**20CYS311 – Cyber Forensics**

**LAB – 1 & 2**

**S Shyam Balaji**

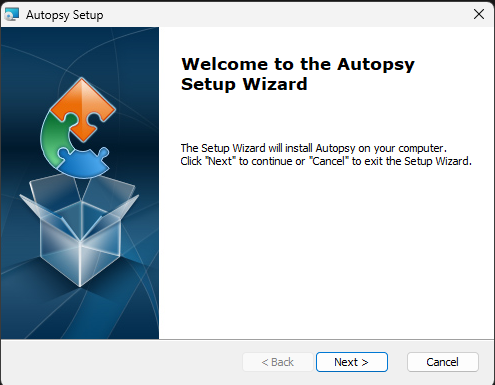
**CH.EN.U4CYS22045**

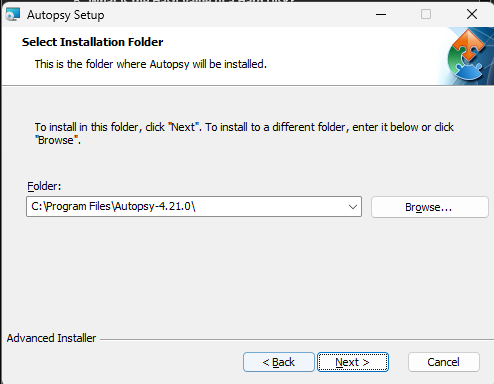
Lab Record

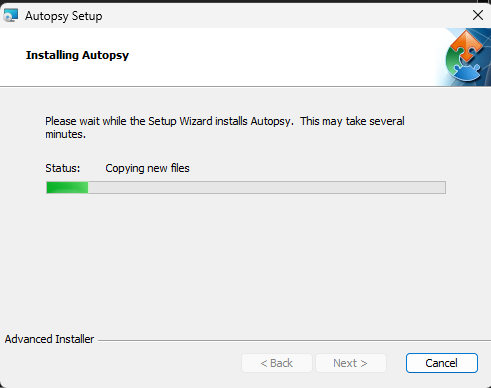
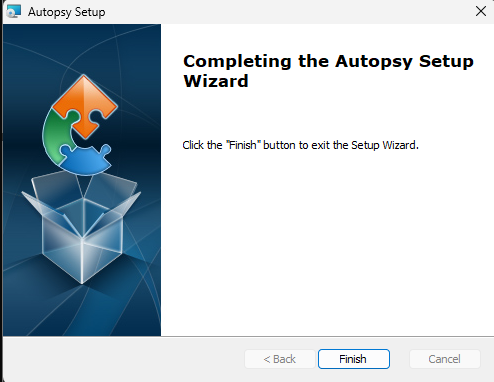
1. **What is Hard Disk Forensics?**  
   Hard disk forensics involves recovering, analyzing, and preserving data from storage devices for investigative purposes. It ensures data integrity while uncovering hidden, deleted, or encrypted files for legal use.
2. **What is an Image File?**  
   An image file is a digital representation of a visual object, like photos or graphics, stored in formats such as JPEG or PNG. It can also refer to disk images in computer forensics, which are exact copies of storage devices.
3. **What is Allocated and Unallocated Space?**  
   Allocated space is used to store active files and data, while unallocated space refers to unused disk areas that may contain remnants of deleted files.
4. **What is Disk Cache and Disk Mirroring?**  
   Disk cache temporarily stores frequently accessed data to improve read/write speed. Disk mirroring duplicates data across multiple disks to enhance redundancy and fault tolerance.
5. **What is a Forensic Image?**  
   A forensic image is a bit-for-bit copy of a storage device, preserving all data, including unallocated and slack space, for analysis without altering the original evidence.
6. **What is the Hash Value of a Hard Disk?**  
   A hash value is a unique string generated by hashing algorithms like MD5 or SHA, used to verify data integrity. Any changes to the disk will result in a different hash value.
7. **What is Shadow Volume, Shadow Copy, and Swap Disk?**  
   Shadow volumes and shadow copies create snapshots of files or drives for recovery. A swap disk extends system memory by using disk space as virtual RAM.
8. **What Tools Can Perform Hard Disk Forensics?**  
   Tools like EnCase, FTK Imager, Autopsy, and Sleuth Kit can create disk images, recover files, and analyze storage devices for forensic purposes.
9. **What is Exif Metadata?**  
   Exif metadata is embedded in image files and includes information like camera settings, date/time of capture, and GPS location, useful in forensic investigations.
10. **What are Common Disk Image Formats?**  
    Common formats include DD (raw image), E01 (EnCase Evidence File), and AFF (Advanced Forensic Format), each designed for forensic imaging and analysis.
11. **What is Bit-by-Bit Copying?**  
    Bit-by-bit copying creates an exact replica of a storage device, capturing all sectors, including hidden and unallocated ones, for complete duplication.
12. **What is Cloning a Disk?**  
    Disk cloning involves creating an exact duplicate of a storage device, including partitions and boot records, for backups or forensic analysis.
13. **What are the Latest Types of Storage Devices?**  
    Modern storage devices include SSDs for faster performance, NVMe drives for high-speed data access, and 3D NAND technology for higher storage densities.
14. **What is BitLocker Encryption?**  
    BitLocker is a Windows feature that encrypts entire disks to protect data against unauthorized access, using strong encryption algorithms.

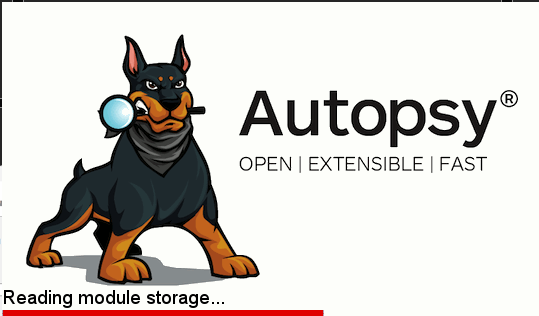
**Experiment – 1 (Analysis of Data source (Local Disk) using Autopsy**

**Step 1: Download Autopsy and Start**

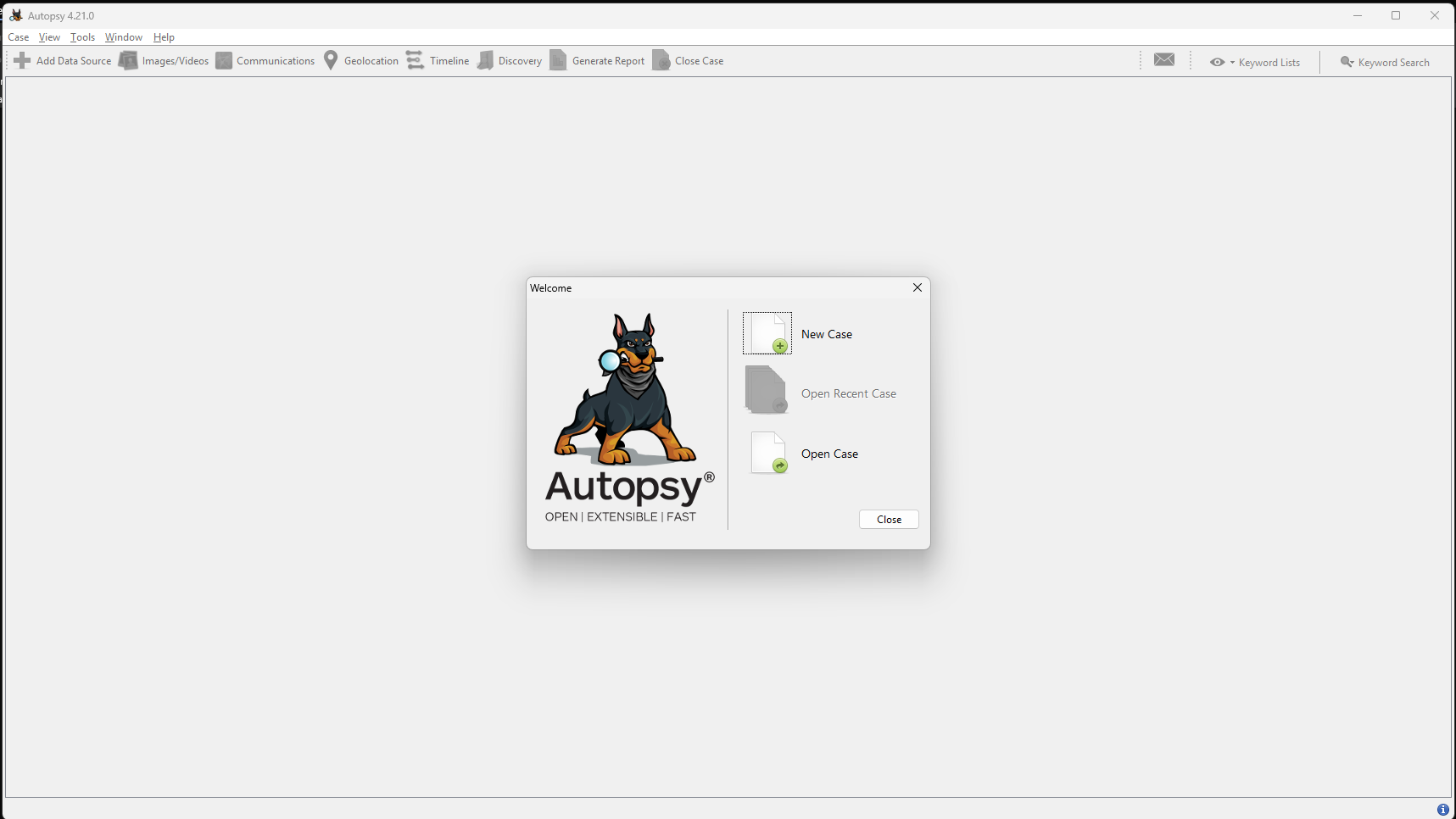


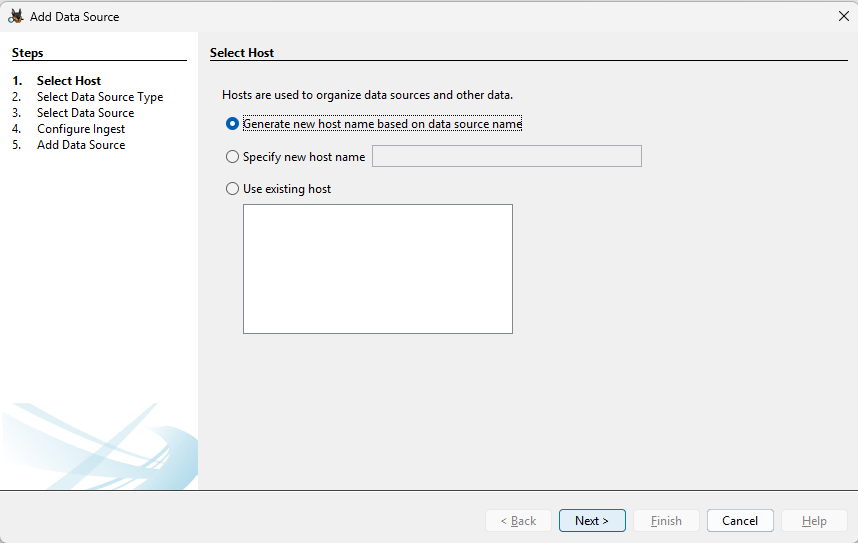


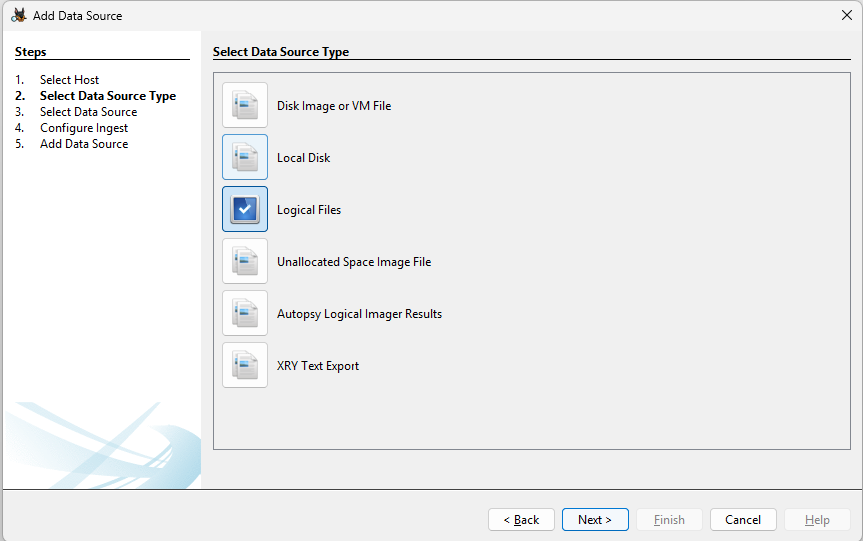
 

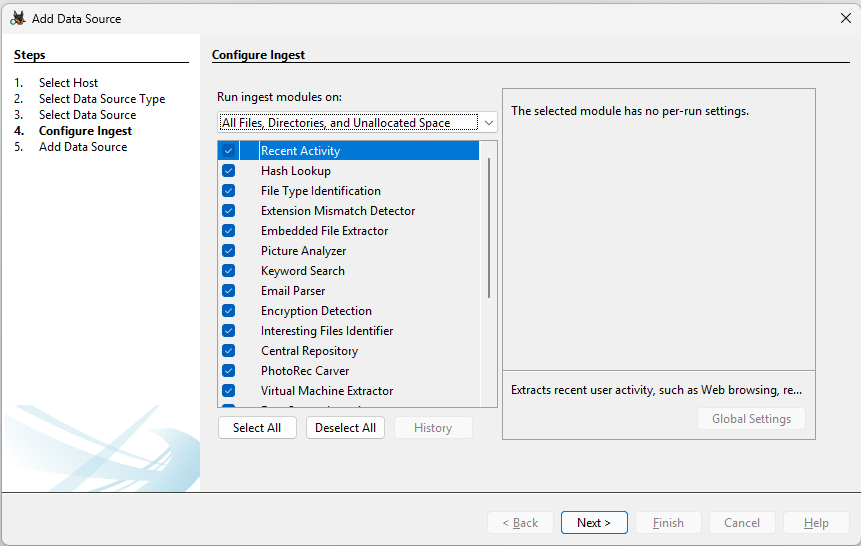


**Step 2: Add a Data Source**

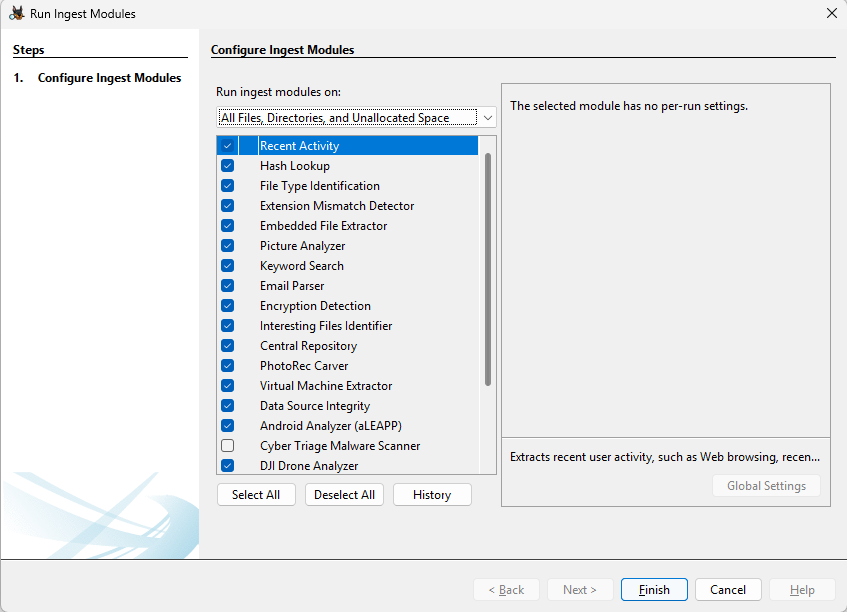


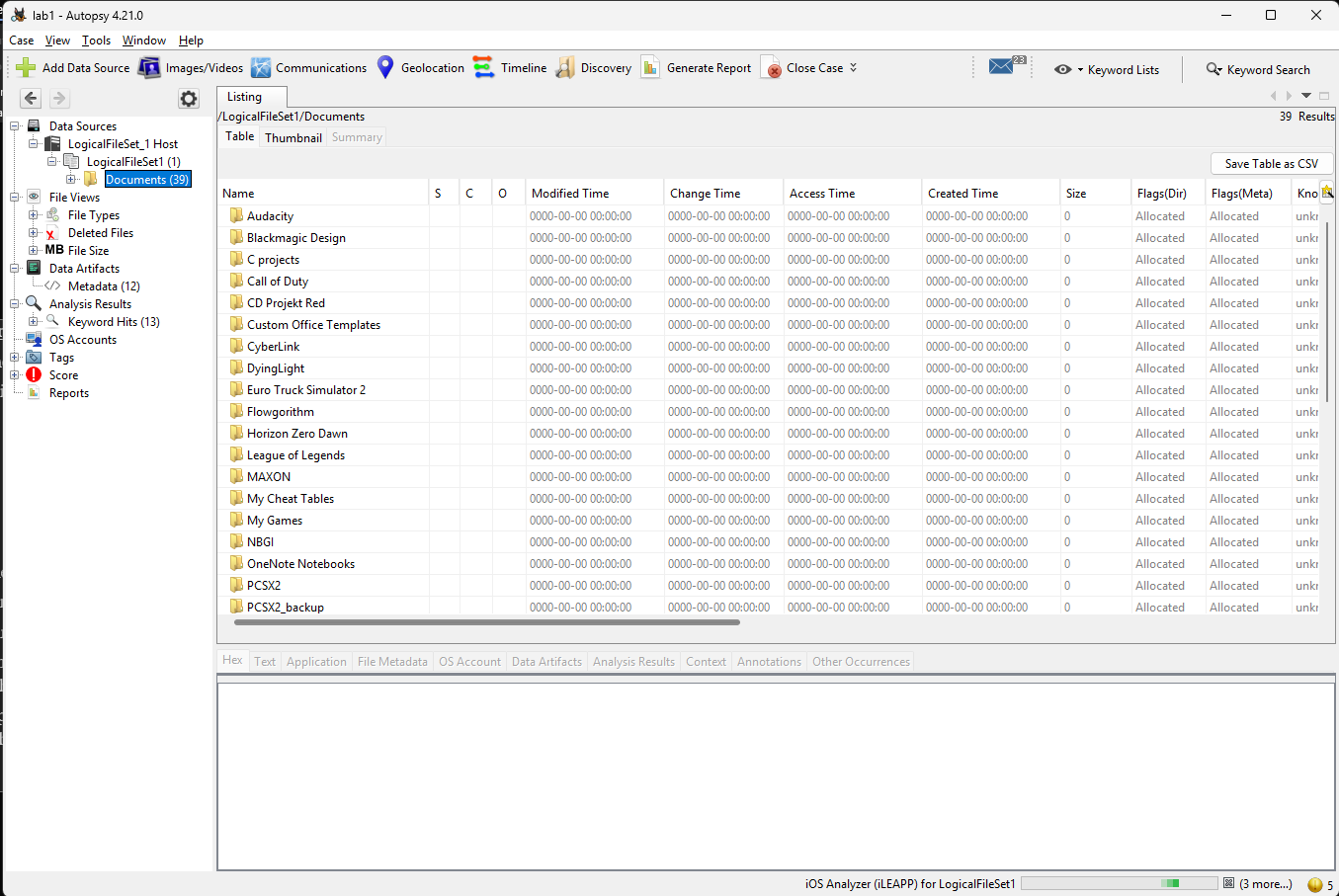




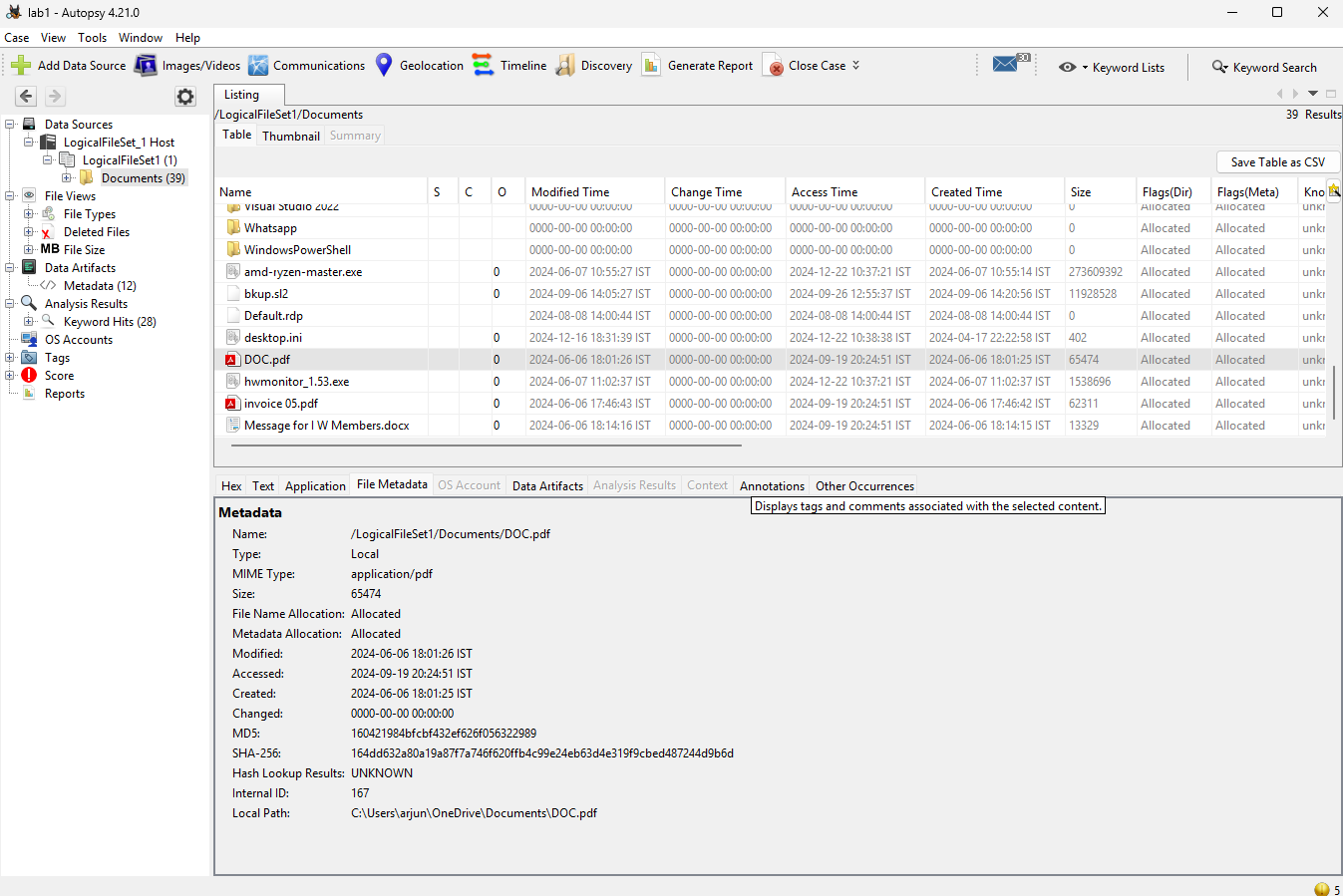


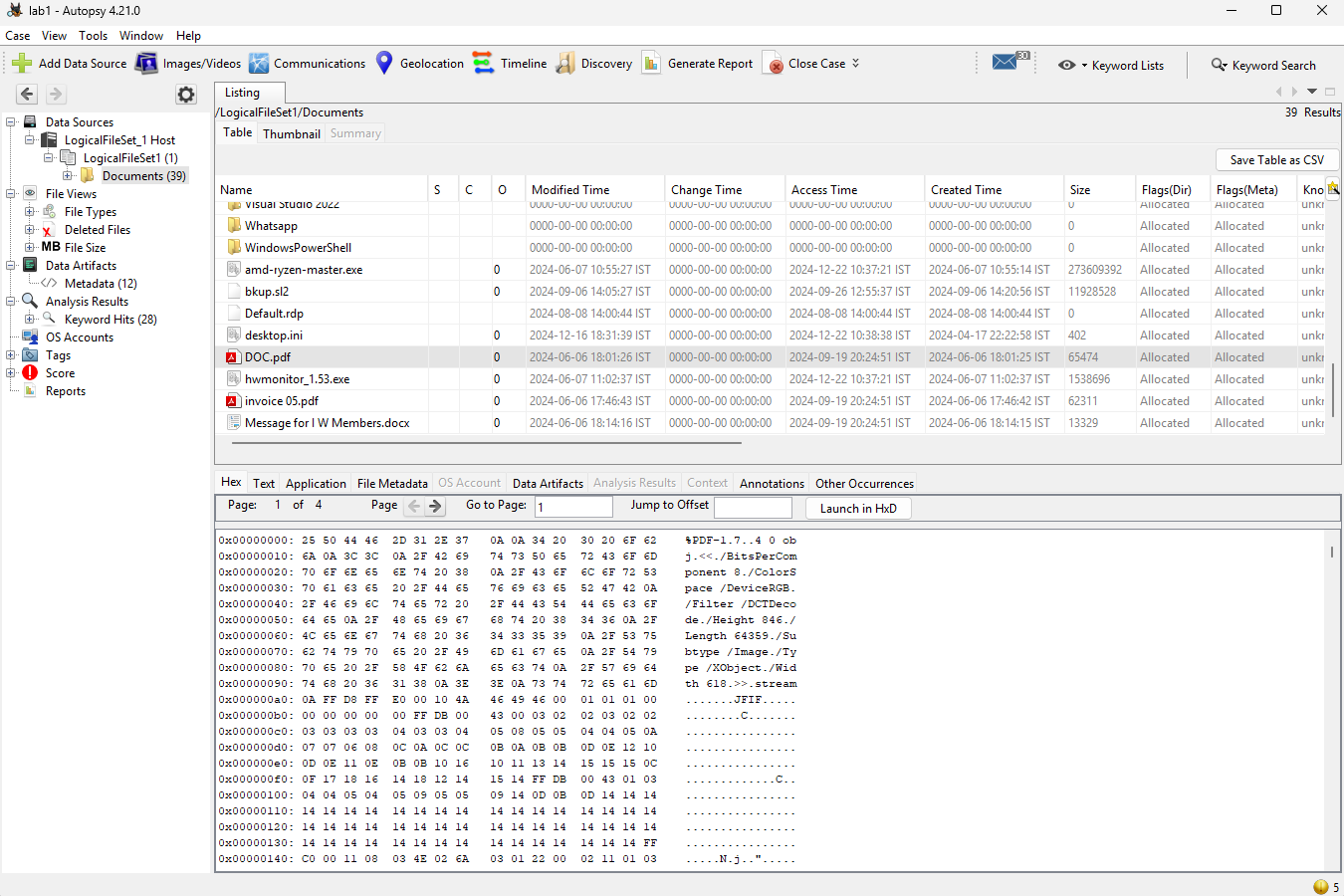
**Step 3: Configure Ingest Modules**



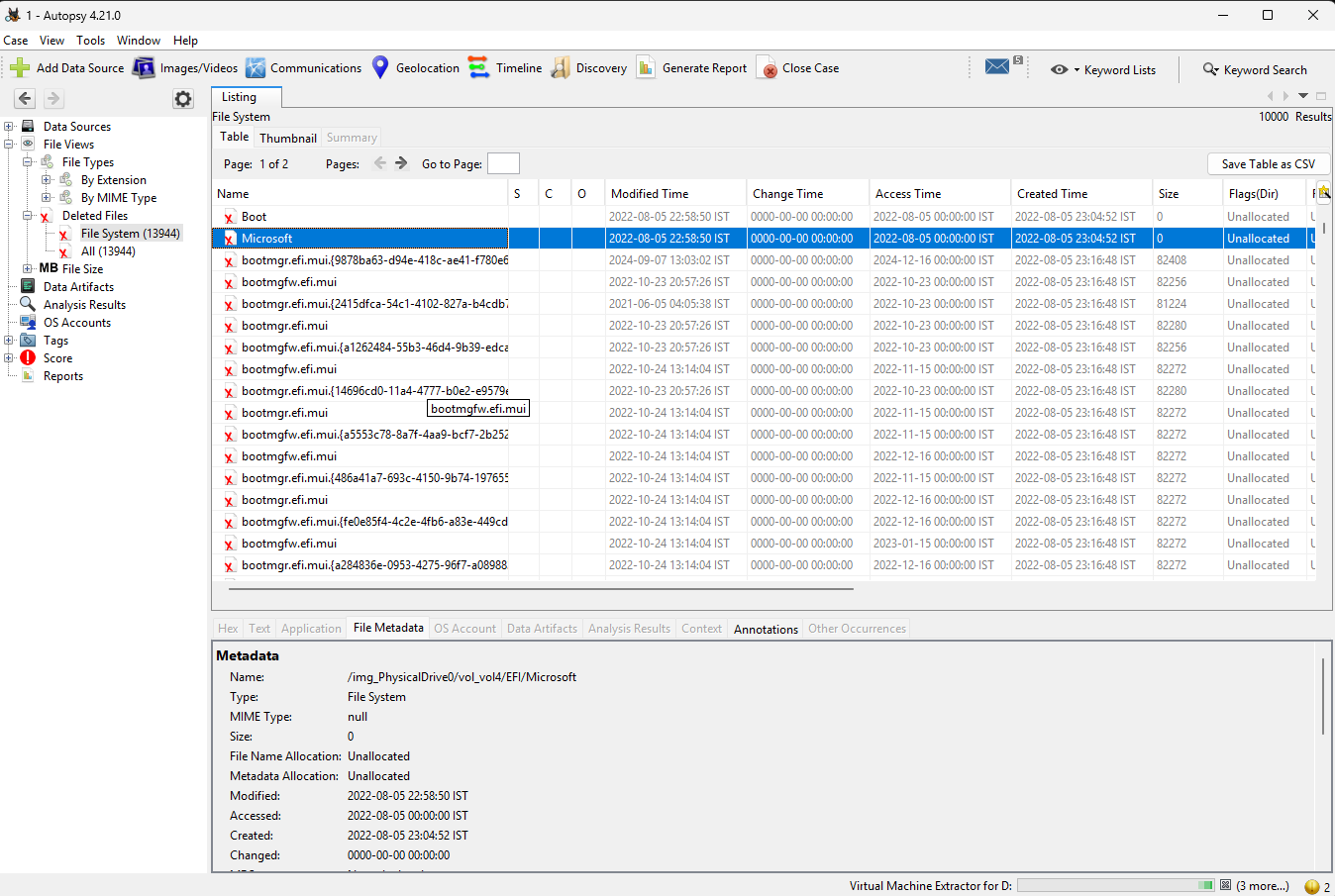


**Step 4: Exploring the Data Source**





**Step 5: Check for Unallocated, Deleted Files, and Extracted Contents**



**Experiment 2: Disk Analysis and Autopsy using TryHackMe**

