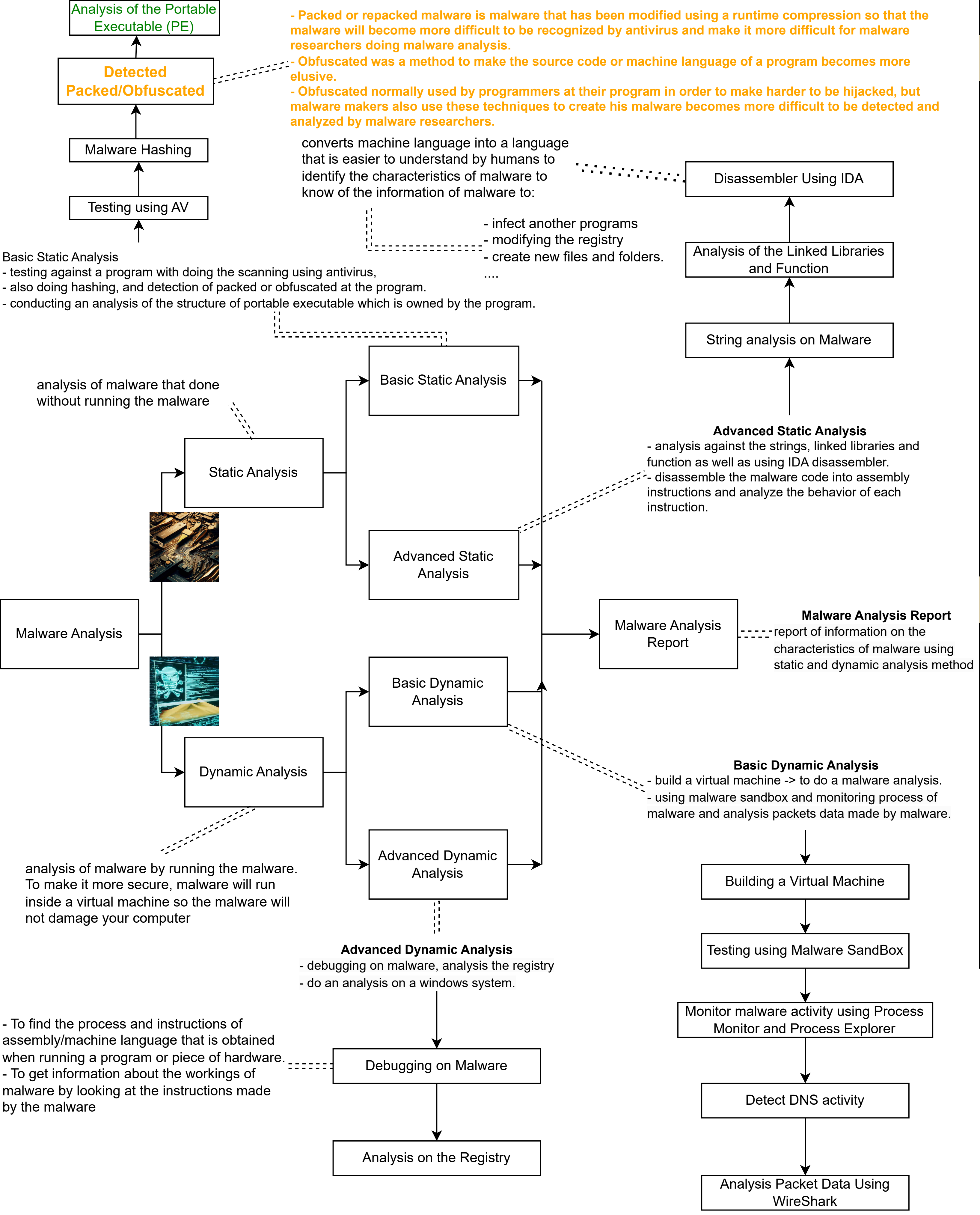

Malware Analysis

Static Analysis

analysis of malware that done without running the malware

Basic Static Analysis

Basic Static Analysis
- testing against a program with doing the scanning using antivirus,
- also doing hashing, and detection of packed or obfuscated at the program.
- conducting an analysis of the structure of portable executable which is owned by the program.

Testing using AV

Malware Hashing

Detected Packed/Obfuscated

- Packed or repacked malware is malware that has been modified using a runtime compression so that the malware will become more difficult to be recognized by antivirus and make it more difficult for malware researchers doing malware analysis.
- Obfuscated was a method to make the source code or machine language of a program becomes more elusive.
- Obfuscated normally used by programmers at their program in order to make harder to be hijacked, but malware makers also use these techniques to create his malware becomes more difficult to be detected and analyzed by malware researchers.

Analysis of the Portable Executable (PE)

Advanced Static Analysis

Advanced Static Analysis
- analysis against the strings, linked libraries and function as well as using IDA disassembler.
- disassemble the malware code into assembly instructions and analyze the behavior of each instruction.

String analysis on Malware

Analysis of the Linked Libraries and Function

Disassembler Using IDA

converts machine language into a language that is easier to understand by humans to identify the characteristics of malware to know of the information of malware to:

- infect another programs
- modifying the registry
- create new files and folders.
....

Dynamic Analysis

analysis of malware by running the malware. To make it more secure, malware will run inside a virtual machine so the malware will not damage your computer

Basic Dynamic Analysis

Basic Dynamic Analysis
- build a virtual machine -> to do a malware analysis.
- using malware sandbox and monitoring process of malware and analysis packets data made by malware.

Building a Virtual Machine

Testing using Malware SandBox

Monitor malware activity using Process Monitor and Process Explorer

Detect DNS activity

Analysis Packet Data Using WireShark

Advanced Dynamic Analysis

Advanced Dynamic Analysis
- debugging on malware, analysis the registry
- do an analysis on a windows system.

Debugging on Malware

- To find the process and instructions of assembly/machine language that is obtained when running a program or piece of hardware.
- To get information about the workings of malware by looking at the instructions made by the malware

Analysis on the Registry

Malware Analysis Report

Malware Analysis Report
report of information on the characteristics of malware using static and dynamic analysis method

Brief overview of basic static tools

Basic static analysis tools	Description
Virustotal.com	Virustotal is a website that provides a malware check against program
Md5deep	md5deep is a set of programs to compute MD5, SHA-1, SHA-256 on an arbitrary number of files.
PEiD	Tools for detecting packed/obfuscated techniques.
Exeinfo PE	Tools for detecting packed/obfuscated techniques.
RDG Packer	Tools for detecting packed/obfuscated techniques.
D4dot	Tools to remove obfuscated .Net Reactor technique.
PEview	- To display the structure and content of the Protable Executable.
CFF Explorer	view and modify the resources of a PE file, you can view the functions that the DLL file can call, and modify the function entry address to achieve the purpose of creating a crash screen

Brief overview of advanced static tools

Advanced static analysis tools	Description
BinText	program - searching and display character strings from a binary file.
Dependency Walker	program - performs the scanning modules on 32 bit or 64 bit programs.
IDA	The Interactive Disassembler (IDA) is a disassembler program.

Brief overview of basic dynamic tools

Basic dynamic analysis tools	Description
Virtualbox	- virtual machine that is used as a place to run the malware.
Anubis	- malware sandbox created specifically for automatic malware analysis.
Comodo Instant Malware Analysis	malware sandbox created specifically for automatic malware analysis
Process Monitor	monitors and displays all activities within the system in real-time.
Process Explorer	monitors the processes that are currently in the system path of the computer.
ApateDNS	find out the IP address which is contacted by the malware
Wireshark	take the data contained in the packet network for analysis malware

Brief overview of advanced dynamic tools

Advanced dynamic analysis tools	Description
OllyDbg	tools used to perform debugging/reverse engineering to malware.
Regshot	- To help analyze the registry. - Toidentify changes which create by malware on registry with compare state of registry before and after malware executed