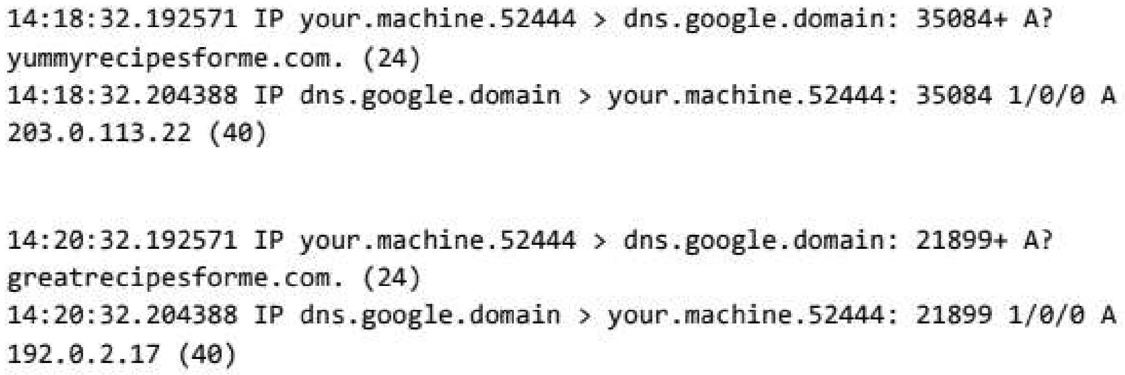
03. Brute Force Attack and Solutions



```
14:18:32.192571 IP your.machine.52444 > dns.google.domain: 35084+ A?
yummyrecipesforme.com. (24)
14:18:32.204388 IP dns.google.domain > your.machine.52444: 35084 1/0/0 A
203.0.113.22 (40)


14:20:32.192571 IP your.machine.52444 > dns.google.domain: 21899+ A?
greatrecipesforme.com. (24)
14:20:32.204388 IP dns.google.domain > your.machine.52444: 21899 1/0/0 A
192.0.2.17 (40)
```

Section 1: Identify the network protocol involved in the incident
It is the HTTP Protocol. The issue that is faced is happening when trying to connect to the company’s website

Section 2: Document the incident
Some users reported that they faced a problem while trying to connect to the company’s website yummyrecipesforme.com. They reported that while trying to connect, they would get redirected to some other website (greatrecipesforme.com) which is completely different. After they are redirected, their computers started downloading a file and ever since then, their computers slowed down and they lost access to their accounts. Cybersecurity analysts used tcpdump to troubleshoot. Soon, it was found that the attackers changed the code of the update download and placed a harmful malware instead of it. Also attackers changed the password of the users to gain full control of their accounts.

Section 3: Recommend one remediation for brute force attacks
The best way to stop brute force attacks from being a problem is using MFA (Multi Factor Authentication). Also it must be mandatory for the users to constantly change their passwords every 6 months. Using one password for a long time is going to help hackers to either guess or steal someone’s password in the company to gain access.