ESOF 422:

Advanced Software Engineering: Cyber Practices

Memory Forensics Conclusion, Disk Forensics

Reese Pearsall

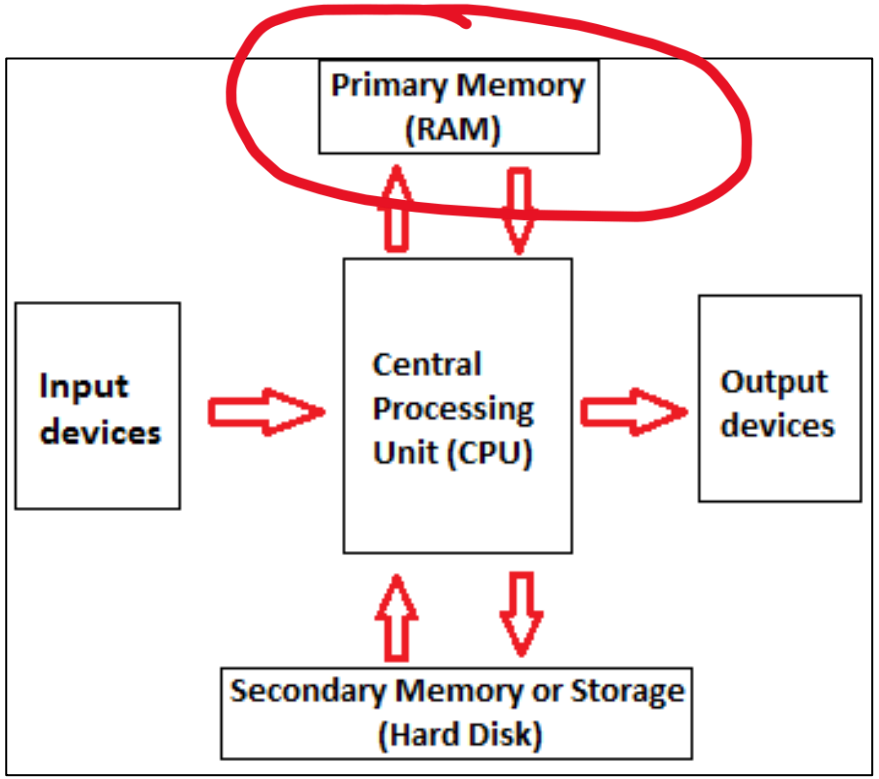
Spring 2025

Memory Forensics

Analysis of data sources from a running system's memory (RAM)

What does RAM contain?

- Programs and files that have been executed
- Running (and sometimes dead) processes
- What programs accessed what files
- Where opens files are/were location on disk
- Information from keyboard (passwords, emails, chats)
- Opened web pages
- Decrypted content
- Network connections
- Content no longer on disk
- Content that was never on disk



Malware Persistence

Malware will try to stay on the machine even after a reboot. One common approach for persistence is to add a new file to the list of programs to run on startup within the Windows Registry

```
┌──(kali㉿kali)-[~]
└─$ python ./volatility3/vol.py -f ./hw6/Lab3/target1/out.vmem windows.registry.printkey.PrintKey --key "\Microsoft\Windows\CurrentVersion\Run" --recurse
```

“`Microsoft\Windows\CurrentVersion\Run`” controls programs that automatically start when the user logs into windows

You may find that an unusual program (.exe) is included in the list

Extracting Specific File

windows.dumpfile may give you *a lot* of files that you may not want. If you do windows.filescan first, you can get the offset of the file you are looking for

```
┌──(kali㉿kali)-[~]
└─$ volatility3/vol.py -f hw6/Lab2/ecorpoffice/win7ecorpoffice2010-36b02ed3.vmem windows.filescan
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
Offset  Name

0×59e2070       \Windows\System32\wscui.cpl
0×59e9070       \$Directory
0×59f3650       \Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-Scripted%4Admin.evtx
0×59f7070       \Windows\System32\wups2.dll
0×59f7470       \Windows\System32\mspatcha.dll
0×59f7970       \Windows\WindowsUpdate.log
0×59f8660       \Windows\SysWOW64\msvfw32.dll
0×59f8bd0       \Users\PHILLI~1.PRI\AppData\Local\Temp\avicap32.dll
0×59f94e0       \Windows\System32\en-US\systemcpl.dll.mui
0×59f9ae0       \Windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.1.7600.16385_none_655452efe0fb810b\smipi.dll
0×59fa070       \Users\scott.knowles\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\4TTPU2O2\css[1].txt
0×59fa5e0       \Windows\ServiceProfiles\LocalService\AppData\Local\Microsoft\Windows\WindowsUpdate.log
0×59fa860       \$Directory
0×59fa9f0       \Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc
0×7fcf9320      \Windows\SysWOW64\shacct.dll
0×7fcfb2e0      \Users\phillip.price\Downloads\easychair.docx
0×7fcfbda0      \Windows\AppPatch\AcSpecfc.dll
```

This will only extract that file that you are looking for!

```
┌──(kali㉿kali)-[~]
└─$ volatility3/vol.py -f hw6/Lab2/ecorpoffice/win7ecorpoffice2010-36b02ed3.vmem windows.dumpfiles --physaddr 0×7fcfb2e0
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
Cache   FileObject      FileName        Result

DataSectionObject       0×7fcfb2e0      easychair.docx  file.0×7fcfb2e0.0×fa80040fe410.DataSectionObject.easychair.docx.dat
```

Malware Taxonomy

VirusTotal is very helpful for identifying the *type* of malware, which will help you analyze the threat

Trojan - disguises itself as legitimate program

Worm - self replicating malware and spreads over a network

Adware - displays and spams user with unwanted ads

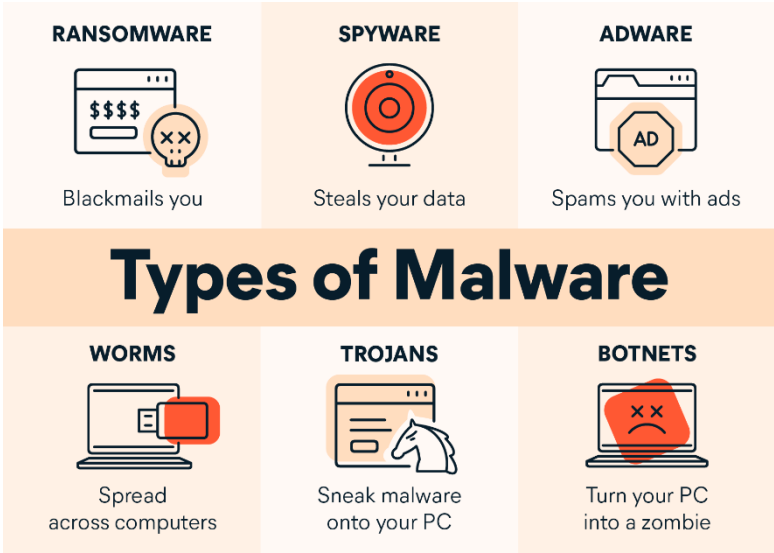
Virus - attaches to legitimate program or file to spread itself

Dropper - attempts to deliver and install additional software

Ransomware - encrypts and locks files until a ransom is paid

RAT (Remote Access Trojan) – Malware designed to allow an attacker to remotely control an infected computer

Spyware- Secretly monitors user activity



Dr. Zhong offers a 500-level malware analysis course if you are interested

CSCI 591-004	Sp: Malicious Code Analysis
Lecture	TR 1215-1330

Disk Forensics

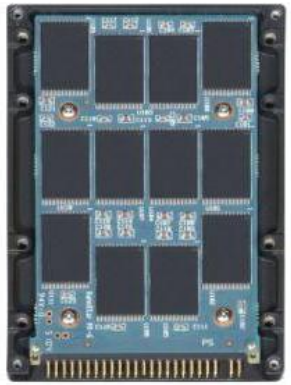
- Disk forensics is the study and analysis of storage volumes

- Disk forensics is typically used when you:
  – Cannot access the running state of the system
  – Are investigating historical activity
  – Are working a Law Enforcement (LE) case

Types of Disks

Magnetic Disks

- Traditional “spinning disks”
- Spinning platter with a thin magnetic coating
- “Head” moves over the platter to write 1’s and 0’s
- Same head used to read data off of the disk
- Sometimes hard to find / access data that’s not sequential (seeking / fragmentation)



Solid State Drives

- No magnets
- Flash memory to store data
- Specifically uses NAND flash which is persistent without power (unlike RAM)
- Can write to a page level, erase at a block level
- Garbage collection

Other types: **VMWare volumes**, **AWS Volumes**

Disk File System Formats

Format	Full Name	Creator	Released	Max File Size	Max Volume Size	Used for
NTFS	New Technology File System	Microsoft	1993	16 TB	256 TB	Windows systems, large disks
FAT	File Allocation Table	Microsoft	1977	2 GB	2 GB	Legacy files
FAT32	File Allocation Table 32 bit	Microsoft	1996	4 GB	32 GB	USB Drives, SD Cards
APFS	Apple File System	Apple	2017	8 EB	8 EB	Modern macOS devices

What is a file?

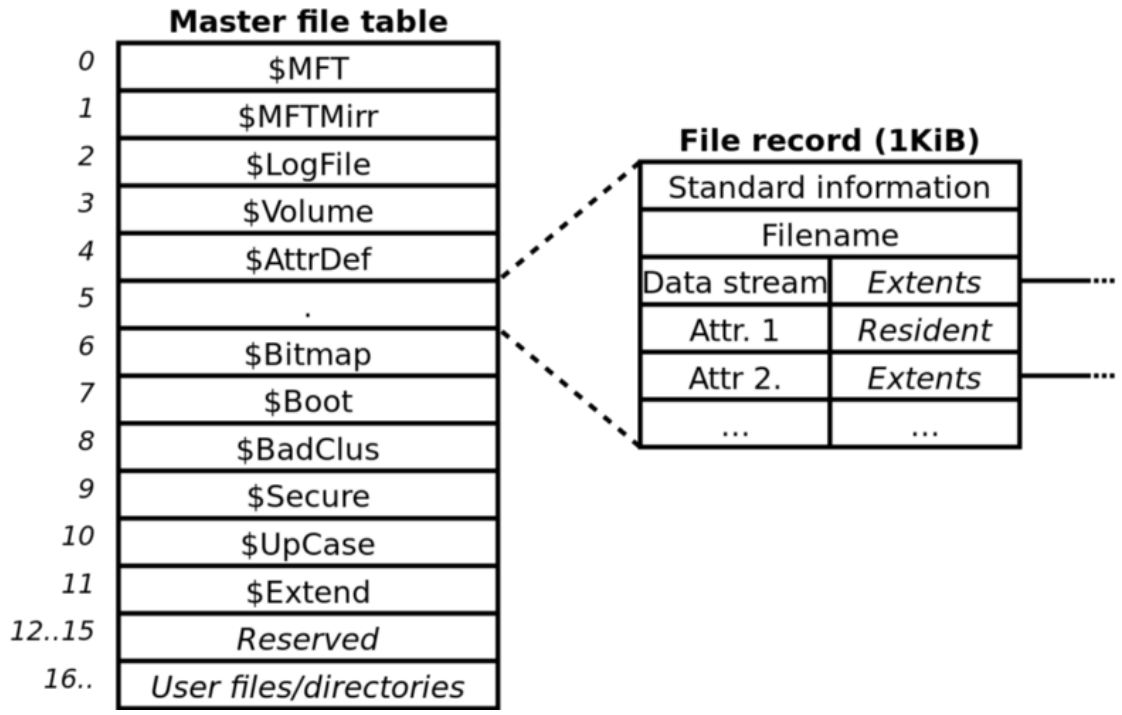
Short answer is that it depends on the file system.

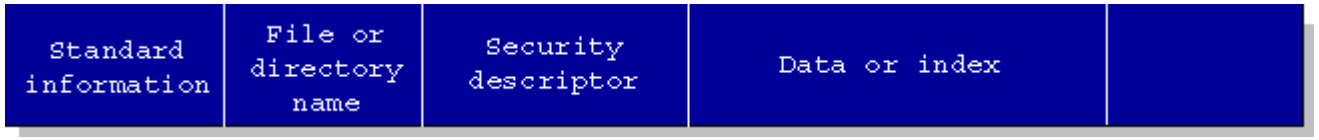
• “indexed” file systems keep an index of every file on the disk

• On an indexed file system the file is a combination of:

– Index entry (record) on **MFT** (Master File Table) for NTFS (metadata)

– Points to a location(s) on disk where the actual bytes reside





File Deletion

- What happens when you “delete” a file in Windows?

- “Delete” -> moves file to recycle bin.
- “Permanently Delete” -> only removes the metadata / journal entry.
- “Slack Space” -> “empty” disk we can look to carve files from.

Physical Disk Capture

Capturing the physical contents of a drive.

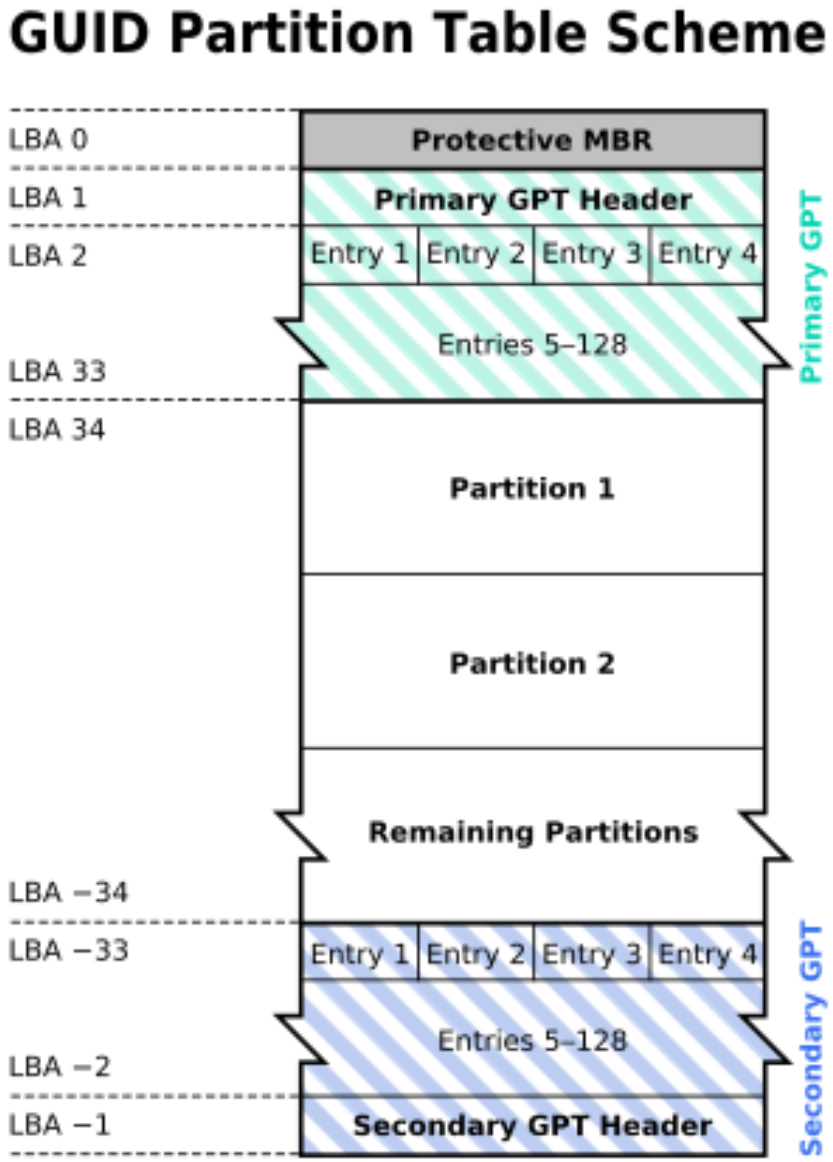
- Pros:
  - May get deleted files.
  - Will be able to parse the entire “raw” disk and data structures.
- Cons:
  - Capture used and “unused” disk space
  - Time consuming.
  - Large output file.

Important Disk Forensics Data Structures

MBR (Master Boot Record)
- Stored in first sector of the hard disk
- Contains the partition table

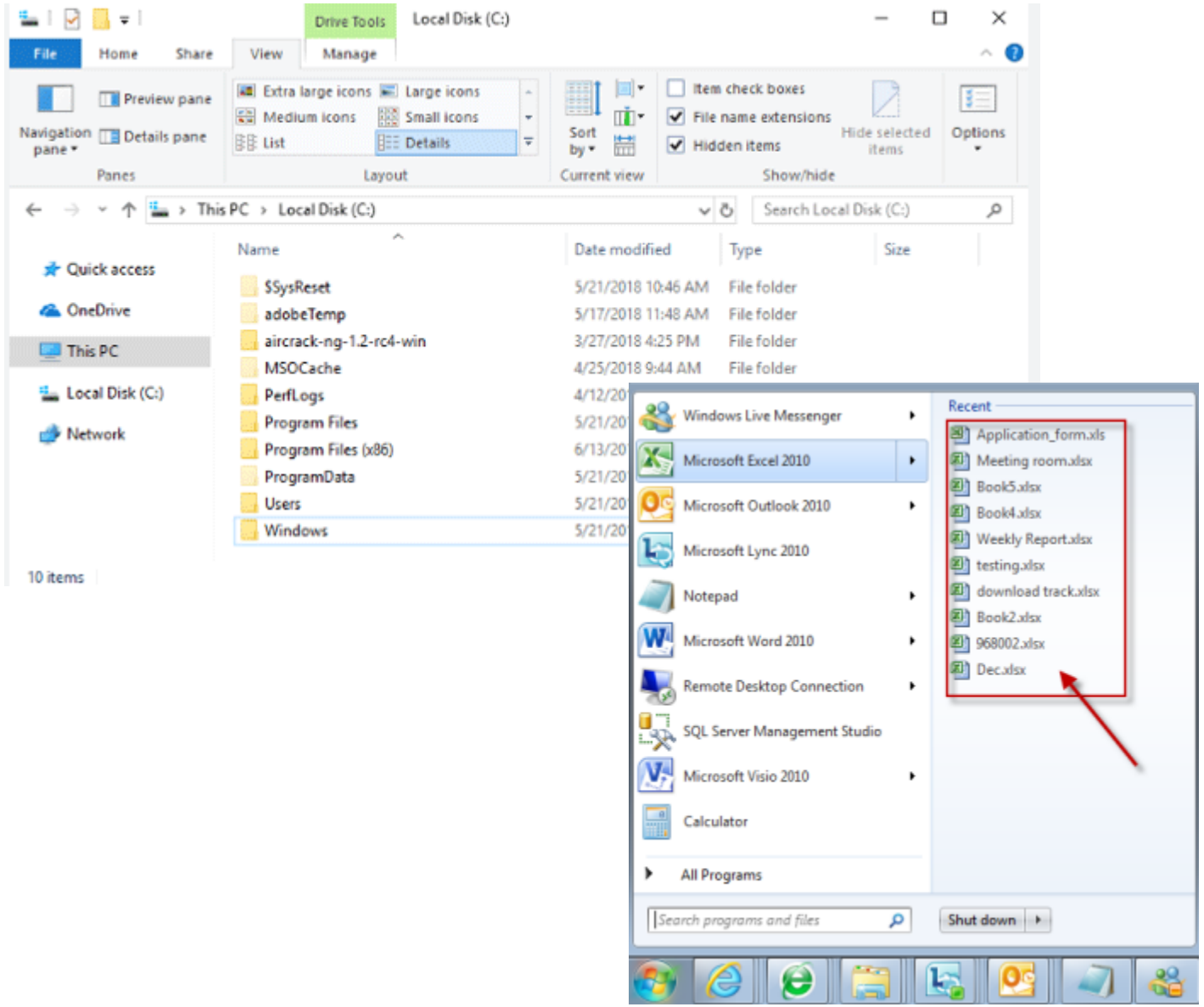
Partition Table
- Table that describes the logical segmentation and portioning of the physical disk

GPT (GUID global unique identifier **Partition Table)**
- Used in most modern (non-Windows) operating systems
- Typically used today unless there are hardware or other backwards-compatibility concerns.



Key Filesystems

- Documents/Desktop/Downloads
- Temporary files
- Browser temp / artifacts
- Browser downloads cache
- Email attachments
- Prefetch
- Windows registry
- Jump lists
- Common log directories



Temporary Files

Attackers will often stage out of temporary directories, can often find useful artifacts.

- C:\Windows\Temp
- C:\Users\<USERNAME>AppData\Local\Temp\
- %USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV*.dat
- %USERPROFILE%\AppData\Roaming\Mozilla\ Firefox\Profiles\<random text>.default\places.sqlite
  - Table:moz_annos
- %USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\History

Browser Downloads Cache

Downloads managers in modern browsers will track files downloaded from the Internet.

- Firefox
  - %userprofile%\AppData\Roaming\Mozilla\ Firefox\Profiles\<random text>.default\downloads.sqlite
- Chrome (also sqlite)
  - C:UsersUSER_NAMEAppDataLocalGoogleChromeUserDataDefaultHistory
  - C:UsersUSER_NAMEAppDataLocalGoogleChromeUserDataChromeDefaultDataHistory
- Edge
  - C:\Users\%USERNAME%\AppData\Local\Microsoft\Edge\User Data\Default

Email Attachments

Lots of malware comes from email attachments.

- %USERPROFILE%\AppData\Local\Microsoft\Outlook

Prefetch

"Increases performance"

- Limited number of files that get effectively pre-cached.
- Get the date / time file by the name and path it was first executed and last executed.
- C:\Windows\Prefetch

AMCACHE

- Application Experience Service Cache
- Win7+
- C:\Windows\AppCompat\Programs\Amcache.hve
- Entry for every application executed:
  - Full path information.
  - Last modification time.
  - SHA1 hash of the executable

Windows Registry

One of the ways we can get access to the registry is on disk. The registry is effectively its own filesystem and a forensically rich source of information.

- %SYSTEMROOT%\System32\config
- %USERPROFILE%\Ntuser.dat

Jump Lists

Related to recent items in the task bar.

- Data is stored in the AutomaticDestinations folder
- C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recnet\AutomaticDestinations

Logon Activity

Attempted and actual system logons.

- Data is stored in Windows Event Logs (winEVT)
- %SYSTEMROOT%\System32\winevt\logs\Security.evtx
  - EVT 4624 – successful logon
  - EVT 4625 – failed logon
  - EVT 4634|4647 – successful logoff
  - EVT 4684 – Runas Logon
  - EVT 4672 – Administrator logon
  - EVT 4720 – Account created

Environment Variables Shortcut

- %USERPROFILE%
  - C:\Users\<USERNAME>
- %TEMP%
  - C:\Users\<USERNAME>AppData\Local\Temp
- %SYSTEMROOT%
  - C:\Windows\
- %USERPROFILE%
  - C:\Users\<USERNAME>