SANS DFIR

NEW TO DFIR
FIELD MANUAL

The Ultimate Guide to Getting Started in Digital Forensics & Incident Response (DFIR)

One of the most asked questions we get is

"How Do I Get Started in DFIR?"

Unfortunately, there isn't a simple answer that works for everyone. This guide was created to help YOU figure out the best path into DFIR. Use it to help develop your skills and find a network of people to support you getting into the industry.

What to expect from this guide

This guide contains nine sections, each focusing on different ways to develop skills. If you focus efforts on each one of these, you will gain exposure to the industry and be able to define your specific pathway.

1. Take advantage of free content
2. Build your skills
3. Surround yourself with industry experts and mentors
4. Attend free and low-cost events
5. Engage with the community
6. Scholarships, sponsorships and community programs
7. Get training and certification
8. 20 coolest careers in cybersecurity (10 are DFIR)
9. Learn from the community – featured interview with Kat Hedley
10. Last word of advice from Heather Mahalik

Why Digital Forensics & Incident Response?

Digital Forensics and Incident Response roles will always be required, and always be in demand. Crimes involving digital assets are becoming increasingly common, and as technology and techniques evolve over time, the field needs to adapt and innovate to stay one step ahead, which makes DFIR such an interesting area to work in. It's also one of the most satisfying and rewarding careers, knowing that you are helping to solve crimes, find the right answers, and stop bad people doing bad things.

1. Take Advantage of Free Content

Take the time to watch webcasts and YouTube videos, read blogs, and start Googling when something piques your interest. Here are some we recommend you start with:

Webcasts

- www.sans.org/webcasts/started-dfir-testing-123-sansatmic-118720
- www.sans.org/webcasts/securing-future-dfir-113305
- www.sans.org/webcasts/building-house-sand-foundational-knowledge-skills-digital-forensics-crucial-116715
- www.youtube.com/watch?v=eftOgRsHK4A

YouTube Channels

- **SANS DFIR** – www.youtube.com/channel/UCwSo89W3KgPrid41vskBDYA
- **13Cubed** – www.youtube.com/c/13cubed
- **DFIR Science** – www.youtube.com/c/DFIRScience

Blogs & Newsletters

- **THIS WEEK IN 4N6 –** https://thisweekin4n6.com
- **SANS Cybersecurity Blog –** www.sans.org/blog

Podcasts

- **4n6 Reformatted –** https://anchor.fm/4n6reformatted
- **Forensic Focus podcast –** www.forensicfocus.com/podcast

2. Build Your Skills

It's important to learn the core concepts and seek out hands-on opportunities to apply them. Familiarize yourself with Windows, Linux, Coding Languages, and Networking. How?

- There are lots of places where people can find test data sets to play with (DFIR Training and AboutDFIR have pages dedicated to these). The test data sets are usually associated with a challenge, which means that people can also have something to search for.
- There are services like Hack The Box which will allow people to test out what attackers are doing, but it's also easy to build your own using freely available toolkits.

- Everyone has a mobile phone or a computer they can use. They can also download VirtualBox or VMWare Player and create virtual machines to create test data on. Microsoft has ones you can download or Azure is inexpensive. The main benefit of building your own datasets is that you know what you did, which means you know when the information presented to you is correct or not.
- There are plenty of books to read, and here's a few that people have recommended. Knowing the authors of those books and having read a few of them I would recommend people picking them up and having a read.
- Download Free Tools – play around with open-source tools like SIFT Workstation. The SANS faculty has created over 150 free tools. Find them here.
- Learn to code! While coding in Python isn't a requirement to get into DFIR it helps. Brooke and Alexis put together this YouTube series on coding for DFIR.
- There are various CTFs happening throughout the year, and there are even people like Kevin Pagano or Shanna Daly who are regularly sharing the process they use to work through these challenges. SANS also hosts the yearly Holiday Hack Challenge as well as various NetWars challenges, including one specifically for DFIR!
- Take a training class! SANS obviously has a lot of them, and if you're just starting out, we recommend the FOR308: Digital Forensics Essentials class to set up a solid foundation.

3. Surround Yourself with Industry Experts and Mentors

Follow

Following industry experts and mentors can open a world of tools, topics and events that you would not otherwise be aware of. SANS Instructors are very active on Twitter and worth following. Here's a full list of SANS Instructors' Twitter handles. In addition to the full list, here are some of our most active:

- Rob Lee | @robtlee
- Jason Jordaan | @DFS_JasonJ
- Katie Nickels | @likethecoins
- Heather Mahalik | @HeatherMahalik
- Chad Tilbury | @chadtilbury
- Ovie Carrol | @ovie
- Phill Moore | @phillmoore
- Kat Hedley | @4enzikat0r
- Robert M. Lee | @RobertMLee
- Phil Hagen | @PhilHagen
- Sarah Edwards | @iamevltwin
- Ryan Chapman | @rj_chap
- Sean O'Connor | @vHUMINT
- Dave Cowen | @HECFBlog
- Megan Roddie | @megan_roddie
- Mike Pilkington | @mikepilkington
- Eric Zimmerman | @EricRZimmerman
- Kevin Ripa | @kevinripa
- Lodrina Cherne | @hexplates
- Lenny Zeltser | @lennyzeltser

You can always find others to follow if you pay attention to hashtags such as **#DFIR**, **#computerforensics**, **#digitalforensics**, **#incidentresponse**, **#cybersecurity**, and **#infosec**.

Mentorships

There are a ton of mentorship opportunities available (found with a quick search). Here are a few of our favorites:

- Cybersecurity Mentoring Hub
- Women in Cybersecurity (WiCyS) Mentorship
- International Consortium of Minority Cybersecurity Professionals (ICMCP)
- Ken Johnson Scholarship opened yearly six months prior to the SANS DFIR Summit

4. Attend Free and Low-Cost Events

There are so many great IT security conferences, and many of them post their content online afterwards.

SANS Summits

All are free in 2022

SANS Summits connect you with cybersecurity practitioners and experts who deliver applicable content based on real-world experience. Through in-depth presentations, panel discussions, interactive workshops, and sharing forums, you'll collaborate with fellow cybersecurity practitioners, learn about tools and generate solutions that will help you protect your organization from ever-evolving threats.

> "I've managed to learn something I didn't know from nearly every session, and I've been made aware of additional tools or methodologies that will help."
>
> —Dallas Moore, **PepsiCo**

Magnet User or Virtual Summit

Originally a showcase of the excellent work the Magnet Forensics team produces, the Magnet User Summit and Magnet Virtual Summit is a month-long extravaganza of forensic goodness for the entire community.

Open Source Digital Forensics Conference (OSDFCon)

OSDFCon is a one-day conference run by Basis Technologies where open-source researchers and developers can showcase their open-source digital forensic efforts.

Digital Forensics Research Workshop (DFRWS)

DFRWS is a series of research-focused conferences held in North America, Europe, and Asia Pacific. The conferences allow researchers to present their research papers in Digital Forensic Science.

BSides

BSides is a community-driven framework for building events for and by information security community members. The goal is to expand the spectrum of conversation beyond the traditional confines of space and time. BSides creates opportunities for individuals to both present and participate in an intimate atmosphere that encourages collaboration. These are intense events with discussions, demos, and interaction among participants. It is where conversations for the "next big thing" are happening.

"BSides is a growing community of real security professionals who want to learn from each other and grow. Unlike most cons we see today, BSides cuts through the hype and allows you to have real conversations among your peers in an environment that's comfortable and welcoming."

—Michelle Schafer

5. Engage with the Community

Get involved with groups, meetups, lists, forums, and LinkedIn communities.

#DFIR on Twitter

https://twitter.com/search?q=%23DFIR

SANS DFIR LinkedIn Community

Keep up with the latest of Digital Forensics & Incident Response topics, look for jobs, training, and more at Linkedin.

SANS Industrial Control Systems Community Forum

Participate in the SANS Industrial Control Systems (ICS) Community Forum, where ICS professionals discuss current security events, share tips, ask questions, and connect with others passionate about securing the critical infrastructure.

AFCEA Chapters

AFCEA provides a forum for military, government, and industry communities to collaborate so that technology and strategy align with the needs of those who serve.

ISACA Local Chapters

ISACA offers access to resources and a community of experts committed to lifetime learning and career progression to help you stay up to date.

ISSA Chapter Directory

ISSA is the community of choice for international cybersecurity professionals dedicated to advancing individual growth, managing technology risk, and protecting critical information and infrastructure.

SANS OSINT Community

This is a place for people who are OSINTers, looking to become an OSINTer, and who are members of the global OSINT community!

Advancing Women in CyberSecurity (WiCys)

WiCyS is where the recruitment, retention and advancement of women in cybersecurity happens.

High Technology Crime Investigation Association (HTCIA)

HTCIA was formed to provide education and collaboration to our global members for the prevention and investigation of high-tech crimes.

IACIS

IACIS, the international association of computer investigative specialists, is a non-profit, volunteer organization wholly dedicated to training, certifying and providing membership services to computer forensic professionals around the world.

Discord

- SANS Blue Team Ops
- The DFIR Discord (with a new SANS-specific channel!)
- Arsenal Recon
- Magnet Forensics

6. Scholarships, Sponsorships and Community Programs

SANS Cyber Academies

To help fill the cybersecurity skills gap, the SANS Institute created the CyberTalent Immersion Academy. It's an intensive, accelerated training program that provides world-class training and GIAC certifications to quickly and effectively launch careers in cybersecurity. More than 600 scholarships have been awarded so far and 90% of our graduates are employed within six months of graduation. Find out if you could be the one to participate and launch a new career in cyber!

Department of Defense STEM

DoD STEM offers opportunities for potential students, educators, and the current workforce.

Scholarships

Here is a list of cybersecurity college scholarships:

- Scholarships.com
- Unigo

Capture-the-Flag Tournaments

Most vendors such as Belkasoft, Cellebrite, and Magnet Forensics offer Capture-the-Flag Tournaments that enhance your knowledge on DFIR topics. These competitions offer datasets, questions and often walk throughs of the answers.

7. Get Training and Certification

SANS offers an accredited college certificate—the Undergraduate Certificate in Applied Cybersecurity from the SANS Technology Institute—that guides you through a sequence of four courses. The program includes an introductory course plus three SANS courses leading to GIAC certifications that provide the foundational knowledge and hands-on skills needed to launch a cybersecurity career. The program provides lifetime career services and also serves as a pathway to the SANS.edu master's degree program and job-specific graduate certificate programs. More than half of the certificate students received their first cybersecurity job offer before they finished the program. A 100% online option is available. Applications are accepted monthly.

SANS Security Essentials courses are designed to provide a range of topics to help you grasp foundations quickly and fill critical knowledge gaps. The certifications associated with the courses provide assurance to employers that their prospective hires can actually do the job. Below is a list of SANS foundational courses and certifications, with supporting resources that can help you get started, and that might give you an idea of the path that interests you the most.

SANS Foundations

SANS Foundations is the best single course available to learn the core knowledge and develop practical skills in computers, technology, and security fundamentals that are needed to kickstart a career in cybersecurity. The course features a comprehensive variety of innovative, hands-on labs and practical exercises that go far beyond what is offered in any other foundational course in cybersecurity. These labs are developed by leading subject-matter experts, drawing on the latest technology, techniques, and concepts in cybersecurity.

The course provides students with the practical learning and key skills to empower future cybersecurity learning and professional development.

> "I was having a hard time getting a job in information security due to my lack of hands-on experience. SANS gave me extraordinary training and the opportunity to rise to the top of the résumé pile."
>
> —AJ Langlois, **BB&T**

FOR308: Digital Forensics Essentials is an introductory course aimed at people from non-technical backgrounds, to give an understanding, in layman's terms, of how files are stored on a computer or smartphone. It explains what Digital Forensics and Incident Response are and the art of the possible when professionals in these fields are given possession of a device.

This course is intended to be a starting point in the SANS catalogue and provide a grounding in knowledge, from which other, more in-depth, courses will expand.

> "I think the biggest value add for SANS Foundations was simply how comprehensive it was. It covered a lot of topics, but each was covered in enough depth for a better handle on the basics without being overwhelming."
>
> —U.S. government federal law enforcement professional

FOR498: Battlefield Forensics & Acquisition, a digital forensic acquisition training course, provides the necessary skills to identify the many and varied data storage mediums in use today, and how to collect and preserve this data in a forensically sound manner despite how and where it may be stored. It covers digital acquisition from computers, portable devices, networks, and the cloud. It then teaches the student Battlefield Forensics, or the art and science of identifying and starting to extract actionable intelligence from a hard drive in 90 minutes or less.

GIAC Battlefield Forensics and Acquisition (GBFA)

> "This course provided information I can take back to my company and begin using immediately. It will be very easy to show leadership the ROI."
>
> Jennifer Welsh, **CNO Financial Group**

> "In DFIR, things rarely go as planned. This course teaches you about the options to control when things aren't working as expected."
>
> —Michael Roberts, **Corvus Forensics**

SEC301: Introduction to Cyber Security, this introductory certification course, is the fastest way to get up to speed in information security. Written and taught by battle-scarred security veterans, this entry-level course covers a broad spectrum of security topics and is liberally sprinkled with real life examples. A balanced mix of technical and managerial issues makes this course appealing to attendees who need to understand the salient facets of information security basics and the basics of risk management. Organizations often tap someone who has no information security training and say, "Congratulations, you are now a security officer." If you need to get up to speed fast, Security 301 rocks!

GIAC Information Security Fundamentals (GISF)

> "Coming from a non-cybersecurity background, this course was perfect for setting my cyber foundation."
>
> —Marco Godinez, **Discover Financial**

> "The best parts of this class are the real-world examples and historical events, which illustrate how these course topics are applicable and why they are important to learn/understand."
>
> —Gia M..

SEC401: Security Essentials: Network, Endpoint, and Cloud

Whether you are new to information security or a seasoned practitioner with a specialized focus, SEC401 will provide the essential information security skills and techniques you need to protect and secure your critical information and technology assets, whether on-premise or in the cloud. SEC401 will also show you how to directly apply the concept learned into a winning defensive strategy, all in the terms of the modern adversary. This is how we fight; this is how we win!

GIAC Security Essentials (GSEC)

> "SEC401 took what I thought I knew and truly explained everything to me. Now, I also UNDERSTAND the security essentials fundamentals and how/why we apply them. I loved the training and cannot wait to come back for more."
>
> —Nicholas Blanton, **ManTech International**

What makes someone good at DFIR?

You don't need a background with computers to succeed. In fact, some of the most successful students at the SANS Technology Institute didn't. As part of the admissions process, you'll take a quiz that tests your natural ability to succeed in DFIR. If you like solving puzzles and have a desire to learn about technology, DFIR could be a great fit for you.

We often get asked about how to get started in DFIR—and really there are just so many different ways that it's difficult to point out "the one way into DFIR." That being said, one of the main things that sets a candidate apart is whether they can demonstrate the qualities that a hiring manager is looking for that are critical to working in digital forensics and incident response:

- Problem solving
- Critical thinking
- Thoroughness and attention to detail
- Communication
- Teamwork
- Ownership

Notice that technical ability is actually less important here at an entry level. We teach people how to do forensics all the time (in fact, it's one of the things SANS is known for!), what we can't teach is the ability to see a problem and say, "I'm going to figure out how to solve that!" In DFIR, we typically have to be across a lot of different data sources, within a very short period of time, and with a high level of accuracy (and even more often the documentation is either non-existent, incomplete, or even incorrect).

Ok, but how does knowing this help you "get started in DFIR"?

Being able to demonstrate you can take a problem, work it through, and share it with your team is unbelievably important. If you can demonstrate that you can take something you don't know anything about, find available resources, and present them at the appropriate level for your audience then you're already ahead of everyone that isn't doing the same. You're demonstrating a key still that your future coworkers want to see! Everyone wants to work with the person they can give a problem to, and that person comes back with the solution!

The best part about all of this is you actually don't need to know a lot about the topic before you start. Perfect for a beginner! But where do you start? There's so many facets of DFIR to start with, and we can tell you, you can spend a long time in this industry and you will never know everything. There will always be things you don't know, and the 'to-do' list of things to learn will always keep getting longer.

We tell everyone, especially newer examiners, that they should dive into the community and start documenting their journey. We're a very welcoming bunch - we like to see others succeed because we're all in this together. Someone brand new to the field may look at something everyone else overlooked, or maybe they validate something we already knew, but that's useful too.

By starting to document your understanding, you are already setting yourself apart from everyone else that isn't. It's definitely a good way to set yourself apart, and a fantastic way to demonstrate the skills you need to get started in DFIR.

8. SANS 20 Coolest Careers in Cybersecurity

Here's the list of Top 20 Coolest Careers in cybersecurity. Challenge your skills, take the next step in your career, and become an invaluable asset to employers. Ten of the coolest careers are DFIR!

- **Threat Hunter**
- **Red Teamer**
- **Digital Forensic Analyst**
- **Purple Teamer**
- **Malware Analyst**
- **CISO/ISO or Director of Security**
- **Blue Teamer/All-Around Defender**
- **Security Architect and Engineer**
- **Incident Response Team Member**
- **Cybersecurity Analyst/Engineer**
- **OSINT Investigator/Analyst Technical Director**
- **Technical Director**
- **Cloud Analyst**
- **Intrusion Detection/SOC Analyst**
- **Security Awareness Officer**
- **Vulnerability Researcher and Exploit Developer**
- **Application Pen Tester**
- **ICS/OT Security Assessment Consultant**
- **DevSecOps Engineer**
- **Media Exploitation Analyst**

For more information about these careers, visit here.

9. Learn from People in the Community

Featured Interview

NAME: **Kathryn Hedley (Kat)**

DAY JOB: **Digital Forensics**

COURSES TAUGHT OR AUTHORED: **SANS FOR308, FOR500**

Q: First of all, tell us a little about your background and how you got to where you are today.

A: After graduating from university, I won a place on a graduate scheme and started out as a developer on the Galileo European satellite navigation system. However, one of the modules in that degree was an introduction to Digital Forensics, and it was by taking that module that I decided my ultimate goal was a career in DFIR. Armed with only the limited knowledge I had from that one module, I applied for a role in Digital Forensics after two years as a developer. With a promise to get up to speed quickly by undertaking a Master's Degree in Computer Forensics, part-time, for the first two years in the role, I got the job. It was the foundational knowledge the Master's Degree gave me, that has allowed me to build a career in DFIR in the 14 years since I started that first job.

Q: There are lots of specializations in DFIR, how did you decide which area to focus on?

A: For me, I've really developed focus organically, and dipped into various specialisms over the years that were required by my role at the time. When I started out, all my investigations were Windows-based, so I focused on Windows artifact analysis. As smartphones became more popular, I saw more investigations coming in that involved these devices, so learned about smartphone acquisition and analysis. At one stage, the organization I was working for decided to create a malware investigation team, so I focused on how to find malware within networks and on endpoints. As part of this work, I also trained in memory analysis, to be able to search for malware and evidence of malware in RAM. My main focus has remained on Windows systems over the years. However, gaining some level of understanding of different specializations broadens overall knowledge, and I'd encourage others to dip into them and use that knowledge to decide their own focus.

Q: How do you recharge or take a break from work?

A: I #DFIRFit! The Twitter hashtag was created by Stacey Randolph around 2017, as a way for people in DFIR to come together and encourage each other to move away from their desks and get moving. I started posting with the hashtag in 2019, and really have Brian Moran to thank for motivating me, and for getting me involved with all the subsequent virtual challenges we've jointly run since then. Exercise is a really great way to de-stress, take a break, and release endorphins, as well as counteract some of the downsides to sitting at a desk all day, every day. It's also something that everyone can do and get involved in. Whether it's going for a walk at lunchtime, doing some stretches to get the limbs moving, going for a run, joining a regular exercise class, or taking up a sport, it all helps. #DFIRFit has also spawned a number of related hashtags for other groups in InfoSec, which is awesome. All of the hashtags are very inclusive, whether you work in those specific fields or not, so do get involved.

Q: What DFIR tools can't you live without?

A: A hex editor, because if all else fails, you can always look at the raw data.

I personally like 010 Editor, because it provides extra features such as file format templates and scripts.

EZ Tools Suite, because if you're dealing with Windows artifacts, there's a tool for everything!

X-Ways, because sometimes you just need a Forensic Suite, and despite a non-intuitive user interface, it's a very fast and accurate, feature-rich tool.

Just remember to always validate your tools before you use them in actual casework, so you know you can trust the output.

Q: What's your best travel hack?

A: Take a drawstring bag with you inside your carry-on bag. Once you're through security, pack the drawstring bag with everything you want at your seat on the plane. When you're about to board the plane, take the drawstring bag out of your carry-on and once you find your seat, you can put the carry-on straight into the overhead locker, and the drawstring bag under the seat in front of you. When it comes to leaving the plane, you can then put everything back into the drawstring bag before everyone stands up. When it comes to your turn, you can grab the drawstring bag, stand up, grab your carry-on from the overhead locker and leave the plane straight away. Makes boarding and leaving the plane super-fast and super-smooth.

Q: What advice would you give to someone just starting out?

A: Check out summit talks, webinars, podcasts; all content you're interested in online. There are lots of free resources provided by the community to help to broaden your knowledge. To name just a few links:

- **SANS Posters:** www.sans.org/posters
- **SANS Webcasts:** www.sans.org/webcasts/archive
- **This Week In Forensics Blog:** https://thisweekin4n6.com
- **Forensic Lunch:** www.youtube.com/user/LearnForensics
- **Magnet Forensics Cache Up Podcast:** www.magnetforensics.com/cache-up
- **Cellebrite's Life Has No Ctrl Alt Delete Podcast:** www.cellebrite.com/en/series/ctrl-alt-del

Also, get involved! Whether it's writing a blog, giving a talk at a summit, contributing to a tool on GitHub, playing a CTF, or Tweeting with the #DFIRFit or another #*fit hashtag, just join in. Doing your own research, playing CTFs, contributing to tools, are all great ways to learn new skills, as well as connect with the community, and it's a fantastic community to be part of.

Q: What do you think are essential skills for people new to DFIR?

A: A thirst for knowledge, and a desire to explore and find answers. Knowledge of how raw data is structured and how it can be understood is more important than being able to use specific tools. If you understand the fundamentals of DFIR, you have solid ground to then build on, and to focus in on any specialization(s) you choose, so start with the basics before jumping into specific platforms, artifacts and tools.

10. Closing Thoughts from the SANS DFIR Curriculum Lead, Heather Mahalik

DFIR is not only a career field, but it's also a passion of many. There are so many avenues one can take once you dip your toe into the pool of digital forensics. Getting started is often the hardest part and we hope this guide pushes you down a road where you land a job that not only pays the bills but fulfills your soul knowing that you are making the world a safer place while fighting digital crimes.

Some advice I have for you based upon how I got started in this field 20 years ago.

- **Leave your fear at the door.** Someone will always be smarter than you. Learn from them and take the opportunities listed in this guide to learn on your own.
- **Don't let your background or education deter you.** As stated, you don't need to be a computer wizard to excel in DFIR. You need to be curious, enjoy puzzles and have a hunger for knowledge.
- **Network.** People will make a difference! The DFIR community is like no other and we all want to help, learn, and grow in our skill craft. Talk to people. Get out of your shell.
- **Take all the training you can.** There is always something new to learn. This is one of the beautiful things about DFIR... something new is always on the horizon.
- **Research.** When you become curious about something, research it. Review the work that others have done and don't be afraid to share your research back with the community via blogs, presentations or even a simple Twitter post.

Never let someone or something make you think you cannot jump into this career field. Take the first step and you may find that you have not only found the job of your dreams, but also a brand-new hobby! If you are ever at a conference or event and you see me, please stop and say hello so I can welcome you to the DFIR family.