SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

DFIR FUNDAMENTALS

Put your investigative skills to good use.

Learn how to get started in Digital Forensics and Incident Response (DFIR) to become a cyber forensics super sleuth and begin your path to an intriguing career.

digital-forensics.sans.org

Poster was created by Kathryn Hedley.

DFIR_START_0324

The first step in any investigation is to identify and gather evidence. Digital forensic investigations are no different. The evidence used in this type of investigation is data, and this data can live in many different locations in a variety of formats. You must be able to first identify the data that you might need to analyze, determine where that data resides, and formulate a plan and procedures for the best way to collect and preserve that data. Then the investigation can really begin!

DEFINITIONS

DIGITAL EVIDENCE

Digital evidence is simply information that is stored or transmitted in a digital format that may be of value to an investigation.

DATA VS METADATA

Data is "information in digital form that can be transmitted or processed."[1]

Metadata is "data that provides information about other data."[1]

Types of Metadata:

- Filesystem Metadata (Filesystem Dependent)
  - For example: filename, file size, file creation date and/or time, file content modification date and/or time
- File Metadata (File Type Dependent)
  - For example: last printed date and time, author, last saved by person, GPS location, make and/or model of device or software used to create or modify the file
  - ExifTool is a tool to view file metadata: **https://exiftool.org**

Beware: A file's extension does not necessarily denote the file's type. This is determined by the file's signature, or Magic Header. A good, comprehensive list of many known file format signatures is provided on Gary Kessler's website: www.garykessler.net/library/file_sigs.html

DIGITAL INVESTIGATION[2]

"A process to answer questions about digital states and events."
—Brian Carrier

DIGITAL FORENSICS

Digital forensics is the underlying methodology that gives examiners the ability to answer the who, what, why, when, where, how, and who questions.

INCIDENT RESPONSE

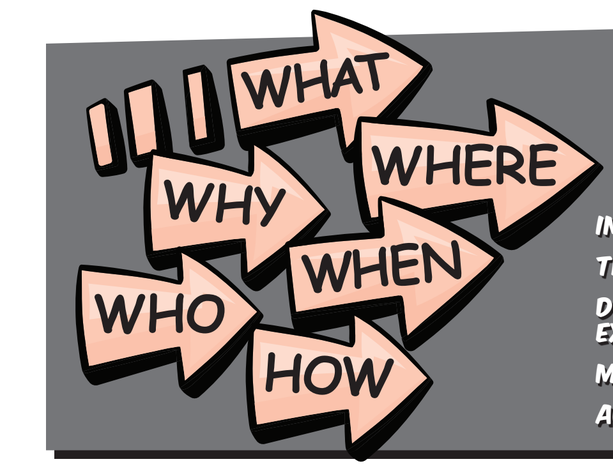
The planned and managed effort by an organization to respond to a computer security incident.

Detecting an incident relies on being able to monitor events and determine the difference between an event and an incident.

- An **event** is something that happened, whether planned or unplanned.
- An **incident** is an event that was unauthorized, against corporate security policy, or otherwise caused disruption.

This is achieved by using Indicators of Compromise (IoCs) and by knowing what is normal for that network/system, to be able to detect what is abnormal.

[1] www.merriam-webster.com/dictionary
[2] https://digital-evidence.org/di_basics.html

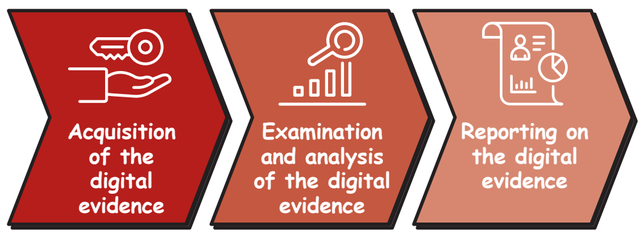


TYPES OF INVESTIGATION

- INCIDENT RESPONSE
- THREAT HUNTING
- DOCUMENT AND MEDIA EXPLOITATION (DOMEX)
- MILITARY ACTION
- AUDITING
- REGULATORY
- ADMINISTRATIVE (HR/INTERNAL)
- CIVIL AND CRIMINAL LITIGATION

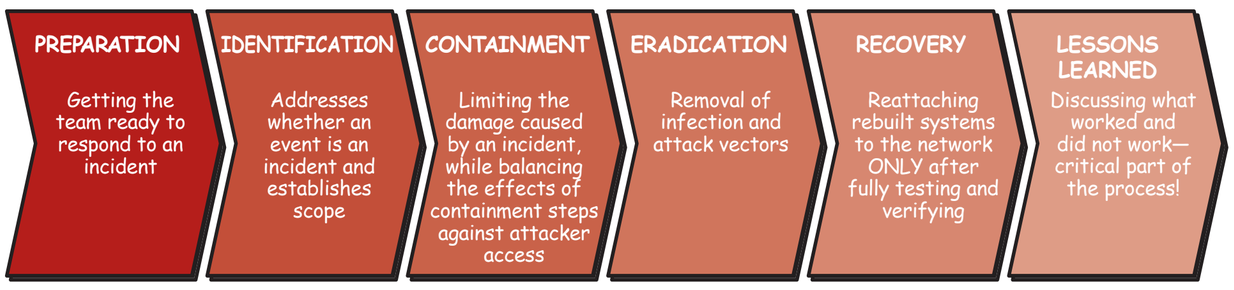
DIGITAL FORENSIC PROCESS

CORE PHASES OF THE DIGITAL FORENSIC PROCESS



Many standards exist to standardize digital forensic process models. One of these, applicable internationally, is the ISO/IEC 27043 Incident Investigation Principles and Processes Standard written by the International Standards Organization (ISO) (www.iso.org/standard/44407.html).

PHASES OF INCIDENT RESPONSE



ROLES IN DFIR

SOC ANALYST

- Responsible for monitoring events and detecting incidents
- Key skills:
  - Network architecture
  - Data sources and system logging
  - Network and endpoint security
  - Network defense
  - Network and endpoint monitoring

FORENSIC INVESTIGATOR

- Skilled and trained in forensic extraction of data
- Key skills:
  - Network and endpoint security
  - Data sources and access
  - Data acquisition
  - Evidence handling and preservation

FIRST RESPONDER

- Responsible for the preservation of evidence, acquisition, and analysis of data
- Critical in evidence identification, collection, and preservation
- Conduct triage investigation
- Key skills:
  - Network and endpoint security
  - Data sources and system logging
  - Data acquisition
  - Digital forensic analysis
  - Evidence handling and preservation

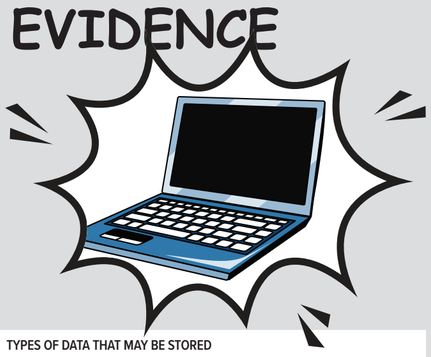
INCIDENT MANAGER

- Responsible for ensuring appropriate resources, tools and support are in place, and monitoring efficiency and mental health of team members—also acts as a buffer between the IR team and clients
- Knows the team's limits and calls in specialists when other skills are required
- Key skills:
  - Team leadership and people management
  - Planning and prioritization
  - Communication, negotiation, and conflict resolution
  - Problem-solving

FORENSIC ANALYST

- Skilled and trained in data analysis to identify data of interest and determine what happened
- Provide factual observations based on evidence
- Subject-matter experts
  Beware of the Expert label!
  in more advanced subjects such as:
  - Host-based digital forensic analysis
  - Memory analysis
  - Reverse engineering
  - Industrial Control Systems
  - Network analysis
  - Advanced acquisition techniques
  - Device repair

SOURCES OF DIGITAL EVIDENCE



DESKTOP COMPUTERS AND LAPTOPS

- Typically running one of four operating systems (OS): Windows, macOS, ChromeOS, or Linux
- Will contain artifacts specific to the OS and to installed applications
- Newer devices employ encryption by default

SERVERS

- Typically running one of two operating systems: Windows, or Linux
- In addition to standard host-based artifacts, different types of other data are stored on different types of server:

TYPE OF SERVER	PURPOSE	TYPES OF DATA THAT MAY BE STORED
Domain Controller	Authentication of user logins to domain	User information, events such as user logon/logoff
Web Server	Hosts webpages	Access logs, including IP addresses
Proxy Server	Intermediary between user systems and the Internet	Log of requests, configuration data
DHCP Server	Assigns IP addresses and network parameters	Log of assignments
Firewall	Monitors and controls incoming and outgoing network connections	Log of network connection attempts, configuration data
Network-Attached Storage	Stores files and folders	Files, log of file accesses
Terminal Server	Manages authentication to remote applications and systems	Log of remote connection attempts, user account and system information
Application Server	Hosts applications and services on a network	Log of application access
Mail Server	Stores and transmits emails	Audit logs, logs and content for emails sent and received by users

VIRTUAL MACHINES (VMs)

- Typically running one of two Operating Systems: Windows, or Linux
- May be stored locally on a system or in the cloud
- Virtual representation of an entire system, so will contain the same types of artifacts as a physical system of that type, relating to both the OS and applications
- Window 11 VMs mandate encryption

TABLETS AND MOBILE DEVICES

- Typically running one of two Operating Systems: Android, or iOS
- Android is based on Linux, iOS is very similar to macOS
- Will contain artifacts specific to the OS and to installed applications
- Newer devices employ encryption by default

REMOVABLE STORAGE MEDIA (USBS)

- Can contain a bootable OS and installed applications, and/or contain files and folders
- Can be read-only or read/write
- May be encrypted, at either hardware or software level
- May not immediately look like a USB device

RAM

- When a system is running, a significant amount of data is stored in memory (RAM).
- Some of this data may never be saved to the disk and so it is lost when the system is powered off. This is known as volatile data.
- It may include, among other data:
  - Running processes
  - Open network connections
  - Live registry data
  - Data copied to the clipboard
  - Commands executed via the command line
  - Encryption keys/passwords

NETWORK DEVICES AND DATA

- Data is sent between devices on a network within packets
- Packets can be captured and analyzed as part of an investigation
- May include data that is not present on the originating or receiving systems

THE CLOUD

- Backup and storage services for devices
- Online services such as social media, or webmail

INTERNET OF THINGS (IoT) DEVICES

- Some devices pair with a mobile or desktop application
- Many upload data to cloud services
- May store data on the device itself, typically whilst waiting to be synced with a paired application or uploaded to a cloud service
- Direct acquisition typically requires very advanced acquisition methods, if it is possible at all

INDUSTRIAL CONTROL SYSTEMS (ICS)

- Devices and systems used to control industrial processes
- Most common type of ICS: Supervisory Control and Data Acquisition (SCADA) systems
  - Used to centrally control geographically distributed devices
  - Typically used in water treatment plants and electrical distribution centers, for example

DRONES OR UNMANNED AERIAL DEVICES

- Features vary but may include cameras to create photos and video content, GPS location tracking, night vision, and/or remote control, as well as automated flying and route mapping.
- Some devices synchronize data with other devices and/or cloud services.
- Some devices store logs and feature-generated content on the device itself.
- Many drones contain an SD card slot, on which data may be stored.

VEHICLES

- Newer vehicles contain a vast number of different computer systems.
- A large volume of data is constantly collected while the vehicle is turned on, irrespective of whether it is moving.
- It can be paired to smartphones and Bluetooth devices, so may contain copies of data from these devices.

OTHER DEVICES

- CCTV systems may provide video evidence of a person's location or provide a visual on a suspect in a particular case that can assist with identification.
- Navigation systems, such as those that work with GPS or Galileo satellite systems
  - Not only present in vehicles; they are sold separately as well
  - These systems may include relevant location data
- Routers may store network information that is relevant to a case.
- Call data records can be requested from a service provider and can be used to triangulate a device's location, and any calls made or received by a particular phone number.
- Other storage media may contain data that is relevant to a case, even if it seems very outdated.

HOW DATA IS STORED

DATA STRUCTURE

APPLICATIONS—Software packages unrelated to the operation of the system itself, that are designed to do specific tasks for the end user or another application

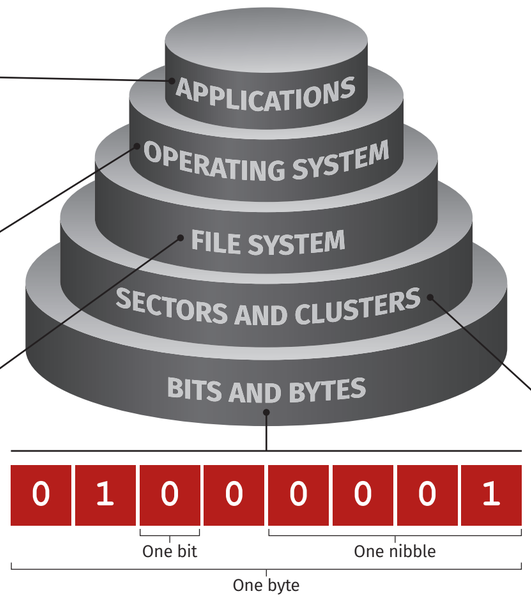
Examples are: word processors, graphics software, or web browsers

OPERATING SYSTEM (OS)—Software that manages the system's resources and provides services required to use the system such as memory management and handling input and output

Examples are: Windows, macOS, Linux, Android, and iOS

FILE SYSTEM—Data structure used by the OS that determines how data is stored and managed, in a similar way to a filing cabinet. The cabinet can contain folders, files, folders within folders, and files within folders, and can also come in many different shapes and sizes with different features

Examples are: NTFS (most common file system on Windows systems), APFS (default on newer macOS systems), exFAT and FAT32 (common on USB devices)



SECTORS AND CLUSTERS—These are the "units" of space to which data can be assigned

- The size of a sector is set to a default value by the device manufacturer, which is typically either 512 or 4,096 bytes.
- A cluster is the smallest addressable space the OS can see.
- A cluster is made up of a multiple of sectors, with this size defined in the file system header and configurable when the file system is created. However, most systems will have this value set as the default, which is typically eight sectors.
- Each cluster is labeled by the OS as either allocated or unallocated:
  - **ALLOCATED**—Cluster is currently allocated to a file.
  - **UNALLOCATED**—Cluster is NOT currently allocated to a file.
- Slack space in a cluster:
  - **RAM SLACK**—Unused space between the end of the logical file and the end of that sector
  - **FILE SLACK**—Unused sectors within the last cluster the file occupies

NUMBER SYSTEMS

Binary = base2

Two possible values for a bit: 0, or 1

- 8 bits = 1 byte = 2 nibbles
- 4 bits = 1 nibble

Octal = base8

Eight possible values: 0, 1, 2, 3, 4, 5, 6, 7

Decimal = base10

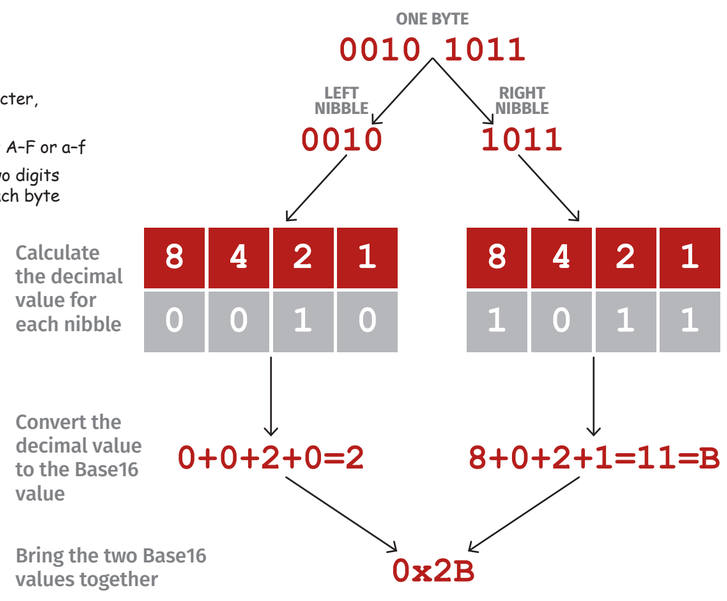
Ten possible values: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9

Hexadecimal = base16

Sixteen possible values for each nibble:
0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F

- As each value must be a single digit or character, we cannot use 10–15, so substitute a–f
- Case is irrelevant and this may be written as A–F or a–f
- One byte is therefore written as a set of two digits or characters, as there are two nibbles in each byte

CONVERTING BINARY TO HEXADECIMAL



DFIR FUNDAMENTALS

DFIR TOOLS

HARDWARE

Forensic Workstation(s) (Server/desktop/laptop)

- High-end system with a fast processor, lots of RAM and a lot of storage
- Laptop required for field work
- A number of companies do workstations specifically designed for forensic analysts

Digital Intelligence workstations:
https://digitalintelligence.com/products/fred

Sumuari forensic workstations:
https://sumuri.com/hardware/forensic-workstations

Continental forensic workstations:
www.continental.co.uk/workstations/forensic-workstations

Disk Duplicators

- Standalone imaging device with built-in write blocker & screen
- Capability to:
  - Image or clone input drive and write to output drive
  - Wipe output drive (ready to receive new image)

IMPORTANT: Make sure you connect the drives the right way round, or you will overwrite your evidence!

Evidence = INPUT (write-blocked/read-only),
Blank drive = OUTPUT (read/write)

WiebeTech duplicators: https://wiebetech.com/products

Tableau duplicators:
www.opentext.com/products/tableau-forensic-duplicators

Sumuri imagers:
https://sumuri.com/product/superimager-plus-complete-portable-rugged-dual-open-os

Bespoke Mobile Device Acquisition Field Toolkits

- Mobile device acquisition requires bespoke toolkits
  - These can be software-based or you can use ruggedized field toolkits
- Typically come with a lot of cables, to allow acquisition of many different devices
- Updated very frequently; need to pay annual Software Maintenance Service (SMS) fees to access updates

Cellebrite UFED mobile acquisition toolkit:
https://cellebrite.com/en/ufed

MSAB Field mobile acquisition toolkit:
www.msab.com/products/platforms/#field

Oxygen Forensic toolkit:
www.teeltech.com/mobile-device-forensic-tools/oxygen-forensic-kit

Grab Bags

- To include as a minimum:
  - A notepad and pen, to record observations and processes followed
  - Blank chain of custody forms, to document physical evidence
  - Camera, fully charged with spare battery
  - Hard drives, external USB drives, and SD cards, with varying (large) capacities, brand-new or wiped
  - One or more laptops, with required acquisition and analysis software pre-installed, updated, and confirmed working
  - An external power supply unit, to provide additional power to the laptop(s), if possible
  - Power extension cables
  - Adapter cables to provide charge to target devices such as smartphones and laptops. This should include as a minimum: micro USB, USB-C, lightning, and a universal laptop charger
  - Various cables for mobile devices and tablets, and internal hard drives
  - Screwdriver set and anti-static equipment to open up devices and remove hard drives
  - Software license dongles
  - Bootable media, on CD/DVD or USB, which can be used to boot a target system to perform acquisition, if required
  - Write blocking equipment and drive adapters, for multiple connection types, including SATA, NVMe, PCIe, and USB as a minimum
  - Disk duplicator equipment, if possible, for faster device acquisition
  - Comfort items such as a personal phone charger, a book or playing cards, a drink and snacks!

Write Blockers

- Portable device to facilitate read-only access to physical evidence
- Need to be connected to workstation that runs acquisition software to acquire a device
- Required for each type of interface you need to acquire: USB, SATA, NVMe, PCIe
- Validate before use & periodically to check it is actually blocking writes!

WiebeTech write blockers: https://wiebetech.com/products

Tableau write blockers:
https://security.opentext.com/tableau/hardware?types=Forensic-Bridges

Network TAPs

- Physical inline device to monitor and/or collect network traffic
- Allows passive collection of data for analysis

- A network switch with a SPAN or mirror port can be used instead, although this is typically not as reliable as a network TAP

Network TAPs: www.garlandtechnology.com/network-tap

Dualcomm devices: www.dualcomm.com/collections/network-tap

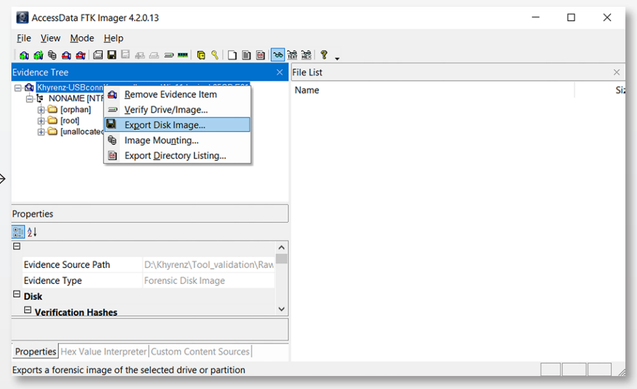
Datacom devices: www.fullcontrolnetworks.co.uk/products/network-taps-from-datacom

SOFTWARE

Acquisition Tools

- View and acquire endpoint devices
- View and acquire removable media
- View and acquire mobile devices and tablets
- Different devices often require different tools, so you need a selection in your toolset

Exterro FTK Imager:
www.exterro.com/ftk-imager



X-Ways Forensics:
www.x-ways.net/forensics

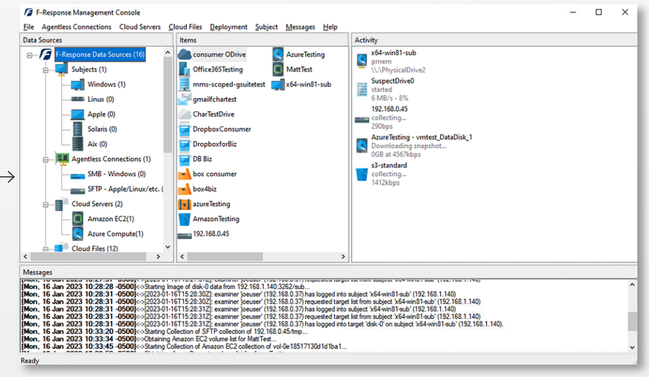
Cellebrite UFED:
https://cellebrite.com/en/ufed

Linux dd command manual:
https://linux.die.net/man/1/dd

Incident Response Tools

- Monitoring, searching, alerting, acquisition, and analysis of systems across a network
- Managed centrally through server software, with small agents running on each client endpoint

F-Response:
www.f-response.com



CrowdStrike Falcon:
www.crowdstrike.com/services/respond/incident-response

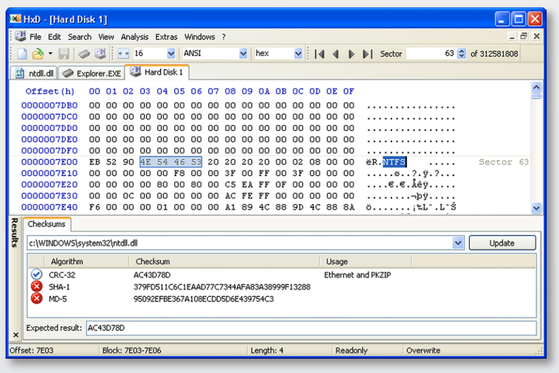
Google Rapid Response (GRR):
https://github.com/google/grr

Velocidex Velociraptor:
https://github.com/Velocidex/velociraptor

Hex Editors

- Create, read, and modify files at the hex level or on a raw device
- Some have advanced features that include templates, scripts, and data analysis tools

HxD:
https://mh-nexus.de/en/hxd



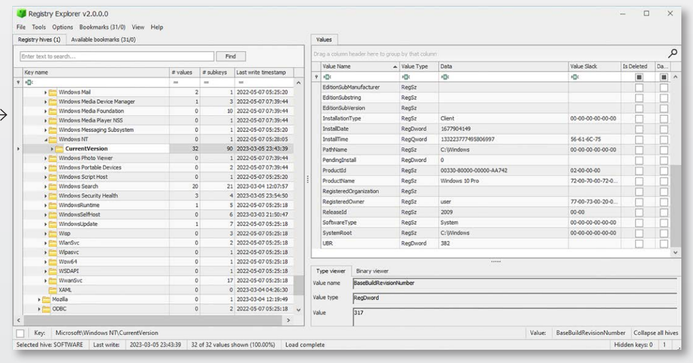
WinHex:
www.x-ways.net/winhex

010 Editor:
www.sweetscape.com/010editor

Task-Specific Individual Tools

- Artifact or function specific - intended to serve a specific purpose
- Typically open source or freemium tools

Free DFIR tools developed by SANS faculty:
www.sans.org/tools/?focus-area=digital-forensics



xLEAPP tools for artifact parsing on specific platforms:
https://github.com/abrignoni

Log2Timeline:
https://github.com/log2timeline/plaso

USB Detective:
https://usbdetective.com/

Arsenal Image Mounter:
https://arsenalrecon.com/products/arsenal-image-mounter

Forensic Analysis Suites

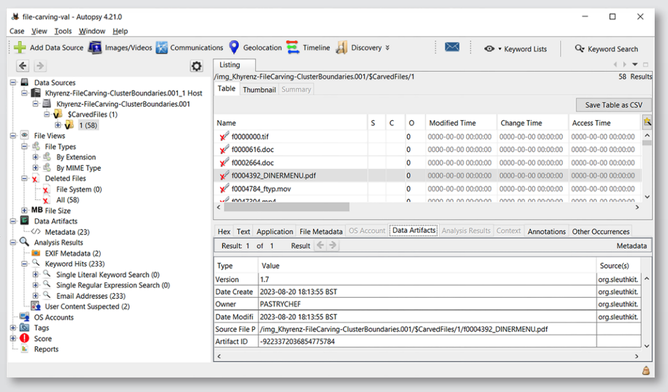
- Deep analysis of devices, forensic images, filesystems,and files/folders
- Advanced features such as:
  - Keyword searching
  - Data carving
  - Stream carving
  - Timeline analysis
  - Artifact parsing and categorization
  - Bookmarking/tagging
  - Automation and customizability
  - Report generation

X-Ways Forensics:
www.x-ways.net/forensics

Magnet AXIOM:
www.magnetforensics.com/products/magnet-axiom

Cellebrite Physical Analyzer:
https://cellebrite.com/en/physical-analyzer

Autopsy:
www.sleuthkit.org/autopsy



SANS SIFT Workstation:
www.sans.org/tools/sift-workstation

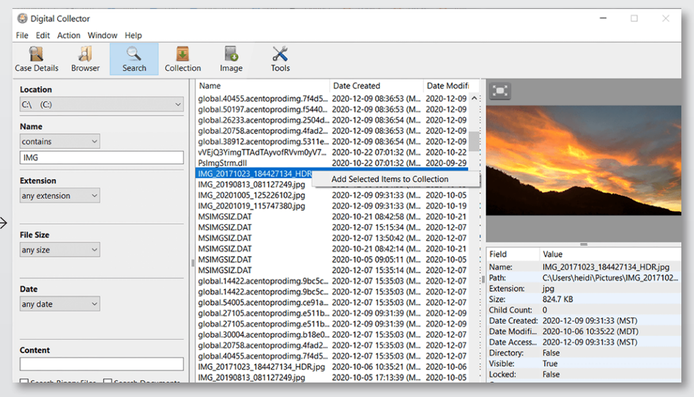
OpenText EnCase Forensic
www.opentext.com/products/encase-forensic

Exterro FTK Forensic Toolkit:
www.exterro.com/forensic-toolkit

Bootable Forensic Devices and ISOs

- Boot evidence device to an Operating System on a USB
- Contain a pre-installed selection of tools for acquisition, triage, and analysis
- Often write-block internal drives by default
- Can mount output drives read/write to acquire data onto
- May or may not support encrypted volumes or disks

Cellebrite Digital Collector:
https://cellebrite.com/en/digital-collector



Tsurugi Linux:
https://tsurugi-linux.org

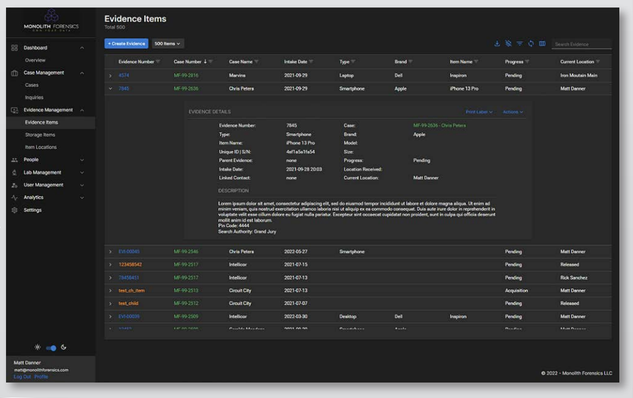
Windows Forensic Environment (WinFE):
www.winfe.net/download

Kali in Forensics Mode:
www.kali.org/docs/general-use/kali-linux-forensics-mode

Case Management and Documentation Tools

- Track the status of individual cases
- Perform statistical analysis and reporting on casework
- Track evidence and produce Chain of Custody
- Create, store, and preserve case notes
- Manage resources and people

Monolith Forensics:
www.monolithforensics.com



Lima Forensic Case Management:
www.intaforensics.com/lima

BlackRainbow NIMBUS:
https://blackrainbow.com/corporate/#case_management

KEY DFIR PRINCIPLES

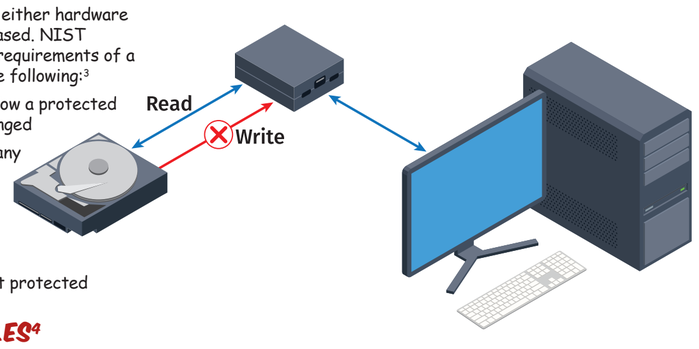
DELETING A FILE

- When a file is deleted (not put into the Recycle Bin/Trash), file system metadata for the file is marked as available for reuse and the clusters allocated to that file are marked as unallocated.
  - Over time, when the OS needs the space, it will overwrite this data.
- While neither the file system metadata nor the file's content has been overwritten, the file system metadata can be used to locate the file and recover it in its entirety, including the original name and timestamps.
- If the file system metadata for the file is overwritten but the file's content is not, the file can potentially be recovered, but its original name and location will not be known. The process of recovering such data is known as **file carving**.
- If the file's content is overwritten, but the file system metadata for the file is not, it will be possible to see that the file previously existed and potentially see its location, size and timestamps, but not possible to recover it. Note that other evidence relating to a previously existing file may also reside on the system.

WRITE BLOCKING

Write blockers can be either hardware devices or software-based. NIST describes the critical requirements of a write blocker to be the following:[3]

- The tool shall not allow a protected disk drive to be changed
- The tool shall allow any information to be obtained from or about any disk drive
- The tool shall allow any operations to a disk drive that is not protected



ACPO PRINCIPLES[4]

The ACPO principles have been widely adopted around the world as the foundational principles in the practice of digital forensics, both for law enforcement and other digital forensics practitioners.

PRINCIPLE	DESCRIPTION
Principle One	No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data that may subsequently be relied upon in court.
Principle Two	In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
Principle Three	An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
Principle Four	The person in charge of the investigation has overall responsibility for ensuring that the law and principles are adhered to.

HASHING

- One-way function commonly used to determine whether data has changed
- The same data will always give the same hash value
- A single change, in most cases, will alter the hash completely
- Two discrete files, in most cases, should have distinct hashes
- Two different inputs having the same hash is called a hash collision
  - Researchers have proved it is possible to create two different random files with the same hash value
  - It is probabilistically highly unlikely that two different data inputs on a user's system in the wild will have the same hash value
  - It is extremely difficult to create a file with a specific hash value to do a specific task
- Common hashing algorithms: MD5, SHA1, SHA256

LOCARD'S EXCHANGE PRINCIPLE

- Anyone or anything entering a crime scene takes something with them and leaves something behind.
- Same is true in everyday life.
  - For example: walking across a field of fresh snow will leave footprints behind and particles of snow on your shoes.
- Same is true of digital devices.
  - For example: reading a text file on a system will produce evidence showing that an application (such as Notepad) was run in order to open the file, and evidence of file access will be produced showing which file was opened, when, where it resides, and by which user account on the system.
- In a similar vein, non-action or anti-forensic action to erase data can also leave evidence in the form of the absence of data that may otherwise have been expected to exist.

ORDER OF VOLATILITY[5]

The order in which digital evidence should be collected to minimize the loss of data.

1. CPU registers and cache, if you have the capability
   - This is extremely difficult and would involve specialist hardware and knowledge; in all of our real-world experience, it is highly unlikely that this will be possible
2. Target system RAM
3. Router data
4. Temporary filesystems
5. Target system hard drive
6. Data stored remotely
7. Network topology and configuration
8. Offsite backup data

CHAIN OF CUSTODY

- Only one document in the required documentation set, but crucial to an investigation
- Tracks the movement of evidence through the entire digital forensic process
- Documents each person who handled the evidence, including relevant dates and times, and the purpose of any transfers between people or into or out of storage locations
- Examples of chain of custody forms can be found at www.dfir.training/downloads/forms-templates

THINK DFIRENTLY

[3] www.nist.gov/system/files/documents/2017/05/09/swbtt_a_validation3.pdf
[4] https://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf
[5] https://tools.ietf.org/html/rfc3227