old downloads, unused program files, and large media files.
- **Move files to another drive:**
 - If you have another hard drive partition with available space, move large files or folders from your system drive to that drive to free up space.
- **Uninstall unnecessary programs:**
 - Review your installed programs and uninstall any that you no longer use to reclaim disk space.
- **Change installation location:**
 - When downloading software, check the installation options and choose to install it on a different drive with more available space if possible.

Task-7: Install Ubuntu in NTFS.

- Not possible install ubuntu in NTFS.

Task-8

Create a bootable pendrive.

Task-9

Difference between MBR and GPT

What is MBR partition?

- The Master Boot Record (MBR) is a crucial component of a computer's storage device that starts the operating system (OS) when the computer is turned on.

What is GPT partition?

- GPT (GUID Partition Table) is a flexible way to partition disks, using universally unique identifiers (UUIDs). It was developed as part of the Unified Extensible Firmware Interface (UEFI) standard, which replaced the BIOS.

Characteristics	MBR	GPT
Definition	MBR (Master Boot Record) is a type of partition used to set up a hard disc.	GPT is crucial to comprehend whether to construct a new division or convert an old one.
Compatibility	MBR is the most common format and is compatible with BIOS systems.	GPT is a newer type that works with UEFI systems.
Limitation	MBR may accommodate up to four primary or three primary partitions plus one extended partition.	GPT can accommodate an infinite number of partitions.
System types	If the system is BIOS, we can use Master Board Record.	If the system is UEFI, we can use either MBR or GPT.
Complexity	MBR is less complex than GPT	GPT is also more complex than MBR and works with all operating systems.

Task-10: Difference between all file system and which file system is best for use?

1. FAT32 (File Allocation Table 32)

- **Key Features:**
 - Simple and widely supported (works on almost all operating systems).
 - Maximum file size: 4 GB.
 - Maximum partition size: 8 TB (theoretical, often limited to 2 TB in practice).
- **Best For:**
 - USB drives and small storage devices for cross-platform compatibility.
 - Situations where you need compatibility with older systems (e.g., Windows XP).
- **Limitations:**
 - No file permissions or advanced features.
 - Limited file and partition sizes.

2. exFAT (Extended File Allocation Table)

- **Key Features:**
 - Designed as an improvement over FAT32.
 - Supports larger file sizes (up to 16 exabytes).
 - Compatible with Windows, macOS, and some Linux distributions (with additional drivers).
- **Best For:**
 - External drives and flash storage where large files need to be transferred between different operating systems.
- **Limitations:**
 - Lacks journaling, which can make it less reliable in the event of crashes or power loss.

3. NTFS (New Technology File System)

- **Key Features:**
 - Default file system for Windows.
 - Supports large files and partitions (up to 16 EB).
 - Advanced features: journaling, file compression, encryption, and permissions.
- **Best For:**
 - Windows system drives and internal storage.
 - Drives requiring advanced features like security and file permissions.
- **Limitations:**
 - Limited compatibility with non-Windows systems (macOS supports read-only; Linux requires NTFS-3G for full access).

4. ext4 (Fourth Extended File System)

- **Key Features:**
 - Default file system for most Linux distributions.
 - Supports large files and partitions (up to 1 EB).
 - Journaling for reliability and fast file access.
- **Best For:**
 - Linux systems for both root and data partitions.
- **Limitations:**
 - Limited cross-platform compatibility (requires drivers on Windows/macOS).
 - Lacks certain modern features like snapshots.

5. Btrfs (B-Tree File System)

- **Key Features:**
 - Advanced Linux file system with features like snapshots, checksums, and built-in RAID support.
 - Designed for scalability and fault tolerance.
- **Best For:**
 - Linux systems needing advanced data management and redundancy.
 - Applications requiring snapshots and backups (e.g., servers).
- **Limitations:**
 - Still considered experimental for some use cases.
 - May not perform as well as ext4 in certain scenarios.

6. XFS

- **Key Features:**
 - High-performance journaling file system for Linux.
 - Optimized for parallel I/O operations and large files.
- **Best For:**
 - High-performance applications and large-scale storage systems.
 - Data centers and enterprise environments.
- **Limitations:**
 - Does not support file system shrinking.
 - Fewer features compared to Btrfs or ZFS.

7. ZFS (Zettabyte File System)

- **Key Features:**
 - Advanced file system with built-in volume management.
 - Features like snapshots, data compression, and self-healing.
 - Scalable and reliable for massive storage systems.
- **Best For:**

- Enterprise environments requiring high reliability and data protection.
- NAS (Network Attached Storage) systems.
- **Limitations:**
- High memory requirements.
- Licensing issues can limit its adoption in some Linux distributions.

8. HFS+ (Hierarchical File System Plus)

- **Key Features:**
- Older macOS file system.
- Journaling for reliability.
- Compatible with macOS and limited support on Windows/Linux.
- **Best For:**
- Legacy macOS systems.
- **Limitations:**
- Outdated; replaced by APFS in modern macOS versions.

9. APFS (Apple File System)

- **Key Features:**
- Default file system for macOS, iOS, and other Apple devices.
- Optimized for SSDs with features like snapshots, cloning, and encryption.
- **Best For:**
- Apple devices with macOS or iOS.
- **Limitations:**
- Limited support on non-Apple platforms.
- Designed primarily for SSDs, less optimized for HDDs.

Which File System Is Best?

- **Windows Users:** NTFS for internal drives; exFAT for external drives.
- **macOS Users:** APFS for SSDs and modern storage; exFAT for external drives shared with Windows.
- **Linux Users:** ext4 for general use; Btrfs or ZFS for advanced features.
- **Cross-Platform Needs:** exFAT for maximum compatibility.
- **High-Performance Applications:** XFS or ZFS for enterprise and server environments.

Task-11: Create a Multiboot pendrive.

❖ **Five methods to create multiboot pendrive.**

Method 1: Make a Multi-Bootable USB Using Ventoy

- Ventoy is a lightweight and open-source tool that helps you to create a multi-bootable USB. It allows you to boot from ISO files directly, with no extractions needed. Besides, it can support various files, including GNU/Linux, BSD, and even Windows ISO files.

Task-12: what connector is use to connect SSD or hardisk to connect in CPU?

1.SATA (Serial ATA) Connector

Most traditional hard drives (HDDs) and some SSDs.

2.M.2 Connector

Used for: Modern SSDs, especially NVMe SSDs

3.PCIe (Peripheral Component Interconnect Express)

Used for: High-performance SSDs, especially for NVMe drives.

4.SCSI (Small Computer System Interface) / SAS (Serial Attached SCSI)

Used