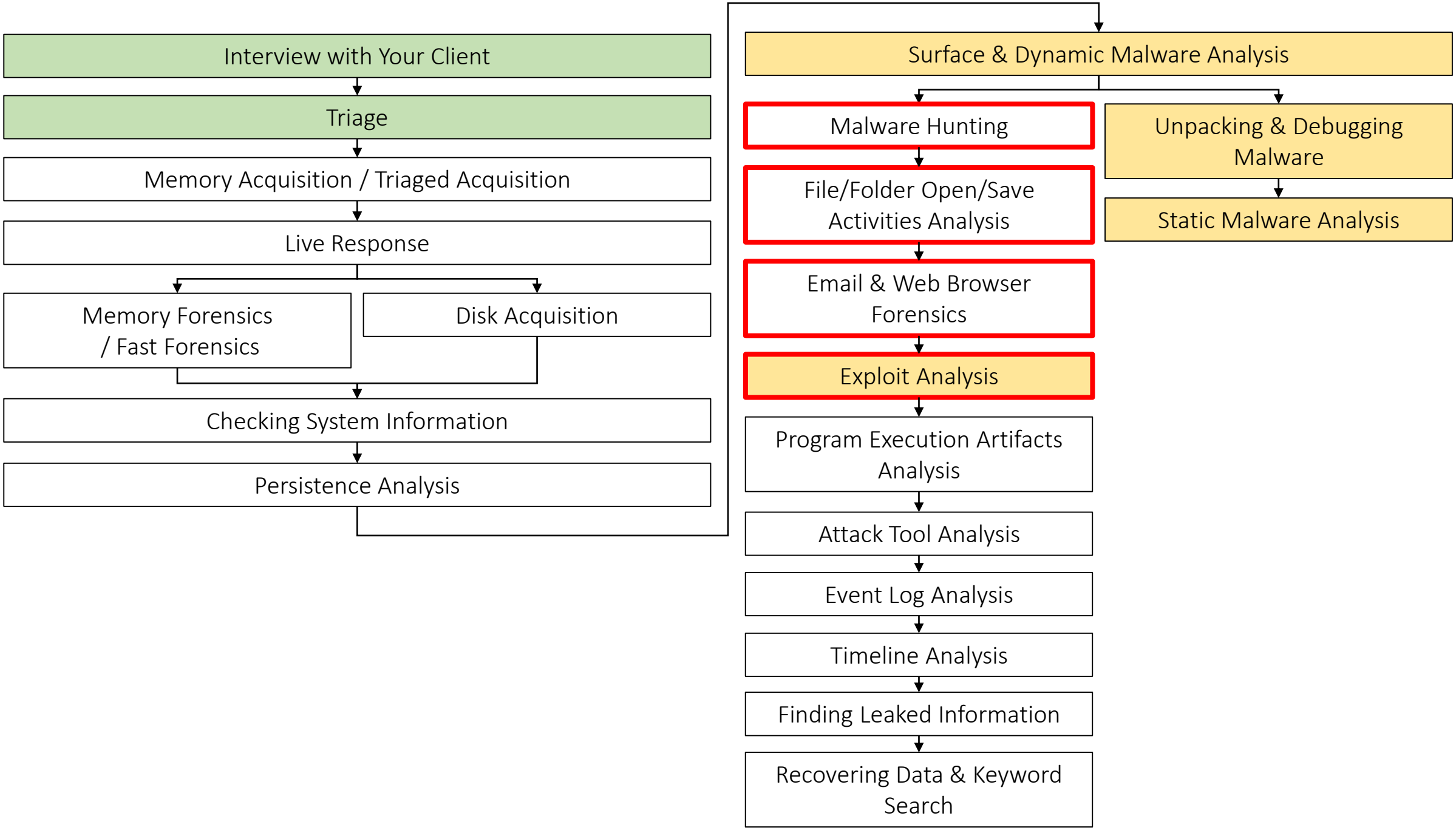
Root Cause Analysis

What Root Cause Analysis is

- Root cause analysis is the analysis aimed to determine the cause of the initial infection in the incident by running through several analysis methods.
- It is necessary for preventing reoccurrence.

Items for Root Cause Analysis

- Malware Hunting
  - In order to determine the hosts infected with malware, we often perform network forensics such as proxy log analysis with some network related IOCs.
- File/Folder Open/Save Analysis
  - The initial infection process is often related to user activities such as opening or executing something. Thus, we should perform this kind of analysis.
- E-mail Forensics
  - Email or its attachment are frequently used as the initial infection method in targeted attacks. It is necessary to confirm emails that were received by the victim user account.
- Web Browser Forensics
  - Web browsing vectors are also used in targeted attacks. It is useful not only for confirming the infection process, but also for determining post exploitation activities.
- Exploit Analysis
  - After finding out the initial infection process, we have to determine the exploit that the attacker used. It is necessary for preventing reoccurrence.


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