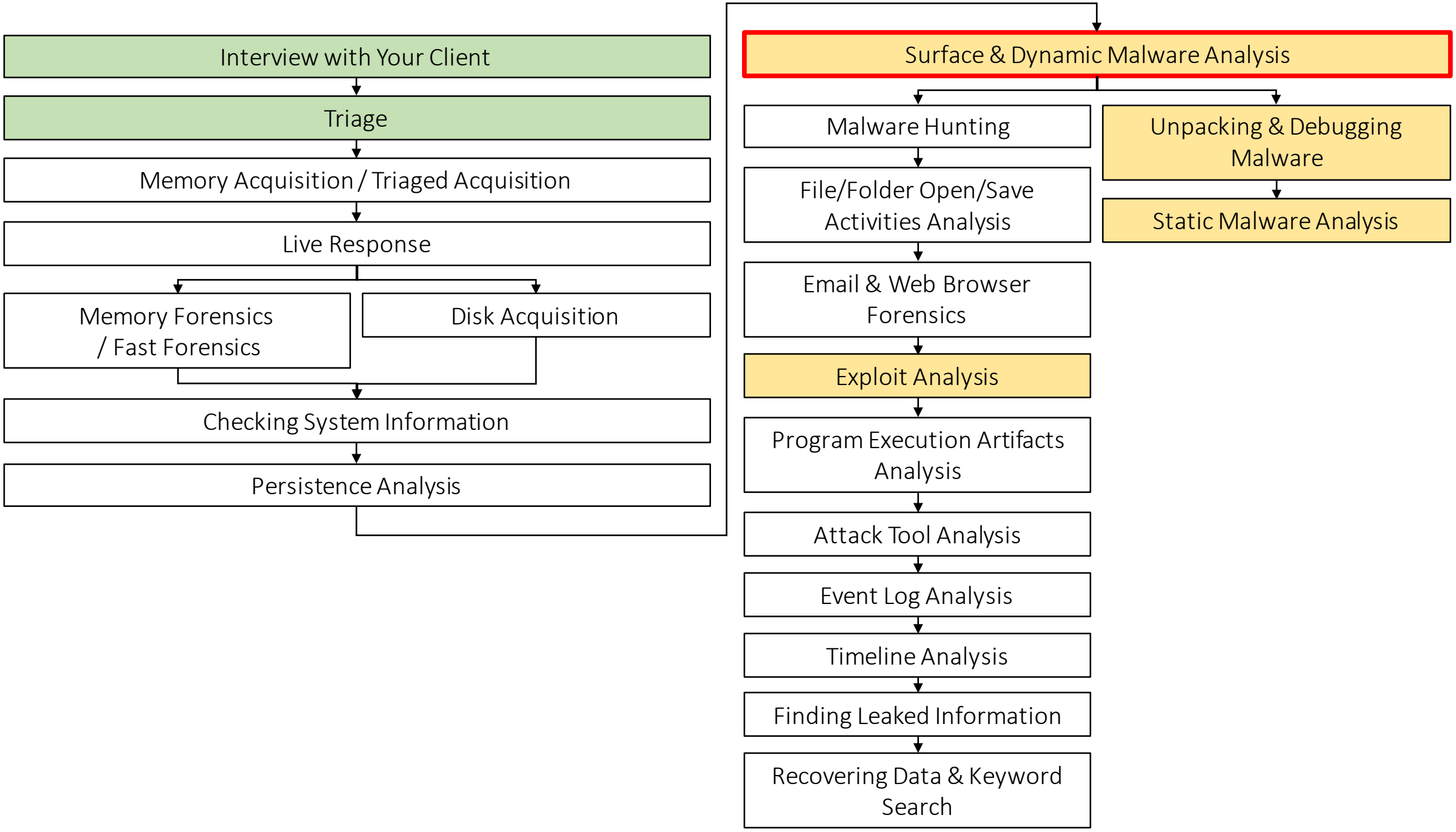
Malware Analysis


Interview with Your Client
Triage
Memory Acquisition / Triaged Acquisition
Live Response
Memory Forensics / Fast Forensics
Disk Acquisition
Checking System Information
Persistence Analysis
Surface & Dynamic Malware Analysis
Malware Hunting
File/Folder Open/Save Activities Analysis
Email & Web Browser Forensics
Exploit Analysis
Program Execution Artifacts Analysis
Attack Tool Analysis
Event Log Analysis
Timeline Analysis
Finding Leaked Information
Recovering Data & Keyword Search
Unpacking & Debugging Malware
Static Malware Analysis

What is Malware Analysis?

- It is a method to reveal malware's behavior combining with the methods below.
  - Surface Analysis
  - Dynamic Analysis (Runtime analysis, Black box analysis)
  - Static Analysis (White box analysis, Reverse (Code) Engineering, Reversing…)
    - Terms and definitions are not fixed.
      - Sometimes, surface analysis is included in static analysis.
    - There is "public source analysis" as well (in other words, googling ;-)).

What is Surface Analysis?

What is Surface Analysis?

- Surface analysis is a set of simple analysis to get information from malware quickly by methods such as:
  - Checking its file size
  - Getting its file hash (such as MD5, SHA-1, SHA-256 and ssdeep)
  - Acquiring its file type (file command)
  - Looking for its readable characters (strings command)
  - Investigating DLLs and APIs that the malware loads
  - Looking into its compiler or its packer
  - Retrieving its compilation date
  - Examining it with antivirus software
  - Finding out any resources
  - …
- They help us to find out malware, which was used in past incidents, or which have already been disclosed publicly.

What

- virustotal

SHA256:	df1f547cdc627d1651bcf52baa74f30455f94a2ae1d76e900eb3c8b84bb99383
File name:	ac1df5c542dd4f4dd91cae217ba4db1e0292b2ca
Detection ratio:	19 / 47
Analysis date:	2013-09-24 03:54:49 UTC (7 months, 3 weeks ago)

Analysis | File detail | Additional information | Comments 0 | Votes | Behavioural information

The file being studied is a Portable Executable file! More specifically, it is a Win32 EXE file for the Windows GUI subsystem.

PE header basic information

Target machine	Intel 386 or later processors and compatible processors
Compilation timestamp	2012-06-09 13:19:49
Link date	2:19 PM 6/9/2012
Entry Point	0x0000AC87
Number of sections	5

PE sections

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
.text	4096	74526	74752	6.56	a8692f5ba740240ef0f9a827376f76f9
.rdata	81920	7445	7680	4.99	d4f36accffde0bf520f52486679ccf0d
.data	90112	96036	512	3.55	b6c7edb5b7fec47a37a622cc5d71f3f4

What is Dynamic Analysis?

What is Dynamic Analysis?

- It is a method to find out malware's behavior by executing malware and recording malware activities with analysis tools on typically a closed environment (e.g. virtual machine).

- We need to record:
  - Process Activities
  - Registry Activities
  - File Activities
  - Network Activities (with Internet emulation)
    - Internet emulation is to redirect communications from malware to Internet emulation software to record host names and/or IP addresses of C2 servers and their communication contents.

What is Dynamic Analysis?

What is Dynamic Analysis?

- To perform dynamic analysis manually, these tools may be helpful.
  - Virtual Machine environments
    - VMware
    - VirtualBox
    - Hyper-V
    - …
  - Process activities
    - Process Explorer
    - Process Hacker
    - Process Monitor
      - noriben
    - Sysmon
- Registry activities
  - Process Monitor
  - regshot
- File activities
  - Process Monitor
  - regshot
- Internet Emulation
  - Fakenet, fakenet-ng
  - InetSim
- Network activities, packet capture
  - fakenet , fakenet-ng
  - wireshark

What is Static Analysis?

What is Static Analysis?

- To read the code of Malware by disassembling it.

Why malware analysis is needed in incident response?

- It is because malware is used in most of the targeted attacks.
- We investigate information that is useful for performing incident responses, such as:
  - Hosts and URLs , which are useful for malware hunting.
  - Activities such as writing to registry or files, which are useful for computer forensics.
  - Malware's internal features or strings such as Mutex and notable readable strings, which are useful for finding extra infected machines with EDR.
- It's not for research purpose.
  - We will not analyze the entire code of malware.
    - We do not have enough time. We need to deal with incidents in a limited time.