Tools :

x86 guide
https://www.begin.re/x86-overview

Windows 7 machine :
https://official-kmspico.com/windows-7-iso-files-version/

Remnux
https://remnux.org/

md5sum:
http://www.pc-tools.net/win32/md5sums/

dotpeek:
https://www.jetbrains.com/decompiler/download/#section=web-installer

peid:
https://www.softpedia.com/get/Programming/Packers-Crypters-Protectors/PEiD-updated.shtml
PEiD detects most common packers, cryptors and compilers for PE files and currently it can detect more than 600 different signatures in PE files. PEiD is special in some aspects when compared to other identifiers already out there!

exeinfope:
https://exeinfo-pe.en.uptodown.com/windows/download

detect it easy (die):
http://ntinfo.biz/index.html

bintext:
http://b2b-download.mcafee.com/products/tools/foundstone/bintext303.zip
Finds Ascii, Unicode and Resource strings in a file.
A small, very fast and powerful text extractor that will be of particular interest to programmers. It can extract text from any kind of file and includes the ability to find plain ASCII text, Unicode (double byte ANSI) text and Resource strings, providing useful information for each item in the optional "advanced" view mode. Its comprehensive filtering helps prevent unwanted text being listed. The gathered list can be searched and saved to a separate file as either a plain text file or in informative tabular format.

pestudio:
https://www.winitor.com/
The goal of pestudio is to spot suspicious artifacts within executable files in order to ease and accelerate Malware Initial Assessment and is used by Computer Emergency Response Teams and Labs worldwide.

cff explorer:
https://ntcore.com/?page_id=388

depdndancy walk:
https://www.dependencywalker.com/
Dependency Walker is a free utility that scans any 32-bit or 64-bit Windows module (exe, dll, ocx, sys, etc.) and builds a hierarchical tree diagram of all dependent modules. For each

module found, it lists all the functions that are exported by that module, and which of those functions are actually being called by other modules. Another view displays the minimum set of required files, along with detailed information about each file including a full path to the file, base address, version numbers, machine type, debug information, and more.

Dependency Walker is also very useful for troubleshooting system errors related to loading and executing modules. Dependency Walker detects many common application problems such as missing modules, invalid modules, import/export mismatches, circular dependency errors, mismatched machine types of modules, and module initialization failures.

resource hacker:
http://www.angusj.com/resourcehacker/#download
Resource Hacker is a tiny software application made to help you examine resources, such as .exe and .res files, extract them, replace icons and bitmaps, and more.
Although it's made for advanced PC users, the app contains intuitive options that can be figured out even by novices

upx:
https://upx.github.io/

regshot:
Regshot is an open-source (LGPL) registry compare utility that allows you to quickly take a snapshot of your registry and then compare it with a second one - done after doing system changes or installing a new software product.
https://sourceforge.net/projects/regshot/

process monitor (procmon):
https://docs.microsoft.com/en-us/sysinternals/downloads/procmon
Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity. It combines the features of two legacy Sysinternals utilities, *Filemon* and *Regmon*, and adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and much more. Its uniquely powerful features will make Process Monitor a core utility in your system troubleshooting and malware hunting toolkit.

process explorer:
https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer
Ever wondered which program has a particular file or directory open? Now you can find out. *Process Explorer* shows you information about which handles and DLLs processes have opened or loaded.

process hacker:
https://processhacker.sourceforge.io/downloads.php
A **free**, powerful, multi-purpose tool that helps you **monitor system resources**, **debug software** and **detect malware**.
Graphs and statistics allow you quickly to track down resource hogs and runaway processes.
Can't edit or delete a file? Discover which processes are using that file.
See what programs have active network connections, and close them if necessary.
See a hightly detailed overview of system activity with highlighting.
Get real-time information on disk access.
Get real-time information on disk usage.
View detailed stack traces with kernel-mode, WOW64 and .NET support.
Get real-time information on network usage.
Go beyond services.msc: create, edit and control services.
Get real-time information on gpu usage.

wireshark:
https://www.wireshark.org/#download

IDA pro:
https://www.hex-rays.com/products/ida/support/download_freeware/