The badge was given to me. It has an eye of Horus on it and the symbol H3... The H indicates Human, meaning general admission into Defcon.

I couldn't really understand what this meant and started to feel disappointed that the badge was not electronic. Perhaps the program will say something. Sure enough the second page explains that the badge is part of a reality based puzzle game. It indicates that there are multiple stages with multiple levels of difficulty. I then closed the program and began looking for clues around defcon.

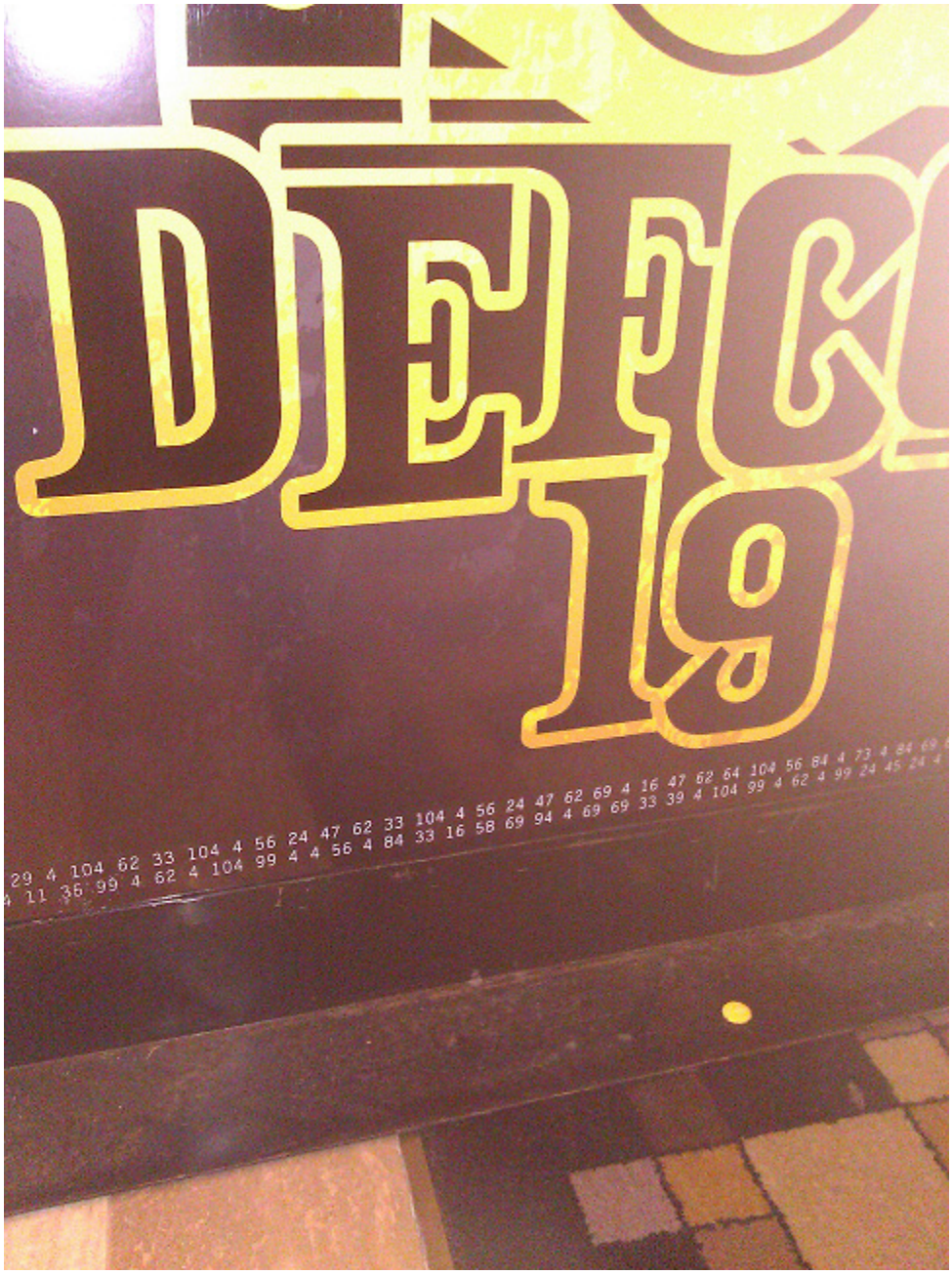
I don’t know if I was just over anxious to be there or not tuned into the world around me but on Thursday I walked around the whole convention center and didn’t spot anything! Haha. So naïve of me.

Friday morning I attended the “Making of the badge” lecture where Lost talks about the process he went through to make the badge. The biggest clues I took away from this are “Lost is narcissistic” and “the signs around Defcon have numbers at the bottom”. There were some others but I don’t remember.

I ran out of there looking for signs in the hallways with numbers on the bottom. While I was looking around I saw this huge image on the ground in the rotunda.

I wrote down all of the number/letter combinations and took photos. The picture above is from the DVD, but the image on the floor was over 25 feet wide. I analyzed this image for a while trying to put every bit of it into memory. I then started walking around the halls looking for posters and signs with clues on them. That's when I stumbled upon this sign:


UP AHEAD
Tracks 3 & 4
Workshops
Dispatch
Q&A 2-4
Info Booth
Hardware Hacking Village
Lockpicking Village
Wireless Village
DEF CON Kids
Speaker Room
Press Room
TO YOUR LEFT
Tracks 1 & 2
Skytalks
TO YOUR RIGHT
Capture the Flag
Contests
DEFCON 19
CONTESTS
DEFCON 19



There’s all these numbers on the bottom of the sign! What’s this! Some king of message!? I quickly wrote them all down which actually started a small crowd of people also doing the same thing and wondering what it says. Even some TV crew from HongKong asked me if they can film me writing this down.

The message had the following numbers:

35 4 24 4 29 4 104 62 33 104 4 56 24 47 62 33 104 4 56 24 47 62 69 4 16 47 62 64 104 46 84 4 73 4 84 69 84 24 24 58 35 64 104 99 64 29 56 24 62 69 4 84 11 35 99 4 62 4 104 99 4 4 56 4 84 33 16 58 69 94 4 69 69 33 39 4 104 99 4 62 4 99 24 45 24 4 69 104 99 47 1 24 11 99 24 62 62 24 62

I then compared each number to the wheel on the floor in the front and a message was soon revealed which said:

WEOENETRATEYOURATEYOURSECURITYLEVELSLOOKWITHINYOURSELFWHERETHEEYELACKSMESSAGETHEREHOBOESTHUDOFHORROR

Cleaned up and looked at we are able to see the following sentence:

"We penetrate your security levels. Look within yourself where the eye lacks message there. - hoboestofhorror."

The last part was garbled! It may have been a password or signature of a person or anagram or acronym. The part about to look within myself for the next clue had me thinking. I thought about something within me, courage, love, strength. Perhaps it was something I couldn't see and that's what it meant as inside me. I thought that the clue will have a message on it or be meaningful. I took the badge off my neck and examined it further. Aha!

The lanyard had a ton of binary digits on it. This is what is meant to look within me. The lanyard has the following markings on it

::1110110000x01:0x11010010100:0110x10010011:1111000x00100:11x1101101000:x101010010000:111x000100001:01101001010x1:001010010x011:0010100x10100:011010x010011:11100x0000101:001010010100x:111010010x100:01001001x0101::1010100010001.1110100000000o.0010100100115.1111000000107.000000000000.000000000000.000000000000.000000000000

That is, there are 15 sets of 13 digits separated by colons, then 7 sets of 12 digits separated by decimals. IPv6 can be ruled out because there are too many sets of colons. Nothing I know of is 13 bits long, or even 12 bits long if the skulls are taken out. Someone told me it's a PEP-8 machine program. More specifically that specific code will square whatever is entered into it. I asked Lost about that and he said that because it's PDP-8 machine code that is just an easter egg and not part of the main line puzzle. This made me think the binary had something else involved with it.

When examining the second set of numbers I thought at first it was an IPv4 address. But again it's 12 bits long, and it's 8 segments long... But wait, it's got the letters at the end 1o57 of the first 4 segments... That spells "LOST" which is the name of the guy who created this puzzle. Hah, this puzzle has been autographed...

I started writing the digits down on paper to try playing around with things. The first thing I attempted looked like this

1110110000x01
0x11010010100
0110x10010011
1111000x00100
11x1101101000
x101010010000
111x000100001
01101001010x1
001010010x011
0010100x10100
011010x010011
11100x0000101
001010010100x
111010010x100
01001001x0101

I went to the info booth and asked for a clue. They told me "The 4th prime number in the fibonocci sequence." Ok I worked it out and that's 13...

Hmm.

Time to look in the manual to see if anything is in there. On page 4 is this cryptic message:

::HACK UPON XYLEM::

Hrm, those colon's may have a connection to the colons on my lanyard. Ok look at that, there's 13 bits on each segment, there's 13 letters in HACKUPONXYLEM and the clue the info booth gave me led to 13. By stacking the segments on top of each other and putting the message at the top. We have this:

```
HACKUPONXYLEM
1110110000x01
0x11010010100
0110x10010011
1111000x00100
```

```
11x1101101000
x101010010000
111x000100001
01101001010x1
001010010x011
0010100x10100
011010x010011
11100x0000101
001010010100x
111010010x100
01001001x0101
```

We looked at that and saw that maybe we are looking at a key so we rearranged the letters in order of the x's. Which resulted in:

LAUNCHKEYNOPMYX

Now that we have the launch key, what do we do with it?

On page 4 of the program was a url: http://defcon.org/1057/xxxx

The x's were really a black marker blocking something out. We tried plugging the launch key nopmyx into the end of the url but got a 404, then we thought it might be a cap sensitive and found that http://defcon.org/1057/NOPMYX did in fact produce the next clue!

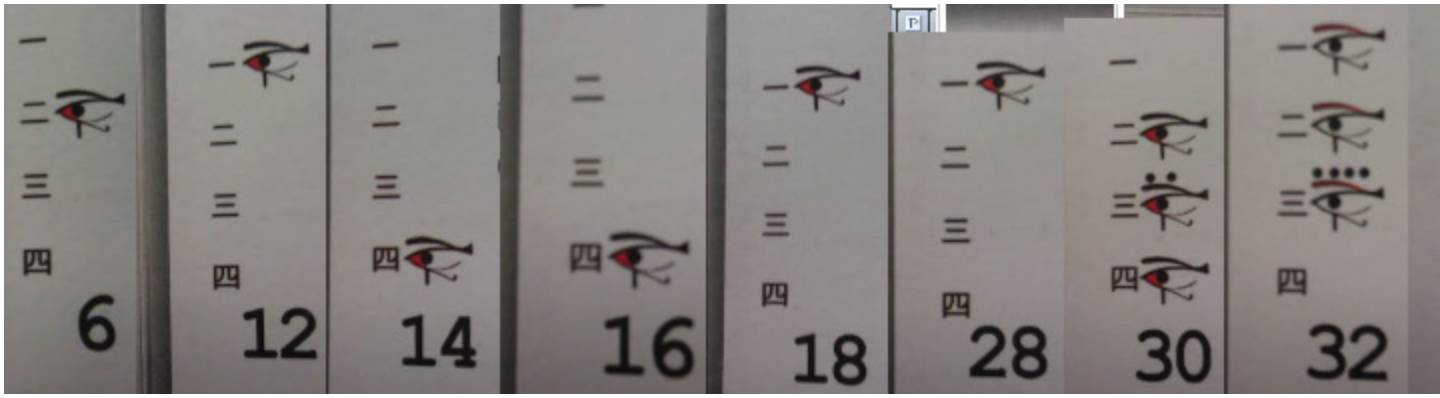
It was a multiple pictures of "Sleeper Agents" or "ZAgents". The bottom of the website says we are supposed to make an exchange with the Zagent and to make it as discrete as possible or they may terminate the conversation.

What message am I supposed to give them? There was this clue that Lost gave saying not all clues are visible and we are seeing a large portion of black on the screen, which looks blank. Upon doing select all we were able to see a secret message!

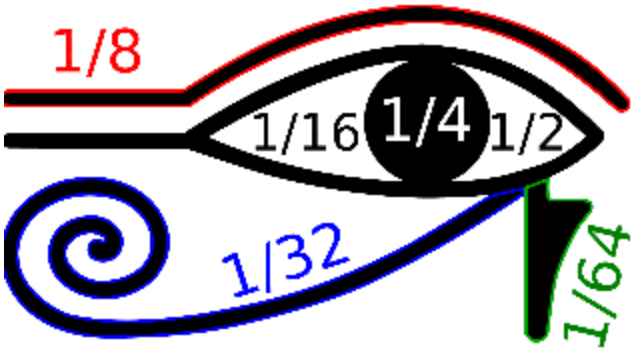
Present an ACE of SPADES to Zagent.
You can *kiss* goodbye mission success if you do not write the password
passed *shortly* before on the face of the card.
Agent will respond with passphrase:
What day is it today?
Proper response to challenge is:
Every day is Halloween.
Agent will confirm:
You're damn right.
Agent will then provide Classification Escalation.

This is all very interesting. We are now given information on what the ZAgents look like and that we are supposed to approach them and give them the password written on an Ace of Spades and then have the coded conversation to confirm. The clues are the word "kiss" and "shortly". We looked all over for a kiss and found one on page 11 of the program. There was a note with a kiss on it. It was written in some scribble, maybe Arabic? But then we saw the second part which said "shortly" and we knew we were looking at shorthand! Damn! Shorthand is super hard to crack. Each little squiggle and curve is meaningful. After asking a dozen or so people how they think we should approach it and after looking online for some help we decide to stop thinking about that for now.

We kept noticing these curious symbols on the bottom of some of the pages in the program. They were little eyes of Ra. Some had red markings on them, some had dots on them. They only appeared on certain pages and we were certain these were a clue. Here are what all the pages with eyes looked like:



The symbols on the left were 1, 2, 3, 4 in Japanese. Not really knowing what to do with this we decided to research the eye. The Wikipedia page says that in ancient Egypt the eye was used in counting. Conveniently enough there was a nice picture of this counting system:



I started writing this stuff down which looked like this:

```
Pg    6   12   14   16   18   28   30   32   36   38   40   46
1 |     1/2          1/2  1/2       1/8
2 |1/2                          1/2  1/8          1/8
```

```
3 |                          1/2 1/8 1/2          1/2
4 |         1/2 1/2          1/2          1/2 1/2
```

When I looked at it like that I decided maybe just doing the math downwards will give something worth while… This looks like this

```
Pg   6  12  14  16  18  28  30  32  36  38  40  46
1 |      6           9  14      4
2 |  3                      15   4           5
3 |                         15   4  13          23
4 |          7   8          15          14  20
```

These numbers don't correspond to the wheel on the floor so maybe they correspond to the alphabet. Where A = 1, B = 2 etc. By using this we now see something emerging…

```
Pg   6  12  14  16  18  28  30  32  36  38  40  46
1 |      F           I   N       D
2 |  C                      O   D           E
3 |                         O   D   R           W
4 |          G   H          O           S   T
```

FIND CODE ODRW GHOST

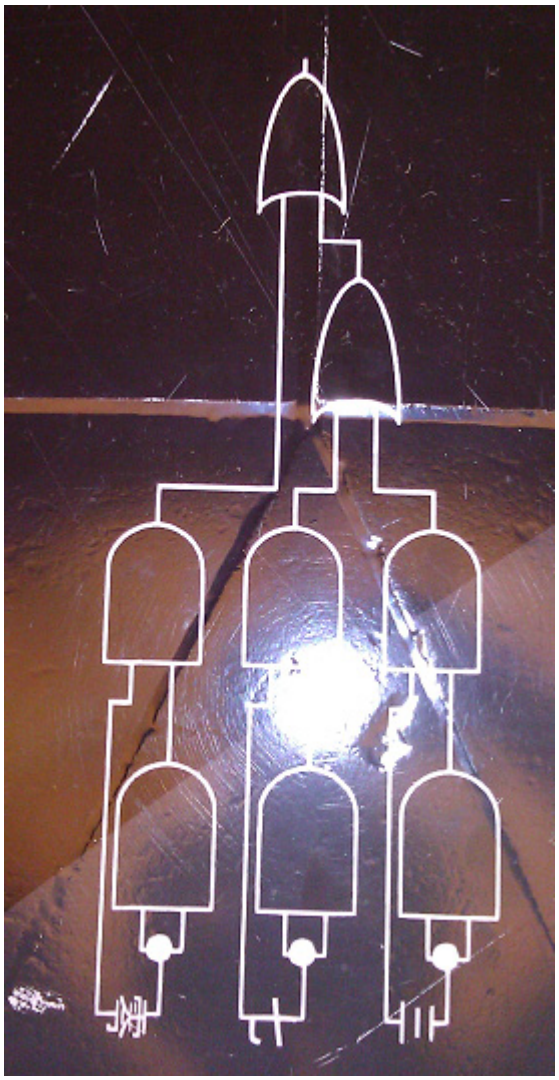
The scrabbled letters in the 3rd word all have those strange dots above them. By arranging the dots in order of 1 dot, 2 dots, 3 dots, 4 dots we have the cracked message:

FIND CODE WORD GHOST

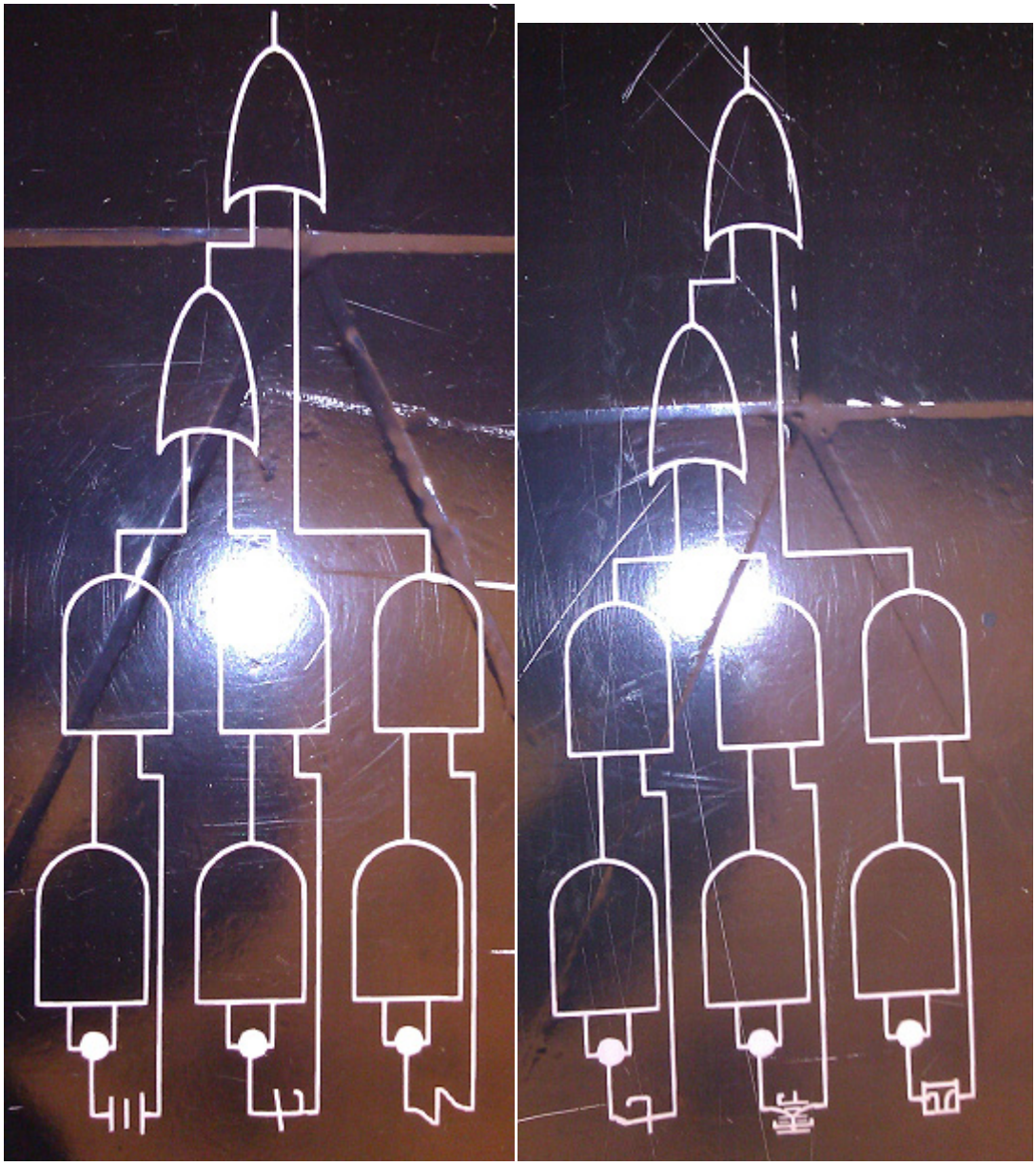
Nice! Now we have to look for ghost. Is that a person? A picture? A movie? The hunt began.

We found another really large circle on the floor at the convention. This one also had symbols which probably are part of a clue.

What hell? Is that a dog? Ok… Anyways if you look closely on the 4 cardinal directions of the image you'll see these markings:




鬼
鬼
鬼



These images show up at the 9 O'clock, 12 O'clock, 3 O'clock and 6 O'clock positions respectfully. We identified that these are logic gates specifically AND and OR gates. There were symbols on the bottom that definitely looked Japanese. Looking around I saw a guy who looked slightly Japanese. I asked him what each of the symbols meant and I wrote it down.

073
Demon Demon Demon
371
704

Demon demon demon!? I asked him more about that symbol. He said it means demon or ghost or monster in Japanese. GHOST!? We found codeword ghost! Great. Now what? It was pointed in a

direction towards the hardware hacking village so I went in that direction looking for more clues. Nothing down there. But I did get to see cool badge hacks down in the HHV. I thought it was very cool that we were able to both be curious about each other. I was curious what some people were doing to add LED's to their badges. They were curious how far along I was with the badge puzzle. People could see that I had pages of notes with badges drawn all over my papers. In fact, I think I personally got at least 10 people interested in solving the badge that weren't previously started.

While I was in the HHV I realized that these guys will know their logic gates and I asked them what they thought of these diagrams. I gave them the numbers with it and we began working it out. We were ANDing and ORing the numbers. Clues just weren't coming out of anything. My notes have truth tables drawn all over them with binary addition and multiplication of each number. I wasn't very good at this and every time I worked out the math I got a different number.

We started to think out of the box. We remember during the making of the badge talk Lost said a clue is that HE is Narcisstic. This had us thinking that maybe Ghost or Demon was a synonym to Narcissist. We started googling around the term Narcissist with Ghost and seeing if we could make a match. It made sense if we were looking for Ghost and it turns out to be Lost then we need to find him! This took us a long time of googling but we finally googled the right term "numbers 037 371 704 narcissistic". It straight up told me "371 is a narcissist number". I hoped that this would be the clue I was looking for so I looked up what exactly a "narcissistic number" is. It specifically is the sum of all the numbers then raised to the power of how many numbers it is (or something like that). Specifically what caught my eye was "there are only 4 of these numbers that exist they are 153, 370, 371, 407." Well 370 and 153 weren't on the floor. But alas! The number on the floor for 037 has it's circuit reversed! So that means it should read 370! That means the only number left is

153

Now that we have the decrypted number for ghost we immediately thought about plugging it into the website:

http://www.defcon.org/1057/153

This is what the website said:

As you seek direction, find the SLEEPER AGENTS. You should know what to do. And what to say. And what to give.
The eye is the key.
We believe you have been compromised.
The relics you hold are believed to be a key, a sequence that unlock truth that has been hidden.
However the sequence has been poisoned.
You must find the flaw!
The ZAGENTS are a clue. FIND THEM.

We then knew we had to crack that shorthand to talk to the Zagents! We searched for shorthand dictionaries and tutorials. We spent a lot of time on this with very little progress. We felt defeated. We started using social engineering to get what we wanted. First we started asking every old person we saw in the casino if they know shorthand. This proved to probably take just as much time as continuing to figure it out ourselves. We decided to work some other contestants to get this information from them. We were able to exchange some information to get it. We learned that the note with the kiss on it said

The password is little sister

We wrote the password on an Ace of Spades and started looking for ZAgents. We also learned that we can confirm they are ZAgents by their badges.
They have a Z on their badge. We spotted one in the vendor area. My partner made the move and executed the exchange flawlessly while I watched his back. The classified information he gave us was:

candy

We thought that this may be used just like the codeword NOPMYX was used. So we went to http://www.defcon.com/1057/candy and sure enough we received the next clue!

Send the phrase : The Jammie Dodger has been eaten.
to
28 14 19 28 39 4 31 28 18 11 36

We searched the webpage for any other secret messages that we couldn't see but didn't really find anything that stood out.

We took the number sequence and began analyzing it. We worked on this piece for hours and hours. Practically all day Saturday and all night I stayed up racking my brain around this. We tried using all of the previous ciphers we found before and any other possible clues we had. We tried Ceasar cipher, modulus, and brute forcing it. We had nothing after a long time. We didn’t even know if it was a phone number, website, email address, address, person or whatever.

We finally got some clues from Lost over twitter:

"Hint : if you have passed a card to z and are stuck- you are now dealing with a OTP. And you have the key"

We learned that in cryptography an OTP is a one time pad. This is a type of cipher and way to hide messages. Now we know we are looking for this and that we have the key... A OTP requires we have a few things, a key, the message and then the algorithm to put these two together. We tried find these things but didn't have luck and a second clue got tweeted.

"The otp info you are looking for is in the program"

Ok, this helps at least. It means we have only 46 pages to examine to find the key. We tried lots of combos and ideas but nothing worked out.

We got another clue over twitter:

"If I SPEAK about the TRACKS that BIG foot left, I might break the LETTEr of the law."

This immediately had us look into the program. In there, each of the speakers had extra big capitol letters for each track description. This lead me to write down all the letters down and got this:

WBDISBPCDFPFTBKPMLAFLKTICSTPFIVSBAVIMSDGHGCUGSBSRSEFAAEJTBHTHSPDBAIDPPWSHCVBDBAH
VBGMTHPMSWWWOBNWAAMAHHSSWBHWWSIDTRNSKSTNPVWJAHOM

This lead us to guess at a few ways to crack this message against this "key".

Eventually we used the one time pad which looked like this

```
Message: 28 14 19 28 39 4 31 28 18 11 36
Key:      W  B  D  I  S B  P  C  D  F  P
Key vals:23  2  4  9 19 2 16  3  4  6 16
Msg-val:  5 12 15 19 20 2 15 25 14  5 20
Decrypte: E  L  O  S  T B  O  Y  N  E  T
```

We looked at the source code of the HTML page and found a space between EL and YN which then looks like this; E LOSTBOY NET. From there we realized we were looking at an email address and emailed the message to them.

The email came back an hour later saying:

We have verified that agents have compromised our communications channel.
You need to identify the compromised H and replace with the Z.
We have verified that there is only one H value that has been compromised.
You may use the SUN/MOON to verify, you do remember how to calculate those, correct?
When you identify the compromised H, analyze and report. The mssage stream will identify for you a name.

Report the identiy here:
____@%LosT 0x2E Organization
Within your message confirm the compromised H, as well as the sum of the moons and stars.

Well this was by far the hardest part to crack. We spent all day Sunday working on it. First we had to gather information about every badge in the entire conference. These were the following badges we found: (H)uman, (C)ontestant, (P)ress, (V)endor, (S)peaker, (G)oon, (U)ber, (Z)agent.
The Uber badge did not have a number on it or the picture of the eye of Horus. All the other badges did have the eye of horus on it. We ran around the entire conference inspecting every badge and photographing every badge. We successfully identified the following unique badges:

C2
H3

H6
H30
H32
H34
Z36
H40
H42
H44
H46
H50
P52
S54
V60

Here are some of the pictures of the badge (unfortunately none of the ZAgents let me take a photo of their badge but it was the same as the human except for a few things. It had a Z instead of an H. It did not have any notches. The eye was facing the other way.

Half way through collecting this info we started realizing that all the H badges had a notch carved in the Human badges which we weren't entirely sure if that was a defect or not. We recorded where the notches were on the badges. We started determining that the notch was in a predictable place! We discovered that the number on the H badge when mod 12 was applied to it would give the number of a clock which the notch was located in that exact same position. We also discovered the H3 badge was curious because it had no notch whatsoever when it was expected to have a notch at the 3 o'clock position. None of the other badges had notches in them.

Since the H3 badge was different than all the others in that it didn't have a notch we determined this was the poisoned badge.

Each badge had the eye of horus on it. We looked up the significance of this and found that when the eye is the right eye it means the sun and when it's the left eye it's the moon.

The note says to send the sum of all the moons and stars. At first we were thrown off because the Goon badge was in the shape of a star and the P, S, V badges were in the shape of a pentagram which is starish shaped. We then realized that the sun is a star!

We emailed a few ideas to the wrong email address and weren't getting anywhere. We didn't know how far along other teams were at this point.

At this stage in the game it was nearing on 4pm on Sunday and all the teams were so desperate to finish the puzzle before having to catch flights or leave town that we grouped up in the chill out room. There were about 40 of us in there all sharing ideas and clues as to what we thought it could be.

We then got a new tweet from 1o57:

The moon can sometimes appear as bright as the sun.

Shortly after he confirmed H3 is the rogue badge.

Shortly after he helped us further by tweeting:

The sun and moon are opposed, kind of. Ra stands opposite Horus.

I stopped Lost in the hall and asked him if I'm close and what I had figured out. He asked me a series of questions which lead to me realizing that when I look at the front of my badge it's a moon and when I look at the back it's a star! Just reversing the eye is all that it was doing but it meant my badge was both a moon and a star!

He then tweeted: The dial is a sequence. It has a name. So do the badges.

The dial he speaks of is on the floor in the main rotunda. It was a circle with an outer wheel of numbers and an inner wheel of corresponding letters. Every letter was there except for Z. We found out after some googling that the wheel uses the Aronson's sequence for the numbers. This means that the number Z should be the number 111.

I took a look at all my data and since there was a “moon” on all of the badges then I added them all up. Since when you turn the badge around it becomes a sun then I doubled that number. We emailed that number but got back an “incorrect” in an email.

We then put all the badges together to see if there was a sequence there. It didn't match any. So we started thinking H3 badge didn't belong and sure enough found a sequence that omitted the number 3! It was called the Eban sequence. The Eban sequence goes like this:

2, 6, 30, 32, 34, 36, 40, 42, 44, 46, 56, 52, 54, 56, 60

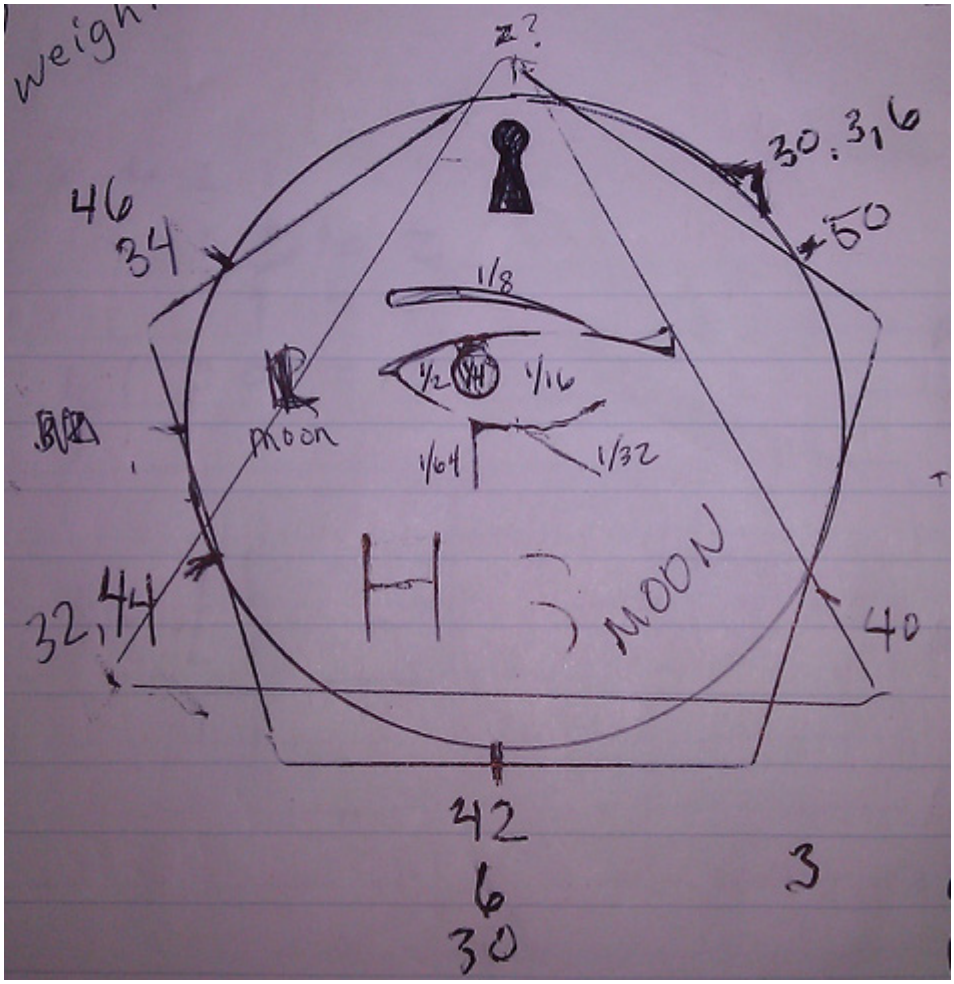
There is no 3, so the H3 badge should really be H56, but since the message said to replace the H3 badge with the Z badge then really the Z badge should have been 56 and the H3 badge should really have been H36.

Now my final tally that I emailed before is different so I adjusted with the new 56 and took out the 3. This email came back as incorrect also.

About now another tweet came over saying:

Sun is position, directly. Moon is position, directly. Every H has a sun and a moon.

Well well well, now it sounds like those little notches we found on all the badges are coming into play. Here is a diagram of all the badges I was able to trace and find where the notch was.



We counted how many times each time a badge was on each hour on the clock.

2 + 4 + 6 + 6 + 6 + 8 + 8 + 10 + 10 = 60

We then flipped this entire chart over we made and did the same for the inverse.

2 + 2 + 4 + 4 + 6 + 6 + 6 + 8 + 10 = 48

We added the two together and got 108.

Now that we have the number we had to figure out what email address. The clue once again looks like this:

____@%LosT 0x2E Organization

The email we used earlier was “lostboy.net”, this one is .org so it can’t be that. Lost’s twitter account says he owns ten-five-seven.org so we assumed that must be it. The name we decided must be the name of the badge sequence eban.

Upon emailing him the number 108 we got back something like:

Infiltration successful! Congratulations on completion of the badge puzzle.

With a tweet soon after from 1o57:

Group has successfully completed the badge puzzle.

We all cheered and gave each other a round of high fives and felt really good about finishing this whole thing up. Our entire group was presented with the black badge during the closing ceremony. There were about 30 of us total and only received 1 badge so were not sure what to do with it yet.

Oh and if you were wondering about the original jumbled message on the signs that read:

"We penetrate your security levels. Look within yourself where the eye lacks message there. - hoboestofhorror."

The end was an anagram which turned out to be:

"We penetrate your security levels. Look within yourself where the eye lacks message there. – Brotherhood of Horus"