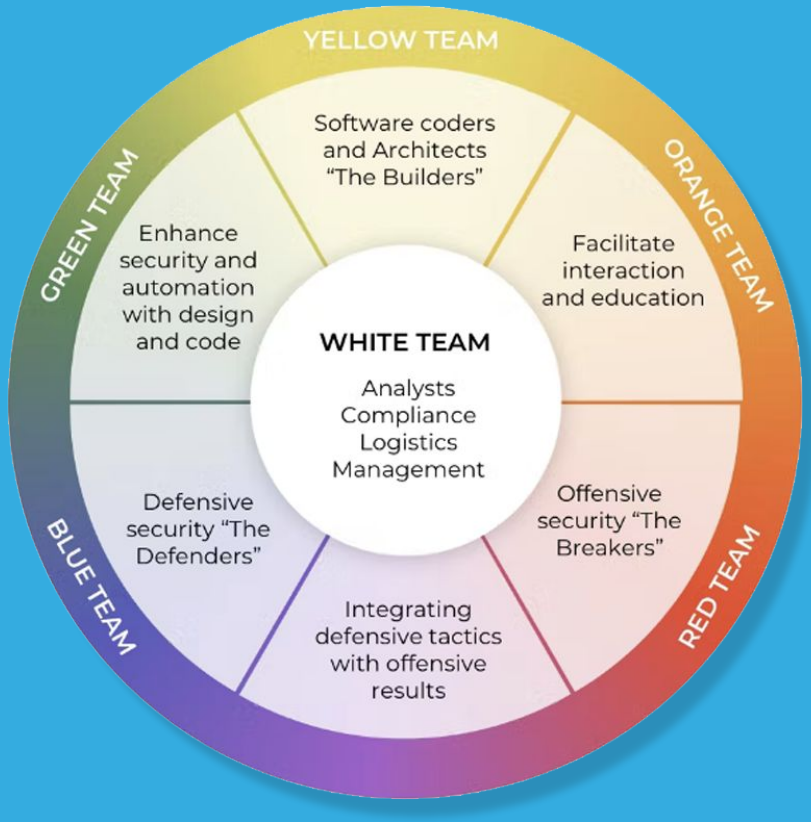
BLUE TEAMS

Deel 2

PXL DIGITAL


YELLOW TEAM
Software coders and Architects "The Builders"
ORANGE TEAM
Facilitate interaction and education
RED TEAM
Offensive security "The Breakers"
Integrating defensive tactics with offensive results
BLUE TEAM
Defensive security "The Defenders"
GREEN TEAM
Enhance security and automation with design and code
WHITE TEAM
Analysts
Compliance
Logistics
Management

PXL DIGITAL

BLUE TEAM

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

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*

PXL DIGITAL

THE INCIDENT RESPONSE PLAN

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

PXL DIGITAL

THE INCIDENT RESPONSE PLAN

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

PXL DIGITAL

2. 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.

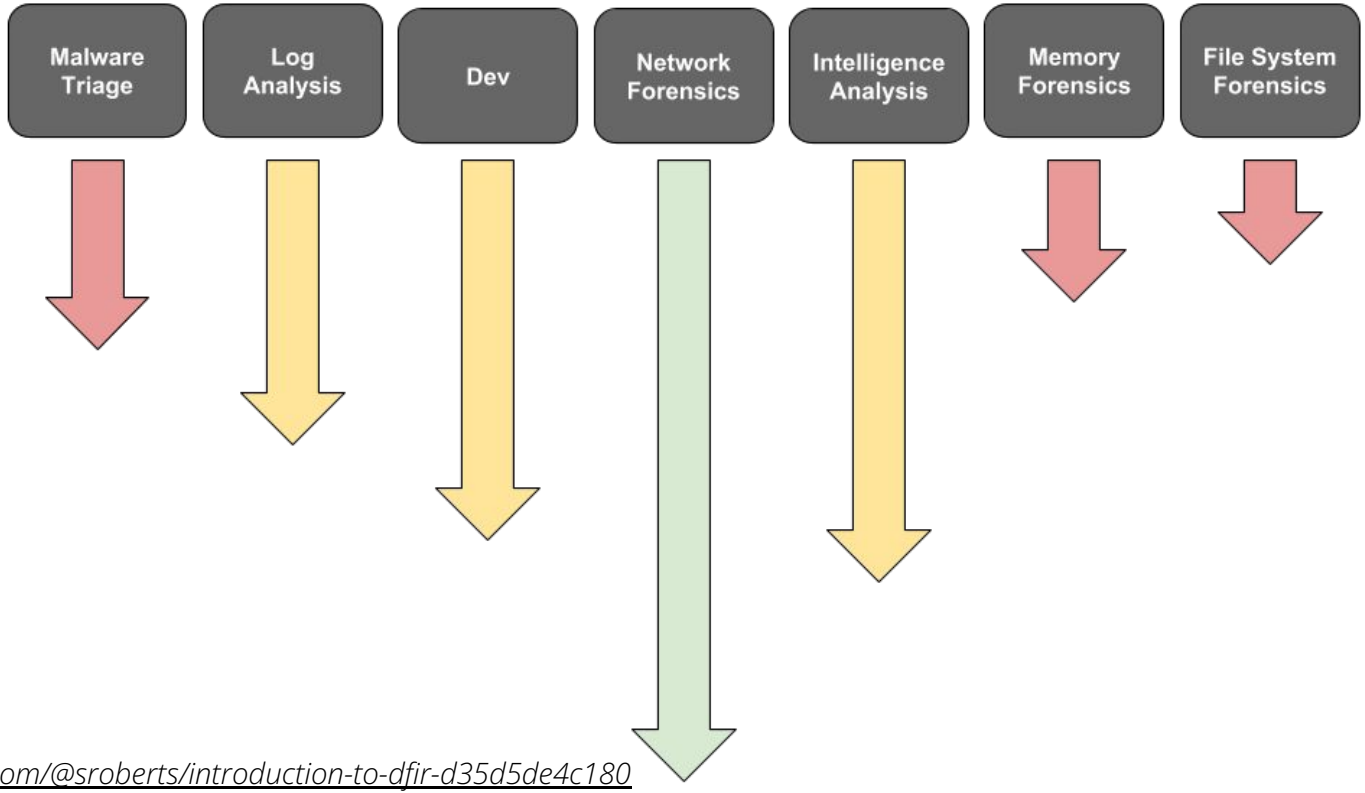
DEFINITION: DFIR

""Digital Forensics & Incident Response is a multidisciplinary profession that focuses on identifying, investigating, and remediating computer network exploitation. "

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

PXL DIGITAL

DFIR SKILLSET

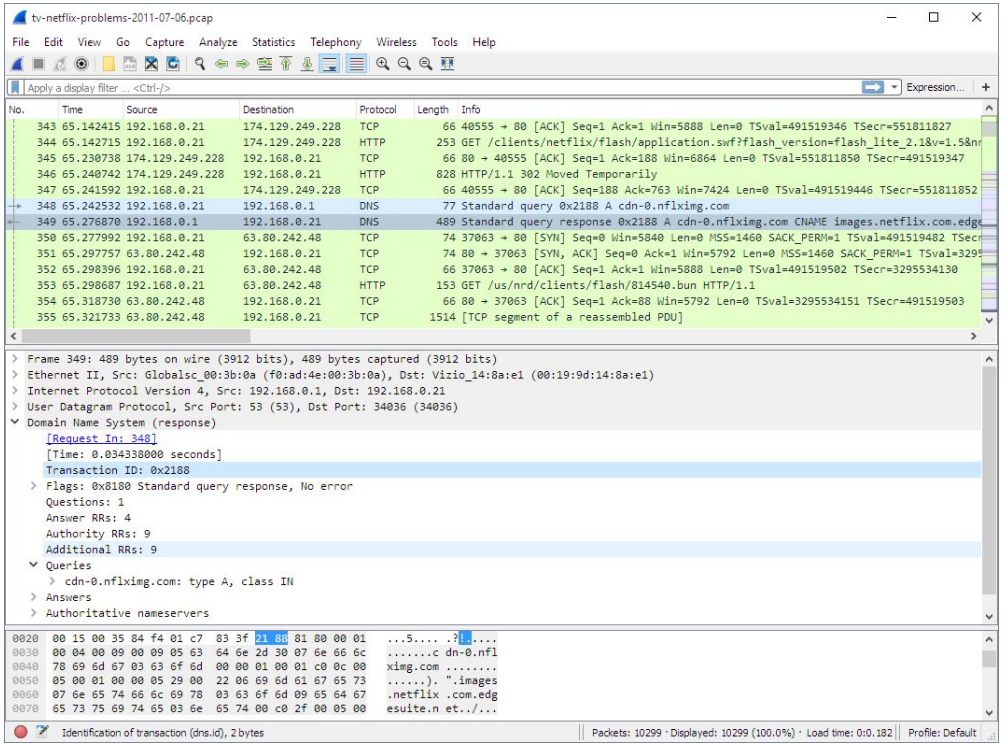


https://medium.com/@sroberts/introduction-to-dfir-d35d5de4c180

DFIR SKILLSET: TECHNICAL

NETWORK FORENSICS

- Wireshark, cf. Security Essentials
- Snort
- Suricata
- ...



PXL DIGITAL

DFIR SKILLSET: TECHNICAL

FILE SYSTEMS FORENSICS

Acquisition

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

PXL DIGITAL

DFIR SKILLSET: TECHNICAL

FILE SYSTEMS FORENSICS

NTFS File System

Extraction

Involves the retrieving of unstructured or deleted data

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

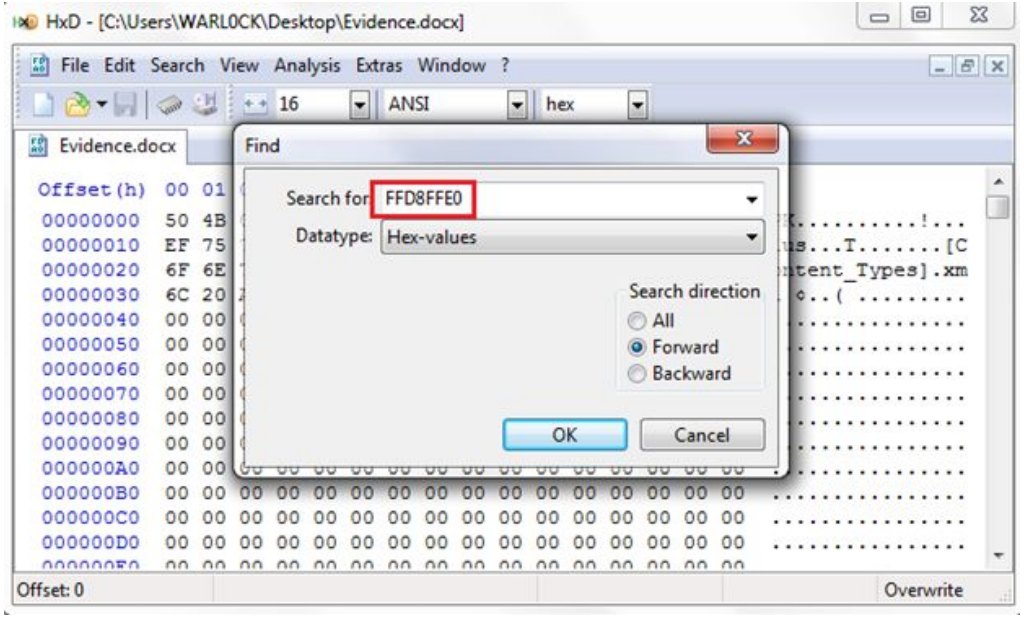
Other hiding techniques: encryption, steganography, file obfuscation…

DFIR SKILLSET: TECHNICAL

FILE SYSTEMS FORENSICS

File Carving

"Extracting data from unallocated space"



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

PXL DIGITAL

DFIR SKILLSET: TECHNICAL

FILE SYSTEMS FORENSICS

Tools

AUTOPSY
DIGITAL FORENSICS

ACCESSDATA®
ForensicToolkit (FTK)

PXL DIGITAL

DFIR SKILLSET: TECHNICAL

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.**

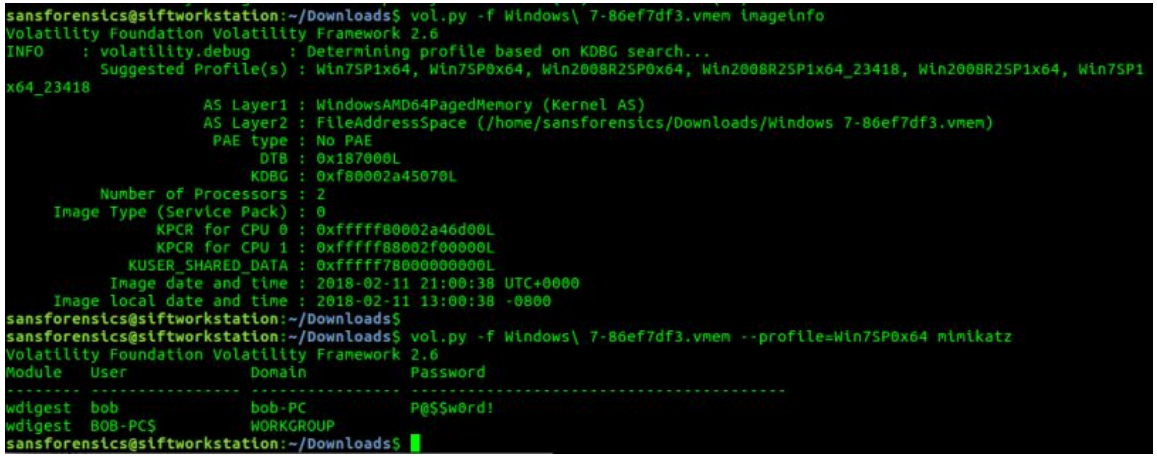
https://resources.infosecinstitute.com/memory-forensics/

DFIR SKILLSET: TECHNICAL

MEMORY FORENSICS

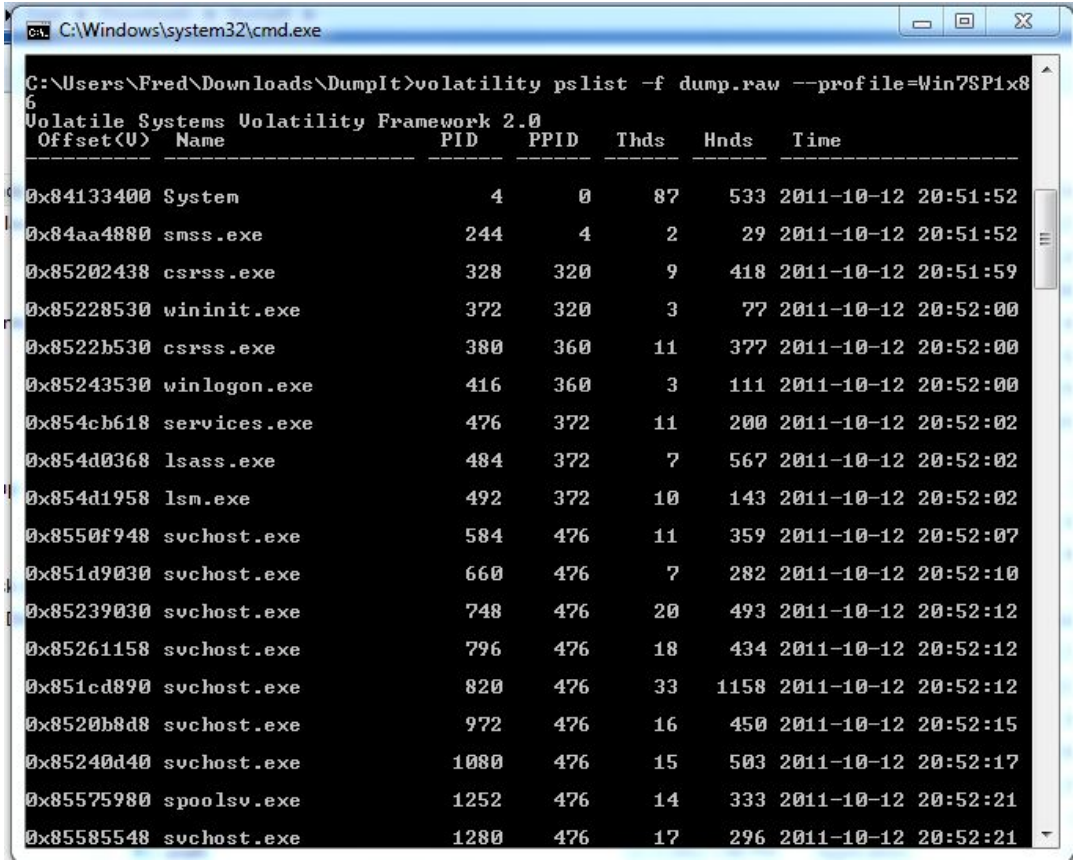
common methods and formats that are used today:

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



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

PXL DIGITAL


C:\Windows\system32\cmd.exe
C:\Users\Fred\Downloads\DumpIt>volatility pslist -f dump.raw --profile=Win7SP1x86
Volatile Systems Volatility Framework 2.0
Offset(V) Name PID PPID Thds Hnds Time
0x84133400 System 4 0 87 533 2011-10-12 20:51:52
0x84aa4880 smss.exe 244 4 2 29 2011-10-12 20:51:52
0x85202438 csrss.exe 328 320 9 418 2011-10-12 20:51:59
0x85228530 wininit.exe 372 320 3 77 2011-10-12 20:52:00
0x8522b530 csrss.exe 380 360 11 377 2011-10-12 20:52:00
0x85243530 winlogon.exe 416 360 3 111 2011-10-12 20:52:00
0x854cb618 services.exe 476 372 11 200 2011-10-12 20:52:02
0x854d0368 lsass.exe 484 372 7 567 2011-10-12 20:52:02
0x854d1958 lsm.exe 492 372 10 143 2011-10-12 20:52:02
0x8550f948 svchost.exe 584 476 11 359 2011-10-12 20:52:07
0x851d9030 svchost.exe 660 476 7 282 2011-10-12 20:52:10
0x85239030 svchost.exe 748 476 20 493 2011-10-12 20:52:12
0x85261158 svchost.exe 796 476 18 434 2011-10-12 20:52:12
0x851cd890 svchost.exe 820 476 33 1158 2011-10-12 20:52:12
0x8520b8d8 svchost.exe 972 476 16 450 2011-10-12 20:52:15
0x85240d40 svchost.exe 1080 476 15 503 2011-10-12 20:52:17
0x85575980 spoolsv.exe 1252 476 14 333 2011-10-12 20:52:21
0x85585548 svchost.exe 1280 476 17 296 2011-10-12 20:52:21

DFIR SKILLSET: TECHNICAL

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 SKILLSET: TECHNICAL

MEMORY FORENSICS

Tools

DFIR SKILLSET: TECHNICAL

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 SKILLSET: TECHNICAL

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 SKILLSET: TECHNICAL

INTELLIGENCE ANALYSIS

Tools & tricks:

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

DFIR SKILLSET: TECHNICAL

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

PXL DIGITAL

DFIR SKILLSET: TECHNICAL

DEVELOPMENT

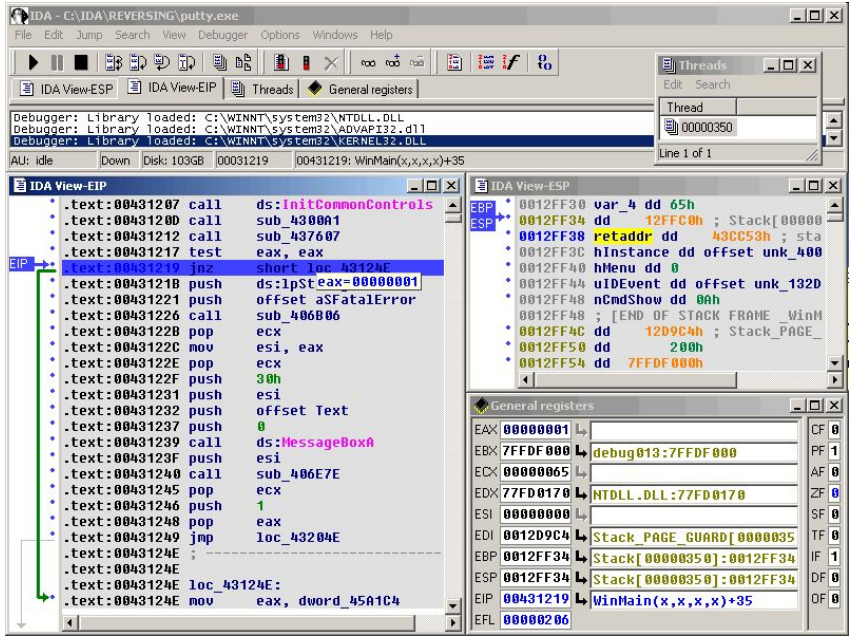
Technology changes quickly, the companies we defend move quickly, and if you're waiting for a company or open source project to build the tool you need you'll always be behind.

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 SKILLSET: TECHNICAL

MALWARE TRIAGE

Recognize, analyse and reverse-engineering



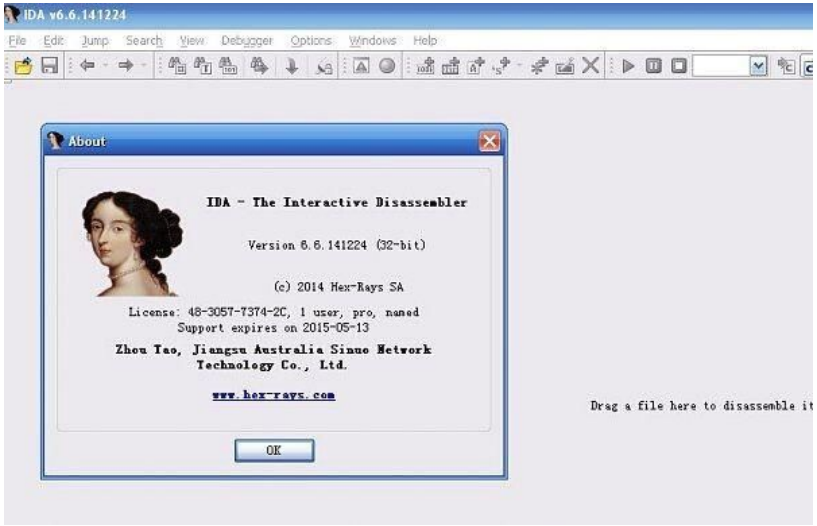
https://resources.infosecinstitute.com/category/certifications-training/malware-analysis-reverse-engineering/

PXL DIGITAL

DFIR SKILLSET: TECHNICAL

MALWARE TRIAGE

Tools



PXL DIGITAL

DFIR SKILLSET: SOFT SKILLS

Often overlooked, but very important!

- Investigation Process & Analysis
- Operational Security

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

DFIR SKILLSET: 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 SKILLSET: 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 VIDEOS

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 : Digital Forensics: Getting Started