

Social Media Investigations: Gun Recovery Unit Edition



Detective Sergeant [REDACTED] JTTF



E1319

Attention Gun Recovery Unit!!!

I am teaching this class as a supplemental to your current knowledge base of social media. It was designed using best practices acquired over my time doing social media investigations. Things we are going to cover today:

- Personal Use of the Social Media
- Legal Process Pitfalls (and how to avoid them)
- Online Covert Accounts



E1320

Personal Use of Social Media

We are getting crushed by Internal Affairs and Citizen Complaints on how we conduct ourselves in our personal lives. Understand that every conversation you make could be screen captured and taken out of context.



E1322

Personal Use of Social Media

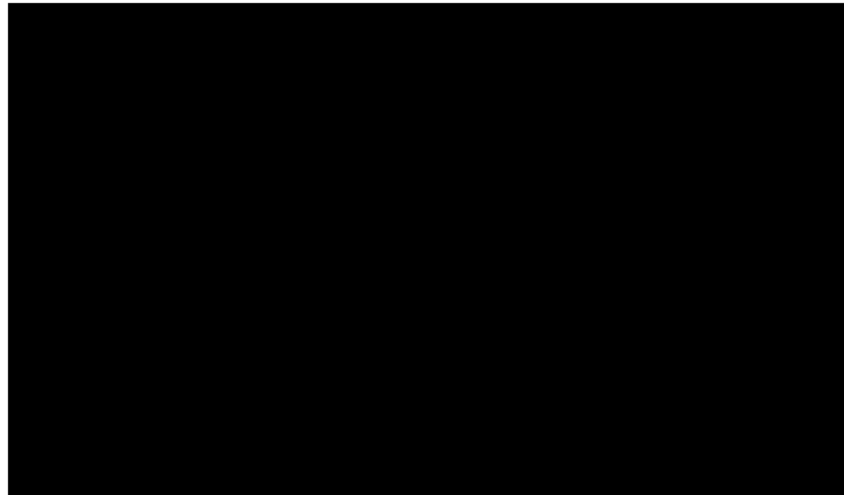
There is no such thing as a secret group on social media. Be cognizant that anything you say even in jest can be taken out of context and exploited.



E1323

Personal Use of Social Media

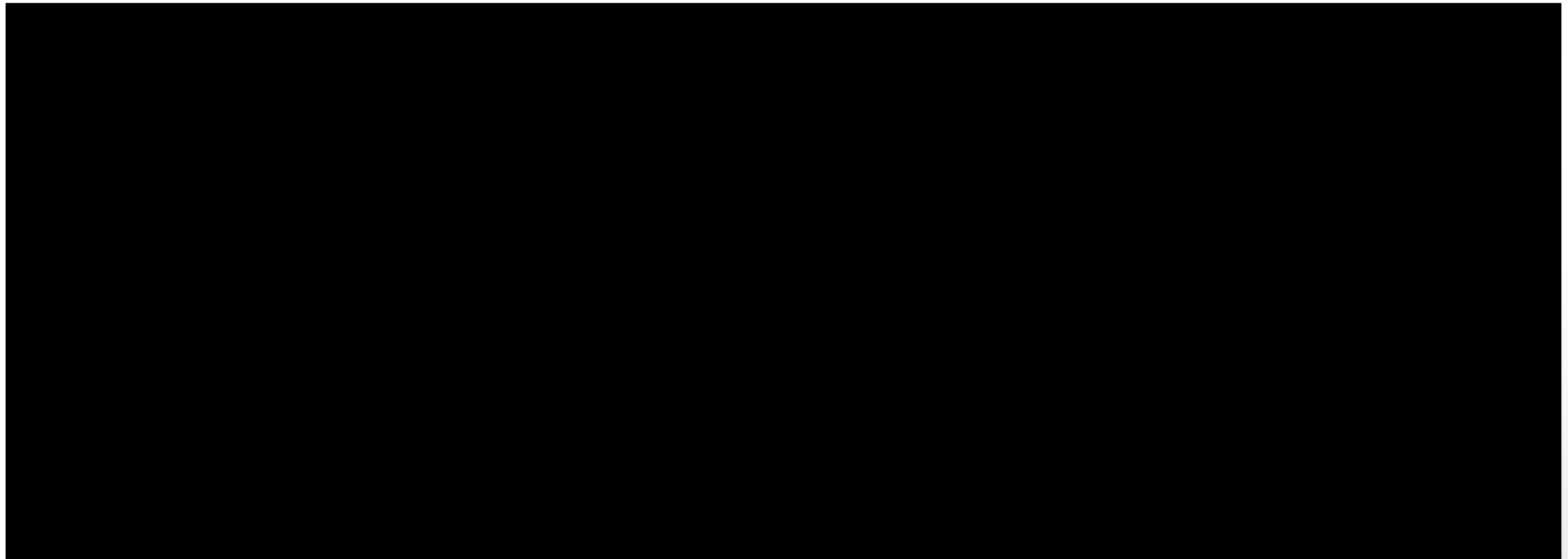
Path of least resistance: Do not use social media while on duty.



E1324

Personal Use of Social Media

Understand as a member of the Metropolitan Police Department, any comments you make reflect on the Department. Context and humor are subjective.



E1325

Personal Use of Social Media

This includes blogs and media outlets.

BLOOMINGDALE, CRIME, TRUXTON CIRCLE

“After the suspect refused to follow numerous commands, two officers discharged their firearms”

[Prince Of Petworth](#) February 5, 2021 at 9:30am



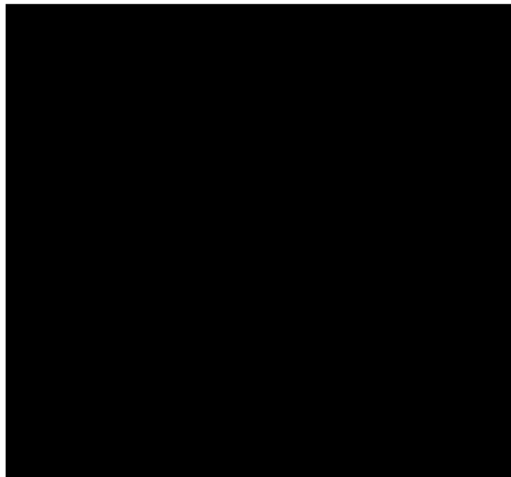
E1326

MPD 8

Social Media Investigations: Gun Recovery Unit Edition Presentation

Personal Use of Social Media

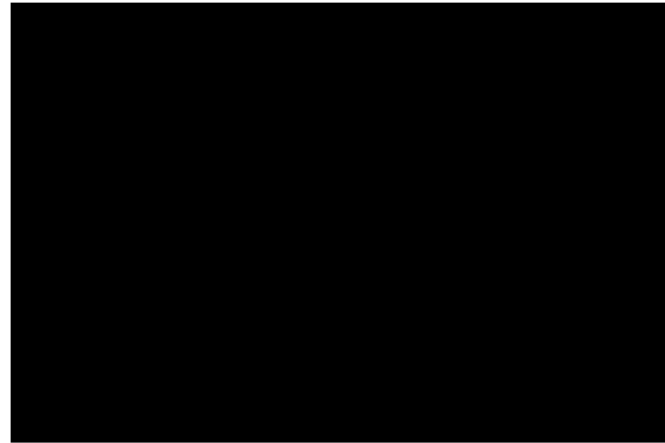
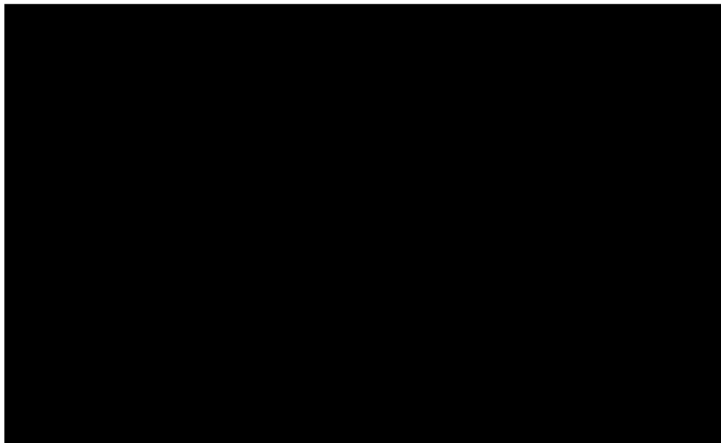
Practice operational security in your personal life



E1327

Personal Use of Social Media

Do not post any work-related content that involves crime scenes, tactics, or investigations.



E1328

Personal Use of Social Media

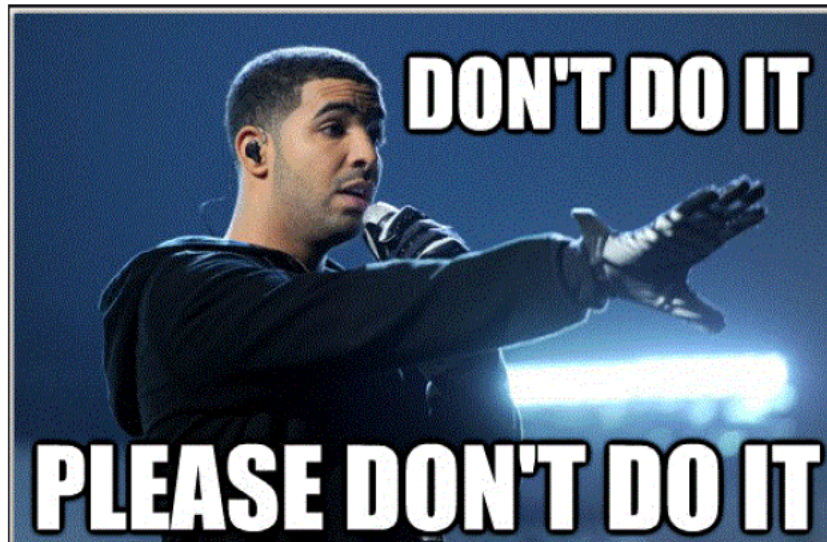
Don't use personal accounts or private workspace for investigations



E1329

Media Contacts through Social Media

Defer to the PIO



E1330

Legal Process for Social Media



E1331

Legal Process and Getting What you Want

- There are three types of legal process that an Investigator will find themselves issuing in an investigation. Those are:
 - 1) Preservation Letters
 - 2) Search Warrants
 - 3) Emergency Disclosures



E1332

Legal Process and Getting What you Want

Preservation Requests

[↑ 18 U.S.C. §2703\(f\)\(1\)](#) states: “A provider of wire or electronic communication service or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.”

- Good for at least 90 days
- Retroactive
- Customer not notified



E1333

Legal Process and Getting What you Want

Preservation Requests

Case	Reference	Status	Account	Request Type	Date Requested
[Redacted]					

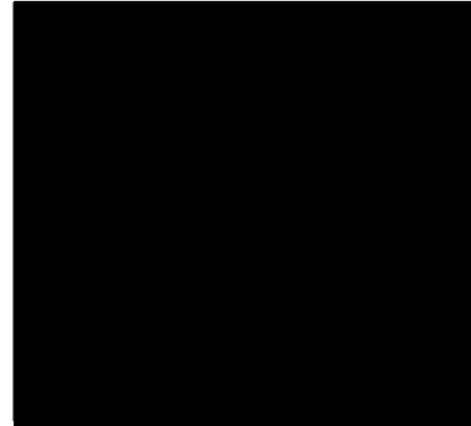


Homeland Security Bureau
Intelligence Division

300 Indiana Avenue, Suite 2000, NW, Washington D.C., 20011 (202) 734-1424 FAX: (202) 727-6518

July 26, 2017

Twitter, Inc.
1355 Market Street, Suite 900
San Francisco, CA 94103

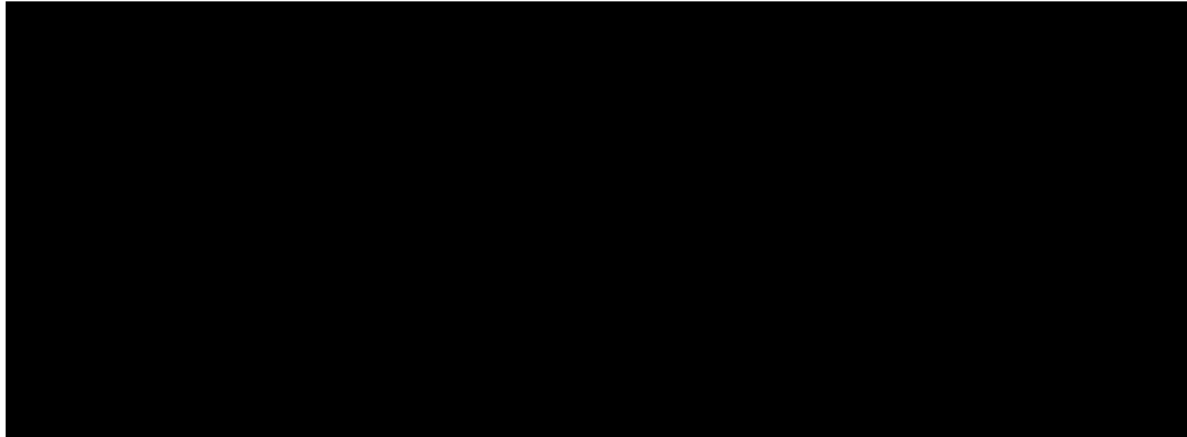


E1334

MPD 16

Legal Process and Getting What you Want

Preservation Requests

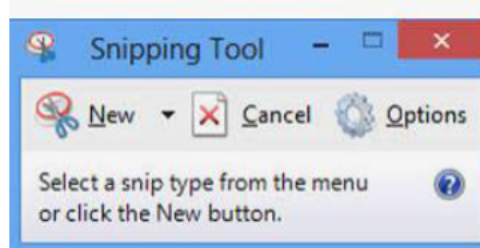


E1335

Legal Process and Getting What you Want

Preservation Requests

Snipping Tool

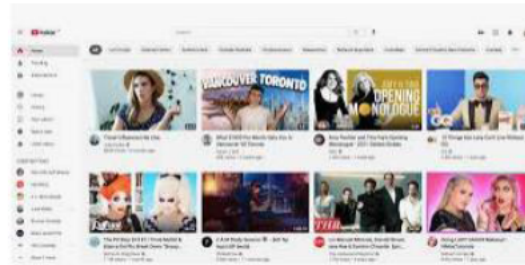


E1336

Legal Process and Getting What you Want

Preservation Requests

Screen Recorders through phone/PC and MP4 downloads through source



E1337

Legal Process and Getting What you Want

Search Warrants



E1338

Legal Process and Getting What you Want

At this point in your career, I am not going to walk you through the warrant process. What I can do is highlight recurring issues with social media search warrants. I have made all of these mistakes myself.



E1339

MPD 21

Social Media Investigations: Gun Recovery Unit Edition Presentation

Legal Process and Getting What you Want

1) Training and Experience

If you are using the phrase “training and experience,” you need to be able to articulate what training and experience you have beyond the Maurice J Turner Institute of Police Science.

Places to get Training

- Private Sector offerings
- Community College
- Government-affiliated offerings (NCTC, HIDTA)

If you want the training, hunt for it. If the Department won't grant you Admin Leave, take personal leave. INVEST IN YOURSELF.

E1340



Legal Process and Getting What you Want

1) Training and Experience

If you are using the phrase “training and experience,” you need to be able to articulate what training and experience you have beyond the Maurice J Turner Institute of Police Science.

Articulating Experience

We all have life experience. In addition to on-the-job experience, your personal life plays a role in justifying that your training and experience



E1341



MPD 23

Social Media Investigations: Gun Recovery Unit Edition Presentation

Legal Process and Getting What you Want

2) “I know statements”

How do you know? Is it just template language or do you actually know?

One of the reasons I create social media accounts for familiarization is to understand how communication works. I know people communicate through direct messages because I have my own account. I know the data that is collected because I read the User Agreement when I created the account.



E1342

Legal Process and Getting What you Want

3) Language is important

If slang is used to describe a firearm, be prepared to discuss how you know a _____ is a firearm or _____ is a shooting. Visuals and criminal records help.

TOP DEFINITION 🐦 f >

blickie

a [firearm](#)

After he [popped off](#) he [tossed](#) the blickie in [the river](#).

by [YoungDon609](#) December 28, 2008

👍 91 🗑️ 33 FLAG

Get a **blickie** mug for your mom Yasemin.



E1343

Legal Process and Getting What you Want

4) High Crime Area

The Gun Recovery Unit is not the low crime response unit. If you are in area, there is probably a reason. Instead of exclusively using high crime area, articulate how you happened upon an investigation or a subject. Things that help:

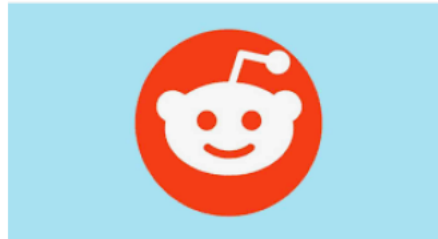
- CRS Analytical Products
- Heat Maps
- Deployment Orders and historical knowledge



E1344

Legal Process and Getting What you Want

5) The social media platform rejected my warrant



E1345

Legal Process and Getting What you Want

5) The social media platform rejected my warrant

Most Common reason: wrong address/company allocation

<https://www.search.org/resources/isp-list/>

<https://www.arin.net/>

Law Enforcement Portals

Google



E1346

Legal Process and Getting What you Want

5) The social media platform rejected my warrant

Second Most Common Reason: No one caught an error on the law enforcement side.

- Does the warrant match the affidavit?
- Is the URL correct?
- Is the charge correct?
- Did you use a template?

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
ONE YOUTUBE ACCOUNT PURSUANT
TO 18 U.S.C. § 2703 FOR
INVESTIGATION OF VIOLATIONS OF
18 U.S.C. 875(e)

SC No. _____

Filed Under Seal



E1347



FOIA Re
Requester

Legal Process and Getting What you Want

Emergency Disclosures

18 U.S. Code § 2702 - Voluntary disclosure of customer communications or records

A social media platform can provide you subscriber level information on an account if you can articulate (in good faith), that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.



E1348

Legal Process and Getting What you Want

Emergency Disclosures

These should not be used in lieu of legal process. It's a handshake agreement with a company to mitigate a threat, with the expectation that legal process will be forthcoming(if applicable).



E1349

Legal Process and Getting What you Want

Emergency Disclosures

The two requirements needed for most companies are:

- A demonstration that there is a threat
- A demonstration that the threat is imminent (not eminent)



E1350

MPD 32

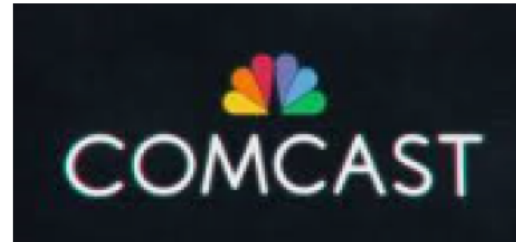
Social Media Investigations: Gun Recovery Unit Edition Presentation

p.32

Legal Process and Getting What you Want

Emergency Disclosures

An Emergency Disclosure may require an additional disclosure request



E1351

Legal Process and Getting What you Want

Emergency Disclosures

Document everything as part of the investigation

Be sure to follow up with legal process (Congress expects it)



E1352

Legal Process and Getting What you Want

A threat is mitigated with an arrest. If the imminent threat from 37th Place is revealed to be the 37th Place from Vero Beach, contact the Vero Beach Police Department or State Police



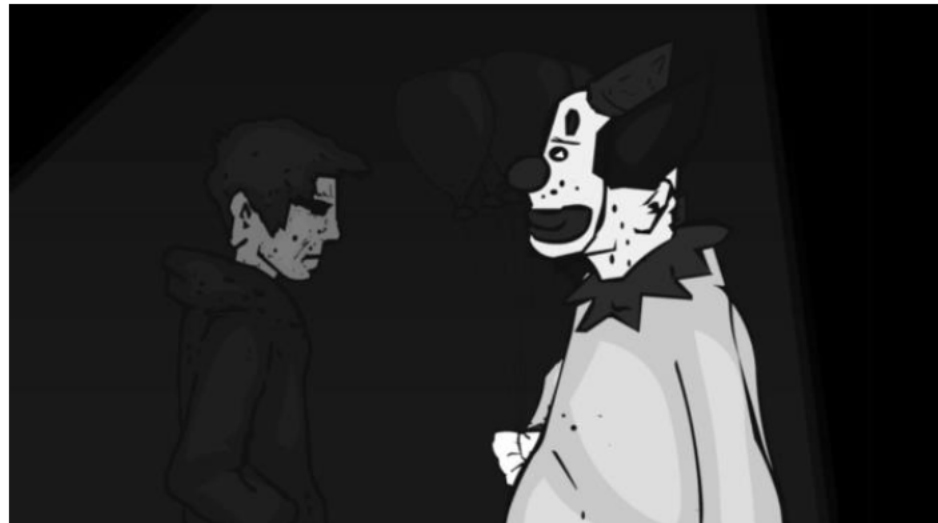
E1353

MPD 35

Social Media Investigations: Gun Recovery Unit Edition Presentation

Online Threats that actually Happened

Jeff Weise and Newgrounds (2005)



E1354

Online Threats that actually Happened

When: March 21, 2005

Number Killed: 9

Number Injured: 5

Killer: Jeffrey Weise



E1355

Online Threats that actually Happened

Adam Lanza and Steam (2012)



E1356

Online Threats that actually Happened



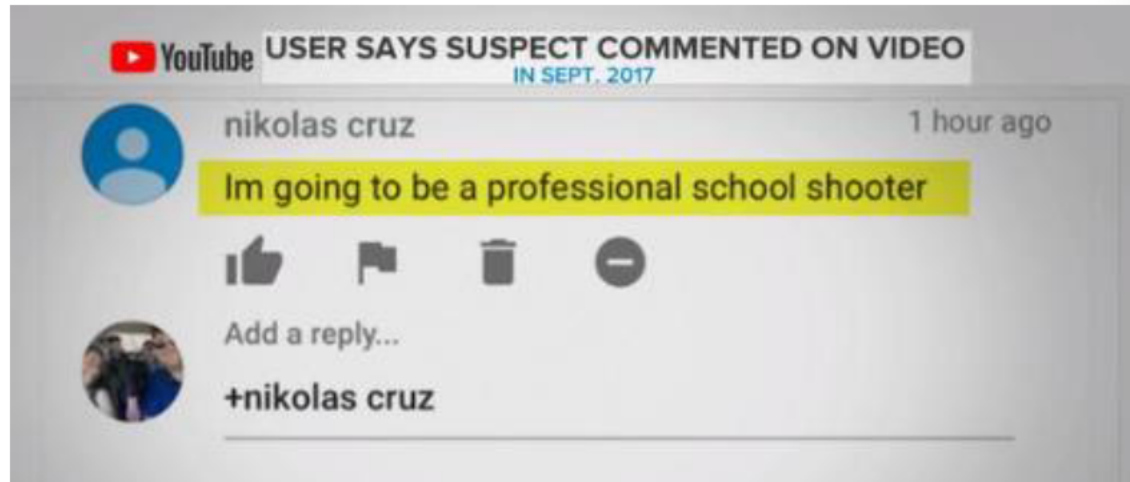
Adam Lanza Threatened Sandy Hook Killings Years Earlier, Records Show



E1357

Online Threats that actually Happened

Nikolas Cruz and Youtube (2018)



E1358

Online Threats that actually Happened

Nikolas Cruz and Youtube (2018)



E1359

Online Threats that actually Happened



E1360

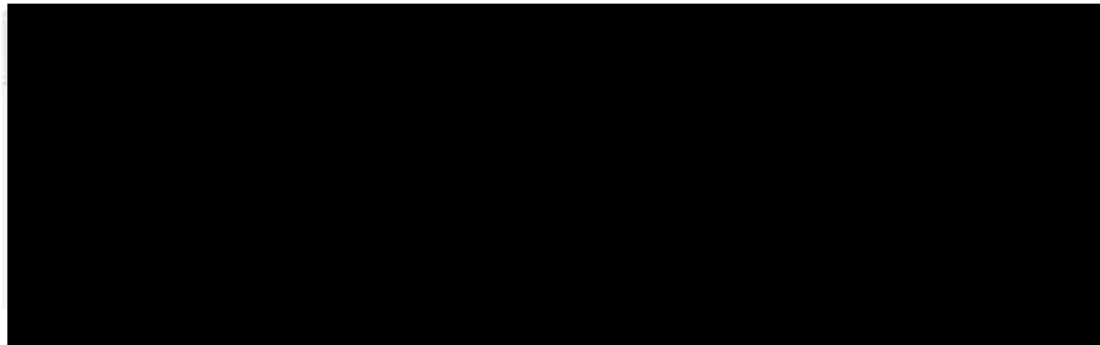
MPD 42

Social Media Investigations: Gun Recovery Unit Edition Presentation

Threat Example

MPD Receives a complaint from a tipster

- When you speak to the complainant, she advises that she knows [REDACTED] from Reddit and he uses the name [REDACTED]. She advises he purports to be a [REDACTED] and provides screen captures of the threats



E1361

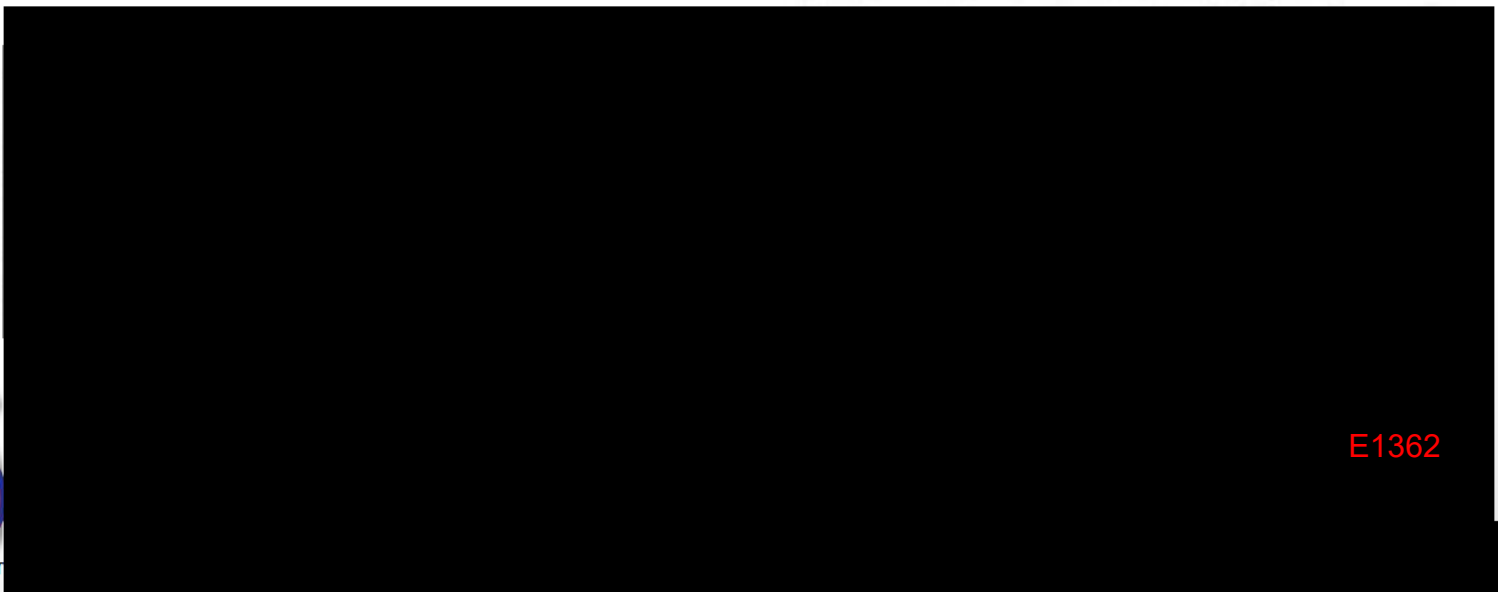


Requester

Threat Example

Assess and Decipher the Threat

- After reviewing the provided information, the Redditor [REDACTED] does openly discuss plans to shoot up the [REDACTED]



E1362

Threat Example

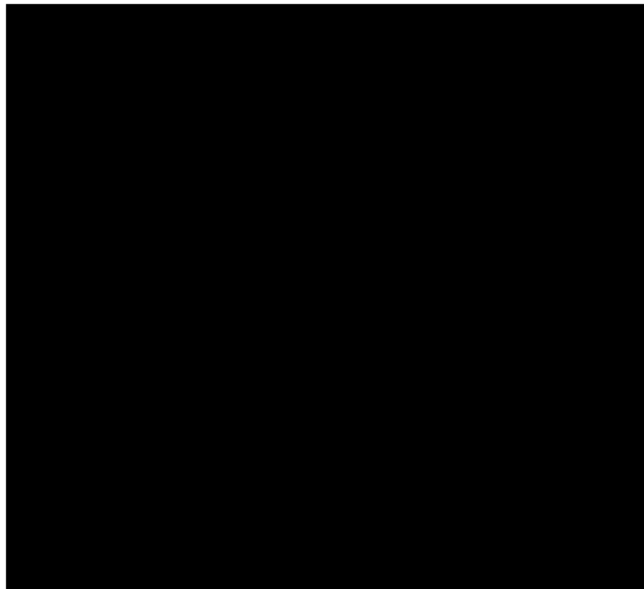
- Based on the [REDACTED] you determine this threat requires immediate action. You contact [REDACTED] who have no record of a [REDACTED] being banned, and you submit a preservation request to Reddit



E1363

Threat Example

- You submit an Emergency Disclosure request to Reddit. It is granted, providing you subscriber level information on the account

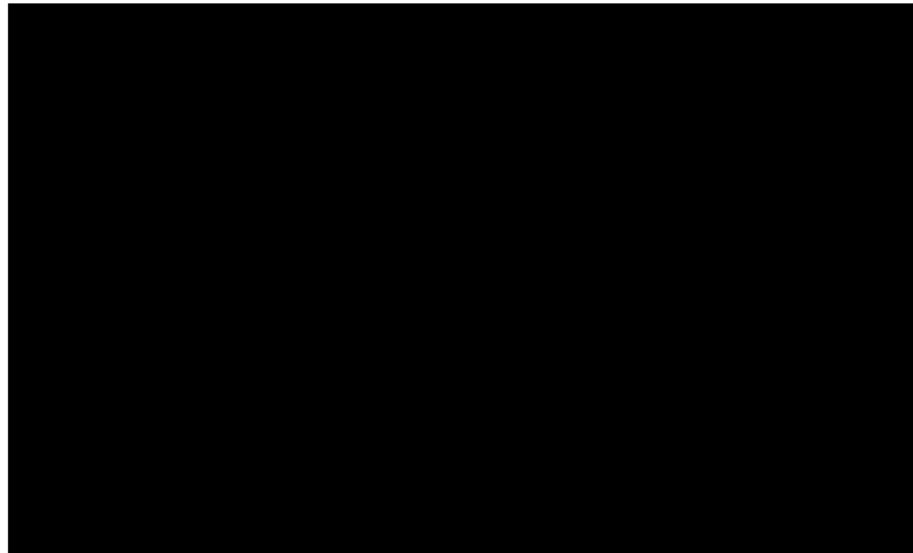


E1364



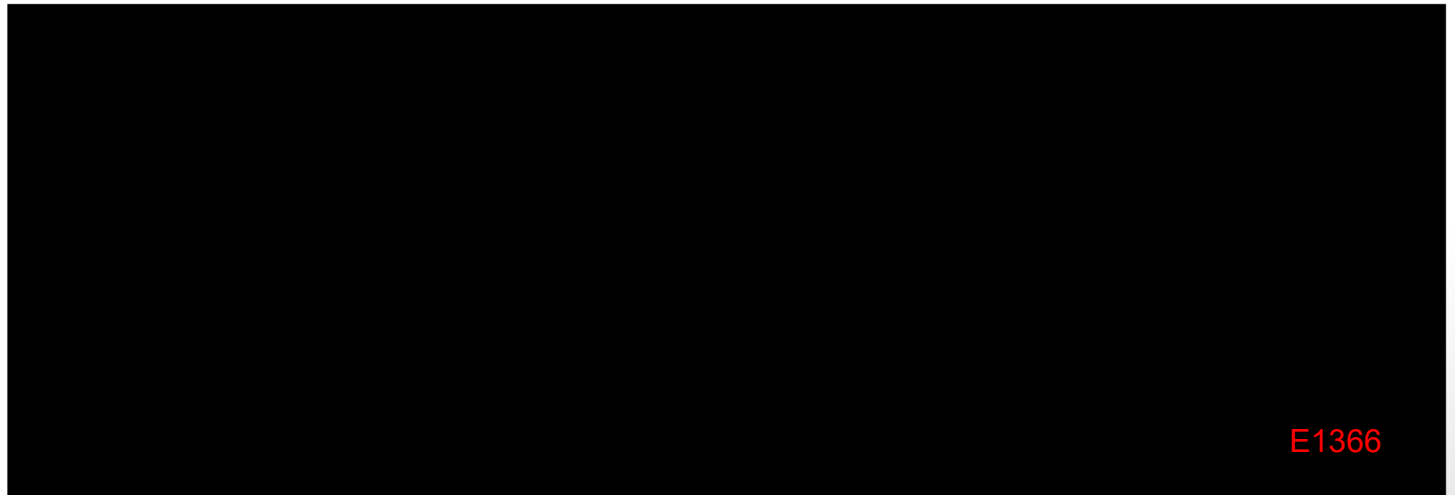
Requester

Threat Example



E1365

Threat Example

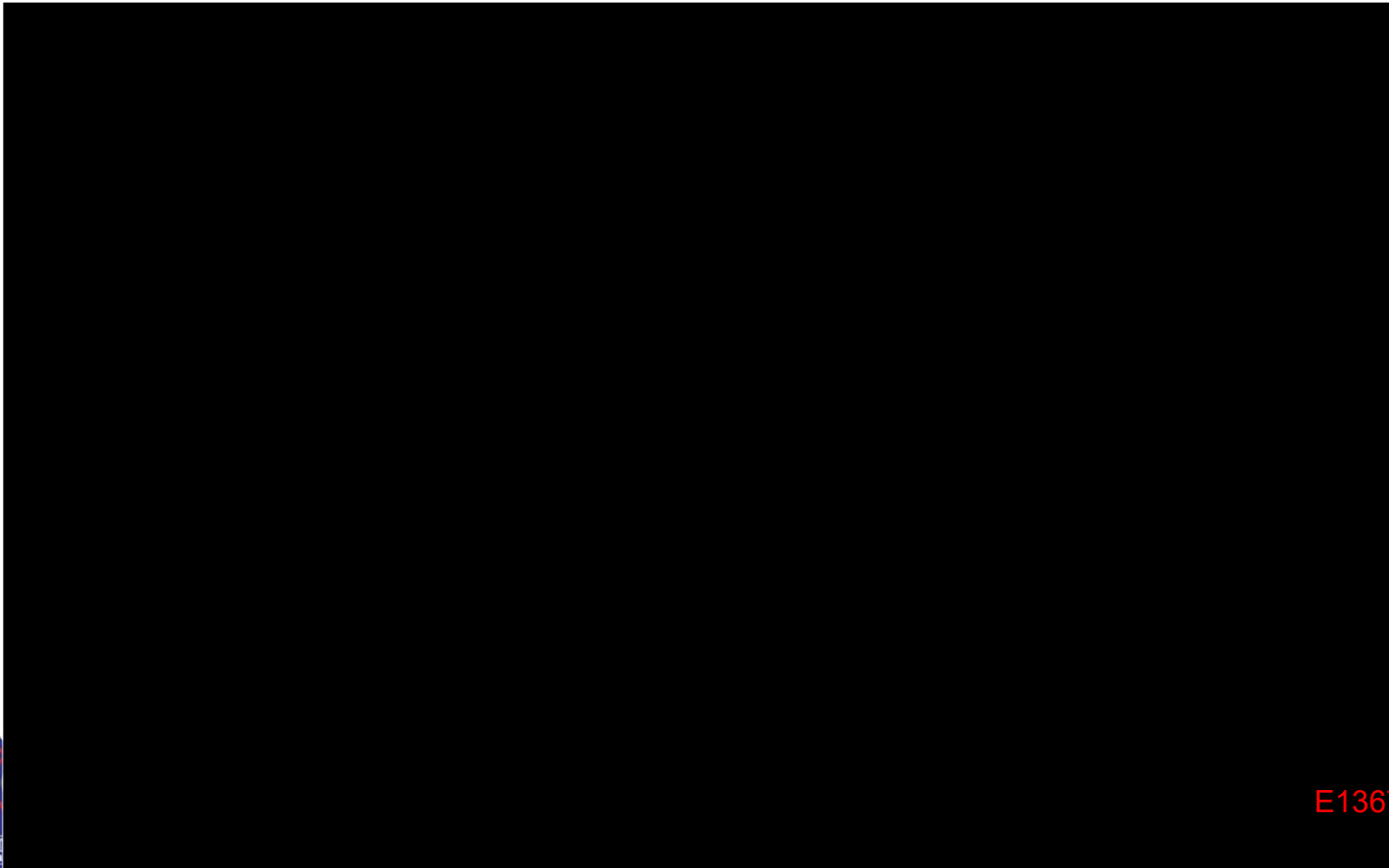


E1366



Requester

Threat Example

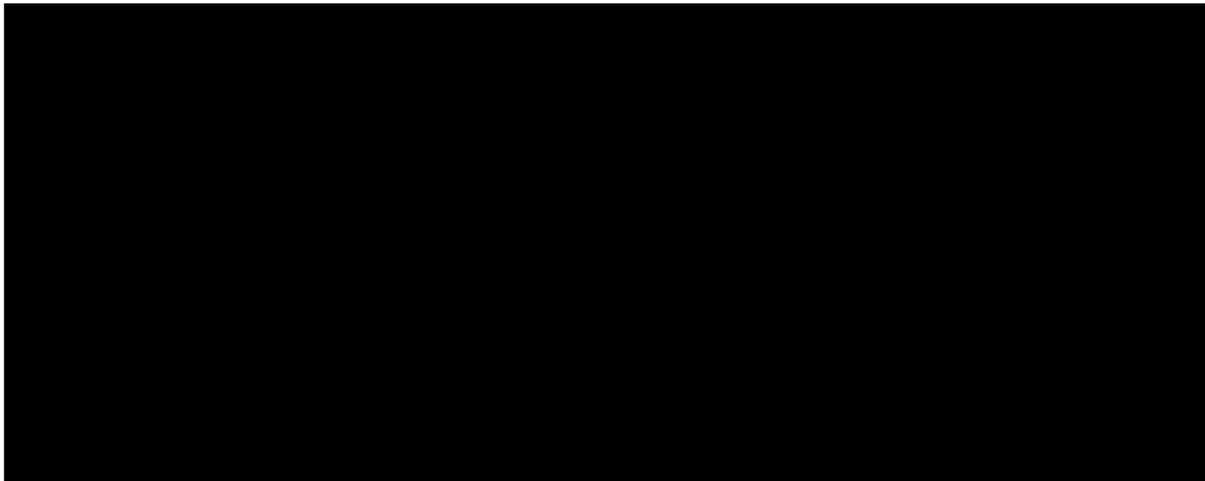


E1367

Requester

Threat Example

- You submit an Emergency Disclosure request to Google for subscriber information on the account, who identify the user as [REDACTED]” [REDACTED] has no record of interaction

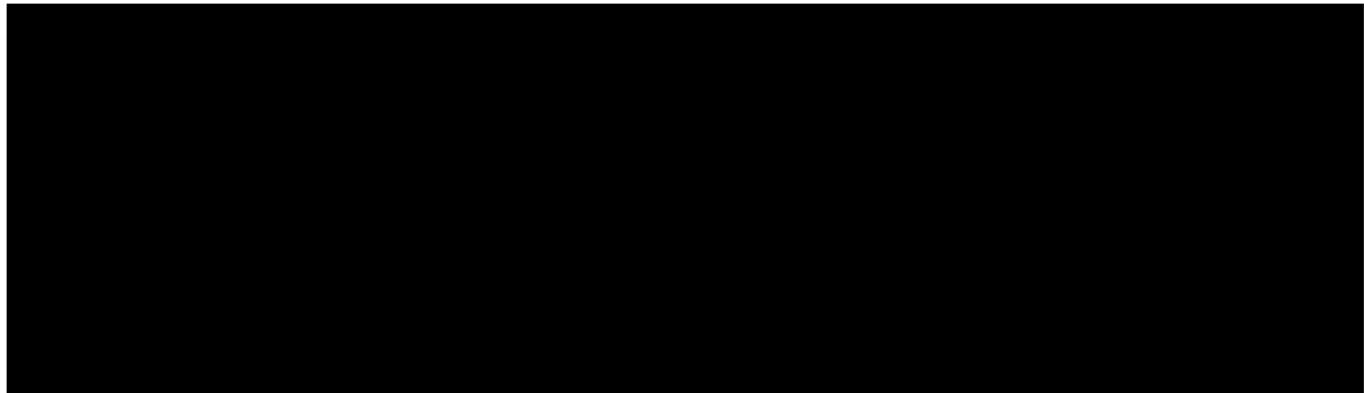


E1368



Threat Example

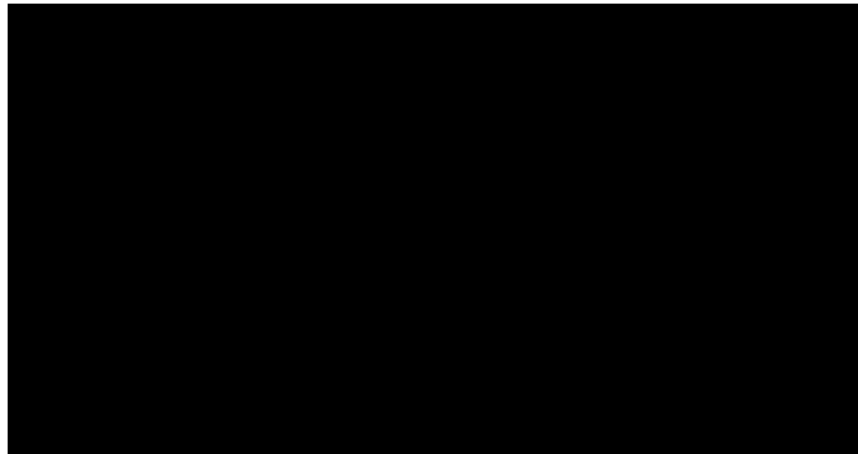
- You submit search warrants to Google and Reddit for the contents of the Users account.



E1369

Threat Example

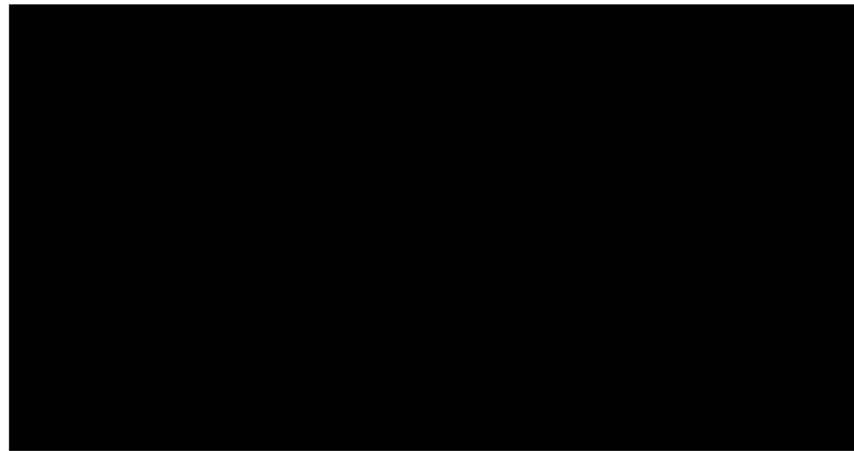
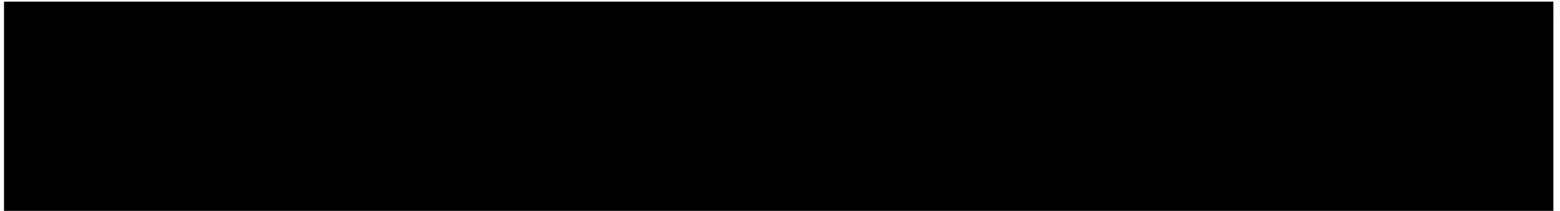
- The returns provide enough information to identify the user as



E1370



Threat Example

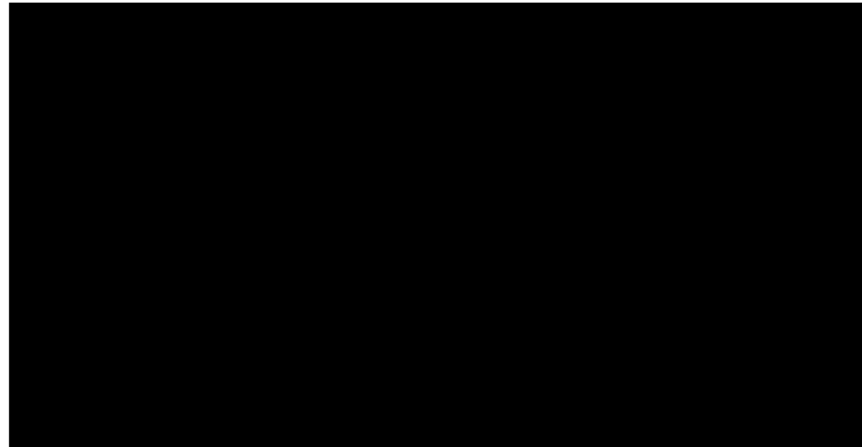


E1371

Threat Example

Threat Mitigated

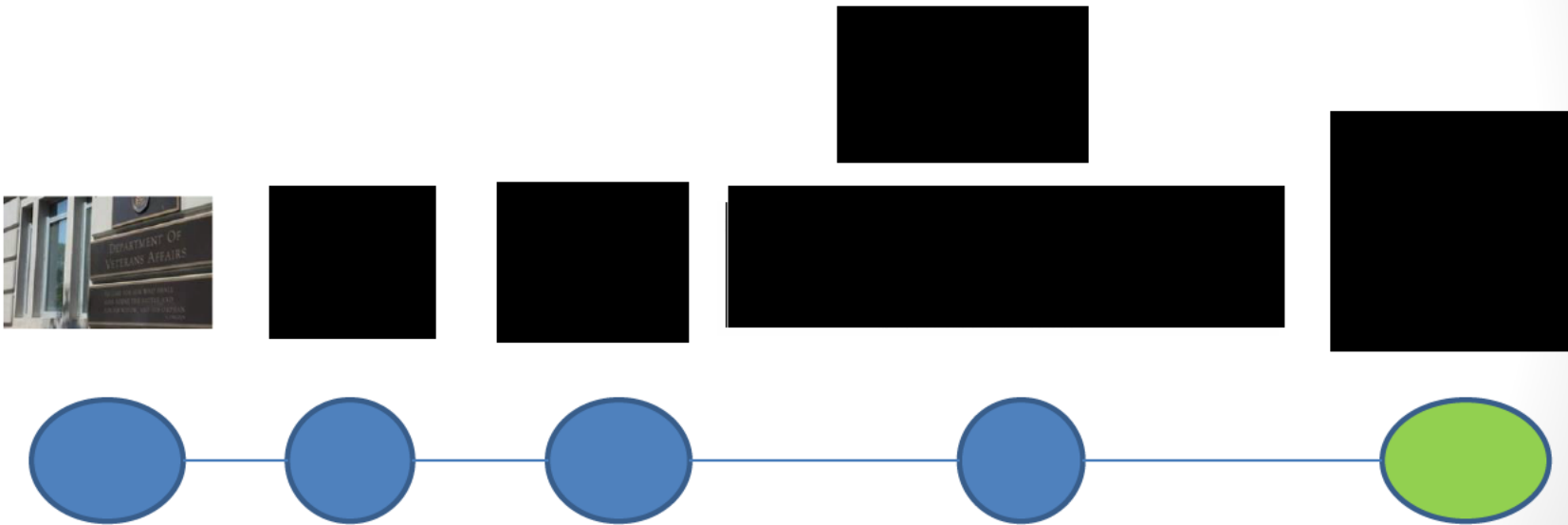
- [REDACTED]
[REDACTED] You notify law enforcement, [REDACTED] and the tipster of the resolution.



E1372

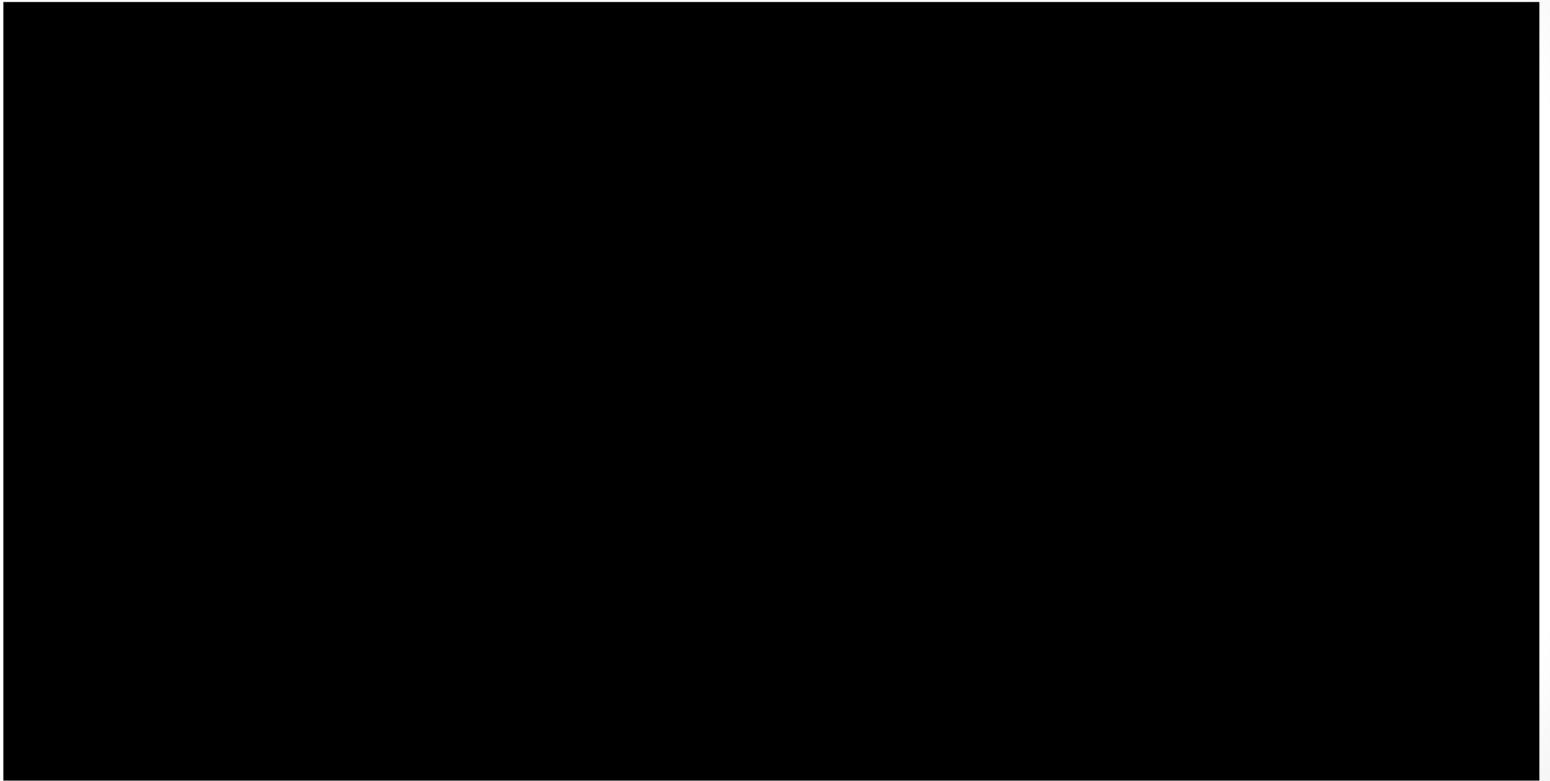


THE FLOWCHART OF JUSTICE



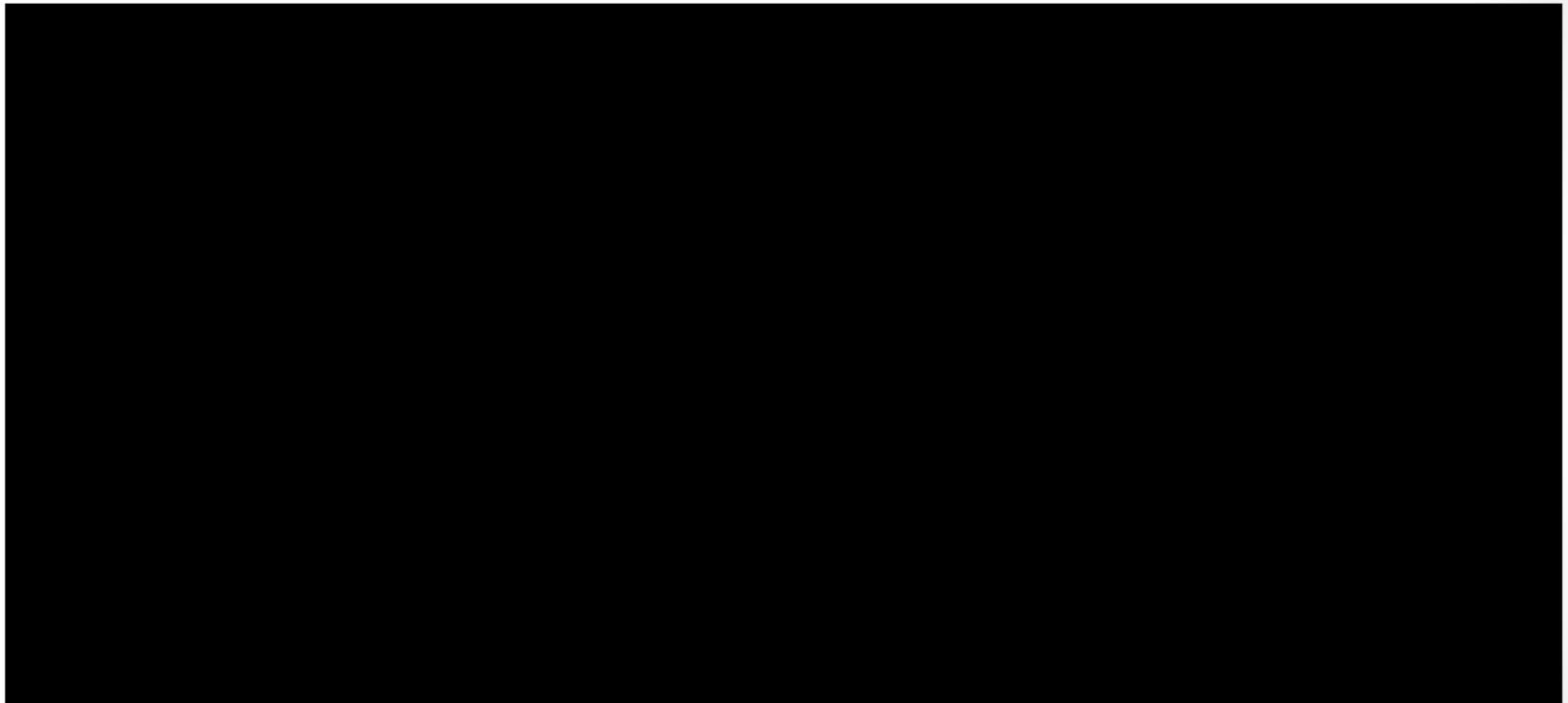
E1373

Unique Threat Cases I've Worked



E1374

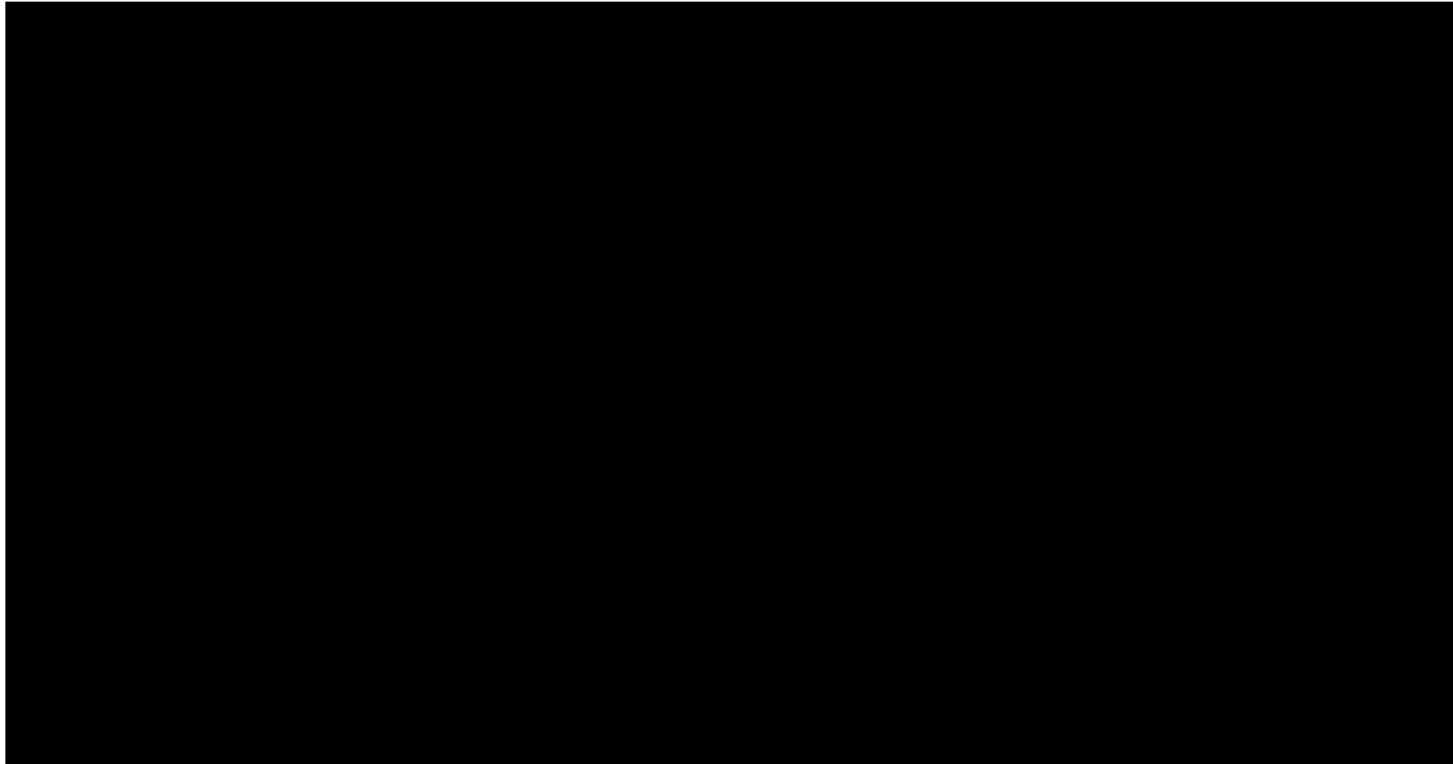
Unique Threat Cases I've Worked



E1375

MPD 57

Unique Threat Cases I've Worked



E1376

Social Media Scenarios: Scenario Edition

Detective Sergeant [REDACTED]

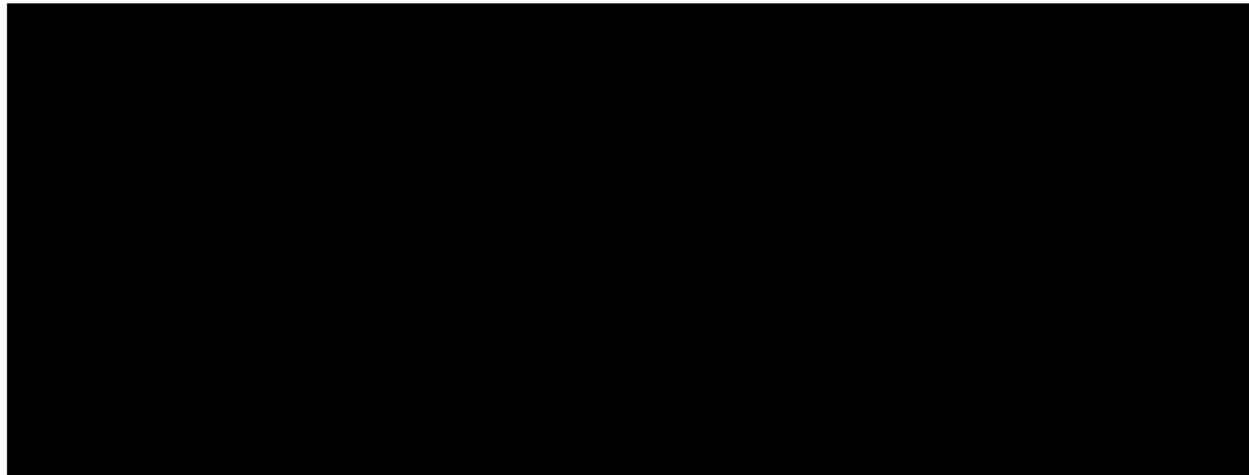
E1377



FOIA Requester

Threat #1: 4Chan hates Kent, DC

- On [REDACTED], 4Chan user [REDACTED] makes threats to the District of Columbia. Mitigate!



E1378

Threat #1: 4Chan hates Kent, DC

- There is a specific date given to shoot the Kent neighborhood. You submit an Emergency Disclosure to 4Chan...and it is denied. You also submit a preservation request



E1379

Threat #1: 4Chan hates Kent, DC

- You notify 2D of the Threat to Kent, and SOD of the threat to the FSK Bridge.



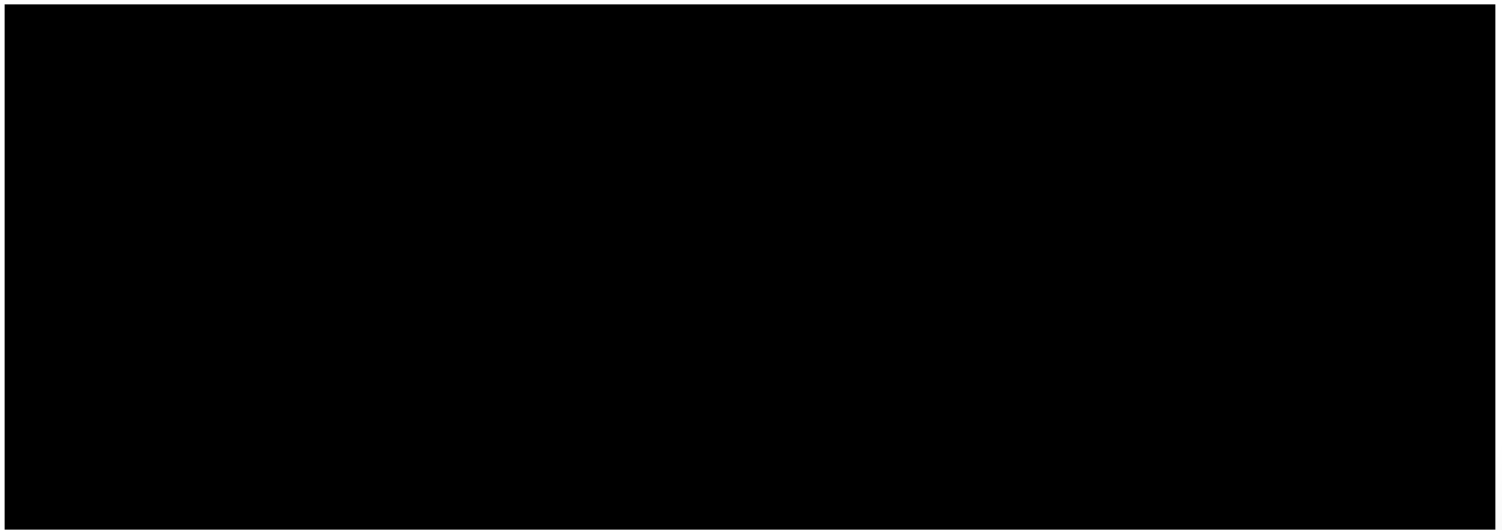
E1380



Requester

Threat #1: 4Chan hates Kent, DC

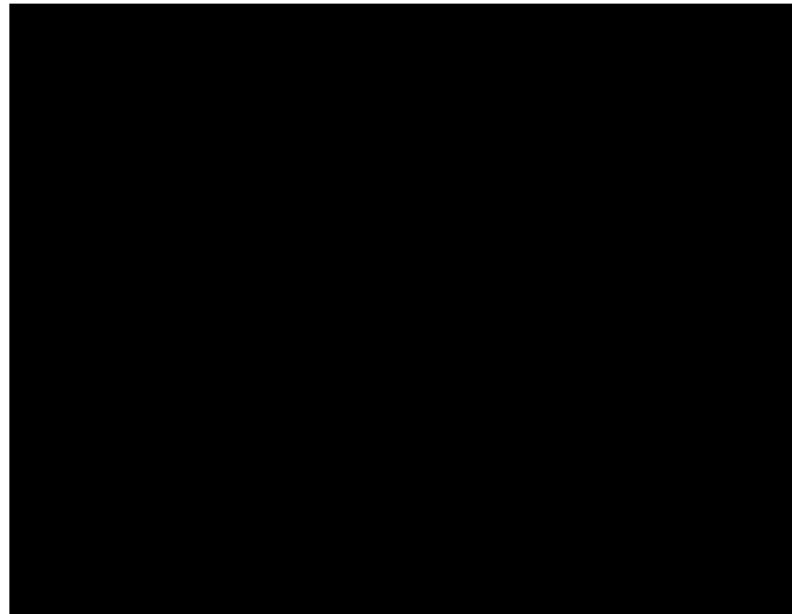
- You obtain a warrant for the account and 4Chan provides you with an IP address and more posts*



E1381

Threat #1: 4Chan hates Kent, DC

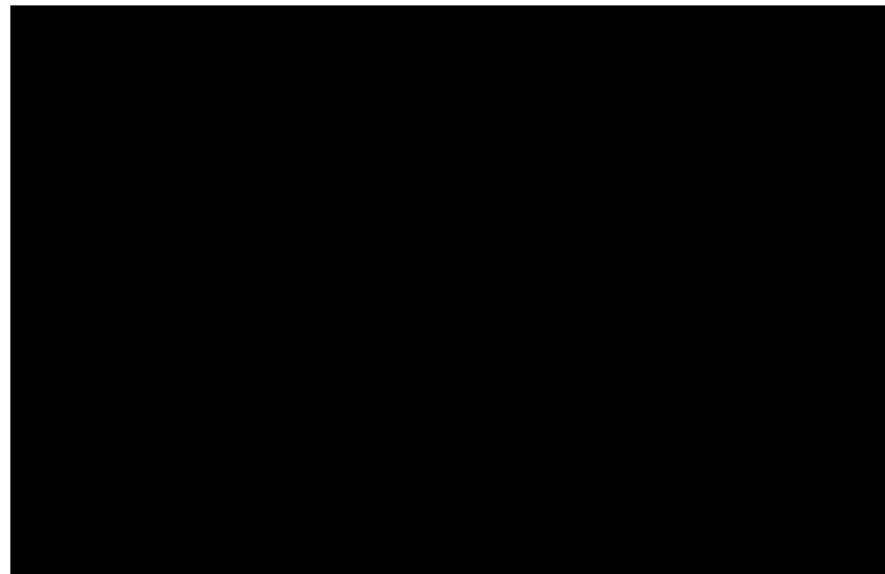
- [REDACTED] A second warrant is submitted, and subsequently declined



E1382

Threat #1: 4Chan hates Kent, DC

- You document the incident, the declination, and you refer the available info to [REDACTED] (also documented)



E1383

Threat #2 A Verizon Caller hates 6D

On [REDACTED] a telephonic threat is made to the Sixth District, threatening to shoot everyone inside. The call comes from Verizon Wireless telephone number [REDACTED] [REDACTED] Mitigate!



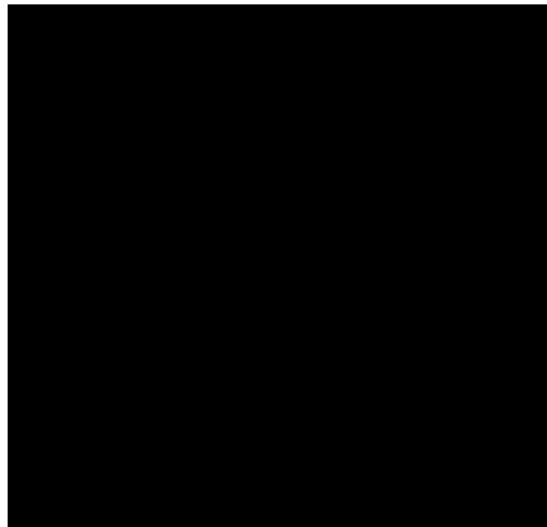
E1384



Requester

Threat #2 A Verizon Caller hates 6D

Emergency Legal Process provides subscriber information on the number, revealing it to belong to a resident at

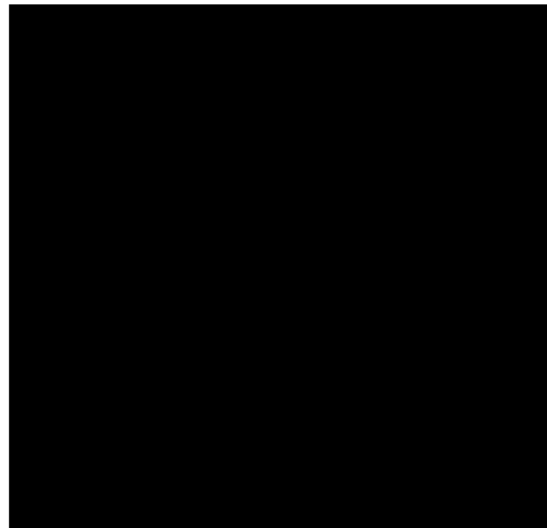


E1385



Threat #2 A Verizon Caller hates 6D

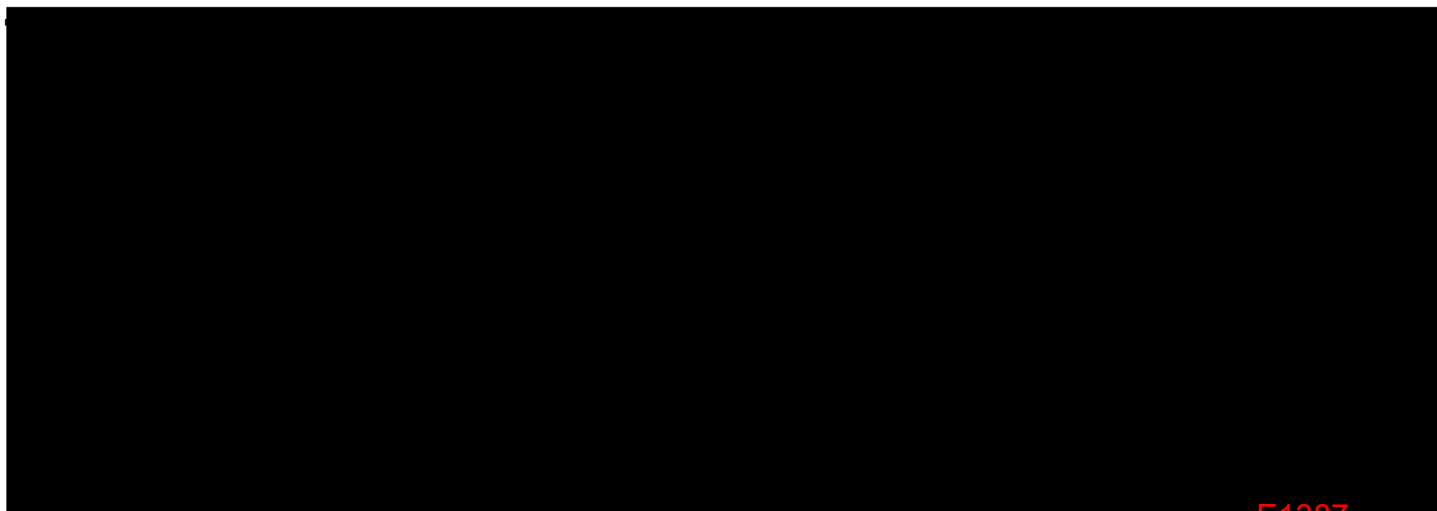
An interview with the building manager confirms the subject resides at [REDACTED] [REDACTED] and an Emergency Search Warrant is obtained for the residence



E1386

Threat #2 A Verizon Caller hates 6D

The Search Warrant is executed, recovering multiple firearms and 3D Printing equipment. The subject is PC arrested on scene



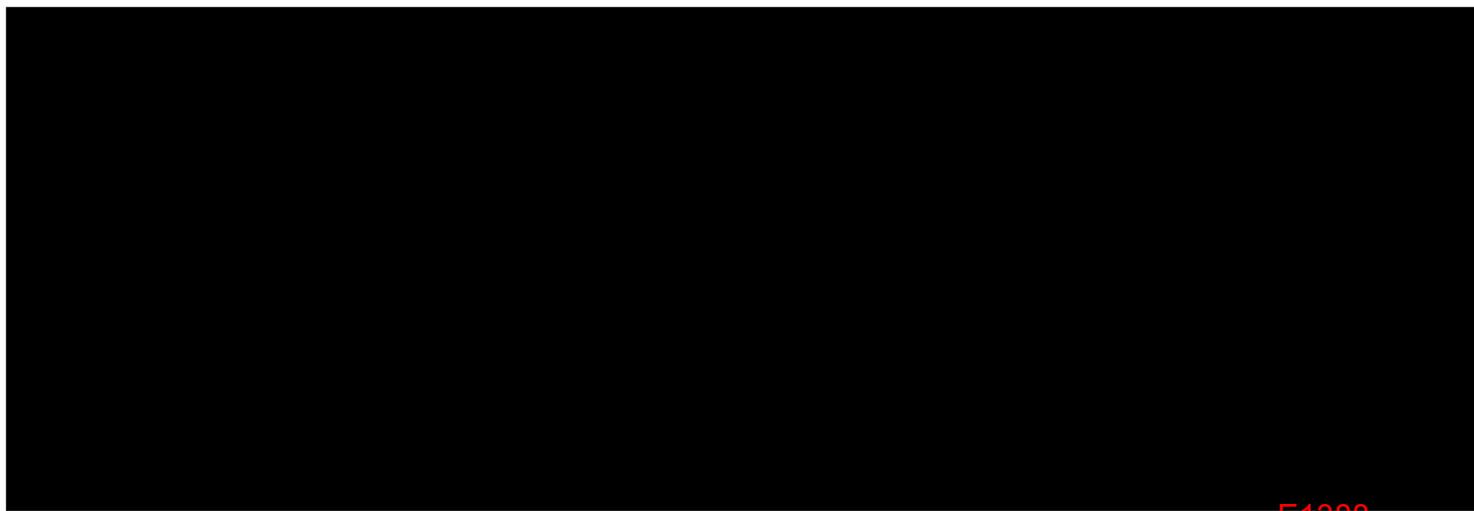
E1387



Requester

Threat #2 A Verizon Caller hates 6D

A follow up subpoena is submitted to the telephone provider.



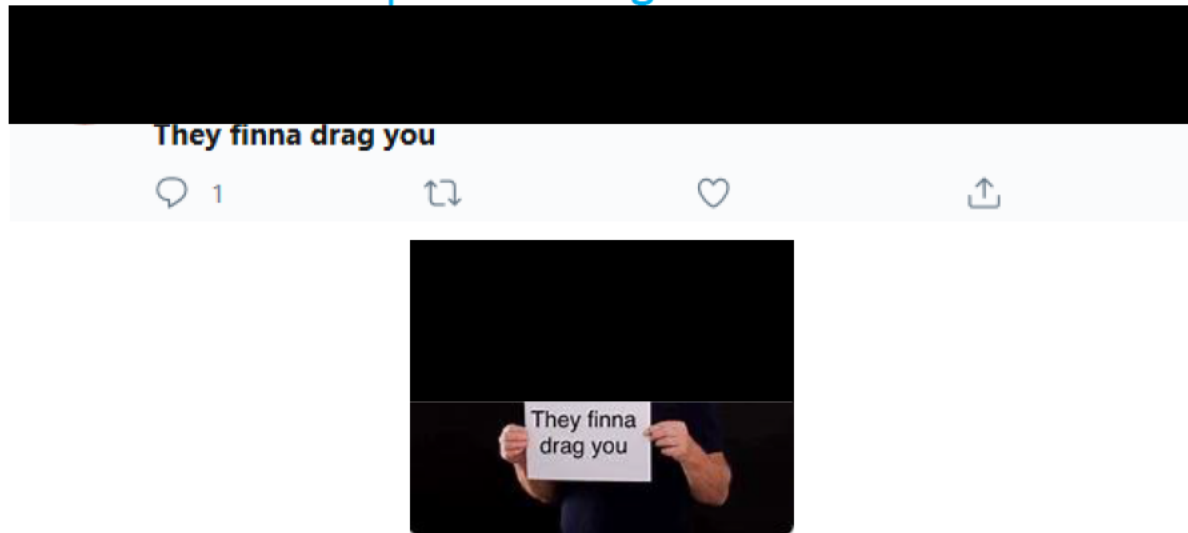
E1388



Requester

Threat #3: Twitter hates block parties

- [REDACTED] [REDACTED] announced on Twitter that she will be holding a Mask-Free Block party in the 1800 Block of Columbia Road, with no concern for Law Enforcement. On [REDACTED] [REDACTED] [REDACTED] reports to law enforcement that she received the below hate crime threat in response. Mitigate!



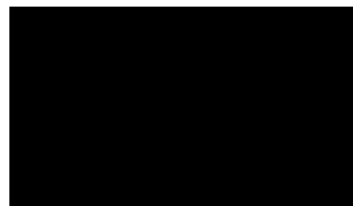
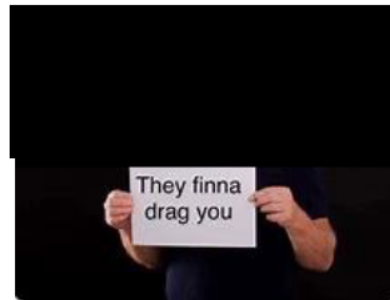
E1389



FOIA Requester

Threat #3: Twitter hates block parties

You consult knowyourmeme and urban dictionary, revealing “They finna drag you” to be a “Finna Woke” reaction meme, used to suggest that someone is going to get dragged through the comments section. A cursory review of the comments from the block party announcement reveal that she was indeed dragged through the comments.



Finna Woke

Part of a series on [redacted] [\[View Related Entries\]](#)

Updated 2 years ago by [redacted]

Added 2 years ago by [redacted]



13,515

0

4

15

E1390



Threat #3: Twitter hates block parties

- If the user is known, interview to ensure it was just internet tomfoolery. Suggest the post be deleted.
- If there is evidence of constant harassment from the account, consider reporting it.
- Advice [REDACTED] of your findings, encourage her to report it.
- Report [REDACTED] party to the 3rd District to ensure it doesn't happen
- Document and save everything

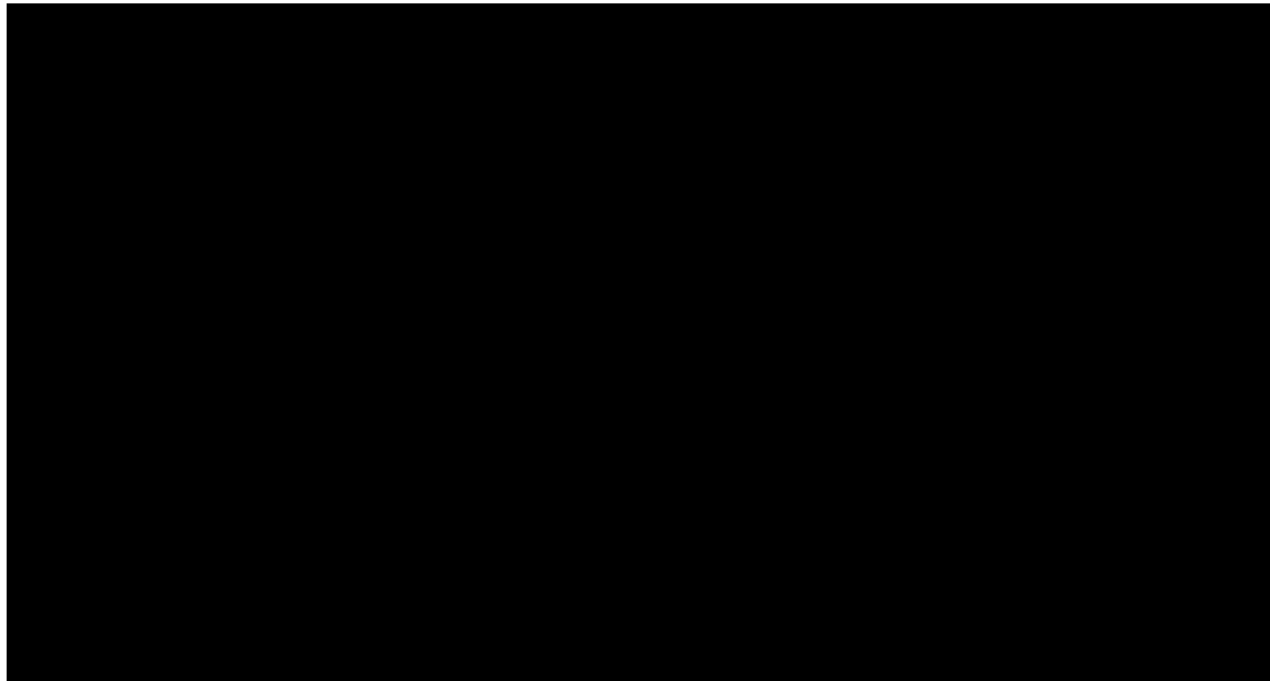


E1391

Threat #4: [REDACTED]

does not like Mondays

On [REDACTED] twitter account [REDACTED] makes threats to shoot up a school. A cursory review of the account shows it is likely in [REDACTED] but you ended up with it as a District Detective. Mitigate!



E1392



Threat #4: [REDACTED] does not like Mondays:

The complaint was submitted anonymously.

The threat should be considered credible and imminent.



E1393

Threat #4: [REDACTED]

does not like Mondays

The complaint was submitted anonymously.

The threat should be considered credible and imminent.

Submit a Preservation Request and Emergency Disclosure to Twitter

Law Enforcement Request

Please fill out all the fields below so we can review your report.

- Tell us about yourself
- I am an authorized law enforcement representative (e.g., police officer, federal agent).
 - I am an authorized government representative (e.g., district attorney, minister).
 - None of the above.

Not what you need help with? [Choose another topic.](#)

E1394



Threat #4: [REDACTED] does not like Mondays

Submit a Preservation Request and Emergency Disclosure to Twitter

- Tell us about yourself
- I am an authorized law enforcement representative (e.g., police officer, federal agent).
 - I am an authorized government representative (e.g., district attorney, minister).
 - None of the above.

Type of request or report

- How can we help?
- Request for account information
 - Non-emergency information request
 - Emergency disclosure request
 - Report potentially illegal content
 - Report other violations
 - Other inquiries

E1395



Threat #4: [REDACTED] does not like Mondays

Submit a Preservation Request and Emergency Disclosure to Twitter

Nature of the emergency

Select all that apply

- Suicide / Self-harm
- Threat to another person
- Threat to a place
- Other threat

Subject of the emergency

Full name

Identify the person(s) in danger of death or serious physical injury

Twitter username

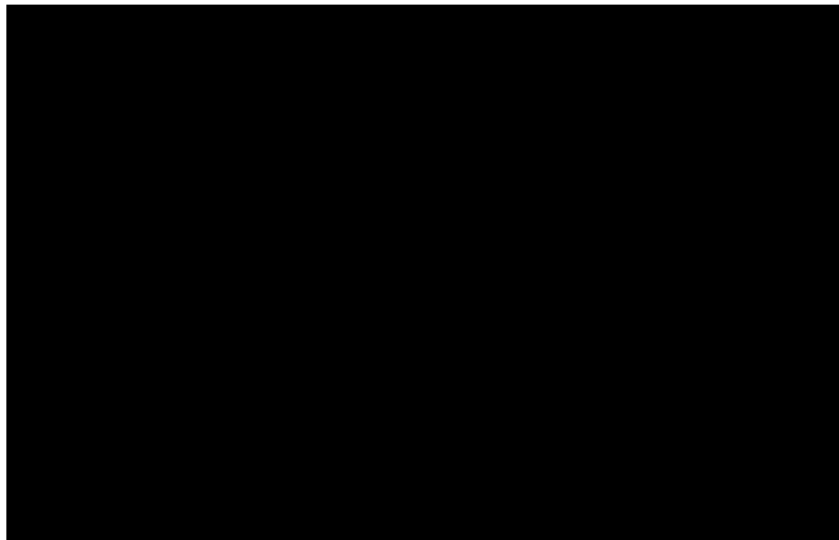
Twitter @username of the subject account(s) whose information is necessary to prevent the emergency (e.g., @safety)

E1396



Threat #4: [REDACTED] does not like Mondays

Twitter provides Subscriber Information, [REDACTED]
[REDACTED]

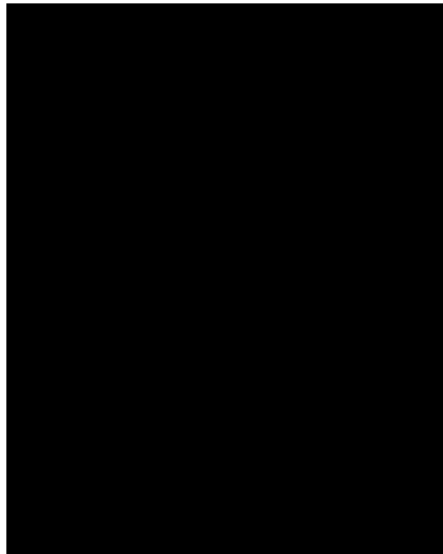


E1397

Threat #4: [REDACTED]

does not like Mondays

You contact [REDACTED] (speaking with a live person), and provide them with the reporting information. [REDACTED] [REDACTED] later advise that the subject was identified, interviewed, and arrested(document).



E1398

Threat #5: Craigslist Missed Connections is still a thing

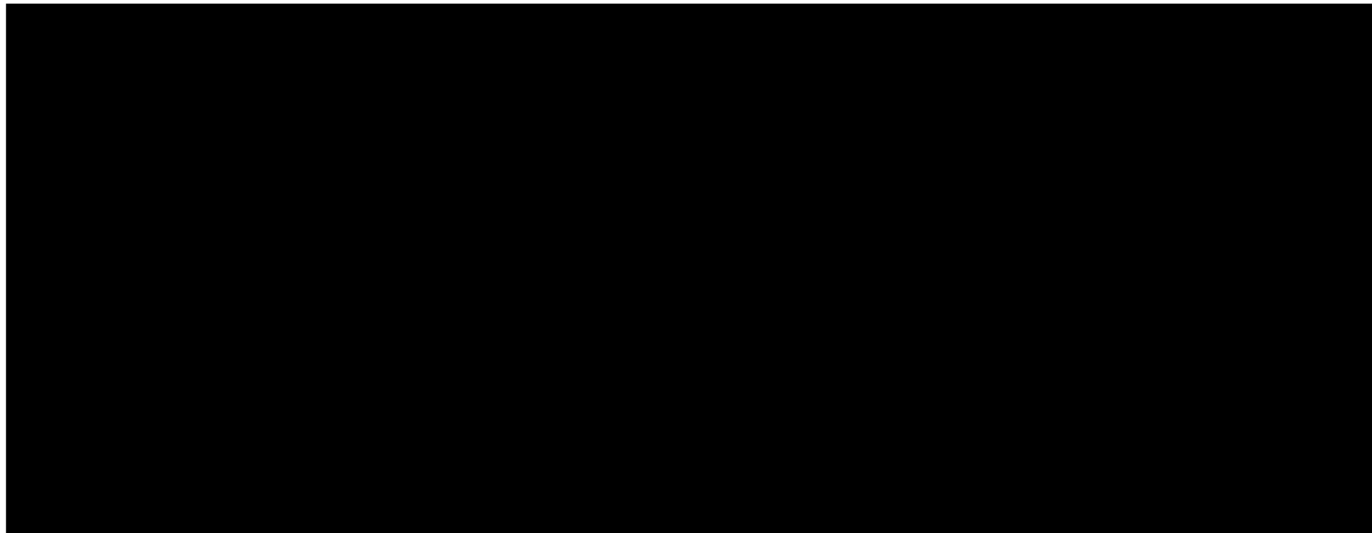
On [REDACTED] you received a threat from the Washington DC Missed Connections section of Craigslist. Mitigate!



E1399

Threat #5: Craigslist Missed Connections is still a thing

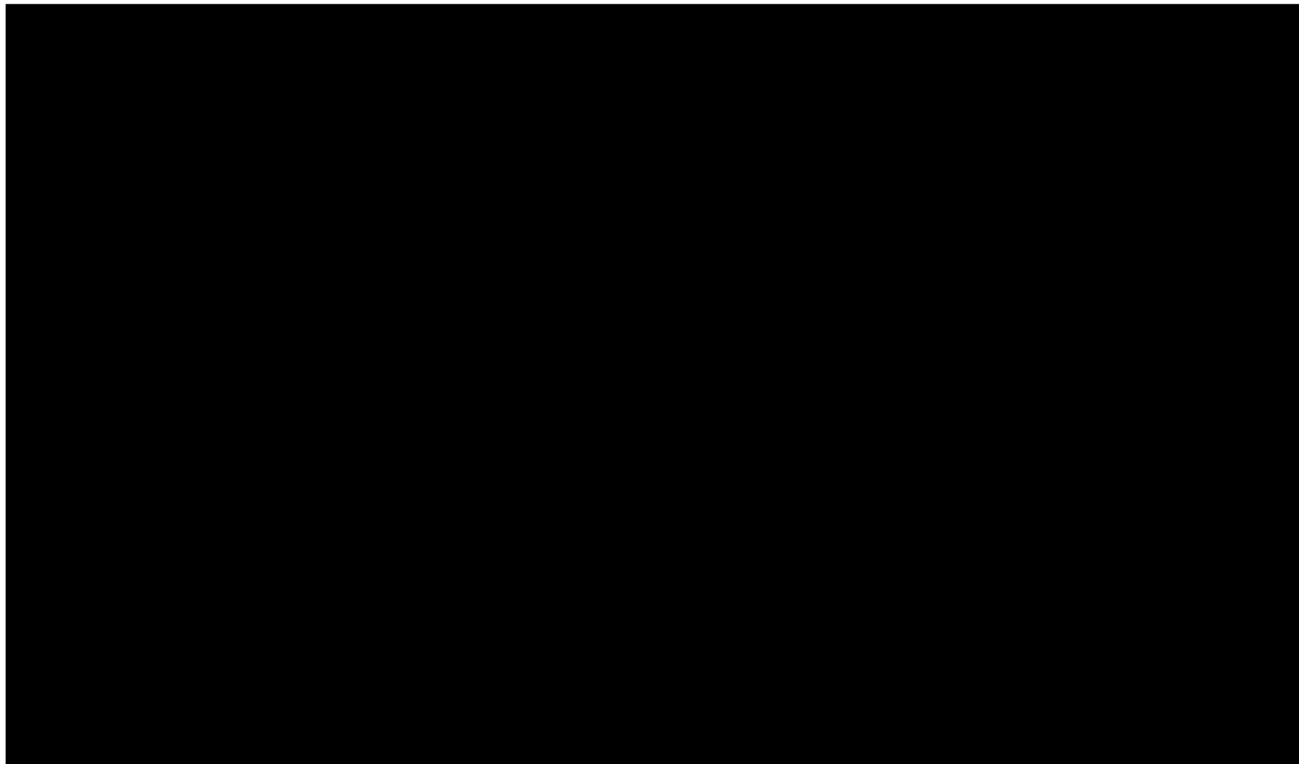
The statement is concerning, but lacks a timeframe to show exigency.



E1400

Threat #5: Craigslist Missed Connections is still a thing

A warrant is submitted to Craigslist



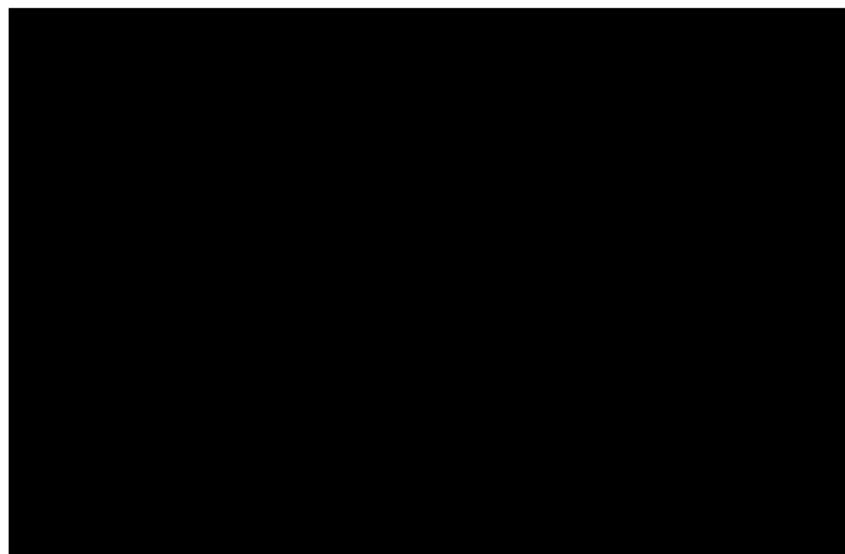
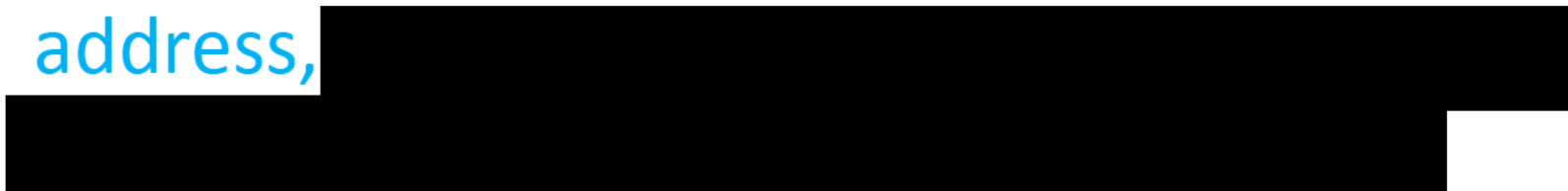
E1401



FOIA Requester

Threat #5: Craigslist Missed Connections is still a thing

The warrant provides an IP address, an email address,



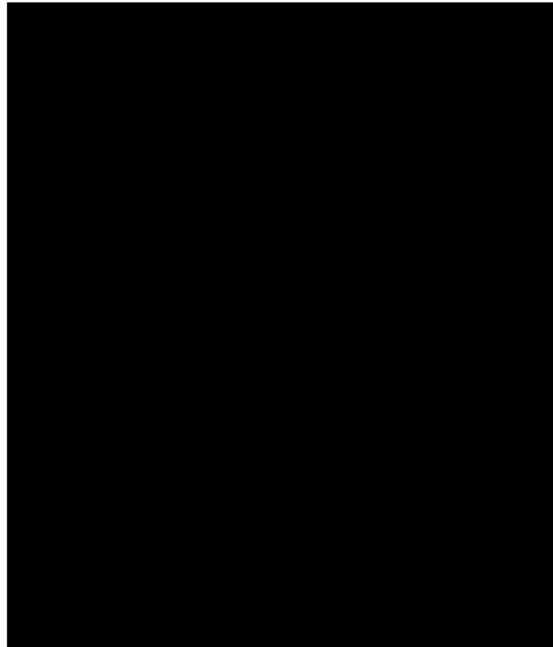
E1402



Requester

Threat #5: Craigslist Missed Connections is still a thing

Follow up warrants are conducted on the email address and ISP, identifying the poster as

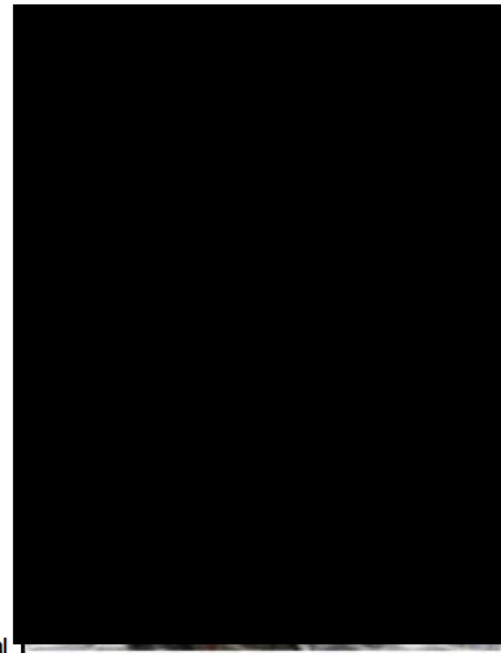
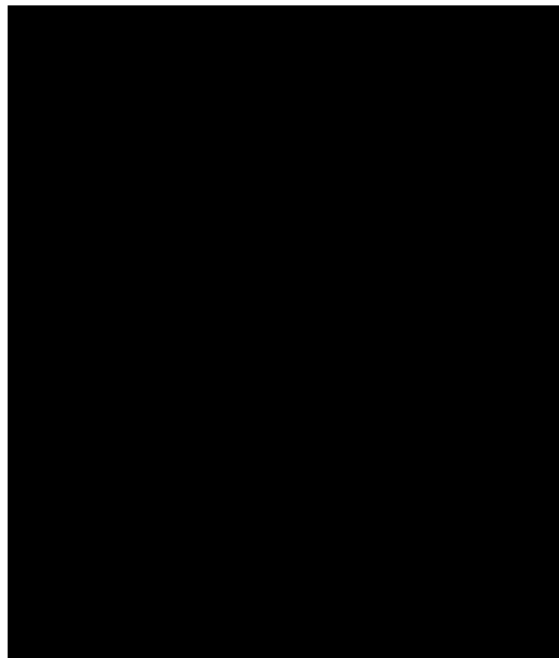


E1403

MPD 85

Threat #5: Craigslist Missed Connections is still a thing

You attempt to interview him and he declines. A warrant is present and signed.



E1404

Social

MPD 86
Sentation

Threat #6: [REDACTED] hates Gallaudet

On [REDACTED] you receive a Facebook threat against Gallaudet University. Gallaudet Staff advise

[REDACTED] Mitigate!



E1405

Threat #6: [REDACTED] hates Gallaudet

The threat account is publically viewable, and you are able to view the threat.

Snip it! Save it! Document it!



E1406



Threat #6: [REDACTED] hates Gallaudet

You submit an Emergency Disclosure request to Facebook, which is granted. A follow up ED is submitted [REDACTED]

[REDACTED]

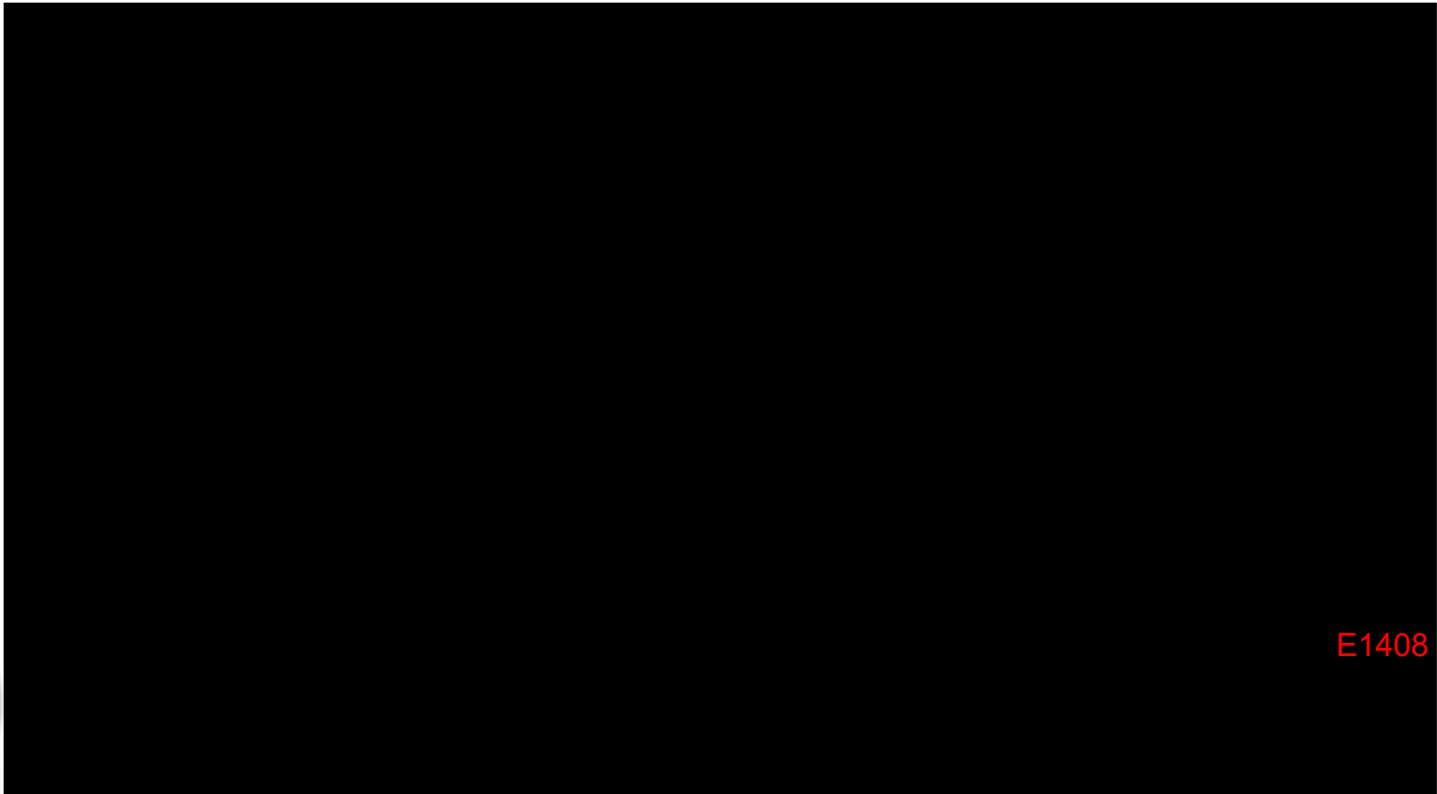
[REDACTED]

E1407



Threat #6: [REDACTED] hates Gallaudet

[REDACTED] Police interview the subject, who admits he did it. A warrant is submitted and signed, and Gallaudet University is advised

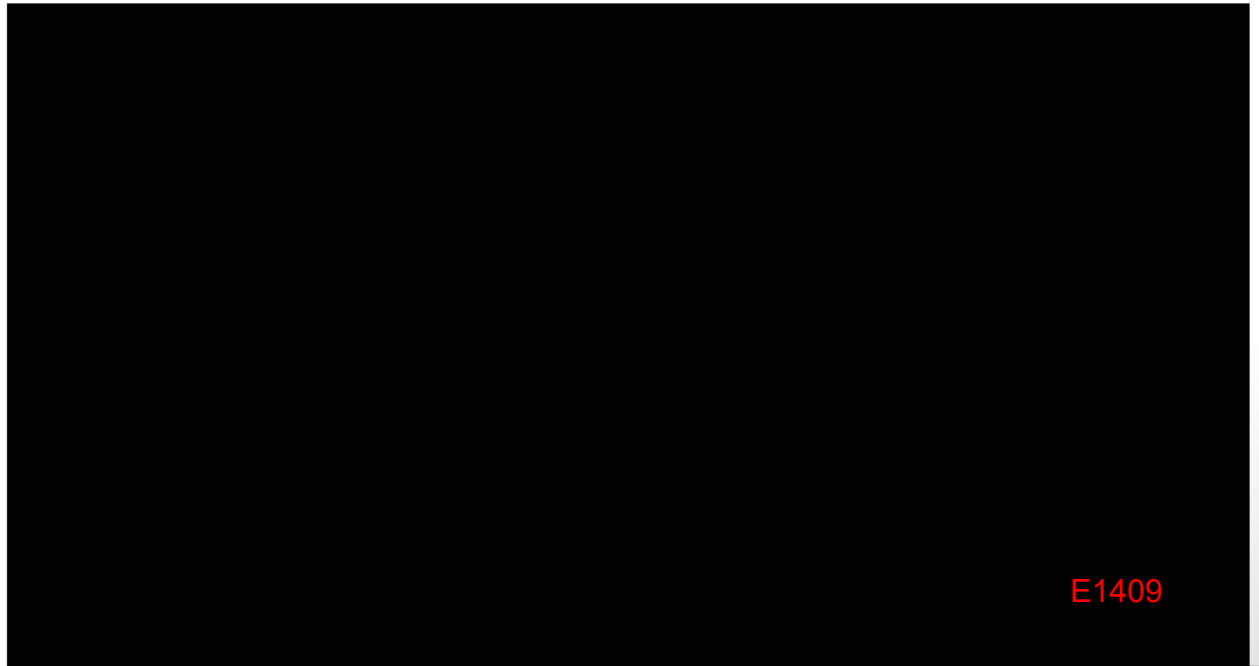


E1408

Threat #7: The Flash hates PlaylistLive

On [REDACTED], [REDACTED]

[REDACTED] She reports to DC that she has received threats from [REDACTED]. Mitigate!



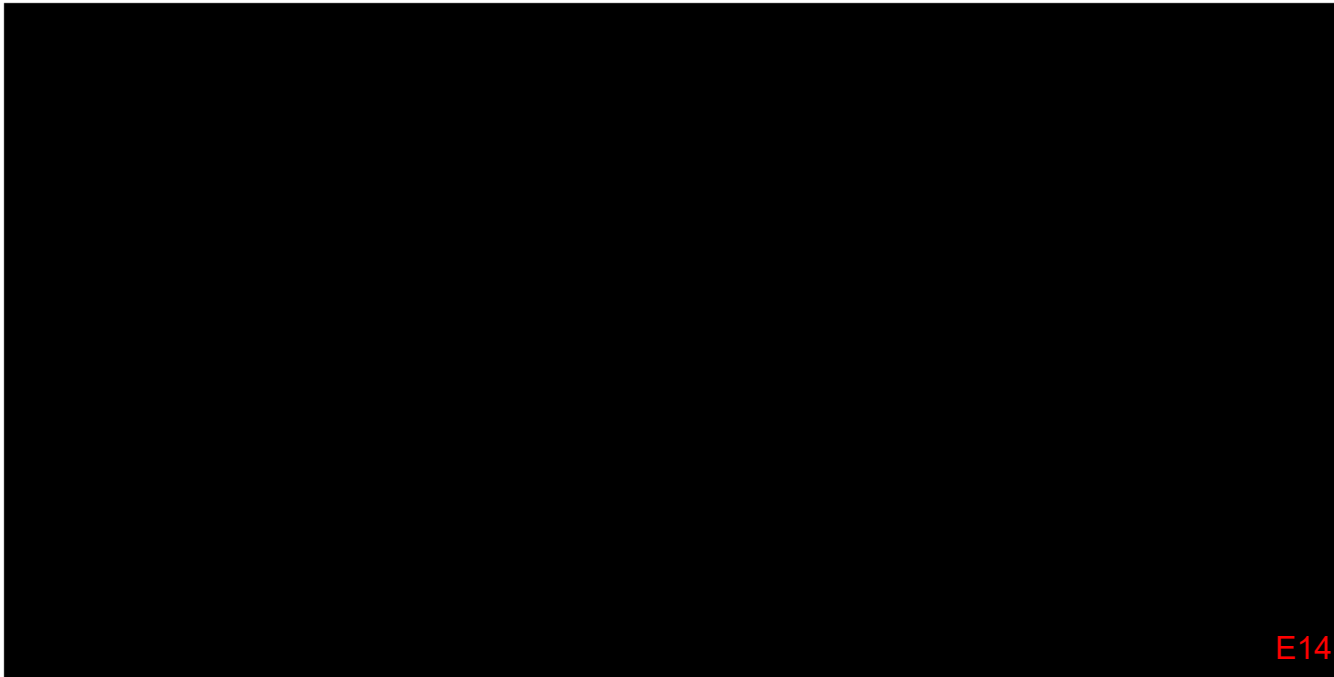
E1409



Requester

Threat #7: The Flash hates PlaylistLive:Answer 3C

You interview [REDACTED] revealing that the subject has contacted her via 19 separate [REDACTED] accounts



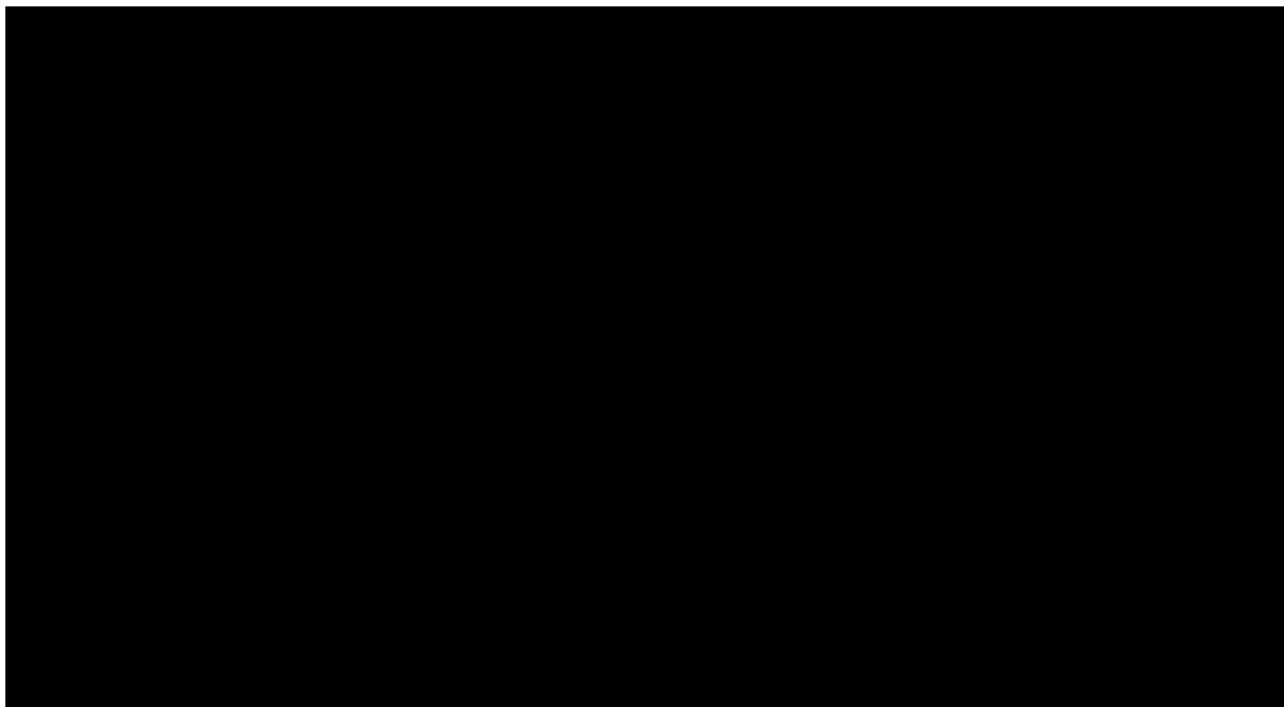
E1410



Requester

Threat #7: The Flash hates PlaylistLive:Answer 3B

You interview [REDACTED] revealing that the subject
has contacted her via 19 separate [REDACTED]
accounts

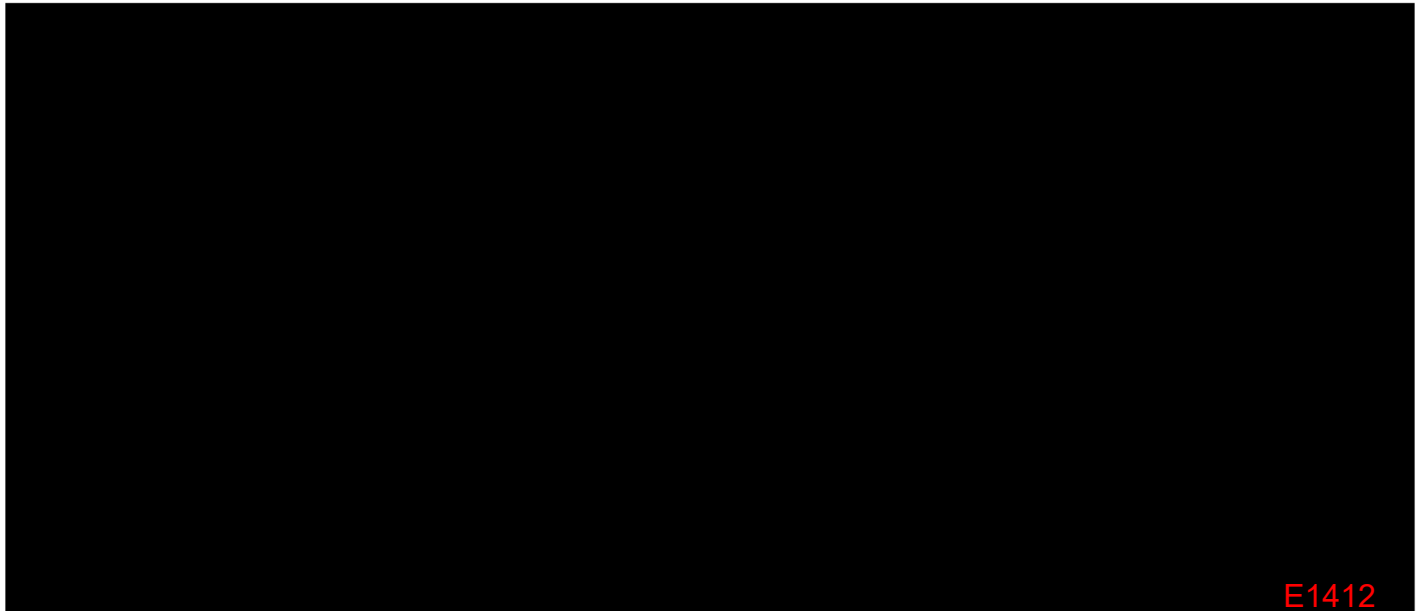


E1411

MPD 93
resentation

Threat #7: The Flash hates PlaylistLive:Answer 3B

You interview [REDACTED] revealing that the subject has contacted her via 19 separate [REDACTED] accounts

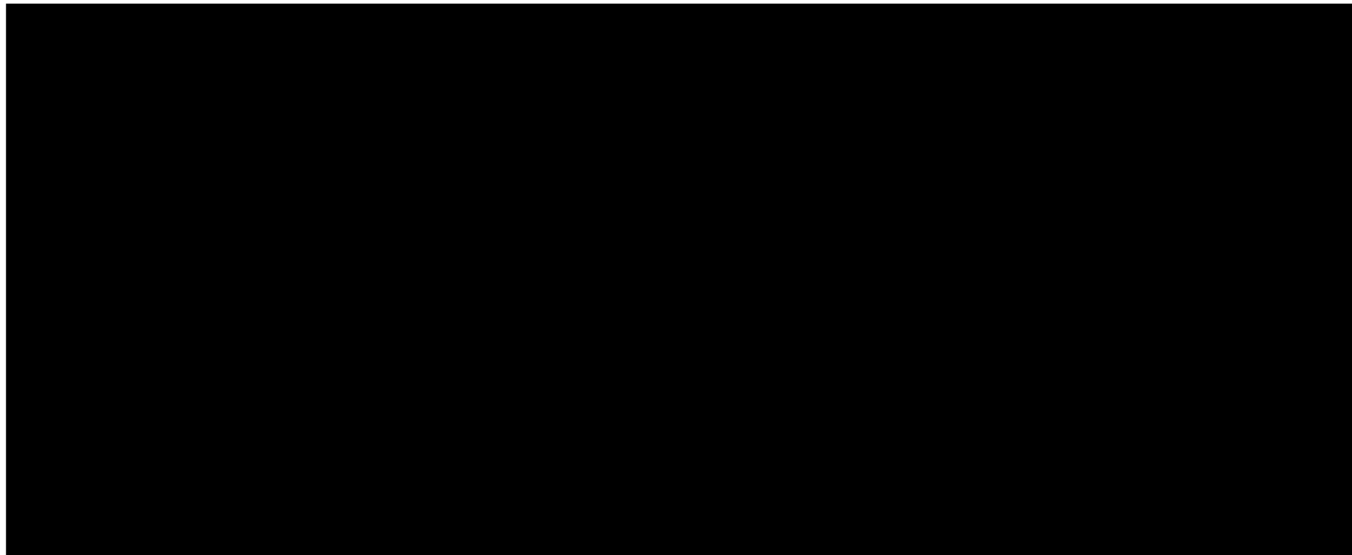


E1412



Threat #7: The Flash hates PlaylistLive:Answer 3B

You submit an Emergency Disclosure to Facebook
for all accounts.



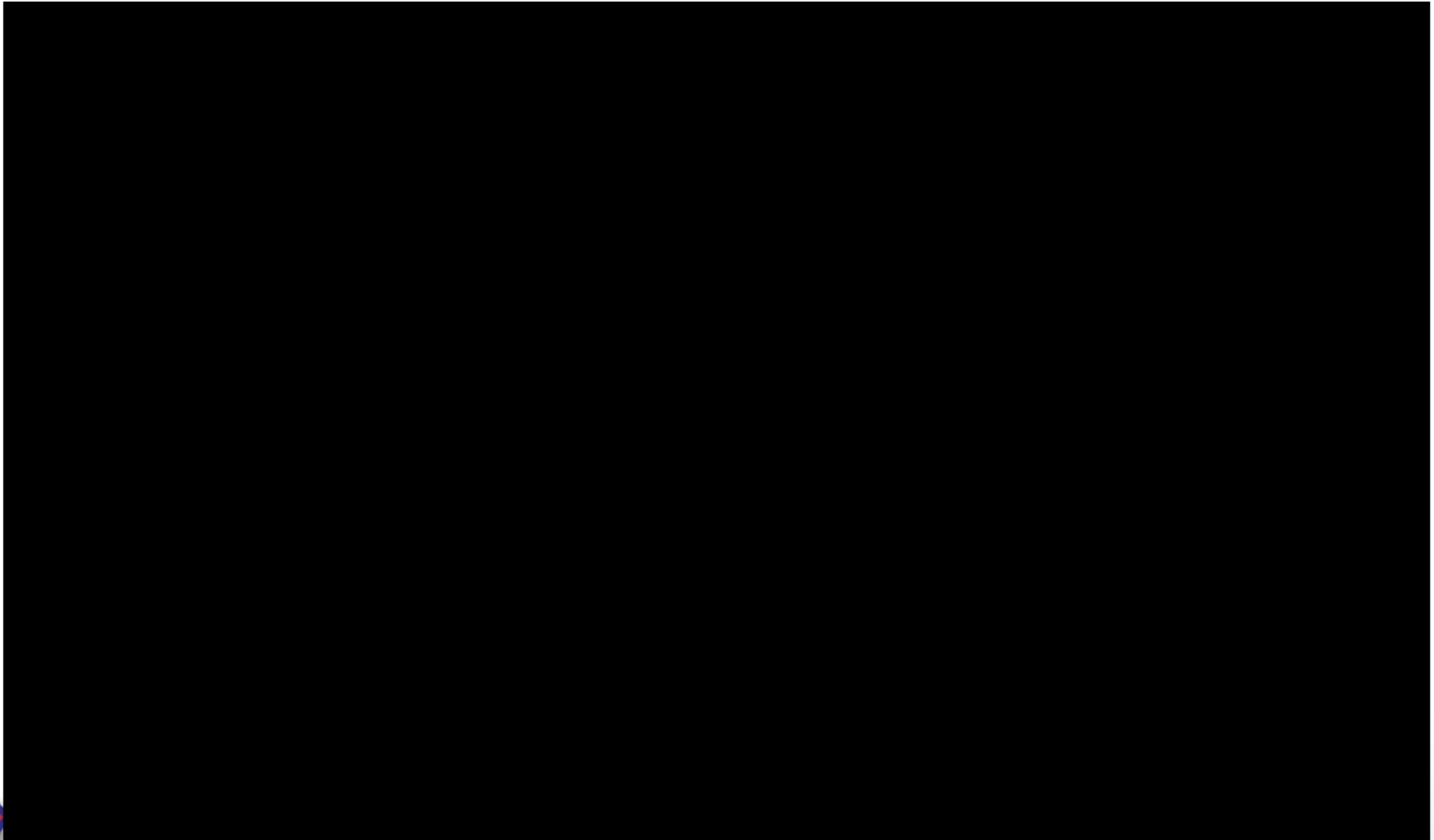
E1413

Threat #7: The Flash hates PlaylistLive: Answer 3B



E1414

Threat #7: The Flash hates PlaylistLive: Answer 3B

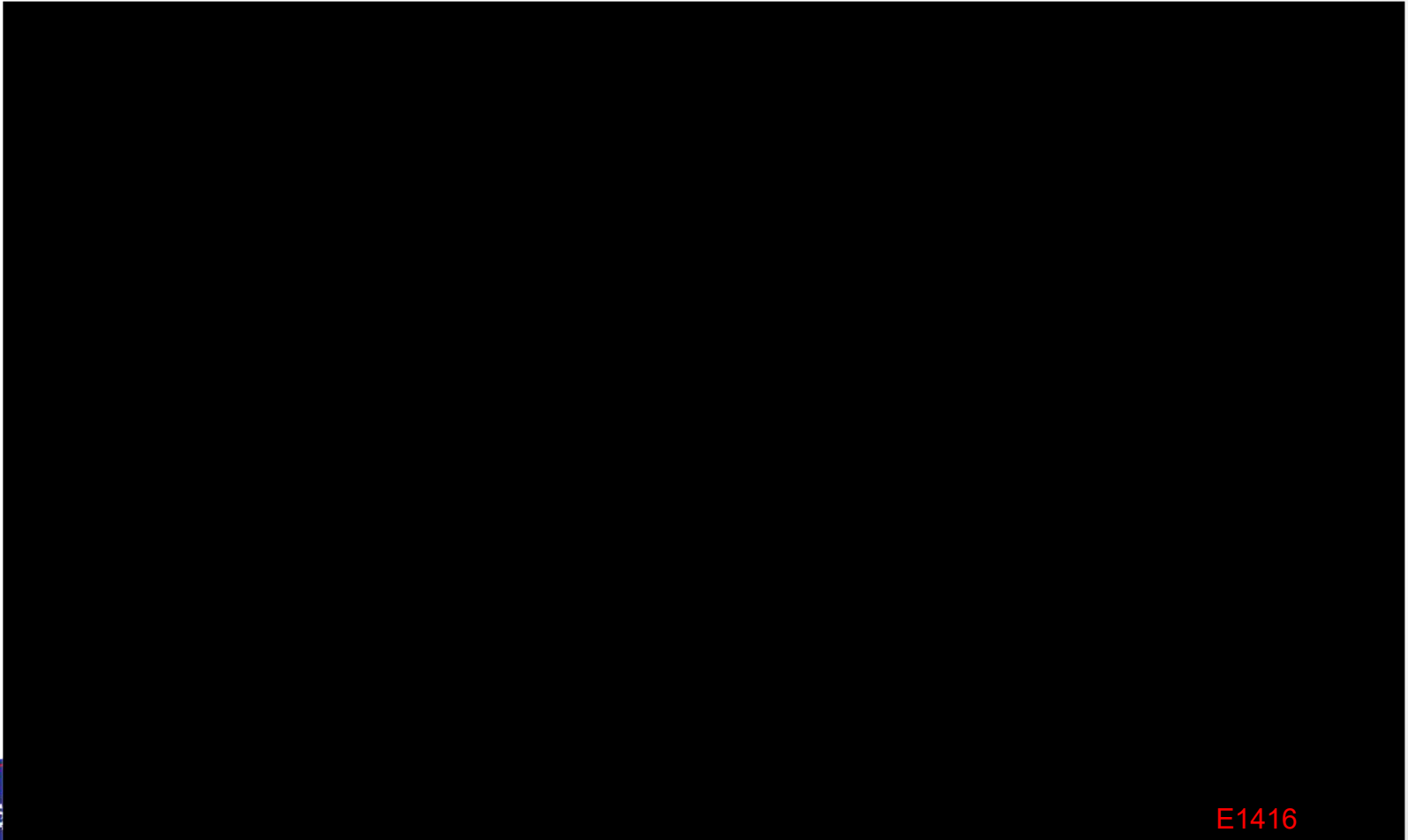


E1415



FOIA Requester

Threat #7: The Flash hates PlaylistLive: Answer 3B



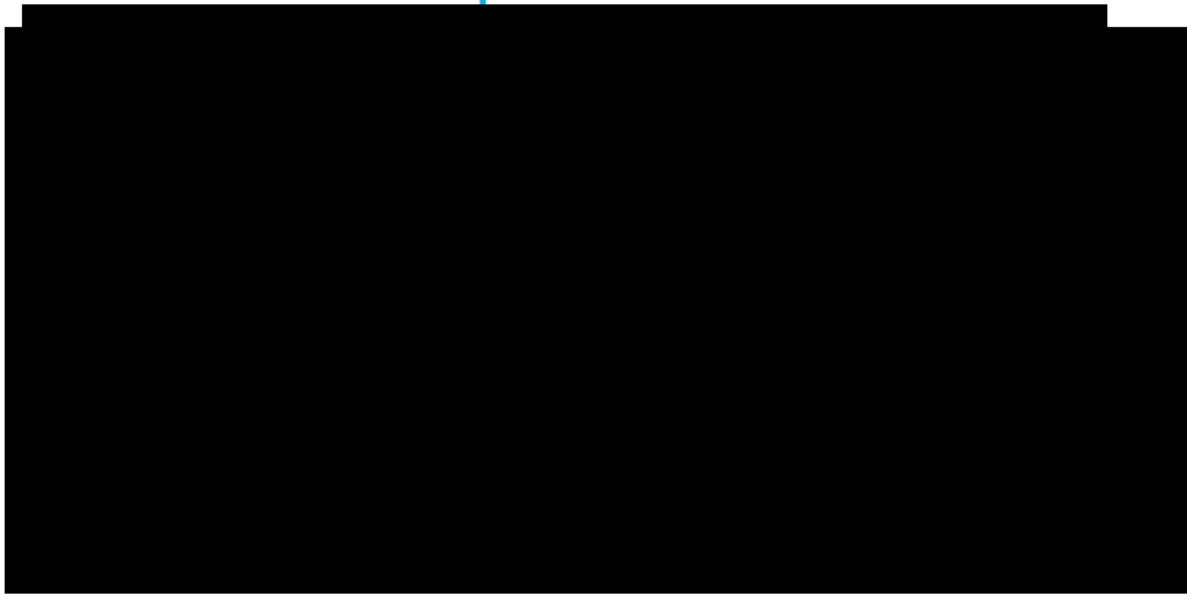
E1416



Requester

Threat #7: The Flash hates PlaylistLive: Answer 3B

[REDACTED] nd denies the incident. You call [REDACTED] from the numbers on his Account returns, and he admits that he made the calls due to “his problems”



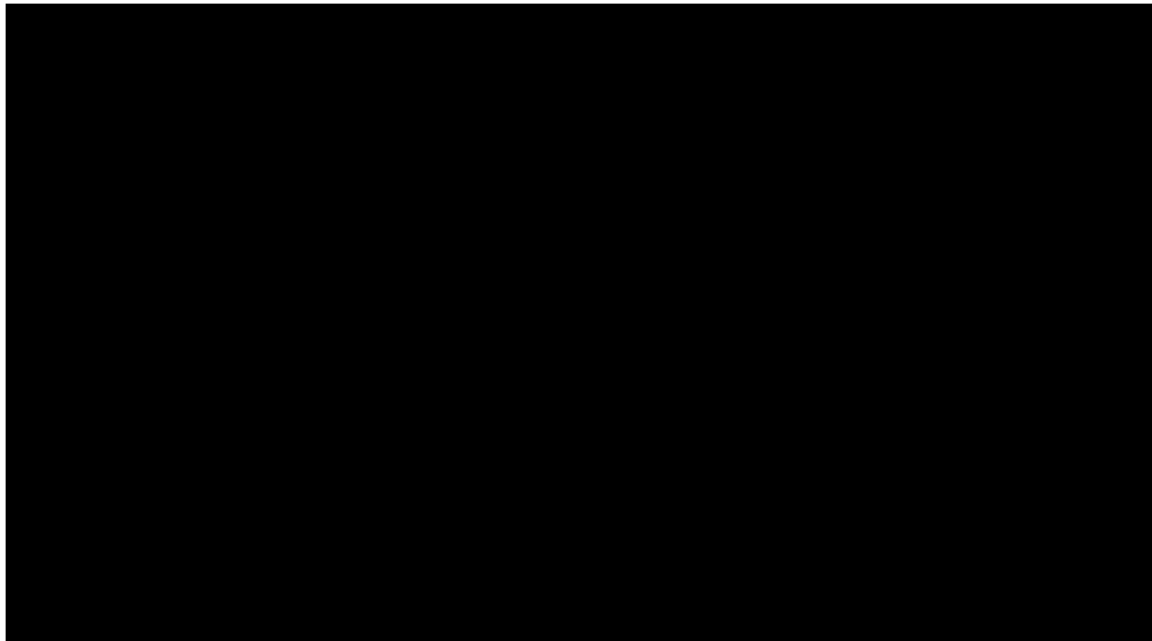
E1417



Requester

Threat #7: The Flash hates PlaylistLive: Answer 3B

You obtain a warrant for [REDACTED] and follow up
subpoenas are submitted to Facebook and the ISP
to serve as legal process



E1418



Requester

Use of Undercover Accounts

- Why create an Online Covert Account (Undercover account)?



E1419

Use of Undercover Accounts

Social Media has become a language of its own over the last two decades. As a form of communication, it is critical to successful Investigations. Things to consider:

- Undercover Accounts typically violate the User Agreement from social media platforms
- Intellectual Property is a thing
- Documentation is the fine line between focused investigations and targeted harassment.



E1420

Use of Undercover Accounts

There are two variations of an OCA, and they should be kept exclusive of each other. Overt accounts are used to monitor opensource social media, and Covert accounts are used for focused contact on predicated individuals.



E1421

Use of Undercover Accounts

Overt Accounts

- An Overt Account monitors social media that is otherwise publicly viewable. The three platforms this is most often seen in are:
 - Facebook
 - Instagram
 - Twitter



E1422

Use of Undercover Accounts

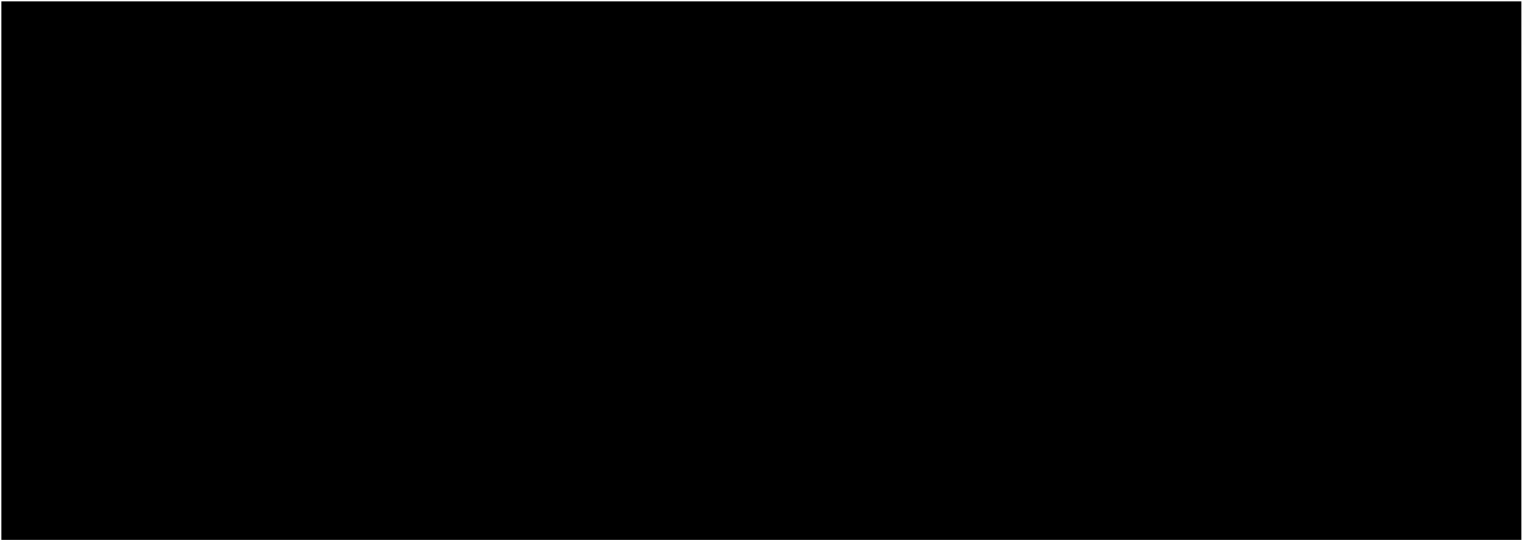
Covert Accounts

- A Covert Account is used for focused investigations. We gain information on bumping (contacting) subjects through a starting point(we need to have a reason). These starting points could include:
- IQ Reports
- Tips from Citizens
- Tips from Officers
- Social Media Aggregators
- Hashtags or Names from your experiences as a law enforcement Officer
- Gang Books and MPD Databases



E1423

Use of Undercover Accounts



E1424

MPD 106

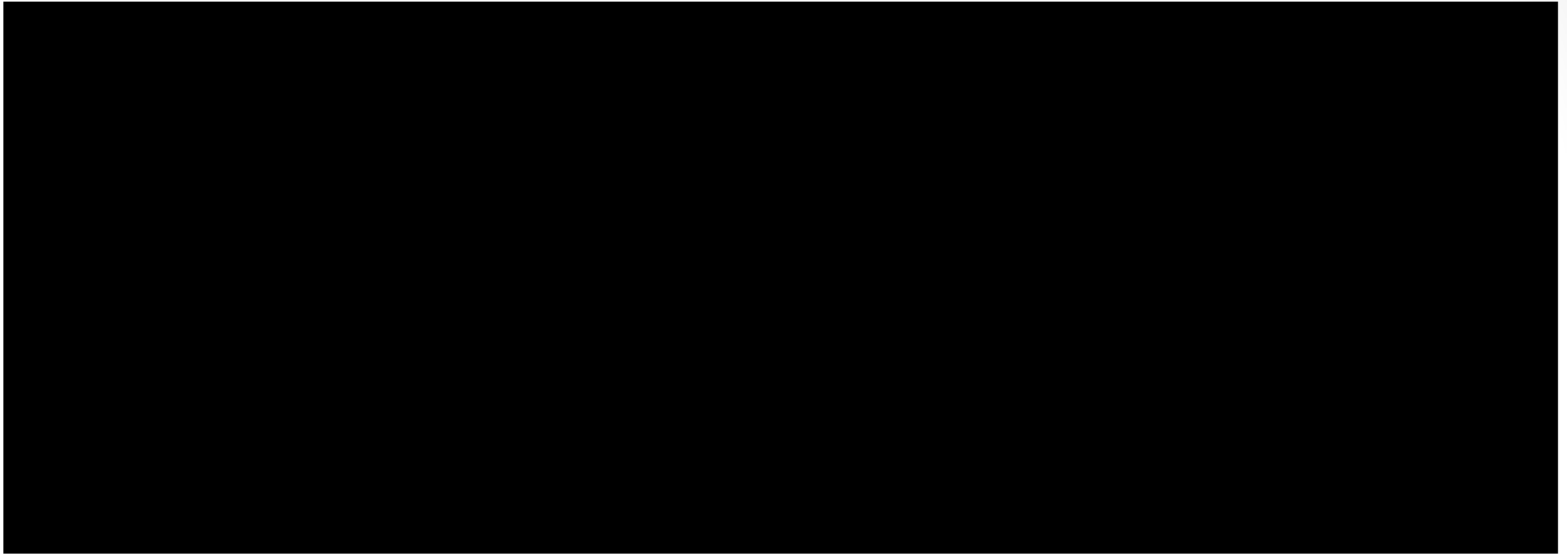
Use of Undercover Accounts



E1425

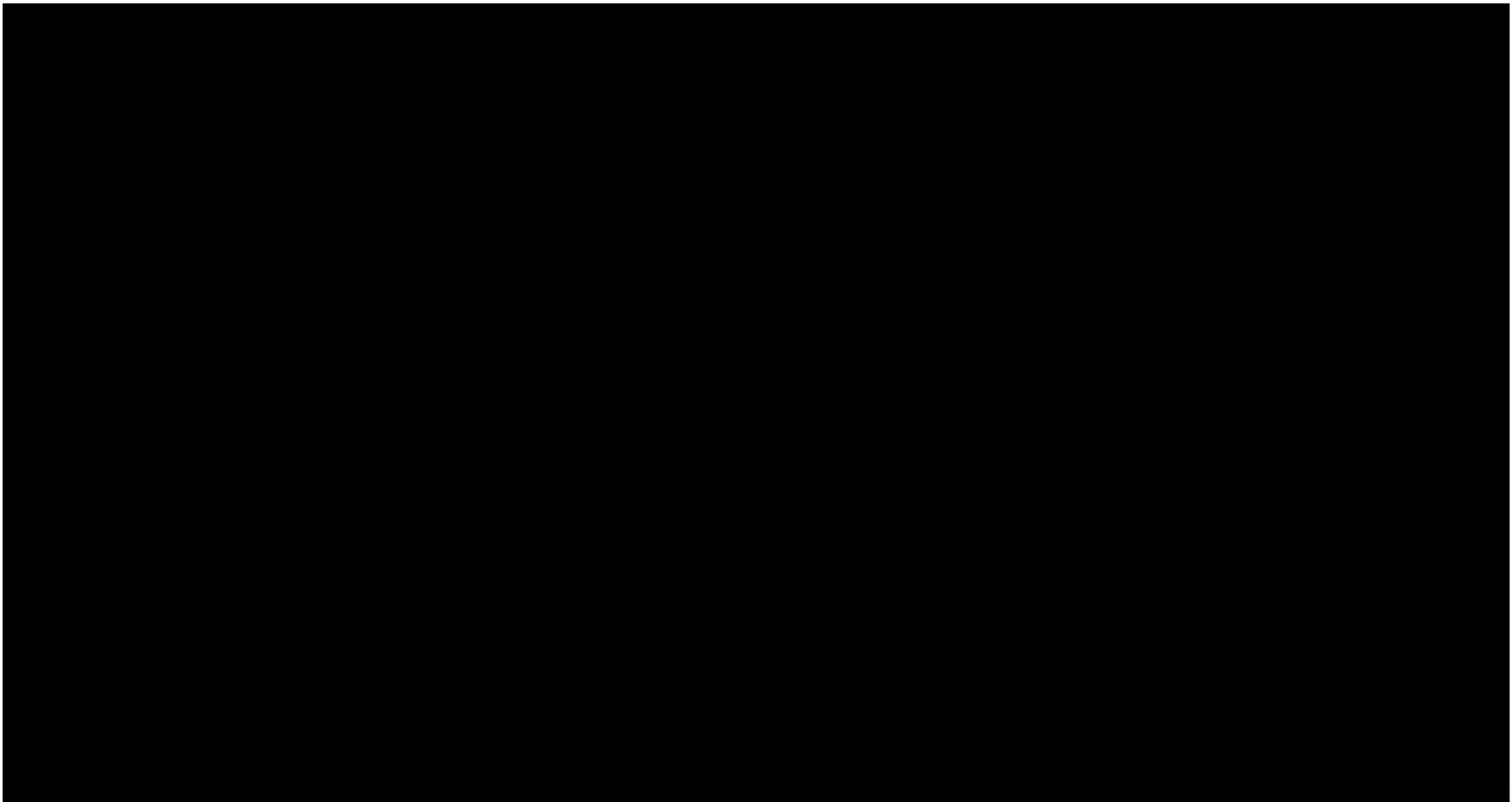
MPD 107

Use of Undercover Accounts



E1426

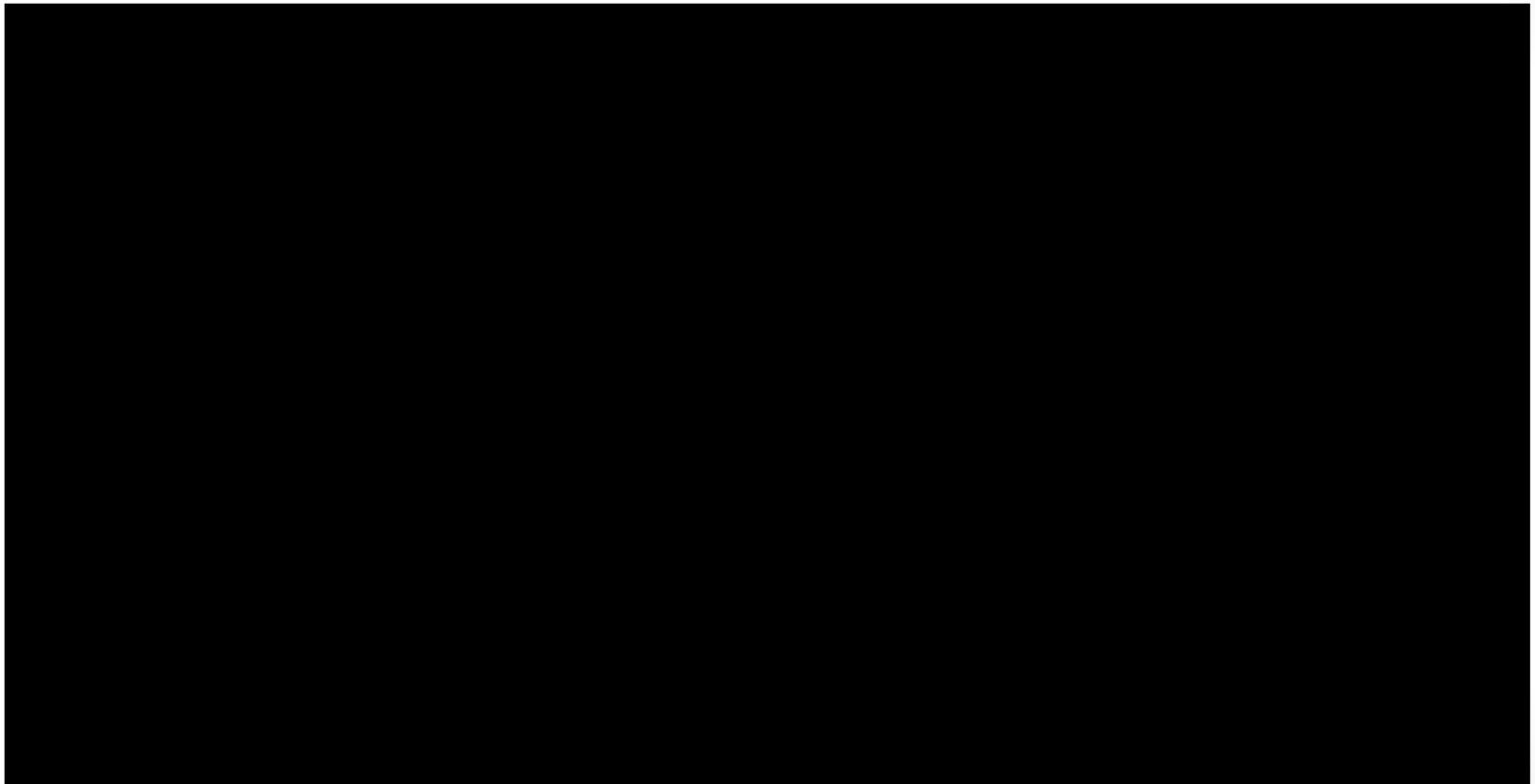
Use of Undercover Accounts



E1427

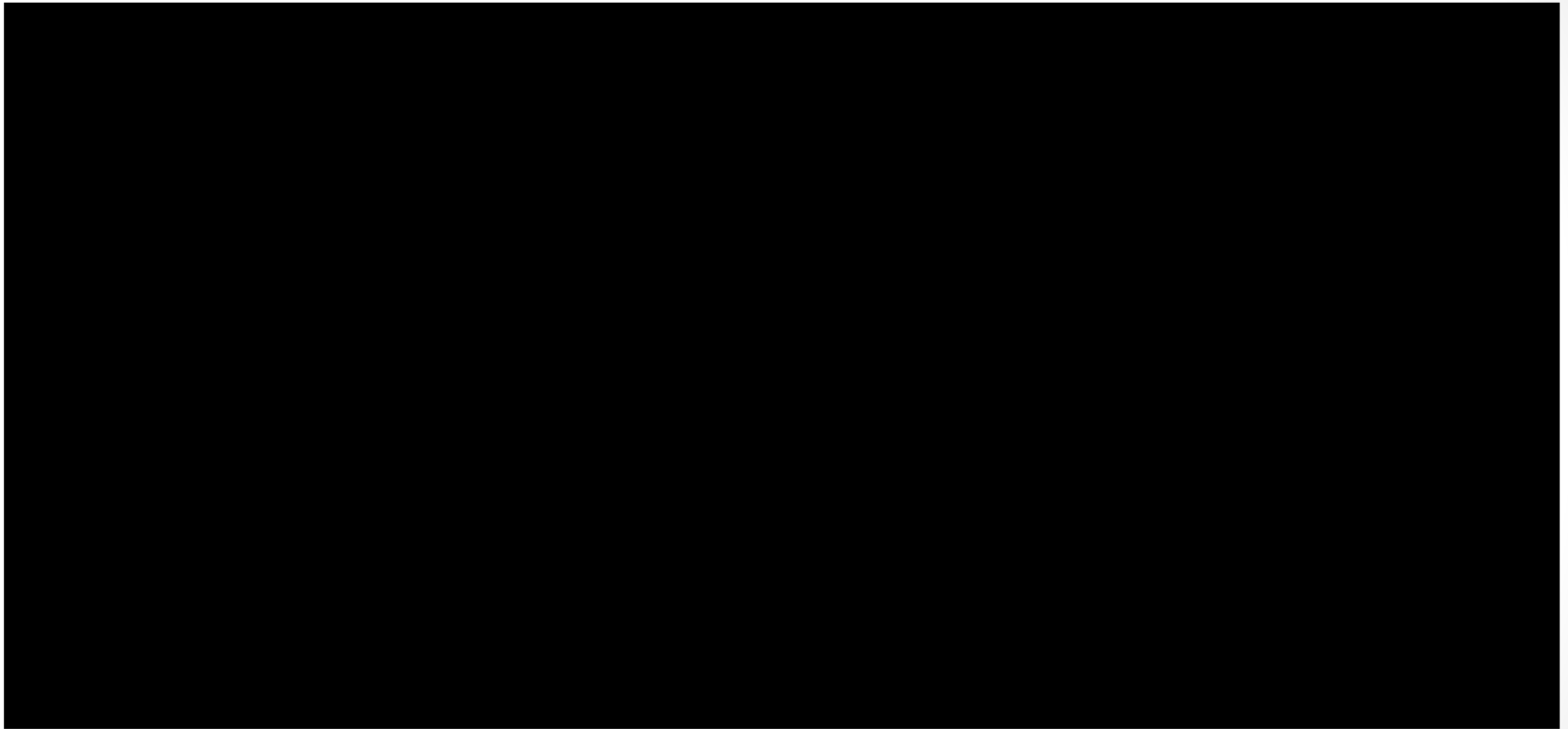
MPD 109

Use of Undercover Accounts



E1428

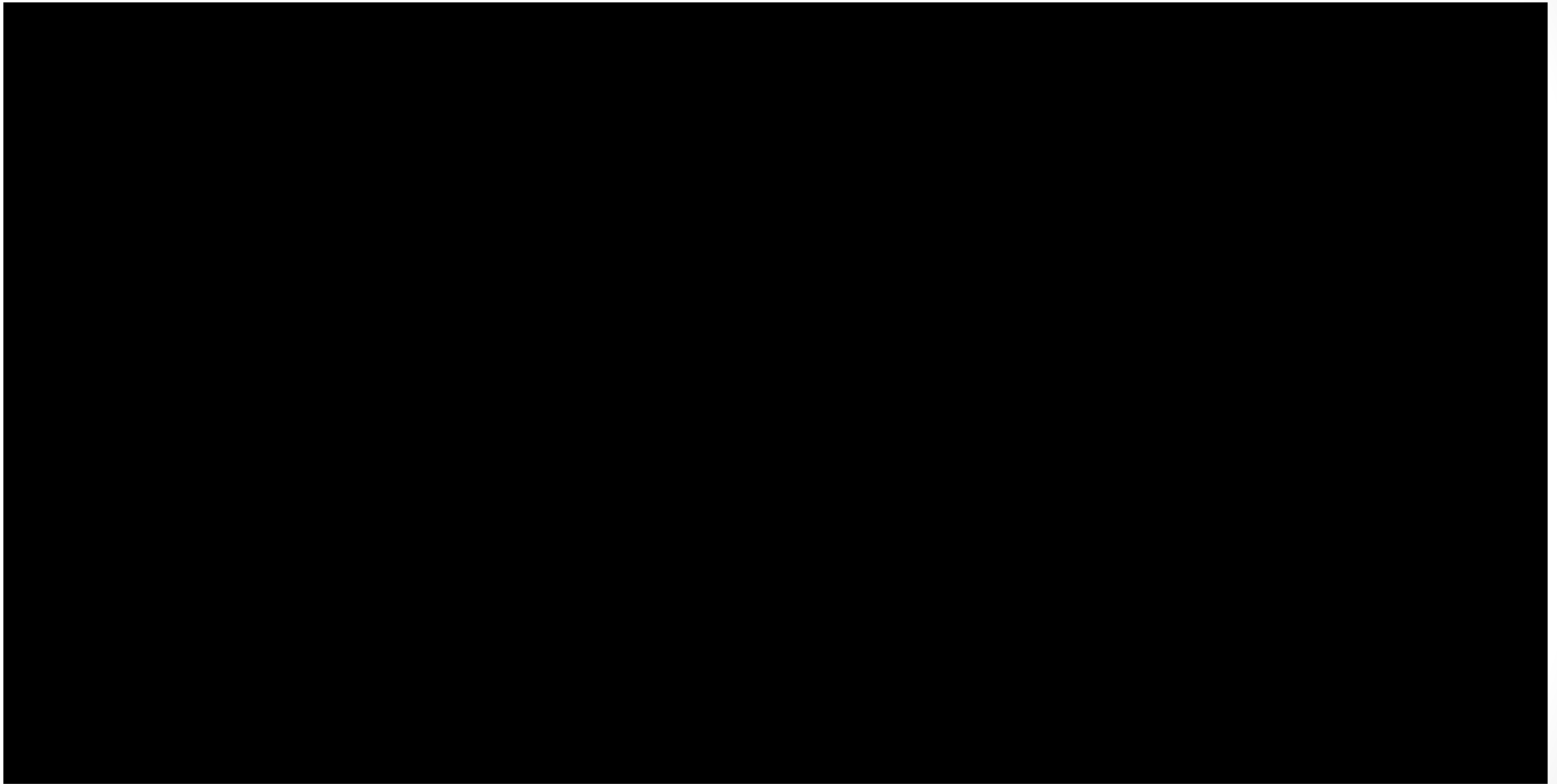
Use of Undercover Accounts



E1429

MPD 111

Use of Undercover Accounts



E1430

MPD 112

Use of Undercover Accounts

Building Your Accounts:

With overt Accounts, no contact should be made with subjects. These are simply made to view opensource platforms. Every search or viewing merits documentation.



E1431

Use of Undercover Accounts

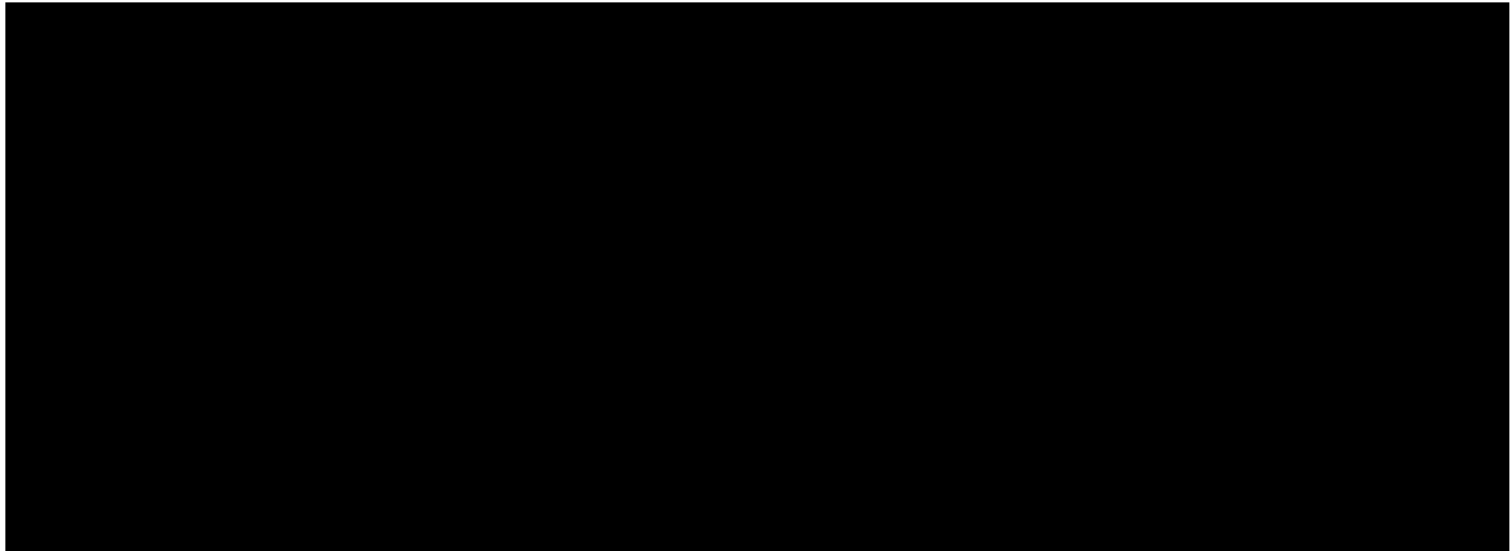
Building Your Accounts:

With covert Accounts, the end goal is an arrest. This may be done through an operation that introduces an Undercover or a Confidential Informant, or in the case of threats by way of a search warrant for the account.



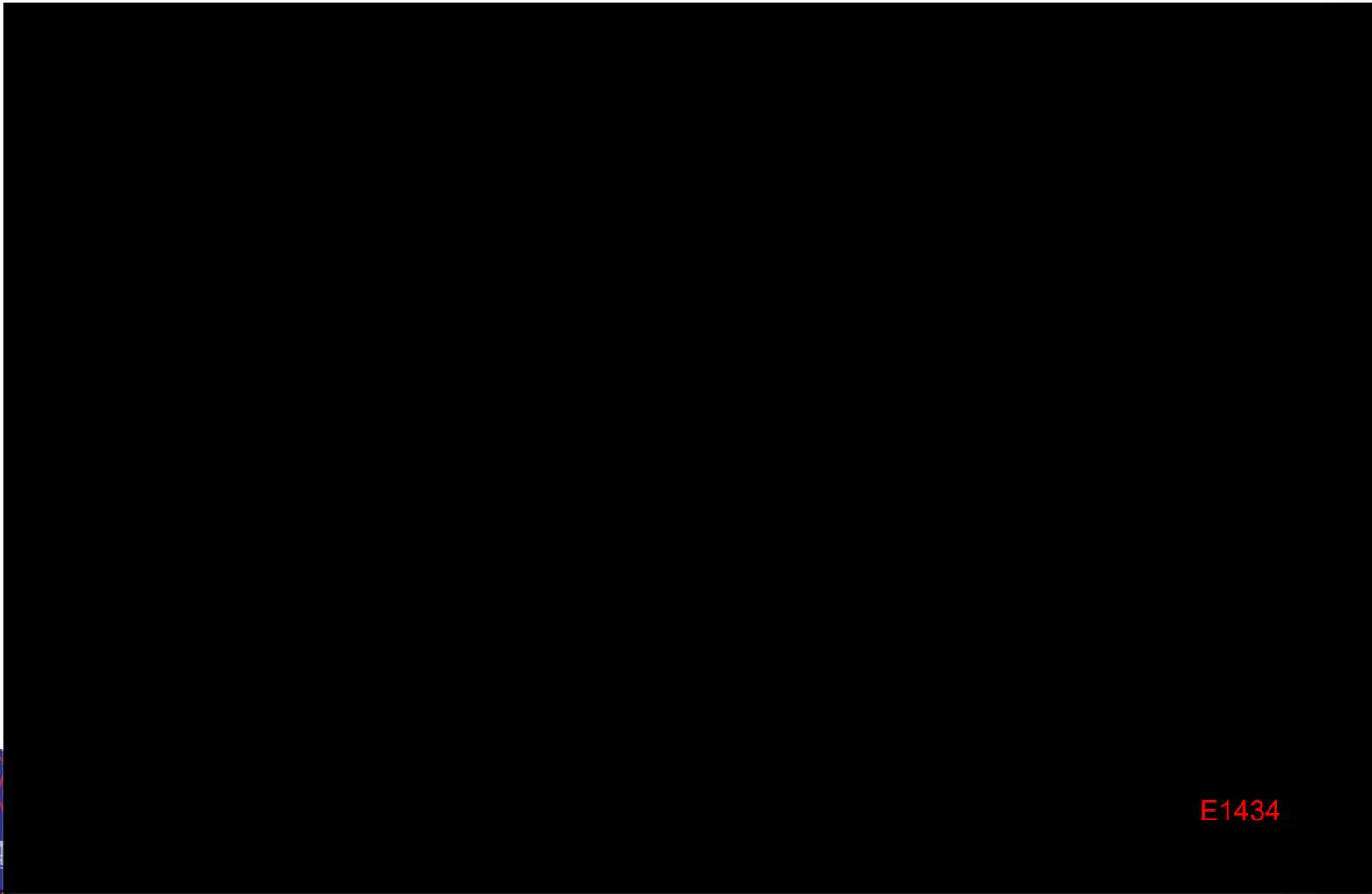
E1432

Use of Undercover Accounts



E1433

Use of Undercover Accounts

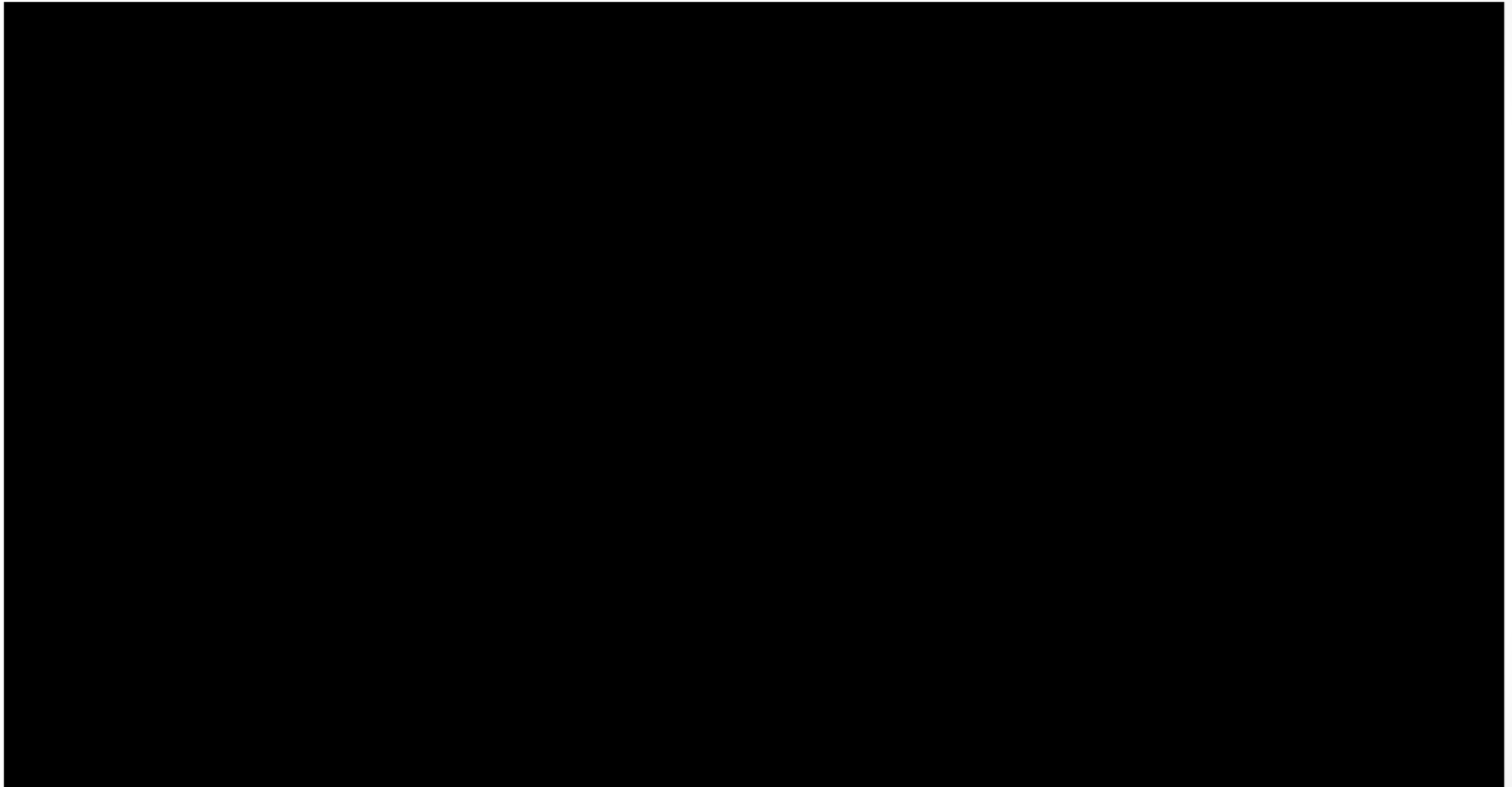


E1434



FOIA Requester

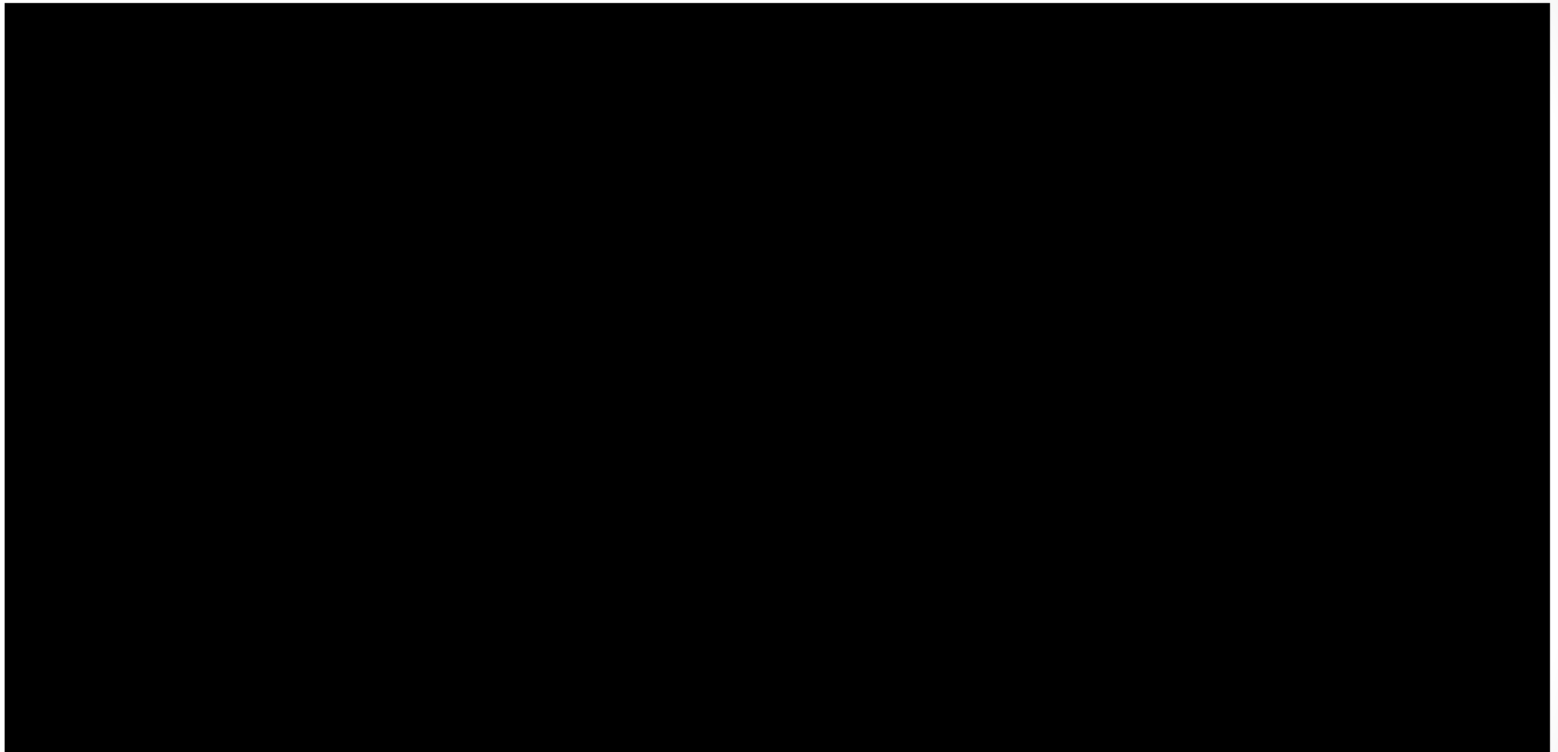
Use of Undercover Accounts



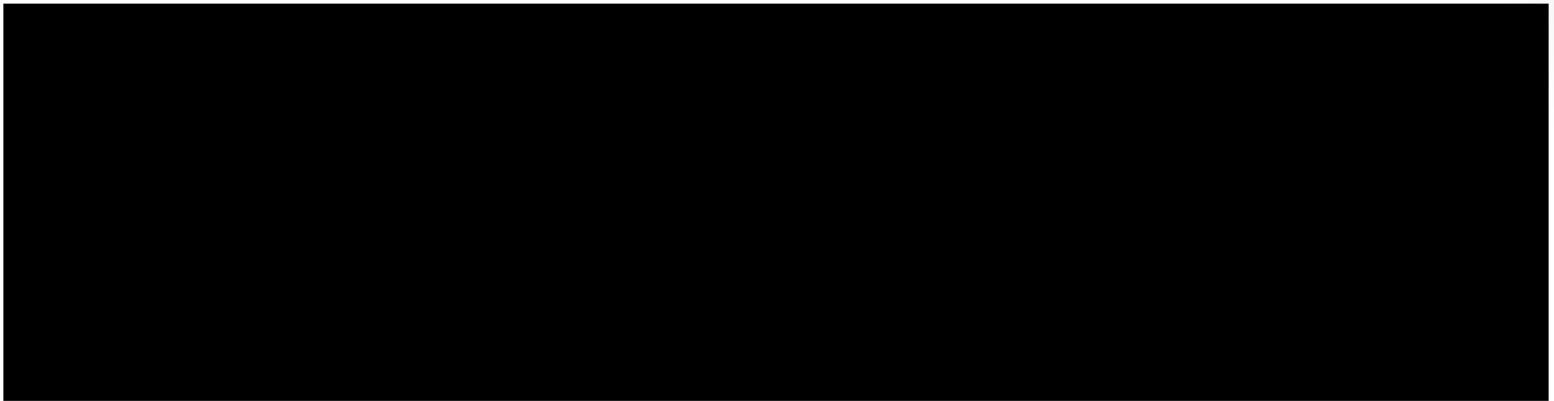
E1435

MPD 117

Use of Undercover Accounts



Use of Undercover Accounts



That's it, Amigos!

