Disk Analysis Process:

- System and User Information:
  - Registry.
- File Analysis:
  - NTFS.
- Evidence of Execution:
  - Backgrount Activity Moderator (BAM).
  - ShimCache.
  - Amcache.
  - Prefetch.
- Persistence Mechanisms:
  - Run Keys.
  - Startup Folder.
  - Scheduled Tasks.
  - Services.
- Event Log Analysis.

Windows Sources of Evidence:

- Memory.
- Disk:
  - NT File System (NTFS).
  - Windows Registry Hives.
  - Windows Event Logs.
  - Other Windows Artifacts (Files or Databases).