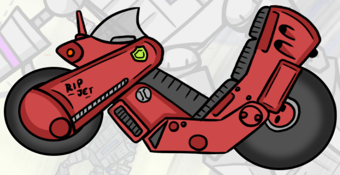
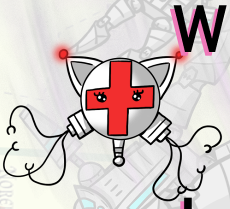
OASIS
CyberDetective

COMIC PART 4 OF 6

PART 4/6



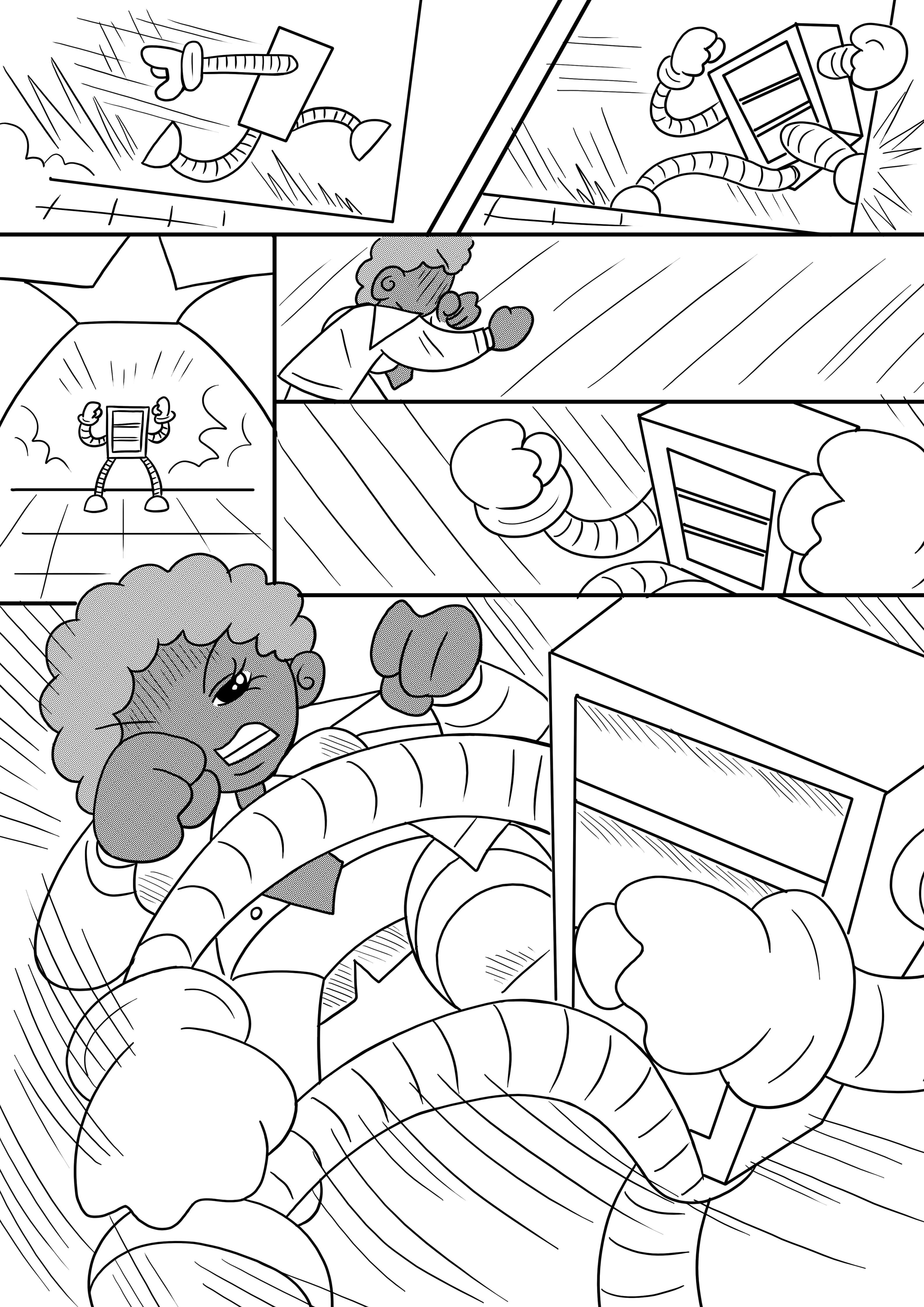
Welcome to the World of Oasis where its inhabitants are kept safe by the technology they surround themselves with as they try to rebuild their lives.



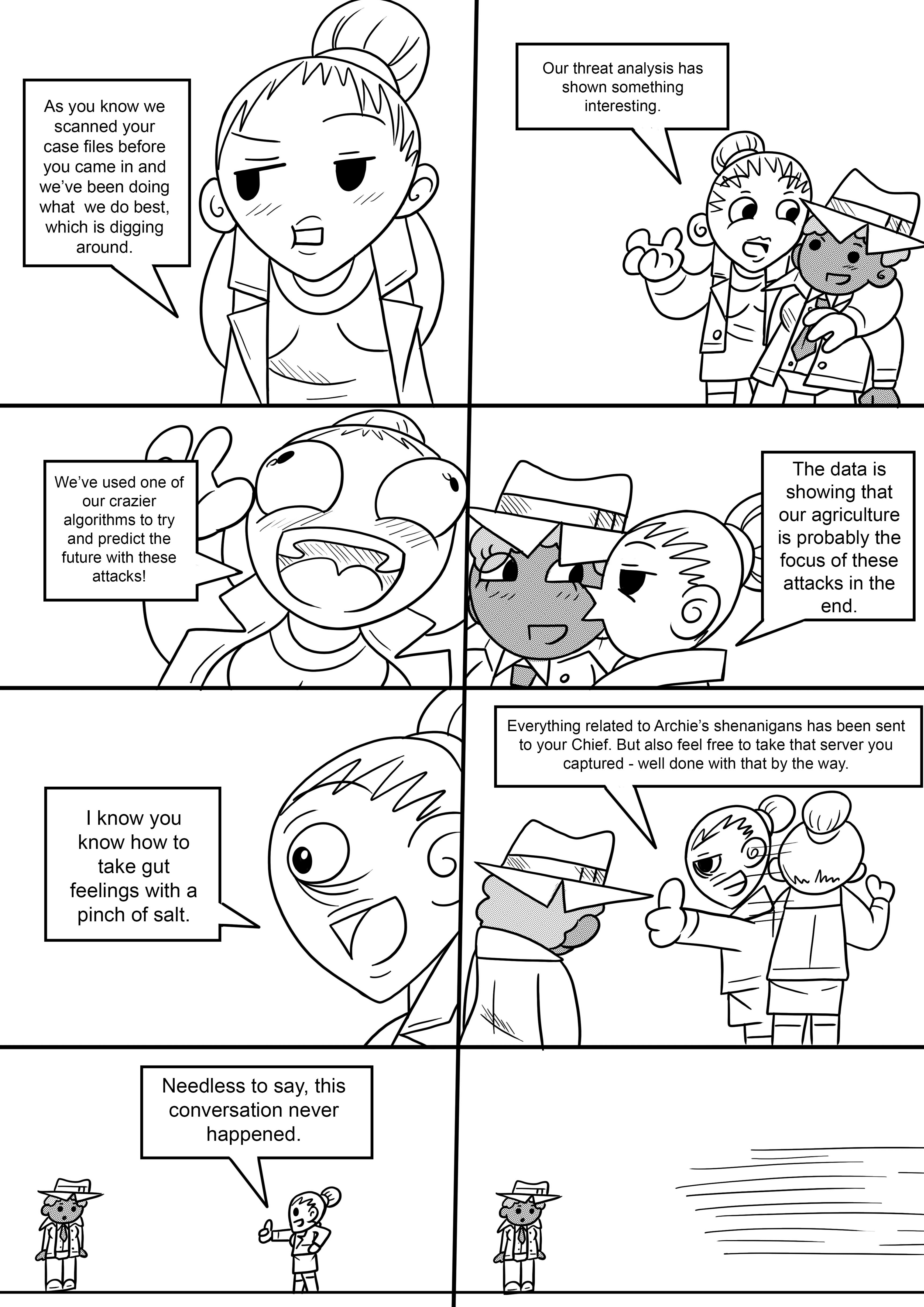
In this episode the detective has to take a trip out to the "sticks".

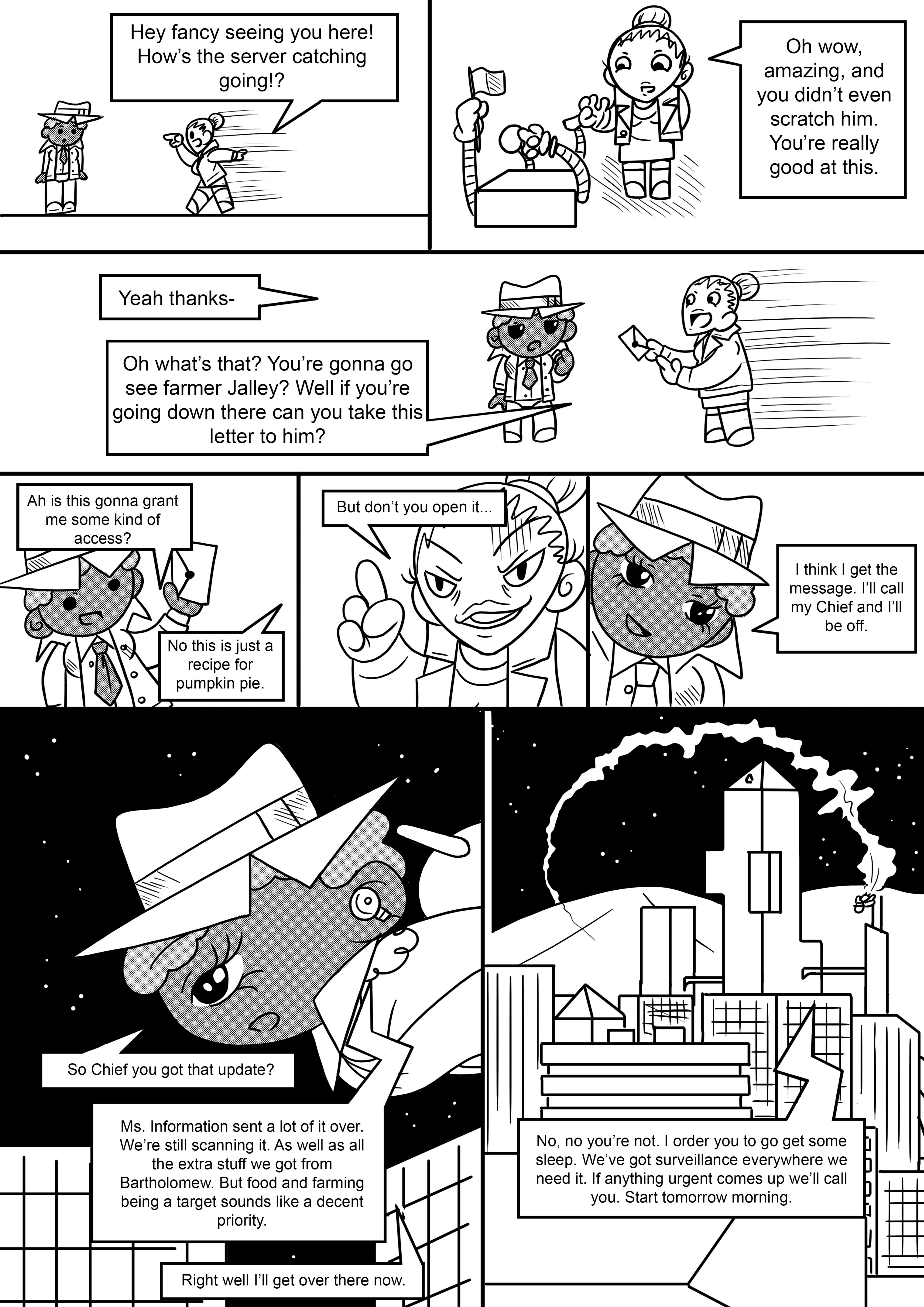
Chief Editor &
Transmedial Producer:
Vincent "South-Blessed" Baidoo
Artist: Connor Rawlings
Front Cover: Jonathan Tonello
Writer: Vincent Baidoo
Editor: Niki Baidoo
Writer & Researcher: Patrick Shortis
Extra Art: Vladimir Rikowski, Francisco Ruiz
Special Thanks: Jeremy Charles, Tomas Hall

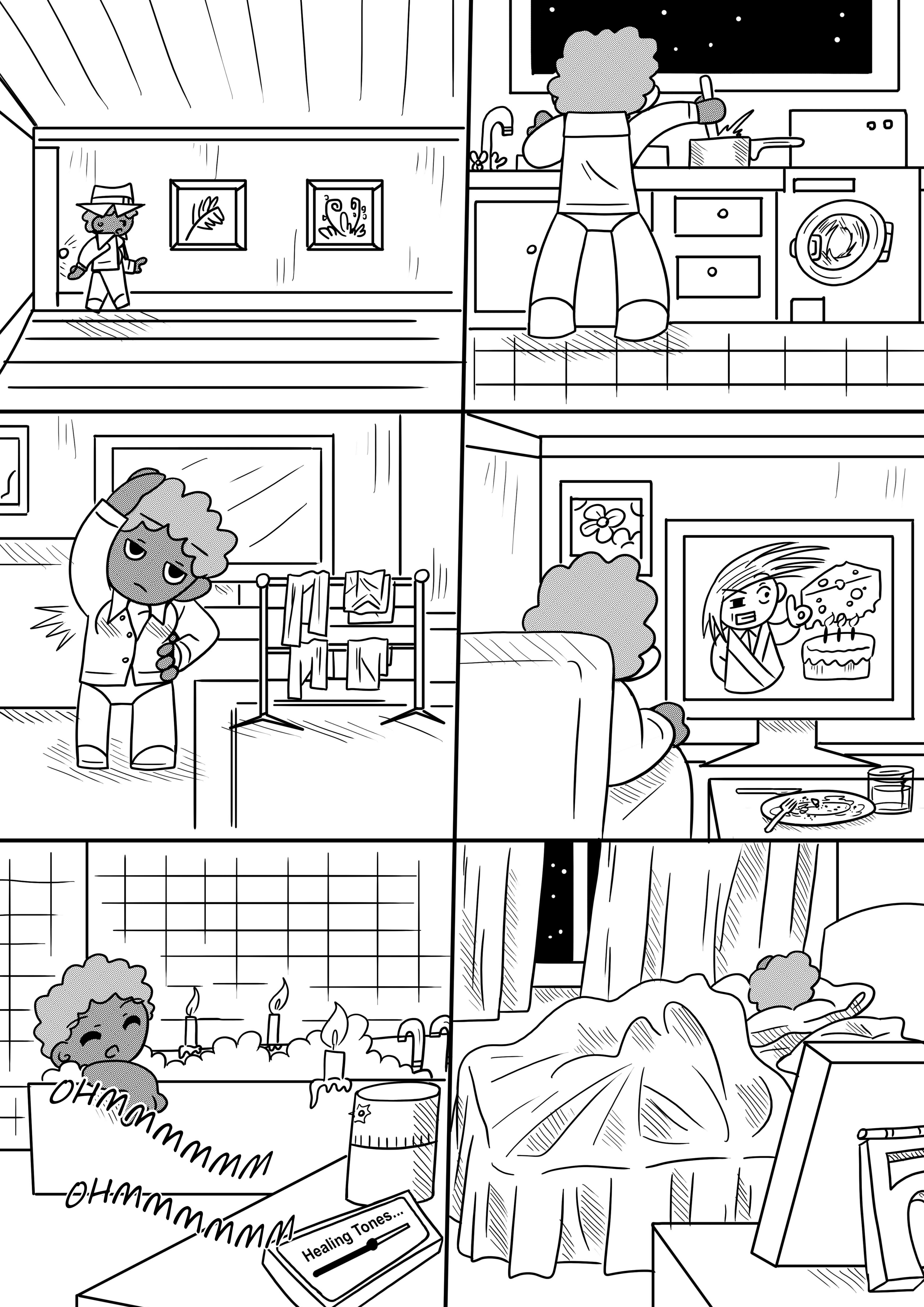
THIS PUBLICATION IS A RESULT OF CYBOK AND CROWNROOT PUBLICATIONS FUNDED BY BRISTOL UNIVERSITY AND RESEARCH ENGLAND UNDER THE CC-BY-NC COPYRIGHT LAWS.
ALL STYLES ARE RETAINED BY CREATORS AND THEIR CONTRACTORS.
CROWNROOT PUBLICATIONS 2020.
ANY RESEMBLANCE TO ACTUAL PERSONS, OR ACTUAL EVENTS IS PURELY COINCIDENTAL.

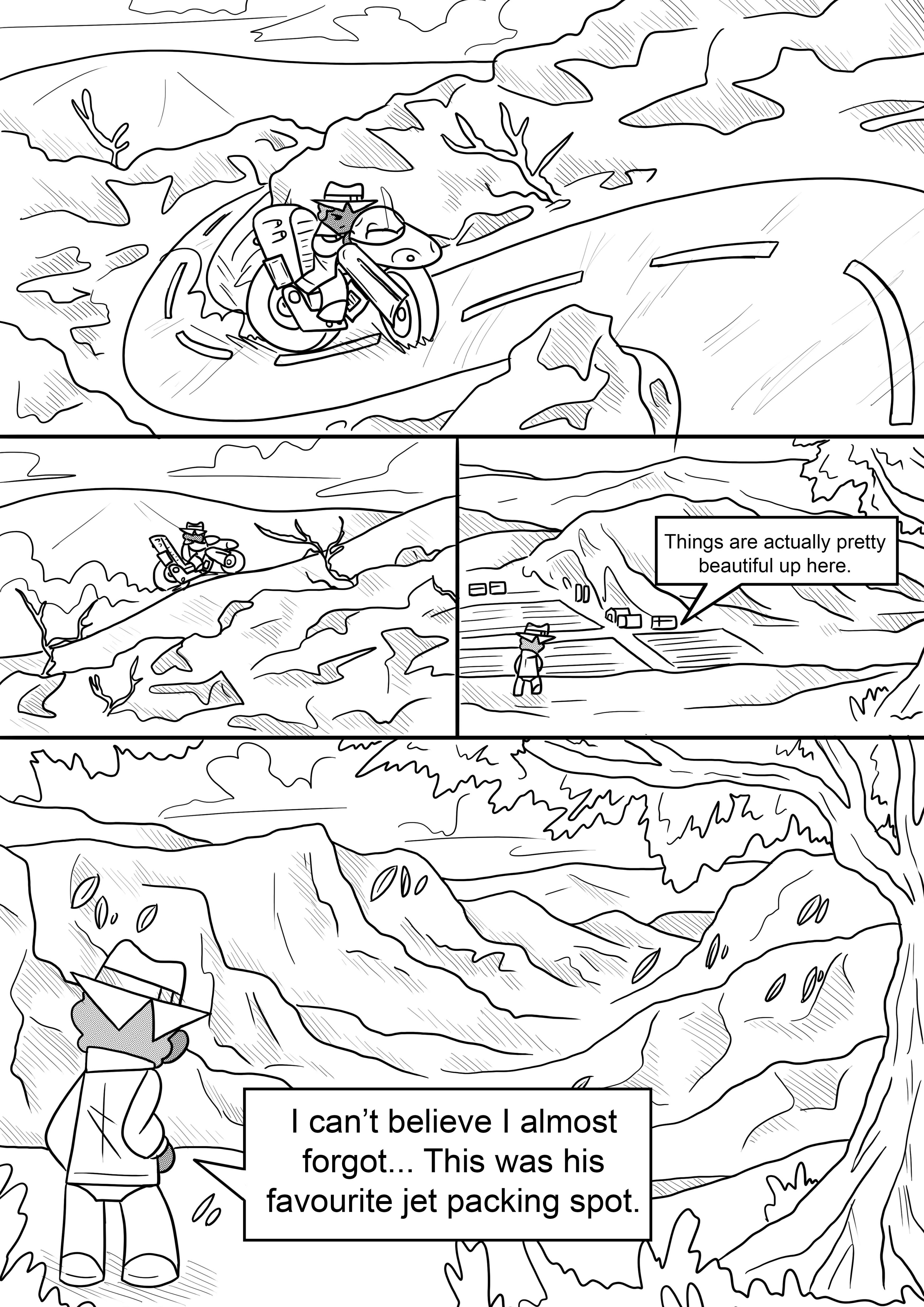


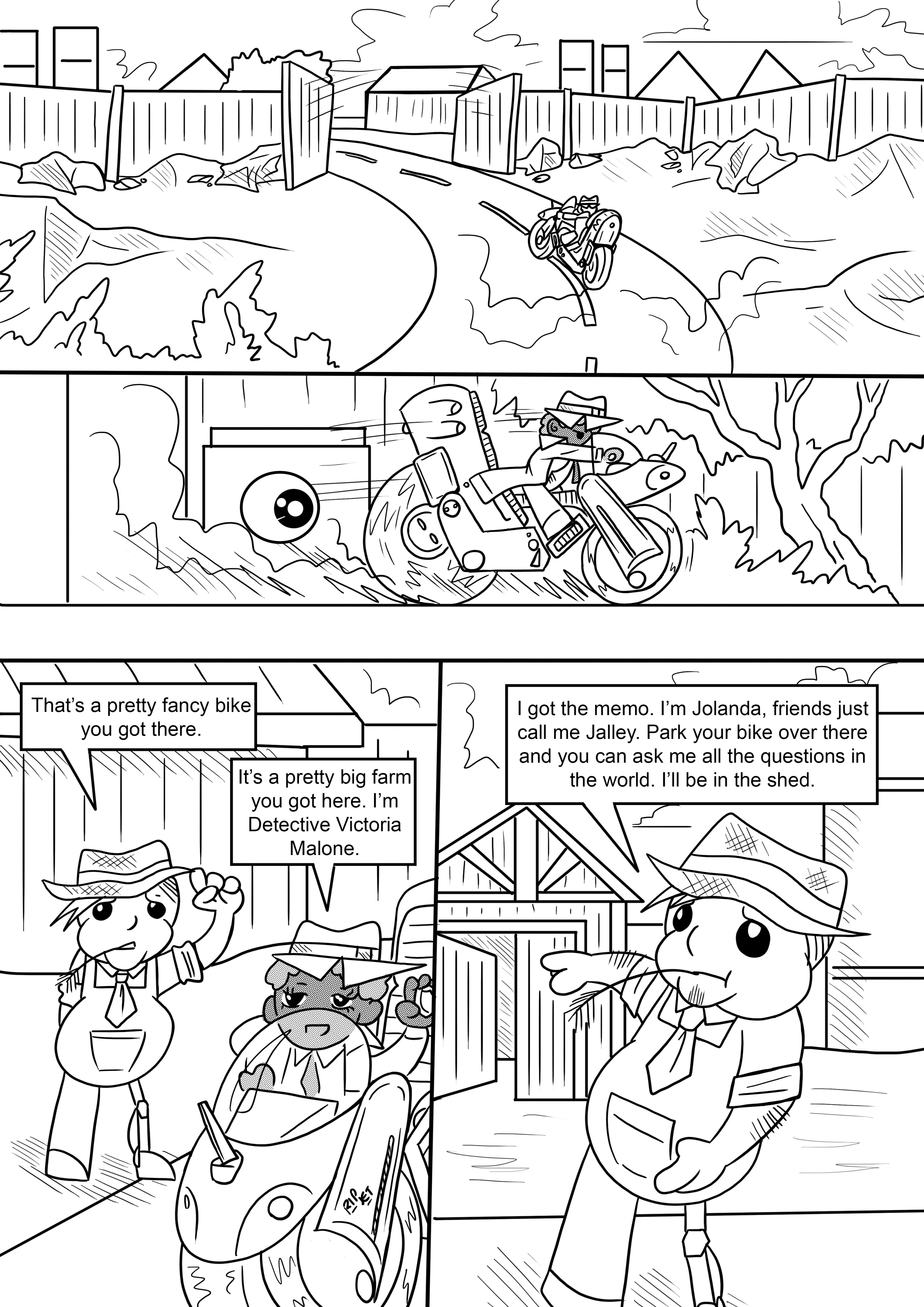
Well done.

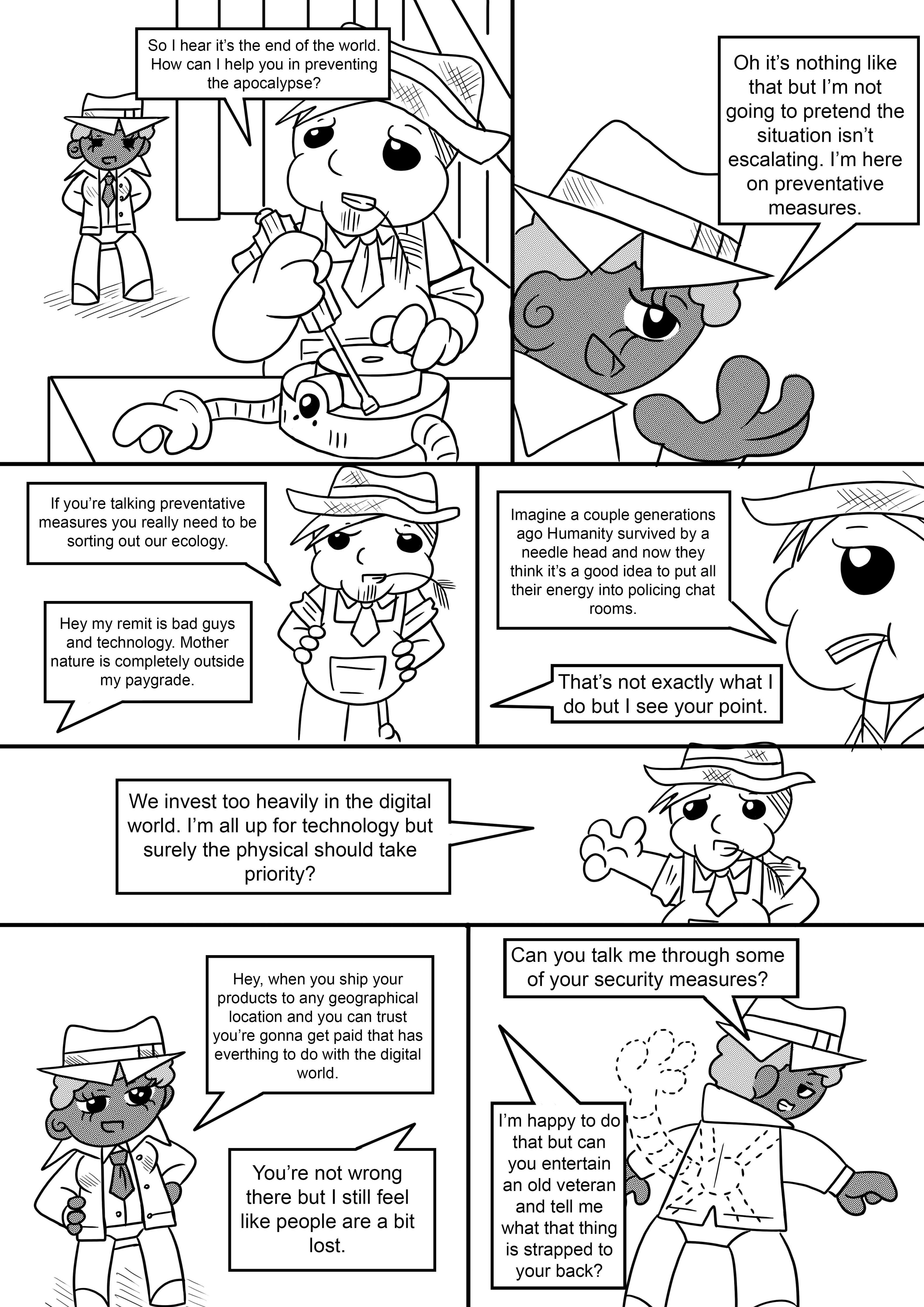

As you know we scanned your case files before you came in and we've been doing what we do best, which is digging around.
Our threat analysis has shown something interesting.
We've used one of our crazier algorithms to try and predict the future with these attacks!
The data is showing that our agriculture is probably the focus of these attacks in the end.
I know you know how to take gut feelings with a pinch of salt.
Everything related to Archie's shenanigans has been sent to your Chief. But also feel free to take that server you captured - well done with that by the way.
Needless to say, this conversation never happened.

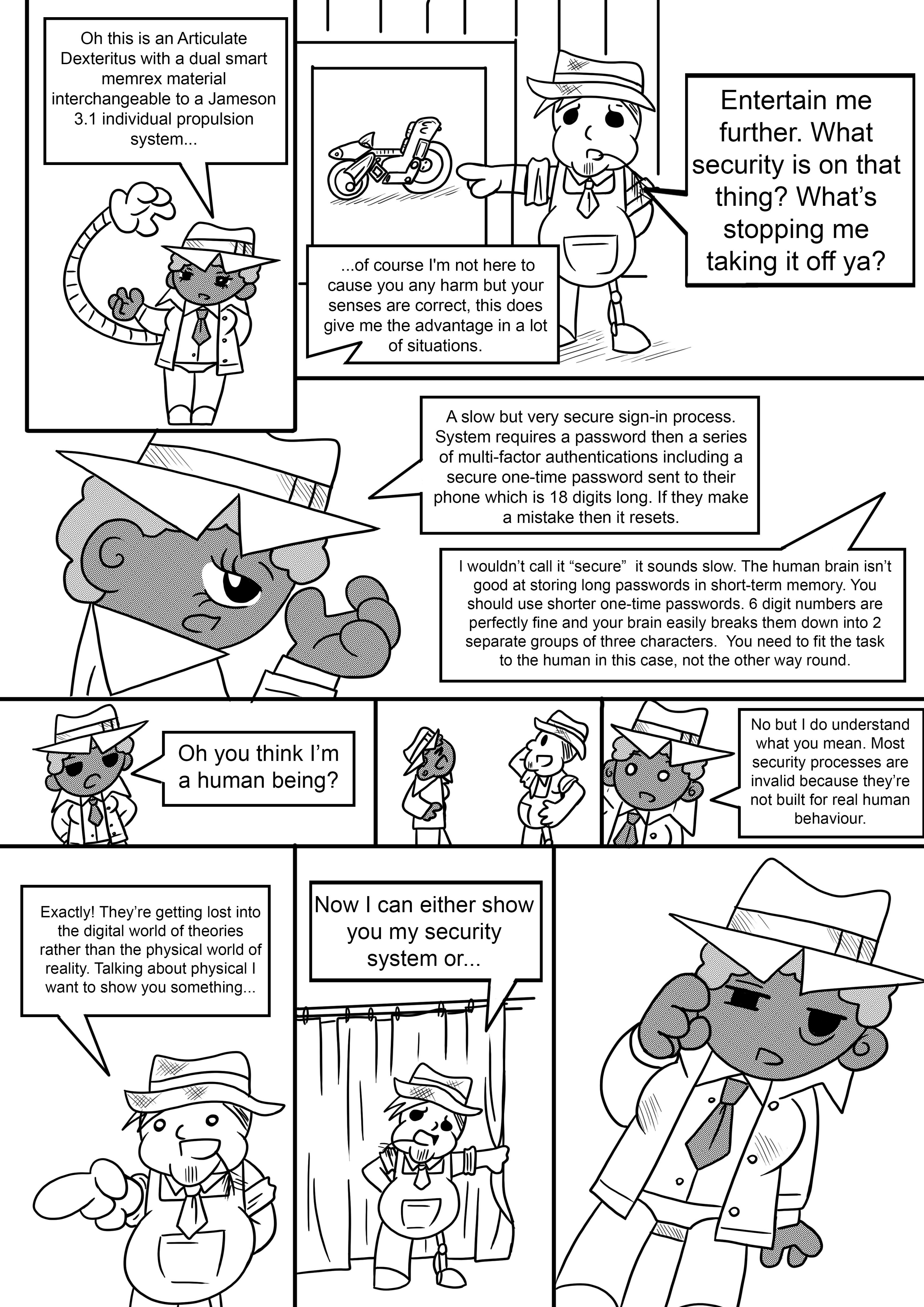

Hey fancy seeing you here! How's the server catching going!?
Oh wow, amazing, and you didn't even scratch him. You're really good at this.
Yeah thanks-
Oh what's that? You're gonna go see farmer Jalley? Well if you're going down there can you take this letter to him?
Ah is this gonna grant me some kind of access?
No this is just a recipe for pumpkin pie.
But don't you open it...
I think I get the message. I'll call my Chief and I'll be off.
So Chief you got that update?
Ms. Information sent a lot of it over. We're still scanning it. As well as all the extra stuff we got from Bartholomew. But food and farming being a target sounds like a decent priority.
Right well I'll get over there now.
No, no you're not. I order you to go get some sleep. We've got surveillance everywhere we need it. If anything urgent comes up we'll call you. Start tomorrow morning.

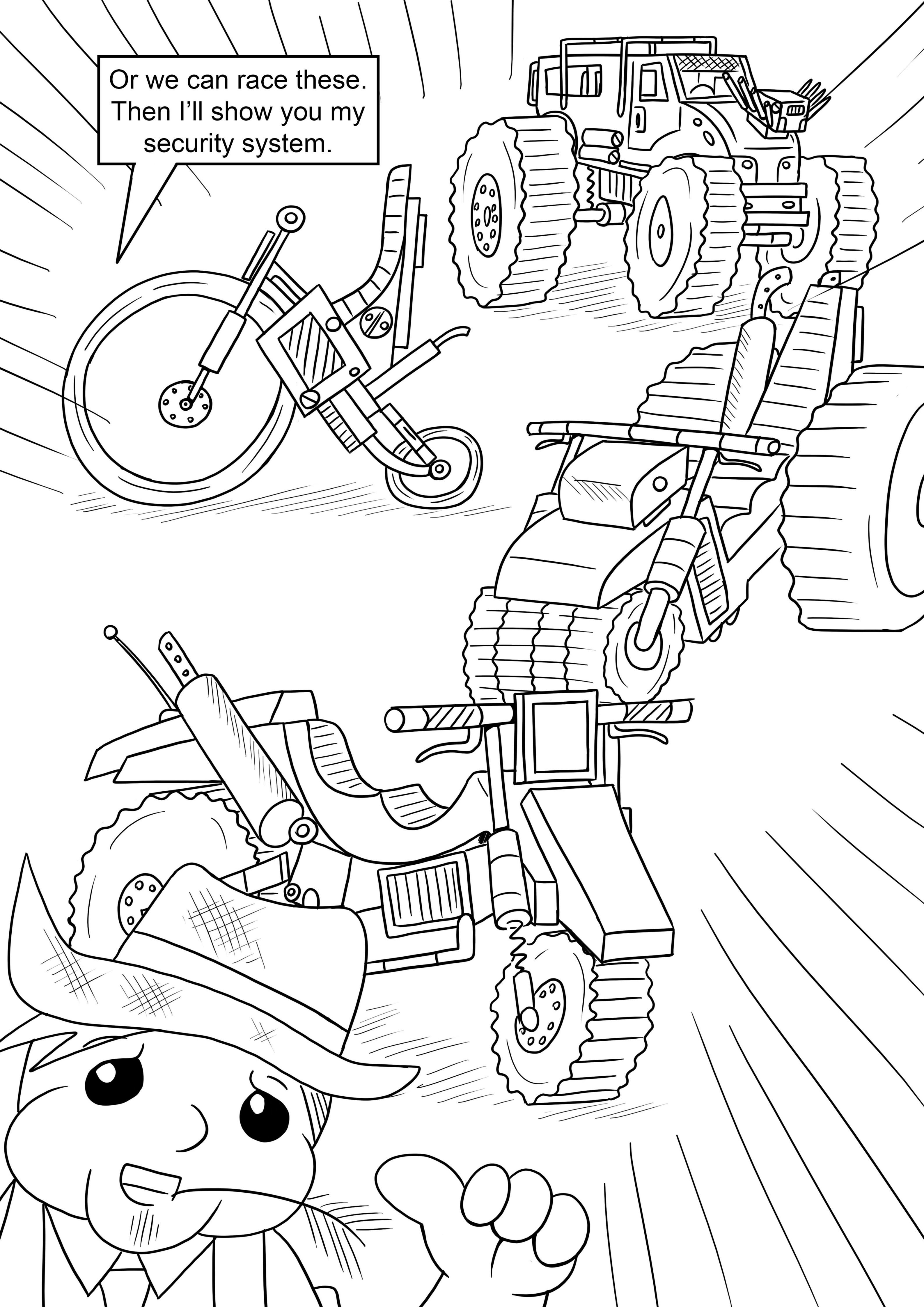

OHMMMMMMMM
OHMMMMMMMMM
Healing Tones...

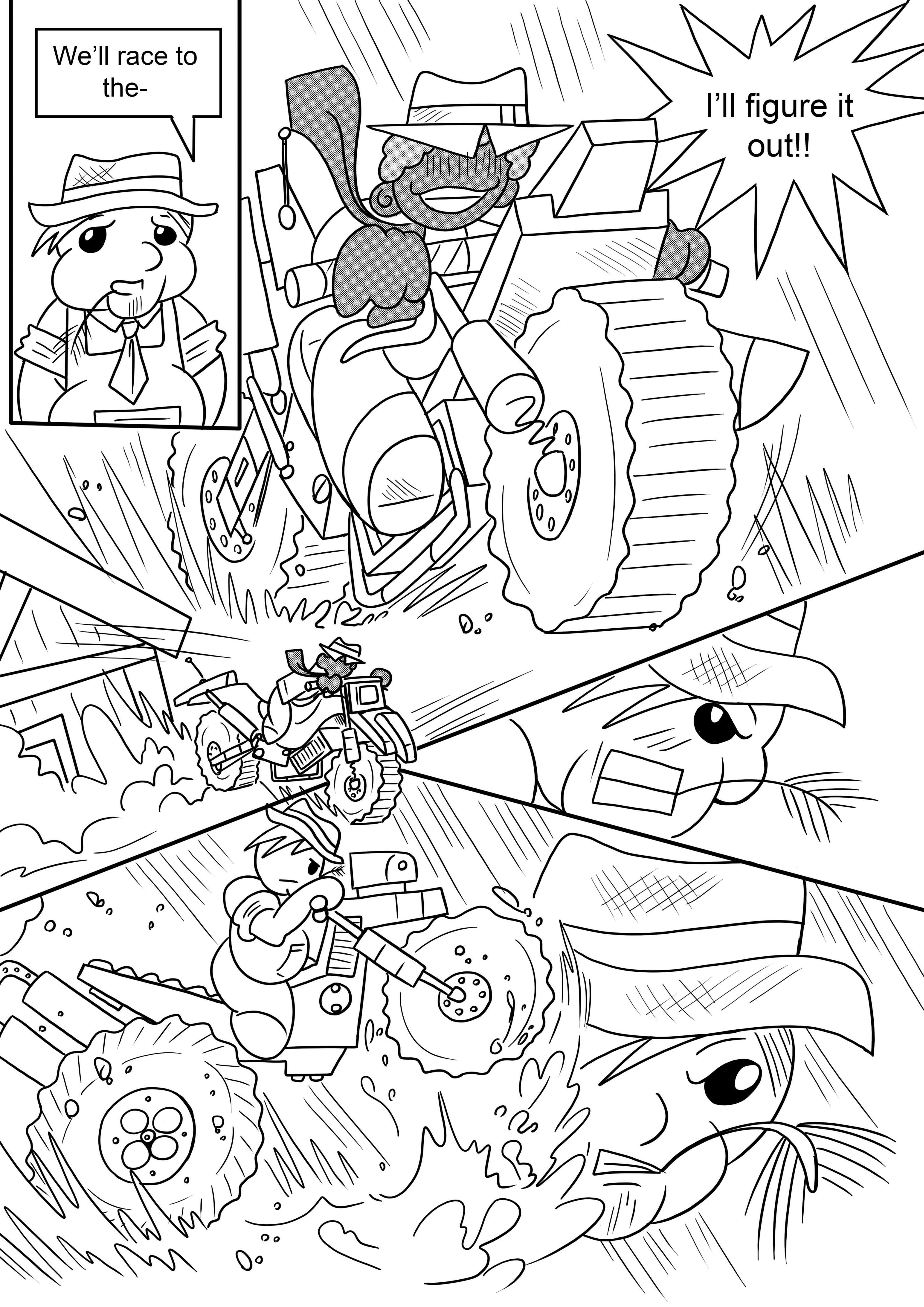

Things are actually pretty beautiful up here.
I can't believe I almost forgot... This was his favourite jet packing spot.

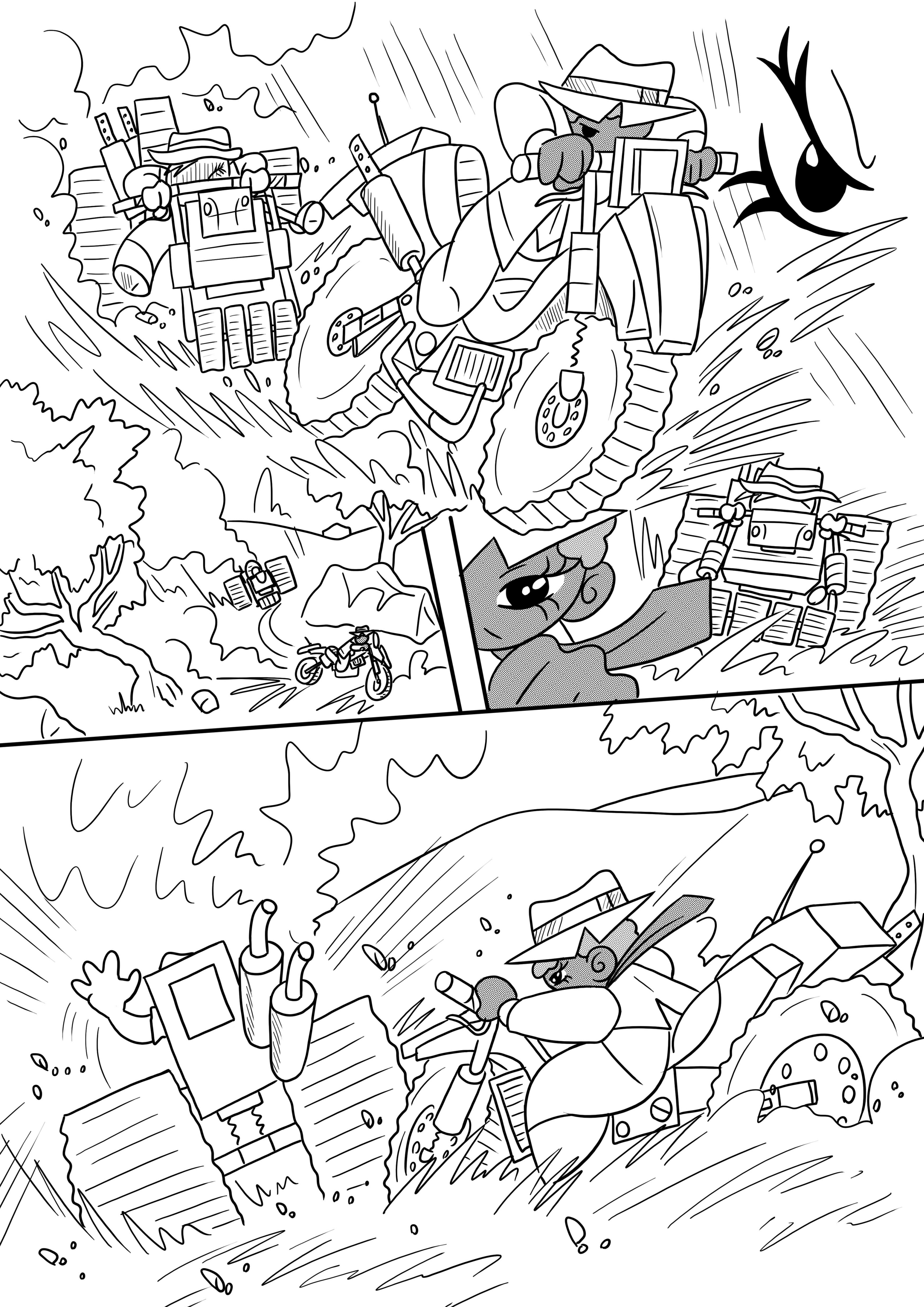

That’s a pretty fancy bike you got there.
It’s a pretty big farm you got here. I’m Detective Victoria Malone.
RIP JET
I got the memo. I’m Jolanda, friends just call me Jalley. Park your bike over there and you can ask me all the questions in the world. I’ll be in the shed.

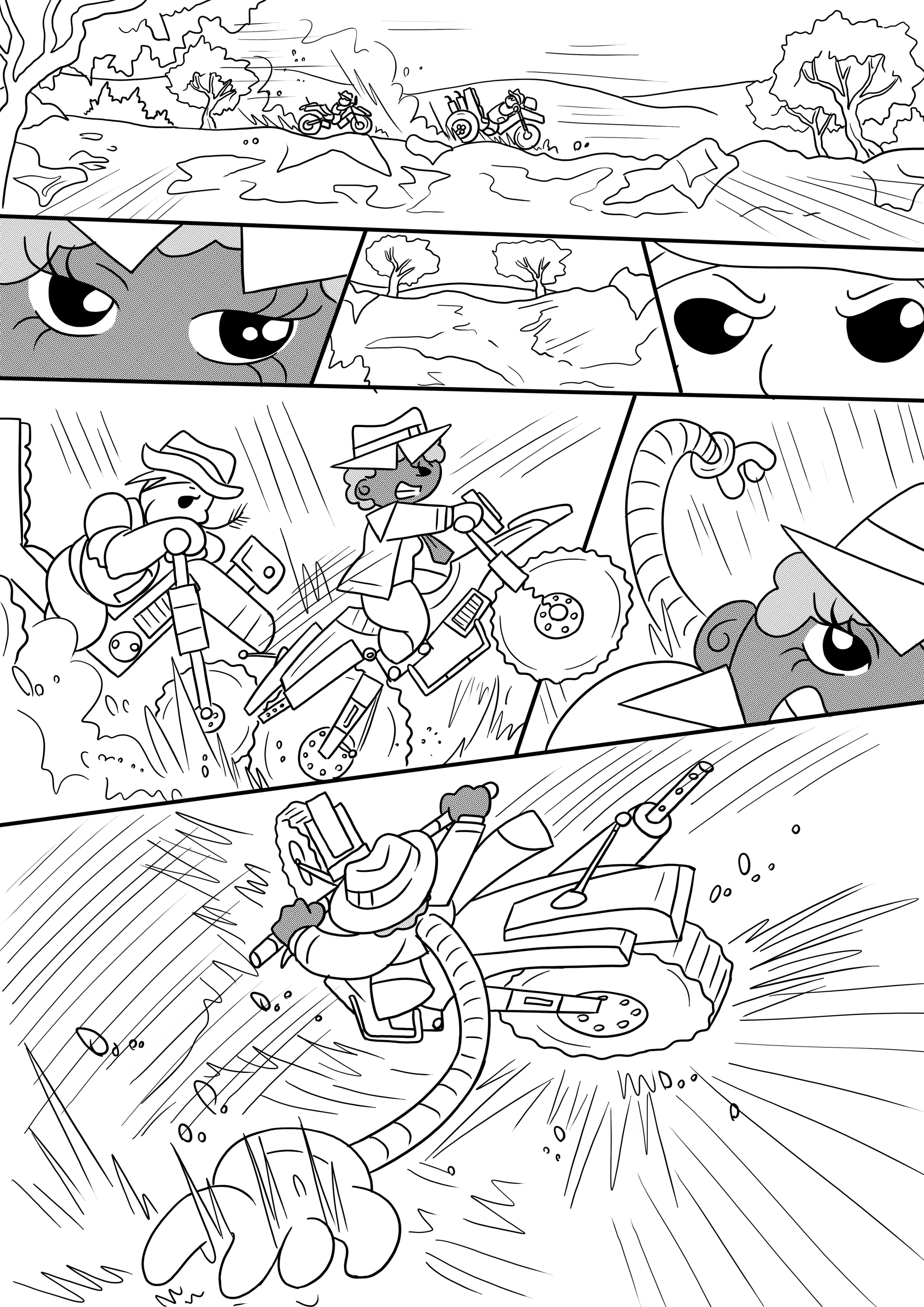

So I hear it's the end of the world. How can I help you in preventing the apocalypse?
Oh it's nothing like that but I'm not going to pretend the situation isn't escalating. I'm here on preventative measures.
If you're talking preventative measures you really need to be sorting out our ecology.
Hey my remit is bad guys and technology. Mother nature is completely outside my paygrade.
Imagine a couple generations ago Humanity survived by a needle head and now they think it's a good idea to put all their energy into policing chat rooms.
That's not exactly what I do but I see your point.
We invest too heavily in the digital world. I'm all up for technology but surely the physical should take priority?
Hey, when you ship your products to any geographical location and you can trust you're gonna get paid that has everthing to do with the digital world.
You're not wrong there but I still feel like people are a bit lost.
Can you talk me through some of your security measures?
I'm happy to do that but can you entertain an old veteran and tell me what that thing is strapped to your back?

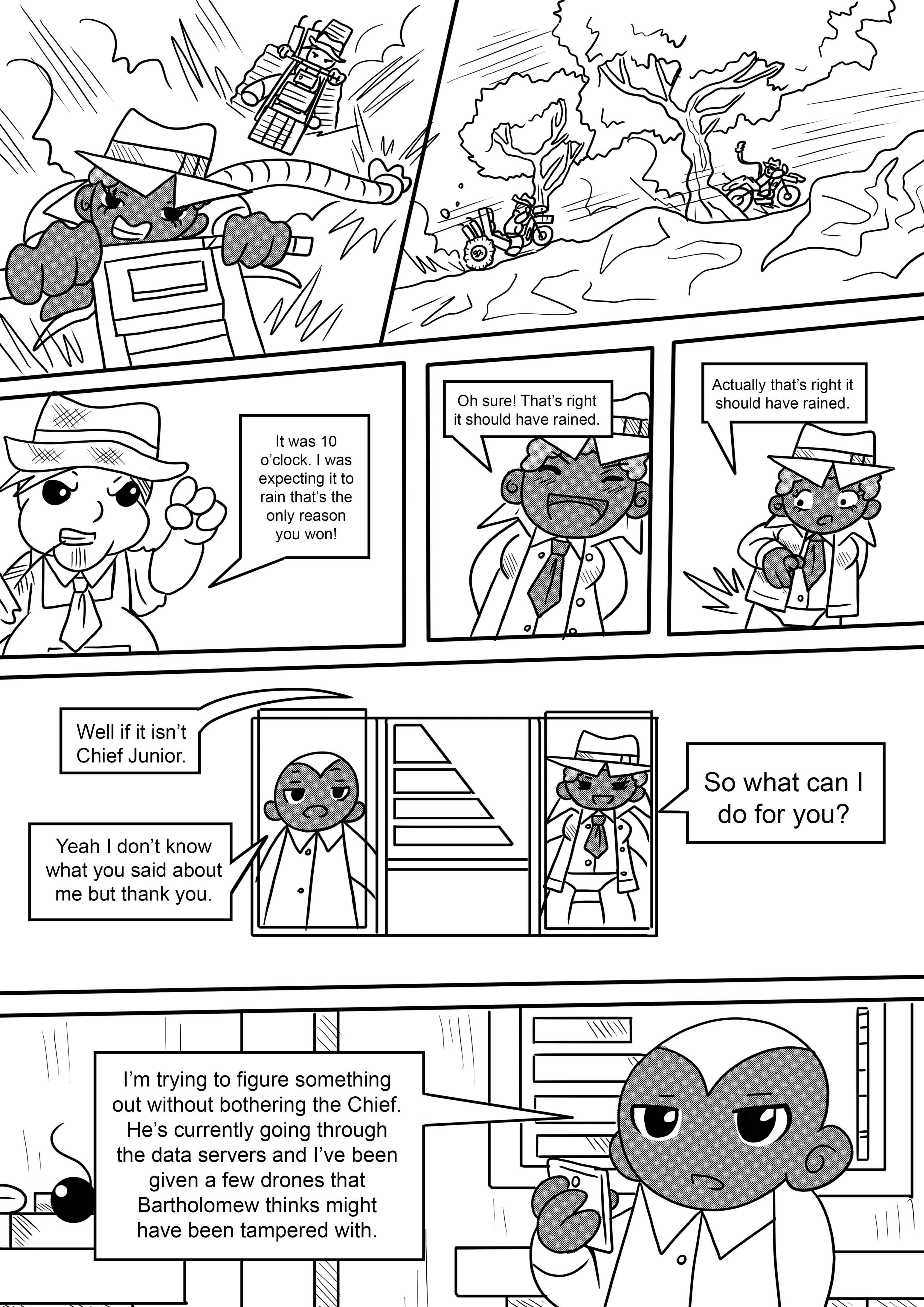

Oh this is an Articulate Dexteritus with a dual smart memrex material interchangeable to a Jameson 3.1 individual propulsion system...
...of course I'm not here to cause you any harm but your senses are correct, this does give me the advantage in a lot of situations.
Entertain me further. What security is on that thing? What's stopping me taking it off ya?
A slow but very secure sign-in process. System requires a password then a series of multi-factor authentications including a secure one-time password sent to their phone which is 18 digits long. If they make a mistake then it resets.
I wouldn't call it "secure" it sounds slow. The human brain isn't good at storing long passwords in short-term memory. You should use shorter one-time passwords. 6 digit numbers are perfectly fine and your brain easily breaks them down into 2 separate groups of three characters. You need to fit the task to the human in this case, not the other way round.
Oh you think I'm a human being?
No but I do understand what you mean. Most security processes are invalid because they're not built for real human behaviour.
Exactly! They're getting lost into the digital world of theories rather than the physical world of reality. Talking about physical I want to show you something...
Now I can either show you my security system or...

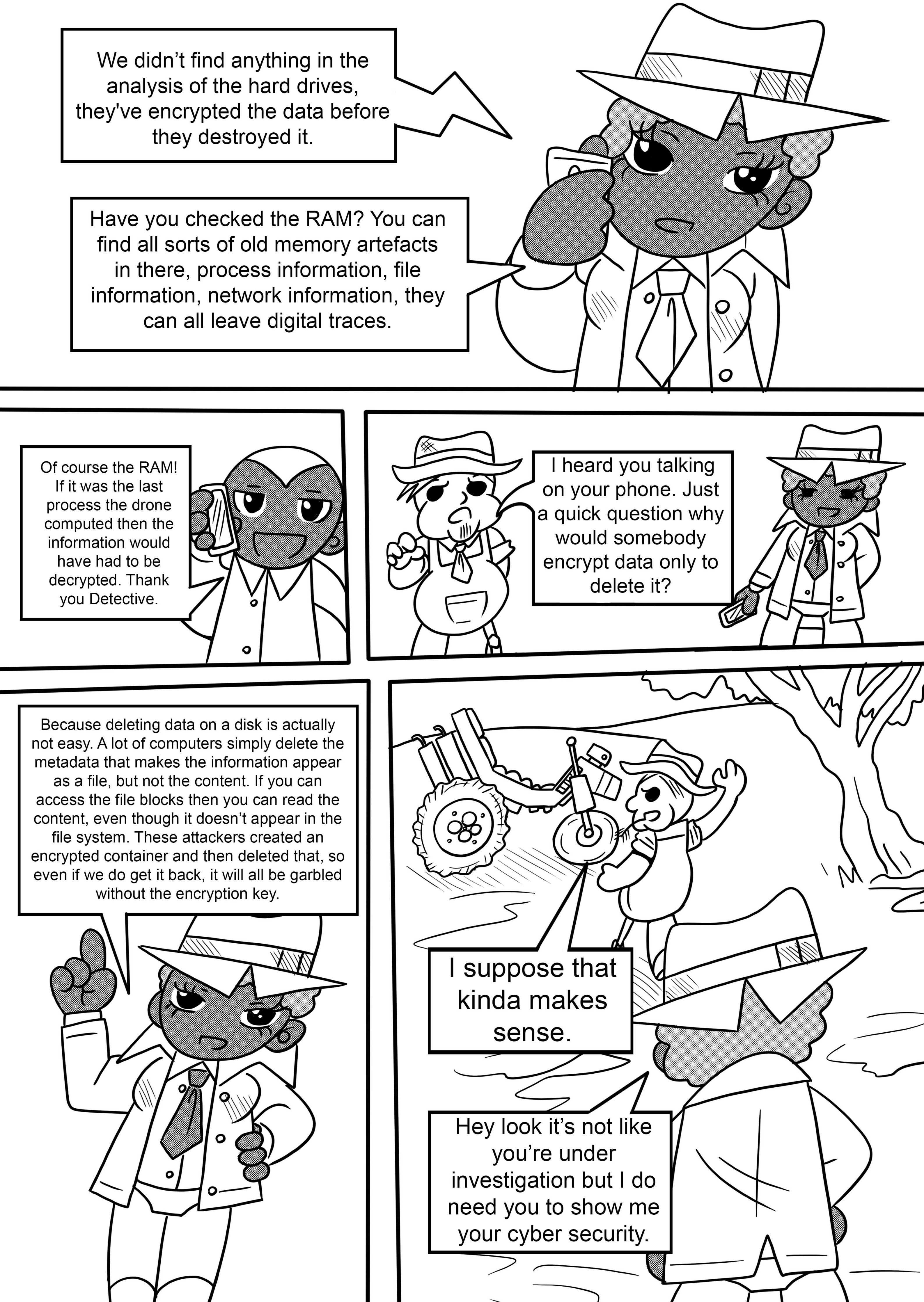

Or we can race these. Then I'll show you my security system.

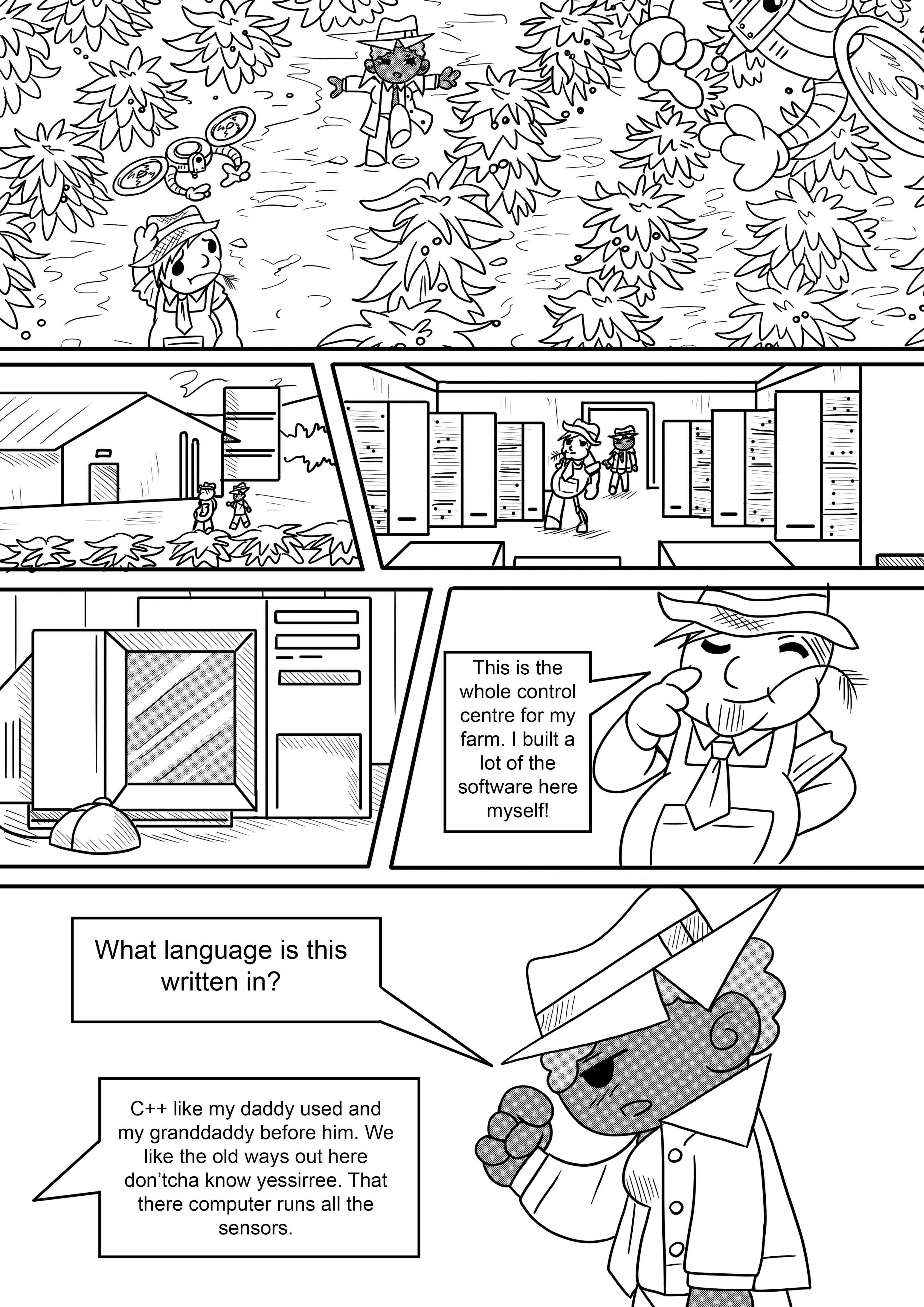

We'll race to the-
I'll figure it out!!

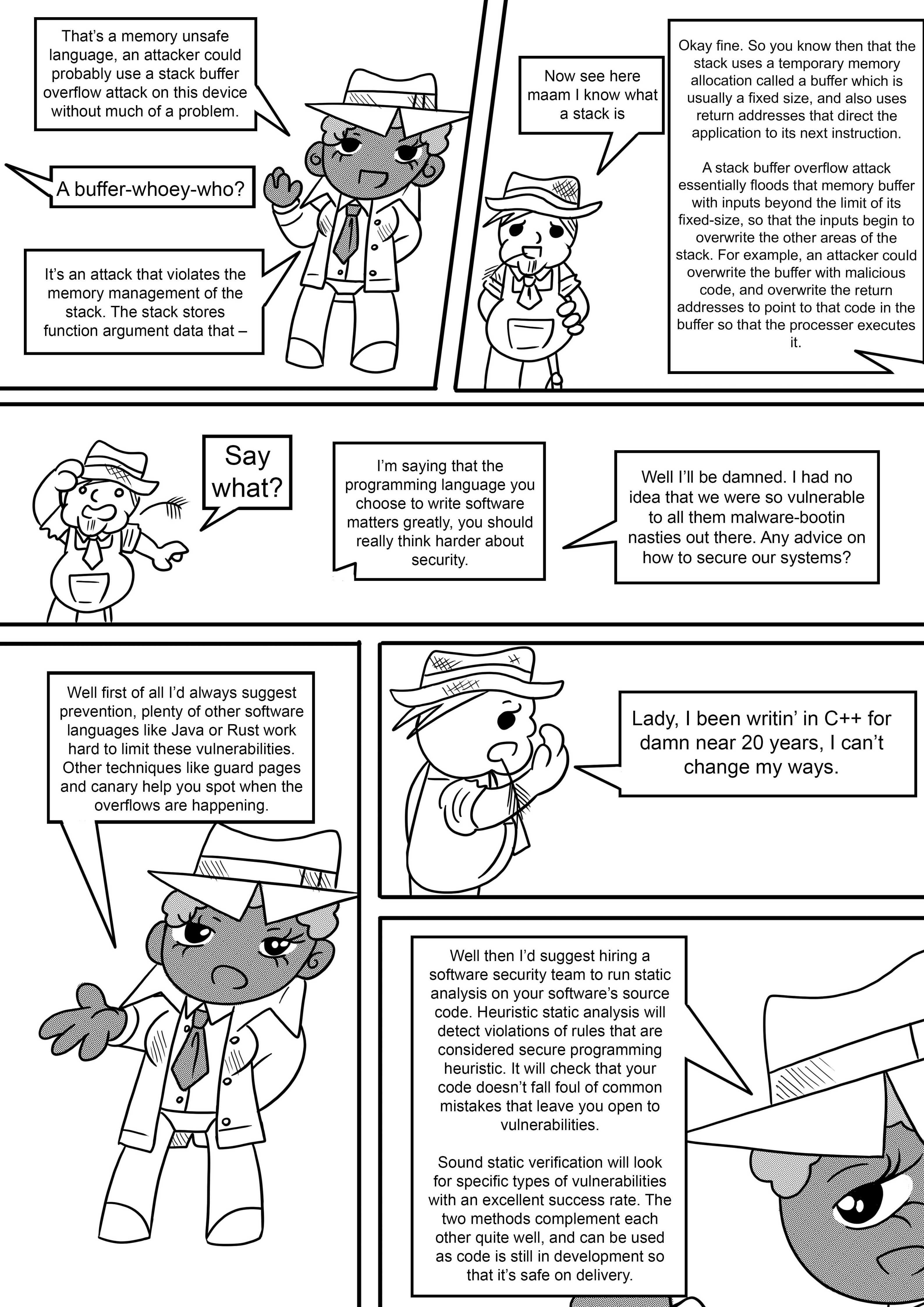





It was 10 o'clock. I was expecting it to rain that's the only reason you won!
Oh sure! That's right it should have rained.
Actually that's right it should have rained.
Well if it isn't Chief Junior.
Yeah I don't know what you said about me but thank you.
So what can I do for you?
I'm trying to figure something out without bothering the Chief. He's currently going through the data servers and I've been given a few drones that Bartholomew thinks might have been tampered with.

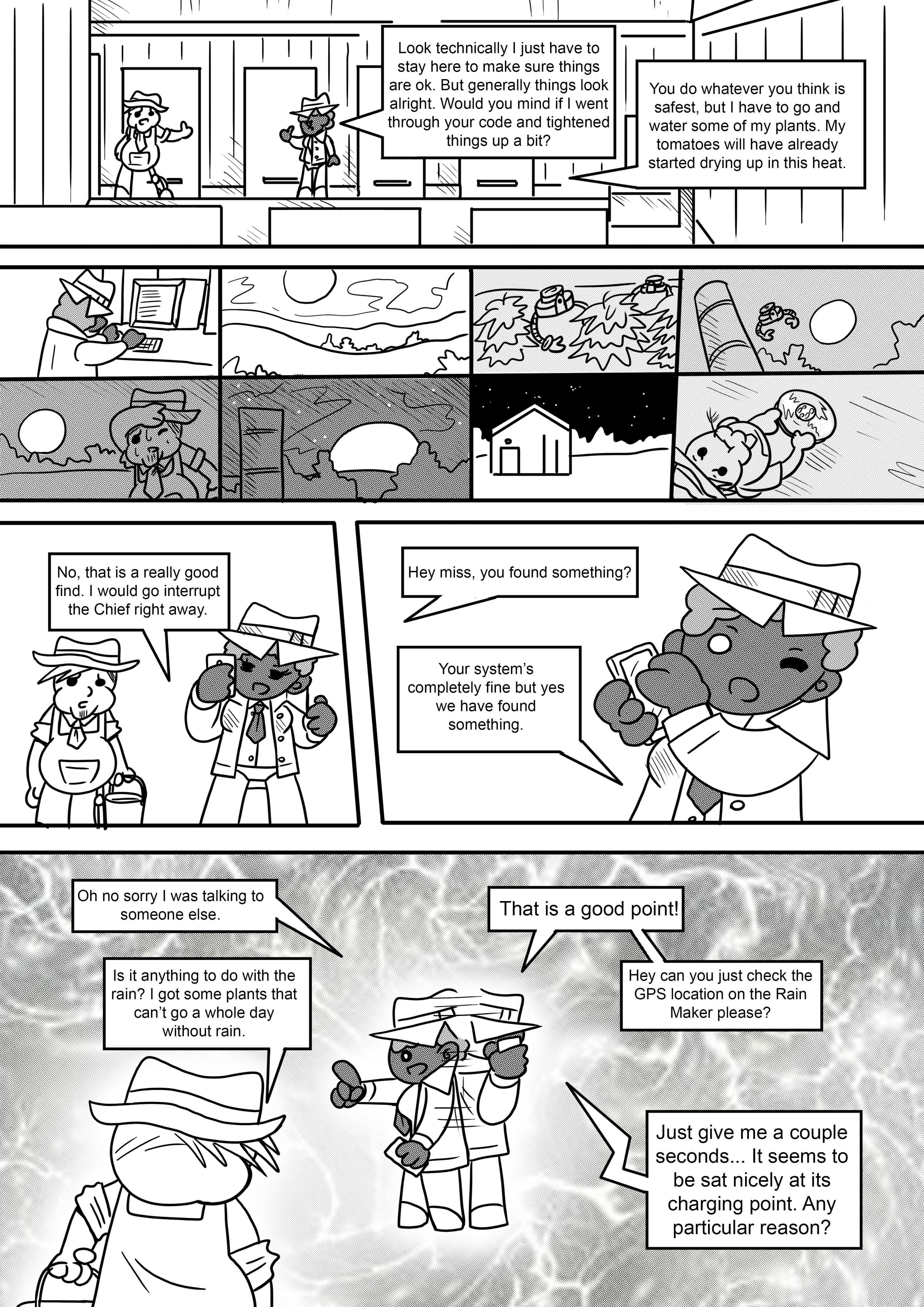

We didn't find anything in the analysis of the hard drives, they've encrypted the data before they destroyed it.
Have you checked the RAM? You can find all sorts of old memory artefacts in there, process information, file information, network information, they can all leave digital traces.
Of course the RAM! If it was the last process the drone computed then the information would have had to be decrypted. Thank you Detective.
I heard you talking on your phone. Just a quick question why would somebody encrypt data only to delete it?
Because deleting data on a disk is actually not easy. A lot of computers simply delete the metadata that makes the information appear as a file, but not the content. If you can access the file blocks then you can read the content, even though it doesn't appear in the file system. These attackers created an encrypted container and then deleted that, so even if we do get it back, it will all be garbled without the encryption key.
I suppose that kinda makes sense.
Hey look it's not like you're under investigation but I do need you to show me your cyber security.

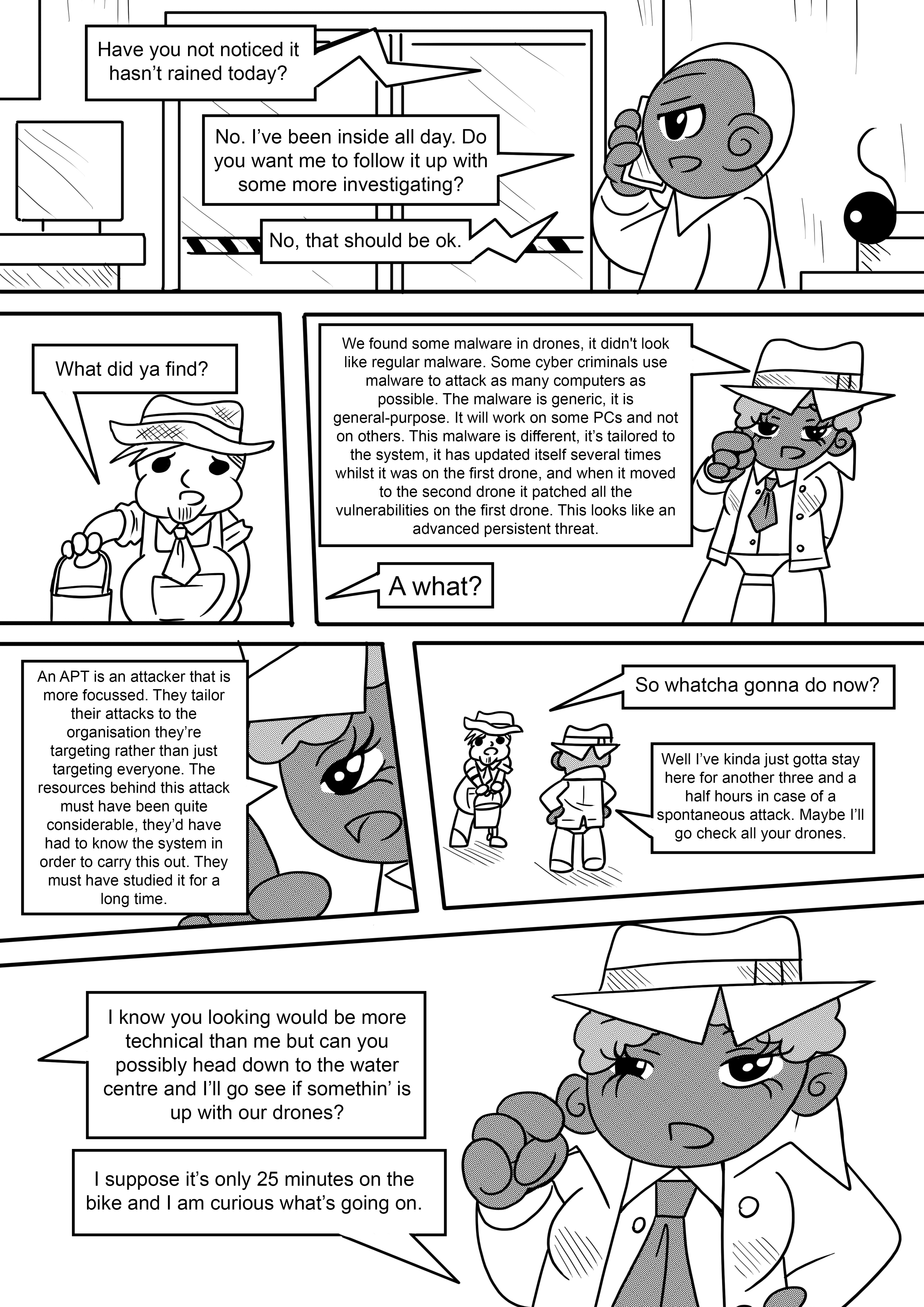

This is the whole control centre for my farm. I built a lot of the software here myself!
What language is this written in?
C++ like my daddy used and my granddaddy before him. We like the old ways out here don'tcha know yessirree. That there computer runs all the sensors.

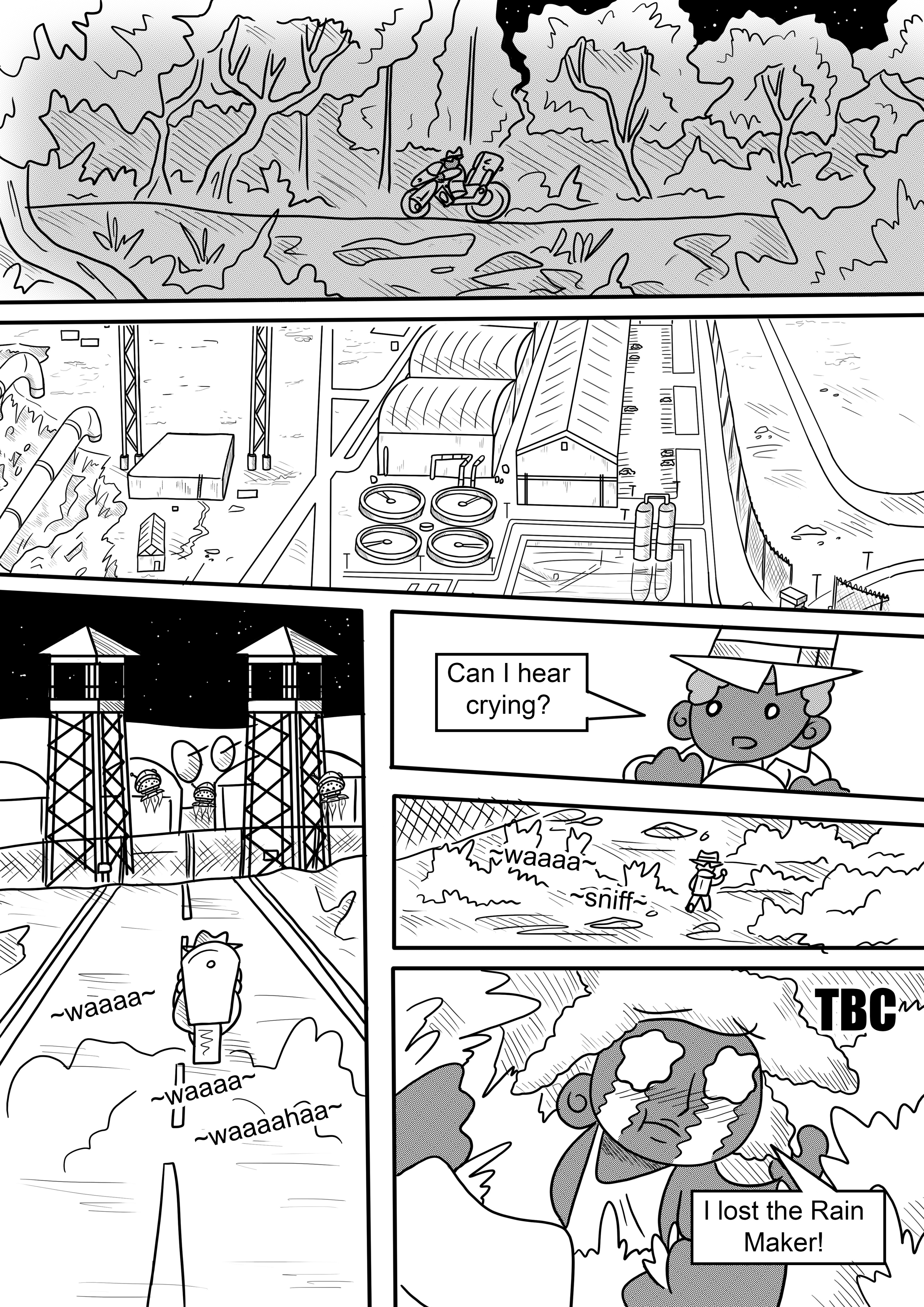

That's a memory unsafe language, an attacker could probably use a stack buffer overflow attack on this device without much of a problem.
A buffer-whoey-who?
It's an attack that violates the memory management of the stack. The stack stores function argument data that –
Now see here maam I know what a stack is
Okay fine. So you know then that the stack uses a temporary memory allocation called a buffer which is usually a fixed size, and also uses return addresses that direct the application to its next instruction.

A stack buffer overflow attack essentially floods that memory buffer with inputs beyond the limit of its fixed-size, so that the inputs begin to overwrite the other areas of the stack. For example, an attacker could overwrite the buffer with malicious code, and overwrite the return addresses to point to that code in the buffer so that the processer executes it.
Say what?
I'm saying that the programming language you choose to write software matters greatly, you should really think harder about security.
Well I'll be damned. I had no idea that we were so vulnerable to all them malware-bootin nasties out there. Any advice on how to secure our systems?
Well first of all I'd always suggest prevention, plenty of other software languages like Java or Rust work hard to limit these vulnerabilities. Other techniques like guard pages and canary help you spot when the overflows are happening.
Lady, I been writin' in C++ for damn near 20 years, I can't change my ways.
Well then I'd suggest hiring a software security team to run static analysis on your software's source code. Heuristic static analysis will detect violations of rules that are considered secure programming heuristic. It will check that your code doesn't fall foul of common mistakes that leave you open to vulnerabilities.

Sound static verification will look for specific types of vulnerabilities with an excellent success rate. The two methods complement each other quite well, and can be used as code is still in development so that it's safe on delivery.


Look technically I just have to stay here to make sure things are ok. But generally things look alright. Would you mind if I went through your code and tightened things up a bit?
You do whatever you think is safest, but I have to go and water some of my plants. My tomatoes will have already started drying up in this heat.
No, that is a really good find. I would go interrupt the Chief right away.
Hey miss, you found something?
Your system's completely fine but yes we have found something.
Oh no sorry I was talking to someone else.
That is a good point!
Is it anything to do with the rain? I got some plants that can't go a whole day without rain.
Hey can you just check the GPS location on the Rain Maker please?
Just give me a couple seconds... It seems to be sat nicely at its charging point. Any particular reason?


Have you not noticed it hasn't rained today?
No. I've been inside all day. Do you want me to follow it up with some more investigating?
No, that should be ok.
What did ya find?
We found some malware in drones, it didn't look like regular malware. Some cyber criminals use malware to attack as many computers as possible. The malware is generic, it is general-purpose. It will work on some PCs and not on others. This malware is different, it's tailored to the system, it has updated itself several times whilst it was on the first drone, and when it moved to the second drone it patched all the vulnerabilities on the first drone. This looks like an advanced persistent threat.
A what?
An APT is an attacker that is more focussed. They tailor their attacks to the organisation they're targeting rather than just targeting everyone. The resources behind this attack must have been quite considerable, they'd have had to know the system in order to carry this out. They must have studied it for a long time.
So whatcha gonna do now?
Well I've kinda just gotta stay here for another three and a half hours in case of a spontaneous attack. Maybe I'll go check all your drones.
I know you looking would be more technical than me but can you possibly head down to the water centre and I'll go see if somethin' is up with our drones?
I suppose it's only 25 minutes on the bike and I am curious what's going on.


~waaaa~
~waaaa~
~waaaahaa~
Can I hear crying?
~waaaa~
~sniff~
I lost the Rain Maker!
TBC