# ECE 40400: Introduction to Computer Security

# Spring 2024

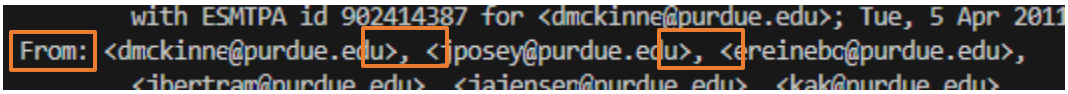
Prateek Yashwant Jannu

Purdue University, West Lafayette

Professor: Dr. Avinash C Kak

# Recipe_1

**Let's take a look at the JunkMail Files:**




All of the files have multiple FROM entries, one of the easiest methods is to check for **multiple purdue.edu** but then what if the email consists of other domains, this would not work hence we check for the **parenthesis following the email highlighted above which when matched we know for sure that there are multiple entries in the FROM header.**

**^From.*>\, \<**

^: Means the pattern to the beginning of a line.

From: Matches the literal characters "From".

.*: Matches any character except newline zero or more times. This allows for flexibility in matching any sequence of characters after "From".

>\, \<: Matches the characters **>, <** exactly. The backslashes \ are used to escape the special characters > and <.

# Recipe_2

This recipe is to examine the subject lines of incoming email messages. If any subject line contains any of the specified keywords the email is processed to file recipe_2.

*****
**^Subject.*(degree|watches|medications|diploma|Diploma|pills|Pills|plills|Ppjills|Magento):**

*: Indicates the beginning of a condition.
^Subject.*: Matches lines in the email's subject header that start with "Subject" followed by any number of characters
(degree|watches|medications|diploma|Diploma|pills|Pills|plills|Ppjills|Magento): It matches any of the listed keywords in the subject line.

# Recipe_3

**:0 B:**
**^*(Ruby|ruby|GEMSTONE|MINING)**

B: This flag specifies that the condition line type is based on the body of the email.

^*: This part indicates that the condition should be checked against the body of the email message, for any number of characters until the condition is met.
(Ruby|ruby| GEMSTONE|MINING): These are the casino/gambling and mining companies we are trying to avoid.

# Recipe_4

**:0 HB:**
*** ^Content-Type: multipart/alternative**
*** ^Content-Type: text/html;( charset = "utf-8"| charset=utf-8|$)**
*** ^Content-Type: text/plain;( charset = "utf-8"| charset=utf-8|$)**
*** ^Content-Transfer-Encoding: (7bit|8bit|quoted-printable)**

HB: Flags indicating that the condition line type is based on the body of the email.

* ^Content-Type: multipart/alternative: Checks if the MIME header "Content-Type" specifies that the email contains a multipart message with alternative This condition targets emails that have the "multipart/alternative" MIME type, which typically includes both plain text and HTML versions of the email content.

* ^Content-Type: text/html;( charset = "utf-8"| charset=utf-8|$): Checks if the MIME header "Content-Type" specifies that the email contains an HTML version with a specified character set of UTF-8. This condition targets emails that have a "text/html" MIME type with a charset of UTF-8.

* ^Content-Type: text/plain;( charset = "utf-8"| charset=utf-8|$): Checks if the MIME header "Content-Type" specifies that the email contains a plain text version with a specified character set of UTF-8. This condition targets emails that have a "text/plain" MIME type with a charset of UTF-8.

* ^ Content-Transfer-Encoding: (7bit|8bit|quoted-printable): Checks if the MIME header "Content-Transfer-Encoding" specifies that the email content is encoded using one of the specified methods (quoted-printable, 8bit, or 7bit). This condition targets emails that have a specified Content-Transfer-Encoding method.