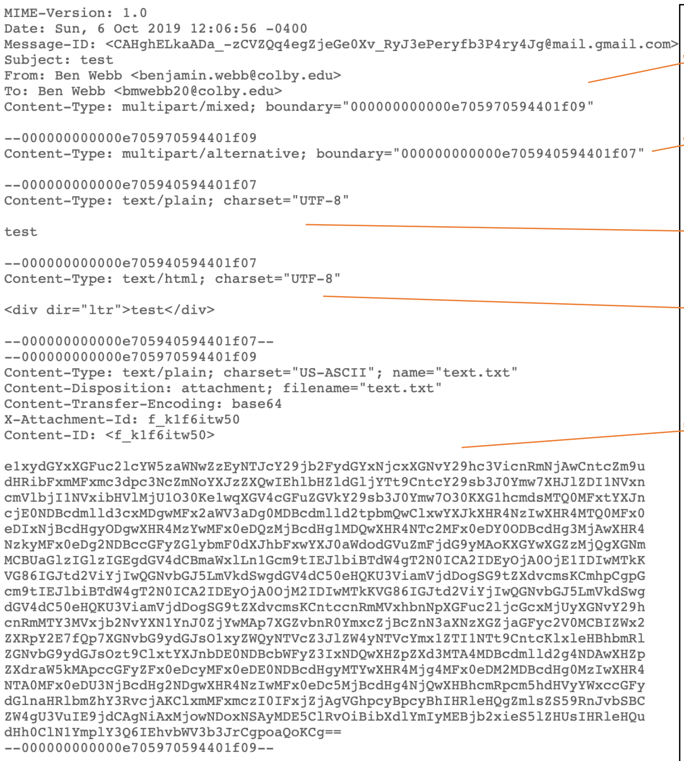
CS331 Project 2 Problems – Ben Webb

1) I used the command `whois colby.edu` because that is Colby's homepage. I also repeated the command but with the IP of Colby.edu (`whois 137.146.24.72`)
   a. The domain name is Colby.edu. This is reported in whois colby.edu.
   b. The nameservers are NS1.P28.DYNECT.NET, NS2.P28.DYNECT.NET, NS3.P28.DYNECT.NET, and NS4.P28.DYNECT.NET. This is reported in whois Colby.edu.
   c. The IP range is 137.146.0.0 - 137.146.255.255. This is reported in whois 137.146.24.72.
   d. The prefix is 16. This is reported in whois 136.146.24.72

2)



```
MIME-Version: 1.0
Date: Sun, 6 Oct 2019 12:06:56 -0400
Message-ID: <CAHghELkaADa_-zCVZQq4egZjeGe0Xv_RyJ3ePeryfb3P4ry4Jg@mail.gmail.com>
Subject: test
From: Ben Webb <benjamin.webb@colby.edu>
To: Ben Webb <bmwebb20@colby.edu>
Content-Type: multipart/mixed; boundary="000000000000e705970594401f09"

--000000000000e705970594401f09
Content-Type: multipart/alternative; boundary="000000000000e705940594401f07"

--000000000000e705940594401f07
Content-Type: text/plain; charset="UTF-8"

test

--000000000000e705940594401f07
Content-Type: text/html; charset="UTF-8"

<div dir="ltr">test</div>

--000000000000e705940594401f07--
--000000000000e705970594401f09
Content-Type: text/plain; charset="US-ASCII"; name="text.txt"
Content-Disposition: attachment; filename="text.txt"
Content-Transfer-Encoding: base64
X-Attachment-Id: f_k1f6itw50
Content-ID: <f_k1f6itw50>

e1xydGYxXGFuc2lcYW5zaWNwZzEyNTJcY29jb2FydGYxNjcxXGNvY29hc3VicnRmNjAwCntcZm9u
dHRibFxmMFxmc3dpc3NcZmNoYXJzZXQwIEhlbHZldGljYTt9CntcY29sb3J0Ymw7XHJlZDI1NVxn
cmVlbjI1NVxibHVlMjU1O30Ke1wqXGV4cGFuZGVkY29sb3J0Ymw7O30KXG1hcmdsMTQ0MFxtYXJn
cjE0NDBcdmlld3cxMDgwMFx2aWV3aDg0MDBcdmlld2tpbmQwClxwYXJkXHR4NzIwXHR4MTQ0MFx0
eDIxNjBcdHgyODgwXHR4MzYwMFx0eDQzMjBcdHg1MDQwXHR4NTc2MFx0eDY0ODBcdHg3MjAwXHR4
NzkyMFx0eDg2NDBccGFyZGlybmF0dXJhbFxwYXJ0aWdodGVuZmFjdG9yMAoKXGYwXGZzMjQgXGNm
MCBUaGlzIGlzIGEgdGV4dCBmaWxlLn1Gcm9tIEJlbiBTdW4gT2N0ICA2IDEyOjA0OjE1IDIwMTkK
VG86IGJtd2ViYjIwQGNvbGJ5LmVkdSwgdGV4dC50eHQKU3ViamVjdDogSG9tZXdvcmsKCmhpCgpG
cm9tIEJlbiBTdW4gT2N0ICA2IDEyOjA0OjM2IDIwMTkKVG86IGJtd2ViYjIwQGNvbGJ5LmVkdSwg
dGV4dC50eHQKU3ViamVjdDogSG9tZXdvcmsKCntccnRmMVxhbnNpXGFuc2ljcGcxMjUyXGNvY29h
cnRmMTY3MVxjb2NvYXN1YnJ0ZjYwMAp7XGZvbnR0YmxcZjBcZnN3aXNzXGZjaGFyc2V0MCBIZWx2
ZXRpY2E7fQp7XGNvbG9ydGJsO1xyZWQyNTVcZ3JlZW4yNTVcYmx1ZTI1NTt9CntcKlxleHBhbmRl
ZGNvbG9ydGJsOzt9ClxtYXJnbDE0NDBcbWFyZ3IxNDQwXHZpZXd3MTA4MDBcdmlld2g4NDAwXHZp
ZXdraW5kMApccGFyZFx0eDcyMFx0eDE0NDBcdHgyMTYwXHR4Mjg4MFx0eDM2MDBcdHg0MzIwXHR4
NTA0MFx0eDU3NjBcdHg2NDgwXHR4NzIwMFx0eDc5MjBcdHg4NjQwXHBhcmRpcm5hdHVyYWxccGFy
dGlnaHRlbmZhY3RvcjAKClxmMFxmczI0IFxjZjAgVGhpcyBpcyBhIHRleHQgZmlsZS59RnJvbSBC
ZW4gU3VuIE9jdCAgNiAxMjowNDoxNSAyMDE5ClRvOiBibXdlYmIyMEBjb2xieS5lZHUsIHRleHQu
dHh0ClN1YmplY3Q6IEhvbWV3b3JrCgpoaQoKCg==
--000000000000e705970594401f09--
```

The first section describes the Mime version, the date, the sender and receiver, as well as the overall content of the message.

The second section describes if there is any complex information (fonts) and how to find a simpler (and compatible) state.

The third section describes the text content of the email as well as including the data.

The fourth section describes the content of the email that is interpretable in html.

The fifth section describes the content of the attachment. The headers describe the type of file that was attached. In this case it was a text file. Mime converted the file into a string of ASCII characters which is seen in the large text subsection at the bottom.

3) a. The server port was 587.
   b. The encrypted content of the message can be seen but the actual content cannot. It cannot be seen because the message is encrypted.
   c. The total bytes transmitted are 1,128. I found this by adding up all of the TLSv1.0 that happened after the exchange of the cipher. The discrepancy between the two is because the message has been encapsulated by the time that the message is captured and thus has additional identifier information.
   d. The server is using ESMTP but with TLS security. TLSV1.0 is not the most up to date version of TLS.
   e. The server is located in the Kansas (MST). I found this by tracking the IP of the destination.

4) I found most of the information for this using this Link.

a. I connected to our project 2 website at the URL: http://cs.colby.edu/courses/F19/cs331/projects/p2.html

The result was:

`HTTP/1.1 200 OK` **-> The HTTP response was accepted.**

`Date: Sun, 06 Oct 2019 18:11:29 GMT` **-> The time.**

`Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16\r\n` **-> Server Information**

`Connection: Keep-Alive\r\n` **-> The connection characteristic (keep alive)**

`Keep-Alive: timeout=5, max=100\r\n` **-> Keep the connection alive with a max time of 100 and timeout of 5 seconds**

`ETag: “1c53-59377e0a99eee”\r\n` **-> This is part of web caching which allows the client to make conditional requests**

`\r\n`

b. I created a local server using the command: `nc -l 80`

When I tried to connect to localhost:80 on Chrome the result in the console was:

`GET / HTTP/1.1` **-> The HTTP response was received.**

`Host: localhost` **-> The host of the server.**

`Connection: keep-alive` **-> The type of connection.**

`Cache-Control: max-age=0` **-> Specifies how caching will happen.**

`DNT: 1` **-> Do not track (0 = tracking ok, 1 = tracking not ok)**

`Upgrade-Insecure-Requests: 1` **-> The client prefers an encrypted connection.**

`User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36` **-> Describes the compatibility of the application.**

`Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3` **-> Describes what content types the client can understand.**

`Accept-Encoding: gzip, deflate, br` **-> Describes what content encoding the client can understand.**

`Accept-Language: en-US,en;q=0.9 ->` **Describes what language types the client can understand.**