Problem Description:

You are tasked with monitoring email communication to detect suspicious content. The first script will simulate sending an email, and the second script will simulate receiving and processing the email. The emails are stored in a file called `email.log`, which you will **keep monitoring** for new emails. If the email is from a suspicious source (e.g., an "enemy"), the second script should trigger an alert showing the sender's name. The first script is provided for you, and you need to write the second script. **You will trigger the alert if the sender is from `enemy@**.**`.**

Write a script that:

- Monitors the `email.log` file for new emails indefinitely (see the hint below).
- Checks if the sender is from `enemy@**.**`. If this condition is met, the script should trigger an alert and display the sender's name and the email content.
- The script should keep running until the user stops it with `Ctrl+C`.
- Do not modify the first script. If the email.log file does not exist, your script should create it.

Example usage for the first script:
`./send_email.sh <receiver> <sender> <message>`
For example:
`./send_email.sh agent@example.com "enemy@example.com" "This is a secret mission"`

The script you write will keep running till you press `Ctrl+C`, and the first script will be used to send emails.

Sample Output

If the email is from an enemy, the script should display an alert with the email content like this:

```
ALERT: Email received from enemy@example.com
Timestamp: 2024-09-17 20:03:38
From: enemy@example.com
To: alice@example.com
Body: Let's kidnap Mosfet and hold him for ransom.
---
```

Hint: `tail -F email.log` will keep the script running and monitor the file for new emails. To monitor the file from your bash script, you can pipe the output of this command to a `while` loop and read line by line. The end of each email is marked by a line containing `---`.