Instructions

These diagram is to show the potential for Forensic capabilities. For forensics, where appropriate, seizure of physical hardware should occur. The term forensics is also very broad, review of Application or system logs is still considered forensics in the Broadest sense of the term.

Forensics in general.

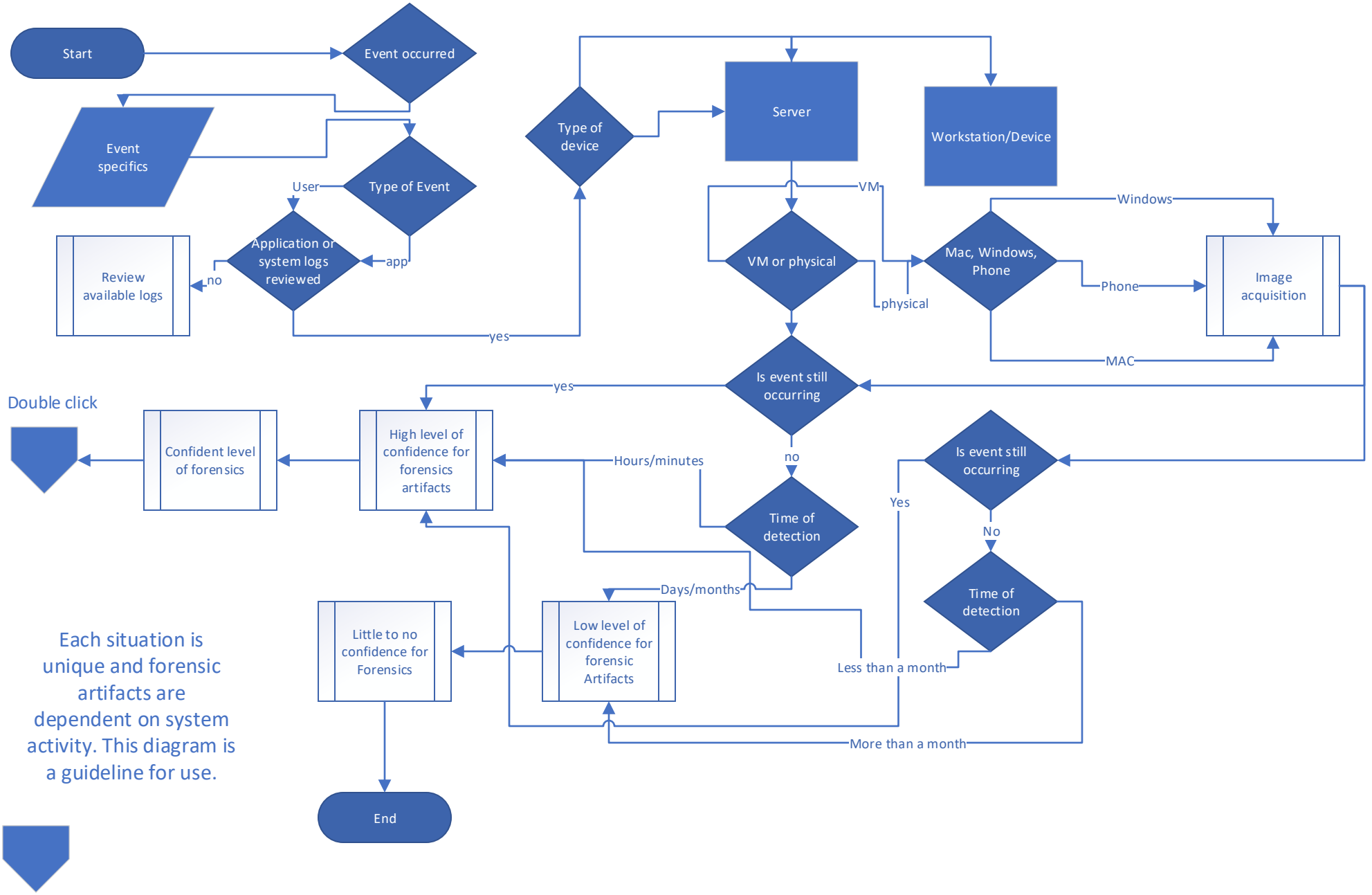
The process of forensics is extremely time consuming. It is important to identify if the goal attempted is reachable.
Two of the main goals are:
Tie an action to a user
Or
Tie a user to an action.
First decide if forensics will return viable data. If possible a off page connector will take you to the forensics process.

System Differential.

All devices contain some forensic data also known as “Forensic Artifacts”. The difference between retrieval of those artifacts are what needs to be considered. for instance, a windows Server holds the same artifacts as a Windows workstation. The passage of time, access methods, and configuration will determine whether the artifacts are viable. To take this one step further. A server drive slack space, may be written 1000's of times a day. Compared to a workstation’s slack space, probably gets written very infrequently. Therefore deleted files on a Server are less likely to be recovered compared to a workstation.

Start by double clicki off page connector below.

Decide if Forensics is Viable



Forensics Process