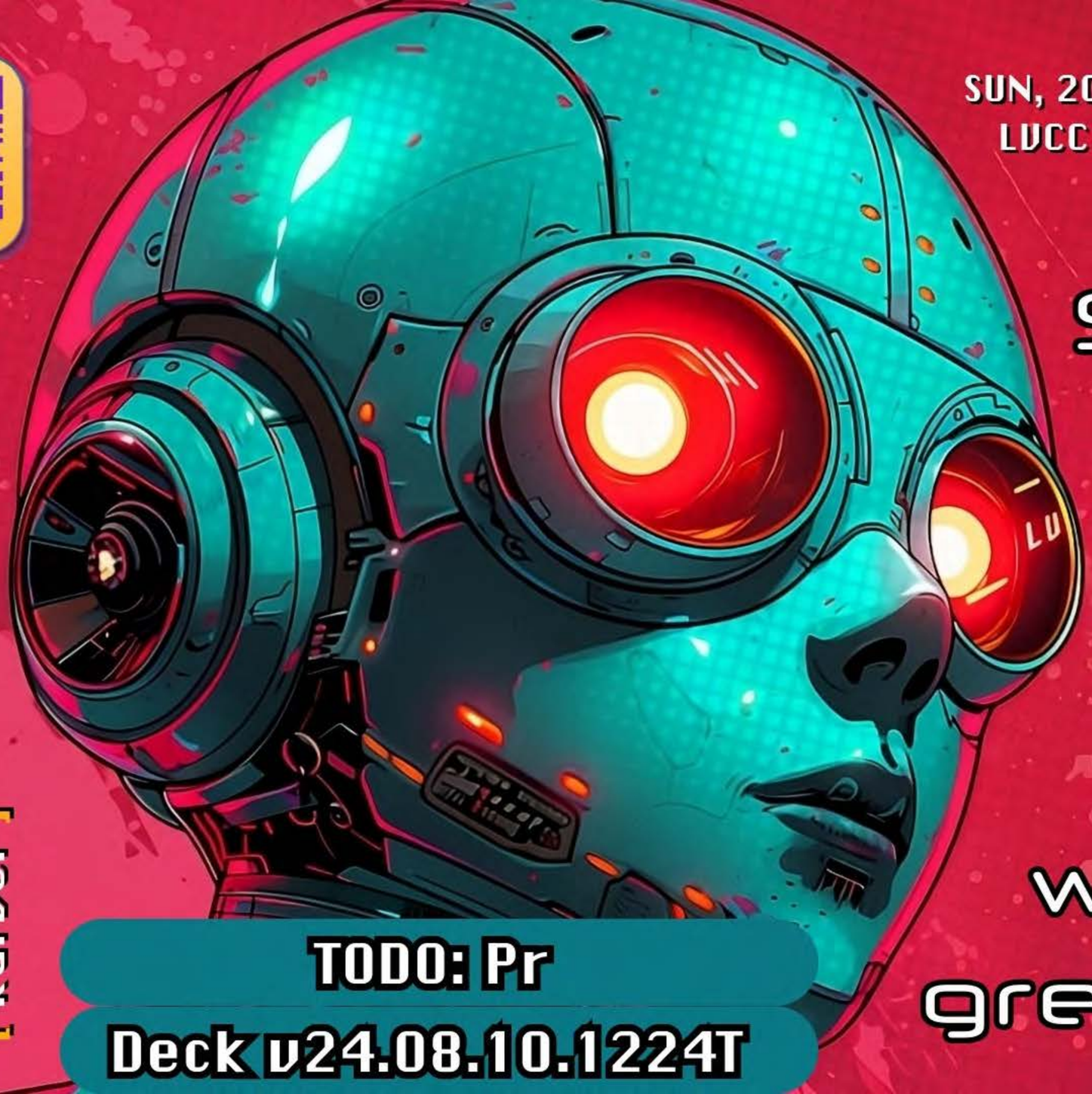
SUN, 2024-08-11 @ 1200T
LVCC - L3 - W322-W327
Warstories Track

DEFCON 32 ENGAGE

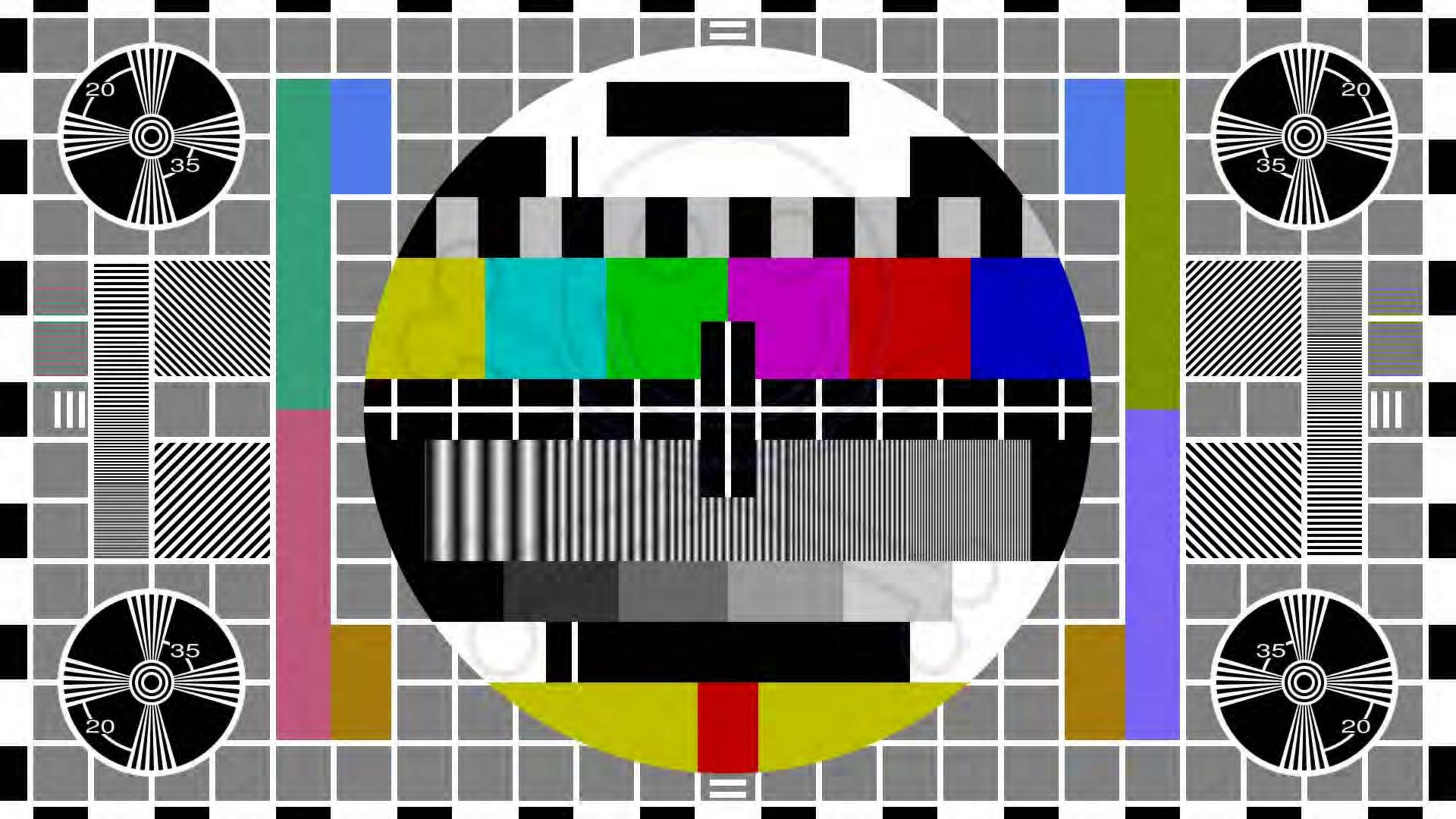
Solving the "Lover, Stalker, Killer" Murder with strings, grep, and Perl



https://forensic.coffee
Anthony Kava
[karver]

TODO: Pr

Deck v24.08.10.1224T


20
35
20
35
35
20
35
20

"This isn't Black Hat. We don't need to shoehorn in a quote from 600 B.C.E."
- Cyber Sun Tzu
Ted, don't forget to wind your watch!

THIS SLIDE HAS BEEN SEIZED.

The Federal Bureau of Investigation seized this slide as part of a coordinated law enforcement action taken against sub-par memes. To report bad memes visit: http://memepolice.lol

ZENTRALE KRIMINALINSPEKTION GÖTTINGEN

Federal Criminal Police Office

NCA National Crime Agency

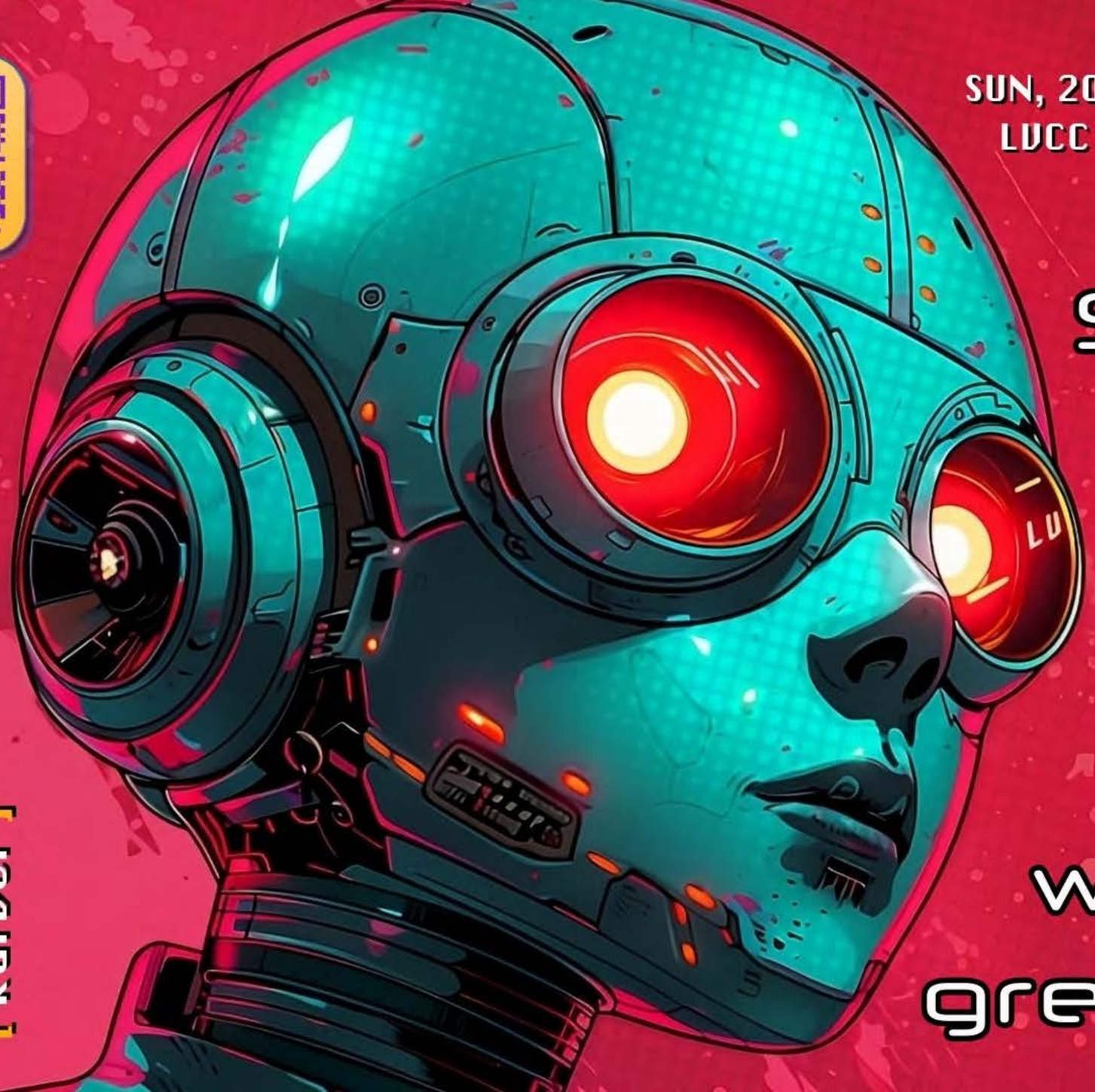
ROCU COUNTER TERRORISM POLICING

REWARDS FOR JUSTICE

SUN, 2024-08-11 @ 1200T
LVCC - L3 - W322-W327
Warstories Track

DEFCON 32 ENGAGE

Solving the "Lover, Stalker, Killer" Murder with strings, grep, and Perl



https://forensic.coffee
Anthony Kava
[karver]

The Goods Is In THE BOX
The Goods Is In THE BOX
diet PEPSI
2000 08 05

SanDisk
16GB
4
micro SD HC
2017/02/06 17:28

THE PLACES YOU'LL GO...

UNDER CARS

AWKWARD CUBICLES

I just kept yelling "ENHANCE!", and it kept working!
ENHANCE
ENHANCE
TO THE KEYBOARD!

WITH HELP FROM DMX?

DISCLAIMER

SOLVING THE "LOVER, STALKER, KILLER" MURDER WITH STRINGS, GREP, AND PERL

T/W: Violence

Spoiler Alert!!1

Personal Opinions

I Love My Job & Also Not Getting Sued

DISCLAIMER

SOLVING THE "LOVER, STALKER, KILLER" MURDER WITH STRINGS, GREP, AND PERL

T/W: Violence

Spoiler Alert!!1

Personal Opinions

I Love My Job &
Also Not Getting Sued

DISCLAIMER

SOLVING THE "LOVER, STALKER, KILLER" MURDER WITH STRINGS, GREP, AND PERL

T/W: Violence

Spoiler Alert!!1

Personal Opinions

I Love My Job &
Also Not Getting Sued

DISCLAIMER

SOLVING THE "LOVER, STALKER, KILLER" MURDER WITH STRINGS, GREP, AND PERL

T/W: Violence

Spoiler Alert!!1

Personal Opinions

I Love My Job &
Also Not Getting Sued

DISCLAIMER

SOLVING THE "LOVER, STALKER, KILLER" MURDER WITH STRINGS, GREP, AND PERL

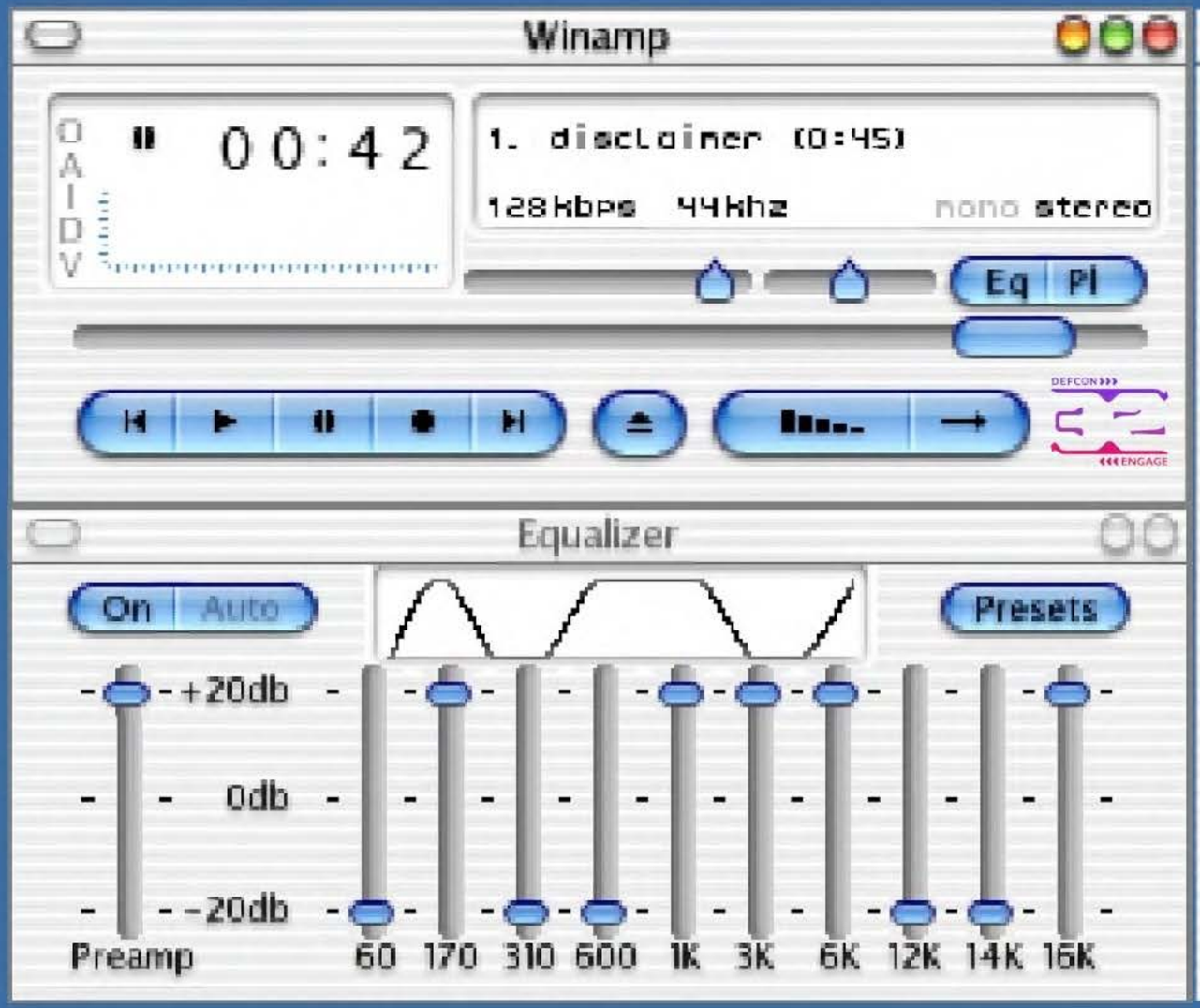
T/W: Violence

Spoiler Alert!!1

Personal Opinions

I Love My Job &
Also Not Getting Sued

AGENDA


Winamp
00:42
1. disclaimer (0:45)
128kbps 44khz
mono stereo
Eq
Pl
Equalizer
On
Auto
Presets
+20db
0db
-20db
Preamp
60 170 310 600 1K 3K 6K 12K 14K 16K

Playlist
1. Disclaimer 0:45
2. Basics of the Case 3:03
3. My Part 3:04
4. The Killer's MO 3:01
5. (Digital) Evidence 5:52
6. Trial and Verdict 1:55
7. Outcomes / Lessons 1:07
8. Questions + Apologies Afterwards 0:34
Add
Rem
Sel
Misc
0:45/19:21
00:26
List

cat

3000h of Work
5h Book Reading
("A Tangled Web" by Leslie Rule)

gz

2h Case Study
2h Dateline NBC

bzip2

90' Netflix Doc
("Lover, Stalker, Killer")

xz -9

20' DEF CON Talk
(You Are Here)

DFIR vs. LE DF
harder | better | faster | stronger | legaler

ENGAGE!

OPENNESS
truth | code | pass Aaron's Law already

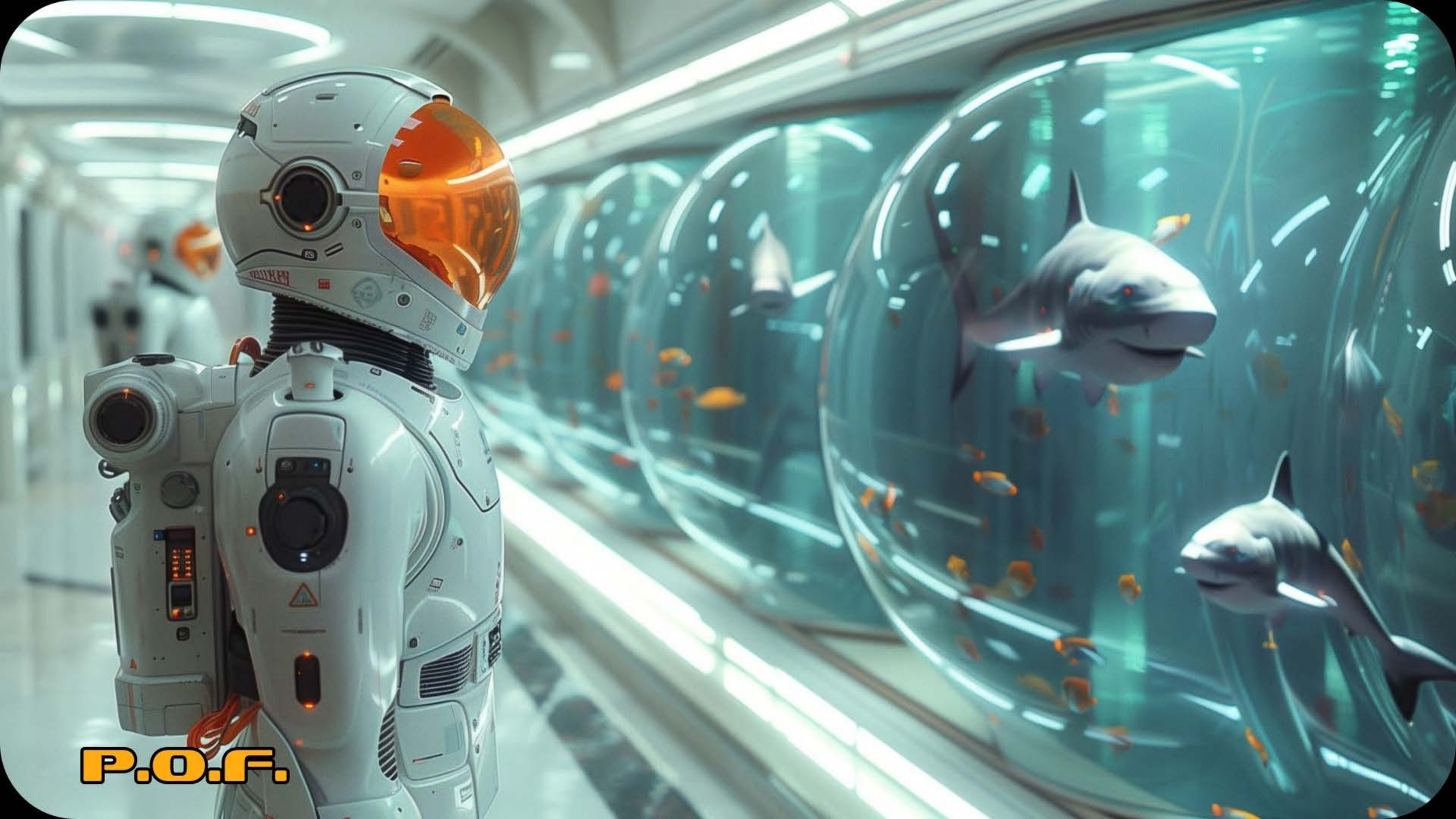
Victims should be our focus, and one attribute or diagnosis does *not* define a person.

CARI

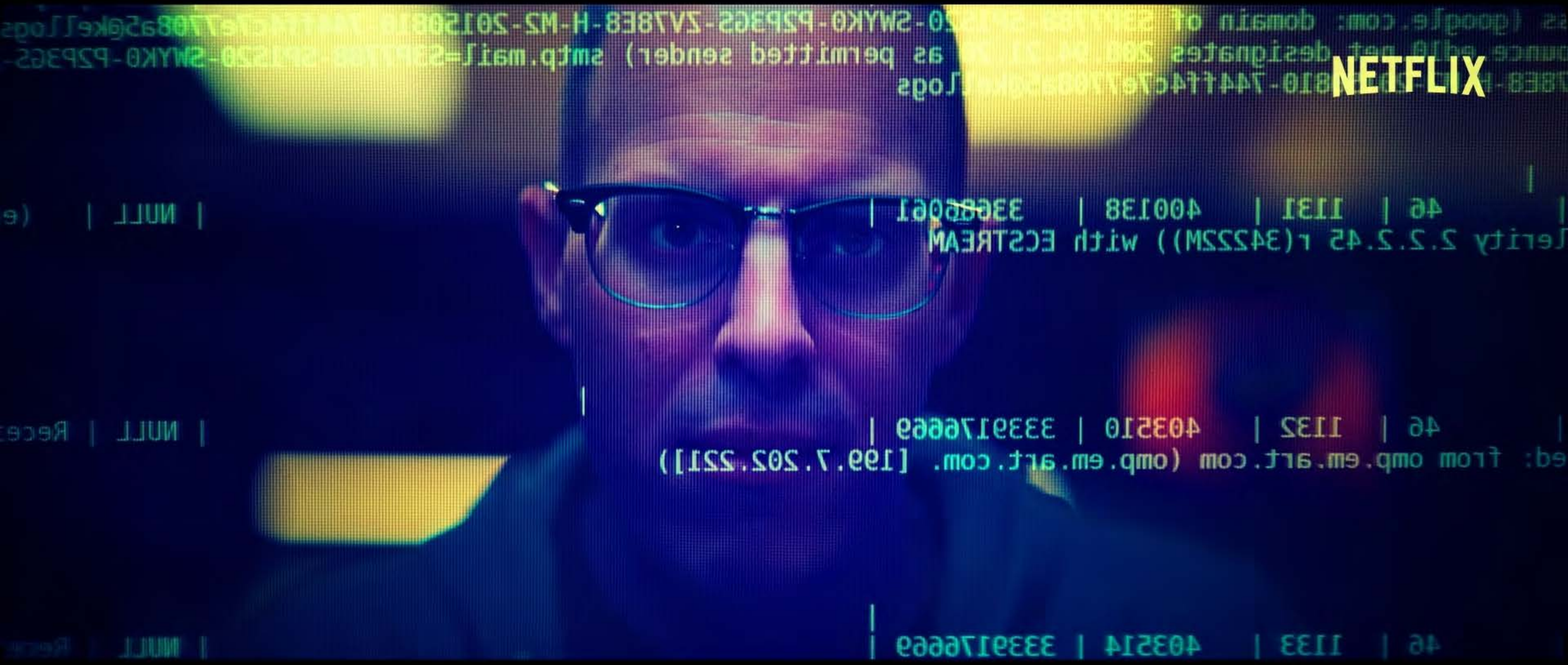
DAVE

DAVE + AMY

MODERN DATING


P.O.F.

“LILITH”



"Lover, Stalker, Killer" © 2024 Netflix / Curious Films UK "My Face" © 19xx My Parents / No Moisturizer Ever

Top 10 Movies in the U.S. Today

1

2

3

4

Top 10 TV Shows in the U.S. Today

1

2

3

4

© 2024 Netflix

DAVE'S PLACE

DEFCON
ENGAGE
COMPLETE
2012-11-13

FROM: CARI
LETS MOVE IN TOGETHER
DEFCON

FROM: CARI
I NEVER WANT TO SEE
YOU AGAIN
DEFCON

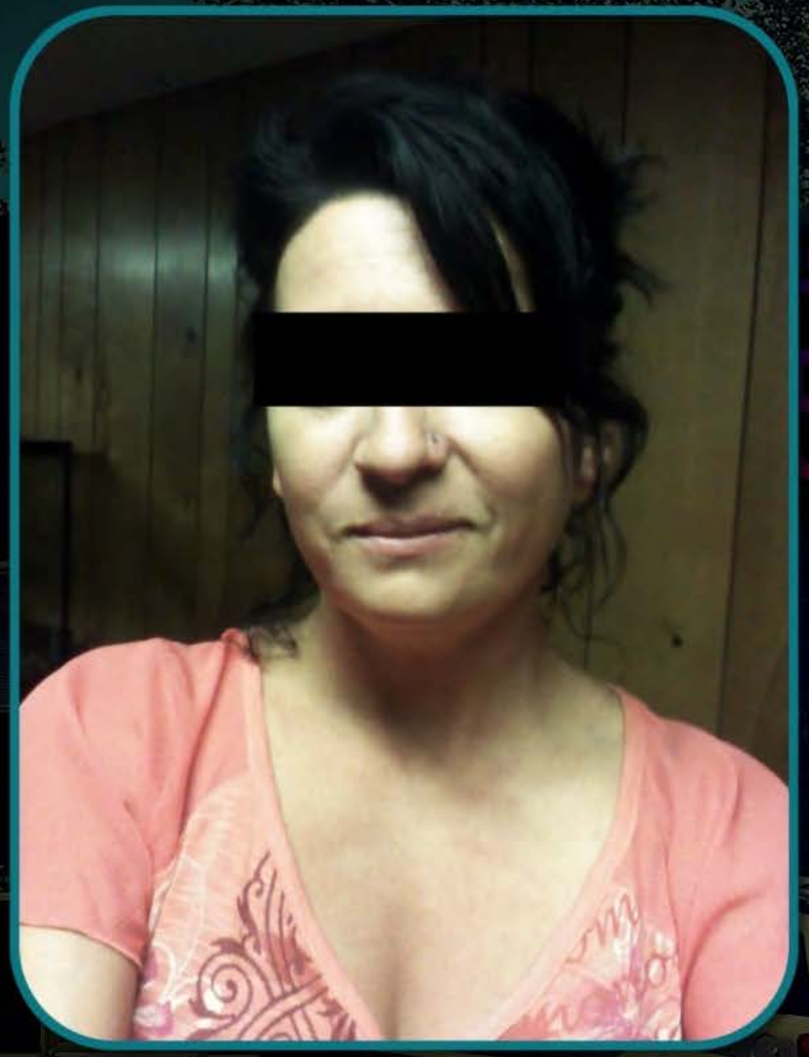
FROM: CARI
I AM SEEING SOMEONE
ELSE
DEFCON

FROM: CARI
I HATE YOU
DEFCON

```
**** DEF CON 32 BASIC VX ****
64T RAM SYSTEM  31337 BASIC BYTES FREE

YOU'RE ABOUT TO ┌ HACK TIME └ !

ARE YOU SURE??!?
YES
```

```
**** DEF CON 32 BASIC VX ****
64T RAM SYSTEM  31337 BASIC BYTES FREE

YOU'RE ABOUT TO ┌ HACK TIME └ !

ARE YOU SURE??!?
YES   NO
```

YES



FROM: CARI
I AM WATCHING YOU
DEFCON

FROM: CARI
I LEFT YOU SOMETHING
DEFCON

WHORE
From
DAVE

FROM: CARI
YOUR SMOKE ALARMS
ARE GOING OFF
DEFCON

08/17/2013 09:46

HUSKY
3
3
08/17/2013 12:17

Me

Cari Lea Kroupa

To: Dave Kroupa, [redacted]

12:56am, Aug 17, 2013

Nasty whore, Dave doesn't want you talking to him anymore. He wants to be with me we are trying a new relationship. We have had sex recently. He loves me and always will he doesn't want you back you nasty fat whore [redacted] Hope you and your kids burn to death.

UNITED STATES DISTRICT COURT

for the

Southern District of Example

United States of America
v.

"Cari"

Defendant

Case No. 13-012345

ARREST WARRANT

To: Any authorized law enforcement officer

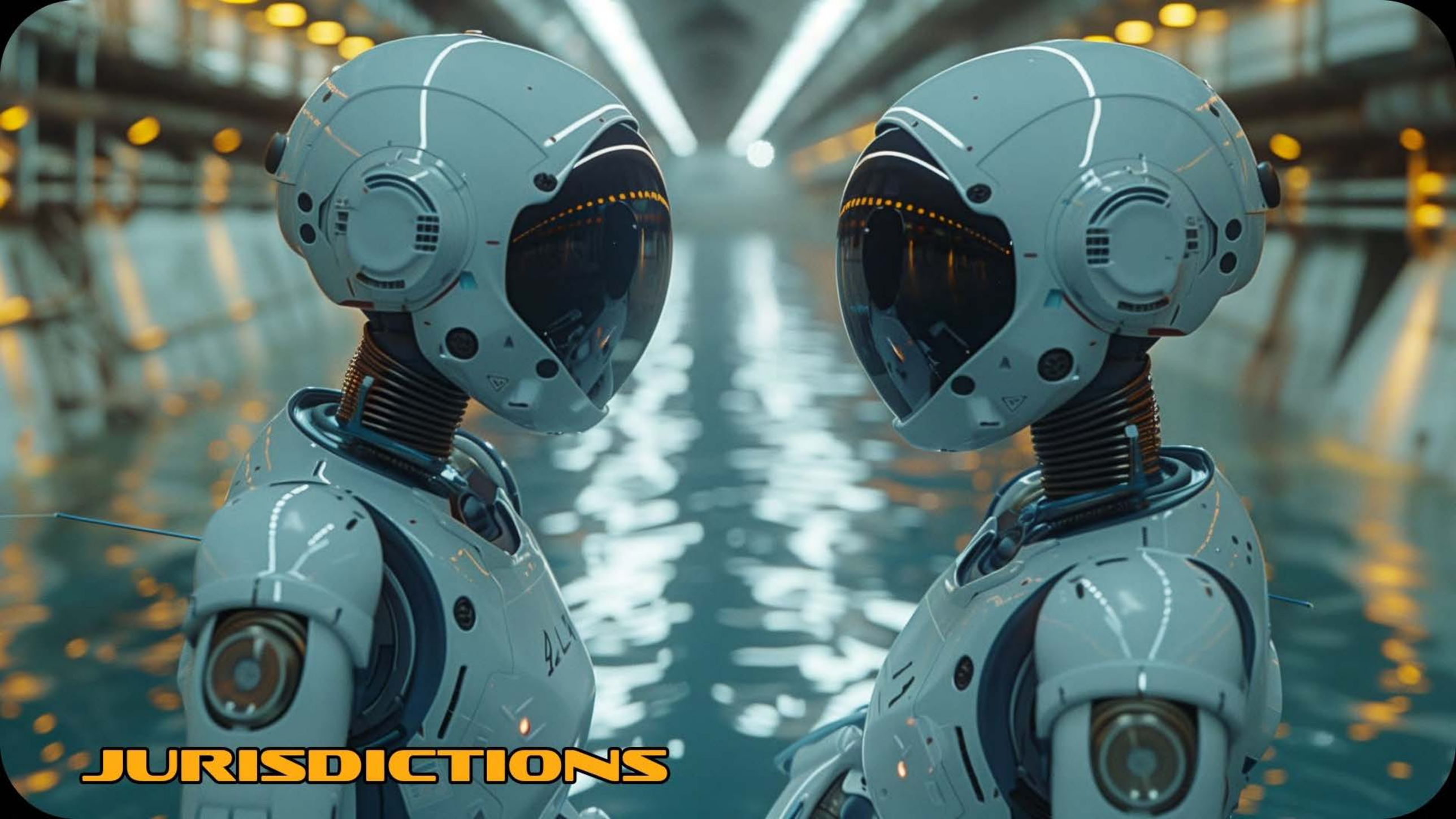
YOU ARE COMMANDED to arrest and bring before a United States magistrate judge without unnecessary delay

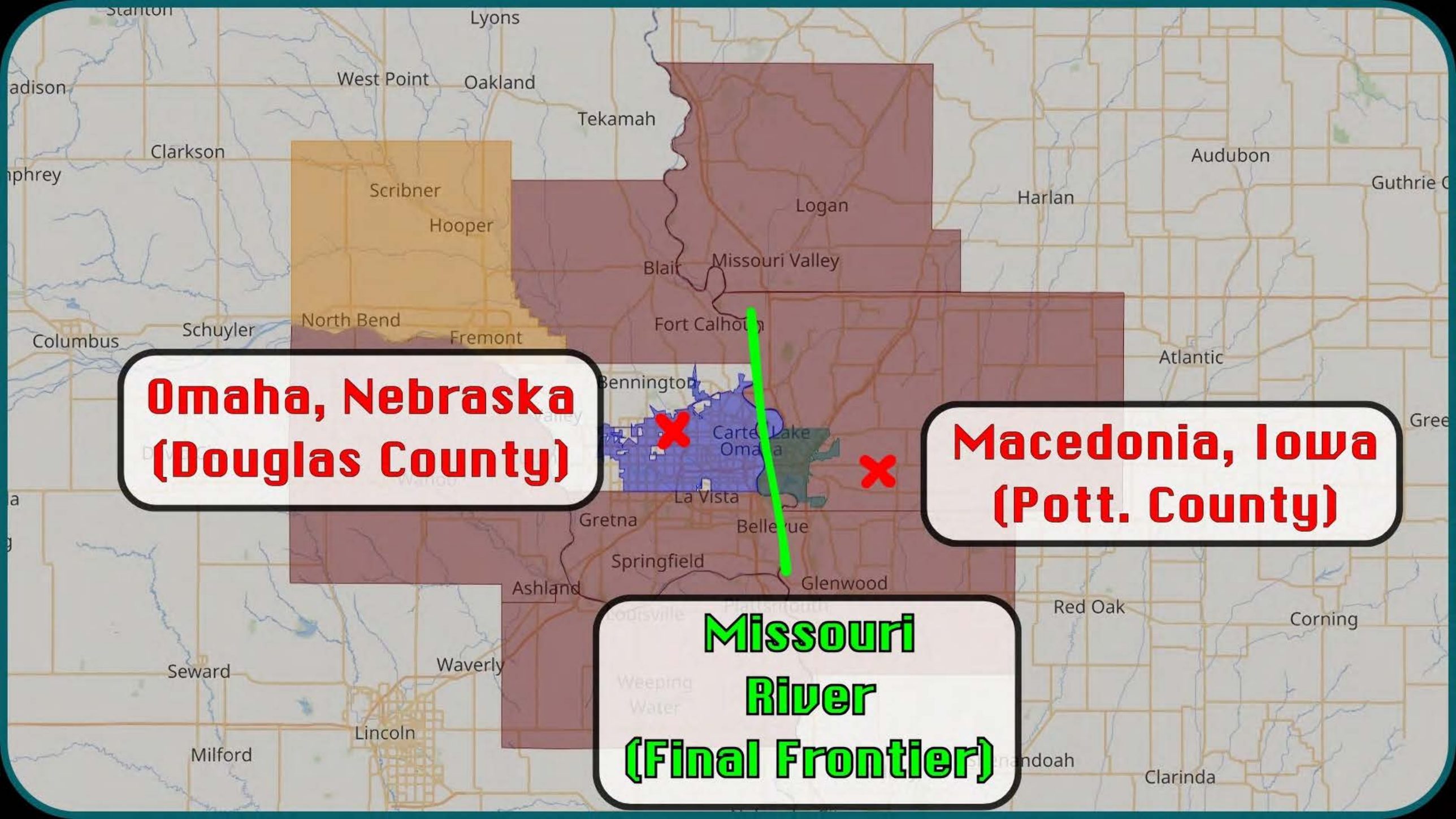
(name of person to be arrested) "Cari",

who is accused of an offense or violation based on the following document filed with the court:

❒ Indictment ❒ Superseding Indictment ❒ Information ❒ Superseding Information ☒ Complaint

❒ Probation Violation Petition ❒ Supervised Release Violation Petition ❒ Violation Notice ❒ Order of the Court


JURISDICTIONS


Omaha, Nebraska
(Douglas County)
Macedonia, Iowa
(Pott. County)
Missouri
River
(Final Frontier)
Lyons
West Point
Oakland
Tekamah
Clarkson
Scribner
Hooper
Logan
Harlan
Audubon
Blair
Missouri Valley
North Bend
Fremont
Schuyler
Columbus
Fort Calhoun
Atlantic
Bennington
Carter Lake
La Vista
Gretna
Springfield
Ashland
Glenwood
Red Oak
Corning
Seward
Waverly
Lincoln
Milford
Clarinda

THE CASE GOES COLD

James T. Doty

Investigator

Ryan Avis

Corporal-Investigator

Anthony Kava

Special Deputy (Nerd)

REVISITED: 2015-04

whoami(4)

Anthony Kava [karver]

https://forensic.coffee

onlyspams[at]forensic.coffee

DEFCON
DEFCON

CURRICULUM VITAE

2001-2003:

[REDACTED] Telco / ISP

ride the layoffs

Qwe[redacted]

2003-2017:

County .GOV IT Drone (Assorted)

2009-2036?

DF, Cyber Investigations, ICAC TF

2017-2036?

Sheriff's Resident Geek

"For career day this kid dressed-up as a 15-year detective with two divorces and a drinking problem."

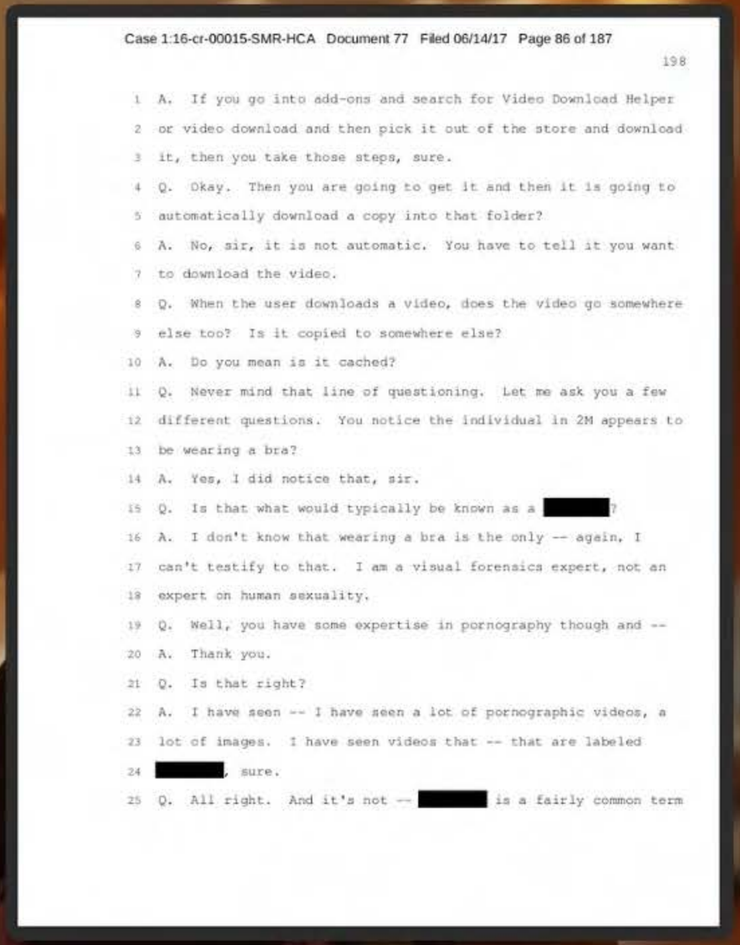
CURRICULUM VITAE (CONT'D)

CURRICULUM VITAE (CONT'D)

CURRICULUM VITAE (CONT'D)

Me, an nOrp eXpErT:

Thank you!



Case 1:16-cr-00015-SMR-HCA Document 77 Filed 06/14/17 Page 86 of 187

198

A. If you go into add-ons and search for Video Download Helper or video download and then pick it out of the store and download it, then you take those steps, sure.

Q. Okay. Then you are going to get it and then it is going to automatically download a copy into that folder?

A. No, sir, it is not automatic. You have to tell it you want to download the video.

Q. When the user downloads a video, does the video go somewhere else too? Is it copied to somewhere else?

A. Do you mean is it cached?

Q. Never mind that line of questioning. Let me ask you a few different questions. You notice the individual in 2M appears to be wearing a bra?

A. Yes, I did notice that, sir.

Q. Is that what would typically be known as a [redacted]?

A. I don't know that wearing a bra is the only -- again, I can't testify to that. I am a visual forensics expert, not an expert on human sexuality.

Q. Well, you have some expertise in pornography though and --

A. Thank you.

Q. Is that right?

A. I have seen -- I have seen a lot of pornographic videos, a lot of images. I have seen videos that -- that are labeled [redacted], sure.

Q. All right. And it's not -- [redacted] is a fairly common term

SKYTALKS
<App
Sec>
Village
DEF CON
402

SKYTALKS
<App Sec>
Village
DEF CON
402

LKSAT
SKYTA
TALKS
ATSKY
<App
Sec>
Village
DEF CON
402

SUCCULENT
SUCCULENT
DEFCON
ENGAGE
BACK TO THE CASE FILE

Subject	From	Date
See what men think of you	Cari Kroupa	2014-01-31 00:47
Is it working	Cari Kroupa	2014-02-01 19:01
Everyone believes me	Cari Kroupa	2014-02-02 15:14
Look I'm getting her off	Cari Kroupa	2014-02-02 20:12
This is the guy	Cari Kroupa	2014-02-24 19:50
Problem with your site	Cari Kroupa	2014-02-25 06:52
Re:	[redacted]@gmail.com	2014-11-04 21:18
Re:	[redacted]@gmail.com	2014-11-04 21:58
Proof	[redacted]@gmail.com	2014-11-14 14:41
More proof	[redacted]@gmail.com	2014-11-14 14:59
Re: facebook	[redacted]@gmail.com	2014-11-15 18:00
Re:	[redacted]@gmail.com	2014-11-16 16:56
See	[redacted]@gmail.com	2014-11-26 10:48
See he is on still	[redacted]@gmail.com	2014-12-14 00:39
So you don't think I got it from your kids mom	[redacted]@gmail.com	2014-12-24 14:32
See I now know Dave	[redacted]@gmail.com	2014-12-25 10:22
See my present	[redacted]@gmail.com	2014-12-25 10:53

From [redacted]@gmail.com

Subject See he is on still

To Dave My Hubby Kroupa <[redacted]@gmail.com>, [redacted]@gmail.com

Reply Forward Junk

12,000+ Fake Emails

1 attachment: image.png 320 KB

contains calendaring functionality by integrating the Lightning extension.

Learn more Disable

Unread: 2095 Total: 2095

>> TL;DR / SPOILERS AHEAD >>

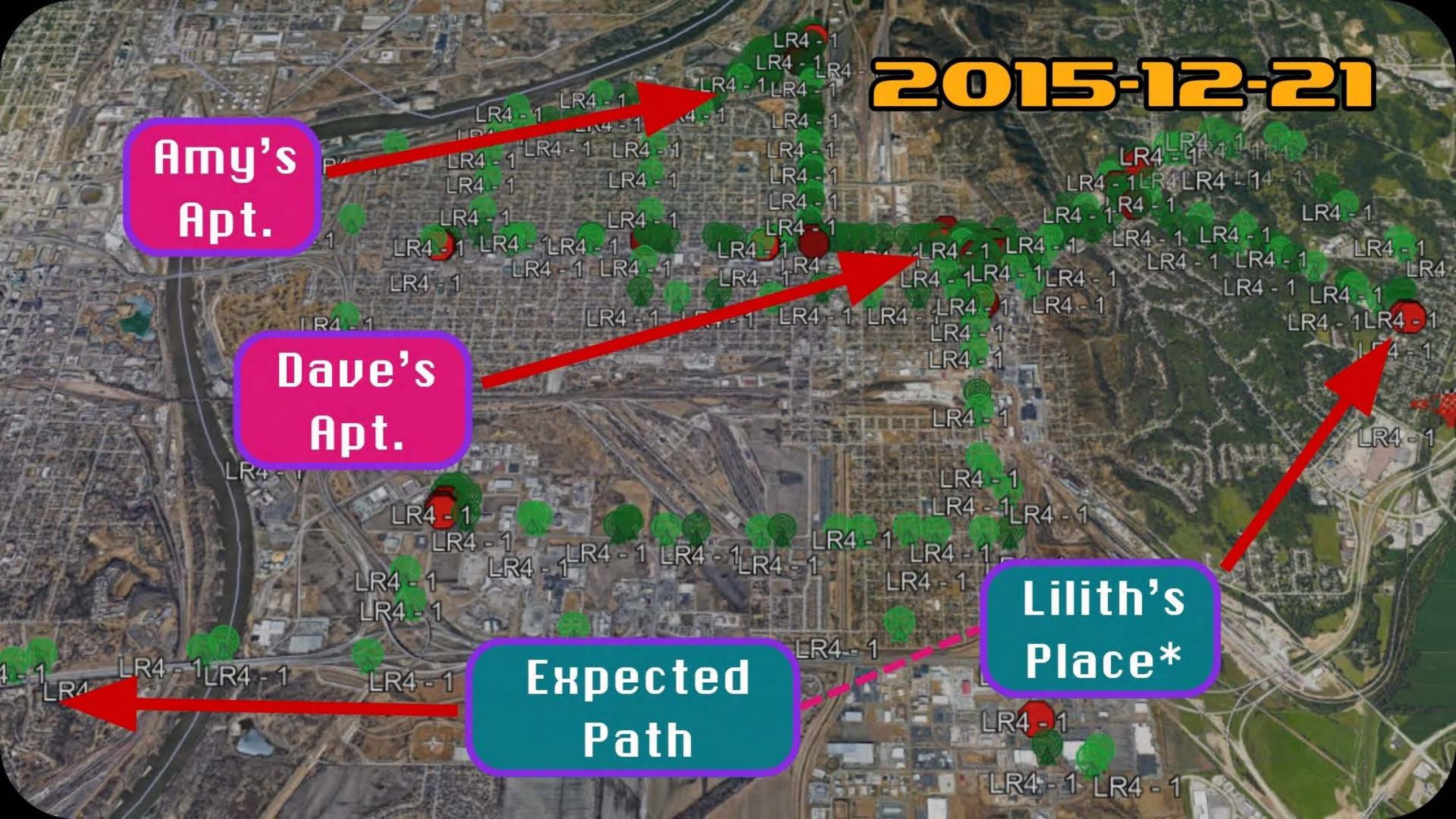
SPOILER:

SPOILER: IT'S "LILITH"

2015-12-05

DAVE + AMY

UNDER CARS


2015-12-21
Amy's Apt.
Dave's Apt.
Lilith's Place*
Expected Path

Makes sense. Actually, you know, I'm gonna be, I'm gonna be honest with you here.
[**Narrator:** *He wasn't.*]

From: “Amy”

To: Lilith

Date: 2015-12-17

I shot you [Lilith] to make sue Dave stayed away from you.

From: “Amy”

To: Lilith

Date: 2015-12-20

Just like your house getting burned was me.

From: “Amy”

To: Lilith

Date: 2015-12-20

I attaked her with a knofe I stabbed her...

IN THE DISTRICT COURT OF IOWA
IN AND FOR POTTAWATTAMIE COUNTY AT COUNCIL BLUFFS

IN THE MATTER OF A CRIMINAL INVESTIGATION	CASE NO. SWMG 1553398
	APPLICATION FOR SEARCH WARRANT

BEING DULY SWORN, I, Investigator Ryan Avis, of the Pottawattamie County Sheriff's Office, the undersigned, say that at the place described as follows:

2016 MAR -7 PM 1:14
CLERK DISTRICT COURT
POTTAWATTAMIE COUNTY
IOWA
FILED

[redacted]

In Pottawattamie County, Iowa, there is now certain property, namely:

-Electronic devices including, but not limited to; Computers, Tablets, Cell Phones, mass media storage devices, USB thumb drives, digital camera(s), wireless router(s), cellular internet USB hotspot device(s), vehicular GPS devices, digital memory cards, and other electronic devices with the capability to, but not limited to, sending and/or receiving text, picture, video messages, emails, phone calls, message(s) within a downloaded application, capturing photos and/or videos, store electronic information, has internet access, has access to cellular service (including active subscription or past/deactivated service), location history, GPS history, IP address history

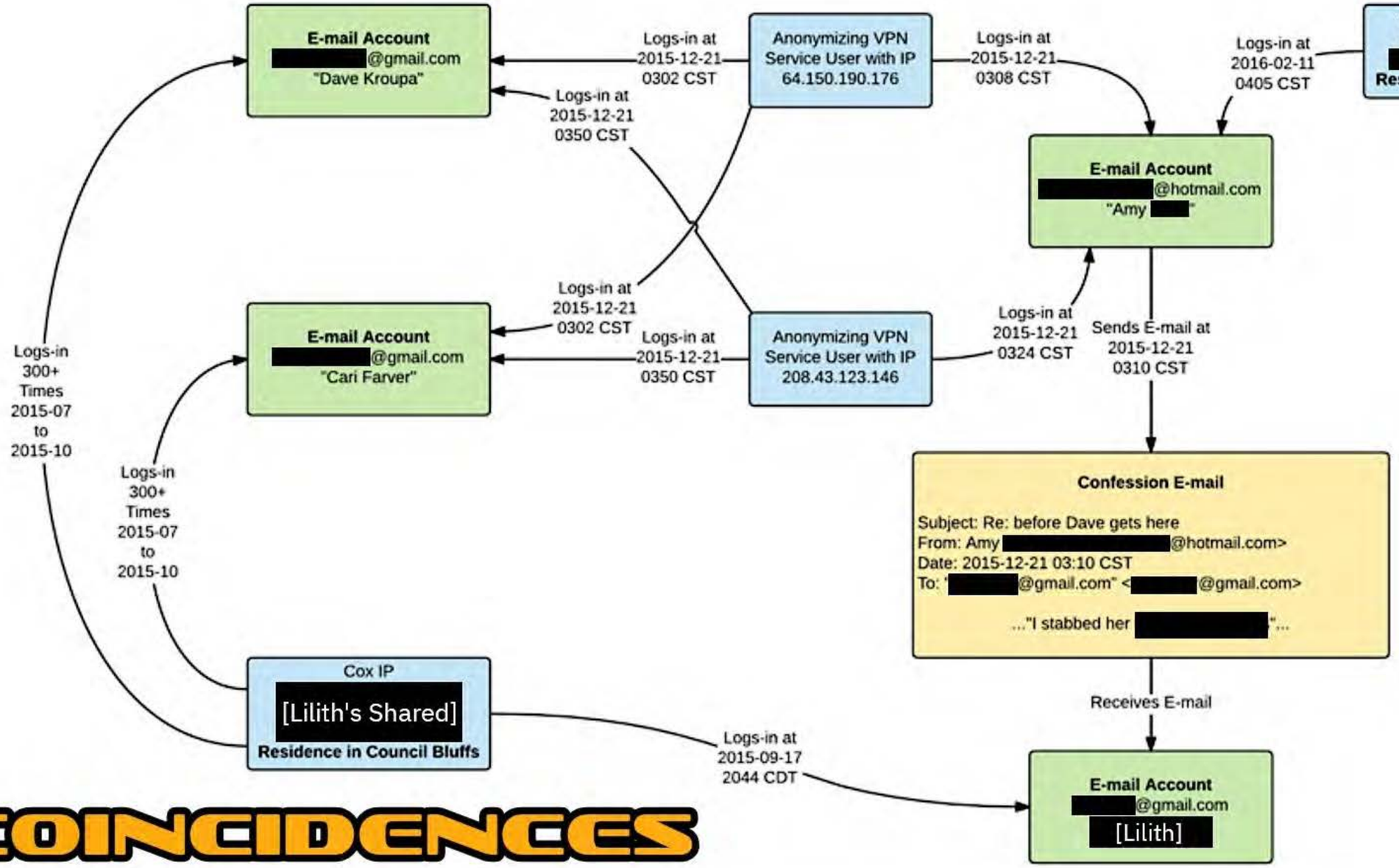
AWKWARD CUBICLES

MAIN ST
MUDGE ST
NO PARKING THIS SIDE OF STREET
WEIGHT LIMIT 5 TONS
SHERIFF
911

SONY
30x
Extended Zoom
Exmor R
8GB
SteadyShot
HANDYCAM
5.3 MEGA PIXELS
STILL IMAGE RECORDING
HDR-CX210
HD
AVCHD

OMAHA MEETINGS

S12-021291: Confession E-mail 2015-12-21 0310 CST



COINCIDENCES

DIGITAL OVERLOAD!

Amazon
AnchorFree VPN
Apple
Banks
CenturyLink
Cox Communications
eBay
Employers
Etsy
Facebook
Google
Hotspot Shield VPN
LetterMeLater.com
MeetMe
Microsoft
OkCupid
PayPal
Pinger
Pinterest
Schools
Sprint
SurfEasy VPN
Tattoo Parlor
Twitter
Valve
Verizon
Windstream
Yahoo

WARRANTS & SUBPOENAS

80+ GB

LEGAL RESPONSES (TEXTUAL)

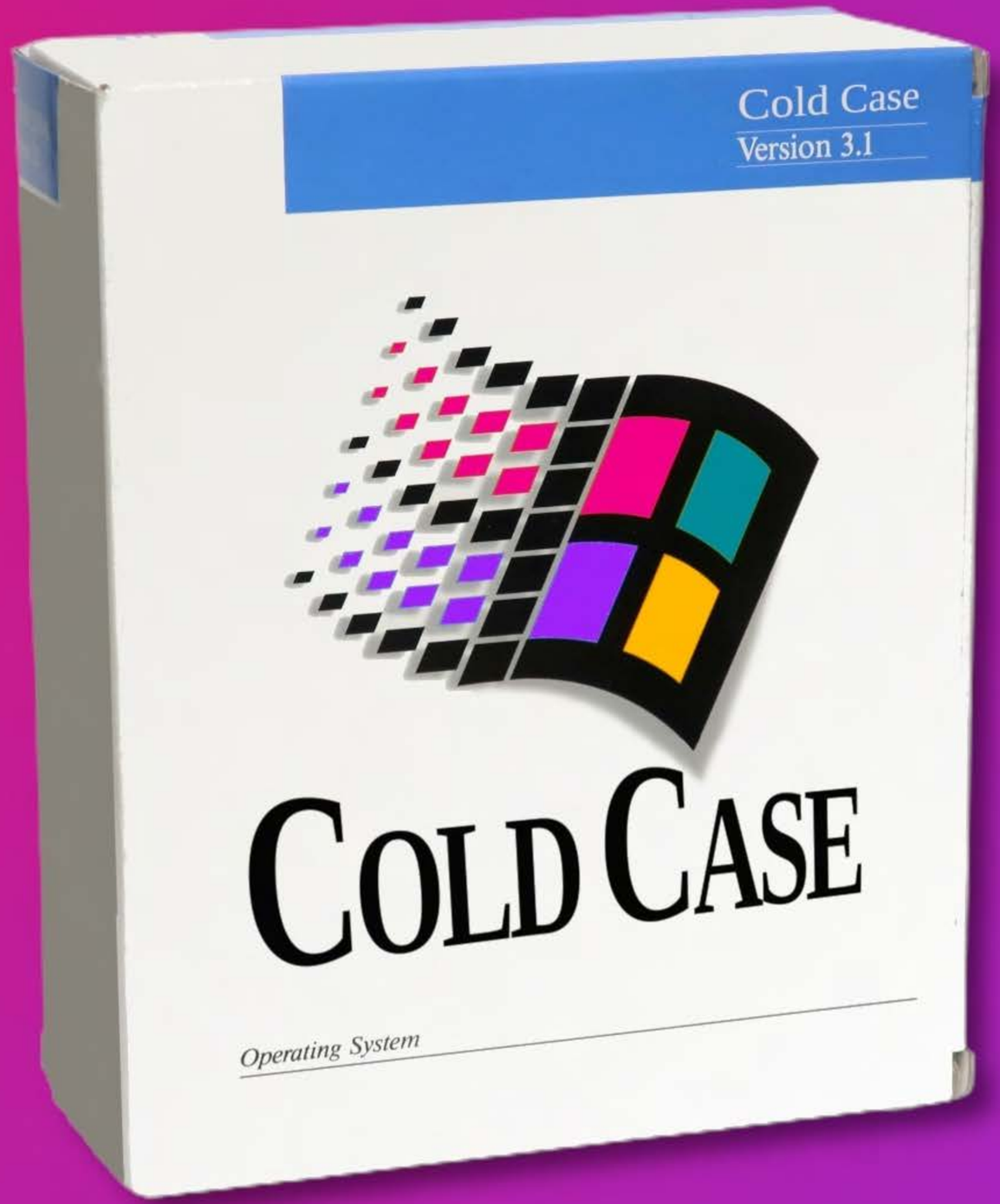
TEBABYTES OF PHYSICAL MEDIA

100,000+

EMAILS, IMs, & TEXTS

500,000+

IP ADDRESS RECORDS


Cold Case
Version 3.1
COLD CASE
Operating System

WHEN THE GOING GETS TOUGH...

DEX
"Perl is just hate mail to your future self."
- u/Zoltaroth

JAVA

PERL

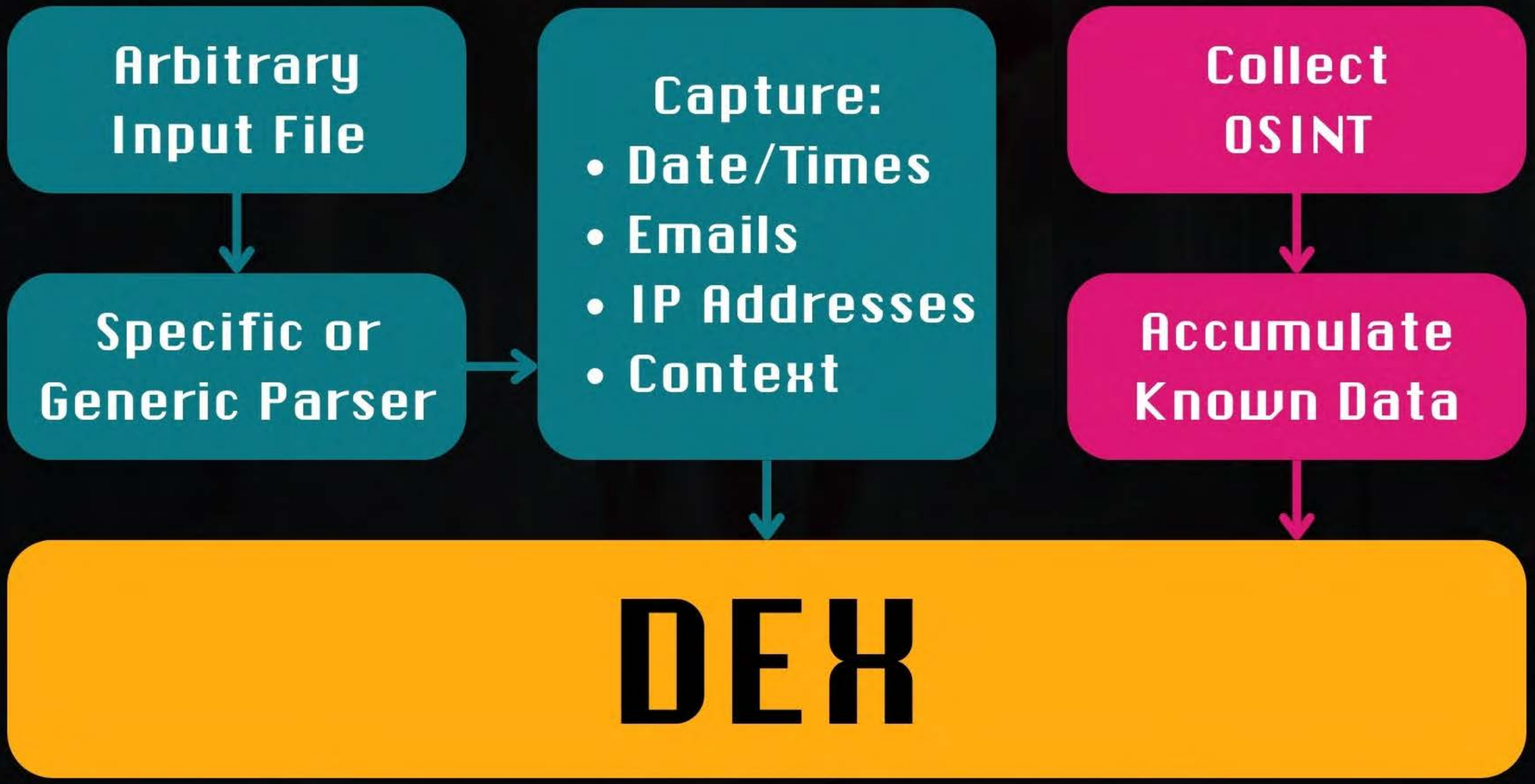
JAVA

```java
import java.util.regex.Pattern;
import java.util.regex.Matcher;
#include <crosstheiostream.h>


Pattern p = Pattern.compile("a(\d+)");
Matcher m = p.matcher("abc123");
Boolean didItEvenWork = m.matches();
cout << m.group() << endl << nullchar;

/*
have to compile? what is JIT even for?
60 years still no real world use for OOP
they have played us for absolute fools!
 */
```

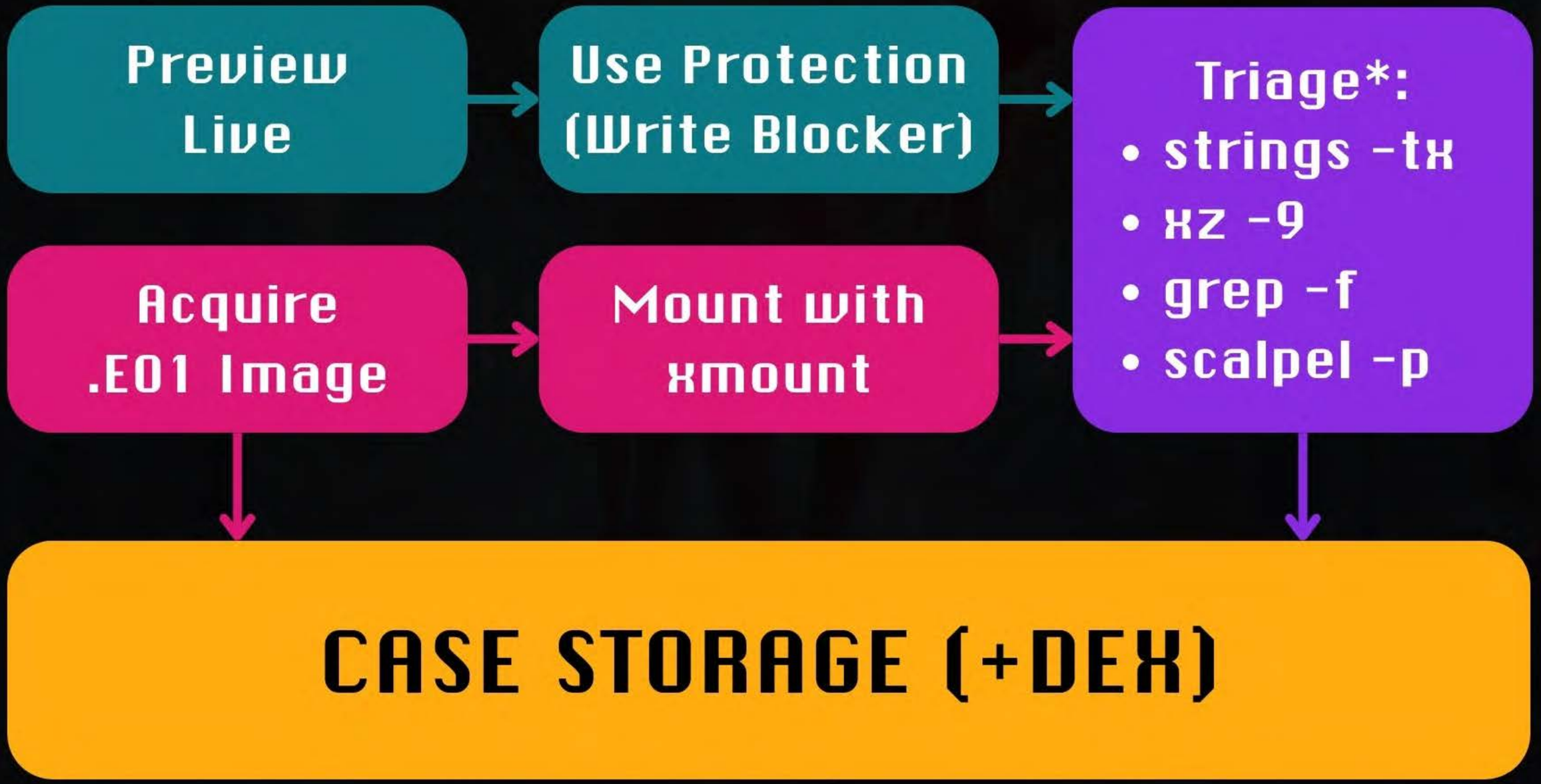
PERL

```perl
# no includes, thanks, this is my job

$_='abc123';          # we are nameless
print $1."\n" if /abc(\d+)/;

# "iNsTaNtiAtInG rEgEx oBjEcT"
# yo, dawg, I heard you like objects...
#
# wait, you're still going?


# wanna use float as a string? whatever
# everyone else has PCRE for a reason!
# quick tweak? just run it again, lol
```

```
$ sort -u < ips.txt # ???
```


Arbitrary Input File
Specific or Generic Parser
Capture:
• Date/Times
• Emails
• IP Addresses
• Context
Collect OSINT
Accumulate Known Data
DEX

MEDIA OVERLOAD


Preview
Live
Use Protection
(Write Blocker)
Triage*:
• strings -tx
• xz -9
• grep -f
• scalpel -p
Acquire
.E01 Image
Mount with
xmount
CASE STORAGE (+DEX)

```
MariaDB [dex]> SELECT ip_dotted, remarks, count(0) as hits FROM
vw_iphit_with_knownip GROUP BY ip ORDER BY count(0) DESC LIMIT 10;
+-------------+-----------------------------------------------+------+
| ip_dotted   | remarks                                       | hits |
+-------------+-----------------------------------------------+------+
| 174.71.x.x  | TB PottCounty VPN 2013-03-14 - 2015-06-08     | 2345 |
| 174.71.x.y  | TB PottCounty VPN 2015-06-12 - 2015-09-27     |  826 |
| 209.191.x.x | SurfEasy host=us.ipsec.surfeasy.mobi 2016-04-23 |  551 |
| 198.23.x.x  | SurfEasy host=us.ipsec.surfeasy.mobi 2016-04-23 |  512 |
| 108.168.x.x | SurfEasy netblock 108.168.x.x/28              |  508 |
| 23.110.x.x  | SurfEasy netblock 23.110.x.x/28               |  505 |
| 209.191.x.x | SurfEasy host=us.ipsec.surfeasy.mobi 2015-06-27 |  503 |
| 69.88.x.x   | SurfEasy host=us.ipsec.surfeasy.mobi 2015-06-27 |  498 |
| 198.23.x.x  | SurfEasy host=us.ipsec.surfeasy.mobi 2015-06-27 |  495 |
| 23.110.x.x  | SurfEasy host=ipsec.surfeasy.mobi 2015-06-27  |  492 |
+-------------+-----------------------------------------------+------+
```

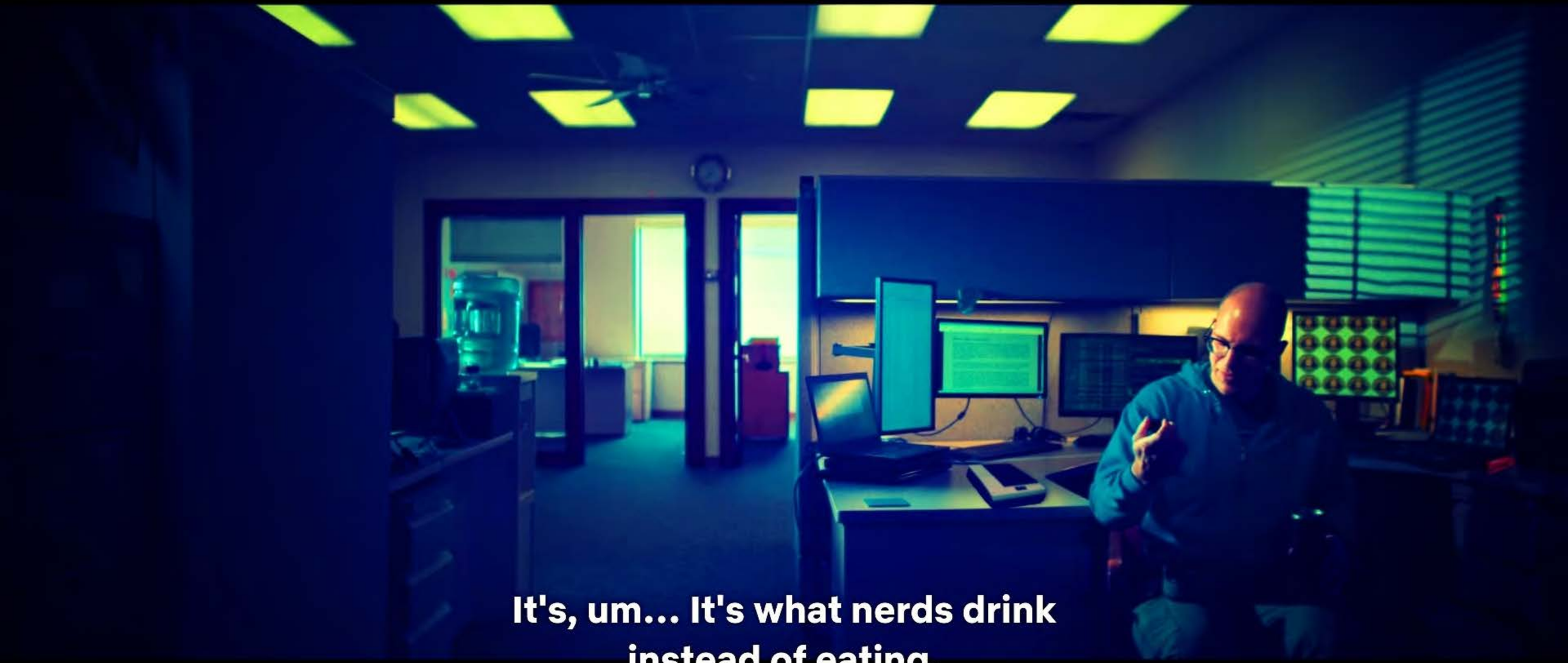
r/masterhacker

Lover stalker killer documentary - IT guy master hacker

IT guy says he traced an IP address to someone's house after writing a program that he asked questions like chatgpt.

Then shows the program that it's just doing sql queries.

While in front of a bunch of screens with green text flying around



"Lover, Stalker, Killer" © 2024 Netflix / Curious Films UK

Expensive Commercial Tools ($$$)

- Crash Like the Two-way Pager Market
- Don't Do Save Points (Zelda >= S/W)
- Liked 'em, Couldn't Trust 'em

DEX

- Let's You Reinvent Wheel (in Perl!)
- Resilient, Fast / Minimalist, Cheap!
- "I'm not a smart man, but I know what grep(1) is." [and what it will do]

:(

Your liver ran into a problem and needs to restart. We're just collecting some Incognito browser history, and then we'll restart for you.

42% complete

For more information about this issue and possible fixes, visit http://memepolice.lol/stopcode

If you call a support animal, give them this info:
Stop code: LAND_TRACTS_TOO_LARGE

I'M TOO POOR TO STORE?

https://github.com/anthonykava/zero.scalpel.fuse

anthonykava / zero.scalpel.fuse Public

Notifications | Fork 0 | Star 0

Code | Issues | Pull requests | Actions | Projects | Security | Insights

master | 1 Branch | 0 Tags | Go to file | Code

anthonykava Added close() for image file (may be moot) d3232ac · 6 years ago 13 Commits

LICENSE	Initial commit	6 years ago
README.md	Minor fix to example	6 years ago
zero.scalpel.fuse.pl	Added close() for image file (may be moot)	6 years ago

README | MIT license

zero.scalpel.fuse.pl

FUSE driver in Perl for reading scalpel's audit.txt file and showing a file system that maps files it would have carved to a disk image -- this allows for zero-storage carving as you can browse and view files with only a 'scalpel -p' (preview, scalpel writes no files) -- tested under Ubuntu Linux 18.04

Useful for me anyway, maybe not for you, but if so then enjoy.

About

Perl FUSE driver for zero-storage file carving using scalpel -p

linux | fuse | perl | forensics | digital-forensics | scalpel | forensic-analysis | carving

https://github.com/anthonykava/zero.scalpel.fuse

anthonykava / zero.scalpel.fuse Public

Notifications | Fork 0 | Star 0

Code | Issues | Pull requests | Actions | Projects | Security | Insights

master | 1 Branch | 0 Tags | Go to file | Code

anthonykava Added close() for image file (may be moot) d3232ac · 6 years ago 13 Commits

LICENSE	Initial commit	6 years ago
README.md	Minor fix to example	6 years ago
zero.scalpel.fuse.pl	Added close() for image file (may be moot)	6 years ago

About

Perl FUSE driver for zero-storage file carving using scalpel -p

linux fuse perl forensics digital-forensics scalpel forensic-analysis carving

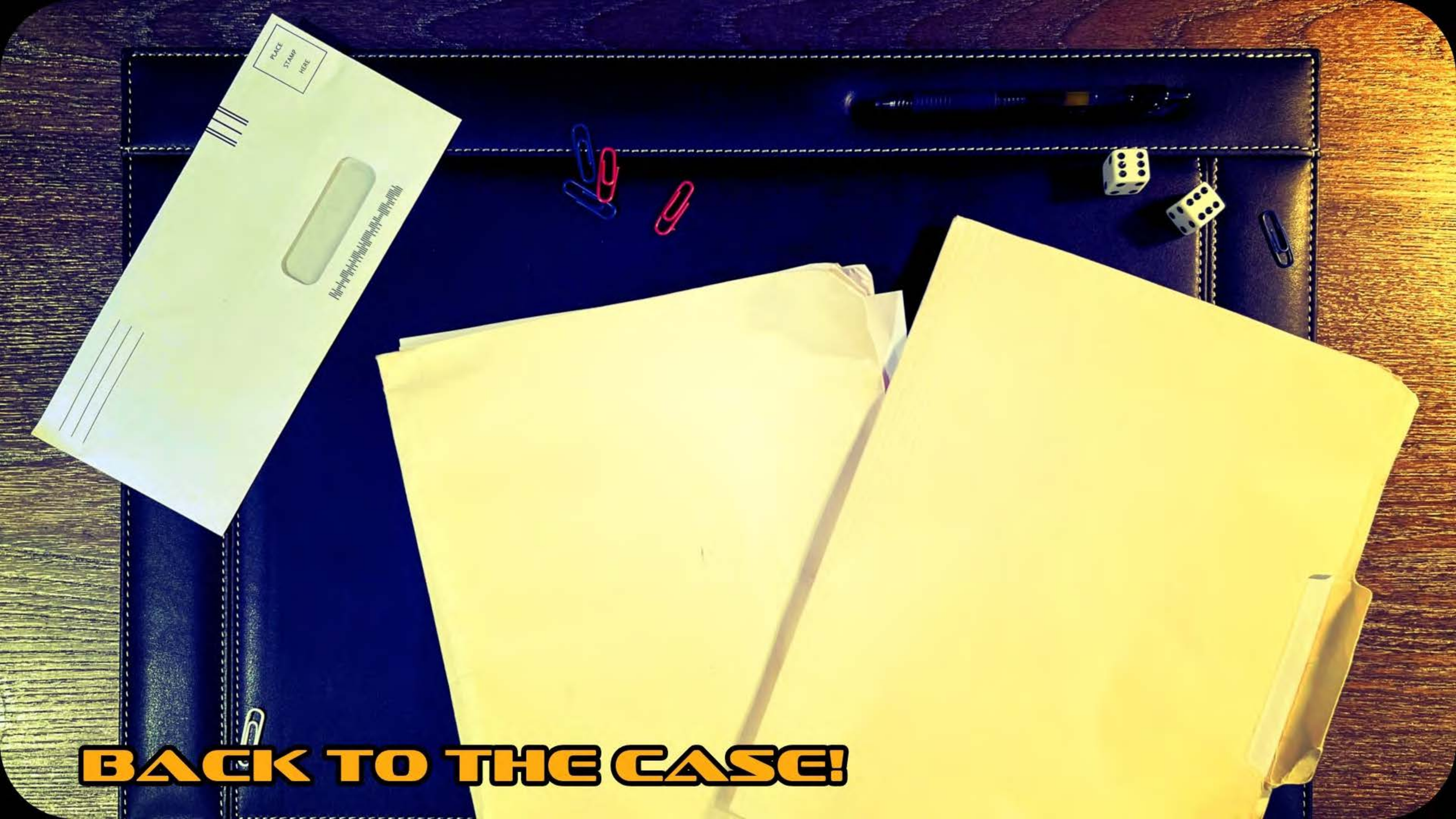
YOUR CODE IS BAD, AND YOU SHOULD FEEL BAD!

README | MIT license

zero.scalpel.fuse.pl

FUSE driver in Perl for reading scalpel's audit.txt file and showing a file system that maps files it would have carved to a disk image -- this allows for zero-storage carving as you can browse and view files with only a 'scalpel -p' (preview, scalpel writes no files) -- tested under Ubuntu Linux 18.04

Useful for me anyway, maybe not for you, but if so then enjoy.


PLACE
STAMP
HERE
BACK TO THE CASE!

I just kept yelling "ENHANCE!", and it kept working!
ENHANCE
ENHANCE
TO THE KEYBOARD!

CIRF NIBRS Supplemental Report-S12-021291 - Print Preview

File | Print Preview

Print | Export | Email | Find | First Page | Previous Page | Next Page | Last Page | Many Pages | Zoom Out | Zoom | Zoom In

Print/Export | Navigation | Zoom

CIRF NIBRS Supplemental Report-S12-021291

A LONG REPORT

10%

State of Nebraska vs. [redacted]

Case No. CR17-140 /// FOR 709 & 750-755 (753)
REPRINT 2017-05-19

1000 SLIDES OF JUSTICE

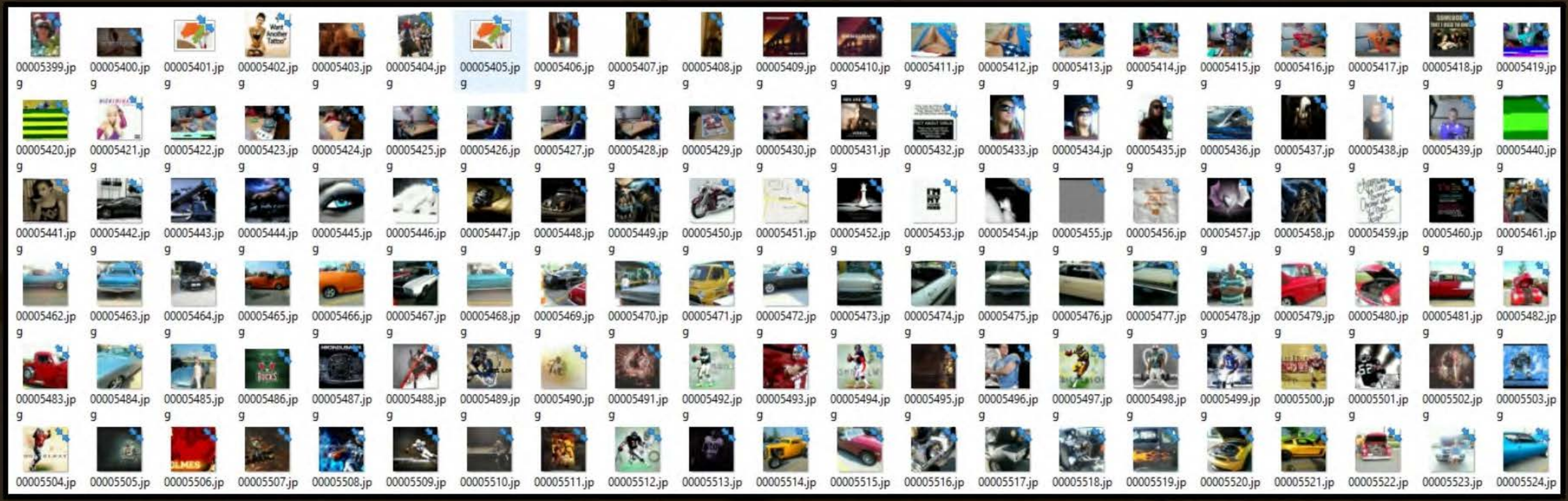
X GONNA GIVE IT TO YOU?

Just one
ore thing.

DEFCON
ENGAGE
COMPLETE
2017-02-01

Just one
more thing

SanDisk
16GB
4
micro SD HC
2017/02/06 17:28



13,337 JPEGs (~400 hash-match 2013 phone dump), plus our best evidence in this case.

96x96

200x200

2017/02/06 17:28

1x
1080x1080
(3024x3024)

2/06 17:28

5x
1000x1000

02/06 17:28

10x
960x960

/02/06 17:28

96x96

200x200

2017/02/06 17:28

WHERE WE WENT...

GUILTY

- 1st Degree Murder -> Life
- 2nd Degree Arson -> +20 Years

CARI FARVER (1974-2012)

The Cari Farver Memorial Scholarship

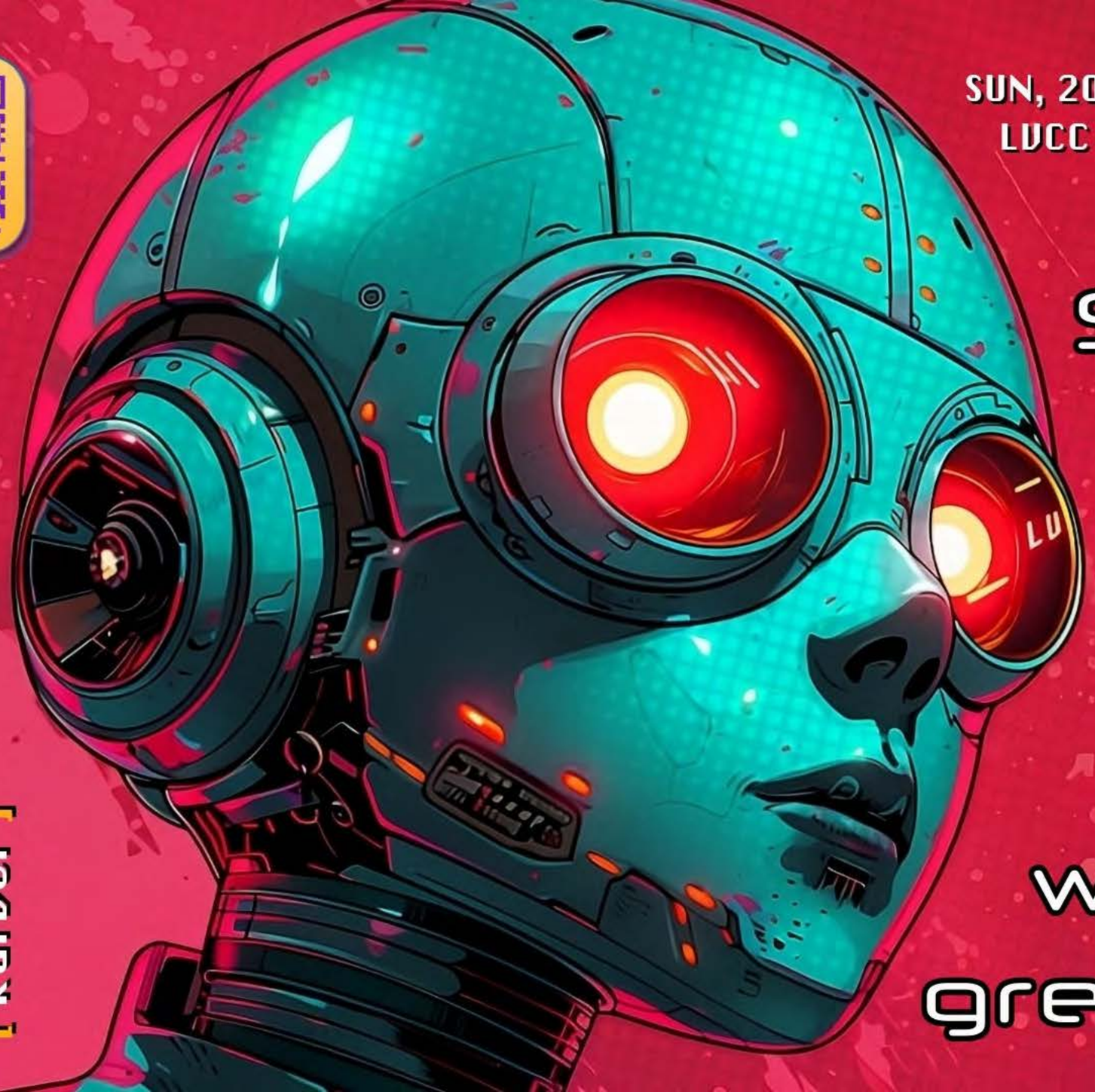
https://farverscholarship.org

CARI FARVER (1974-2012)

SUN, 2024-08-11 @ 1200T
LVCC - L3 - W322-W327
Warstories Track

DEFCON 32 ENGAGE

Solving the "Lover, Stalker, Killer" Murder with strings, grep, and Perl



https://forensic.coffee
Anthony Kava
[karver]

Media Sources:

Images not specifically identified here were created by Anthony Kava, who claims no copyright for any of this material, or are taken from public records and/or exhibits offered in open court, e.g., those of people, places, or evidence.

All AI graphics were generated by Midjourney with unique prompts by paid subscriber Anthony Kava.
#1, 4-5, 8-12, 19-25, 27-29, 35, 54, 56, 58, 61-63, 69-71, 74, 81, 93, 106, 110, 113-114, 116, 124, 129-132
ToS: https://docs.midjourney.com/docs/terms-of-service

#2: 16:9 Test Pattern, CC BY 3.0, Wikimedia User "Ldo" (2010), Wikimedia User "Glide08" (2021) (modified)
License: https://creativecommons.org/licenses/by/3.0/deed.en
Source: https://commons.wikimedia.org/wiki/File:PM5644.svg

#12, 59, 114: "Dr. Tobias Funke" (portrayed by David Cross II), "Insert Me Anywhere" viral marketing promotional chroma key image of character from Arrested Development, (c) Netflix 2013 (inserted), fair use intended by (1) using a minimal part, (2) following pattern of popular memes encouraged by owner, (3) using for educational purposes
Source: http://insertmeanywhere.biz

#18: Screen shot from Webamp, MIT, (c) 2015 Jordan Eldredge, Winamp (c) 2024 Winamp (modified)
License: https://github.com/captbaritone/webamp/blob/master/LICENSE.txt
Source: https://webamp.org

#30 (single still frame), 31 (app screenshot), 105 (single still frame): "Lover, Stalker, Killer" and Netflix, (c) 2024 Netflix / (c) 2024 Curious Films UK, fair use intended by (1) using a minimal part, (2) including for commentary and educational purposes

#34, 36-38, 43, 45, 47: Jupiter alphanumeric pager, CC BY-SA 4.0, Jochem Pluim (heavily modified)
License: https://creativecommons.org/licenses/by-sa/4.0/deed.en
Source: https://commons.wikimedia.org/wiki/File:Apollo_Jupiter_Pro_v9.1_Pager_%28P2000%29.jpg

PERSONAL VIEWS ONLY. NO ENROSEMENTS OF ANY KIND ARE INTENDED OR IMPLIED, NOR SHOULD ANY ENDORSEMENT BE CONSTRUED.
VIEWS EXPRESSED DO NOT REPRESENT ANYONE OTHER THAN THE PRESENTER.

Media Sources (cont'd):

#39-41: Parody / Mock Commodore 64 screen shots, GPL-3, Foone Turing (heavily modified)
License: https://github.com/foone/SierraDeathGenerator/blob/master/LICENSE.txt
Source: https://deathgenerator.com/

#55: OpenStreetMap screen shot, Open Database License, (c) OpenStreetMap 2024
License: https://www.openstreetmap.org/copyright

#59: Photo of from DEF CON 22, CC BY-SA 3.0, Sonofapharmacist (heavily modified)
License: https://creativecommons.org/licenses/by-sa/3.0/deed.en
Source: https://commons.wikimedia.org/wiki/File:Defcon_22_.jpg

#92: Photo of Japanese box for Windows 3.1, CCO 1.0 UNIVERSAL, Darklanlan, Microsoft Windows (c) Microsoft Corporation (heavily modified)
License: https://creativecommons.org/publicdomain/zero/1.0/deed.en
Source: https://commons.wikimedia.org/wiki/File:Microsoft_Windows_3.1_Jpn_box.jpg

#99: Photo of floppy disks, Pexels license, Photo by "S J" (modified)
License: https://www.pexels.com/license/
Source: https://www.pexels.com/photo/assorted-floppy-disks-12093423/

#125: Gavel image, CC BY 2.0, Brian Turner (https://www.flickr.com/photos/steakpinball/) (heavily modified)
License: https://creativecommons.org/licenses/by/2.0/deed.en
Source: https://commons.wikimedia.org/wiki/File:My_Trusty_Gavel.jpg

ALL MEDIA IN THIS PRESENTATION IS USED FOR EDUCATIONAL / INSTRUCTIONAL PURPOSES OR TO PARODY ITS SOURCE MATERIAL.
NO RIGHTS CLAIMED BY THE PRESENTER.

Software and Other References:

#94-96: Perl (Perl5) -- Copyright (c) Larry Wall and others
Link https://www.perl.org/

#100, 104: strings, grep -- Copyright (c) Free Software Foundation, Inc.
Link: https://www.gnu.org/software/grep/
Link: https://www.gnu.org/software/binutils/

#100: xz -- Copyright (c) The XZ Utils authors and contributors
Link: https://tukaani.org/xz/

#100: scalpel -- Copyright (c) Golden and Vico (?? LICENSE.txt didn't have names in it as of 2024-08-10)
Link: https://github.com/sleuthkit/scalpel

#100: xmount -- Copyright (c) Gillen Daniel and/or (c) SITS Sarl
Link: https://pinguin.lu/xmount
Link: https://www.sits.lu/xmount

#101: MariaDB -- Copyright (c) MariaDB Foundation
Link: http://www.mariadb.org/

#102: Reddit r/masterhacker post entitled, "Lover stalker killer documentary - IT guy master hacker"
Link: https://www.reddit.com/r/masterhacker/comments/1aqduer/lover_stalker_killer_documentary_it_guy_master/

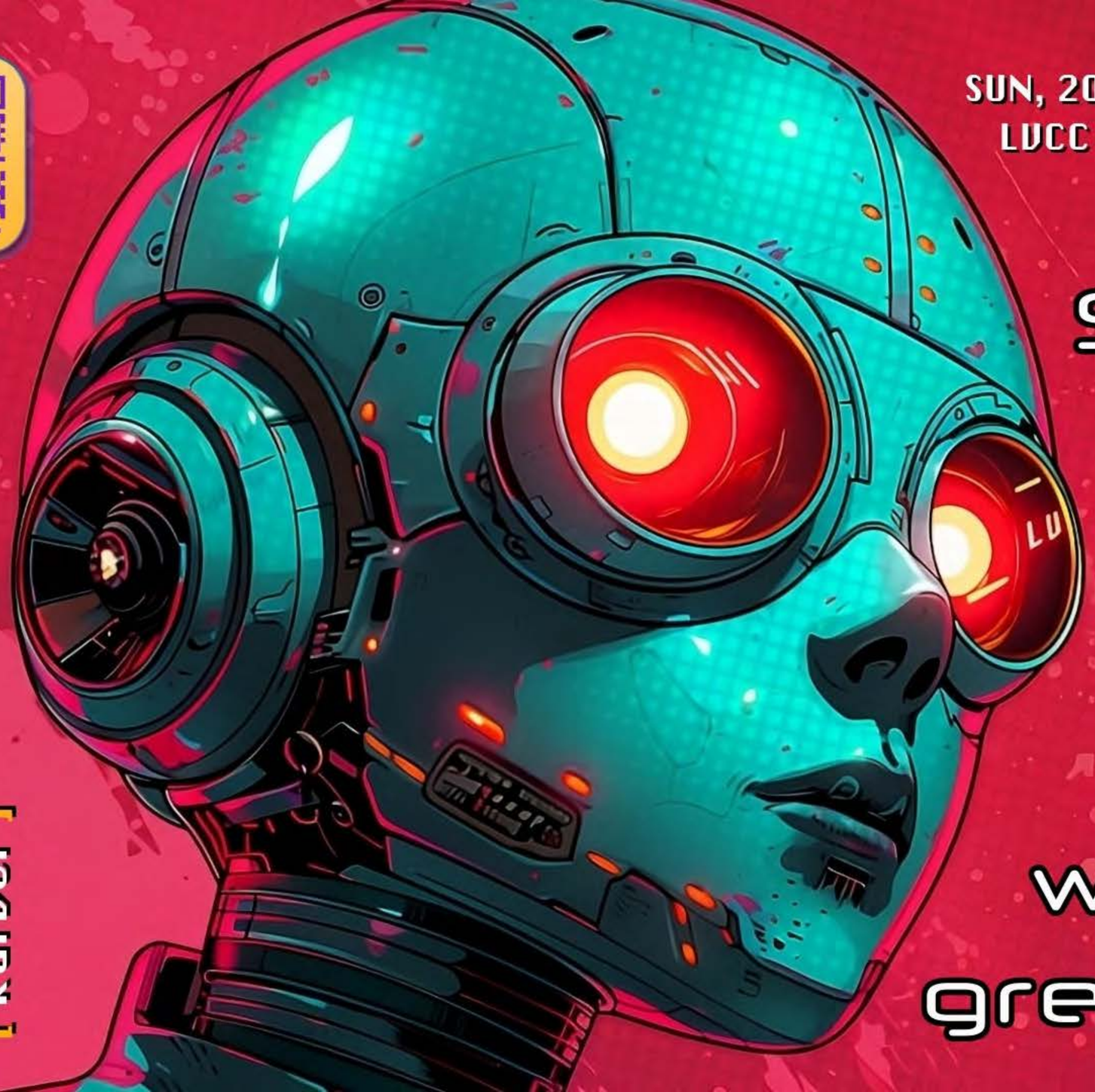
Looking for a good Y2K time? Modern Action Quake 2: free, cross-platform, beautiful: https://q2online.net/action

THANKS SO MUCH, DEF CON, DC32 ATTENDEES, DC32 NON-ATTENDEES, MEDIA.DEFCON.ORG LEECHERS, & YOUTUBE WATCHERS !!!1!
GREETZ TO DC402 AND KERNELCON, SKYTALKS 303, APPSEC VILLAGE, RECON VILLAGE, AND LARRY WALL.

SUN, 2024-08-11 @ 1200T
LVCC - L3 - W322-W327
Warstories Track

DEFCON 32 ENGAGE

Solving the "Lover, Stalker, Killer" Murder with strings, grep, and Perl



https://forensic.coffee
Anthony Kava
[karver]