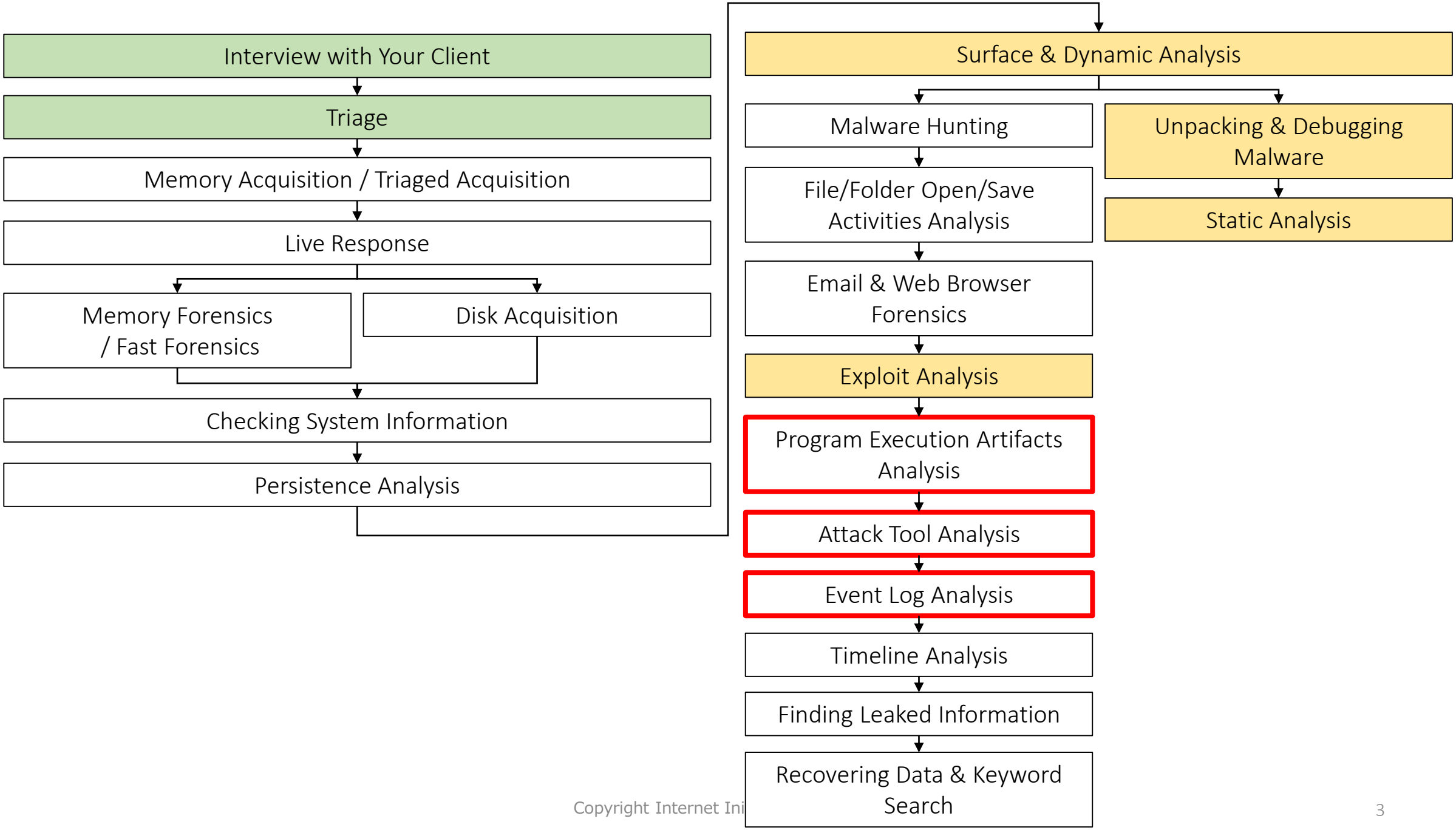
Lateral Movements Investigation

Lateral Movements Investigation

- What is the lateral movements investigation?
  - Up until this point, we have found the initial infection vector.
  - Now, it is necessary to build a whole picture of the incident.
  - From here, we will trace post exploitation activities and reveal the tools used, where the attackers penetrated and their goal.
  - In this chapter, we will investigate various artifacts such as registry, prefetch, and event logs for tracing lateral movements from the initial infected host to others.
- What topics will we learn in this section?
  - Program Execution Artifacts Analysis
  - Event Log Analysis
  - Attack Tools Analysis

Copyright Internet Initiative Japan Inc.



Copyright Internet Ini