Below is a table containing various literature, the specific citation in question and why is it picked.

|  |  |  |
| --- | --- | --- |
| Source | Citation | Explanation |
| Towards Enhanced Threat Detection: Leveraging Honeypots, Machine. Learning, and Malware Analysis Sunil Selvaraj  (SUPERVISOR THESIS) | Chapter 2.4 Malware Analysis: “Dynamic and static analysis are the two primary techniques for analysing malware (Mohamed and Ngah, Syahrulanuar Bin, 2020).” & “Dynamic analysis aims to identify malicious activity occurring within the executable while it is operating, all while maintaining the security of the analysis platform (OrMeir et al., 2019).”  *“When it comes to honeypots, studying attacks based on the data collected by the honeypot results in fully utilising its capability.”* | Ties to my project theme regarding malware propagation. Dynamic analysis within a sandbox aligns with idea of my sandboxing – studying whether malware can spread *outside* its contained environment. Supports my research question  Mentions the tool (ELK) I will use for collecting data (pcaps) within a sandboxed environment. Further influences and supports both my research question and methodology |
| [A Survey of Honeypots and Honeynets for Internet of Things, Industrial Internet of Things, and Cyber-Physical Systems | IEEE Journals & Magazine | IEEE Xplore](https://ieeexplore.ieee.org/document/9520645) | C. Level of Interaction: However, one has to be extremely careful when deploying a high interaction honeypot especially in IIoT…  “Virtual resources have been widely used in IoT honeypot/honeynet environments … However … one does not see any study which considers [attacker] techniques to detect the virtual environment in medium/high interaction decoy systems.” | Motivation as to explaining why honeypots (regarding IoT IP Devices) should be contained, as the high-interaction honeypot is within a Docker and FireJail Container  Supports project need to not only measure propagation, but fidelity (whether sandboxing changes attacker behaviour) |
|  |  |  |
|  |  |  |