# Certified Hacking Forensics Investigator

**Module #06 Windows Forensics**

**Eng. Mohammad Khreesha**
**Twitter: @banyrock**
**Facebook : http://www.fb.com/khreesha**

## Module Objectives

➔ **After Successfully completing this module, you will be able to :**

1. Understand how to collect and examine volatile and non-volatile data in Windows machines.
2. Perform windows memory and registry analysis.
3. Examine the cache, cookie, and history recorded in web browsers.
4. Examine Windows files and metadata.
5. Analyze text based logs and Windows even logs.

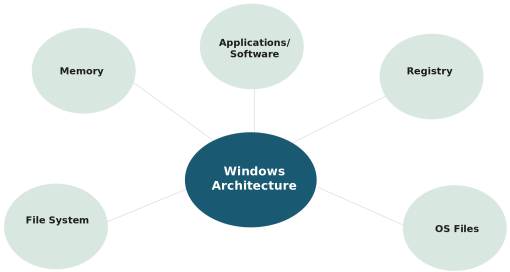
## Windows Forensics

➔ Windows is one of the most widely used OSs. Thus, the probability for an investigator to face it at the crime scene is very high.

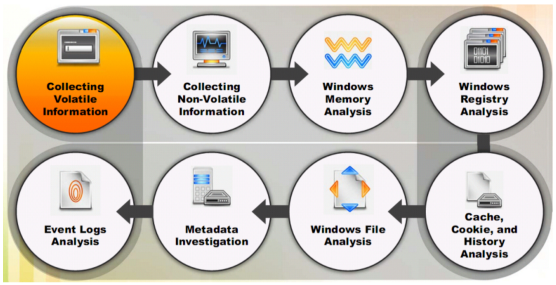
➔ Performing OS forensics to uncover the underlying evidence is slightly difficult task for an investigator as they were not specifically designed to be forensics friendly.

➔ To conduct a successful digital forensics examination in Windows, one should be familiar with it working, commands or methodologies, which meant to extract volatile and non-volatile data, Windows specific tools, ... etc.

## Windows Architecture




## Windows Forensics Methodology




## Collecting Volatile Information

- Volatile information can be easily modified or lost when the system is shut down or rebooted.
- Collection volatile information helps to determine a logical timeline of the security incident.
- Volatile data reside in registers, cache, and RAM.

**Volatile information includes:**

- System time
- Logged-on user(s)
- Network information
- Open files
- Network connections
- Network status
- Process information
- Process-to-port mapping
- Process memory
- Mapped drives
- Shares
- Clipboard contents
- Service/driver information
- Command history

## Collecting Non-Volatile Information

- Non-volatile data remain unchanged when a system is shut down or be unable to find power.
- Example: Emails, word documents, spreadsheets and various "deleted" files.
- Such data usually resides in HDD (swap files, slack space, unlocated drive space, ... etc).
- Other non-volatile data sources include DVDs, USB thumb drives, smartphone's memory, ... etc.


Follow us :
- https://www.fb.com/technawidotcom
- https://www.twitter.com/technawidotnet
- http://www.technawi.net