Computer Forensics

Week 4: Working with Windows and CLI Systems

Kumi University

Lecturer: Lemi Agrey Oliver

codingissweet@gmail.com

Content

- Understanding File Systems
- Exploring Microsoft File Structures
- Examining NTFS Disks
- Understanding Whole Disk Encryption
- Creating a Virtual Machine

Understanding File Systems in windows

- For one to be effective in digital investigation, having a good knowledge of the common operating systems and their specific file systems is important
- A file system is a method used by computers and operating systems to organize and store files on storage devices such as hard drives, SSD or flask drives
- It provides a structured way of to access, manage and manipulate files and directories.
- The file system of an operating system determines how data is stored in the computer

Understanding File Systems in windows+

- Examples of file systems include NTFS & FAT (used by Windows), HFS+ (used by macOS), and ext4 (used by many Linux distributions).
- Familiarity with the operating system and the file system helps an investigator to easily access and modify system settings in the source computer if necessary.

File structure

- Files can be understood and recovered by understanding their common structure, which typically includes a header containing metadata, followed by the actual data, and ending with a trailer.
- The metadata often includes a file signature that identifies the file type (e.g., JPEG, PDF), allowing for file recovery even if the file is deleted from the Master File Table (MFT).
- File signatures, such as "FF D8 FF E0" for JPEG files or "25 50 44 46 2D" for PDF files, can be used to search for deleted files on a hard drive.
- Some files, like Microsoft Office files, are stored as compound files, which maintain their own structured storage approach. These files must be unpacked to be fully analyzed because their data is represented differently in their compressed state.

Understanding the Boot Sequence

- The boot sequence is the process that a computer follows to start up and load the operating system into memory.
- Before discussing the steps that are involved in the boot process it important to note that in order to avoid altering or contaminating data on the suspect's computer, the investigator must know how to access and modify Complementary Metal Oxide Semiconductor (CMOS), BIOS, Extensible Firmware Interface (EFI), and Unified Extensible Firmware Interface (UEFI) settings
- The CMOS is the medium of storage for system configuration settings plus date and time settings.
- The BIOS or EFI contains program that performs input and output operations at the hardware level

Understanding the Boot Sequence +

- To access the CMOS screen each manufacturer allows use of specific key/keys which includes Ctrl+Alt+Insert, Ctrl+A, Ctrl+S, or Ctrl+F1, F2, or F10 etc
- A secure approach to confirm the BIOS settings is by removing all hard drives from the computer. This allows you to start the computer and check its BIOS date and time without accessing the disk drive.[1]
- Change the boot sequence if necessary to allow booting from CD, DVD or flask drive

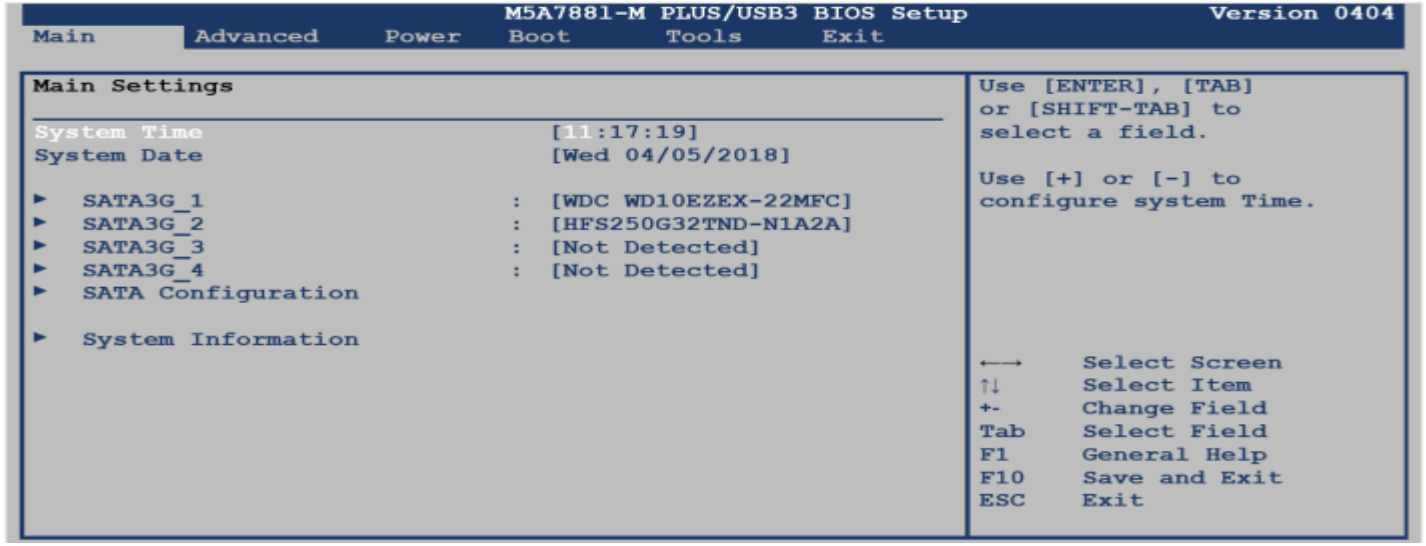


Figure 1: CMOS Screen[1]

Understanding the Boot Sequence +

- BIOS is designed for x86 computers and typically used on disk drives with Master Boot Records (MBRs)
- EFI is designed for x64 computers and uses GUID Partition Table (GPT)–formatted disks.
- BIOS and EFI are tailored for particular firmware. To lessen the dependence on firmware, Intel created UEFI, which establishes the interface connecting a computer's firmware and the operating system.
- To avoid overriding and changing evidentiary data, the suspect’s computer must be configured to boot from a forensically configured CD, DVD or flask drive.

Generic boot process steps

- Power-On Self-Test (POST),when the computer is powered on, the BIOS (Basic Input/Output System) or UEFI (Unified Extensible Firmware Interface) firmware runs a series of tests called POST. These tests check the hardware components, such as the processor, memory, and storage devices, to ensure they are functioning properly.
- BIOS/UEFI Initialization, after the POST is completed successfully, the BIOS or UEFI initializes the hardware components and loads the boot loader.

Generic boot process steps+

- **Boot Loader**, the boot loader is a small program stored in the Master Boot Record (MBR) or EFI System Partition (ESP) of the storage device.
- It is responsible for loading the operating system into memory. Common boot loaders include GRUB (Grand Unified Bootloader) for Linux systems and NTLDR (NT Loader) or BOOTMGR for Windows systems.
- **Loading the Operating System Kernel**, the boot loader loads the operating system kernel into memory. The kernel is the core of the operating system that manages the computer's resources and provides essential services.

Generic boot process steps++

- Once the kernel is loaded, the operating system initializes and starts running. During this process, the operating system configures the hardware, loads device drivers, and prepares the system for user interaction.
- After the operating system is initialized, it starts essential system services and applications, such as the graphical user interface (GUI) or network services.
- Finally, the user is presented with a login screen where they can log in to the system and start using the computer.

Components of a Disk Drive

- A drive, such as a hard disk drive (HDD) or a solid-state drive (SSD), consists of several key components that work together to store and retrieve data.

Components of the disk drive

- **Platters**, in HDDs, platters are the circular disks coated with a magnetic material where data is stored. Each platter has two surfaces (top and bottom) where data is written using a read/write head.

- **Read/Write Head,** the read/write head is a tiny electromagnetic component that reads data from and writes data to the platters. It floats just above the surface of the spinning platters and moves rapidly to access different parts of the disk.

Components of a Disk Drive+

- **Actuator Arm**, the actuator arm is a mechanical arm that holds the read/write head. It moves the read/write head across the surface of the platters to access different tracks and sectors for reading and writing data.

- **Spindle**, the spindle is the motor that spins the platters at a constant speed (measured in revolutions per minute, or RPM). The spindle speed affects the performance of the drive, with higher speeds generally resulting in faster data access.

Components of a Disk Drive++

- **Controller**, the controller is the circuitry that manages the operation of the drive. It controls the movement of the actuator arm, the speed of the spindle, and the reading and writing of data. It also interfaces with the computer's operating system to transfer data to and from the drive.

- **Cache**, the cache is a small amount of high-speed memory located on the drive. It is used to temporarily store data that is frequently accessed, which can help improve overall performance by reducing the need to access the slower main storage area of the drive.

- **Interface**, the interface is the connection between the drive and the computer's motherboard. Common interfaces include SATA (Serial ATA) for HDDs and SSDs, and NVMe (Non-Volatile Memory Express) for high-speed SSDs.

Components of a Disk Drive+++

- *Geometry*—Geometry refers to a disk's logical structure of platters, tracks, and sectors.
- *Tracks*—**T**racks are concentric circles on a disk platter where data is located.
- *Cylinders*—A cylinder is a column of tracks on two or more disk platters. Typically, each platter has two surfaces: top and bottom.
- *Sectors*—A sector is a section on a track, usually made up of 512 bytes.
- Other disk properties, such as **zone bit recording (ZBR)**, **track density**, **areal density**, and **head and cylinder skew**, are handled at the drive's hardware or firmware level.

Components of a Disk Drive++++

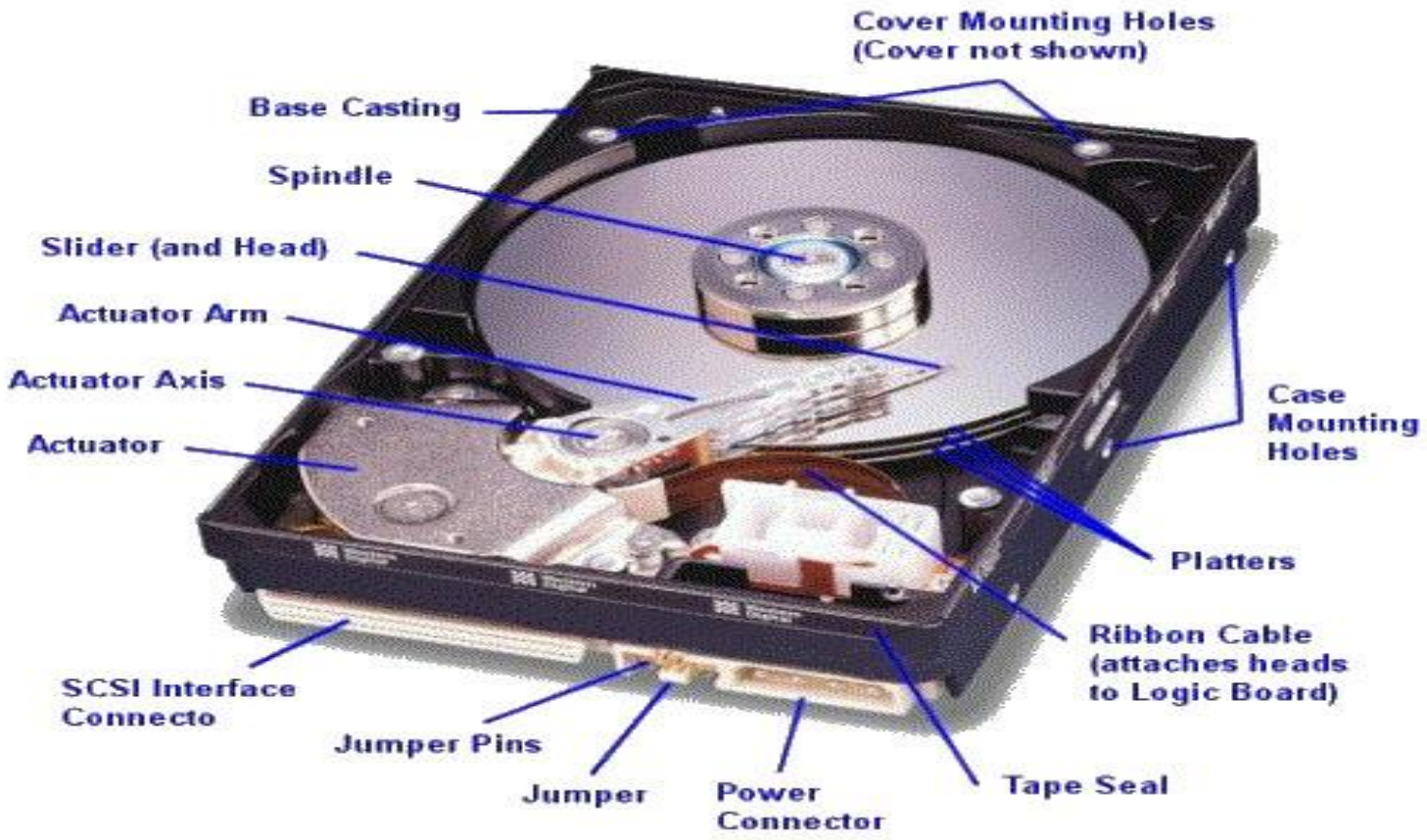


Figure 2: Components of a Disk Drive[2]

Solid-State Storage Devices

- Solid-state storage devices, such as solid-state drives (SSDs) and flash drives, use non-volatile memory to store data. Unlike traditional hard disk drives (HDDs), which use spinning disks and mechanical parts, solid-state storage devices have no moving parts, which makes them faster, more durable, and more energy-efficient
- Flash memory storage devices used in USB drives, laptops, tablets, and cell phones can be a challenge for digital forensics examiners because if deleted data isn't recovered immediately, it might be lost forever because of wear leveling. [1]
- Deleted data from Hard Disk drive can be restored easily using forensic tools because during deletion only the address is removed and the data is moved to unallocated space.

Solid-State Storage Devices

- In Solid State drives, wear-leveling redistributes data across memory cells to ensure even wear, making deleted data recovery difficult.
- Deleted data is overwritten and becomes unrecoverable after a certain number of reads/writes.
- Forensic examiners must create a full forensic copy of the device immediately after data deletion to increase recovery chances.
- Mobile device forensics benefit from understanding and managing wear-leveling, especially in criminal investigations.
- Legal limitations on data acquisition timing may apply, requiring guidance from local prosecutor's offices.

Exploring Microsoft File Structures

- Having a grasp of Microsoft file systems is crucial for forensic investigators working with Windows and DOS systems to understand how files are stored.
- Knowledge of clusters, File Allocation Table (FAT), and NT File System (NTFS) is particularly important.
- The storage method employed by an operating system determines potential data hiding spots, which forensic investigators must explore to uncover possible evidence of illegal activities or policy violations.
- In Microsoft file architectures, sectors are combined into clusters, which serve as storage allocation units ranging from 512 bytes to 32,000 bytes each.

Exploring Microsoft File Structures+

- Clusters are numbered sequentially, starting at 0 in NTFS and 2 in FAT, and are specific to a logical disk drive, representing a disk partition.
- Logical addresses, assigned by the OS, point to clusters, while physical addresses refer to sector numbers on the disk.

Disk Partitions

- Hard disks are often divided into multiple partitions, each functioning as a logical drive.
- Windows operating systems can have up to three primary partitions, followed by an extended partition that can contain multiple logical drives.
- To hide data on a hard disk, one can create hidden partitions or voids, which are large unused gaps between partitions.
- These gaps, known as partition gaps, can be created between primary or logical partitions containing unused space.
- Data can be hidden in the partition gap by creating a partition, adding data to it, and then removing references to the partition.

Disk Partitions+

- Using a disk editor utility, such as WinHex or Hex Workshop, one can access hidden or empty areas of the disk where data may be stored.
- Another technique involves declaring a smaller number of bytes than the actual drive size to hide incriminating digital evidence at the end of a disk.
- Disk editors allow examination of a partition's physical level, including viewing file headers and other critical file system structures.
- To learn more above how to identify unknown OS visit **http://x-ways.net** and learn how to use the X-Ways to identify an OS

Partition table

Hexadecimal code	File system
01	DOS 12-bit FAT (floppy disks)
04	DOS 16-bit FAT for partitions smaller than 32 MB
05	Extended partition
06	DOS 16-bit FAT for partitions larger than 32 MB
07	NTFS and exFAT
08	AIX bootable partition
09	AIX data partition
0B	DOS 32-bit FAT
0C	DOS 32-bit FAT for interrupt 13 support
0F	Extended Partition with Logical Block Address (LBA)
17	Hidden NTFS partition (XP and earlier)
1B	Hidden FAT32 partition
1E	Hidden VFAT partition
3C	Partition Magic recovery partition
66–69	Novell partitions
81	Linux
82	Linux swap partition (can also be associated with Solaris partitions)
83	Linux native file systems (Ext2, Ext3, Ext4, Reiser, Xiafs)

Hexadecimal code	File system
86	FAT16 volume/stripe set (Windows NT)
87	High Performance File System (HPFS) fault-tolerant mirrored partition or NTFS volume/stripe set
A5	FreeBSD and BSD/386
A6	OpenBSD
A9	NetBSD
C7	Typical of a corrupted NTFS volume/stripe set
EB	BeOS

❖Figure 3 : Hexadecimal codes in partition table[1]

Examining FAT Disks

- File Allocation Table (FAT) , this is a file structured that was designed by Microsoft for floppy disk
- The FAT helps to organized the files on the disk to allow the OS locate them easily
- Other than windows, other operating systems like linux and Mac OS can read, write and format to FAT drives
- The latest versions of FAT are FAT16, FAT32, and exFA
- FAT was the primary file system on MS-DOS systems and floppy diskettes and was also used extensively on Windows 3.x and Window 95 and 98 [3]

Examining NTFS files

- NTFS was introduced with Windows NT and remains the primary file system in Windows 10, with incremental changes over generations of Windows.
- NTFS was inspired by Microsoft's project for IBM's OS/2 operating system, which used the High Performance File System (HPFS). Windows NT provided backward compatibility with OS/2 HPFS disk drives, but this was discontinued after Windows 2000.
- NTFS provides more file information, including security features and ownership, compared to FAT file systems, offering greater control over files and folders.
- NTFS introduced journaling, which records transactions like file deletion or saving before executing them, aiding in recovering from interruptions like power failures.

Examining NTFS files+

- In NTFS, everything written to the disk is considered a file. The Master File Table (MFT), akin to FAT in older Microsoft OSs, is the first file on the disk and expands as data is added.
- NTFS results in less file slack space compared to FAT, with smaller cluster sizes for smaller disk drives, saving space on all disks using NTFS.
- NTFS uses Unicode, supporting UTF-8, UTF-16, and UTF-32 configurations, useful for keyword searches on disk drives.
- Due to its many features, NTFS requires more utilities for management compared to FAT.

Master File Table (MFT)

- What we need to know about this file is that it contains the Master File Table (MFT) that is basically a dictionary of all files and folders on the NTFS partition. [4]
- The Master File Table (MFT) is a special file in NTFS that contains a record for every file and directory on the volume.
- It serves as a database storing information such as file name, timestamps, attributes, and pointers to file data.
- Each entry in the MFT is called an MFT record and is identified by a unique number.
- Windows creates a backup copy of the first few MFT records called the MFT mirror to ensure integrity.
- The MFT is crucial for file system operations, used by the OS to locate and access files on the disk.

NTFS Compressed Files

- NTFS allows for file, folder, or volume compression, improving data storage similar to the FAT DriveSpace 3 utility.
- Compressed data appears normal in Windows Explorer or applications like Microsoft Word on Windows NT or later systems.
- In investigations, forensic tools can analyze compressed Windows data, including Lempel-Ziv-Huffman (LZH) compressed data and formats like PKZip, WinZip, and GNU gzip. However, third-party compression utilities like .rar may pose difficulties and require the utility that created them for decompression.

NTFS Encrypting File System

- NTFS Encrypting File System (EFS) added to Windows 2000 for file encryption.
- EFS uses public and private key encryption.
- Only the file owner can access encrypted files, holding the private key.
- The public key is held by a certification authority like VeriSign.
- A recovery certificate is generated for file recovery if the original private key is lost.
- The recovery key is sent to the local Windows administrator account.
- EFS can be applied to files on local workstations or remote servers.

NTFS Encrypting File System +

- Windows automatically decrypts EFS data when accessed by the user or an application.
- Users can grant other users access to their EFS data.
- If an EFS file is copied to an unencrypted folder, it is saved in unencrypted format

EFS Recovery Key Agent

- The Recovery Key Agent manages the recovery certificate in the Windows administrator account.
- Windows administrators can recover keys using the cipher or copy commands from a command prompt.
- The cipher command works only on NTFS systems from Windows 2000 Professional onwards, while the copy command works on both FAT and NTFS.
- Vista Business Edition and later versions have added features to the cipher command, like the /w switch that overwrites deleted files for added security.
- When an encrypted file is copied from an EFS-enabled NTFS disk to a non-EFS storage, it is automatically decrypted.

EFS Recovery Key Agent +

- To recover an encrypted EFS file, it can be emailed or copied to the administrator for restoration using the Recovery Key Agent function.
- For more information, refer to Microsoft's articles on "How It Works" and "The Encrypting File System."

Understanding Whole Disk Encryption

- Loss of personal identity information (PII) and trade secrets due to computer theft is a growing concern.
- PII includes employees' personal information, which can be used for identity theft.
- Trade secrets, if released, can harm a business's competitive edge.
- Whole disk encryption (WDE) is used to prevent unauthorized access to data.
- WDE tools offer preboot authentication, full or partial disk encryption, and advanced encryption algorithms.

Understanding Whole Disk Encryption+

- Decryption of a drive encrypted with WDE requires running a vendor-specific program.
- BitLocker is Microsoft's utility for protecting drive data, available in certain Windows editions.
- Third-party WDE utilities offer more features than BitLocker, such as encryption of FAT drives.
- Decrypting with third-party utilities follows a similar process to BitLocker.
- Improved encryption methods make extracting digital evidence more challenging, necessitating knowledge of remote live acquisitions.

Examining Microsoft BitLocker

- BitLocker is a Microsoft tool for encrypting data
- Encase software can be used to decrypt bitLocker encrypted files

BitLocker Requirements[1]

- A computer capable of running Windows Vista or later (non-home editions)
- The Trusted Platform Module (TPM) microchip, version 1.2 or newer
- A computer BIOS compliant with Trusted Computing Group (TCG)
- Two NTFS partitions for the OS and an active system volume with available space
- The BIOS configured so that the hard drive boots first before checking the CD/
- DVD drive or other bootable peripherals

Merits of WDE With BitLocker

- **Data Security,** WDE protects data at rest, ensuring that even if a device is lost or stolen, the data remains encrypted and inaccessible without the decryption key.
- **Compliance, m**any regulatory requirements and standards (e.g., GDPR, HIPAA) mandate the use of encryption to protect sensitive data, making WDE essential for compliance.
- **Data Integrity,** WDE can also help ensure data integrity by protecting against unauthorized modifications to encrypted data.
- **Ease of Us,** modern WDE solutions are designed to be transparent to users, requiring minimal interaction once set up, thus not hindering user experience.
- **Platform Agnostic,** WDE can be implemented across various platforms and devices, including laptops, desktops, and servers

Demerits of WDE With BitLocker

- **Performance Overhead,** encrypting and decrypting data can introduce a performance overhead, although modern hardware and encryption algorithms have minimized this impact.
- **Key Management,** managing encryption keys can be complex, especially in large organizations with numerous devices and users. Proper key management practices are essential.
- **Data Recovery,** if encryption keys are lost or corrupted, recovering data can be challenging or even impossible without a backup or recovery mechanism in place.
- **Compatibility,** WDE may not be compatible with certain hardware or software configurations, requiring careful consideration during implementation.
- **User Education,** users need to be educated on the importance of encryption and the implications of data loss, as well as the proper handling of encryption keys.

Examining Third-Party Disk Encryption Tools

- A lot of software companies offers third party encryption tools that have more features that the BitLocker

Some of the common encryption tools includes

- Endpoint Encryption (*www.symantec.com/products/endpoint-encryption*)
- Voltage SecureFile (*www.voltage.com/products/data-security/hpe-securefile/*)
- Jetico BestCrypt Volume Encryption (*www.jetico.com/products/personal-privacy/ bestcrypt-volume-encryption*)

Understanding the Windows Registry

- The Windows Registry stores hardware and software configuration information, network connections, user preferences, and setup information.
- It replaced initialization (.ini) files in Windows 95 and is still used in Windows Vista and later versions.
- The Registry can contain valuable evidence for investigations.
- Regedit and Regedt32 are tools used to view the Registry in different Windows versions.
- You can use the Registry Editor's Find command to locate entries containing trace evidence, such as user account information and recently accessed files.

Understanding the Windows Registry+

- Installed programs store information in the Registry, including accessed websites, recent files, and chat rooms.
- Digital forensics investigators should explore the Registry of all Windows systems but should avoid altering any settings on a live system to prevent system corruption.

Exploring the Organization of the Windows Registry

❖ The Windows Registry is organized hierarchically, similar to a file system, with keys and values that store configuration settings for the operating system and installed applications.

Main components of the Windows Registry:

- **HKEY_CLASSES_ROOT (HKCR)**: Contains file extension associations, OLE object class identifiers, and shortcut information. It merges two other keys, HKEY_LOCAL_MACHINE\Software\Classes and HKEY_CURRENT_USER\Software\Classes, into a single view.
- **HKEY_CURRENT_USER (HKCU)**: Contains configuration information for the user currently logged on. It includes settings for the desktop, Windows Explorer, and other user-specific settings.

Exploring the Organization of the Windows Registry +

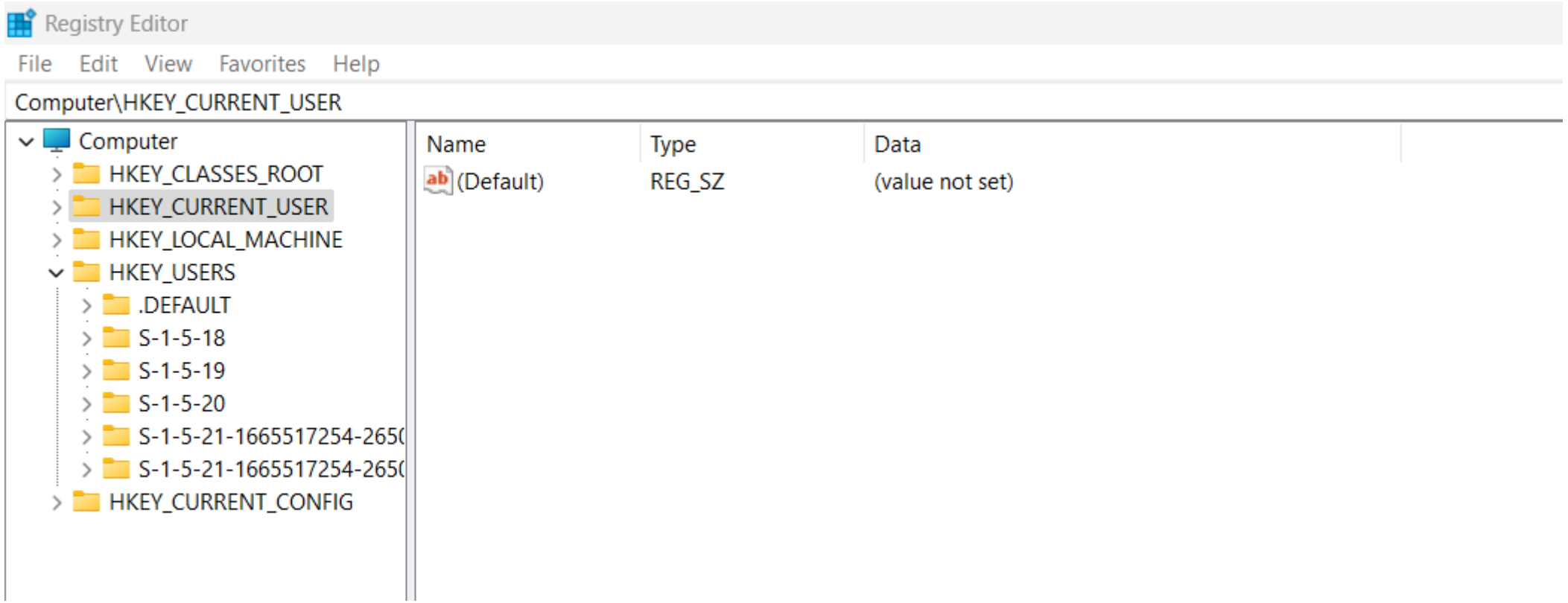
- **HKEY_LOCAL_MACHINE (HKLM)**: Contains configuration information for the computer's hardware and software. It includes settings for installed hardware, software settings, and system settings that apply to all users.
- **HKEY_USERS (HKU)**: Contains user profiles and settings for all users who have logged on to the computer. Each user's settings are stored in a separate subkey.
- **HKEY_CURRENT_CONFIG (HKCC)**: Contains information about the current hardware profile used by the computer.
- **HKEY_CURRENT_USER\Software**: Contains settings for applications installed for the current user.

Exploring the Organization of the Windows Registry ++

- **HKEY_LOCAL_MACHINE\Software**: Contains settings for applications installed for all users on the computer.
- **Subkeys and Values**: Keys can contain subkeys, which can further contain subkeys or values. Values are used to store configuration data. They can be strings, binary data, or integers.
- **Registry Editor**: The Registry can be viewed and edited using the Registry Editor (Regedit.exe or Regedt32.exe). It allows users to navigate the Registry, view keys and values, and make changes to the configuration settings.

Exploring the Organization of the Windows Registry +++

❖Registry Editor screen



Exploring the Organization of the Windows Registry ++++

❖Registry Locations and purposes

Filename and location	Purpose of file
Users*user-account*\Ntuser.dat	User-protected storage area; contains the list of most recently used files and desktop configuration settings
Windows\system32\config\Default.dat	Contains the computer's system settings
Windows\system32\config\SAM.dat	Contains user account management and security settings
Windows\system32\config\Security.dat	Contains the computer's security settings
Windows\system32\config\Software.dat	Contains installed programs' settings and associated usernames and passwords
Windows\system32\config\System.dat	Contains additional computer system settings
Windows\system32\config\systemprofile	Contains additional NTUSER information

Figure 5: File Locations and purpose[1]

Examining the Windows Registry:

- Forensics tools like X-Ways Forensics, OSForensics, Forensic Explorer, and FTK offer built-in or add-on Registry viewers.
- The Legal Department requests a search for email addresses with the name Okwir or Hong See Kee and the domain outlook.com in a forensic image of a Windows 8 computer's hard drive.
- OSForensics is used to examine Okwir Hong See Kee NTUser.dat file, and any relevant items are added to a case report.
- HKEY_CURRENT_CONFIG is a symbolic link to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware ProfileVxxxx and contains hardware configuration settings.
- HKEY_DYN_DATA, used in Windows 9x/Me systems, stores hardware configuration settings.

Steps for Examining Registry Files with OSForensics:

- Start OSForensics as an administrator and click "Continue Using Trial Version."
- Click "Manage Case" and create a new case named EImage01.img, specifying your name as the investigator.
- Mount the EImage01.img file in OSForensics.
- Open the Registry Viewer in OSForensics and select the drive letter where the registry hive file is located.
- Search for "Outlook.com" in the NTUSER.DAT file and add relevant items to the case report.
- Exit Registry Viewer when the examination is complete.

Understanding Virtual Machines

- Newer versions of operating systems and applications are frequently released, yet older versions remain prevalent.
- Investigators often struggle with resource limitations when dealing with the diverse range of software they encounter.
- The adoption of virtualization by many companies to cut hardware expenses is leading to an increase in investigations involving virtual machines.
- Investigators may find themselves needing a virtual server to access older systems and to analyze virtual machines belonging to suspects.

Understanding Virtual Machines+

- Virtual machines allow the operation of a different OS on a host computer by mimicking its hardware environment.
- Typically, a virtual machine is composed of multiple files, including a configuration file detailing hardware settings and a virtual hard disk file containing the necessary boot loader program, operating system files, and user data files.

Setting up a virtual machine

- **Choose a Virtualization Software**: Select a virtualization software such as VMware, VirtualBox, or Hyper-V.

- **Download and Install the Virtualization Software**: Download the software from the official website and follow the installation instructions.

- **Download the Operating System ISO**: Obtain the ISO file for the operating system you want to install on the virtual machine.

- **Create a New Virtual Machine**: Open the virtualization software and create a new virtual machine. Specify the operating system type and version.

Setting up a virtual machine+

- **Allocate Resources**: Allocate resources such as CPU, RAM, and storage space to the virtual machine.
- **Select Installation Media**: Choose the ISO file you downloaded as the installation media for the virtual machine.
- **Install the Operating System**: Start the virtual machine and follow the on-screen instructions to install the operating system.
- **Install Virtual Machine Tools (Optional)**: Install the tools provided by the virtualization software to enhance the virtual machine's performance and functionality.

Setting up a virtual machine+

- **Configure Network Settings**: Configure network settings for the virtual machine to connect to the internet or other network devices
- **Install Software and Updates**: Install any additional software or updates needed for the operating system running on the virtual machine.
- **Configure Virtual Machine Settings**: Adjust settings such as display resolution, shared folders, and hardware acceleration as needed.

Setting up a virtual machine++

- **Save and Back Up the Virtual Machine**: Save the virtual machine configuration and consider creating a backup to protect against data loss.

- **Start and Use the Virtual Machine**: Start the virtual machine to begin using the installed operating system and software.

- For practical installation from this link (https://www.instructables.com/How-to-Create-a-Virtual-Machine/)

Summary of week 4 lecture

- In this lecture, we discussed about file systems, exploring their definition and crucial role in organizing data effectively. We then shift our focus to the common file systems used in Windows environments, including FAT32, NTFS, and exFAT, discussing their features and limitations.
- Next, we took a deep dive into the NTFS (New Technology File System) structure, understanding how it manages files, directories, and metadata. We explore the NTFS disk structures, highlighting the Master File Table (MFT) and its pivotal role in file system operations. Additionally, we examine disk allocation methods and how NTFS optimizes storage for improved performance.
- Moving on, we explore the importance of whole disk encryption for data security, introducing BitLocker Drive Encryption in Windows as a powerful tool for encrypting entire disk volumes. We discuss the benefits and challenges of whole disk encryption, emphasizing its role in protecting sensitive data.

Summary of week 4 lecture

- Finally we introduce the concept of virtualization and its myriad benefits for testing and development. We provide a step-by-step guide to creating a virtual machine using popular virtualization platforms like Hyper-V or VirtualBox.
- This lecture provides a comprehensive overview of file systems, disk structures, encryption, virtualization, and best practices, equipping you with the knowledge and tools to manage data effectively in Windows environments.
- Next week we shall discuss about the current digitals tools. I hope to see you there.

Reference

[1] Nelson, B., Phillips, A., & Steuart, C. (2019). *Guide to computer forensics and investigations* Course Technology Cengage Learning.

[2] Wikimedia Foundation. (2024, March 26). *Hard disk drive*. Wikipedia. https://en.wikipedia.org/wiki/Hard_disk_drive

[3] Carvey, H., & Altheide, C. (2011). *Digital forensics with open source tools*. Elsevier.

[4] Kävrestad, J. (2017). *Guide to digital forensics: a concise and practical introduction*. Springer.