

Cybersecurity Professional Program

# Introduction to DFIR

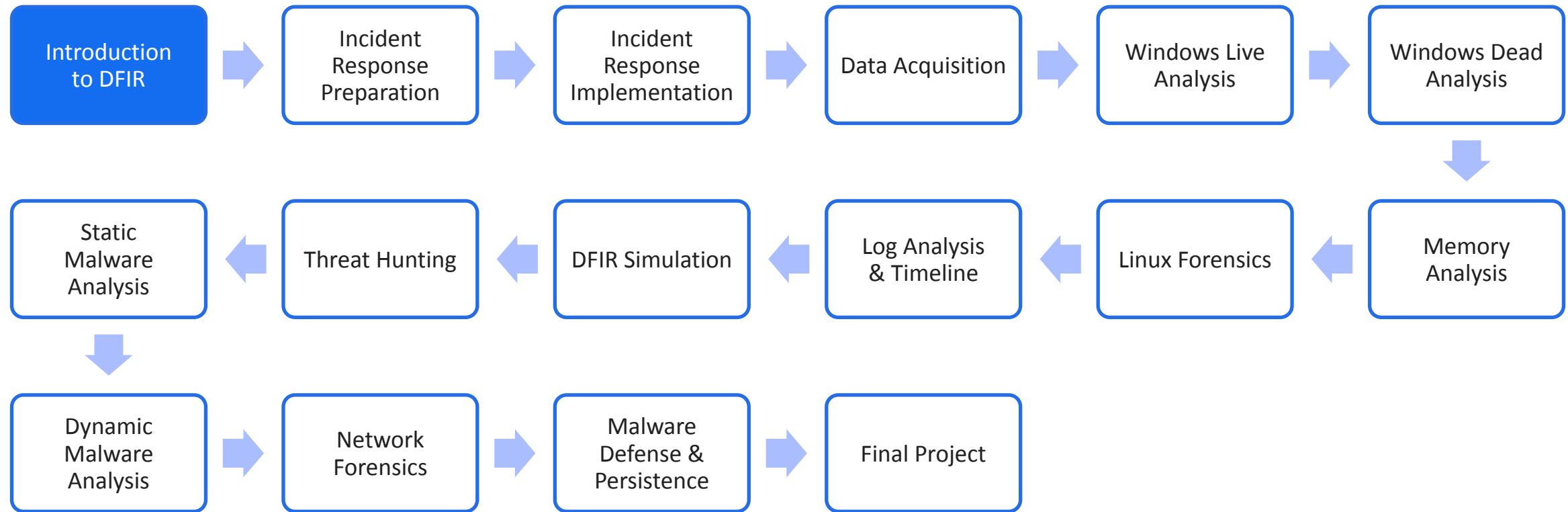
Digital Forensics & Incident Response





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.





# Introduction to DFIR

# 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

---

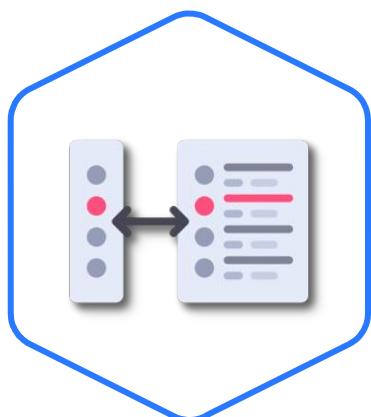
# Introduction to DFIR

# Digital Forensics & Incident Response



## Digital Forensics (DF)

Examining and analyzing artifacts after a cyberattack

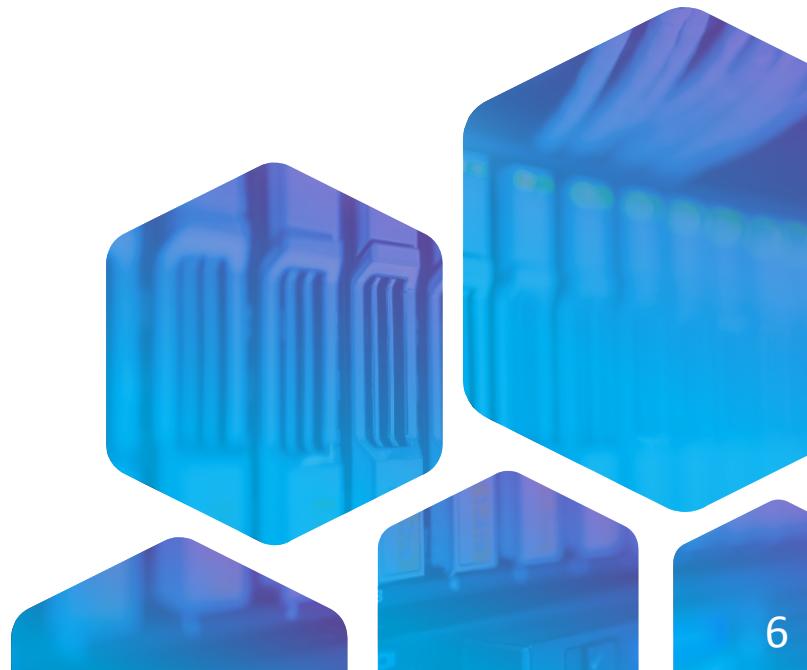


## Incident Response (IR)

Performing actions when a security breach occurs

## DFIR

Investigating and responding to a cyberattack after an incident





Introduction to DFIR

# 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**

Digital forensics

After an attack

Find evidence

Host and network

Tier 3 in an SOC

**IR**

Incident response

During an attack

Reduce further damage

Host and network

Tier 2 in an SOC

**TH**

Threat hunting

All the time

Find undetected threats

Host and network

Tier 3 in an SOC

**VS.**

**VS.**



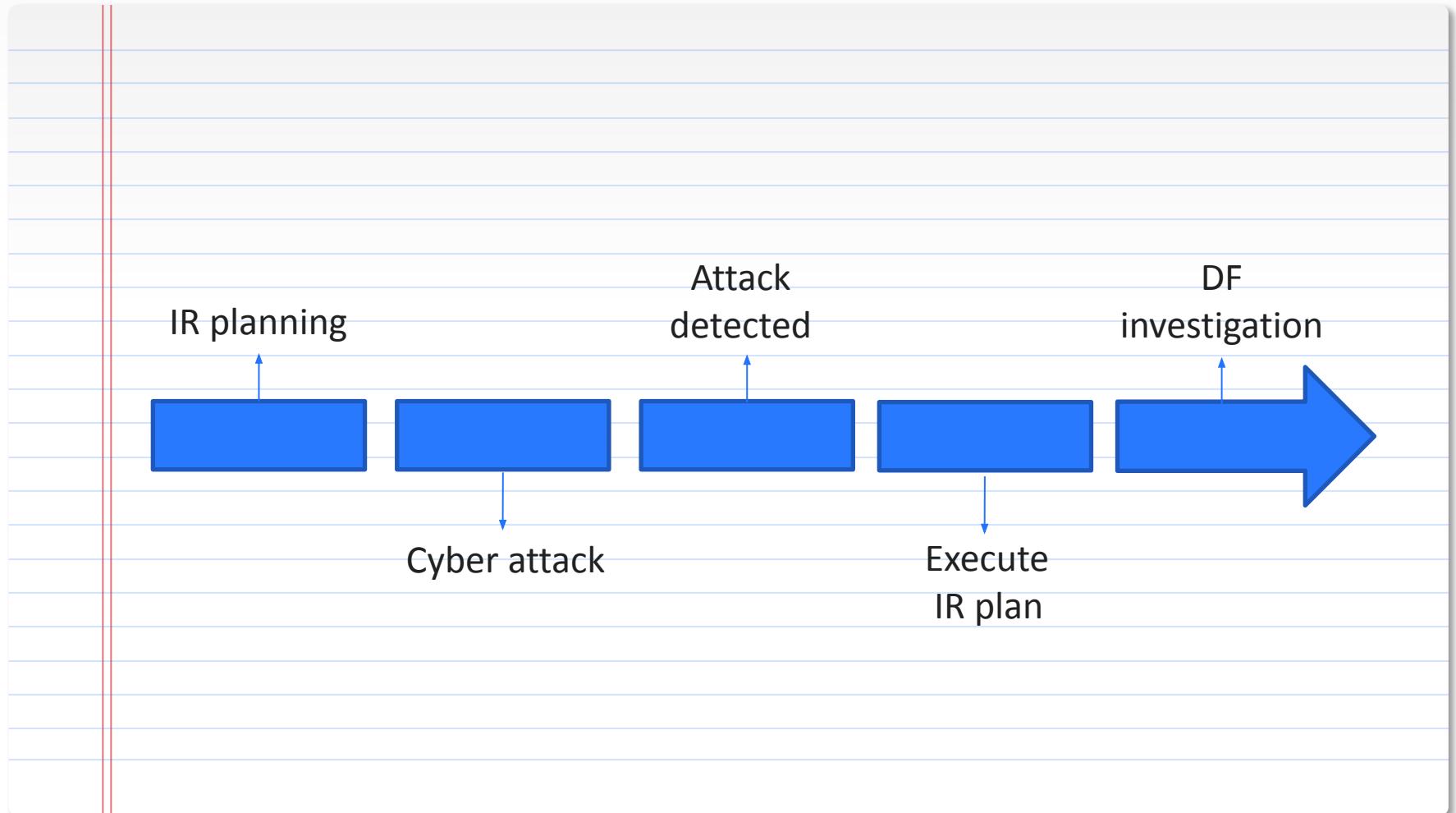
Introduction to DFIR

# 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.



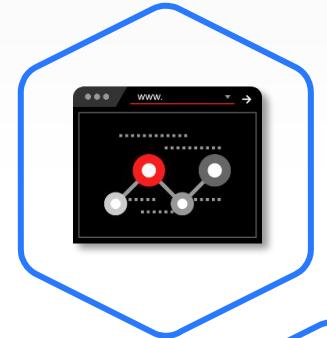


Introduction to DFIR

---

# Incident Response Planning

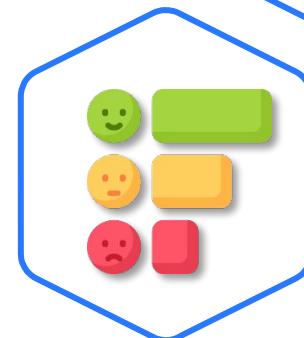
# Incident Responder Responsibilities



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



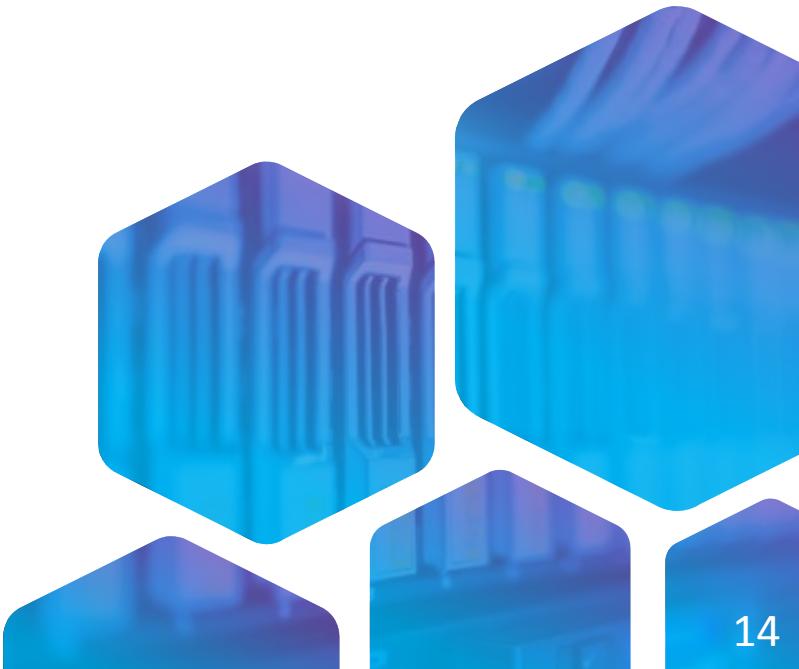
## Successful IR

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



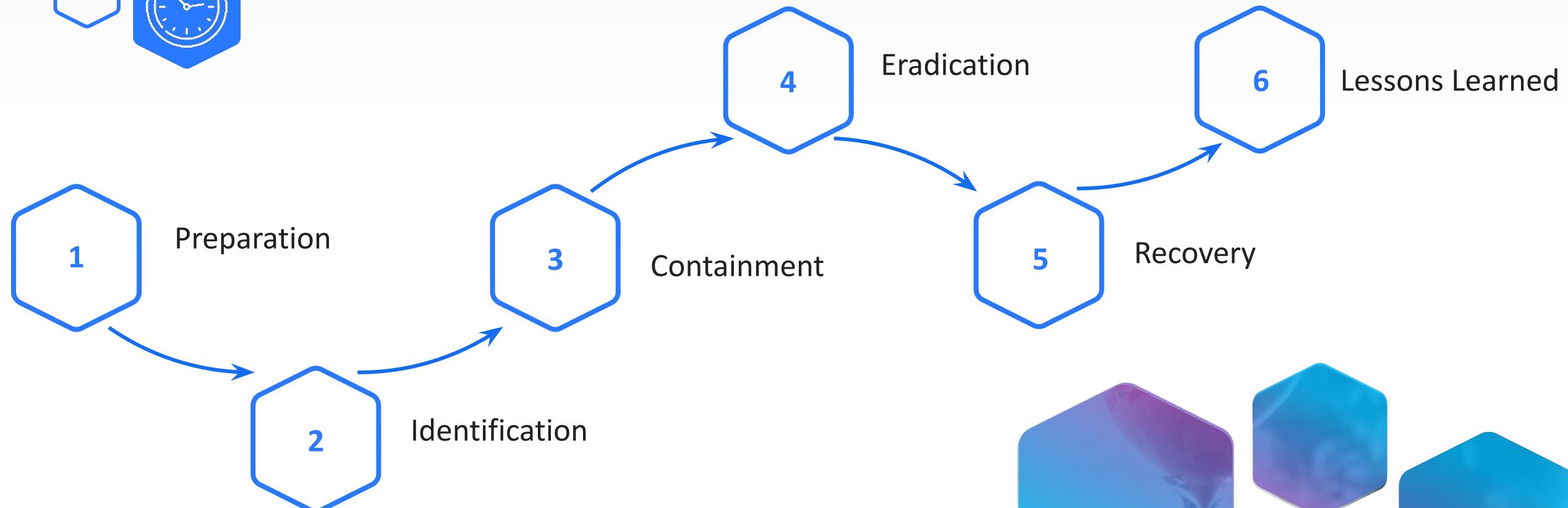
## Following the Steps

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



Incident Response Planning

# Six Stages





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.





DFIR Process

# Example of Evidence

Autoruns identifies possible startup locations.

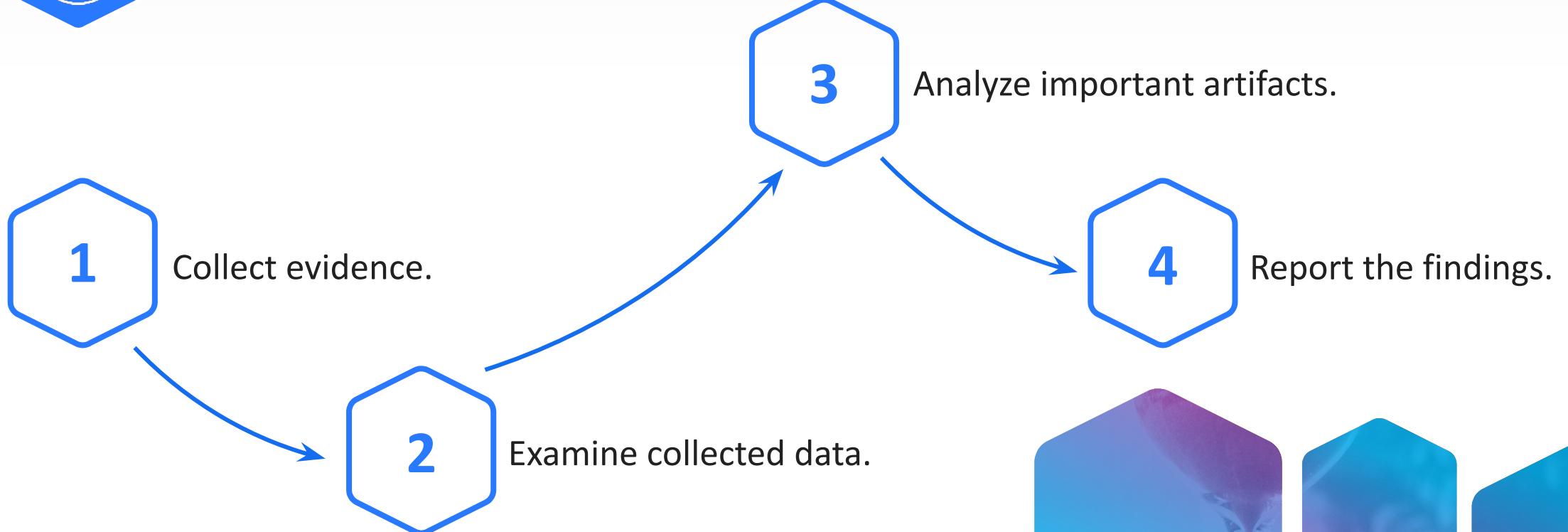
Startup programs can be evidence of persistent malware.

The programs reside in known folders and registry keys.

Autoruns - Sysinternals: www.sysinternals.com						
Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\10/2019 14:31						
Acrobat A...	AcroTray	(Verified) Adob...	c:\program files...	28/03/2017 14:50		
Adobe A...	Adobe Reader ...	(Verified) Adob...	c:\program files...	23/11/2016 9:28		
Adobe Cr...	Adobe Creative...	(Verified) Adob...	c:\program files...	13/09/2018 11:32		
Dropbox	Dropbox	(Verified) Drop...	c:\program files...	17/12/2019 21:28		
KeePass ...	KeePass	(Verified) Open...	c:\program files...	10/09/2019 11:24		
Kraken05...	Razer Kraken 7...	(Verified) Razer...	c:\program files...	08/09/2016 7:59		
QfinderPro	Qfinder Pro	(Verified) QNA...	c:\program files...	19/09/2019 10:29		
Razer Sy...	Razer Synapse	(Verified) Razer...	c:\program files...	28/09/2018 4:57		
SunJavaU...	Java Update Sc...	(Verified) Oracl...	c:\program files...	16/12/2018 7:51		
Truelmag...		(Verified) Acron...	c:\program files...	23/09/2019 9:29		
vmware-tr...	VMware Tray P...	(Verified) VMw...	c:\program files...	17/09/2019 4:03		
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				06/11/2019 17:20		
com.squir...		(Verified) Slack...	c:\users\lionk\la...	13/12/2016 21:53		
Docker D...				File not found: ...		
Fences	Fences Settings	(Verified) Stard...	c:\program files...	25/05/2018 7:37		
GoogleC...	Google Chrome	(Verified) Goog...	c:\program files...	06/12/2019 23:30		
GoogleDr...		(Verified) Goog...	c:\program files...	01/01/1970 2:00		
JetBrains ...	JetBrains Tool...	(Verified) JetBr...	c:\users\lionk\la...	21/10/2019 17:00		
kpm.exe	Kaspersky Pas...	(Verified) Kasp...	c:\program files...	02/12/2019 14:25		
NordVPN	NordVPN	(Verified) TEFI...	c:\program files...	01/10/2019 15:28		
OneDrive	Microsoft OneD...	(Verified) Micro...	c:\users\lionk\la...	08/11/2019 0:48		
OPENVP...		(Verified) Open...	c:\program files...	01/01/1970 2:00		
Outlook G...				File not found: ...		
uTorrent	μTorrent	(Verified) BitTo...	c:\users\lionk\la...	30/09/2019 21:14		
WindowG...	WindowGrid	(Not Verified) w...	c:\program files...	17/05/2016 13:19		
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup				18/07/2019 8:51		
AnyDesk.l...		(Verified) phil...	c:\program files...	18/11/2019 20:16		

Signed Windows Entries Hidden.

# DFIR Process



# DF Analysis Types



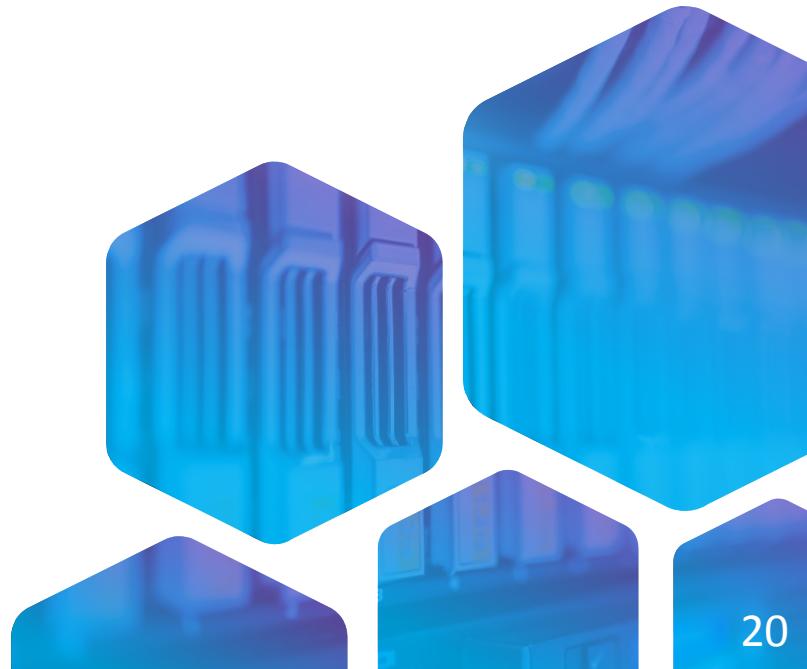
## Dead Analysis

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



## Live Analysis

- Analyzing powered-on computers

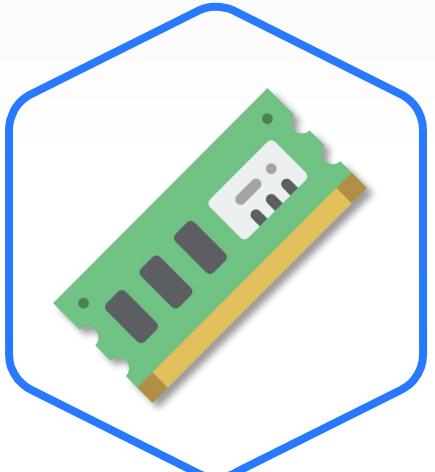




# Targeted Artifacts



Files on a Drive



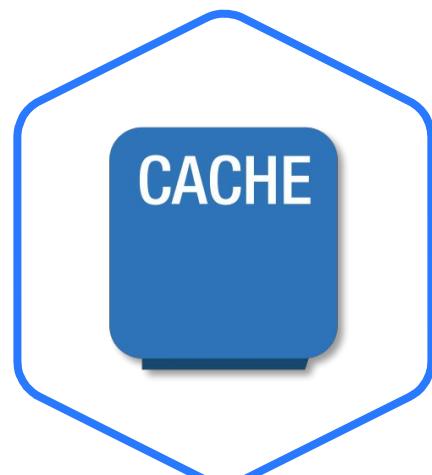
Memory  
Artifacts



Processes



Log Files



Cached Data

# DF Domains



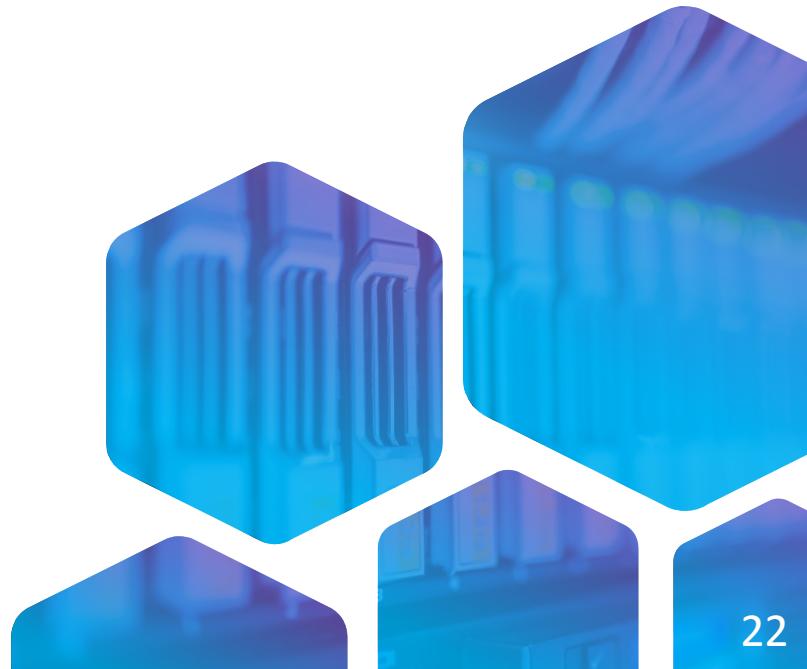
## Network Forensics

Focuses on gathering data about traffic passing through network equipment



## Host Forensics

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



# 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.

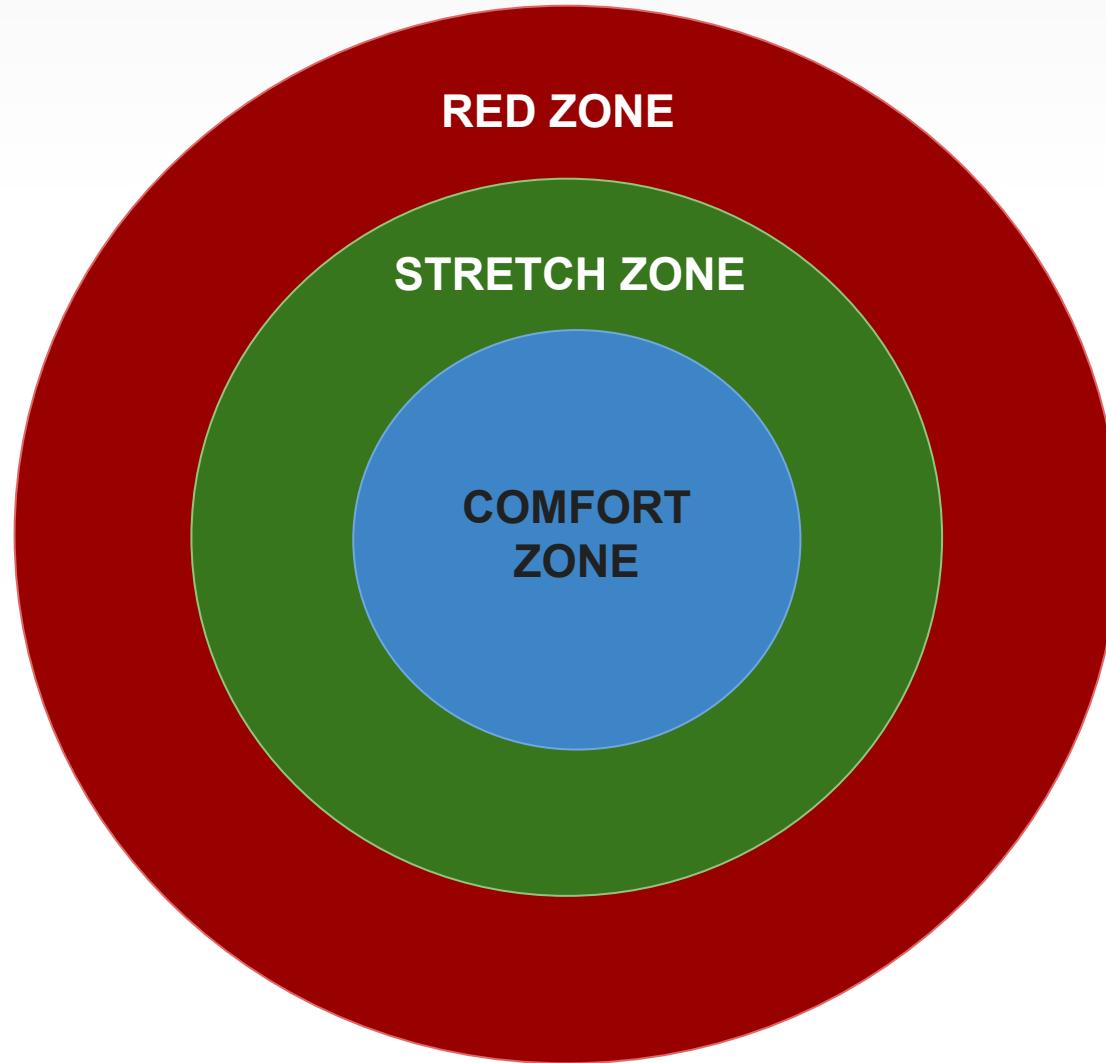
## Environment & Tools

- VirtualBox
- Windows 10
- Autoruns
- AnyDesk

## Related Files

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

# Pulse Check



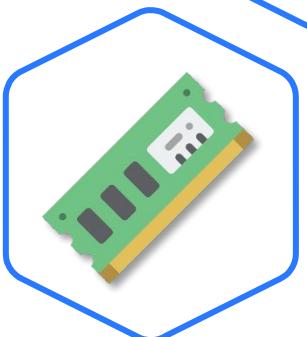


Introduction to DFIR

---

# DFIR Toolset

# Acquisition Tools



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

**DumplIt: 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



## Rekall

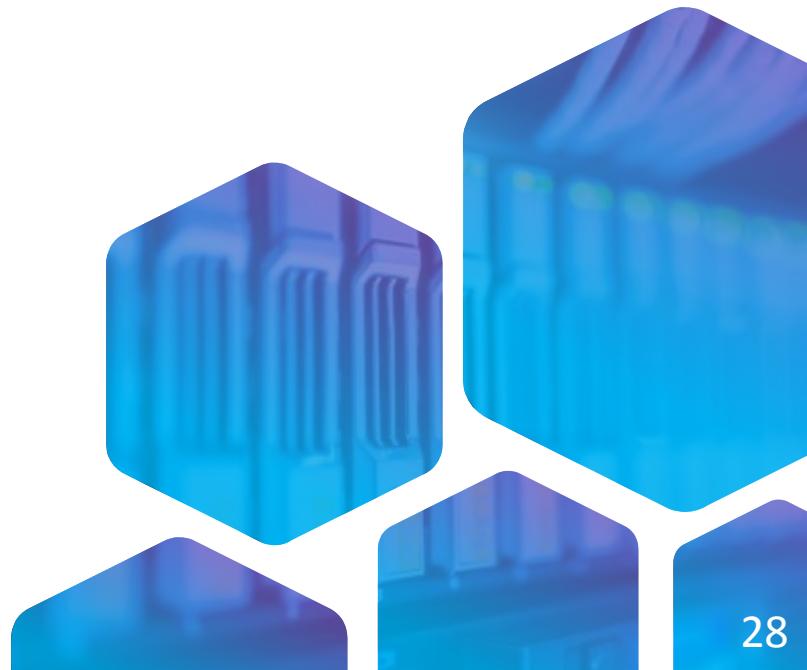
Open-source framework for advanced forensic and incident response

Not many tools exist that can perform computer memory forensics.



## Volatility Framework

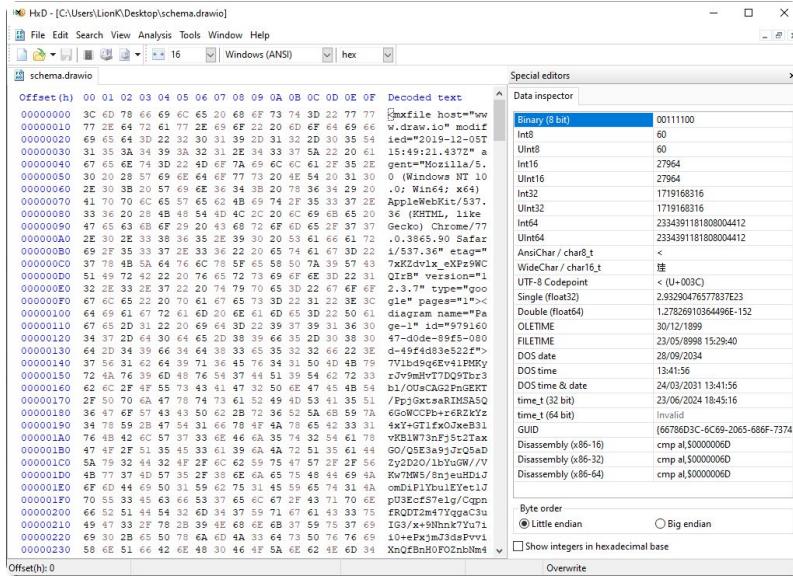
Open-source collection of Python tools supported by both Linux and Windows





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

The screenshot shows a web browser window with the URL <https://docs.microsoft.com/>. The page is titled "Windows Sysinternals". The left sidebar contains a navigation menu with links like Home, Learn, Downloads, File and Disk Utilities, Networking Utilities, Process Utilities, Security Utilities, System Information, Miscellaneous, Sysinternals Suite, Community, Software License Terms, and Licensing FAQ. The main content area features the Windows Sysinternals logo and a brief history of the site. It also includes a list of recommended actions and information about Sysinternals Live.

**Windows Sysinternals**  
12/11/2019 • 5 minutes to read • 1 contributor

The Sysinternals web site was created in 1996 by [Mark Russinovich](#) to host his advanced system utilities and technical information. Whether you're an IT Pro or a developer, you'll find Sysinternals utilities to help you manage, troubleshoot and diagnose your Windows systems and applications.

- Read the official guide to the Sysinternals tools, [Troubleshooting with the Windows Sysinternals Tools](#)
- Read the [Sysinternals Blog](#) for a detailed change feed of tool updates
- Watch Mark's top-rated [Case-of-the-Unexplained](#) troubleshooting presentations and other webcasts
- Read [Mark's Blog](#) which highlight use of the tools to solve real problems
- Check out the Sysinternals [Learning Resources](#) page
- Post your questions in the [Sysinternals Forum](#)

**Sysinternals Live**

Sysinternals Live is a service that enables you to execute Sysinternals tools directly from the Web without hunting for and manually downloading them. Simply enter a tool's Sysinternals Live path into Windows Explorer or a command prompt as `live.sysinternals.com/<toolname>` or `\live.sysinternals.com\tools\<toolname>`.

You can view the entire Sysinternals Live tools directory in a browser at <https://live.sysinternals.com/>.

[Download PDF](#)

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).



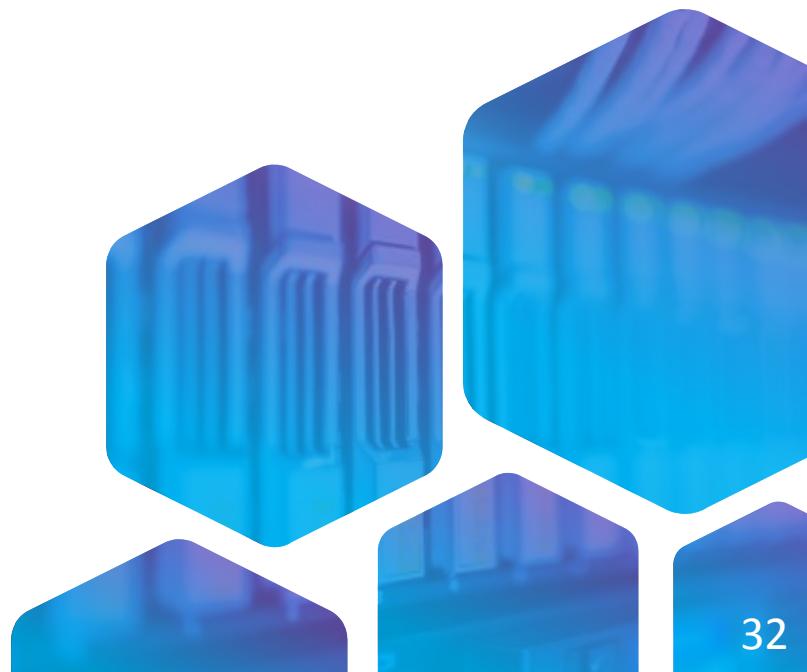
# Customized Tools



- 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



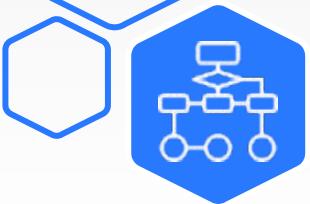


Introduction to DFIR

---

# DFIR Use Case

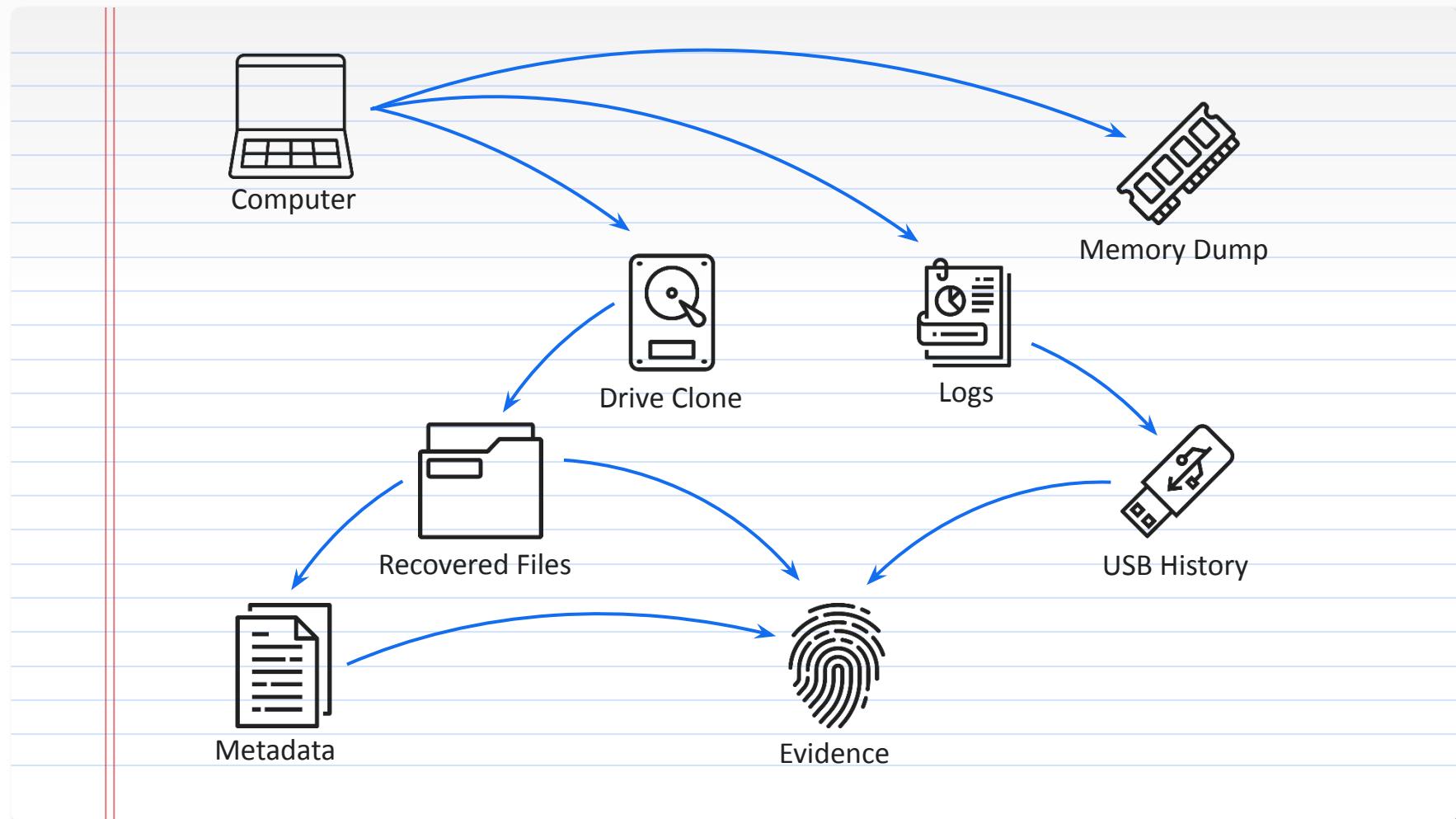
# DF Scenario: Data Leak



DF can be used to prove data leak events.

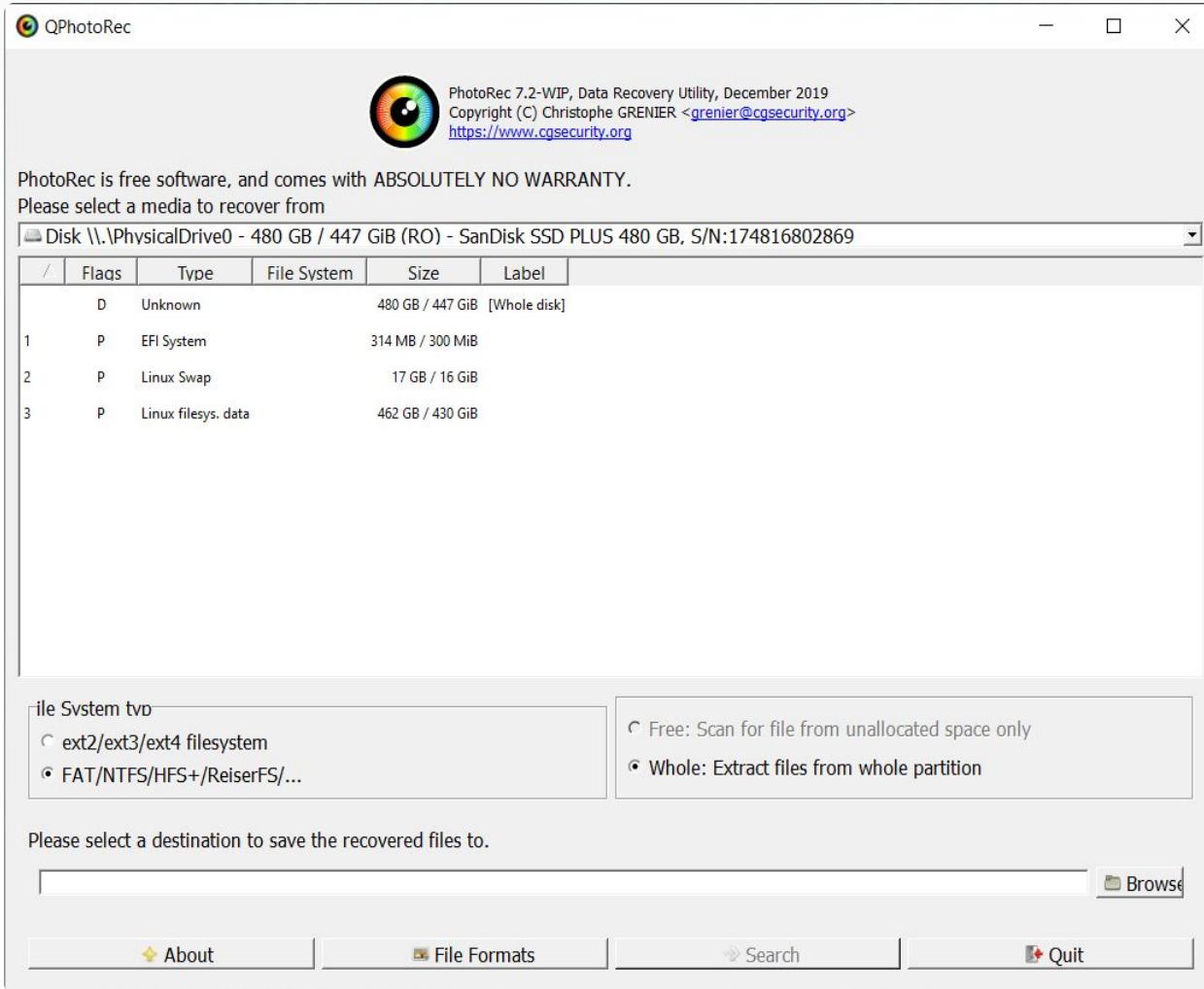
File carving can be used to identify if files existed on media devices even after deletion.

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.



# 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
```

# 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



# 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



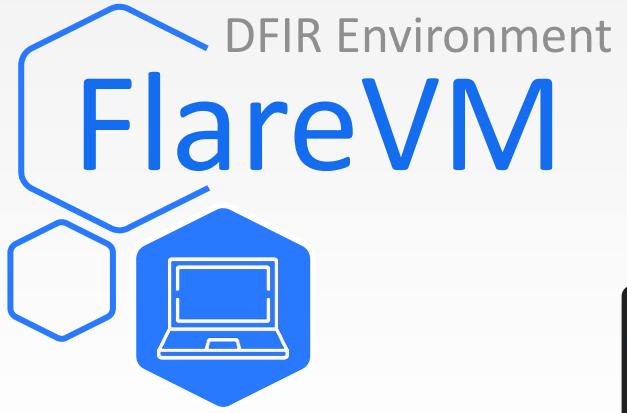
**REMnux**

Used mainly as a persistent forensics system for memory artifacts



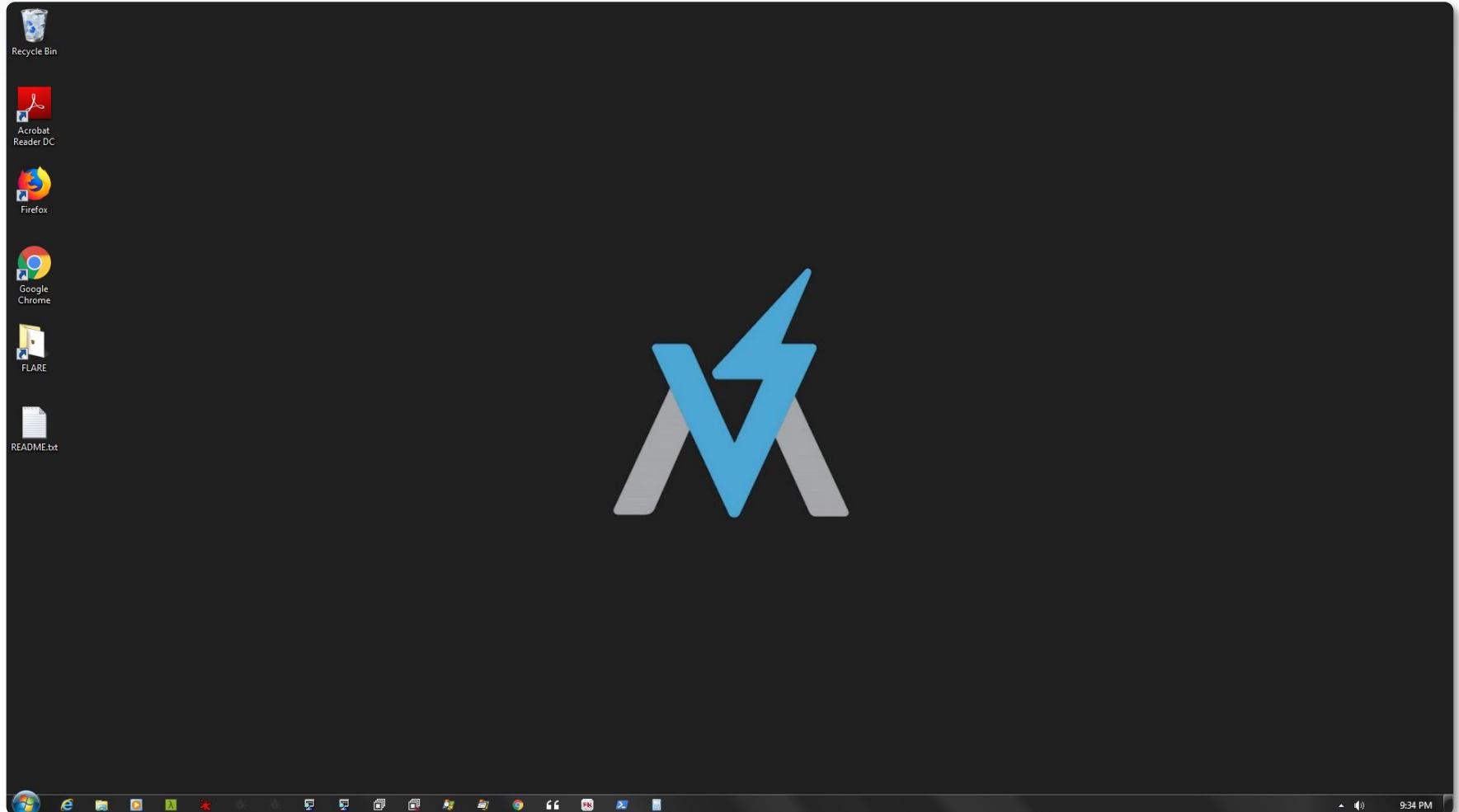
**FLARE VM**

Used mainly for malware analysis



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

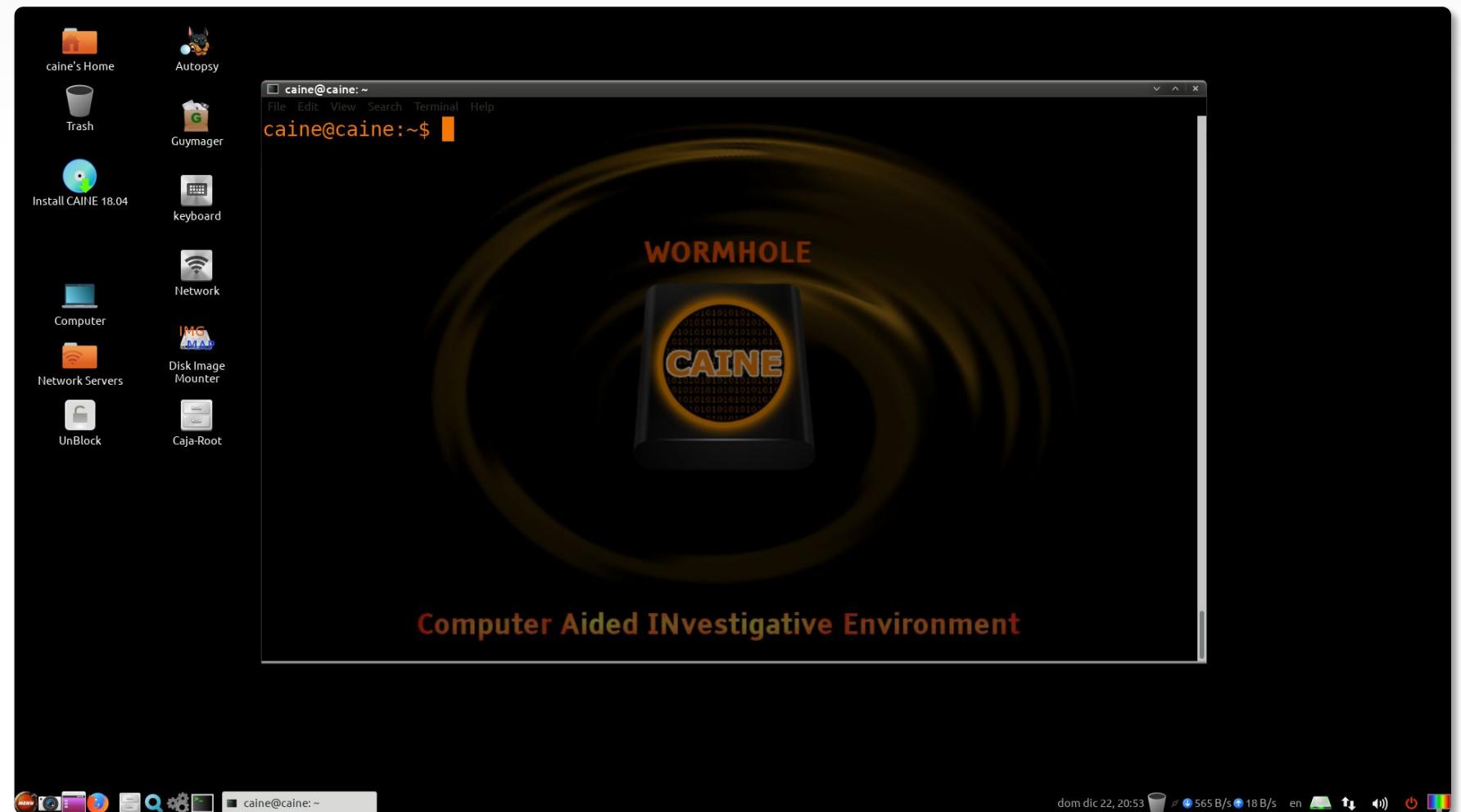




CAINE is a distribution that runs from a live USB.

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

The screenshot shows the NirSoft Launcher application window. The title bar reads "NirLauncher - NirSoft Utilities". The menu bar includes File, Edit, View, Options, Launcher, Packages, and Help. The main area is a grid of tool icons and names. The columns are categorized at the top: Password Recovery Utilities, Network Monitoring Tools, Web Browser Tools, Video/Audio Related Utilities, Internet Related Utilities, Command-Line Utilities, Desktop Utilities, Outlook/Office Utilities, Programmer Tools, and Disk Utilities. The "All Utilities" tab is selected. A tooltip for "WirelessKeyDump" indicates it "dumps the list of all wireless keys stored by Wind...". The bottom of the window has buttons for Run, Advanced Run, Web Page, Help File, Web Search, Package, and Package. It also displays "24 Utilities, 1 Selected" and the website "NirSoft Freeware, http://www.nirsoft.net".

NirLauncher - NirSoft Utilities				
Password Recovery Utilities		Network Monitoring Tools	Web Browser Tools	Video/Audio Related Utilities
Command-Line Utilities		Desktop Utilities	Outlook/Office Utilities	Internet Related Utilities
System Utilities	Other Utilities	All Utilities	Programmer Tools	Disk Utilities
Name	Description	Version	Updated On	Web Page URL
WirelessKeyDump	dumps the list of all wireless keys stored by Wind...	2.10	22/12/2019 20:33:00	<a href="https://www.nirsoft.net/utils/wirelesskeydump">https://www.nirsoft.net/utils/wirelesskeydump</a>
Wireless Key View	recovers lost wireless network keys (WEP/WPA) st...	2.10	22/12/2019 20:33:00	<a href="https://www.nirsoft.net/utils/wirelesskeyview">https://www.nirsoft.net/utils/wirelesskeyview</a>
WebBrowserPassView	Recover lost passwords from your Web browser.	1.92	22/12/2019 20:33:00	<a href="https://www.nirsoft.net/utils/web_browserpassview">https://www.nirsoft.net/utils/web_browserpassview</a>
VNCPassView	Recover the passwords stored by the VNC tool.	1.05	22/12/2019 20:32:59	<a href="https://www.nirsoft.net/utils/vnc_passview">https://www.nirsoft.net/utils/vnc_passview</a>
VaultPasswordView	Decrypts passwords stored in Windows Vault	1.08	22/12/2019 20:32:59	<a href="https://www.nirsoft.net/utils/vault_passwordview">https://www.nirsoft.net/utils/vault_passwordview</a>
RunWithoutElevation	RunWithoutElevation	1.00	22/12/2019 20:32:56	<a href="https://www.nirsoft.net/utils/runwithoutelevation">https://www.nirsoft.net/utils/runwithoutelevation</a>
Remote Desktop PassView	Reveals the password stored by Microsoft Remote...	1.02	22/12/2019 20:32:56	<a href="https://www.nirsoft.net/utils/remote_desktop_passview">https://www.nirsoft.net/utils/remote_desktop_passview</a>
PstPassword	Recover lost password of Outlook PST file.	1.20	22/12/2019 20:32:56	<a href="https://www.nirsoft.net/utils/pst_password">https://www.nirsoft.net/utils/pst_password</a>
PCAnywhere PassView	Reveals the passwords of pcANYWHERE items.	1.12	22/12/2019 20:32:55	<a href="https://www.nirsoft.net/utils/pcanywhere_passview">https://www.nirsoft.net/utils/pcanywhere_passview</a>
PasswordFox	View passwords stored in Firefox Web browser.	1.60	22/12/2019 20:32:55	<a href="https://www.nirsoft.net/utils/passwordfox">https://www.nirsoft.net/utils/passwordfox</a>
OperaPassView	Password recovery tool for Opera Web browser.	1.10	22/12/2019 20:32:55	<a href="https://www.nirsoft.net/utils/operapassview">https://www.nirsoft.net/utils/operapassview</a>
Network Password Recovery	Recover network passwords on Windows XP/2003...	1.50	22/12/2019 20:32:55	<a href="https://www.nirsoft.net/utils/network_password_recovery">https://www.nirsoft.net/utils/network_password_recovery</a>
MessenPass	Recover the passwords of instant messenger pro...	1.43	22/12/2019 20:32:54	<a href="https://www.nirsoft.net/utils/messenpass">https://www.nirsoft.net/utils/messenpass</a>
Mail PassView	Recover email passwords	1.90	22/12/2019 20:32:54	<a href="https://www.nirsoft.net/utils/mailpassview">https://www.nirsoft.net/utils/mailpassview</a>
LSASecretsDump	Dump the LSA secrets from the Registry.	1.21	22/12/2019 20:32:54	<a href="https://www.nirsoft.net/utils/lsasecretsdump">https://www.nirsoft.net/utils/lsasecretsdump</a>
LSASecretsView	displays the list of all LSA secrets stored in the Re...	1.25	22/12/2019 20:32:54	<a href="https://www.nirsoft.net/utils/lsasecretsview">https://www.nirsoft.net/utils/lsasecretsview</a>
IE Pass View	Recover passwords stored by Internet Explorer (Ve...	1.41	22/12/2019 20:32:54	<a href="https://www.nirsoft.net/utils/ie_pass_view">https://www.nirsoft.net/utils/ie_pass_view</a>
HTTPNetworkSniffer	Captures and displays HTTP requests/responses.	1.63	22/12/2019 20:32:53	<a href="https://www.nirsoft.net/utils/httpnetworksniffer">https://www.nirsoft.net/utils/httpnetworksniffer</a>
EncryptedRegView	Scans the Registry and decrypts the data encrypt...	1.03	22/12/2019 20:32:51	<a href="https://www.nirsoft.net/utils/encryptedregview">https://www.nirsoft.net/utils/encryptedregview</a>
Dialupass	Recover Dial-Up passwords in all versions of Win...	3.61	22/12/2019 20:32:50	<a href="https://www.nirsoft.net/utils/dialupass">https://www.nirsoft.net/utils/dialupass</a>
DataProtectionDecryptor	Decrypt DPAPI-encrypted data of Windows.	1.10	22/12/2019 20:32:50	<a href="https://www.nirsoft.net/utils/dataprotectiondecryptor">https://www.nirsoft.net/utils/dataprotectiondecryptor</a>
CredentialsFileView	Decrypts Credentials files of Windows.	1.07	22/12/2019 20:32:50	<a href="https://www.nirsoft.net/utils/credentialsfileview">https://www.nirsoft.net/utils/credentialsfileview</a>
ChromePass	Password recovery tool for Google Chrome Web ...	1.46	22/12/2019 20:32:50	<a href="https://www.nirsoft.net/utils/chromepass">https://www.nirsoft.net/utils/chromepass</a>
BulletsPassView	Reveals the passwords stored behind the bullets.	1.32	22/12/2019 20:32:50	<a href="https://www.nirsoft.net/utils/bulletspassview">https://www.nirsoft.net/utils/bulletspassview</a>

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

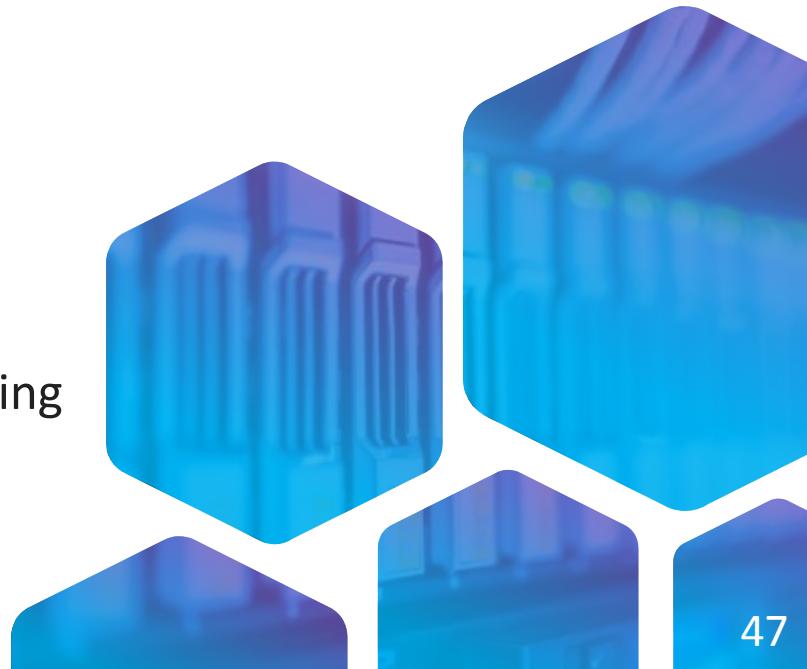


- In phishing, SE refers to investigating the message and attached links.
- In real-world social engineering, the IR team can set up decoys.



- 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.



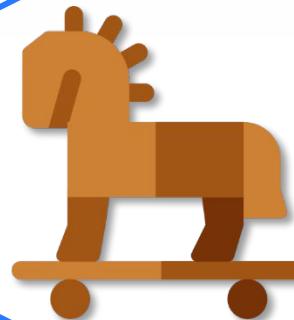
**Intrusion Detection**  
Detect the intrusion point.



**Identifying Persistence**  
Detect if any backdoors remain.



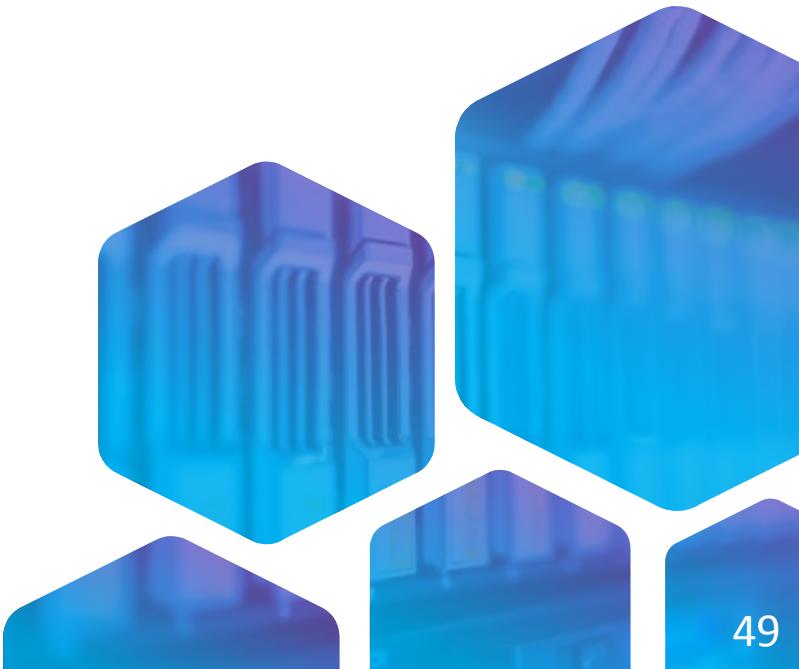
# DFIR for Trojan Delivery



- 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



# 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

# 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?**