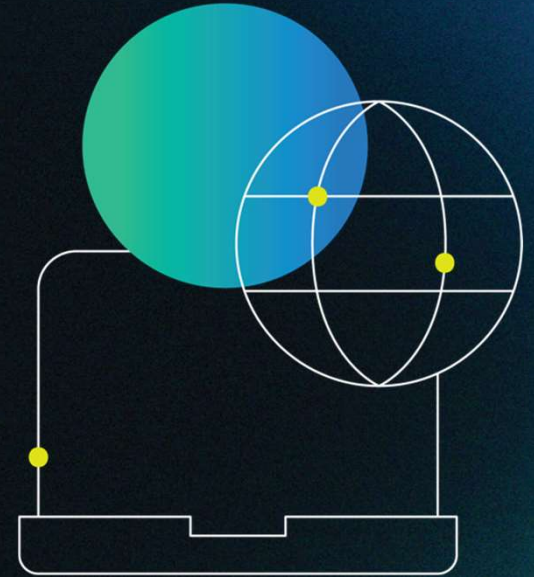




MAGNET
VIRTUAL SUMMIT
2023

Growing in Digital Forensics – Practical Mentorship and Resources



Jessica Hyde

#MVS2023





#MVS2023

MEET JESSICA

FOUNDER & OWNER, HEXORDIA

- Adjunct Professor, George Mason University

Previous:

- Director Forensics, Magnet Forensics**
- Basis Technology**
- Ernst and Young**
- American Systems**

DFIR Review, Chair

FSI: Digital Investigations, Associate Editor

HTCIA IEC, 2nd VP

SWGDE, Member

OSAC, Member



Value of Mentorship



Ask Yourself

- What do you plan to get out of mentorship?
- Has mentorship been of value to you?
- What are you looking to improve?



Every stage of your
career: Mentor and
Mentee





What is in it for a
mentor/mentee

Mentors can help with

- Goal Setting
- Resume reviews
- Building portfolio
- How to get noticed
- Skill growth identification
- How to produce something
- How to grow
- Connections
- Resources



Types of Mentorship

Two types of Mentorship

- Formal
 - Employer assigned
 - Part of a program
 - External mentor with formal relationship
- Informal
 - No official relationship
 - Folks you seek advice from
 - Often bidirectional



Internal Employment Mentorship

- Often assigned
- May be part of your annual review process
- Can be your advocate for reviews/promotions/adverse actions
- Navigates workplace politics
- Can be excellent – takes initiative or can be mediocre





Practical Mentorship

Providing structure to mentorship



Where to start

- Resume Review
 - Have mentee send BEFORE Meeting
 - I request this as a starting point when I meet with a mentee
 - Allows me to get to know them (OSINT as well)
 - Draft questions about areas that I am curious if they are skilled?
 - Scripting languages, tools, certifications
 - Folks have trouble talking about themselves



First Meeting (30-45 min)

- Open ended questions to get to know them
- Go through areas to update resume and provide feedback
 - (1st Action item for next meeting)
- Ask them about their goals for mentorship
 - Draft personal/professional goals (2nd Action item for next Meeting)



Second Meeting (45-55min)

- Resume updates sent ahead of meeting
- Discussion about frequency of CV updates (monthly at most)
- Determine THREE Goals based on meeting
- Determine schedule of frequency for meeting



Goal Setting

- Three goals for the period (6 months to 1 year)
 - Learn a skill (ex: Python, YARA rules, Cloud)
 - Obtain a certification
 - Find a role
 - *Public contribution*
- Be specific
- Based on Passion areas (or figuring them out)
- Base goals on needs or roles desired



Maintenance Meetings

- Actions to goals
- Missed opportunities
- Help please
- Next steps



Actions to
goals



The image features a teal background with several puzzle pieces scattered across it. A vertical white line is positioned on the right side of the text. The text 'Missed opportunities' is written in white, sans-serif font, centered vertically and horizontally relative to the left side of the line.

Missed
opportunities

Help, please



The background is a teal color with a complex geometric pattern of overlapping lines and shapes, creating a sense of depth and movement. A thin white vertical line runs down the center of the image, separating the text on the left from the abstract pattern on the right.

Next steps

Check-ins (15 min)

- 1) Goal Review
- 2) Mentee answers:
 - What have I done towards my goal?
 - What are missed opportunities towards my goal?
 - How can my mentor help me?
- 3) Mentor Answers
 - How have I observed you meeting goal
 - What are areas for refinement
 - How can I help the mentee
- 4) Draft Action Steps

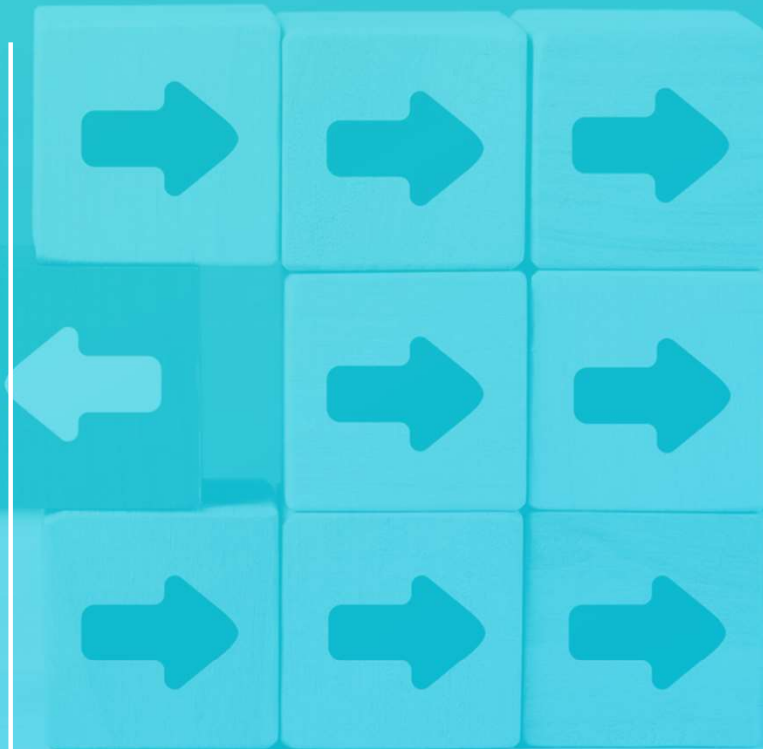


Create Action Items from Goals

- Learn a Skill
 - Find a program of study for the skill
 - Make measured goals for progress and a time for completion
- Obtain a cert
 - Research roles and certs they require
 - Determine study plan
 - Register for cert
 - Practice tests
- Find a role
 - Prep resume
 - Identify skill gaps
 - Look at network
 - Figure out where to look for roles
 - Application goals



Goals
Staying
consistent
and showing
up



Goal Adjustments

- Regular intervals
- Longer session to see if goals are still a good fit
- Adjust and make more specific
- Adapt to changes from learnings or life
- Ensure they are measurable
- SMART
 - Specific, measurable, achievable, relevant, time-bound





Doing the homework





Career Stages

DFIR Veterans and new folks need mentorship





Practical Mentorship



Folks Looking for Mentors

- Students
- Career switchers
- DFIR Veterans looking for new roles
- LE/Military transition to IR
- Folks moving from the SOC



Student

- Great research colleagues
- Promote their work
- Introduce them to folks
- Help push boundaries to get them to promote themselves
- Skills to learn



Career Switcher

- Articulating cross- industry relevant skills
 - Technical
 - Networking
 - Troubleshooting
 - Soft skills
 - Briefing executives
 - Customer service
 - Writing Experience





Camille



Transition (DF > IR)

- Often LE and Military finishing their “first” career
- Sometimes ready to transition out of LE
- Often times concerned about Skills Gap
- Employers sometimes underestimate!
- How to get noticed in industry and stand out



Folks moving from the SOC

- Self-advocacy
- Networking withing the organization
- Translatable skills to demonstrate on resume
- Hands on exercises or research to demonstrate
- Building a portfolio



Veterans looking for new roles

- Salary negotiations
- People leader vs technical contributor
- Connecting people
- Can be on learning how to balance life/work



Finding a mentor



What is in it for a mentor/mentee

- Advice
- Connection
- See the things you are missing!
- Help you prepare
- Someone in your corner
- Gas them up!
- Provide critical feedback



Reaching out to a possible Mentor

- Don't be discouraged
- Find someone doing the thing you want to be doing
 - Next step or many steps away!
- Offer to help them with research, collaboration, etc.
- Make a specific request
- Share information
- Do the homework!



Mentors sometimes seek out mentees

- See someone who has potential
- Excited to see where they can take it with just one more step
- Sometimes you identify folks you know can take it to the next level





Elizabeth

Formal Mentorship Programs



Programs that exist

WiCyS

Share the Mic In Cyber

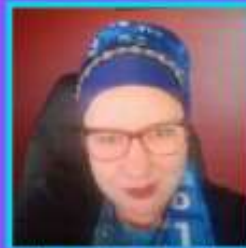
Play Like a Girl

Magnet Mentorship Day

Resume Review Programs at conferences



Join us on October 22nd as we
#ShareTheMicInCyber
FOLLOW . SHARE . RETWEET . ACT



Jessica Hyde
Hexordia



Tanisha L. Turner
Elastic





Nick

by Con
w Workshop

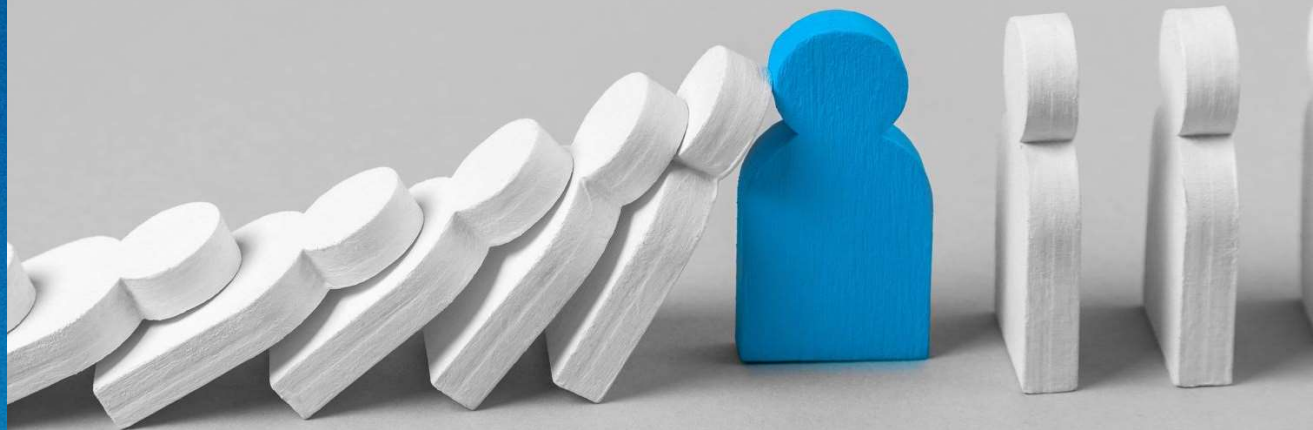


Mentorship Relationship

Maintaining the relationship



**Mentorship
is nurtured
relationship.**



Based on...

- Humility
- Respect
- Mutual interests
- Boundaries
- Structure
- Flexibility
- Personality compatibility
- Caring



Professional Respect & Interesting Work



Successful Mentorship

Kindness

Understanding

Communication

Impactful

Establishes trust and
vulnerability

Allows for honesty and
openness



Gas them up... but be real

- It is important to provide critique and areas for improvement
- Challenge them to make them better



Take the time to check in



Maintaining the relationship

- Mentee needs to continue the work
- Should be able to report on assignment completion or have new things they want to reach
- It is okay for mentorship to reach a natural end
- It is okay to not be a fit
- It is okay to take a pause and come back
- It is okay to check back in after a period – especially after major goal success!
- Both people should be invested and active in the relationship



You ARE a
mentor



Person you can call

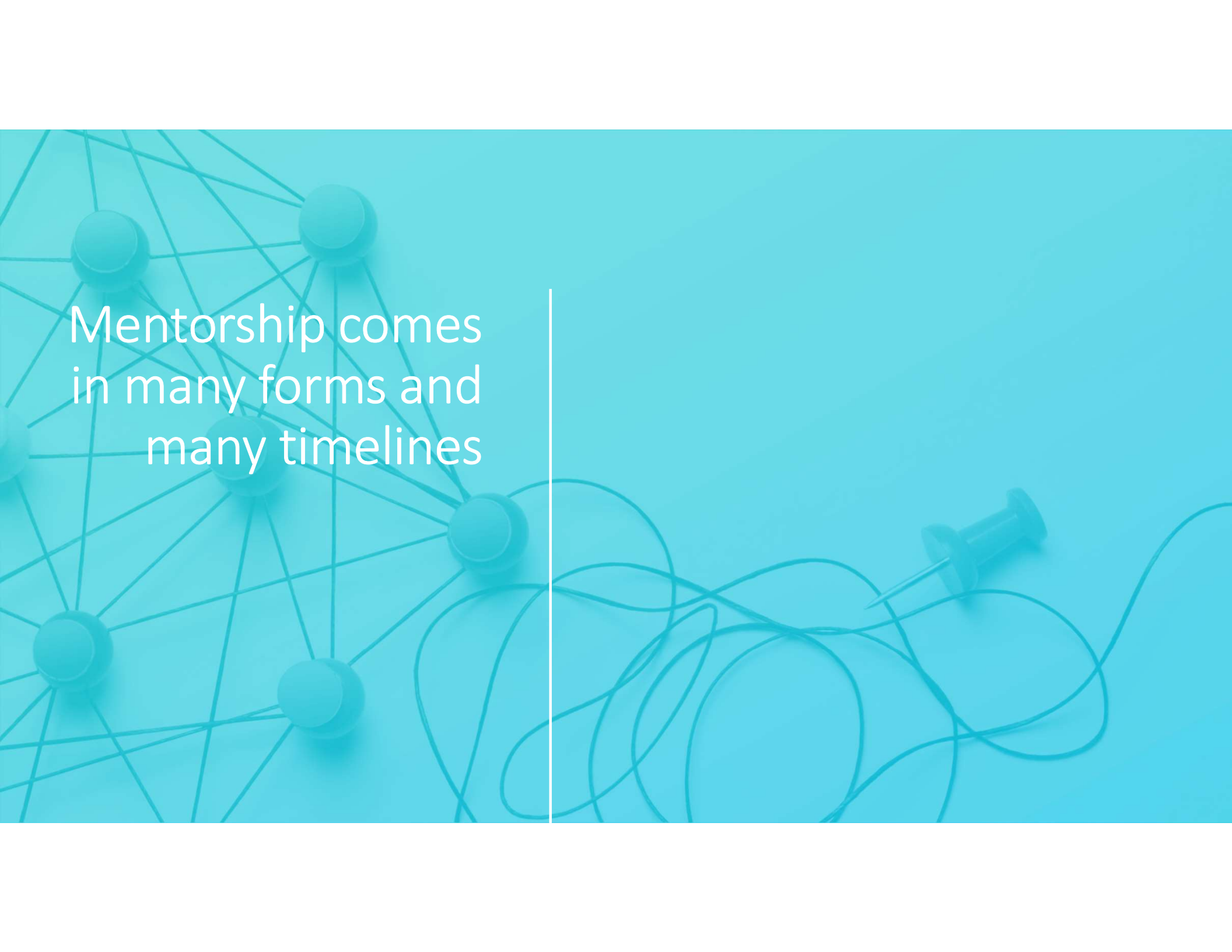
- May not always need them
- May have different mentors for different situations
- Someone who has been through a particular thing
- Sometimes when you least expect it



Bidirectional Mentors

- Peers
- Colleagues
- Folks in tangential places
- Inspire each other





Mentorship comes
in many forms and
many timelines

Hot Topics



Imposter Syndrome

- The elephant in the room
- Find the value in it = You CARE
- Leverage that to be awesome
- But don't let it disable you!
- Name it and tell it to be quiet



How Do I Break in to DFIR

- DFIR is not always entry level!
- Migrate from other roles
(SOC, IT, LE)
- Find a mentor
- Public Works!



Education

- Formal university programs
 - Undergraduate or Graduate
- Training Programs
 - DFIR Diva's affordable training list
 - SANS
 - Cyber5W



What Certification should I Get?

- Look up the roles you are interested in!
- Tool vendor cert?
- Agnostic certification?
- Maintenance requirements?
- What/how is it testing?
- Practicum? Knowledge questions?
- Prerequisite training or experience?
- Cost?



Resume / Curriculum Vitae

- Formats change!
- Keep a master document, submit specific
- Regularly update (monthly) and Linked In
- CV vs Resume
- Proposals, expert witness, professional orgs, peer review submissions, speaking submissions
- Technical Skills – Proficient with vs Familiar with



Networking

- Local low-cost events
 - BSides
 - 2600 groups
 - DefCon groups
 - High-Tech Crime Investigation Association (HTCIA)
- Conferences
 - Techno Security
 - DFRWS
 - SANS DFIR Summit
 - Magnet User Summit



Social Media

- Separate DFIR only accounts
- Keep it professional and positive
- Places to connect
 - Digital Forensics Discord Server
 - #DFIR on Mastodon
 - #DFIR on Twitter
 - #DFIR on LinkedIn
 - Computer Forensics Subreddit
 - Even Tik Tok and Instagram



Share and Contribute

- Most important thing you can do to stand out!
 - Contribute Code (LEAPP project, Autopsy Modules, Volatility))
 - Build CTFs
 - Artifact Information (Artifact Genome Project, Artifact Museum)
 - Share images (CFReDS, Digital Corpora)
 - Write! Blogs – thisweekin4n6.com
- GOAL – Share TECHNICAL work first!



Job Postings



Ninja Jobs

The screenshot displays a grid of six job listings on the ninjajobs.org website. Each listing includes the job title, employer, a five-star rating, a brief job description, and key details such as the posting date, telework availability, and location. At the bottom of each listing, there are icons for views, bookmarks, and applications, along with a 'See Details' link.

Job Title	Employer	Rating	Job Description	Posted	Telework	Location	Views	Bookmarks	Applications	Action
(Part-Time) Cyber Security Operation Center (CSOC) Analyst (Night Shift)	XOR Security	★★★★★	Night time Weekend (Part-Time) Cyber Security Operation Center (CSOC) AnalystXOR Se...	2022-06-29	Not Provided	Vienna, Virginia, United States	399	0	3	See Details
Security Engineer - REMOTE	XOR Security	★★★★★	XOR Security is currently seeking a talented Security Engineer to support an Agency-...	2022-11-16	Not Provided	Arlington, Virginia, United States	454	0	3	See Details
Security Engineer - Remote	XOR Security	★★★★★	XOR Security is currently seeking a Cyber Security Engineer. Applies a broad understanding of monito...	2022-09-15	Not Provided	Washington, District of Columbia, United States	250	0	0	See Details
Cloud Security Engineer	XOR Security	★★★★★	XOR Security is currently seeking talented Cloud Engineer to support an Agency-level...	2022-09-01	Not Provided	Washington, District of Columbia, United States	246	0	0	See Details
Program Lead - Phishing	AbbVie	★★★★☆	Security Awareness Training Lead (Phishing) If you enjoy working with people and love working with ...	2023-02-21	Full Telecommute	United States	148	0	2	See Details
Security Operations Center (SOC) Manager/Team Lead	XOR Security	★★★★★	XOR Security is currently seeking a talented and ambitious self-starting Security Operations Center ...	2022-07-22	Not Provided	Washington, District of Columbia, United States	105	0	1	See Details



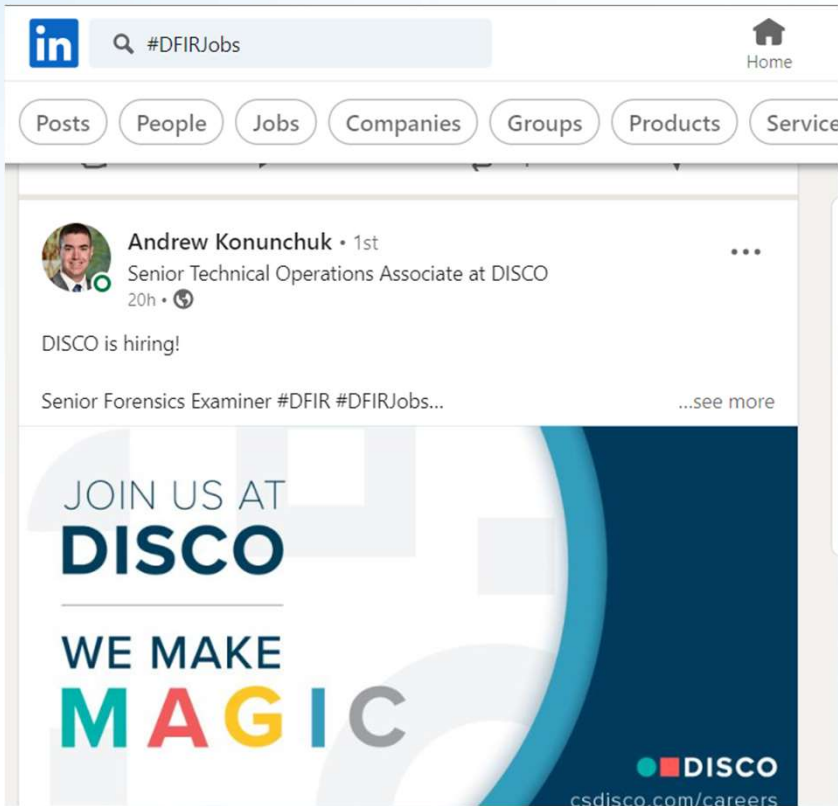
About DFIR

aboutdfir.com/jobs/

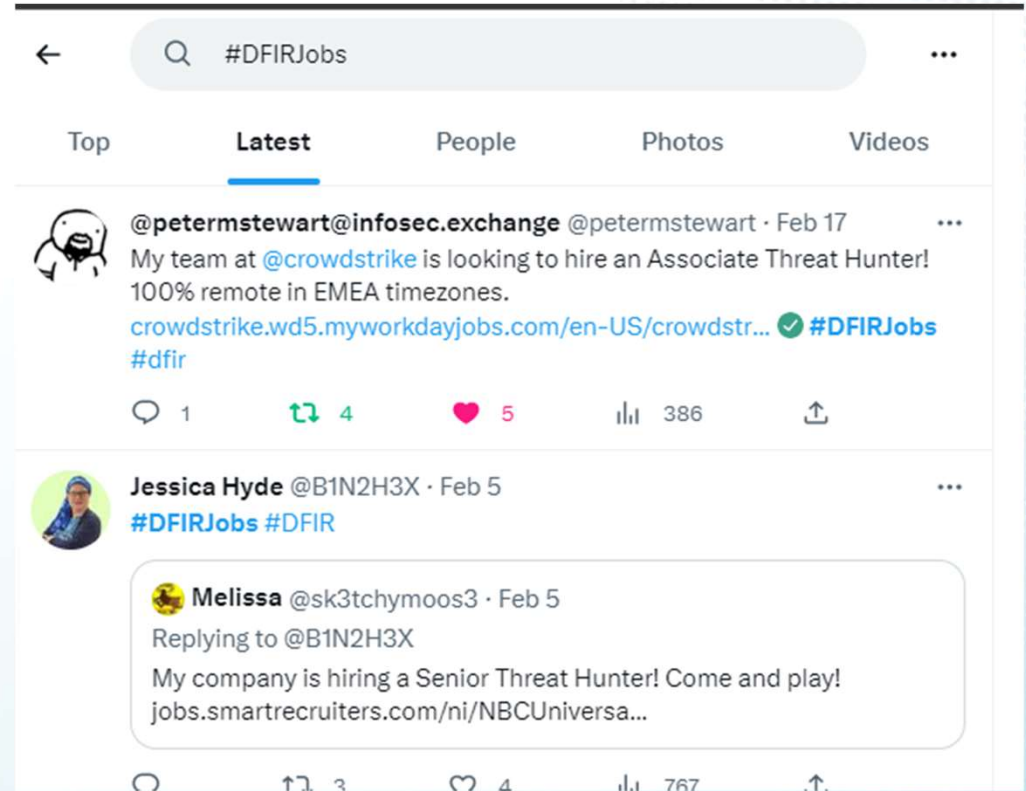
Date Added	Post Expires	Employer	Location	Description
2023-02-17 00:00:00	Ongoing	Detego Global	Horsham, West Sussex	Senior Digital Forensics Analyst
2023-02-17 00:00:00	Ongoing	Detego Global	Horsham, West Sussex	Junior Digital Forensic Analyst
2023-01-28 00:00:00	Ongoing	Charles Schwab	Phoenix, AZ	Sr. Staff - Forensics Analyst - US \$110k-220k
2023-01-28 00:00:00	Ongoing	Cisco Talos	Remote US	Incident Response Consultant, Talos
2023-01-28 00:00:00	Ongoing	Columbia Sportswear	Portland, OR	Cybersecurity Engineer
2023-01-28 00:00:00	Ongoing	Costco	Issaquah, WA	Cyber Threat Intelligence Analyst
2023-01-28 00:00:00	Ongoing	IHG Hotels & Resorts	Atlanta, GA	Senior Analyst, Cyber Threat Intelligence
2023-01-28 00:00:00	Ongoing	Raytheon	Arlington, VA	Cyber Threat Hunter - ONSITE
2023-01-28 00:00:00	Ongoing	Toyota Tsusho Systems US, Inc	US Remote	Threat Hunting Operations Analyst (100% Remote)
2023-01-28 00:00:00	Ongoing	Trustwave Government Solutions	US Remote	Sr. Security Consultant, DFIR



#DFIRJobs (Linked In, Twitter, Mastodon)



A screenshot of the LinkedIn mobile app interface. At the top, the search bar contains "#DFIRJobs". Below the search bar are navigation tabs for "Posts", "People", "Jobs", "Companies", "Groups", "Products", and "Services". The main content area shows a post by Andrew Konunchuk, a Senior Technical Operations Associate at DISCO, posted 20 hours ago. The post text reads "DISCO is hiring! Senior Forensics Examiner #DFIR #DFIRJobs...". Below the text is a large blue and white graphic with the text "JOIN US AT DISCO WE MAKE MAGIC" and the DISCO logo. The URL "csdisco.com/careers" is visible at the bottom of the graphic.



A screenshot of the Twitter mobile app interface. The search bar at the top contains "#DFIRJobs". Below the search bar are navigation tabs for "Top", "Latest", "People", "Photos", and "Videos". The "Latest" tab is selected. The first tweet is from @petermstewart@infosec.exchange, dated Feb 17. The tweet text is "My team at @crowdstrike is looking to hire an Associate Threat Hunter! 100% remote in EMEA timezones. crowdstrike.wd5.myworkdayjobs.com/en-US/crowdstr... #DFIRJobs #dfir". It has 1 reply, 4 retweets, and 5 likes. The second tweet is from Jessica Hyde @B1N2H3X, dated Feb 5, with the text "#DFIRJobs #DFIR". It is a reply to @B1N2H3X. The reply text is "My company is hiring a Senior Threat Hunter! Come and play! jobs.smartrecruiters.com/ni/NBCUniversa...". It has 3 retweets and 4 likes.



Digital Forensics Discord Server

The screenshot shows the Discord interface for the 'Digital Forensics' server. The left sidebar lists various channels, including 'forensics-reformatted', 'forensic-focus', 'forensic-happy-hour', 'forensic-lunch', 'sans-dfir', 'this-week-in-4n6', and several channels under 'DFIR COMMUNITY ROOM' and 'DFIR CHANNELS'. The main channel, '#dfir-job-postings', is selected and displays a list of job postings. The top of the channel has a 'Sort & View' dropdown and filters for 'Remote', 'In-Person', 'Hybrid', 'EMEA', 'APAC', 'Americas', and 'All'. The first post is an 'Information Only' message from Andrew Rathbun, dated October 25, 2022, with 1 reaction. The second post is for an 'eDisco /forensics analyst' position, categorized as 'In-Person' and 'Private Sector', posted 1 hour ago. The third post is for an 'Incident Response Consultant (EMEA Remote)' position, categorized as 'EMEA', 'Private Sector', and 'Remote', posted 2 days ago. The fourth post is for an 'Incident Response Identity Consultant - Active-Directory (EMEA remote)' position, also categorized as 'EMEA', 'Private Sector', and 'Remote', posted 2 days ago. The fifth post is for 'Senior & Junior Digital Forensic Analyst Positions [UK]', categorized as 'In-Person', posted by DFIRDetective.



Get Your Start in DFIR



Get Your Start in DFIR

[About](#) [Contact](#) [Donate](#) [View Jobs](#) [Post a Job](#) [Become a Training Partner](#)

Intern, Incident Response

Full Time

Internship

[Herndon, VA](#)

Posted 1 week ago



Sony

Sony Corporation of America, located in New York, NY, is the U.S. headquarters of Sony Group Corporation, based in Tokyo, Japan. Sony's principal U.S. businesses include Sony Electronics Inc., Sony Interactive Entertainment LLC, Sony Music Entertainment, Sony Music Publishing and Sony Pictures Entertainment Inc. With some 900 million Sony devices in hands and homes worldwide today, a vast array of Sony movies, television shows and music, and the PlayStation Network, Sony creates and delivers more entertainment experiences to more people than anyone else on earth. To learn more:

www.sony.com/en.

Position Summary:

Sony Corporation of America (SCA), is seeking an **Intern, Incident Response** to join the Global Information Security Department (GISD) located in **Herndon, VA** for the 2023 summer internship program. This position will assist the Security Operations Center (SOC) team within the Global Security Incident Response Team (GSIRT).



USAJobs

Save this search. We'll email you new jobs as they become available.

Senior Computer Scientist

Department of the Air Force - Agency Wide

Department of the Air Force

Linthicum, Maryland

Starting at \$171,268 Per Year (ST 00)



Open 02/14/2023 to 02/27/2023

Forensic Examiner - FT/Permanent

U.S. Courts

Judicial Branch

Saint Louis, Missouri

Open until filled - applications will be considered as they are received.

Starting at \$49,082 Per Year (CL 26-27)



Open 11/04/2022 to 11/03/2023

Computer Investigative Forensic Analyst - Direct Hire 'AMENDED'

Internal Revenue Service

Department of the Treasury

Multiple Locations

Starting at \$116,393 Per Year (GS 14)



Open 01/10/2023 to 01/09/2024

Special Agent - Cybersecurity/Technology Background

Federal Bureau of Investigation

Department of Justice

Location Negotiable After Selection

Starting at \$73,916 Per Year (GL 10)

Permanent - Must work a minimum of a 50-hour workweek, which may include irregular hours, and be on call 24/7, including holidays and weekends.



Open 01/25/2023 to 01/24/2024

Digital Forensic Analyst

U.S. Army Criminal Investigation Command

Department of the Army

Fort Benning, Georgia

Army Criminal Investigation Division

Starting at \$69,107 Per Year (GS 11-13)



Open 02/17/2023 to 03/03/2023

INTELLIGENCE OPERATIONS SPECIALIST (CYBER)

Defense Threat Reduction Agency

Department of Defense

Fort Belvoir, Virginia

Operations and Integration Directorate (OI)

Starting at \$112,015 Per Year (GG 13)



Open 02/10/2023 to 03/06/2023



Forensic Focus



Full time

Digital Forensic Specialist

🏠 Serious Fraud Office
📍 Hybrid (Serious Fraud Office, Cockspur Street, London, UK)

The Digital Forensic Unit (DFU) is responsible for the processing and analysis of all digital evidence seized by or provided to the Serious Fraud Office. This includes the investigation of

23 Feb, 2023



Full time

Senior Digital Forensic Engineer

🏠 National Crime Agency
📍 Hybrid (Tamworth, UK)

National Crime Agency Location: Tamworth
Salary: £36,742 – £44,912 + £3,000
Recruitment and Retention Allowance Closing

20 Feb, 2023



Full time

Senior Digital Forensics Examiner

🏠 National Crime Agency
📍 Hybrid (Bristol, Warrington, Kingston-Upon-Thames)

National Crime Agency Location: Bristol, Warrington, Kingston-Upon-Thames Salary:

20 Feb, 2023



Full time

Cyber Digital Forensics Officer

🏠 National Crime Agency
📍 Hybrid (Bristol, Warrington, Tamworth and Kingston-Upon-Thames)

National Crime Agency Location: Bristol, Warrington, Tamworth and Kingston-Upon-

20 Feb, 2023



Full time

Digital Forensics Operations Officer

🏠 National Crime Agency
📍 Hybrid (Stevenage, Dover, Gillingham, Warrington, Tamworth, Nottingham, Birmingham, Leicester, Bristol and Kingston-Upon-Thames)



Full time

Digital Forensics Examiner

🏠 National Crime Agency
📍 Hybrid (Bristol, Tamworth, Warrington, Kingston-Upon-Thames)

National Crime Agency Location: Bristol, Tamworth, Warrington, Kingston-Upon-Thames Salary: £28,840 – £37,748 + £3,000





Resources:



Mentorship Resources

- <https://dfirdiva.com/getting-into-dfir/>
- <https://www.magnetforensics.com/blog/job-hunting-dfir-field/>
- <https://www.hexordia.com/blog-1-1/pathway-to-digital-forensics>
- <https://tisiphone.net/2023/01/03/lessons-learned-from-cybersecurity-mentoring/>



Getting Started

- [DFIR Diva](#)
- [Cyber5W](#)
- [Startme.stark4n6.com](https://startme.stark4n6.com)



Keeping Current

- Phill Moore's
 - This Week in 4n6 - blog of all the week's forensic content
- Michael's
 - Digital Forensic Survival Podcast
- Richard Davis'
 - 13 Cubed You Tube Channel
- Joshua James'
 - DFIR Science You Tube Channel



Keep Practicing

- Magnet Forensic Summit CTFs
- Cyber Defenders Blue Team CTFs





Skill Up



Python

Alexis Brignoni's You Tube based course

- DFIR Specific class
- https://www.youtube.com/playlist?list=PLz61osc7c3OqQ_xBZJbzZdlkVd8HnxLmC

DFIR Python Study Group

Class 0 - DFIR Python Study Group



Alexis Brignoni

1.06K subscribers

Subscribe



YARA

Resources:

- Twitter
#100DaysOfYara
- 100 Days of Yara
<https://dmfrsecurity.com/2021/12/20/100-days-of-yara-day-1-basics/>
- <https://github.com/InQuest/awesome-yara>



Victor M. Alvarez
@plusvic

Replying to @milliped and @yaraules

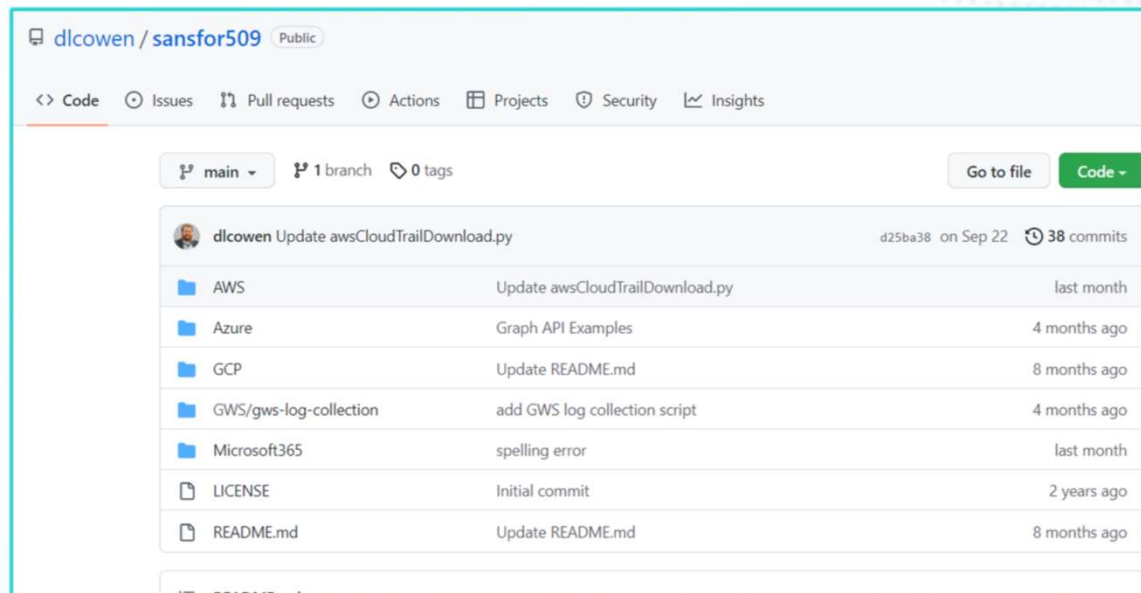
YARA is an acronym for: YARA: Another Recursive Acronym, or Yet Another Ridiculous Acronym. Pick your choice.

10:45 AM · Sep 22, 2016 · Twitter for Android



Cloud

- Basic Cloud Understanding: A Cloud Guru
- SANS FOR 509 Public GitHub
<https://github.com/dlcowen/sansfor509>



dlcowen / sansfor509 Public

<> Code Issues Pull requests Actions Projects Security Insights

main 1 branch 0 tags Go to file Code

dlcowen Update awsCloudTrailDownload.py d25ba38 on Sep 22 38 commits

AWS	Update awsCloudTrailDownload.py	last month
Azure	Graph API Examples	4 months ago
GCP	Update README.md	8 months ago
GWS/gws-log-collection	add GWS log collection script	4 months ago
Microsoft365	spelling error	last month
LICENSE	Initial commit	2 years ago
README.md	Update README.md	8 months ago



Collaborate with the DFIR Community



Standards groups

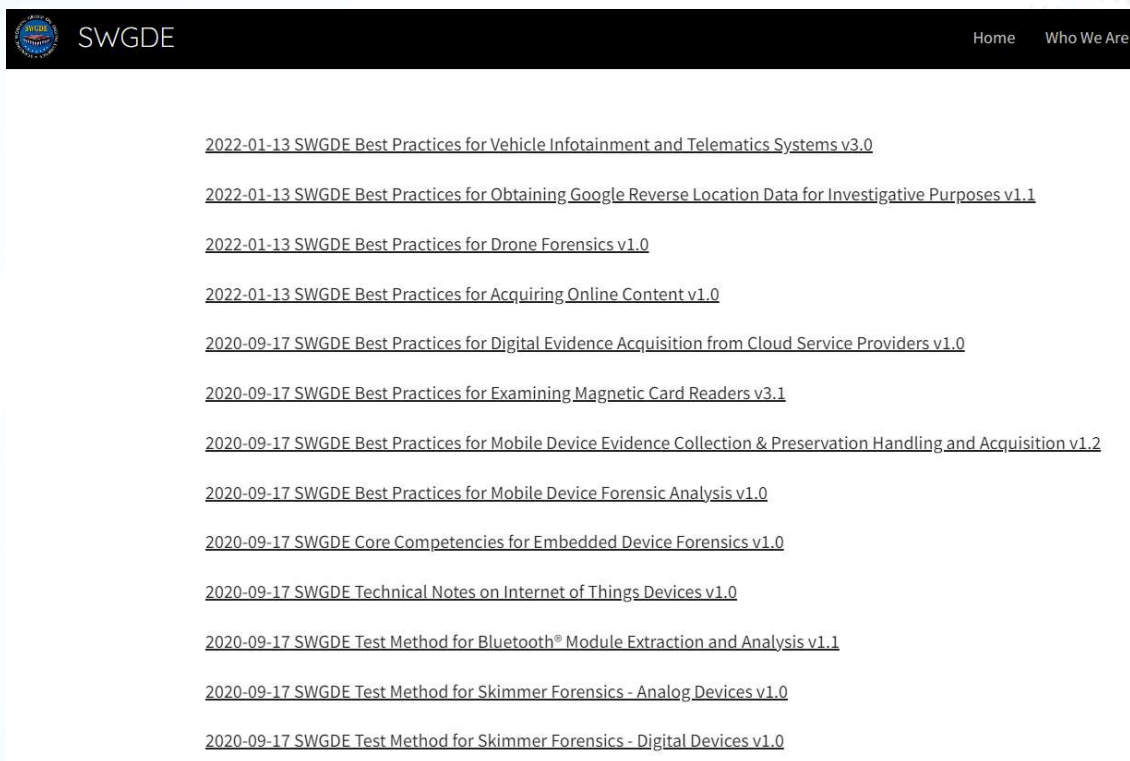
SWGDE

NIST OSAC



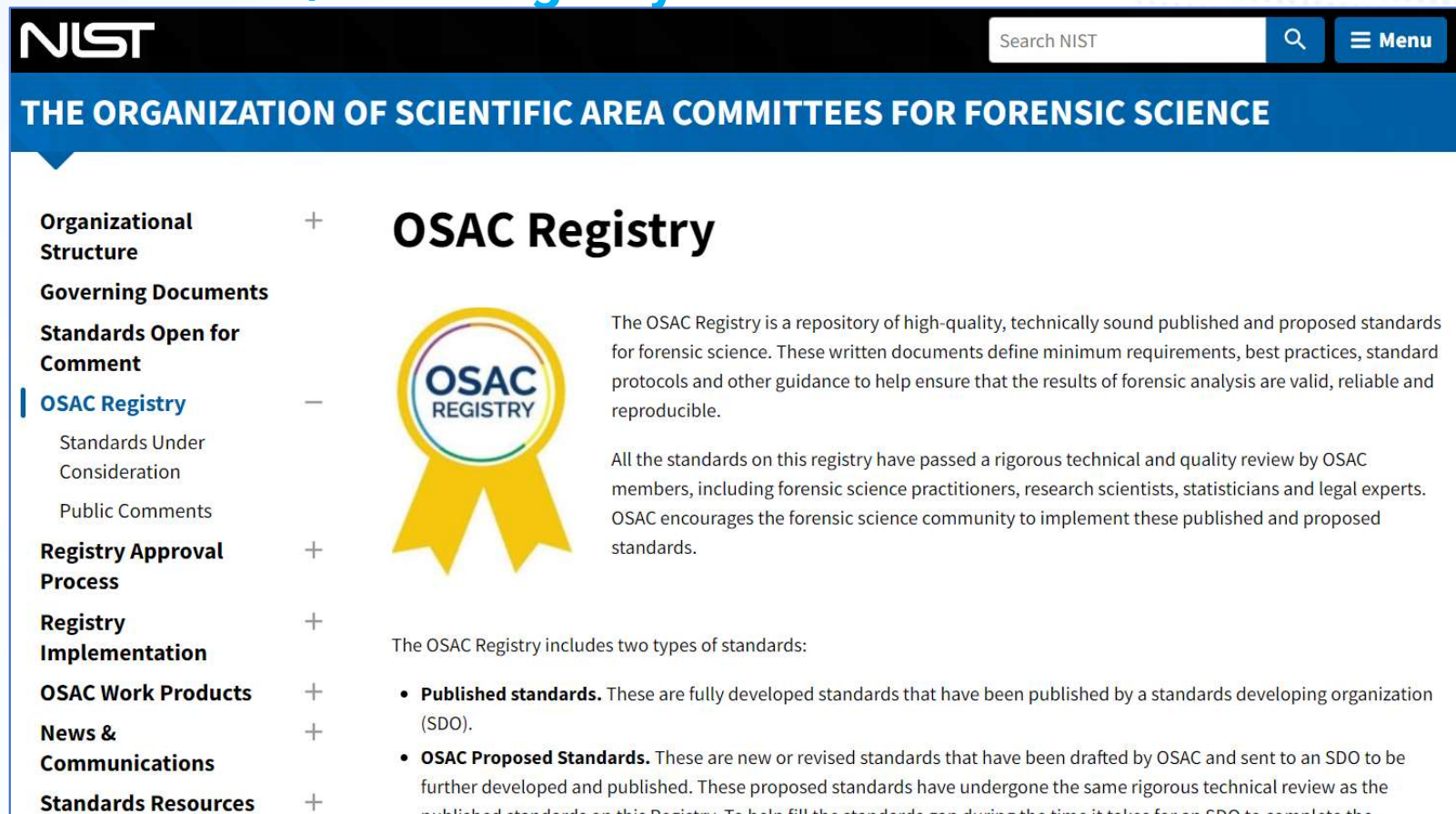
SWGDE

swgde.org



NIST OSAC

www.nist.gov/organization-scientific-area-committees-forensic-science/osac-registry




NIST Search NIST Menu

THE ORGANIZATION OF SCIENTIFIC AREA COMMITTEES FOR FORENSIC SCIENCE

- Organizational Structure +
- Governing Documents
- Standards Open for Comment
- OSAC Registry** -
 - Standards Under Consideration
 - Public Comments
- Registry Approval Process +
- Registry Implementation +
- OSAC Work Products +
- News & Communications +
- Standards Resources +

OSAC Registry



The OSAC Registry is a repository of high-quality, technically sound published and proposed standards for forensic science. These written documents define minimum requirements, best practices, standard protocols and other guidance to help ensure that the results of forensic analysis are valid, reliable and reproducible.

All the standards on this registry have passed a rigorous technical and quality review by OSAC members, including forensic science practitioners, research scientists, statisticians and legal experts. OSAC encourages the forensic science community to implement these published and proposed standards.

The OSAC Registry includes two types of standards:

- **Published standards.** These are fully developed standards that have been published by a standards developing organization (SDO).
- **OSAC Proposed Standards.** These are new or revised standards that have been drafted by OSAC and sent to an SDO to be further developed and published. These proposed standards have undergone the same rigorous technical review as the published standards on this Registry. To help fill the standards gap during the time it takes for an SDO to complete the



Journals and Peer reviewed work

AAFS

FSI:DI

DFRWS
DFIR Review



American Academy of Forensic Science

www.aafs.org



Digital & Multimedia Sciences—2022

C5 Methods for Evaluating and Optimizing Automated Detection/Classification Systems in the Forensic Environment

Jeff Smith, MS*, MITRE, McLean, VA

Learning Overview: After attending this presentation, attendees will better understand the foundational principles underlying detection/classification systems used in forensics, such as biometric recognition and multimedia manipulation detection, considerations for their operational use, and novel techniques for implementing these systems in a forensic environment.

Impact Statement: This presentation will impact the forensic science community by increasing baseline knowledge in the operating principles behind automated systems and by proposing best practices and new methods for their implementation in a forensic environment.

It is necessary to implement automated systems in forensics and intelligence in application areas such as biometric recognition and multimedia manipulation detection. These analytics leverage machine learning techniques that output a confidence value or posterior probability of classification given the evidence input.¹ This probability is typically a value between 0 and 1. A threshold, set to 0.5, would assign samples of outputs larger or equal 0.5 to the positive class, and the rest to the negative class.² While this arbitrary threshold can work well in many cases, as will be shown in this presentation, an optimal threshold can be found by evaluating performance against known data.

The results of these systems when evaluated against known data can be summarized with a Confusion Matrix (example in Figure 1) of True Positives (TP), False Positives (FP), True Negatives (TN), and False Negatives (FN).

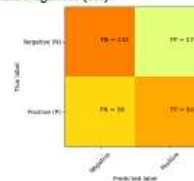


Figure 1: Example Confusion Matrix at an arbitrary threshold shows count of False Positives, False Negatives, True Positives, and True Negatives.

The most common evaluation technique is the area under the Receiver Operating Characteristic (ROC) curve in order to establish overall system performance. The ROC curve (example seen below in Figure 2) is a plot of the system's True Positive Rate (TPR):

$$TPR = \frac{\text{true positives}}{\text{true positives} + \text{false negatives}}$$

over its False Positive Rate (FPR):

$$FPR = \frac{\text{false positives}}{\text{false positives} + \text{true negatives}}$$



Forensic Science International: Digital Investigations (FSI:DI)



#MVS2023

MAGNE I VIRTUAL SUMMIT 2023



DFRWS 2023
HYBRID EUROPE
SAVE THE DATE

March 21-24, 2023

Bonn, Germany



DFRWS EU 2023

March 21, 2023

The DFRWS-EU 2023 Conference will be held Tuesday, March 21 through Friday, March 24....

DFRWS 2022
HYBRID APAC
September 28-30, 2022
Adelaide, Australia



DFRWS APAC 2022

September 28, 2022

The DFRWS-APAC 2022 Conference will be held Wednesday, September 28 through Friday, September 30....



DFRWS 2022
VIRTUAL USA

July 11-14

REGISTER NOW!

DFRWS USA 2022

July 11, 2022

The DFRWS-USA 2022 Virtual Conference was held Monday July 11 through Thursday, July 14,...

DFRWS 2022
HYBRID EUROPE

MARCH 29-APRIL 1, 2022
Oxford, England

DFRWS 2021
VIRTUAL USA

JOIN US
JULY 12-14, 2021



DFRWS 2021
VIRTUAL EUROPE

PROGRAM ANNOUNCED!

Registration Discounts Available



DFIR Review

dfir.pubpub.org

Featured Posts

iOS Location Services and System Services are they ON or OFF

by Scott Koenig and Ian Whiffin



Published: Jul 11, 2022

iOS Settings Display Auto-Lock & Require Passcode

by Scott Koenig



Published: Jun 02, 2022

Turbo Speed: Parsing Device Health Services from Google

by Kevin Pagano



Published: Sep 28, 2022

Ain't That a Kik in the Head: Kik Messenger iOS Analysis

by Kevin Pagano and Alexis Brignoni



Published: Apr 11, 2022



Community Organizations

HTCIA


IACIS

DFIR
Discord



High Tech Crime Investigation Association

htcia.org

		HOME	ONLINE TRAINING	EVENTS +	ABOUT +	MEMBER LOGIN	f	t	in	v
M O N	February 27	HTCIA Ontario Chapter Townhall 6:30 PM - 7:30 PM HTCIA Ontario Chapter members, your attendance is requested to an important townhall of all current members. We need your support and attendance discussing an important matter regarding your chapter.								Register
W E D	March 8	March Virtual Meeting - Hunch.ly (Silicon Valley and Southern California Chapters) 10:00 AM - 11:00 AM ALL CHAPTERS WELCOME (Virtual Chapter Meeting) Click this link to automatically register for all 2023 HTCIA-SV/SoCal meetings: https://us06web.zoom.us/meeting/register/tZAtce-srz0qE9Z0mLh2L14s61r_LN5axvz Justin Seitz on ...								
W E D	March 15	HTCIA New England Chapter March 15th 2023 Meeting 8:00 AM - 1:00 PM SAVE THE DATE Speaking Slot Speaker Bio Topic title Summary of topic 9-10 Nilay R Mistry Nilay Mistry is the most senior and first faculty of Digital Forensics and Cyber Security in the ...								Register
W E D	March 15	Zoom Mid-Atlantic Chapter Meeting 2:00 PM - 4:00 PM Join us on March 15 at 2:00 PM via Zoom with Michael Robinson. Michael will be regaling us with mystical tales from the world of Incident Response; about battles fought and lessons learned. " Michael is currently a Director at ...								Register



IACIS
iacis.com



DFIR Discord

incident-response

αβο γαρσουβ 10/17/2022

@Matt Hi Matt! I Added New Features:

- User Status
- Has Password
- Sudo Access

https://github.com/3gbCyber/User_Accounts_Hunting

GitHub

GitHub - 3gbCyber/User_Accounts_Hunting: The scrip will help you to...

The scrip will help you to find some values info for the user that you need as DFIR - GitHub - 3gbCyber/User_Accounts_Hunting: The scrip will help you to find some values info for the user that you...

3gbCyber/
User_Accounts_Hunting

The scrip will help you to find some values info for the user that you need as DFIR

1 Contributor 0 Issues 8 Stars 0 Forks

user	password	other
admin	admin	
root	root	
www	www	
ftp	ftp	
mail	mail	
mysql	mysql	
postgres	postgres	
ssh	ssh	
telnet	telnet	
vsftpd	vsftpd	
xmms	xmms	
zabbix	zabbix	
zabbix2	zabbix2	
zabbix3	zabbix3	
zabbix4	zabbix4	
zabbix5	zabbix5	
zabbix6	zabbix6	
zabbix7	zabbix7	
zabbix8	zabbix8	
zabbix9	zabbix9	
zabbix10	zabbix10	
zabbix11	zabbix11	
zabbix12	zabbix12	
zabbix13	zabbix13	
zabbix14	zabbix14	
zabbix15	zabbix15	
zabbix16	zabbix16	
zabbix17	zabbix17	
zabbix18	zabbix18	
zabbix19	zabbix19	
zabbix20	zabbix20	
zabbix21	zabbix21	
zabbix22	zabbix22	
zabbix23	zabbix23	
zabbix24	zabbix24	
zabbix25	zabbix25	
zabbix26	zabbix26	
zabbix27	zabbix27	
zabbix28	zabbix28	
zabbix29	zabbix29	
zabbix30	zabbix30	
zabbix31	zabbix31	
zabbix32	zabbix32	
zabbix33	zabbix33	
zabbix34	zabbix34	
zabbix35	zabbix35	
zabbix36	zabbix36	
zabbix37	zabbix37	
zabbix38	zabbix38	
zabbix39	zabbix39	
zabbix40	zabbix40	
zabbix41	zabbix41	
zabbix42	zabbix42	
zabbix43	zabbix43	
zabbix44	zabbix44	
zabbix45	zabbix45	
zabbix46	zabbix46	
zabbix47	zabbix47	
zabbix48	zabbix48	
zabbix49	zabbix49	
zabbix50	zabbix50	
zabbix51	zabbix51	
zabbix52	zabbix52	
zabbix53	zabbix53	
zabbix54	zabbix54	
zabbix55	zabbix55	
zabbix56	zabbix56	
zabbix57	zabbix57	
zabbix58	zabbix58	
zabbix59	zabbix59	
zabbix60	zabbix60	
zabbix61	zabbix61	
zabbix62	zabbix62	
zabbix63	zabbix63	
zabbix64	zabbix64	
zabbix65	zabbix65	
zabbix66	zabbix66	
zabbix67	zabbix67	
zabbix68	zabbix68	
zabbix69	zabbix69	
zabbix70	zabbix70	
zabbix71	zabbix71	
zabbix72	zabbix72	
zabbix73	zabbix73	
zabbix74	zabbix74	
zabbix75	zabbix75	
zabbix76	zabbix76	
zabbix77	zabbix77	
zabbix78	zabbix78	
zabbix79	zabbix79	
zabbix80	zabbix80	
zabbix81	zabbix81	
zabbix82	zabbix82	
zabbix83	zabbix83	
zabbix84	zabbix84	
zabbix85	zabbix85	
zabbix86	zabbix86	
zabbix87	zabbix87	
zabbix88	zabbix88	
zabbix89	zabbix89	
zabbix90	zabbix89	

Digital Forensics

DFIR COMMUNITY ROOM

- # dfir-open-source-projects
- # dfir-job-postings
1 New Post
- # dfir-python-study-group
- # dfir-review
- # dfir-science
- # i-beg-to-dfir
- # sans-dfir

DFIR CHANNELS

- # general-discussion-and-questi...
- # mobile-forensic-extractions
- # mobile-forensic-decoding
- # training-education-employment
- # policies-and-procedures
- # jtag-isp-chip-off-flasherbox
- # computer-forensics
- # network-forensics
- # dvr-multimedia-surveillance
- # programming_reverse-enginee...
- # malware-analysis

incident-response

October 22, 2022

@Murst This is very broad but does anyone have resources they can share around triage processes? We...

sam0x90 10/22/2022

Not sure that's what you are looking for but these IRM from Societe generale might give you some inspiration <https://github.com/certsocietygenerale/IRM>

GitHub

GitHub - certsocietygenerale/IRM: Incident Response Methodologies

Incident Response Methodologies. Contribute to certsocietygenerale/IRM development by creating an account on GitHub.

certsocietygenerale
/IRM

Incident Response Methodologies

2 Contributors 1 Issue 992 Stars 217 Forks

sam0x90 10/22/2022

There is also this <https://awesomedfir.com/>

Awesome DFIR - Digital Forensics & Incident Response

Awesome DFIR - Digital Forensics & Incident Response

The definitive guide through the best articles, books, podcasts, tweets, tools, videos and...



Summary

- You can be a mentor and mentee at any phase
- Self reflect and do the work
- There are practical ways to work with others
- Multiple mentors for multiple parts of your journey





MAGNET
VIRTUAL SUMMIT
2023

MOVING UP IN DFIR: A MENTORSHIP DAY PANEL

February 27, 2023 | 1:00 PM EST

[REGISTER NOW!](#)



QUESTIONS?

Jessica Hyde
@b1n2h3x
@b1n2h3x@infosec.exchange
Hexordia.com

