THM_S3BOTS2 [100 series questions]

In this exercise, you assume the persona of Alice Bluebird, the analyst who successfully assisted Wayne Enterprises and was recommended to Grace Hoppy at Frothly (*a beer company*) to assist them with their recent issues.

What Kinds of Events Do We Have?

The SPL (Splunk Search Processing Language) command metadata can be used to search for the same kind of information that is found in the Data Summary, with the bonus of being able to search within a specific index, if desired. All time-values are returned in EPOCH time, so to make the output user readable, the eval command should be used to provide more human-friendly formatting.

In this example, we will search the botsv2 index and return a listing of all the source types that can be found as well as a count of events and the first time and last time seen.

Resources:

- http://docs.splunk.com/Documentation/Splunk/latest/SearchReference/Metadata
- https://www.splunk.com/blog/2017/07/31/metadata-metalore.html

Metadata command:

```
| metadata type=sourcetypes index=botsv2 | eval firstTime=strftime(firstTime,"%Y-%m-%d %H:%M:%S") | eval lastTime=strftime(lastTime,"%Y-%m-%d %H:%M:%S") | eval recentTime=strftime(recentTime,"%Y-%m-%d %H:%M:%S") | sort - totalCount
```

Task 3 100 series questions

Question 1

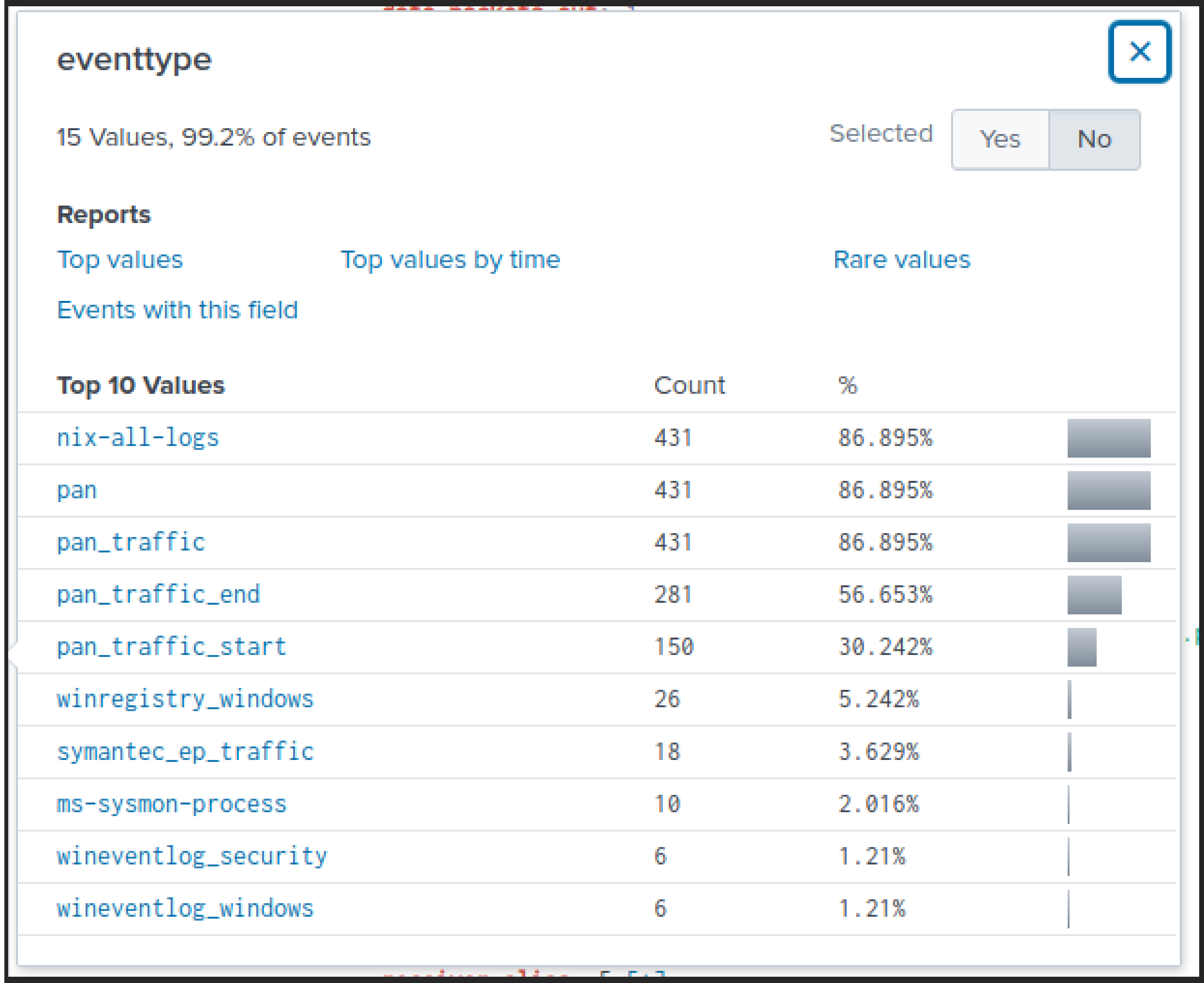
Amber Turing was hoping for Frothly to be acquired by a potential competitor which fell through, but visited their website to find contact information for their executive team. What is the website domain that she visited?

www.berkbeer.com

The first objective is to find out what competitor website she visited. What is a good starting point?

When it comes to HTTP traffic, the source and destination IP addresses should be recorded in logs. You need Amber's IP address.

You can start with the following command, index="botsv2" amber, and see what events are returned. Look at the events on the first page.



eventtype

15 Values, 99.2% of events

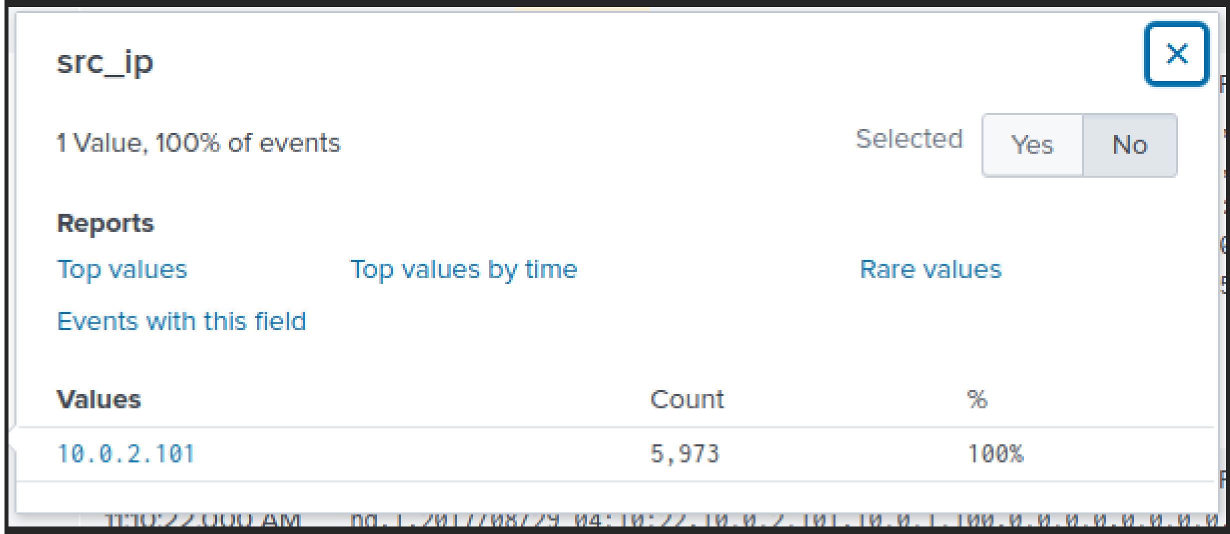
Top 10 Values	Count	%
nix-all-logs	431	86.895%
pan	431	86.895%
pan_traffic	431	86.895%
pan_traffic_end	281	56.653%
pan_traffic_start	150	30.242%
winregistry_windows	26	5.242%
symantec_ep_traffic	18	3.629%
ms-sysmon-process	10	2.016%
wineventlog_security	6	1.21%
wineventlog_windows	6	1.21%

Amber's IP address is visible in the events related to PAN traffic, but it's not straightforward.

To get her IP address, we can hone in on the PAN traffic source type specifically.

Command: index="botsv2" sourcetype="pan:traffic"

```
index="botsv2" sourcetype="pan:traffic" amber
```



src_ip

1 Value, 100% of events

Reports

Values	Count	%
10.0.2.101	5,973	100%

10.0.2.101

From here, you should have Amber's IP address. You can build a new search query using this information.

It would be best if you used the **HTTP stream** source type in your new search query.

Using Amber's IP address, construct the following search query.

Command: index="botsv2" ***IPADDR*** sourcetype="stream:HTTP"

You must substitute **IPADDR** with **Amber's IP address**.

After this query executes, there are many events to sift through for the answer. How else can you narrow this down?

Look at the additional fields.

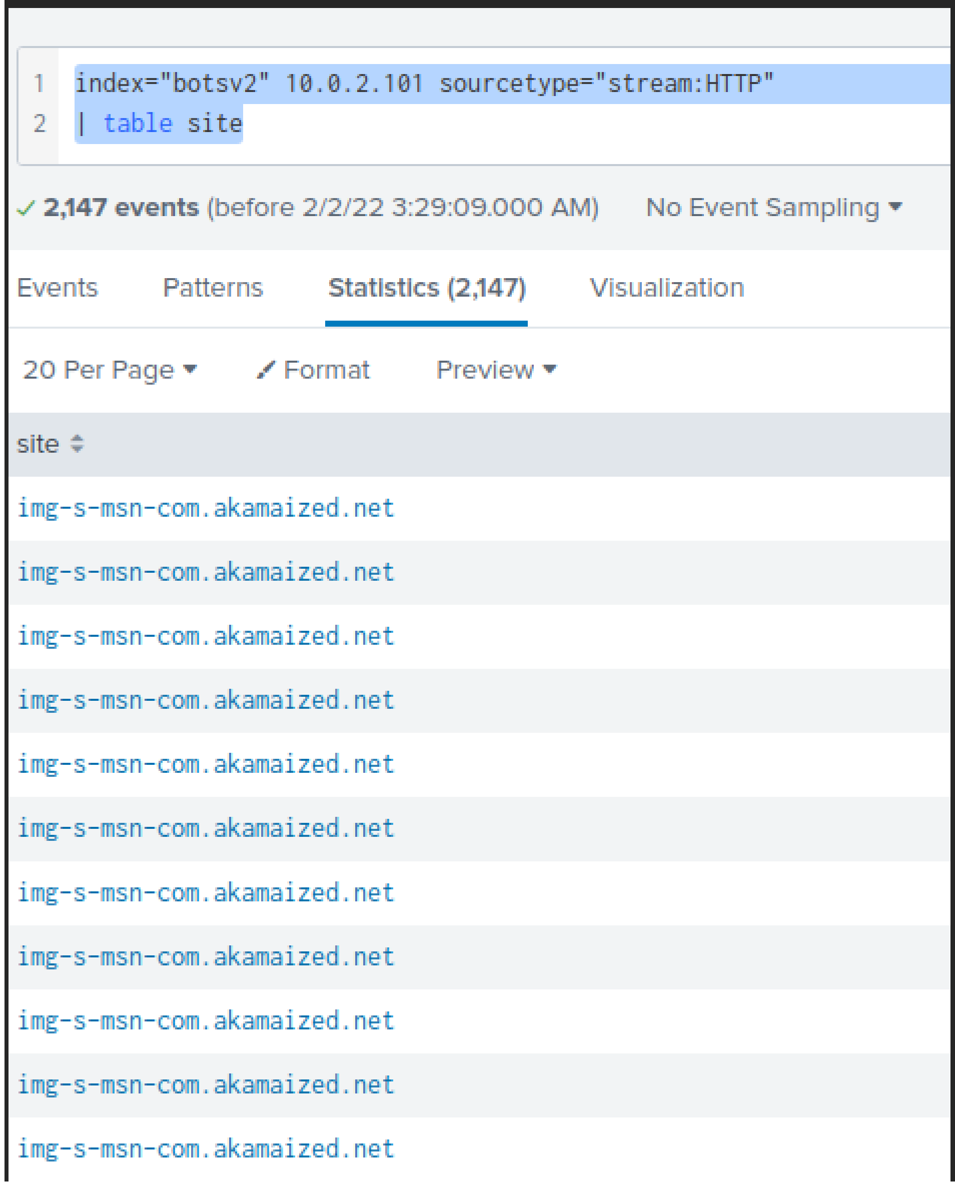
Another field you can add to the search query to further shrink the returned events list is the **site** field.

Think about it; you're investigating what competitor website Amber visited.

Expand the search query only to return the site field. Additionally, you can remove duplicate entries and display the results nicely in a table.

Command: index="botsv2" ***IPADDR*** sourcetype="stream:HTTP" | ***KEYWORD*** site | ***KEYWORD*** site

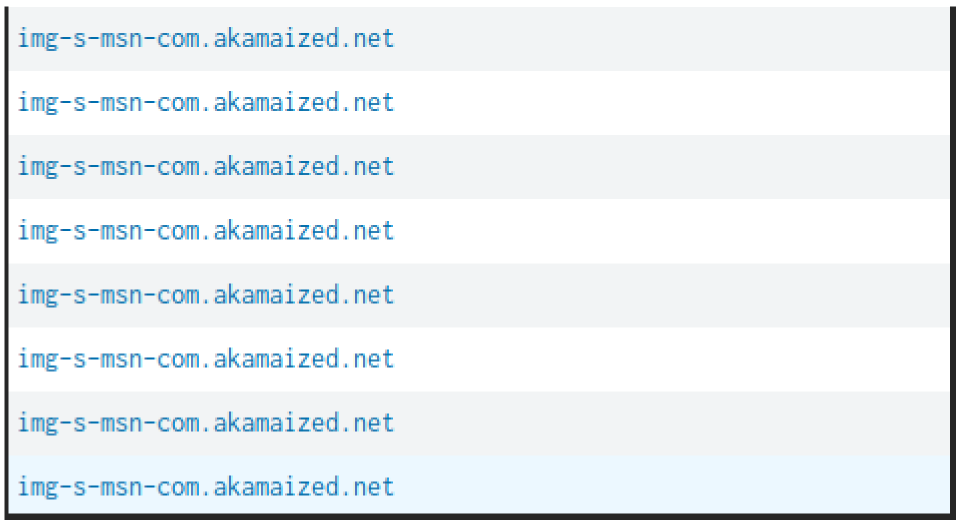
```
index="botsv2" 10.0.2.101 sourcetype="stream:HTTP"
| table site
```



```
index="botsv2" 10.0.2.101 sourcetype="stream:HTTP"
| table site
```

✓ **2,147 events** (before 2/2/22 3:29:09.000 AM) No Event Sampling ▾

site
img-s-msn-com.akamaized.net
img-s-msn-com.akamaized.net
img-s-msn-com.akamaized.net
img-s-msn-com.akamaized.net
img-s-msn-com.akamaized.net
img-s-msn-com.akamaized.net
img-s-msn-com.akamaized.net
img-s-msn-com.akamaized.net
img-s-msn-com.akamaized.net
img-s-msn-com.akamaized.net
img-s-msn-com.akamaized.net

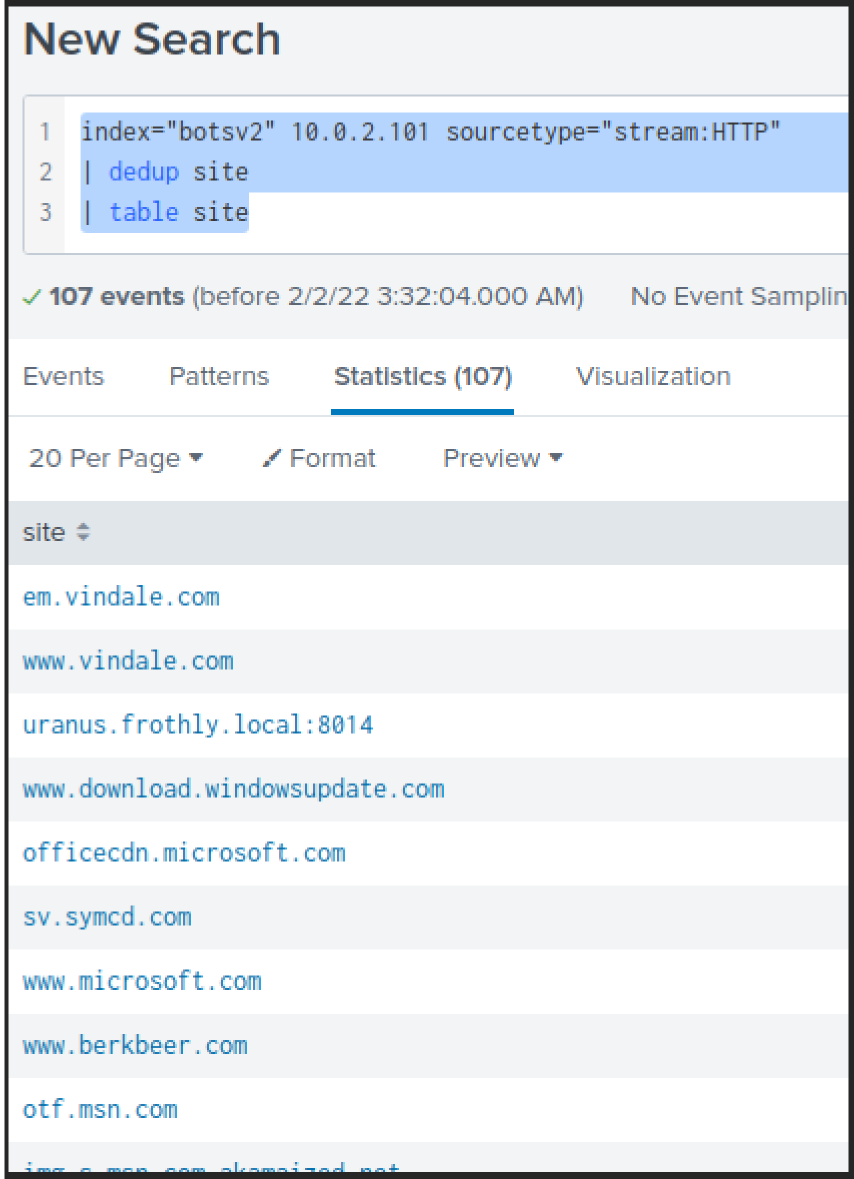


```
img-s-msn-com.akamaized.net
img-s-msn-com.akamaized.net
img-s-msn-com.akamaized.net
img-s-msn-com.akamaized.net
img-s-msn-com.akamaized.net
img-s-msn-com.akamaized.net
img-s-msn-com.akamaized.net
img-s-msn-com.akamaized.net
```

A lot of msn. I don't thin that is what we need exactly.

"dedup site" will elimate duplications

```
index="botsv2" 10.0.2.101 sourcetype="stream:HTTP"
| dedup site
| table site
```



New Search

```
index="botsv2" 10.0.2.101 sourcetype="stream:HTTP"
| dedup site
| table site
```

✓ 107 events (before 2/2/22 3:32:04.000 AM) No Event Samplin

site
em.vindale.com
www.vindale.com
uranus.frothly.local:8014
www.download.windowsupdate.com
officecdn.microsoft.com
sv.symcd.com
www.microsoft.com
www.berkbeer.com
otf.msn.com
img-s-msn-com.akamaized.net

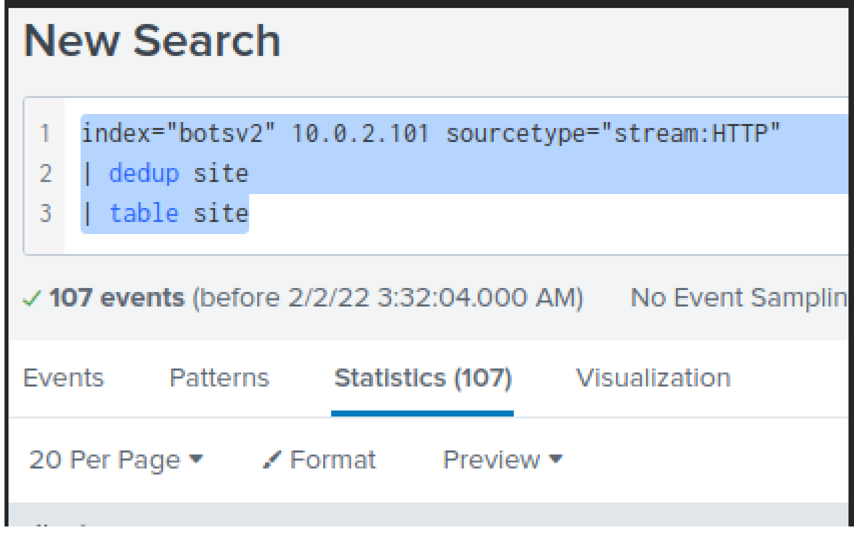
You must substitute **KEYWORD** with the Splunk commands to remove the duplicate entries and display the output in a table format.

Note: The first **KEYWORD** is to remove the duplicate entries, and the second is to display the output in a table format.

The results returned to show the URIs that Amber visited, but which website is the one that you're looking for?

To help answer these questions: Who does Amber work for, and what industry are they in?

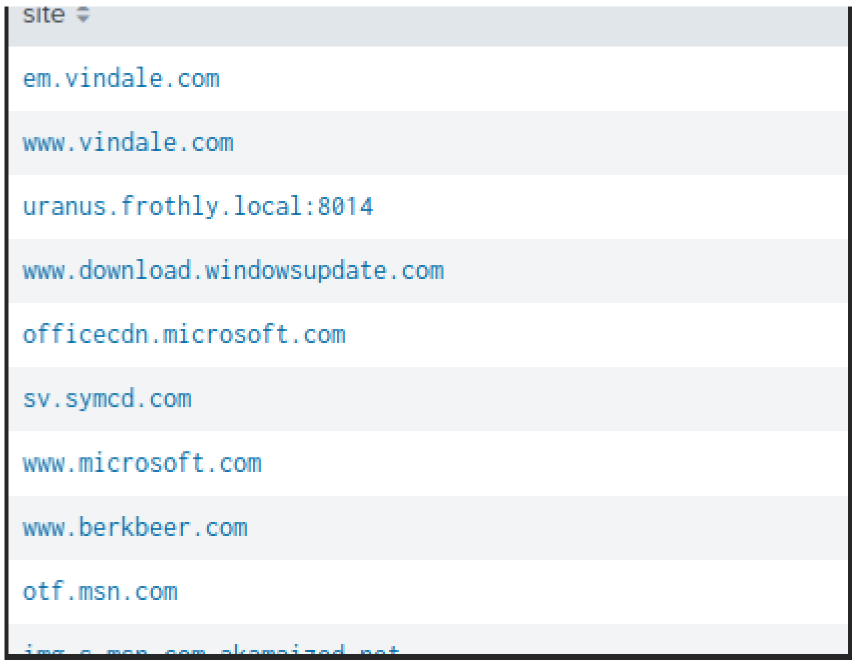
The competitor is in the same industry. The competitor website now should clearly be visible in the table output.



New Search

```
index="botsv2" 10.0.2.101 sourcetype="stream:HTTP"
| dedup site
| table site
```

✓ 107 events (before 2/2/22 3:32:04.000 AM) No Event Samplin



site ⇕
em.vindale.com
www.vindale.com
uranus.frothly.local:8014
www.download.windowsupdate.com
officecdn.microsoft.com
sv.symcd.com
www.microsoft.com
www.berkbeer.com
otf.msn.com
img-s-msn-com.akamaized.net

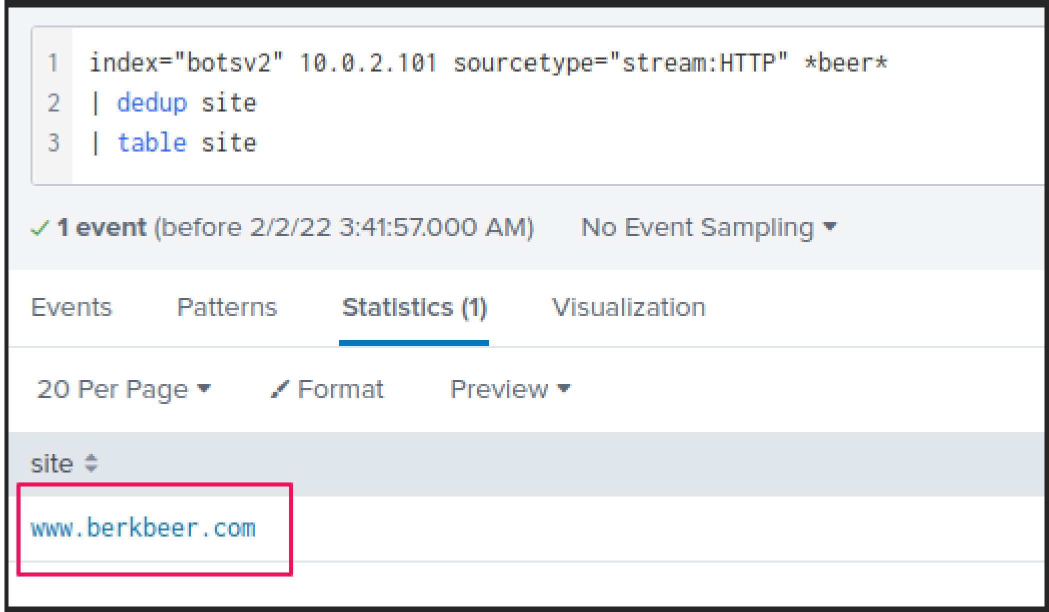
Extra: You can also use the industry as a search phrase to narrow down the results to a handful of events (1 result to be exact).

Command: index="botsv2" ***IPADDR*** sourcetype="stream:HTTP" ****INDUSTRY**** | ***KEYWORD*** site | ***KEYWORD*** site

Note: Use asterisks to surround the search term.

Adding "beer" in there really helps

```
index="botsv2" 10.0.2.101 sourcetype="stream:HTTP" *beer*
| dedup site
| table site
```



```
index="botsv2" 10.0.2.101 sourcetype="stream:HTTP" *beer*
| dedup site
| table site
```

✓ 1 event (before 2/2/22 3:41:57.000 AM) No Event Sampling ▾

site ⇕
www.berkbeer.com

Questions 2-7

QUESTION 2

Amber found the executive contact information and sent him an email. What image file displayed the executive's contact information? Answer example: /path/image.ext

/images/ceoberk.png

Amber found the executive contact information and sent him an email. Based on question 2, you know it's an image.

Since you now know the competitor website, you can construct a more specific search query isolating the results to focus on Amber's HTTP traffic to the competitor website.

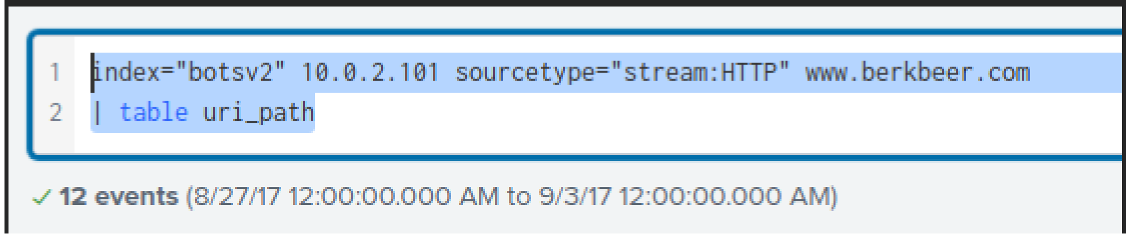
Command: index="botsv2" ***IPADDR*** sourcetype="stream:HTTP" ***COMPETITOR_WEBSITE***

Replace **COMPETITOR_WEBSITE** with the actual URI of the competitor website.

```
index="botsv2" 10.0.2.101 sourcetype="stream:HTTP" www.berkbeer.com
```

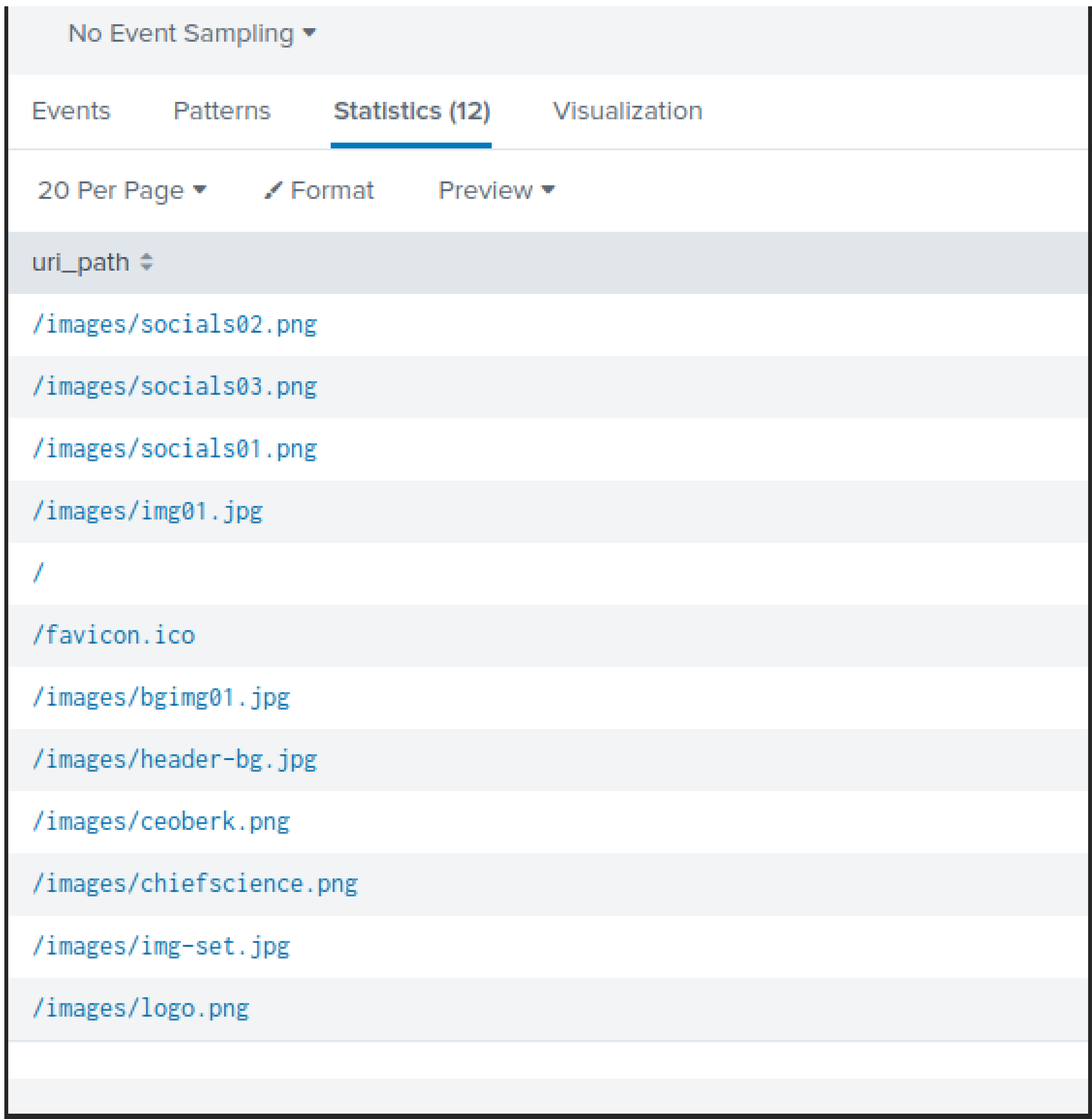
You can expand on the search query to output the specific field you want in a table format for an easy-to-read format, as we did for the previous objective.

```
index="botsv2" 10.0.2.101 sourcetype="stream:HTTP" www.berkbeer.com
| table uri_path
```



```
index="botsv2" 10.0.2.101 sourcetype="stream:HTTP" www.berkbeer.com
| table uri_path
```

✓ 12 events (8/27/17 12:00:00.000 AM to 9/3/17 12:00:00.000 AM)



uri_path
/images/socials02.png
/images/socials03.png
/images/socials01.png
/images/img01.jpg
/
/favicon.ico
/images/bgimg01.jpg
/images/header-bg.jpg
/images/ceoberk.png
/images/chiefscience.png
/images/img-set.jpg
/images/logo.png

QUESTION 3

What is the CEO's name? Provide the first and last name.

~~Heinz Bernhard~~ Martin Berk

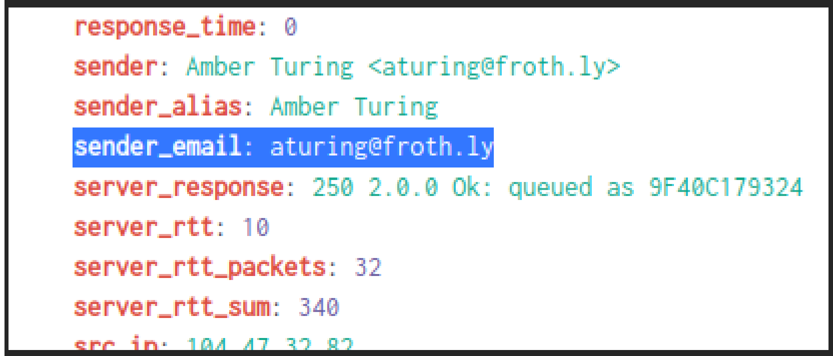
Based on the image, you have the CEO's last name but not his first name. Maybe you can get the name in the email communication.

You can now draw your attention to email traffic, SMTP, but you need Amber's email address. You should be able to get this on your own. :)

index="botsv2" sourcetype="stream:smtp"

But maybe a key word search *amber* could help and also *berk* because of answer 2 /images/ceo**berk**/png

index="botsv2" sourcetype="stream:smtp" amber



```
response_time: 0
sender: Amber Turing <aturing@froth.ly>
sender_alias: Amber Turing
sender_email: aturing@froth.ly
server_response: 250 2.0.0 Ok: queued as 9F40C179324
server_rtt: 10
server_rtt_packets: 32
server_rtt_sum: 340
src_ip: 104.47.32.82
```

Once you have Amber's email address, you can build a search query to focus on her email address and the competitor's website to find events that show email communication between Amber and the competitor.

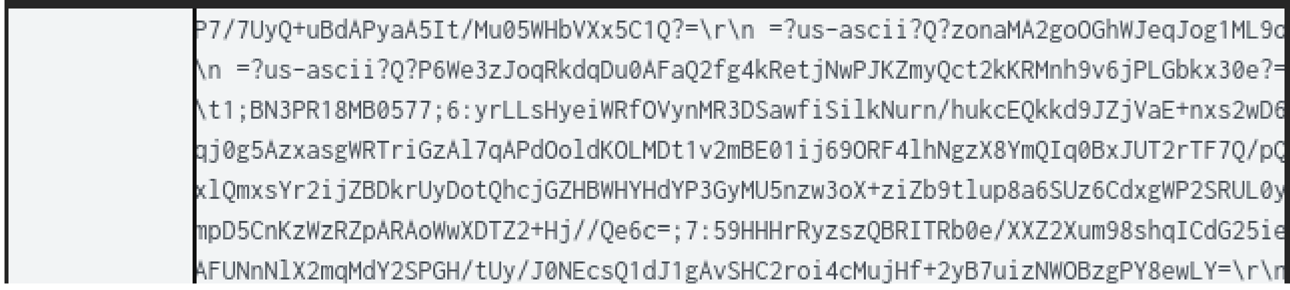
Command: index="botsv2" sourcetype="stream:smtp" ***AMBERS_EMAIL COMPETITOR_WEBSITE***

Replace **AMBERS_EMAIL** with her actual email address.

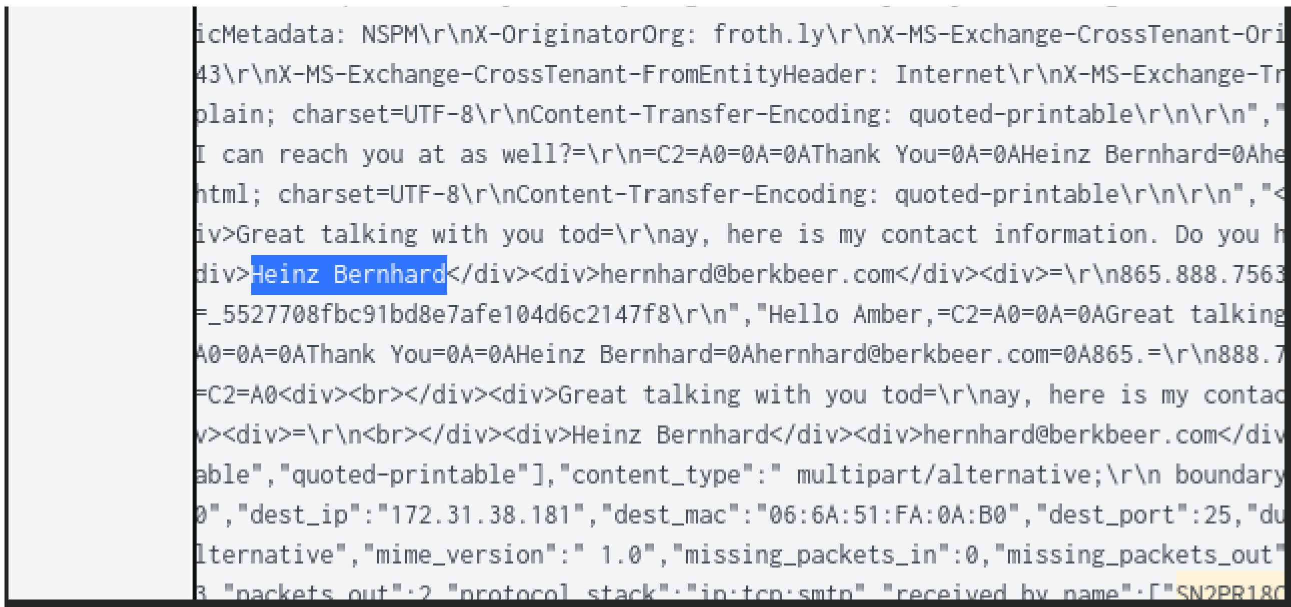
```
index=botsv2 sourcetype="stream:smtp" sender="Amber Turing <aturing@froth.ly>"
```

index="botsv2" sourcetype="stream:smtp" aturing@froth.ly berkbeer.com

```
index=botsv2 sourcetype="stream:smtp" "mberk@berkbeer.com"
```

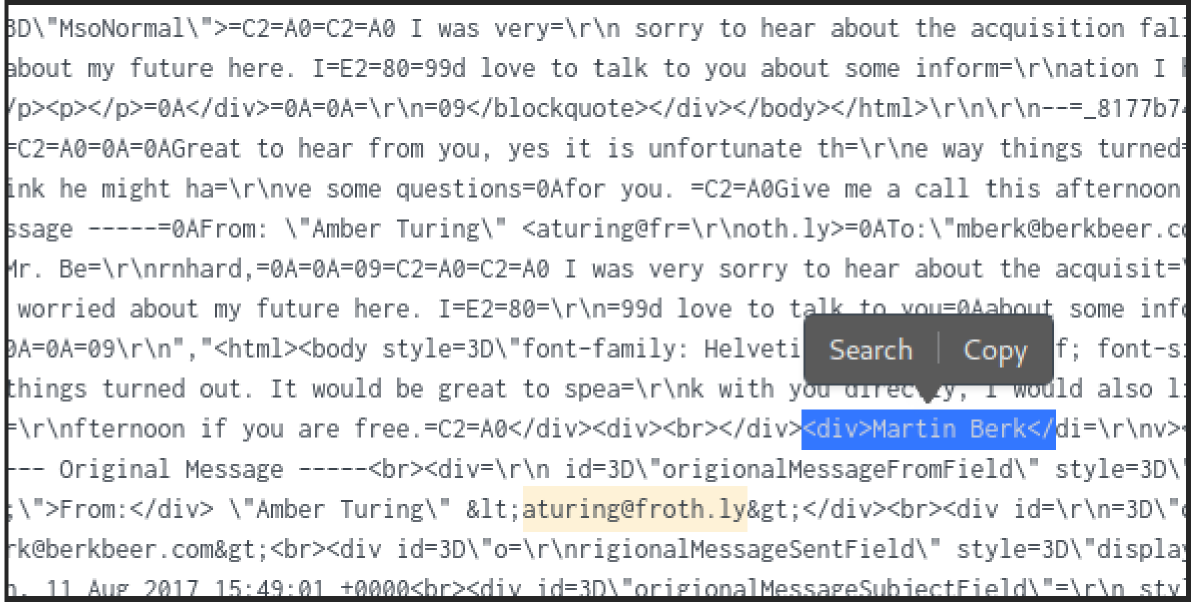


```
P7/7UyQ+uBdAPyaA5It/Mu05WHbVXx5C1Q?=\r\n =?us-ascii?Q?zonaMA2goOGhWJeqJog1ML9d
\n =?us-ascii?Q?P6We3zJoqRkdqDu0AFaQ2fg4kRetjNwPJKZmyQct2kKRMnh9v6jPLGbkx30e?=
\t1;BN3PR18MB0577;6:yrLLsHyeiWRfOVynMR3DSawfiSilkNurn/hukcEQkkd9JZjVaE+nxs2wD6
qj0g5AzxasgWRTriGzAl7qAPdOoldKOLMDt1v2mBE01ij69ORF4lhNgzX8YmQIq0BxJUT2rTF7Q/pQ
xlQmxsYr2ijZBDkrUyDotQhcjGZHBWHYHdYP3GyMU5nzw3oX+ziZb9tlup8a6SUz6CdxgWP2SRUL0y
mpD5CnKzWzRZpARAoWwXDTZ2+Hj//Qe6c=;7:59HHHrRyzszQBRITRb0e/XXZ2Xum98shqICdG25ie
AFUNnNlX2mqMdY2SPGH/tUy/J0NEcsQ1dJ1gAvSHC2roi4cMujHf+2yB7uizNWOBzgPY8ewLY=\r\n
```



```
icMetadata: NSPM\r\nX-OriginatorOrg: froth.ly\r\nX-MS-Exchange-CrossTenant-Ori
43\r\nX-MS-Exchange-CrossTenant-FromEntityHeader: Internet\r\nX-MS-Exchange-Tr
plain; charset=UTF-8\r\nContent-Transfer-Encoding: quoted-printable\r\n\r\n","
I can reach you at as well?=\r\n=C2=A0=0A=0AThank You=0A=0AHeinz Bernhard=0Ahe
html; charset=UTF-8\r\nContent-Transfer-Encoding: quoted-printable\r\n\r\n","<
iv>Great talking with you tod=\r\nay, here is my contact information. Do you h
div>Heinz Bernhard</div><div>hernhard@berkbeer.com</div><div>=\r\n865.888.7563
=_5527708fbc91bd8e7afe104d6c2147f8\r\n","Hello Amber,=C2=A0=0A=0AGreat talking
A0=0A=0AThank You=0A=0AHeinz Bernhard=0Ahernhard@berkbeer.com=0A865.=\r\n888.7
=C2=A0<div><br></div><div>Great talking with you tod=\r\nay, here is my contac
v><div>=\r\n<br></div><div>Heinz Bernhard</div><div>hernhard@berkbeer.com</div
able","quoted-printable"],"content_type":" multipart/alternative;\r\n boundary
0","dest_ip":"172.31.38.181","dest_mac":"06:6A:51:FA:0A:B0","dest_port":25,"du
lternative","mime_version":" 1.0","missing_packets_in":0,"missing_packets_out"
3,"packets_out":2,"protocol_stack":"ip:tcp:smtp","received_by_name":["SN2PR18C
```

Wrong guy!



```
3D\"MsoNormal\">=C2=A0=C2=A0 I was very=\r\n sorry to hear about the acquisition fal
about my future here. I=E2=80=99d love to talk to you about some inform=\r\nation I
/p><p></p>=0A</div>=0A=0A=\r\n=09</blockquote></div></body></html>\r\n\r\n--=_8177b7
=C2=A0=0A=0AGreat to hear from you, yes it is unfortunate th=\r\ne way things turned
ink he might ha=\r\nve some questions=0Afor you. =C2=A0Give me a call this afternoon
ssage -----=0AFrom: \"Amber Turing\" <aturing@fr=\r\noth.ly>=0ATo:\"mberk@berkbeer.c
Mr. Be=\r\nrnhard,=0A=0A=09=C2=A0=C2=A0 I was very sorry to hear about the acquisit=
 worried about my future here. I=E2=80=\r\n=99d love to talk to you=0Aabout some inf
0A=0A=09\r\n","<html><body style=3D\"font-family: Helveti               f; font-s
things turned out. It would be great to spea=\r\nk with you directly, I would also l
=\r\nfternoon if you are free.=C2=A0</div><div><br></div><div>Martin Berk</di=\r\nv>
--- Original Message -----<br><div=\r\n id=3D\"origionalMessageFromField\" style=3D\
;\">From:</div> \"Amber Turing\" &lt;aturing@froth.ly&gt;</div><br><div id=\r\n=3D\"
rk@berkbeer.com&gt;<br><div id=3D\"o=\r\nrigionalMessageSentField\" style=3D\"displa
n, 11 Aug 2017 15:49:01 +0000<br><div id=3D\"origionalMessageSubjectField\"=\r\n sty
```

With the returned results from the above search query, you can answer your own remaining questions. :)

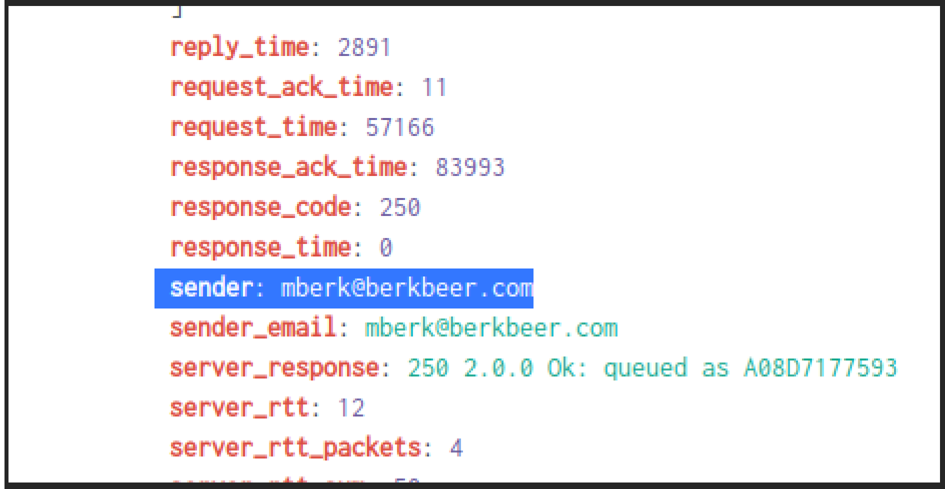
Question 4

What is the CEO's email address?

mberk@berkbeer.com

Filtering for

index="botsv2" sourcetype="stream:smtp" "Martin Berk"



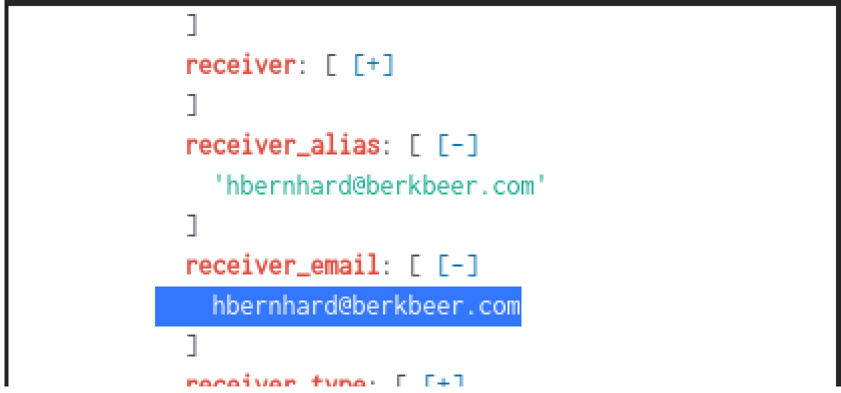
```
]
reply_time: 2891
request_ack_time: 11
request_time: 57166
response_ack_time: 83993
response_code: 250
response_time: 0
sender: mberk@berkbeer.com
sender_email: mberk@berkbeer.com
server_response: 250 2.0.0 Ok: queued as A08D7177593
server_rtt: 12
server_rtt_packets: 4
server_rtt_sum: 50
```

Question 5

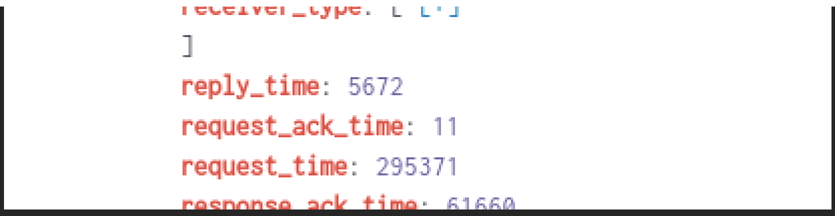
After the initial contact with the CEO, Amber contacted another employee at this competitor. What is that employee's email address?

hbernhard@berkbeer.com

index=botsv2 sourcetype="stream:smtp" aturing@froth.ly



```
]
receiver: [ [+]
]
receiver_alias: [ [-]
  'hbernhard@berkbeer.com'
]
receiver_email: [ [-]
  hbernhard@berkbeer.com
]
receiver_type: [ [+]
```



```
        receiver_type: [ [+]
        ]
        reply_time: 5672
        request_ack_time: 11
        request_time: 295371
        response_ack_time: 61660
```

Question 6

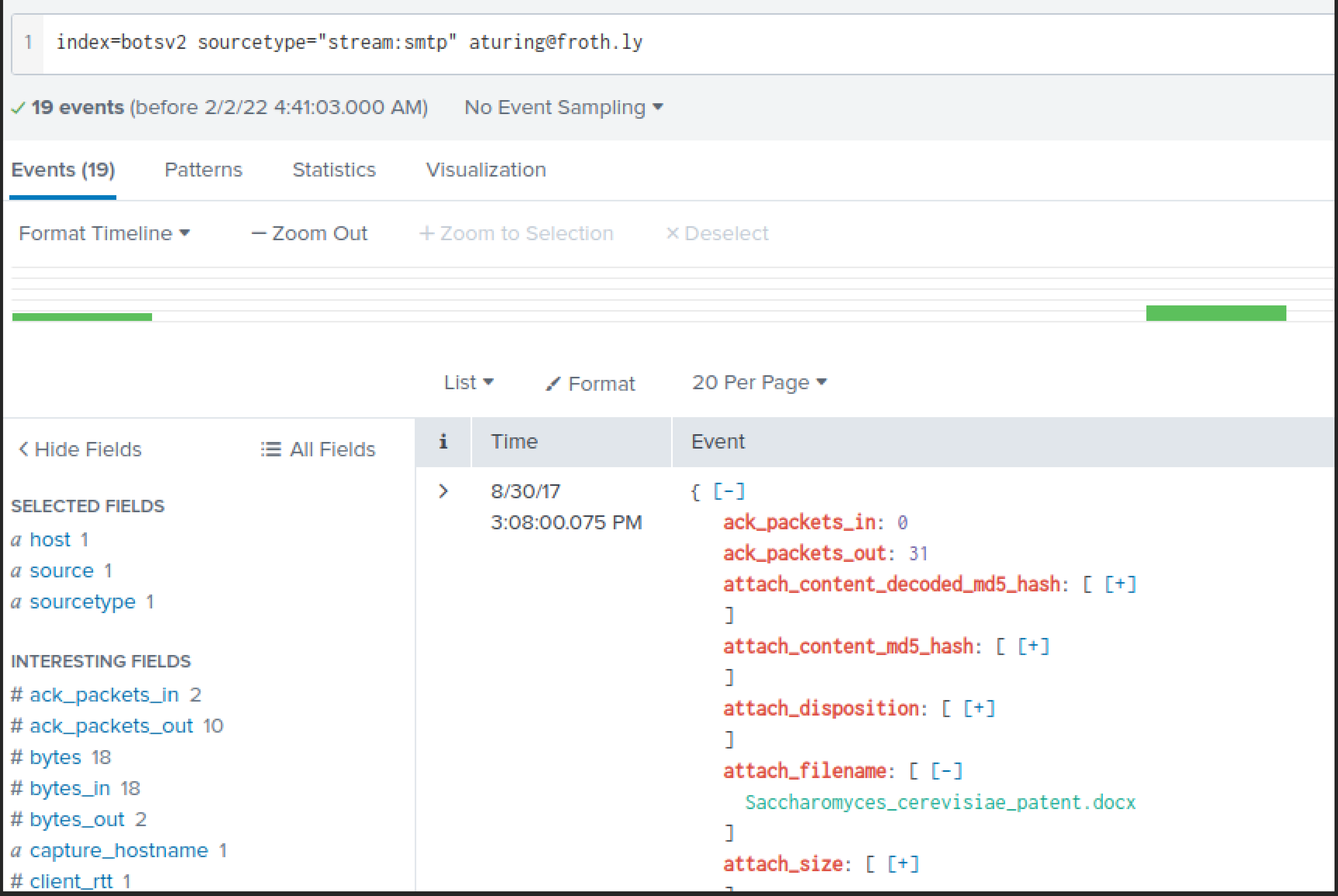
What is the name of the file attachment that Amber sent to a contact at the competitor?

Saccharomyces_cerevisiae_patent.docx

Using filter

index=botsv2 sourcetype="stream:smtp" aturing@froth.ly

we find the attachement



```
index=botsv2 sourcetype="stream:smtp" aturing@froth.ly
```

✓ 19 events (before 2/2/22 4:41:03.000 AM) No Event Sampling ▾

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# ack_packets_in 2
# ack_packets_out 10
# bytes 18
# bytes_in 18
# bytes_out 2
a capture_hostname 1
# client_rtt 1

i	Time	Event
>	8/30/17 3:08:00.075 PM	{ [-]

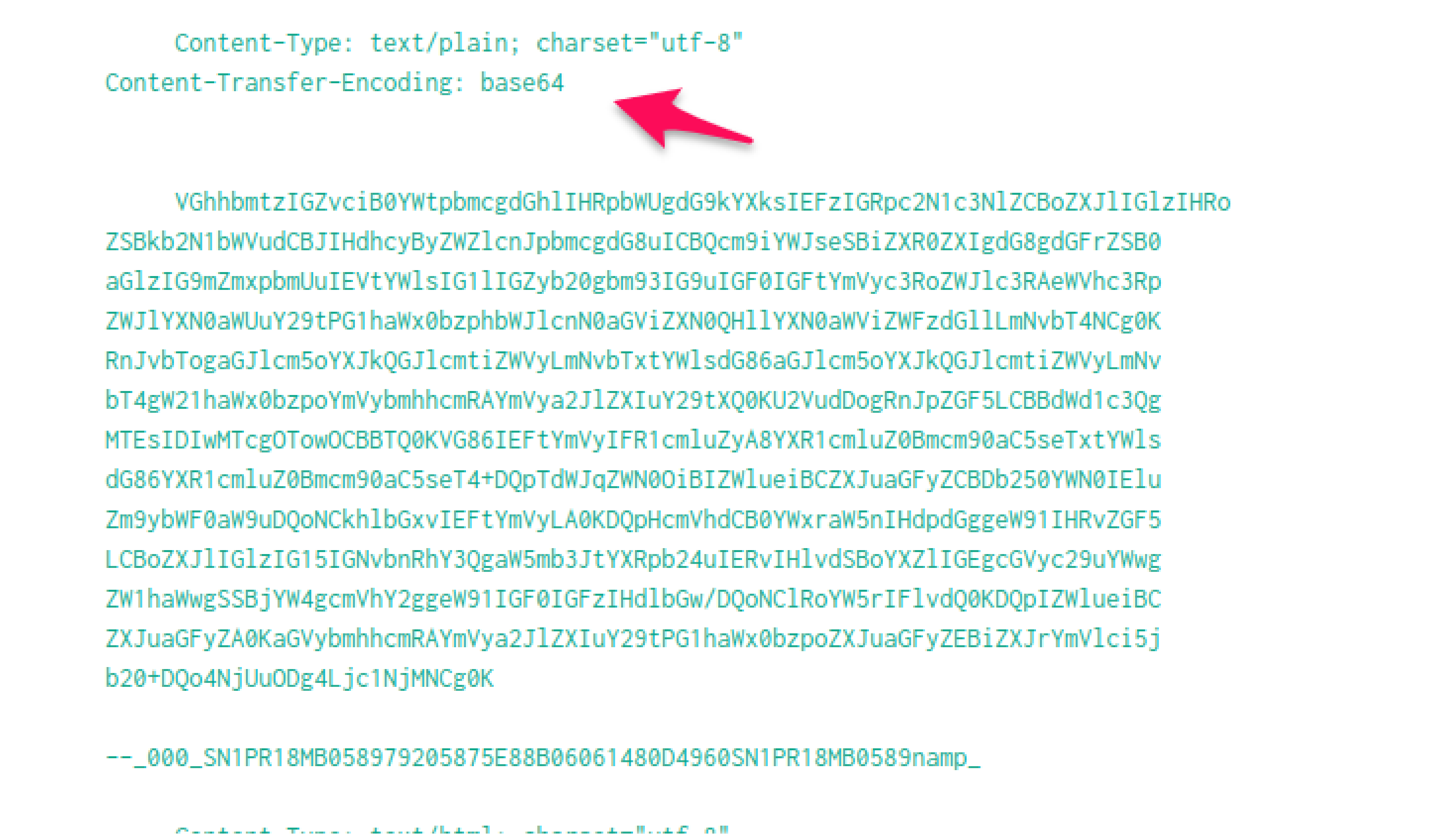
```
{ [-]
   ack_packets_in: 0
   ack_packets_out: 31
   attach_content_decoded_md5_hash: [ [+]
   ]
   attach_content_md5_hash: [ [+]
   ]
   attach_disposition: [ [+]
   ]
   attach_filename: [ [-]
     Saccharomyces_cerevisiae_patent.docx
   ]
   attach_size: [ [+]
```

Question 7

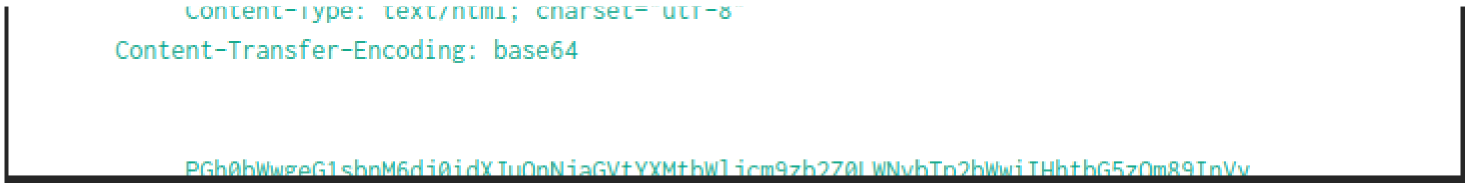
What is Amber's personal email address?

ambersthebest@yeastiebeastie.com

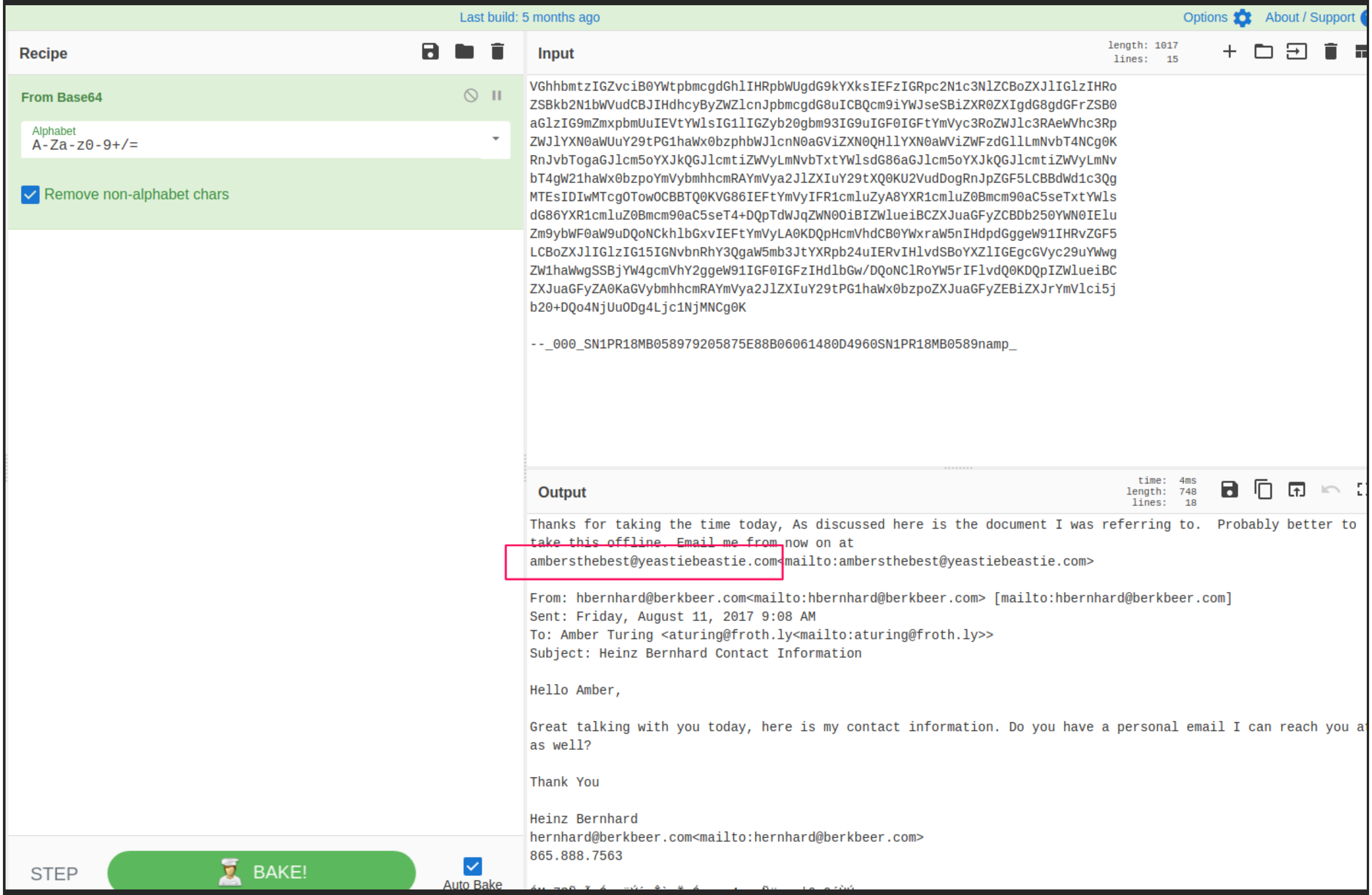
Still using the above filter, in the most recent email was found:



```
     Content-Type: text/plain; charset="utf-8"
Content-Transfer-Encoding: base64


     VGhhbmtzIGZvciB0YWtpbmcgdGhlIHRpbWUgdG9kYXksIEFzIGRpc2N1c3NlZCBoZXJlIGlzIHRo
ZSBkb2N1bWVudCBJIHdhcyByZWZlcnJpbmcgdG8uICBQcm9iYWJseSBiZXR0ZXIgdG8gdGFrZSB0
aGlzIG9mZmxpbmUuIEVtYWlsIG1lIGZyb20gbm93IG9uIGF0IGFtYmVyc3RoZWJlc3RAeWVhc3Rp
ZWJlYXN0aWUuY29tPG1haWx0bzphbWJlcnN0aGViZXN0QHllYXN0aWViZWFzdGllLmNvbT4NCg0K
RnJvbTogaGJlcm5oYXJkQGJlcmtiZWVyLmNvbTxtYWlsdG86aGJlcm5oYXJkQGJlcmtiZWVyLmNv
bT4gW21haWx0bzpoYmVybmhhcmRAYmVya2JlZXIuY29tXQ0KU2VudDogRnJpZGF5LCBBdWd1c3Qg
MTEsIDIwMTcgOTowOCBBTQ0KVG86IEFtYmVyIFR1cmluZyA8YXR1cmluZ0Bmcm90aC5seTxtYWls
dG86YXR1cmluZ0Bmcm90aC5seT4+DQpTdWJqZWN0OiBIZWlueiBCZXJuaGFyZCBDb250YWN0IElu
Zm9ybWF0aW9uDQoNCkhlbGxvIEFtYmVyLA0KDQpHcmVhdCB0YWxraW5nIHdpdGggeW91IHRvZGF5
LCBoZXJlIGlzIG15IGNvbnRhY3QgaW5mb3JtYXRpb24uIERvIHlvdSSBoYXZlIGEgcGVyc29uYWwg
ZW1haWwgSSBjYW4gcmVhY2ggeW91IGF0IGFzIHdlbGw/DQoNClRoYW5rIFlvdQ0KDQpIZWlueiBC
ZXJuaGFyZA0KaGVybmhhcmRAYmVya2JlZXIuY29tPG1haWx0bzpoZXJuaGFyZEBiZXJrYmVlci5j
b20+DQo4NjUuODg4Ljc1NjMNCg0K

--_000_SN1PR18MB058979205875E88B06061480D4960SN1PR18MB0589namp_

     Content-Type: text/html; charset="utf-8"
```



```
Content-Type: text/html; charset=utf-8
Content-Transfer-Encoding: base64

    PGh0bWwgeG1sbnM6dj0idXJuOnNjaGVtYXMtbWljcm9zb2Z0LWNvbTp2bWwiIHhtbG5zOm89InVy
```



From Base64

Alphabet A-Za-z0-9+/=

☑ Remove non-alphabet chars

Input length: 1017 lines: 15

```
VGhhbmtzIGZvciB0YWtpbmcgdGhlIHRpbWUgdG9kYXksIEFzIGRpc2N1c3NlZCBoZXJlIGlzIHRo
ZSBkb2N1bWVudCBJIHdhcyByZWZlcnJpbmcgdG8uICBQcm9iYWJseSBiZXR0ZXIgdG8gdGFrZSB0
aGlzIG9mZmxpbmUuIEVtYWlsIG1lIGZyb20gbm93IG9uIGF0IGFtYmVyc3RoZWJlc3RAeWVhc3Rp
ZWJlYXN0aWUuY29tPG1haWx0bzphbWJlcnN0aGViZXN0QHllYXN0aWViZWFzdGllLmNvbT4NCg0K
RnJvbTogaGJlcm5oYXJkQGJlcmtiZWVyLmNvbTxtYWlsdG86aGJlcm5oYXJkQGJlcmtiZWVyLmNv
bT4gW21haWx0bzpoYmVybmhhcmRAYmVya2JlZXIuY29tXQ0KU2VudDogRnJpZGF5LCBBdWd1c3Qg
MTEsIDIwMTcgOTowOCBBTQ0KVG86IEFtYmVyIFR1cmluZyA8YXR1cmluZ0Bmcm90aC5seTxtYWls
dG86YXR1cmluZ0Bmcm90aC5seT4+DQpTdWJqZWN0OiBIZWlueiBCZXJuaGFyZCBDb250YWN0IElu
Zm9ybWF0aW9uDQoNCkhlbGxvIEFtYmVyLA0KDQpHcmVhdCB0YWxraW5nIHdpdGggeW91IHRvZGF5
LCBoZXJlIGlzIG15IGNvbnRhY3QgaW5mb3JtYXRpb24uIERvIHlvdSBoYXZlIGEgcGVyc29uYWwg
ZW1haWwgSSBjYW4gcmVhY2ggeW91IGF0IGFzIHdlbGw/DQoNClRoYW5rIFlvdQ0KDQpIZWlueiBC
ZXJuaGFyZA0KaGVybmhhcmRAYmVya2JlZXIuY29tPG1haWx0bzpoZXJuaGFyZEBiZXJrYmVlci5j
b20+DQo4NjUuODg4Ljc1NjMNCg0K

--_000_SN1PR18MB058979205875E88B06061480D4960SN1PR18MB0589namp_
```

Output time: 4ms length: 748 lines: 18

```
Thanks for taking the time today, As discussed here is the document I was referring to.  Probably better to
take this offline. Email me from now on at
ambersthebest@yeastiebeastie.com<mailto:ambersthebest@yeastiebeastie.com>

From: hbernhard@berkbeer.com<mailto:hbernhard@berkbeer.com> [mailto:hbernhard@berkbeer.com]
Sent: Friday, August 11, 2017 9:08 AM
To: Amber Turing <aturing@froth.ly<mailto:aturing@froth.ly>>
Subject: Heinz Bernhard Contact Information

Hello Amber,

Great talking with you today, here is my contact information. Do you have a personal email I can reach you at
as well?

Thank You

Heinz Bernhard
hernhard@berkbeer.com<mailto:hernhard@berkbeer.com>
865.888.7563
```

Good 'ol cyberchef