SIEM Homework Assignment

Using Splunk:

source="buttercupgames_email_log.csv" host="email_logs" Sender="*@buttercupgames.com" incoming_address!="10.0.0.0/8" incoming_address="74.207.253.34" | stats earliest(_time) latest(_time) by incoming_address | convert timeformat=" %m/%d/%y %H:%M:%S" ctime(earliest(_time)) AS earliest_time ctime(latest(_time)) as latest_time

Things to Capture About the Incident:

*1. What **incoming IP address** was used in the attack?*

74.207.253.34

*2.Who was the **Sender** in the Phishing attack?*

address34@buttercupgames.com

***3.** Who was the **Recipient** of the attack?*

address15@ buttercupgames.com
address37@buttercupgames.com

*4.What was the **Subject** of the email?*

Phishing Subject 19

*5.What is the **Time** of the event?*

2/1/17 4:29:19.000 AM

6.*Where there any **Attachments**?*

Yes, Email Data was an attachment.