

POLICE APPsec:

Protecting Cases, Citizens, and Ourselves



COVER SLIDE

W: NEbraskaCERT Cyber Security Forum

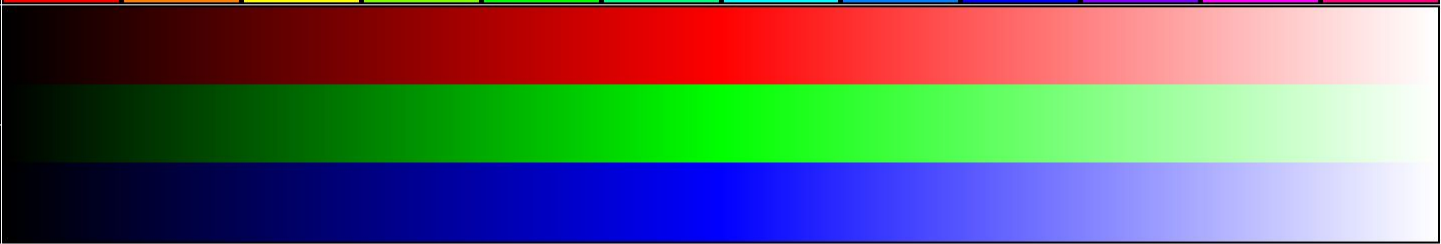
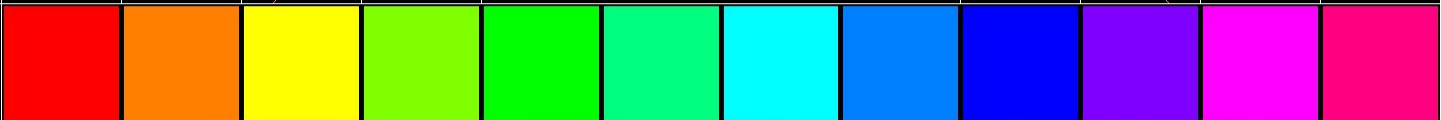
W: 2021-05-19 @ 11.30-13.00 CDT

W: Google Meet - <https://www.nebraskacert.org/CSF>

"In Cyberspace Your Mic is Always Muted"



tig 0.0.3 <http://tig.bulix.org>



1%	2%	3%	4%	5%	6%	7%	8%	9%	10%	11%	12%
2%	5%	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%

1920x1080 16:9

POLICE APPsec:

Protecting Cases, Citizens, and Ourselves



W: NEbraskaCERT Cyber Security Forum

W: 2021-05-19 @ 11.30-13.00 CDT

W: Google Meet - <https://www.nebraskacert.org/CSF>

"In Cyberspace Your Mic is Always Muted"



.-=[Anthony Kava | Tactical Computer Geek | <https://forensic.coffee>]=-.

***** COMMODORE 64 BASIC V2 *****

64K RAM SYSTEM 38911 BASIC BYTES FREE

READY.
█



POLICE APPsec:

Protecting Cases, Citizens, and Ourselves



W: NEbraskaCERT Cyber Security Forum

W: 2021-05-19 @ 11.30-13.00 CDT

W: Google Meet - <https://www.nebraskacert.org/CSF>

"In Cyberspace Your Mic is Always Muted"



.-=[Anthony Kava | Tactical Computer Geek | <https://forensic.coffee>]=-.

POLICE APPsec:

Protecting Cases, Citizens, and Ourselves



W: NEbraskaCERT Cyber Security Forum

W: 2021-05-19 @ 11.30-13.00 CDT

W: Google Meet - <https://www.nebraskacert.org/CSF>

"In Cyberspace Your Mic is Always Muted"



.-=[Anthony Kava | Tactical Computer Geek | <https://forensic.coffee>]=-.



I LOVE THIS. I FEEL SO SOCIAL.





HBO



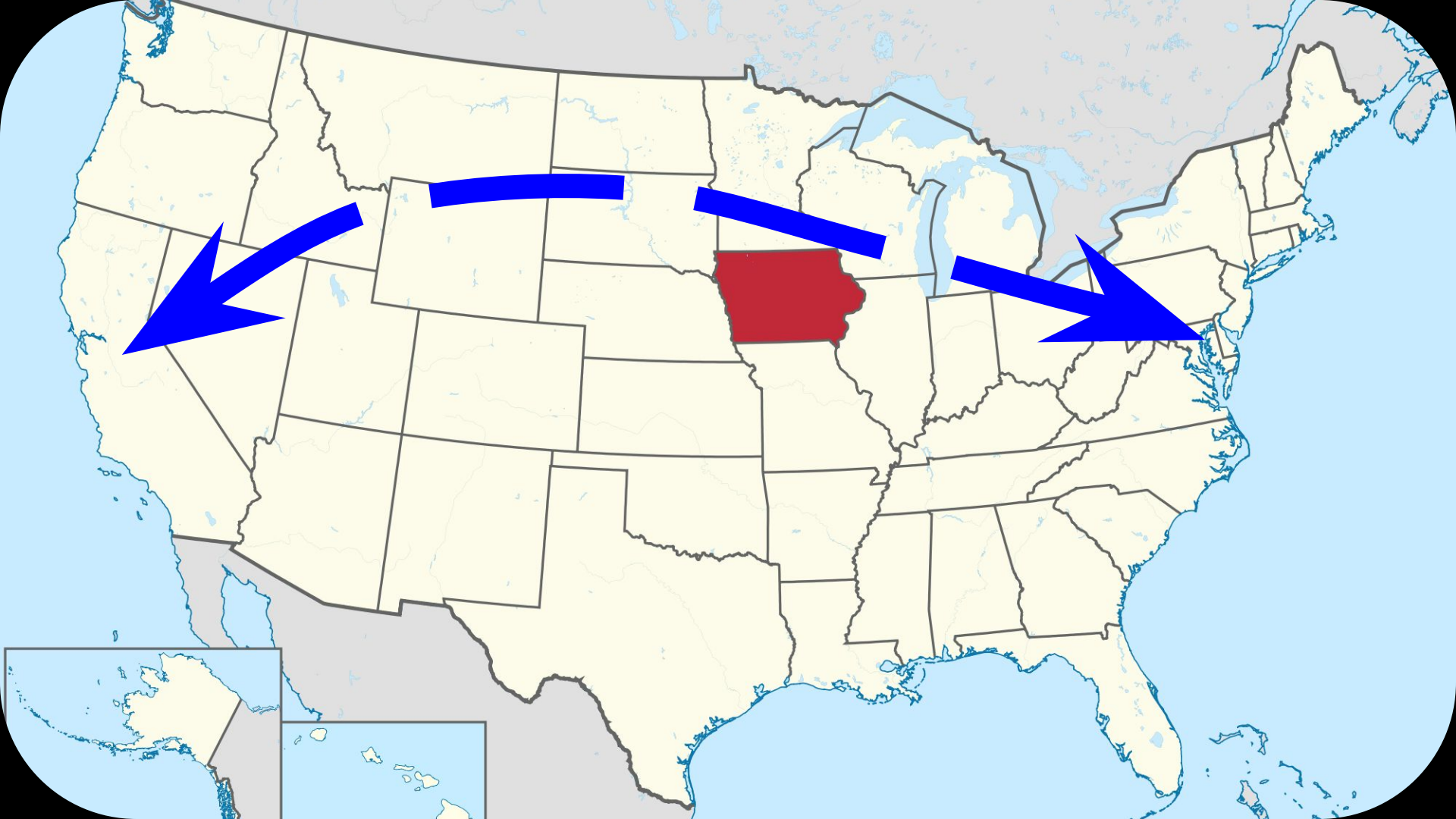
Rules of (Audience) Engagement

- Opinions expressed are poorly-formed and mine.
- Statements are not official positions of PCSO.
- I can't hear you so I will assume all jokes land.
- There may be some bad words; blame Google Meet.



AGenda

- ?** : ~~Where the hell is Iowa?~~ Intro
- I** : US Police Cyber Threats and Woes
- II** : AppSec and Software Vulnerabilities
- III** : #BlueLeaks: Breach, Leak, and Pain
- IV** : Conclusion / Apologies









COMING SOON:

2228-03-22

(a Saturday)



Pottawattamie County

a.k.a. PottCounty



pottcounty-ia.gov



potcounty-ia.gov

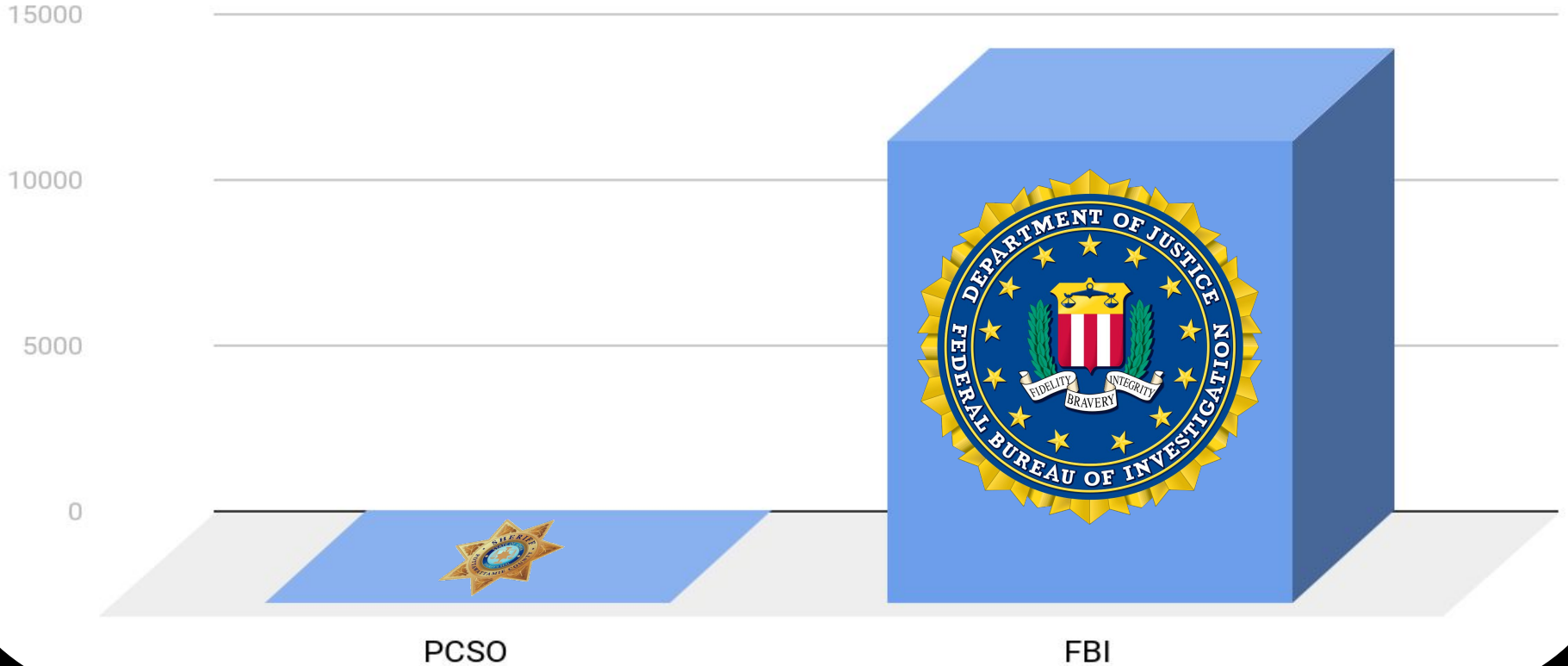






Sworn Personnel

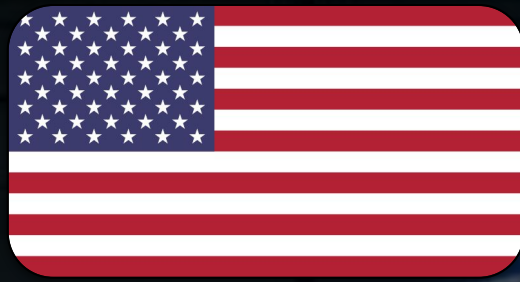
(not to scale)











1.1MM

Employees

18K

L.E. Agencies

12K

Local Agencies

75

Federal Agencies











FBI

FBI
TASK FORCE

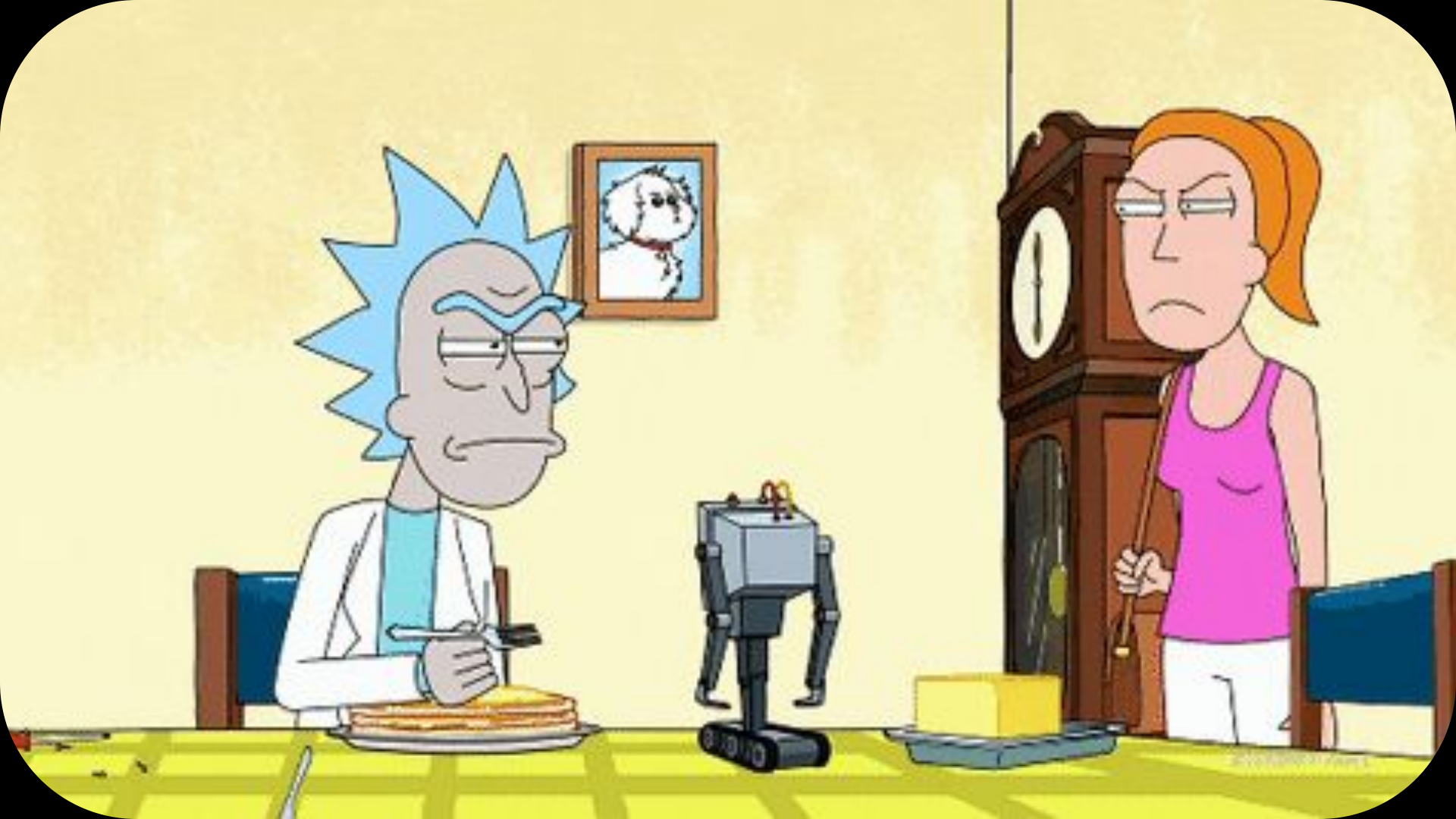
FBI

FBI

FBI





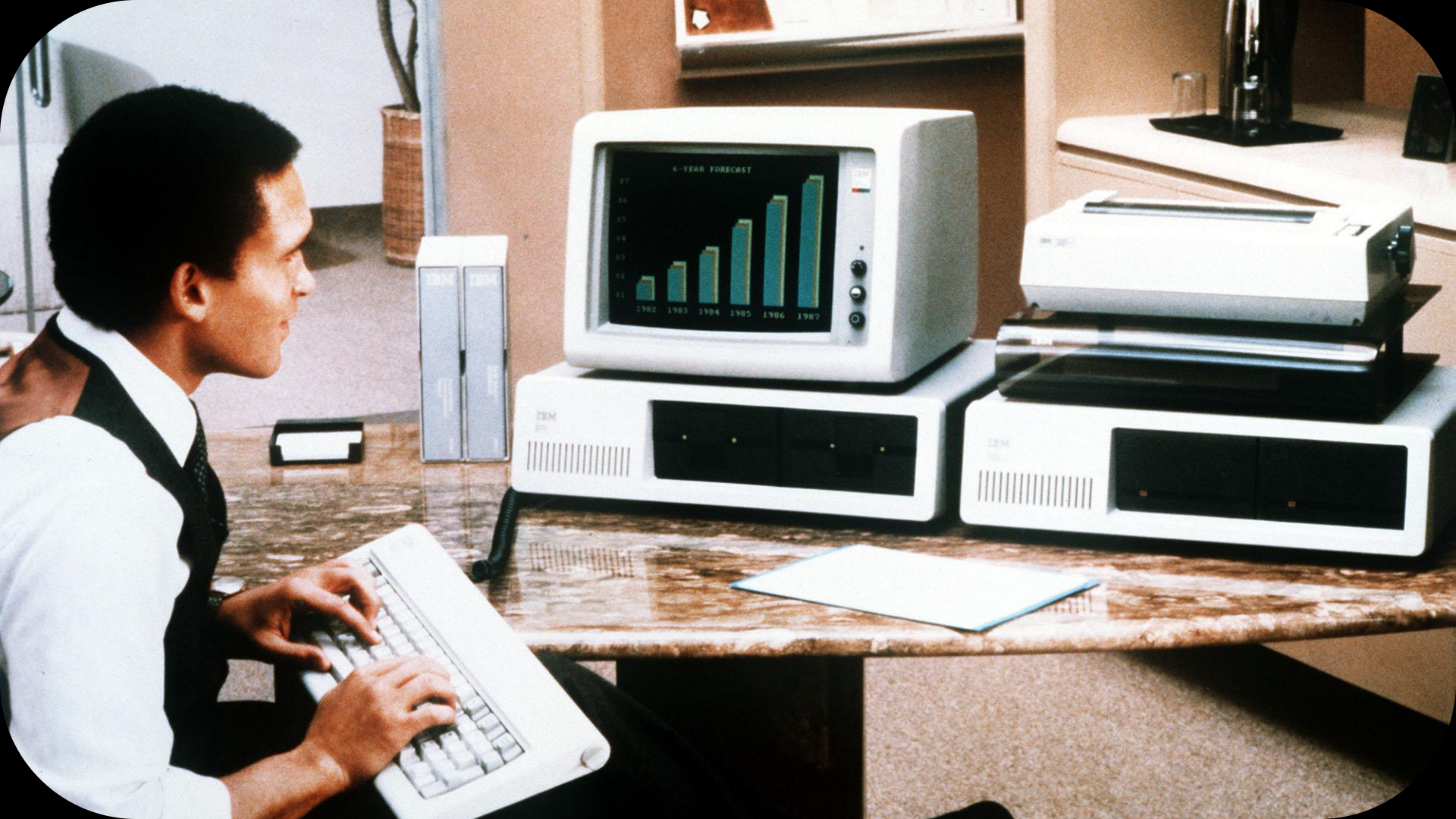




SECURITY



INFOSEC



6-YEAR FORECAST



CASE: 13-9953

Police Department Controlled Document - Do Not Duplicate

Officer SHEFFIELD and a Remsa building. Myself and Officer.

SPARKS POLICE DEPARTMENT INCIDENT REPORT

DA POST P&P DA
 OVA PAT DA
 JUC SCS-SER JUC BMC SJC BMC RJC
 SPLIT RMC RJC

CASE SUMMARY

ADDRESS/LOCATION

Occurred from (or at) 2275

Occurred to 10 Mo. 21 Day 13 Year 1871 Wk. Day 5

When Reported 10 Mo. 21 Day 13 Year Tues Time 0716

PRIMARY CODE 010110

CASE CROSS REFERENCE 1 10 Mo. 21 Day 13 Year Tues Time 0716

CASE CROSS REFERENCE 2 10 Mo. 21 Day 13 Year Tues Time 0716

HOW ORIGINALLY RECEIVED

DD = DESK OFFICER

DI = IN PERSON

OM = MAIL

OP = OTHER

OR = PHONE

OS = REFERRAL

DS = SELF-INITIATED

STATUS

A ACTIVE

JC CASE CLOSED/NO FURTHER

JI INFO ONLY

OK CLEARED ARREST, CIT. ETC.

OS OTHER

SU SUSPENDED

UF UNFOUNDED

Z COURTESY

2ND CODE 261116

CASE CROSS REFERENCE 2

Info Only

Gross Misdemeanor

Misdemeanor

Felony

CLEARED

A UNFOUNDED

B EXCEPT/ADULT

C EXCEPT/JUV

D NO FOLLOW UP

E SINGLE ADULT ARR/CITE

F SINGLE JUV ARR/CITE

G MULT ADULT ARR/CITE

H MULT JUV ARR/CITE

I JUV REPRIMAND

SPARKS CASE NO. 13-9953

PRIMARY CRIME/INCIDENT TYPE Homicide

BUSINESS NAME Sparks Middle School

APR/SUITE X

PERSON REPORTING (Signature) Lt. Hawkins

Reporting Officer Lt. Hawkins

Approving Supervisor Lt. Hawkins

ID NO. 076

ID NO. 076

3RD CODE 058

4TH CODE

PAGE 1 of 1 PAGES

PHOTOS TAKEN YES NO

WHO HS AMT Several

SUBPOENA RETURNED YES NO

INVOLVE VM

HEIGHT

WEIGHT

BUILD

NAME (LAST, FIRST, MIDDLE) Landsberry

DC TRIAL

EV

WIT CODE

K REF OTHER AGENCY

L FILED

M ADMIN CLOSURE

O OTHER

R REFER OT

S CITE

T

INVOLVE

RP = REP

VM =

Info Only

Gross Misdemeanor

Info Only

Gross Misdemeanor

Misdemeanor

Felony





Evidence

TAMPER EVIDENT SEAL
T.R.A.C. Seal™
"TAMPER" appears in contents may be pilfered.
SECURED
If the word
400751
Date
By

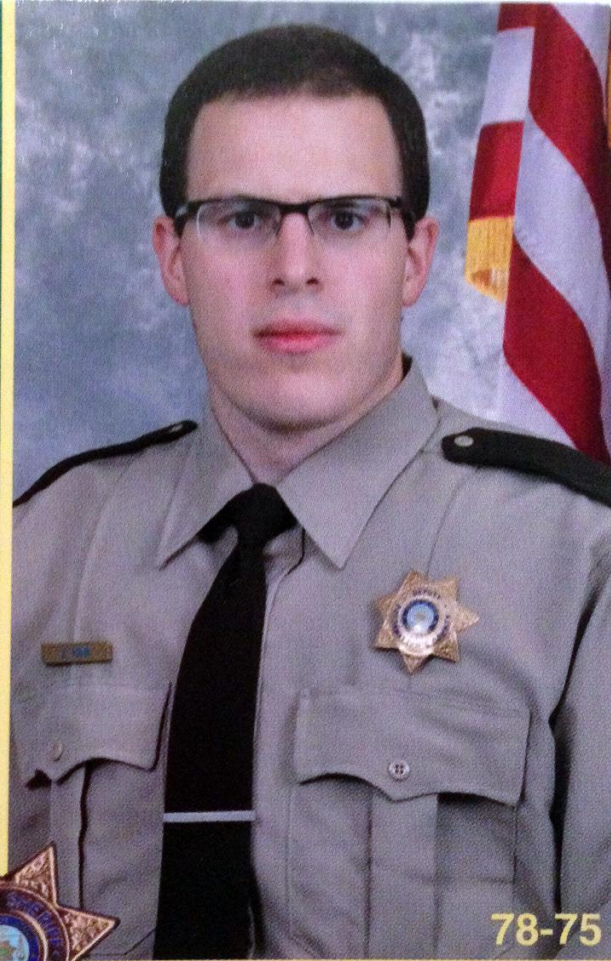
TAMPER EVIDENT SEAL
"TAMPER" appears
SECURED
If the word
400751
Date
By

FBI
VICTIM
ASSISTANCE





POTTAWATTAMIE COUNTY
SHERIFF'S OFFICE



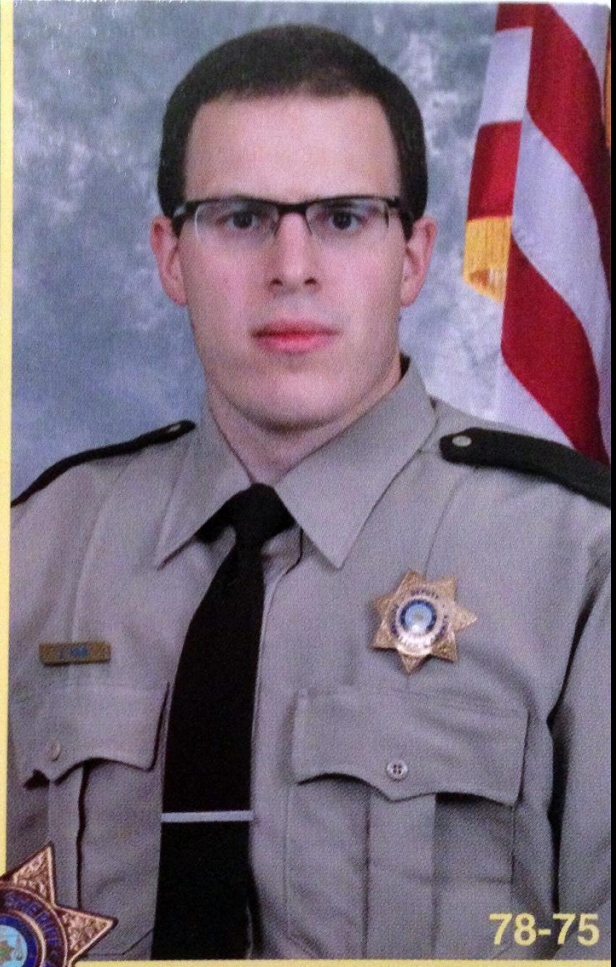
78-75



Special Deputy
ANTHONY KAVA



POTTAWATTAMIE COUNTY
SHERIFF'S OFFICE



78-75

Special Deputy
ANTHONY KAVA



IOWA
Internet Crimes
Against Children
TASK FORCE



POLICE
ICI

IOWA

Internet Crimes
Against Children

TASK FORCE





"We're the good guys, Marty."





HACKING
IS GOOD

EXIT









DIGITAL FORENSICS

CYBERSECURITY

CYBER CRIME

BIT O' I.T.



INFOSEC



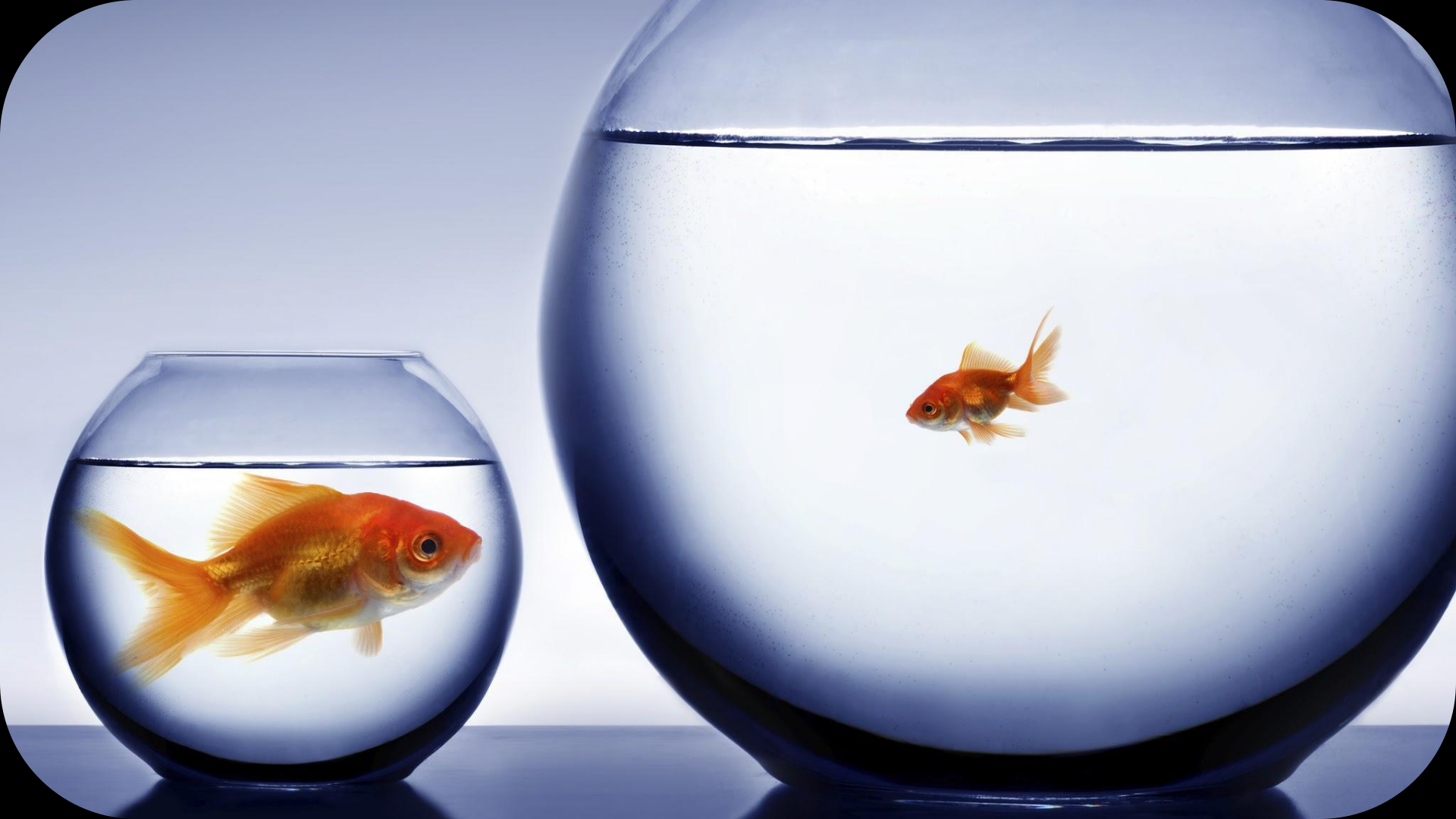
CYBERSEC





**SLOW
MINEFIELD**







Cockrell Hill police lose years worth of evidence in ransom hacking

The Cockrell Hill Police Department lost video evidence and a cache of digital documents after hackers invaded the department's computer system last month.

2016-12 Cockrell Hill PD, TX



The malware, which most likely originated from either Russia or Ukraine, gained access to the department's computer servers after someone clicked on a cloned email made to look like it was sent from a department email address, Barlag said. Messages generated by the computer virus demanded \$4,000 worth of internet currency known as Bitcoin as ransom for the return of the files, he said.

Lost videos and files back to 2009

2016-12 Cockrell Hill PD, TX

Ransomware Strikes Baltimore's 911 Dispatch System

Fortunately, Baltimore's IT office managed to isolate the threat and quickly restore the city's dispatch system.

2018-03 City of Baltimore, MD



Baltimore ransomware attack will cost the city over \$18 million

City residents are still facing issues.

2019-05 City of Baltimore, MD



Muscatine cyber attack targets government financial server

POSTED 8:44 AM, OCTOBER 19, 2018, BY [WQAD DIGITAL TEAM](#), UPDATED AT 08:50AM, OCTOBER 19, 2018

2018-10 City of Muscatine, IA

MUSCATINE, Iowa – A **MUSCOM server and the City of Muscatine Shieldware**, Springbrook (financial) server, and other city servers were the victims of a ransomware attack at approximately 1 a.m. Wednesday, Oct. 10. City of Muscatine IT staff along with other IT personnel have been working to isolate the ransomware and restore servers since that time.

2018-10 City of Muscatine, IA



LOCAL NEWS

Cybersecurity a top priority for West Des Moines

Posted: Jun 27, 2019 / 09:33 PM CDT / Updated: Jun 27, 2019 / 09:33 PM CDT

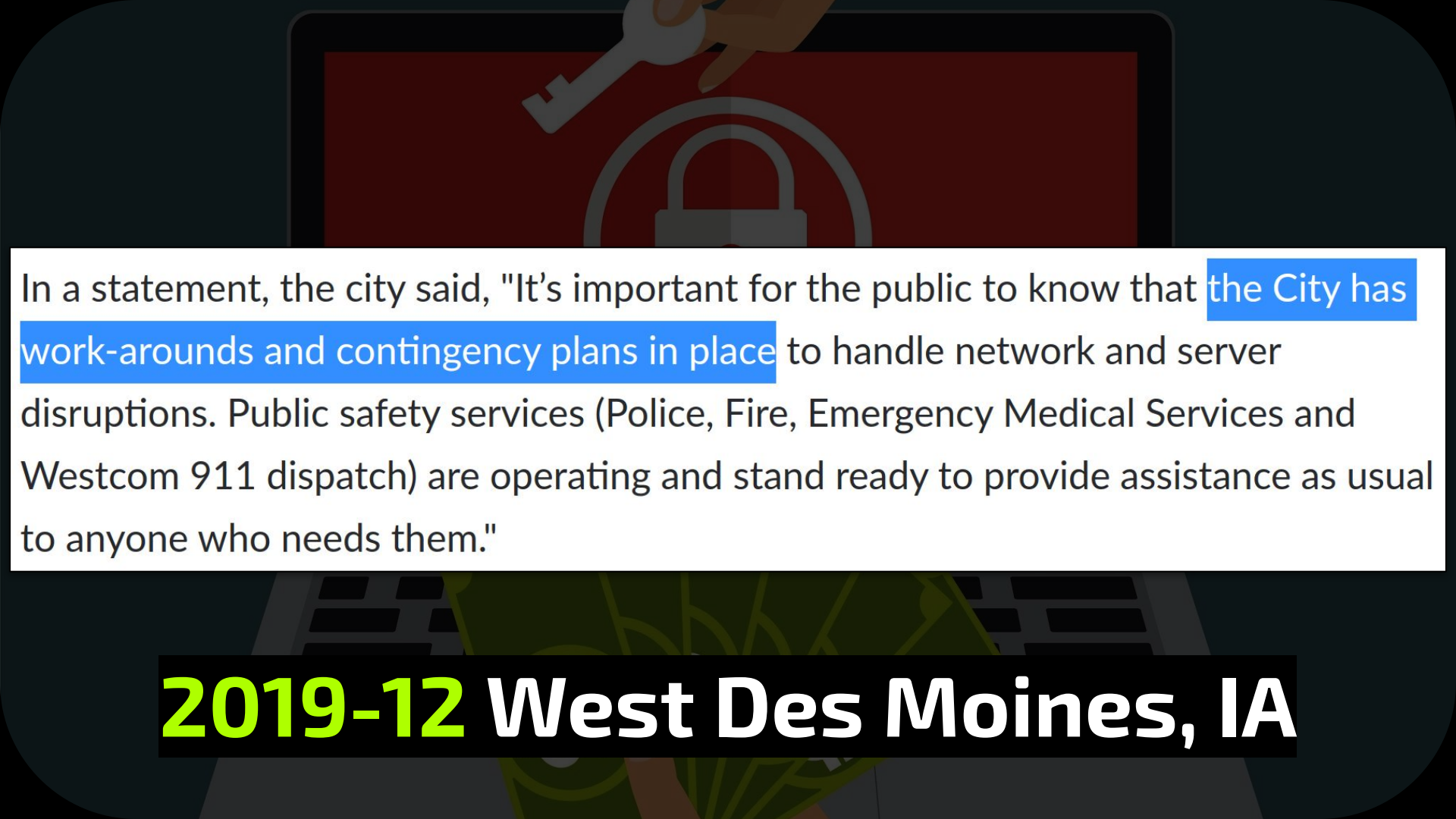
2019-06 Foreshadowing, IA

LOCAL NEWS

West Des Moines reports cyber attack on city operations

posted by Jason Taylor - Dec 13, 2019

2019-12 West Des Moines, IA



In a statement, the city said, "It's important for the public to know that the City has work-arounds and contingency plans in place to handle network and server disruptions. Public safety services (Police, Fire, Emergency Medical Services and Westcom 911 dispatch) are operating and stand ready to provide assistance as usual to anyone who needs them."

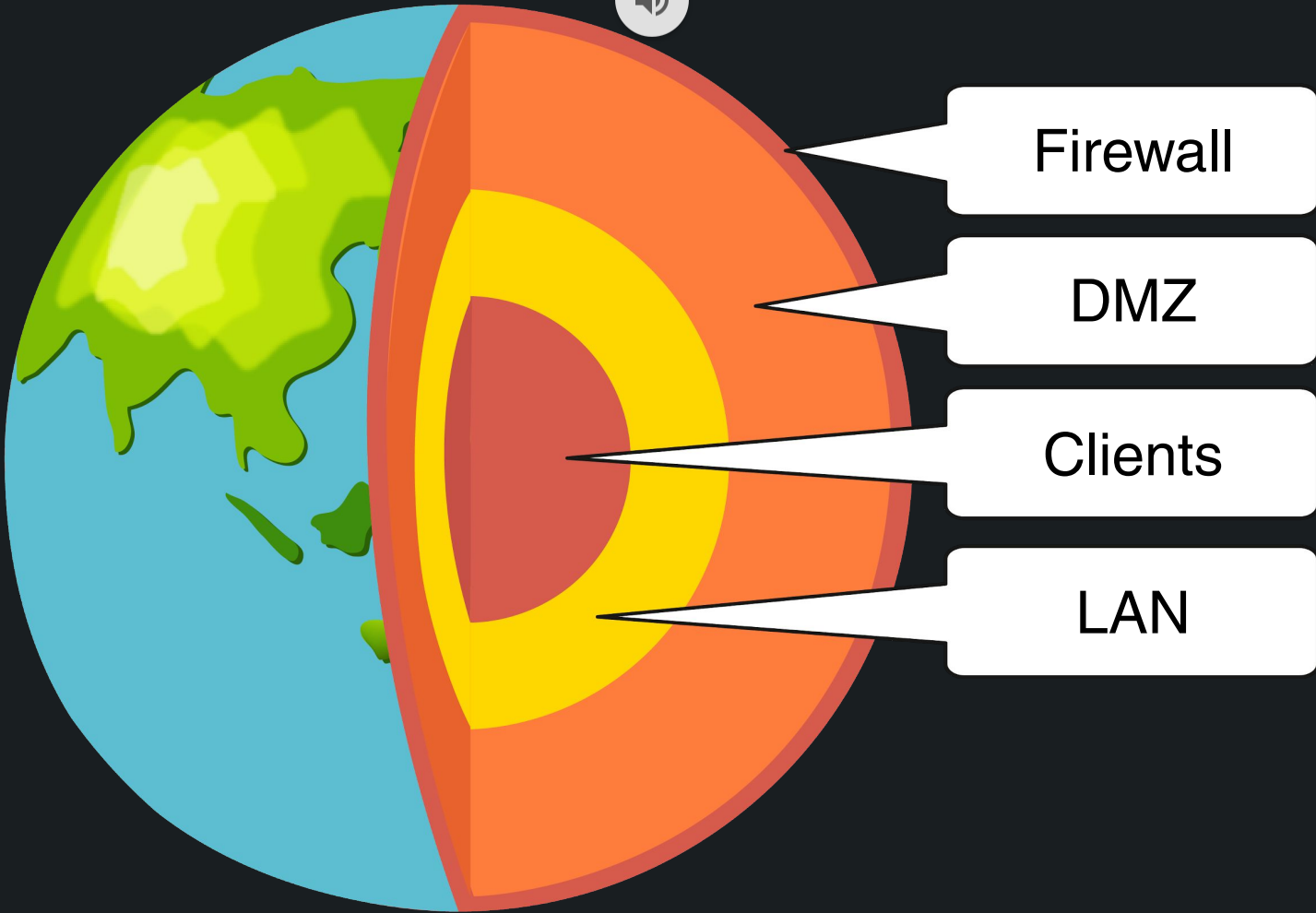
2019-12 West Des Moines, IA

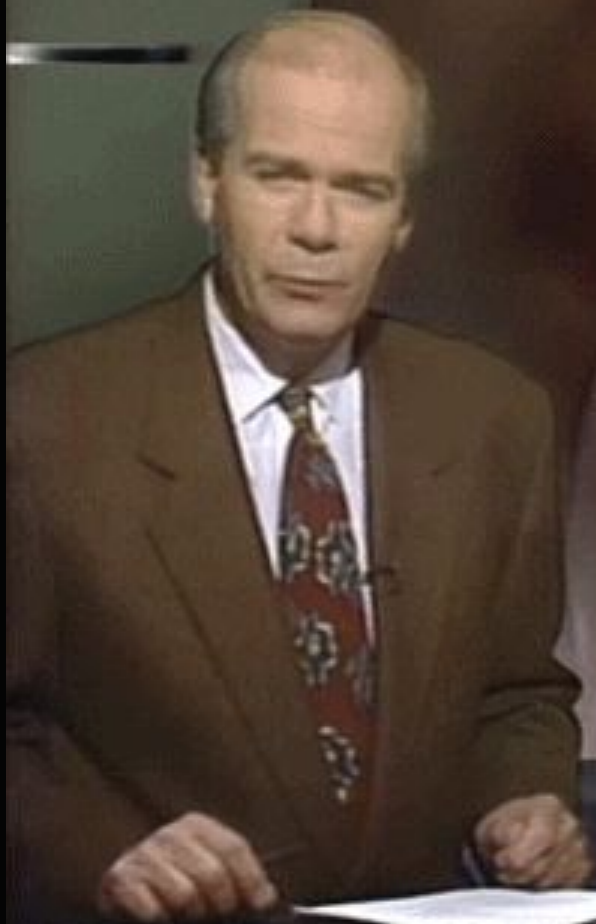


CONTRACT

CONFIDENTIAL
DATA

(nougat not pictured)









APPSEC

Main



File Manager



Control Panel



Print Manager



Clipboard
Viewer



Paintbrush



Terminal



Windows
Setup



PIF Editor



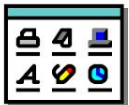
Read Me



MS-DOS
Prompt



Notepad



Accessories



Games

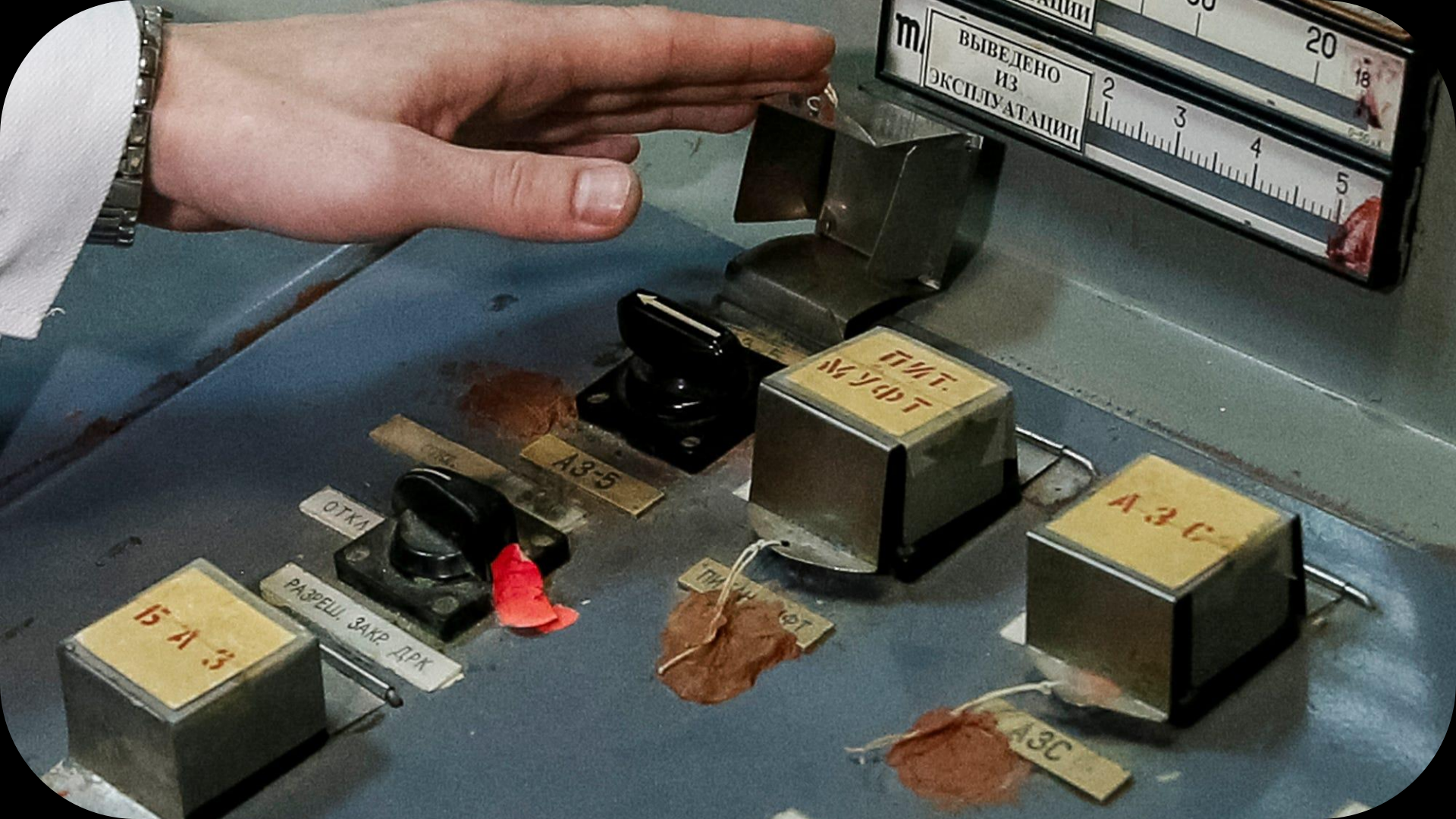


StartUp



Applications





м. ВЫВЕДЕНО ИЗ ЭКСПЛУАТАЦИИ

2 3 4 5

20

А3-5

ОТКА

РАЗРЕШ. ЗАКР. ДРК

15 А 3

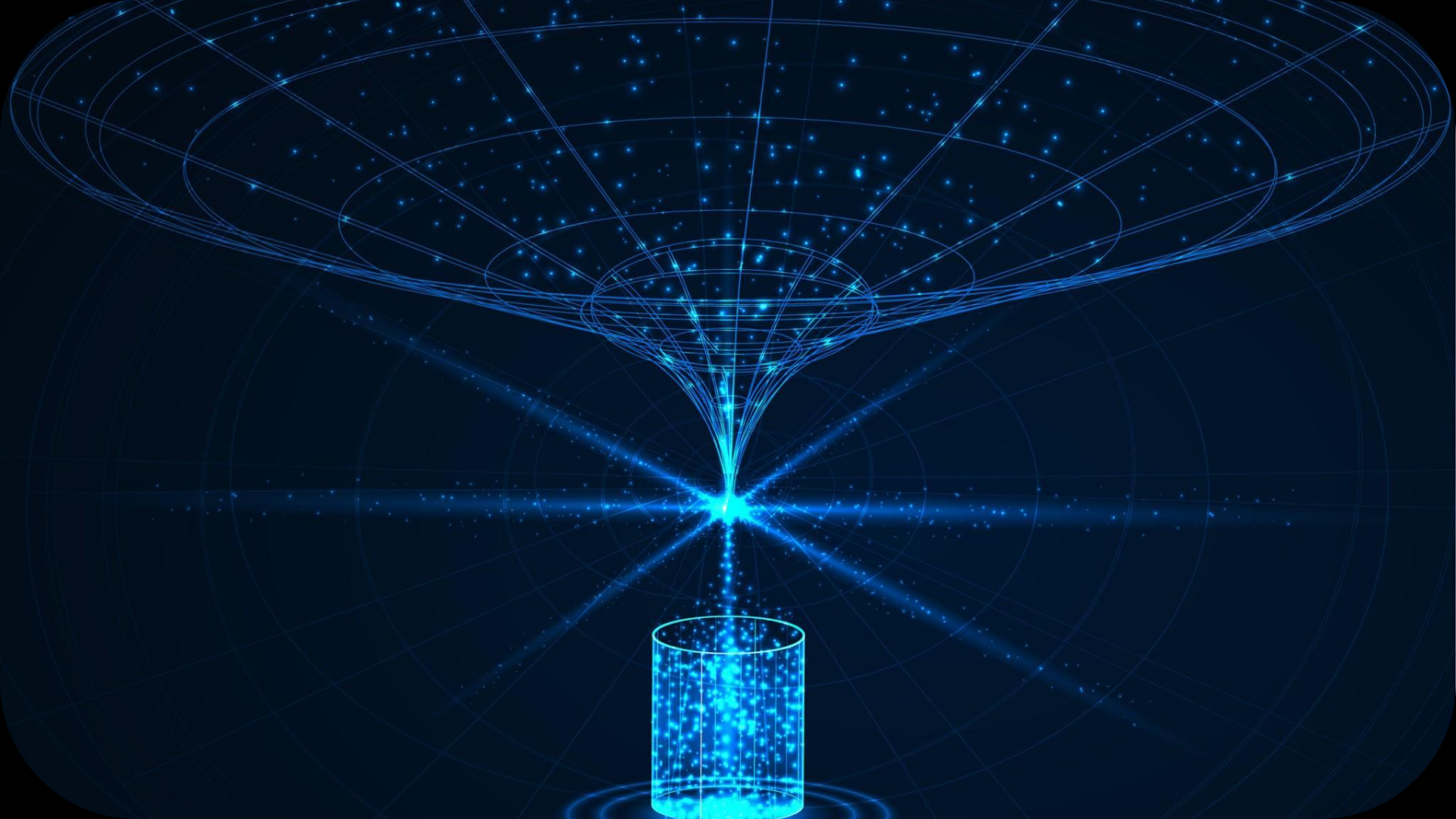
ТМТ. МУФТ

ТМТ. МУФТ

А3С

А3С













1

EMPLOYEE



250

EMPLOYEES



18K

EMPLOYEES

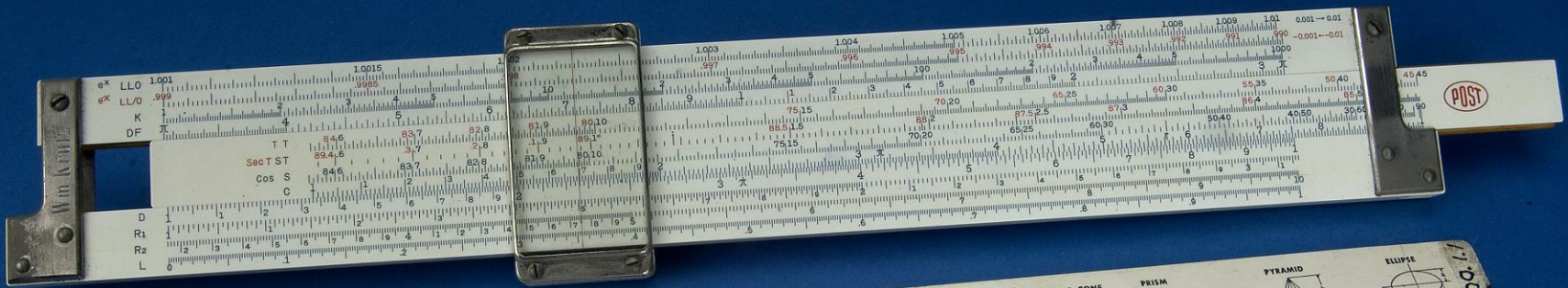


MS-DOS 3.0 / V.1.0
Version 3.1



Microsoft

Policing



RIGHT TRIANGLE



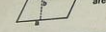
$\sin A = \frac{a}{c}$ $\cot A = \frac{b}{a}$
 $\cos A = \frac{b}{c}$ $\sec A = \frac{c}{b}$
 $\tan A = \frac{a}{b}$ $\operatorname{cosec} A = \frac{c}{a}$
 area = $\frac{1}{2} ab$ $c^2 = a^2 + b^2$

ANY TRIANGLE



area = $\frac{1}{2} bh$
 area = $\frac{1}{2} a(b \sin C)$
 $s = \frac{1}{2}(a + b + c)$

PARALLELOGRAM



area = ah

TRAPEZOID



area = $\frac{1}{2} h(a + b)$

CIRCLE



area = πr^2
 $c = 2\pi r$
 $\pi = 3.14159$

SECTOR OF CIRCLE



$\text{arc} = \frac{\theta}{360} \pi r$
 area = $\frac{1}{2} r^2 \frac{\theta}{360}$

PARABOLA



length of arc = $\frac{d}{2} \left[\sqrt{1 + \frac{16h}{d}} + \sqrt{1 + \frac{16h}{d}} \right]$
 area = $\frac{1}{2} dh$

DIETZGEN
The Slide Rule of World Famous Quality

Copyright Boreas Dietzgen Co., 1950
Form No. 1700-SK1/5008/PM25

FRUSTUM OF CONE



lateral surface = $\pi(R + r)h$
 R = radius of lower base
 r = radius of upper base
 Volume = $\frac{1}{3} \pi h (R^2 + Rr + r^2)$

CIRCULAR CONE



lateral surface = $\pi r s$
 r = radius of base
 volume = $\frac{1}{3} \pi r^2 h$

PRISM



lateral surface = perim. of base x h
 volume = A. of base x h

CYLINDER



lateral surface = $2\pi r h$
 volume = $\pi r^2 h$

PYRAMID



lateral area = $\frac{1}{2}$ perim. of base x l
 volume = $\frac{1}{3}$ A. of base x h/3

SPHERE



surface = $4\pi r^2$
 volume = $\frac{4}{3}\pi r^3$

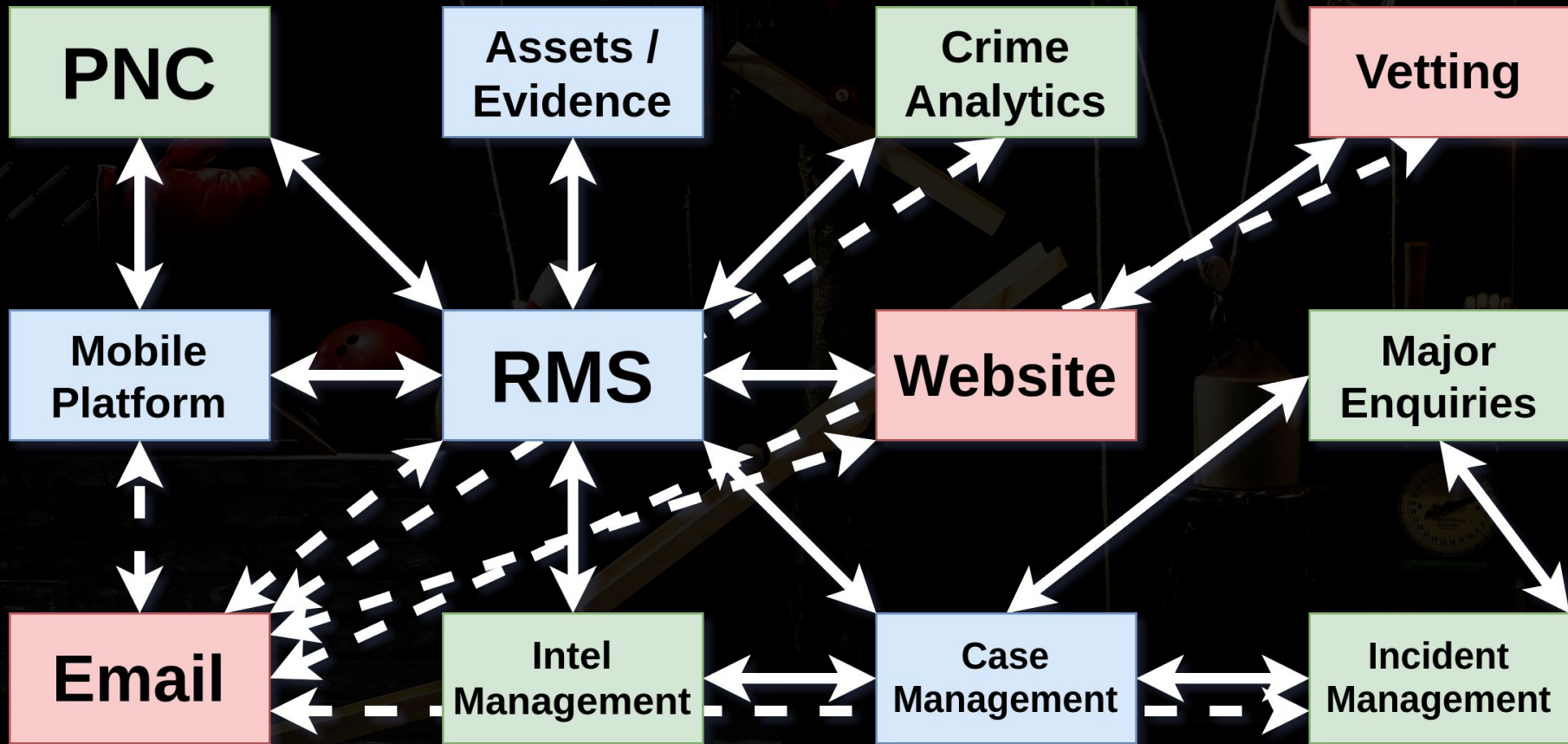
ELLIPSE



circumference (close approx.) = $2\pi \sqrt{\frac{a^2 + b^2}{2}}$
 area = πab



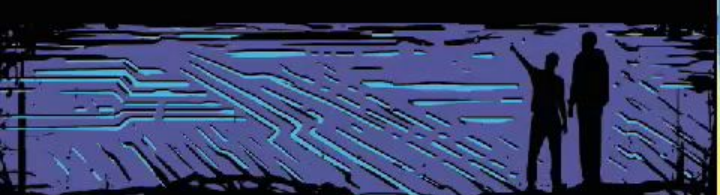








VISIT THE WORLD OF TOMORROW



DEFCON

AUGUST 9-11, 2019

WELCOME

/* DC27 APPSEC VILLAGE */
FRI 2019-08-09.1600 LOCUST TIME

HOW BAD COULD IT BE?
INSIDE LAW ENFORCEMENT AND LOCAL.GOV APPSEC

[Anthony "karver" Kava || @anthonykava || <https://forensic.coffee>]





The Local.gov
AppSec
Experience



How many **VULNS** could you find if you spent quality time with **local.gov** s/w?





LOCAL.GOV SOFTWARE

TL;DR: same stuff, different industry

(SPOILER ALERT)



Why is this stuff **IMPORTANT** ?

ING
RAILROAD

INCOME TAX



PAY 10%

OR

\$200

BALT
AVEN



0



**** COMMODORE 64 BASIC V2 ****
64K RAM SYSTEM 38911 BASIC BYTES FREE
READY.

OOOPS, YOUR FILES HAVE BEEN ENCRYPTED



WHAT HAPPENED TO MY
COMPUTER?

CAN I RECOVER MY
FILES?

HOW DO I PAY?

BITCOIN ACCEPTED HERE

WAITING FOR BLOCKCHAIN...
?

commodore

VIDEO MONITOR
MODEL 1702

commodore

1541

commodore

1541







Every vendor:
We assume customer has a
“SECURE ENVIRONMENT”

COMMON FEATURES



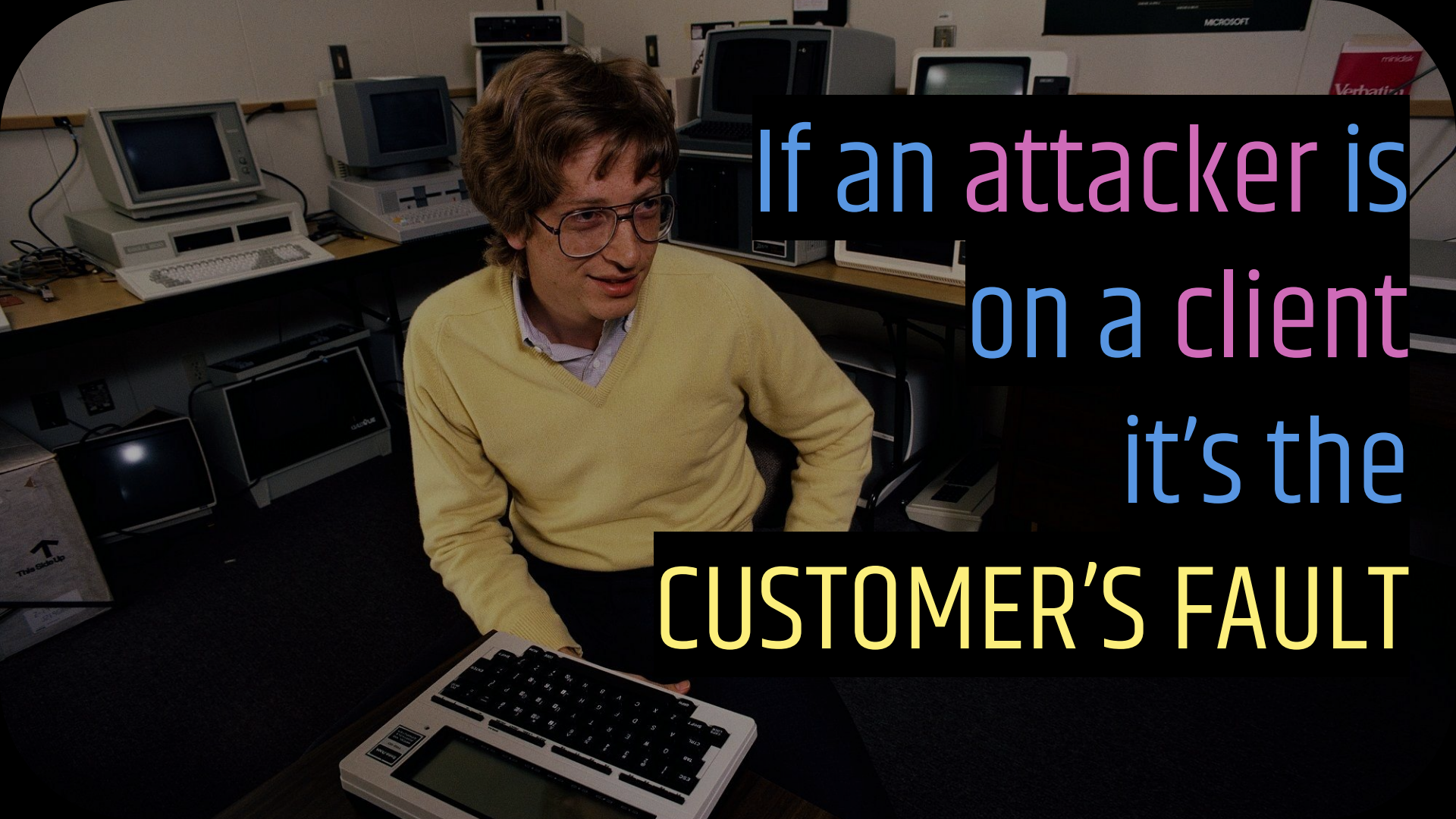
- Crypto is 0-BAD
- Hard-coded Creds
- Client-side Enforcement

A person is seen from behind, sitting at a desk in a room filled with vintage computer workstations. The person is looking at a monitor that displays some text. The room has wooden desks and several other similar computer setups. The overall atmosphere is that of a computer lab or office from the late 1980s or early 1990s.

Client-side vulns are

NOT CONSIDERED IMPORTANT





If an attacker is
on a client
it's the

CUSTOMER'S FAULT



lies,
damned lies,
and

'we take security seriously'




DANGER



DANGER



Local.gov
often can't
**LOOK UNDER
THE HOOD**

A man with long brown hair and a mustache, wearing a light-colored striped shirt, looks distressed with a pained expression. He is standing in front of a light blue door. On the door, the number '217' is printed above the words 'TECHNICAL SUPPORT'.

217

TECHNICAL
SUPPORT

Small Local.gov and LE orgs are
LUCKY IF THEY EVEN HAVE I.T.

We need people who CAN AND WILL

(LOOK UNDER THE [BONNET])

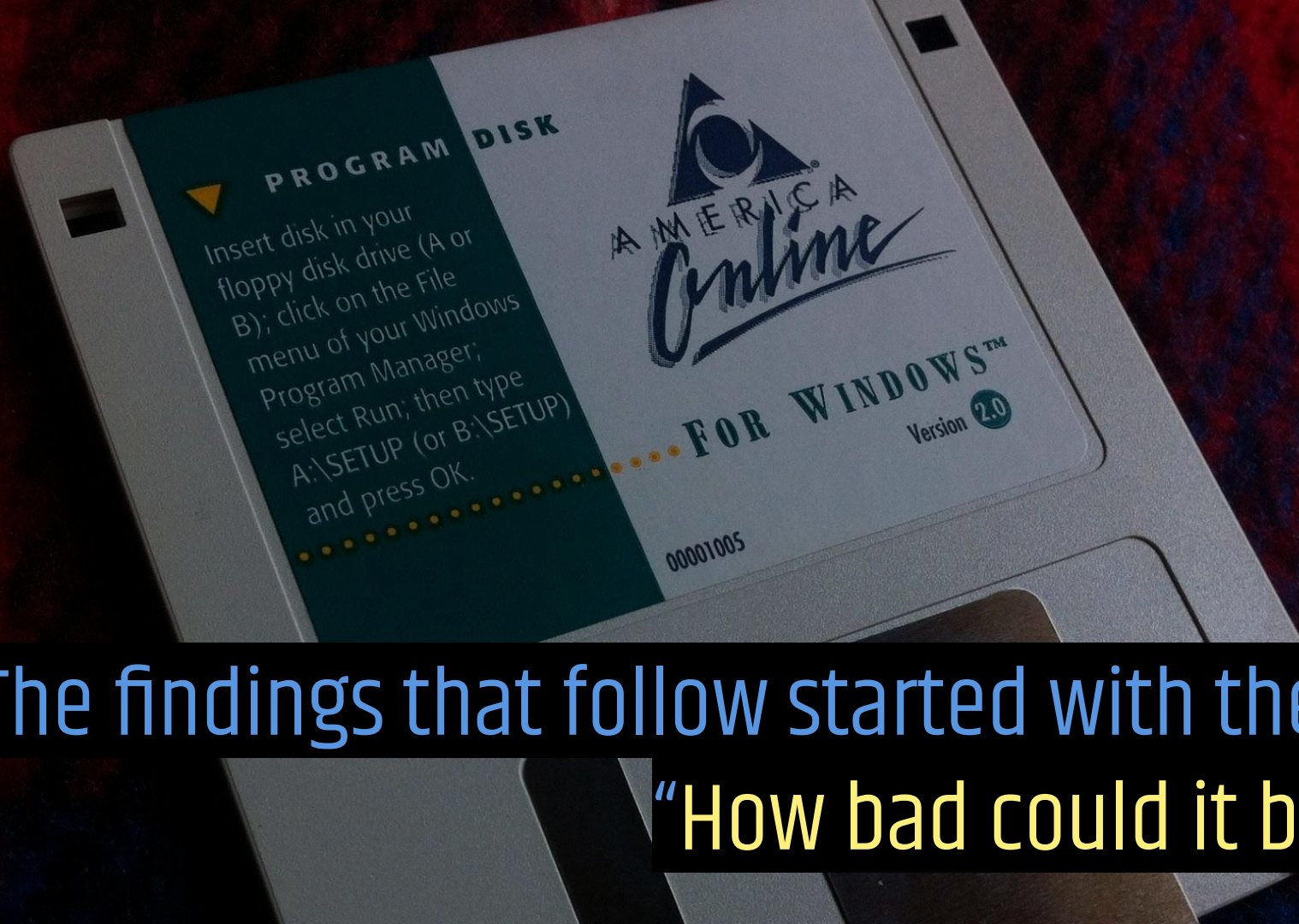




Cases in point: **THREE (3) VENDORS**



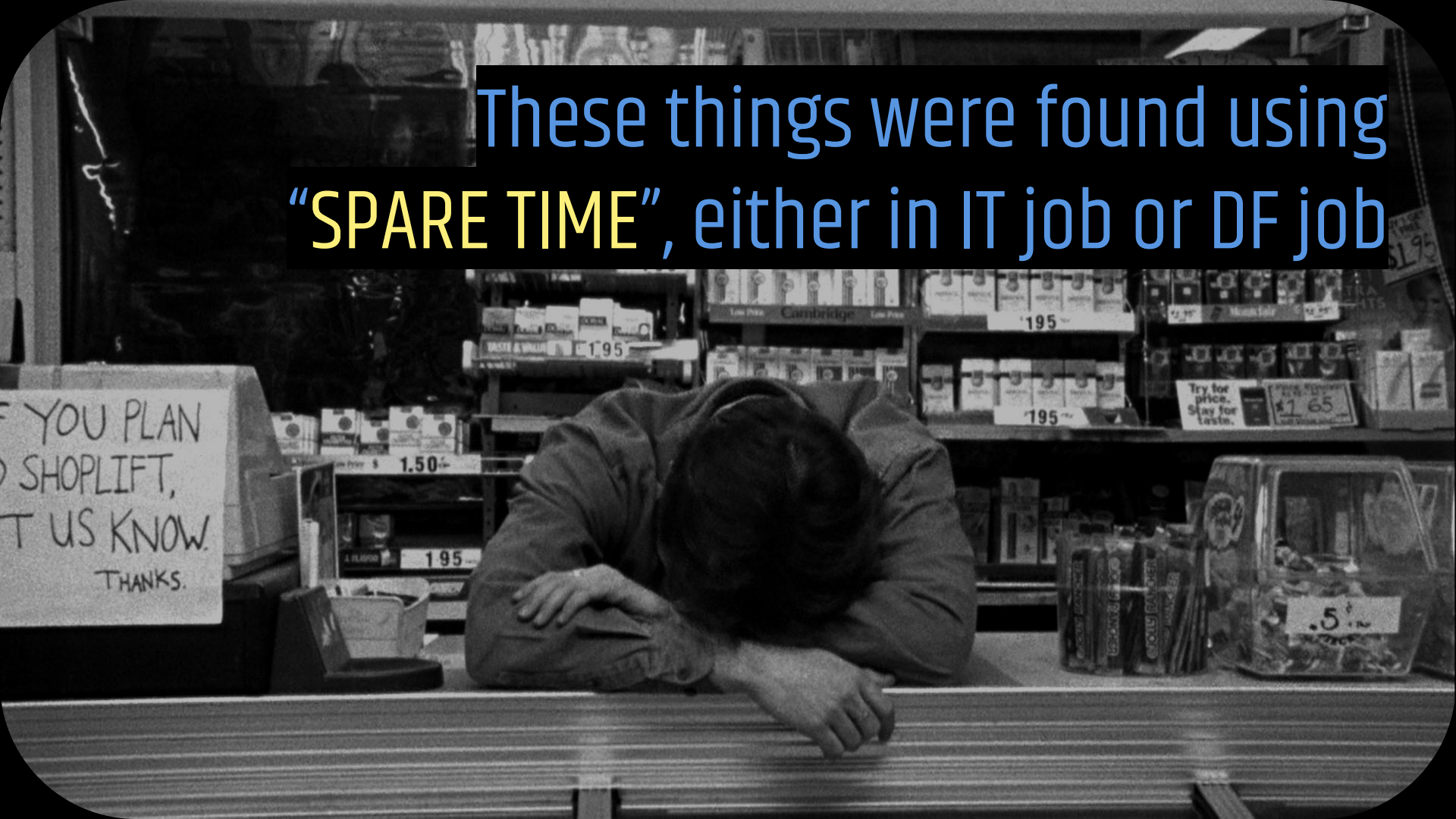
Names redacted to protect **SPEAKER**
All vulns **REPORTED** 1-5+ years ago, and
either **ADDRESSED** -or- products **RETIRED**

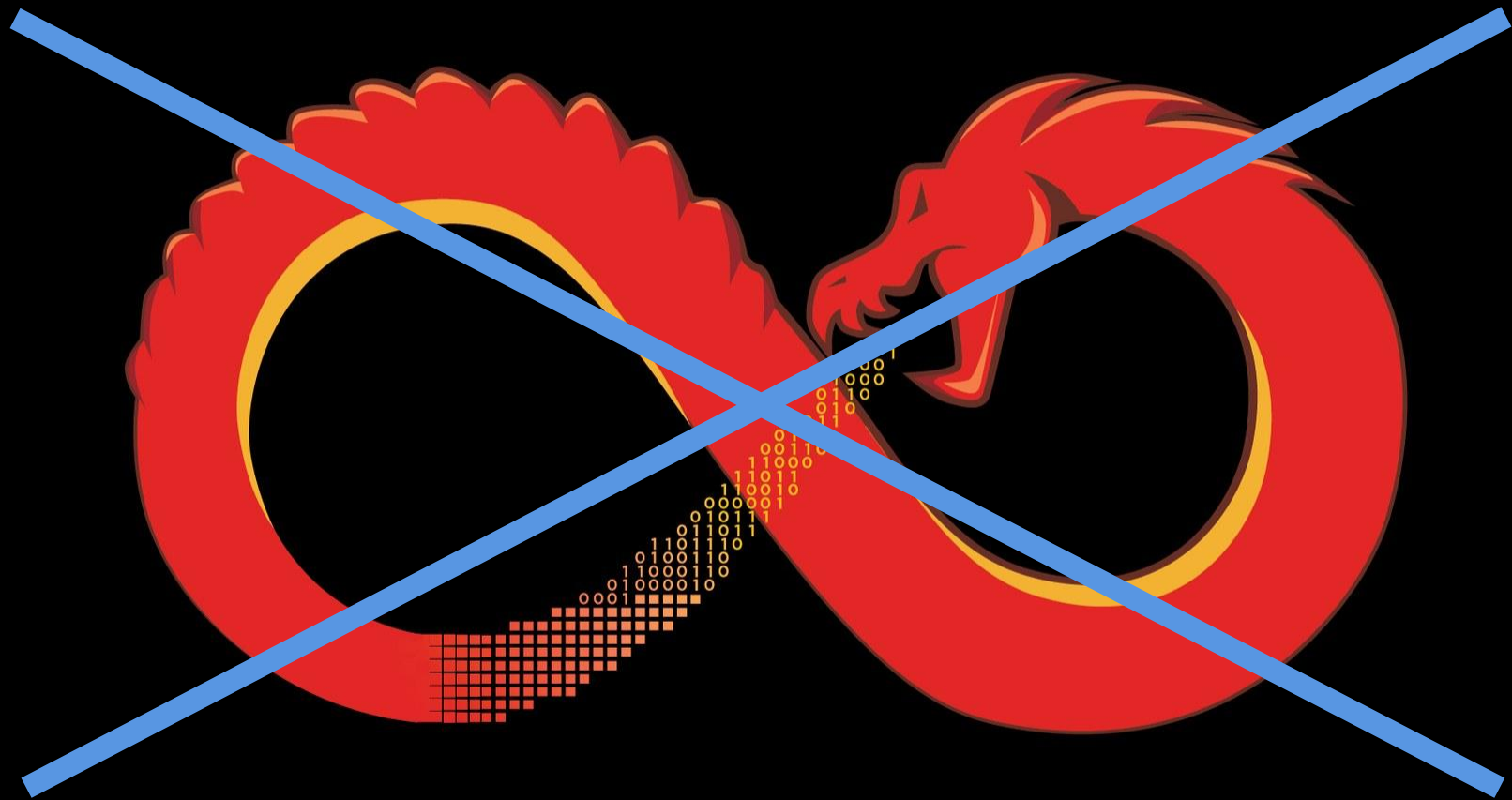


The findings that follow started with the Q,
“How bad could it be?”

These things were found using
“SPARE TIME”, either in IT job or DF job

IF YOU PLAN
TO SHOPLIFT,
LET US KNOW.
THANKS.







A Tale of Three Vendors





Vendor A

FINANCES, HR, PAYROLL,
INVENTORY, REAL ESTATE,
LAW ENFORCEMENT MGMT.

version
<person id="0.4

- SQL creds baked-into CLIENT INSTALL
- Oh, yeah, p/w is l33tsP3aK username
- *cough* Also has SA !?!?! address
- Bonus: Same at EVERY SITE <street



- API traffic is in **PLAIN TEXT**
- Auth tokens **NEVER EXPIRE** (weeks+)
- Access controls **NOT ENFORCED** in API





BUT WAIT, THERE'S MORE !

What about that **payroll website** ?

A blue folder with a white label that says "PAYROLL" is the central focus. It's on a desk with a calculator and a "WEEKLY TIME SHEET" form. There are also some other folders in the background.

PAYROLL

WEEKLY TIME SHEET

- That time **API TRAFFIC** was in the clear...
- ... with all your **PII** and whatnot for **WEEKS**
- Also **XSS**, but **XSS** is "NOT A SECURITY ISSUE"

Local App Server

Local DB Server

Usually HTTPS

Hosted Payroll Website

WEEKLY TIME SHEET

	Mon	Tue	Wed	Thu
6/10	8.00	8.00	8.00	8.00
		16.00	16.00	16.00
	7	7	7	7
	2	-	-	-
	10	7	7	7

54

Employee

Please...

- Tell customers about HTTP period ->
- Let us suppress SSN (okay, but not DOB/etc.)
- Stop using same SA p/w at all sites (okay...)
- Support p/w complexity + lock-outs! (okay)
- Put someone in charge and audit (...)





Believe it or not, this has a **HAPPY ENDING**

- 2014-03 Denial
- 2015-07 Anger
- 2015-08 Taunting (Bargaining?)
- 2016-07 Depression (Ours)
- 2016-08 Acceptance (Theirs)
- 2016-12 API Audit Underway!
- 2017-04 Vendor Promotes Employee!

Beta



Vendor B

911 DISPATCH, LE MGMT.,

JAIL MGMT., MOBILE CAD/COMMS



DEF
CON

Panasonic
Squad #228 (CF-30)

AT&T
Sprint

Radio

FEATURES!

Source Code
• Web Forms Express
• SQL-Programmer

SQL SERVER 6.5

CONCEPTS[®]

- 90% "serverless" b/c **DIRECT SQL**
- **EVERY** user has a SQL account w/ **DBO**
- One piece has users table, uses **PLAINTEXT**

Web records tool meant for INTERNET USE

- Creds stored PLAINTEXT (later XOR tho)
- Trivial SQLi AUTH BYPASS
- XSS, again, "XSS is not a VULN"
- Bonus: Ampersands (&) break the product

SQL Injection in a Nutshell

```
SELECT phoneNumber FROM employees WHERE lastName = 'Kava';  
712-555-1212
```

Department:

```
UPDATE dept SET name = 'Sheriff's Office' WHERE id = 42;  
*** SYNTAX ERROR NEAR: s Office' ***
```

Department:

```
UPDATE dept SET name = ''; DELETE FROM dept; --' WHERE id = 42;  
*** Deleted all rows from table "dept" ***
```




PUSH-TO-TALK SWITCH

Mobile CAD Software

- Don't need VPN b/c "WE DO CRYPTO"
- Rolled their own CRYPTO, 64-bit blocks...
- Questionable PADDING (next slide)
- Default keys, same crypto w/ PASSWORDS

ACCEPTED

A young boy with short brown hair and glasses is shown in profile, looking to the left. He has a red lollipop in his mouth. He is wearing a brown, textured sweater. The background is a dark, textured wall, possibly stone or brick. The overall lighting is dim and moody.

DIY-Crypto / Usage

- Password **MAX 12 CHAR**
- Part >8 chars is **PLAINTEXT** (0x20 if short)
- Asked for help for I.T. **PASSWORD RESETS...**



Password Reset Capability

- Set from app on **SERVER CONSOLE**
- Vendor updated p/w expiry feature
- **1st 90-day cycle**: 3x shifts of lock-outs

A man in a dark suit and tie is shown from the chest up, holding a black telephone receiver to his ear. He has a frustrated expression, with his mouth wide open as if shouting or yelling. The background is a blurred office setting with colorful binders on a shelf. The entire image is overlaid with a semi-transparent dark grey filter.

Password Reset Capability

- Asked for **RECIPE, CODE, or a TOOL**
- Vendor: Will dev tool, 6 months, PM, \$10K?
- Our hack? **TWELVE (12) LINES OF PYTHON...**

```
# 2015-06-02.[karver]
#... yada yada yada ...
dll=windll.product # load DLL
key=b'SECURITY' # key?
length=12 # length in bytes
if(operation[:3].lower()=='enc' and input):
    dll.encfunc(input,key,length) # encrypt
    print('0x' + hexlify(input).decode('utf-8'))
if(operation[:3].lower()=='dec' and input):
    input=input.decode('utf-8') # decode to string
    if input[:2]=='0x': input=input[2:] # drop leading 0x
    input=unhexlify(input) # convert to bin
    dll.decfunc(input,key,length) # decrypt
    print(input.decode('utf-8'))
```



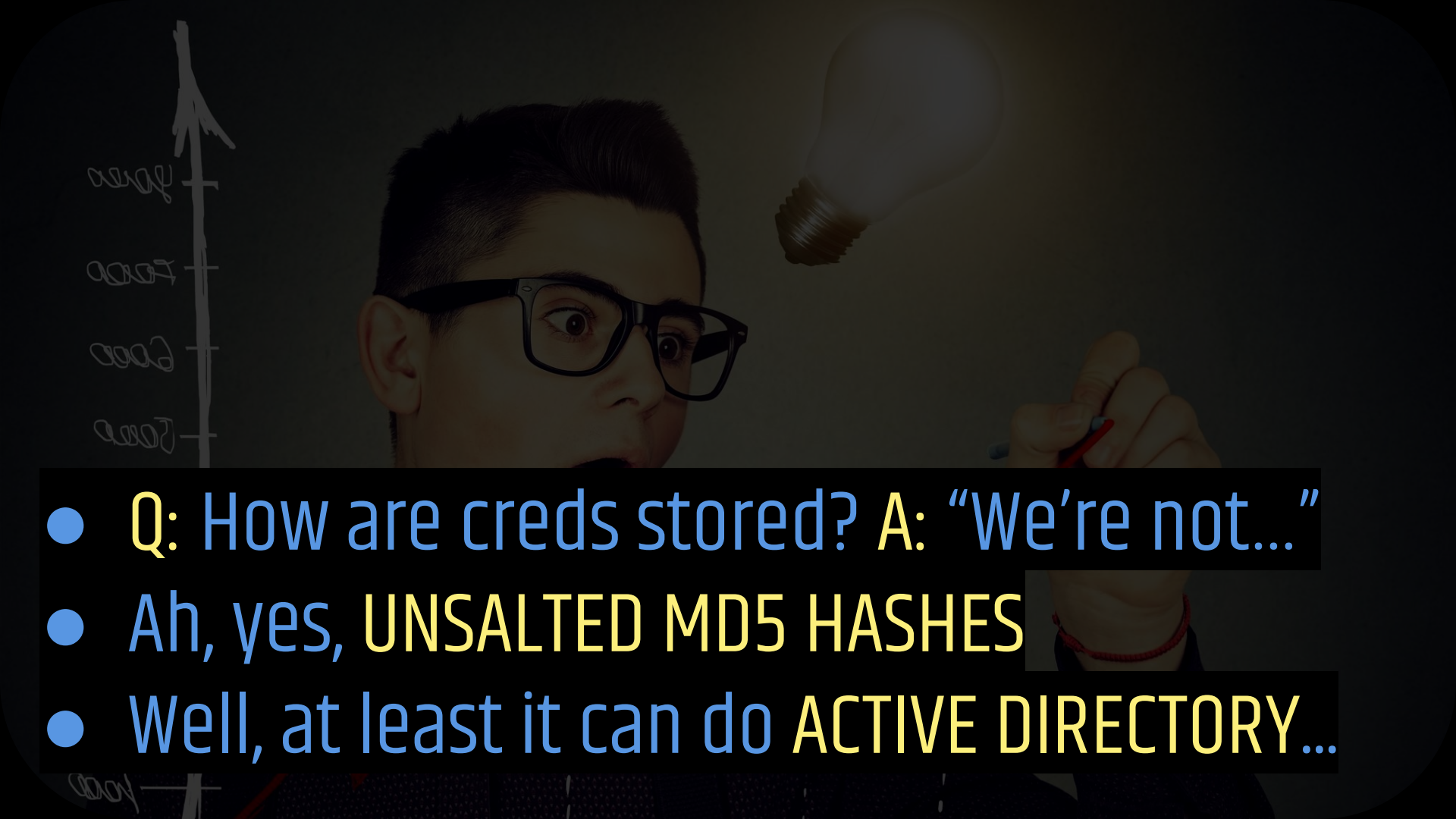




Vendor C


911 DISPATCH, LE MGMT.,


JAIL MGMT., MOBILE CAD/COMMS

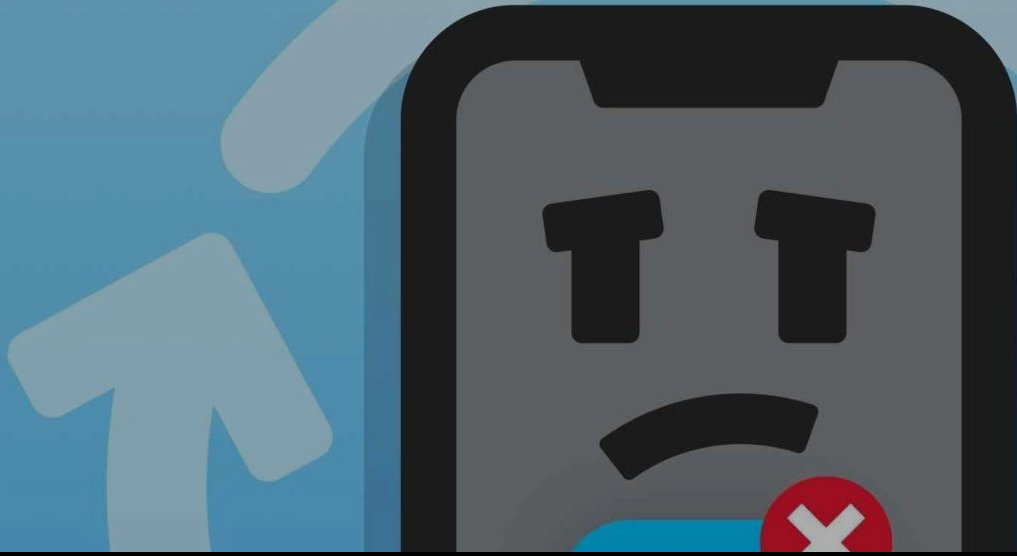
- 
- Q: How are creds stored? A: “We’re not...”
 - Ah, yes, **UNSALTED MD5 HASHES**
 - Well, at least it can do **ACTIVE DIRECTORY...**




- Who even knows what S means in LDAPS?
- AD works, but stores MD5 vals ANYWAY
- Correction: `strtolower(md5($pass))`

- 
- A small brown dog, possibly a pug or similar breed, is wearing a brown, textured hood or blanket that covers its head and ears. The dog is looking directly at the camera with a neutral expression. The background is a plain, light-colored wall. The dog is sitting on a white, textured surface, likely a bed or a couch.
- TLS/SSL certs not validated
 - BLIND HYPERLINKS in messaging
 - AD auth only done ONCE, no time limit

- 
- TLS/SSL certs not validated
 - BLIND HYPERLINKS in messaging
 - AD auth only done ONCE, no time limit



- Updater doesn't need **ADMIN RIGHTS**, cool
- B/C '**Everyone**' on `%ProgramFiles%\Client`
- Uses **librsync**, only checks **SIZE + MTIME**

- 
- Client **DIRECT SQL FOR AUTH**
 - Powerful SQL user, **ROT13** for safety
 - Oh yeah, client handles **AUDIT TRAIL** too

```
s/WHERE password =  
:password/WHERE 1 = 1  
\x00\x00\x00\x00\x00  
\x00\x00\x00\x00\x00  
\x00\x00\x00\x00\x00/g
```



Look, ma, no local admin needed

0. Hex editor + SQL

1. Size + mtime

2. Auth/Aud BYPASS

3. ???

4. DEMO (1' 05")

My Messages

[View Messages](#)[- No Subject](#)[Inmate - Released - Inmate #IN201800013 -](#)[Inmate - Released - Inmate #IN201800003 - DOE, JANE - PCJ \(AA-1\)](#)

Web Links

[E-File](#)
[PCSO - Website](#)
[Weather](#)

Food Check

Last, First Name

COBAIN, KURT
COBAIN, KURT

Current Cell

C-8
[Booking-2](#)
AA-5
[Booking-2](#)
[C-19](#)

Total Records: 5

Released Today

Last, First Name	Inmate #	Release Date	Last, First Name	Release Reason
Total Records: 0				

Disposal

Item #	Description	Target Disposal Date/Time
Total Records: 0		

My Shortcuts

- [Dashboard](#)
- [Main Menu](#)
- [CFS Log](#)
- [Cases](#)
- [Current Inmates](#)
- [Civil Processes](#)
- [Customers](#)
- [Name Search](#)
- [Address Search](#)

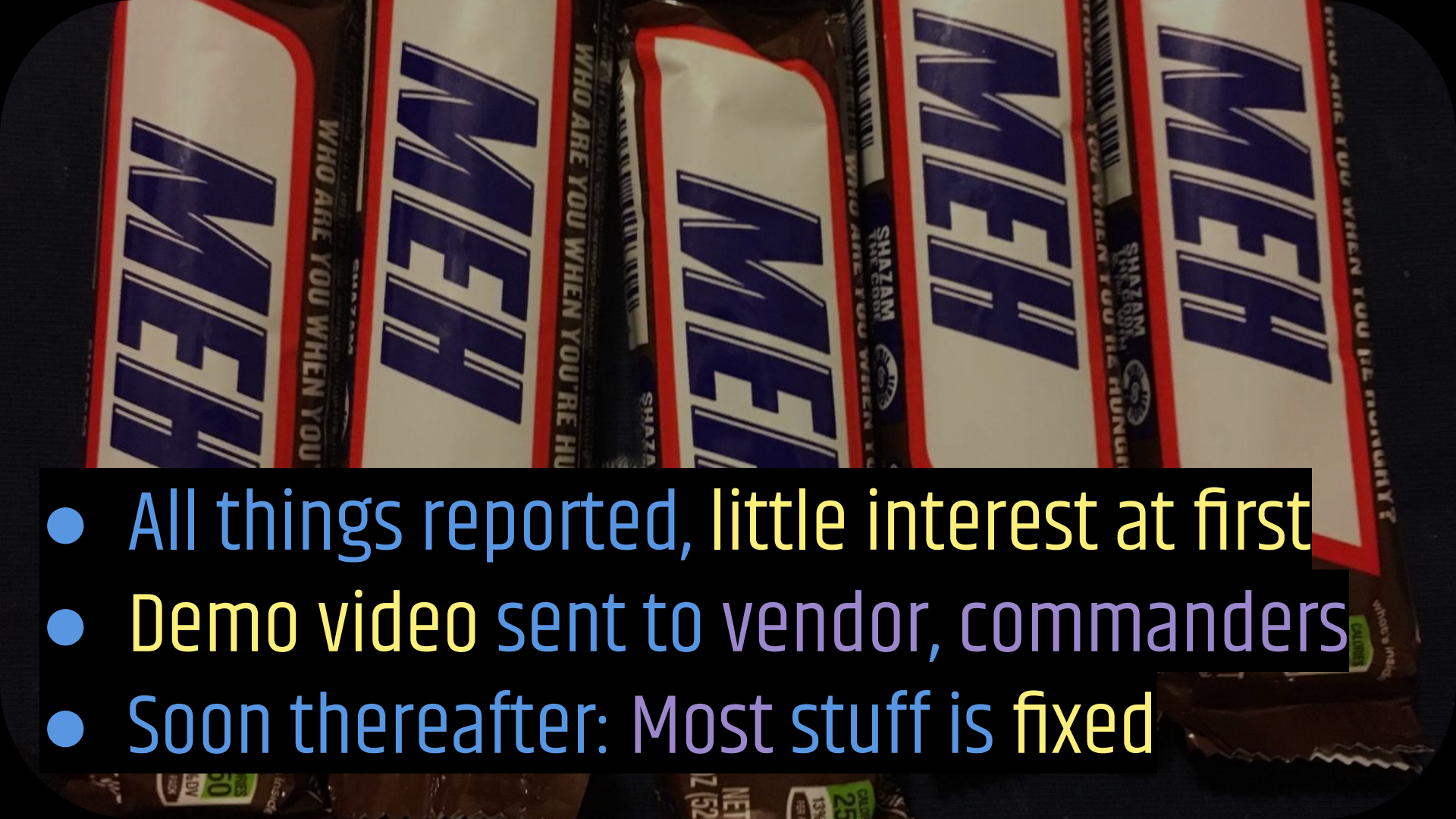
Unfinished Tasks

Complete Case	Case #U201800114 - ABUSE : ABUSE OR NEGLECT	
Complete Case	Case #IA201800113 - 911 : 911 HANGUP CALL	
Complete Case	Case #U201800083 - THEFT : THEFT	Due 02/28/18 11:31
Investigative Lead Assigned	#IL1800009, Lead Reported By	
Complete Case	Case #U201800057	
Complete Case	Case #U201800021	Due 02/01/18 14:31
Complete Case	Case #U201700027 - RIOT : RIOT - RIOT - CIVIL DISTURBANCE	
Case Kicked Back	Case #U201700027 - RIOT : RIOT - RIOT - CIVIL DISTURBANCE	
Complete Case	Case #P201800002	
Complete Case	Case #P201800001	
Complete Case	Case #U201700028 - ASSA : ASSA - ASSAULT - GENERIC	
Complete Case	Case #P201700026	
Investigative Case Review	Case #U201700019	
Complete Case	Case #U201700020	
Complete Case	Case #U201700015	
Approve Case	Case #P201700002 - VEHSTLN : Stolen Vehicle	
Complete Case	Case #P201700001 - ASSAULT : Assault	
Complete Case	Case #P201700004 - VEHSTLN : Stolen Vehicle	
Complete Case	Case #U201700008	
Approve Case	Case #P201700003 - VEHSTLN : Stolen Vehicle	
Approve Case	Case #P201700005 - VEHSTLN : Stolen Vehicle	
Approve Case	Case #P201700004 - VEHSTLN : Stolen Vehicle	

Menu

- [Main Menu](#)
- [Tasks](#)
- [Instant Messaging](#)
- [Messages](#)
- [Notes](#)
- [Download Manager](#)
- [Change My Password](#)
- [Change My Dashboard](#)
- [Manage My Shortcuts](#)
- [Dark Color Scheme](#)
- [About](#)

[Dashboard](#)[Main Menu](#)[CFS Log](#)[Cases](#)[Property / Evidence](#)[Civil Processes](#)[Current Inmates](#)[Reports](#)[System Admin](#)[Sign Out](#)

- 
- A row of five Meeth candy bars is shown, slightly out of focus. The packaging is white with a red border and features the word 'MEETH' in large, bold, blue letters. Below the name, the text 'SHAZAM' and 'WHO ARE YOU WHEN YOU'RE HUNGRY?' is visible. The bars are arranged horizontally across the top half of the image.
- All things reported, little interest at first
 - Demo video sent to vendor, commanders
 - Soon thereafter: Most stuff is fixed

**DON'T
PANIC**






C: Who is your (C)ISO? Who is in charge?

R: We can't tell you...

C: **AUDIT** your software! Shouldn't be on the customer to do it.

R: Someday...maybe

The End ?

A slice of Swiss cheese is in the foreground, and a man in a white lab coat is in the background, looking stressed with his hands on his head.

NICHE software used by **local.govs** needs
AppSec **TLC** like everything else





#BlueLeaks

Hack Brief: Anonymous Stole and Leaked a Megatrove of Police

Do
The so

Feds are treating BlueLeaks organization as 'a criminal hacker group,' documents show

The group says it's not involved in hacking

By [Ali Winston](#) | Aug 13, 2020, 9:53am EDT



HACK OF 251 LAW ENFORCEMENT WEBSITES EXPOSES PERSONAL DATA OF 700,000 COPS

The BlueLeaks archive contains over 16 million rows of data, including emails, descriptions of alleged crimes, and detailed personal information.

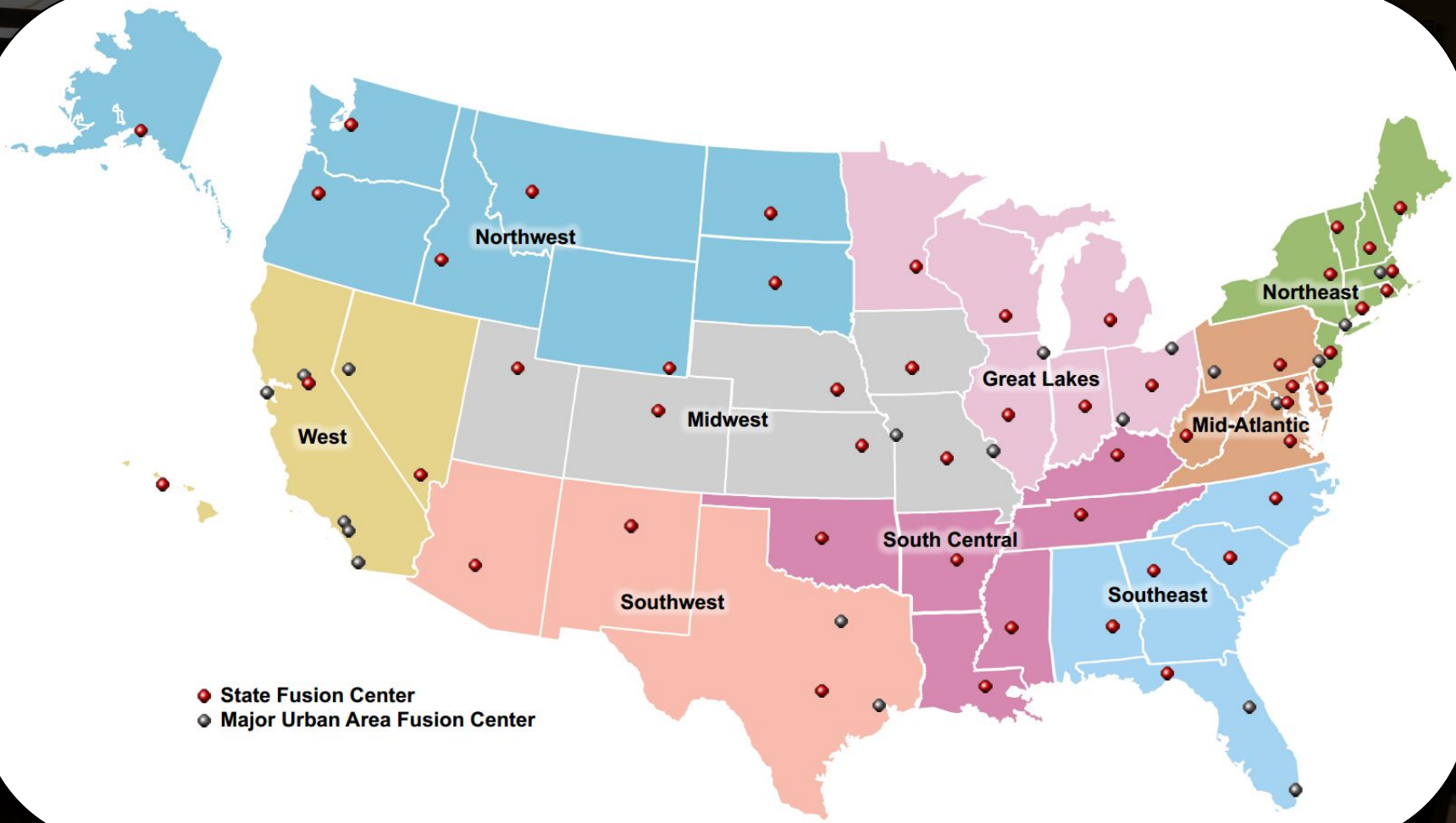


Micah Lee

July 15 2020, 3:00 p.m.

The Intercept_






- ◆ State Fusion Center
- Major Urban Area Fusion Center

kjiiiv.com





A man with grey hair, wearing a dark blue suit jacket over a white shirt, is shown from the chest up. He has a confused or questioning expression on his face. The background is a room filled with various pieces of electronic equipment and debris, suggesting a workshop or a place where things have been broken down. The lighting is somewhat dim, with a brighter area behind him, possibly a window or a light source. The overall tone is humorous or ironic.

 #SchittsCreek

I HAVE **NO** IDEA WHAT THAT MEANS



netsential

website developers

Home Website Developers Check Email

Websites that Generate Returns
Keeping you one step ahead of your competition

Netsential has the Experience - Our software is currently being used by Fortune 500 companies, financial institutions, small and medium sized businesses, associations, online publications, government agencies and schools throughout the United States.

Netsential Sites are Easy to Maintain - If you can cut and paste - you can maintain and update your website with Netsential's browser-based software.

Netsential Sites are Affordable & Effective - Websites are no longer labor-intensive and costly to maintain. Netsential provides flexible, customizable modules so you don't have to program everything from scratch.

Flexible, Customizable and Low Cost - Netsential builds sites with as much or as customer involvement that is desired. We train your staff to make updates - you are in control of your website. Netsential can host and manage the applications from its facilities and coordinate ongoing support, maintenance and upgrades. Netsential can customize or build modules to fit a specific market driven need.



[Click here to tell us "What you Need"](#)

© 1998-2020, Netsential.com, Inc.. All rights reserved.

[Send to a friend](#) - [Make a Request](#) - [Add to Favorites](#)

Netsential - Website Developers

12832 Willow Centre Drive, Suite C - Houston, Texas 77066
toll free: 877-993-6433 x108 - e-mail: sales@netsential.com

Info This is archived material from the Federal Bureau of Investigation (FBI) website. It may contain outdated information and links may no longer function.

2011 Director's Community Leadership Awards

Houston

Stephen Gartrell



The Houston Division is pleased to honor Mr. Stephen Gartrell, of Netsential, for his work designing and hosting websites that educate the public about crime and terrorism. Through his work, Mr. Gartrell has encouraged the public to work with law enforcement in an effort to reduce crime in the community.

FBI Director Recognizes Distinguished Community Leaders



In a ceremony at FBI Headquarters, Director Robert S. Mueller, III recognized the recipients of the 2011 Director's Community Leadership Award. These leaders, selected by their area FBI field office, have

demonstrated outstanding contributions to their local communities through service. The FBI is grateful for the work of each of these individuals and organizations on behalf of their communities.

"Whatever the motivation—an unfilled need, a tragic occurrence, a desire to give back—these are people who make things happen and enlist others in their cause," said Director Mueller. "They are activists who have earned their prestige through good works."

Recipients of the 2011 Director's Community Leadership Award include:

- Albany
- Albuquerque
- Anchorage
- Atlanta
- Baltimore
- Birmingham
- Boston
- Buffalo
- Charlotte
- Chicago
- Miami
- Milwaukee
- Minneapolis
- Mobile
- New Haven
- New Orleans
- New York
- Newark
- Norfolk
- Oklahoma City



OAKLAND '09
FERGUSON '14
BALTIMORE '15
MINNEAPOLIS '20

END
POLICE
VIOLENCE

ABOLISH
POLICE

END
POLICE
VIOLENCE

SERV
ABOLISH STOP
THE POLICE BLACK

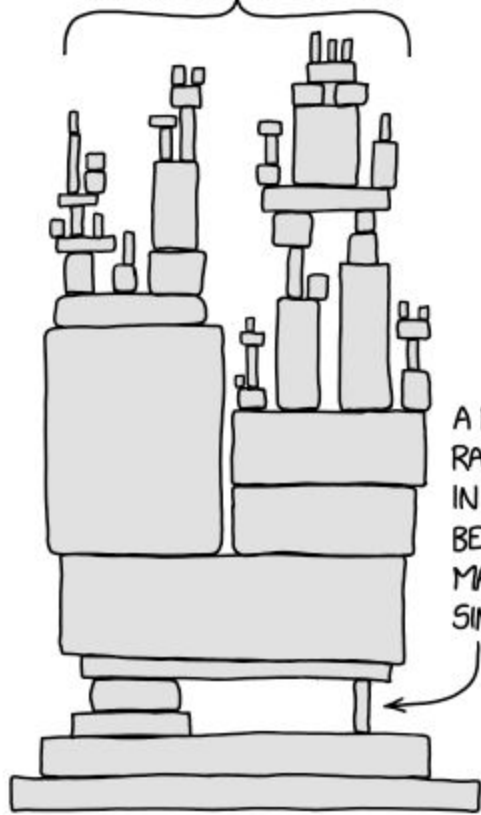
BLACK
LIVES
MATTER



~06/06/20



ALL MODERN DIGITAL INFRASTRUCTURE



A PROJECT SOME
RANDOM PERSON
IN NEBRASKA HAS
BEEN THANKLESSLY
MAINTAINING
SINCE 2003

SQL Injection in a Nutshell

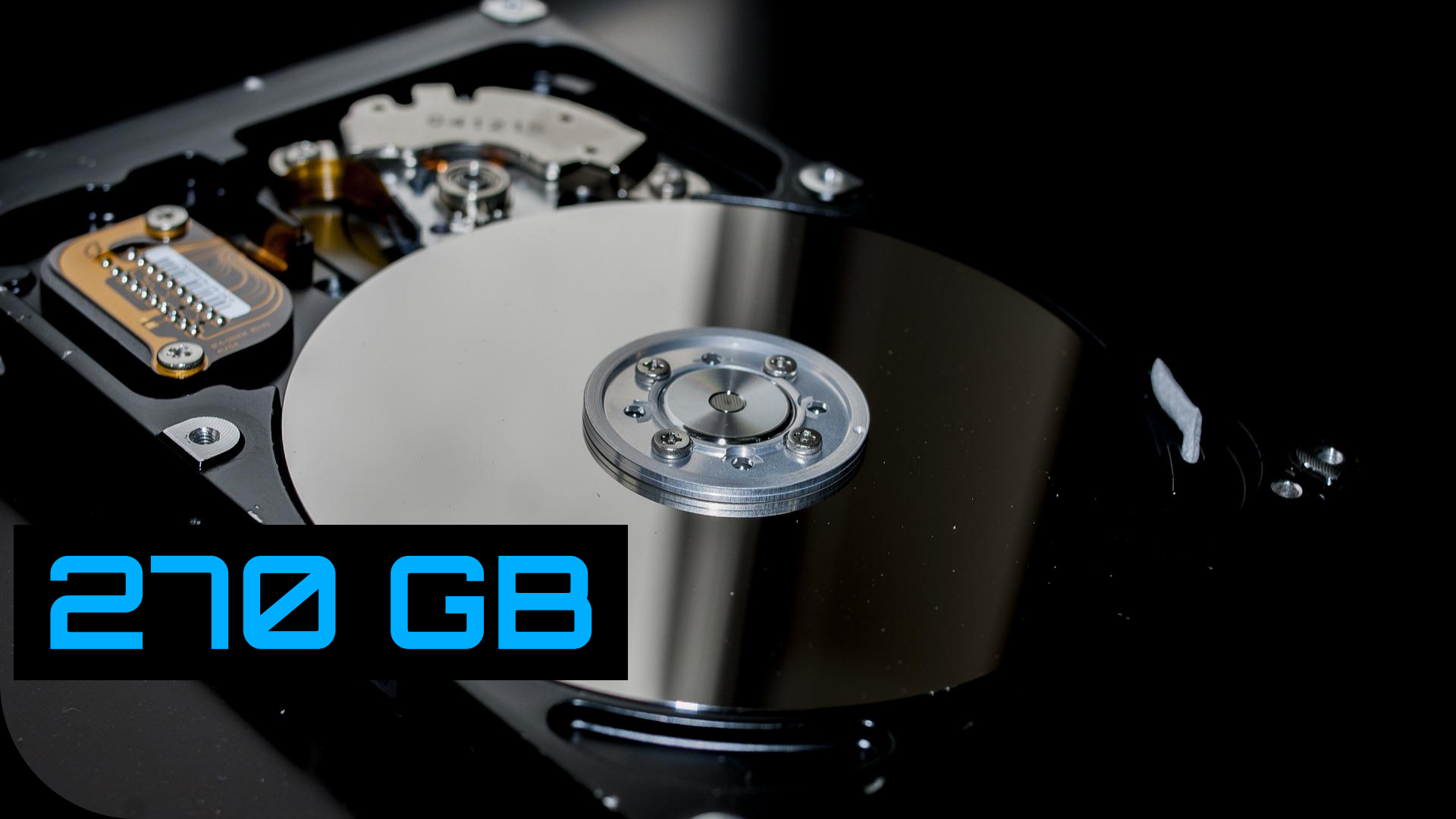
```
SELECT phoneNumber FROM employees WHERE lastName = 'Kava';  
712-555-1212
```

Department:

```
UPDATE dept SET name = 'Sheriff's Office' WHERE id = 42;  
*** SYNTAX ERROR NEAR: s Office' ***
```

Department:

```
UPDATE dept SET name = ''; DELETE FROM dept; --' WHERE id = 42;  
*** Deleted all rows from table "dept" ***
```



270 GB



Distributed Denial of Secrets

Transparency is Not A
Crime

**“Distributed Denial of Secrets is
501(c)(3) non-profit devoted to
enabling the free transmission of
data in the public interest.**

**We aim to avoid political, corporate
or personal leanings, to act as a
beacon of available information.”**



Distributed Denial of Secrets

@DDoSecrets



RELEASE: **#BlueLeaks** (269 GB)

Ten years of data from over 200 police departments, fusion centers and other law enforcement training and support resources. Among the hundreds of thousands of documents are police and FBI reports, bulletins, guides and more.

hunter.ddosecrets.com/datasets/102

10:05 PM · Jun 19, 2020 · [Twitter Web App](#)



5.2K Retweets **10.9K** Likes



1996 - 2020



1996 - 2020



Distributed
Denial
of
Secrets
Transparency is Not A
Crime



BlueLeaks ▾

Search in BlueLeaks



Datasets

Sign in

Leaks > BlueLeaks

Leaks

BlueLeaks

Ten years of data from over 200 police departments, fusion centers, and other law enforcement training and support resources, courtesy of Anonymous.

Publisher Distributed Denial of Secrets

Data URL data.ddosecrets.com

Manager Mxyzptk

Country United States

Last updated 06/19/2020

Overview

Documents 1m

People 292

Cross-reference

13

Types

Images	564,701
Documents	291,672
Tables	167,319
Web pages	102,445
Text files	28,594
Folders	15,751
Files	4,936
Packages	4,665
Workbooks	1,468
Videos	1,468

254

Countries

United States	70,481
Seychelles	4,265
Mexico	3,372
Honduras	1,785
Canada	1,520
Guatemala	976
Ireland	971
France	948
Syria	857
China	844

1m

Names

Netsential.com Inc	58,714
All Rights Reserved	45,591
AGENCY / CASE	14,015
D.L. State Male Female Driv...	13,690
First DOB:(mm/dd)	13,420
Cross Streets	12,197
Permission to Disseminate ...	11,771
St. Louis Intelligence Project...	11,348
Car Clouting	10,524
MIAC Intel	10,140



blueleaks



Top

Latest

People

Photos

Videos



· Jun 20



The FBI is watching all tweets regarding the protests, and sending them to your local police. [#BlueLeaks](#)

UNCLASSIFIED//FOUO



SITUATIONAL INFORMATION REPORT
FEDERAL BUREAU OF INVESTIGATION
Potential Activity Alert
LOS ANGELES DIVISION

Approved for Release: 29 May 2020

SIR Number: SIR-00334076587

(U//FOUO) Civil Unrest in Response to Death of George Floyd Threatens Law Enforcement Supporters' Safety, as of May 2020

SOURCE: (U) A documentary source.

(U) On 27 May 2020, an identified Twitter account dedicated to anarchist ideology and activity in the Long

276

8.9K

14.7K












<input type="checkbox"/>	Bolos BOLO	443
<input type="checkbox"/>	U) Outlook (U//FOUO	442
<input type="checkbox"/>	info@counterdrugtraining.com counterdrug...	441
<input type="checkbox"/>	Clothing / Shoes Value of Goods Taken	440
<input type="checkbox"/>	Cybersecurity and Infrastructure Security ...	440
<input type="checkbox"/>	US Customs	440
<input type="checkbox"/>	Wall Street Journal	439
<input type="checkbox"/>	ADDITIONAL FACTORS K-9	438
<input checked="" type="checkbox"/>	George Floyd	438
<input type="checkbox"/>	Justice Department	438
<input type="checkbox"/>	Perpetrator Information Center	437
<input type="checkbox"/>	Larry Mack	436
<input type="checkbox"/>	Leticia False Compartment	436
<input type="checkbox"/>	Royal Canadian Mounted Police	436
<input type="checkbox"/>	John McCoy	435
<input type="checkbox"/>	Suspicious Ac	434
<input type="checkbox"/>	Updated Informa	433
<input type="checkbox"/>	Prophet Muhammad	431



Search > Found 2,936 results

Export

▶ **Datasets** 1 selected▶ **Types**▶ **Countries**▶ **Languages**▶ **E-Mails**▶ **Phone numbers**▶ **Names**▶ **Addresses**

Name	Dataset
 FIR CA-0006-18.pdf TOP SECRET/JWICS...	 BlueLeaks
 DEA-SDO-BUL-008-1... Top Secret...	 BlueLeaks
 UFOUO DHS FIR DC-... TOP SECRET/JWICS...	 BlueLeaks
 DEA-SDO-BUL-008-1... Top Secret...	 BlueLeaks
 5-9-13 Officer Safety... Top Secret under Executive Order 12958...	 BlueLeaks



EmailBuilder.csv

Title unknown

File name EmailBuilder.csv

MIME type text/html

Folder counterdrugtraining

Checksum 1bca7971be82cc5eae60fe52a88fe1a2d81c87a4

File size 6 MB

Number of rows 1,978

Dataset



Ten years of data from over 200 police departments, fusion centers, and other law enforcement training and support resources, courtesy of...

1m entries

View Mentions

	Column 1	Column 2	Column 3	Column 4	Column 5	Column 6	Column 7	Column 8	Col
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									
13									
14									
15									
16									
17									
18									
19									
20									
21									
22									
23									
24									
25									
26									
27									
28									
29									
30									
31									
32									
33									
34									
35									

- **Intel Bulletins**
- **Shared Files, Emails, Reports**
- **User Registrations**
- **Training Registrations**
- **Survey Responses**

TRAINING

Orange County License Plate Reader Program



The purpose of this training bulletin is to provide Orange County law enforcement officers with a brief tutorial on the new license plate reader initiative, which was purchased under the US Department of Homeland Security's Anaheim/Santa Urban Area Security Initiative (UASI) grant program. The Automated License Plate Reader (ALPR) technology provided by Vigilant Video has deployed to all Orange County law enforcement agencies in the Operational Area. To access the ALPR program, law enforcement personnel must contact their agency representative for training and log-in information. In addition, users of the ALPR system will be required to follow agency policies involving the system, which may vary amongst agencies.

OVERVIEW

The standard configuration of the ALPR system on a patrol vehicle is a set of two forward facing cameras and two rear facing cameras mounted on the vehicle. Mounted cameras can capture two types of images, standard color images during daylight and infrared (IR) images using IR light to reflect an image of the license plate. In both instances, only the license plate image is captured. However, older style license plates (California Blue and Black) may not successfully be captured by ALPR since the older versions are non-reflective.

Stolen Vehicle Alert



Exact match



NBR LPR Number

NBR352

Detected Number

NBR352

Rear Camera
09/19/2009 14:52:51
30.651296
-93.896589

State ID: California
 Order ID: CVRNBR352032309
 Status: Stolen Vehicle
 Source: NCC: Data File
 Registered: Jason Kodals
 Date of Order: 3-23-09
 Comments: Armed & Dangerous

Powered By:





NCRIC

Northern California Regional
Intelligence Center

Fusing Information, Talent And Training For A Safer Society.

NCRIC Cyber Alert Bulletin (CyAB) – Officer Safety

(U) Scope: The CyAB provides immediate updates and analysis on cyber trends and threats of interest to NCRIC Partners. Information within CyABs may often include raw reporting that has not been fully evaluated, and is provided for situational awareness only.

2 February 2017

(U//FOUO) iPhone App May Expose Officer Phones

(U//LES) In late January, a local law enforcement officer working at a large event received a message on his iPhone apparently from an attendee standing nearby. The message was likely delivered using the AirDrop application and may have been an attempt to compromise the officer's phone with a malicious file. Law enforcement officers are encouraged to keep AirDrop turned off, especially when working at large events.

- (U) AirDrop is a file transfer application found on Apple devices that uses Bluetooth to establish a secure connection between two Apple devices in order to share an image, video, or other file.
- (U//FOUO) When AirDrop is enabled, users can select other Apple devices with AirDrop enabled within a 30 foot radius and send files. If the device name includes the officer's name or agency, the app displays this information to anyone also using AirDrop.
- (U) Malicious actors can technically infect a device by sending a malicious link or image via AirDrop. A user must accept and then click on the message to enable the malicious activity.

(U//FOUO) The NCRIC has no additional reporting of similar events. Open source reporting does not show any discussion of the tactic being advocated to compromise iPhones. AirDrop has been used to send prank



(U) Example of AirDrop message

- **Full Names**
- **Email Addresses**
- **Postal Addresses**
- **Phone Numbers**
- **Identity Numbers (SOC, OLN)**
- **IP Addresses**
- **Passwords**



µTorrent[®]



**NATIONAL SITUATIONAL INFORMATION REPORT
FEDERAL BUREAU OF INVESTIGATION**

Activity Alert
CRIMINAL INVESTIGATIVE DIVISION
SACRAMENTO DIVISION

(U) Approved for Release:

(U) SIR Number: NSIR-00328015082

(U//FOUO) Unidentified Darknet User(s) Sent Personally Identifiable Information of Federal Law Enforcement Officials to Darknet Website Administrators

(U) Source: An anonymous tip reported to a monitored FBI e-mail account.

(U//LES) The purpose of this National Situational Information Report is to advise law enforcement personnel and public safety officials about threats to life by unidentified Darknet user(s) using the name DEEPSTATE.

(U) LAW ENFORCEMENT SENSITIVE: The information marked (U//LES) in this document is the property of the Federal Bureau of Investigation and may be distributed within the federal government (and its contractors), US intelligence, law enforcement, public safety, or protection officials and individuals with a need to know. Distribution beyond these entities without FBI authorization is prohibited. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access. Information bearing the LES caveat may not be used in legal proceedings without first receiving authorization from the originating agency. Recipients are prohibited from subsequently posting the information marked LES on a website on an unclassified network without first obtaining FBI approval.

(U) Warning: This is an information report, not finally evaluated intelligence. It is being shared for informational purposes but has not been fully evaluated, integrated with other information, interpreted or analyzed. Receiving agencies are requested not to take action based on this raw reporting without prior coordination with the FBI.

(U) Note: This product reflects the views of the SACRAMENTO DIVISION and CRIMINAL INVESTIGATIVE DIVISION.



Emerging Intelligence Report

(U) PREPARED BY FBI WASHINGTON FIELD OFFICE

9 MARCH 2020
FBI EIR154 20200309

(U//LES) Darknet Market Actors Likely Convert Illicit Bitcoin to Monero Using MorphToken Cryptocurrency Exchange, Impeding Law Enforcement Tracing Efforts

(U) This document is classified: Unclassified//Law Enforcement Sensitive.
(U) EIR template approval for fiscal year 2020, as of 1 October 2019.
(U) LAW ENFORCEMENT SENSITIVE: The information marked (U//LES) in this document is the property of the Federal Bureau of Investigation and may be distributed within the federal government (and its contractors), U.S. intelligence, law enforcement, public safety or protection officials, and individuals with a need to know. Distribution beyond these entities without FBI authorization is prohibited. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access. Information bearing the LES caveat may not be used in legal proceedings without first receiving authorization from the originating agency. Recipients are prohibited from subsequently posting the information marked LES on a website on an unclassified network without first obtaining FBI approval.

(U//LES) The FBI assesses Darknet Market (DNM) actors likely⁴ convert illicitly obtained Bitcoin into anonymity-enhanced cryptocurrency (AEC)⁵ Monero using the MorphToken⁶ cryptocurrency exchange, impeding law enforcement's ability to trace the destination of the proceeds. This assessment is made with high confidence,⁴ based on FBI investigations, blockchain analysis,² use of proprietary software, information from MorphToken, and information obtained from Darknet sites and forums that cater to DNM actors. The FBI assumes the DNM actors' intent of converting cryptocurrencies is not to diversify their cryptocurrency portfolio. If this assumption is incorrect, it could mean DNM actors are not adopting AECs for operational security purposes and the FBI's confidence in the assessment would decrease. The FBI bases this assessment on reporting of DNM actors converting Bitcoin to Monero, the availability of information on the inability to trace Monero, and the means of acquiring it without providing user information.

- (U//FOUO) As of January 2020, DNM actors associated with Apollon DNM sent at least 11 bitcoin (worth approximately \$80,000) to MorphToken to convert to Monero between December 2019 and January 2020, according to a proprietary software tool that analyzes financial

transactions of the Bitcoin blockchain and use of MorphToken's automated programming interface (API).⁷

- (U//FOUO) As of October 2019, FBI analysis revealed commission fees from Bitcoin transactions conducted on Cryptonia DNM between May and September 2019 were sent to addresses associated with MorphToken, based on an FBI investigation and blockchain analysis. All Bitcoin transactions able to be queried using MorphToken's API were converted to Monero.^{2,3,4}
- (U//LES) As of November 2019, the FBI identified at least four DNM vendors that sent Bitcoin drug sale proceeds to MorphToken, based on FBI investigations, open source blockchain tracing, and use of a proprietary software tool that analyzes financial transactions of the Bitcoin blockchain.^{5,6,7,8}
- (U) As of January 2020, sites and forums that cater to DNM actors provided guides to obtain and use Monero.^{9,10} Many user posts on the topic discussed the use of

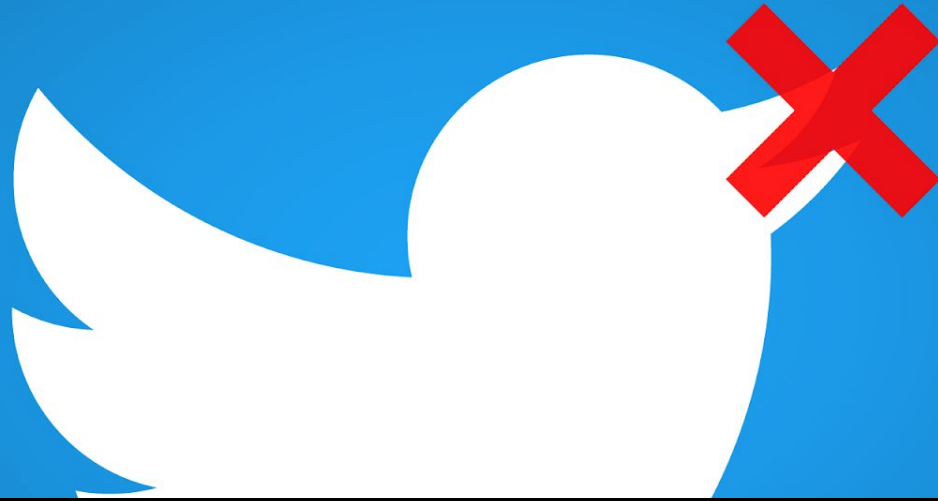
⁴ (U) See Appendix A: Expressions of Likelihood.

⁵ (U//FOUO) Analyst Note: AECs, unlike Bitcoin, do not publish fully public records of all transactions. This prevents law enforcement from exploiting those records to follow the flow of value through blockchain analysis, a key tool in de-anonymizing DNM actors.

⁶ (U) MorphToken is a fee-based cryptocurrency exchange service. Customers select which cryptocurrency to send and receive from MorphToken. MorphToken operates without user accounts and does not collect user information.

⁷ (U) See Appendix B: Confidence in Assessments and Judgments Based on a Body of Information.

⁸ (U) Analyst Note: A blockchain is a digital public ledger that records online cryptocurrency transactions, including those in Bitcoin. Open source tools enable the analysis of these transactions to identify movement of funds.



2020-06-23



Emma Best   Demon Hacker

@NatSecGeek

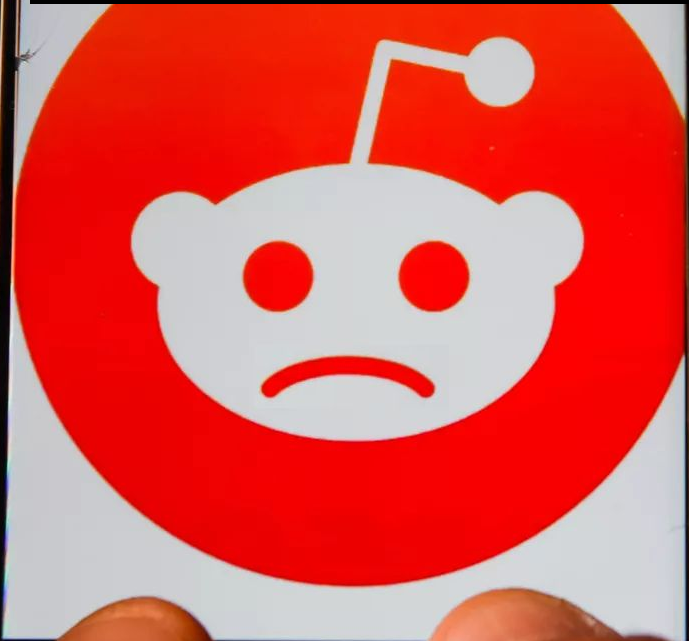


We have received official confirmation that [#DDoSecrets](#)' primary public download server was seized by German authorities (Department of Public Prosecution Zwickau file number AZ 210 AR 396/20)

We are working to obtain additional information, but presume it is re [#BlueLeaks](#).

10:08 AM · Jul 7, 2020 · Twitter for Android

2020-07-09





If your seeding the [#BlueLeaks](#) data dump I'd highly suggest putting a copy on a ps3 or ps4 as it won't be confiscated when a raid happens

4:20 PM · Jul 10, 2020 · [Twitter for iPhone](#)

BlueLeaks

BlueLeaks

Datasets Sign in

Leaks
BlueLeaks

BlueLeaks

Ten years of data from over 200 police departments, fusion centers, and other law enforcement training and support resources, courtesy of Anonymous.

Publisher: [Distributed Denial of Secrets](#)

13

Types

254

Countries

1m

Names

Images	504,701	United States	70,401	NetScout.com Inc	58,714
Documents	291,872	Seychelles	4,205	All Rights Reserved	40,591
Tables	142,319	Mexico	3,392	AGENCY / CASE	14,201
Web pages	102,445	Honduras	1,705	DL State Male Female Driver/Passenger	13,890

BLUELEAKS

Situational awareness bulletins, training materials and fusion center reports for more than 200 law enforcement agencies. dated August 1996 to June 2020.

DATASET DETAILS

COUNTRY United States

TYPE Hack

SOURCE Anonymous

FILE SIZE 269 GB

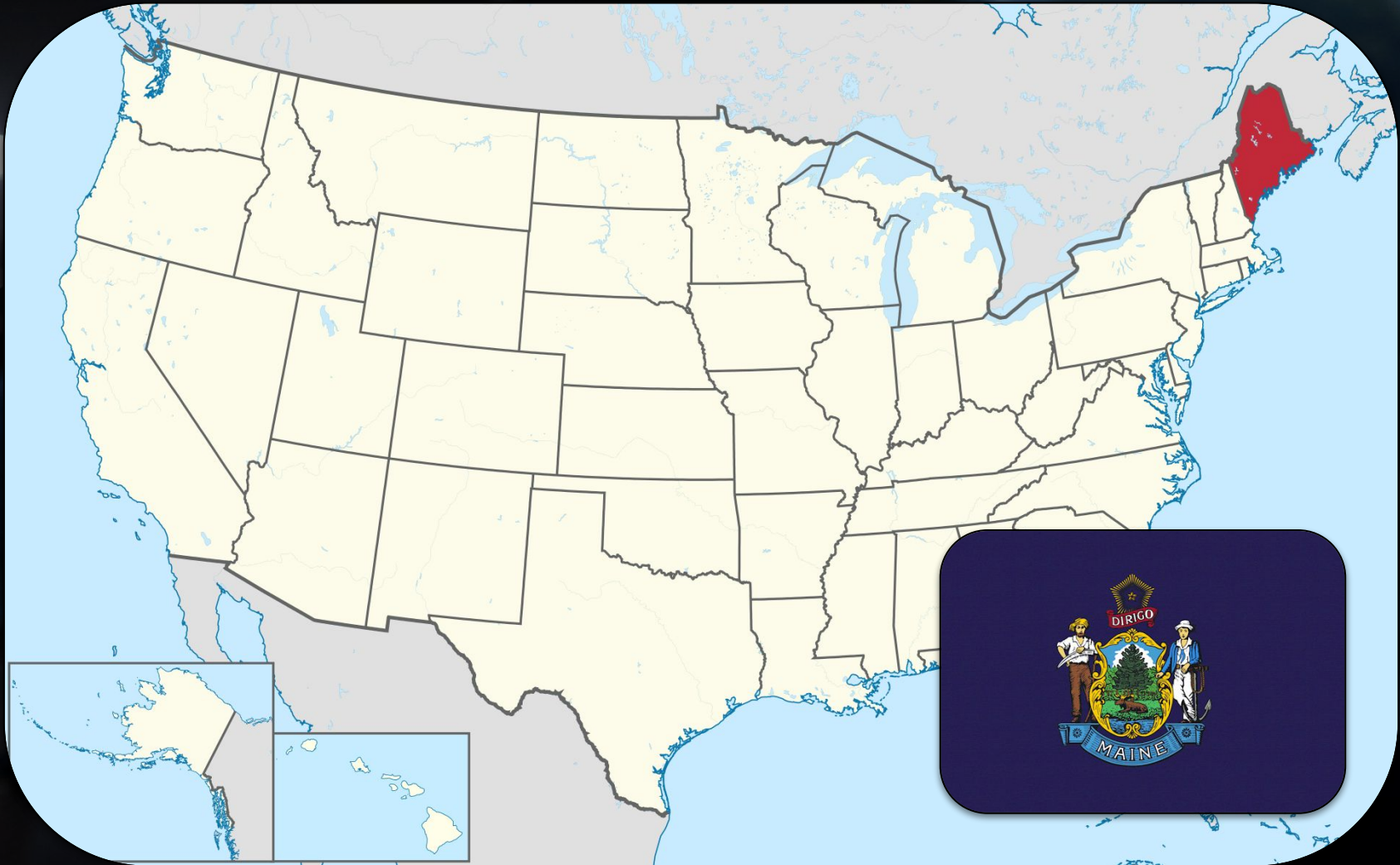
DOWNLOADS (How to Download)

MAGNET [Link](#)

TORRENT

IPFS Qmd [REDACTED] VIA







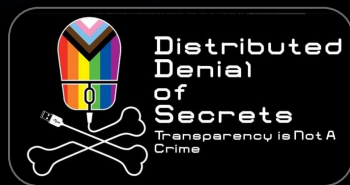
Maine Information Analysis Center

**** ATTENTION: NOTICE OF DATABASE BREACH ****

Consistent with Title 10, Chapter 210-B of the Maine Revised Statutes, this notice is being posted to notify the general public information that a database utilized by the Maine Information & Analysis Center (“MIAC”) was unlawfully accessed in June 2020. If you have reason to think you have been affected by this breach, please contact LT Michael P. Johnston, Director of the MIAC, at

“June 24, Maine Department of Public Safety commissioner Michael Saushuck faced questions about the activities of their fusion center at a legislative hearing...

The Maine fusion center was found to be sending their reports about political activists to ... large corporations and lobbyists.”



Mainer

NEWS, VIEWS, HAPPINESS PURSUED



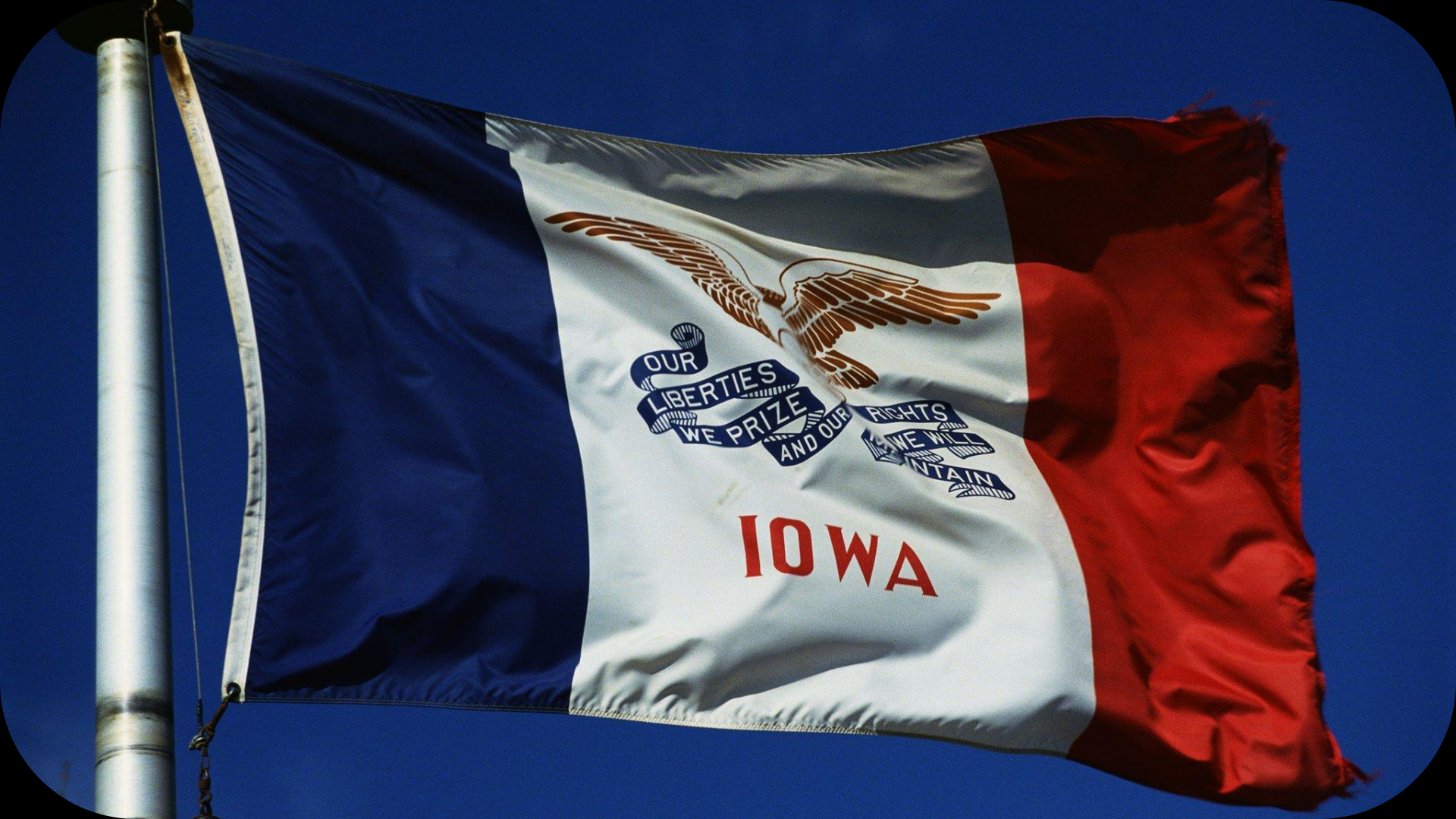
BILL WOULD GUT MAINE SPY AGENCY

DHS “Fusion Center” under fire for spreading far-right conspiracies, pushing racially and politically biased intel

by NATHAN BERNARD | Mar 8, 2021

251 WEBSITES

	A	B	C	D	E	F
1	BlueLeaks Directory	Website	Description	City	State	Size (MiB)
2	211sfbay	211sfbay.org	San Francisco Bay Area Robbery Investigators	San Francisco	CA	2,806.77
3	acprlea	acprlea.org	Amarillo College Panhandle Regional Law Enforcement Academy		TX	215.76
4	actcaz	new.actcaz.org	Arizona Counter Terrorism Information Center		AZ	64.41
5	akorca	akorca.org	Alaska Organized Retail Crime Alliance (AKORCA)		AK	747.25
6	alabamafusioncenter	alabamafusioncenter.org	Alabama Fusion Center	Montgomery	AL	571.45
7	alabamalecc	alabamalecc.org	Alabama LECC	Orange Beach	AL	24.86
8	alertmidsouth	alertmidsouth.org	Alert Mid-South Organized Retail Crime Alliance			747.22
9	aorca	aorca.org	Arkansas Organized Retail Crime Association		AR	121.70
10	arictexas	new.arictexas.org	Austin Regional Intelligence Center (ARIC)	Austin	TX	9,530.08
11	atlantahidta	www.achidta.org	Atlanta Carolinas HIDTA		GA	1,387.01
12	attackwa	attackwa.org	ATTACK WA		WA	204.68
13	azhidta	www.azhidta.org	Welcome to Arizona HIDTA	Chandler	AZ	5,644.75
14	azorca	azorca.org	Arizona Organized Retail Crime Association (AZORCA)		AZ	1,658.24
15	bostonbric	survey.bostonbric.org	Boston Regional Intelligence Center		MA	1,003.72
16	burlingamepolice	coplink.burlingamepolice.info	Burlingame PD	Burlingame	CA	1,180.36
17	cal-orca	cal-orca.org	California Organized Retail Crimes Association		CA	1,962.58
18	calema	caloes.org	California Governor's Office of Emergency Services - Training and Exercise	Mather	CA	488.18
19	calstas		Milwaukee High Intensity Drug Trafficking Area (HIDTA)			2,679.36
20	cbaghidta	sdhidta.org	San Diego - Imperial HIDTA	San Diego	CA	206.14
21	ccroc	ccroc.us	Cook County Regional Organized Crime Task Force (CCROC)		IL	377.35
22	chicagoheat	chicagoheat.org	Chicago Heat	Chicago	IL	820.11
23	chicagolandfsg	chicagolandfsg.org	Chicagoland Financial Security Group		IL	118.19
24	ciacco	new.reportstreetracing.com	Report Colorado Street Racing		CO	2,919.32
25	cnoa3	cnoaregionaltraining.com	California Narcotic Officers Association	Santa Clarita	CA	814.66
26	cnoatraining	site.cnoatraining.org	California Narcotic Officers Association	Los Angeles	CA	102.71
27	cnyorca	new.nyorca.org	New York Organized Retail Crime Alliance (NYORCA)		NY	336.67
28	coorca	COORCA.org	Colorado Organized Retail Crime Alliance (COORCA)		CO	3,202.97
29	corca	corca.org	Carolinas Organized Retail Crime Alliance			1,242.39
30	counterdrugtraining	new.counterdrugtraining.com	Midwest Counterdrug Training Center	JOHNSTON	IA	5,118.84



OUR
LIBERTIES
WE PRIZE
AND OUR RIGHTS
WE WILL
MAINTAIN

IOWA





35,275 / 247,354 (14.3%)

Password Hashes Cracked
(Cheaply in Three Days)



1999 - 2020

The background of the page is a dark, circular image of the Iowa State flag. The flag features a white field with a red eagle in the center, a red vertical stripe on the right, and a blue vertical stripe on the left. The word "IOWA" is printed in red on the white field. A white horizontal bar is overlaid across the center of the image.

FOR OFFICIAL USE ONLY

This document contains information EXEMPT FROM MANDATORY DISCLOSURE UNDER THE FREEDOM OF INFORMATION ACT (FOIA)









**THE
END
IS
NIGH**

CONCLUSION



PRIVATE SECTOR

PUBLIC SECTOR

















LOW | MEDIUM | HIGH

TRUST





???



I'm doing my part!

???







<https://forensic.coffee>
[akava\[at\]sheriff\[dit\]pottcounty-ia.gov](mailto:akava[at]sheriff[dit]pottcounty-ia.gov)





<https://forensic.coffee>
[akava\[at\]sheriff\[dit\]pottcounty-ia.gov](mailto:akava[at]sheriff[dit]pottcounty-ia.gov)