Introduction

Batnet Laboratories Inc. is a successful and expanding company working on military related projects. Suspicions DNS traffic with heavy load was recognized recently. Therefore, a network administrator sent you a PCAP dump of the network traffic and mentioned that the suspicious DNS behavior was recorded on July 12, 2021 around 7:27 PM.
Goals and Tasks

Analyze the given network traffic and answer to the following questions in a written report:

- Which kind of attack was detected in the network traffic dump?
- Based on what characteristics the attack can be detected?
- What is the exact starting point (packet number) of the attack?
- What operating system (not version) and source IP the attack was originating from?
- What was the motivation for the attack and which goal most likely was to be achieved?

Submission

Submit a written report as PDF document with your answers. Make sure that your answers can be clearly assigned to the question numbers in the goal and task section.