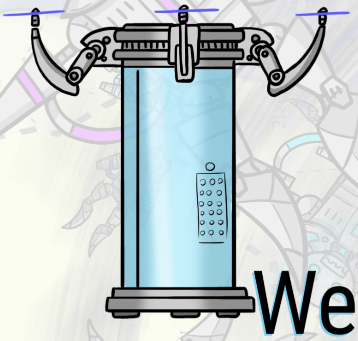
OASIS

CyberDetective

COMIC PART 1 OF 6



PART 1/6

Welcome to the World of Oasis where its inhabitants are kept safe by the technology they surround themselves with as they try to rebuild their lives. In this episode the detective gets a new job.

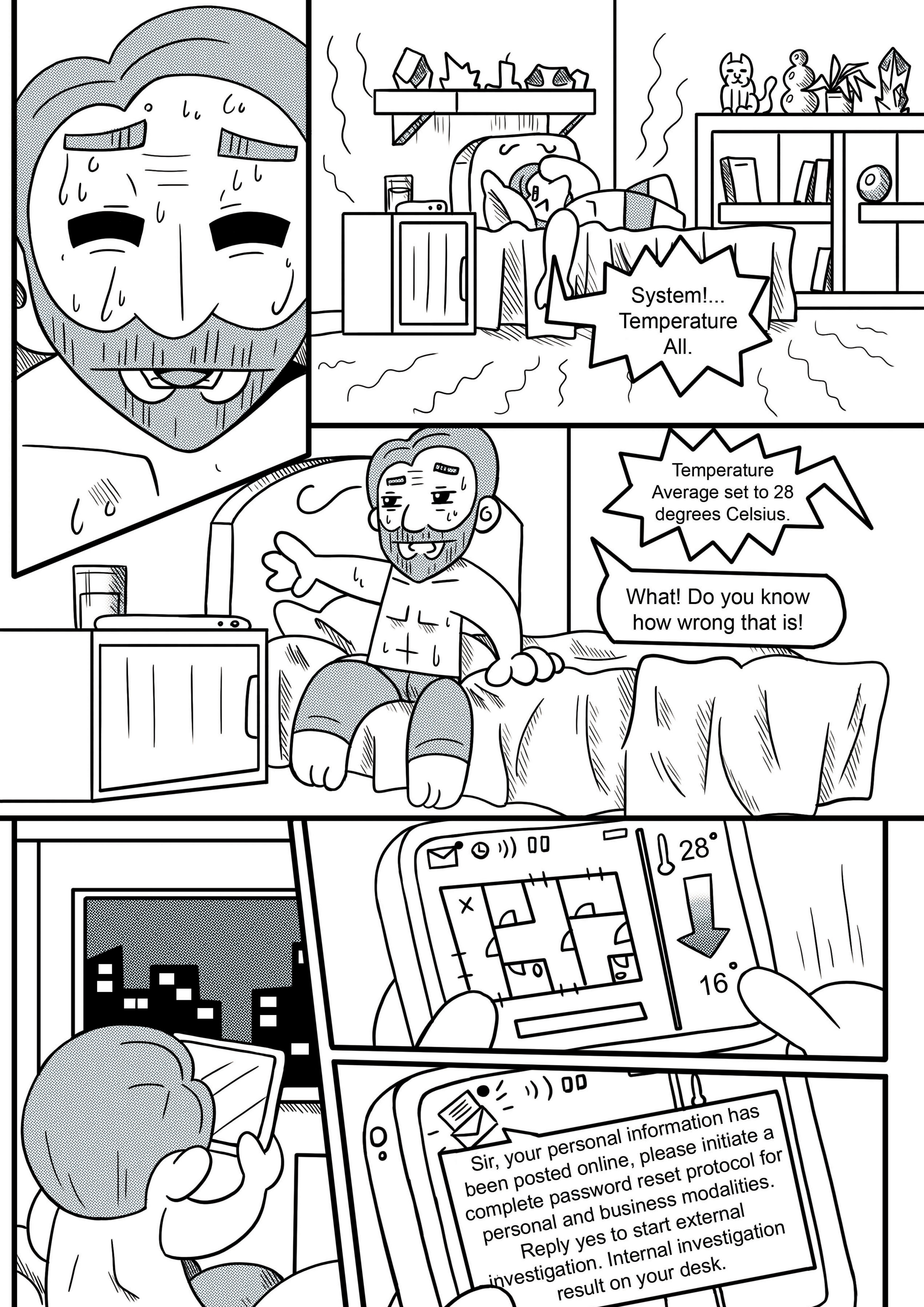
Chief Editor &
Transmedial Producer:
Vincent "South-Blessed" Baidoo
Artist: Connor Rawlings
Front Cover: Jonathan Tonello
Writer: Vincent Baidoo
Editor: Niki Baidoo
Writer & Researcher: Patrick Shortis
Extra Art: Vladimir Rikowski, Francisco Ruiz
Special Thanks: Jeremy Charles, Tomas Hall

CyBOK
CROWNROOT publications

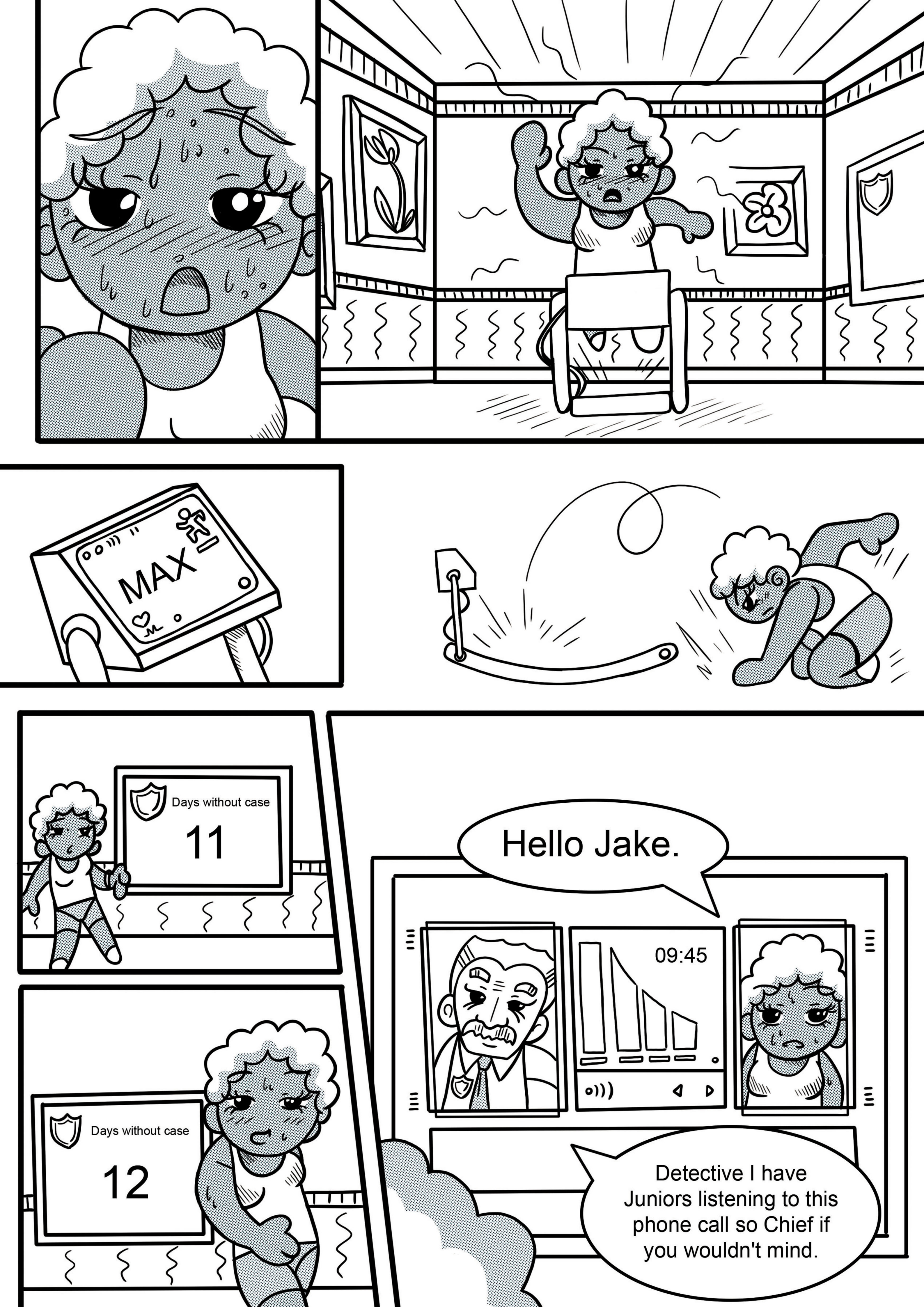
University of BRISTOL
UKRI Research England

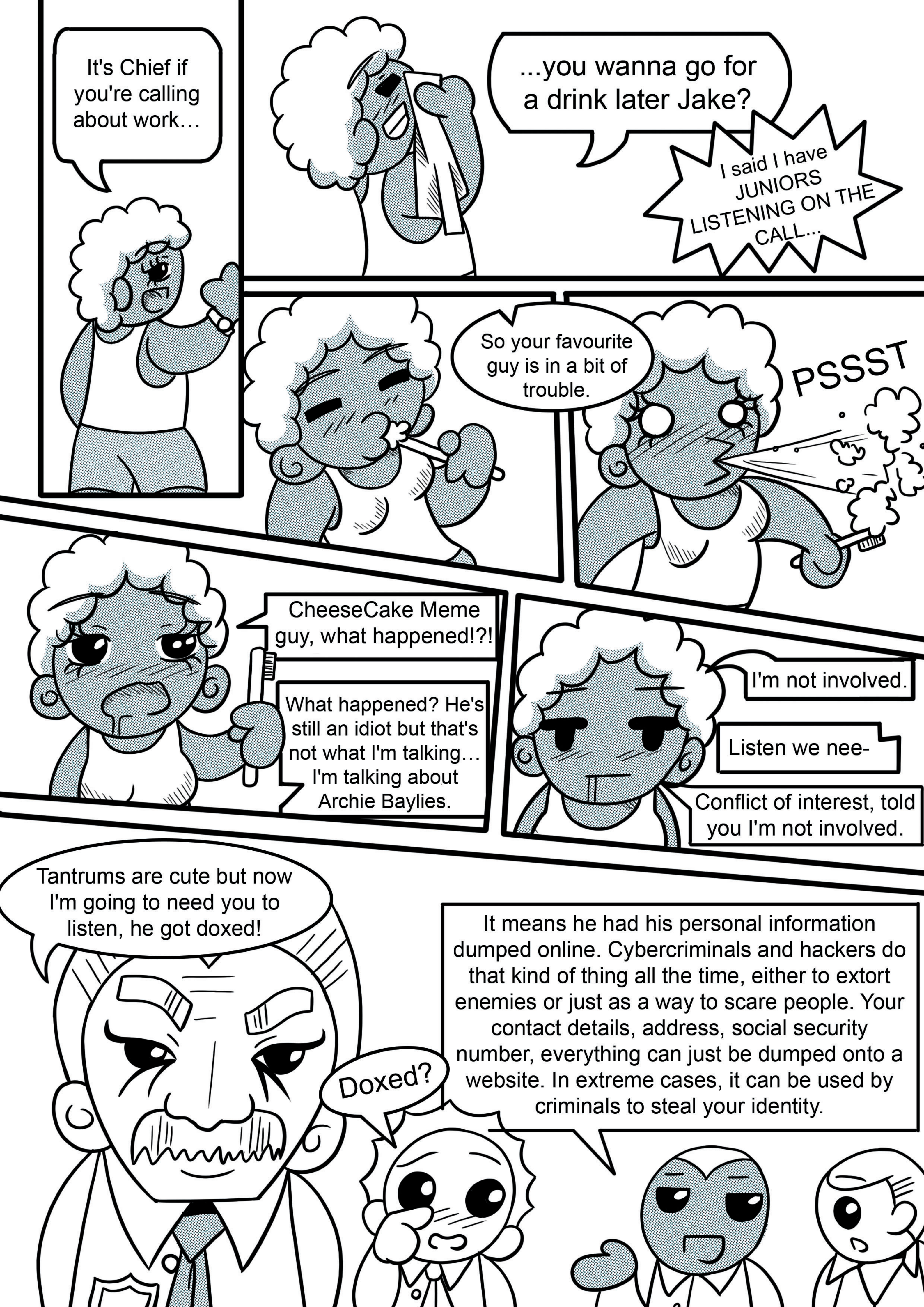
THIS PUBLICATION IS A RESULT OF CYBOK AND CROWNROOT PUBLICATIONS FUNDED BY BRISTOL UNIVERSITY AND RESEARCH ENGLAND UNDER THE CC-BY-NC COPYRIGHT LAWS.

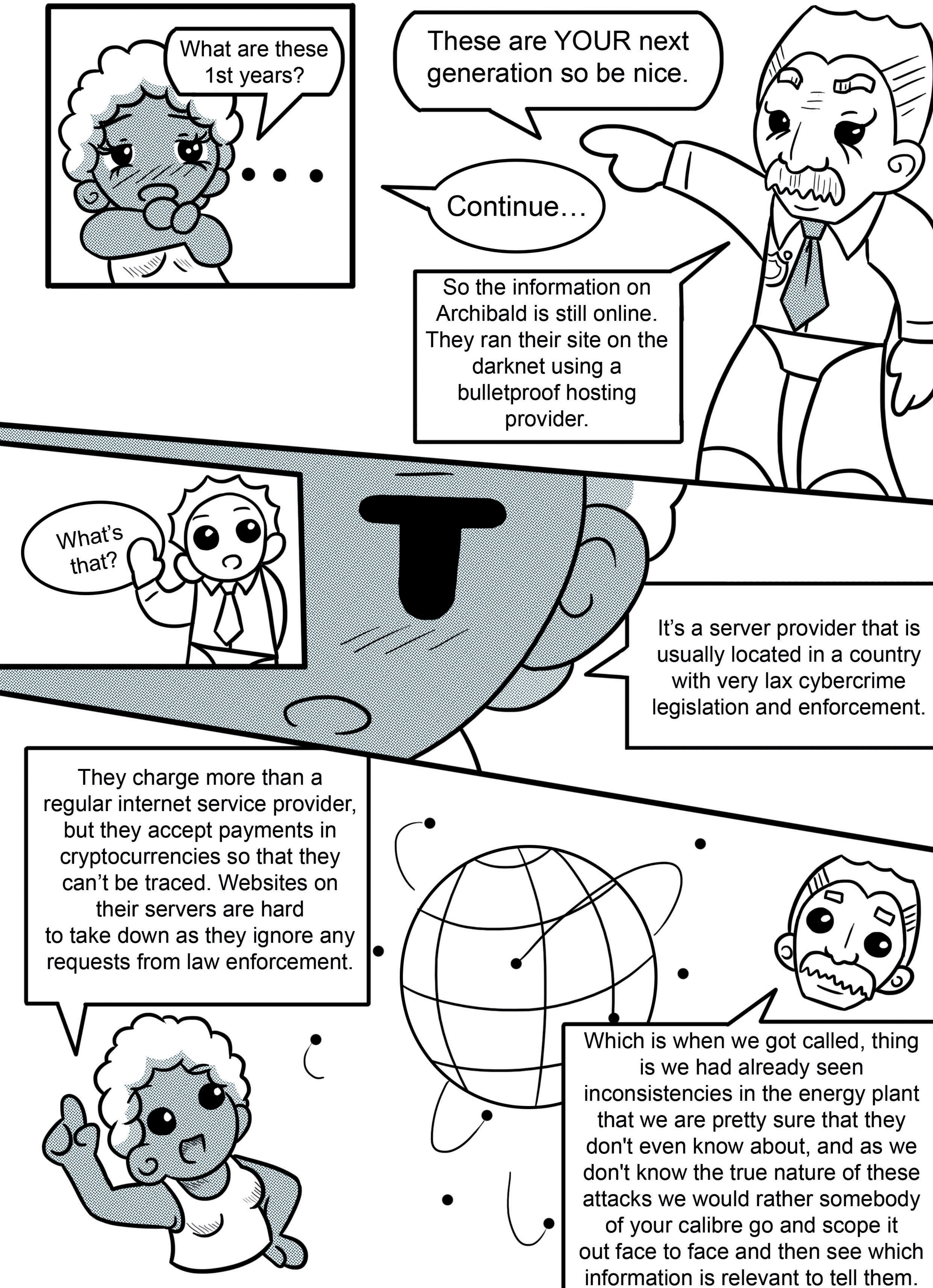
ANY RESEMBLANCE TO ACTUAL PERSONS, OR ACTUAL EVENTS IS PURELY COINCIDENTAL.

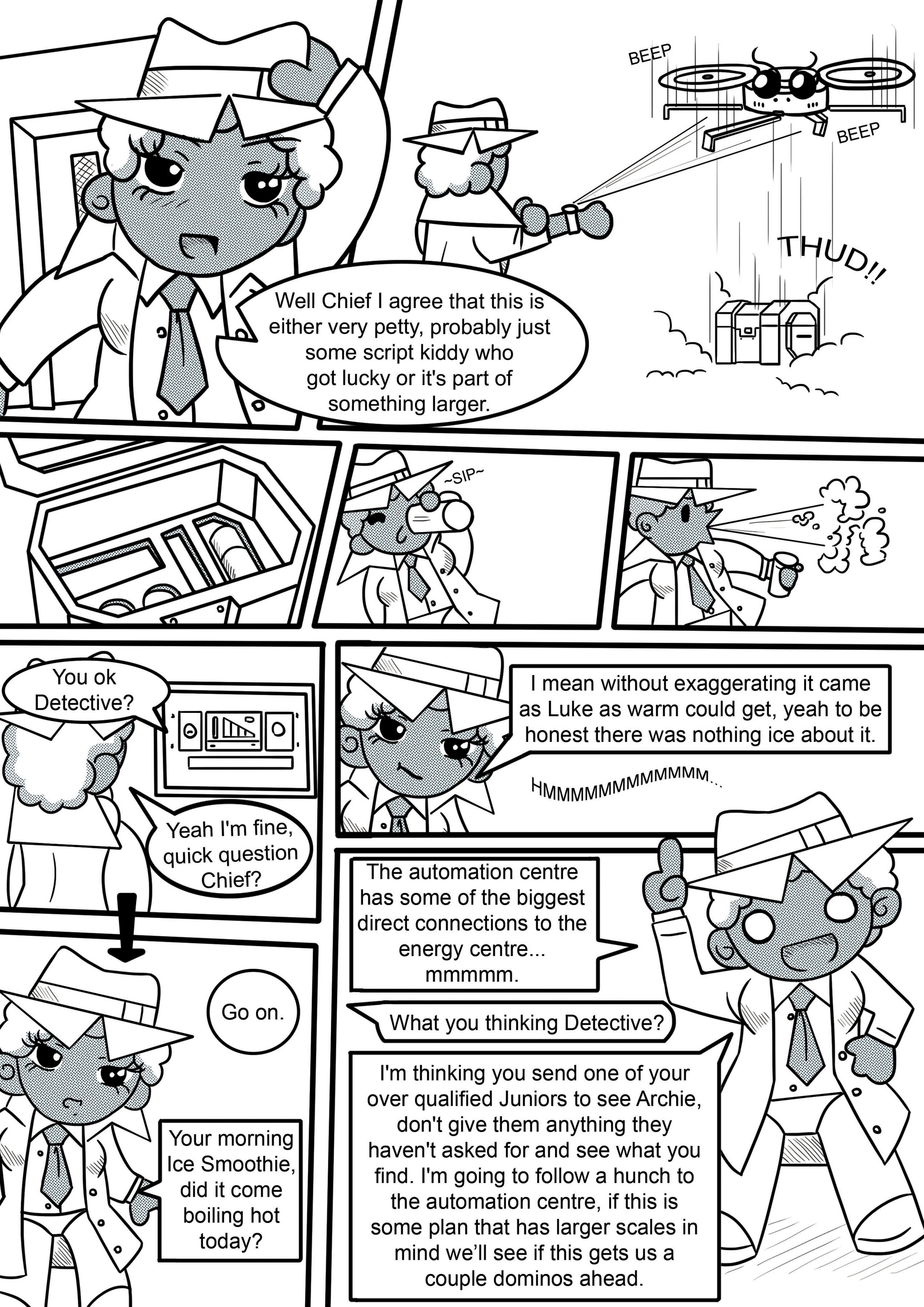

System!... Temperature All.
Temperature Average set to 28 degrees Celsius.
What! Do you know how wrong that is!
28°
16°

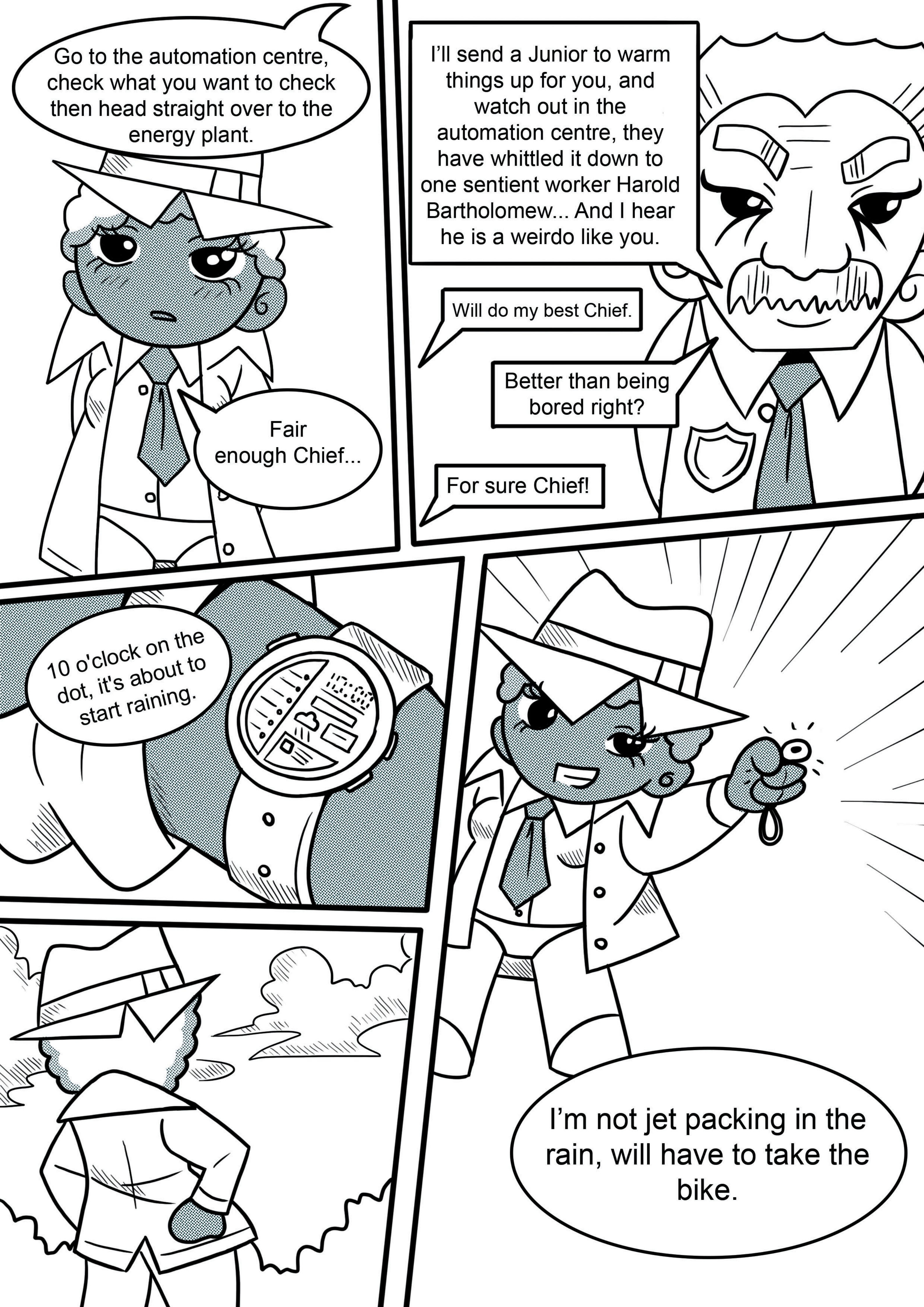
Sir, your personal information has been posted online, please initiate a complete password reset protocol for personal and business modalities. Reply yes to start external investigation. Internal investigation result on your desk.

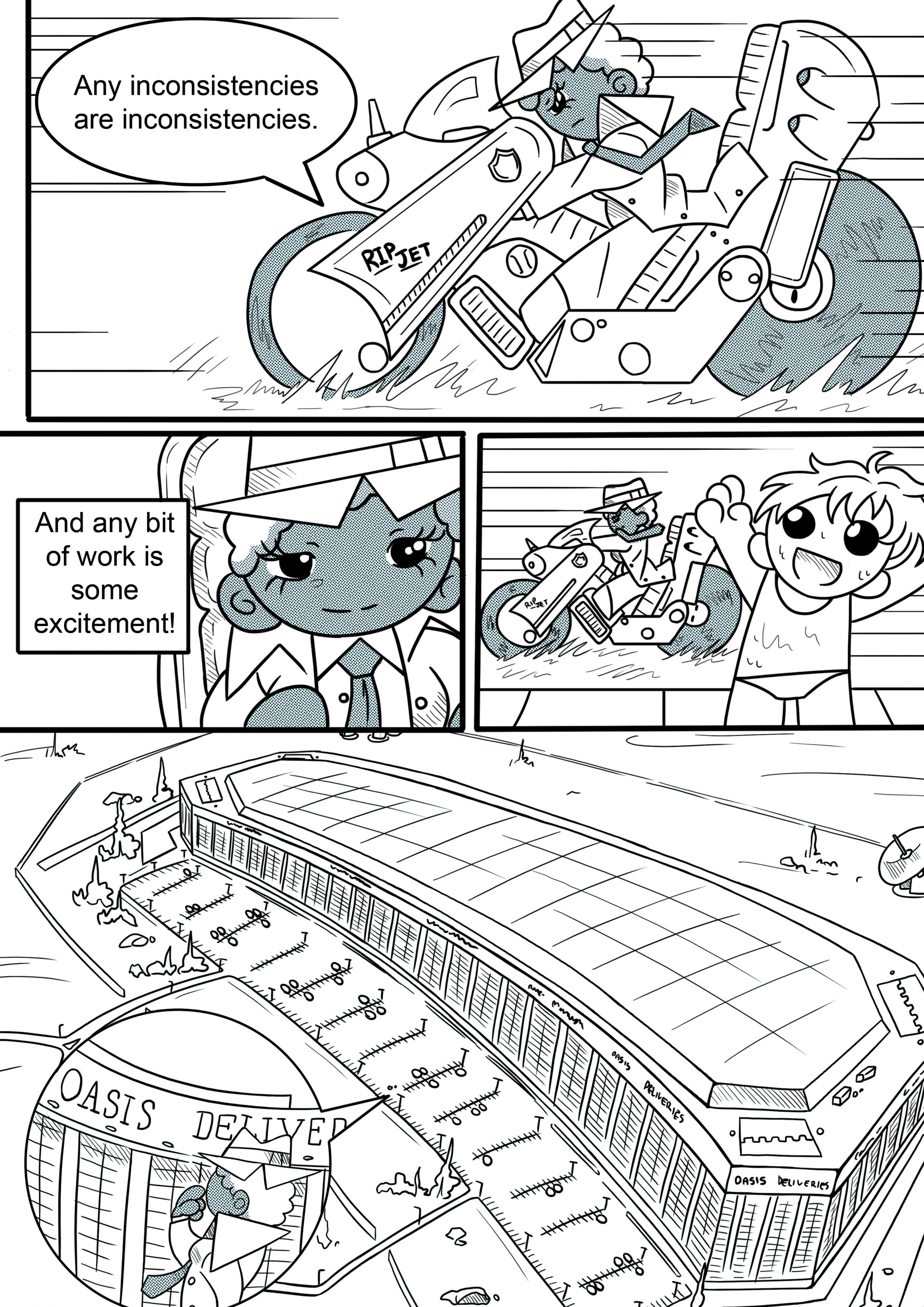

MAX
Days without case
11
Days without case
12
Hello Jake.
09:45
Detective I have Juniors listening to this phone call so Chief if you wouldn't mind.

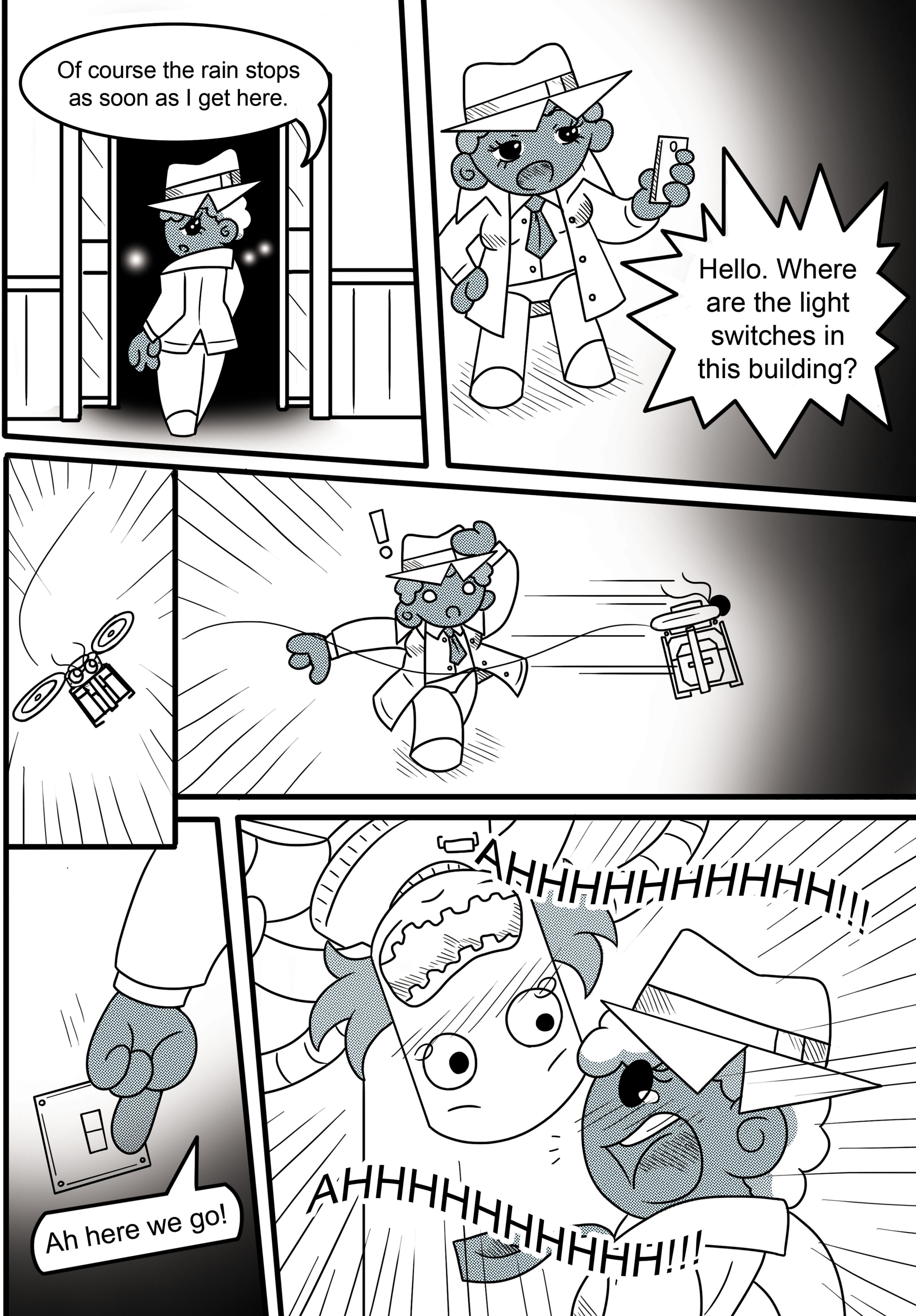

It's Chief if you're calling about work…
...you wanna go for a drink later Jake?
I said I have JUNIORS LISTENING ON THE CALL...
So your favourite guy is in a bit of trouble.
PSSST
CheeseCake Meme guy, what happened!?!
What happened? He's still an idiot but that's not what I'm talking… I'm talking about Archie Baylies.
I'm not involved.
Listen we nee-
Conflict of interest, told you I'm not involved.
Tantrums are cute but now I'm going to need you to listen, he got doxed!
Doxed?
It means he had his personal information dumped online. Cybercriminals and hackers do that kind of thing all the time, either to extort enemies or just as a way to scare people. Your contact details, address, social security number, everything can just be dumped onto a website. In extreme cases, it can be used by criminals to steal your identity.

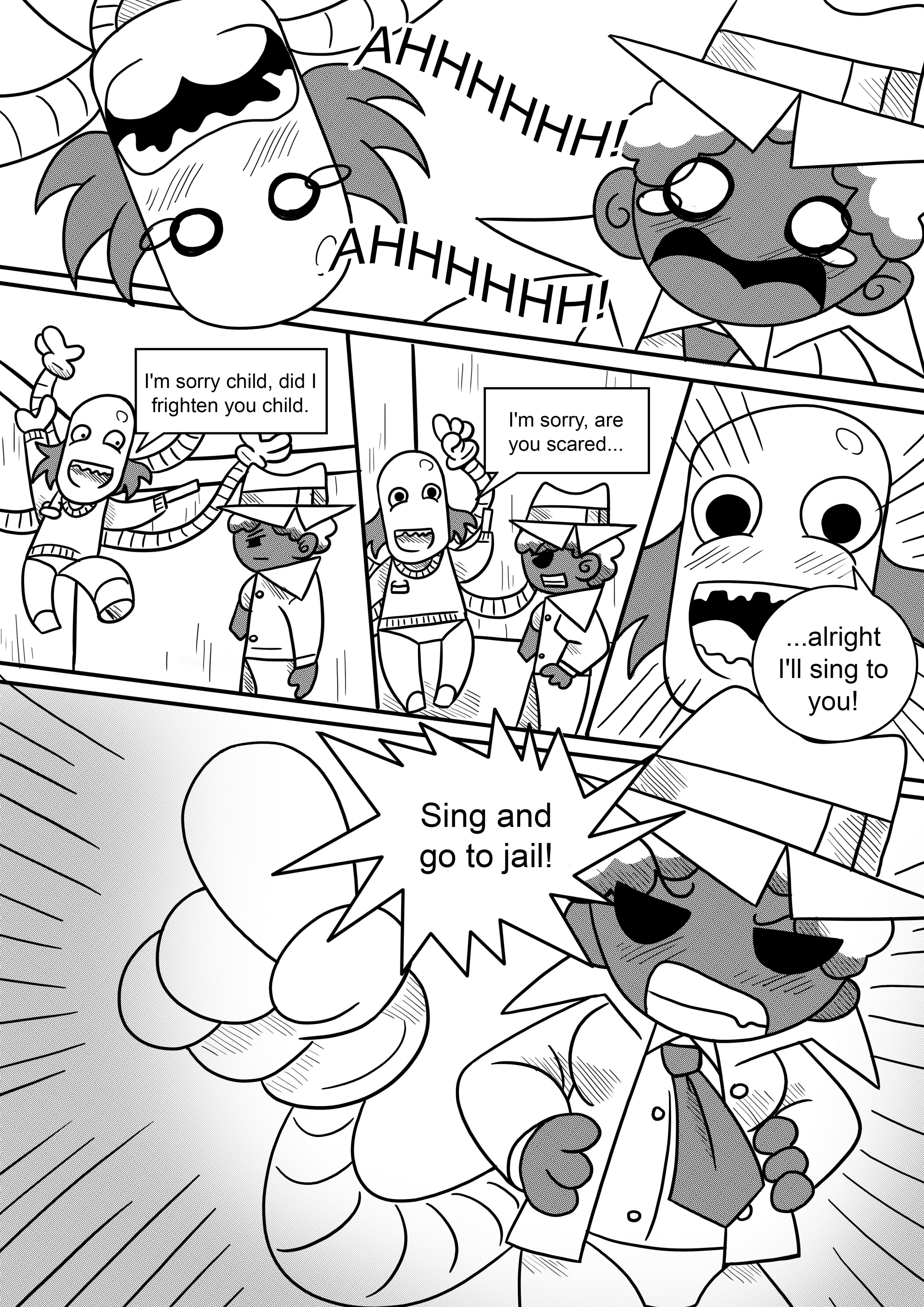

What are these 1st years?
. . .
These are YOUR next generation so be nice.
Continue…
So the information on Archibald is still online. They ran their site on the darknet using a bulletproof hosting provider.
What's that?
It's a server provider that is usually located in a country with very lax cybercrime legislation and enforcement.
They charge more than a regular internet service provider, but they accept payments in cryptocurrencies so that they can't be traced. Websites on their servers are hard to take down as they ignore any requests from law enforcement.
Which is when we got called, thing is we had already seen inconsistencies in the energy plant that we are pretty sure that they don't even know about, and as we don't know the true nature of these attacks we would rather somebody of your calibre go and scope it out face to face and then see which information is relevant to tell them.

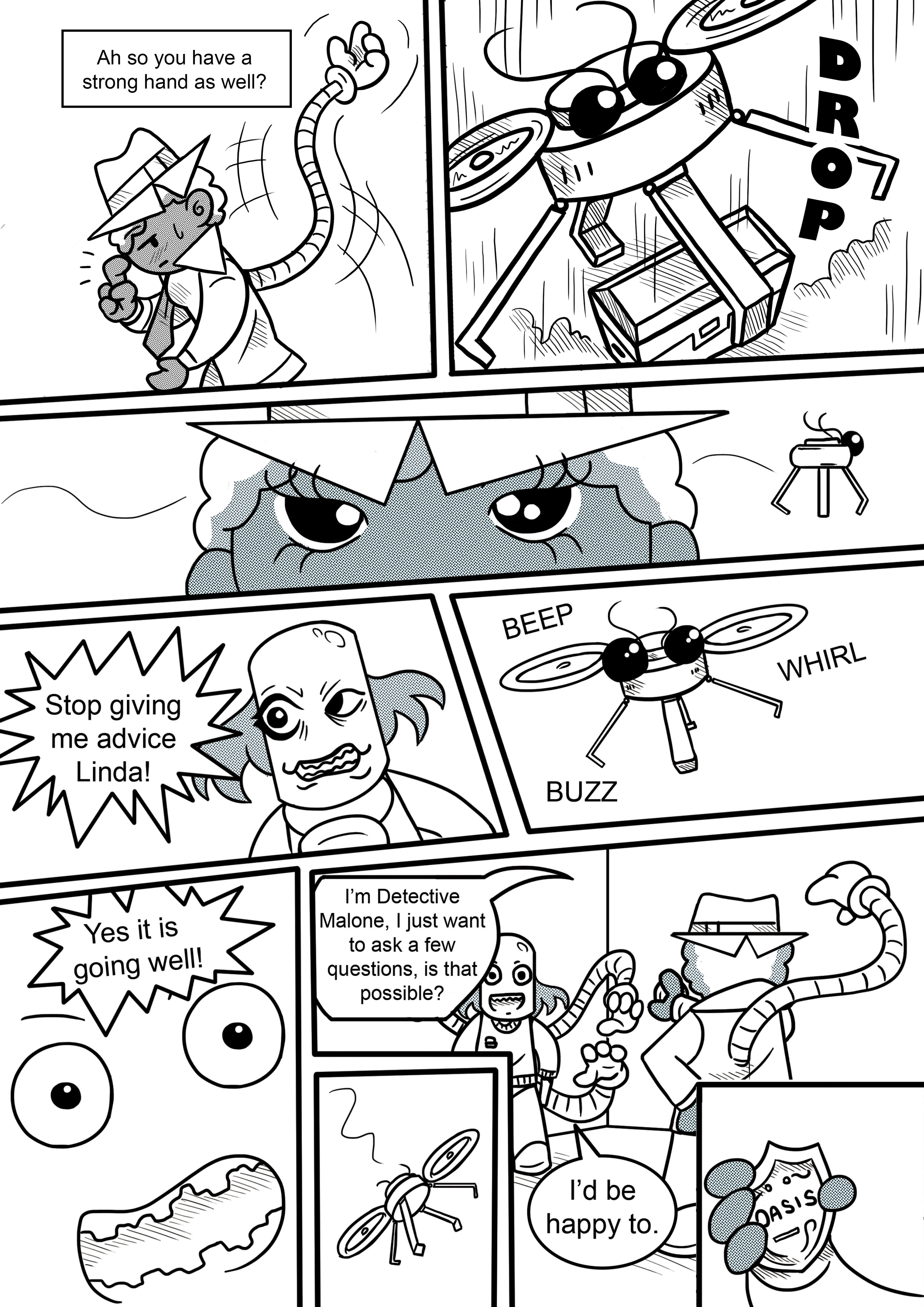

Well Chief I agree that this is either very petty, probably just some script kiddy who got lucky or it's part of something larger.
BEEP
BEEP
THUD!!
~SIP~
You ok Detective?
Yeah I'm fine, quick question Chief?
I mean without exaggerating it came as Luke as warm could get, yeah to be honest there was nothing ice about it.
HMMMMMMMMMMMM...
Go on.
Your morning Ice Smoothie, did it come boiling hot today?
The automation centre has some of the biggest direct connections to the energy centre... mmmmm.
What you thinking Detective?
I'm thinking you send one of your over qualified Juniors to see Archie, don't give them anything they haven't asked for and see what you find. I'm going to follow a hunch to the automation centre, if this is some plan that has larger scales in mind we'll see if this gets us a couple dominos ahead.

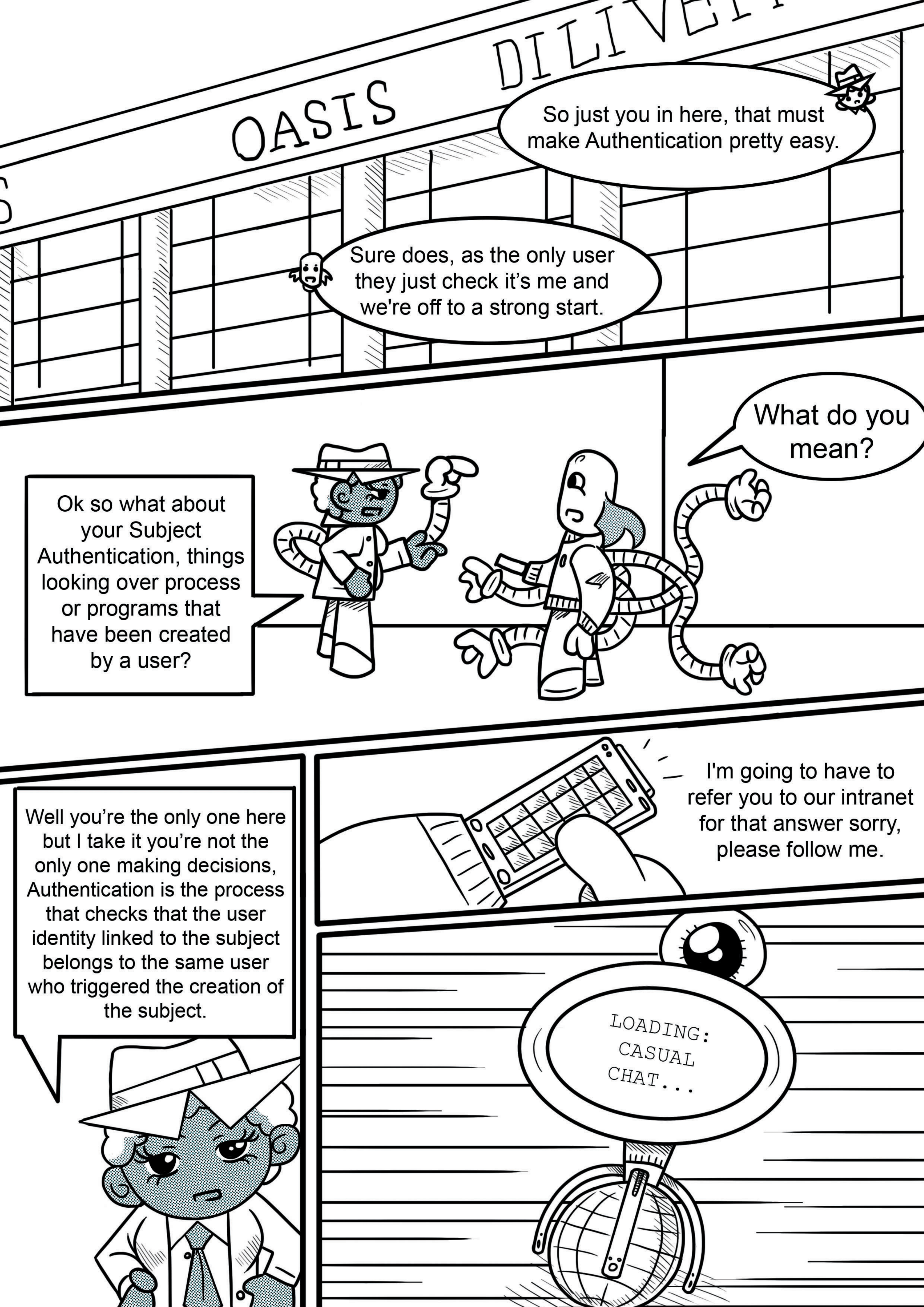

Go to the automation centre, check what you want to check then head straight over to the energy plant.
Fair enough Chief...
I'll send a Junior to warm things up for you, and watch out in the automation centre, they have whittled it down to one sentient worker Harold Bartholomew... And I hear he is a weirdo like you.
Will do my best Chief.
Better than being bored right?
For sure Chief!
10 o'clock on the dot, it's about to start raining.
I'm not jet packing in the rain, will have to take the bike.

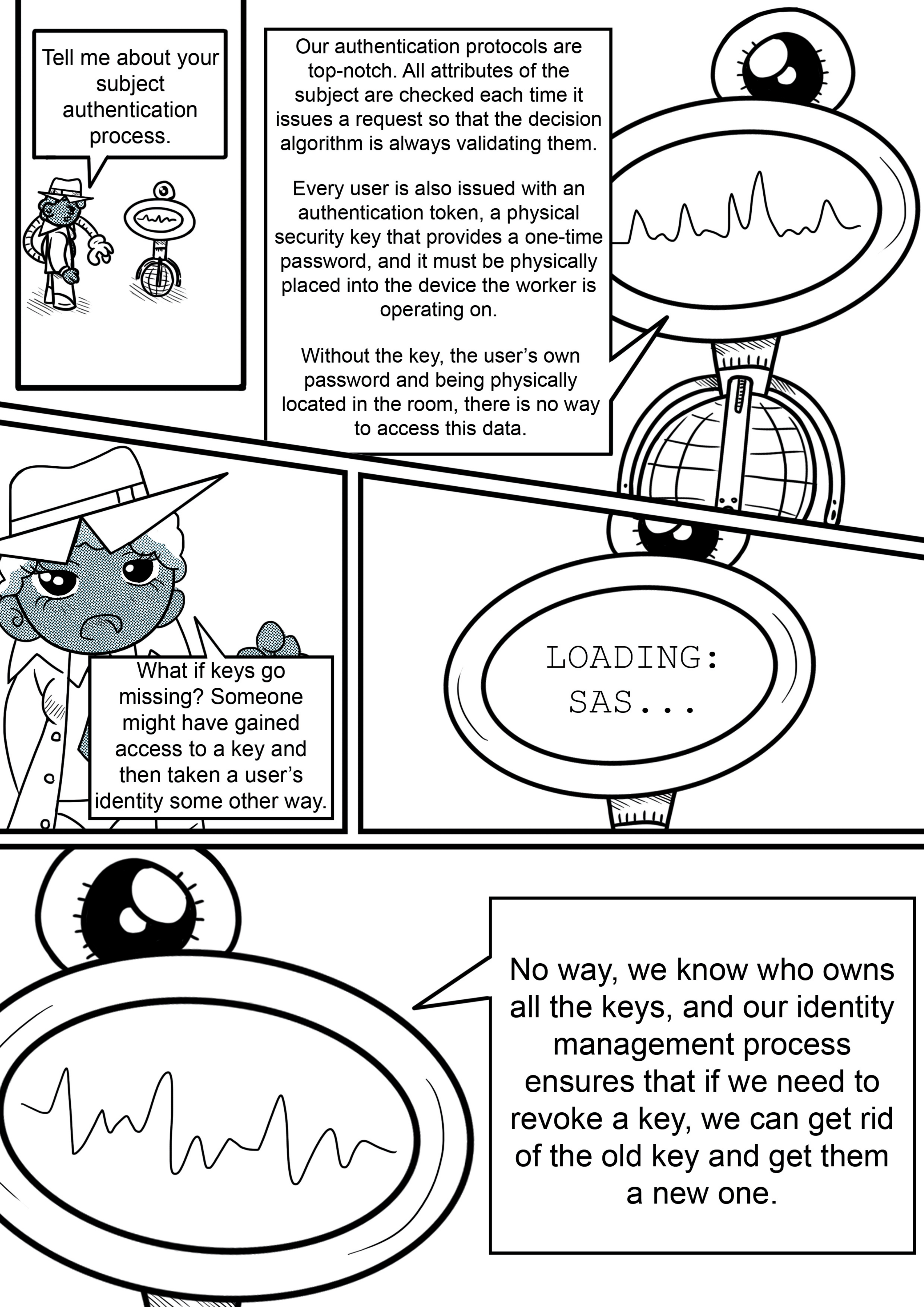

Any inconsistencies are inconsistencies.
RIP JET
And any bit of work is some excitement!
RIP JET
OASIS DELIVERIES
OASIS DELIVERIES
OASIS DELIVER

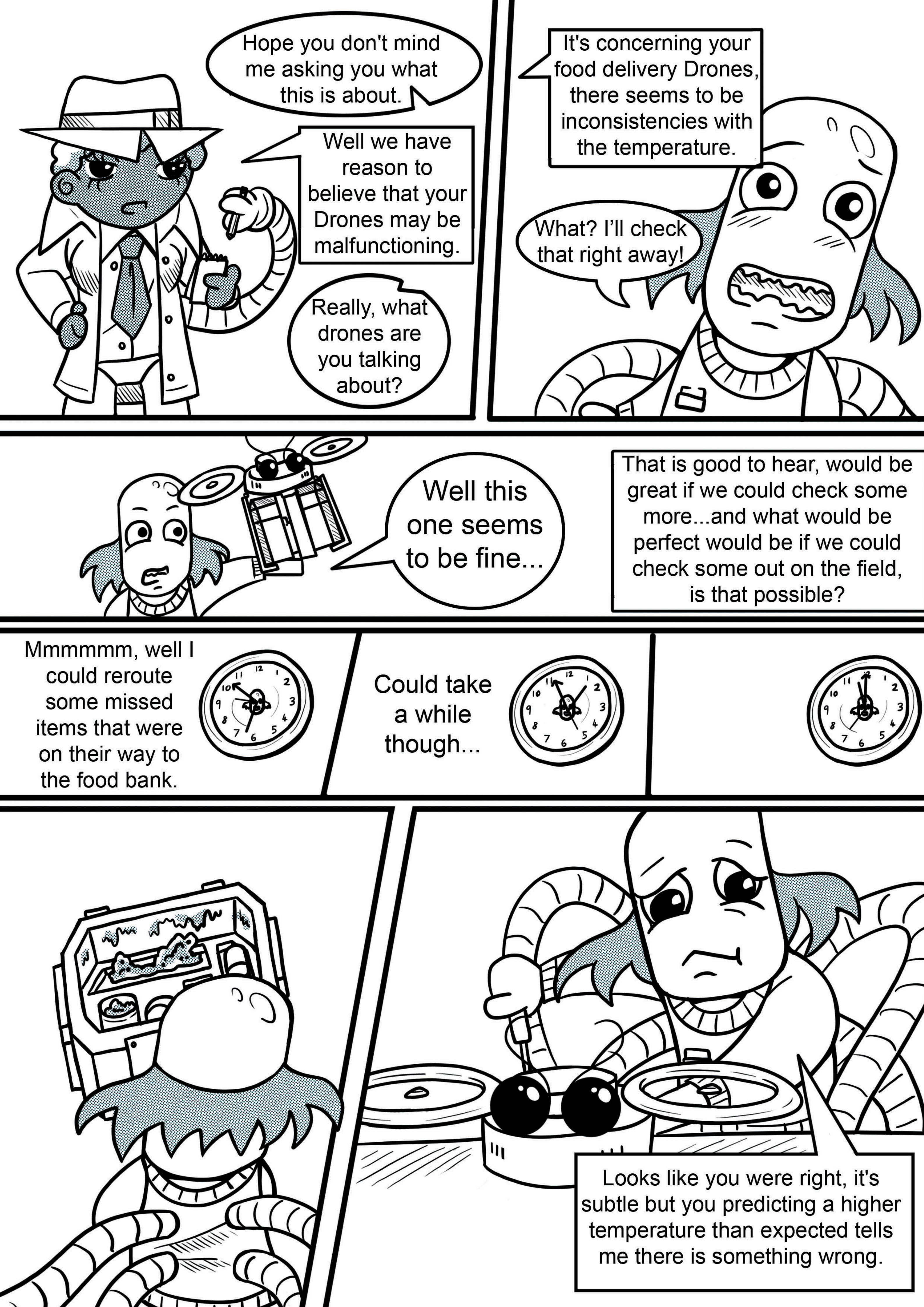

Of course the rain stops as soon as I get here.
Hello. Where are the light switches in this building?
!
Ah here we go!
AHHHHHHHHHH!!!
AHHHHHHHHHH!!!

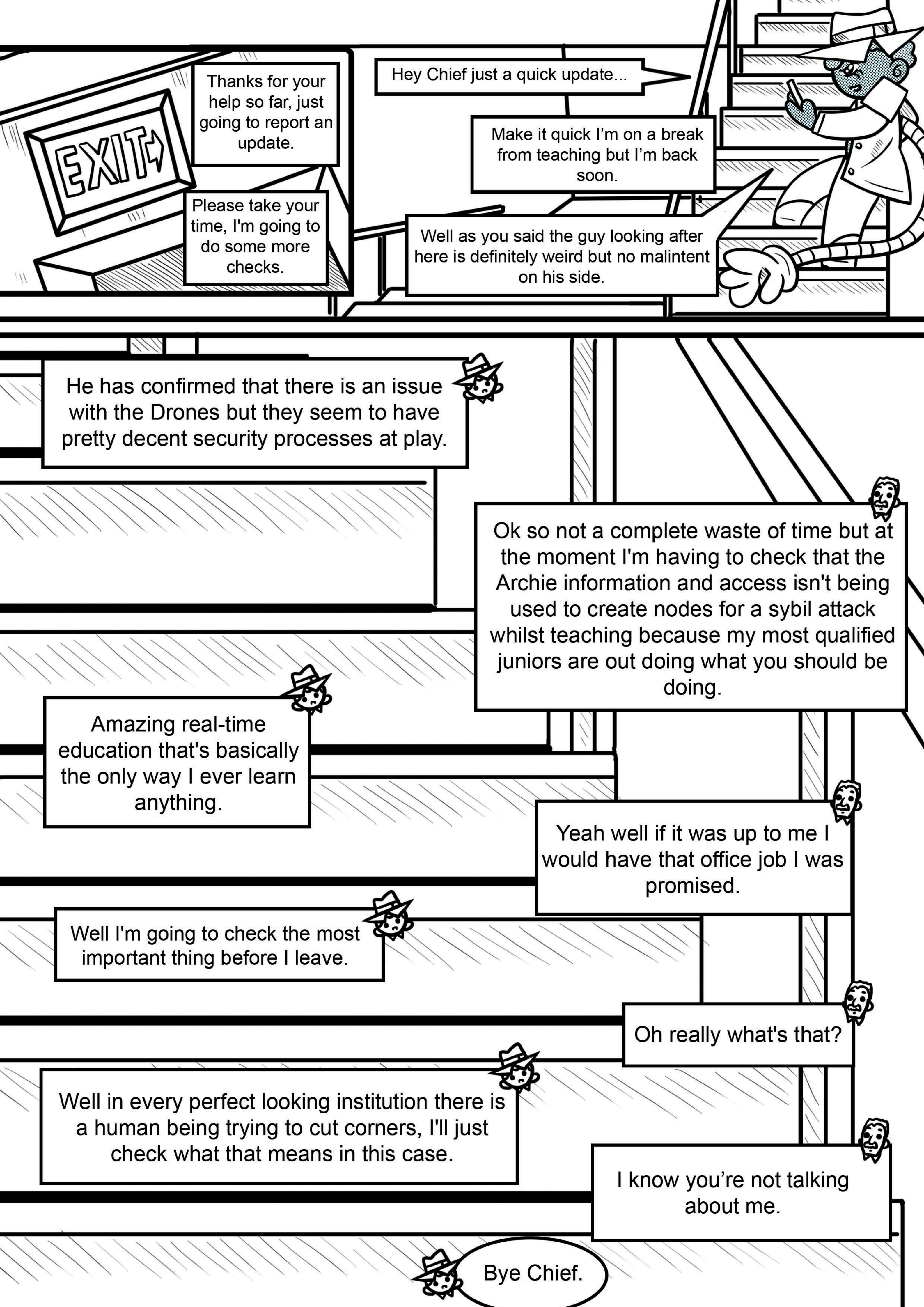

AHHHHHHH!
AHHHHHHH!
I'm sorry child, did I frighten you child.
I'm sorry, are you scared...
...alright I'll sing to you!
Sing and go to jail!

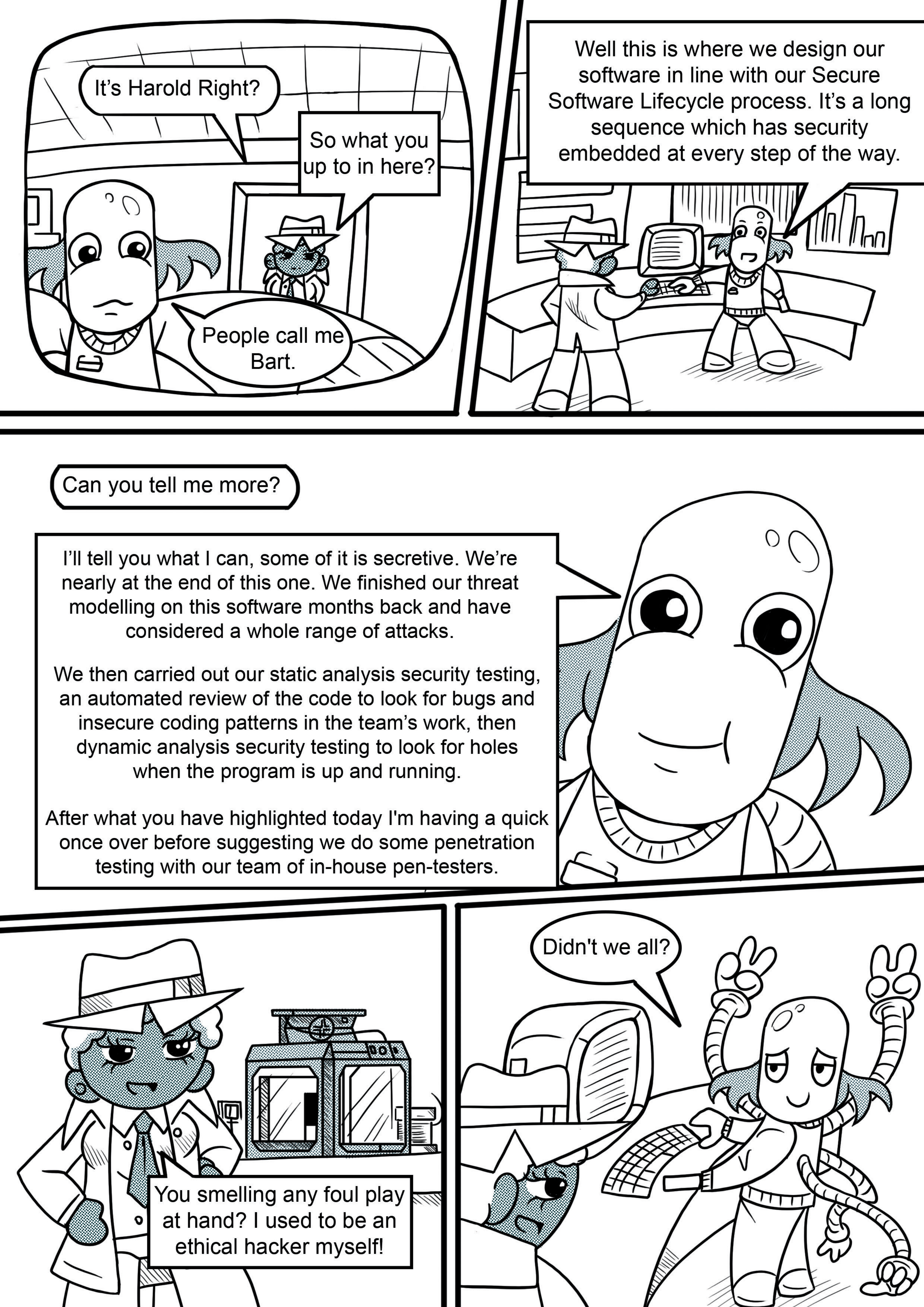

Ah so you have a strong hand as well?
DROP
Stop giving me advice Linda!
BEEP
WHIRL
BUZZ
Yes it is going well!
I'm Detective Malone, I just want to ask a few questions, is that possible?
I'd be happy to.
OASIS

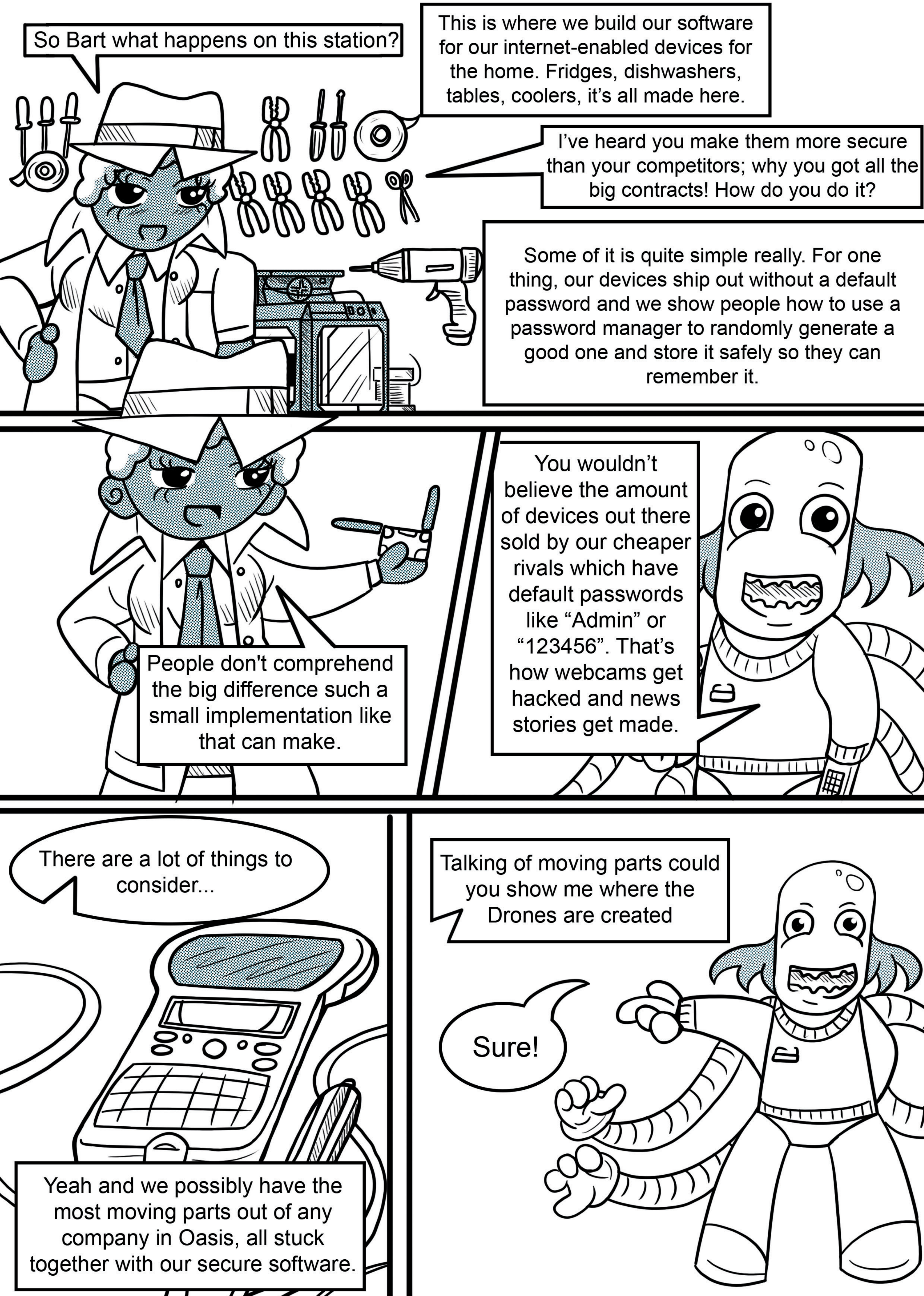

OASIS DILIVE
So just you in here, that must make Authentication pretty easy.
Sure does, as the only user they just check it's me and we're off to a strong start.
Ok so what about your Subject Authentication, things looking over process or programs that have been created by a user?
What do you mean?
Well you're the only one here but I take it you're not the only one making decisions, Authentication is the process that checks that the user identity linked to the subject belongs to the same user who triggered the creation of the subject.
I'm going to have to refer you to our intranet for that answer sorry, please follow me.
LOADING: CASUAL CHAT...

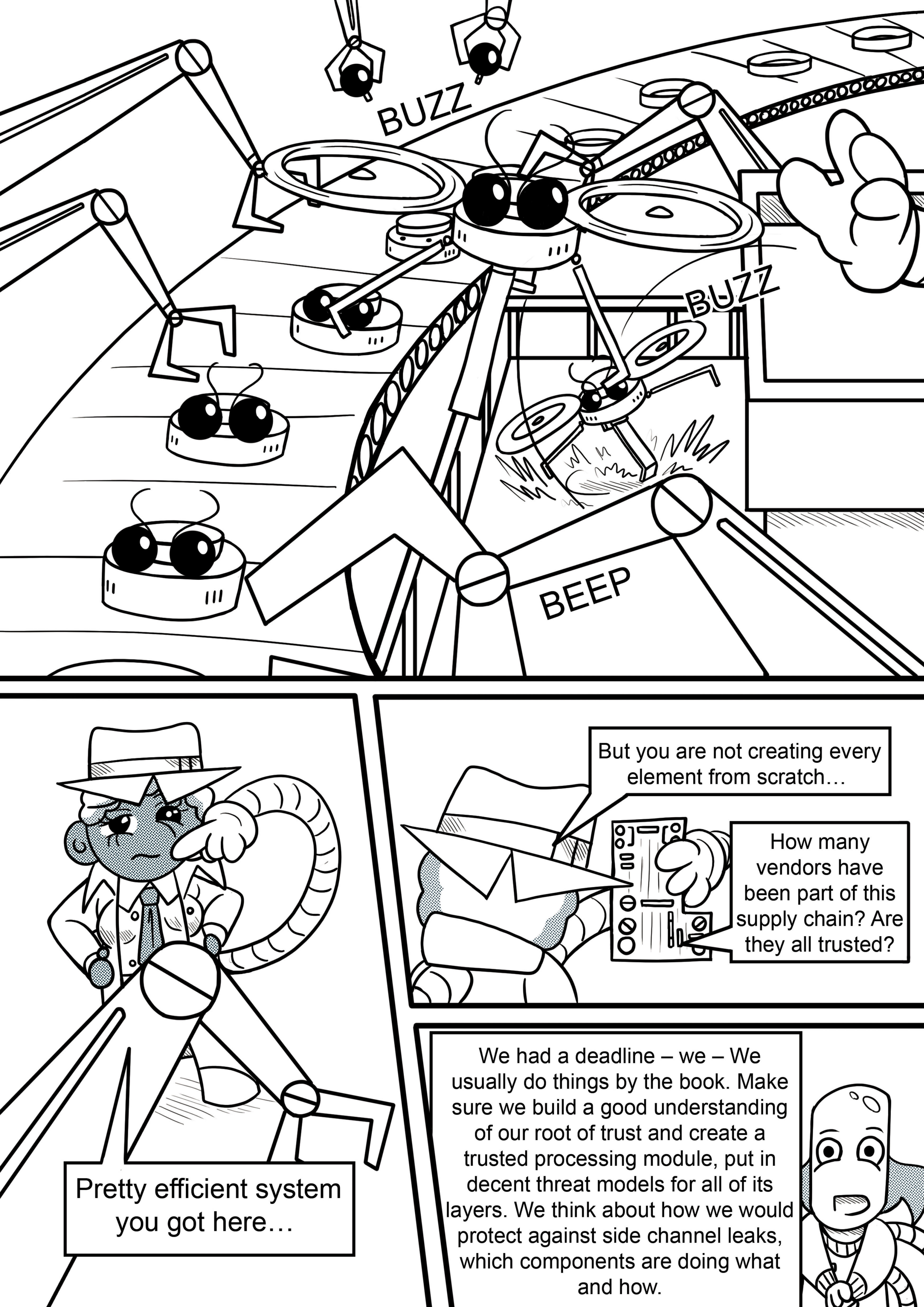

Tell me about your subject authentication process.
Our authentication protocols are top-notch. All attributes of the subject are checked each time it issues a request so that the decision algorithm is always validating them. Every user is also issued with an authentication token, a physical security key that provides a one-time password, and it must be physically placed into the device the worker is operating on. Without the key, the user's own password and being physically located in the room, there is no way to access this data.
What if keys go missing? Someone might have gained access to a key and then taken a user's identity some other way.
LOADING: SAS...
No way, we know who owns all the keys, and our identity management process ensures that if we need to revoke a key, we can get rid of the old key and get them a new one.

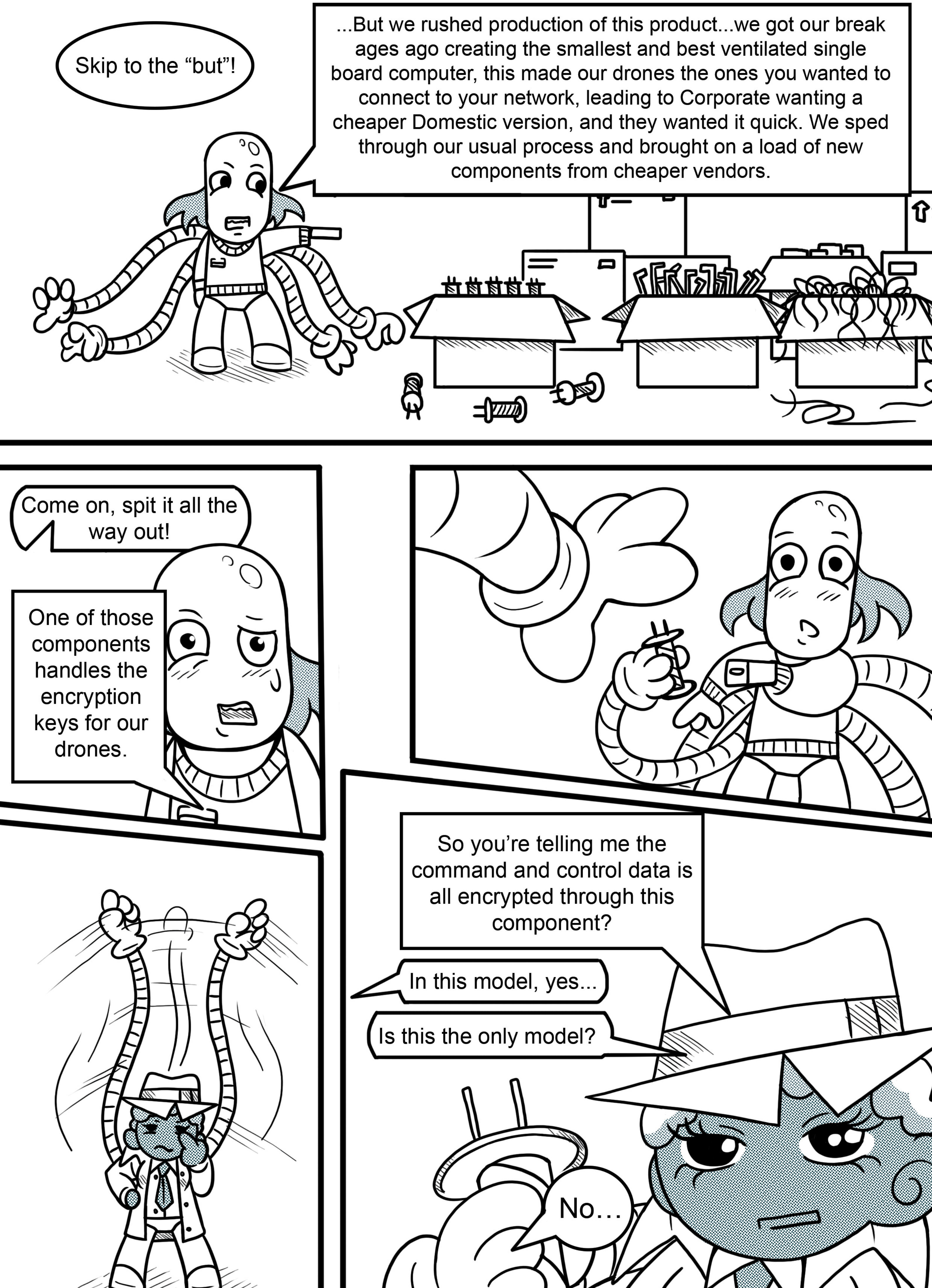

Hope you don't mind me asking you what this is about.
Well we have reason to believe that your Drones may be malfunctioning.
Really, what drones are you talking about?
It's concerning your food delivery Drones, there seems to be inconsistencies with the temperature.
What? I'll check that right away!
Well this one seems to be fine...
That is good to hear, would be great if we could check some more...and what would be perfect would be if we could check some out on the field, is that possible?
Mmmmmm, well I could reroute some missed items that were on their way to the food bank.
Could take a while though...
Looks like you were right, it's subtle but you predicting a higher temperature than expected tells me there is something wrong.

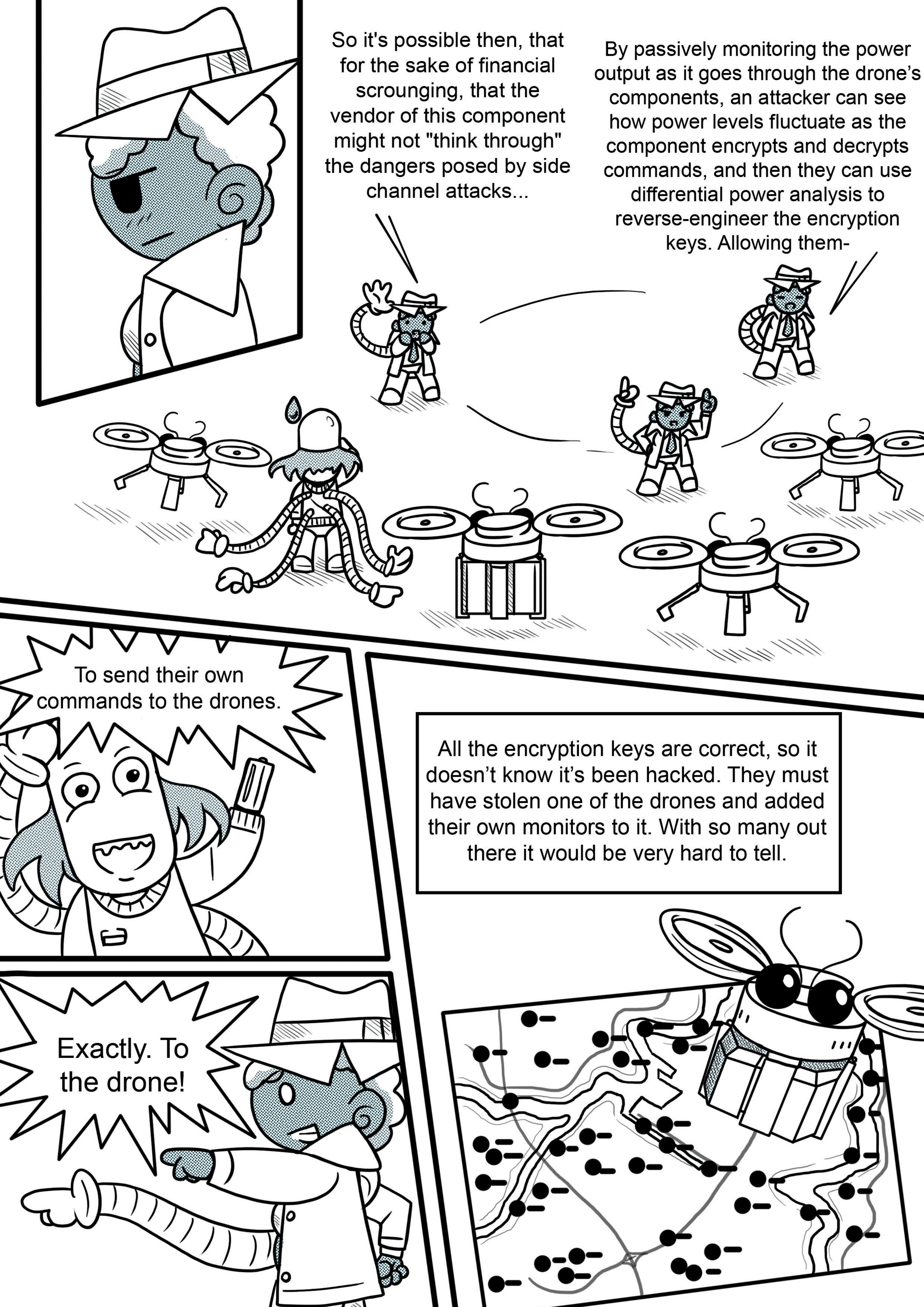

EXIT
Thanks for your help so far, just going to report an update.
Please take your time, I'm going to do some more checks.
Hey Chief just a quick update...
Make it quick I'm on a break from teaching but I'm back soon.
Well as you said the guy looking after here is definitely weird but no malintent on his side.
He has confirmed that there is an issue with the Drones but they seem to have pretty decent security processes at play.
Ok so not a complete waste of time but at the moment I'm having to check that the Archie information and access isn't being used to create nodes for a sybil attack whilst teaching because my most qualified juniors are out doing what you should be doing.
Amazing real-time education that's basically the only way I ever learn anything.
Yeah well if it was up to me I would have that office job I was promised.
Well I'm going to check the most important thing before I leave.
Oh really what's that?
Well in every perfect looking institution there is a human being trying to cut corners, I'll just check what that means in this case.
I know you're not talking about me.
Bye Chief.

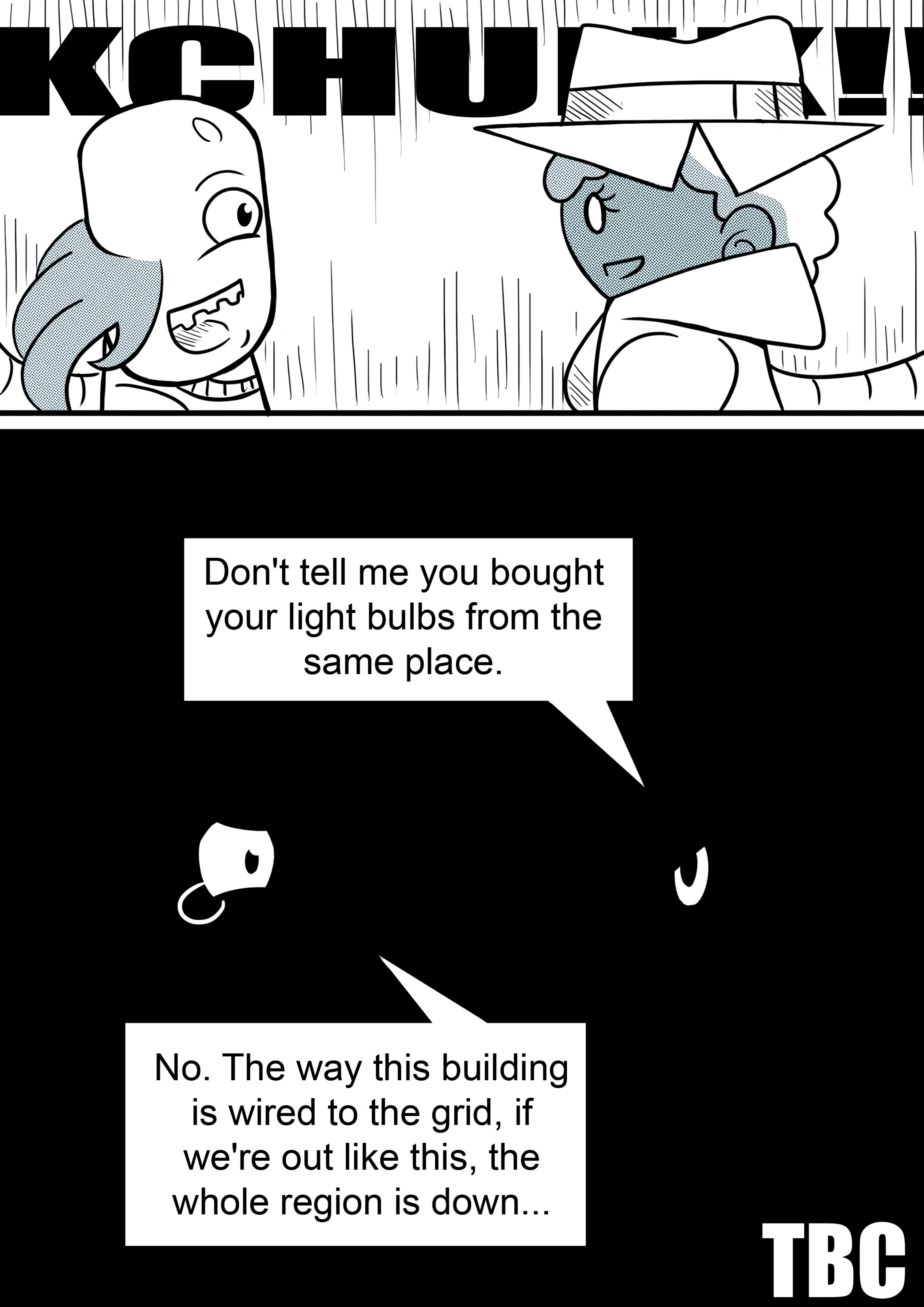

It’s Harold Right?
So what you up to in here?
People call me Bart.
Well this is where we design our software in line with our Secure Software Lifecycle process. It’s a long sequence which has security embedded at every step of the way.
Can you tell me more?
I’ll tell you what I can, some of it is secretive. We’re nearly at the end of this one. We finished our threat modelling on this software months back and have considered a whole range of attacks. We then carried out our static analysis security testing, an automated review of the code to look for bugs and insecure coding patterns in the team’s work, then dynamic analysis security testing to look for holes when the program is up and running. After what you have highlighted today I'm having a quick once over before suggesting we do some penetration testing with our team of in-house pen-testers.
You smelling any foul play at hand? I used to be an ethical hacker myself!
Didn't we all?


So Bart what happens on this station?
This is where we build our software for our internet-enabled devices for the home. Fridges, dishwashers, tables, coolers, it's all made here.
I've heard you make them more secure than your competitors; why you got all the big contracts! How do you do it?
Some of it is quite simple really. For one thing, our devices ship out without a default password and we show people how to use a password manager to randomly generate a good one and store it safely so they can remember it.
People don't comprehend the big difference such a small implementation like that can make.
You wouldn't believe the amount of devices out there sold by our cheaper rivals which have default passwords like "Admin" or "123456". That's how webcams get hacked and news stories get made.
There are a lot of things to consider...
Yeah and we possibly have the most moving parts out of any company in Oasis, all stuck together with our secure software.
Talking of moving parts could you show me where the Drones are created
Sure!


BUZZ
BUZZ
BEEP
Pretty efficient system you got here…
But you are not creating every element from scratch…
How many vendors have been part of this supply chain? Are they all trusted?
We had a deadline – we – We usually do things by the book. Make sure we build a good understanding of our root of trust and create a trusted processing module, put in decent threat models for all of its layers. We think about how we would protect against side channel leaks, which components are doing what and how.


Skip to the “but”!
...But we rushed production of this product...we got our break ages ago creating the smallest and best ventilated single board computer, this made our drones the ones you wanted to connect to your network, leading to Corporate wanting a cheaper Domestic version, and they wanted it quick. We sped through our usual process and brought on a load of new components from cheaper vendors.
Come on, spit it all the way out!
One of those components handles the encryption keys for our drones.
So you’re telling me the command and control data is all encrypted through this component?
In this model, yes...
Is this the only model?
No…


So it's possible then, that for the sake of financial scrounging, that the vendor of this component might not "think through" the dangers posed by side channel attacks...
By passively monitoring the power output as it goes through the drone’s components, an attacker can see how power levels fluctuate as the component encrypts and decrypts commands, and then they can use differential power analysis to reverse-engineer the encryption keys. Allowing them-
To send their own commands to the drones.
All the encryption keys are correct, so it doesn’t know it’s been hacked. They must have stolen one of the drones and added their own monitors to it. With so many out there it would be very hard to tell.
Exactly. To the drone!


KCHUNK!!
Don't tell me you bought your light bulbs from the same place.
No. The way this building is wired to the grid, if we're out like this, the whole region is down...
TBC