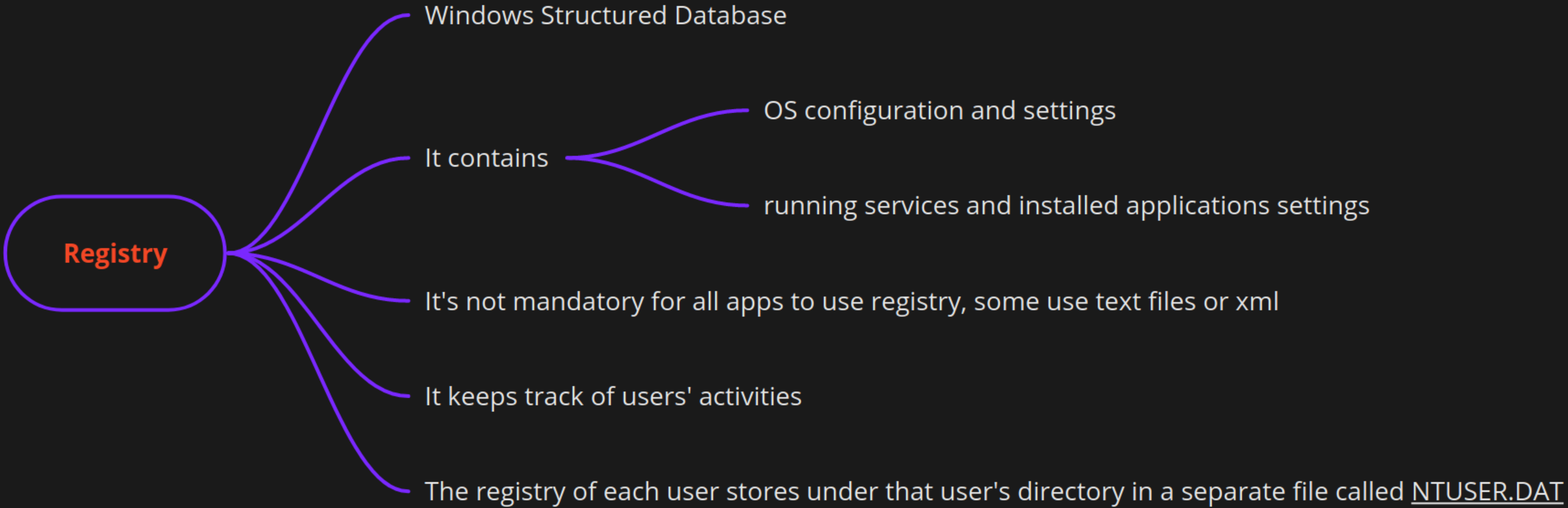
Practical Windows Forensics

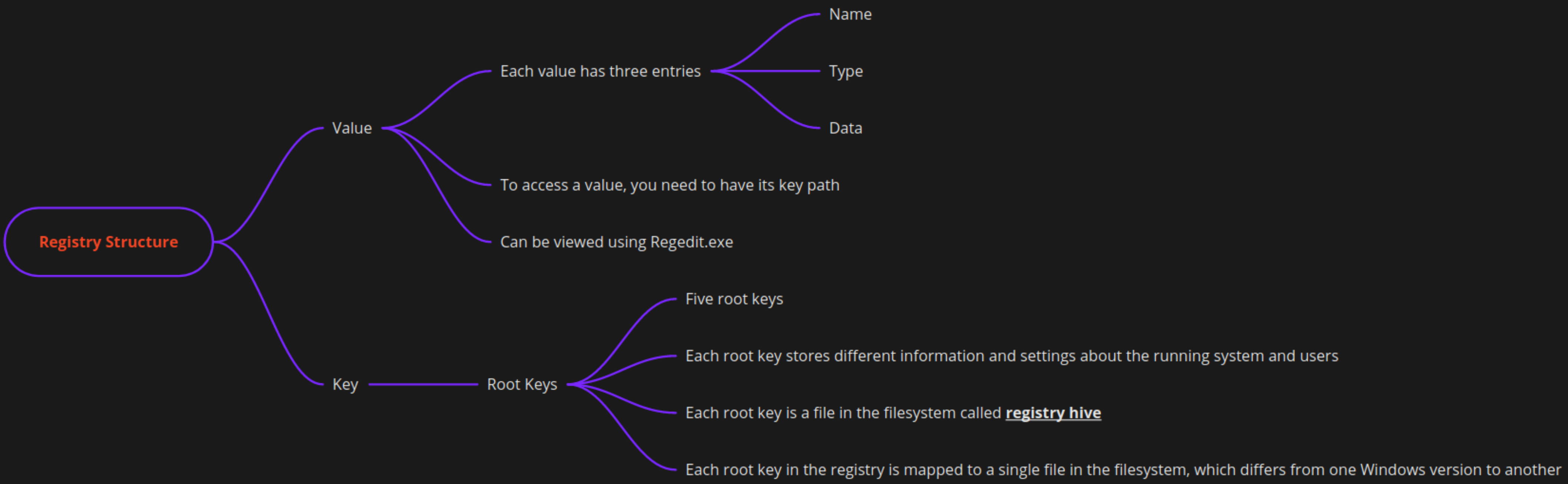
Chapter 7 - Registry Analysis

0x1411



Registry

- Windows Structured Database
- It contains
  - OS configuration and settings
  - running services and installed applications settings
- It's not mandatory for all apps to use registry, some use text files or xml
- It keeps track of users' activities
- The registry of each user stores under that user's directory in a separate file called NTUSER.DAT



Registry Structure

Value

Each value has three entries

Name

Type

Data

To access a value, you need to have its key path

Can be viewed using Regedit.exe

Key

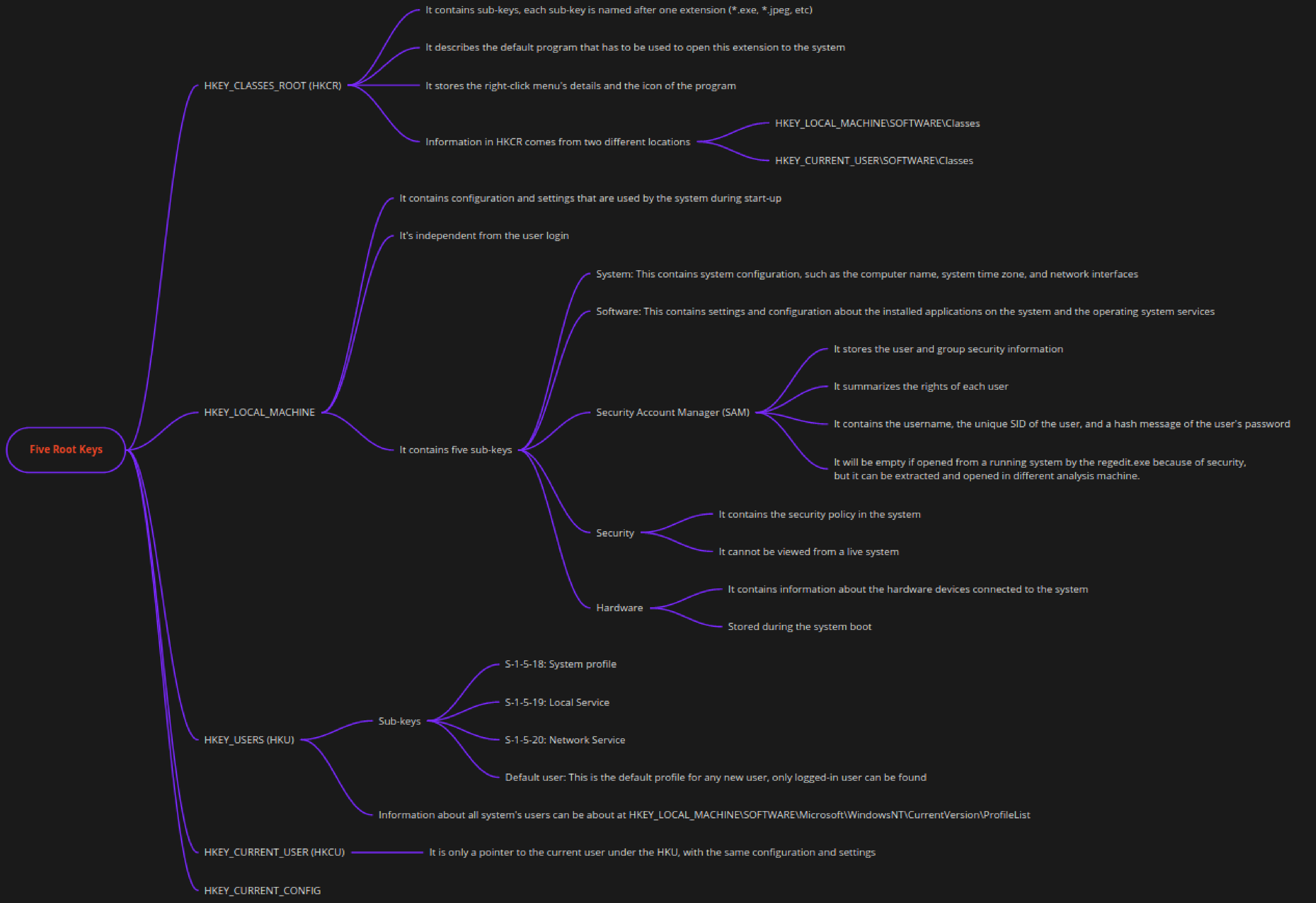
Root Keys

Five root keys

Each root key stores different information and settings about the running system and users

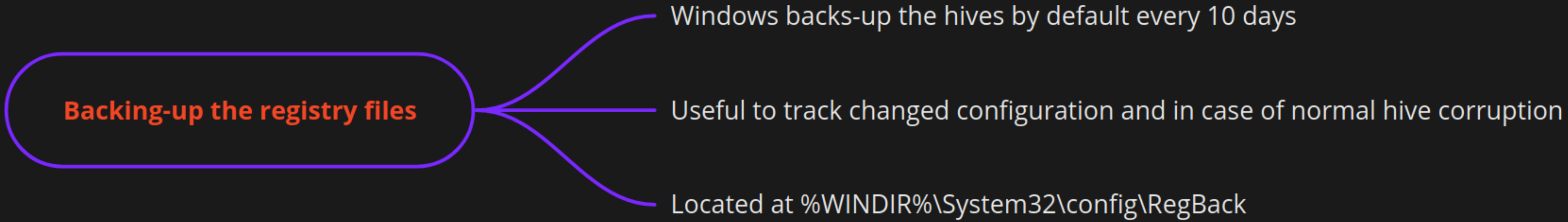
Each root key is a file in the filesystem called **registry hive**

Each root key in the registry is mapped to a single file in the filesystem, which differs from one Windows version to another



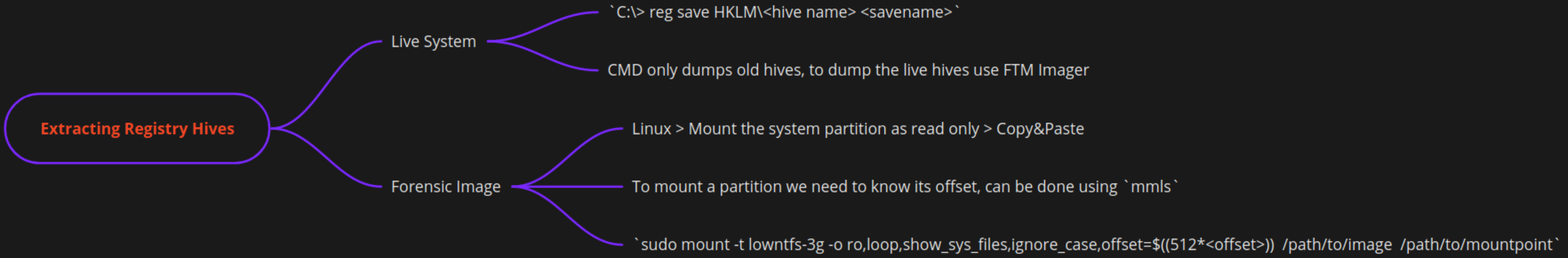
Five Root Keys

- HKEY_CLASSES_ROOT (HKCR)
  - It contains sub-keys, each sub-key is named after one extension (*.exe, *.jpeg, etc)
  - It describes the default program that has to be used to open this extension to the system
  - It stores the right-click menu's details and the icon of the program
  - Information in HKCR comes from two different locations
    - HKEY_LOCAL_MACHINE\SOFTWARE\Classes
    - HKEY_CURRENT_USER\SOFTWARE\Classes
- HKEY_LOCAL_MACHINE
  - It contains configuration and settings that are used by the system during start-up
  - It's independent from the user login
  - It contains five sub-keys
    - System: This contains system configuration, such as the computer name, system time zone, and network interfaces
    - Software: This contains settings and configuration about the installed applications on the system and the operating system services
    - Security Account Manager (SAM)
      - It stores the user and group security information
      - It summarizes the rights of each user
      - It contains the username, the unique SID of the user, and a hash message of the user's password
      - It will be empty if opened from a running system by the regedit.exe because of security,
        but it can be extracted and opened in different analysis machine.
    - Security
      - It contains the security policy in the system
      - It cannot be viewed from a live system
    - Hardware
      - It contains information about the hardware devices connected to the system
      - Stored during the system boot
- HKEY_USERS (HKU)
  - Sub-keys
    - S-1-5-18: System profile
    - S-1-5-19: Local Service
    - S-1-5-20: Network Service
    - Default user: This is the default profile for any new user, only logged-in user can be found
  - Information about all system's users can be about at HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ProfileList
- HKEY_CURRENT_USER (HKCU)
  - It is only a pointer to the current user under the HKU, with the same configuration and settings
- HKEY_CURRENT_CONFIG



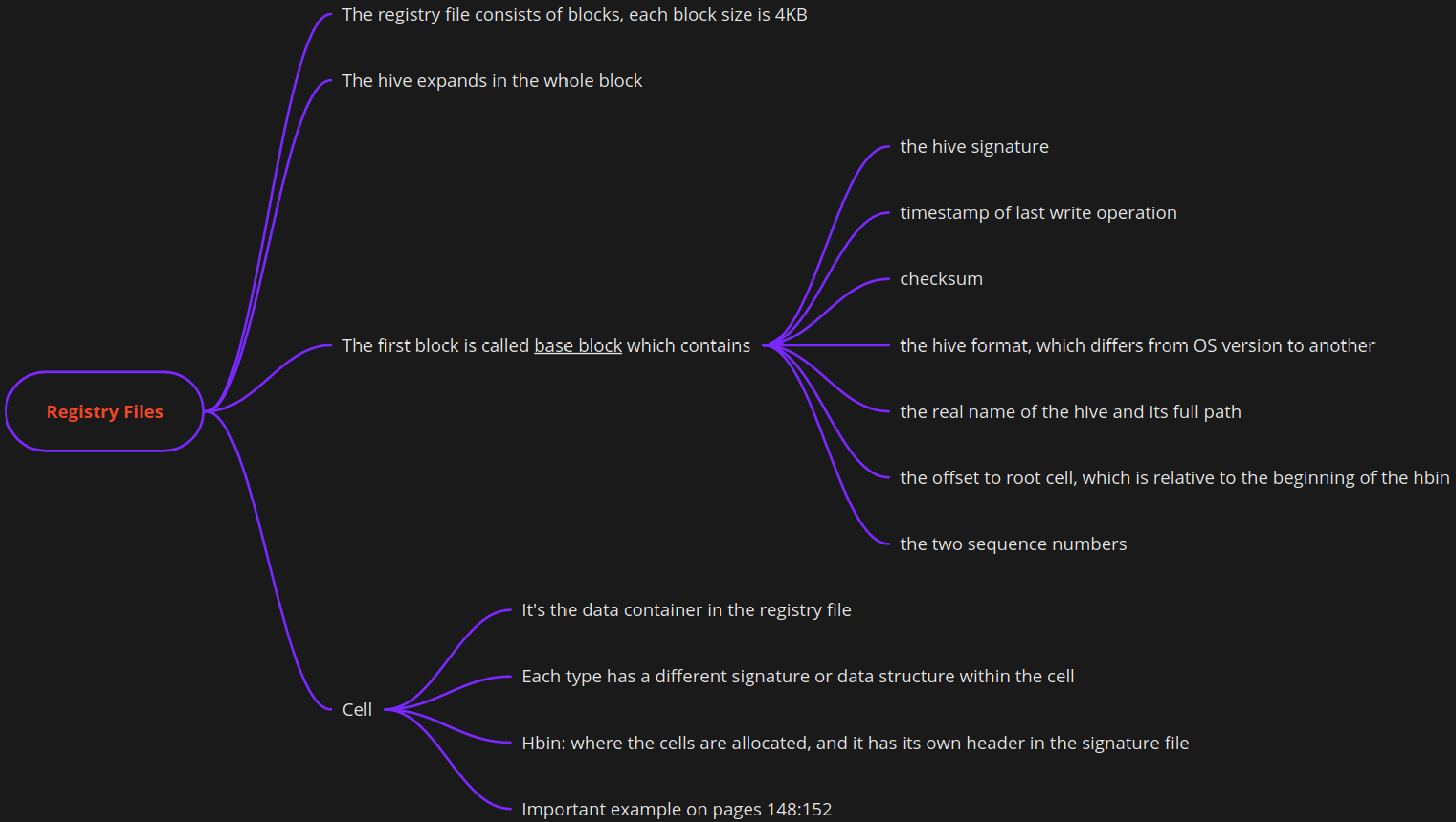
Backing-up the registry files

- Windows backs-up the hives by default every 10 days
- Useful to track changed configuration and in case of normal hive corruption
- Located at %WINDIR%\System32\config\RegBack



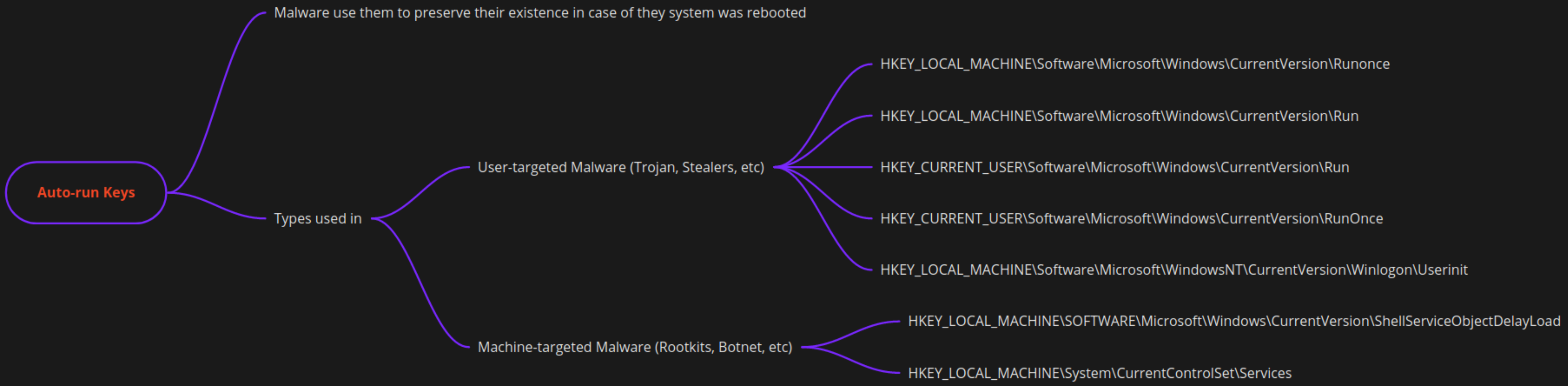
Extracting Registry Hives

- Live System
  - `C:\> reg save HKLM\<hive name> <savename>`
  - CMD only dumps old hives, to dump the live hives use FTM Imager
- Forensic Image
  - Linux > Mount the system partition as read only > Copy&Paste
  - To mount a partition we need to know its offset, can be done using `mmls`
  - `sudo mount -t lowntfs-3g -o ro,loop,show_sys_files,ignore_case,offset=$((512*<offset>))  /path/to/image  /path/to/mountpoint`



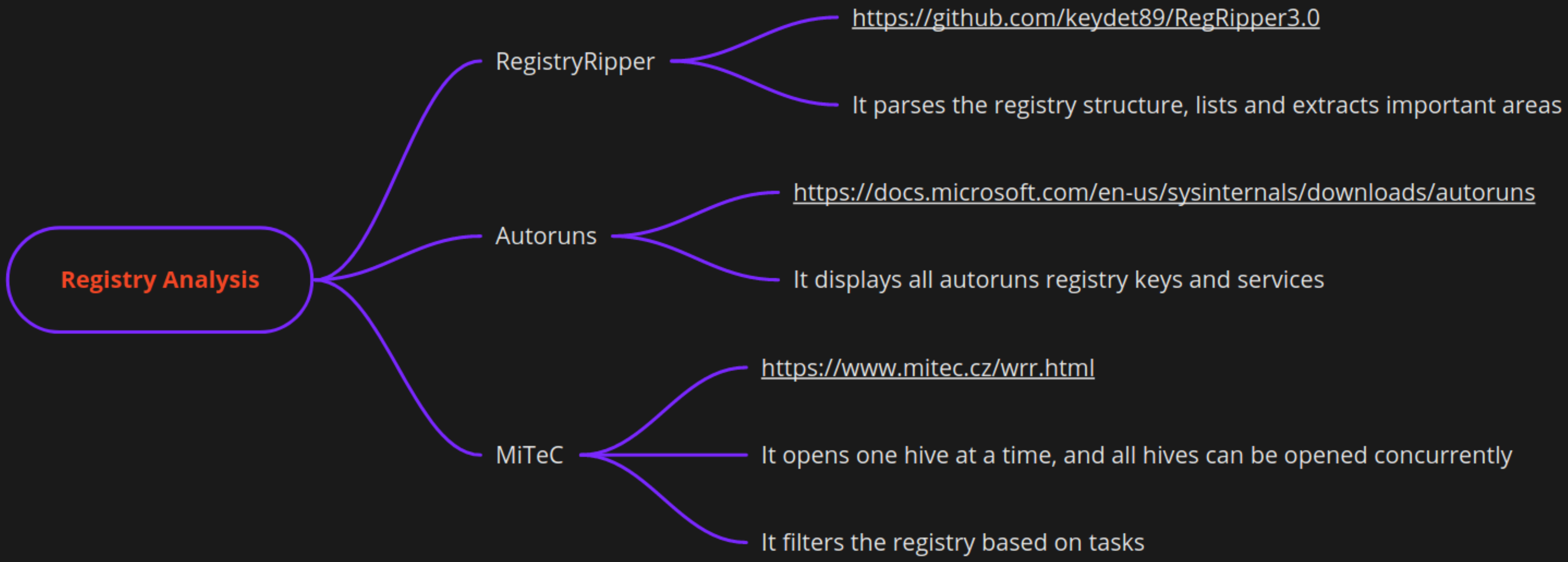
Registry Files

- The registry file consists of blocks, each block size is 4KB
- The hive expands in the whole block
- The first block is called base block which contains
  - the hive signature
  - timestamp of last write operation
  - checksum
  - the hive format, which differs from OS version to another
  - the real name of the hive and its full path
  - the offset to root cell, which is relative to the beginning of the hbin
  - the two sequence numbers
- Cell
  - It's the data container in the registry file
  - Each type has a different signature or data structure within the cell
  - Hbin: where the cells are allocated, and it has its own header in the signature file
  - Important example on pages 148:152



Auto-run Keys

- Malware use them to preserve their existence in case of they system was rebooted
- Types used in
  - User-targeted Malware (Trojan, Stealers, etc)
    - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runonce
    - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
    - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
    - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
    - HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\Userinit
  - Machine-targeted Malware (Rootkits, Botnet, etc)
    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad
    - HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services



Registry Analysis

- RegistryRipper
  - https://github.com/keydet89/RegRipper3.0
  - It parses the registry structure, lists and extracts important areas
- Autoruns
  - https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns
  - It displays all autoruns registry keys and services
- MiTeC
  - https://www.mitec.cz/wrr.html
  - It opens one hive at a time, and all hives can be opened concurrently
  - It filters the registry based on tasks