COMPUTER HACKING FORENSIC INVESTIGATOR

Jan Marek | Cyber Rangers

OSEP | PNPT | OSCP | eCPPT | CEH | CHFI | CASP+ | Pentest+ | CEI | MVP | MCT | MCC | MCSA | MCSE

Co-founder | Red Teamer | DFIR

jan@cyber-rangers.com | www.cyber-rangers.com

DIGITAL FORENSICS INTRODUCTION

MODULE 0: COURSE INTRODUCTION

WHAT ARE YOUR EXPECTATIONS?

WHAT DO YOU WANT TO LEARN? WHAT'S YOUR CURRENT KNOWLEDGE?

FACILITIES

- Training hours
- Meals
- Phones & Messages
- Online presence
  - Please mute
  - Would be great to see you, but not required
  - Ask questions directly or “Raise your hand”
- Focus on the training content
- Practice, practice, practice

AUDIENCE AND REQUIREMENTS

- Already experienced in Windows operating systems
- Strong security background
- Familiar with Incident Response

COURSE MATERIALS

- PowerPoint slides
- Recommended Reading

DIGITAL FORENSICS INTRODUCTION

MODULE 1: CYBERCRIME AND INVESTIGATIONS

DIGITAL FORENSICS IS A DISCIPLINE OF FORENSIC SCIENCE, WHICH IS THE RECOVERY AND INVESTIGATION OF ARTIFACTS FOUND IN DIGITAL DEVICES, OFTEN IN RELATION TO A COMPUTER CRIME.

WHAT -> WHERE -> WHEN -> WHO -> HOW

ATTACK TYPES

- Internal attacks
  - Insider Threat
  - Physical Access available
  - Internal Processes known
  - Network Access available
- External attacks
  - Automated malware
  - APTs
  - Malicious Actors
  - Script Kiddies

DIGITAL EVIDENCE

- Any digital information that is stored, transmitted or produced from electronic devices and/or software
- Examples
  - Digital pictures
  - Print logs saved on printers
  - Web browser temporary files
  - Email messages
  - Deleted files
- is circumstantial
- is fragile
  - and usually volatile
- Locard's exchange principle

PROPERTIES OF DIGITAL EVIDENCE

- Believable
  - the judge is BFU
- Admissible
  - Accepted in a court
  - Relevant (prove or disapprove a hypothesis related to the case)
  - Reliable
  - Competent (must have been acquired through legal ways and not violate the confidentiality of an information protected by law or constitution)
- Authentic
  - Relevant to the case
  - Chain of Custody (CoC)
- Complete
  - No missing information

VOLATILE VS. NON-VOLATILE DATA

- volatile data examples
  - system time, logged-on users, open files, running processes, TCP connections, clipboard contents, services and drivers, command history, ...
  - encryption keys and passwords
    - from memory, or non-volatile storage
- non-volatile data examples
  - files and databases, hidden files and slack space, swap files, hidden partitions, registry settings and data, event logs, ...
  - browser history, cloud storage client (OneDrive, GoogleDrive, ...), installed applications, installed malware, installed rootkit, ...

CYBERCRIME CHALLENGES

- Time and speed
- Dynamic and volatile nature of evidence
- Evidence size and distribution
- Anti - digital forensics (ADF)
  - steganography, slack space, bad sectors, inter-partition space, …
- Global origin and difference in laws
  - jurisdiction, attribution
  - due care
- Legal
- Privacy
- Circumstantial essence of digital evidence

INVESTIGATION TYPES

- Administrative investigation
  - non-criminal
  - government agency internally
  - disciplinary action on employees
- Civil/tort cases
  - supporting civil claims and induce settlement
  - searches voluntary
  - monetary compensations and no jail
  - poor chain of custody
- Criminal investigation
  - law enforcement agencies
  - standard forensic processes
  - court's warrant for seizures
  - formal reports required
  - fine and/or jail

WARRANTED OR WARRANTLESS SEIZURE

- warranted seizure
  - exact detailed specification what and why
  - must not collide with rights and privacy of other subjects
- warrantless seizure
  - arranged on good grounds with the company/employer/ISP/cloud provider
  - faster equipment returns
  - or only data extracted by the third-party
    - possible court testimony

PRIVACY ISSUES

- charges against unlawful search and seizure
- keep anonymity/privacy in internal investigations
  - reasonable expectation of privacy
  - reasonable expectation of work-related activities
    - company devices vs. BYOD

RULES OF INVESTIGATION

- record any changes to scene and evidence
- chain of custody
- store securely
- set and comply with your own standards for the procedures
- evidence should be strictly related to the incident
- use recognized tools

RISK ASSESSMENT AND IMPACT OF FORENSIC INVESTIGATION

- long business disruptions
- replacements of collected hardware
- returns into the production
  - from the lab, policy custody
  - cleaning or physical destruction
- privacy issues with employees

PHASES

- pre-investigation
  - computer forensics lab
  - tools and processes
- investigation
  - acquisition
  - preservation
  - analysis
- post-investigation
  - documentation
  - adequate and acceptable to target audience
  - report

INVESTIGATION PROCESS

1. First response
2. Search and seizure
3. Evidence collection
4. Securing of the evidence
5. Data acquisition
6. Data analysis
7. Evidence assessment
8. Documentation and reporting
9. Testimony as expert witness

NIST FORENSIC TIMELINE

- Collection
- Examination
- Analysis
- Reporting
- After Action Review

- Media -> Data -> Information -> Evidence

DIGITAL FORENSICS INTRODUCTION

MODULE 2: EVIDENCE AND CRIME SCENE

ORIGINAL EVIDENCE VS. COPY

- best evidence rule
  - prevent an alteration of digital evidence
- court can accept copy if original evidence was destroyed
  - due to fire/flood
  - due to normal course of business
  - in possession of a third party
- original evidence vs. primary vs. secondary disk images

HEARSAY

- somebody says he/she heard something about something else
- documentation
- former testimony is not hearsay

CHAIN OF CUSTODY

- It is a form that is used to keep track of the evidence since it was acquired until the finish of the analysis
- What, where, when, by whom, transfers
- Marking evidence bags
  - pre-agreed and documented format
- Content
  - What is the evidence?
  - How the evidence was acquired?
  - When the evidence was acquired?
  - Who acquired the evidence?
  - Where the evidence was stored?
  - And any other action that was performed on the evidence.

NOTES

- consent, acceptable-use policy, activity monitoring
- jurisdiction
- warrants
  - electronic devices search warrant
  - service provider search warrant
- preliminary interviews
  - purpose of the system and current work
  - passwords, social network accounts, off-site storage, unique security schemes or destructive devices
  - backups
- witness signatures + clear understanding
- health and safety issues

ISOLATING ELECTRONIC SYSTEMS

- unplug internet cables or close connectivity?
- unplug cables from the other ports of switches?
  - quarantine VLAN?
- unplug the device or stop WiFi?
- shutdown the device?

WARRANTLESS SEIZURE

- When destruction of evidence is imminent, a warrantless seizure of that evidence is justified if there is probable cause to believe that the item seized constitutes evidence of criminal activity.

- Agents may search a place or object without a warrant or, for that matter, without probable cause, if a person with authority has consented.

TRANSPORTING AND STORING ELECTRONIC EVIDENCE

- Avoid computers upside-down
- Avoid electromagnetic sources
  - Faraday Bags
- Safe areas
  - not leaving in vehicles
- Heat/cold/humidity/vibrations
- Back-seat instead of trunk

DIGITAL FORENSICS INTRODUCTION

MODULE 3: FIRST RESPONSE

FIRST RESPONDER

- Who
  - law enforcement officer
  - IT/ICT administrator
  - CIRT member
  - On-site User
- Goal
  - To protect, integrate and preserve the evidence

TASKS AND TOOLS

- Stop and think
- Identify and protect crime scene
- Preserve as much temporary and fragile evidence as possible
- Collect all information about the incident
- Document the findings
- Optionally package and transport the electronic evidence

- PowerForensics
- RedLine

WHAT NOT TO DO

- Recover data
- Do not forget about other hardware items
  - copiers, desktop switches, chain locks, keyboard/mouse cord, flash drive, photo-frames, cabling, ...
  - non-electronical evidence such as tables, chairs, ...
- Let others to the scene
- Forget about environmental or health hazard

DOCUMENTING THE SCENE

- Photographing and video shooting
  - 360-degree
  - from entire scene to details
  - use numbered markers
  - cabling and other non-visible areas
  - trash bins, paper shelves, ...
- Notes
  - power state of electronic devices
  - persons in the scene

DIGITAL FORENSICS INTRODUCTION

MODULE 4: COLLECTION AND ANALYSIS OF DIGITAL EVIDENCE

PREPARE FOR THE INVESTIGATION

FORENSICS LAB

- Secured
  - badges, cameras, guards, access log, one entrance, ...
  - fire suppression, humidity, ...
- Software and hardware from trusted vendors
  - inventory with hashes
- Use workstations, laptops, servers, NAS,...
- LAN and internet connectivity
  - air-gap
- safe lockers and shelves
- work area
  - mixing of evidence and results
  - chain of custody
- removable media for evidence collection, storage and transport
- digital cameras and video recorders
- everything documented and trusted
- everything tracked at anytime

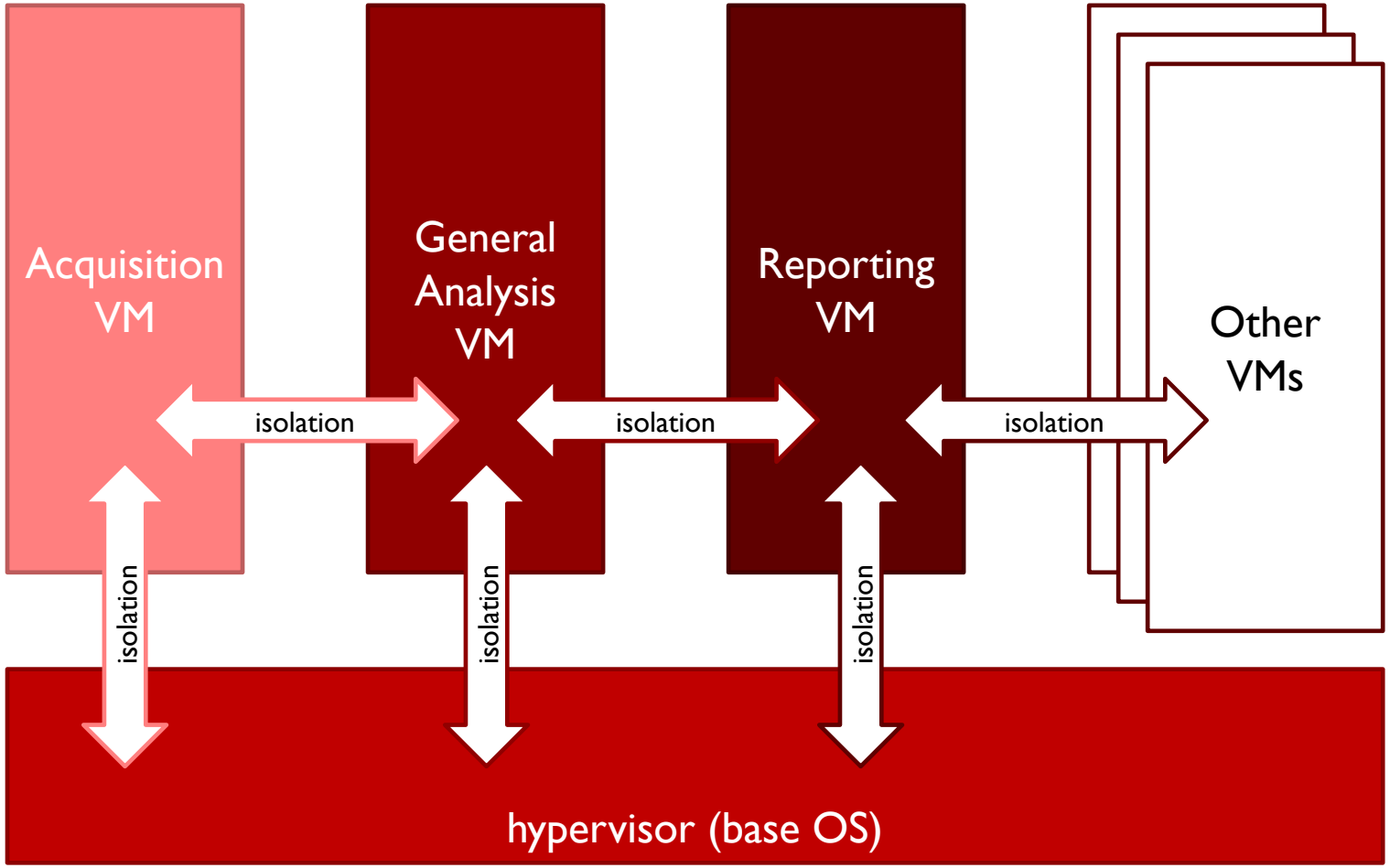
FORENSIC WORKSTATIONS

- trusted installation sources
  - hash inventory stored separately
- do not update images
- cleaning and sanitizing after every investigation
  - US DoD 5220.22-M (3 passes, 0/1/rnd)
  - German VSITR (7 passes, 0/1/0/1/0/1/rnd)
  - SSD?, format?, SDELETE, TRIM/UNMAP
- virtualization
  - one case at a time

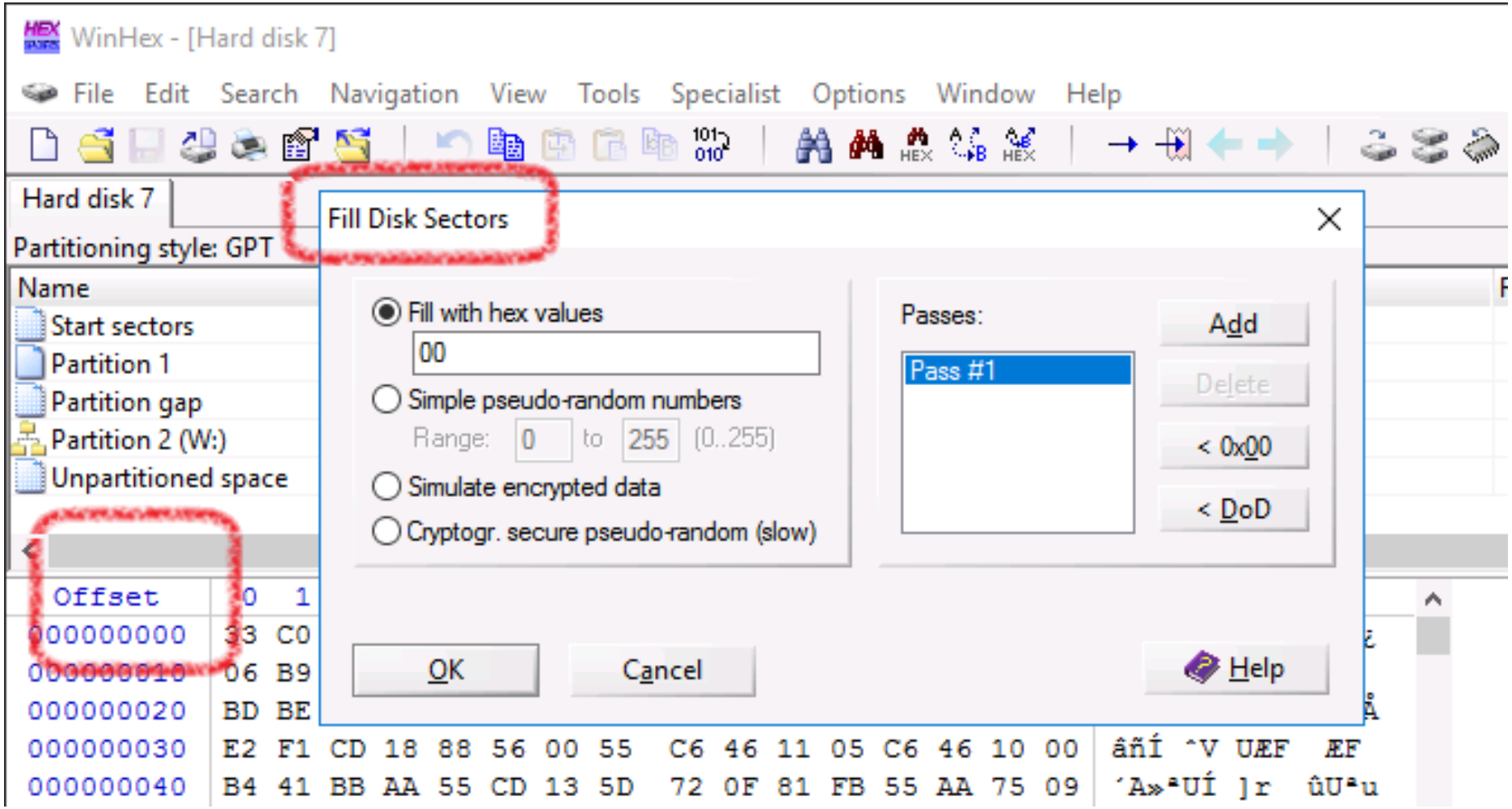
- removable media and disk imaging tech, cameras, ...
  - cleaning, documentation, tracking, ...

- there is no exact court list of forensic lab/tools etc. only a trusted accreditation
  - ISO 17025
  - ASCLD/LAB (American Society of Crime Laboratory Directors)

USE VIRTUALIZATION FOR FORENSIC LAB



ZEROING DISK WITH WINHEX



COLLECT THE EVIDENCE

COLLECTION (ACQUISITION) IS THE PROCESS OF OBTAINING A FORENSIC SOUND IMAGE OF THE EVIDENCE TO BE ANALYZED.

COULD WE COLLECT VOLATILE EVIDENCE?

- Nothing
- Mouse, keyboard
  - be careful about some complex actions
- Introducing any tools on removable device or from network
  - leave them there and collect as evidence
- Mobile phone click-through bench

- Video shoot everything

PHYSICAL EVIDENCE COLLECTION

- Powered off devices
  - Leave it off -> Put it in a container -> Seal the container with tape -> Mark the tape
- Power off devices
  - standard shutdown procedure
  - unplugged batteries if possible
- Antistatic bags and pads
- Black-hole bags
  - remote-wipe
- Cables, peripherals
- Papers
- Trash bin items
- Maintain temperature and humidity

COLLECTING EVIDENCE FROM SOCIAL NETWORKS AND SERVICE PROVIDERS

- Warrants
- E-discovery by the service provider
  - standard file formats
  - trusted by no-motive, no-conflict-of-interest
- Social network data extraction from "friends" or other public profiles
  - may require expert witness to confirm the behavior
  - documentation/witness from the social network provider

- Communication logs, messages, photos, friend reactions
  - trusted time synchronization?

E-DISCOVERY NOTES

- let them verify time synchronization
  - + timezone
- zip/encrypt
  - single file to send
- compute hash
  - and provide (signed) statement (email, paper)

```
certutil -hashfile
```

NOTES

- No unauthorized users
- Forensically clean devices used to obtain the evidence
- Write-protection
- Primary image -> analyze copies

IMAGE CREATION

- Any suitable solution trusted by the expert examiner
- Write-protection and write-blockers
- Bitwise copy, Bit-by-Bit copy, Sector-by-sector copy
- Hash creation and integrity verification

- Tools
  - WinHex
  - AccessData FTK Imager
  - EnCase
  - Paraben
  - dd, dcfldd, dc3dd, guymager

DISK (PHYSICAL OR VHDX) SECTOR SIZES

- physical sector size
  - physical hardware storage unit
  - 512B or 4096B (4K disk)
- logical sector size
  - what an operating system works with
  - logical 512B on physical 512B
  - logical 4096B on physical 4096B (4K drive)
    - compatibility with older applications?
    - ok for normal file read/writes which use cluster size (NTFS defaults 4kB)
  - logical 512B on physical 4096B (512e emulation drive)
    - some performance spent in the controller

VHDX SECTOR SIZES AND BLOCK SIZE

```
New-VHD -LogicalSectorSizeBytes `
        -PhysicalSectorSizeBytes `

        -BlockSizeBytes
```

- PhysicalSectorSizeBytes
  - works on 512B physical disks as well
  - aligned correctly by Windows 2016+ even on 512B physical disks
  - if ever hosted on 4K use 4K, think about the future
- LogicalSectorSizeBytes
  - what the virtual OS will see
  - compatibility with low-level applications?

- BlockSizeBytes
  - only differencing and dynamic disks
  - unit of the "different" or "dynamic allocation"
  - default 32MB

DISK IMAGE FORMATS

- DD
  - raw disk data
  - no header
  - no 512/4K sector info
- E01
  - header + info
  - compressed

- VHD, VHDX
  - Hyper-V virtualization - boot, attach
  - Windows 7/2008+ can mount as a disk (R/O possible)

USE VIRTUALIZATION FOR FURTHER ANALYSIS

- Isolates the possibly insecure environment
- Running imaged OS live (copy)

HYPER-V VM FROM DISK IMAGES

- original boot UEFI/BIOS
  - VM generation 2 (UEFI) resp VM generation 1 (BIOS)
    - note UEFI Secure Boot state on the real hardware
- OS Vista/2008/7/2008R2+
  - boot always (basic SCSI/IDE controller drivers always loaded)
  - no NIC (original device and config kept in registry)
  - deactivated
- image -> .VHDX
  - 512 B vs. 4096 B sector

- XP/2003
  - VM generation 1 + offline IDE controller enable in registry

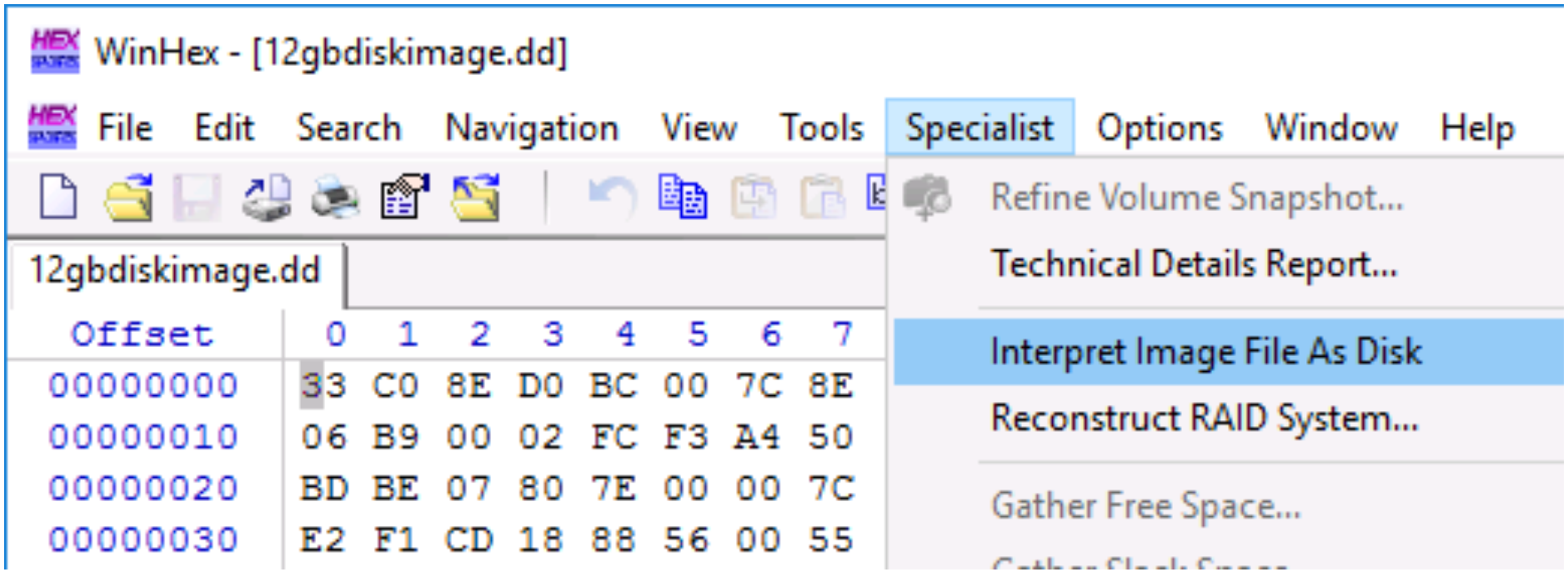
WINDOWS FORENSIC ENVIRONMENT

- HKLM\System\CurrentControlSet\Services
  - MountMgr
    - NoAutoMount = DWORD = 1
  - PartMgr\Parameters
    - SanPolicy = DWORD = 3

- USB flash devices cannot be mounted from diskmgmt.msc
  - DISKPART
  - LIST DISK
  - SELECT DISK
  - ATTRIBUTES DISK SET READONLY
  - ONLINE DISK

WINHEX INTERPRET IMAGE FILE AS DISK

- Open the first .DD or .001 image file
- select Specialist - Interpret Image File as Disk



ANALYZE THE EVIDENCE

SCIENTIFIC METHOD

- The Scientific Method is a body of techniques for:
  - Investigating phenomena
  - Acquiring new knowledge
  - Correcting and integrating previous knowledge

- The Scientific Method is the investigator's most useful ally in his/her mission to present reliable evidence.

- OBSERVE -> COLLECT DATA AND FACTS -> BUILD HYPOTHESIS BASED ON DATA COLLECTED

MULTIPLE DATA TYPES

- Active data (OS, Word, browser)
- Archive and backup data
- Hidden data
  - Metadata
    - Most valuable piece of evidence
  - Residual data
    - Deleted objects remain on the drive until overwritten
  - Replicant data
    - Temporary copies of open files (Word, Windows 11 notepad AutoSave)

ANALYSIS TOOLS

- Multiple single-purpose tools
  - Nirsoft
  - PowerShell
  - Sysinternals
  - …
- Timeline and data analysis
  - SOF-ELK®
  - Autopsy®
  - Log2Timeline
  - SIFT Workstation
  - EnCase
  - AccessData FTK
  - Flare-VM

DIGITAL FORENSICS INTRODUCTION

MODULE 5: ANTI-FORENSICS TECHNIQUES

ANTI-FORENSICS TYPES

- Evidence destruction
- Evidence hiding
- Evidence source elimination
- Evidence tampering

- To increase the examiner’s time
- Overwhelm the logging facility
- Run code on the forensic appliance
- Break the investigative software
- Leak info about the investigator
- Implicate investigator

ANTI-FORENSICS TECHNIQUES

- Disabling logging
- Data/File Deletion and Artifact Wiping
- Password Protection
- Steganography
- Data Hiding in File System Structures
- Trail Obfuscation
- Overwriting Data/Metadata, Changing timestamps
- Encryption
- Rootkits
- Spoofing
- Tunneling and Onion Routing
- Exploiting Forensics Tool Bugs

ANTI-FORENSICS TOOLS

- Slacker — Hides data in slack space
- FragFS — Hides in NTFS Master File Table
- RuneFS — Stores data in “bad blocks”
- KY FS — Stores data in directories
- Data Mule FS — Stores in node reserved space

- Live CDs
- Virtual Machines
- Memory Injections and syscall proxying
- Compression bombs

DIGITAL FORENSICS INTRODUCTION

MODULE 6: REPORT WRITING

TIPS AND RULES

- No “right” format! Create your own template, suitable for your company!
- Time, time and time! And use the same consistent format (MM.DD.YYYY vs. DD.MM.YYYY)
- Don’t copy from old reports!
- Create report during the investigation, not in the end!
- Investigators analysis and reasoning what gives the evidence its value!
- Don’t use phrases like “we are sure” or “we are certain”!
- Organize the content!
- Use the past tense!
- Avoid using exhaustively long phrases!
- Report what you have not done!
- Avoid using jargons!
- Avoid inconsistency of content! (use the same term for the same thing; use the same format/font/..)

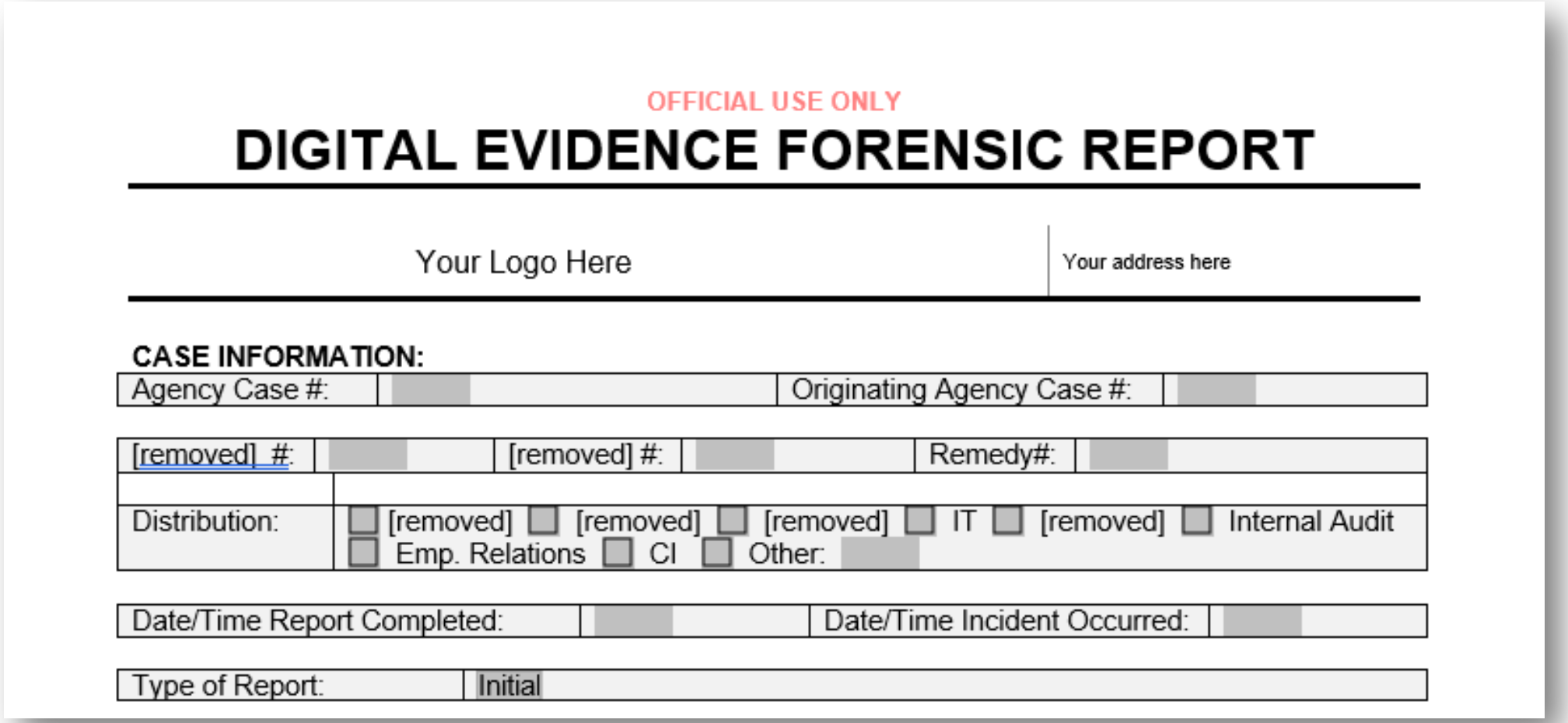
STRUCTURE

- Cover page
- Table of content, list of tables and figures
- Executive summary (overall high-level description and the most important findings)
- Objective (client requests, reasons for investigation, goals)
- Evidence (serial numbers, hashes, investigator name and ID, CoC)
- Analysis (tools used, processes, approaches)
- Reconstruction of the crime (timeline)
- Conclusion (list and summarize the most important parts of the report)
- References
- Acronyms
- Appendices (log files, large files, testimonies)
- Last Page info

ADDITIONAL CHAPTERS

- First responders and witnesses list and their testimonies
- Crime scene description
- Chain of custody

REPORT EXAMPLE



OFFICIAL USE ONLY

DIGITAL EVIDENCE FORENSIC REPORT

Your Logo Here	Your address here

CASE INFORMATION:

Agency Case #:		Originating Agency Case #:			
[removed] #:		[removed] #:		Remedy#:	
Distribution:	☐ [removed] ☐ [removed] ☐ [removed] ☐ IT ☐ [removed] ☐ Internal Audit ☐ Emp. Relations ☐ CI ☐ Other:				
Date/Time Report Completed:		Date/Time Incident Occurred:			
Type of Report:	Initial				

Q & A

COMPUTER HACKING FORENSIC INVESTIGATOR

Jan Marek | Cyber Rangers

OSEP | PNPT | OSCP | eCPPT | CEH | CHFI | CASP+ | Pentest+ | CEI | MVP | MCT | MCC | MCSA | MCSE

Co-founder | Red Teamer | DFIR

jan@cyber-rangers.com | www.cyber-rangers.com