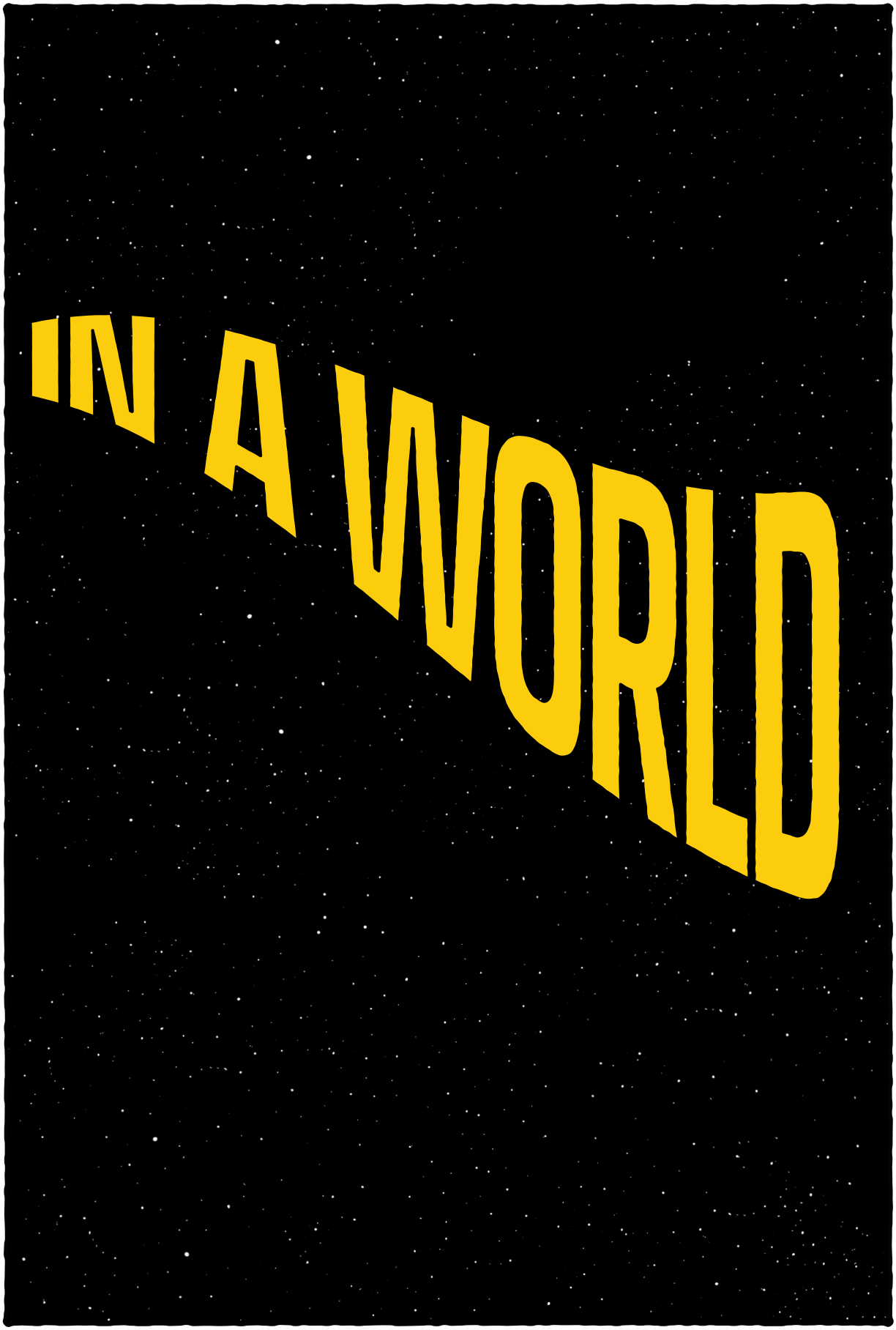
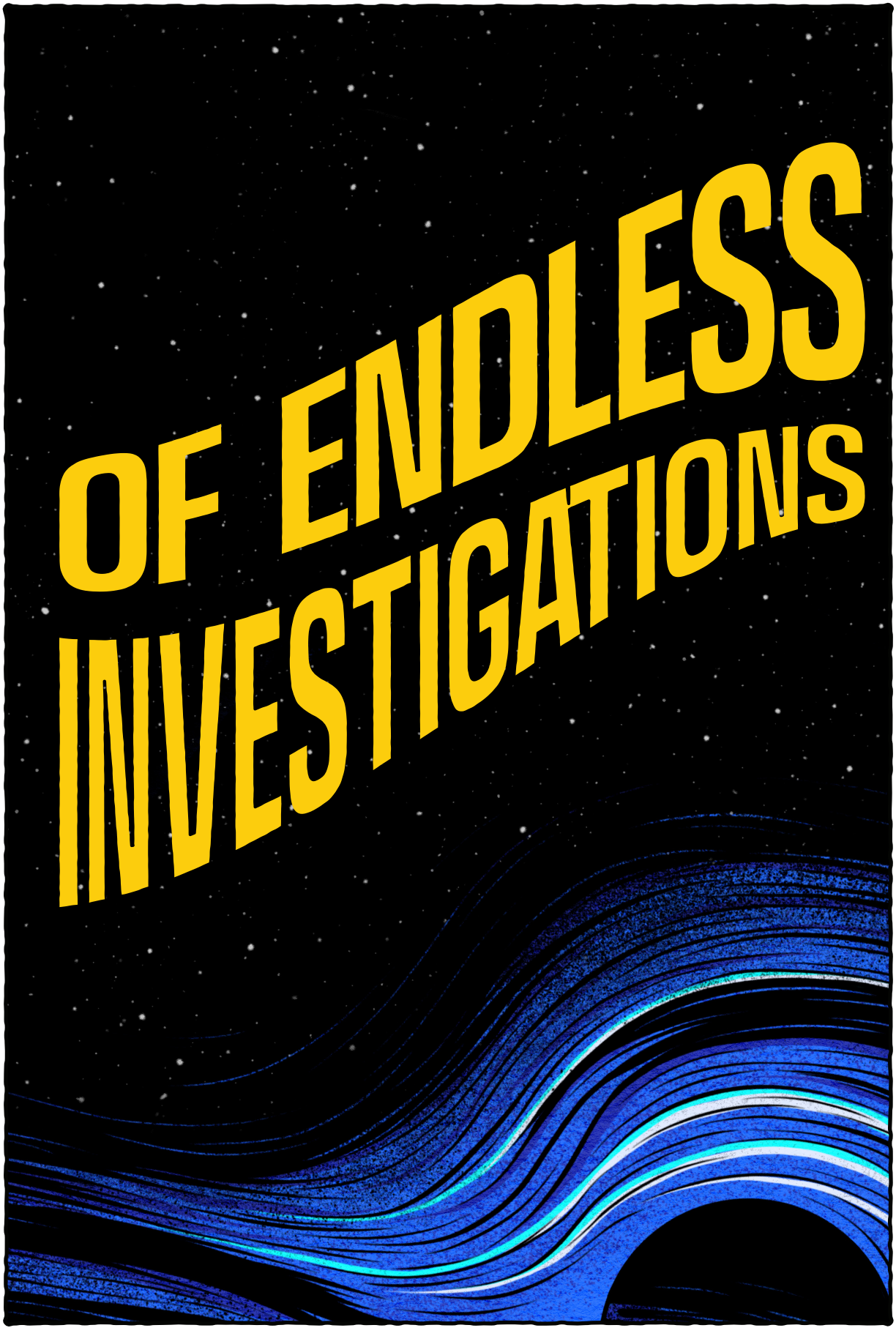
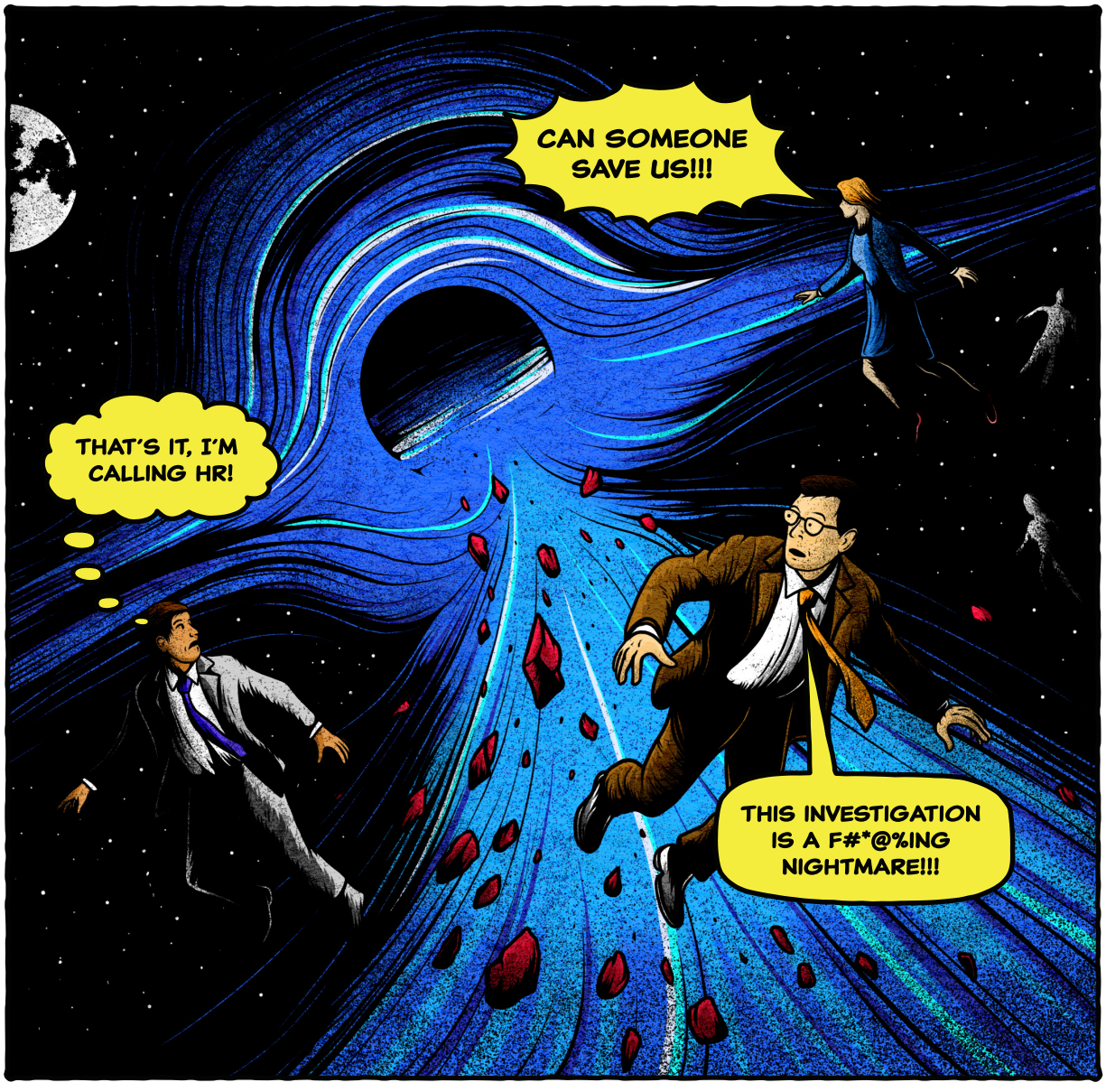

binalyze!
COMICS
5.0
AIR
13
SEPT
ESCAPE THE SOC
BLACKHOLE
AIR 5.0
IS LIVE
AIR 5.0
BINALYZE COMICS


IN A WORLD

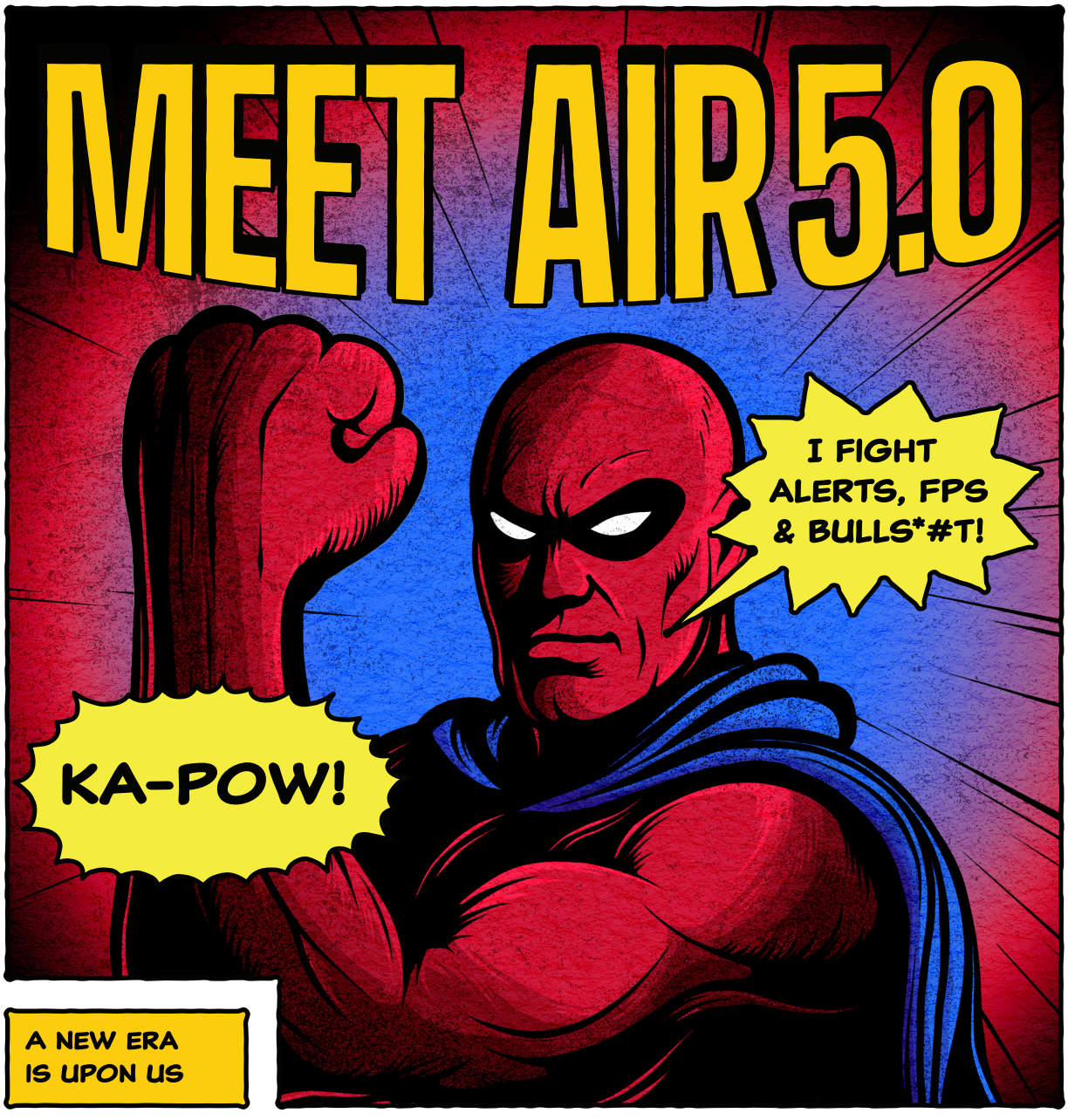

OF ENDLESS
INVESTIGATIONS

WHERE ANALYSTS DISAPPEAR, AND SOC TIME IS LOST FOREVER IN THE VACUUM OF SPACE. WITH ENDLESS TICKETS, OUTDATED TOOLS, AND WORKFLOWS BUILT FOR A DECADE AGO... SOUNDS ABSURD, BUT IT'S ALL TOO REAL!

WELCOME TO THE INVESTIGATIONS BLACKHOLE

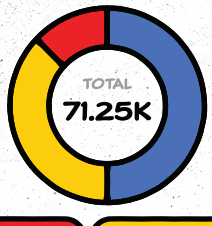


MEET AIR 5.0



A NEW ERA IS UPON US

SCALABLE PRECISION HUNTING



104 HIGH | 14,715 MEDIUM | 20,187 LOW

UNIFIED HUB FOR DEEPER ANALYSIS

AIR

DASHBOARD

ASSETS 14

EVIDENCE CATEGORIES 159

TOTAL EVIDENCE 32,644,850

AUTOMATED TRIAGE

INITIAL ACCESS (244)

4 TECHNIQUES

EXPLOIT PUBLIC-FACING APPLICATION (7)

EXPLOIT PUBLIC-FACING APPLICATION (7)

EXTERNAL REMOTE SERVICES (1)

EXTERNAL REMOTE SERVICES (1)

SUPER-CHARGED TIMELINE ANALYSIS

TOTAL EVENTS

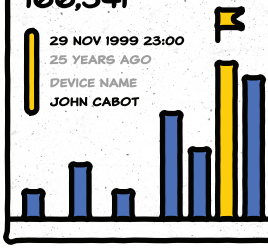
166,341

29 NOV 1999 23:00

25 YEARS AGO

DEVICE NAME

JOHN CABOT



THESE GUYS GIVE NEW MEANING TO THE TERM "LEGACY TOOLS"

YOU'RE NOT JUST FIGHTING BREACHES, YOU'RE FIGHTING...

MR. SPINNER

THE MASTER OF WASTED TIME. HE'LL TRAP YOU IN ENDLESS LOOPS UNTIL YOUR DEADLINES TURN TO DUST.

- STALLS EVERY RESPONSE
- SPINS INVESTIGATIONS IN CIRCLES
- TURNS MINUTES INTO MARATHONS
- DELAYS UNTIL CHAOS WINS

CAPT. RED TAPE

THE BUREAUCRATIC BRAWLER WHO STRANGLES PROGRESS WITH ENDLESS FORMS AND DENIALS.

- WRAPS TEAMS IN ENDLESS RULES
- STAMPS "DENIED" ON EVERY MOVE
- TURNS SIMPLE TASKS INTO EPIC SAGAS
- SMOTHERS SPEED WITH PROCEDURE

FORENSICO

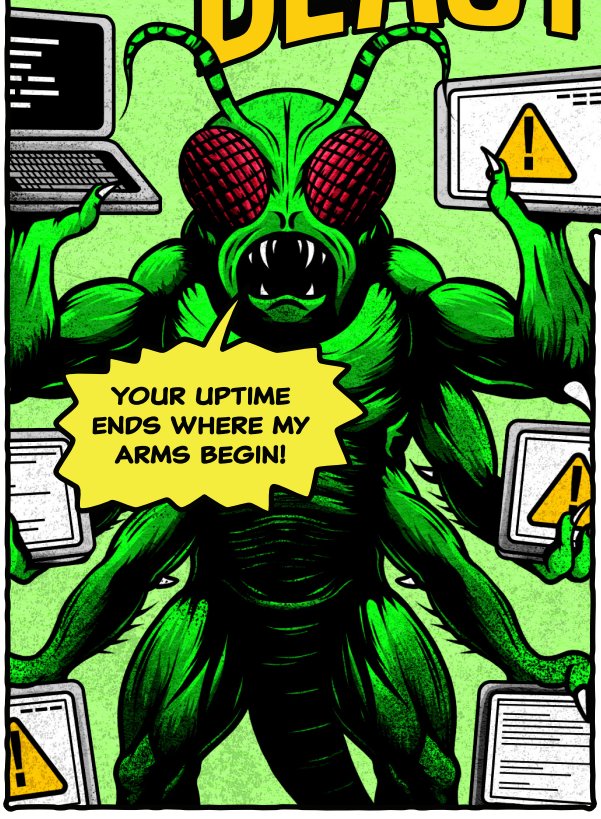
THE MENACE WITH A MILLION GADGETS. HE'LL TANGLE YOUR SYSTEMS AND BURY THE TRUTH IN ENDLESS SEARCHES.

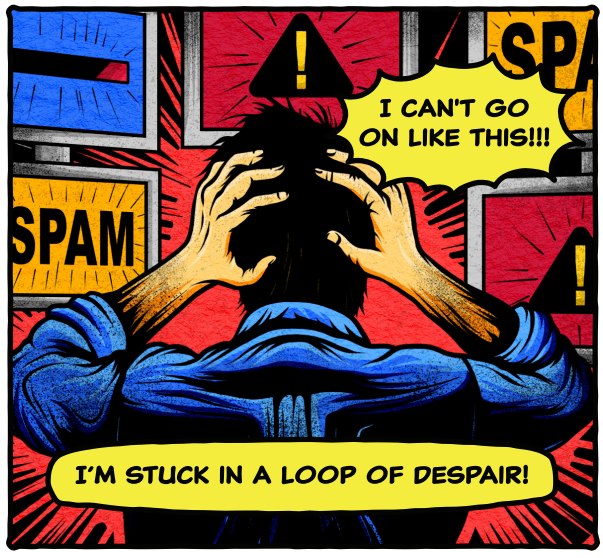
- SLOWS EVERY INVESTIGATION
- HIDES EVIDENCE IN PLAIN SIGHT
- OVERWHELMS TEAMS WITH USELESS DATA
- TURNS MINUTES INTO WEEKS

CONSOLE BEAST

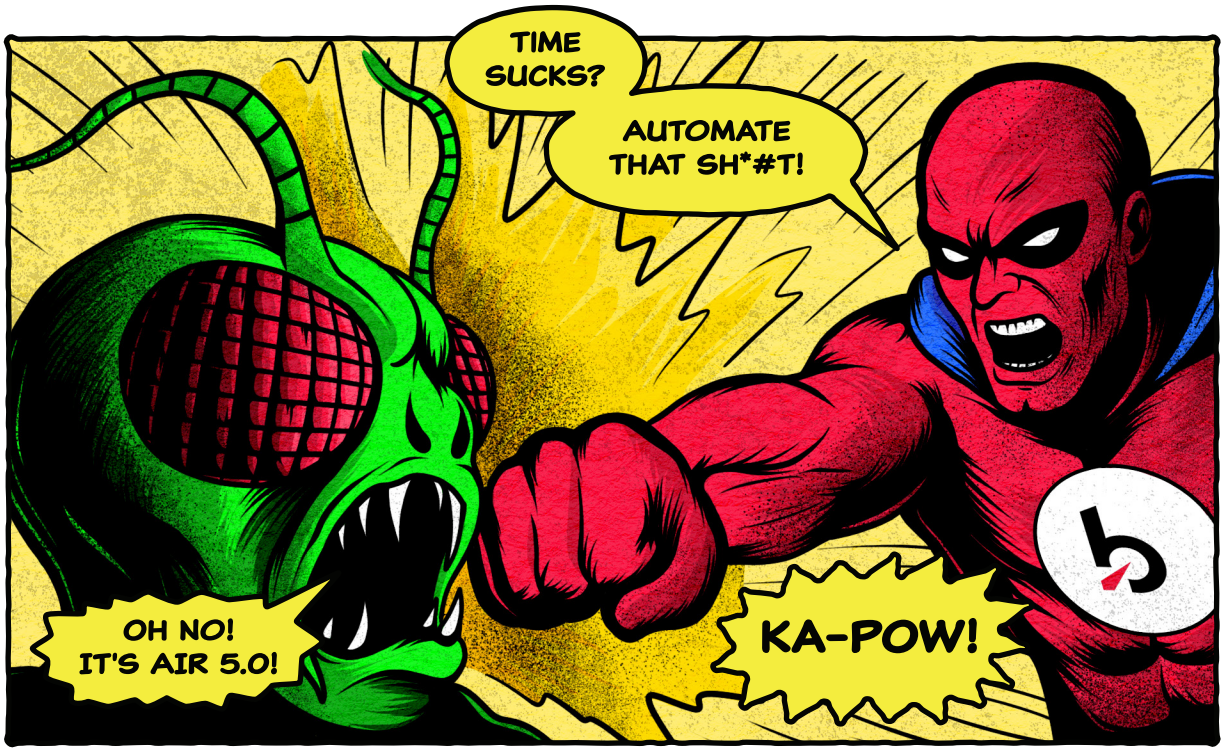
THIS BUG-EYED BRUTE SWARMS YOUR SYSTEMS, SMASHING STABILITY WITH EVERY LEAP.

- CRASHES APPS WITHOUT WARNING
- FLOODS SCREENS WITH ERROR ALERTS
- JUMPS FROM SYSTEM TO SYSTEM SPREADING CHAOS
- LEAVES DOWNTIME IN HIS WAKE






IN A WORLD WITHOUT AIR 5.0...
THAT SOC IS PURE MAYHEM!
YOU'RE CONSTANTLY WAITING ON APPROVALS!
DENIED
WATCH YOUR ALERTS AGE GRACEFULLY IN MY APPROVAL QUEUE!
YOU'RE SPINNING IN CIRCLES CHASING ARTIFACTS MANUALLY.
MANUAL LABOR BUILDS CHARACTER.
DON'T CRY...
YOU'RE WAITING IN AN ENDLESS QUEUE OF TIME SUCKING MONOTONY!
PATIENCE IS A VIRTUE...
AND I'M THE MASTER OF YOUR WAITING!
I CAN'T BREATHE!
HELPPPP



INVESTIGATE WITH AUTO ASSET TAGGING

REMOTE TRIAGE AT SCALE

AUTOMATED DECISION SUPPORT

1-CLICK TIMELINE COLLABORATION

AUTOMATED CYBER INVESTIGATIONS

INTERACTIVE REMOTE SHELL

INTEGRATED INSIGHTS, CONSOLIDATED

FORENSIC DIFFERENTIAL ANALYSIS

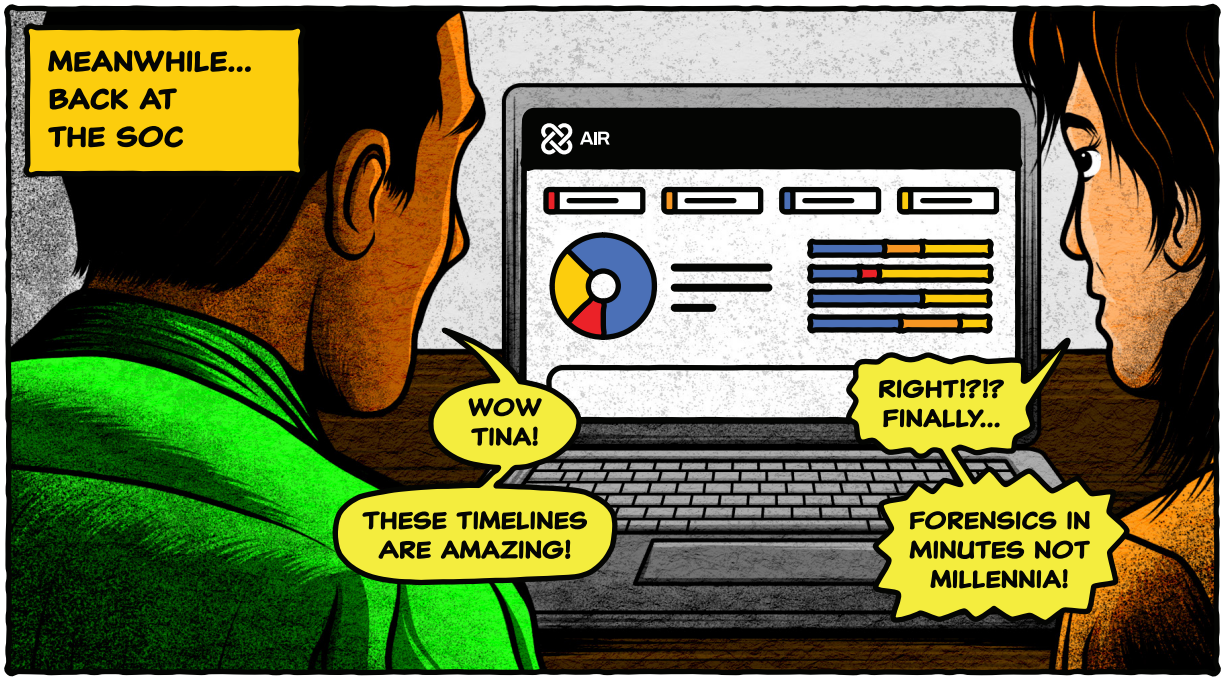
AIR COLLECTS 100+ ENDPOINTS REMOTELY... BAM!

ARTIFACTS + FINDINGS + TIMELINES... IN JUST MINUTES!

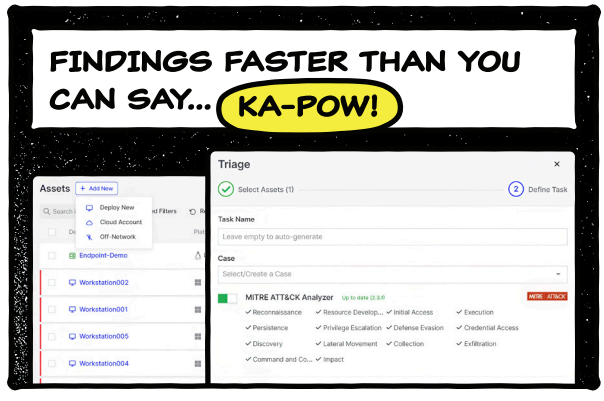
CLEAR, INSTANT REPORTS... YOU'RE WELCOME!

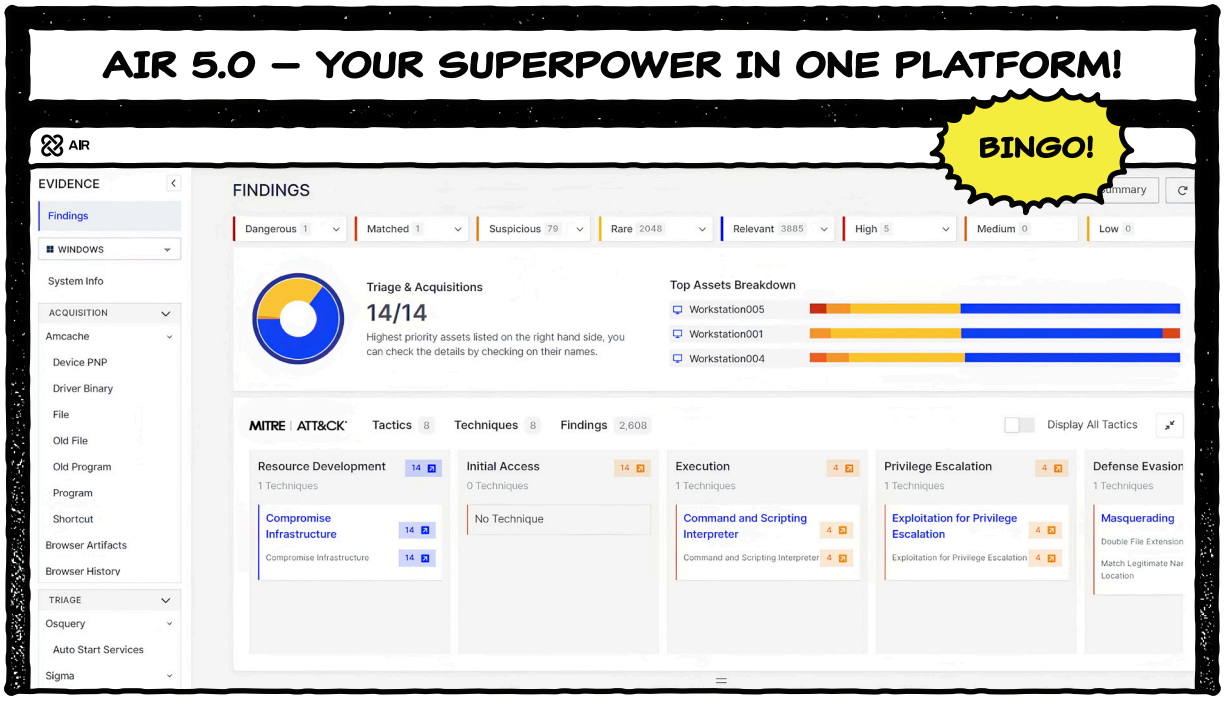

MY AIR SENSES ARE TINGLING
OH NO! FORENSICO'S TRACTOR BEAM IS SUCKING HER INTO THAT HOLE OF FORENSIC DATA. ALL TIME & HOPE ARE LOST!!!
I WAS SUPPOSED TO BE MEETING MY GIRLFRIENDS FOR HAPPY HOUR...WTF!
I DON'T GET PAID ENOUGH FOR THIS!
HAHAHA!
THESE ANALYSTS, DON'T HAVE A CHANCE
I'LL PULL EVERY ONE OF THEM INTO MY BLACKHOLE OF FORENSIC DATA.
THEY WON'T KNOW WHERE MY LIES END & THE TRUTH BEGINS

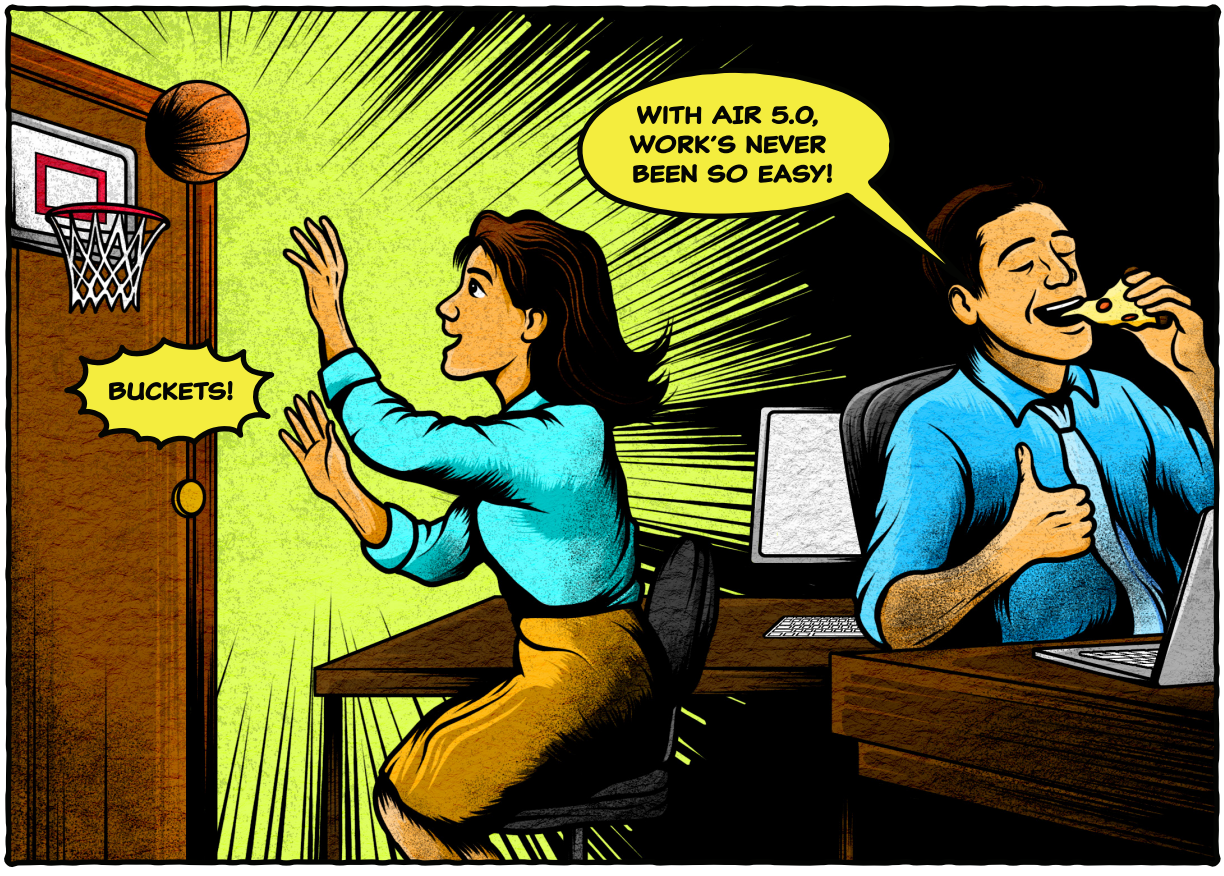

AIR IS NO ORDINARY HERO... HE SEES THROUGH THE CHAOS, CUTTING THROUGH ENDLESS NOISE & EXPOSING THE TRUTH HIDDEN IN THE DATA. WHERE OTHERS ARE LOST, AIR BRINGS CLARITY.
SMASH!
AIR! I KNEW YOU WOULD SAVE ME!
CRACK!
KA-POW!
KICKING A$$, & TAKING NAMES
HA!
PIECE OF CAKE!!
DID YOU SAY CAKE?
...I LOVE CAAAKKE!
THANKS AIR!


MEANWHILE... BACK AT THE SOC
AIR
WOW TINA!
THESE TIMELINES ARE AMAZING!
RIGHT!?!? FINALLY...
FORENSICS IN MINUTES NOT MILLENNIA!


LIGHTENING QUICK INVESTIGATIONS
WOW!
Asset Details
Workstation002
Computers
Off-Network
Unreachable
CPU: 0.00%
Memory: 58.43%
Disk: 27.58%
Offline
Acquire
Triage
interACT
Timeline
Compare
Reboot
Shutdown
Reload
Off-Network
Duration
Created At
Actions
Case 001 Triage 001
Baseline Acquisition
Acquisition Task-Ca
Completed
3 months ago


FINDINGS FASTER THAN YOU CAN SAY...
KA-POW!
Assets
Add New
Deploy New
Cloud Account
Off-Network
Endpoint-Demo
Workstation002
Workstation001
Workstation005
Workstation004
Triage
Select Assets (1)
Define Task
Task Name
Leave empty to auto-generate
Case
Select/Create a Case
MITRE ATT&CK Analyzer
Reconnaissance
Resource Develop...
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
Command and Co...
Impact


AIR 5.0 — YOUR SUPERPOWER IN ONE PLATFORM!
BINGO!
AIR
EVIDENCE
Findings
WINDOWS
System Info
ACQUISITION
Amcache
Device PNP
Driver Binary
File
Old File
Old Program
Program
Shortcut
Browser Artifacts
Browser History
TRIAGE
Osquery
Auto Start Services
Sigma
FINDINGS
Dangerous 1
Matched 1
Suspicious 79
Rare 2048
Relevant 3885
High 5
Medium 0
Low 0
Triage & Acquisitions
14/14
Highest priority assets listed on the right hand side, you can check the details by checking on their names.
Top Assets Breakdown
Workstation005
Workstation001
Workstation004
MITRE | ATT&CK
Tactics 8
Techniques 8
Findings 2,608
Display All Tactics
Resource Development
1 Techniques
Compromise Infrastructure
Initial Access
0 Techniques
No Technique
Execution
1 Techniques
Command and Scripting Interpreter
Privilege Escalation
1 Techniques
Exploitation for Privilege Escalation
Defense Evasion
1 Techniques
Masquerading
Double File Extension


WITH AIR 5.0, WORK'S NEVER BEEN SO EASY!
BUCKETS!

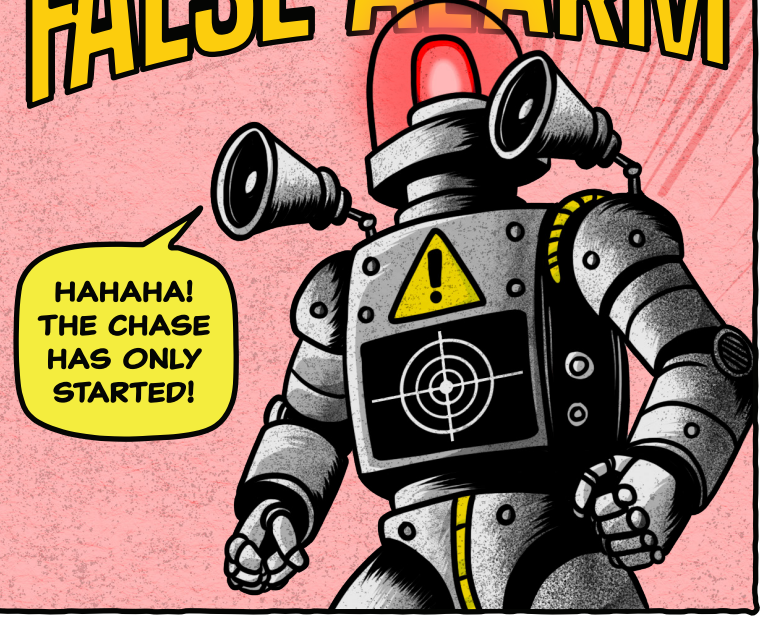

THANKS, AIR!
YOU'VE GOT SOME PIZZA SAUCE ON YOUR TIE THERE BUB!

NEXT TIME... TUNE IN FOR THE EDR / XDR TAKEDOWN!

FALSE ALARM

HE FLOODS YOUR SOC WITH ENDLESS FALSE POSITIVES, EMPTY WARNINGS, AND CONSTANT NOISE.

- FLOODS DASHBOARDS WITH MEANINGLESS ALERTS
- RINGS ALARMS FOR EVERY SHADOW
- SENDS YOU CHASING DEAD ENDS
- WASTES HOURS ON FALSE INVESTIGATIONS



TRY AIR 5.0 TODAY

SNAP THIS!

TRY NOW!

binalyze!

BINALYZE.COM/AIR