
Monthly News and Commentary from ICJE

1 message

ICJE, Inc. <jimrechel@icje.org>
Reply-To: jimrechel@icje.org
To: pcalvert@faulkner.edu

Wed, May 11, 2022 at 8:33 AM



Footprints in the Digital Sand

Somehow, while doing digital research I ended up on a site for a Mobile, AL based wedding planning site called "Footprints in the Sand - Beach Weddings". As I am happily married, I started thinking about what a strange entry that will be in my internet History page.

With none of our kids discussing wedding plans, that may leave my wife wondering what's going on if she examines my History page, not unlike what Tiger's ex-wife did with his text histories - (I have removed all my golf clubs from the house, but my current wife still has her golf clubs so I'm on full alert).

(....My wife made me add the word "**current**" after proof reading this month's newsletter!)

If you read on, this month we are focused on all things related to OSInt (Open Source Intelligence) and related online identity issues. Hopefully you'll find some information you can use in your online research and investigative efforts. And maybe find some footprints in the digital sand!

Best regards,

Jim Rechel, Newsletter Editor
ICJE, Inc.
jimrechel@icje.org

Please feel free to email comments or suggestions. Thanks, Jim

"Officer Down"

A great awakening is occurring. Evil vs. Good has been with us from the beginning of time.

But the time has arrived for all of those who believe in the values that are so precious to a strong United States to stand against evil.

Celebrate those in our communities who seek to do good, and who honor our communities by their willingness to risk their lives for our safety.

As we honor those officers who have given the ultimate sacrifice, we must stand tall against the forces of evil that seek to destroy our country.

That is the greatest individual tribute we can give to the fallen officers.

The ICJE Board and extended staff owes a debt of gratitude that we cannot ever repay to all those Alabama officers, and those across our country, who have lost their lives in the line of duty. May their families find peace in the knowledge that they were loved by Him. May they Rest in Peace!.





Synthetic ID Fraud and Job Postings?

While conducting a fraud and security conference last week in West Virginia, one of the attendees from a bank approached me during a break and alerted me to a recent scam they had not experienced before. They have a newly opened position in their bank for an IT professional. They have not yet begun a formal job search via on-line sites but mentioned it to other IT professionals in the financial services industry.

Within 10 days, the IT Director began receiving resumes in his Inbox. As he began researching their backgrounds in detail, he discovered through extensive digging, that some of the resumes appeared to be from hackers posing as legitimate job seekers. While our conversation was too short for many more details, the banker saw enough evidence to convince him of the accuracy of the information. I was unable to verify it as of the deadline to send the ICJE newsletter out, but I thought I would pass it on as it fits the pattern of ID thieves and synthetic ID fraudsters.

He did tell me that one common denominator for the fraudulently submitted resumes was the desire to work remotely, which the bank now offers to some IT employees.

Through December 31, 2022, Experian, TransUnion and Equifax are offering all U.S. consumers free weekly credit reports through AnnualCreditReport.com to help protect against synthetic ID fraud. Synthetic identity fraud occurs when someone uses a combination of real and fake personal information to create an identity and commit fraud. For details go to "Read More".

[Read More](#)

Let's look into the most popular OSINT techniques used in

cyber security:

- Gather full names, job roles, as well as any known social media and software they use.
- Assess and monitor search engine information from Google (especially using Google Dorks), Bing, Yahoo, and others.
- Monitoring personal and corporate blogs, as well as evaluating user activity on digital forums.
- Identify various social networks used by the potential user or organization.
- Evaluate content available on social networks like Facebook, Google Plus, LinkedIn, or Twitter.
- Utilize people data collection tools like Pipl, who will help you to reveal a lot of information about individuals in one place, all together.
- Accessing old cached data from Google – often reveals fascinating information.
- Exploring old versions of websites to reveal the most important information using sites like the Wayback Machine.
- Recognize mail addresses, mobile phone numbers from social media networks, or Google results.
- Look for photographs & videos on common social photo-sharing sites, like Flickr, Google Photos, & more.
- Utilize Google Maps and other open satellite imagery sources to retrieve images of users' geographic location.
- Utilize tools like GeoCreepy to track down geographic location information to have a clear picture of the users' current locations.
- Utilize automated **OSINT tools** to retrieve information, such as Sunartek's OSINT Tools.
- Utilize popular OSINT extensions that include useful sources like OSINT Browser.
- Exploring of DNS Services, as well as domains, subdomains, and IP addresses utilizing our own SecurityTrails toolkit.
- Run port scanners against the target company server infrastructure to discover running services.
- Utilize tools to search for internet-connected devices like Shodan used by your target.

These are some of the most popular techniques you will find. However, after you've taken action towards carrying out OSINT research, you'll have plenty of data to analyze. That's when you will have to refine your results and carry a detailed search for all the necessary things you need & discard the rest.

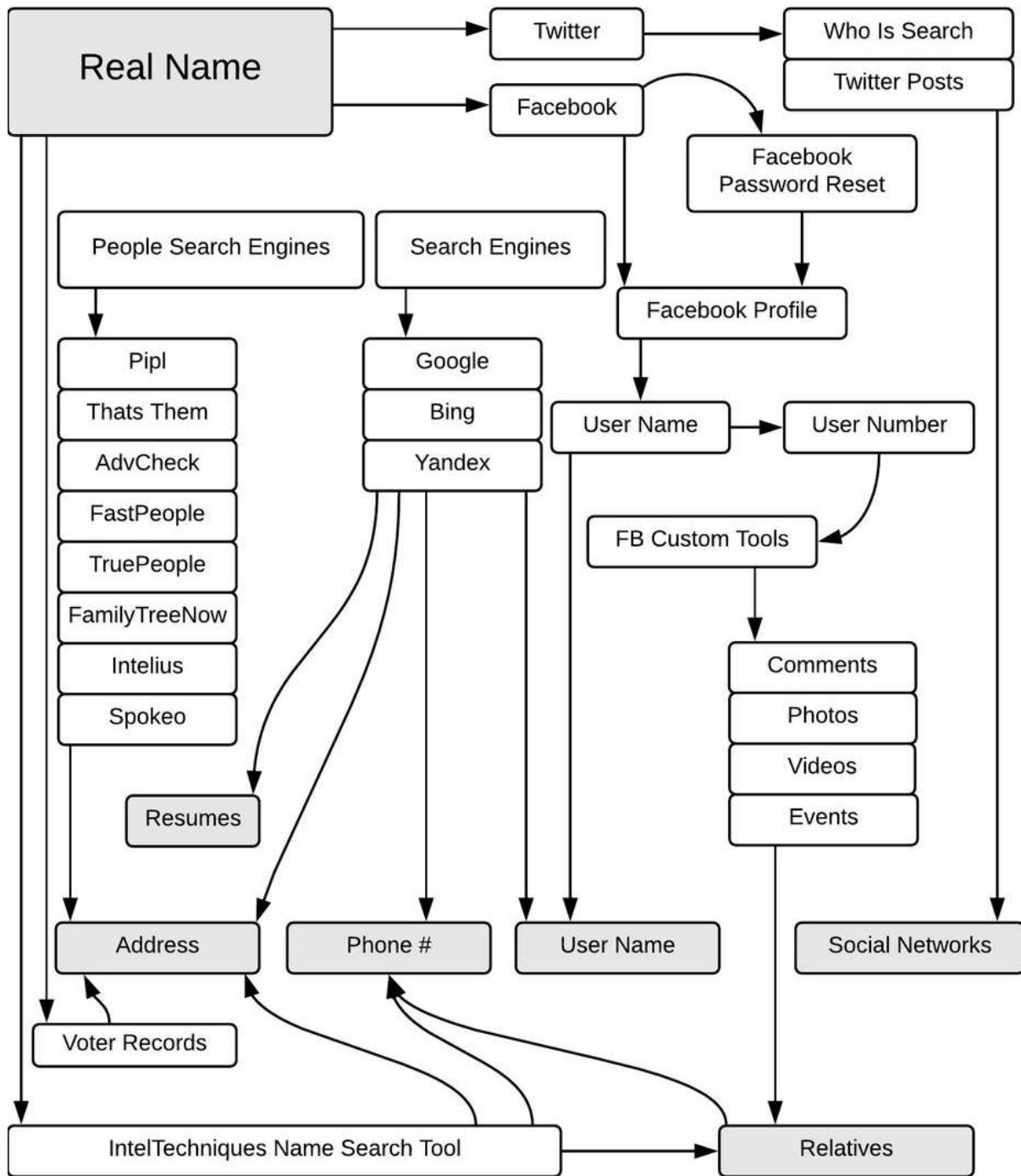
Source: [Osint Framework | How to use OSINT framework? - Sunartek Labs](#)



OSINT: How to Find Information on Anyone

Open Source Intelligence (OSINT) - is information gathering from publicly available sources and its analysis to produce an actionable intelligence. The scope of OSINT is not limited to cybersecurity only but corporate, business and military intelligence or other fields where information matters.

[Read More](#)



From: IntelTechniques.com OSINT Workflow Chart: Real Name

People search

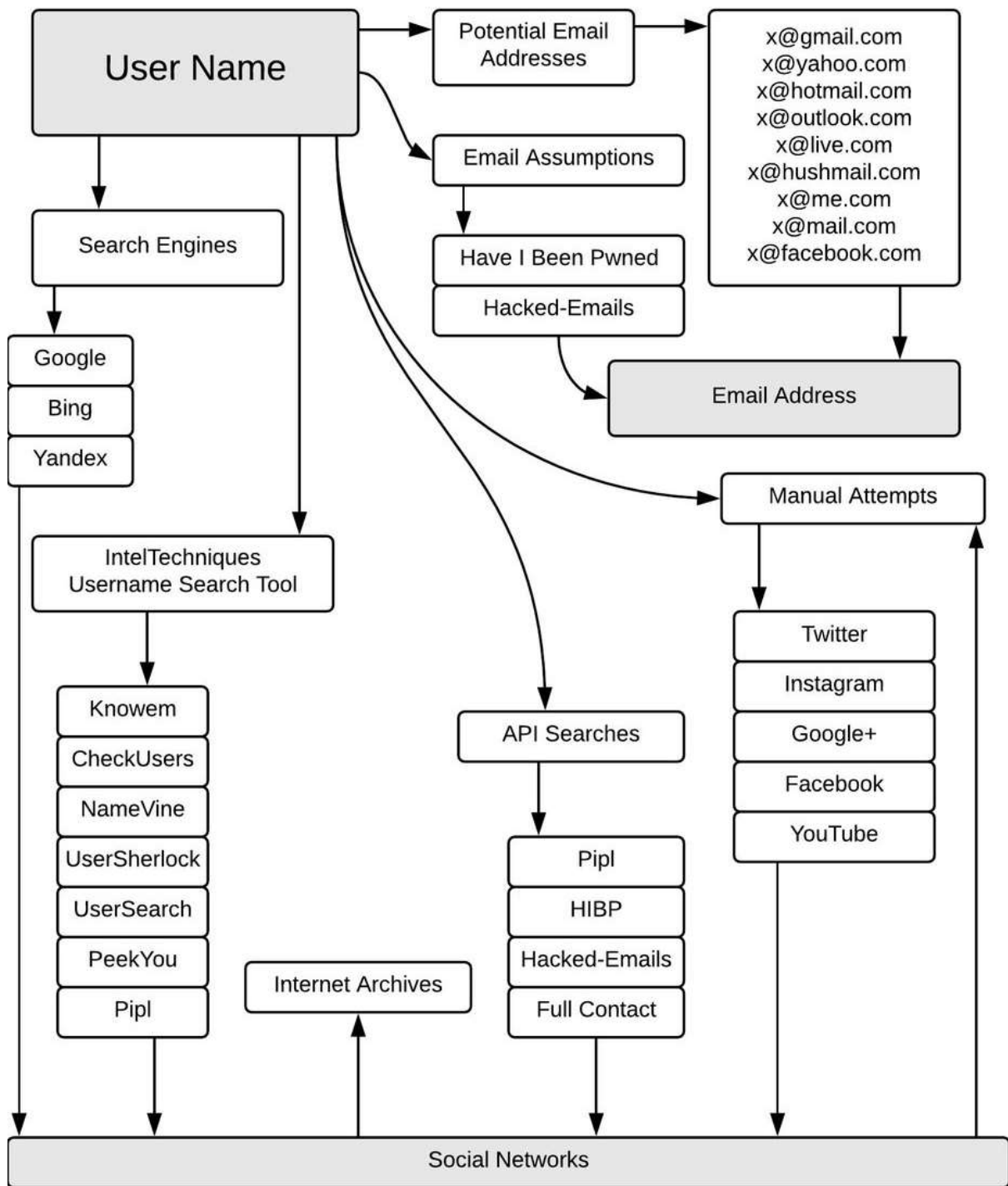
There are websites that specialize in people search which can be done providing a real name, username, email or phone number.

- <https://www.spokeo.com>
- <https://thatsthem.com>
- <https://www.beenverified.com>
- <https://www.fastpeoplesearch.com>
- <https://www.truepeoplesearch.com>
- <https://www.familytreenow.com>

- <https://people.yandex.ru>

People search websites allow to opt out, but after people remove themselves from listings, new search services appear with their records in them. The reason for that is the same dataset is bought and used by different services. Some companies own those datasets and even if on one of their websites a person removes the listing, on the new domain the old data is repopulated again so the previously removed profile reappears in the search.

Consequently, if people did a pretty good at cleaning their stuff up you just have to wait for a new database to appear. One of the methods to find people that opted out is to go the people search service, find a unique paragraph, do a quoted Google search on it and find all of the domains that the company owns. There are chances that information your target removed from site A is now on site B.



From: YIntelTechniques.com OSINT Workflow Chart: User Name

First, we have to find a username. Usually, it is a name plus surname combination or derived from the email, domain name of the website the person uses or owns.

Start with data you have and do a reverse lookup towards what you need. Obviously, the simplest way is to Google any relevant data known to you at the moment and try to find any pages with the username.

Also, you can use special websites that do a reverse username search, like socialcatfish.com, usersearch.org, or peekyou.com.

A Great PowerPoint on OSInt



Developed by Reynaldo Gonzalez, it is available by typing in the title shown in the image above to your favorite Search Engine, or going to:

<https://cybersecmentorship.org/wp-content/uploads/2020/06/OpenSourceIntelligence-OSINT.pptx>

While it is titled for Cybersecurity, a lot of the information contains valuable material and links for all investigators, public and private. Some of the links are dead when I tested them, but most of them can be resolved by going to the general entity and relinking to current information. The PPTX was developed in 2019, but has great information.

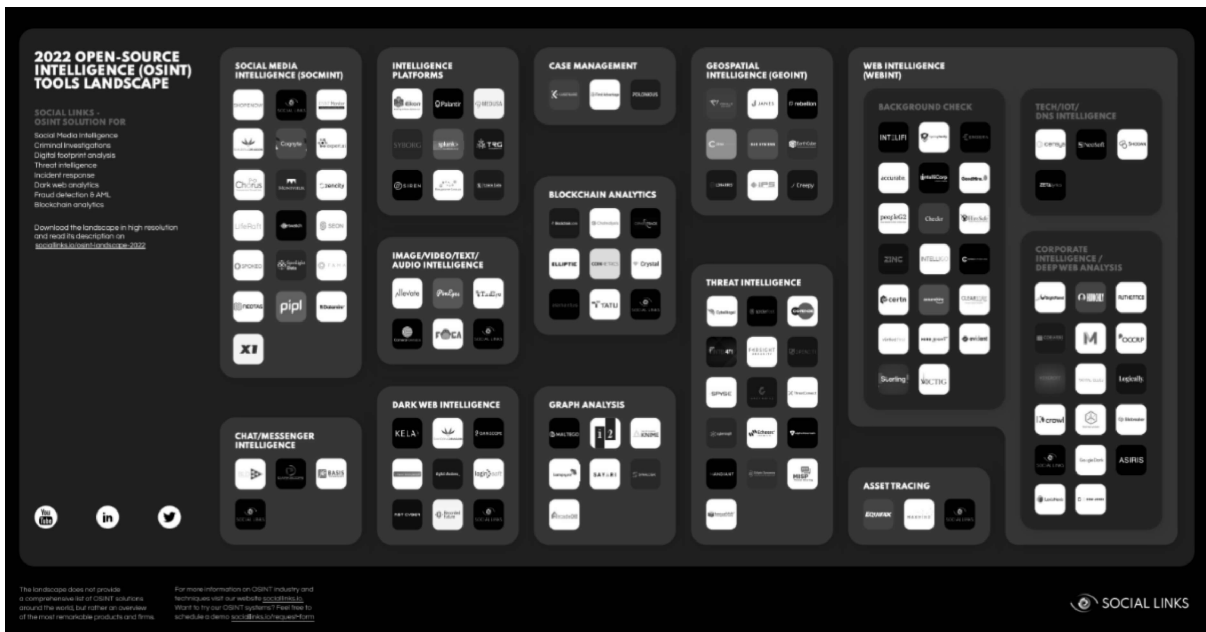
Here are Top 14 OSINT Tools as of 2021:

1. **OSINT Framework**
 2. **theHarvester**
 3. **SHODAN**
 4. **Searchcode**
 5. **Nmap**
 6. **SpiderFoot**
 7. **ExifTool**
 8. **Metagoofil**
 9. **Aircrack-ng**
 10. **Censys**
 11. **Google Dorks**
 12. **ZoomEye**
 13. **Maltego**
 14. **BuiltWith**
-

Source: [Top 14 OSINT tools as of 2021 | Knowledgenile](#)

Social Links

The Social Links website has a great graphic available for download that provides a general guide to sites sorted by their type.

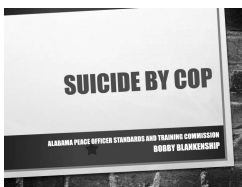
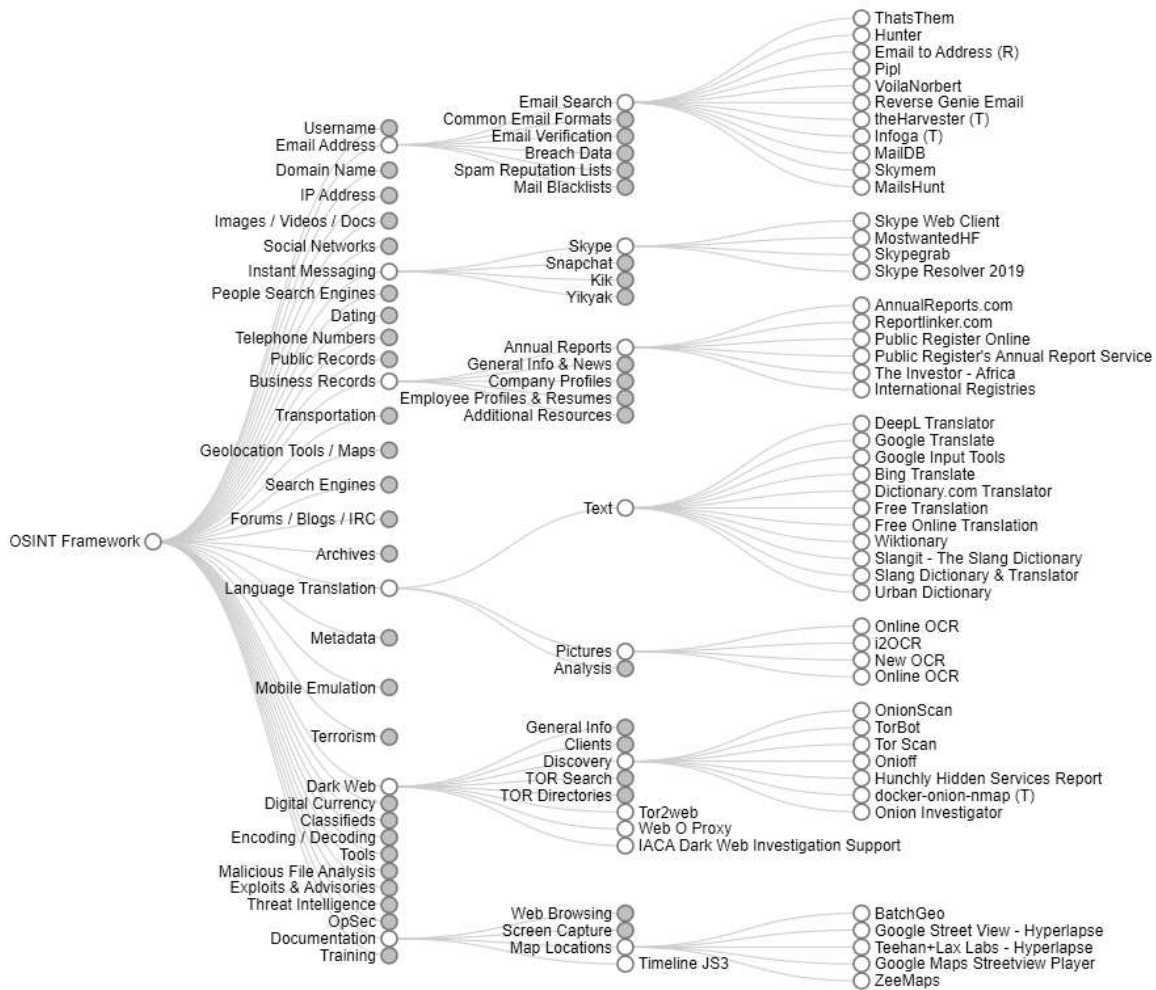


Source: [OSINT_landscape_2022.pdf](#) (mcusercontent.com)

OSInt Framework

Shown below is a sample page of the website OsInt Framework which is a really interesting tool. On its website you can click on the blue circle and it expands to additional resources for the respective topic. (Example shown below.)

To use the site visit: **OSINT Framework**



"Suicide by Cop" Training Session

Date: May 24, 2022

Meets: Tu from 9:00 AM to 4:00 PM

Location: Center for Lifelong Learning 157-158

APOST Hours: 6.00

Cost: \$0.00

Go to the ICJE Website (link if needed in next section) to link to the registration page for this training **conducted by Bobby Blankenship, APOST Commission and ICJE Board Member.**

Audience: Law Enforcement Officers

Description: Have you ever encountered a person that seemed to want to die? Did they force you to engage them? Let's talk about what your next stage may have been in your encounter. Were you forced into an Officer involved shooting? Let's discuss this type of encounter where law enforcement is forced to use deadly force. We will discuss the following topics.

- Know what suicide by cop means and some statistics that illustrate the frequency of this type of incident.
- Understand sBc typology
- Identify “suicide by cop” indicators
- Recognize some key signs that may be observed during and after an incident by which they came to realize they were in a “suicide by cop” situation

Training Information from ICJE Website

Visit the ICJE Website

May 12, 2022 - ICJE Child Sex Trafficking Training for First Responders - Montgomery, Alabama

May 24, 2022 - ICJE Suicide By Cop - Montgomery, Alabama

May 26, 2022 - ICJE Psychological Profiling - Montgomery, Alabama

June 6-10, 2022 - FBI LEEDA Supervisor Leadership Institute - Huntsville, Alabama

August 1-5, 2022 - FBI LEEDA Supervisor Leadership Institute - Fultondale, Alabama

August 22-26, 2022 - FBI LEEDA Managing and Conducting Internal Affairs Investigations - Huntsville, Alabama

August 31-September 2, 2022 - 2022 LECC Conference - Orange Beach, Alabama
Pending DOJ approval. Save the date

September 26-30, 2022 - FBI LEEDA Media and Public Relations - Decatur, Alabama

November 14-18, 2022 - FBI LEEDA Command Leadership Institute - Fultondale, Alabama

January 9-13, 2023 - FBI LEEDA Supervisor Leadership Institute - Columbiana, Alabama

February 27-March 3, 2023 - FBI LEEDA Executive Leadership Institute - Fultondale, Alabama

March 13-17, 2023 - FBI LEEDA Command Leadership Institute - Columbiana, Alabama

May 15-19, 2023 - FBI LEEDA Executive Leadership Institute - Columbiana, Alabama

Other Training Opportunities:

AUM Continuing Education and Community Engagement

FEMA Emergency Management Institute

APOST Law Enforcement Training Academy - Tuscaloosa

Jefferson County Sheriff's Department Training Center

Northeast Alabama Law Enforcement Academy

Ozark Police Department Training Division

University of North Alabama Public Safety Institute

[Link to Visit the ICJE Website for Registration and More Dates](#)

Additional Resources



Mobile Forensics - Law Enforcement Cyber Center

Mobile devices have become an integral part of peoples' daily lives, and as such, they are prone to facilitating criminal activity or otherwise being involved when crimes occur. Whereas computers, laptops, servers, and gaming devices might have many users, in the vast majority of cases, mobile devices generally belong to an individual.

[Read More](#)

Thought of the Month

Source: **Sergeant James Timothy Chapin (Officer Down Memorial Page)**

I Heard a Siren for the First Time Today

I heard a Siren for the first time today

What made it different were my thoughts have changed

Over my life it was always the same, someone had an accident, committed a crime, or needed help in some way

It's as if my eyes were opened, as I heard them say

"The man in blue died today."

I heard a Siren for the first time today

Never will I hear it, in quite the same way

For when the sound pierces the air

My attention turns to offer a prayer

To protect the man answering a plea

From another asking, "Please come to me."

My thoughts are for his safety, and family I pray.

I heard a Siren for the first time today.

Dedicated to the memory of Sergeant Timothy Chapin, Chattanooga Police Department who died in service on April 2, 2011, God truly blessed us with your presence.

Richard L. Cox, Sr

Reprinted with permission

ICJE, Inc. | P.O. Box 293, Montgomery, AL 36101

[Unsubscribe pcalvert@faulkner.edu](mailto:pcalvert@faulkner.edu)

[Update Profile](#) | [Constant Contact Data Notice](#)

Sent by jimrechel@icje.org in collaboration with



Try email marketing for free today!