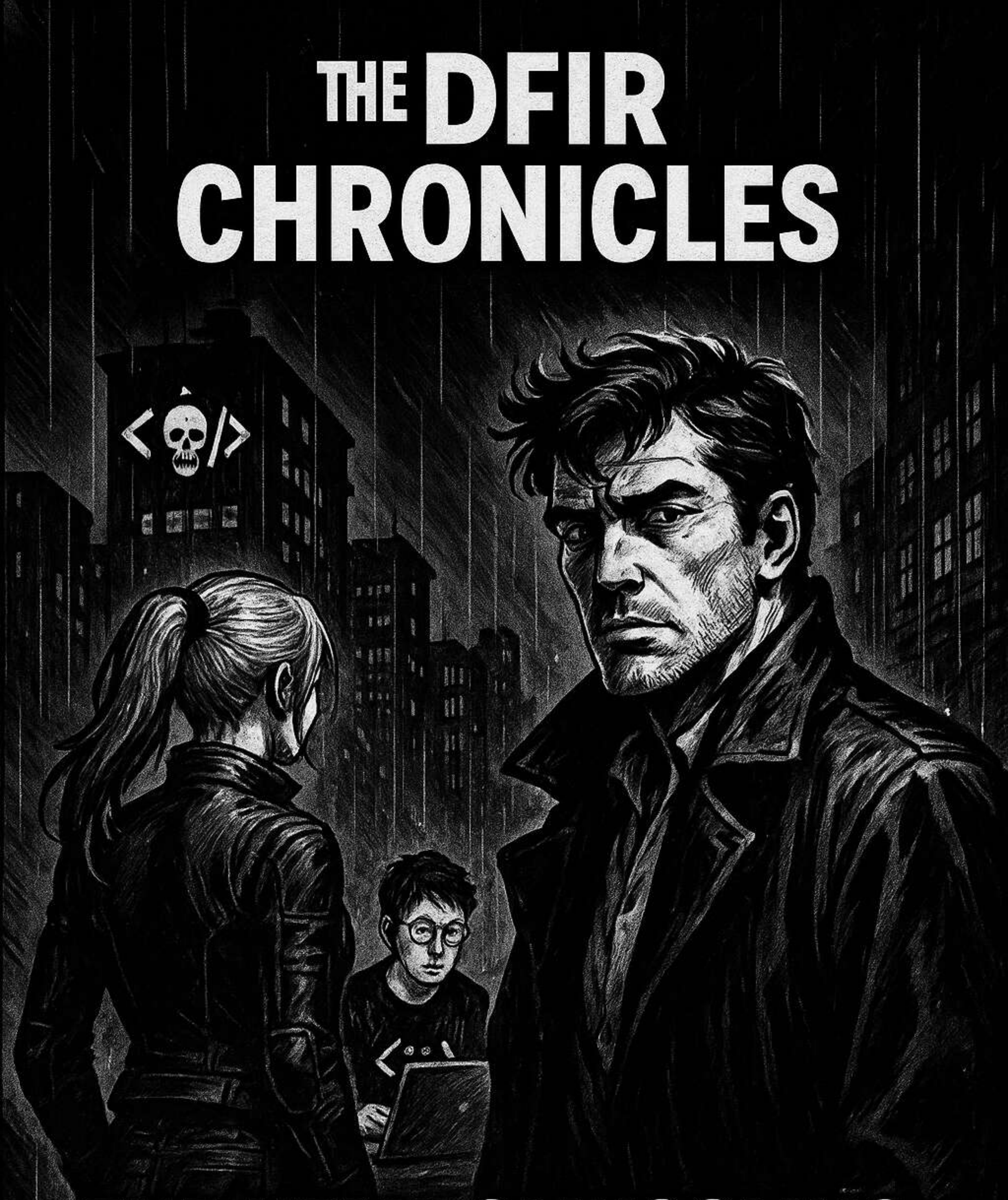
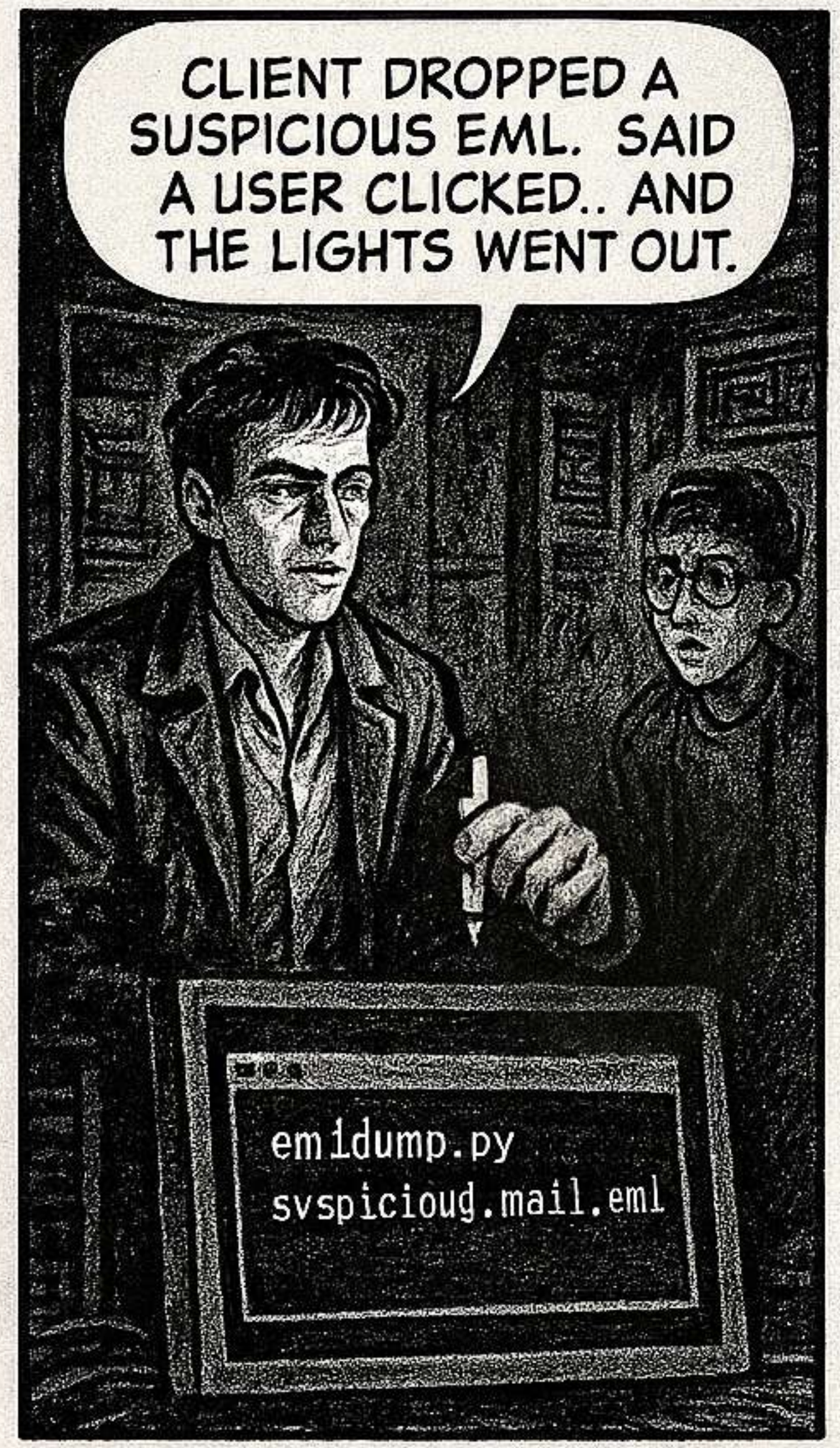
THE DFIR CHRONICLES



THE HTML SMUGGLING PHISHING ATTACK

THE DFIR CHRONICLES



THE DFIR CHRONICLES

Single attachment: invoice...Q2..update.html. Let's peel this onion.

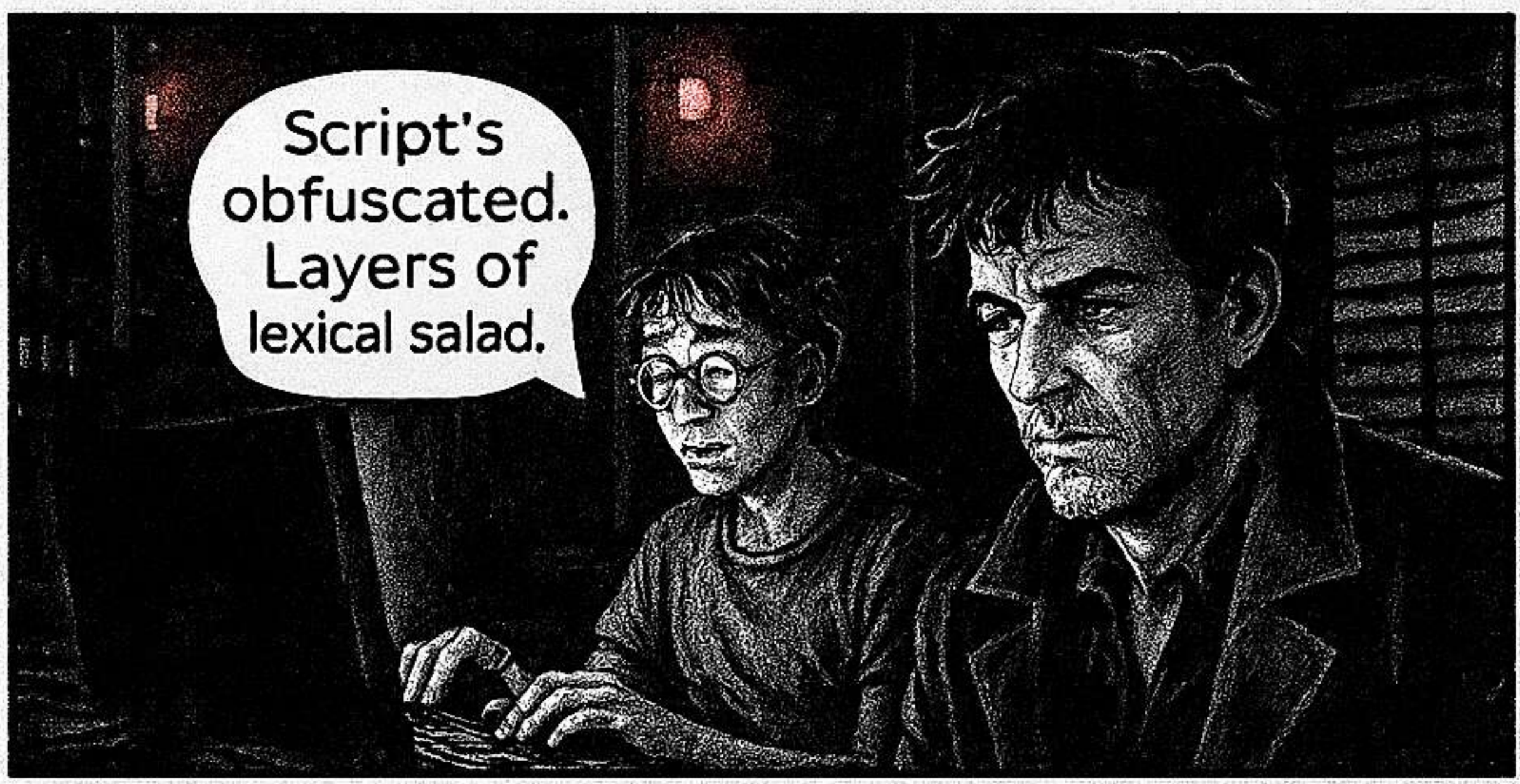
Client said nothing about scripts?

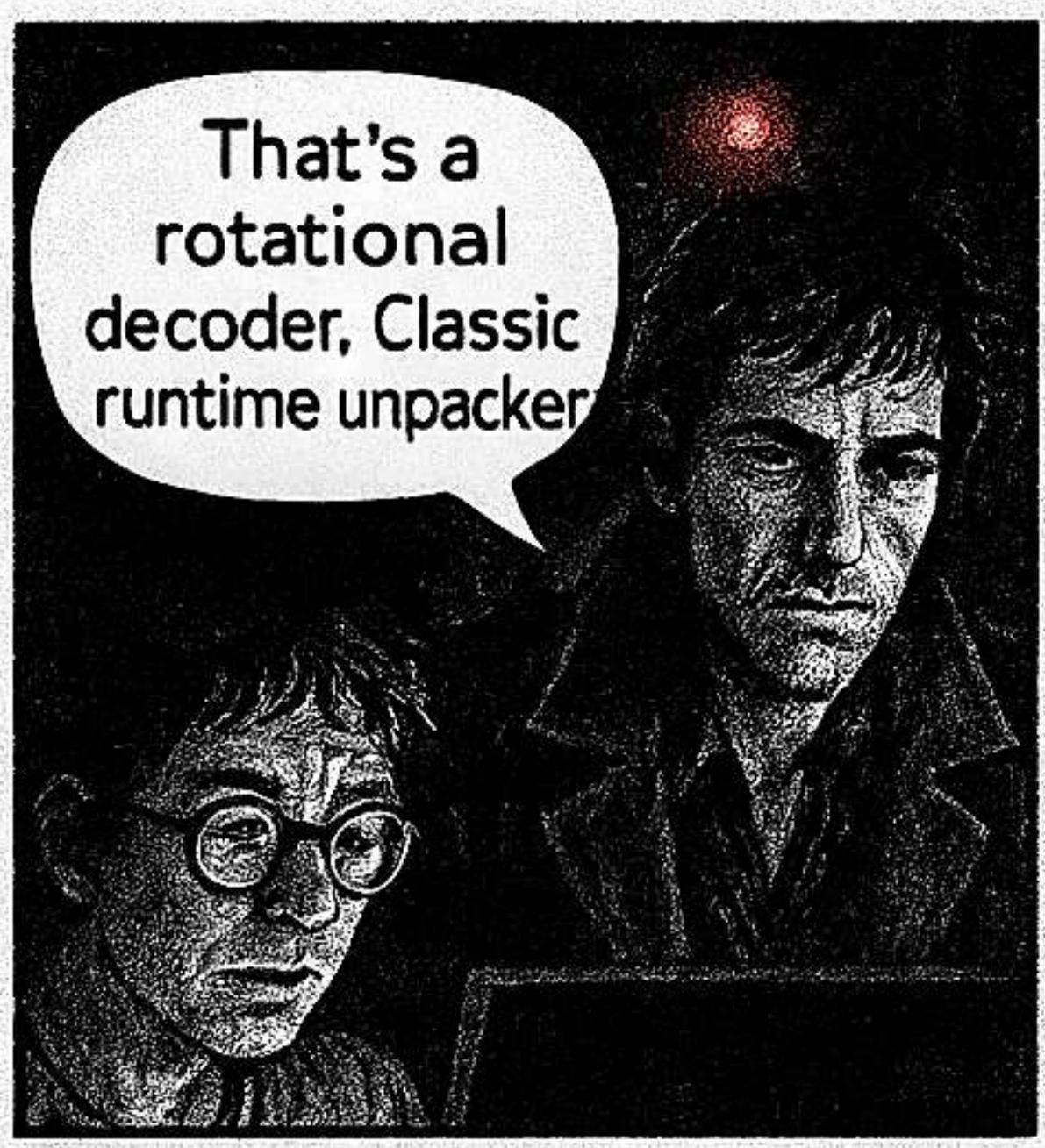
<script> tag detected inside the HTML

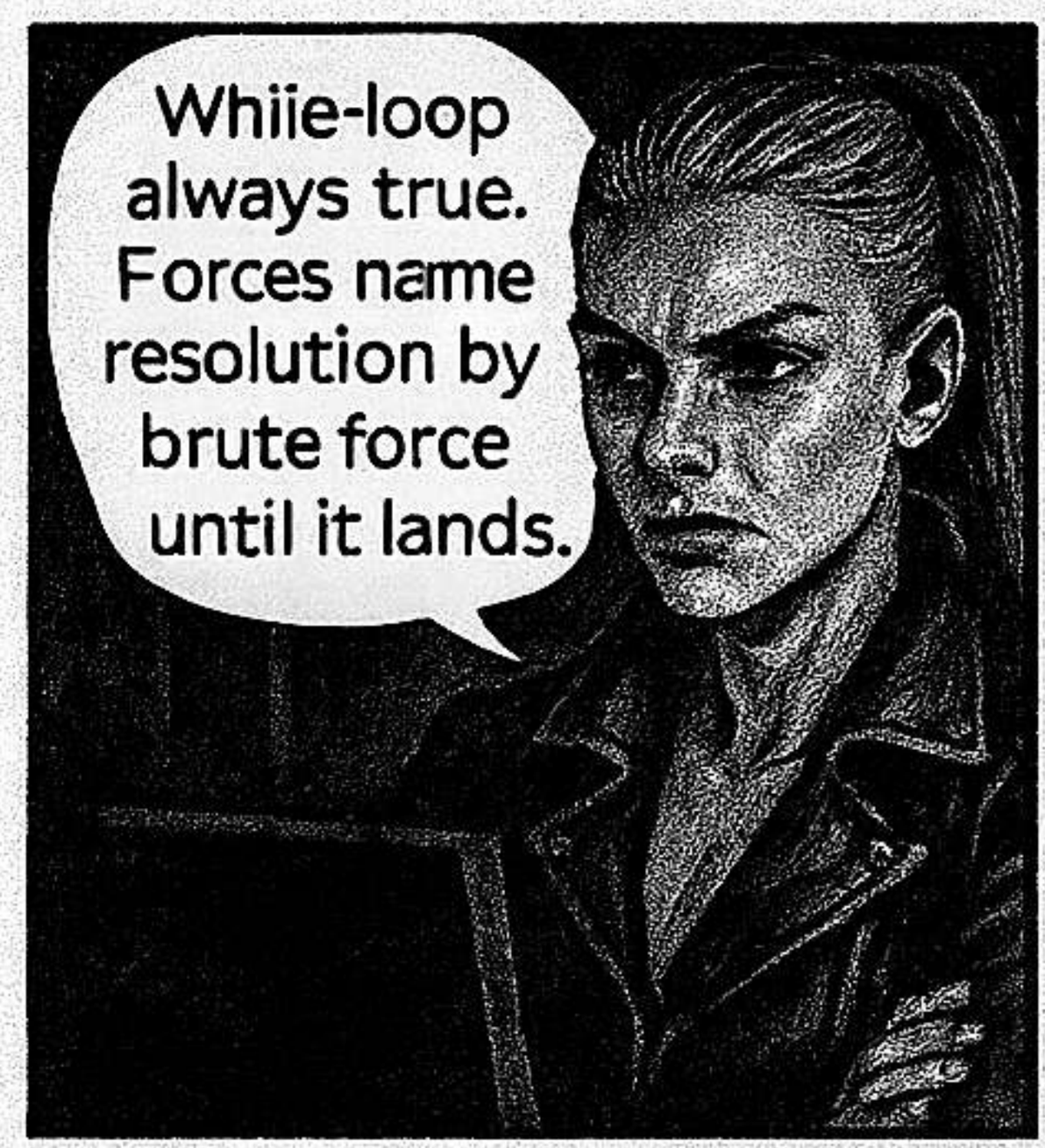
They never do. They just see a blinking PDF icon and click.

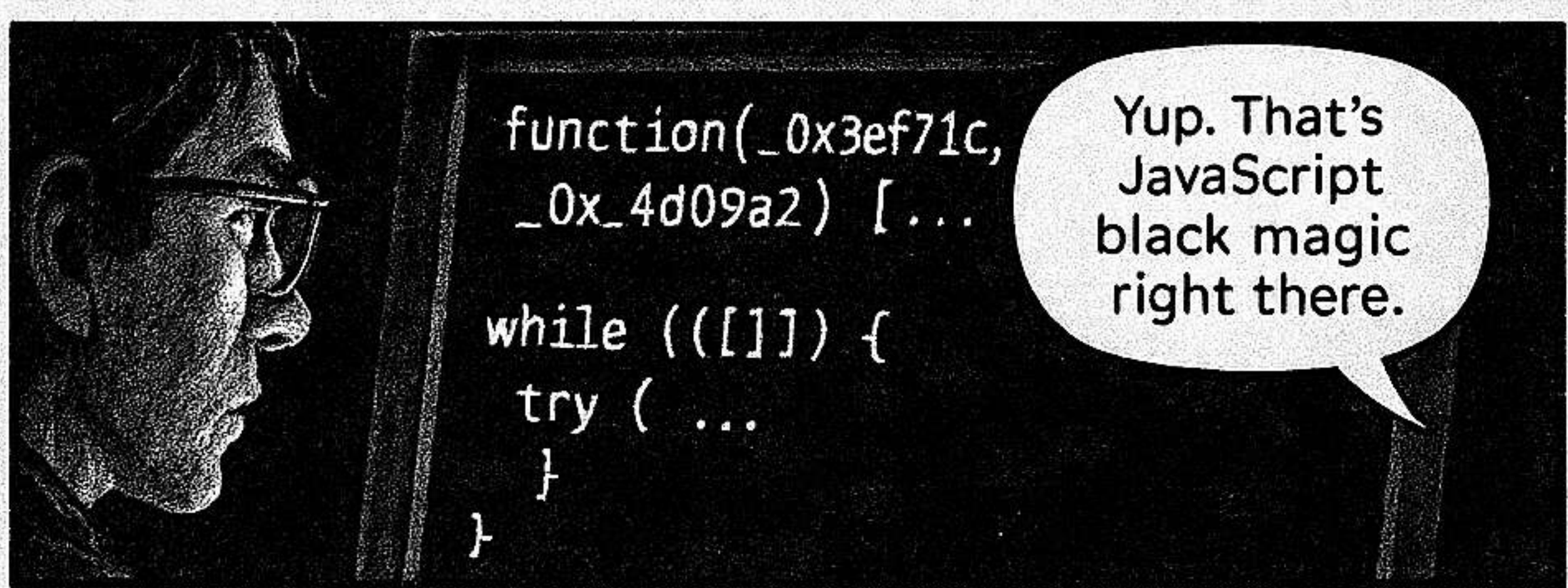
Classic move. This one's hiding something deep.

THE DFIR CHRONICLES





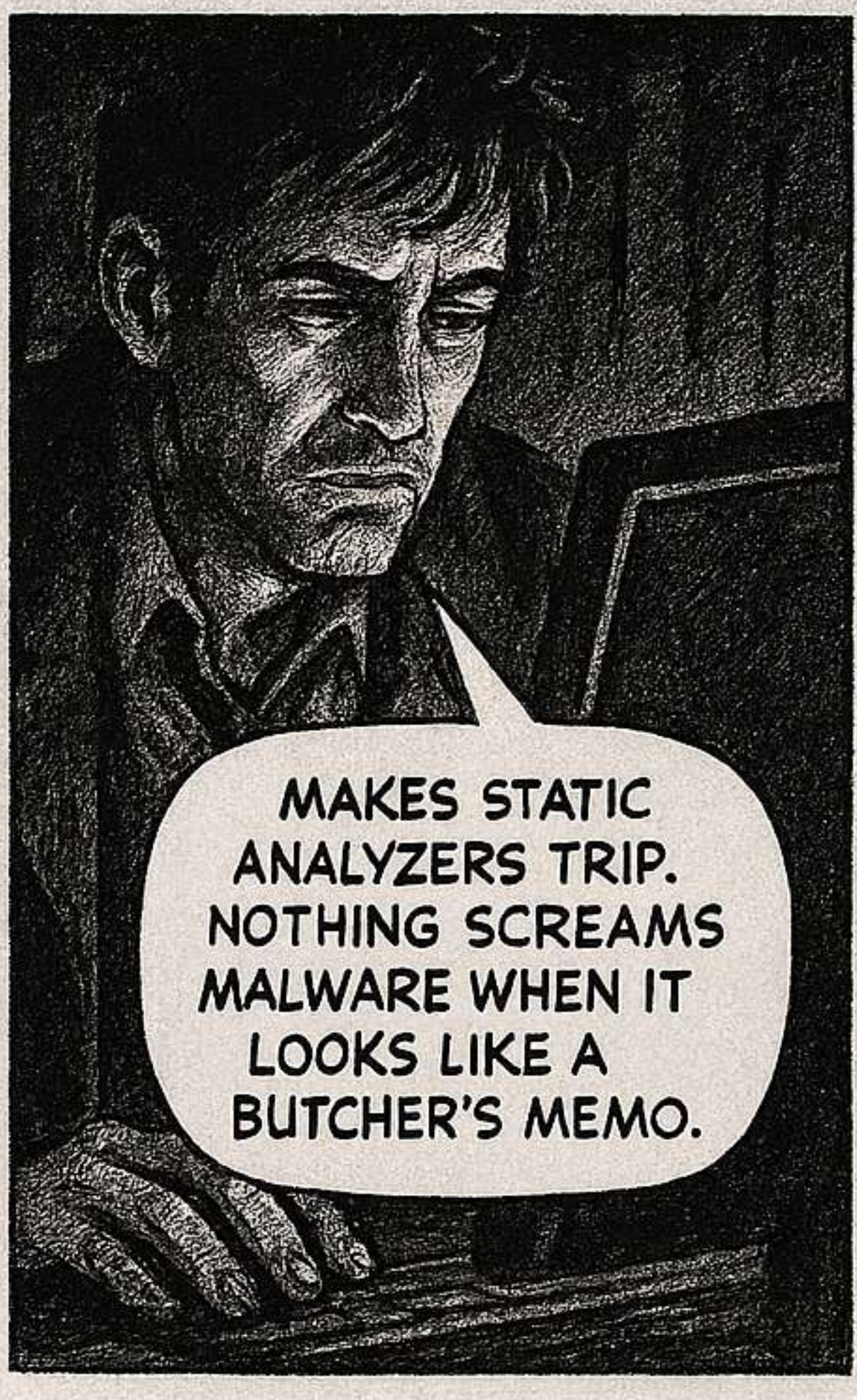




THE DFIR CHRONICLES

LOOK HERE. EMBEDDED NOISE WORDS.

burgdoggen
beef pancetta
sirloin
porchetta
alcatra pork



THE DFIR CHRONICLES

FOUND THESE TAGS BURRIED INSIDE THE HTML.,

mario.rossi@
company.it<
</om>

<az
ad0ãcBov
LzJk2BV:

THE IS THE BAIT. THE <a> IS ENCODED– BASE 64. CLEARLY.

<a>HRDcDovLzJJk2GVrci
jcrmVhc2ViaGAFtmGiivn
mu.Y29t≠20s<
</a>

DECODE IT. NOW.

```
echo "ahRTcDovLzJZjk2GVrci.jcmVhcz2
jcmJejAFtmcPivbnSu.V20"
| base64 -d
```

THE DFIR CHRONICLES

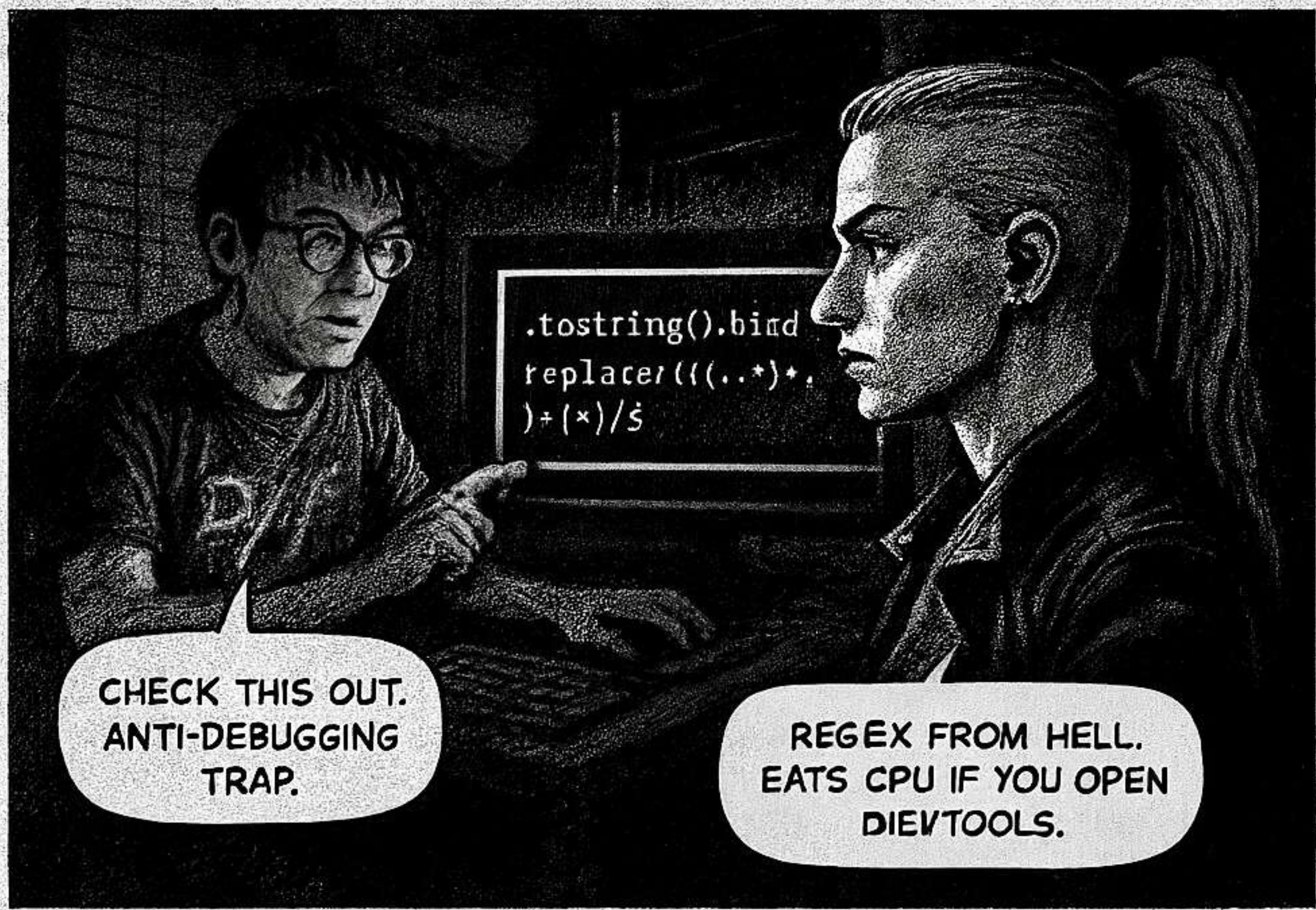
THE DFIR CHRONICLES

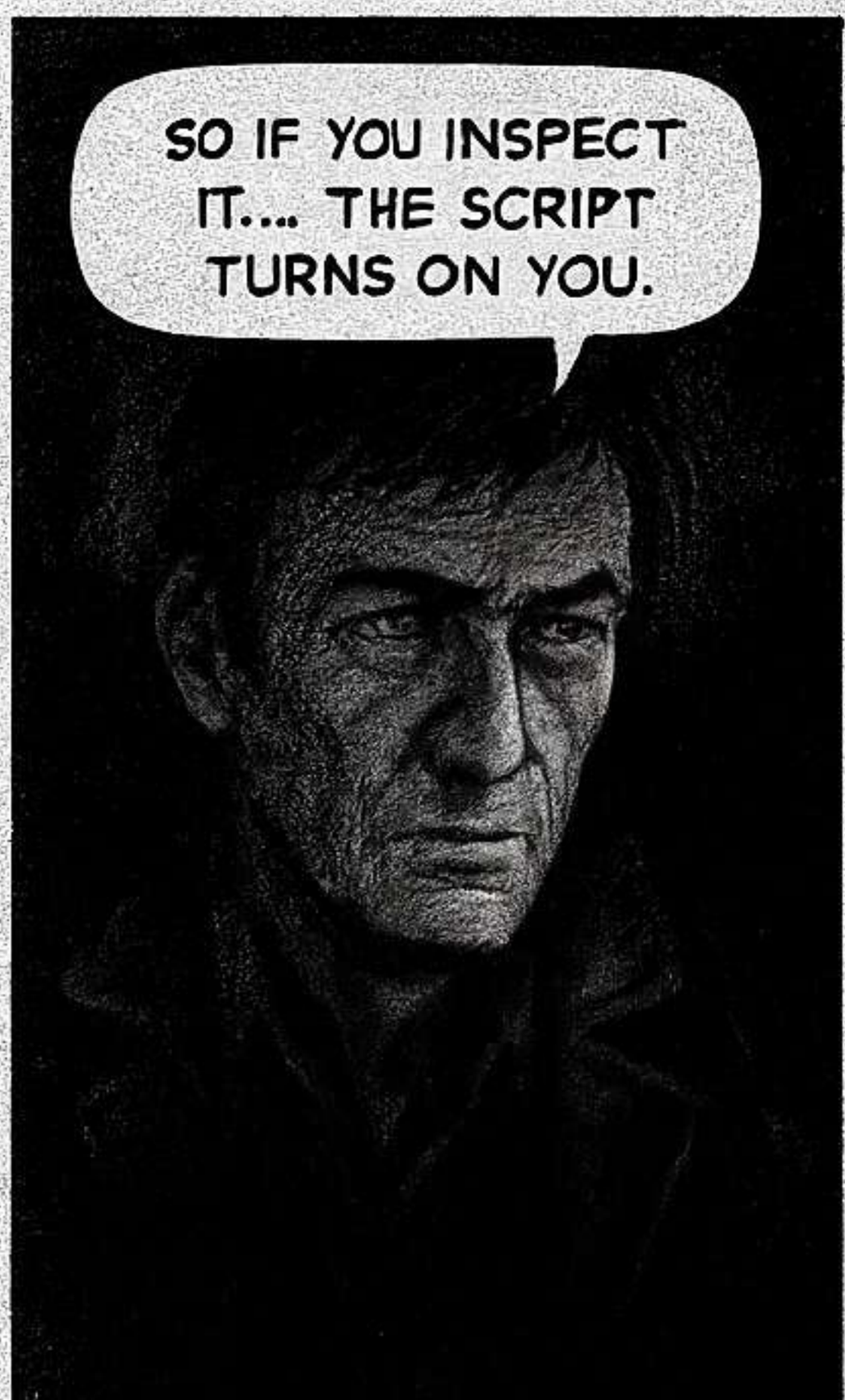
SHOW ME THE PAYLOAD TRIGGER,

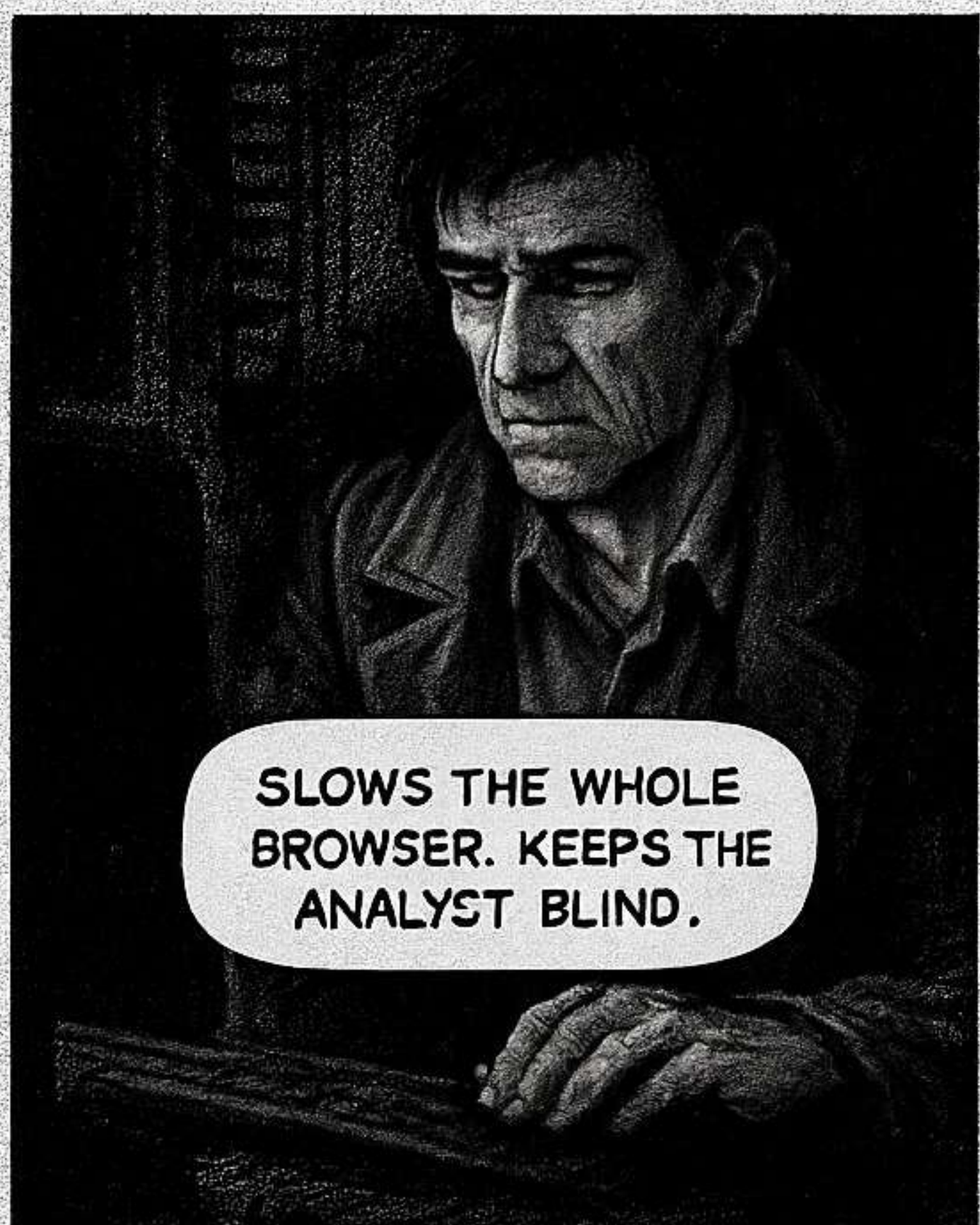
```
var em-document['getElements
ByTagName>('em'][0]'InerHTML;
 var a-ateb{
document['gelFlementByTName
'(5][[0]'InnerHTML'];
  Location
['search"(a)+'+em);
```

A smooth ride into vicin-mis trust zone.

THE DFIR CHRONICLES.

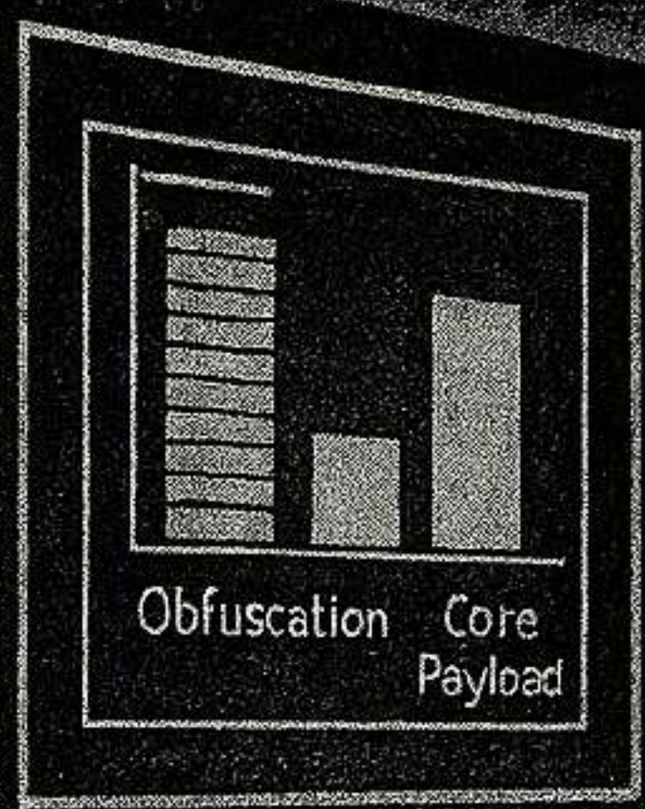




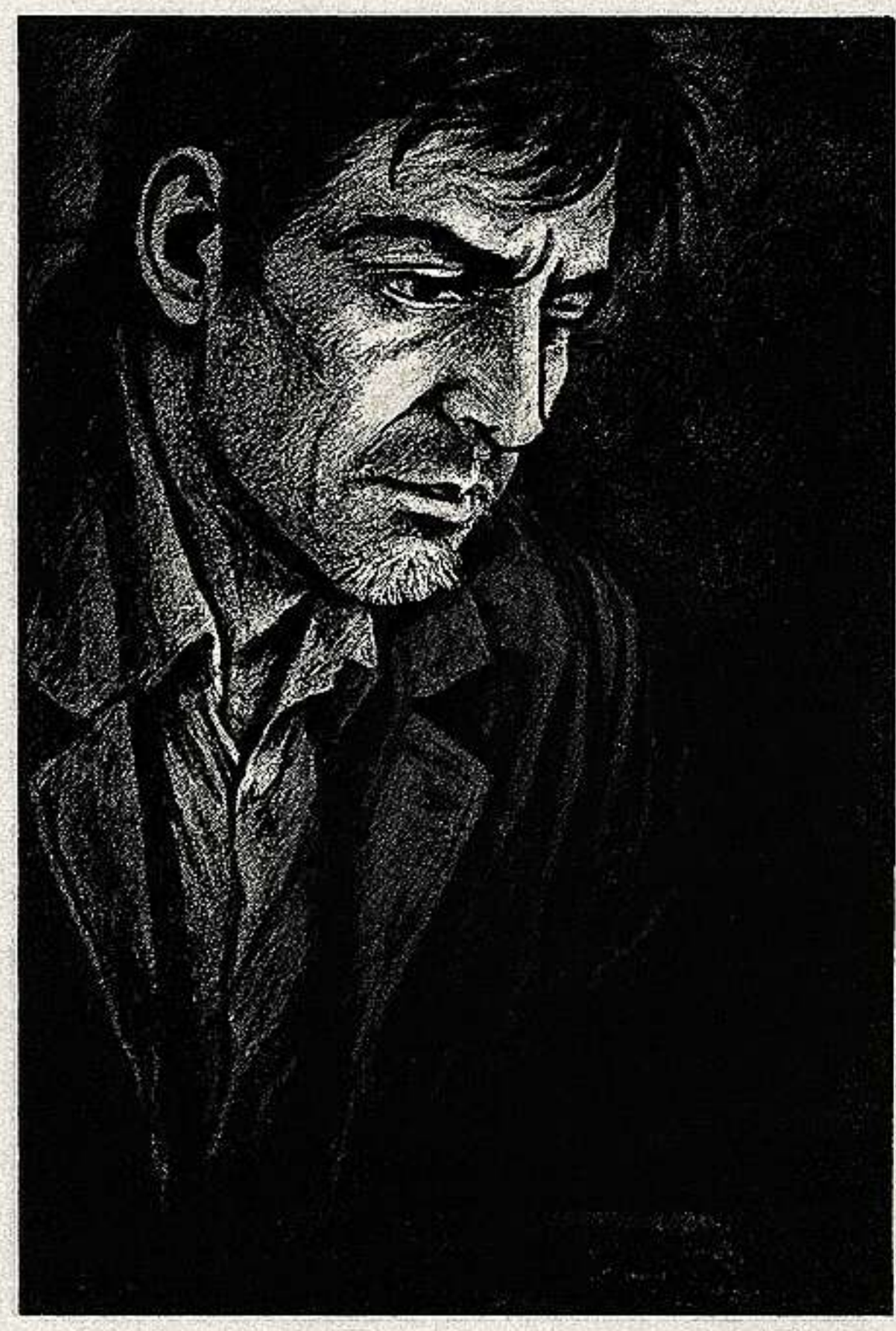


The DFIR Chronicles

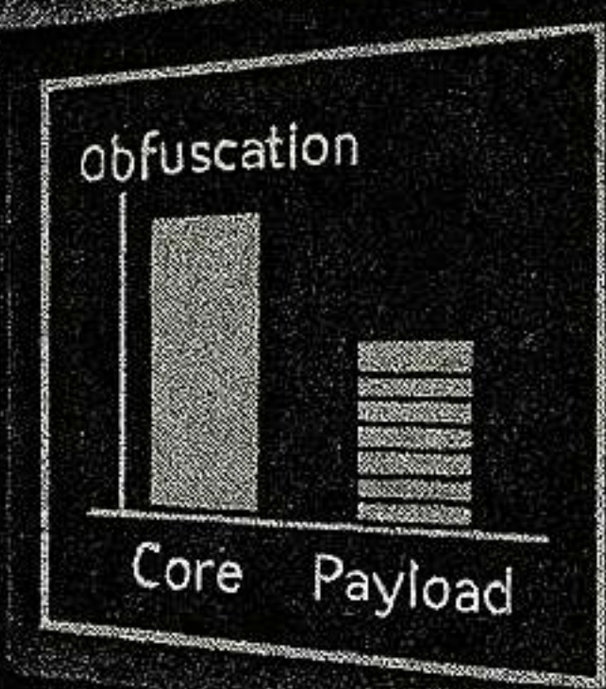
Estimate: 65% of script is pure evasion.



That's dedication. No payload until the script's sure it's safe.



It's like a snake that checks for footprints before slithering out.



THE DFIR CHRONICLES

TELL ME SOMETHING, BYTE. COULD WE CATCH THIS BEFORE THE CLICK?

IF WE BLOCKED HTML ATTACHMENTS, SURE.

IF WE LOGGED '.INNERHTML' AND 'atob()' ABUSE, MAYBE.

AND IF WE EDUCATED USERS?

NOW THAT'S FANTASY, DETECTIVE.

THE DFIR CHRONICLES

Mitigations, Let's be clear.

Block HTML on gateways. Detect runtime behavior. Teach the

Mitigation summary:

Block HTML
Detect Js Behavior
Awareness Training

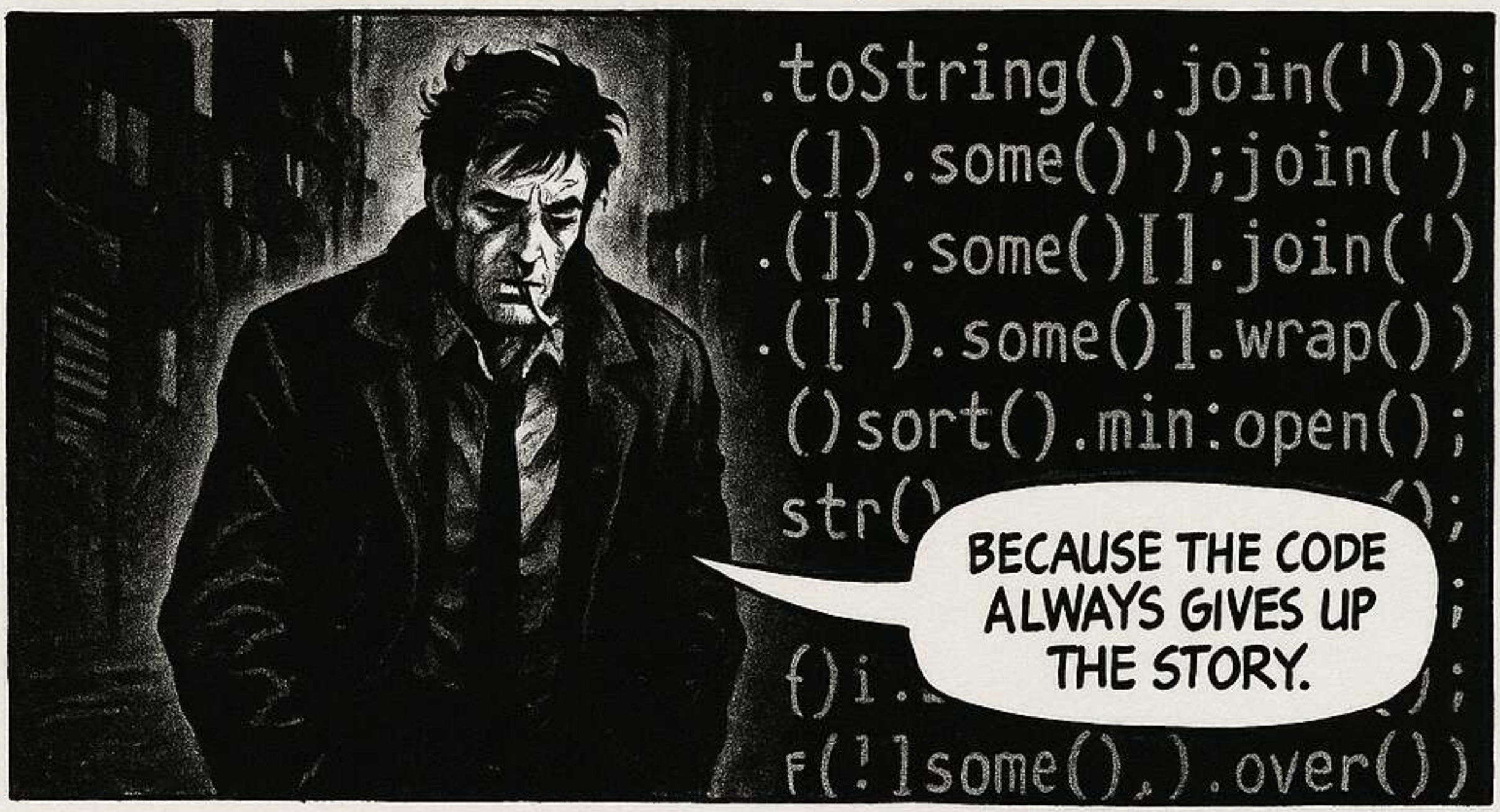
Let's not start a culinary war, Bitty.

And maybe... ban bacon wards from scripts?

THE DFIR CHRONICLES

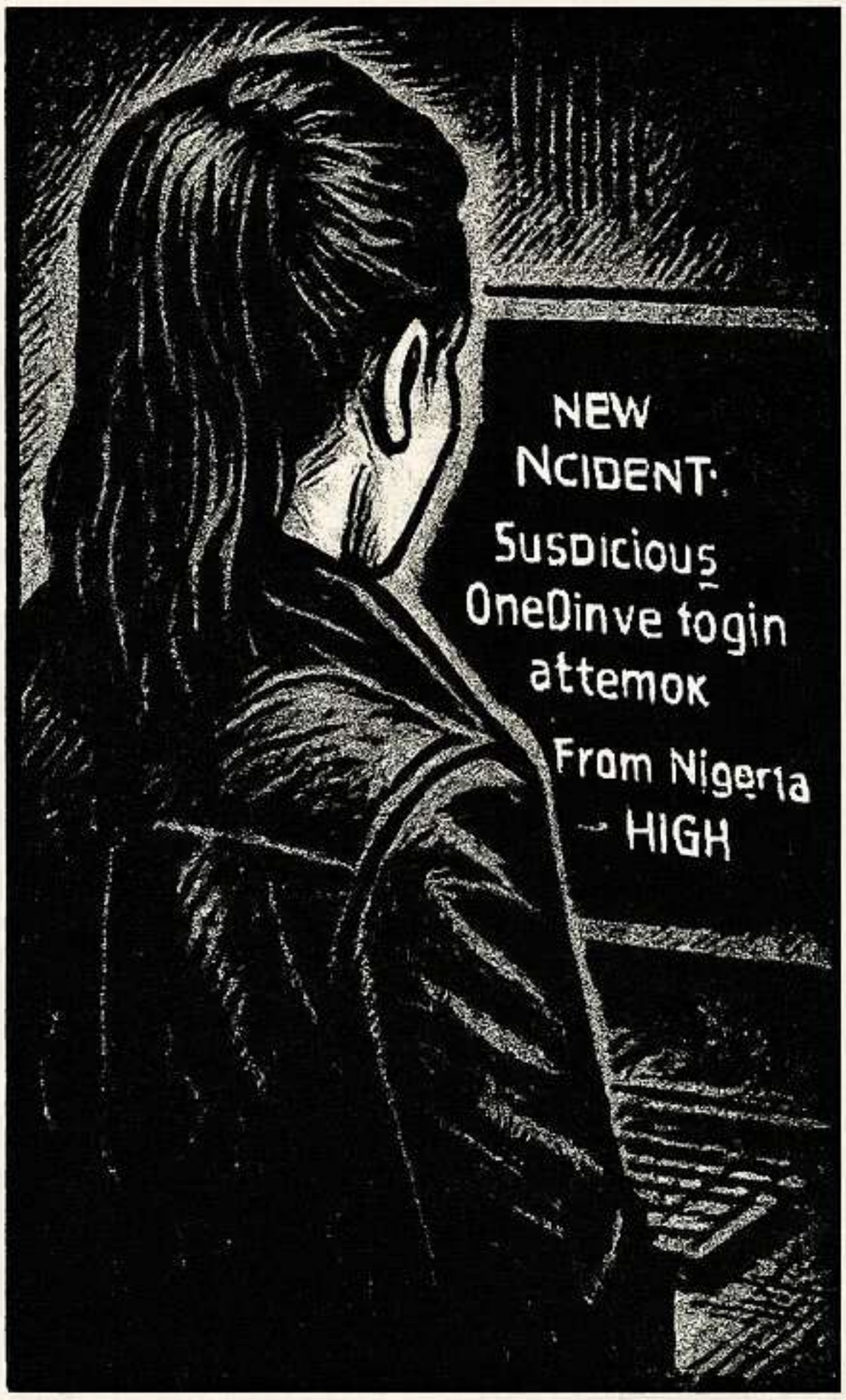
THE DFIR CHRONICLES

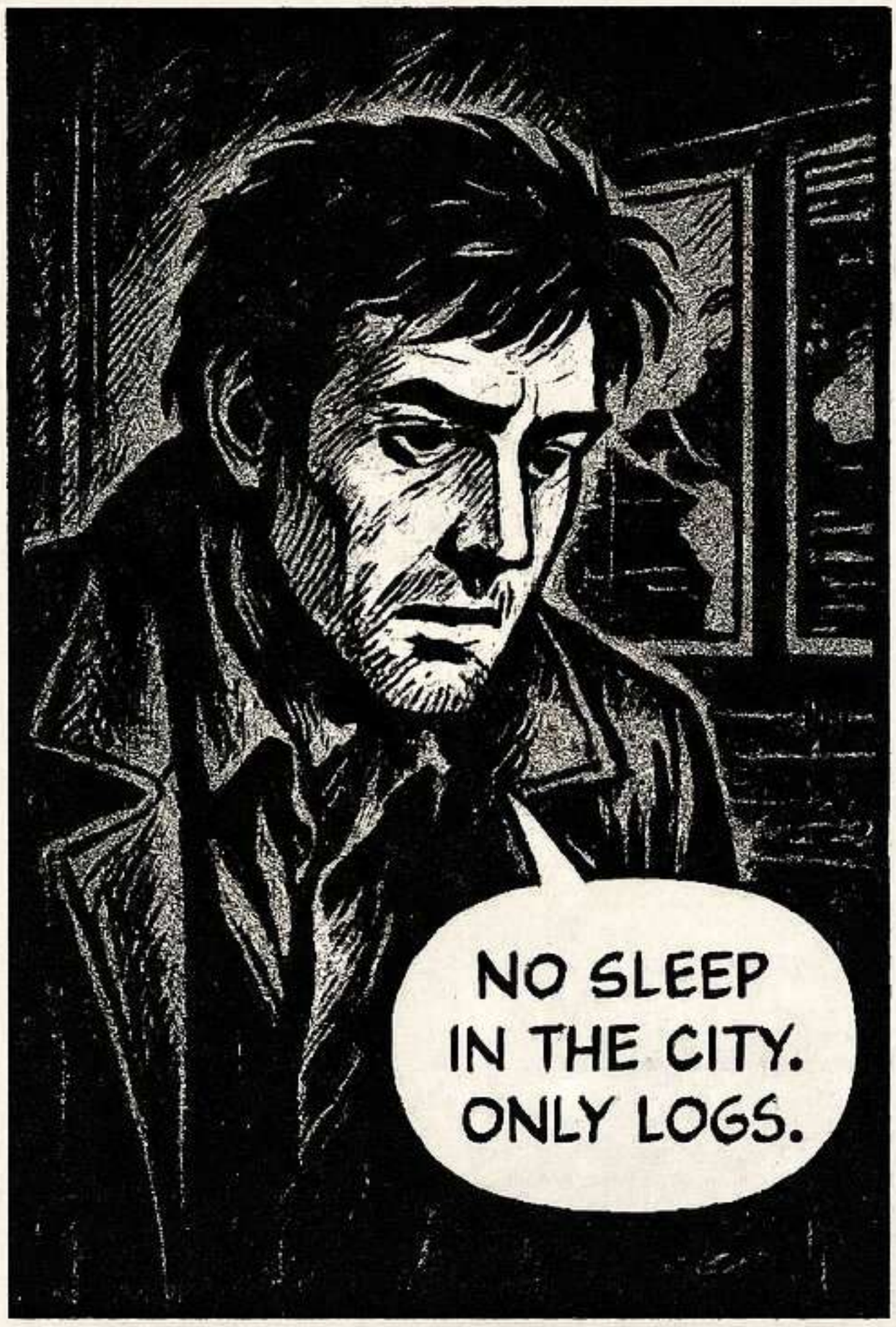
THEY HIDE IN THE STATIC, WRAP MALWARE IN LAYERS OF MEAT AND MADNES. BUT WE SEE THEM.



THE DFIR CHRONICLES

NO REST FOR THE ANALYSTS.





THE DFIR CHRONICLES

ANOTHER SMUGGLER STOPPED.

FOR NOW.

UNTIL THE NEXT ONE BRINGS FOIE GRAS AND SHELLCCODE.

```
GET /office-login.php?e
=mario.rossi@company.it
```

...TO BE CONTINUED