Introduction to Windows Digital Forensics

Thomas Benos

MSc UniWA, Cisco CyberOps
GR CSIRT Incident Responder
thomasbenos1291@gmail.com

Agenda

- Introduction to Digital Forensics
- Digital Forensics Process & Methology
- Evidence Handling & Chain of Custody
- Data Collection/Acquisition: Volatile and Non-Volatile data
- Timeline Analysis
- Challenges in Windows Forensics

Introduction to Digital Forensics

What is Digital Forensics?

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

- Digital forensics is the field of forensic science that is concerned with retrieving, storing and analysing electronic data that can be useful in criminal investigations. This includes information from computers, hard drives, mobile phones and other data storage devices.
- Source:

  https://www.nist.gov/digital-evidence

SANS

- Digital forensics is the forensic discipline that deals with the preservation, examination and analysis of digital evidence.
- Source:

  https://www.sans.org/cyber-security-courses/digital-forensics-essentials/

Types of Digital Forensics

- **Computer/ OS Forensics**: Computers, laptops
- **Mobile Device Forensics**: Smartphones, tablets, wearables
- **Network Forensics**: Network traffic (packet capture)
- **Memory Forensics**: Running processes and other artifacts
- **Database Forensics**
- **Email Forensics**
- **Malware forensics**: behavior, origins and impact of malware
- **Cloud Forensics**
- **Live Forensics**: running system, real-time
- **Incident Response**: identify and mitigate security incidents
- **Social Media Forensics**
- **Automotive Forensics**: vehicles (e.g accidents)
- **IoT Forensics**: smart home appliances, wearables

Digital Forensics Artifacts

- Any trace, residue, or piece of digital information left behind during a cyber incident -> **Digital Forensic Artifact**
- digital information -> anything with OS or anything that can be used in OS (media, USB, external disks, CDs, DVDs)
- derived from the user OR the OS itself

Digital Forensics Artifacts Examples

- Event Logs
- Network traffic packet capture
- Temporary files
- Downloaded files
- Email messages
- Deleted files
- Metadata
- Print logs
- System Memory
- Windows Registry

Why Digital Forensics?

- Digital Forensic Investigations:
  - Recover evidence
  - Recover lost data
  - Reconstruct events (timeline)

- Cyber Incidents:
  - Identify attackers
  - Understand Tactics, Techniques and Procedures (TTPs)
  - Cause, origin, impact of security breaches

Importance

- Crime Investigation
  - Identity theft
  - Electronic fraud
- Legal Proceedings
  - Digital evidence
  - Link of suspects
- Incident Response
  - Identify and mitigate security breaches
  - Prevent future incidents
  - Origin of cyber-attack / source of a leak
- Data Recovery
  - Business continuity

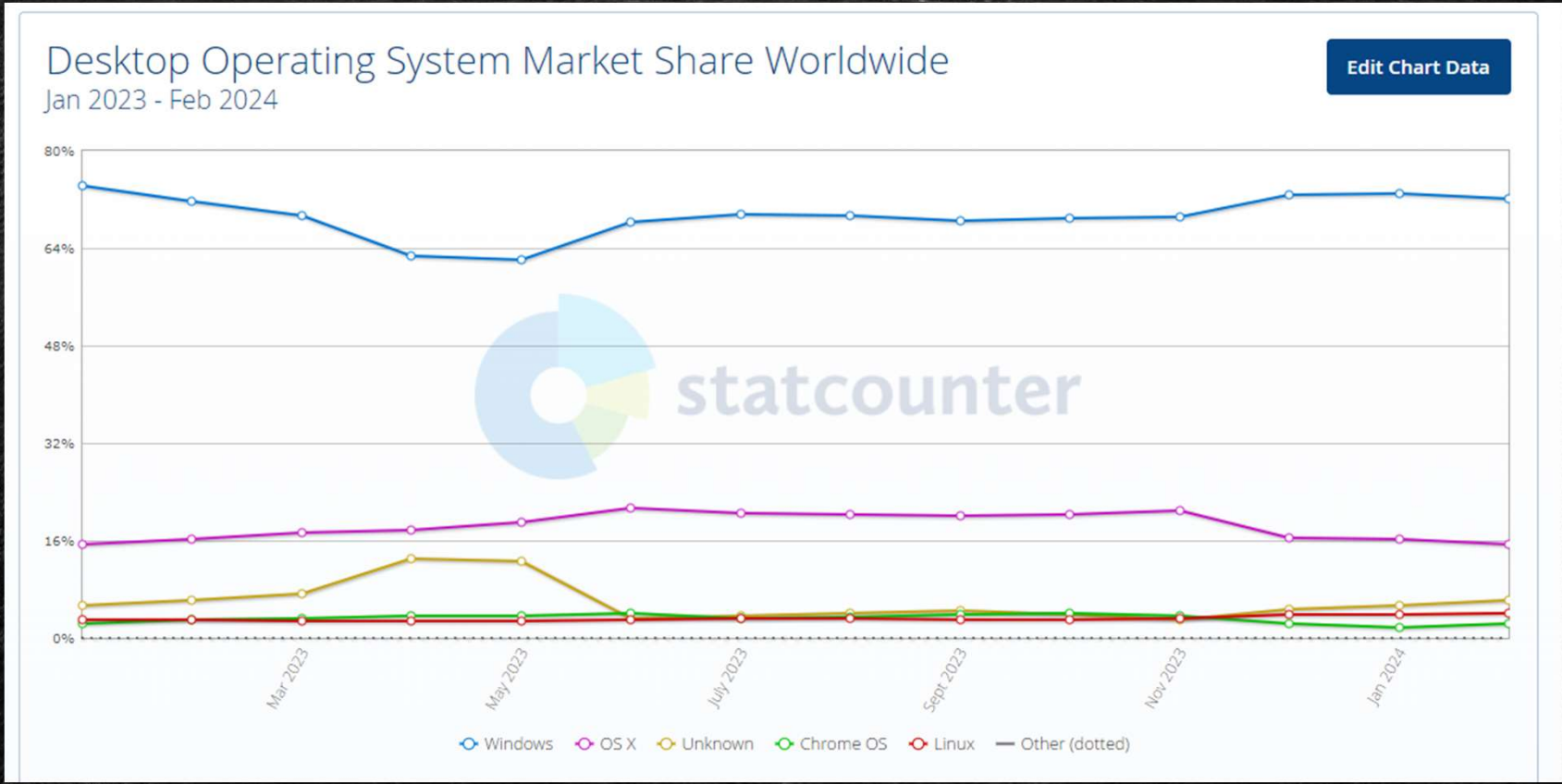
Applications

- Military
  - Cyber Threat Intelligence
  - Cyber Threat Mitigation
- Law Enforcement
  - Cybercrime Investigation
  - Evidence Collection
  - Counterterrorism
- Corporate Investigations
  - Intellectual Property Protection
  - Employee Misconduct

Lesson Scenario

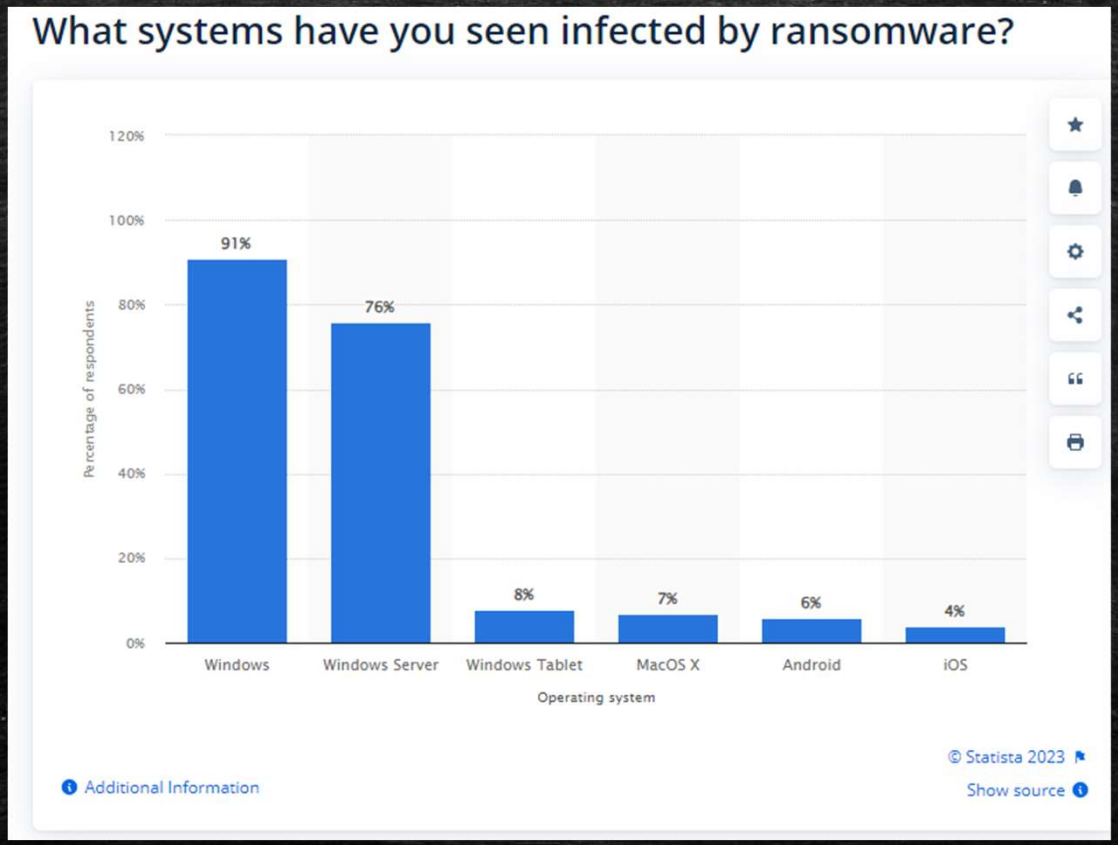
- Cyber Incident
  - Incident Response triggered on .pcap analysis
  - a Windows host is breached
- Mainly dead forensics
- Objectives:
  - Perform data volatile and non-volatile data acquisition
  - Identify Windows Forensic Artifacts
  - Perform analysis of Windows Forensic Artifacts
- Assignment: Perform digital forensics -> answer the questions

Why Windows Digital Forensics?



https://gs.statcounter.com/os-market-share/desktop/worldwide/#monthly-202301-202402

Why Windows Digital Forensics?



https://www.statista.com/statistics/701020/major-operating-systems-targeted-by-ransomware/

Purpose of the analyst

- Analyze in detail & present facts
  - What
  - When
  - Where
  - Who
  - How
- Reconstruct the events
- Stage of Cyber Kill Chain

Cyber Kill Chain Stages

Cyber Kill Chain Process – MITRE ATT&CK

MITRE | ATT&CK®

- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration

Purpose of the analyst (Cyber Kill Chain)

- Find the delivery mechanism
- Find the malware and its actions on the system
- Find the malware communications with the attacker (C&C)
- Find the motive of the attack
- Find the scope of the infection
- Find the next step of the attacker
- Find the impact of the successful attack

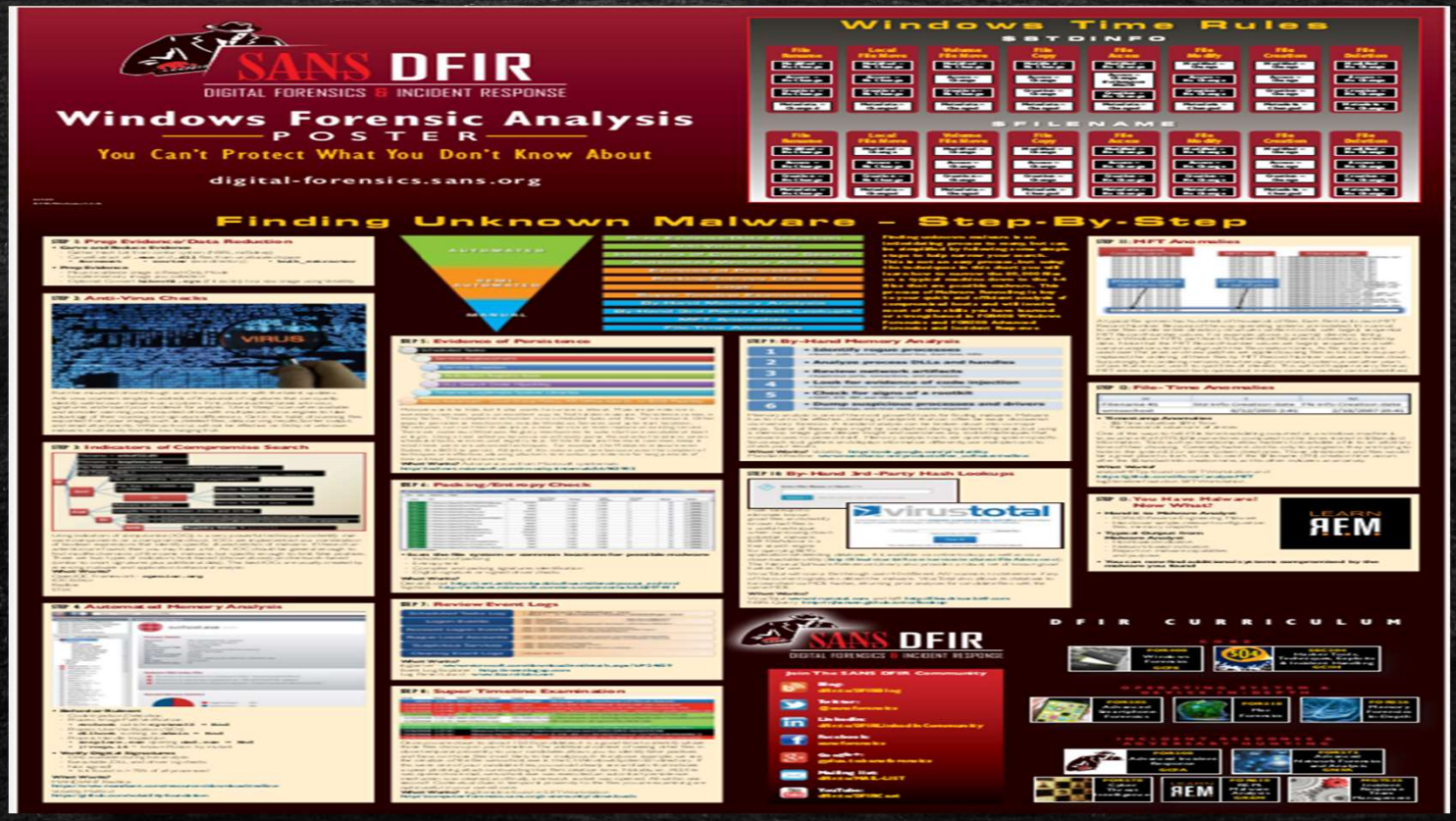
Digital Forensics Process & Methology

Digital Forensics Process

- **Collection**
  - Identify – Acquire – Preserve
- **Examination**
  - Extract data of interest
  - Maintain integrity
- **Analysis**
  - Legally justifiable methods/techniques
  - Answers to the questions
- **Reporting**
  - Actions – tools/procedures + chain of custody

https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf

Digital Forensics SANS Methology



https://networkforensic.dk/Tools/Files/cheat-sheets/Poster_Find_Evidence.pdf

Digital Forensics Practical Methology

- **(Incident Response Trigger)**
- **System Description**
- **Evidence Collection/Acquisition**
  - Order of Volatility
  - Chain of Custody
- **Examination/Analysis**
  - Anti-Virus check & IOC Search
  - Event Logs - Timeline analysis
  - File system analysis (e.g MFT, File Time anomalies)
  - Registry analysis (evidence of persistence or execution, USB)
  - Memory analysis (malfind, processes, network artifacts, code injection, rootkits)
  - Browser analysis
- **Reporting**

Evidence Handling & Chain of Custody

Chain of Custody - Definition

NIST | NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer.

https://csrc.nist.gov/glossary/term/chain_of_custody

Chain of Custody

- Document
- Chronological documentation of electronic evidence
- Indicates the collection, sequence of control, transfer, analysis
- Tracks movement and control of the evidence from the crime scene through to the courtroom
- Documents:
  - Description of the evidence (e.g memory image)
  - date and time it was collected/transfered
  - every person who handled it
  - purpose of a transfer
- Proof that evidence is untampered
- Tampered evidence –> inadmissible in court

Chain of Custody – Impacts if Broken

- Untrusted integrity of the system
- Unguaranteed reliability/accuracy of evidence
- Inadmissible in a court of law.
- Inability to determine malicious activity

Chain of Custody Form

Case Num.: 1	Pag.: 1	De: 2

Eletronic Media/Equipament Details

Item:	Description:
0002	HD 80 GB

Manufacturer:	Model:	Serial Number:
Maxtor	3.5 SERIES	Y2CFBP8C FY42A

Details about the data image

Date/Time:	Create by:	Method used:	Image Name:	Parts:
11/26/2010 at 05:30 PM	STAN SMITH	dd	hd_forense.dd	0001

Drive:	HASH:
Full Disc	9e9b4086ce24574182b342ac0a1e22ff

Chain Custody

Sequence:	Date/Time:	Source:	Destination:	Reason
0001	Date: 11/26/10 Time: 05:30 PM	Name/Crg.: Suspect Signature:	Name/Crg.: Lab. Perícia CIA Signature:	Investigation into complaint of pedophilia network.

Print Form

PROPERTY / EVIDENCE CHAIN OF CUSTODY FORM

APLCS, LLC (http://www.aplcs.com)

Case Name:	Reason Obtained:
Case Number:	

Item Number:	Evidence Type / Manufacturer:	Model Number:	Serial Number:

Content Owner / Title:	Content Description:

Content Owner Contact Information:

Forensic Agent:	Creation Method:	HASH Value:	Creation Date/Time:

Forensic Agent Contact Information:

CHAIN OF CUSTODY

Tracking Number	Date / Time	Released By	Received By	Reason for Change
	Date: / Time:	Name / Title / Signature	Name / Title / Signature	
	Date: / Time:	Name / Title / Signature	Name / Title / Signature	
	Date: / Time:	Name / Title / Signature	Name / Title / Signature	

Item Number: _____

Page: 1 of _____

Chain of Custody - Establishment practices and procedures

- Save the original materials - **ALWAYS WORK ON COPIES**
- Take photos of physical evidence
- Take screenshots of digital evidence content
- Document date, time, and any other information of receipt
- Make a digital forensic image
- Perform a hash test analysis to further authenticate the working clone

Data Collection/Acquisition: Volatile and Non-Volatile data

Live VS Dead Forensics

- **Live forensics** –> running machine
  - Real-time analysis – Dynamic response
    - Volatile data – RAM(active processes, network connections, system state)
    - Dynamic response
  - Non-invasive - Minimal Impact
    - No shutting down/altering system – minimum disruption
  - Useful for Incident Response
    - Ongoing security incidents

- **Dead forensics** –> powered down machine
  - Post-Incident Analysis – Static image/Persistent data
  - Evidence Integrity
  - Deleted data recovery
  - Thorough Examination - Useful for historical analysis

Volatile Data

- RAM (Random Access Memory)
- temporary – does not persist across reboots
- data from the programs that the CPU is processing in real-time
- all the frequently-used information and data
- data actively used and processed by the OS and applications

Volatile Data Types in Windows Systems

- Running Processes: currently running programs/apps
- System State: current OS state (open files, network connections, active user sessions)
- Network Connections
- Logged-in Users
- Clipboard Contents (copy-paste)
- Encryption Keys & Passwords
- FILELESS MALWARE!!!!!!

Order of Volatility (1/2)

1. **CPU cache and CPU registers content (volatile)**
   - Data stored in CPU registers.
   - Information stored in processor caches.
2. **Routing Table, ARP Cache, Process Table (volatile)**
   - Routing table: make determinations for where packets should be addressed
   - ARP Cache: maps IP addresses to their corresponding physical (MAC) addresses
   - Process table: running processes with their associated PID
3. **Memory (volatile)**
   - data and processes actively loaded into memory.
   - active network connections, listening ports

https://www.ietf.org/rfc/rfc3227.txt

Order of Volatility (2/2)

3. **Temporary File Systems (TMPFS) (volatile)**
4. **Data on hard disk (non-volatile)**
   - deleted files may be overwritten.
5. **Remote Logging and Monitoring Data (non-volatile)**
   - System logs, event logs, and application logs that record system activities, errors, and security events.

Order of Volatility (2/2)

6. **Physical configuration / Network topology (non-volatile)**
   - physical arrangement of the devices and connections in a network (type, number, and location of devices)
   - The way the devices are connected (type of connections, layout)
7. **Archival media (non-volatile)**
   - static data that has been written and read occasionally

Volatile Data Acquisition & Preservation

- Create a response tool kit.
- Don’t shutdown until completed the evidence collection.
  - Tools in external device – Dump stored in external drive
  - Adequate free space (pagefile, hiberfil, swapfile, memory dump).
- Don’t trust any program on system.
- Don’t run programs that modify the access time of all files on system.
- Always collect the volatile data first (order of volatility)
- Verify the acquisition after collection (Hash values).
- Never work on original evidence. Always work on a copy.
- Record Every Step.
- Always remember the chain of custody.

Volatile Data Acquisition (1/4)

- **System Information**.
- **Data to Collect**:
  - Hardware specifications (CPU model, RAM size, etc).
  - Operating system version and Build No.
  - Registered users/ Logged on accounts.
  - Computer name.
  - OS Configuration (Installed languages, Time zone, uptime info, updates & hotfixes, network configuration, etc).
- **Tools**:
  - SystemInfo, ipconfig \all, hostname
  - msinfo32 (built-in System Information tool).
  - Logon sessions, PsLoggedOn (SysInternals Suite)

Volatile Data Acquisition (2/4)

- **Process Enumeration**
- **Data to Collect:**
  - List of running processes and associated details (PID, memory usage, etc.).
  - Process handles and Dlls
  - Autoruns
- **Tools:**
  - Task Manager (built-in Windows tool).
  - Process Explorer, Pslist , Handle , Listdll, Autoruns, Procmon (Sysinternals Suite).

Volatile Data Acquisition (3/4)

- **Network State Examination**
- **Data to Collect**:
  - Active/Established network connections.
  - Listening ports.
- **Tools**:
  - Netstat, nslookup (built-in Windows command).
  - TCPView (Sysinternals Suite).

Volatile Data Acquisition (4/4)

- **System State Information**
- **Data to Collect**:
  - Open files.
  - Loaded drivers.
  - Active user sessions.
  - Clipboard Content
- **Tools**:
  - System Configuration (msconfig, built-in Windows tool).
  - Process Explorer, Autoruns, Listdll (Sysinternals Suite).
  - Last Activity View (Nir Soft Tools)

Memory Acquisition Process

- Determine the state of the machine
- Identify the operating system
- Insert acquisition medium
- Perform Volatile Memory Dump
  - Execute tool on the host machine
  - Store memory dump **directly** in the external forensic medium
- Collect SWAP, PAGEFILE.sys and system protected files
- Hash and verify the acquired files
- Create Investigator copies

Post Aquisition - Examination

- Extract information
- Tools for extraction:
  - Access Data FTK Imager
  - Magnet AXIOM
  - Volatility Framework (open source)

Need to know

- Risky yet provides crucial information about:
  - malware behaviour
  - dark web sessions
  - anti-forensics software usage
  - Passwords
  - clipboard stored data
- Minimal footprints and minimum system resources
- Requires close examination of the system stability
  - BOD crash

Non Volatile Data

- Information that persists across system reboots
- Acquired during static data acquisition.
- Essential for long-term storage/data retention
- Critical OS functions & configuration settings.
- Facilitates system recovery and continuity of operations.

Non Volatile Data Types in Windows Systems

- **Operating System Files** (DLLs, kernel components)
- **Registry (**Hierarchical database with OS config settings)
- **Boot Configuration Data (BCD)** (manages the boot process)
- **OS Files and Directories** (C:\Windows\)
- **Security Databases** (e.g, Active Directory)
- **User Data (**Documents, images, videos etc)
- **User Profiles (**preferences, app-specific data)
- **Event Logs** (record events, errors, activities)
- **Device Drivers** (software for graphic cards, network adapters, etc)
- **PageFile** (virtual memory offloaded from RAM)
- **Web browser cache** (local cache of browsers)

Non Volatile Data Acquisition

- **Methods of Acquisition:**
  - Disk Imaging
  - File-Level Backups
  - Registry Extraction
  - Event Log Retrieval
- **Tools for Non-Volatile Data Acquisition**:
  - FTK Imager
  - EnCase
  - Disk2vhd
  - Windows Backup and Restore
  - KAPE (Kroll Artifact Parser Extractor)
  - Velociraptor
- **Best Practices:**
  - Ensure Legal Authorization
  - Document Chain of Custody
  - Use Forensically Sound Tools
  - Maintain Data Integrity with Hashing

Forensic Imaging

- **Forensic image:** a bit-by-bit, sector-by-sector direct copy of a physical storage device, including all files, folders and unallocated, free and slack space.
  - Exact copy of the source device disk drive
  - Data cannot be accidentally changed
  - DD, AFF, E01 (most common)
- Tools
  - FTK Imager
  - DD (Disk Dump)

Drive Duplicator and Write Blocking

Drive Duplicator – Write Blocker

- **Definition**: Hardware device that is used to create exact copies (forensic images) of storage media, e.g. hard drives (HDDs), solid-state drives (SSDs), USB or other storage devices and media.
- **Bit-by-bit** duplication ensures an exact replica of the original drive.
  - Preserve the original state of the evidence.
  - Ensure data integrity during the duplication process.
  - Adheres to legal and procedural requirements for handling digital evidence.

Forensic Imaging Process

1. Connect the Write-Blocking Device
2. Check for disk encryption (EDD)
   - Encrypted (Veracrypt, Bitlocker) -> Live acquisition of unencrypted data (KAPE)
   - Unencrypted -> Proceed with caution
3. Select the Imaging Tool
4. Configure Imaging Options (source drive to image, destination path, image format)
5. Initiate the Imaging Process
6. Verify Image Integrity (hash)

VM Imaging

- VMware
  - .vmdk file
- VirtualBox
  - .vdi file
- Analysis
  - .vmdk → Opens directly to the FTK imager
  - .vdi disks → converted and mounted

    "VboxManage.exe convertfromraw image.dd test.vmdk --format vmdk"

KAPE (Kroll Artifact Parser and Extractor)

What is KAPE?

- Open-source digital forensic tool designed to streamline and automate the process of data acquisition and artifact extraction from digital devices.

- Artifact Parsing
- Modularity and Extensibility
- Automation Capabilities
- Cross-Platform Support

Examination/Artifact categorization

SANS Windows artifacts categorization (1/2)

Category Name	Artifacts
System Information	OS Version, Computer Name, System Boot & Autoruns, System Last Shutdown Time
Application Execution	User Assist, Windows 10 Timeline, Shimcache, Jump Lists, Amcache.hve, System Resource Usage Monitor (SRUM), BAM/DAM, Last-Visited MRU, Prefetch, etc.
File/Folder Opening	Open/Save MRU, Recent Files, Jump Lists, Shell Bags, Shortcut (LNK) Files, Last-Visited MRU, IE|Edge file://
Deleted File or File Knowledge	Windows Search Database, Thumbscache, Thumbs.db, IE|Edge File://, Search–WordWheelQuery, Recycle Bin, User Typed Paths
Cloud Storage	OneDrive, Google Drive, Box Drive, Dropbox

SANS artifacts categorization (2/2)

Category Name	Artifacts
Network Activity/ Physical Location	Timezone, Cookies, Network History, WLAN Event Log, Browser URL Parameters, System Resource Usage Monitor (SRUM), Network Interfaces
External Device/USB usage	Key Identification, First/Last Times, User, PnP Events, Volume Serial Number, Drive Letter and Volume Name, Shortcut (LNK) Files.
Account Usage	Last Login and Password Change, RDP Usage, Services Events, Logon Event Types, Authentication Events, Success/Fail Logons, Cloud Account Details, User Accounts
Browser Activity	History and Download History, Bookmarks, Media History, Stored Credentials, Browser Downloads, Cache, Cookies, Session Restore, Extensions, Auto-Complete Data etc.

https://www.sans.org/posters/windows-forensic-analysis/

Challenges in Windows Forensics

Challenges in Windows Forensics

1. **Encryption and Data Protection**
   - specialized tools and techniques /encryption keys and certificates
2. **Anti-Forensic Techniques**
   - employment of advanced recovery and analysis techniques.
3. **Volume Shadow Copies**
   - proficiency in navigating and extracting data from VSC
4. **User and Application Activity Logs**
   - thorough analysis
5. **Cloud and Online Data**
   - employ cloud forensics techniques

Labs

- Lab #1: Run Kape to acquire non-volatile data
- Lab #2: Check disk encryption with EDD
  - Run the command .\EDD.exe, and select "I Accept" on the window that opens
  - Review the result.
- Lab #3: Explore forensic images with FTK Imager

Thank you for your patience