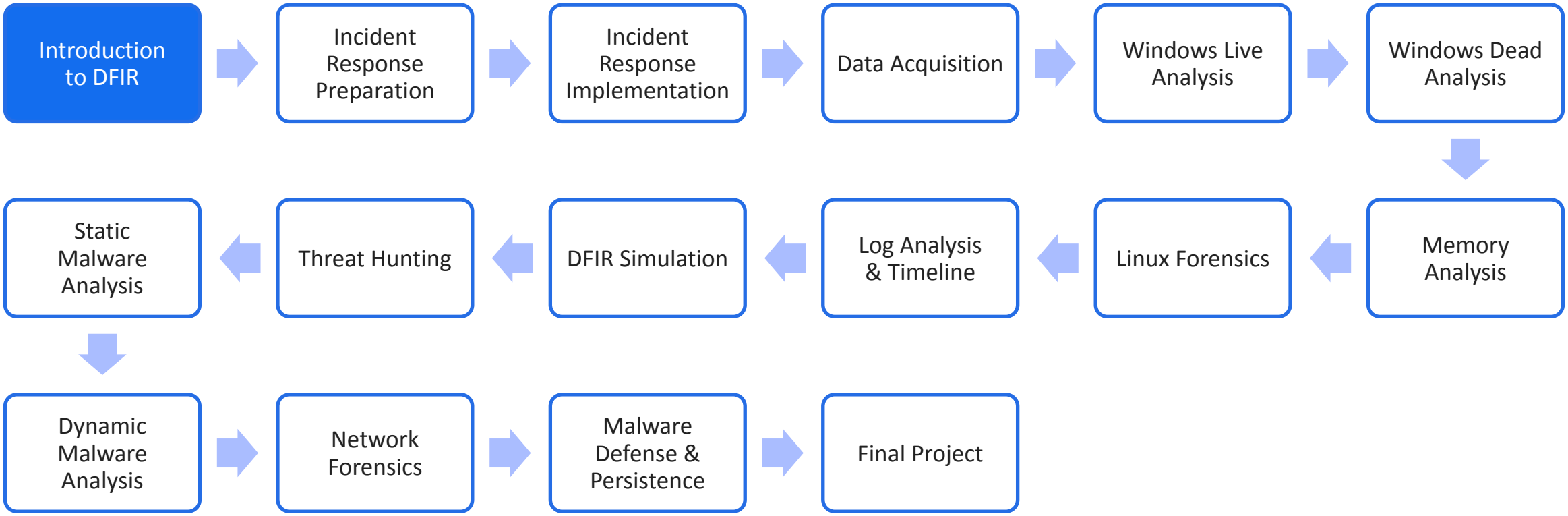
Cybersecurity Professional Program

Introduction to DFIR

Digital Forensics & Incident Response

Digital Forensics & Incident Response

Course Path



Digital Forensics & Incident Response

Technical Interview Workshop

- Designed to help you prepare and practice for technical interview scenarios
- We want you to feel as comfortable and confident as possible during the technical interview process.
- Complete the Career Outcomes curriculum.

Objectives

Learn about DFIR, including how it is planned and its processes, tools, and methods.

- Introduction to DFIR
- Incident Response Planning
- DFIR Process
- DFIR Toolset
- DFIR Use Case
- DFIR Environment
- DFIR Scenarios

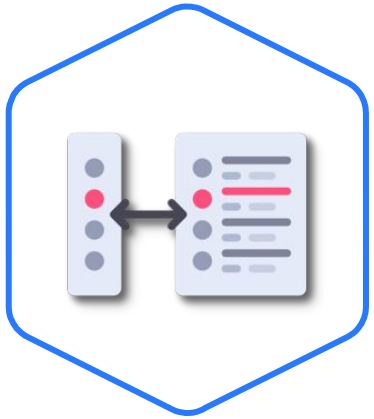
Introduction to DFIR

Introduction to DFIR

Digital Forensics & Incident Response

Digital Forensics (DF)

Examining and analyzing artifacts after a cyberattack



Incident Response (IR)

Performing actions when a security breach occurs

DFIR

Investigating and responding to a cyberattack after an incident

What Is Digital Forensics?

- Revealing and collecting all electronic data without modifying or contaminating it
- Preserving evidence and reconstructing past events

What Is Incident Response?

- Confronting and managing a security breach or attack
- Reducing damage and the cost of the recovery effort

What Is Threat Hunting?

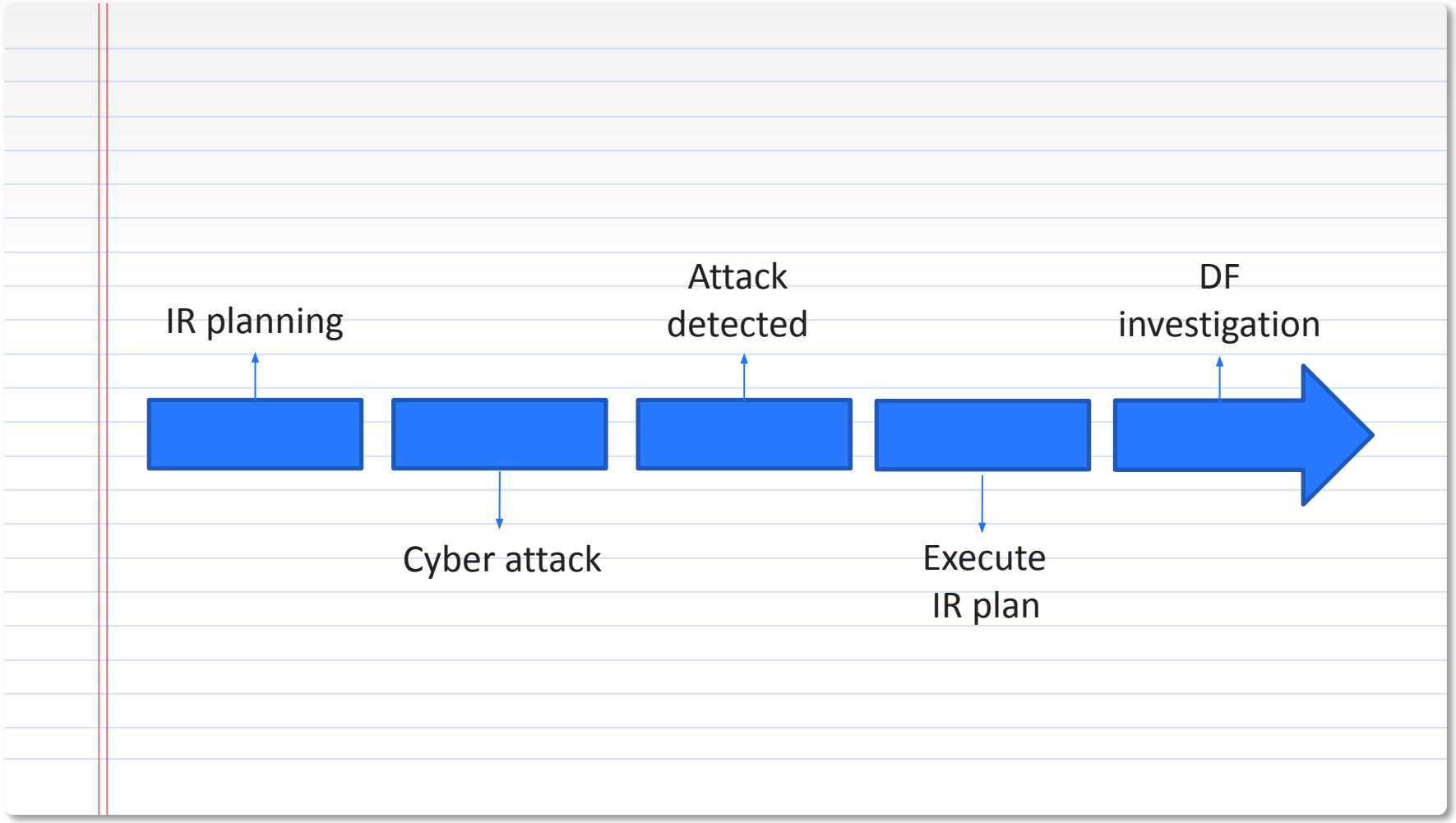
- Active defense
- Proactively searching for threats

DF vs. IR vs. TH

DF		IR		TH
Digital forensics		Incident response		Threat hunting
After an attack		During an attack		All the time
Find evidence	VS.	Reduce further damage	VS.	Find undetected threats
Host and network		Host and network		Host and network
Tier 3 in an SOC		Tier 2 in an SOC		Tier 3 in an SOC

DFIR Timeline

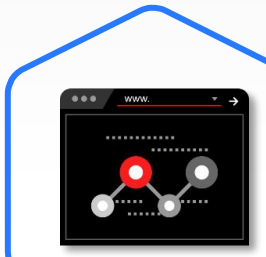
- IR planning should be done prior to an attack.
- The average time for an attack to be detected is 6 months.
- Digital forensics relies on data collected during IR.



Introduction to DFIR

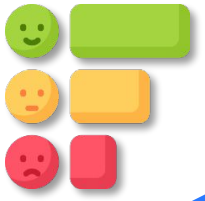
Incident Response Planning

Incident Responder Responsibilities



Establish an effective incident response plan (IRP) and maintain its effectiveness based on potential threats.

Investigate current and past incidents and analyze them.



Provide recommendations according to analyzed incident findings.

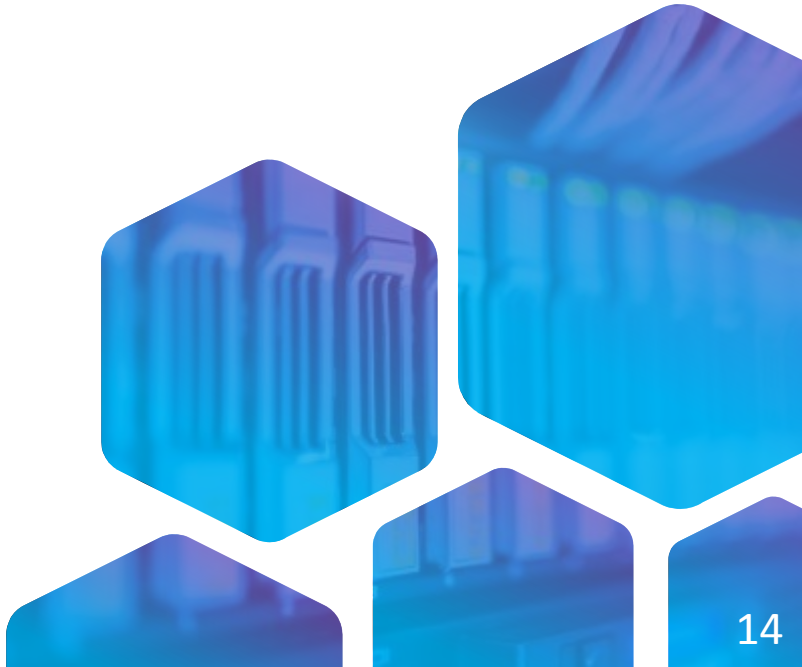
IR Execution

Successful IR

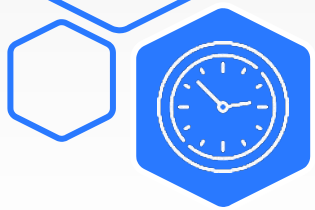
A good plan will provide a response for any relevant issue.

Following the Steps

The plan should include various steps, such as containment and eradication.



Six Stages



1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

Introduction to DFIR

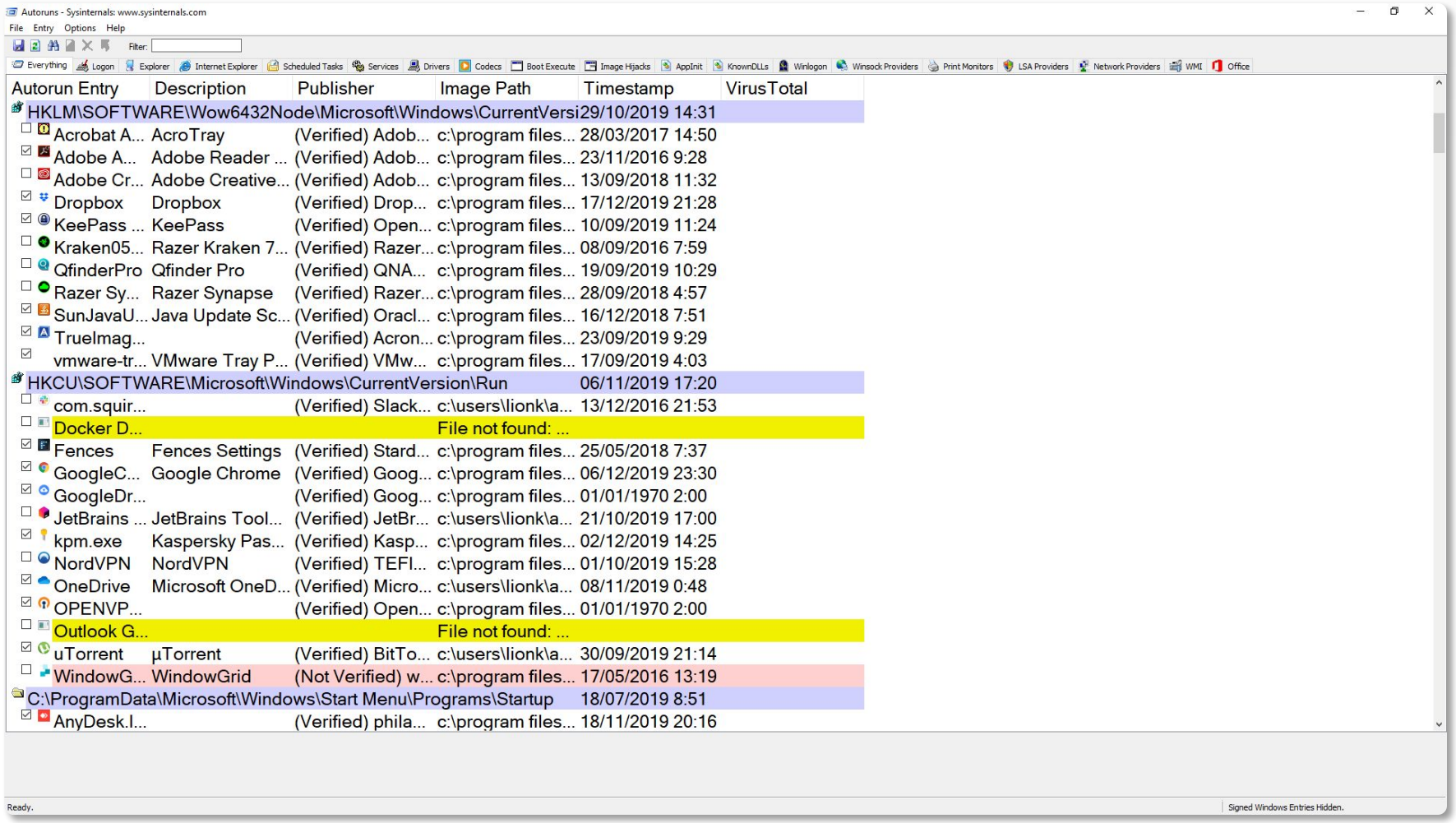
DFIR Process

What Is Evidence?

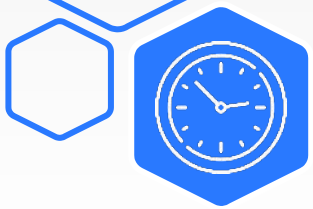
- **In a court of law:** Anything you saw, heard, or said that proves something occurred
- **In digital forensics:** Log records, files, processes, etc.

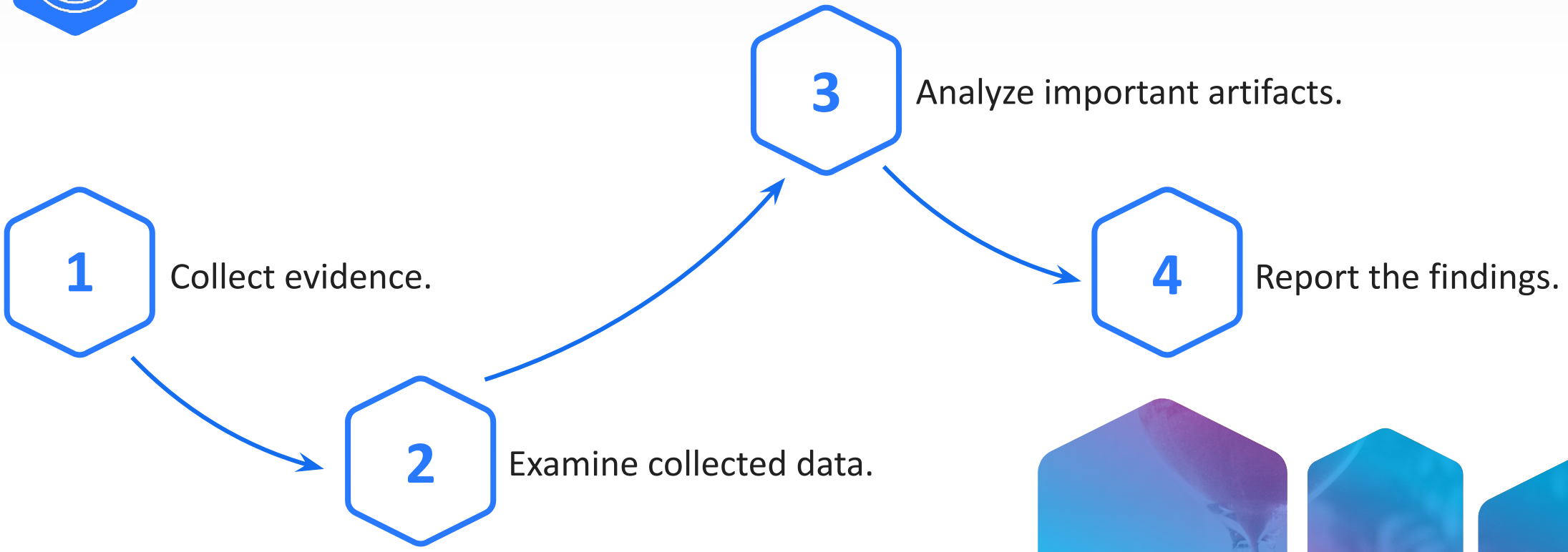
Example of Evidence

- Autoruns identifies possible startup locations.
- Startup programs can be evidence of persistent malware.
- The programs reside in known folders and registry keys.



DFIR Process





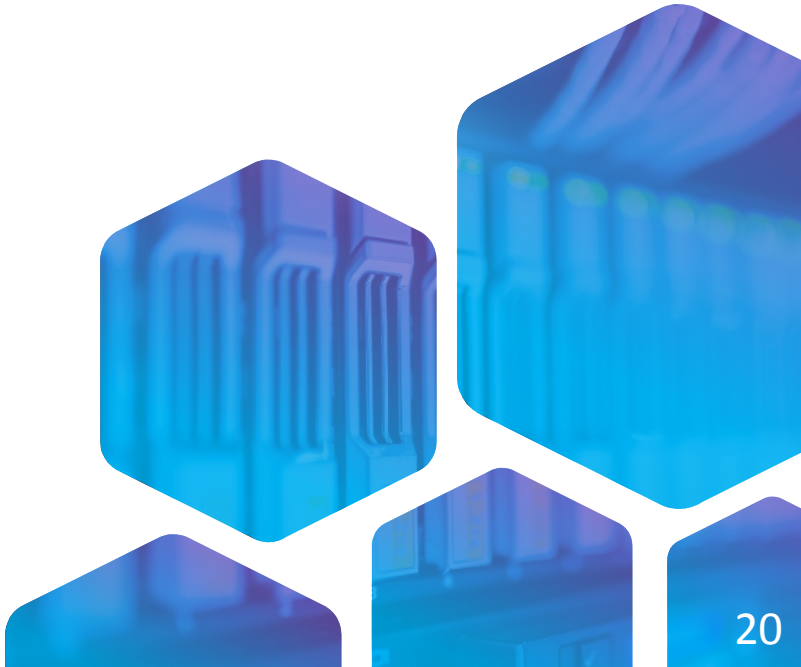
DF Analysis Types

Dead Analysis

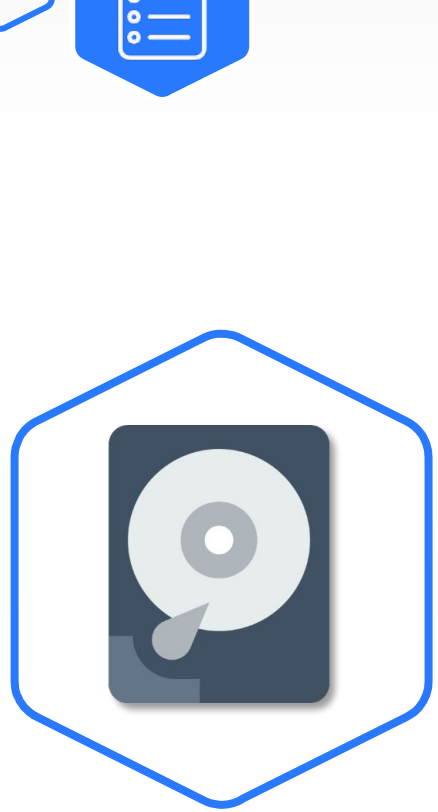
- Analyzing powered-off computers
- May include analysis of cloned drives

Live Analysis

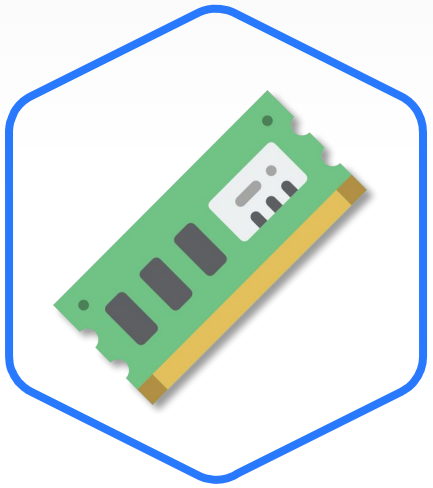
- Analyzing powered-on computers



Targeted Artifacts



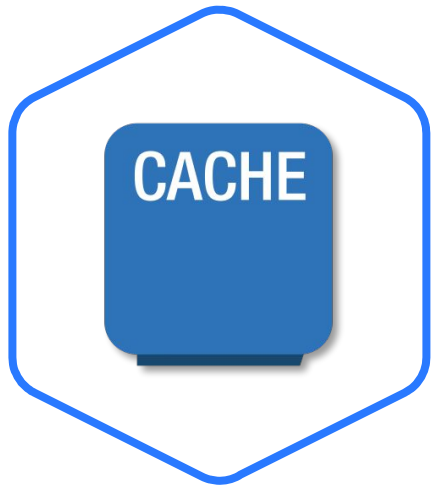
Files on a Drive



Memory Artifacts

Processes

Log Files

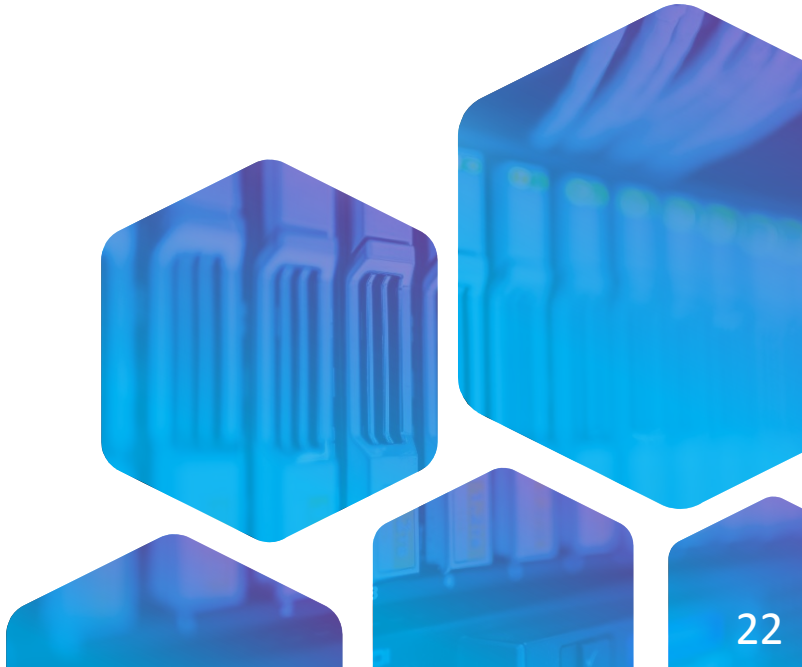


Cached Data

DF Domains

Network Forensics
Focuses on gathering data about traffic passing through network equipment

Host Forensics
Focuses on gathering data regarding hosts, such as files or memory



DFIR Process

Lab DFIR-01-L1

Detecting Startup Programs

20–30 min.

Mission

> Discover evidence of programs executed upon startup in your PC.

Steps

- Download and install Autoruns.
- Complete the requested tasks.

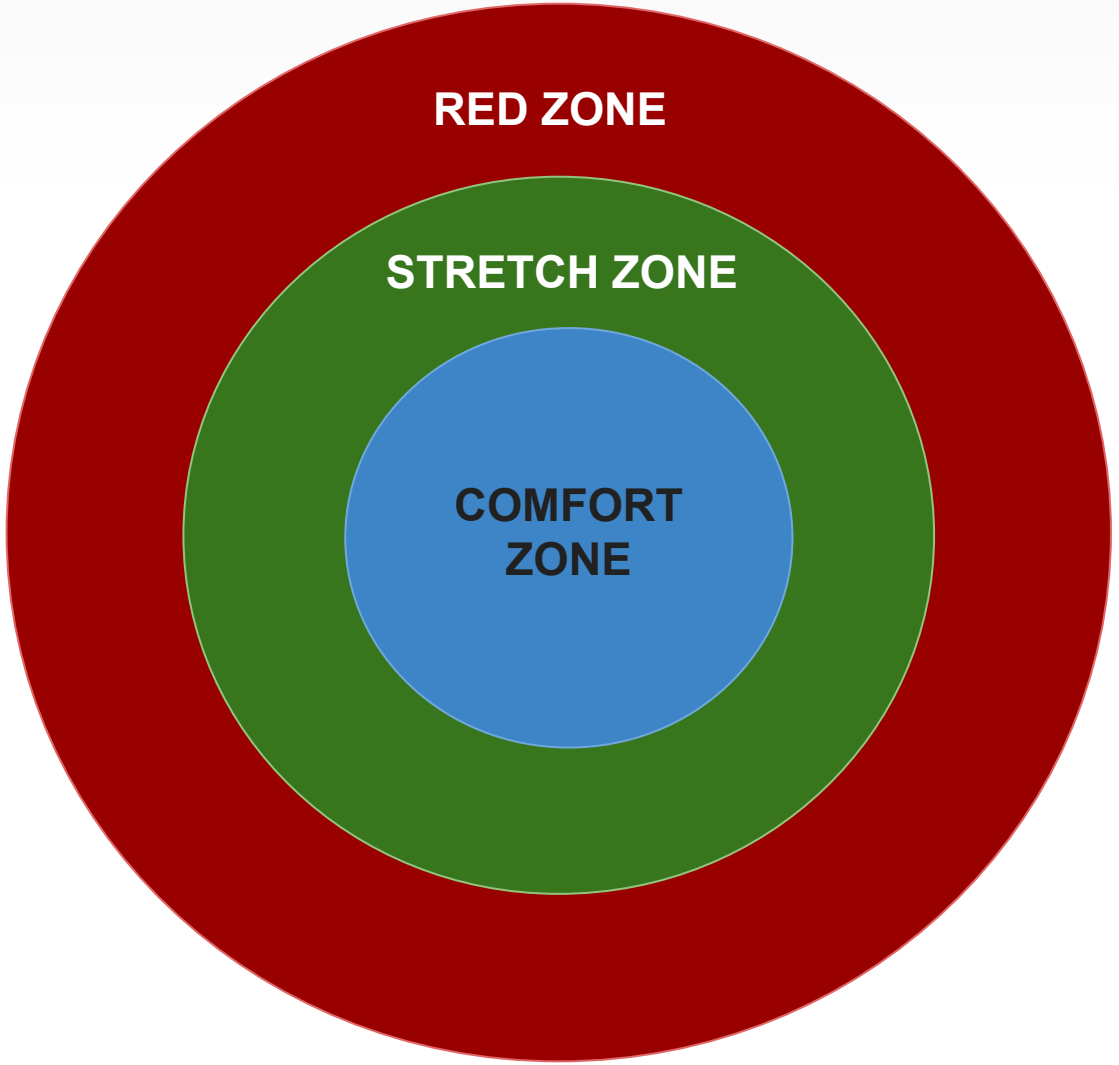
Environment & Tools

- VirtualBox
- Windows 10
- Autoruns
- AnyDesk

Related Files

- Lab document
- ***Autoruns.zip***
- ***AnyDesk.exe***

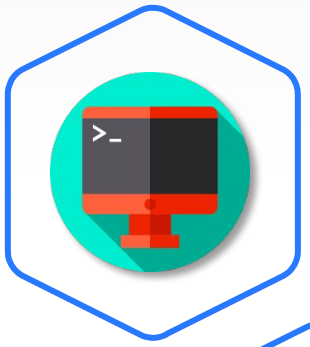
Pulse Check



Introduction to DFIR

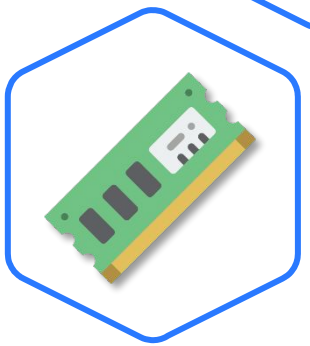
DFIR Toolset

Acquisition Tools



dd (Data Dump): Drive Acquisition
A Linux utility for managing and converting storage drives

FTK Imager: Drive and Memory Acquisition
Advanced forensic GUI-based program that enables multiple operations on images



DumpIt: Memory Acquisition
A memory acquisition tool often used in Windows-based systems

Drive Inspection Tools

Autopsy: Open-Source
Autopsy is part of the sleuth kit collection of Python tools used for forensic investigations.

FTK: Proprietary
Includes tools for cloned drive inspection

EnCase: Proprietary
Includes many advanced features for image inspection

Memory Inspection

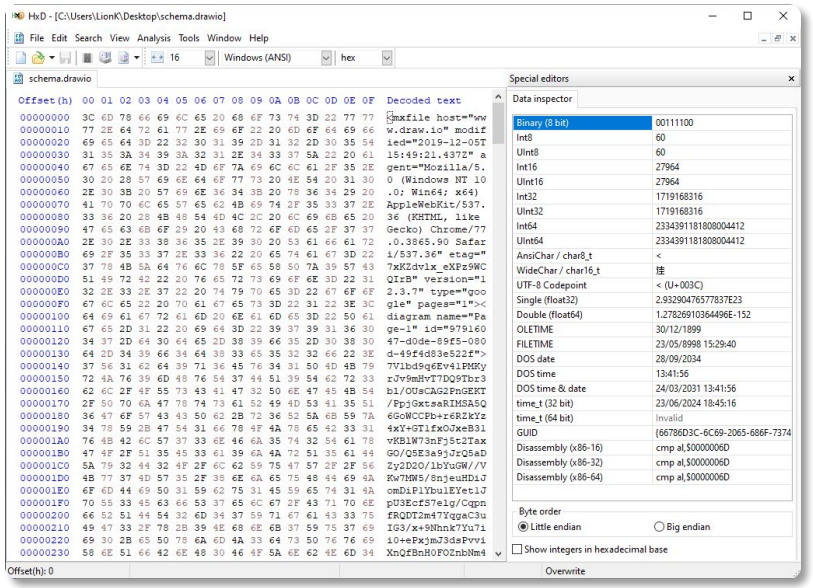
Volatility Framework
Open-source collection of Python tools supported by both Linux and Windows

Rekall
Open-source framework for advanced forensic and incident response

> Not many tools exist that can perform computer memory forensics.

DFIR Toolset

Data Carving



Bulk Extractor
Attempts to recover files without using a file system structure

HxD
Although not carving software, it is commonly used to view raw data.

PhotoRec
A powerful carving tool mainly focused on media files

DFIR Toolset

Process Investigation

A key step in DFIR is investigating processes of infected systems.

In Windows, this can be done using Sysinternals tools.

The tools include a process explorer and process monitor.

Network Forensics

Wireshark: Static Analysis
Operates on data that was already captured

NetworkMiner
Focuses more on artifact recovery than protocol analysis

> If network monitoring was not configured prior to an attack, it will only be relevant for memory artifacts (MA).

Customized Tools

- Some tools can only be used for specific devices, such as DVRs.
- Some forensic tools are custom-made for dedicated parsing.

- Hashing is a common identification method
- Can prove the identity of specific files

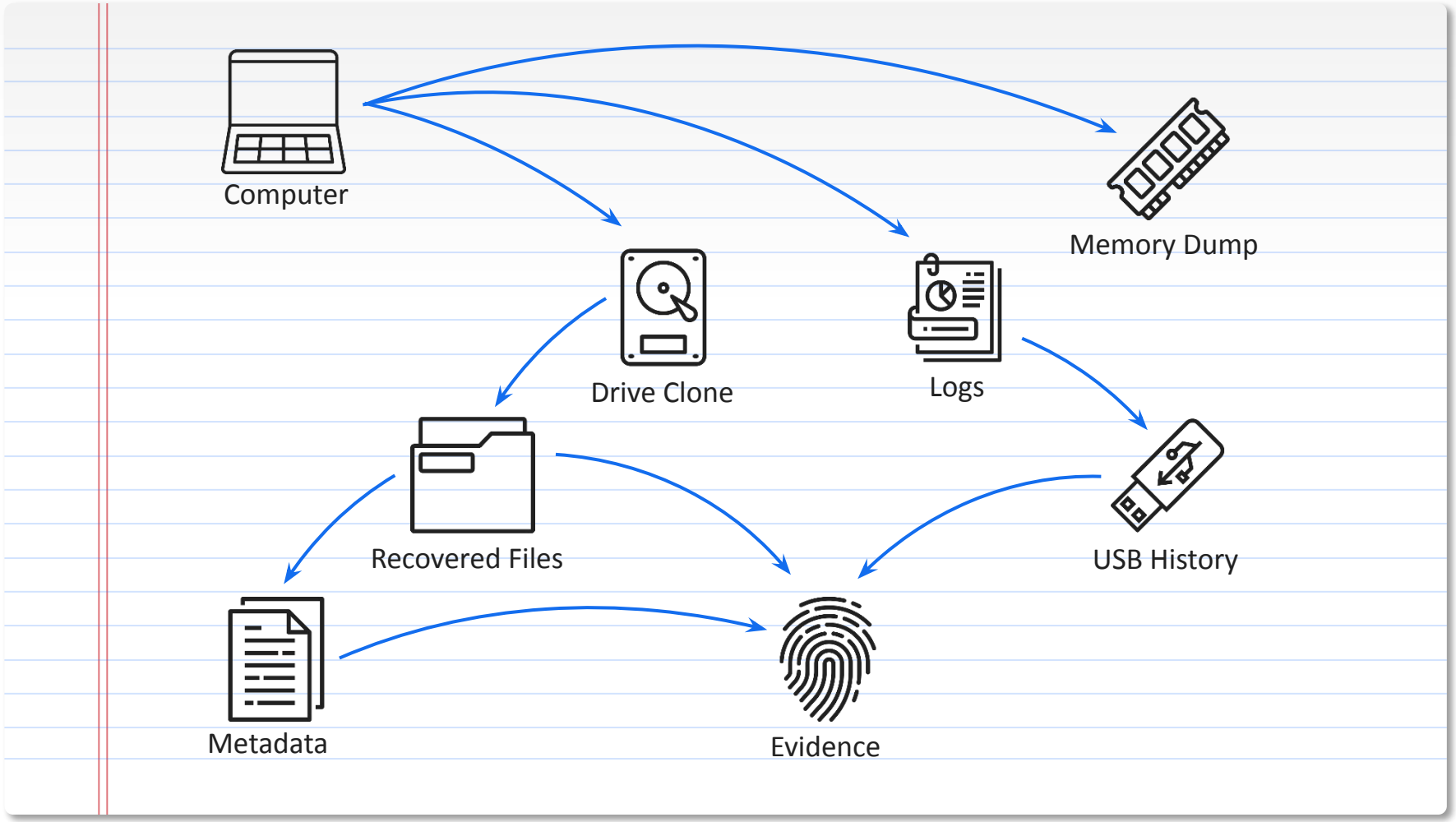
Introduction to DFIR

DFIR Use Case

DFIR Use Case

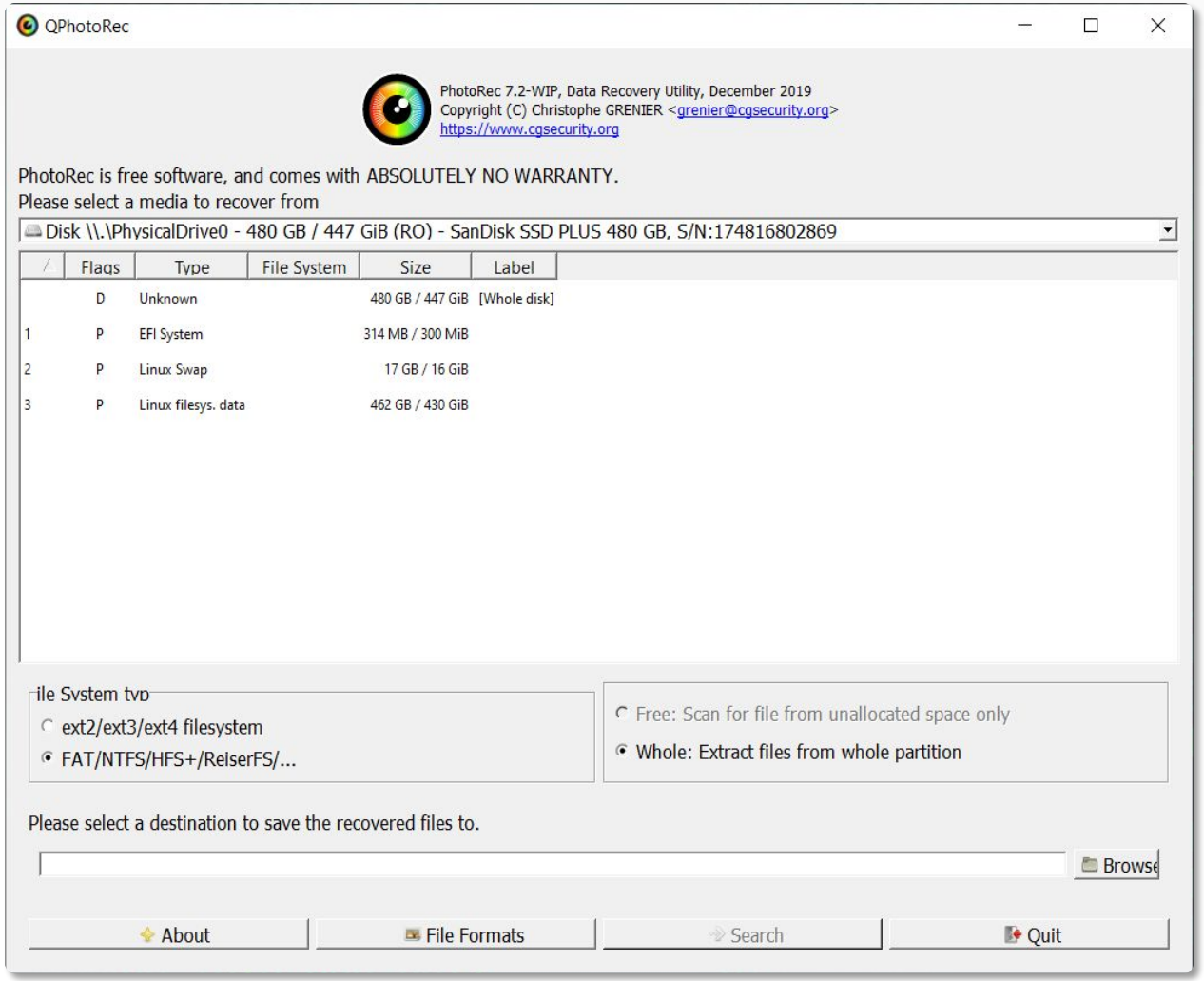
DF Scenario: Data Leak

- DF can be used to prove data leak events.
- File carving can be used to identify if files existed on media devices even after deletion.
- Hashing can be used to verify file identification.



DFIR Use Case

PhotoRec



Files deleted from a drive are not necessarily destroyed.

They can often be recovered using special software.

Tools like PhotoRec can parse drive images without accessing the file system.

DFIR Use Case

Metadata and EXIF

- Files contain metadata hidden from the user.
- Metadata can include information regarding camera model and location.
- Tools like ExifTool can read this data and help the investigation.

```
C:\Users\JohnD\Desktop>exiftool Photo.jpg
ExifTool Version Number         : 11.80
File Name                       : Photo.jpg
Directory                       : .
File Size                       : 78 kB
File Modification Date/Time     : 2019:07:24 09:49:41+03:00
File Access Date/Time           : 2019:12:22 18:39:08+02:00
File Creation Date/Time         : 2019:12:22 18:39:08+02:00
File Permissions                : rw-rw-rw-
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.02
...
Red Tone Reproduction Curve     : (Binary data 2060 bytes, use -b option to extract)
Technology                      : Cathode Ray Tube Display
Viewing Cond Desc               : Reference Viewing Condition in IEC 61966-2-1
Media White Point               : 0.9642 1 0.82491
Profile Copyright               : Copyright International Color Consortium, 2009
Chromatic Adaptation            : 1.04791 0.02293 -0.0502 0.0296 0.99046 -0.01707 -0.00925 0.01506
0.75179
Image Width                     : 628
Image Height                    : 960
Encoding Process                : Progressive DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 628x960
```

DFIR Use Case

What Is EXIF?

- Includes GPS coordinates, camera models, and the exact time a photo was taken
- Can be used as evidence when an investigator recovers photos

DFIR Use Case

Lab DFIR-01-L2

Data Leak Investigation

20–30 min.

Mission

> Recover files from a suspicious USB drive image and prove they were used to steal sensitive data.

Steps

- Recover files from a USB image.
- Prove they match the sensitive data.
- Extract EXIF and metadata.
- Find the identity of the leaker.

Environment & Tools

- VirtualBox
- Windows 10
- PhotoRec
- ExifTool
- Hashing software

Related Files

- Lab document
- ***Evidence.zip***
- ***testdisk-7.2-WIP.win.zip***
- ***hashmyfiles-x64.zip***
- ***exiftool-11.81.zip***

Introduction to DFIR

DFIR Environment

DF Distributions

Computer Aided INvestigative Environment (CAINE)
Used mainly for acquisition and live forensics

REMnux
Used mainly as a persistent forensics system for memory artifacts

FLARE VM
Used mainly for malware analysis

DFIR Environment

FlareVM

- Windows can be turned into a DF environment using the FlareVM script.
- The script installs and configures many MA and RE tools.

DFIR Environment

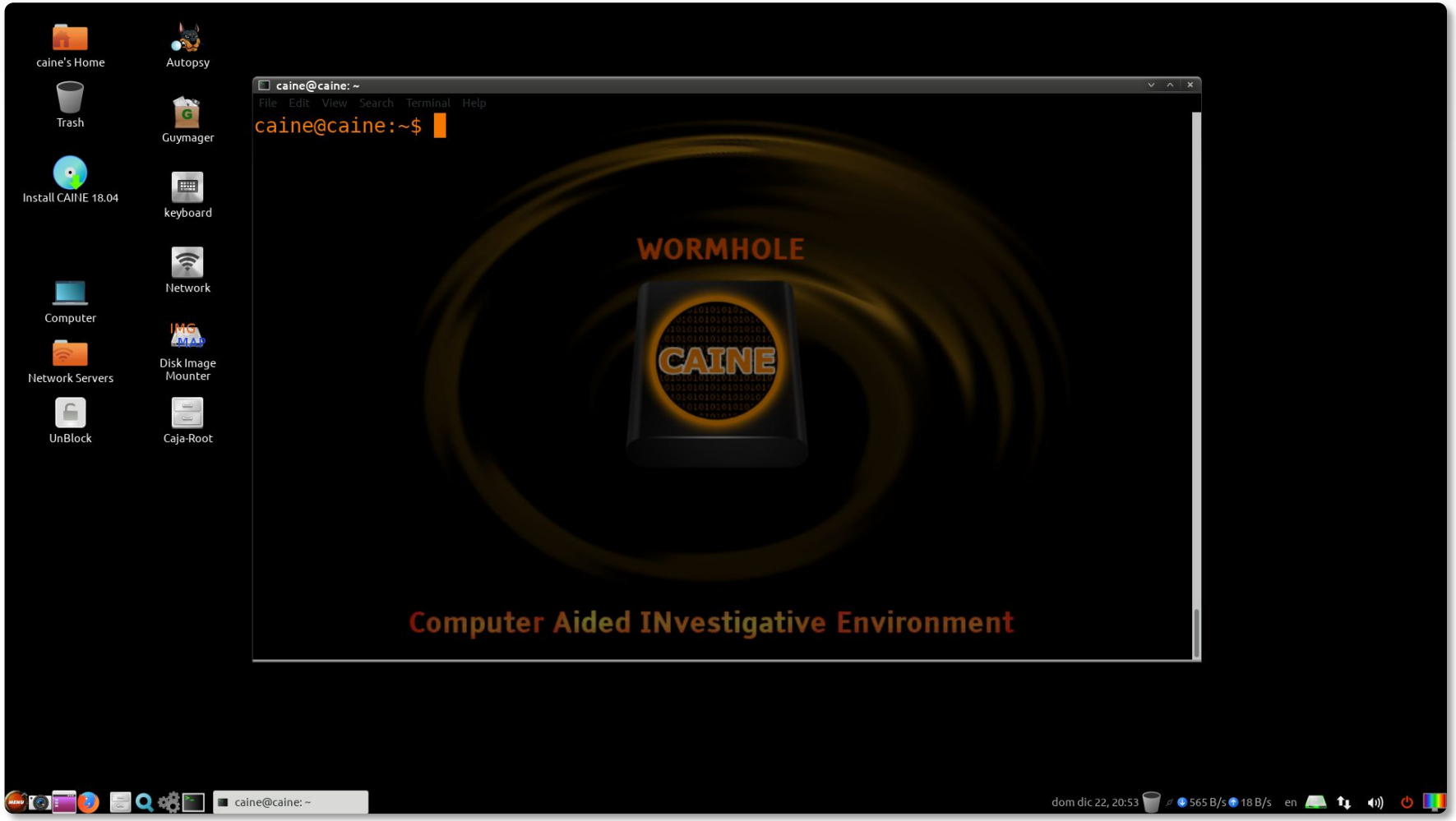
SIFT Workstation

- SIFT is a virtual Debian appliance dedicated to DF.
- Developed by SANS, a leading cybersecurity training institution
- Comes as a pre-packed OVA

DFIR Environment

CAINE Live

- CAINE is a distribution that runs from a live USB.
- Its main feature is the ability to run entirely from RAM.
- It enables real-time forensic acquisition.

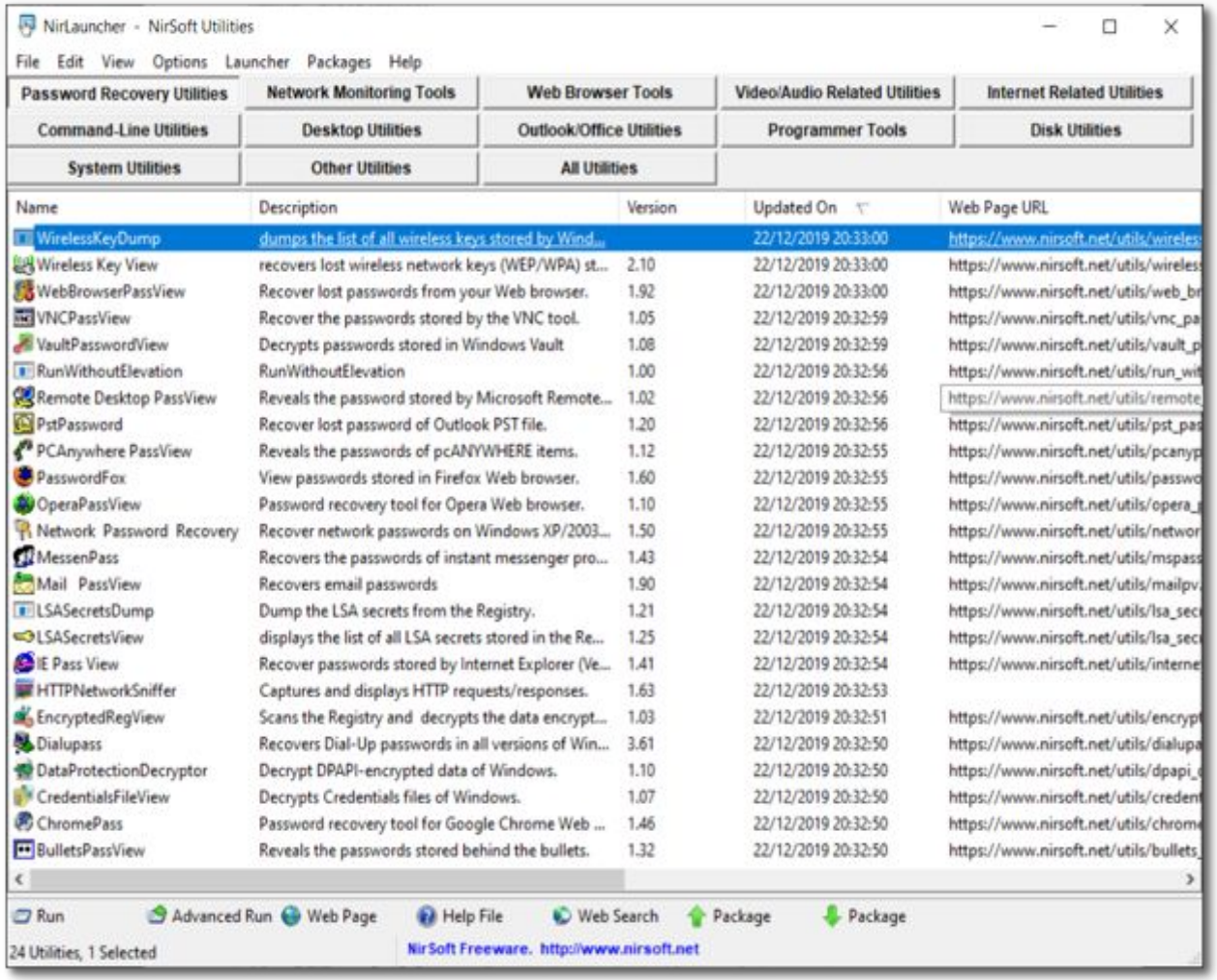


Benefits of Live USB

- An essential part of any forensics toolkit
- Used for data acquisition and live forensics

DFIR Environment

NirSoft Launcher



As with a live USB, most forensic distros include additional tools.

The tools can be executed without booting the distro.

NirSoft Launcher is an example of a unified interface for such tools.

Introduction to DFIR

DFIR Scenarios

DFIR for Social Engineering

- In phishing, SE refers to investigating the message and attached links.
- In real-world social engineering, the IR team can set up decoys.

- Traces are usually emails, messages, and suspicious links.
- The evidence is typically collected from employees.

DF for social engineering is followed by threat hunting to determine whether other employees were also affected.

DFIR for Web Server Defacing

Detect if and how the defacing occurred.

Restore the content of the original site from backup.

Intrusion Detection

Detect the intrusion point.

Identifying Persistence

Detect if any backdoors remain.

DFIR for Trojan Delivery

- Response depends on whether the trojan was already executed.
- If executed, it focuses on containment and eradication.

- Involves malware analysis
- Reveals actions the trojan performed in the system

DFIR Scenarios

Lab DFIR-01-L3

DFIR Incidents Overview

10–15 min.

Mission

Analyze multiple attack scenarios in an organization and suggest the best DFIR methodology.

Steps

- Review the scenario.
- Answer the questions.

Environment & Tools

- Text editor

Related Files

- Lab document

DFIR Scenarios

TDX Arena Challenge

Mission

> You were hired by a company to spy on its rivals.

Steps

- Select the lab link in Canvas to access TDX Arena.

Bird Watch

Thank You

Questions?