In [ ]:

```
Training Day 21 Report– 13 July 2025
 Introduction
 Day 21 introduced safe and ethical malware analysis methodologies: static and
 analysis principles and sandboxing.
 Key Concepts Discussed
 We examined metadata analysis, signature-based detection limitations, and the
 behavioral analysis to understand unknown samples.
 Lab Preparation in Theory
 The class discussed building isolated analysis environments with strict netwo
 and telemetry capture to analyze the behavior of suspicious samples safely.
 Practical Understanding (Theory)
 The trainer explained how to derive indicators of compromise (IoCs) from samp
 to document behaviors, and how to feed findings back into defensive controls.
 Key Takeaways
 Safe analysis yields actionable IoCs that improve detection and response acro
ronment.
 Conclusion
 We will proceed to ransomware threat models and incident response considerati
```