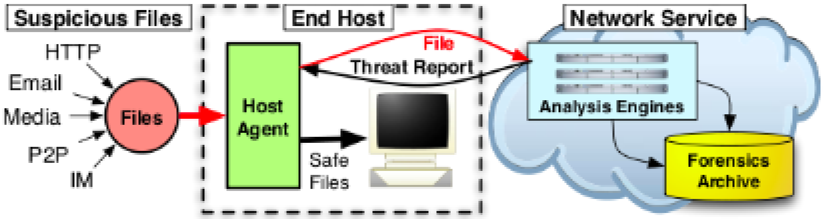
"By submitting this homework, I attest that the homework is my own work and I have not copied any text verbatim from any online or offline source, or from other students (past or present). I also attest that I have not used any paraphrasing tool or any homework solution websites. In addition, I attest that any information taken from course slides and handouts or any websites is properly attributed and referenced. I understand that any violation of the UAB Academic Integrity Code for any portion of the homework will result in a zero score for the entire homework and will be reported to the academic integrity coordinator per university policy."

1. The N-version approach itself means multiple programs or scanners scanning for any malware/virus or attack, meaning better results than a single one by itself. The cloud itself improves detection, forensic capabilities, retrospective detection, deployability, and management.



   - Lightweight host agent run on end hosts.
   - A network service that receives files from hosts and identifies malicious content.
   - An archival and forensics service that stores information about analyzed files and provides a management interface for operators.

2. The unique nature of clouds disrupts the traditional forensics mechanisms and render established digital forensics tools ineffective in trustworthy forensics in clouds. The key goals of cloud forensics is identifying data related to a particular user, attributing data to its creator/owner, and identifying intrusions/reconstructing events. First thing that would need to be done is pinpointing the physical location of data and hosts in a cloud. Then, unearth the root cause of the problems (Who created them, who stored/sent them, who has access to them). Finally, handling the evidence/data where it can’t be stolen or changed and done within forensic protocol.