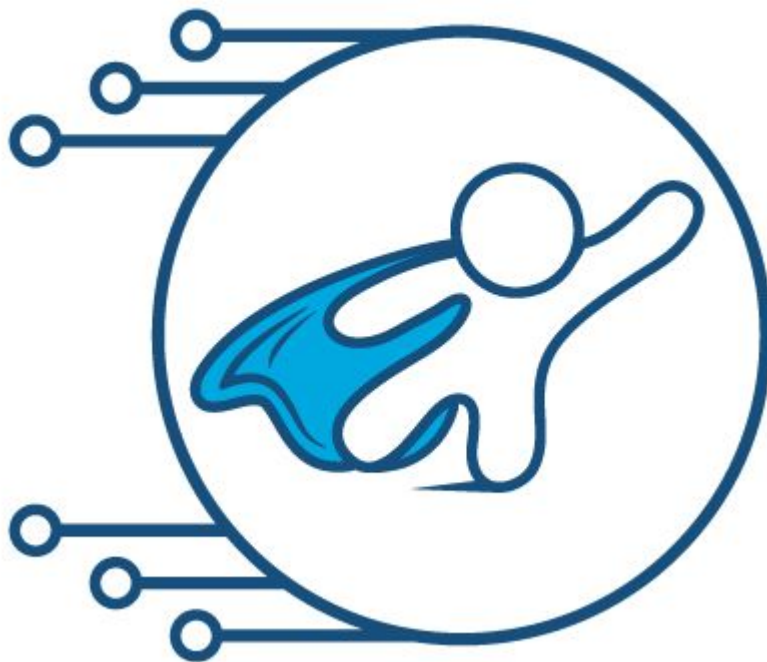


# Blue Teams



# INFOSEC WHEEL





## 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*

# 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

/əˈnælɪsɪs/

*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

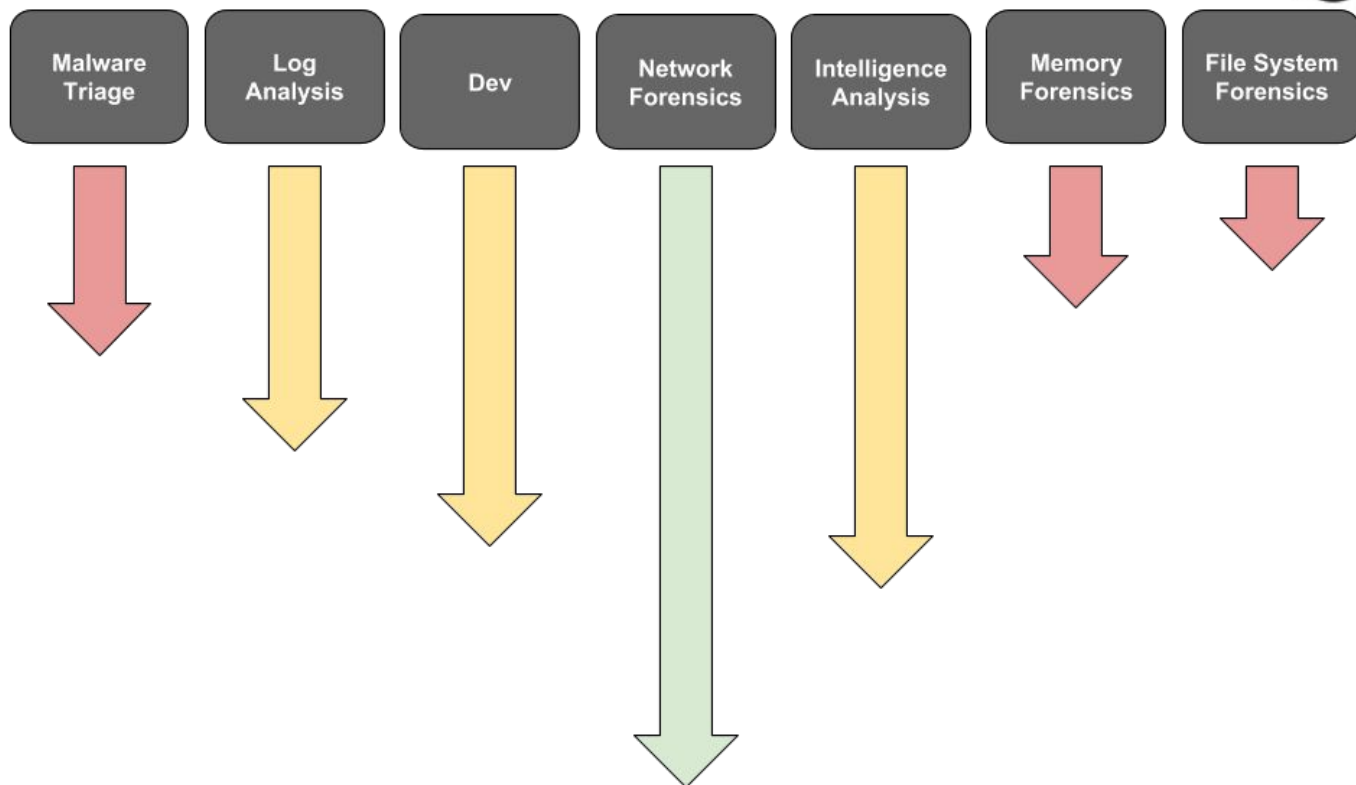


Definition:

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



# DFIR Skills



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



# DFIR skills

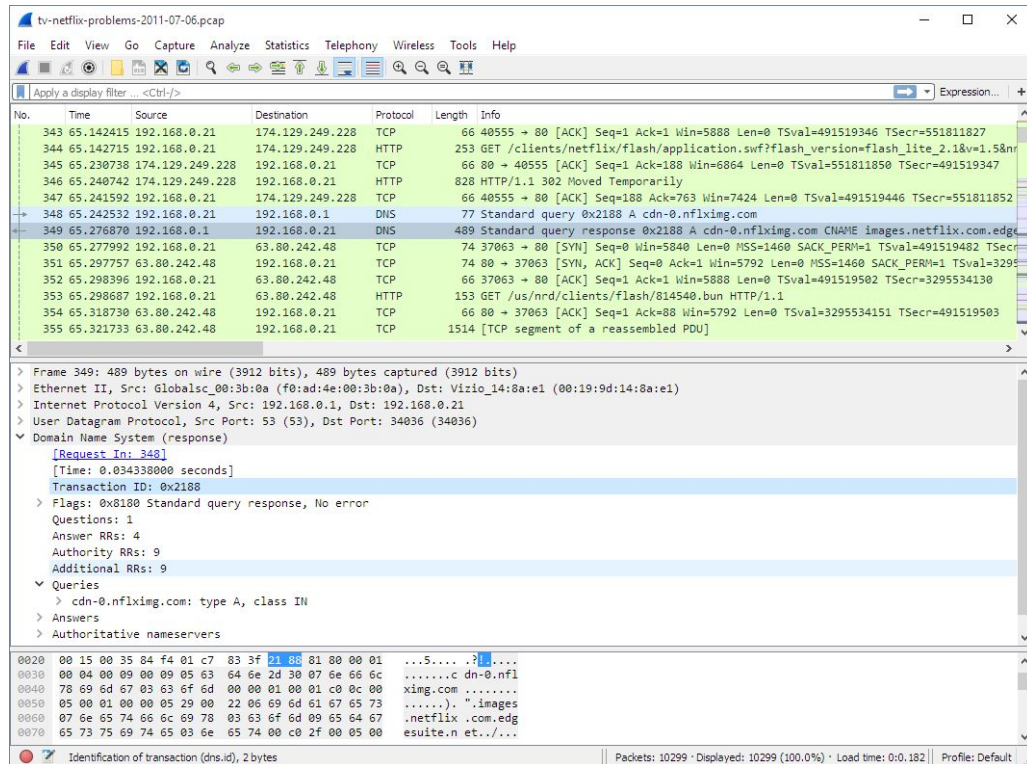


## Technical Skills

- Network Forensics

Covered in part in Security Essentials:  
Wireshark

Also with tools such as Snort & Suricata



# DFIR skills



## Technical Skills

- File System Forensics

### Acquisition

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



# DFIR skills



## 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...



NTFS File System

# DFIR skills



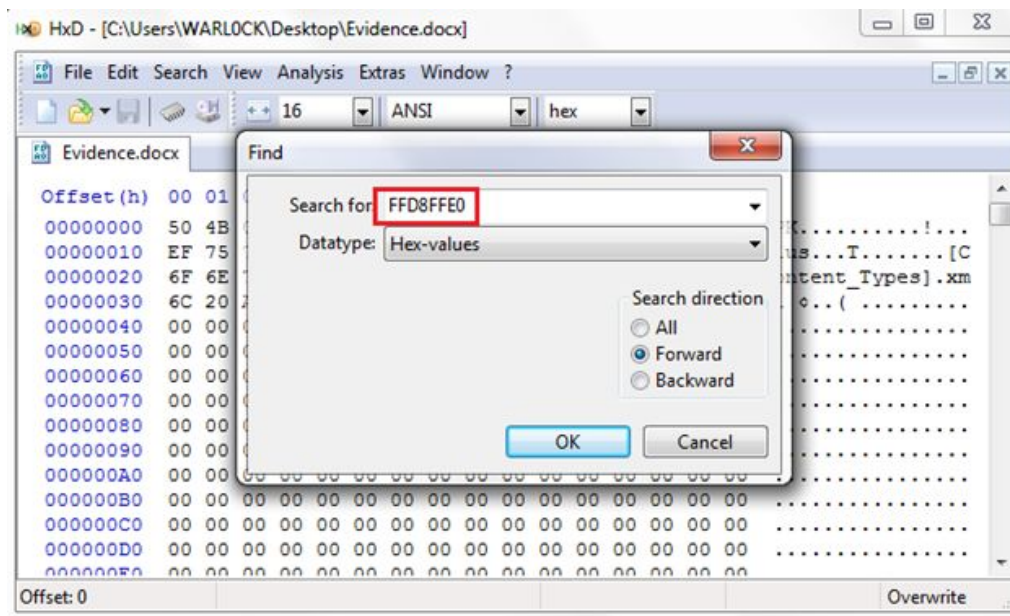
## Technical Skills

- File System Forensics

### File Carving

*“Extracting data from unallocated space”*

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



# DFIR skills



## Technical Skills

- File System Forensics

Practical Tools



**ACCESSDATA**<sup>®</sup>  
ForensicToolKit (FTK)



**AUTOPSY**  
DIGITAL FORENSICS

# 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**.

# DFIR skills



## Technical Skills

- Memory Forensics

common methods and formats that are used today:

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

```
sansforensics@siftworkstation:~/Downloads$ vol.py -f Windows\ 7-86ef7df3.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1
x64_23418
                        AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                        AS Layer2 : FileAddressSpace (/home/sansforensics/Downloads/Windows 7-86ef7df3.vmem)
                        PAE type : No PAE
                        DTB : 0x187000L
                        KDBG : 0xf80002a45070L
                        Number of Processors : 2
                        Image Type (Service Pack) : 0
                        KPCR for CPU 0 : 0xfffff80002a46d00L
                        KPCR for CPU 1 : 0xfffff80002f00000L
                        KUSER_SHARED_DATA : 0xfffff78000000000L
                        Image date and time : 2018-02-11 21:00:38 UTC+0000
                        Image local date and time : 2018-02-11 13:00:38 -0800
sansforensics@siftworkstation:~/Downloads$
sansforensics@siftworkstation:~/Downloads$ vol.py -f Windows\ 7-86ef7df3.vmem --profile=Win7SP0x64 mimikatz
Volatility Foundation Volatility Framework 2.6
Module  User          Domain          Password
-----
wdigest bob             bob-PC         P@$Sw0rd!
wdigest BOB-PCS    WORKGROUP
sansforensics@siftworkstation:~/Downloads$
```



# DFIR skills

## Technical Skills

```
C:\Windows\system32\cmd.exe

C:\Users\Fred\Downloads\DumpIt>volatility pslist -f dump.raw --profile=Win7SP1x86
Volatility Systems Volatility Framework 2.0
Offset(U)  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 skills



## Technical Skills

- Memory Forensics

### Examining Your Captured Data

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



# DFIR skills



## 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

## 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

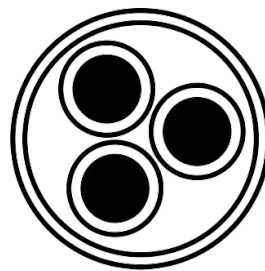


## Technical Skills

- Intelligence Analysis <sup>[OBJ]</sup>

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.

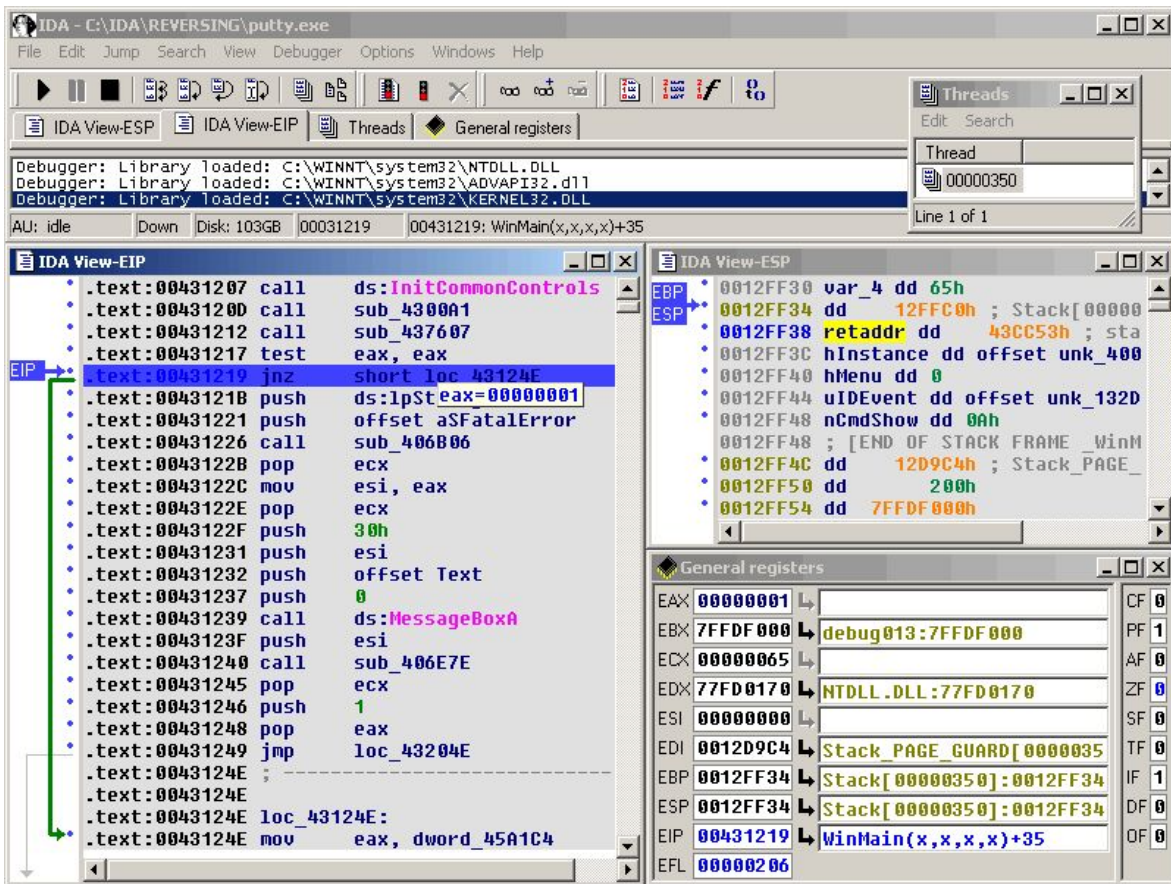
# DFIR skills

## Technical Skills

- Malware Triage

Recognize, analyse and reverse-engineering

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





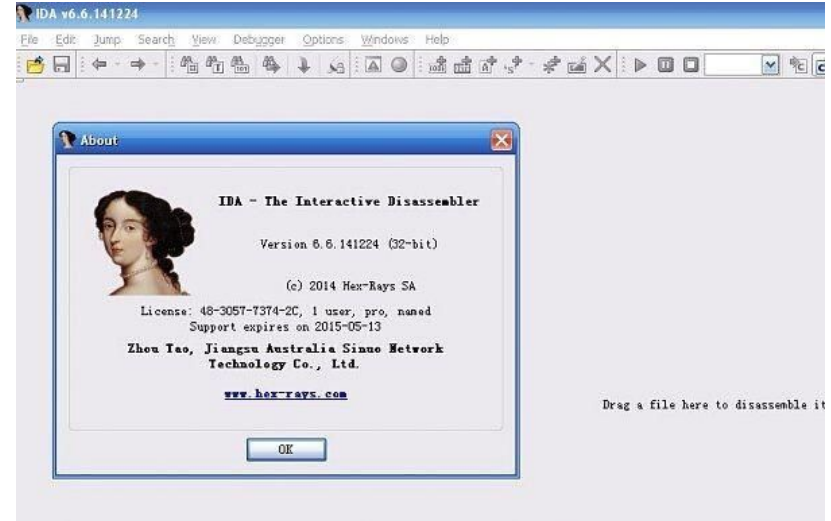
# DFIR skills



## 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



## 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

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