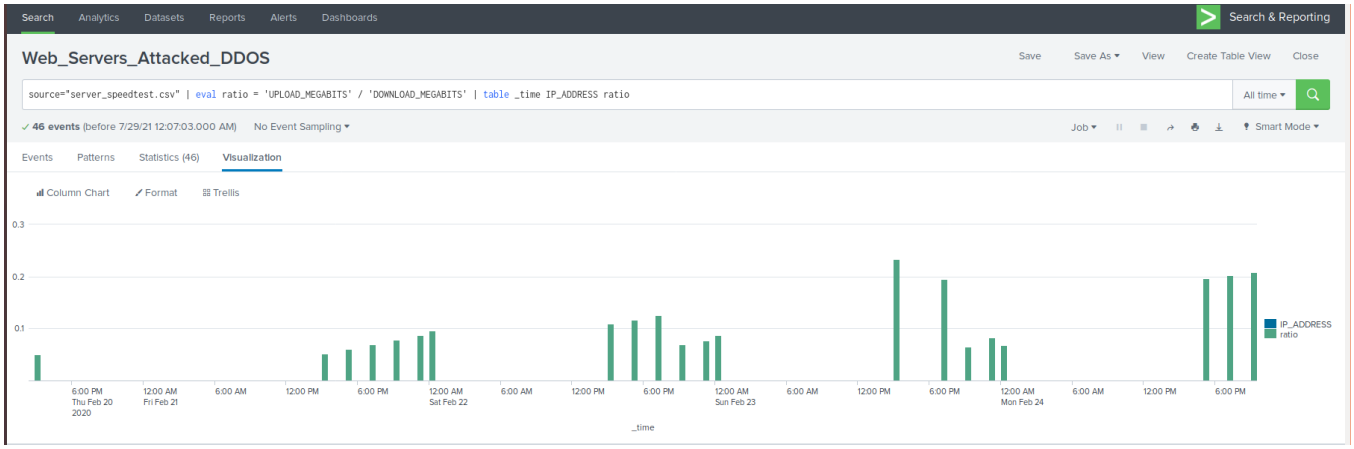
WEEK 18: Homework Lets Go Splunking

Step 1: DDOS Attack

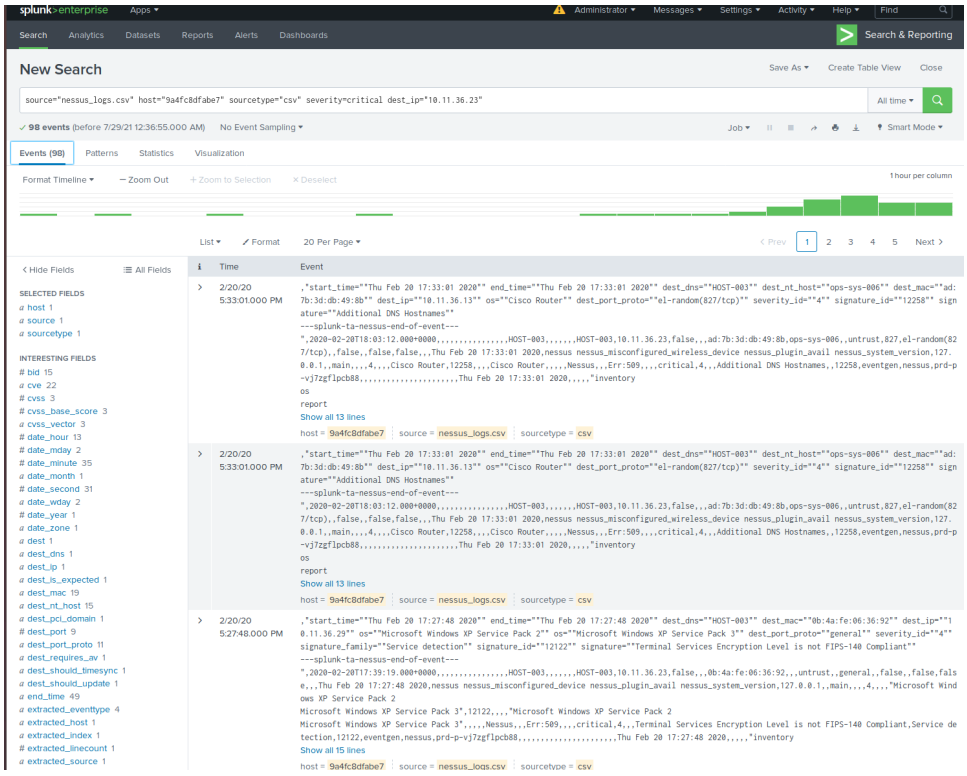
Based on the report created, what is the approximate date and time of the attack?

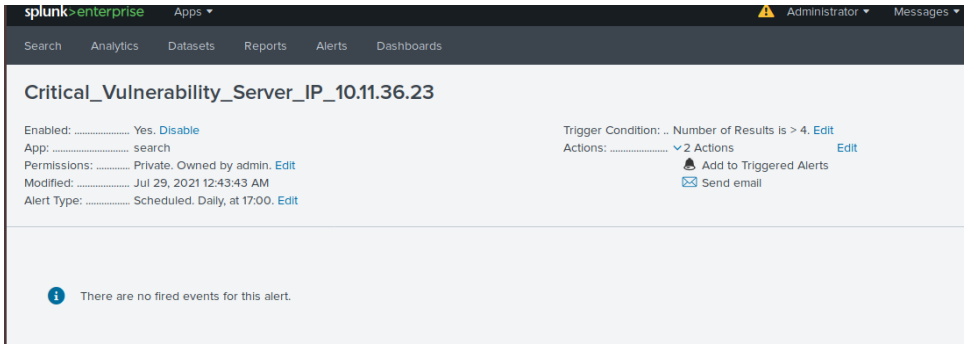
02-23-2020 at 2:30pm

How long did it take your systems to recover? Full recovery after 9 hours



Step 2: Creating Critical Vulnerability Alert

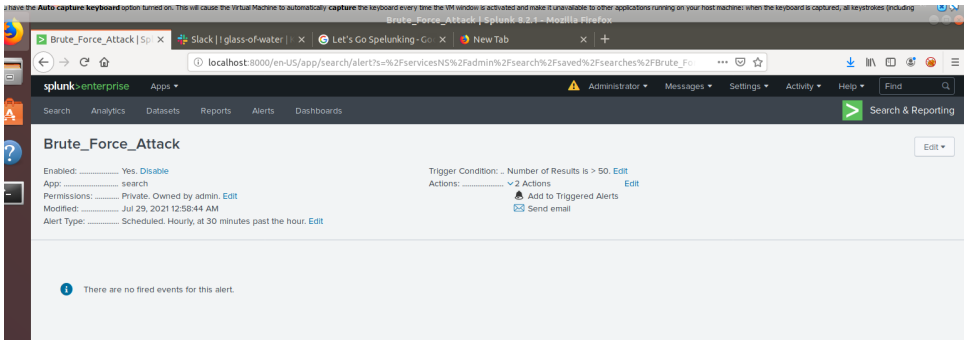


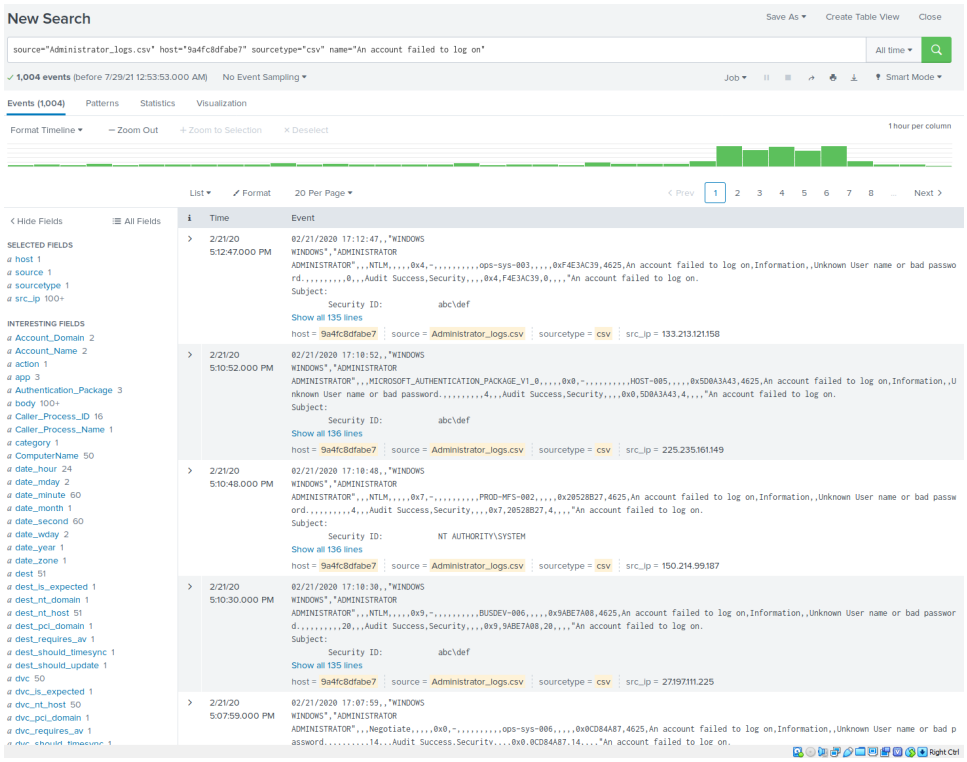


Step 3: Brute Force, Failed Login Attempts Alert

Baseline is 10 Failed Logins

Brute Force trigger is 50+





Reports created: