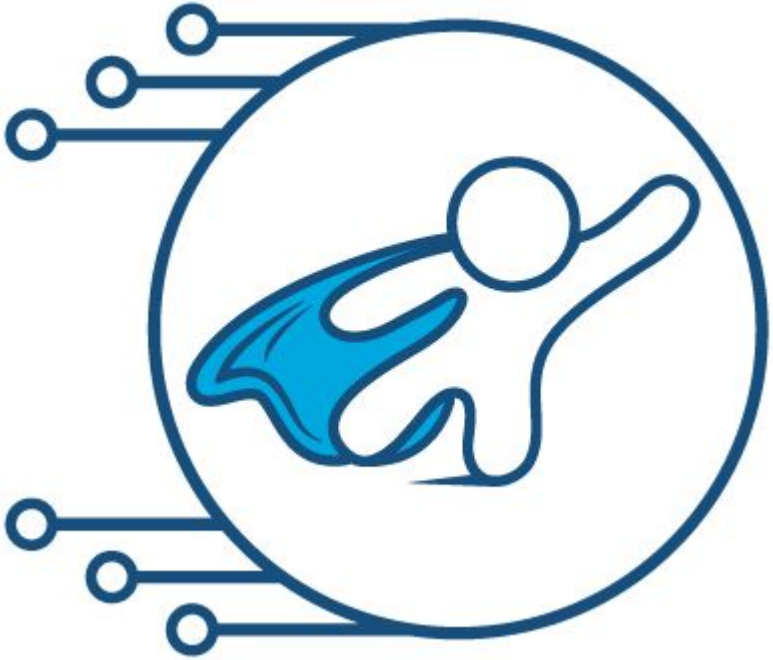
PXL DIGITAL

Blue Teams



INFOSEC WHEEL

@aprilwright
@proxyblue

PXL DIGITAL

BLUE TEAM

- Defensive Security
- Infrastructure protection
- Damage Control
- Incident Response(IR)
- Operational Security
- Threat Hunters
- Digital Forensics

PXL DIGITAL

Definition

*“A **blue team** is a group of individuals who perform an analysis of information systems to ensure security, identify security flaws, verify the effectiveness of each security measure, and to make certain all security measures will continue to be effective after implementation” - Wikipedia*

The 5 phases in the incident response plan

1. Preparation
2. Detection & Analysis
3. Containment, Eradication, Recovery
4. Post-Incident Review
5. Update the plan !

Analysis

analysis

/əˈnalɪsɪs/

oun

noun: **analysis**; plural noun: **analyses**

1. detailed examination of the elements or structure of something.
2. the process of separating something into its constituent elements.

Used in all steps of the process, as a continuous flow to achieve the end goal.

DFIR

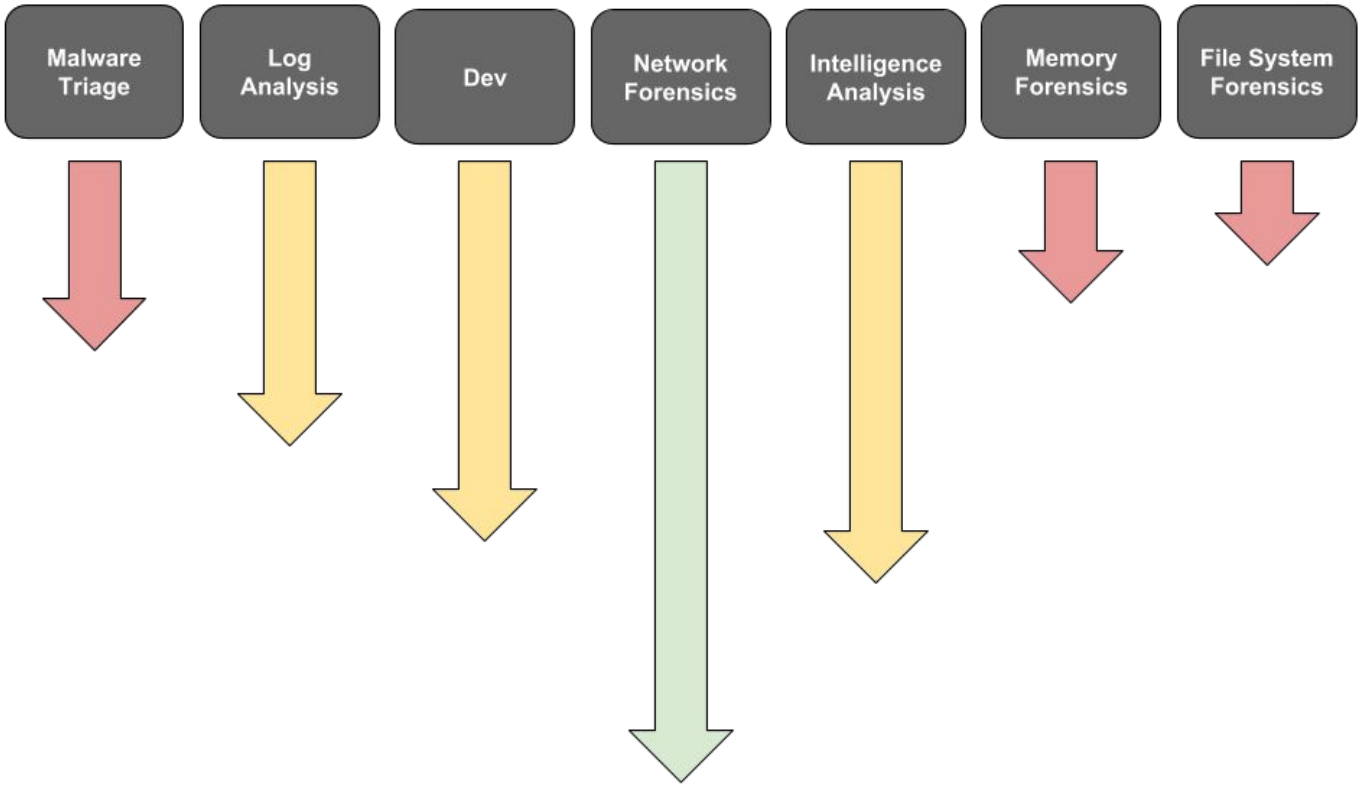
Definition:

*"**D**igital **F**orensics & **I**ncident **R**esponse is a multidisciplinary profession that focuses on identifying, investigating, and remediating computer network exploitation. "*

https://medium.com/@sroberts/introduction-to-dfir-d35d5de4c180

DFIR Skills

PXL DIGITAL



https://medium.com/@sroberts/introduction-to-dfir-d35d5de4c180

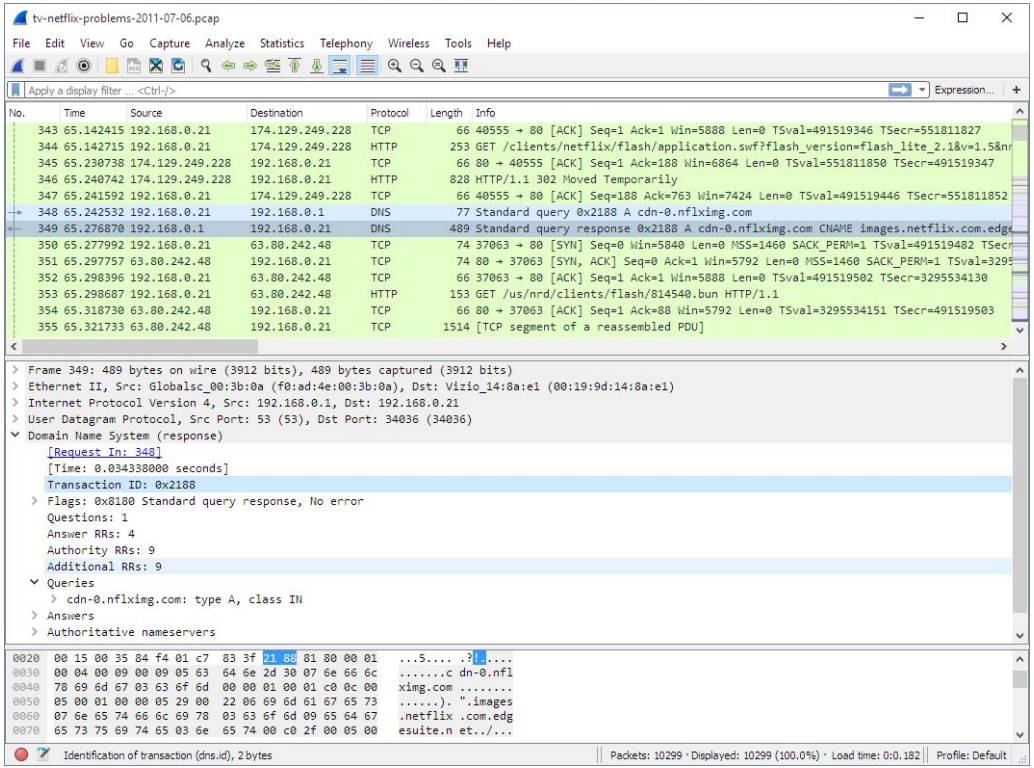
DFIR skills

Technical Skills

- Network Forensics

Covered in part in Security Essentials: Wireshark

Also with tools such as Snort & Suricata



DFIR skills

PXL DIGITAL

Technical Skills

- File System Forensics

  Acquisition

  - Disk-to-Image
  - Disk-to-Disk
  - Logical
  - Sparse

DFIR skills

PXL DIGITAL

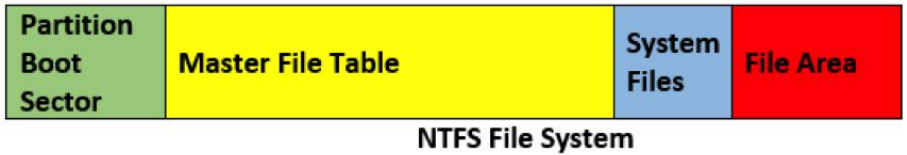
Technical Skills

- File System Forensics

  Extraction

  Involves the retrieving of unstructured or deleted data

  Deleted != gone: Deleting files only removes it from the disc contents table.



Other hiding techniques: encryption, steganography, file obfuscation...

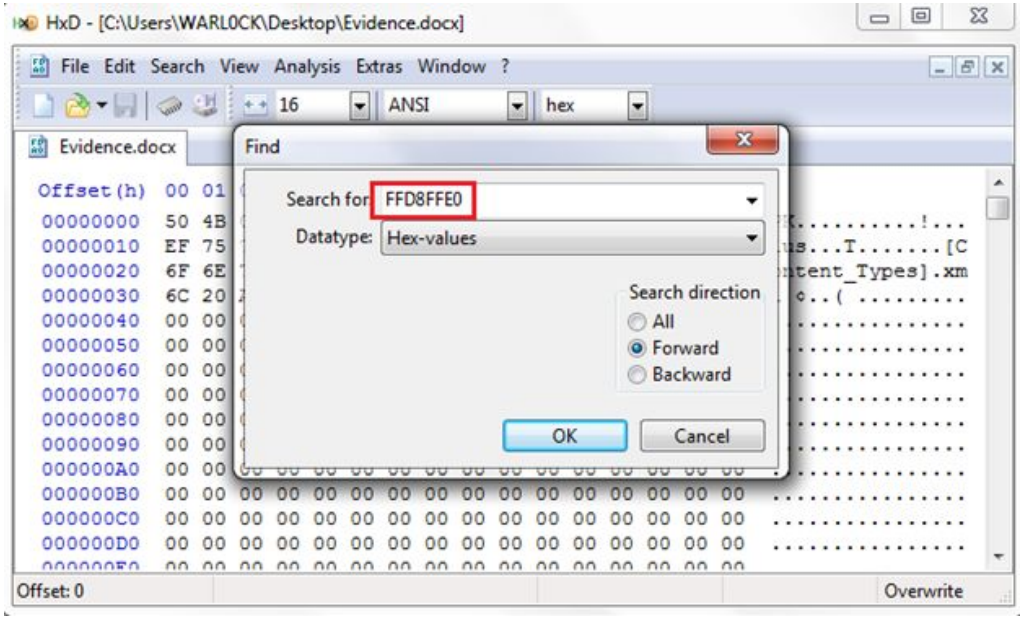
DFIR skills

Technical Skills

- File System Forensics

  File Carving

  “*Extracting data from unallocated space*”



https://resources.infosecinstitute.com/file-carving/

DFIR skills

PXL DIGITAL

Technical Skills

- File System Forensics

  Practial Tools

AUTOPSY
DIGITAL FORENSICS

ACCESSDATA®
ForensicToolkit (FTK)

DFIR skills

Technical Skills

- Memory Forensics

  A lot of malicious software hides in memory, so only File System forensics aren't enough

  This is usually achieved by running special software that captures the current state of the system's memory as a snapshot file, also known as a **memory dump**.

https://resources.infosecinstitute.com/memory-forensics/

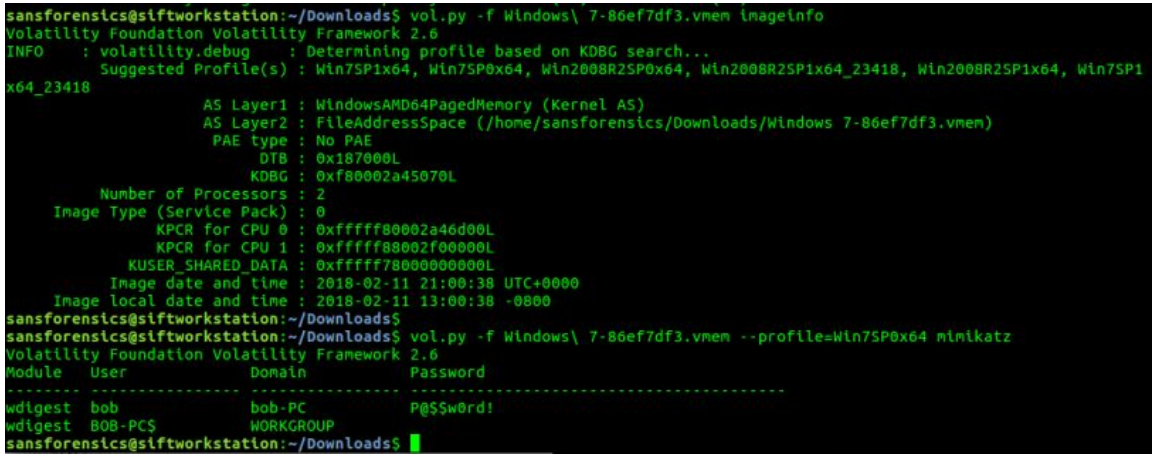
DFIR skills

Technical Skills

- Memory Forensics

  common methods and formats that are used today:

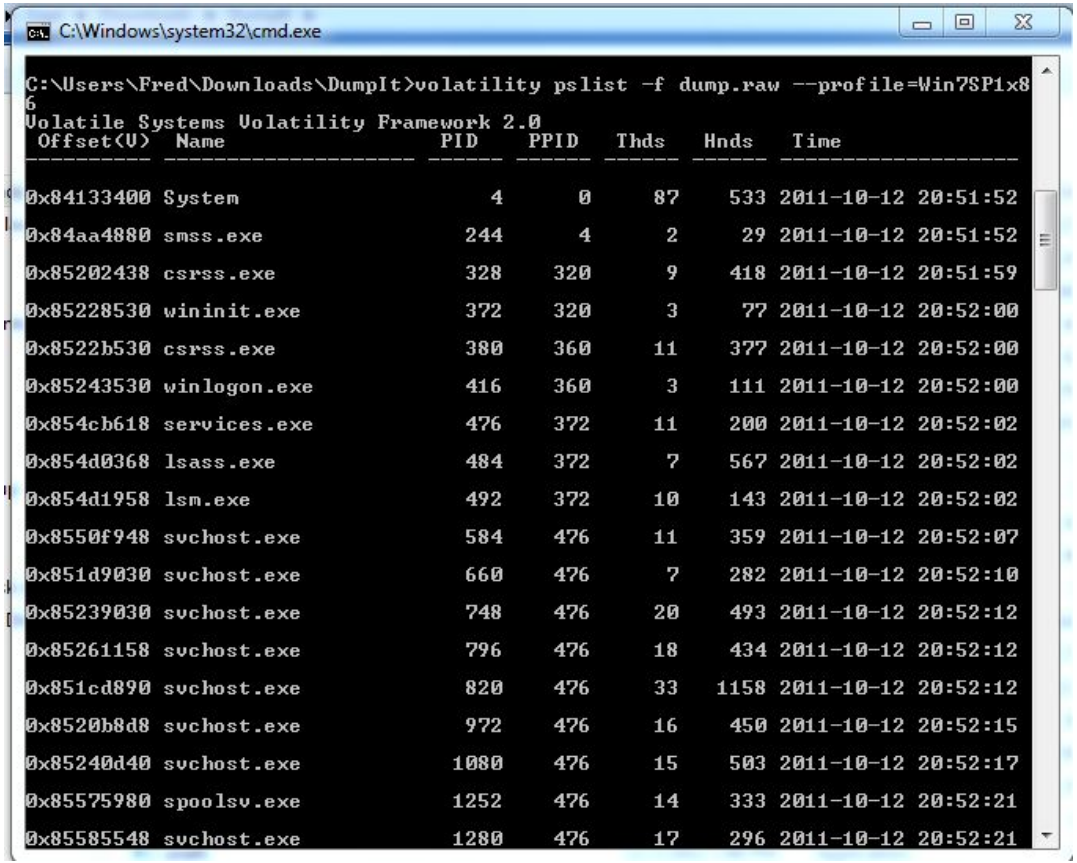
  - RAW Format
  - Crash Dump
  - Hibernation File
  - Page File
  - VMWare Snapshot



https://resources.infosecinstitute.com/memory-forensics/

DFIR skills

Technical Skills



DFIR skills

PXL DIGITAL

Technical Skills

- Memory Forensics

  Examining Your Captured Data

  - Open Files Associated With Process
  - Decoded Applications in Memory
  - Timestamp Comparison
  - Network Information
  - User Activity

https://resources.infosecinstitute.com/memory-forensics/

DFIR skills

PXL DIGITAL

Technical Skills

- Memory Forensics

  Practical Tools:

DFIR skills

Technical Skills

- Log Analysis

  SIEMs were supposed to do this for us...but alas.

  Logs can be analyzed system by system, but the real power shows up when you **search logs at enterprise scale**. It's tool driven, but the skills are the same for most of them.

  Enter: **Security Onion** (or any ELK based stack)

DFIR skills

PXL DIGITAL

Technical Skills

- Intelligence Analysis

  determine the relationships between the following entities:

  - People.
    - Names.
    - Email addresses.
    - Aliases.
  - Groups of people (social networks).
  - Companies.
  - Organizations.
  - Web sites.
  - Internet infrastructure such as:
    - Domains.
    - DNS names.
    - Netblocks.
    - IP addresses.
  - Affiliations.
  - Documents and files.

Sounds a lot like OSINT! But more organized and with a bigger goal (most of the time)

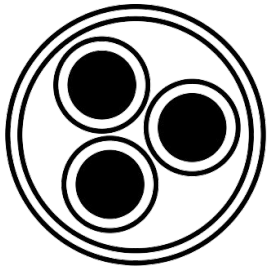
DFIR skills

Technical Skills

- Intelligence Analysis

  Tools & tricks:

https://medium.com/@raebaker/a-beginners-guide-to-osint-investigation-with-maltego-6b195f7245cc



MALTEGO

DFIR skills

Technical Skills

- Attacker Methodology

“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.”

- Sun Tzu

DFIR skills

Technical Skills

- Development

  Technology changes quickly, the companies we defend move quickly, and if you're waiting for a company or open source project to build the tool you need you'll always be behind.

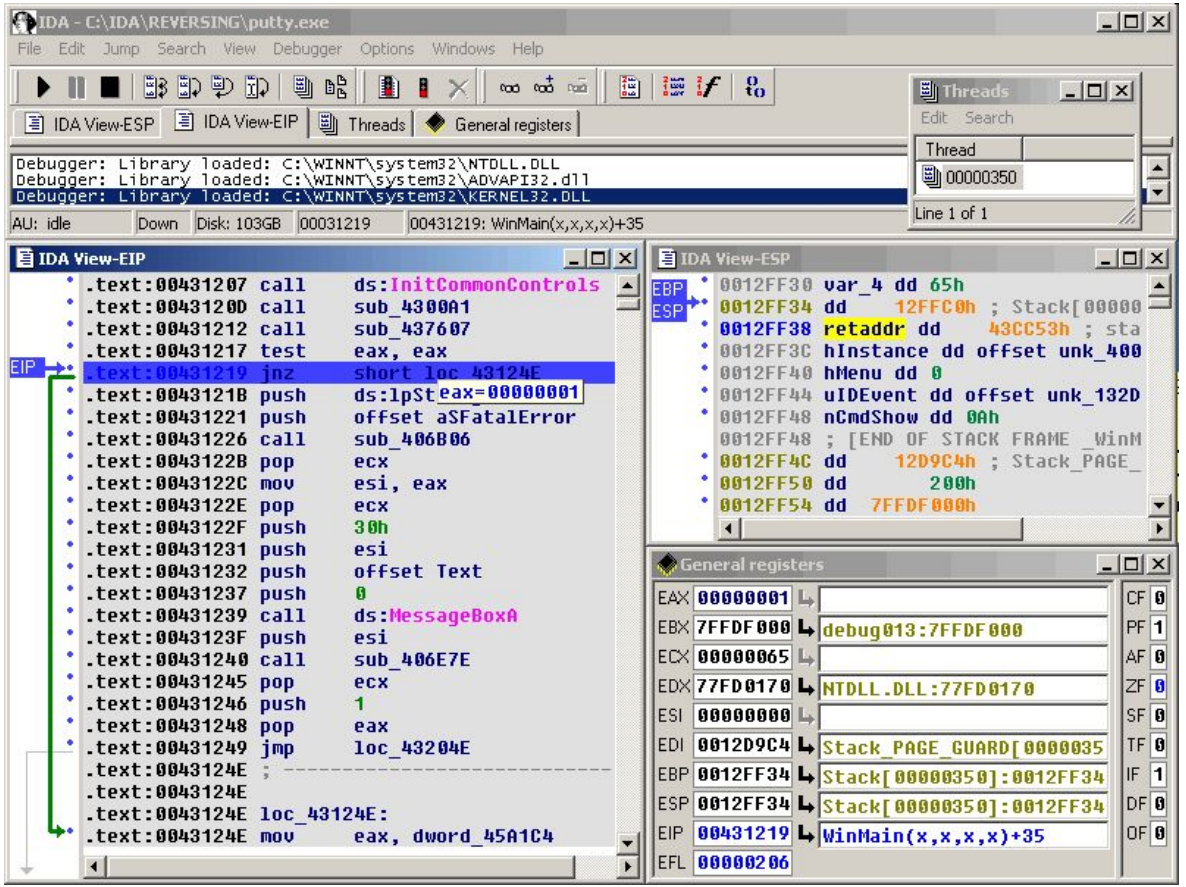
  The fact is the best DFIRs I've worked with are able to create their own solutions and even if it's just basic scripting being able to code is a game changer.

DFIR skills

Technical Skills

- Malware Triage

Recognize, analyse and reverse-engineering



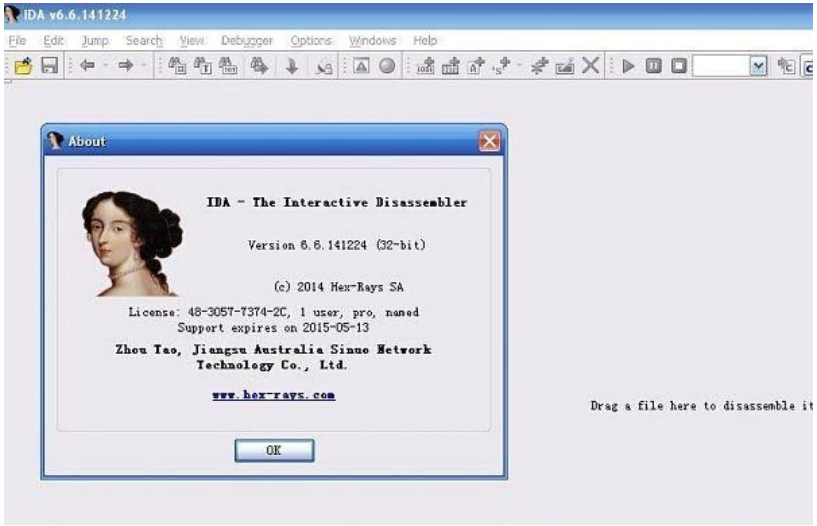
https://resources.infosecinstitute.com/category/certifications-training/malware-analysis-reverse-engineering/

DFIR skills

Technical Skills

Malware Triage

Tools & tricks:



DFIR skills

Soft Skills

Often overlooked, but very important!

- Investigation Process & Analysis

- Operational Security

  Being a DFIR, or security researcher of any kind, is dangerous.

DFIR skills

PXL DIGITAL

Soft skills

- Communication

  A good incident response leaves the IR team.

  • Communication to victims.

  • Communication to management.

  • Communication to customers.

  • Communication to 3rd party peers.

  • Even communication with law enforcement.

DFIR skills

Soft skills

- Working in a Team

  Working in a Team DFIR is a team sport. We work in groups, being able to delegate, be delegated to, sharing, coordinating, and doing so effectively in a time crunch is a big deal.

- Gaining Experience

  Lifelong learning

Pluralsight video’s

PLURALSIGHT

PXL DIGITAL

Pluralsight video: link
Relevant : Digital Forensics: The Big Picture

Pluralsight video: link
Relevant : Digital Forensics: Getting Started with File Systems

Pluralsight video: link
Relevant : Getting Started with Memory Forensics Using Volatility

Pluralsight video: link
Relevant : Network Security Monitoring (NSM) with Security Onion