



Prifysgol Cymru

Y Drindod Dewi Sant

University of Wales

Trinity Saint David

Trawsnewid Addysg, Trawsnewid Bywydau
Transforming Education, Transforming Lives

During our previous lecture, we discussed about digital evidences and roles, responsibilities of a Forensic Investigator, Incident Response, challenges and Legal Compliances.

Today, lets continue our discussion further to understand more about Investigation. We shall try to understand the forensics investigation process and the importance of it by looking into the pre-investigation phase, first response, investigation and post-investigation phase.



INVESTIGATION



*UNDERSTANDING
INVESTIGATION
PROCESS*



PHASES'



RESPONSES

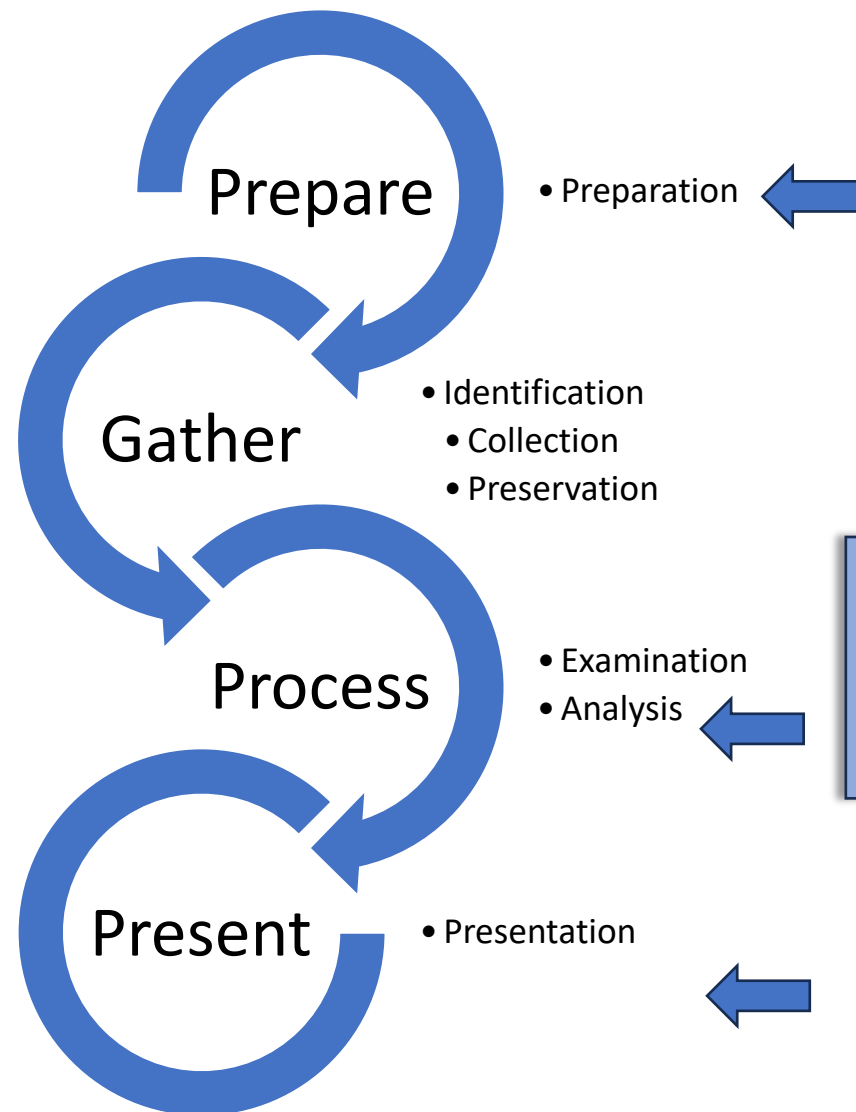
Today's Discussion

- Detection of an incident
- Approved techniques to retrieve relevant data
- Proper evidence gathering
- Chain of custody

RECAP

Last week review...

[This Photo](#) by Unknown Author is licensed under [CC BY-NC](#)



- Administrative, Technical & Physical Provisions
- Equipment and Personnel

- Evaluate Digital Evidence
- Examine the context and content to determine relevancy

- Document Preparation

Process

Process

- Preparation

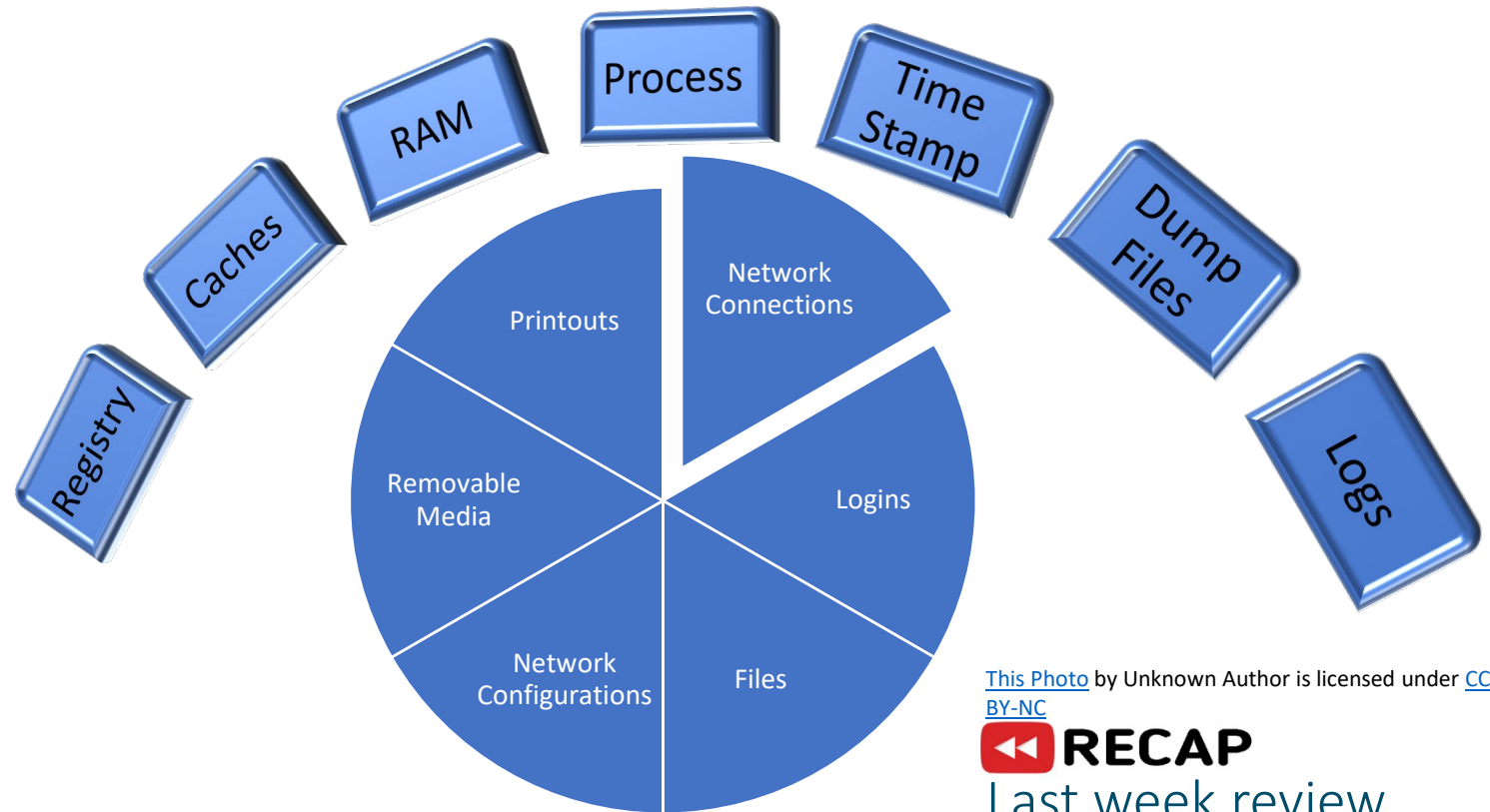
- Process and Procedure (Framework, SOP)
- Education, Training and Awareness
- Technology and Toolsets

- Gathering

- Electronically Stored Evidence
- Evidence Handling Techniques
- Securing the Scene
- Documenting the Scene
- Search and Seizure
- Collection and Preservation

Always remember

“maintaining the authenticity and integrity of evidence is essential for guaranteeing a forensically sound investigation”



[This Photo](#) by Unknown Author is licensed under [CC BY-NC](#)



RECAP

Last week review...

Process

Always remember

“maintaining the authenticity and integrity of evidence is essential for guaranteeing a forensically sound investigation”

■ Processing

- Always in a controlled environment
- Follow the least privilege access methodology
- Look for encrypted/ deleted files

■ Presentation

- Content should be clear and concise to accurately demonstrate a chronology of events
- Use of jargon, slang, and technical terminology should be limited or avoided.
- Where used, a glossary should be included to define terms in a layperson’s language.
- Where acronyms and abbreviations are used, they must be written out in full expression on the first use.
- Because final reports are written after the fact, meaning after an investigation, content should be communicated in the past tense, but can change tense where conclusions or recommendations are being made.
- Format a final report not only for distribution within the organization, but also with the mindset that it may be used as testimony in a court of law.



Summary

- **Computer forensics**

- Methodological procedures to identify, gather, preserve, interpret, and present evidence from computing equipment admissible in court.

- **Cybercrime**

- Illegal acts involving computing devices categorized into internal and external attacks.

- **Challenges**

- Speed, anonymity, volatile evidence, global origin, legal differences, limited understanding.

- **Investigation Approaches**

- Civil, criminal, administrative.

 **RECAP**
Last week review...

[This Photo](#) by Unknown Author is licensed under [CC BY-NC](#)

Summary

- **Digital Evidence**

- Stored or transmitted digital information, volatile and non-volatile.

- **Forensic Readiness**

- Organization's ability to use digital evidence efficiently and cost-effectively.

- **Incident Response**

- Integration of computer forensics in response plans for tracking and prosecuting perpetrators.

- **Legal Framework**

- Relevance of laws to forensic investigations in the US and other jurisdictions.

 **RECAP**
Last week review...

[This Photo](#) by Unknown Author is licensed under [CC BY-NC](#)

Investigation

- **Examination/Investigation Goals**
 - **Clear understanding** of examination goals.
 - **Technical expertise** and systematic approach.
- **Hypothesis Formulation/Criteria:**
 - Answering questions about **previous events**.
 - **Observations** aid in hypothesizing.
 - Consider **client's question** and establish hypotheses.
- **Experimental Design:**
 - **Prepare** to experiment and test hypotheses.
 - **Simulate** suspect machine environment.
 - Conduct **mock drills** to refine methods and tool selection.

Investigation

- **Tool Selection:**

- Choose tools based on **case specifics**.
- Consider digital forensic tools (software/hardware).
- **Evaluate** commercial vs. open-source options.
- Prefer tools designed for **specific purposes**.

- **Results Review and Evaluation:**

- Review results from **various perspectives**.
- Communicate findings to the client with **realistic expectations**.

- **Conclusion and Opinion Formulation:**

- Conclusion is a judgment **based on facts**.
- **Opinion is a belief** based on science or experience.
- Be prepared to **explain conclusions or opinions** in court testimony.

Investigation – To Remember!!!

- **Importance of Forensic Investigation Process:**

- Necessity due to increase in cybercrimes. Development of laws & standards defining cybercrimes and evidence handling.

- **Compliance and Standards:**

- Investigators must adhere to local laws and established standards.
- Deviation may jeopardize the investigation.

- **Preservation of Digital Evidence:**

- Digital evidence is fragile; integrity must be maintained.
- Strict guidelines and thorough investigation process are crucial.

- **Repeatability and Documentation:**

- Investigators must follow repeatable and well-documented steps.
- Consistency in findings is essential to avoid invalidation in court.

- **Adoption of Standard Processes:**

- Adoption of standard computer forensics processes is recommended.

Investigation – Setting up your Lab

- **Computer Forensics Lab (CFL):**

- + Designated location for computer-based investigations.
- + Houses instruments, software, hardware tools, and forensic workstations.

- **Planning and Budgeting Considerations:**

- + Types of Investigations:
 - ✓ Based on crime statistics and expected trends (criminal, civil, corporate).
- + Number of Investigators/Examiners:
 - ✓ Dependent on case complexity; hire trained professionals.
- + Equipment Requirement:
 - ✓ Forensic and non-forensic workstations, safe lockers for equipment storage.
- + Software Requirement:
 - ✓ Use licensed versions of required software; avoid demo versions for full functionality.

Investigation – Setting up your Lab

- **Physical and Structural Design Considerations:**

- + Lab Size: Determine size based on budget and case complexity.
- + Access to Essential Services: Ensure access to emergency services without compromising security.
- + Space Estimation: Allocate sufficient space for work areas and evidence storage.
- + Heating, Ventilation, and Air-Conditioning: Maintain suitable environmental conditions for lab equipment and personnel.

- **Work Area Considerations:**

- + Workstation Requirement: Determine workstation needs based on case types and complexity.
- + Ambience: Ensure a comfortable working environment for investigators.
- + Internet, Network, and Communication Line: Install dedicated networks for forensic computers; provide dial-up internet access.
- + Lighting Systems and Emergency Power: Install emergency power systems and optimize lighting for productivity and comfort.

Investigation – Setting up your Lab

- **Physical Security Considerations:**

- + Level of Security:
 - ✓ Tailor security measures to the nature of investigations.
- + Visitor Log and Access Control:
 - ✓ Maintain visitor logs and issue passes for identification; deploy intrusion alarm systems and surveillance cameras.
- + Fire Safety Measures:
 - ✓ Install fire extinguishers, train personnel on their use, and shield workstations from electromagnetic signals.

- **Human Resource Considerations:**

- + Importance of Experience and Training:
 - ✓ Success relies on experience gathering, knowledge sharing, ongoing education, and human resources development.
- + Staffing Requirements:
 - ✓ Estimate personnel needs based on case nature and required skills; recruit certified professionals for key roles.

Investigation – Setting up your Lab

- **Forensic Lab Licensing:**

- + Importance of Licensing: Labs should be licensed by relevant authorities to demonstrate trustworthiness.
- + Accreditation Standards: Obtain accreditations such as ASCLD/LAB and ISO/IEC 17025 to ensure quality assurance and compliance with international standards.

Discussion Point: “Overall, accreditation bodies for digital forensics play a critical role in upholding standards, ensuring quality, and enhancing the reliability of forensic investigations”. In addition to this, accreditation provides assurance of competence, credibility, and adherence to legal requirements, ultimately contributing to the effectiveness and integrity of the criminal justice system.



Break and Discuss

[This Photo](#) by Unknown Author is licensed under [CC BY](#)

Investigation

- Incident Response
 - Identify the Crime Scene
 - Protect the Crime Scene
 - Preserve Evidences (Temporary/ Fragile etc)
- Gathering Evidence
 - Questioning
 - Consent & Signatures
 - Formal Interviews
- Analysis
- Documentation

Search Warrant

Health & Safety

Planning

Visual

Exhibit ID's

Photographic Evidence

Evidence Bag

Seizing evidence

Time

Transporting

Damages

Chain of Custody

Pre-investigation

- Planning for an investigation is the key.
- Setting up the Infrastructure
 - Required Tools, Software's, Hardware's, Media, Workstation
 - Consider – Types of Investigation, Cases, Workforce, Workstation requirements, Safe, Connectivity, Storages
 - Access Control
 - Regular Audits
- Roles and Responsibilities
- Physical Hardware's and Licensed Tools
- Local Policies and Laws of the Land
- Best Practices
- Industry Standards
- Risk Assessment

Pre-Investigation – Your Team

- **Building the Investigation Team:**

- + Identify team members and assign responsibilities – Eg: Technical lead for the investigation etc.
- + Keep the team small for confidentiality and to avoid leaks.
- + Provide necessary clearance and authorization to team members.
- + Enlist help from trusted external investigation teams if needed.

- **Roles in Evidence Collection:**

- ✓ Photographer: Captures crime scene and evidence.
- ✓ Incident Responder: Secures incident area and collects evidence.
- ✓ Incident Analyzer: Analyzes incidents and their impact on systems.
- ✓ Evidence Examiner/Investigator: Examines and prioritizes evidence.
- ✓ Evidence Documenter: Documents investigation phases and evidence.
- ✓ Evidence Manager: Manages evidence and maintains records.
- ✓ Expert Witness: Offers formal testimony in court. - Attorney: Provides legal advice for the investigation process.

Pre-Investigation – Your Team

- **Understanding Hardware and Software Requirements:**

- + Hardware:

- ✓ Forensic workstations
 - ✓ Specialized cables, write-blockers, duplicators
 - ✓ Archive and restore devices, media sterilization systems
 - ✓ Forensic hardware toolkit

- + Software:

- ✓ Operating systems, data discovery and recovery tools
 - ✓ Password-cracking and acquisition tools
 - ✓ Data analyzers, file viewers, security utilities
 - ✓ Forensic software tools like Wireshark, FTK, etc.

Pre-Investigation – Your Team

- **Validating Laboratory Software and Hardware:**

- + Validate hardware and software tools before use.
- + Ensure licensed versions of all software.
- + Update and test tools regularly.
- + Maintain proper documentation of testing methodology and results.
- + Ensure compliance with licensing and standards.

- **Ensuring Quality Assurance:**

- ✓ Arrange formal trainings and proficiency tests.
- ✓ Validate equipment and maintain documentation.
- ✓ Follow appropriate standards and procedures. (*Attain ASCLD/LAB or ISO/IEC 17025 accreditation*)
- ✓ Conduct quality audits and reviews regularly.
- ✓ Ensure physical plant security and health and safety measures.
- ✓ Review and update policies and standards annually.

Investigation – Response

“First response involves the initial action taken after a security incident to prevent further damage and facilitate investigation. It includes identification of victim systems and individuals for further action”

■ First Response Basics:

- + First responder assesses the scene and alerts management and response teams.
- + Their actions significantly impact investigation processes and outcomes.

+ Non-forensics Staff:

- ✓ Protects the crime scene and maintains security until forensics team arrives.
- ✓ Notes and photographs the scene and individuals present for forensic team.
- ✓ Secures surrounding area and electronic devices linked to the incident.

+ System/Network Administrators:

- ✓ Responsible for system and network security and maintenance.
- ✓ Monitor system activities, report incidents, and follow organizational procedures.
- ✓ Take measures like recording on-screen activities, isolating systems, and documenting incident details.

Investigation – Response

- **First Response Basics:**

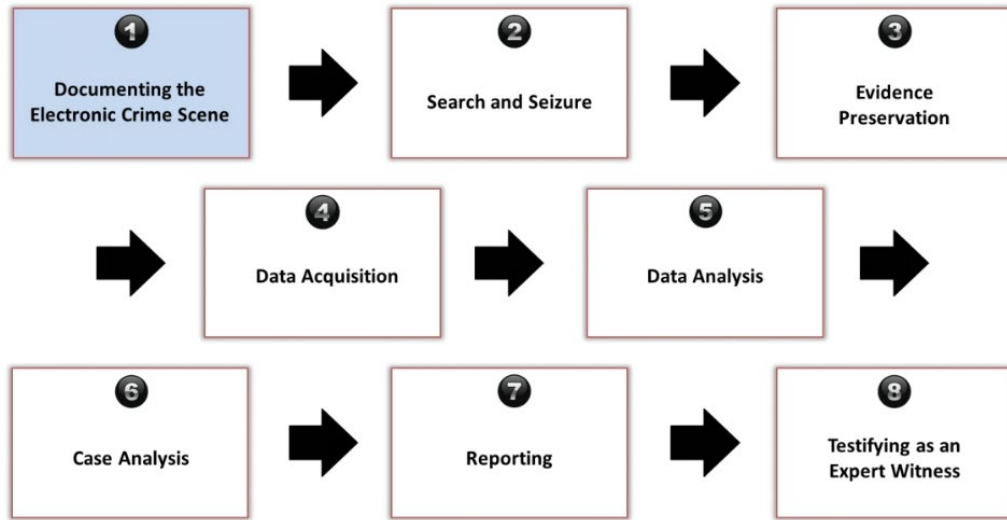
- + **System/Network Administrators:**

- ✓ Responsible for system and network security and maintenance.
 - ✓ Monitor system activities, report incidents, and follow organizational procedures.
 - ✓ Take measures like recording on-screen activities, isolating systems, and documenting incident details.

- + **Laboratory Forensics Staff: (six stages)**

- ✓ Documenting the Electronic Crime Scene
 - ✓ Collecting Incident Information
 - ✓ Planning for Search and Seizure
 - ✓ Identifying and Collecting Electronic Evidence
 - ✓ Packaging Electronic Evidence
 - ✓ Transporting Electronic Evidence

Investigation – In Detail



Points to consider:

- + Immediate photography upon arrival.
- + Photographs should be clear and comprehensive.
- + Multiple angles to capture entire scene.
- + Capture back of computer system and label cables.
- + Prepare sketches detailing objects and locations.

Documenting the Electronic Crime Scene:

+ Documentation creates a permanent record of the crime scene and investigation processes.

- ✓ Includes details of crime location, system status, connected devices, storage media, etc.
- ✓ Process involves taking photographs, videos, notes, and sketches to recreate the scene later.

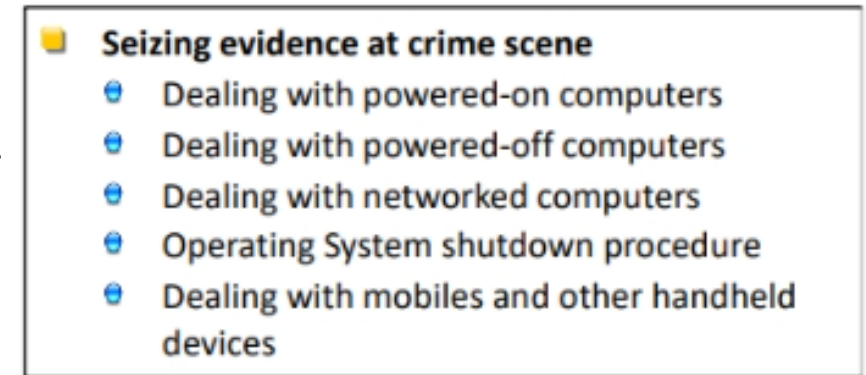
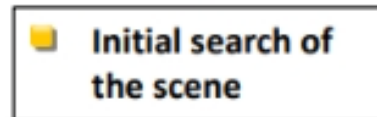
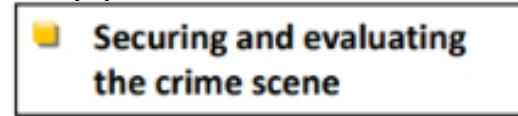
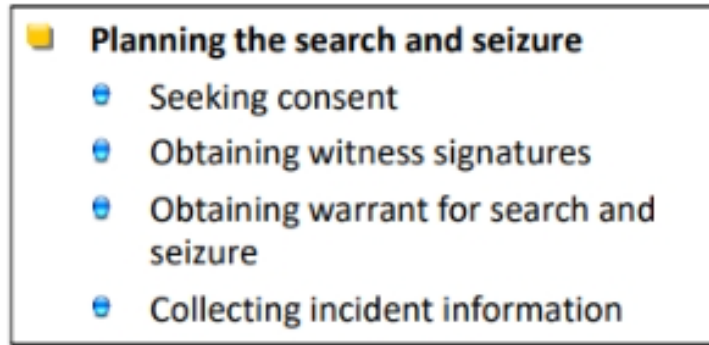
+ Key considerations:

- ✓ Continuous documentation during investigation.
- ✓ Detailed recording of system and device states.
- ✓ Documenting physical crime scene and related electronic components.
- ✓ Recording power status and screen contents.
- ✓ Photographing and Sketching the Scene:
- ✓ Provides visual reference and aids in scene recreation.

Investigation – In Detail

Designing the Search and Seizure Plan:

- + Strategic process to distribute tasks and utilize time efficiently.
- + Includes description, location, jurisdiction, extent of authority, and chain of custody details.
- + **Considerations:** equipment details, seizure type, local management approval, health and safety precautions.



Seeking Consent:

- + Process of obtaining formal permission from owner of victim organization or individual.
- + Written consent with properly written banners and suitable use policies.
- + Use appropriate forms for jurisdiction and carry documents in forensic grab bag.

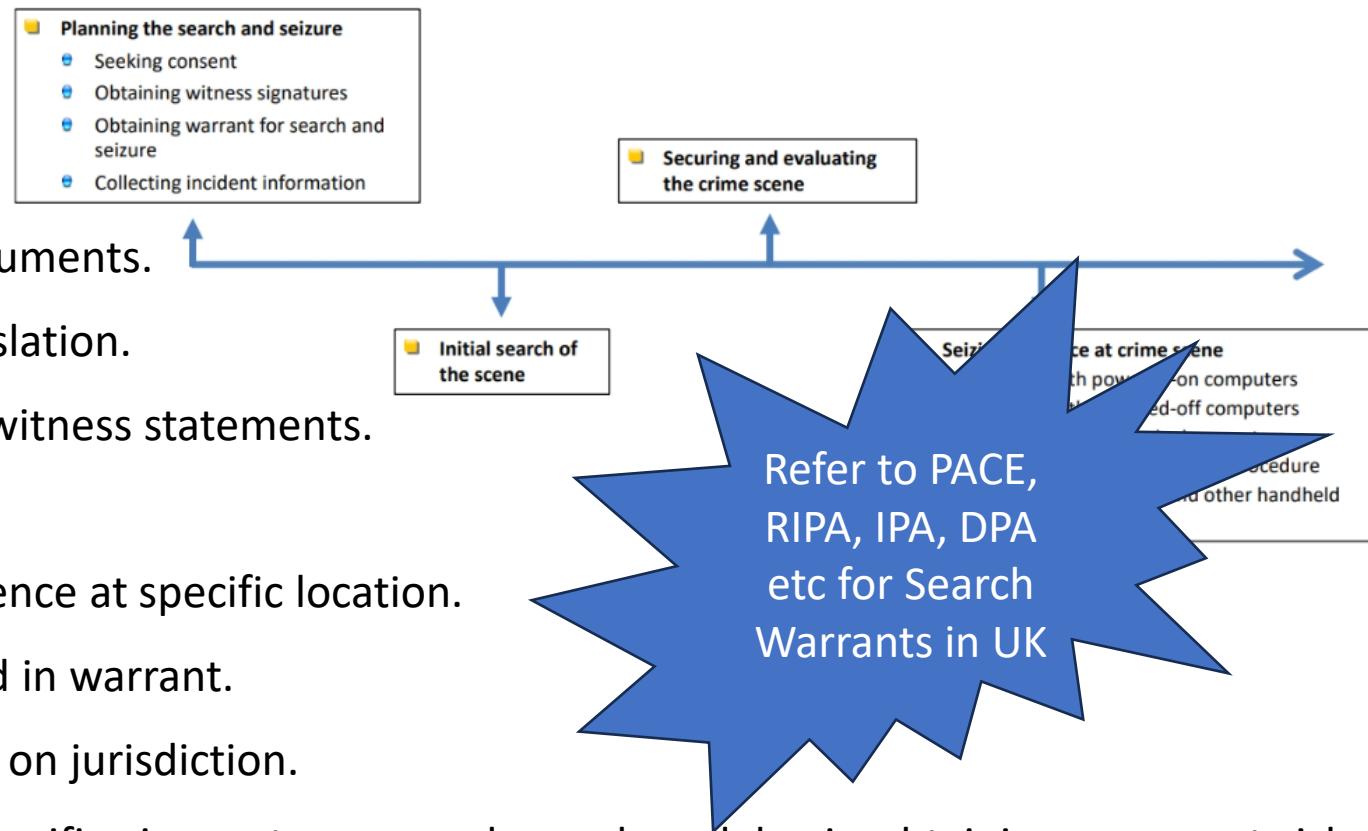
Investigation – In Detail

■ Obtaining Witness Signatures:

- + Verification of consent form and other written documents.
- + One or two witness signatures required as per legislation.
- + Witnesses understand their role and may provide witness statements.

■ Obtaining Warrant for Search and Seizure:

- + Written order from judge directing search for evidence at specific location.
- + Details of objects and devices to be seized included in warrant.
- + Note the validity of the Warrant. – Vary depending on jurisdiction.
- + **Searches without a warrant** are allowed under specific circumstances, such as when delay in obtaining a warrant risks evidence destruction or manipulation.
- + If there is probable cause to believe that seized items constitute evidence of criminal activity, a warrantless seizure may be justified.
- + Consent from a person with authority can also justify a search without a warrant or probable cause.



Investigation – In Detail

- **Collecting Incident Information:**
 - + Gather information about victim devices, connected systems, and users.
 - + Includes usernames, passwords, purpose of system usage, installed hardware/software, etc.
 - + Conduct preliminary interviews to gather more information about the incident.
- **Initial Search of the Scene:**
 - + Survey crime scene, protect physical evidence, and observe current situation.
 - + Maintain search and seizure evidence log.
 - + Secure and evaluate the crime scene using standard procedures.
- **Seizing Evidence at the Crime Scene:**
 - + Collect electronic devices and storage media.
 - + Package seized items carefully and tag with details.
 - + Different handling for powered-on and powered-off computers.

Investigation – In Detail

- **Dealing with Open Files and Startup Files:**
 - + Examine open files and startup folders for sensitive data.
 - + Record date and time of files, and unusual access times.
- **Operating System Shutdown Procedure:**
 - + Proper shutdown procedure to prevent data loss.
 - + Different procedures for Windows, Mac OS X, and UNIX/Linux OS.
- **Dealing with Smartphones or Other Handheld Devices:**
 - + Photograph device and screen display.
 - + Do not turn OFF if already ON.
 - + Collect necessary information and tag evidence accordingly.

Investigation – In Detail

- **Preserving Evidence:**
 - + Importance of handling and preserving evidence intact.
 - + Key steps include recording observations, tagging evidence, and maintaining a chain of custody record.
- **Chain of Custody:**
 - + Legal document tracking evidence from crime scene to forensic lab.
 - + Ensures integrity and accountability of evidence handling.
 - + Includes details of evidence collectors, actions taken, and technology/methodology used.
 - + Information recorded in chain of custody: case number, source, date/time, description, and reason for obtaining evidence.
- **Evidence Bag Contents List:**
 - + Details required on evidence bags: date/time of seizure, incident responder, exhibit number, location seized from, and submitting agency.

Investigation – In Detail

- **Packaging Evidence:**
 - + Correct documentation, labeling, and listing before packaging.
 - + Safeguard hidden or trace evidence.
 - + Use appropriate antistatic packaging and avoid static-generating materials.
- **Exhibit Numbering:**
 - + Tagging evidence with sequential numbers for identification.
 - + Format includes initials, date of seizure, sequential number, and sequence number for parts.
- **Determining Examination Location:**
 - + Considerations for onsite vs. laboratory examination.
 - + Factors include time required, logistics, workforce concerns, and business impact.

Investigation – In Detail

- **Transporting and Storing Evidence:**
 - + Special care during transportation to prevent damage.
 - + Avoidance of extreme weather conditions, physical shock, static electricity, and magnetic fields.
 - + Proper storage away from extreme heat, cold, moisture, and magnetic sources.
 - + Maintaining chain of custody during transportation.

Understanding Investigation Process - Storage Formats

- Data acquisition is the **process of copying data**.
- In the perspective of Digital Forensics, it's the task of **collecting digital evidence from electronic media**.
- Formats
 - **Raw format:** Makes it possible to write bit-stream data to files
 - **Advantages**
 - ✓ Fast data transfers
 - ✓ Can ignore minor data read errors on source drive
 - ✓ Most computer forensics tools can read raw format
 - **Disadvantages**
 - ✓ Requires as much storage as original disk or data
 - ✓ Tools might not collect marginal (bad) sectors
 - Proprietary formats
 - Advanced Forensics Format (AFF)

Understanding Investigation Process - Storage Formats

- Data acquisition is the **process of copying data**.
- In the perspective of Digital Forensics, it's the task of **collecting digital evidence from electronic media**.
- Formats
 - **Raw format:** Makes it possible to write bit-stream data to files
 - **Proprietary formats:**
 - **Features offered**
 - ✓ Option to compress or not compress image files
 - ✓ Can split an image into smaller segmented files
 - ✓ Can integrate metadata into the image file
 - **Disadvantages**
 - ✓ Inability to share an image between different tools
 - ✓ File size limitation for each segmented volume
 - Advanced Forensics Format (AFF)

Understanding Investigation Process - Storage Formats

- Data acquisition is the **process of copying data**.
- In the perspective of Digital Forensics, it's the task of **collecting digital evidence from electronic media**.
- Formats
 - **Raw format:** Makes it possible to write bit-stream data to files
 - **Proprietary formats:**
 - **Advanced Forensics Format (AFF):** Developed by Dr. Simson L. Garfinkel of Basis Technology Corporation
 - **Design goals**
 - ✓ Provide compressed or uncompressed image files
 - ✓ No size restriction for disk-to-image files
 - ✓ Provide space in the image file or segmented files for metadata
 - ✓ Simple design with extensibility
 - ✓ Open source for multiple platforms and Oss
 - ✓ Internal consistency checks for self-authentication
 - **File extensions include .afd for segmented image files and .afm for AFF metadata**
 - **AFF is open source**

Acquisition Methods

Types of acquisitions

- ✓ Static acquisitions
- ✓ Live acquisitions

Methods

- **Bit-stream disk-to-image file**
 - ↪ Most common method
 - ↪ Can make more than one copy
 - ↪ Copies are bit-for-bit replications of the original drive
 - ↪ ProDiscover, EnCase, FTK, SMART, Sleuth Kit, X-Ways, etc.
- **Bit-stream disk-to-disk**
 - ↪ When disk-to-image copy is not possible
 - ↪ Consider disk's geometry configuration
 - ↪ EnCase, SafeBack, SnapCopy etc

Acquisition Methods

Types of acquisitions

- ✓ Static acquisitions
- ✓ Live acquisitions

Methods

- **Logical disk-to-disk or disk-to-disk data and Sparse data copy of a file or folder**
 - ↪ When your time is limited
 - ↪ Logical acquisition captures only specific files of interest to the case
 - ↪ Sparse acquisition also collects fragments of unallocated (deleted) data
 - ↪ For large disks
 - ↪ PST or OST mail files, RAID servers etc

Acquisition Methods

Methods

○ Rule of Thumb

- ↯ When making a copy, consider the **size of the source** disk
 - ↯ Lossless compression might be useful
- ↯ Use digital signatures for verification
- ↯ When working with large drives, an alternative is using advanced backup systems

○ Contingency Plan

- ↯ Create a duplicate copy of your evidence image file. Make at least two images of digital evidence
- ↯ Use different tools or techniques
- ↯ Copy host protected area of a disk drive as well
- ↯ Consider using a hardware acquisition tool that can access the drive at the BIOS level
- ↯ Be prepared to deal with encrypted drives
- ↯ Consider whole disk encryption feature in Windows

Acquisition Tools

Acquisition tools for Windows

- **Advantages**

- ↪ Make acquiring evidence from a suspect drive more convenient
- ↪ Especially when used with hot-swappable devices

- **Disadvantages**

- ↪ Must protect acquired data with a well-tested write-blocking hardware device
- ↪ Tools can't acquire data from a disk's host protected area
- ✓ **USB write-protection feature**, blocks any writing to USB devices
- ✓ **Target drive needs to be connected to an internal PATA (IDE), SATA, or SCSI controller**
- ✓ **Back up the Registry and modify the Registry with the write-protection feature.** *Consider creating two desktop icons to automate switching between enabling and disabling writes to USB device*

Acquisition Tools

Acquisition tools for Linux

- **Linux can access a drive that isn't mounted**
- **Forensic Linux Live CDs don't access media automatically**
 - ↯ Which eliminates the need for a write-blocker
 - ↯ Contain additionally utilities
 - ↯ Configured not to mount, or to mount as read-only, any connected storage media
 - ↯ Well-designed Linux Live CDs for computer forensics
 - ↯ Helix, Penguin Sleuth, FCCU
- **Preparing a target drive for acquisition in Linux**
 - ↯ Linux distributions can create Microsoft FAT and NTFS partition tables
 - ↯ fdisk command lists, creates, deletes, and verifies partitions in Linux
 - ↯ mkfs.msdos command formats a FAT file system from Linux

Acquisition Tools

Acquisition tools for Linux

- **Preparing a target drive for acquisition in Linux**

- ↪ Linux distributions can create Microsoft FAT and NTFS partition tables
- ↪ fdisk command lists, creates, deletes, and verifies partitions in Linux
- ↪ mkfs.msdos command formats a FAT file system from Linux

- **Acquiring data with dd in Linux**

- ↪ dd (“data dump”) command
 - ↪ Can read and write from media device and data file
 - ↪ Creates raw format file that most computer forensics analysis tools can read

- **Shortcomings of dd command**

- ↪ Requires more advanced skills than average user
- ↪ Does not compress data
- ↪ dd command combined with the split command - Segments output into separate volumes

Acquisition Tools

Acquisition tools for Linux

- **Acquiring data with dcfldd in Linux**

- ↪ dd command is **intended as a data management tool**
- ↪ Not designed for forensics acquisitions

- **dcfldd Functions**

- ↪ **Specify hex patterns** or text for clearing disk space
- ↪ **Log errors** to an output file for analysis and review
- ↪ Use several **hashing options**
- ↪ Refer to a status display **indicating the progress of the acquisition** in bytes
- ↪ **Split data acquisitions into segmented volumes** with numeric extensions
- ↪ **Verify** acquired data with original disk or media data

Acquisition Tools

Acquisition tools for Linux

- **Acquiring data with dcfldd in Linux**
 - ↪ dd command is **intended as a data management tool**
 - ↪ Not designed for forensics acquisitions

The Process

- **Connecting the suspect's drive to your workstation**
 - ↪ Document the chain of evidence for the drive
 - ↪ Remove the drive from the suspect's computer
 - ↪ Configure the suspect drive's jumpers as needed
 - ↪ Connect the suspect drive
 - ↪ Create a storage folder on the target drive

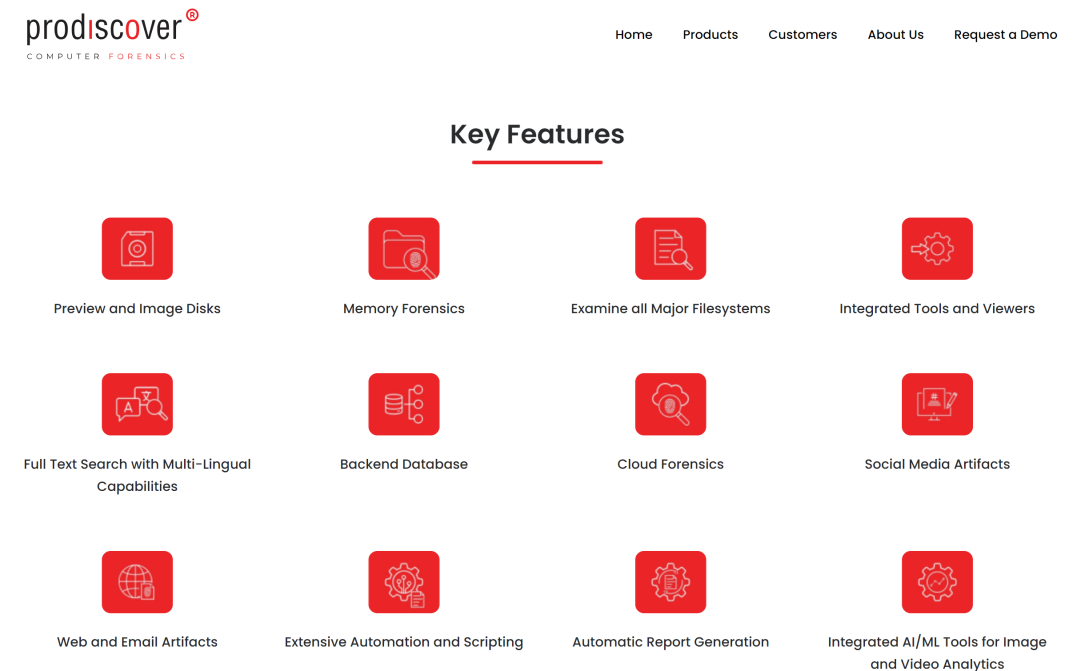
The Tools

○ Using ProDiscover's Proprietary Acquisition Format

- ↪ Image file will be split into segments of 650MB
- ↪ Creates image files with an .eve extension, a log file (.log extension), and a special inventory file (.pds extension)

○ Using ProDiscover's Raw Acquisition Format

- ↪ Select the UNIX style dd format in the Image Format list box
- ↪ Raw acquisition saves only the image data and hash value

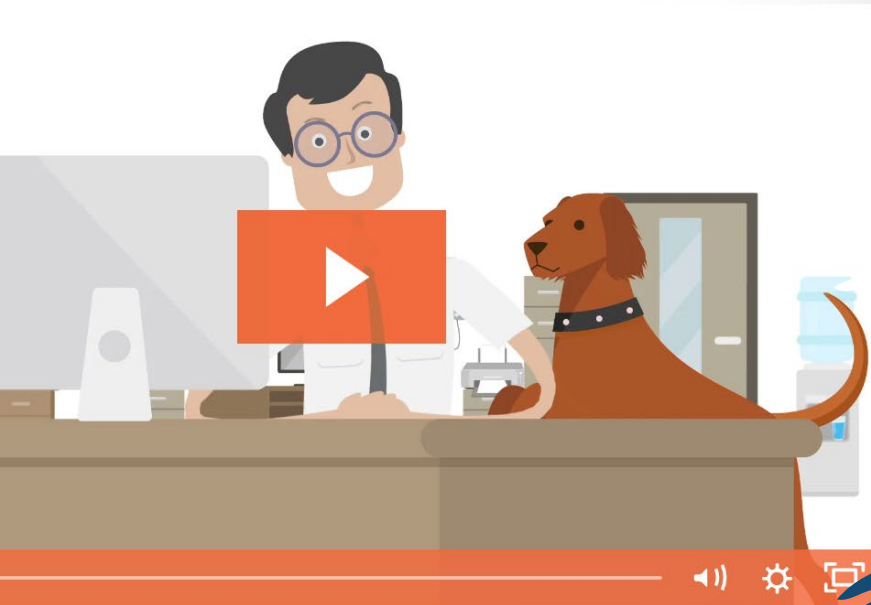


Forensic Toolkit

Standard in Digital Forensics For Over 15 Years

LOAD FREE FTK[®] IMAGER

SCHEDULE A MEETING



○ FTK Imager

- ↪ Included on FTK Forensic Toolkit
- ↪ View evidence disks and disk-to-image files
- ↪ Makes disk-to-image copies of evidence drives
 - ↪ At logical partition and physical drive level
 - ↪ Can segment the image file
- ↪ Evidence drive must have a hardware write-blocking device, Or the USB write-protection Registry feature enabled
- ↪ FTK Imager can't acquire drive's host protected area

○ Validating the acquired Data:

- ↪ Most critical aspect of digital forensics
- ↪ Requires using a hashing algorithm utility
- ↪ Use validation techniques like CRC-32, MD5, and SHA-1 to SHA-512

Acquisition Tools

Validating dd acquired data

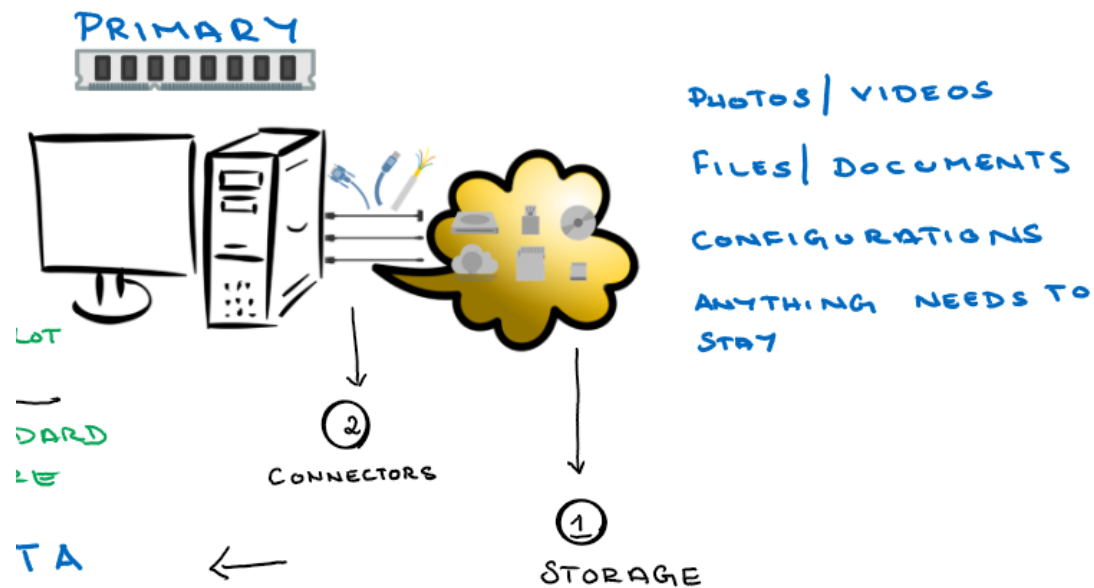
- You can use md5sum or sha1sum utilities
- md5sum or sha1sum utilities should be run on all suspect disks and volumes or segmented volumes

Validating dcfldd acquired data

- Use the hash option to designate a hashing algorithm of md5, sha1, sha256, sha384, or sha512
- hashlog option outputs hash results to a text file that can be stored with the image files
- vf (verify file) option compares the image file to the original medium
- **Windows has no built-in hashing algorithm tools** for digital forensics, however third-party utilities can be used
- Commercial digital forensics programs also have built-in validation features. Each program has its own validation technique
- **Raw format image files don't contain metadata**
 - ▮ Separate manual validation is recommended for all raw acquisitions

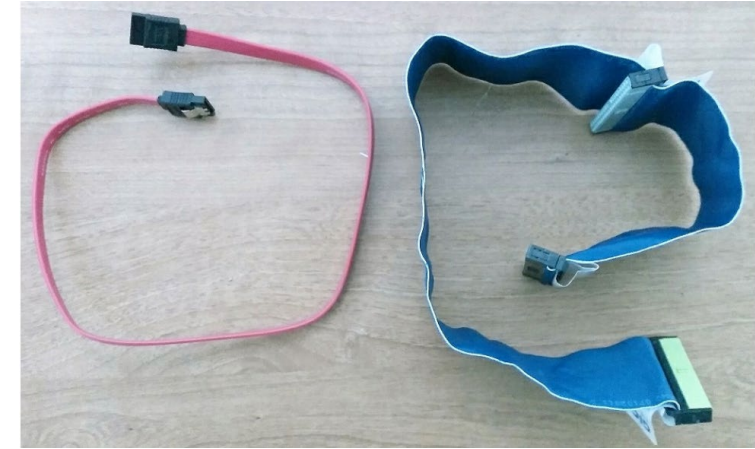
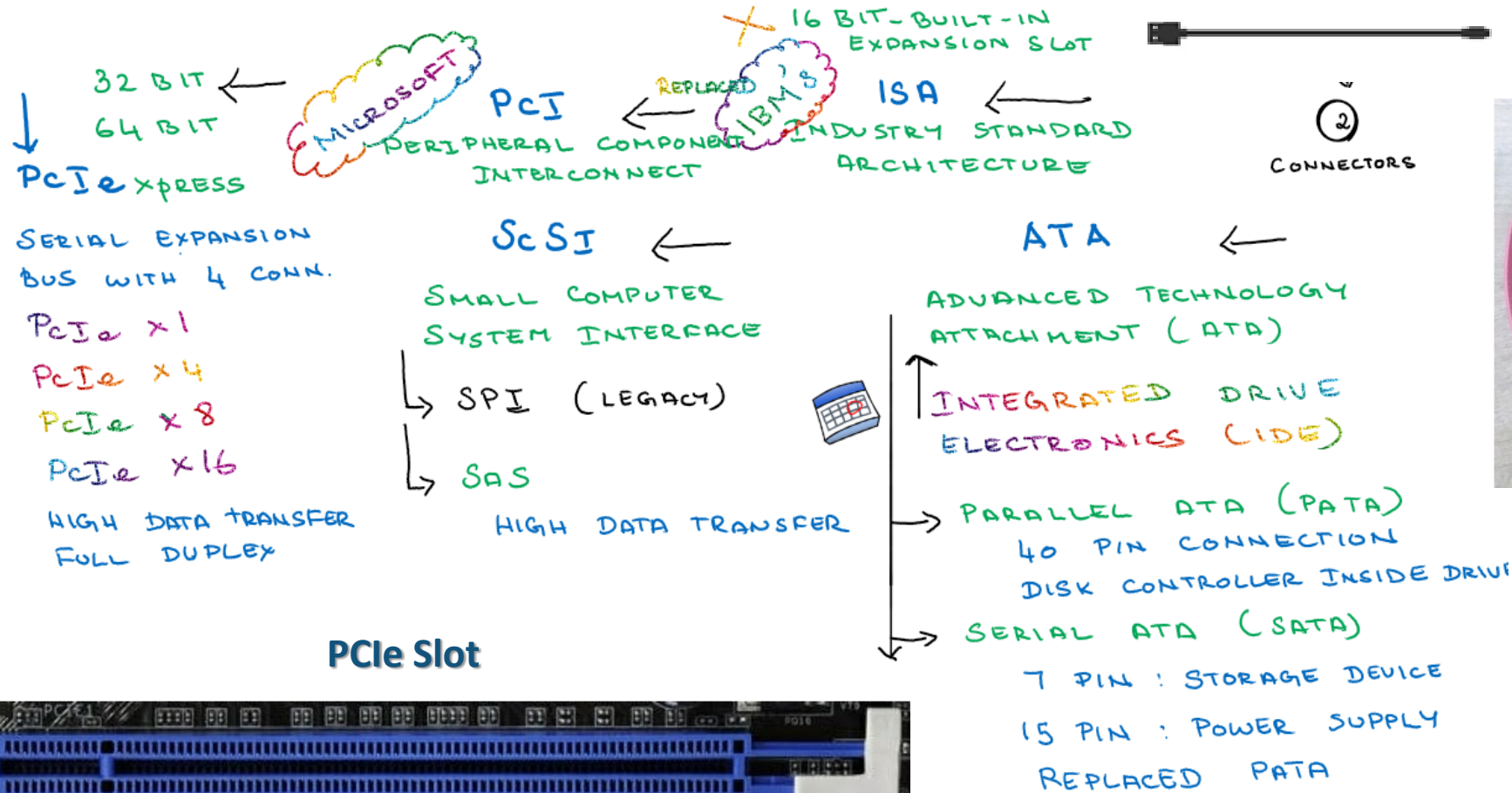
Storage

- **STORAGE SPACE** is also a vital information to consider.
- Technologies like IDE, SAS, SCSI DAS, NAS, SAN, RAID are some of the storage technology options.



1890	PUNCH CARDS
1932	MAGNETIC DRUM
1947	1st RAM (Very small memory)
1951	Magnetic Tape Drive
1956	Hard Disk Drive (HDD)
1967	Floppy Disk Drive
1982	Compact Disc
1994	Zip Drive
1995	Digital Video Disc (DVD)
1999	SD Card
1999	USB Flash Drive
2003	Blu-ray Optical Disc
2006	Cloud Data Storage

Storage



PATA and SATA Cables



Storage Protocols

- Protocols that help in storage and retrieval process from storage devices
- **SCSI:**
 - ✓ *Used in Block – level Storage Systems*
 - ✓ *Server OS use this protocol to read/ write data on SCSI Controller which is managing the storage device*
- **iSCSI:**
 - ✓ *Takes SCSI in an IP Packet – For extendable functionalities.*
 - ✓ *Clients (Initiators) connected with iSCSI use IP Protocol to send SCSI Commands (Command Descriptor Blocks) to Storage Devices (Targets).*
 - ✓ *TCP Ports 860 is reserved for iSCSI system Port and 3260 is iSCSI default port*
- **Fibre Channel:**
 - ✓ *For extendable functionalities enabling storage consolidation and longer distance coverage*
- **Fibre Channel over Ethernet:**
 - ✓ *Extends across Ethernet Networks*

File Sharing Protocols

File Sharing Protocols enable data sharing over LAN's, WAN's and Internet...

Server Message Block (SMB), also known as the **Common Internet File System (CIFS)**, is a file sharing protocol used mostly by Windows OSes.

Network File System (NFS) is a file sharing protocol used mostly by Unix and Linux.

File Transfer Protocol (FTP) enables file sharing by transferring files from site to site.

Hypertext Transfer Protocol (HTTP) enables file sharing over a **World Wide Web (WWW)** service.

Secure Shell (SSH) enables remote file sharing over a secure connection.

Redundant Array of Independent Disks (RAID)

- ***There are a lot of different ways a RAID may be configured.***

- ✓ These are numbered, from 0 to 6, with it also being possible to combine RAID 1 and RAID 0, usually named 1 + 0, or just RAID 10 (said “ten”).
- ✓ We usually only ever see configurations of RAID 0, 1, 5, 6 and 10. 2, 3 and 4 fill specific purposes which don’t come up that often – we won’t look at them, but feel free to investigate if especially interested.

- ***Different RAID levels suit different circumstances, have different levels of performance in different situations, in addition to added implied risk.***

- ***Some assumptions about hard drives and RAID to be aware of:***

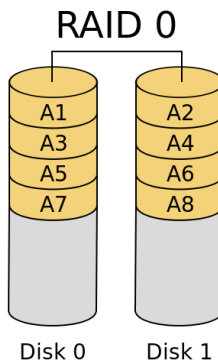
- ✓ They fail, a lot.
- ✓ They fail more the older they are. Multiple hard drives bought simultaneously and used evenly have a reasonable chance of dying quite close to one another.
- ✓ They’re usually the “slowest” component in a computer.

Redundant Array of Independent Disks (RAID)

- ***Drives in a RAID are effectively “combined” into a single drive. So, 4 hard drives might be combined to make 1 area of storage which uses all 4 drives.***
 - ✓ Drives are usually the same size. If they aren't, larger drives allocate the size of the smallest drive.
- ***RAID IS NOT A BACKUP. No matter how redundant your RAID is, or how safe it appears.***
 - ✓ RAID's can very, very occasionally fail for no discernible reason.
 - ✓ Are usually built so that the hard drives are in the same physical area – highly vulnerable to power fluctuations and natural disasters.

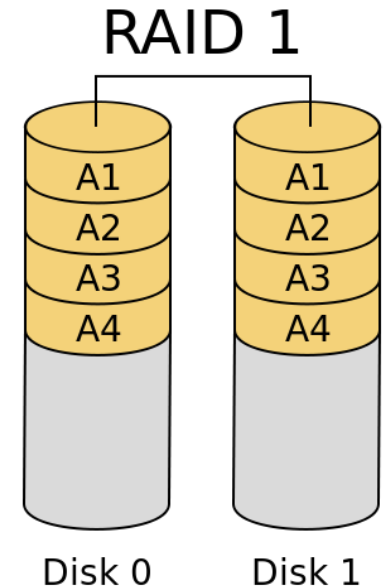
RAID levels – RAID 0 (striped)

- **RAID 0 is strange, because it isn't actually redundant. In fact, it's sort of the opposite of what we're trying to achieve.**
 - ↪ Some people argue it shouldn't be considered a RAID level at all.
- When we write data to a RAID 0 configuration, it's evenly split across each disk. So, in the picture **on the right, 50% of the data is written to disk 0, 50% to disk 1.**
 - ↪ This is called "striping"
 - ↪ Files are split across both disks.
 - ↪ This is extremely fast – two disks are twice as fast at 1.
 - ↪ Also, extremely risky – if any disk in a RAID 0 configuration fails, the entire RAID fails. If you don't have a backup, your data is permanently lost, and cannot be recovered from the remaining functional disk(s).
- **Lots of people use RAID 0 for performance.**
 - ↪ You can have lots of disks in a RAID 0 configuration, but more disks means more risk of any one disk failing.
 - ↪ Speed of writing to, or reading from, a RAID 0 array scales fairly linearly with the number of disks.
 - ↪ Storage scales with the number of disks. 4 x 1TB disks in a RAID 0 array gives 4TB of storage.



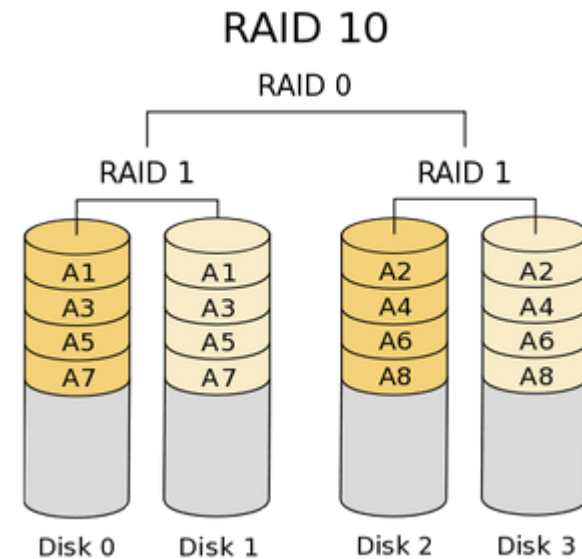
RAID levels – RAID 1 (mirrored)

- **All data written to the array is written to all disks in the array simultaneously.**
 - ↪ Writing is as slow as writing to 1 disk.
 - ↪ Reading scales reasonably well with the number of disks.
 - ↪ This is called mirroring.
- **Sometimes considered the opposite of RAID 0 – true, absolute redundancy.**
- **In a 4-disk array, all 4 have to fail before you lose your data.**
 - ↪ Array rebuilds unlikely to result in data loss for large RAID 1 arrays.
- **Storage does not scale at all. If you have 4 x 1TB disks in a RAID 1 array, you have 1TB of storage. If you have 100 disks, you still have 1TB of storage.**



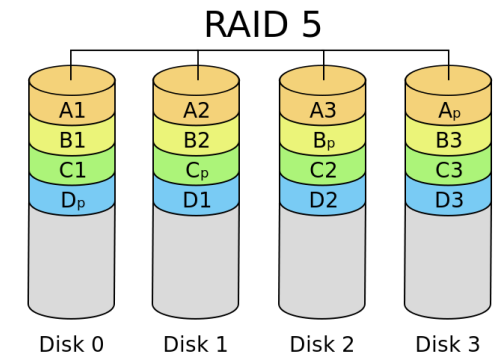
RAID levels – RAID 10 (striped + mirrored)

- **This applies mirroring AND striping.** The image on the right shows mirroring then striping (which is by far the most normal approach), but it can happen either way, and has some subtle differences when done in reverse.
- **A good combination of performance and redundancy – most of the benefits of RAID 0 and RAID1.**
 - ↪ Fast write times (due to striping).
 - ↪ Fast read times (due to mirroring and/or striping).
- **Requires a minimum of 4 disks, and must always have a multiple of two.**
 - ↪ Effectively divides available space in half. In a 4 x 1TB RAID 10 array, you have 2TB of available storage.
- **Two copies of all pieces of data.**
 - ↪ Some risk during an array rebuild (more on this on the next slide).
 - ↪ Failure of 2 disks can cause the array to fail, while it may tolerate the failure of up to 50% - very luck-dependent on which disks fail.



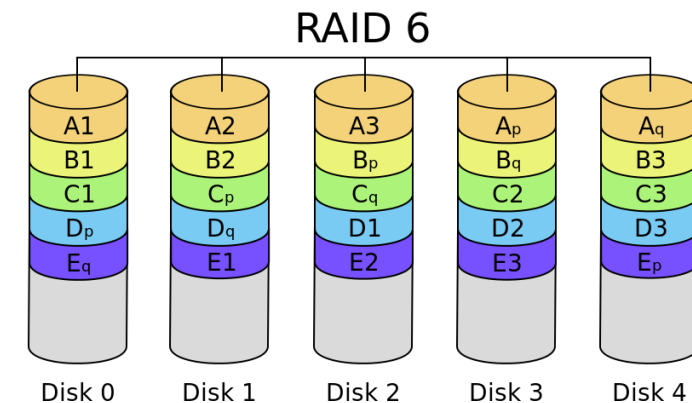
Raid levels – RAID 5

- **Uses a form of striping with an added (distributed) “parity” block.**
 - ↪ Direct (but very small) upgrade from RAID 4 – which is the same, but with a single, dedicated parity disk. This puts stress on a single disk.
 - ↪ Parity information can be used to re-calculate the data on a failed disk, in combination with the other data.
 - ↪ The parity value itself must be calculated, making RAID 5 more computationally expensive than the RAID levels we’ve looked at before it.
- **Storage is effectively size of disk array -1. So a 4 x 1TB RAID 5 array is of size 3TB.**
- **Can consist of between 3 and ∞ disks. Large numbers of disks are extremely inadvisable for this array type.**
- **Can tolerate the failure of exactly 1 disk. If a second disk dies, the array is entirely lost without a full restore from backup.**
- **Should not use large disks for this array.**



RAID levels – RAID 6

- Same as RAID 5, but with two disks worth of distributed parity information.
- Much safer than RAID 5 – always tolerates the failure of two disks (though always fails on 3).
- Near-identical read-write performance to RAID 5.
- Write slightly worse than RAID 5.
- The maths underpinning how this works is quite complex.
- Storage size is always size of array – 2. So for a 4x1TB RAID 6 array, 2TB of data can be stored. For a 6x1TB array, 4TB.
- Still somewhat risky – but suffers from the same mass-read problem as RAID 5, but with an extra layer of safety.
- Minimum of 4 drives, theoretically ∞ maximum, but not usually used for more than 6.



Redundant Array of Independent Disks (RAID)

- **Challenges**

- ✓ How much data storage is needed?
- ✓ What type of RAID is used?
- ✓ Do you have the right acquisition tool?
- ✓ Can the tool read a forensically copied RAID image?
- ✓ Can the tool read split data saves of each RAID disk?

- **Older hardware-firmware RAID systems can be a challenge when you're making an image**

- **Occasionally, a RAID system is too large for a static acquisition**

- ✓ Retrieve only the data relevant to the investigation with the sparse or logical acquisition method

Remote Acquisition

- **You can remotely connect to a suspect computer via a network connection and copy data from it**
- **Remote acquisition tools vary in configurations and capabilities**
- **Challenges**
 - ✓ LAN's data transfer speeds and routing table conflicts could cause problems
 - ✓ Gaining the permissions needed to access more secure subnets
 - ✓ Heavy traffic could cause delays and errors
- **With available remote acquisition tools, you can:**
 - ✓ Preview a suspect's drive remotely while it's in use
 - ✓ Perform a live acquisition
 - ✓ Encrypt the connection
 - ✓ Copy the suspect computer's RAM
 - ✓ Use the optional stealth mode

Remote Acquisition

- **Utilities**

- ✓ DiskExplorer for FAT
- ✓ DiskExplorer for NTFS
- ✓ HDHOST

- **Features for acquisition**

- ✓ Create a raw format image file
- ✓ Segment the raw format or compressed image
- ✓ Access network computers' drives

-:-Key Terms to Remember-:-

- Approved Secure Container
- Bit Stream Copy
- Bit Stream Image
- Chain of Custody
- Interrogation
- Single Evidence Form
- Multi Evidence Form
- American Society of Crime Laboratory Directors
- Certified Electronic Evidence Collection Specialist
- Certified Forensic Computer Examiner
- Risk Management