Investigating with Splunk 2 - 100 series Questions

The questions below are from the BOTSv2 dataset, questions 100-104. Some additional questions were added.

In this task, we'll attempt to help guide you to each question's answer.

Note: The approach outlined in this task is not the only approach to tackle each question.

Reading the questions below, the focus is on **Amber Turing and her communication with a competitor.**

Question 1

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.

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"

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

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?

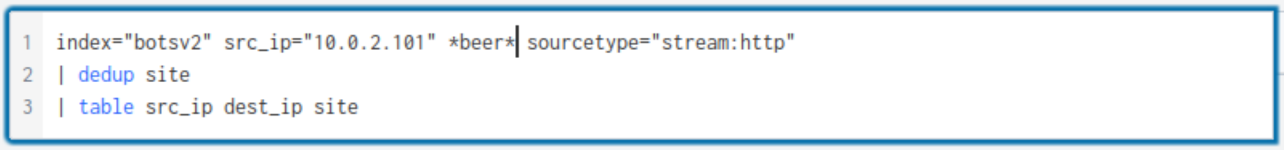
To help answer these questions: Who does Amber work for, and what industry are they in? The competitor is in the same industry. The competitor website now should clearly be visible in the table output.

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.

Questions 2-7
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.
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.
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. :)
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.
With the returned results from the above search query, you can answer your own remaining questions. :)

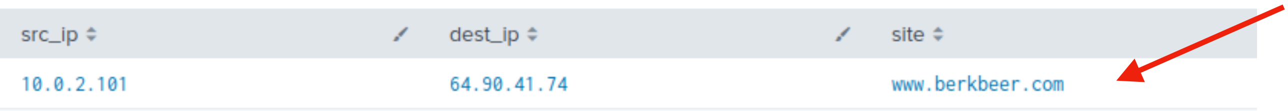
Question 1:
Amber Turing was hoping for Frothly to be acquired by a potential competitor which fell through, but visited their website to find contact information for their executive team. What is the website domain that she visited?
www.berkbeer.com

Findings



```
index="botsv2" src_ip="10.0.2.101" *beer* sourcetype="stream:http"
| dedup site
| table src_ip dest_ip site
```

The above search fetches any websites competitor that Amber had visited trough her *Ip_address*, I *dedup* (deduplicate) all sites then the created a *table* below.



src_ip	dest_ip	site
10.0.2.101	64.90.41.74	www.berkbeer.com

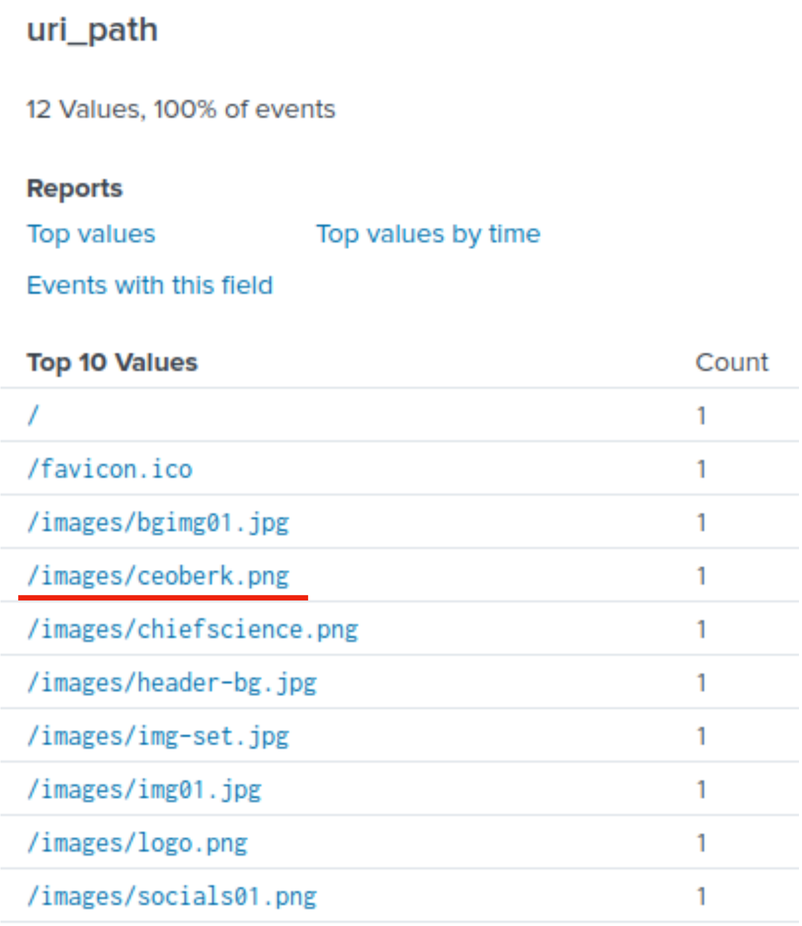
Question 2:

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

Findings

Looking at the interesting Field " uri path":



uri_path

12 Values, 100% of events

Reports

Top values

Top values by time

Events with this field

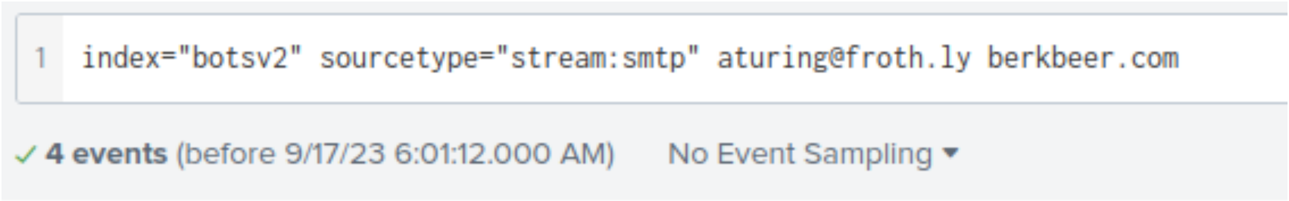
Top 10 Values	Count
/	1
/favicon.ico	1
/images/bgimg01.jpg	1
/images/ceoberk.png	1
/images/chiefscience.png	1
/images/header-bg.jpg	1
/images/img-set.jpg	1
/images/img01.jpg	1
/images/logo.png	1
/images/socials01.png	1

Question 3:

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

Martin Berk

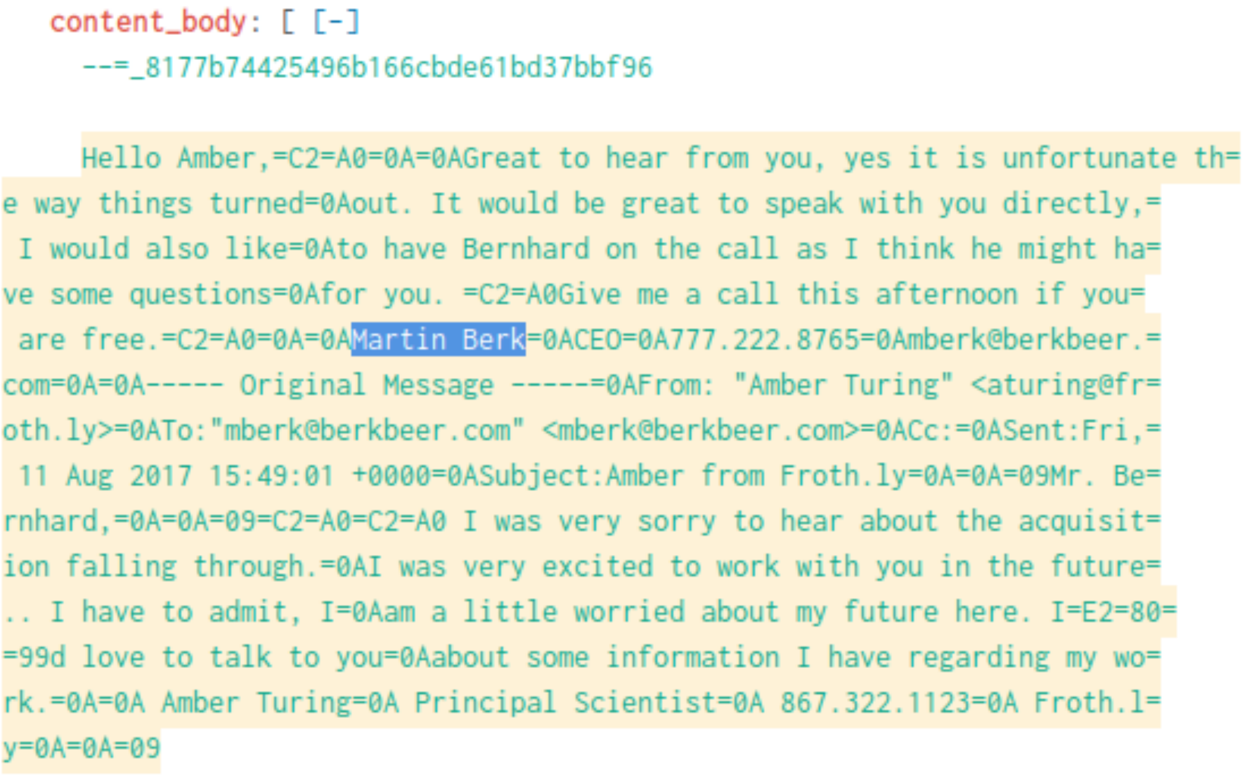
Findings



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

✓ **4 events** (before 9/17/23 6:01:12.000 AM)   No Event Sampling ▾

The above search fetches through the mail server(SMTP) WHERE Amber (aturing@froth.ly) had any communications with the competitor company(berkbeer.com) resulting only 4 events.
After the initial contact, the CEO replied to amber:

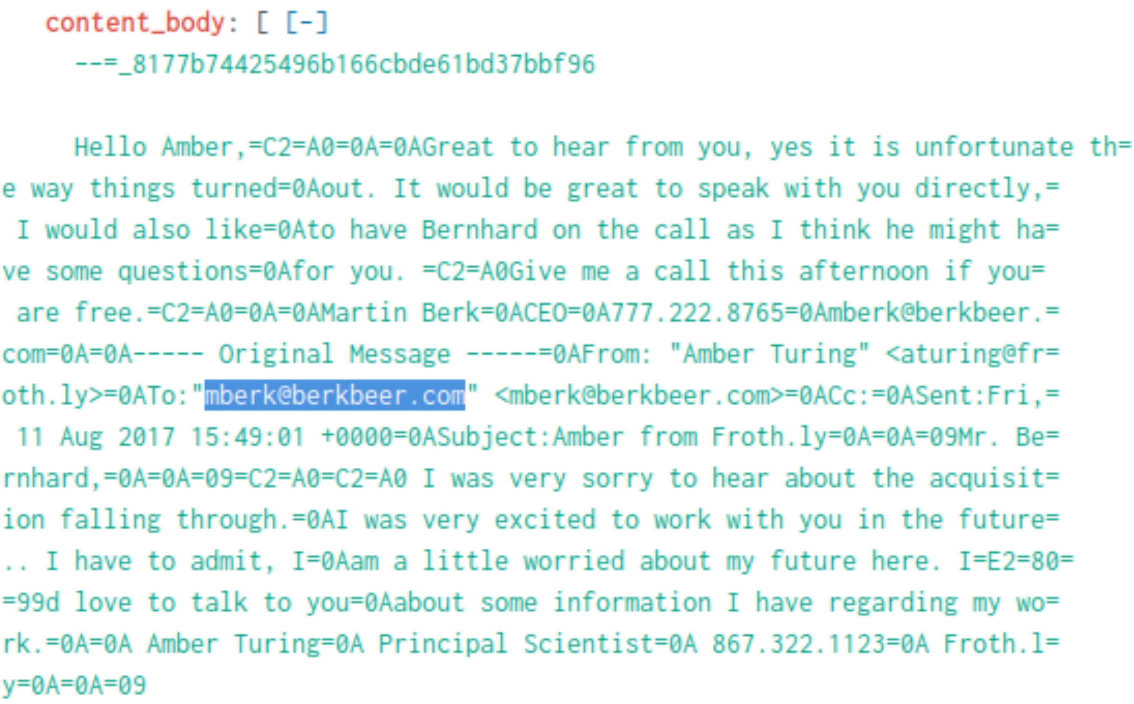


```
content_body: [ [-]
  --=_8177b74425496b166cbde61bd37bbf96

    Hello Amber,=C2=A0=0A=0AGreat to hear from you, yes it is unfortunate th=
e way things turned=0Aout. It would be great to speak with you directly,=
 I would also like=0Ato have Bernhard on the call as I think he might ha=
ve some questions=0Afor you. =C2=A0Give me a call this afternoon if you=
 are free.=C2=A0=0A=0AMartin Berk=0ACEO=0A777.222.8765=0Amberk@berkbeer.=
com=0A=0A----- Original Message -----=0AFrom: "Amber Turing" <aturing@fr=
oth.ly>=0ATo:"mberk@berkbeer.com" <mberk@berkbeer.com>=0ACc:=0ASent:Fri,=
 11 Aug 2017 15:49:01 +0000=0ASubject:Amber from Froth.ly=0A=0A=09Mr. Be=
rnhard,=0A=0A=09=C2=A0=C2=A0 I was very sorry to hear about the acquisit=
ion falling through.=0AI was very excited to work with you in the future=
.. I have to admit, I=0Aam a little worried about my future here. I=E2=80=
=99d love to talk to you=0Aabout some information I have regarding my wo=
rk.=0A=0A Amber Turing=0A Principal Scientist=0A 867.322.1123=0A Froth.l=
y=0A=0A=09
```

Question 4:

What is the CEO's email address?
mberk@berkbeer.com

Findings



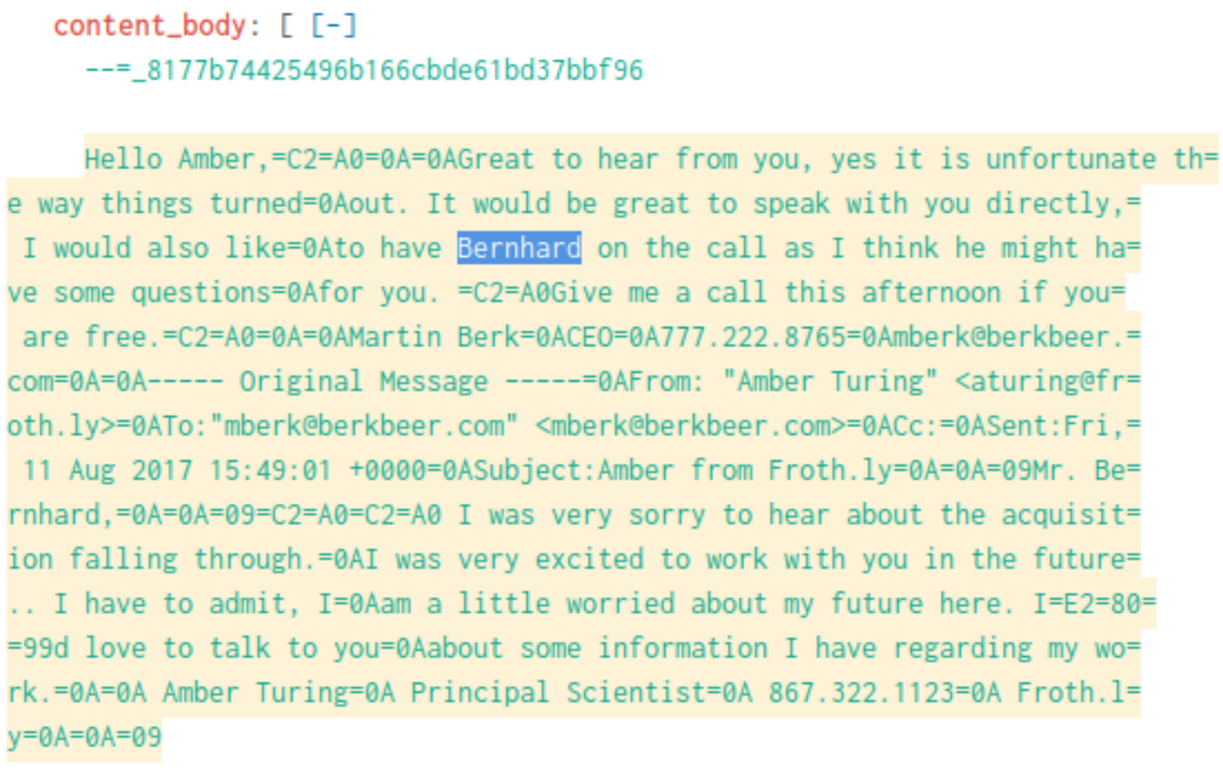
```
content_body: [ [-]
  --=_8177b74425496b166cbde61bd37bbf96

    Hello Amber,=C2=A0=0A=0AGreat to hear from you, yes it is unfortunate th=
e way things turned=0Aout. It would be great to speak with you directly,=
 I would also like=0Ato have Bernhard on the call as I think he might ha=
ve some questions=0Afor you. =C2=A0Give me a call this afternoon if you=
 are free.=C2=A0=0A=0AMartin Berk=0ACEO=0A777.222.8765=0Amberk@berkbeer.=
com=0A=0A----- Original Message -----=0AFrom: "Amber Turing" <aturing@fr=
oth.ly>=0ATo:"mberk@berkbeer.com" <mberk@berkbeer.com>=0ACc:=0ASent:Fri,=
 11 Aug 2017 15:49:01 +0000=0ASubject:Amber from Froth.ly=0A=0A=09Mr. Be=
rnhard,=0A=0A=09=C2=A0=C2=A0 I was very sorry to hear about the acquisit=
ion falling through.=0AI was very excited to work with you in the future=
.. I have to admit, I=0Aam a little worried about my future here. I=E2=80=
=99d love to talk to you=0Aabout some information I have regarding my wo=
rk.=0A=0A Amber Turing=0A Principal Scientist=0A 867.322.1123=0A Froth.l=
y=0A=0A=09
```

Analysing the same email content_body, the CEO email address is clearly visible.

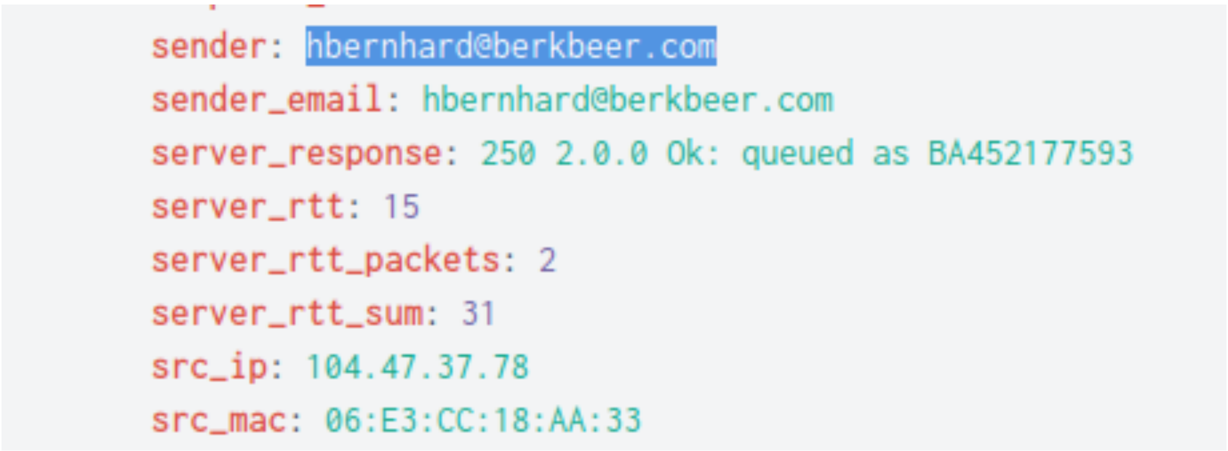
Question 5:
After the initial contact with the CEO, Amber contacted another employee at this competitor. What is that employee's email address?
hbernhard@berkbeer.com

Findings

If you look closely at the same email content_body, Mr berk was inviting Bernhard to the call. So what's bernhard email?



```
content_body: [ [-]
  --=_8177b74425496b166cbde61bd37bbf96

    Hello Amber,=C2=A0=0A=0AGreat to hear from you, yes it is unfortunate th=
e way things turned=0Aout. It would be great to speak with you directly,=
 I would also like=0Ato have Bernhard on the call as I think he might ha=
ve some questions=0Afor you. =C2=A0Give me a call this afternoon if you=
 are free.=C2=A0=0A=0AMartin Berk=0ACEO=0A777.222.8765=0Amberk@berkbeer.=
com=0A=0A----- Original Message -----=0AFrom: "Amber Turing" <aturing@fr=
oth.ly>=0ATo:"mberk@berkbeer.com" <mberk@berkbeer.com>=0ACc:=0ASent:Fri,=
 11 Aug 2017 15:49:01 +0000=0ASubject:Amber from Froth.ly=0A=0A=09Mr. Be=
rnhard,=0A=0A=09=C2=A0=C2=A0 I was very sorry to hear about the acquisit=
ion falling through.=0AI was very excited to work with you in the future=
.. I have to admit, I=0Aam a little worried about my future here. I=E2=80=
=99d love to talk to you=0Aabout some information I have regarding my wo=
rk.=0A=0A Amber Turing=0A Principal Scientist=0A 867.322.1123=0A Froth.l=
y=0A=0A=09
```



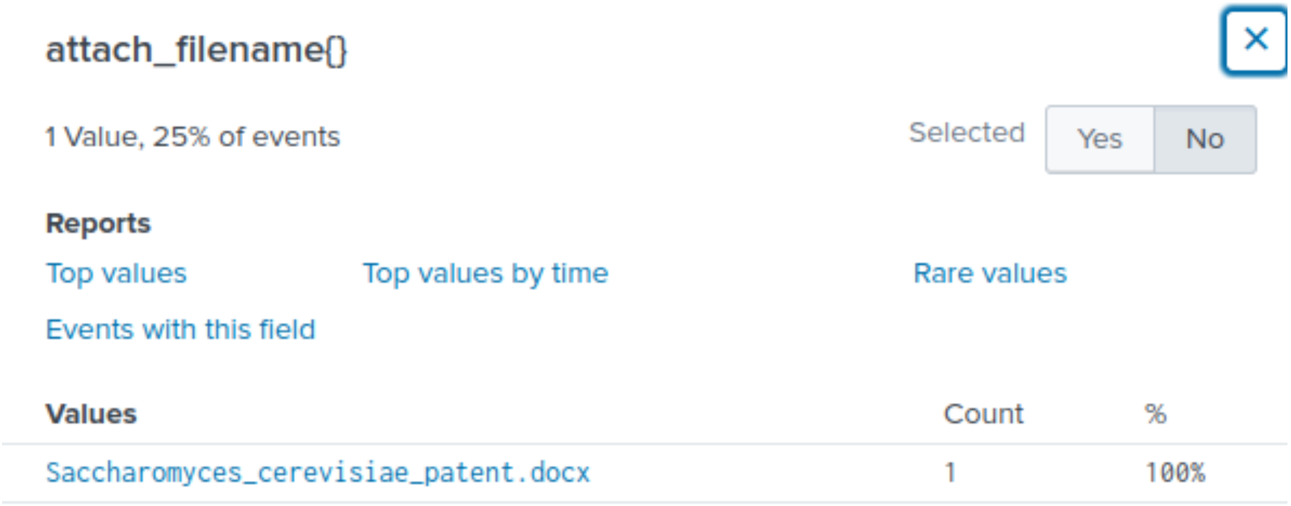
```
sender: hbernhard@berkbeer.com
sender_email: hbernhard@berkbeer.com
server_response: 250 2.0.0 Ok: queued as BA452177593
server_rtt: 15
server_rtt_packets: 2
server_rtt_sum: 31
src_ip: 104.47.37.78
src_mac: 06:E3:CC:18:AA:33
```

Question 6:

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

Saccharomyces_cerevisiae_patent.docx

Findings



attach_filename{}

1 Value, 25% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
Saccharomyces_cerevisiae_patent.docx	1	100%

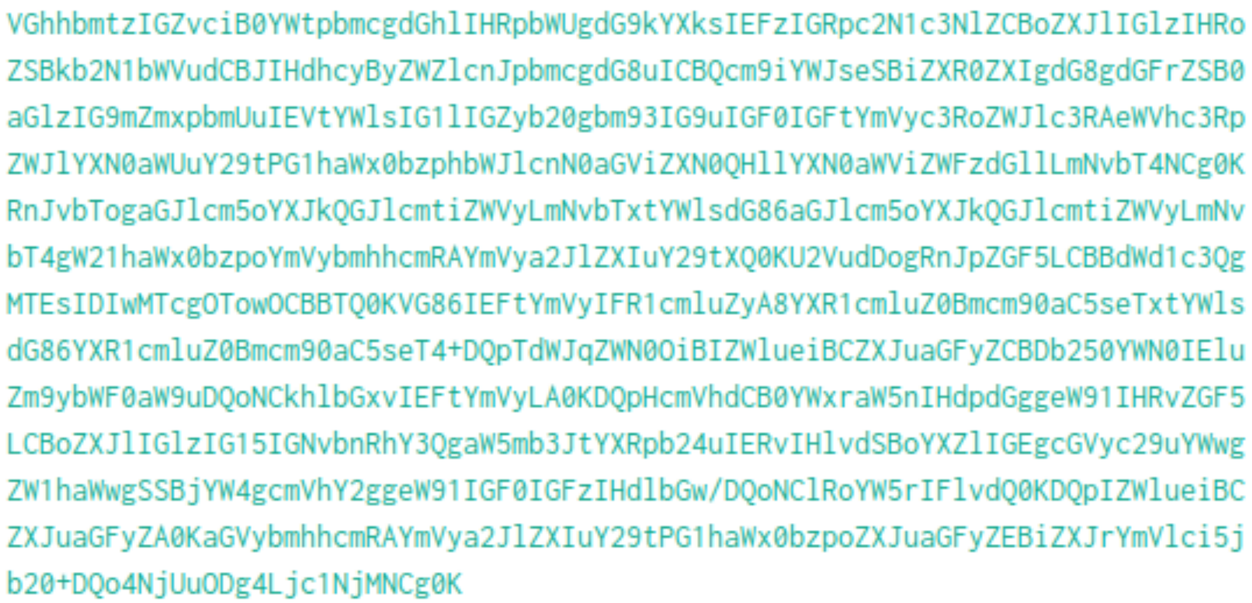
Question 7:

What is Amber's personal email address?

ambersthebest@yeastiebeastie.com

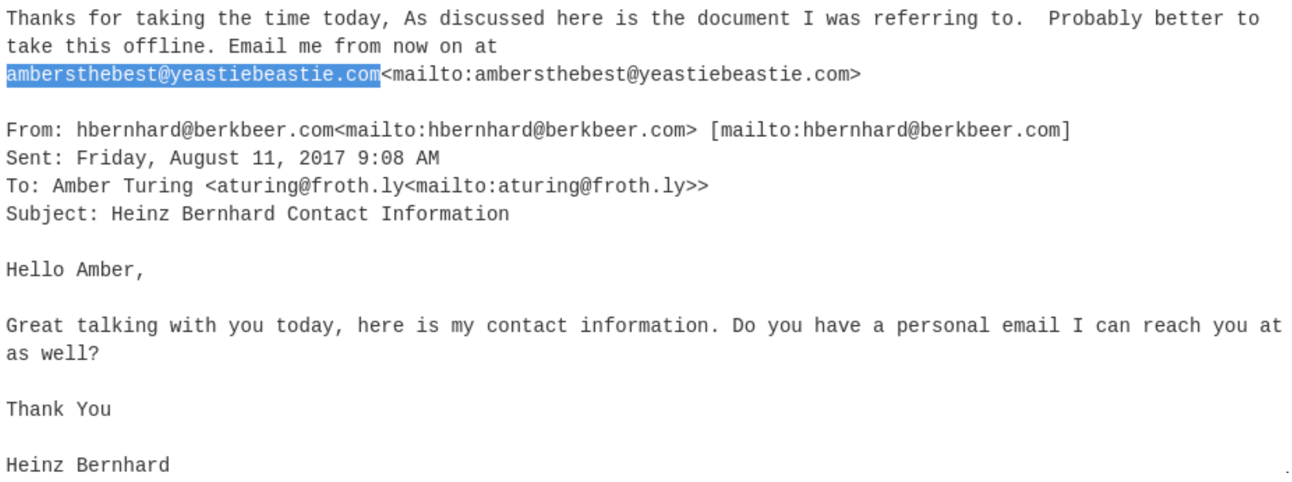
Findings

To respond Amber have encrypted her reply using to base64. Below is a sample of the first part of the actual email.



VGhhbmtzIGZvciB0YWtpbmcgdGhlIHRpbWUgdG9kYXksIEFzIGRpc2N1c3NlZCBoZXJlIGlzIHRo
ZSBkb2N1bWVudCBJIHdhcyByZWZlcnJpbmcgdG8uICBQcm9iYWJseSBiZXR0ZXIgdG8gdGFrZSB0
aGlzIG9mZmxpbmUuIEVtYWlsIG1lIGZyb20gbm93IG9uIGF0IGFtYmVyc3RoZWJlc3RAeWVhc3Rp
ZWJlYXN0aWUuY29tPG1haWx0bzphbWJlcnN0aGViZXN0QHllYXN0aWViZWFzdGllLmNvbT4NCg0K
RnJvbTogaGJlcm5oYXJkQGJlcmtiZWVyLmNvbTxtYWlsdG86aGJlcm5oYXJkQGJlcmtiZWVyLmNv
bT4gW21haWx0bzpoYmVybmhhcmRAYmVya2JlZXIuY29tXQ0KU2VudDogRnJpZGF5LCBBdWd1c3Qg
MTEsIDIwMTcgOTowOCBBTQ0KVG86IEFtYmVyIFR1cm5pbmcgA8YXR1cmluZ0Bmcm90aC5seTxtYWls
dG86YXR1cmluZ0Bmcm90aC5seT4+DQpTdWJqZWN0OiBIZWxueiBCZXJuaGFyZCBDb250YWN0IElu
Zm9ybWF0aW9uDQoNCkhlbGxvIEFtYmVyLA0KDQpHcmVhdCB0YWxraW5nIHdpdGggeW91IHRvZGF5
LCBoZXJlIGlzIG15IGNvbnRhY3QgaW5mb3JtYXRpb24uIERvIHlvdSBoYXZlIGEgcGVyc29uYWwg
ZW1haWwgSSBjYW4gcmVhY2ggeW91IGF0IGFzIHdlbGw/DQoNClRoYW5rIFlvdQ0KDQpIZWlueiBC
ZXJuaGFyZA0KaGVybmhhcmRAYmVya2JlZXIuY29tPG1haWx0bzpoZXJuaGFyZEBiZXJrYmVlci5j
b20+DQo4NjUuODg4Ljc1NjMNCg0K

I have copied the whole encrypted email and paste it in cyberchef "input" converted from base64 and the result was stunning.



```
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
```